

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.
- Evidence collected or handled wrongly can be refused by a court.
- Inadmissible evidence cannot support a finding, however strong.



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



100%

1. *Journal of Management Studies*, 1997, 34, 103-117.





Case Study: State of Connecticut v. Julie Amero I

State of Connecticut v. Julie Amero

- A real example of failed authentication and context analysis.
- Amero, a substitute teacher, convicted January 2007 on four counts of risk of injury to a minor.
- Cause: pornographic pop-up ads appeared on her classroom computer.
- The first police investigation was not detailed.
- Independent experts later showed spyware caused the pop-ups.
- Amero was trying to close the windows, not open them on purpose.
- June 2007: conviction vacated, new trial granted on that analysis.
- The state dropped the felony charges.
- November 2008: plea to one disorderly conduct charge, \$100 fine, teaching licence surrendered.
- Lesson: poor forensic analysis produces wrong conclusions, and undoing them takes enormous work [6].



Hearsay and Digital Statements I

- Hearsay is a major challenge for digital evidence, but one that can be overcome.

Definition: Hearsay

- A statement made outside of court, presented to prove the statement is true [15].
- Usually not allowed: the *declarant* is not in court and cannot be questioned.

Digital Evidence as Statements

- An email, a text message, or a document written by a person: clear examples.
- Computer-generated data, like a server log entry, can be seen as a statement by the system.



The Business Records Exception I

Definition: Business Records Exception

- The most important hearsay exception for digital forensics.
- Allows records from a business to be used as evidence.
- Made at or near the time of the event, by someone who knew about it.
- Kept as part of a regular business activity.
- Created as a normal practice of that business [16].
- Covers Internet Service Provider (ISP) connection logs, financial transaction records, system event logs, company emails.



The Business Records Exception II

Two Types of Digital Record

- **Computer-Stored Records:** created by a person using a computer.
- Word processing documents, emails, spreadsheets.
- Hearsay if offered to prove the truth of what they say: human statements on a machine.
- **Computer-Generated Records:** created automatically, without direct human input.
- Login attempt logs, web server access logs, file system timestamps.
- Usually not hearsay: a machine, not a person, created them.
- Considered more reliable: produced automatically as part of a normal process [7].



Cryptographic Hash Functions I

- Proving authenticity is extremely important; hashing is the main method.

Definition: Hash Function

- A mathematical algorithm: any amount of data in, a short fixed-size string out.
- The output is the *hash value* or *digital fingerprint*.
- Common algorithms: Message-Digest Algorithm 5 (MD5) and the Secure Hash Algorithm (SHA) family, especially SHA-256.
- MD5 is now weak for security, still sometimes used for integrity checks.

Key Properties

- 1 Almost impossible to find two inputs with the same hash: *collision resistance*.
- 2 Changing a single bit produces a completely different hash.
- 3 The original data cannot be recovered from its hash.



Cryptographic Hash Functions II

The Verification Process

- Hash the original evidence at collection time.
- Recompute the hash after copying or analysing.
- Matching hashes are strong proof the evidence is unchanged.



Practical Demo: File Hashing in Linux Bash I

- Hashing and verifying data is simple with modern tools.
- Step 1: hash the acquired image at once; that hash is the official record.
- The value is recorded in the chain of custody documents.
- Step 2: copy, then recompute on the working copy; the two must match exactly.

```

1  # Step 1: acquire the disk image and immediately hash it.
2  $ sha256sum /evidence/original_file.dd
3  A1B2C3D4E5F6...[a long hexadecimal string]...7890 /evidence/original_file.dd
4  # Recorded in the chain of custody documents.
5
6  # Step 2: make a working copy and later verify it.
7  $ cp /evidence/original_file.dd /working_copy/original_file.dd
8  $ sha256sum /working_copy/original_file.dd
9  A1B2C3D4E5F6...[a long hexadecimal string]...7890 /working_copy/original_file.dd
10 # Identical hashes prove the working copy is an exact duplicate.

```



Frye and Daubert I

- Forensic science must follow standards so its methods are reliable.
- In the United States, two standards have controlled scientific testimony.

The Frye Standard

- From *Frye v. United States* (1923): the "general acceptance" test.
- A method is usable only if experts in the field generally accept it as reliable [1].
- Relies on the agreement of the scientific community.



Frye and Daubert II

The Daubert Standard

- From *Daubert v. Merrell Dow Pharmaceuticals, Inc.* (1993).
- Used in U.S. federal courts and many state courts; more modern and flexible.
- The judge decides whether expert testimony is relevant and reliable.
- Factor: has the method or theory been tested?
- Factor: peer reviewed and published?
- Factor: known or possible rate of error.
- Factor: standards controlling how the method is used.
- Factor: wide acceptance in the relevant community (Frye as one factor) [3].



Daubert in Digital Forensics I

- An investigator must be able to defend the tools and methods used.
- A statement that the tool found the evidence is not sufficient.
- Explain how the tool works and discuss its known errors.
- Show it has been tested and confirmed.
- Prove the forensic community accepts the methods.
- Hence testing and validating forensic software and hardware are core lab jobs.



Figure Analysis: Requirements for Admitting Digital Evidence I

- Relevance, authenticity, hearsay, best evidence, method reliability: five separate questions.
- Evidence that fails any one of them is excluded.
- The investigator answers each with specific material.
- A custody log and hash for one, the business-records exception for another.
- A defensible method for the last.



Hands-On: Hash Verification of a Working Copy II

Expected Outcome

- Identical hashes for original and untouched copy.
- A completely different hash after the one-byte change.

Common Pitfalls

- Hashing the copy only, never the original at collection time.
- Using MD5 where a court may question its collision resistance.



Section 1: Assessment (1/3) I

Question 1

Under the Federal Rules, when is a forensic image admissible in place of the original device?

- A. Never; the Best Evidence Rule always requires the physical device.
- B. To the same extent as an original, unless its authenticity is genuinely disputed.
- C. Only when the original device has been destroyed.
- D. Only when the defence agrees in writing.



Section 1: Assessment (1/3) - Answer I

Question 1

Under the Federal Rules, when is a forensic image admissible in place of the original device?

- A. Never; the Best Evidence Rule always requires the physical device.
- B. To the same extent as an original, unless its authenticity is genuinely disputed. (✓)
- C. Only when the original device has been destroyed.
- D. Only when the defence agrees in writing.

Explanation:

- Rule 1001(d) defines an ESI original; Rule 1003 admits duplicates [12, 11, 13].
- The investigator still proves the copy is unchanged, normally by hashing.



Section 1: Assessment (2/3) I

Question 2

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 (2/3) - Answer I

Question 2

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].
- Computer-stored records (emails, documents) remain human statements and are hearsay.



Section 1: Assessment (3/3) I

Question 3

Which Daubert factor is the Frye test equivalent to?

- A. Whether the method has a known error rate.
- B. Whether the method has been tested.
- C. Whether the method is generally accepted in the relevant scientific community.
- D. Whether standards control how the method is applied.



Section 1: Assessment (3/3) - Answer I

Question 3

Which Daubert factor is the Frye test equivalent to?

- A. Whether the method has a known error rate.
- B. Whether the method has been tested.
- C. Whether the method is generally accepted in the relevant scientific community. (✓)
- D. Whether standards control how the method is applied.

Explanation:

- Frye is the "general acceptance" test [1].
- Daubert keeps it as one factor among several [3].



Outline

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





Search Warrants I

Definition: Warrant

- A legal paper signed by a judge.
- Permits police to search a specific person, place or car for evidence of a crime.
- The main tool for a legal search in a criminal investigation.

Probable Cause

- Facts making a reasonable person believe a crime has happened.
- And that evidence of it will probably be found in the place to be searched.



Search Warrants II

Particularity Requirement

- The warrant must "particularly describ[e] the place to be searched, and the persons or things to be seized."
- Hard for digital evidence: criminal data is mixed with unrelated personal data.
- Cannot be a "general warrant" to search for anything.
- Must still be broad enough to reach hidden, encrypted or disguised evidence.
- Courts often permit seizing the whole device; the data search happens later in a lab.

Scope of the Search

- Limited to what the warrant allows.
- A warrant for financial documents covers spreadsheets, not the rest of the drive.
- Evidence of another crime in plain view can still be taken.



The Third-Party Doctrine I

- Much evidence is held by third parties: ISPs, email providers, cloud storage.

Definition: Third-Party Doctrine

- U.S. rule: less privacy right in information willingly given to companies [2].

Carpenter v. United States (2018)

- Acquiring historical cell-site location information from a carrier is a Fourth Amendment search.
- Generally requires a warrant: the records reveal a comprehensive account of movements.
- Third-party possession did not defeat the privacy interest [5].
- Holding confined to historical cell-site records.
- Real-time tracking and tower dumps left unresolved.
- Treat the doctrine's boundaries as unsettled, not fixed.



The Stored Communications Act I

Definition: Stored Communications Act (SCA)

- U.S. law controlling how police force companies to hand over user data.
- A system of legal requests at different levels.
- **Subpoena:** basic user information: name, address, payment records.
- **Court Order:** non-content records: email to/from and timestamps, IP address logs.
- **Search Warrant:** content: email bodies, cloud files, private messages stored 180 days or less.



- Ulbricht created the Silk Road dark-web marketplace.
- Key evidence sat on servers owned by a third-party company in Iceland.
- U.S. investigators used a Mutual Legal Assistance Treaty (MLAT) request (see Jurisdictional Frameworks).
- Icelandic police made a forensic image of the server and gave it to the Federal Bureau of Investigation (FBI).
- Forcing a foreign third-party provider to produce data was key to the conviction [22].



Hands-On: Picking the Right SCA Instrument I

Objective

- Match each data request in a scenario to the legal instrument it needs.

Prerequisites

- The SCA disclosure tiers and the *Carpenter* holding from this section.

Steps

- 1 List the data wanted from a provider: subscriber name, login IP log, email bodies, historical cell-site records.
- 2 For each item, name the lowest tier that reaches it.
- 3 Mark the items *Carpenter* moved to the warrant tier.
- 4 Note which items remain unsettled (real-time tracking, tower dumps).
- 5 Write one sentence of probable cause the warrant items would need.



Expected Outcome

- Subpoena, court order and warrant each assigned correctly.
- Historical cell-site location placed in the warrant tier.

- Treating a court order as sufficient for message content.
- Assuming the third-party doctrine is settled after *Carpenter*.



Section 2: Assessment (1/3) I

Question 1

What does the particularity requirement demand of a digital search warrant?

- A. That it name every file to be seized in advance.
- B. That it describe the place and the things to be seized, without becoming a general warrant.
- C. That the search of the device happen at the scene, never in a lab.
- D. That it exclude all personal data from the seizure.



Section 2: Assessment (1/3) - Answer I

Question 1

What does the particularity requirement demand of a digital search warrant?

- A. That it name every file to be seized in advance.
- B. That it describe the place and the things to be seized, without becoming a general warrant. (✓)
- C. That the search of the device happen at the scene, never in a lab.
- D. That it exclude all personal data from the seizure.

Explanation:

- Specific, yet broad enough to reach hidden or encrypted evidence.
- Courts often allow seizing the whole device for later lab examination.



Section 2: Assessment (2/3) I

Question 2

What did *Carpenter v. United States* decide?

- A. All third-party records now require a warrant.
- B. Historical cell-site location records generally require a warrant.
- C. Real-time tracking and tower dumps require a warrant.
- D. The third-party doctrine was overruled entirely.



Section 2: Assessment (2/3) - Answer I

Question 2

What did *Carpenter v. United States* decide?

- A. All third-party records now require a warrant.
- B. Historical cell-site location records generally require a warrant. (✓)
- C. Real-time tracking and tower dumps require a warrant.
- D. The third-party doctrine was overruled entirely.

Explanation:

- The holding was confined to historical cell-site records [5].
- Real-time tracking and tower dumps were left unresolved.



Section 2: Assessment (3/3) I

Question 3

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 (3/3) - Answer I

Question 3

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 reach non-content records.
- Only a warrant reaches content such as email bodies and cloud files.



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



Why the Chain of Custody Matters I

- Establishes that evidence is trustworthy and usable in court.
- A mistake makes a court doubt authenticity and refuse admission.
- The technical findings then cannot be used, however strong.

ISO/IEC 27037:2012

- From the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC).
- Official rules for identifying, collecting, acquiring and protecting digital evidence.
- Standardises many of these processes [4].



What the Log Must Contain I

- The log proves two things: same evidence as collected, and unchanged.
- Every move or change of hands gets an entry with:

Required Fields

- Case number and a unique evidence item number.
- Detailed description: manufacturer, model, serial number.
- Name and signature of every person who handles the evidence.
- Date and time of collection or transfer.
- Reason for the transfer: seizure location to lab, storage to workbench, to courtroom.





- _____



Chain-of-Custody Transfers from Seizure to Storage I

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.





Hands-On: Auditing a Custody Log I

Objective

- Find every defect in a sample chain of custody log before accepting the item.

Prerequisites

- A sample log with five transfers, prepared with three planted defects.
- The required-fields list and the three common failures.

Steps

- 1 Check that every transfer carries a releasing and a receiving signature.
- 2 Check that no time gap exists between one receipt and the next release.
- 3 Check each entry for date, time, reason and item description.
- 4 Check the seal note at lab intake against the bagging entry.
- 5 Write an intake decision: accept, or return with the defects listed.



Hands-On: Auditing a Custody Log II

Expected Outcome

- All three planted defects found and classified as broken chain, improper sealing or incomplete documentation.

Common Pitfalls

- Accepting the item first and auditing the log later.



Section 3: Assessment (1/3) I

Question 1

Which international standard sets out rules for identifying, collecting, acquiring and preserving digital evidence?

- A. ISO/IEC 27001.
- B. ISO/IEC 27037:2012.
- C. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53.
- D. Request for Comments (RFC) 3227 only.



Section 3: Assessment (1/3) - Answer I

Question 1

Which international standard sets out rules for identifying, collecting, acquiring and preserving digital evidence?

- A. ISO/IEC 27001.
- B. ISO/IEC 27037:2012. (✓)
- C. NIST SP 800-53.
- D. RFC 3227 only.

Explanation:

- ISO/IEC 27037 standardises evidence handling processes [4].



Section 3: Assessment (2/3) I

Question 2

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 (2/3) - Answer I

Question 2

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:

- Secure storage itself is fine; the defect is any period with nobody signed for the item.
- Intake and every removal must be logged with a signature.



Section 3: Assessment (3/3) I

Question 3

What is the first thing an analyst does when handed an evidence bag?

- A. Open it and begin imaging immediately.
- B. Check the packaging and verify the custody log is complete and correct.
- C. Photograph the analyst's workbench.
- D. Re-assign a new item number.



Section 3: Assessment (3/3) - Answer 1

Question 3

What is the first thing an analyst does when handed an evidence bag?

- A. Open it and begin imaging immediately.
- B. Check the packaging and verify the custody log is complete and correct. (✓)
- C. Photograph the analyst's workbench.
- D. Re-assign a new item number.

Explanation:

- Never accept evidence unchecked; an EMS can enforce this [18].



- ## 4 Jurisdictional Frameworks



The Jurisdiction Problem I

- Chapter 1 set out the problem: an attack crossing three legal systems in a second.
- Investigators face a mix of international agreements, regional rules and national laws.
- Legal at home may be illegal if it means accessing data stored abroad.



The Budapest Convention on Cybercrime I

Council of Europe Convention on Cybercrime

- The first and most important international agreement on computer crime.
- Approved by dozens of countries: the United States, Japan, most of Europe.

Three Main Goals

- 1 Harmonise cybercrime laws: illegal access, data interference, computer-related fraud.
- 2 Give countries investigative powers at home, e.g. ordering a company to preserve data.
- 3 Fast cooperation, including a "24/7 Network" of contacts for urgent requests [8].

Second Additional Protocol

- Opened for signature May 2022.
- Direct routes to subscriber information and traffic data from foreign providers.
- Quick preservation of evidence without waiting for treaty channels [9].



The UN Convention and MLATs I

United Nations Convention against Cybercrime

- Adopted by the General Assembly December 2024.
- Opened for signature in Hanoi, October 2025; more than seventy states signed.
- First cybercrime treaty of global rather than regional reach.
- Enters into force ninety days after the fortieth ratification [20].

Mutual Legal Assistance Treaties (MLATs)

- A formal government-to-government request under a treaty.
- The default route when no faster instrument applies.
- Also the slowest: around ten months on average.
- The newer instruments exist largely to route around it.



The U.S. CLOUD Act I

Clarifying Lawful Overseas Use of Data (CLOUD) Act, 2018

- Made important changes to the Stored Communications Act.
- U.S. police can compel U.S.-based technology companies to produce data stored abroad.
- Creates executive agreements with trusted foreign countries.
- Each side's police request data directly from the other's providers.
- Avoids the slow MLAT process [21].



The EU e-Evidence Regulation I

Regulation (EU) 2023/1543

- Adopted July 2023, applies from 18 August 2026 [10].
- Does for the EU roughly what CLOUD Act agreements do for the U.S.
- A judicial authority in one Member State orders a provider in another directly.
- The request does not pass through the second country's government.
- **European Production Order Certificate (EPOC):** provider must hand over data.
- **European Preservation Order Certificate (EPOC-PR):** provider must freeze data.



The EU e-Evidence Regulation II

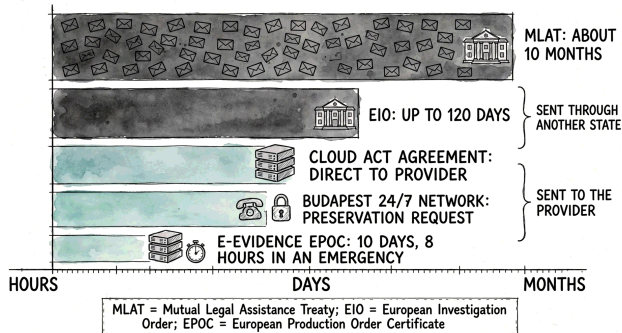
Production Deadlines

- Production within ten days as a rule.
- Within eight hours in an emergency threatening life or physical safety.
- Compare: a European Investigation Order (EIO) up to 120 days; MLAT ten months.
- Reaches non-EU providers offering services to users inside the Union.
- Planning turns on which provider holds the data and whether the order conditions are met, not on which government to approach.



- MLAT and European Investigation Order route through another state: counted in months.
- CLOUD Act agreements, the Budapest 24/7 network and e-Evidence orders go directly to the provider.
- Their deadlines are therefore set in days, or in hours in an emergency.





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

GDPR and CCPA/CPRA I

- Strong data privacy laws can limit an investigation.

General Data Protection Regulation (GDPR, Europe)

- EU law on data protection and privacy across the EU and the European Economic Area (EEA).
- Strict rules for handling "personal data".
- **Data Minimisation:** collect only data adequate, relevant and needed for a specified purpose.
- **Purpose Limitation:** data for one purpose is not reused for an unrelated one.
- Imaging a whole multi-user server for one employee's files may breach GDPR.
- Collection must be reasonable for the investigation's goal [19].



GDPR and CCPA/CPRA II

California Consumer Privacy Act / California Privacy Rights Act (CCPA/CPRA)

- Strong consumer rights: know what is collected, request deletion.
- Large exceptions for police activity and legal compliance.
- Corporate internal investigators must still be careful.
- Employees may hold rights over personal data on company systems.
- Incident response must not violate those rights.



CFAA and the Computer Misuse Act I

- Many nations' basic computer crime laws have been copied elsewhere.

Computer Fraud and Abuse Act (CFAA, USA)

- The main U.S. anti-hacking law.
- Forbids "accessing a computer without authorization" or "exceeding authorized access".
- Very broad wording; much debate.
- Used for serious hacking for money and for breaking a website's rules.
- Defines the basic crimes investigators are asked to investigate.



CFAA and the Computer Misuse Act II

Computer Misuse Act (UK, 1990)

- One of the first and most complete computer crime laws.
- 1 Unauthorised access to computer material: digital trespass.
- 2 Unauthorised access with intent to commit other crimes.
- 3 Unauthorised acts intending or reckless as to harming a computer: malware, denial of service.
- Its clear structure and early date made it influential worldwide.



Hands-On: Choosing a Cross-Border Instrument I

Objective

- Pick the fastest lawful route to data held by a provider in another country.

Prerequisites

- The instrument list from this section and the response-times figure.

Steps

- 1 Take a scenario: an EU investigator needs email content from a U.S. provider serving EU users.
- 2 List every applicable instrument: MLAT, EIO, CLOUD Act agreement, e-Evidence EPOC, 24/7 network.
- 3 Write the expected response time for each.
- 4 Decide whether an EPOC-PR should go first to freeze the data.
- 5 Note the GDPR minimisation limit on what is requested.

Section 4: Assessment (1/3) I

Question 1

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 (1/3) - Answer I

Question 1

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].
- An EPOC then demands production within ten days, or eight hours in an emergency.



Section 4: Assessment (2/3) I

Question 2

Why is an MLAT request typically the slowest route?

- A. It must be translated into every EU language.
- B. It is a government-to-government request routed through the foreign state.
- C. It requires the fortieth ratification of the UN convention.
- D. It can only be filed by the 24/7 Network.



Section 4: Assessment (2/3) - Answer I

Question 2

Why is an MLAT request typically the slowest route?

- A. It must be translated into every EU language.
- B. It is a government-to-government request routed through the foreign state. (✓)
- C. It requires the fortieth ratification of the UN convention.
- D. It can only be filed by the 24/7 Network.

Explanation:

- Around ten months on average; the direct-to-provider instruments exist to route around it.



Section 4: Assessment (3/3) I

Question 3

Imaging a whole shared server to investigate one employee most directly risks breaching which GDPR principle?

- A. Data minimisation.
- B. The right to be forgotten.
- C. Breach notification.
- D. Data portability.



Section 4: Assessment (3/3) - Answer I

Question 3

Imaging a whole shared server to investigate one employee most directly risks breaching which GDPR principle?

- A. Data minimisation. (✓)
- B. The right to be forgotten.
- C. Breach notification.
- D. Data portability.

Explanation:

- Collect only what is adequate, relevant and needed for the purpose [19].



- 

- 

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.

أكاديمية جوعان بن جاسم للدراسات الدفاعية
Jasssem Bin Jo'ayan Al-Jasssem Al-Difa'iyah Al-Darasaat Al-Difa'iyah

- 

- 

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 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.



