STRANDS AND STANDARDS

CYBER FORENSICS

Learning that works for Utah
CTE®

Course Description

Cyber Forensics is a course that introduces students to the investigative techniques and analytical tools used in the field of digital forensics. Students will explore the principles of ethical hacking and computer forensic investigation, learning how to detect, analyze, and document cyberattacks. The course emphasizes the proper collection, preservation, and presentation of digital evidence for legal proceedings, while also covering auditing practices and proactive security measures to prevent future breaches. Through hands-on labs and real-world scenarios, students will develop critical thinking, problem-solving, and communication skills essential for navigating the complex landscape of cybercrime and cybersecurity.

Intended Grade Level	9-12
Units of Credit	0.5
Core Code	35.01.00.00.038
Concurrent Enrollment Core Code	35.01.00.13.038
Prerequisite	Digital Literacy
Skill Certification Test Number	830
Skill Certification Cut Score	**80% PILOT**
Test Weight	0.5
License Area of Concentration	CTE and/or Secondary Education 6-12
Required Endorsement(s)	
Endorsement 1	Information Technology Systems
Endorsement 2	Cybersecurity

These educational standards are intentionally flexible, allowing teachers to create hands-on, interactive classroom experiences. This adaptability ensures activities meet safety guidelines set by the Local Education Agency (LEA) while engaging students in active learning. Teachers should adjust lessons to meet LEA requirements, prioritizing both safety and effective education.

Updated: JULY 2025

STRAND 1

Forensic Basics

Standard 1

Understand how to analyze forensic images

- Apply basic forensic analysis using NIST accepted forensic techniques.
- Outcomes include:
  - Understand how to use a forensic tool to analyze an image.
  - Identifying actors, authenticity verification (integrity), violation of company policy.
  - Being able to compare side by side analysis of reference image and current image - spotting differences.
  - Ensure following a defined procedure and documenting.

Standard 2

Outline the process for creating a forensically sound image.

- Understand that when a device is found leave it in the same state to preserve the integrity of the data.
- Isolate the image and create a hash to ensure data integrity.
- Write blocking to prevent modifying or writing over the data.

Standard 3

Understand Metadata

- Understand what is metadata and why it is important including: metadata found in email, images, webfiles, files, GPS (Global Positioning System), etc.
- Analyze metadata to identify anomalies and outliers to find an incident.
- Alter metadata to find and hide a secret message.

STRAND 2

Network Forensics

Standard 1

Network Basics

- Understand network protocols including UDP, TCP/IP model, ICMP.
- Understand the difference between connection and connectionless transmission.
- Understand 6 most common ports used including: FTP/21, SSH/22, SMTP/25, DNS/53, HTTP/80, HTTPS/443.
- Understand the purpose and use of port forwarding.
- Understand the purpose behind subnet masks and be able to read slash notation. 10.10.10.0/8.
- Understand how to set up and configure an Intrusion Detection System (IDS) on a network.

Standard 2

Understand how to analyze network data

- Understand the purpose and use of packet capture software.
- Apply the principles of packet captures to a message between two computers.
- Analyze the packets captured to find a hidden message.
- Identify the ports, protocol, source and destination IP's of a network capture.

STRAND 3

Anti Forensic Techniques

Standard 1

Understand Steganography

- Understand the principles behind steganography and why a threat actor would use it.
- Apply principles of steganography to hide information inside a text and image file.
- Apply principles of steganography to find information inside a text and image file.

Standard 2

Understand Trail Obfuscation techniques

- Understand the principles behind trail obfuscation techniques and why a threat actor would use them including - altering or deleting logs, spoofing, timestamp alteration, data sanitization and disk destruction.
- Apply the principles of trail obfuscation to hide information using data sanitization (as a minimum).
- Apply the principles of trail obfuscation to find altered information from an altered log and timestamp alteration (as a minimum).
- Apply one of the above techniques to a different Operating System.

STRAND 4

Collecting Forensic Evidence.

Standard 1

Determine and report logon/logoff times for a specific use

- Outcomes -
  - Students should be able to find a user breaking the company's AUP assigned time.

Standard 2

Understand how to use hashes

- Understand the basics of hash algorithms, their uses and salting.
- Outcomes -
  - Students know how to create a hash output for a file.
  - Students compare hash values to verify file integrity.

Standard 3

Summarize the proper handling of evidence.

- Understand the purpose of evidence logs.
- Understand how to implement a chain of evidence policy.
- Understand the purpose and value of a chain of custody.
- Discriminate between a live acquisition and static acquisition.
- Document the incident by taking photos of the scene before removing evidence.

Standard 4

Determine the important content of event logs in forensics.

- Understand the purpose of event logs.
- Outcomes -
  - Students will be able to read event logs and find suspicious activity.

STRAND 5

Incident Response

Standard 1

Incident Response Team (IRT)

- Understand the purpose of an incident response team.
- Identify the members of an incident response team including: team leader, team communicator, team members, share and stakeholders.

Team Leader	The team leader is the individual responsible for overseeing and coordinating all activities within an incident response team during a security breach or other critical event.
Team Communicator	The team communications lead is the spokesperson for the IRT. They are in charge of communication between the IRT and its various stakeholders.
Team Members	These are individuals within the cybersecurity department tasked with securing the organization's network. They assess the network for vulnerabilities and work to fix those vulnerabilities.
Shareholder	Shareholders refer to an individual or group that owns shares in a company, making them financially invested and therefore a key stakeholder who needs to be informed and considered during a cyber incident.
Stakeholder	Stakeholders can include internal parties such as employees from various departments, management, IT staff, and security personnel, as well as external entities like customers, vendors, regulatory bodies, and the media

- Identify the process of how a general user will report an incident to the team.

Standard 2

Identify the emergency contact list for incident response

- Identify who should be on the list, including position, responsibilities.
- Identify who needs to be contacted and availability.
- Create a process for keeping the list updated regularly.

Standard 3

Create an incident report process

- How to ensure the integrity of the documents.
- What is the standard information needed for each incident.
- How are the reports maintained and backed up.
- Understand the parts of the incident report- Summary, Timeline of events, description of events, analysis of root cause and impact.
- Communicate the results of an investigation to an internal team.

Standard 4

Create a post incident response process

- Configuration changes - firewall rules and device management setup, etc.
- Update loss prevention policies.
- Update certificates.
- Update incident response processes as needed.

Skill Certification Test Points & Questions by Strand

Test Name	Test #	Number of Test Points by Strand										Total Points	Total Questions
		1	2	3	4	5							
Cyber Forensics	830	5	8	9	9	4							
		Number of Questions by Strand											
		1	2	3	4	5							
		5	6	8	8	3						35	30

Cyber Forensics - VOCABULARY

Protocols	A set of rules used by two or more communicating entities that describe the message order and data structures for information exchanged between the entities.
NIST - link to framework	https://www.nist.gov/cyberframework
Forensic Image	The process of making an exact copy of digital storage media for the purposes of preserving its contents and structure for later analysis.
Actor	An entity responsible for a cybersecurity incident
metadata	Data about data. For filesystems, metadata is data that provides information about a file's contents.
udp	UDP stands for User Datagram Protocol, which is a communication protocol used to transfer data across the internet.
tcp / ip	TCP/IP stands for Transmission Control Protocol/Internet Protocol. It is a set of rules that governs the connection of computer systems to the internet.
icmp	ICMP stands for Internet Control Message Protocol. It is used for reporting errors and performing network diagnostics.
Port	The entry or exit point from a computer for connecting communications or peripheral devices
Subnet Mask	A 32-bit binary number that separates an IP address into its network and host addresses.

Cyber Forensics – VOCABULARY (cont.)

IDS	An IDS is Intrusion Detection Software. It is software that looks for suspicious activity and alerts administrators.
Packet	The logical unit of network communications produced by the transport layer.
Steganography	The art, science, and practice of communicating in a way that hides the existence of the communication.
Obfuscation	The action of making data obscure, unclear, or unintelligible.
Data Sanitization	Data sanitization involves purposely, permanently deleting, or destroying data from a storage device, to ensure it cannot be recovered.
Certificate	A file or electronic password that proves the authenticity of a device, server, or user through the use of cryptography and the public key infrastructure (PKI).