Digital Forensics
Dr Harjinder Singh Lallie

VIDEO: I have produced a set of videos to accompany my module(s). Videos relevant to this handbook will be highlighted using this box and supported with an accompanying URL.

Contents

Part I

Fundamental Principles

Chapter 1

Fundamental Principles

The term *forensics* refers to the systematic application of scientific methods to reveal and present admissible evidence relating to incidents and/or events. The term is derived from the Latin word *forensis* which means 'legal' or 'pertaining to the courts' and *fora* which means 'the forum' - also indicating a 'court'. The reference to 'courts' is important, the investigator aims to produce evidence which is admissible in court. Although many investigations do not end up in court, this remains the litmus test for evidence gathered throughout an investigation.

There are numerous branches of forensics which include: forensic psychology/psychiatry, forensic DNA analysis, forensic anthropology, forensic odontology, forensic sociology, forensic pathology, forensic chemistry/toxicology, wild life forensic science, forensic engineering, forensic accounting, forensic nursing and forensic odontology. Many of these are older and more mature disciplines, digital forensics is a newer and much younger discipline.

The term *digital forensics* refers to the systematic application of scientific methods to investigate digital devices and reveal and present admissible evidence relating to incidents and/or events. The term encompasses computer forensics, computational forensics, network forensics, cyber forensics, e-forensics and eDiscovery[1].

Although digital forensics is often linked with the investigation of crime, a large section of the digital forensics industry has little or nothing to do with criminal investigation and is involved in civil/corporate investigations related to employment issues, corporate investigations and the investigation of hard-

[1]The term eDiscovery generally refers to the application of digital forensics techniques in the investigation of documents and files in live cases. For more information: Lawton et al. (2014)

ware/system failures. A large branch of this discipline is focused on the investigation of cyber incidents. For instance:

- A network server fails. An investigation is conducted to discover why it has failed. This may involve the investigation of particular logs to discover whether there was an 'event' leading up to the failure.
- A member of staff is suspected of IP (intellectual property) theft. A covert investigation is conducted to establish whether there is enough evidence to dismiss the member of staff. This is critical given the employee could subject the organisation to an employment tribunal at which point the organisation may need to demonstrate that due process was followed and that there was sufficient evidence supporting the decision.

1.1 Responsibilities

The investigator is responsible to two entities, the 'case manager' leading the investigation, and the 'court' to which the evidence will be presented. The responsibility of the investigator to the court overrides the responsibility to the case manager. The investigator cannot be overtly influenced or swayed in their opinion by the case manager or any other party involved or not involved in the investigation.

The case manager has overall responsibility for the case. Although the case manager may delegate that responsibility to multiple persons – each accountable to the case manager, the overall responsibility is not delegated.

The term 'court' is used loosely to refer to a court of law, tribunal, human resources, CEOs or any other entity that has either requested the investigation or to whom the outcome of the investigation may be presented.

Occasionally, an investigation begins as one type, but changes into another. For example, an internal investigation into the alleged exfiltration of corporate designs, reveals that the suspect also exfiltrated personal client data. This may need to be reported as a criminal matter and there could be pressure to report this to the Information Commissioner's Office as a matter of regulatory compliance.

1.1.1 Roles

There are typically several other roles involved within an investigation, these include:

- **The case technician.** The technician is responsible for managing all the digital evidence, imaging it, and preparing the forensic case ready for investigation. The technician manages the chain of custody forms, and secures the physical evidence.
- **The examiner.** The examiner performs the initial investigation, bookmarking and categorising evidence as required.
- **The analyst.** The analyst performs the 'final' investigation and produces the report. Some LEAs merge the two roles into one.

Forensic investigators require a multitude of skills which include: technical knowledge of computer systems (including networks, hardware and operating systems), knowledge of legal background – or at least the ability to present information in a scientifically sound manner whilst recognising the challenges of presenting this to legal audiences, and excellent communication skills - investigators have to write reports which are presented to a jury, most of whom do not understand computing or IT and good interpersonal/team-working skills.

1.1.2 Burden of Proof

The rules regarding burden of proof and the form that the investigation, reporting and decision making takes place varies between each of these incidents.

Criminal Cases Criminal incidents are investigated by a *law enforcement authority* (LEA). A case manager will be internally assigned to the case. We refer to the two parties of the case as the *prosecution* and *defence*. Typically a judge and jury make a decision concerning the case and the burden of proof generally rests with the prosecution who have to prove their case 'beyond reasonable doubt'.

Amongst the case manager's many responsibilities, the case manager must ensure that anybody working on a case has proper authority to act. This might include managing search and seizure warrants as well as a statement outlining the remit, intended outcomes and boundaries of the investigation.

Although many cases are investigated 'in-house', LEAs have often outsourced cases to independent digital forensic firms.

Civil Cases In a civil case, the investigation might typically be done by a commercial/private entity, an independent digital forensic firm for instance, and the case will be heard by a civil court presided over by a district/circuit

judge. We refer to the two parties as the *plaintiff* and the *defendant*. In this case, the plaintiff has to prove the case 'on a balance of probabilities'.

Internal investigations are often conducted in the mode of a civil investigation. We do not use the terms *plaintiff* and *defendant*, however, we do test the case 'on a balance of probabilities'.

1.2 Digital Storage Systems

A computer system comprises of three fundamental components: a digital storage system (referred to herein as DSS), a central processing unit (CPU) and an input/output system (I/O system).

A considerable part of the investigator's work revolves around the analysis of a DSS to identify evidence. Consequently, the investigator often needs to understand the architecture/operating system of the device as well as how it stores data.

The range of DSS' that an investigator may encounter is quite broad and includes any device capable of storing data in electronic format including: hard disk drives, portable storage systems such as SD/CF cards, USB sticks, smartphone storage systems, satellite navigation systems and even home alarm systems, in-car audio systems, satellite/cable TV systems, games consoles, certain IOT devices, and even autonomous vehicles.

There are two types of DSS: *permanent* and *volatile*. The data on a permanent DSS does not disappear following the removal of power to the device. Examples of permanent storage systems include hard disk drives, USB drives and SD cards.

Volatile storage systems use electrical current to organise the data in their memory, when that electrical current is removed from, the data is also removed. RAM and certain types of cache memory are examples of volatile storage systems. It is important to understand these subtle differences as they can have a significant impact on the nature of the investigation. For instance, a hard disk drive can be removed from a computer system prior to investigation, the RAM inside a PC based computer cannot be removed for examination as it would lose the electrical power and therefore the data contents.

Case Study

Autonomous Vehicles. Autonomous vehicles will contain multiple computer systems.[2], NVIDIA Drive products[3] These include components such as environment sensors - examples of which include: the Neobotix Ultrasonic Sensor System and Mobileye collision avoidance systems and the IntelGo autonomous driving products.
Each of these products conforms to the basic architecture of a computer system and contains a CPU, I/O system and a DSS. Collectively, 'computer systems' interact with the main vehicle control system. A forensic investigation of an autonomous vehicle is therefore a investigation of multiple computer systems and DSS'

Chapter 2

Evidence

The outcome of an investigation is evidence which supports a set of given assertions.

Evidence is 'information and data of value to an investigation that is stored on, received or transmitted by an electronic device'[1] and which supports an assertion or hypothesis. Evidence is not fact, and what might be evidence to one person, might not be seen that way by another, in other words evidence is only evidence once a 'decision maker' (a judge, jury, chair of an investigation panel) determines that it is evidence. Generally, experienced investigators are able to exercise good judgement in determining whether the case is likely to succeed on the basis of the evidence they have presented.

The burden of proof is the obligation of a party in an argument or dispute to provide sufficient evidence to shift the other party's or a third party's belief from their initial position.

The evidence in an investigation may consist of numerous items of data which can include combinations of textual data, pictures, communications and other items. A number of assertions may have been presented – for instance that the suspect:

- used and/or was in control of a particular computing device at a given time
- conducted communications with particular persons at a given time using a particular computing device

[1]The National Forensic Science Technology Center (https://www.nij.gov/topics/forensics/evidence/digital/pages/welcome.aspx)

- transferred documents/images to particular systems or people during his/her use of a particular computing device

Digital evidence takes multiple forms, the ownership of a computer, the hard disk itself, a file on the hard disk, a selection of text within the file, and the metadata that accompanies the file.

Many of the theories relating to the prevalence of digital evidence are inspired by traditional evidence theories such as those propagated by Professor Edmond Locard who outlined that: *"Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. 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."*

Locard's theories can be applied directly to digital evidence and consequently, every time a computing device is turned on, whenever a user accesses a file, runs a program, inserts a USB stick etc, 'evidence' is created. Generally, a digital transaction must have been conducted resulting in a change of state for a file. The job of the digital investigator is to search for the relevant transactions to find the evidence.

TASK

What evidence is created when a user installs an email client and sets it as the default email client?
What evidence is created when a user is using an iPhone and iTunes and is using WhatsApp on the phone?

Evidence can be divided into four categories: inculpatory, exculpatory, direct evidence and circumstantial evidence. The investigator searches for, and reasons with all four, and evaluates the value of evidence in each category.

Inculpatory evidence supports a given theory. This could include things like emails, text messages, social media posts, or other types of digital communications that show the person planning or discussing a crime, or that provide other evidence of their involvement in the crime.

Examples of inculpatory evidence include:

- An employee is accused of harassment (sending abusive/ harassing emails to a colleague). The case relies on 13 emails sent from the machine of the accused (evidenced by MAC addresses coupled with static IP addresses and corroborated with email logs).
- Browser history showing that the user was searching for information about how to commit a crime, or purchase an illegal item.

Exculpatory evidence contradicts a given theory and could introduce reasonable doubt. In the example cited above, the accused claims that he was on annual leave during the time that the emails were sent, somebody else must have logged into the machine and sent the emails.

Direct evidence supports the truth of an assertion directly, without an intervening inference. Testimony can be direct evidence or it can be circumstantial. For example, a witness claims he saw a crime take place (direct evidence). Another witness claims she saw the defendant enter a house, heard screaming, and saw the defendant leave the house with what appeared to be a bloody knife.

Circumstantial evidence shows circumstances that logically lead to a conclusion of fact. An inference is required to connect it to a conclusion of fact, judgements can be based entirely on circumstantial evidence. Circumstantial evidence usually accumulates into a collection - with the pieces in the collection becoming corroborating evidence. Together, they more strongly support one particular inference over another. An explanation involving circumstantial evidence becomes more valid as proof of a fact when the alternative explanations have been ruled out.

TASK

John Smith is accused of murdering his wife between the hours of 19:30 and 20:30pm on 1st January 2018 at his home address. Neighbour 'a' saw John enter the home address at around 19:15, and then leave at 20:35 in a 'panicked rush'. Neighbour 'b' heard John screaming "I will kill you!". John's mate 'Dave' said they were both in a tavern sitting in a corner waiting to be served between 19:30 and 20:30 and did not engage with anybody during this time.
In this case study, outline what you believe to be inculpatory, exculpatory, direct evidence and circumstantial evidence.

2.1 Admissibility

The admissibility of evidence is one of the most important elements of a forensic investigation. A long and strenuous investigation could be rendered ineffective because the evidence is considered to be inadmissible. Various standards and guidelines exist to help ensure consistency and adherence to good practice. Possibly one of the most important elements in terms of competency and admissibility concerns adherence to the Forensic Science Regulator's Code of Practice (FCR, 2023) which came into effect on 2nd October 2023.

TASK

The Forensic Science Regulator's Code of Practice (FCR, 2023) relates to all forms of forensic science. What are the salient points applicable to digital forensics?

The rules concerning *admissibility* generally state that the evidence must be relevant, accurate, unaltered/unchanged, authentic, and stored in a system that was secure throughout the item's lifetime. Furthermore, the evidence must have been revealed legally, properly and fairly, and there must be full disclosure of both exculpatory and inculpatory evidence.

2.1.1 Authority

Searches and seizures have to have been authorised and conducted within the parameters of the authority and scope given. An investigation of artefacts seized without due authorisation could render the evidence inadmissible. This is discussed in further detail in Section 4 (p 22).

2.1.2 Unaltered and Untampered Evidence

Various procedures exist to prevent the alteration and tampering of evidence. The two most important of these are the use of digital forensic images (Chapter 5, p26) in which the use of hashes ensures that the artefact being investigated is identical to that which was seized (Section 5.5, p29), and Chain of Custody forms.

2.1.3 Relevant Evidence

Irrelevant evidence not only wastes court time and money, but also runs the risk of confusing a jury and altering the perception of the case. Evidence presented both in written and verbal form must be relevant. Relevance includes evidence which:

- Links or rules out a connection between two relevant entities within the investigation, e.g. victim and suspect, suspect and a website, suspect and a file.
- Supports or refutes suspect, victim and/or witness testimony
- identifies one or more suspects
- Helps reveal the suspect's modus operandi
- Demonstrates that a crime has taken

TASK

A study by Miller (2023) proposed that in *"11,000 digital forensics laboratories across the United States, prosecutors often have a poor understanding of digital data's relevance to their cases, or how to use the evidence"*. Study this paper to understand the results of the survey and its' potential implications of the admissibility of evidence in the UK.

2.2 Integrity

Integrity refers to both the integrity of evidence and associated arguments presented in the report, as well as the integrity of the investigator and their approach to the investigation. The failure to act objectively and in an unbiased manner, and/or interpret and present the findings appropriately, can render the evidence inadmissible.

2.2.1 Tools and Methods

Forensically sound methods have to be used to obtain, process, and help analyse the evidence. This means that the tool has to be reliable, has to produce repeatable results, and should have some acceptance within the digital forensics community. To cater for this, it is common for the investigator to declare the

tools used to process given points of the investigation. The investigator must also specify version numbers.

That said, most tools have bugs and errors. If these are known and can be catered for, it is often acceptable to continue the investigation.

TASK

There have been several miscarriages of justice brought about because of the way evidence was processed or handled. One of the most well known in the UK judicial system was that of Police Sergeant (PS) Virdi who was sacked on the basis of evidence produced through what the Metropolitan Police Service referred to as the 'document reconstruction technique' (Metropolitan Police Authority, 2001).

What happened in this case? What was the 'document reconstruction technique'? What were the problems with this technique?

2.2.2 Investigatory Limitations

Potential uncertainties and limitations of the findings should be disclosed. To cater for this, it is common at this point for an investigator to outline that *"if ... then this would change my opinion"*. Example limitations may be artefacts that are obviously missing – obvious because the investigation revealed other artefacts not discovered in the crime scene seizure, or unexplained gaps in the timeline which could have a meterial effect on the conclusions of the investigation.

2.2.3 Full Disclosure and Exculpatory Evidence

Exculpatory evidence and any evidence revealed in the process of examination which may cast doubt on the findings and assertions or even the validity of the charges made, must be disclosed in full. Failure to disclose this could have a range of impacts on the outcome. This could result in a trial collapse. It could lead to a miscarriage of justice which could either see an innocent suspect found guilty, or a guilty suspect found innocent.

The rules concerning evidence disclosure vary between jurisdictions. In the UK for example, each party is *expected* to disclose evidence relevant to the issue under investigation (CPS, 2012).

In the United States, the law requires that all relevant evidence, including exculpatory evidence, be disclosed to the defendant in a criminal case. This requirement is referred to as the "duty of disclosure" and is based on the principle of fairness, which holds that the defendant should have access to all of the evidence that is relevant to their case in order to ensure a fair trial.

The failure to provide full disclosure can impact the outcome of proceedings and consequently affect the credibility of the parties and arguments concerned. The court has the power to impose severe sanctions on relevant parties in these cases.

Case Study

An example of where this went wrong is exemplified in the case of Liam Allan. Liam Allan was charged with 12 counts of rape and sexual assault. Amongst the key evidence were 57,000 messages which were never revealed until the case came for trial - two years after the charges were raised. When the messages were revealed, it transpired that the alleged victim had "pestered" Liam Allan for "casual sex" (BBC, 2018). The messages were never passed to Liam Allan's defence because the officer in the case proposed that there was "nothing relevant" in their content.
A similar problem transpired in the case of Oliver Mears, a University of Oxford student who had the case against him dropped once a diary from the alleged victim was reviewed by a new prosecution lawyer (Dodd, 2018)

The investigation can only be repeated if the evidence source is available and fully disclosed. Consequently, the original or an exact copy must be made available to relevant parties.

As a result of Liam Allan and other similar cases, thousands of rape and serious sexual assault cases in England and Wales were reviewed in 2018 to ensure that evidence had been properly disclosed (Attorney General's Office, 2018). The review resulted in 47 cases being dropped. As a consequence, the attorney general called for zero tolerance on failures to disclose relevant evidence. According to Angela Rafferty QC, the chair of the Criminal Bar Association, the failure to make full and relevant disclosures came about in these cases as a result of "unconscious bias" (Blindel, 2017).

Examples of the failure to disclose digital evidence in a criminal case include:

- A prosecutor fails to disclose a video that shows the defendant being attacked by the victim, even though the video contradicts the prosecution's

theory of the case.
- A police officer fails to disclose a message that was sent from the victim's phone to the defendant's phone, which suggests that the victim was planning to harm the defendant.
- A forensic analyst fails to disclose analysis results which show that the defendant was not using the computer at the time of the incident.

In each of these examples, the failure to disclose the digital evidence could have a significant impact on the outcome of the case and could lead to an unfair trial.

2.2.4 Investigator Competency and Reliability

The investigator has to be **competent**. There is no charter, or standard against which such competency can be determined, and it is left largely to the court to determine de facto the competency of an investigator. Investigators declare their competency within a report by outlining their qualifications and experience.

Concerns about the competency of experts led to the formation of the Daubert tracker (Daubert Tracker, 2023). Primarily used in the US, the tracker is used to keep a record of experts that have a 'gatekeeping history'. The tracker maintains a database of experts who have, for instance: been found to be unqualified, applied questionable or invalid methods, were not credible or believable, were unreliable, were incompetent, and/or presented conclusory evidence.

In the UK, the Criminal Practice Direction (CPD) 19A.5 (Courts and Tribunals Judiciary, 2015) outlines the factors that a court can take into account when determining the reliability of an expert's opinion. These include:

- The validity of methods used to process data
- The extent and quality of the data on which the expert's opinion is based
- The reliability of inferences is fully contextualised and considered
- Where the expert's opinion relies on the results of methods the opinion considers the degree of precision and margin of uncertainty
- Whether the expert's opinion has been reviewed by other experts
- Experts giving opinion outside their area of expertise
- The completeness of information presented
- A full contextualisation of the expert's opinion where that opinion lies in a range of expert opinion
- Whether the expert's opinion complies with established practice and if not why not.

In the same direction, clause 19A.6 relates to the reliability of expert scientific opinion and outlines that the court should identify potential weaknesses and flaws related to hypotheses that have: not been subjected to sufficient scrutiny, been based on an unjustifiable assumption, been based on flawed data, relied on techniques/processes which were either improperly conducted or were not appropriate for use, and relied on improperly reached inferences and/or conclusions.

2.2.5 Standards

At the time of writing, there are no agreed standards, rules or protocols relating to the handling of digital evidence. However, a digital investigator adheres to a set of basic principles - which in the UK, are enshrined in the ACPO (the Association of Chief Police Officers, now The National Police Chiefs' Council) 'Good Practice Guide for Computer-Based Electronic Evidence'. The 'ACPO guidelines' have become the de-facto standard as far as evidence management and investigation is concerned and have been modified to suit other jurisdictions. The four principles outlined therein are:

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.
2. In 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.
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.
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.

The ACPO principles are intended for criminal investigations conducted by police forces in the United Kingdom. Adherence to the principles help to remove doubts in the investigative process and reduce the opportunity for challenge in court. The guidelines are not directly applicable to corporate or civil investigations.

TASK

More than a decade ago, (Lallie, 2012) argued that there were no ACPO accepted equivalent guidelines for digital investigation in India. Are there any accepted guidelines in your home country? If so, how do they compare and diverge from ACPO? If not, what are the closest set of local guidelines applicable in your country? If you are from the UK or USA, select another country for this exercise.

The digital forensics industry is beset with a problem of lack of standardisation. Where standards have been introduced, there have been challenges in companies and individuals being able to comply with the standards.

Although there is now a standard for labs, there is no 'governing body' to whom investigators are answerable and there is no standard test of 'expertise'. Quite often, proficiency in the use of a tool such as Encase - backed up by experience in the field, is deemed adequate. This means that if an investigator makes a mistake in an investigation, at worst, it will result in embarrassment for his/her company and possibly internal disciplinary action, however, the investigator can continue operating in the industry.

2.2.6 Laboratory standards and competency

Competency has been enforced from a laboratory perspective with the introduction of *ISO/IEC 17025 - Testing and calibration laboratories* (CYFOR, 2023). ISO17025 sets the standard that all laboratories handling, preparing, and presenting digital evidence must comply with. Although an international standard, ISO/IEC 17025 has not yet gained universal acceptance, for example in the UK, the standard only applies to criminal investigations and not all countries enforce it. Another important standard is ISO17020 which guides the handling of evidence at a crime scene (Forensic Computing Ltd, 2012).

Part II

Investigations

Chapter 3

The Investigation Process

Extensive guidance has been published about the process of investigation, for example by ENFSI (ENFSI Working Group , 2016). This guidance has been synthesised and condensed into Figure 3.1.

A *case* typically involves multiple entities including forensic toxicologists, crime scene experts, and fingerprint specialists. Your involvement is one element of the case, and the case manager is probably managing multiple personnel and specialists.

A case normally begins with the receipt of *intelligence*. For example, in the case of drug dealing, law enforcement authorities might receive complaints/reports of *'someone dealing drugs'*. The police have the option of turning up and interviewing suspects, or to gather intelligence as this may be part of a larger crime ring. The decision on what to do as a first step is risk managed. If there is a risk the suspects might abscond or that there is an immediate threat to safety, they might attempt to make immediate arrests, otherwise they will continue gathering intelligence.

They will gather intelligence about people meeting at certain places, leaving their homes at certain times, appearing to distribute drugs, driving certain cars, their address etc. Law enforcement authorities then evaluate the value of this intelligence. When they believe they have enough intelligence they want to be able to make arrests, enter property and seize artefacts which may include computer systems.

They need authority to be able to do this. In the UK, this authority comes from a magistrate who grants a search warrant and an arrest warrant. However, before going to a magistrate, a case manager, the officer in charge of the case, must be sure that there is enough intelligence to convince the magistrate to grant

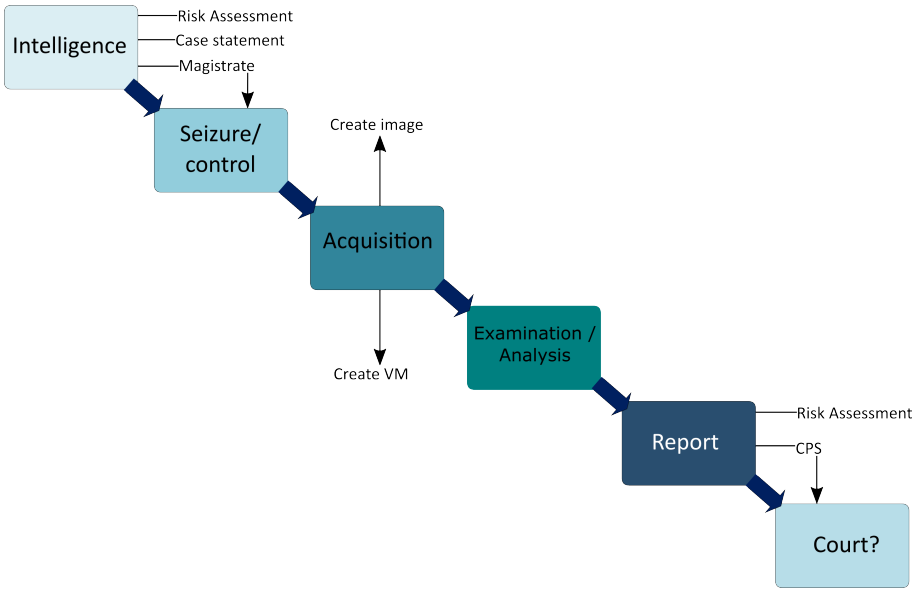

Figure 3.1: The Investigative Process

the two warrants. The College of Policing (2023) provides plenty of guidance on search warrants.

When and if warrants are granted, the law enforcement authority needs to plan the raid. They need to mobilise numerous entities which could involve firearms officers, fingerprint specialists, dogs, and crime scene investigators. The law enforcement authority plans the date/time and has to manage the operation very carefully.

Eventually, the law enforcement authority raids a property and makes arrests. Digital investigators rarely attend the raid. They rely on trained crime scene investigators seizing equipment and bringing it into the laboratory, and the case technician making forensic images of each artefact.

This section deals with the process of investigation, largely from a procedural viewpoint, occasionally from a technical viewpoint.

Chapter 4

Seizure

A crime scene seizure is a process in which law enforcement or other authorities take control of a crime scene and take possession of artefacts that may be relevant to the digital investigation. Relevant artefacts include laptops, PCs, iPads, and mobile phones. These can include a range of other items too such as SD cards, USB sticks, external hard disks, and now even IoT devices and dashcams. These items are referred to as *artefacts*.

ACPO principle 1 states that *"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."*. The implication of this is that care must be taken from the crime scene through to the end of the investigation to ensure that items seized are not modified or tampered in any way. Modification could happen at a crime scene through negligence. For example, a crime scene investigator discovers a laptop hard disk plugged into a laptop and accidentally moves it whilst still operational, thereby causing damage to it.

To abide with ACPO principle 1, the crime scene must be carefully controlled and managed to avoid accidental or even deliberate tampering. If despite this, data is deliberately or inadvertently altered, a satisfactory explanation must be provided outlining what happened.

To prevent problems at the crime scene, several steps can be taken, for example, there must be an officer in charge of the crime scene, and the crime scene must be preserved.

The officer in charge is responsible for the management of the crime scene. This officer is responsible for securing the crime scene and preventing unauthorised personnel from entering the area. They must ensure that the crime scene is carefully managed, that the seizure of items is carefully and professionally

handled, and that the crime scene is not tainted in any way.

Once the crime scene is secured, a thorough search of the area is performed to identify and collect artefacts that may be relevant to the investigation. Crime scene investigators (CSI) will note of any clues or evidence that they find. This can include things like fingerprints, DNA samples, weapons, or other physical evidence. The investigators will also take photos, videos, and/or sketches of the scene to document its condition and any evidence that is present. This could include a record of how devices were connected and running programs/processes

CSIs specialising in IT equipment must turn off all equipment, remove their batteries – if possible – and then bag and tag them. This process involves identifying the item, recording its serial number, recording the date, recording the name of the crime scene investigator, and placing the item into a bag. This is also referred to as chain of custody. A sample chain of custody form has been published by NIST (2023).

IT equipment must be handled carefully to ensure evidence preservation. Power in a computer system should be removed by pulling the power cord from the back, not by entering shutdown mode, or using the on/off button. This protects against PC systems that are connected to UPS (uninterruptible power supply) systems. Screenshots should not be taken of processes on a computer system, instead the investigator should take a photograph. Screenshots overwrite the RAM and save a temporary file to the hard disk, this contravenes ACPO principle 1. CSIs should keep a log of activity at a crime scene, this not only supports ACPO principle 4, but also enables the CSI to retrace steps in the investigation. If the contents of RAM are that important, the CSI should perform a forensic acquisition of the memory.

The principle of integrity comes under strain when investigations involve networks, the cloud or live forensics. In such a case, it is inevitable that evidence will change whilst 'in the control' of the investigator. The investigator must be able to explain the process of evidence acquisition. In such cases it isn't easily possible to maintain full control.

TASK

ISO17020 guides the handling of evidence at a crime scene (Forensic Computing Ltd, 2012). Study this standard to understand the implications on a crime scene seizure

4.1 Chain of custody

Items seized at a crime scene must be logged and their movement, i.e. between people, laboratories, and other entities must be carefully recorded. This process involves invoking a *chain of custody* procedure.

Chain of custody enables investigators to demonstrate continuity of evidence. The first recipient of an artefact is recorded on the form. When possession is handed to another entity, the holder and the recipient cross-complete the form. The form should enable observers to understand the precise movements and possession of the artefact from the moment it was seized to the moment it appears in a trial.

As far as a forensic analyst/examiner are concerned, he/she may not need to complete a chain of custody form because the investigation is always conducted on a digital forensic image of the original artefact and never on the original. There is rarely a need to handle the original artefact.

NOTE

You will rarely need to be involved with Chain of Custody in a piece of coursework as you are likely to be dealing with a forensic copy of the original.

4.2 Triage

Occasionally, there are too many artefacts involved in an investigation and an investigator needs to prioritise the investigation of artefacts that are more likely to render sufficient evidence to secure a conviction. Consider the following scenario: an LEA enter a suspect's home and discover more than 40 laptop devices. The full investigation of all devices is likely to take up to 9 months. In this case, artefacts can be triaged to determine which artefacts are more important as far as an investigation is concerned.

There are multiple ways of performing the triage process. Tools such as *Triage Investigator* (ADF, 2023) can be used to help prioritise artefacts. This tool operates as a boot device and pre-processes artefacts. Pre-configured searches and hash checks are run on the device and the results are analysed to determine whether devices should be investigated.

This process is performed before the device is even imaged. An alternative,

more time consuming method, is to image all devices and then perform a brief analysis of each artefact carefully investigating the thumbnails and especially the data sources summary to determine whether the artefact is likely to generate results.

TASK

(1) Investigate a publicly available chain of custody form and familiarise yourself with the information required on the form and how the chain of custody works.
(2) ACPO proposes that a level of 'proportionality' be applied so that CSIs don't seize items simply because *'they are there'* and *'the person in charge of the search must have reasonable grounds to remove property and there must be justifiable reasons for doing so.'*. There were several issues relating to the raid at the home of Lord Bramhall. Investigate these and categorise and explain these issues.
(3) Read: Hitchcock et al. (2014); Jusas et al. (2017); Cichonski et al. (2012)

Chapter 5

Acquisition

Before a digital investigation can begin, the case technician creates a digital forensic image (DFI) of each artefact. A DFI is a bit for bit copy of every binary bit of data on the original artefact copied to create a compact image file.

The DFI is created using specialist software such as FTK Imager and can be processed by digital forensics software such as Autopsy and Encase

5.1 Write blockers

ACPO principle 1 requires that no data is changed on the original artefact. If the original artefact was plugged directly into the forensic workstation for the purpose of copying, there is a risk the artefact could inadvertently be written to. A write blocker is used to prevent this.

The write blocker intercepts all commands between the computer and the artefact. It returns a successful write response when the computer tries to write to the artefact, without actually writing to it, thereby fooling it into believing the write has been successful and in turn protecting the hard disk from a read/write operation.

5.2 Virtual Machines

It is common for a case technician, where possible, to also create a virtual machine (VM) of each computer system. VMs help the jury understand the functions of the desktop/laptop by enabling the prosecution team to demonstrate the functions and configuration of the artefact in question. This is especially

helpful when uncommon software, which members of the jury are unlikely to have seen before, was used. For example, a suspected fraud case involves the use of specialist accounting software which the Court is likely not to have seen before. The demonstration of how invoices were recorded within this accounting software can be very helpful.

Virtual machines enable investigators to access social media accounts, assuming that the cookie settings in a browser enable them to go straight in without a password. Virtual machines might also trigger automated cloud storage synchronisation. This might contravene ACPO principle 1, so explicit permission is required before converting the original artefact, or the DFI, to a VM.

NOTE

It is possible to convert a DFI to a VM. If you are involved in a forensic examination in your course, it is unlikely you will need to convert the DFI. If you feel you do need to you must seek written permission from the module tutor before converting the DFI to a VM. Failure to do so could be seen as a contravention of ACPO 1 and result in reduced marks in the assessment.

5.2.1 Virtual Machines and Social Media Accounts

A case investigator needs to attend to social media accounts with caution. The guidance provided by the CPS (Crown Prosecution Service, 2020) is conclusive on the steps that must be followed by an investigator. Investigators can browse user accounts from third party machines. However, the information available therein will be limited to that which the suspect has chosen to share. The investigator will not see messages.

Should an investigator choose to engage with the social media account using the suspect's machine (through a virtual machine of course), the investigator is advised to use a body cam or take screenshots of every page. When reading unread messages, the status of those messages will change to 'read' and this will need to be explained to the courts.

5.3 Case Preparation

Next, the case technician prepares the case file, carefully selecting appropriate ingest modules. At this stage, a number of ingest modules, also referred ro as

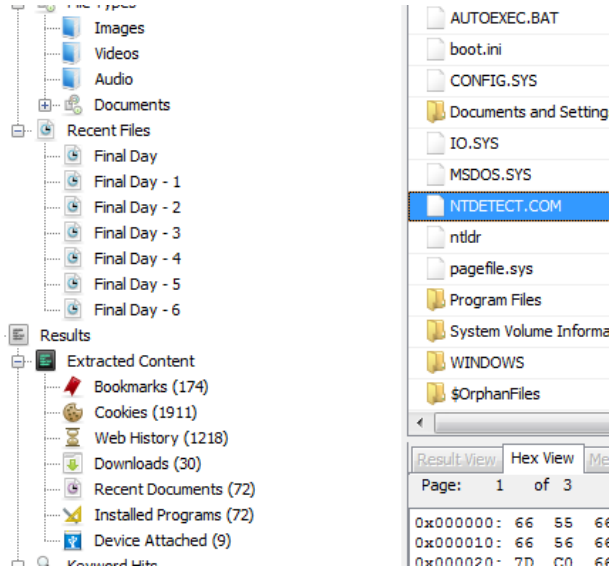

Figure 5.1: The results of an Ingest

pre-processing modules, may need to be activated.

These modules process the data within each storage system to make it more easily accessible. They front load a lot of the investigative work by pre-processing a case and auto-categorising evidence.

Ingest modules can reveal file/data patterns, highlight hash matches, reveal mismatched extensions, URLs, email addresses, web bookmarks, and USBs attached to a computer etc. The results of an ingest are displayed for an examiner to see. For example, the ingest in Figure 5.1 has pre-processed the DFI and highlighted all the web cookies, the web history, and the browser bookmarks. These are visible in the left window.

Although Ingest modules are very useful to an examiner, more work needs to be done in developing more ingest modules. This is ripe territory for further research.

5.4 Forensic Hygiene

There are several tasks that must be performed and reported within the report to indicate basic investigative facts.

The investigator should report the software used for the investigation, with version numbers, and explain the machine used to do the investigation. The

workstation should be disconnected from the network and confirmation given to this effect in the report.

One of the most common defences is the malware defence wherein a suspect claims that a malware must be responsible for the alleged misdemeanour. The malware defence could be presented in the first or subsequent interviews, or even at a subsequent interview, maybe even in the courtroom. To protect against this, the investigator must malware check all artefacts and the forensic workstation.

If malware is found on the artefact, the investigator not only needs to declare this, but also needs to gather further information which includes: when it was installed, what its functions are, and whether the malware could have contributed to the issues under investigation.

5.5 Hashes

An investigator must work on a forensic copy(DFI) of the original artefact. The DFI must be unaltered and be an exact provable copy of the original. To achieve this, a hash is made of the original DFI. The hash is stored in the container (for instance in the .E01 or .DD file). The hash is also supplied separately to the investigator. The investigator (or rather the tools) calculate a hash of the DFI provided, the two hashes are compared. If the hashes are identical, then the investigation proceeds as normal (and an explicit statement made in the case report to confirm this). If the hashes are not identical, the DFI is referred back to the case manager for further advice.

To better understand this, look at the two hashes reported by the tool FTK in Figure 5.2 for two DFIs: 'Animal' on the left and 'Trashed Disk' on the right. The two hashes being reported are:

`animal.E01` MD5 Hash: `c00fd4ce8d3b7145243fab14fe608ef1`,
SHA1: `1205eb6f1ca7db056e9b2456d6e50241b31b4ed8`
`TrashedDisk.E01` MD5 Hash: `5fac16f52ca3ccac4cfdb512aeac2b3c`
SHA1: `92906d4f34fdd27a584903d3b4c5c3314f21706e`.
Let's try to understand what these hashes are.

When a DFI is created, the tool that creates the DFI calculates a CRC (cyclic redundancy check) of each block of data, and an MD5 and/or SHA1 hash of the entire storage space of the source from byte 0 to the last byte as shown in Figure 5.3 top. The CRC is stored at the end of each block in the resulting DFI, and the hash is stored in the footer. The hash is referred to as a *Stored verification hash.*

Some of the earlier tools did not have the facility to calculate SHA1 hashes, hence they stored the MD5, but did not store a SHA1. This is probably what has happened in Figure 5.2 right.

Note also, that although some tools had the provision to calculate both MD5 and SHA1, they provided a user with the option as to which hash they whether wanted to store. If a user opted not to store a SHA1, the tool stored zeroes in the DFI where the SHA1 hash should have been. This is what has happened in Figure 5.2 left.

When *FTK Imager* verifies the hash in the last few steps outlined above, FTK take the data blocks from the DFI and recalculates the hash, this is referred to as a *Computed hash*. The *Computed Hash* is compared with the *Stored Verification Hash* and returns a *match* or *mismatch*.

Some DFI creation tools, FTK Imager being an example, also create a text report of the DFI creation process. An example of what this looks like follows:

```
Status:  Completed
Start:  10/30/12 10:46:43AM
Stop:  10/30/12 10:48:03AM
Time:  0:01:20
Name:  animal
Path:  J:\Forensic cases\Animal\animal.E01
GUID: 3EF87E38CF45F049B33E2DCD7819AF49
Acquisition MD5:  C00FD4CE8D3B7145243FAB14FE608EF1
```

We can see from the contents of this file that the MD5 hash is given in upper case and matches the hash in the verification dialogue box presented by FTK (Figure 5.3 left). This is referred to as a *Report Hash*.

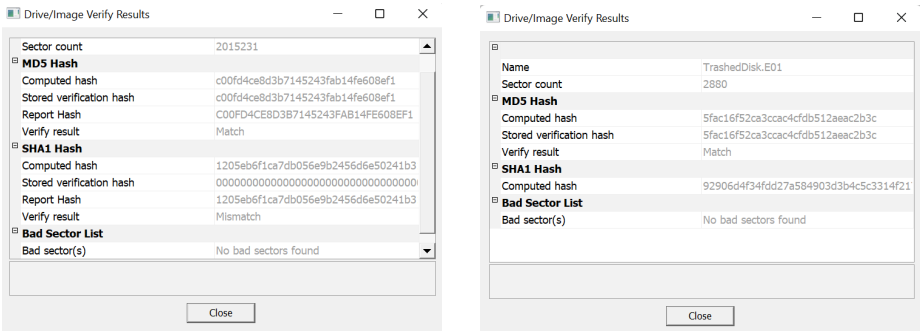

Figure 5.2: Case details

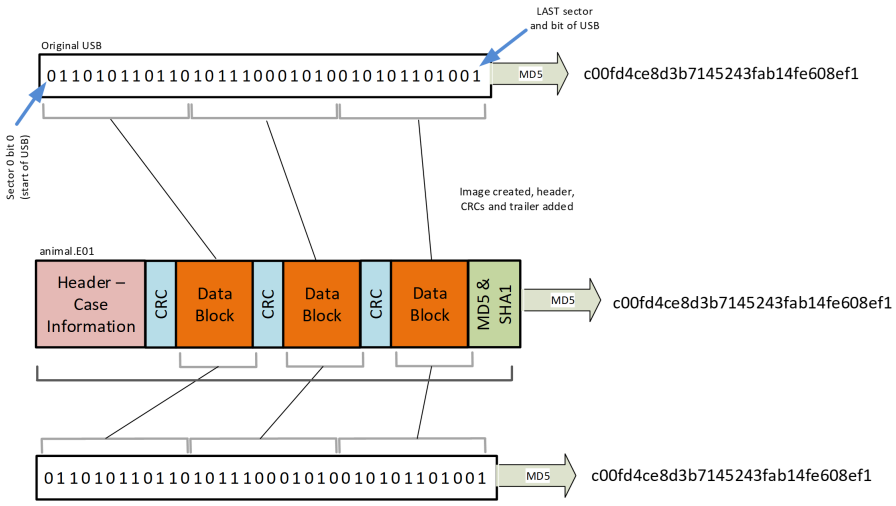

Figure 5.3: Understanding DFI hashes

In both cases, The MD5 hashes match. However, the `TrashedDisk.E01` returns a SHA1 hash, but does not confirm whether it is a match or mismatch. Let's try to understand what has happened here.

Not all DFI creation tools create both the MD5 and the SHA1 hash. Figure 5.2 returns a SHA1 hash for both DFIs, reports a *mismatch* for `Animal.E01` and neither a *match* or *mismatch* for `TrashedDisk.E01`. When the `Animal.E01` was

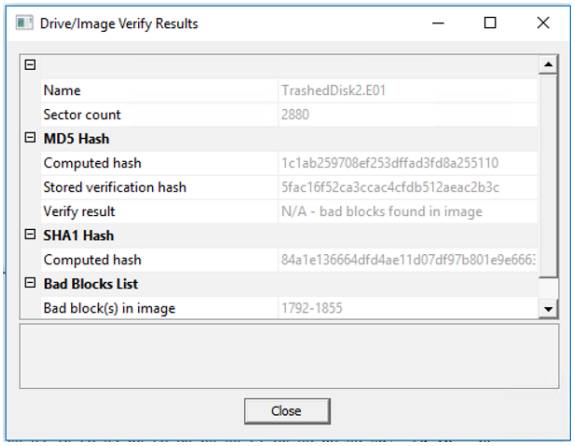

Figure 5.4: Bad Blocks

created, DFI creation tool did not create or insert a SHA1 hash. There is no SHA1 hash to compare with, hence Autopsy cannot confirm whether it is a match or mismatch.

5.5.1 Bad blocks

Occasionally, hashes do not match because of bad blocks on the original medium. Bad blocks are areas of the storage system which have deteriorated and which now render unreliable data. Figure 5.4 illustrates a DFI taken from an artefact which contained bad blocks. 63 of the 2880 sectors are marked as bad blocks and verification has failed. However, this does not mean that the investigation cannot proceed. The remaining functional 2817 sectors might render useful evidence. The investigator proceeds with examining the DFI and if any evidence is found, it is reported along with an overview of the problems with the original artefact.

Chapter 6

Examination and Analysis

The examination process aims to reveal, explain the provenance of, and categorise evidence. The examiner performs varying levels of examination, revealing potentially useful evidence and bookmarking it. Later an analyst will determine the probative value of each bookmark and decide whether to include it within the report. Some forensic labs merge the two roles into one, whilst others keep these separated.

The examiner must attempt to explain the provenance of evidence, i.e., how it got there. This includes analysing the timestamps, searching through browser search histories and cookies, examining emails, analysing zone identifiers to determine whether for instance cloud storage was involved, and analysing metadata to see if other third parties are involved and whether the source camera and potential photograph locations can be identified.

The examiner is also looking for potential third parties not already identified in the case statement. These could be identified through emails, contact lists, and photos - both as a presence in the photo but also in the metadata. These must be third parties of interest, not everyone and anyone that is found within the DFI.

At this stage, amongst the objectives provided by the case manager, the examiner must respond to some of the responses and claims made in interview. These included the 'malware defence' wherein a suspect proposes that malware and/or hacking activity must be responsible for activity on the artefact, and the 'ownership defence' wherein the suspect proposes that he/she is not the owner, or that there is shared ownership and that somebody else must have perpetrated the offence.

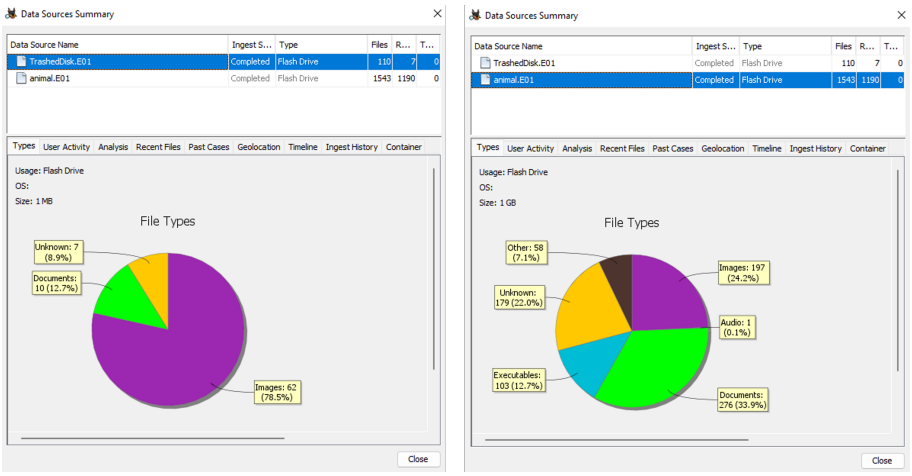

Figure 6.1: The Data Source Summary

6.1 Modus Operandi

What might a typical examination modus operandi look like? There is not a standard workflow in terms of how a DFI should be investigated. However, there are some straightforward steps that could make the process easier.

6.1.1 Technical Inspection

The first step, normally conducted as standard forensic hygiene, should be to inspect the DFI to understand its configuration. The examiner may want to know: what type of device did it come from, e.g. a laptop running Windows, an SD card, a drone? how many partitions are there? How are the partitions formatted? Are there any unformatted partitions? Do these contain any data?

A summary of the DFI, such as that offered in Autopsy (Figure 6.1) is useful in providing an overview of what to expect to see. This may help to triage a case. For instance, consider an illegal images case involving 20 DFIs, where 10 return a very high image count, and the other 10 return a 'normal' level of images. In this case, the examiner might want to prioritise the examination of the DFIs that contain a high image count.

Similarly, fraud, drugs, and IP theft cases may comprise a different profile of documents. Fraud might rely largely on emails, PDFs and other forms of documents. Drugs cases may involve a lot of emails, some photos and social media activity. IP exfiltration may involve emails, photos (possibly on phones) PDFs, USB activity, cloud storage.

Ten Asians named in 21-strong tax crime gang jailed

The final defendant of a twenty-one strong crime gang was sentenced this week for his part in a £37.5 million tax fraud. In total all twenty-one were jailed for a total of seventy-four years.

Harbans Singh Kohli, 47, from Ealing, London, was sentenced to two years and six months, following two re-trials, for laundering just over £1 million in associated 'missing trader' fraud. He was disqualified from being a company director for 10 years. He was originally sentenced in 2007 but released by the Court of Appeal.

The sentencing which ended one of the most complex investigations undertaken by HM Revenue & Customs (HMRC) came at the end of seven trials and retrails. Investigations began in April 2002 into the 'missing trader' fraud, involving the dishonest manipulation of the VAT system through the import and export of computer processing units (CPUs). The gang used highly complex chains of VAT registered companies both here and abroad. One of the 'missing traders' used was Shivani (Limited) - an anagram of 'I Vanish'

Criminal investigators from HMRC exposed the fraud which has resulted in seven interlinked trials and retrials, codenamed Operation Devout. Reporting restrictions have now been lifted following the conclusion Monday of the seventh and final trial.

Adrian Farley, Assistant Director of Criminal Investigation for HMRC, said: "This was not some kind of victimless crime, but organised fraud on a massive scale by criminals masquerading as legitimate businesses all bent on making fast and easy profits at the expense of the British taxpayer. Multiple businesses and bank accounts were deliberately set up to carry out the fraud and hide the proceeds of these crimes. However, each defendant knew the purpose of the payments they received were for money laundering and not legitimate trade."

The conspiracy involved the import of CPUs mainly from Ireland, VAT free. The goods would then be sold more cheaply, but with VAT added, through a chain of companies each involved in the plot and sham invoices would be issued. Once the goods had been sold on a number of times they would be exported back to the EU. The exporter would then claim a VAT credit from HMRC for the VAT paid on the purchase of the goods. The gang would then divide the profits of the fraud and launder them through various bank accounts both in the UK and abroad before withdrawing the bulk of the cash. They were paid a commission for their dishonest service. Some of the money is believed to have been invested in a third a tonne of gold bullion, substantial property in Dubai and a luxury flat near Harrods.

Confiscation proceedings to reclaim the proceeds of the crime are now being pursued.

The twenty-one defendants included: - nine from the West Midlands, one defendant from Buckinghamshire, two defendants from Middlesex, six defendants from London and three defendants from Essex.

Kohli was one of ten Asians arrested. Others included: Somasuntharam Jeyakumar (49), Syed Mubarak Ahmed (58), Shakeel Ahmed (38), Jaswender Singh Chahal (51), Sukhdave Singh More (45), Tariq Kamal (45), Pravin Jogia (63), Babak Cherazi (38), Khaled Hamidi (34), Mustapha Mehmet (54) and Timur Mehmet (57).

Harbans Singh Kohli | Somasuntharam Jeyakumar | Syed Mubarak Ahmed | Shakeel Ahmed | Mustapha Mehmet

Sukhdave Singh More | Tariq Kamal | Pravin Kumar Jogia | Babak Cherazi | Khaled Hamidi

Figure 6.2: £37.5m VAT Fraud

Case Study

As an example of the importance of understanding the type of evidence an investigator should be prepared for, consider the case of Kohli et al, a £37.5m fraud case which is still the largest HMRC VAT fraud case in the UK (Figure 6.2). In such a fraud case, the perpetrator establishes companies in three countries, let's say Ireland, England, and France. The perpetrator imports CPUs from Ireland. Prior to Brexit, VAT was not payable on these imports. The CPUs are sold to a company in France, but later purchased again with VAT added. All the while, invoices have been exchanging hands as has actual money. The perpetrators then file a VAT refund claim, resulting in VAT being reimbursed by HMRC. For a case such as Kohli et al, the original invoice amounts may have been in the region of £187.5M (to render VAT invoices to the value £37.5M).

In this case, the bulk of evidence would have been PDFs and emails. There may have been photos of cartons. Some of the PDFs may have been readable by tools such as Autopsy, others will not have as they were scanned in and may have been of poor quality.

TASK

Famous cases of fraud include Enron (Thomas, 2002), Serenity Travel and Serenity Community Transport Ltd (Crown Prosecution Service, (CPS), 2022), and the £35m VAT fraud (Express and Star, 2010).
Explore some of the case studies identified above. Also consider exploring the Coca Cola IP case and the Motorola IP case

6.1.2 Low Hanging Fruits

There is often a lot to examine and the process can take a long time. The examiner must have a system in place to help get through the multiple DFIs involved in a case.

At this point, the examiner strategises the work depending on the type of case. For a case involving the exfiltration of IP which exists say as PNGs, or a case involving illegal images, the examiner might begin with examining the thumbnail view (Figure 6.3) to see immediate results and obvious evidence.

The ingest results will vary depending on the ingest options selected. The ingest results presented in Figure 5.1 (p 28) show bookmarks, cookies, and web history. This data has been gathered by the ingest module to avoid the examiner

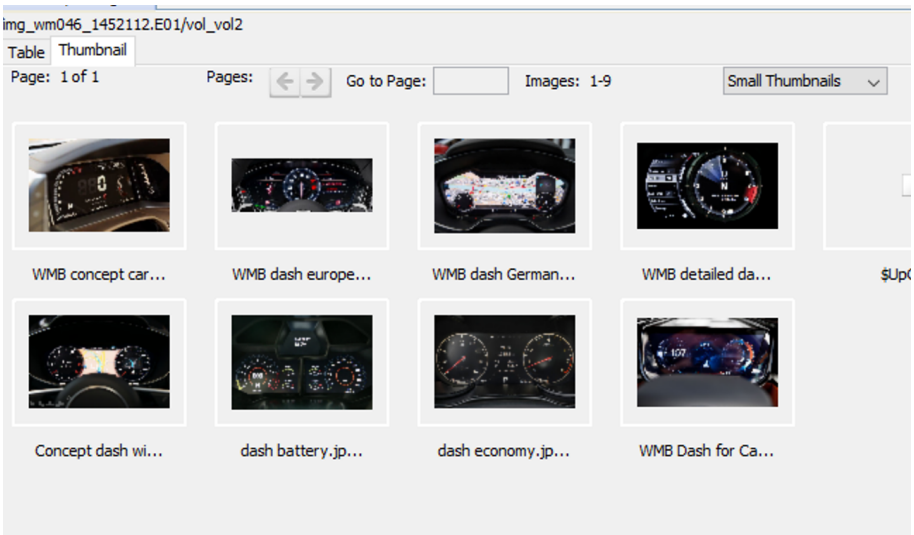

Figure 6.3: Thumbnail views

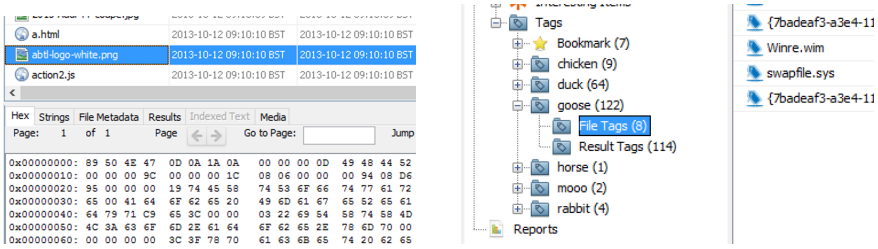

Figure 6.4: File signatures (left) and bookmarks in Autopsy (right)

having to manually find the data within the DFI.

The typical sources of evidence in a DFI include the file system - including volumes, partitions, and folders; the metadata contained within files - both system and application; and the registry.

Whilst most of the evidence can be revealed through browsing through the forensic tool interface, often the examiner needs to do more intrusive analysis. For example, this could involve developing searches, and analysing file signatures (Figure 6.4).

NOTE

I have deliberately avoided detailing all the steps of an investigation here. That information is found in the accompanying handbook which takes you through a series of practical exercises.

6.2 Bookmarking

As the examiner proceeds through the investigation, important evidence is bookmarked (Figure 6.4) for consideration later. Bookmarks enable the examiner and/or analyst to return to the evidence and consider its probative value. If, on reflection, the bookmark does not reveal anything useful, it can be deleted.

Files, directory structures, photos, deleted documents/text etc can be bookmarked. Bookmarks are important as they contain the bulk of the information required in the report.

One of the differences between the work of an examiner and an analyst is that the examiner creates bookmarks of evidence they consider to have probative value. The analyst scrutinises these bookmarks and determines which to include in the report, i.e. which items of evidence should be included in the final report.

The analyst is likely to delete bookmarks at this point.

Examiners should avoid 'over-bookmarking'. It can be tempting to bookmark anything that might remotely be useful. This can result in too many bookmarks for the analyst to consider and the examiner should therefore avoid 'overbookmarking'.

Chapter 7

Reporting

Digital evidence has a reputation for being complex, overwhelming and hard to understand (Sammons, 2012) Added to this is the problem of the *CSI effect* wherein courts could inadvertently be influenced bin their understanding of scientific reality by TV shows (Shelton et al., 2006). Although the *CSI effect* has been commented on largely in the mid-late 2000s, the problem still exists today.

The failure to interpret the findings in an unbiased manner, can render the evidence inadmissible. Table 7.1 provides examples of cases which resulted in case dismissal or a miscarriage due to problems in reporting. This has an implication on the report. The report must be constructed carefully and diligently, always mindful of the audience it is intended for. The rest of this section outlines the key attributes of a report.

Section **??** details the report format that you must use to complete your coursework.

7.1 Uncertainty, and Limitations

Potential uncertainties and limitations of the findings should be disclosed. To cater for this, it is common at this point for an investigator to outline that *"if ... then this would change my opinion"*. For example: *'if the suspect is not in a relationship with xxx, this would change my opinion in respect of Section 2.1 in that...'*

Phrases such as 'it is likely' are commonly used to express a conclusion, but only in genuine cases of likelihood which does not lead to firm opinion. In other words, *'it is likely'* should not be used to back out of giving firm opinion. As

Table 7.1: Sample cases demonstrating problems in understanding digital evidence

Case	Detail
Harrowell, McEwan and Edmond	Case dismissed as the prosecutor was not able to clearly present the digital evidence against the defendants (Fort, 2015)
Regina v Caffrey	Caffrey acquitted of all charges related to the Computer Misuse Act despite overwhelming inculpatory evidence due to the prosecution failing to adequately present the digital evidence to the members of the jury (Boddington, 2012).
State of Western Australia v Buchanan	a charge relating to the protection of children went to an appeal because 'the report and presentation lacked complete contextualisation to help the legal teams and defendant understand the significance of the evidence... no timeline, no storyboard and confusing analysis presentation [which were] problematic for the defence lawyers.' (Boddington, 2012)
Conneticut v Amero	A teacher was charged with offences relating to the protection of children because of what appeared to be concrete digital evidence brought against her. This case went through an appeals process because of questions regarding how the evidence was attained and later presented, where the charges were then reversed. Following this case, Judge Paul W. Grimm gave his opinion on the issues that arose from the trial, stating that 'basic computer literacy and understanding of the digital forensics process [should be] made requirements in schools of law' (Alva & Endicott-Popovsky, 2012)
	A second district court judge from Massachusetts, USA also expressed concerns stating 'computer forensics, it's extremely highly technical. I find in a lot of cases, that much of it [goes] over the jurors' heads even with an expert trying to explain it. A lot of experts have a hard time bringing it down to a layperson's level'. (Kessler, 2010)

practitioners, if we express that something is 'likely' then we are indicating our conclusion is based on a likelihood. This is calculated using something called a 'posterior probability'.

For example, the following: *'it is likely that the files were downloaded from the internet or were emailed to the Suspect'* must only be used if the investigator is not absolutely able to assert that the files came from the internet, and their research has revealed the presence of the files on given websites, there is no history of access to those websites, and there are no emails or other explanations. In this case 'it is likely' that the files were downloaded, it is possible the browser history has been deleted (maybe quite naturally over time).

Another common phrase you can expect to encounter in expert testimony is the ambiguous expression 'is consistent with', which states some (unknown) degree of similarity between two things. An example of this might be: *'The keywords used are consistent with an individual searching for hacking tools.'*

When these types of expressions are used, typically there is no indication how common the 'consistent' features are in the wider population.

Coming from the lips of a practitioner with expertise in the subject, such words can be compelling to the court. The expertise of the practitioner is thus another potential risk to the reliability of evidence.

7.2 Exceeding Expertise

Practitioners typically specialise in relatively narrow areas of expertise, such as DNA profiling, ballistics, computer forensics or mobile phones. Whatever their field, each must steer a very narrow course to stay within their field of expertise when presenting their testimony.

7.3 Misuse of scientific language

Because much of the evidence can be complex, it must be expressed in a language that is both comprehensible to a layperson, yet exact enough to avoid any ambiguity or misinterpretation. A study of 500 randomly selected forensic science reports found that 'questionable communication practices' were common and that 'little information' was provided to support their 'absolute conclusions'.

7.4 Bias

7.4.1 Unconscious bias

Like most of us, practitioners can be subject to unconscious bias, impacting on the reliability of any evidence they tender at court.

Unconscious bias is not new as an idea but has been recognised by the Forensic Science Regulator (FSR) who articulate several categories of unconscious bias. These can ultimately impact on the reliability of evidence tendered at court:

- Expectation bias
- Confirmation bias
- Anchoring bias
- Contextual
- Role effects
- Motivational bias
- Reconstructive effects

The impact of bias is also recognised by rule 19.2 of the UK's Criminal Procedure Rules, which covers the use of expert evidence in Court. It states that any opinions a practitioner acting as an expert witness offers must be 'objective and unbiased'. Furthermore, the expert's duty is to assist the court and that this duty 'overrides any obligation to the person from whom the expert receives instructions or by whom the expert is paid'. Thus, despite acting for either the defence or the prosecution, the practitioner is expected to maintain a level of neutrality in their work and testimony.

Regardless of any bias, the conclusions drawn by the practitioner must be communicated to the court. This then presents another challenge: the use of appropriate scientific language.

7.4.2 Confirmation Bias

As a practitioner, you need to be very alert to the risks of exceeding your expertise, as many opportunities exist for stepping outside your area of specialism. For example, confirmation bias can happen when attempting to corroborate your findings from another (related) field. This might be a practitioner trained in mobile forensics attempting to interpret the findings of a cell site analysis survey. Not all mobile forensics experts are also cell site experts, and quite often, they need to draw on specialist cell site support.

Similarly, you may try to quantify the uncertainties in your data with the use of statistics without fully understanding how to do so correctly. This issue led to the flawed evidence tendered by paediatrician Professor Sir Roy Meadow who fell foul of the prosecutor's fallacy in the now infamous trials of R v Clark [2003] EWCA Crim 1020, R v Cannings [2004] EWCA Crim 1 and R v Patel [2003]. This error continued to appear in cases as recently as R v London Borough of Croydon (EWHC 1473).

With or without error, data will often need meaningful inference in the context of the investigation. This is typically provided by the practitioner, whose expertise will interpret meaning from the data. In addition, the practitioner and their methods may come under scrutiny. One example of this is the potential issue of practitioner bias.

Part III

Appendices

Bibliography

ADF. Triage investigator, 2023. URL https://www.adfsolutions.com/triage-investigator.

Attorney General's Office. Review of the efficiency and effectiveness of disclosure in the criminal justice system, 2018. URL https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/756436/Attorney_General_s_Disclosure_Review.pdf.

BBC. Met police apologise for liam allan rape case errors, 2018. URL https://www.bbc.co.uk/news/uk-england-42873618.

J. Blindel. Yes, there's a major problem with rape prosecutions. but it's not that women are lying, 2017. URL https://www.theguardian.com/commentisfree/2017/dec/20/problem-rape-prosecution-women-lying-collapse-liam-allan-victims.

P. Cichonski, T. Millar, T. Grance, K. Scarfone, et al. Computer security incident handling guide. *NIST Special Publication*, 800(61):1–147, 2012.

College of Policing. Search powers, and obtaining and executing search warrants, 2023. URL https://www.college.police.uk/app/investigation/investigative-strategies/search-powers-and-obtaining-and-executing-search-warrants.

Courts and Tribunals Judiciary. Criminal practice directions 2015, 2015. URL https://www.judiciary.uk/wp-content/uploads/2022/03/CrimPD-12-CONSOLIDATED-March-2022.pdf.

CPS. Disclosure, 2012. URL https://www.cps.gov.uk/about-cps/disclosure.

Crown Prosecution Service. Social media: Reasonable lines of enquiry, 2020. URL https://www.cps.gov.uk/legal-guidance/social-media-reasonable-lines-enquiry.

Crown Prosecution Service, (CPS). Three fraudsters convicted for scamming the taxpayer for over £1 million to pay for their lavish lifestyles, 2022. URL https://www.cps.gov.uk/cps/news/three-fraudsters-convicted-scamming-taxpayer-over-ps1-million-pay-their-lavish-lifestyles#:~:text=Serenity%20Community%20Transport%20Ltd%20claimed,the%20hands%20of%20Lee%20Hickinbottom.

CYFOR. Cyfor achieves iso 17025 accreditation, 2023. URL https://cyfor.co.uk/cyfor-achieves-iso-17025-accreditation,urldate={2023-10-14}.

Daubert Tracker. Daubert tracker, 2023. URL https://www.dauberttracker.com/.

V. Dodd. Police accept making errors as oxford student rape case is dropped, 2018. URL https://www.theguardian.com/law/2018/jan/19/oxford-student-case-oliver-mears-dropped-days-before-trial.

ENFSI Working Group . Forensic examination of digital technology, 2016. URL https://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf.

Express and Star. £37.5m vat fraud gang get 74 years, 2010. URL https://www.expressandstar.com/news/2010/05/26/37-5m-vat-fraud-gang-get-74-years/#:~:text=The%20details%20can%20be%20revealed,at%20Birmingham%20Crown%20Court%20yesterday.

FCR. Code of practice, 2023. URL https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1178250/FINAL_2023.1.18_Code_of_Practice.pdf.

Forensic Computing Ltd. Iso 17020 consultancy, 2012. URL http://www.forensic-computing.ltd.uk/iso-17020-consultancy/.

M. Hitchcock, B. Gillespie, J. Crilly, and W. Chaboyer. Triage: an investigation of the process and potential vulnerabilities. *Journal of advanced nursing*, 70 (7):1532–1541, 2014.

V. Jusas, D. Birvinskas, and E. Gahramanov. Methods and tools of digital triage in forensic context: Survey and future directions. *Symmetry*, 9(4):49, 2017.

H. S. Lallie. An overview of the digital forensic investigation infrastructure of india. *Digital Investigation*, 9(1):3–7, 2012.

D. Lawton, R. Stacey, and G. Dodd. ediscovery in digital forensic investigations. *CAST Publication*, (32/14), 2014.

Metropolitan Police Authority. The virdi inquiry report, 2001. URL http://image.guardian.co.uk/sys-files/Guardian/documents/2002/01/09/virdia.pdf.

C. M. Miller. A survey of prosecutors and investigators using digital evidence: A starting point. *Forensic Science International: Synergy*, 6:100296, 2023.

NIST. Nist's sample chain of custody form, 2023. URL https://www.nist.gov/document/sample-chain-custody-formdocx.

J. Sammons. *The basics of digital forensics: the primer for getting started in digital forensics*. Elsevier, 2012.

D. E. Shelton, Y. S. Kim, and G. Barak. A study of juror expectations and demands concerning scientific evidence: Does the csi effect exist. *Vand. J. Ent. & Tech. L.*, 9:331, 2006.

C. W. Thomas. The rise and fall of enron. *JOURNAL OF ACCOUNTANCY-NEW YORK-*, 193(4):41–52, 2002.