
FORENSIC SCIENCE

Forensic Toxicology & Digital Forensics

A Comprehensive 2-Week Unit for Grades 10–12

10 Detailed Lesson Plans • Case Studies • Hands-On Activities

Expert Witness Role-Play • Unit Assessment & Answer Key

UM Printables

Subject:	Forensic Science	Grades:	10–12
Duration:	2 Weeks (10 Lessons)	Prepared by:	UM Printables
Focus Areas:	Toxicology & Digital Forensics	Type:	Complete Unit Resource

TABLE OF CONTENTS

Unit Overview

Week 1: Forensic Toxicology

- Lesson 1: Introduction to Forensic Toxicology
- Lesson 2: Pharmacokinetics Basics — ADME
- Lesson 3: Drug Detection Methods in Autopsies
- Lesson 4: Poisons & Their Detection
- Lesson 5: Toxicology Case Study Analysis (3 Scenarios)

Week 2: Digital Forensics

- Lesson 6: Introduction to Digital Forensics
- Lesson 7: Metadata & Digital Evidence
- Lesson 8: Deleted Files, IP Tracking & Social Media Evidence
- Lesson 9: Digital Forensics Evidence Analysis Activity
- Lesson 10: Expert Witness Role-Play & Unit Review

Toxicology Case Study — Three Scenarios

Digital Forensics Evidence Analysis Activity

Metadata Scavenger Hunt Activity

Expert Witness Role-Play Guide

Unit Assessment

Unit Assessment Answer Key

UNIT OVERVIEW

Forensic Toxicology & Digital Forensics Unit

This two-week unit introduces students in Grades 10–12 to two of the most dynamic and rapidly evolving specialties in modern forensic science. In Week 1, students explore forensic toxicology — the science of detecting drugs, poisons, and other chemical substances in biological specimens. They will learn the fundamental principles of pharmacokinetics (how the body absorbs, distributes, metabolizes, and excretes substances), examine the analytical methods used in forensic laboratories, and apply their knowledge to realistic case scenarios. In Week 2, students transition to digital forensics, where they investigate how electronic evidence — from metadata embedded in files to IP address logs and social media traces — is identified, preserved, and analyzed. The unit culminates in an expert witness role-play activity and a comprehensive assessment.

Essential Questions

- How do forensic scientists detect and quantify drugs and poisons in the human body?
- What role does pharmacokinetics play in understanding the effects and detection of substances?
- How is digital evidence identified, preserved, and analyzed in criminal investigations?
- What are the legal and ethical considerations in both toxicology and digital forensics?
- How does an expert witness communicate complex scientific findings to a jury?

Unit at a Glance

Week	Lesson	Topic	Key Activity
1	1	Introduction to Forensic Toxicology	Toxicology career exploration
1	2	Pharmacokinetics Basics — ADME	ADME diagram activity
1	3	Drug Detection Methods in Autopsies	Lab technique matching
1	4	Poisons & Their Detection	Historical poisoning case study
1	5	Toxicology Case Study Analysis	3-scenario investigation
2	6	Introduction to Digital Forensics	Digital evidence identification
2	7	Metadata & Digital Evidence	Metadata scavenger hunt
2	8	Deleted Files, IP Tracking & Social Media	IP tracing simulation
2	9	Digital Forensics Evidence Analysis	Full evidence analysis activity
2	10	Expert Witness Role-Play & Review	Mock trial + Unit assessment

NGSS & Standards Alignment

This unit aligns with the following standards and practices:

-
- NGSS Science and Engineering Practices: Analyzing and Interpreting Data; Constructing Explanations
 - NGSS Crosscutting Concepts: Patterns; Cause and Effect; Systems and System Models
 - CSTA Standards: 2-DA-07 (data collection and analysis); 3A-DA-12 (create and analyze data visualizations)
 - Common Core ELA: WHST.9-12.2 (write informative texts); SL.9-12.4 (present information clearly)
 - Criminal Justice Education Standards: Forensic science laboratory procedures and legal frameworks

Prerequisites

- Basic understanding of human body systems (circulatory, digestive, nervous)
- Familiarity with the scientific method and laboratory safety
- Basic computer literacy (file management, internet navigation)
- Introduction to the legal system and chain of custody concepts

LESSON 1

Introduction to Forensic Toxicology

Duration: 50 minutes | Grade Level: 10–12

Learning Objectives

- Define forensic toxicology and explain its role in death investigations and legal proceedings.
- Identify the types of biological specimens collected for toxicological analysis.
- Distinguish between postmortem and antemortem toxicology.
- Describe the career pathway and responsibilities of a forensic toxicologist.

Key Vocabulary

Forensic Toxicology: The study of the effects of drugs, poisons, and other chemicals on the human body in the context of legal investigations.

Postmortem: After death; refers to analysis of specimens collected during autopsy.

Antemortem: Before death; refers to analysis of specimens collected from living individuals.

Specimen: A sample of biological material (blood, urine, tissue) collected for analysis.

Chain of Custody: The documented record of who handled a specimen from collection to analysis.

Toxicology Report: A formal document presenting the findings of toxicological analysis.

Materials Needed

- Whiteboard and markers
- Student notebooks
- Handout: Forensic Toxicology Overview (provided in this resource)
- Projector for presentation slides (optional)
- Internet-enabled devices for career research

Warm-Up / Bell-Ringer (5 minutes)

Display the following question on the board: *"If a person is found deceased with no visible injuries, how might investigators determine whether drugs or poisons were involved?"* Have students write a brief response in their notebooks, then share with a partner. Facilitate a 2-minute class discussion, guiding students toward the concept of internal chemical analysis — the foundation of forensic toxicology.

Direct Instruction (20 minutes)

What Is Forensic Toxicology?

Forensic toxicology is the application of toxicological knowledge to assist the legal system in determining whether drugs, poisons, or other chemical substances contributed to a person's death, injury, or impairment. Unlike clinical toxicology, which focuses on treating patients, forensic toxicology operates within a legal framework and must meet strict evidentiary standards. Forensic toxicologists work closely with medical examiners, law enforcement, and attorneys to provide objective, scientifically valid results.

The Scope of Forensic Toxicology

Forensic toxicology encompasses three main areas:

- 1. Postmortem Toxicology:** Analysis of specimens collected during autopsy to determine if drugs or poisons contributed to or caused death. Specimens typically include blood, urine, vitreous humor (fluid from the eye), liver tissue, gastric contents, and hair.
- 2. Human Performance Toxicology:** Analysis of specimens from living individuals to determine impairment, such as in DUI/DWI cases. Blood alcohol concentration (BAC) and drug testing are common examples.
- 3. Forensic Drug Testing:** Routine drug screening in workplace settings, probation/parole monitoring, and sports anti-doping programs. This area follows strict protocols for specimen collection and chain of custody.

Specimen Collection and Chain of Custody

The integrity of toxicological findings depends entirely on proper specimen collection and documentation. Every specimen must be labeled with the case number, date and time of collection, the collector's identity, and the specimen type. The chain of custody form documents every person who handled the specimen from the moment of collection through analysis and reporting. Any break in the chain of custody can render evidence inadmissible in court. Specimens must be stored under appropriate conditions — refrigeration for most biological samples, and freezing for long-term preservation — to prevent degradation or contamination.

Guided Practice (10 minutes)

Provide students with a blank "Specimen Collection and Chain of Custody" form. Walk students through a mock scenario: A 42-year-old male is found unresponsive at home and pronounced dead at the scene. The medical examiner orders a full toxicological workup. Have students practice filling out the chain of custody form for blood, urine, and liver tissue specimens. Discuss common errors such as missing timestamps, unsigned transfers, and improper labeling.

Independent Practice (10 minutes)

Students research a career in forensic toxicology using provided guiding questions:

- What education and training are required to become a forensic toxicologist?
- What certifications are available (e.g., American Board of Forensic Toxicology)?
- What are the typical work environments for forensic toxicologists?
- What is the approximate salary range for entry-level and experienced forensic toxicologists?

Students write a one-paragraph summary of their findings.

Closure (5 minutes)

Review the three main areas of forensic toxicology. Ask students to share one surprising fact they learned about the field. Emphasize the critical importance of chain of custody and specimen integrity — concepts that will recur throughout the unit.

Exit Ticket

- 1. Define forensic toxicology in your own words.**

2. Name three types of biological specimens collected during an autopsy.

3. Why is chain of custody critical in forensic toxicology?

Differentiation

- **Support:** Provide a word bank and partially completed chain of custody form for struggling students.
- **Extension:** Have advanced students research a famous toxicology case (e.g., the poisoning of Viktor Yushchenko via dioxin) and present their findings.

Homework / Extension

Read the provided article excerpt on the history of forensic toxicology (from Mathieu Orfila's pioneering work in the 19th century to modern analytical techniques). Write a 5-sentence summary of how the field has evolved over the past two centuries.

LESSON 8

Deleted Files, IP Tracking & Social Media Evidence

Duration: 50 minutes | Grade Level: 10–12

Learning Objectives

- Explain what happens to a file when it is 'deleted' and how forensic examiners recover it.
- Describe the structure and purpose of an IP address and how it is used to track digital activity.
- Understand the role of Internet Service Providers (ISPs) and the legal process (subpoenas) required to link an IP address to a person.
- Evaluate the forensic value and legal limitations of social media evidence.

Key Vocabulary

Unallocated Space: Space on a hard drive that is not currently assigned to a file. When a file is deleted, its data moves to unallocated space and remains there until it is overwritten by new data.

File Slack: The unused space at the end of a file's last cluster. When a file is smaller than the cluster size, the leftover space (slack) can contain remnants of previously deleted files.

IP Address: Internet Protocol Address; a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication (e.g., 192.168.1.1).

ISP: Internet Service Provider; a company that provides individuals and organizations access to the Internet and related services. ISPs log which customer was assigned a specific IP address at a specific time.

Subpoena: A written order commanding a person or organization to produce evidence (such as ISP logs) for a court proceeding.

Ephemeral Data: Data that is temporary or short-lived, such as Snapchat messages or RAM contents, which are designed to disappear after being viewed or when power is lost.

Materials Needed

- Whiteboard and markers
- Student notebooks
- Handout: IP Tracking and ISP Flowchart
- Case study: The Social Media Cyberbullying Incident
- Projector for visual demonstration

Warm-Up / Bell-Ringer (5 minutes)

Ask students: *"When you delete a file from your computer and empty the Recycle Bin, is it really gone forever?"*

Take a show of hands. Reveal that 'deleting' a file usually just removes the pointer to the file, not the actual data. The data remains until it is overwritten.

Direct Instruction (22 minutes)

The Myth of Deletion

When a user deletes a file on a Windows computer, the operating system removes the file's entry from the Master File Table (MFT) or File Allocation Table (FAT), and marks the space the file occupies as 'unallocated'

or free. The actual 1s and 0s of the file remain on the physical disk. The file only truly disappears when the operating system saves a new file and overwrites those sectors. Digital forensic tools (like EnCase or FTK) scan this unallocated space to reconstruct deleted files.

- **File Slack:** Hard drives store data in clusters (e.g., 4KB clusters). If a file is only 2KB, it takes up one cluster, and the remaining 2KB is 'slack space.' This slack can contain fragments of the previous file that occupied that cluster.
- **Secure Deletion:** To permanently delete data, one must use a 'wiping' program that overwrites the file with random 1s and 0s multiple times (e.g., the Gutmann method or DoD 5220.22-M standard). Criminals aware of forensics may use these, but many do not.

IP Tracking

Every device connected to the internet is assigned an Internet Protocol (IP) address. In forensic investigations, an IP address is used to trace digital activity back to a source.

- **IPv4:** The traditional format (e.g., 203.0.113.42), consisting of four sets of numbers. Due to the explosion of internet devices, the world is transitioning to IPv6, which is much longer.
- **Dynamic vs. Static:** Most home users have dynamic IP addresses assigned by their ISP, which change periodically. Servers and businesses often have static IPs that never change.
- **The Forensic Process:** If a threat is sent via email, the email header contains the sender's IP address. The investigator identifies the IP, then uses publicly available databases to find which ISP owns that block of addresses. Law enforcement must then serve a subpoena to the ISP, demanding the name and address of the customer who was assigned that IP address at the specific date and time of the crime.
- **Limitations:** An IP address identifies a network, not a specific person. A Wi-Fi router's public IP is shared by all devices in the house. Furthermore, if a router is unsecured, a neighbor or a person in a parked car could have used the connection (the 'it wasn't me, someone hacked my Wi-Fi' defense). VPNs and the Tor network can also mask true IP addresses, complicating investigations.

Social Media Evidence

Social media is a goldmine for digital forensics, but it comes with strict legal and procedural requirements.

- **Public vs. Private:** Public posts can often be viewed and documented without a warrant, but private messages and restricted profiles generally require a subpoena or search warrant directed at the platform (e.g., Meta, Google).
- **Authentication:** Because it is easy to create fake accounts or alter screenshots, social media evidence must be authenticated. Forensic experts capture the evidence using specialized tools that record the URL, timestamp, HTML source code, and IP address at the time of collection, rather than just taking a screenshot on an iPhone.
- **Ephemeral Data:** Apps like Snapchat are designed to delete messages after viewing. While they may temporarily reside on the device's storage or RAM, they vanish quickly, making real-time preservation or server-side subpoenas necessary.

Guided Practice (10 minutes)

Walk students through the process of tracing an IP address. Provide the following mock email header snippet:

Mock Email Header

UNIT ASSESSMENT

Forensic Toxicology & Digital Forensics

Name: _____ Date: _____ Period: _____

Part 1: Multiple Choice (2 points each)

1. What does the 'M' stand for in the ADME pharmacokinetic model?

- a) Movement b) Metabolism c) Mitosis d) Measurement

2. What is the primary purpose of a hardware write-blocker in digital forensics?

- a) To speed up the data copying process
b) To decrypt locked files
c) To prevent the forensic computer from altering the source drive
d) To bypass the suspect's password

3. Which of the following is the 'gold standard' confirmatory test for identifying volatile drugs in forensic toxicology?

- a) ELISA
b) Immunoassay
c) Reinsch Test
d) GC-MS

4. Carbon monoxide causes asphyxiation by binding to:

- a) Hemoglobin b) Acetylcholinesterase c) Liver enzymes d) Red blood cell membranes

5. When a file is 'deleted' on a Windows computer, what actually happens to the data?

- a) It is immediately overwritten with zeros.
b) It is moved to the CPU cache.
c) The pointer is removed, but the data remains until overwritten.
d) It is permanently destroyed.

6. The SLUDGE syndrome is characteristic of poisoning by which class of chemicals?

- a) Heavy metals b) Opioids c) Organophosphates d) Barbiturates

7. What type of metadata is most useful for determining the exact geographic location where a smartphone photo was taken?

- a) Document Properties b) EXIF GPS data c) File slack d) HTML headers

8. How do forensic examiners mathematically prove that a bit-stream image is an exact replica of the original hard drive?

- a) By comparing file sizes
b) By checking the timestamps

(decreasing its bioavailability).

Part 3: Scenario Analysis

16. The blood concentration of 0.35 mg/L falls in the *toxic* range, which is below the generally lethal threshold of >0.50 mg/L. This concentration alone does not prove the drug caused her death. Factors that complicate interpretation include: **1) Tolerance:** Because she had been taking the medication for three years, she likely developed a tolerance, meaning she could survive and function at a concentration that would be lethal to an opioid-naïve person. **2) Postmortem Redistribution:** If the sample was taken from the heart rather than the femoral vein, the concentration could be artificially elevated. **3) Underlying health:** The cause of death could be unrelated to the drug (e.g., a cardiac event) with the drug level being incidental.

17. No, Employee A cannot be conclusively proven to be the leaker based on this evidence alone. **Unallocated space:** The file was found in unallocated space, meaning it was deleted. This proves the file was on the laptop, but does not prove who put it there or who deleted it. **Author metadata:** The document author is listed as Employee B. This suggests Employee B created or last modified the document, not Employee A. It is possible Employee A stole it from Employee B's computer, or that Employee B is the actual leaker. **IP Address:** The email came from the company's public Wi-Fi, meaning anyone in the building or nearby could have sent it. The evidence is circumstantial; corroboration (e.g., login logs, MAC addresses, additional metadata) would be required.

UM Printables

Thank you for purchasing this premium resource!

Your feedback is incredibly valuable and helps other educators find quality resources. If you found this Forensic Toxicology & Digital Forensics Unit comprehensive and engaging for your students, please consider taking a moment to leave a review on Teachers Pay Teachers.

Follow my store, **UM Printables**, for more high-quality, rigorous secondary science resources!

Happy Teaching!
