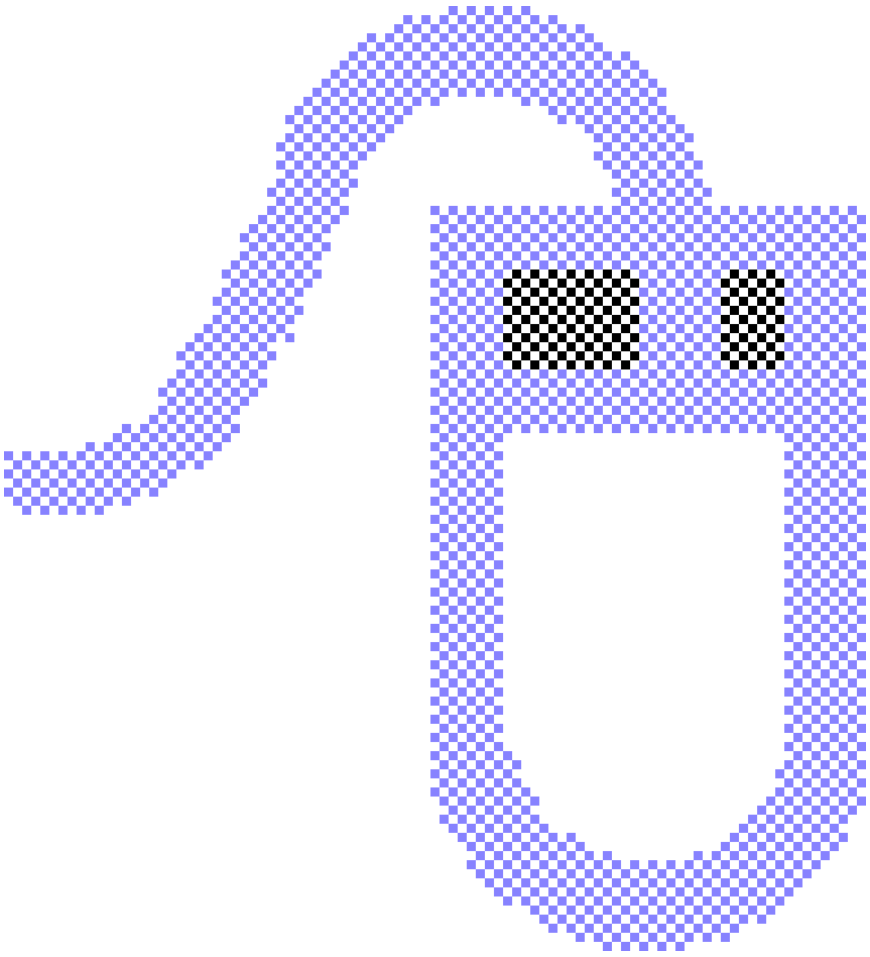
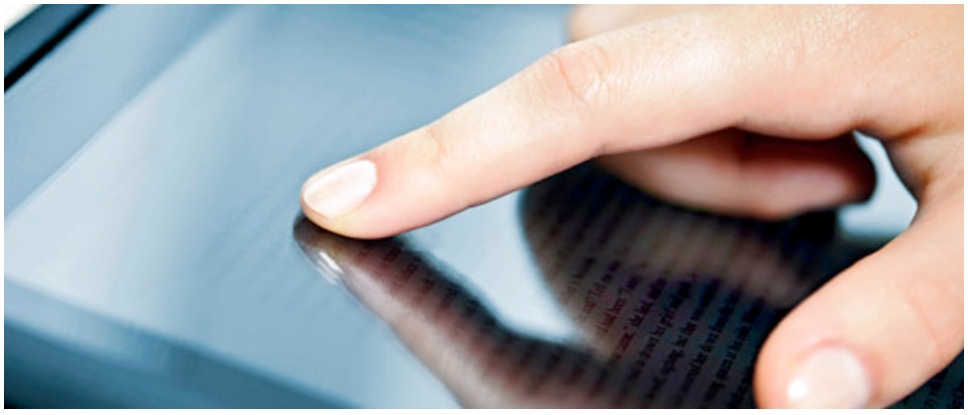


A Simplified Guide To Digital Evidence

Introduction to Digital Evidence

Digital devices are everywhere in today's world, helping people communicate locally and globally with ease. Most people immediately think of computers, cell phones and the Internet as the only sources for digital evidence, but any piece of technology that processes information can be used in a criminal way. For example, hand-held games can carry encoded messages between criminals and even newer household appliances, such as a refrigerator with a built-in TV, could be used to store, view and share illegal images. The important thing to know is that responders need to be able to recognize and properly seize potential digital evidence.



Digital evidence is defined as information and data of value to an investigation that is stored on, received or transmitted by an electronic device[1]. This evidence can be acquired when electronic devices are seized and secured for examination. Digital evidence:

- Is latent (hidden), like fingerprints or DNA evidence
- Crosses jurisdictional borders quickly and easily
- Can be altered, damaged or destroyed with little effort
- Can be time sensitive

There are many sources of digital evidence, but for the purposes of this publication, the topic is divided into three major forensic categories of devices where evidence can be found: Internet-based, stand-alone computers or devices, and mobile devices. These areas tend to have different evidence-gathering processes, tools and concerns, and different types of crimes tend to lend themselves to one device or the other.

[1] **ELECTRONIC CSI, A GUIDE FOR FIRST RESPONDERS, 2ND EDITION**, National Institute of Justice, April 2008

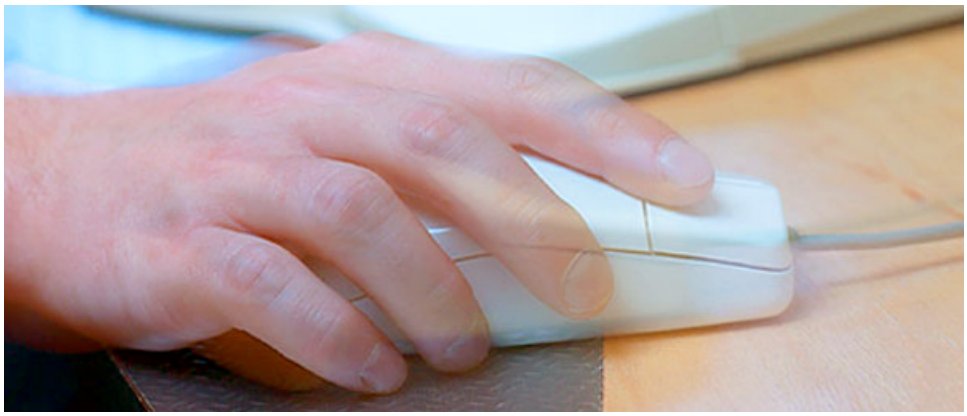
The Principles of Digital Evidence

Information that is stored electronically is said to be 'digital' because it has been broken down into digits; binary units of ones (1) and zeros (0), that are saved and retrieved using a set of instructions called software or code. Any kind of information—photographs, words, spreadsheets—can be created and saved using these types of instructions. Finding and exploiting evidence saved in this way is a growing area of forensics and constantly changes as the technology evolves.

Internet: The launch of the Internet or World Wide Web in the mid 1990's truly ushered in the 'age of access.' For the first time, individuals outside the academic world could use it to connect with others (and their computers) in a brand new way. The Internet opened up access to a world of information and resources, but also provided a highway for the traffic of illegal images, information and espionage.

Because of the global access to information and to other computers, criminals are able to use this access to hack into financial and communications systems, major corporations and government networks to steal money, identities and information, or to sabotage systems. One of the biggest challenges in Internet crime is for investigators, laboratory and technical personnel to understand how the process works and to stay closely engaged with advances in software and tracking technologies.

How it works: Any computer that connects to an Internet Service Provider (ISP) becomes part of the ISP's network, whether it is a single computer or part of a local area network (LAN) at a work place. Each ISP connects to another network, and so on. In this way, the Internet is literally a web of networks where information can be sent and received to any point on the web from any other point. This global collection of networks has no 'owner' or overall controlling network, so it operates like a community with all the pros and cons you might find in any other community.



Computers: In the late 1970s, employees at the Flagler Dog Track in Florida used a computer to create and print fraudulent winning tickets. This prompted Florida to enact the first computer crime law, the Florida Computer Crimes Act, which declared un-authorized use of computing facilities a crime. Federal laws followed in 1984.

Computer crimes continue to be a growing problem in both the public and private sector. A single computer can contain evidence of criminal activity carried out on the web, or the criminal use can be contained in the computer itself, such as pornography, copyright infringement, extortion, counterfeiting and much more. Digital evidence is located on the computer's hard drive and peripheral equipment, including removable media such as thumb drives and CD-ROM discs.

Mobile devices: Although handheld voice transmission devices using radio transmission have been in use since the 1940s (the Walkie-Talkie), the first version of what we would now call a cell phone was not developed until the 1980s. Cell phone use around the world skyrocketed in the 1990s and hit 4.6 billion cell subscriptions by the end of 2009. Cell phone and wireless technology has expanded to include many types of mobile devices such as tablet computers and hand-held video games.

Once used only for voice communications, today's cell phones are also used to take digital photos and movies, send instant messages, browse the web and perform many of the same tasks as a computer. Mobile devices allow criminals to engage in an ever-growing variety of activities and the devices keep track of every move and message. It is this tracking capability that turns mobile devices into key evidence in many cases.

Why and when is digital evidence used?

Digital evidence may come into play in any serious criminal investigation such as murder, rape, stalking, car-jacking, burglary, child abuse or exploitation, counterfeiting, extortion, gambling, piracy, property crimes and terrorism. Pre- and post-crime information is most relevant, for example, if a criminal was using an online program like Google Maps™ or street view to case a property before a crime; or posting stolen items for sale on Craigslist or E-Bay®; or communicating via text-message with accomplices to plan a crime or threaten a person. Some crimes can be committed entirely through digital means, such as computer hacking, economic fraud or identity theft.

In any of these situations, an electronic trail of information is left behind for a savvy investigation team to recognize, seize and exploit. As with any evidence-gathering, following proper procedures is crucial and will yield the most valuable data. Not following proper procedures can result in lost or damaged evidence, or rendering it inadmissible in court.

How It's Done

Evidence that May be Gathered Digitally

Computer documents, emails, text and instant messages, transactions, images and Internet histories are examples of information that can be gathered from electronic devices and used very effectively as evidence. For example, mobile devices use online-based based backup systems, also known as the 'cloud', that provide forensic investigators with access to text messages and pictures taken from a particular phone. These systems keep an average of 1,000–1,500 or more of the last text messages sent to and received from that phone.

In addition, many mobile devices store information about the locations where the device traveled and when it was there. To gain this knowledge,

investigators can access an average of the last 200 cell locations accessed by a mobile device. Satellite navigation systems and satellite radios in cars can provide similar information. Even photos posted to social media such as Facebook may contain location information. Photos taken with a Global Positioning System (GPS)-enabled device contain file data that shows when and exactly where a photo was taken. By gaining a subpoena for a particular mobile device account, investigators can collect a great deal of history related to a device and the person using it.

Who Conducts the Analysis

According to the National Institute of Justice (**http://www.nij.gov/nij/topics/forensics/evidence/digital/investigative-tools/welcome.htm**), "Digital evidence should be examined only by those trained specifically for that purpose." With the wide variety of electronic devices in use today and the speed with which they change, keeping up can be very difficult for local law enforcement. Many agencies do not have a digital evidence expert on hand and, if they do, the officer might be a specialist in cell phones but not social media or bank fraud. A detective may be able to log onto e-Bay® and look for stolen property but may be unable to capture cell phone text message histories and could destroy evidence just by trying. Many take an interest in the area and learn what they can, but there is no single path to digital evidence expertise—qualifications and certifications are not standardized across the country. Incorporation of digital seizure techniques is becoming more widespread in first responder training.

Certified Digital Media Examiners are investigators who have the education, training and experience to properly exploit this sensitive evidence. That said, there is no single certifying body, and certification programs can contain different courses of study. Generally speaking, these professionals have demonstrated core competencies in pre-examination procedures and legal issues, media assessment and analysis, data recovery, specific analysis of recovered data, documentation and reporting, and presentation of findings. While certification of examiners is not required in most agencies, it is becoming a widely valued asset and the numbers of certified examiners will increase. Vendor-neutral (not software based, but theory- and process-based) certification is offered through the Digital Forensics Certification Board (DFCB), an independent certifying organization for digital evidence examiners, the National Computer Forensics Academy at the High Tech Crime Institute and some colleges.

Most states have at least one laboratory or section for digital forensics and a variety of task forces including Internet Crimes Against Children (ICAC), Joint Terrorism Task Force (JTTF), and Narcotics and Property Crimes.

These forces comprise officers with specialized training, including search, seizure and exploitation of digital evidence as it pertains to their area of expertise. Agencies and investigators must work together to ensure the highest level of security and evidence handling is used. In the United States, the FBI can provide assistance in some specialty areas.

How Digital Devices are Collected

On the scene: As anyone who has dropped a cell phone in a lake or had their computer damaged in a move or a thunderstorm knows, digitally stored information is very sensitive and easily lost. There are general best practices, developed by organizations like SWGDE and NIJ, to properly seize devices and computers. Once the scene has been secured and legal authority to seize the evidence has been confirmed, devices can be collected. Any passwords, codes or PINs should be gathered from the individuals involved, if possible, and associated chargers, cables, peripherals, and manuals should be collected. Thumb drives, cell phones, hard drives and the like are examined using different tools and techniques, and this is most often done in a specialized laboratory.

First responders need to take special care with digital devices in addition to normal evidence collection procedures to prevent exposure to things like extreme temperatures, static electricity and moisture.

Seizing Mobile Devices

Devices should be turned off immediately and batteries removed, if possible. Turning off the phone preserves cell tower location information and call logs, and prevents the phone from being used, which could change the data on the phone. In addition, if the device remains on, remote destruction commands could be used without the investigator's knowledge. Some phones have an automatic tier to turn on the phone for updates, which could compromise data, so battery removal is optimal.

If the device cannot be turned off, then it must be isolated from its cell tower by placing it in a Faraday bag or other blocking material, set to airplane mode, or the Wi-Fi, Bluetooth or other communications system must be disabled. Digital devices should be placed in antistatic packaging such as paper bags or envelopes and cardboard boxes. Plastic should be avoided as it can convey static electricity or allow a buildup of condensation or humidity.

In emergency or life threatening situations, information from the phone can be removed and saved at the scene, but great care must be taken in the documentation of the action and the preservation of the data.

When sending digital devices to the laboratory, the investigator must indicate the type of information being sought, for instance phone numbers and call histories from a cell phone, emails, documents and messages from a computer, or images on a tablet.

Seizing Stand Alone Computers and Equipment: To prevent the alteration of digital evidence during collection, first responders should first document any activity on the computer, components, or devices by taking a photograph and recording any information on the screen. Responders may move a mouse (without pressing buttons or moving the wheel) to determine if something is on the screen. If the computer is on, calling on a computer forensic expert is highly recommended as connections to criminal activity may be lost by turning off the computer. If a computer is on but is running destructive software (formatting, deleting, removing or wiping information), power to the computer should be disconnected immediately to preserve whatever is left on the machine.

Office environments provide a challenging collection situation due to networking, potential loss of evidence and liabilities to the agency outside of the criminal investigation. For instance, if a server is turned off during seizure that is providing a service to outside customers, the loss of service to the customer may be very damaging. In addition, office equipment that could contain evidence such as copiers, scanners, security cameras, facsimile machines, pagers and caller ID units should be collected.

Computers that are off may be collected into evidence as per usual agency digital evidence procedures.

How and Where the Analysis is Performed

Exploiting data in the laboratory: Once the digital evidence has been sent to the laboratory, a qualified analyst will take the following steps to retrieve and analyze data:

1. Prevent contamination: It is easy to understand cross contamination in a DNA laboratory or at the crime scene, but digital evidence has similar issues which must be prevented by the collection officer. Prior to analyzing digital evidence, an image or work copy of the original storage device is created. When collecting data from a suspect device, the copy must be stored on another form of media to keep the original pristine. Analysts must use 'clean' storage media to prevent contamination—or the introduction of data from another source. For example, if the analyst was to put a copy of

the suspect device on a CD that already contained information, that information might be analyzed as though it had been on the suspect device. Although digital storage media such as thumb drives and data cards are reusable, simply erasing the data and replacing it with new evidence is not sufficient. The destination storage unit must be new or, if reused, it must be forensically 'wiped' prior to use. This removes all content, known and unknown, from the media.

2. Isolate Wireless Devices: Cell phones and other wireless devices should be initially examined in an isolation chamber, if available. This prevents connection to any networks and keeps evidence as pristine as possible. The Faraday bag can be opened inside the chamber and the device can be exploited, including phone information, Federal Communications Commission (FCC) information, SIM cards, etc. The device can be connected to analysis software from within the chamber. If an agency does not have an isolation chamber, investigators will typically place the device in a Faraday bag and switch the phone to airplane mode to prevent reception.

3. Install write-blocking software: To prevent any change to the data on the device or media, the analyst will install a block on the working copy so that data may be viewed but nothing can be changed or added.

4. Select extraction methods: Once the working copy is created, the analyst will determine the make and model of the device and select extraction software designed to most completely 'parse the data,' or view its contents.

5. Submit device or original media for traditional evidence examination: When the data has been removed, the device is sent back into evidence. There may be DNA, trace, fingerprint, or other evidence that may be obtained from it and the digital analyst can now work without it.

6. Proceed with investigation: At this point, the analyst will use the selected software to view data. The analyst will be able to see all the files on the drive, can see if areas are hidden and may even be able to restore organization of files allowing hidden areas to be viewed. Deleted files are also visible, as long as they haven't been over-written by new data. Partially deleted files can be of value as well.

Files on a computer or other device are not the only evidence that can be gathered. The analyst may have to work beyond the hardware to find evidence that resides on the Internet including chat rooms, instant messaging, websites and other networks of participants or information. By using the system of Internet addresses, email header information, time stamps on messaging and other encrypted data, the analyst can piece together strings of interactions that provide a picture of activity.

FAQs

What kind of results can be expected from analysis of digital evidence?

If evidence collection and analysis is conducted properly, examiners can secure information that can support criminal activity claims through dialog or message exchange, images and documents. The examiner will generally provide all the supporting documentation, highlighting relevant information, but also a report detailing what was done to extract the data. As with evidence of other types, chain of custody and proper collection and extraction techniques are critical to the credibility of evidence and must be thoroughly documented.

What are the limitations regarding the evidence that can be gained from digital devices?

Investigative limitations are primarily due to encryption and proprietary systems that require decoding before data can even be accessed. Unlike what is portrayed on popular television crime shows, decoding an encrypted password can take a very long time, even with sophisticated software.

There are both legal and technical limitations in this area of investigation. Laws governing processing and prosecution are different from state to state. Digital crime can easily cross jurisdictions, making standardization an increasingly critical law enforcement issue.

Data ownership can be an issue as well. In a recent ruling in Colorado, the holder of a password was compelled to divulge the password, but in doing so did not have to admit knowledge or ownership of the data protected by the password[1]. This is akin to a landlord being able to unlock a rental apartment with no responsibility for what might be inside the unit. In this case, it would still be up to the investigator to tie the two together.

[1] *United States vs. Fricosu*, 247 10 (Colorado 2012)

Wiretapping laws can also come into play particularly with regard to mobile phone seizure. Intercepting a call without a court order violates an expectation of privacy. Even after a phone has been seized, any calls or messages received by that phone cannot be used as the holders of the phone (law enforcement) are not the intended recipient.

Privacy laws and issues are the most limiting areas of search. Without proper authority to search or seize electronics, the information contained on the device may not be used. Internet and personal device privacy laws can be confusing. In addition, people's understanding of privacy tends to be generational – younger people tend to believe they should have access to information freely but that their movements and communications are inherently private; older users tend to understand that their movements and communications can be tracked and have a lesser expectation of privacy. Today there has been no major case law to clearly define new limits in the United States.

In the United Kingdom examiners usually follow guidelines issued by the Association of Chief Police Officers (**http://www.acpo.police.uk/**) (ACPO) for the authentication and integrity of evidence. The guidelines consist of four principles:

1. No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

2. In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

3. An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

4. The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

These guidelines are widely accepted in courts of England and Scotland, but they do not constitute a legal requirement and their use is voluntary.

How is quality control and assurance performed?

Quality control and assurance is similar to other forensic specialties in that the laboratory must have and follow guidelines in addition to the responders and analysts. SWGDE brings together organizations actively engaged in the

field of digital and multimedia evidence in the U.S. and other countries to foster communication and cooperation as well as to ensure quality and consistency within the forensic community. Practices have been cited by the European Network Forensic Science Institute – Forensic Information Technology Working Group (ENFSI-FITWG) and in publications.

According to SWGDE's Minimum Requirements for Quality Assurance in the Processing of Digital and Multimedia Evidence (**http://www.swgde.org/documents/current-documents/2010-05-15 SWGDE Min Req for QA in Proc Digital Multimedia Evidence_v1.pdf**), Digital Evidence Laboratories (DEL) must have and follow a written Quality Management System (QMS) that is documented in a Quality Manual (QM). The QMS is similar to those in other types of forensic laboratories in that it defines structure, responsibilities, procedures, processes, and resources sound and error-free work and documentation.

To ensure the most accurate analysis of evidence, the management of forensic laboratories puts in place policies and procedures that govern facilities and equipment, methods and procedures, and analyst qualifications and training. Depending on the state in which it operates, a crime laboratory may be required to achieve accreditation to verify that it meets quality standards. There are two internationally recognized accrediting programs focused on forensic laboratories: The American Society of Crime Laboratory Directors Laboratory Accreditation Board (**http://www.ascld-lab.org**) and ANSI-ASQ National Accreditation Board / FQS (**http://www.forquality.org**).

What information does the report include and how are the results interpreted?

Like other forms of evidence, digital evidence must remain pristine and unaltered. In a courtroom, text messages would most likely be shared on the actual phone or digital device, but other evidence might be printed out, such as a string of emails or email headers.

```
Received: from SERVERNAME-Exch1.place.com ([172.16.102.10]) by SERVERNAME-exch1
 ([172.16.102.10]) with mapi; Mon, 27 Feb 2012 09:53:10 -0500
Content-Type: application/ms-tnef; name="winmail.dat"
Content-Transfer-Encoding: binary
From: Bad Guy  Bad.Guy@place.com
To: Worse Guy worse.guy@place.com
Date: Mon, 27 Feb 2012 09:53:09 -0500
Subject: Here's the plan
Thread-Topic: Here's the plan
Thread-Index: Acz1X4VRzKScTInUTWSTqYrRhGJhqg==
Message-ID: <2E95727AD62F534E9A60644CAB99079D011790B7E201@servername-exch1>
Accept-Language: en-US
Content-Language: en-US
X-MS-Has-Attach:
X-MS-Exchange-Organization-SCL: -1
X-MS-TNEF-Correlator: <2E95727AD62F534E9A60644CAB99079D011790B7E201@server-exch1>
MIME-Version: 1.0
```

Sample email header showing the path and timing of the message.

This can show a track record of information exchange, and the "hash value", also referred to as a checksum, hash code or hashes, is the mark of authenticity and must be present and explained to courtroom participants.

Results	
Original text	forensic science
Original bytes	66:6f:72:65:6e:73:69:63:20:73:63:69:65:6e:63:65 (length=16)
Adler32	36890654
CRC32	65b2a252
Haval	ec53e6b5a3315da4ac3fab83ec9f8f7a
MD2	e27cc4e242c05896e7e1b4be08159724
MD4	1fd5241554970223a34acae2b9de2cef
MD5	769aaa196bf49c716c905b4b91d6d94c
RipeMD128	32d26d2b1b10c3adbf292b86da8b766f
RipeMD160	3aee598566cb9cecff5dda29686463c1aa91848c
SHA-1	a728a136e1fbfafef6205e423423c62efd9fd12f
SHA-256	02d0779148771712a27d93ed92b5240c041a8c6a048ab9078cb1d83610e82df7
SHA-384	40b63414a6c7ef4f6c53d5915521fec4d8e83c46a2e864c7535923502a130c6a3f6e1d1e56eba05654bc22a8229c4f2e
SHA-512	146a6257bb58b4305f00ec92d41edb419efb9b60373f302c5edf0107dfca6eba86548d1276870a0b3572c231a6f513fae2befcae68f2f3db0b3590ff930d9dcf
Tiger	2cb2b89ca649f106d72d14e565df217245967b3069538b61
Whirlpool	89f0f8e2403a13cc12057071503a7b7a7d9734811869df0c6e859826c0f35c2de611af7bcf77e6c63e6e5c9581c7e9b80e1589752a3f4c9f64a38237f75e96be

Hash values calculated for the text string "forensic science". Each line contains the search term value calculated using the unique algorithm in the left hand column.

A hash value is the result of a calculation (hash algorithm) performed on a string of text, electronic file or entire hard drive contents. Hash values are used to identify and filter duplicate files (i.e. email, attachments, and loose files) from a given source and verify that a forensic image or clone was captured successfully. For example, a hash function performed on a suspect's hard drive should generate a hash value report that exactly match the report generated by using the same algorithm on the hard drive's image, typically created by the laboratory for use in the investigation.

Hash values are a reliable, fast, and a secure way to compare the contents of individual files and media. Whether it is a single text file containing a phone number or five terabytes of data on a server, calculating hash values is an invaluable process for evidence verification in electronic discovery and computer forensics.

Once verified, the information pulled from the files can be shown in the courtroom, such as photos or emails. In addition, email headers, showing the path and timing emails took to get from source to destination could be displayed.

Are there any misconceptions or anything else about digital evidence that might be important to the non-scientist?

There are a number of common misperceptions about the retrieval and usefulness of digital evidence, including:

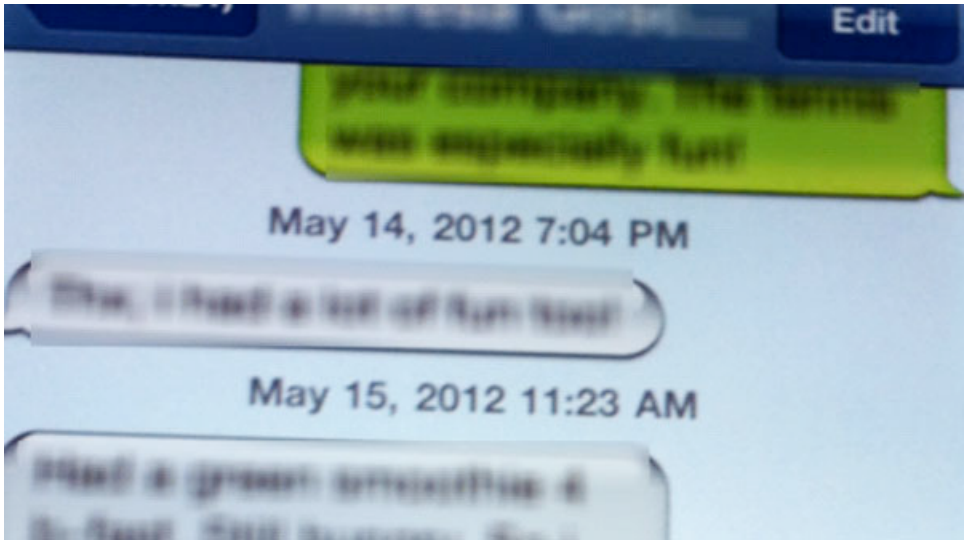
Anything on a hard drive or other electronic media can always be retrieved. This is incorrect as over-written or damaged files, or physical damage to the media can render it unreadable. Highly specialized laboratories with clean rooms may be able to examine hard drive components and reconstruct data, but this process is very laborious and extremely expensive.

Decrypting a password is quick and easy, with the right software. With the increasing complexity of passwords including capitals, numbers, symbols and password length, there are billions of potential passwords. Decryption can take a great deal of time, up to a year in some cases, using system resources and holding up investigations. Gathering passwords from those involved in a case is much more efficient and should be done whenever possible.

Any digital image can be refined to high definition quality. Images can be very useful for investigations, but a low resolution image is made by capturing fewer bits of data (pixels) than higher resolution photos. Pixels that are not there in the first place cannot be refined.

Investigators can look at digital evidence at the crime scene or any time. Just looking at a file list does not damage the evidence. It is crucial to note that opening, viewing or clicking on files can severely damage forensic information because it can change the last access date of a file or a piece of hardware. This changes the profile and can be considered tampering with

evidence or even render it completely inadmissible. Only investigators with the proper tools and training should be viewing and retrieving evidence.



First responder training lags behind advancements in electronics. Without regular updates to their training, responders may not be aware of what new digital devices might be in use and subject to collection. For example, there should be an awareness that thumb drives and SD cards can be easily removed and discarded by a suspect in the course of an encounter with law enforcement.

Common Terms

Common terminology is critical in the digital evidence world. The Scientific Working Group on Digital Evidence (SWGDE) in collaboration with the Scientific Working Group on Imaging Technology (SWGIT) has developed and continuously maintains a glossary of terms used within the digital and multimedia disciplines. SWGDE has used ASTM International, a recognized standards organization, to establish international acceptance of terminology. SWGDE/SWGIT's full glossary is available online: (**http://www.swgde.org/documents/current-documents/SWGDE SWGIT Combined Glossary V2.5.pdf**)

Some common terms include:

Cloud Computing - software, applications and digital storage that is accessed on the Internet through a web browser or desktop or mobile app. The software and user's data are stored on servers at a remote location.

Data - Information in analog or digital form that can be transmitted or processed.

Data Extraction - A process that identifies and recovers information that may not be immediately apparent.

Encryption - procedure that converts plain text into symbols to prevent anyone but the intended recipient from understanding the message.

File Format - The structure by which data is organized in a file.

Forensic Wipe - A verifiable procedure for sanitizing a defined area of digital media by overwriting each byte with a known value; this process prevents cross-contamination of data.

Handheld (Mobile) Devices - Handheld devices are portable data storage devices that provide communications, digital photography, navigation systems, entertainment, data storage, and personal information management.

Hash or Hash Value - Numerical values that represent a string of text (search term), generated by hashing functions (algorithms). Hash values are used to query large sums of data such as databases or hard drives for specific terms. In forensics, hash values are also used to substantiate the integrity of digital evidence and/or for inclusion and exclusion comparisons against known value sets.

Log File - A record of actions, events, and related data.

Media - Objects on which data can be stored. Includes hard drives, thumb drives, CD/DVD, floppy discs, SIM cards from mobile devices, memory cards for cameras, etc.

Metadata - Data, frequently embedded within a file, that describes a file or directory, which can include the locations where the content is stored, dates and times, application specific information, and permissions. Examples: Email headers and website source code contain metadata.

Partition - User defined section of electronic media. Partitions can be used to separate and hide information on a hard drive.

Source Code - The instructions written in a programming language used to build a computer program.

Work Copy - A copy or duplicate of a recording or data that can be used for subsequent processing and/or analysis. Also called an image.

Write Block/Write Protect - Hardware and/or software methods of preventing modification of content on a media storage unit like a CD or thumb drive.

Resources & References

You can learn more about this topic at the websites and publications listed below.

Resources

ELECTRONIC CRIME SCENE INVESTIGATION: A GUIDE FOR FIRST RESPONDERS, SECOND EDITION, **http://www.nij.gov/pubs-sum/219941.htm**

BEST PRACTICES FOR SEIZING ELECTRONIC EVIDENCE: A POCKET GUIDE FOR FIRST RESPONDERS, V.3, DHS/Secret Service **http://publicintelligence.net/u-s-secret-service-best-practices-for-seizing-electronic-evidence/**

DIGITAL EVIDENCE IN THE COURTROOM: A GUIDE FOR LAW ENFORCEMENT AND PROSECUTORS, **http://www.nij.gov/pubs-sum/211314.htm**

FORENSIC EXAMINATION OF DIGITAL EVIDENCE: A GUIDE FOR LAW ENFORCEMENT **http://www.ojp.usdoj.gov/nij/pubs-sum/199408.htm**

Electronic Crime Prevention Center of Excellence **http://www.ectcoe.net/**

National Institute of Justice **http://www.nij.gov/topics/forensics/evidence/digital/welcome.htm**

Scientific Working Group Digital Evidence **http://www.swgde.org/**

References

ELECTRONIC CRIME SCENE INVESTIGATION: A GUIDE FOR FIRST RESPONDERS, 2ND ED, 2008. Department of Justice, Office of Justice Programs, National Institute of Justice. **http://www.nij.gov/pubs-sum/219941.htm** (accessed July 5, 2012).

DIGITAL EVIDENCE AND FORENSICS, 2010. Department of Justice, Office of Justice Programs, National Institute of Justice. **http://www.nij.gov/topics/forensics/evidence/digital/welcome.htm** (accessed July 5, 2012).

U.S. Secret Service, **BEST PRACTICES FOR SEIZING ELECTRONIC EVIDENCE: A POCKET GUIDE FOR FIRST RESPONDERS**, Version 3, 2006. Public Intelligence.net. **http://publicintelligence.net/u-s-secret-service-best-practices-for-seizing-electronic-evidence/** (accessed July 5, 2012).

DIGITAL EVIDENCE IN THE COURTROOM: A GUIDE FOR LAW ENFORCEMENT AND PROSECUTORS, 2007. Department of Justice, Office of Justice Programs, National Institute of Justice. **http://www.nij.gov/pubs-sum/211314.htm** (accessed July 5, 2012).

FORENSIC EXAMINATION OF DIGITAL EVIDENCE: A GUIDE FOR LAW ENFORCEMENT, 2004. Department of Justice, Office of Justice Programs, National Institute of Justice. **http://www.ojp.usdoj.gov/nij/pubs-sum/199408.htm** (accessed July 5, 2012).

Scientific Working Group Digital Evidence. **http://www.swgde.org/** (accessed July 5, 2012).

Acknowledgements

The authors wish to thank the following for their invaluable contributions to this forensic guide:

Stephen Pearson, *Managing Partner*, High Tech Crime Institute Group

Chris Hendry, *Crime Lab Analyst in Computer Evidence Recovery*, Florida Department of Law Enforcement, Florida Computer Crime Center Tallahassee

Dagmar Spencer, *Research and Training specialist*, Florida Department of Law Enforcement, Florida Computer Crime Center Tallahassee

Alastair Ross, *Director*, National Institute of Forensic Science at Australia New Zealand Policing Advisory Agency

Forensic Evidence Admissibility and Expert Witnesses

How or why some scientific evidence or expert witnesses are allowed to be presented in court and some are not can be confusing to the casual observer or a layperson reading about a case in the media. However, there is significant precedent that guides the way these decisions are made. Our discussion here will briefly outline the three major sources that currently guide evidence and testimony admissibility.

The *Frye* Standard – Scientific Evidence and the Principle of General Acceptance

In 1923, in *Frye v. United States*[1], the District of Columbia Court rejected the scientific validity of the lie detector (polygraph) because the technology did not have significant general acceptance at that time. The court gave a guideline for determining the admissibility of scientific examinations:

Just when a scientific principle or discovery crosses the line between the experimental and demonstrable stages is difficult to define. Somewhere in this twilight zone the evidential force of the principle must be recognized, and while the courts will go a long way in admitting experimental testimony deduced from a well-recognized scientific principle or discovery, the thing from which the deduction is made must be **sufficiently established to have gained general acceptance** *in the particular field in which it belongs.*

Essentially, to apply the "*Frye* Standard" a court had to decide if the procedure, technique or principles in question were generally accepted by a meaningful proportion of the relevant scientific community. This standard prevailed in the federal courts and some states for many years.

Federal Rules of Evidence, Rule 702

In 1975, more than a half-century after *Frye* was decided, the Federal Rules of Evidence were adopted for litigation in federal courts. They included rules on expert testimony. Their alternative to the *Frye* Standard came to be used more broadly because it did not strictly require general acceptance and was seen to be more flexible.

The first version of Federal Rule of Evidence 702 provided that a witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:

[1] 293 Fed. 1013 (1923)

a. the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
b. the testimony is based on sufficient facts or data;
c. the testimony is the product of reliable principles and methods; and
d. the expert has reliably applied the principles and methods to the facts of the case.

While the states are allowed to adopt their own rules, most have adopted or modified the Federal rules, including those covering expert testimony.

In a 1993 case, *Daubert v. Merrell Dow Pharmaceuticals, Inc.,* the United States Supreme Court held that the Federal Rules of Evidence, and in particular Fed. R. Evid. 702, superseded *Frye's* "general acceptance" test.

The *Daubert* Standard – Court Acceptance of Expert Testimony

In *Daubert* and later cases[2], the Court explained that the federal standard includes general acceptance, but also looks at the science and its application. Trial judges are the final arbiter or "gatekeeper" on admissibility of evidence and acceptance of a witness as an expert within their own courtrooms.

In deciding if the science and the expert in question should be permitted, the judge should consider:

- What is the basic theory and has it been tested?
- Are there standards controlling the technique?
- Has the theory or technique been subjected to peer review and publication?
- What is the known or potential error rate?
- Is there general acceptance of the theory?
- Has the expert adequately accounted for alternative explanations?
- Has the expert unjustifiably extrapolated from an accepted premise to an unfounded conclusion?

The *Daubert* Court also observed that concerns over shaky evidence could be handled through vigorous cross-examination, presentation of contrary evidence and careful instruction on the burden of proof.

In many states, scientific expert testimony is now subject to this *Daubert* standard. But some states still use a modification of the *Frye* standard.

[2] The "Daubert Trilogy" of cases is: **DAUBERT V. MERRELL DOW PHARMACEUTICALS**, **GENERAL ELECTRIC CO. V. JOINER** and **KUMHO TIRE CO. V. CARMICHAEL**.

Who can serve as an expert forensic science witness at court?

Over the years, evidence presented at trial has grown increasingly difficult for the average juror to understand. By calling on an expert witness who can discuss complex evidence or testing in an easy-to-understand manner, trial lawyers can better present their cases and jurors can be better equipped to weigh the evidence. But this brings up additional difficult questions. How does the court define whether a person is an expert? What qualifications must they meet to provide their opinion in a court of law?

These questions, too, are addressed in **Fed. R. Evid. 702**. It only allows experts "qualified … by knowledge, skill, experience, training, or education." To be considered a true expert in any field generally requires a significant level of training and experience. The various forensic disciplines follow different training plans, but most include in-house training, assessments and practical exams, and continuing education. Oral presentation practice, including moot court experience (simulated courtroom proceeding), is very helpful in preparing examiners for questioning in a trial.

Normally, the individual that issued the laboratory report would serve as the expert at court. By issuing a report, that individual takes responsibility for the analysis. This person could be a supervisor or technical leader, but doesn't necessarily need to be the one who did the analysis. The opposition may also call in experts to refute this testimony, and both witnesses are subject to the standard in use by that court (*Frye, Daubert*, Fed. R. Evid 702) regarding their expertise.

Each court can accept any person as an expert, and there have been instances where individuals who lack proper training and background have been declared experts. When necessary, the opponent can question potential witnesses in an attempt to show that they do not have applicable expertise and are not qualified to testify on the topic. The admissibility decision is left to the judge.

Additional Resources

Publications:

Saferstein, Richard. **CRIMINALISTICS: AN INTRODUCTION TO FORENSIC SCIENCE**, Pearson Education, Inc., Upper Saddle River, NJ (2007).

McClure, David. Report: Focus Group on Scientific and Forensic Evidence in the Courtroom (online), 2007, **https://www.ncjrs.gov/pdffiles1/nij/grants/220692.pdf** (accessed July 19, 2012)

Acknowledgements
The authors wish to thank the following for their invaluable contributions to this guide:

Robin Whitley, *Chief Deputy*, Appellate Division, Denver District Attorney's Office, Second Judicial District

Debra Figarelli, *DNA Technical Manager*, National Forensic Science Technology Center, Inc.

About This Project

This project was developed and designed by the National Forensic Science Technology Center (NFSTC) under a cooperative agreement from the Bureau of Justice Assistance (BJA), award #2009-D1-BX-K028. Neither the U.S. Department of Justice nor any of its components operate, control, are responsible for, or necessarily endorse, the contents herein.

National Forensic Science Technology Center®
NFSTC *Science Serving Justice*®
8285 Bryan Dairy Road, Suite 125
Largo, Florida 33777
(727) 395-2511
info@nfstc.org