|  |
| --- |
|  |
| Capstone Experience IST 894  Carl Laneave |
| Lab 10 Report |

Table of Contents

[1.0 Introduction – Computer Forensics Investigations 3](#_Toc150113900)

[1.1 Lab Results – Computer Forensics Investigations 4](#_Toc150113901)

[2.0 References: 5](#_Toc150113902)

[5.0 Activity Log 6](#_Toc150113903)

# Introduction – Computer Forensics Investigations

In this lab, the tools and procedures related to computer forensics were evaluated. Starting with the processes, as well as challenges that go into collecting digital evidence. This was discussed at length through the labs including handling data, using data in criminal cases, and intellectual property investigations.

An example of usage during intellectual property was around the discussion of digital evidence captured when songs were being illegally downloaded. In this case, the music companies had to prove how the downloads affected their overall business and distribution while at the same time proving that the downloader did not actually own the CDs. This type of IP law and forensics investigations focused on determining damage when IP was stolen.

Another example that was investigated was around collecting digital evidence in criminal cases. The lab talked about how to transfer data to drivers, how to do it with speed, tracking of data being saved, and how to handle said copied data in court. For example, as was discussed in the lab, when a digital forensics security engineer comes to court, they must only bring evidence related to that case. If they bring, for example, a notebook containing information on other cases it then becomes part of the case itself.

Lastly, the lab talked about how digital forensics data was used in court. An example they spoke about was timestamps. While timestamps can be manipulated by malware, it is not always the case. Many times, if a timestamp is manipulated, it is from the original offender trying to hide information. So, when defending your findings, it's important to understand that yes, timestamps could be manipulated, but the reality is that it is not a common action.

Collecting, handling, and managing digital forensics evidence is a key part of any security investigation. Not only is it important to understand how to do everything related to data, but also how it needs to be represented in court and pertaining to the law. The success of any computer forensics relies on this understanding and processes to be successful.

# Lab Results – Computer Forensics Investigations

A certificate of completion

Description automatically generated

# 2.0 References:

[1] moor. (2021, September 4). *Understanding Your Rights: Digital Evidence & Forensics*. Boulder Criminal Defense Lawyer. https://www.boulderdefenseattorney.com/understanding-your-rights-digital-evidence-forensics/#:~:text=Proper%20Search%20of%20Digital%20Evidence%20Requires%20a%20Search%20Warrant&text=A%20proper%20search%20warrant%20is

‌[2] *Fourth Amendment*. (n.d.). EPIC - Electronic Privacy Information Center. https://epic.org/issues/privacy-laws/fourth-amendment/#:~:text=The%20Fourth%20Amendment%20to%20the

[3] *The Warrant Clause in the Digital Age*. (n.d.). American Civil Liberties Union. <https://www.aclu.org/cases/digital-age-warrants>

[4] Wright, C. (2008, December 22). *SANS Digital Forensics and Incident Response Blog | Searches and the US 4th Amendment | SANS Institute*. Www.sans.org. https://www.sans.org/blog/searches-and-the-us-4th-amendment/

‌

‌

‌

‌

# 5.0 Activity Log

| **Member Name** | **Task Date** | **Task Details** |
| --- | --- | --- |
| Carl Laneave | 11/05/2023 | Created Template, executed all labs, took screenshots, and completed report |
|  |  |  |
|  |  |  |