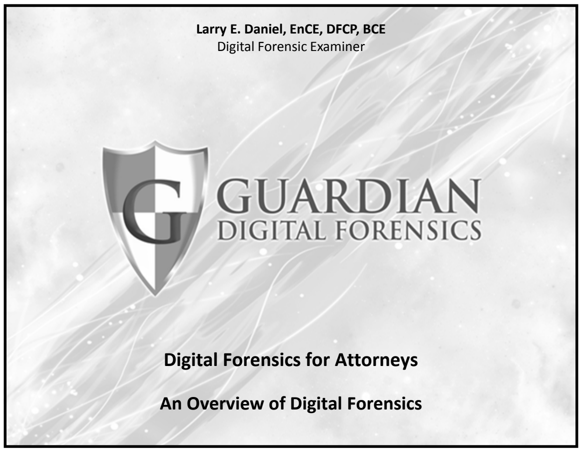
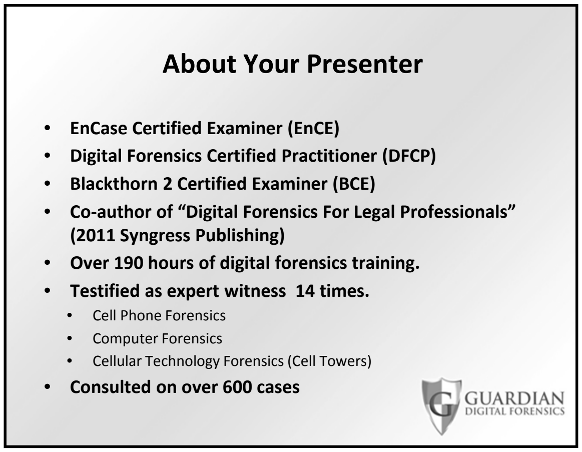


Larry E. Daniel, EnCE, DFCP, BCE
Digital Forensic Examiner

GUARDIAN
DIGITAL FORENSICS

Digital Forensics for Attorneys

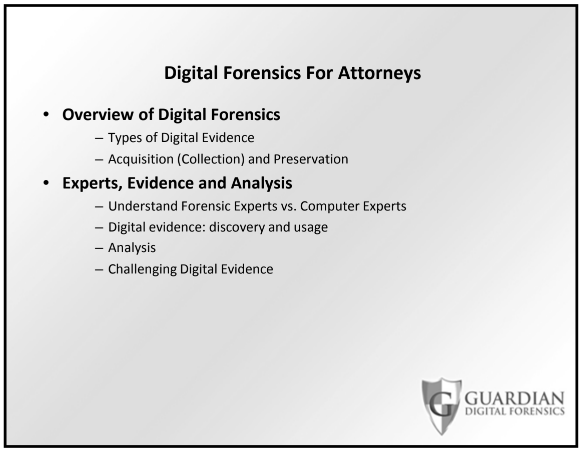
An Overview of Digital Forensics



About Your Presenter

- **EnCase Certified Examiner (EnCE)**
- **Digital Forensics Certified Practitioner (DFCP)**
- **Blackthorn 2 Certified Examiner (BCE)**
- **Co-author of "Digital Forensics For Legal Professionals" (2011 Syngress Publishing)**
- **Over 190 hours of digital forensics training.**
- **Testified as expert witness 14 times.**
  - Cell Phone Forensics
  - Computer Forensics
  - Cellular Technology Forensics (Cell Towers)
- **Consulted on over 600 cases**

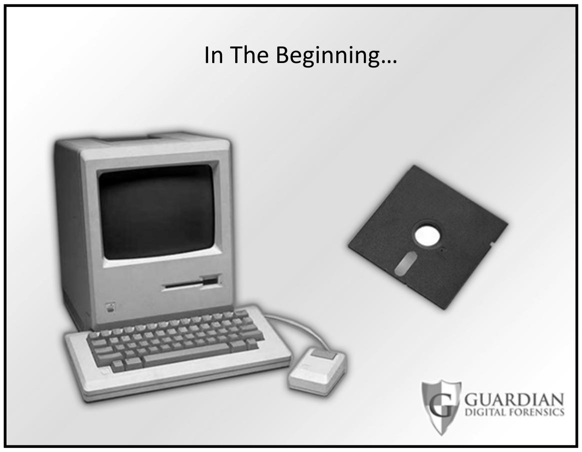
GUARDIAN DIGITAL FORENSICS



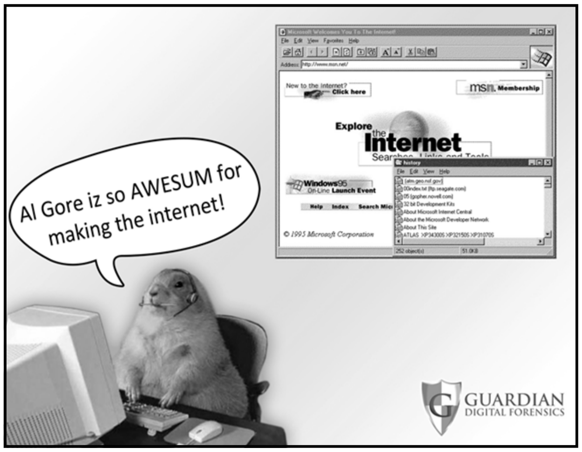
Digital Forensics For Attorneys

- **Overview of Digital Forensics**
  - Types of Digital Evidence
  - Acquisition (Collection) and Preservation
- **Experts, Evidence and Analysis**
  - Understand Forensic Experts vs. Computer Experts
  - Digital evidence: discovery and usage
  - Analysis
  - Challenging Digital Evidence

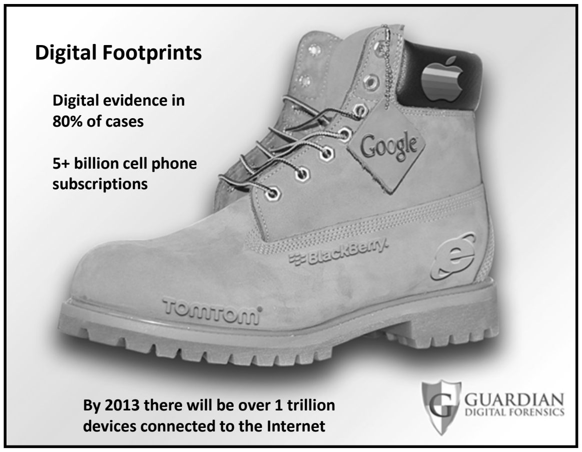
GUARDIAN DIGITAL FORENSICS



In The Beginning…



Al Gore iz so AWESUM for making the internet!
Microsoft Welcomes You To The Internet!
New to the Internet? Click here
msn Membership
Explore the Internet
Windows95 On-Line Launch Event
© 1995 Microsoft Corporation
GUARDIAN
DIGITAL FORENSICS



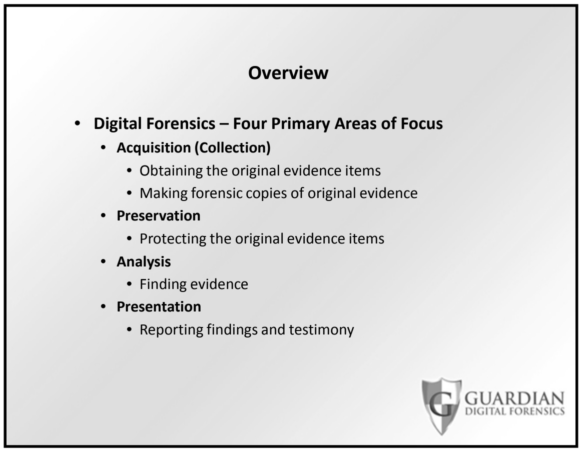
Digital Footprints

Digital evidence in 80% of cases

5+ billion cell phone subscriptions

By 2013 there will be over 1 trillion devices connected to the Internet

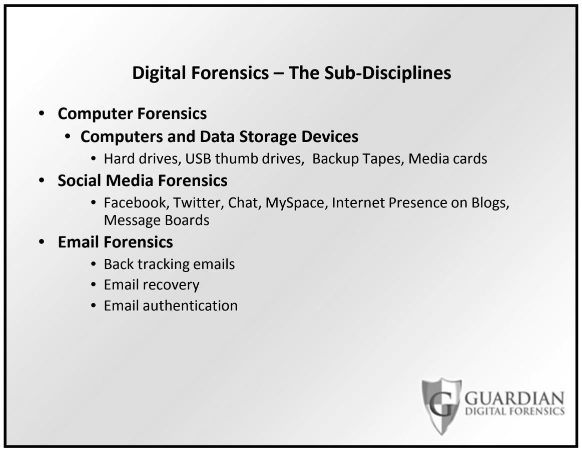
Google
BlackBerry
TomTom
GUARDIAN DIGITAL FORENSICS



Overview

- Digital Forensics – Four Primary Areas of Focus
  - **Acquisition (Collection)**
    - Obtaining the original evidence items
    - Making forensic copies of original evidence
  - **Preservation**
    - Protecting the original evidence items
  - **Analysis**
    - Finding evidence
  - **Presentation**
    - Reporting findings and testimony

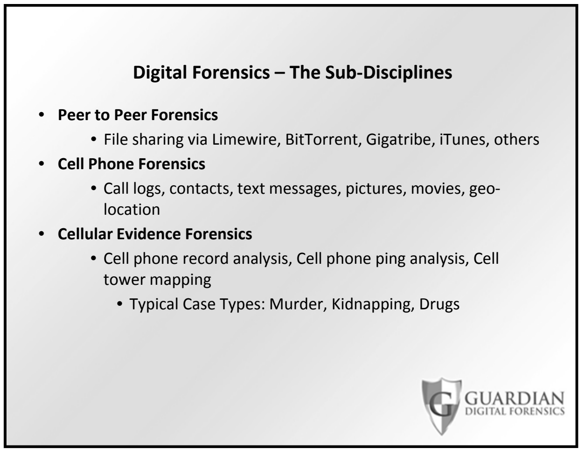
GUARDIAN DIGITAL FORENSICS



Digital Forensics – The Sub-Disciplines

- **Computer Forensics**
  - **Computers and Data Storage Devices**
    - Hard drives, USB thumb drives, Backup Tapes, Media cards
- **Social Media Forensics**
    - Facebook, Twitter, Chat, MySpace, Internet Presence on Blogs, Message Boards
- **Email Forensics**
    - Back tracking emails
    - Email recovery
    - Email authentication

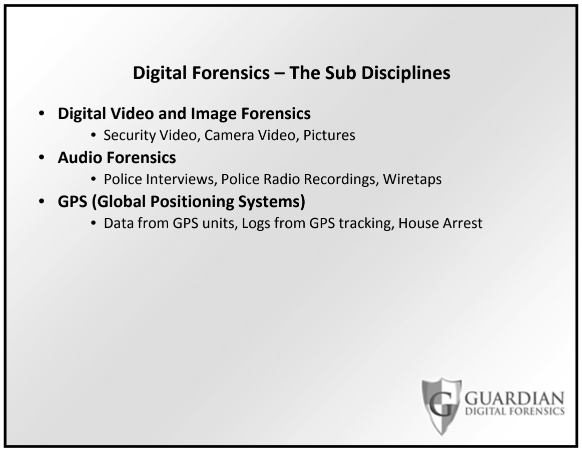
GUARDIAN DIGITAL FORENSICS



Digital Forensics – The Sub-Disciplines

- **Peer to Peer Forensics**
    - File sharing via Limewire, BitTorrent, Gigatribe, iTunes, others
- **Cell Phone Forensics**
    - Call logs, contacts, text messages, pictures, movies, geo-location
- **Cellular Evidence Forensics**
    - Cell phone record analysis, Cell phone ping analysis, Cell tower mapping
      - Typical Case Types: Murder, Kidnapping, Drugs

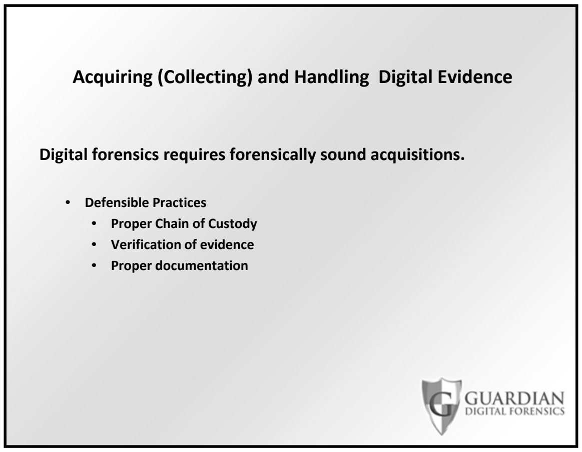
GUARDIAN DIGITAL FORENSICS



Digital Forensics – The Sub Disciplines

- **Digital Video and Image Forensics**
    - Security Video, Camera Video, Pictures
- **Audio Forensics**
    - Police Interviews, Police Radio Recordings, Wiretaps
- **GPS (Global Positioning Systems)**
    - Data from GPS units, Logs from GPS tracking, House Arrest

GUARDIAN DIGITAL FORENSICS

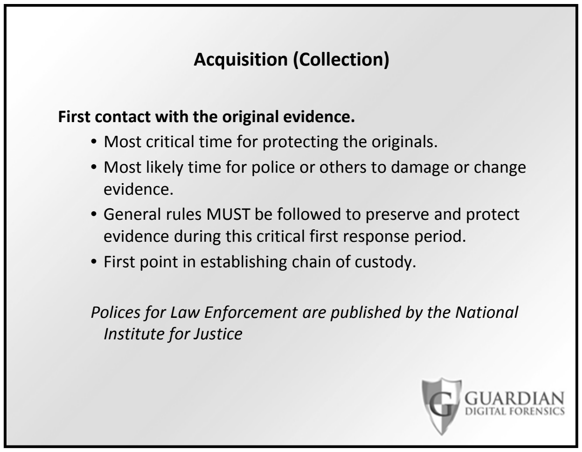


Acquiring (Collecting) and Handling Digital Evidence

Digital forensics requires forensically sound acquisitions.

- **Defensible Practices**
  - **Proper Chain of Custody**
  - **Verification of evidence**
  - **Proper documentation**

GUARDIAN
DIGITAL FORENSICS



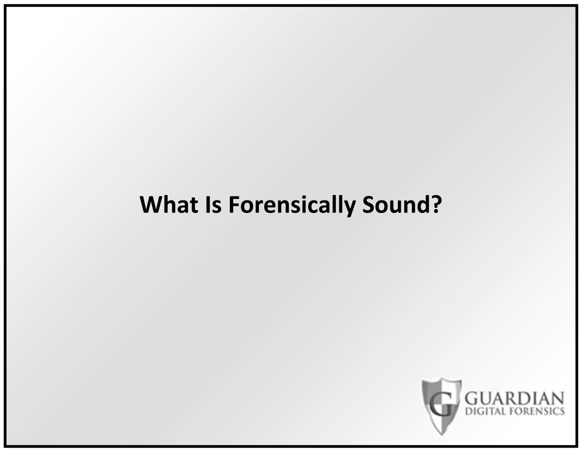
Acquisition (Collection)

First contact with the original evidence.

- Most critical time for protecting the originals.
- Most likely time for police or others to damage or change evidence.
- General rules MUST be followed to preserve and protect evidence during this critical first response period.
- First point in establishing chain of custody.

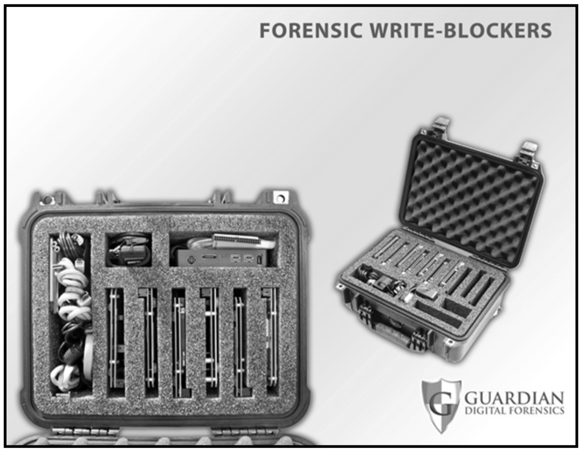
Polices for Law Enforcement are published by the National Institute for Justice

GUARDIAN
DIGITAL FORENSICS

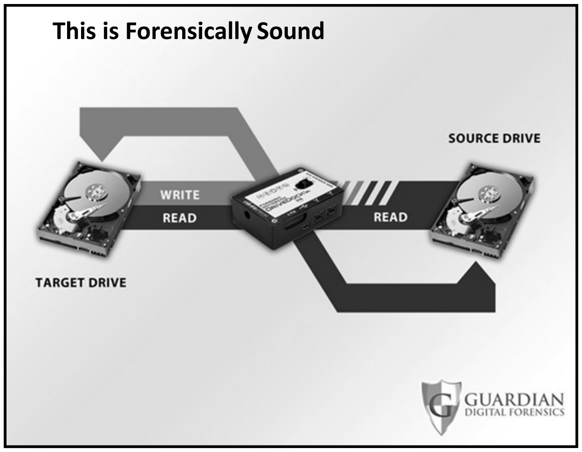


What Is Forensically Sound?

GUARDIAN
DIGITAL FORENSICS



FORENSIC WRITE-BLOCKERS



This is Forensically Sound

Verification Must Be Done

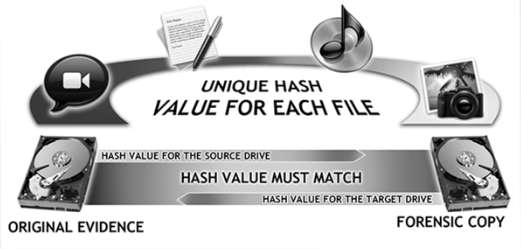
MD5 HASH

9e107d9d372bb6826bd81d3542a419d6

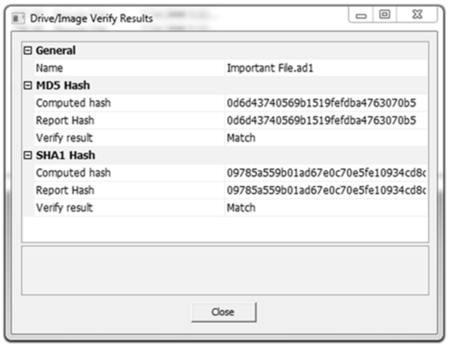
2^{128}

1 in 340 billion billion billion billion

How Verification Works



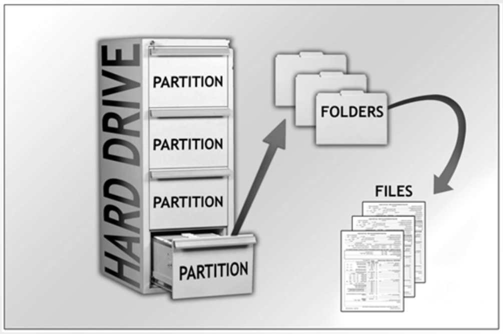
GUARDIAN
DIGITAL FORENSICS



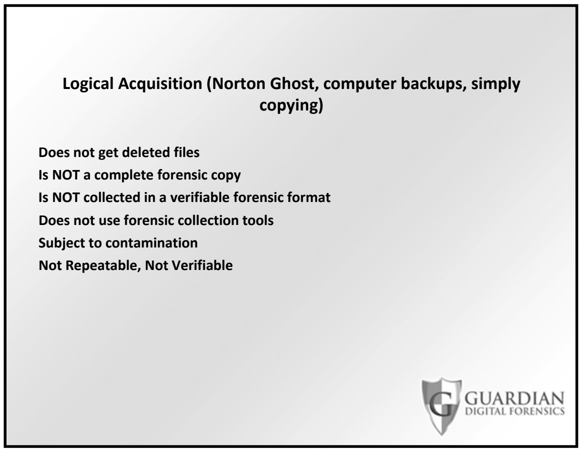
```
⊟ General
   Name                 Important File.ad1
⊟ MD5 Hash
   Computed hash        0d6d43740569b1519fefdba4763070b5
   Report Hash          0d6d43740569b1519fefdba4763070b5
   Verify result        Match
⊟ SHA1 Hash
   Computed hash        09785a559b01ad67e0c70e5fe10934cd8c
   Report Hash          09785a559b01ad67e0c70e5fe10934cd8c
   Verify result        Match
```

GUARDIAN
DIGITAL FORENSICS

Organization of Logical Data on a Hard Drive

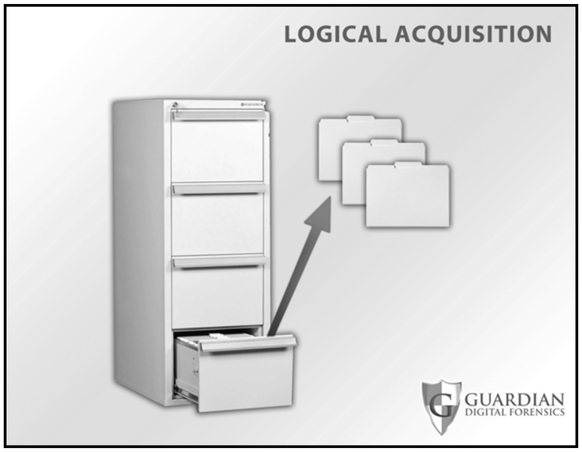


GUARDIAN
DIGITAL FORENSICS

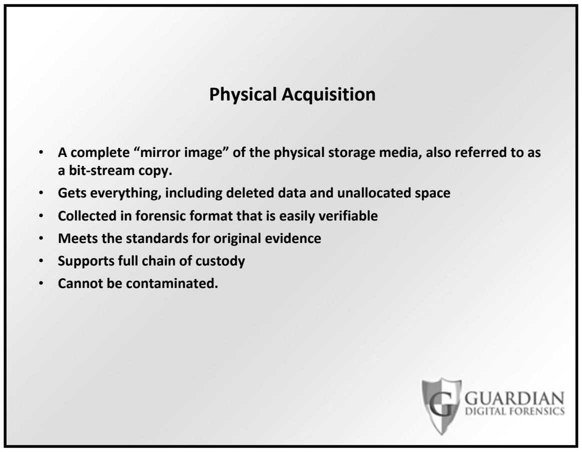


Logical Acquisition (Norton Ghost, computer backups, simply copying)

Does not get deleted files
Is NOT a complete forensic copy
Is NOT collected in a verifiable forensic format
Does not use forensic collection tools
Subject to contamination
Not Repeatable, Not Verifiable

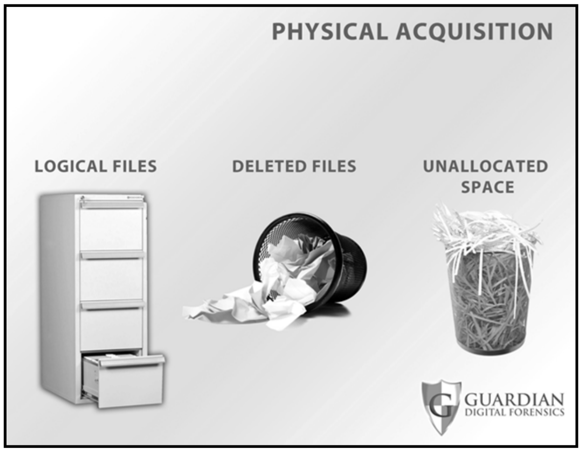


LOGICAL ACQUISITION



Physical Acquisition

- A complete “mirror image” of the physical storage media, also referred to as a bit-stream copy.
- Gets everything, including deleted data and unallocated space
- Collected in forensic format that is easily verifiable
- Meets the standards for original evidence
- Supports full chain of custody
- Cannot be contaminated.

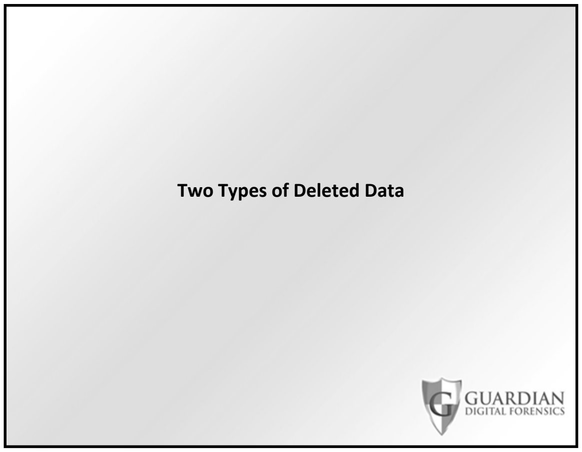


PHYSICAL ACQUISITION

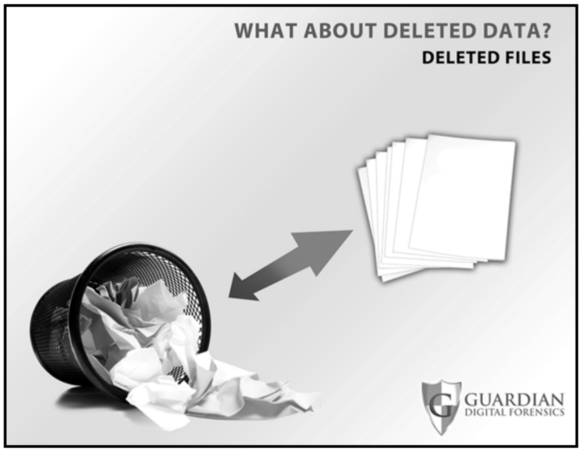
LOGICAL FILES

DELETED FILES

UNALLOCATED SPACE

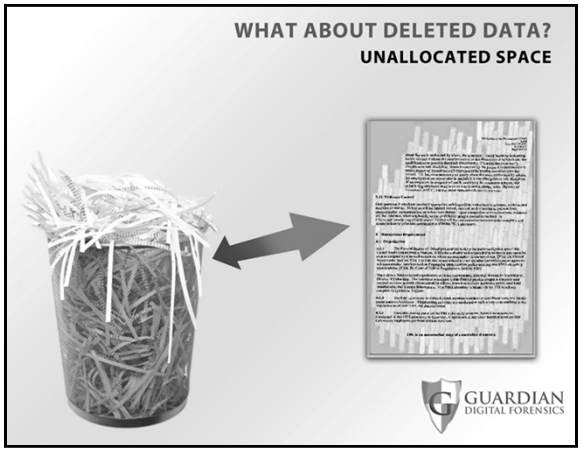


Two Types of Deleted Data



WHAT ABOUT DELETED DATA?

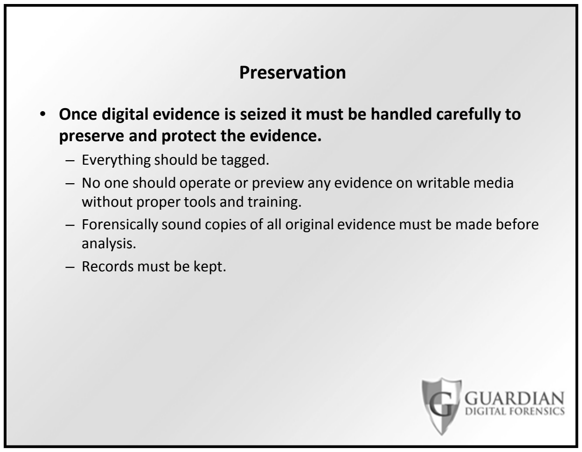
DELETED FILES



WHAT ABOUT DELETED DATA?

UNALLOCATED SPACE

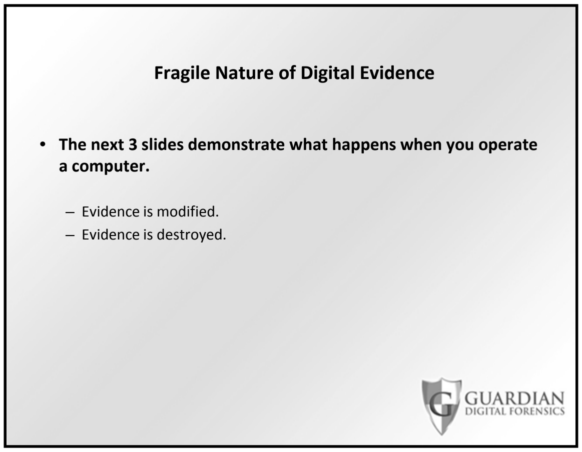
GUARDIAN DIGITAL FORENSICS



Preservation

- **Once digital evidence is seized it must be handled carefully to preserve and protect the evidence.**
  - Everything should be tagged.
  - No one should operate or preview any evidence on writable media without proper tools and training.
  - Forensically sound copies of all original evidence must be made before analysis.
  - Records must be kept.

GUARDIAN DIGITAL FORENSICS

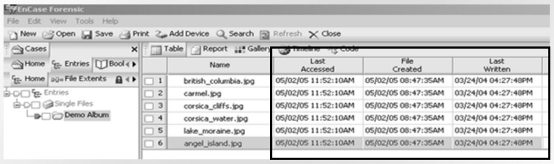


Fragile Nature of Digital Evidence

- **The next 3 slides demonstrate what happens when you operate a computer.**
  - Evidence is modified.
  - Evidence is destroyed.

GUARDIAN DIGITAL FORENSICS

Files In Original Condition

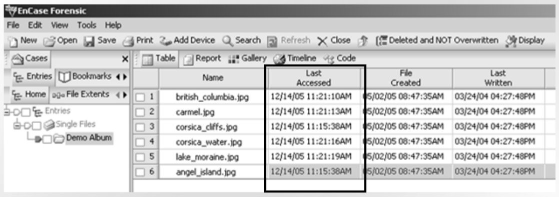

EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search Refresh Close
Cases
Home Entries Bool
Home File Extents
Entries
Single Files
Demo Album
Table Report Gallery Timeline Code

	Name	Last Accessed	File Created	Last Written
□ 1	british_columbia.jpg	05/02/05 11:52:10AM	05/02/05 08:47:35AM	03/24/04 04:27:48PM
□ 2	carmel.jpg	05/02/05 11:52:10AM	05/02/05 08:47:35AM	03/24/04 04:27:48PM
□ 3	corsica_cliffs.jpg	05/02/05 11:52:10AM	05/02/05 08:47:35AM	03/24/04 04:27:48PM
□ 4	corsica_water.jpg	05/02/05 11:52:10AM	05/02/05 08:47:35AM	03/24/04 04:27:48PM
□ 5	lake_moraine.jpg	05/02/05 11:52:10AM	05/02/05 08:47:35AM	03/24/04 04:27:48PM
□ 6	angel_island.jpg	05/02/05 11:52:10AM	05/02/05 08:47:35AM	03/24/04 04:27:48PM

All of the dates and times are the same for the three file time stamps.

GUARDIAN DIGITAL FORENSICS

Files After Opening and Viewing


EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search Refresh Close Deleted and NOT Overwritten Display
Cases
Entries Bookmarks
Home File Extents
Entries
Single Files
Demo Album
Table Report Gallery Timeline Code

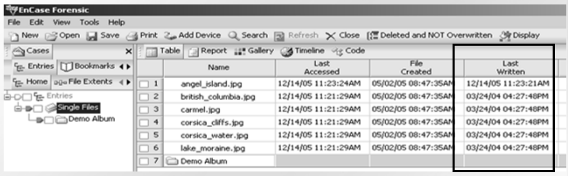
	Name	Last Accessed	File Created	Last Written
□ 1	british_columbia.jpg	12/14/05 11:21:10AM	05/02/05 08:47:35AM	03/24/04 04:27:48PM
□ 2	carmel.jpg	12/14/05 11:21:13AM	05/02/05 08:47:35AM	03/24/04 04:27:48PM
□ 3	corsica_cliffs.jpg	12/14/05 11:15:38AM	05/02/05 08:47:35AM	03/24/04 04:27:48PM
□ 4	corsica_water.jpg	12/14/05 11:21:16AM	05/02/05 08:47:35AM	03/24/04 04:27:48PM
□ 5	lake_moraine.jpg	12/14/05 11:21:19AM	05/02/05 08:47:35AM	03/24/04 04:27:48PM
□ 6	angel_island.jpg	12/14/05 11:15:38AM	05/02/05 08:47:35AM	03/24/04 04:27:48PM

The last accessed date and time changes any time a file is opened and viewed while the computer is in operation.

This is true only for MS Windows prior to Vista and 7. The Last Accessed Time is no longer updated in those versions.

GUARDIAN DIGITAL FORENSICS

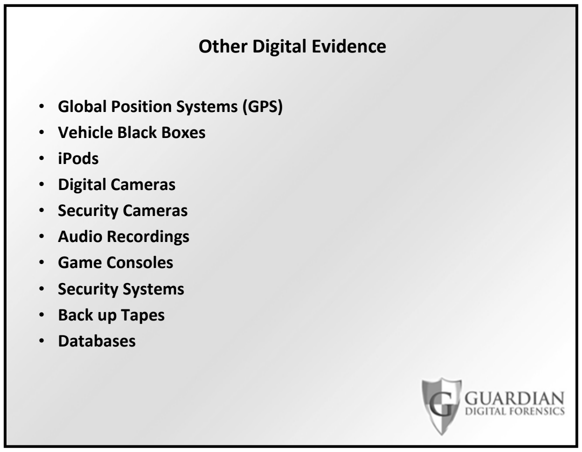
Files After Saving


EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search Refresh Close Deleted and NOT Overwritten Display
Cases
Entries Bookmarks
Home File Extents
Entries
Single Files
Demo Album
Table Report Gallery Timeline Code

	Name	Last Accessed	File Created	Last Written
□ 1	angel_island.jpg	12/14/05 11:23:24AM	05/02/05 08:47:35AM	12/14/05 11:23:21AM
□ 2	british_columbia.jpg	12/14/05 11:21:29AM	05/02/05 08:47:35AM	03/24/04 04:27:48PM
□ 3	carmel.jpg	12/14/05 11:21:29AM	05/02/05 08:47:35AM	03/24/04 04:27:48PM
□ 4	corsica_cliffs.jpg	12/14/05 11:21:29AM	05/02/05 08:47:35AM	03/24/04 04:27:48PM
□ 5	corsica_water.jpg	12/14/05 11:21:29AM	05/02/05 08:47:35AM	03/24/04 04:27:48PM
□ 6	lake_moraine.jpg	12/14/05 11:21:29AM	05/02/05 08:47:35AM	03/24/04 04:27:48PM
□ 7	Demo Album			

The last written date and time changes any time a file is saved or copied while the computer is in operation.

GUARDIAN DIGITAL FORENSICS



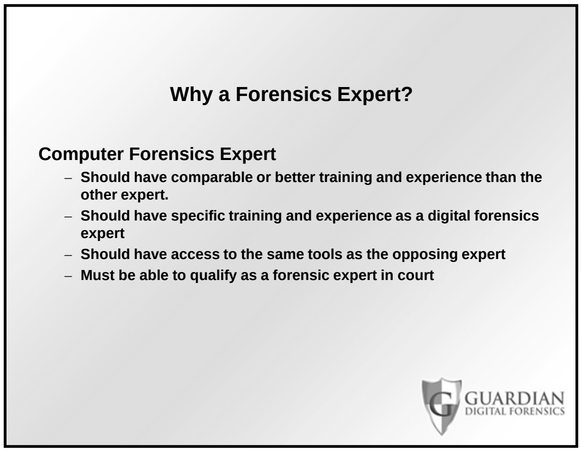
Other Digital Evidence

- Global Position Systems (GPS)
- Vehicle Black Boxes
- iPods
- Digital Cameras
- Security Cameras
- Audio Recordings
- Game Consoles
- Security Systems
- Back up Tapes
- Databases

GUARDIAN
DIGITAL FORENSICS

Experts

GUARDIAN
DIGITAL FORENSICS

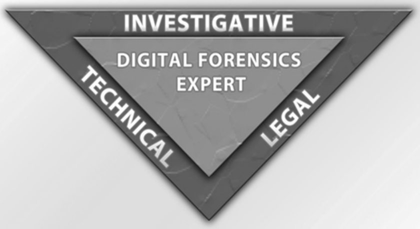


Why a Forensics Expert?

Computer Forensics Expert

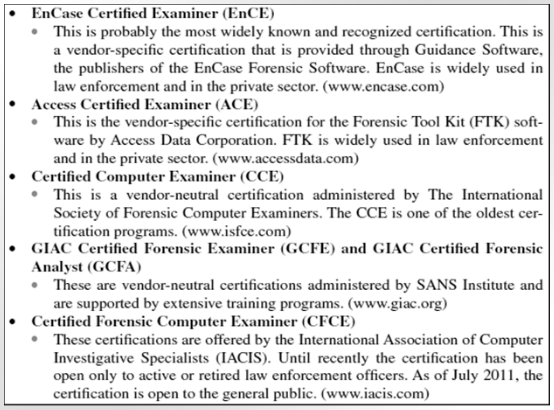
- Should have comparable or better training and experience than the other expert.
- Should have specific training and experience as a digital forensics expert
- Should have access to the same tools as the opposing expert
- Must be able to qualify as a forensic expert in court

GUARDIAN
DIGITAL FORENSICS

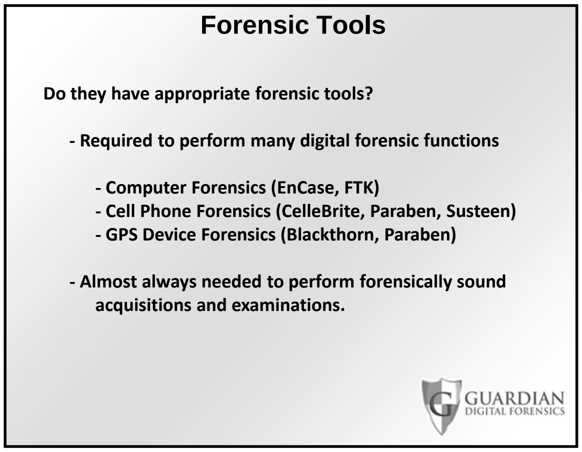


Selecting a Digital Forensics Expert

Certifications



- **EnCase Certified Examiner (EnCE)**
  - This is probably the most widely known and recognized certification. This is a vendor-specific certification that is provided through Guidance Software, the publishers of the EnCase Forensic Software. EnCase is widely used in law enforcement and in the private sector. (www.encase.com)
- **Access Certified Examiner (ACE)**
  - This is the vendor-specific certification for the Forensic Tool Kit (FTK) software by Access Data Corporation. FTK is widely used in law enforcement and in the private sector. (www.accessdata.com)
- **Certified Computer Examiner (CCE)**
  - This is a vendor-neutral certification administered by The International Society of Forensic Computer Examiners. The CCE is one of the oldest certification programs. (www.isfce.com)
- **GIAC Certified Forensic Examiner (GCFE) and GIAC Certified Forensic Analyst (GCFA)**
  - These are vendor-neutral certifications administered by SANS Institute and are supported by extensive training programs. (www.giac.org)
- **Certified Forensic Computer Examiner (CFCE)**
  - These certifications are offered by the International Association of Computer Investigative Specialists (IACIS). Until recently the certification has been open only to active or retired law enforcement officers. As of July 2011, the certification is open to the general public. (www.iacis.com)



Forensic Tools

Do they have appropriate forensic tools?

- Required to perform many digital forensic functions

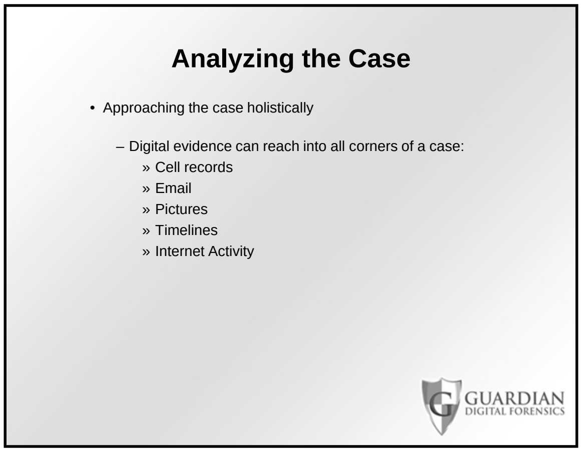
- Computer Forensics (EnCase, FTK)
- Cell Phone Forensics (CelleBrite, Paraben, Susteen)
- GPS Device Forensics (Blackthorn, Paraben)

- Almost always needed to perform forensically sound acquisitions and examinations.

GUARDIAN
DIGITAL FORENSICS

Analysis

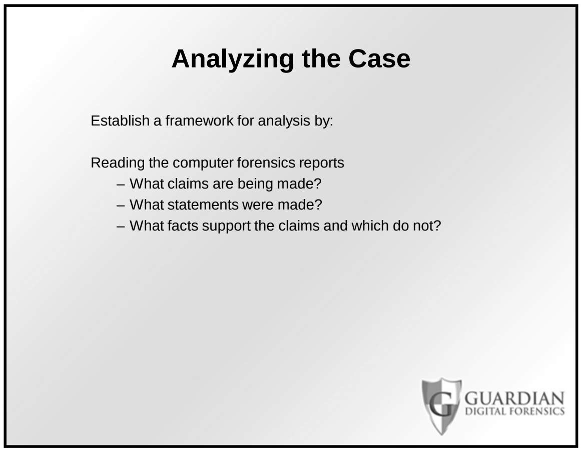
GUARDIAN
DIGITAL FORENSICS



Analyzing the Case

- Approaching the case holistically
  - Digital evidence can reach into all corners of a case:
    - » Cell records
    - » Email
    - » Pictures
    - » Timelines
    - » Internet Activity

GUARDIAN
DIGITAL FORENSICS

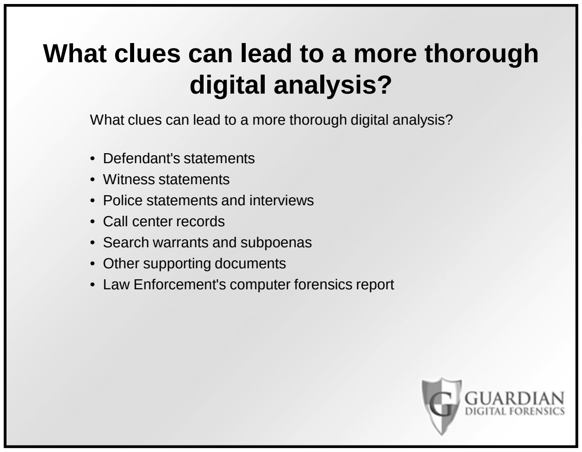


Analyzing the Case

Establish a framework for analysis by:

Reading the computer forensics reports

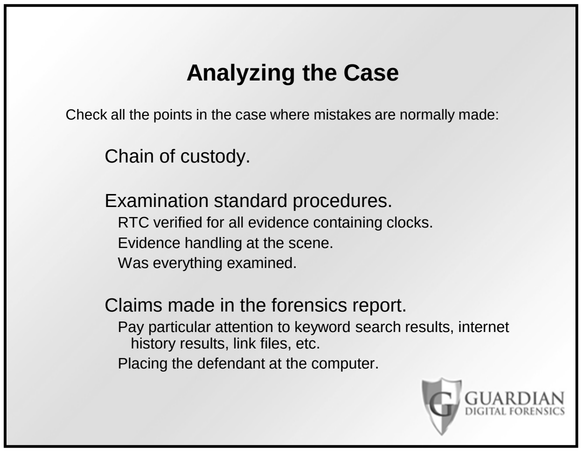
- What claims are being made?
- What statements were made?
- What facts support the claims and which do not?



What clues can lead to a more thorough digital analysis?

What clues can lead to a more thorough digital analysis?

- Defendant's statements
- Witness statements
- Police statements and interviews
- Call center records
- Search warrants and subpoenas
- Other supporting documents
- Law Enforcement's computer forensics report



Analyzing the Case

Check all the points in the case where mistakes are normally made:

Chain of custody.

Examination standard procedures.

RTC verified for all evidence containing clocks.

Evidence handling at the scene.

Was everything examined.

Claims made in the forensics report.

Pay particular attention to keyword search results, internet history results, link files, etc.

Placing the defendant at the computer.

Performing the Analysis

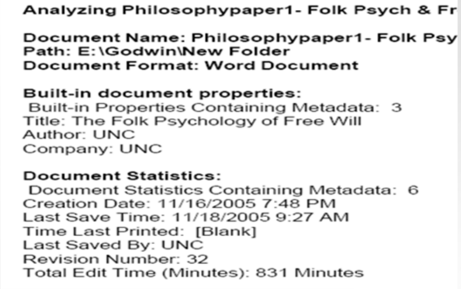
– Duplicate the other side’s work.

- Verify the accuracy of their findings
  - Did they represent their findings correctly?
  - How thorough was the examination?
- Verify the completeness of their report
  - Is everything they found in the report?
    - » Why or why not?
  - Was exculpatory evidence ignored or missed?

Case Analysis

Examples

Document Metadata Example



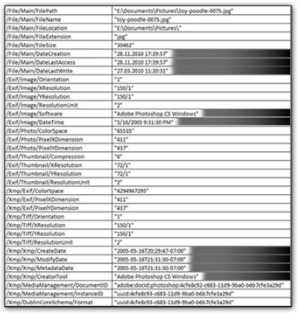
Analyzing Philosophypaper1- Folk Psych & Fr

Document Name: Philosophypaper1- Folk Psy
Path: E:\Godwin\New Folder
Document Format: Word Document

Built-in document properties:
Built-in Properties Containing Metadata: 3
Title: The Folk Psychology of Free Will
Author: UNC
Company: UNC

Document Statistics:
Document Statistics Containing Metadata: 6
Creation Date: 11/16/2005 7:48 PM
Last Save Time: 11/18/2005 9:27 AM
Time Last Printed: [Blank]
Last Saved By: UNC
Revision Number: 32
Total Edit Time (Minutes): 831 Minutes

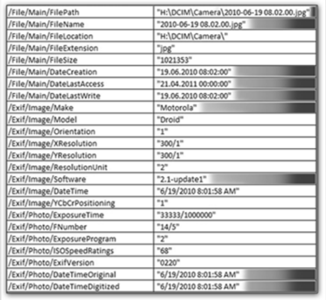
Picture Metadata Example



/File/Main/FilePath	"E:\Documents\Pictures\toy-poodle-0075.jpg"
/File/Main/FileName	"toy-poodle-0075.jpg"
/File/Main/FileLocation	"E:\Documents\Pictures\"
/File/Main/FileExtension	"jpg"
/File/Main/FileSize	"30462"
/File/Main/DateCreation	"28.11.2010 17:39:57"
/File/Main/DateLastAccess	"28.11.2010 17:39:57"
/File/Main/DateLastWrite	"27.03.2010 11:20:31"
/Exif/Image/Orientation	"1"
/Exif/Image/XResolution	"150/1"
/Exif/Image/YResolution	"150/1"
/Exif/Image/ResolutionUnit	"2"
/Exif/Image/Software	"Adobe Photoshop CS Windows"
/Exif/Image/DateTime	"5/16/2005 9:31:30 PM"
/Exif/Photo/ColorSpace	"65535"
/Exif/Photo/PixelXDimension	"411"
/Exif/Photo/PixelYDimension	"437"
/Exif/Thumbnail/Compression	"6"
/Exif/Thumbnail/XResolution	"72/1"
/Exif/Thumbnail/YResolution	"72/1"
/Exif/Thumbnail/ResolutionUnit	"2"
/Xmp/Exif/ColorSpace	"4294967295"
/Xmp/Exif/PixelXDimension	"411"
/Xmp/Exif/PixelYDimension	"437"
/Xmp/Tiff/Orientation	"1"
/Xmp/Tiff/XResolution	"150/1"
/Xmp/Tiff/YResolution	"150/1"
/Xmp/Tiff/ResolutionUnit	"2"
/Xmp/Xmp/CreateDate	"2005-05-16T20:29:47-07:00"
/Xmp/Xmp/ModifyDate	"2005-05-16T21:31:30-07:00"
/Xmp/Xmp/MetadataDate	"2005-05-16T21:31:30-07:00"
/Xmp/Xmp/CreatorTool	"Adobe Photoshop CS Windows"
/Xmp/MediaManagement/DocumentID	"adobe:docid:photoshop:4cfe8c92-c683-11d9-9ba0-b6b7cfe3a29d"
/Xmp/MediaManagement/InstanceID	"uuid:4cfe8c93-c683-11d9-9ba0-b6b7cfe3a29d"
/Xmp/DublinCoreSchema/Format	"uuid:4cfe8c93-c683-11d9-9ba0-b6b7cfe3a29d"

GUARDIAN
DIGITAL FORENSICS

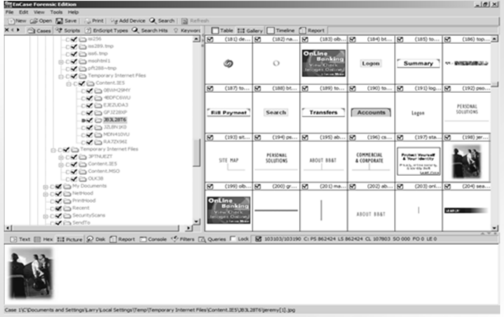
Picture Metadata Example



/File/Main/FilePath	"H:\DCIM\Camera\2010-06-19 08.02.00.jpg"
/File/Main/FileName	"2010-06-19 08.02.00.jpg"
/File/Main/FileLocation	"H:\DCIM\Camera\"
/File/Main/FileExtension	"jpg"
/File/Main/FileSize	"1021353"
/File/Main/DateCreation	"19.06.2010 08:02:00"
/File/Main/DateLastAccess	"21.04.2011 00:00:00"
/File/Main/DateLastWrite	"19.06.2010 08:02:00"
/Exif/Image/Make	"Motorola"
/Exif/Image/Model	"Droid"
/Exif/Image/Orientation	"1"
/Exif/Image/XResolution	"300/1"
/Exif/Image/YResolution	"300/1"
/Exif/Image/ResolutionUnit	"2"
/Exif/Image/Software	"2.1-update1"
/Exif/Image/DateTime	"6/19/2010 8:01:58 AM"
/Exif/Image/YCbCrPositioning	"1"
/Exif/Photo/ExposureTime	"33333/1000000"
/Exif/Photo/FNumber	"14/5"
/Exif/Photo/ExposureProgram	"2"
/Exif/Photo/ISOSpeedRatings	"68"
/Exif/Photo/ExifVersion	"0220"
/Exif/Photo/DateTimeOriginal	"6/19/2010 8:01:58 AM"
/Exif/Photo/DateTimeDigitized	"6/19/2010 8:01:58 AM"

GUARDIAN
DIGITAL FORENSICS

Internet History – Before Clearing

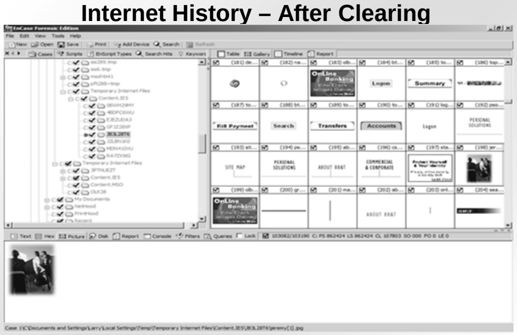


103103/103190 C: PS 862424 LS 862424 CL 107803 SO 000 FO 0 LE 0

Case 1\C\Documents and Settings\Larry\Local Settings\Temp\Temporary Internet Files\Content.IE5\JB3L28T6\jeremy[1].jpg

GUARDIAN
DIGITAL FORENSICS

Internet History – After Clearing


EnCase Forensic Edition
File Edit View Tools Help
New Open Save Print Add Device Search Refresh
Cases Scripts EnScript Types Search Hits Keyword
Table Gallery Timeline Report
Temporary Internet Files
Content.IE5
JB3L28T6
My Documents
NetHood
PrintHood
Recent
OnLine Banking
Logon
Summary
Bill Payment
Search
Transfers
Accounts
PERSONAL SOLUTIONS
SITE MAP
ABOUT BB&T
COMMERCIAL & CORPORATE
Protect Yourself & Your Identity
Text Hex Picture Disk Report Console Filters Queries Lock

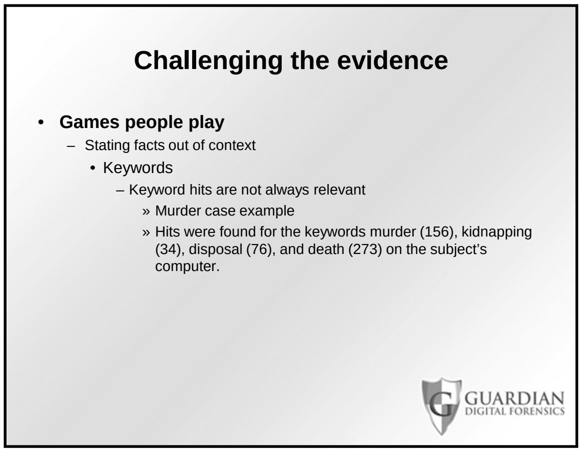
Case 1\C\Documents and Settings\Larry\Local Settings\Temp\Temporary Internet Files\Content.IE5\JB3L28T6\jeremy[1].jpg

Challenging the evidence

- **Common mistakes that open digital evidence to challenges**
  - Failing to verify clock times
    - Computer Clocks (Real Time Clock Setting)
      - Affects everything related to time lines:
        - Internet history
        - Emails
        - Computer activity
    - Digital Cameras
      - Affects the metadata inside the digital images.

Challenging the evidence

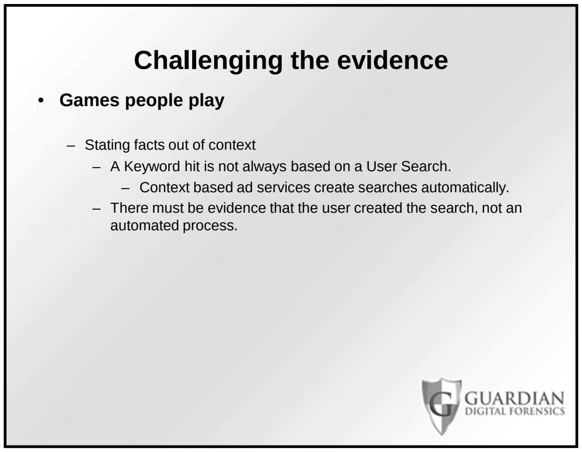
- **Is there an attempt to place a person at a computer without adequate proof?**
    - How can you tell?
      - Did the analyst check for unique user accounts with passwords?
      - Is there evidence anyone else used the computer under that person's account or profile?
      - Was the computer in a common area?
      - Did others know the passwords to the user's account?
      - Was access to the computer restricted by physical boundaries or location?



Challenging the evidence

- **Games people play**
  - – Stating facts out of context
    - Keywords
      - – Keyword hits are not always relevant
        - » Murder case example
        - » Hits were found for the keywords murder (156), kidnapping (34), disposal (76), and death (273) on the subject’s computer.

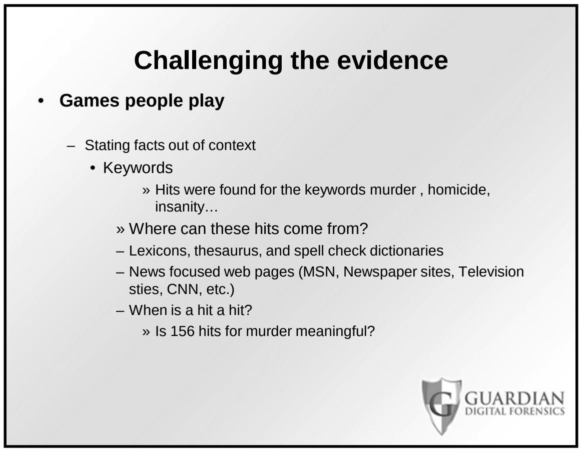
GUARDIAN DIGITAL FORENSICS



Challenging the evidence

- **Games people play**
  - – Stating facts out of context
    - – A Keyword hit is not always based on a User Search.
      - – Context based ad services create searches automatically.
    - – There must be evidence that the user created the search, not an automated process.

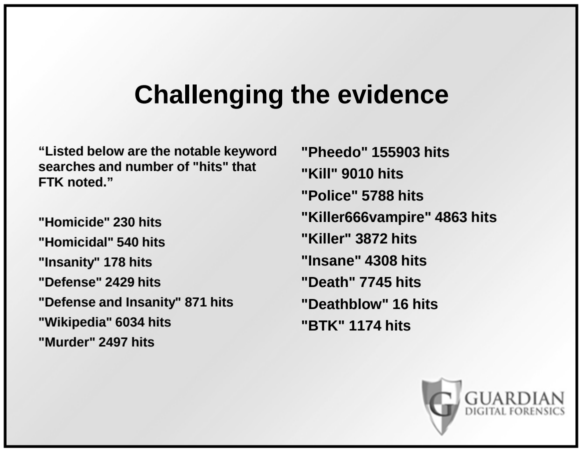
GUARDIAN DIGITAL FORENSICS



Challenging the evidence

- **Games people play**
  - – Stating facts out of context
    - Keywords
      - » Hits were found for the keywords murder , homicide, insanity…
      - » Where can these hits come from?
      - – Lexicons, thesaurus, and spell check dictionaries
      - – News focused web pages (MSN, Newspaper sites, Television sties, CNN, etc.)
      - – When is a hit a hit?
        - » Is 156 hits for murder meaningful?

GUARDIAN DIGITAL FORENSICS

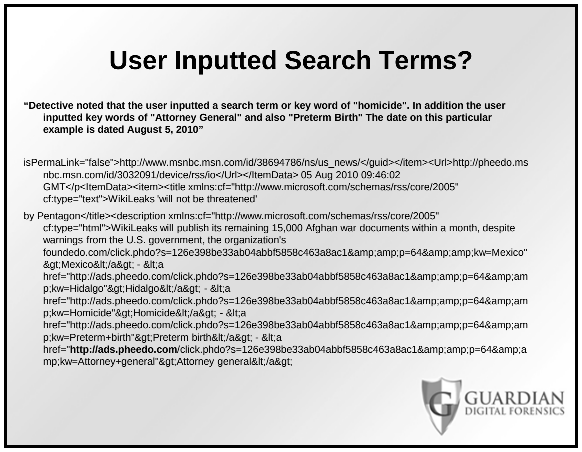


Challenging the evidence

“Listed below are the notable keyword searches and number of "hits" that FTK noted.”

"Homicide" 230 hits
"Homicidal" 540 hits
"Insanity" 178 hits
"Defense" 2429 hits
"Defense and Insanity" 871 hits
"Wikipedia" 6034 hits
"Murder" 2497 hits

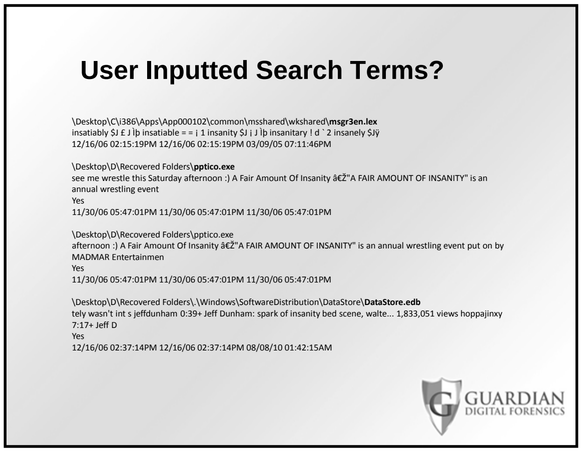
"Pheedo" 155903 hits
"Kill" 9010 hits
"Police" 5788 hits
"Killer666vampire" 4863 hits
"Killer" 3872 hits
"Insane" 4308 hits
"Death" 7745 hits
"Deathblow" 16 hits
"BTK" 1174 hits



User Inputted Search Terms?

“Detective noted that the user inputted a search term or key word of "homicide". In addition the user inputted key words of "Attorney General" and also "Preterm Birth" The date on this particular example is dated August 5, 2010”

```
isPermaLink="false">http://www.msnbc.msn.com/id/38694786/ns/us_news/</guid></item><Url>http://pheedo.ms
      nbc.msn.com/id/3032091/device/rss/io</Url></ItemData> 05 Aug 2010 09:46:02
      GMT</p<ItemData><item><title xmlns:cf="http://www.microsoft.com/schemas/rss/core/2005"
      cf:type="text">WikiLeaks 'will not be threatened'
by Pentagon</title><description xmlns:cf="http://www.microsoft.com/schemas/rss/core/2005"
      cf:type="html">WikiLeaks will publish its remaining 15,000 Afghan war documents within a month, despite
      warnings from the U.S. government, the organization's
      foundedo.com/click.phdo?s=126e398be33ab04abbf5858c463a8ac1&amp;amp;p=64&amp;amp;kw=Mexico"
      &gt;Mexico&lt;/a&gt; - &lt;a
      href="http://ads.pheedo.com/click.phdo?s=126e398be33ab04abbf5858c463a8ac1&amp;amp;p=64&amp;am
      p;kw=Hidalgo"&gt;Hidalgo&lt;/a&gt; - &lt;a
      href="http://ads.pheedo.com/click.phdo?s=126e398be33ab04abbf5858c463a8ac1&amp;amp;p=64&amp;am
      p;kw=Homicide"&gt;Homicide&lt;/a&gt; - &lt;a
      href="http://ads.pheedo.com/click.phdo?s=126e398be33ab04abbf5858c463a8ac1&amp;amp;p=64&amp;am
      p;kw=Preterm+birth"&gt;Preterm birth&lt;/a&gt; - &lt;a
      href="http://ads.pheedo.com/click.phdo?s=126e398be33ab04abbf5858c463a8ac1&amp;amp;p=64&amp;a
      mp;kw=Attorney+general"&gt;Attorney general&lt;/a&gt;
```



User Inputted Search Terms?

```
\Desktop\C\i386\Apps\App000102\common\msshared\wkshared\msgr3en.lex
insatiably $J £ J Ìþ insatiable = = ¡ 1 insanity $J ¡ J Ìþ insanitary ! d ` 2 insanely $Jÿ
12/16/06 02:15:19PM 12/16/06 02:15:19PM 03/09/05 07:11:46PM

\Desktop\D\Recovered Folders\pptico.exe
see me wrestle this Saturday afternoon :) A Fair Amount Of Insanity â€Ž"A FAIR AMOUNT OF INSANITY" is an
annual wrestling event
Yes
11/30/06 05:47:01PM 11/30/06 05:47:01PM 11/30/06 05:47:01PM

\Desktop\D\Recovered Folders\pptico.exe
afternoon :) A Fair Amount Of Insanity â€Ž"A FAIR AMOUNT OF INSANITY" is an annual wrestling event put on by
MADMAR Entertainmen
Yes
11/30/06 05:47:01PM 11/30/06 05:47:01PM 11/30/06 05:47:01PM

\Desktop\D\Recovered Folders\.\Windows\SoftwareDistribution\DataStore\DataStore.edb
tely wasn't int s jeffdunham 0:39+ Jeff Dunham: spark of insanity bed scene, walte... 1,833,051 views hoppajinxy
7:17+ Jeff D
Yes
12/16/06 02:37:14PM 12/16/06 02:37:14PM 08/08/10 01:42:15AM
```

Challenging the evidence

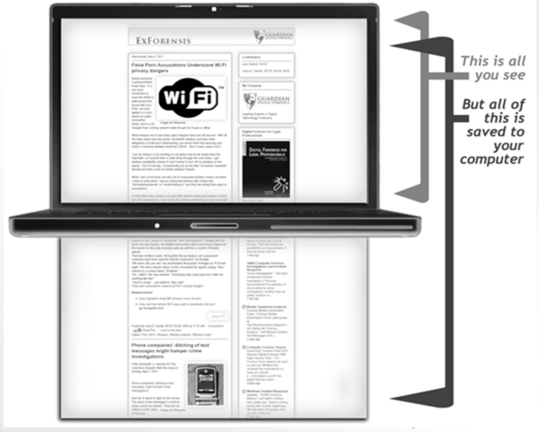
- **Games people play**
  - Playing the techie game
    - Technical words no one understands
      - Unallocated space
      - Slack space
      - Browser cache
      - Typed URLs
      - Gnutella and Limewire
    - What does that mean?

GUARDIAN DIGITAL FORENSICS

Challenging the evidence

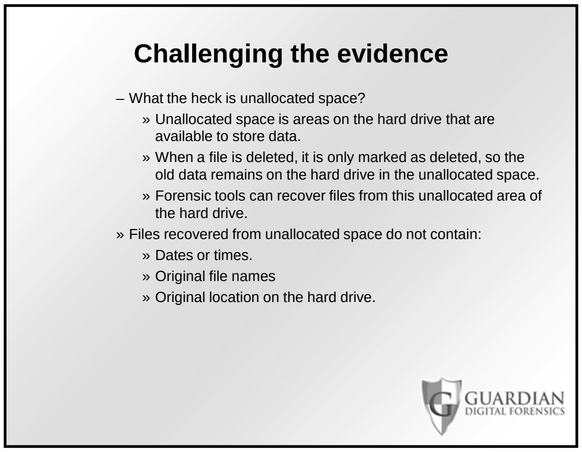
- What does that mean?
  - If it is in the browser cache, does that mean the user did it on purpose?
    - » How browser caching works.
  - » Federal courts have ruled that files recoevred:
    - » in the internet cache do not constitute possession unless the prosecution can prove the user knew about the files in the cache.
    - » In unallocated space do not constitute possession.
  - » Same ruling in Georgia in 2007.

GUARDIAN DIGITAL FORENSICS


ExForensis
GUARDIAN DIGITAL FORENSICS
False Porn Accusations Underscore Wi-Fi privacy dangers
Wi Fi
Digital Forensics for Legal Professionals
Phone companies' ditching of text messages might hamper crime investigations

This is all you see

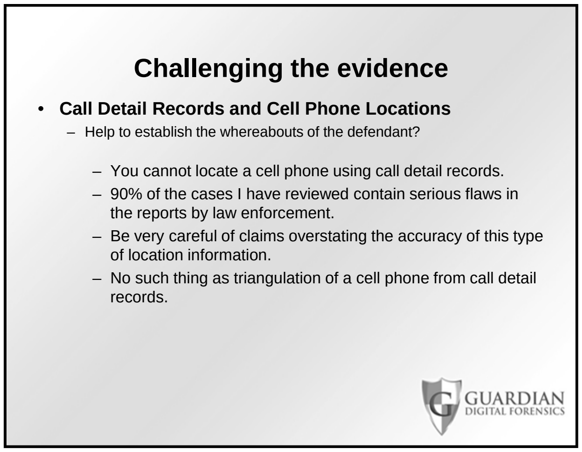
But all of this is saved to your computer



Challenging the evidence

- What the heck is unallocated space?
  - » Unallocated space is areas on the hard drive that are available to store data.
  - » When a file is deleted, it is only marked as deleted, so the old data remains on the hard drive in the unallocated space.
  - » Forensic tools can recover files from this unallocated area of the hard drive.
- » Files recovered from unallocated space do not contain:
  - » Dates or times.
  - » Original file names
  - » Original location on the hard drive.

GUARDIAN
DIGITAL FORENSICS



Challenging the evidence

- **Call Detail Records and Cell Phone Locations**
  - Help to establish the whereabouts of the defendant?
    - You cannot locate a cell phone using call detail records.
    - 90% of the cases I have reviewed contain serious flaws in the reports by law enforcement.
    - Be very careful of claims overstating the accuracy of this type of location information.
    - No such thing as triangulation of a cell phone from call detail records.