

FIRST

RESPONSE

consulting services, inc.



Digital Evidence & Computer Forensics

David Nardoni CISSP, EnCE

President

First Response Consulting Service, Inc.

dnardoni@firstresponseconsulting.com

626.795.6510



Overview

- What is digital evidence and computer forensics?
- How to succeed at retrieving digital evidence and the importance of proper evidence handling
- Forensic procedures and tools
- Importance of proper planning in order to be able to respond effectively to computer incidents
- Encase Demo



Legal Disclaimer

- This Presentation shall not be considered legal advice and is only provided as a resource and starting reference point for further legal research
- All cited authorities should be verified and updated.



Electronic or Digital Evidence

Definitions

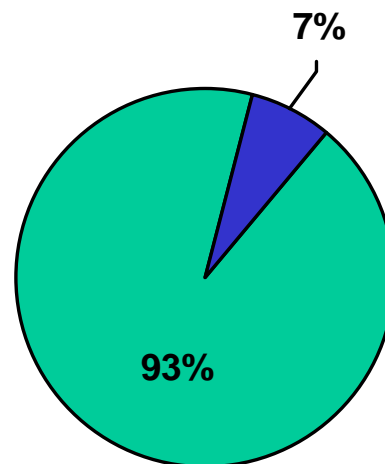
Electronic record : any data that is recorded or preserved on any medium in or by a computer system or other similar device, that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout or other output of that data.

Computer Forensics : Computer forensics is the scientific examination and analysis of data held on, or retrieved from, computer storage media in such a way that the information can be used as evidence in a court of law.



Digital evidence is everywhere

Digital vs. Non-Digital



■ Digital ■ Non-digital

According to a study by University of California-Berkeley in 2001 found that 93% of all new information at that time was created entirely in digital format.



What types of media hold digital evidence

- Hard disks, CD's, DVD's, floppies
- PDA's, compact flash, zip disks, jazz disks
- Backup tapes, copiers, printers, scanners, cell phones





Forensic Methodology

The three A's

Acquire

Do not alter or damage the original.

Authenticate

Proof that your recovered evidence is the same as the original.

Analyze

Inspect evidence without altering it.



Types of Crimes that can involve Computer Forensics

- Child Porn
- Breach of Computer Security
- Fraud/Theft
- Copyright Violations
- Identity Theft
- Narcotics Investigations
- Threats
- Burglary
- Suicide
- Obscenity
- Homicide
- Administrative Investigations
- Sexual Assault
- Stalking



How to succeed at retrieving digital evidence

Assessing the Case

- Do you have proper consent to acquire and search for the evidence?
Consult your legal council, proper security policies, search warrants
- Consider scope of examination
Email servers, ISP logs, remote storage, PDA's, cell phones, other peripherals
- Determine what type of evidence is being sought
Text documents, spreadsheets, email, photographs, financial records
- Prioritize order in which evidence is to be examined
- Determine amount of personnel needed and hours to perform (Covert operation)



How to succeed at retrieving digital evidence

Assessing the Case continued

- Good communication – clearly define what you need, otherwise you are fishing
- How much time is needed to search for the data and is it indexed
- Allocate enough time to gather the data – consider IT people's time, try and remember they do have jobs besides helping us.
- Estimate amount of data to be retrieved & where it is located
- Creating a proper environment to review the data
- Getting comfortable with technology – If you don't know what you are doing do not touch anything and find an expert.



First steps to preserve the evidence

Technical Steps – Top 5 mistakes

- Don't run programs on the computer
- Don't shutdown the computer if it is turned on, don't turn it on if off
 - Start-up and shut down deletes hundreds of files. (Excel example)
- Don't get help from the computer owner/suspect
- Don't run your anti-virus programs.
 - Anti-virus programs change date/time stamps of every file they scan.
- Don't view files on the system or browse the folders.
 - Any time you browse a folder in windows explorer you change the date/time stamps of every file within the folder.



Steps to preserve the evidence

So what do we do?

- Physically secure the system(s) in question
- Take pictures of the room and area surrounding the system(s)
- Take pictures of system(s) and document all details of system(s)
- Pull the plug from the system (Win95, Win98, WinMe, Win2K, WinXP)
- Disassemble the system and document inside components, disconnect power supply from HD
- Retrieve configuration from CMOS (boot sequence, CMOS date/time)
- Write protect suspect system(s) and make bit stream image on to sterile media



Where do we look for the smoking gun?

- Address Books
- Audio/Video files
- Backup files
- Calendars
- Compressed Files
- Configuration files
- Cookies
- Database files
- Documents
- Email files
- Encrypted files
- Hidden files
- History files
- Image/graphics files
- Internet bookmarks/favorites
- Log files
- Metadata
- Misnamed files
- Password-Protected files
- Printer spool files
- Steganography
- Swap files
- System files
- Temporary files



Why can't we just copy the files?

Bit Stream Image

Gets everything from byte 1 - n



File Copy

Missing slack space, deleted files, file remnants





Proper tools preserve evidence

NIST requires that disk imaging tools meet certain standards

- The tool shall make a bit-stream duplicate or an image of an original disk or partition.
- The tool shall not alter the original disk.
- The tool shall be able to verify the integrity of a disk image file.
- The tool shall log I/O errors.
- The tool's documentation shall be correct.



Need for proper policies & procedures

Develop proper security policy addressing incident response and evidence handling

- Limit your company or your clients liability by implementing proper information security policies

- Create procedures that adhere to security policies and follow standard (NIST 800-61, ISO 17799)
- Today we must plan for the possibility of legal action any time we encounter a computer incident.



Forensic Tools

- dd <http://www.gnu.org>
- Encase <http://www.encase.com>
- FTK <http://www.accessdata.com>
- Paraben <http://www.paraben-forensics.com/>
- NTI <http://www.forensics-intl.com>



How not being prepared can cause things to go wrong

Case Study

Law firm 50 Attorneys with Outsourced IT dept

Poor security practices and lack of incident response procedures

Vendor fired rogue IT employee without taking proper security precautions

Two major servers failed to reboot after installing security patch

Discovered trojans on both compromised systems

After trying to re-install OS twice Vendor noticed firewall admin access was denied

No incident response policy or plan – Vendor did not give client option of preserving the evidence

Backup tapes were not working properly due to lack of testing

No security logging on host systems, no logs on firewall

No regular review of firewall logs before during or after incident

Total estimated cost to Firm : \$28,000 (IT Costs) + \$47,000 (Lost productivity) = **\$75,000**