



**Homeland
Security**

Science and Technology

TechNote

U.S. Department of Homeland Security



System Assessment and Validation for Emergency Responders

The U.S. Department of Homeland Security (DHS) established the System Assessment and Validation for Emergency Responders (SAVER) Program to assist emergency responders making procurement decisions. Located within the Science and Technology Directorate (S&T) of DHS, the SAVER Program conducts objective assessments and validations on commercially available equipment and systems, and develops knowledge products that provide relevant equipment information to the emergency responder community.

SAVER Program knowledge products provide information on equipment that falls under the categories listed in the DHS Authorized Equipment List (AEL), focusing primarily on two main questions for the emergency responder community: "What equipment is available?" and "How does it perform?" These knowledge products are shared nationally with the responder community, providing a life- and cost-saving asset to DHS, as well as to Federal, state, and local responders.

The SAVER Program is managed by the National Urban Security Technology Laboratory (NUSTL), which also prepared this TechNote.

For more information on this and other technologies, contact the SAVER Program by [e-mail](mailto:SAVER@hq.dhs.gov) or visit the [SAVER website](https://www.dhs.gov/science-and-technology/saver).

E-mail: NUSTL@hq.dhs.gov

Website: <https://www.dhs.gov/science-and-technology/saver>

Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement, recommendation, or favoring by the U.S. Government. Neither the U.S. Government nor any of its employees make any warranty, expressed or implied, including but not limited to the warranties of merchantability and fitness for a particular purpose for any specific commercial product, process, or service referenced herein.

Digital Forensics Tools

Forensics is the application of scientific tests or techniques used in criminal investigations. Digital forensics is the process of recovering and preserving materials found on digital devices. Digital forensics is needed because data are often locked, deleted, or hidden. There are five primary branches of digital forensics and they are categorized by where data is stored or how data is transmitted. Digital forensics tools are hardware and software tools that can be used to aid in the recovery and preservation of digital evidence. Law enforcement can use digital forensics tools to collect and preserve digital evidence and support or refute hypotheses before courts.

Digital Evidence

Digital evidence is any information stored in digital devices that can be used in courts. Conventional examples are files stored in a computer or mobile device, such as e-mails, images, and internet browser histories. Other examples include the navigation history of a vehicle, logs from an electronic door lock, swipes/scans on a public transportation card, and settings of a digital thermometer. Due to the ubiquitous nature of digital devices used in crimes, digital evidence tends to be more voluminous, more expressive, and more readily available than other types of evidence. Digital evidence is often associated with cybercrimes, such as cyberattacks, child pornography, and credit card fraud, but it can also be recovered in many different crimes due to the proliferation of digital devices in our daily lives. Digital evidence is often questioned for its authenticity since it can be modified or duplicated, but courts in the United States tend to reject this argument without proof of tampering. Law enforcement agencies should have proper chain of custody when handling digital evidence and ensure that all evidence is preserved for proper forensic analysis. The agencies should also take proper precautions when handling digital evidence. When investigators collect evidence from a digital device, evidence related to another crime might be discovered. Investigators need to obtain a second warrant in order for the evidence to be admissible to courts. In general, criminals often leave digital footprints in their digital devices.

Branches of Digital Forensics

The five branches of digital forensics are computer forensics, mobile device forensics, network forensics, database forensics, and forensics data analysis. Computer forensics focuses on recovering and preserving evidence in computers and storage devices such as hard drives and flash drives. Mobile device forensics, on the other hand, is the recovery and preservation of digital evidence in mobile devices, such as smartphones and/or tablets. Network forensics monitors network intrusion and analyzes

network traffic, such as local and WAN/Internet. Database forensics focus on evidence found in databases. Forensics data analysis studies the structure of data and aims to discover patterns.

Digital Forensic Tools

Law enforcement uses digital forensics software and hardware interchangeably. Most products available to law enforcement, whether open source or commercial, concentrate on computer and mobile device forensics, as these two branches are more prevalent.

The performance requirements for computers used in digital forensics are high, requiring larger capacity hard drives, faster central processing units (CPUs), bigger memory, etc.

Hardware

Hardware tools are designed primarily for storage device investigations, and they aim to keep suspect devices unaltered to preserve the integrity of evidence.

A forensic disk controller or a hardware write-blocker is a read-only device that allows the user to read the data in a suspect device without the risk of modifying or erasing the content. Conversely, a disk write-protector prevents the content in a storage device from being modified or erased. A hard-drive duplicator is an imaging device that copies all files on a suspect hard drive onto a clean drive; it can also duplicate data in flash drives or secured digital (SD) cards. A password recovery device employs algorithms, such as brute-force or dictionary attacks, to attempt to crack password-protected storage devices.

Software

Most forensic software applications are multi-purpose and can perform various tasks in one application. Some applications are open source, which allow experienced programmers to modify the code to meet their specific needs and provide cost savings for law enforcement. Some can process multiple devices simultaneously or manage different operating systems (e.g., Windows and Linux). The capabilities of these applications can be categorized by the branches of digital forensics employed.



Hard-drive duplicator
Photo courtesy of Guidance Software

Computer forensics software complement the hardware tools available to law enforcement. While the hardware tools such as write-blockers primarily focus on preserving the evidence in a target device, software applications can acquire and analyze the digital evidence collected from the suspect device. Suspects often hide or delete their files or partition the hard drives of their computers so that evidence is difficult to discover; however, forensic software applications can assist investigators in recovering this evidence. Windows Registry records when, where, and how a file is created, renamed, viewed, moved, or deleted, and some applications can perform registry analysis to collect and analyze these traces. In short, certain user activities can be recovered and investigated with digital forensics software.

For mobile device forensics, while the focus is primarily on mobile phones, most digital devices with internal memory and communication ability, such as GPS devices, smartwatches, or tablets, can be investigated with these applications. The applications focus on the suspect's activities on a mobile device. For instance, the applications can analyze when and how a crucial piece of evidence was sent from a suspect's smartphone. Phone call logs can be recovered to verify alibis or establish timelines. When unlocked, instant messages from SMS or apps like WhatsApp can be searched with keywords to assist the investigation and be presented as evidence in courts. Similar to hard drives and other storage devices, data stored in the flash memory of a mobile device can be recovered. Investigators can also recover geolocation from a mobile device itself or from location based services, if the feature was turned on, to establish the record of use of the mobile device.

Encryption is considered by experts as the greatest challenge to law enforcement and a major limitation in digital forensics as it disrupts initial examination where pertinent evidence might be located. Encryption is a security measure that transforms data to a secured format that is unreadable to unauthorized parties. Authorized users can enter the password or a pin code to decrypt the data and transform it back to their original, readable format. In theory it is possible to decrypt encrypted data without the password or a pin code, but for a well-design encryption scheme, large computational resources and skills are required.