HERIOT WATT UNIVERSITY

Topic 2: Digital forensics & digital evidence

F20FO/F21FO – Digital Forensics

Mike Just (Edinburgh)

Ryad Soobhany (Dubai)

LEADERS IN IDEAS AND SOLUTIONS

HERIOT WATT UNIVERSITY

Recap – Topic 1

- Topic 1: Introduction to digital forensics
  - Computer security
  - Computer crimes
  - Digital evidence & forensics
  - Our lab study environment

LEADERS IN IDEAS AND SOLUTIONS

Topic overview

- Topic 2 overview: Digital forensics & digital evidence
  - Digital forensics evolution
  - Digital investigations & evidence
  - Digital forensics tools

Learning Outcomes

- Define and understand concepts in digital forensics
- Appreciate the importance of chain of custody in handling digital evidence
- Guidelines for dealing with digital evidence
- Identify and explain different imaging toolkits

HERIOT WATT UNIVERSITY

LEADERS IN IDEAS AND SOLUTIONS

Digital forensics evolution

What is Digital Forensics

Some definitions:

Computer Forensics is the scientific **examination** and **analysis** of **data** held on, or retrieved from, **device storage media** in such a way that the information can be used as **evidence** in a court of law

Computer forensics is the practice of **collecting, analysing and reporting** on **digital data** in a way that is **legally admissible**. It can be used in the detection and prevention of crime and in any dispute where evidence is stored digitally. Computer forensics follows a similar process to other forensic disciplines and faces similar issues.

What is Digital Forensics

Some important points:

- There are many definitions for DF. While the specific wording might differ, there are key similarities
- The output of a digital forensics process is to produce **data**
- The data is used as **evidence** in a court of law that a crime occurred (what, when, who, how)
- Digital forensics follows a **scientific process** for the data collection, similar to other forensics disciplines

What is Digital Forensics

The digital forensics process:

- The names of the steps can vary, but are essentially the same
  - Collection, analysis, reporting

1. **Collection** of data
   - Requires acquisition of data sources, e.g., drives, cloud data, mobile devices, …
   - Requires identification of data related to reason for investigation, e.g., approach might differ depending on whether I'm looking for malware, or indecent images
   - Collection process can have several options/questions, e.g.,
     - Should focus by on static data (e.g., hard drive) or also on temporary memory (e.g., RAM)?
     - Should I anticipate encrypted data
     - How much data, how many devices, should data be sought from cloud sources, etc.?
   - Above questions answered with interaction with investigation team

What is Digital Forensics

2. **Analysis** of data
   - Similarly iterative with follow-up questions to investigations team
     - E.g., initial search of one device related to its use in drug trade might lead to connections to multiple accounts and devices
   - Any “evaluation” of the data should remain objective
3. **Reporting** of data
   - Results must be grounded in the evidence
   - Report might lead to more questions and further analysis

What is Digital Forensics

- The steps in the DF process might vary (depending on the source) but the same activities occur, e.g.,
  - Previous slides: collection, analysis, reporting
  - Later in these slides we refer to a 4-step process: Acquisition, identification, evaluation, presentation
- The core activities are happening for each step, however they might be named
- Hence, there needs to be activities that
  1. Acquire devices, identify and collect data
  2. Evaluate/analyse the data
  3. Report/present the results

What is Digital Forensics

- Other DF terminology will also vary, depending on your source, e.g., “digital forensics” vs “computer forensics”
  - “Digital forensics” is more common now (and even “cyber forensics”) since it more clearly includes digital technologies beyond traditional computers, e.g., phones, smartphones, cameras, cloud systems, networks, doorbell cameras, etc.
- Don’t worry too much about the differing terminology, so long as a scientific process is followed
- We’ll mention some of the efforts to standardize digital forensics terminology and processes later

Digital Forensics Goals

Some more tangible goals of digital forensics:

1. Deleted file recovery. Retrieving files that have been logically removed but still leave recoverable traces on disk.
2. Timeline analysis. Helps to reconstruct the timeline of file (user) actions by examining metadata such as access, modification, and creation times.
3. Metadata extraction. retrieves embedded information (e.g., file owner, origin device, creation tool) that supports attribution and contextualisation.

Digital Forensics Goals

To achieve these goals, DF practitioners have

1. Several specialised tools, such as imaging and carving tools, and write blockers (discussed later in lecture)
2. Access to existing tools used to manage an OS and filesystem, and potential access to existing data such as metadata, system information (discussed next lecture)

Digital Forensics Evolution

1888: Francis Galton made the first-ever recorded study of fingerprints

1893: Hans Gross was the first person to apply science to a criminal investigation

1910: Albert Osborn became the first person to develop the essential features of documenting evidence during the examination process

1932: The FBI set up a laboratory to provide forensic services to all field agents and other law authorities

Digital Forensics Evolution

1970s: Electronic crimes were increasing, especially in the financial sector. Most law enforcement officers didn't know enough about computers to ask the right questions or to preserve evidence for trial

1980s: PCs gained popularity and different OSs emerged. Disk Operating System (DOS) was available. Forensic tools were simple, and most were generated by government agencies

Mid-1980s: Xtree Gold appeared on the market able to recognize file types and retrieve lost or deleted files. Norton DiskEdit soon followed and became the best tool for finding deleted files

Digital Forensics Evolution

1984: Scotland Yard: Computer Crime Unit & FBI computer forensics departments

Early 1990s: Tools for computer forensics were available

- International Association of Computer Investigative Specialists (IACIS)
- Training on software for forensics investigations
- IRS created search-warrant programs
- ExpertWitness for the Macintosh
- First commercial GUI software for computer forensics created by ASR Data
  - Recovers deleted files and fragments of deleted files

1990: Computer Misuse Act (CMA)

Digital Forensics Evolution

1993: The first international conference on computer evidence was held in the United States

1995: The International Organization on Computer Evidence (IOCE) was formed to provide a forum to global law enforcement agencies for exchanging information regarding cyber crime investigation

2000: The first FBI Regional Computer Forensic Laboratory (RCFL) was established for the examination of digital forensic in support of criminal investigations such as identity theft, hacking, viruses, etc

Digital Forensics Evolution

2000-2010s: The Mobile and Cloud Era

- Development of specialized tools for mobile device forensics
- Emergence of cloud forensics to deal with distributed and virtualized systems
- Increased focus on live forensics and memory analysis
- Growing importance of network forensics

2010s-present: Big Data and AI

- Use of big data analytics to process large volumes of digital evidence
- Application of machine learning for pattern recognition and anomaly detection
- Advancements in handling encrypted data and cryptocurrencies
- Increased focus on IoT device forensics

https://www.cadosecurity.com/wiki/history-of-digital-forensics-how-it-evolved-over-time

Need for Digital Forensic

- Ensures the overall integrity and continued existence of computer systems and network infrastructure in organisations
- Helps the organisation capture important information if their computer systems are compromised
- Extracts, processes, and interprets the actual evidence in order to prove the offence of the attacker
- Efficiently tracks down cyber criminals and terrorists
- Saves the organisation money and valuable time
- Tracks complicated cases such as child sexual exploitation (CSE)

HERIOT WATT UNIVERSITY

Digital investigations and evidence

Digital Investigation

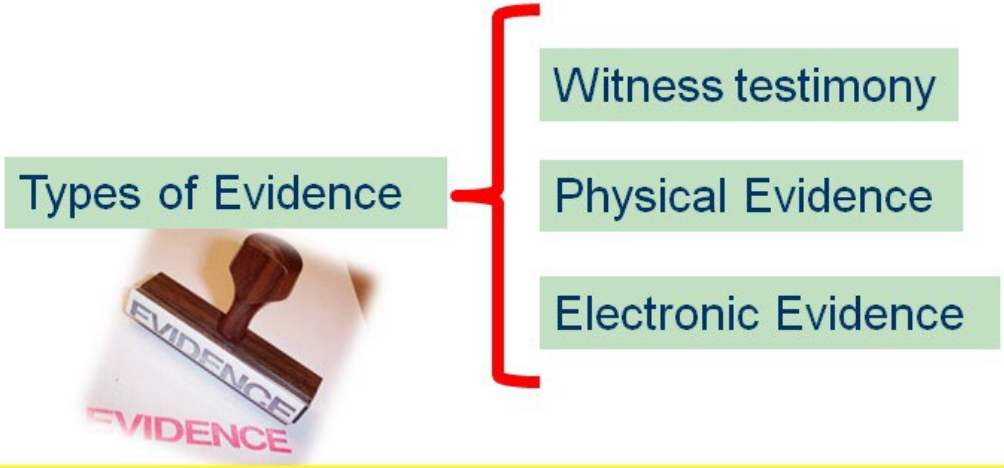
- A digital investigation is a process where we develop and test hypotheses that answer questions about digital events

- Digital evidence is a digital object that contains reliable information that supports or refutes a hypothesis.

- B. Carrier, 2006
  File System Forensic Analysis

Digital Evidence

- Digital Evidence is any information of probative value, which is stored or transmitted in digital form*



- In legal terms
  - Evidence is factual proof of what did or did not happen

SWGDE: Scientific Working Group on Digital Evidence
https://www.swgde.org

Examples of Digital Evidence

- Computer system
  - PC, Monitor, Keyboard, mouse
  - Laptop
  - Other peripherals or externally connect drivers

- Storage devices
  - Hard drives, e.g. SATA drive
  - laptop hard drives, e.g. IDE drive
  - External hard drives
  - Removable media e.g. CD, DVD, Floppy disk
  - Thumb drives including hidden ones in pens, keys, watches

Examples of Digital Evidence

- Memory card e.g. SD / Micro SD card, compact flash card
- Handheld devices e.g. mobile phones, tablets, gaming devices
- Peripheral devices e.g. Web cam, VoIP devices, printer, scanner, surveillance camera
- Computer network e.g. Network hub, wireless access point, wireless USB devices

Characteristics of Evidence

- Data can be viewed at different levels of abstraction
- Data requires interpretation
- Data is fragile
- Data is voluminous
- Data is difficult to associate with reality

Some Case Examples

- Let's consider a few examples of criminal cases and the integration of digital forensics activities
- Take note of the steps followed to collect the data
- And also, how the DF expert is integrated with the investigations team (e.g., police, legal)
- We'll consider two criminal cases, and one corporate case

Example 1 – Criminal Case

- Person A suspected of crime against B (victim)
  - A obtained B's website credentials and modified the website
- B filed a police report
  - Indicated suspicions of A's actual identity
  - Investigators collected **evidence** related to website (e.g., contents, access dates), including some graphic images
- Based on this, a warrant was obtained
  - A was questioned, and their **computing equipment** seized
  - Questioning revealed that A used a **chat client** to communicate with B
  - A claimed to be a web designer offering to help B with their website, and convinced B to share their credentials

Example 1 – Criminal Case

- Investigation of A's **computing equipment**
  - Focused on modification to B's website
  - Found modified versions of B's website on A's **laptop**
  - Also, evidence of **graphic images** that were uploaded on B's website
  - Subsequent search on A's **other devices** (smartphone) found evidence of downloaded images

Example 2 – Criminal Case

- Person A accused of murdering B (victim)
- A had an alibi from their partner – they were 90mins away from the victim's location at the time of the crime
- A warrant was obtained for A's computing equipment
  - Data collected from A's smartphone
  - The IMEI (International Mobile Equipment Identity) was obtained from the phone*
  - Mobile carriers contacted to confirm whether the phone (IMEI) connected to any mobile towers close to the crime scene at the time of the crime
- There was a connection to such a tower in the time window – evidence used to convict A

* Dial *#06# on your own phone to see your IMEI

Example 3 – Corporate Case

- Person A terminated by company B (victim)
- Suspected that A installed Trojan horse on company network to allow subsequent access
  - Trojan detected by IT department
  - Trojan configured to connect to IP address located near address of employee A
  - Company decided not to involve police (which would have been required to search devices and match the IP address)
  - Further investigation determined Trojan was installed from USB
  - Identifier from USB linked back to employee (via company-issued USB)
- Employee was confronted with evidence, admitted their role and a civil lawsuit was filed

Digital Forensics Methodology – 4 Phases

1 - Acquisition

Physically or remotely obtaining possession of the computer, all network mappings from the system, and external physical storage devices

2 - Identification

Identifying what data could be recovered and electronically retrieving it by running various Computer Forensic tools and software suite

Digital Forensics Methodology – 4 Phases

3 - Evaluation

Analysis of the information/data recovered to determine if and how it could be used.

4 - Presentation

Presentation and reporting of evidence discovered in a manner which is understood by lawyers, non-technical staff/management, and suitable as evidence

Assurance of the Forensic Expert

- No possible evidence is damaged, destroyed, or compromised by the forensics procedures used to investigate the computer (Preservation of evidence)
- No possible data corruption is introduced to the computer being investigated during the analysis process (Prevention of contamination of evidence)
- Any extracted and possibly relevant evidence is properly handled and protected from damage (Extraction and Preservation of evidence)

Assurance of the Forensic Expert

- A complete documentation of the investigation procedure (Accountability of the evidence)
- Ensuring minimum interference with the normal life of the organisation
- Details of the client-attorney relationship are not disclosed in order to maintain professional ethics and legality (Ethics of investigation)

Locard's Exchange Principle

"Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him…

It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value"

- A key concept in forensic examinations and processing
  - more suited to traditional forensics
- What significance is there to digital forensics?

Investigation principles and strategies

- Evidence investigation can be labour intensive
- Electronic evidence is volatile and may be easily changed
- Electronic evidence conversely is difficult to delete entirely
- Association of Chief Police Officers (ACPO) suggested a good practice guide (ACPO guidelines)
- Four principles of computer based electronic evidence
- Ensure that all forensic investigators use the same framework /standard

Why Standardise?

- Human errors occur
- Difficult to quantify
- Standards provide consistency for
  - Practices
  - Processes
  - Procedures
- To allow evidence to stand test of court

ACPO Guidelines

Principle 1

No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court

ACPO: Association of Chief Police Officers
Copy of ACPO guidelines on Canvas

ACPO Guidelines

Principle 2

In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions

ACPO Guidelines

Principle 3

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

ACPO Guidelines

Principle 4

The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to

ISO and Accreditation

- Standards introduced for forensic laboratories
  - ISO 9001
  - ISO 17025
  - ISO 27001
- Accreditation for individual Forensic Analysts
  - EnCE (Encase Certified Examiner)
  - ACE (FTK examiner)

Advantages of Standards

- Promote market efficiency and expansion
- Foster trade
- Encourage competition and lower barriers to market entry
- Diffuse new technologies
- Protect consumers against unsafe or substandard products
- Enable interoperability among products
- External validation of processes and procedures

Advantages of DF Standards

- Consistency with all legal systems
- Allowance for the use of a common language
- Durability
- Ability to cross international boundaries
- Ability to instill confidence in the integrity of evidence
- Applicability to all forensic evidence
- Applicability at every level including that of individual, agency, and country

Disadvantages of Standards

- When standards work poorly, they can:
  - Raise transaction costs and barriers to trade/significant burden for smaller operations
  - Constrain innovation and entrench inferior technologies
  - Hinder the development of interoperable systems

UAE Digital Evidence

- Law to address e-crime adopted in 2006
  - First in GCC
- Cybercrime laws being adopted and reviewed

- UAE's Criminal Procedure Law (CPL)
  - Deals with electronic evidence

Chain of Custody

The chain of custody means keeping a complete log (including time, date, actions taken and reasons) of the steps taken in the investigation from the beginning (i.e. seizure of the digital equipment) to the presentation phase in a way that one can follow the steps and obtain the same results

Chain of Custody Documentation I

- Case description:
  - Case Number (ID)
  - Investigation unit
  - Lead Investigator
  - Incident Type
- Evidence description:
  - Evidence ID
  - Description of evidence (item): Name of evidence, colour, marking
  - Item serial number
  - Evidence obtained: Location, Reason for evidence, Date/time

Chain of Custody (CoC) Documentation II

Date & Time	From	To	Purpose of transfer	Description of action	Location	Signature

- CoC should have the case description, evidence information and log table
- Log table should document the exchange of evidence between people
  - Location is optional for some cases

Chain of Custody Example

Mobile phone seized from suspected drug dealer

Case description:

- Case Number (ID) DF-5246
- Investigation unit: Digital Forensics Unit
- Lead Investigator Taper Lo
- Incident Type Drug Dealing

Evidence description:

- Evidence ID ED-01
- Description of evidence Mobile phone, Apple iPhone 13, white
- Item serial number (IMEI) 258963147633985
- Seized location Suspect's front jeans pocket
- Reason for evidence device used part of drug dealing
- Date/time 10/06/2025 13:50

Chain of Custody Example

Date & Time	From	To	Purpose of transfer	Description of action	Location	Signature
10/06/2025 13:50	Joe Lewis (suspect)	Officer R. Shah	Seizure of phone	Device seized	City Land Mall	R. Shah
10/06/2025 13:55	Officer R. Shah	Officer R. Shah	Prevent remote access	Device placed in Faraday bag	Officer's car	R. Shah
10/06/2025 17:00	Officer R. Shah	Mel Sue	Storage	Secure storage	Evidence room	R. Shah
12/06/2025 10:00	Mel Sue	Taper Lo	Evidence checked out	For Data acquisition	Forensic lab	Taper Lo
12/06/2025 15:00	Taper Lo	Taper Lo	Analysis	Physical extraction (oxygen Forensics) and hash verified	Forensic lab	Taper Lo
12/06/2025 15:30	Taper Lo	Mel Sue	Evidence checked in	Return to Secure storage	Evidence room	Taper Lo

Rules of Evidence

- There are five rules of collecting electronic evidence. These relate to five properties that evidence must have to be useful

1. Admissible
2. Authentic
3. Complete
4. Reliable
5. Believable

Search Warrant for Admissible Evidence

- Search warrants are issued if law enforcement provides sufficient proof that there is probable cause a crime has been committed
- The law officer must specify what premises, things, or persons will be searched
- Evidence discovered during the search can be seized
- An expert witness is a qualified specialist who testifies in court
- Expert testimony is an exception to the rule against giving opinions in court

HERIOT WATT UNIVERSITY

Volatile Evidence

- Not all of the evidence on a system is going to last very long
- Try to proceed from the most volatile data to the least
  - Registers and cache
  - Routing tables
  - Process table
  - Main memory
  - Temporary file systems
  - Router configuration

Evidence Collection Principles

- Maintain chain of custody of the evidence
- Acquire evidence from volatile as well as non-volatile memory without altering or damaging original evidence
- Maintain the authenticity and reliability of evidence gathered
- No modification of data while analysing it

- How might we achieve this?

HERIOT WATT UNIVERSITY

Digital forensics tools

Forensics Laboratory Tools

- Storage bags
- Remote chargers to power devices
- Write block protection devices
- Rapid Action Imaging devices (RAIDs)
- SIM card readers

HERIOT WATT UNIVERSITY

Data Acquisition

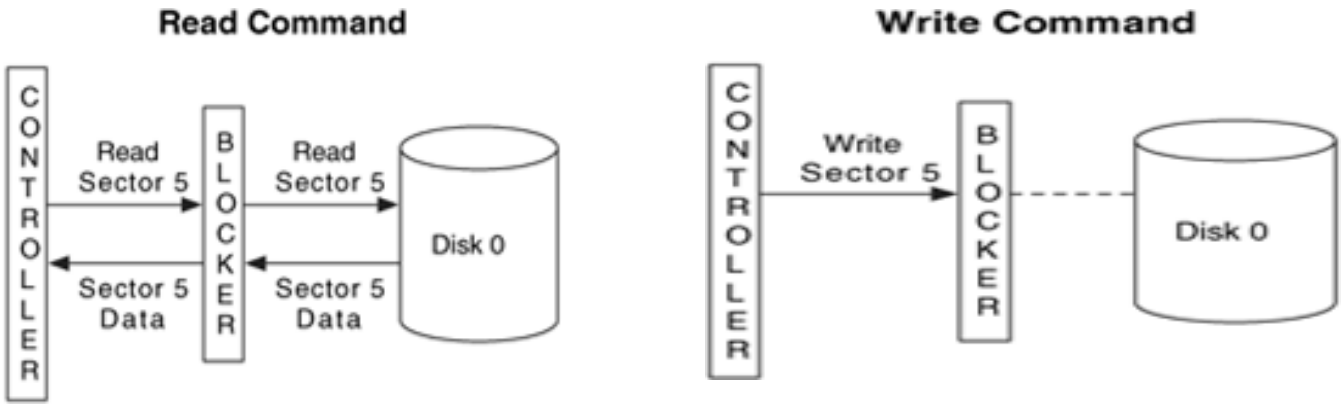
- Data acquisition is the act or process of gathering information and evidence
- Use established methods to acquire data from a suspect computer or storage media to gain insight into a crime or other incident and potentially use it as evidence
- Goal of data acquisition is to preserve evidence, so any tools that are used should not alter the data in any way and should provide an exact duplicate
- To prevent contamination, any data that is duplicated should be stored on forensically sterile media, meaning that the disk has no other data on it and has no viruses or defects

Data Duplication

- Duplication of data is a critical part of any computer forensic investigation
- To effectively examine data on a suspect machine, a person performing a forensic examination of the machine needs to create an **image** of the disk
- To ensure that all data is acquired, a bitstream copy needs to be made
- Each physical sector of the disk is copied so that the data is distributed in the same way, and then the image is compressed into a file called an image file
- This will acquire any hidden files, temp files, corrupted files, deleted files (not yet been overwritten), file fragments, slack space, and other data

Write Blocker

- It is important to modify the original data as little as possible
- Many acquisition techniques do not modify any of the original data, but there are techniques that can modify the original data, and this has to be prevented

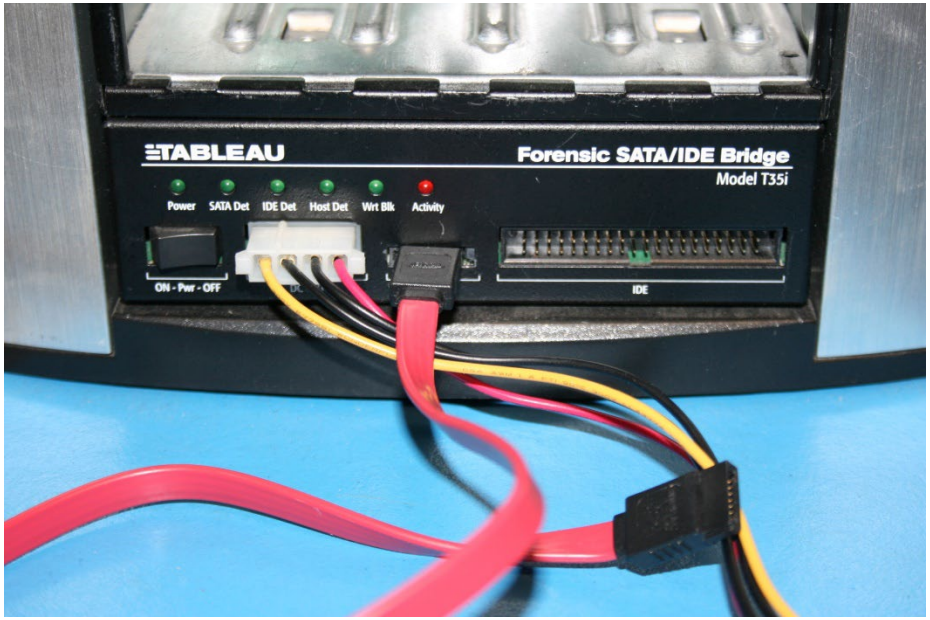


Write Blocker

- A hardware write protector is a device that sits in the connection between a computer and a storage device
- It monitors the commands that are being issued and prevents data being written to the disk
- These devices are important when using an OS that could mount the original disk

Write Blocker

- Prevents examiner from altering data that is being collected or analysed
- IDE, SATA, SCSI and USB devices
- FireWire and removable storage devices



Hashing

- A hash function 128-bit take out a variable length input and produce a fixed length output that will uniquely identify the input
  - Fingerprint of the data
- Used to validate that the digital investigator has not altered the integrity of the acquired data
- MD5 (Message Digest 5)
  - 128-bit output
- SHA-1 (Secure Hashing Algorithm)
  - 160-bit output
  - SHA-256

Hashing

- Hash codes can be used to quickly match files found during investigations to lists of “Known Files”
  - innocent files, such as components of MS Windows and “off the shelf” application software, that can safely be ignored
  - contraband files, such as child pornography and hacker tools, that should be highlighted

Evidence Imaging/Acquisition

- In order to perform analysis on *digital artefacts*, a *forensic duplicate* of the media is created
- This process is known as *imaging* or *acquisition*
- As you've learned already *write blockers* are used to preserve the disk state
- And *cryptographic hash functions* to verify the image against the original artefact

Evidence Imaging/Acquisition

- Some of the previous terms require some more precision:
  - *Digital artefact*: A reproducible file, setting or system change that occurs every time an application or OS performs an action
  - *Forensic duplicate*: Bit-for-bit copies of the original disk (full disk or some partitions)

Imaging Tools

- Access Data FTK
  - FTK Imager free for use with registration
- Guidance Software – Encase
  - Tool most used by LEA and private companies
  - Good level of support
- ProDiscover Basic
- Cellebrite – UFED

DD Imaging

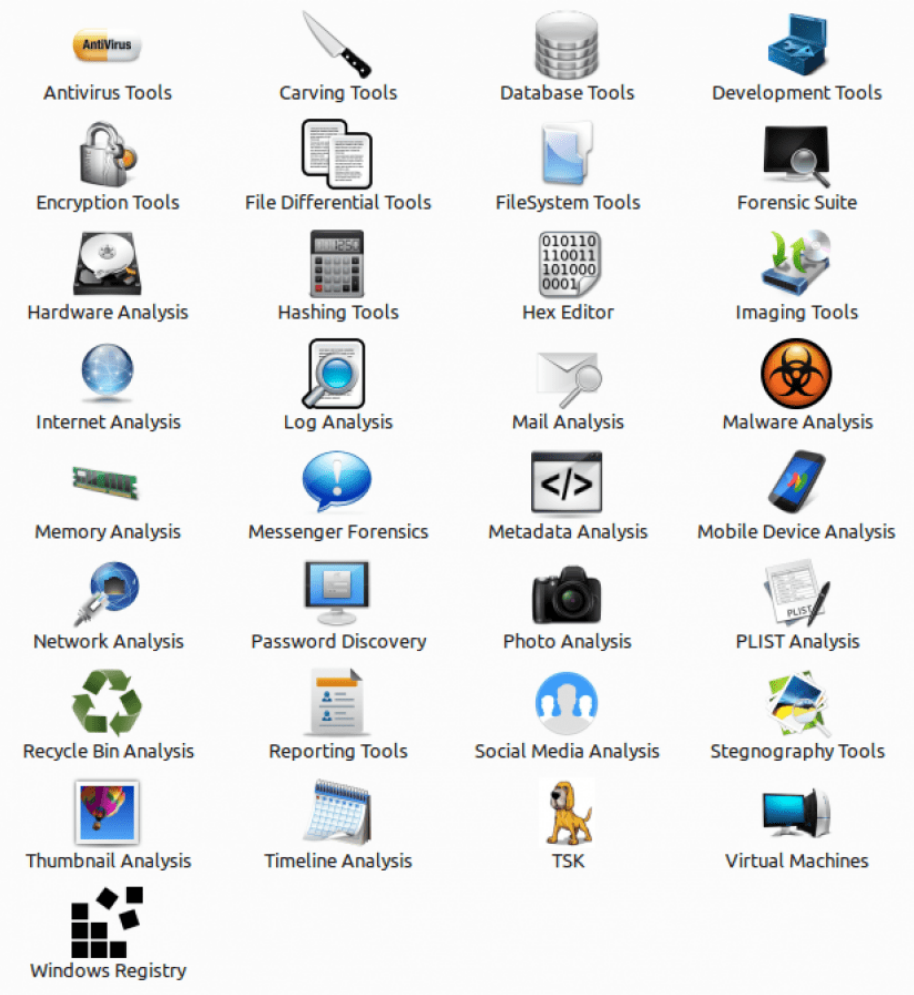
- Example steps to create image
  - Create MD5 checksum of the disk using the md5sum command
  - Create image file of the disk using the dd command
  - Create MD5 checksum of the image file using the md5sum command
  - Compare the MD5 checksum of the disk image file with the MD5 checksum of the disk
- Using a different disk
  - Restore the disk from the disk image file
  - Create MD5 checksum of the restored disk
  - Test MD5 checksum against the altered image file

Forensic Suites

- CAINE Computer Aided INvestigative Environment
- Linux live distribution aimed at Digital Forensics
- Collection of open source and freeware tools

Forensic Suites

- PALADIN
  - https://sumuri.com/software/paladin/
- Collection of open source and freeware tools
- Used by LEAs



Digital Evidence Challenges

- Size of storage devices
- Embedded flash devices
- Proliferation of operating systems and file formats
- Multi-device analysis
- Pervasive Encryption
- Cloud computing
- RAM-only Malware
- Legal Challenges decreasing the scope of forensic investigations

Example Technical Challenges

- Solid State Drives (SSDs), such as flash memory USB sticks, can be imaged in the same way as traditional hard disk drives (HDDs)
- However, there are some technology-specific issues that can cause problems for forensic investigators

Imaging Challenges with SSD

Following two issues can result in unallocated space being overwritten earlier than on a HDD:

- Program-Erase Cycles
  - Sequences of events that result in data being written, then erased and re-written
  - Can result in physical damage to drive (“bad sectors”)
- Wear Levelling
  - Rewrites distributed evenly across medium
  - Intent is for even wear to prolong life

Topic overview

- Topic 2 overview: Digital forensics & digital evidence
  - Digital forensics evolution
  - Digital investigations & evidence
  - Digital forensics tools

HERIOT WATT UNIVERSITY

Next topic

- Topic 3: Technical concepts
  - Operating systems
  - Data storage
  - File systems
  - Numbering systems

LEADERS IN IDEAS AND SOLUTIONS