Syllabus

Course Overview

This course introduces you to many of the foundational and fascinating aspects of modern digital forensics including subpoenas, chain-of-custody procedures, accessing evidence on devices, and the use of modern forensic tools and techniques to identify and analyze digital information.

Forensic investigations take time and often last for days, weeks, or even months. To simulate an actual investigation, you will complete a seven-week-long course project using scenario-based course assignments presented in a virtual lab environment. At the end of the class you will compile your findings into a professional forensic report.

Let's investigate!

Technology Resources

Use of the following third-party resource is strongly recommended to support you in completing the course objectives. If you have access to other tools that you believe may still meet course requirements or if you have any difficulties accessing this resource or completing the related assignments, please contact your course faculty member to discuss potential alternatives.

- This Capella course offers labs through Jones and Bartlett Learning (JBL). These labs offer guided practice in performing tasks related to achieving course competencies and completing assessments.

Kaltura Activities

As part of this course, you are required to record video presentations using Kaltura or similar software. Refer to Using Kaltura [PDF] for more information about this courseroom tool.

Disability Services

Note: If you require the use of assistive technology or alternative communication methods to participate in any activity in this course, please contact DisabilityServices@Capella.edu to request accommodations.

Course Competencies

(Read Only)

To successfully complete this course, you will be expected to:

1. Describe common digital forensic data detection methods.
2. Assess forensics procedures for adherence to applicable laws
3. Apply common digital forensics processes.
4. Analyze digital evidence using current forensic processes.
5. Communicate effectively and professionally.

Course Prerequisites

Prerequisite(s): IAS5030.

Syllabus >> Course Materials

Required

The materials listed below are required to complete the learning activities in this course.

Integrated Materials

Many of your required books are available via the VitalSource Bookshelf link in the courseroom, located in your Course Tools. Registered learners in a Resource Kit program can access these materials using the courseroom link on the Friday before the course start date. Some materials are available only in hard-copy format or by using an access code. For these materials, you will receive an email with further instructions for access. Visit the Course Materials page on Campus for more information.

Book

Easttom, C. (2019). *System forensics, investigation, and response* (3rd ed.). Burlington, MA: Jones & Bartlett Learning. ISBN: 9781284121841.

Easttom, C. (2019). *System forensics, investigation, and response* [Online labs] (3rd ed.). Burlington, MA: Jones & Bartlett Learning. ISBN: 9781284320718.

Hardware

Capella University requires learners to meet certain minimum computer requirements. The following hardware may go beyond those minimums and is required to complete learning activities in this course. **Note:** If you already have the following hardware, you do not need to purchase it. Visit the Course Materials page on Campus for more information.

Hardware for Kaltura

- Headset with microphone
- Broadband Internet connection

Library

The following required readings are provided in the Capella University Library or linked directly in this course. To find specific readings by journal or book title, use Journal and Book Locator. Refer to the Journal and Book Locator library guide to learn how to use this tool.

- Jackson, B. A. (2017). Using digital data in criminal investigations: Where and how to draw the line? *Forensic Magazine*.

External Resource

Please note that URLs change frequently. While the URLs were current when this course was designed, some may no longer be valid. If you cannot access a specific link, contact your instructor for an alternative URL. Permissions for the following links have been either granted or deemed appropriate for educational use at the time of course publication.

- Banfield, J. (2015). *Kali Linux hacking tutorial and basic Linux command line interface* [Video]. | Transcript Retrieved from https://www.youtube.com/watch?v=VMTNoIDvz3o
- Carroll, O. L., Brannon, S. K., & Song, T. (n.d.). Computer forensics: Digital analysis methodology. Retrieved from https://www.crime-scene-investigator.net/computer-forensics-digital-forensic-analysis-methodology.html
- Chaddha, S. (2015). *Helix v3 forensic tool* [Video]. | Transcript Retrieved from https://www.youtube.com/watch?v=VhTWhrv2gbU
- Claridge, J. (2016). Building a criminal case using forensic evidence [Blog post]. Retrieved from http://www.exploreforensics.co.uk/building-a-case-using-forensic-evidence.html
- De Alwis, W. C. (2017, Jun 29). An introduction to challenges in digital forensics [Blog post]. Retrieved from https://articles.forensicfocus.com/2017/06/29/an-introduction-to-challenges-in-digital-forensics/
- Devendran, V. K., Shahriar, H., & Clincy, V. (2015). A comparative study of email forensic tools. *Journal of Information Security*, *6*(2), 111–117. Retrieved from https://www.researchgate.net/publication/275027885_A_Comparative_Study_of_Email_Forensic_Tools
- Easttom, C. (2017). Writing a forensics/expert report [Blog post]. Retrieved from https://allegiantinvestigation.com/writing-a-forensics-expert-report/
- Eliyahu, T. (2016). Practical guide to USB forensics - Data breach test case [Blog post]. Retrieved from https://www.linkedin.com/pulse/practical-usb-forensics-test-case-tal-eliyahu
- Evans, B. (2015). Is your computer forensic laboratory designed appropriately? [Blog post]. Retrieved from https://securityintelligence.com/is-your-computer-forensic-laboratory-designed-appropriately/
- FindLaw. (2018). What is a subpoena? Retrieved from https://litigation.findlaw.com/going-to-court/what-is-a-subpoena.html
- Flynn, M. (2018, Nov 14). Police think Alexa may have witnessed a New Hampshire double homicide. Now they want Amazon to turn her over. Retrieved from https://www.washingtonpost.com/nation/2018/11/14/police-think-alexa-may-have-witnessed-new-hampshire-double-slaying-now-they-want-amazon-turn-her-over/?noredirect=on&utm_term=.db683e607f8a
- Forensic Control. (2018). Introduction to computer forensics. Retrieved from https://forensiccontrol.com/resources/beginners-guide-computer-forensics/
- Forensics Colleges. (2018). Great apps for forensic science & investigation [Blog post]. Retrieved from https://www.forensicscolleges.com/blog/resources/forensic-science-and-investigation-apps
- Gubanov, Y. (2012, May 5). Retrieving digital evidence: Methods, techniques, and issues: Part 1 [Blog post]. Retrieved from https://www.forensicmag.com/article/2012/05/retrieving-digital-evidence-methods-techniques-and-issues-part-1
- Henry, P. (2009, Sep 12). Best practices in digital evidence collection [Blog post]. Retrieved from https://digital-forensics.sans.org/blog/2009/09/12/best-practices-in-digital-evidence-collection/
- Holton, T. R. (2018). What is a subpoena? Retrieved from https://www.holtonlaw.com/library/understanding-when-and-why-subpoenas-are-served.cfm
- InfoSec Institute. (2013). Forensic investigation on Windows machines [Blog post]. Retrieved from https://resources.infosecinstitute.com/forensic-investigation-windows-machines/
- InfoSec Institute. (2018). Computer forensics: Chain of custody. Retrieved from https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/legal-and-ethical-principles/chain-of-custody-in-computer-forensics/
- InfoSec Institute. (2018, Mar 26). Popular computer forensics top 21 tools [Updated for 2018] [Blog post]. Retrieved from https://resources.infosecinstitute.com/computer-forensics-tools/

- InfoSec Institute. (n.d.). Computer forensics: Web, email, and messaging forensics. Retrieved from https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/application-forensics/web-email-and-messaging-forensics/
- Kelley, M. (2012, May 30). Report writing guidelines [Blog post]. Retrieved from https://www.forensicmag.com/article/2012/05/report-writing-guidelines
- Kessler, G. C. (2015). An overview of steganography for the computer forensics examiner. Retrieved from https://www.garykessler.net/library/fsc_stego.html
- Kröger, K., & Creutzburg, R. (2013). A practical overview and comparison of certain commercial forensic software tools for processing large-scale digital investigations. Retrieved from https://www.researchgate.net/publication/258332973_A_practical_overview_and_comparison_of_certain_commercial_forensic_software_tools_for_processing_large-scale_digital_investigations
- Kumar, C. (2018). 23 FREE forensic investigation tools for IT security expert [Blog post]. Retrieved from https://geekflare.com/forensic-investigation-tools/
- Law Enforcement Cyber Center. (n.d.). Legal considerations. Retrieved from http://www.iacpcybercenter.org/topics/legal-issues/
- Law Enforcement Cyber Center. (n.d.). Common electronic devices that generate digital evidence. Retrieved from http://www.iacpcybercenter.org/officers/cyber-crime-investigations/common-electronic-devices-that-generate-digital-evidence/
- Law Enforcement Cyber Center. (n.d.). Litigation guides (Digital evidence and witnesses). Retrieved from http://www.iacpcybercenter.org/prosecutors/litigation-resources/
- Law Enforcement Cyber Center. (n.d.). Relevant federal statutes. Retrieved from http://www.iacpcybercenter.org/prosecutors/8-2relevant-federal-statutes/
- Law Enforcement Cyber Center. (n.d.). Understanding digital evidence. Retrieved from http://www.iacpcybercenter.org/investigators/digital-evidence/understanding-digital-evidence/
- Legal Dictionary. (n.d.). Subpoena. Retrieved from https://legaldictionary.net/subpoena/
- Legal Information Institute. (n.d.). Daubert standard. Retrieved from https://www.law.cornell.edu/wex/daubert_standard
- Legal Information Institute. (n.d.). Rule 45. Subpoena. Retrieved from https://www.law.cornell.edu/rules/frcp/rule_45
- Mariah. (2018, Feb 15). Importance of email header analysis in digital forensics investigation [Blog post]. Retrieved from https://www.acquireforensics.com/blog/importance-email-header-analysis-digital-forensics.html
- Microsoft. (2018). TechNet. Retrieved from https://technet.microsoft.com/en-us/ms376608.aspx
- Moulin, J. (2013, Sep 2). Creating a mobile digital forensics laboratory [Blog post]. Retrieved from https://www.joshmoulin.com/creating-a-mobile-digital-forensics-lab/
- Nelson, D. (2016, Nov 11). Steganography: The art & science of hiding things in other things–Part 4 [Blog post]. Retrieved from https://www.blackhillsinfosec.com/steganography-the-art-and-science-of-hiding-things-in-other-things-part-4/
- Nelson, D. (2016, Nov 4). Steganography: The art & science of hiding things in other things–Part 3 [Blog post]. Retrieved from https://www.blackhillsinfosec.com/steganography-the-art-and-science-of-hiding-things-in-other-things-part-3/
- Nelson, D. (2016, Oct 21). Steganography: The art & science of hiding things in other things–Part 2 [Blog post]. Retrieved from https://www.blackhillsinfosec.com/steganography-the-art-and-science-of-hiding-things-in-other-things-part-2/
- Nelson, D. (2016, Oct 7). Steganography: The art & science of hiding things in other things–Part 1 [Blog post]. Retrieved from https://www.blackhillsinfosec.com/steganography-the-art-science-of-hiding-things-in-other-things-part-1/
- Ozkaya, E., Alshakarti, H., & Comvalius, R. (2015). *Windows security and forensics* [Video]. | Transcript Retrieved from https://mva.microsoft.com/en-us/training-courses/windows-security-forensics-14383?
- SANS Digital Forensics & Incident Response. (2018). Windows forensic analysis poster. Retrieved from https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download
- Staib, M. (2017). How to write a forensic report. Retrieved from https://legalbeagle.com/5858380-write-forensic-report.html
- Stone, A. (2015, Sep 17). Chain of custody: How to ensure digital evidence stands up in court [Blog post]. Retrieved from https://www.govtechworks.com/chain-of-custody-how-to-ensure-digital-evidence-stands-up-in-court/
- Tabona, A. (2018, Jul 10). Top 20 free digital forensic investigation tools for sysadmins [Blog post]. Retrieved from https://techtalk.gfi.com/top-20-free-digital-forensic-investigation-tools-for-sysadmins/
- Wolfe, H. (n.d.). Setting up an electronic evidence forensics laboratory [PDF]. Retrieved from https://www.cengage.com/resource_uploads/downloads/1111036985_258972.pdf

Suggested

The following materials are recommended to provide you with a better understanding of the topics in this course. These materials are not required to complete the course, but they are aligned to course activities and assessments and are highly recommended for your use.

Optional

The following optional materials are offered to provide you with a better understanding of the topics in this course. These materials are not required to complete the course.

External Resource

Please note that URLs change frequently. While the URLs were current when this course was designed, some may no longer be valid. If you cannot access a specific link, contact your instructor for an alternative URL. Permissions for the following links have been either granted or deemed appropriate for educational use at the time of course publication.

- Baluja, S. (n.d.). Hiding images in plain sight: Deep steganography [PDF]. Retrieved from https://papers.nips.cc/paper/6802-hiding-images-in-plain-sight-deep-steganography.pdf
- E-fense. (n.d.). Helix3 download. Retrieved from https://www.e-fense.com/store/index.php?_a=viewProd&productId=11
- Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). Digital evidence and the U.S. criminal justice system: Identifying technology and other needs to more effectively acquire and utilize digital evidence [PDF]. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR800/RR890/RAND_RR890.pdf
- Kali. (2018). Retrieved from https://www.kali.org/
- National Institute of Standards and Technology (NIST). (2018). Forensic Science Standards Board. Retrieved from https://www.nist.gov/topics/forensic-science/forensic-science-standards-board
- NIST. (2018). Digital forensics. Retrieved from https://www.nist.gov/itl/ssd/digital-forensics
- NIST. (n.d.). The Computer Forensic Reference Data Sets (CFReDS) project. Retrieved from https://www.cfreds.nist.gov/
- Sleuthkit.org. (2018). Open source digital forensics. Retrieved from https://www.sleuthkit.org/
- Thycotic. (n.d.). The anatomy of a privileged account hack. Retrieved from https://thycotic.com/resources/anatomy-of-a-privileged-account-hack/
- Tittel, E., & Lindros, K. (2018, May 23). Best digital forensics certifications [Blog post]. Retrieved from https://www.businessnewsdaily.com/10755-best-digital-forensics-certifications.html

Projects

Project >> Digital Forensics Report

Project Overview

Your course project is a professional forensic report based on activities that you complete throughout the course. A template is provided to help you complete the report, which is due in Unit 10.

You will assume the role of a digital forensics technician working for a police department who has been assigned to retrieve digital evidence associated with an arrest for a suspected drug trafficker.

You will examine subpoenas and other legal aspects of digital forensics, retrieve and decode evidence, and follow established procedures to create a professional forensic report, including:

- Identifying information necessary for inclusion in a subpoena.
- Documenting a workstation configuration.
- Uncovering digital evidence using bootable forensics tools.
- Discovering a hidden message.
- Creating a forensic system case file for analyzing evidence.

You will also prepare an executive summary after filling in the information from previous units.

Scenario: Opening Brief

Imagine that a suspect has been arrested for suspicion of drug smuggling. He was an employee at the Quality Motors car dealership. It is suspected that he may have used cars from the dealership to transport drugs as a part of his operation. An investigation is now underway and you have been asked to assess devices, retrieve data, and perform analysis on a computer specified in a subpoena.

Additional information on the scenario is provided as the course progresses.

Introduction

This week you:

- Apply the Daubert standard to forensic evidence in a virtual lab.
- Explore foundational principles of digital forensic evidence processing and acquisition.

Digital forensics is a topic that encompasses several types of evidence available on a various digital devices. Before any evidence can be collected, the forensic examiner must master evidence acquisition procedures and be familiar with relevant legal considerations.

While foundational principles (search and seizure, labeling and describing evidence, the Daubert standard, documenting and preserving the chain of custody, and so on) may not be the most exciting part of digital forensics, they are extremely important to understand, as failure to comply could result in the dismissal of a case, lost or corrupted evidence, and liability or contempt of court charges for the person responsible for improper handling. Every action has consequences and many decisions may have ethical ramifications to consider, as we will discuss.

Learning Activities

u01s1 - Studies

Readings

Use your *System Forensics, Investigation, and Response* text to read the following:

- Chapter 1, "Introduction to Forensics," pages 3–34.

Use the Internet to read the following:

- Henry, P. (2009). Best practices in digital evidence collection [Blog post]. Retrieved from https://digital-forensics.sans.org/blog/2009/09/12/best-practices-in-digital-evidence-collection/
  - In this blog post, one of the foremost experts in digital evidence collection offers clear procedures that should be followed and in the order in which each step should be completed. While older than other resources used in the course, it still provides the best collection of information on the topic in the most concise format.
- Law Enforcement Cyber Center (n.d.). Understanding digital evidence. Retrieved from http://www.iacpcybercenter.org/investigators/digital-evidence/understanding-digital-evidence/
  - In addition to defining *digital evidence*, this site discusses seizure of digital evidence for use in a lawsuit.
- Legal Information Institute. (n.d.). Daubert standard. Retrieved from https://www.law.cornell.edu/wex/daubert standard
  - The LII offers a concise listing of the elements necessary to meet the Daubert standard.
- Stone, A. (2015, Sep 17). Chain of custody: How to ensure digital evidence stands up in court [Blog post]. Retrieved from https://www.govtechworks.com/chain-of-custody-how-to-ensure-digital-evidence-stands-up-in-court/

Optional Internet Resources

Refer to the following resources for course activities as necessary:

- NIST. (n.d.). The Computer Forensic Reference Data Sets (CFReDS) project. Retrieved from https://www.cfreds.nist.gov/
  - The CFReDs project page is a resource repository with information, tools, and digital data sets that can be used when practicing digital forensics.
- NIST. (2018). Digital forensics. Retrieved from https://www.nist.gov/itl/ssd/digital-forensics
  - This page links to three forensics resources in annotated bibliography format.

u01s1 - Learning Components

- Explain fundamental applications of the Daubert standard to digital forensics investigations.
- Explain what unallocated space on a Windows system is.
- Identify what information is typically recorded on unallocated Windows system space.

u01s2 - Kaltura Media Preparation

An assignment in this course requires you to record audio for a presentation using Kaltura Media or other software. Refer to the Using Kaltura [PDF] tutorial for directions on recording and submitting your recording in the courseroom using Kaltura.

If you have not already done so, set up and test your microphone and headset using the installation instructions provided by the manufacturer. Then practice using it to ensure the audio quality is sufficient.

Note: If you require the use of assistive technology or alternative communication methods to participate in this activity, please contact DisabilityServices@Capella.edu to request accommodations.

u01v1 - Lab: Applying the Daubert Standard to Forensics Evidence

Overview

This lab offers you the opportunity to apply the Daubert standard, evaluate potential evidence, and apply a forensics tool to digital evidence to retrieve data.

Instructions

Read the requirements for all related course activities before completing this lab. Take notes as needed as you complete the lab to help you with those activities.

Select the linked title heading above to access a lab arranged through the textbook publisher.

1. Use the **assignment template** found in the Resources for your **lab screenshots** and your **assignment responses**.
2. Follow the lab instructions carefully and complete the entire lab.
3. Take the following screenshots:
    - Steps 9 and 14.

Jones & Bartlett Technical Support

If you have technical issues pertaining to accessing JBLvirtual labs, contact JBL Technical Support:

- E-mail: support@jblearning.com
- Phone: 1-800-832-0034, option 5.

Course Resources
Applying the Daubert Standard to Forensics Evidence
Assignment Template [DOCX]

u01a1 - Applying the Daubert Standard to Forensics Evidence

By now you should have completed the lab in the Virtual Resource Activity for this unit and saved your screenshots to a Word document for submission with this assignment.

Overview

When testifying in court, it is essential that the tests used to assess evidence meet the requirements set forth in *Daubert*. This lab offers you a chance to assess the criteria for yourself as you analyze data in a forensic case so you will be able to apply the standard if you conduct a forensic investigation.

Instructions

Consider your lab work and studies to address the following in the Word document that contains your lab screenshots. Label each section clearly.

Do the following:

- Identify the hash value in 043458.csv.
- Explain the origin of the Daubert standard and its significance to the digital forensics technologist.
- Explain the significance of the INFO2 file in the lab to the investigation.
- Explain the value of unallocated Windows system space to forensic investigations.

Submission Requirements

Submit your Word document with well-labeled responses.

u01d1 - Daubert: Preparing a Forensics Technician for a Deposition

Discuss how you would prepare an inexperienced digital forensics technician for examination of their credentials by legal teams during a deposition. Focus on the relevant aspects of Daubert.

Response Guidelines

Read the posts of your peers and respond to at least two, expanding on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience; provide substantive and appropriate responses.

Course Resources
Graduate Discussion Participation Scoring Guide

u01d1 - Learning Components

- Identify ways that Daubert impacts digital forensics investigators.

Unit 2 >> Digital Forensics Evidence Characteristics

Introduction

This week you:

- Explore types of crimes and digital evidence that may be found during an investigation.
- Discuss aspects of evidence seizure and how evidence may be used.

Digital forensics is the application of scientific tests and techniques to detect crime or digital evidence. Today, most crimes have a digital component or are investigated with the assumption of the presence of a digital element until there is proof that no device is relevant. When investigating a crime, it is important to understand what constitutes evidence and how to determine if that evidence is relevant. *Evidence* is the term used to identify an object or eyewitness account as proof of some action or fact.

Consider a traffic accident. A usual part of the investigation is to ascertain if any driver was using a mobile phone or other device while operating their vehicle. To assess the situation, the mobile devices of all parties involved may be confiscated and examined. The automobile may also have potential evidence stored as data.

In this example, imagine that a cell phone is found on the floor of the car after an accident. It does not have a screen saver and a live video feed is playing when the cellphone is viewed by an evidence technician. The cellphone is potential evidence that must be documented, as is the video content that is streaming on it. This evidence supports the theory that the driver was looking at the phone and therefore distracted at the time of the accident.

Learning Activities

u02s1 - Studies

Readings

Read the following in your *System Forensics, Investigation, and Response* text:

- Chapter 2, "Overview of Computer Crime," pages 35–57.

Use the Internet and the Capella University Library to read the following:

- Forensic Control. (2018). Introduction to computer forensics. Retrieved from https://forensiccontrol.com/resources/beginners-guide-computer-forensics/
  - This article provides an overview of the various elements of an investigation and serves as a review of the concepts covered to this point.

- Gubanov, Y. (2012, May 5). Retrieving digital evidence: Methods, techniques, and issues: Part 1 [Blog post]. Retrieved from https://www.forensicmag.com/article/2012/05/retrieving-digital-evidence-methods-techniques-and-issues-part-1
  - This post identifies several places to look for digital evidence, including Internet-enabled game systems and social media.
- Jackson, B. A. (2017). Using digital data in criminal investigations: Where and how to draw the line? *Forensic Magazine*.
  - This article forms the basis for study in the first discussion question in this unit. It offers several thought-provoking questions in favor of and opposing the generation, distribution, and ease of access of data generated by IoT devices.
- Law Enforcement Cyber Center. (n.d.). Common electronic devices that generate digital evidence. Retrieved from http://www.iacpcybercenter.org/officers/cyber-crime-investigations/common-electronic-devices-that-generate-digital-evidence/
  - This site features a list of devices and digital evidence in a convenient tabular format.
- Law Enforcement Cyber Center. (n.d.). Legal considerations. Retrieved from http://www.iacpcybercenter.org/topics/legal-issues/
- Law Enforcement Cyber Center. (n.d.). Litigation guides (Digital evidence and witnesses). Retrieved from http://www.iacpcybercenter.org/prosecutors/litigation-resources/
- Law Enforcement Cyber Center. (n.d.). Relevant federal statutes. Retrieved from http://www.iacpcybercenter.org/prosecutors/8-2relevant-federal-statutes/

Optional Readings

Use the Internet to read the following:

- Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). Digital evidence and the U.S. criminal justice system: Identifying technology and other needs to more effectively acquire and utilize digital evidence [PDF]. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR800/RR890/RAND_RR890.pdf
  - This document provides several very good real-world examples of ways digital evidence was essential to understanding the elements of a crime or in solving a crime.
- Thycotic. (n.d.). The anatomy of a privileged account hack. Retrieved from https://thycotic.com/resources/anatomy-of-a-privileged-account-hack/
  - This is a whitepaper sponsored by the cybersecurity company Thycotic. While it promotes this firm's products and services, it offers valid statistics, solid practices for attack prevention, and free resources. It is an easy read and includes several graphs.

u02d1 - Is There Evidence of a Crime?

There is potential digital evidence generated by or stored in every digital device. Consider what you read in this unit about lawful search and crimes with digital components. A thought-provoking two-page article serves as the basis for this discussion of several sensitive topics. Make sure that you have read Using Digital Data in Criminal Investigations: Where and How to Draw the Line? from this unit's studies before you begin preparing your post.

The article's author observes, “The decision to allow data from implanted medical devices to be used in criminal proceedings may affect whether patients are willing to even use such devices” (Jackson, 2017). Consider the implications of this and discuss the following:

- What types of evidence should be allowable for capture and analysis?
- Who should perform that capture and analysis? For example, if it is medical equipment evidence, should it be a doctor, technician, or forensic examiner?
- Does the type or severity of the crime (such as misdemeanor versus felony, crime against an entity versus a person, or crime against a child versus an adult) make a difference?

Support your positions with examples where appropriate.

Response Guidelines

Read the posts of your peers and respond to at least two, expanding on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience; provide substantive and appropriate responses.

Reference

Jackson, B. A. (2017). Using digital data in criminal investigations: Where and how to draw the line? *Forensic Magazine*.

Course Resources

Graduate Discussion Participation Scoring Guide

u02d2 - Evidence of Innocence or Guilt?

As we have discussed, there is potential digital evidence generated by or stored in every digital device. Consider the various digital devices you use every day: how many portable devices do you have at hand now? Does the list include a cell phone, tablet, watch, or fitness equipment? In addition to our cars, how many of the electronics at home and work can generate, send, or store data, like copiers, printers, computers, refrigerators, burglar alarms, and security cameras?

Consider the computer you are using. What types of files are stored on it (personal, business, academic, a mixture), and for how many different people? If you were subject to subpoena and required to turn over your computer, besides inconvenience, what problems would it cause? Do you have a backup of essential files?

Take a quick visual inventory of the files on your computer. How old are they? Is the software up-to-date and under license? (Note: If not, this is a great time to purge anything from your system that you do not hold legal license to have.)

Often when we hear the term *evidence* we assume it means proof of guilt, when evidence is simply a proof of fact and the fact may be innocence or guilt. Describe a simple scenario in which a crime has been committed and discuss the following:

- What digital devices might have evidence of the crime and therefore should be considered.
- How and what type of data from one or more of the devices could be used as evidence in a crime.
- How the evidence could be used to exonerate or convict someone, depending on its relationship to the timeline of the crime narrative.

Response Guidelines

Read the posts of your peers and respond to at least two, expanding on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience; provide substantive and appropriate responses.

Course Resources
Graduate Discussion Participation Scoring Guide

Unit 3 >> Obtaining and Documenting Forensic Evidence

Introduction

This week you:

- Use a template to create and properly scope a subpoena related to the course scenario.
- Present evidence seizure and safeguarding best practices.

How does the examiner procure potential evidence? Depending on the case, the evidence may be retrieved at the time of a crime or incident, such as the police confiscating a cell phone after an accident when the driver is believed to have been on that phone when the crash occurred. In other cases, the suspect may freely provide the evidence at the request of law enforcement to prove or imply that they are innocent.

The police and courts also obtain evidence via subpoenas. A *subpoena* is a legal document that compels a person to testify in court or to relinquish property such as documents, a cell phone, a computer, or other electronic devices.

No matter how the evidence is collected, it must be properly described and tracked through documentation in an evidence log. The evidence log provides information about the specifics of the evidence. For example, the type could be a cell phone located on a desk at 123 Main Street, Brookview, IL 23450. The log would include photos of the cell phone *in situ* (meaning unmoved from where it was originally found), close-up photos of the cell phone, and information on its make and model. It would also include information about the state of the evidence. Was the screen locked or unlocked? Does the cell phone require a passcode, biometrics, or a swipe design to gain access? The log includes all pertinent details of any officer or evidence technician who interacted with the evidence once it was collected. This provides a chain of custody for that piece of evidence.

When the forensic technician performs forensic analysis on the device, additional information will be generated, including what programs were found on the device and if any deleted files were recovered—all of which becomes part of the log. The log of evidence is a legal record and is required to be free of errors, complete, and legible. While the evidence may be digital, parts of the evidence log are handwritten and signed so the evidence may be given from one technician or officer to someone else with a need to examine or transport that evidence.

You will begin work on your course project in the unit lab and assignment as you imagine yourself as a digital forensics technician who is helping a detective ensure that a subpoena is scoped properly.

Learning Activities

u03s1 - Studies

Readings

Use your *System Forensics, Investigation, and Response* text to read the following:

- Chapter 4, "Collecting, Seizing, and Protecting Evidence," pages 83–105.

Use the Internet to complete the following:

- InfoSec Institute. (2018). Computer forensics: Chain of custody. Retrieved from https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/legal-and-ethical-principles/chain-of-custody-in-computer-forensics/
- Legal Information Institute. (n.d.). Rule 45. Subpoena. Retrieved from https://www.law.cornell.edu/rules/frcp/rule_45
  - Read everything above the Notes section on this reference page.

u03s2 - Kaltura Media

Complete the following **if you plan to use Kaltura for recording your presentation** required for this unit's assignment:

- If you have not already done so, set up and test your audio recording device on your computer, using the installation instructions from the manufacturer.
- Practice using the audio equipment to ensure the audio quality is sufficient.
- Refer to the Using Kaltura [PDF] tutorial for directions on recording and uploading your recordings in the courseroom.

Note: If you require the use of assistive technology or alternative communication methods to participate in this activity, please contact DisabilityServices@Capella.edu to request accommodations.

u03d1 - Subpoenas

Discussion Resources

Use the following resources to help you complete this discussion:

- FindLaw. (2018). What is a subpoena? Retrieved from https://litigation.findlaw.com/going-to-court/what-is-a-subpoena.html
  - FindLaw defines a subpoena in layman's terms, including what is legally required of a recipient and how a subpoena is used to collect evidence or ensure the presence of a witness in court.
- Holton, T. R. (2018). What is a subpoena? Retrieved from https://www.holtonlaw.com/library/understanding-when-and-why-subpoenas-are-served.cfm
  - Read the definition or watch the video.
- Legal Dictionary (n.d.) Subpoena. Retrieved from https://legaldictionary.net/subpoena/
  - This Web page offers *recursive definitions* for terms associated with a subpoena. When a term is used in definition of another term, the descriptive term is linked to its definition so you may understand how the terms and concepts are related.

Overview

Subpoenas are a part of most digital forensic cases and act as the means by which the evidence is legally seized for examination. Detective Morales, the lead detective on the case, is new to the Digital Crimes division and has asked for your assistance to ensure she crafts a subpoena that will be broad enough in scope to include all digital devices in the suspect's possession and at his home. In the unit assignment, you will create a subpoena appropriate for the scenario; this discussion is designed to prepare you for that assignment.

Instructions

Consider the breadth of digital devices used in a typical household and others that you might carry: smart phones, laptops, desktop computers and servers, printers, PDAs, tablets, fitness monitors and equipment, kitchen appliances, surveillance equipment and security systems—even game consoles. Obviously, it is doubtful that anything of probative value will be found in an Internet-accessible refrigerator, for example, so a statement such as "everything that can be plugged in" is not appropriate.

Imagine a case where a suspected interstate drug smuggler has been arrested and police detectives want to gather evidence to support the case against the suspect.

Discuss the following:

- What devices might the suspect have that may be of forensic value (contain data that could be evidence of crimes)?
- How specific should the description of each device be so that it may be retrieved?
- How would you advise Detective Morales safeguard any device from alteration once it is in her custody?
- How should Detective Morales document devices in situ to avoid compromising the forensic investigation?

Response Guidelines

Read the posts of your peers and respond to at least two, expanding on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience; provide substantive and appropriate responses.

Course Resources
Graduate Discussion Participation Scoring Guide

u03a1 - Subpoena and Presentation of Evidence Seizure and Safeguarding Practices

Overview

Subpoenas are used to gather evidence to verify, validate, and incriminate a suspect. There are special considerations associated with creating a subpoena for digital devices that you should understand. As you perform the functions of a forensic tech, you must not underestimate the importance of a properly scoped subpoena. The cost of securing and transporting evidence prohibits writing an overly broad subpoena.

This assignment requires you to scope a subpoena for the scenario to include all devices that may have evidence without demanding every electronic device that can be plugged in. It is doubtful that the suspect's refrigerator, electric toothbrush, or hair clippers would offer any data of value, for instance.

Adherence to proper evidence seizure and safeguarding protocols is also important for ensuring that digital forensics techs receive electronics in optimal condition for investigation. In the second part of the assignment, you create a presentation that outlines best practices for seizing and safeguarding evidence.

Scenario

This scenario expounds upon your unit discussion and will be used as a basis for the course project.

A suspected interstate drug smuggler has been arrested and police detectives want to gather evidence to support that case against the suspect. The lead detective on the case, Detective Morales, is new to the Digital Crimes division and has asked for your assistance to ensure that she has a subpoena to submit for court approval that is broad enough in scope to include all digital devices in the suspect's possession and at his home, but is not unnecessarily wide-ranging. You are tasked with crafting that subpoena.

You also been asked to present best practices for evidence seizure and preservation of device integrity related to this subpoena to remind department detectives and forensics personnel of the nuances of digital evidence seizure and preservation.

Preparation

- Make sure you have contributed to the unit discussion before starting this assignment.
- Review the subpoena template (linked in Resources) that you will use to complete the assignment.

Kaltura

For this assignment, you may choose to create your presentation using Kaltura. Refer to Using Kaltura (linked in Resources) for instructions. You may also use another program of your choice, provided your final presentation is compatible with the courseroom.

Note: If you require the use of assistive technology or alternative communication methods to participate in these activities, please contact DisabilityServices@Capella.edu to request accommodations.

Instructions

Part 1: Subpoena

Use the supplied template to create a properly scoped subpoena for the scenario. It should identify appropriate items for inclusion in this subpoena.

Part 2: Presentation

Prepare and record a 5–7 minute recorded presentation (with voice and supporting visuals) as a brief refresher on nuances of digital evidence search and seizure for department detectives and forensics personnel.

Do the following in your presentation:

- Explain four best practices for securing and transporting an Internet-connected device listed in the subpoena. Make sure to include the importance of documenting the disposition of the device (such as *on* or *off*). Include examples specific to your chosen device.
- Provide an example of a log entry for one of the items.
- Describe two safeguards designed to prevent device alteration. Include a specific example of a possible alteration vector or method that is appropriate for your chosen device to illustration the relevance and application of the safeguard.

Review the assignment scoring guide to ensure that you meet all criteria before submitting your subpoena and presentation for grading.

Course Resources
Subpoena Template [DOCX]
Using Kaltura [PDF]
DisabilityServices@Capella.edu

Unit 4 >> Data Discovery and Data Hiding Techniques

Introduction

This week you:

- Document a workstation configuration using common forensics tools in a virtual lab.
- Study forensics methods and labs.
- Discuss chain of custody and remote-data-acquisition tools.

This unit investigates the requirements to properly identify digital evidence and includes concepts like examining a device in situ and logging a computer system's configuration, both of which are important for assuring evidence is properly logged, tracked, and listed in a forensic report. You also explore forensic methods, lab examples, and discuss chain-of-custody procedures.

Learning Activities

u04s1 - Studies

Readings

Use your *System Forensics, Investigation, and Response* text to read the following:

- Chapter 3, "Forensics Methods and Labs," pages 59–79.

Use the Internet to read the following:

- Evans, B. (2015). Is your computer forensic laboratory designed appropriately? [Blog post]. Retrieved from https://securityintelligence.com/is-your-computer-forensic-laboratory-designed-appropriately/
  - This post discusses several items that must be considered in the planning phase of a lab to prevent lost or ruined data and devices.
- Moulin, J. (2013, Sep 2). Creating a mobile digital forensics laboratory [Blog post]. Retrieved from https://www.joshmoulin.com/creating-a-mobile-digital-forensics-lab/
  - This post is a fun look at what it takes to create a mobile lab (in a converted ambulance), covering hardware, software, faraday bags, and isolation units.
- Wolfe, H. (n.d.). Setting up an electronic evidence forensics laboratory [PDF]. Retrieved from https://www.cengage.com/resource_uploads/downloads/1111036985_258972.pdf
  - This paper provides a high-level overview of considerations necessary when constructing an electronic evidence lab.

Optional Readings

- E-fense. (n.d.). Helix3 download. Retrieved from https://www.e-fense.com/store/index.php?_a=viewProd&productId=11

- This is the last free distribution of the popular Helix Live Linux Distribution mentioned in the textbook that included the full version of Forensic Tool Kit (at that time, as the product has since been improved and is now licensed for commercial use). This is a great tool to practice forensics techniques. If loaded to a USB, it will not alter the source system, as this is a live distro.

- Kali. (2018). Retrieved from https://www.kali.org/
  - This is the Kali Linux suite mentioned in the textbook. Be careful when using this suite of tools, as there are many hacking tools included as well as tools with forensic value. Every tool included comes with detailed documentation and a community of support providers where you can ask questions.
- National Institute of Standards and Technology (NIST). (2018). Forensic Science Standards Board. Retrieved from https://www.nist.gov/topics/forensic-science/forensic-science-standards-board
  - This is one of many organizations that oversees the proper use and operations of forensics laboratories including digital forensics laboratories.
- Sleuthkit.org. (2018). Open source digital forensics. Retrieved from https://www.sleuthkit.org/
  - This is the Sleuthkit tool mentioned in the text. The full, current version is available on this site, as is the Autopsy GUI enhancement program, should you want an alternative to the command line interface (CLI).

u04s1 - Learning Components

- Identify items generated by WinAudit log files.
- Understand how WinAudit log files are used in a forensic investigation.
- Understand hidden partitions.
- Understand that files can have unexpected applications associated with them.

u04v1 - Lab: Documenting a Workstation Configuration Using Common Forensic Tools

Overview

As a forensic technician, you may be required to identify and document the configuration of various devices seized as evidence. In a corporate setting, this may be done by the incident response team after incident detection. As a part of your course project, you will use some of the configuration information listed in the lab report to build your forensic report.

Scenario

As the forensic tech on the investigation, you are presented with a computer (one of the items identified on the subpoena) and a properly executed and maintained chain-of-custody sheet (not shown). Now you must assess the computer, documenting its attributes, and then perform forensic retrieval of a bitstreamed image from its hard drive.

Instructions

Read the requirements for all related course activities before completing this lab. Take notes as needed as you complete the lab to help you complete those activities.

Select the linked title above to access a lab arranged through the textbook publisher.

1. Download the **assignment template** from Resources and use it for your **lab screenshots** and your **assignment responses**.
2. Follow the lab instructions carefully and complete the entire lab.
3. Take **only the following screenshots** (others are identified in the lab, but you only need to take these) and paste them into the template:
   - Steps 3, 8, and 11.

Jones & Bartlett Technical Support

If you have technical issues pertaining to accessing JBL virtual labs, contact JBL Technical Support:

- E-mail: support@jblearning.com
- Phone: 1-800-832-0034, option 5.

Course Resources
Assignment Template [DOCX]
Documenting a Workstation Configuration Using Common Forensic Tools

u04v1 - Learning Components

- Identify items generated by WinAudit log files.

- Understand how WinAudit log files are used in a forensic investigation.
- Understand hidden partitions.
- Understand that files can have unexpected applications associated with them.

u04a1 - Documenting a Workstation Configuration

By now you should have completed the lab in the Virtual Resource Activity for this unit and saved your screenshots to a Word document for submission with this assignment.

Overview

The hands-on lab offered the opportunity to use a common forensic tool to identify key information about the configuration of a specific system. This information may be used to complete your final forensic report.

Instructions

Do the following in your assignment template. *Note that some of your work here may go into your final forensic report.*

- Identify the Frhed file type.
- Describe the item(s) generated by WinAudit that are of critical importance in a computer forensic investigation.
- Describe the value of information learned from opening the Target.jpg file.

Review the scoring guide before submitting your assignment to ensure that you meet all criteria.

u04d1 - Chain of Custody

Establishing chain of custody is an essential step in any digital forensic investigation, as it is the official record of how evidence is processed. This includes:

- How the evidence was obtained.
- Where specifically it was found.
- When it was collected.
- Who had the evidence previously, and in what capacity.
- How the evidence was transported (conditions, type of vehicle, who supervised the delivery).
- Where the evidence was stored after analysis and who, if anyone, inspected that evidence once it was in storage.

Accordingly, the chain-of-custody documentation and testimony by those who performed actions listed in the documentation are presented by the prosecution to establish that the data in evidence was in fact in the possession of the defendant.

For this discussion, consider one of the following situations:

1. A mobile phone is seized by police as evidence on February 2, 2019 at 05:19 CST. The phone receives a text message while the initial possessing officer is logging the device in to evidence.
2. A laptop is seized by police as evidence on January 11, 2019 at 14:03 EST. The laptop is set to automatically run an antivirus scan with administrator permissions at 14:00 hours each day. The scan typically lasts for 20 minutes.
3. A printer is seized by police as evidence on January 27, 2019 at 16:08 CST. To move the printer, it must be unplugged. The officer removing the printer hears the system cycle after unplugging the printer.

Respond to the following questions using the situation you chose:

- What error or errors did the seizing officer make?
- How should the events be captured in the digital evidence log?
- How would you modify the existing procedure to prevent future errors?

Response Guidelines

Read the posts of your peers and respond to at least two, expanding on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience. Provide a substantive and appropriate response.

Course Resources

Graduate Discussion Participation Scoring Guide

Unit 5 >> Recovering Data

Introduction

This week you:

- Use common forensic tools to acquire data.
- Learn best practices for acquiring data when you are not colocated with the device.
- Differentiate between local and remote data acquisition.

Data generation and storage occur at an incredible pace. Often there is no thought given to data storage—just that the data is "there" and accessible when needed. The location of the data is important for forensic examiners, as there are additional steps and considerations when the data needed is not stored locally. In this unit, you investigate those nuances and learn best practices for ensuring proper retrieval without altering the data or its source.

Learning Activities

u05s1 - Studies

Readings

Use your *System Forensics, Investigation, and Response* text to read the following:

- Chapter 6, "Recovering Data," pages 135–153.

Use the Internet to read the following:

- Eliyahu, T. (2016). Practical guide to USB forensics - Data breach test case [Blog post]. Retrieved from https://www.linkedin.com/pulse/practical-usb-forensics-test-case-tal-eliyahu
  - This post takes you through the process of forensics retrieval on a USB drive.
- InfoSec Institute. (2018, Mar 26). Popular computer forensics top 21 tools [Updated for 2018] [Blog post]. Retrieved from https://resources.infosecinstitute.com/computer-forensics-tools/
- Kröger, K., & Creutzburg, R. (2013). A practical overview and comparison of certain commercial forensic software tools for processing large-scale digital investigations. Retrieved from https://www.researchgate.net/publication/258332973_A_practical_overview_and_comparison_of_certain_commercial_forensic_software_tools_for_processing_large-scale_digital_investigations
  - This comparison of popular forensic tools used by law enforcement offers insight into the benefits of each tool as well as how law enforcement uses each tool.
- Kumar, C. (2018). 23 FREE forensic investigation tools for IT security expert [Blog post]. Retrieved from https://geekflare.com/forensic-investigation-tools/
  - With more than 3.3 billion records breached in the first half of 2018 alone, according to data security firm Gemalto (2018), it is important to do everything possible to safeguard sensitive data. This article offers many valuable tools and techniques for ensuring data security.
- Tabona, A. (2018, Jul 10). Top 20 free digital forensic investigation tools for sysadmins [Blog post]. Retrieved from https://techtalk.gfi.com/top-20-free-digital-forensic-investigation-tools-for-sysadmins/
  - The top 20 forensics tools are compared and evaluated for usability, options, and applicable benefits from the perspective of a systems administrator.

Videos

Use the Internet to view the following:

- Banfield, J. (2015). *Kali Linux hacking tutorial and basic Linux command line interface* [Video] | Transcript. Retrieved from https://www.youtube.com/watch?v=VMTNolDvz3o
  - This video covers the basic installation of Kali Linux—including as a bootable operating system on a USB drive—and demonstrates how to navigate using the command line. Remember, the Kali Linux suite includes many forensic tools even though it is primarily identified as a hacking suite.
- Chaddha, S. (2015). *Helix v3 forensic tool* [Video] | Transcript. Retrieved from https://www.youtube.com/watch?v=VhTWhrv2gbU
  - This video covers the basics of how to use Helix v3, the last version of this tool available at no cost.

Reference

Gemalto. (2018). Data breaches compromised 3.3 billion records in first half of 2018 [Press release]. Retrieved from https://www.gemalto.com/press/Pages/Data-Breaches-Compromised-3-3-Billion-Records-in-First-Half-of-2018.aspx

u05v1 - Lab: Uncovering New Digital Evidence Using Bootable Forensic Utilities

There are many tools available for use in forensic examinations. Some tools are inherent in a device's operating system, while others are available as Web-based programs or on removable media. This lab provides experience using tools that are introduced from bootable media, which take control of the device under investigation, superseding the default operating system. Information on the tools used in the lab can be found in the unit studies so you may continue to use the tools after the class concludes.

Scenario

The next step in your data retrieval process requires you to use bootable forensic tools including Helix Linux with Forensic Tool Kit (FTK) to retrieve data artifacts from the hard drive on the computer identified in the subpoena.

Instructions

Read the requirements for all related course activities before completing this lab. As you complete the lab, take notes to help you complete those activities.

Select the linked title above to access a lab arranged through the textbook publisher.

1. Download the **assignment template** found in the Resources and use it for your **lab screenshots** and your **assignment responses**.
2. Follow the lab instructions carefully and complete the entire lab.
3. Take **only the following screenshots** (others are identified in the lab, but you only need to take these) and place them in the template:
    - Steps 4, 8, and 16.

Jones & Bartlett Technical Support

If you have technical issues pertaining to accessing JBL virtual labs, contact JBL Technical Support:

- E-mail: support@jblearning.com
- Phone: 1-800-832-0034, option 5.

Course Resources
Assignment Template [DOCX]
Uncovering New Digital Evidence Using Bootable Forensic Utilities

u05v1 - Learning Components

- Identify the five features of Process Explorer (ProcExp).
- Understand how Process Explorer (ProcExp) files are used in an forensic investigation.
- Understand how to access IECacheView.
- Understand the purpose of IECacheView.

u05a1 - Uncovering New Digital Evidence Using Bootable Forensic Utilities

By now you should have completed the lab in the Virtual Resource Activity for this unit and saved your screenshots to a Word document for submission with this assignment.

Instructions

Address the following lab-related items in your assignment template. *Note that some of your work here may go into your final forensic report.*

1. Describe the five Process Explorer (ProcExp) features that are of critical importance in a computer forensic investigation and why they are important to the investigation.
2. Describe the potential value of information learned from reviewing recent pages viewed by the suspect in his computer Internet browser.
3. Explain how IECacheView may help the forensic investigator assigned to this case.

Review the scoring guide to ensure that you meet all criteria before submitting your assignment.

u05d1 - Tools to Acquire Data Remotely

Because forensics investigations may be made anywhere, it is important for a forensics investigator to have tools for remote data acquisition. For this discussion, complete the following:

- Identify a few tips, tricks, and techniques available in the forensic tools to support remote data collection activities.
- Describe one method available to collect data remotely.
- Describe and discuss the elements you found most interesting about the tools and data acquired in this week's lab.

Response Guidelines

Read the posts of your peers and respond to at least two, expanding on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience; provide substantive and appropriate responses.

Course Resources
Graduate Discussion Participation Scoring Guide

Unit 6 >> Data Discovery and Data Hiding Techniques

Introduction

This week you:

- Decrypt a character string found in a message.
- Explore how to identify and restore data.

Part of a forensic examiner's job is knowing where to look for valuable data within a system. Criminals may use data hiding and scrambling techniques to conceal evidence. This unit explores these techniques and discusses how to identify and restore this data so it is readable and potentially useful to the investigation.

Learning Activities

u06s1 - Studies

Readings

Use your *System Forensics, Investigation, and Response* text to read the following:

- Chapter 5, "Understanding Techniques for Hiding and Scrambling Information," pages 107–134.

Use the Internet to complete the following:

- Kessler, G. C. (2015). An overview of steganography for the computer forensics examiner. Retrieved from https://www.garykessler.net/library/fsc_stego.html
  - Gary Kessler is one of the foremost experts in steganography and was one of the first to share his knowledge with law enforcement and the world. This tutorial includes samples of before-and-after stegoed images and audio.
- Nelson, D. (2016, Oct 7). Steganography: The art & science of hiding things in other things–Part 1 [Blog post]. Retrieved from https://www.blackhillsinfosec.com/steganography-the-art-science-of-hiding-things-in-other-things-part-1/
- Nelson, D. (2016, Oct 21). Steganography: The art & science of hiding things in other things–Part 2 [Blog post]. Retrieved from https://www.blackhillsinfosec.com/steganography-the-art-and-science-of-hiding-things-in-other-things-part-2/
- Nelson, D. (2016, Nov 4). Steganography: The art & science of hiding things in other things–Part 3 [Blog post]. Retrieved from https://www.blackhillsinfosec.com/steganography-the-art-and-science-of-hiding-things-in-other-things-part-3/
- Nelson, D. (2016, Nov 11). Steganography: The art & science of hiding things in other things–Part 4 [Blog post]. Retrieved from https://www.blackhillsinfosec.com/steganography-the-art-and-science-of-hiding-things-in-other-things-part-4/

- In this four-part series, the author details the concepts and process of steganography:

Optional Reading

Use the Internet to read the following:

- Baluja, S. (n.d.). Hiding images in plain sight: Deep steganography [PDF]. Retrieved from https://papers.nips.cc/paper/6802-hiding-images-in-plain-sight-deep-steganography.pdf
  - This paper, sponsored by Google Research, delves into the tools and techniques used in steganography. There is a valuable reference list of resources at the end.

u06a1 - Decrypting a Hidden Message

Overview

Make sure you have completed the readings for this unit before beginning this assignment.

This assignment requires you to apply one of the simple encryption techniques learned in this unit to a string of letters found on the suspect's computer. You are tasked with unscrambling the message and relaying the contents to the detective in charge of the investigation. Once you have the message, you will write an email to Detective Debbie Morales that includes pertinent information from the message, including where you found it.

Preparation

Access a decryption program from the readings or choose one of your own that is appropriate for a decoding a substitution cipher.

Instructions

Imagine that you found the following scrambled instant message on the suspect's hard drive:

- gur cvpxhc jvyy or ng gur pbeare bs znva naq sberfg ng 2:30 nz. v'yy or va n oyhr pnzel

Decrypt the characters and share your work (include tools and methods) and findings in an email (simulate it using Microsoft Word) addressed to Detective Morales at dmorales@capellacitysheriff.gov.

Review the scoring guide to ensure that you meet all criteria before submitting the assignment.

u06d1 - How to Conceal a Message

It is common in digital forensics investigations to encounter a message or message fragment that has been encrypted or hidden using steganography to avoid interception or render it unreadable should it be detected.

For this discussion, address one of the following scenarios:

1. You are a forensic technician and believe you have found a valuable piece of information but it is unreadable without use of special tools. Discuss how you would identify if an item is stegoed text, video, audio, or an encrypted message. Describe the steps you might take to access the message.
2. You are working on an investigation and discover important information about a possible meeting that you must relay quickly to the detective on the case. Unfortunately, there are rumors that her partner is corrupt and colluding with criminals on this or another case. Choose a method of concealment to be make sure that your message reaches the detective unaltered and without alerting her partner. How will you relay the method to the detective electronically so only she can decipher the message? How would you ensure that the hidden message was properly received and unscrambled?
3. You work in a forensic lab. Each case you work on may result in someone being sent to jail, fined, or subject to civil actions. You wonder if you should devise a code to make it difficult for unauthorized people to review your case notes. What should you consider before devising and implementing a code for your notes? Should you seek approval or is this a personal decision? What ethical considerations to your choice exist?

Response Guidelines

Read the posts of your peers and respond to at least two, expanding on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience; provide substantive and appropriate responses.

Course Resources

Graduate Discussion Participation Scoring Guide

Unit 7 >> Email Investigations

Introduction

This week you:

- Investigate the uses and recovery techniques for email in forensic investigations.
- Identify and examine information associated with a recovered email.

Email is one of the most common forms of digital communication, with most of us sending and receiving dozens of emails each week to stay in touch with friends, facilitate business, and receive special offers from favorite retailers. As an investigative tool, email can be a gold mine. Sometimes it isn't the actual email but the contact list and frequency of contact that matters. Message drafts—messages that are not addressed or sent—often have the most value.

The use of shared email accounts and initiating changes to a draft email have long been a preferred method of communication among criminals who assume incorrectly that if an email is never sent, there is no record of it. The truth is that whether saved, sent, or deleted, there is a record of it somewhere on the local system or on the email server.

Learning Activities

u07s1 - Studies

Readings

Read the following in your *System Forensics, Investigation, and Response* text:

- Chapter 7, "Email Forensics," pages 155–172.

Use the Internet to read the following:

- Devendran, V. K., Shahriar, H., & Clincy, V. (2015). A comparative study of email forensic tools. *Journal of Information Security*, *6*(2), 111–117. Retrieved from https://www.researchgate.net/publication/275027885_A_Comparative_Study_of_Email_Forensic_Tools
  - This article compares several email retrieval tools but the value is in the information that can be retrieved from an email using free open-source software or a commercial solution.
- InfoSec Institute. (n.d.). Computer forensics: Web, email, and messaging forensics. Retrieved from https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/application-forensics/web-email-and-messaging-forensics/
  - This resource provides an overview of the types of information that may be retrieved from these communication media.
- Mariah. (2018, Feb 15). Importance of email header analysis in digital forensics investigation [Blog post]. Retrieved from https://www.acquireforensics.com/blog/importance-email-header-analysis-digital-forensics.html
  - This post breaks down an email exchange into parts and indicates where valuable information could be stored at each step.

u07s2 - Preparing for Your Email Assignment

Your assignment in this unit requires to you share an email with one of your peers.

To prepare, read Email Lab [DOC].

u07a1 - Retrieving Forensic Information From an Email

Scenario

The hard drive on the computer you are investigating contains hundreds of emails. One of them is the email that you create in this assignment and it represents a communication initiated on the suspect's computer.

Overview

You will partner with a peer or someone outside class for this assignment in which you will "play detective." The findings from this assignment will be used in your final forensic report in Unit 10.

Follow the directions in Email Lab (linked in Resources).

Review the scoring guide to ensure you understand all criteria before submitting the assignment.

Course Resources
Email Lab [DOC]

u07d1 - Live Data Acquisition

While conducting a forensics investigation, forensics specialists may need to capture live data as it streams across a network. For this discussion, imagine that you are attempting to capture data from a live stream. Choose a stream type, such as a video chat. Use the study materials and engage in any research necessary to close knowledge gaps and discuss the following, being sure to identify the type of stream you chose:

- A tool that you might use for capturing and analyzing data.
- How encryption impacts the ability to engage in this activity.
- Challenges involved with engaging in this type of forensics investigation.

Response Guidelines

Read the posts of your peers and respond to at least two, expanding on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience; provide substantive and appropriate responses.

Course Resources
Graduate Discussion Participation Scoring Guide

Unit 8 >> Working a Forensics Case

Introduction

This week you:

- Examine the elements of a professional forensic report.
- Create a forensic system case file for analyzing forensic evidence in a virtual lab.

This unit begins to pull together the elements of a forensics case in one place and provides insight as to how all the information gathered can be combined into a single, comprehensive report.

Learning Activities

u08s1 - Studies

Readings

Read the following in your *System Forensics, Investigation, and Response* text:

- Chapter 15, "Systems Forensics Resources," pages 295–308.

Use the Internet to read the following:

- Carroll, O. L., Brannon, S. K., & Song, T. (n.d.). Computer forensics: Digital analysis methodology. Retrieved from https://www.crime-scene-investigator.net/computer-forensics-digital-forensic-analysis-methodology.html
  - The authors offer insight into the methodology applied to digital forensics investigations.
- Claridge, J. (2016). Building a criminal case using forensic evidence [Blog post]. Retrieved from http://www.exploreforensics.co.uk/building-a-case-using-forensic-evidence.html
  - This post offers a high-level view of how all the facets of many forensic investigations come together to form a case. Digital forensics is shown in context with other types of evidence.
- Forensics Colleges. (2018). Great apps for forensic science & investigation [Blog post]. Retrieved from https://www.forensicscolleges.com/blog/resources/forensic-science-and-investigation-apps
  - This post discusses many valuable resources, such as free tools, organizational aids, and technology, including Faraday bags.

u08s1 - Learning Components

- Identify the purpose of Paraben's P2 Commander Software within a forensic investigation.
- Identify specific protections available when using Paraben's P2 Commander.

u08v1 - Lab: Creating a Forensic System Case File for Analyzing Forensic Evidence

Investigators often prepare forensic reports for presentation to the internal customer (management) or the detective or prosecutor in a criminal investigation. This lab builds some of the basics used in a forensic report. A normal part of all forensic investigations is documenting the findings from disparate devices and systems into a cohesive report. This lab offers you an opportunity to do that on a small scale. These techniques should be used when crafting your final forensic report in Unit 10; the major difference is that in Unit 10 you are required to write an executive summary. This lab also gives you hands-on experience with Paraben's P2 Commander software.

Instructions

Read the requirements for all related course activities before completing this lab. As you complete the lab, take notes to help you complete your Unit 10 assignment.

Select the linked title above to access a lab arranged through the textbook publisher.

1. Download the **assignment template** found in the Resources and use it for your **lab screenshots** and your **assignment responses**.
2. Follow the lab instructions carefully. Complete the entire lab.
3. Take **only the following screenshots** (others are identified in the lab, but you only need to take these) and place them in the template:
   - Steps 11, 26, and 30.

Jones & Bartlett Technical Support

If you have technical issues pertaining to accessing JBL virtual labs, contact JBL Technical Support:

- E-mail: support@jblearning.com
- Phone: 1-800-832-0034, option 5.

Course Resources
Creating a Forensic System Case File for Analyzing Forensic Evidence
Assignment Template [DOCX]

u08v1 - Learning Components

- Identify the purpose of Paraben's P2 Commander Software within a forensic investigation.
- Identify specific protections available when using Paraben's P2 Commander.
- Understand that files can be hidden or not associated with any program.

u08a1 - Creating a Forensic System Case File for Analyzing Forensic Evidence

By now you should have completed the lab in the Virtual Resource Activity for this unit and saved your screenshots to a Word document for submission with this assignment.

Instructions

Use your assignment template to complete the following. *Note that some of your work here may go into your final forensic report.*

- Explain the protections Paraben's P2 Commander offers for chain-of-custody protection.
- Analyze the value of information for the investigation learned from opening the Target.jpg file.

Review the scoring guide to ensure that you meet all criteria before submitting your assignment.

u08d1 - Can Alexa Be Sworn as a Witness?

Advances in technology have drastically changed the face of forensics. Read the article Police Think Alexa May Have Witnessed a New Hampshire Double Homicide. Now They Want Amazon to Turn Her Over. Be sure to select "Read More" at the bottom of the first page to view the entire article, which presents the basics in a case in which two women were murdered and the police believe the Alexa device that was recording when the murders took place may hold the key to a suspect and solve that case.

After reading the article, discuss two or three of the following:

- How the recording stored in the Alexa device could be used as evidence in a crime.
- How the recording could be used to incriminate or exonerate someone from having committed a crime.
- The issues of privacy versus public safety.
- We can create advance directives for our health care should we be incapacitated (like after an accident or crime). Should you be able to create a digital advanced directive to grant permission to release any electronic evidence that may be available concerning your situation? What if your injury is caused by someone else? What if your injury may have occurred as a result of your committing a crime and the release could have legal consequences against you?

Response Guidelines

Read the posts of your peers and respond to at least two, expanding on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience; provide substantive and appropriate responses.

Course Resources
Graduate Discussion Participation Scoring Guide

u08d1 - Learning Components

- Understand what constitutes evidence.

Unit 9 >> Windows Forensics and Anti-Forensics

Introduction

This week you:

- Investigate conducting forensic analysis on a Windows machine.
- Discuss ethical issues associated with digital forensics.

This unit investigates the process for conducting forensic analysis on a Microsoft Windows system. As most current business systems use some version of Microsoft Windows, this unit will provide tools and techniques employed in most digital forensics investigations that involve computers.

Learning Activities

u09s1 - Studies

Readings

Use your *System Forensics, Investigation, and Response* text to read the following:

- Chapter 8, "Windows Forensics," pages 173–198.

Use the Internet to complete the following:

- InfoSec Institute. (2013). Forensic investigation on Windows machines [Blog post]. Retrieved from https://resources.infosecinstitute.com/forensic-investigation-windows-machines/
  - This post covers the registry keys in all current Windows operating systems, detailing the purpose and information stored in each registry key.
- Ozkaya, E., Alshakarti, H., & Comvalius, R. (2015). *Windows security and forensics* [Video]. Retrieved from https://mva.microsoft.com/en-us/training-courses/windows-security-forensics-14383? | Transcript.
  - This Microsoft video discusses how to best access data stored in the various areas of the Windows environment.
- SANS Digital Forensics & Incident Response. (2018). Windows forensic analysis poster. Retrieved from https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download
  - Download and print the poster for a handy reference to tools and techniques used frequently in Windows system forensics.

u09d1 - Anti-Forensics: Ethical Use?

To prepare for this discussion, use the Internet to read the following:

- De Alwis, W. C. (2017, Jun 29). An introduction to challenges in digital forensics [Blog post]. Retrieved from https://articles.forensicfocus.com/2017/06/29/an-introduction-to-challenges-in-digital-forensics/

Choose one of the anti-forensic techniques discussed to share with the class or select another technique not highlighted in the blog post (there are hundreds of anti-forensic techniques). Address the following in your initial post:

- Name and introduce the anti-forensic technique to the class.
- Identify why this technique poses a challenge to traditional digital forensics.
- Describe the value of the technique as someone learning digital forensics.
- State whether you consider it ethical to employ anti-forensic techniques knowing the challenges faced in crime investigation.
- State whether, as a forensic technician, it is ethical to share anti-forensic techniques with family and friends.

Response Guidelines

Read the posts of your peers and respond to at least two, expanding on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience; provide substantive and appropriate responses.

Course Resources
Graduate Discussion Participation Scoring Guide

u09d2 - Finding Resources to Help Solve an Impasse

Microsoft Windows is the most common business operating system in the United States. Within the Windows family, there are several current desktop options (Windows 7, 8, and 10) and server options (Windows Server 2012 and 2016). The primary resource for Microsoft Windows versions is TechNet, a Microsoft-sponsored website for all things Microsoft. Unfortunately there is little information for accessing content for forensic analysis. The investigator must be savvy and utilize the materials for accessing different areas of the registry, cache, and logs. If you have not visited TechNet, please do so before proceeding with this discussion.

Imagine you are in the midst of a difficult case and your attempts to retrieve the needed data have failed thus far. How would you further your knowledge and close any gaps in understanding that may be keeping you from the desired result? Where would you go? Whom would you consult?

Discuss the following:

- If the data is on a device but is inaccessible due to a passcode or other security measure, how would you try to access that data?
- What are some of the resources you found useful as you worked on solving the problem?

Response Guidelines

Read the posts of your peers and respond to at least two, expanding on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience; provide substantive and appropriate responses.

Course Resources
Graduate Discussion Participation Scoring Guide

Unit 10 >> Final Forensics Report

Introduction

This week you:

- Compile your course forensics report.
- Discuss and ethical question and reflect upon your course experience.

Maintaining the highest level of ethical behavior is essential for computer forensics examiners. In this unit, you learn how computer forensics experts and other professionals apply ethics and codes of conduct to their work. Computer forensics examiners are responsible for meeting the highest standards when conducting examinations, preparing reports, and giving testimony to ensure that evidence is accurate, reliable, and impartial. In addition, you must know when to recuse yourself from an investigation.

Learning Activities

u10s1 - Studies

Readings

Use the Internet to read the following:

- Easttom, C. (2017). Writing a forensics/expert report [Blog post]. Retrieved from https://allegiantinvestigation.com/writing-a-forensics-expert-report/
  - The author of your textbook outlines the major points to include and how to form each section of a forensics or expert report in this post.
- Kelley, M. (2012, May 30). Report writing guidelines [Blog post]. Retrieved from https://www.forensicmag.com/article/2012/05/report-writing-guidelines
  - This 2012 post remains relevant, providing several techniques for organizing forensic reports.
- Staib, M. (2017). How to write a forensic report. Retrieved from https://legalbeagle.com/5858380-write-forensic-report.html
  - This Web page provides an overview of common sections included in a forensic report.

Optional Reading

Use the Internet to read the following:

- Tittel, E., & Lindros, K. (2018, May 23). Best digital forensics certifications [Blog post]. Retrieved from https://www.businessnewsdaily.com/10755-best-digital-forensics-certifications.html

u10a1 - Forensic Report

Overview

By now you should have completed all labs and assignments for the previous units. If any lab is incomplete or points were lost, be sure to review the assignment and add the missing elements.

Throughout the course we have used several forensic tools and completed lab reports and separate assignments on each element. This assignment brings together the seemingly disparate aspects of an investigation into one final report that is suitable for submission to a supervisor or for use in court proceedings.

Scenario

It is time to compile your forensics report and write its executive summary for submission to Detective Morales.

Preparation

- Use the Digital Forensic Report Template linked in Resources to complete this assignment.
- Collect your submissions for your Units 3–8 assignments.

Instructions

- Compile your digital forensics report using information from your course assignments. Include an executive summary.
- Review the scoring guide before submitting your assignment to ensure that you meet all criteria.

Course Resources
Digital Forensic Report Template [DOCX]

u10d1 - How Authentic is CSI TV?

As a learner in this course, there is a good chance that you have watched television dramas or movies involving crime scene investigations. Although you have probably not had much training in the subject yet, share your impressions or opinions of some of the tools and procedures that are commonly used in these shows. Do they follow proper procedure? What digital technologies do they use? Are they realistic? If possible, include specific examples as you share your thoughts.

Response Guidelines

Read the posts of your peers and respond to at least two, expanding on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience; provide substantive and appropriate responses.

Course Resources
Graduate Discussion Participation Scoring Guide

u10d2 - Ethics: What You Need to Know

Not all digital forensic investigators know that professional codes of conduct and ethical practices must be followed in every examination. Experts specializing in training offer courses on digital forensics ethics to educate investigators.

For this discussion, expand your knowledge base by researching three or more training organizations that offer professional ethics courses.

- Focus on the ethical issues that can affect the ability of a forensics professional to be an expert witness in a court of law.
- Experts are typically paid by the organization for which they are hired. Consider the impact of this on the ability for paid experts to be impartial witnesses in a court of law.

Address the following:

- Often the experts employed by large companies perform analysis in multiple jurisdictions—potentially multiple countries. What additional concerns does this pose and how can those concerns be addressed appropriately?