12.5.9 Forensic Investigation Facts

This lesson covers the following topics:

- Key areas of digital forensics
- Sequence of events
- Digital data collection

Key Areas of Digital Forensics

There are procedures you must follow when you gather and preserve evidence. Any of these procedures could make or break your legal case. Learning how to go about this evidentiary process is vital to any electronic forensic investigation. Become familiar with procedures related to the following areas.

Area	Description
Legal hold	A legal hold, also called a litigation hold, is a formal notice sent out to all employees of a company when litigation is eminent. The notice instructs all employees to retain electronically stored information (ESI). This includes emails, memos, invoices, and any other stored document. A legal hold also covers printed, physical copies of documents.
Video	Video evidence in criminal cases has become the norm not the exception. Video evidence may come from security cameras or videos stored on a computer. The key to ensuring that video evidence is admissible is the ability to prove the video has not been manipulated. If this cannot be done, the video is likely to be excluded. Caution must be taken when retrieving videos to ensure that the integrity of the video is preserved. Video evidence can be very persuasive and many times even the deciding factor in a legal case. It can also be fatal to a case if shown to have been gathered in an illegal, sloppy, or reckless manner.
Admissibility	Admissibility refers to evidence allowed to be used in court. For evidence to be admissible, it must meet certain criteria. First, it must be obtained by legal means. If evidence is discovered through an illegal procedure, then the evidence will not be admissible. In law, this is called fruit of the poisonous tree. This why it is so important to understand what you are and are not allowed to do when collecting evidence. Retaining the services of a legal expert, law enforcement, or other outside help is recommended.
Chain of custody	Chain of custody is a record of the handling of each piece of gathered evidence. This gives all parties involved confidence that the evidence has not been tampering with. The chain of custody begins immediately upon gathering the evidence. The person who gathers the evidence is responsible to secure it so that it is protected from any harmful conditions and cannot be tampered with. For example, a hard drive would need to be placed inside an anti-static bag, maybe even a Faraday bag. It would then be sealed inside an evidence bag that would have date, time, originator, and description of evidence it contains. The evidence bag would document all persons who take custody of the evidence. Evidence bags are tamper-resistant. Any signs of tampering must be investigated.

Sequence of Events

Forensic investigations require that an accurate and provable sequence of events be established. There are several items that help to create this accurate narrative.

Item	Description
Time stamps	Time stamps provide an exact date and time of an event. The event could be when a document is created, edited, moved, or downloaded. It could be when a video is captured or a picture is taken. Time stamps also apply to emails, instant messages, video downloads, video uploads, and data packets extracted from a network. A time stamp must be accurate for admissibility. An inaccurate or missing time stamp creates doubt and can lead to evidence being inadmissible. It is important for you to ensure that all servers, wireless access points, security cameras, and physical entry points are recording time stamps correctly.
Time offset	Time offset refers time on a computer or device compared to Greenwich Mean Time (GMT). All offsets use GMT as a baseline from which you are either + or – a number of hours. For example, if your computer is set to Mountain Daylight Time, then it is -7 hours or GMT -06:00. Because a computer will use different formats to record time stamps, you must understand the offset needed to show consistency. In a Windows NTFS file system, all time stamps are logged using GMT not the local time zone. Documents manipulated within the NTFS will show local time within the document but GMT when retrieved.
Tags	Evidence must be tagged when collected. Tags provide a clear, precise, and consistent way of marking evidence. Everything must be tagged, including cables, monitors, machines, and even the ports on a machine. The tags need to be very specific. For example, you are collecting evidence on a personal computer that has power cables, an Ethernet cable, USB ports, monitor cables, etc. All these items must be tagged. Even empty ports must be tagged as such. The exact location each cable or other device must also be on the tag. For evidence to be admissible the tagging must be done correctly the first time.
Reports	Once the analysis of the evidence is done, you must report the findings. You should present the information in a well-written document that is legally appropriate and defensible. Therefore, you should probably engage the services of a lawyer to write this document to make sure it's done correctly. This document needs to be self-contained, meaning that all necessary information necessary is in the document. It shouldn't contain references or links to other documents. Everything needed is in the document itself. It should: ▪ Describe the incident. ▪ Describe the computer forensics team's response. ▪ Report what happened during the acquisition of evidence. ▪ Describe how the evidence was analyzed. ▪ Report what was found in the evidence.
Event logs	Computers, servers, and other network appliances produce event logs. These logs are time stamped and show exactly what happened on a specific computer or appliance. The event log may contain the affected process, application, protocol, or other pertinent information. Caution must be exercised when retrieving any data from a system. Trying to recover event logs from a machine is dangerous. Do a bit-for-bit copy first. Recover evidence from this copy. Remember, event logs are only as accurate and reliable as the system from which they come. Therefore, you should make sure that all client computers on a network have the time set by a time server and rechecked on a regular basis.

Interviews	Conducting interviews with people involved in a computer crime is a useful tool. The interviews need to be done with caution and in a way that makes them legally admissible. All interviews should be either video recorded or audio recorded. These artifacts must be accurately time stamped and conducted in accordance with local, state, and federal laws. The interviews should be handled by legal professionals to avoid improper or inadmissible testimony. Interviews can be a powerful investigative tool if done correctly.

Digital Data Collection

A forensic investigator gathers potential evidence from many software, hardware and other sources. There is an order in which the evidence needs to be gathered.

The order of volatility describes the process of capturing data based on the volatility of the data. The most volatile data should be captured first followed by progressively less volitile (more persistent) data. If an attack is underway, your computer forensics response team will probably capture data as follows.

Source	Description
Random Access Memory	RAM is the most volatile of all computer data storage. RAM is cleared when a computer is shutdown. Once gone, it cannot be recovered. Data on RAM can be copied as long as the system is running but should be done only by someone with proper training. The data stored on RAM can have valuable information. Many times malware such as worms, viruses and Trojan horses are created as memory-resident only. This makes identifying them difficult.
Swap/page file	Swap files or page files are a virtual extension of RAM. An OS is designed so that if you are running low on RAM, it can place files not in use into the swap or page file to be accessed later. An administrator can determine how much space to allocate to page files. For the forensic investigator, this is another potential source of evidence. The page file data does not automatically delete at shutdown unless you change the default settings.
Hard drive	The data on the hard disk drive is a key piece of evidence in a computer forensics investigation. A lot of the things that we do on a computer system are saved in some way on the hard disk drive, including data in virtual memory. A wealth of data is there. In addition, information attached to deleted files may still be on the disk. Therefore, the hard drive itself is a gold mine of evidence for a prosecutor. Caution must be exercised when making a copy of the disk. A regular file-for file-copy is not good enough. It needs to be a sector-by-sector copy that includes formerly deleted but still accessible data.
Remote logs	Remote logs are logs that document events on a computer system and are stored on a device other than the device that the events occurred on.
Archived data	Archived data are documents, logs, etc. that are not used regularly and are stored on a device other than the device under forensic investigation.

In the last 30 years technology has changed dramatically. With the increase of digital devices there is an equal increase in the number of devices that may require forensic examination. These devices can contain the evidence a forensic investigator needs. Each smart phone, tablet, laptop, and smart watch shares common elements, namely RAM, CPU, logs, and storage space. A trained investigator must be familiar with all platforms.

Network forensic data plays an important role in an investigation. Network appliances that can be important in a forensic examination include: firewalls, routers, switches, domain controllers, DHCP servers, application servers, and web proxy servers. Also included are network applications including intrusion detection and intrusion protection systems.