Digital Forensics: Architectural and Engineering Facility Design Requirements

By Michael Mount, Adam Denmark

A fully equipped digital forensics laboratory contains numerous specialty spaces, each with its own unique and specific architectural/engineering design issues that must be addressed.

Digital forensics is currently one of the fastest growing laboratory sections in the crime lab. Most laboratories without digital forensics capabilities in their old facilities are either remodeling existing spaces or planning space for digital forensics in their new facilities.

There appear to be two forensic disciplines pertaining to digital media, “digital forensics” and “cyber forensics,” which have not yet been formally separated and defined. These terms have been used as labels for these disciplines, yet not consistently, since much of the literature on this subject uses these terms interchangeably between the two disciplines. For purposes of this article, these two disciplines will be generally defined and labeled as follows:

Digital forensics is the forensic investigation of devices capable of storing digital data, the purpose of which is to extract the digital data from such devices in order to assist in the investigation and prosecution of crime, and/or to be used as evidence in civil court cases. Examples of these devices include (but are not necessarily limited to):

- Computers and their digital components.
- Digital audio devices such as MP3 players, iPods, voice recognition devices, and audio surveillance devices.
- Digital video devices such as digital cameras, digital video surveillance devices, scanners, plotters, facsimile machines, and photocopiers.
- Combination audio/video devices such as CDs, DVDs, floppy discs, and USB drives.
- Communication devices such as cell phones, Blackberries, and iPhones.

Cyber forensics is the forensic investigation of unlawful security breaches in computer network systems. This would include the investigation of cyber worms and viruses, and hacking into secure networks, whether they are government, military, or private industry networks. Cyber examinations also include cases pertaining to classified information, espionage, and digital investigative support for the war on terrorism. Pursuit of persons responsible for child pornography, narcotics transactions, internet fraud, and any other illegal activities involving cyber space fall under the purview of cyber forensics. When these investigations uncover those responsible for unlawful cyber activities the violator’s computer hardware, software, and any device containing digital information becomes digital forensics evidence.

This article will focus on the architectural and engineering facility design requirements for digital forensics laboratories, not necessarily facility requirements for cyber forensics. This article will also explore some of the history and background that has led to the emergence of digital forensics as an essential and valuable forensic tool. We will look at the individual laboratory components that comprise digital forensics and address each of their unique facility design requirements. Finally this article will address the future of digital forensics as one of the forensic laboratory’s major investigative laboratory sections.
Digital Forensics Comes of Age
By the 1960s and 1970s the law enforcement community was becoming aware that computers were beginning to play an increasingly significant role in the world of crime. Typically, the investigation divisions in police departments began examining computers for digital data, and within a short period some crime labs began establishing a separate laboratory section for this purpose. These new lab sections were known as the “computer crimes” sections. At that time the facility design requirements for computer crimes included not much more than electronics laboratory bench space and a room for the storage of computer hardware exemplars and references.

Over the next two decades advances in digital technology led to a seemingly endless array of new digital devices which became available to businesses, the government, and the general public. All of these devices had the potential of becoming the subject of examinations as forensic evidence. The computer crimes section gradually became known as the digital forensics section and evolved to include several specialized spaces within this section, each with its own specialized design requirements.

In the early part of the 2000s, several government and law enforcement agencies were developing significant, large scale digital forensics units. Some of these agencies included the Federal Bureau of Investigation, the Defense Intelligence Agency, and the U.S. Department of Defense. In 2005 the Defense Department’s digital forensics laboratory was accredited by the American Society of Crime Laboratory Directors-Laboratory Accreditation Board (ASCLDLAB).

Many police agencies still examine and retrieve digital data from operable devices. However, if a device is inoperable due to damage by fire or if it is intentionally damaged prior to being seized, it is sent to one of the larger federal or regional forensic laboratories that have the resources for more expensive and complex investigative tools in its digital examination arsenal. For example, microprobe equipment using a combination of electronic and microscopic components can successfully restore a cell phone’s subscriber identification module (SIM card) that has been damaged or intentionally broken in half. In addition, the Department of Defense has developed technology that enables viable digital data to be retrieved from broken or otherwise damaged CDs.
Although many police agencies have limited digital forensic capabilities, the current trend is for digital forensics to become an integral and increasingly vital section of the crime labs, thereby keeping this investigative discipline under the forensic umbrella.

**Facility Design Requirements: General**

A fully equipped digital forensics laboratory contains numerous specialty spaces, each with its own unique and specific architectural/ engineering design issues that must be addressed. However, there are some general design requirements that are applicable for all of the spaces within the digital forensics unit.

*Laboratory Casework.* Casework typical for a wet chemistry laboratory is not desirable. Instead, casework components should be designed specifically for electronics repair, assembly, and examination and should be provided with electrostatic discharge (ESD) protection. This casework is available with numerous computer accessories, including door and drawer base cabinets, display mounts, keyboard trays, CPU placement, cable management, power distribution, rack mounts, and parts and supplies bins.

*Finishes.* For floor finish materials, an anti-static flooring must be considered. An acceptable product is one comparable to StaticWorx Grounded Solutions, Newton, Massachusetts. Wall and ceiling finishes for a digital forensics lab do not have any critical requirements. These finishes can be those typically applied to any laboratory environment.

*Mechanical Systems.* The Digital Forensics Section is one section in the crime lab that does not need to be designed like a wet chemistry laboratory. There are no requirements for single-pass air, extensive exhausts, and other high energy consuming features.

Instead heating, ventilation, and air conditioning (HVAC) systems can be designed similar to that of an office occupancy with a low velocity air handling system, resulting in substantial energy savings.

The biosafety/wet lab and the audio examination lab are exceptions, since they will require some additional HVAC design considerations. In the biosafety/wet lab spaces devices are examined that are biologically contaminated or require chemical processing. These rooms can be part of the central HVAC system, with the addition of single-pass air features and a negative relative pressure differential. Mechanical HVAC features that are designed to abate noise that are applicable to the audio lab include insulated ducts, silencers, and multiple diffusers.

Unlike other crime lab sections, no special water treatment is required, just sinks with hot and cold water conveniently located for cleaning dirty devices and hand washing. Chemical waste systems are not required, but an emergency shower/eyewash should be installed in the biosafety/chemical room.

*Electrical Systems.* The reliability and quality of the source of power at each building site should be examined. In addition to determining the adequacy of the power source, it must also be determined if additional power protection, such as surge protection, is required due to the sensitivity of digital devices. Typical bench power as part of the electronics casework should be the equivalent of a single 110V outlet at 6 inches on centers. Rooms for the examination of digital video devices will require special attention to the quality and control of lighting.
Facility Design Requirements: Specific Spaces
As a minimum, the ideal digital forensics laboratory should contain the following individual, special purpose rooms:

- General examination
- Audio examination
- Video examination
- Radio frequency shielded examination
- Hardware exemplar and reference storage

**General Examination.** This is the portion of the digital forensics laboratory where each examiner will be provided his or her individual examination workstation. Multiple workstations should typically be laid out in an open laboratory design. A reasonable size for an individual workstation ranges from 15 linear feet of electronics bench to 100 square feet of bench space in a U-shaped configuration.

**Audio Examination.** “An audio recording is subject to a number of possible distortions and artifacts. For example, the persistence of sound, due to multiple reflections from various surfaces in a room, causes temporal and spectral smearing of the recorded sound. This distortion is referred to as audio reverberation time... Because reverberation depends on the shape and composition of a room, differences in the estimated reverberation can be used in a forensic and ballistics setting.” (Hafiz Makik, Department of Electrical and Computer Engineering, University of Michigan, Dearborn.)

The examination of digital audio media necessitates an acoustically isolated space to allow the examiner to concentrate on the evidence without any interference from outside noise. Stephen Katz, an audio engineer, is the Director of Applied Research and Technology at Troy Acoustics of Santa Clarita, California. His recommendations for the design of an audio forensics laboratory are as follows:

The Noise Criterion (NC), a single numerical index commonly used to define design goals for the maximum allowable noise in a given space, should be NC-15 for audio analyses. NC-15 should be achievable at multiple frequencies ranging from 63Hz to 8000Hz, and
shall consider all ambient noise. Sound Transmission Class (STC), an integer rating commonly used in the building industry to classify how well building partitions and doors attenuate airborne sound, should strive for STC-70. Doors need to be solid core with full seals and gaskets. At the rear wall of the space, opposite the speakers, the Noise Reduction Coefficient (NRC), a scalar representation of the amount of sound energy absorbed upon striking a particular surface, should be equal to or less than 1.1 when tested at frequencies ranging from 125Hz to 4000Hz.

The HVAC ducting needs to be rigid, acoustically lined, and ideally sized by a factor of 3. There should be a sound attenuating device at the fan unit, and an inline diffuser before the room air register. Since electronic light dimmers can generate noise in the bulbs as well as electrical interference, auto transformers should be used for dimming.

**Video Examination.** With the increasing ease in digitally manipulating photo images, there is a significant need for mathematical and computational algorithms to aid forensic examiners to detect tampering in digital media. Video itself has always been a ground breaking weapon against crime, but now even poor-quality videos can be enhanced to provide even more valuable data through an extremely powerful, yet cost-effective, toolset for forensic video enhancement.

Lighting control is the primary requirement for the design of a video examination space, which should include dimmable lighting and variable light quality sources. In order to enhance the concentration ability of the examiner, the space should be acoustically controlled, yet not to the extent required for digital audio analysis.

**Radio Frequency Shielded Examination.** The world today is increasingly electronic, with electronic devices producing millions of waves and signals permeating the air at any given moment. The electromagnetic waves generated by electronic devices may negatively affect other, similar, electronic devices. Such effects are called Electromagnetic Interference (EMI) and Radio Frequency Interference (RFI). EMI and RFI cause suppression of signals generated internally in a device. It also causes external ambient interference with equipment operation and emissions generated internally that will interfere with equipment operation. Therefore, EMI and RFI are problems in forensic investigations where EMI and RFI can corrupt the digital evidence within a device.

The primary line of defense against this contamination is to provide EMI/RFI shielded rooms in which to conduct the examinations of any device that sends or receives a radio frequency signal. Various shielding systems can be used including spray-on agents, wire mesh enclosures, Faraday shielding, and other solutions. Special attention must be given to the design of any penetrations into the shielded space, such as plumbing, electrical conduit, or mechanical ducts, to ensure that each penetration is adequately shielded. Access into a shielded room should be through a shielded ante room or airlock.

**Exemplar and Hardware Reference Storage.** The Digital Forensics section requires a collection of digital hardware references for the same reason that the Firearms Section maintains a weapons collection. A weapons reference collection for the Firearms Section of a crime lab can typically include several thousand handguns and long guns. The two-fold purpose of such collections is (1) to be able to identify an evidence weapon of questionable identity with a known weapon, and (2) to render an inoperable evidence weapon operable by using parts from a similar reference weapon. Digital devices seized
as evidence may be unidentifiable or inoperable, and the digital reference collection can be used to identify a device or render a device operable in preparation for examination.

The quantity of digital devices comprising a comprehensive reference collection can reach the thousands and will include any and all of the types of devices that are the subject of this article. Design requirements for the storage of these references include substantial quantities of adjustable storage shelving, preferably high-density mobile systems, and environmental controls for temperature and humidity.

Additional Examination Spaces
Depending on the established procedures, function, and examination policies for the digital forensics section, the following additional functions might be incorporated into the laboratory design:

- Computer data recovery
- Hard drive repair
- Electronics laboratory
- Electronics workshop
- Biosafety/wet laboratory

All of these functions, with exception of the biosafety/wet laboratory can be undertaken in the General Examination laboratory. However, in the larger regional laboratories with a very high caseload, it might be practical to design dedicated spaces for one or more of these functions. Depending on the caseload, a Class 100 cleanroom might be required for hard drive repair work. A dedicated space should be provided for the examination of any devices that might be biologically contaminated or that require examinations using chemicals. The room should be equipped with a chemical fume hood and be accessed through an airlock.

Conclusion
It has been an exciting transformation from the emergence of Computer Crimes Sections, through the advancements in digital technology, and the resulting development of Digital Forensics as a viable crime fighting tool. Will digital technology continue to change the face of the cyber world as it has in past decades? If so, what does this mean to the future of Digital Forensics? In 2009 Symantec Corporation of Mountain View, California, released its new Internet Security Threat Report, volume XV, which highlights key trends in cyber crime over 2009. The report reveals continued growth in both the volume and sophistication of cyber crime attacks." (DFI News, April 30, 2010.) For the first time, incidence of theft of information and electronic data at global companies has overtaken physical theft, according to the latest edition of the Kroll Annual Global Fraud Report. (DFI News e-Newsletter, October 29, 2010.)

“Your ordinary bank robber can now steal hundreds of account numbers from ATMs without so much as lifting a finger.” (Robert Vamosi, “High-tech bank robbers phone it in,"C-Net News, October 9, 2008.) “The FBI has arrested and charged a group of individuals suspected of being involved in a global bank fraud scheme…to steal millions of dollars from U.S. bank accounts, netting more than $3million in stolen funds." (The New New Internet, October 1, 2010.) It is possible that in the near future, the traditional bank robber with a gun, ski mask, and a demand note will be obsolete.
All indicators point to continued advancements in digital technology, possibly at a more rapid rate than in the past. Safeguards, software, and investigative techniques designed to stop cyber crimes will continue to be developed, and cyber criminals will continue to develop methods to thwart those efforts. The future will see more forensic agencies devoting space to digital and cyber forensics, so the architects and engineers that design these spaces must continually keep updated and well informed of the unique and specialized facility design requirements for digital forensics laboratories.

Michael Mount, AIA, LEED Architect, has devoted the past 25 years of his career as an architect almost exclusively to the planning and design of forensic facilities. He is currently a principal with Smith Group. The combined experience within Smith Group’s eleven offices includes the planning and design of over 7-million square feet of forensic facilities throughout the United States and abroad. Michael leads Smith Group’s team of forensic design specialists, and can be reached at micheal.mount@smithgroup.com.

Adam Denmark, AIA, LEED Architect, is an associate architect with Smith Group. He has 15 years of diversified architectural practice, and for the past five years has been a key member of Smith Group’s team of forensic facilities specialists. He was one of the key laboratory planners for the 650,000 square foot forensic facility in Toronto, Ontario, currently under construction, which contains an extensive digital forensic section. Adam can be reached at adam.denmark@smithgroup.com.

Reprinted with Permission of Forensic Magazine®.
www.forensicmag.com