Computer Forensic

Emil SIMION

Agenda

- Characteristics of computer forensic
- Types of digital evidence
- Rules for evidence
- Locations for evidence
- Methodology
- Applications
- Skills
- Conclusions

Characteristic of computer forensic

- Identifying
- Preserving
- Analyzing
- Presenting

Types of Digital Evidence

- Persistent data
- Volatile data

Rules of evidence

- Admissible
- Authentic
- Complete
- Reliable
- Believable

Location for evidence

- Internet history files
- Temporary internet files
- Slack/Unallocated space
- Settings, folder structure, file names
- File storage dates
- Software/hardware added
- File sharing ability
- Emails
- Personal chat room records
- Club list/posting

Computer forensic methodology

1. Shut down the computer
2. Document the hardware configuration of the system
3. Transport computer system to a secure location
4. Make a bit stream backup of the hard disks
5. Mathematically verify data an all storage devices
6. Document the system date and time
7. Make a list of the key search words

Computer forensic methodology- cont

8. Evaluate the windows swap file
9. Evaluate file slack
10. Evaluate unallocated space
11. Search files, file slack and unallocated space for the key words
12. Document file names, dates and times
13. Identify file, program and storage anomalies
14. Evaluate program functionality
15. Document your findings

Applications

- Financial fraud detection
- Criminal prosecution
- Civil litigation
- Corporate security policy violation

Skills

- Programming or computer-related experience
- Understanding operating systems and applications
- Analytical skills
- Computer science fundamentals
- System administrative skills
- Intruder tools
- Cryptography and steganography
- Rules of evidence and evidence handling
- Ability to be an expert witness in a court of law

Tools

Cloud services

Delete file recovery

Disk Imaging

Email parsing

File carving (searching for and reconstructing files based on content, rather than file system metadata.)

Forensic boot enviroment

Forensic Tool Suite (Mac Investigations)

Forensic Tool Suite (Windows Investigations)

GPS Forensics

Hardware Write Block

Hash Analysis

Tools-cont

Image Analysis (Graphics Files)

Infotainment & Vehicle Forensics

Instant Messenger

Media Sanitization/Drive Re-use

Memory Capture and Analysis

Mobile Device Acquisition, Analysis and Triage

P2P Analysis

Password Recovery

Remote Capabilities / Remote Forensics

Social Media

Tools-cont

Software Write Block

Steganalysis

String Search

Web Browser Forensics

Windows Registry Analysis

Conclusions

References

- http://www.cftt.nist.gov/