|  |
| --- |
|  |
| Capstone Experience IST 894  Carl Laneave |
| Lab 9 Report |

Table of Contents

[1.0 Introduction – Digital Evidence and Legal Issues 3](#_Toc149511190)

[1.1 Lab Results – Digital Evidence and Legal Issues 5](#_Toc149511191)

[2.0 References: 6](#_Toc149511192)

[5.0 Activity Log 7](#_Toc149511193)

# Introduction – Digital Evidence and Legal Issues

The purpose of this lab was to go through the different legalities, as well as scenarios, that are related to cyber security as well as forensics. The focus, which is around the 4th amendment, is around evidence collection, legality of data, civil versus criminal cases and examples of cases related to each domain and subject.

The 4th amendment in the Constitution is designed to protect people from unreasonable searches as well as seizures. This is important to cyber security professionals as it directly correlates to how evidence may be collected and/or handled.

The first part of the lab focuses on what is considered a civil law case versus a criminal law case. A civil law case is a non-criminal case involving property rights while a criminal is a violation of law. Once the type of case has been determined, the next step is around discovery. Discovery as discussed is the process in which each side of the case obtains direct evidence related to the case itself. This occurs pre-trial to allow the defendants and plaintiffs to prepare for evidence presented at the trial. Another key part discussed was what a warrant means in the authorization of search and seizure of property.

Legal issues around cybersecurity are extremely tough in many regards. For one, evidence and forensics as discussed have to be handled at the highest level. Copies can be dismissed as the data copied may not hold its original integrity. Furthermore, if the tool used to do the forensics is new or not standard, the review can be dismissed such as it was in the Casey Anthony case around her Firefox search history. In this case, the security team used a non-validated tool to do their forensics which was called into question and caused the evidence to be dismissed. Key pieces of evidence such as her search history could not be used in court.

Another heavy focus was on probable cause and consent of search. Things such as wiretapping and recording conversations have several rules and laws around it. If someone is yelling in the street for all, that is legal to record. However, if you are having a private conversation in your home, that cannot be recorded without a warrant. Furthermore, data sent that is encrypted is protected unless there is probable cause to review it. Otherwise, there is no way for someone to intercept that data legally.

As cybersecurity researchers, professionals, and engineers, it's critical to understand the gathering, handling, and usage of digital evidence. Furthermore, it is important to understand the law clearly, as to avoid doing something inadvertently illegal or disruptive to a case. This field is still ever-growing and challenging when it comes to cyber legality. We as cyber security professionals must continue to grow, learn, and adapt to the laws around technology and digital evidence if we are to be successful in our roles.

# Lab Results – Digital Evidence and Legal Issues

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 | 10/29/2023 | Created Template, executed all labs, took screenshots, and completed report |
|  |  |  |
|  |  |  |