

# Computer forensics

## As part of a security incident response plan



Raemarie Schmidt  
Digital Intelligence, Inc.  
June 28, 2005

©2005 Digital Intelligence, Inc. All rights reserved. May not be reproduced or distributed in whole or in part without the prior written permission of Digital Intelligence, Inc.

## 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

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



# 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

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



# In the beginning...



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



And now...

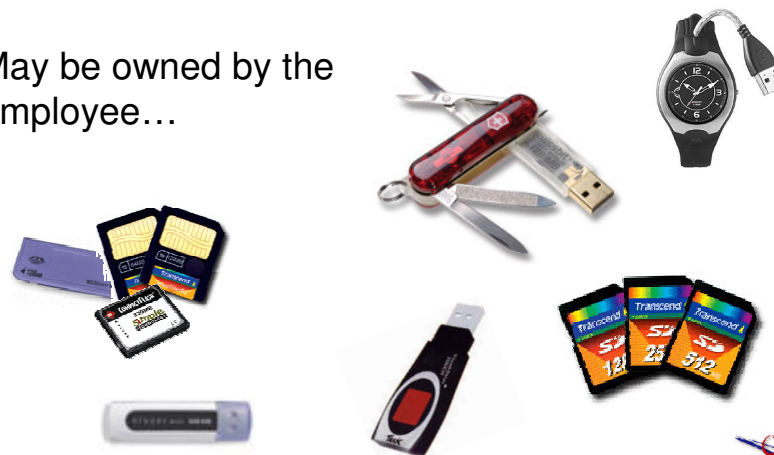


©2005 Raemarie Schmidt & Digital Intelligence, Inc. All rights reserved.



## Various types of media

- May be owned by the employee...



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



# 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

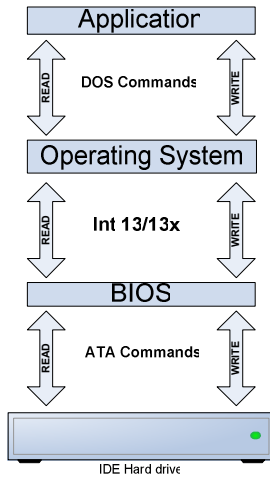
©2005 Raemarie Schmidt & Digital Intelligence, Inc. All rights reserved.



## Protect the data

Software & hardware  
write-blockers

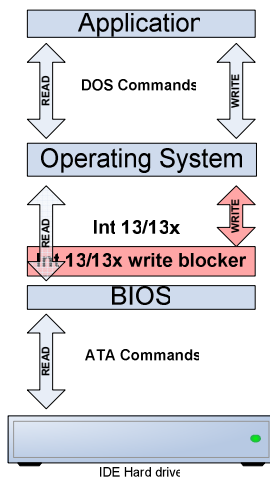
# Traditional disk access



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



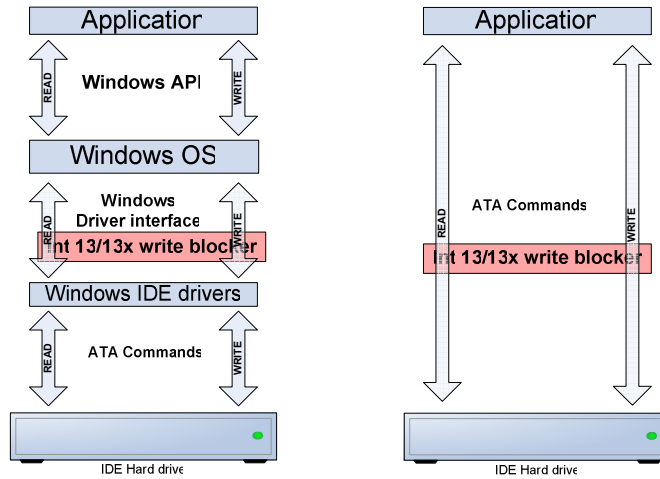
# Interrupt 13/13x write blocker



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



# Other types of drive access



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



# Hardware write blockers

- Blocks all writes to a connected device
- Examples
  - IDE to IDE
  - IDE to SCSI
  - IDE to USB or Firewire



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





# 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

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



## Duplicate image hardware

- Hardware based

- Drive to drive
- Drive to image file



HardCopy



Logicube



ImageMASter

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



## Duplicate image tools

- Software based

- Linux dd
- Encase en
- FTK
- Safeback
- Ghost
- Digital Intelligence
- Etc.



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





# Recover the data

## Popular automated tools

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



## Specialized individual tools

- Digital Intelligence
- Imaging
- NTFS
- Internet
- File Viewers
- Password recovery
- Multifunction

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



## Types of data that can be recovered



## Forensic analysis

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

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



## Forensic analysis

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

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



## 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

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



## 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

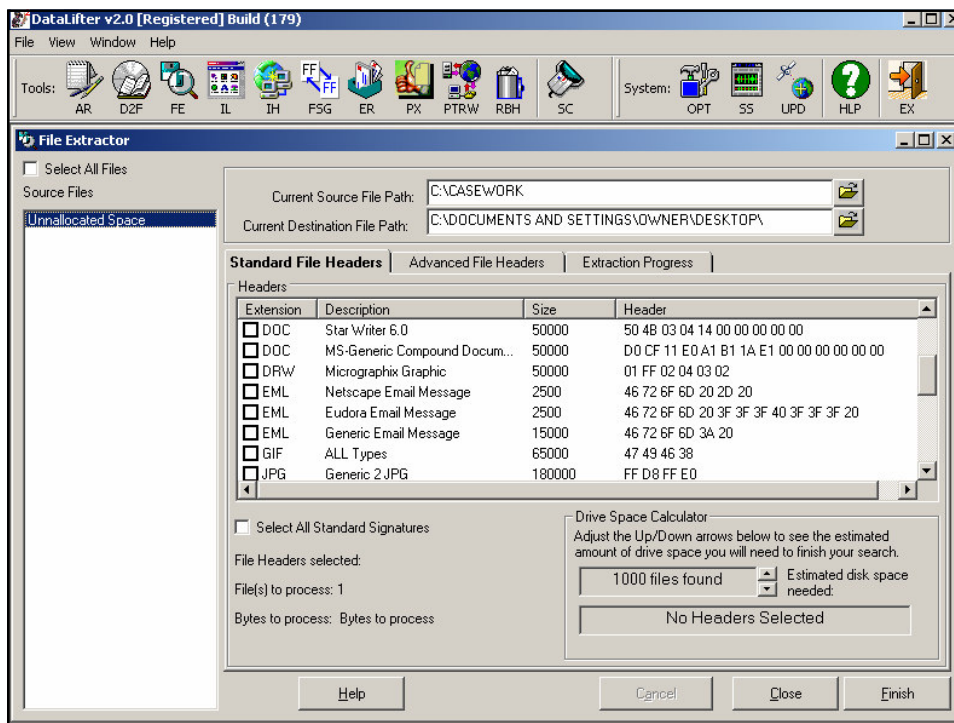
©2005 Raemarie Schmidt & Digital Intelligence, Inc. All rights reserved.



# 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

```

..nevada>ports >chedule.....*.....S.....K.....
.....'A.'A.'A.'L.....L.....|.....
.....S.'S.'S.'L.....'A.'AC'.....L.....
.....SportsGazette.....S.....P.....
.....'A.'A.'A.'L.....L.....|.....
.....S.'S.'S.'L.....'A.'As'...../.....
.....L.....Product/Offers.....*.....JF
IF.....C.....!.....
....."$.$.$.C.....
.....).....!A..Qa."q.2.....#B...R..$3br.....$4'()*456789:
CDEFCHIJUSTUVWXYZcdefghijstuvwxyz
.....w.....!1..AQ.aq."2...B.....#3R..br...$4.*.....4'()
*56789:CDEFCHIJUSTUVWXYZcdefghijstuvwxyz
.....?.....*.....+.....?.....~
.6.6.5..4.$..n.e7>lH.VP...4J.D...7H.X\...\i+...b...e...L.x.DfM>
jZ{II'...+n..e.C.o+...eI..J&'...3....._...x...5.....A$.n.M
?.....".....[...>!BV.Z.m.i.F.T.....F.>-h...n...58t...S#X...RI..
em.....F.....moM?>.....i.[.../...' ]...r>#lw...>[...QJ\..SL...*(|A
{...j:..^'.C&...qk>.h#.N..w..S..6..'n.OS..\...i^...S.n.C...j
u4.H..N...{mP2P.cpl.m.u4.fOM.J.I;...y.G.Q\%...Q.y..OT...W..Z
U$E..H.etbFP1...$...tj..2.mgo}....y...DU.{(.G...c.6
..I.@.s.{?..yb.*...yH..H...[...d...L.d..2<o).I..G..|X.7
..b..Z)...yb.*...yH..H...[...d...L.d..2<o).I..G..|X.7
..^;6.....N:...O..lg...X.7...W...D...iD..i)Z...h.Y..p.S.<2
..p.l...N:...O..lg...X.7...W...D...iD..i)Z...h.Y..p.S.<2
.....f\..F..S.n...q...D...-j...K...4...#td7^d.tq...\..w)?

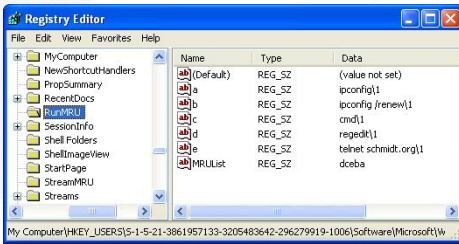
```

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



# Forensic analysis of the registry

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



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





# Analyze the data

Put it into perspective



## Location

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



## 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

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



## User specific information

- Recycle Bin
- Logfiles
- Security descriptors
- Print spool files
- Who was at the keyboard?

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





# 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

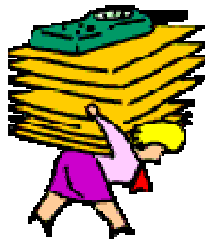
- Identify individual(s) involved
- Identify method used
  - Removable media?
  - Remote access?
- Determine other media to examine
  - LNK files
  - Mounted devices
  - Network storage



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

## Mergers and acquisitions

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



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

# Intrusion analysis

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

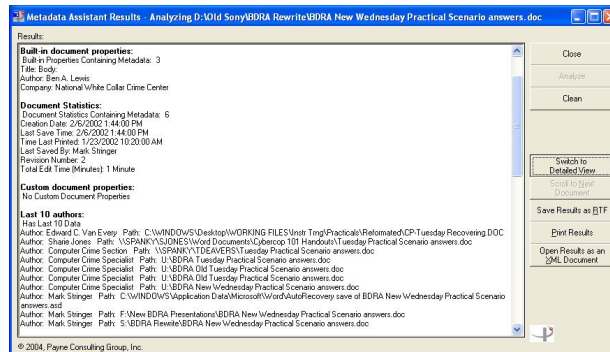


©2005 Raemarie Schmidt & Digital Intelligence, Inc. All rights reserved.



# Intellectual property

- Protect against accidental loss through document *metadata*

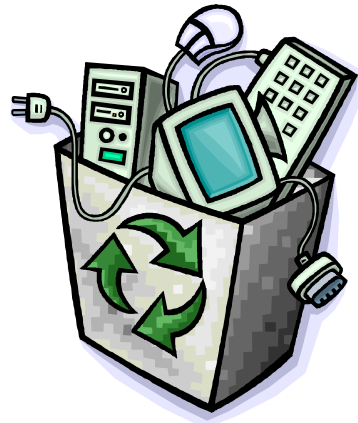


©2005 Raemarie Schmidt & Digital Intelligence, Inc. All rights reserved.



## Equipment recycling

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



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

## Establishing a forensic capability



# Identify personnel

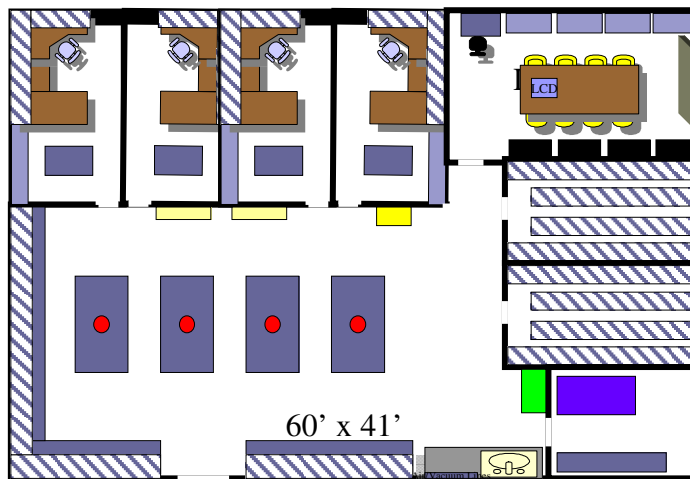
- IT/CS/MIS education does NOT prepare a forensic examiner
- Basic & advanced computer forensics training required
- Tool-specific training advised

Monday	Tuesday	Wednesday	Thursday	Friday
Welcome	Review	Review	Review	Review
Class scenario	Encryption	Long Filenames		
		File Types		Forensic Lab Design
				Expert Testimony
			Email	Lunch
Lunch	Lunch	Lunch	Lunch	12:30 Final Practical
			Date Stamps	
IDE Drive Config	File Systems			
SCSI Drive Config			Controlled Boot Floppy	
Physical Drive Structure		Recycle Bin		Review
Bits and Bytes			Forensic Problem Solving	
		Compression	Hardware Write-Protect	
Imaging	Boot Sequence		Developing Forensic Procedures	
		Keyword Searching		

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



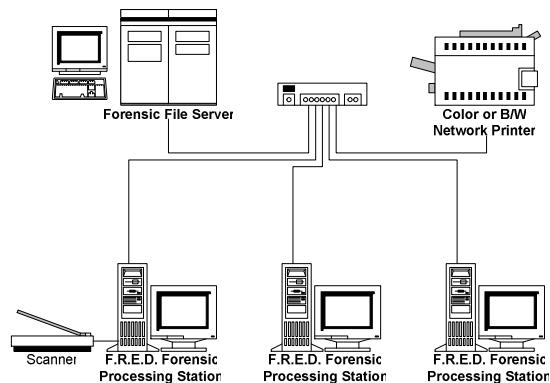
# Dedicated area



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



## Consider a dedicated network



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



## 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

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



## Dedicated forensic systems

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



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

## 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



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



## 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



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

## Dedicated forensic systems

- Data center
  - Processing
  - RAID-5 storage
  - Forensic network
  - File server



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

## Dedicated forensic systems

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



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



## Outsource?

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

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



# 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

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



# Preparation

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

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



## Preserve data

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

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



## Questions?

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

email: [rschmidt@digitalintelligence.com](mailto:rschmidt@digitalintelligence.com)

Web: <http://www.digitalintelligence.com>

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

