Lab 9 Report

Jason Tolbert

The Pennsylvania State University

IST 894-001: Capstone Experience

Dr. Michael Bartolacci, Instructor

Sunday, March 30th

Table of Contents

General Overview 3

Technical Overview 5

References 7

Screenshots 8

General Overview

This lab introduces participants to the world of digital forensics, especially as they relate to law and ethics.

A major focus on the lab is on the proper, forensically-sound, handling of evidence. Participants learn about write blockers, disk imaging software, and other tools that help ensure digital evidence is preserved in its original, unaltered, form. The proper preservation of evidence is critical, especially as it gets increasingly easier for emerging technologies like AI to shake the public trust in digital evidence (Klasén et al., 2024).

Participants examine several legal standards that shape how digital investigations are conducted, including the Fourth Amendment, Stored Communications Act, and Daubert standard. These policies help participants understand the level of caution that is needed to ensure that digital investigations remain compliant with the law. The difficulty of identifying the line between legal and illegal collections of evidence makes it difficult to realize when that line has been crossed — from an outsider's perspective, it can be hard to distinguish between criminals and people engaged in legitimate evidence gathering, and legitimate forensic professionals may find themselves subjects of criminal investigations as a result (United States Department of Justice, 2020).

To further illustrate the challenges of working in digital forensics, the lab goes over several case studies where there were either significant forensic failures or legal issues. For instance, the lab discusses the 2013 takedown of the illicit Silk Road marketplace, in which two DEA agents working on the case were found guilty of corruption (Sandick, 2017). It also discusses the 2011 murder trial of Casey Anthony, in which investigators made several mistakes that significantly weakened the prosecution's case — for example, only analyzing Anthony's browser history in Internet Explorer when Firefox was also installed on her computer (Goodison et al., 2015).

Technical Overview

This lab walks participants through the technical, legal, and ethical aspects of digital investigations.

Much of lab is about evidence preservation and integrity. Participants are taught how to use write blockers and forensic imaging software to prevent evidence from being modified. They also learn how to verify the integrity of digital evidence using cryptographic hash functions and gain and understanding of the importance of documenting every step in forensic acquisition processes to support defensible chains of custody.

Another part of the lab addresses the validation and legal admissibility of forensic methods and tools. It outlines the criteria set forth by the Fourth Amendment, Stored Communications Act, and Daubert standard to paint a picture how difficult – yet important — it is to only use forensic tools that are tested, validated, and widely accepted. Participants review several noteworthy incidents where failure to meet these standards – such as the 2013 Silk Road takedown and the 2011 Casey Anthony investigation — resulting in significant legal consequences for investigators.

The lab also covers ethical issues in digital investigations. Stingray cell phone interceptors are used as an example; they intercept cell data from *all* nearby phones, regardless of whether they belong to subjects of the investigation, raising questions about the ethics of spying on people who are not criminals or suspected criminals. Participants learn of the delicate scale on which ethics and legality sit in digital investigations and the importance of keeping that scale as balanced as possible.

References

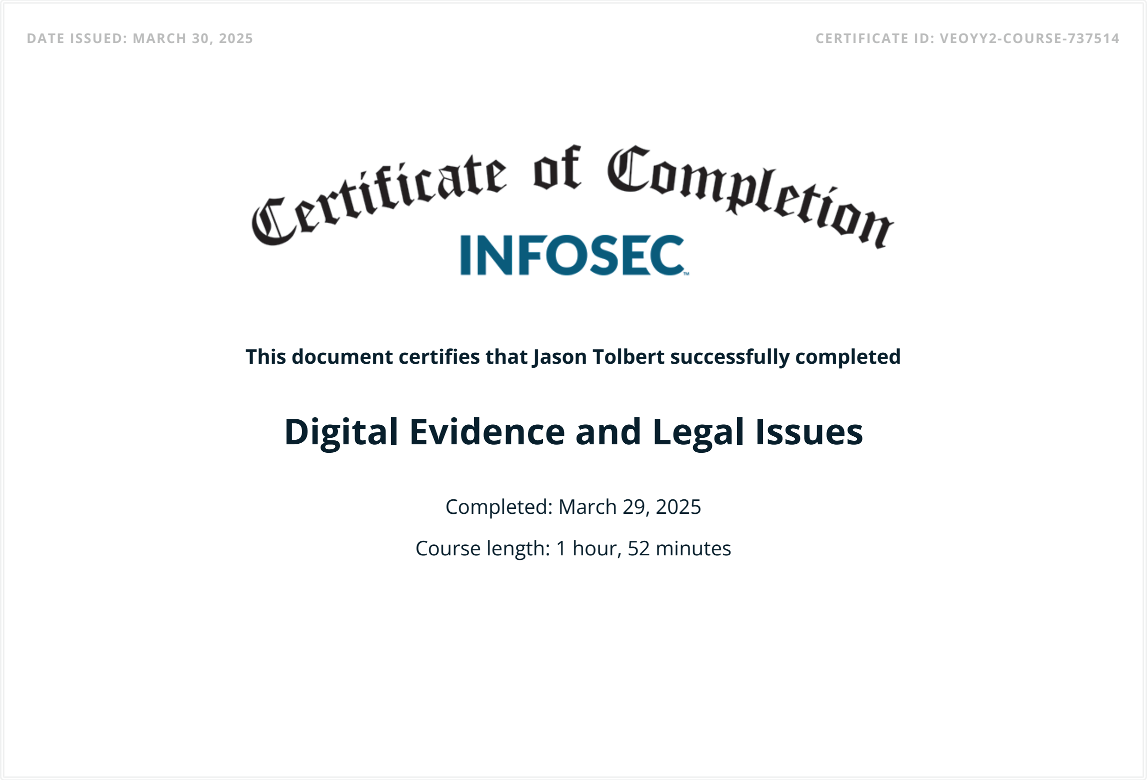
Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). Digital evidence and the U.S. criminal justice system: Identifying technology and other needs to more effectively acquire and utilize digital evidence. In *Digital Evidence and the U.S. Criminal Justice System* (pp. 1–32). RAND Corporation. https://www.jstor.org/stable/10.7249/j.ctt15sk8v3.1

Klasén, L., Fock, N., & Forchheimer, R. (2024). The invisible evidence: Digital forensics as key to solving crimes in the digital age. *Forensic Science International*, *362*, 112133. https://doi.org/10.1016/j.forsciint.2024.112133

Sandick, H. (2017, June 8). *A long journey through "Silk Road" appeal: Second circuit affirms conviction and life sentence of Silk Road mastermind*. https://www.pbwt.com/second-circuit-blog/a-long-journey-through-silk-road-appeal-second-circuit-affirms-conviction-and-life-sentence-of-silk-road-mastermind

United States Department of Justice. (2020, February). *Legal considerations when gathering online cyber threat intelligence and purchasing data from illicit sources*. https://www.justice.gov/criminal/criminal-ccips/page/file/1252341/dl

Screenshots



DATE ISSUED: MARCH 30, 2025

CERTIFICATE ID: VEOYY2-COURSE-737514

Certificate of Completion

INFOSEC

This document certifies that Jason Tolbert successfully completed

Digital Evidence and Legal Issues

Completed: March 29, 2025

Course length: 1 hour, 52 minutes

Figure 1. Certificate of completion.