Lesson Plan

LESSON TITLE: Module 2: Digital Forensics and Steganography

SUMMARY:

Topic Outline

- Digital forensics concepts, techniques, and tools
- Investigation, preservation, and analysis
- Concepts and techniques of steganography
- Steganographic analysis

GRADE BAND:

☐ K-2 ☒ 6-8

☐ 3-5 ☒ High School

Time Required:

60 minutes

Lesson Learning Objective/Outcomes: Upon completion of this lesson, students will be able to:

- Understand basic digital forensics investigation, preservation, and analysis;
- Gain an understanding of steganographic techniques, tools, and analysis.

Materials List:

Software tools: STools4, File Checksum Integrity Verifier (FCIV), USB Image Tool (USBIT), Autopsy/Sleuthkit

How will you facilitate the learning?

- Describe the Warm-up Activity/Focused Activity/Closure and/or Reflection
- Describe the Teacher Instruction

We adopt the following best instructional practices and strategies to facilitate learning:

- Multimodal presentation of information
- Cooperative active learning
- Team building
- Periodic checking for understanding

This lesson includes:

☒ Mapping to Cyber Security First Principles
☒ Assessments
☒ Learning Objectives

Mapping to Cyber Security First Principles:

☐ Domain Separation
☒ Process Isolation
☐ Resource Encapsulation
☒ Modularity
☐ Least Privilege
☒ Abstraction
☒ Data Hiding
☐ Layering
☐ Simplicity
☐ Minimization

Assessment of Learning:

TYPE (Examples Listed Below)	NAME/DESCRIPTION
Quiz/Test Presentation Oral Questioning Observation Choose an item. Choose an item. Choose an item.	Online pop-quiz/survey using gosoapbox.com will be utilized to check understanding of key indicators. Key Indicators of Understanding • Recognition of Cyber Security Principle involved • Basic knowledge of evidence preservation • Basic knowledge digital forensic analysis • Familiarity with concepts of steganography Hands-on exercises will be conducted to reinforce learning. Participants will be asked to present their observations on pertinent case studies.

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

We provide digital videos with closed captions of software tools and hands-on exercises.

Description of Extension Activity(ies):

Background Materials

Digital Forensics

Digital forensics is the identification, preservation, and the analysis of information stored, transmitted, or produced by a computer system or computer network. Its main purpose is to establish the validity of the hypotheses used in an attempt to explain the circumstances or the cause of an activity under investigation (Anderson, et al., 2003). The practice was initiated by the U.S. military and intelligence agencies in the early 1970's. Although little is known about these activities due to their classified environments, it is reasonable to presume that they had a counter-intelligence focus via computer mainframes. In the 1980's, the Internal Revenue Service Criminal Investigations Division (IRS-CID) and Revenue Canada were two of the first government agencies with an obvious and openly noticeable obligation to carry out forensics on external systems linking to criminal offences. Also in 1984, the FBI established the Computer Analysis and Response Team (CART), to provide computer forensic support (Culley, 2003).

There are a number of computer forensic training courses offered today. However, most of them are specifically focused on a certain set of tools. A computer forensic examiners training course should be broad enough to familiarize the student with all methodologies of the field. The National Cybercrime Training Partnership (NCTP) was set up by the U.S. government, to provide guidance and assistance to local, state, and federal law enforcement agencies. Other U.S. organizations involved in training include NCJIS (The National Consortium for Justice Information and Statistics), and the High-Tech Crime Investigation Association (HTCIA). In Europe, NATO's Lathe Gambit Information Security program and Interpol both offer similar training course for allied countries.

Steganography

Steganography traces its roots to ancient times. One of the earliest documented uses of steganography involved tattooing a message on a slave's head. When their hair grew back, the messenger was sent to their destination. Historically, steganography was primarily used by the military during times of conflict. During the American Revolution, George Washington received messages written in invisible ink. Special patterns were sewn into quilts and displayed to guide escaping slaves along the Underground Railroad. World War I and II saw even further advances in steganography with the use of the Turning Grille and microdots. In the 1960's, the crew of the USS Pueblo, having been captured off the coast of North Korea, used sign language to convey messages in photographs (Kipper, 2004).

In addition to hiding messages, steganography is used to identify the source of messages. This application of steganography is called digital watermarking. A unique identifier is hidden within a digital medium. Since these identifiers are unique to each instance of that medium, they can determine where that transmission was sent to or from originally.

Associated Problem-based Laboratory Exercises:

I. Hands-on Information Hiding using Steganography

There are three visible files in a folder named **Module2** in the **C:\ drive** of your computer: a word document (TestFile.doc), a spreadsheet (TestLedger.xlsx), and an image file (TestPics.bmp). For this exercise, you are required to embed the word document and the spreadsheet into the image file as steganographic information. Delete those two files after accomplishing the task. Finally, recover those two files by extracting them from the Steg image.

II. Hands-on exercise on steganography using Digital Forensics Tools

Central Terrorism Unit (CTU) agents of the Department of Highest Security (DHS) raided a suspected terrorist hideout and captured a single piece of digital evidence: a USB jump drive that contains a single JPG file. Upon examination, the CTU IT personnel found that the image is quite suspicious. Jack Bummer, the current CTU head, had a very strong intuition that there is something in that image file. After hearing so many good things about the Computer Security and Forensic course at the GenCyber camp, he decided to hand over the evidence to your course instructor and requested an immediate forensic analysis. Due to the fact that the CTU informer has indicated that some dirty bombs may have been planted around the country, this stage of the investigation is very critical and time is paramount. Thus, Jack Bummer and your instructor have agreed to give you at most a day to develop a thorough digital investigation of the jump drive which includes: evidence preservation, analysis, and report of findings. You are asked to produce a final report that will be used in the court of law to prosecute the perpetrators of the crime. Here are the initial steps:

1) Task: Create an image of the evidence using the USBIT tool. Calculate its MD5 signature using the FCIV tool and save the signature in a text file. What is the importance of this step of the investigation?

2) Task: It looks like there are files that were purposely deleted from the USB drive to make it appear to be almost empty and uninteresting. Your assignment is to recover deleted files from the USB drive using the RECUVA tool. What files did you recover from the disk?

3) Task: Uncover the password that will be used for the steganalysis. How did you find it? What password did you manage to reveal?

4) Task: Using Autopsy and Sleuthkit, gather all string information that you can find in the deleted files. Again, perform a recovery all deleted files. Note that you will, most likely recover the same files similar to those that were recovered with the RECUVA tool. Establish the timeline in which files were created and modified.

5) Task: Perform a steganalysis of the images. How did you extract the data? What information did the data reveal? Are there additional steganographic data hiding within those extracted files? What does the word document contain? Investigate the geolocation of the people involved using the IP addresses found (Hint: the IPTracker file is interesting).

6) Task: Analyze the images. What information about the impending attack do they reveal?

Acknowledgements: