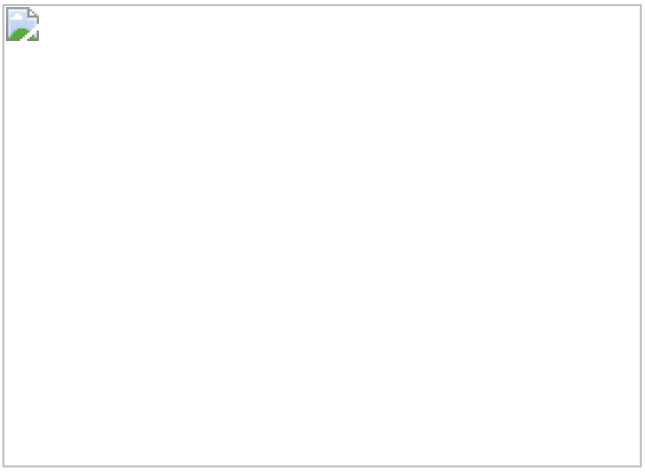
Forensic MAGAZINE

Crime Lab

Wal-Mart Stores, Inc. Leads with E-Discovery: Part 2

Wed, 05/07/2014 - 8:08am by Ken Mohr and Larry Depew



During the development time of this article and publishing "Part One"; Walmart's E-Discovery and Forensic Services Laboratory has *achieved* ASCLD/LAB accreditation. Ken Mohr, a principal at Crime Lab Design, will now continue to explore some of the physical space needs that attributed to the project's success with Larry Depew whose company, Digital Forensics.US, LLC consulted on the project.

Describe the existing conditions in the laboratories and the changes that have occurred over time through your recommendations?

The first thing that was evident during my first visit to the lab was management's desire to ensure operations met best practices and accreditation standards.

The lab personnel associates were exceptionally talented and

DEEPER INSIGHTS

competent. Lab space was at a premium with each associate being assigned a 6′ x 6′ cubicle. They maximized the space by placing forensic equipment on shelves above the workbench. This was challenging for the examiners since access to the forensic machine is a routine requirement. Further, it reduced productivity since it made multi-tasking difficult. Over the course of the past two years, the laboratory has expanded and there are plans for a much larger expansion. Associates are working smarter; maximizing space usage more efficiently. For example, they merged common technical procedures into one common area.

Walk us through the experience of entering the facility and getting into the lab.
The security of the building in which the laboratory is housed is very good. It is manned with uniformed personnel and each person entering the building must badge in through an electronically secured door. Visitors must register and are escorted. The laboratory itself is secured with a dual-authentication hand-geometry scanner combined with a password created by each authorized associate. I considered the overall security to be exceptional. Procedurally, we had to made adjustments such as logging visitors into the lab.

Describe some of the enhancements that have occurred in the lab.
The laboratory's policies and technical procedures, generally maintained on an internal Wiki, were formalized into Quality, Technical, Operations, and Training Manuals that map to the international standards and industry best practices. We identified the core knowledge, skills, and abilities that each associate would be required to establish to be internally certified as being competent to conduct independent casework. During our first year, we focused on evolving those policies and procedures into the routine of the laboratory's work. At the end of the first year of the project, my staff conducted a mock ASCLD/LAB assessment with recommendations for continuing process improvements.

The physical plant expansion offered opportunities for more workspace. With expansion, the original space was reconfigured so that the hard drive recovery team could build

a mini-lab within the lab. This allows for microscopes and soldering equipment to be set up in a single area with adequate room to disassemble and repair hard drives for data recovery. Previously, this equipment was located in three areas of the laboratory. Conference rooms and training rooms are at a premium and shared with other Wal-Mart Stores, Inc. business units, but are carefully managed to ensure that training is afforded on a regular basis.

The following list of spaces is important for Digital Forensic Labs. Can you tell us a bit about these spaces in this project?

Secure entry and leave your personal cell phone behind: For security of the Walmart facility and its employee's privacy, photographs are prohibited. While relinquishing cell phones is not required, visitors cannot help but be cognizant that just about every area of the work space is monitored by video cameras.

Main exam/workstation area: Each examiner has his or her own cubicle for conducting examinations. As I mentioned earlier, the hard drive recovery examiners have a common work area where they can share not only equipment and work space, but ideas on how to troubleshoot problematic devices. Several machines are continuously running programs to recover data on corrupted hard drives. There are also common areas for mobile and video forensics.

Takedown room: There is no room dedicated for disassembly. The fact is that most data collected by the examiners comes from network-acquired sources. A very small number of cases have physical devices submitted to the laboratory. As an example, during October the lab responded to nearly 400 requests for services and only about 5% of those involved a physical device.

What types of equipment and software does the laboratory use to provide services: The laboratory is well equipped. They have a wide variety of hardware and software common to any law enforcement forensic laboratory. Forensic workstations, write blockers, disk duplicators, mobile device equipment, and more can be observed throughout the lab. They use the most common forensic software, but have developed in-house methods to efficiently collect data from unique sources.

Together, we tested and validated those in-house methods over the course of this project.

Their methodologies are quite similar to what we would see in a sophisticated laboratory. Data is identified, securely collected, imaged logically or physically, hashed, analyzed, reported, and archived. Each associate has a staging drive or server to facilitate casework. The results are provided to the customer electronically under cover of a report. The collected data results are archived to a storage area network in a designated location outside of the lab.

Storage (evidence): As mentioned previously, unlike law enforcement labs, the laboratory handles relatively few physical devices since data collected and preserved often resides on the Walmart internal network storage. However, when physical devices are encountered, the lab's processes and evidence storage are no different than a law enforcement facility. There are two types of evidence storage: Long-term and short-term. Long-term evidence storage is located in a separate facility data center facility which has a very high level access control procedure. Each examiner is assigned a temporary storage locker to store digital devices while the associated service request is ongoing. Physical evidence is documented to a paper chain of custody while data collected and processed virtually is verified through process logs and hash verification throughout the process from collection to archiving.

Storage (in process evidence): When physical evidence is undergoing examination or processing by associates and the evidence is unattended, a warning placard is placed on or around the evidence to ensure that other personnel are aware and cautious when entering the examination area.

Finally, as Larry walked the halls of the facility he had this to say "I noted the following quote on the white board of former lab director and Senior Director Jerry Geisler: 'We must all suffer one of two things: the pain of discipline or the pain of regret or disappointment.'" That quote set the tone for the project's success.

Ken Mohr *(kenm@crimelabdesign.com) is a principal and senior forensic planner with Crime Lab Design which provides*

full architectural and engineering services for forensic and medical examiner facilities worldwide.

Larry Depew *(larry@larrydepew.com), founder of Digital Forensics.US LLC., is a retired FBI Supervisory Special Agent and Laboratory Director of the New Jersey Regional Computer Forensic Laboratory (RCFL). He was certified by the FBI in computer and mobile forensics. He is a certified ASCLD/LAB and A2LA assessor. He is a graduate of the University of Maryland. He later attended George Washington University earning a graduate certification in Project Management and undertook management training at Northwestern University, Kellogg School of Management. He is a certified PMP through the Project Management Institute. He has guided many laboratories internationally to accreditation.*

Crime Lab