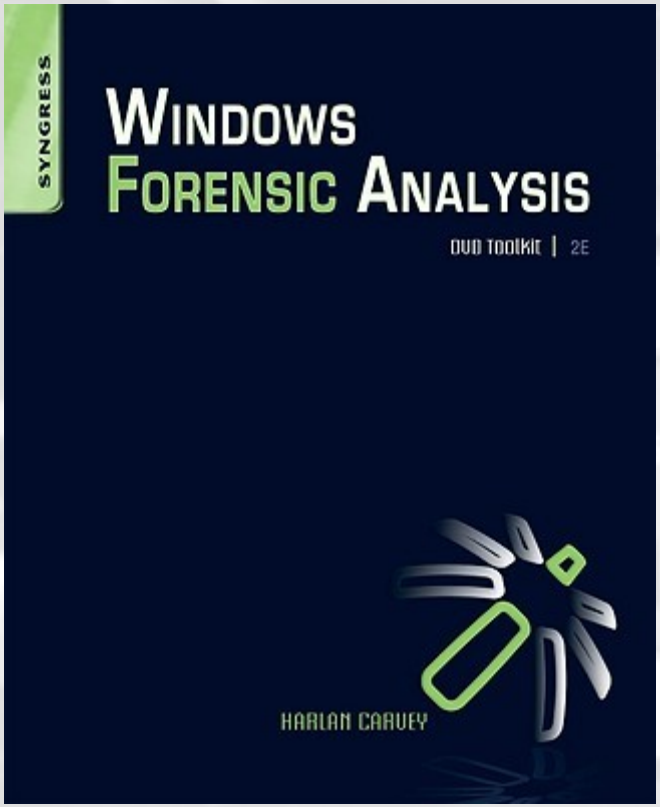
Introduction to Windows Forensics



Robert Baldi, CISSP-ISSEP
Robert Clauff

Session 1 & 2

Session 1 focuses on:

- Intro to forensic investigation
- Basic Windows GUI tools

Session 2 focuses on:

- Advanced tools
- Command line tools and scripts

What do I do first?

- Unplug the computer?
- Attach my computer to the network and capture traffic?
- Make a DD image?
- Start my documentation?
- Talk to the system/security administrator?

Understanding Computer Forensics

- Computer forensics involves obtaining and analyzing digital information for use as evidence in civil, criminal, or administrative cases

- The Fourth Amendment to the U.S. Constitution protects everyone's rights to be secure in their person, residence, and property from search and seizure

- When preparing to search for evidence in a criminal case, include the suspect's computer and its components in the search warrant

Computer Forensics Versus Other Related Disciplines

- Involves scientifically examining and analyzing data from computer storage media so that the data can be used as evidence in court

- Investigating computers includes:

  - Securely collecting computer data
  - Examining suspect data to determine details such as origin and content
  - Presenting computer-based information to courts
  - Applying laws to computer practice

Computer Forensics Versus Other Related Disciplines

Network forensics uses log files to determine:

- When users logged on or last used their logon IDs
- Which URLs a user accessed
- How he or she logged on to the network
- From what location

Computer investigations functions

- Vulnerability assessment and risk management
- Network intrusion detection and incident response
- Computer investigations

Network Forensics

Network forensic functions:

- Detect intruder attacks using automated tools and monitoring network firewall logs manually
- Track, locate, and identify the intruder and deny further access to the network
- Collect evidence for civil or criminal litigation against the intruders

Computer Forensics

Computer investigation functions:

- **Manage investigations and conduct forensic analysis of systems**
- **Draw on resources from those involved in vulnerability assessment, risk management, and network intrusion detection and incident response**
- **Resolve or terminate all case investigations**

Understand the law!

Understand:

- **Local city, county, state or province, and federal laws on computer-related crimes**
- **Legal processes and how to build a criminal case**
- **Corporate policy and limitations**

Criminal cases

A criminal case follows three stages:

- **Complaint**
  - **Someone files a complaint**
- **Investigation**
  - **A specialist investigates the complaint**
- **Prosecution**
  - **Prosecutor collects evidence and builds a case**

Corporate cases

A corporate case follows three stages:

- Complaint/policy violation
  - Someone files a complaint (Mary has installed a cool new software game and I am jealous)
  - A policy is violated (i.e. Joe visits an unauthorized website like monster.com)
- Investigation
  - A specialist investigates the complaint
- Management action
  - If in violation of a civil law, turn over employee to the feds
  - If not, terminate or discipline per company policy

Most of us are corporate forensics

- During private investigations, search for evidence to support allegations of abuse of a company or person's assets and, in some cases, criminal complaints
- Silver-platter doctrine: handing the results of private investigations over to the authorities because of indications of criminal activity
- Forensics investigators must maintain an impeccable reputation to protect credibility

Three levels of investigators

Levels of forensics vary based on:

- **Level 1 (street police officer/rent-a-cop)**
  - **Acquiring and seizing digital evidence**
- **Level 2 (detective/HR)**
  - **Managing high-tech investigations**
  - **Teaching the investigator what to ask for**
  - **Understanding computer terminology**
  - **What can and cannot be retrieved from digital evidence**
- **Level 3: (computer forensics expert/system admin)**
  - **Specialist training in retrieving digital evidence**

Key points

Maintaining objectivity

- **Sustain unbiased opinions of your cases**

Avoid making conclusions about the findings until all reasonable leads have been exhausted

Considered all the available facts

Ignore external biases to maintain the integrity of the fact-finding in all investigations

Keep the case confidential

Plan your investigation

Make sure you:

- **Prepare a forensics workstation**
- **Obtain the evidence from the secure container**
- **Make a forensic copy of the evidence**
- **Return the evidence to the secure container**
- **Process the copied evidence with computer forensics tools**

Document, document, document

An evidence custody form helps you document what has been done with the original evidence and its forensics copies (chain of custody)

There are two types:

- Single-evidence form
- Multi-evidence form

Example evidence form

Security Investigations

This form is to be used for one to ten pieces of evidence

Case No.:		Investigating Organization:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

	Description of evidence:	Vendor Name	Model No./Serial No.
Item #1			
Item #2			
Item #3			
Item #4			
Item #5			
Item #6			
Item #7			
Item #8			
Item #9			
Item #10			

Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	

Item #	Evidence Processed by	Disposition of Evidence	Date/Time
			Page __ of ___

Secure your evidence

- Use evidence bags to secure and catalog the evidence
- Use computer safe products
  - Antistatic bags
  - Antistatic pads
- Use well-padded containers
- Use evidence tape to seal all openings
  - Floppy disk or CD drives
  - Power supply electrical cord
- Write your initials on tape to prove that evidence has not been tampered
- Consider computer-specific temperature and humidity ranges

Understand data recovery

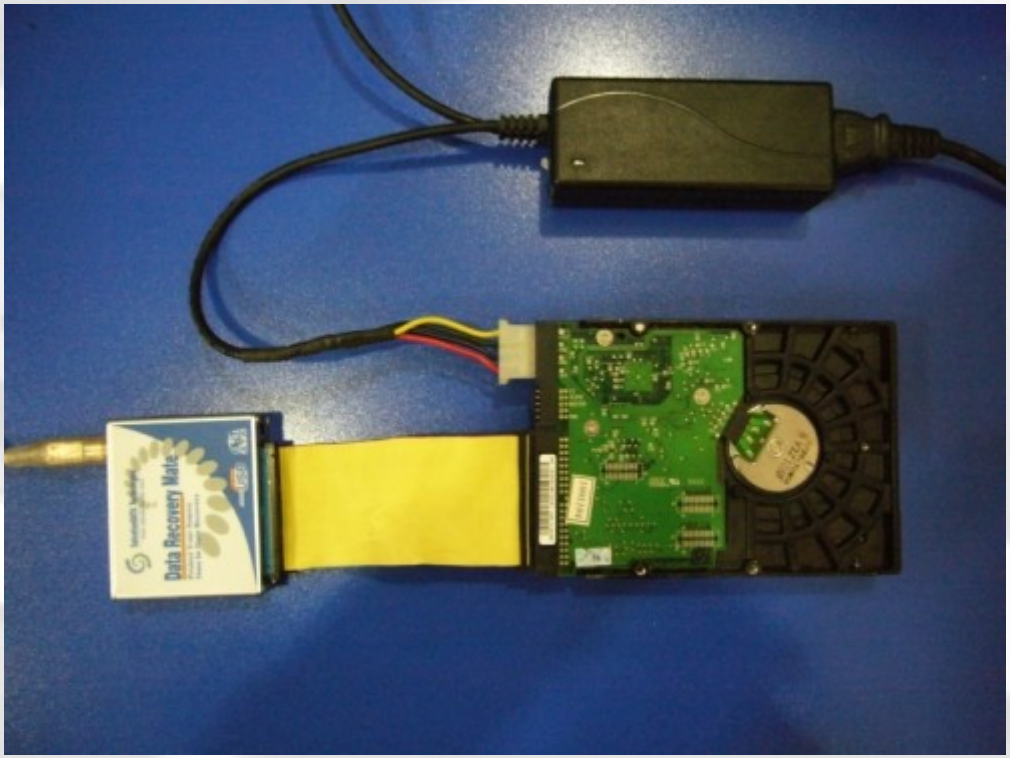
- Investigations are conducted on a computer forensics lab (or data-recovery lab)

- Computer forensics and data-recovery are related but different

- Computer forensics workstation
  - Specially configured personal computer

- To avoid altering the evidence, use:
  - Forensics boot floppy disk
  - Write-blockers devices

Write blocker … or linux!



Conducting an Investigation

Begin by copying the evidence using a variety of methods

- Recall that no single method retrieves all data
- The more methods you use, the better

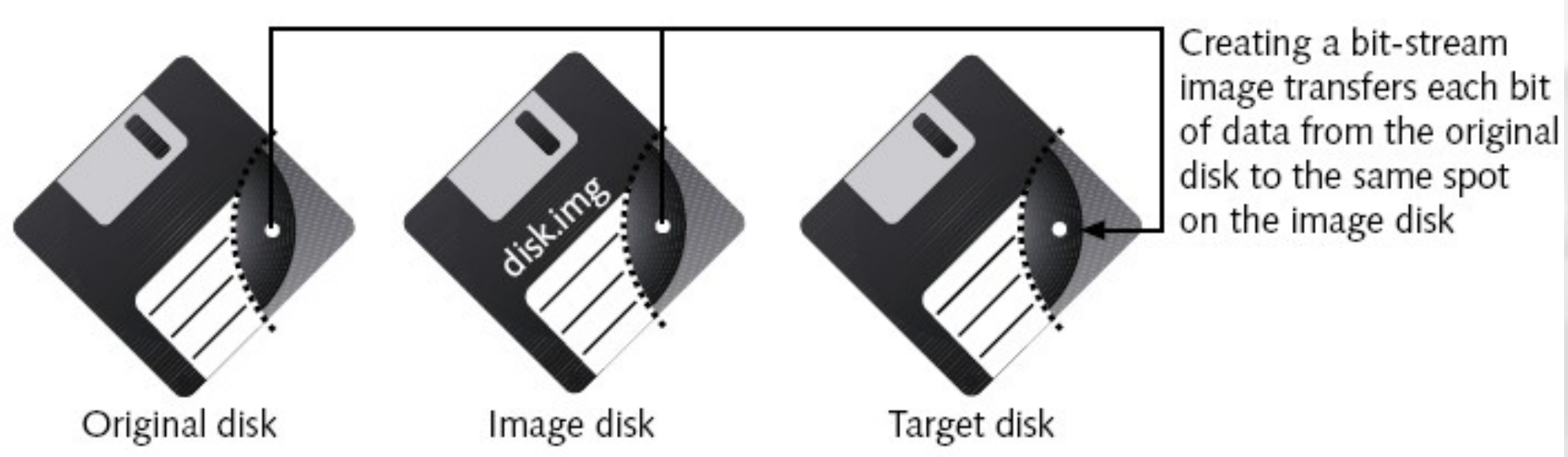
Gathering the Evidence

- Take all necessary measures to avoid damaging the evidence
  - Place the evidence in a secure container
- Complete the evidence custody form
- Transport the evidence to the computer forensics lab
- Create forensics copies (if possible)
- Secure evidence by locking the container

Understand bit-stream copies

- Bit-by-bit copy of the original storage medium
- Exact copy of the original disk
- Different from a simple backup copy
  - Backup software only copy known files
  - Backup software cannot copy deleted files or e-mail messages, or recover file fragments
- A bit-stream image file contains the bit-stream copy of all data on a disk or partition
- Preferable to copy the image file to a target disk that matches the original disk's manufacturer, size, and model

Understand bit-stream copies



Creating a bit-stream image with FTK Imager

- Start Forensic Toolkit (FTK) Imager by double-clicking the icon on your desktop
- Click File, Image Drive from the menu; insert floppy disk labeled “Domain Name working copy #2”
- In the dialog box that opens, click the A: drive to select a local drive, then click OK

- A wizard walks you through the steps
  - Accept all the defaults
  - Specify the destination folder
  - If necessary, create a folder called Forensics Files
  - Name the file Bootimage.1

Tools covered

- Forensic Toolkit 2.0
- FTK Imager Lite
- LiveView
- Libpff
- Pasco
- Rifiuti
- Vision
- Harlan Carvey Tools

Forensic Toolkit 2.0

- AFind is the only tool that lists files by their last access time without tampering the data
- FileStat is a quick dump of all file and security attributes
- HFind scans the disk for hidden files
- SFind scans the disk for hidden data streams

http://www.foundstone.com/us/resources/proddesc/forensictoolkit.htm

FTK Imager Lite

- Create images
- Perform live acquisitions
- Recover deleted USB data
- Use ProDiscover to make each live acquisition into a VMware image

http://www.accessdata.com/downloads.html

LiveView

- Java-based graphical forensics tool
- Creates a VMware virtual machine out of a raw (dd-style) disk image or physical disk
- All changes made to the disk are written to a separate file, the examiner can instantly revert all of his or her changes back to the original pristine state of the disk

http://liveview.sourceforge.net/

Libpff

- Pffexport exports the items stored in PAB, PST and OST (PFF) files
- pffinfo, shows information about PFF files.
- pffrecover, exports recovered items stored in PAB, PST and OST (PFF) file

http://sourceforge.net/projects/libpff/

Pasco

- Examine the contents of IE cache
- Parse the information in index.dat
- Export to spreadsheet

http://www.foundstone.com/us/resources/proddesc/pasco.htm/

Rifiuti v1.0

- Examine the contents of the INFO2 file in the Recycle Bin
- Output the results in a field delimited manner

http://www.foundstone.com/us/resources/proddesc/rifiuti.htm

Vision 1.0

- Shows all of the open TCP and UDP ports on a machine
- Displays the service that is active on each port
- Interrogate ports and identify potential "Trojan" services
- List applications, services, etc running

http://www.foundstone.com/us/resources/proddesc/vision.htm

Harlan Carvey

- Registry guru
- Creator of must-have scripts
- Reverse Engineering
- Rootkit analysis
- In-depth registry analysis

http://www.amazon.com/Windows-Forensic-Analysis-Including-Toolkit/

Other resources...

Portable applications

http://www.e-evidence.info/other.html

Cell Phone Fornesics

http://www.bitpim.org/

Review

- Review corporate policy and gain management approval
- Create an initial low-cost lab & read, read, read
- Maintain objectivity and professionalism
- Follow the proper investigation process (document!)
- Provide a detailed log and your guidance to managment

robert.baldi at gmail.com