Session 11 – Chapter 19 (pg. 919-945)

2025 CISSP Mentor Program

CHAPTER 19

Evan Francen

FRSecure

2025 CISSP MENTOR PROGRAM

AGENDA – SESSION 11

Chapter 19 (from the book)

Investigations and Ethics

- Investigations
- Major Categories of Computer Crime
- Ethics

A fairly short chapter!


You know what time it is, right?!
It’s time for a dad joke!


INTEGRITY FIRST
Why did the ethical investigator refuse to join the poker game?
Because he couldn’t stand bluffing—it violated his code of conduct.

CHAPTER 19

Investigations

Think of it like digital detective work—you're building a case, not just fixing a system.

The structured processes used to identify, collect, analyze, and document evidence related to security incidents, policy violations, or legal matters.

Key Goals:

- Determine what happened, how, who was involved, and what the impact was.
- Support disciplinary actions, legal proceedings, or policy adjustments.
- Maintain evidence integrity through chain of custody and proper handling.

CISSP Relevance: CISSP professionals must understand how to support and protect investigations—ensuring technical actions align with legal standards, due process, and organizational policies.

CHAPTER 19

Investigations

Investigation Types

Think of it as an internal affairs case—you're not building for court, but you still need your facts tight.

Administrative Investigations are internal inquiries conducted by an organization to determine if policies, procedures, or internal rules have been violated.

Key Characteristics:

- Initiated by HR, legal, compliance, or management.
- Often involve employee misconduct, policy violations, or internal misuse of systems.
- May lead to disciplinary action, retraining, or policy updates.
- Typically, lower stakes than legal cases, but still require documented evidence and fairness.

CISSP Relevance: Security professionals must support fact-finding while protecting confidentiality and adhering to due process and internal protocols.

CHAPTER 19

Investigations

Investigation Types

Think of it as an internal affairs case—you're not building for court, but you still need your facts tight.

Administrative Investigations are internal inquiries conducted by an organization

Root Cause Analysis (RCA) is the systematic process of identifying the underlying reason why an incident or failure occurred—not just the symptoms, but the true origin.

Key Steps:

1. Define the problem clearly.
2. Collect evidence and data.
3. Identify contributing factors.
4. Determine the root cause(s) using methods like the 5 Whys or fishbone diagrams.
5. Develop corrective actions to prevent recurrence.

CISSP Relevance: RCA is critical after a security incident, failure, or breach—not just to fix what's broken, but to stop it from happening again. It feeds into lessons learned, risk mitigation, and improved security controls.

CHAPTER 19

Investigations

Investigation Types

Think of it like playing defense in a court match—one wrong move with the evidence, and the case could fall apart.

Criminal investigations involve the collection and analysis of evidence related to potential violations of criminal law, such as hacking, data theft, fraud, or sabotage.

Key Characteristics:

- Led by law enforcement or authorized government agencies.
- Requires strict chain of custody and adherence to legal standards (e.g., search warrants, probable cause).
- May result in criminal charges, arrests, and prosecution.
- Evidence must be forensically sound and admissible in court.

CISSP Relevance: CISSPs may be responsible for preserving digital evidence, coordinating with law enforcement, and ensuring that incident handling doesn't compromise a legal case.

CHAPTER 18

Investiga

Investigati

Criminal inve
potential viol

Key Charac
- Led by law
- Requires s
  search wa
- May result
- Evidence r

Think of it like playing defense in a court match—one wrong move with the evidence, and the case could fall

Proof Beyond a Reasonable Doubt

Proof beyond a reasonable doubt is the highest standard of evidence used in criminal cases. It means the evidence must be so convincing that there's no reasonable doubt left in the mind of a rational person about the defendant's guilt.

Key Points:
- Applies only to criminal proceedings.
- Requires clear, consistent, and credible evidence.
- Protects against wrongful conviction by favoring innocence unless proven guilty.

CISSP Relevance:
When supporting a criminal investigation, CISSPs must ensure evidence integrity and proper handling, as their data may be used to meet this strict legal threshold.

enforcement, and ensuring that incident handling doesn't compromise a legal case.

CHAPTER 18

Investiga

Think of it like playing defense in a court match—one wrong move with the evidence, and the case could fall

Proof Beyond a Reasonable Doubt

vidence used in
hat there's no
he defendant's guilt.

e unless proven

evidence integrity
trict legal threshold.

handling

Color of Law

Color of Law refers to actions taken by government officials (e.g., police, investigators) that appear to be within their legal authority but may violate someone's rights if misused.

Key Points:

- Applies to searches, seizures, investigations, or enforcement actions.
- If someone acts under the color of law, they're using their official position.
- Abuse of this power can lead to evidence being thrown out or civil rights violations.

CISSP Relevance:

Security professionals must understand the limits of law enforcement authority, especially when collaborating during investigations—overstepping or cooperating improperly could taint evidence or trigger legal backlash.

CHAPTER 19

Investigations

Investigation Types

Think of it like playing defense in a court match—one wrong move with the evidence, and the case could fall

As a CISSP, you're more likely to support civil investigations than criminal ones—especially around data breaches, misuse of company resources, or violations of acceptable use policies.

Civil Investigations involve the collection of evidence for non-criminal legal disputes, such as breach of contract, intellectual property theft, privacy violations, or workplace issues.

Key Characteristics:

- Typically initiated by private parties or organizations, not the government.
- Standard of proof is "preponderance of the evidence"—more likely than not.
- May lead to financial penalties, injunctions, or corrective actions—not jail time.
- Often involve forensic evidence, interviews, and documentation.

CISSP Relevance: Security professionals may support these investigations by gathering logs, emails, access records, or system activity, ensuring evidence integrity and privacy compliance.

CHAPTER 19

Investigations

Investigation Types

Think of it like a digital IRS audit—they're not accusing you of a crime (yet), but they're here to see if you've followed the rules.

Regulatory Investigations are conducted by government agencies or regulatory bodies to ensure that organizations are complying with laws, industry regulations, and standards.

Key Characteristics:

- Triggered by audits, complaints, data breaches, or routine inspections.
- Conducted by entities like FTC, SEC, HIPAA enforcers, GDPR regulators, PCI DSS councils, etc.
- Focus on data protection, financial reporting, privacy, safety, and consumer protection.
- Can result in fines, sanctions, corrective action plans, or license revocation.

CISSP Relevance: Security professionals play a key role by providing evidence of compliance, supporting audits, and responding to regulator demands—often under tight timelines and legal scrutiny.

CHAPTER 19

Investigations

Investigation Types

Think of it like the “user manual” for responsible security—follow the standard, and you’ve got a strong defense when things go sideways.

Industry Standards are widely accepted best practices, frameworks, and guidelines that organizations use to ensure security, compliance, and operational consistency—even if they’re **not legally binding**.

Key Characteristics:

- Often created by standards bodies like ISO, NIST, IEEE, or sector-specific groups (e.g., PCI DSS for payment data).
- Used to benchmark security programs, drive audits, and reduce liability.
- May become mandatory if incorporated into contracts, regulations, or compliance frameworks.

CISSP Relevance: CISSPs must understand and apply relevant standards to design secure environments, guide investigations, and demonstrate due diligence and best practice alignment.

CHAPTER 19

Investigations

Investigation Types

Think of it like a digital evidence hunt—if it exists, can be found, and is relevant, it can end up in court.

Electronic Discovery (eDiscovery) is the process of identifying, collecting, preserving, and producing electronically stored information (ESI) for use in legal or regulatory proceedings.

Key Characteristics:

- Includes emails, documents, databases, logs, metadata, chats, backups, and more.
- Must follow strict protocols to maintain data integrity, chain of custody, and admissibility in court.
- Often involves legal teams, IT/security, and third-party eDiscovery platforms.

CISSP Relevance: CISSPs support eDiscovery by ensuring systems are configured to log and retain data appropriately, and that data can be searched, exported, and handed over securely and legally.

Think of it like a digital evidence hunt—if it exists, can be found, and is relevant, it can end up in court.

Electronic Discovery Reference Model (EDRM)

The Electronic Discovery Reference Model (EDRM) is a framework that outlines the stages of the eDiscovery process, from initial information management to the presentation of evidence in legal proceedings.

EDRM Phases:

1. Information Governance – Proactively manage data to reduce risk.
2. Identification – Locate potentially relevant data.
3. Preservation – Protect data from alteration or deletion.
4. Collection – Gather data in a legally sound manner.
5. Processing – Reduce volume, convert formats, and filter.
6. Review – Examine data for relevance and privilege.
7. Analysis – Interpret patterns, facts, and content.
8. Production – Deliver data in usable, legal formats.
9. Presentation – Share findings in court or legal settings.

eDiscovery can be very expensive—often shockingly so, depending on the size and complexity of the case.

Typical Cost Range

- Small case: $10,000–$100,000
- Mid-size investigation: $100,000–$500,000
- Large enterprise or regulatory case: $1M+

CISSP Relevance:

Understanding the EDRM helps CISSPs support secure, defensible data handling during investigations and litigation—ensuring compliance, integrity, and admissibility.

Think of it like a digital evidence hunt—if it exists, can be

Investigation Type	Initiated By	Purpose	Standard of Proof	Outcomes	CISSP Role
Administrative	Organization (HR, Legal)	Address internal policy violations	Internal policies & fairness	Disciplinary actions, training	Support internal review, preserve internal evidence
Criminal	Law enforcement	Prosecute violations of criminal law	**Beyond a reasonable doubt**	Arrests, fines, incarceration	Ensure forensic integrity, maintain chain of custody
Civil	Private party (individual/org)	Resolve non-criminal legal disputes	**Preponderance of the evidence**	Financial damages, injunctions	Provide relevant logs, access records, documentation
Regulatory	Government agency	Enforce compliance with laws/regulations	Compliance with laws/regulations	Fines, sanctions, corrective actions	Respond to audits, provide secure evidence trail
Industry Standards	Industry bodies, orgs	Validate adherence to best practices	Not legally binding (unless contracted)	Certification, audit outcomes	Align systems to frameworks, assist in assessments
Electronic Discovery	Legal teams / courts	Collect digital evidence for legal use	Must ensure integrity & relevance	Used in any legal case	Preserve, collect, and produce ESI securely

CHAPTER 19

Investigations

Evidence

Think of evidence as the building blocks of your investigation—if it's weak, missing, or mishandled, the entire case can collapse.

Evidence is any information, data, or material that is collected, preserved, and presented to support findings in an investigation—whether it's criminal, civil, regulatory, or administrative.

Types of Evidence:

- **Digital/Logical**: Logs, emails, file metadata, access records.
- **Physical**: Devices, printed documents, hardware.
- **Testimonial**: Statements from witnesses or involved parties.
- **Demonstrative**: Charts, timelines, diagrams explaining evidence.

CISSP Relevance: CISSPs are often responsible for identifying, collecting, securing, and preserving digital evidence in a way that ensures its integrity, admissibility, and chain of custody.

CHAPTER 19

Investigations

Evidence

Think of admissible evidence as your “court-ready” proof—if it’s mishandled or irrelevant, it might get thrown out before anyone sees it.

Admissible Evidence is evidence that is legally accepted by a court or tribunal as valid and can be used to support a case.

Key Requirements:

- **Relevant**: Must relate directly to the case or issue.
- **Reliable**: Collected using proper methods and tools.
- **Legally obtained**: Not gathered through unlawful or unethical means.
- **Authentic**: Proven to be what it claims to be (often via chain of custody).

CISSP Relevance: Security professionals must ensure digital evidence is gathered and preserved in a way that protects its admissibility, especially in criminal or civil investigations.

Scenario: Insider Data Theft

Background: An employee at a financial services company is suspected of stealing sensitive client data and sending it to a competitor before resigning.

Investigation Actions:

1. HR flags suspicious behavior.
2. The security team reviews SIEM logs, showing:
   - The employee accessed and exported client data after hours.
   - A personal email address was used to send encrypted attachments.
3. Email archives, access logs, and endpoint DLP alerts are collected using forensic tools.
4. All evidence is preserved with proper hashing and chain of custody documentation.
5. The data is reviewed, confirmed to be authentic, and turned over to legal counsel.

Why This Evidence is Admissible:

- **Relevance**: Directly shows unauthorized access and data exfiltration.
- **Reliability**: Logs and files were collected using verified forensic tools.
- **Legal Collection**: Done under internal monitoring policies and acceptable use agreements.
- **Integrity Maintained**: Chain of custody was documented from acquisition to delivery.

2025 CISSP MENTOR PROGRAM

CHAPTER 19

Investigations

Types of Evidence

CHAPTER 19

Investigations

Types of Evidence

Think of it as the “hold-it-in-your-hands” kind of proof—the stuff you could plop on a table in court.

Real Evidence (also called physical evidence or object evidence) is any tangible, physical object directly involved in the case and can be presented in court to prove or disprove a fact.

Examples:

- A laptop used in a cybercrime.
- A USB drive containing stolen data.
- Printed documents, hard drives, or network hardware.

CISSP Relevance: Security professionals may be responsible for identifying, preserving, and securing physical devices that serve as real evidence—ensuring proper handling and documentation to maintain admissibility.

Conclusive Evidence

Conclusive Evidence is undeniable proof that establishes a fact with such certainty that it cannot be reasonably disputed.

Key Characteristics:

- Overrides other types of evidence—no additional proof is needed.
- Often based on scientific, mathematical, or irrefutable data.
- Can directly lead to a legal conclusion or judgment.

Examples:

- A cryptographic hash that matches a file exactly.
- Surveillance footage clearly showing the suspect committing the act.
- Verified system log entries showing unauthorized access from a unique, traceable user account.

CISSP Relevance:

CISSPs contribute to conclusive evidence by ensuring data authenticity, forensic accuracy, and technical certainty when collecting logs, hashes, or other artifacts.

nds" kind of proof—
court.

tangible,

Think of it as the smoking gun with fingerprints—it's so strong, it ends the argument.

onsible for
at serve as
tation to

Circumstantial Evidence

Circumstantial Evidence is indirect evidence that implies a fact but does not prove it outright. It requires inference or reasoning to connect it to the conclusion.

Key Characteristics:

- Doesn't directly show the act—but suggests it occurred based on surrounding facts.
- Often used to build a case when direct evidence is unavailable.
- Can be powerful when combined with other evidence types.

Think of it like digital footprints—they don't show the face, but they paint a picture of who was likely there.

Examples:

- User account accessed a sensitive file at 2:00 AM, and data was later found missing.
- IP address from a data breach ties back to an employee's home network.
- A disgruntled employee was seen near the server room before a sabotage event.

CISSP Relevance:

Security pros often rely on circumstantial evidence like logs, access times, and behavioral anomalies—especially in insider threat cases where direct proof is rare.

accuracy, and technical certainty when collecting logs, hashes, or other artifacts.

Circumstantial Evidence

Circumstantial Evide
requires inference o

Key Characteristics:

- Doesn't directly s
- Often used to bui
- Can be powerful

Think of it like the second opinion that confirms the diagnosis—you already suspected it, and now it's backed up.

CISSP Relevance:

Security pros often r
especially in insider

Corroborative Evidence

Corroborative Evidence is used to support or strengthen other existing evidence, making a case more credible and harder to dispute.

Key Characteristics:

- Doesn't prove something on its own but backs up another piece of evidence.
- Increases the overall reliability of the investigation.
- Often connects or validates circumstantial or testimonial evidence.

Examples:

- An access log (primary evidence) shows a login at 3 AM; CCTV footage (corroborative evidence) confirms the user entered the building at the same time.
- A witness says an employee copied sensitive files; DLP alerts confirm large file transfers during that period.

CISSP Relevance:

CISSPs often provide corroborative evidence through system logs, file metadata, alerts, and monitoring tools to reinforce the findings of legal or internal investigators.

accuracy, and technical ce

CHAPTER 19

Investigations

Types of Evidence

Think of it as the paper (or digital) trail that tells the story in black and white—if it's written, logged, or recorded, it's documentary evidence.

Documentary Evidence is any written or recorded material used to prove or support facts in an investigation or legal proceeding.

Key Forms:

- Emails, memos, policies, contracts
- System logs, access reports, file metadata
- Screenshots, audit trails, configuration files

CISSP Relevance: CISSPs play a key role in preserving and validating documentary evidence—especially digital records that must be authenticated and protected to remain admissible in court.

Best Evidence Rule

The Best Evidence Rule requires that the original version of a document or recording be presented in court when proving its content—not a copy or summary, unless a valid reason is given.

Key Points:

- Ensures accuracy and authenticity of evidence.
- Applies especially to writings, recordings, photos, and digital files.
- Copies may be admissible if the original is lost, destroyed, or unavailable—but only with justification.

CISSP Relevance:

In the digital world, CISSPs must ensure that original log files, emails, or configurations are preserved and not altered, supporting admissibility under this rule.

trail that tells the
itten, logged, or
ce.

Think of it like this: the court wants the real deal—not your "trust me, it said this" version.

erving and
l records that
missible in court.

Best Evidence Rule

The Best Evidence Rule re
recording be presented ir
summary, unless a valid r

Key Points:

- Ensures accuracy and
- Applies especially to v
- Copies may be admiss
  only with justification

CISSP Relevance:

In the digital world, CISSP
configurations are preser
rule.

Parol Evidence Rule

The Parol Evidence Rule states that if a written contract is intended to be the complete and final agreement, then no outside oral or prior written statements can be used to alter or contradict the contract's terms in court.

Key Points:

- Applies mainly in contract disputes.
- Prevents parties from introducing side conversations, emails, or informal notes to override the official document.
- Exceptions exist (e.g., fraud, ambiguity, or incomplete contracts).

CISSP Relevance:

Security professionals involved in contract enforcement, vendor disputes, or software licensing may encounter this rule when handling supporting evidence—only what's in the signed doc counts.

Think of it as "if it's not in the contract, it doesn't exist"—no verbal loopholes allowed.

Best Evidence Rule

The Best Evidence Rule
recording be presented
summary, unless a valid

Key Points:

- Ensures accuracy an
- Applies especially to
- Copies may be admi
  only with justificatio

CISSP Relevance:

In the digital world, CIS
configurations are pres
rule.

Parol Evidence Rule

The Parol Evidence Rule states that if a written contract is intended to be the

an

s

Chain of Evidence

(Also known as Chain of Custody)

Chain of Evidence refers to the documented and unbroken trail of handling, storage, and transfer of evidence from the time it's collected until it's presented in court.

Key Elements:

- Who collected the evidence
- When and where it was collected
- How it was stored and protected
- Who had access to it and when
- Ensures evidence integrity and admissibility

Think of it like the evidence passport—every stop is stamped and recorded, or the whole thing gets thrown out.

CISSP Relevance:

CISSPs must follow strict procedures to ensure digital evidence is not altered or tampered with, maintaining trust and legal credibility throughout investigations.

CHAPTER 19

Investigations

Types of Evidence

Think of it as a human log file—valuable, but prone to bias, memory gaps, and cross-examination.

Testimonial Evidence is verbal or written statements given by witnesses under oath, describing what they saw, heard, or know about an incident.

Key Characteristics:

- Comes from people, not devices or documents.
- Must be given under oath (e.g., in court or deposition).
- Can be challenged for credibility or accuracy.

CISSP Relevance: While CISSPs don't typically give legal testimony, they may provide factual statements, act as expert witnesses, or help validate technical testimony with supporting data.

CHAPTER 19

Hearsay Rule

Hearsay is a statement made outside of court that's offered as evidence to prove the truth of what it says—and it's generally not admissible in legal proceedings.

Key Points:

- Example: "Bob told me he saw Jane delete the logs."
  Not admissible—Bob needs to testify himself.
- The rule protects against unreliable, secondhand information.
- There are many exceptions, like business records, dying declarations, or excited utterances.

CISSP Relevance:

When gathering evidence, CISSPs must focus on direct, verifiable sources (e.g., logs, original files) rather than hearsay statements, especially if preparing materials for legal use.

Think of it as a human log file—valuable, but prone to bias, memory gaps, and cross-examination.

witnesses under

Think of it like digital gossip—it might sound useful, but unless it comes straight from the source, it usually doesn't make it into court.

ically give legal
ents, act as expert
ony with supporting

CHAPTER 19

Investigations

Types of Evidence

Think of it like security evidence with training wheels—it helps tell the story, but only if it reflects the facts faithfully.

Demonstrative Evidence is evidence that illustrates, explains, or supports other evidence—typically in the form of visual aids, models, diagrams, charts, or simulations.

Key Characteristics:

- Doesn't prove the fact by itself but helps the jury or judge understand the evidence better.
- Must be accurate, fair, and based on facts already in the case.
- **Examples**: Network breach timeline, attack path diagram, data flowchart, or a simulation of a malware infection.

CISSP Relevance: CISSPs often help create demonstrative evidence by visualizing log data, forensic timelines, or network activity—making complex tech understandable in legal or executive settings.

2025 CISSP MENTOR PROGRAM

CHAPTER 19

Evidence

Artifacts, Evidence Collection, and Forensic Procedures

CHAPTER 19

Evidence

Think of it like security evidence with training wheels—it helps tell the story, but only if it reflects the facts faithfully.

Artifacts, Evidence Collection, and Forensic Procedures

Artifacts are residual data or indicators left behind on systems that can be used to reconstruct events or trace activity.

Examples:

- Log entries
- Deleted files
- Registry changes
- Timestamps
- Browser history

Key Characteristics:

- Doesn’t prove the fact by itself but helps the jury or judge understand the evidence better.
- Must be accurate, fair, and based on facts already in the cas
- **Examples**: Network breach timeline, attack path diagram, c flowchart, or a simulation of a malware infection.

2025 CISSP MENTOR PROGRAM

CHAPTER 19

Evidence

Artifacts, Evidence Collection, and Forensic Procedures

Evidence Collection is the process of gathering data and objects in a way that maintains their integrity and legal admissibility.

Key Steps:

- Identify and isolate relevant systems or data
- Capture forensic images (bit-by-bit copies)
- Use write blockers for physical media
- Label, document, and maintain chain of custody

CHAPTER 19

Evidence

Artifacts, Evidence Collection, and Forensic Procedures

Think of it like crime scene work for computers—don't trample the digital footprints, and document everything like your job depends on it (because it might).

Forensic Procedures are standardized methods used to identify, collect, preserve, analyze, and present evidence in a defensible and repeatable manner.

Includes:

- Using **validated tools and techniques**
- Maintaining **chain of custody**
- Ensuring **non-repudiation and evidence integrity**
- Documenting **every step of the process**

If you're going to fast to document EVERYTHING, you're going too fast.

CISSP Relevance: Security pros must ensure artifacts are not corrupted, evidence is collected legally, and procedures follow forensic standards to support investigations and legal actions.

Digital Forensics Handling Checklist

Before Collection

- Identify the scope and objective of the investigation
- Obtain proper legal authorization or consent
- Document who initiated the request and why
- Prepare necessary tools (write blockers, imaging software, evidence bags)

Collection Phase

- Isolate the device (physically or via network) to prevent tampering
- Capture screenshots or photos of system state (if active)
- Use write-blockers for physical drives
- Create bit-for-bit forensic images (not logical copies)
- Hash original and copied data (e.g., MD5, SHA-256) and record them
- Collect volatile data (RAM, active connections) if device is on
- Bag, tag, and label devices properly

for computers—don't
d document everything
use it might).

llect, preserve,
er.

going to fast to
nt EVERYTHING,
oing too fast.

e artifacts are not
corrupted, evidence is collected legally, and procedures follow forensic
standards to support investigations and legal actions.

Digital Forensics Handling Checklist

Before Collection

- Identify the scope and objecti
- Obtain proper legal authorizat
- Document who initiated the r
- Prepare necessary tools (write

Collection Phase

- Isolate the device (physically c
- Capture screenshots or photo
- Use write-blockers for physica
- Create bit-for-bit forensic ima
- Hash original and copied data
- Collect volatile data (RAM, act
- Bag, tag, and label devices pro

Documentation & Chain of Custody

- Record time, date, and who performed each action
- List all hardware and tools used
- Fill out a Chain of Custody form at every transfer point
- Secure all evidence in tamper-proof storage
- Restrict access to authorized personnel only

Analysis Phase

- Analyze only the forensic copy, never the original
- Maintain logs of all analysis steps
- Use validated forensic tools (e.g., EnCase, FTK, Autopsy)
- Recalculate hashes to confirm no data was altered

Reporting & Presentation

- Summarize findings clearly and factually
- Include supporting artifacts and hash values
- Use demonstrative evidence (timelines, charts) if needed
- Ensure the report is admissible and defensible

for computers—don't
d document everything
use it might).

rensic

CHAPTER 19

Evidence

Artifacts, Evidence Collection, and Forensic Procedures

Think of it like digital archaeology—digging through the layers of a drive to find what was there, what changed, and what shouldn't be there.

Media Analysis is the forensic process of examining digital storage devices—like hard drives, USBs, SSDs, CDs/DVDs—to uncover, recover, and analyze data relevant to an investigation.

Key Activities:

- Creating forensic images (bit-by-bit copies) of the media.
- Recovering deleted files, hidden partitions, or slack space data.
- Analyzing file structures, timestamps, and metadata.
- Searching for evidence of malicious activity or policy violations.

CISSP Relevance: CISSPs must understand how media analysis supports investigations and how to preserve integrity, ensure admissibility, and use validated tools during the process.

CHAPTER 19

Evidence

Artifacts, Evidence Collection, and Forensic Pr

Think of it like digital archaeology—digging through the layers of a drive to find what was there, what changed, and what shouldn't be there.

Think of it like digital "read-only mode" with legal weight—you can look, but you absolutely cannot touch.

Media Analysis is the forensic process of examining digit

Write Blocker

A write blocker is a forensic hardware or software tool that allows investigators to read data from a storage device without allowing any modifications or writes to that device.

Key Purpose:

- Prevents accidental or intentional alteration of evidence.
- Ensures the original media remains unchanged and legally admissible.
- Commonly used when imaging hard drives, USBs, or SD cards.

CISSP Relevance:

CISSPs involved in forensic work must use write blockers to preserve evidence integrity, maintain chain of custody, and support admissibility in court.

CHAPTER 19

Evidence

Artifacts, Evidence Collection, and Forensic Procedures

Think of it like the brain of the system—you grab it fast or it forgets everything.

In-Memory Analysis is the process of examining a system's RAM (volatile memory) to uncover live, transient data that doesn't persist after shutdown.

Key Insights You Can Find:

- Running processes, open files, and loaded modules
- Network connections and session details
- Malware operating only in memory (fileless attacks)
- Encryption keys, passwords, and clipboard contents

CISSP Relevance: CISSPs must recognize the critical importance of capturing memory before system shutdown during investigations—once lost, this data is unrecoverable.

CHAPTER 19

Evidence

Artifacts, Evidence Collection, and Forensic Procedures

Think of it like the brain of the system—you grab it fast or it forgets everything.

In-Memory Analysis is the pro

Think of it like taking a digital snapshot of a computer's brain—a flash freeze of everything it's thinking about before it forgets.

Memory Dump

A Memory Dump is the process of capturing the contents of a system's RAM at a specific moment—used to analyze live, volatile data during an investigation.

Key Uses:

- Investigate running processes, malware, network activity, and encryption keys.
- Detect fileless attacks or data exfiltration tools operating in memory only.
- Support incident response and forensic reconstruction.

CISSP Relevance:

CISSPs should ensure memory is dumped quickly and properly before a system is powered off, using forensically sound tools like FTK Imager, Volatility, or DumpIt.

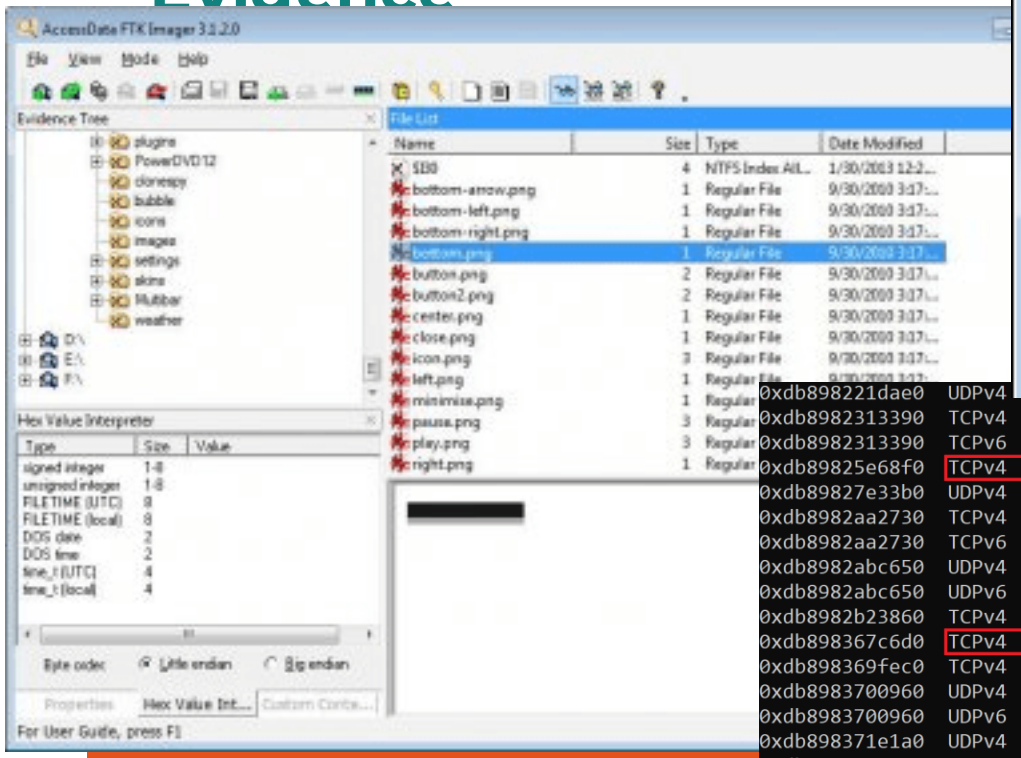
g

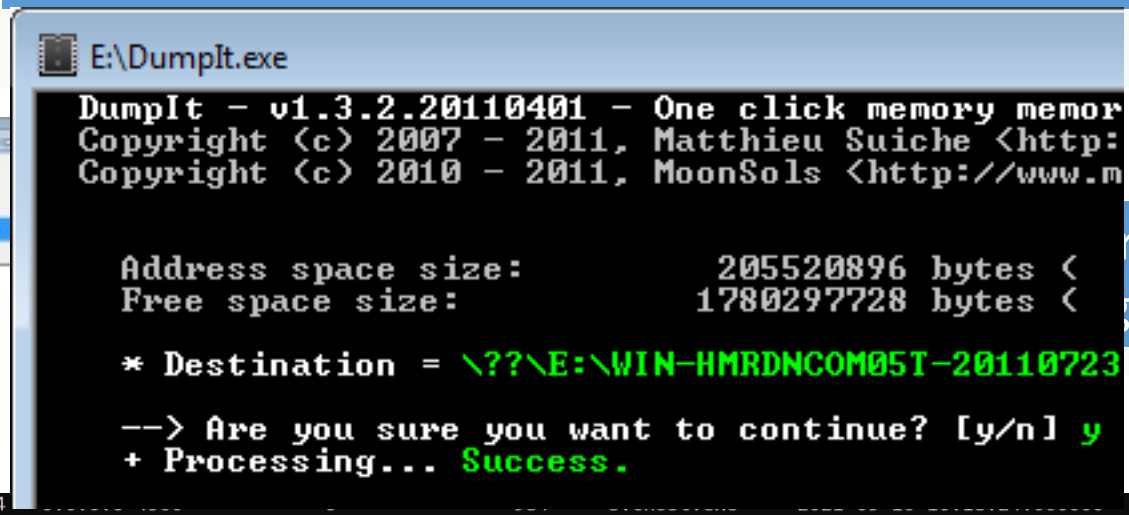
2025 CISSP MENTOR PROGRAM

CHAPTER 19

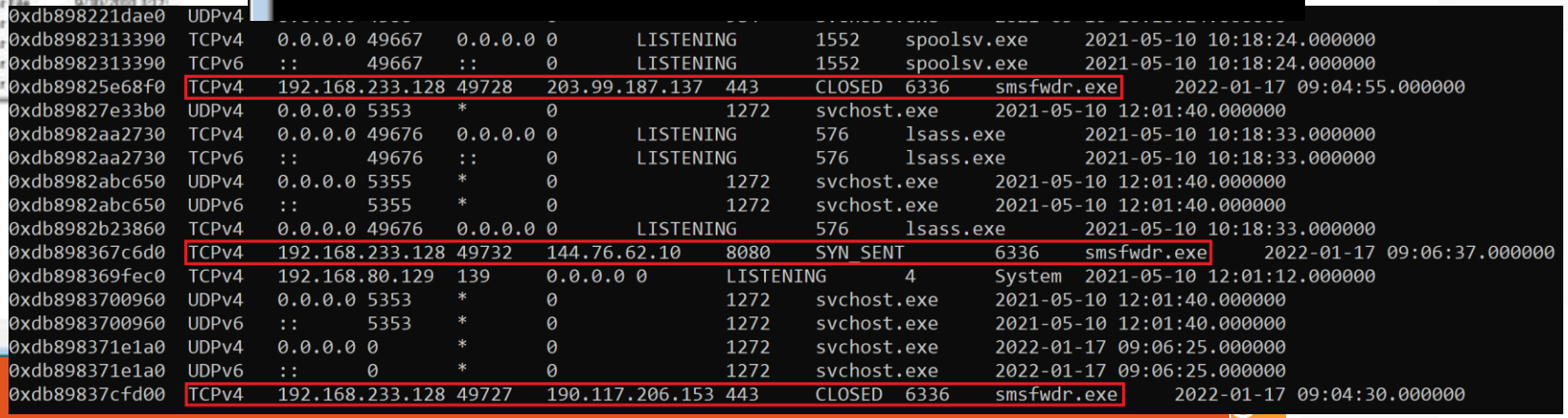
Evidence

Think of it like the brain of the system—you grab it fast or it forgets everything.





rain—a
gets.



CISSP Relevance:

CISSPs should ensure memory is dumped quickly and properly before a system is powered off, using forensically sound tools like FTK Imager, Volatility, or DumpIt.

CHAPTER 19

Evidence

Artifacts, Evidence Collection, and Forensic Procedures

Think of it like tapping into the wires of a digital crime scene—everything flows through the network, and if you know what to look for, it tells a hell of a story.

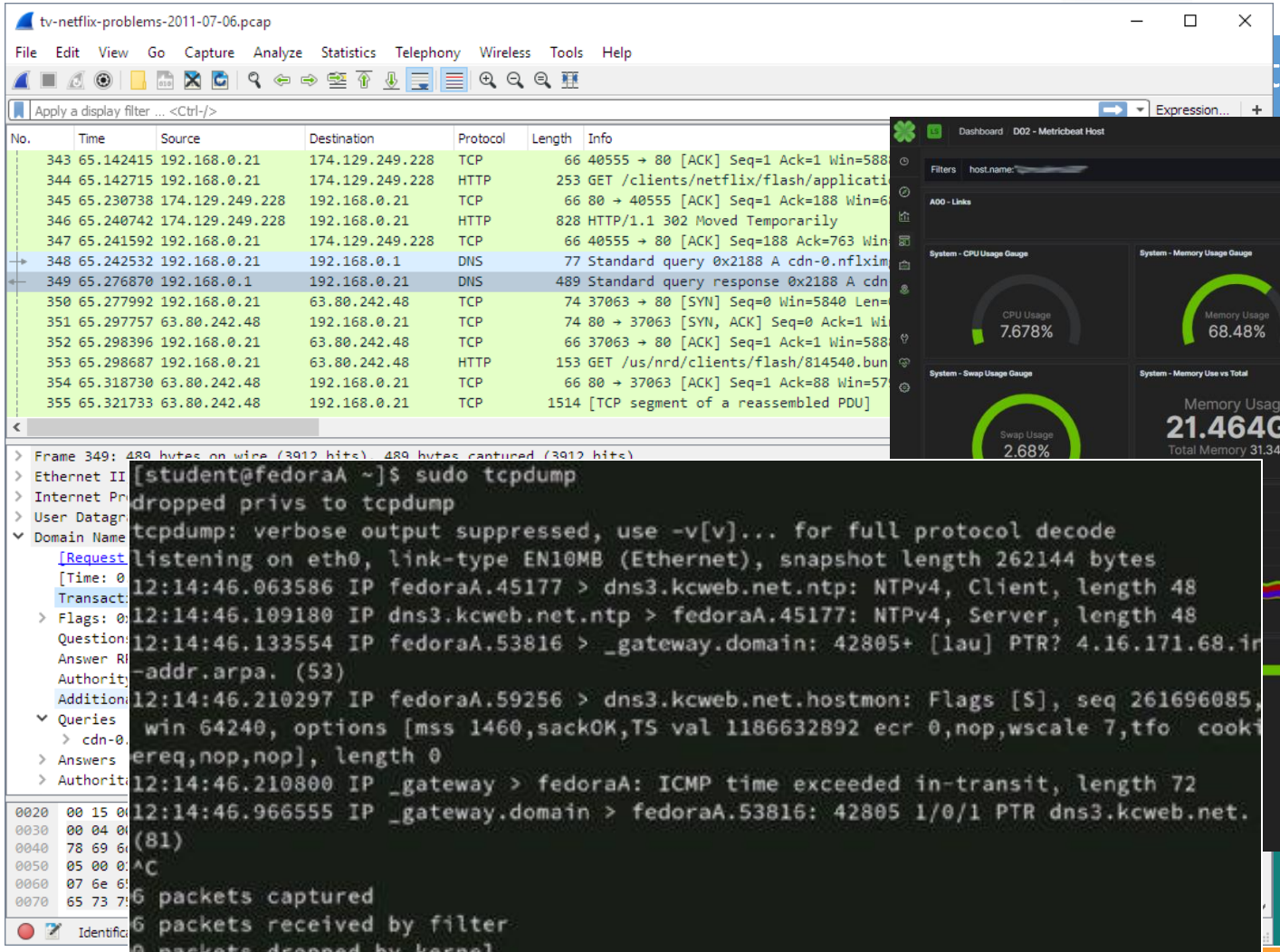
Network Analysis is the process of monitoring, capturing, and examining network traffic and communication patterns to detect anomalies, security incidents, or unauthorized activity.

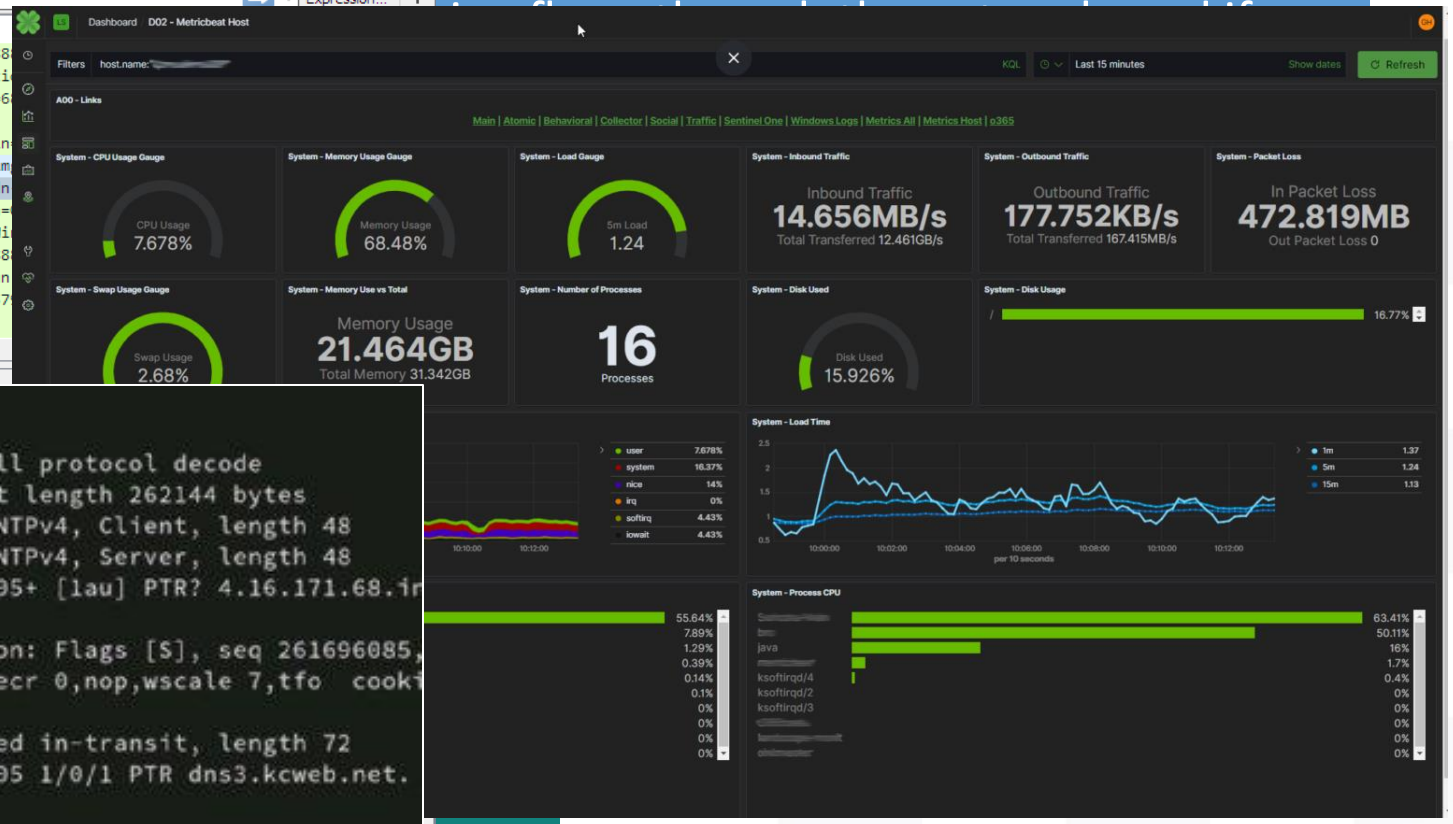
Key Focus Areas:

- Packet captures (PCAPs) to review real-time data flow
- Log analysis from firewalls, IDS/IPS, proxies, and routers
- Detection of malware callbacks, data exfiltration, port scanning, and more
- Identifying source/destination IPs, protocols, and suspicious behavior

CISSP Relevance: CISSPs must ensure networks are instrumented to log and preserve traffic data, and that analysts have access to tools like Wireshark, Zeek, or tcpdump for timely response.

tapping into the wires of a digital crime





suspicious behavior

CISSP Relevance: CISSPs must ensure networks are instrumented to log and preserve traffic data, and that analysts have access to tools like Wireshark, Zeek, or tcpdump for timely response.

CHAPTER 19

Evidence

Artifacts, Evidence Collection, and Forensic Procedures

Think of it as opening the hood on a suspicious app—you're looking for booby traps, sloppy code, or outright sabotage.

Software Analysis is the process of examining applications or code to identify vulnerabilities, malicious behavior, or policy violations—critical in both security investigations and secure development.

Key Activities:

- **Static Analysis**: Reviewing source code or binaries without executing them to detect flaws (e.g., buffer overflows, hardcoded credentials).
- **Dynamic Analysis**: Running the software in a controlled environment (sandbox) to observe real-time behavior.
- **Reverse Engineering**: Disassembling compiled code to understand how unknown or malicious programs work.

CISSP Relevance: CISSPs must support or enable secure software practices and investigations by ensuring tools, environments, and expertise are in place to safely analyze software.

CHAPTER 19

Evidence

Artifacts, Evidence Collection, and Forensic Procedures

Think of it like tech surgery—you're not just looking at what the device does, but what it's hiding inside.

Hardware/Embedded Device Analysis involves examining physical devices and their firmware or embedded software to identify security flaws, tampering, or malicious modifications.

Key Activities:

- Extracting and analyzing firmware, configuration data, and system logs
- Using tools to access JTAG, UART, SPI interfaces, or chip-off methods
- Investigating IoT devices, routers, PLCs, USBs, and other specialized tech
- Checking for unauthorized components, backdoors, or code injections

CISSP Relevance: CISSPs should understand the risks of embedded systems and supply chain vulnerabilities and ensure secure handling of hardware involved in investigations.

CHAPTER 19

Think of it like tech surgery—you're not just looking at what the device does, but what it's hiding inside.

Locard's Exchange Principle Locard's Exchange Principle states: *"Every contact leaves a trace."*

In other words, whenever two objects interact, they exchange material, leaving evidence behind.

Think of it like digital glitter—attackers always leave a sparkle behind, even if they try to clean it up.

In Forensics:

- A hacker leaves digital fingerprints—logs, metadata, timestamps.
- A malicious device connected to a network leaves configuration changes or traffic anomalies.
- Even attempted concealment leaves traces (e.g., deleted logs, altered files).

CISSP Relevance:
This principle supports the idea that no cyberattack occurs without some form of residual data or artifact—it's your job to find and interpret those traces.

ices and
ing, or

risks of
s and ensure
ons.

2025 CISSP MENTOR PROGRAM

CHAPTER 19

Investigations

Investigation Process

2025 CISSP MENTOR PROGRAM

CHAPTER 19

Investigations

Investigation Process

Think of it as your digital detective playbook—follow the process, or risk compromising the truth.

The **Investigation Process** is a structured approach to identify, analyze, and resolve incidents—whether they involve security breaches, policy violations, or legal issues.

Key Phases:

1. **Initiation** – Determine if an investigation is warranted and define scope.
2. **Planning** – Establish objectives, assign roles, and gather necessary resources.
3. **Evidence Gathering** – Collect data and artifacts while preserving integrity.
4. **Analysis** – Examine evidence to identify facts, root causes, and impact.
5. **Interviews** – Speak with involved individuals to clarify actions and motives.
6. **Reporting** – Document findings, conclusions, and recommendations.
7. **Closure** – Ensure lessons are learned, systems are restored, and improvements are made.

CISSP Relevance: CISSPs must ensure the process is conducted with integrity, confidentiality, and adherence to legal and organizational standards, especially when incidents may escalate to litigation or regulatory scrutiny.

CHAPTER 19

Investigations

Investigation Process

Think of it like a digital crime scene—grab what matters, touch nothing else, and write everything down.

Gathering Evidence is the critical step of identifying, collecting, and securing information or artifacts that may prove what happened during a security incident or policy violation.

Key Principles:

- **Preserve integrity**: Use proper tools and techniques (e.g., write blockers, forensic imaging).
- **Follow chain of custody**: Document who collected it, when, and how.
- **Prioritize volatile data**: Capture memory, active sessions, or logs before they're lost.
- **Minimize disruption**: Avoid altering systems or operations during collection.

CISSP Relevance: CISSPs are responsible for ensuring evidence is legally defensible, forensically sound, and aligns with internal policies and external legal standards.

CHAPTER 19

Think of it like a digital crime scene—grab what matters, touch nothing else, and write everything down.

Voluntary Surrender

When an individual willingly hands over evidence without being compelled by law.

Key Points:

- No legal order needed.
- Still must be properly documented and handled to ensure admissibility.

ifying, collecting, and securing
appened during a security incident

- **Preserve integrity**: Use proper tools and techniques (e.g., write blockers, forensic imaging).
- **Follow chain of custody**: Document who collected it, when, and how.
- **Prioritize volatile data**: Capture memory, active sessions, or logs before they're lost.
- **Minimize disruption**: Avoid altering systems or operations during collection.

CISSP Relevance: CISSPs are responsible for ensuring evidence is legally defensible, forensically sound, and aligns with internal policies and external legal standards.

CHAPTER 19

Think of it like a digital crime scene—grab what matters, touch nothing else, and write everything down.

Voluntary Surrender

When an individual willingly hands over evidence without being compelled by law

Key Points:

- No legal order neede
- Still must be properly ensure admissibility.

ecuring
rity incident

- **Preserve int** s, forensic imaging).
- **Follow chai**
- **Prioritize vo** they're lost.
- **Minimize disruption**: Avoid altering systems or operations during collection.

Subpoena

A legal document that compels someone to provide evidence (documents, records, or testimony) in a civil or criminal investigation.

Key Points:

- Typically used in civil or regulatory cases.
- Must be complied with or challenged legally—not optional.

CISSP Relevance: CISSPs are responsible for ensuring evidence is legally defensible, forensically sound, and aligns with internal policies and external legal standards.

CHAPTER 19

Think of it like a digital crime scene—grab what matters, touch nothing else, and write everything down.

Voluntary Surrender

When an individual willingly hands over evidence without being compelled by law

Key Points:

- No legal order neede
- Still must be properly ensure admissibility.

ecuring
rity incident

- **Preserve int** imaging).
- **Follow chai**
- **Prioritize vo**
- **Minimize disruption**: Avoid alter

Subpoena

A legal document that compels someone to provide evidence (documents, records, or testimony) in a civil or criminal investigation

Key Points:

- Typically used in
- Must be complie optional.

Plain View Doctrine

Allows law enforcement to seize evidence without a warrant if it's clearly visible while they are lawfully present.

Key Points:

- Applies during routine access or lawful searches.
- Evidence must be obvious and immediately apparent as relevant to a crime.

CISSP Rel
legally defe
and extern

CHAPTER 19

Think of it like a digital crime scene—grab what matters, touch nothing else, and write everything down.

Voluntary Surrender

When an individual willingly hands over evidence without being compelled by law

Key Points:

- No legal order neede
- Still must be properly ensure admissibility.

Subpoena

A legal document that compels someone to provide evidence (documents, records, or testimony) in a civil or criminal investigatio

ecuring
rity incident

Plain View Doctrine

w enforcement to seize evidence without a
f it's clearly visible while they are lawfully

ts:
es during routine access or lawful searches.
nce must be obvious and immediately apparent
evant to a crime.

Search Warrant

A court-issued order authorizing law enforcement to search specific locations and seize specific items.

Key Points:

- Requires probable cause.
- Must be executed according to scope and time limits.

CHAPTER 19

Exigent Circumstances

Situations where immediate action is needed to prevent harm, destruction of evidence, or escape—allowing search/seizure without a warrant.

Key Points:

- Applies when waiting for a warrant could compromise the investigation.
- Must be justified and documented to hold up in court.

Voluntary Surrender

When an individual willingly hands over e
without being compelled by law

Key Points:

- No legal order neede
- Still must be properly
ensure admissibility.

Subpoena

A legal documen
evidence (docun
criminal investigation

Plain View Doctrine

w enforcement to seize evidence without a

es during routine access or lawful searches.
nce must be obvious and immediately apparent
evant to a crime.

Search Warrant

A court-issued order authorizing law
to search specific locations and seiz

Key Points:

- Requires probable cause.
- Must be executed according to scope and time limits.

CISSPs must understand these concepts when interfacing with law enforcement or legal teams, especially during digital evidence handling—one wrong move could invalidate critical evidence.

CHAPTER 19

Investigations

Investigation Process

Calling in Law Enforcement refers to involving official agencies (local, state, federal) when a security incident involves potential criminal activity, significant data breaches, or threats to public safety.

When to Involve Law Enforcement:

- Evidence of unauthorized access, theft, fraud, or sabotage
- Incidents that cross jurisdictions or involve critical infrastructure
- Cases where legal authority is needed for search, seizure, or prosecution

CHAPTER 19

Investigations

Investigation Process

Think of it like escalating to the big leagues—once the badges show up, the rules (and stakes) change fast.

Calling in Law Enforcement refers to involving
federal) when a security incident involves pot
data breaches, or threats to public safety.

CISSP Relevance: CISSPs need to know how and when to escalate incidents appropriately, how to interface with law enforcement, and how to protect the organization's legal and operational interests during the process.

When to Involve Law Enforcement:

- Evidence of unauthorized access, theft, fraud,
- Incidents that cross jurisdictions or involve critical infrastructure
-

Key Considerations:

- Chain of custody must be preserved from the moment law enforcement is involved.
- Ensure internal policies and legal counsel are consulted first.
- Once involved, control of the investigation may shift to authorities.
- Disclosure may trigger regulatory notifications (e.g., breach notification laws).

Reasons Organizations May Avoid Law Enforcement Involvement

1. Loss of Control

Once law enforcement steps in, the company may lose control of the investigation.
Systems might be seized, data taken, or operations disrupted.

2. Reputation Damage

Involving police or federal agencies often becomes public, potentially damaging brand trust, investor confidence, and customer relationships.

3. Business Disruption

Investigations can slow down or halt operations, especially if systems are taken offline or evidence is confiscated.

4. Exposure of Internal Issues

Law enforcement may uncover unrelated problems (e.g., compliance failures, improper practices), leading to regulatory fines or legal action.

5. Legal and Regulatory Complexity

It can open the door to civil lawsuits or government investigations, especially in highly regulated industries.

6. Desire for Quiet Resolution

Companies may prefer to handle issues internally or with private investigators to maintain discretion and negotiate quietly with affected parties.

Reasons Organizations May Avoid Law Enforcement Involvement

1. Loss of Control

Once law enforcement steps in, the company may lose control of the investigation.
Systems might be seized, data taken, or operations disrupted.

2. Reputation Damage

Involving police or federal agencies often b r confidence, and customer relationships.

While security pros must be ready to coordinate with law enforcement, they should also understand why executives might hesitate—and work with legal and compliance teams to make informed decisions.

3. Business Disruption

Investigations can slow down or halt operations, especially if systems are taken offline or evidence is confiscated.

4. Exposure of Internal Issues

Law enforcement may uncover unrelated problems (e.g., compliance failures, improper practices), leading to regulatory fines or legal action.

5. Legal and Regulatory Complexity

It can open the door to civil lawsuits or government investigations, especially in highly regulated industries.

6. Desire for Quiet Resolution

Companies may prefer to handle issues internally or with private investigators to maintain discretion and negotiate quietly with affected parties.

CHAPTER 19

Investigations

Investigation Process

Conducting the Investigation involves the structured, methodical process of gathering facts, analyzing evidence, and documenting findings to determine what happened, how, why, and by whom.

Key Steps:

1. **Define scope and objectives** – What are you trying to prove or uncover?
2. **Assemble the team** – Include legal, HR, IT, security, and management as needed.
3. **Secure the scene** – Prevent further tampering or data loss.
4. **Collect and preserve evidence** – Use forensic methods to protect integrity.
5. **Analyze findings** – Look for patterns, anomalies, and correlations.
6. **Maintain chain of custody** – Log all handling and access to evidence.
7. **Follow legal and ethical guidelines** – Avoid rights violations or overreach.

CHAPTER 19

Investigations

Investigation Process

Think of it like digital detective work—you're not just chasing "whodunnit," you're building a bulletproof timeline of what happened and how to fix it.

Conducting the Investigation involves the structured, methodical process of gathering facts, analyzing evidence, and documenting findings to determine what happened, how, why, and by whom.

Key Steps:

1. **Define scope and objectiv**
2. **Assemble the team** – Incl
3. **Secure the scene** – Prever
4.
5. elations.
6. o evidence.
7. ns or overreach.

CISSP Relevance: CISSPs may lead or support investigations and must ensure that all actions are legally defensible, forensically sound, and clearly documented.

Important Considerations:

- Remain objective and impartial—don't assume guilt.
- Follow internal policies and regulatory obligations.
- Prepare for the possibility of civil, criminal, or regulatory consequences.

CHAPTER 19

Investigations

Investigation Process

Interviewing Individuals during an investigation involves gathering firsthand accounts from those involved or affected—whether they're witnesses, suspects, or stakeholders.

Goals:

- Clarify facts, timelines, and potential motives
- Corroborate or challenge technical evidence
- Understand behaviors or decisions that led to the incident

Considerations:

- In some cases, individuals may need to be informed of their rights or allowed legal representation
- Information gathered may be privileged or confidential, depending on company policies or legal context

Best Practices:

- Always document who was interviewed, when, and what was said
- Ensure interviews are conducted ethically and legally (e.g., avoid coercion)
- Be neutral and non-accusatory—interviews are for gathering info, not assigning blame
- Pair with another interviewer or record (with consent) for accuracy
- Ask open-ended questions and avoid leading language

2025 CISSP MENTOR PROGRAM

CHAPTER 19

Investigations

Investigation Process

Interviewing Individuals du
accounts from those involv
stakeholders.

r

Goals:

- Clarify facts, timelines, and potential motives
- Corroborate or challenge technical evidence

Considerations:

- In some cases, individuals may need to be informed of their rights or allowed legal representation
- Information gathered may be privileged or confidential, depending on company policies or legal context

Think of it like piecing together a timeline from voices—the logs tell you what happened, but people tell you why.

Best Practices:

- Always document who was interviewed, when, and what was said
- Ensure interviews are conducted ethically and legally (e.g., avoid coercion)
- Be neutral and non-accusatory—interviews are for
  nfo, not assigning blame
  nother interviewer or record (with consent)
  y
  nded questions and avoid leading language

CISSP Relevance: CISSPs must understand the importance of interviewing in building a complete and legally sound investigation, especially when correlating human actions with technical events.

CHAPTER 19

Investigations

Investigation Process

Data Integrity and Retention focuses on preserving the accuracy, completeness, and security of data throughout the investigation and beyond, in accordance with legal, regulatory, and business requirements.

Data Integrity:

- Ensure that evidence is not altered or tampered with during collection, analysis, or storage.
- Use hashing algorithms (e.g., SHA-256) to verify data integrity.
- Maintain chain of custody logs and secure storage protocols.

Data Retention:

- Follow company policy and legal mandates on how long data must be kept.
- Avoid over-retention, which increases legal exposure and costs.
- Use secure archiving solutions to store data with proper access controls.
- Know what to do when litigation holds are issued (pause data deletion).

CHAPTER 19

Investigations

Investigation Process

Think of it like guarding the truth in a vault—the data has to stay exactly as it was, for exactly as long as needed, or the whole investigation's credibility is toast.

Data Integrity and Retention foc
and security of data throughout
legal, regulatory, and business re

CISSP Relevance: CISSPs play a critical role in implementing systems and policies that protect data integrity and enforce appropriate retention schedules—especially when data may become legal evidence.

Data Integrity:

- Ensure that evidence is not altered or tampered with during collection, analysis, or storage.
- Use hashing algorithms (e.g., SHA-256) to verify data integrity.
- Maintain chain of custody logs and secure storage protocols.

Data Retention:

- Follow company policy and legal mandates on how long data must be kept.
- Avoid over-retention, which increases legal exposure and costs.
- Use secure archiving solutions to store data with proper access controls.
- Know what to do when litigation holds are issued (pause data deletion).

CHAPTER 19

Investigations

Investigation Process

Reporting and documenting investigations is the final phase where findings, evidence, actions taken, and conclusions are formally recorded to support internal decision-making, legal proceedings, or regulatory compliance.

Key Components:

- **Executive Summary** – High-level overview for leadership
- **Timeline of Events** – Chronological breakdown of actions and discoveries
- **Evidence Log** – What was collected, from where, when, and by whom
- **Findings** – Factual outcomes supported by evidence
- **Root Cause Analysis** – Why it happened and how
- **Recommendations** – Fixes, controls, and policy updates
- **Lessons Learned** – What to improve for future prevention

2025 CISSP MENTOR PROGRAM

CHAPTER 19

Investigations

Investigation Process

Think of this phase as writing the final chapter in a forensic novel—make it clean, clear, and ready for the lawyers, regulators, or boardroom warriors who'll be reading it.

Reporting and documenting investig
evidence, actions taken, and conclus
decision-making, legal proceedings,

Critical Guidelines:

- Keep documentation factual, objective, and jargon-free
- Ensure reports are legally defensible and audit-ready
- Limit access to those with a legitimate need to know
- Review reports with legal and compliance teams before distribution

Key Components:

- **Executive Summary** – High-level overview for leadership
- **Timeline of Events** – Chronological breakdown of actions and discoveries
- **Evidence Log** – What was collected, from where, when, and by whom
- **Findings** – Factual outcomes supported by evidence
- **Root Cause Analysis** – Why it happ
- **Recommendations** – Fixes, control
- **Lessons Learned** – What to improv

CISSP Relevance: CISSPs are often responsible for contributing technical insights and ensuring the accuracy, completeness, and confidentiality of investigative reports.

CHAPTER 19

Major Categories of Computer Crime

Computer crimes come in various forms, each driven by different motives, targets, and tactics. Understanding these categories helps security professionals anticipate threats, recognize patterns, and design better defenses.

Here's a quick breakdown of the main categories we'll explore:

1. **Military and Intelligence Attacks** – Nation-state espionage and cyber warfare.
2. **Business Attacks** – Targeted at competitive advantage or disruption.
3. **Financial Attacks** – Driven by profit through fraud, theft, or ransomware.
4. **Terrorist Attacks** – Intended to cause fear, disruption, or damage infrastructure.
5. **Grudge Attacks** – Personal revenge or retaliation.
6. **Thrill Attacks** – Motivated by boredom, challenge, or ego.
7. **Hacktivist Attacks** – Ideologically driven; targeting organizations in protest.

Each type involves unique threat actors, techniques, and consequences.

CHAPTER 19

Major Categories of Computer Crime

Military and Intelligence Attacks

Military and Intelligence Attacks are typically conducted by nation-states or state-sponsored actors with goals tied to national security, espionage, or cyber warfare.

Objectives:

- Steal classified or sensitive government data
- Disrupt or sabotage critical infrastructure
- Conduct cyber-espionage against foreign adversaries
- Gain strategic advantage in geopolitical conflicts

Common Tactics:

- Advanced Persistent Threats (APTs)
- Zero-day exploits and custom malware
- Spear phishing targeting military or defense contractors
- Supply chain attacks on national defense systems

Notable Examples:

- **Stuxnet** – Sabotaged Iranian nuclear centrifuges.
- **SolarWinds** – Breach impacting U.S. federal agencies.
- **China's APT10 & Russia's APT29** – Known for cyber-espionage operations.

CHAPTER 19

Major Categories of Computer Crime

Military and Intelligence Attacks

These aren't your script kiddies—these are the digital special forces of cyber conflict.

Military and Intelligence Attacks are typically conducted by nation-states or state-sponsored actors with goals tied to national security, espionage, or cyber warfare.

Objectives:

- Steal classified or sensitive government data
- Disrupt or sabotage critical infrastructure
- Conduct cyber-espionage against foreign adversaries
- Gain strategic advantage in geopolitical conflicts

Common Tactics:

- Advanced Persistent Threats (
- Zero-day exploits and custom
- Spear phishing targeting milit
- Supply chain attacks on natio

Notable Examples:

- **Stuxnet** – Sabotaged Iranian nuclear centrifuges.
- **SolarWinds** – Breach impacting U.S. federal agencies.
- **China's APT10 & Russia's APT29** – Known for cyber espionage

CISSP Relevance: CISSPs working in critical infrastructure or defense sectors must understand these threats and implement robust, layered defenses and monitoring to counter highly skilled adversaries.

CHAPTER 19

Major Categories of Computer Crime

Business Attacks

Business Attacks are targeted at commercial organizations, aiming to steal intellectual property, disrupt operations, or gain competitive advantage.

Objectives:

- **Corporate espionage**—stealing trade secrets or proprietary tech
- **Sabotage**—crippling systems to gain market share or damage reputation
- **Disruption**—causing downtime to impact productivity or client trust

Common Tactics:

- Phishing and social engineering to gain access to sensitive systems
- Insider threats (disgruntled employees, contractors)
- Ransomware and DDoS attacks for extortion or chaos
- Credential stuffing and malware implants to access data systems

CHAPTER 19

Major Categories of Computer Crime

Business Attacks

Business attackers don't want publicity—they want your blueprints, customers, and competitive edge.

Business Attacks are targeted at c
intellectual property, disrupt opera

CISSP Relevance: CISSPs in corporate environments must defend against both external and internal threats, applying security controls, insider monitoring, and incident response plans.

Objectives:

- **Corporate espionage**—stealing trade secrets or proprietary tech
- **Sabotage**—crippling systems to gain market share or damage reputation
- **Disruption**—causing

Common Tactics:

- Phishing and social
- Insider threats (disg
- Ransomware and DI
- Credential stuffing and malware implants to access data systems

Notable Examples:

- Operation Shady RAT – Widespread business espionage operation.
- Target breach (2013) – Attackers entered through a third-party vendor.
- NotPetya (2017) – Masqueraded as ransomware, but targeted business operations globally.

CHAPTER 19

Major Categories of Computer Crime

Financial Attacks

Financial Attacks are cybercrimes committed with the primary goal of stealing money or monetizable data—targeting individuals, financial institutions, and businesses.

Objectives:

- Steal credit card numbers, bank credentials, or payment data
- Commit wire fraud, tax fraud, or identity theft
- Distribute ransomware or create fraudulent financial transactions
- Exploit cryptocurrency wallets or exchanges

Common Tactics:

- Phishing and pharming for login credentials
- ATM skimming and POS malware
- Business Email Compromise (BEC)
- Fake invoicing, account takeovers, and SIM swapping
- Use of cryptojacking malware to mine cryptocurrency covertly

CHAPTER 19

Financial attackers don't care about ideology—they care about cash flow, fast payouts, and clean getaways.

Major Categories of Computer Crime

Financial Attacks

Financial Attacks are cybercrimes committed with the primary goal of stealing money or monetizable data—targeting individuals, financial institutions, and businesses.

Objectives:

- fraudulent financial tran
- Exploit cryptocurrency v
  exchanges

Common Tactics:

rming for login

nd POS malware
ompromise (BEC)
ccount takeovers, and SIM
e

Notable Examples:

- WannaCry (2017) – Ransomware that locked data for Bitcoin payments
- Silk Road takedown – Illicit marketplace used for money laundering
- FIN7 Group – Infamous cybercrime group targeting financial data

CISSP Relevance: CISSPs must implement strong access controls, transaction monitoring, and fraud detection to prevent and detect financial crimes—especially in fintech and retail sectors.

CHAPTER 19

Major Categories of Computer Crime

Terrorist Attacks

Terrorist Attacks in cyberspace are driven by groups or individuals seeking to instill fear, cause disruption, or advance ideological, political, or religious agendas—often targeting critical infrastructure or public services.

Objectives:

- Disrupt essential services like power, water, or transportation
- Spread propaganda, recruit followers, or coordinate activities
- Undermine public trust in governments or institutions
- Trigger mass panic or psychological trauma

Common Tactics:

- Defacement of government websites
- DDoS attacks on public services or emergency systems
- Use of encrypted platforms for communication and planning
- Attempts to breach critical infrastructure control systems (ICS/SCADA)
- Spread of misinformation or deepfake campaigns

CHAPTER 19

Major Categories of Computer Crime

Terrorist Attacks

These attacks don't just steal—they're aimed at psychological and societal impact.

Terrorist Attacks in cyberspace are driven by groups or individuals seeking to instill fear, cause disruption, or advance ideological, political, or religious agendas—often targeting critical infrastructure or public services.

Objectives:

- Undermine publ
  or institutions
- Trigger mass par
  trauma

Common Tactics:

t of government websites
ks on public services or
systems
ypted platforms for
frastructure
deepfake

Notable Examples:

- Cyberterrorism plots targeting power grids and hospitals
- ISIS digital campaigns using encrypted apps for coordination
- 2021 Florida water treatment facility hack—potential sabotage

CISSP Relevance: CISSPs in critical sectors must implement robust segmentation, access control, and incident response plans, and stay aware of nation-state overlaps with terrorist tactics.

CHAPTER 19

Major Categories of Computer Crime

Grudge Attacks

Grudge Attacks are fueled by personal vendettas, resentment, or revenge. They're often carried out by disgruntled employees, former staff, or individuals with a personal score to settle.

Objectives:

- Sabotage systems or data to hurt the organization
- Leak confidential information to cause embarrassment or damage
- Disrupt operations out of spite
- Inflict reputational or financial harm without financial gain

Common Tactics:

- Deleting or corrupting data
- Changing configurations or disabling services
- Exfiltrating sensitive documents
- Misusing administrative privileges
- Planting logic bombs or backdoors before departure

CHAPTER 19

Grudge attacks are like digital breakups with a scorched-earth clause—hell hath no fury like a sysadmin scorned.

Major Categories of Computer Crime

Grudge Attacks

Grudge Attacks are fueled by personal vendettas, resentment, or revenge. They're often carried out by disgruntled employees, former staff, or individuals with a personal score to settle.

Objectives:

Common Tactics:

lata

s or disabling

cuments

privileges

backdoors before

Notable Examples:

- The San Francisco Muni system hack (2008)—former employee locked out admin access
- Edward Snowden (though often debated, his actions had an ideological element mixed with personal motives)
- Countless insider sabotage cases involving fired IT admins or angry engineers

CISSP Relevance: CISSPs must enforce least privilege, user activity monitoring, and have solid termination procedures to reduce the insider threat risk.

CHAPTER 19

Major Categories of Computer Crime

Thrill Attacks

Thrill Attacks are motivated by curiosity, ego, challenge, or just the desire to stir things up. The attackers aren't in it for money or politics—they're in it for the rush, recognition, or bragging rights.

Objectives:

- Prove technical skill or "hacktivity" to peers
- Gain notoriety or status in online communities
- Satisfy personal curiosity or boredom
- Trigger reactions from companies, media, or law enforcement

Common Tactics:

- Website defacements
- Unauthorized access just to "see if they could"
- Denial-of-Service attacks "for the lols"
- Data leaks or pranks with minimal planning

CHAPTER 19

Major Categories of Computer Crime

Thrill Attacks

These folks don't want to ruin your life—they just want to make headlines or impress their Discord server.

Thrill Attacks are motivated by curiosity, ego, challenge, or just the desire to stir things up. The attackers aren't in it for money or politics—they're in it for the rush, recognition, or bragging rights.

Objectives:

- Prove technical skill or "hacktivity" to peers

Common Tactics:

- Website defacements

ust to "see if

cks "for the lols"

vith minimal

Notable Examples:

- Lizard Squad and Teenage hacktivists showing off skills
- Many members of the original Anonymous movement started this way
- The infamous Morris Worm (1988)—written by a student "just to explore"

CISSP Relevance: CISSPs need to build controls that prevent unauthorized access—even from non-malicious actors—because intent doesn't soften impact. Educating staff, monitoring networks, and reducing attack surfaces are key defenses.

CHAPTER 19

Ethics

Ethics in information security refers to the moral principles and professional standards that guide behavior in the handling of data, systems, and responsibilities.

Key Principles:

- Protect confidentiality, integrity, and availability of information
- Respect privacy and the rights of individuals and organizations
- Avoid harm—don't exploit knowledge or access for personal gain
- Act with honesty, objectivity, and fairness
- Report unethical behavior or vulnerabilities responsibly

Think of ethics as your internal firewall—if your values aren't configured right, no amount of tech can secure your integrity.

CHAPTER 19

Ethics

Organizational Code of Ethics

Think of it as the organization's ethical blueprint—follow it, and you're part of the mission; violate it, and you're a liability.

An Organizational Code of Ethics is a formal document that outlines a company's core values, expectations, and ethical standards for employee conduct.

Key Components:

- Integrity and honesty in all actions
- Respect for confidentiality and privacy
- Proper use of company resources
- Compliance with laws, regulations, and policies
- Accountability and reporting of unethical behavior

CISSP Relevance: Security professionals must follow these codes to maintain trust, reduce legal risk, and align with corporate governance. Violating the code—intentionally or not—can lead to disciplinary action, termination, or legal consequences.

CHAPTER 19

Ethics

(ISC)² Code of Professional Ethics

The (ISC)² Code of Professional Ethics is a formal set of guiding principles all CISSPs and (ISC)² credential holders must follow. It ensures members act with integrity, professionalism, and in a way that supports the public good.

Preample:

"Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior."

What It Means:

- The role of a CISSP is not just technical—it's ethical.
- You're expected to act with integrity and transparency, even when no one is watching.
- The public, employers, and fellow professionals must be able to trust your judgment and actions.

CHAPTER 19

Ethics

(ISC)² Code of Professional Ethics

Think of it as your digital Hippocratic Oath—first, do no harm… and always do what's right, even when it's hard.

The (ISC)² Code of Professional Ethics is a formal set of guiding principles all CISSPs and (ISC)² credential holders must follow. It ensures members act with integrity, professionalism, and in a way that supports the public good.

Preample:

"Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be se

CISSP Relevance: The preamble reminds us that being a CISSP is more than holding a cert—it's about being a trusted steward of information, systems, and societal well-being.

What It Means:

- The role of a CISSP
- You're expected to act with integrity and transparency, even when no one is watching.
- The public, employers, and fellow professionals must be able to trust your judgment and actions.

CHAPTER 19

Ethics

(ISC)² Code of Professional Ethics

Canon 1: Protect society, the common good, necessary public trust, and confidence

What It Means: This canon is all about serving the greater good. As a security professional, your actions impact not just your organization, but also society at large.

Responsibilities:

- Act in ways that build trust in information systems.
- Avoid actions that could harm the public, like ignoring known vulnerabilities or hiding breaches.
- Disclose significant risks responsibly (e.g., through coordinated vulnerability disclosure).
- Promote security awareness, education, and transparency.

2025 CISSP MENTOR PROGRAM

CHAPTER 19

Ethics

(ISC)² Code of Professional Ethics

Canon 1: Protect society, the common good, necessary public trust, and confidence

What It Means: This canon is all about serving the greater good. As a security professional, your actions impact not just your organization, but also society at large.

Responsibilities:

- Act in ways that build trust in infc
- Avoid actions that could harm the breaches.

Real-World Example:
If you discover a critical flaw in a widely used application, you must report it responsibly—not exploit it, ignore it, or post it publicly without coordination.

oordinated vulnerability

arency.

CISSP Relevance: This canon puts ethics above the employer's convenience—if protecting the public means raising a red flag, do it. You're not just a tech pro; you're a guardian of digital trust.

CHAPTER 19

Ethics

(ISC)² Code of Professional Ethics

Canon 2: Act honorably, honestly, justly, responsibly, and legally

What It Means: This canon is about personal and professional integrity. It requires you to be a truth-teller, a law-follower, and someone who treats others fairly—no shortcuts, no shady behavior.

Responsibilities:

- Tell the truth, even when it's uncomfortable.
- Follow the law and company policies at all times.
- Avoid conflicts of interest—and disclose them if they arise.
- Never use your skills to harm others or gain unfair advantage.
- Don't cover for mistakes—own them and correct them.

2025 CISSP MENTOR PROGRAM

CHAPTER 19

Ethics

(ISC)² Code of Professional Ethics

Canon 2: Act honorably, honestly, justly, responsibly, and legally

What It Means: This canon is about personal and professional integrity. It requires you to be a truth-teller, a law-follower, and some[illegible] shortcuts, no shady behavior.

Responsibilities:

- Tell the truth, even when it's uncomfortable.
- [illegible]
- [illegible]ect them.

Real-World Example:
If you discover your company is violating compliance regulations, you can't just look the other way. You're obligated to raise the issue internally, and possibly externally if there's a legal requirement to report.

CISSP Relevance: This canon is your ethical safety net. It reinforces the idea that being technically skilled isn't enough—you must also be morally grounded and legally compliant.

CHAPTER 19

Ethics

(ISC)² Code of Professional Ethics

Canon 3: Provide diligent and competent service to principals

What It Means: This canon is about being a reliable, capable professional for those you serve—whether that's your employer, clients, or stakeholders. It demands competence, care, and loyalty.

Responsibilities:

- Know your stuff—don't take on tasks you're not qualified for.
- Stay current on technology, threats, and best practices.
- Act in your principal's best interest, as long as it doesn't violate the other canons.
- Communicate risks and recommendations clearly, even if they're not what management wants to hear.

2025 CISSP MENTOR PROGRAM

CHAPTER 19

Ethics

(ISC)² Code of Professional Ethics

Canon 3: Provide diligent and competent service to principals

What It Means: This canon is about being a reliable, capable professional for those you serve—whether that's your employer, clients, or stakeholders. It demands competence, care, and loyalty.

Responsibilities:

- Know your stuff—don't take on tasks you're not c
- Stay current on technology, threats, and best pra

it c

arly

Real-World Example:
If your client asks you to secure a cloud environment you're unfamiliar with, you either get trained fast or bring in someone who knows it well. Delivering "good enough" isn't ethical—it's risky.

CISSP Relevance: CISSPs are expected to bring expert-level competence to the table and to work diligently and transparently. Your role isn't just to do what you're told—it's to advise and protect.

CHAPTER 19

Ethics

(ISC)² Code of Professional Ethics

Canon 4: Advance and protect the profession

What It Means: This canon emphasizes your role in strengthening the cybersecurity field—through education, integrity, and mentorship. It's about making the industry better, safer, and more respected.

Responsibilities:

- Uphold high standards in your work and interactions.
- Report unethical behavior or negligence that harms the profession.
- Share knowledge with peers, juniors, and the community.
- Support diversity, inclusion, and ethical growth in the field.
- Reject shortcuts and snake oil—protect the reputation of real security pros.

2025 CISSP MENTOR PROGRAM

CHAPTER 19

Ethics

(ISC)² Code of Professional Ethics

Canon 4: Advance and protect the profession

What It Means: This canon emphasizes your role in strengthening the cybersecurity field—through education, integrity, and mentorship. It's about making the industry better, safer, and more respected.

Responsibilities:

- Uphold high standards in your work a
- Report unethical behavior or negligen
- Share knowledge with peers, juniors

ity.
he field.
ion of real security pros.

Real-World Example:
If you spot someone in your org pushing untested, unethical solutions—or lying to clients—you don't ignore it. You speak up. And if you can mentor a new practitioner, you do that too.

CISSP Relevance: This canon reminds us that being a CISSP means more than technical chops—it's about raising the bar for the entire industry. If we don't protect the profession, no one will trust us to protect anything else.

CHAPTER 19

The (ISC)² Canons are listed in order of priority.

This means: Canon 1 takes precedence over all others, followed by Canon 2, and so on.

So, if you ever face a situation where two canons seem to conflict, here's how a CISSP should approach it:

Conflict Resolution Between Canons:

1. **Start at the top**: Always prioritize the protection of society, the public good, and trust (Canon 1).
   - If acting in your employer's best interest (Canon 3) would harm society, Canon 1 wins.
2. **Follow the legal and moral path (Canon 2)**: Even if it means pushing back against your principal (Canon 3) or harming business interests, the law and ethical conduct come first.
3. **Be loyal, but not blindly (Canon 3)**: Serve your principal diligently, as long as it doesn't violate Canons 1 or 2.
4. **Elevate the profession (Canon 4)**: This is the "bonus round"—do it whenever possible, but not at the expense of the others.

CHAPTER 19

The (ISC)² Canons are listed in order of priority.

This means: Canon 1 takes precedence over all others, followed by Canon 2, and so on.

So, if you ever face a situation where two canons seem to conflict, here's how a CISSP should approach it:

Conflict Resolution

1. **Start at the to**
   - If acting in
2. **Follow the leg**
   (Canon 3) or h
3. **Be loyal, but r**
   Canons 1 or 2.
4. **Elevate the profession (Canon 4)**: This is the "bonus round"—do it whenever possible, but not at the expense of the others.

Example Scenario:

If your employer wants you to cover up a data breach:

- Canon 1: Hiding the breach puts the public and society at risk.
- Canon 2: It's dishonest and likely illegal.
- Canon 3: You're serving your employer, but that doesn't override the higher canons.

Result: You're obligated to report the breach appropriately, even if it's unpopular.

CHAPTER 19

Ethics

RFC 1087 – Ethics and the Internet

RFC 1087, published in 1989 by the Internet Activities Board (IAB), outlines the ethical behavior expected of individuals using the internet—back when it was still a budding research network.

Core Message: The Internet is a privilege and a tool for research and education, and any use that disrupts its integrity, availability, or goals is considered unethical.

Specifically Prohibited

RFC 1087 defines unethical use as:

- Seeking to gain unauthorized access to internet resources
- Disrupting the intended use of the internet
- Wasting resources (people, bandwidth, computing cycles)
- Destroying data integrity
- Compromising privacy of users

CHAPTER 19

Ethics

RFC 1087 – Ethics and the Internet

Think of it as the internet's original golden rule—don't be a digital jerk.

RFC 1087, published in 1989 by the Internet Activities Board (IAB), outlines the ethical behavior expected of individuals using the internet—back when it was still a budding research network.

Core Message: The Internet is a privilege and a tool for research and education and any use that disrupts its integr

Specifically Prohibited

RFC 1087 defines unethical use as:

- Seeking to gain unauthorized a
- Disrupting the intended use of the internet
- Wasting resources (people, bandwidth, computing cycles)
- Destroying data integrity
- Compromising privacy of users

CISSP Relevance:

RFC 1087 laid the groundwork for early network ethics and still influences modern views on responsible internet use. While dated, its principles echo in today's acceptable use policies, security standards, and professional codes of conduct.

CHAPTER 19

Ethics

Ten Commandments of Computer Ethics

Published by the Computer Ethics Institute in 1992, these “commandments” provide a simple ethical framework for using computers and information systems responsibly.

The 10 Commandments:

1. Thou shalt not use a computer to harm other people.
   → No hacking, bullying, or crashing systems.
2. Thou shalt not interfere with other people’s computer work.
   → Don’t disrupt or sabotage others’ operations.
3. Thou shalt not snoop around in other people’s computer files.
   → Respect privacy and data confidentiality.
4. Thou shalt not use a computer to steal.
   → This includes data theft, software piracy, or financial fraud.
5. Thou shalt not use a computer to bear false witness.
   → No spreading false info, impersonation, or fake data.

CHAPTER 19

Ethics

Think of them as your moral firewall ruleset—simple, powerful, and still totally relevant.

Ten Commandments of Computer Ethics

Published by the Computer Ethics Institute in 1992, these "commandments" provide a simple ethical framework for responsibly.

CISSP Relevance:
While a bit dated and idealistic, these commandments are still a great foundation for ethical behavior in cybersecurity—especially for training, policy writing, or awareness programs.

The 10 Commandments:

1. Thou shalt nc
   → No hac
2. Thou shalt nc
   → Don't c
3. Thou shalt nc
   → Respec
4. Thou shalt nc
   → This inc
5. Thou shalt nc
   → No spre
6. Thou shalt not copy or use proprietary software you have not paid for.
   → Don't pirate or misuse licensed software.
7. Thou shalt not use other people's computer resources without authorization.
   → Unauthorized access = unethical, even if harmless.
8. Thou shalt not appropriate other people's intellectual output.
   → Respect authorship, credit, and copyright.
9. Thou shalt think about the social consequences of the program you write.
   → Code ethically—don't create tools for abuse or harm.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.
    → Tech should empower—not degrade—others.

CHAPTER 19

Ethics

Think of FIPs as the ethical backbone of data privacy—if you're handling personal info, this is your golden rulebook.

Code of Fair Information Practices (FIPs)

The Code of Fair Information Practices is a foundational set of privacy principles developed by the U.S. Department of Health, Education, and Welfare (HEW) in 1973. It laid the groundwork for modern data privacy laws and frameworks worldwide.

Core Principles:

1. **Notice/Awareness** - Individuals should be informed when their data is collected and why.
2. **Choice/Consent** - Individuals should have a say in how their data is used and shared.
3. **Access/Participation** - People should be able to view and correct their personal data.
4. **Integrity/Security** - Data must be accurate and reasonably protected from misuse or breach.
5. **Enforcement/Redress** - There must be a way to enforce these rules and resolve violations.

CISSP Relevance:

CISSPs must be familiar with FIPs because they influence laws like GDPR, HIPAA, CCPA, and organizational policies around data collection, consent, and protection.

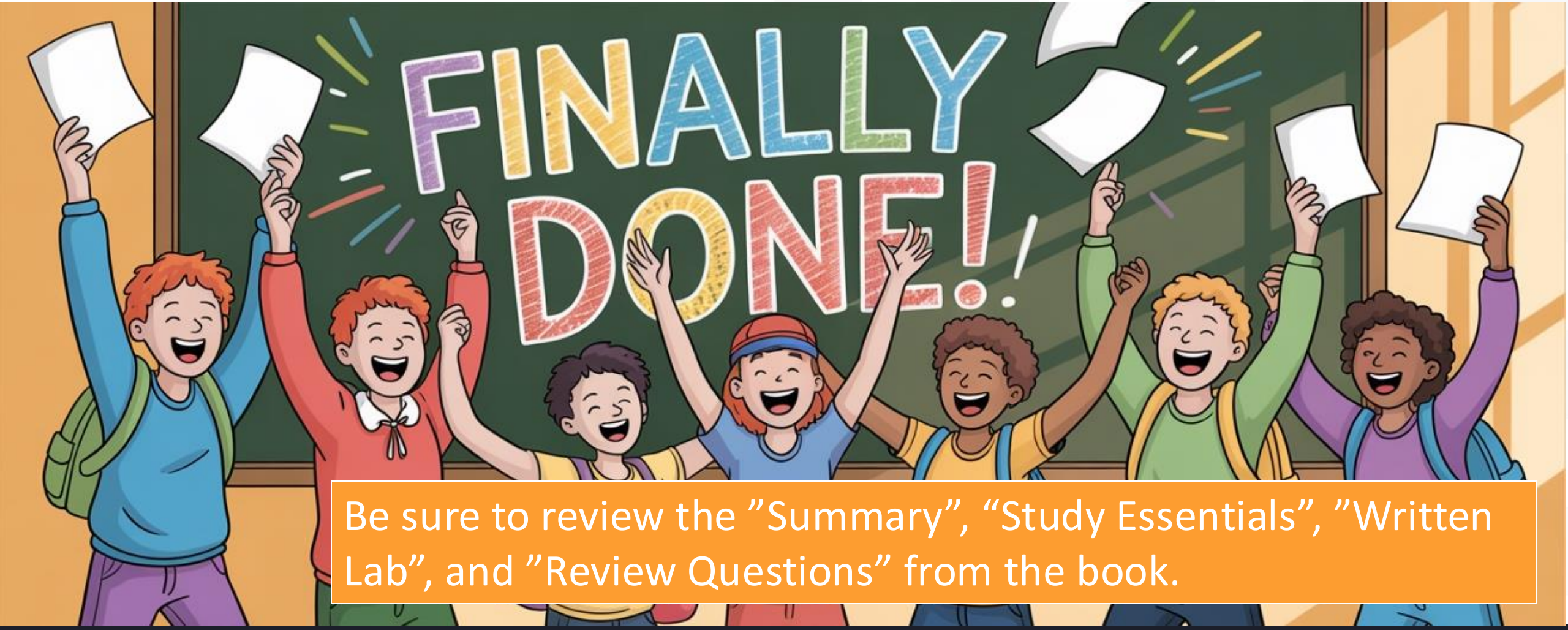
2025 CISSP MENTOR PROGRAM

CHAPTER 19

Investigations and Ethics

CONGRATULATIONS!

You stuck it out. (only 100 slides later)



Be sure to review the ”Summary”, “Study Essentials”, ”Written Lab”, and ”Review Questions” from the book.