



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Digital Forensics Analysis (ACCA7031_LON)

Lecture 1

Introduction to Digital / Cyber Forensics

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk

Content covered

- Introduce Cyber Forensics and Incident Response (DFIR)
- Overview of Cyber Crime, Technology, and Law
- Cyber Forensic Investigations (Corporate, law enforcement, and private)
- Digital forensics Laboratory
- Tools and Frameworks used in DFIR, Testing and Validation Process

Learning Objectives

- Understanding of the Cyber Forensics domain
- Be aware of the different types of Cyber Crime committed and the tools used
- Differentiate between law enforcement and corporate investigation
- Understand the requirement for Digital Forensics Laboratory
- Enumerate major Tools and Frameworks used in DFIR

What Is Cyber Forensics?

- Cyber forensics deals with the application of law to the cyber domain.
- **The application of forensic science techniques to digital material such as computers, mobiles, networks, and clouds -**
- **In Detail, the process of identifying, preserving, analysing, and presenting digital evidence in a manner that is acceptable in a legal proceeding.**

What Is Cyber Forensics? (Cont.)

- **Cyber forensics:** can also be described as the scientific and critical analysis of a digital asset memory (**hard disk, RAM, external storage, networking logs, cloud storage**) after an intrusion, crime or policy violation (**memory?**).
- This involves examining existing data and **retrieving deleted data** from memory that have been authorised (subpoenaed) in court or seized by law enforcement.

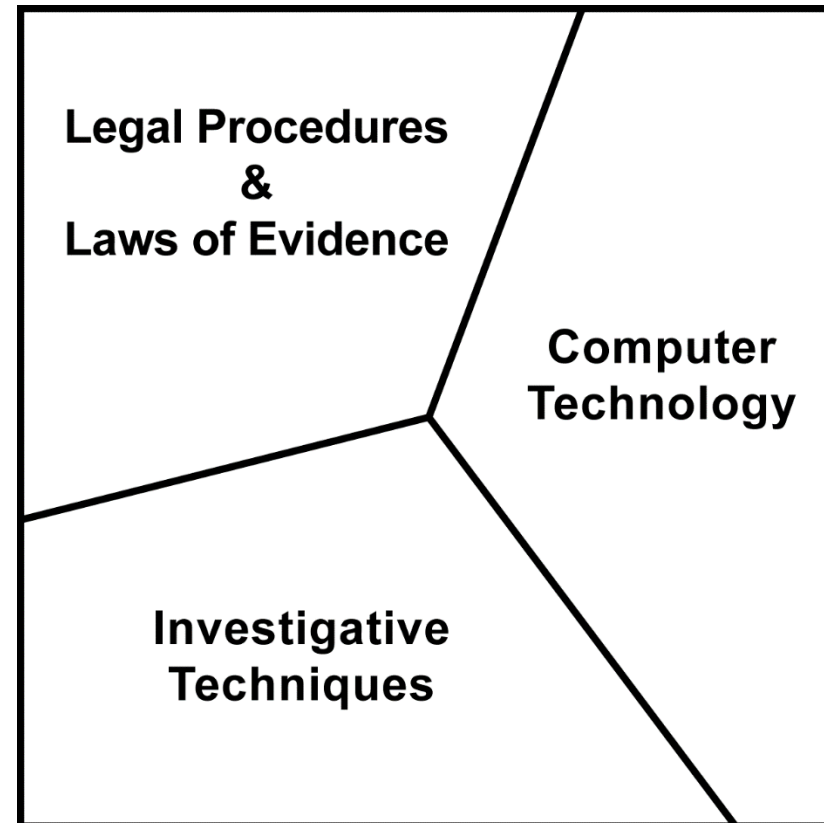
What Is Cyber Forensics? (Cont.)

- The following image demonstrates some of the different aspects of Cyber Forensics.



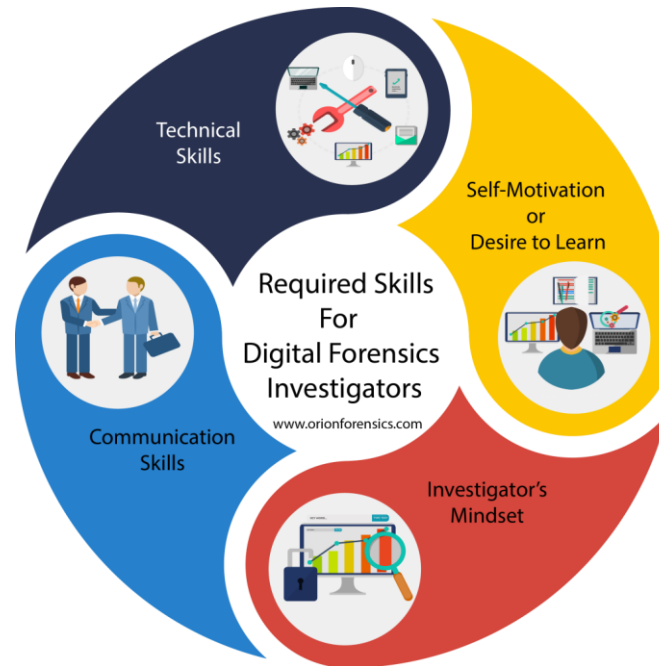
Cyber Forensics Skills

- An investigator's success depends on three skill sets
- Value of recovered evidence depends on expertise in these areas



Cyber Forensics Skills (cont.)

- Additional qualities required for a Cyber Forensic investigator



Cyber Forensic Profession

- Numerous companies and professionals now offer computer forensic services.
- A computer forensic profession needs to be a computer scientist with forensic science knowledge.
- The ideal background for this field includes legal, technical, and law enforcement experience.
- A computer forensic professional can fill a variety of roles such as private investigator, corporate compliance professional, or law enforcement official.

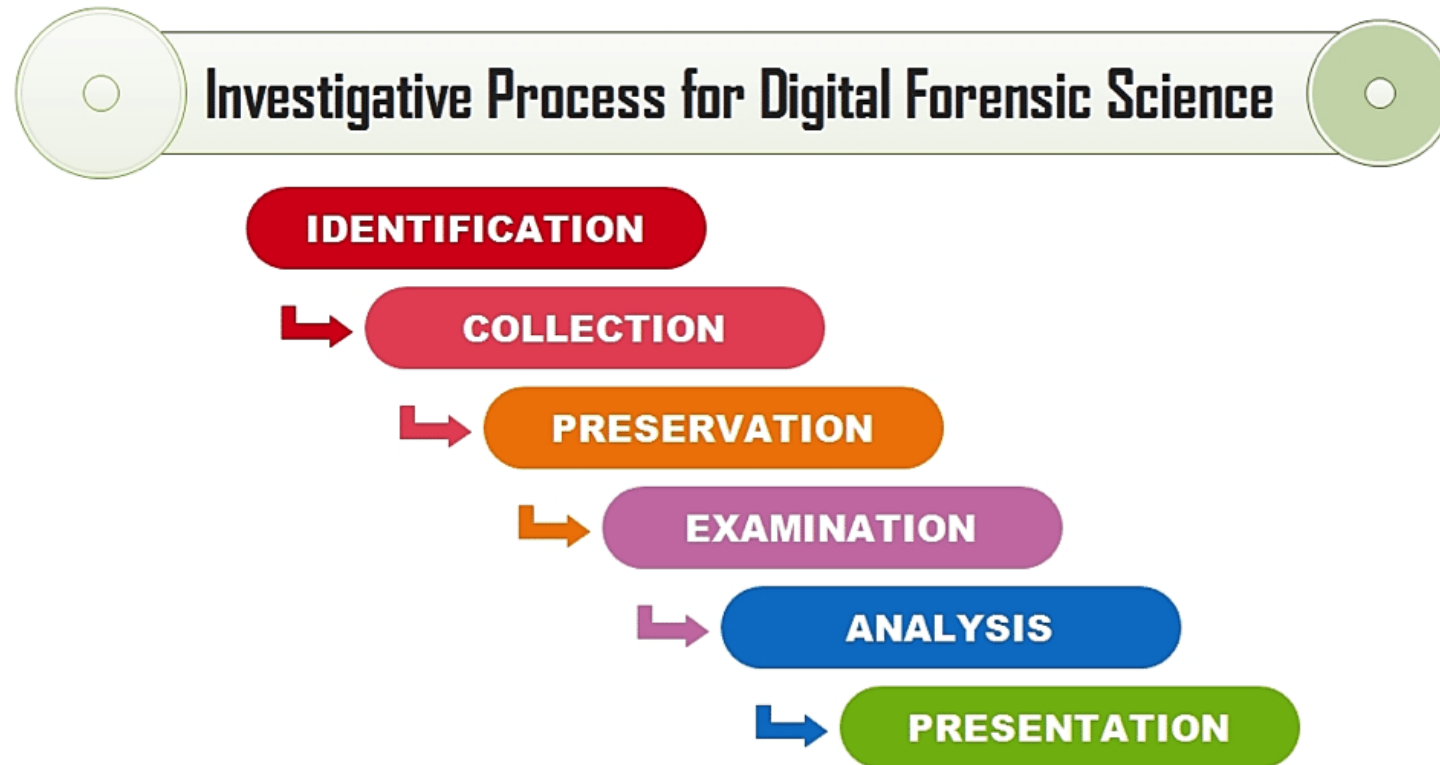
Cyber Investigation and Analysis Techniques

- Computer investigation and analysis techniques involve :
 - Identification
 - Preservation
 - Extraction
 - Documentation
 - Interpretation of computer data to determine potential legal evidence

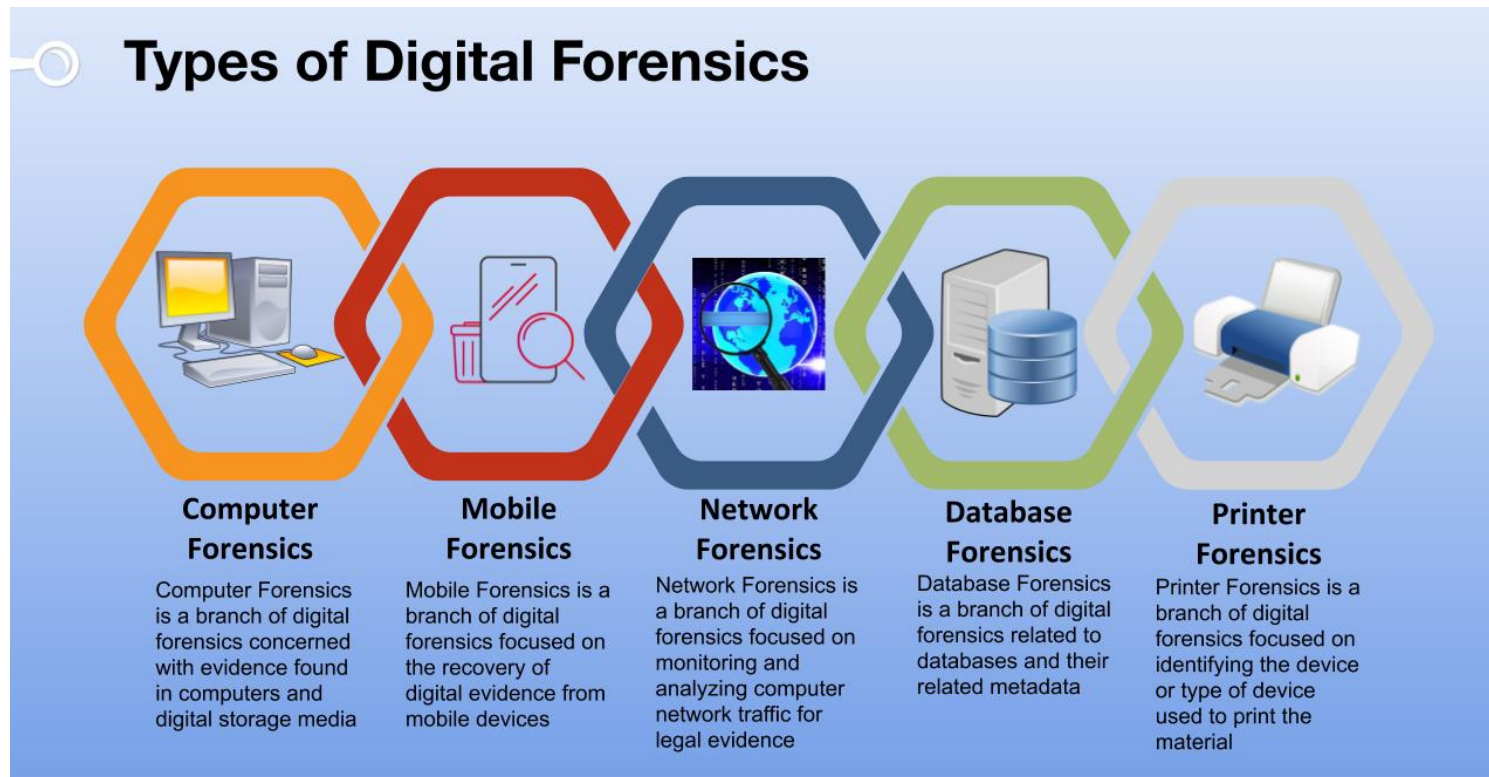
Computer Forensics Process

- Similar to other forms of legal forensics
- Computer forensics process, however, requires a vast knowledge of computer hardware and software
 - To avoid the accidental invalidation or destruction of evidence and to preserve the evidence for later analysis.
 - To analyze and interpret the evidence

Computer Forensics Process (cont.)



Types of Computer Forensics



Computer Forensic Review

- Computer forensic review involves the application of investigative and analytical techniques to acquire and protect potential legal evidence;
- A professional within this field needs to have a detailed understanding of the local, regional, national, and sometimes even international laws affecting the process of evidence collection and retention.
 - This is especially true in cases involving attacks that may be waged from widely distributed systems located in many separate regions.

Electronic Discovery

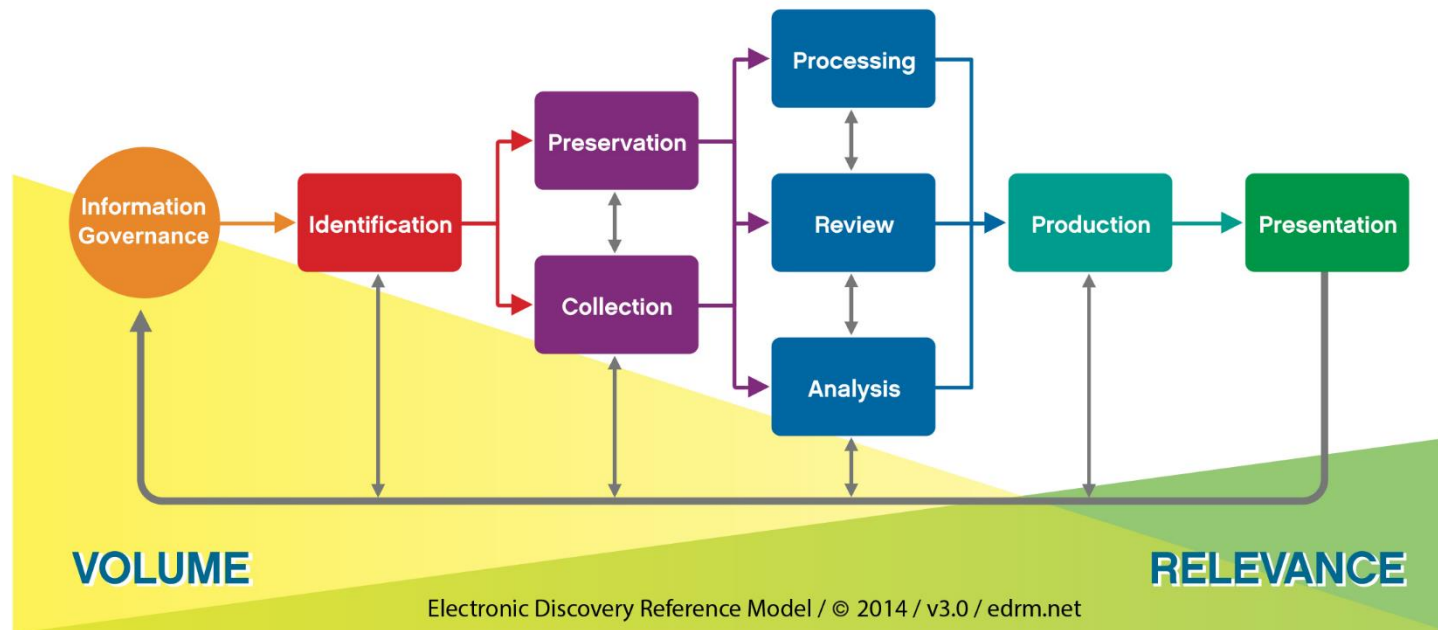
- Electronic discovery produces electronic documents for litigation – the process of taking legal action.
- Items included in electronic discovery include data that is created or stored on a computer, computer network, or other storage media.
 - E.g., e-mail
 - Word documents, PPTs, spreadsheets, plaintext files
 - Database files
 - Digital art or photos

Electronic Discovery (Cont.)

- During the *Electronic Discovery*, electronic documents are **collected, prepared, reviewed, and distributed** in association with legal and government proceedings.
- Main emphasis is on recovery of data.
 - Identify the evidence
 - Determine how to preserve the evidence
 - Extract, process, and interpret the evidence
 - Ensure that the evidence is acceptable in a court of law

Electronic Discovery (Cont.)

Electronic Discovery Reference Model



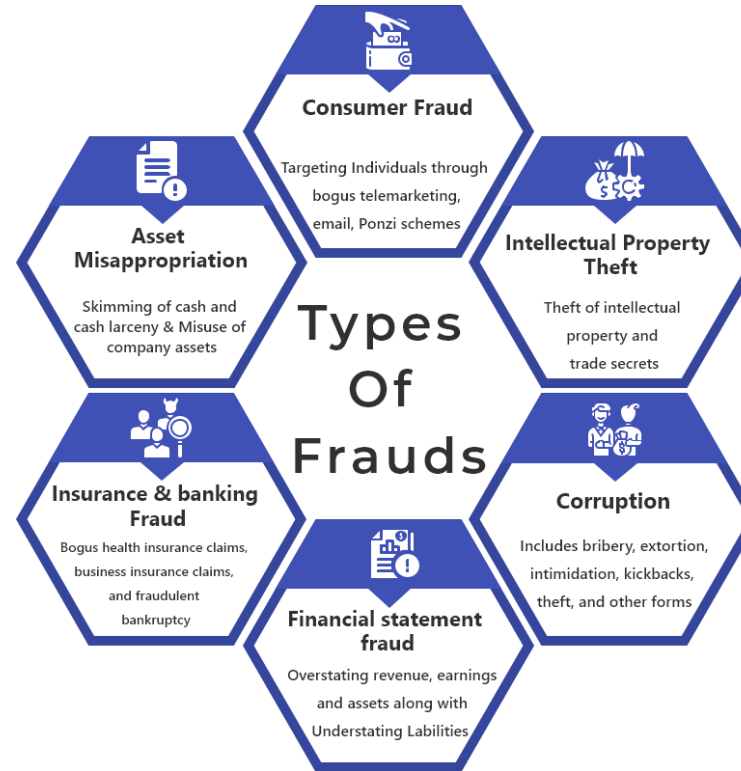
Understanding Corporate Investigations

- Business must continue with minimal interruption from your investigation
- Corporate computer crimes:
 - E-mail harassment
 - Falsification of data
 - Gender and age discrimination
 - Embezzlement
 - Sabotage
 - Industrial espionage

Computer Forensic Investigation from Corporate

- Examples:
 - Monitor the activities of employees
 - Assist in locating evidence of industrial espionage
 - Provide support in defending allegations of misconduct by senior management

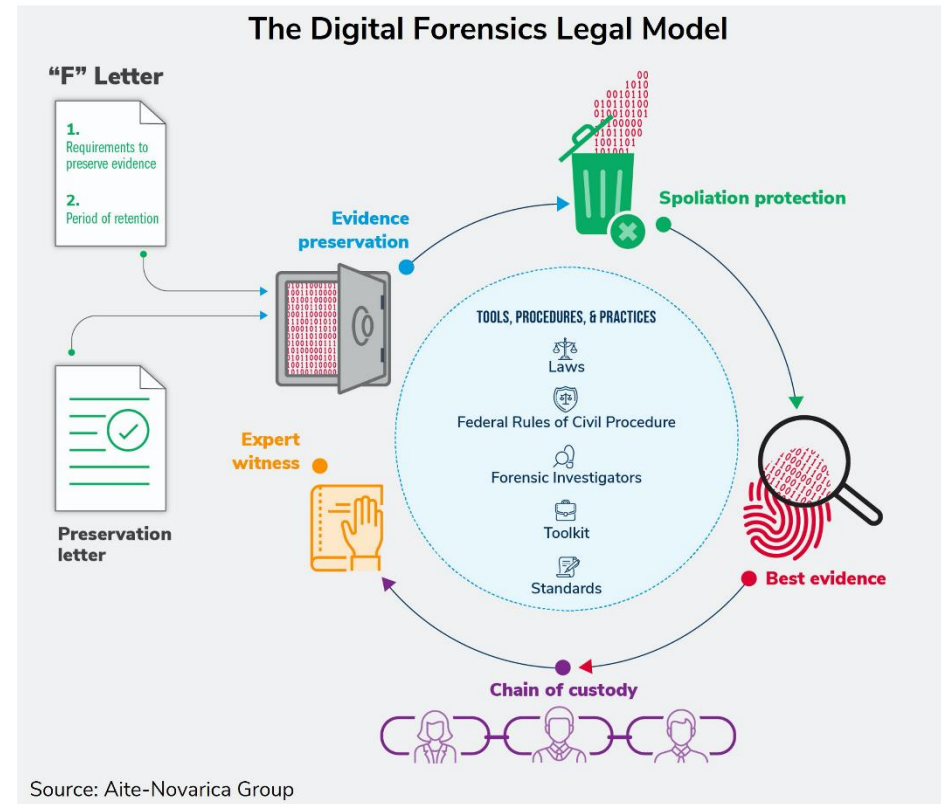
Computer Forensic Investigation from Corporate (cont.)



Computer Forensic Investigation from Law Enforcement

- Examples :
 - Sometimes, it's as simple as making sure government employees **don't misuse the access** they have been granted to view the tax information by periodically reviewing their activities.
 - Many times, it's as serious as helping to defend the government **by protecting the most vital top secret** information by working within a counter intelligence group.

Computer Forensic Investigation from Law Enforcement (cont.)



(Plus) Private Investigations

- Examples:
 - **Divorce:** Divorce lawyers ask examiners to assist in the examination of personal computers belonging to spouses involved in divorce proceedings.
 - The focus of such investigations usually is to find information about **assets** that the spouse may be hiding and to which the other spouse is entitled.
 - **Crime:** Defense lawyers also ask forensic examiners to reexamine computers belonging to criminal defendants in order to refute the findings of the law enforcement investigations.

Corporate versus Law Enforcement Concerns

- The needs of the corporate world and those of law enforcement differ on several levels
 - Corporate focuses on detection and prevention
 - Law enforcement focuses on prosecution

Understanding investigator's office and laboratory

- A computer forensics lab is where you conduct your investigations, store your evidence, and do most of your work
- Lab facility must be physically secure so that evidence is not lost, corrupted, or destroyed
- It is harder to plan for a computer forensics lab for a police department than for a private organization or corporation
- Prepare a business case to enlist the support of your managers and other team members when building a forensics lab

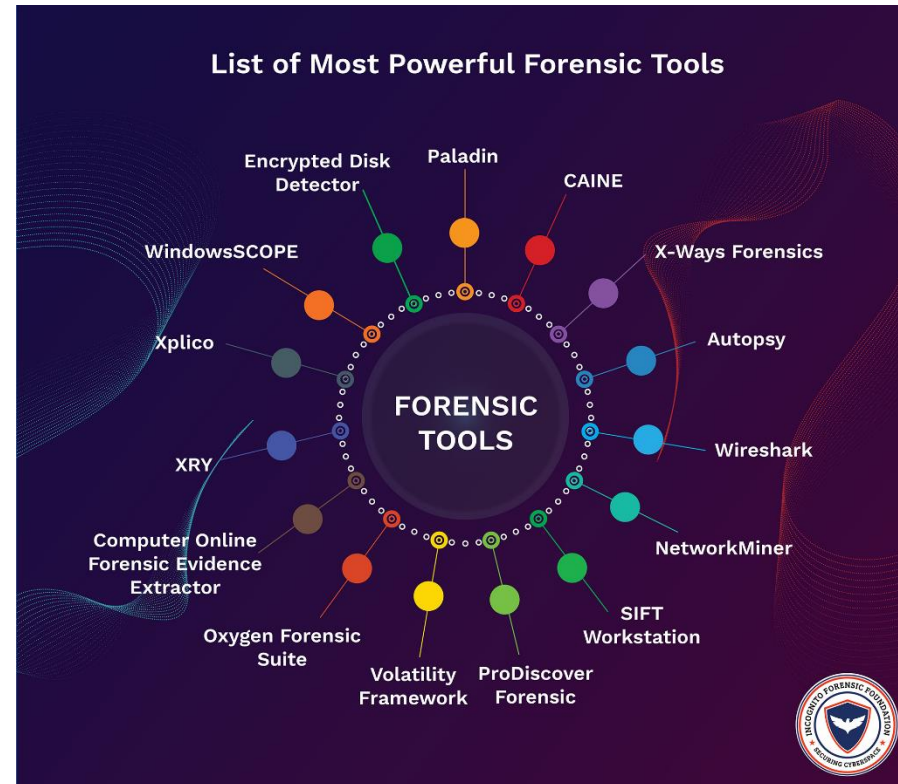
Digital Forensics Laboratory

- Transport evidence to your lab
 - Ensure security and integrity of digital evidence
- Record your activities and findings
- Goal
 - Reproduce the same results
- Save your journal for future references
 - At court
 - Training

DFIR Tools and Frameworks

- Hardware forensic tools
 - Single-purpose components
 - Complete computer systems and servers
- Software forensic tools
 - Command-line applications
 - GUI applications

DFIR Tool Examples



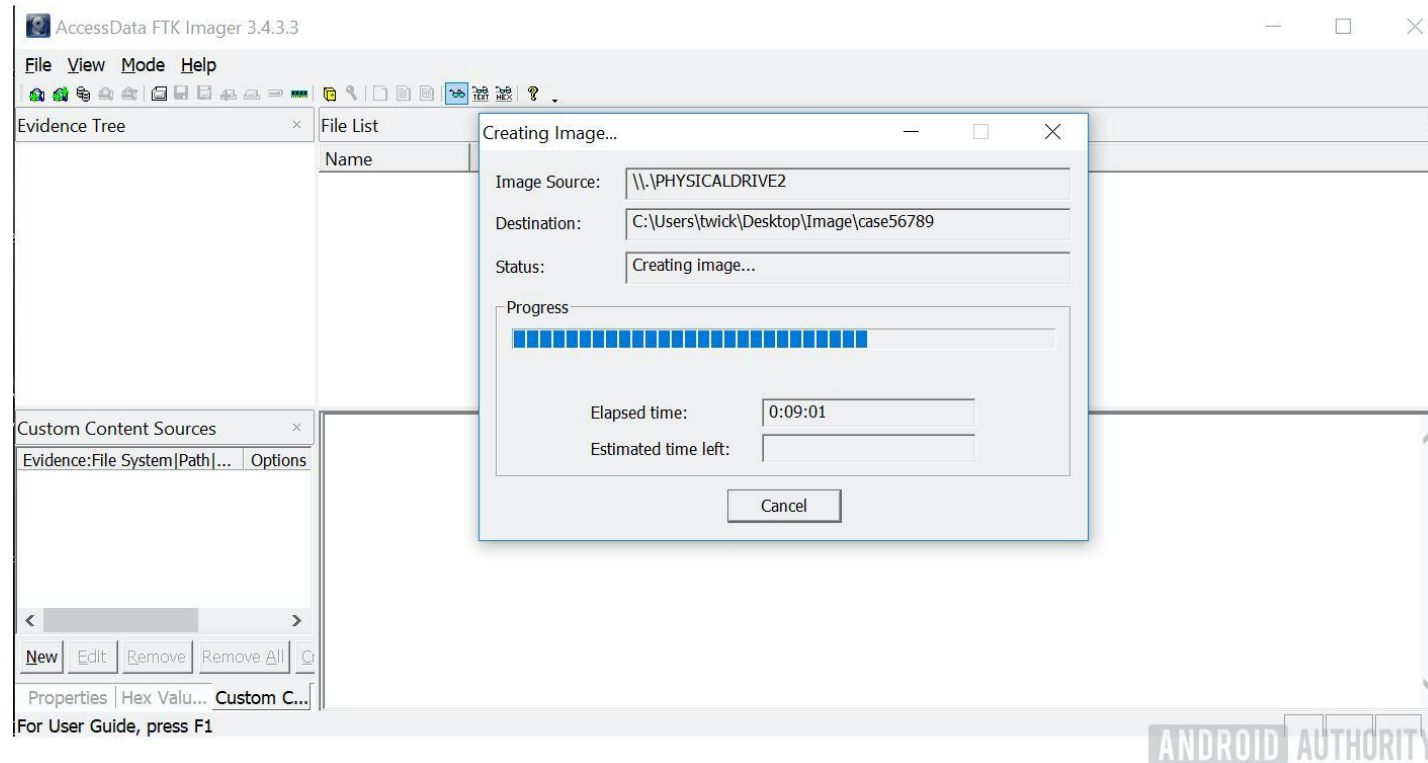
Tasks Performed by Computer Forensics Tools

- Acquisition
- Validation and discrimination
- Extraction
- Reconstruction
- Reporting

Acquisition

- Acquisition categories:
 - Physical data copy
 - Logical data copy
 - Data acquisition format
 - Command-line acquisition
 - GUI acquisition
 - Remote acquisition
 - Verification

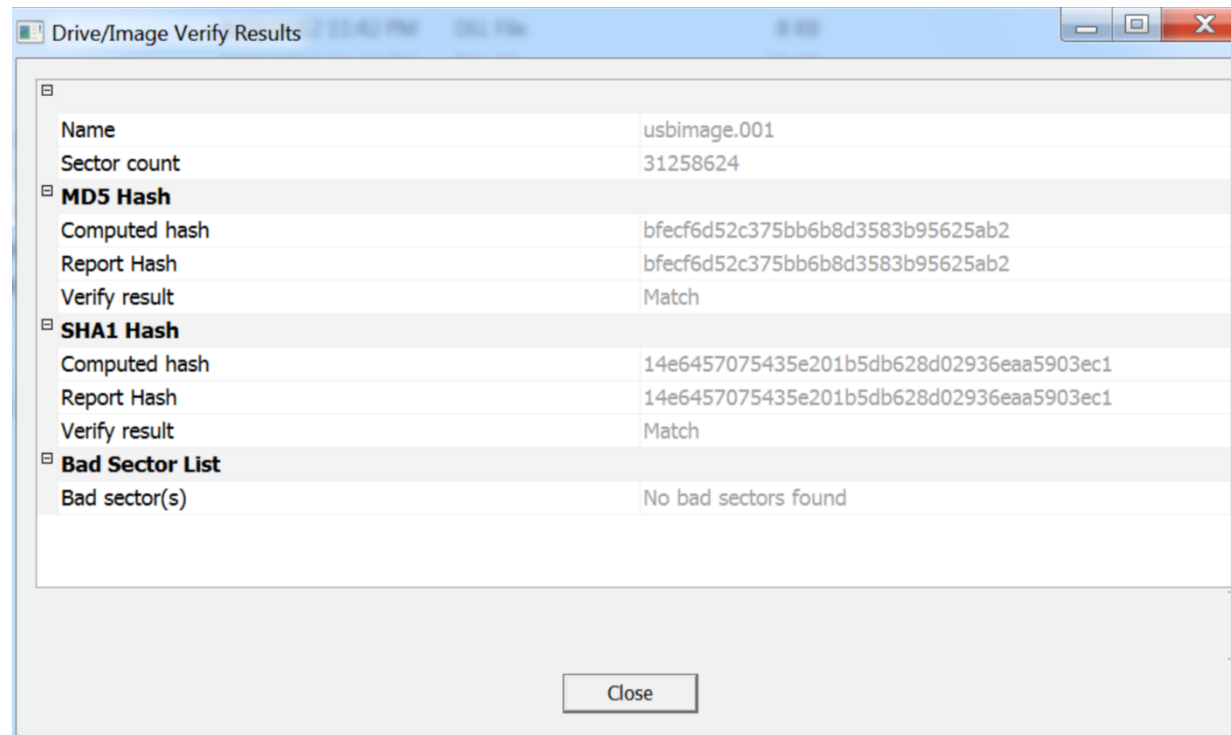
Acquisition (cont.)



Validation and Discrimination

- Hashing
 - Cyclic Redundancy Check (CRC)-32, MD5, Secure
 - Hash Algorithms (SHAs)
- Filtering
 - Based on hash value sets
- Analyzing file headers
 - Discriminate files based on their types

Validation and Discrimination (cont.)



Using a Write-Blocker

- Prevents data writes to a hard disk/Discards the written data
- Software options:
 - Software write-blockers are OS-dependent
 - PDBlock (Physical Drive (Write) BLOCKer))
- Hardware options
 - Ideal for GUI forensic tools
 - Act as a bridge between the disk and the workstation
- Connecting technologies
 - FireWire
 - USB 2.0
 - SCSI controllers

Using a Write-Blocker (cont.)



Extraction

- Major techniques include:
 - Data viewing
 - How data is viewed depends on the tool used
 - Keyword searching
 - Recovers key data facts
 - Decompressing
 - Archive and cabinet files

Extraction (cont.)

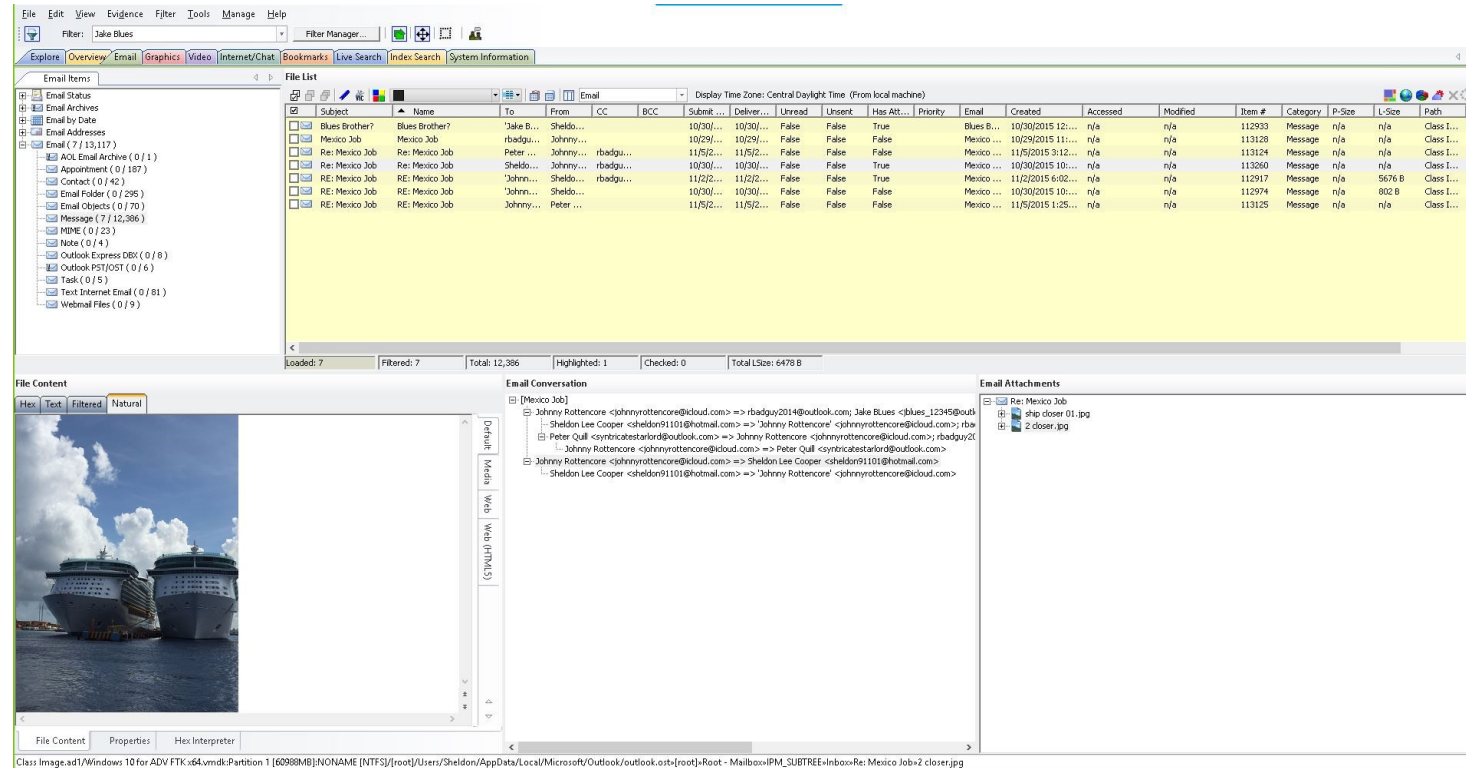
- Major techniques include:
 - Carving
 - Reconstruct fragments of deleted files
 - Decrypting
 - Password dictionary attacks
 - Brute-force attacks
 - Bookmarking
 - First find evidence, then bookmark it

Reconstruction

- Re-create a suspect's disk drive
 - Techniques
 - Disk-to-disk copy
 - Image-to-disk copy
 - Partition-to-partition copy
 - Image-to-partition copy

Reconstruction (cont.)

Exterro FTK



Reporting

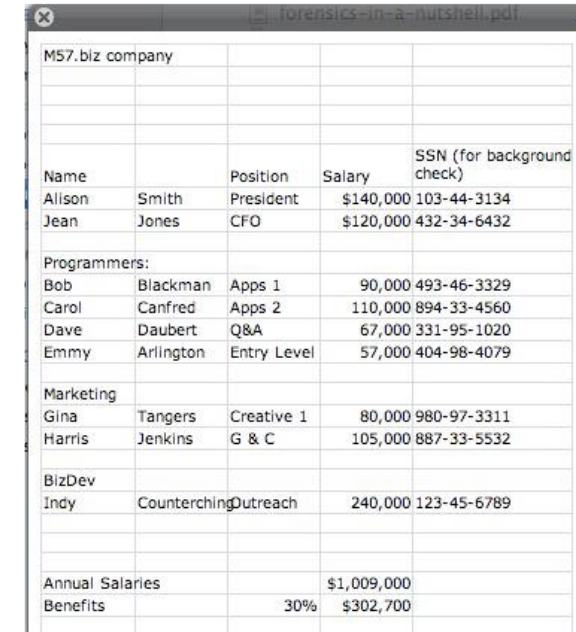
- Configure your forensic tools to:
 - Log activities
 - Generate reports
- Use this information when producing a final report for your investigation (this will be expanded upon in a future lesson)

Cyber Forensics Case Study, M57-Jean, Case of Corporate Exfiltration

- M57.biz is a hip web start-up developing a body art catalog
- M57.biz is a virtual corporation
 - Programmers:
 - Work out of their houses
 - Daily online chat session; Weekly in-person meetings office park
 - Marketing & BizDev:
 - Work out of hotel rooms or Starbucks (mostly on the road)
 - In-person meetings once every two weeks.
 - Most documents are exchanged by email.
- A spreadsheet containing confidential information was posted as an attachment in the "technical support" forum of a competitor's website.
- The spreadsheet came from CFO Jean's computer
- How did the documents get on the competitor's website?

Cyber Forensics Case Study, M57-Jean, Case of Corporate Exfiltration

- Summaries of interviews:
 - Alison (President):
 - I don't know what Jean is talking about.
 - I never asked Jean for the spreadsheet.
 - I never received the spreadsheet by email.
 - Jean (CFO):
 - Alison asked me to prepare the spreadsheet as part of new funding round.
 - Alison asked me to send the spreadsheet to her by email.
 - That's all I know.
- Spreadsheet in question:



The screenshot shows a PDF document titled "forensics-in-a-nutshell.pdf" containing a spreadsheet for "M57.biz company". The spreadsheet lists employee details including Name, Position, Salary, and SSN (for background check). It is divided into sections for Programmers, Marketing, and BizDev.

M57.biz company				
Name		Position	Salary	SSN (for background check)
Alison	Smith	President	\$140,000	103-44-3134
Jean	Jones	CFO	\$120,000	432-34-6432
Programmers:				
Bob	Blackman	Apps 1	90,000	493-46-3329
Carol	Canfred	Apps 2	110,000	894-33-4560
Dave	Daubert	Q&A	67,000	331-95-1020
Emmy	Arlington	Entry Level	57,000	404-98-4079
Marketing				
Gina	Tangers	Creative 1	80,000	980-97-3311
Harris	Jenkins	G & C	105,000	887-33-5532
BizDev				
Indy	Counterch	Outreach	240,000	123-45-6789
Annual Salaries			\$1,009,000	
Benefits			30%	\$302,700

Cyber Forensics Case Study, M57-Jean, Case of Corporate Exfiltration

- Analysing this case, Jean's computer hard drive is imaged, and this image is then processed using a relevant forensic tool such as FTK
- By finding the relevant spreadsheet and further details, it is revealed that Alison's email address was spoofed, and the unsuspecting Jean created and sent the information to who he thought was Alison

From: Jean User <jean@m57.biz>
Sent: 20/07/2008 02:28:47 +0100
To: alison@m57.biz
Subject: RE: Please send me the information now
Attachments: m57biz.xls

I've attached the information that you have requested to this email message.

-----Original Message-----
From: alison@m57.biz [mailto:tuckgorge@gmail.com]
Sent: Sunday, July 20, 2008 2:23 AM
To: jean@m57.biz
Subject: Please send me the information now

Hi, Jean.

I'm sorry to bother you, but I really need that information now --- this VC guy is being very insistent. Can you please reply to this email with the information I requested --- the names, salaries, and social security numbers (SSNs) of all our current employees and intended hires?

Thanks.

Alison

Name	m57biz.xls
Item Number	17515
File Type	Excel 2000
Path	nps-2008-jean.E01/Partition 1/NONAME [NTFS]/[root]/Documents and Settings/jean/Desktop/m57biz.xls
General Info	
File Size	
Physical Size	294,912 bytes (288.0 KB)
Logical Size	291,840 bytes (285.0 KB)
File Dates	
Date Created	20/07/2008 02:28:03 (2008-07-20 01:28:03 UTC)
Date Accessed	20/07/2008 02:28:03 (2008-07-20 01:28:03 UTC)
Date Modified	20/07/2008 02:28:03 (2008-07-20 01:28:03 UTC)
File Attributes	
General	
Actual File	True
Start Cluster	645,029
Compressed	False
File Type (FBFS)	OLE Archive
Start Sector	5,160,295
File has been examined for slack	True
Child Order	0
DOS Attributes	
Hidden	False
System	False
Read Only	False
Archive	True
NTFS Information	
MFT Record Number	32,712

Summary

1. What Is Cyber Forensics
2. Cyber Forensics Skills
3. Cyber Forensic Profession
4. Cyber Forensics Process, Investigation and Analysis
5. Electronic Discovery
6. Computer Forensic Investigation from Corporate
7. Computer Forensic Investigation from Law Enforcement
8. Private Investigations



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Any Questions?

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk