The Digital Investigation

Goh Weihan

ICT3215 Digital Forensics

BEng (Hons) in Information and Communications Technology (Information Security)

September 2024

Principles of Digital Forensics

Principles of Digital Forensics

SINGAPORE INSTITUTE OF TECHNOLOGY

Forensic Soundness

Error Handling

Authentication

Evidence Integrity

Forensic Soundness

Digital evidence must be preserved and examined in a forensically sound manner to be of use in an investigation

What is meant by forensically sound?

- Preserving or examining digital evidence in a way that does not alter the original evidence source

- **"Preserve everything but change nothing"?**

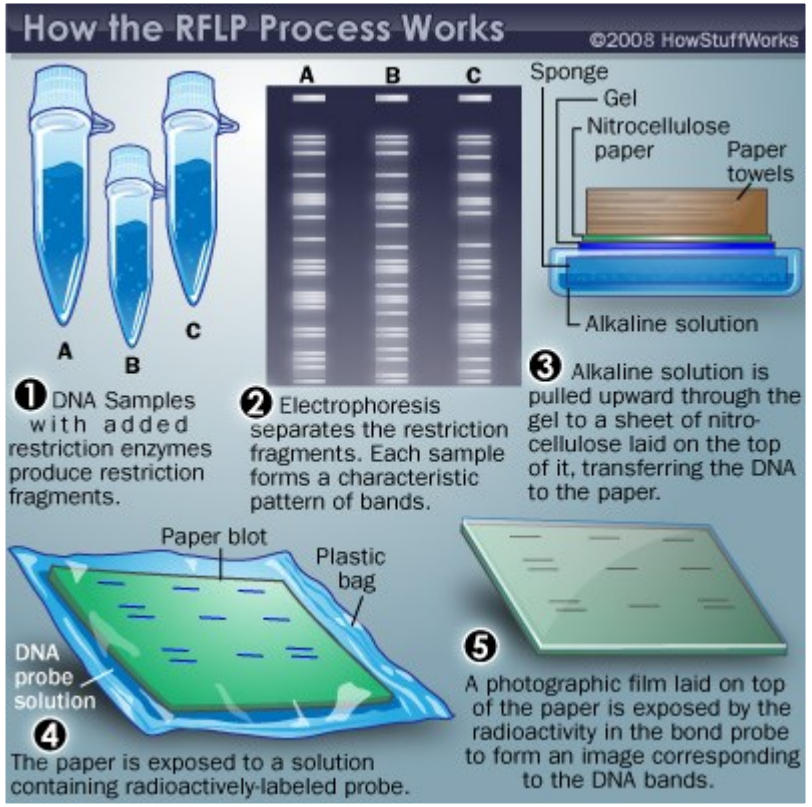
Forensic Soundness

"Preserve everything but change nothing"?

Let us consider DNA profiling

- **Collecting DNA samples:** Generally, involves scraping / smearing original evidence
- **Forensic analysis of DNA samples:** Typically alters the sample further due to the techniques used

Both methods produce changes, yet they are considered forensically sound

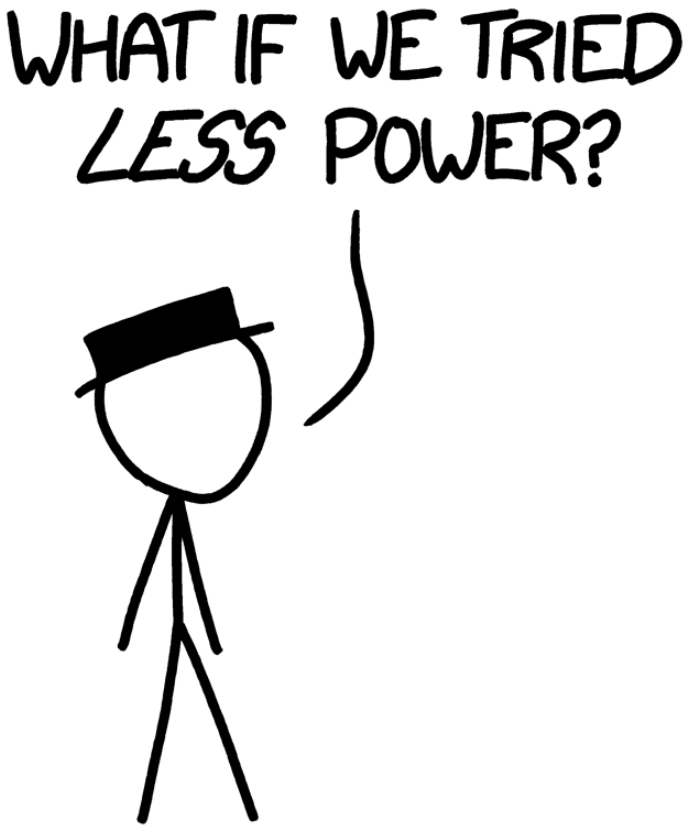


Forensic Soundness

Now consider the digital forensics domain

- Data acquisition from a hard drive will result in S.M.A.R.T. information being updated, **even if a write-blocker is used**
- Acquiring data from hidden areas of a disk **may require overriding certain settings on the disk** to make those areas accessible
- Memory acquisition in live systems or mobile devices **will require overwriting / altering portions of the memory**

Forensic Soundness



Should "preserve everything but change nothing" be the "best practice" for digital forensics?

- Inconsistent with other forensic disciplines
- May be impossible in some circumstances
- May be dangerous in a legal context

Forensic Soundness

General consideration for forensic soundness

Preservation of a complete and accurate representation of the original data, where its authenticity and integrity can be validated

One of the keys to forensic soundness is documentation

Proper, supporting documentation that reports on

- Where the evidence originated from
- How it was handled

Forensic Soundness in a Nutshell

SINGAPORE INSTITUTE OF TECHNOLOGY

Acquisition process should change the original evidence as little as possible

Do not attempt to conceal mistakes, ever!

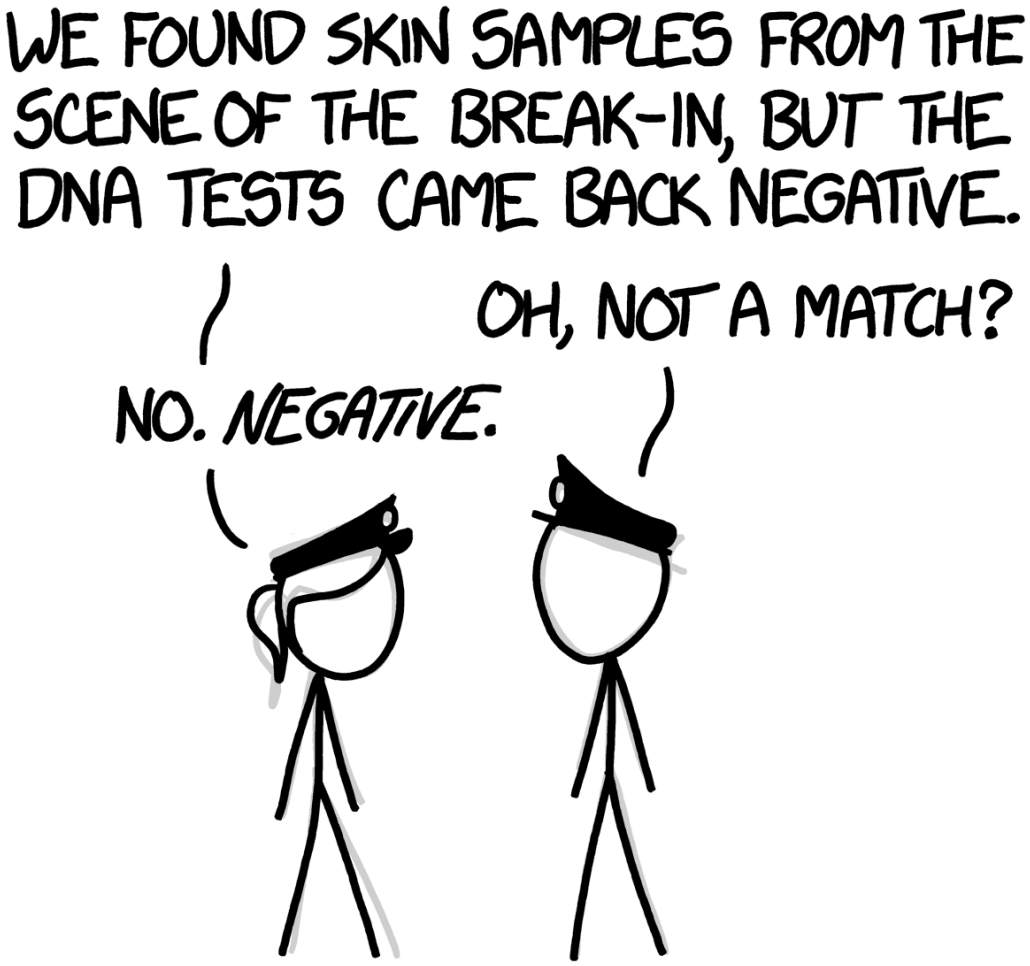
Any changes should be documented, and assessed in the context of the final analytical results

Error Handling

Inadvertent errors / omissions in processing digital evidence may not invalidate the evidence

- Concerns regarding evidence handling may be addressed through documentation, forensic analysis, or testimony

If any problems do occur, document them thoroughly, and seek ways to mitigate the impact on the evidence



Do not attempt to conceal mistakes 

Do Not Conceal Mistakes

This can cause confusion down the road

This will affect and call into question *your* credibility

Authentication

"Authentication means satisfying the court that (a) the contents of the record have remained unchanged, (b) that the information in the record does in fact originate from its purported source, whether human or machine, and (c) that extraneous information such as the apparent date of the record is accurate. As with paper records, the necessary degree of authentication may be proved through oral and circumstantial evidence, if available, or via technological features in the system or the record."

- Reed, 1990 (as quoted by Sommer, 1997)

Authentication

From a technical standpoint, not always possible to compare acquired data with the original

- RAM on a running computer changes constantly; captured RAM is a *snapshot* of the running state at a given time
- Network traffic is transient, and must be captured while in transit; once captured, only the copies remain, and no 'original data' is available for comparison

Chain of Custody Document

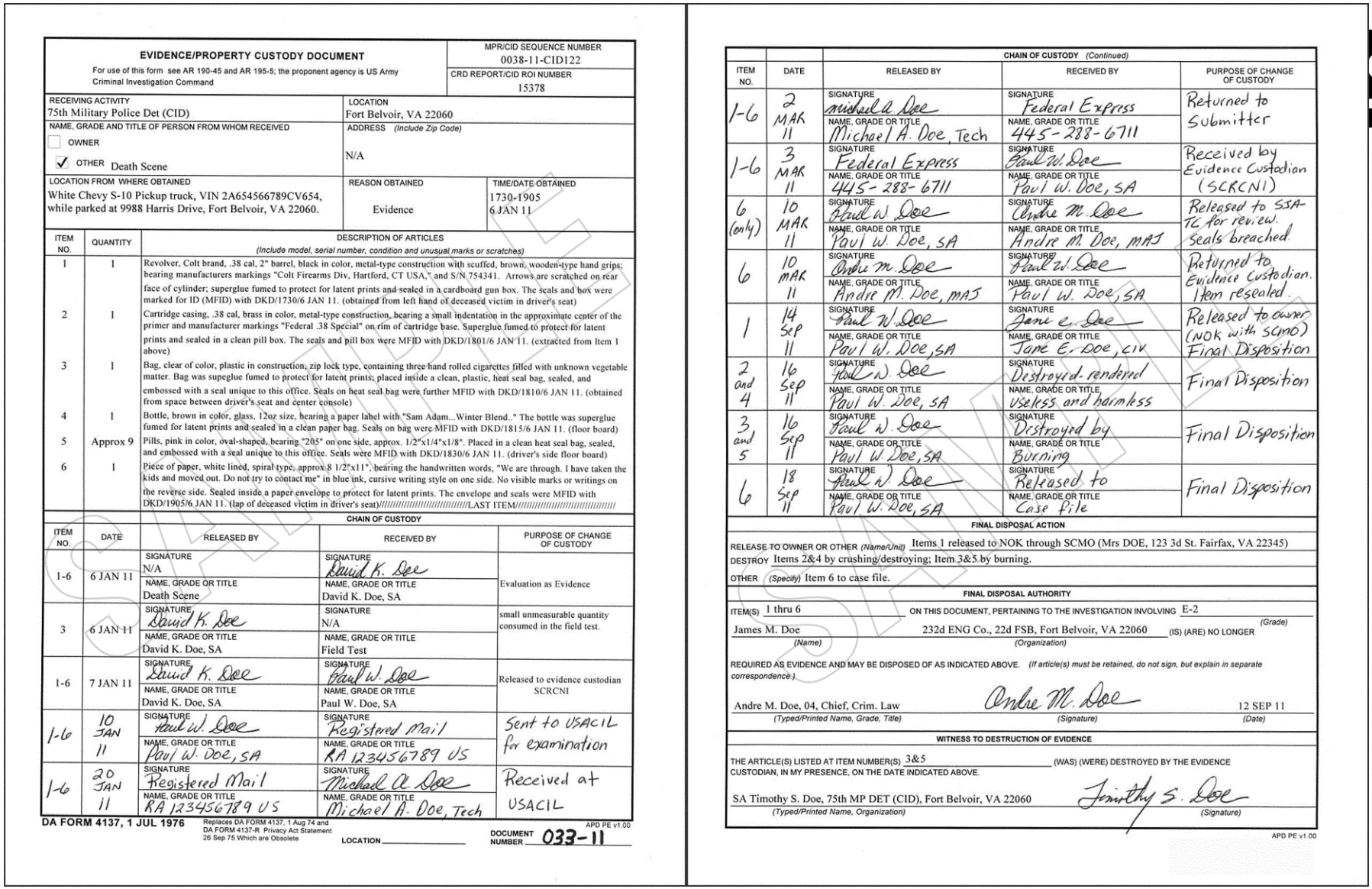
A chain of custody document records the continuity of evidence possession

- One of the most important aspects of authentication
- Demonstrate that digital evidence has not been altered since it was collected

Allegations of improper evidence handling may surface if there is no proper chain of custody

- Can be argued that evidence may have been altered, replaced, or contaminated in some other fashion
- Misidentification of evidence, contamination of evidence, and / or loss of evidence or pertinent elements may result from breaking chain of custody

Each person who handled the evidence may be required to testify that the evidence was properly preserved and not altered from the time it was collected through to the subsequent stages of the investigation



EVIDENCE/PROPERTY CUSTODY DOCUMENT

For use of this form see AR 190-45 and AR 195-5; the proponent agency is US Army Criminal Investigation Command

MPR/CID SEQUENCE NUMBER: 0038-11-CID122
CRD REPORT/CID ROI NUMBER: 15378

RECEIVING ACTIVITY: 75th Military Police Det (CID)	LOCATION: Fort Belvoir, VA 22060
NAME, GRADE AND TITLE OF PERSON FROM WHOM RECEIVED: ☐ OWNER ☑ OTHER Death Scene	ADDRESS (Include Zip Code): N/A
LOCATION FROM WHERE OBTAINED: White Chevy S-10 Pickup truck, VIN 2A654566789CV654, while parked at 9988 Harris Drive, Fort Belvoir, VA 22060.	REASON OBTAINED: Evidence / TIME/DATE OBTAINED: 1730-1905 6 JAN 11

ITEM NO.	QUANTITY	DESCRIPTION OF ARTICLES (Include model, serial number, condition and unusual marks or scratches)
1	1	Revolver, Colt brand, .38 cal, 2" barrel, black in color, metal-type construction with scuffed, brown, wooden-type hand grips; bearing manufacturers markings "Colt Firearms Div, Hartford, CT USA," and S/N 754341. Arrows are scratched on rear face of cylinder; superglue fumed to protect for latent prints and sealed in a cardboard gun box. The seals and box were marked for ID (MFID) with DKD/1730/6 JAN 11. (obtained from left hand of deceased victim in driver's seat)
2	1	Cartridge casing, .38 cal, brass in color, metal-type construction, bearing a small indentation in the approximate center of the primer and manufacturer markings "Federal .38 Special" on rim of cartridge base. Superglue fumed to protect for latent prints and sealed in a clean pill box. The seals and pill box were MFID with DKD/1801/6 JAN 11. (extracted from Item 1 above)
3	1	Bag, clear of color, plastic in construction, zip lock type, containing three hand rolled cigarettes filled with unknown vegetable matter. Bag was supeglue fumed to protect for latent prints, placed inside a clean, plastic, heat seal bag, sealed, and embossed with a seal unique to this office. Seals on heat seal bag were further MFID with DKD/1810/6 JAN 11. (obtained from space between driver's seat and center console)
4	1	Bottle, brown in color, glass, 12oz size, bearing a paper label with "Sam Adam...Winter Blend.." The bottle was superglue fumed for latent prints and sealed in a clean paper bag. Seals on bag were MFID with DKD/1815/6 JAN 11. (floor board)
5	Approx 9	Pills, pink in color, oval-shaped, bearing "205" on one side, approx. 1/2"x1/4"x1/8". Placed in a clean heat seal bag, sealed, and embossed with a seal unique to this office. Seals were MFID with DKD/1830/6 JAN 11. (driver's side floor board)
6	1	Piece of paper, white lined, spiral type, approx 8 1/2"x11", bearing the handwritten words, "We are through. I have taken the kids and moved out. Do not try to contact me" in blue ink, cursive writing style on one side. No visible marks or writings on the reverse side. Sealed inside a paper envelope to protect for latent prints. The envelope and seals were MFID with DKD/1905/6 JAN 11. (lap of deceased victim in driver's seat)////////////////////////////LAST ITEM////////////////////////////

CHAIN OF CUSTODY

ITEM NO.	DATE	RELEASED BY	RECEIVED BY	PURPOSE OF CHANGE OF CUSTODY
1-6	6 JAN 11	SIGNATURE: N/A NAME, GRADE OR TITLE: Death Scene	SIGNATURE: David K. Doe NAME, GRADE OR TITLE: David K. Doe, SA	Evaluation as Evidence
3	6 JAN 11	SIGNATURE: David K. Doe NAME, GRADE OR TITLE: David K. Doe, SA	SIGNATURE: N/A NAME, GRADE OR TITLE: Field Test	small unmeasurable quantity consumed in the field test.
1-6	7 JAN 11	SIGNATURE: David K. Doe NAME, GRADE OR TITLE: David K. Doe, SA	SIGNATURE: Paul W. Doe NAME, GRADE OR TITLE: Paul W. Doe, SA	Released to evidence custodian SCRCNI
1-6	10 JAN 11	SIGNATURE: Paul W. Doe NAME, GRADE OR TITLE: Paul W. Doe, SA	SIGNATURE: Registered Mail NAME, GRADE OR TITLE: RA 123456789 US	Sent to USACIL for examination
1-6	20 JAN 11	SIGNATURE: Registered Mail NAME, GRADE OR TITLE: RA 123456789 US	SIGNATURE: Michael A. Doe NAME, GRADE OR TITLE: Michael A. Doe, Tech	Received at USACIL

DA FORM 4137, 1 JUL 1976 — Replaces DA FORM 4137, 1 Aug 74 and DA FORM 4137-R Privacy Act Statement 26 Sep 75 Which are Obsolete — APD PE v1.00

LOCATION _____ DOCUMENT NUMBER 033-11

CHAIN OF CUSTODY (Continued)

ITEM NO.	DATE	RELEASED BY	RECEIVED BY	PURPOSE OF CHANGE OF CUSTODY
1-6	2 MAR 11	SIGNATURE: Michael A. Doe NAME, GRADE OR TITLE: Michael A. Doe, Tech	SIGNATURE: Federal Express NAME, GRADE OR TITLE: 445-288-6711	Returned to Submitter
1-6	3 MAR 11	SIGNATURE: Federal Express NAME, GRADE OR TITLE: 445-288-6711	SIGNATURE: Paul W. Doe NAME, GRADE OR TITLE: Paul W. Doe, SA	Received by Evidence Custodian (SCRCNI)
6 (only)	10 MAR 11	SIGNATURE: Paul W. Doe NAME, GRADE OR TITLE: Paul W. Doe, SA	SIGNATURE: Andre M. Doe NAME, GRADE OR TITLE: Andre M. Doe, MAJ	Released to SSA-TC for review. Seals breached
6	10 MAR 11	SIGNATURE: Andre M. Doe NAME, GRADE OR TITLE: Andre M. Doe, MAJ	SIGNATURE: Paul W. Doe NAME, GRADE OR TITLE: Paul W. Doe, SA	Returned to Evidence Custodian. Item resealed.
1	14 Sep 11	SIGNATURE: Paul W. Doe NAME, GRADE OR TITLE: Paul W. Doe, SA	SIGNATURE: Jane E. Doe NAME, GRADE OR TITLE: Jane E. Doe, CIV	Released to owner (NOK with SCMO) Final Disposition
2 and 4	16 Sep 11	SIGNATURE: Paul W. Doe NAME, GRADE OR TITLE: Paul W. Doe, SA	SIGNATURE: Destroyed - rendered NAME, GRADE OR TITLE: Useless and harmless	Final Disposition
3 and 5	16 Sep 11	SIGNATURE: Paul W. Doe NAME, GRADE OR TITLE: Paul W. Doe, SA	SIGNATURE: Destroyed by NAME, GRADE OR TITLE: Burning	Final Disposition
6	18 Sep 11	SIGNATURE: Paul W. Doe NAME, GRADE OR TITLE: Paul W. Doe, SA	SIGNATURE: Released to NAME, GRADE OR TITLE: Case File	Final Disposition

FINAL DISPOSAL ACTION

RELEASE TO OWNER OR OTHER (Name/Unit): Items 1 released to NOK through SCMO (Mrs DOE, 123 3d St. Fairfax, VA 22345)
DESTROY: Items 2&4 by crushing/destroying; Item 3&5 by burning.
OTHER (Specify): Item 6 to case file.

FINAL DISPOSAL AUTHORITY

ITEM(S) 1 thru 6 ON THIS DOCUMENT, PERTAINING TO THE INVESTIGATION INVOLVING E-2 (Grade)
James M. Doe (Name) 232d ENG Co., 22d FSB, Fort Belvoir, VA 22060 (Organization) (IS) (ARE) NO LONGER

REQUIRED AS EVIDENCE AND MAY BE DISPOSED OF AS INDICATED ABOVE. (If article(s) must be retained, do not sign, but explain in separate correspondence.)

Andre M. Doe, 04, Chief, Crim. Law (Typed/Printed Name, Grade, Title) — Andre M. Doe (Signature) — 12 SEP 11 (Date)

WITNESS TO DESTRUCTION OF EVIDENCE

THE ARTICLE(S) LISTED AT ITEM NUMBER(S) 3&5 (WAS) (WERE) DESTROYED BY THE EVIDENCE CUSTODIAN, IN MY PRESENCE, ON THE DATE INDICATED ABOVE.

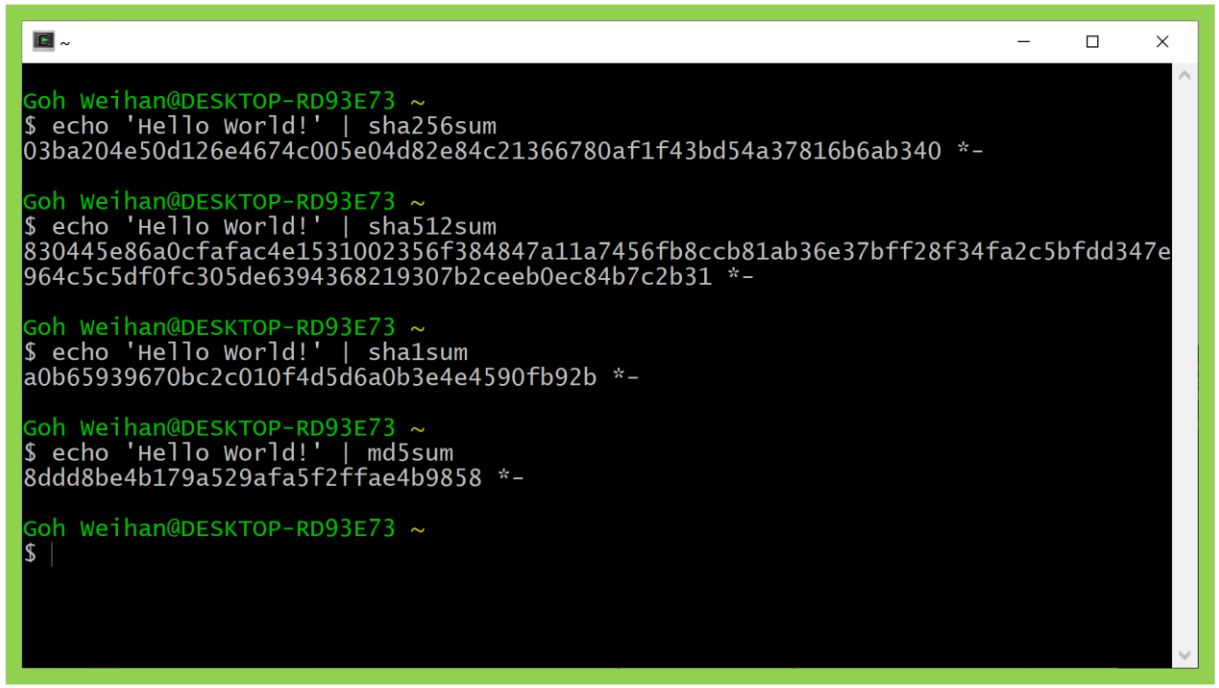
SA Timothy S. Doe, 75th MP DET (CID), Fort Belvoir, VA 22060 (Typed/Printed Name, Organization) — Timothy S. Doe (Signature)

APD PE v1.00

SAMPLE

Chain of custody report example (DA Form 4137; US Army)

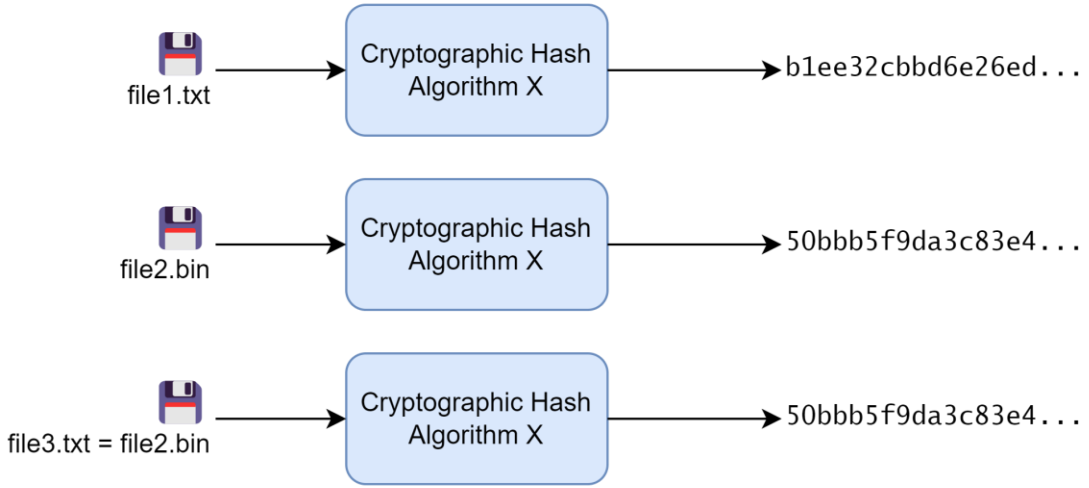
Evidence Integrity



Integrity checks are used to support authentication by showing that evidence has not been altered since collected

- Generally, involves comparing digital 'fingerprints'
- Digital fingerprinting typically done using **cryptographic hash functions**
  - SHA-2 set of functions (e.g., SHA-256, SHA-512) are commonly used nowadays
  - You may still encounter MD5 or SHA-1, but if given a choice, you may want to avoid them

Message Digest / Cryptographic Hash Functions



For now, think of message digest / cryptographic hash functions as a black box

- Accepts a *message* (e.g., string, file, disk, etc.) as input, and computes a *message digest* (sometimes called *hash value*) as output

- The exact copy of an input will have the **exact same message digest**

Introducing even the slightest change to an input will result in a totally different message digest

$$message\_digest = \text{Cryptographic\_Hash\_Function}(message)$$

$$h = \text{hash}(m)$$

Message Digest / Cryptographic Hash Functions

Message 1

Message: **"His name is John"**

MD5 (128-bit digest)

`cda93362633cf7c8d3954d4ba6582aba`

SHA-256 (256-bit digest)

`a53f61139838fe55e53a5d9daeb996af6972fca`
`4d8797c544ab2842daefef27f`

Message 2

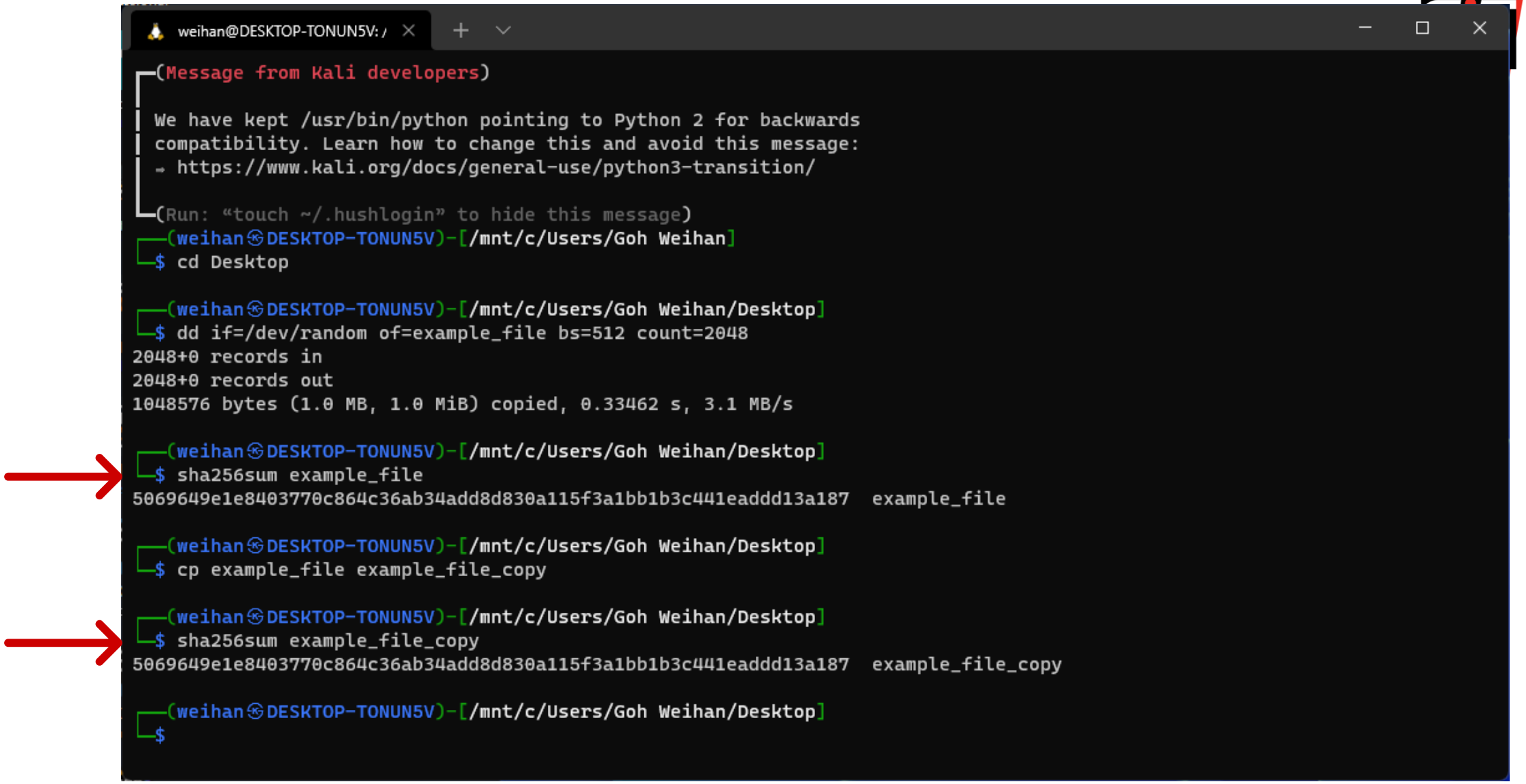
Message: **"His name is Jonn"**

MD5 (128-bit digest)

`129a7bdc45ec220a67ec48bfb0014e72`

SHA-256 (256-bit digest)

`dc911cd95039ce95596f271202fc5a5f156ddfa`
`617647613558dac8e87d7479b`


weihan@DESKTOP-TONUN5V:
(Message from Kali developers)
We have kept /usr/bin/python pointing to Python 2 for backwards
compatibility. Learn how to change this and avoid this message:
→ https://www.kali.org/docs/general-use/python3-transition/
(Run: "touch ~/.hushlogin" to hide this message)
(weihan㉿DESKTOP-TONUN5V)-[/mnt/c/Users/Goh Weihan]
$ cd Desktop
(weihan㉿DESKTOP-TONUN5V)-[/mnt/c/Users/Goh Weihan/Desktop]
$ dd if=/dev/random of=example_file bs=512 count=2048
2048+0 records in
2048+0 records out
1048576 bytes (1.0 MB, 1.0 MiB) copied, 0.33462 s, 3.1 MB/s
(weihan㉿DESKTOP-TONUN5V)-[/mnt/c/Users/Goh Weihan/Desktop]
$ sha256sum example_file
5069649e1e8403770c864c36ab34add8d830a115f3a1bb1b3c441eaddd13a187 example_file
(weihan㉿DESKTOP-TONUN5V)-[/mnt/c/Users/Goh Weihan/Desktop]
$ cp example_file example_file_copy
(weihan㉿DESKTOP-TONUN5V)-[/mnt/c/Users/Goh Weihan/Desktop]
$ sha256sum example_file_copy
5069649e1e8403770c864c36ab34add8d830a115f3a1bb1b3c441eaddd13a187 example_file_copy
(weihan㉿DESKTOP-TONUN5V)-[/mnt/c/Users/Goh Weihan/Desktop]
$

Properties of Cryptographic Hash Functions

SINGAPORE INSTITUTE OF TECHNOLOGY

Preimage resistance

Collision resistance

Second preimage resistance

Properties of Cryptographic Hash Functions

Preimage resistance

- Given a hash value h_1, it should be *computationally infeasible* to find a message m such that

$$h_1 = \text{hash}(m)$$

- Example
  - `c7c931e5abf68d5804232a90530e7533a035d5e595d4c3194ae6fdbaee8a9fb5`
  - You should not be able to find *any* message that hashes to the above SHA-256 hash value

Collision resistance

- It should be *computationally infeasible* to find any two different messages m_1 and m_2 such that

$$\text{hash}(m_1) = \text{hash}(m_2)$$

- Example
  - You should not be able to find any pair of messages m_1 and m_2 that produces the same hash value when hashed using SHA-256

Second preimage resistance

- Given a message m_1, it should be *computationally infeasible* to find any message m_2 such that

$$\text{hash}(m_1) = \text{hash}(m_2)$$

- Example
  - m_1 = *"some message 9lx4"*
  - You should not be able to find a different message m_2 that produces the same hash value as SHA-256(m_1)

The Digital Investigation

The Digital Investigation

Know the goals of your investigation

Have proper and systematic processes in place to identify, acquire, and examine evidence

Have in-depth technical understanding of what you will be facing

Seek Questions

Your investigation will likely involve a series of questions, answers, and questions that stem from your answers...

Finding an answer to a previous question may yield more questions that leads to more answers

Goal: ***Find out if equipment X has been sabotaged***

Question: How can someone input codes / malware / commands into equipment X?

Answer: *One avenue is through the USB port; it is important to note also that there are no network hardware installed by default on the equipment*

Question: How was the USB port misused in this case?

Answer: *Analysis of OS logs show that a USB mass storage device was plugged in to equipment X and...*

Conclusions and Opinions

Conclusion is a judgement based on facts

"Based on forensic analysis of the employee's email account and system logs, it is concluded that the breach was initiated through a phishing email received on June 10, 2024, at 9:15 AM. The email contained a malicious attachment, which, when opened, deployed malware onto the employee's device. The malware then ..."

Opinion is a judgement or belief without certainty or proof, but backed by science and / or experience

"Given the analysis of the malware's code and the patterns of its propagation, it is my opinion that the breach likely originated from a phishing email that tricked an employee into downloading a malicious attachment. This assessment is based on the known delivery methods of similar malware strains found in previous incidents."

The Digital Investigation Process

Follow the digital investigation process model adopted by your organization

Ensure that forensic soundness and evidence integrity can be preserved

Comply with laws and any other regulations / policies in place; breaching them may jeopardize the investigation (and your career!)

Follow a repeatable, well-documented set of steps so that findings can be reproduced and validated

Preparing to Handle a Scene

Questions, and More Questions

What happened?

Who is in charge?

Where did the incident happen?

What is to be seized and preserved?

What else do we need to do at the scene?

Are we required to be covert, or can we be overt?

Is it localized to just that one location?

Under which jurisdiction are we dealing with?

The Scene

A scene may or may not be obvious

- e.g., Suspected data theft by ex-employee; no evidence of theft, but exist some suspicion

There could be specific areas where investigator can enter and protocols to follow

Always find out what you can, and what you cannot do!!!

Determine Who is in Charge

Likely, it is not you 😳

If not you (and again, it is likely not you…)

- Identify the chain of command, and document who has what authority

Preparing to Handle a Scene

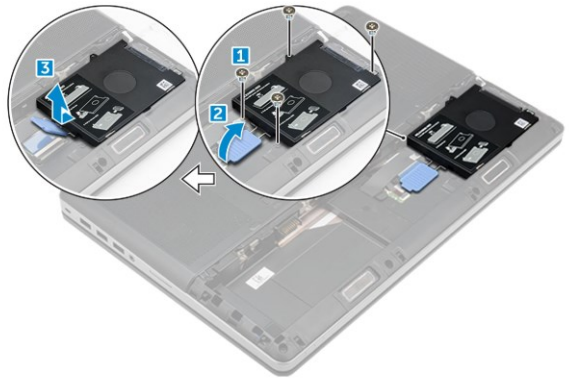
Find out about devices and media of interest

- Computer systems, storage media, peripherals, consumer electronics, online accounts, etc.
- Know their characteristics, physical locations, and possible use of encryption / security mechanisms / anti-forensics, etc.

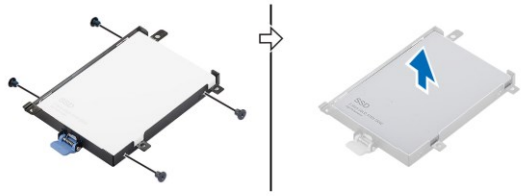
Useful for determining the equipment, software, storage media, etc. that *you* will require

Sources of information about devices and media of interest

- Device documentation
- Interviewing (trusted) individuals
- In certain cases, surveillance



4 Remove the M3.0x3.0 screws that secure the hard drive. Lift the hard drive from the bracket.



Installing the hard drive

1 Replace the M3.0x3.0 screws to secure the hard drive to the hard drive bracket.
2 Insert the hard drive into its slot in the computer.
3 Replace the M3.0x3.0 screws to secure the hard drive to the computer.
4 Install the:
  a battery
  b battery cover
5 Follow the procedure in After working inside your computer.

12 Disassembly and reassembly

Preparing to Handle a Scene

Prepare questions for interviewing individuals at the crime scene

- Ensure information is gathered and documented in a consistent manner
- Can be a formal questionnaire

Things to request for should include, but not limited to

- Passwords and encryption keys from all individuals with access to systems
- Details about all mobile devices, removable storage media, backup systems, etc.
- Details about other locations where data may be stored

Preparing to Handle a Scene

Consider the suspect's technical competency and skill level

- A highly technical suspect may necessitate assistance from more experienced / skilled investigators
- May sometimes be necessary to employ independent consultants / experts
- Plan well ahead **what to expect**, **what to look out for**, and **what actions to take or not to take** when a situation arise

Preparing to Handle a Scene

Some strategy is needed for

- Securing the crime scene
- Surveying and documenting the crime scene
- Collecting digital evidence

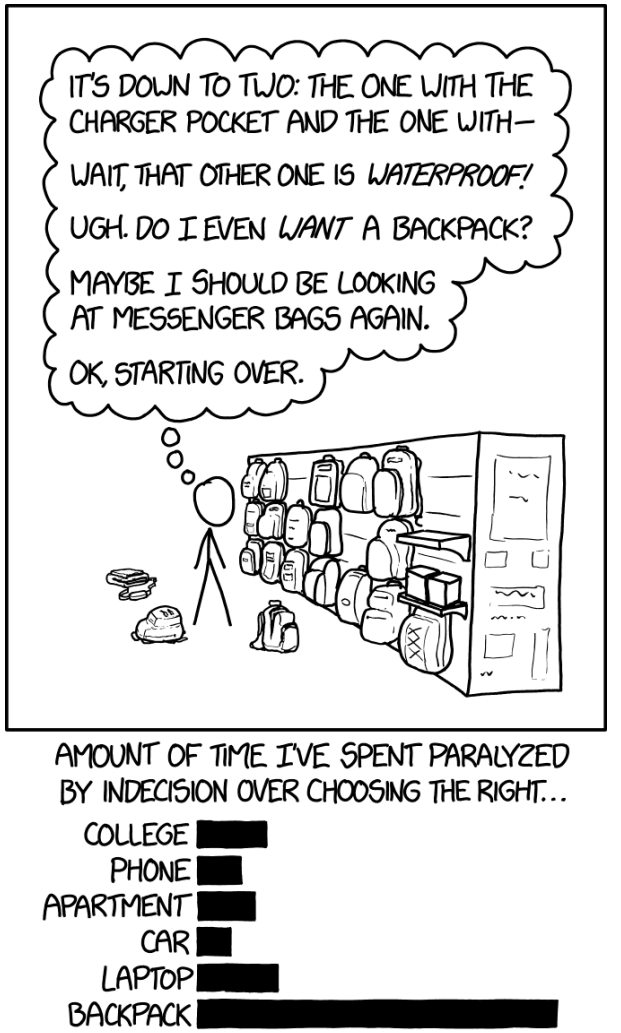
Every case is different

- Amount of planning / preparation required depends on the case and situation
- **No two cases are the same!!!**

Things to Bring to the Scene

Items to bring to the scene, include, but not limited to

- Mobile workstation or laptop
- Hardware, software, and equipment to perform forensic tasks / collect digital data
- Data storage devices
- Material to preserve and document digital evidence
- Tools to for disassembling systems
- Photography / videography equipment to document the scene



Things to Bring to the Scene

Equipment to perform forensic tasks / collect digital data, e.g.,

- Forensic disk duplicators + write blockers
- Forensics software + associated license keys
- Live bootable disks and CDs (e.g., Kali, etc.)
- Mobile device forensic kits + cables
- Data cables (e.g., USB-C, micro-USB, lightning, etc.), straight and crossover network cables
- **Extra keyboard and mouse, external optical drive, etc.**

Forensic imager / duplicator (Tableau TX1 with attached TX1-S1 drive bay)

Forensic write blocker (Tableau T8u)

Things to Bring to the Scene

Data storage devices to store collected data

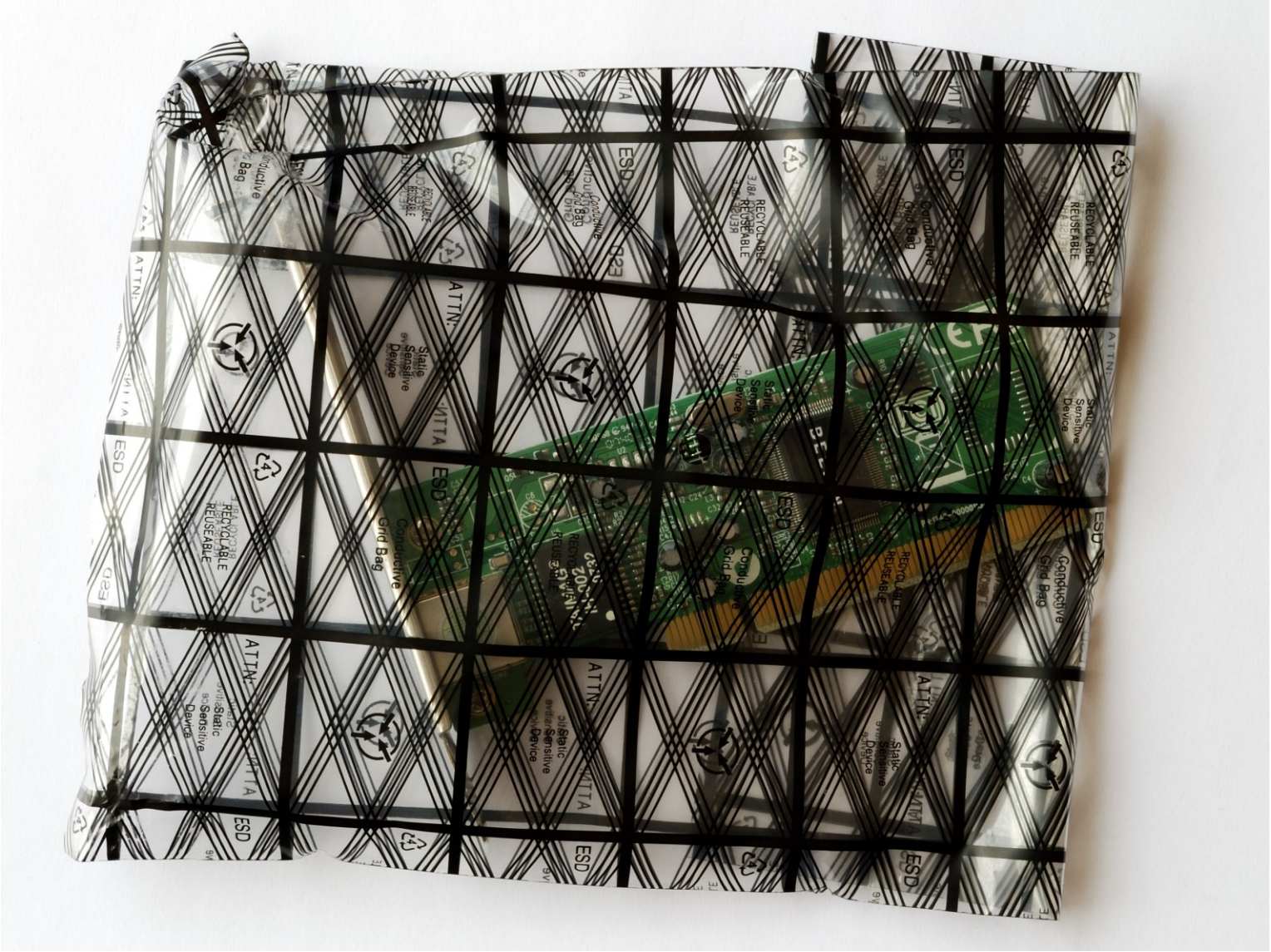
- Hard disks / SSDs for storing disk images, USB drives for storing smaller amounts of data, etc.
- Bring **large capacity disks** to avoid having to divide images / data into smaller files
- Ensure media is **blank and sanitized** to avoid confusion between data collected at different crime scenes

Things to Bring to the Scene

Material to preserve and document digital evidence properly, such as

- Evidence containers, labels, pens, tape, and cable ties to uniquely mark and package each item being treated as evidence

- Specialized storage bags such as **faraday bags** and **antistatic bags**
  - **Antistatic bags** to store components prone to damage by electrostatic discharge (ESD)
  - **Faraday bags** to isolate device from radio-based interference



Antistatic bag

Antistatic bag

Faraday bag (OffGrid Utility Faraday Bag Window)

Things to Bring to the Scene

Tools to for disassembling systems

- Screwdrivers with a wide variety of attachments
  - Or a set of screwdrivers of different sizes
- Several types of pliers, especially a needle nose pliers
- Wire cutters, flashlight, etc.

Things to Bring to the Scene

Camera with enough batteries to document the scene

- Ensure the date, time, and time zone are properly set
- Configure the camera to both place a **timestamp on the photo** and **embed the timestamp in the photo meta-data**

Bring blank, sanitized, removable storage cards to avoid confusion between photographs taken at different crime scenes

Always Have a Backup Plan

"Everybody has a plan until they get punched in the mouth"

- Mike Tyson

Important to have contingency

- **Bring extra storage and equipment**
- **Know where and how to quickly purchase additional equipment**

If planned well, most of your plan should still work, but you will need to deal with the now

No plan survives contact with the scene

- Rare to have perfect foresight before entering a scene
- Common to encounter things that were not part of the original plan, e.g.,
  - Additional computers
  - High-capacity backup media
  - Unusual configurations
  - Mobile devices
  - etc.

Surveying the Scene

When on the Scene

Ensure no unauthorized person has access to the electronic devices at scene

Do not accept help / technical assistance from unauthorized persons

Peripherals (e.g., mouse, keyboard, etc.) and physical surfaces may contain other evidence such as fingerprints or DNA

Human safety first, always

- People may not be at risk, but not entirely true all the time
  - e.g., Hostage situation, kidnaps, pedophilia, etc.
- After that, safety and integrity of the evidence

Surveying the Scene

Surveying and documenting

- **To find *all* potential sources of digital evidence**
- **To make informed, reasoned decisions about what digital evidence to preserve at the crime scene**

In ideal scenario, preserve every potential source of digital evidence

- Not very feasible in reality… 😟
- Constrained by law, time, resources, and interests of business 😟
  - Generally authorized to preserve only what is directly pertinent to the investigation
  - You can be faulted for privacy violations and exceeding legal authorization

Surveying the Scene

When first entering a scene

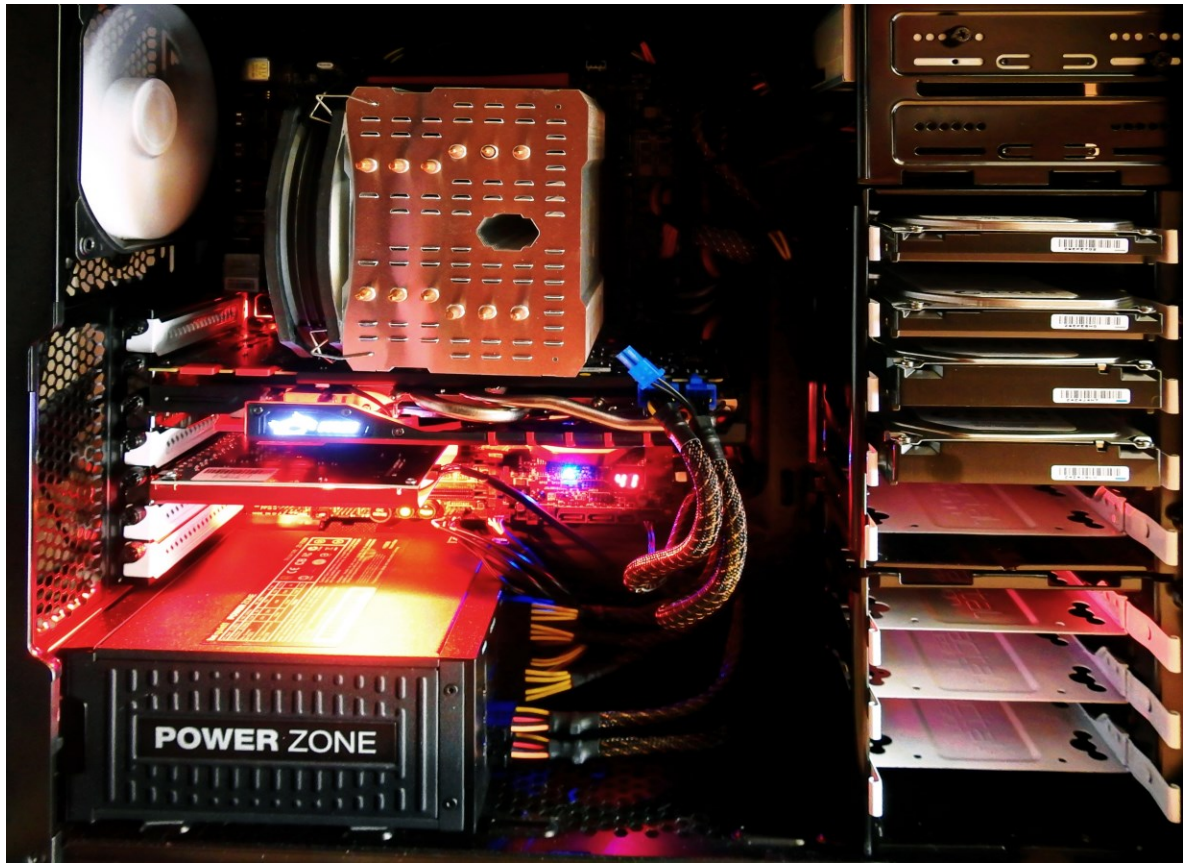
- Avoid being too narrow in the survey process
- Trying to look for specific items may lead to missed evidence / opportunities

Digital evidence may be found in unexpected places

Surveying the Scene

Where can you find data?

- Persistent storage devices within computer systems, e.g., hard disks, solid state drives, etc.
- Active memory (RAM), network, and other volatile data storage within computer systems
- **Devices other than computer systems**



Surveying the Scene

Other potential information containers

- External storage devices (e.g., hard disks, flash drives, memory cards, network storage, etc.)
- Mobile phones, tablets, digital media players
- Game consoles, smart TVs, home entertainment devices
- Printers, copiers, scanners
- Telecommunication equipment, routers, switches, etc.
- Digital cameras, digital audio recorders, digital camcorders, etc.

Surveying the Scene

Devices that you find may be in various power states

Devices have different power profiles and may support different power modes

Computer systems may be in one of few possible power states, e.g.,

- Suspend to RAM (typically referred to as *standby* or *sleep*)
- Suspend to disk (i.e., *hibernate*)
- Soft-off, mechanical off, etc.

How do you know if a computer system is currently *powered on* or *powered off*? 

How do you know if a computer system is currently *on standby* or *hibernating*? 

Surveying the Digital Crime Scene

Backups may exist on-site or off-site

- Determine the hardware / software that was used to make the backups
- Determine if backups are *only* accessible via the type of hardware / software that created them

Advisable to collect unusual backup hardware / software

Surveying the Digital Crime Scene

Items that contain incriminating or valuable information may be physically hidden

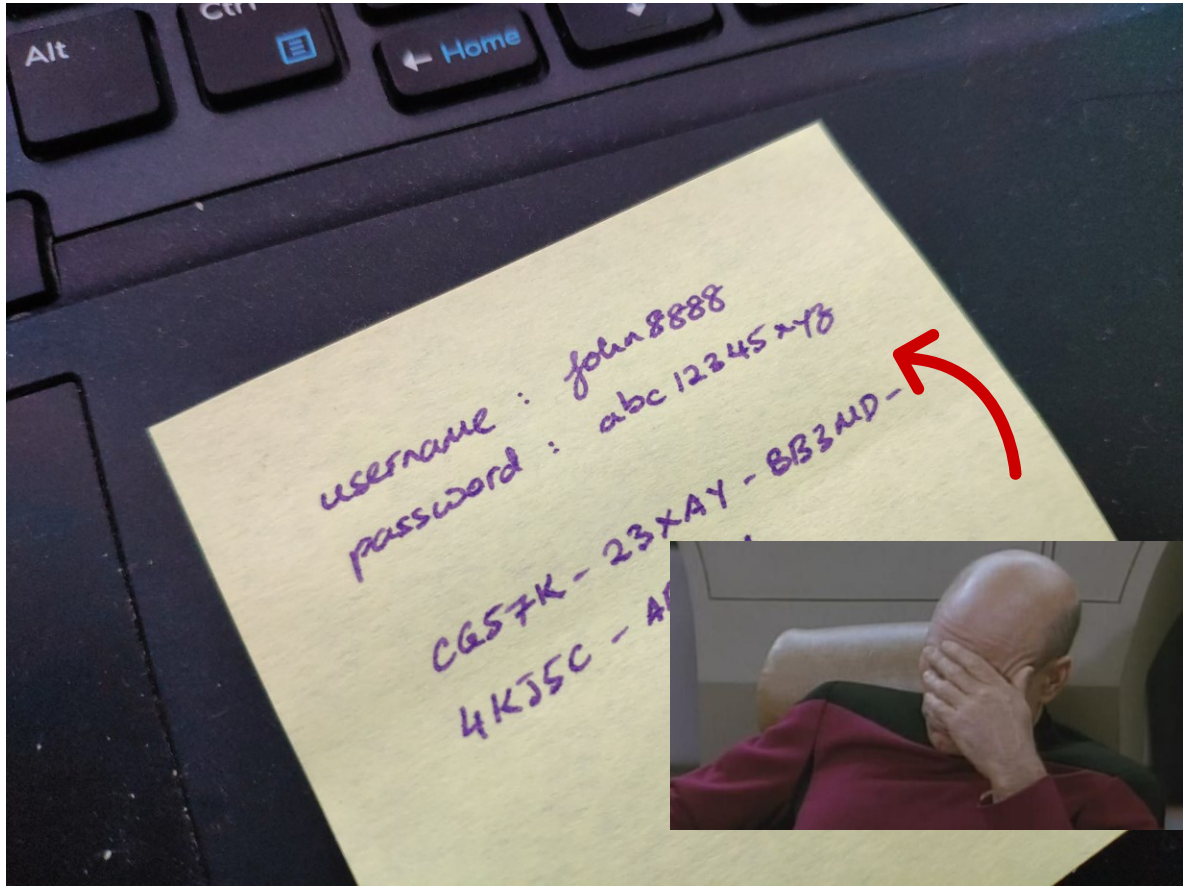
- Be detail-oriented when surveying the crime scene
- Look for **hidden items** e.g., by following network cables, looking in drop ceilings, raised flooring, etc.
- Be alert to the possibility that some items may be hard to find

Surveying the Digital Crime Scene

Look for account details, passwords, important phone numbers, software and hardware documentation, etc.

- Individuals may write **down account details and passwords** for their various accounts
  - **Especially true for hackers (why?)**

- Information may also be obtained through interviews with people involved



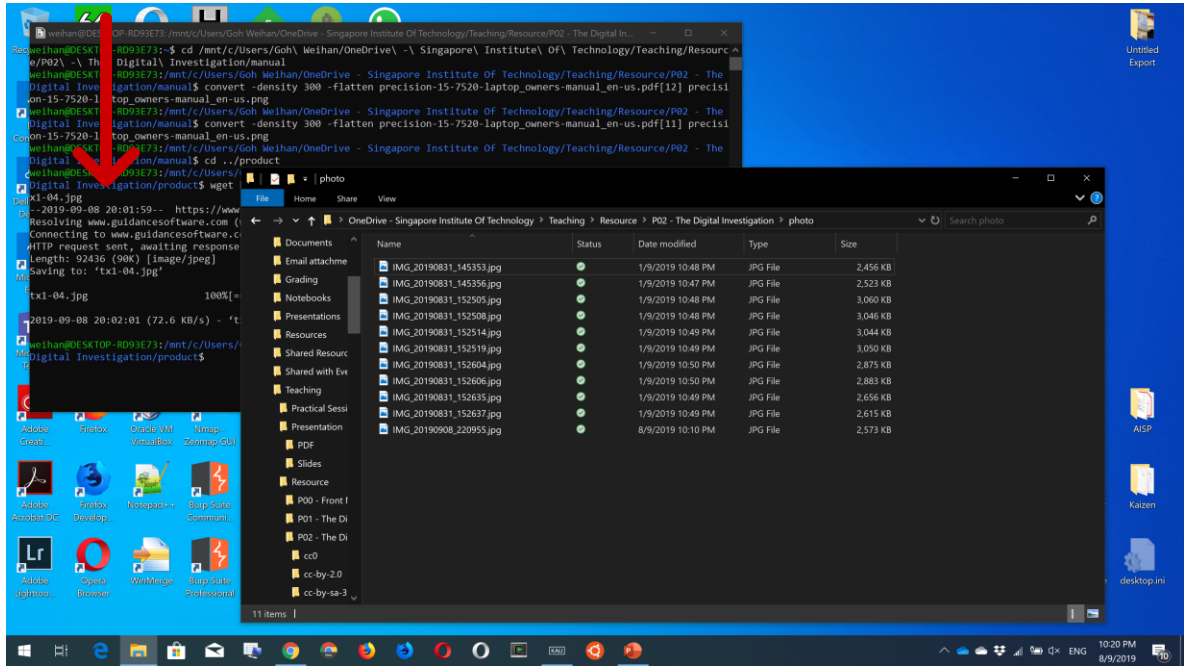
Surveying the Digital Crime Scene

Look out for the types of documentation and books around the scene

- Documentation may contain details about hardware, software, backup process, etc.
- Books on technical topics can help assess the **technical skill level** of the suspect
- Computer printouts (e.g., printed pages, etc.) may contain valuable evidence
  - Printers may contain **device-specific identifiers**
  - Marks on printouts may be **unique of the printer**

Surveying the Digital Crime Scene

Is the suspect downloading something?



Be extremely alert for volatile data that must be preserved immediately

- Look for systems that are **powered on**
- Generally, focus on RAM contents, but also include network connections
- Such data can help you find additional sources of evidence
  - Active network connections may direct you to other systems

Surveying the Digital Crime Scene

Photograph / record a video of the area and items of potential interest

- In situ; **in their current state / on-site**
  - Computers, laptops, removable media, mobile devices, cameras, etc.
  - Record the fact that the items were found at the scene
- Pay attention to **serial numbers** and **wiring** to help identify / reconstruct equipment later
- Photographs should also convey **item size** if possible (how?)

Consider removing computer casings and photographing internal components, including close-ups of jumper settings and other details

For running systems, photograph contents of the computer screen

If data destruction is occurring, consider disconnecting power to the system immediately

Surveying the Digital Crime Scene

Create diagrams of complex systems to ensure that each computer or component is independently documented and correctly identified

- Rack of servers, networks, cabling, etc.
  - Document each cable and its connection point
- Such diagram can assist you in identifying each component and how they are connected

Surveying the Digital Crime Scene

Suspect has this connected to PC

Create an inventory of all items and their characteristics

- Manufacturer, model, and serial number, etc.

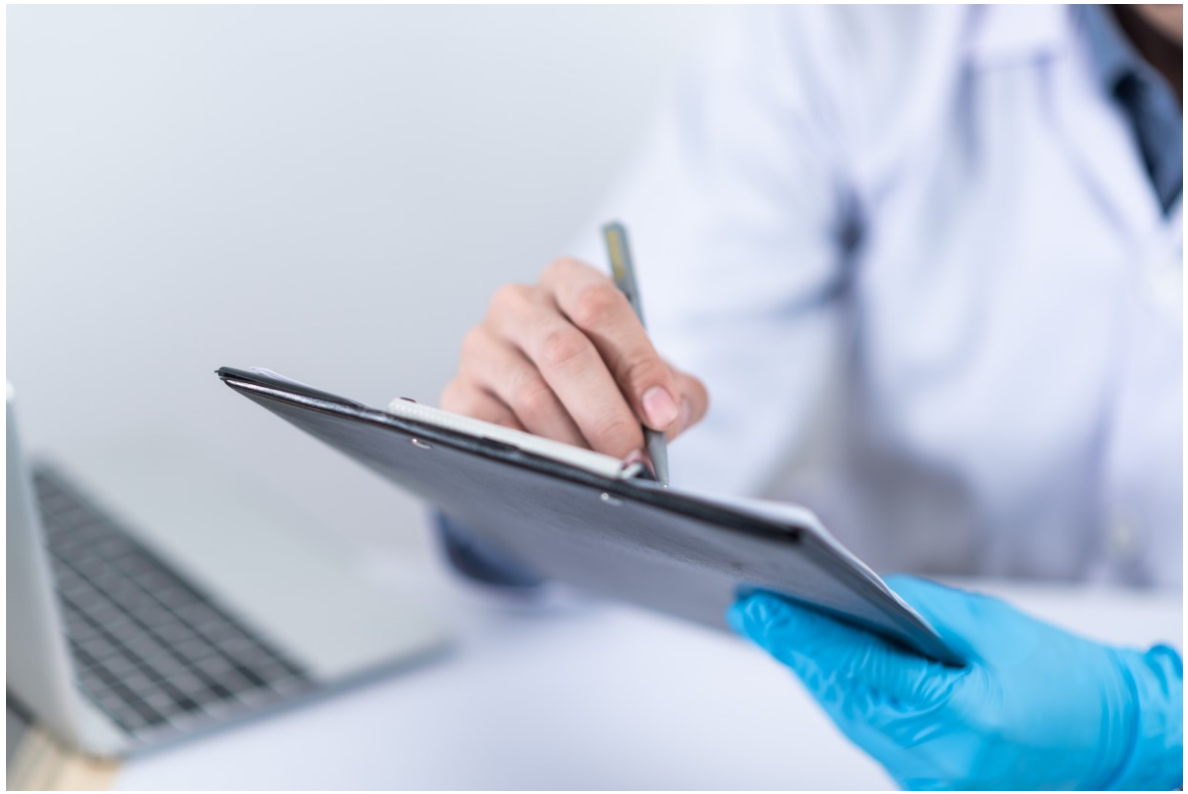
Specialized equipment should be documented, even if its purpose is not known

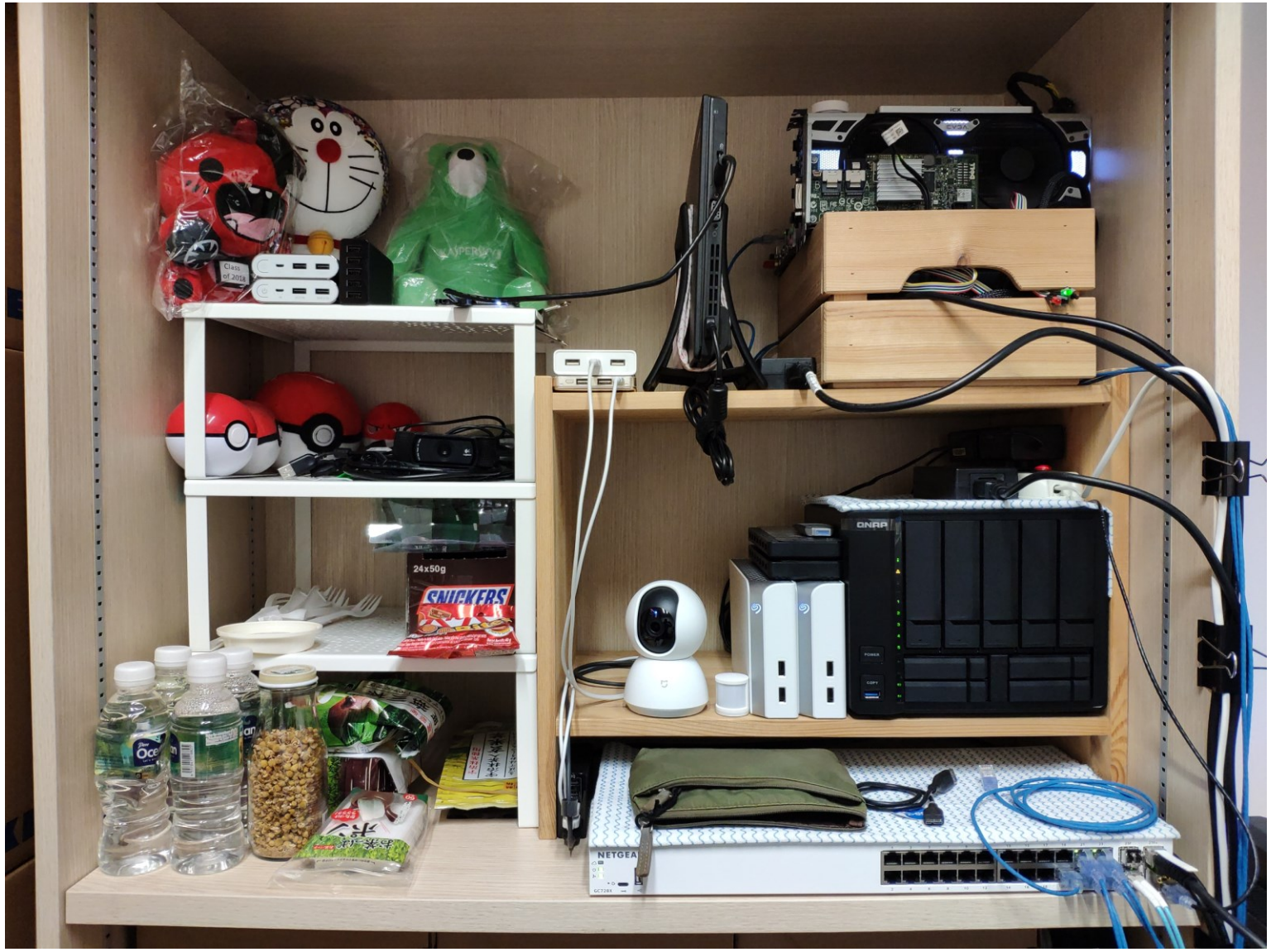
- e.g., Antennas, custom-made hardware / circuits, triggers / switches, etc.

Surveying the Digital Crime Scene

Other records to keep

- Sketch map of scene
- Details of all persons present where computers are located
- Remarks / comments / information offered by user(s) of computer(s)
- Actions taken at scene showing exact time





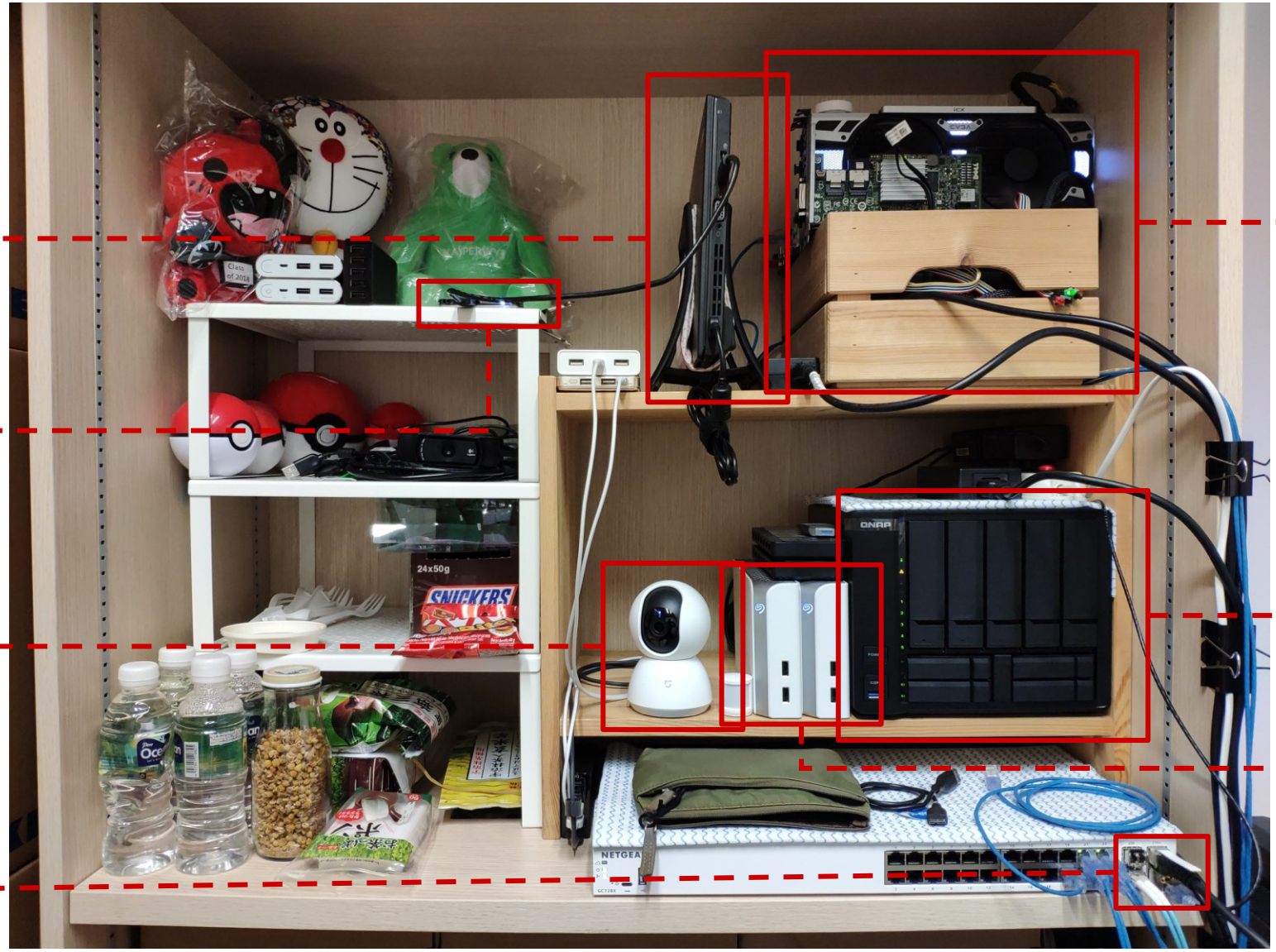
Where are the evidence?

Lenovo X240 laptop
One DDR3L slot
One SATA slot
One mSATA slot

USB hard disk
WD WDBUZG5000ABK
500GB
(Removed from enclosure)

Xiaomi Mi Home Security Camera 360° 1080P

Connected SFP and SFP+ ports

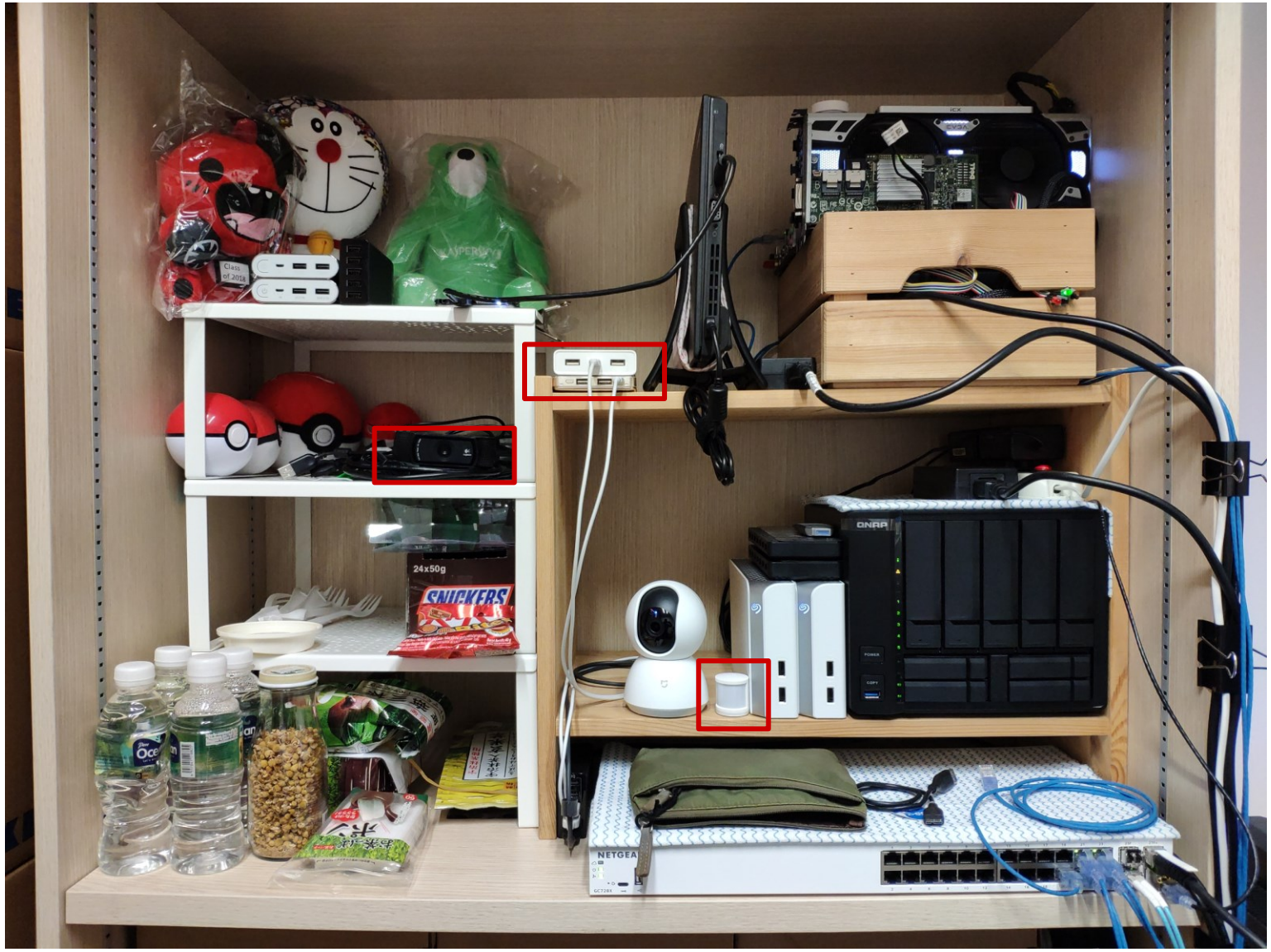


Computer on a crate
NVIDIA GTX 1080 GPU
Dell H200 SAS HBA
(connected to SSD)

QNAP TVS-951X 9-bay NAS
Unknown capacity

Seagate Backup Plus Hub for Mac, 2 units
Unknown capacity
8TB max

Where are the evidence?



Where are the evidence?

Preserving the Scene

Developing a Forensic Preservation Strategy

Triage inspection of digital evidence sources

- **Rapid inspection to determine priority in an investigation**
- **Helps you prioritize preservation efforts based on volatility and importance of the data**

Preserving digital evidence depends on

- The type of evidence
- The severity of the crime
- The importance of the evidence to the investigation

Approach to preserving a specific item of digital evidence depends on the circumstances

- No one approach fits all
  - e.g., In some situations, enough to take screen captures / make copies of select information from a system
  - e.g., In situations when there are too many files to copy or when the computer contains deleted data, may be necessary to preserve the entire computer / media that contains the contents

Decision to e.g., seize an entire computer versus create a forensic duplicate of the internal hard drive will be influenced by the role of the system

What to Preserve	Implications
Original hard drive	Any operations that are needed can be performed; however, physical damage / failure of the original hard drive may render its contents inaccessible
Forensic duplicate of original hard drive	The entire contents of the hard drive are preserved, including deleted data; however, it may be infeasible or not permitted under certain circumstances (e.g., very large hard drives, legal protection of certain files, etc.)
Select files from original hard drive	Other files on the hard drive that may be relevant will not be preserved; deleted data will not be preserved; furthermore, for the selected files, important information or metadata may be lost or misinterpreted during acquisition
Converted versions of files from original hard drive	For the selected files, important information or metadata may be lost or misinterpreted during conversion
Relevant portions of files from original hard drive	Digital investigators only know what is relevant at a certain moment and may miss other relevant information, particularly if new facts come to light later
Written notes detailing portions of files on original hard drive	This approach does not preserve the original digital evidence and is not feasible with large amounts of data

Various approaches to preserving digital evidence on a hard drive

Inside the Scene

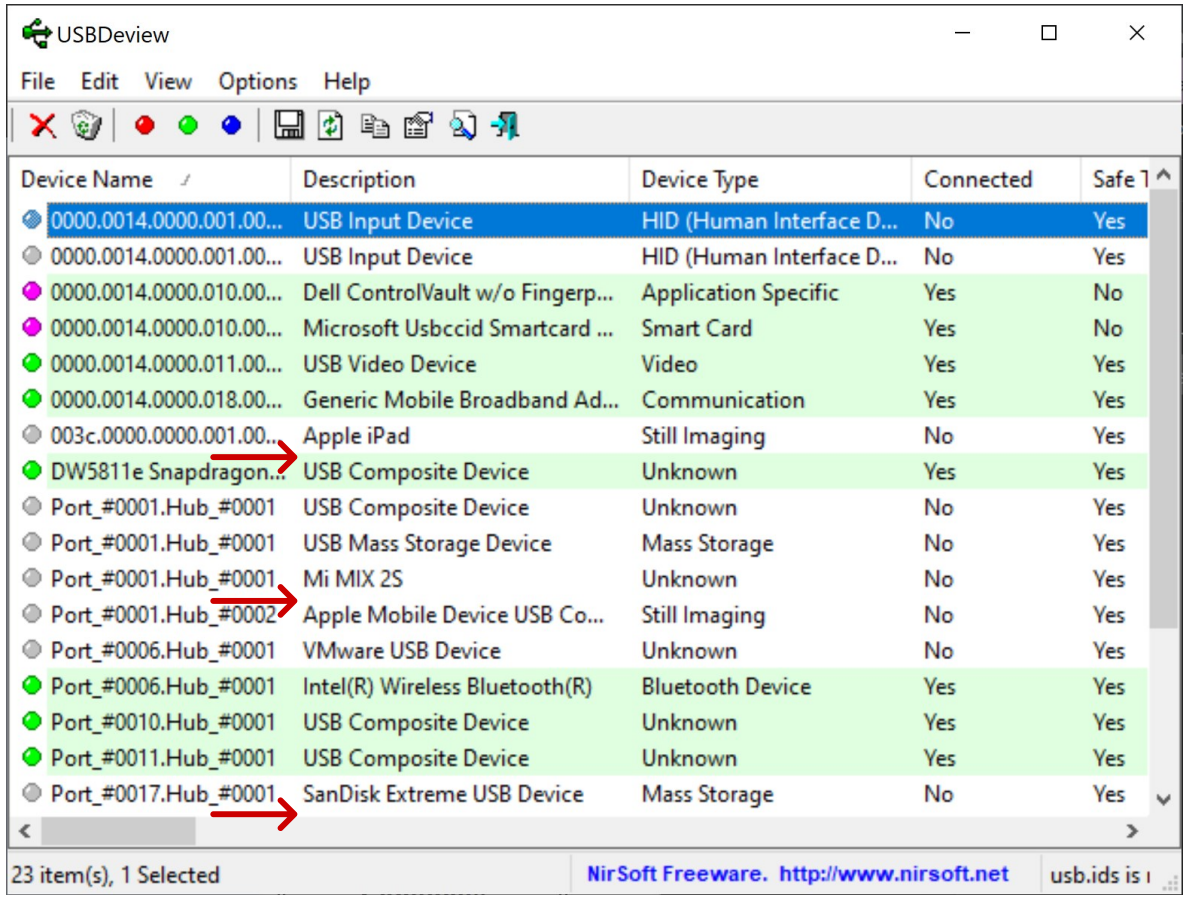
Perform preliminary inspection of each item

- Determine whether special actions are needed to preserve data
- Look for presence of encryption or other data concealment
- Look for password / passcode protection
  - May consider disabling such protection to prevent being locked out of the system / device later, especially with mobile devices

Inside the Scene

Information revealing other sources of evidence may not be directly apparent

- May only become apparent after some forensic analysis
  - e.g., Traces left by removable USB devices, network and cloud-based accounts, associations with other computers, etc.
- Triaging of systems can be used determine if there exist additional sources of digital evidence that should be preserved



Preserving the Scene

The preservation process involves

- Protecting the digital crime scene against **unauthorized alterations**
- Acquiring digital evidence in a manner that ensures its **authenticity and integrity**
  - e.g., Isolating systems from the network, imaging disks, securing relevant log files, collecting volatile data that would be lost when the system is turned off, etc.

Preservation can be a delicate process

Information may be lost almost immediately upon collection, e.g., RAM, network, etc.

May be necessary to perform operations directly on systems that contains evidence

Do not accept help / technical assistance from unauthorized persons

Controlling Entry Points to Scenes

Secure the physical scene by removing everyone to prevent them from contaminating evidence

May also be advisable, depending on the situation, to

- Disable biometric access and video surveillance equipment at the scene (why?)
- Change locks for all entry points and keep strict control over keys (why?)
- Disable network connectivity on all systems in the scene, and prevent remote access to systems

Considerations for "Wet" Forensics

Precautions must be taken when fingerprints and / or biological evidence may exist on the evidential computers

Consider using a separate set of input devices to prevent contamination and preserve fingerprints and biological evidence on the original input devices

Do not use chemicals that may damage electronics

- e.g., Aluminum powder when dusting for fingerprints on electronics (potential short-circuit)

Controlling Access to Systems

For mobile devices, it is recommended to isolate the devices from networks

- **Goal:** Prevent the device from receiving calls, messages, and / or commands that can alter or destroy evidence
- Keep in mind the connectivity options available on the mobile device (e.g., Wi-Fi, Bluetooth, etc.)
- How?


FOLD TOP OF FARADAY BAG OVER TWICE FOR PROPER SIGNAL SHIELDING
EDEC

Controlling Access to Systems

Information may be stored on network or servers at a different physical location

- Widespread use of networks and cloud services
  - e.g., Dropbox, OneDrive, Google Drive, iCloud, etc.
  - May not be immediately apparent that information is stored elsewhere

Even if you can determine where these locations are, you may not be able to reach / gain access to them immediately

Ideally, learn about remote storage locations during interviews in the preparation step of a digital investigation

Realistically, may only come after triage or forensic analysis of computer systems

Approach remote storage locations as secondary digital crime scenes

Freezing the Networked Scene

Preserving evidence on an organization's network may require the assistance of system and network administrators

- Copy all available network log files and disable log rotation to prevent overwriting of old logs
- Preserve all backup media; disable mechanisms that may overwrite backups
- Preserve e-mail and files on centralized servers
- Disable all of a suspect's user accounts

Investigators must not assume that network and system administrators know how to preserve digital evidence properly

Must supervise the process closely

- **Provide detailed instructions**
- **Clearly indicate what needs to be preserved**
- **Otherwise, may result in mishandled or missed digital evidence**

The system administrator may not be your friend

To Disconnect Power or Not to Disconnect Power

Stop and think!

For computers or mobile devices that are powered on and running

- Decide what actions to take prior to turning the system off
- Whether to turn the system off

Contents of volatile memory can be important

- e.g., Active processes, network connections, which account is running a certain process, etc.

Challenge: *How to capture volatile memory while making minimal changes to the system?*

At minimum, any information displayed on the screen should be documented

To Disconnect Power or Not to Disconnect Power

Disconnect power if

- Exist indicators that data is being overwritten / deleted
- The computer screen shows a typical desktop environment

In such cases, disconnecting power may preserve valuable information such last user login information, recently used documents / commands, etc.

Do not disconnect power if

- Data of evidential value is visible on the computer screen
- There are active programs or files in use, such as chatrooms / IM windows, open documents, etc.

In such situations, photograph and document all on-screen information, then perform volatile data collection and preservation

Disconnect power once volatile data has been collected

When disconnecting power, unplug power cable from the computer instead of from the wall plate (why?) 

Preserving Data on Live Systems

Have a competent individual when volatile data or specific files must be collected from a live system

- Should have training and experience in acquiring digital evidence from a live system
- Should document the acquisition process
- Should be able to explain and justify each step that was taken

When working with a live system, attempt to minimize potential alterations of the evidence

- e.g., Run programs from (and save data to) external device
- e.g., Connect a different keyboard and mouse to the computer in order to preserve fingerprints and biological evidence on the original input devices

Preserving Data on Live Systems

Sometimes, may be sufficient to collect specific information from memory if you know exactly what you are looking for

- e.g., Network connections, list of running processes, etc.
- Again, every action must be documented
  - Hash value of acquired data must be calculated to initiate chain of evidence and preserve integrity

Other times, may be necessary to acquire the full contents of memory

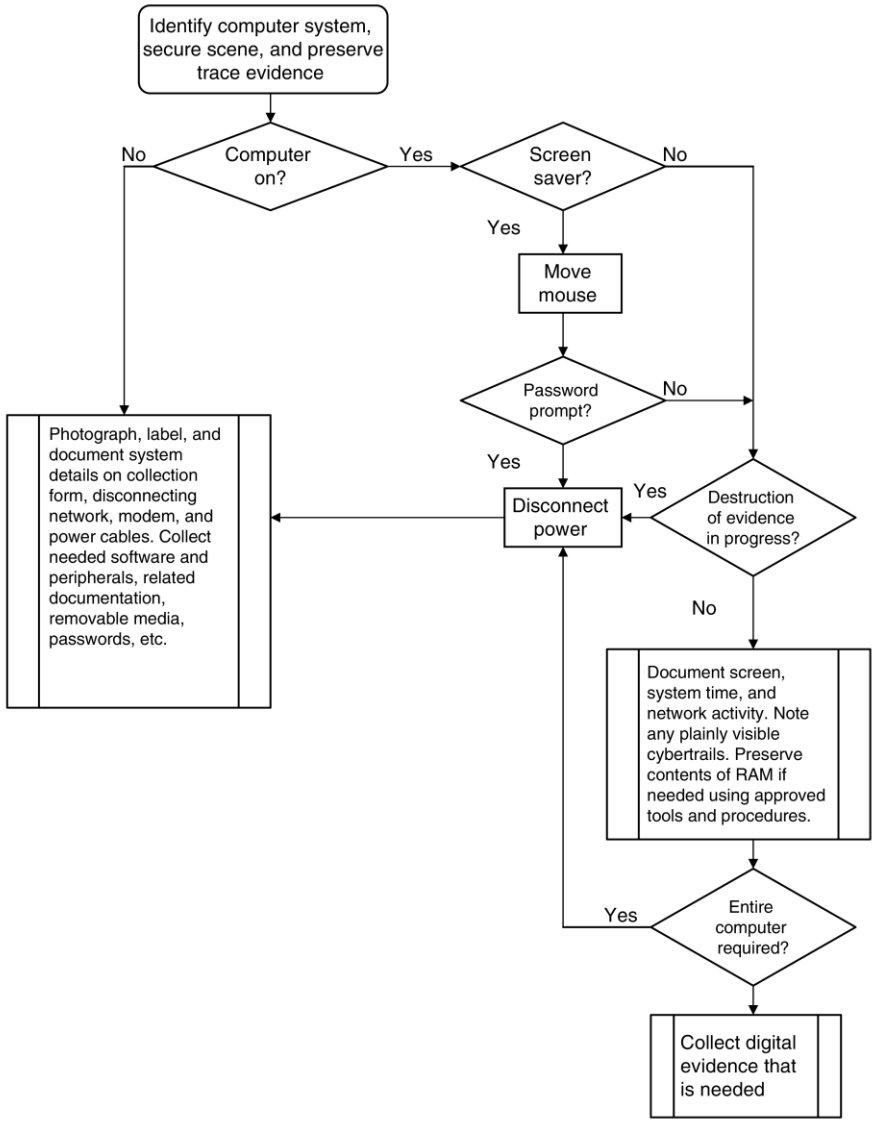
- e.g., In computer intrusion or malware investigations, or when encryption keys may reside in memory
- Like before, document all actions taken and calculate hash value of acquired data

Preserving Data on Live Systems

Sometimes, may also be necessary to make a forensic image of the hard drive while the computer is running

- e.g., When full disk encryption is in use
- e.g., When the system is hosted on the cloud
- e.g., When the computer cannot be shut down for some reason

Gentle reminder that if a system is powered down, leave it turned off ⚡



Decision Process for Preserving Computer (Casey, 2011)

👋 Questions?
Thank You!

📨 Weihan.Goh {at} Singaporetech.edu.sg

📌 https://www.singaporetech.edu.sg/directory/faculty/weihan-goh

📌 https://sg.linkedin.com/in/weihan-goh