UNC SCHOOL OF GOVERNMENT

2022 Spring Public Defender Attorney & Investigator Conference INVESTIGATOR TRACK (May 11 & 13)

May 11-13, 2022 – Asheville, NC

ELECTRONIC CONFERENCE MATERIALS*

*This PDF file contains "bookmarks," which serve as a clickable table of contents that allows you to easily skip around and locate session documents within the larger file. A bookmark panel should automatically appear on the left-hand side of this screen. If it does not, click the icon—located on the left-hand side of the open PDF document—that looks like a dog-eared page with a ribbon hanging from the top.

UNC | SCHOOL OF GOVERNMENT

2022 Investigator Spring Conference

May 11-13, 2022
Asheville, NC

Sponsored by the UNC-Chapel Hill School of Government,
North Carolina Office of Indigent Defense Services,
North Carolina Association of Public Defenders, &
North Carolina Association of Public Defender Investigators

****

INVESTIGATOR AGENDA (Updated)

(This conference offers at least 6 hours with the North Carolina Private Protective Services Board)

WEDNESDAY, MAY 11

Attorney Track Room:

11:00-12:20 p.m.	**Check-in**
12:20-12:30 p.m.	**Welcome**

Investigator Track Room:

12:45-1:45 p.m.	**Strategies for Working with Attorneys** [60 min.] Fred Friedman, Attorney and Professor, University of Minnesota Duluth, MN
1:45-2:15 p.m.	**Court and Testimony: Roundtable Discussion** [30 min.] Timothy Heinle, Civil Defender Educator UNC School of Government, Chapel Hill, NC
2:15 p.m.	*Break*

Attorney Track Room:

2:45-4:00 p.m.	**Criminal Case and Legislative Update** [75 min.] Phil Dixon, Teaching Assistant Professor UNC School of Government, Chapel Hill, NC

Investigator Track Room:

4:00-5:00 p.m.	**Blunt Force Trauma** [60 min.] Tara Godoy, BSN, RN, Chief Forensic Nurse, Godoy Medical Forensics, Inc. San Francisco, CA
5:00 p.m.	*Adjourn*
5:15 p.m.	**Optional Social Gathering** – *Details to be announced.*

THURSDAY, MAY 12

Investigators are invited to join any sessions of interest from the misdemeanor or felony tracks. Please see the attorney program agenda for more information.

FRIDAY, MAY 13

Attorney Track Room:

9:00-10:00 a.m.	**Challenging Digital Surveillance** [60 min.] Larry Daniel, Technical Director – Digital Forensics Practice, Envista Forensics, Morrisville, NC

Investigator Track Room:

10:05-11:05 a.m.	**They Have No Evidence, and She is Not Coming to Court: Investigating Allegations of Child Sex Offenses.** [60 minutes] Susan Weigand, Special Felonies Chief Melani R. McIntosh, Investigator Mecklenburg County Office of the Public Defender Charlotte, NC
11:05-11:50 a.m.	**Ethical Considerations for Investigators** [45 minutes] Fred Friedman, Attorney and Professor, University of Minnesota Duluth, MN
11:50 a.m.-12:05 p.m.	**NC Public Defender Investigator Business Meeting** [15 mins] Marvin Jeffcoat, Chief Investigator, Mecklenburg County Office of the P.D. Charlotte, NC
12:05 p.m.	*Adjourn* -- The Honorable Justice Anita Earls will be presenting 'A View from the North Carolina Supreme Court' from 12:15 p.m. to 12:45 p.m. in the attorney track room. Investigators are welcome to attend.

STRATEGIES FOR INVESTIGATORS WORKING WITH PUBLIC DEFENDERS

1) EARN THEIR TRUST AND RESPECT

2) TWO WAY STREET

3) CONFIDENTIALITY AND INTEGRITY ARE EVERYTHING

4) INSTINCTS

5) INITIATIVE

6) CONTACTS WITH CLIENTS

7) KNOW YOUR STATE'S RULES OF PROFESSIONAL CONDUCT

8) KEEP NOTHING FROM THE ATTORNEY ASSIGNED THE CASE

9) WHEN YOU ARE ASSIGNED A CASE, REQUIRE SPECIFIC GOALS AND EXPECTATIONS

10) AGREE ON WHETHER YOUR REPORT IS TO BE WRITTEN OR NOT, TAPED, OR NOT.

11) USE A FORM THAT AS A MINIMUM INCLUDES THE CLIENT'S NAME ADDRESS, FILE NUMBER, ALL CONTACT INFORMATION OF EVERYONE YOU ARE TO INVESTIGATE, SPECIFIC ASSIGNMENT, CHARGING DOCUMENT, DATE CASE CHARGED OUT, DATE OF ASSIGNMENT, DATE REPORT NEEDED, AND DATE OF TRIAL.

12) OBTAIN AND READ ALL DISCOVERY

Phil Dixon
dixon@sog.unc.edu
UNC School of Government©

2022 Annual Spring Public Defender Conference
Criminal Law Update
May 11, 2022
Renaissance Hotel, Asheville, NC

Cases covered include published criminal and related decisions from the U.S. Supreme Court, the Fourth Circuit Court of Appeals, and North Carolina appellate courts decided between May 4 and October 5, 2021. Summaries are prepared by School of Government faculty and staff. To view all of the case summaries, go the Criminal Case Compendium. To obtain summaries automatically by email, sign up for the Criminal Law Listserv. Summaries are also posted on the North Carolina Criminal Law Blog.

Warrantless Stops and Seizures

(1) In the absence of a plea arrangement, a defendant is not required to give notice of his intent to appeal to pursue right to appeal denial of motion to suppress; (2) Officer did not have reasonable suspicion to stop the car in which the defendant was traveling based on its transporter license plate, and officer's mistake of law regarding license plate was not objectively reasonable.

State v. Jonas, ___ N.C. App. ___; 867 S.E.2d 563; 2021-NCCOA-660 (Dec. 7, 2021). In this Cabarrus County case, the defendant was convicted of possession of a Schedule II controlled substance based on 0.1 grams of methamphetamine found in a backpack in the trunk of a vehicle in which the defendant was a passenger. The defendant moved to suppress the evidence on the basis that it was seized in connection with a traffic stop that was not supported by reasonable suspicion. The trial court denied the motion. Defendant pled guilty, without a plea arrangement with the State, and appealed.

(1) G.S. 15-979(b) provides that an order finally denying a motion to suppress may be reviewed upon an appeal from a judgment of conviction, including a judgment entered upon a plea of guilty. The North Carolina Supreme Court held in *State v. Reynolds*, 298 N.C. 380 (1979), that when a defendant intends to appeal from the denial of a motion to suppress pursuant to G.S. 15A-979(b), the defendant must give notice of that intention to the prosecutor and the court before plea negotiations are finalized. Absent such notice, the right to appeal is waived. The Court of Appeals held that the *Reynolds* notice requirement did not apply in the instant case because the defendant did not plead guilty as part of a plea arrangement. Thus, the defendant had a statutory right to appeal without having provided notice to the State and the trial court before entering his guilty plea.

(2) The officer who stopped the car in which the defendant was traveling testified that he stopped the car because it emerged from the empty parking lot of a closed business, a trailer had recently been stolen in that area, and the car was equipped with transporter plate, which the officer had never seen placed on a vehicle other than a truck. The Court of Appeals noted that, despite the officer's belief to the contrary, G.S. 20-79.2 "clear[ly] and unambiguous[ly]" permits transporter plates to be used on motor vehicles generally, not just trucks. Though the Fourth Amendment tolerates objectively reasonable mistakes, the Court concluded that the officer's mistake about the transporter plates was not objectively reasonable because the statute was not ambiguous. Thus, the officer's belief regarding

the transporter plates could not support reasonable suspicion. The Court determined that the additional facts that the business was closed and there was a recent trailer theft in the area were insufficient to support reasonable suspicion. Accordingly, the Court held that the trial court erred in denying the defendant's motion to suppress. It reversed the trial court's order and remanded the case to the trial court for entry of an order vacating the defendant's guilty plea.

Reasonable suspicion of trespassing, impaired driving, and illegal parking supported stop of defendant parked in high school parking lot during school hours, even without presence of crossbow in backseat; crossbow alternatively provided reasonable suspicion and any mistake of law as to the legality of the weapon on school property was reasonable

U.S. v. Coleman, 18 F.4th 131 (Nov. 9, 2021). A school official in the Western District of Virginia noticed a man parked in the high school's parking lot one morning as the school day began. The man appeared to be asleep in his car and had a crossbow in the backseat. The car was running, had its brakes on, and was parked partially in a lane of travel. The school resource officer responded. As the deputy pulled behind the defendant's car, the defendant began to drive away. The deputy then stopped the car. He saw the crossbow upon making contact and asked the defendant about other weapons. The defendant acknowledged a gun in the car, and the deputy asked him out of the car. As the defendant exited, the deputy noticed apparent marijuana inside. The defendant appeared tired and submitted to field sobriety testing. The car was searched and a gun, baggies, a scale, and methamphetamine was discovered. The defendant was charged with various federal drug and gun offenses and moved to suppress, arguing that the stop was unjustified because possession of a crossbow on school grounds is not illegal in Virginia. The district court denied the motion, finding that the deputy had reasonable suspicion to stop the vehicle based on the corroborated report from the school official about a sleeping man on school grounds with a weapon and the defendant's driving away upon the deputy's approach. It further found that any mistake by the deputy about the legality of the crossbow on school grounds was an objectively reasonable mistake of law under *Heien v. N.C.*, 574 U.S. 54 (2014). The defendant was convicted at trial and sentenced to 211 months.

On appeal, a unanimous panel of the Fourth Circuit affirmed. Even without the crossbow, the deputy had reasonable suspicion to stop the defendant's car for suspicion of trespassing on school grounds, impaired driving, and illegal parking. In the alternative, the court found that the crossbow provided reasonable suspicion by itself or in combination with other factors. The deputy was not required to ignore the presence of a strange man with a weapon on school grounds, whether or not the crossbow was legal to possess. "Here, as in *Terry*, the underlying behavior does not have to be illegal for us to conclude that Deputy Johnson had reasonable suspicion to stop Coleman." *Id*. at 15. The district court's denial of the motion to suppress was therefore affirmed.

Though none of the circumstances alone would satisfy constitutional requirements, together they provided officers with reasonable suspicion to stop the defendant

State v. Royster, ___ N.C. App. ___; 867 S.E.2d 204; 2021-NCCOA-595 (Nov. 2, 2021). In this Forsyth County case, the defendant was charged with possession of a firearm by a felon, several drug crimes including trafficking opium or heroin by possession, possession of a weapon on school property, and attaining the status of habitual felon after an investigatory stop on school grounds stemming from an anonymous tip. The police received a detailed anonymous report saying that a black male named Joseph Royster who went by the nickname "Gooney" had heroin and a gun in the armrest of his black Chevrolet Impala with a specific license plate number, that he was wearing a white t-shirt and blue jeans, had gold

teeth and a gold necklace, and that he was parked near South Fork Elementary School. An experienced officer who received the tip searched a police database that showed a person by that name as a black male with gold teeth and a history of drug and weapon charges. Officers went to the named elementary school, saw a vehicle with the specified license plate number matching the description in the tip in the parking lot, and eventually saw a person matching the description in the tip return to the vehicle. When that person quickly exited the vehicle, reached back into it and turned it off, began to walk away from officers and reached for his waistband, officers frisked him for weapons and detained him for a narcotics investigation. The defendant moved to suppress, arguing that officers did not have reasonable articulable suspicion for the stop. The trial court denied the motion and the defendant pled guilty.

On appeal of the denial of the motion to suppress, the defendant argued that the anonymous call did not demonstrate sufficient reliability. The Court of Appeals noted that the anonymous call itself merely provided identifying information, and there was nothing inherent in the tip itself that would give officers reasonable suspicion to make the stop. The Court rejected the State's argument, based on *Navarette v. California*, 572 U.S. 393 (2014), that the caller's use of a phone to make the tip sufficiently bolstered its reliability, because there was no evidence as to whether the caller used 911 or a non-emergency number or otherwise preserved her anonymity. The Court was likewise unpersuaded that the caller's use of the defendant's nickname showed a level of familiarity with the defendant that made the call sufficiently reliable in its assertion of illegality. Thus, the anonymous call itself was insufficient to provide officers with reasonable articulable suspicion.

Looking at the totality of the circumstances, however, the Court concluded that officers did have reasonable articulable suspicion. The defendant's actions in exiting the vehicle, reaching back into it, walking away from officers, and reaching for his waistband demonstrated evasive behavior that went beyond merely walking away from officers and supported a finding of reasonable suspicion for the stop. Additionally, the caller's allegation that the defendant was in possession of a firearm, coupled with his presence on school grounds and his prior criminal record obtained through the police database gave officers reasonable suspicion that he was in possession of a firearm, and that he was thus violating the criminal statute prohibiting the possession of a firearm on school property. As a result, the stop was deemed proper, and the Court concluded that the trial court did not err in denying the defendant's motion to suppress.

(1) Stop was not unreasonably extended where officer had not yet determined whether to charge the defendant; (2) Consent was freely and voluntarily given

State v. Jordan, ___ N.C. App. ___; 2022-NCCOA-214 (April 5, 2022). Law enforcement in Guilford County received information that the defendant was selling drugs from his girlfriend's apartment. They conducted a controlled buy at the location with the help of an informant, who identified the defendant as the seller. Police were later surveilling the home and saw the defendant leave with his girlfriend in her car. The car was stopped for speeding 12 mph over the limit. The stopping officer saw the defendant reach for the center console and smelled a strong odor of marijuana upon approach. The officer removed the occupants from the car and searched it, leading to the discovery of marijuana. During the search, an officer contacted the drug investigators about the possibility of notifying the defendant of the wider drug investigation. This took approximately five to seven minutes. The on-scene officers then informed the pair of the ongoing drug investigation of the defendant and sought consent to search the apartment, which the girlfriend gave. A gun and cocaine were discovered there, and the defendant was charged with firearm by felon and possession of cocaine. He moved to suppress, arguing that the traffic stop was unreasonably extended and that any consent was invalid. The trial court denied the motion,

and the defendant entered a guilty plea, preserving his right to appeal the denial of the motion. On appeal, the Court of Appeal unanimously affirmed.

(1) The defendant argued since the police never acted on the speeding or marijuana offenses discovered during the traffic stop, the mission of the stop was complete, and the officer deviated from the mission of the stop by delving into an unrelated drug investigation and seeking consent to search the apartment. The court disagreed:

> [A]t the time Officer Fisher asked for consent to search the Apartment, there is no evidence to suggest Officer Fisher had already made a determination to refrain from charging Defendant for the traffic violation or marijuana possession. Instead, the Record seems to indicate that at the time of Officer Fisher's request for consent to search the Apartment, the stop had not been 'otherwise-completed' as he had not yet made a decision on whether to charge Defendant for the marijuana possession." *Jordan* Slip op. at 9-10.

The act of asking for consent to search the apartment therefore occurred during the lawful course of the stop. Further, officers had reasonable suspicion that the defendant was selling drugs, justifying extension of the stop even if the original mission of the stop was complete at the time of the request for consent. Given the tip, the controlled purchase, law enforcement surveillance of the residence (which included observing a high volume of guests visiting the home), law enforcement likely had probable cause to arrest the defendant or obtain a warrant to search the apartment. "Consequently, the officer was justified in extending the seizure to question Defendant about the sale of heroin and crack-cocaine even though it was unrelated to the traffic violation." *Id*. at 12.

(2) Officers had informed the pair that police would seek a search warrant, or that they could consent to a search of the apartment. The defendant argued that this was improper coercion and that any consent was therefore involuntary and invalid. The court disagreed. The defendant and his girlfriend were informed of the right to refuse consent, the girlfriend signed a written consent form, and neither person objected or attempted to revoke consent during the search. Further, the officers did not use any threats or other "inherently coercive tactics" in obtaining consent. Thus, the trial court properly determined that consent was freely and voluntarily given. The trial court's judgment was consequently affirmed.

Exigent circumstances supported warrantless acquisition of cell phone location and call log data

U.S. v. Hobbs, 24 F.4th 965 (Feb. 1, 2022). In this case from the District of Maryland, the defendant broke into his ex-girlfriend's home, threatened her with a firearm, and took a television. He also threatened to kill the woman, her child, other family members, and any police officers who may be alerted. When the victim reported the incident to law enforcement, she recounted that the defendant was "obsessed" with guns and had possessed assault rifles in the past. She was aware of the defendant's violent criminal history, which included robbery and attempted murder convictions. She also provided the defendant's cell phone number. A detective submitted an "exigent form" to a cell phone provider seeking to locate the defendant by way of pinging the phone and to access the phone's call log. The form noted that the defendant was suspected of threatening the victim with a gun and that he had stated that he would not surrender peacefully. Police were able to locate the defendant with the information from the cell phone company and eventually arrested him, finding a loaded firearm in his vehicle. He was charged with felon in possession and moved to suppress the cell phone evidence. The

district court denied the motion, finding that officers had exigent circumstances. On appeal, a unanimous panel of the Fourth Circuit agreed.

The defendant was suspected of serious offenses, including firearms offenses, and swore to kill any responding law enforcement officers, in addition to the threats to the victim and her family. Police found the victim credible and corroborated the damage to the victim's home. Coupled with the defendant's criminal history, there was an imminent threat of harm to the victim, her family, and to law enforcement. Additionally, the data obtained was limited to location and call logs and could be produced by the cell phone company in an hour. The same company was known to typically require days to comply with a search warrant. This was sufficient exigent circumstances, and the search was therefore reasonable under the Fourth Amendment. According to the court:

> [W]e agree with the district court's observation that even a brief delay in apprehending Hobbs placed many individuals at significant risk of harm. We therefore conclude that the district court did not clearly err in finding that 'the only way to get help from T-Mobile' in a timely fashion was by submitting an 'exigent form.' *Hobbs* Slip op. at 10 (citation omitted).

Another challenge to the verdict was similarly rejected, and the district court affirmed in full.

Search Warrants

(1) The defendant had standing to contest the search of a building where he was a late-night occupant and exercised apparent control of the door and a safe within; (2) Potential loss of car keys tied to stolen car was not exigent circumstance justifying warrantless entry and drugs discovered inside the building likewise could not support warrantless entry; (3) Purported consent was invalid as the product of an illegal warrantless entry and was not sufficiently attenuated from the illegal police actions; (4) Search warrant for safe based on sight of drugs inside the home did not establish probable cause

State v. Jordan, ___ N.C. App. ___; 2022-NCCOA-215 (April 5, 2022); *temp. stay allowed*, ___ N.C. ___; ___ S.E.2d ___ (April 21, 2022). Charlotte-Mecklenburg police received a report of a stolen car and information about its possible location. Officers went to the location, which was part residence and part commercial establishment. A car matching the description of the stolen vehicle was in the back parking lot. As police watched, a man came out of the building and approached the car as if to enter it. He noticed the unmarked police car and immediately returned to the building, alerting the occupants to the presence of police. Police pulled into the driveway intending to detain the man. The defendant opened the door of the building from inside and the man who had approached the stolen car went inside, although the door was left open. An officer approached and asked the man to come out and speak with police before immediately stepping into the building through the open door. That officer noticed a safe next to the defendant and saw the defendant close the safe, lock it, and place the key in his pocket. More officers arrived on scene and noticed drug paraphernalia in plain view. Officers swept the house and discovered a gun in a bedroom. At this point, officers established that a man inside either owned or leased the building and requested his consent to search. The man initially refused but assented when officers threatened to place everyone in handcuffs and to obtain a search warrant. The defendant informed officers that anything they found in the home was not his and that he did not live there. He denied owning the safe, but a woman who was present at the time later informed officers that the safe

belonged to the defendant. Officers obtained a search warrant for the safe and discovered money, drugs, paraphernalia, and a gun inside. The defendant was subsequently charged with trafficking, firearm by felon, habitual felon, and other offenses. He moved to suppress. The trial court denied the motion, apparently on the basis that the defendant lacked standing (although because no written order was entered, the findings and conclusions of the trial court were not easily determined). The defendant was convicted at trial of the underlying offenses and pled guilty to having obtained habitual felon status. The trial court imposed a minimum term of 225 months in consecutive judgments. On appeal, a unanimous panel of the Court of Appeals reversed.

(1) The defendant had a reasonable expectation of privacy in the building. He opened the door when it was knocked and was one of only four people inside the home at a late hour. The defendant further had apparent permission to keep the safe inside and clearly had an interest in it as the person with its key and the ability to exclude others. While the defendant did not own or lease the property, this was not enough to defeat his expectation of privacy. The defendant also disclaimed ownership of the safe to police, and the State argued that this amounted to abandonment, defeating any privacy interest in the safe. The court disagreed, noting that the defendant only made that remark after the police illegally entered the home and that abandonment does not apply in such a situation. In its words:

> [W]hen an individual 'discards property as the product of some illegal police activity, he will not be held to have voluntarily abandoned the property or to have necessarily lost his reasonable expectation of privacy with respect to it[.]' *Jordan* Slip op. at 14 (citation omitted).

Thus, the defendant had standing to challenge the police entry and search.

(2) The trial court determined that officers had reasonable suspicion to speak with the man who was seen approaching the stolen car. However, this did not justify warrantless entry into the home. The State argued that the entry was supported by exigent circumstances, in that the keys to the stolen car and the drug paraphernalia seen inside the building could have been easily destroyed. However, there was no evidence that the first officer who approached the home saw any drug paraphernalia at the time and the officer therefore could not have had a legitimate concern about its destruction. There was likewise no explanation from the State regarding the need for immediate warrantless entry to preserve the car keys evidence. Because officers had already seen the man approach the car with the keys and because possession of a stolen car may be established by constructive possession, there was no immediate need to obtain the car keys. Further, there was no immediate risk of destruction of evidence where the occupants of the home left the door open, and an officer entered the home within "moments" of arrival. Exigent circumstances therefore did not support the warrantless entry.

(3) The State also argued that the person with a property interest in the building gave valid consent, and that this consent removed any taint of the initial illegal entry. Illegally obtained evidence may be admissible where the link between the illegal police activity and the discovery of evidence is sufficiently attenuated. *Brown v. Illinois*, 422 U.S. 590, 603-04 (1975). Here, the taint of the illegal entry had not dissipated. Officers obtained consent soon after entering the home, no intervening circumstances arose between the entry and the obtaining of consent, and officers purposefully and flagrantly entered the building without a warrant or probable cause. Any consent was therefore tainted by the initial police illegality and could not justify the search.

(4) Although police did ultimately obtain a search warrant for the safe, the information contained in the search warrant application was based on information obtained by police after they were inside the building. There was no evidence that officers saw any drugs prior to entry, so any evidence obtained as a result was the fruit of the poisonous tree. Without the drugs evidence, the stolen car in the parking lot, the man walking up to the stolen car, and his abrupt return from the car to the building did not supply probable cause to search the building or safe. According to the court:

> Because the affidavit supporting the issuance of the search warrant, stripped of the facts obtained by the officers' unlawful entry into the residence, does not give rise to probable cause to search the residence for the evidence of drugs and drug paraphernalia described in the warrant, 'the warrant and the search conducted under it were illegal and the evidence obtained from them was fruit of the poisonous tree.' *Id*. at 24.

The denial of the motion to suppress was therefore reversed and the case was remanded for any further proceedings.

Standing

The defendant did not have standing to challenge the placement of a GPS tracking device on a vehicle he did not own or possess

State v. Lane, ___ N.C. App. ___; 866 S.E.2d 912; 2021-NCCOA-593 (Nov. 2, 2021). In this Wake County case, evidence of the defendant's crimes was obtained using a GPS tracking device installed, pursuant to a court order, on a car owned by Sherry Harris and driven by Ronald Lee Evans. Evans was the target of the investigation. When officers intercepted the vehicle as it returned from a trip to New York, the defendant was driving, and Evans was a passenger. The defendant ultimately pled guilty to attempted trafficking and trafficking heroin by transportation and preserved his right to appeal the denial of his motion to suppress the GPS evidence.

The Court of Appeals concluded that the defendant did not have standing to challenge use of the GPS device. Under the common law trespass theory of a search, a search happens when government agents intrude into a constitutionally protected area to obtain information. Here, the defendant offered no evidence that he possessed the car to which the GPS device was attached such that any trespass by the government violated his rights as opposed to the rights of the owner (Harris) or usual driver (Evans). Likewise, under a reasonable expectation of privacy theory, the defendant could not show that he had a reasonable expectation of privacy in his movements in someone else's car on a public thoroughfare. To the contrary, the Court said, "[f]or the Defendant, the [car] was a vehicle for a trip to conduct a heroin transaction. Defendant did not have a reasonable expectation of privacy to confer standing to challenge the court order issue on probable cause." Slip op. ¶ 30.

Recent occupant of car did not have standing to challenge search or stop when he was not actually present at the time and otherwise had no possessory or other interest in the property

U.S. v. Smith, 21 F.4th 122 (Dec. 17, 2021). Greensboro police were surveilling a nightclub and saw the defendant leave in a car with a known felon around 2 am. The defendant was sitting in the front passenger seat of car, which police followed from the nightclub to a gas station. Officers believed the car had a fake license plate, but it was later determined that an officer misread the license plate number. At

the gas station, the defendant exited the car with the driver and was inside the convenience store when police arrived. The backseat passenger was in the parking lot at the time and was detained at gunpoint by law enforcement. Officers shined a light inside the car the men had been travelling in and immediately saw a gun on the floorboard of the front passenger area. Another officer soon noticed a second gun. Two other officers approached the two men inside the store and informed the defendant he was being detained for fictitious tags. The defendant immediately stated that the car did not belong to him. During the encounter inside the store, the officers did not know that guns had been discovered in the car by other officers outside. A full search of the car lead to the discovery of heroin on the front passenger side of the car, where the defendant had been sitting, along with the defendant's cell phone. When the defendant was informed that he was being charged with trafficking heroin, he protested that the drugs did not weigh more than 3.5 grams and were therefore under the state trafficking amount of 4.0 grams. The drugs in fact weighed 3.3 grams. The defendant was charged with various federal drug and gun offenses and moved to suppress. The trial court denied the motion, and the Fourth Circuit affirmed.

It is the defendant's burden to demonstrate a reasonable expectation of privacy in property in order for Fourth Amendment protections to apply. Here, the defendant neither owned nor claimed any other interest in the car searched by the police. "[I]f a passenger asserts neither a property or possessory interest in the car and simultaneously disclaims any interest in the seized objects, that passenger normally has no legitimate expectation of privacy." *Smith* Slip op. at 6-7 (citation omitted). The presence of the defendant's cell phone in the car was another factor to be considered but was insufficient on its own to confer an expectation of privacy in the car, particularly in light of the fact that the defendant left it in the car when he went inside the store. According to the court: "When someone leaves personal belongings behind in another's car, he assumes the risk that the car's owner will consent to a search of the car or that the car's contents will come into plain view of the police." *Id*. at 8 (citation omitted). The fact that the defendant was detained inside the store also did not convert the defendant from a recent passenger to an actual one. Once inside, the defendant appeared to ignore the activity in the parking lot outside and admitted to attempting to mislead the police inside about his connection to the car. "Smith cannot initially pretend to be unassociated with the Malibu and then later declare a privacy interest in it. Such conduct suggests that his assertion of privacy is contrived rather than legitimate." *Id.* at 9. For the same reasons that the defendant lacked standing to object to the search of the car, he lacked standing to challenge the stop of the vehicle, and the district court was correct to deny the suppression motion.

Other challenges were similarly rejected, and the district court's judgment affirmed in all respects. Judge Wynn dissented in part and dissented in judgment. He would have granted the defendant a new trial based on the trial court's failure to instruct on a lesser-included drug offense, but otherwise concurred in the majority opinion.

Crimes

Video sweepstakes games as modified remain games of chance under the predominant factor test and violate the sweepstakes ban statute

Gift Surplus, LLC v. State of North Carolina, 380 N.C. 1; 2022-NCSC-1 (Feb. 11, 2022). The plaintiffs sought a declaratory judgment that their sweepstakes video games were lawful and did not violate G.S. 14-306.4 (banning certain video sweepstakes games). For the third time, the North Carolina Supreme Court held that the video games at issue are primarily games of chance in violation of the statute. While

the games were modified to award more nominal money prizes and to allow players to "double nudge" game symbols into place to win, these changes did not alter the chance-based character of the games. The question of whether a game falls within the prohibition on games of chance in G.S. 14-306.4 is a mixed question of law and fact and is subject to de novo review where there is no dispute about how the game is played. Applying that standard, the Court unanimously held the modified games remained games of chance. In its words:

> After considering plaintiffs' game when viewed in its entirety, we hold that the results produced by plaintiffs' equipment in terms of whether the player wins or loses and the relative amount of the player's winnings or losses varies primarily with the vagaries of chance and not the extent of the player's skill and dexterity. *Gift Surplus Slip op.* at 22 (cleaned up).

Because the Court determined the games at issue violated G.S. 14-306.4, it declined to consider whether the games also constituted illegal gambling.

The Court of Appeals majority opinion below held that the games violated the statute regardless of whether or not they were games of chance because the games constituted an "entertaining display" under the statute. This was error, as entertaining displays are not banned under the statute unless the game is one of chance. "Any doubt about whether the statute is only concerned with games of chance is resolved by subsection (i), the statute's 'catch-all provision,' which prohibits sweepstakes through '[a]ny other video game not dependent on skill or dexterity.'" *Id.* at 12. The Court of Appeals was consequently affirmed as modified.

There was sufficient evidence that the defendant committed multiple assaults against his girlfriend where a "distinct interruption" occurred between the assaults

State v. Dew, 379 N.C. 64; 2021-NCSC-124 (Oct. 29, 2021). There was sufficient evidence that the defendant committed multiple assaults against his girlfriend and the Court was equally divided as to whether there was sufficient evidence to establish that the defendant used his hands, feet, or teeth as deadly weapons. The Court characterized "the question of how to delineate between assaults—to know where one assault ends and another begins—in order to determine whether the State may charge a defendant with multiple assaults" as an issue of first impression. Reviewing case law, the Court explained that a single assault "might refer to a single harmful contact or several harmful contacts within a single incident," depending on the facts. The Court declined to extend the three-factor analysis of *State v. Rambert*, 341 N.C. 173 (1995), applicable to discharging a firearm into occupied property, to assault cases generally, saying that the *Rambert* factors were "not the ideal analogy" because of differences in the nature of the acts of discharging a firearm and throwing a punch or kick. The Court determined that a defendant may be charged with more than one assault only when there is substantial evidence that a "distinct interruption" occurred between assaults. Building on Court of Appeals jurisprudence, the Court said:

[W]e now take the opportunity to provide examples but not an exclusive list to further explain what can qualify as a distinct interruption: a distinct interruption may take the form of an intervening event, a lapse of time in which a reasonable person could calm down, an interruption in the momentum of the attack, a change in location, or some other clear break delineating the end of one assault and the beginning of another.

The Court went on to explain that neither evidence of a victim's multiple, distinct injuries nor evidence of different methods of attack alone are sufficient to show a "distinct interruption" between assaults.

Turning to the facts at hand, the Court concluded that evidence showing that the defendant beat the victim for hours inside a trailer and subsequently beat the victim in a car while driving home was sufficient to support multiple charges of assault. The assaults were separated by an intervening event interrupting the momentum of the attack – cleaning the trailer and packing the car. The assaults also were distinct in time and location. Though the defendant was charged with at least two assaults for conduct occurring inside the trailer, the Court concluded that the evidence indicated that there was only a single assault inside the trailer as the attack was continuous and ongoing. [Brittany Williams blogged about this case, here.]

In this human trafficking case involving multiple victims, (1) the indictments were sufficient to convey subject matter jurisdiction; (2) Trial court did not err by entering judgments for multiple counts of human trafficking for each victim

State v. Applewhite, ___ N.C. App. ___; 867 S.E.2d 692; 2021-NCCOA-610 (Dec. 21, 2021). (1) The Court of Appeals rejected the defendant's arguments concerning the sufficiency of the seventeen indictments charging him with human trafficking of six different victims. The Court noted that the indictments alleged every element of the offense within a specific time frame for each victim and tracked the language of the relevant statute word for word.

(2) The Court then turned to and rejected the defendant's argument that human trafficking is a continuous offense and may only be charged as one crime for each victim. The Court explained that the defendant's interpretation of G.S. 14-43.11, which explicitly provides that each violation of the statute "constitutes a separate offense," would "result in perpetrators exploiting victims for multiple acts, in multiple times and places, regardless of the length of the timeframe over which the crimes occurred as long as the Defendant's illegal actions and control over the victim were 'continuous.'" The Court characterized human trafficking as "statutorily defined as a separate offense for each instance."

Judge Arrowood concurred in part and dissented in part by separate opinion, expressing his view that it was improper to convict the defendant of multiple counts per victim of human trafficking. Judge Arrowood explained that North Carolina precedent, specifically involving issues of first impression addressing statutory construction, "clearly instructs that, where a criminal statute does not define a unit of prosecution, a violation thereof should be treated as a continuing offense." Judge Arrowood then proceeded with a lengthy and detailed analysis of the appropriate unit of prosecution for human trafficking in North Carolina.

Sufficient evidence existed for the jury to find that the defendant was aware of a DVPO; Court of Appeals erred in failing to view the evidence in the light most favorable to the State

State v. Tucker, 380 N.C. 234; 2022-NCSC-15 (Feb. 11, 2022). In this case from Mecklenburg County, the defendant was convicted of violating a domestic violence protective order ("DVPO") while in possession of a deadly weapon, as well as felony breaking or entering in violation of the DVPO, assault with a deadly weapon, and assault on a female. The defendant was served with an ex parte DVPO and a notice of hearing on the question of a permanent DVPO. He failed to attend the hearing, and a year-long DVPO was entered in his absence. On appeal, a unanimous Court of Appeals vacated the breaking or entering

and DVPO violation convictions, finding that the defendant lacked notice of the permanent DVPO and therefore could not have willfully violated that order (summarized here). On discretionary review, the North Carolina Supreme Court reversed.

The ex parte DVPO was served on the defendant and indicated that a hearing would be held to determine whether a longer order would be entered. Though the defendant was not present at the hearing, he acknowledged his awareness of the DVPO during his arrest in the victim's apartment the day after the hearing on the permanent order by stating he knew the plaintiff had obtained a DVPO—a remark captured on an officer's bodycam. While this remark could have referred to the ex parte DVPO, it was sufficient evidence of the defendant's knowledge of the permanent order when viewed in context in the light most favorable to the State. The Court of Appeals erred by failing to apply that standard. According to the unanimous Court:

> Defendant's statement, 'I know,' in addition to his other statements, conduct, and the timing of such conduct, supports this holding. The existence of evidence that could support different inferences is not determinative of a motion to dismiss for insufficient evidence. The evidence need only be sufficient to support a reasonable inference. *Tucker* Slip op. at 10 (citations omitted).

The Court of Appeals was therefore reversed, and the defendant's convictions reinstated.

(1) Conviction for making a threat under G.S. 14-16.7(a) requires proof that it was a "true threat," meaning that the statement was both objectively threatening to a reasonable recipient and subjectively intended as a threat by the speaker; (2) the state presented sufficient evidence of such a threat to withstand defendant's motion to dismiss, but conviction was vacated and remanded for new trial where the jury was not properly instructed on the First Amendment

State v. Taylor, 379 N.C. 589; 2021-NCSC-164 (Dec. 17, 2021). The facts of this case were previously summarized following the Court of Appeals decision in *State v. Taylor,* 270 N.C. App. 514 (2020), available here. Briefly, the defendant in this case wrote several social media posts allegedly threatening an elected district attorney over her decision not to seek criminal charges in connection with the death of a child. The defendant was convicted of threatening a court officer under G.S. 14-16.7(a) and appealed. The Court of Appeals held that the defendant's convictions were in violation of the First Amendment and vacated the conviction. The state sought and obtained discretionary review at the state Supreme Court. The higher court concluded that the defendant's conviction was properly vacated but remanded the case for a new trial rather than entry of a judgment of acquittal.

The Supreme Court began its analysis by reviewing the events that prompted the defendant's Facebook posts, the contents of those posts, and the state's evidence purportedly supporting the charges, such as evidence that the prosecutor was placed in fear by the threats. Next, the higher court summarized the opinion of the Court of Appeals, which held that the offense required proof of both general and specific intent on the part of the defendant. The appellate court held that the defendant could only be constitutionally convicted under this statute if he made a "true threat," meaning that the defendant not only made a statement that was objectively threatening (i.e., one which would be understood by those who heard or read it as a serious expression of intent to do harm), but also that he made that statement with the subjective intent that it be understood as a threat by the recipient. Finding that the state failed to make a sufficient showing of those requirements, the Court of Appeals held the statements were protected speech under the First Amendment and vacated the conviction.

Undertaking its own review, the state Supreme Court noted that the First Amendment broadly protects the fundamental right of free speech, and only certain limited categories of speech involving obscenity, defamation, incitement, fighting words, and "true threats" can be constitutionally restricted. The court reviewed *Watts v. United States*, 394 U.S. 705 (1969), which distinguished true threats from other types of protected speech. The court identified three factors from *Watts* that were relevant to evaluating the case at hand, although no single factor is dispositive: (i) the statute at issue must be interpreted with the First Amendment in mind; (ii) the public's right to free speech is even more substantial than the state's interest in protecting public officials; and (iii) the court must consider the context, nature and language of the statement, and the reaction of the listener. Next, the court reviewed the fractured opinions from another true threats case, *Virginia v. Black*, 538 U.S. 343 (2003). After considering the contrasting interpretations offered by the state and the defendant in the present case as to how *Black's* holdings should be construed, the court ultimately concluded that "a speaker's subjective intent to threaten is the pivotal feature separating constitutionally protected speech from constitutionally proscribable true threats." Based on the precedent above and reiterating the importance of the free speech interest at stake, the court held that a true threat is defined as "an objectively threatening statement communicated by a party which possesses the subjective intent to threaten a listener or identifiable group," and "the State is required to prove both an objective and a subjective element in order to convict defendant under N.C.G.S. § 14-16.7(a)."

Applying that definition and framework, the state Supreme Court then considered whether the trial court erred by denying the defendant's motion to dismiss. On a motion to dismiss, the question for the trial court is whether there is substantial evidence, when viewed in the light most favorable to the state, to support each element of the offense and find that the defendant was the perpetrator. In this case there was no dispute that the defendant wrote the posts at issue, and they contained ostensibly threatening language that was not clearly "political hyperbole" or other protected speech. The state Supreme Court acknowledged that cases raising First Amendment issues are subject to an independent "whole record review," but explained that this supplements rather than supplants traditional appellate review, and it is not inconsistent with the traditional manner of review on a motion to dismiss. Under this standard of review, the trial court did not err by ruling that the state had presented sufficient evidence to withstand a motion to dismiss and submit the case to the jury.

However, because the trial court did not properly instruct the jury on the charged offense consistent with the the subjective intent requirement under the First Amendment, the conviction was vacated and the case was remanded to the trial court for a new trial and submission of the case to a properly instructed jury.

Justice Earls concurred with the majority's conclusion that the First Amendment requires the state to prove both the objective and subjective aspects of the threat, but dissented on the issue of whether the state's evidence was sufficient to withstand a motion to dismiss in this case, and disagreed with the majority's interpretation and application of whole record review. In Justice Earls' view, the defendant's Facebook posts could not have been viewed as a serious intent to inflict harm when considered in context by a reasonable observer, and even if they could, the state offered insufficient evidence to show that this was the defendant's subjective intent.

(1) State failed to establish that an objectively reasonable hearer would have construed juvenile's statement about bombing the school as a true threat; (2) State presented sufficient evidence that the juvenile communicated a threat to harm a fellow student

In Re: Z.P., __ N.C. App. ___; 868 S.E.2d 317; 2021-NCCOA-655 (December 7, 2021). In this Iredell County case, the juvenile, "Sophie," was adjudicated delinquent for communicating a threat of mass violence on educational property in violation of G.S. 14-277.6 after making a statement, in the presence of four classmates, that she was going to blow up the school. She was also adjudicated delinquent for communicating a threat to harm a fellow student in violation of G.S. 14-277.1 after stating that she was going to kill him with a crowbar and bury him in a shallow grave. Sophie argued that the State failed to present sufficient evidence to support the allegations of the charged offenses.

(1) Proof of a "true threat" is required for an anti-threat statute. The true threat analysis involves both how a reasonable hearer would objectively construe the statement and how the perpetrator subjectively intended the statement to be construed. While there is a split in cases regarding what the State must prove regarding the perpetrator's subjective intent, this case is resolved because the State did not meet its burden of showing that a reasonable hearer would have construed Sophie's statement as a true threat. The three classmates who heard the threat and testified at the adjudication hearing did not think she was serious when she made the threat. Sophie had made outlandish threats before and never carried them out. Most of the classmates believed that Sophie was joking when she made the statement. There is not enough evidence to support an inference that it would be objectively reasonable for the hearers to think Sophie was serious in this threat. The adjudication is reversed with respect to the offense of communicating a threat of mass violence on educational property.

(2) The evidence provided regarding the threat to the classmate was sufficient. That evidence, when analyzed in the light most favorable to the State, established that the statement was made so that the classmate could hear it, the classmate took the threat seriously, and it would be reasonable for a person in the classmate's position to take the threat seriously because the classmate was smaller than Sophie and had previously been physically threatened by her. The Court of Appeals affirmed the adjudication of communicating a threat to harm a fellow student and remanded the case to allow the trial court to reconsider the disposition in light of the reversal of the adjudication of communicating a threat of mass violence on educational property.

Extortion is unprotected speech as speech integral to criminal conduct and the "true threats" analysis does not apply to the offense

State v. Bowen, ___ N.C. App. ___; 2022-NCCOA-213 (April 5, 2022). The defendant and victim met on a website arranging "sugar daddy" and "sugar baby" relationships, and the two engaged in a brief, paid, sexual relationship. The victim was a married man with children at the time. Years later, the defendant contacted the man, stating that she planned to write a book about her experiences on the website and that she intended to include information about their relationship within. The woman repeatedly contacted the man and threatened to include information that the man had shared with her about his ex-wife and their marriage. She also threatened to contact the man's ex-wife, as well as his current wife. Eventually, she offered the man a confidentiality agreement, whereby she would keep the details of their relationship private in exchange for a large sum of money. The man went to the police, and the woman was charged with extortion. She was convicted at trial and appealed.

Although the defendant did not raise a constitutional challenge in her motions to dismiss at trial, her motion to dismiss for insufficient evidence preserved all sufficiency issues for review, including her constitutional argument.

Under the First Amendment to the U.S. Constitution, threat crimes must be interpreted to require a "true" threat. "A 'true threat' is an 'objectively threatening statement communicated by a party which possess the subjective intent to threaten a listener or identifiable group.'" *Bowen* Slip op. at 10 (citing *State v. Taylor*, 379 N.C. 589 (2021)). The defendant argued that extortion under G.S. 14-118.4 must be interpreted to require proof of a true threat. The court disagreed. It found that extortion falls within another category of unprotected speech—speech integral to criminal conduct, or speech that is itself criminal (such as solicitation to commit a crime). This approach to extortion is consistent with treatment of the offense by federal courts. Although an extortion statute may sweep too broadly in violation of the First Amendment, North Carolina's extortion statute requires that the defendant possess the intent to wrongfully obtain a benefit via the defendant's threatened course of action. The statute therefore only applies to "extortionate" conduct and does not reach other types of protected speech, such as hyperbole or political and social commentary. According to the unanimous court:

> Following the U.S. Supreme Court and federal appellate opinions, we hold extortionate speech is criminal conduct in and of itself and, as such, is not constitutionally protected speech. Therefore, the First Amendment does not require that the 'true threat' analysis be applied to N.C. Gen. Stat. § 14-118.4. *Bowen* Slip op. at 16.

Here, the evidence clearly established the defendant's wrongful intent and threats, and she was properly convicted of extortion.

(1) Sufficient evidence supported the defendant's convictions for embezzlement in excess of $100,000; (2) The trial court did not err in declining to give a special jury instruction on joint ownership

State v. Steele, ___ N.C. App. ___; 868 S.E.2d 876; 2022-NCCOA-39 (Jan. 18, 2022). The defendant was close friends with older couple in Pamlico County. They considered each other family. When the husband of the couple unexpectedly died, the defendant offered to assist the surviving widow. She ultimately turned over complete control of her finances to the defendant. Two months later, she signed a power of attorney making the defendant her attorney in fact and named the defendant as the primary beneficiary of her will. Money was withdrawn from the widow's accounts and deposited into new bank accounts opened jointly in the names of the widow and the defendant. The defendant then used the widow's funds to make personal purchases and pay individual debts. Additionally, some of the widow's funds were automatically withdrawn by the bank from the joint accounts to cover overdrafts owed by the defendant on his individual bank accounts. After the discovery that more than $100,000.00 had been withdrawn from the widow's accounts, the defendant was charged with embezzlement and multiple counts of exploitation of an older adult. At trial, the defense requested a special jury instruction regarding the rights of joint account holders based on provisions in Chapter 54C ("Savings Banks") of the North Carolina General Statutes. The trial court declined to give the proposed instruction, the jury convicted on all counts, and the defendant was sentenced to a minimum 73-months imprisonment.

On appeal, a unanimous Court of Appeals found no error. (1) The defendant's motion to dismiss for insufficient evidence was properly denied. The evidence showed a fiduciary relationship existed between the defendant and the widow, even before the execution of the power of attorney. "[T]he evidence sufficiently established that a fiduciary relationship existed between Defendant and Mrs. Monk prior to that point, when he 'came into possession of the funds in Mrs. Monk's bank accounts.'" *Steele* Slip op. at 10. The defendant also argued that, as a joint account holder with the widow, the money in the accounts was properly considered his property. The court disagreed. While joint account holders

may be presumed to be the owners of the money in a joint account, that presumption can be overcome when ownership is disputed. Then, ownership of the funds is determined by examining the history of the account, the source of the money, and whether one party intended to gift money to the other joint account holder (among other factors). It was clear here that the widow was the source of the funds in the joint accounts and that she did not intend to make any gift to the defendant. "[T]here was sufficient evidence that the funds taken were the property of Mrs. Monk, and that she did not have the requisite 'donative intent' to grant Defendant the money to withdraw and use for his personal benefit." *Id*. at 14 (citation omitted). There was also sufficient evidence that the defendant intended to embezzle an amount exceeding $100,000. While more than $20,000 of the missing funds had been automatically withdrawn by a bank to cover the defendant's preexisting overdraft fees and the defendant denied being aware of this, the overdraft repayments occurred over a 9-month period of time. The defendant received bank statements recounting the repayments each month during that time frame. The total amount deducted as overdraft repayments exceeded $20,000, more than one-fourth of the defendant's yearly salary. There was also evidence of the defendant's financial problems. This was sufficient circumstantial evidence of the defendant's fraudulent intent to embezzle over $100,000. The defendant's various sufficiency arguments were therefore all properly rejected.

(2) The trial court did not err in failing to give the jury a special instruction on joint accounts and joint tenancy. The proposed instruction was based on the language of G.S. 54C-165 and related laws regarding banking regulations. These laws are intended to protect banks and allows them to disburse joint funds to either party listed on the account. The laws do not allow a joint account holder to wrongfully convert the funds to their own use simply by virtue of being a joint account holder. The proposed instruction therefore would have been confusing and misleading to the jury. In the words of the court:

> Because the requested special instruction could have misled the jury and was likely to create an inference unsupported by the law and the record—that Defendant's lawful access to the funds in the joint accounts entitled him to freely spend the money therein—the trial court properly declined to deliver Defendant's requested special jury instruction. *Steele* Slip op. at 19.

There was sufficient circumstantial evidence that the defendant was the driver of a moped

State v. Ingram, ___ N.C. App. ___; 2022-NCCOA-264 (Apr. 19, 2022). In this Rowan County case, the defendant appealed after being convicted of impaired driving after a jury trial. The conviction stemmed from a 2017 incident in which the defendant was found unresponsive on a fallen moped in the middle of the road. Field sobriety tests and a toxicology test indicated that the defendant was impaired. The trial court denied the defendant's motion to dismiss and the defendant was convicted. On appeal, the defendant contended that the trial court erred by denying his motion to dismiss because there was insufficient evidence that he drove the moped. Though no witness testified to seeing the defendant driving the moped, the Court of Appeals concluded that there was sufficient circumstantial evidence that he did. He was found alone, wearing a helmet, lying on the double yellow line in the middle of the road and mounted on the seat of the fallen moped. The Court thus found no error.

Defenses

(1) Statutory self-defense provisions of G.S. 14-51.3 and 14-51.4 abolished the common law right of perfect self-defense; (2) Defendant's argument that the felony disqualification required a causal nexus was preserved; (3) Felony disqualification provisions of G.S. 14-51.4 require a causal nexus between the felony and the need for defensive force (4) Based on the jury's guilty verdict for armed robbery, the trial court's failure to instruct on a causal nexus did not prejudice the defendant

State v. McLymore, 380 N.C. 185, 2022-NCSC-12 (Feb. 11, 2022). Under G.S. 14-51.4, a person may not claim self-defense if the person was attempting a felony, committing a felony, or escaping from the commission of a felony at the time of the use of force. The defendant was charged with first-degree murder, armed robbery, and fleeing to elude in Cumberland County. He claimed self-defense and testified on his behalf. Evidence showed that the defendant had multiple prior felony convictions and that he possessed a weapon at the time of the murder. The trial court gave a general instruction on statutory self-defense and instructed the jury that the defendant could not claim self-defense if he was committing the felony of possession of firearm by a felon at the time of his use of force. The jury convicted on all counts and the defendant was sentenced to life without parole. On appeal, the Court of Appeals affirmed, finding that the defendant was disqualified from claiming statutory self-defense under *State v. Crump,* 259 N.C. App. 144 (2018) (strictly interpreting the felony disqualification) and determining that G.S. 14-51.4 supplanted the common law right in the situations covered by the statute. On discretionary review, the Supreme Court modified and affirmed.

(1) The trial court and Court of Appeals correctly rejected the defendant's argument that the statutory self-defense disqualification did not apply because the defendant was claiming common law, rather than statutory, self-defense. The Court agreed with the lower courts that G.S. 14-51.3 and 14-51.4 were intended to abolish the common law right to perfect self-defense in the circumstances identified by the statute, noting that the language of G.S. 14-51.3 closely followed the common law definition of self-defense and that the legislature had failed to express an intent to retain the common law (unlike other parts of the statutory self-defense laws, where such an intention was expressly stated). In the words of the Court:

> [A]fter the General Assembly's enactment of G.S. 14-51.3, there is only one way a criminal defendant can claim perfect self-defense: by invoking the statutory right to perfect self-defense. Section 14-51.3 supplants the common law on all aspects of the law of self-defense addressed by its provisions. Section 14-51.4 applies to the justification described in G.S. 14-51.3. Therefore, when a defendant in a criminal case claims perfect self-defense, the applicable provisions of G.S. 14-51.3—and, by extension, the disqualifications provided under G.S. 14-51.4—govern. *McLymore* Slip op. at 8-9 (cleaned up).

The trial court therefore did not err by instructing the jury on statutory self-defense, including on the felony disqualifier.

(2) The defendant's objections to the jury instructions were sufficient to preserve his arguments relating to a "causal nexus" requirement for the felony disqualification provisions of G.S. 14-51.4, and his arguments were also apparent from the record. Among other reasons, the State argued, and the trial

court relied on, the *Crump* decision (finding no causal nexus requirement for the felony disqualifier) in rejecting the defendant's proposed jury instruction.

(3) The Court agreed that G.S.14-51.4 must be read to require a nexus between the defendant's use of force and felony conduct used to disqualify the defendant from use of defensive force. A strict interpretation of this statute would lead to absurd and unjust results and would also contract the common law right to self-defense. "[A]bsent a causal nexus requirement, each individual [committing a felony not related to the need for defensive force] would be required to choose between submitting to an attacker and submitting to a subsequent criminal conviction." *McLymore* Slip op. at 18. The Court also noted that a broad interpretation of the felony disqualifier may violate the North Carolina Constitution's protections for life and liberty. N.C. Const. art. I, sec. 1. The Court therefore held that the State has the burden to demonstrate a connection between the disqualifying felony conduct and the need for the use of force, and the jury must be instructed on that requirement. *Crump* and other decisions to the contrary were expressly overruled. In the Court's words:

> [W]e hold that in order to disqualify a defendant from justifying the use of force as self-defense pursuant to N.C.G.S. § 14-51.4(1), the State must prove the existence of an immediate causal nexus between the defendant's disqualifying conduct and the confrontation during which the defendant used force. The State must introduce evidence that 'but for the defendant' attempting to commit, committing, or escaping after the commission of a felony, 'the confrontation resulting in injury to the victim would not have occurred.' *McLymore* Slip op. at 20.

(4) Though the trial court's instructions on the felony disqualification were erroneous, this error did not prejudice the defendant under the facts of the case. The jury convicted the defendant of armed robbery based on his theft of the victim's car immediately after the murder. This necessarily showed that the jury found the defendant was committing or escaping from the commission of a felony related to his need to use force. The Court observed:

Based upon the outcome of McLymore's trial, it is indisputable that there existed an immediate causal nexus between his felonious conduct and the confrontation during which he used assertedly defensive force, and the felony disqualifier applies to bar his claim of self-defense. *Id*. at 23.

However, the Court rejected the State's argument that the defendant would be categorically barred from self-defense with a firearm due to this status as a convicted felon. The defendant was not charged with possession of firearm by felon in the case and had no opportunity to defend against that charge. Additionally, the jury was not instructed on a causal connection between the defendant's mere possession of the firearm and his need for use of force. According to the Court:

> To accept the State's argument on this ground would be to effectively hold that all individuals with a prior felony conviction are forever barred from using a firearm in self-defense under any circumstances. This would be absurd. *Id*. at 22.

The Court of Appeals was therefore modified and affirmed. Chief Justice Newby wrote separately to concur in result only, joined by Justice Barringer. They would have found that the causal nexus argument was not preserved and should have not been considered. Alternatively, they would have ruled that the felony disqualification does not require a causal nexus.

(1) Request for involuntary manslaughter instruction was preserved for appellate review; (2) Failure to instruct the jury on involuntary manslaughter was reversible error where the jury could have found that the defendant acted recklessly instead of with malice

State v. Brichikov, ___ N.C. App. ___; 869 S.E.2d 339; 2022-NCCOA-33 (Jan. 18, 2022). In this Wake County murder case, the defendant admitted to having assaulted his wife and she was found with physical trauma to her face. She also had cocaine and fentanyl in her blood, had recently overdosed, and had a serious heart condition. There was conflicting evidence at trial on whether the facial injuries alone could have caused her death. The defendant requested instructions on voluntary and involuntary manslaughter. The trial court declined to give the requested instructions and the jury convicted on second-degree murder. A divided Court of Appeals reversed and remanded for a new trial.

(1) The defendant's request for an involuntary manslaughter instruction was preserved. While an initial request for the instruction focusing on the defendant's failure to act would have been a special instruction (as it deviated from the pattern instruction) and would have needed to be in writing in order to preserve the issue, the defendant articulated multiple theories in support of an involuntary manslaughter instruction. He also objected to the lack of manslaughter instructions at the charge conference and again after the jury was instructed. This preserved the issue for review.

(2) The defendant argued that his evidence contradicted the State's evidence of malice with evidence of recklessness, and that he was entitled to an involuntary manslaughter instruction when the evidence was viewed in the light most favorable to him. The State argued that the defendant's use of a deadly weapon—his hands—"conclusively established" the element of malice, so that no lesser-included instructions were required. The court agreed with the defendant:

> Viewing the evidence in the light most favorable to Defendant, the evidence was not "positive" as to the element of malice for second-degree murder. The jury could reasonably have found Defendant did not act with malice, but rather committed a reckless act without the intent to kill or seriously injure–he spent the day declaring his love for Mrs. Brichikov, they used drugs together . . . and her body was in a weakened state from a recent overdose, heart blockage, and fentanyl overdose. *Brichikov* Slip op. at 17-18.

The failure to give an involuntary manslaughter instruction prejudiced the defendant and required a new trial. The court declined to consider the propriety of the defendant's proposed special jury instruction on culpable negligence by omission, finding that issue moot in light of its ruling and expressing no opinion on the merits of the instruction.

Judge Carpenter dissented and would have found that any error in the jury instructions was not prejudicial in light of the aggravating factor found by the jury that the defendant acted especially cruelly.

Right to Counsel

Trial court did not err by failing to further investigate defendant's complaints about trial counsel or by denying his mid-trial request to represent himself

State v. Ward, ___ N.C. App. ___; 868 S.E.2d 169; 2022-NCCOA-40 (Jan. 18, 2022). In this Pasquotank County case, the defendant was convicted at trial of statutory rape and abduction of a child. (1) During the first day of trial, the defendant complained about his attorney and claimed to have repeatedly fired him during the case. In response, the trial court allowed the defendant to express his concerns and attempted to address them. On the second day of trial, the defendant asked to represent himself, a request the trial court refused. On appeal, he argued that the trial court failed to inquire into an alleged impasse between trial counsel and the defendant and erred by not allowing him to represent himself. A unanimous Court of Appeals disagreed. While the defendant expressed some dissatisfaction with his attorney, his comments did not evince an absolute impasse in the case. In the court's words:

> Defendant's complaints . . .were deemed misunderstandings that were corrected during the colloquies by the trial court. . .Defendant may have had a personality conflict with his counsel, and asserted he did not believe defense counsel had his best interest at heart. Defendant has failed to show an 'absolute impasse as to such tactical decisions' occurred during trial. *Ward* Slip op. at 9.

Thus, the trial court did not err by failing to more fully investigate the issue. The trial court also did not err by refusing to allow the defendant to proceed pro se after trial had begun, or by failing to conduct the colloquy for self-represented individuals in G.S. 15A-1242. While waiver of the right to counsel requires a knowing, voluntary, and intelligent waiver by the defendant, the right to self-representation may be waived by inaction, as occurred here. Further, without the defendant making a timely request to represent himself, the defendant is not entitled to be informed about the right to self-representation. The trial court did not err in disallowing self-representation, or in failing to make the statutory inquiry required for self-representation, under these circumstances. According to the court:

> Defendant did not clearly express a wish to represent himself until the second day of trial. The trial court gave Defendant several opportunities to address and consider whether he wanted continued representation by counsel and personally addressed and inquired into whether Defendant's decision was being freely, voluntarily, and intelligently made. Defendant's arguments are without merit and overruled. *Id*. at 10-11.

(1) Challenge to earlier order extending probation following later revocation was not an impermissible collateral attack on the underlying judgment; (2) Violation of defendant's right to counsel at probation extension hearing voided extension order, which deprived the trial court of jurisdiction to later revoke probation

State v. Guinn, ___ N.C. App. ___; 868 S.E.2d 672; 2022-NCCOA-36 (Jan. 18, 2022). The defendant was on supervised probation in Gaston County after pleading guilty to two counts of uttering a forged instrument. 24 months into a 30-month period of probation, a probation violation was filed, accusing the defendant of willful failure to pay. The defendant was not represented by counsel at the hearing, and the trial court ultimately extended probation by 12 months. A year later, probation filed a violation report accusing the defendant of numerous violations. An absconding violation was filed soon after. A hearing was held where the defendant's probation was revoked, and his sentence activated.

On appeal, the defendant argued that the initial extension of his probation was invalid based on a violation of his right to counsel. (1) The State argued that the defendant was not permitted to collaterally attack the underlying judgment. The court disagreed, finding that the defendant sought to challenge the order extending his probation, not the underlying criminal judgment placing him on

probation. Because the defendant had no right of appeal from that order, he retained the right to challenge it in the present case.

(2) The trial court failed to conduct a colloquy pursuant to G.S. 15A-1242 to ensure the defendant knowingly, intelligently, and voluntarily waived his right to counsel at the first probation hearing. While the defendant and judge had signed a waiver of counsel form indicating that the defendant waived all counsel, the judge failed to check either box (indicating partial or total waiver of counsel) on the certification section of the form. The certification attests that the G.S. 15A-1242 colloquy with the defendant was completed. This was a substantive error and not a clerical mistake—the trial court only had jurisdiction to revoke probation in the current case if the initial extension was valid, and the initial extension was only valid if the defendant's right to counsel was honored, so a mistake here spoke directly to the length of the defendant's probation. While a knowing, voluntary, and intelligent waiver of counsel may be presumed from the defendant's signature on the waiver form, that presumption will not be indulged where other record evidence contradicts that conclusion. According to the court:

> [A]lthough a signed written waiver is generally 'presumptive evidence that a defendant wishes to act as his or her own attorney,' we conclude that the written waiver in the instant case is insufficient—notwithstanding the presence of both parties' signatures—to pass constitutional and statutory muster. *Guinn* Slip op. at 18 (cleaned up).

Further, the transcript revealed that no waiver of counsel colloquy occurred. Even assuming the signed waiver of counsel form was valid, the trial court still has a duty to conduct the colloquy of G.S. 15A-1242 and its failure to do so was prejudicial error. The trial court's original order extending probation by 12 months was therefore invalid, as those proceedings violated the defendant's right to counsel. Accordingly, the trial court lacked jurisdiction at the later probation violation hearing, and the order of revocation was vacated.

Judge Tyson dissented. He would have found that the signed form conclusively established the defendant's valid waiver of counsel and would have affirmed the trial court's revocation order.

The trial court did not abuse its discretion by allowing the defendant to represent himself

State v. Applewhite, ___ N.C. App. ___; 868 S.E.2d 137; 2021-NCCOA-610 (Dec. 21, 2021). In this human trafficking case involving multiple victims, the trial court did not abuse its discretion by allowing the defendant to represent himself. The Court of Appeals rejected the defendant's argument that the trial court's statements concluding that he had an "absolute right" to represent himself coupled with the trial court's failure to consider whether he fell into the "gray area" of being competent to stand trial but incapable of representing himself was a mistake of law requiring a new trial. While the defendant suffered from an unspecified personality disorder and drug use disorders, the record showed that the trial court "undertook a thorough and realistic account of Defendant's mental capacities and competence before concluding Defendant was competent to waive counsel and proceed *pro se*." The Court of Appeals noted that after interacting with him, considering his medical conditions, and receiving testimony concerning his forensic psychiatric evaluation, two judges had ruled that Defendant was competent to proceed and represent himself. The Court of Appeals said that even if the trial court erred in allowing the defendant to represent himself, he invited the error by disagreeing with the manner of representation of appointed counsel and any such error was harmless beyond a reasonable doubt.

Pleadings

An attempted robbery with a dangerous weapon indictment was not fatally defective for failing to include the name of a specific victim

State v. Oldroyd, ___ N.C. ___; 869 S.E.2d 193; 2022-NCSC-27 (Mar. 11, 2022). In this Yadkin County case, a defendant pled guilty to second-degree murder, attempted robbery with a dangerous weapon, and conspiracy to commit robbery with a dangerous weapon in 2013. The defendant filed a motion for appropriate relief asserting that the indictment for the attempted robbery charge was fatally defective in that it did not include the name of a victim, but rather described the victims as "employees of the Huddle House" located at a particular address. The trial court denied the motion. A divided panel of the Court of Appeals agreed with the defendant. *State v. Oldroyd*, 271 N.C. App. 544 (2020). The Supreme Court reversed the Court of Appeals, concluding that the indictment sufficiently informed the defendant of the crime he was accused of and protected him from being twice put in jeopardy for the same offense. The Court rejected the defendant's argument, based on cases decided before the enactment of the Criminal Procedure Act of 1975, that indictments for crimes against a person must "state with exactitude" the name of a person against whom the offense was committed. The Court also distinguished prior cases finding indictments defective when they named the wrong victim or did not name any victim at all. Under the modern requirements of G.S. 15A-924(a)(5), the Court concluded that the attempted robbery with a dangerous weapon charge here was not defective. Therefore, the Court reversed the Court of Appeals and reinstated the trial court order denying the defendant's motion for appropriate relief.

There was no fatal variance in charge for injury to personal property where named victim was not the legal owner, but had a special interest in the property

State v. Redmond, __ N.C. App. __; 868 S.E.2d 661; 2022-NCCOA-5 (Jan. 4, 2022). Upon trial de novo in superior court, the defendant in this case was convicted of misdemeanor injury to personal property for throwing a balloon filled with black ink onto a painting during a protest at an arts event in Asheville. The defendant received a suspended 30-day sentence and was ordered to pay $4,425 in restitution. On appeal, the defendant argued that her motion to dismiss the injury to personal property charge should have been granted due to a fatal variance, and argued that the restitution amount was improperly based on speculative value. The appellate court rejected both arguments.

The charging document alleged that the defendant had damaged the personal property of the artist, Jonas Gerard, but the evidence at trial indicated that the painting was the property of the artist's corporation, Jonas Gerard Fine Arts, Inc., an S corporation held in revocable trust, where Jonas Gerard was listed as both an employee and the sole owner. Although this evidence established that the artist and the corporation were separate legal entities, each capable of owning property, the court held that the state's evidence sufficiently demonstrated that the artist named in the pleading was nevertheless a person who had a "special interest" in the property and was therefore properly named in the charging instrument. The painting was not yet complete, it was still in the artist's possession at the time it was damaged, and the artist regarded himself and the corporation as functionally "one and the same" and he "certainly held out the paintings as his own." Finding the facts of this case analogous to *State v. Carr*, 21 N.C. App. 470 (1974), the appellate court held that the charging document was "sufficient to notify Defendant of the particular piece of personal property which she was alleged to have damaged," and the trial court did not err in denying the motion to dismiss for a fatal variance.

The superior court had original jurisdiction to try a misdemeanor charge that was initiated by indictment but amended by a statement of charges

State v. Barber, ___ N.C. App. ___; 868 S.E.2d 601; 2021-NCCOA-695 (Dec. 21, 2021). In this case arising from a high-profile incident where William Joseph Barber was convicted of second-degree trespass for refusing to leave the office area of the General Assembly while leading a protest related to health care policy after being told to leave by security personnel for violating a building rule prohibiting causing disturbances, the Court of Appeals found that the superior court had subject matter jurisdiction to conduct the trial and that the trial was free from error.

The Court of Appeals rejected the defendant's argument that the superior court lacked jurisdiction to try him for the misdemeanor because the charging document upon which the State proceeded in superior court was a statement of charges rather than an indictment and Defendant had not first been tried in district court. Here, the defendant was indicted by a grand jury following a presentment but the prosecutor served a misdemeanor statement of charges on him on the eve of trial and proceeded on that charging document in superior court. The Court of Appeals noted that the superior court does not have original jurisdiction to try a misdemeanor charged in a statement of charges but went on to explain that because the prosecution in this case was initiated by an indictment, the superior court had subject matter jurisdiction over the misdemeanor. The Court characterized the statement of charges as a permissible amendment to the indictment (because it did not substantially change the nature of the charged offense) rather than a new charging document.

Continuances

(1) Denial of defense motion for continuance compromised defendant's right to effective counsel in this case; (2) Error was harmless in conviction for general intent offense, but warranted reversal on specific intent offense, where the evidence at issue related only to negating affirmative defenses to specific intent

State v. Johnson, 378 N.C. 236, 2021-NCSC-165 (Dec. 17, 2021). The state obtained recordings of several hundred phone calls that the defendant made while he was in jail awaiting trial on charges of murder, armed robbery, and assault on a government official. The charges arose out of a robbery at a gas station where the clerk was killed and an officer was threatened with a firearm. The defendant gave notice of the affirmative defenses of diminished capacity, mental infirmity, and voluntary intoxication (insanity was also noticed, but not pursued at trial). Copies of the jail calls were provided to the defense in discovery, but the recordings could not be played. Defense counsel emailed the prosecutor to request a new copy of the calls, and asked the state to identify any calls it intended to use at trial. The prosecutor provided defense counsel with new copies of the calls that were playable, but also indicated that the state did not intend to offer any of the calls at trial, so defense counsel did not listen to them at that time. The evening before trial, the prosecutor notified defense counsel that the state had identified 23 calls that it believed were relevant to showing the defendant's state of mind and memory at the time of the murder. At the start of trial the next morning, the defense moved for a continuance on the basis that it had not had time to review the calls or asses their impact on the defendant's experts' testimony, and argued that denial of a continuance at this point would violate the defendant's state and federal constitutional rights to due process, effective counsel, and right to confront witnesses. The trial court denied the continuance, as well as defense counsel's subsequent request to delay opening statements

until Monday (after jury selection concluded mid-day Friday) in order to provide the defense an opportunity to listen to the calls and review them with the defendant's experts.

The defendant was subsequently convicted of armed robbery, assault on a government official, and felony murder based on the assault. He was sentenced to life imprisonment for the murder and 60-84 months for the robbery; judgment was arrested on the assault. The defendant appealed, and a divided Court of Appeals found that the trial court did not err in denying the continuance, and furthermore any error would not have been prejudicial because the felony murder was a general intent crime and the calls were only offered by the state as rebuttal evidence regarding defendant's diminished capacity. The dissent concluded that the majority applied the wrong standard of review, since the denial of the motion to continue was based on constitutional grounds, and would have found error and ordered a new trial. The defendant appealed to the state Supreme Court based on the dissent.

The higher court found no prejudicial error regarding the felony murder conviction, but vacated the armed robbery judgment. First, regarding the correct standard of review, a trial court's decision on a motion to continue is normally reviewed only for abuse of discretion, but if it raises a constitutional issue it is reviewed de novo; however, even for constitutional issues, denial of a motion to continue is only reversible if the error was prejudicial. In this case, the trial court erred because the time allowed to review the calls was constitutionally inadequate. Defense counsel relied on the state's representation that it would not use the calls until receiving a contrary notice the evening before trial began, and defense counsel did not have an opportunity to listen to the nearly four hours of recordings or consult with his expert witnesses before starting the trial. Under the circumstances of this case, the impact this had on defense counsel's ability to investigate, prepare, and present a defense demonstrated that the defendant's right to effective counsel was violated. Additionally, the defendant was demonstrably prejudiced by this violation, since defense counsel could not accurately forecast the evidence or anticipated expert testimony during the opening statements.

However, the state Supreme Court concluded that as to the felony murder conviction, the error was harmless beyond a reasonable doubt. The murder conviction was based on the underlying assault, a general intent crime "which only require[s] the doing of some act," unlike specific intent offenses "which have as an essential element a specific intent that a result be reached." The recorded calls were only offered as rebuttal evidence on this issue of intent, and therefore the error was harmless as to the assault and felony murder offenses as a matter of law, since "any evidence in this case supporting or negating that defendant was incapable of forming intent at the time of the crime is not relevant to a general-intent offense." But the defendant's conviction for armed robbery, a specific intent offense, was vacated and remanded for a new trial.

Joinder

(1) Court of Appeals erred in finding that the trial court should have granted defendant's motions to dismiss for vindictive prosecution and failure to join; (2) Remanded for reconsideration of defendant's double jeopardy argument

State v. Schalow, 379 N.C. 639, 2021-NCSC-166 (Dec. 17, 2021) ("*Schalow II*"). The facts of this case were previously summarized following the Court of Appeals decision in *State v. Schalow*, 269 N.C. App. 369 (2020) ("*Schalow II*"), available here. The defendant was initially charged with attempted murder and several counts of assault against his wife, but the state only proceeded to trial on attempted murder

and dismissed the assault charges. After discovering the indictment for attempted murder failed to allege malice, the court granted the state a mistrial over the defendant's objection. The defendant was subsequently tried for that charge on a new indictment and convicted. On appeal, the defendant argued in *State v. Schalow*, 251 N.C. App. 354 (2018) ("*Schalow I*") that the mistrial was granted in error because it sufficiently alleged manslaughter as written, and therefore the second prosecution violated double jeopardy. The appellate court agreed and vacated the conviction. In addition to seeking discretionary review of the decision in *Schalow I* (which was ultimately denied), the state obtained several new indictments against the defendant for felony child abuse and the related assaults against his wife. The defendant's pretrial motion to dismiss the new charges on the basis of vindictive prosecution, double jeopardy, and failure to join charges under G.S. 15A-926 was denied, and the defendant sought discretionary appellate review, which was granted. The Court of Appeals held that the trial court erred by denying the defendant's motion to dismiss in *Schalow II*, finding that the defendant was entitled to a presumption of prosecutorial vindictiveness and also met his burden of showing that the state withheld the prior indictments to circumvent the joinder requirements of G.S. 15A-926, which required dismissal of the charges. Based on those holdings, the appellate court did not reach the double jeopardy issue.

The state sought discretionary review of the appellate court's rulings in *Schalow II*, which was granted and resulted in the current decision. On review, the state Supreme Court reversed the Court of Appeals on the two issues it decided, and remanded the case to the lower court to reconsider the remaining double jeopardy argument.

First, regarding vindictive prosecution, the higher court explained that *North Carolina v. Pearce*, 395 U.S. 711 (1969) and *Blackledge v. Perry*, 417 U.S. 21 (1974) establish a presumption of vindictiveness when a defendant receives a more serious sentence or faces more serious charges with significantly more severe penalties after a successful appeal, but noted that subsequent cases have declined to extend that presumption to other contexts. The filing of new or additional charges after an appeal, without more, "does not necessarily warrant a presumption of prosecutorial vindictiveness," even when there is "evidence that repeated prosecution is motivated by the desire to punish the defendant for his offenses." The Court of Appeals erred in concluding that the defendant faced a more severe sentence for substantially the same conduct under the new set of charges, since G.S. 15A-1335 independently prohibits imposing a more severe sentence in these circumstances, making that outcome a "legal impossibility" in this case. The court also rejected the defendant's argument that under *U.S. v. Goodwin*, 457 U.S. 368 (1982), the presumption of vindictiveness applies whenever there has been a change in the charging decision after an initial trial is completed. The language in *Goodwin* regarding the lower likelihood of vindictiveness in pretrial charging decisions did not establish "that such a presumption was warranted for all post-trial charging decision changes," and given the harshness of imposing such a presumption, the court was unwilling to find that it applied here. Additionally, although the prosecutor in this case made public statements about his intent to pursue other charges against the defendant if the ruling in *Schalow I* were upheld, those statements indicated an intent to punish the defendant for his underlying criminal conduct, not for exercising his right to appeal. Concluding that the presumption of vindictiveness did not apply and actual vindictiveness was not established, the state Supreme Court reversed the appellate court on this issue.

Second, the state Supreme Court also disagreed with the Court of Appeals' conclusion that the defendant's motion to dismiss should have been granted for failure to join offenses under G.S. 15A-926. The statute provides that after a defendant has been tried for one offense, his pretrial motion to dismiss another offense that could have been joined for trial with the first offense must be granted unless one

of the enumerated exceptions applies. Pursuant to *State v. Furr*, 292 N.C. 711 (1977), this statute does not apply to charges that were not pending at the time of the earlier trial. However, under *State v. Warren*, 313 N.C. 254 (1985), the later-filed charges must nevertheless be dismissed if the prosecutor withheld those charges in order to circumvent the statutory requirement. If either or both of two circumstances are present — (i) during the first trial the prosecutor was aware of evidence that would support the later charges, or (ii) the state's evidence at the second trial would be the same as the first trial — those factors will "support but not compel" a finding that the state did withhold the other charges to circumvent the statute. At the trial level, the defendant in this case only argued that dismissal was required by the statute, but did not argue that dismissal was required under *Warren* even though the charges were not pending at the time of the prior trial; therefore, the argument presented by the defendant on appeal was not properly preserved for review, and the appellate court erred by deciding the issue on those grounds. Additionally, the Court of Appeals erred by holding that the trial court was required to dismiss the charges upon finding that both *Warren* factors were present. Even if one or both *Warren* factors were found, that will "support" a dismissal by the trial court, but it does not "compel" it. The appellate court incorrectly converted "a showing of both *Warren* circumstances into a mandate requiring dismissal," contrary to case precedent.

The case was remanded for reconsideration of the defendant's remaining argument that prosecution for the assault charges would also violate double jeopardy, which the Court of Appeals declined to address.

Jury Selection

Where the prosecutor's race-neutral explanations for use of a peremptory strike were unsupported by the record, the defendant should have prevailed on his *Batson* challenge; order denying defense *Batson* challenge reversed on the merits

State v. Clegg, 380 N.C. 127; 2022-NCSC-11 (Feb. 11, 2022). The defendant was tried for armed robbery and possession of firearm by felon in Wake County. When the prosecution struck two Black jurors from the panel, defense counsel made a *Batson* challenge. The prosecution argued the strikes were based on the jurors' body language and failure to look at the prosecutor during questioning. The prosecution also pointed to one of the juror's answer of "I suppose" in response to a question on her ability to be fair, and to the other juror's former employment at Dorothea Dix, as additional race-neutral explanations for the strikes. The trial court initially found that these reasons were not pretextual and overruled the *Batson* challenge. After the defendant was convicted at trial, the Court of Appeals affirmed in an unpublished opinion, agreeing that the defendant failed to show purposeful discrimination. The defendant sought review at the North Carolina Supreme Court. In a special order, the Court remanded the case to the trial court and retained jurisdiction of the case.

On remand, the defense noted that the "I suppose" answer used to justify the prosecutor's strike was in fact a mischaracterization of the juror's answer—the juror in question responded with that answer to a different question about her ability to pay attention (and not about whether she could be fair). The defense argued this alone was enough to establish pretext and obviated the need to refute other justifications for the strike. As to the other juror, the defense noted that while the juror was asked about her past work in the mental health field, no other juror was asked similar questions about that field. The defense argued with respect to both jurors that the prosecutor's body language and eye contact explanations were improper, pointing out that the trial court failed to make findings on the issue despite trial counsel disputing the issue during the initial hearing. It also noted that the prosecutor referred to

the two women collectively when arguing this explanation and failed to offer specific reasons for why such alleged juror behavior was concerning. This evidence, according to the defendant, met the "more likely than not" standard for showing that purposeful discrimination was a substantial motivating factor in the State's use of the strikes.

The State argued that it struck the juror with a history in mental health as someone who may be sympathetic to the defendant but did not argue the juror's body language or eye contact as explanations for its use of that strike at the remand hearing. As to the other juror, the State reiterated its original explanations of the juror's body language and eye contact. It also explained that the mischaracterization of the juror's "I suppose" answer was inadvertent and argued that this and another brief answer of "I think" from the juror during voir dire indicated a potential inability of the juror to pay attention to the trial.

The trial court ruled that the strike of the juror with previous employment in the mental health field was supported by the record, but that the prosecution's strike of the other juror was not. It found it could not rely on the mischaracterized explanation, and that the body language and eye contact justifications were insufficient explanations on their own without findings by the trial court resolving the factual dispute on the issue. The trial court therefore determined that the prosecutor's justifications failed as to that juror. The trial court considered the defendant's statistical evidence of racial discrimination in the use of peremptory strikes in the case and historical evidence of racial discrimination in voir dire statewide. It also noted disparate questioning between Black and White jurors on the issue of their ability to pay attention to the trial but found this factor was not "particularly pertinent" under the facts of the case. The trial court ultimately concluded that this evidence showed the prosecutor's explanation was improper as to the one juror, but nonetheless held that no purposeful discrimination had occurred, distinguishing the case from others finding a *Batson* violation. Thus, the objection was again overruled, and the defendant again sought review at the North Carolina Supreme Court.

A majority of the Court reversed, finding a *Batson* violation by the State. The prosecutor's shifting and mischaracterized explanation for the strike of the juror who answered "I suppose"—initially argued as an indication the juror could not be fair, but later argued as going to her ability to pay attention—indicated the reason was pretextual, and the trial court correctly rejected that justification for the strike. The trial court also correctly determined that the demeanor-based explanations for the strike of this juror were insufficient without findings of fact on the point. However, the trial court erred in several critical ways. For one, when the trial court rejects all of the prosecutor's race-neutral justifications for use of a strike, the defendant's *Batson* challenge should be granted. According to the Court:

> If the trial court finds that all of the prosecutor's proffered race-neutral justifications are invalid, it is functionally identical to the prosecutor offering no race-neutral justifications at all. In such circumstances, the only remaining submissions to be weighed—those made by the defendant—tend to indicate that the prosecutor's peremptory strike was 'motivated in substantial part by discriminatory intent.' *Clegg* Slip op. at 47.

Further, while the trial court correctly recited the more-likely-than-not burden of proof in its order, it failed to meaningfully apply that standard. While the present case involved less explicit evidence of racial discrimination in jury selection than previous federal cases finding a violation, it is not necessary for the defendant to show "smoking-gun evidence of racial discrimination." *Id*. at 41. The trial court also erred in reciting a reason for the strike not offered by the prosecution in its order denying relief. Finally, there was substantial evidence that the prosecutor questioned jurors of different races in a disparate

manner, and the trial court failed to fully consider the impact of this evidence. Collectively, these errors amounted to clear error and required reversal. Because the Court determined that purposeful discrimination occurred as to the one juror, it declined to consider whether discrimination occurred with respect to the strike of the other juror.

The conviction was therefore vacated, and the matter remanded to the trial court for any further proceedings. A *Batson* violation typically results in a new trial. The defendant here had already served the entirety of his sentence and period of post-release, and the Court noted the statutory protections from greater punishment following a successful appeal in G.S. 15A-1335. In conclusion, the Court observed:

> [T]he *Batson* process represents our best, if imperfect, attempt at drawing a line in the sand establishing the level of risk of racial discrimination that we deem acceptable or unacceptable. If a prosecutor provides adequate legitimate race-neutral explanations for a peremptory strike, we deem that risk acceptably low. If not, we deem it unacceptably high. . . Here, that risk was unacceptably high. *Clegg* Slip op. at 56-57.

Justice Earls wrote separately to concur. She would have considered the *Batson* challenge for both jurors and would have found clear error with respect to both. She also noted that this is the first case in which the North Carolina Supreme Court has found a *Batson* violation by the State. Her opinion argued the State has been ineffective at preventing racial discrimination in jury selection and suggested further action by the Court was necessary to correct course.

Justice Berger dissented, joined by Chief Justice Newby and Justice Barringer. The dissenting Justices would have affirmed the trial court's finding that a *Batson* violation did not occur in the case.

Confrontation Clause

Assuming the admission of substitute analyst testimony and 404(b) evidence was error, the defendant was not prejudiced in light of overwhelming evidence of his guilt

State v. Pabon, 380 N.C. 241, 2022-NCSC-16 (Feb. 11, 2022). The defendant was charged with second-degree rape and first-degree kidnapping in Cabarrus County and was convicted at trial. Benzodiazepines were found in the victim's urine, and the State presented expert testimony at trial on the urinalysis results. The expert witness did not conduct the forensic testing but independently reviewed the test results. The defendant's hearsay and Confrontation Clause objections were overruled. Expert testimony from another witness established the presence of a muscle relaxant in the victim's hair sample and indicated that the two drugs in combination would cause substantial impairment. There was additional evidence of a substantial amount of the defendant's DNA on the victim, as well as evidence of prior similar sexual assaults by the defendant admitted under Rule 404(b) of the North Carolina Rules of Evidence. He was convicted of both charges and appealed. A divided Court of Appeals affirmed, finding no error (summarized here). Among other issues, the majority rejected the defendant's arguments that the admission of the substitute analyst testimony and the 404(b) evidence was error. The defendant appealed the Confrontation Clause ruling and the North Carolina Supreme Court later granted discretionary review on the Rule 404(b) issue.

Assuming without deciding that admission of the substitute analyst testimony was error, the error was harmless beyond a reasonable doubt. Testimony from the substitute analyst established the presence of benzodiazepines in the victim's blood based first on a preliminary test, and then a confirmatory test. While the defendant objected to all of this testimony at trial, only the testimony regarding the confirmatory test was challenged on appeal. Thus, "[e]ven in the absence of [the substitute analyst's] subsequent testimony regarding the confirmatory testing, there was still competent evidence before the jury of the presence of Clonazepam in [the victim's] urine sample." *Pabon* Slip op. at 23. The Court noted that evidence from the other analyst established a different impairing substance in the victim's hair which could have explained the victim's drugged state on its own. In light of this and other "overwhelming" evidence of guilt, any error here was harmless and did not warrant a new trial.

As to the 404(b) evidence, the Court likewise assumed without deciding that admission of evidence of the previous sexual assaults by the defendant against other women was error but determined that any error was not prejudicial under the facts. Unlike a case where the evidence amounts to a "credibility contest"—two different accounts of an encounter but lacking physical or corroborating evidence—here, there was "extensive" evidence of the defendant's guilt. This included video of the victim in an impaired state soon before the assault and while in the presence of the defendant, testimony of a waitress and the victim's mother regarding the victim's impairment on the day of the offense, the victim's account of the assault to a nurse examiner, the victim's vaginal injury, the presence of drugs in the victim's system, and the presence of the a significant amount of the defendant's DNA on the victim's chest, among other evidence. "We see this case not as simply a 'credibility contest,' but as one with overwhelming evidence of defendant's guilt." *Id*. at 34. Thus, even if the 404(b) evidence was erroneously admitted, it was unlikely that the jury would have reached a different result. The Court of Appeals decision was therefore modified and affirmed.

Chief Justice Newby concurred separately. He joined in the result but would not have discussed the defendant's arguments in light of the Court's assumption of error.

The defendant's Confrontation Clause rights were violated by the introduction of an unavailable witness's plea allocution in a related case; no "opening the door" exception to the right to confront

Hemphill v. New York, 595 U.S. __, 142 S. C.t 681 (2022). In this murder case, the Supreme Court determined that the defendant's Sixth Amendment right to confront witnesses against him was violated when the trial court admitted into evidence a transcript of another person's plea allocution. In 2006, a child in the Bronx was killed by a stray 9-millimeter bullet. Following an investigation that included officers discovering a 9-millimeter cartridge in his bedroom, Nicholas Morris was charged with the murder but resolved the case by accepting a deal where he pleaded guilty to criminal possession of a .357-magnum revolver in exchange for dismissal of the murder charge. Years later, the defendant Hemphill was charged with the murder. At trial, for which Morris was unavailable as a witness, Hemphill pursued a third-party culpability defense and elicited undisputed testimony from the State's law enforcement officer witness indicating that a 9-millimeter cartridge was discovered in Morris's bedroom. Over Hemphill's Confrontation Clause objection, the trial court permitted the State to introduce Morris's plea allocution for purposes of proving, as the State put it in closing argument, that possession of a .357 revolver, not murder, was "the crime [Morris] actually committed." Relying on state case law, the trial court reasoned that Hemphill had opened the door to admission of the plea allocution by raising the issue of Morris's apparent possession of the 9-millimeter cartridge.

After finding that Hemphill had preserved his argument by presenting it in state court and accepting without deciding that the plea allocution was testimonial, the Supreme Court determined that admission of Morris's plea allocution violated Hemphill's confrontation rights and rejected various arguments from the State advocating for an "opening the door" rule along the lines of that adopted by the trial court. Describing the "door-opening principle" as a "substantive principle of evidence that dictates what material is relevant and admissible in a case" the Court distinguished it from procedural rules, such as those described in *Melendez-Diaz*, that the Court has said properly may govern the exercise of the right to confrontation. The Court explained that it "has not held that defendants can 'open the door' to violations of constitutional requirements merely by making evidence relevant to contradict their defense." Thus, the Court reversed the judgment of the New York Court of Appeals which had affirmed the trial court.

Justice Alito, joined by Justice Kavanaugh, concurred but wrote separately to address the conditions under which a defendant can be deemed to have validly waived the right to confront adverse witnesses. Justice Alito wrote that while it did not occur in this case, there are circumstances "under which a defendant's introduction of evidence may be regarded as an implicit waiver of the right to object to the prosecution's use of evidence that might otherwise be barred by the Confrontation Clause." He identified such a situation as that where a defendant introduces a statement from an unavailable witness, saying that the rule of completeness dictates that a defendant should not be permitted to then lodge a confrontation objection to the introduction of additional related statements by the witness.

Justice Thomas dissented based on his view that the Court lacked jurisdiction to review the decision of the New York Court of Appeals because Hemphill did not adequately raise his Sixth Amendment claim there.

Sentencing and Probation

The trial court did not err by ordering restitution for all the seized animals or by failing to explicitly consider the defendant's ability to pay, but erred in converting the restitution award to a civil judgment absent statutory authorization

State v. Crew, ___ N.C. App ___; 868 S.E.2d 351; 2022-NCCOA-35 (Jan. 18, 2022). The defendant was charged with and convicted of dogfighting and related offenses in Orange County. The trial court ordered the defendant to pay Animal Services restitution in the amount of $70,000 for its care and keep of the animals and immediately converted the award to a civil judgment (presumably based on the 60-month minimum active portion of the sentence imposed in the case). Thirty dogs were seized from the defendant's property, but he was only convicted of offenses relating to 17 of the animals. According to the defendant, the restitution award should have therefore been proportionally reduced. The court disagreed, observing that "[t]he trial court may impose restitution for 'any injuries or damages arising directly and proximately out of the offense committed by the defendant,'" pointing to G.S. 15A-1340.34(c). *Crew* Slip op. at 9. Because the defendant's crimes resulted in the removal of all the animals, he could properly be held responsible for the cost of caring for the animals.

The defendant also argued that the trial court erred in failing to consider his ability to pay before ordering restitution. While the trial court need not make express findings on the issue, G.S. 15A-1340.36(a) requires the judge to consider the defendant's ability to pay among several other factors

when deciding restitution. Here, there was evidence in the record concerning the defendant's income, the price of a "good puppy," and of the defendant's living arrangements. "Based on this evidence, the trial court's determination that the defendant had the ability to pay was within the court's sound discretion and certainly not manifestly arbitrary or outside the realm of reason." *Crew* Slip op. at 10-11.

Finally, the defendant argued the trial court improperly converted the restitution award to a civil judgment. The court agreed. The restitution statutes distinguish between offenses subject to the Crime Victim's Rights Act ("VRA") and offenses exempt from that law. G.S. 15A-1340.38 expressly authorizes a trial court to convert an award of restitution to a civil judgment in VRA cases. No similar statutory authorization exists for non-VRA cases. While some other offenses have separate statutory provisions permitting conversion of a restitution award to a civil judgment (*see, e.g.,* G.S. 15-8 for larceny offenses), no such statute applied to the crimes of conviction here. The court noted that G.S. 19A-70 authorizes animal services agencies to seek reimbursement from a defendant for the expenses of seized animals and observed that the agency failed to pursue that form of relief. The court rejected the State's argument that the trial court's action fell within its inherent authority. The civil judgments were therefore vacated. The convictions and sentence were otherwise undisturbed.

Defendant failed to properly make or preserve statutory confrontation objection at probation violation hearing; State presented sufficient evidence of absconding

State v. Thorne, 279 N.C. App. 655; 2021–NCCOA–534 (Oct. 5, 2021). The defendant was placed on 36 months of supervised probation after pleading guilty to one count of conspiracy to obtain property by false pretenses. The defendant's probation officer subsequently filed a violation report alleging that the defendant had violated his probation by using illegal drugs, and an addendum alleging that the defendant had absconded from probation. At the violation hearing, the defendant admitted to using illegal drugs, but denied that he absconded. The state presented testimony at the violation hearing from a probation officer who was not involved in supervising the defendant, but who read from another officer's notes regarding the defendant's alleged violations. The trial court found the defendant in violation, revoked his probation for absconding, and activated his suspended 10-to-21-month sentence. The defendant filed a *pro se* notice of appeal, which was defective, but the court granted his petition for *writ of certiorari* and addressed the merits.

On appeal, the defendant argued that his confrontation rights under G.S. 15A-1345(e) were violated when the trial court allowed another probation officer to testify from the supervising officer's notes, over the defendant's objection. However, at the hearing the defendant did not state that the objection was based on his statutory confrontation right, nor did he request that the supervising officer be present in court or subjected to cross-examination. The court held that, at most, it could be inferred that the defendant's objection was based on hearsay grounds or lack of personal knowledge. The court rejected the defendant's argument that the issue was preserved despite the absence of an objection because the trial court acted contrary to a statutory mandate, per *State v. Lawrence*, 352 N.C. 1 (2000). In this case, the trial court did not act contrary to the statute because the objection made at the hearing was insufficient to trigger the trial court's obligation to either permit cross-examination of the supervising officer or find good cause for disallowing confrontation. Therefore, the officer's testimony based on the notes in the file was permissible, and it established that the defendant left the probation office without authorization on the day he was to be tested for drugs, failed to report to his probation officer, did not respond to messages, was not found at his residence on more than one occasion, and could not be located for 22 days. Contrasting these facts with *State v. Williams*, 243 N.C. App. 198 (2015), in which the evidence only established that the probationer had committed the lesser violation of failing to allow

his probation officer to visit him at reasonable times, the evidence here adequately showed that the defendant had absconded. The court therefore affirmed the revocation but remanded the case for correction of a clerical error because the order erroneously indicated that both violations justified revocation, rather than only the absconding per G.S. 15A-1344(d2).

Restitution amount was not speculative where it was based on evidence of fair market value

State v. Redmond, ___ N.C. App. __; 868 S.E.2d 661; 2022-NCCOA-5 (Jan. 4, 2022). The restitution amount was supported by competent evidence. A witness for the state testified that a potential buyer at the show asked what the painting would cost when completed and was told $8,850, which was the gallery's standard price for paintings of that size by this artist. The artist also testified that the canvas was now completely destroyed, and the black ink could not be painted over. The trial court ordered the defendant to pay half that amount as restitution. The appellate court held that the fact that the painting "had not yet been purchased by a buyer does not mean that the market value assigned by the trial court for restitution was speculative." The evidence presented at trial was sufficient to establish a fair market value for the painting prior to it being damaged, and the trial court's restitution order would not be disturbed on appeal.

The trial court abused its discretion in concluding a crime was committed and revoking defendant's probation where there was no evidence beyond the fact that the defendant was arrested that tended to establish he committed a crime

State v. Graham, ___ N.C. App. ___; 869 S.E.2d 776; 2022-NCCOA-132 (Mar. 1, 2022). The defendant pled guilty to second-degree murder and possession of a firearm by a convicted felon. The defendant was sentenced to active terms of 176-221 months imprisonment for the second-degree murder charge and 16-20 months imprisonment for the possession of a firearm by a convicted felon charge. The active sentence for possession of a firearm by a convicted felon was suspended for 36 months of supervised probation, which commenced in August 2019 after the defendant was released from prison following his active sentence for second-degree murder.

In February 2021, the State filed a violation report alleging that the defendant violated his probation by failing to pay the full monetary judgment entered against him and because he was arrested and charged with possession of a firearm by a felon. Following a hearing, the trial court found that the defendant committed a crime and revoked the defendant's probation. The Court of Appeals granted the defendant's petition for writ of certiorari.

On appeal, the defendant argued that the trial court erred in revoking his probation. The Court of Appeals agreed, reasoning that in order to revoke a defendant's probation for committing a criminal offense, there must be some form of evidence that a crime was committed. The only evidence presented at the probation revocation hearing was the probation officer's violation report and testimony from the probation officer. The Court concluded that this evidence only established that defendant was arrested for possession of a firearm by a felon and that there was no evidence beyond the fact that defendant was arrested that tended to establish he committed a crime. The Court thus held that the trial court abused its discretion in concluding a crime was committed and revoking defendant's probation.

Post-Conviction and Appeals

The trial court properly applied the multi-factor test for evaluating an MAR based on newly discovered evidence.

State v. Reid, 2022-NCSC-29, ___ N.C. ___ (Mar. 11, 2022). In this Lee County case, the trial judge granted a motion for appropriate relief and awarded a new trial for a defendant who was convicted of first-degree murder committed when he was fourteen years old, largely on the basis of a confession made during a police interrogation conducted outside the presence of a parent or guardian. Years later, postconviction counsel located a new witness who claimed a different person had confessed to the crime, exculpating the defendant. The trial court found the new witness's testimony credible and granted the MAR based on the newly discovered evidence and ordered a new trial. The Court of Appeals reversed, saying the trial court abused its discretion and erred in granting a new trial, in that the defendant's affidavit failed multiple prongs of the seven-factor test for evaluating newly discovered evidence set forth in *State v. Beaver*, 291 N.C. 137 (1976). *State v. Reid*, 274 N.C. App. 100 (2020).

After allowing the defendant's petition for discretionary review, the Supreme Court reversed the Court of Appeals, concluding that the trial court properly applied the *Beaver* test. First, the trial court did not err in concluding that the newly discovered evidence was "probably true," despite the inconsistencies in the new witness's testimony. It was the factfinder's role—not the role of the Court of Appeals—to evaluate the credibility of the witness and make findings of fact, which are binding on appeal if supported by the evidence. The Court of Appeals thus erred by reweighing the evidence and making its own findings as to whether the new evidence was "probably true."

Second, the trial court did not err in finding that the defendant's trial counsel had exercised due diligence in attempting to procure the newly discovered evidence. The trial court's findings that an investigator had earlier attempted to find the new witness and that those efforts were unsuccessful due in part to interference by the witness's mother were supported by the evidence and binding on appeal. The Court noted that the "due diligence" prong of the *Beaver* test requires "reasonable diligence," not that the defendant have done "everything imaginable" to procure the purportedly new evidence at trial. Where, as here, neither the defendant nor his lawyer knew whether the sought-after witness actually had any information about the victim's killing, hiring an investigator was deemed reasonable diligence without the need to take additional steps such as issuing an subpoena or asking for a continuance.

Third, the Court concluded that the trial judge did not err in concluding that the new witness's testimony was "competent" even though it was hearsay. The evidence was admitted without objection by the State, and was therefore competent. And in any event, the test for competence within the meaning of the *Beaver* test is not admissibility at the MAR hearing, but rather whether it would be material, competent, and relevant in a future trial if the MAR were granted. Here, the trial court properly concluded that the new witness's testimony would have been admissible at trial under the residual hearsay exception of Rule 803(24).

Finally, the trial court did not err in concluding that the addition of the newly discovered evidence would probably result in a different outcome in another trial. Though the defendant's confession was admissible, it was nonetheless the confession of a fourteen-year-old and might therefore receive less probative weight in a case like this where the other evidence of the defendant's guilt was not overwhelming.

The Supreme Court reversed the Court of Appeals and remanded the case for a new trial.

Chief Justice Newby, joined by Justice Barringer, dissented. He wrote that the defendant failed to meet the "due diligence" prong of the *Beaver* test in that he did not take reasonable action at trial to procure the evidence he later argued was newly discovered. The Chief Justice disagreed with the majority's conclusion that hiring an investigator was enough. Rather, he wrote, the defense lawyer should have gone to the trial court for assistance in obtaining testimony from the witness (such as through a material witness order), or spoken to other witnesses who likely had the same information (such as the sought-after witness's brother).

BLUNT FORCE TRAUMA

What the soft tissues can tell us (external injuries)

GODOY MEDICAL FORENSICS INCORPORATED

1

Tara M Godoy, BSN, RN, CFN

President/Founder of Godoy Medical Forensics

Bachelor's Degree in Nursing, 2001
University of Southern California

Forensic Experience
Forensic Nurse – 10 years
Certificate in Forensic Nursing, 2012
UC Riverside

Clinical Experience:
Stanford Medical Center ER – 4 yrs
Other ER experience – 2 years Critical Care
Transport – AMR – 1 year

Testimony Experience:
*Blunt Force Trauma
*Strangulation

Testified in Superior and Federal Courts
Testified for both Prosecution and Defense

GODOY MEDICAL FORENSICS INCORPORATED

2

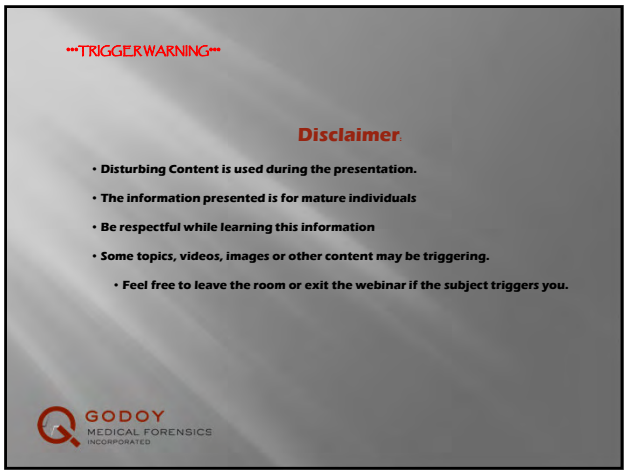
RN's
- All have ER/Trauma background
- Located all over the nation
- Highly educated
- Experienced in criminal law

See photos and bios of our team at www.godoymedical.net/forensic-nurse-experts/

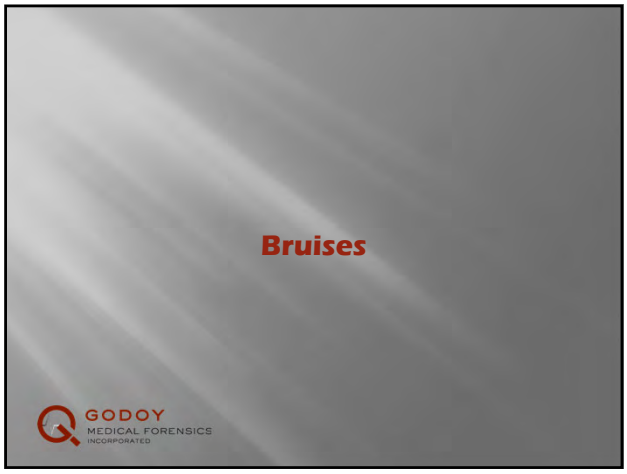
MD's
- ER/Trauma (N. CA)
- Orthopedic Surgery (N. CA)
- Neurosurgeon (S. FL)

Forensic Toxicologist (So Cal.)

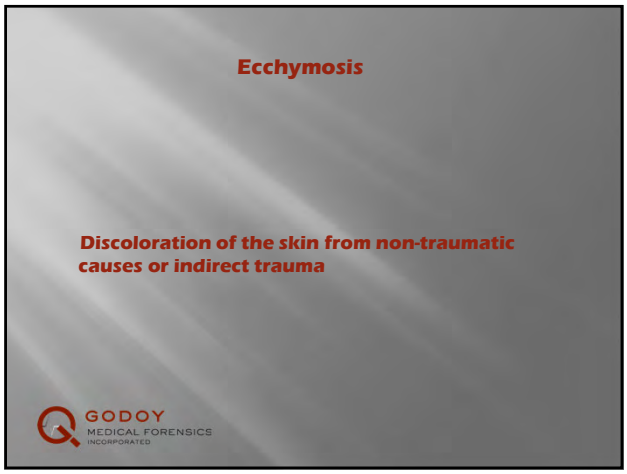
3


TRIGGER WARNING
Disclaimer
• Disturbing Content is used during the presentation.
• The information presented is for mature individuals
• Be respectful while learning this information
• Some topics, videos, images or other content may be triggering.
• Feel free to leave the room or exit the webinar if the subject triggers you.
GODOY
MEDICAL FORENSICS
INCORPORATED

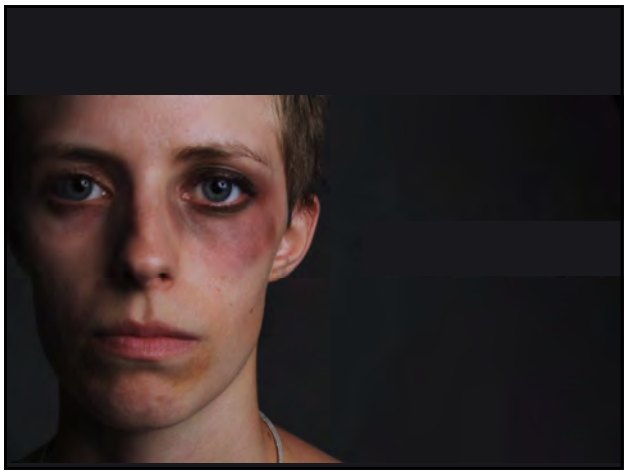
4


Bruises
GODOY
MEDICAL FORENSICS
INCORPORATED

5


Ecchymosis
Discoloration of the skin from non-traumatic causes or indirect trauma
GODOY
MEDICAL FORENSICS
INCORPORATED

6



7

Contusions

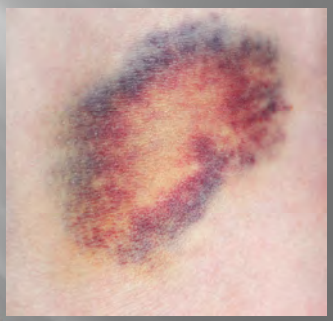
Impact with a hard object or pressure that causes the blood vessels to burst and blood to leak out into the cellular space.

May involve multiple layers and go as deep as the underlying organs.

GODOY MEDICAL FORENSICS INCORPORATED

8

Bruises/Contusions



GODOY MEDICAL FORENSICS INCORPORATED

9

Can you date bruises?

TABLE 1 Bruise dating scales and coloration. Adapted: [2]

Source	Bruise color	Bruise age
Camps	Red	Immediately
	Dark purple/black	Shortly after
	Green	4 to 5 d
	Yellow	7 to 10 d
	Disappearance	14 to 15 d
Glaister	Violet	Immediately
	Blue	day 3
	Green	5 to 7 d
	Yellow	8 to 10 d
	Disappearance	13 to 18 d
Polson and Gee	Dark red /red and black	less than 24 h
	Greenish	day 7
	Yellowish	day 14
	Disappearance	up to 30 d
Smith and Fides	Red	Immediately
	Purple/black	Shortly after
	Green	4 to 5 d
	Yellow	7 to 10 d, but small and superficial on day 3
	Disappearance	14 to 15 d

GODOY MEDICAL FORENSICS INCORPORATED

Tirado, J., & Mauricio, D. (2020, Aug 31). Bruise dating using deep learning. *Journal of Forensic Sciences, 00*, 1-11. doi:https://doi.org/10.1111/1556-4029.14578

10

Can you age bruises accurately in children? A systematic review.

-(S Maguire, MK Mann, J Sibert, A Kemp, 2005)

Reviewed 167 studies, only 3 met inclusion criteria

- Dating of Bruises in Children: An Assessment of Physician Accuracy (Bariciak, Plint, Gaboury, & Bennett, 2003)
- Estimation of the age of bruising (Stephenson & Bialas, 1996)
- The prevalence and distribution of bruising in babies (Carpenter, 1998)

Conclusions of reviewers:

- assessment of age of bruise in children is inaccurate
- color discrimination with human eye is poor
- different colors can be observed in bruise anytime prior to resolution

GODOY MEDICAL FORENSICS INCORPORATED

11

The Life Cycle of Bruises in Older Adults.

- (Mosqueda, Burnight, & Liao, 2005)

- **Assessed bruises in adults 65+ years**
  - Sample: 101 patients, 108 bruises
  - Examined daily
- **Findings:**
  - Bruises remained visible from 4-41 days
  - Yellow: 16/108 (14.8%) within 24 hours**, 60% at 6 days
  - Purple: uncommon after 11 days (<5%)
  - Red: Present up to 6 weeks

GODOY MEDICAL FORENSICS INCORPORATED

12

The ageing of bruises: a review and study of the colour changes with time.
- (Langlois & Gresham, 1991)

- **369 photographs**
  - **Sample: 89 patients, aged 10-100**
  - **Bruises 6h to 21d old**
- **Findings:**
  - **Yellow develops faster in patients <65 years**
  - **Yellow: 18h+ old**

GODOY MEDICAL FORENSICS INCORPORATED

13

Problems with dating bruises

- **Inter-rater reliability**
- **In person versus photographs**
- **Photographs are affected by lighting/filters**

GODOY MEDICAL FORENSICS INCORPORATED

14

Assessment of bruise age on dark-skinned individuals using tristimulus colorimetry.
- (Thavarajah, Vanezis, & Perrett, 2012)

18 subjects of South Indian or Sri-Lankan ethnicity
- **Bruises inflicted using vacuum pump**
- **Daily color measurements**
- **Control – 2 Caucasians**

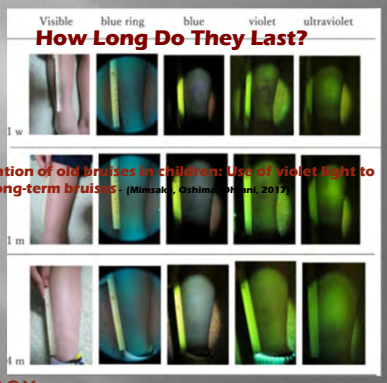
Findings:
- **Bruises on dark skinned individuals can be measured, even if bruises are unclear visually**
- **Yellow: can't be seen or measured on dark skinned individuals**

GODOY MEDICAL FORENSICS INCORPORATED

Thavarajah, D., Vanezis, P., & Perrett, D. (2012). Assessment of bruise age on dark-skinned individuals using tristimulus colorimetry. *Medicine, Science and the Law*, *52*(1), 6-11. doi:https://doi.org/10.1258/msl.2011.011038

15

How Long Do They Last?



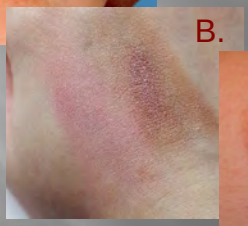
Visualization of old bruises in children: Use of violet light to record long-term bruises - (Mimsaki, Oshima, Ohkami, 2017)

GODOY MEDICAL FORENSICS INCORPORATED

17

Poll 1: Which is a bruise?
select all that apply

A.



B.

C.

GODOY MEDICAL FORENSICS INCORPORATED

18

Poll 2: Which is abuse?

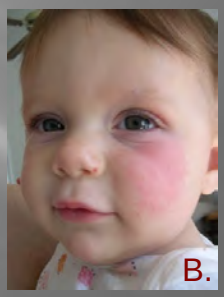
A.

B.

GODOY MEDICAL FORENSICS INCORPORATED

19

Poll 3: Which is abuse?



GODOY MEDICAL FORENSICS INCORPORATED

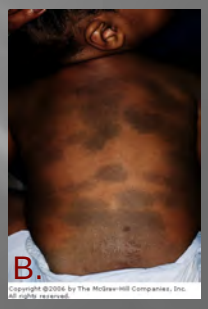
20

What is it?

GODOY MEDICAL FORENSICS INCORPORATED

21

Poll 4: Which is a bruise?



GODOY MEDICAL FORENSICS INCORPORATED

22

Poll 5: Which is abuse?

GODOY MEDICAL FORENSICS INCORPORATED

23

Case Study 1

GODOY MEDICAL FORENSICS INCORPORATED

24

Case Study 1

GODOY MEDICAL FORENSICS INCORPORATED

25

Case Study 1

GODOY MEDICAL FORENSICS INCORPORATED

26

Hematoma

A collection of blood under the skin from a burst blood vessel.

GODOY MEDICAL FORENSICS INCORPORATED

27

"Goose Egg"

GODOY MEDICAL FORENSICS INCORPORATED

28

Abrasions

A scrape from friction between the skin and another surface.

GODOY MEDICAL FORENSICS INCORPORATED

29

"Scratch"

GODOY MEDICAL FORENSICS INCORPORATED

30

Abrasion

GODOY MEDICAL FORENSICS INCORPORATED

31

Abrasion

GODOY MEDICAL FORENSICS INCORPORATED

32

Cuts

An opening in the skin caused by a sharp object - such as a knife or scalpel.

GODOY MEDICAL FORENSICS INCORPORATED

34

Cut or Incision

GODOY MEDICAL FORENSICS INCORPORATED

35

Lacerations

A tear in the skin from an impact that causes the skin to split apart.

GODOY MEDICAL FORENSICS INCORPORATED

36

Laceration

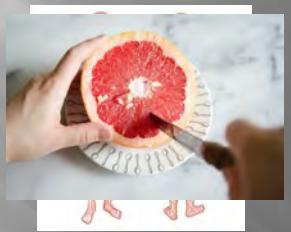
Matthew M. Lunn, in Essentials of Medicolegal Death Investigation, 2017

GODOY MEDICAL FORENSICS INCORPORATED

https://www.aceponow.com/article/laceration-incised-wound-know-difference/

37

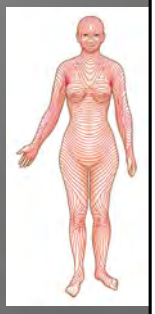
Langer's lines



GODOY MEDICAL FORENSICS INCORPORATED

38

Langer's lines



GODOY MEDICAL FORENSICS INCORPORATED

39

Mtn Bike Crash

GODOY MEDICAL FORENSICS INCORPORATED

40

Cut or Laceration??

GODOY MEDICAL FORENSICS INCORPORATED

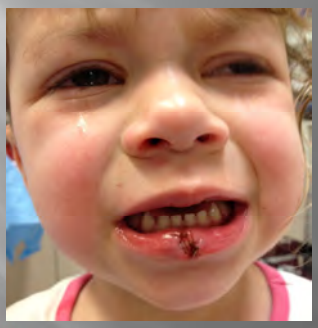
41

Case Study 2

GODOY MEDICAL FORENSICS INCORPORATED

42

Poll: CPS case?



GODOY MEDICAL FORENSICS INCORPORATED

43

Avulsion

Soft tissues, musculature, and/or bone are torn away from the normal points of attachment.

GODOY MEDICAL FORENSICS INCORPORATED

45

Types of Avulsion

- Eyelid–MVA, dog bites, human bites
- Nerve–MVA or neonate injury during delivery
- Tooth–exposure of dental pulp
- Surgical–ingrown nail, varicose veins
- Periosteal–peeling the bone covering off the bone

GODOY MEDICAL FORENSICS INCORPORATED

46

Avulsions

Ear

Nail

GODOY MEDICAL FORENSICS INCORPORATED

47

Leg Avulsion

GODOY MEDICAL FORENSICS INCORPORATED

48

49

Avulsion–degloving

GODOY MEDICAL FORENSICS INCORPORATED

50

Avulsion–degloving

GODOY MEDICAL FORENSICS INCORPORATED

51

Multiple Injuries

GODOY MEDICAL FORENSICS INCORPORATED

52

Laceration, Abrasion and Bruise

GODOY MEDICAL FORENSICS INCORPORATED

53

Case Study 3

GODOY MEDICAL FORENSICS INCORPORATED

54

Case Study 3

GODOY MEDICAL FORENSICS INCORPORATED

55

Other Injuries - Patterned Injuries

GODOY MEDICAL FORENSICS INCORPORATED

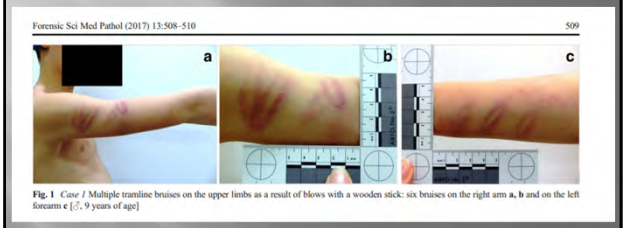
56

What do you see?

GODOY MEDICAL FORENSICS INCORPORATED

59

Pattern Injuries-contusion


Forensic Sci Med Pathol (2017) 13:508–510 509

a b c

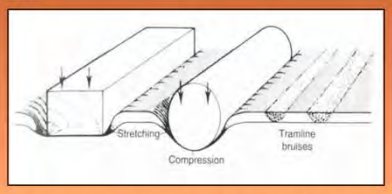
Fig. 1 *Case 1* Multiple tramline bruises on the upper limbs as a result of blows with a wooden stick: six bruises on the right arm **a**, **b** and on the left forearm **c** [♂, 9 years of age]

GODOY MEDICAL FORENSICS INCORPORATED

60

Pattern Injuries-contusion

Tram line contusions are caused by - canes, wires, batons, rubber hoses, PVC pipes, whips



Due to the compression the bruising will be prominent over margins making parallel lines

GODOY MEDICAL FORENSICS INCORPORATED

https://med.pdn.ac.lk/departments/forensic

61

Medical records or traumatic injuries

Services – Expert Witness

Expert Review and Consultation

Written reports
- Opinion based
- Summary reports for sentencing/mitigation

Testimony
- Experienced and professional experts

Services – Consulting

Trial support
- Direct/Cross Questions
  - Other experts
  - Vic/Def
- Med record organization
- Fact Chronology
- Expert witness search/vetting services

Summary reports (without testimony)

http://godoymedical.net/services/

GODOY MEDICAL FORENSICS INCORPORATED

62

We have expertise!

DUI - Medical
- FST's
- Underlying medical conditions
- Concussions
- Blood draws (AMP)

Injury Assessment
- Bodily Injury Severity (SBI/GBI)
- Mechanism
- Homicide – autopsy analysis
- Elder abuse
  - Pressure sores
  - Traumatic injuries

Toxicology
- DUI
- Homicide
- Possession
- Intoxication
- Symptoms/effects on body

Child Abuse
- AHT/Shaken Baby
- Physical Abuse
- Neglect/FTT
- Munchausen's by Proxy

Strangulation
- Non-fatal
- Fatal

SART/SANE

GODOY MEDICAL FORENSICS INCORPORATED

63

www.GodoyMedical.net
Info@GodoyMedical.net

What's on our website?

GodoyMedical.net/tools
- SDT list for medical records
- Medical abbreviation cheat sheet
- Case studies

GodoyMedical.net/new/
- Online case submission

GodoyMedical.net/blog/
- Years of valuable posts!
- (Newsletter subscription on homepage)

GodoyMedical.net/calendar
- FREE CLE eligible webinars!
  - Blunt Force Trauma
  - Reading Medical Records
  - Strangulation
  - Traumatic Brain Injury
  - Bodily Injury
  - NEW: THC – Recognizing Impairment
  - Coming soon: AHT and Long Term TBI

GODOY MEDICAL FORENSICS INCORPORATED

64

DIGITAL FORENSICS //

ENVISTA FORENSICS

Expert Testimony: Digital Forensics

Lars Daniel, EnCE, CCPA, CCO, CTNS, CTA, CWA, CIPTS
Practice Leader – Digital Forensics

What is an Expert?

In the field of digital forensics, there is no governing body at the national or state level than accredits examiners is being competent in their field. The industry does not have a bar exam or other system in place to ensure that experts in digital forensics possess even the minimum qualifications necessary to practice in this field. This complicates selecting a digital forensics expert, and the complications multiply when numerous forms of digital evidence are in a case. For example, an expert may be competent in computer forensics, but have no experience in mobile phone or GPS forensics.

Depending on your state or jurisdiction, the test used to determine whether or not expert testimony will be allowed by the court may be the Frye test (Frye v. United States . 293 F. 1013 (D.C. Cir. 1923) 1 , Daubert test (Daubert v. Merrell Dow Pharmaceuticals , 509 U.S. 579 (1993)) 2 , Porter test (State v. Porter , 241 Conn. 57, 698 A.2d 739 (1997) 3 , cert. denied, 523 U.S. 1058, 118 S. Ct. 1384, 140 L. Ed.2d 645 (1998), Sec. 7-2 Connecticut Code of Evidence), 4 or other test outlined in that state's code. Many states have practice manuals and a set of specific statutes that govern experts and expert testimony. Contacting your state bar association is an excellent way to locate this type of information. The Federal system uses Section 700 of the Federal Rules of Evidence, and specifically Rule 702 to define expert witness testimony.

> Federal Rules of Evidence: Rule 702. Testimony by Experts:
>
> If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case.

No matter which rule governs your particular case, all experts must first qualify as an expert in any case in the United States where they will be asked to provide expert testimony. When determining what expert is best for your case, it is important to establish a selection criterion.

What evidence is part of your case?

If your case includes multiple types of evidence, such as computers, mobile phones, social media accounts, and call detail records, it is critical that your expert is qualified and all of these areas. To cover all the bases, it may be necessary to have multiple digital forensic experts on a single case to cover all the forms of evidence. Given the complexity and myriad of sub disciplines within digital forensics, this is a highly probable reality.

What type of case do you have?

The expert you employee should have expertise and experience in a particular type of case that you have. If you have a data breach with a loss of personally identifiable information, an expert in cyber security and protocols related to proper cyber hygiene is exactly what you need. However, that same expert may not have the correct tool set to handle a medical malpractice case where a mobile phone examination is needed to determine the location of a doctor the night before, or to recover deleted text messages that might be of evidentiary value.

The Prequalification Process

Once you have determined a list of potential experts, it is helpful to go through a prequalification process to determine which one is the best fit. Resumes and curriculum vitae should be examined, and the following questions can assist in the decision making process.

Does the examiner have forensic training and experience?

Well a technical expert may have an impressive resume, digital forensics is a niche and specialized field. Technical certifications related to networking, computer repair, or other information technology disciplines are not the same as digital forensic certifications. There are numerous certifications specific to digital forensics that show a level of competency. The certifications also greatly improve the likelihood that the expert will be able to qualify as an expert in court.

CASE EXAMPLE

In the NC vs. Cooper homicide case Google map evidence was critical in the defense of Bradley Cooper according to defense counsel. In order to proffer this evidence, the defense attempted to call Jay Ward as their expert. Jay Ward had over 15 years of experience in network security and information technology. Despite this, the court ruled that he could not testify to the evidence because he lacked the necessary qualifications:

"The State focused on Ward's lack of training and experience as a forensic computer analyst. The trial court agreed with the State and, on 19 April 2011, ruled that Ward could not testify specifically about the Google Map files."

https://lawprofessors.typepad.com/evidenceprof/2013/09/in-2006-i-was-living-inchelsea-one-day-my-wife-our-friend-and-i-went-to-thewhole-foodsin-chelsea-while-we-were-in-the-c.html#

What are the fees charged by the examiner? Are they reasonable?

Wow there is a range of hourly rates within all professional services, there is a range that is reasonable. If rates are too high it should raise suspicions, and if they are too low this is likewise the case. If they are too high, you're potentially getting fleeced, and if they are too low it should bring in the question if the expert has the appropriate tools and expertise to do the work. Remember, anyone can hang a shingle on their door and claim to do digital forensics since there is no governing agency for the field. The best way to get an estimate on appropriate hourly rates is to get quotes from numerous repeatable digital forensic companies.

What tools and software does the examiner have?

Since there is no governing agency ensuring that a client will have an actual qualified examiner, knowing the tools and software that the digital forensics expert utilizes in the process of their examination is critical. This is because the true barrier to entry to actually doing digital forensics work is the cost to acquire the forensic tools and software to do the work properly. A list of example forensic certifications and the corresponding forensic tools, software, and disciplines are as follows:

Computer Forensics

Magnet Forensics Certified Examiner (MCFE)
Certified Expert in Cyber Investigations (CECI)

Encase Certified Examiner (EnCE)

Digital Forensics Certified Practitioner (DFCP)

Certified Blacklight Examinar (CBE)

Certified Computer Examiner (CCE)

Certified Forensic Investigation Professional (CFIP)

Certified Mac Forensics Specialist (CMFS)

OSForensics Certified Examiner (OSFCE)

Cell Phone Forensics

XRY Certified Examiner (XRY)

Cellebrite Certified Operator (CCO)

Cellebrite Certified Physical Analyst (CCPA)

Cellebrite Advanced Smartphone Analysis (CASA)

Cellebrite Certified Mobile Examiner (CCME)

Cell Phone Tracking and Location

Certified Telecommunications Analyst (CTA)

Certified Wireless Analysis (CWA)

Certified Telecommunications Network Specialist (CTNS)

Certified IP Telecommunications Specialist (CIPTS)

GPS Forensics

Blackthorn Certified Examiner (BCE)

CASE EXAMPLE

In a civil case that later became a Federal RICO case, the opposing expert was ordered by the court to provide forensic images (copies) of all the computers at the defendant's location. The opposing expert used an information technology tool to make copies of the computers. This tool is not a forensic tool and does not have the capability to provide the forensic hash algorithms or cyclical redundancy checks that allow an examiner to know, without a doubt, that the evidence is above reproach. Our examiner testified as an expert witness in the case explaining the problem with these copies. At the end of our expert's testimony, the judge ruled from the bench in favor of the plaintiff due to the improper handling of the evidence by the opposing expert and the lack of cooperation by the defense due to their refusal to provide the original evidence items to us.

What to Expect from an Expert

When you contact a forensics expert, you may not know exactly what you need or where the Data will be located that could be a potential evidentiary value. Further, depending on the case, the steps that must be taken for a proper examination and very considerably. An expert should be able to assist you in every step of the process, including:

1. Obtaining evidence

    a. An expert should be able to assist you in the technical portions when developing motions and orders to access evidence. In many instances, if the evidence is not asked for correctly with the proper technical terminology, it will result in receiving the wrong information, or nothing at all.

    b. An expert should be able to assist you in determining where valuable data is to your case. This includes if the data is on local devices such as mobile phones and computers, network share drives, in cloud storage, or social media accounts.

2. Analysis

    a. In order to perform an analysis, it is often required that a protocol be in place before an work can even begin. An expert should be able to assist you in creating a protocol for the examination of evidence, and this protocol should provide the necessary information to ensure all parties involved that the original evidence items will remain exactly as they were

before the examination. Every attempt should always be made in a digital forensics analysis to preserve digital evidence as a "snapshot in time" of exactly how they existed upon seizure or forensic imaging (copying).

b. Your expert should be able to verify the work of an opposing expert to determine if the findings are valid. This involves performing an independent analysis of the evidence to ensure all the facts are accurate, and also that all of the evidence has been completely analyzed. It is not uncommon for some experts to find their alleged "smoking gun", and then proceed to end their examination prematurely as they have not taken all of the data into account.

3. Court Preparation
    a. If a case is going to go to trial, your expert should be able to assist you in understanding what an opposing expert is going to say based upon their forensic report. Further, your expert should be able to assist you in writing direct examination for themselves, and in preparing cross examination for an opposing expert.

Expert testimony is the culmination of everything that goes into a digital forensic examination, from consultation, acquisition, analysis, reporting, and finally to the courtroom. Selecting the expert with the appropriate technical expertise and experience is vital, but just as important is that expert's ability to explain technical concepts, forensic procedures, and digital artifacts in plain language. The use of jargon and acronyms is detrimental to the triers of fact. At the end of the day, if an expert has an airtight analysis but cannot communicate effectively to a judge and jury, the words are meaningless. As a final parting recommendation, when selecting an expert choose one or you can have a conversation with. If that expert cannot explain technical details to you in an accessible way, they likely don't understand what they are talking about themselves.

DIGITAL FORENSICS //

ENVISTA FORENSICS

Don't Geofence Me In: Have You Been Caught in a Google Location History Warrant?

Spencer McInvaille, CCPA, CCO, CTNS, CWA

Digital Forensic Examiner at Envista Forensics

You roll out of bed, prepare for work, help the kids get ready for school, and say your morning farewells. About the time you start your car, you receive the first notification for the day, "Light traffic to Starbucks this morning, approximately 15 minutes."

With technology so embedded into our daily lives, many have become desensitized to its implications on privacy. Some argue that modern life's hectic pace requires a mobile phone to act as a digital assistant, providing reminders, intel, document storage, and even location information. How else would you know if traffic allowed for a coffee before work?

For our mobile phones to be helpful assistants, they must collect data about us, and, unsurprisingly, they do. People today are aware that our phones track us now more than ever before. Perhaps you have heard how your cellular provider records your location data in Call Detail Records (CDRs) or how social media applications geotag pictures and videos with location information.

Most people are unconcerned about this, claiming they have nothing to hide. Why would I be concerned about the location data I generate if I do nothing wrong? Luis Molina, a man wrongfully charged with murder based upon geofence data, might have something to say about that.[1] Molina's attorney, Heather Hamel, told the Phoenix New Times, “Police had arrested the wrong man based on location data obtained from Google and the fact that a white Honda was

spotted at the crime scene. The case against Molina quickly fell apart and he was released from jail six days later. Prosecutors never pursued charges against Molina, yet the highly publicized arrest cost him his car, his job, and his reputation."[2]

Across the country, Google location history is utilized as evidence in many cases.[3] However, the geofence warrants used to obtain this location data are being litigated against in many states.

What are Geofence Warrants?

Google has responded to thousands of search warrants for geographical searches for all known users in the area, referred to as geofence warrants. The warrant requests Google to search its repository of user location data and turn that data over *anonymously*. These warrants set out a three-step process by which Google will search for location data on its users for a predetermined area and time.

The Three-Step Process in a Geofence Warrant

Step One: Set the Geofence

Step one is a search limited by a geographical area or geofence. This is typically achieved by using a circle or square drawn using geographic coordinates. The search is also defined by time, which encompasses the incident being investigated. Google is instructed to search user data for location data that meets the time and geographic coordinates outlined in the warrant. Once this search is complete, Google returns the users' data to law enforcement. At this stage, the data is advertised as *anonymous* data.

Location History Database Search

It is important to understand, limiting the size of the geofence has no impact on the number of users searched. This is because all location history data is stored in a single database. Since all of the data is stored in one container, the entire container must be searched to find the users' data responsive to the warrant request.

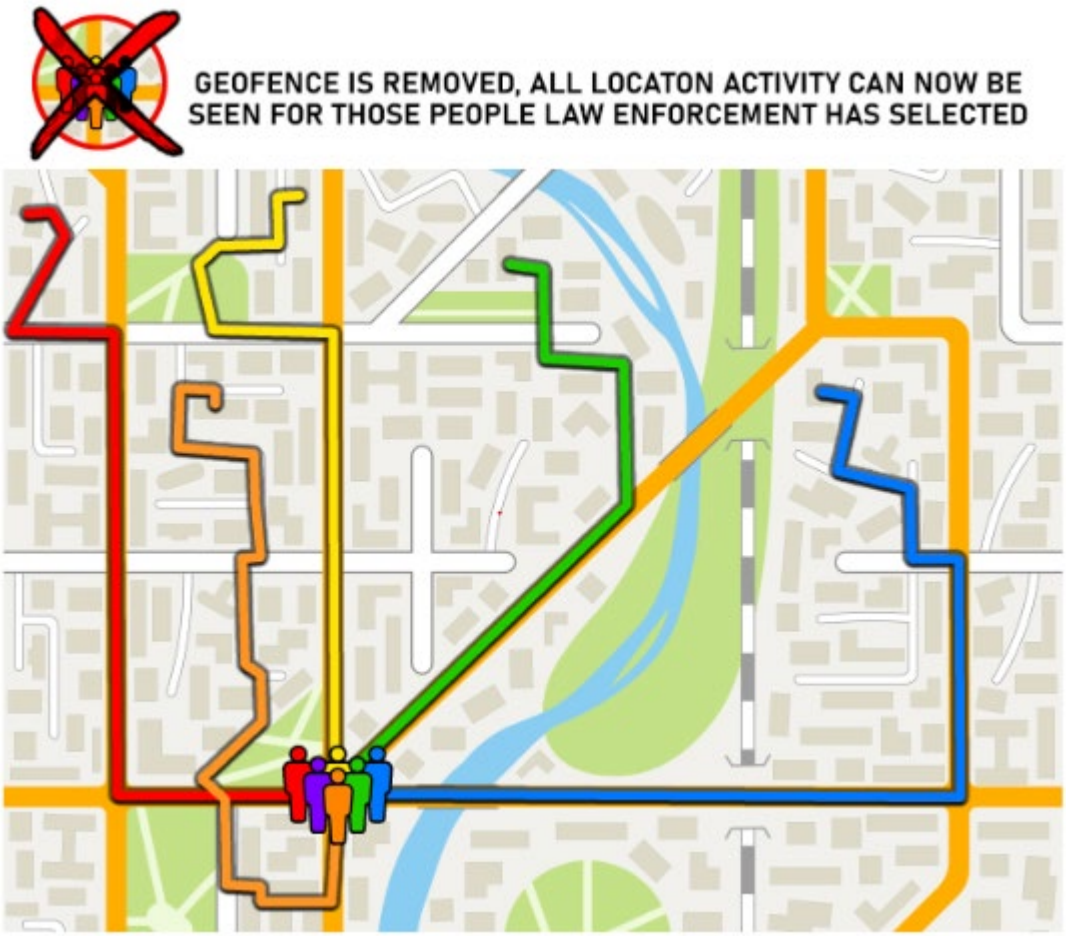
The most unsettling part of this seems to be the indiscriminate search of users' data without their knowledge. In other words, Google needs to search every account with location history to conduct this search. Yes, you read that correctly, ***every account***.

Google representatives declared in documents from United States v. Okello Chatrie, that every warrant requires a search of tens of millions of user accounts.[4] To put that in perspective, Google responded to approximately 9,000 of these search warrants in 2018. That means a search of tens of millions of Google users' data occurred thousands of times. This type of search continues to this day.

Step Two: Examine Contextual Data

Law enforcement determines who they believe are the most likely suspects, and makes a request of Google to provide the contextual data on the step one users. Step two removes the geographical limits and expands the timeframe. This data now shows the step one users before and after they appear in the geofence. You will see the users as they travel from their homes, businesses, places of worship, or any other locations they visited that day. Finally, based on this

data, law enforcement will select the users they believe are suspects or associated with the incident and make the final request.

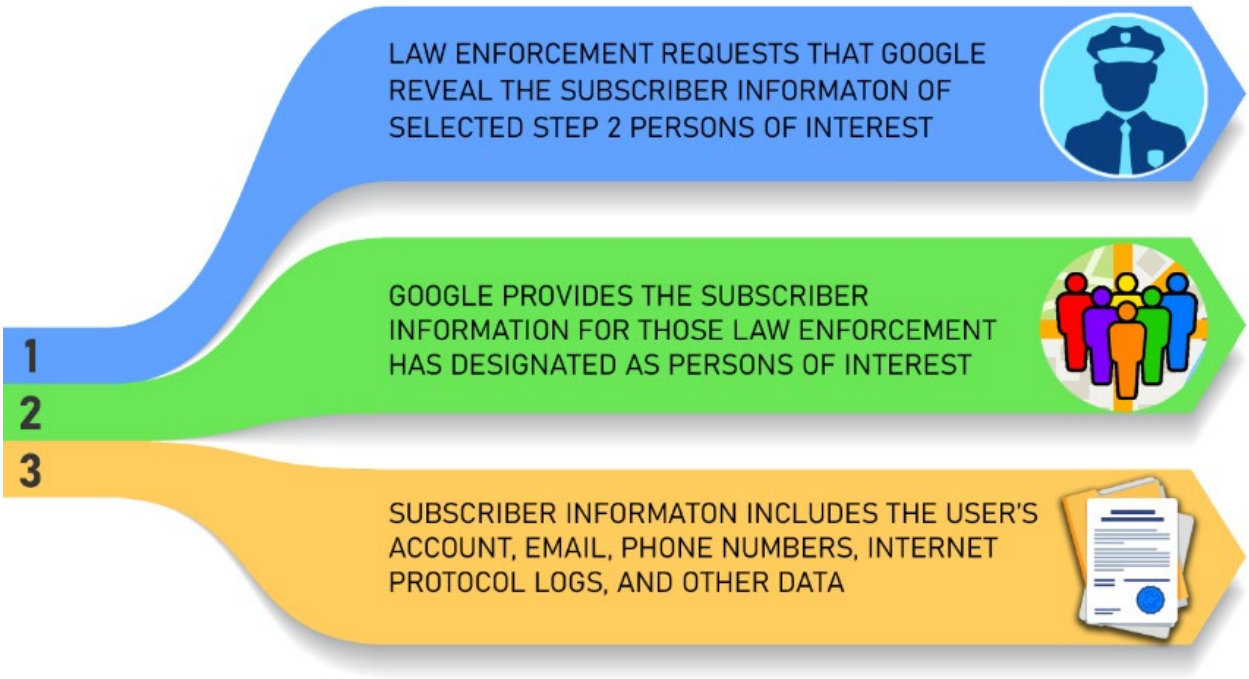


This geofence search warrant process yields private location data about all the parties captured in the search. In step two, users can be tracked when traveling to protected places they frequent in their daily lives. These unique movements are not anonymous but are very identifiable. Think about each place you have been today. What is the likelihood of another person, besides a close family member, going to each of those places simultaneously? Imagine you were caught inside a geofence in the morning. Later that day you visit your doctor, grab

lunch with a love interest, pick your kids up from school, and meet up with friends for a drink that evening before calling it a day. All that activity would be recorded.

Step Three: Subscriber Information

Step three is the final request made based on a geofence warrant. Law enforcement will request the step two users and have Google reveal their subscriber information. This may include the subscriber's Gmail address, telephone number, account number, Google services used, and internet protocol logs associated with the account. This is the "de-anonymization" of the user(s).



Have I been Targeted by a Geofence?

In many instances, these warrants are accompanied by non-disclosure orders that limit Google from notifying their subscribers when their data has been turned over. When a non-disclosure order is not provided, Google has notified targeted users by email. Zachary McCoy of Gainesville, FL received a notification as a result of a geofence warrant that targeted suspects of a burglary in his own neighborhood.[5] "I didn't realize that by having location services on that

Google was also keeping a log of where I was going," McCoy stated. "I'm sure it's in their terms of service but I never read through those walls of text, and I don't think most people do either." McCoy was determined not to be the suspect as a result of the investigation.[6]

Caleb Kenyon, Attorney at Turner, O'Connor, Kozlowski who represented Mr. McCoy, shared his opinion on geofence warrants and stated, "Geofence warrants are law enforcement's latest machinations to harness data harvested by big tech and claim that they aren't conducting a search. But a government entrance through the back door to search your data is still a search under the Constitution. The general geofence warrant fails on multiple fronts: it lacks probable cause for all persons searched and it lacks particularity in the discretion allowed during the execution of the warrant."

Litigation against the use of this technique is heating up. Cases across the nation are receiving attention from the media and Fourth Amendment arguments are at the heart of these cases. The National Association of Criminal Defense Lawyers (NACDL) and the Electronic Frontiers Foundation (EFF) have assisted defense attorneys in litigating these issues. The obvious over-breadth and lack of particularity are among the arguments against the use of these warrants.

Sources:

1 https://www.phoenixnewtimes.com/news/google-geofence-location-data-avondale-wrongful-arrest-molina-gaeta-11426374
2 Avondale Man Sues After Google Data Leads to Wrongful Arrest for Murder | Phoenix New Times
3 https://support.google.com/accounts/answer/3118687?hl=en
4 https://www.nacdl.org/Content/United-States-v-Chatrie,-No-3-19-cr-130-(E-D-Va-)
5 https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761
6 https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761

DIGITAL FORENSICS //

ENVISTA FORENSICS

Data Collections: The Critical Link in Protecting Your Organization in the Face of Potential Litigation

Lars Daniel, EnCE, CCPA, CCO, CTNS, CTA, CIPTS, CWA
Practice Leader – Digital Forensics at Envista Forensics

If a situation arises where litigation is even a remote possibility, it is in an organization's best interest to ensure that the collection of digital data is done in such a way that it is above reproach. Digital forensics tools and methodologies allow for data to be collected in a forensically sound manner that meet industry standards, best practices, and have been tested in the court of law.

As defined by the National Institute for Standards in Technology, digital forensics is the "…application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data."[1]

There is a chain of events that occurs as part of a forensic examination. These events are:

Consultation

During a thorough consultation, a digital forensics expert will work with counsel and the information technology team at an organization to ascertain the location of relevant data and explain the various methods by which this data can be collected.

Acquisition

During the acquisition phase, digital forensics experts utilize forensic tools and methodologies to collect data from various electronic sources. This includes on-site collections, where our experts go on location to make forensic images, or copies, of computers, servers, cell phones, cloud data, social media

[1] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

accounts, and other electronic media. All efforts are made in this process to limit the impact on an organization.

In many instances, remote collections can also be performed, allowing our experts to collect data from anywhere in the world with minimal impact on a business.

Acquisitions of electronic data can also be performed pro-actively. When an employee leaves a business, it is becoming increasingly common for the organization to work with digital forensic specialists to forensically image the employee's computer, phone, or other electronic data. This prepares an employer for potential litigation if this evidence is needed as evidence in court.

Analysis

Using specialized forensic technology and methods, our experts examine the data, including the recovery of deleted data. In our in-depth analysis process, we seek to accurately determine what occurred, how it occurred, and who the responsible parties could be. In the analysis phase, we seek to answer questions such as…

- Did the employee engage in bad faith, providing sensitive information to outside parties?
- Was a documented altered, forged, or otherwise manipulated electronically?
- What actions did a user perform on specific dates and time frames?
- Did the user attempt to delete electronic data?
- Did the user use anti-forensic tools to try and cover their tracks?
- Was company policy broken concerning acceptable computer usage?
- Did an employee steal customer lists on the way out the door?

Reporting

If requested by the client, the reporting phase begins. This is where the technical roadmap is laid out of what happened in a matter. For example, if there was concern that a former employee stole intellectual property, this report would include the explanation and analysis of forensic artifacts that point toward evidence of user attribution. In other words, what files are accessed, how these files were exfiltrated from the organization, who took the data, when the data was stolen, and how it is potentially being used.

Expert Testimony

To provide expert testimony in court, that expert needs to be able to qualify first. If the expertise of the expert is challenged, the attorney calling the expert must make a showing that the expert has the necessary background experience. This includes questions related to the expert's education, certifications, case experience, training, and special knowledge. While in information technology professional is certainly an expert in their field, they are rarely an expert in digital forensics, which require specialized knowledge in niche technical domains. There is a distinct probability that an information technology expert will not be able to qualify as a digital forensic expert, and therefore would be unable to render an expert opinion or at best would have their testimony severely limited by the court.

The Critical Link

The acquisition, or forensic collection phase, is the critical link in the chain of events between consultation and expert testimony that protects a client from accusations of data manipulation, incomplete collections, and spoliation. The forensic process of collecting data utilizes algorithms and checksums that guarantee that collected data is a perfect snapshot in time of what existed on an electronic device.

Using information technology tools in lieu of forensic tools to collect data does not offer this protection and has led to unfavorable outcomes for organizations countless numbers of times. Further, if expert testimony is needed by a digital forensics expert, the only way they can attest to the authenticity and completeness of the data is if it was collected in a forensically sound manner and they have the information needed to back it up. This information comes in the form of forensic software audit logs, and the aforementioned checksums and algorithms.

There is also a benefit to utilizing a neutral third-party to collect data from an organization. This in many ways invalidates the claim that could be brought by opposing parties of bias in the collection process if employees of the organization self-collect or if the data is collected by internal information technology staff.

DIGITAL FORENSICS IN CHILD EXPLOITATION CASES

FINDING YOUR WAY THROUGH

Justin Ussery, Digital Forensics Examiner
Jake Green, Digital Forensics Examiner

About the Authors

Jake and Justin have are both Former Law Enforcement Officers who were assigned as Digital Forensic Examiners and Task Force Officers of the United States Secret Service Electronic Crimes Task Forces in South Carolina and California. Jake and Justin both work matters and cases involving all aspects of Digital Forensics, including Cellular Phones, Tablets, Computers, and Cloud data. This article is meant to give you a brief overview of the frequently and daunting amount of confusing electronic evidence you receive in discovery and an overview of this information you often find in the discovery process of a Child Exploitation matter.

Introduction

This article is meant to give you a brief overview of what is frequently a daunting amount of confusing electronic evidence you may receive via discovery in a child pornography case.

Uniqueness of Child Exploitation or Child Pornography cases

Child pornography cases present unique difficulties because of how attorneys can view the evidence and how experts can examine that evidence. These cases are controlled at the federal level by the Adam Walsh Child Safety and Protection Act of 2006. This act explicitly says government examiners cannot send a report containing child pornography in any form to any person outside of law enforcement. The evidence review likely will take place at a government facility, and we are often supervised by law enforcement officials, often the same ones who performed the original forensics. The Adam Walsh Act prevents child pornography from being disseminated, which is a good thing. However, this places a burden on the defense, as examinations of forensic data need to occur at a law enforcement facility. The examiner may only leave with certain artifacts, which do not contain images or videos, making the onsite review of the evidence critical, as this typically does not take place more than once due to the cost of placing a forensic examiner on site.

Law Enforcement Investigations: Before the Search Warrant

CyberTips

Law Enforcement typically deals with two main entities when it comes to dealing with child pornography: Internet Crimes Against Children (ICAC) and The National Center for Missing and Exploited Children (NCMEC). NCMEC acts as a clearinghouse for business and Electronic Services Providers (ESPs) to report possible illicit media.

After ESPs notify NCMEC, a “CyberTip” is created and forwarded to a Regional ICAC Task Force or local law enforcement agency. The Regional ICAC Taskforce or agency then investigates and collects evidence. The investigating officer may perform a forensic examination of this evidence or may assign this to a qualified forensic examiner.

All of this activity originates with the Cyber Tip.

The Cyber Tip will generally include dates and times of said activity, Internet Protocol (IP) addresses during the period of the event, and account information such as email addresses, phone numbers, mailing addresses, and possible user names of the account utilized during the actions.

Online Law Enforcement Investigation Tools and Resources

Detectives and investigators across our country conduct digital or online investigations with a variety of digital tools and software. Many of these tools are deemed to be "law enforcement sensitive" and in our experience as law enforcement examiners, a court order may be required to gain access to these specific tools for review by a forensic examiner working with defense counsel.

Several keywords and processed should be defined at a basic level before continuing:

IP Addresses

An Internet Protocol address is an identifying number for a computer network. A unique Public IP address is assigned by an Internet Service Provider (ISPs like CenturyLink, RCN, Frontier, Verizon, or AT&T). These assignments are unique to physical locations (modems or gateways), which can distribute the connection physically via a wired network switch or a broadcast wireless network via a Wi-Fi router. Public IP addresses are unique to physical locations (home, business, public Wi-Fi) and are not typically unique to physical devices like cellphones, computers, and tablets.

Once an IP address is documented, the owner of the IP address can be found. IP addresses are owned by Internet Service Providers (ISP).

This identification process proceeds in steps:

The IP address is obtained by law enforcement from an online investigation.

The owner of the IP address is identified using a "reverse" lookup to locate the company that owns the IP address. This is accomplished using a "WHOIS" lookup service. One such service is "whatismyip.com". For instance, looking up a text IP Address shows that the owner of the IP Address is Charter Communications.

One the owner of the IP address is known; the law enforcement officer will create a warrant or subpoena and send that to the owner of the IP address to obtain the subscriber information for the IP address on the date of interest.

GUID: Globally Unique Identifier

GUIDs are an alphanumeric series of numbers that can be assigned by a computer system. For this article, a GUID is assigned to each asset or device within a P2P network. This GUID is unique but can be changed or updated by the P2P network.

Metadata: "Data about data."

While the colloquial definition "data about data" is often used, we prefer "information about data." Metadata is a collection of information about the source or creation of data. This information could

be the manufacturer or model of a camera, GPS location, file metadata such as date and time of creation; or modifications, source, author, or editor.

Hash Value: Electronic DNA

A hash value is the application of a mathematical formula (algorithm) to produce a unique alphanumeric string associated with a single file or a set of files. Changes to the data (even a single bit) will result in the change of the hash value. Hash values allow investigators to identify known images, accurately preserve and reproduce data. Common hash values are MD5 (message-digest algorithm), SHA-1, and SHA-256 (Secure Hash Algorithm).

Through our background, experience, and review of software documentation, we're able to offer some insight into these investigative aids. We cover three unique pieces of software used by law enforcement to conduct online investigations. It should be noted that the log files discussed in each section are unique to each piece of software and should be requested through discovery or court order. The below listed log files do not contain illicit content, images, or media and can be released by law enforcement to a civilian defense examiner.

ShareazaLE

One of the most common investigative tools is a variant of the peer to peer (or "P2P") program, Shareaza, that has enhanced features for investigations. This piece of software allows law enforcement to single out an IP address (known as a "single source download"). ShareazaLE produces a log called "ShareazaLE Summary Report for IP: "0.0.0.0"," where "0.0.0.0" is the target or identified IP address.

Torrential Downpour

This is another free piece of software that has been modified to suit the needs of law enforcement investigators. However, this piece of software operates using a different protocol, called torrents. In the most basic sense, torrents are a series or set of files. The torrent file itself is a set of instructions related to the source file and metadata. These source files can be a single file (i.e., movie) or an archived folder containing multiple files (i.e., sets of photos or music from an album). Torrent files are typically sourced from search engines, websites, or forums, but some Bit Torrent software packages have built-in search features. Torrential Downpour produces a series of log files: Datawritten.xml, Details.txt, Downloadstatus.xml, Netstat.txt, summary.txt, and Torrentinfo.txt. It should be noted that the torrent file itself is not illegal to possess as it contains only metadata.

RoundUp eMule

RoundUp was designed to investigate the eD2K or eDonkey2000 file-sharing network. EMule and similar P2P networks are built around keyword searches. A user enters a general keyword (like "porn"), and the search results in the return of any files containing the keyword (i.e., "child porn" or "adult porn"). RoundUp produces logs named: SummaryLog.txt, DetailedLog.txt, Netstat.txt, IdentityLogging.txt, and IndentitySignatures.xml.

Law Enforcement Investigations:
After the Search Warrant

Major Software Vendors

There are several major software vendors utilized by both government examiners and private examiners alike. For cellular device forensics, you will likely see Cellebrite UFED with Physical Analyzer, Oxygen Forensics Detective, Axiom by Magnet Forensics, and GrayKey by Grayshift. Most cellular device tools rely on three general types of extractions from the phones, but all produce very similar results with a few caveats. There are thousands of applications operated on four major smartphone operating systems: Android, Apple iOS, Windows Mobile, and Blackberry OS. Not every tool can decode and make sense of every single application in the world and that is a primary reason why it is beneficial to utilize a variety of different tools during examinations.

As for computer forensics, you will see Axiom or IEF by Magnet Forensics, Forensic Took Kit by Access Data, Encase by OpenText, Analyze by Griffeye, Forensic Explorer by GetData and BlackLight by Cellebrite (formerly Blackbag Technologies).

Many of these tools can redact child pornography images and safely provide a good deal of metadata about the activities without the dissemination of child pornography by Law Enforcement or prosecutors.

Review of Digital Forensic Evidence

If law enforcement recovers electronic evidence and utilizes forensic tools, the scope of their investigation should not be limited to the simple question of "Is illicit media on this device?" Digital investigations need to be a great deal more comprehensive. An expert should search for any known evidence such as suspect IP Address, GUID, hash values, user attribution, as well as a possible indication of file use and knowledge.

Many law enforcement forensic tools and Cyber Tips identify IP Addresses and GUIDs. A review of these records is essential to identify the physical location of an IP address (possibly the defendant's home or work). The subsequent investigation of a network, like a broadcasting Wi-Fi router, may be necessary to determine what devices were connected at a location. While gathering evidence, an investigator should collect and review network connection logs (if logging is enabled) or records from an ISP. Knowing when and what devices were connected to a network can significantly assist in the identification of a suspect. Failing to gather these logs can result in their overwriting or deletion.

If a law enforcement investigator is adequately trained and utilizes online tools, like those outlined above, they should retain the available logs. These logs should become part of the investigator's digital case file. The logs should be maintained as a unique piece of digital evidence, as printing will result in the loss of file metadata (i.e., the creation and modification dates and times).

This metadata is critical to what is referred to as "user attribution."; putting a specific person behind the keyboard at the time of the offense. This will likely make or break the case for a prosecutor. These indicators of user attribution are often forgotten or overlooked by examiners who are providing evidence to the investigating officer or prosecutor.

These user attribution indicators are held in a variety of places on a computer and consist of jump lists, .lnk files (pronounced "Link"), Shellbags, Windows MRU, and search terms found within browsing histories.

Jump Lists

A "jump list" is a system-provided menu that appears when the user right-clicks a program in the taskbar or on the Start menu. It is used to provide quick access to recently or frequently used documents and offers direct links to app functionality.

Link Files

An LNK (short for LiNK) is a file extension for a shortcut file used by Microsoft Windows to point to an executable file. LNK file icons use a curled arrow to indicate they are shortcuts, and the file extension is typically hidden from the computer user. Generally, if the "linked" or source file is deleted, the LNK file will remain behind and will contain information not only of when the LNK file was created, but about the target file of interest.

Shellbags

Windows uses the "Shellbag" to store user preferences for folder display within Windows Explorer. Everything from visible columns to display mode (i.e., icons, details, or list) to sort order and are tracked.

Most Recently Used files (MRU)

The Most Recently Used "MRU" is a list that contains a history of recent activity on a computer. MRUs can include open documents or webpages.

If user attribution indicators are disregarded for any reason, the case weakens. The user attributes held within these specific items can show a pattern of behavior by a computer user. This makes it much more unlikely that this offense was an isolated incident and was occurring over an extended time period. Again, these crucial artifacts frequently go unexamined. These are in many cases, "make or break" items worth looking at when it comes to a defense strategy.

Defense of Child Pornography Cases

U.S. vs. Flyer

In *U.S. vs. Flyer*,[i] defense counsel made successful arguments regarding the lack of possession for images found in unallocated space. Unallocated space is not accessible by ordinary users. We have reviewed many cases where government examiners find child pornography in unallocated space

but do not identify additional forensic artifacts. An inability to exercise "dominion and control," no proof of "file use and knowledge," and lack of user attribution makes a case easier to defend as there is a lack of knowing possession and intent.

Thumbnails and Cache Files

Thumbnail images are an image that is a smaller representation of the original photograph. These thumbnail images by themselves usually are devoid of metadata and are created by the operating system without use interaction.

The Internet browser cache contains images saved by the browser to help speed up your rendering of web pages. By avoiding downloading the same image again and again the computer user experiences a faster web page viewing experience.

In both instances, the operating system or web browser application is automatically doing this as an automated process. The computer user has no knowledge of or access to these files.

ISP Connections

The way that the law enforcement agency determines where to go for a search warrant or "knock and talk" is to find out the subscriber account for an internet download.

When law enforcement performs a lookup of the IP address for a download, they will then research to determine which Internet Service Provider owns that IP address.

Once the owner of the IP address is determined, i.e. Spectrum or Charter Cable, the law enforcement officer will send a subpoena to the ISP and find out who the subscriber is for that IP address on the date and time of the download.

The subscriber account information will also provide a physical address for the internet connection.

Once the law enforcement officer has that information in hand, he or she will then apply for a warrant to search the residence or business at the address, This is based on the probable cause in the form of the download history from one of the tools used for the online investigation and the subscriber information from the ISP.

There are times when the connection is not being made from the address, i.e. someone is stealing a connection from a nearby address.

"The sound of his door being broken down awoken the man at 6:20 a.m. on March 7. Seven armed officers greeted the homeowner, whose name has not been released. He was forced to lie down on the floor while the officers pointed guns at him while calling him a pedophile and a pornographer. According to the Associated Press, the officers had the initials of I.C.E. on their jackets, which the man didn't know stood for Immigration and Customs Enforcement, and we don't blame him.

The agents searched the man's desktop for about two hours that morning looking for evidence, and eventually confiscated the computer, as well as his and his wife's iPads and iPhones. It took three days for investigators to realize the man, who had told the officers at the time of the intrusion that they had the wrong guy, was actually telling the truth and was indeed not the kiddie-porn downloader. A week later, investigators arrested a 25-year-old neighbor and charged him with distribution of child pornography. However, he did not get in trouble for piggybacking off the man's WiFi signal."

Source: https://www.geek.com/news/man-wrongly-accused-of-child-porn-learns-to-password-protect-wifi-the-hard-way-1347033/

Conclusion

Nearly every case in today's digital age has an electronic evidence component. These components can supply both supporting and damning information for your case. The question is: How do you obtain and interpret the evidence? A qualified and experienced expert can assist you with a thorough discovery review and comprehensive analysis of the electronic evidence.

[i] 633 F.3d 911 (9th Cir. 2011).

DIGITAL FORENSICS //

ENVISTA FORENSICS

Spoofs, Fakes, and Manipulation: The Challenge of Validating Messages and Social Media Content on Mobile Phones

Lars Daniel EnCE, CCPA, CCO, CTNS, CTA, CIPTS, CWA
Practice Leader - Digital Forensics at Envista Forensics
919-621-9335 / lars.daniel@envistaforensics.com

We would all like to believe that when we view a photo, the contents therein are a true and accurate representation of what they purport to be. Unfortunately, this is not always the case. We are all aware of software tools that allow for manipulating photos to create convincingly real fakes. Sometimes, these fakes are so convincing that veracity cannot be determined by examining the picture alone with the naked eye.

This has been true with photos for a long time and is true today with videos using deep fake technology. Software applications are widely available that allow a person to manipulate video or audio in order to make it appear that he or she is saying something that they never said. Like with the Reface App[i], where a person's face can be replaced with another's. It seems that the technology has advanced to the point where anyone can create a very convincing fake video of events and do so using an application on his or her phone. The individual need not have any special expertise in creating videos, all they need is the software.

Making fake photos and videos is relatively simple but making faked and spoofed social media and messaging content is even easier.

Additionally, a person can alter or fake text message communications, and someone can do it with a low level of technical sophistication and relative ease.

In mobile device forensics, the best method to collect the evidence from a phone is performed by utilizing cell phone forensics software and hardware. Before we cover the problems with verifying pictures and screenshots of social media content and text messages, it is pertinent to have a high-level overview of how data is collected.

The forensic acquisition process encompasses all the methods and procedures utilized to collect digital evidence. This collection process can take many forms with mobile phones and the data from mobile devices can reside in numerous locations. With mobile phones, the data extraction methods used are determined by multiple factors, including the cell phone's make, model, operating system version, and physical damage, to name a few.

How Mobile Phone Forensic Tools Verify Evidence

When a forensic acquisition is performed on a computer hard drive, a bit-for-bit duplicate of the data is created. In other words, all the data contained on the hard drive, including existing data, deleted data, and unallocated space, are collected in a forensic image file. This forensic image file is exactly like the data contained on the computer hard drive. However, a forensic acquisition of a mobile device is different, as it almost always has to be powered on.

The forensic data collection process from the mobile device is better called a "forensics extraction," as data is extracted from the device instead of a perfect bit-for-bit copy of the evidence item. With the mobile phone powered on, the forensic software cannot access some areas of data. However, that inaccessible data is usually of little to no value evidentiarily.

Following the forensic copying comes the hashing process. A mathematical algorithm is run against the copied data, producing a unique hash value. This hash value can be thought of as a digital fingerprint, uniquely identifying the copied evidence exactly as it exists at that point in time.

Preemptively raising the question, “Why bother hashing the forensic copy of a cell phone if it is not exactly the same as the original evidence like a computer?” Well, suppose you made a forensic copy of a phone today and hashed it, and sometime later an opposing attorney claimed you manipulated data. In that case, you could go back to the original forensic copy to prove you did not.

But what happens when the evidence is collected from a cell phone using screenshots or pictures? Since there is no mathematical algorithm or any other kind of forensic verification, how do we know that the messages or social media content are real?

Manual Examinations

To have confidence in the evidence gathered from mobile phones without forensic software and hardware begins with a correctly performed manual examination. A physical acquisition is the best option with mobile phone forensics, followed by a logical or filesystem acquisition. Manual examinations should be utilized as a last resort when other forensic acquisition methods are not possible. The risk of changing or deleting evidence on a mobile phone is significantly increased when performing a manual examination because it introduces a higher potential for human error.

A manual examination of a cell phone involves an examiner manipulating the mobile phone to the different areas of information, such as text messages or call history, and taking pictures of the screen with a camera. A correctly performed manual examination will reduce the risks of modifying the original evidence. Therefore, a manual examination is a viable option when acquiring cell phone evidence with correct procedures and thorough documentation.

The quality of a manual cell phone examination depends on the competency of the examiner. For example, suppose proper procedures and detailed documentation are not part of the manual examination. In that case, it can call into question whether or not the evidence was properly preserved and if tampering, intended or otherwise, occurred during the examination of the cell phone.

Pictures only tell part of the story. What happened during the time between the individual pictures being taken? Pictures alone do not provide any real verification that the phone evidence has not been altered. A video camera running continuously throughout the manual examination process, with no breaks, pauses, or edits, is the only method for evidence verification in the absence of a mathematical hash value. The video should begin before the phone is powered up. At the end of the examination, the phone should be powered down in view of the camera.

In my experience, it is uncommon for forensic examiners to properly follow best practices and protocols when it comes to manual examinations. A video recording rarely accompanies the photos of the mobile phone contents.

Why It Matters: Fakes Are Spoofs Are Real and On The Rise

Social Media Fakes

The pervasiveness of social media in our culture and the frequency at which users access these platforms to communicate, share, and consume content have broadened and deepen the amount of courtroom evidence. However, social media evidence has one particular vulnerability, the ability to be altered or forged.

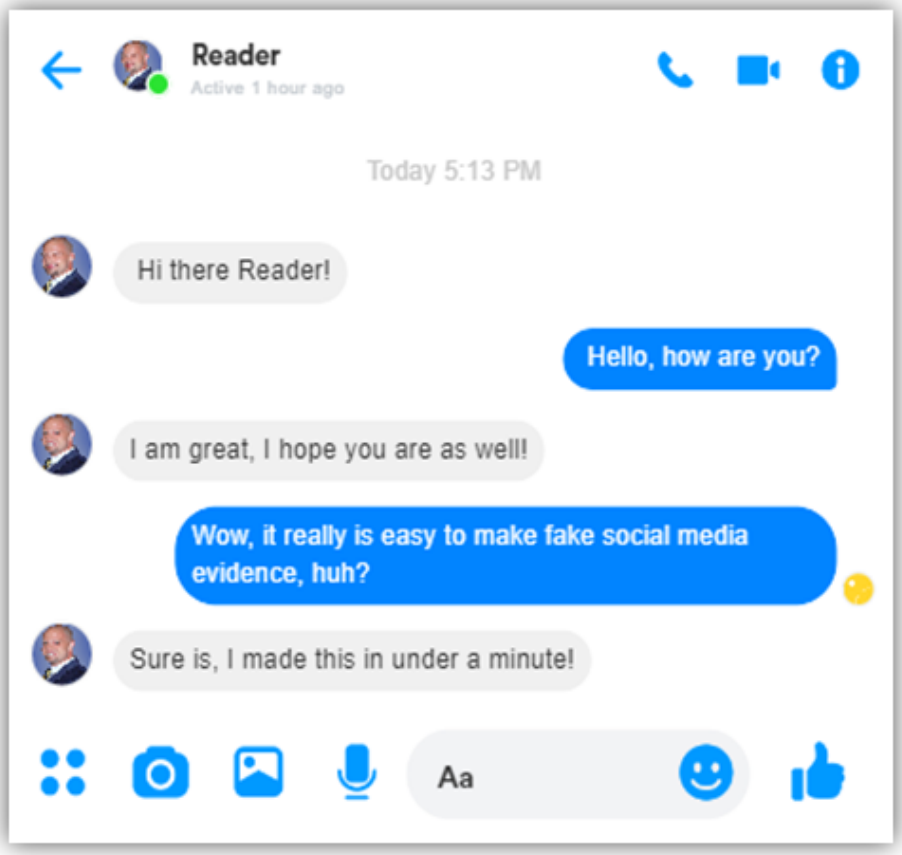
It does not take a high degree of technical capability or access to special software to create fake social media posts. Anyone can find websites that allow you to make fake social media posts and messages that look real, indistinguishable from authentic content.

For example, here are posts I made between myself and you, the reader, as a means of illustration. In addition, I can create fake posts and messages for all major social media platforms. The following faked social media messages and posts were created using a web-based application that is both simple to use and free.[ii]

Facebook

The time, date, location, content, comments, reactions, and chat messages contained in these photos are all fake.

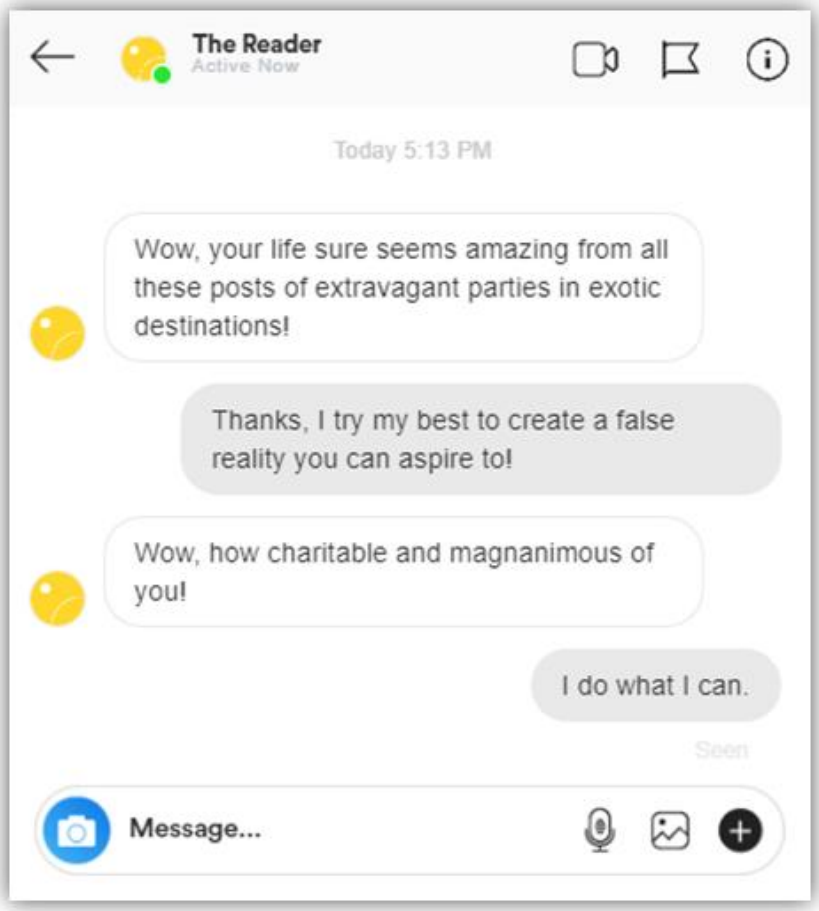

Lars Daniel is with You the Reader at My Backyard
Yesterday at 4:45am
Hello reader, here is a fake post I created just for you . I have even written a fake comment on your behalf!
I HATE COVID-19
26
21 Comments 10 Shares
Like
Comment
Share
View more 16 Comments
Reader Wow, where can I get that shirt!
10
Like · Reply · 1h
Write a comment...



Instagram

The account, blue check showing that I am a verified user, location, photo, content, comments, reactions, and chat communications are all fake.

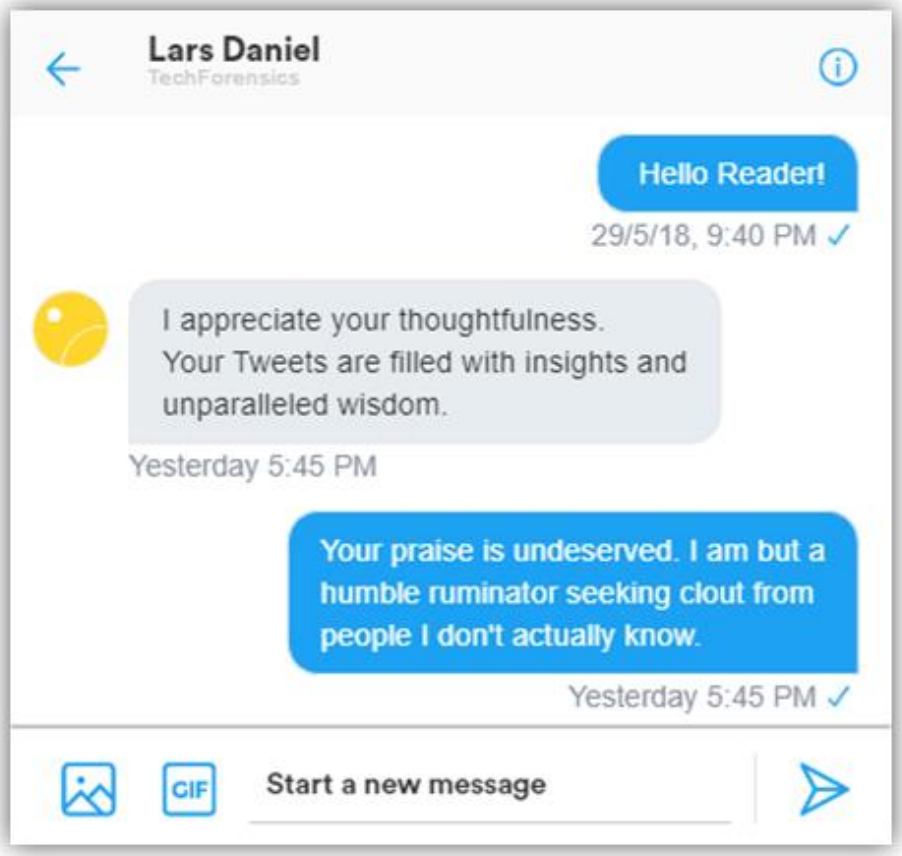

Lars Daniel · Follow
Chuckle Cheesers, Raleigh NC
Liked by The Reader and 120 others
Lars Daniel Fake post of my fake life on Instagram! ... more
View all 16 comments
Reader Wow, I wish I was as cool as you!
Add a comment...
6 August



Twitter

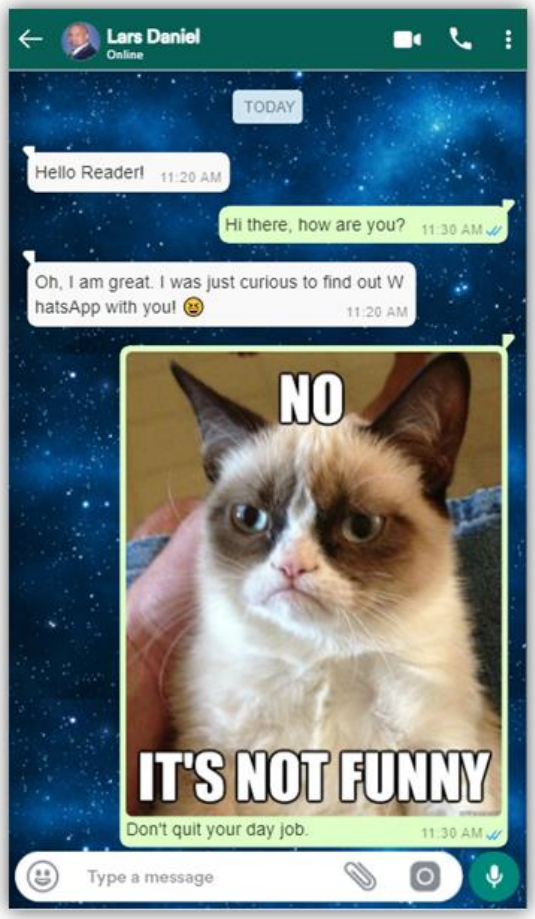
The account, tweets, time, retweets, likes, comments, and chats communications are fake.


Lars Daniel
TechForensics
Tweeting is the best. I prefer communicating in 280 characters or less. I find it encourages open, thoughtful dialogue.
4:17 PM. Aug 14, 2021 Twitter for iPhone
18k Retweets 160 Likes
The Reader @ReadingThisBook · 4h
Replying to @The Reader
I agree, Twitter's format in no way promotes logical fallacies and unnecessarily combative exchanges.



WhatsApp

The account, name, status, content, photo, and time are all fake.

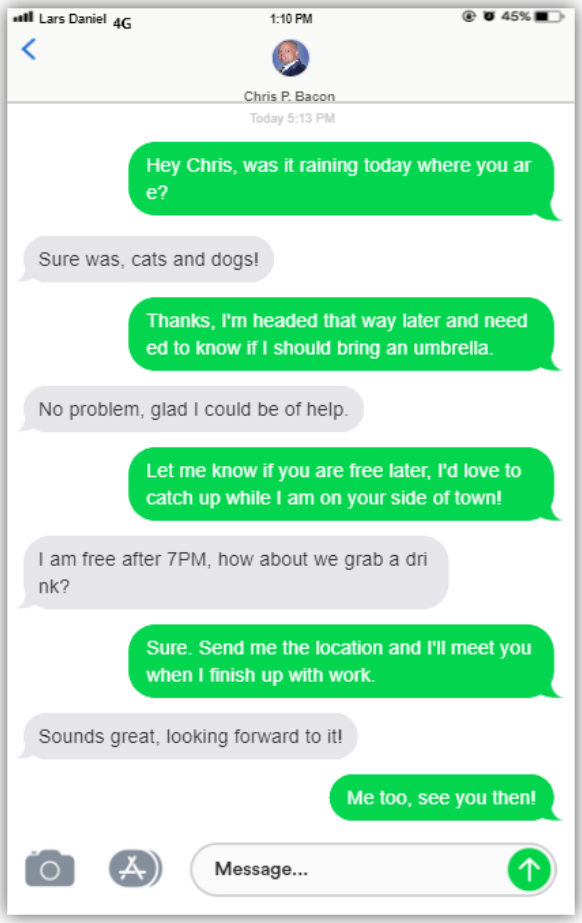


Snapchat

The image, text, time, name, account, and content are all fake

Texting

The account, contact, connection, name, content, time, icons, battery, and cellular service bars are all fake.

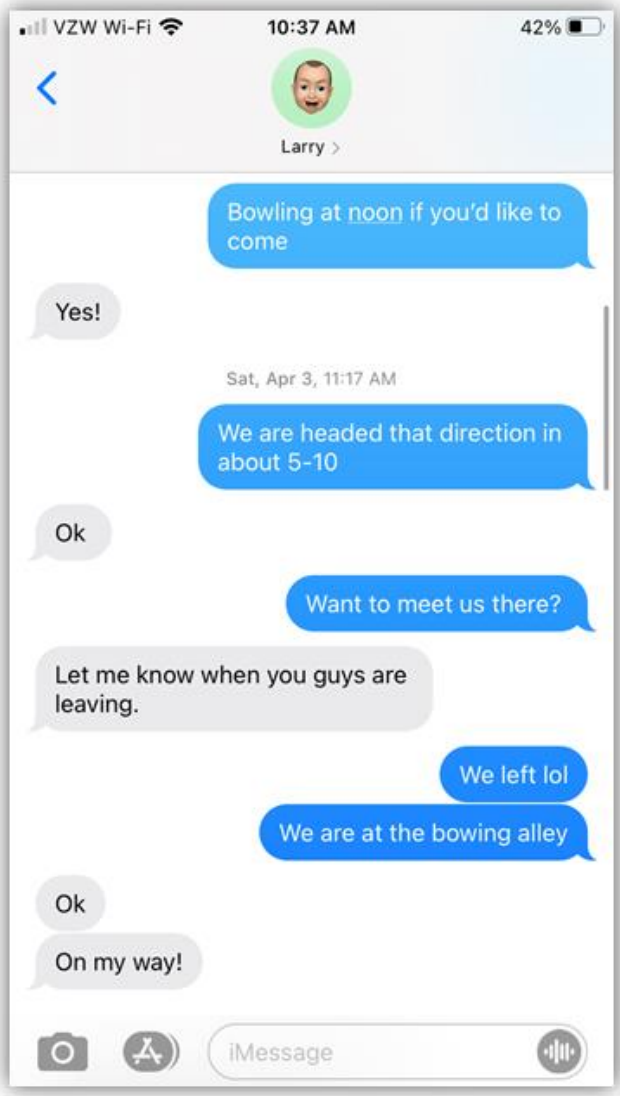


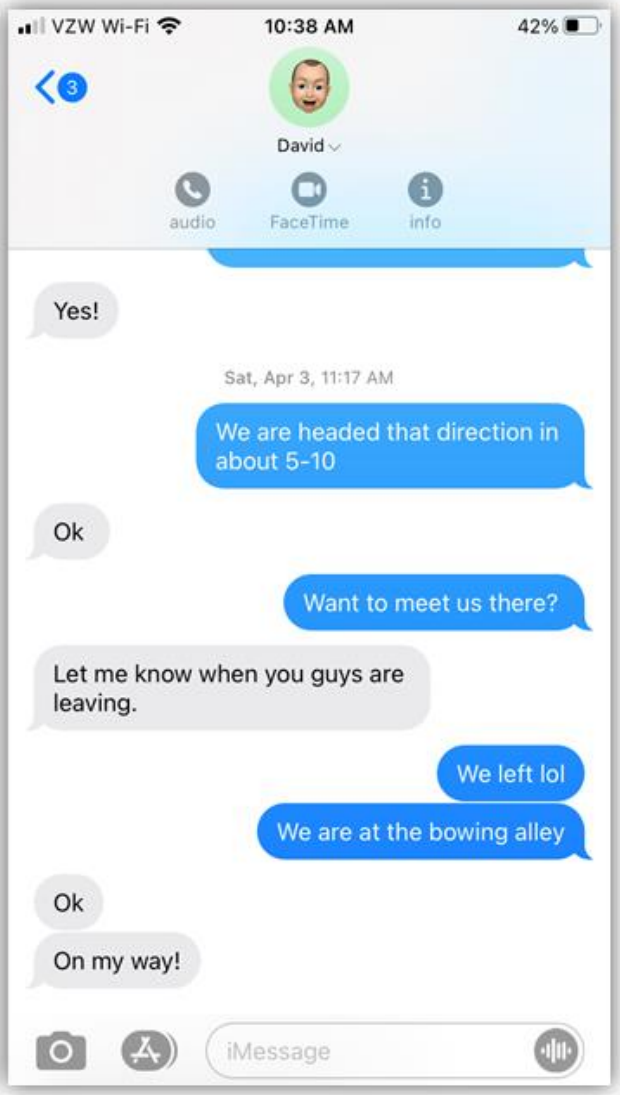
Spoofs and Fakes: Just the Phone

Creating fake messaging application communications on a cell phone doesn't require any outside tools, like the web-based application from the previous section. Instead, a user can make a fake with just the phone that they have in their hands that looks the same as a screenshot or photo provided as evidence.

Name Change

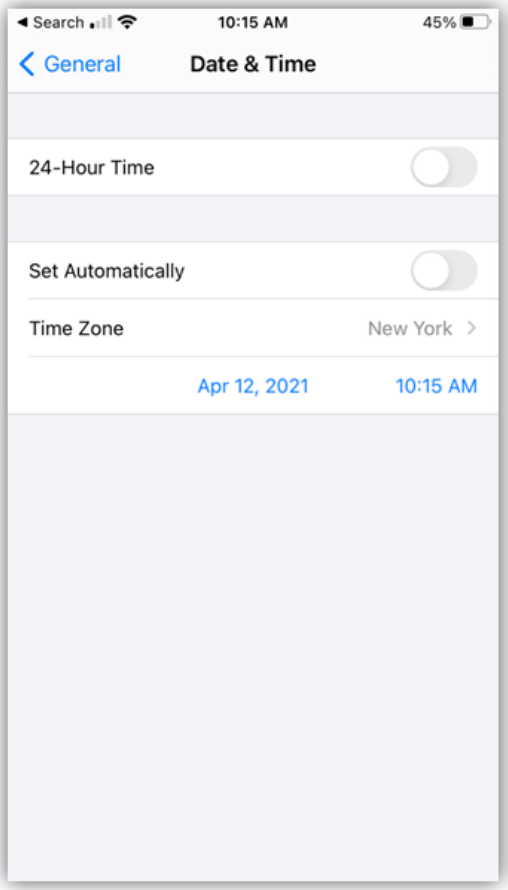
Screenshots of a text message conversation cannot verify the actual identity of a person alone. This is because the contact name can be changed at any time and the phone numbers of the sender or recipient are not recorded in the actual conversation itself in any way. For example, a person could change the contact on their phone named "Larry" to "David" by only editing the contact information, then take the pictures of the conversations to provide as evidence. All the messages sent between the person and Larry would appear to be between the person and David.

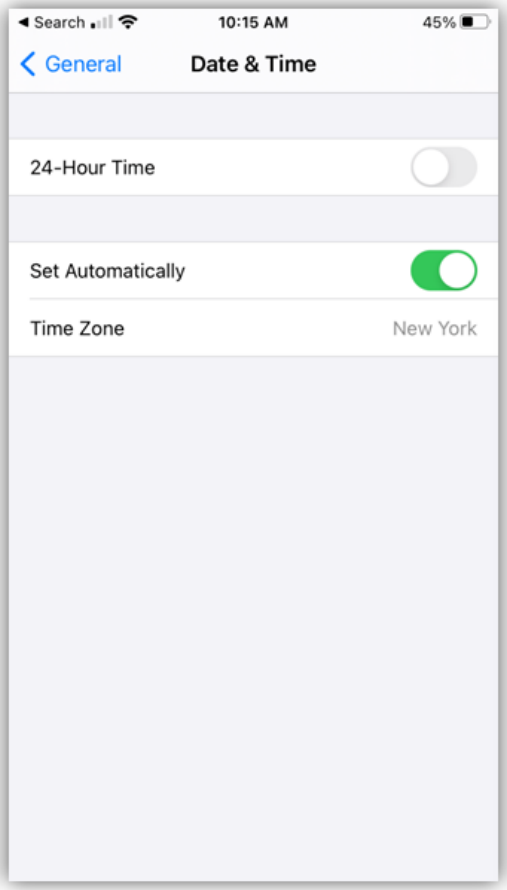

VZW Wi-Fi
10:37 AM
42%
Larry
Bowling at noon if you'd like to come
Yes!
Sat, Apr 3, 11:17 AM
We are headed that direction in about 5-10
Ok
Want to meet us there?
Let me know when you guys are leaving.
We left lol
We are at the bowing alley
Ok
On my way!
iMessage

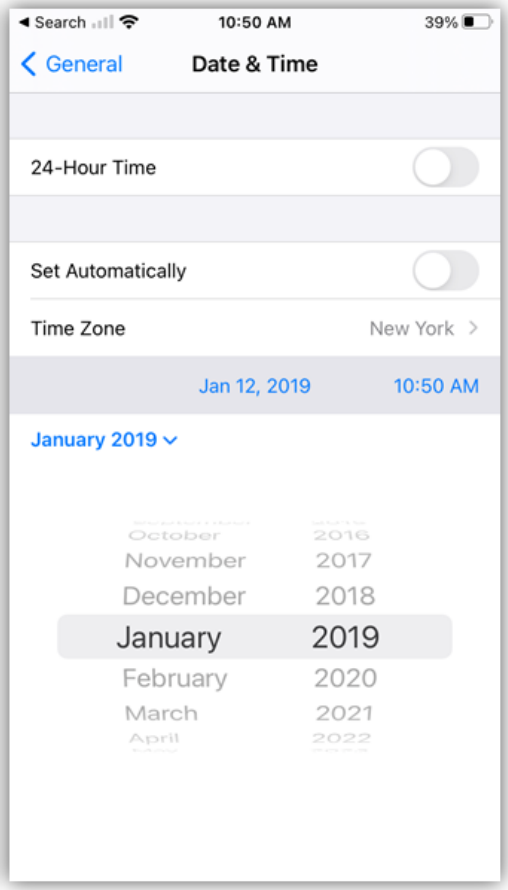

VZW Wi-Fi
10:38 AM
42%
3
David
audio
FaceTime
info
Yes!
Sat, Apr 3, 11:17 AM
We are headed that direction in about 5-10
Ok
Want to meet us there?
Let me know when you guys are leaving.
We left lol
We are at the bowing alley
Ok
On my way!
iMessage

Time Travel - Back Dating

It is possible to backdate an iPhone and to create text messages with fake dates and times. This can be done by going to the "Settings" application, selecting "General" from the menu, and then selecting "Date & Time." Next, from the "Date & Time" menu, turn off "Set Automatically." From there, click the menu option "Set Date & Time," and now the date and time can be set to anything. I can then send a text message that will show any date and time I select.



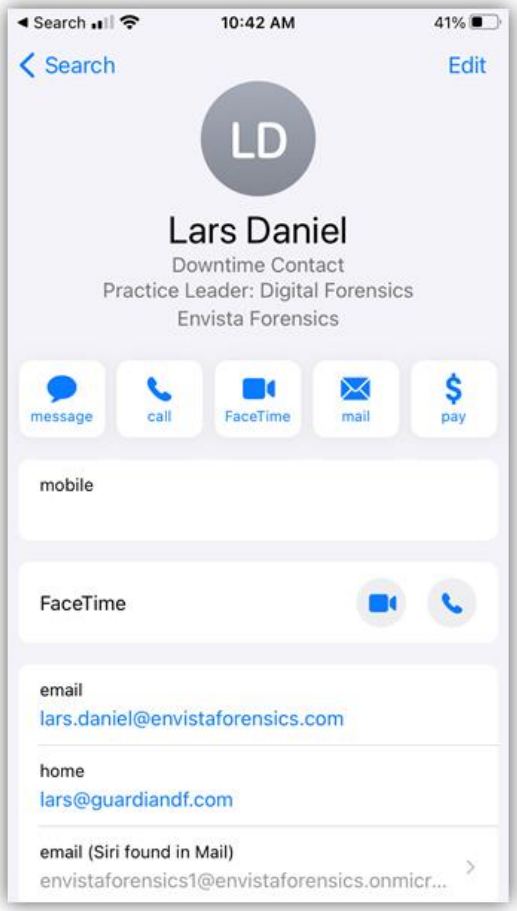


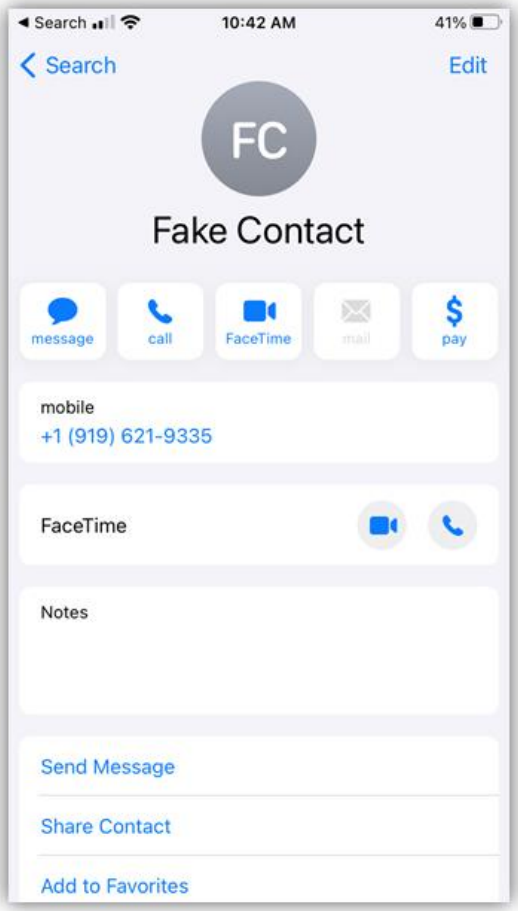


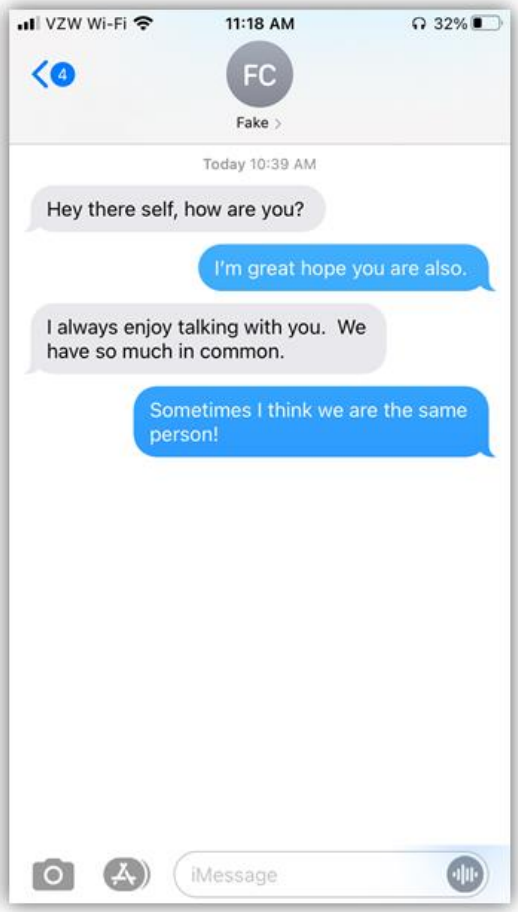
Talking to Myself - iMessage

Using only an iPhone, you can create a contact that uses your email address for iMessage communication. You then make a different contact on the phone that uses your cell phone number. While both the email and cell phone number are associated with you, you can have a conversation with yourself by naming them differently on the phone.

Couple this with the ability to backdate an iPhone, and it's possible to create months' or even years' worth of messages between two parties in an afternoon whom you can name anything you want and the screenshots would look exactly the same as a real message conversation.







When in Doubt Challenge the Evidence

When performing a manual examination, there are two critical components. One, the phone needs to be isolated from cellular and wireless networks. If you're looking at photos of text messages and see that there are Wi-Fi or cellular bars, you know that the phone was not isolated from the networks. Isolation of the device itself is achieved by eliminating all forms of data transmission, including the cellular network, Bluetooth, wireless networks (Wi-Fi), and infrared connections. By isolating the phone from all networks, the mobile phone is prevented from receiving any new data that would cause other data to be deleted, or worse, overwritten. The goal is to preserve the evidence as a snapshot in time of exactly how the evidence existed when it was received into custody.

Isolation

Did they Use a Faraday Bag?

A Faraday bag blocks any signals that a cell phone might pick up by blocking electrical fields and radio frequencies. A microwave uses this same technology, utilizing a Faraday cage to contain the magnetron's radio frequency within the cooking chamber. A cell phone can also be isolated from networks by wrapping the phone in a radio frequency shielding cloth and placing it into Airplane Mode.

Airplane Mode

After a digital forensic examiner has placed the phone into a Faraday bag or other device to ensure that the phone cannot receive any data, it is acceptable to put it into Airplane Mode. Once this is done, the phone can be removed for the duration of the examination. However, there is one caveat to this. The examiner must ensure that the phone is placed in Airplane Mode and that wireless functionality is turned off. You have likely experienced this in real life when flying. Even though you must turn off your cellular service while on an airplane, you can still access the Internet and transmit data using Wi-Fi; both wireless and cellular connectivity must be turned off for device isolation.

Video Verification

The other critical component, as previously discussed, is the continuous video footage of the examination of the cell phone, using photos of the contents, such as text messages or emails, for verification. Documentation from the National Institute of Standards and Technology (NIST) is an excellent resource for cross-examining experts or whoever documented messages via photo or screenshot.

In the following short example, we will utilize NIST documentation as exhibits to show the need for video verification. We will assume that no video was taken during the manual examination for the purpose of our example.

Cross-Examination Example: Video Verification

Q: Are you familiar with the National Institute of Standards and Technology (NIST)?

A: Yes

Q: Would you consider NIST to be a reliable source for information concerning cell phone forensics?

A: Yes

Q: Would you consider NIST to be an authority in the digital forensics community on how digital evidence should be handled?

A: Yes

INTRODUCE EXHIBIT: ***NIST Special Publication 800-101 Revision 1 Guidelines on Mobile Device Forensics***

Q: Please read the second to last paragraph on page 51.

A: "Invariably, not all relevant data viewable on a mobile device using the available menus may be acquired and decoded through a logical acquisition. Manually scrutinizing the contents via the device interface menus while video recording the process not only allows such items to be captured and reported but also confirms that the contents reported by the tool are consistent with observable data. Manual extraction must always be done with care, preserving the integrity of the device in case further, more elaborate acquisitions are necessary."

Q: What exactly is a manual examination of a cell phone?

A: A manual examination is where you take pictures of the contents from the phone, such as pictures of the text messages or emails.

Q: And that is what NIST is talking about in that paragraph, is that correct?

A: yes

Q: Did you video record your manual examination?

A: No

Q: Is there a reason you chose not to videotape the examination?

A: I didn't think I needed to since I was documenting the text messages with photos.

Q: Since the examination was not video recorded, can you prove if any of the text messages on the phone were deleted **UNINTENTIONALLY** during the manual examination?

A: No

Q: Since the examination was not video recorded, is there any way you can prove if any of the text messages on the phone were deleted **INTENTIONALLY** during the manual examination?

A: No

Q: Since the examination was not video recorded, is there any way you can prove if any of the text messages on the phone were modified **UNINTENTIONALLY** during the manual examination?

A: No

Q: Since the examination was not video recorded, is there any way you can prove if the text messages on the phone were modified **INTENTIONALLY** during the manual examination?

A: No

Q: Since the examination was not video recorded, is there any way you can prove if the text messages on the phone were created **UNINTENTIONALLY** during the manual examination?

A: No

Q: Since the examination was not video recorded, is there any way you can prove if the text messages on the phone were created **INTENTIONALLY** during the manual examination?

A: No

Q: If you had video recorded your examination, you could provide proof that there was no intentional or unintentional manipulation of the cell phone. Is that correct?

A: Yes

Conclusion

It is not hard to imagine this line of questioning expanded and enhanced by an attorney being a long and arduous experience for the witness. All because they skipped a simple step of video recording the process of their examination. Having testified as an expert witness on evidence verification and the authenticity of photos or screenshots of text messages, I can tell you that this is a common scenario.

Often basic forensic procedures are not followed in manual examinations. Mobile phones are not isolated from networks, exposing them to data manipulation and deletion. Manual examinations are not recorded, leaving the trier of fact with only the word of the examiner instead of verifiable proof in the form of a video recording. We all walk around with a video camera in our pocket. Beyond extreme circumstances, there is no excuse for an improperly performed manual examination, and if your encounter one in your case, it can be challenged from a forensic perspective.

---

[i] Reface. Face swap videos

[ii] Zeoob | Generate Instagram, TikTok, Snapchat, Twitter, Facebook Chats & Posts with comments to offer your students some variety in dealing with storytelling.

DIGITAL FORENSICS //

ENVISTA FORENSICS

Resource Packet for Legal Professionals

Lars Daniel, EnCE, CCPA, CCO, CTNS, CTA, CIPTS, CWA

Practice Leader – Digital Forensics at Envista Forensics

M: 919-621-9335 // lars.daniel@envistaforensics.com

This document is ever-changing. Our team is consistently adding and updating information. You can contact me to check for the most up-to-date version. ***Disclaimer: None of our experts are attorneys, and we do not offer legal advice. Nothing in this resource guide should be viewed as providing legal advice or instruction.***

Call Detail Record Subpoena Language

If you do not see the carrier you are looking for, particularly Tracfone or other prepaid (Mobile Virtual Network Operators (MVNO) companies, or have any questions regarding call detail records, please contact us.

- Other important steps prior to sending legal process:
- If your matter is civil litigation, please contact our experts for assistance as the service process may vary from these samples.
- Contact the carrier to ensure they are the correct carrier to request data.
- Send preservation letters to hold all available records, this can be done for 90 days at a time.
- Refer to search.org for the most current contact numbers and delivery methods for legal process. https://www.search.org/resources/isp-list/

AT&T Wireless

AT&T Wireless

11760 US Highway 1 Suite 600 North Palm Beach, FL 33408

Contact Phone Number: 800-635-6840

SERVICE BY FAX OR EMAIL: 888-938-4715 or gldc@att.com

Language:

Defendant, by and through their attorney, requests the following information be provided regarding cell phone communications in the form of historical call detail records with cell site locations tower location listings, for cell phone number(s) 000-000-0000 for the period of time between 00-00-2000 and 00-00-2000.

All information including but not limited to:

1. Subscriber information for the above listed numbers, including financially responsible party, billing address, features and services and equipment,

2. Call Detail Records with cell site location, all call originations, call terminations, call attempts, voice and text message transactions, including push to talk, data communications, SMS and MMS communications, and voice communications, LTE and/or IP sessions and destinations with cell site information, including the originating and receiving phone numbers or network IDs for all incoming and outgoing call transactions, data transactions and push to talk sessions.

3. Records are to include the IMEI, IMSI or other equipment or handset identification information for the target phone number if known.

4. All stored SMS content, MMS content and / or Browser Cache if available.

5. Beginning and ending switch and cell site / tower identifiers for each call, SMS MMS and data transmission, including the location information and azimuth for the tower and sector used for the call.

6. A legend and definition for any and all abbreviations used in the reports provided

7. An explanation of how to read the call detail records.

8. Any precise measurement data such as e-911 location data, NELOS data and or any other data recorded for the time period that will provide additional location data.

9. Specific information regarding the time stamps / time zones of the records.

Provide the following information regarding cell tower locations for the following areas containing cell towers actively in service between 00-00-2000 and 00-00-2000.

Include the below AT&T cell tower information:

Mobile Country Code (MCC), Mobile Network Code (MNC), Location Area Code (LAC), System Identification Number (SID), Network Identity (NID), Tracking Area Code (TAC), Cell ID, E-UTRAN Cell Global Identifier (ECGI), eNodeB ID (eNBID), Technology, Band, Frequency, Channel, EARFCN, Sector Identifier, Sector Orientation (azimuth), Beamwidth, PCI, PSC, PN Offset, and Tower Height.

10. Any records or information regarding cell towers that were undergoing maintenance, or were out of service the time period in this request.

All responsive data is to be provided in both Adobe PDF format and Microsoft Excel format, .TXT or .CSV format.

Please indicate in your response to this subpoena if there is any data loss due to the time difference between the date of the receipt of this subpoena and the time period requested, and if so, a detailed description of what data is not recoverable versus what data would be recoverable based on the carrier's retention period for call detail records.

Please respond to this subpoena via email to: your email & Expert with Envista Forensics

Verizon Wireless

180 Washington Valley Road Bedminster, NJ 07921

Contact Phone Numbers: Subpoena contact: 888-483-2600

SERVICE BY FAX :Subpoenas: 888-667-0028

Orders & Warrants: 888-667-0026

Language:

Defendant, by and through their attorney, requests the following information be provided regarding cell phone communications in the form of historical call detail records with cell site locations tower location listings, for cell phone number(s) 000-000-0me between 00-00-2000 and 00-00-2000.

All information including but not limited to:

1. Subscriber information for the above listed numbers, including financially responsible party, billing address, features and services and equipment,

2. Call Detail Records with cell site location, all call originations, call terminations, call attempts, voice and text message transactions, including push to talk, data communications, SMS and MMS communications, and voice communications, LTE and/or IP sessions and destinations with cell site information, including the originating and receiving phone numbers or network IDs for all incoming and outgoing call transactions, data transactions, VOLTE with cell sites.

3. Records are to include the IMEI, IMSI or other equipment or handset identification information for the target phone number if known.

4. All stored SMS content, MMS content and / or Browser Cache if available.

5. Beginning and ending switch and cell site / tower identifiers for each call, SMS MMS and data transmission, including the location information and azimuth for the tower and sector used for the call.

6. A complete table of cell towers / cell site information for all cell towers / cell sites in the

Mobile Country Code (MCC), Mobile Network Code (MNC), Location Area Code (LAC), System Identification Number (SID), Network Identity (NID), Tracking Area Code (TAC), Cell ID, E-UTRAN Cell Global Identifier (ECGI), eNodeB ID (eNBID), Technology, Band, Frequency, Channel, EARFCN, Sector Identifier, Sector Orientation (azimuth), Beamwidth, PCI, PSC, PN Offset, and Tower Height.

8. An explanation of how to read the call detail records.

9. Any precise measurement data such as e-911 location data, RTT, RTTL, RTTM, ERLTE, ALULTE or reports of similar nature data that provide estimated locations of the device or distances from the base station. Any other data recorded for the time period that will provide additional location data.

10. Specific information regarding the time stamps / time zones of the records.

11. Any records or information regarding cell towers that were undergoing maintenance, or were out of service the time period in this request.

All responsive data is to be provided in both Adobe PDF format and Microsoft Excel format, .TXT or .CSV format.

Please indicate in your response to this subpoena if there is any data loss due to the time difference between the date of the receipt of this subpoena and the time period requested, and if so, a detailed description of what data is not recoverable versus what data would be recoverable based on the carrier's retention period for call detail records.

Please respond to this subpoena via email to: your email & Expert with Envista Forensics

T-Mobile/Metro PCS

4 Sylvan Way

Parsippany, New Jersey 07054

Contact: 866-537-0911

SERVICE BY E-MAIL AND FAX: Lerinbound@T-Mobile.com, 973-292-8697

Language:

Defendant, by and through their attorney, requests the following information be provided regarding cell phone communications in the form of historical call detail records with cell site locations tower location listings, for cell phone number(s) 000-000-0me between 00-00-2000 and 00-00-2000.

All information including but not limited to:

1. Subscriber information for the above listed numbers, including financially responsible party, billing address, features and services and equipment,

2. Call Detail Records with cell site location, all call originations, call terminations, call attempts, voice and text message transactions, including push to talk, data communications, SMS and MMS communications, and voice communications, LTE and/or IP sessions and destinations with cell site information, including the originating and receiving phone numbers or network IDs for all incoming and outgoing call transactions, data transactions and push to talk sessions.

3. Records are to include the IMEI, IMSI or other equipment or handset identification information for the target phone number if known.

4. All stored SMS content, MMS content and / or Browser Cache if available.

5. Beginning and ending switch and cell site / tower identifiers for each call, SMS MMS and data transmission, including the location information and azimuth for the tower and sector used for the call.

6. Cell Site List including; Mobile Country Code (MCC), Mobile Network Code (MNC), Location Area Code (LAC), System Identification Number (SID), Network Identity (NID), Tracking Area Code (TAC), Cell ID, E-UTRAN Cell Global Identifier (ECGI), eNodeB ID (eNBID), Technology, Band, Frequency, Channel, EARFCN, Sector Identifier, Sector Orientation (azimuth), Beam width, PCI, PSC, PN Offset, and Tower Height.

7. A legend and definition for any and all abbreviations used in the reports provided

8. An explanation of how to read the call detail records.

9. Any precise measurement data such as e-911 location data, TDOA (Time Delay of Arrival) Truecall, Timing Advance or reports of similar nature data and or any other data recorded for the time period that will provide additional location data.

10. Specific information regarding the time stamps / time zones of the records.

All responsive data is to be provided in both Adobe PDF format and Microsoft Excel format, .TXT or .CSV format.

Please indicate in your response to this subpoena if there is any data loss due to the time difference between the date of the receipt of this subpoena and the time period requested, and if so, a detailed description of what data is not recoverable versus what data would be recoverable based on the carrier's retention period for call detail records.

Please respond to this subpoena via email to: your email & Expert with Envista Forensics

Sprint Corporation

6480 Sprint Pkwy

Overland Park, Kansas 66251 Contact: 800-877-7330

SERVICE BY FAX: 816-600-3111; To receive status updates for Subpoenas and Search Warrants by contacting 800-877-7330 extension 3.

Language:

Defendant, by and through their attorney, requests the following information be provided regarding cell phone communications in the form of historical call detail records with cell site locations tower location listings, for cell phone number(s) 000-000-0me between 00-00-2000 and 00-00-2000.

All information including but not limited to:

1. Subscriber information for the above listed numbers, including financially responsible party, billing address, features and services and equipment,

2. Call Detail Records with cell site location, all call originations, call terminations, call attempts, voice and text message transactions, including push to talk, data communications, SMS and MMS communications, and voice communications, LTE and/or IP sessions and destinations, eHRPD with cell site information, including the originating and receiving phone numbers or network IDs for all incoming and outgoing call transactions, data transactions and push to talk sessions.

3. Records are to include the IMEI, IMSI or other equipment or handset identification information for the target phone number if known.

4. All stored SMS content, MMS content and / or Browser Cache if available.

5. Beginning and ending switch and cell site / tower identifiers for each call, SMS MMS and data transmission, including the location information and azimuth for the tower and sector used for the call.

6. A complete table of cell towers / cell site information for all cell towers / cell sites;

a. Cell Site List including; Mobile Country Code (MCC), Mobile Network Code (MNC), Location Area Code (LAC), System Identification Number (SID), Network Identity (NID), Tracking Area Code (TAC), Cell ID, E-UTRAN Cell Global Identifier (ECGI), eNodeB ID (eNBID), Technology, Band, Frequency, Channel,

EARFCN, Sector Identifier, Sector Orientation (azimuth), Beamwidth, PCI, PSC, PN Offset, and Tower Height.

7. a legend and definition for any and all abbreviations used in the reports provided

8. An explanation of how to read the call detail records.

9. Any precise measurement data such as e-911 location data, Per Call Measurement Data (PCMD) or reports of similar nature data that provide estimated locations of the device or distances from the base station. Please provide a PCMD report for each Vendor/Call type. Any other data recorded for the time period that will provide additional location data.

10. Include reports for VOVoice (VOWIFI, VOLTE, VOCDMA)

11. Specific information regarding the time stamps / time zones of the records.

12. Any records or information regarding cell towers that were undergoing maintenance, or were out of service the time period in this request.

All responsive data is to be provided in both Adobe PDF format and Microsoft Excel format, .TXT or .CSV format.

Please indicate in your response to this subpoena if there is any data loss due to the time difference between the date of the receipt of this subpoena and the time period requested, and if so, a detailed description of what data is not recoverable versus what data would be recoverable based on the carrier's retention period for call detail records.

Please respond to this subpoena via email to: your email & Expert with Envista Forensics

Cell Site List Request

This request should be used for all carriers, and is important to complete an analysis or cell site survey.

Look up each carrier and their subpoena compliance info using, https://www.search.org/resources/isp-list/

Language:

Please include a list of the following information regarding Cell Sites for the State of Insert State, during Insert Month, Year.

To include (but not limited to):

Mobile Country Code (MCC), Mobile Network Code (MNC), Location Area Code (LAC), System Identification Number (SID), Network Identity (NID), Tracking Area Code (TAC), Cell ID, E-UTRAN Cell Global Identifier (ECGI), eNodeB ID (eNBID), Technology, Band, Frequency, Channel, EARFCN, Sector Identifier, Sector Orientation (azimuth), Beamwidth, PCI, PSC, PN Offset, and Tower Height.

Please provide the list in excel, .csv or similar format.

Please respond to this subpoena via email to: your email & Expert with Envista Forensics

Mobile Virtual Network Operator (MVNO) Subscriber/Billing request

This request can be used for all MVNO, and supplements the call detail record request to the company providing cell service. Look up each carrier and their subpoena compliance info using, https://www.search.org/resources/isp-list/

A separate request needs to be made to the company providing service (ie. Verizon, AT&T)

Language:

Defendant, by and through their attorney, requests the following information be provided regarding cell phone communications in the form of historical call detail records with cell site locations tower location listings, for cell phone number(s) 000-000-0me between 00-00-2000 and 00-00-2000.

1. Subscriber information for the above listed numbers, including financially responsible party, billing address, features and services and equipment.
2. All call originations, call terminations, call attempts, voice and text message transactions, including push to talk, data communications, SMS and MMS communications, and voice communications, LTE and/or IP sessions and destinations.
3. Records are to include the IMEI, IMSI or other equipment or handset identification information for the target phone number if known.
4. A legend and definition for any and all abbreviations used in the reports provided.
5. An explanation of how to read the call detail records.

All responsive data is to be provided in both Adobe PDF format and Microsoft Excel format, .TXT or .CSV format.

Please indicate in your response to this subpoena if there is any data loss due to the time difference between the date of the receipt of this subpoena and the time period requested, and if so, a detailed description of what data is not recoverable versus what data would be recoverable based on the carrier's retention period for call detail records.

Please respond to this subpoena via email to: your email & Expert with Envista Forensics

Call Detail Records – What You Should Get in Discovery from Opposing Counsel

Subpoena responses and warrant returns from wireless phone companies will contain specific files that are delivered via email, on disk or via a secure web portal. It is very important that you received all of the files returned to the requester. Also, copies of the original subpoena and or warrant with the affidavit are very helpful for your expert.

There are spreadsheets and documents that provide such information as subscriber information; the call detail records themselves, cell tower location keys, explanation forms and disclaimers. These disclaimers are important, as they provide pertinent information regarding location accuracy or time-zone information. Each carrier stores their records in various formats and below you will find the specific data you should receive organized by four of the major carriers. Other carriers like US Cellular follow a similar pattern.

Verizon Wireless

Verizon Wireless call detail records also require a cell tower key to determine the location of the towers in the area. Call detail records will often be labeled "Cell sites incoming outgoing" and the tower key with contain a city name and "LEA". Verizon records may also contain Voice Over LTE records which will contain "VOLTE" in the spreadsheet name. If requested in the proper timeframe, you may receive Real Time Tool records, the spreadsheet name will contain "RTTM". Verizon also provides subscriber information, explanation information for each of the different spreadsheets as well as disclaimers. Each of the spreadsheets containing location information will be in Microsoft Excel format and explanation forms are typically in Portable Document Format (.pdf).

Sprint

Sprint also provides call detail records and cell site keys in separate spreadsheets. Again, both are needed to analyze the records. Sprint's records also come in Microsoft Excel format and are typically labeled with a number. There will be several spreadsheets all containing the various information. They may also provide Per Call Measurement Data (PCMD) if requested in the proper timeframe. Sprint also provides need explanation forms and disclaimers.

AT&T/Cricket

provides their call detail records and text detail, with location information, in one spreadsheet. This is typically labeled "Reports AU" and comes in two formats, Text format (.txt) and Portable Document Format (.pdf). This is standard for all requests, unless otherwise specified. At&t will provide subscriber information, as well as needed explanation forms and disclaimers. At&t may also provide, if requested, Network Event Location Service (NELOS) data. It is important for your expert to receive the text format (.txt) files for analysis, this format allows for data to be imported into various software platforms for converting time zones and analysis.

T-Mobile / MetroPCS

T-Mobile / MetroPCS provides call detail records in Microsoft Excel spreadsheets that are typically labeled "CDR Mediations". This spreadsheet will provide the call record as well as the tower location information needed. Subscriber information will be provided and explanation forms will also be provided. Depending on the year the records were provided, they may be kept in different time-zones, for this reason the explanation form is important. No other location information is available from T-Mobile at this time.

Google Location History Subpoena Language

Request the following for accounts: googleuser@gmail.com

INFORMATION SOUGHT: Google location services to include: account information, date, time (UTC), latitude, longitude, maps display radius (accuracy in meters), device source, device tag, and platform.

FOR THE DATE RANGE: December 5, 2015

SEND TO:

Google, Inc.

Contact Name:	Google Legal Investigations Support
Online Service Address:	1600 Amphitheatre Parkway Mountain View, CA 94043
Phone Number:	(844)383-8524
E-mail Address:	uslawenforcement@google.com
Note(s):	For a faster response time, submit your legal requests through the Law Enforcement Request System (LERS). The system requires each user to register for a unique account to submit legal requests. Register for an account at https://support.google.com/legal-investigations/contact/LERS From Googles LERS FAQ: https://lers.google.com/u/2/app/faq "Notwithstanding Title 18, United States Code, Section 2252A [or similar statute or code] Google shall disclose responsive data, if any, by delivering encrypted files through Google's Law Enforcement Request System" Oct 2016: telephone number listed for google and the message said the number has changed. The message said the new number is (844)383-8524 or (650)417-9011

Questions can be emailed to USLawEnforcement@google.com

For Emergency Disclosure Requests leave a message with details of the emergency and your contact information at 650-253-3425. Google will only return calls from sworn law enforcement officers handling emergency situations.

Google has launched a new Law Enforcement System. Here is the link to sign up in advance for an account: https://support.google.com/legal-investigations/contact/LERS

Last Updated: July 2017

Previous Information: As of Feb, 2016: Voice # :650-253-3425 In February 2015, Notes was: For a faster response time, Google has created a web form for submitting legal demands. Use of fax and email are still options for delivering, but the web form is preferred by Google: Google Legal Portal: https://support.google.com/legal-investigations. For Custodian of Records and Legal Investigations Support call the "Emergency Disclosure Request" department at: 650-253-3425. Leave a message and an agent will call you back. For search warrant requests, please send them to: Email: USLawEnforcement@google.com (preferred by Google) or by Fax: 650-249-3429. Attention: Custodian of Records Google, Inc. 1600 Amphitheatre Parkway Mountain View, CA 94043 At Google's request, please include the following language in any subpeona: "Please do not disclose/notify the user of the issuance of this subpoena. Disclosure to the user could impede an investigation or obstruct justice." Additionally, please include the following in your search warrant "Google shall disclose responsive data, if any, by sending to [LE's postal address] using the US Postal Service or another courier service, notwithstanding 18 U.S.C. 2252A or similar statute or code." Google will disclose release of information unless in violation of law or court order or if convinced doing so will place a child at risk. A short affidavit arguing the last will be considered. Google does not disclose preservation of data actions to account holders. For Gmail: Custodian of Records and Legal Investigations Support can be reached at: 650-253-3425. For search warrant requests, please submit them to:
Email: USLawEnforcement@google.com(preferred by Google) or by Fax: 650-249-3429. Attention: Custodian of Records Google, Inc. 1600 Amphitheatre Parkway Mountain View, CA 94043 At Google's request, please include the following language in any subpoena: "Please do not disclose/notify the user of the issuance of this subpoena. Disclosure to the user could impede an investigation or obstruct justice."

Video Recording System (DVR) Subpoena Language

1) Any and all records related to the recording device , specifically for the period of time beginning on _____ and ending upon _____ used in the recording of the interviews of persons _____ and _____

2) All information related to the recording device including but not limited to:

    a. user manuals
    b. service records
    c. training materials
    d. installation manuals
    e. manufacturer, make, model, and serial number
    f. date the recording device went into service
    g. known issues or problems with the recording device
    h. firmware version
    i. software version

3) Any and all maintenance records for the recording device.

4) Any and all information concerning the recording device hardware in regards to the installation and operation. This information is to include, but is not limited to how it is installed in the facility, and any possible errors in the installation that could have an effect on the operation of the recording device.

5) Any and all information concerning the software and firmware of the recording device. This information is to include, but is not limited to how the software and firmware are installed on the recording device, how any upgrades to the software and firmware have been performed,

and any possible errors in the installation of the software or firmware that could have an effect on the operation of the recording device.

6) The qualifications, resume, curriculum vitae, and any records related to the training of the person who created and/or exported the video and audio recordings from the recording device for the persons _____ and _____.

7) Any protocols, operation manuals, guidelines, standard operating procedures, and any and all documents created by the (LAW ENFORCEMENT AGENCY/PRIVATE COMPANY) concerning the particular recording device, audio forensics, video forensics, chain of custody in relation to video and audio, and the preservation methods of video and audio.

8) Any and all documentation, reports, narratives, or other documents concerning the method by which the video recordings were extracted from the device to include, but not limited to, the quality settings, file type, and compression ratio.

9) Any and all documentation, reports, narratives, or other documents concerning the settings of recording device between the dates of _____ and _____ including, but not limited to, the quality settings, number of cameras, multiplexing, file type, import settings, export settings, compression ratio, encryption, and audio settings.

GPS (Global Positioning System) Records Subpoena Language

1) Any and all records related to the GPS records identified by serial numbers _____ specifically for the period of time beginning on _____ and ending upon _____.

2) All Information related to GPS units identified by serial numbers _____ and _____, to include but not limited to GPS activity such as powering up, powering down, distance traveled, mileage, latitude and longitude, location by address, speed of travel, distance traveled, long stop, short stop, dilution of precision ratings, and so forth.

3) Any information that is available regarding the physical GPS units installed in the vehicle(s) identified by GPS Unit serial number(s) _____. This is to include, but is not limited to; user manuals, installation manuals, owner manuals, manufacturer, make, model, dates units went into service, dates unites went out of service, known issues or problems with GPS models such as loss of signal, problems with calibration, pinging, areas of service, problems due to extraneous factors such as weather and so forth.

4) Any information that is available regarding the software used by both Vehiclepath.com and their clients. This is to include, but is not limited to; user manuals, installation manuals, owner manuals, online documentation, known problems with the software either used by Vehiclepath.com or their clients, user errors that could have an effect upon GPS records, and so forth.

5) Any and all maintenance records for the GPS units identified by serial number(s) _____.

6) A list of all GPS units supported by COMPANY NAME'S tracking system up to MONTH of 20XX.

7) Any and all information on the GPS units regarding their installation and operation. This information is to include, but is not limited to how and where they are installed in vehicles, possible errors in installation that could have an effect on GPS records, how the tracking ability of GPS units could be manipulated by being turned on and off by the user, otherwise disabling of the GPS unit, the use of software or hardware that could modify the unit, other ways of intentionally causing a GPS unit to function in any way other than intended.

Digital Evidence Generic ESI Request

With regard to any electronic data that you expect to use as evidence in this case, please produce the following:

1. a duplicate of any forensic copies made by the expert of any computer hard drive, digital storage media including but not limited to CD-ROMS, USB flash drives, floppy disks, memory cards, digital camera storage, smart cards and portable hard drives.

2. a complete inventory of all items supplied to the expert that may contain any type of digital data, whether or not such items were examined or copied by the expert.

3. a complete copy of all forensics reports, chain of custody records, and lab notes generated by the expert pertaining to the acquisition, preservation, analysis, and or reporting by said expert.

4. any documents produced from the electronic sources examined by the expert in this case, both in printed and electronic formats, including, but not limited to:
    a. log files;
    b. any or all printer artifacts;
    c. user access histories;
    d. user account information including all known access times to the server by any of the persons named in this lawsuit;
    e. user account information including security levels and access control lists;
    f. user account information including user names, account type and passwords;

With regard to any person whom you expect to call as an expert witness at the trial of this case, please produce the following:

1) All materials and documents of any kind in the possession, custody, or control of the expert witness that pertain to the subject matter of this case, including, but not limited to, all correspondence between you and the expert witness, all correspondence between your attorney and the expert witness, all e-mail communications between you and the expert witness, all e-mail communications

between your attorney and the expert witness, all notes that pertain to the subject matter of this case, all diaries or personal journals that pertain in any manner to the subject matter of this case, and all records, depositions, statements, transcripts, reports, writings, drawings, graphs, calculations, estimates, exhibits, charts, photographs, audio tapes, video tapes, plans, invoices, bills, and receipts from any source that relate in any manner to this litigation;

2) All documents prepared by the expert that pertain to this case, including, but not limited to, true, correct, and complete copies of all reports concerning this case that have been prepared by the expert. This request for production specifically includes all preliminary drafts of reports as well as final drafts of reports;
    a) All documents that you or your attorney or any of your representatives have sent to the expert witness that pertain in any manner to this case;
    b) All documents, data, or other information used, considered, or reviewed by the expert witness that pertain in any manner to this case;
    c) All documents that pertain to any compensation agreement for the expert's services in this case;
    d) All documents that have been or will be shown to the expert prior to the expert's trial testimony; and,
    e) All documents, including current curriculum vitae, used to establish the expert's qualifications as an expert witness.

With regard to the usage, operation and maintenance of the servers,

software and or computers in this case, please provide the following:

1) Any and all software manuals, including but not limited to user manuals, training materials, administrator manuals and setup guides for the software that may contain customer data.
2) Any and all maintenance records, including invoices, paid or unpaid, from any vendor involved in the maintenance of the servers, patient accounting software, or other electronic sources of information that will be used as evidence in this case. Such records are to include trouble tickets, user setup tickets, service tickets, password changes, password settings, user account lists, administrative changes and training session information.
3) Any administrative records regarding the installation, maintenance and or usage of the server, the computer network and the patient records software.

Cell Phone Preservation Letter

Cell Phone Preservation / ESI

[date/address]

Re: Notice to Preserve Electronic Evidence [Legal Matter]

Dear _____ :

Our law firm represents [name] in the above legal matter in which you [your business] are [is] [will be] named as a defendant. This letter requests your immediate action to preserve electronically stored information that may contain evidence important to the above legal matter. Briefly, the matter involves [short statement of facts in case].

This notice applies to your [custodian] cell phone, cell phone backups, removable electronic media, and computer systems. This includes, but is not limited to, e-mail and other electronic communications; electronically stored documents, records, images, graphics, recordings, spreadsheets, databases; calendars, system usage logs, contact manager information, telephone logs, internet usage files, deleted files, cache files, user information, and other data. Further, this notice applies to archives, backup and disaster recovery tapes, discs, drives, cartridges, voicemail and other data. All operating systems, software, applications, hardware, operating manuals, codes, keys and other support information needed to fully search, use, and access the electronically stored information must also be preserved.

The importance of immediate action cannot be overstated. Electronically stored information is easily corrupted, altered, and deleted in normal daily operations. Even booting an electronic device, running an application, or reviewing a document can permanently alter evidence.

The cell phone should be powered off, sealed inside of an evidence container, and placed in secure evidence storage until such a time whereas a cell phone forensics expert can create a forensic image of the device. Full chain of custody should also be kept.

Further, any external media or computer system used to create backups of the cell phone should also be powered off according to digital forensics best practices, placed into sealed evidence containers, and securely stored until forensic images of the evidence items can be created. Full chain of custody should also be kept.

Online accounts associated with the cell phone, including but not limited to, social media accounts, application based accounts, cloud data storage accounts, email accounts, messaging accounts, and/or any other application than can be accessed via the cell phone device should be preserved.

[If known, identify any key persons', officers', supervisors', and employees' computers to which special attention for forensic imaging must be directed.] This preservation notice covers the above items and information between the following dates: [state dates].

Follow the above procedures to preserve electronic information created after this notice. Current law and rules of civil procedure clearly apply to the discovery of electronically stored information just as they apply to other evidence, and confirm the duty to preserve such information for discovery.

You [company] and your officers, employees, agents, and affiliated organizations must take all reasonable steps to preserve this information until this legal matter is finally resolved. Failure to take the necessary steps to preserve the information addressed in this letter or other pertinent information in your possession or control may result in serious sanctions or penalties. Further, to properly fulfill your preservation obligation, stop all scheduled data destruction, electronic shredding, rotation of backup tapes, and the sale, gift or destruction of hardware. Notify all individuals and affiliated organizations of the need and duty to take the necessary affirmatives steps to comply with the duty to preserve evidence.

Sincerely, [attorney/address]

Cellular Account Preservation Letter

Date

Dear Custodian of Records,

Now comes _____ , by and through his attorney, and requests the following information be preserved regarding cell phone communications for cell phone number(s) **000-000-0000 and 000-000-0000.** _____ requests that the data and information outlined below be preserved to include the time period of _____ to _____ for a period of 180 days beginning on 00/00/2018. If and when additional preservation time is needed, or if the time that the data is preserved is extended, an additional preservation order will be presented for that purpose.

All information including but not limited to:

Subscriber information for the above listed numbers, including financially responsible party, social security number, billing address, features and services and equipment,

2. Call Detail Records with cell site location, all call originations, call terminations, call attempts, voice and text message transactions, including push to talk, data communications, SMS and MMS communications, and voice communications, including the originating and receiving phone numbers or network IDs for all incoming and outgoing call transactions, data transactions and push to talk sessions.

3. Records are to include the IMEI, IMSI, ICCID or other equipment or handset identification information for the target phone number.

4. All stored SMS content, MMS content and / or Browser Cache

5. Beginning and ending switch and cell site / tower identifiers for each call, SMS MMS and data transmission.

6. Central office identifiers and or switch identifiers for the area of coverage for the time period requested

7. All connection attempts including completed and failed connections with call duration times to one second

8. Any available information regarding the state of the towers for the time period requested, including trouble tickets, maintenance tickets, maintenance schedules and tower downtime records.

9. Any precise measurement data or call detail records with cell site such as, PCMD, RTT, RTTM, RTTL, ERLTE, ALUTE, NELOS, VOLTE, Truecall, TDOA, VOVoice, VOWIFI, VOCDMA e-911 location data, and or any other data recorded for the timeperiod that will provide additional location data.

10. Any information or event activities related to law enforcement activities regarding these phone number to include, but not limited to, a. Pen trap and trace activity

- Content captured or any other CALEA data provided to law enforcement, with or without a warrant or court order for the phone number or numbers for this request.
- Any location data provided to law enforcement under CALEA or as the result of any filing or request by law enforcement for such data.

Respectfully submitted,

Name

Video Evidence Preservation Letter

DATE:

Dear Legal Department,

My client is the subject of an ongoing criminal investigation in which surveillance video from your location, (Store name, address, city, state) was initially collected by the (police department or agency).

In preparation for criminal litigation in this matter, I am requesting that the video device and video data for the surveillance system located at the aforementioned location be preserved in total and specifically for the period of (date and time through date and time).

I am also requesting that you allow our office to have an independent forensics expert travel to the location and collect the original video data for preservation purposes.

Please respond immediately as time is of the essence due to the limited storage capability of video surveillance systems. It is imperative that we collect this data as soon as possible.

You can respond to this request via email to email@email.com or via facsimile to 555-555-5555.

Sincerely,

ATTORNEY NAME

Motion to Compel Production of Cellular Phone (Example)

Motion to Compel Production of Cellular Phone

Please modify the facts to suit your case.

Comes now DEFENDANT, by and through his attorney ATTORNEY NAME, and moves this Court to compel production of the alleged victim's cellular phone for forensic examination.

DEFEDANT is charged with _____, of the most serious offenses under STATE law. Considering the seriousness of this charge, it is absolutely imperative that DEFENDANT have all relevant resources available for his defense.

FACTS of the case:

On _____, 20XX, VICTIM claimed that DEFENDANT sexually assaulted her in her hotel room. Her claim is that she left her hotel room door open in anticipation of a friend's later arrival and then fell asleep. She further claims that the defendant entered her room and sexually molested her.

It is the defendant's belief that evidence contained in the electronic storage of her cellular phone (smart phone), specifically related to Twitter messages she sent to the Internet and subsequently deleted from her Twitter timeline can be recovered from the cellular phone device and that such "tweets" are critical to his defense.

In the same way that evidence collected from a cellular phone can be used to link a perpetrator to a victim, in this case, such evidence can be used to show that the victim posted information related to the alleged assault to the Internet via the service, Twitter, via "tweets", that is in conflict with her account of the crime.

Therefore the defendant respectfully requests that the court compel the alleged victim to produce the cellular "smart" phone for forensic examination for evidence of said "tweets" and other electronic communications, including email and other correspondence that would prove exculpatory to the defendant.

Forensic examinations of cellular phones are conducted every day on a routine basis by law enforcement agencies in the US and such examinations yield a great deal of evidence that is brought to bear in cases by the government. _____ is simply asking the court to allow an expert in cellular phone examinations to provide the same services for the purpose of producing exculpatory evidence

that the victim may have produced communications that are in conflict with her claims via the use of her cellular phone.

Such forensic examinations are well known at this point in time with current forensic examination methods to have the ability to recover information and data that has been deleted from cellular phones, even for a significant period of time after such a deletion has occurred.

Due to the personal nature of a cellular phone, in that such devices are carried on or about a person nearly at all times, this makes the cellular phone a critical repository of evidence and as such, should be produced for examination by the defense's expert, in the same way that a defendant's cellular phone would have been examined by the government's expert in a criminal case with an accusation of such a serious crime as this one.

Temporary Restraining Order + Order for Expedited ESI Discovery

Temporary Restraining Order and Order for Expedited Discovery

THIS CAUSE came on to be heard before the undersigned Superior Court Judge Presiding over the Civil Session of _____ County Superior Court, on___ , on Plaintiff's Motion for Temporary Restraining Order and for Expedited Discovery.

The Court, having reviewed the pleadings of record, finds that the Plaintiff has shown that reasonable grounds exist to believe the following:

1. This is an action by Plaintiff seeking damages and injunctive relief relating to Defendants_____ and _____ breach of a contract containing a covenant not to compete: and relating to all Defendants misappropriation and use of Confidential Information and trade secrets of Plaintiff.
2. Defendants do business in competition with Plaintiff, and using Confidential Information and trade secrets of Plaintiff, _____, from a location whose address is _____ ("The Business Location").
3. Defendants have misappropriated and used Confidential Information and trade secrets of Plaintiff: the Confidential Information and trade secrets are stored on computers owned or operated by Defendants which are a the Business Location (and which may be at other locations): and Defendants may secrete or destroy evidence of their use of the same irreparably and immediately injuring the Plaintiff if they are not enjoined from doing so.

BASED UPON THE FOREGOING FINDING OF FACT, THE COURT CONCLUDES AS A MATTER OF LAW that a temporary restraining order should be entered, preventing Defendants from removing, destroying, or tampering with any of the computers; hard drives, disks, CDs, DVDs, memory sticks, thumb drives, or any other medium upon which information is stored electronically, that they may have at any location.

BASED UPON THE FOREGOING FINDINGS OF FACT, THE COURT FURTHER CONCLUDES AS A MATTER OF LAW that an order should be entered granting expedited discovery by permitting Plaintiff's inspection and copying of all of the computers; hard drives, disks, CDs, DVDs, memory sticks, thumb drives, magnetic tapes, or any other medium upon which information is stored electronically, which are at the Business Location.

NOW, THEREFORE, IT IS HEREBY ORDERED, ADJUDGED AND

DECREED AS FOLLOWS:

1. Defendants are temporarily restrained and enjoined from removing, destroying, or tampering with any of the computers; hard drives, disks, CDs, DVDs, memory sticks, thumb drives, magnetic tapes, or any other medium upon which information is stored electronically, that they may have under their possession, custody or control, at any location.
2. Hearing on Plaintiff's motion for preliminary injunction, extending the restraints set forth herein, shall be held in the _____, _____ of _____at_____ on the _____day of___, 2010, or as soon thereafter as may be reached.
3. Plaintiff shall post as a bond, with respect to entry of the restraints set forth, the principal amount of $_____.

IT IS FURTHER ORDERED, ADJUDGED AND DECREED as follows:

1. Defendants shall allow representatives of Plaintiff to enter the Business Location (_____) and conduct an examination of any of the computers; hard drives, disks, CDs, DVDs, memory sticks, thumb drives, or any other medium upon which information is stored electronically, which are at the Business Location. Such examination may include copying of all hard drives, disks, CDs, DVDs, memory sticks, thumb drives, or any other medium upon which information is stored electronically. Defendants may permit Plaintiff's representatives to remove such items to expedite copying process, or may permit the inspection and copying to be performed at the Business Location, as Defendants may elect.

2. Defendants shall permit the entry and copying described above beginning at____ on the ___day of _____, 2010 and continuing until finished.
3. The _____Sheriff shall serve this Temporary Restraining Order and Order for Expedited Discovery upon Defendants as immediately as possible.
4. The information discovered in response to the inspection and copying permitted herein shall be used by Plaintiff solely for the prosecution of its claims, and for no other purpose whatsoever, unless and until the Court orders otherwise.

_____

Superior Court Judge

DATE AND TIME ENTERED: _____

Digital Evidence Examination Procedure (Example)

If an expert is appointed or retained onto a case, they should provide a procedure detailing how evidence will be handled and examined. If they have no such protocol, I would question their capability and training. Protocols provide a roadmap for you, opposing counsel, and their expert.

A comprehensive procedure can help you get things done, moving the ball forward in your case. Often, both parties want the evidence contained on the mobile phone. However, concerns of those involved can impede the process. These concerns center on how evidence will be handled and if the examiner will properly protect the device's data or the device itself, as well as how much of the data the examiner and opposing attorney have access to.

Here is an example protocol our team developed for a transportation (trucking) accident case:

Digital Device Examination Procedures of MAKE AND MODEL

PRIVACY PROTECTION

A representative of Envista Forensics' Digital Forensics group will perform a forensically sound acquisition or extraction of data from the computers, cell phones, GPS devices, or electronic storage devices.

The forensic hardware and software employed by Envista Forensics is considered the industry standard and is in use all over the world by a large number of private forensic consulting firms and law enforcement agencies worldwide, including the Federal Bureau of Investigation (FBI), Homeland Security, the Department of Defense, Naval Criminal Investigation Services (NCIS), the Secret Service and hundreds of other national, state and local agencies.

Software and hardware tools in use by Envista include Cellebrite, Logicube Forensic Falcon, MacQuisition, EnCase Forensic Software, Forensic Tool Kit (FTK), Paladin, Magnet Axiom, Tableau Write Blockers, Image MASSter, Encase Portable, WeibeTech Forensic UltraDock, DI USB 3.0 Media Card Write Blocker and other tools as needed.

In the particular case of cell phones, the Cellebrite tool does not allow the examiner to restrict the data retrieved from the phone. The data that is ultimately delivered to the parties involved can be limited to a particular time frame and limited to a selected portion of the complete data set, such as only producing text messages or call history.

The digital forensic examiners at Envista Forensics are trained and experienced in the collection and protection of data so that nothing is exposed that is outside of the parameters set in civil agreements, court orders, or protective orders.

All of the data collected during the forensic extraction process is secured and stored in our locked, secure storage area. No data is provided to anyone outside the scope of the disclosure limits agreed to by the parties of this matter unless so ordered by a court of law.

NON-DESTRUCTIVE PROCESS

All of the processes, hardware, and software used in the acquisition (copying) of data from cell phones, computers, GPS devices, or other electronic storage devices are non-destructive.

The basic tenet of forensic acquisitions (forensic copying) and examination of digital evidence from electronic storage devices of all kinds are that the process must protect the original data from any change. There is a built-in method of verification to ensure that the original data matches the forensic copy of the data at the time the data is forensically copied. This verification is in the form of a "hash value."

A hash value is a mathematical calculation using the contents of the data to create a computed value unique to the contents of the data as it exists when acquired.

To prevent the engagement of possibly destructive processes (Brute Force, JTAG, ISP, Chip Off), Envista Forensics should be provided the following:

- Device PIN (Personal Identification Numbers), typically between four and six digits
- Device Passwords (alphanumeric combination containing letters and numbers)
- Device Unlock Patterns
- Encryption Passwords
- Smart Lock

Presence of Mobile Device Management (MDM) applications such as AppTec360 Enterprise Mobility Management, Baramundi Management Suite, ManageEngine Mobile Device Manager Plus, SOTI MobileControl, Citrix XenMobile, IBM MaaS360, Microsoft Intune, VMware AirWatch, and MobileIron.

MDM applications are typically utilized by government, businesses, and schools

EVIDENCE TRANSFER

After completing the below-described chain of custody form, the evidence custodian should package the evidence to prevent damage during shipment.

Regardless of the shipping vendor the custodian chooses, Envista typically requests the following:

- Shipment Tracking Number
- Overnight Shipping (if authorized by paying party)
- Direct Signature Required
- Please ship evidence to the following:

  ENVISTA FORENSICS

  ATTN: Jake Green

  2700 Gateway Centre Blvd, Suite 100

  Morrisville, NC 27560

Please provide the tracking number, estimated delivery date, and time by email to jake.green@envistaforensics.com

CHAIN OF CUSTODY

Complete a chain of custody form for receipt of the computer, cell phone, GPS device, or electronic storage device and any accessories.

- Each item is to be listed separately on the chain of custody form.
- The device will be inspected at the Envista Forensics Lab office in Morrisville, NC.
- The device is logged into custody, identified, and assigned a unique identifying lab number.
- The device is identified by make, model, and unique identifying number (IMEI, DEC, ESN)
- The device is tagged with a lab number.
- The device is isolated from network/internet connections.
- The device is physically inspected.

CONDITION

All items of interest will be photographed before any work is performed for chain of custody purposes.

If the computer, cell phone, GPS device, or electronic storage device is in a bag or other container, take a photo of the container before removing the computer, cell phone, GPS device, or electronic storage device for inspection from the front, back, and top of the container.

If the computer, cell phone, GPS device, or electronic storage device is not in a container, take a photo of the computer, cell phone, GPS device, or electronic storage device in its current state of the top, bottom, front, back, left side and right side.

Take close-up photos of any identifying information, including any asset tags, the serial number, MEID HEX, product number, ESN, and any other identifying information.

If the computer, cell phone, GPS device, or electronic storage device is a flip phone or a clamshell design, open the device to show the screen and keypad. Take photos of the screen and the keyboard area.

Have the producing custodian sign the chain of custody form indicating that they have reviewed the inventory on the Chain of Custody form and are transferring the items to a representative of Envista Forensics.

RESEARCH

The device is fully researched before extraction. Research includes:

- Operating system
- CPU Chipset
- Memory type/size
- Carrier limitations
- Manufacturer limitations
- Forensic tool compatibility
- Research sources include:
- Lab notes
- Peer networks
- Internet
- Manufacturer

REPAIR (If required)

- Physical damage will be closely assessed and triaged.

- Physical part damage
- Internal component damage
- Liquid damage
- Physical part damage will be repaired by part replacement.
- Screen
- Buttons
- USB port
- Battery
- Sensors
- Internal component damage will be repaired by component replacement.
- Liquid damage will be repaired by following liquid damage protocols.
- Isolation
- Ultra-Sonic cleaner

The repair goal is to achieve an extractable device, not a permanent repair. Repair methods/techniques will move towards that goal.

EXTRACTION

An extraction method is chosen based on research and device status. The least invasive, non - destructive method that produces the desired results will be used.

Desired results in order of importance (most preferred to least preferred)

- Full Physical extraction
- File system extraction
- Logical/Advanced Logical extraction

Only industry-accepted digital forensic methods will be used for extraction. User data WILL NOT be modified.

ENVISTA EXPERT NAME will conduct the extraction at the Envista Forensics Lab in CITY, STATE.

Equipment/Software used MUST be licensed to Envista Forensics Laboratory or individual examiner.

Extraction Tools for the MAKE AND MODEL: (in order of preference)

- Cellebrite UFED

- Axiom

EXTRACTION RESULTS

- A successful extraction will result in a forensic copy of the device's memory.
- The result will be a .bin file or forensic container.
- Results will be assigned a hash value for self-authentication
- Counsel for the parties may be present during the extraction process.
- Opposing counsel's expert may be present during the extraction process to monitor the work.

POST EXTRACTION

Open the forensic image of the computer, cell phone, GPS device, or electronic storage device in the associated forensics software program to ensure the image was completed successfully, thoroughly, and verifiably.

Have the producing custodian sign the chain of custody form indicating that they have reviewed the inventory on the Chain of Custody form and are receiving the items back into their custody from Envista Forensics.

Create master and working copies of the forensic image on separate storage locations for backup redundancy.

VALIDATION

Validation is conducted whenever possible to ensure equipment/software operation.

ANALYSIS

Data carving/parsing will be conducted on the extracted forensic copy (.bin file, .rar file) only. Only industry-accepted digital forensic software will be used for Analysis.

Analysis software includes (in order of preference):

- Cellebrite Physical Analyzer
- Axiom

Analysis TBD after the acquisition and not completed until scope has been agreed on by both parties.

- Experts will be authorized to review data during the following timeframe:
- 90 minutes before and after 12:00 PM on January 1, 2020

- No other data may be exported or retained.
- Defendant's expert will retain the originally extracted data.
- REPORTING
- The scope of Analysis governs the final examination report.
- Final examination report formats:
    - Adobe PDF,
    - Microsoft Excel, or
    - UFDR (with reader)
    - Included with the final examination report:
    - Analyst report (PDF of technical data)
    - The report will be on electronic media (depending on size)
    - DVD
    - Flash Drive

Envista Forensics' disclosure to Defendant, _____, shall be limited to a written report summarizing recovered electronically stored data of Defendants usage of device functions during the aforementioned period including, but not limited to, application usage, voice usage, messaging usage, GPS usage, Bluetooth pairings, locations, SIM Data, and wireless network usage.

Envista Forensics shall not disclose or shall redact any "Personal Information" extracted from the device.

Envista Forensics acknowledges and agrees to the term "Personal Information" as used herein and as defined below. Forensic expert agrees it shall keep secret, retain in the strictest confidence and prevent the unauthorized duplication, use, and disclosure of the Personal Information. Personal Information shall be used and duplicated (as is reasonably required) only so that Forensic Expert may accomplish the Extraction and Analysis and for no other purpose. Forensic expert agrees, except when required by law, to maintain and keep confidential Defendants Personal Information and not disclose the same to the Receiving Parties or third parties to this Agreement. "Personal Information" includes the following data during the period of time analyzed pursuant to the Analysis: email content (recipient name and number, subject line, body text), text message content (recipient name and/or number, body text), SMS/MMS content (recipient name and/or number, body text), Instant Messenger (IM) content (recipient name and/or number, body text), social media posting content made during the period in question, photographs, videos, website addresses or URLs, Social Security numbers, PINs (Personal Identification

Numbers), user names, passcodes, passwords, voicemails, recorded messages, notes, cookies, browser history, bookmarks, phone numbers, the identification of callers to or from the Mobile Device(s).

Plaintiff's counsel will receive an additional copy of the complete raw binary extraction (.bin file or.rar file)

EVIDENCE RETURN

The device is resealed in its original evidentiary container and marked with initials/date.

If the device is submitted without an evidentiary container, it will be sealed in a new container and marked with initials/date

The device will be immediately returned to plaintiff's counsel via a prepaid shipping label or FedEx.

CONFIDENTIALITY

Envista Forensics acknowledges that it may be held liable for disseminating Personal Information to parties other than opposing counsel unless and until such time as the Trial Court approves of such dissemination by written order.

Except as required by law, Envista Forensics agrees to take commercially reasonable steps to protect from disclosure to third parties any confidential and proprietary information of the plaintiff that may be exchanged in connection with this examination. Except as required by law, Envista Forensics agrees to take commercially reasonable steps to protect the confidentiality of information in or on electronic data and media made available or furnished to them for examination. Plaintiff agrees that if during the course of this examination, Envista Forensics shall find within any electronic data or media evidence of child exploitation (e.g., child pornography) or of a credible threat of physical harm to any person, Envista Forensics shall be entitled to immediately bring such matters to the attention of federal or state law enforcement authorities and that no assertion of privilege, confidentiality or breach of contract will be raised as a bar to such action.

_____

PLAINTIFF

_____

DEFENDANT

Facebook Subpoena Language/ Self-Download

Facebook can be difficult to obtain records from via subpoena. Included in this section is Facebook's reasoning , and how to do a self-direct download of Facebook data.

Subpoena Language

Facebook

Facebook, Inc.

Contact Name:	Security Department/ Custodian of Records
Online Service Address:	1601 S. California Avenue Palo Alto, CA 94304
Fax Number:	650-644-3229
E-mail Address:	subpoena@fb.com
Note(s):	Requests may be faxed, emailed, or mailed.

Any and all subscriber records regarding the identification of Facebook friend ID(s): **10000000000**, emailaddress@email.com to include real name, screen names, status of account, login log, ip address log, detailed billing logs, date account opened and closed, method of payment and detailed billing records. Also, to be included, but limited to, are all stored emails and all profile pages including wall posts, communications and chat logs.

Such stored information is to include any deleted and or archived pages or email or communications, that Facebook has retained as part of its normal business operations for the period of _____ to _____.

In the case of archived or deleted pages for the above account, the archive URLs for the pages may be returned as part of this request, provided that the URLs are accessible via the Internet. If any credentials are required to access the archive URLs, then those must be provided as part of the response to this request.

Download Facebook Account (Reason)

The following is Facebook's response to the question, "May I obtain any account information or account contents using a subpoena?"

Account Contents

Federal law does not allow private parties to obtain the content of communications (example: messages, timeline posts, photos) using subpoenas. See the Stored Communications Act, 18 U.S.C. § 2701 et seq.

Parties to litigation may satisfy party and non-party discovery requirements relating to their Facebook accounts by producing and authenticating the content of communications from their accounts and by using Facebook's "Download Your Information" tool, which is accessible through the Settings drop down menu. Facebook does not respond to requests to disclose information that are accompanied by purported user consent because Facebook account holders may access, produce and authenticate information from their accounts.

If a person cannot access their content, Facebook may, to the extent possible, attempt to restore access to deactivated accounts to allow the person to collect and produce their content. However, Facebook cannot restore account content that has been deleted.

Account Information

Facebook may provide the available basic subscriber information (not content) where the requested information is indispensable to the case, and not within a party's possession upon personal service of a valid subpoena or court order and after notice to affected account holders.

Your subpoena or Court order must be directed to the entity mentioned in the Terms of Service that are applicable to your use of the Facebook service (i.e. Facebook Ireland or Facebook, Inc., depending on where you are domiciled meaning if serving the subpoena on Facebook, Inc., the subpoena must be a valid federal, California or California domesticated subpoena, addressed to and served on Facebook, Inc. If serving Facebook Ireland Limited, the subpoena or court order must be addressed to and served on Facebook Ireland Limited.")

Any such subpoena or court order should be limited in scope to seek basic subscriber information only, and set out the specific accounts at issue by identifying them by URL or Facebook user ID (UID). Names, birthdays, locations, and other information are insufficient.[1]

[1] https://www.facebook.com/help/133221086752707?helpref=related&ref=related&source_cms_id=1332210867527 07

Download Facebook Account (Instructions)

This is the method Facebook provides for users to download Facebook accounts:

If you want to download a copy of your information from Facebook, you can use the **Download Your Information** tool.

To download a copy of your Facebook data:

Click in the top right of Facebook.

Select **Settings & Privacy**, then click **Settings**.

In the left column, click **Your Facebook Information**.

Next to **Download Your Information**, click **View**.

To add or remove categories of data from your request, click the boxes on the right side of Facebook.

Select other options, including:

The format of your download request.

The quality of photos, videos and other media.

A specific date range of information. If you don't select a date range, you'll request all the information for the categories you've selected.

Click **Create File** to confirm the download request.

After you've made a download request, it will appear as **Pending** in the **Available Copies** section of the **Download Your Information** tool. It may take several days for us to finish preparing your download request.

Once we've finished preparing your download request, we'll send a notification letting you know it's ready.

To download a copy of data you requested:

Go to the **Available Copies** section of the **Download Your Information** tool.

Click **Download** and enter your password.

You can also click **Show more** to view information about your download request, such as the format and when it will expire.

Note: You can always view your Privacy Shortcuts to learn about the ways you can control your data and privacy on Facebook. If you want to review recent activity on your Facebook account or want to review your Facebook account information, you can use the Access Your Information tool.

Adam Walsh Act (Child Exploitation) Language

Contraband cases are unique in the sense that they are covered by the Adam Walsh Child Safety and Protection Act of 2006. Because of this federal law, barriers are in place to prevent actions that would result in the distribution of the materials to defense attorneys and defense experts. An expert working on behalf of the defense must perform their examination onsite at a law enforcement facility and under their supervision. Data can be taken from this examination, such as log files, file listings, and other forensics artifacts. However, no images or videos of contraband, even suspected contraband, should be taken.

Language for Access to Evidence in Child Exploitation Cases

ACCESS TO FORENSIC EVIDENCE

The Defendant requests that government's agent provide to the Defendant's expert access to the physical evidence seized by the State in the course of its investigation under the following conditions:

1. The defense expert will supply in advance an external hard drive, factory new, if required by the law enforcement agency, for the purpose of providing forensic copies of the evidence to be examined during the defense expert's forensic examination and will be kept in the custody of law enforcement at all times.
2. The law enforcement agency shall copy to the provided hard drive any FTK, Encase or other type of forensic image files that are an exact forensic copy of the hard drive(s), CD-ROM or DVD-ROM media, flash cards, floppy disks, smart media cards or any other digital evidence seized and copied by law enforcement.
3. The law enforcement agency shall provide to the defense expert an un-redacted copy of any computer forensic reports for the use of the defense expert while performing the forensic examination. Such un-redacted reports shall be returned to the law enforcement agent at the end of each day's examination period at the discretion of the supervising agent.
4. The law enforcement agency shall have available for inspection by the defense expert copies of any derivative evidence created and supplied to the prosecution, including but not limited to media created for the purpose of prosecution review, submission to the National Center for Missing and Exploited Children, or for the use by other law enforcement parties to the investigation of the charges, pending or otherwise.

5. The expert will perform all of his work on the provided hard drive, using forensic analysis equipment provided by the law enforcement agency, provided that hardware provided by the law enforcement agency is no more than 18 months old, has a current version of 64 bit Windows OS (7, 8 or 10), and current versions of Microsoft Office Professional, Adobe PDF reader, a video player that is fully configured to play all types of video files such as VLC Media player, and any other software normally used in the course of forensic examinations, excepting actual forensic software. The expert may install other forensic analysis software on the provided computer for the purpose of performing his examination as needed and will bring his own licensing keys or USB dongles for that purpose.
6. At the end of the forensic examination session, the examination hard drive will be sealed in the presence of the defense expert and given to the law enforcement agent and kept in the custody of the police in case further review is needed at a future time or the review room will be locked so that processes on the computer can continue overnight as needed.
7. The law enforcement agency shall make such supervisory arrangements as deemed appropriate in accordance with the law enforcement agencies' policies and procedures for the forensic examination of contraband material by a defense expert.
8. The expert will show to the law enforcement agent any items he wishes to copy or print, to provide to defense counsel as part of his analysis or reporting, to ensure that no contraband images are copied or transferred.
9. The expert will be given a minimum window of 6 hours per day, scheduled in advance, to perform the analysis.
10. All items and information discovered by the expert are to be treated as attorney work product, and protected as such even though the law enforcement agent will review said documents and information for the presence of contraband.

GUIDE –Digital Forensics in Child Exploitation Cases – Finding Your Way Through

Justin Ussery, Digital Forensics Examiner
Jake Green, Digital Forensics Examiner

About the Authors

Jake and Justin have are both Former Law Enforcement Officers who were assigned as Digital Forensic Examiners and Task Force Officers of the United States Secret Service Electronic Crimes Task Forces in South Carolina and California. Jake and Justin both work matters and cases involving all aspects of Digital Forensics, including Cellular Phones, Tablets, Computers, and Cloud data. This article is meant to give you a brief overview of the frequently and daunting amount of confusing electronic evidence you receive in discovery and an overview of this information you often find in the discovery process of a Child Exploitation matter.

Introduction

This article is meant to give you a brief overview of what is frequently a daunting amount of confusing electronic evidence you may receive via discovery in a child pornography case.

Uniqueness of Child Exploitation or Child Pornography cases

Child pornography cases present unique difficulties because of how attorneys can view the evidence and how experts can examine that evidence. These cases are controlled at the federal level by the Adam Walsh Child Safety and Protection Act of 2006. This act explicitly says government examiners cannot send a report containing child pornography in any form to any person outside of law enforcement. The evidence review likely will take place at a government facility, and we are often supervised by law enforcement officials, often the same ones who performed the original forensics. The Adam Walsh Act prevents child pornography from being disseminated, which is a good thing. However, this places a burden on the defense, as examinations of forensic data need to occur at a law enforcement facility. The examiner may only leave with certain artifacts, which do not contain images or videos, making the onsite review of the evidence critical, as this typically does not take place more than once due to the cost of placing a forensic examiner on site.

Law Enforcement Investigations: Before the Search Warrant

CyberTips

Law Enforcement typically deals with two main entities when it comes to dealing with child pornography: Internet Crimes Against Children (ICAC) and The National Center for Missing and Exploited

Children (NCMEC). NCMEC acts as a clearinghouse for business and Electronic Services Providers (ESPs) to report possible illicit media.

After ESPs notify NCMEC, a "CyberTip" is created and forwarded to a Regional ICAC Task Force or local law enforcement agency. The Regional ICAC Taskforce or agency then investigates and collects evidence. The investigating officer may perform a forensic examination of this evidence or may assign this to a qualified forensic examiner.

All of this activity originates with the Cyber Tip.

The Cyber Tip will generally include dates and times of said activity, Internet Protocol (IP) addresses during the period of the event, and account information such as email addresses, phone numbers, mailing addresses, and possible user names of the account utilized during the actions.

Online Law Enforcement Investigation Tools and Resources

Detectives and investigators across our country conduct digital or online investigations with a variety of digital tools and software. Many of these tools are deemed to be "law enforcement sensitive" and in our experience as law enforcement examiners, a court order may be required to gain access to these specific tools for review by a forensic examiner working with defense counsel.

Several keywords and processed should be defined at a basic level before continuing:

IP Addresses

An Internet Protocol address is an identifying number for a computer network. A unique Public IP address is assigned by an Internet Service Provider (ISPs like CenturyLink, RCN, Frontier, Verizon, or AT&T). These assignments are unique to physical locations (modems or gateways), which can distribute the connection physically via a wired network switch or a broadcast wireless network via a Wi-Fi router. Public IP addresses are unique to physical locations (home, business, public Wi-Fi) and are not typically unique to physical devices like cellphones, computers, and tablets.

Once an IP address is documented, the owner of the IP address can be found. IP addresses are owned by Internet Service Providers (ISP).

This identification process proceeds in steps:

The IP address is obtained by law enforcement from an online investigation.

The owner of the IP address is identified using a "reverse" lookup to locate the company that owns the IP address. This is accomplished using a "WHOIS" lookup service. One such service is "whatismyip.com". For instance, looking up a text IP Address shows that the owner of the IP Address is Charter Communications.

One the owner of the IP address is known; the law enforcement officer will create a warrant or subpoena and send that to the owner of the IP address to obtain the subscriber information for the IP address on the date of interest.

GUID: Globally Unique Identifier

GUIDs are an alphanumeric series of numbers that can be assigned by a computer system. For this article, a GUID is assigned to each asset or device within a P2P network. This GUID is unique but can be changed or updated by the P2P network.

Metadata: "Data about data."

While the colloquial definition "data about data" is often used, we prefer "information about data." Metadata is a collection of information about the source or creation of data. This information could

be the manufacturer or model of a camera, GPS location, file metadata such as date and time of creation; or modifications, source, author, or editor.

Hash Value: Electronic DNA

A hash value is the application of a mathematical formula (algorithm) to produce a unique alphanumeric string associated with a single file or a set of files. Changes to the data (even a single bit) will result in the change of the hash value. Hash values allow investigators to identify known images, accurately preserve and reproduce data. Common hash values are MD5 (message-digest algorithm), SHA-1, and SHA-256 (Secure Hash Algorithm).

Through our background, experience, and review of software documentation, we're able to offer some insight into these investigative aids. We cover three unique pieces of software used by law enforcement to conduct online investigations. It should be noted that the log files discussed in each section are unique to each piece of software and should be requested through discovery or court order. The below listed log files do not contain illicit content, images, or media and can be released by law enforcement to a civilian defense examiner.

ShareazaLE

One of the most common investigative tools is a variant of the peer to peer (or "P2P") program, Shareaza, that has enhanced features for investigations. This piece of software allows law enforcement to single out an IP address (known as a "single source download"). ShareazaLE produces a log called "ShareazaLE Summary Report for IP: "0.0.0.0"," where "0.0.0.0" is the target or identified IP address.

Torrential Downpour

This is another free piece of software that has been modified to suit the needs of law enforcement investigators. However, this piece of software operates using a different protocol, called torrents. In the most basic sense, torrents are a series or set of files. The torrent file itself is a set of instructions related to the source file and metadata. These source files can be a single file (i.e., movie) or an archived folder containing multiple files (i.e., sets of photos or music from an album). Torrent files are typically sourced from search engines, websites, or forums, but some Bit Torrent software packages have built-in search features. Torrential Downpour produces a series of log files: Datawritten.xml, Details.txt, Downloadstatus.xml, Netstat.txt, summary.txt, and Torrentinfo.txt. It should be noted that the torrent file itself is not illegal to possess as it contains only metadata.

RoundUp eMule

RoundUp was designed to investigate the eD2K or eDonkey2000 file-sharing network. EMule and similar P2P networks are built around keyword searches. A user enters a general keyword (like "porn"), and the search results in the return of any files containing the keyword (i.e., "child porn" or "adult porn"). RoundUp produces logs named: SummaryLog.txt, DetailedLog.txt, Netstat.txt, IdentityLogging.txt, and IndentitySignatures.xml.

Law Enforcement Investigations: After the Search Warrant

Major Software Vendors

There are several major software vendors utilized by both government examiners and private examiners alike. For cellular device forensics, you will likely see Cellebrite UFED with Physical Analyzer, Oxygen Forensics Detective, Axiom by Magnet Forensics, and GrayKey by Grayshift. Most cellular device tools rely on three general types of extractions from the phones, but all produce very similar results with a few caveats. There are thousands of applications operated on four major smartphone operating systems: Android, Apple iOS, Windows Mobile, and Blackberry OS. Not every tool can decode and make

sense of every single application in the world and that is a primary reason why it is beneficial to utilize a variety of different tools during examinations.

As for computer forensics, you will see Axiom or IEF by Magnet Forensics, Forensic Took Kit by Access Data, Encase by OpenText, Analyze by Griffeye, Forensic Explorer by GetData and BlackLight by Cellebrite (formerly Blackbag Technologies).

Many of these tools can redact child pornography images and safely provide a good deal of metadata about the activities without the dissemination of child pornography by Law Enforcement or prosecutors.

Review of Digital Forensic Evidence

If law enforcement recovers electronic evidence and utilizes forensic tools, the scope of their investigation should not be limited to the simple question of "Is illicit media on this device?" Digital investigations need to be a great deal more comprehensive. An expert should search for any known evidence such as suspect IP Address, GUID, hash values, user attribution, as well as a possible indication of file use and knowledge.

Many law enforcement forensic tools and Cyber Tips identify IP Addresses and GUIDs. A review of these records is essential to identify the physical location of an IP address (possibly the defendant's home or work). The subsequent investigation of a network, like a broadcasting Wi-Fi router, may be necessary to determine what devices were connected at a location. While gathering evidence, an investigator should collect and review network connection logs (if logging is enabled) or records from an ISP. Knowing when and what devices were connected to a network can significantly assist in the identification of a suspect. Failing to gather these logs can result in their overwriting or deletion.

If a law enforcement investigator is adequately trained and utilizes online tools, like those outlined above, they should retain the available logs. These logs should become part of the investigator's digital case file. The logs should be maintained as a unique piece of digital evidence, as printing will result in the loss of file metadata (i.e., the creation and modification dates and times).

This metadata is critical to what is referred to as "user attribution."; putting a specific person behind the keyboard at the time of the offense. This will likely make or break the case for a prosecutor. These indicators of user attribution are often forgotten or overlooked by examiners who are providing evidence to the investigating officer or prosecutor.

These user attribution indicators are held in a variety of places on a computer and consist of jump lists, .lnk files (pronounced "Link"), Shellbags, Windows MRU, and search terms found within browsing histories.

Jump Lists

A "jump list" is a system-provided menu that appears when the user right-clicks a program in the taskbar or on the Start menu. It is used to provide quick access to recently or frequently used documents and offers direct links to app functionality.

Link Files

An LNK (short for LiNK) is a file extension for a shortcut file used by Microsoft Windows to point to an executable file. LNK file icons use a curled arrow to indicate they are shortcuts, and the file extension is typically hidden from the computer user. Generally, if the "linked" or source file is deleted, the LNK file will remain behind and will contain information not only of when the LNK file was created, but about the target file of interest.

Shellbags

Windows uses the "Shellbag" to store user preferences for folder display within Windows Explorer. Everything from visible columns to display mode (i.e., icons, details, or list) to sort order and are tracked.

Most Recently Used files (MRU)

The Most Recently Used "MRU" is a list that contains a history of recent activity on a computer. MRUs can include open documents or webpages.

If user attribution indicators are disregarded for any reason, the case weakens. The user attributes held within these specific items can show a pattern of behavior by a computer user. This makes it much more unlikely that this offense was an isolated incident and was occurring over an extended time period. Again, these crucial artifacts frequently go unexamined. These are in many cases, "make or break" items worth looking at when it comes to a defense strategy.

Defense of Child Pornography Cases

U.S. vs. Flyer

In *U.S. vs. Flyer*,[i] defense counsel made successful arguments regarding the lack of possession for images found in unallocated space. Unallocated space is not accessible by ordinary users. We have reviewed many cases where government examiners find child pornography in unallocated space but do not

identify additional forensic artifacts. An inability to exercise "dominion and control," no proof of "file use and knowledge," and lack of user attribution makes a case easier to defend as there is a lack of knowing possession and intent.

Thumbnails and Cache Files

Thumbnail images are an image that is a smaller representation of the original photograph. These thumbnail images by themselves usually are devoid of metadata and are created by the operating system without use interaction.

The Internet browser cache contains images saved by the browser to help speed up your rendering of web pages. By avoiding downloading the same image again and again the computer user experiences a faster web page viewing experience.

In both instances, the operating system or web browser application is automatically doing this as an automated process. The computer user has no knowledge of or access to these files.

ISP Connections

The way that the law enforcement agency determines where to go for a search warrant or "knock and talk" is to find out the subscriber account for an internet download.

When law enforcement performs a lookup of the IP address for a download, they will then research to determine which Internet Service Provider owns that IP address.

Once the owner of the IP address is determined, i.e. Spectrum or Charter Cable, the law enforcement officer will send a subpoena to the ISP and find out who the subscriber is for that IP address on the date and time of the download.

The subscriber account information will also provide a physical address for the internet connection.

Once the law enforcement officer has that information in hand, he or she will then apply for a warrant to search the residence or business at the address, This is based on the probable cause in the form of the download history from one of the tools used for the online investigation and the subscriber information from the ISP.

There are times when the connection is not being made from the address, i.e. someone is stealing a connection from a nearby address.

"The sound of his door being broken down awoken the man at 6:20 a.m. on March 7. Seven armed officers greeted the homeowner, whose name has not been released. He was forced to lie down on the floor while the officers pointed guns at him while calling him a pedophile and a pornographer. According to the Associated Press, the officers had the initials of I.C.E. on their jackets, which the man didn't know stood for Immigration and Customs Enforcement, and we don't blame him.

The agents searched the man's desktop for about two hours that morning looking for evidence, and eventually confiscated the computer, as well as his and his wife's iPads and iPhones. It took three days for investigators to realize the man, who had told the officers at the time of the intrusion that they had the wrong guy, was actually telling the truth and was indeed not the kiddie-porn downloader. A week later, investigators arrested a 25-year-old neighbor and charged him with distribution of child pornography. However, he did not get in trouble for piggybacking off the man's WiFi signal."

Source: https://www.geek.com/news/man-wrongly-accused-of-child-porn-learns-to-password-protect-wifi-the-hard-way-1347033/

Conclusion

Nearly every case in today's digital age has an electronic evidence component. These components can supply both supporting and damning information for your case. The question is: How do you obtain and interpret the evidence? A qualified and experienced expert can assist you with a thorough discovery review and comprehensive analysis of the electronic evidence.

[i] 633 F.3d 911 (9th Cir. 2011).

DIGITAL FORENSICS //

ENVISTA FORENSICS

Vehicle Infotainment Forensics: It's About More Than Accidents

Lars Daniel, EnCE, CCPA, CCO, CTNS, CTA, CIPTS, CWA
Practice Leader – Digital Forensics at Envista Forensics

With the new technologies developed for vehicle infotainment systems, principally by BERLA, digital forensic experts can access digital evidence from many of today's vehicles. This evidence can include location history, connected devices, and operating system data, including hard braking events, gear shifts, the speed of the wheel, and hard acceleration.

Further, the forensic artifacts recovered from vehicle infotainment systems allow an examiner to determine where hands were in a vehicle at a particular point in time. For example, if someone used the controls on the steering wheel to change the volume or reached across to the center console to turn the volume knob.

The digital evidence that an examiner can recover from vehicles is not relegated to vehicle accident cases. Imagine the following scenario. A defendant allegedly drove to a location and committed a crime. According to the state's theory, the defendant traveled there and committed the crime alone. However, upon analysis of the infotainment system data from the vehicle, it is determined that three doors opened simultaneously upon arrival at the incident location: the front driver door and the two rear passenger doors. This action is an interesting trick, an impressive physical feat, or, most reasonably, the defendant was not alone.

With an event data recorder or EDR, the purpose is to store pre and post-crash data. The resulting data from an EDR extraction applies primarily to accident reconstruction alone. This does produce more robust crash evidence than the infotainment system. Still, it does not produce as much or the same types of evidence as the data collected in infotainment forensics analysis. Further, some accident events are too small for an EDR to record, including a low-impact collision with a bicycle or pedestrian. In these situations, the methods by which an infotainment system records vehicle event data, with less total data but over a long period, may be the best or sole source of crash data evidence.

Except in a crash event, infotainment system data is superior in answering the who, what, when, where, and why questions. This is especially true when a person connects their phone to

the vehicle infotainment system. When this connection occurs, data from the phone is synced to the vehicle. An infotainment system is formally defined as:

"A factory original or aftermarket console system that uses some form of connectivity to provide drivers and passengers with vehicle specific information, navigation, and standalone or integrated applications and/or multimedia entertainment including audio and video" [1]

In other words, an infotainment system is a combination of capabilities, typically including GPS, satellite radio, Bluetooth, Wi-Fi, the ability to pair and interact with a mobile phone, and the ability to play audio and video. These capabilities are represented to the user on the screen with a Graphical User Interface or GUI, which makes the functionality of the infotainment system accessible to non-technical consumers.

The data contained falls into one of three primary categories: navigation data, vehicle event data, and user data.

Vehicle Event Data

The vehicle information data includes evidence related to braking, gear shifts, wheel speed, and hard acceleration. It can also record Wi-Fi and Bluetooth connections and disconnections. While this information may seem useless outside of an accident investigation, this is not the case. In the previous example, we utilized multiple doors opening simultaneously to show how this evidence could answer the question if the defendant were alone or with others at a particular time.

If it is critical in a case to determine if someone is impaired in some way, the vehicle event data around the time the person is believed to be impaired could be compared to the entirety of the vehicle event data to see if it is different. In other words, if they historically drive responsibly, but during the period of interest, these data points paint a picture of erratic and unusual driving, the data could be utilized with other evidence to bolster or refute the claim of impairment, even if that impairment does not lead to a vehicle accident.

For example, a defendant is accused of burglarizing a business. The vehicle event data shows that they usually drive safely, within normal parameters. However, the driving was erratic and unusual on the day in question. This information is provided to counsel. Holistically looking at their case, counsel connects the erratic driving to the fact the defendant had changed from one medication to another as instructed by their doctor the day before.

Navigation Data

The navigation data recoverable from an infotainment system includes saved locations, recent locations, and track points, among other forensic artifacts. It is not uncommon for many thousands of data points related to navigation to be recovered from the vehicle. This data allows an examiner to determine where that vehicle has been historically, potentially going back to the car's genesis, resulting in potentially years of location data.

This data is exceptionally well utilized when conjoined with other forms of location evidence in the same case. Not only is the infotainment system in your car tracking where you go. Your mobile phone is also recording your location activity to act as a personal assistant, predicting when you're about to leave for work and informing you that traffic will be heavy. Your digital camera includes geolocation coordinates in the metadata of the pictures you take. Call detail records, or CDRs, which can be subpoenaed from a cellular provider, also record the cell tower and sector utilized when a phone makes a call or SMS/MMS text message.

If the reliability of the navigation data is called into question or is, in fact, questionable, utilizing other forms of location from different devices can assist in the verification or dismissal of the evidence.

User Data

User data is where it gets interesting. When you connect your phone to a vehicle, it syncs much of the data contained on your phone onto the internal storage of the car itself. The result is that an examiner can collect mobile phone data without having the phone. The user data recoverable from vehicles includes messages, emails, social media content, call logs and application data, and the list continues to expand as time passes and technology advances.

Previously reserved only for luxury vehicles, infotainment systems are seen in almost every car produced. The widespread distribution of this technology and its rapid advancement create an environment of innovation and customer demand.

This demand is for cars to do more. Ever-increasing connectivity and functionality with a mobile phone, more conveniences, and more features require the infotainment system to record more information about you. For your car to do helpful things, it needs to know how to personalize the experience just for you. To do that means that it must collect as much information as

possible from your mobile phone and the interactions with the infotainment system itself. Of course, this leads to more digital evidence.

Looking Forward

Hyper-connectivity is the future with connected vehicles, smart devices, wearable technology, and even entire smart cities. This future means that more data than ever will be collected concerning our habits, location, activities, health, and financial information. Virtues and vices will be stored electronically, and when that data is collected and stored, it can often be recovered using forensic tools and methodology.

Not only will more devices will talk to each other. We are not far off from a world whereby everything talks to everything. This is apparent if we look at the relationship between wearable technology and phones. Ultimately, we will see biometric data, sleep patterns, markers of healthiness and disease, physical activity, and heart rate contained in the infotainment data. If that sounds far-fetched, consider the following scenario, which happens every day. First, you sync your fitness watch to your phone. Then you connect your phone to your car, which syncs your phone data to the infotainment system. It would now be possible for biometric data collected from your fitness watch to be contained in the infotainment system of your car. It's a brave new world.

END

[1] TIBCO Software. The connected car: finding the intersection of opportunity and consumer demand. Palo Alto (CA): 2016

ENVISTA FORENSICS

LARRY DANIEL
TECHNICAL DIRECTOR– DIGITAL FORENSICS

CHALLENGING DIGITAL SURVEILLANCE

DIGITAL FORENSICS //

My Team

Lab Locations

Dallas TX,

Columbia, SC

Raleigh, NC

Richmond, VA

Larry Daniel
TECHNICAL DIRECTOR
DIGITAL FORENSICS
Raleigh, NC

Lars Daniel
PRACTICE LEADER
DIGITAL FORENSICS
Raleigh, NC

Eric Grabski
DIGITAL FORENSICS ANALYST
DIGITAL FORENSICS
Raleigh, NC

Kyle Richards
DIGITAL FORENSICS ANALYST
DIGITAL FORENSICS
Richmond, VA

Josh Lorencz
DIGITAL FORENSICS EXAMINER
DIGITAL FORENSICS
Dallas, TX

Spencer McInvaille
DIGITAL FORENSICS EXAMINER
Raleigh, NC

Jake Green
SENIOR DIGITAL FORENSICS
EXAMINER
Raleigh, NC

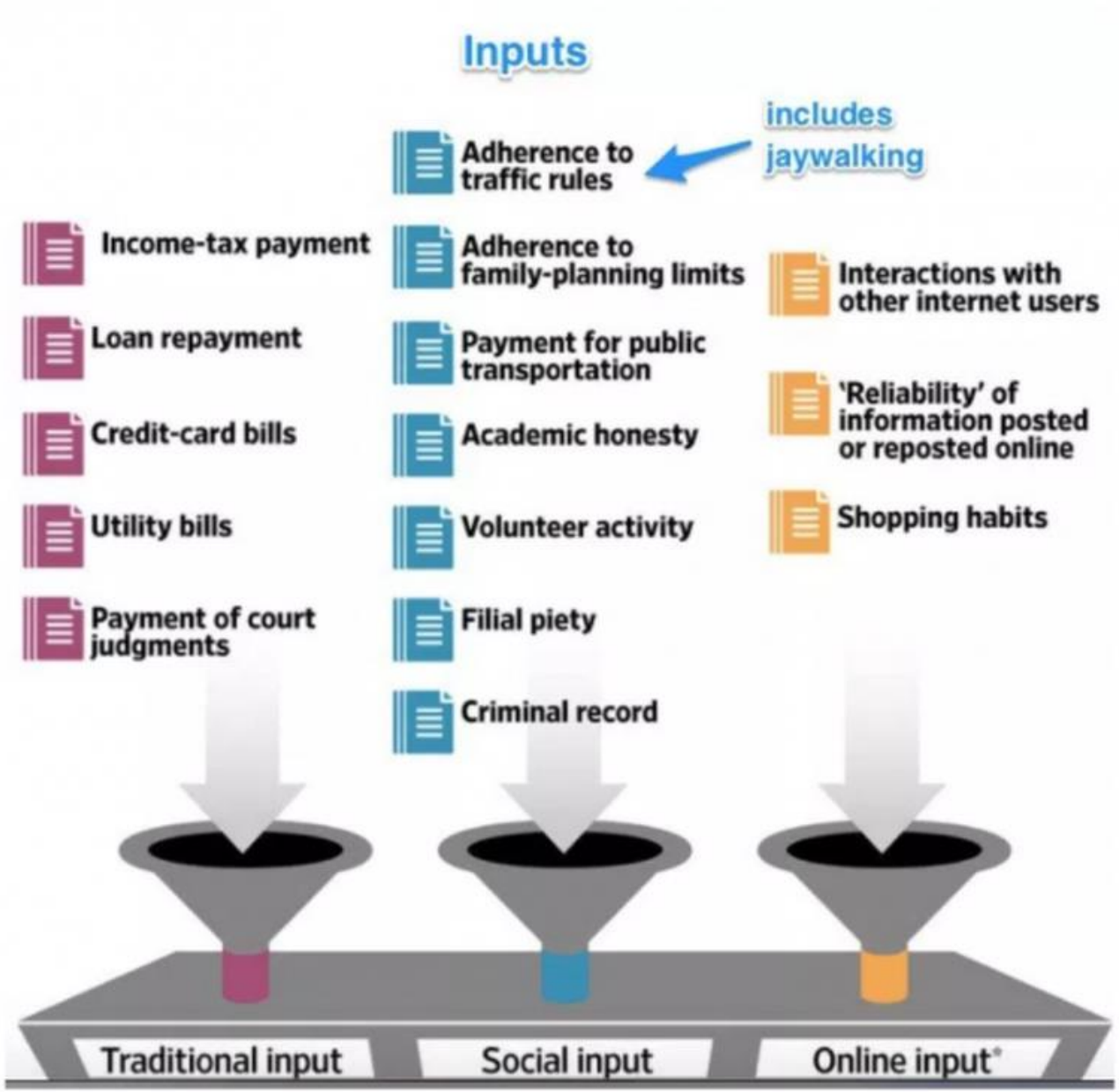
Justin Ussery
DIGITAL FORENSICS EXAMINER
Dallas, TX

Chinese Social Credit System

https://www.zerohedge.com/news/2018-05-24/chinas-terrifying-social-credit-system-has-already-blocked-11-million-taking

Chinese Social Credit System

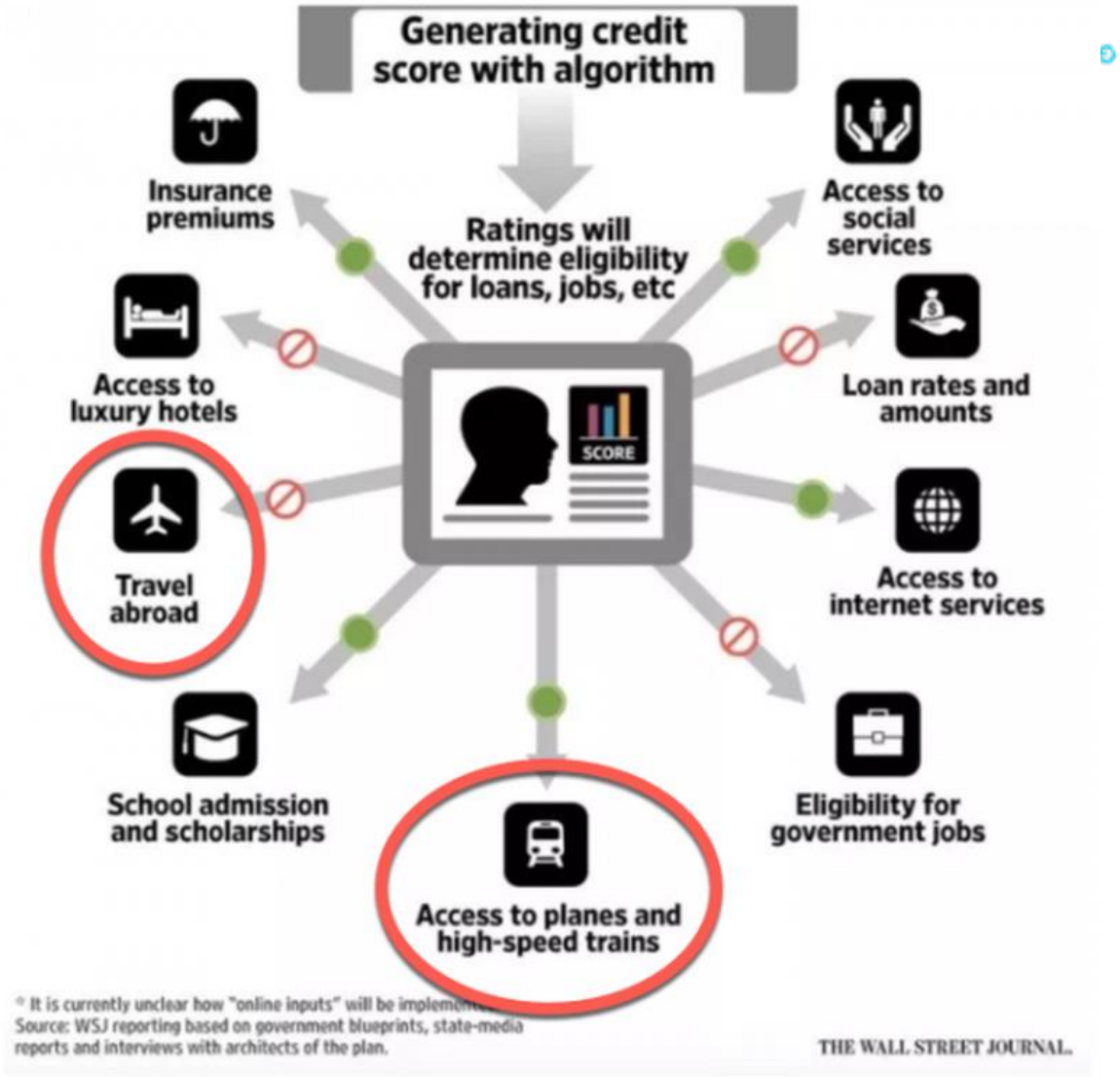
- Inputs
  - Traditional
  - Social
  - Online



https://www.zerohedge.com/news/2018-05-24/chinas-terrifying-social-credit-system-has-already-blocked-11-million-taking

Chinese Social Credit System

- Banning you from flying or getting the train
- Throttling your internet speeds
- Banning you, or your kids, from the best school
- Stopping you getting the best jobs
- Keeping you out of the best hotels
- Getting your dog taken away
- Being publicly named as a bad citizen
- Unable to secure loans, credit cards, financial assistance



https://www.zerohedge.com/news/2018-05-24/chinas-terrifying-social-credit-system-has-already-blocked-11-million-taking

Chinese Social Credit System

- Facial Recognition
  - As of 2019, it is estimated that 200 million monitoring CCTV cameras of the "Skynet" system have been put to use in mainland China, four times the number of surveillance cameras in the United States. By 2021, the number of surveillance cameras in mainland China is expected to reach 570 [illegible]

https://medium.com/@ivonne.teoh/chinas-tech-companies-help-government-to-set-up-social-credit-system-by-2020-ebbd96bc0b06

Chinese Social Credit System

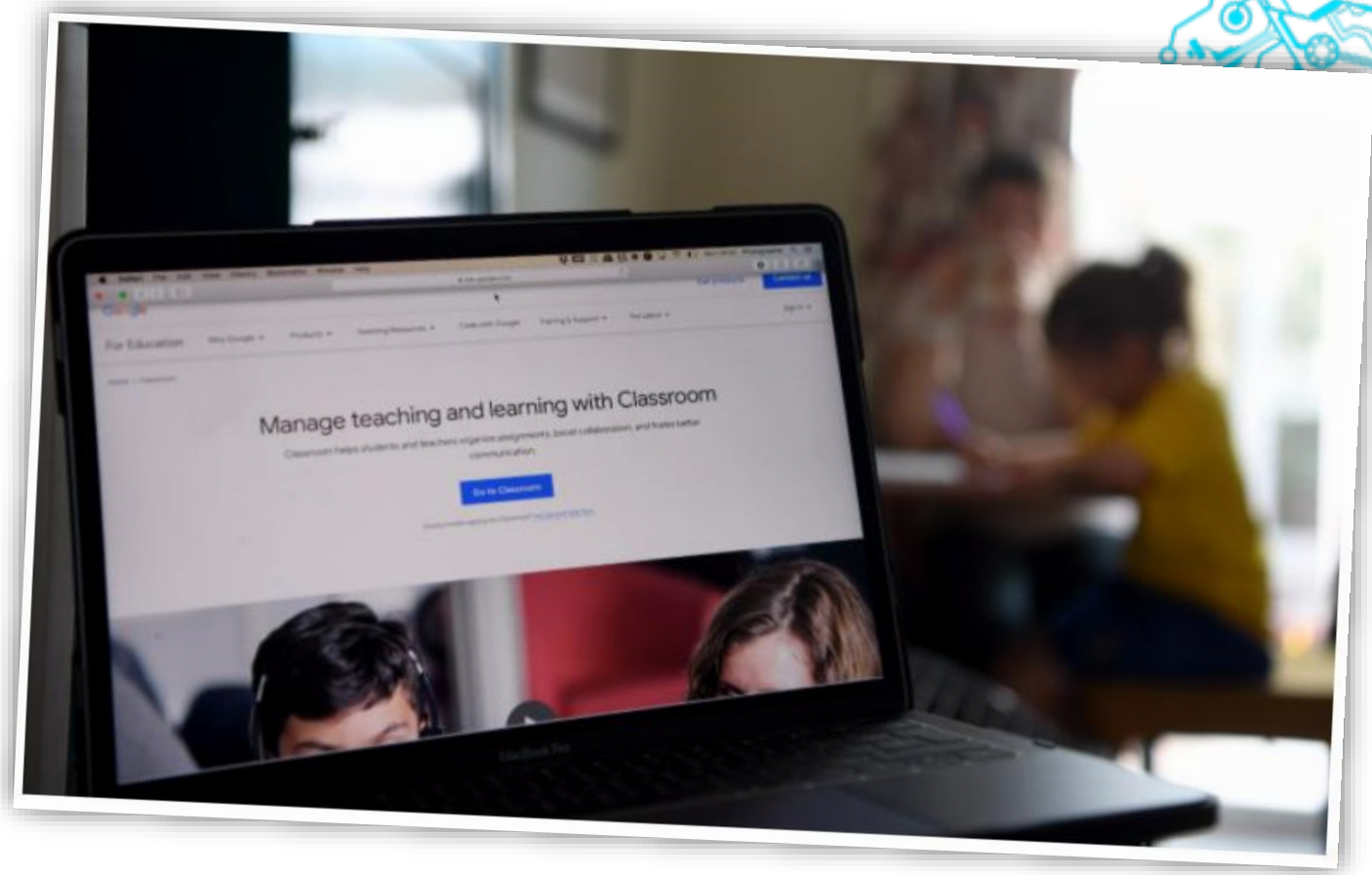
• Facial Recognition

- Every movement of pupils at Hangzhou Number 11 High School in eastern China is watched by three cameras positioned above the blackboard.The "smart classroom behaviour management system," or "smart eye", is the latest highly-intrusive surveillance equipment to be rolled out in China, where leaders have rushed to use the latest technology to monitor the wider population…The computer will pick up seven different emotions, including neutral, happy, sad, disappointed, angry, scared and surprised.

https://www.telegraph.co.uk/news/2018/05/17/chinese-school-uses-facial-recognition-monitor-student-attention/

Google in the Classroom

- Facial Recognition
  - Google is using its services to create face templates and "voiceprints" of children, the complaint says, through a program in which the search giant provides school districts across the country with Chromebooks and free access to G Suite for Education apps. Those apps include student versions of Gmail, Calendar and Google Docs.



https://www.cnet.com/news/two-children-sue-google-for-allegedly-collecting-students-biometric-data/

Chinese Social Credit System

- Facial Recognition
- "Officers wear augmented-reality smart glasses that recognize facial features and license plates in near real time checking them against a database of subjects"

EUTERS/Thomas Peter

https://www.businessinsider.com/china-police-using-smart-glasses-facial-recognition-2018-3

Lower Manhattan

- **Facial Recognition**

  The **Domain Awareness System** is a surveillance system developed as part of Lower Manhattan Security Initiative in a partnership between the New York Police Department and Microsoft to monitor New York City. This allows them to track surveillance targets and gain detailed information about them. The system is connected to 6,000 video cameras around New York City.

https://www.cityandstateny.com/articles/opinion/commentary/new-york-should-regulate-law-enforcement-use-of-facial-recognition
https://en.wikipedia.org/wiki/Domain_Awareness_System

Facebook

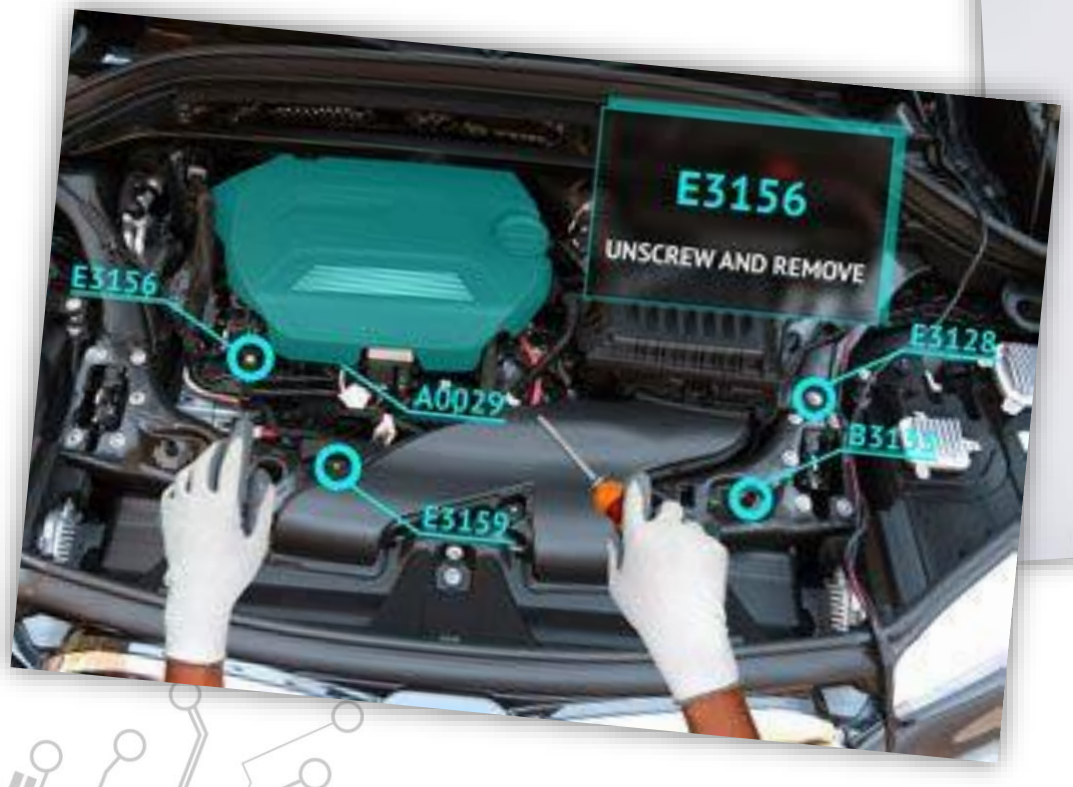
- Facial Recognition
  - A judge has approved what he called one of the largest-ever settlements of a privacy lawsuit, giving a thumbs-up Friday to Facebook paying $650 million to users who alleged the company created and stored scans of their faces without permission.
  - "Biometrics is one of the two primary battlegrounds, along with geolocation, that will define our privacy rights for the next generation," Attorney Jay Edelson, who filed the lawsuit, said in January of 2020.

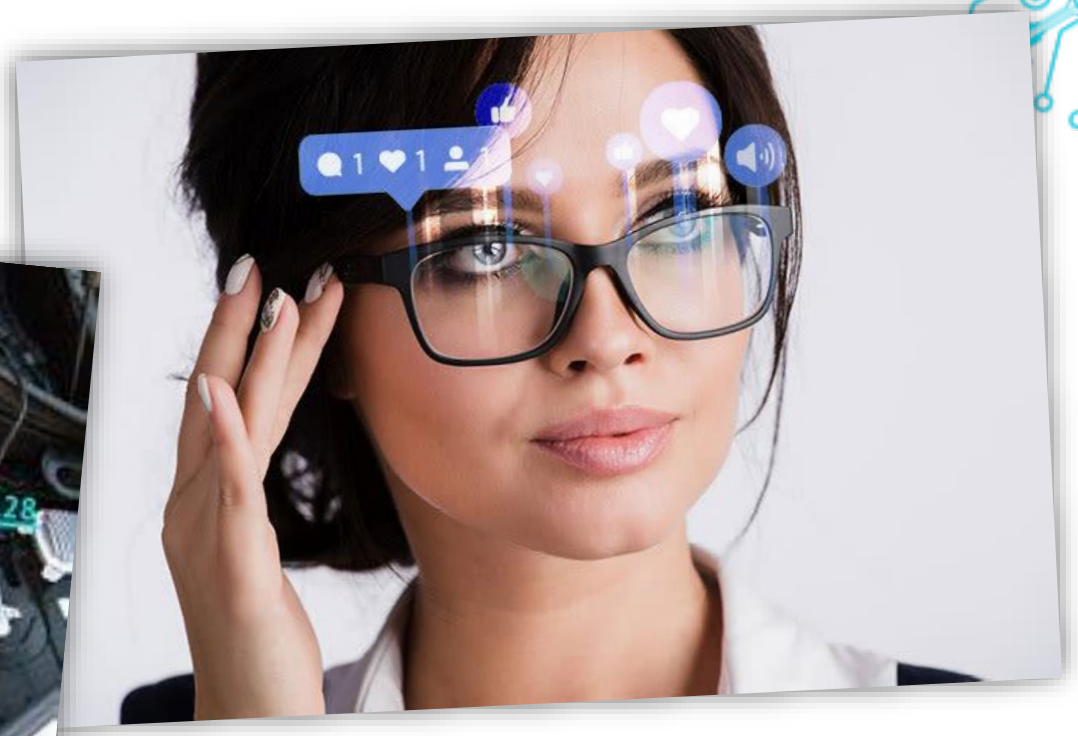
Facebook CEO Mark Zuckerberg.
James Martin/CNET

https://www.cnet.com/news/facebook-privacy-lawsuit-over-facial-recognition-leads-to-650m-settlement/

Facebook: Smart Glasses

- Facial Recognition…?
  - Augmented Reality





https://www.allaboutvision.com/eyeglasses/smart-glasses/

Sony

- Facial Recognition
  - In order to mimic the behavior of an actual pet, an Aibo device will learn to behave differently around familiar people. To enable this recognition, Aibo conducts a facial analysis of those it observes through its cameras. This facial-recognition data may constitute "biometric information" under the law of Illinois, which places specific obligations on parties collecting biometric information. Thus, we decided to prohibit purchase and use of Aibo by residents of Illinois.

https://www.cnet.com/home/security/what-sonys-robot-dog-teaches-us-about-biometric-data-privacy/

Facial Recognition

- Facial Recognition
  - Facial recognition software essentially treats everyone as a suspect. More than 20 states allow federal law enforcement to search state databases of driver's license photos
  - In 2017, a British journalist tested the system in Guiyang, a massive metropolis. The reporter provided police his photograph, then began walking the city streets to see how long he could elude capture. Chinese police surrounded the journalist after just seven minutes.

- https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/
- https://techcrunch.com/2017/12/13/china-cctv-bbc-reporter/

Chinese Social Credit System

- Surveillance Drones
- Over recent years, more than 30 Chinese military and government agencies have reportedly been using drones made to look like birds to surveil citizens in at least five provinces, according to the South China Morning Post. The program is reportedly codenamed "Dove" and run by Song Bifeng, a professor at Northwestern Polytechnical University in Xi'an. Song was formerly a senior scientist on the Chengdu J-20, Asia's first fifth-generation stealth fighter jet, according to the Post.The bird-like drones mimic the flapping wings of a real bird using a pair of crank-rockers driven by an electric motor. Each drone has a high-definition camera, GPS antenna, flight control system and a data link with satellite communication capability, the Post reports.

https://www.cnet.com/news/china-launches-high-tech-bird-drones-to-watch-over-its-citizens/?fbclid=IwAR3LwxkR81A99QKa72t4Cx1gGq3QBIShvEA0bPGmc0muCn9f4myPNGpHHHE

ALPRs (Automatic License Plate Readers)

- ALPRs
  - ALPRs can be mounted on police cruisers or placed in one location. They record license plates' physical locations.
  - Manufacturers – ALPRs spot stolen cars or determine whether the registered owner of a vehicle is a fugitive. They're the equivalent of police running every plate they see through a crime database.
- 2019
  - California's state auditor found that ALPRs captured some 320 million images of license plates, none of which aroused any suspicion of a crime. The agencies gathering the information enforced no privacy or data retention policies. With little in the way of safeguards, ALPRs could have a chilling effect on citizens' decisions to attend, for example, political events or religious services.

Photos by Mike Katz-Lacabe (CC BY)

https://www.eff.org/pages/automated-license-plate-readers-alpr

Chinese Social Credit System

- Data Collection
  - The Chinese government aims at assessing the trustworthiness and compliance of each person. Data stems both from peoples' own accounts, as well as their network's activities. Website operators can mine the traces of data that users exchange with websites and derive a full social profile, including location, friends, health records, insurance, private messages, financial position, gaming duration, smart home statistics, preferred newspapers, shopping history, and dating behavior.
- Algorithms
  - Automated algorithms are used to structure the collected data, based on government rules

https://en.wikipedia.org/wiki/Social_Credit_System

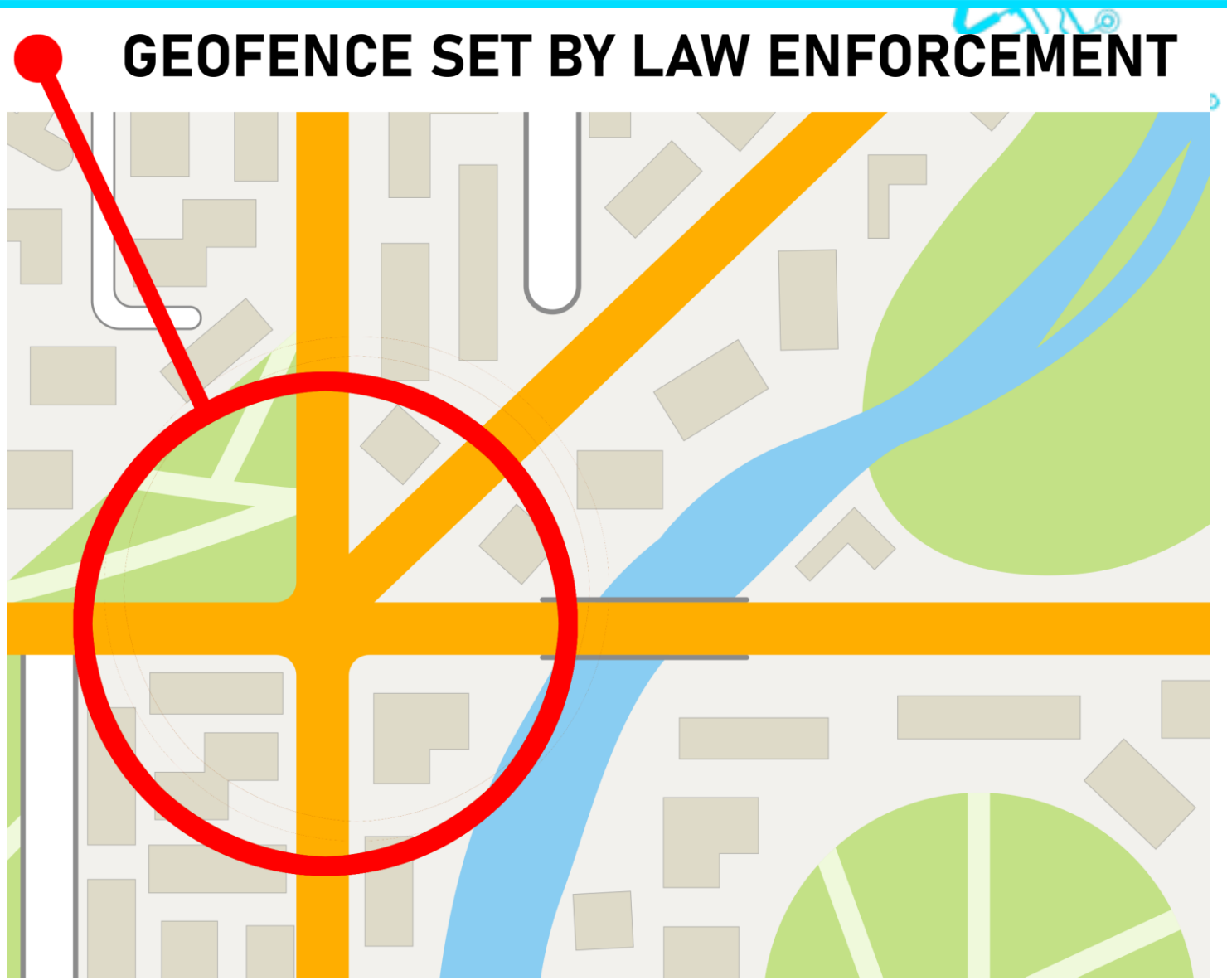
Data Collection in the USA

- Data Collection
  - License Plate Databases
    - License plate records and geo-tagged photos
  - Credit Reporting Agencies
    - Collect sensitive data and sell it to banks, creditors, insurers…
  - Smartphone Location Tracking
    - Extremely precise, allows for real time traffic, location busyness…
      - Google tells you how busy the gym or restaurant is at a particular time
  - Digital Ads/Purchases
    - Location data sold to retailers (online and brick and mortar) to generate targeted ads.
  - Smart Home Objects
    - iRobot Roomba mapping your home

https://en.wikipedia.org/wiki/Social_Credit_System

Location Data: Google GeoFence (GeoFence Warrant)

- GeoFence Warrant



Location Data: Google GeoFence (GeoFence Warrant)

1. LAW ENFORCEMENT DETERMINES THE COVERAGE AND TIMEFRAME OF INTEREST FOR THE GEOFENCE

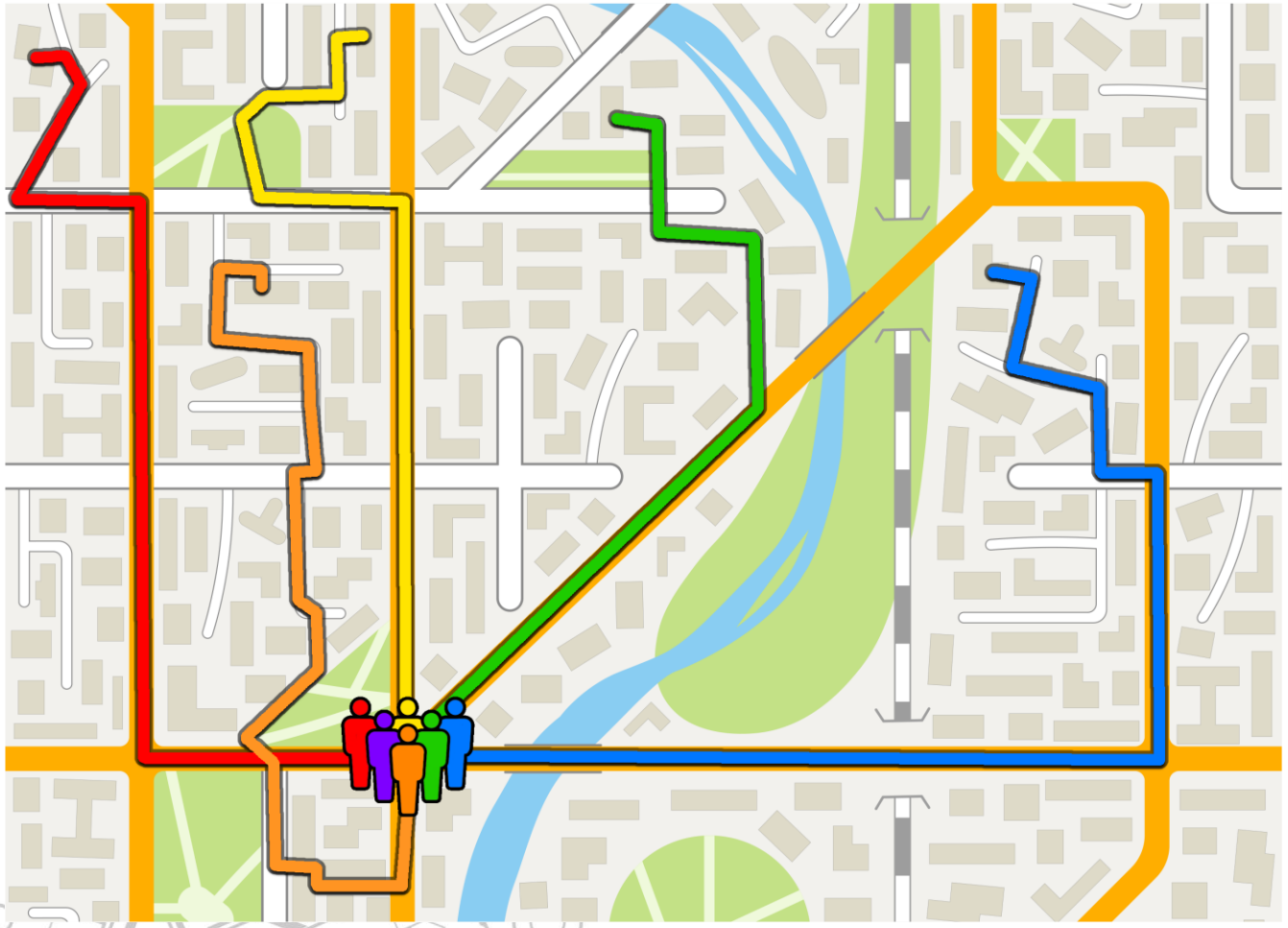
2. EVERY SINGLE GOOGLE ACCOUNT WITH LOCATION HISTORY IN THE WORLD IS SEARCHED

3. GEOFENCE IS POPULATED WITH EVERY PERSON IN THE AREA FOR THE DESIGNATED PERIOD

4. LAW ENFORCEMENT SELECTS SUSPECTS. THEY CAN NOW SEE THEIR ACTIVITY WITH NO GEOGRAPHIC LIMITS. (STEP 2)

Location Data: Google GeoFence (GeoFence Warrant)

GEOFENCE IS REMOVED, ALL LOCATON ACTIVITY CAN NOW BE SEEN FOR THOSE PEOPLE LAW ENFORCEMENT HAS SELECTED



Location Data: Google GeoFence (GeoFence Warrant)

ENVISTA FORENSICS

1. LAW ENFORCEMENT REQUESTS THAT GOOGLE REVEAL THE SUBSCRIBER INFORMATON OF SELECTED STEP 2 PERSONS OF INTEREST

2. GOOGLE PROVIDES THE SUBSCRIBER INFORMATION FOR THOSE LAW ENFORCEMENT HAS DESIGNATED AS PERSONS OF INTEREST

3. SUBSCRIBER INFORMATON INCLUDES THE USER'S ACCOUNT, EMAIL, PHONE NUMBERS, INTERNET PROTOCOL LOGS, AND OTHER DATA

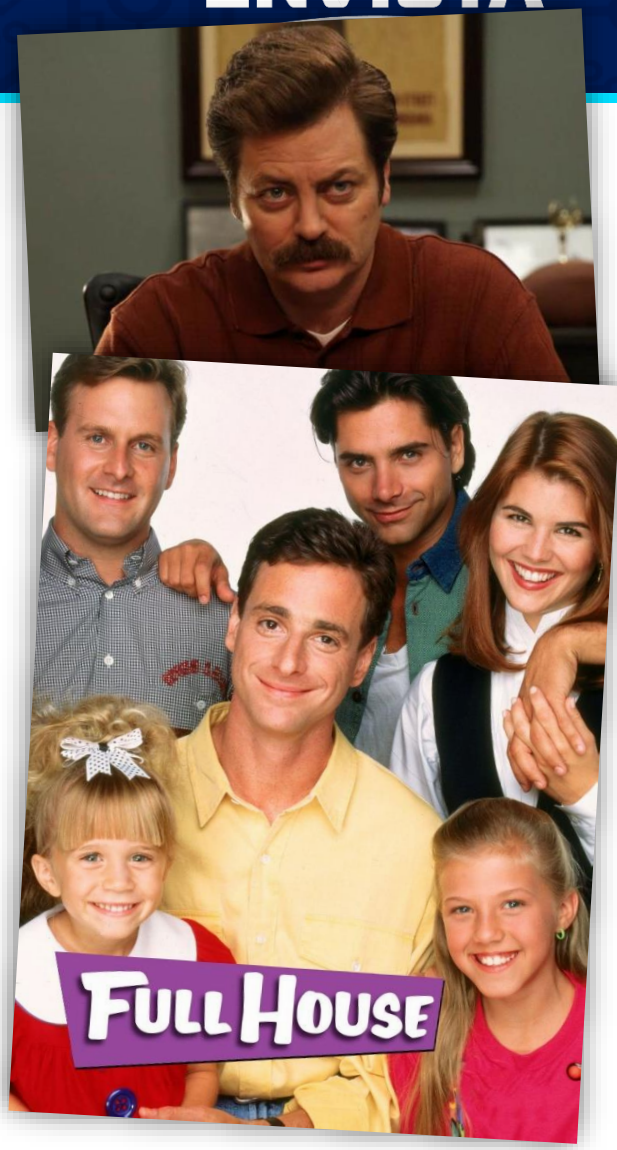
Chinese Social Credit System

- For example, buying something like diapers is seen as “responsible” and will improve your score, while things like video games are seen as idle and irresponsible and will bring your score down.
- your score also goes up or down based on interaction with friends who have a higher or lower score than you. Meaning, if a friend is given a low score and therefore deemed “less trustworthy,” you would be urged to spend less time with that person…(by Gov’t)

humancreativecontent.com/news-and-politics/2016/3/8/sypxe6b7dm2o8by6m4cwz1bh2kcszl

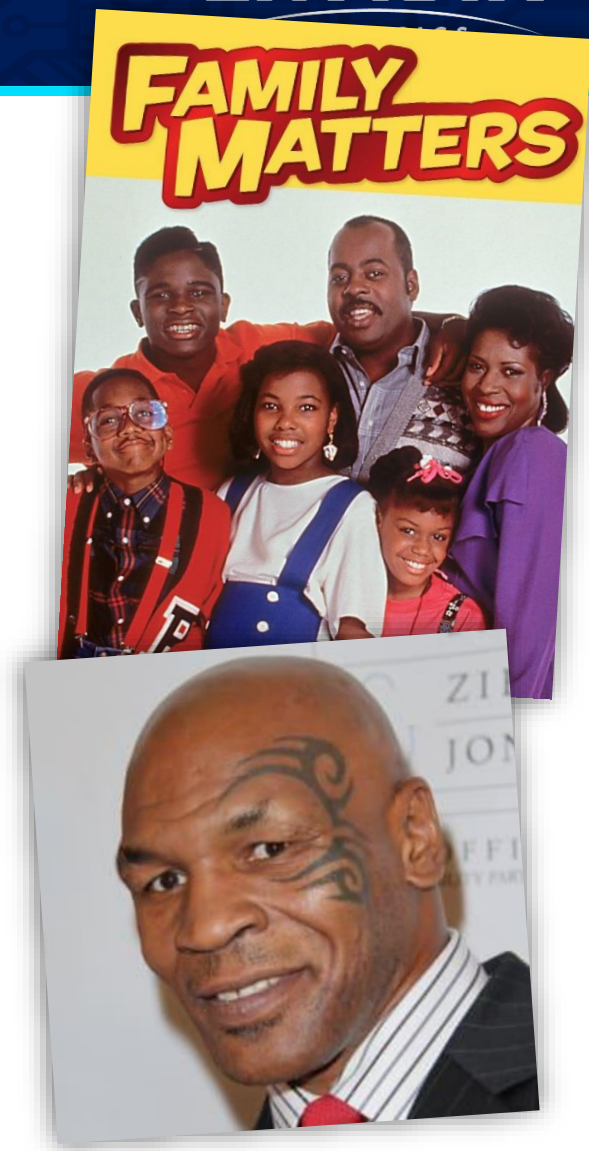
What determines the “truth” of content?

- Deepfake Videos – Nick Offerman



Will sharing this lower your score?

- Deepfake Videos – Mike Tyson



The Fake News Problem – what about this?

ENVISTA FORENSICS

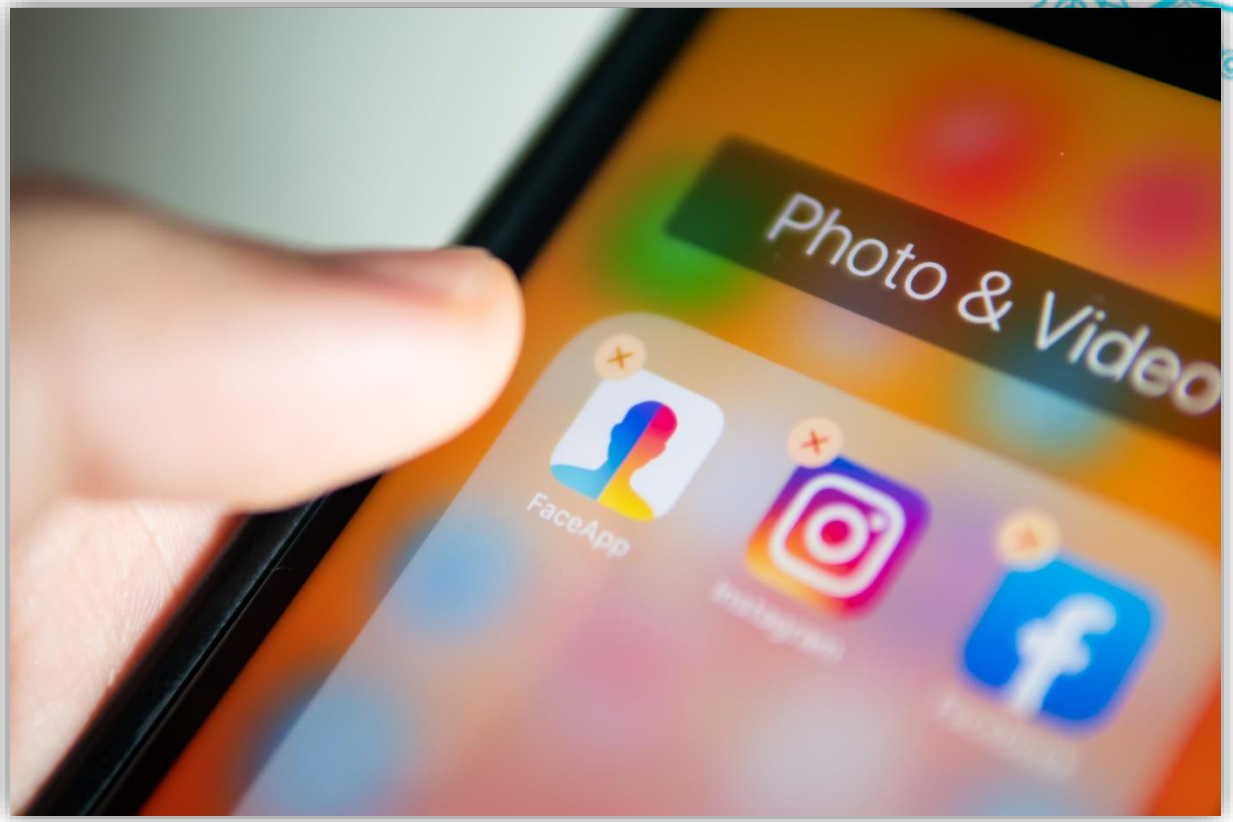
LARRY DANIEL
TECHNICAL DIRECTOR– DIGITAL FORENSICS

REALITY CAPTURE

DIGITAL FORENSICS //

Reality Capture

- New Territory
  - The ultimate social engineering
    - Virtual reality deepfakes




LOS ANGELES, CA
ONE WILSHIRE
nightline

ENVISTA FORENSICS

LARRY DANIEL
TECHNICAL DIRECTOR– DIGITAL FORENSICS

WHAT IS THE IOT?

INTERNET OF THINGS

DIGITAL FORENSICS //

Internet of Things (IoT)

- What is the Internet of Things?
  - 1980's
    - Carnegie Melon University
      - Programmers would connect via the internet to the Coke machine to see if a drink was available, and if it was cold.

> In the mid-seventies expansion of the department caused people's
> offices to be located ever further away from the main terminal room
> where the Coke machine stood. It got rather annoying to traipse down
> to the third floor only to find the machine empty - or worse, to shell
> out hard-earned cash to receive a recently loaded, still-warm Coke.
> One day a couple of people got together to devise a solution.
>
> They installed micro-switches in the Coke machine to sense how many
> bottles were present in each of its six columns of bottles. The
> switches were hooked up to CMUA, the PDP-10 that was then the main
> departmental computer. A server program was written to keep tabs on
> the Coke machine's state, including how long each bottle had been in
> the machine. When you ran the companion status inquiry program, you'd
> get a display that might look like this:
>
> EMPTY EMPTY 1h 3m
> COLD   COLD   1h 4m
>
> This let you know that cold Coke could be had by pressing the
> lower-left or lower-center button, while the bottom bottles in the two
> right-hand columns had been loaded an hour or so beforehand, so were
> still warm. (I think the display changed to just "COLD" after the
> bottle had been there 3 hours.)

https://www.cs.cmu.edu/~coke/history_long.txt

Internet of Things (IoT)

- What is the Internet of Things?
  - Any device with that is connected to the internet
  - Shared processing power
    - The **Internet of Things (IoT)** is the network of physical objects—devices, vehicles, buildings and other items embedded with electronics, software, sensors, and network connectivity—that enables these objects to collect and exchange data

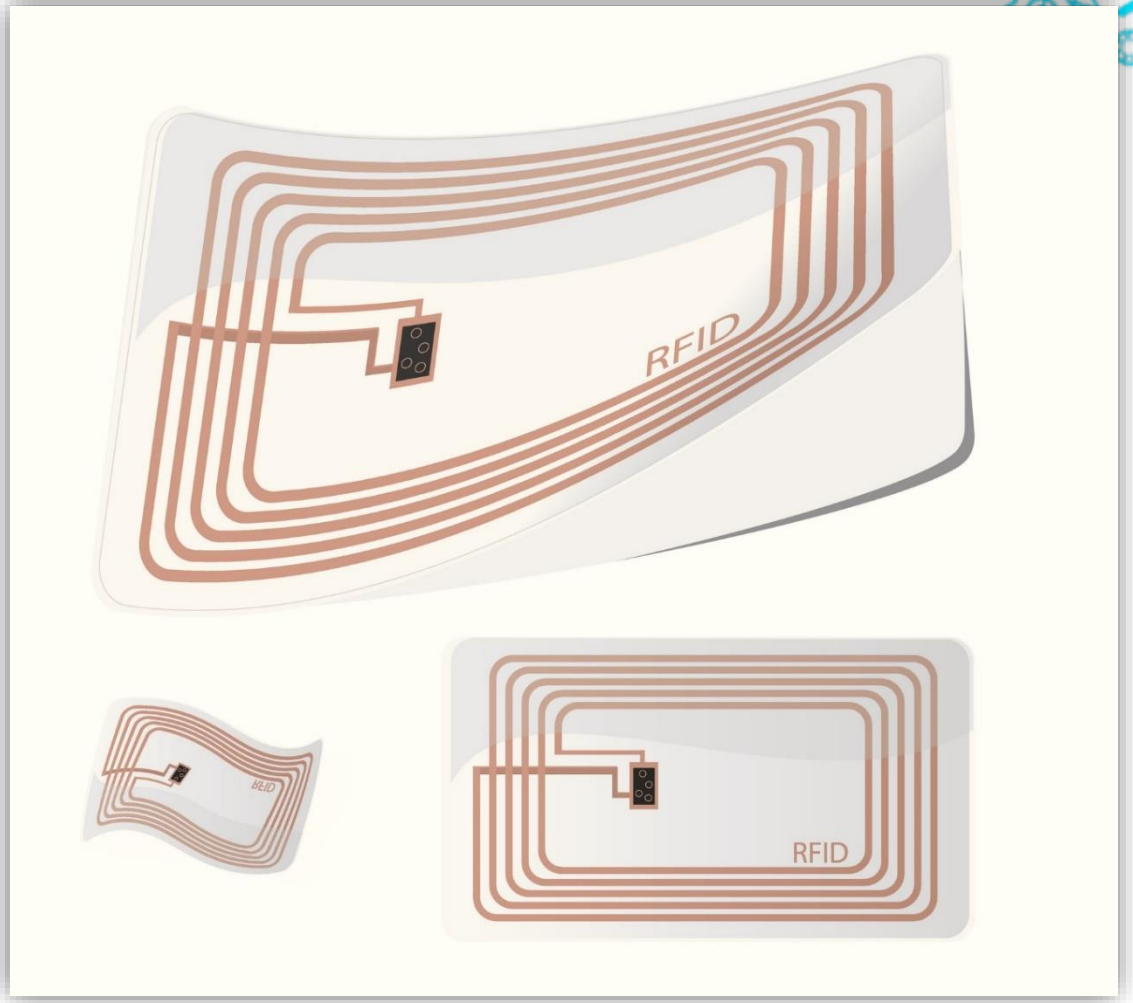
Petchatz.com

Internet of Things (IoT)

- Milestones
  - Barcode Reader
    - 1952
      - First ever built in a New York apartment by Norman Joseph and Bernard Silver
      - Ability to create and store data for retailers, shipping, inventory management…powerful when coupled with RFID

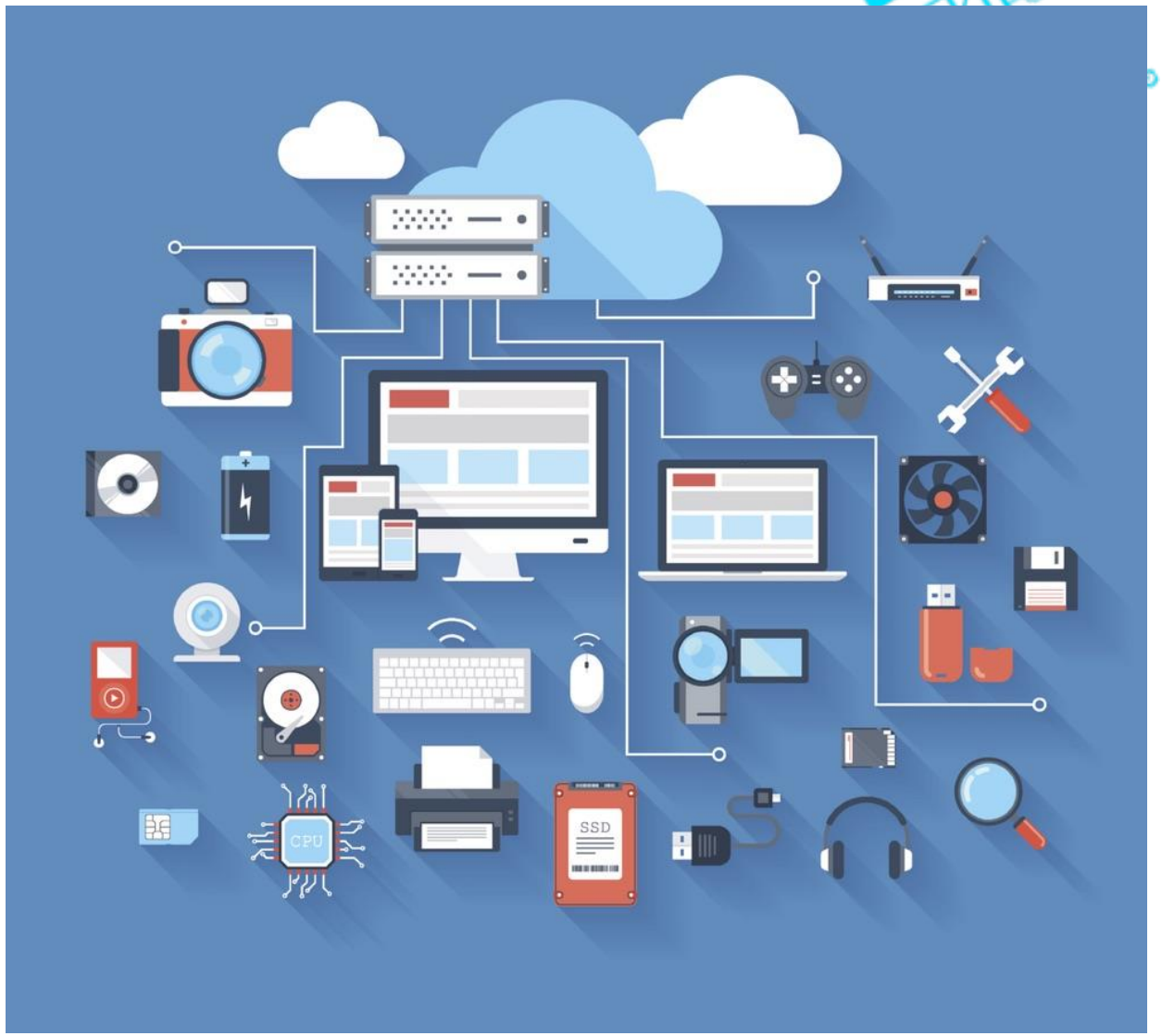
Internet of Things (IoT)

- Milestones
  - RFID
    - 1990's (becomes commonplace)
      - Automatic tracking without the need for a human to scan or capture data
      - Much more efficient that barcodes



Internet of Things (IoT)

- Milestones
  - Sensors
    - Everything talks to everything
    - Stores and transmits data
    - Talks to RFID

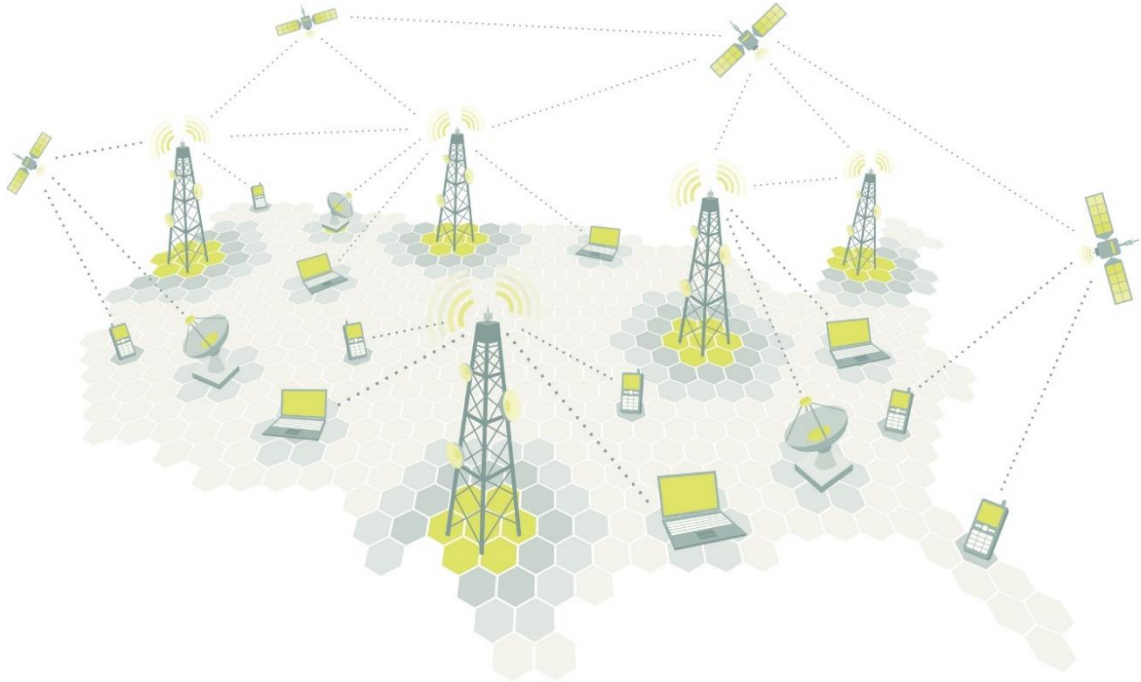


Internet of Things (IoT)

- Milestones
  - Big Data / Cloud
    - 2008-2009
      - According to Cisco Internet Business Solutions Group (IBSG), the Internet of Things was born in between 2008 and 2009 at simply the point in time when more “things or objects” were connected to the Internet than people.
    - 12.5 billion connected devices in 2010
  - Why is needed
    - Ability to store and transmit massive amounts of data generated by devices, sensors, websites, applications, etc.

Internet of Things (IoT)

- Cellular Network
  - Big Data / Cloud
    - Around 29 billion connected devices[1] are forecast by 2022, of which around 18 billion will be related to IoT
    - 90% of the world covered by cellular signal
    - 70% of wide-area IoT devices will use cellular technology in 2022
    - LTE and Beyond



https://www.ericsson.com/en/mobility-report/internet-of-things-forecast

ENVISTA FORENSICS

LARRY DANIEL
TECHNICAL DIRECTOR– DIGITAL FORENSICS

IOT DEVICES

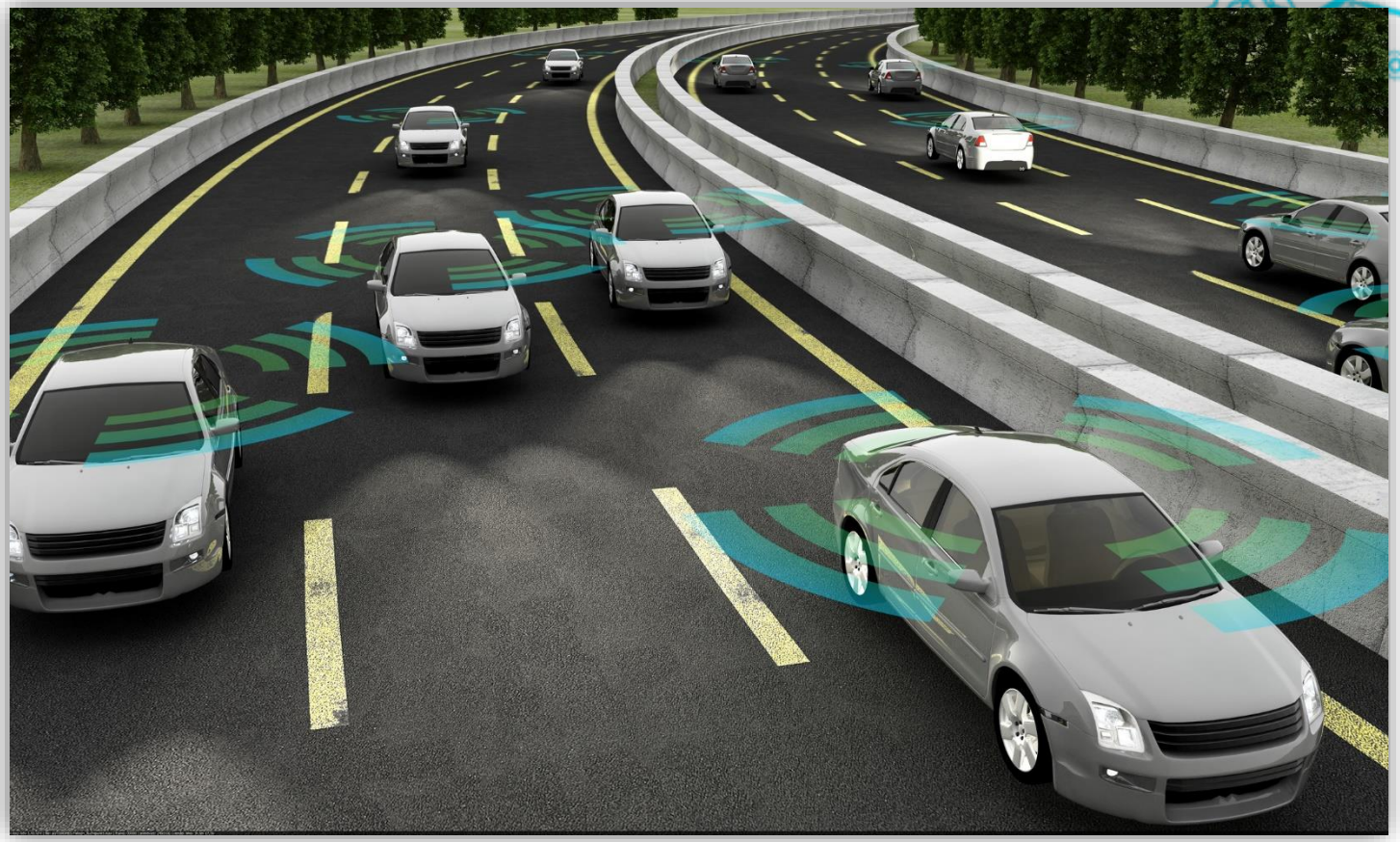
DIGITAL FORENSICS //

IoT Devices

- Always on devices
  - Always listening…?
  - Data collection
  - Data stored on local devices
    - Cell phones, computers
  - Data stored in the cloud
    - Association accounts

IoT Devices

- Vehicles
  - Cellular connection
  - Autonomous
  - Semi-autonomous
  - Video



IoT Devices

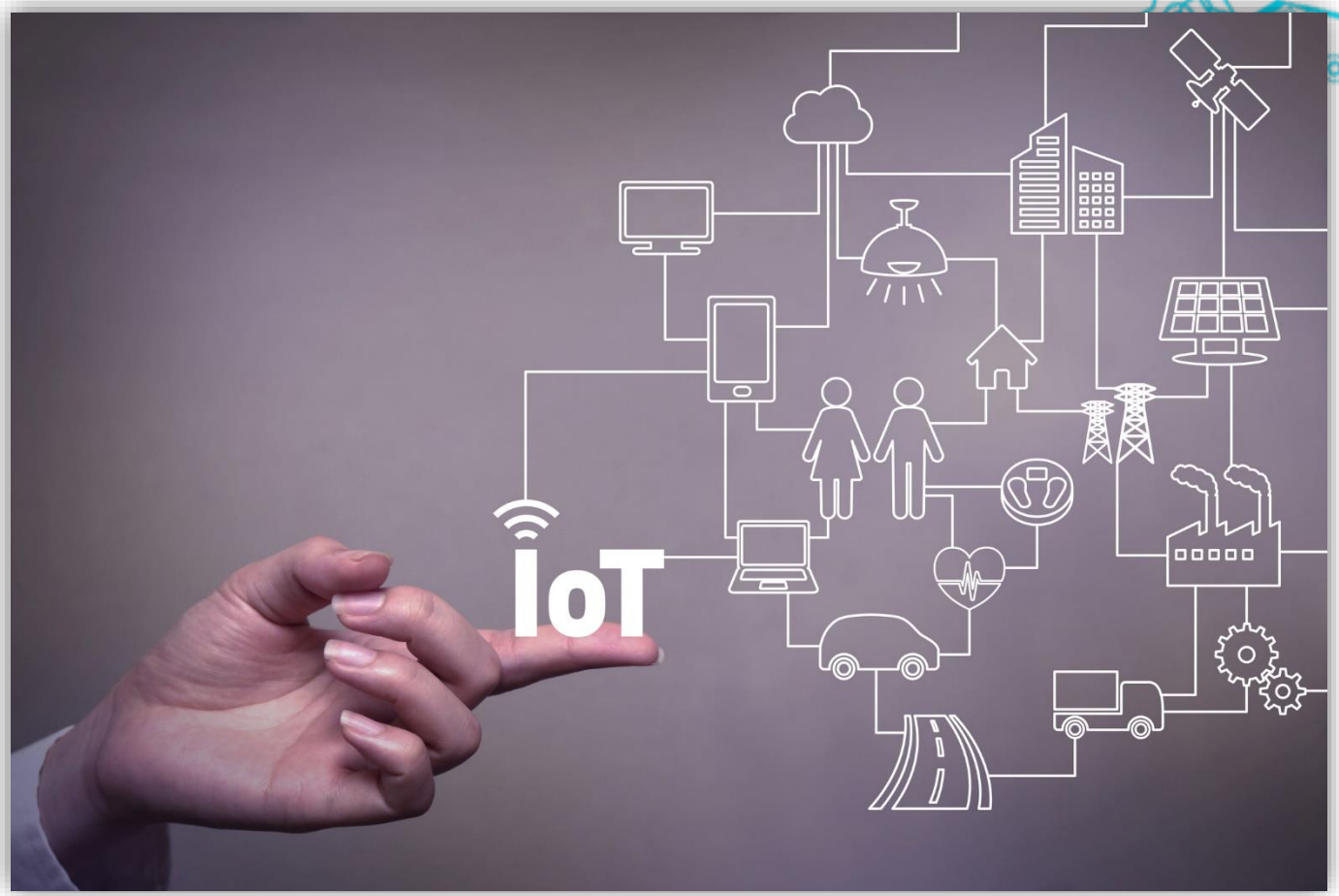
- Wearable technology
  - Beyond fitness!
  - Medical
    - Athletic performance, medical analytics
  - Logistics
    - People movement, animal movement
      - Livestock are one of the first uses of IoT, including tracking movement, fertility, behavior, lactation…
  - Government
    - Tracking, monitoring

Digital Forensics – Murder Cases

- Case Example
  - SODDI Defense
    - (Some Other Dude Did It)
      - Computer Forensics
      - Cell Phone Forensics
      - Cellular Location
      - Xbox Forensics
      - Alarm System Logs

Internet of Things (IoT)

- What the Future Holds
  - Hyper-connection is the future, and it is coming fast.



ENVISTA FORENSICS

LARRY DANIEL
TECHNICAL DIRECTOR– DIGITAL FORENSICS

IOT CYBER SECURITY

TODAY'S HACKING = TOMORROW'S EVIDENCE

DIGITAL FORENSICS //

IoT Security Risks

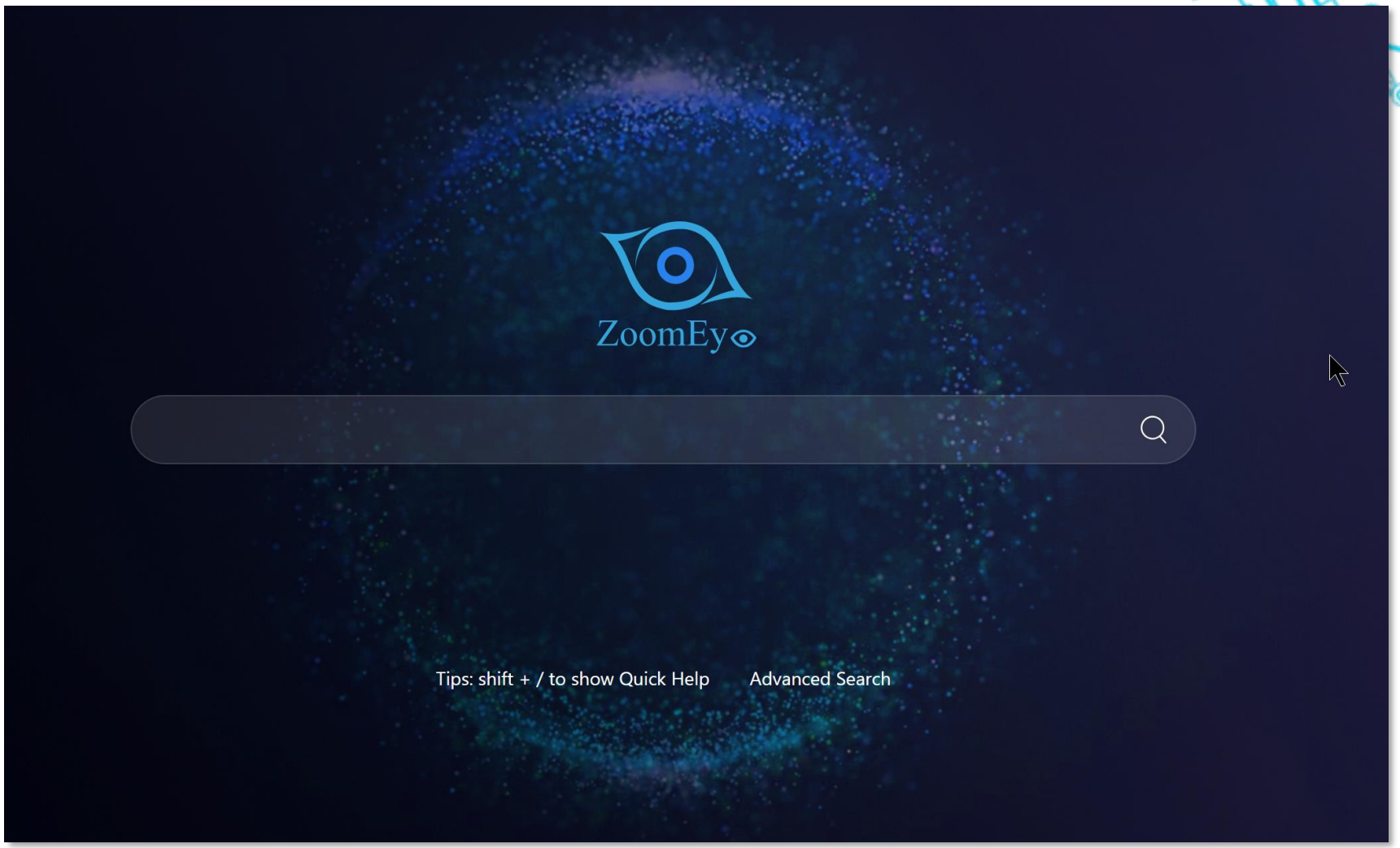
- Hacking
  - millions of insecure connected devices
  - Leaves critical systems and data around the world at risk

IoT Hacking Tools and Techniques

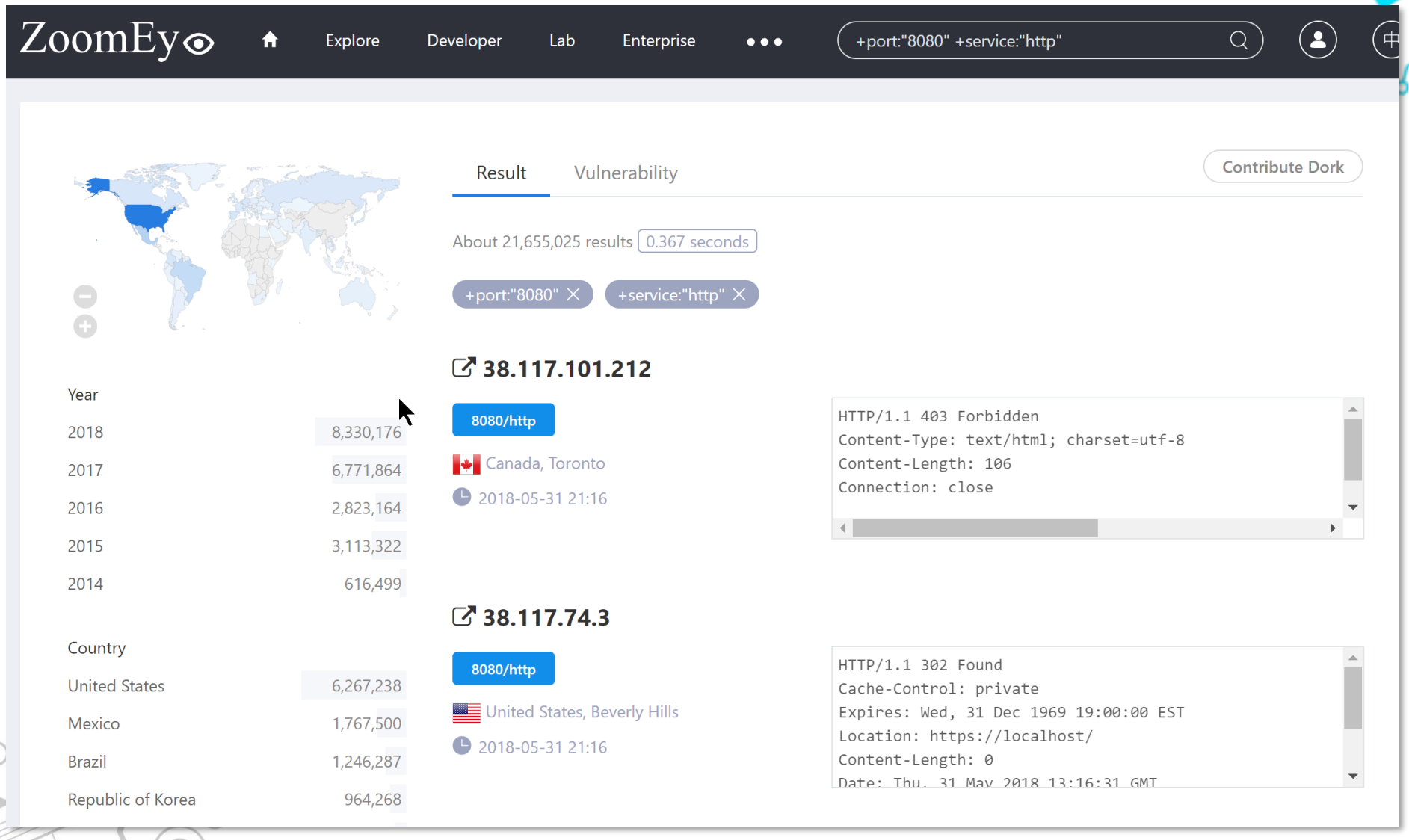
- Finding Attackable Hosts –
  - There are three difference search engines that scan for open ports and vulnerable services:
    - Censys.io
    - Zoomeye.org
    - Shodan.io

IoT Hacking Tools and Techniques

- Zoomeye.org

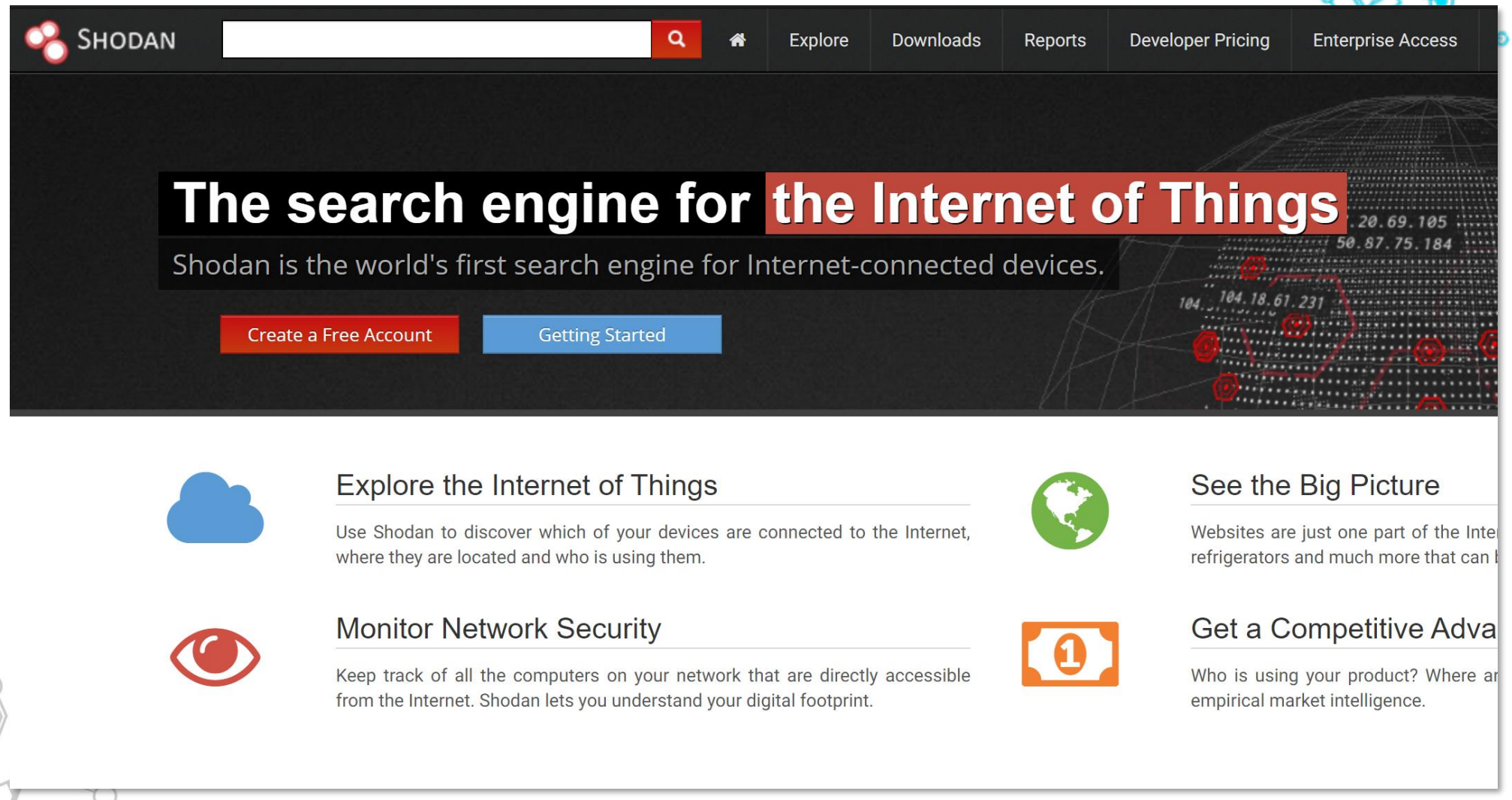


IoT Hacking Tools and Techniques



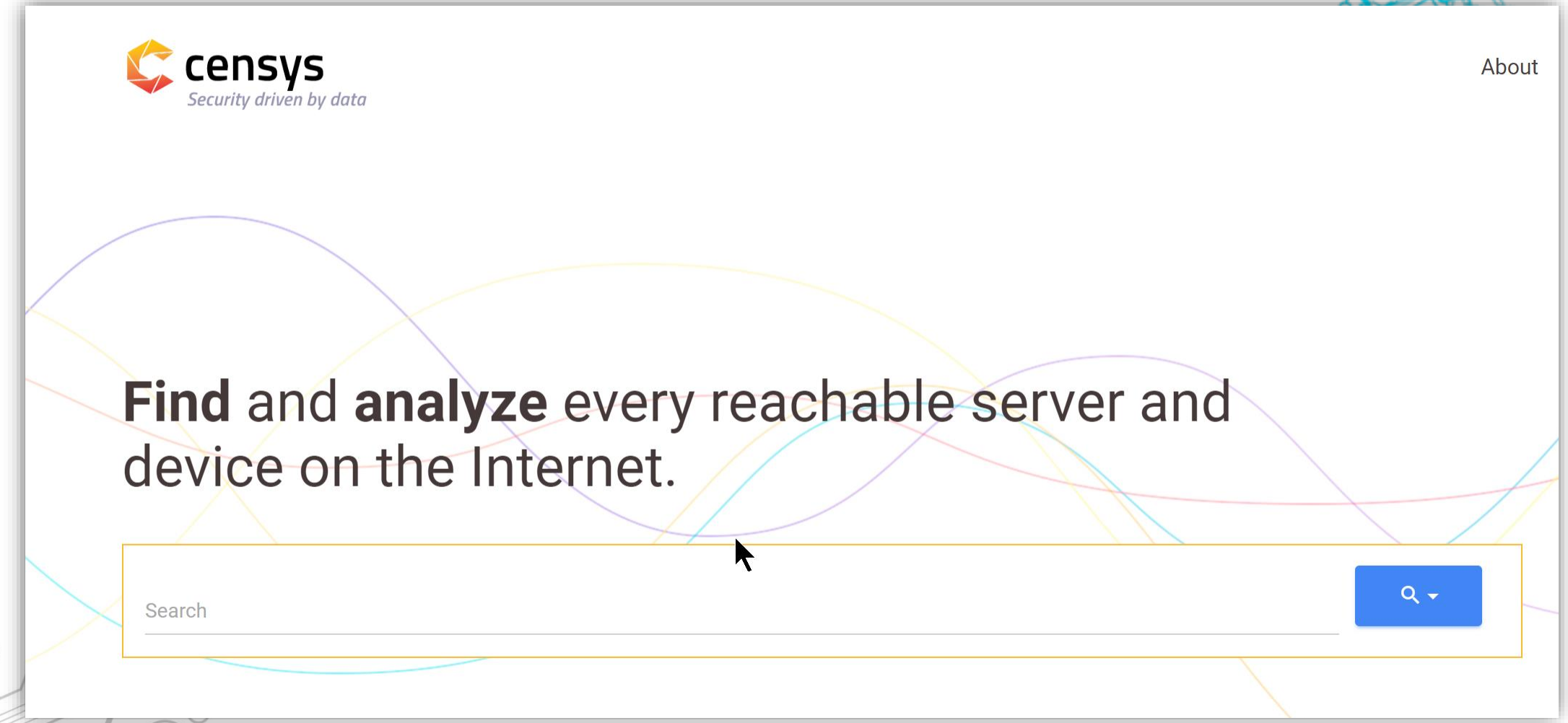
IoT Hacking Tools and Techniques

- Shodan.io

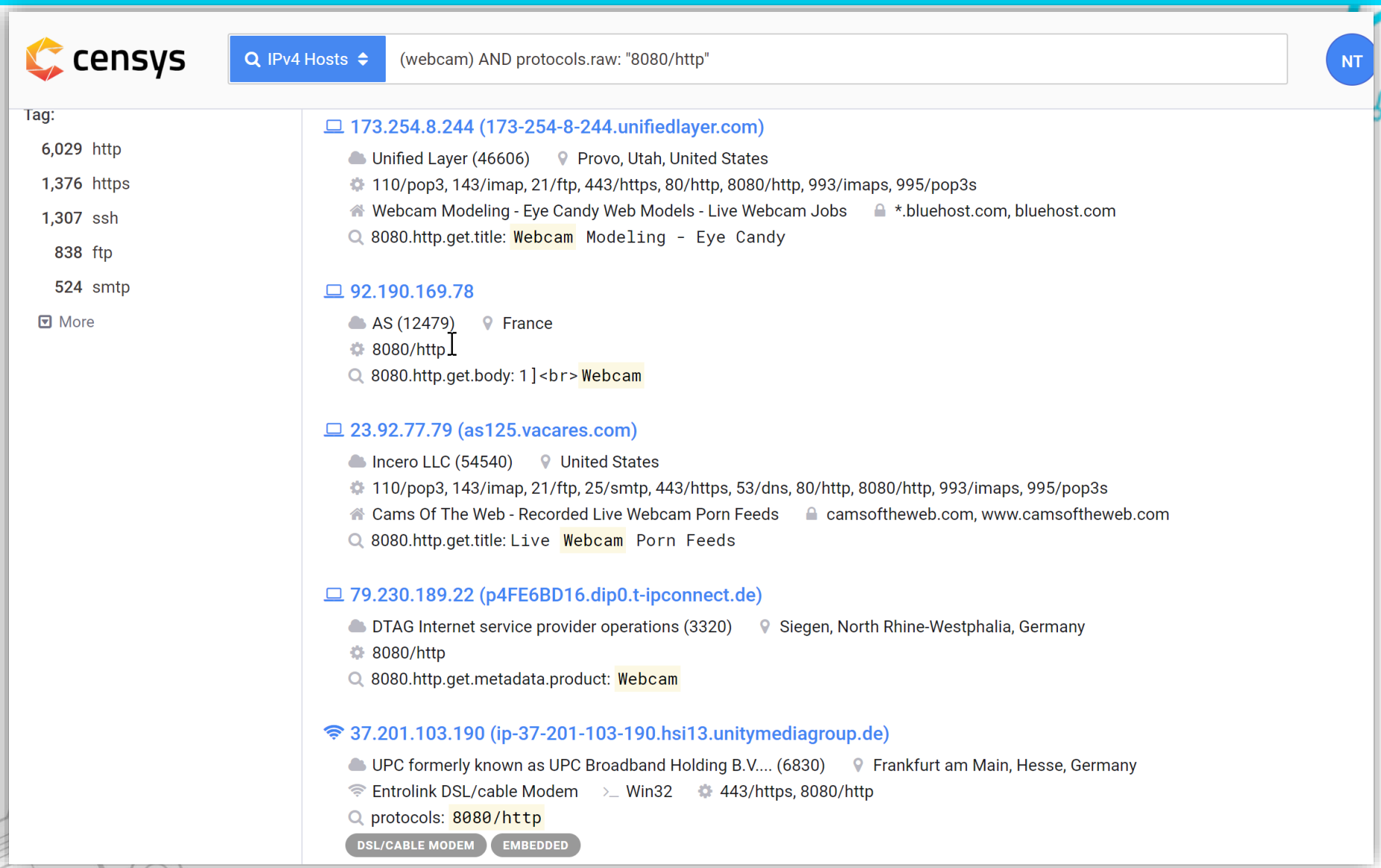


IoT Hacking Tools and Techniques

- Censys.io



IoT Hacking Tools and Techniques



IoT Hacking Tools and Techniques

- Live Webcam

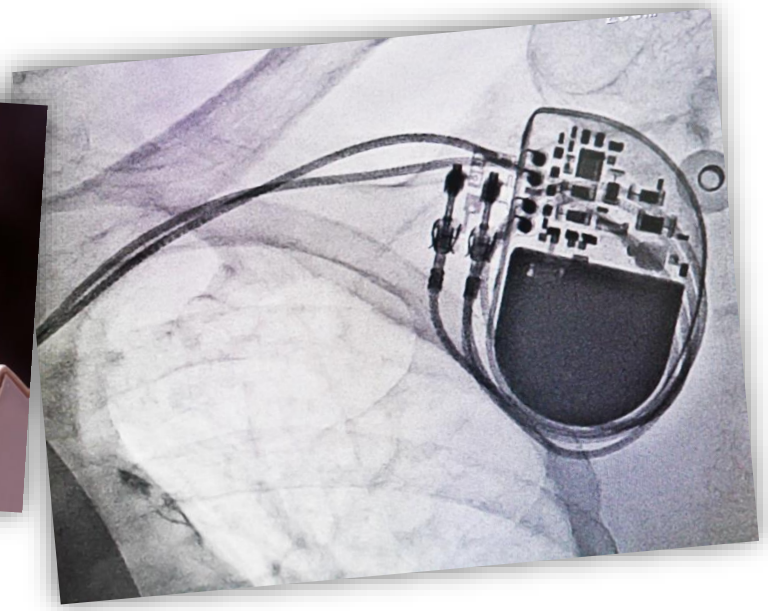
IoT Security Risks

- Hacking
  - Cardiac devices
    - Early this year, CNN wrote, "The FDA confirmed that St. Jude Medical's implantable cardiac devices have vulnerabilities that could allow a hacker to access a device. Once in, they could deplete the battery or administer incorrect pacing or shocks, the FDA said.
    - "The vulnerability occurred in the transmitter that reads the device's data and remotely shares it with physicians. The FDA said hackers could control a device by accessing its transmitter."

https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/

Who cares about Pacemaker data?

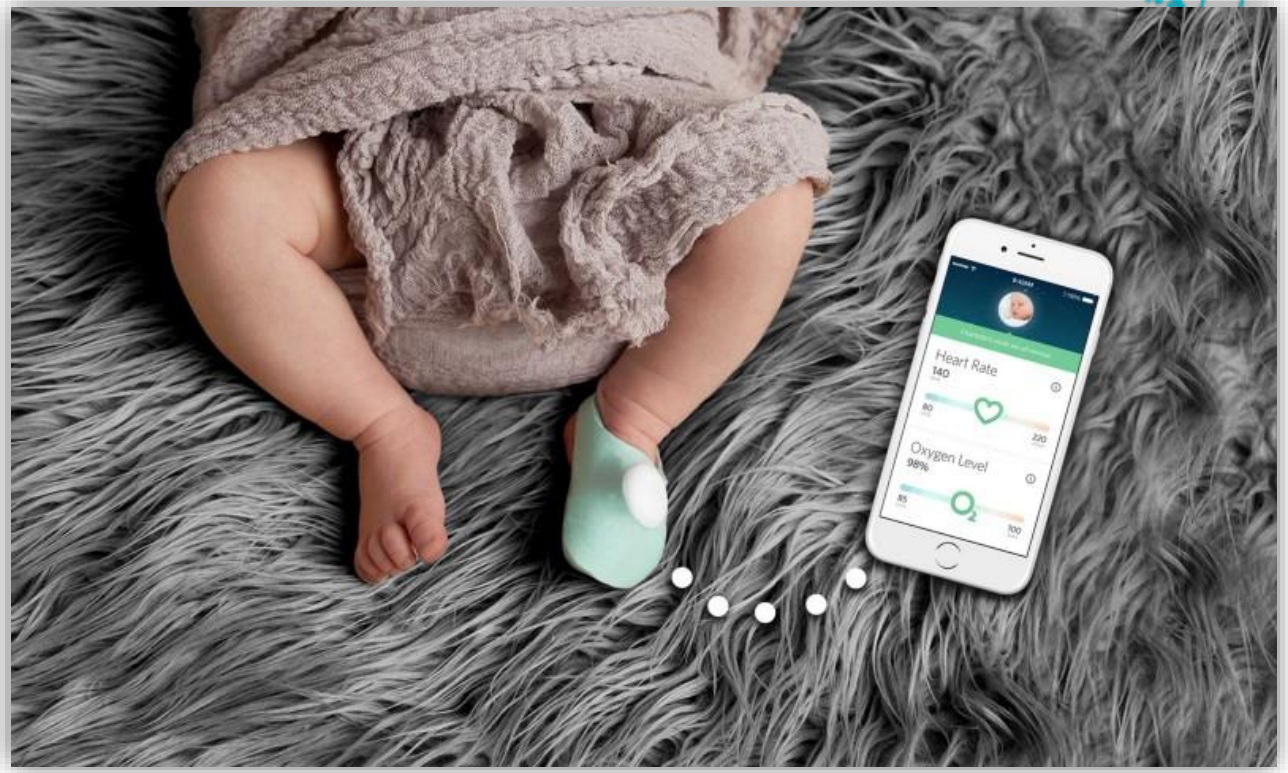
- Home arson case
  - **pacemaker**: In a home arson case, the homeowner told police that he did a number of things as soon as he discovered the fire: he gathered his belongings, packed them in a suitcase and other bags, broke out the bedroom window with his cane, threw his belongings outside, and rushed out of the house. The police searched the 59-year old's pacemaker. Its data showed that the man's heart rate barely changed during the fire. And after a cardiologist testified that it was "highly improbable" that a man in his condition could do the things claimed, the man was charged with arson and insurance fraud.



https://www.crowelldatalaw.com/2017/07/recent-iot-device-cases/

IoT Security Risks

- Hacking
  - Owlet Baby Monitor
    - Alerts parents if baby is having heart trouble
    - Hackers could cause false signals or cause device to stop reporting



https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/

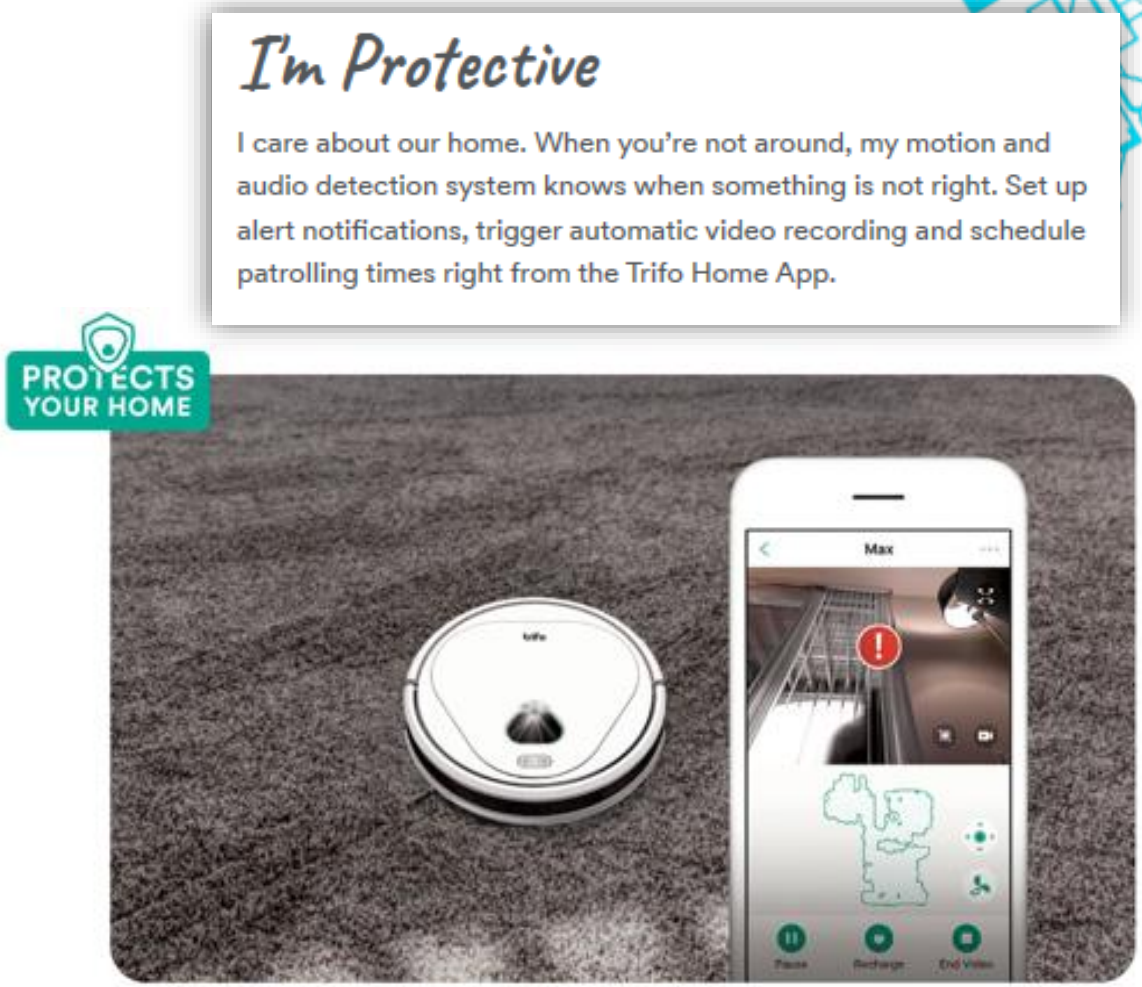
IoT Security Risks

- Hacking
  - TRENDnet Webcam Hack
    - TRENDnet transmitted user login credentials in clear, readable text over the Internet, and its mobile apps for the cameras stored consumers' login information in clear, readable text on their mobile devices, the FTC said.
    - Allowed hackers to watch the video feed from the camera in real time.

https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/

IoT Security Risks

- Hacking
  - Robot Vacuum Cleaner
    - According to researchers with Checkmarx, the vacuum has several high-severity flaws that open the device to remote attacks. Those include a denial of service (DoS) attack that bricks the vacuum, to a hack that allows adversaries to peer into private homes via the vacuum's embedded camera.



https://threatpost.com/vacuum-cleaners-baby-monitors-and-other-vulnerable-iot-devices/153294/

IoT Security Risks

- Hacking
  - Industrial Robot Arm
    - At the IEEE Security & Privacy conference later this month, they plan to present a case study of attack techniques they developed to subtly sabotage and even fully hijack a 220-pound industrial robotic arm capable of wielding gripping claws, welding tools, or even lasers.

https://www.wired.com/2017/05/watch-hackers-sabotage-factory-robot-arm-afar/

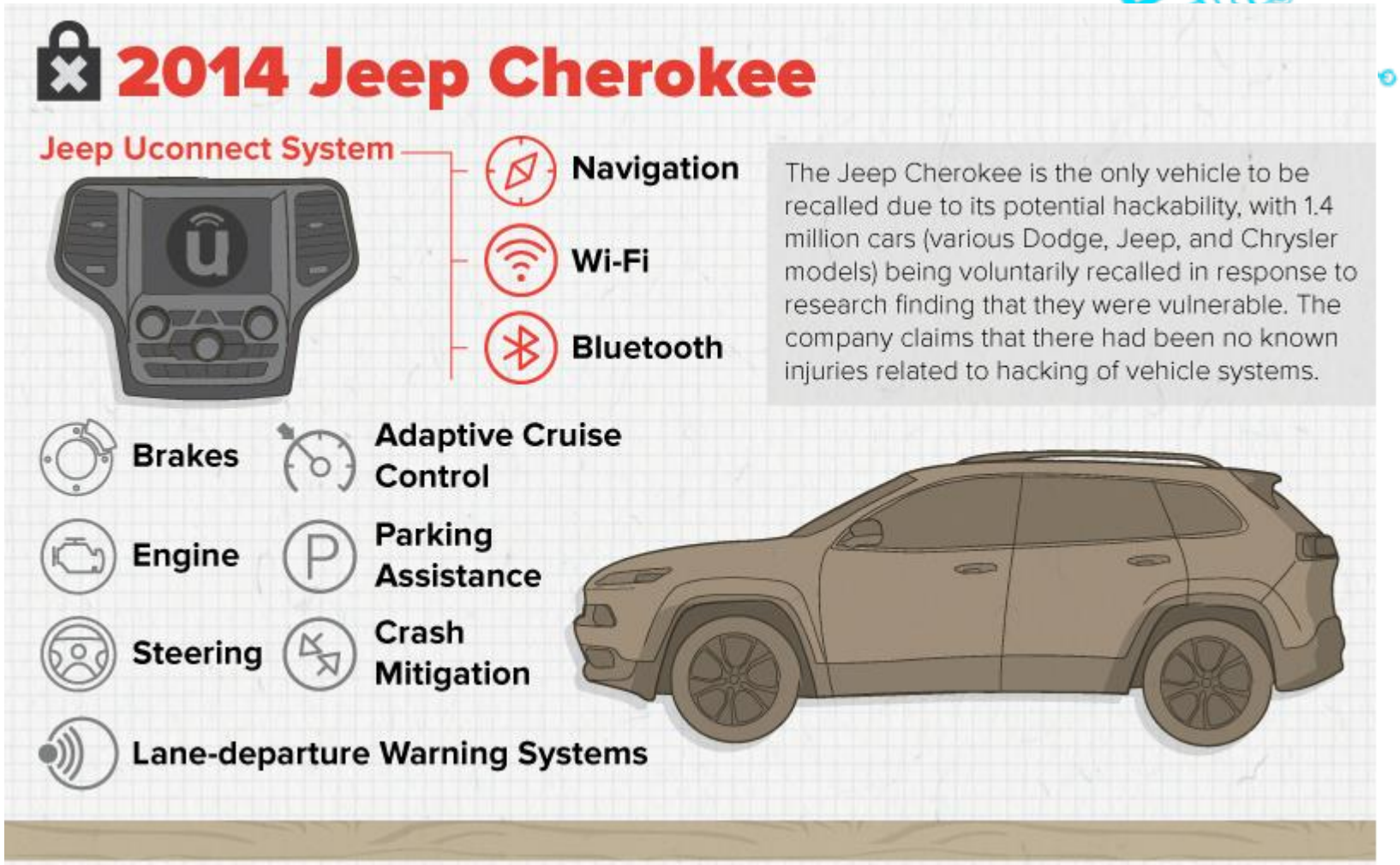
IoT Security Risks

- Physical Ransomware..?
- DDOS Attacks
  - Hackers are actively searching the internet and hijacking smart door/building access control systems, which they are using to launch DDoS attacks, according to firewall company SonicWall…(due to the type of exploit) meaning it can be exploited remote, even by low-skilled attackers without any advanced technical knowledge…these vulnerable systems can also be used as entry points into an organization's internal networks.

https://www.wired.com/2017/05/watch-hackers-sabotage-factory-robot-arm-afar/

IoT Security Risks

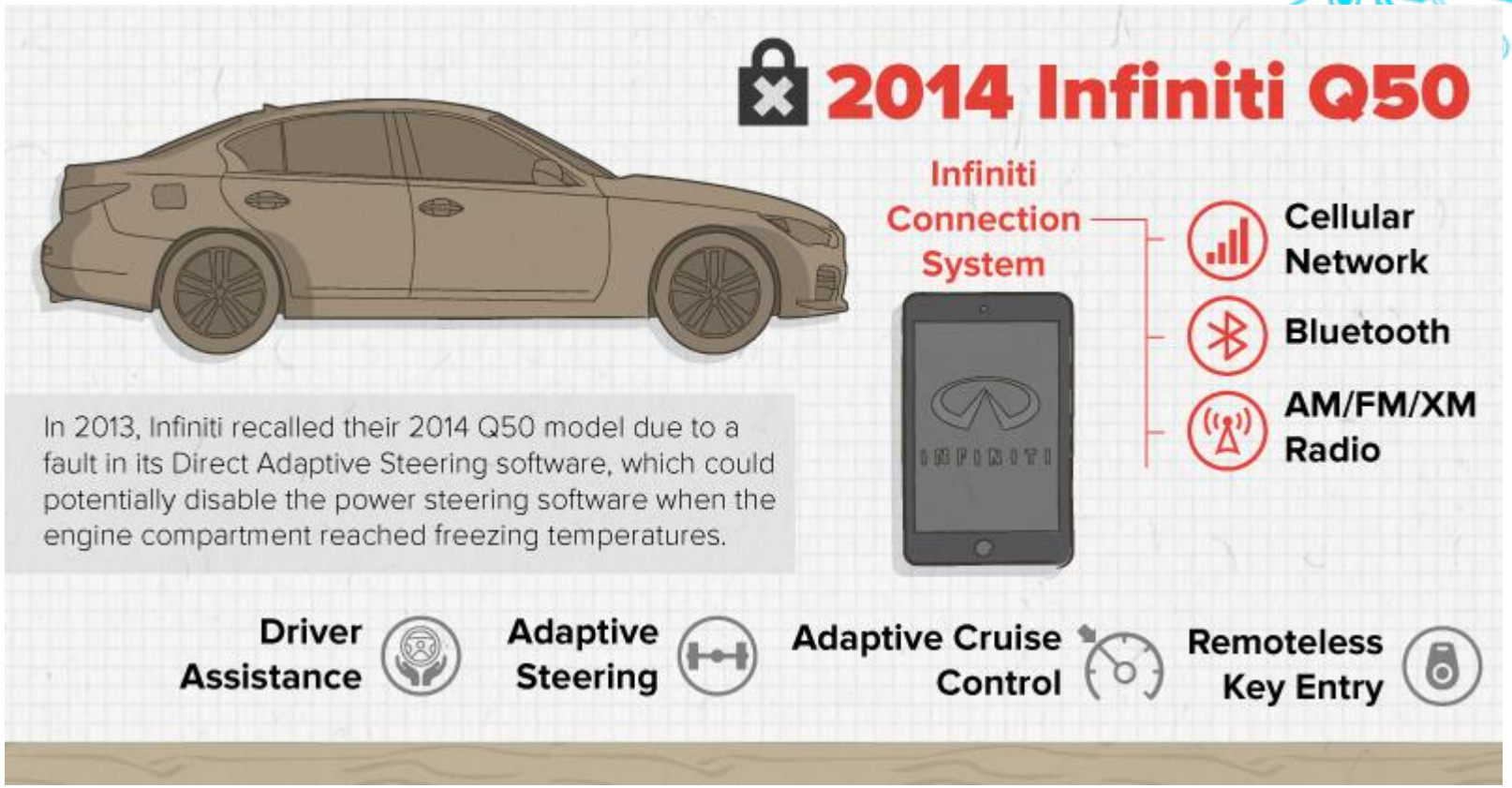
- Hacking
  - Connected vehicles



https://www.envistaforensics.com/news/the-most-hackable-cars-on-the-road-1

IoT Security Risks

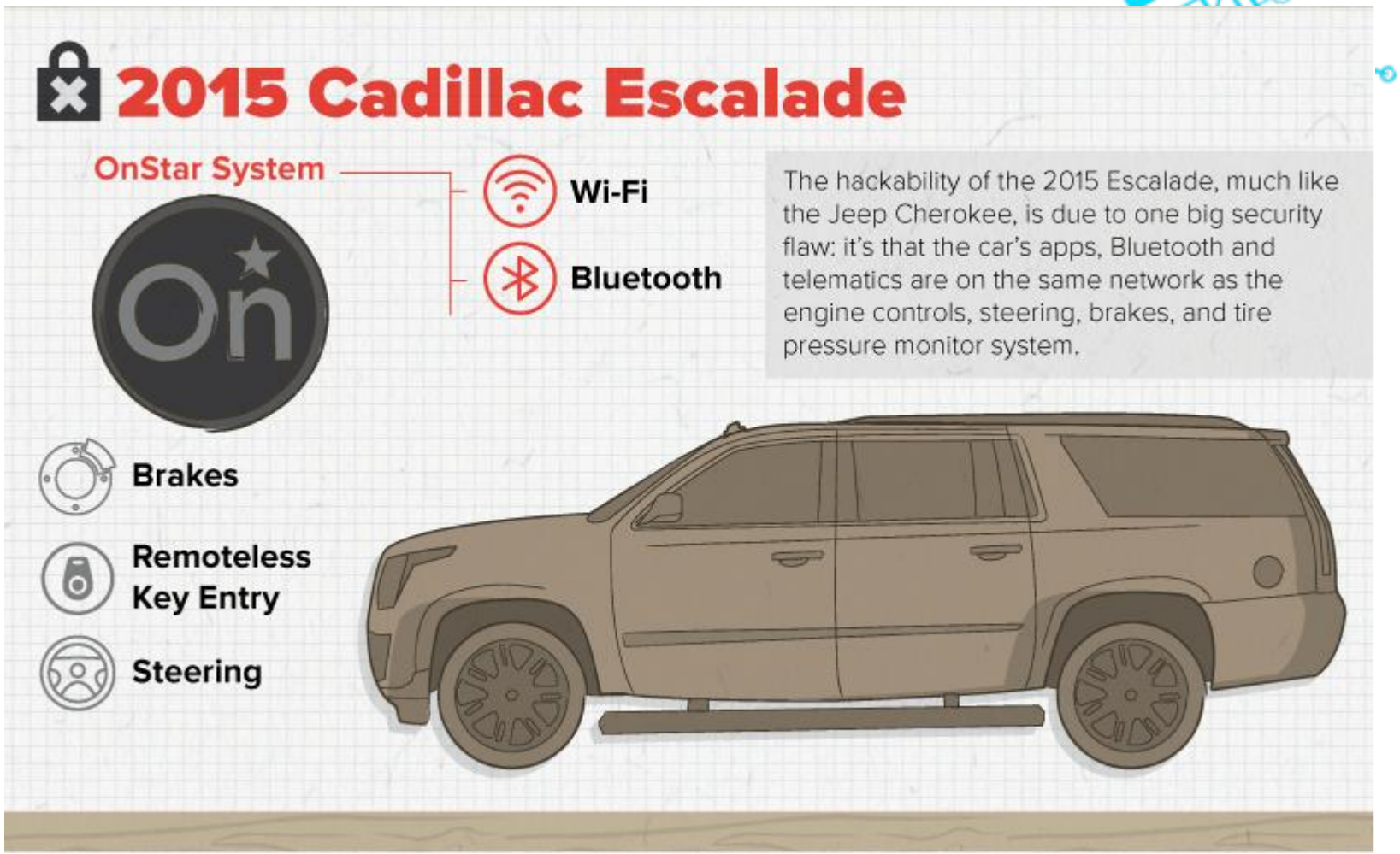
- Hacking
  - Connected vehicles



https://www.envistaforensics.com/news/the-most-hackable-cars-on-the-road-1

IoT Security Risks

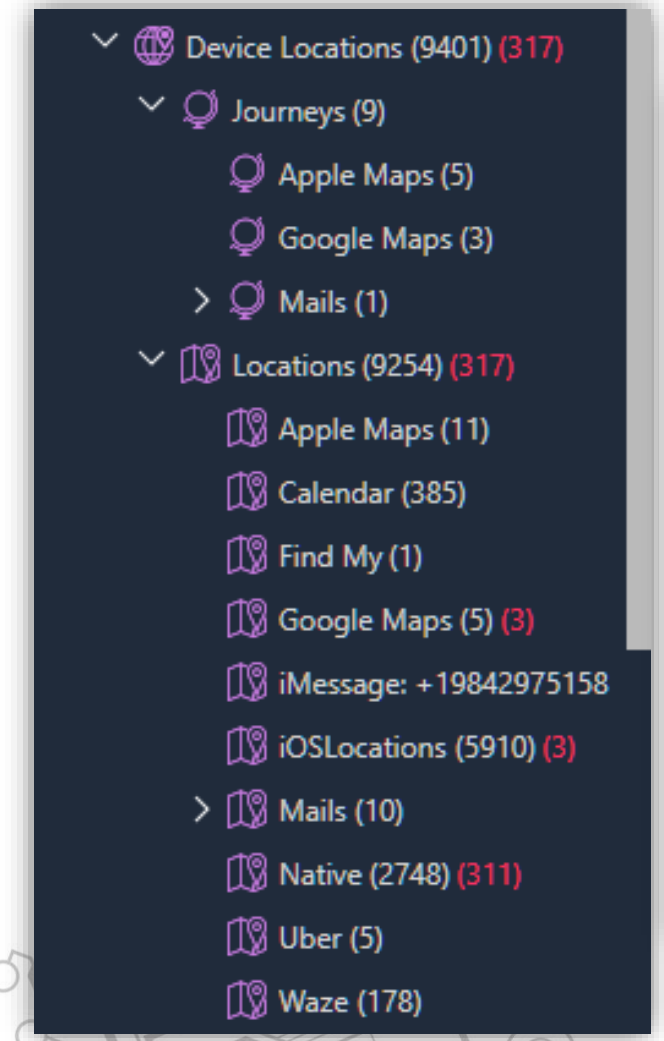
- Hacking
  - Connected vehicles

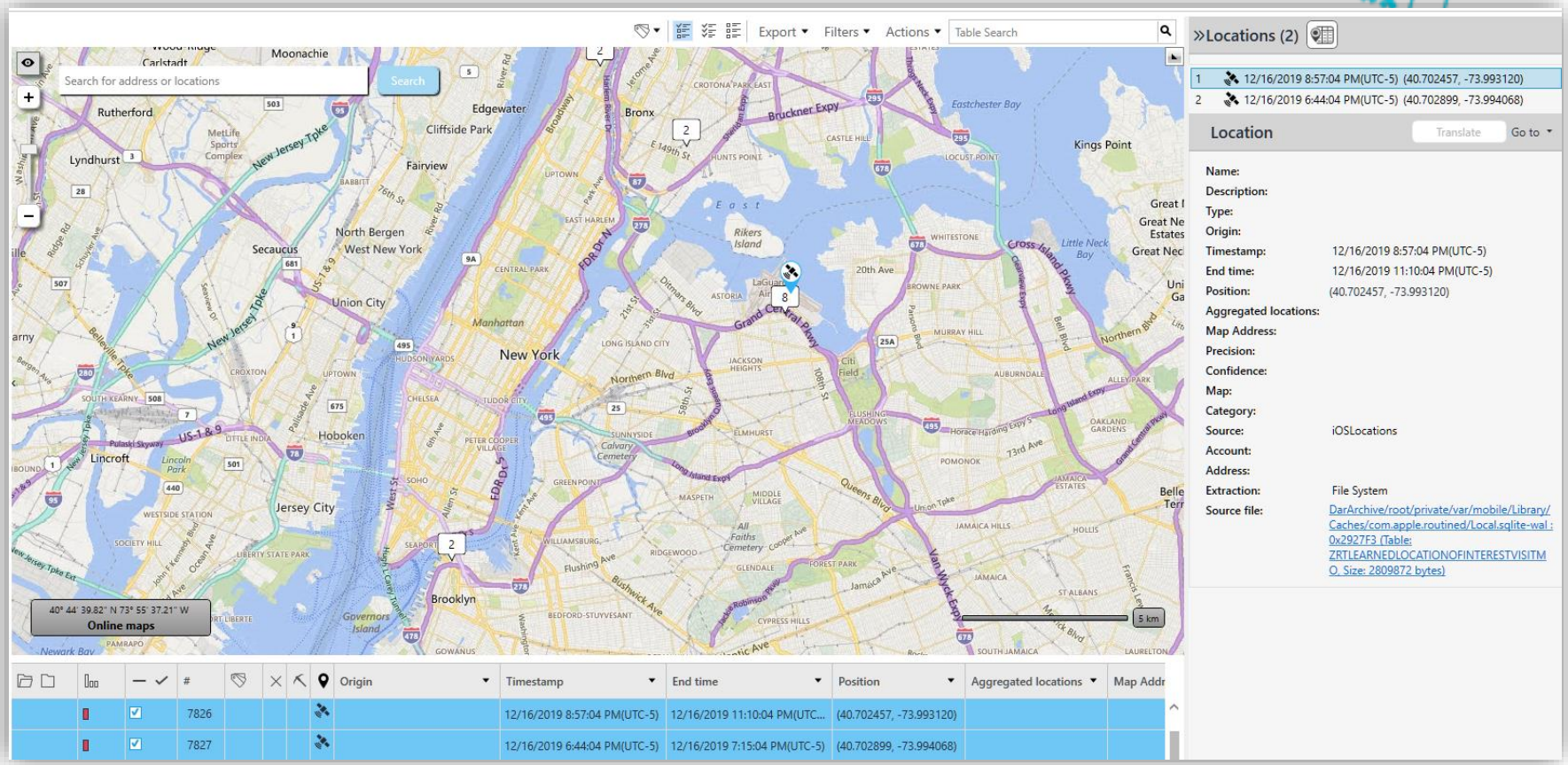


https://www.envistaforensics.com/news/the-most-hackable-cars-on-the-road-1

Location Data

- Location data from multiple sources within the cell phone





Application Events - CarPlay

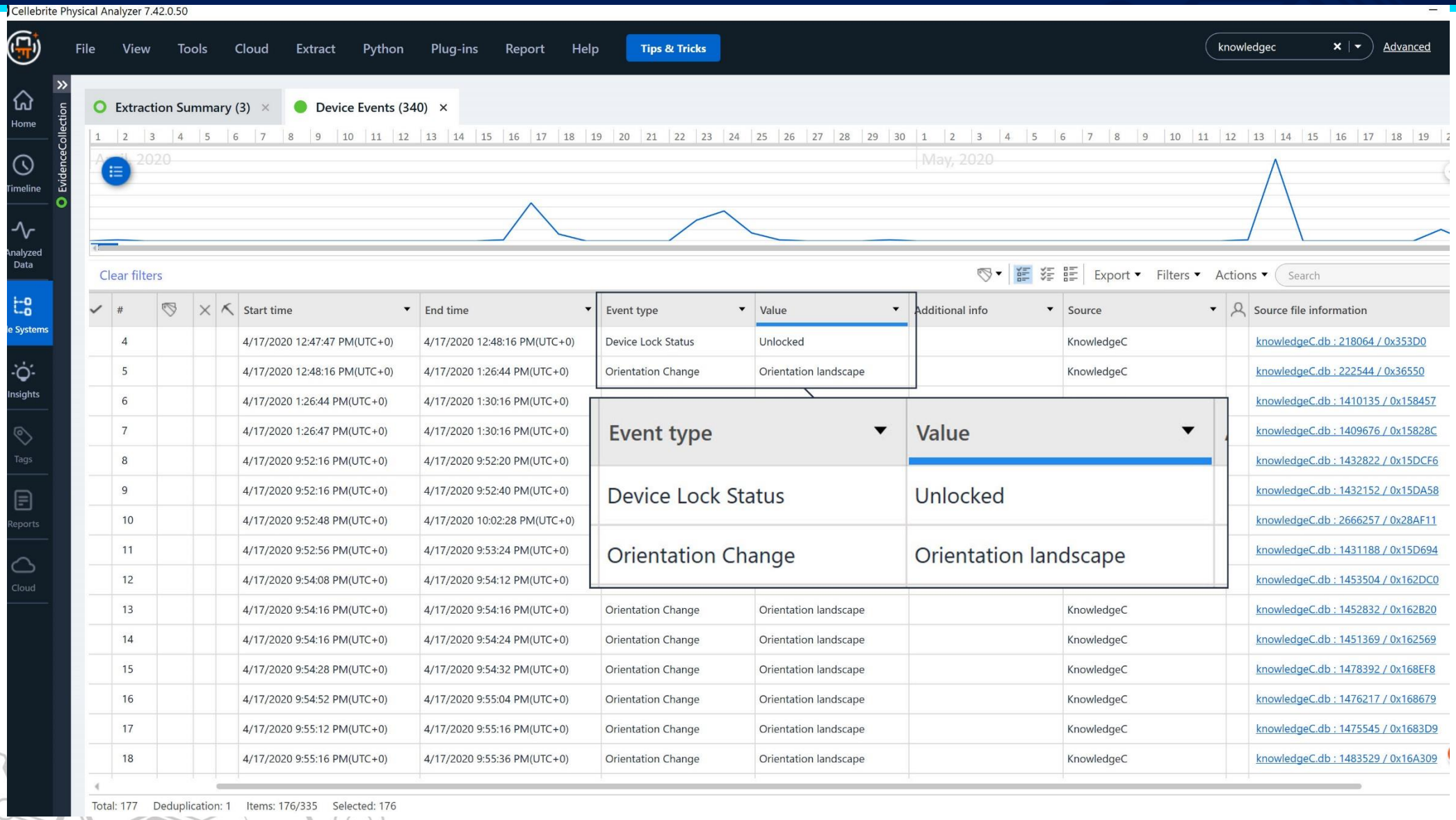
Identifier	Start time	End time
com.apple.CarPlaySplashScreen	7/28/2020 3:27:38 PM(UTC-5)	7/28/2020 3:27:38 PM(UTC-5)
com.apple.CarPlaySplashScreen	7/28/2020 4:44:02 PM(UTC-5)	7/28/2020 4:44:13 PM(UTC-5)
com.apple.CarPlaySplashScreen	7/28/2020 6:22:30 PM(UTC-5)	7/28/2020 6:22:38 PM(UTC-5)
com.apple.CarPlaySplashScreen	7/28/2020 9:06:25 PM(UTC-5)	7/28/2020 9:06:35 PM(UTC-5)
com.apple.CarPlaySplashScreen	7/29/2020 6:34:03 AM(UTC-5)	7/29/2020 6:34:14 AM(UTC-5)
com.apple.CarPlaySplashScreen	7/30/2020 6:36:57 AM(UTC-5)	7/30/2020 6:37:07 AM(UTC-5)
com.apple.CarPlaySplashScreen	7/30/2020 2:53:32 PM(UTC-5)	7/30/2020 2:53:45 PM(UTC-5)

The screen activates on connecting an iPhone via USB. (Some cars can use Bluetooth.)

Application Events – iPhone

Identifier	Start time	Additional info
com.apple.mobilephone	7/30/2020 7:20:16 AM(UTC-5)	Launch reason: com.apple.SpringBoard.transitionReason.homescreen
com.apple.InCallService	7/30/2020 7:20:18 AM(UTC-5)	
com.apple.InCallService	7/30/2020 7:20:38 AM(UTC-5)	Launch reason: com.apple.SpringBoard.backlight.transitionReason.idleTimer
com.apple.InCallService	7/30/2020 7:20:54 AM(UTC-5)	Launch reason: com.apple.SpringBoard.backlight.transitionReason.liftToWake
com.apple.InCallService	7/30/2020 7:20:54 AM(UTC-5)	
com.apple.mobilephone	7/30/2020 7:20:59 AM(UTC-5)	Launch reason: com.apple.SpringBoard.transitionReason.systemgesture
com.pandora	7/30/2020 7:21:07 AM(UTC-5)	Launch reason: com.apple.SpringBoard.transitionReason.homescreen
com.pandora	7/30/2020 7:21:30 AM(UTC-5)	Launch reason: com.apple.SpringBoard.backlight.transitionReason.idleTimer
com.pandora	7/30/2020 7:25:02 AM(UTC-5)	Launch reason: com.apple.SpringBoard.transitionReason.systemgesture

Device Events – User Interactions



Examination of Plaintiff's Phone

- Timelines

Time	Category	Item
11:48:44 AM(UTC-6)	DB	Phone (dialer.db)
11:48:44 AM(UTC-6)	Text File	com.android.dialer.xml
11:48:47 AM(UTC-6)	Picture	1841 task thumbnail.DELETED.png
11:48:55 PM(UTC-6)	E-Mail	Received E-Mail from [redacted] (Assistant Services)
11:49:17 AM(UTC-6)	SMS From: [redacted] Mother	Ohhhh, well if it can be gotten for less than$5 a sheet it might be worth it, but i don't think This truck could haul it all at once and 2 trips would probably break even with $12 delivered
11:49:17 AM(UTC-6)	SMS From: [redacted] Mother	Ohhhh, well if it can be gotten for less than$5 a sheet it might be worth it, but i don't think This truck could haul it all at once and 2 trips would probably break even with $12 delivered
11:51:02 AM(UTC-6)	Text File	rti.mqtt.counter.MqttLite.tp.DELETED.xml
11:52:23 PM(UTC-6)	Text File	event data [redacted]
11:55:47 AM(UTC-6)	Text File	BattStatsPrefs.DELETED 1.xml
11:55:48 AM(UTC-6)	Text File	com.google.android.gms.auth.devicesignals.DeviceSignalsStore.DELETED.xml
11:55:48 AM(UTC-6)	Text File	com.google.android.gms.tapandpay.service.TapAndPayServiceStorage.DELETED.xml
11:55:48 AM(UTC-6)	Text File	settings secure.DELETED.xml
11:56:14 AM(UTC-6)	Picture	1843 task thumbnail.png
11:59:00 AM(UTC-6)	Cookie: E-Mail	mail.google.com
11:59:00 AM(UTC-6)	Cookie: E-Mail	mail.google.com
11:59:00 AM(UTC-6)	Cookie: E-Mail	mail.google.com
11:59:00 AM(UTC-6)	DB	Gma l (Cookies)
11:59:02 PM(UTC-6)	Text File	AnalyticsPlatformPrefsFile.xml
11:59:02 PM(UTC-6)	Text File	AnalyticsPlatformPrefsFile.DELETED.xml
11:59:39 AM(UTC-6)	Text File	Account[redacted].DELETED.xml
11:59:58 AM(UTC-6)	Text File	com.google.android.gms.auth.authzen.cryptauth.DeviceStateSyncManager.xml
12:00:01 AM(UTC-6)	Text File	com.motorola.motodisplay.analytics.MD BREATHS.DELETED.xml
12:00:01 AM(UTC-6)	Text File	com.motorola.motodisplay.analytics.MD NOTIF.DELETED.xml
12:00:01 AM(UTC-6)	Text File	com.motorola.motodisplay.analytics.TOUCH.DELETED.xml
12:00:05 AM(UTC-6)	Text File	rti.mqtt.counter.MqttLite.tp.DELETED 1.xml
12:00:05 AM(UTC-6)	Text File	DebugAnalytics.DELETED 1.xml
12:00:20 PM(UTC-6)	Picture	IMG [redacted] 120016201.jpg
12:00:23 PM(UTC-6)	DB	Google Photos (media store extras)
12:00:23 PM(UTC-6)	Picture	IMG [redacted] 120021204.jpg
12:00:23 PM(UTC-6)	Text File	com.google.android.apps.photos preferences.DELETED 4.xml
12:00:24 AM(UTC-6)	Text File	BattStatsPrefs.DELETED 2.xml
12:00:24 PM(UTC-6)	Picture	IMG [redacted] 120022835.jpg
12:00:24 PM(UTC-6)	Text File	com.google.android.apps.photos preferences.DELETED 3.xml
12:00:25 PM(UTC-6)	DB	Google+ (trash.db)
12:00:25 PM(UTC-6)	Text File	com.google.android.apps.photos preferences.DELETED 2.xml
12:00:25 PM(UTC-6)	Text File	com.google.android.apps.photos preferences.DELETED 5.xml
12:00:26 PM(UTC-6)	Text File	com.google.android.apps.photos preferences.xml
12:00:26 PM(UTC-6)	Text File	com.google.android.apps.photos preferences.DELETED.xml
12:00:26 PM(UTC-6)	Text File	com.google.android.apps.photos preferences.DELETED 1.xml
12:00:58 PM(UTC-6)	Text File	MailAppProvider.DELETED 1.xml
12:00:59 AM(UTC-6)	Text File	Pmaps.xml
12:00:59 PM(UTC-6)	Text File	Account[redacted].DELETED 1.xml
12:00:59 PM(UTC-6)	Text File	MailAppProvider.DELETED.xml

Case Study: Distracted Driving

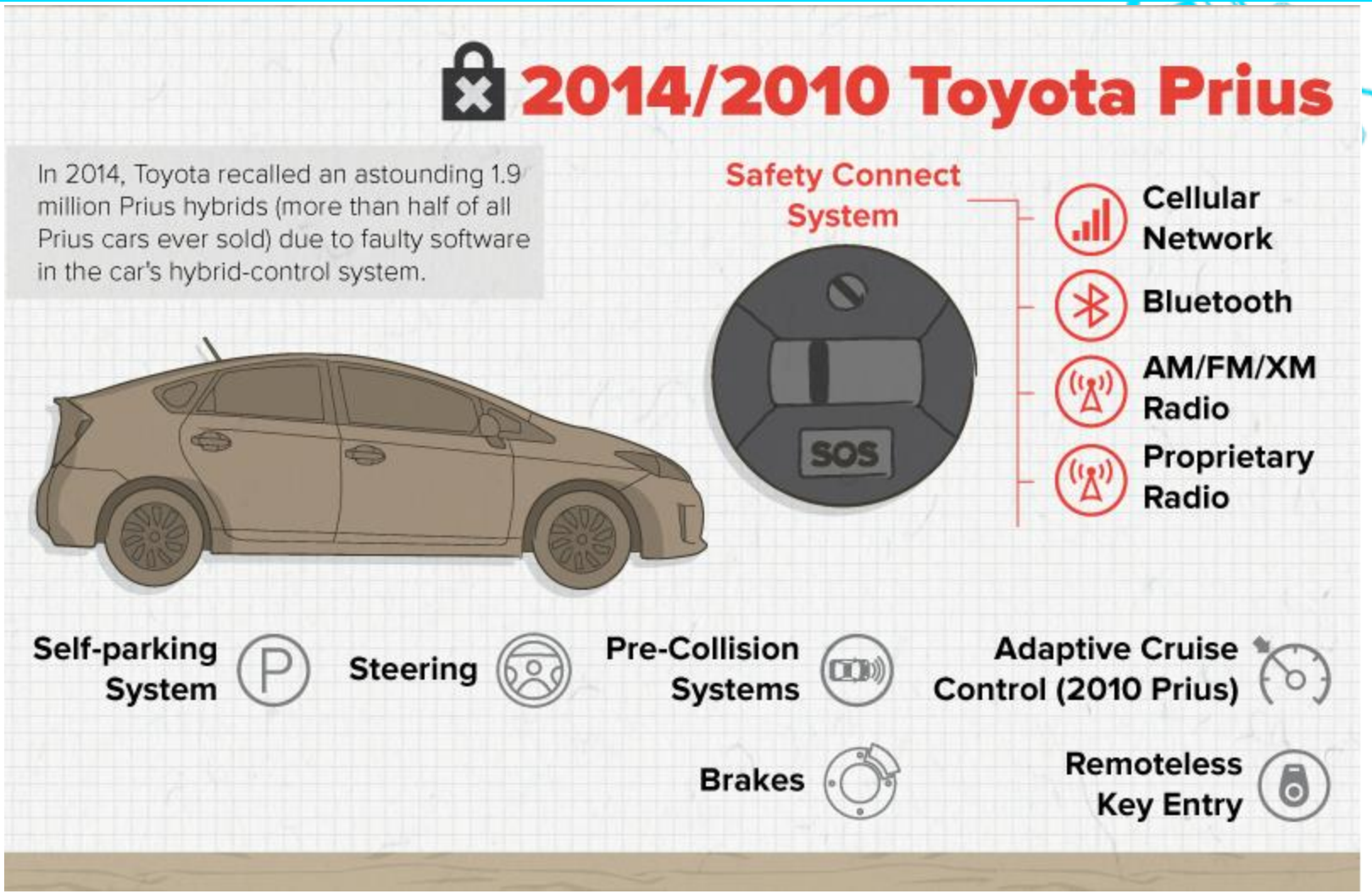
- Detailed timeline analysis at point of impact

Case Study: Distracted Driving

- Searching at time of impact

IoT Security Risks

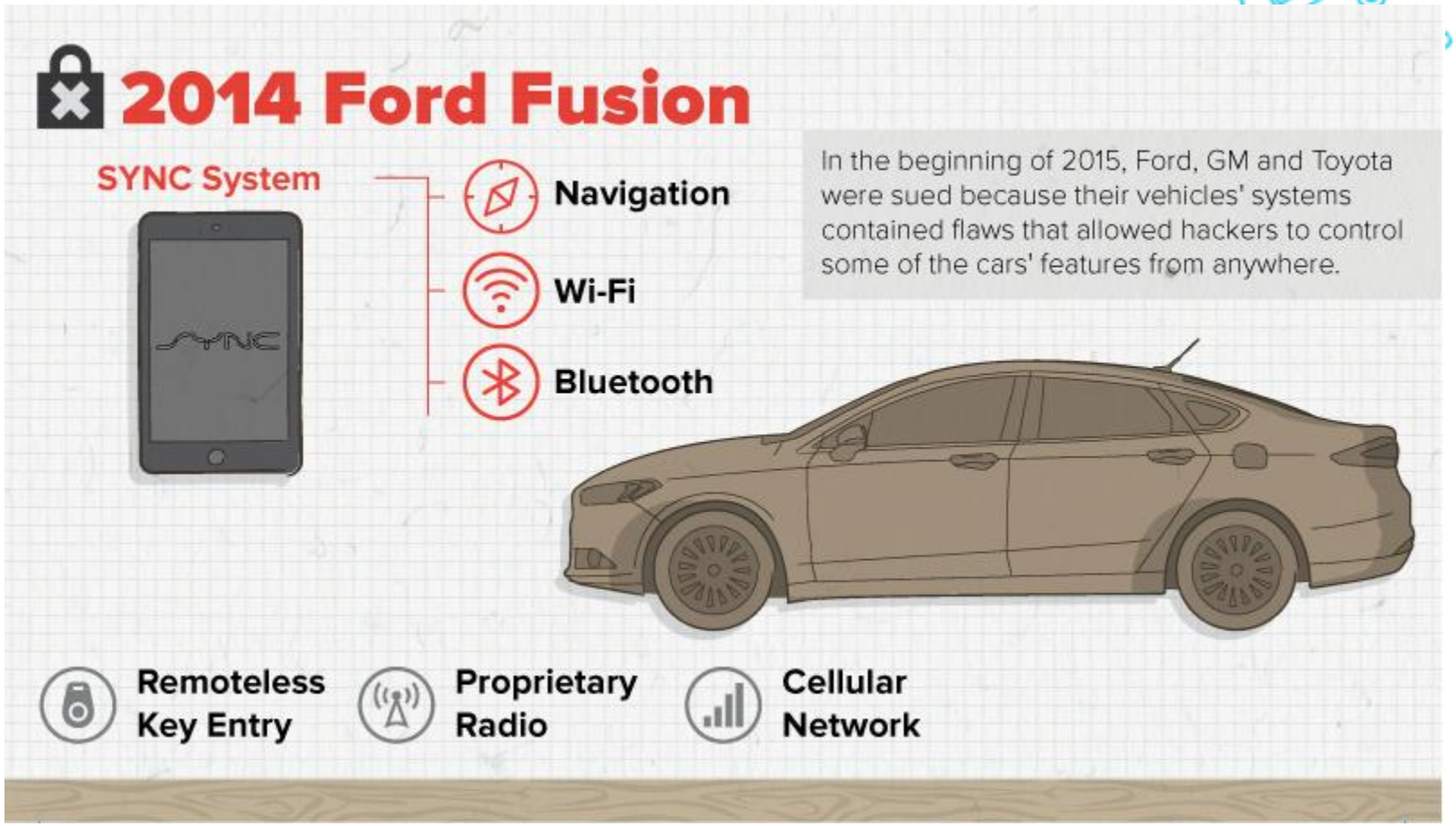
- Hacking
  - Connected vehicles



https://www.envistaforensics.com/news/the-most-hackable-cars-on-the-road-1

IoT Security Risks

- Hacking
  - Connected vehicles



https://www.envistaforensics.com/news/the-most-hackable-cars-on-the-road-1

ENVISTA FORENSICS

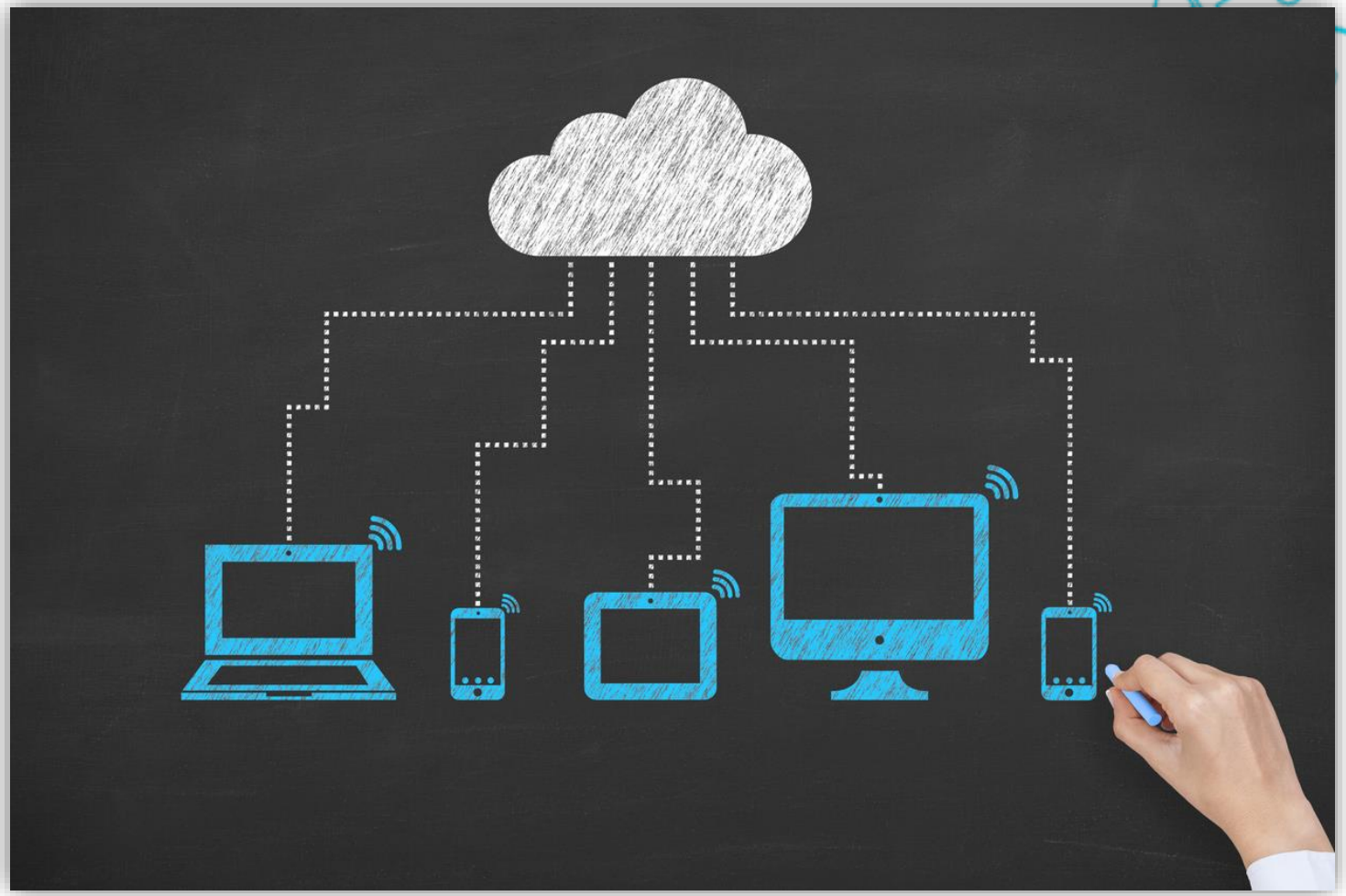
LARRY DANIEL
TECHNICAL DIRECTOR– DIGITAL FORENSICS

DATA SILOS

DIGITAL FORENSICS //

Data Silos

- IoT Devices lack
  - Processing power
  - Storage capacity
  - Transmission capabilities
- Data silos are
  - Computers
  - Cell phones
  - Online accounts



ENVISTA FORENSICS

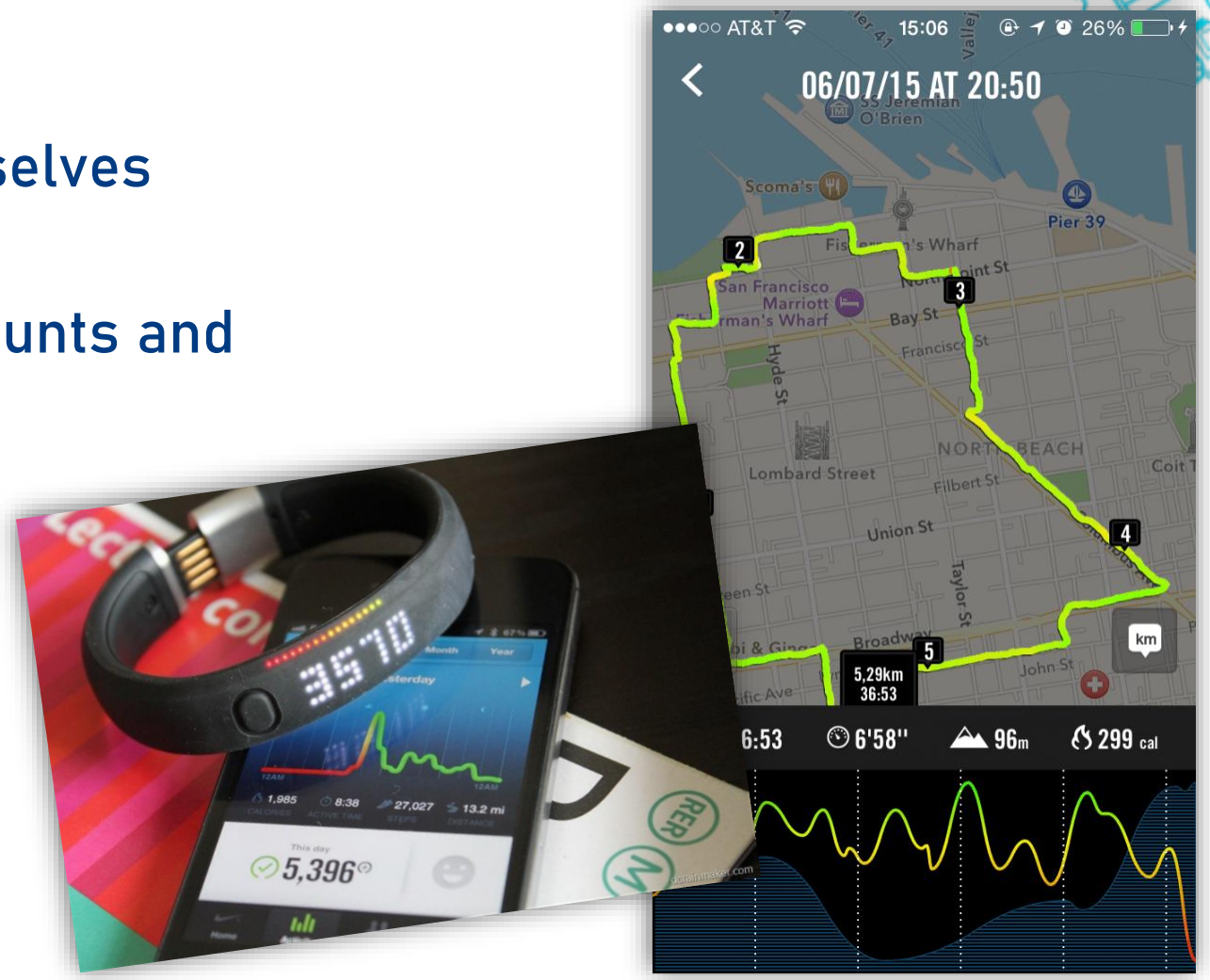
LARRY DANIEL
TECHNICAL DIRECTOR– DIGITAL FORENSICS

WEARABLE DEVICES

DIGITAL FORENSICS //

IoT Investigations

- Wearable Technology
  - Cell Phone Forensics
    - Data contained in apps themselves
  - Computer Forensics
    - Data contained in online accounts and local computer
  - Wearable Forensics
    - Data contained on actual wearable



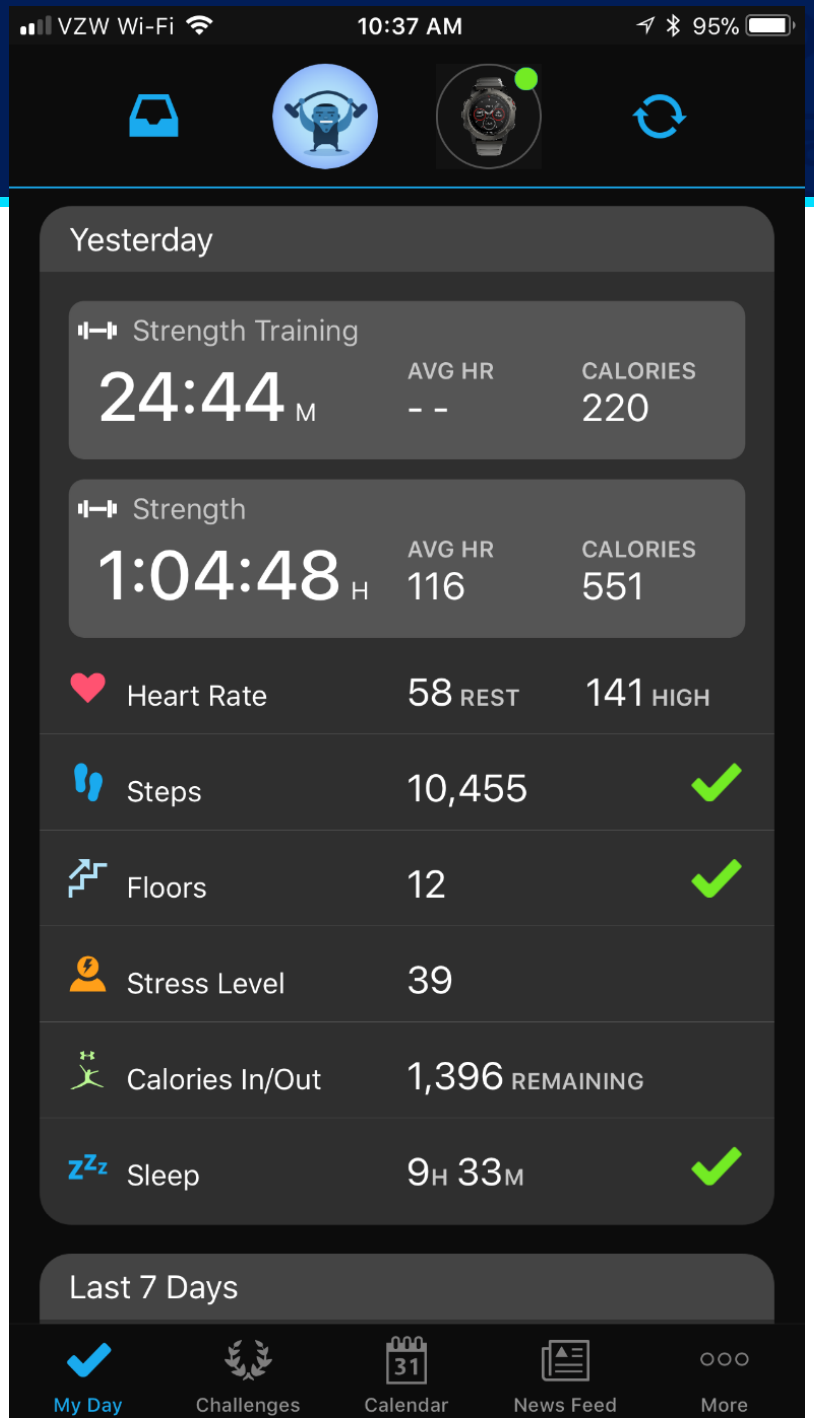
IoT Devices

- Garmin Fenix 5X
  - Unlimited timeline of activity / currently 1.5 years.

Image Licensed; (c) Lar

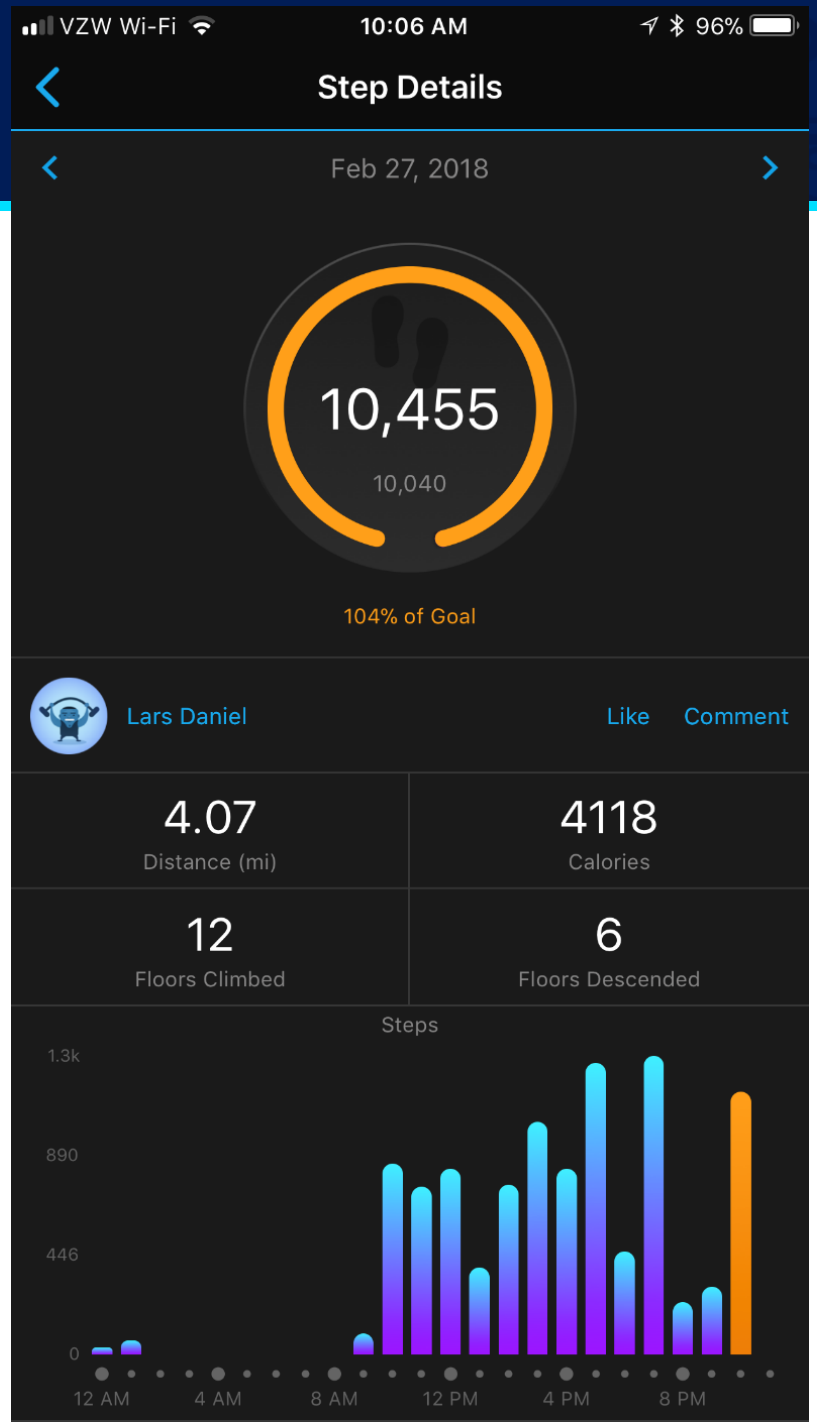
IoT Devices

- Garmin Fenix 5X
  - Tracks almost everything about me



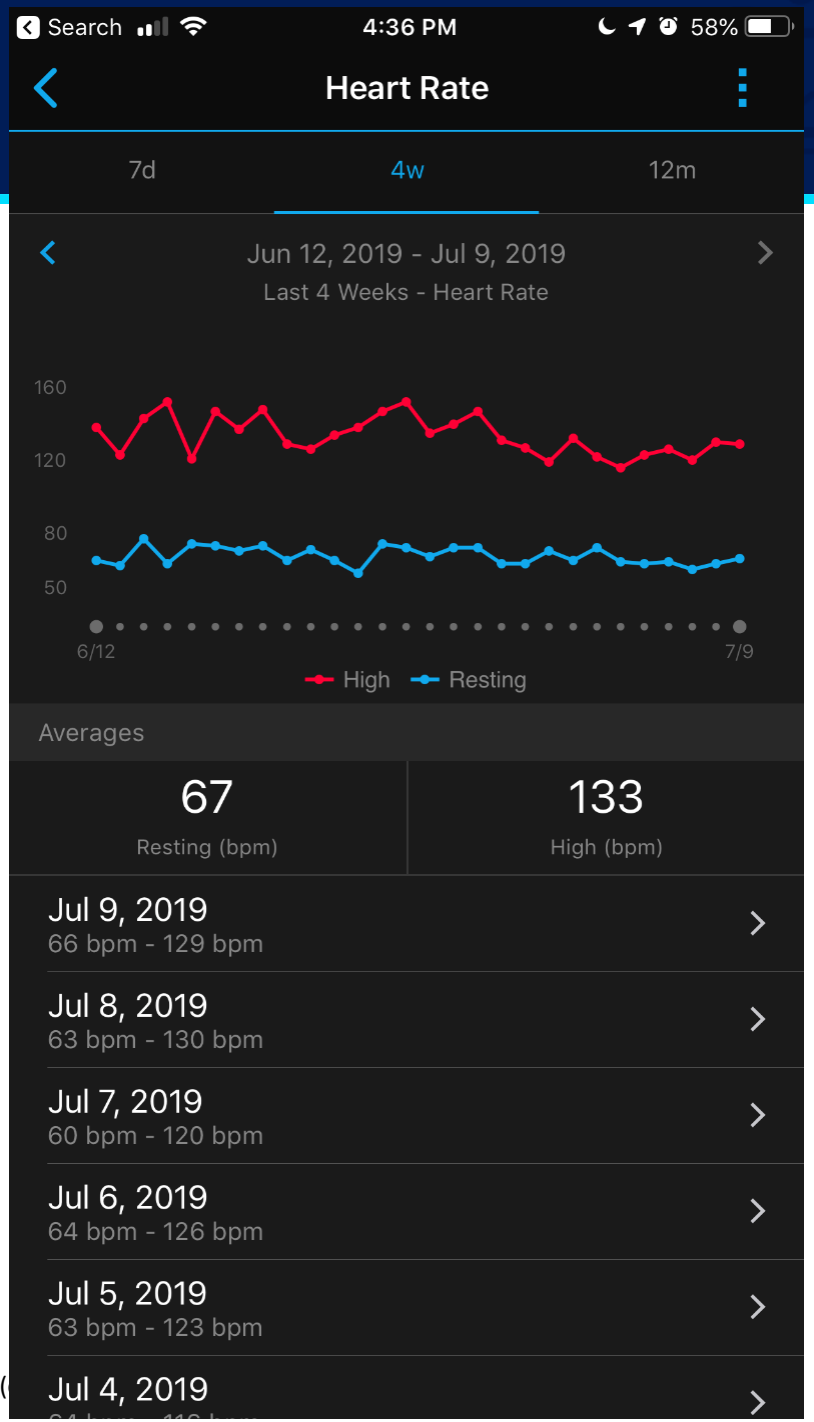
IoT Devices

- Garmin Fenix 5X
  - Tracks my performance metrics
    - Daily steps and when they were taken



IoT Devices

- Garmin Fenix 5X
  - Tracks almost everything about me
    - Down to the minute heartrate tracking



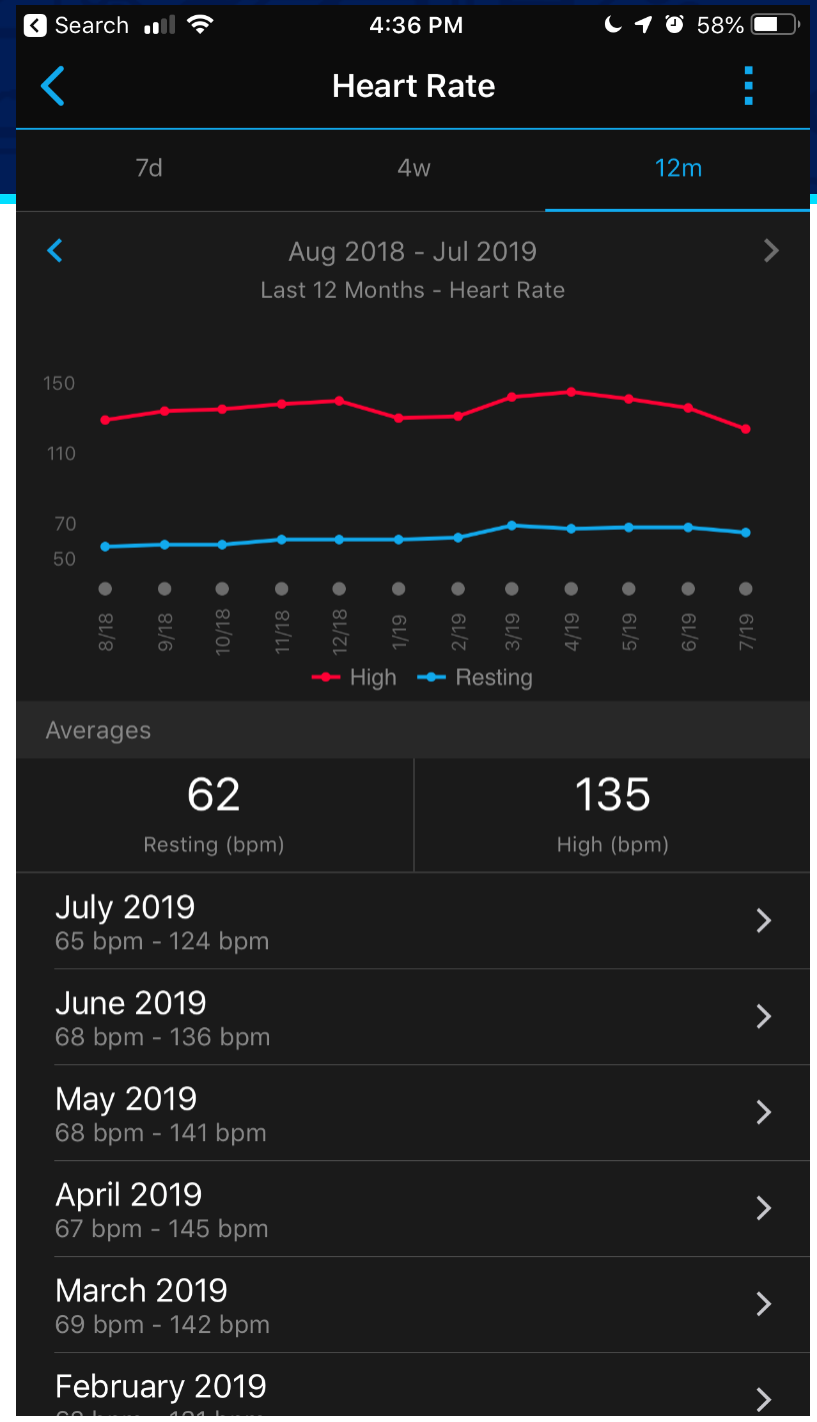
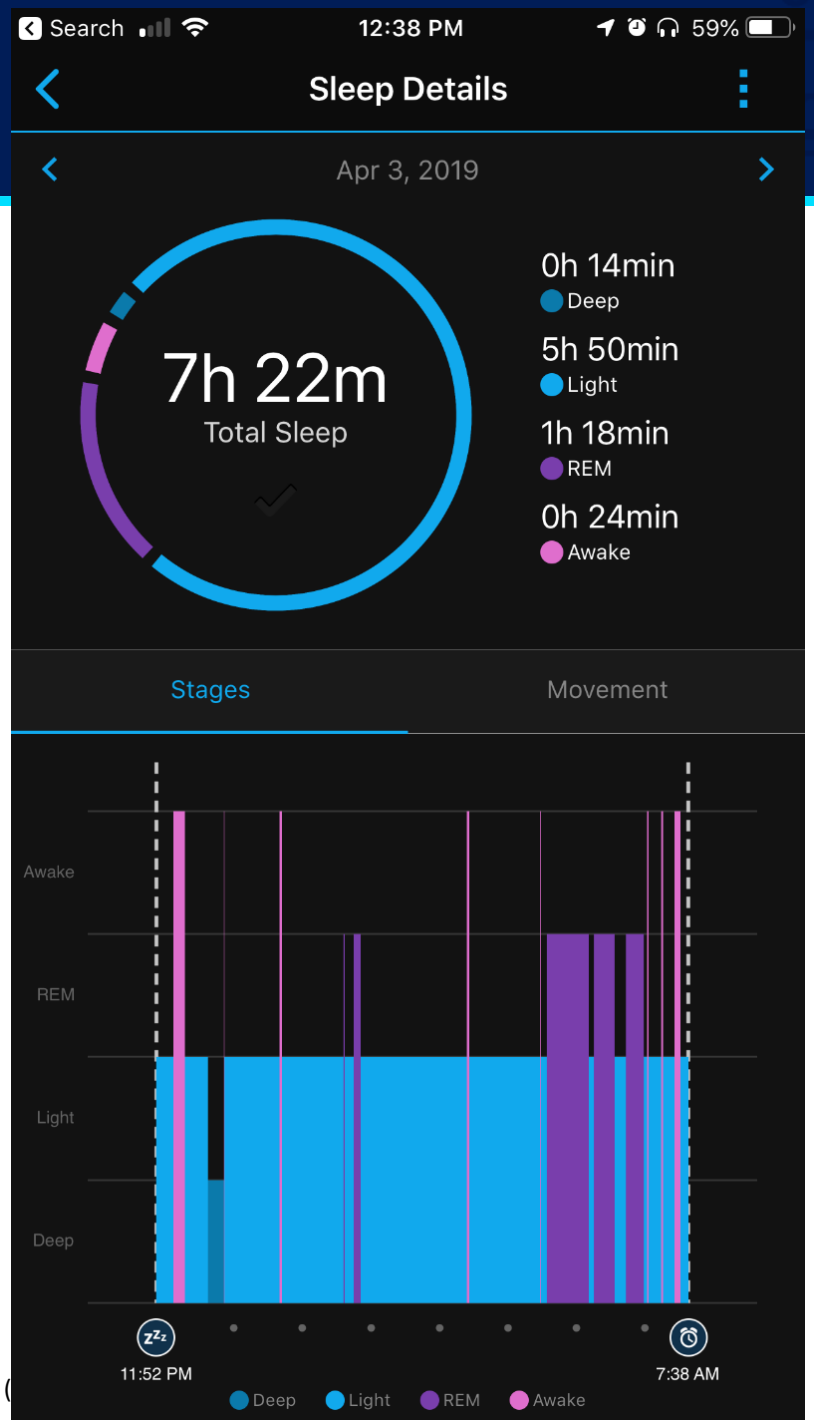


Image Licensed; (

IoT Devices

- Garmin Fenix 5X
  - Tracks sleep down to the minute



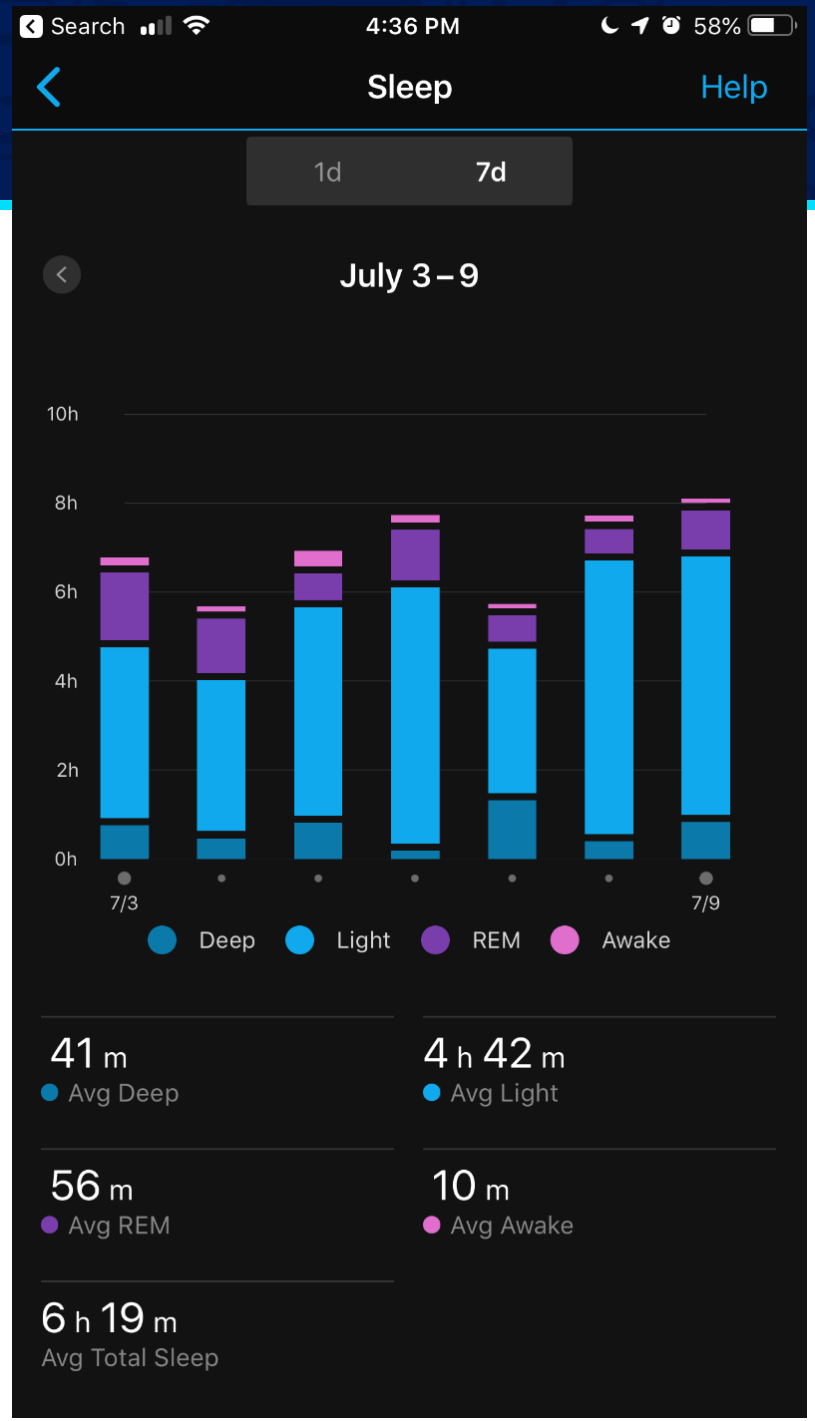


Image Licensed; (

IoT Devices

- Garmin Fenix 5X
  - Tracks almost everything about me
    - Stress analytics based upon heart rate and HRV (heart rate variability)

IoT Devices

- Garmin Fenix 5X
  - Tracks almost everything about me
    - Location activity, routes, maps, saved segments
    - Can contain maps inside the watch for almost the entire world

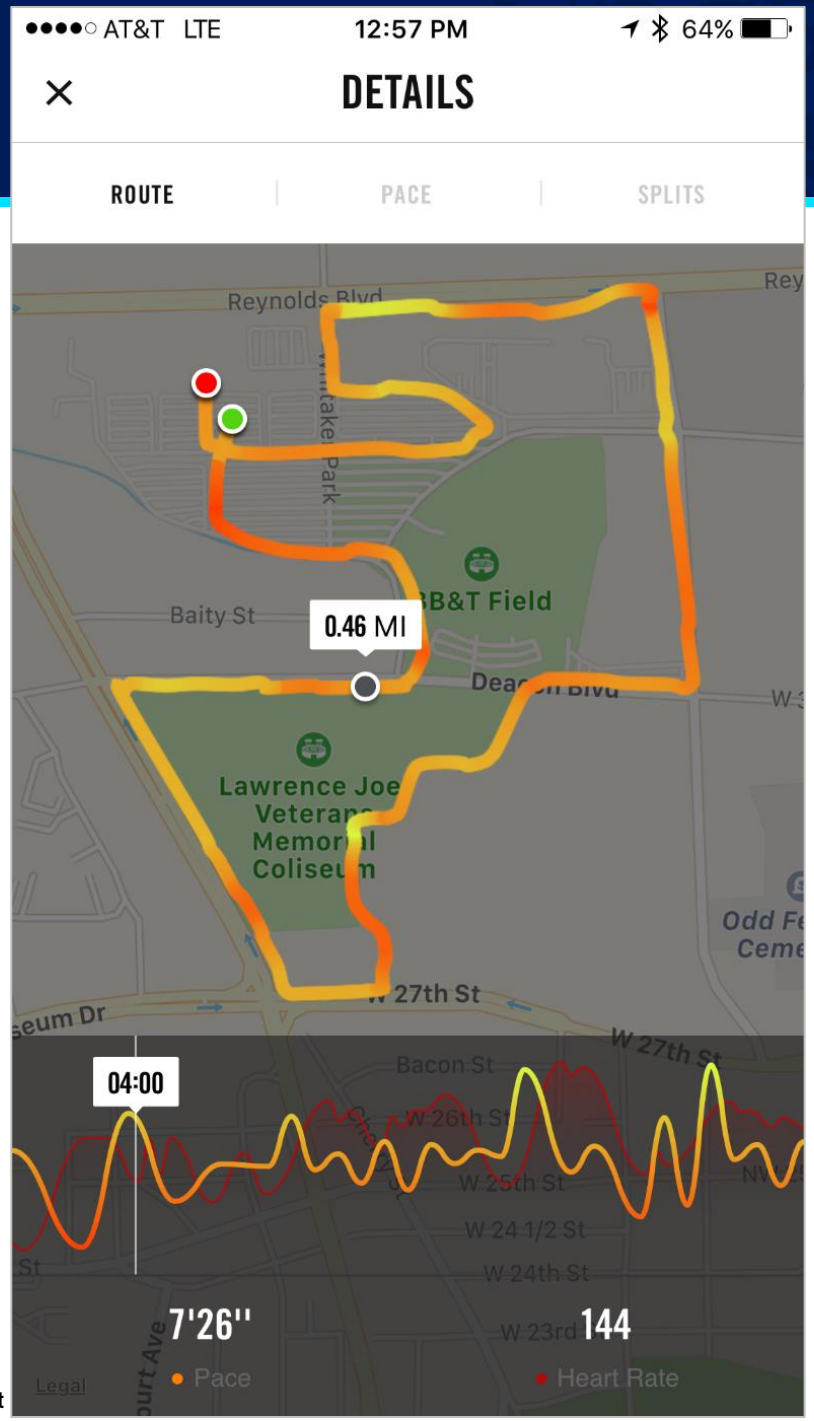
Fitness Wearables

- Fitness wearable (FitBit)
  - Victims husband told police that he was at home fighting off an intruder when his wife returned from the gym no later than 9 am. According to the husband, the intruder then shot his wife, tied him up, and ran out of the house. The police searched the wife's fitness wearable. Its data showed that the wife was still moving about the home a distance of 1,217 feet between 9:18 am and 10:05 am…he was having an affair and attempting to cash in on wife's life insurance

https://www.crowelldatalaw.com/2017/07/recent-iot-device-cases/.

Border Crossing

- Did defendant cross the border?
  - Data acquired from online account and the cell phone



Running at time of incident?

- Was suspect using treadmill?
  - Workout can be created after the fact – will be missing some data.

Did cyclist slow down?

- IoT Devices
  - Data Silo = Phone Application

Vector™ 3/3S

Measure power at the pedal to gauge your performance.

fēnix® 5 Series

Premium multisport GPS watches available in three sizes and a variety of styles, all featuring wrist-based heart rate

Case Example – Insurance Fraud

- Scenario
  - Employee is on business trip out of Country in Europe. Last night of the week stay, he explores the town and upon his return to work the following week the company notices large transactions on his corporate card. Prior to this time, no report of issues were made to the company. When questioned, the Employee advises he was the victim of a kidnapping and the charges were made when his card was stolen and used during that night.

Case Example – Insurance Fraud

- Scenario
  - Advised his card was compromised but not lost.
  - Alleges to be held for 6+ hours through the night.
  - Vivid details about the attackers, (action movie like)
  - No report of attack to company or authorities
  - A $100,000.00 claim was made to Insurance over the incident

Case Example – Insurance Fraud

- Evidence
  - We are contacted by SIU to assist in the investigation and complete a examinations
    - Apple Watch
    - iPhone XR
  - They also have videos, financial records and statements to compare detail to.

Case Example – Insurance Fraud

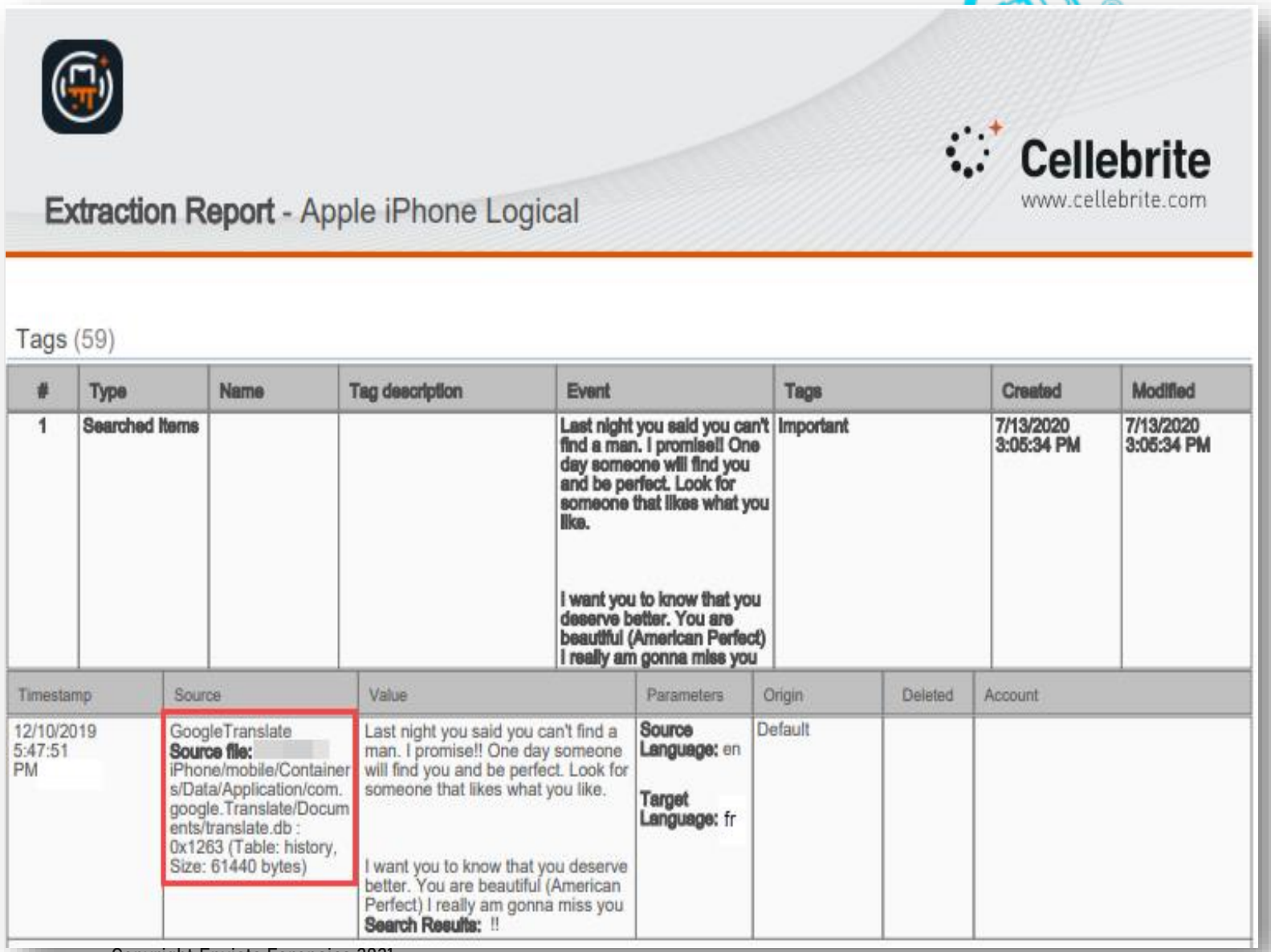
- Analysis
  - The Analysis yielded two critical data types allowing the SIU Investigator to call into question the statements give in the Interviews.
    - The health app on the evening of this incident was very active. Miles worth of steps were logged, contradictory of sitting still for 6+ hours while being held captive.

25	Activities				Important	7/13/2020 3:06:40 PM	7/13/2020 3:06:40 PM

Name	Originates from	Value	Time	Location	Source	Deleted
Steps and Distance	Device	174 Steps 89.90 Meters	**Last Launch:** 12/9/2019 7:19:32 PM(**Start time:** 12/9/2019 7:08:11 PM(**End time:** 12/9/2019 7:14:04 PM((		**Source:** Health **Source file:** iPhone/mobile/Library/Health/healthdb_secure.sqlite : 0x3A6839B (Table: samples, objects, Size: 113782784 bytes)	

Case Example – Insurance Fraud

- Analysis
- Right before taking off from the airport to come home, the employee crafted to messages in google translate, (the app had been removed from the device) to profess his love for the nice lady he spent the evening with “last night”, the evening of the incident.



Extraction Report - Apple iPhone Logical

Cellebrite
www.cellebrite.com

Tags (59)

#	Type	Name	Tag description	Event	Tags	Created	Modified
1	Searched Items			Last night you said you can't find a man. I promise!! One day someone will find you and be perfect. Look for someone that likes what you like. I want you to know that you deserve better. You are beautiful (American Perfect) I really am gonna miss you	Important	7/13/2020 3:05:34 PM	7/13/2020 3:05:34 PM

Timestamp	Source	Value	Parameters	Origin	Deleted	Account
12/10/2019 5:47:51 PM	GoogleTranslate **Source file:** iPhone/mobile/Containers/Data/Application/com.google.Translate/Documents/translate.db : 0x1263 (Table: history, Size: 61440 bytes)	Last night you said you can't find a man. I promise!! One day someone will find you and be perfect. Look for someone that likes what you like. I want you to know that you deserve better. You are beautiful (American Perfect) I really am gonna miss you **Search Results:** !!	**Source Language:** en **Target Language:** fr	Default		

Case Example – Insurance Fraud

- Outcome
  - Now armed with this information, SIU was able to confront the employee and his employer – claim was denied.

ENVISTA FORENSICS

LARRY DANIEL
TECHNICAL DIRECTOR– DIGITAL FORENSICS

MEDICAL DEVICES

INGESTIBLES AND INSERTABLES

DIGITAL FORENSICS //

Medical Ingestibles

- Late 2017
  - US Food and Drug Administration (FDA) approved first digital pill for general human consumption.
    - Part medication delivery system, part IoT device.
    - Inserted within tablet is an ingestible sensor
    - Tracks exact moment pill hits the stomach

https://www.godaddy.com/garage/the-iot-in-healthcare-forget-wearables-now-there-are-ingestibles/

Medical Ingestibles

- Proteus Digital Health
  - Designed to address patient non-compliance
    - 20 to 30 percent of patient prescriptions are never filled.
    - 50 percent of medications for chronic diseases are not taken as prescribed.
    - Typically, only one-half of a full prescription is consumed by the patient.
    - Non-compliance causes approximately 125,000 deaths annually and 10 percent of all hospitalizations.
    - This costs U.S. hospitals somewhere between $100 and $289 billion annually.

https://www.godaddy.com/garage/the-iot-in-healthcare-forget-wearables-now-there-are-ingestibles/

Medical Ingestibles

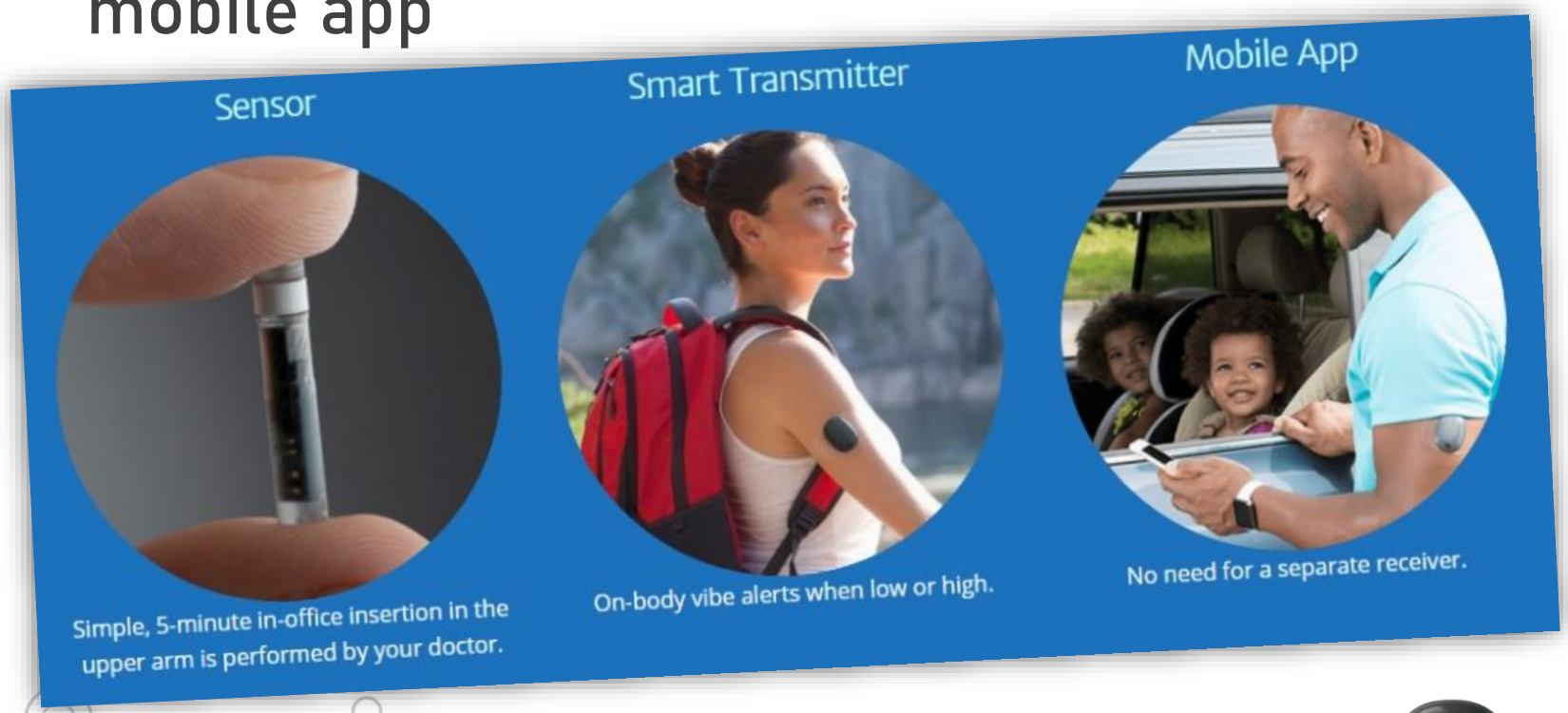
- Proteus Digital Health
  - Proteus Discover

Proteus Discover consists of an ingestible sensor the size of a grain of sand, a small wearable sensor patch, an application on a mobile device and a provider portal. The patient activates Proteus Discover by taking medication with an ingestible sensor. Once the ingestible sensor reaches the stomach, it transmits a signal to the patch worn on the torso. A digital record is sent to the patient's mobile device and then to the Proteus cloud where with the patient's permission, healthcare providers and caregivers can access it via their portal. The patch also measures and shares patient activity and rest.

https://www.godaddy.com/garage/the-iot-in-healthcare-forget-wearables-now-there-are-ingestibles/

Medical Implants

- Eversense CGM (Continuous Glucose Monitoring)
  - Remote monitoring by friends/family and providers via mobile app



https://ous.eversensediabetes.com/products/

Medical Implants

- Verichip

- The US Food and Drug Administration has approved Verichip, an implantable radiofrequency identification device for patients, which would enable doctors to access their medical records. Doctors hope that use of the device will result in be better treatment for patients in emergencies or when a patient is unconscious or lacks medical records. Some people have raised fears, however, that it could lead to infringements of patients' privacy. The chip is the size of a grain of rice and is implanted under local anaesthesia beneath the patient's skin in the triceps area of the right arm, where it is invisible to the naked eye. It contains a unique 16 digit identification number. A handheld scanner passed near the injection site activates the chip and displays the number on the scanner. Doctors and other medical staff use the identification number to access the patient's records on a secure database via encrypted internet access.

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC526112/?fbclid=IwAR3f3EezRq0LP-bgVgVxFyXfhAEHKqWMHUye6AlTRRsu49YuwAyXjc3bVL8

ENVISTA FORENSICS

LARRY DANIEL
TECHNICAL DIRECTOR– DIGITAL FORENSICS

SMART VEHICLES

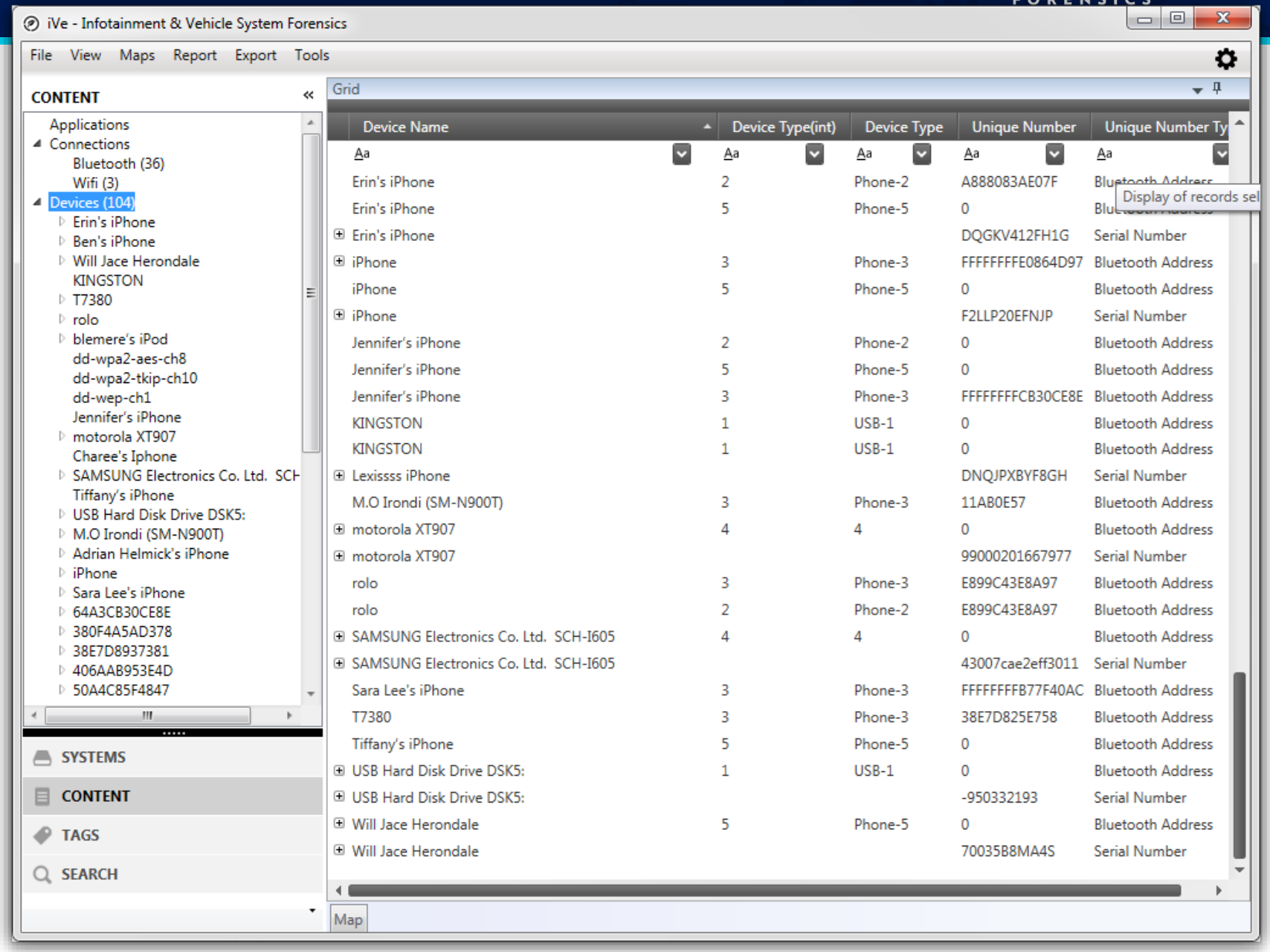
DIGITAL FORENSICS //

IoT Investigations

- Vehicle Forensics
  - In-vehicle infotainment
  - Vehicle telematics
- Data types
  - 3rd part application data
  - USB, Bluetooth, WiFi connections
  - Call logs, contact lists, messages
  - Pictures, videos, social media feeds
  - Location data, navigation information
  - Event data with associated time and location

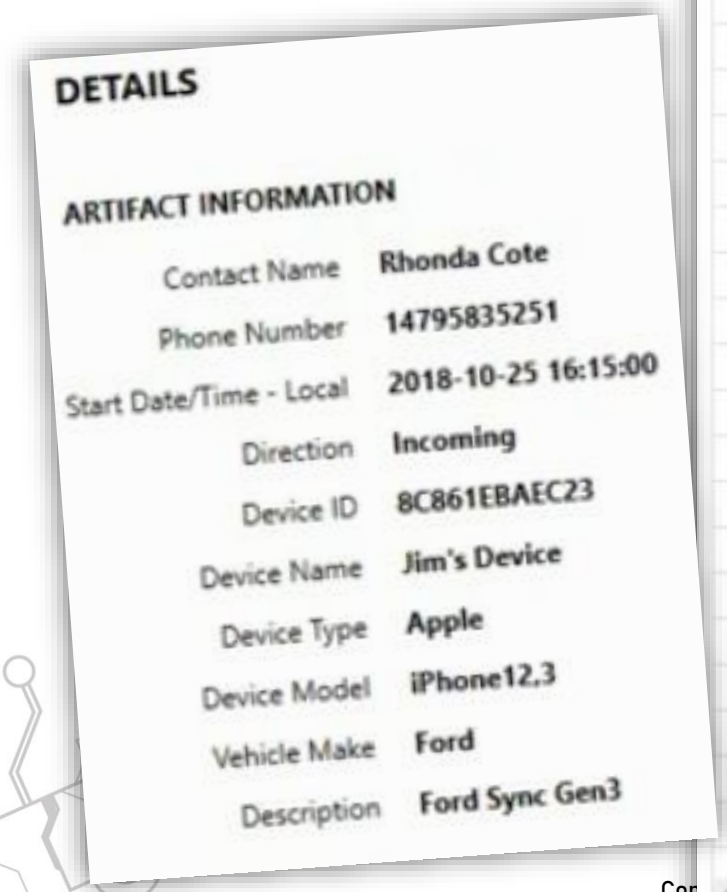
Forensic Artifacts

- Connected Devices
  - Rental Car



Forensic Artifacts

- Call Logs
  - Tied to specific account
  - Records Device ID



DETAILS

ARTIFACT INFORMATION

Contact Name	Rhonda Cote
Phone Number	14795835251
Start Date/Time - Local	2018-10-25 16:15:00
Direction	Incoming
Device ID	8C861EBAEC23
Device Name	Jim's Device
Device Type	Apple
Device Model	iPhone12,3
Vehicle Make	Ford
Description	Ford Sync Gen3

EVIDENCE (201)

Column view

Conta...	Phon...	Start...	Start Date/T...	Dire...	Device ID	Devi...	Devi...
Rhonda Cote	14795835251		2018-10-25 16:15:00	Incoming	8C861EBAEC23	Jim's Device	Apple
	3904567733		2018-10-26 16:12:00	Incoming	8C861EBAEC23	Jim's Device	Apple
Jin Contreras	9029306440		2018-10-25 13:43:00	Incoming	8C861EBAEC23	Jim's Device	Apple
Akeem Jensen	18612229018		2019-08-23 08:22:59	Incoming	8C861EBAEC23	Jim's Device	Apple
	8927942810		2018-10-25 07:53:00	Incoming	8C861EBAEC23	Jim's Device	Apple
Unknown	6876755339		2018-10-24 16:25:00	Incoming	8C861EBAEC23	Jim's Device	Apple
Hadley Bell	9042066849		2018-10-24 15:20:00	Incoming	8C861EBAEC23	Jim's Device	Apple
Akeem Jensen	18612229018		2018-10-24 15:18:00	Incoming	8C861EBAEC23	Jim's Device	Apple
	3904567733		2018-10-24 15:18:00	Incoming	8C861EBAEC23	Jim's Device	Apple
Rhonda Cote	14795835251		2018-10-24 08:17:00	Incoming	8C861EBAEC23	Jim's Device	Apple
Jin Contreras	9029306440		2018-10-23 20:03:00	Incoming	8C861EBAEC23	Jim's Device	Apple
	8927942810		2018-10-23 11:07:00	Incoming	8C861EBAEC23	Jim's Device	Apple
Unknown	6876755339		2018-10-22 17:22:00	Incoming	8C861EBAEC23	Jim's Device	Apple
Hadley Bell	9042066849		2018-10-22 15:05:00	Incoming	8C861EBAEC23	Jim's Device	Apple
Akeem Jensen	18612229018		2018-10-22 11:43:00	Incoming	8C861EBAEC23	Jim's Device	Apple
	3904567733		2018-10-22 08:03:00	Incoming	8C861EBAEC23	Jim's Device	Apple
Rhonda Cote	14795835251		2018-10-21 20:42:00	Incoming	8C861EBAEC23	Jim's Device	Apple
Jin Contreras	9029306440		2018-10-18 17:36:00	Incoming	8C861EBAEC23	Jim's Device	Apple
	8927942810		2018-10-18 14:44:00	Incoming	8C861EBAEC23	Jim's Device	Apple
Unknown	6876755339		2018-10-17 21:11:00	Incoming	8C861EBAEC23	Jim's Device	Apple
Hadley Bell	9042066849		2018-10-17 17:31:00	Incoming	8C861EBAEC23	Jim's Device	Apple
Akeem Jensen	18612229018		2018-10-17 16:50:00	Incoming	8C861EBAEC23	Jim's Device	Apple
	3904567733		2018-10-17 16:43:00	Incoming	8C861EBAEC23	Jim's Device	Apple
Akeem Jensen	18612229018		2018-10-29 13:37:00	Missed	8C861EBAEC23	Jim's Device	Apple
	3904567733		2018-10-29 13:06:00	Missed	8C861EBAEC23	Jim's Device	Apple
Rhonda Cote	14795835251		2018-10-29 09:25:00	Missed	8C861EBAEC23	Jim's Device	Apple
Jin Contreras	9029306440		2018-10-28 11:45:00	Missed	8C861EBAEC23	Jim's Device	Apple
	8927942810		2018-10-26 20:45:00	Missed	8C861EBAEC23	Jim's Device	Apple

Forensic Artifacts

- Contacts
  - All contact details contained on the phone are copied onto the vehicle.

ARTIFACT INFORMATION

First Name	**Akeem**
Last Name	**Jensen**
Phone Number(s)	**(579) 259-1955, (861) 222-9018, 1 (338) 123-4572, 1-663-721-0007**
Email Address	**eleifend.nunc@urnasuscipit.org**
Device ID	**8C861EBAEC23**
Device Name	**Jim's Device**
Device Type	**Apple**
Device Model	**iPhone12,3**
Vehicle Make	**Ford**
Description	**Ford Sync Gen3**

EVIDENCE (531) — Column view

First...	Last...	Com...	Phone Number(s)	Email Address
Akeem	Jensen		(579) 259-1955, (861) 222-9018, 1 (338) 123-4572, 1...	eleifend.nunc@urnasuscipit.org
Jin	Contreras		(493) 420-1022, (902) 930-6440, 1 (244) 824-2105, 1...	tristique.ac@tempusloremfring
Eleanor	Hardy		(390) 456-7733, (391) 733-8580, 1 (153) 205-8018, 1...	vestibulum@feugiat.net
Rhonda	Cote		(440) 951-4121, (479) 583-5251, 1 (502) 840-1172, 1...	scelerisque@aliquetodioEtiam.c
Macy	Salazar		(782) 888-4844, (892) 794-2810, 1 (133) 525-0453, 1...	felis.adipiscing@eunequepeller
Kenyon	Evans		(585) 254-8743, (687) 675-5339, 1 (933) 866-6243, 1...	Sed.eget.lacus@in.net
Hadley	Bell		(427) 295-4996, (904) 206-6849, 1 (297) 541-1052, 1...	quis@ametdiam.net
Ella	Osborne		(368) 223-5058, (720) 769-9476, 1 (934) 495-2224, 1...	lacus@maurisutmi.com
Ira	Hardy		(510) 450-6751, (556) 523-3644, 1 (556) 655-3936, 1...	neque@justosit.net
Kylee	Rodriguez		(354) 896-7542, (857) 992-3702, 1 (507) 413-6337, 1...	Praesent.luctus.Curabitur@sem
Uriah	Elliott		(407) 323-8458, (994) 626-3761, 1 (265) 473-3564, 1...	vitae.dolor@eros.com
Judith	York		(188) 831-1999, (612) 790-8488, 1 (416) 798-9428, 1...	Cum@famesac.com
Jason	Flynn		(335) 868-1488, (829) 356-6942, 1 (311) 805-8260, 1...	nisi@lorem.ca
Desirae	Burris		(604) 557-6137, (666) 372-4136, 1 (722) 234-8813, 1...	mus@Nullaeuneque.co.uk
Ivan	Gordon		(400) 240-5076, (454) 255-7337, 1 (558) 431-3125, 1...	lorem.ipsum@tristiquenequeve
Lucius	Mccall		(564) 573-3359, (811) 204-3672, 1 (268) 765-1722, 1...	neque.Sed.eget@Namconsequ
Aubrey	Crawford		(228) 148-2325, (474) 280-7997, 1 (652) 363-5802, 1...	scelerisque.mollis@luctuset.cor
Gay	Velazquez		(395) 395-5481, (763) 497-3142, 1 (261) 885-0766, 1...	nisi@fermentumvel.edu
Gavin	Carney		(208) 345-1346, (405) 719-8612, 1 (978) 560-4737, 1...	ipsum.non@congueln.net
Lara	Frost		(219) 627-9338, (380) 762-4623, 1 (551) 413-3181, 1...	auctor.ullamcorper.nisl@enimg
Chancellor	Cash		(244) 941-9707, (480) 399-4784, 1 (873) 923-8314, 1...	Sed.eu.nibh@luctusvulputateni
Genevieve	Cohen		(966) 690-3485, (992) 210-8874, 1 (955) 690-5521, 1...	nec.mauris@eget.com
Pandora	Foley		(145) 311-7506, (541) 750-8106, 1 (912) 628-6613, 1...	vitae.sodales.nisi@orcilobortis.c
Adrienne	David		(167) 226-8276, (438) 195-7026, 1 (963) 282-4840, 1...	risus@lacusNulla.org
Larissa	Crawford		(420) 818-4606, (717) 722-8172, 1 (574) 128-4868, 1...	non.leo@euismodet.net
Keith	Romero		(472) 614-8831, (635) 214-9549, 1 (919) 618-8352, 1...	Nullam.lobortis.quam@libero.o
Inga	Stark		(129) 933-9214, (132) 741-4811, 1 (892) 714-6440, 1...	molestie.Sed.id@interdum.co.u
Uriel	Bird		(241) 529-4711, (826) 300-6773, 1 (755) 522-8838, 1...	eget.nisi@felis.com

Forensic Artifacts

- Files
  - Lifestyle analysis
    - Listening History

File Path	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\storage\bk1\MediaIAP2_28.db
Original Path	C:\SG3-eMMC\p6\storage\bk1\MediaIAP2_28.db
Device ID	8C861EBAEC23
Device Name	Jim's Device
Device Type	Apple
Device Model	iPhone12,3
Vehicle Make	Ford
Description	Ford Sync Gen3

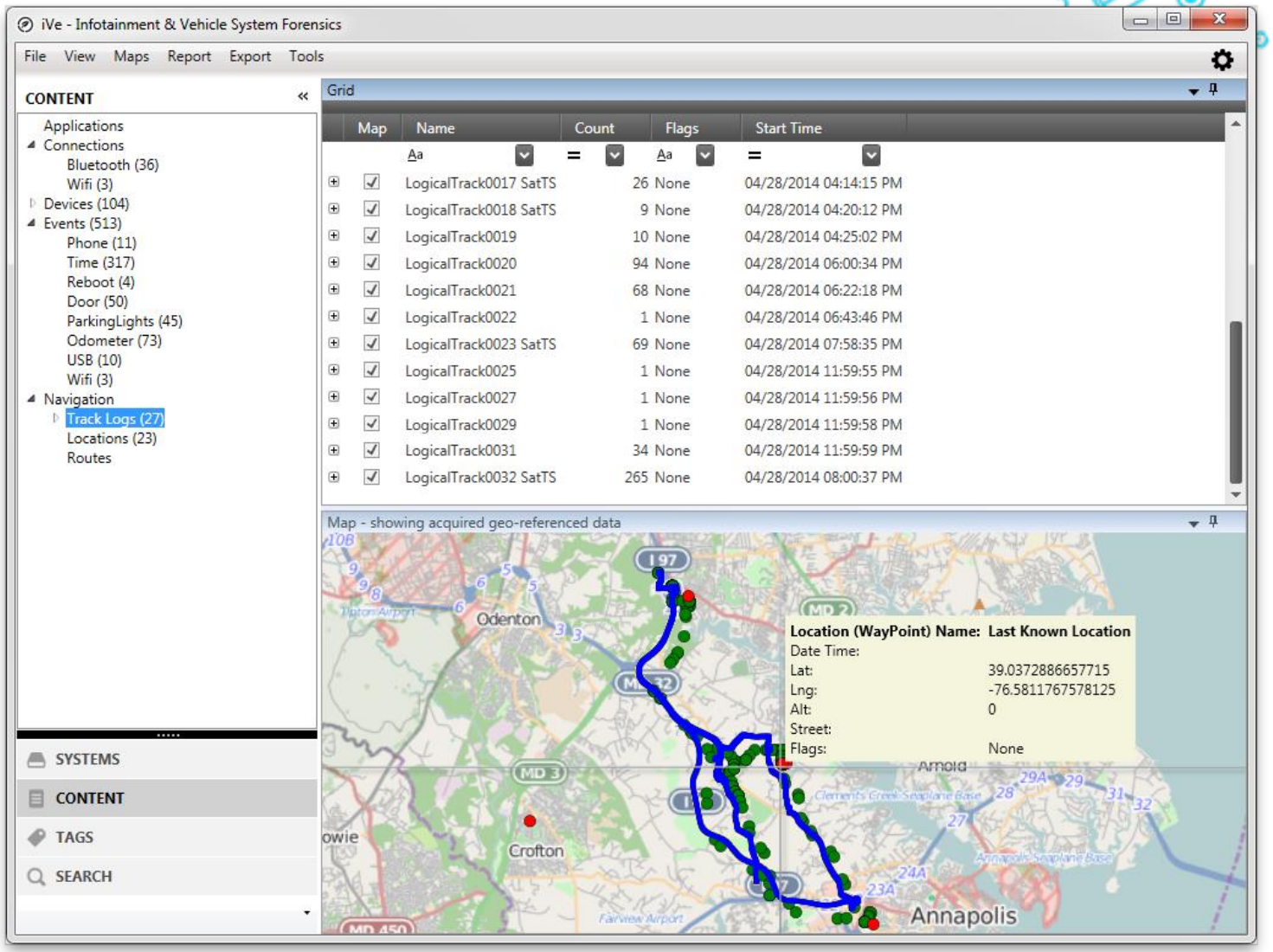
EVIDENCE (12,725)

Column view

File Name	File Path	Original Path
Roar	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
Live While We're Young	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
What Makes You Beautiful	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
Cruise	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
Story of My Life	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
028: The Price of Freedom	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
080: A Prisoner for Christ	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
082: Heatwave	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
087: Elijah, Part 1 Of 2	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
088: Elijah, Part 2 Of 2	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
088a: BONUS! Creating the Sounds for "Elijah"	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
089: That's Not Fair!	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
090: But, You Promised	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
091: A Mission for Jimmy	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
091a: BONUS! The Production of "a Mission for Ji...	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
092: The Ill-Gotten Deed	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
092a: BONUS! The Voices of Host Chris Anthony, f...	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
093: Rescue from Manatugo Point	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
102: The Treasure of LeMonde!	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
102a: BONUS! The Very First Focus dramas - Spar...	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
102b: BONUS! Spare Tire	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
102c: BONUS! House Guest	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
066: the Imagination Station, Pt. 1 of 2	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
067: the Imagination Station, Pt. 2 of 2	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
067A: the Creation of the Imagination Station (Bo...	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
072: an Encounter With Mrs. Hooper	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
073: a Bite of Applesauce	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6
073A: the Inspiration For "A Bite of Applesauce" (...	C:\Users\Ben LeMere\Desktop\Truck\SG3-eMMC\p6\sto...	C:\SG3-eMMC\p6

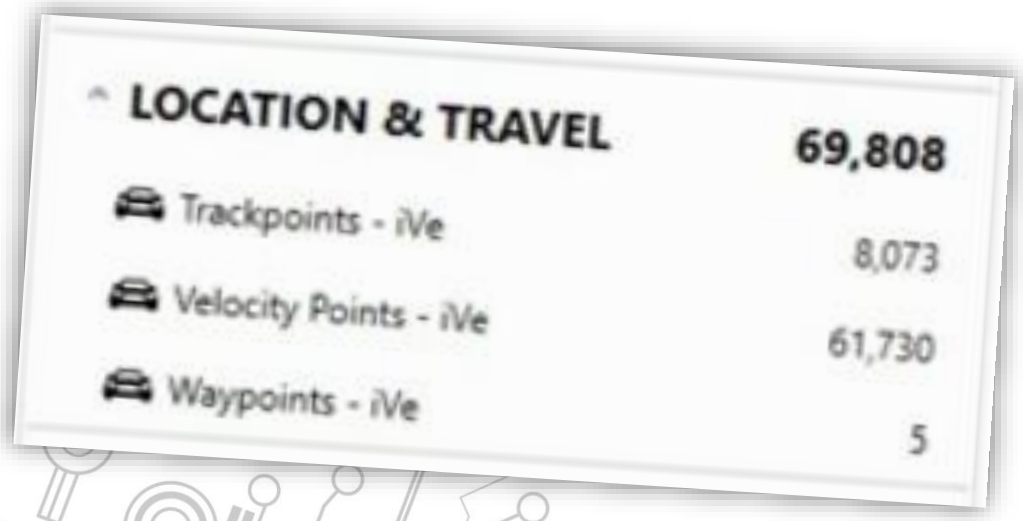
Track Logs

- Connected Devices
  - Rental Car



Forensic Artifacts

- Track Logs
  - Location history
  - Lifestyle analysis
  - Different that CDR (Crash Data Recorder)



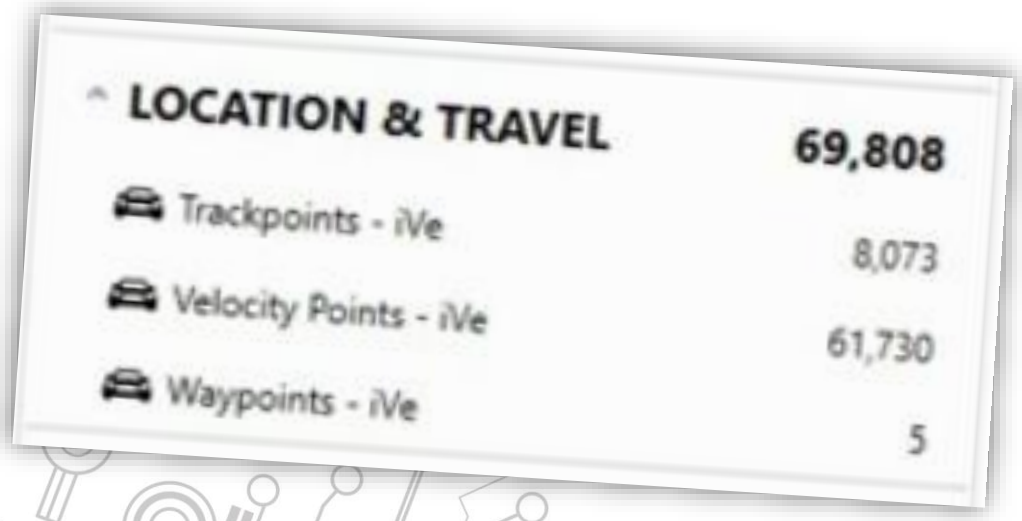
EVIDENCE (8,073)

Column view

Track Na...	Date/Time - Local Time	Latitude	Longitude	Geohash	
Track 001	2020-08-14 15:02:11	38.987276	-76.574943	dqctc3rv6e00	0
Track 001	2020-08-14 15:02:14	38.987167	-76.575157	dqctc3rstw8q	1
Track 001	2020-08-14 15:02:14	38.987186	-76.575184	dqctc3rsufhr	7
Track 001	2020-08-14 15:02:12	38.987124	-76.57517	dqctc3rsmnwv	3
Track 001	2020-08-14 15:02:20	38.987324	-76.575594	dqctc3rme7fw	1
Track 001	2020-08-14 15:02:21	38.987349	-76.575679	dqctc3rmc2e5	1
Track 001	2020-08-14 15:02:23	38.987379	-76.575757	dqctc3rjzw1n	1
Track 001	2020-08-14 15:02:23	38.987408	-76.575846	dqctc3rnj7we	1
Track 001	2020-08-14 15:02:24	38.987437	-76.57593	dqctc3rn7900	1
Track 001	2020-08-14 15:02:26	38.987466	-76.576015	dqctc3rn3w2t	1
Track 001	2020-08-14 15:02:27	38.987494	-76.576097	dqctc3qyxees	1
Track 001	2020-08-14 15:02:27	38.987522	-76.576186	dqctc3qyv8c5	1
Track 001	2020-08-14 15:02:28	38.987547	-76.576272	dqctc3qygt90	1
Track 001	2020-08-14 15:02:29	38.987566	-76.576358	dqctc3qz190f	1
Track 001	2020-08-14 15:02:30	38.987576	-76.576433	dqctc3qxpfcj	1
Track 001	2020-08-14 15:02:31	38.987584	-76.576509	dqctc3qxnh2m	1
Track 001	2020-08-14 15:02:32	38.98759	-76.57658	dqctc3qxhme3	1
Track 001	2020-08-14 15:02:34	38.987603	-76.57664	dqctc3qx4zyw	1
Track 001	2020-08-14 15:02:34	38.987628	-76.5767	dqctc3qx3s9u	1
Track 001	2020-08-14 15:02:36	38.987666	-76.576739	dqctc3qx8esy	1
Track 001	2020-08-14 15:02:36	38.987707	-76.576747	dqctc3qxb7qg	1
Track 001	2020-08-14 15:02:37	38.987744	-76.576729	dqctc3w80fhr	9
Track 001	2020-08-14 15:02:38	38.987797	-76.576682	dqctc3w83upk	1
Track 001	2020-08-14 15:02:39	38.987865	-76.576607	dqctc3w8g8z3	2
Track 001	2020-08-14 15:02:41	38.987945	-76.576522	dqctc3w9jxww	2
Track 001	2020-08-14 15:02:41	38.988031	-76.576431	dqctc3w9xzf8	2
Track 001	2020-08-14 15:02:43	38.988128	-76.576339	dqctc3wf3cz4	2
Track 001	2020-08-14 15:02:43	38.988229	-76.576251	dqctc3wfuh8t	3

Forensic Artifacts

- Velocity Points
  - Driving patterns
  - Different that CDR (Crash Data Recorder)



EVIDENCE (61,730)

Column view

Trac...	Point...	Date/Time - Local...	Velocity	Vehi...	Descrip...	Source
Track 001	85	2020-08-14 15:02:05.078	0.0	Ford	Ford Sync Gen3	Entire Disk (Micrc
Track 001	85	2020-08-14 15:02:05.465	0.15534275	Ford	Ford Sync Gen3	Entire Disk (Micrc
Track 001	85	2020-08-14 15:02:05.465	0.62758471	Ford	Ford Sync Gen3	Entire Disk (Micrc
Track 001	85	2020-08-14 15:02:07.965	0.8699194	Ford	Ford Sync Gen3	Entire Disk (Micrc
Track 001	85	2020-08-14 15:02:07.982	1.04390328	Ford	Ford Sync Gen3	Entire Disk (Micrc
Track 001	85	2020-08-14 15:02:08.006	1.37322991	Ford	Ford Sync Gen3	Entire Disk (Micrc
Track 001	85	2020-08-14 15:02:08.021	1.57206863	Ford	Ford Sync Gen3	Entire Disk (Micrc
Track 001	85	2020-08-14 15:02:08.023	1.65284686	Ford	Ford Sync Gen3	Entire Disk (Micrc
Track 001	85	2020-08-14 15:02:08.041	1.77712106	Ford	Ford Sync Gen3	Entire Disk (Micrc
Track 001	85	2020-08-14 15:02:08.042	1.82683074	Ford	Ford Sync Gen3	Entire Disk (Micrc
Track 001	85	2020-08-14 15:02:08.042	1.73362509	Ford	Ford Sync Gen3	Entire Disk (Micrc
Track 001	85	2020-08-14 15:02:08.097	1.59692347	Ford	Ford Sync Gen3	Entire Disk (Micrc
Track 001	85	2020-08-14 15:02:08.099	1.46643556	Ford	Ford Sync Gen3	Entire Disk (Micrc
Track 001	85	2020-08-14 15:02:08.108	1.23652829	Ford	Ford Sync Gen3	Entire Disk (Micrc
Track 001	85	2020-08-14 15:02:08.113	0.9941936	Ford	Ford Sync Gen3	Entire Disk (Micrc
Track 001	85	2020-08-14 15:02:08.126	0.75807262	Ford	Ford Sync Gen3	Entire Disk (Micrc
Track 001	85	2020-08-14 15:02:08.155	0.56544761	Ford	Ford Sync Gen3	Entire Disk (Micrc
Track 001	85	2020-08-14 15:02:08.155	0.35418147	Ford	Ford Sync Gen3	Entire Disk (Micrc
Track 001	85	2020-08-14 15:02:08.156	0.24233469	Ford	Ford Sync Gen3	Entire Disk (Micrc
Track 001	85	2020-08-14 15:02:08.156	0.1864113	Ford	Ford Sync Gen3	Entire Disk (Micrc
Track 001	85	2020-08-14 15:02:08.158	0.14291533	Ford	Ford Sync Gen3	Entire Disk (Micrc
Track 001	85	2020-08-14 15:02:08.174	0.08077823	Ford	Ford Sync Gen3	Entire Disk (Micrc
Track 001	85	2020-08-14 15:02:08.260	0.01864113	Ford	Ford Sync Gen3	Entire Disk (Micrc
Track 001	85	2020-08-14 15:02:08.266	0.0	Ford	Ford Sync Gen3	Entire Disk (Micrc
Track 001	85	2020-08-14 15:02:10.360	0.02485484	Ford	Ford Sync Gen3	Entire Disk (Micrc
Track 001	85	2020-08-14 15:02:10.470	0.31689921	Ford	Ford Sync Gen3	Entire Disk (Micrc
Track 001	85	2020-08-14 15:02:10.572	0.50952422	Ford	Ford Sync Gen3	Entire Disk (Micrc
Track 001	85	2020-08-14 15:02:10.680	0.69593552	Ford	Ford Sync Gen3	Entire Disk (Micrc

Forensic Artifacts

- Waypoints
  - When and Where

EVIDENCE (5)

Column view

Name	Date/Time - Local Time	Latitude	Longitude
300 W Station Square Dr, Pittsburgh, PA 15219, USA	2017-12-22 20:35:49	40.43495	-80.00745
152 Station Sq, Pittsburgh, PA 15219, USA	2018-05-04 22:33:49	40.4333367391304	-80.0043539130435
White River Junction, VT 05001, USA	2018-08-11 08:57:16	43.66375	-72.38827
2684 Lebanon Rd, Manheim, Rapho Twp, PA 17545,...	2019-02-13 14:36:14	40.22706	-76.43192
445 Defense Hwy, Annapolis, MD 21401, USA	2020-08-19 16:34:54	38.98896	-76.57628

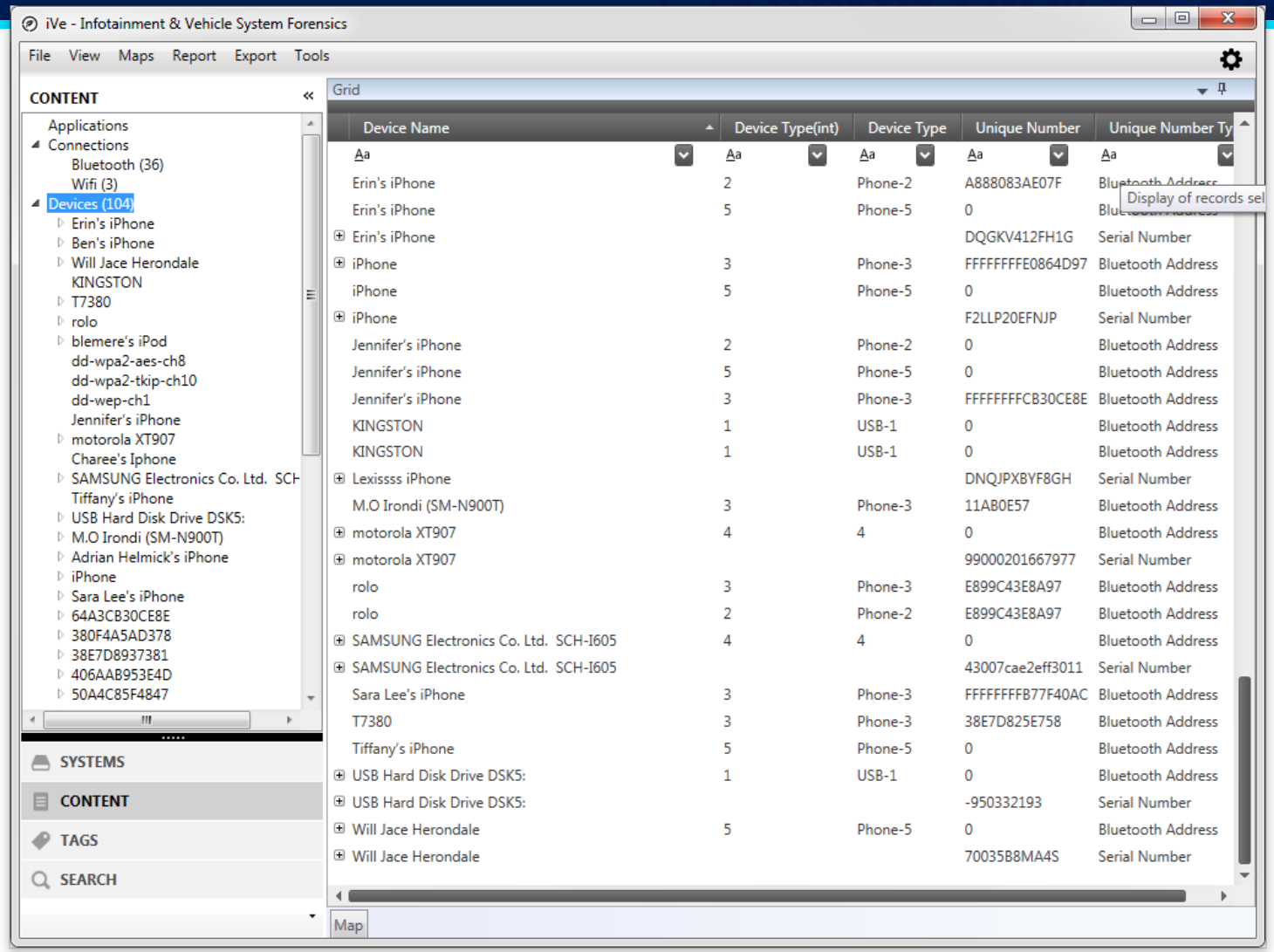
Forensic Artifacts

- Locally Accessed Files and Folders
  - Did they store files locally?
    - Data theft
    - Improper usage
    - Company policies

Path	Accessed Date/Time...
C:\Users\Accounting new\Desktop\Invoices\Picture [redacted]7.pdf	2019-06-14 14:55:00
C:\Users\Accounting new\Desktop\Invoices\Picture [redacted]7.pdf	
C:\Users\Accounting[redacted]	2019-06-14 14:57:16
C:\Users\Accounting new\AppData\Local\Packages\Microsoft.MicrosoftEdge_8w...	2019-05-22 14:35:33
C:\Users\Accounting new\Desktop\Paypal Transactions.csv.xlsx	2019-05-21 13:14:40
C:\Users\Accounting new\Desktop\SHOP INVENTORY SHEET-[redacted].xls	2019-05-21 15:14:58
C:\Users\Accounting new\Desktop\Invoices\M[redacted]5.pdf	2019-05-20 14:31:52
C:\Users\Accounting new\Desktop\Commercial Invoices\Bh[redacted]13...	2019-05-22 11:31:00
C:\Users\Accounting new\Dropbox\Public\pricelist[redacted]order_form_4-16-1...	2019-05-20 09:56:00
C:\Users\Accounting new\Desktop\Commercial Invoices\COMMERCIAL INVOICE...	2019-05-21 08:32:12
C:\Users\Accounting new\Desktop\PAYDATES.xlsx	2019-05-20 11:55:07
C:\Users\Accounting new\AppData\Local\Packages\Microsoft.MicrosoftEdge_8w...	2019-05-22 14:38:44
C:\Users\Accounting new\Desktop\Invoices\W[redacted].pdf	2019-05-23 14:54:13
C:\Users\Accounting new\Desktop\WIRE TRANSFER[redacted].doc	2019-05-20 14:35:15
C:\Users\Accounting new\Desktop\Credit Card Coding.xlsx	2019-05-21 13:52:59
C:\Users\Accounting new\Desktop\Commercial Invoices\Tracking number[redacted]...	2019-05-22 10:30:21

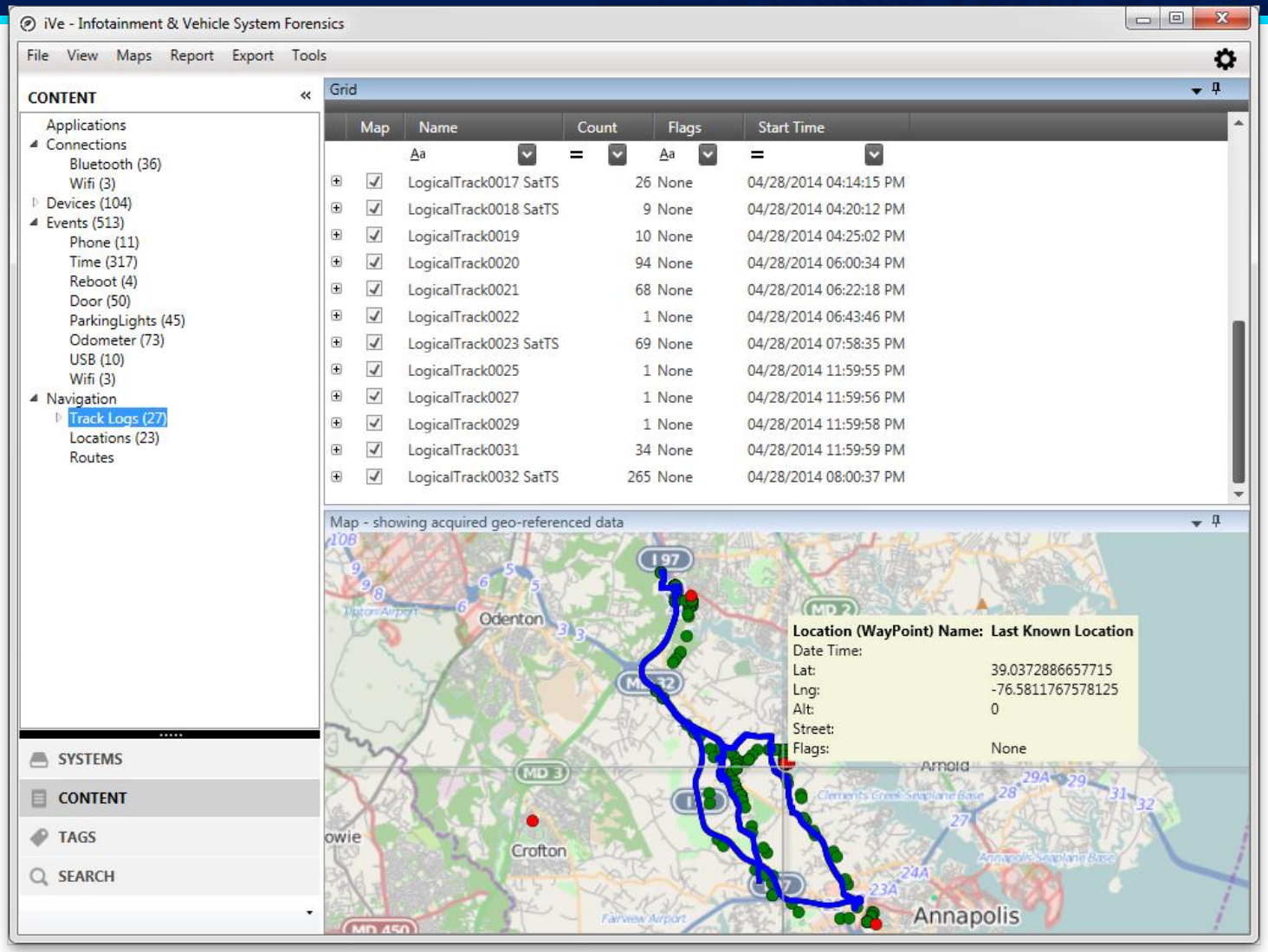
IoT Investigations

- Vehicle Forensics
  - In-vehicle infotainment
  - Vehicle telematics
- Connected devices



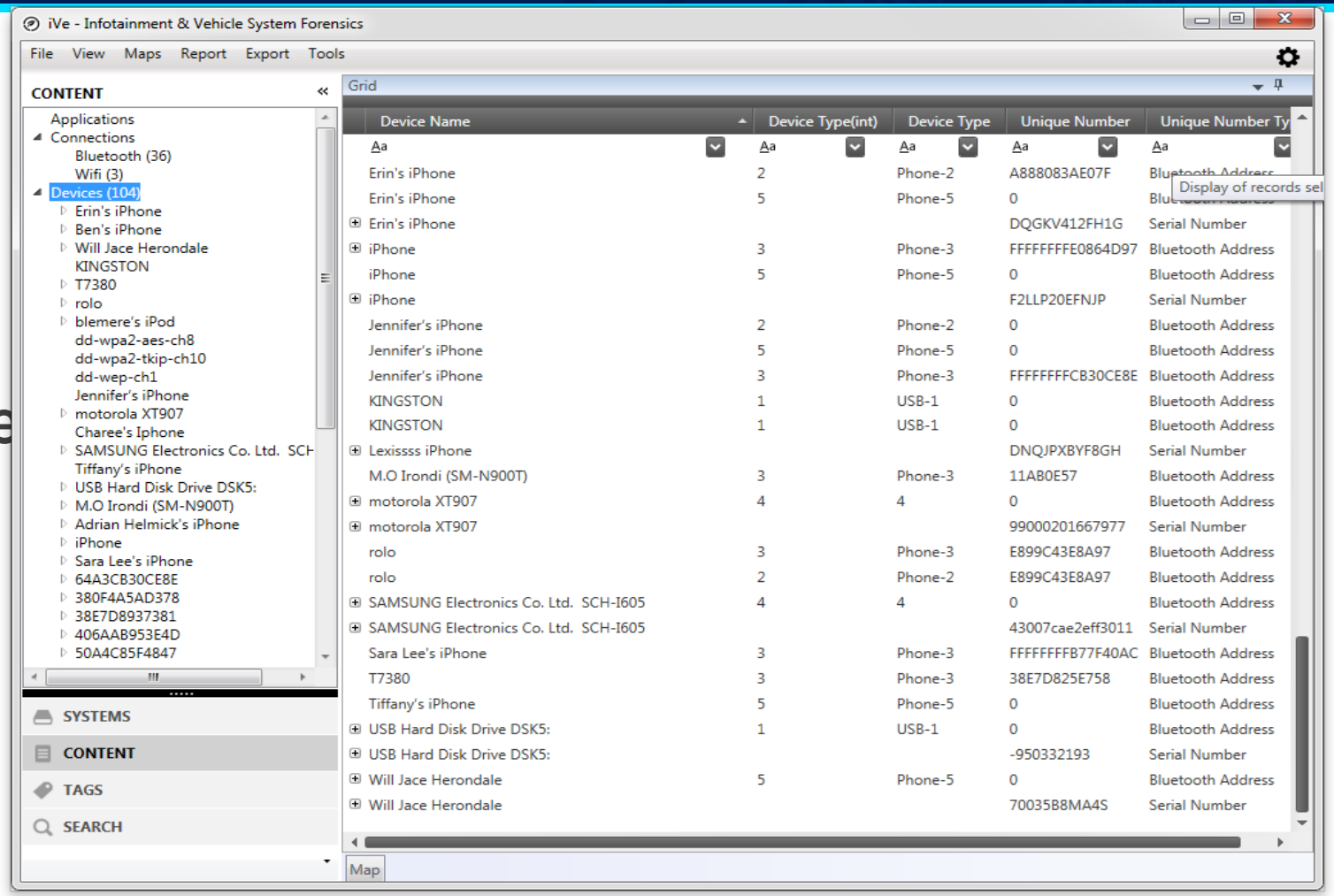
IoT Investigations

- Vehicle Forensics
  - In-vehicle infotainment
  - Vehicle telematics
- Track logs



IoT Investigations

- Vehicle Forensics
  - In-vehicle infotainment
  - Vehicle telematics
- Velocity Logs
  - Vehicle velocity and corre



Teleporting Car?

- Rental car location records
- Original data needed.

ENVISTA FORENSICS

LARRY DANIEL
TECHNICAL DIRECTOR– DIGITAL FORENSICS

SMART HOME

DIGITAL FORENSICS //

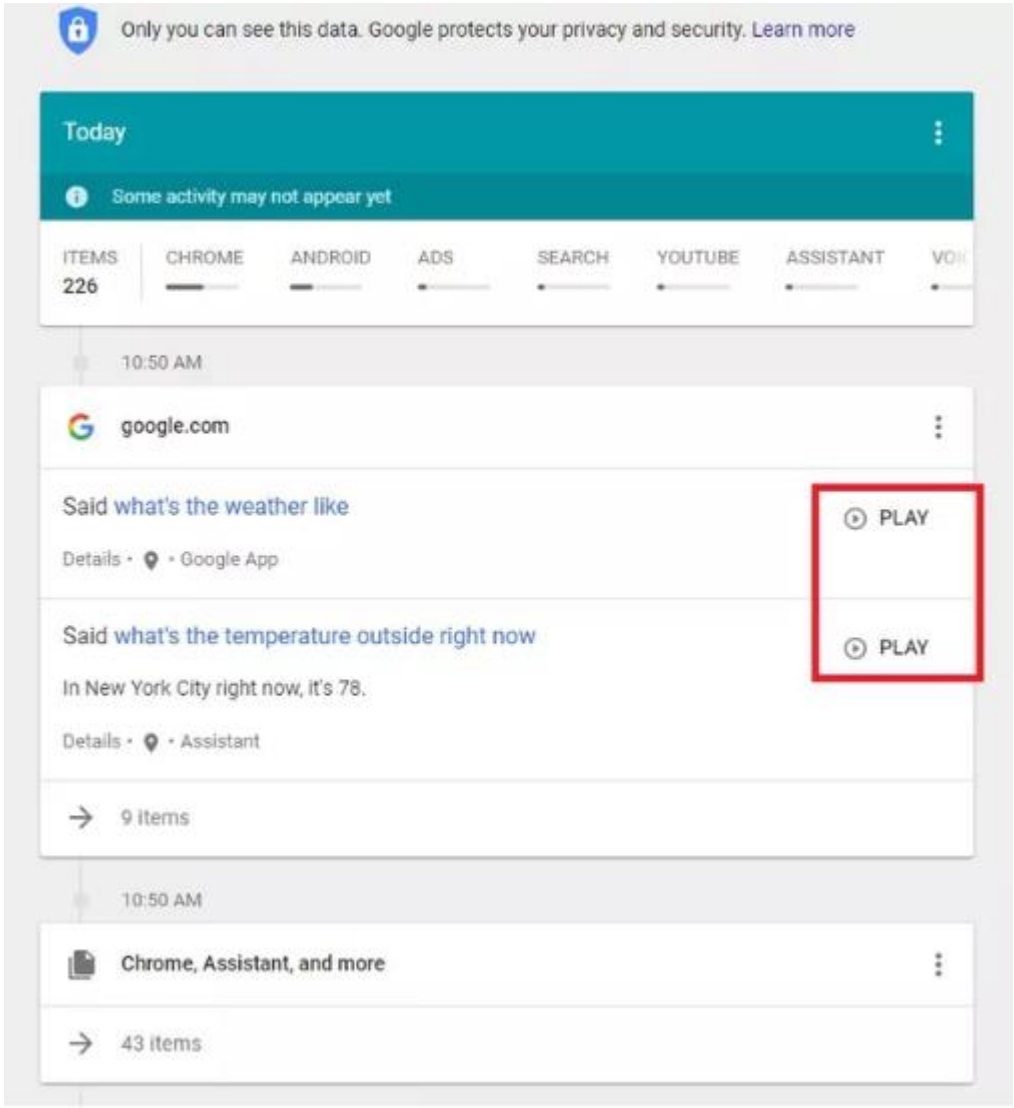
Alexa as a home assistant

- Murder case – *Arkansas v. Bates*, No. CR-2016-370 (Cir. Ct. Benton County, Arkansas).
  - Police seized the defendant's smart speaker believing it might contain evidence of what happened the night of the murder at defendant's home.
    - Amazon moved to quash warrant, contenting 1st amendment rights to publish and speak through the speaker
    - Motion later mooted when defendant gave manufacturer permission to turn over audio recordings
      - Recordings kept by Amazon, organized and identifiable (not-anonymized for "research")
      - Only contained provider side

https://www.crowelldatalaw.com/2017/07/recent-iot-device-cases/

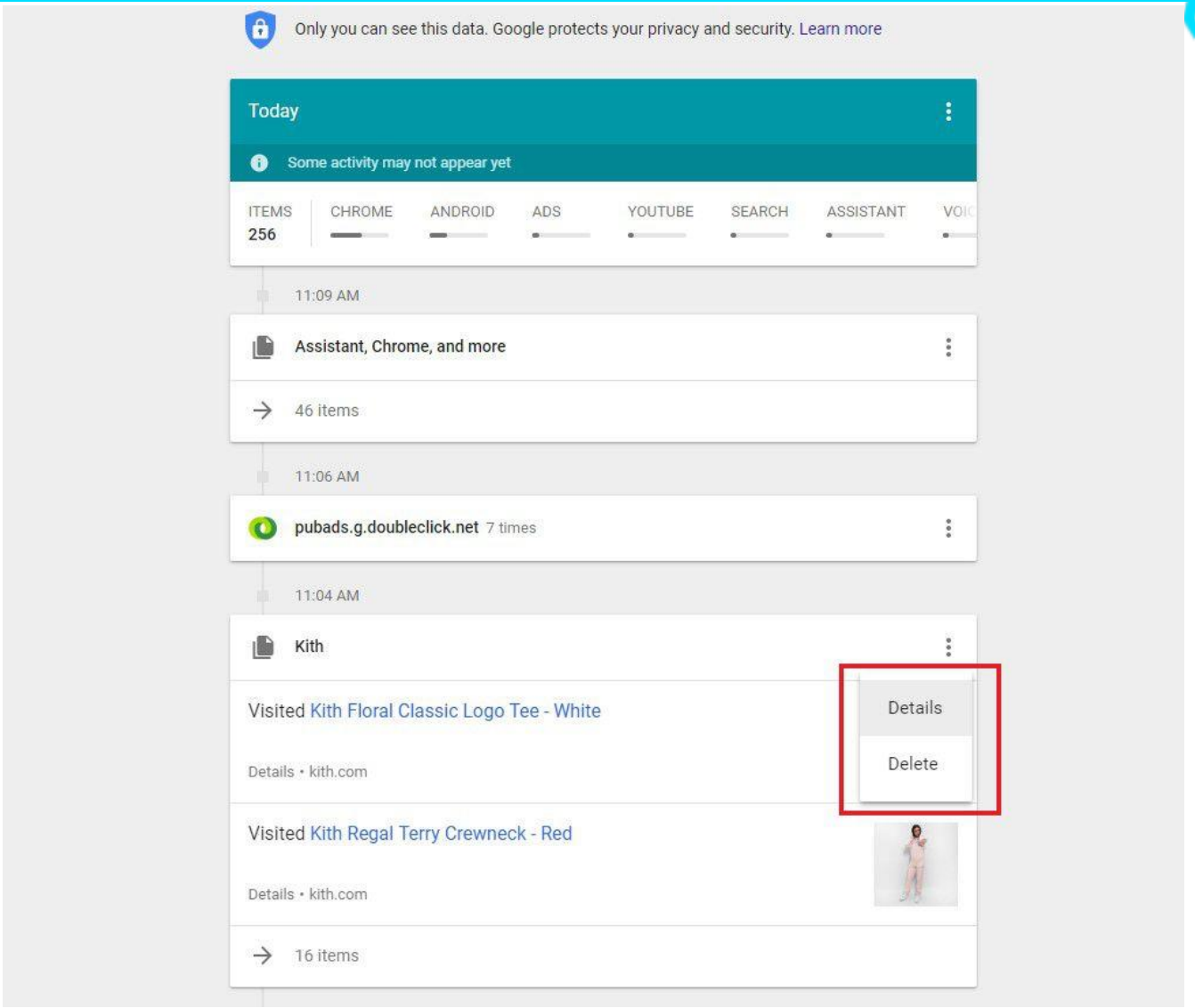
Smart Home Assistants

- Google Home
  - Google queries



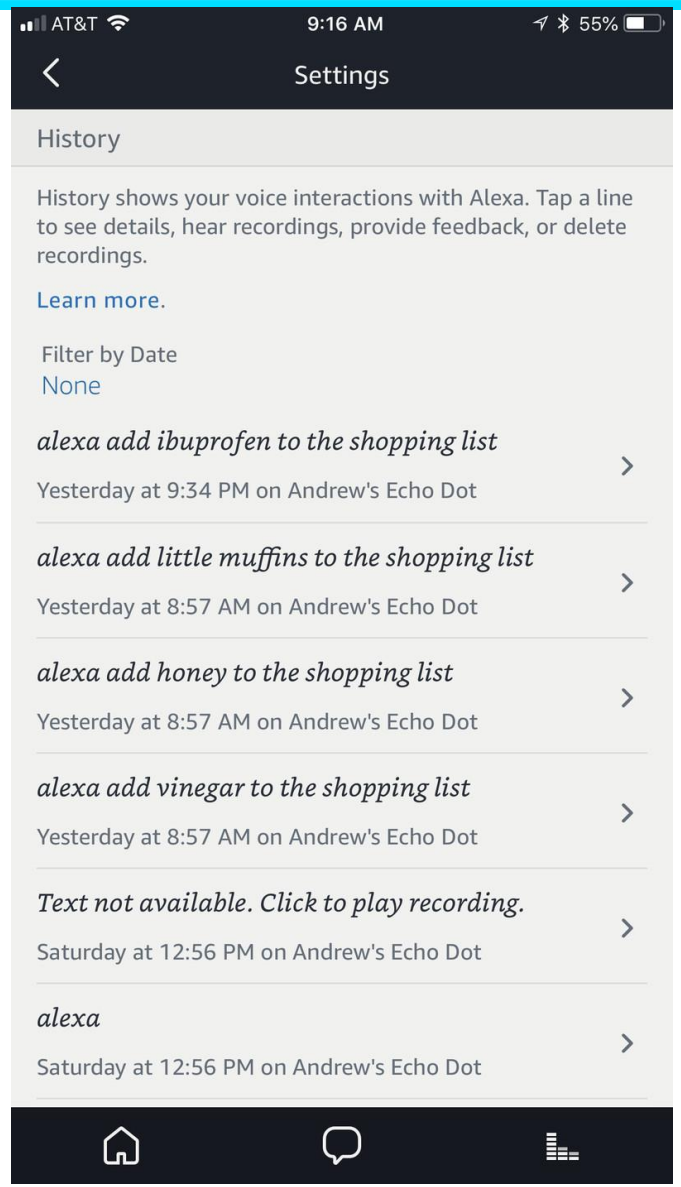
Smart Home Assistants

- Google Home
  - Shopping



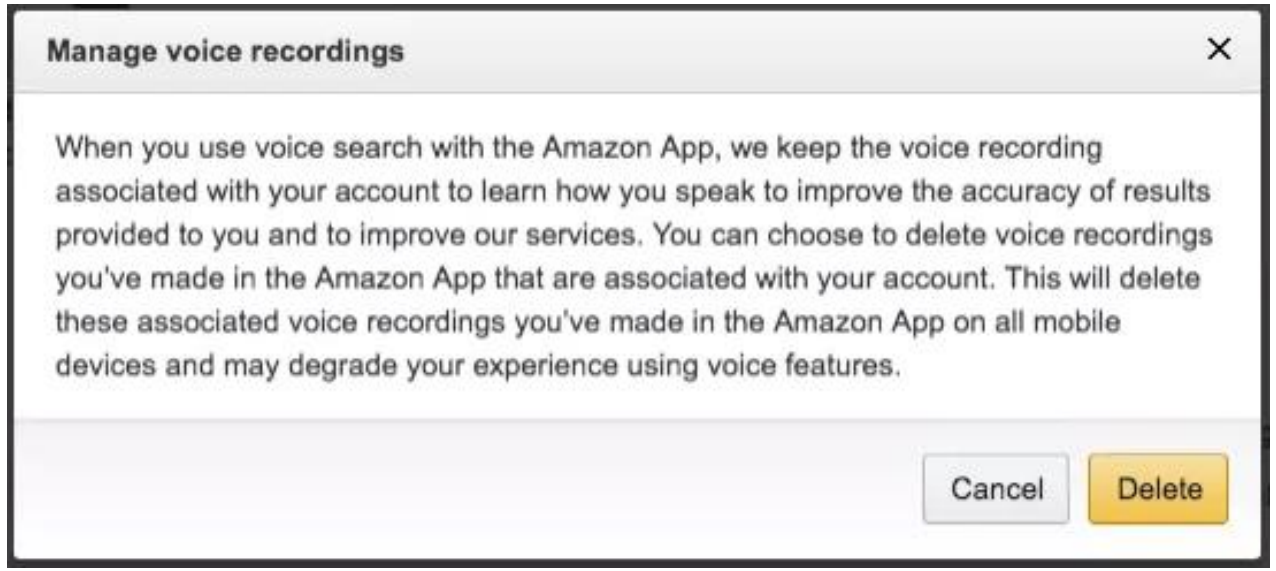
Smart Home Assistants

- Amazon Alexa
  - Search queries



Smart Home Assistants

- Amazon Alexa
  - Voice recordings



Smart Home Assistants

- Interrogate the device
  - Low tech works too…
    - Careful with the Christmas lists!

Smart Home Security

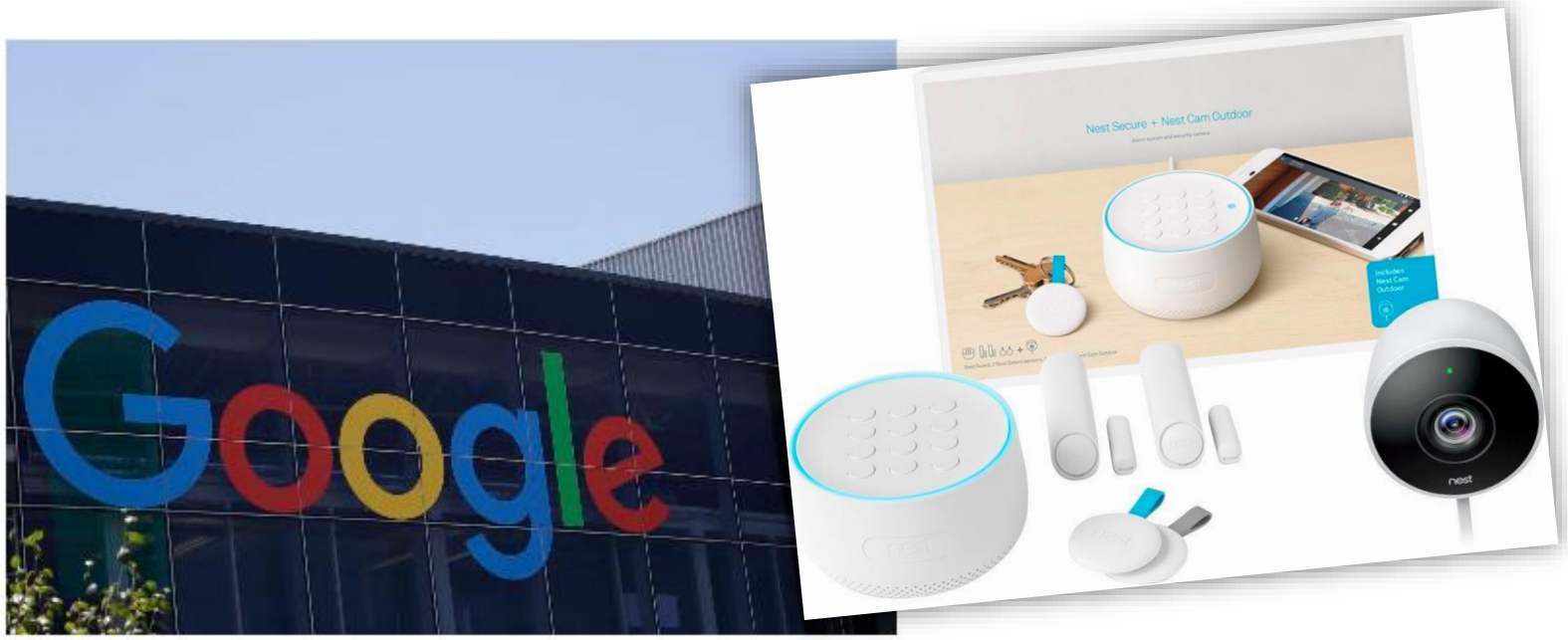
- Recording video
- Timeline data
- Account data

Smart Home Security

- Recording video
- Timeline data
- Account data
- Hidden microphone

Business

Google failed to notify customers it put microphones in Nest security systems



https://www.washingtonpost.com/business/2019/02/20/google-forgot-notify-customers-it-put-microphones-nest-security-systems/?noredirect=on&utm_term=.cfa73cc39212

Smart Home Security

- Nest – Neighbors home

Smart Home Security

- Nest – Neighbors home

https://nest.com/video/clip/burglar-tries-to-steal-nest-cam/

Smart Home Cameras

- Collecting Biometric Data
  - The Nest Hello doorbell recognizes familiar faces to tell you who's come calling and the Nest Cam IQ Indoor and Nest Cam IQ Outdoor both use it to keep tabs on who's at home or just outside.

ENVISTA FORENSICS

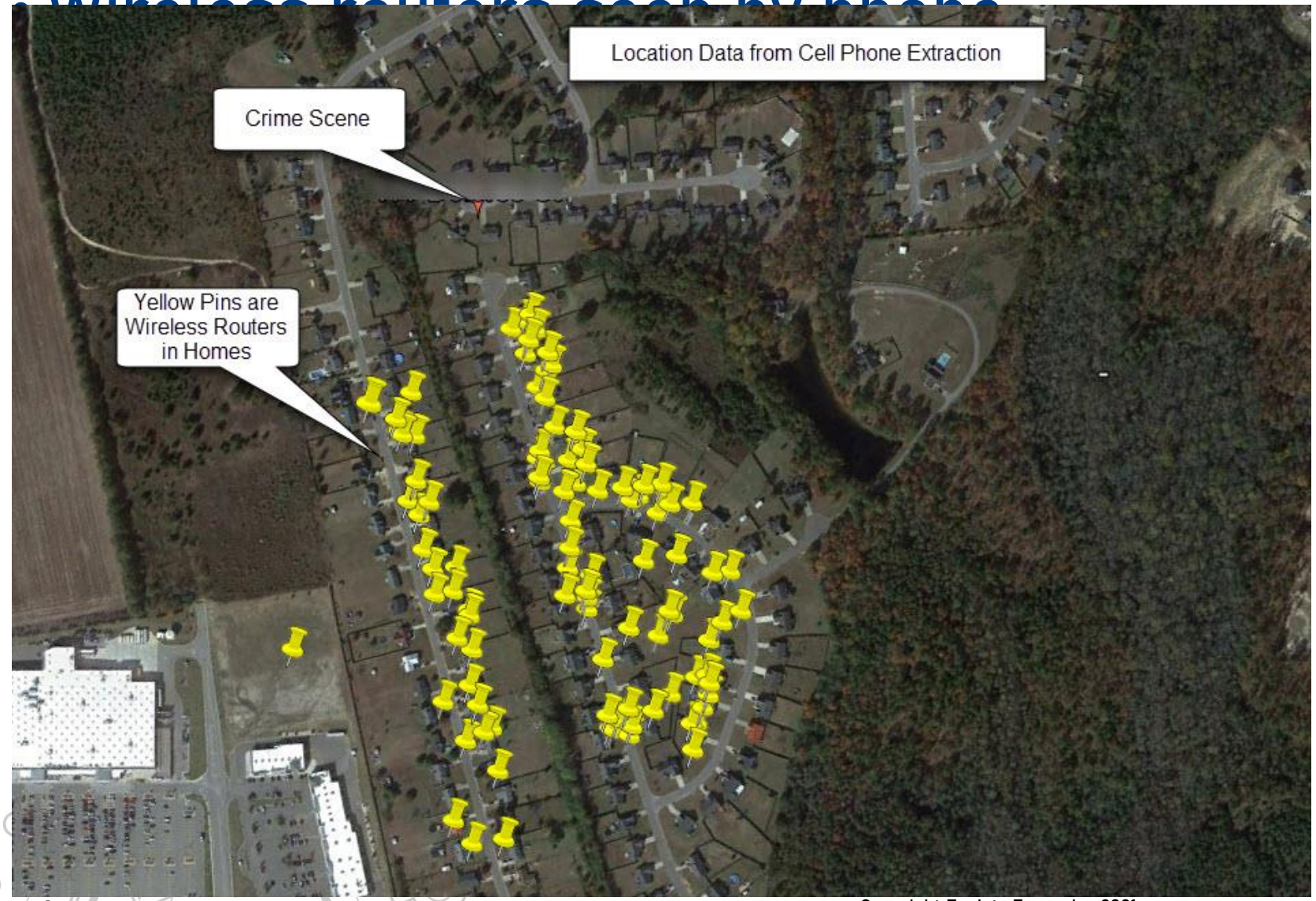
LARRY DANIEL
TECHNICAL DIRECTOR– DIGITAL FORENSICS

CASE EXAMPLES

DIGITAL FORENSICS //

Case Example: WiFi Phone Location

- Wireless routers seen by phone



Capabilities: Examples

- Location
  - Wireless Networks

	Timestamp	Description	Category	Name
	4/1/2016 9:30:32 AM(UTC-4)	GooglePlay	Wireless Networks	Bill Wi the Science Fi (e4:f4:c6:0b:5f:51)
	3/31/2016 12:26:16 PM(UTC-4)	GooglePlay	Wireless Networks	Bill Wi the Science Fi (e4:f4:c6:0b:5f:51)
	3/31/2016 12:06:15 PM(UTC-4)	GooglePlay	Wireless Networks	Bill Wi the Science Fi (e4:f4:c6:0b:5f:51)
	3/31/2016 12:00:30 PM(UTC-4)	GooglePlay	Wireless Networks	Bill Wi the Science Fi (e4:f4:c6:0b:5f:51)
	3/30/2016 10:38:17 AM(UTC-4)	GooglePlay	Wireless Networks	Bill Wi the Science Fi (e4:f4:c6:0b:5f:51)
	3/30/2016 8:13:03 AM(UTC-4)	YouTube	Wireless Networks	Bill Wi the Science Fi (e4:f4:c6:0b:5f:51)
	3/30/2016 8:08:37 AM(UTC-4)	YouTube	Wireless Networks	Bill Wi the Science Fi (e4:f4:c6:0b:5f:51)
	3/30/2016 8:04:30 AM(UTC-4)	YouTube	Wireless Networks	Bill Wi the Science Fi (e4:f4:c6:0b:5f:51)
	3/30/2016 8:00:35 AM(UTC-4)	YouTube	Wireless Networks	Bill Wi the Science Fi (e4:f4:c6:0b:5f:51)
	3/30/2016 7:56:44 AM(UTC-4)	YouTube	Wireless Networks	Bill Wi the Science Fi (e4:f4:c6:0b:5f:51)
	3/30/2016 7:53:09 AM(UTC-4)	YouTube	Wireless Networks	Bill Wi the Science Fi (e4:f4:c6:0b:5f:51)
	3/30/2016 7:49:32 AM(UTC-4)	YouTube	Wireless Networks	Bill Wi the Science Fi (e4:f4:c6:0b:5f:51)
	3/30/2016 7:45:45 AM(UTC-4)	YouTube	Wireless Networks	Bill Wi the Science Fi (e4:f4:c6:0b:5f:51)
	3/30/2016 7:21:48 AM(UTC-4)	GooglePlay	Wireless Networks	FiOS-TA0VP (48:5d:36:55:34:38)
	3/30/2016 7:20:43 AM(UTC-4)	GooglePlay	Wireless Networks	FiOS-TA0VP (48:5d:36:55:34:38)
	3/30/2016 7:18:22 AM(UTC-4)	GooglePlay	Wireless Networks	FiOS-TA0VP (48:5d:36:55:34:38)
	3/29/2016 11:39:26 PM(UTC-4)	YouTube	Wireless Networks	FiOS-TA0VP (48:5d:36:55:34:38)

Wireless Network

Go to

BSSID:	e4:f4:c6:0b:5f:51
SSId:	Bill Wi the Science Fi
Security Mode:	
Last Connected:	
Last Auto Connected:	
Timestamp:	4/1/2016 9:30:32 AM(UTC-4)
End Time:	
Package:	GooglePlay
Extraction:	File System
Source file:	

Map

Position:	[redacted]
Map Address:	[redacted]

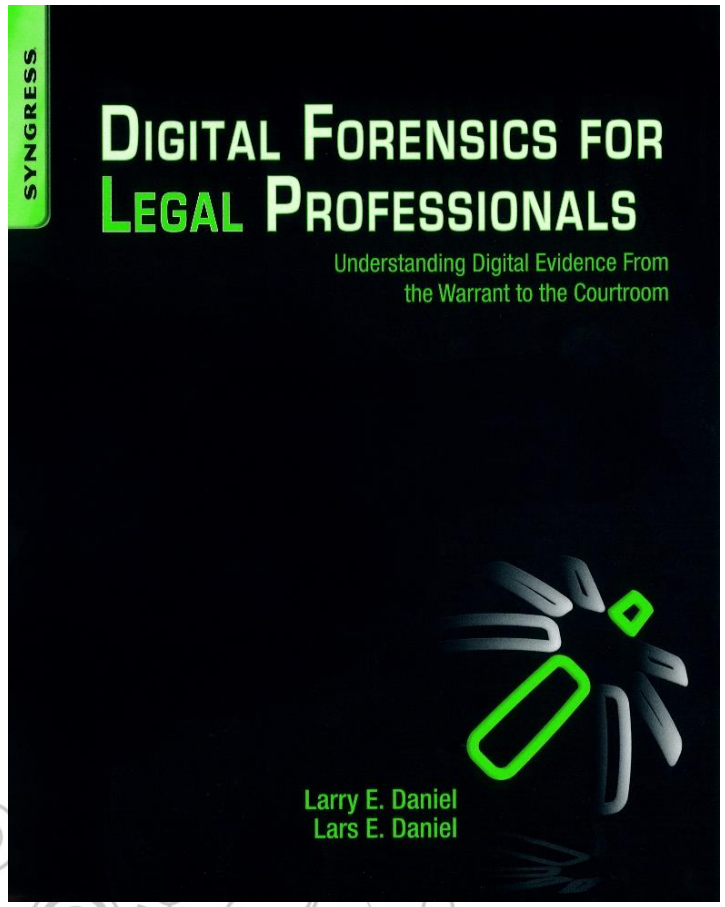
Examination of Plaintiff's Phone

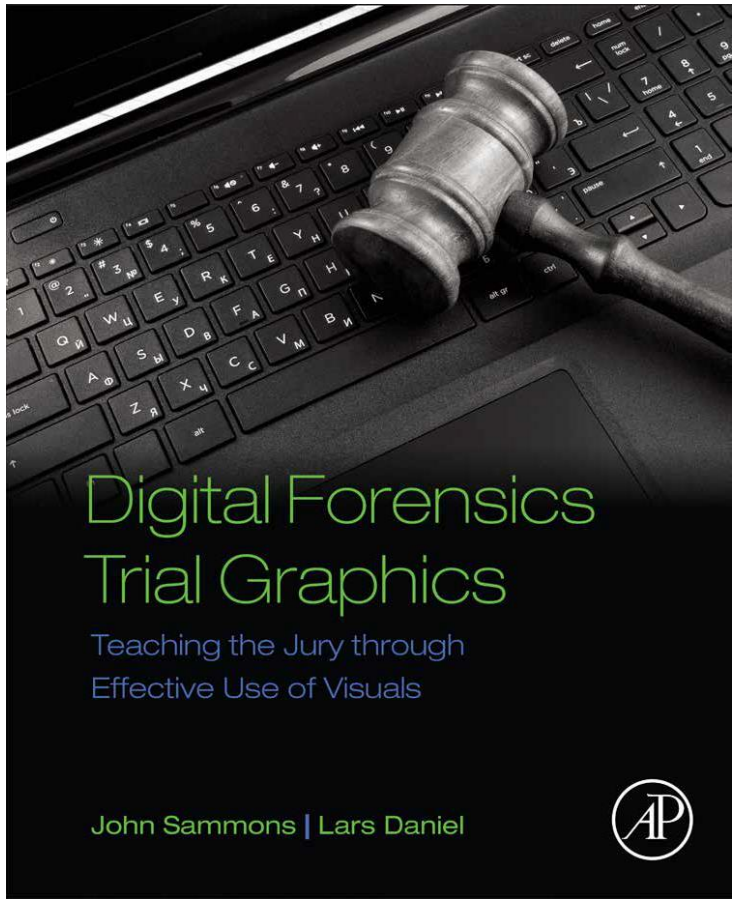
- Application data
  - Synced to account
  - and phone

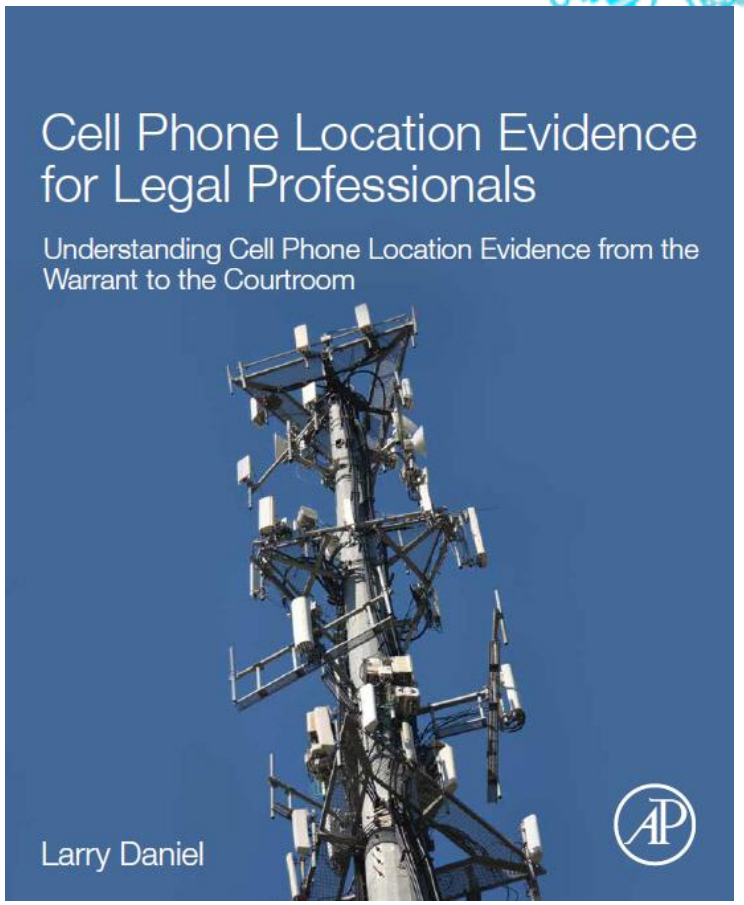
Time	Category	Item
11:48:44 AM(UTC-6)	DB	Phone (dialer.db)
11:48:44 AM(UTC-6)	Text File	com.android.dialer.xml
11:48:47 AM(UTC-6)	Picture	1841 task thumbnail.DELETED.png
11:48:55 PM(UTC-6)	E-Mail	Received E-Mail from [redacted] (Assistant Services)
11:49:17 AM(UTC-6)	SMS From: [redacted] Mother	Ohhhh, well if it can be gotten for less than$5 a sheet it might be worth it, but i don't think This truck could haul it all at once and 2 trips would probably break even with $12 delivered
11:49:17 AM(UTC-6)	SMS From: [redacted] Mother	Ohhhh, well if it can be gotten for less than$5 a sheet it might be worth it, but i don't think This truck could haul it all at once and 2 trips would probably break even with $12 delivered
11:51:02 AM(UTC-6)	Text File	rti.mqtt.counter.MqttLite.tp.DELETED.xml
11:52:23 PM(UTC-6)	Text File	event data [redacted]
11:55:47 AM(UTC-6)	Text File	BattStatsPrefs.DELETED 1.xml
11:55:48 AM(UTC-6)	Text File	com.google.android.gms.auth.devicesignals.DeviceSignalsStore.DELETED.xml
11:55:48 AM(UTC-6)	Text File	com.google.android.gms.tapandpay.service.TapAndPayServiceStorage.DELETED.xml
11:55:48 AM(UTC-6)	Text File	settings secure.DELETED.xml
11:56:14 AM(UTC-6)	Picture	1843 task thumbnail.png
11:59:00 AM(UTC-6)	Cookie: E-Mail	mail.google.com
11:59:00 AM(UTC-6)	Cookie: E-Mail	mail.google.com
11:59:00 AM(UTC-6)	Cookie: E-Mail	mail.google.com
11:59:00 AM(UTC-6)	DB	Gmail (Cookies)
11:59:02 PM(UTC-6)	Text File	AnalyticsPlatformPrefsFile.xml
11:59:02 PM(UTC-6)	Text File	AnalyticsPlatformPrefsFile.DELETED.xml
11:59:39 AM(UTC-6)	Text File	Account [redacted] .DELETED.xml
11:59:58 AM(UTC-6)	Text File	com.google.android.gms.auth.authzen.cryptauth.DeviceStateSyncManager.xml
12:00:01 AM(UTC-6)	Text File	com.motorola.motodisplay.analytics.MD BREATHS.DELETED.xml
12:00:01 AM(UTC-6)	Text File	com.motorola.motodisplay.analytics.MD NOTIF.DELETED.xml
12:00:01 AM(UTC-6)	Text File	com.motorola.motodisplay.analytics.TOUCH.DELETED.xml
12:00:05 AM(UTC-6)	Text File	rti.mqtt.counter.MqttLite.tp.DELETED 1.xml
12:00:05 AM(UTC-6)	Text File	DebugAnalytics.DELETED 1.xml
12:00:20 PM(UTC-6)	Picture	IMG [redacted] 120016201.jpg
12:00:23 PM(UTC-6)	DB	Google Photos (media store extras)
12:00:23 PM(UTC-6)	Picture	IMG [redacted] 120021204.jpg
12:00:23 PM(UTC-6)	Text File	com.google.android.apps.photos preferences.DELETED 4.xml
12:00:24 AM(UTC-6)	Text File	BattStatsPrefs.DELETED 2.xml
12:00:24 PM(UTC-6)	Picture	IMG [redacted] 120022835.jpg
12:00:24 PM(UTC-6)	Text File	com.google.android.apps.photos preferences.DELETED 3.xml
12:00:25 PM(UTC-6)	DB	Google+ (trash.db)
12:00:25 PM(UTC-6)	Text File	com.google.android.apps.photos preferences.DELETED 2.xml
12:00:25 PM(UTC-6)	Text File	com.google.android.apps.photos preferences.DELETED 5.xml
12:00:26 PM(UTC-6)	Text File	com.google.android.apps.photos preferences.xml
12:00:26 PM(UTC-6)	Text File	com.google.android.apps.photos preferences.DELETED.xml
12:00:26 PM(UTC-6)	Text File	com.google.android.apps.photos preferences.DELETED 1.xml
12:00:58 PM(UTC-6)	Text File	MailAppProvider.DELETED 1.xml
12:00:59 AM(UTC-6)	Text File	Pmaps.xml
12:00:59 PM(UTC-6)	Text File	Account [redacted] .DELETED 1.xml
12:00:59 PM(UTC-6)	Text File	MailAppProvider.DELETED.xml

Questions?

lars.daniel@envistaforensics.com / 919-621-9335







Questions?

LARS DANIEL EnCE, CCO, CCPA, CTNS, CTA, CIPTS, CWA
PRACTICE LEADER – DIGITAL FORENSICS

M: 919-621-9335
E: lars.daniel@envistaforensics.com

Books Published
- Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom, Syngess.
- Digital Forensics Trial Graphics: Educating the Jury Through Effective Use of Visuals", Published by Academic Press
- (2022) The Attorneys Field Guide to Digital Evidence: Mobile Phones

Certifications
- EnCase Certified Examiner (EnCE)
- Cellebrite Certified Logical Operator (CCLO)
- Cellebrite Certified Physical Analyst (CCPA)
- Certified Telecommunications Network Specialist (CTNS)
- Certified Wireless Analyst (CWA)
- Certified Internet Protocol Telecommunications Specialist (CIPTS)
- Certified Telecommunications Analyst (CTA)

Expert Testimony
- 33 times in State and Federal Court
- Qualified as an expert in computer forensics, digital forensics, cell phone forensics, video forensics, and photo forensics
- Testified for the defense and prosecution in criminal cases, and the plaintiff and defense in civil cases.

Case Experience
- Hundreds of cases involving murder, sex crimes, terrorism, kidnapping, intellectual property, fraud, wrongful death, employee wrongdoing, motor carrier accidents, and insurance losses among others.

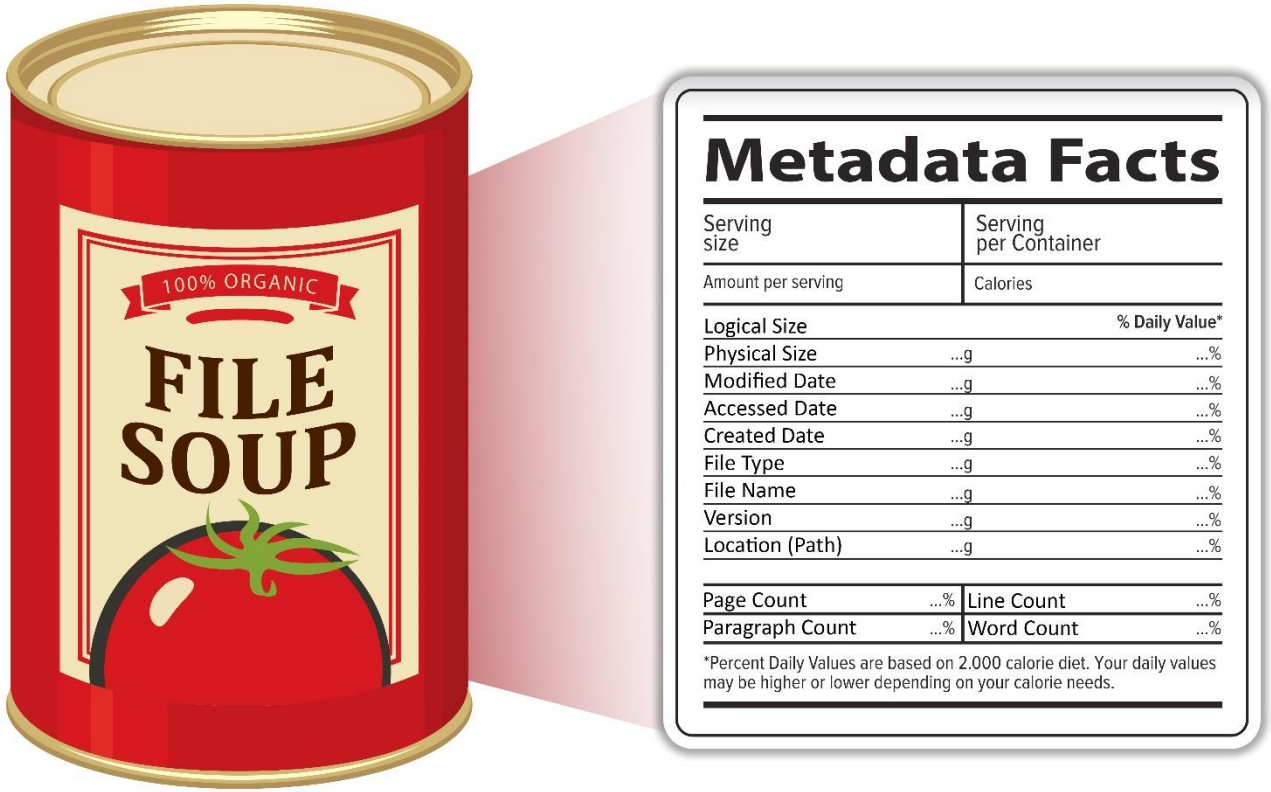
Speaking Engagements
- Largest Digital Forensics conference in the world, the Computer Enterprise Investigations Conference (CEIC, now EnFuse) in 2011, 2013, 2016, and 2019
- Over 300 CE and CLE classes taught across United States

Case Study: Distracted Driving

- Detailed timeline analysis at point of impact
  - Cell phone, event data recorder, online accounts

Case Example: Cell Phone Picture

- Photo Editing and Metadata
  - Web based (cloud) photo editing application



Civil Case Becomes Criminal

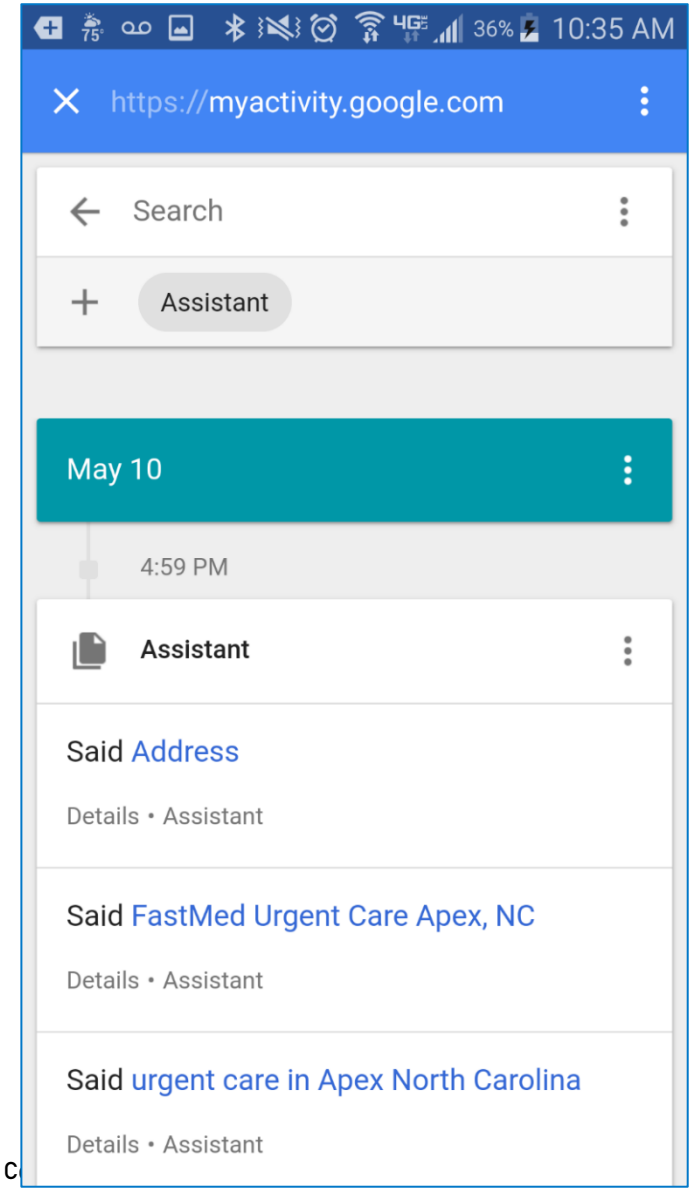
- Data theft turns criminal
  - Assisting Federal Marshalls
    - Data thief becomes a fugitive
    - Syncing between IOT devices p

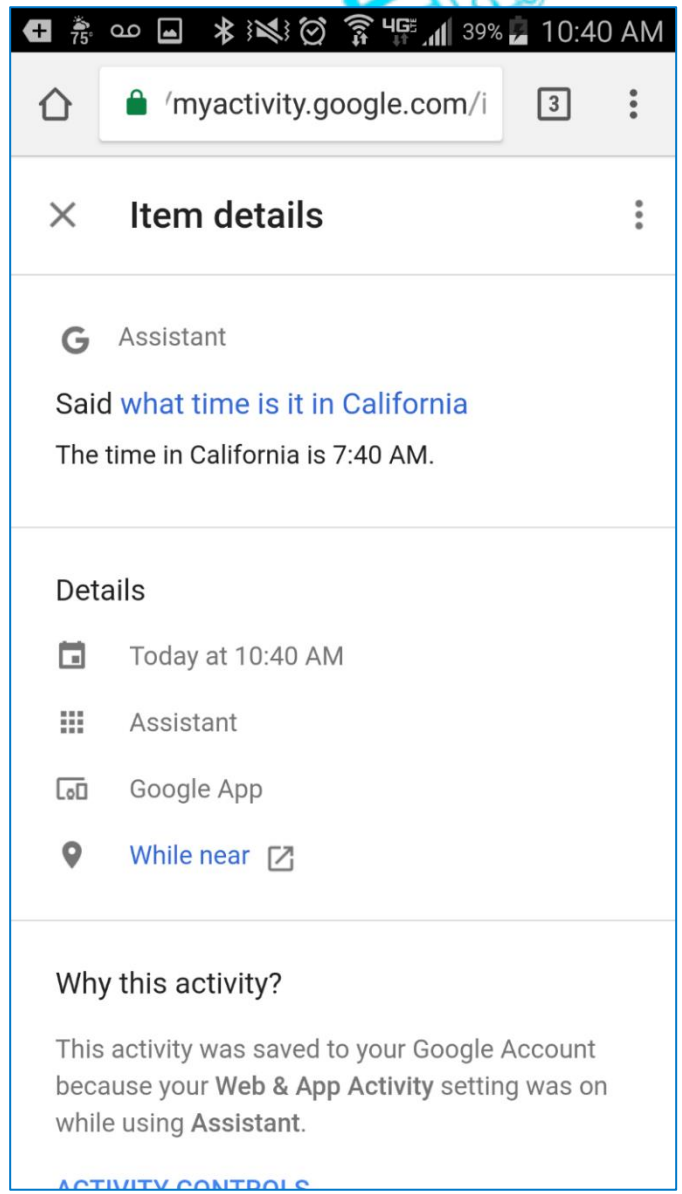
11. There is also a photograph stored on the Cell Phone that appears to be a picture of a New Mexico driver's license in the name of [redacted] with the date of birth of XX/XX/19XX. A copy of the photograph with the date of birth redacted is attached hereto as **Exhibit 4**.

Cell Phone:	**Hey! Want to make some fast cash?**
[redacted] Number:	**Who is this**
Cell Phone:	**[redacted] You moved my lazy boy chairs about 2 months ago. I am putting in for a name change and one of the many things they want is an affidavit attesting to my morel [sic]character. They want 2 of them. I already have them both ready to go so now I am just looking for 2 people that will sign them in front of a notary. I am offering $100 cash per person. Know anyone that might be interested?**
[redacted] Number:	**I will let y**
Cell Phone:	**Awesome!**
[redacted] Number:	**When and where. When do you have to have this done**
Cell Phone:	**Whenever is good for you will be fine. We can do it at the UPS store on [redacted] I think they have a notary there. If not then any bank would do but i am pretty sure that the UPS store has one.**

Capabilities: Examples

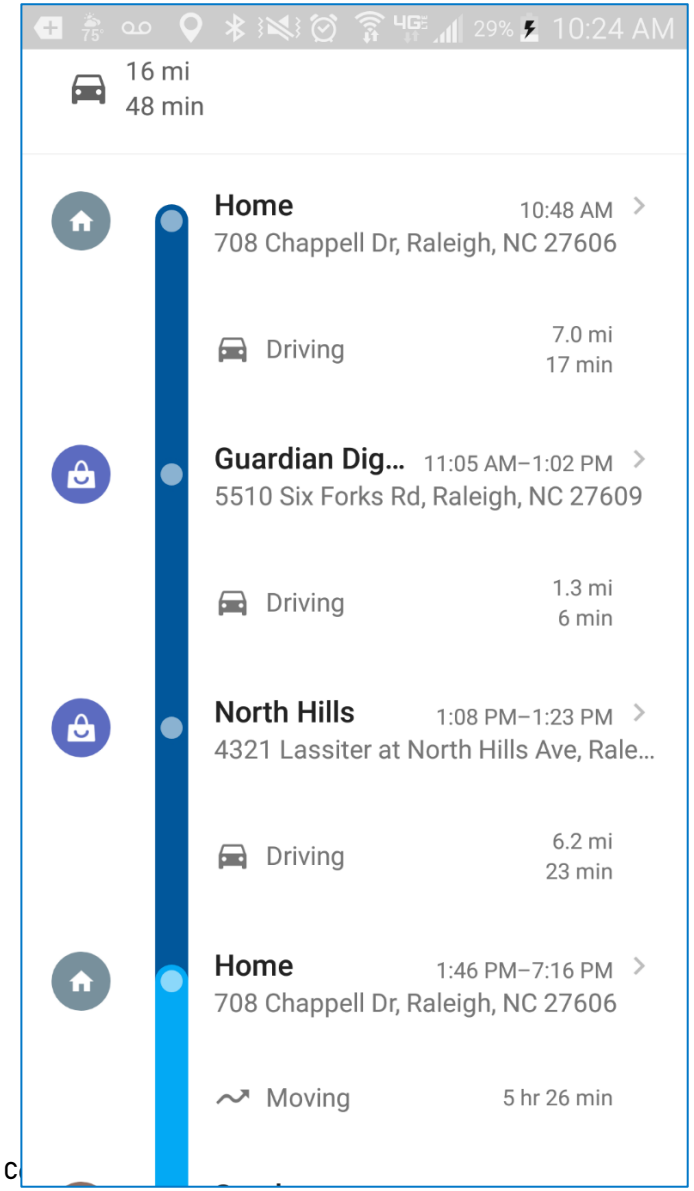
- Google is listening
  - Location activity
  - Full route

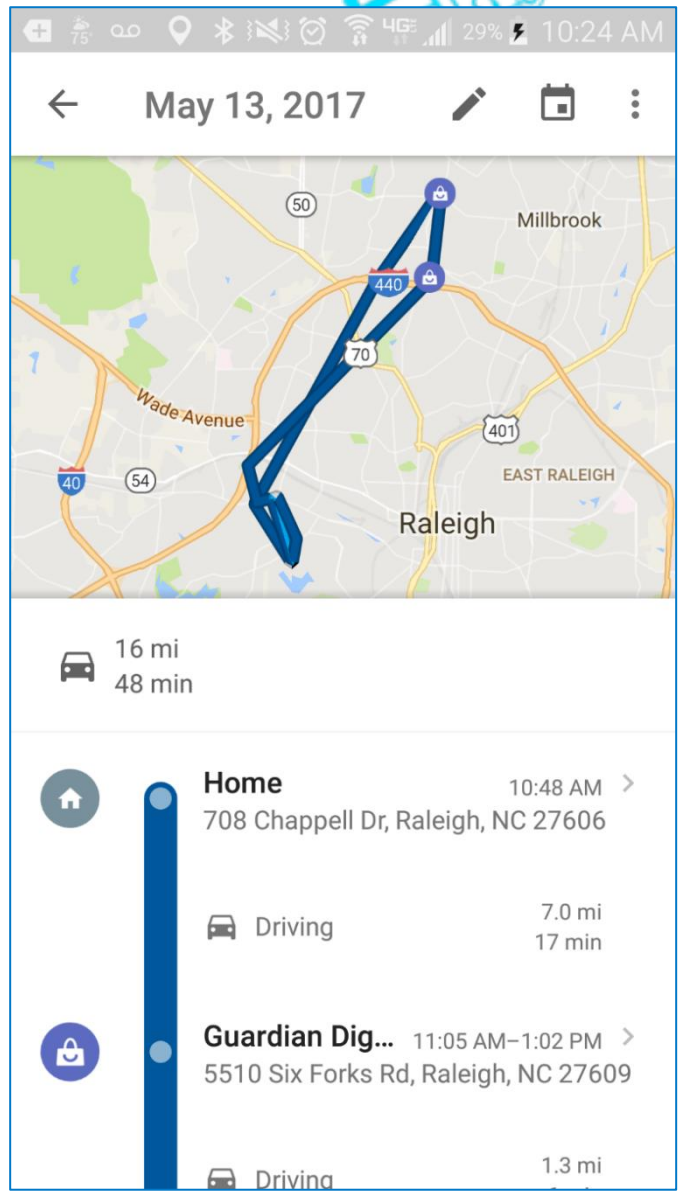




Capabilities: Examples

- Google is listening
  - Location activity
  - Full route





Investigating Allegations of Child Sex Offenses

Susan Weigand, Attorney ~ Melani McIntosh, Investigator

Defense or No Defense

"There's no evidence, no DNA, she's not coming to court"

"She said she was 22, she looked 22, she lied about her age"

"She came onto me, always wearing those short shorts"

"I'm her step-father, I was never alone with her"

"I believe in the power of prayer, God will heal her heart"

"They planted my DNA, I did not have sex with her"

Common Scenarios in Child Sex Offense Cases

Things to Consider

- Allegation dates
- Timeline from offense to report date
- Parties involved
- NCGS § 14-318
- NC Child Advocacy Centers

Client Interview

- DSS involvement
- Another lawyer
- Living situation
- Client/Child relationship
- Prior accusations
- About the child
  - Age, grade
  - Juvenile Court
  - IEP
  - MH/Medications
  - Prior accusations

WMS: Worthless Mother Syndrome


Can We Talk?

Dear Ms. Weigand,

My name is Nita Stanley, I am attorney with the Charlotte Mecklenburg Guardian ad Litem Program.

I represent a juvenile in Department of Social Services, Youth and Family Services (YFS) custody, with proceedings before the Honorable Judge Aretha Blake. The mother of this juvenile is a client of yours in a criminal proceeding. Your client's name is [redacted]. The pending criminal matters involving my child/client as the victim are:

[redacted]

This letter is to make it clear that I represent the child of [redacted] **I AM NOT CONSENTING AT THIS TIME TO PERMIT MY CLIENT TO SPEAK WITH YOU OR ANY OTHER ATTORNEY.** As I am sure you are aware, for any attorney, including a defense attorney or assistant district attorney, to communicate with my client without my prior consent, even in an "unrelated" matter, would constitute a very clear violation of Rule 4.2 of North Carolina Rules of Professional Conduct, Rule 7.4 of North Carolina Rules of Professional Conduct, NC State Bar Ethics Opinion RPC 61, and NC State Bar Ethics Opinion RPC 249.

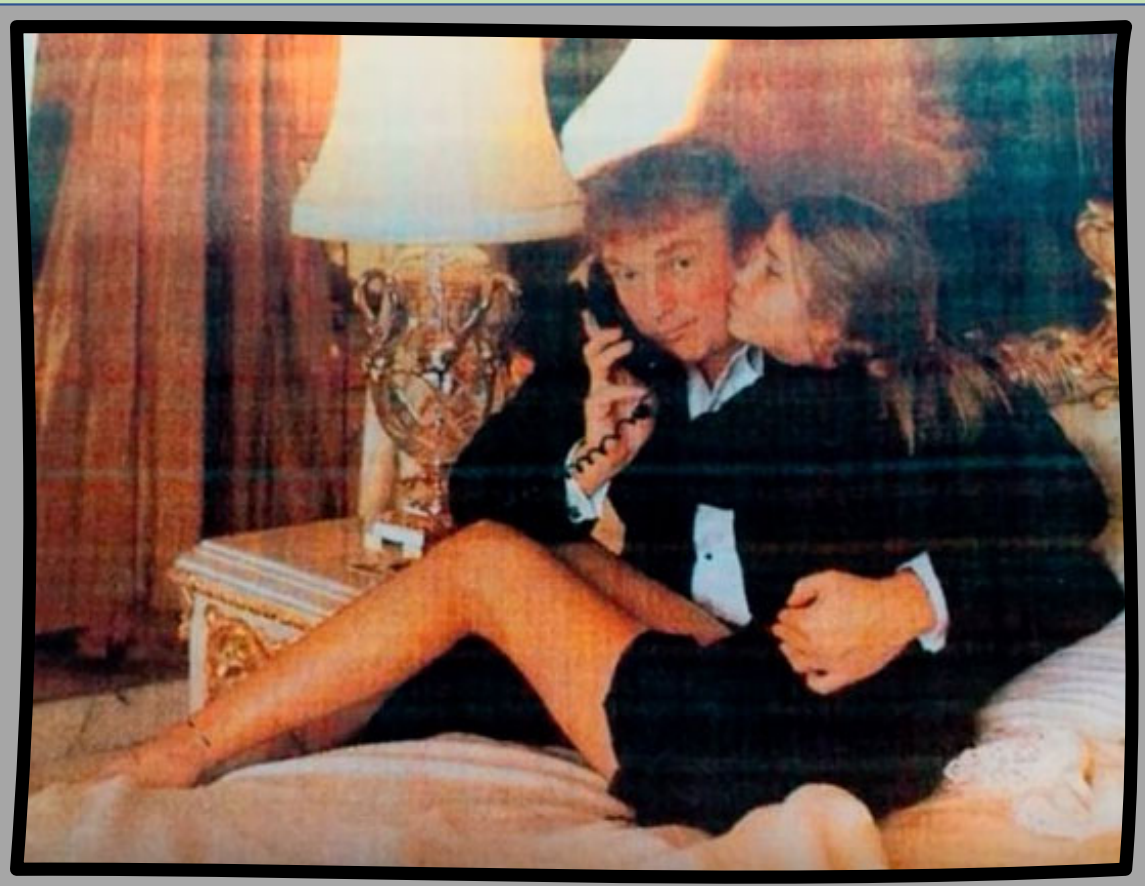
Please feel free to contact me at any time if I can be of assistance in this matter.

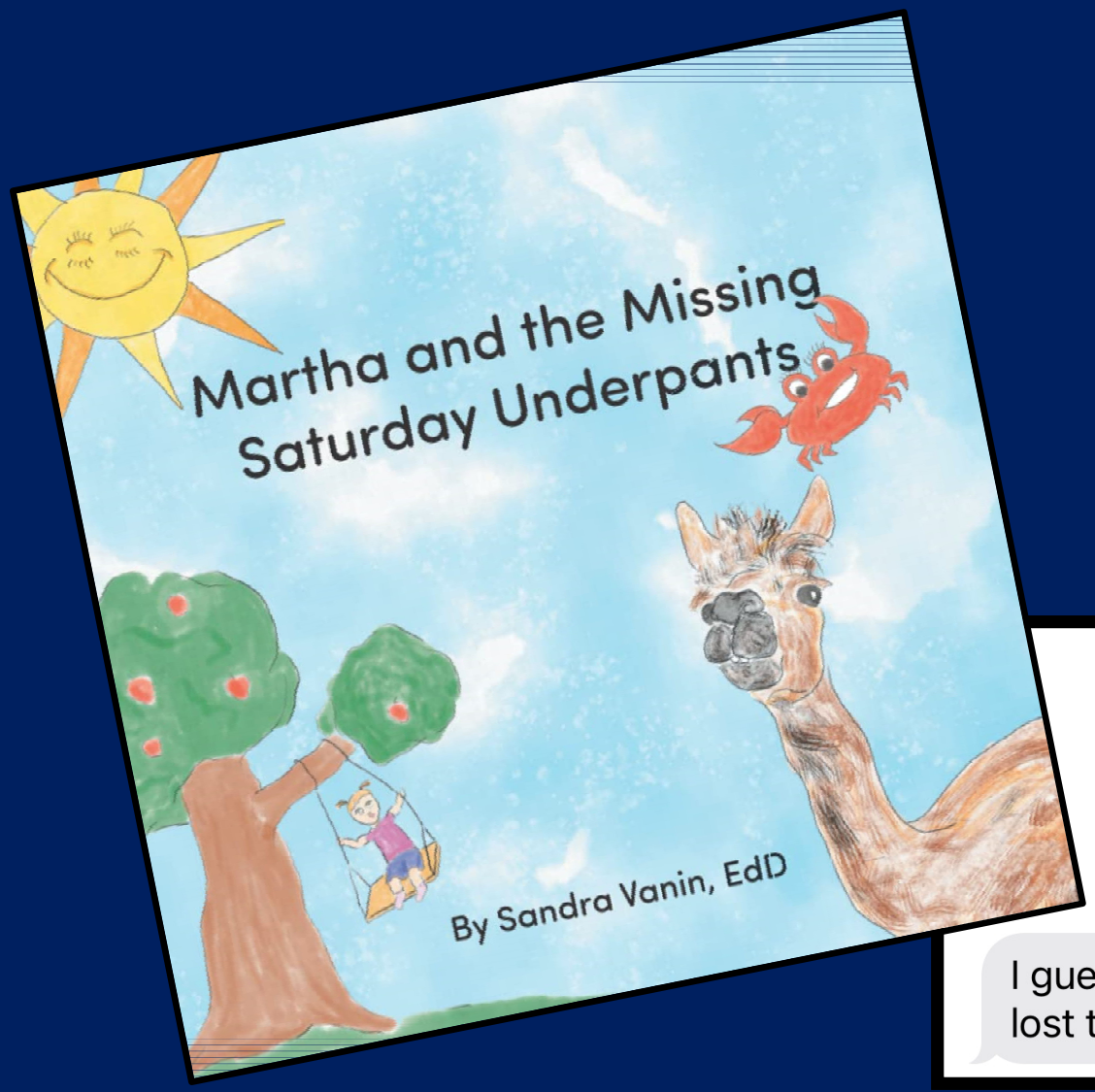
Sincerely,

Nita K. Stanley

Nita K. Stanley, JD., CWLS
700 East 4th Street, Suite 300
Charlotte, NC 28202

Inappropriate Behavior





Maybe I've been working with you too long. I can't see this ending anywhere but Superior Court.

HA HA

I guess it depends on how she lost them and who has them!

ETHICAL CONSIDERATIONS FOR INVESTIGATORS

1) NEVER VIOLATE A CONFIDENCE

2) NEVER KEEP INFORMATION FROM THE ASSIGNED ATTORNEY

3) ALWAYS COMPLETE ASSIGNMENTS ON TIME OR GIVE THE LAWYER AMPLE TIME IF YOU CANNOT

4) NEVER MAKE A PROMISE YOU CANNOT KEEP

5) AVOID WORKING ON CASES THAT PRESENT CONFLICTS SUCH AS CO-DEFENDANTS

6) PROBLEM OF DISCOVERING FACTS THAT ARE EXCULPABLE TO ONE CLIENT AND INCRIMINATING TO ANOTHER?

7) BE CAREFUL WORKING WITH INTERNS AND VOLUNTEERS

8) PROBLEMS OF CHANGING SIDES WHEN YOU CHANGE JOBS?

9) NEVER FALSIFY ANYTHING IN A REPORT

10) KNOW AND KEEP A COPY OF YOUR STATE'S RULES OF PROFESSIONAL CONDUCT

NORTH CAROLINA TASK FORCE FOR RACIAL EQUITY IN CRIMINAL JUSTICE

END OF YEAR REPORT 2021

TABLE OF CONTENTS

2 PROGRESS 8

DEAR GOVERNOR COOPER,

Last year, you created the Task Force for Racial Equity in Criminal Justice and charged us with finding real solutions to eliminate racial disparities and inequities in our criminal justice system. We spent nearly six months immersed in this effort and in December 2020, we submitted 125 recommendations to you spanning every part of the criminal justice system. And while that report was a milestone in our work to make North Carolina a more equal state, our work was not complete.

This year, we've worked to turn those recommendations into reality. Implementation is not an easy or simple process. Our criminal justice system is vast, and the inequities that unfairly harm Black North Carolinians and North Carolinians of color are deeply entrenched in its policies and, often unintentionally, in the ways we carry them out. But this work is urgent. This year has been proof that while change will not happen overnight, it is possible.

In concert with our Task Force members, local leaders, community advocates, elected representatives, and many others, North Carolina has made significant progress to address disparities in our criminal justice system. This year, Task Force members organized themselves into committees based on how our solutions would be implemented – executive, judicial, legislative, and local policy. We've also created communications and data committees to support the ongoing information and data needs of the other committees and the Task Force as a whole. Our committees have met monthly, and the full Task Force has met quarterly.

Committees have worked to establish strategies that would best realize their assigned recommendations, including, but not limited to, shaping training offerings, providing model policies and assistance, promoting collaboration between law enforcement and local governments, finding and leveraging funding opportunities, and raising awareness with the public.

Earlier this year, our Task Force supported several pieces of landmark legislation that advance many of our recommendations. The General Assembly passed and you signed into law several changes that will improve our criminal justice system. Those include improving law enforcement accountability by establishing a duty to intervene, requiring more enhanced data on officer-involved use of force incidents, and better training law enforcement officers to address the myriad of issues they face in communities while maintaining their own mental and physical health. These laws will also help stem the school-to-prison pipeline and keep many young people out of our criminal justice system, strengthen pretrial system practices, and ensure more dignity for pregnant women and other vulnerable people while they are incarcerated.

We are grateful to you for taking action to implement some of our recommendations, such as creating the Juvenile Sentence Review Board. We've worked to address state policies with other appropriate state actors – on substance use treatment, charging decisions, crisis intervention programs, school safety and discipline, and pretrial practices, among others. We've also partnered with local governments and community organizations to help them find ways to fund and develop these solutions in their communities. After all, many of our recommendations are local in nature and will be most successful if they are tailored to the unique needs of each community. We call on all North Carolinians to help champion our recommendations in their communities.

This is only a snapshot of some of the work the Task Force has accomplished in the past year. More details are included in the following pages of this report. All of these efforts are rooted in the hard work of so many North Carolinians from every corner of the state. Members of the Task Force and its staff have put countless hours toward these efforts, as have community advocates, directly impacted people, law enforcement, public health and public safety experts, researchers, legislators, and victims and survivors. Their contributions have led to much-needed improvements to our law enforcement and criminal justice systems in 2021.

Our work is by no means finished. Our state has a distance yet to go to create a fairer North Carolina – one where every person is guaranteed equal justice under the law. We need teamwork and collaboration at every level of government and from every stakeholder in our communities. We thank you for your continued dedication and interest in this work. As co-chairs of the Task Force, we are committed to working alongside you to create a safer, more just North Carolina for all.

Sincerely,

Anita Earls
Associate Justice
Supreme Court of North Carolina

Josh Stein
Attorney General
North Carolina

Co-Chairs of the North Carolina Task Force for Racial Equity in Criminal Justice

CO-CHAIR

THE HONORABLE ANITA S. EARLS

Associate Justice, Supreme Court of North Carolina

CO-CHAIR

THE HONORABLE JOSH STEIN

Attorney General, North Carolina

SHERIFF CLARENCE BIRKHEAD

Sheriff, Durham County

Committees: Executive Branch Action

SECRETARY EDDIE BUFFALOE

NC Department of Public Safety

Committees: Executive Branch Action

MS. TARRAH CALLAHAN

Executive Director, Conservatives for Criminal Justice Reform

Committees: Legislative Action, Communications

THE HONORABLE BROOKE LOCKLEAR CLARK

District Court Judge, Robeson County

Committees: Judicial Branch Action

THE HONORABLE MITCH COLVIN

Mayor, Fayetteville

Committees: Local Policy Action

PROFESSOR APRIL DAWSON

Associate Dean of Technology and Innovation and Professor of Law, NCCU School of Law

Committees: Judicial Branch Action

THE HONORABLE JAMES D. GAILLIARD

North Carolina House of Representatives

Committees: Legislative Action

SERGEANT BILLY GARTIN

Raleigh Police Department

Committees: Executive Branch Action

CHIEF GINA HAWKINS

Chief, Fayetteville Police Department

Committees: Local Policy Action, Executive Branch Action

THE HONORABLE MIKE HAWKINS

Former Transylvania County Commissioner

Committees: Local Policy Action

MR. HENDERSON HILL

Senior Counsel, ACLU Capital Punishment Project

Committees: Judicial Branch Action

MS. DEBORAH DICKS MAXWELL

President, North Carolina NAACP, New Hanover NAACP

Committees: Local Policy Action

THE HONORABLE MUJTABA A. MOHAMMED

North Carolina Senate

Committees: Legislative Action

THE HONORABLE MARCIA H. MOREY

North Carolina House of Representatives

Committees: Legislative Action

MR. KERWIN PITTMAN

Founder, Recidivism Reduction Educational Program Services

Committees: Executive Branch Action

MS. MARY SHEEHAN POLLARD

Executive Director, North Carolina Office of Indigent Defense Services

Committees: Judicial Branch Action

THE HONORABLE RONNIE SMITH

Chair, Martin County Board of Commissioners

Committees: Local Policy Action

DIRECTOR JEFF SMYTHE

Director, NC Criminal Justice Standards Division

Committees: Local Policy Action

THE HONORABLE ALAN THORNBURG

Superior Court Judge, Buncombe County

Committees: Judicial Branch Action

MR. TALLEY WELLS

Executive Director, NC Council on Developmental Disabilities

Committees: Legislative Action

MS. ANGELICA R. WIND

Healthier Together Regional Director, Region 1, NC Counts Coalition

Committees: Local Policy Action, Communications

THE HONORABLE JAMES RAEFORD WOODALL, JR.

District Attorney, Prosecutorial District 18

Committees: Judicial Branch Action

PROGRESS

LEGISLATION PASSED

North Carolina made important progress toward accomplishing a number of Task Force for Racial Equity in Criminal Justice (TREC) recommendations when Governor Cooper signed the following pieces of legislation into law in 2021:

SENATE BILL 300
(SESSION LAW 2021-138)

Recommendations #6-9: Strengthen community policing practices.

- Part 11 of SB 300. Expands mandatory in-service training to include community policing.

Recommendations #31-35: Revise use of force policies.

- Part 3 of SB 300. Requires the Criminal Justice Standards Division to create and maintain a statewide database for law enforcement agencies that tracks all critical incident data of law enforcement officers in North Carolina. A "Critical Incident" is defined as an incident involving use of force by a law enforcement officer that results in death or serious bodily injury to a person.
- Part 8 of SB 300. Requires law enforcement agencies to create an early warning system within the agency to monitor officer actions and behaviors, including discharge of a firearm, use of force, vehicle collisions, and citizen complaints.
- Part 14 of SB 300. Establishes a duty for law enforcement officers to intervene and report excessive use of force by another officer.

Recommendations #36-46: Improve law enforcement accountability and culture.

- Part 1 of SB 300. Requires the North Carolina Sheriffs' Education and Training Standards Commission and the North Carolina Criminal Justice Education and Training Standards Commission (Standards Commissions) to develop and maintain a statewide database accessible to the public on its website that contains all revocations and suspensions of law enforcement officer certifications.

- Part 2 of SB 300. Provides a process to have all law enforcement officers' fingerprints entered in state and federal databases and authorizes agencies to participate in the Rap Back service which would alert the State Bureau of Investigation (SBI) if the officer has a subsequent arrest. The Rap Back Program would maintain and continuously compare fingerprints to arrest records throughout the United States so that the Standards Commissions can quickly and efficiently identify when a certified individual has been arrested and take appropriate investigative action.
- Part 3 of SB 300. Requires the Criminal Justice Standards Division to create and maintain a statewide database for law enforcement agencies that tracks all critical incident data of law enforcement officers in North Carolina. A "Critical Incident" is defined as an incident involving use of force by a law enforcement officer that results in death or serious bodily injury to a person.
- Part 5 of SB 300. Requires the Standards Commissions to develop uniform, statewide minimum standards for law enforcement officers and justice officers and adopt these standards as rules.
- Part 7 of SB 300. Requires a psychological screening prior to initial certification.
- Part 8 of SB 300. Requires law enforcement agencies to create an early warning system within the agency to monitor officer actions and behaviors, including discharge of a firearm, use of force, vehicle collisions, and citizen complaints.
- Part 10 of SB 300. Requires the SBI to investigate upon the request of the governor or a sheriff, chief of police, district attorney, head of a state law enforcement agency, or the commissioner of prisons if a law enforcement officer uses force against an individual that results in the death of the individual.

Recommendation #51: Recruit and retain a racially equitable work force.

- Part 9 of SB 300. Requires the Standards Commissions to develop a best practice guide to help law enforcement agencies recruit and retain a diverse workforce.

Recommendations #56-59: Train law enforcement to promote public safety and earn community support.

- Part 11 of SB 300. Expands mandatory in-service training to include community policing, minority sensitivity, use of force, duty to intervene and report, mental health for criminal justice officers, ethics, response to domestic violence cases, and juvenile justice issues.
- Part 12 of SB 300. Allows the Standards Commissions to revise law enforcement training requirements more quickly in response to changes in the field.

Recommendation #60: Enhance the law enforcement profession.

- Part 7 of SB 300. Requires the Standards Commissions to jointly study the benefits, if any, of requiring physical fitness testing throughout the career of a law enforcement officer and if it should be incrementally adjusted based upon the age of the law enforcement officer.

Recommendations #74-78: Shrink the criminal code.

- Part 13 of SB 300. Limits some local ordinances that may impose a criminal penalty and provides a compliance defense for certain violations.
- Part 20 of SB 300. Creates a legislative study of the criminal code.

Recommendations #79-83: Improve pre-trial release and accountability practices.

- Part 14 of SB 300. Requires first appearance within 72 hours (This legislation was later amended to allow first appearances to be held within 96 hours when the court is closed for more than 72 hours) for all charges when the defendant is in custody.

These new laws represent necessary reforms to our public safety system that advance criminal justice policy in our state. But there is more to do to improve our general statutes to address disparities so people are treated fairly and our communities are made safer.

SENATE BILL 207
(SESSION LAW 2021-123)

Recommendations #66-70: Stem the school to prison pipeline and rethink juvenile justice.

- Part 4 of SB 207. Allows a prosecutor to decline to prosecute in superior court a matter that would otherwise be subject to mandatory transfer if the juvenile allegedly committed an offense that would be a Class D, E, F, or G felony if committed by an adult. This would allow 16- and 17- year-olds to remain in the juvenile justice system with the district attorney's consent.
- Part 5 of SB 207. Raises the minimum age of juvenile jurisdiction from six to ten, unless the juvenile is alleged to have committed an A-G felony, in which case the minimum age is eight.

HOUSE BILL 608
(SESSION LAW 2021-143)

Recommendation #106: Protect pregnant people in jails and prisons.

- Part 2 of HB 608. Prohibits the North Carolina Department of Public Safety (DPS) and correctional employees from applying restraints on a pregnant woman incarcerated during the second and third trimester of pregnancy, during labor and delivery, and during the postpartum recovery period. An incarcerated person who is in the postpartum recovery period may only be restrained if a correctional facility employee makes an individualized determination that an important circumstance exists. In this case, only wrist handcuffs held in front of the incarcerated person's body may be used and only when she is ambulatory.

B

EXECUTIVE ORDER ISSUED

Recommendation #70: Establish a juvenile review board within the Governor's Clemency Office.

In April 2021, Governor Cooper formed the Juvenile Sentence Review Board based on TREC's recommendation. The four-person advisory board, established by Executive Order 208, is tasked with reviewing certain sentences imposed in North Carolina on individuals who were tried and sentenced in adult criminal court for acts committed before turning 18. The review board makes recommendations to the governor concerning clemency and commutation of such sentences when appropriate.

NEW STATE GOVERNMENT FUNDING OPPORTUNITIES ALIGNED WITH TREC RECOMMENDATIONS

THE GOVERNOR'S CRIME COMMISSION

The Governor's Crime Commission (GCC) approved several new priorities for Federal Fiscal Year (FFY) 2022 that are based on TREC recommendations. These new priorities were included in the FFY 2022 request for applications (RFA) released on Nov. 1, 2021. The RFA will solicit applicants for grant projects that begin performance on Oct. 1, 2022.

Recommendation #1: Respond more appropriately to situations concerning mental illness, autism, intellectual disabilities, substance abuse, homelessness, and other non-emergency situations.

GCC approved the implementation of two new priorities for FFY 2022 Byrne Justice Assistance Grants (JAG) federal funds. One of the new JAG priorities seeks to fund three to five pilot programs providing mental health diversion and co-responder projects. Models that can be used include those that are promoted by the National Alliance on Mental Illness. These pilot projects must show collaboration among local law enforcement agencies, mental health service providers, and local governments.

Recommendation #2: Add crisis intervention training for current law enforcement officers.

The other new FFY 2022 Byrne JAG priority will provide grants to law enforcement agencies that are seeking to utilize the Memphis crisis intervention training (CIT) model. The funding can be used by law enforcement agencies working to ensure that their officers complete CIT, an important TREC recommendation. Funds will also be available to support the North Carolina Justice Academy (Justice Academy) and/or other community partners' efforts to broaden and enhance the Crisis Intervention Model as implemented in North Carolina.

Recommendation #4: Develop and provide funding to help communities build violence prevention programs.

Recommendation #61: Establish and fund restorative justice programs in local communities across the state and at various points of the criminal justice system.

GCC recently approved a new funding priority for Victims of Crime Act funds. The new priority, victim-focused violence intervention, will focus on funding agencies that provide the following services: a) community violence intervention, b) hospital-based violence intervention, and c) restorative justice.

THE NORTH CAROLINA DEPARTMENT OF HEALTH AND HUMAN SERVICES

Recommendation #16: Establish and expand access to diversion programs.

Recommendation #17: Treat addiction as a public health crisis.

Recommendation #89: Study and adopt evidence-based reforms for reducing and eventually eliminating racial disparities in charging decisions and prosecutorial outcomes.

In October 2021, the North Carolina Department of Health and Human Services (DHHS) released a funding opportunity that will award a total of $5.8 million to at least nine organizations statewide to increase access to high-quality opioid use disorder treatment for people in the criminal justice system. This funding will help establish or expand programs including pre-arrest or pre-conviction diversion, comprehensive jail-based medication assisted treatment programs, and overdose prevention education and naloxone distribution upon release programs. This funding is responsive to several TREC recommendations, including the goal to treat addiction as a public health crisis.

Recommendation #1: Respond more appropriately to situations concerning mental illness, autism, intellectual disabilities, substance abuse, homelessness, and other non-emergency situations.

DHHS also is working to help local communities establish non-law enforcement responses to public health issues. They recently received a planning grant for mobile crisis teams. While the state can support these efforts, regional collaboration is also important to build the expertise and framework needed for pilot programs. Localities like Pitt County, Chapel Hill, Durham, Greensboro, and Buncombe County have been willing to share their expertise and experiences with interested local leaders.

THE GOVERNOR'S HIGHWAY SAFETY PROGRAM

The Governor's Highway Safety Program also funds data-driven initiatives related to traffic safety and may support a number of projects that align with TREC recommendations.

$5.8 Million

to be awarded by DHHS to at least 9 organizations statewide to expand addiction treatment in the criminal justice system

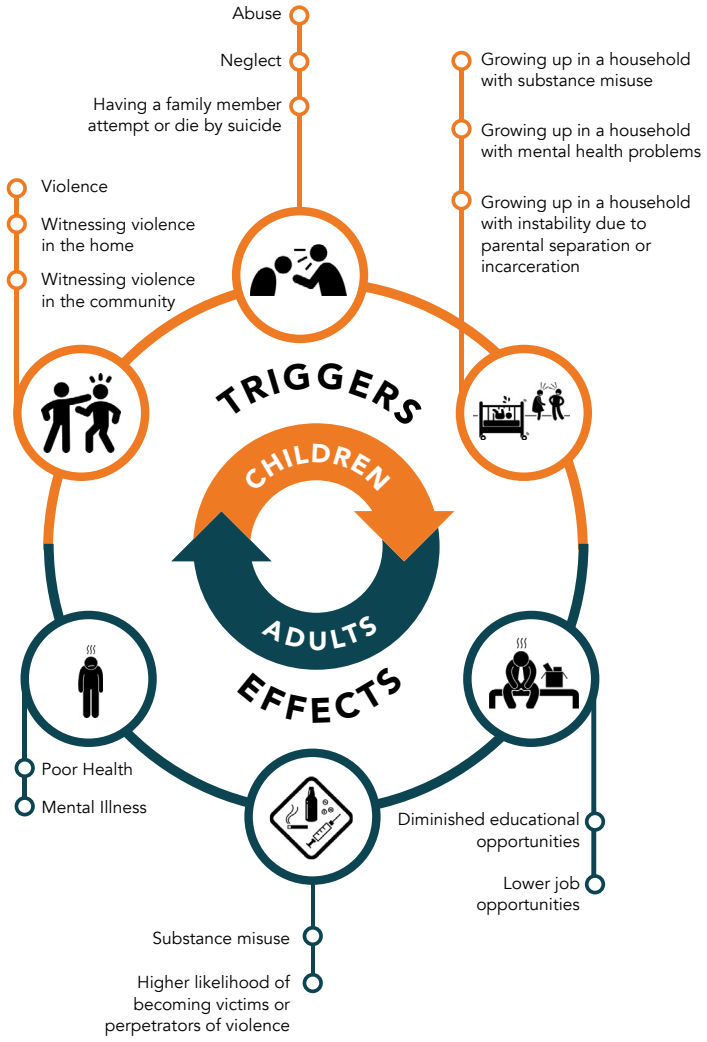
STATE AGENCY POLICY REFORMS

ADMINISTRATIVE OFFICE OF THE COURTS

In our 2020 report, we identified Adverse Childhood Experiences (ACEs) and their impact as a key area of study to improve our criminal justice system. As such, TREC was heartened to learn about the establishment of the Chief Justice's Task Force on ACEs-Informed Courts, which will help ensure that the judicial system is responsive to the needs of individuals who have experienced or are experiencing trauma. We look forward to collaboration with the new Task Force as we explore implementation of ACEs-informed TREC recommendations relevant to the judicial system.

Recommendation #101: In December 2021, the North Carolina Supreme Court issued an Order Adopting Rule 28 of the General Rules of Practice for Superior and District Courts that creates a procedure for defendants to file a motion for an assessment of their ability to pay legal financial obligations. Once a defendant files a motion, the court must consider the motion and, if necessary, conduct a hearing prior to imposing costs, fees, fines, restitution or other monetary obligations. This rule provides defendants across the state the opportunity to advocate for relief from financial penalties they are unable to pay and requires courts to consider defendants' economic status. The official motion form, AOC-CR-415 "Request for Relief from Fines, Fees, and Other Monetary Obligations," can be accessed here.

Recommendation #82: Promote court appearance strategies and develop alternative responses to failure to appear. Additionally, the Administrative Office of the Courts is advancing its court reminder system initiative to improve compliance with court dates and reduce the need for pretrial detention.

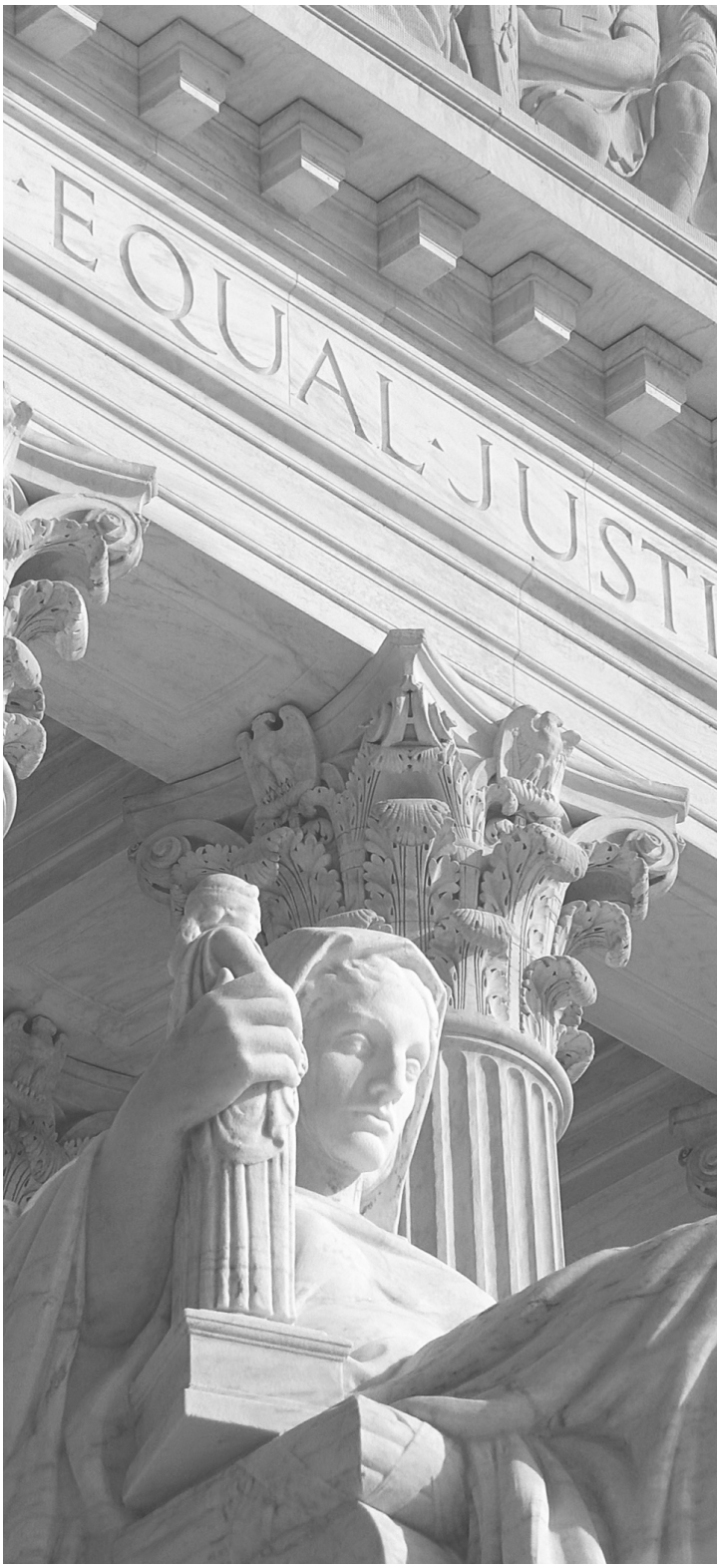


Court reminder systems have been shown to decrease failures to appear by up to 26%

Source: https://nccriminallaw.sog.unc.edu/improving-north-carolinas-criminal-court-date-notification-system/

DEPARTMENT OF PUBLIC SAFETY

Over the past year, DPS has proactively addressed a variety of TREC recommendations in support of strengthening public safety while also eliminating disparate outcomes in the criminal justice system for communities of color. Below are some highlights of TREC recommendations being addressed by DPS entities.



DPS LAW ENFORCEMENT

Recommendation #2: Reimagine public safety and reinvest in communities.

All DPS law enforcement agencies have either already implemented or are scheduled to implement CIT.

Recommendation #14: Require all consent searches to be based on written, informed consent.

State Highway Patrol (SHP) policy requires troopers to obtain owner/operator written consent to search a vehicle whenever practical.

Recommendation #27: Adopt a mandatory statewide policy on law enforcement facilitation of peaceful demonstrations.

In April 2021, State Capitol Police (SCP) updated its policies to better facilitate peaceful demonstrations. SCP adopted written directive 900-02 Response to Protests and Civil Disturbances. It states that SCP recognize the First Amendment right of citizens to peaceably assemble and articulates its policy to respect and facilitate lawful First Amendment activity.

Recommendation #31: Strengthen use of force practices including to prohibit neck holds and require the use of the minimum amount of force necessary.

SHP, SCP, and Alcohol Law Enforcement (ALE) policies all prohibit chokeholds and require the minimum amount of force necessary to apprehend a suspect.

Recommendation #32: Require officers to have first aid kits and render aid.

All DPS law enforcement agencies require their sworn members to render medical aid, when safe to do so, to persons in their custody who are injured. All state troopers, ALE agents, SCP officers, Community Corrections officers, and Special Operations and Intelligence Unit officers have been issued first aid kits.

Recommendation #33: Enact agency policies requiring a duty to intervene and report excessive use of force or other abuse.

All DPS law enforcement agencies require their sworn members to intervene and report in any case where a law enforcement officer may be a witness to what they know to be excessive use of force by another officer.

Recommendation #34: Establish early intervention systems for officers repeatedly violating use of force policies.

All DPS law enforcement agencies have early intervention systems in place to identify patterns of misconduct that could be mitigated through early intervention.

Recommendation #44: Support psychological screenings for all law enforcement officers.

All DPS law enforcement agencies require psychological screening as part of their pre-employment hiring process. Additionally, adult correctional officers and juvenile justice officers also are required to pass psychological screening prior to hiring.

DPS OFFICE OF VICTIM SERVICES

Recommendation #63: Improve and expand access to North Carolina's victim compensation fund to increase racial equity.

The Office of Victims Services (OVS) is working to improve data collection and analysis capabilities to better focus victim compensation outreach and education on under-served and under-represented communities. Additionally, OVS recently launched a GCC grant-funded public communications and outreach campaign to raise awareness of programs and services OVS offers. The campaign utilizes multiple media formats including television, display banners, newspaper, social media, DMV video boards, and radio.

DPS PRISONS

DPS Prisons has pursued new policies and either introduced or augmented programs as a direct result of TREC's recommendations to amend correctional facilities' practices and programming and address prison discipline.

Recommendation #64: Screen incarcerated individuals for victimization and provide appropriate services.

Prisons utilizes a comprehensive screening process through intake, case management, and internal transfer targeting physical, emotional, or sexual abuse and previous trauma. Prisons recently implemented screening within 24 hours of intake (previously screenings occurred within 72 hours of intake). Prisons has also implemented screening 30 days after intake as part of its regular case management process. Additionally, a variety of programs for victims are offered, to include trauma-informed therapy, mental health counseling, anger management, and stress management. The Juvenile Justice Section also screens for victimization upon admission to youth development centers and provides programming and treatment targeted towards individual juvenile needs.

Recommendation #108: Increase funding for mental health services and programs in prisons.

Prisons currently operates five therapeutic diversion units (TDU) with expansion to a sixth site in progress. TDUs provide an evidence-based treatment approach for incarcerated persons diagnosed with serious and persistent mental illness. Prisons has also implemented a new disciplinary credit program, incentivizing good behavior by reducing disciplinary sentences for those who remain infraction free.

Recommendation #110: Expand use of restorative justice and rehabilitation programming.

Availability and quality of programming available to individuals while incarcerated is crucial to their success once released. To this end, Prisons is actively implementing enhanced rehabilitative programming through cognitive behavioral interventions (e.g., Carey Guides for use by case managers). Prisons has also launched a tablet initiative that will expand access to rehabilitative programming, self-help, and increased family contact through tablet computers. A variety of other restorative justice and targeted programming is being implemented, to include expanding the rehabilitative diversion unit (RDU) at Pasquotank Correctional Institute and restorative justice circles at Central Prison and N.C. Correctional Institute for Women.

There are many recommended changes still under consideration and Prisons will continue to keep TREC updated on the progress of the efforts highlighted below.

Recommendation #96: Increase DPS flexibility on incarcerated individuals' release dates.

Approximately 81 percent of the 20,000 people released from prison annually receive sentence credits. Prisons currently awards sentence credits for working prison jobs, attending schools, good behavior, disciplinary release credits and credits for becoming fully vaccinated for COVID-19.

Prisons established a work group to evaluate additional types of sentence credits, as well as to review and recommend updates for policies dealing with the medical release of those who are ill and/or disabled, extension of limits of confinement, and advanced supervised release.

Recommendation #105: Transform the use of restrictive housing

Prisons established a work group to become American Correctional Association (ACA) -compliant with restrictive housing and special management expected practices by reviewing policies that need to be changed to reduce the number of incarcerated people assigned to restrictive housing, increasing the use of special management housing instead of restrictive housing, decreasing the types of infractions that result in restrictive housing, and reviewing locations which can provide step down facilities and additional TDUs and RDUs.

Recommendation #106: Protect pregnant people in jails and prisons

Prisons established a work group to review maternity leave programs in other jurisdictions for operational details. Prisons is also ensuring its compliance with the Dignity of Women who are Incarcerated Act (Session Law 2021-143).

Recommendation #107: Enhance prison personnel.

Prisons is currently working to implement CIT for all staff, making it a part of annual in-service training, and offering an introductory version during basic training. As of September 2021, more than 4,800 Prisons staff had completed crisis intervention training. Additionally, Prisons staff have completed an online racial bias training, and the Office of Staff Development and Training developed and received approval for a racial equity

and implicit bias training for correctional officer basic training students which will begin in January 2022. Furthermore, the General Assembly recently recently passed and Governor Cooper signed into law a step pay plan for correctional officers that will help Prisons with recruiting and retention.

Recommendation #109: Increase due process protections for people accused of disciplinary offenses.

- Prisons established a working group to review potential changes to disciplinary processes. Process changes will align with ACA standards. This involves reviewing other states' disciplinary processes to gather innovative ideas. To date, nine policies from other state jurisdictions have been received, reviewed, and compared to North Carolina's policies. They have initiated ongoing focus groups with staff and incarcerated persons regarding possible improvements.
- Prisons established a working group to review security risk group (SRG) management and additional expansion of the security threat group management unit (STGMU) program model that Foothills Correctional Institution uses. Expansion of STGMU beds will occur, as well as the tablet program to include programming of this nature.
- Prisons has collected demographic data of disciplinary hearing officers (DHOs) and people who are incarcerated who were involved in the hearing process and is currently analyzing the information and discussing ways to track the process through an easily accessible method such as a dashboard or automated report.
- Prisons revised policy B .0200 - Offender Disciplinary Procedures - and is currently reviewing potential cost/benefit outcomes to enacting the changes by conducting mock hearings using the revised disciplinary language on previously heard cases.
- Prisons completed its review of how confidential information is reviewed during the disciplinary process. Current data obtained shows that Prisons' policy is consistent on this topic with other states. The goal is to ensure accuracy and truthfulness of confidential statements or sources and that the process remains safe for all persons involved while also ensuring that accused persons are provided with what is needed to defend themselves during the hearing. Prisons continues to expand its training plan for new and existing DHOs and new and existing facility staff.
- In July 2021, Prisons trained 90 staff members on proper referrals for STGMU. The survey submitted to field staff regarding improvements in the SRG process is pending results.

DPS JUVENILE JUSTICE

Recommendation #33: Collect data on discipline in schools.

DPS recently released a public-facing school discipline dashboard, which details school-based offense data by juvenile judicial district. It includes information on race and sex and exists as a resource to School Justice Partnerships (SJPs) across the state in assessing progress toward goals.

Additionally, the State Board of Education published Phase 1 of its strategic dashboard monitoring tool, which displays information at the state, district, and school level on a range of educational metrics, including exclusionary discipline practices. Information on subgroups like gender, race, and disability status is also available in many instances.

Recommendation #67: Require a school administrator or school social worker to sign a school-based petition initiated by an SRO before it can be accepted for filing in juvenile court.

Although statewide application of this recommendation would require legislation, its spirit was to have better controls on when and how children are referred to the juvenile justice system. In addition to the legislature's raising the age of minimum jurisdiction, this work can be advanced by augmenting training opportunities for SROs. Juvenile Justice has been conducting trainings with SROs across the state and educating them on the types of matters that will not be accepted to discourage inappropriate referrals from schools.

Recommendation #84: Require racial equity training for court system personnel, including judges, DAs, and public defenders.

Juvenile Justice was awarded a $237,000 GCC grant, of which $177,787 was federally funded through the Office of Juvenile Justice and Delinquency Prevention (OJJDP). This grant, effective Jan. 1, 2022, will provide racial equity training to all Juvenile Justice staff and community program providers. Juvenile Justice is seeking another competitive opportunity with Georgetown University to convene local decision-makers and stakeholders in one North Carolina jurisdiction to create opportunities where barriers to racial equity exist in their communities. If selected, the "Transforming the Youth Justice System" grant will provide intensive, action-focused training designed to support local jurisdictions in their efforts to reduce racial and ethnic disparities and transform the role of the justice system.

POST RELEASE SUPERVISION AND PAROLE COMMISSION

Recommendation #85: Require implicit bias and racial equity training for parole staff.

Post Release Supervision and Parole Commission staff have completed both an "Implicit Bias Workshop" and a "Fairness and Bias in Risk Assessment" training. Community Corrections will begin to incorporate implicit bias training into its annual in-service training curriculum in Spring 2022.

$237,000 GCC Grant

awarded to DPS Juvenile Justice to expand racial equity training

E

CRIMINAL JUSTICE AND SHERIFFS' TRAINING AND STANDARDS COMMISSIONS AND NORTH CAROLINA JUSTICE ACADEMY

The Standards Commissions are critical partners in the successful implementation of TREC's law enforcement-focused recommendations. Similarly, the Justice Academy develops and delivers law enforcement training. In the section below, we discuss progress and efforts related to TREC recommendations under the purview of the Commissions and the Justice Academy.

CHANGES TO LAW ENFORCEMENT TRAINING

Recommendation #2: Add crisis intervention training.

Recommendation #29: Review and update protest training.

Recommendation #56: Revamp basic law enforcement training.

Recommendation #57: Recommend changes to in-service trainings.

Prior to the work of TREC, law enforcement training was an area of intense focus and reform in North Carolina. Over the past several months, numerous stakeholder groups have engaged with the Justice Academy and the Standards Commissions on the right trainings for law enforcement officers and the frequency of those trainings. TREC was heartened to know that many of its training recommendations related to basic law enforcement training (BLET) either have been or will have an opportunity to be implemented as the new BLET is developed. The new BLET is the result of a long-term revamp with input from law enforcement officers, leaders, community advocates, and the general public. It will be released in 2023. Woven throughout the new BLET is a focus on ensuring that officers have a guardian mindset as opposed to a warrior mindset. It will have an increased emphasis on de-escalation, crisis/mental health training, and implicit bias. The Justice Academy has also created many other training topics, such as training on protest response and an optional de-escalation training model as a "train-the-trainer" course in April of this year. To date, 180 officers from 179 agencies have received this training.

As this reform work was ongoing, legislation was passed (Session Law 2021-138) which allows both Standards Commissions to more quickly set in-service training topics instead of going through administrative rulemaking. This change will enable the Standards Commissions to make changes more efficiently in response to immediate needs and should prove critical to the success of the state's law enforcement training efforts.

Going forward, the Standards Commissions' Joint In-Service Training (Joint IST) committee has identified its plan to set new training requirements periodically that are consistent with these new legislative mandates, advancements in the field, and the call for policing reform. In this context, TREC recently presented several recommendations to the Standards Commission's Joint IST committee, including updates to baseline crisis intervention training, duty to intervene, protest response, and robust de-escalation training as periodic requirements. Other stakeholders, from advocacy groups to the SBI, have made similar recommendations, and the Standards Commissions are considering all options.

Recommendation #22: Train all public school employees and SROs on the proper role of SROs.

The Standards Commissions have already recognized that SROs need specialized training and have created a mandate accordingly. At the same time, TREC recommended that both SROs and school personnel receive training on the proper use of an SRO to keep the juvenile system out of areas that should be handled by school discipline and/or restorative practices. The North Carolina Department of Public Instruction's Center for Safer Schools is working to develop a training on this issue and the Justice Academy is considering updates to its SRO training on this topic.

RULE CHANGES UNDERWAY AT THE COMMISSIONS

Recommendation #27: Adopt a mandatory statewide policy on law enforcement facilitation of peaceful demonstrations.

Recommendation #28: Create and update protest guidelines to consider best practices and First Amendment concerns.

Recommendation #40: Revise standards to require that officers not engage in excessive or unjustified use of force or abuse the power of the position.

Recommendation #41: Expand authority to allow for suspension, revocation, or denial of certification based upon an officer's excessive use of force or abuse of power.

Recommendation #42: Require notification by both the officer and the agency for specific use of force incidents.

Recommendation #43: Increase transparency about officer discipline and decertification through a publicly available database.

Recommendation #44: Support psychological screenings for all law enforcement officers.

Recommendation #45: Repeat psychological evaluations either after a certain number of years of service or before promotion.

Recommendation #46: Strengthen the ongoing development of a statewide law enforcement accreditation program.

Recommendation #51: Develop and disseminate best practices guide for recruitment and retention.

Recommendation #52: Expand Criminal Justice Fellows program statewide.

Recommendation #53: Collect data on law enforcement recruitment and diversity efforts.

Recommendation #55: Require law enforcement agencies of a certain size to create a diversity task force.

Recommendation #60: Study the effects of officers' physical and mental health on job performance.

TREC presented to both Standards Commissions regarding its policy recommendations to improve accountability for use of force, mandate accreditation statewide, and the creation of diversity task forces for law enforcement agencies. Both Standards Commissions agreed to refer our recommendations to the appropriate committees for rulemaking consideration. The Standards Commissions have developed a voluntary pilot NC Law Enforcement Accreditation program using GCC funding.

We look forward to the Standards Commissions' consideration of these important ideas. In the case of accreditation, the General Assembly would need to require the mandate, but the Standards Commissions' collaboration and support is critical.

LOCAL IMPLEMENTATION OF TREC RECOMMENDATIONS

Many of the recommendations made in TREC's December 2020 report require local implementation. Depending on the specific nature of the recommendation and/or the locality in question, a variety of different stakeholders, from law enforcement to non-profits to court officials, can be the principal instigator for change. Much of our work to date has been creating materials that clarify the exact steps different local actors can take to implement these system-changing programs and policies.

Our local strategy moving forward will rely on these materials to promote change in cities and counties across the state. The details of our strategy can be found in the sections below. But first, we would like to highlight some of the great and numerous ways localities around North Carolina have implemented the TREC recommendations in the past year.

EXAMPLES OF TREC SOLUTIONS IN PRACTICE

Across North Carolina, communities are working to implement racial equity reforms recommended in the TREC report. In May, Wake County approved changes to the role of SROs in schools. In June, Buncombe County approved a plan to improve justice outcomes for communities impacted by racial inequity, which included a number of criminal justice recommendations. In June, Fayetteville approved plans to create a citizen's advisory board. In September, New Hanover County committed to funding violence prevention and invention programs in the wake of school violence. In September, the city of Durham earned a partnership with the Harvard Kennedy School Government Performance Lab to implement an alternative responder program. The Greensboro Police Department deployed a co-responder team to respond to mental health calls. The Raleigh Police Department trained its entire department on its duty to intervene policy. In June, the town of Chapel Hill issued a "Reimagining Community Safety" Task Force report, which built on many ideas from the TREC report. Several communities are engaging in the process to create SJPs, including Judicial District 13 in Jackson County which formalized their SJP in October 2021. Judicial districts are continuing to participate in court reform pilot projects like the newly launched UNC School of Government's Court Appearance project in New Hanover, Orange, and Robeson counties. Bond policy revisions and pretrial reforms are also are also underway, including a new bond policy in Cumberland County as of September 2021 and an ongoing reform project in Orange County. These changes represent progress toward implementing TREC's recommendations and promoting racial equity in communities across the state. TREC's informational materials and presentations aim to build on these local efforts.

JUDICIAL DISTRICT SURVEYS

TREC made clear in the December 2020 report that quantitative research and empirical evidence are critical to understanding the scope of our challenges and track our progress. This includes collecting data related to our own recommendations and their implementation status. Therefore, over the summer of 2021, TREC drafted three separate surveys for all law enforcement agencies, prosecutors, and superior and district court judges in North Carolina on their current policies and practices in areas covered in the TREC report. We will use the results to understand how these stakeholders are addressing TREC-recommended changes, to serve as a baseline for assessing implementation progress, and to direct resources and assistance.

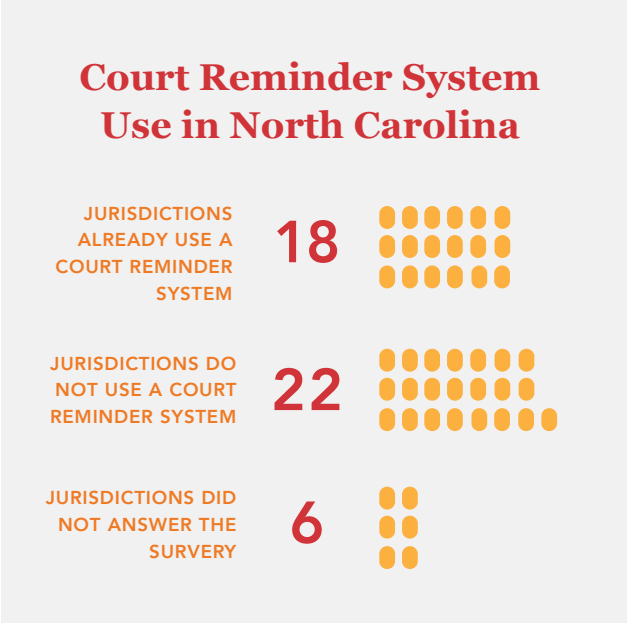
TREC partnered with the Duke School of Science and Law to analyze the results of the judicial survey. The researchers found that most judicial jurisdictions are interested in policy reforms, but the time investment needed for policy development and a lack of partnerships pose barriers to change for many. TREC aims to work with jurisdictions to expand the below recommended policies, along with others included in the survey, to more judicial jurisdictions across the state.

We will conduct a survey again in one year to assess adoption of model policies and implementation of recommended programs.

COURT REMINDER SYSTEM

Recommendation #82: Automatically enroll defendants for the NCAOC's court reminder system.

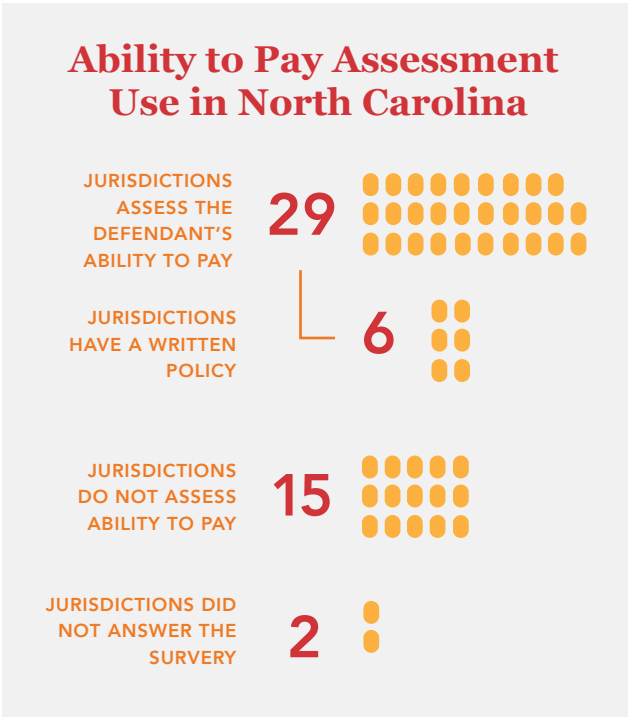
There are administrative changes that could be adopted to help mitigate some of the disproportionate burdens people of color face when interacting with the criminal justice system. That includes implementing a court reminder system to improve attendance and reduce the chances an individual fails to appear in court.



ASSESSMENT OF ABILITY TO PAY

Recommendation #101: Assess a defendant's ability to pay prior to levying any fines and fees.

Trial court judges retain significant discretion under existing law to waive or reduce certain fines and fees imposed on individuals in criminal or civil proceedings, and the Supreme Court of North Carolina could enact a general rule of practice addressing some aspects of this issue.



MODEL POLICY DEVELOPMENT

Many recommendations by TREC advocated for the implementation of specific policies or establishment of new programs. Over the past year, we realized a resource gap exists for many stakeholders to research and draft policies on top of their regular duties. On the programmatic front, getting started can be the hardest part – gathering best practices, understanding funding options and thinking through necessary partnerships can be a big lift for already busy stakeholders.

To advance local reform, TREC has established a project to create or collect model policies and information sheets for TREC recommended programs. We have also created one-pagers to distill the TREC report into immediate, actionable steps to be taken by a specific system actor. These will help guide North Carolina's law enforcement agencies implementing these policies and programs that advance racial equity and uphold public safety.

Several documents are already live on the TREC model policy package webpage, and the catalogue will continue to grow. These will serve as an integral part of our local implementation strategy.

MODEL POLICIES

- Traffic Stops
- Consent Searches
- Early Intervention Systems
- Suggested Jury Practices to Judges
- Nonpayment of Fines and Fees
- Prosecutor Guide
  - Data Collection
  - Habitual Felony Review Process/Restrictions
  - Officer Involved Use of Force
  - Minimum Age of Prosecution
  - School-based Referrals
  - Ability to Pay
  - Advanced Supervised Release
  - Bail / Pretrial Policy
  - Juries
  - Dismissal of Criminal Justice Debt
  - Expunction Efforts
  - De-prioritization of Low-Level Offenses: Marijuana / Traffic Offenses / Class 3 Misdemeanors

INFORMATION SHEETS

- Pre-Arrest Diversion
- Post-Arrest Diversion
- Reimaging 911
- Use of Force
- Violence Prevention
- Restorative Justice

ONE PAGERS

- Prosecutors
- Judges and Judicial Officers
- Local Government Officials
- Juvenile Justice System Actors
- Local Law Enforcement

COMMUNITY ENGAGEMENT

Since its formation, TREC has been committed to engaging with the public and key partners in the implementation of the report's recommendations. TREC's outreach has been ongoing and responsive to a range of identified opportunities and needs for local decision-makers. Outreach events have provided education for the public on complex topics and for local elected officials on best practices and time-sensitive funding opportunities. Additionally, TREC has continued to welcome and receive feedback from citizens committed to a fairer justice system.

LEARNING SERIES

TREC's "Learning Series" presents an opportunity to dive deeper into complex, cross-cutting issues relating to racial disparities in the criminal justice system. These sessions bring together experts, practitioners, advocates, and community members for an honest, in-depth conversation, with the goal of building knowledge and a shared commitment to advancing TREC's mission. To date, TREC has hosted four learning sessions.

The first learning session, "Race, Data, and Policing," examined law enforcement's increased reliance on data and predictive analytics to make policing decisions and the ways this reliance can have the unintended consequence of exacerbating the racial discrimination and disparity in the criminal legal system. The second session, "Victims of Color," explored whether victims of color are treated differently than white victims by police, prosecutors, judges, and juries, in general or in specific kinds of cases. The third session, "Local Solutions to Substance Misuse," discussed the public health crisis of addiction and local solutions to help those struggling with substance use. The fourth session, "Embracing Inclusive Juries," explored the challenges and possibilities of racially-equitable jury system reform. Going forward, TREC will continue to host learning series to spotlight important and emerging issues.

TREC's "Learning Series" present an opportunity to dive deeper into complex, cross-cutting issues.

COUNTY COMMISSIONERS

Local government actors are critical to the system changes that TREC has recommended. This includes county commissioners, who provide funding for schools, court systems, and community-based interventions to public safety issues. In 2021, the North Carolina Association of County Commissioners (NCACC) agreed to forge an ongoing partnership with TREC to discuss these ideas among county commissioners across the state. In August 2021, TREC presented to the NCACC's annual meeting and brought experts on pretrial services, emergency response reform, and diversion/ school justice partnerships. TREC will continue collaboration with the NCACC's Justice and Public Safety Steering Committee to continue these conversations with local government leaders.

COUNCIL OF GOVERNMENTS

TREC presented to regional councils of government (COGs) across the state whose boards are comprised entirely of municipal and county officials. To date, teams have presented to eight COGs including the statewide Board of Council of Governments. More presentations are scheduled.

ARP SESSIONS

3 technical assistance sessions

for local communities preparing to utilize their American Rescue Plan (ARP) funding

500+ attendees participated on these calls

PUBLIC COMMENT SESSIONS

14 members of the public

reached out across four public comment sessions

75+ letters recieved in 2021 sharing constituents perspectives

COUNCIL OF GOVERNMENT

8 COG presentations

given by our teams

including the statewide Board of Council of Governments

STAKEHOLDER GROUPS FORMED

From its beginnings, TREC has sought to engage stakeholder groups in its work. As we seek to implement recommendations, particularly on the local level, it is important to consult with stakeholder groups. That means continuing to consult with partners like the GCC and the North Carolina Commission on Racial and Ethnic Disparities. We also created new stakeholder groups including the Law Enforcement Advisory Group (LEAG) to provide real world insight into policing policy recommendations. TREC believes that law enforcement engagement and buy-in is critical in our work. The LEAG has met a half a dozen times and has provided valuable input. We will be starting similar groups for prosecutors, victims/survivors, and victim advocates in the coming months.

THE WORK AHEAD

Significant work remains to accomplish TREC's recommendations to improve law enforcement and the courts in North Carolina and make these systems more racially equitable. Priority areas for 2022 include continuing to:

- Improve policing practices, including our recommendations around training and use of force.
- Enhance law enforcement accountability, including recommendations such as establishing a statewide sentinel event review process and a comprehensive public use of force database, requiring body-worn cameras, releasing footage promptly during critical incidents, and further addressing the wandering officer problem.
- Invest in community-based solutions to reduce violence.
- Reduce reliance on fines and fees, and financial conditions in the pretrial period.
- Improve data systems so that policymakers, researchers, and the public better understand the criminal justice system and its impacts.
- Promote ideas that reduce the number of school-based juvenile justice system referrals, including hiring more behavioral health professionals in schools, and better equipping all adults with the tools they need to work with our children by training them on mental health, first aid, cultural competence/ diversity/inclusion, and developmental disability.

TREC will advance its goals through a variety of strategies including:

- Pursuing a legislative agenda in the short session
- Working with state agencies
- Partnering with local governments and law enforcement agencies and promoting regional collaboration
- Leveraging funding opportunities within state government and working with philanthropic partners
- Developing trainings, model policies, and resources to aid stakeholders in implementation, and
- Educating the public about our recommendations and the need to improve racial equity in the criminal justice system.

The following TREC committees will continue to meet and refine implementation strategies throughout 2022: executive, legislative, local policy, judicial, data, and communications.

Recognizing that there are a variety of different perspectives on the state of the criminal justice system in North Carolina, we will continue to work with all interested stakeholders and identify common ground in order to continue making tangible progress.

Finally, TREC recommendations were not intended to be the final word on changes necessary to improve criminal justice in North Carolina. The nature of ambitious and far-reaching recommendations is that they are unlikely to be accomplished in a single year or two, and as changes are implemented and the results studied and understood, new goals and needs will emerge. To that end, TREC recommended its work be institutionalized in state government beyond 2022. Next year, we will explore sustainability strategies so that the work of advancing racial equity in criminal justice continues.

IMPLEMENTATION STATUS CHARTS

The charts below reflect the status of TREC's 125 Recommendations as of December 2021. The listed solutions, recommendations, and necessary actions were defined in the original report published in December 2020. The implementation effort and status columns reflect TREC's progress over the past year.

DEFINITIONS OF THE RECOMMENDATION STATUSES

Success: Recommendation and/or necessary action identified by TREC is complete.

Partial Success: Part of the recommendation and/or necessary action is complete and additional effort is needed to fulfill the full recommendation or accomplish implementation.

Under Consideration: TREC has presented the recommendation to relevant stakeholders associated with the determined implementation effort and they are considering enactment.

Strategy in Development by Task Force: TREC is actively developing a strategy on this recommendation, including the development of model policies, stakeholder convenings and meetings, facilitation of funding opportunities, and other advocacy.

Not Accomplished: Implementation efforts have not been successful to date or have not yet begun.

Reimagining Public Safety

Solution Number	Recommendation	Soution	Necessary Action	Implementation Effort	Status
1	Reimagine public safety and reinvest in communities	Respond more appropriately to situations concerning mental illness, autism, intellectual disabilities, substance abuse, homelessness, and other non-emergency situations	Local policy change; Administrative rule change by Standards Commissions; Legislative change	Governor's Crime Commission / DHHS - Funding Opportunity	Partial Success
2	Reimagine public safety and reinvest in communities	Add crisis intervention training for current law enforcement officers	Local policy change; State administrative rule change by the Standards Commissions; Legislative change	Standards Commissions	Under Consideration
3	Reimagine public safety and reinvest in communities	Fund grassroots organizations that employ promising and peaceful strategies to help communities promote public safety	Local policy change; State policy change	Local Implementation Work	Under Consideration
4	Reimagine public safety and reinvest in communities	Develop and provide funding to help communities build violence prevention programs	Local policy change; State policy change	Governor's Crime Commission - Funding Opportunity	Partial Success
5	Reimagine public safety and reinvest in communities	Form local Community Safety and Wellness Task Forces to examine public safety and wellness needs	Local policy change	Local Implementation Work	Under Consideration

Improving Policing Practices

Solution Number	Recommendation	Soution	Necessary Action	Implementation Effort	Status
6	Strengthen community policing practices	Adopt community policing philosophies and plans in collaboration with the communities law enforcement serve	Local agency policy change; State agency policy change	Local Implementation Work	In Development
7	Strengthen community policing practices	Train law enforcement agency heads on community policing	State policy change by North Carolina Justice Academy	Legislative	Partial Success
8	Strengthen community policing practices	Encourage or require officers to spend non-enforcement time, or live in, the neighborhoods they serve	Local agency policy change; State agency policy change; Local government policy change	Local Implementation Work	In Development
9	Strengthen community policing practices	Publicly acknowledge mistakes by law enforcement to build trust and transparency	Local agency policy change; State agency policy change	Local Implementation Work	In Development
10	Reform investigations	Improve law enforcement drug enforcement data collection and reporting	Legislative change	Legislative	Not Accomplished
11	Reform investigations	Use data and objective criteria, instead of officers' subjective perceptions and beliefs, to drive the level of police presence in neighborhoods	State policy change; Local policy change	Recommendation with Task Force	Not Accomplished
12	Reform investigations	Deemphasize felony drug posession arrests for trace quantities under .25 grams	State agency policy change; Local agency policy change	Local Implementation Work - Model Policy	In Development
13	Reform investigations	Prioritize traffic stops that improve traffic safety	State agency policy change; Local agency policy change	Local Implementation Work - Model Policy	In Development
14	Reform investigations	Require all consent searches to be based on written, informed consent	State agency policy change; Local agency policy change; Legislative change	Local Implementation Work - Model Policy	In Development
15	Reform investigations	Restrict state law enforcement use of asset forfeiture on low-level seizures where there is no conviction	Agency policy change; Task Force collaboration; Legislative change	Recommendation with Task Force	Not Accomplished
16	Promote diversion and other alternatives to arrest	Establish and expand access to diversion programs	State policy change; Local policy change; Legislative change	Department of Health and Human Services - Funding Opportunity; Inclusion in Budget	Partial Success
17	Promote diversion and other alternatives to arrest	Treat addiction as a public health crisis, including substance use addictions that disproportionately impact Black and brown communities, such as crack cocaine	State policy change; Task Force collaboration	Local Implementation Work - Model Policy	In Development

Improving Policing Practices

Solution Number	Recommendation	Soution	Necessary Action	Implementation Effort	Status
18	Promote diversion and other alternatives to arrest	Encourage citations and summons in lieu of arrest whenever possible	State agency policy change; Local agency policy change; Legislative change	Local Implementation Work - Model Policy	In Development
19	Revise the role of School Resource Officers	Hire behavioral health professionals in schools	Local policy change; Legislative change	Legislative	Under Consideration
20	Revise the role of School Resource Officers	Fund school personnel training on mental health, first aid, cultural competence/ diversity/inclusion, and developmental disability	Local policy change; Legislative change	Legislative	Not Accomplished
21	Revise the role of School Resource Officers	Develop inclusive processes for selecting and overseeing SROs	Local policy change	Local Implementation Work	Under Consideration
22	Revise the role of School Resource Officers	Train all public school employees and SROs on the proper role of SROs	State policy change by the Department of Public Instruction and the Justice Academy	North Carolina Center for Safer Schools/ North Carolina Justice Academy	Under Consideration
23	Revise the role of School Resource Officers	Collect data on discipline in schools and school-based referrals to the juvenile courts	State policy change by the Department of Public Instruction and the Department of Public Safety; Local agency policy change	Department of Public Safety	Success
24	Revise the role of School Resource Officers	Encourage School Justice Partnerships to reduce students' juvenile court involvement	Local policy change	Adminstrative Office of the Courts	Partial Success/Under Consideration
25	Revise the role of School Resource Officers	Support Task Force on Safer Schools State Action Plan	Task Force collaboration	Recommendation with Task Force	Success
26	Codify judicial approval of no-knock warrants and clarify requirements for use of force in serving search warrants	Change entry by force statute to require the necessary probable cause be specifically listed in the warrant before breaking and entering to execute a warrant and to clarify the meaning of unreasonable delay after an officer announces presence in the execution of a search warrant	Legislative change	Legislative	Not Accomplished

Improving Policing Practices

Solution Number	Recommendation	Soution	Necessary Action	Implementation Effort	Status
27	Peacefully facilitate protests and demonstrations	Adopt a mandatory statewide policy on law enforcement facilitation of peaceful demonstrations	Local agency policy change; State agency policy change; State administrative rule change by the Standards Commissions	Department of Public Safety	Partial Success
28	Peacefully facilitate protests and demonstrations	Create and update protest guidelines to consider best practices and First Amendment concerns	State administrative rule change by the Standards Commissions	Standards Commissions	Under Consideration
29	Peacefully facilitate protests and demonstrations	Review and update protest and demonstration training	State policy change by North Carolina Justice Academy; State administrative rule change by the Standards Commissions; Task Force collaboration	North Carolina Justice Academy	Success
30	Peacefully facilitate protests and demonstrations	Commission a study on racial disparities in how protests and demonstrations are policed in North Carolina	State policy change	Study	In Development
31	Revise use of force policies	Strengthen use of force practices including to prohibit neck holds and require the use of the minimum amount of force necessary	Local agency policy change; State agency policy change; Legislative change	Legislative	Not Accomplished
32	Revise use of force policies	Require officers to have first aid kits and render aid	Local agency policy change; State agency policy change	Legislative	Not Accomplished
33	Revise use of force policies	Enact agency policies requiring a duty to intervene and report excessive use of force or other abuse	Local agency policy change; State agency policy change	Legislative	Partial Success
34	Revise use of force policies	Establish early intervention systems for officers repeatedly violating use of force policies	Local agency policy change; State agency policy change; Legislative change	Legislative	Success
35	Revise use of force policies	Define and collect use of force data	Local agency policy change; State agency policy change	Legislative	Partial Success

Enhancing Accountability

Solution Number	Recommendation	Soution	Necessary Action	Implementation Effort	Status
36	Improve law enforcement accountability and culture	Expand investigative and oversight authority of local citizen oversight boards	Local policy change; Legislative change	Legislative	Not Accomplished
37	Improve law enforcement accountability and culture	Reform investigation and prosecution procedures for officer-involved use of force incidents	Legislative change	Legislative	Partial Success
38	Improve law enforcement accountability and culture	Establish statewide sentinel event reviews to evaluate law enforcement practices and suggest policy changes	State agency policy change by Standards Commission; Local agency policy change; Legislative change	Recommendation with Task Force	Not Accomplished
39	Improve law enforcement accountability and culture	Support Rap Back Program	Task Force collaboration; Legislative change	Legislative	Success
40	Improve law enforcement accountability and culture	Revise standards to require that officers not engage in excessive or unjustified use of force or abuse the power of the position	State administrative change by Standards Commissions	Standards Commissions	Under Consideration
41	Improve law enforcement accountability and culture	Expand authority to allow for suspension, revocation, or denial of certification based upon an officer's excessive use of force or abuse of power	State administrative change by Standards Commissions	Standards Commissions	Under Consideration
42	Improve law enforcement accountability and culture	Require notification by both the officer and the agency for specific use of force incidents	State administrative change by Standards Commissions; Task Force collaboration	Standards Commissions	Under Consideration
43	Improve law enforcement accountability and culture	Increase transparency about officer discipline and decertification through a publicly available databse	NCDOJ policy and procedure change; Task Force collaboration	Legislative	Success
44	Improve law enforcement accountability and culture	Support psychological screenings for all law enforcement officers	State administrative change by Standards Commissions	Legislative	Success

Enhancing Accountability

Solution Number	Recommendation	Soution	Necessary Action	Implementation Effort	Status
45	Improve law enforcement accountability and culture	Repeat pscyhological evaluations either after a certain number of years of service or before promotion	State administrative change by Standards Commissions	Standards Commissions	Under Consideration
46	Improve law enforcement accountability and culture	Strengthen the ongoing development of a statewide law enforcement accreditation program	Administrative rule change by Standards Commissions; Task Force collaboration; Legislative change	Standards Commissions	Under Consideration
47	Mandate use of body worn/ dashboard cameras and increase transparency of footage	Mandatory body worn cameras for all law enforcement agencies	Legislative change	Legislative	Not Accomplished
48	Mandate use of body worn/ dashboard cameras and increase transparency of footage	Deploy dashboard cameras in all patrol and field vehicles, except for undercover vehicles	Local agency policy change; State agency policy change; Legislative change	Legislative	Not Accomplished
49	Mandate use of body worn/ dashboard cameras and increase transparency of footage	Provide citizen oversight boards and local government governing bodies access to law enforcement recordings	Local agency policy change; State agency policy change; Legislative change	Legislative	Not Accomplished
50	Mandate use of body worn/ dashboard cameras and increase transparency of footage	Require police recordings of critical incidents to be publicly released within 45 days	Legislative change	Legislative	Not Accomplished

Strengthening Recruitment, Training, and the Profession

Solution Number	Recommendation	Soution	Necessary Action	Implementation Effort	Status
51	Recruit and retain a racially equitable work force	Develop and disseminate best practices guide for recruitment and retention	Local agency policy change; State agency policy change; Administrative rule change by Standards Commissions; Task Force collaboration; Legislative change	Legislative	Success
52	Recruit and retain a racially equitable work force	Expand Criminal Justice Fellows program statewide	Legislative change	Legislative	Partial Success
53	Recruit and retain a racially equitable work force	Collect data on law enforcement recruitment and diversity efforts	Local agency policy change; State agency policy change; Administrative rule change by Standards Commissions; Legislative change	Standards Commissions	Under Consideration
54	Recruit and retain a racially equitable work force	Ensure the North Carolina Administrative Code provisions regarding Minimum Standards and Revocation, Denial, and Decertification are the same for both Commissions	Administrative rule change by Standards Commissions	Standards Commissions	Success
55	Recruit and retain a racially equitable work force	Require law enforcement agencies of a certain size to create a diversity task force	Local agency policy change; State agency policy change; Task Force collaboration; Legislative change	Standards Commissions/ Legislative	Under Consideration
56	Train law enforcement to promote public safety and earn community support	Revamp basic enforcement training	State policy change by the Standards Commissions and the North Carolina Justice Academy; Administrative code changes; Legislative change	North Carolina Justice Academy	Partial Success
57	Train law enforcement to promote public safety and earn community support	Recommend changes to in-service training	State policy change by North Carolina Justice Academy; Administrative rule change by Standards Commissions; Legislative change	Legislative	Partial Success

Strengthening Recruitment, Training, and the Profession

Solution Number	Recommendation	Soution	Necessary Action	Implementation Effort	Status
58	Train law enforcement to promote public safety and earn community support	Require trainings on internal law enforcement agency policies	Local agency policy change; State agency policy change	North Carolina Justice Academy	Under Consideration
59	Train law enforcement to promote public safety and earn community support	Evaluate law enforcement training programs for effectiveness and desired outcomes	State policy change by North Carolina Justice Academy; Task Force collaboration; Legislative change	North Carolina Justice Academy	Under Consideration
60	Enhance the law enforcement profession	Study the effects of officers' physical and mental health on job performance	Local agency policy change; State agency policy change; State administrative rule change by the Standards Commissions	Standards Commissions	Partial Success

Eliminating Racial Disparities in the Courts

Solution Number	Recommendation	Soution	Necessary Action	Implementation Effort	Status
61	Support restorative justice initiatives and victim equity	Establish and fund restorative justice programs in local communities across the state and at various points of the criminal justice system	Local policy change	Governor's Crime Commission - Funding Opportunity	Partial Success
62	Support restorative justice initiatives and victim equity	Form a victim advisory group to help develop restorative justice programs and other equity programs for crime victims	Local policy change; Task Force collaboration	Recommendation with Task Force	In Development
63	Support restorative justice initiatives and victim equity	Improve and expand access to North Carolina's Victim Compensation Fund to increase racial equity	State policy change by the Department of Public Safety	Department of Public Safety	Not Accomplished
64	Support restorative justice initiatives and victim equity	Screen incarcerated individuals for victimization and provide appropriate services	State policy change by the Department of Public Safety	Department of Public Safety	Under Consideration
65	Support restorative justice initiatives and victim equity	Recognize racial equity and the rights and perspectives of, and the potential consequences to, harmed parties, survivors, and their families during the justice system process and when any reform is proposed	State policy change; Task Force collaboration	Recommendation with Task Force	In Development
66	Stem the school to prison pipeline and rethink juvenile justice	Raise the minimum age of juvenile court jurisdiction to 12	Legislative change	Legislative	Partial Success
67	Stem the school to prison pipeline and rethink juvenile justice	Require a school administrator or school social worker to sign a school-based petition initiated by a School Resource Officer before it can be accepted for filing in juvenile court	Legislative change	Legislative	Not Accomplished
68	Stem the school to prison pipeline and rethink juvenile justice	Allow prosecutors the discretion to accept pleas in juvenile court for juveniles charged with Class A through G felonies, in line with the Raise the Age Act	Legislative change	Legislative	Partial Success

Eliminating Racial Disparities in the Courts

Solution Number	Recommendation	Soution	Necessary Action	Implementation Effort	Status
69	Stem the school to prison pipeline and rethink juvenile justice	Replace juvenile life without parole with life with parole sentences and parole eligibility after twenty-five years for first degree murder convictions	Legislative change	Legislative	Not Accomplished
70	Stem the school to prison pipeline and rethink juvenile justice	Establish a juvenile review board within the Governor's Clemency Office	State policy change	Executive Order	Success
71	Decriminalize marijuana possession	Deprioritize marijuana-related arrests and prosecution	State agency policy change; Local agency policy change; Prosecutorial policy change	Local Implementation Work - Model Policy	In Development
72	Decriminalize marijuana possession	Decriminalize the possession of up to 1.5 ounces of marijuana	Legislative change	Legislative	Not Accomplished
73	Decriminalize marijuana possession	Convene a task force of stakeholders to study the pros and cons and options for legalization of possession, cultivation and/or sale of marijuana	State policy change; Legislative change	Legislative	Not Accomplished
74	Shrink the criminal code	Reclassify Class III misdemeanors that do not impact public safety or emergency management as noncriminal/civil infractions	Legislative change	Legislative	Partial success
75	Shrink the criminal code	Enact legislation with a sunset provision for all local ordinance crimes that criminalize poverty or behavior in public places	Legislative change	Legislative	Success
76	Shrink the criminal code	Eliminate citizen-initiated criminal charges	Legislative change	Legislative	Not Accomplished
77	Shrink the criminal code	Review and recommend changes to the criminal code	Legislative change	Legislative	Success
78	Shrink the criminal code	Provide for the appointment of counsel in cases where the defendant is facing a $200 fine	Legislative change	Legislative	Not Accomplished
79	Improve pre-trial release and accountability practices	Eliminate cash bail for Class I, II, and III misdemeanors unless risk to public safety	Judicial policy change; State policy change by Administrative Office of the Courts; Legislative change	Local Implementation Work - Model Policy	In Development

Eliminating Racial Disparities in the Courts

Solution Number	Recommendation	Soution	Necessary Action	Implementation Effort	Status
80	Improve pre-trial release and accountability practices	Require first appearance within 48 hours or next day in which District Court is in session	Judicial policy change; State policy change by Administrative Office of the Courts; Legislative change	Legislative	Partial Success
81	Improve pre-trial release and accountability practices	Require preventative detention hearing within five days and repeal bond doubling	Legislative change	Legislative	Not Accomplished
82	Improve pre-trial release and accountability practices	Promote court appearance strategies and develop alternative responses to failure to appear	Judicial policy change; State policy change by Administrative Office of the Courts; Local policy change; Legislative change	Legislative/Local Implementation Work	In Development
83	Improve pre-trial release and accountability practices	Create independent pretrial services and improve data collection	Local policy change; State policy change by Administrative Office of the Courts	Local Implementation Work	Under Consideration
84	Implement racial equity training for court system actors	Require racial equity training for court system personnel, including judges, DAs, and public defenders	State policy change by Admistrative Office of the Courts	State Agency Work	Partial Success
85	Implement racial equity training for court system actors	Require implicit bias and racial equity training for parole staff	State policy change by the Department of Public Safety	Department of Public Safety	Success
86	Implement racial equity training for court system actors	Require racial equity and victim services training for Victim Compensation Fund employees and members	State policy change by the Department of Public Safety	Department of Public Safety	In Development
87	Promote racially equitable prosecutorial practices	Educate prosecutors, their staff, and officers of justice on unconscious bias in the criminal justice process and prosecutorial decision-making	State policy change by the Conference of District Attorneys	Conference of District Attorneys	Under Consideration
88	Promote racially equitable prosecutorial practices	Enhance prosecutors' data collection, technology, training opportunities, and staffing	Prosecutorial policy change; Legislative change	Local Implementation Work - Model Policy	In Development

Eliminating Racial Disparities in the Courts

Solution Number	Recommendation	Soution	Necessary Action	Implementation Effort	Status
89	Promote racially equitable prosecutorial practices	Study and adopt evidence-based reforms for reducing and eventually eliminating racial disparities in charging decisions and prosecutorial outcomes	Prosecutorial policy change; Legislative change	Local Implementation Work - Model Policy	In Development
90	Promote racially equitable prosecutorial practices	Establish working groups led by district attorneys to review and approve every habitual felony charging decision	Prosecutorial policy change	Local Implementation Work - Model Policy	In Development
91	Facilitate fair trials	Increase representation of North Carolinians serving on juries through expanded and more frequent sourcing, data transparency, and compensation	Local policy change; Local policy change by county jury commisions; Judicial change by senior resident superior court judges; Task Force collaboration; Legislative change	Study	In Development
92	Facilitate fair trials	Broaden protection against the use of preemptory challenges in jury selection for discriminatory purposes	Administrative rule change by North Carolina Supreme Court	Rule change by North Carolina Supreme Court	Not Accomplished
93	Facilitate fair trials	Provide implicit bias training to all jury system actors	State policy change; State policy change of the Administrative Office of the courts; Local judicial district change; Local judicial district change by clerks of court; Task Force collaboration; Legislative change	Administrative Office of the Courts	Not Accomplished
94	Facilitate fair trials	Establish a state commission on the jury system, with an eye towards comprehensive reform	State policy change; Legislative change	Study	In Development

Promoting Racial Equity
Post-Conviction

Solution Number	Recommendation	Soution	Necessary Action	Implementation Effort	Status
95	Reduce current sentencing and incarceration disparities	Increase funding for Governor's Clemency Office and Parole Commission	State policy change; State policy change by the Parole Commission; Legislative change; legislative appropriations	Legislative	Not Accomplished
96	Reduce current sentencing and incarceration disparities	Increase NCDPS flexibility on incarcerated individuals' release dates	State policy change by Department of Public Safety	Department of Public Safety	Under Consideration
97	Reduce current sentencing and incarceration disparities	Establish a Second Look Act to reduce racially disparate sentences through the review and action of those currently incarcerated	Legislative change	Legislative	Not Accomplished
98	Reduce current sentencing and incarceration disparities	Create and fund an independent Conviction Integrity Unit with representation from prosecutors and defense lawyers and to ensure Indigent Defense Services has significant funding to pay lawyers who handle post-conviction work	Legislative change	Legislative	Not Accomplished
99	Reduce current sentencing and incarceration disparities	Amend Motion for Appropriate Relief statute to allow a judge to overcome technical defects in the interest of justice or where the petition raises a significant claim of race discrimination	Legislative change	Legislative	Not Accomplished
100	Reduce current sentencing and incarceration disparities	Reinstate the Racial Justice Act for individuals sentenced to death	Legislative change	Legislative	Not Accomplished
101	Reduce use of fines and fees	Assess a defendant's ability to pay prior to levying any fines and fees	Administrative rule change by North Carolina Supreme Court	Rule change by North Carolina Supreme Court	Success
102	Reduce use of fines and fees	Reduce court fines and fees	Legislative change	Legislative	Not Accomplished
103	Reduce use of fines and fees	Eliminate state government reliance on fines and fees	Legislative change	Inclusion in Budget	Partial Success

Promoting Racial Equity
Post-Conviction

Solution Number	Recommendation	Soution	Necessary Action	Implementation Effort	Status
104	Reduce use of fines and fees	Develop a process to eliminate criminal justice debt	State agency policy change; Local government action; NC Supreme Court rule change; Task Force collaboration; Legislative change	Local Implementation Work - Model Policy	In Development
105	Amend incarceration facilities' practices and programming and address prison discipline	Transform the use of restrictive housing	State policy change by Department of Public Safety	Department of Public Safety	Under Consideration
106	Amend incarceration facilities' practices and programming and address prison discipline	Protect pregnant people in jails and prisons	State policy change by Department of Public Safety	Legislative	Success
107	Amend incarceration facilities' practices and programming and address prison discipline	Enhance prison personnel	State policy change by Department of Public Safety; Legislative changes	Legislative	Partial Success
108	Amend incarceration facilities' practices and programming and address prison discipline	Increase funding for mental health services and programs in prisons	State policy change by Department of Public Safety	Department of Public Safety	In Development
109	Amend incarceration facilities' practices and programming and address prison discipline	Increase due process protections for people accused of disciplinary offenses	State policy change by the Department of Public Safety	Department of Public Safety	Under Consideration

Promoting Racial Equity
Post-Conviction

Solution Number	Recommendation	Soution	Necessary Action	Implementation Effort	Status
110	Amend incarceration facilities' practices and programming and address prison discipline	Expand use of restorative justice and rehabilitation programming	State policy change by Department of Public Safety	Department of Public Safety	Partial Success
111	Study and revise future sentencing guidelines	Broaden the use of Advanced Supervised Release	Prosecutorial policy change; Legislative change	Local Implementation Work - Model Policy	In Development
112	Study and revise future sentencing guidelines	Eliminate the future use of Violent Habitual Felony Status	Legislative change	Legislative	Not Accomplished
113	Study and revise future sentencing guidelines	Eliminate future use of Habitual Felony Status for individuals under the age of 21 or convicted of non-violent drug offenses	Legislative change	Legislative	Not Accomplished
114	Study and revise future sentencing guidelines	Amend the habitual felony statute to limit the "look back" period to within 8 years of the charged offense	Legislative change	Legislative	Not Accomplished
115	Study and revise future sentencing guidelines	Analyze and report on racial disparities in sentencing laws and recommend possible changes	State policy change by the Sentencing Commission	Study	In Development
116	Study and revise future sentencing guidelines	Review all future sentences after 20 years or before	Legislative change	Legislative	Not Accomplished
117	Study and revise future sentencing guidelines	Prohibit capital punishment for people with serious mental illness and people 21 or younger at the time of the offense and prohibit the use of juvenile adjudications to be considered as aggravating factors	Legislative change	Legislative	Not Accomplished
118	Study and revise future sentencing guidelines	Establish a truth and reconciliation commission to study North Carolina's history of criminal justice and race	State policy change; Legislative change	Recommendations with Task Force	Not Accomplished

Promoting Racial Equity
Post-Conviction

Solution Number	Recommendation	Soution	Necessary Action	Implementation Effort	Status
119	Reduce collateral consequences of criminal convictions	Expand voting rights to those on probation, parole, or post-release supervision for a felony conviction	Legislative change	Legislative	Not Accomplished
120	Reduce collateral consequences of criminal convictions	Opt out entirely of federal ban on SNAP benefits for individuals convicted of certain felony drug charges, eliminating 6-month disqualification period and other eligibility requirements	Legislative change	Legislative	Not Accomplished
121	Reduce collateral consequences of criminal convictions	Allow NCDMV hearing officers to waive license restoration fees and other service fees for failure to appear or failure to pay	Legislative change	Legislative	Under Consideration
122	Reduce collateral consequences of criminal convictions	Reform the Certificate of Relief petition process to create efficiencies for individuals with multiple convictions across multiple counties	Legislative change	Legislative	Not Accomplished
123	Reduce collateral consequences of criminal convictions	Support the Statewide Reentry Council Collaborative's recommendations	State agency policy changes; Local government policy changes; Task Force collaboration; Legislative changes	Recommendation with Task Force	Success

Criminal Justice Data Collection and Reporting

Solution Number	Recommendation	Soution	Necessary Action	Implementation Effort	Status
124	Improve data collection	Identify the places along the criminal justice system where data collection directly impacts the implementation, evaluation, and monitoring of the Task Force's recommendations and broader questions of racial equity within the criminal justice system	State agency policy changes; Local government policy changes; Task Force collaboration; Adminstrative rule change; Legislative changes	Fact finding / Research	In Development

Going Forward

Solution Number	Recommendation	Soution	Necessary Action	Implementation Effort	Status
125	Create permanent structure	Establish the Commission for Racial Equity in the Criminal Justice System as a permanent, independent commission.	State policy change; Task Force collaboration; Legislative changes	Recommendation with Task Force	Not Accomplished