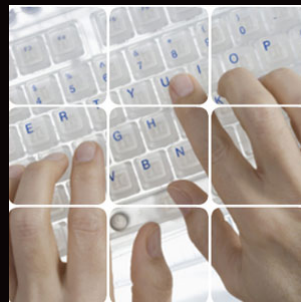


Computer Forensics



April 10, 2009
Presentation for Dr. Maria Schiza's Forensics class



Reference: Computer Forensics: Principles and Practice
Valerina Anzaldúa Cedeno



Dr. Nazli Hardy, 2009

Introduction

- Managing a case
 - authenticating evidence
 - searching and analyzing data

Computer forensics tools and toolkits



Reference: Computer Forensics: Principles and Practice
Valerina Anzaldúa Cedeno



Dr. Nazli Hardy, 2009

Managing the Life-Cycle of a Case

- No Shortcuts

- I. Evidence must be *'defensible'* (objective, unbiased):

- a. Performed in accordance with forensic science principles
 - b. Conducted with verified tools to identify, collect, filter, tag and bag, store, and preserve e-evidence
 - c. Conducted by individuals who are certified or credible
 - d. Documented thoroughly
 - e. Follow process - as opposed to "I feel" or "I think" or "I believe"

- Why?



Managing the Life-Cycle of a Case

- II. Preserving the chain of custody for e-evidence requires proving that:

- a. No information has been added, deleted, or altered in the copying process or during analysis
 - b. A complete copy was made and verified (usually work from copy)
 - c. A reliable copying process was used
 - d. All media were secured

- What would forensics specialists do first thing?



In Practice: Easy Access to Criminal Tools

- Many tools are freely available that help criminals hide evidence of cybercrimes
 - a. Nuker
 - b. Anonymous remailers
 - c. Password cracker
 - d. Scanner
 - e. Spoofer
 - f. Steganography
 - g. Trojan horse



Reference: Computer Forensics: Principles and Practice
Valerina Anzaldúa Cedeno



Dr. Nazli Hardy, 2009

Investigation Objectives and Chain of Custody Practices

Investigation Objectives	Chain of Custody Practices
Document the scene, evidence, activities, and findings	Document everything that is done; keep detailed records and photographs, etc.
Acquire the evidence	Collect and preserve the original data, and create an exact copy
Authenticate the copy	Verify that the copy is identical to the original
Analyze and filter the evidence	Perform the technical analysis while retaining its integrity
Be objective and unbiased	Ensure that the evaluation is fair and impartial to the person or people being investigated
Present the evidence/evaluation in a legally acceptable manner	Interpret and report the results correctly

Reference: Computer Forensics: Principles and Practice
Valerina Anzaldúa Cedeno



Dr. Nazli Hardy, 2009

In Practice: Write Blocking and Protection

- Never turn on a PC without having *write-blocking* software or devices in place
- Write-blocking devices prevent any writes to a drive such as may occur when simply turning on a system
 - e.g. NoWrite Hardware Write Blocker



Create a Drive Image

- Original data must be protected from any type of alteration
- To protect original data, work from a *forensic copy* of the original drive or device
- How many copies?
- What are possible complication in making copies



Residual Data

- Residual data is data that has been deleted but not erased
- Residual data may be found in unallocated storage or file slack space
- File slack



Effective Data Searches

Forensic specialists:

- Identify search terms for data filtering to help locate relevant data and filter out what is irrelevant
- Look at metadata - can be invaluable to the filtering process
- Find out usernames and passwords for network and e-mail accounts
- Check for other computers or devices that might contain relevant evidence



Identify Data Types

- Active data
- Deleted files
- Hidden, encrypted, and password-protected files
- Automatically stored data
- E-mail and instant messages
 - *Smoot vs. Comcast Cablevision* case regarding just cause of an employee based on instant message transcripts
- Background information



Reference: Computer Forensics: Principles and Practice
Valerina Anzaldúa Cedeno

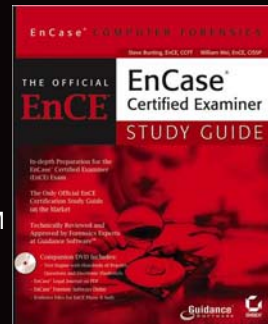


Dr. Nazli Hardy, 2009

Forensic Tools and Toolkits

- EnCase® Forensic
 - A DOD-approved tool for gathering and evaluating electronic information
 - Supports the following e-mail investigation file types:
 - MSN Hotmail
 - Outlook and Outlook Express
 - Yahoo!
 - AOL 6, 7, 8, and 9
 - Netscape
 - mBox (Unix)

Encase Demo on YouTube:
<http://www.youtube.com/watch?v=O4ce74q2zqM>



Reference: Computer Forensics: Principles and Practice
Valerina Anzaldúa Cedeno



Forensic Tools and Toolkits (Windows)

- Forensic Toolkit® (FTK™)—used for finding and examining computer evidence
- Ultimate Toolkit™—contains FTK plus other modules for recovering passwords, analyzing registry data, and wiping hard drives
- WinHex—used for forensics, data recovery and processing, and IT security

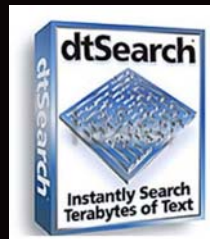


Forensic Tools and Toolkits (UNIX and Linux)

- Autopsy and Sleuth Kit (TSK) —for investigating file systems and volumes of suspect computers



- dtSearch—for combing through large amounts of data for up to 250 different file types



Forensic Tools and Toolkits (Macintosh)

- MacQuisition—forensic acquisition tool used to safely image Macintosh systems
- BlackBag—a set of 19 tools for examining Macintosh computers, including
 - Directory Scan
 - FileSpy
 - HeaderBuilder

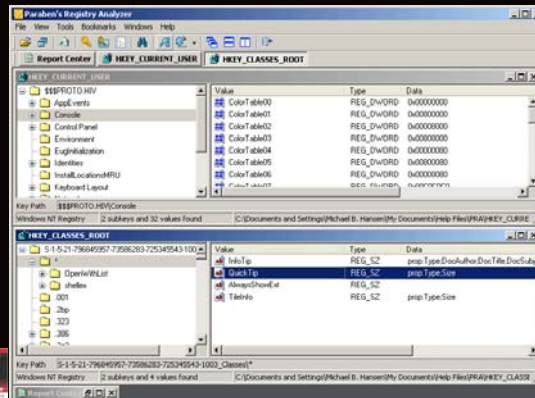


Reference: Computer Forensics: Principles and Practice
Valerina Appaldin, Cedric

Dr. Nazli Hardy, 2009

Forensic Tools and Toolkits (PDA's)

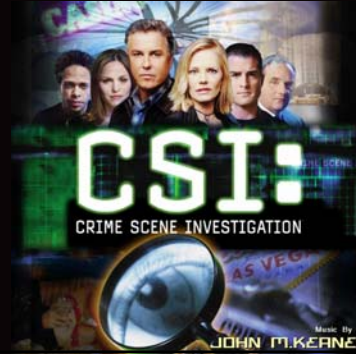
- Paraben
 - A comprehensive forensic tool for investigating Palm, Pocket PCs, and BlackBerry devices
 - Can produce forensic images and perform data searches as well as crack passwords for Palm



Reference: Computer Forensics: Principles and Practice
Valerina Appaldin, Cedric

In Practice: Do Nothing Without Competence

- Prosecutions may be jeopardized if untrained personnel compromise data by not following correct procedures
- Companies should have a proper incident response plan and policies in place



Reference: Computer Forensics: Principles and Practice
Valerina Anzaldúa Cedeno



Forensics Equipment (for you to investigate)

Type	Tool or Toolkit	Free Demo	Web Site
Password cracker	Passware kit	Yes	www.lostpassword.com/kit.htm
Password cracker	John the Ripper	Yes	www.openwall.com/john
Forensic intrusion detection, and scanning tools	Foundstone	Yes	www.foundstone.com/resources/forensics.htm

Reference: Computer Forensics: Principles and Practice
Valerina Anzaldúa Cedeno



Dr. Nazli Hardy, 2009

Career in Computer Forensics: Certification and Training Programs

- EnCE®—EnCase Certified Examiner
- Global Information Assurance Certification (GIAC)
- Computer Hacking Forensic Investigator (CHFI)
- Computer Forensic External Certification (CCE)
- TruSecure ICSA Certified Security Associate
- Computer Forensic Training Center Online
- Certified International Information Systems Forensics Investigator (CIFI)

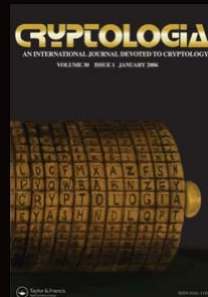
Reference: Computer Forensics: Principles and Practice
Valerina, Anandhu, Cedric



Dr. Nazli Hardy, 2009

Sources

- International Journal of Digital Evidence
- The Journal of Applied Forensics and eDiscovery
- International Journal of Digital Crimes and Forensics
- Journal of Digital Forensics Practice
- Digital Investigation
- Cryptologia



Reference: Computer Forensics: Principles and Practice
Valerina, Anandhu, Cedric



Dr. Nazli Hardy, 2009

Summary of Computer Forensics (remember it is a science)

- Quality of e-evidence depends on skilled investigators
- Maintaining the integrity of e-evidence requires a defensible approach
- There can be no weak links in the investigative process
- It is vital for the investigator to be able to extract and analyze data quickly and present the evidence in an understandable format
- Investigators frequently have to defend their findings, methods, tools, and techniques
- Technologies and methodologies must be well documented and repeatable
- Specialized software and hardware tools are needed for documentation, collection, authentication, analysis, preservation, and production and reporting of findings and e-evidence
- There are several certification and training programs that computer forensics investigators can complete to help them become credible in the field



Contact for Further Discussions

Nazli Hardy

- Website: <http://cs.millersville.edu/fs/nhardy/>
- Email: Nazli.Hardy at Millersville.edu

