IT Forensics – Week 6

Digital Evidence in the Courtroom

Overview

- Hardware and Software Environments
- Filesystems Evidence
- Categories
- Locating Evidence in Filesystems
- Duty of Experts
- Admissibility
- Levels of Certainty in Digital Forensics
- Direct versus Circumstantial Evidence
- Scientific Evidence
- Presenting Digital Evidence

Hardware and Software Environments

- **Magnetic hard drives and tapes**
- **Optical media storage devices**
- **Random Access Memory (RAM)**
  - May be important
  - Details of recent activity (keyboard etc)
  - Can be difficult to capture
  - Powering down machine may be an issue (password / encryption)

Hardware and Software Environments

- **Solid State Drives**
  - This new mode of operation can thwart forensic recovery

- **Network stored data**
  - Data stored on network servers
  - Forensic analyst can be provided with network authentication details
  - External connection to network to access/image datasets. Less frequent, mainly for serious crime.
  - Imaging can be the preferred option for network servers, rather than gathering logical data from OS. Imaging can present challenges.

Hardware and Software Environments

- **Cloud**
  - Acquiring evidence can be challenging
  - Difficult to create a forensics image
  - Logistics / jurisdictions an issue
  - May need help from third party / vendor

Hardware and Software Environments

- **Operating systems**
  - Wide variety of different types (Windows, Mac, Unix, Linux, Andriod, etc…)

- **Software**
  - Program Installed
  - Potentially creating new files (CRUD)
  - Recoverable from machine/OS
  - Files may be shared (upload/cloud/email etc)

Filesystems Evidence

- This will be stored evidence and will be different for each type of Operating System distribution.
- OS can have completely different file systems
  - Windows (NTFS)
  - Linux (Ext4)
  - Mac (APFS)
  - Etc…

Filesystems Evidence

- Commands received from the operating system are used to read and write files and are stored in a directory structure.
- Windows uses a Master File Table (MTF) and stores data/attributes for every file/directory.
- The filesystem is used to store data.

Filesystem Category

- The filesystem category records the general filesystem info.
- It follows a standard pattern but can be unique for each device.
- It offers a map of the filesystem
- It tells us where to find files.

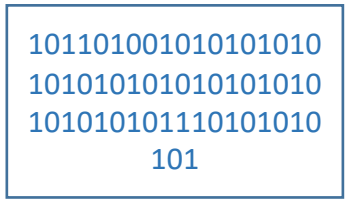
- Benefits of the filesystem for forensic analysis:
  - Lots of metadata

Filename Category

- Assigns a name to each file
- Consists of directories and filenames with the corresponding metadata.
- Deleted filenames and their metadata addresses can be used to recover the file content using metadata based recovery.

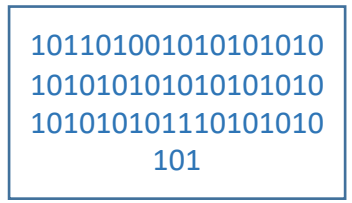
- The listing of filenames is an important part of forensics analysis.
- Can identify files and parent directories.
- Search for evidence (filename, path, file extension)

Filename Category – filename information schema



Process file name data

Del	Name	Metadata
No	Phone.txt	1
Yes	Contacts.docx	3



Process metadata

Del	Type	Size	Last Update	Data Unit	Data Unit
No	File	2008	1/1/2021 01:02:03		

The Metadata Category

- Stores properties and attributes for a file
- Gives the history for a file
- Does not store contents of the file name

- Different file types provide basic metadata and the versions of a file.
- Eg. Windows Properties (screen shot here)

The Metadata Category

- If no forensic protection is offered the act of copying a file to a new location will alter the metadata.
- This is a problem for a forensic investigation
  - Contamination of the evidentiary state of the file

The Content Category

- This is the contents of a file
- A file can be recovered from unallocated space
- May have no linked metadata or filename
- Information can be retrieved from file signature and content

Locating Evidence in Filesystems

- Can be specific to the type of transgression
- Locards Exchange Principle
  - A conflict between two items will result in an exchange
- Looking for the “Smoking Gun”
- Timestamps
  - Are they correct? Format / Time zones?
- Who had access to the laptop? Who had access? Passwords?
- Need to locate info/data relevant to the case.
- Investigation approach will be linked to the transgression.

Locating Evidence in Filesystems

- Need to correlate and corroborate the evidence.
- Approach with a vigilant open mind
- Trying to determine:
  - Means
  - Opportunity
  - Motive

Means – how the transgression occurred

- Means or the process followed
  - What illegal act was undertaken
- How was the transgression carried out?
  - How was this carried out?
  - Can we reconstruct the transgression?
- Trying to source conclusive information that the transgression was performed by a person on this device/account etc.
- Does the person have the skills to perform this?

Opportunity – chance to perform transgression

- It can be easy to prove opportunity.
  - Difficult to link suspect to transgression alone.
- Looking to link person to the computer or network in the absence of any corroboration.
- Examine audit logs / logins etc
  - Has another person used this persons computer?
  - Can CCTV or door access help with this?
- Need to establish who really had access

Motive – why transgression occurred

- Not essential to prove motive
- Can be difficult to confirm without a confession
- Data may exist to offer some insights into this
- Need to be aware that false evidence may be generated/planted to implicate a third(innocent) person.

Where to look for Evidence

- If a transgression has occurred we have:
  - Means
  - Opportunity
  - Motive
- Operating System / Storage / Files / Logs can help provide some insights

- Trying to understand what happened:
  - The who, why, when, where, what and how

Where to look for Evidence

- Using Forensic Toole to explore system.
- Looking for files/data.
- Can be in different file categories:
  - Archives, audio, databases, emails, event logs, Internet browser files, link files, MS Office, recycler, registry files, system files, video.
- Can index and search for files
- Search for specific files
- Can index based on file type and signature:
  - Filename, contents, metadata, time frame, size, etc….

Duty of Experts

- Experts have a duty to present the objective, unbiased truth of the matter before the court.
- It is not their role to advocate for one side; that burden is on the attorneys.
- The UK Criminal Procedure Rules (CPR) specifically address this issue with the following statements:
  - An expert must help the court to achieve the overriding objective by giving objective, unbiased opinion on matters within his expertise.
  - This duty overrides any obligation to the person from whom he receives instructions or by whom he/she is paid.
  - This duty includes an obligation to inform all parties and the court if the expert's opinion changes from that contained in a report served as evidence or given in a statement.

Duty of Experts – Resisting Influence

- Digital investigators are often pressured, both subtly and overtly, to concentrate on specific areas of inquiry and to reach conclusions that are favorable to a particular party.
- Some cases and the nature of the evidence uncovered (digital or otherwise) will take digital investigators to emotional limits, testing their resolve.
- Members of law enforcement who conducted an investigation to apprehend a defendant may be required to present digital evidence objectively in court and may have the duty to identify weaknesses in a prosecution case.
- Computer security professionals in the private sector often have to investigate longtime coworkers and cases in all sectors can involve brutal abuse of innocent victims, inciting distraught individuals and communities to strike out at the first available suspect.
- The effectiveness of the investigative process depends upon high levels of objectivity applied at all stages.
- A good digital investigator must resist such influences and remain objective in the most trying situations.

Duty of Experts – Resisting Influence

- A common error is to use a verification methodology, focusing on a likely suspect and trying to the evidence around that individual.
- When a prime suspect has been identified and a theory of the offense has been formed, experienced investigators will try to prove themselves wrong. Implicating an individual is not the job of investigators—this is for the courts to decide and unlike scientific truth, legal truth is judgment based

Avoiding Preconceived Theories

- Trained, experienced investigators will begin by considering whether a crime or infraction has actually occurred.
- When a large amount of data is missing on a computer and an intruder is suspected, digital investigators should determine if the damage is more consistent with disk corruption than an intrusion.
- When an investigator has ruled out innocent explanation, the focus shifts toward determining what happened, where, when, and how, who was involved, and why.
- The process by which digital evidence is uncovered and applied to these issues involves several steps, each employing strict protocols, proven methods, and, in some cases, trusted tools.
- The success of this process depends heavily on the experience and skill of the digital investigators, forensic analysts, and crime scene technicians who must collaborate to piece the evidence together and develop a convincing account of the offense.

Scientific Truth and Legal Judgement

- in the prosecutorial environment, theories based upon scientific truth are subordinate to legal judgment and digital investigators must accept the ruling of the court.
- For instance, in common law countries, the standard of proof for criminal prosecutions is *beyond a reasonable doubt* and for civil disputes it is the *balance of probabilities.*
- Legal judgment is influenced by ideas like fairness and justice, and the outcome may not conform to the scientific truth.
- In a trial, the object is to assess the case as a whole to determine whether there is sufficient proof of guilt. The decision on the facts is specific to that trial.
- In “science,” we are trying to identify rules that are universally true. In nearly all trials, scientific and technical evidence is only part of the total picture.
- A court may convict an individual even if the case is weak or some evidence suggests innocence.

Admissibility

- The concept of admissibility is a simple one. Courts need to determine whether evidence is “safe” to put before a jury and will help provide a solid foundation for making a decision in the case.
- In practice, admissibility is a set of legal tests carried out by a judge to assess an item of evidence.
- This assessment process can become complicated, particularly when the evidence was not handled properly or has traits that make it less reliable or more prejudicial.
- Some jurisdictions have rules relating to admissibility that are formal and sometimes inflexible, while other jurisdictions give judges more discretion.

Admissibility

- In 2007, a case in Maryland (US) dealt with the admissibility of digital evidence specifically and provided general guidelines for reaching a decision.
- In this case, both parties offered copies of e-mail messages that could not be authenticated properly.
- The magistrate judge would not admit the e-mail messages, noting that unauthenticated e-mails are a form of computer-generated evidence that pose evidential issues.
- The magistrate outlined five issues that must be considered when assessing whether digital evidence will be admitted:
  - Relevance
  - Authenticity
  - Not hearsay or admissible hearsay
  - Best evidence
  - Not unduly prejudicial
- Although some of these issues may not be applicable in certain instances, each must be considered.

Authentication of Digital Evidence

- Courts generally ask if the recovered evidence is the same as the originally seized data when considering whether digital evidence is admissible.
- To demonstrate that digital evidence is authentic, it is generally necessary to satisfy the court that it was acquired from a specific computer and/ or location, that a complete and accurate copy of digital evidence was acquired, and that it has remained unchanged since it was collected.
- In some cases it may also be necessary to demonstrate that specific information is accurate, such as dates associated with a particular le that is important to the case.
- The reliability of digital evidence clearly plays a critical role in the authentication process

Authentication of Digital Evidence

- Chain of custody and integrity documentation are important for demonstrating the authenticity of digital evidence.
- Proper chain of custody demonstrates that digital evidence was acquired from a specific system and/or location, and that it was continuously controlled since it was collected.
- Proper chain of custody documentation enables the court to link the digital evidence to the crime.
- Incomplete documentation can result in confusion over where the digital evidence was obtained and can raise doubts about the trustworthiness of the digital evidence.

Reliability of Digital Evidence

- To authenticate digital evidence, it may also be necessary to assess its reliability.
- There are two general approaches to assessing whether digital evidence can be relied upon in court.
  - Focus on whether the computer that generated the evidence was functioning normally,
  - Examine the actual digital evidence for evidence of tampering and other damage.
- The majority of legislation in the United States and United Kingdom followed the first approach, instructing courts to evaluate computer generated records on the basis of the reliability of the system and process that generated the records.

Reliability of Digital Evidence

- The Federal Rules of Evidence 901 (b) (9) titled “Requirement of Authentication or Identification” includes “evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.”
- In the United Kingdom, under Section 69 of PACE, there was a formal requirement for a positive assertion that the computer systems involved were working properly.
- The rationale for this approach is that, because records of this type are not the counterpart of a statement by a human declarant, which should ideally be tested by cross-examination of that declarant, they should not be treated as hearsay, but rather their admissibility should be determined on the basis of the reliability and accuracy of the process involved

Reliability of Digital Evidence

- In 1997, the UK Law Commission recommended the repeal of Section 69 of PACE (Law Commission, 1997), noting the difficulties in assessing the reliability of computer systems, and criticizing Section 69 of PACE because it required a complex certification of the system even when there is no sign that the evidence might be unreliable, and it failed to address the major causes of inaccuracy in digital evidence.
- Without section 69, a common law presumption comes into play: in the absence of evidence to the contrary, the courts will presume that mechanical instruments were in order at the material time.
- Where a party sought to rely on the presumption, it would not need to lead evidence that the computer was working properly on the occasion in question unless there was evidence that it may not have been in which case the party would have to prove that it was

Best Evidence

- When dealing with the contents of a writing, recording, or photograph, courts sometimes require the original evidence.
- The original purpose of this rule was to ensure that decisions made in court were based on the best available information.
- With the advent of photocopiers, scanners, computers, and other technology that can create effectively identical duplicates, copies became acceptable in place of the original, unless “a genuine question is raised as to the authenticity of the original or the accuracy of the copy or under the circumstances it would be unfair to admit the copy in lieu of the original” (Best Evidence Rule).
- Because an exact duplicate of most forms of digital evidence can be made, a copy is generally acceptable.
- In fact, presenting a copy of digital evidence is usually more desirable because it eliminates the risk that the original will be accidentally altered.

Hearsay

- Digital evidence might not be admitted if it contains hearsay because the speaker or author of the evidence is not present in court to verify its truthfulness.
- For instance, an e-mail message may be used to prove that an individual made certain statements, but cannot be used to prove the truth of the statements it contains.
- For example, although Larry Froistad sent a message to an e-mail list indicating that he killed his daughter, investigators needed a confession and other evidence to prove this fact The Canadian case against Pecciarich provides an interesting example of what may be considered hearsay in the context of online activities.

http://www.nytimes.com/1998/04/30/us/on-line-trail-to-an-off-line-killing.html

Hearsay Exceptions

- There are several exceptions to the hearsay rule to accommodate evidence that portrays events quite accurately and that is easier to verify than other forms of hearsay.
- For instance, the U.S. Federal Rules of Evidence specify that records of regularly conducted activity are not excluded by the hearsay rule:
  - A memorandum, report, record, or data compilation, in any form, or acts, events, conditions, opinions or diagnoses, made at or near the time by, or from information transmitted by a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, unless the source of the information or the method or circumstances of preparation indicate lack of trust- worthiness the term “business” as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.

Hearsay Exceptions

- The Irish Criminal Evidence Act (1992), has a similar exception in Section 5(1):
  - ... information contained in a document shall be admissible in any criminal proceedings as evidence of any fact therein of which direct oral evidence would be admissible if the information
- Although some courts evaluate all computer-generated data as business records under the hearsay rule, this approach may be inappropriate when a person was not involved.
- Computer-generated data may not be considered hearsay at all because they do not contain human statements or they do not assert a fact but simply document an act.

Levels of Certainty in Digital Forensics

- Analysis of digital evidence requires interpretation that forms the basis of any conclusions reached.
- Digital investigators should be able to estimate and describe the level of certainty underlying their conclusions to help fact finders determine what weight to attach.
- The field of digital forensics does not currently have formal mathematics or statistics to evaluate levels of certainty associated with digital evidence.
- There is currently a lack of consistency in the way that the reliability or accuracy of digital evidence is assessed, partly because of the complexity and multiplicity of computer systems.
- Furthermore, the level of certainty that digital investigators assign to their findings is influenced by their knowledge and experience.

Direct Versus Circumstantial Evidence

- Direct evidence establishes a fact. Circumstantial evidence may suggest one. It is a common misconception that digital evidence cannot be direct evidence because of its separation from the events it represents. However, digital evidence can be used to prove facts.
- Although digital evidence is generally only suggestive of human activities, circumstantial evidence may be as weighty as direct evidence and digital evidence can be used to firmly establish facts.
- For example, a computer log on record is direct evidence that a given account was used to log in to a system at a given time but is circumstantial evidence that the individual who owns the account was responsible. Somebody else might have used the individual's account and other evidence would be required to prove that he/she actually logged in to the system.
- It may be sufficient to demonstrate that nobody else had access to the individual's computer or password. Alternately, other sources of digital evidence such as building security logs may indicate that the account owner was the only person in the vicinity of the computer at the time of the log on.

Scientific Evidence

- In addition to challenging the admissibility of digital evidence directly, tools and techniques used to process digital evidence have been challenged by evaluating them as scientific evidence.
- Because of the power of science to persuade, courts are careful to assess the validity of a scientific process before accepting its results.
- If a scientific process is found to be questionable, this may influence the admissibility or weight of the evidence, depending on the situation.

Scientific Evidence

- In most U.S. states, novel scientific evidence is evaluated using four criteria developed in Daubert v. Merrell Dow Pharmaceuticals, Inc. (1993).
- These criteria are as follows:
  - Whether the theory or technique can be (and has been) tested.
  - Whether there is a high known or potential rate of error, and the existence and maintenance of standards controlling the technique's operation.
  - Whether the theory or technique has been subjected to peer review and publication.
  - Whether the theory or technique enjoys "general acceptance" within the relevant scientific community.
- The problems relating to admissibility and understanding of scientific evidence have become sufficiently complicated to require new approaches.
- In the United Kingdom and Ireland, law reform commissions have published recommendations on how to address challenges relating to admissibility of scientific evidence in general, and digital evidence in specific (Irish Law Reform Commission, 2009; UK Law Commission, 2009).

Presenting Digital Evidence

- Digital investigators are commonly asked to testify or produce a written summary of their findings in the form of an affidavit or expert report.
- Testifying or writing a report is one of the most important stages of the investigative process because, unless findings are communicated clearly in writing, others are unlikely to understand or make use of them.

Expert Reports

- Whenever possible, digital investigators should support assertions in their reports with multiple independent sources of evidence to ensure that any potential weakness in one source of digital evidence does not undermine an other- wise valid conclusion.
- They should clearly state how and where all evidence was found, to help decision makers to interpret the report and to enable another competent digital investigator to verify results.
- Including important items of digital evidence as figures or attachments can be useful when testifying in court as it may be necessary to refer to the supporting evidence when explaining findings in the report.
- Presenting alternative scenarios and demonstrating why they are less reasonable and less compatible with the evidence can help strengthen key conclusions.
- Explaining why other explanations are unlikely or impossible demonstrates that the scientific method was applied—that an effort was made to disprove the given conclusion but that it withstood critical scrutiny.

Expert Reports

- A formal report of forensic findings should give readers all of the information they need to evaluate the evidence and associated conclusions.
- The following is a sample report structure:
  - Introduction
  - Evidence Summary
  - Examination Summary
  - File System Examination
  - Forensics Analysis and Findings
  - Conclusions

Expert Reports

- Introduction
  - Provide an overview of the case, the relevance of the evidential media being examined, who requested the forensic analysis, and what was requested.
  - The introduction should provide the bonafides of those who performed the work, including a summary of relevant experience and training.
  - A full CV can be provided as an attachment to the report.
- Evidence Summary
  - Describe the items of digital evidence that were analyzed, providing details that uniquely identify such as make, model, and serial number.
  - Also consider including MD5 values, photographs, laboratory submission numbers, details of when and where the evidence was obtained, from whom the evidence was obtained and its condition (note signs of damage or tampering), and processing methods and tools.

Expert Reports

- Examination Summary
  - Provide an overview of the critical findings relating to the investigation. Think of this as the executive summary, with any recommendations or conclusions in short form.
  - This section is intended for decision makers who may not have time to read the full report and just need to know the primary results of the forensic analysis.
  - In certain situations, it is advisable to summarize tools used to perform the examination, how important data were recovered (e.g., decryption and undeletion), and how irrelevant les were eliminated (e.g., using NSRL hash sets).
  - Whenever feasible, use the same language in the examination summary as is used in the body of the report to avoid confusion and to help the attentive reader associate the summary with the relevant section in the detailed description.

Expert Reports

- File System Examination
  - When dealing with storage media, provide an inventory of files, directories, and recovered data that are relevant to the investigation with important characteristics such as path names, date- time stamps, MD5 values, and physical sector location on disk.
  - Note any unusual absences of data that may be an indication of data destruction, such as mass deletion, reformatting, or wiping.

Expert Reports

- Forensic Analysis and Findings
  - Provide a detailed description of the forensic analysis performed and the resulting findings, along with supporting evidence.
  - Any detailed forensic analysis of particular items that requires an extensive description can be provided in a separate subsection.
  - The report should clearly specify the location where each referenced item was found, enabling others to replicate and verify the results in the future. In addition to describing important findings in the report, it can be more clear and compelling to show a photograph, screenshot, or printout of the evidence.
  - Describe and interpret temporal, functional, and relational analysis and other analyses performed such as evaluation of source and digital stratigraphy.

Expert Reports

- Conclusions
  - A summary of conclusions should follow logically from previous sections in the report and should reference supporting evidence.
  - It is important not to jump to conclusions or make statements about innocence or guilt.
  - Conclusions must be objective and be based on fact.
  - Let the evidence speak for itself and avoid being judgmental.

Expert Reports

- In the United Kingdom, information that must be provided in an expert report is described in the Criminal Procedure Rules and includes the following:
  - The expert's qualifications, relevant experience, and accreditation.
  - The substance of all facts given to the expert which are material to the opinions expressed in the report or upon which those opinions are based.
  - A summary of conclusions.
- In addition, the UK Criminal Procedure Rule indicates that, where there is a range of opinion on the matters dealt with in the report, the range of opinion should be explained and the basis for the expert's own opinion should be provided with any necessary caveats

Testimony

- When digital investigators first take the stand, they must first be accepted as an expert by the court.
- During this process, called *voir dire*, digital investigators will generally be asked to provide a summary of their qualifications and experience and, in some cases, will be asked questions about their training, credentials, etc.
- After this process, the court will decide whether to accept the digital investigator as an expert who can testify in the case.
- During cross-examination, attorneys often attempt to point out aws and details that were overlooked by the digital investigator.
- The most effective response to this type of questioning is to be prepared with clear explanations and supporting evidence.
- In some cases, the goal of the opposing counsel may be to raise doubts about digital forensic findings.

Summary

- The foundation of any case involving digital evidence is proper evidence handling.
- Therefore, the practice of seizing, storing, and accessing evidence must be routine to the point of perfection.
- Standard operating procedures with forms are a key component of consistent evidence handling, acting as both memory aids for digital investigators and documentation of chain of custody.
- Also, training and policies should provide digital investigators with a clear understanding of acceptable evidence handling practices and associated laws.
- Verifying that evidence was handled properly is only the first stage of assessing its reliability.
- Courts may also consider whether digital evidence was altered before, during, or after collection, and whether the process that generated the evidence is reliable.
- Claims of tampering generally require some substantiation before they are seriously considered.
- Someone familiar with the system in question, who can testify that the computer was operating normally at the time, can generally address questions regarding the process that generated a given piece of digital evidence

Questions