

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



Digital Forensics for Attorneys - Part 1

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 witnesses 14 times.
 - Cell Phone Forensics
 - Computer Forensics
 - Cellular Technology Forensics (Cell Towers)
- Worked on over 600 cases



Digital Forensics For Attorneys

Part 1

- Overview of Digital Forensics
 - Types of Digital Evidence
 - Acquisition (Collection) and Preservation

Part 2

- Experts, Evidence and Analysis
 - Understand Forensic Experts vs. Computer Experts
 - Digital evidence: discovery and usage
 - Overview of Digital Forensics – Analysis
 - Challenging Digital Evidence



In The Beginning...











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



Some Basics



Common Mistakes



Calling these monitors, CPUs, Hard Drives, etc.



CPU



- CPU – Central Processing Unit
 - Only performs calculations.
 - Stores nothing.
 - The “brain” of the computer.



Inside The Computer

- **RAM – Random Access Memory**
 - Only contains data while the computer is turned on.
 - Temporary processing storage only used while operating the computer.
 - Is cleared when the computer shuts down or re-starts.



Inside The Computer



- The Hard Drive stores the evidence...



Inside The Computer

- **Hard drives today can store several hundred thousand**
 - Documents
 - Pictures
 - Music files
 - Movies
 - Passwords
 - Emails
 - Web Pages



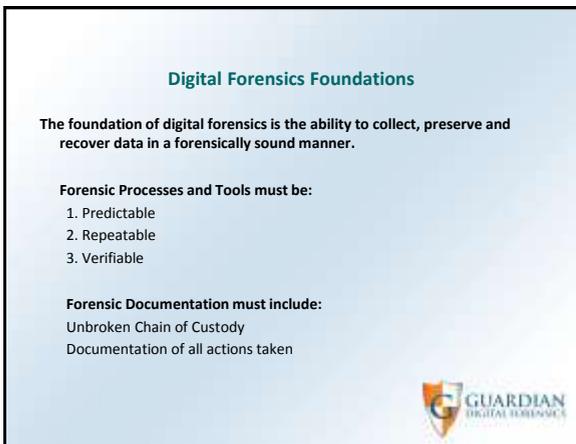












Digital Forensics – The Sub-Disciplines

- **Computer Forensics**
 - **Computers and Data Storage Devices**
 - Typical Case Types: All
- **Social Media Forensics**
 - Facebook, Twitter, Chat, MySpace, Internet Presence on Blogs, Message Boards
 - Typical Case Types: Infidelity, Libel and Slander, Employee Wrongdoing
- **Email Forensics**
 - Back tracking emails
 - Email recovery
 - Typical Case Types: Murder, Rape, Infidelity, Sexual Harassment, Child Pornography



Digital Forensics – The Sub-Disciplines

- **Peer to Peer Forensics**
 - File sharing via Limewire, BitTorrent, others
 - Typical Case Types: Child Pornography, Copyright Violations, Data Theft
- **Cell Phone Forensics**
 - Call logs, contacts, text messages, pictures, movies, geo-location
 - Typical Case Types: Murder, Sexting, Infidelity, Rape, Kidnapping, Drugs
- **Cellular Evidence Forensics**
 - Cell phone record analysis, Cell phone ping analysis, Cell tower mapping
 - Typical Case Types: Murder, Kidnapping, Drugs



Digital Forensics – The Sub Disciplines

- **Digital Video and Image Forensics**
 - Security Video, Camera Video, Pictures
 - Typical Case Types: Murder, Theft, Employee Misconduct, Wrongful Death
- **Audio Forensics**
 - Police Interviews, Police Radio Recordings, Wiretaps
 - Typical Case Types: Murder, Conspiracy, Wrongful Death
- **GPS (Global Positioning Systems)**
 - Data from GPS units, Logs from GPS tracking, House Arrest
 - Typical Case Types: Murder, Parole Violations, Kidnapping



Acquiring (Collecting) and Handling Digital Evidence

Digital forensics requires forensically sound acquisitions.

Defensible Practices

- Proper Chain of Custody
- Verification of evidence
- Proper documentation



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.

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



Acquisition (Collection)

- First responders should be trained to handle this type of evidence.
- Digital evidence is fragile.
- Digital evidence is easily altered if not handled properly.
- Simply turning a computer on or operating the computer changes and damages evidence.



What Is Forensically Sound?



This is Not Forensically Sound



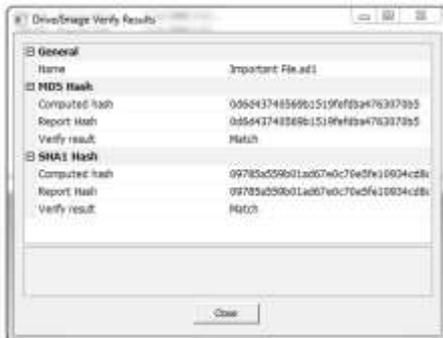
FORENSIC WRITE-BLOCKERS



This is Forensically Sound





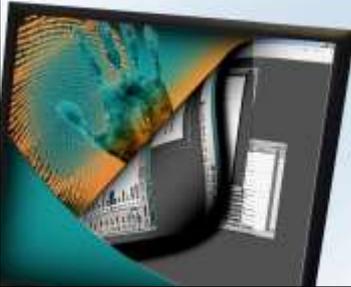


Verification Must Be Done

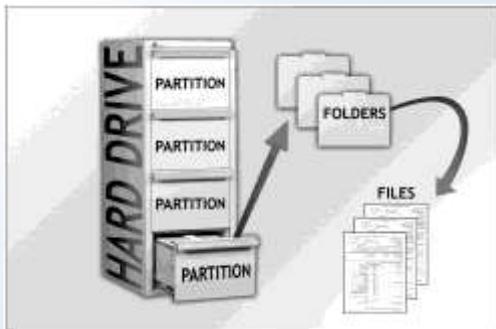
MDS HASH
9e107d9d372bb6826bd81d3542a419d6

2¹²⁸

1 in 340 billion billion billion billion



Organization of Logical Data on a Hard Drive



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





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.





Two Types of Deleted Data



WHAT ABOUT DELETED DATA?
DELETED FILES



WHAT ABOUT DELETED DATA?
UNALLOCATED SPACE



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.



Fragile Nature of Digital Evidence

- **The simple act of turning a computer on can destroy or change critical evidence and render that evidence useless.**
 - *Maryland State Police - Criminal Enforcement Command - Computer Crimes Unit*
- **Even the normal operation of the computer can destroy computer evidence that might be lurking in unallocated space, file slack, or in the Windows swap file.**
 - *Computer Forensics, Computer Crime Scene Investigation, 2 Ed. John R. Vacca*



Fragile Nature of Digital Evidence

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

Source: Preservation of Fragile - Digital Evidence by First Responders - Special Agent Jesse Kuehlman - Air Force Office of Special Investigations



Other Digital Evidence

- Global Position Systems (GPS) Units (location data)
- Vehicle Black Boxes (trucking industry)
- iPods – (employee theft)
- Digital Cameras – (sex crimes)
- Security Cameras – (robberies, wrongful death)
- Audio Recordings (wrongful death, terrorism, murder, defendant interviews)
- Game Consoles (murder)
- Security Systems (murder)
- Back up Tapes (data recovery, fraud)



Questions?

Contact Information:

Email: larry@guardiandf.com
Web: www.guardiandf.com
Blog: www.exforensics.com
Phone: 919-868-6281

Book: Digital Forensics for Legal Professionals
Syngress Publishing
Amazon.com (Print and Kindle)
Larry E. Daniel and Lars E. Daniel