Computer forensics

As part of a security incident response plan

Raemarie Schmidt
Digital Intelligence, Inc.
June 28, 2005

Raemarie J. Schmidt

- Vice President, Digital Intelligence, Inc.
- 8 years Supervisory Computer Crime Specialist, NW3C
- 21 years forensic crime laboratory
  - Wisconsin State Crime Laboratory
  - Virginia Division of Forensic Sciences
Topics

- “Computer forensics”
- Areas to examine for information
- How computer forensics can be useful in a corporation
- Creating an in-house capability
- Incident response considerations

In the beginning…
And now…

Various types of media

- May be owned by the employee…
Computer forensics

- **Protect** the data
  - Software & hardware write-blockers
- **Preserve** the data
  - Duplicate image software & hardware
- **Recover** the data
  - Examination of allocated/unallocated space & system and application specific areas
- **Analyze** recovered data
  - Put the results in perspective

©2005 Raemarie Schmidt & Digital Intelligence, Inc. All rights reserved.

Protect the data

Software & hardware write-blockers
Traditional disk access

Interrupt 13/13x write blocker
Other types of drive access

- Application
  - Windows API
  - Windows OS
  - Windows IDE drivers
- Hardware write blockers
  - Blocks all writes to a connected device
  - Examples
    - IDE to IDE
    - IDE to SCSI
    - IDE to USB or Firewire
- Examples
  - IDE to IDE
  - IDE to SCSI
  - IDE to USB or Firewire
Preserve the data

Preserve data

- File copy
  - Gets ONLY content of active files
- Forensic copy
  - Gets ALL data of object being imaged
    - Partition or logical drive
    - Physical drive
Duplicate image hardware

- Hardware based
  - Drive to drive
  - Drive to image file

Duplicate image tools

- Software based
  - Linux dd
  - Encase en
  - FTK
  - Safeback
  - Ghost
  - Digital Intelligence
  - Etc.
Recover the data

Popular automated tools

- Forensic Tool Kit (FTK)
  - Access Data
- Encase
  - Guidance Software
- ILook Investigator
  - Rights owned by IRS
  - Law enforcement only

©2005 Raemarie Schmidt & Digital Intelligence, Inc. All rights reserved.
Specialized individual tools

- Digital Intelligence
- Imaging
- NTFS
- Internet

File Viewers
- Password recovery
- Multifunction

Types of data that can be recovered
Forensic analysis

- Files
  - Active
  - Temporary
  - Deleted
- Print spool
- Document “metadata”
- Internet activity

Forensic analysis

- Encryption
- Email & deleted email
  - Content & attachments
  - Detailed header information
- Slack and unallocated space examination
- Information from damaged media
Unallocated space

- Area of a logical drive not assigned to an active file
  - FAT – “0” in the File Allocation Table
  - NTFS – “0” in $Bitmap
- May contain deleted files that no longer have a pointer in the file system

Virtual memory

- Used by Windows to store data that does not fit in (and is not currently required by) RAM
  - Win9x – called the “swap file”
    - win386.swp
  - WinNTx – called the “pagefile”
    - pagefile.sys
- Can contain data from RAM that was never stored as a file
Data carving

- Data can be recovered from unallocated space, virtual memory and contents of RAM saved to a file, where no directory information exists
  - Uses file headers
  - Called “data carving”
- DataLifter - http://www.datalifter.com/

©2005 Raemarie Schmidt & Digital Intelligence, Inc. All rights reserved.
Data carving

- RunMRU
- RecentDocs
- TypedURLs
- MountedDevices
- IE AutoComplete and stored passwords
- And on, and on, and on....
Analyze the data

Put it into perspective

Location

- Temporary Internet Files (TIF)
- Specifically named subdirectory structure
- Non-traditional locations
  - Named data streams
  - “Hidden” areas

©2005 Raemarie Schmidt & Digital Intelligence, Inc. All rights reserved.
Date & time

- Modified, Access, Creation dates/times
- Relative to UTC?
- What computer is the date/time coming from?
  - Local system clock
  - Network server
- System clock accuracy

User specific information

- Recycle Bin
- Logfiles
- Security descriptors
- Print spool files
- Who was at the keyboard?
Potential uses of computer forensics

Data preservation

- Routine data archival
  - Protect against catastrophic loss
  - Support record retention policies
- Employee termination
  - Preserve information under employee control & not stored elsewhere
  - Maintain status of system prior to assigning to a new employee

©2005 Raemarie Schmidt & Digital Intelligence, Inc. All rights reserved.
Data recovery

- Deletion of data (e.g. files or email)
  - Intentional
  - Accidental
- Operating system or file system malfunction
- Hardware failure
- Virus or Trojan activity

Employee misconduct

- Confirm or refute allegation
- Recover information thought to be removed (e.g. deleted files, deleted email)
- Protect against a wrongful-termination suit
Theft of Intellectual property

- Identify individual(s) involved
- Identify method used
  - Removable media?
  - Remote access?
- Determine other media to examine
  - LNK files
  - Mounted devices
  - Network storage

Mergers and acquisitions

- Identify misrepresentations
- Respond to discovery requests
- Provide litigation support
Intrusion analysis

- Determine method
  - Use for remedial action
- Identify intruder
- Determine information compromised
  - Trade secret?
  - Client personal information?
  - Legal/medical records?

Intellectual property

- Protect against accidental loss through document *metadata*
Equipment recycling

- What else is being recycled?
  - Format or delete is not sufficient
  - Residual Information left behind
- “Wipe” media prior to disposal

Establishing a forensic capability
Identify personnel

- IT/CS/MIS education does NOT prepare a forensic examiner
- Basic & advanced computer forensics training required
- Tool-specific training advised

Dedicated area

60' x 41'

©2005 Raemarie Schmidt & Digital Intelligence, Inc. All rights reserved.
Consider a dedicated network

Use a dedicated forensic system

- Not part of corporate network
- Configured for forensic work
  - To prepare a “forensic copy”
  - To perform a forensic examination
- Restored to original configuration after each incident
Dedicated forensic systems

- Digital Intelligence
- Forensic Computers
- Vogon
- Dibs
- Etc.

Dedicated forensic systems

- Removable drive trays
- Master/slave switch
- Write-protect hardware
  - Floppy drive
  - IDE, SATA, SCSI
  - Multimedia card reader
- RAID capability for increased storage
Dedicated forensic systems

- Removable drive trays
- Master/slave switch
- Write-protect hardware
  - Floppy drive
  - IDE, SATA, SCSI
  - Multimedia card reader
- RAID capability for increased storage

Dedicated forensic systems

- Data center
  - Processing
  - RAID-5 storage
  - Forensic network
  - File server
Dedicated forensic systems

- Commercial Off The Shelf (COTS) with hardware write-blockers will work…

Outsource?

- In-house forensics is expensive
  - Evaluate the frequency of need
  - Determine the investment in resources
  - Do the math
- Evaluate the credentials of 3rd party companies offering services
Incident Response

At a minimum

Preparation

- Document system baselines
- Create SOPs and prepare logbook
- Identify contact information
  - Responding law enforcement agency
  - Additional resources
  - Management reporting structure

©2005 Raemarie Schmidt & Digital Intelligence, Inc. All rights reserved.
Preparation

- Create trusted response disk
  - Command shell
  - Tested and validated utilities
    - Identify system dependencies
    - Document command line options
  - Baseline records
    - Computer systems
    - Utilities and dlls

Preparation

- Identify method of storing data output
  - Network share
  - Floppy disk
  - USB drive
  - Etc.
Preserve data

- Collect volatile data
- Protect non-volatile data
  - Shutdown methods
  - Chain of custody
  - Write-blockers

Questions?

Raemarie Schmidt
Digital Intelligence, Inc.
Tel: 262-524-9363 Ext 32

email: rschmidt@digitalintelligence.com
Web: http://www.digitalintelligence.com