The Digital Investigator

Goh Weihan

ICT3215 Digital Forensics

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

September 2024

Digital Forensics in Real Life

Silk Road

What is Silk Road?

An online black market operated as a Tor Hidden Service

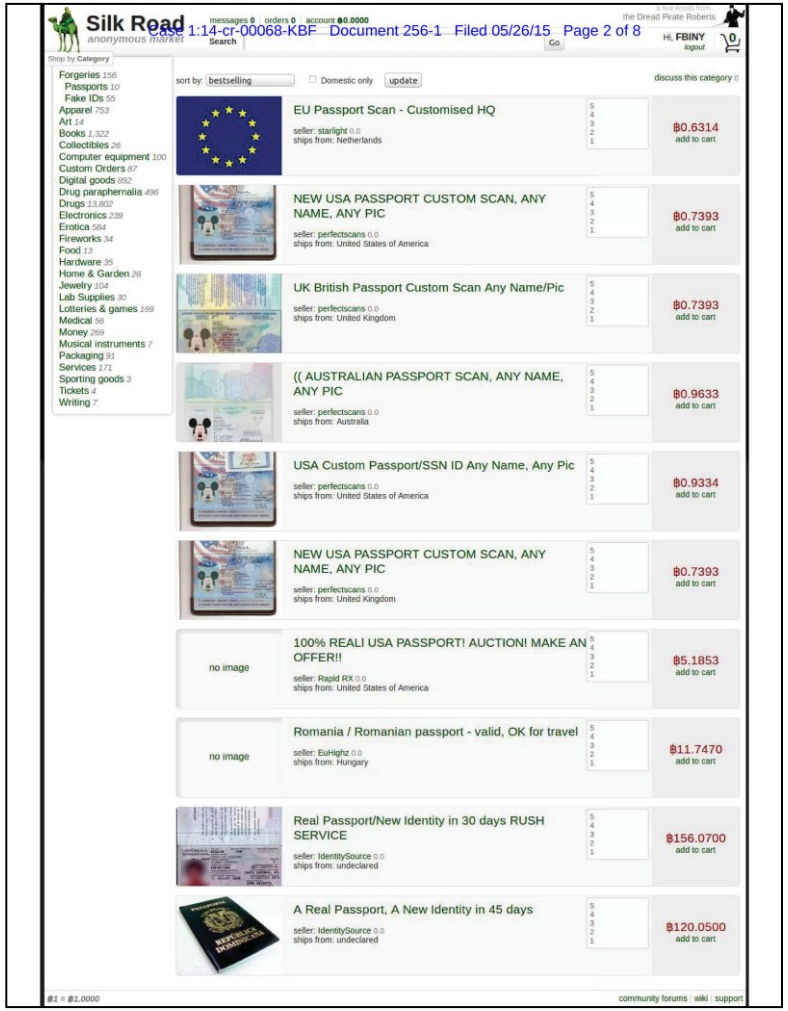
Primarily used as a place to deal drugs and other illegal items

Launched in February 2011

Owned by a person called *Dread Pirate Roberts*

Server located in Iceland, taken down by the FBI in October 2013

How? Leaky code, according to the FBI



Silk Road

Silk Road's leaky code

In some packets sent by the Silk Road server, there was a non-Tor source IP address

Keying in IP address into web browser revealed part of the Silk Road's login screen (the CAPTCHA prompt)

IP address points to **Iceland**

600 **Silk Road discussion / A brand new annonymous market!**
« **on:** February 26, 2012, 07:57 am »

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

We are happy to announce a brand new site called The Armory. It focuses exclusively on the sale of small-arms weaponry for the purpose of self defense.

The issue of whether weapons should be sold on Silk Road has been brought up and debated too many times to count. I have heard good arguments on both sides of the debate and had to really think hard before choosing to take this direction. Here is a brief summary of my thoughts on the matter and why I chose to spin-off a new site rather than ban weapon sales completely, or allow them to continue here:

First off, we at Silk Road have no moral objection to the sale of small-arm weaponry. We believe that an individual's ability to defend themselves is a cornerstone of a civil society. Without this, those with weapons with eventually walk all over defenseless individuals. It could be criminals who prey on others, knowing they are helpless. It could be police brutalizing people with no fear of immediate reprisal. And as was seen too many times in the last century, it could be an organized government body committing genocide on an entire unarmed populace. Without the ability to defend them, the rest of your human rights will be eroded and stripped away as well.

That being said, there is no reason we have to force everyone into a one-size-fits-all market where one group has to compromise their beliefs for the benefit of another. That's the kind of narrow thinking currently used by governments around the world. It's why we are in this mess in the first place. The majority in many countries feel that drugs and guns should be illegal or heavily regulated, so the minority suffers.

Here at Silk Road, we recognize the smallest minority of all, YOU! Every person is unique, and their human rights are more important than any lofty goal, any mission, or any program. An individual's rights ARE the goal, ARE the mission, ARE the program. If the majority wants to ban the sale of guns on Silk Road, there is no way we are going to turn our backs on the minority who needs weaponry for self defense.

So, without further ado, I give you our answer to this whole conundrum:

The Armory: ayjkg6ombrsahbx2.onion

The Armory is run on the same codebase that runs Silk Road, with all of the same features you know and love. However, it is run completely independently with it's own servers, Bitcoin wallets, databases, etc. If it becomes popular, we'll even look into putting it under separate management.

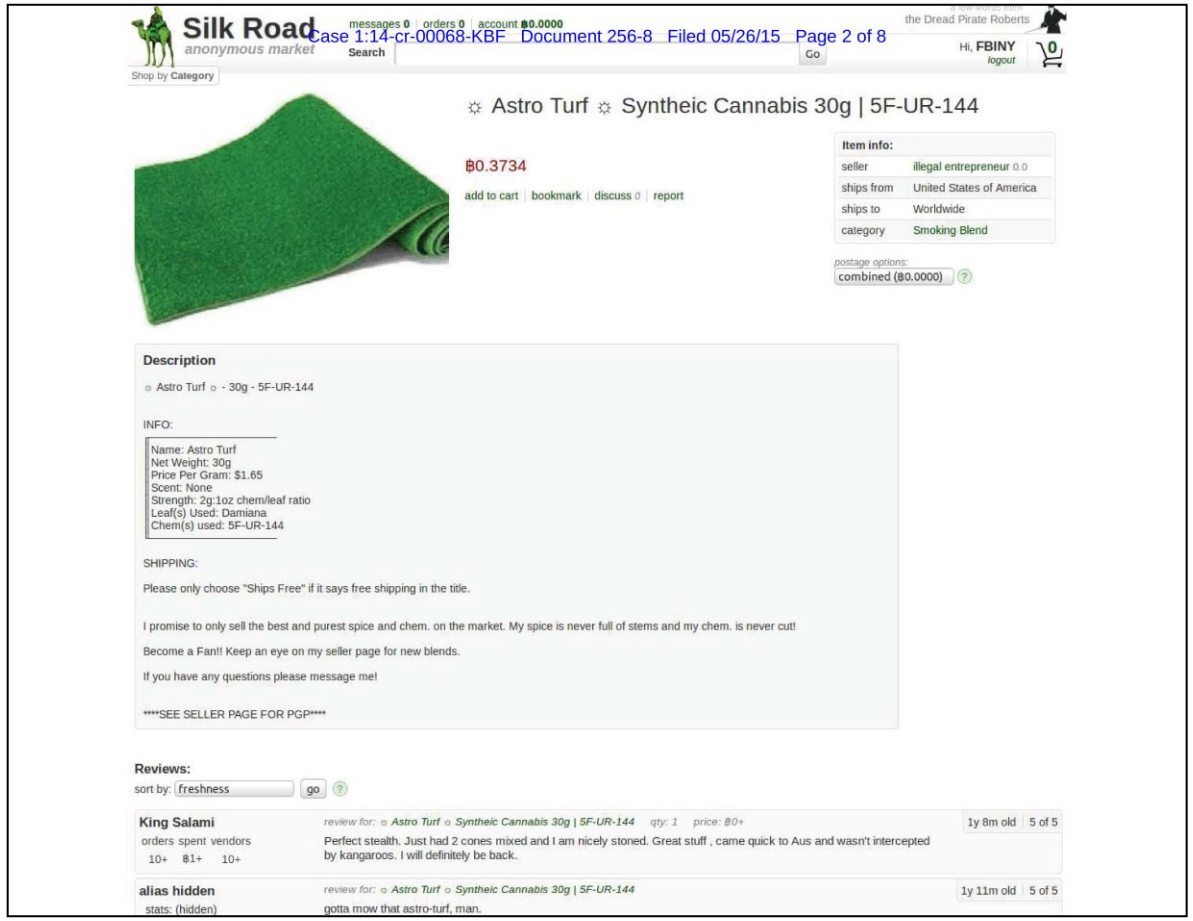
A note to vendors: If you have items in the Silk Road weapons category, please relist them at The Armory asap. We will be shutting down weapons sales on Silk Road on Sunday March 4th.

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v2.0.14 (GNU/Linux)

iQEcBAEBAgAGBQJPSt5DAAoJEAIiQjtnt/olO9IH/jIH9+bqUjakcOSbbOxqKe7g
lGBQwpNdTVcvyi/5/EX7Y6DtJs3sR5OhQpXoeQHI+aGvNoF+iUrot0TiYmiTDa72
cBI3AD9TaxrbLuuuKhNuXTQ3BhoZMKx8VLdLK6HallIlTW9Qwn5Fp2lr54tOV29a
BQXvhqfibg7+BZRM38yZJT/GFw2+FCjxMnp3o6oD/nXDrYDqtRJjfuas4Yad3JkB
owsH3+mZO014//UuLawUqJ/EKU7GA1xZ+YXy2fgn6U+hHNH9STLGXj3klHKgN8QV
KsoP/fxpiGeZyUprkVUarCs1LtSNHBsbiz+MzsaTYltVwSagZId+3X33n7AH2Mo=
=+nt5
-----END PGP SIGNATURE-----

Reply Quote Notify

Silk Road



FBI requested subscriber information, server routing data, and image of the server contents from Icelandic authorities

Traffic data showed very large volume of Tor traffic flowing to the server

Supports notion that server is highly likely used as a Tor Hidden Service

Silk Road

Covert imaging of server performed after Reykjavik Metropolitan Police obtained court order

- Forensic examination of the image showed that the server hosts the Silk Road
- Analysis of codes and data from the Silk Road server revealed IP addresses of other servers at various different locations
- *But who is Dread Pirate Roberts?*

Who is Dread Pirate Roberts?

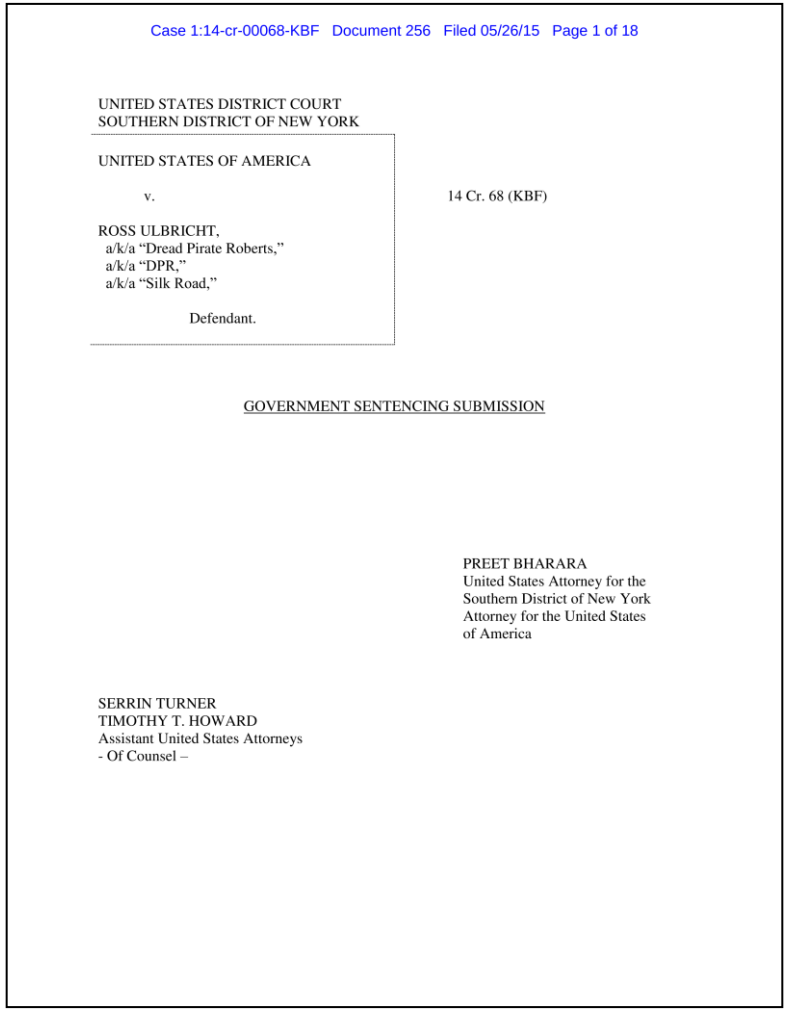
Ross Ulbricht

- Arrested on October 2, 2013 in San Francisco
- Internet surveillance used to confirm identity prior to arrest
- Search warrants obtained for his residence, laptop, Gmail, and Facebook accounts

Charged with, and subsequently convicted of seven offences

- **Charges**
  - Narcotics trafficking
  - Distribution of narcotics by means of the Internet
  - Narcotics trafficking conspiracy
  - Continuing criminal enterprise
  - Conspiracy to commit and aid and abet computer hacking
  - Conspiracy to traffic in fraudulent identification documents
  - Money laundering conspiracy

Ross Ulbricht



Case 1:14-cr-00068-KBF Document 256 Filed 05/26/15 Page 1 of 18

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

v.

14 Cr. 68 (KBF)

ROSS ULBRICHT,
a/k/a "Dread Pirate Roberts,"
a/k/a "DPR,"
a/k/a "Silk Road,"

Defendant.

GOVERNMENT SENTENCING SUBMISSION

PREET BHARARA
United States Attorney for the
Southern District of New York
Attorney for the United States
of America

SERRIN TURNER
TIMOTHY T. HOWARD
Assistant United States Attorneys
- Of Counsel –

- One 20 years for money laundering
- One 15 years for trafficking fraudulent identification documents
- One 5 years for aiding and abetting computer hacking
- Two life sentences for the drug charges

Collection of more than 300 exhibits, including digital evidence like chat logs, screen captures, and electronic documents, were used

Sentenced to life in prison, without possibility of parole

What about Silk Road Users?

Who is Paul Leslie Howard?

- Paul Leslie Howard was one such drug dealer using the Silk Road to peddle goods
- In two months from March 2012, used the Silk Road 11 times to buy and import illicit drugs

- **Recovered 10,700 text messages on one cell phone, and 9,700 text messages on the other**
  - *"I got 5 grand worth if you want"*
  - *"...promote the LSD i got more in. I sold 200 cubes last week"*
  - *"no cubes left atm but some other 'things' u might like!"*

Police raided his home and found quantities of marijuana, 35 stun guns (disguised as cell phones), a money counter, and $2300 in cash

Police also seized three computers and two mobile phones...

Paul Leslie Howard

Who is Paul Leslie Howard?

- Paul Leslie Howard was one such drug dealer using the Silk Road to peddle goods
- In two months from March 2012, used the Silk Road 11 times to buy and import illicit drugs

- **In the computer, investigators found other things…**
  - Pictures of drugs on a piece of paper with *'shadh1'* (Howard's Silk Road handle) written on it, kept in a Dropbox folder called *'SR'*
  - Google search history
    - *"Does Australia Post record tracking"*
    - *"Silk Road Tor address"*

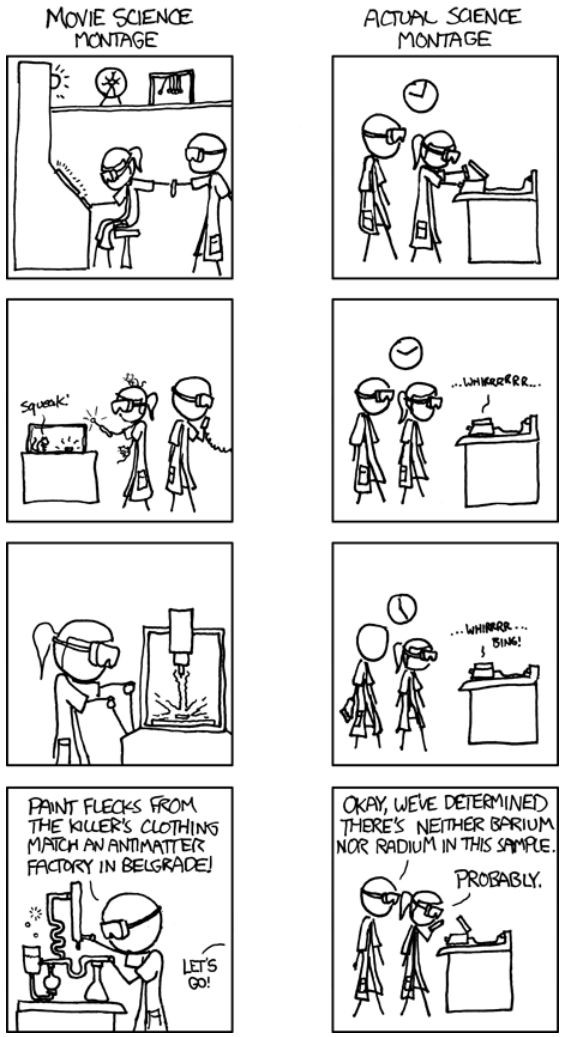
Police raided his home and found quantities of marijuana, 35 stun guns (disguised as cell phones), a money counter, and $2300 in cash

Police also seized three computers and two mobile phones…

The Digital Investigator

Forensics and Computer Science

Digital forensics is the application of computer science in the systematic collection, processing, and study of digital data suitable for use in courts or to the just resolution of conflict



A digital forensic investigator, or forensic analyst

- Acquires data and information from electronic devices, which can be used as evidence
- Should **never do harm** to the investigation

Why Investigate?

Widespread adoption of digital systems used for information storage, communication, etc.

Investigations / disputes will (almost) likely involve information from the digital domain

Information of interest may not present themselves readily

Entities may engage in action to hinder or prevent retrieval of information

Why Investigate?

Investigation can be done for criminal cases, civil cases, or internal incidents

Criminal cases: Government as the plaintiff, brings a case against one or more defendants

Civil cases: Dispute between two entities; either side can be plaintiff or defendant

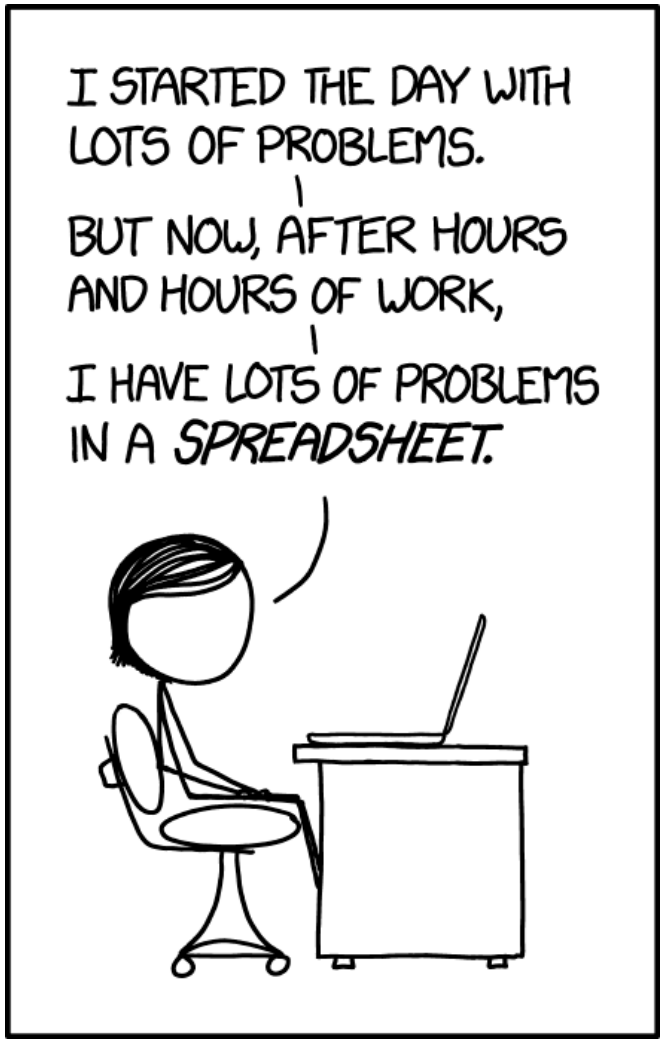
Internal incidents: Within boundaries of an organization, may not be meant for public review

May or may not be civil or criminal in nature, but escalation may be possible

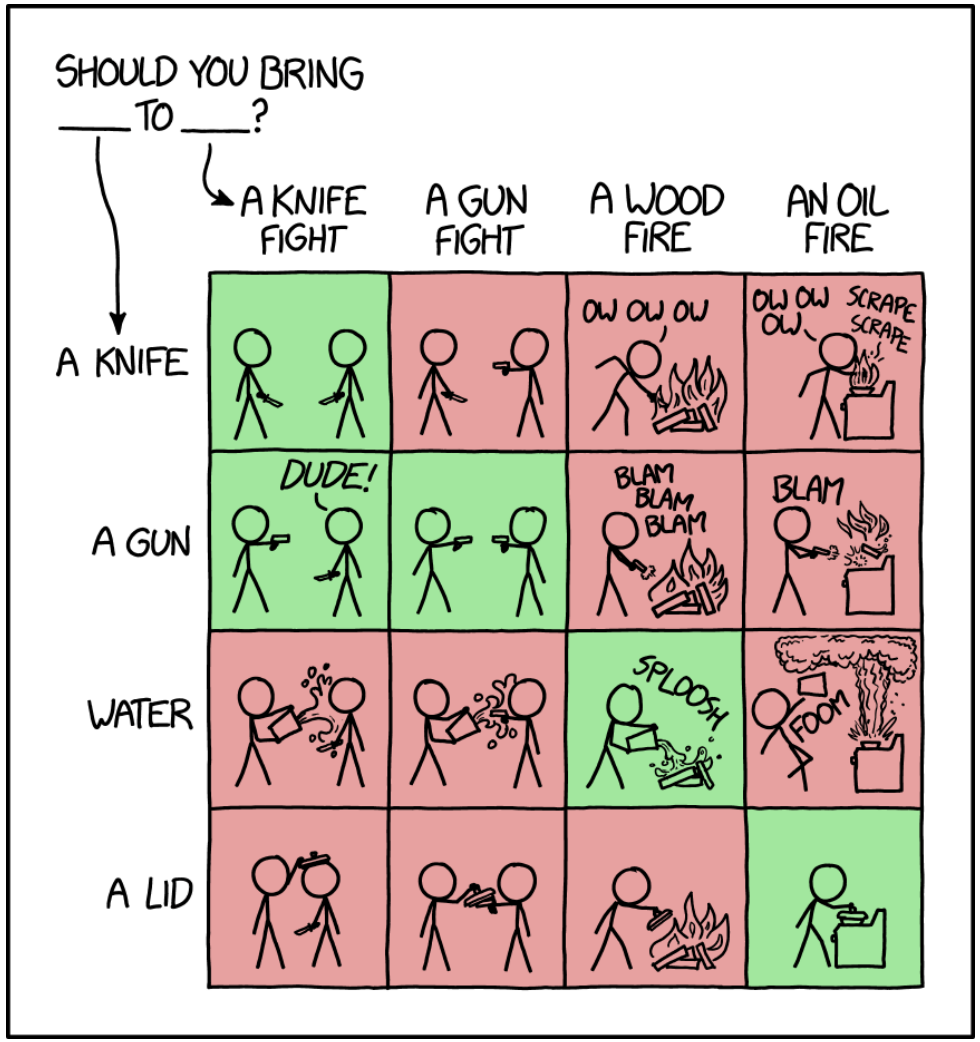
The Digital Investigator

A digital forensic investigator should possess

- Strong understanding and knowledge about
  - How **computer systems** and **digital devices** work
  - How **file systems** work
  - How data is **generated**, **stored**, and **accessed** by operating systems
- Strong foundation in **computer networks**
- Good **hardware** knowledge and skills to be able to extract data from electronic devices



The Digital Investigator



Qualities of a digital forensic investigator

- **High standard of ethics and professionalism**
- Critical thinker and problem solver
- Detail oriented, inquisitive, and resourceful
- Good judgement and perceptiveness
- Good communication skills
- Poise under pressure
- Patience

Digital Evidence

The Many Definitions of Digital Evidence

"Information stored or transmitted in binary form that may be relied on in court." - International Organization on Computer Evidence (IOCE)

"Information of probative value that is stored or transmitted in binary form." - Scientific Working Group on Digital Evidence (SWGDE)

"Computer-based electronic evidence is information and data of investigative value that is stored on or transmitted by a computer." - Association of Chief Police Officers (ACPO) UK

"Any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi." - Casey, 2011 (adapted from Chisum, 1999)

Understanding Digital Evidence

Digital evidence is generally defined as "information of probative value that is stored or transmitted in digital form"

Digital data can be fragile in nature, necessitating proper handling procedures

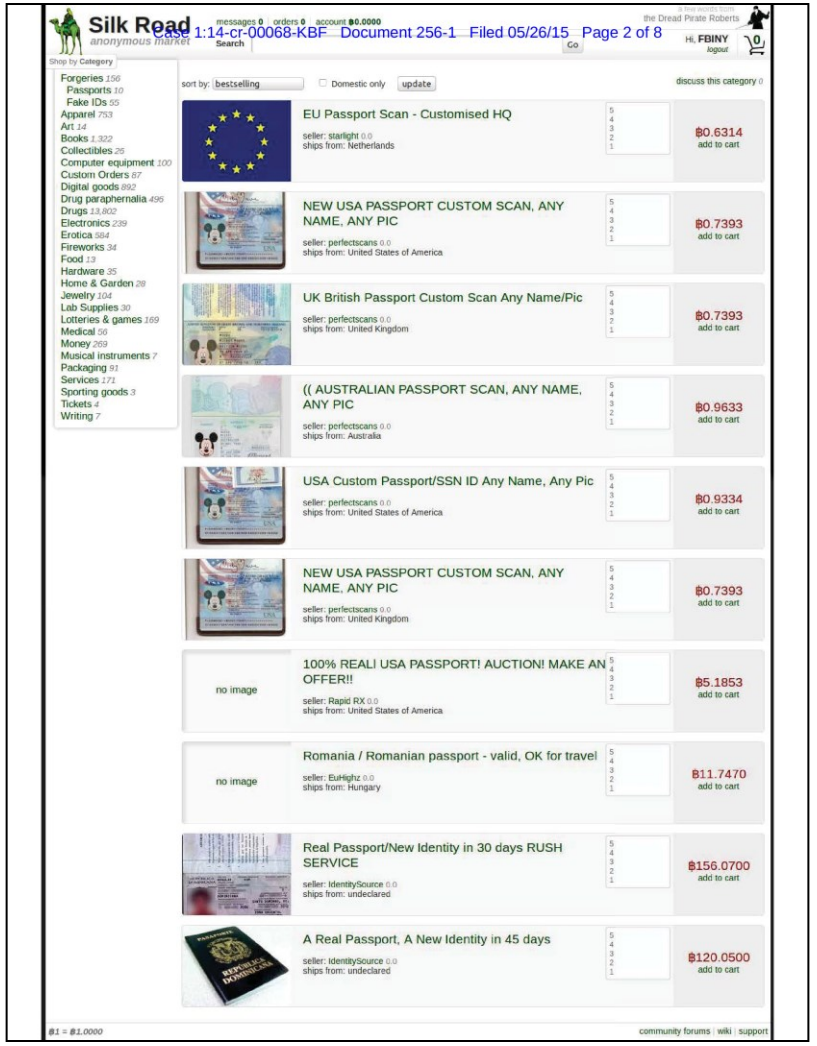
Information of interest can be found while examining digital storage media, monitoring network traffic, duplicating copies of digital data, etc.

Increasing Awareness of Digital Evidence

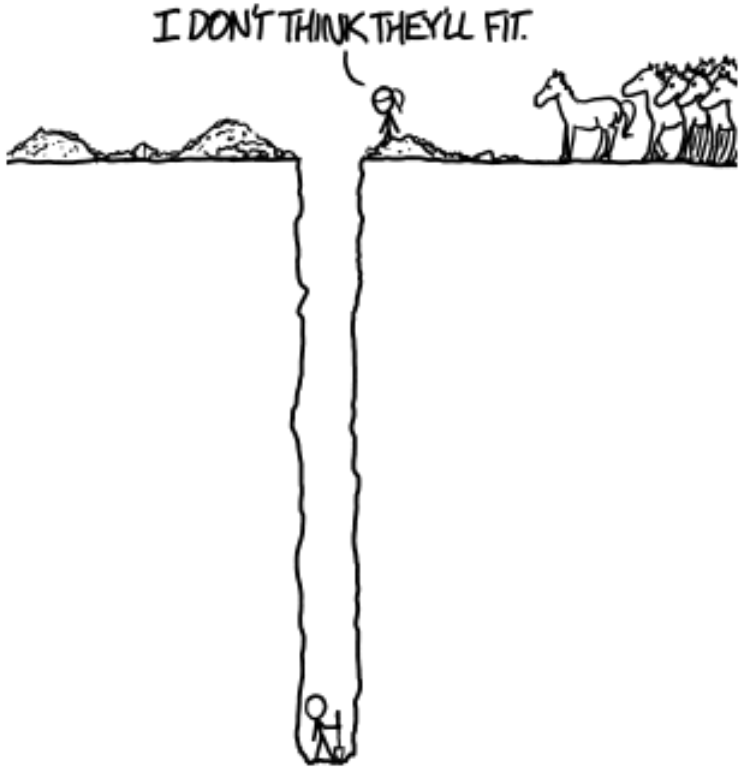
Criminals and terrorists are using technology to facilitate offenses and avoid detection / apprehension

- Use of such systems has resulted in an abundance of **digital evidence**

- Digital evidence can be used to **apprehend and prosecute offenders**, e.g., Dennis Rader, Ross Ulbricht, Paul Leslie Howard



Increasing Awareness of Digital Evidence



Hence, criminals are also concerned with digital evidence

- Will attempt to manipulate electronic systems to **evade discovery and capture**
- Engage in **anti-forensics**, i.e., countering, hindering, or preventing digital forensics

Locard's Exchange Principle

"Every contact leaves a trace"

Describes the concept of evidence exchange

- An entity at a crime scene **leaves with something** from the scene, and **leaves something behind** at the scene
- Applies to both **physical** and **digital** domain
- Applies to **any contact** at a crime scene, including those by the investigator

May not be easily detectable

- e.g., Fingerprint, DNA, etc.
- e.g., File metadata, timestamps, log entries, deleted files, remnant data, etc.

Evidence Characteristics

Two general categories of evidence - evidence with class characteristics, and evidence with individual characteristics

Discovery of individual characteristics

- **Reduces margin of error**
- **Link becomes less circumstantial**
- **Harder to refute**

Class characteristics

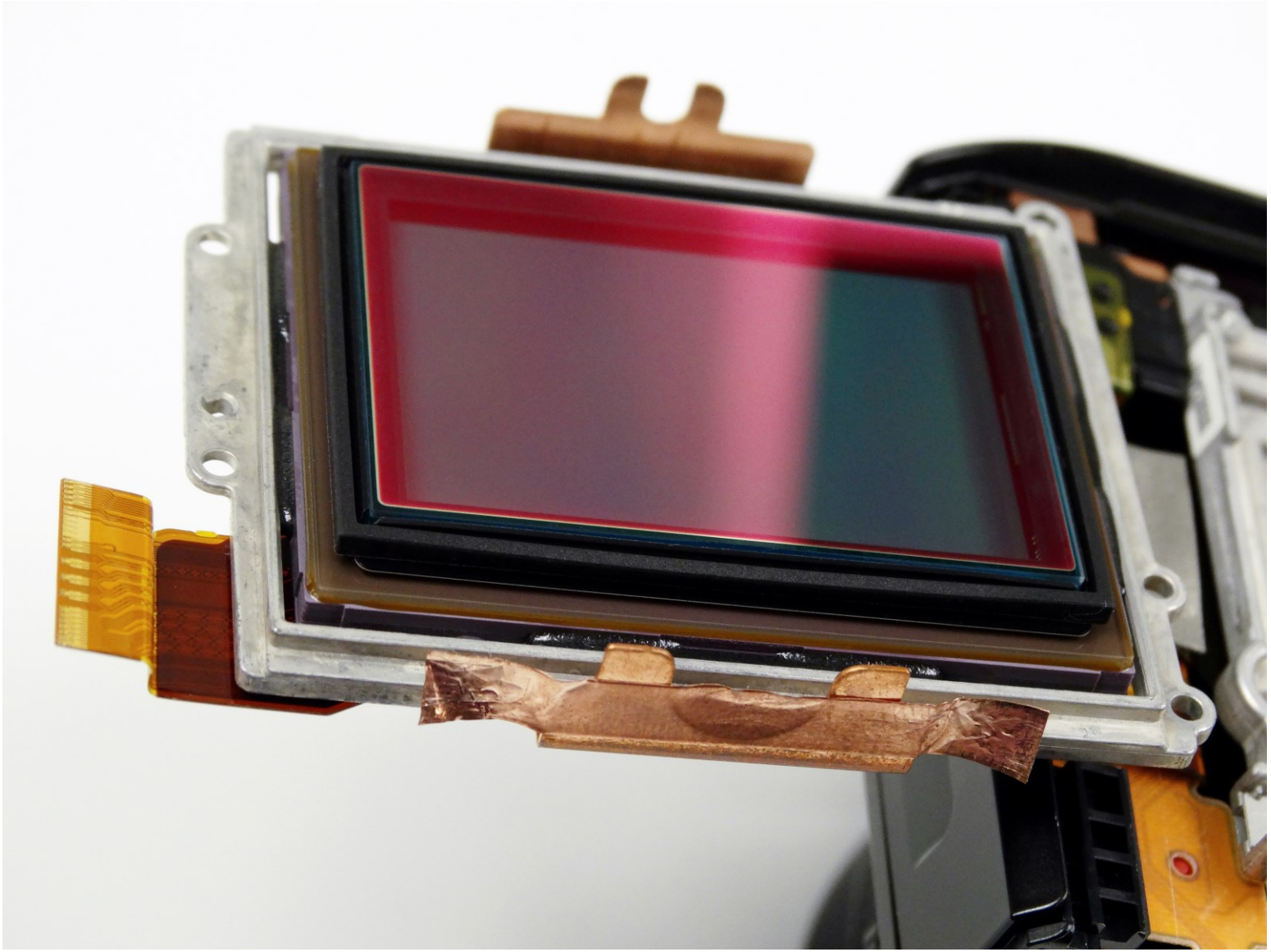
- **Common traits** in similar items
- Can be used to **narrow the search**

Individual characteristics

- Traits **more unique** to a particular sample
- May be linked to a specific person / activity with **greater certainty**

Sensor dust pattern captured on a photograph

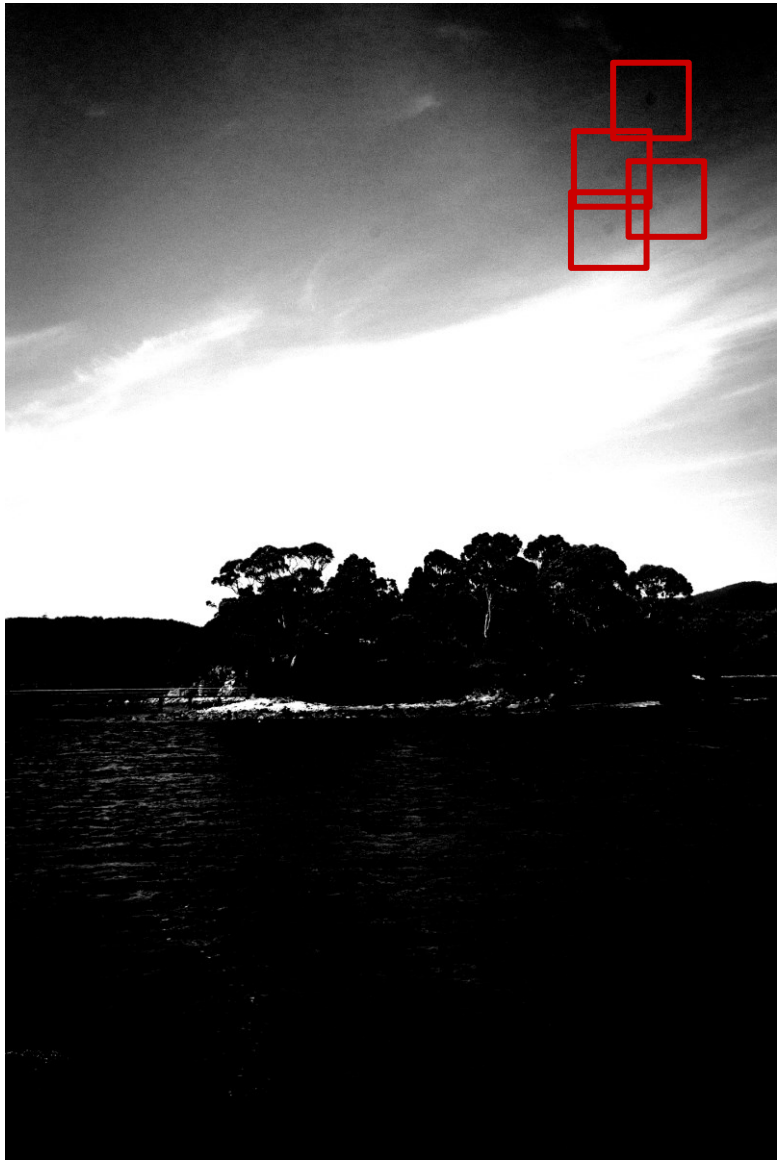
Sensor dust pattern captured on a photograph

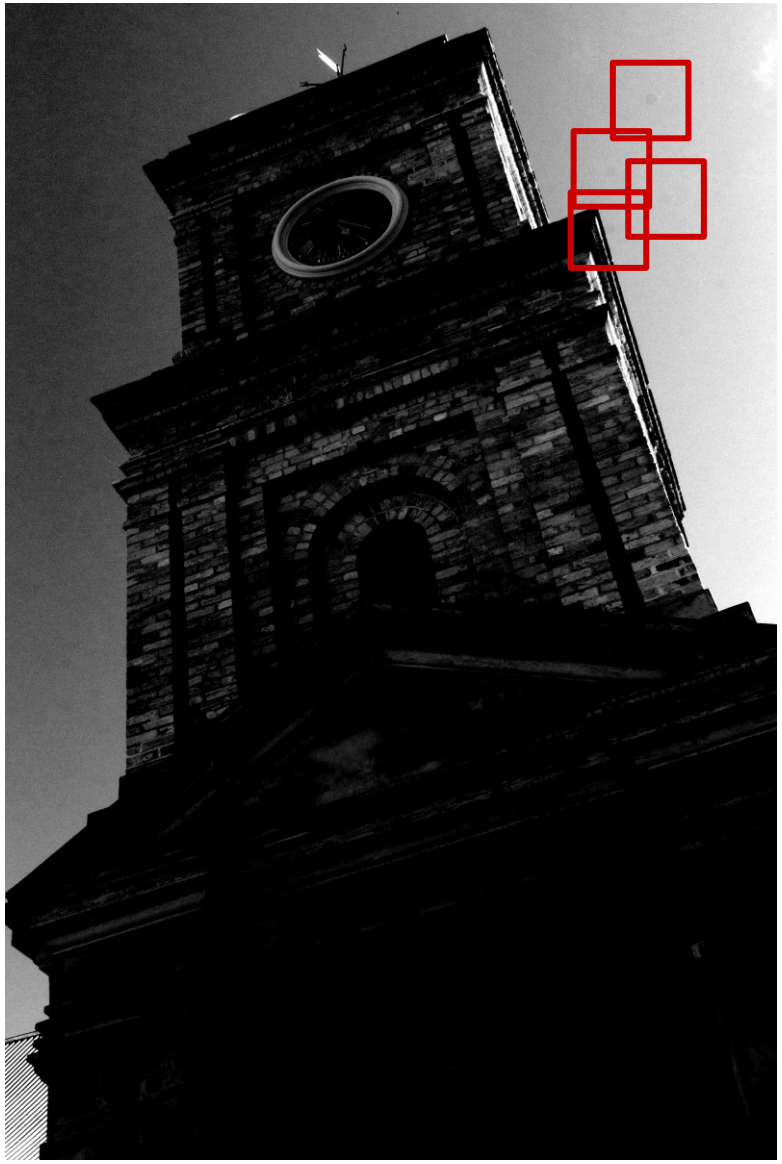


Camera sensor (Sony DSC-RX1, 35mm full frame)

SINGAPORE INSTITUTE OF TECHNOLOGY

Sensor dust pattern comparison





SINGAPORE INSTITUTE OF TECHNOLOGY

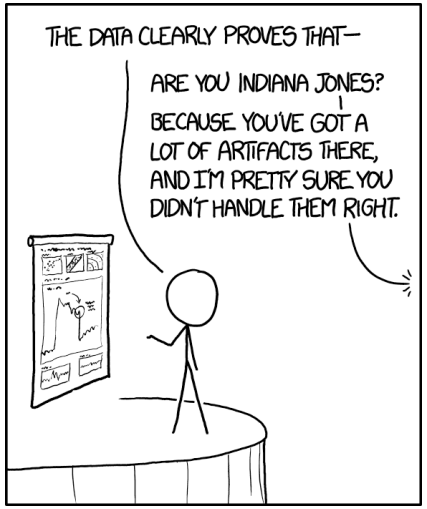
Sensor dust pattern comparison

Evidence Characteristics

More conclusive individual characteristics are

- **Rare**, but not impossible to identify
- **Desirable** given their strong association to an entity
- May require **detailed forensic analysis**; amount of work to ascertain such level of information may be **significant**

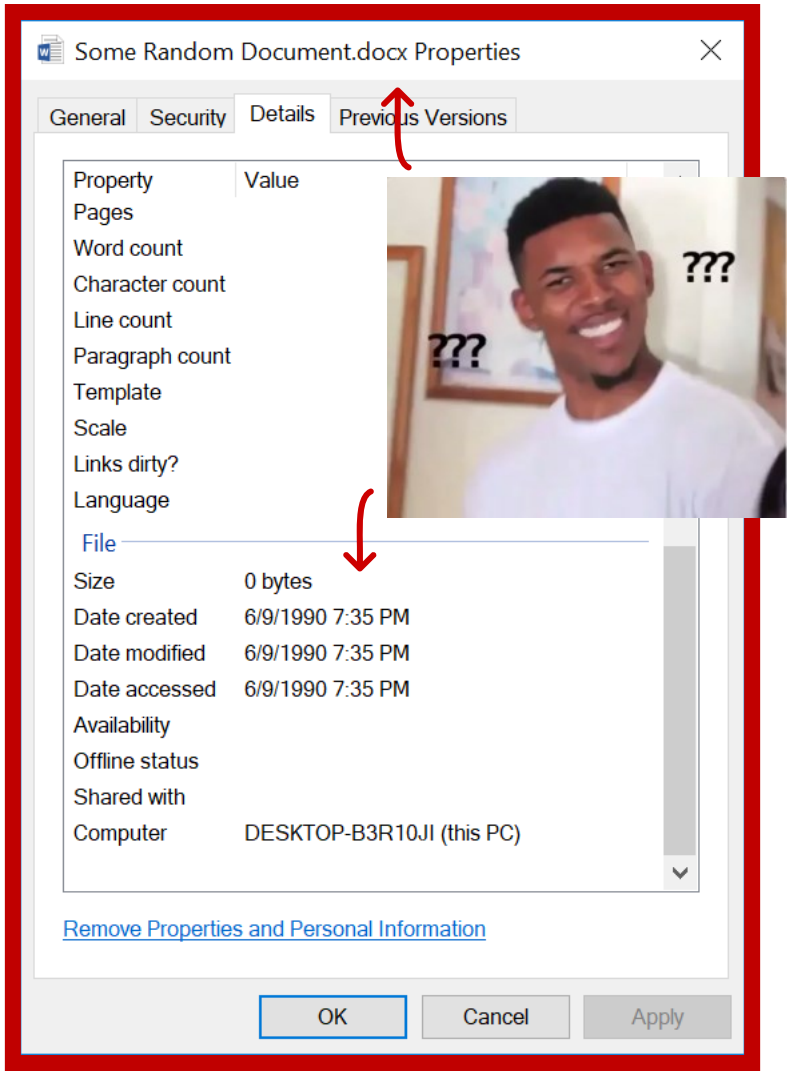
Exist risk if proven method for recovery has yet to be researched and / or accepted in the digital forensic community / used to establish precedent in the courts



Evidence Characteristics

Class characteristics can be useful when concerns exist that digital evidence has been **concealed**, **destroyed**, or **fabricated**

Class characteristics can collectively be used to determine *probability of involvement*



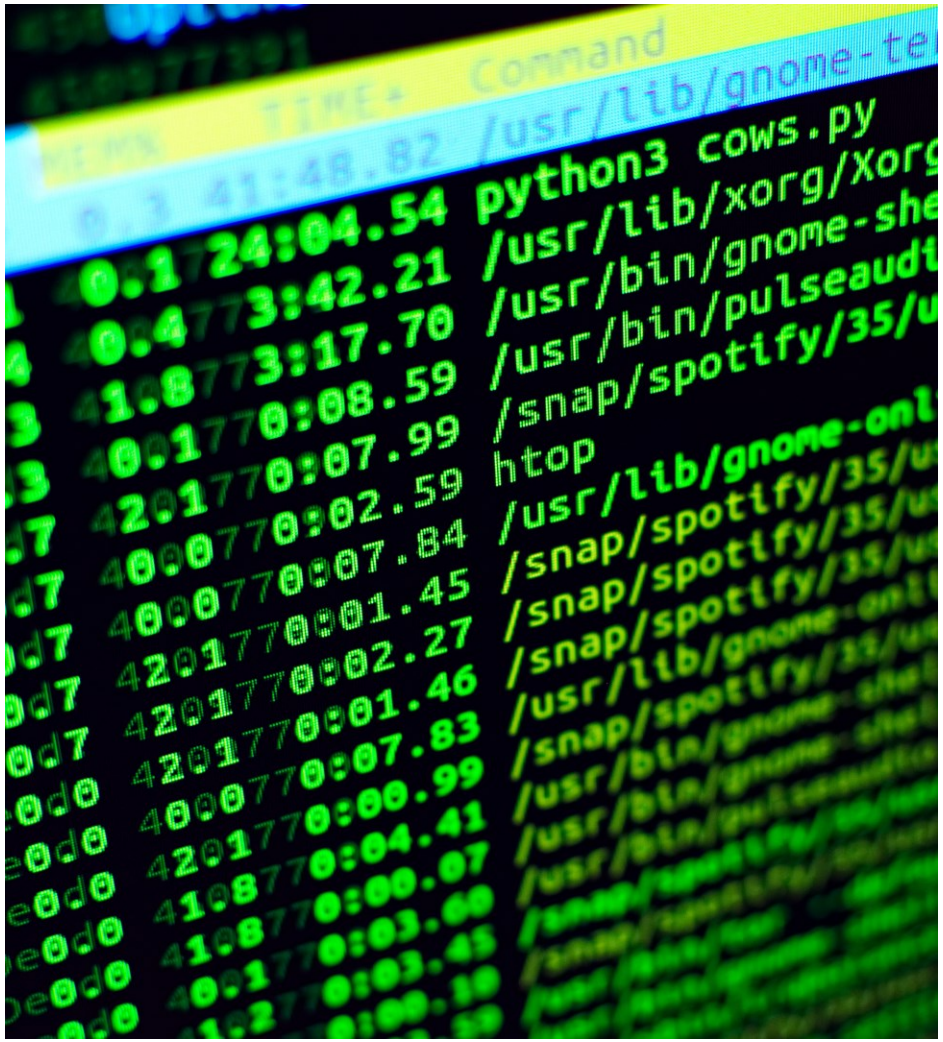
Data Volatility

Digital evidence can be found in various locations

These locations can have different characteristics

- Data retention capability
- Power requirement
- Performance
- Portability

Data that can be found can be broadly categorized into two categories - **volatile**, and **non-volatile**



Volatile data on a live system is lost after a computer is powered down 

Non-volatile data persists even after a computer is powered down 

Volatile and Non-Volatile Data

Volatile data: Data on a live system that is lost after a computer is powered down

Examples of volatile data

- Network traffic
- Process information
- Clipboard contents

Non-volatile data: Data that persists even after a computer is powered down

Examples of non-volatile data

- User files
- Swap file
- Event logs
- Unallocated cluster in filesystem

Guidelines for Handling Digital Evidence

SINGAPORE INSTITUTE OF TECHNOLOGY

Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition, National Institute of Justice, 2008

Best Practices for Seizing Electronic Evidence: A Pocket Guide for First Responders, Version 3.0, United States Secret Service, 2007

Good Practice Guide for Computer Based Electronic Evidence, Association of Chief Police Officers, 2007

Good Practice Guide for Digital Evidence, Association of Chief Police Officers, 2012

Principles in the Good Practice Guide for Digital Evidence

Principle 1: No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.

Principle 2: In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

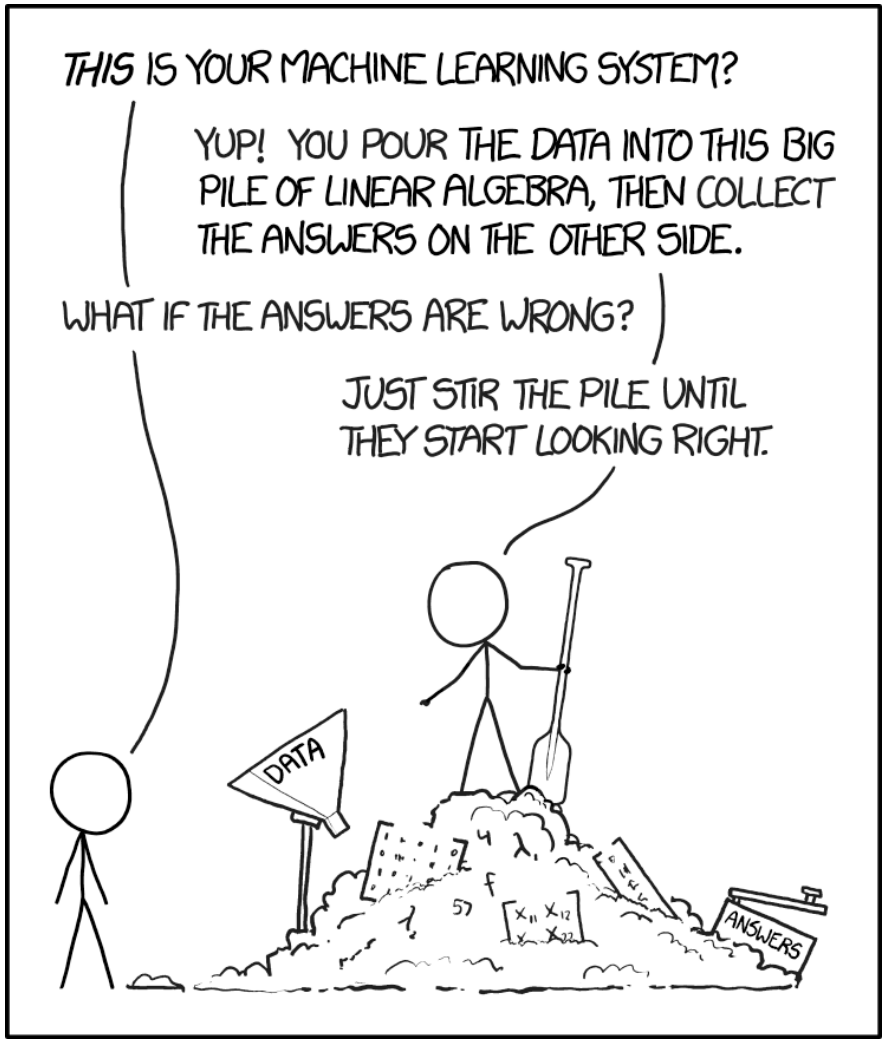
Principle 3: An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4: The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

Guidelines for Handling Digital Evidence

The principles in the Good Practice Guide for Digital Evidence are ideals

- Should always be kept in mind, but may not be feasible to achieve in certain situations
- Many methods for acquiring digital evidence in a forensically sound manner causes alteration (violating **Principle 1**)
- However, provided **Principles 2 and 3** are met, such alterations do not necessarily negate the authenticity of evidence or forensic soundness



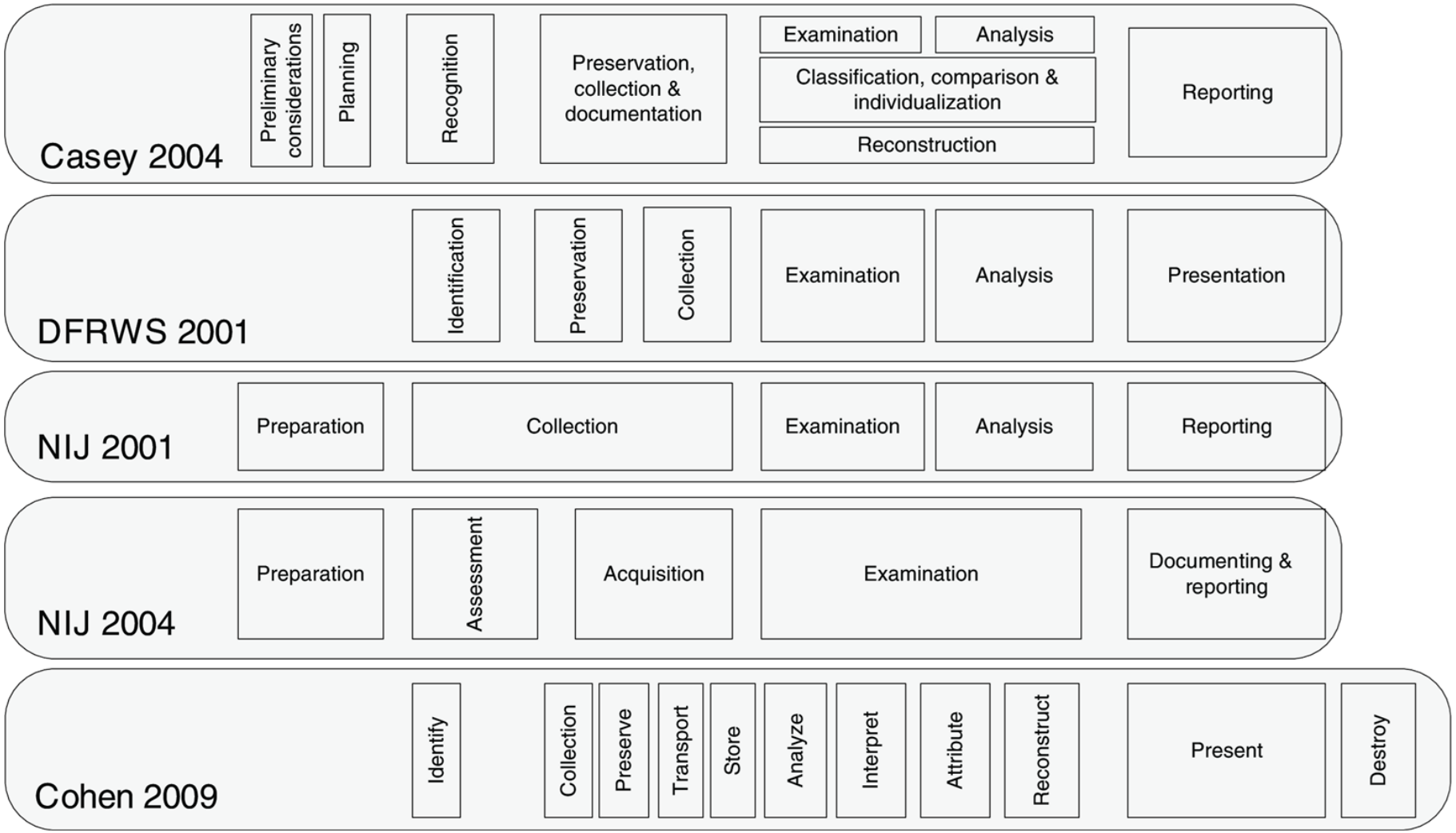
Digital Investigation Process Models

Digital Investigation Process Models

"The process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable."

- McKemmish, 1999

Evolution of Digital Investigation Process Models



Digital Investigation Process Models

Identification
"Knowing what evidence is present, where it is stored, and how it is stored"

Preservation
"Imperative that any examination of the electronically stored data be carried out in the least intrusive manner"

Analysis
"The extraction, processing and interpretation of digital data"

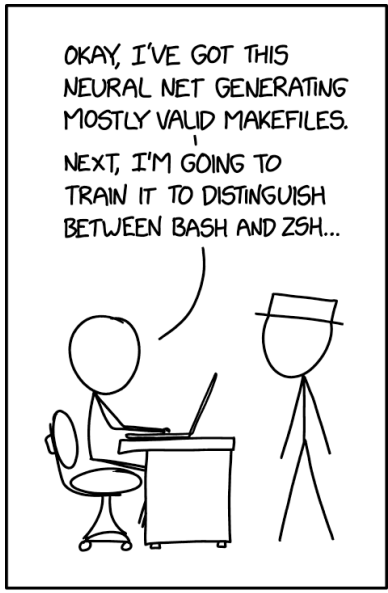
Presentation
"Actual presentation in a court of law"

👋 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



PEOPLE OFTEN USE ANCIENT TOOLS AND UIs TO DEVELOP MODERN CUTTING-EDGE TECHNOLOGY, BUT I DO IT THE OTHER WAY AROUND.