

A close-up photograph of a hand moving a chess piece on a chessboard. The scene is dimly lit with a blue tint. The chessboard is in the foreground, and the hand is in the upper right corner, moving a dark piece. The background is dark and out of focus.

A Forensic Process For Organizational Computer Security

William “Bill” Mee
MS, ISSA, GSEC

Bio

- Security Analyst – VCUHS/MCV (Forensics)
- Dept. Chair - ITT (BA Security)
- IT Director – Augusta County
- Technical Services Mgr. – Chesterfield County
- Sr. Systems Engineer - Hitachi
- Expert Witness Experience
- MS (Information Systems from VCU)
- SANS GSEC Security
- Information Systems Security Association (ISSA Central VA)
- 8th Annual Security Conference, Las Vegas, 2009
- Computer Measurement Group (CMG)

Agenda

- What is Computer Forensics?
- Accepted Methodology
 - Steps in an Investigation
- Tools and Resources
- The Case “For” and “Against” DIY

Computer Forensics and Implications to the organization Organization

- Computer forensics basic should be part of organization's "defense-in-depth"
 - Use basic forensic techniques that does not hinder law enforcement and investigations of crime
 - Policy makers should understand the issues needed to address privacy and security

Why Computer Forensics?

- Most Organizations - Low Hanging Fruit
 - Hackers find the computer systems an easy target for their crimes and have become sophisticated in hiding their illegal activities
 - Most operating system and applications leave behind important information in multiple places

A Short History of Computer Forensics

- Early 1980's
 - Kevin Mitnick broke into the University of Southern California's VAX/VMS and DEC systems with a stated goal to “liberate” disk space
 - Kevin Poulsen electronically seizes phone lines of a major Los Angeles radio station to win “the 101st caller”

1990's Evolution of Computer Forensics

- First International Conference on Computer Evidence was held in 1993.
 - Mitnick convicted on charges of stealing computer time from a phone company.
 - Poulsen - first computer hacker to be charged with espionage for obtaining a classified document from a military database.

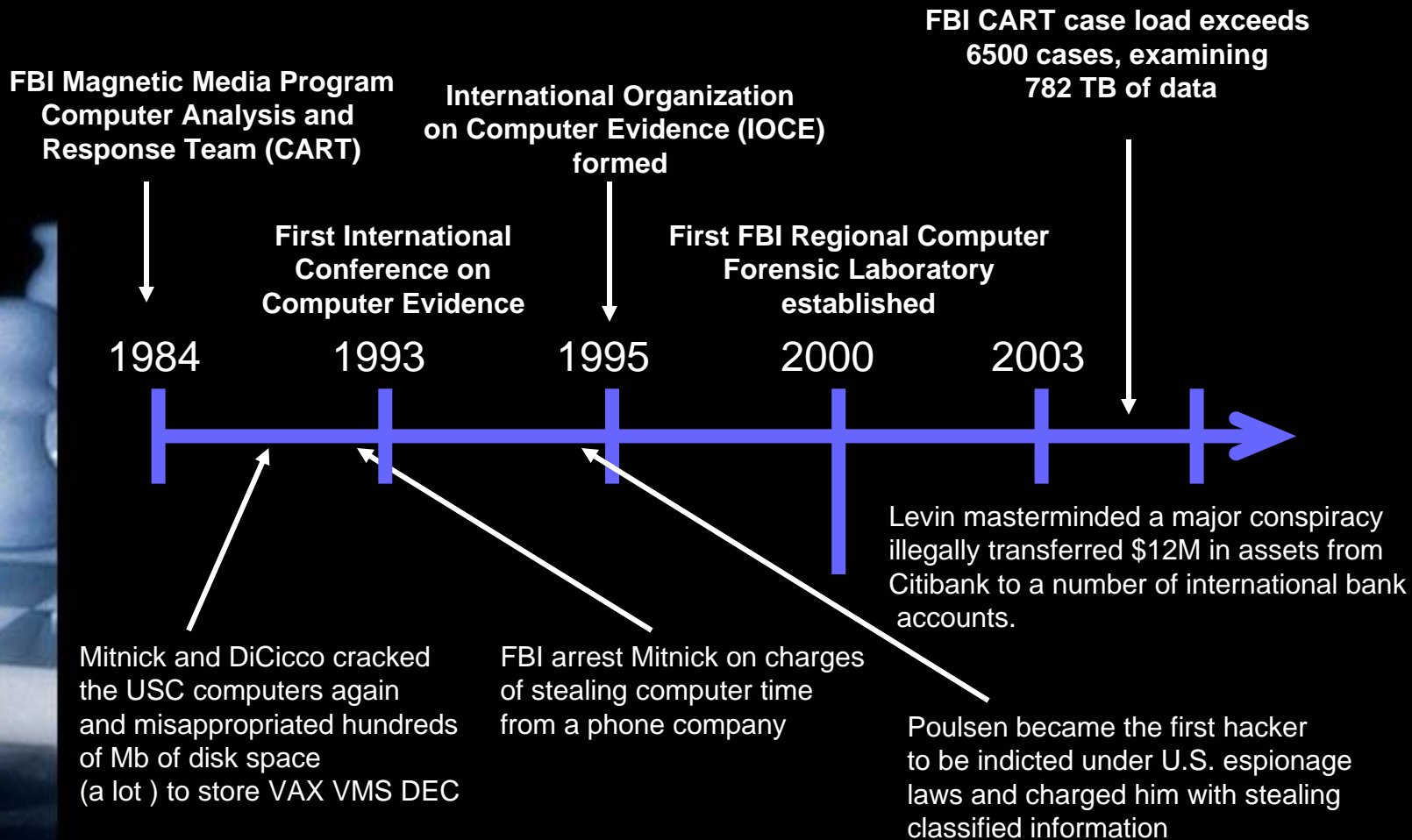
The Dark Side of Hacking

- Citibank discovered \$400,000 missing in July 1994
 - Levin illegally transfers \$12M in assets from Citibank to a number of off-shore bank accounts
 - First Chief Information Security Officer (CISO) position with the hiring of Stephen R. Katz

Government Response

- 2000
 - FBI established the first FBI Regional Computer Forensic Laboratory
- 2003
 - FBI CART case load exceeds 6500 cases and consists of about 782 TB of data

Computer Forensics Still Evolving – Definitions & Standards



Current Threats – A Reason for Computer Forensics

- *Identity Thefts and Phishing Scams*
 - Specialized hacking tools and services are commonly traded on international cyber sites.
 - Such sites often include sophisticated money laundering operations that operate as virtual banks

Compliance and Security Best Practices

A Reason for Computer Forensics

- Personal Identifiable Information (PII)
 - organization should be able to demonstrate that a Computer Forensics investigation was applied in such a way that meets *standards*
- Ability to satisfy regulatory audits
 - formal organizational policy,
 - incident response procedures

What is Computer Forensics?

It depends on who you ask

- Computer forensics is a branch of forensic science pertaining to legal evidence found in computers and digital storage mediums. ...
en.wikipedia.org/wiki/Computer_forensics

What is Computer Forensics?

It depends on who you ask

ISACA – IS Auditing Guideline
(Doc G28)

- Computer forensics can be defined as the process of extracting information and data from computer storage media using court validated tools and technology and proven forensic best practices to establish its accuracy and reliability for the purpose of reporting on the same as evidence.

What is Computer Forensics?

- “Computer forensics is a science as well as an art” - ISACA –

IS Auditing Guideline

- extracting and gathering data from a computer
- determine if and how an abuse or intrusion has occurred
- when it occurred
- who was the intruder or perpetrator

What is Computer Forensics?

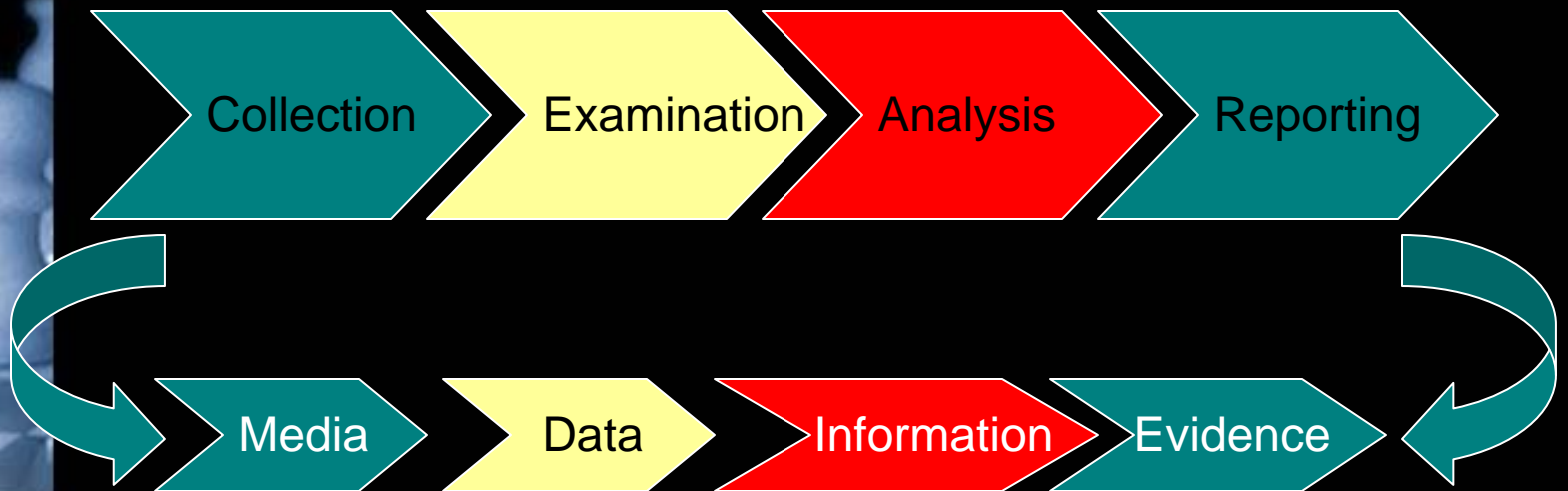
It depends on what you're asked to do

- What are you looking for?
- What's the time-scale?
- Where's the physical/virtual location?
- Which applications?

Is There a Clear Definition?

- Lacking a clear definition of Computer Forensics results in:
 - organizations ignore its place in the arsenal of cyber defense
 - address events that require an investigative process on an *ad hoc* basis

Not a Definition But a Process



Collection Phase

- Conducted in such a manner as to be legally admissible in a court case
 - What is the evidence?
 - How did you get it?
 - When was it collected (time-stamp)?
 - Who has handled it (signatures)?
 - Why did that person handle it?
 - Where has it traveled, and where was it ultimately stored?

Request/Mandate

REQUEST FOR SERVICE

CASE INFORMATION:		RCFL Case #:
Submitting Person/ID#:	Date:	Agency Case #:
Submitting Agency:	Service: Field Lab Tech	Case Title:
Agency Property Tag #:	Suspect's Name:	
Case Agent:	Phone #:	
DDA/AUSA Assigned:	Phone #:	
Date Seized:	Case/Crime Type:	
Location Seized:	Pending Court Dates:	
Site #:	Date Analysis Needed:	
Suspect In Custody:	Yes/No	Expected Evidence Return Date:
Narcotics Related:	Yes/No	Number of Computers Anticipated:
Type of Seizure: (Circle) Search Warrant Probation Parole Consent Admin Fed. Grand Jury Other:		
Has this evidence been previously viewed and/or accessed by anyone? (Explain)		
Are you aware of any privileged information contained within evidence? (Explain)		
Do you want Standard Case Related Search Strings run against evidence? Yes/No		
(Circle Requested Searches) Child Porn Narcotics Financial Crimes Internet Crimes Extortion Other:		

Understand the Implications

- Containment
 - disconnecting network cables,
 - unplugging power,
 - increasing physical security measures, gracefully shutting down a host)
- Business Impact
 - Operations?
 - Physical Security limited access to ensure that the evidence is not altered

Procedures Designed to Prevent Modification of Media

- Use a hard disk write block tool to intercept any inadvertent disk writes.
- When possible, set a hardware jumper to make the disk read only.
- Use an operating system and other software that are trusted not to write to the disk unless given explicit instructions.

Volatility: Dead or Alive?



Examination Phase

- Builds on the *Collection Phase*
 - original evidence must be protected from accidental or unintentional damage or alteration
 - must be duplicated exactly to create a copy that is true and accurate

Original
Evidence

"Best"
Evidence

Secondary
"Working"
Copies

Decision Determines Data

Non-Volatile

- Configuration files
- Users & Groups
- Password Files
- Scheduled Jobs
- Logs
- System Events
- Audit Records
- Application Files
- Data Files

Evidence

Volatile

- Slack Space
- Free Space
- Network Connections
- Network Config
- Running Processes
- Open Files
- Login Sessions
- Operating System
time

Decide on How to Collect

Bit-Stream Image

Bit-for-bit copy
Free space
Slack Space
More Storage
Takes longer

Media

Logical Backup

Copies only files
& directories
No other data like:
- Slack space
- Deleted files

Tools

- The Coroner's Toolkit (TCT)
 - Suite of tools written by Wietse Venema and Dan Farmer to help a System Admin doing forensic analysis on their cracked Unix box (C and Perl).
- Access Data's Forensic Toolkit® (FTK™)
 - File filtering and search functionality. FTK's customizable filters allow you to sort through thousands of files.
 - FTK is recognized as the leading forensic tool to perform email analysis.

Analysis Phase

- How does the “data” correlate to the “reason for the investigation” ?



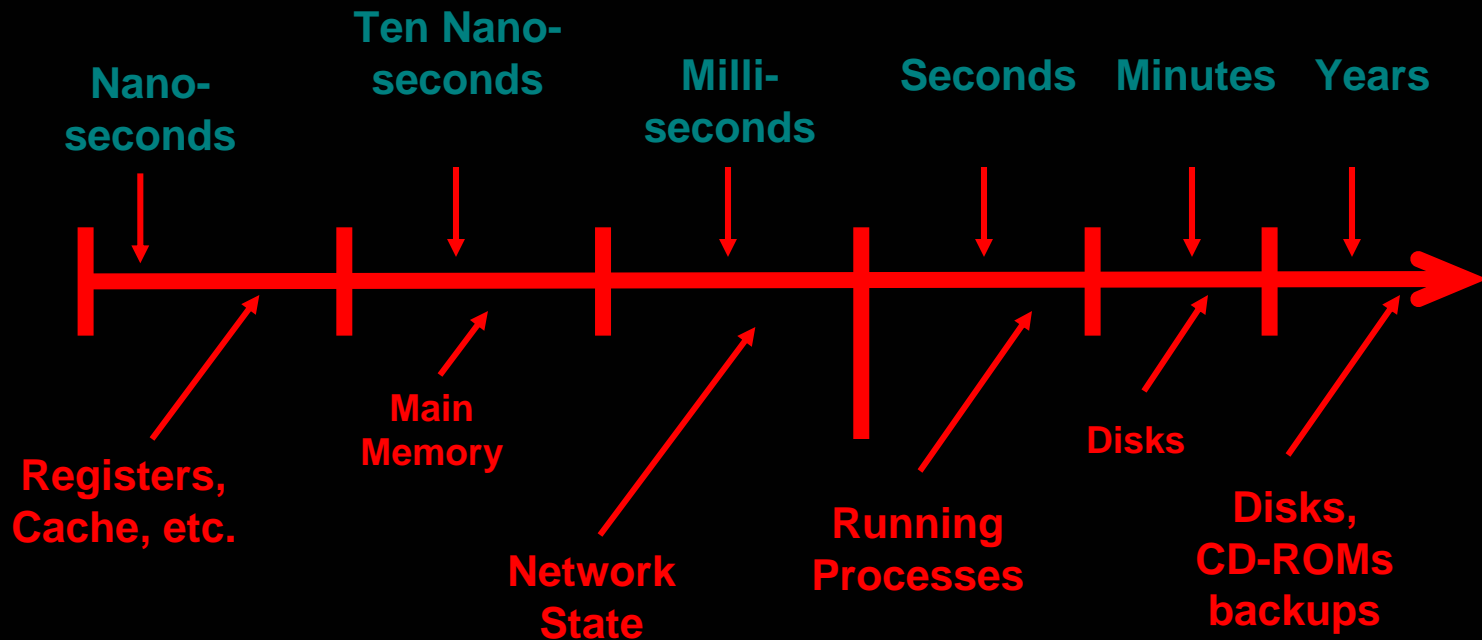
File Carving Utilities

- Reveal details that may not have been readily apparent. For example, the investigator might review file names for patterns before examining the details of the file or its content.
- Keyword and string or text searches are helpful to identify specific related to the scope of the investigation.
- *Thumbnails* in Encase present graphic images.

Analysis Techniques

- Timeframe
 - Review the time and date stamps contained in the file system metadata (e.g., last modified, last accessed, created, change of status) to link files of interest to the relevant timeframes
 - Review system and application logs that may be present. These may include error logs, installation logs, connection logs, security logs
- Data hiding
 - Correlate file headers to the corresponding file extensions to identify any mismatches.
 - Gain access to all password-protected, encrypted, and **compressed files**
 - Gaining access to a **host-protected area (HPA)**
 - Steganography

Life Span



Type of Data

Reporting Phase

- A Forensic Report typically is used to support *incident response* activities
 - The qualifications and the relevant experience of the expert;
 - The instructions and any material facts that were given to the expert;
 - The material facts as it relates to the expert's own knowledge;
 - The details of the tests on the validity of the data performed;
 - The opinions and any qualifications of the expert as well as the range of professional opinion;
 - A summary of the conclusions reached.

Document Data and Evidence

Computer Evidence Worksheet

Case Number: _____ Exhibit Number: _____

Laboratory Number: _____ Control Number: _____

Computer Information

Manufacturer: _____ Model: _____

Serial Number: _____

Examiner Markings: _____

Computer Type: Desktop Laptop Other: _____

Computer Condition: Good Damaged (See Remarks)

Number of Hard Drives: _____ 3.5" Floppy Drive 5.25" Floppy Drive

Modem Network Card Tape Drive Tape Drive Type: _____

100 MB Zip 250 MB Zip CD Reader CD Read/Write

DVD Other: _____

Report Considerations

- **Alternative Explanations.** When the information regarding an event is incomplete, it may not be possible to arrive at a definitive explanation of what happened.
- **Audience Consideration.** Knowing the audience to which the data or information will be shown is important.
- **Actionable Information.** Reporting also includes identifying actionable information gained from data that may allow an analyst to collect new sources of information

Resources

- **Forensic Examination of Digital Evidence: A Guide for Law Enforcement, U.S. Department of Justice, Office of Justice Programs, National Institute of Justice-**
<http://www.ncjrs.gov/pdffiles1/nij/199408.pdf>
- **IS AUDITING GUIDELINE, COMPUTER FORENSICS DOCUMENT G28, ISACA IS Auditing Standards, www.isaca.org**
- **SANS Forensics Blog - <https://computer-forensics.sans.org/>**

Books

- **Computer Forensics Library Boxed Set (Paperback) Keith J. Jones (Author), Richard Bejtlich (Author), Curtis W. Rose (Author), Dan Farmer (Author), Wietse Venema (Author), Brian Carrier (Author)**
- **EnCase Computer Forensics, includes DVD: The Official EnCE: EnCase Certified Examiner Study Guide (Paperback) ~ Steve Bunting**

NIST

- NIST
- <http://csrc.nist.gov/publications/nistpublications/800-86/SP800-86.pdf>
- **Special Publication 800-86**

The Case “For” and “Against” a DIY Forensics Approach

- Are measures are in place to prevent information from being destroyed, corrupted or becoming unavailable?
- Are all parties informed that electronic evidence will be sought through discovery from the computer?
- Are there specific protocols requiring all parties to preserve electronic evidence?
- Do you have an Incident Response Team and forensic investigation capabilities already in place?
- Do you have the infrastructure and processes to handle incidents?

Questions?

Thank You For Your Time and
Encouragement!

Bill Mee

wmee@mcvh-vcu.edu

bmee@wirelessdatadesign.com

(cell) 804-543-3266