|  |
| --- |
| **TEXAS CTE LESSON PLAN**[www.txcte.org](http://www.txcte.org) |
| **Lesson Identification and TEKS Addressed** |
| **Career Cluster** | Law, Public Safety, Corrections, and Security |
| **Course Name** | Federal Law Enforcement and Protective Services |
| **Lesson/Unit Title** | Computer Forensics |
| **TEKS Student Expectations** | **130.341. (c) Knowledge and Skills**(7) The student analyzes the role of computer forensics in security operations. (A) The student is expected to summarize the role of computer applications relating to forensics investigations and(B) The student is expected to investigate criminal activity in areas such as cybercrime, the Internet, and Internet trafficking. |
| **Basic Direct Teach Lesson**(Includes Special Education Modifications/Accommodations and one English Language Proficiency Standards (ELPS) Strategy) |
| **Instructional Objectives** | The students will be able to:* Summarize the role of computer applications relating to forensics investigations
* Investigate criminal activity in areas such as cybercrime, the Internet, and Internet trafficking
 |
| **Rationale** | Computers have permeated society and are used in countless ways with innumerable applications. Similarly, the role of electronic data in investigative work has realized exponential growth in the last decade. The usage of computers and other electronic data storage devices leaves the footprints and data trails of their users. |
| **Duration of Lesson** | 4 to 5 hours |
| **Word Wall/Key Vocabulary***(ELPS c1a,c,f; c2b; c3a,b,d; c4c; c5b) PDAS II(5)* | Refer Computer Forensics Key Terms |
| **Materials/Specialized Equipment Needed** | **Materials*** Computer Forensics computer-based presentation
* Computer Forensics Key Terms
* Electronic Crime Scene Sketch Sample
* White board/chalk board
* Computer with Internet Access
* Discussion Rubric
* Group Evaluation Rubric
* Individual Work Rubric
* Peer Evaluation Rubric
* Presentation Rubric
* Research Rubric
 |
| **Anticipatory Set**(May include pre-assessment for prior knowledge) | Divide the class into several small groups and have them brainstorm/discuss the following questions:* What are the components of a computer?
* What is your own knowledge of computers? What data might be of evidentiary value? Where it might be found?
* How would you preserve computer evidence at a crime scene?
* Why is the Internet referred to as “a network of networks” or the “information superhighway”?
 |
| **Direct Instruction \*** | 1. Computer Forensics Introduction
	1. Computer forensics
		1. The acquisition, extraction, preservation, and interpretation of computer data
		2. Includes many devices that are capable of storing data
	2. Hardware is the physical material that creates a computer
	3. Software are the programs and applications that carry out a set of instructions on the hardware
2. Elements of Hardware
	1. Computer Case/Chassis – the box that typically rests besides the computer monitor and houses the internal components for the computer
	2. Power Supply – converts the power from the wall outlet to a usable form for the computer and its components
	3. Motherboard – the primary board that contains the main circuitry for the computer
	4. System Bus – a vast complex network of wires that carries data from one hardware device to another and is located on the motherboard
	5. Read Only Memory (ROM) – chips that store programs called firmware and are used to start the boot process and configure a computer’s components
	6. Random Access Memory (RAM) – the location in a computer where the operating system that is in use can be stored and retrieved for quick reference by the CPU
	7. Central Processing Unit (CPU) – the central component of a computer where all of the data is processed
	8. Input Devices – used to get data into the computer
		1. Keyboard
		2. Mouse
		3. Joy Stick
		4. Scanner
	9. Output Devices – used to get data from the computer
		1. Monitor
		2. Printer
		3. Speakers
	10. Hard Disk Drive (HDD) – the location in a computer where data is stored and retrieved
3. Data Storage and Retrieval
	1. Examiners must be familiar with the file system they are examining
	2. Evidence may be found in various computer locations and formats
	3. There are two categories for data-related evidence:
		1. Visible data
		2. Latent data
	4. The formatting process initializes portions of the hard drive so that it can store data, and it creates the structure of the file system
	5. Different operating systems map out (partition) HDDs in different manners
	6. RAM
	7. Sector – the smallest unit of data addressable by a hard disk drive, generally consisting of 512 bytes (Saferstein, 2009)
	8. Cluster – a group of sectors in multiples of two, typically the minimum space allocated in a file (Saferstein, 2009)

IV. Processing the Computerized Crime Scene1. Similar to processing a traditional crime scene (i.e. warrants, documentation, investigation techniques)
2. Documentation is a significant component in the computerized crime scene
	1. The scene should be initially documented in as much detail as possible before any evidence is moved and examined
	2. Crime scene documentation is accomplished through two actions:
		1. Sketching – the crime scene must be thoroughly diagramed and sketched in a floor plan format
		2. Photographing – from all locations and all possible angles, and include wide and close-up images
	3. After documentation is complete, a label should be placed on the cord of each peripheral, with a corresponding label placed on the port to which it is connected
	4. At a computerized crime scene most, if not all of the equipment will be seized, but before the peripherals are disconnected from the computer, a decision must be made about whether or not a live acquisition of the data is necessary (i.e. shutdown or unplug the computer)
		1. Example: unplugging the computer is imprudent
			1. If it will initiate data encryption, rendering it unreadable without a password or key
			2. If crucial evidentiary data exists in RAM that is not saved to the HDD will be lost with discontinuation of power to the system
3. Forensic Image Acquisition
	1. After the crime scene has been processed, the computer needs to be analyzed
	2. All electronic devices will be processed in the same manner
	3. The examination process that the forensic investigator uses on the computer must be intrusive
	4. All evidence (data) must be obtained without altering or destroying it
	5. Because booting a HDD to its operating system changes many files and could destroy evidentiary data, the data is generally obtained by removing the HDD from the system and placing it in a laboratory forensic computer so that a forensic image can be created
	6. Occasionally, in cases with specialized or unique equipment/systems the image of the HDD must be obtained by using the seized computer
	7. The examiner must be able to extract all forensic data/images and cause no changes to the HDD
	8. A signature or fingerprint of the drive is taken before and after imaging
		1. This fingerprint is created by using a Message Digest 5 (MD5), a Secure Hash Algorithm (SHA) or a similarly validated algorithm
		2. Before imaging the drive, the algorithm is run and a 32-character alphanumeric string is produced based on the drive’s contents
		3. The same algorithm is then run against the created forensic image which will result in the same alphanumeric string if none of the original content is changed

VI. Visible Data1. Data from a computer that is openly visible and easily available to users
2. Can encompass (from an evidentiary standpoint) any type of user- created data like
	1. Word processing documents
	2. Spreadsheets
	3. Accounting records
	4. Databases
	5. Pictures
3. Most criminal cases involving computers relate to financial investigations (or white-collar crimes) which require any data related to personal and business finance
4. Advances in printer technology have made high quality color printing affordable and common, which creates criminal opportunities
	1. Counterfeiting
	2. Check Fraud
	3. Document Fraud
5. Investigators must become familiar with the various computer applications that are used for criminal activities
6. The ability to recognize the data produced by these applications and to display the images is essential to identifying the evidence

VII. Temporary Files1. Can be valuable as evidence
2. Can sometimes be recovered during a forensic examination including some of the data that may have been altered from a previous version
3. Can be recovered when created through unsaved means (such as a computer being shut off manually)
4. Most programs automatically save a temporary copy of the file in progress
5. After working on a file or document, the user can save the changes, which promotes the temporary copy to a saved (or actual) file
6. Another type of temporary file valuable to the computer investigator is the printer spool
	1. When a print job is sent to the printer a spooling process delays the sending of the data so the application can continue to work while the printing takes place in the background
	2. When the print job occurs, a temporary print spool file is created
	3. This file contains a copy of all of the data from the printer

VIII. Latent Data1. The areas of files and disks that are typically not apparent to the computer user (and often not to the operating system), but contain data nonetheless (Saferstein, 2009); the data which the operating system has hidden
2. One of the reasons a forensic image of the media is created is because a standard copy only captures the logical data (that which the operating system is aware)
3. Can be evidentiary data
4. Includes data in the
	1. Swap space (used to conserve the valuable RAM within the computer system)
	2. RAM slack – the area from the end of the logical file to the end of the sector
	3. File slack – the remaining area from the end of the final sector containing data to the end of the cluster
	4. Unallocated space – the space on a hard drive that contains available space; the space may also contain temporary and deleted files

IX. Defragmenting/Swap File/Swap Space* 1. Defragmenting a HDD involves reconnecting noncontiguous data
	2. The HDD has minimum space reservation requirements (i.e. a file might require 100 bytes of space, but the operating system allocates much more)
	3. If a file grows past the allocated amount, another cluster is required
	4. If a different file occupies the next cluster, the operating system must find another place for the first file on the drive
	5. The file is said to be fragmented because data for the same file is contained in noncontiguous clusters
	6. The constant shuffling of data through deletion, defragmentation, swapping, etc., is one of the ways data is orphaned in latent areas
	7. Fragmentation of numerous files can degrade the performance of a HDD, causing the read/write heads to have to traverse the platters to locate the data
	8. The constant read and write operations of RAM cause a constant change in the swap file or swap space
1. Deleted Files
	1. Another source of latent data to be examined by forensic investigators
	2. The actions that occur when a file is deleted vary among file systems
	3. When a user deletes files, the data typically remains behind
		1. The first character in the files directory entry (its name) is replaced with the Greek letter sigma
		2. When the sigma replaces the first character, the file is no longer viewable through conventional methods and the operating system views the space previously occupied by the file as available
	4. Data will remain in the computer even though attempts are made to delete it
	5. When files in a Recycle Bin are deleted, the data remains there as well, until it is overwritten

XI. The Internet1. A computer network that provides information globally (also called the “information superhighway”)
2. Affects all subjects and professions including law enforcement and security services
3. Can be considered a series of networks
	1. A single network consists of two or more computers that are connected to share information
	2. The Internet connects thousands of these networks so all of the information can be exchanged worldwide

 D. Includes various methods of connection* 1. Wire
		1. Modem – a device that allows computers to exchange and transmit information through telephone lines
		2. Cable lines or DSL telephone lines – provide higher speed broadband connections
	2. Wireless (Wi-Fi)

E. Each computer that connects to the Internet has a unique numerical Internet Provider (IP) address and usually a nameXII. The World Wide Web and E-Mail1. The World Wide Web
	1. The most popular area of the Internet
	2. Considered a depository of information stored in the computers connected to the Internet across the world
	3. Web browsers allow the user to search all the information available on the web and retrieve any web pages the viewer wishes to explore
	4. Several directories and indexes on the Internet, known as search engines, are available to assist the user in locating a particular topic from the hundreds of thousands of web sites located on the Internet
	5. Keywords or phrases entered into a search engine will locate sites on the Internet that are relevant to that subject
	6. Commercial Internet service providers connect computers to the Internet while offering the user an array of options
2. Electronic mail (e-mail)
	1. The service most commonly used in conjunction with the Internet
	2. Carries messages across the world in a matter of seconds

XIII. Internet Crimes1. There are more cybercriminals than available law enforcement agents
2. Cybercriminals feel safe committing crimes in a “comfort zone” and often from the privacy of their own homes
3. Law enforcement faces new challenges with Internet crimes
	1. Most law enforcement officers are not trained in the technologies
	2. Internet crimes span multiple jurisdictions
	3. There is a need to retrofit new crimes to existing laws
4. Computers are used to commit a variety of crimes
	1. Identity Theft
	2. Fraud
	3. Industrial espionage
	4. Child pornography
	5. Harassment
	6. Gambling
	7. Piracy
	8. Computer viruses and spam
5. There are numerous methods and techniques criminals use to hide their crimes and evidence, which include
	1. Deleting files and emails
	2. Hiding files with encryption
	3. Password protection
	4. Embedding information in unrelated files
	5. Using WI-FI networks and cyber cafes to cover tracks
6. The task of forensic investigators includes
	1. Restoring deleted files and emails
	2. Finding the hidden files through complex password encryption programs and searching techniques
	3. Tracking criminals through the digital trail — IP addresses, to ISPs, to the offender

*Individualized Education Plan (IEP) for all special education students must be followed. Examples of accommodations may include, but are not limited to:*none |
| **Guided Practice \*** | *Individualized Education Plan (IEP) for all special education students must be followed. Examples of accommodations may include, but are not limited to:*none |
| **Independent Practice/Laboratory Experience/Differentiated Activities \*** | 1. Have the students process an electronic crime scene by creating a sketch complete with the appropriate measurements (see the Electronic Crime Scene Sketch Sample). The activity can best be conducted in the school library or computer lab with students taking measurements, obtaining photographs, and illustrating a diagram of the computer room. Students will identify and label all items located, including modems, ports, printers, and connecting wires. This activity can be completed either individually or in small work groups. Use the Individual Work Rubric, the Group Evaluation Rubric and the Peer Evaluation Rubric as needed for assessment.
2. Have the students write a research paper and/or a computer-based presentation regarding a cybercrime of their choice (identity theft, harassment, piracy, etc). Use the Research Rubric and/or the Presentation Rubric for assessment.

*Individualized Education Plan (IEP) for all special education students must be followed. Examples of accommodations may include, but are not limited to:*none |
| **Lesson Closure** |  |
| **Summative/End of Lesson Assessment \***  | Computer Forensics Exam and Key*Individualized Education Plan (IEP) for all special education students must be followed. Examples of accommodations may include, but are not limited to:*For reinforcement, the students will research and explain the difference between hardware and software. Use the Individual Work Rubric for assessment.  |
| **References/Resources/****Teacher Preparation** | 0135158494, Forensic Science: From the Crime Scene to the Crime Lab, Richard Saferstein, Prentice Hall, 20080205592406, *Introduction to Private Security: Theory Meets Practice,* Cliff Roberson and Michael L. Birzer, Prentice Hall, 20090750684321, *Introduction to Security,* Robert J. Fischer and Gion Green, Butterworth-Heinemann, 2008Investigator/Officer’s Personal Experience |
| **Additional Required Components** |
| **English Language Proficiency Standards (ELPS) Strategies** |  |
| **College and Career Readiness Connection[[1]](#footnote-1)** | **Mathematics Standards**1. Geometric Reasoning

A. Figures and their properties* + 1. Identify and represent the features of plane and space figures.

IV. Measurement ReasoningA. Measurement involving physical and natural attributes1. Select or use the appropriate type of unit for the attribute being measured. |
| **Recommended Strategies** |
| **Reading Strategies** |  |
| **Quotes** |  |
| **Multimedia/Visual Strategy****Presentation Slides + One Additional Technology Connection** |  |
| **Graphic Organizers/Handout** |  |
| **Writing Strategies****Journal Entries + 1 Additional Writing Strategy** |  |
| **Communication****90 Second Speech Topics** |  |
| **Other Essential Lesson Components** |
| **Enrichment Activity**(e.g., homework assignment) | For enrichment, the students will write a research paper about the instruments that cybercriminals use to commit their crimes. Use the Research Rubric for assessment |
| **Family/Community Connection** |  |
| **CTSO connection(s)** | SkillsUSA |
| **Service Learning Projects** |  |
| **Lesson Notes** |  |

1. Visit the Texas College and Career Readiness Standards at <http://www.thecb.state.tx.us/collegereadiness/CRS.pdf>, Texas Higher Education Coordinating Board (THECB), 2009. [↑](#footnote-ref-1)