PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Technical Project (ACCA7053)

Investigative Process

This Photo by Unknown Author is licensed under CC BY-NC

Lab Activities are based on

TryHackMe, EC Council – CHFI, and other Industry Digital Forensic Curriculum

Objectives

In continuation to our lectures, this hands-on Activity helps in providing you an overview of digital forensic investigation process.

ETHICAL STATEMENT

As discussed during our lectures, it is very important to adhere to Personal Ethics, Professional Ethics, Computer Ethics and Business Ethics.

We, the participants and stakeholders in the digital forensics laboratory, recognize the significance of ethical conduct when using digital forensics tools and processes for academic purposes. Our commitment to ethical standards is grounded in the principles of integrity, privacy, and responsible handling of digital data.

The tools and techniques you are exposed to' in this lab is to work only on a virtual machine environment and the purpose is entirely to demonstrate various digital forensic activities. Experimentation with these tools, techniques, and resources is at the discretion of the instructor and institution. If you as a student consider using these tools for educational purposes on an outside environment, you should contact your lecturer prior to any experimentation.

Note: Unauthorized access to data, computer, and network systems is a crime in many jurisdictions and often is accompanied by severe consequences, regardless of the perpetrator's motivations. It is the learner's responsibility, as the user of this material, to be cognizant of and compliant with computer use laws.

Task 1: Team Activity – Investigation and Image Acquisition
Task 2: Individual Activity – Analysis of Data from the acquired Image

ICONS Used in this document:

Find out the outcome/ Answers/ Solution

Do research and complete the task. Need referencing/ in-text citations. Shall be included as a part of your coursework.

Recommended Screenshot (with Timestamp) for your Coursework.

Recommended to address this part in your Coursework.

Scenario

Using the knowledge on Incident Response and Principles of Digital Forensics and its process, complete the following activities.

Task 1:

(Team Activity)

Team Size: 3 – 4

1. **Your team is part of an digital forensic investigation. The investigation scene is pictured below.**
    a. **Document the steps you need to do as part of digital forensic process. (Refer to the lecture: The process is to prepare, gather, Process and Present. Address each step)**
2. **Let's focus on the Preparation process. As a team, discuss and research various acquisition tools that are available for the following requirements. It is an open book activity. Feel free to use Internet, Books or any other resources to identify the tools. List out 5 tools (including open source and licensed tools). Include Vendor Name, Tool Name, Latest Version and the features of the tool. Make all assumptions. (Like OS etc)**

Task 2:

(Individual Activity)

Lets assume from the image you acquired as a Team, you found out a folder. (Your Lecturer will provide the Folder) *(Alternatively, complete it via tryhackme.com – Sign in and Click Intro to Digital Forensics)*

1. **Analyse the documents in the folder to find out information to help your investigation.**
2. **Document the steps you have taken and the details you have identified. Make sure that the authenticity and integrity of the evidence is essential for guaranteeing a forensically sound investigation.**
    a. **Document the tools you used**
    b. **Procedure followed**
    c. **Evidences found**
    d. **Ensure the authenticity and integrity of the evidence**

Overall Reflection

1. Understanding on the concepts discussed in the lecture and its relation to the activity done.
2. Understanding about various tools used and various frameworks available for DF Investigations.
3. Rate yourself: Understanding of Preparation – DF Investigation

----------End of Activity----------