B23 Seize All Find All: Crime Scene Recovery of Digital Evidence

Megan L. Bishop, MFS, and Sarah E. Nolton, BA, Department of Defense Computer Forensics Laboratory, 911 Elkridge Landing Road, Suite 300, Linthicum, MD*

The goal of this presentation is to present to the forensic community several guidelines for proper crime scene recovery of digital evidence.

The burgeoning field of computer forensics is expanding into almost every traditional forensic situation. Whether at an on-site seizure, in the laboratory, or responding to an unknown crime scene, the traditional investigator or first responder must be aware of some special considerations that may prove crucial to their ensuing investigation. Digital evidence is present in almost every crime scene and permeates every type of crime. It is paramount for an investigator to be aware of the need to properly search for, handle, and process digital evidence. Digital evidence is regularly processed in such varied investigations as death, drug, fraud, counter-intelligence or counter-terrorism, child abuse or exploitation, and sexual assault cases.

In addition to home or business computers, digital evidence is present in almost every format; cell phones, pagers, Personal Digital Assistants (PDAs), internal phone systems, fax machines, mp3 players, videotapes, digital cameras, and audiotapes are just a few of the many types of digital evidence that may be encountered and merit consideration. Many of these types of digital evidence have special time constraints or processing requirements that are tantamount to evidence retrieval in the laboratory. Pagers, cell phones, laptops, and PDAs may be unable to be processed without properly charging or having power supplied during evidence collection or storage. PDAs in particular need a constant power source such as batteries or a charger in order to preserve data stored within its extremely volatile memory. Addresses, names, phone numbers, calendars, or other significant leads may be lost without proper evidence collection technique specific to these types of digital evidence.

Another area of consideration is the expanded role first responders must take when encountering a crime scene with digital evidence. In addition to their traditional roles of securing the crime scene, first responders must uncover and assess telephone or Internet connections and the possibilities of remote access. It is important to immediately seize control of all computer and communication systems and networks by disabling external connections and stopping any potentially destructive processes. Any actions taken by the first responder should be thoroughly documented with notes or photographs.

Investigators must also expand their documentation when encountering digital evidence in the field. Paper, software and notes found on or near digital media may provide user names, passwords, account information or other information useful to laboratory analysis. When encountering a computer, investigators should carefully document any processes running including email applications, Internet access or open files. If possible, investigators should close all documents and running processes to perform a proper shutdown. If necessary, investigators may choose to simply power off or pull the power cord. It is important to note that investigators not do anything that could possibly alter digital media. Simply opening a file on a computer can unintentionally alter or destroy data. At the very least, date and time information may be lost that later proves to be relevant to the investigation; at worst, the investigator may start a destructive process unintentionally.

After initially stabilizing the digital crime scene, investigators need to assess any special constraints presented by digital evidence. Searches, seizures and analysis may be limited by time, equipment or legal restrictions. Investigators can triage digital media to determine what, if anything, can be processed on-site or if media should be seized and processed in the laboratory. Processing on-site may consist of creating an exact duplicate of the media or simply copying files depending on the needs of the crime scene. In the majority of cases, it is important to make a forensic copy of the original media.

If processing on-site is not possible and seizure is necessary, simple steps ensure proper packaging and handling of digital evidence. Most media found in the digital crime scene is magnetic and highly susceptible to electrostatic discharge. Anti-static bags and packaging materials mitigate loss or corruption of data during shipment. Traditional investigators, first responders and crime scene technicians need to be aware of some of the special considerations of digital evidence handling in the field to preserve data for later analysis.

Computer Forensics, Digital Evidence, Crime Scene Investigation

 ** Presenting Author*