

Legal and Regulatory Frameworks

MSCS630: Cybercrime Investigation and Digital Evidence

Dr. Mouatez Karbab



أكاديمية جوعان بن جاسم للدراسات الدفاعية
Joaan Bin Jassim Academy for Defence Studies

September 30, 2026



Outline

- 1 Digital Evidence Admissibility
- 2 Authority to Search and Seize Digital Evidence
- 3 Maintaining the Chain of Custody
- 4 Jurisdictional Frameworks



Introduction to Legal and Regulatory Frameworks I

Objectives

- What evidence needs to be usable in court.
- The legal authority needed to search for and seize data.
- The correct process for documenting the chain of custody.
- The international, regional and national rules an investigation crosses.

Why This Matters

- Every investigator action is subject to legal review.
- Inadmissible evidence cannot support a finding, however strong.



Outline

- 1 Digital Evidence Admissibility
- 2 Authority to Search and Seize Digital Evidence
- 3 Maintaining the Chain of Custody
- 4 Jurisdictional Frameworks



Admissibility and the Best Evidence Rule I

- Findings go to a *trier of fact*; first the court must approve them as admissible.
- Admissibility applies to all evidence, digital or physical.

Best Evidence Rule for Digital Evidence

- Traditionally the original document or recording had to be shown.
- A *forensic image*, a bit-for-bit copy, is now usually accepted as the original.
- Rule 1001(d): for Electronically Stored Information (ESI), an "original" is any accurate readable output.
- Rule 1003: a duplicate is admissible unless authenticity is genuinely disputed [12, 11, 13].
- The copy is accepted only if proven unchanged, normally by hashing.



Relevance and Authenticity I

Relevance

- Evidence that makes an important fact more or less likely [14].
- A file timestamp, a GPS log; the report must say why it matters.

Authenticity

- The presenter must prove the item is genuine [17].
- Stating where an email was found does not authenticate it.
- Prove it is real, unaltered, and from the claimed source.
- Needs chain of custody, tested tools and detailed notes.

Relevance and Authenticity II

State of Connecticut v. Julie Amero

- Teacher convicted in 2007 over classroom pop-ups; first investigation was superficial.
- Independent analysis showed spyware; conviction vacated, felony charges dropped.
- Poor forensic analysis produces wrong conclusions that are difficult to reverse [6].

Hearsay and the Business Records Exception I

Definition: Hearsay

- An out-of-court statement offered to prove it is true [15].
- Usually excluded: the *declarant* cannot be questioned.
- Emails, texts, documents, even server logs can be "statements".

Business Records Exception

- Records made near the time, by someone who knew, in regular business practice [16].
- Covers Internet Service Provider (ISP) logs, transaction records, system event logs, company email.

Computer-Stored and Computer-Generated Records

- **Computer-stored:** human statements on a machine (email, documents): hearsay.
- **Computer-generated:** made automatically (logs, timestamps): usually not hearsay [7].

Authentication by Hashing I

Definition: Hash Function

- Any data in, a fixed-size *digital fingerprint* out.
- Message-Digest Algorithm 5 (MD5); Secure Hash Algorithm 256 (SHA-256).
- Collision resistant; one changed bit changes the whole hash; irreversible.
- Hash at collection, recompute later; a match proves the evidence is unchanged.

```
$ sha256sum /evidence/original_file.dd      # recorded in the custody log
$ cp /evidence/original_file.dd /working_copy/original_file.dd
$ sha256sum /working_copy/original_file.dd  # must match exactly
```

Frye and Daubert I

Frye (1923)

- "General acceptance": the field's experts must accept the method [1].

Daubert (1993)

- The judge decides whether expert testimony is relevant and reliable.
- Tested? Peer reviewed? Known error rate? Controlling standards? Generally accepted? [3]

Daubert Requirements for Examiners

- A statement that the tool found the evidence is not sufficient.
- Explain how the tool works, its known errors, its validation, its acceptance.
- Hence tool testing and validation are core lab jobs.

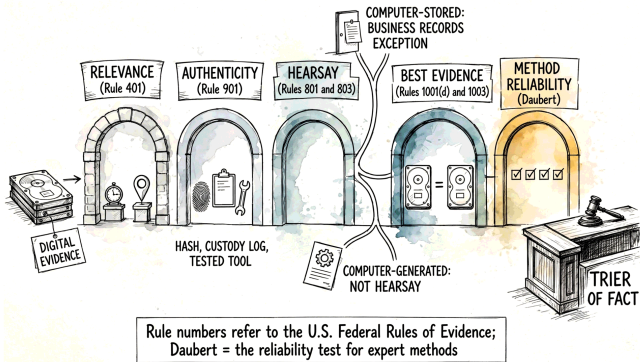


Requirements for Admitting Digital Evidence I

- Five separate requirements; evidence that fails any one is excluded.
- The investigator brings the answer to each: custody log and hash, the business-records exception, a defensible method.



Requirements for Admitting Digital Evidence II



Each requirement is a separate question the investigator must answer.

Evidence that fails any one requirement is excluded.



Section 1: Assessment I

Question

Why are web server access logs usually not treated as hearsay?

- A. Because the business records exception waives the rule for all logs.
- B. Because they are computer-generated, not statements by a person.
- C. Because the server administrator testifies to their contents.
- D. Because logs are never offered to prove the truth of their contents.



Section 1: Assessment - Answer I

Question

Why are web server access logs usually not treated as hearsay?

- A. Because the business records exception waives the rule for all logs.
- B. Because they are computer-generated, not statements by a person. (✓)
- C. Because the server administrator testifies to their contents.
- D. Because logs are never offered to prove the truth of their contents.

Explanation:

- A machine created the record automatically as part of a normal process [7].

Outline

- 1 Digital Evidence Admissibility
- 2 Authority to Search and Seize Digital Evidence
- 3 Maintaining the Chain of Custody
- 4 Jurisdictional Frameworks



Warrants: Probable Cause, Particularity, Scope I

- Evidence obtained without legal permission risks suppression, however probative.
- Basis: the Fourth Amendment against unreasonable government searches.

Definition: Warrant

- Judge-signed permission to search a specific person, place or car.
- **Probable cause:** facts a reasonable person would take as evidence of a crime, findable there.
- **Particularity:** describe the place and the things; no "general warrant".
- Yet broad enough for hidden or encrypted data; courts often allow seizing the whole device.
- **Scope:** a warrant for financial documents covers spreadsheets, not the rest of the drive.



Exceptions to the Warrant Requirement I

- **Consent:** free, informed, from someone with authority; record it in writing.
- **Exigent circumstances:** danger to life or imminent destruction of evidence, e.g. remote deletion.
- **Plain view:** lawfully present, evidence clearly visible, e.g. an open laptop showing a criminal email.



Third Parties, Carpenter and the SCA I

Third-Party Doctrine

- Less privacy in information willingly given to companies [2].
- *Carpenter* (2018): historical cell-site location generally needs a warrant [5].
- Confined to historical records; real-time tracking and tower dumps unresolved.

Stored Communications Act (SCA)

- **Subpoena:** name, address, payment records.
- **Court order:** non-content records: to/from, timestamps, IP logs.
- **Warrant:** content: email bodies, cloud files, stored messages.

Silk Road

- Key evidence on an Icelandic third-party server; a Mutual Legal Assistance Treaty (MLAT) request produced the image that convicted Ulbricht [22].

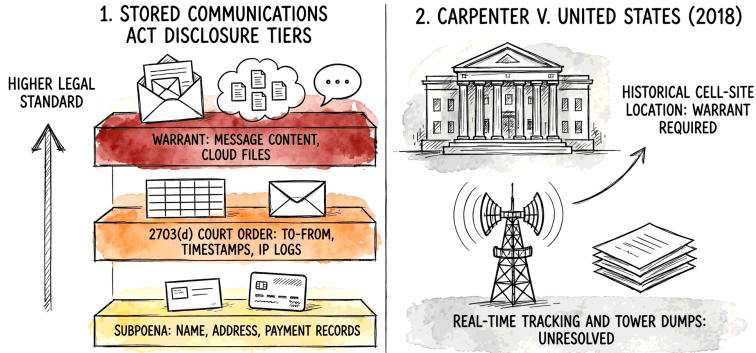


Stored Communications Act Disclosure Tiers I

- Each tier reaches more private data and requires more legal justification.
- *Carpenter* moved historical cell-site location to the warrant tier.



Stored Communications Act Disclosure Tiers II



2703(d) = THE COURT PROVISION OF THE STORED COMMUNICATIONS ACT; CONTENT = WHAT A MESSAGE SAYS; RECORDS = WHO SENT IT AND WHEN

EACH TIER DISCLOSES MORE PRIVATE DATA AND REQUIRES A HIGHER LEGAL STANDARD.

CARPENTER MOVED HISTORICAL LOCATION DATA TO THE WARRANT TIER.



Section 2: Assessment I

Question

Under the SCA, which instrument is needed for the body of stored emails?

- A. A subpoena.
- B. A court order.
- C. A search warrant.
- D. A written consent form from the provider.



Section 2: Assessment - Answer I

Question

Under the SCA, which instrument is needed for the body of stored emails?

- A. A subpoena.
- B. A court order.
- C. A search warrant. (✓)
- D. A written consent form from the provider.

Explanation:

- Subpoenas reach subscriber details, court orders non-content records; only a warrant reaches content.



Outline

- 1 Digital Evidence Admissibility
- 2 Authority to Search and Seize Digital Evidence
- 3 Maintaining the Chain of Custody**
- 4 Jurisdictional Frameworks



The Chain of Custody I

- A gap can lead the court to doubt authenticity and exclude the evidence.
- International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) 27037:2012 standardises identification, collection, acquisition and preservation [4].
- The log proves two things: same evidence as collected, and unchanged.

Contents of Each Transfer Entry

- Case and item number; description with make, model, serial.
- Name and signature of every handler; date and time; reason for the transfer.

Logging a New Item

- 1 Assign numbers; create the log; photograph in place.
- 2 First entry by the collecting officer, with a full description.
- 3 Seal in a *tamper-evident bag*; sign across the seal.
- 4 Every handover signed by the receiver; lab intake checks the seal.
- 5 Every removal from storage is a new entry.



Common Failures and Their Mitigation I

Three Common Failures

- **Broken chain:** a period with nobody signed for the item.
- **Improper sealing:** containers that reopen without trace.
- **Incomplete documentation:** missing dates, times or reasons.

Mitigation

- Never accept evidence without checking the packaging and the log first.
- Evidence Management Systems enforce fields and log automatically [18].



Chain-of-Custody Transfers from Seizure to Storage I

- Each transfer is signed by the person releasing and the person receiving the item.
- Failures appear as a missing signature, a resealable container or an undated entry.



Chain-of-Custody Transfers from Seizure to Storage II

1. SEIZURE TO COURT (The Custody Chain)



2. WHERE THE CHAIN BREAKS (Three Failure Points)

Every handoff is a signature pair,
from the desk to the courtroom.

Signature pair = one person hands over,
one person receives; a link without
both signatures is a break

A break in the chain is a gap
the court cannot see across.



Section 3: Assessment I

Question

A log shows the item received at the lab on Monday and next released on Thursday, with no entry between. What failure is this?

- A. Improper sealing.
- B. Incomplete documentation.
- C. Broken chain.
- D. No failure; storage time needs no entry.



Section 3: Assessment - Answer I

Question

A log shows the item received at the lab on Monday and next released on Thursday, with no entry between. What failure is this?

- A. Improper sealing.
- B. Incomplete documentation.
- C. Broken chain. (✓)
- D. No failure; storage time needs no entry.

Explanation:

- Intake and every removal must be logged; any unsigned period is a break.

Outline

- 1 Digital Evidence Admissibility
- 2 Authority to Search and Seize Digital Evidence
- 3 Maintaining the Chain of Custody
- 4 Jurisdictional Frameworks**



Budapest Convention, Second Protocol and UN Convention I

- An attack crosses three legal systems in a second; lawful at home may be unlawful abroad.

Budapest Convention on Cybercrime

- First and principal agreement; ratified by the U.S., Japan and most of Europe.
- Harmonise offences; domestic investigative powers; fast cooperation via a 24/7 Network [8].
- Second Additional Protocol (2022): direct routes to subscriber and traffic data abroad, quick preservation [9].

UN Convention against Cybercrime

- Adopted December 2024, signed in Hanoi October 2025 by seventy-plus states.
- First treaty of global reach; in force ninety days after the fortieth ratification [20].

Alternatives to the MLAT Process I

MLAT

- Government-to-government; the default route, and the slowest: around ten months.

U.S. CLOUD Act (2018)

- Clarifying Lawful Overseas Use of Data (CLOUD) Act: U.S. providers must produce data wherever stored; executive agreements let partners ask providers directly [21].

EU e-Evidence Regulation 2023/1543

- Applies from 18 August 2026; a judicial authority orders a provider in another Member State directly [10].
- **European Production Order Certificate (EPOC)** produces data.
- **European Preservation Order Certificate (EPOC-PR)** freezes it.
- Ten days as a rule, eight hours in an emergency; a European Investigation Order (EIO) can take 120 days.
- Reaches non-EU providers serving EU users.
- Planning turns on which provider holds the data and whether the order conditions are met.

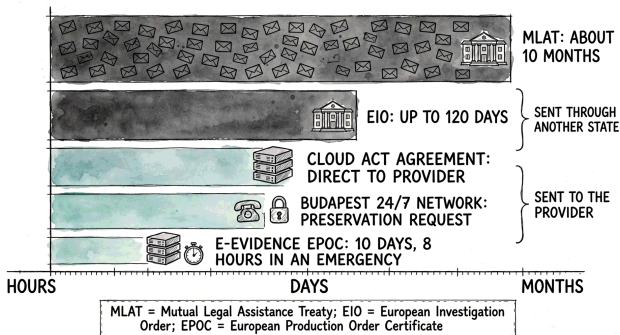


Response Times of Cross-Border Instruments I

- Instruments that go through a foreign government are counted in months.
- Instruments that go straight to the provider are counted in days, or hours.

Response Times of Cross-Border Instruments II

RESPONSE TIMES OF CROSS-BORDER EVIDENCE INSTRUMENTS



Requests sent through another state take months.

Requests sent to the provider take days, or hours in an emergency.



GDPR, CCPA/CPRA, CFAA and the Computer Misuse Act I

Privacy Limits

- **General Data Protection Regulation (GDPR):** data minimisation and purpose limitation; imaging a whole shared server for one employee may breach it [19].
- **California Consumer Privacy Act / California Privacy Rights Act (CCPA/CPRA):** police exceptions, but corporate investigators must respect employees' data rights.

National Statutes

- **Computer Fraud and Abuse Act (CFAA, USA):** "without authorization" or "exceeding authorized access"; broad, debated, defines the offences investigated.
- **Computer Misuse Act (UK, 1990):** unauthorised access; access with intent; acts impairing a computer. Widely copied.

Section 4: Assessment I

Question

Which instrument lets an EU judicial authority order a provider in another Member State to freeze data?

- A. A European Investigation Order.
- B. An MLAT request.
- C. A European Preservation Order Certificate (EPOC-PR).
- D. A CLOUD Act warrant.



Section 4: Assessment - Answer I

Question

Which instrument lets an EU judicial authority order a provider in another Member State to freeze data?

- A. A European Investigation Order.
- B. An MLAT request.
- C. A European Preservation Order Certificate (EPOC-PR). (✓)
- D. A CLOUD Act warrant.

Explanation:

- Regulation (EU) 2023/1543 sends the order straight to the provider [10].



Conclusion: Key Takeaways I

- **Admissibility:** five requirements, each met with specific evidence.
- **Search authority:** warrant first; know the exceptions and the SCA disclosure tiers.
- **Chain of custody:** every handoff signed, sealed and dated.
- **Jurisdiction:** choose the instrument whose response time fits the case.

Next Step

Analysing filesystems to find digital evidence.

References I

- [1] Frye v. united states.
D.C. Circuit Court of Appeals Reports, 1923.
293 F. 1013.
- [2] Smith v. maryland.
U.S. Supreme Court Reports, 1979.
442 U.S. 735.
- [3] Daubert v. merrell dow pharmaceuticals, inc.
U.S. Supreme Court Reports, 1993.
509 U.S. 579.
- [4] Iso/iec 27037:2012 information technology – security techniques – guidelines for identification, collection, acquisition and preservation of digital evidence, 2012.
- [5] Carpenter v. united states.
U.S. Supreme Court, 2018.
585 U.S. 296 (2018); No. 16-402.



References II

- [6] Radley Balko.
The prosecution of julie amero.
Reason, 12 2008.
Accessed: 2026-08-16.
- [7] Eoghan Casey.
Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet.
Academic Press, San Diego, CA, 3rd edition, 2011.
- [8] Council of Europe.
Convention on cybercrime (budapest convention), 11 2001.
Opened for signature 23 November 2001.
- [9] Council of Europe.
Second additional protocol to the convention on cybercrime on enhanced co-operation and disclosure of electronic evidence, 5 2022.
Adopted 17 November 2021, opened for signature 12 May 2022.

References III

- [10] European Parliament and Council of the European Union.
Regulation (EU) 2023/1543 on European production orders and European preservation orders for electronic evidence in criminal proceedings.
Official Journal of the European Union L 191; adopted 12 July 2023, applicable from 18 August 2026, 7 2023.
Accessed: 2026-09-05.
- [11] Legal Information Institute.
Federal rules of evidence, rule 1001. definitions that apply to this article, 2023.
Accessed: 2026-08-16.
- [12] Legal Information Institute.
Federal rules of evidence, rule 1002. requirement of the original.
Cornell Law School, 2023.
- [13] Legal Information Institute.
Federal rules of evidence, rule 1003. admissibility of duplicates, 2023.
Accessed: 2026-08-16.

References IV

- [14] Legal Information Institute.
Federal rules of evidence, rule 401. test for relevant evidence.
Cornell Law School, 2023.
- [15] Legal Information Institute.
Federal rules of evidence, rule 801. definitions that apply to this article; exclusions from hearsay.
Cornell Law School, 2023.
- [16] Legal Information Institute.
Federal rules of evidence, rule 803. exceptions to the rule against hearsay.
Cornell Law School, 2023.
- [17] Legal Information Institute.
Federal rules of evidence, rule 901. authenticating or identifying evidence.
Cornell Law School, 2023.
- [18] Technical Working Group for the Examination of Digital Evidence.
Forensic examination of digital evidence: A guide for law enforcement.
Technical Report NCJ 199408, National Institute of Justice, U.S. Department of Justice, 4 2004.



References V

- [19] The European Parliament and the Council of the European Union.
Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation), 2016.
Official Journal of the European Union, L 119/1.
- [20] United Nations.
United nations convention against cybercrime, 12 2024.
Adopted by General Assembly resolution 79/243 of 24 December 2024; opened for signature in Hanoi, 25–26 October 2025.
- [21] U.S. Congress.
H.r.4943 - cloud act, 2018.
Public Law No: 115-141, Division V.
- [22] U.S. Department of Justice.
Ross ulbricht, a/k/a 'dread pirate roberts,' sentenced in manhattan federal court to life in prison.
Press Release, 5 2015.

Acronyms and Terminology I

Admissibility The legal requirement that evidence must meet before it can be presented and accepted in a court of law.

Authenticity The principle of proving that a piece of evidence is genuine, unaltered, and what it claims to be.

Best Evidence Rule A legal rule, now adapted for the digital age, that traditionally required the original version of a document or recording to be presented in court. A verified forensic image is often accepted as the original.

Budapest Convention on Cybercrime The first major international treaty designed to address computer crime by harmonizing laws between nations and promoting cooperation.

Business Records Exception An exception to the hearsay rule that allows records made during regular business activities (such as company emails or system logs) to be admitted as evidence.

CCPA / CPRA The California Consumer Privacy Act / California Privacy Rights Act; a California law giving consumers rights over their personal data held by businesses.

CFAA The Computer Fraud and Abuse Act; the primary federal anti-hacking law in the United States, which makes it illegal to access a computer without authorization.

Chain of Custody The chronological, documented log of everyone who has handled a piece of evidence, from collection to courtroom presentation, to prove its integrity.



Acronyms and Terminology II

CLOUD Act The Clarifying Lawful Overseas Use of Data Act; a U.S. law allowing authorities to compel U.S.-based tech companies to provide requested data, even if it is stored in another country.

Collision Resistance A property of a strong cryptographic hash function ensuring that it is practically impossible for two different pieces of data to produce the same hash value.

Computer-Generated Records Data created automatically by a computer system without direct human input, such as system logs. Courts often consider this type of record more reliable and not hearsay.

Computer-Stored Records Information created by a person using a computer, such as a word document or email. These are considered human statements and may be subject to the hearsay rule.

Computer Misuse Act The United Kingdom's primary law against computer crime, which defines offenses like unauthorized access and modification of data.

Consent Voluntary permission given by an individual for law enforcement to conduct a search, which removes the need for a warrant.

Daubert Standard A legal standard used in U.S. federal courts where the judge acts as a "gatekeeper" to ensure that scientific expert testimony and methods are both relevant and reliable.

Data Minimisation A privacy principle, central to GDPR, which states that only the personal data that is strictly necessary for a specific purpose should be collected and processed.



Acronyms and Terminology III

Declarant The legal term for a person who makes a statement, particularly one made outside of court that might be considered hearsay.

Digital Fingerprint Another term for a hash value; a unique string of characters generated by a hash function to identify a piece of data.

EMS Evidence Management Systems; software used to digitally track and manage the chain of custody for evidence, helping to reduce human error.

Exigent Circumstances An emergency situation that allows law enforcement to conduct a search without a warrant, typically to prevent physical harm or the imminent destruction of evidence.

Forensic Image An exact, bit-for-bit copy of a digital storage device (like a hard drive), which preserves the original data, including deleted files and unused space.

Frye Standard An older legal standard for admitting scientific evidence, which requires that the method used be "generally accepted" as reliable by the relevant scientific community.

GDPR General Data Protection Regulation; a comprehensive European Union law that sets strict rules for protecting personal data and privacy.

Hash Function A mathematical algorithm that takes data of any size and produces a short, fixed-size output string (the hash value). It is used to verify data integrity.



Acronyms and Terminology IV

Hash Value The unique, fixed-size string of text produced by a hash function. If the hash values of two files match, the files are identical.

Hearsay A statement made outside of court that is offered as evidence to prove the truth of the matter asserted. It is generally not admissible in court unless an exception applies.

ISO/IEC 27037:2012 An international standard providing formal guidelines for the identification, collection, acquisition, and preservation of digital evidence to ensure a consistent and reliable process.

MD5 A once-common hashing algorithm that is now considered cryptographically weak but is sometimes still used for simple file integrity checks.

MLAT Mutual Legal Assistance Treaty; a formal agreement between two or more countries to provide help in criminal investigations, such as by gathering evidence on each other's behalf.

Particularity Requirement A Fourth Amendment rule requiring that a search warrant must specifically describe the location to be searched and the items to be seized.

Plain View Doctrine A legal rule that allows a police officer to seize evidence and contraband found in plain sight during a lawful observation.

Probable Cause A standard of proof required to obtain a search warrant, consisting of reasonable grounds to believe that a crime has been committed and that evidence of the crime will be found at the location to be searched.



Acronyms and Terminology V

- Purpose Limitation** A privacy principle, central to GDPR, stating that data collected for one specific purpose should not be used for another unrelated purpose without legal justification.
- Relevance** The legal principle that evidence must have a tendency to make a fact that is important to the case more or less probable.
- SCA** Stored Communications Act; a U.S. law that regulates how the government can obtain stored user data (like emails or files) from third-party service providers.
- SHA** Secure Hash Algorithm; a family of cryptographic hash functions (e.g., SHA-256) considered to be strong and secure for verifying evidence integrity.
- Subpoena** A legal command ordering someone to produce evidence or provide testimony. Under the SCA, it can be used to obtain basic subscriber information.
- Tamper-Evident Evidence Bag** A specially designed bag for storing evidence that will show visible signs if it has been opened or compromised, helping to ensure the integrity of the item inside.
- Third-Party Doctrine** A U.S. legal theory that a person has a reduced expectation of privacy for information they voluntarily share with a third party, such as an internet service provider or bank.
- Trier of Fact** The person or group who determines the facts in a legal case; typically a judge or a jury.
- Warrant** A legal document, issued by a judge, that authorizes law enforcement to perform a specific act, such as a search or an arrest.

Thank You!

