Introduction To Computer Forensics

Notices

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM19-0488

What is Forensics?

Main Entry: **[1]fo·ren·sic**

Pronunciation: \fə-ˈren(t)-sik, -ˈren-zik\

Function: *adjective*

Etymology: Latin *forensis* public, forensic, from *forum* forum

Date: 1659

1 : belonging to, used in, or suitable to courts of judicature or to public discussion and debate
2 : argumentative, rhetorical
3 : relating to or dealing with the application of scientific knowledge to legal problems <*forensic* medicine> <*forensic* science> <*forensic* pathologist> <*forensic* experts>

— **fo·ren·si·cal·ly** \-si-k(ə-)lē, -zi-\ *adverb*

Source: http://www.merriam-webster.com/dictionary/forensic

What is *Computer* Forensics?

The discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible in a court of law.

AKA Cyber Forensics

Source: US-CERT

What is the Goal of Computer Forensics?

Identify, collect, preserve, and analyze data in a way that preserves the integrity of the evidence collected so it can be used effectively in a legal setting.

Source: US-CERT

The Word *Forensics* Means Something

Forensics is an overworked word

Forensics implies

- Formal methods and procedures
- Well-understood and accepted tools
- Legal setting is the forum for the results

Wrong: “forensics analysis”; right: “incident analysis”

Wrong: “network forensics”; right: “network analysis”

Consider the phrase “forensically sound manner”, as in “incident analysis in a forensically sound manner”

Unfortunately, “forensics *blah*” is in the vernacular

What Is This Module?

An overview

Gives the 30,000 foot view

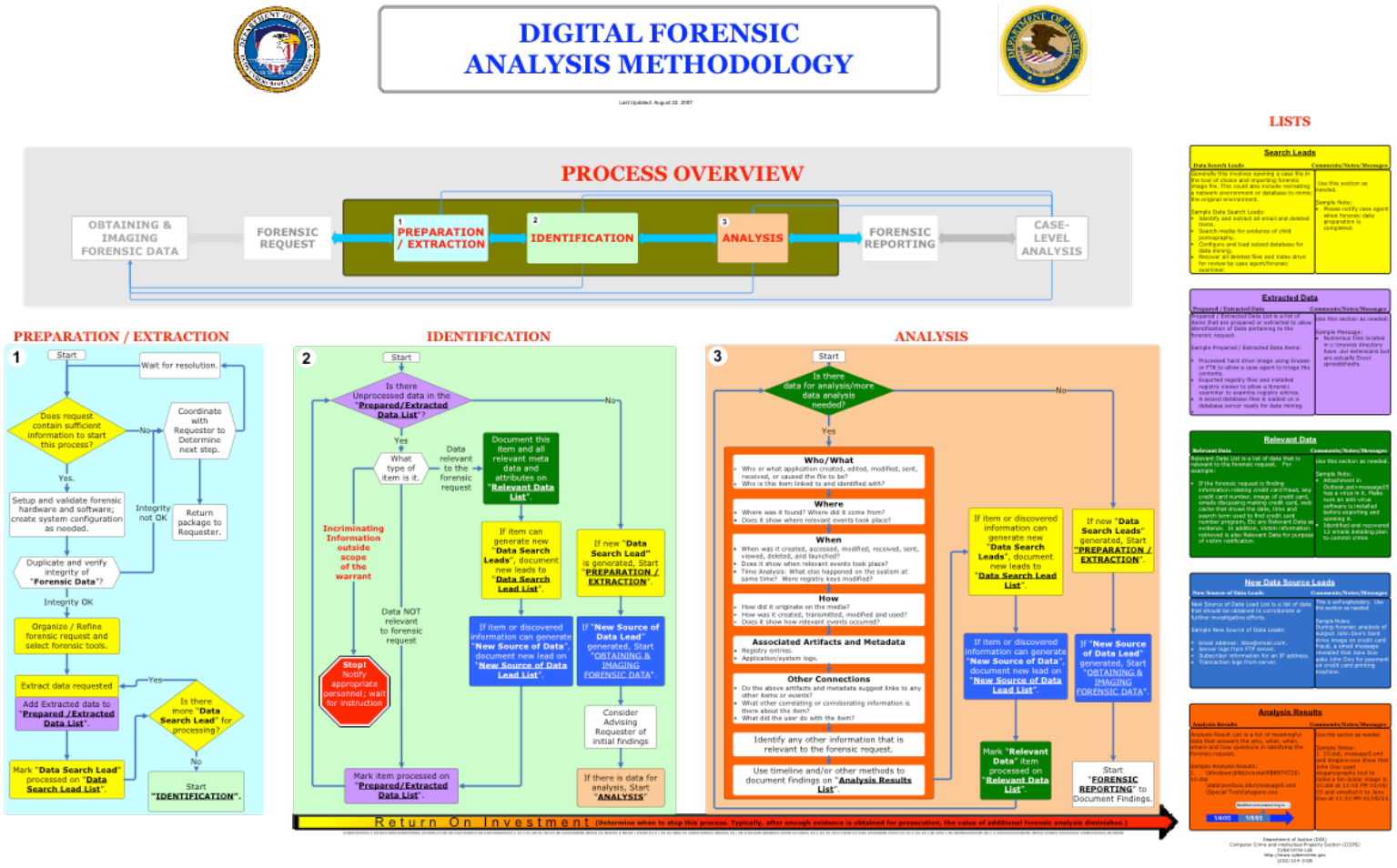
Minutiae left out on purpose

You'll get the general idea

You'll see a general process

The devil *is* in the details

Digital Forensic Analysis Process



Key Point #1 – Plan for others to reproduce your efforts

Document everything – *everything!*

- Keep a journal
- Date and time stamp entries
- Describe activity
- Describe what you found, called *findings*
- Unless you are an expert witness, don't draw conclusions

Before Obtaining and Imaging Forensic Data - 1

Need authority to obtain/image forensic data

This means:

- Search warrants
- Policies
- US Government Laws
  - Electronic Communications Privacy Act
  - Wiretap Act
  - Pen/Trap Statute

Key is to know what you're looking for and that you are allowed to be looking for it – be very careful!

Fishing may not be allowed

Before Obtaining and Imaging Forensic Data - 2

Prepare imaging equipment

- Acquire and wipe disks
- Acquire connectors, power supplies
- Acquire and test imaging appliances
- Acquire and test imaging software
- Extras
  - Power cords, networking cables, internet access
  - Note taking paraphernalia

Obtaining and Imaging Data - 1

Goal: image what could be written by suspects, during the period of importance

What is that list?

- Media - obvious
  - Disks, USB flash drives, CDs/DVDs
- Media – less obvious
  - DVR/TiVo
  - Printers
  - Disguised devices – broach, hair clip, articles of clothing
  - Unrelated devices – Videos, cell phones, etc.
  - ???

Obtaining and Imaging Data - 2

Goal: image efficiently

Questions

1. How much disk space exists in the organization?
2. How long would it take to image all of it?
3. Can you be more selective in what is imaged, yet image all that is writable by the suspect?

Key Point #2 – Make an imaging plan

Once on site, make an imaging plan

Take into account:

- Speed of networks
- Speed of connections (USB, Firewire, etc)
- Speed of source and target hosts
- Size of disks to image

Plan should contain:

- Order of file systems to image
- Method (network, local connection, powered down and removed, etc)
- Approximate size
- Checksum of source (if possible) and target once imaged

Obtaining and Imaging Data - 3

Goal: capture all identified data for analysis

How to image

- Media should be “at rest”
  - Computer system off
  - Media removed from suspect computer
  - Write blockers
- Useful information may be stored on media that is not part of a file (free space, slack space, “unused” partitions, etc)
- Use bit-for-bit copy (UNIX/Linux **dd** command or equivalent) to capture entire media (**dc3dd**, **dcfldd**)
- Never (rarely?) use tools that access files directly (**tar**, **cpio**, etc)
- Consider media with “errors”

Obtaining and Imaging Data - 4

Goal: perform imaging

Equipment needed:

- Media to image to
- Hardware and software to perform imaging process – includes write blockers for original disks
- Hardware and software to verify images
- Lockable containers to transport images (chain of custody)
- Note taking materials
- Time, potentially lots of time

Obtaining and Imaging Data - 5

Goal: verify imaged data

Checksums: MD5, SHA1, etc.

Record in journal

Problem: If source disk has errors, checksums will *never* match – inadmissible?

Counter Forensics Tip #1

Situation: media “at rest”

Disconnected from computer

If media encrypted, decrypted version lost when at rest

Solution: image live, decrypted disk

How do you know it is encrypted?

Solution: CryptHunter!

Acquisition-time screening utility for Windows systems

Detects

- Mounted virtual volumes
- Active, software-based full-disk encryption

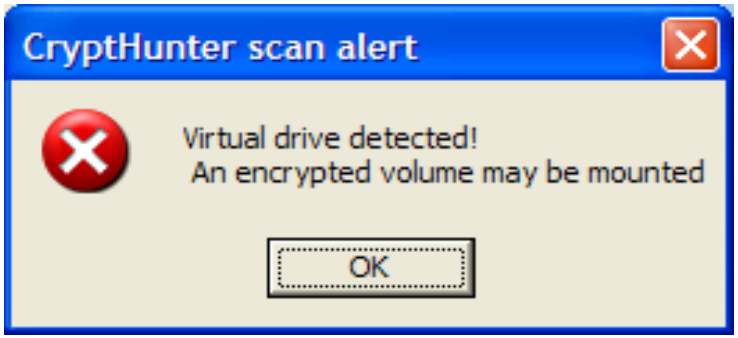
Tiny footprint – designed to minimize use of memory and system resources

Standalone software that runs from external media for rapid screening

See http://www.cert.org/forensics/tools.html if you are Law Enforcement to request tools.

Green light / Red light approach

```
CryptHunter v.0.3 started.
Commencing hunt for active encryption on system.

Scanning for Full Disk Encryption ...
Non-standard boot code found on device \\.\physicaldrive0.
FDE scan complete. Proceeding with second detection phase.

Scanning for encrypted containers mounted as drives ...
Analyzing logical drive at: C:\

CryptHunter scan complete.
Summary of results:

      -- Full Disk Encryption --
CryptHunter found no recognized Full Disk Encryption
signatures.
However, a non-standard boot sector was reported. This may
be
due to a rescue partition scheme (e.g. some Dell and IBM
systems), a custom dual-boot system or other common
reasons.
However, it might indicate the presence of a Full Disk
Encryption
package that CryptHunter doesn't recognize. ...
This may be worth further investigation before powering down
system.

      -- Virtual Disk Encryption --
No instances of mounted encrypted containers found.

Hit <enter> when you are ready to close this window.
```



Alert boxes report results of scan

CryptHunter can differentiate between and identify full-disk encryption software packages

Warns only of ACTIVE encryption

CryptHunter – Applications Covered

Full Disk Encryption
✓ DriveCrypt Plus
✓ SafeGuard Easy
✓ PGP Whole Disk encryption
✓ CompuSec
✓ SecureDoc Enterprise
✓ SafeBoot Device Encryption
✓ PointSec Full Disk Encryption ✓ Vista Bit Locker

Virtual Disk Encryption
✓ **BestCrypt**
✓ **Cryptainer LE**
✓ **CryptoExpert 2006**
✓ **SafeHouse Drive Encryption**
✓ **Sentry 2020**
✓ **Cross Crypt / FileDisk**
✓ **CleverCrypt**
✓ **DriveCrypt**
✓ **CryptArchiver**
✓ **DeKart Private Disk**
✓ **SafeGuard Private Disk**
✓ **TrueCrypt**
✓ **CyProtect Drive Encryption**
✓ **SafeBoot's Vdisk volume encryption**
✓ **PGPDisk virtual disks**
✓ **Cryptic Disk**

Counter Forensics Tip #2

What if screensaver/screenlocker enabled and running?

If computer has firewire:

- Firewire allows direct access to computer memory
- Techniques to rewrite computer memory
- Start *cmd.exe* application
- Bypasses screensaver/screenlocker
- Mouse “jiggler” to keep screen from locking again

Counter Forensics Tip #3

There's important information in computer memory

Passwords, passphrases, encryption/decryption keys, etc.

Image memory too – **win32dd** and **winen** from Helix, **mdd** from ManTech

Process with Volatility Framework - https://www.volatilesystems.com/default/volatility/

Obtaining and Imaging Data - 6

Before leaving site, check that images are “usable”

- Readable
- Understandable
- Able to be further analyzed

Once you leave, you may not be able to get more or better information

Solution: CERT Linux Forensics Appliance

VMware-based Fedora Acquisition and Analysis platform

Analysis tools

- Volatility
- The Sleuthkit plus Autopsy
- Many command-line acquisition and analysis tools

Run appliance and check imaged media and memory on-site

See http://www.cert.org/forensics/tools/ for appliance and Linux Tools Repository

Summary – Obtaining and Imaging

Before on-site

- Authority
- Equipment (disks, connectors, imaging)

On-site

- Imaging plan
- Image
- Testing/verifying images

Leaving site

- Secure transport/storage

Analysis - 1

Goal: search for evidence cited in original forensic request

Key point: knowing the imaged device

- Computer System
  - Disk specifics
    - Bad blocks, host protected area, ???
  - File system specifics (FAT, NTFS, ext2, ext3, etc)
    - Arrangement, file allocation/deletion, free space, slack space
  - Operating system specifics
    - Where information resides
      - Configuration information
      - Application-specific data (email, browser history, chat logs)
- Other devices
  - Cell phones, PDAs, DVR/Tivo, etc

Analysis - 2

Goal: Analyze imaged information

Analysis platform

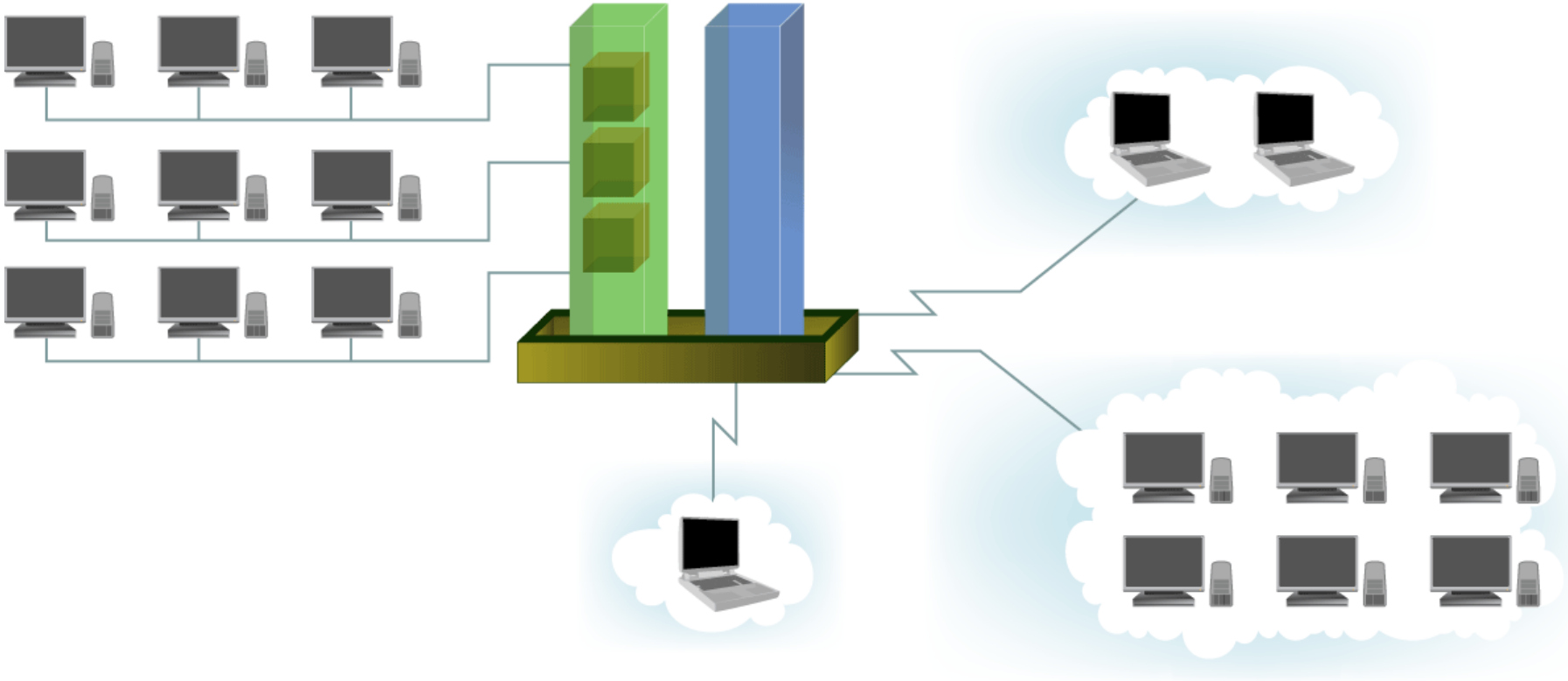
- Lots and lots of disk space
  - Wiped – cross-case contamination
- Processing power
  - Analyze large number of files
  - Brute force decryption

Old method

- One analysis platform/per analyst
- Operations tend to be serial
- One case at a time

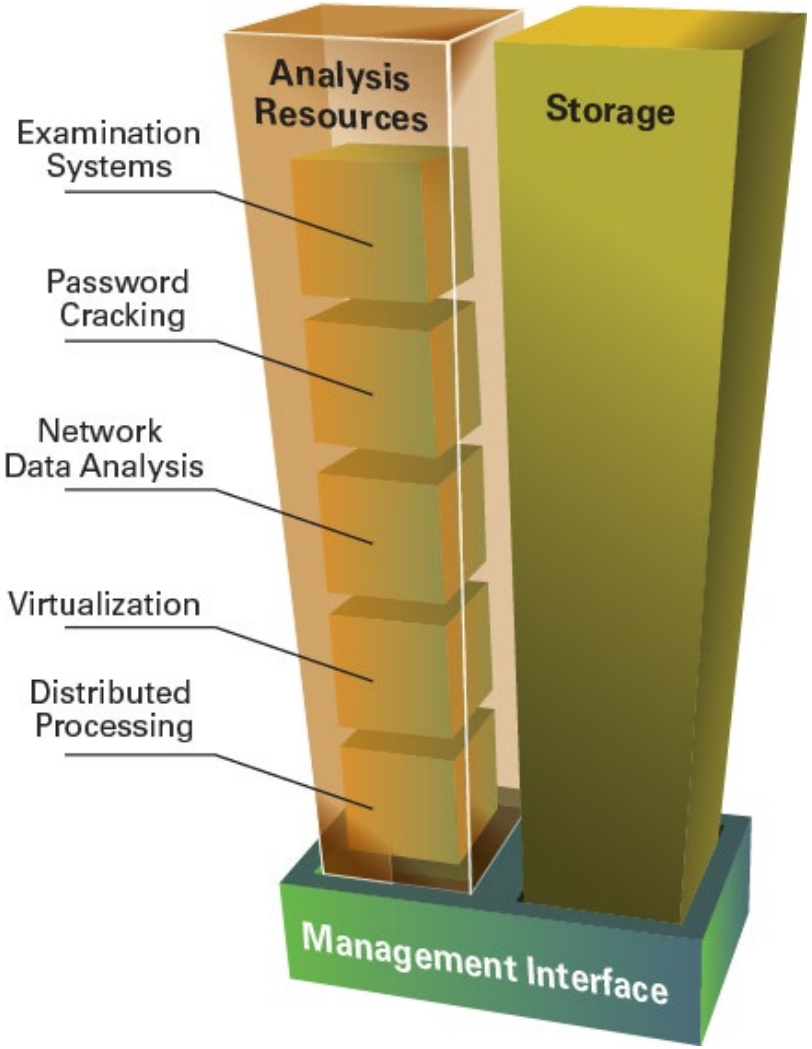
A New Approach: C-CAP

Clustered-Computing Analysis Platform



Clustered-Computing Analysis Platform - 1

CERT's Clustered-Computing Analysis Platform (C-CAP) is a state-of-the-art forensics analysis environment that provides a complete suite of tools for host-based and network investigations. The environment maximizes the application of specialized computing resources to the forensic and incident response missions. Analysts and investigators enjoy flexible, secure access to high-performance systems, increasing productivity and enabling distributed collaboration.



Clustered-Computing Analysis Platform - 2

Scalable Resources

Allows the addition of functionality, storage, and processing power to meet changing mission demands.

Collaborative Environment

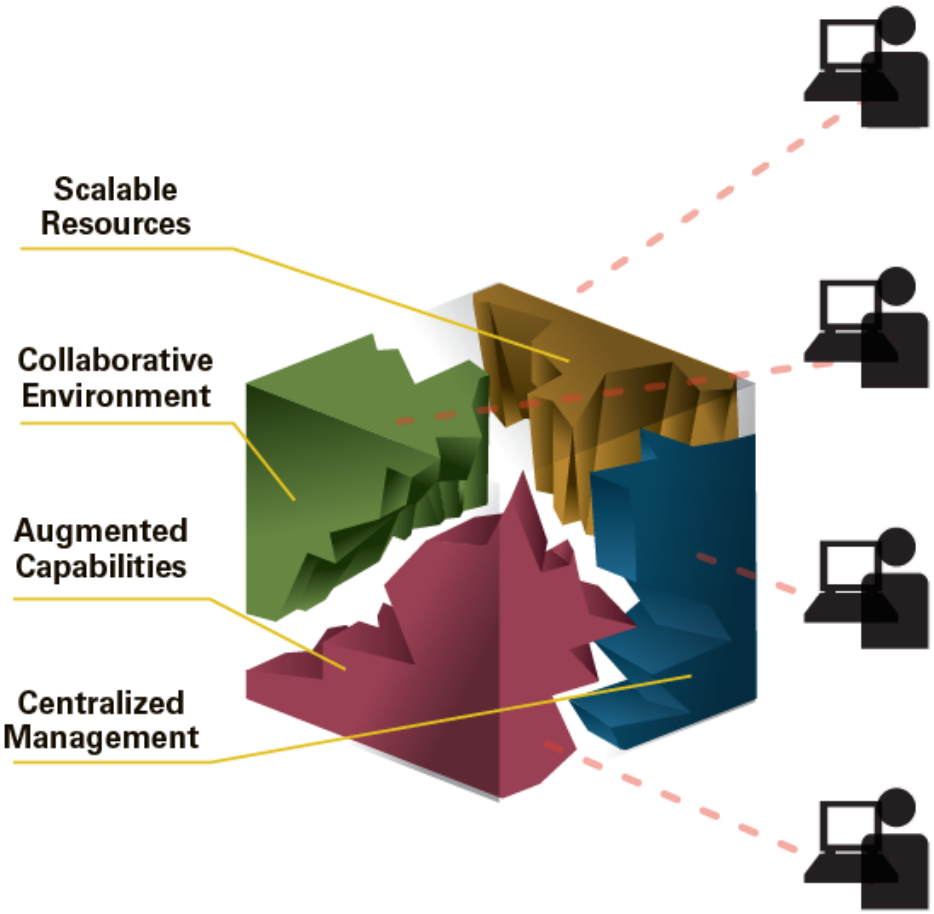
Permits multiple analysts to focus on the same or related events in concurrent examinations. Enables organizations to coordinate geographically dispersed analysts.

Centralized Management

Provides rapid allocation of platform resources to tasks or analysts. Ensures resources can be flexibly and securely reassigned on demand.

Augmented Capabilities

Provides integrated access to a comprehensive array of analytical tools and resources.



Analysis - 3

Goal: Do analysis

Steps

- Image captured images to analysis platform
- Store captured images under lock and key
- Begin analysis

Analysis - 4

Goal: Construct a time line of events

What is a timeline?

- An ordered list of changes on the device
- What was changed and when
- If file system, use file system metadata
  - Modified, accessed, created/changed (MAC)
  - Only last MAC time saved – intermediate changes lost
  - Can zero in on a specific period
  - File system independent (NTFS, FAT, ext{2,3})

Analysis - 5

Goal: Find what you're looking for

Specific file types

- Email, images, executables, Office, etc

Files with specific strings

Files around an event

- Based on timeline
- May be deleted

Counter Forensics Tip #4

There are commercial tools that hinder forensics analysis

Designed to eliminate specific records and files but leave system otherwise functional

- Overwrite deleted data to thwart recovery
- Cope with system files, like the Registry

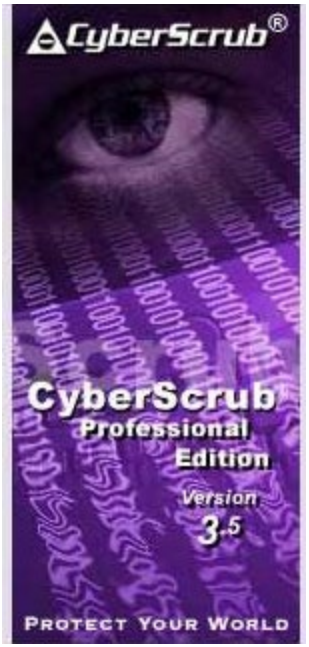
Aimed at users that may not be proficient

More than twenty commercial software packages

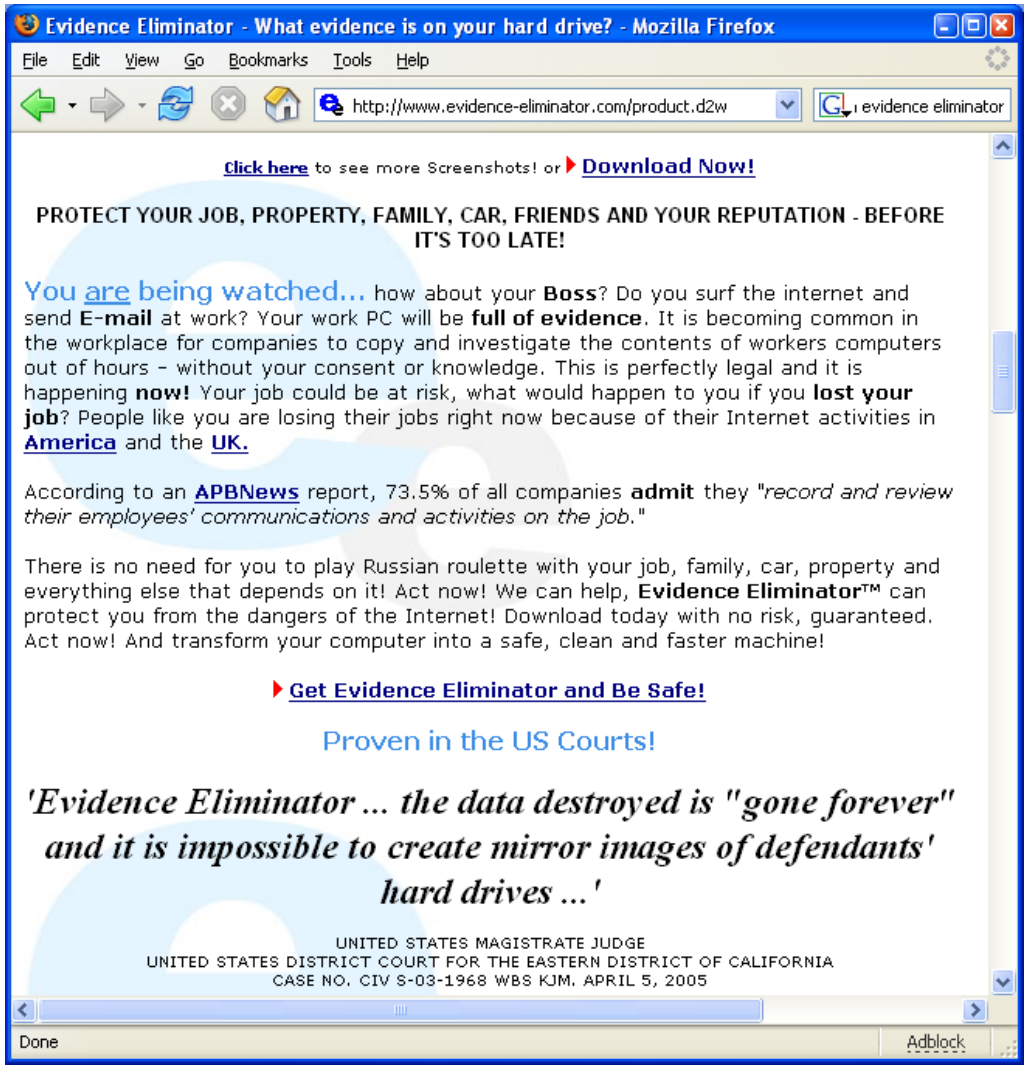
Who Produces Them?

The vendor marketplace:

- Competitive
- Wide range of enterprises
  - Unincorporated entities
  - Well-financed companies
- Marketed as
  - Safeguarding privacy
  - Protecting corporate data
  - Helping avoid consequences



Example: Evidence Eliminator



Aperio

Forensic utility allows examiners to screen for the use of counter-forensic tools

Uses Linux-NTFS libraries to address MFT, file system structures

Configuration file specifies elements of tool signatures:

```
# Sample regex specification file for Aperio
# This file specifies terms, where applicable, for
# setting up Aperio searches. Fields are white-space separated.
#
#Name                Version MFT Name Pattern          Mod Time      File Length     Data Pattern
Evidence Eliminator         5.508  [0-9]{6,10}[a-z]{210,245}    NA              0            NA
```

Analysis - 6

"Run" the imaged windows computer system

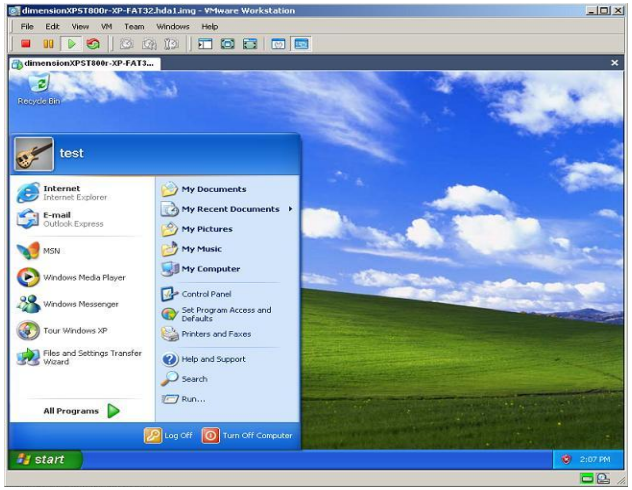
See what the imaged computer system user would see

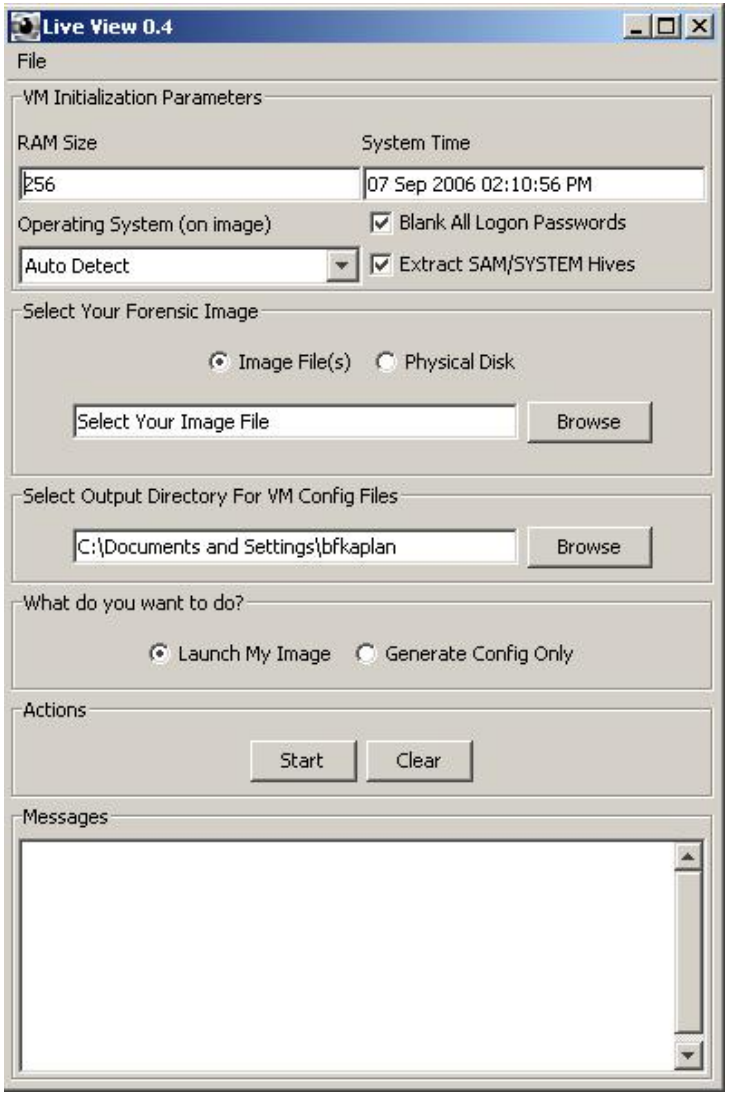
Speeds analysis

Live View

Live View

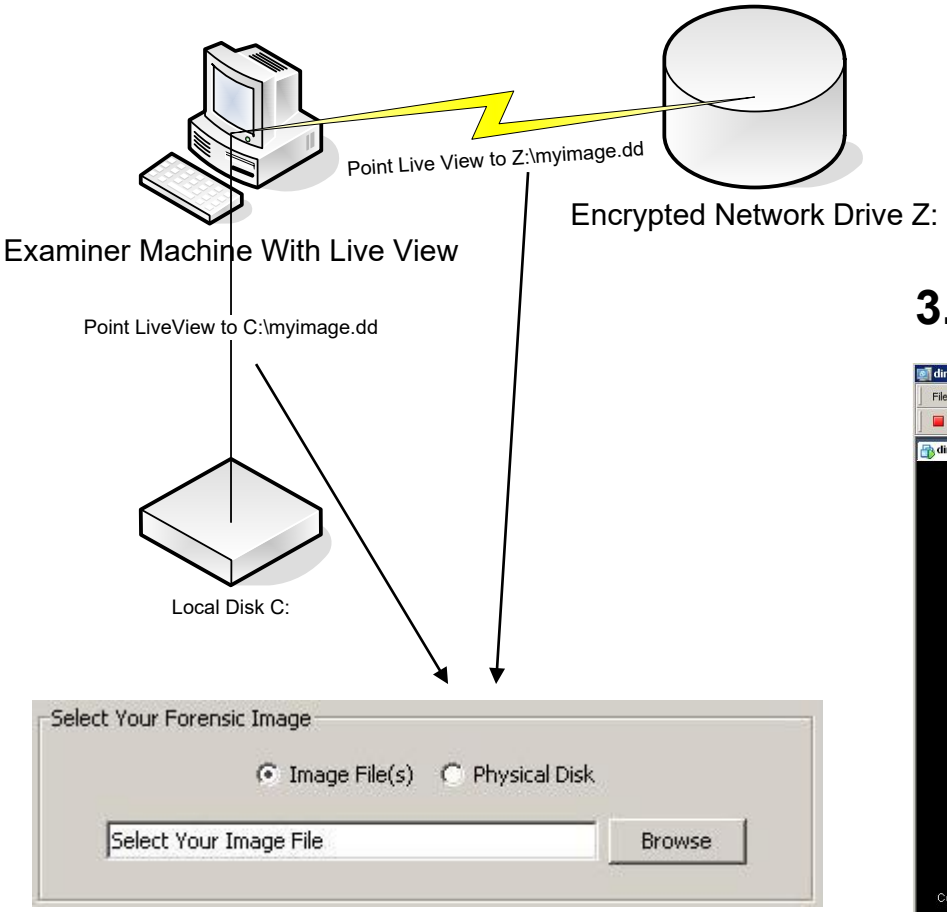
- Boot dd image, EnCase image, or a physical device as a VM with a few clicks
- No lengthy disk restoration required
- Image is not altered in any way (can even be read-only or hardware write-blocked)
- Automates troubleshooting process of preparing image to boot on new hardware
- LE version clears passwords and exports SYSTEM / SAM hives





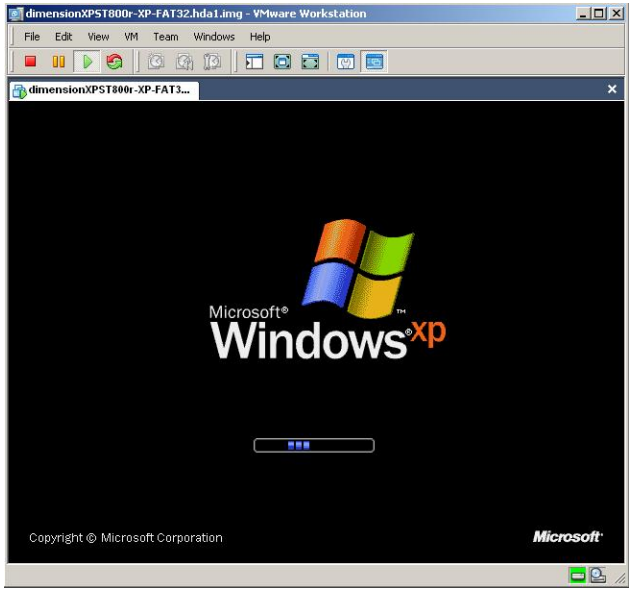
It's Easy As "1–2–3"

1. Select Your Image or Device



2. Set Some Input Parameters

3. Click Start



Live View Supports

Bit-For-Bit Forensic Images

- Windows (2003, XP, 2K, NT, Me, 98)
- Linux (Limited)

Virtual Machines (on examination box)

- VMware Server 1.0 (Free)
- VMware Workstation 5.5 +

Analysis - 7

Analysis is an iterative process

- Finding one thing leads to …
- Another thing, which leads to …
- Another thing, which leads to …
- And so on, and so on

Keep track of and document each finding

Findings should be *repeatable* by others

Analysis - 8

Key to analysis is knowing the specifics of the item(s) being analyzed

For example:

- Computer systems
  - File system operations
    - File deletion, creation, meta information
  - Where applications store information
  - Form of stored information
  - What information means

The Cyber Forensics Analyst knows these things about computer systems (and perhaps cell phones, PDAs, networks, etc.)

Summary - Analysis

Search for evidence cited in original forensic request

Analyze imaged information

- What are you looking for?
- How will you recognize it when you find it?
- Where might you find it?
- What does it mean once you've found it?

Construct a time line of findings

- How did you find what you found (repeatability)?

Tools

- CryptHunter, Aperio, Forensic Appliance, Live View, C-CAP
- What for counter forensics tools

TAKE NOTES WHILE DOING ANALYSIS!

Reporting - 1

Report writing goals:

- Inform
- Provide permanent record
- Provide record of analysis
- Professional
- No slang, prejudice, bias, or unsupported opinions

Report gives findings

Reporting is defined as "An accurate, fair, complete, concise, clear, and neatly written account of an event or series of events presented in a logical format which will accurately communicate to the reader."

Reporting - 2

General Rules:

- Written in past tense
- Written in third person
- Written immediately after concluding analysis
- Written from notes, not memory
- Unbiased and impartial
- Clear – person who is not knowledgeable can understand
- Establish a time line

Reporting - 3

Recipe:

On date at approximately time who? action verb (observed, copied, collected, analyzed) what where with whom and found findings.

Example:

On August 5th, 2010, at approximately 3:00 PM, Tom Smith observed Henry Smith opening a FedEx package at 210 North First Street, Pittsburgh, PA, sent from Chicago, IL and found a request for assistance in analyzing the contents of this package which consisted of a 1Tb hard disk drive, serial number 12345.

Reporting – 4

References

- *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* (http://www.ncjrs.gov/pdffiles1/nij/199408.pdf)
- *SANS 508 – System Forensics, Investigation, and Response*

Summary – Report Writing

Report findings, findings, findings!

Past tense

Establish timeline

Concise, clear, and concise

Miscellaneous - Chain of Custody

All evidence must be accounted for at all times

Evidence has not been altered

- Digital evidence – checksums

Party offering evidence has burden of proof as to its veracity

Materials

- Evidence handling forms
- Evidence containers
- Safes/locked cabinets
- Logs

Miscellaneous - Data Preservation

Secure location

- Safe
- Locked cabinet

Well defined and understood storage procedures

Records showing that procedures were followed

Evidence custodian – who is this in your world?

Miscellaneous - Laws

Real-time interception vs. Stored communications

Content vs. headers and logs

US Laws

- Electronic Communications Privacy Act – stored communications
- Wiretap Act – Real-time contents
- Pen/Trap Statute – Real-time headers and logs

Decide what you need to capture then look for applicable laws

Bottom line – work with your legal folks and Law Enforcement agencies *before* acquisition starts

Summary

Forensics has a clearly defined meaning – use it correctly

There is a well-defined process

- Preparation
  - Reconnaissance, equipment procurement and configuration, legal
- Identification (on-site)
  - Reconnaissance, imaging plan, imaging, chain-of-custody, note taking
- Analysis
  - Tools, note taking, chain-of-custody
- Report writing
  - Document findings
- Follow-on activities
  - Evidence preservation, chain-of-custody, testifying(!)

There are laws that must be followed or your work may be invalidated.