PI magazine .com

professional investigator magazine

$9.95

January/February 2026

HISTORY'S REVOLVING DOOR

Forensics Challenge of the Slaying of Jennie Wade of Gettysburg

Traffic Crash Investigations: The Critical Role of the PI

The Case for Policy & Procedure Manuals in PI Agencies

Beware of Wolves in Sheep's Clothing

Decoding Investigative Databases

DEPARTMENTS

IN EVERY ISSUE

Building a Digital Forensic Laboratory: From the Floor Plan to the Documentation

BY **ROBERT B. FRIED**, EVP OF FORENSICS AND CHIEF INVESTIGATIVE OFFICER, PAGE ONE, INC.

The laboratory plays a critical role in digital forensics, serving as the space where practitioners can document, collect, receive, properly handle, securely store, examine, transfer, and dispose of electronic evidence. Throughout my career, I have been fortunate to work in or manage the operations of digital forensic laboratories. More recently, I have designed laboratories from the ground up for organizations. I consider every detail, from floor plans and building materials to furniture, environmental conditions, security systems, hardware, software, and documentation. Building such an important space requires careful attention to a wide range of factors.

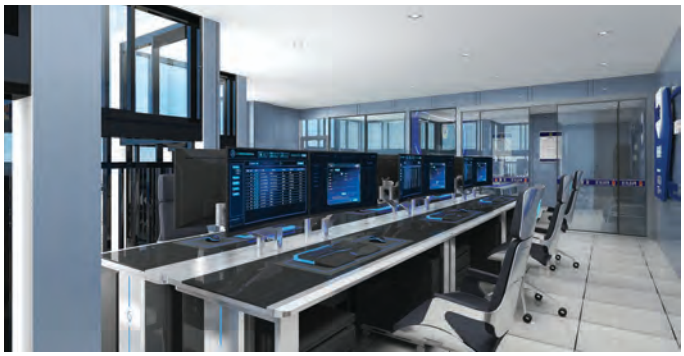
THE FLOOR PLAN

The digital forensic laboratory should be in a designated area of a building, with access restricted to authorized personnel. This is especially important when the laboratory is part of a multipurpose space, such as an office suite. The laboratory should provide ample space for all necessary tasks and functions, in compliance with local fire codes, depending on the number of team members staffing it. Organizations often have different setups for their laboratories. For example, the same space might include a staging area for data intake tasks, evidence lockers storing devices and media, and workbenches where digital forensic practitioners examine data. If the laboratory includes windows for natural light, additional considerations are necessary to ensure the integrity and security of the workspace.

BUILDING MATERIALS & FURNITURE

Constructing a digital forensic laboratory involves more than just building four walls. The materials used in the walls are also important. For example, incorporating a layer of metal mesh between drywall provides extra security against unauthorized entry. Walls should extend from floor-to-ceiling, with no drop ceiling, to prevent anyone from scaling them.

Selecting the right laboratory door is equally critical. A steel door with a saddle at the base to prevent objects from entering is ideal. The door should fit tightly with no gaps along the sides and be equipped with a key lock, accessible only to authorized personnel. Flooring should be made of materials that are safe from static discharge, which can damage electronics, and work surfaces, including benches, should use similar materials.



Many laboratories also require secure storage for electronic evidence. This is typically achieved with a separate room or designated area within the laboratory, equipped with security safes and storage lockers. These come in various sizes to accommodate different types of evidence and feature unique identifiers and locking mechanisms, ensuring access is limited to authorized personnel.

ENVIRONMENTAL CONDITIONS

The digital forensic laboratory must provide a safe environment, both for the personnel who work there and for the electronic evidence stored within. Proper temperature control is essential, and the laboratory should have its own thermostat. If the building's maintenance team regulates temperature, a supplemental HVAC unit may be necessary to allow lab personnel to maintain optimal conditions.

Lighting is another key consideration. Blackout shades are ideal to prevent unauthorized individuals from observing activities inside or around the laboratory, and windows should have locking mechanisms to prevent entry from outside. The laboratory also requires ample lighting, with LED lights often preferred for their energy efficiency and clarity.

SECURITY SYSTEMS

Monitoring activities in and around the laboratory is critical for maintaining security. Security cameras and guards should oversee the building and common areas where the laboratory is located. Cameras should cover all entry and exit points, whether the lab is in an office suite or a designated area, and be positioned strategically to provide unobstructed views. Organizations should determine whether to store recordings locally or in the cloud, based on internal policies. If the building's security system is separate from the laboratory's, it is important to understand the building's policies regarding access to those recordings.

Many organizations also use security devices to control entry to and exit from the laboratory. These devices typically have a built-in intercom and may work with an access badge, key fob or mobile app, and some even scan fingerprints. I have configured such devices to require multi-factor authentication, ensuring that personnel must use their access badge and fingerprint to enter and exit the laboratory.

HARDWARE AND SOFTWARE

Digital forensic laboratory personnel perform many of their tasks using specialized forensic hardware and software. These tools allow them to collect and examine electronic data sources while maintaining the integrity of the original data. Laboratories typically maintain a wide range of tools, including forensic workstations, write blockers, and examination software for computers, mobile devices, email, and other sources, to address the variety of evidence they may encounter.

In addition to forensics tools, laboratories often require hardware and software to create a secure network for storing operational data, working copies of evidence, and work products generated by lab personnel. This network should be separated from all other organizational resources and accessible only to authorized personnel.

DOCUMENTATION

In the field of digital forensics, documentation is crucial. I often say, no documentation equals no evidence! It is therefore no surprise that thorough documentation is a cornerstone of digital forensic laboratory operations. Personnel rely on a controlled set of documents, including standard operating procedures, to carry out many of their tasks. Documentation is also central to ANSI National Accreditation Board (ANAB) ISO/17025 accreditation, a globally recognized standard that ensures laboratories meet rigorous quality and technical requirements.

Key documents used by a digital forensic laboratory that support the lifecycle of electronic evidence include a Media Submission Form, Chain of Custody Form, Forensic Acquisition Form,

DATA COLLECTION LOG, AND DATA DISPOSITION FORM

- **The Media Submission Form** is completed by the sender and contains high-level information about the devices or media sent.
- **The Chain of Custody Form** is completed by all parties involved in transferring devices / media / data related to a matter. The form is updated every time evidence is transferred or moved.
- **The Forensic Acquisition Form** is completed by digital forensic practitioners and records information about the device, media, forensic practitioner, forensic tool used for acquiring evidence, and the results.
- **The Data Collection Log** is completed by digital forensic practitioners and contains a listing of sources and associated details for those sources that were collected for a matter. It is typically in spreadsheet format.
- **The Data Disposition Form** is completed by a party that is requesting specific actions to be taken with devices / media / data for a matter. The request may be to return or transfer it or physically destroy or permanently delete it.

To help keep this documentation organized, many laboratories use evidence management solutions. These data repositories track information about devices, media, and data that an organization currently holds or has previously handled. They can take various forms, including spreadsheets, databases, or ticketing systems.

Designing a digital forensic laboratory requires careful attention to many details, from construction materials to documentation practices. A well-designed laboratory protects evidence, preserves its integrity, and maintains meticulous documentation throughout its lifecycle. These measures are essential to ensure that laboratory activities are defensible and that the evidence remains admissible in court — a fundamental goal of every investigation. **PI**

Robert B. Fried is an accomplished expert with decades of experience performing data collections and forensic investigations of electronic evidence. He attained a BS and MS in Forensic Science from the University of New Haven. He holds and actively maintains industry certifications and is a licensed PI in Michigan, New York, and South Carolina. Robert serves on the Board of Advisors for the Masters in Investigations program at the University of New Haven, the Global Advisory Board for EC-Council's CHFI certification and is a Fellow at The Henry C Lee Institute of Forensic Science at the University of New Haven. He is the author of the books: Forensic Data Collections 2.0: A Selection of Trusted Digital Forensics Content *and Forensic Data Collections 2.0: The Guide for Defensible & Efficient Processes.*