

University of Rochester
CSC290B
Introduction to Computer Security

Computer Forensics

April 24, 2009

What is Computer Forensics?

- After the fact, understand what happened
 - Reconstruct data
 - Reconstruct sequence of events
 - Provide evidence for sanctions or law enforcement process
- Often similar problems to Audit
 - *But what if audit trail inadequate?*
 - Audit information incomplete/insufficient
 - Audit trail damaged
 - We don't own the computer

What is the challenge?

- Audit information incomplete/erased
 - Reconstruct deleted information
- “Acceptable” state of system unknown
 - Need to identify violation in spite of this
- Goal not obvious
 - Transformations may have been applied to data
- Strong burden of proof
 - Not enough to know what happened
 - Non-repudiation: Must be able to prove it (modulo a legal standard, such as “beyond a reasonable doubt”), even in the face of some deniability story

FBI List of Computer Forensic Services

- Content (what type of data)
- Comparison (against known data)
- Transaction (sequence)
- Extraction (of data)
- Deleted Data Files (recovery)
- Format Conversion
- Keyword Searching
- Password (decryption)
- Limited Source Code (analysis or compare)
- Storage Media (many types)

Forensic Tools

- Capture system state
- Filesystem exploration
 - Time-based
 - Metadata
 - Unallocated space
- Specialized databases such as Windows registry present similar issues for data available for tools
- Reconstruction, detection, brute-force decryption

Tools for Capture

- Disk imaging
 - Capture exact state of disk, calculate integrity checks (typically MD5 or SHA1)
 - Commercial products EnCase or FTK Imager are common. Linux ‘dd’ is also in use (with integrity checks alongside).
- It is possible to capture live system state (with some risk of system modification)
 - Hardware, sometimes DMA
 - Has been done with PCI or Firewire
 - “Cold RAM” RAM remanence after shutdown
 - Software, copying process state, file state, kernel state

Filesystem exploration – time-based

- Tools for sorting file information by time:
 - Modify time
 - Access time
 - Change of inode time (Unix concept)
 - Deletion time
- May be limited to existing files or may include information on deleted files as well

Filesystem exploration – metadata

- Exploring raw filesystem data, aware of internal data structures
 - E.g. Unix/Linux filesystems describe files with inodes, which point to indirect address blocks and direct data blocks
 - Data is often still present even for deleted files
- Tools
 - List inode information
 - Copy files by inode
 - Undelete
- Other filesystems have features that benefit from specialized exploration tools (e.g. Windows NTFS files can have multiple streams of data)

Filesystem exploration – reconstruction

- Raw filesystem data includes remnants of deleted data, which may be usable even if metadata (e.g. indirect blocks) are gone.
- Filetype-aware file reconstructors can recover stretches of contiguous blocks that represent fragments of original files, make tentative filetype identifications.
- Even scattered fragments of files may be usefully identified as candidates for rejoining.

Filesystem exploration – identification

- Recognizing hidden data structures
 - File streams (Windows)
 - Encrypted filesystems
 - Steganography (embedding one file in another)
 - Placing a file in the lower-order bits (or unused bits) of another file, for filetypes where that looks like imperceptible noise (various image or audio filetypes)
 - Placing an encrypted filesystem in what appears to be unallocated data blocks of a conventional filesystem (StegFS)

Filesystem exploration – brute-force decryption

- With awareness of encryption method, perform dictionary attacks on files, filesystems, key stores.
- Prepopulate dictionary with other filesystem contents to make educated guesses for a user's possible passwords

Law Enforcement Challenges

- Many findings will not be evaluated to be worthy of presentation as evidence.
- Many findings will need to withstand rigorous examination by another expert witness
 - Credentials are relevant
- The evaluator of evidence may be expected to defend their methods of handling the evidence being presented
 - Training is relevant
- The Chain of Custody may be challenged

Incident Response

- Documented procedures are important
- Minimum modification or disturbance of the system is important
 - Removal from network, examination of process state, network connection state
 - Avoidance of filesystem-modifying examination
- Maintain a journal, with dates, times, detailed notes
- Collate system logs to support analysis
- Take care with storage, packaging, labeling

Tools

- Commercial:
 - EnCase and AccessData are prominent vendors (and vendor certification and training matter if testifying)
- Free:
 - Various open source tools are available; easy way to use them is with a bootable Live CD distribution, e.g. Helix.

Anti-forensics

- Data wiping
 - Simple overwrite may not suffice
 - Disk remanence: multiple overwrites may be necessary
 - Flash memory write leveling may put new data in new physical locations
 - Filesystem journalling may put new data in new logical locations
 - Sensitive data may remain in memory or in page/swap files longer than expected

Anti-forensics

- Activity hiding
 - Timestamps can be overwritten
 - Timestamp updating can be disabled on some systems
- Data hiding
 - Steganography
 - Placement in various unused locations in filesystems or files or hardware devices
 - Obscured packing of hostile executable content

Anti-forensics

- Detect forensic activity, then:
 - Trigger defensive data destruction (or at least destruction of in-memory encryption keys)
 - Quiesce into an innocuous or “plausible deniability” stance
 - Invoke hostile code against known weaknesses in forensic tools (e.g. buffer overflows)