Stewart Pawley

Digital Forensics

L-09

Dr. Finkbine

06/10/2025

Executive Summary: Digital Forensics in Federal Investigations

This executive summary presents an overview of digital forensics as outlined in the FBI Handbook of Forensic Services (2019) and the National Institute of Justice (NIJ) Forensics website. Both documents highlight the critical role of digital forensics in modern criminal investigations, emphasizing procedural rigor, scientific integrity, and strategic investment.

# Introduction

The FBI and NIJ collectively establish the federal framework for managing digital evidence. The FBI provides direct forensic services and operational support, while the NIJ advances forensic science through research, policy development, and resource allocation. Together, they shape the collection, analysis, and application of digital evidence in criminal justice (Federal Bureau of Investigation [FBI], 2019; National Institute of Justice [NIJ], n.d.).

# Key Points

Digital forensics involves acquiring, preserving, analyzing, and presenting data from digital devices such as computers, mobile phones, and cloud platforms. The FBI’s protocol ensures digital evidence is handled securely, avoiding contamination or alteration. Devices are to be submitted in antistatic packaging, with no prior access or manipulation by contributors. Chain-of-custody documentation is critical, and the FBI only accepts evidence from agencies that lack internal forensic capabilities (FBI, 2019).

The NIJ complements this operational approach with strategic support. It funds research in areas such as encryption, cloud forensics, forensic software validation, and data triage. NIJ initiatives also promote standardized methods to ensure evidence is legally admissible and scientifically reliable (NIJ, n.d.).

# Supporting Details

FBI forensic services prioritize investigative accuracy and evidentiary integrity. Submission policies prohibit duplicate testing unless justified and approved. For digital evidence, contributors must follow specific packaging and documentation requirements, including clear labeling, use of tamper-evident containers, and no device manipulation prior to submission (FBI, 2019).

In contrast, the NIJ serves as a research and policy agency, focusing on the development of tools and standards for future digital forensic needs. NIJ supports the integration of artificial intelligence, cross-jurisdictional access frameworks, and digital forensic examiner training. It also provides courtroom resources to assist prosecutors in presenting digital evidence effectively (NIJ, n.d.).

# Conclusion

Digital forensics is essential in solving complex modern crimes. The FBI maintains high standards for the collection and analysis of digital evidence, ensuring legal validity and investigative usefulness. Simultaneously, the NIJ drives innovation and strategic capacity-building across forensic disciplines. Their combined efforts foster a secure, effective, and forward-looking digital forensic ecosystem in the U.S. justice system (FBI, 2019; NIJ, n.d.)

#### Annotated Bibliography

Federal Bureau of Investigation. (2019). Handbook of forensic services. U.S. Department of Justice. https://www.fbi.gov/file-repository/laboratory/handbook-of-forensic-services-pdf.pdf/view

This manual offers detailed guidelines for submitting, packaging, and analyzing forensic evidence through the FBI Laboratory. Although focused broadly across all forensic disciplines, the handbook includes protocols relevant to digital forensics, such as secure transport, evidentiary integrity, and chain-of-custody procedures. It is an operational resource for law enforcement and supports the legal admissibility of forensic results.

National Institute of Justice. (n.d.). Forensics. Office of Justice Programs, U.S. Department of Justice. https://nij.ojp.gov/topics/forensics

The NIJ website provides an in-depth overview of the agency’s role in supporting forensic sciences through research, policy development, and training. Its digital forensics content emphasizes advancements in areas such as encrypted data access, forensic software validation, and evidence admissibility. It is a key reference for understanding the federal government’s strategic direction in forensic science and digital investigation.