

Defining Cybercrime

MSCS630: Cybercrime Investigation and Digital Evidence

Dr. Mouatez Karbab



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

September 23, 2026



Outline

- 1 The Evolution of Digital Crime
- 2 A Modern Cybercrime Taxonomy
- 3 The Global Threat Landscape
- 4 Key Legal and Jurisdictional Challenges



Introduction to Defining Cybercrime I

Chapter Objectives

- What cybercrime is, and how it evolved.
- How motive shapes an attack and its legal problems.
- Who commits these crimes and why.
- How modern cybercrime is classified.

Why This Matters

- Understanding cybercrime is essential for any modern digital investigator.
- Motive shapes an attack, and shapes the legal challenges too.
- Classification decides method, tools and applicable law.



Outline

- 1 The Evolution of Digital Crime
- 2 A Modern Cybercrime Taxonomy
- 3 The Global Threat Landscape
- 4 Key Legal and Jurisdictional Challenges



Reading the History Correctly I

- To understand today's cybercrime, first look at its history.
- The history tracks changing motives, not single technical events.
- It also tracks growing damage.
- And a constant back-and-forth between criminals and investigators.
- Shift from system exploration to government-backed attacks.
- Mirrors the internet's own growth: academic network to global foundation.



Early Days: Phone Phreaking I

- Earliest precursors were not about making money.
- Driven by curiosity and the wish to become famous.
- 1970s: exploration of how telephone systems worked.

Definition: Phone Phreaks

- People who explored the telephone network's inner workings.
 - Famous example: John Draper, called "Captain Crunch".
 - Used simple tools to make free long-distance calls [11].
-
- This was exploration, not organized crime.
 - First proof: clever people could control complex systems.
 - Control followed from understanding the rules.

From Exploration to Harm I

- As computers became connected, exploration turned into harm.
- Hacking groups such as the Legion of Doom broke into systems.
- No longer curious: they stole data and damaged systems.
- The true turning point came in 1988.
- One action could now cause huge damage everywhere.



Case Study: The Morris Worm I

Real-World Story: The Morris Worm

- November 2, 1988: Robert Tappan Morris, a Cornell student.
- Released a small program onto the early internet.
- Stated purpose: measure how big the network was.

Definition: Worm

- Malicious software that copies itself to spread between computers.
- Spreads automatically, without a user opening anything.



- A coding mistake made it spread far faster than expected.
- Infected and crashed roughly 6,000 of about 60,000 machines.
- About one machine in ten, then on the internet.
- One person could cause widespread damage, even by accident.
- Produced the first Computer Emergency Response Team (CERT/CC).
- First person convicted under the Computer Fraud and Abuse Act [14].

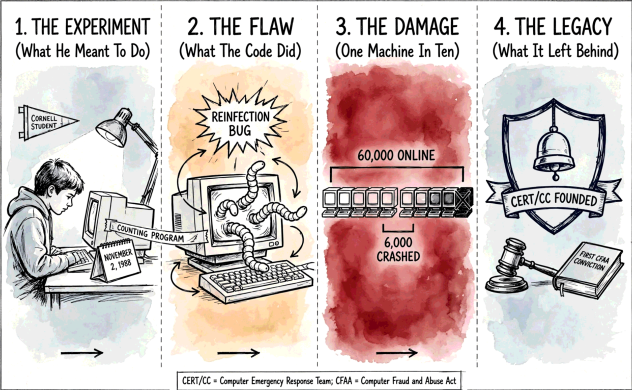


The Morris Worm I

- Four stages: experiment, reinfection flaw, mass damage, legal response.
- The defect was reinfection: each host accepted the worm repeatedly.
- Intent was measurement; outcome was one machine in ten.
- Damage scale, not intent, drove the institutional response.
- CERT/CC and the first CFAA conviction both date from this case [14].



The Morris Worm I



Intent: a program written to measure the size of the network.

Outcome: one machine in ten down, and the first computer-crime conviction.

- Digital evidence then was very basic compared with today.
- Notes written by system administrators.
- Server logs.
- Records of telephone connections.
- Digital forensics was just beginning as a field.
- It was still learning to handle this new type of crime.



Commerce Arrives, Crime Follows I

- Late 1990s: businesses started using the internet to make money.
- As legal business moved online, crime moved with it.
- Many non-technical people came online for the first time.
- That mix created a good environment for fraud.
- Early e-commerce sites such as eBay saw auction fraud.
- The first major phishing emails appeared.

Definition: Phishing

- Fake emails that trick users into giving up personal data.
- Target is personal and financial information.



Malware Becomes a Profession I

- Simple viruses were often written to show off skill.
- They changed into complex tools built only to make money.
- Banking trojans were developed in this period.

Definition: Banking Trojan

- Malware designed specifically to steal online banking information.
- By the late 2000s the professionalization was complete.



Zeus and the Command-and-Control Model I

- Zeus trojan first identified in July 2007.
- Built to steal banking credentials on a very large scale.
- Infected computers, called *bots*, connected to a central server.

Definition: Command-and-Control (C2) Server

- The central server the criminals control.
- From it they collect data and record keystrokes.
- From it they start fake money transfers [2].



Exploit Kits Lower the Bar I

Definition: Exploit Kit

- Software package that automates attacks on computers.
- Uses known weaknesses in browsers and other software.
- Appeared during the same period as the banking trojans.
- Allowed criminals with fewer technical skills to infect victims.



- By the late 2000s the motive was settled: money.
- Each gang still did most of the work itself.
- The next change was organisational rather than technical.



CryptoLocker Solves the Payment Problem I

- 2013: CryptoLocker combined strong file encryption with Bitcoin payment.

Definition: Bitcoin

- Digital currency payable without a bank account or a name.
- Solved the problem that had always limited extortion: collecting money safely.
- Once payment worked, encryption beat stealing banking passwords.
- The victim pays the criminal directly.
- No stolen data has to be matched to a buyer.



Division of Labour: RaaS, Affiliates, Brokers I

Definition: Ransomware-as-a-Service (RaaS)

- One group writes and maintains the malware, and rents it out.
- Renters break in, deploy it, hand back a share of proceeds.

Definition: Affiliate

- The criminal who rents the ransomware and runs the intrusion.

Definition: Initial Access Broker (IAB)

- Specialist who only breaks into company networks.
- Sells that access on to whoever wants it.
- A third group launders the proceeds.
- Chapter 2 covers this service economy and its roles in full.



What the Model Made Possible I

WannaCry, May 2017

- Worm that spread ransomware automatically machine to machine.
- Reached more than 150 countries in a few days.
- Disrupted hospitals, factories and transport operators.
- Victims had no connection to each other [17, 9].

Colonial Pipeline, 2021

- A single affiliate of the DarkSide service.
- Stopped fuel supplies along the United States East Coast [6].



Double Extortion and the Leak Site I

- Around 2019 the same groups added a second lever.
- Before encrypting, they copy the data out.
- Then threaten to publish it on a public *leak site*.

Definition: Double Extortion

- Encrypt the data and threaten to publish it.
- A victim with good backups still has a problem.

How Far Professionalization Went

- Conti internal chat logs leaked in 2022.
- They show salaries, performance reviews and an office structure [10].
- Payments through the economy are measured in billions of dollars a year [3].



What This Changes for the Investigator I

- Break-in, encryption and payment may be three different people.
- Three countries, and they may never have met.
- The evidence is scattered to match.
- Access sold on a forum months before the intrusion.
- A payment address on a public blockchain.
- An affiliate identifier in the ransom note.
- A leak-site post fixing the date data left the network.

Consequence

- No single machine holds the whole story any more.



A New Speed, Not a New Motive I

- The most recent shift is not a new motive.
- Money is still the point.
- More of the work is done by software that decides its next action.

Europol Assessment

- 2026 assessment of organised cybercrime.
- A phase defined by speed, scale and sophistication.
- Warns of a widening gap between offender speed and police response [7].

Two Documented Cases I

Espionage Campaign, November 2025

- An AI system carried out the intrusion work itself.
- Took direction from a small human team.
- Not merely doing preparation for one [1].
- Now a named campaign in MITRE ATT&CK [13].

Unit 42 Investigation, September 2026

- Agentic tooling ran a full attack chain.
- Work an experienced operator would take about two weeks to do.
- Finished in under ten hours [5].

- Chapter 2 takes up what this does to the criminal supply chain.



Two Consequences for the Investigator I

Response Time

- Incident-response plans are sized for intrusions lasting days.
- They are not sized for one finishing inside a single shift.
- Monitoring read each morning reports a completed attack.

Where the Decision Record Lives

- When software chooses the next action, the reasoning is recorded.
- That record sits in the attacker's own AI infrastructure.
- Not on the victim's network.
- Material that would settle attribution is out of reach.

- Motive still predicts where the evidence lands.
- The last two eras changed how widely it is scattered.
- And how little time there is to collect it.

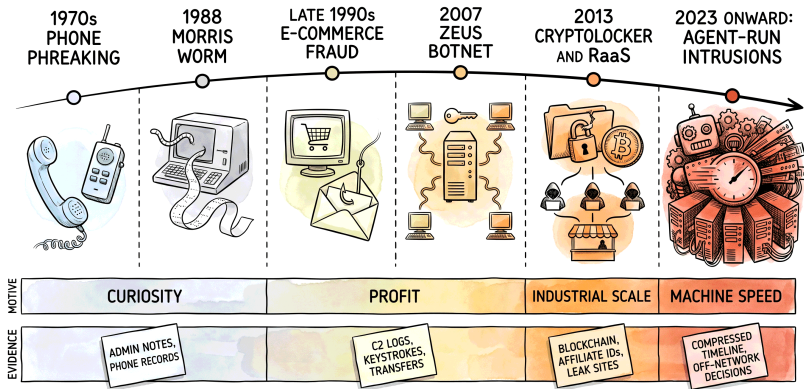


Motive and Evidence Over Time I

- One arc, with the motive band aligned to the evidence band beneath.
- Curiosity: administrator notes, server logs, telephone records.
- Profit: C2 logs, keystroke captures, bank transfer records.
- Industrial scale: blockchain flows, affiliate identifiers, leak-site posts.
- Machine speed: a compressed timeline, decision record held off-network.
- Reading rule: name the motive, and you can predict the evidence.



The Evolution of Digital Crime I



Early eras: one offender, and the evidence sat on the machine he touched.

LEGEND: C2 = Command-and-Control server;
RaaS = Ransomware-as-a-Service

Later eras: a supply chain and an agent, and the evidence is scattered and short-lived.



Hands-On: Mapping an Era to Its Evidence I

Objective

- Predict the available evidence from an incident's era and motive.

Prerequisites

- The four eras from this section: curiosity, profit, industrial, machine speed.
- Public write-ups of Morris, Zeus, WannaCry and Colonial Pipeline.

Steps

- 1 Draw four columns, one per era.
- 2 Place each of the four incidents in its column.
- 3 List the evidence sources each incident would have left.
- 4 Mark which sources sit on the victim's own network.
- 5 Mark which sit with a third party or an attacker.
- 6 Repeat the exercise for a hypothetical agent-run intrusion.



Hands-On: Mapping an Era to Its Evidence II

Expected Outcome

- Victim-held evidence shrinks as you move right.
- Third-party and off-network evidence grows.

Common Pitfalls

- Treating era as technology; it is motive plus organisation.
- Assuming the victim's network still holds the whole story.



Section 1: Assessment (1/3) I

Question 1

Primary motivation for 1970s phone phreaks?

- A. Financial gain via wire fraud.
- B. Political protest.
- C. Intellectual curiosity and exploration.
- D. Selling compromised phone lines.



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

Question 1

Primary motivation for 1970s phone phreaks?

- A. Financial gain via wire fraud.
- B. Political protest.
- C. Intellectual curiosity and exploration. (✓)
- D. Selling compromised phone lines.

Explanation:

- Driven by exploration and notoriety, not profit [11].



Section 1: Assessment (2/3) I

Question 2

What made CryptoLocker a turning point in 2013?

- A. It was the first self-replicating worm.
- B. It paired strong encryption with anonymous Bitcoin payment.
- C. It stole banking credentials at scale.
- D. It targeted industrial control systems.



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

Question 2

What made CryptoLocker a turning point in 2013?

- A. It was the first self-replicating worm.
- B. It paired strong encryption with anonymous Bitcoin payment. (✓)
- C. It stole banking credentials at scale.
- D. It targeted industrial control systems.

Explanation:

- Collecting the money safely had always limited extortion.
- Bitcoin solved it, and the victim then pays the criminal directly.



Section 1: Assessment (3/3) I

Question 3

In the machine-speed era, why is attribution harder?

- A. Encryption is stronger than before.
- B. Victims stop keeping logs.
- C. The attacker's decision record sits off the victim's network.
- D. Blockchains are unreadable.



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

Question 3

In the machine-speed era, why is attribution harder?

- A. Encryption is stronger than before.
- B. Victims stop keeping logs.
- C. The attacker's decision record sits off the victim's network. (✓)
- D. Blockchains are unreadable.

Explanation:

- When software chooses the action, the reasoning lives in attacker infrastructure [1].
- Response windows also compress from weeks to hours [5].

Outline

- 1 The Evolution of Digital Crime
- 2 A Modern Cybercrime Taxonomy
- 3 The Global Threat Landscape
- 4 Key Legal and Jurisdictional Challenges



Why Classification Matters I

- Investigating and prosecuting well needs a clear way to organize crimes.
- A good classification system is called a *taxonomy*.

Definition: Taxonomy

- A formal system for naming and classifying things.

What It Buys the Investigator

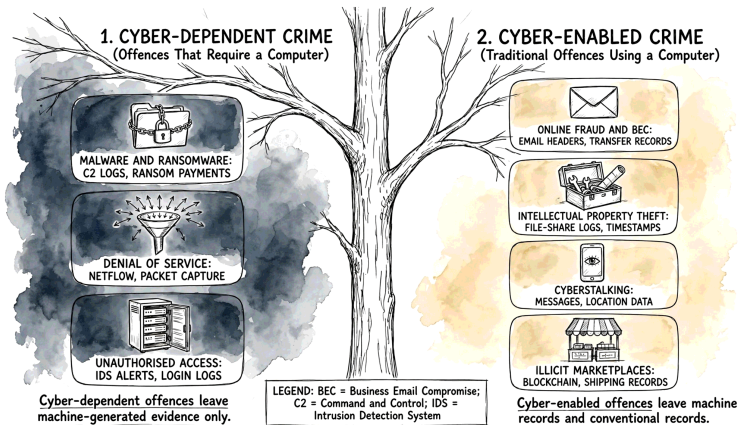
- The right investigation method.
 - The correct tools.
 - The relevant laws.
-
- Modern cybercrimes divide into two main groups.
 - Cyber-dependent and cyber-enabled [12].

The Taxonomy Split I

- One trunk splitting two ways, each leaf tagged with its evidence.
- Cyber-dependent leaves only machine-made traces.
- Cyber-enabled mixes machine traces with ordinary business records.
- The evidence tags make it a forensics chart, not a definition chart.
- Choosing the branch tells you which records to request first.



The Taxonomy Split I



Cyber-Dependent Crimes: Definition I

Definition

- Crimes that can only happen using computers or networks.
- Or other information technology.
- They exist only because of digital technology.
- They have no equivalent in the physical world.

Using Malware and Ransomware I

- Creation, changing and sharing of malicious software.

Definition: Ransomware

- Malware that locks a victim's files.
- Demands a payment, a ransom, to unlock them.
- Using malware is the basic action behind many other crimes.

Key Evidence

- The malware program itself, for detailed analysis.
- Logs from C2 servers.
- Network traffic data showing the malware's activity.
- Records of cryptocurrency payments for ransoms.

Denial-of-Service Attacks I

Definition: Denial-of-Service (DoS)

- Overloads a target system, service or network with traffic.
- Makes the system unavailable to normal users.

Definition: Distributed Denial-of-Service (DDoS)

- A larger attack using many computers to send the traffic.

Key Evidence

- *Network flow data* such as NetFlow: summary traffic information.
- *Full packet capture (PCAP)*: a complete recording of network data.
- Logs from botnet C2 servers.
- Logs from illegal "booter/stresser" services rented to run the attack.



Case Study: SYN Flood Attack I

Practical Demo: SYN Flood Attack

- A classic DoS attack against the TCP connection setup.
- Abuses the normal *three-way handshake* used to start a connection.
- Attacker sends many connection requests (SYN packets) to the server.
- The packets usually carry fake sender IP addresses.
- The server replies to each one and waits for a final response.
- That response never comes.
- The server's memory for new connections fills up.
- Real users can no longer connect.



SYN Flood: The Attacker's Loop I

```

1  # Attacker's script (concept)
2  function syn_flood(target_ip, target_port):
3      while True:
4          # Spoof the source IP to hide origin and
5          # prevent reset packets from reaching us.
6          spoofed_ip = generate_random_ip()
7
8          # Create and send the SYN packet.
9          packet = create_syn_packet(
10             source_ip=spoofed_ip,
11             dest_ip=target_ip,
12             dest_port=target_port
13         )
14         send(packet)

```

- In pseudocode the main action is simple: spoof, build, send, repeat.
- Spoofing hides the origin and keeps reset packets away from the attacker.
- Thousands of bots doing this at once is a DDoS.
- It can easily use up all the resources of a powerful server.

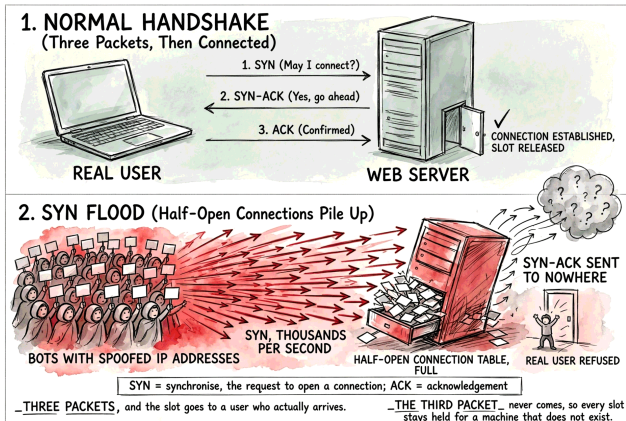


The SYN Flood I

- Upper panel: normal handshake, SYN, SYN-ACK, ACK, connection established.
- Lower panel: spoofed source IPs, so SYN-ACKs go to addresses that never reply.
- The half-open connection table fills, and the real user is refused.
- The missing third packet, not packet volume, is the mechanism.
- Complements the pseudocode rather than replacing it.



The SYN Flood I



Hacking and Unauthorized Access I

- Illegally entering a computer system or network.
- This is the main act of breaking in.

Definition: IDS/IPS

- Intrusion Detection and Prevention Systems.
- Security tools that monitor a network for malicious activity.

Key Evidence

- Firewall logs and IDS/IPS logs.
- System login records: Windows Event Logs, Linux auth.log.
- Clues that an attacker moved between internal computers.
- That movement is called *lateral movement*.



Cyber-Enabled Crimes: Definition I

Definition

- Traditional crimes made bigger or easier by computers and the internet.
- The crime could happen without technology.
- Technology acts as a powerful amplifier.



Online Fraud and Scams I

- A wide category of crimes.
- *Business Email Compromise (BEC)*.
- Romance scams.
- Investment fraud.
- The internet reaches many victims worldwide at once.
- It also makes hiding identity easier.

Key Evidence

- *Email headers*: technical details showing an email's true origin.
- Records of fake money transfers.
- Data from social media accounts.



Intellectual Property Theft I

- Theft of business secrets.
- Illegal copying of copyrighted software, movies and music.

Definition: Intellectual Property (IP)

- Creations of the mind, such as inventions or artistic works.
- Protected by law.

Key Evidence

- Logs from file-sharing networks.
- Records of who accessed company servers.
- File timestamps showing when secret data was viewed or stolen.



Cyberstalking and Harassment I

- Use of digital communications to threaten or scare a person.

Key Evidence

- Content of social media posts.
- Private messages and emails.
- Location data from mobile phones, showing where suspect and victim were.



Selling Illegal Goods Online I

- Online websites used to sell drugs, weapons or stolen data.
- Especially sites on the *dark web*.

Definition: Dark Web

- Part of the internet reachable only with special software.
- Designed for anonymity.

Key Evidence

- Dark web forum posts.
- Cryptocurrency transaction records on the blockchain.
- Normal shipping information.



Hands-On: Classifying an Incident I

Objective

- Place an incident on the taxonomy and derive its evidence list.

Prerequisites

- The two branches and their leaves from this section.
- Three short incident descriptions, one ambiguous on purpose.

Steps

- 1 Ask whether the crime could exist without computers.
- 2 Assign the branch: cyber-dependent or cyber-enabled.
- 3 Name the leaf under that branch.
- 4 Write the evidence sources the chapter attaches to that leaf.
- 5 For a ransomware case with data theft, list both branches' evidence.
- 6 Mark which sources need a third-party legal request.



Hands-On: Classifying an Incident II

Expected Outcome

- An evidence list derived from the classification, not from guesswork.
- A worked example of an incident that spans both branches.

Common Pitfalls

- Classifying by tool used instead of by whether the crime needs computers.
- Forgetting that ordinary business records matter for cyber-enabled crime.



Section 2: Assessment (1/3) I

Question 1

Which best defines a cyber-dependent crime?

- A. Any crime where a computer was present.
- B. A crime that can only exist because of digital technology.
- C. A traditional crime made easier by the internet.
- D. Any crime investigated by a digital forensics team.



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

Question 1

Which best defines a cyber-dependent crime?

- A. Any crime where a computer was present.
- B. A crime that can only exist because of digital technology. (✓)
- C. A traditional crime made easier by the internet.
- D. Any crime investigated by a digital forensics team.

Explanation:

- Cyber-dependent offences have no physical-world equivalent [12].
- Option C describes the cyber-enabled branch.



Section 2: Assessment (2/3) I

Question 2

Why does a SYN flood exhaust the server?

- A. The SYN packets are unusually large.
- B. The server's disk fills with log entries.
- C. The final ACK never arrives, so entries stay half-open.
- D. Encryption makes each handshake expensive.



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

Question 2

Why does a SYN flood exhaust the server?

- A. The SYN packets are unusually large.
- B. The server's disk fills with log entries.
- C. The final ACK never arrives, so entries stay half-open. (✓)
- D. Encryption makes each handshake expensive.

Explanation:

- Spoofed sources never answer the SYN-ACK.
- The half-open connection table fills and real users are refused.



Section 2: Assessment (3/3) I

Question 3

Which evidence pair does the chapter attach to DDoS investigation?

- A. Email headers and bank transfer records.
- B. NetFlow data and booter/stresser service logs.
- C. File timestamps and file-share logs.
- D. Mobile location data and social media posts.



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

Question 3

Which evidence pair does the chapter attach to DDoS investigation?

- A. Email headers and bank transfer records.
- B. NetFlow data and booter/stresser service logs. (✓)
- C. File timestamps and file-share logs.
- D. Mobile location data and social media posts.

Explanation:

- Flow data summarises the traffic; PCAP records it in full.
- Booter logs and botnet C2 logs identify who rented the attack.
- The other pairs belong to cyber-enabled leaves.



Outline

- 1 The Evolution of Digital Crime
- 2 A Modern Cybercrime Taxonomy
- 3 The Global Threat Landscape
- 4 Key Legal and Jurisdictional Challenges



Know Your Enemy I

- A good investigator must "know their enemy."
- Understand why a criminal acts.
- Understand what resources they have.
- Understand what methods they usually use.

Motive Is Not Abstract

- It predicts what an attacker will touch.
- It predicts what they will take.
- Therefore it predicts where the evidence will be.
- Money: encrypt file servers and move funds.
- Secrets: read mail archives quietly, leave the files alone.
- The two leave very different trails.



Four Broad Actor Groups I

Financially Motivated Actors

- Often organized crime groups (OCGs).
- Treat crime as a business.
- Ransomware, business email compromise, phishing.
- Theft of data for resale.

Nation-State Actors

- Usually called advanced persistent threats (APTs).
- Funded by a government.
- Work slowly and quietly.
- Espionage, IP theft, sabotage of critical infrastructure.



Four Broad Actor Groups II

Ideological Actors

- Hacktivists and terrorist groups.
- Act for a political or social cause, not for profit.

Insiders

- Current or former employees, contractors or partners.
- Misuse access they were legitimately given.
- Motive is money or revenge.

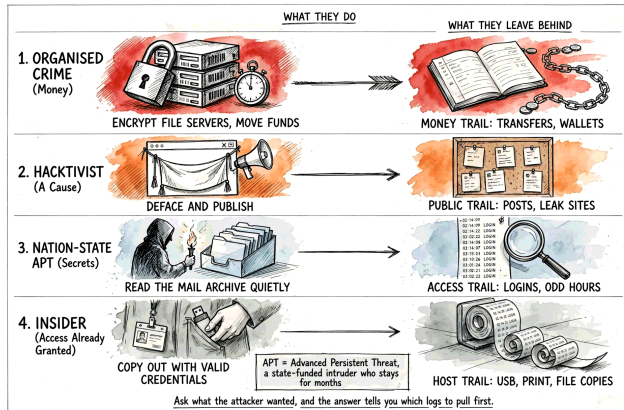


Motive Predicts Evidence I

- Four lanes, one per actor group.
- Each lane runs motive, then typical action, then the trail left behind.
- Ransomware leaves a money trail: encryption plus fund movement.
- Espionage leaves an access-pattern trail, with files untouched.
- An untouched file set is itself a finding, not an absence of evidence.
- Chapter 2 owns adversary profiling; this stays on motive to evidence.



Motive Predicts Evidence I



Where This Goes Next I

- These categories are developed further in the next chapter.
- So is the range of skill within each of them.
- So is the service economy that supplies all of them with tools.
- Chapter 2 covers adversary profiling and Cybercrime-as-a-Service.
- Two examples are worth meeting here.
- Each shows how directly a motive shapes the evidence left behind.



Case Study: A Typical BEC Attack I

Real-World Story: A Typical BEC Attack

- 1 Attacker registers a look-alike domain name.
- 2 For example legitcorp.com versus legitc0rp.com.
- 3 Uses a site like LinkedIn to find the CEO and CFO names.
- 4 Emails the CFO while pretending to be the CEO.
- 5 Claims an urgent, secret transfer for a new partner in Asia.
- 6 Asks to pay invoice #7892 immediately.
- 7 Urgency plus apparent authority makes the CFO skip safety checks.
- 8 Money goes to a bank account the attacker controls.
- 9 Funds are withdrawn or moved through many accounts to hide them.



Case Study: A Typical BEC Attack II

Impact and Evidence

- Losses can reach hundreds of thousands of dollars [8].
- Motive is money, so the trail is a money trail.
- A look-alike domain registration.
- A set of email headers.
- A chain of bank transfers.



Case Study: Stuxnet I

Real-World Story: Stuxnet

- Worm found in 2010, a top example of a nation-state cyber weapon.
- Very advanced malware, believed built by the United States and Israel.
- One specific, physical goal: damage Iran's nuclear program.
- Targeted the industrial control systems at the Natanz facility.

Definition: Industrial Control System (ICS)

- A computer system that manages physical machinery.



100

10. *Journal of the American Medical Association*, 2000; 284: 2689-2695.

- Secretly changed centrifuge speeds, making them destroy themselves.
- Simultaneously reported normal operation to the engineers.
- Proved that code could cause real physical damage.
- Blurred the line between digital attacks and traditional warfare [18].
- Motive was sabotage, so the evidence was not financial.
- The decisive evidence was the machinery's own behaviour.
- And the gap between what controls did and what they reported.



Hands-On: Reasoning from Motive to Evidence I

Objective

- Build an evidence collection list from a stated motive alone.

Prerequisites

- The four actor groups from this section.
- The BEC and Stuxnet case studies.

Steps

- 1 Take one scenario: a file server encrypted overnight.
- 2 Take a second: a mail archive read for six months, nothing changed.
- 3 For each, name the most likely actor group.
- 4 List the first five evidence sources you would collect.
- 5 Note which source would disprove your chosen motive.
- 6 Swap the assumed motives and redo both lists.



Hands-On: Reasoning from Motive to Evidence II

Expected Outcome

- Two clearly different collection lists from the same network.
- An explicit disproof condition for each hypothesis.

Common Pitfalls

- Treating quiet access as "no incident" rather than espionage.
- Collecting everything instead of collecting what the motive predicts.



Section 3: Assessment (1/3) I

Question 1

An intruder reads a mail archive for months and changes nothing. Most likely group?

- A. Financially motivated organized crime group.
- B. Nation-state actor conducting espionage.
- C. Hacktivist seeking publicity.
- D. Booter service customer.



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

Question 1

An intruder reads a mail archive for months and changes nothing. Most likely group?

- A. Financially motivated organized crime group.
- B. Nation-state actor conducting espionage. (✓)
- C. Hacktivist seeking publicity.
- D. Booter service customer.

Explanation:

- APTs work slowly and quietly, and leave the files alone.
- Only the pattern of access gives them away.



Section 3: Assessment (2/3) I

Question 2

In a BEC case, which artefact set is decisive?

- A. Centrifuge speed logs and ICS telemetry.
- B. Look-alike domain registration, email headers, bank transfers.
- C. NetFlow summaries and PCAP files.
- D. Mobile location data and forum posts.



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

Question 2

In a BEC case, which artefact set is decisive?

- A. Centrifuge speed logs and ICS telemetry.
- B. Look-alike domain registration, email headers, bank transfers. (✓)
- C. NetFlow summaries and PCAP files.
- D. Mobile location data and forum posts.

Explanation:

- The motive is money, so the trail is a money trail [8].
- Option A belongs to the Stuxnet sabotage case [18].



Section 3: Assessment (3/3) I

Question 3

What made Stuxnet significant beyond its technical sophistication?

- A. It was the first ransomware to demand Bitcoin.
- B. It proved code could cause real physical damage.
- C. It was the first worm to spread over the internet.
- D. It introduced double extortion.



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

Question 3

What made Stuxnet significant beyond its technical sophistication?

- A. It was the first ransomware to demand Bitcoin.
- B. It proved code could cause real physical damage. (✓)
- C. It was the first worm to spread over the internet.
- D. It introduced double extortion.

Explanation:

- It destroyed centrifuges while reporting normal operation.
- It blurred the line between digital attack and warfare [18].



Outline

- 1 The Evolution of Digital Crime
- 2 A Modern Cybercrime Taxonomy
- 3 The Global Threat Landscape
- 4 Key Legal and Jurisdictional Challenges



Borderless Crime, Bordered Law I

- Cybercrime investigation carries legal problems traditional crime does not.
- The internet has no borders.
- Laws are based on physical countries.
- That mismatch is the source of the difficulty.

Attribution: The Main Challenge I

Definition: Attribution

- Proving who was responsible for an attack.
- Extremely difficult to prove who was at the keyboard.
- Attackers use tools to hide their location.
- They use hacked computers in other countries as relays.
- They use fake information to hide where they are from.



The Jurisdiction Problem I

- The technical problem is made worse by independent national laws.

The Chapter's Scenario

- An attacker in Russia.
- Uses a hacked server in Malaysia.
- Attacks a victim in Canada.

The Open Questions

- Which country's laws should be used?
- How can a Canadian investigator legally get evidence from Malaysia?
- When the server is controlled by a person in Russia?



The Legal Instruments I

Computer Fraud and Abuse Act (CFAA)

- United States law.
- The main law against hacking into computers.

Budapest Convention

- The Council of Europe's Convention on Cybercrime.
- The most important international agreement for cross-border cases.
- Tries to make national cybercrime laws more similar.
- Improves investigation methods.
- Encourages countries to work together [4].
- The framework has widened considerably since it was drafted.
- A protocol now speeds up cross-border requests.
- A first cybercrime treaty of global rather than regional reach exists.
- Chapter 2 takes up these instruments in detail.

MLATs and the Speed Mismatch I

Definition: Mutual Legal Assistance Treaty (MLAT)

- Formal agreement between countries to help each other with legal cases.
- Even with agreements, cross-border evidence is slow to obtain.
- The process carries many official rules.
- An MLAT request can take months or even years.

Why It Fails Digital Cases

- Far too slow for digital investigations.
- Evidence can be deleted in seconds.

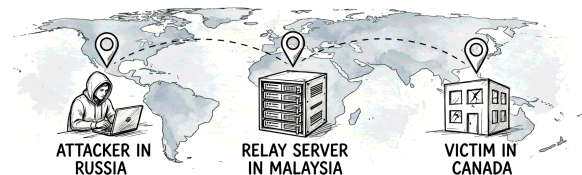
The Jurisdiction Gap I

- A three-country hop: Russia, Malaysia, Canada.
- Two clocks set against each other are the point of the figure.
- Attack clock: three legal systems crossed in one second.
- Process clock: an MLAT measured in months to years.
- CFAA and the Budapest Convention are marked as what exists.
- The gap between the clocks is what they do not close [4].



The Jurisdiction Gap I

1. ATTACK PATH ACROSS THREE COUNTRIES



2. ATTACK TIME COMPARED WITH LEGAL PROCESS TIME



One attack crosses three legal systems in about one second.

MLAT = Mutual Legal Assistance Treaty;
CFAA = Computer Fraud and Abuse Act

Evidence is often deleted before an MLAT request is completed.



Case Study: The Anonymity Challenge I

Practical Demo: The Anonymity Challenge

- Criminals use *The Onion Router (Tor)* to hide location and activity.
- A site hosted on Tor is called a *hidden service*.
- Its address ends in `.onion`, like this:

`http://2gzyxa5ihm7nsggfxnu52rck2vv4rvmdlkiu3zzui5du4xyc1en53wid.onion/`

Reading the Address

- The address is not a name at all.
- It is the service's own public key, written out in 56 characters.
- This is the version 3 format.
- It replaced the 16-character version 2 format.
- Tor withdrew version 2 support in October 2021 [15].





Hands-On: Timing a Cross-Border Request I

Objective

- Show why evidence expires before formal cooperation delivers it.

Prerequisites

- The Russia, Malaysia, Canada scenario from this section.
- Published retention periods for a hosting provider and an ISP.

Steps

- 1 Draw the attack path and mark each legal system it crosses.
- 2 Write the retention period beside each evidence source.
- 3 Write a realistic MLAT duration beside the request.
- 4 Mark every source whose retention is shorter than that duration.
- 5 Identify which sources a preservation request could hold.
- 6 Note what remains unreachable if the host is a Tor hidden service.



Hands-On: Timing a Cross-Border Request II

Expected Outcome

- A written list of evidence lost purely to process delay.
- A short list of actions that must happen before the MLAT is filed.

Common Pitfalls

- Assuming a treaty exists between every pair of countries.
- Treating preservation and production as the same request.



Section 4: Assessment (1/3) I

Question 1

What is attribution in a cybercrime investigation?

- A. Assigning a case to the correct court.
- B. Proving who was responsible for an attack.
- C. Classifying the crime under a taxonomy.
- D. Calculating the financial loss.



Section 4: Assessment (1/3) - Answer I

Question 1

What is attribution in a cybercrime investigation?

- A. Assigning a case to the correct court.
- B. Proving who was responsible for an attack. (✓)
- C. Classifying the crime under a taxonomy.
- D. Calculating the financial loss.

Explanation:

- Relays, anonymising tools and false data make it extremely hard.
- Proving who was at the keyboard is the difficult part.



Section 4: Assessment (2/3) I

Question 2

Why is the MLAT process poorly matched to digital evidence?

- A. It only covers financial crime.
- B. It requires the suspect's consent.
- C. It takes months or years, while evidence can be deleted in seconds.
- D. It cannot be used between treaty signatories.



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

Question 2

Why is the MLAT process poorly matched to digital evidence?

- A. It only covers financial crime.
- B. It requires the suspect's consent.
- C. It takes months or years, while evidence can be deleted in seconds. (✓)
- D. It cannot be used between treaty signatories.

Explanation:

- The Budapest Convention improves cooperation but does not close the timing gap [4].



Section 4: Assessment (3/3) I

Question 3

What is a version 3 .onion address, technically?

- A. A DNS name registered with a special registrar.
- B. The service's public key written out in 56 characters.
- C. A hash of the server's IP address.
- D. A randomly assigned 16-character identifier.



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

Question 3

What is a version 3 .onion address, technically?

- A. A DNS name registered with a special registrar.
- B. The service's public key written out in 56 characters. (✓)
- C. A hash of the server's IP address.
- D. A randomly assigned 16-character identifier.

Explanation:

- Option D describes the version 2 format, withdrawn in October 2021 [15].
- The address does not resolve through DNS at all [16].



Conclusion: Key Takeaways I

- **Motive predicts evidence:** it decides what an attacker touches.
- **Money:** a financial trail, a look-alike domain, a chain of transfers.
- **Espionage:** altered logs, a mailbox read quietly rather than emptied.
- **Evolution:** curiosity, then profit, then supply chain, then machine speed.
- **Taxonomy:** the branch decides which evidence exists to collect.
- **Legal reality:** attribution and jurisdiction are the hard limits.

Next Step

- Move to the first practical step: collecting digital evidence.

References I

- [1] Anthropic.
Disrupting the first reported AI-orchestrated cyber espionage campaign.
Anthropic Threat Intelligence Report, 11 2025.
Accessed: 2026-09-05.
- [2] Hamad Binsalleeh, Thomas Ormerod, Amine Boukhtouta, Prosenjit Sinha, Amr Youssef, Mourad Debbabi, and Lingyu Wang.
On the analysis of the Zeus botnet crimeware toolkit.
In *Eighth Annual International Conference on Privacy, Security and Trust (PST)*, pages 31–38. IEEE, 2010.
- [3] Chainalysis Inc.
Crypto crime reaches record high in 2025 as nation-state sanctions evasion moves on-chain at scale.
The 2026 Crypto Crime Report, 1 2026.
Accessed: 2026-09-05.
- [4] Council of Europe.
Convention on cybercrime (budapest convention), 11 2001.
Opened for signature 23 November 2001.

References II

- [5] Renzon Cruz, Nicolas Bareil, Eric Semaan, and Omar Jbari.
An AI-assisted cyber attack: Inside a Unit 42 investigation.
Palo Alto Networks Unit 42, 9 2026.
Accessed: 2026-09-05.
- [6] Cybersecurity and Infrastructure Security Agency.
Alert (aa21-131a): Darkside ransomware: Best practices for preventing business disruption from ransomware attacks.
Technical report, CISA, 5 2021.
Accessed August 2, 2025.
- [7] Europol.
The evolving threat landscape: How encryption, proxies and artificial intelligence are expanding cybercrime.
Internet organised crime threat assessment (iocta), European Union Agency for Law Enforcement Cooperation (Europol), 4 2026.
11th edition, published 28 April 2026; accessed 2026-09-06.
- [8] Federal Bureau of Investigation Internet Crime Complaint Center.
Business email compromise: The \$50 billion scam.
Technical Report I-060923-PSA, FBI, 6 2023.



References III

[9] Brian Krebs.
Who is marcus hutchins?
Krebs on Security, 9 2017.
Account of the WannaCry kill-switch sinkholing; accessed 2026-08-16.

[10] Brian Krebs.
Conti ransomware group diaries, part i: Evasion.
Krebs on Security, 3 2022.
Accessed August 2, 2025.

[11] Phil Lapsley.
Exploding the Phone: The Untold Story of the Teenagers and Outlaws Who Hacked Ma Bell.
Grove Press, 2013.

[12] Mike McGuire and Samantha Dowling.
Cyber crime: A review of the evidence.
Research Report 75, Home Office, United Kingdom, 10 2013.

References IV

- [13] MITRE.
 Anthropic AI-orchestrated campaign, campaign C0062.
 MITRE ATT&CK, 2026.
 Accessed: 2026-09-05.
- [14] Eugene H. Spafford.
 The internet worm program: An analysis.
ACM SIGCOMM Computer Communication Review, 19(1):17–57, 1989.
- [15] The Tor Project, Inc.
 V2 onion services deprecation.
<https://support.torproject.org/onionservices/v2-deprecation/>, 2021.
 Accessed: 2026-08-15.
- [16] The Tor Project, Inc.
 How do onion services work?
<https://community.torproject.org/onion-services/overview/>, 2024.
 Accessed: 2026-08-15.



References V

- [17] US-CERT.
Alert (ta17-132a): Indicators associated with wannacry ransomware.
Cybersecurity & Infrastructure Security Agency, 5 2017.
- [18] Kim Zetter.
Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.
Crown, 2014.



Acronyms and Terminology I

- APT (Advanced Persistent Threat)** A highly skilled and well-funded hacking group, often sponsored by a government, that conducts long-term, stealthy cyberattacks for espionage or sabotage.
- Attribution** The process in a cybercrime investigation of identifying and proving who was responsible for an attack.
- Banking Trojan** A type of malicious software specifically designed to steal online banking credentials, such as usernames, passwords, and PINs.
- BEC (Business Email Compromise)** A type of scam where an attacker impersonates a company executive to trick an employee into making an unauthorized money transfer to an account controlled by the criminal.
- Bot** A computer that has been infected with malware, allowing it to be controlled remotely by an attacker as part of a larger network of infected machines (a botnet).
- Budapest Convention** The first international treaty that addresses cybercrime by seeking to harmonize national laws, improve investigative techniques, and increase cooperation among nations.
- CaaS (Cybercrime-as-a-Service)** A business model in the criminal underworld where advanced hacking tools, services, and infrastructure are sold or rented, allowing less-skilled criminals to launch sophisticated attacks.



Acronyms and Terminology II

CERT/CC (Computer Emergency Response Team/Coordination Center) The pioneering organization created to provide a central point of contact for coordinating responses to and reporting on major cybersecurity incidents.

CFAA (Computer Fraud and Abuse Act) The primary United States federal law that makes unauthorized access to computers and computer networks a criminal offense.

Critical Infrastructure Essential assets, systems, and networks, such as power grids, financial systems, and transportation, that are vital for a society's functioning and security.

Cyber-dependent Crime A crime that can only exist in the digital world and has no real-world equivalent, such as creating malware or launching a DDoS attack.

Cyber-enabled Crime A traditional crime, such as fraud or theft, that is made easier to commit or larger in scale through the use of computers and the internet.

Cyberstalking The use of electronic communication, such as social media or email, to harass, threaten, or repeatedly monitor another person.

Dark Web A section of the internet that is not indexed by standard search engines and requires special software (like Tor) to access, offering users a high degree of anonymity.



Acronyms and Terminology III

DDoS (Distributed Denial-of-Service) An attack where multiple compromised computer systems are used to flood a single target (like a website) with so much traffic that it becomes unavailable to legitimate users.

DoS (Denial-of-Service) An attack intended to shut down a machine or network, making it inaccessible to its intended users by overwhelming it with traffic.

Email Headers The technical metadata within an email that contains information about its path across the internet, which can be analyzed to help trace its true origin.

Exploit Kit A pre-packaged software toolkit that automates the process of attacking vulnerabilities in web browsers and plugins to deploy malware onto a victim's computer.

Full Packet Capture (PCAP) The process of intercepting and logging all data packets that pass across a computer network, creating a complete record for in-depth investigation.

Hacktivist A person or group who uses hacking techniques to promote a political agenda or social cause.

Hidden Service A website or online service hosted on an anonymity network like Tor, which conceals the IP address and physical location of the server.

ICS (Industrial Control System) Computer-based systems that monitor and control physical industrial processes, such as those found in manufacturing plants, power grids, and water treatment facilities.



Acronyms and Terminology IV

IDS/IPS (Intrusion Detection/Prevention System) A network security tool that monitors network traffic for malicious activity and can either alert administrators (IDS) or actively block the threat (IPS).

IP (Intellectual Property) Legally protected creations of the mind, such as inventions, trade secrets, artistic works, and designs.

Lateral Movement The process an attacker uses to move through a compromised network from one computer to another to find valuable assets or gain deeper access.

Malware Short for "malicious software," a general term for any software designed to cause damage, disrupt operations, or gain unauthorized access to a computer system.

MLAT (Mutual Legal Assistance Treaty) A formal agreement between countries to facilitate the exchange of evidence and assistance in legal investigations, including for cybercrime cases.

Network Flow Data Summary statistics about network traffic between two points, providing information like source/destination IPs and data volume without capturing the content of the communication.

OCG (Organized Crime Group) A structured group of individuals working together to commit crimes on an ongoing basis, often for financial gain.

Phone Phreak An early type of hacker who explored and exploited telephone systems, often to make free long-distance calls.



Acronyms and Terminology V

Phishing A type of social engineering attack where criminals send deceptive emails pretending to be from a legitimate company to trick people into revealing sensitive information.

PHI (Protected Health Information) Any individually identifiable health information that is protected by law, such as medical records or treatment history.

Ransomware A type of malware that encrypts a victim's files, making them inaccessible until a ransom payment is made to the attacker.

SYN Flood A type of DoS attack that sends a rapid succession of connection requests to a target's server, tying up its resources so that it cannot respond to legitimate traffic.

Taxonomy A formal system of classification for organizing items into ordered groups or categories based on their characteristics.

Three-way Handshake The standard method used by the TCP protocol to initiate a reliable connection between two computers on a network.

Tor (The Onion Router) A free and open-source software that enables anonymous communication by directing internet traffic through a worldwide, volunteer overlay network.

Worm A standalone piece of malware that replicates itself to spread to other computers over a network, often without any human action.



Thank You!

