Ungraded Pre-Lecture Quiz

- In a password-file stealing cybercrime, what's the role of the **extracted password file**?
- Suppose you want to create several VMs that:
  - Can talk to each other on a network segment;
  - Can access the Internet, e.g. to install software packages;
  - Do not need to talk to your host OS.

  What **networking mode in VirtualBox** should you select?

IFS4102: Digital Forensics

Lecture 2: Digital Evidence Handling, Forensics Lab & Static Acquisition

Outline

- Digital evidence handling
- Evidence acquisition
- Digital forensics lab and tools
- Static acquisition
- Lab 2 exercises
- Offline case discussion

Digital Evidence Handling

Digital Evidence & Characteristics

- ***Digital evidence*** (in our module):
  a **digital object** that contains **reliable information** that either **supports or refutes** a hypothesis of an incident or crime

- **Characteristics** of digital evidence:
  - An **abstraction** of some **digital object** or **event**
  - Easily **copied**
  - Easily **modified**
  - Easily **destroyed**
  - **Volatile**

Type of Digital Evidence in an Investigation

- Two types of digital evidence w.r.t. a particular **hypothesis**
- **Inculpatory** evidence:
  - Tends to indicate that the suspect is **guilty** of the alleged crime, or had a criminal intent
  - I.e. **support/"prove"*** the allegation hypothesis
- **Exculpatory** evidence:
  - Tends to indicate that the suspect is **innocent** of the alleged crime
  - I.e. **refute/"disprove"*** the allegation hypothesis or fails to support it

* Note: We will discuss *levels of certainty* later in the module

Digital Evidence Requirements

- Digital evidence needs to be ***admissible*** in a court of law
- **Admissibility requirements**:
  - **Relevant**: it has a direct bearing on the incidence in question
  - **Authentic/integral**: it hasn't been tampered with
  - ***Forensically sound***: collected/acquired and stored in a forensically-sound manner
  - Based on the **best available evidence**
- ***Forensically sound***:
  the operation adheres to **established** digital forensics **principles**, **standards** and **processes**

Caution/Issue: Evidence Dynamics

- In handling digital evidence, be mindful of **evidence dynamics**
- ***Evidence dynamics***:
  any **influence** that **changes**, **relocates**, **obscures**, or **obliterates** evidence, regardless of intent, between the time evidence is transferred and the time the case is resolved
- Can be **caused by**:
  - Offenders
  - Victims
  - **Digital evidence first responders**
  - **Digital evidence examiners/specialists**
  - **Anyone else who had access to digital evidence**

Examples of Evidence Dynamics

- A **first responder** did **not** follow SOP and failed to collect important evidence
- **Digital evidence examiners** installed a **pirated version of a forensic tool** on the compromised server
- On an evidential computer, a **system admin** attempted to **recover deleted files** from a hard drive **by installing software** or **saving recovered files** onto the *same* drive
- [IR:] Responding to a computer intrusion, a **system admin intentionally deleted** an account that the intruder had created, and attempted to preserve digital evidence using the **standard backup** facility (e.g. cp, tar, cpio)

Yet, Supportive Aspect of Digital Evidence

- Digital evidence can be **duplicated *exactly***:
  a **copy** can be examined as if it were the original
- It is very easy to **determine** if digital evidence
  has been **modified** or **tampered with**:
  by comparing it with an original copy using the right tools
- Digital evidence can be **resistant to deletion**:
  even when a file is "deleted" or a hard drive is formatted,
  digital evidence could still be **recovered**
- When criminals attempt to destroy digital evidence,
  copies & associated remnants can remain in places
  that they were not aware of

Digital Forensic Investigation's Steps

Review

- ***Most common steps*** in conducting a digital investigation (Casey, 2011):
  - **Preparation**: Generating a plan of action to conduct an effective digital investigation, and obtaining supporting resources and materials
  - **Identification**: Finding potential sources of digital evidence (at a crime scene, within an organization, on the Internet)
  - **Preservation**: Preventing changes of digital evidence at the crime site
  - **Collection/acquisition**: Collecting evidence data
  - **Examination & analysis**: Searching for and interpreting trace evidence in acquired evidence data
  - **Presentation**: Reporting of findings

Review

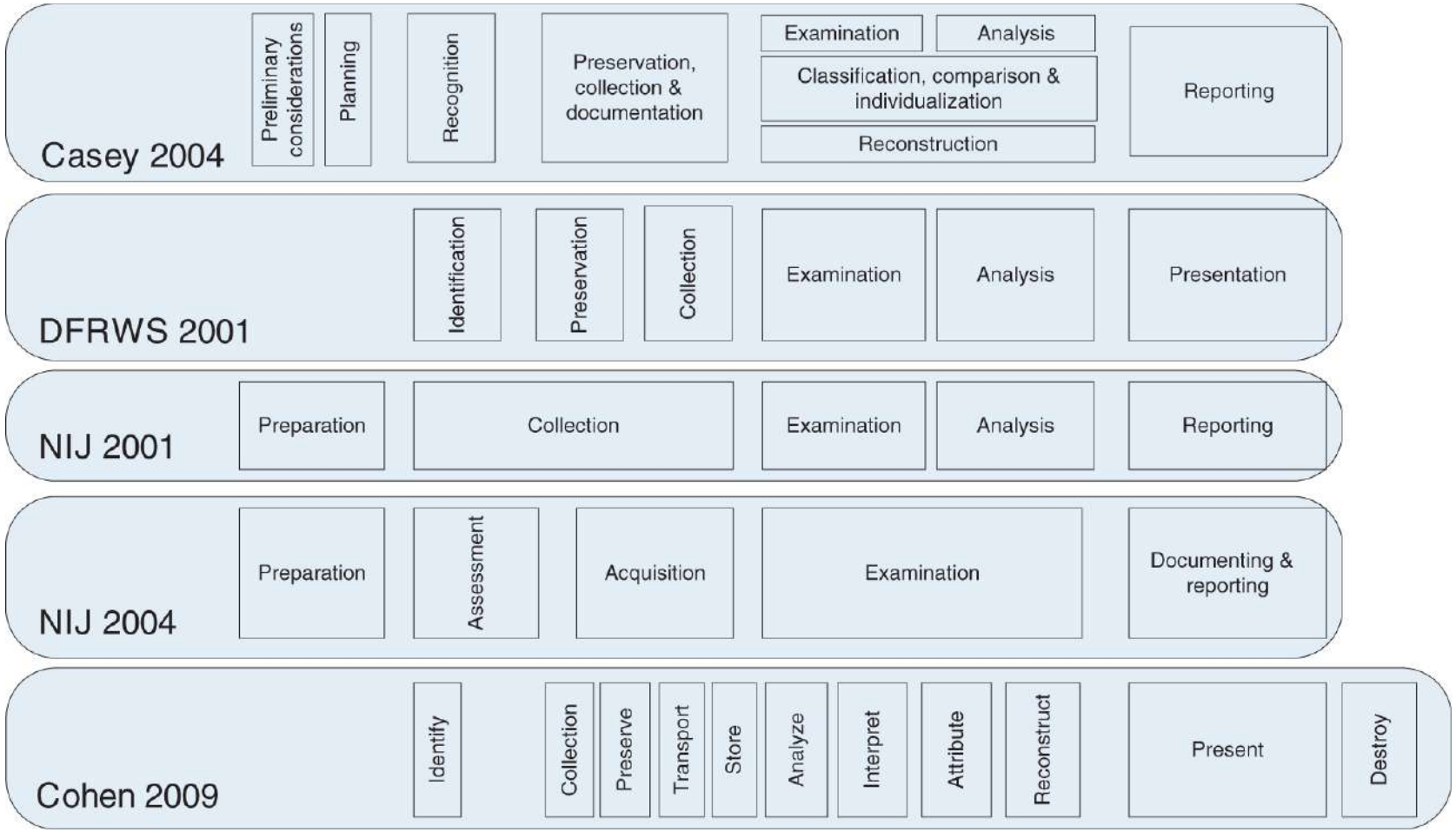


FIGURE 6.1 A comparison of terminology related to digital investigation process models.

Proper Digital Evidence Handling

- Goal of ***proper*** **handling**:
  - To present evidence that is **admissible** to the court of law
- Required **procedure** during the investigation steps:
  - Sufficient preparation, good identification, valid preservation, valid acquisition, valid examination & analysis, valid presentation
- **Applicable guidelines**:
  - Standard/best-practice/widely-accepted methodology and procedures
  - Examples:
    - **Scientific Working Group on Digital Evidence (SWGDE)** https://www.swgde.org/, which act as the U.S representative of the International Organization Computer Evidence (IOCE)
    - The UK **Association of Chief Police Officers**, *"ACPO Good Practice Guide"*, https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

Preparation: For Evidence Search and Seizure

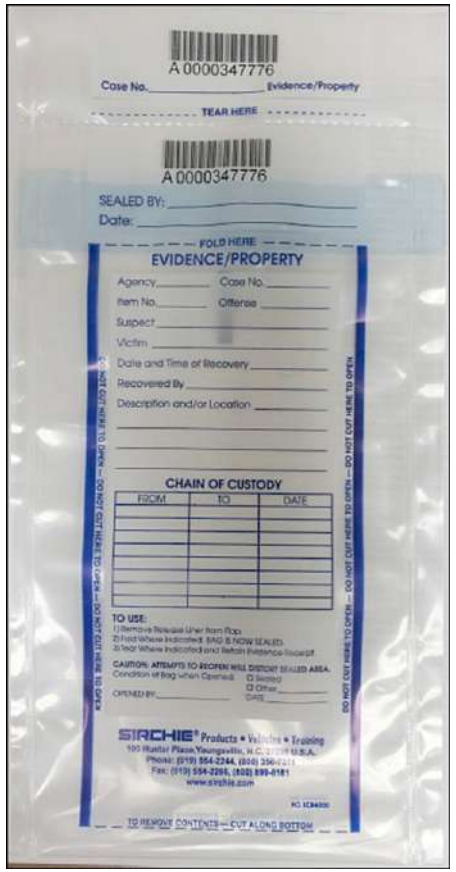
- The **Fourth Amendment** to the U.S. Constitution:
  - Protects everyone's right to be secure in their person, residence, and property from search and seizure
  - Basically **restricts unreasonable search and seizure**
- ***Search warrant*** is thus required:
  - In a criminal case: can be based on an affidavit given a probable cause
- Reference on "*Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*": https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf

Identification & Preservation: General Handling Procedures

- **Identification**:
  - **Identify** relevant pieces of evidence
  - **Tag** them
- **Preservation**:
  - During the seizure, also **bag** them: thus "**bag-and-tag**" all evidence
  - Use **anti-static bags** if needed
  - The evidence is stored in a tamper-proof manner:
    put mobile devices inside **signal-blocking** bags (*Why??*)
  - In general, affect evidence data as little as possible

Acquiring Evidence in a Computer Forensics Lab (cont.)

Evidence Bags



Signal-Blocking Bag

https://www.idstronghold.com/

Collection/Acquisition: General Handling Procedures

- **Collection:**
  - **Document/record** evidence origin
  - Keep track of ***chain-of-custody*** (continuity-of-possession), which accounts for **who** did **what** on the evidence **where** and **when** until that object is entered into evidence in the courtroom
  - Sample chain-of-custody form: http://www.nist.gov/oles/forensics/upload/Sample-Chain-of-Custody-Form.docx
- **Acquisition**:
  - Valid evidence **acquisition**: do not alter the original evidence! *How??*
  - Create **two forensic duplicates** whenever possible, and **validate** the duplication integrity

Sample Chain-of-Custody Form

Property Record Number: _____

Anywhere Police Department

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: _____ Offense: _____
Submitting Officer: (Name/ID#) _____
Victim: _____
Suspect: _____
Date/Time Seized: _____Location of Seizure: _____

Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)

Chain of Custody				
Item #	**Date/Time**	**Released by** (Signature & ID#)	**Received by** (Signature & ID#)	**Comments/Location**

APD_Form_#PE003_v.1 (12/2012) Page 1 of 2 pages (See back)

EVIDENCE CHAIN-OF-CUSTODY TRACKING FORM
(Continued)

Chain of Custody				
Item #	**Date/Time**	**Released by** (Signature & ID#)	**Received by** (Signature & ID#)	**Comments/Location**

Final Disposal Authority

Authorization for Disposal

Item(s) #: _____ on this document pertaining to (suspect): _____
is(are) no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method)
☐ Return to Owner ☐ Auction/Destroy/Divert
Name & ID# of Authorizing Officer: _____ Signature: _____Date: _____

Witness to Destruction of Evidence

Item(s) #: _____ on this document were destroyed by Evidence Custodian _____ID#:_____
in my presence on (date) _____.
Name & ID# of Witness to destruction: _____ Signature: _____Date: _____

Release to Lawful Owner

Item(s) #: _____ on this document was/were released by Evidence Custodian _____ID#:_____ to
Name _____
Address: _____ City: _____State: _____ Zip Code: _____
Telephone Number: (____) _____
Under penalty of law, I certify that I am the lawful owner of the above item(s).

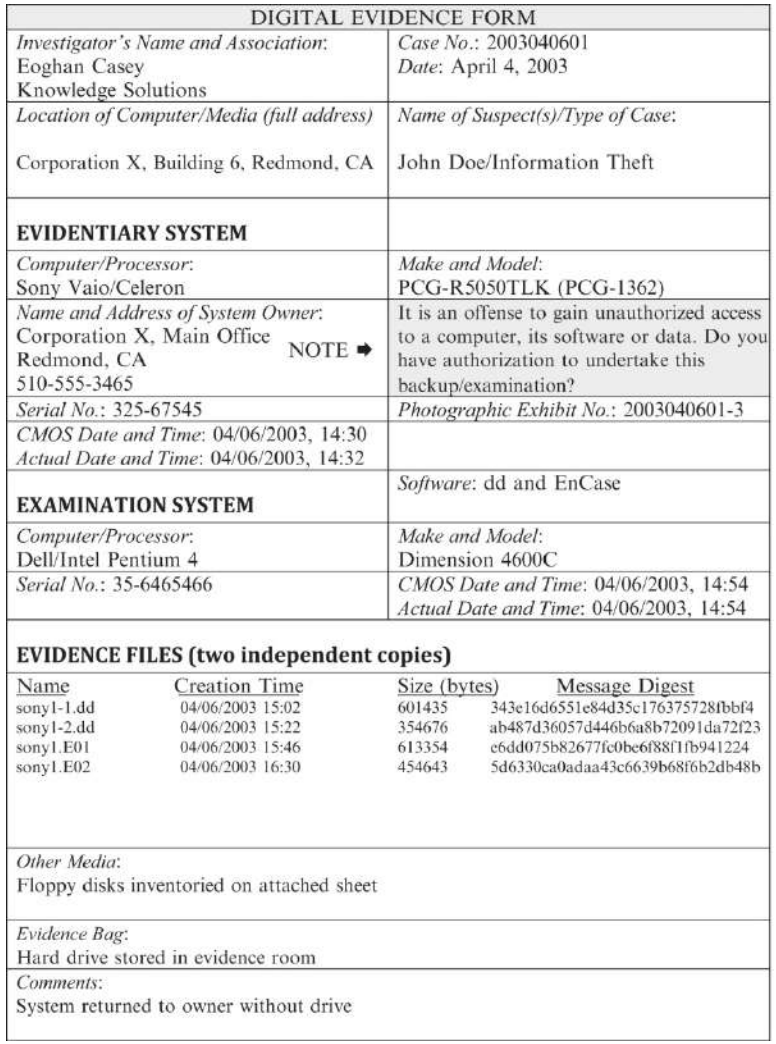
Signature: _____ Date: _____

Copy of Government-issued photo identification is attached. ☐ Yes ☐ No

This Evidence Chain-of-Custody form is to be retained as a permanent record by the Anywhere Police Department.

APD_Form_#PE003_v.1 (12/2012) Page 2 of 2 pages (See front)

From: http://www.nist.gov/oles/forensics/upload/Sample-Chain-of-Custody-Form.docx



DIGITAL EVIDENCE FORM

Investigator's Name and Association: Eoghan Casey Knowledge Solutions	*Case No.*: 2003040601 *Date*: April 4, 2003
Location of Computer/Media (full address) Corporation X, Building 6, Redmond, CA	*Name of Suspect(s)/Type of Case*: John Doe/Information Theft
EVIDENTIARY SYSTEM	
Computer/Processor: Sony Vaio/Celeron	*Make and Model*: PCG-R5050TLK (PCG-1362)
Name and Address of System Owner: Corporation X, Main Office Redmond, CA 510-555-3465 NOTE ➡	It is an offense to gain unauthorized access to a computer, its software or data. Do you have authorization to undertake this backup/examination?
Serial No.: 325-67545	*Photographic Exhibit No.*: 2003040601-3
CMOS Date and Time: 04/06/2003, 14:30 *Actual Date and Time*: 04/06/2003, 14:32	
EXAMINATION SYSTEM	*Software*: dd and EnCase
Computer/Processor: Dell/Intel Pentium 4	*Make and Model*: Dimension 4600C
Serial No.: 35-6465466	*CMOS Date and Time*: 04/06/2003, 14:54 *Actual Date and Time*: 04/06/2003, 14:54

EVIDENCE FILES (two independent copies)

Name	Creation Time	Size (bytes)	Message Digest
sony1-1.dd	04/06/2003 15:02	601435	343e16d6551e84d35c176375728fbbf4
sony1-2.dd	04/06/2003 15:22	354676	ab487d36057d446b6a8b72091da72f23
sony1.E01	04/06/2003 15:46	613354	e6dd075b82677fc0be6f88f1fb941224
sony1.E02	04/06/2003 16:30	454643	5d6330ca0adaa43c6639b68f6b2db48b

Other Media:
Floppy disks inventoried on attached sheet

Evidence Bag:
Hard drive stored in evidence room

Comments:
System returned to owner without drive

FIGURE 16.2 Digital evidence form.

Examination, Analysis & Reporting: General Handling Procedures

- **Examination**:
  - Always work on the **duplicates**, never on the original
  - ***Dual-tool verification*** *(more in the next few slides)*
- **Analysis**:
  - Accurately perform various **types of analysis** (e.g. a time-line analysis, event correlation) to discover findings and draw conclusions
- **Reporting**:
  - Present the findings in a **technically correct yet understandable** manner

Dual-Tool Verification

- **Bugs** do exist in DF software, and can result in evidence being lost or interpreted incorrectly
- ***Dual-tool verification*** technique:
  - Use **two tools** to verify that the results are correct
  - Either by **comparing the results** from both tools; or by using one tool to **verify** that data has been interpreted/ processed correctly by another tool
- **Examples**: two tools should recover the same deleted files from a given file system, should calculate date-time stamps correctly

Additional Notes on Tool Verification

- **US NIST Computer Forensic Tool Testing (CFTT)** program: to establish a **methodology for testing** computer forensic software tools by development of general tool specifications, test procedures, test criteria, test sets, and test hardware
- Example: CFTT provides **formal requirements** for write blockers, "*The Hardware Write Block (HWB) Device Specification*", http://www.cftt.nist.gov/hardware_write_block.htm
  - Shall not transmit a command to a protected storage device that modifies the data on the storage device
  - Shall return the data requested by a read operation
  - …
- US NIST's **Computer Forensic Reference Data Sets (CFReDS)** can additionally be used to **validate** DF software tools

Evidence Acquisition

Data Volatility: Overview

- Target system's data exists in both **non-volatile** and **volatile** states
- ***Non-volatile*** data: data **persists** even after a computer is powered down, e.g. a file system stored on a hard drive
- ***Volatile*** data: data will be **lost** after a computer is powered down, e.g. the current network connections to and from the system
- ***Volatility problem***:
  you may **never** have access to your target system's data again:
  e.g. lost physical memory (RAM) content, encrypted file system
- A proper handling at the crime scene is thus needed!

Evidence Acquisition: Some Options to Choose

- Given a seized computer, *what can you do?*
- *One question*: should we disconnect it from a **network**?
- **Live/volatile memory acquisition** and **live analysis**:
  - The evidential computer is running the OS installed on that computer
  - An important *question*: Can we do data collection **using the evidential computer itself**?
    - **Pros**: The system potentially holds evidence that may be lost or hard to acquire if the system is shut down (e.g. encrypted disk)
    - **Cons**: Can we trust the system in generating the evidence?
- *Another question*: when powering-off the computer, should we do a **graceful/orderly** shutdown or a **forceful** shutdown?

Evidence Acquisition: Some Options to Choose

- **Static/dead/non-volatile acquisition**:
  - Utilizes an OS that is ***not*** running on the evidential machine
  - *Question*: where should this be done?
    → Typically done in a forensic lab
- *Question*: How about the order of evidence acquisition?
  - Evidence acquisition should be **done/ordered** based on the **Order of Volatility (OOV)**:
    most volatile → least volatile → non-volatile memory

Order of Volatility (OOV)

- **OOV**:
  - *CPU, cache and register content*
  - Routing table, ARP cache, process table, kernel statistics
  - Memory
  - Temporary file system/swap space
  - Data on hard disk
  - Remotely logged data
  - Data contained on archival media
- Reference: P. Henry, https://www.sans.org/blog/best-practices-in-digital-evidence-collection/

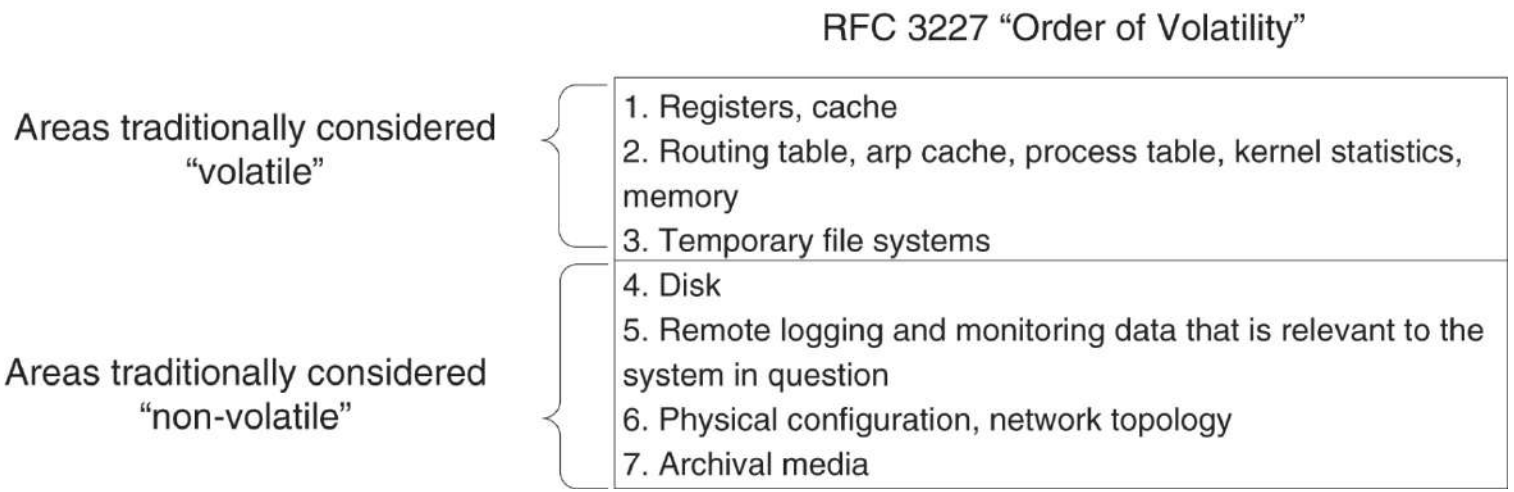


FIGURE 13.5 Order of volatility.

Data Acquisition at Crime Site

- Some ***widely-followed protocols*** at the crime site
- First, **document** the evidence:
  - Take **photos and video** of the scene and computer (including all cables)
  - Sketch the **incident scene**: diagram and label all cords
- If a computer is **off**:
  - *Don't turn it on*
  - A much simpler decision procedure
  - But, if the disk is encrypted, what can we do during our analysis?
    - Possible **disk decryption tools**, e.g. Elcomsoft Forensic Disk Decryptor
    - Any ways to recover passwords/passphrases from RAM?
      Cold-boot attack (https://en.wikipedia.org/wiki/Cold_boot_attack):
      relies on the data remanence property of DRAM/SRAM to retrieve memory contents that remain readable **in the seconds to minutes** after power has been removed;
      Ref: Halderman, et al., "*Lest we remember: Cold-boot attacks on encryption keys*", Communications of the ACM. 52 (5): 91–98.

Data Acquisition at Crime Site

- If a computer is **on**:
  - Should you perform a **live/volatile acquisition***?*
    - It is considered necessary if the suspect encrypts his hard drives
    - *Question*: Can we check if the disk is encrypted?
      A tool like **Encrypted Disk Detector (EDD)** could help check
      the local drives on a system for TrueCrypt/PGP/Bitlocker/…. encrypted volumes
    - **Live acquisition steps**: see **Lecture 3** and **Lab 3 exercise** later
  - Should you additionally perform a **live analysis**??
    - How about a self-destruct or self-wipe machine??
  - How should you **shutdown** the machine?
    - Graceful/orderly shutdown vs forceful ("pull the power plug"): pros & cons?
    - Relevant adopted best shutdown procedure

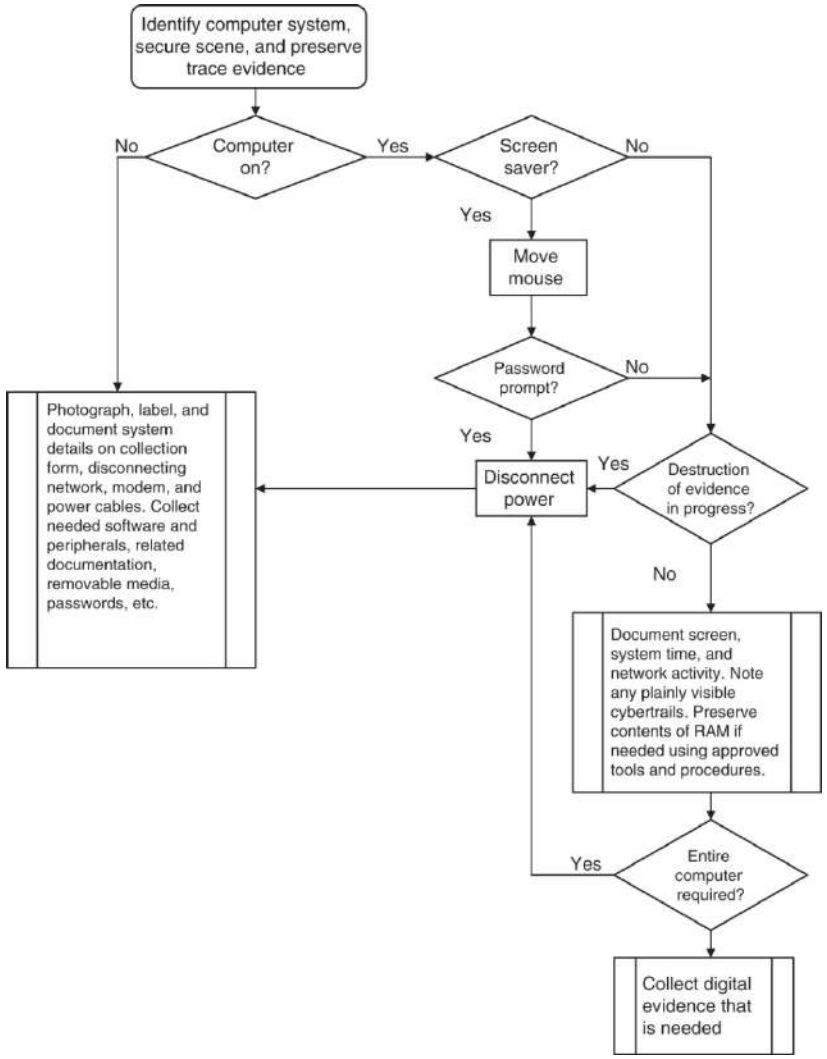
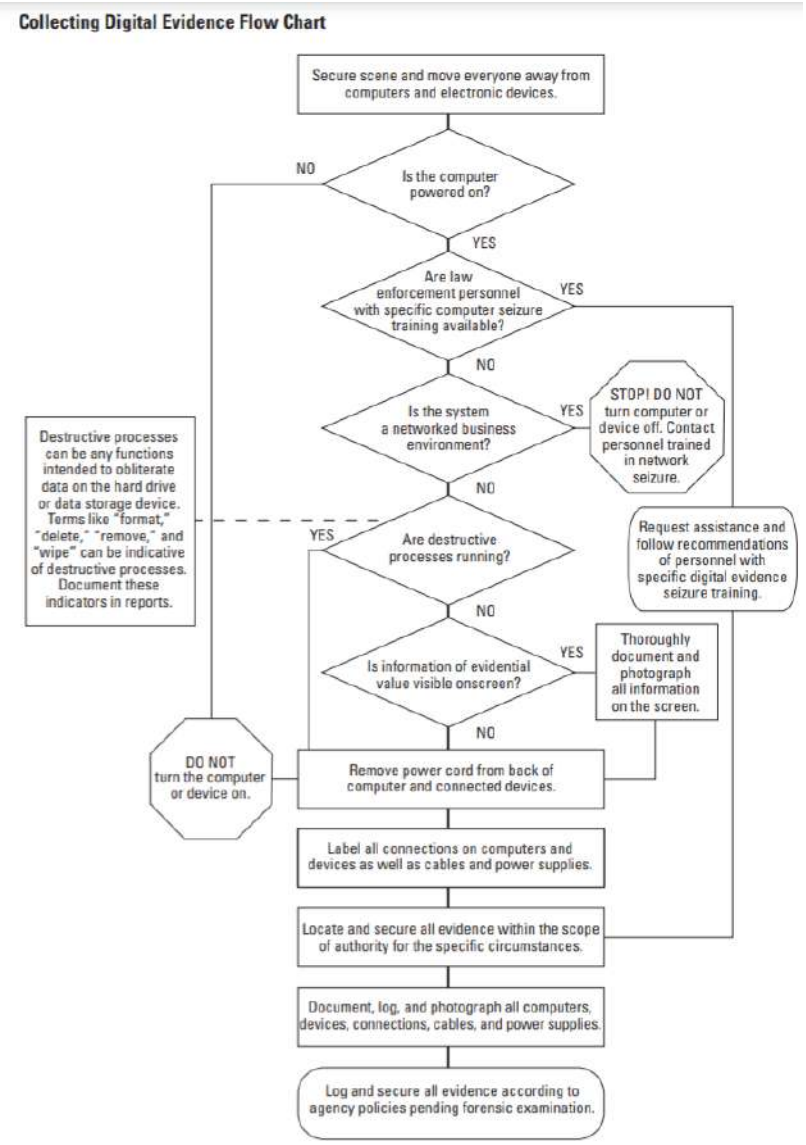


FIGURE 7.7 An overview of the decision process when preserving a computer.

Guidelines for First Responders: Resources

"*Electronic Crime Scene Investigation: A Guide for First Responders*", U.S. Department of Justice, 2008: https://www.ncjrs.gov/pdffiles1/nij/219941.pdf



Guidelines for First Responders: Resources

"*Digital Evidence Guide for First Responders*" from Massachusetts Digital Evidence Consortium, 2015: https://www.iacpcybercenter.org/wp-content/uploads/2015/04/digitalevidence-booklet-051215.pdf

Step 4 – If the system is on, proceed with **CAUTION**

- Do not type, click the mouse, or explore files or directories without advanced training or expert consultation

- Ask about passwords and/or encryption of the system
- Observe the screen, and look for any running programs that indicate access to internet-based accounts, open files, encryption, or the presence of files or data of potential evidentiary value
- If you see anything on the screen that concerns you or needs to be preserved, consult with an expert (if you don't know who to contact, call the number on the inside cover of this manual)
- Photograph the screen
- Once you are prepared to power down the system, pull the plug from the back of the computer system
- Remove the battery from a laptop system

Data Acquisition at Crime Site

- **Subsequent** steps:
  - Unplug power cord, remove notebook's removable battery if required
  - Bag up all electronic devices in ***evidence bags*** as their safe containers:
    - For magnetic media: use **anti-static bags**
    - For mobile devices: use **signal-blocking bags**!
  - Collect all available instruction manuals, CDs, notes, etc.
  - Document all pieces of collected evidence
  - Perform **a static/non-volatile acquisition** at the forensic lab:
    - Use your forensic workstation: see **Lab 2**
    - What if you **cannot** remove the non-volatile storage devices from the suspect/evidential computers?
      → Boot up using **forensically-safe live CD boot** (more in this slide deck)

Break!

US Dept of Defense Computer Forensic Workstation (http://www.dcfl.gov/photo.html)

Digital Forensics Lab & Tools

Digital Forensics Lab: Standard & Guidelines

- While there is **no standard** on digital forensics lab (DFL), a number of organizations look at **similar areas** to find an appropriate standard
- "**ISO/IEC 17025 General requirements for the competence of testing and calibration laboratories**": general requirements for the competence of testing and calibration laboratories is being used to **model** a standard for computer forensic labs
- **Guidelines** for a DFL:
  - The **American Society of Crime Laboratory Directors (ASCDL)** https://www.ascld.org/
  - "***INTERPOL*** *global guidelines for digital forensics laboratories*", https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf *(more in the next slide)*

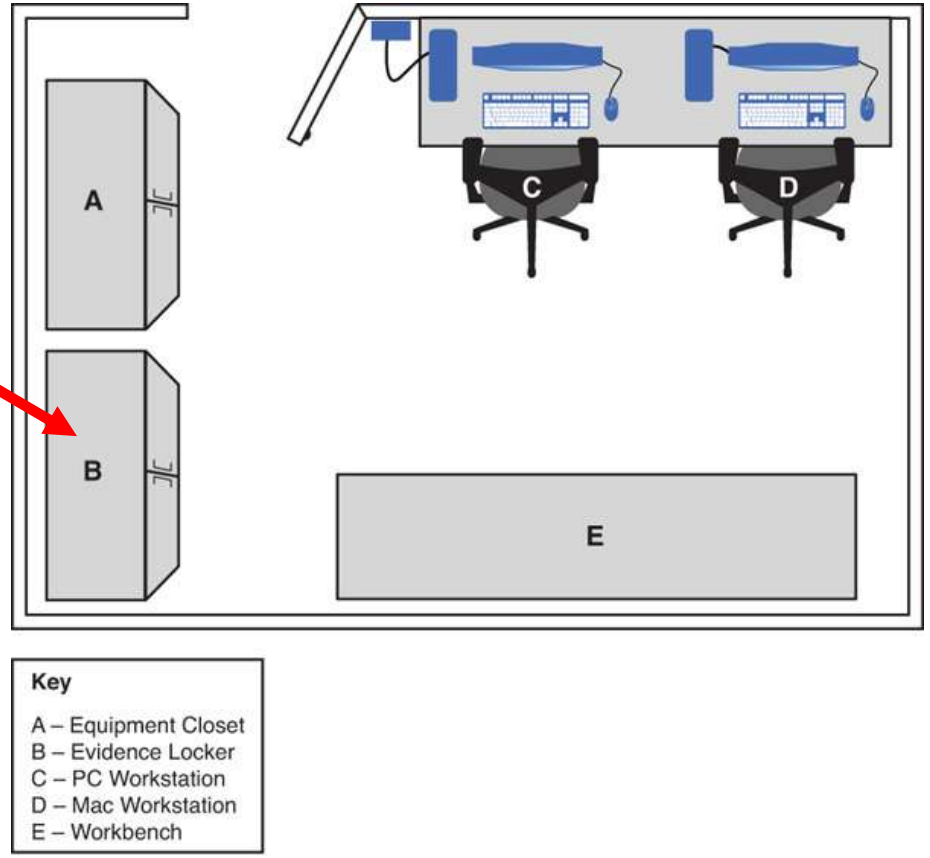
INTERPOL Global Guidelines for DFLs

- Issued by the Digital Forensics Laboratory at the INTERPOL Global Complex for Innovation, Napier Road, **Singapore**, **2019**
- **Management** of a digital forensics laboratory, including about:
  - Premises: location, facility, physical security, …
  - Staff
  - Equipment: software, Hardware, Tools & accessories
  - (And also) laboratory analysis procedure
- A good recent reference for planning and managing a DFL

Acquiring Evidence in a Computer Forensics Lab (cont.)

Laboratory Requirements

Note: "***evidence lockers***" in a digital forensic lab (vs "***evidence bags***" during evidence search & seizure

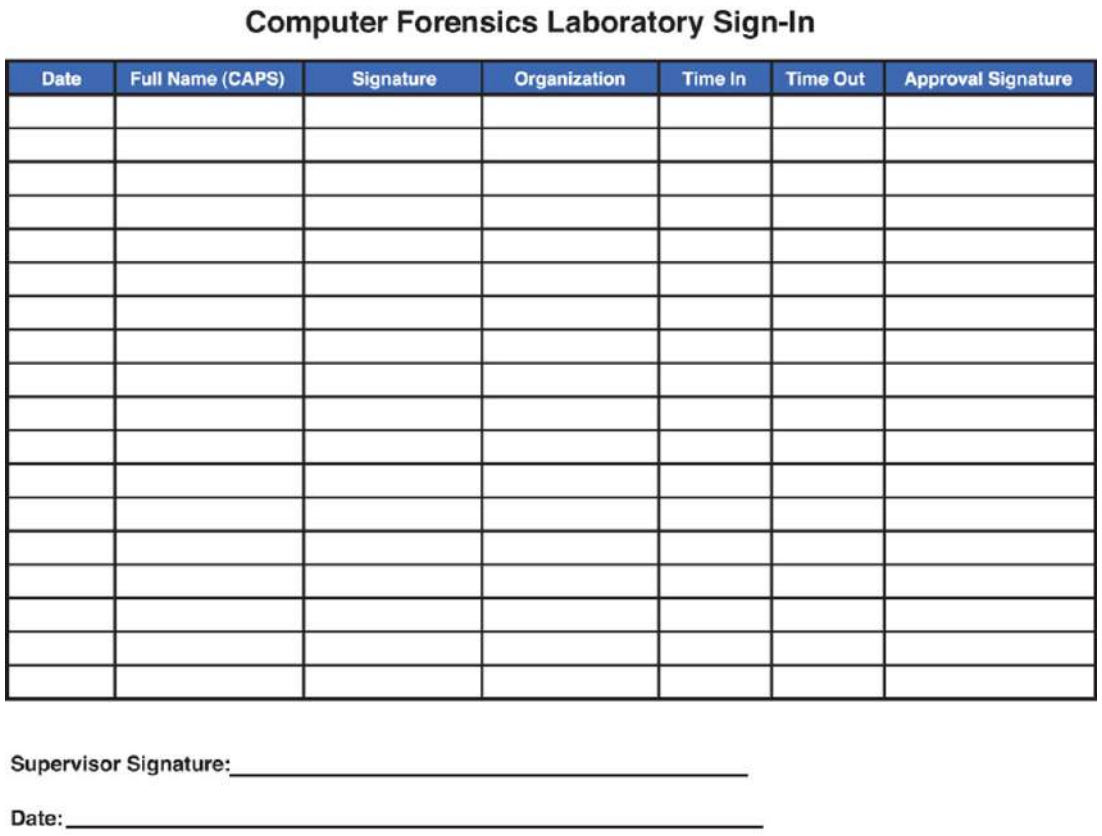


Acquiring Evidence in a Computer Forensics Lab (cont.)

Evidence Locker

Acquiring Evidence in a Computer Forensics Lab (cont.)

Computer Forensics Laboratory Sign-In



Computer Forensics Laboratory Sign-In

Date	Full Name (CAPS)	Signature	Organization	Time In	Time Out	Approval Signature

Supervisor Signature:_____

Date:_____

Determining Floor Plans for Digital Forensics Labs

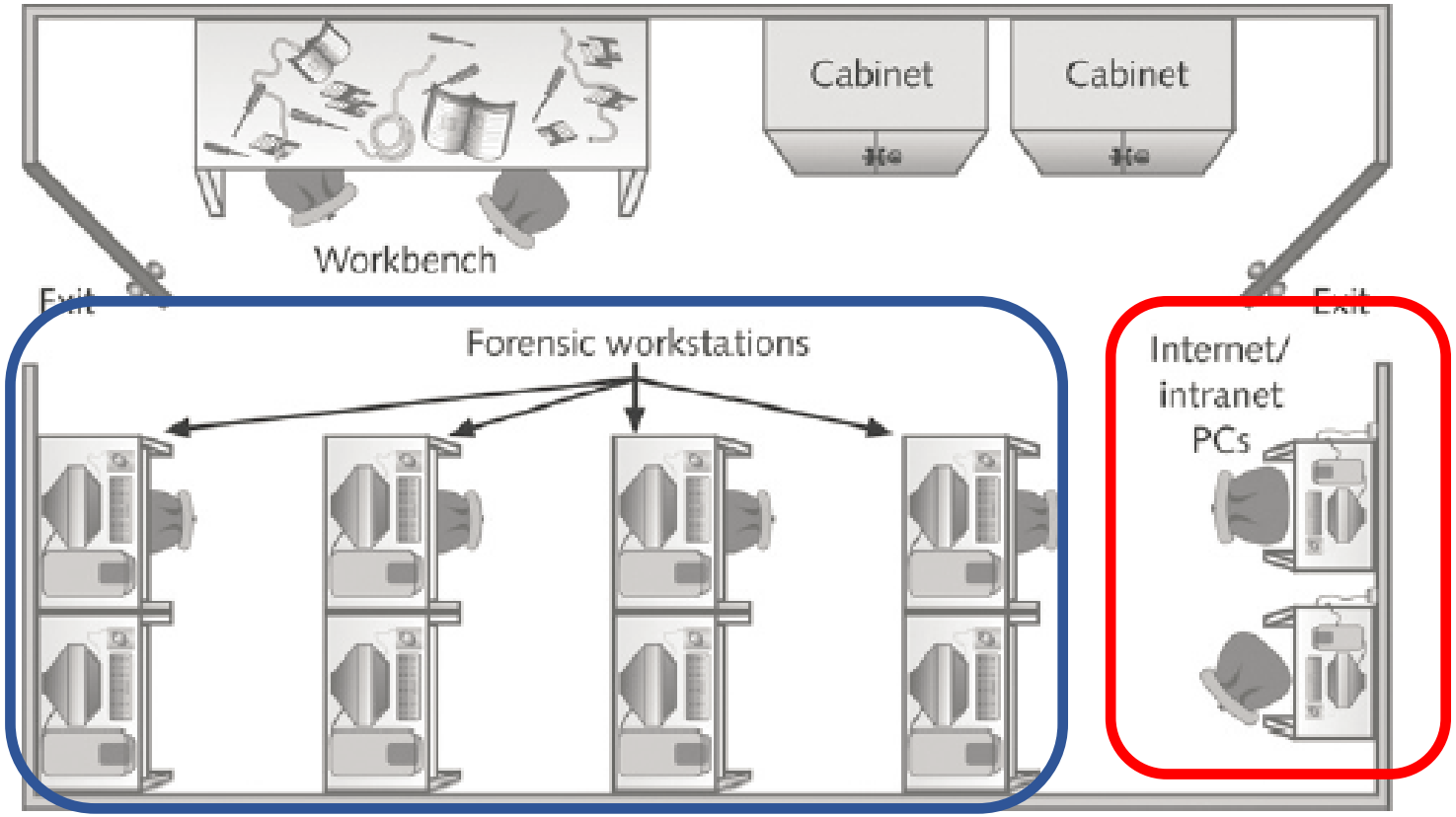


Figure 2-3 Mid-size digital forensics lab

Digital Forensics Hardware & Other Equipment

- ***Forensic workstation***: a powerful computer with plenty of storage
- **Portable forensic workstation**:
  a field-kit for use in the field at the crime site
- Other **supporting equipment**:
  - Hardware write blocker
  - Hard disk duplicator
  - Anti-static evidence bags
  - Mobile-phone signal blocker bags
  - …

Forensics Workstation Example

- Cellebrite forensics workstation

Source:
https://www.cellebrite.com/en/cellebrite-forensic-workstation/

Portable Forensic Workstation Example

- Cellebrite UFED

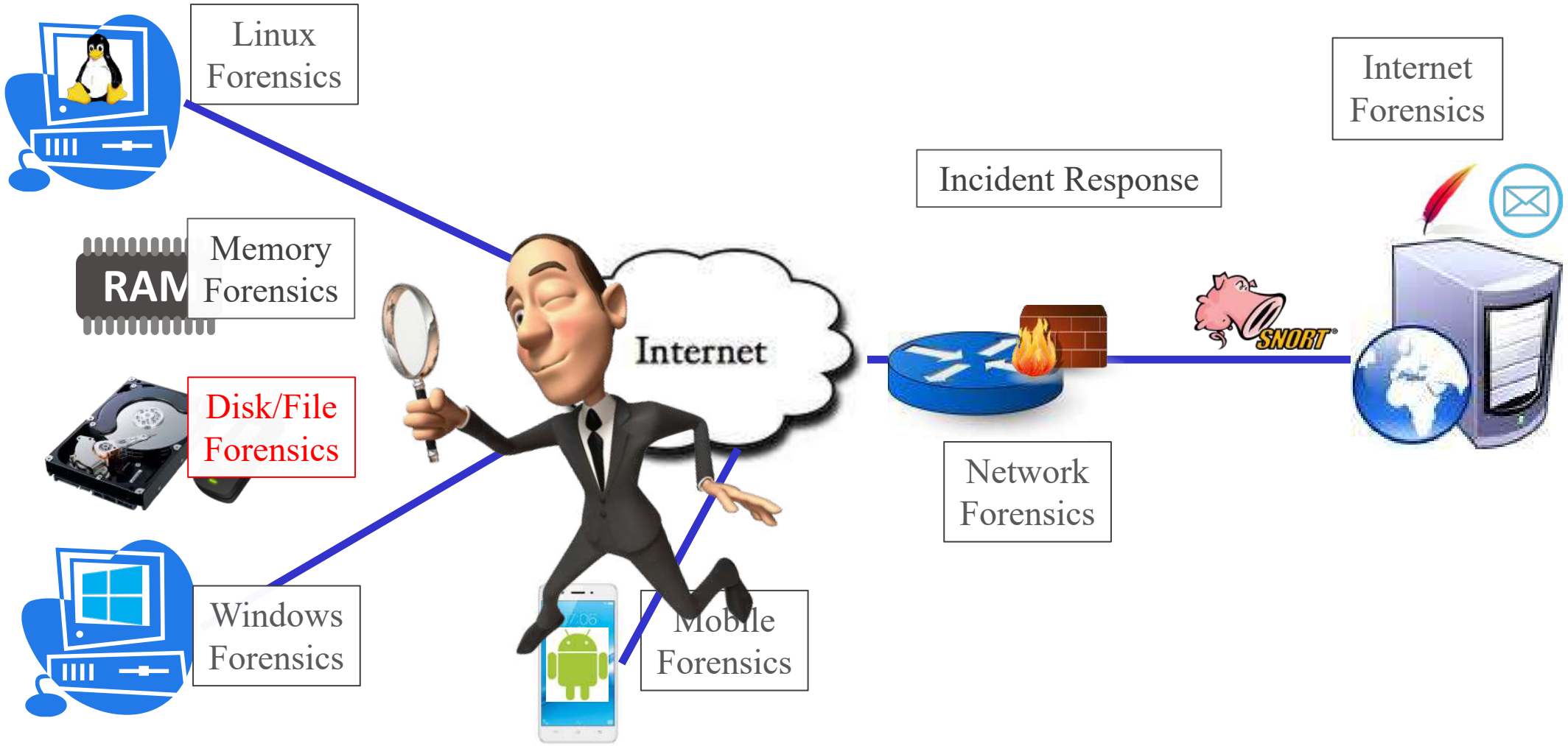
Source:
https://www.scmagazine.com/review/cellebrite-ufed-series-of-tools/

Handling Computer Hardware (cont.)

Cloning a Hard Disk Drive with Disk Jockey PRO Forensic Edition

Static Acquisition

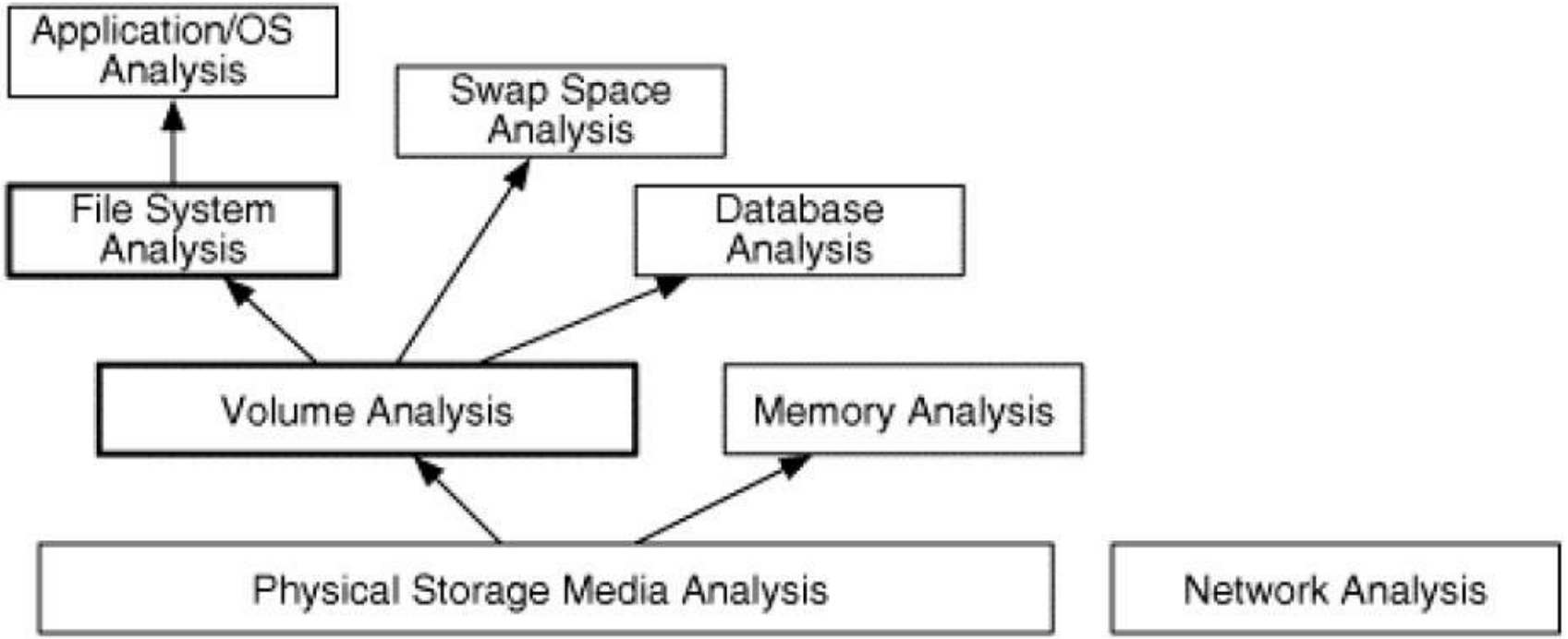
Memory Forensics



Static Acquisition

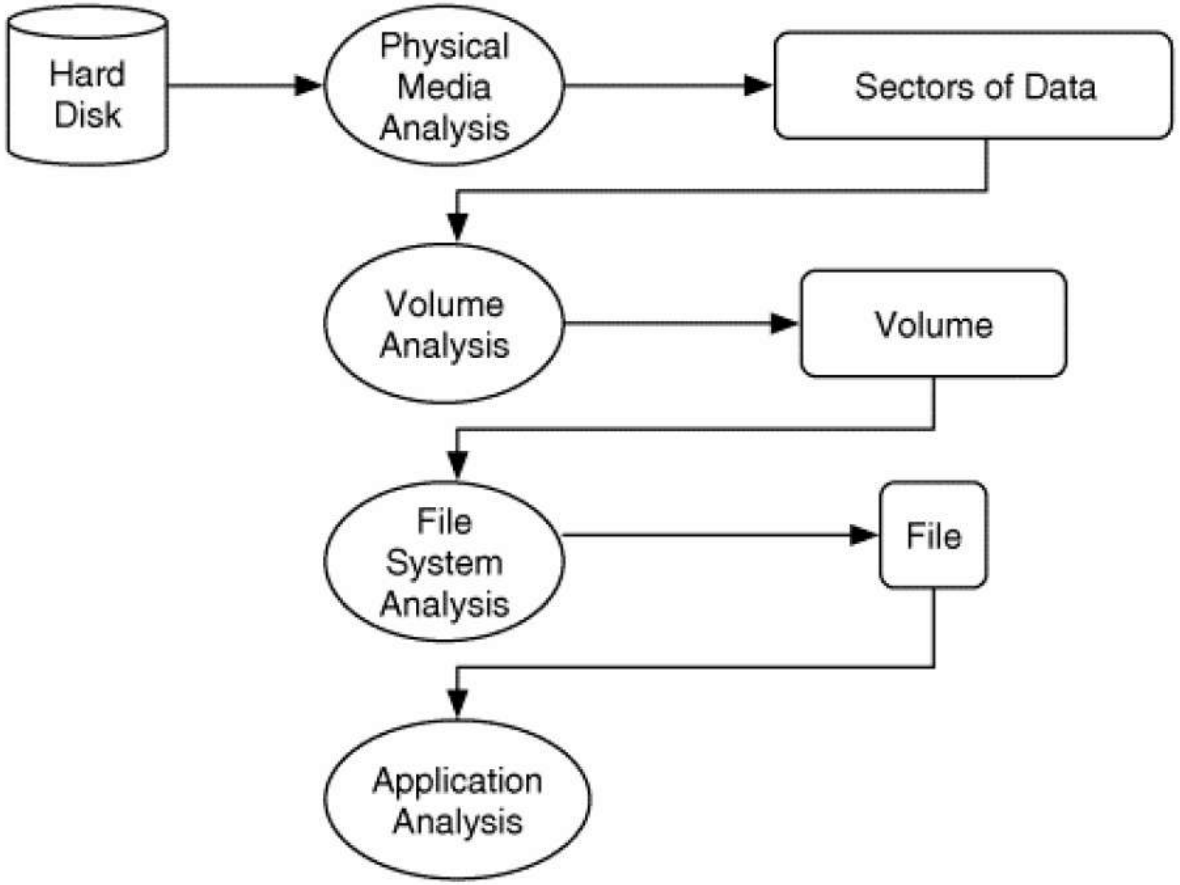
- ***Static acquisition***: image creation of **persistent storage devices (non-volatile memory)**, e.g. hard disk, USB drive, SD cards
- **Bit-stream/bit-by-bit/forensic** copy:
  - **Goal**: to create an *exact duplicate* of a storage device, including its *slack space*
  - **Technique**: make a bit-for-bit copy of **all sectors** on the media
  - **Output**: a bit-stream image or forensics image/copy
- Tool **requirements**:
  - "*Data Acquisition Tool Test Assertions and Test Plan*" from NIST CFTT (www.cftt.nist.gov)
  - Can we use tools like tar or copy? Why or why *not*?
- Also the importance of a **write blocker**!

Static Acquisition & Volume+File-System Analysis



From: Brian Carrier, “File System Forensic Analysis”

Layers of Disk & File Analysis



From: Brian Carrier, “File System Forensic Analysis”

Write Blockers

- **Protect/preserve** your evidence drives
- Some OSes with journaling file system **may** write into drives
- Types:
  - **Hardware**:
    - Sits between a forensics workstation and evidence drives
    - **USB connection** to the forensics workstation
    - A number of **interfaces** to evidence drives: USB, IDE, SATA, eSATA, FireWire, …
    - **Professional grade** with various switches and indicators:
      e.g. hardware blockers from Tableau
    - Video: https://www.youtube.com/watch?v=7eT8KSHMGFw

Hardware Write Blocker

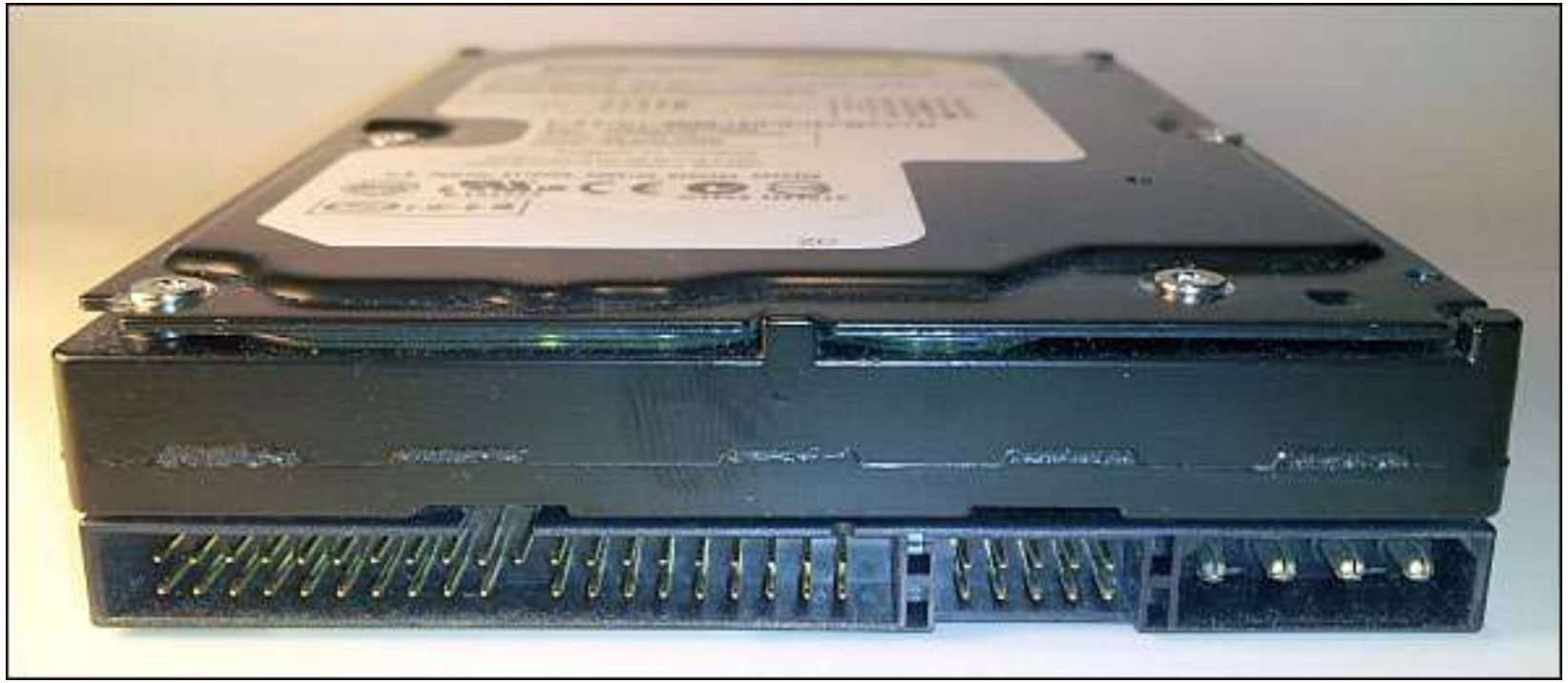
Source: Wikipedia

Handling Computer Hardware (cont.)

SATA Data Cable and SATA Power Cable

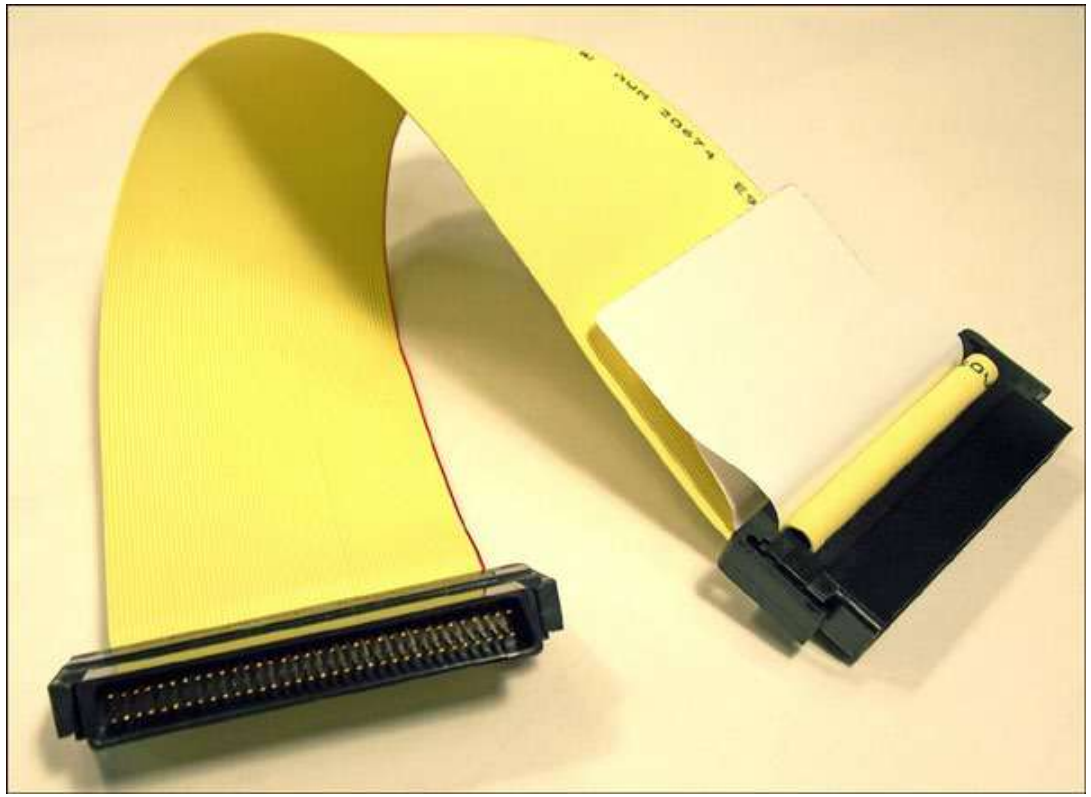
Handling Computer Hardware (cont.)

IDE Interface on a Hard Disk



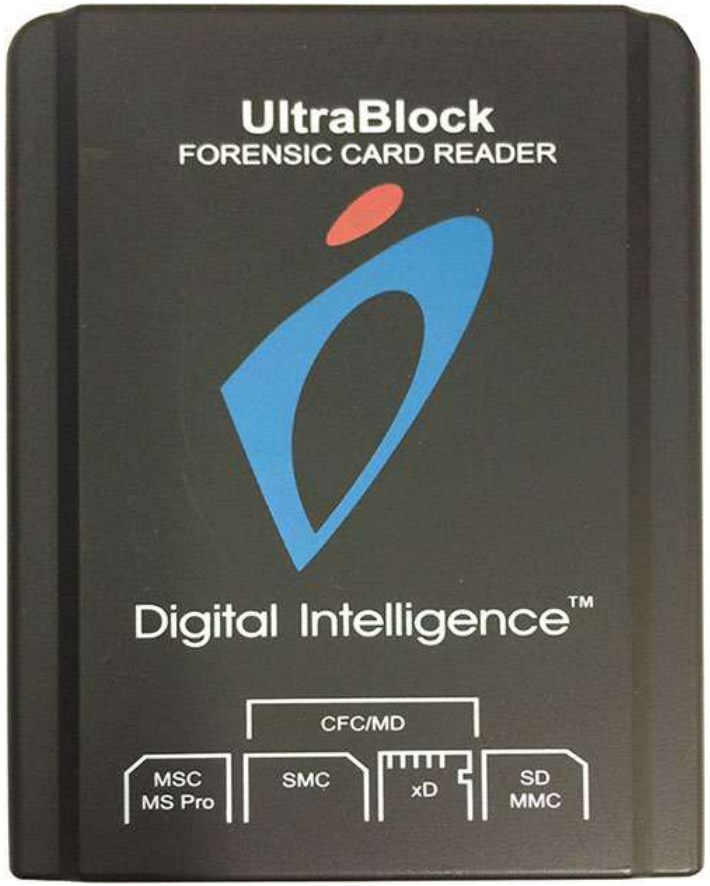
Handling Computer Hardware (cont.)

SCSI Connector



Handling Computer Hardware (cont.)

UltraBlock Forensic Card Reader and Writer



Write Blockers

- **Software**:
  - **OS configuration** on your forensic workstation
  - Done by either a **manual OS configuration**; or a **forensics software,**
    e.g. FastBloc SE (Software Edition) from EnCase, SAFE Block Win8 from ForensicSoft Inc.
  - Windows-based write blocker using the **Registry Editor (**see **Lab 2, Task 1)**:
    - Registry entry:
      `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies`
    - Value: `WriteProtect`=1 (DWORD/32-bit value)
  - Linux write-blocker kernel patch:
    - Some patches are available, e.g.
      https://github.com/msuhanov/Linux-write-blocker/

- Which one should you use: a hardware or a software write blocker? *Why?*

Windows Registry: Quick Notes for Lab 2

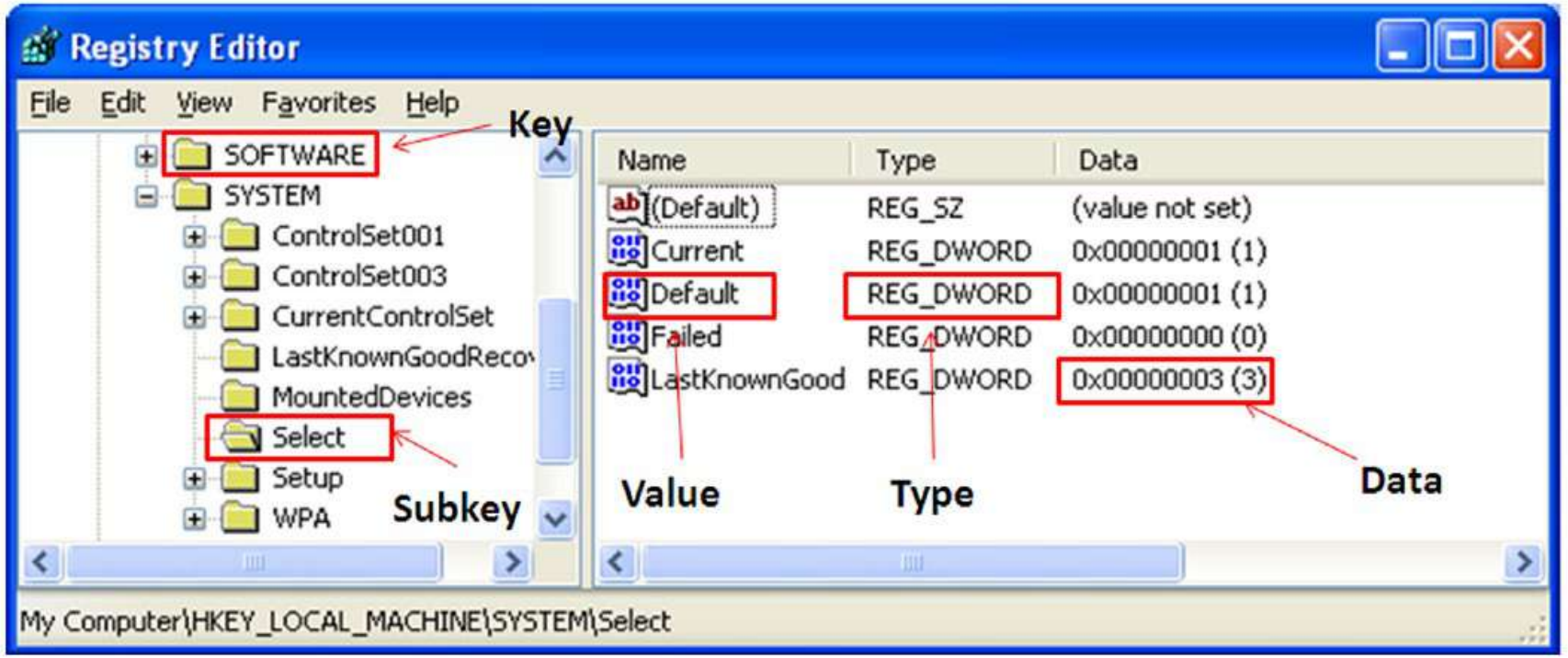


Figure 1.4 Registry nomenclature.

From: Harlan Carvey, “Windows Registry Forensics", 2nd Edition

Static Acquisition Methods

- **Disk to image** (***forensic container***): the most common method
  - Expert Witness Format (EWF):
    used by EnCase, unofficial/de-facto industry standard, **.E01** extension,
    also .**Ex01** (a new variation offering encryption and compression)
  - Advanced Forensics Format (AFF):
    open format by Simson Garfinkel, used in TSK/Autopsy, .**AFF** extension
  - **AFF4**: a redesign of AFF
  - **Raw/dd** format
  - SMART
- **Disk to disk**:
  - Produce a **disk clone**
  - Done is if disk-to-image method is not possible due to HW/SW issues

FIGURE 7.2 Tableau hardware duplicator used to acquire evidence from hard drives.

More on Static Acquisition

- Benefits of **newer disk image formats** (EWF, AFF):
  - Option to **compress** the image files (using lossless compression)
  - Capability to **split** an image into **smaller segmented files**
  - Capability to store and integrate **metadata** into the image files, including case information
  - Due to these features, the size of the *target device* is ***not*** the same as the *created image file* (forensic container)
- Note: If you **don't need** to or **can't examine** the entire drive (e.g. from a very large drive):
  - **Logical acquisition**: captures only specific **files of interest**
  - **Sparse acquisition**: logical acquisition + collects **fragments** of unallocated/deleted data

Static Acquisition

- In **Windows**:
  - **FTK Imager** (**Lab 2**): not open source, but free to use
  - Various other forensics suites
- In **Linux**:
  - **dd** (data dump):
    - `dd if=<`*source-drive*`> of=<`*image-file*`> conv=noerror,sync`
    - Split image file:
      `dd if=<`*source-drive*`> conv=noerror,sync |`
      `split -b <`*size-in-MB*`>m - <`*image-file*`>`
  - **dcfldd** (forensics version of dd, from Defense Computer Forensics Laboratory):
    - `dcfldd if=<`*source-drive*`> of=<`*image-file*`> hash=<`*hash-function*`>`
      `hashlog=<`*logfile*`>`

Static Acquisition

- **dc3dd** (another forensics version of dd, from DoD Cyber Crime Centre):
  - `dcfldd if=<`*source-drive*`> hof=<`*image-file*`> hash=<`*hash-function*`> log=<`*logfile*`>`
- **Benefits** of dcfldd/dc3dd over dd:
  - Logging
  - Improved error handling
  - Available hashing options
  - Verification of the acquired data
  - Progress monitoring: note that forensic imaging can take many hours!
- **GUI tool**: Guymager

Write output to a file/device, *then* hash the output bytes, and verify the hash

- Demo of dd & dcfldd: https://www.youtube.com/watch?v=aJp7_OVW2FA

Copy Integrity and Hash Values

- **Compare** an original evidence drive and created forensics image
- Typical **hash functions** used: MD5, SHA1 (*are these still "secure"?*)
- Imager component a forensics suite computes and compares hash values
- Alternatively, we can compute hash values using **Linux** commands:
  - MD5: `md5sum` , SHA-1: `sha1sum` , SHA-2: `sha224sum`, `sha256sum`, `sha384sum`, `sha512sum`
  - For recursive hash calculation, use `md5deep` or `hashdeep` with `-r`: support MD5, SHA-1, SHA-256
- For **Windows** hashing command/tools, see Lab 2

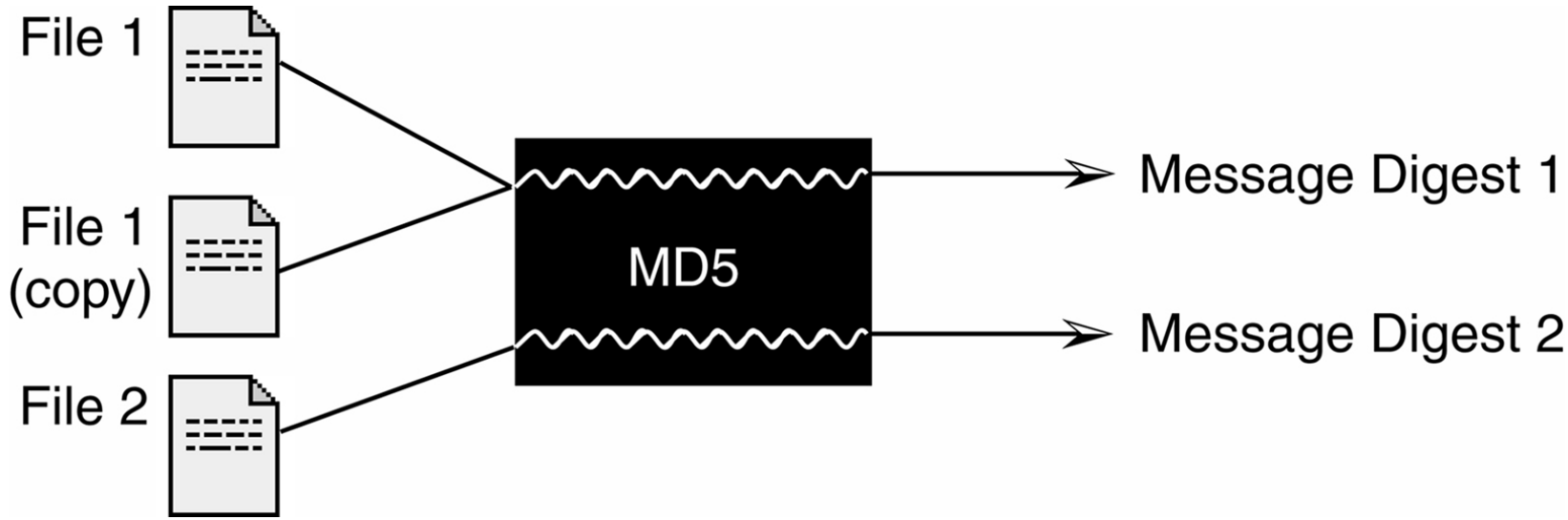


FIGURE 1.3 Black box concept of the message digest.

Remote/Network Acquisition Tools

- It is possible to do a **remote/network** static acquisition
- But potential **issues**: interfering antivirus, antispyware, firewall
- Example of dd with netcat (nc), with the latter's `-w` **timeout option**:
  - `Source# dd if=/dev/sda conv=noerror,sync | nc -w 5 <destination-IP> <destination-port>`
  - `Destination# nc -lp <destination-port> > <image-file>`
  - `Destination# nc -lp <destination-port> | dd of=<image-file>`
- Also there's CryptCat, which enhances netcat with **encryption**
- Extra features of modern forensics software suites:
  - Encrypted data transfer
  - Better user interface
  - …

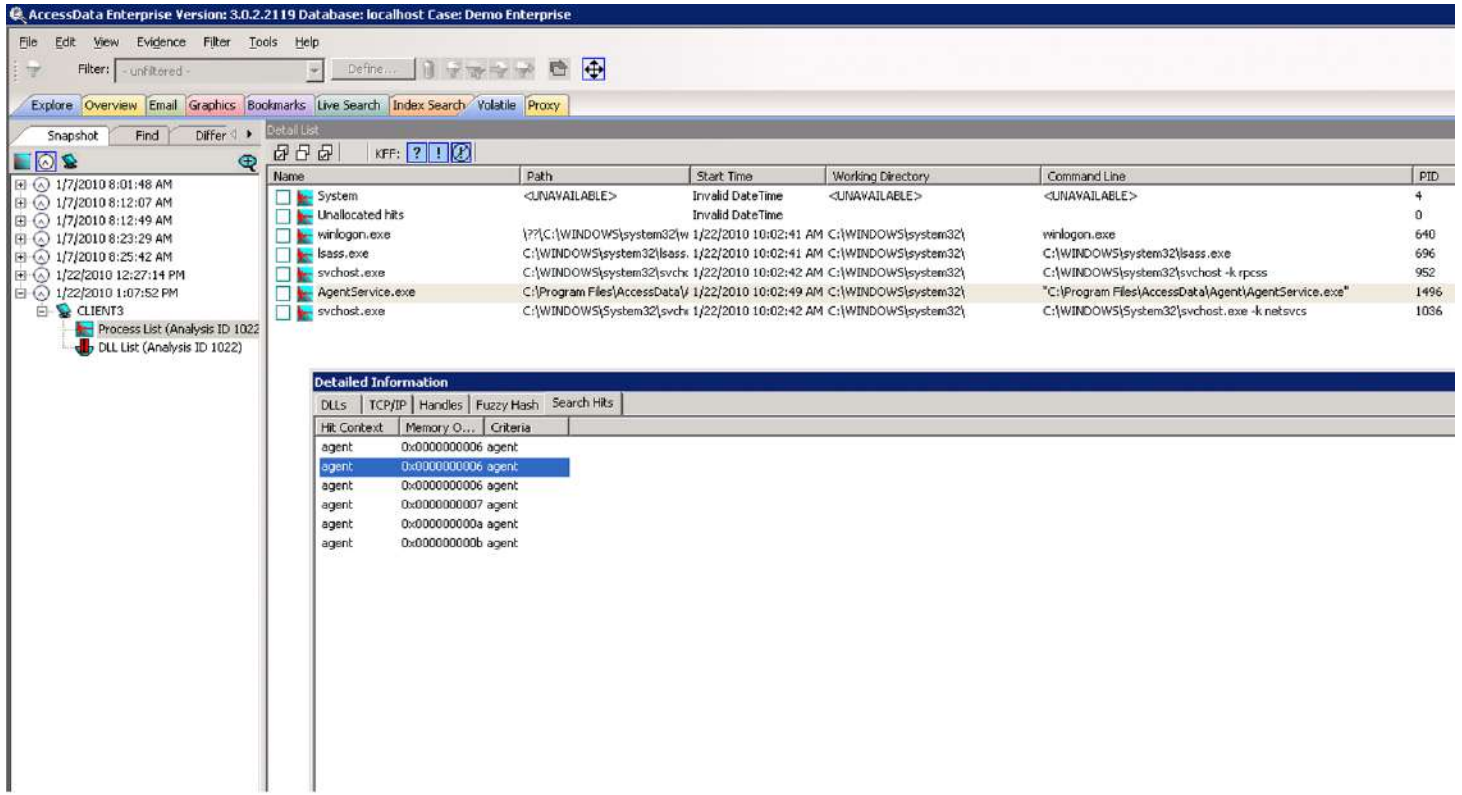


FIGURE 7.5 Remote forensic tool used to acquire digital evidence from a computer over the network.

How about *Unremovable* Storage Media?

- Sometimes a disk ***cannot* be removed** from the suspect's computer
- How can we perform a static acquisition on it?
- Use the ***suspect's computer*** (provided the following are feasible):
  - Can modify the computer's **boot order**
  - Can **connect** a USB/SATA external drive for **USB or CD-ROM boot-up**
  - Can run a **forensically-safe *live* boot CD** → the OS will **not** mount, or mount as **read-only** any connected storage media
    - **Windows** boot utility: Mini WinFE (https://github.com/bshavers/Mini-WinFE)
    - **Linux live CD**: Kali Linux, SIFT, DEFT Linux, ….
  - If there is no available port to plug a **target storage device**: do a **remote acquisition** over the network

Inspecting/Examining Forensic Image File

- Disk image file:
  - Can be inspected using FTK Imager and other forensics suites
- Accessing a forensic image using **FTK Imager** (**Lab 2**):
  - **Add/access image** as **evidence**:
    - Allow you to **browse** file system, and **extract/export** files of interest
    - FTK Imager's evidence-analysis features are limited compared to FTK forensics suite's
    - Autopsy suite can alternatively be used: *to be discussed in Lecture 3 and Labs 3-5*
  - **Mount image** as a **drive**:
    - Make a disk **visible** to the OS
    - Allows **external tools** to inspect the files, e.g. anti-virus software
- Deeper analysis on the image file will require further disk and file analyses (in subsequent lectures and labs!)

Lab 2 Exercises

Lab 2 Exercises

- *Task 1-A: Setting up Windows-based **software write blocker**
- Task 1-B & 1-C: Creating **a forensic image** of your target drive using Windows Forensic Workstation (with FTK Imager)
- Task 2: **Accessing** the created image file and export some files
- *Task 3: **Mounting** the acquired image file and scan for malware
- Task 4: Creating a forensic image of your target drive using Linux Forensic Workstation (with **dd & dcfldd***)

*: Optional

Your Post-Lecture Self-Review

For Your Self-Review before Lecture 3

Definition

Alibi: a plea that a person charged with a crime was **somewhere else** when the crime was committed (Dictionary of Law 2007)

A Scenario:

- A computer crime was committed last Friday in the afternoon
- Was it committed **by you**?
- **Task**: explain the trail of digital evidence left by your activities on that day that can serve as an alibi
- Identify what elements that would be **easily faked**, and which would be **more reliable indicators** of your actual movements

Your TO-DO for Lab 3:

Get a USB thumb drive or external hard drive with free space > your notebook's RAM size

Questions?
See you next week!