PennState
College of Information Sciences and Technology

Lab Assignment Report

COURSE:	**IST 894**
ASSIGNMENT:	**LAB ASSIGNMENT REPORT 9**
SUBMITTED BY:	**BRANTLEY PRICE**
DUE DATE:	**AUGUST 3RD, 2025**
INSTRUCTOR:	**DR. BARTOLACCI**

Contents

General Context

This lab report covers an Infosec course entitled “Digital Evidence and Legal Issues.” It provides a reasonably detailed overview of the legal and ethical landscape IT professionals must be familiar with during the execution of their daily duties. One of the key takeaways is the careful balance between effective investigation and the fundamental right to be free from unreasonable search and seizure guaranteed by the Fourth Amendment. To that end, the course identified digital devices, like phones and laptops, as devices that contain large amounts of personal data. Because of this, the government generally requires a search warrant based on probable cause, as affirmed in the Riley v. California Supreme Court ruling (U.S. Supreme Court, 2014).

Beyond rights afforded by the Constitution, the course also covered complex laws that govern data held by third-party companies such as Verizon or AT&T. For instance, the Electronic Communications Privacy Act (ECPA) was covered. This federal law outlines the process by which law enforcement can obtain digital communications from these companies. The process was presented in a categorically tiered system, which determines how law enforcement agencies must obtain the data. Basic account information carries a lessened burden than the specific contents of a text message or email, for instance. This is important for IT professionals to understand, as data privacy is of the utmost importance, whether under the requirements of the EU’s General Data Protection Regulation (GDPR) or the United States’ Health Insurance Portability and Accountability Act (HIPAA) (Verimatrix, 2024).

The course effectively drove home the reality that a high level of proficiency is worthless without the underpinning of strong professional ethics. The mishandling of potential evidence or misrepresentation of findings can scuttle legal cases and destroy both personal and professional reputations. As IT professionals, it is vital to understand that ethical responsibility and compliance with legal and statutory frameworks are as important as the development of technical proficiency. Failures in this area could prove to be far more costly than simple technical errors.

Technical Context

This course taught practical considerations in the application of the Fourth Amendment when carrying out digital forensic workflows. When considering policy and procedure development, one of the core skills required is the ability to translate legal requirements into procedural documentation. Any amount of mishandling or chain of custody issues with data can result in said data becoming inadmissible in court. This is one of the reasons data confidentiality and integrity from previous courses and cyber ranges are so important. In the Federal Rules of Evidence, Rule 901. Authenticating or Identifying Evidence speaks to the requirements for the authentication of evidence. (b) (8) (A) states that data should be in a condition that creates no suspicion about its authenticity (Cornell Law School, n.d.-b). The proper technical controls and procedures must be in place to ensure this requirement is met.

Additionally, the Daubert Rules were covered in this course. The Daubert Rules are guidelines for determining whether an expert's methodology is valid. Consider things like whether or not the expert's technique can be tested for reliability or if the technique or theory has been subjected to peer review and publication (Cappellino, 2024). In this context, when being used in court, it is unlikely that a novel concept that is untested or not well-known to the community will withstand legal scrutiny. The Daubert Rules are just another ethical requirement for IT professionals to consider.

The statutory instruments used to compel the disclosure of electronic records, like the Stored Communications Act (SCA), are necessary to understand, especially within certain companies. Leaders and IT professionals alike must be able to differentiate the legal thresholds for the differing data types. 18 U.S. Code § 2703 outlines many of the requirements, including whether there is wiretapping, a compulsory court order, and even the disclosure to a foreign government (Cornell Law School, n.d.-a). Understanding this information and how to navigate the potential legal and ethical pitfalls therein will go a long way.

Screenshots

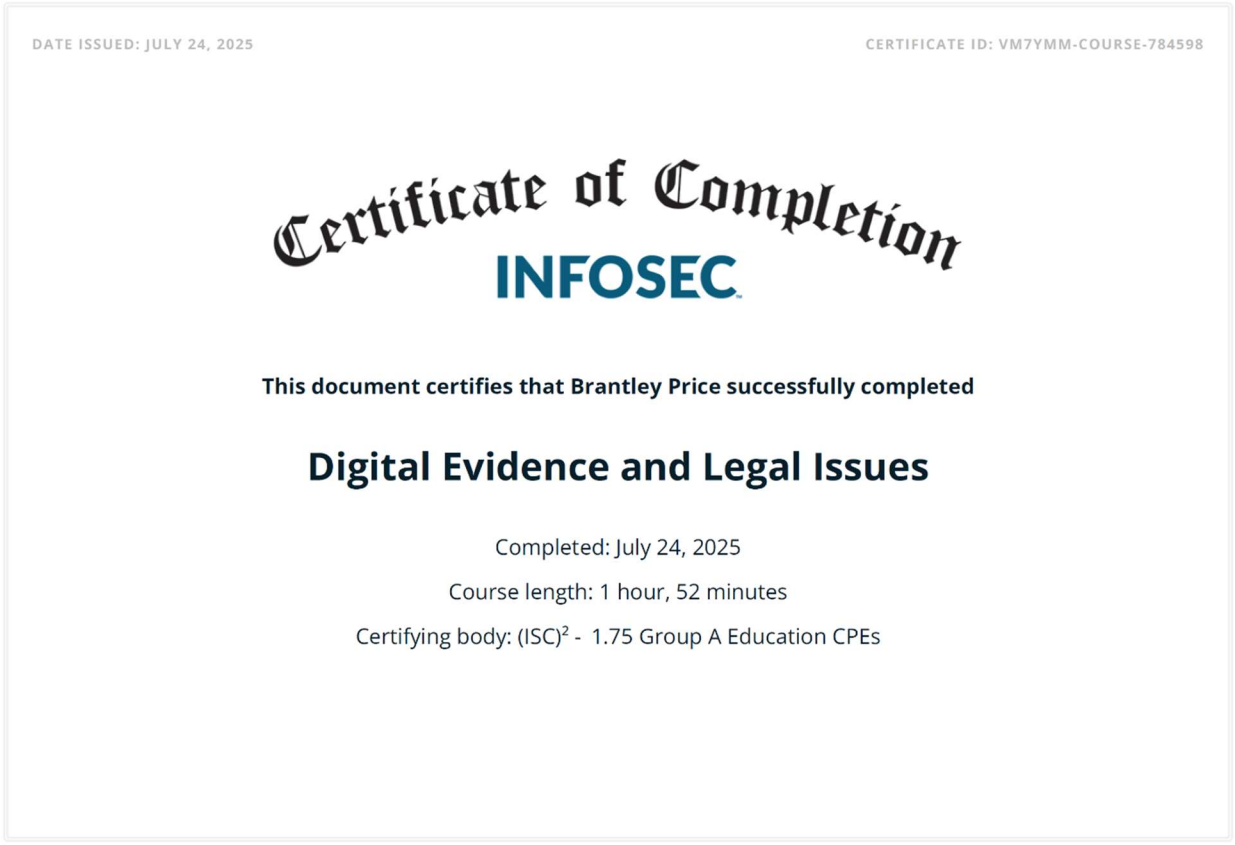

Figure 1: Certificate of Completion

References

Cappellino, A. (2024, May 9). *The Daubert Standard*. Expert Institute. Retrieved August 2, 2025, from https://www.expertinstitute.com/resources/insights/the-daubert-standard-a-guide-to-motions-hearings-and-rulings/

Cornell Law School. (n.d.-a). *18 U.S. Code § 2703 - Required disclosure of customer communications or records*. LII / Legal Information Institute. Retrieved August 2, 2025, from https://www.law.cornell.edu/uscode/text/18/2703

Cornell Law School. (n.d.-b). *Rule 901. Authenticating or identifying evidence*. LII / Legal Information Institute. Retrieved August 2, 2025, from https://www.law.cornell.edu/rules/fre/rule_901

U.S. Supreme Court. (2014, June 25). *Riley v. California, 573 U.S. 373 (2014)*. Justia Law. Retrieved August 2, 2025, from https://supreme.justia.com/cases/federal/us/573/373/

Verimatrix. (2024, November 25). *Why data privacy is key for cybersecurity professionals*. Verimatrix Cybersecurity. Retrieved August 2, 2025, from https://www.verimatrix.com/cybersecurity/knowledge-base/ensuring-data-privacy-is-an-essential-skill-for-cybersecurity-professionals/