



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

Digital Forensics Analysis (ACCA7031_LON)

Lecture 2

Cyber Forensics and the Law

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk

Content covered

- Chain of custody
- Digital Evidence collection and handling in practice
- Legal framework for different countries
- The role of digital evidence in court trials

Objectives

- Understand the chain of custody in DFIR context
- Understand key principles for evidence collection and handling
- Be aware of Legal framework and IT law in different countries
- Differentiate between written report and expert witness verbal report law enforcement and corporate investigation

Chain of Custody

- **Chain of Custody** - Documentation of all the steps that evidence has taken from the time it is located at the crime scene to the time it's introduced in the courtroom. All steps include collection, transportation, analysis, and storage processes. All accesses of the evidence must be documented as well.
- You'll be required to prove to the court that the evidence did not change during the investigation.
- You'll have to provide your *own evidence* that all collected evidence exists, without changes, as it did when it was collected.

Chain of Custody (cont.)

- The chain of custody is so named because evidence has the potential to change each time it is accessed. You can think of the path evidence takes to the courtroom as a chain in which each access is a link in the chain.
- If any one link breaks, (i.e., breaks the integrity of the evidence), the whole chain breaks at that point.
- The court expects the chain of custody to be complete and without gaps.

Chain of Custody (cont.)

- You demonstrate a complete chain of custody by providing the evidence log that shows every access to evidence, from collection to appearance in court.
- A complete chain of custody log also includes procedures that describe each step.
- For example, an entry might read "checked out hard disk drive serial number BR549 to create a primary analysis image." You should also include a description of what "creating a primary analysis image" means.

Chain of Custody (cont.)

- The defense will examine the chain of custody documents, looking for any gaps or inconsistencies.
- Any issue with the chain of custody has the real potential of causing the court to throw out the evidence in question.
- Once that happens, the evidence you have collected becomes useless and your credibility will probably be questioned.

Chain of Custody (cont.)

- The following is an example of a form:

<https://www.scribd.com/document/372094922/Chain-of-Custody-Form>

Single Evidence Form		
Case No.		Evidence No.
PLEASE COMPLETE FORM IN UPPERCASE		
Section B: Evidence Collection		
Date/Time Collected		Collected by
Site Address		
Section C: Evidence Details		
Date/Time Stored		
Storage Location		
Device Type	Capacity	
Manufacturer	Model	
Serial No.		
MD5 Sum		
SHA-1 Sum		
Additional Information...		
Note any damage, marks and scratches		
Digital Image Taken		☐ Yes ☐ No
Section D: Image Details		
Date/Time Imaged		Imaged by
Storage Location		
Image Filename	Image Size	(inc. vnt)
Additional Information...		
This form is to be used when collecting a hardware device containing data that may be of interest in a case. Guidelines:		
• Ensure that this form only refers to one item of evidence and that one is completed for each item of evidence • This form must be accompanied by Chain of Custody forms which detail the individuals that have handled the evidence • Further remarks can be noted overleaf in Section E: Remarks • It is important that these forms are kept with the evidence at all times • Upon handover or disposal please complete Section F: Evidence Handover		

Digital Evidence

- Security violations involving computers (two ways)
 - ❑ a computer can be used in the commission of crimes or violations of policy
 - ❑ a computer can be the target of crime or an attack.
- Any violation of security policy is called a ***security incident***, regardless of whether an action is a crime.
- The main purpose of computer forensics is the proper identification and collection of computer evidence.
- To properly investigate an incident and possibly take action against the perpetrator, you'll need evidence that provides proof of the identity and actions of an attacker.

Digital Evidence (cont.)

- The existence of some files, such as pictures or executable files, can provide evidence of an incident.
- In other cases, the contents of files, such as log files, provide the necessary proof.
- Recognizing and identifying hardware, software, and data you can use is the first step in the evidence collection process.
- U.S. courts accept digital evidence as physical evidence
 - Digital data is a tangible object
- Some require that all digital evidence be printed out to be presented in court

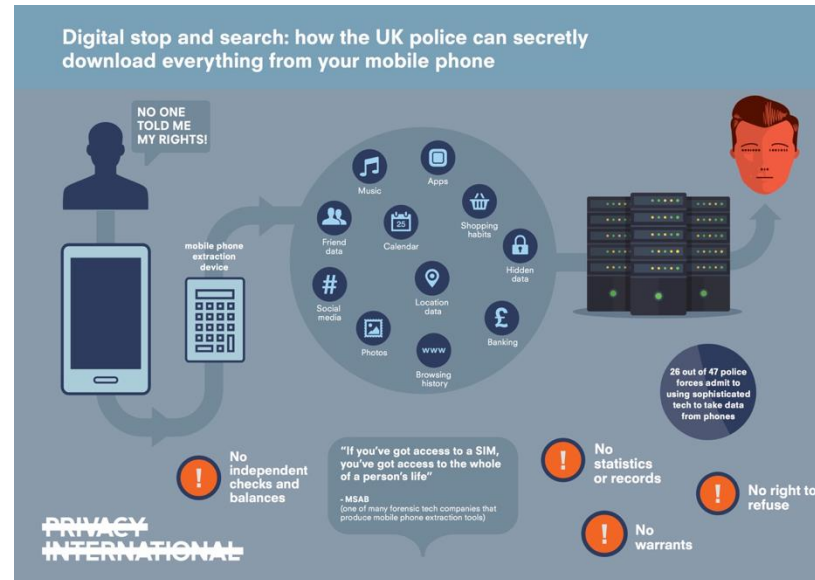
Digital Evidence (cont.)

- **Digital Evidence** - any digital device hardware, software, or data that can be used to prove one or more of the five Ws and a H of a security incident (i.e., who, what, when, where, why, and how).
- **Digital Evidence** consists of files and their contents that are left behind after an incident.

Digital Evidence Examples

- Examples of digital evidence on a mobile phone

<https://privacyinternational.org/explainer/3022/push-button-evidence-digital-forensics>



Differences between Digital Evidence and Regular Evidence

- Before you start looking for evidence, understand that most successful cases are based on several types of evidence. As you conduct an investigation, be aware of the different types of evidence you can gather.
- Four basic types of evidence can be used in a court of law:
 - real evidence
 - documentary evidence
 - testimonial evidence
 - demonstrative evidence
- Digital evidence generally falls into the first two categories of evidence. A complete investigation, however, should address all types of available evidence.

Real Evidence

- **Real Evidence**: any physical objects that you can bring into court. Real evidence can be touched, held, or otherwise observed directly.
- Other types of real evidence in a computer forensics investigation could be the hard drive from a suspect's computer or any other memory of digital devices.
- Real evidence is the most tangible and easiest to understand type of evidence. When presenting a case to a jury, real evidence can make the case seem more concrete.
- Real evidence that is conclusively associated with a suspect or activity is called ***hard evidence***.

Real Evidence (Cont.)

- Real evidence is conclusively associated with a suspect or activity.
- Never overlook potential evidence when conducting an investigation. Other types of evidence may involve or refer to real evidence.
- It is very common to use log file contents when arguing a case. The process of establishing the credibility and authenticity of such data is often easier when you start with the physical disk drive and/or computer from which you extracted the log file.

Real Evidence Examples



<https://upload.wikimedia.org/wikipedia/commons/thumb/f/f8/Laptop-hard-drive-exposed.jpg/1200px-Laptop-hard-drive-exposed.jpg>



<https://upload.wikimedia.org/wikipedia/commons/1/17/SanDisk-Cruzer-USB-4GB-ThumbDrive.jpg>

Looking for Real Evidence

- Assume you have been asked to investigate an e-mail spammer. Due to the nature and volume of e-mails being sent, local law enforcement has been called in to investigate and they have called you. You arrive on the scene to begin your investigation.
- Before you touch anything, look around the scene and take pictures of everything. Digital pictures are inexpensive, but they can be valuable later.
- As you progress through the investigation, you'll want to be able to refer back to images of the way you found everything.
- It's not uncommon to find additional evidence in the original pictures after extracting digital evidence from a suspect's machine.

Looking for Real Evidence (cont.)

- After you take pictures of everything, start identifying all of the real evidence you think is pertinent and that you have permission to search or seize. Notice the suspect's laptop. It has a printer and a mobile phone cable plugged into it. That tells you to look for the mobile and printer source or target data.
- Mobiles can be a valuable source of documentary evidence. Most people who use Mobiles store a lot of personal data on them. Find the mobile and make sure it has power. If you are authorised to seize the mobile phone, make sure you take the cable as well.
- After looking for the mobile, look for any source documents (for example, printed hard copies) the suspect might have printed or scanned. Also look for removable storage the suspect might have used to store scanned images.

Looking for Real Evidence (cont.)

- Next, examine the physical laptop and surrounding area for other clues of evidence. You should look for additional clues such as:
 - handwritten notes. Even technically savvy people use notes. In fact, because handwritten notes are not stored on a computer, many people consider them to be more "secure."
 - any peripheral device that is, or can be, connected to the computer. This could include:
 - Storage devices
 - Communication devices
 - Input/output devices
 - all removable media, such as:
 - CD/DVD-ROMs (CD/DVD-Rs and CD/DVD-RWs as well, Blu-Rays)
 - Flash drives, Floppy disks
 - Tapes and other magnetic media
- This is not an exhaustive list.

Documentary Evidence

- **Documentary Evidence**: Written evidence, such as printed reports or data in log files. Such evidence cannot stand on its own and must be authenticated.
- Authenticating documentary evidence can be quite complex when you're trying to convince nontechnical jurors (or judges) that the contents of a file conclusively prove an attacker performed a specific action.
- We have all heard of hard evidence that was thrown out of court because it was collected illegally.
- Computer evidence can be even more difficult to collect properly.

Best Evidence Rule

- **Best Evidence Rule** - anytime you introduce documentary evidence, you must introduce the original document, not a copy.
- The purpose of this rule is to protect evidence from tampering. If the original document is required, there is less opportunity for a modification to occur during a copy operation.
- Most of your documentary evidence will come directly from items on the real evidence list. Some documentary evidence will be supplied by third parties, such as access logs from an Internet Service Provider (ISP), but most will come from your own investigation activities.
- Always document and document every step of your investigation.

Testimonial Evidence

- **Testimonial Evidence** – the evidence that consists of witness testimony, either verbal or in written form.
- Testimonial evidence can be presented in person by the witness in a court or through a recorded deposition.

Demonstrative Evidence

- **Demonstrative Evidence** – the evidence that illustrates, helps explain, or demonstrates other evidence. Many times, demonstrative evidence consists of some type of visual aid.

Search and Seizure

- You probably won't have unobstructed access to all evidence. Before you collect evidence, you must make sure you have the right to either search or seize the evidence in question.
- Law enforcement officer may search for and seize criminal evidence only with **probable cause**
- In the United States, The Fourth Amendment states that only warrants “particularly describing the place to be searched, and the persons or things to be seized” can be issued
- The options and restrictions of searching and seizing evidence:
 - Voluntary Surrender
 - Subpoena
 - Search Warrant

Voluntary Surrender

- **Voluntary Surrender** - Permission granted by a computer equipment owner to search and/or seize the equipment for investigative purposes.
- The easiest method of acquiring the legal right to search or seize computer equipment
- Never assume you have consent to search or seize computer equipment. Always ensure you are in compliance with all policies and laws when conducting an investigation.
- Few things are more frustrating than having to throw out good evidence because it was acquired without proper consent.

Subpoena

- **Subpoena** - A court order that compels an individual or organization to surrender evidence.
- A subpoena is appropriate when it is unlikely that notifying the computer equipment owner will result in evidence being destroyed.

Subpoena

<https://percipient.co/wp-content/uploads/2020/03/Document-and-ESI-subpoena-1200x1551.png>

AO 88 (Rev. 11/94) Subpoena in a Civil Case

Issued by the
UNITED STATES DISTRICT COURT
Northern DISTRICT OF California

Digital Millennium Copyright Act,
section 512(h) subpoena to online
service provider

SUBPOENA IN A CIVIL CASE

Case Number: **CV 06 - 80304 MISC. JW**

TO: Google, Inc., Google Video Support, DMCA Complaints
1600 Amphitheatre Parkway
Mountain View, CA 94043

☐ YOU ARE COMMANDED to appear in the United States District Court at the place, date, and time specified below to testify in the above case.

PLACE OF TESTIMONY: COURTROOM
DATE AND TIME:

☐ YOU ARE COMMANDED to appear at the place, date, and time specified below to testify at the taking of a deposition in the above case.

PLACE OF DEPOSITION: DATE AND TIME:

☒ YOU ARE COMMANDED to produce and permit inspection and copying of the following documents or objects at the place, date, and time specified below (list document or object):
Documents sufficient to allow Landmark Education to identify the infringer
"Anatgaire" who posted videos labeled "Introduction" and "Inside the Landmark
Forum" (1 through 6 of 6), as described in the letter of notification in Exh. A.

PLACE: DATE AND TIME:
Sleevefel, Levitt & Weiss, PC October 28, 2006
One Embarcadero Center, 30th Floor 10:00 AM
San Francisco, CA 94111-3719

☐ YOU ARE COMMANDED to permit inspection of the following premises at the date and time specified below.

PREMISES: DATE AND TIME:

Any organization not a party to this suit that is subpoenaed for the taking of a deposition shall designate one or more officers, directors, or managing agents, or other persons who consent to testify on its behalf, and may set forth, for each person designated, the matters on which the person will testify. Federal Rules of Civil Procedure, 30(b)(6).

ISSUING OFFICER'S SIGNATURE AND TITLE (INDICATE IF ATTORNEY FOR PLAINTIFF OR DEFENDANT): DATE
Sandy Morris 10-19-06

ISSUING OFFICER'S NAME ADDRESS AND TELEPHONE NUMBER
L5506, 280 So. 1st St. Rm 2112, San Jose, CA 95113 (408) 535-5342

(Use Rule 65, Federal Rules of Civil Procedure, parts C & D on reverse)

¹ If action is pending in district other than district of issuance, state district under case number.

AO-88

Search Warrant

- **Search Warrant** - A court order that allows law enforcement to search and/or seize computer equipment without providing advance warning to the equipment owner.
- You need to have the court grant law enforcement officers permission to search and/or seize the identified computer equipment without giving the owner any prior notice. A search warrant allows law enforcement officers to acquire evidence

Search Warrant

<https://www.deviantart.com/phatraver/art/Real-Search-warrant-413010870>

ITEMS TO BE SEARCHED FOR Attachment #1

5-1-12
REVIEW SV.
JFC

1. Controlled substances, including but not limited to marijuana.
2. Paraphernalia for packaging, weighing, and distributing marijuana or other controlled substances.
3. Books, records, receipts, airline tickets, notes, ledgers, and other papers relating to the transportation, ordering, purchasing and distribution of marijuana or other controlled substances.
4. Address and/or telephone books, papers and other items reflecting names, addresses and telephone numbers.
5. Books, records, receipts, bank statements, money drafts, letters of credit, money orders and cashier's check receipts, passbooks, documents indicating locations of safe deposit boxes and other items evidencing the obtaining, secreting, transfer and/or expenditures of monies.
6. United States currency, precious metals, jewelry, financial instruments including stocks and bonds, and other valuables purchased with the fruits of the proceeds of controlled substance transactions, which your affiant has reason to believe are subject to forfeiture.
7. Indicia of occupancy, residency or payments of utilities and rent.
8. Photographs, including still photos, negatives, videotapes, films, undeveloped film and the contents therein, in particular photographs of co-conspirators, assets and/or controlled substances.
9. Digital pagers and cellular phones and any information contained therein.
10. Keys to safes, safe deposit boxes, and rental storage lockers.
11. Safes, deposit boxes, lockers or lockboxes.
12. Electronic equipment such as computers, fax machines, etc. used to place orders, transfer, record or store information related to the possession or sale of controlled substances. Additionally computer software, tapes, discs, audiotapes and the contents therein, containing the information generated by the aforementioned electronic equipment and communication devices.
13. Firearms and ammunition, and any records or receipts pertaining to firearms and ammunition.

Evidence Admissibility in a Court of Law

- Specific rules to the evidence submitted.
- A waste of time to carefully analyse evidence that the court refuses to consider
- Good evidence can be tainted by an investigator on its way to court, making it unacceptable

Evidence Admissibility in a Court of Law (cont.)

- **Relevance** and **Admissibility** - two basic standards to all evidence
- ***Relevant evidence*** is any evidence that proves or disproves the facts in a case
- ***Admissible evidence*** is the evidence that meets all regulatory and statute requirements, and has been properly obtained and handled.

Evidence Preservation

- The main goal of evidence preservation is to ensure that absolutely no changes have taken place since the evidence was collected.
- Your collection and handling procedures will be examined.
- Take all necessary precautions to protect collected evidence from damage that might change its state.

Evidence Preservation (cont.)

- You will have to address several concerns throughout your investigation.
 - do not handle any evidence until you are absolutely sure you can legally acquire the evidence
 - the collection and analysis process will not change the evidence

Combatting Digital Crime Legally

- Laws and regulations in the United States:
 - Computer Fraud and Abuse Act (CFAA)
 - associated with the unauthorized access to a computer system and DoS attacks
 - Electronic Communications Privacy Act (ECPA)
 - makes illegal the unauthorized interception of communications through electronic means
 - Economic Espionage Act of 1996 (EEA)
 - makes economic espionage and the theft of trade secrets a crime

Combating Digital Crime Legally (cont.)

- Laws and regulations in the United Kingdom:
 - Computer Misuse Act 1990
 - Handles many of the malicious attacks or offences against computer solutions, including hacking and ransomware.
 - Protection Acts for Businesses Data Protection Act (1998)
 - Key in safeguarding all types of private, confidential, or business information. It ensures that data is handled in a safe, fair, and lawful manner.
 - Data Protection Act (2018)
 - Continues the goals from the previous legislation, controlling how “information is used by organisations, businesses, or the government”. This is part of the UK’s General Data Protection Regulation.

Combating Digital Crime Legally (cont.)

- Laws and regulations in the EU:
 - EU Cybersecurity Act (2019)
 - Establish a European cyber security certification framework for ICT products, services and processes.
 - General Data Protection Regulation (GDPR) (2018)
 - Set up in 2018 to harmonise data protection and privacy laws across member states, the GDPR is already in full force. It enables member states to impose heavy sanctions against organisations that fail to comply.
 - Common Foreign and Security Policy (CFSP)
 - It instructs each member state to implement sound cybersecurity measures.

Combating Digital Crime Legally (cont.)

- Applying the general laws found in different countries affects how Cyber Forensics can be conducted
- Within the United States for example, the fourth amendment of the constitution ensures lawful application of search and seizure, emphasising the importance of the correct documentation such as subpoenas as mentioned previously
- Legislation such as GDPR in Europe and the Data Protection Act in the UK govern how sensitive data is stored and processed, which is highly important in a forensics environment where evidence will often contain very sensitive information pertaining to both victims and suspects

Ethical considerations for Cyber Forensics

- Privacy is generally seen as a central issue for Computer Forensics.
- The most common ethical problem is managing the discovery of confidential data that is irrelevant to the case at hand.
- Different professional bodies provide their own interpretations
- One example, the International Association of Computer Investigative Specialists (IACIS)
 - Members should maintain the utmost objectivity in all forensics investigations and present the facts accurately.
 - The evidence should be examined and analyzed thoroughly.
 - Only unbiased opinions should be given.
 - Members must not conceal any findings that would cause the facts of a case to be distorted or misrepresented.

Legislative Lag

- Laws tend to lag significantly behind the industry's advances, largely because most legislation has been reactionary
- A longer period of time elapse between innovations in criminal enterprise and the response of the state and law enforcement agencies
- Illusion - digital crime develops and changes very rapidly, but it may take years for legislation to be enacted, by which time the crime may well be mutated or developed to assume a different form
- UK government does not share the view that specific e-related legislation is always necessary, or that there is necessarily a problem of legislative lag.

Summary

1. Chain of custody in context of Digital Crime
2. Laws applying to Digital Evidence collection and handling
3. Digital Evidence preservation and admissibility
4. Laws governing the Cyber Forensics Profession
5. Legal context in the UK, EU and US to Combat Digital Crime
6. Ethical Issues in Cyber Forensic Investigation
7. Legislative Lag



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

Any Questions?

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk