





Chapter 9 - Key Topics

 Description	 Element	 Page	 Summary
<u>The role of attribution in a cybersecurity investigation</u>	Paragraph	342	One of the key topics in digital forensics is attribution of assets and threat actors. There is undeniable motivation to support an evidence-led approach to digital forensics to achieve good attribution. Due to the large number of technical complexities, it is often impractical for digital forensics experts to determine fully the reliability of endpoints, servers, or network infrastructure devices and provide assurances to the court about the soundness of the processes involved and the complete attribution to a threat actor.
<u>The use of digital evidence</u>	Paragraph	342	During cybersecurity investigations, the forensics expert may revisit portions of the evidence to determine its validity. From a practical and realistic perspective, the amount of time and effort involved in the digital forensic process should pass an acceptable "reasonableness test" due to the large amounts of volume.
<u>Defining what digital forensic evidence is</u>	Paragraph	343	Digital forensic evidence is information its digital form found on a wide range of endpoint, server, and network devices—basically, any information that can be processed by a computing device or stored on other media.
<u>What is best evidence?</u>	Paragraph	343	Best Evidence - refers to evidence that can be presented in court in the original form (for example, an exact copy of a hard disk drive). However, in cyber forensics, what is the original when it comes to digital photography, copier machines, computer storage, and cloud storage? Typically, properly collected system images and appropriate copies of files can be used in court.

Aa Description	:≡ Element	▼ Page	≡ Summary
<u>What is corroborating evidence?</u>	Paragraph	343	Corroborating evidence (or corroboration) - is evidence that tends to support a theory or an assumption deduced by some initial evidence. This corroborating evidence confirms the proposition.
<u>What is indirect or circumstantial evidence?</u>	Paragraph	343	Indirect or circumstantial evidence - relies on an extrapolation to a conclusion of fact (such as fingerprints, DNA evidence, and so on). This is, of course, different from direct evidence. Direct evidence supports the truth of a proclamation without the need for any additional evidence or interpretation. For example, an expert witness.
<u>Collecting evidence from endpoints & servers</u>	Paragraph	344	To prevent or minimize contamination of the suspect's source device, you can use different tools, such as a piece of hardware called a write blocker , on the specific device so you can copy all the data (or an image of the system).
<u>Collecting evidence from mobile devices</u>	Paragraph	346	Mobile devices such as cell phones, wearables, and tablets are not imaged in the same way as desktops. For example, an iPhone cannot be accessed without know the manufacturing code from Apple. Evidence may also need to be collected from Mobile Device Management (MDM) solutions as well.
<u>Collecting evidence from network infrastructure devices</u>	Paragraph	346	Networked devices are a treasure trove of info. A central log repo where networked devices send log information is critical and efficient from a digital forensics point of view. A solution such as Syslog.
<u>Understanding evidentiary chain of custody</u>	Paragraph	348	Clear documentation on the following: 1. How was the evidence collected? 2. When was it collected? 3. How was it transported? 4. How was it tracked? 5. How was it stored? 6. Who had access to the evidence and how was it was accessed? Failure to maintain proper chain of custody is likely you wont be able to use as evidence in court of law.

Aa Description	≡ Element	▼ Page	≡ Summary
<u>Defining reverse engineering</u>	Paragraph	351	<p>Reverse engineering - is the methodology for acquiring architectural information about anything originally created by someone else.</p> <p>Disassemblers - Tools that take a program's executable binary as input and generate textual files that contain the assembly language code for the entire program or parts of it. Debuggers - Tools that allow reverse engineers to observe the program while it is running and to set breakpoints; they also provide the ability to trace through code. Reverse engineers can use debuggers to step through the disassembled code and watch the system as it runs the program, one instruction at a time. Decompilers - Programs that take an executable binary file and attempt to produce readable high-level language code from it. Examples, Ghidra, Binary Ninja, IDA Pro, Radare2, Evan's Debugger (edb)</p>
<u>What are processes, threads, & services?</u>	Paragraph	353	<p>Process - is a program that the system is running. Thread - basic units an OS allocates process time to. Primary Thread - each program starts with a single thread known as a primary thread, can also create additional threads thereafter. Job Object - processes that are grouped together and managed as a unit. Thread Pool - a group of worker threads that efficiently execute asynchronous callbacks for the application. Fiber - a unit of execution that is manually scheduled by the application. Services - long-running executable applications that run their own Windows session.</p>

Aa Description	:≡ Element	▼ Page	≡ Summary
<u>Understanding Memory Management</u>	Paragraph	356	Memory Management or Memory Allocation - managing system memory. Static Memory Allocation - a program allocates memory at compile time. Dynamic Memory Allocation - A program allocates memory at runtime. Stack - memory set aside as scratch space for a thread of execution. Heap - memory set aside for dynamic allocation, put data on the fly.
<u>Understanding the Windows Registry</u>	Paragraph	357	Windows Registry - a hierarchical database used to store information necessary to configure the system for one or more users, applications, and hardware devices. Anything performed in Windows refers to or is recorded into the Registry, meaning any actions taken by a user reference the Windows Registry.
<u>The Windows File System</u>	Section	359	Master Boot Record (MBR) - The master boot record (MBR) is the first sector (512 bytes) of the hard drive. It contains the boot code and information about the hard drive itself. Master File Table (\$MFT) - The first sector (512 bytes) of each partition contains information, such as the type of the file system, the booting code location, the sector size, and the cluster size in reference to the sector. Data Area, Free Space, Clusters, & Blocks - The rest of the partition space after the file system's area has been reserved will be available for data. Each unit of the data area is called a cluster or block. Allocated Cluster - This cluster holds data that is related to a file that exists and has an entry in the file system's MFT area. Unallocated Cluster - This cluster has not been connected to an existing file and may be empty or "not empty," thus containing data that is related to a deleted file and still hasn't been overwritten with a new file's data.

Aa Description	:≡ Element	▼ Page	≡ Summary
<u>What is FAT?</u>	Paragraph	360	File Allocation Table (FAT) - The file allocation table (FAT) was the default file system of the Microsoft disk operating system (DOS) back in the 1980s. Then other versions were introduced, including FAT12, FAT16, FAT32, and exFAT.
<u>What is NTFS?</u>	Paragraph	361	New Technology File System (NTFS) - NTFS is the default file system in Microsoft Windows since Windows NT and is a more secure, scalable, and advanced file system compared to FAT.
<u>What is MFT?</u>	Paragraph	361	NTFS has a file called \$MFT (Master File Table) . In this file is an entry for each file in the partition. This entry is 1,024 bytes in size. It even has an entry for itself. Each entry has a header of 42 bytes at the beginning and a signature of 0xEB52904E, which is equivalent to FILE in ASCII. The signature also can be BAD, which in this case indicates that an error has occurred. After the header is another 982 bytes left to store the file metadata. If there is space left to store the file contents, the file's data is stored in the entry itself and no space in the data area is used by this file. MFT uses attributes to stockpile the metadata of the file. Different attribute types can be used in a single MFT entry and are assigned to store different information.
<u>Understanding timestamps, MACE, & alternate data streams</u>	Paragraph	361	Each file in NTFS has a timestamp for Modify, Access, Create, & Entry Modified (MACE) . Alternate Data Streams (ADS) - Exists with the goal of supporting the resource forks employed by the Hierarchal File System (HFS) employed by Apple Macintosh systems. Also been referred to as "multiple data streams" as well as "alternative data streams." Also used by Microsoft System Resource Manager (FSRM) as part of "data classification"

Aa Description	:≡ Element	▼ Page	≡ Summary
What is EFI?	Paragraph	362	EFI System Partition (ESP) - is a partition on a hard disk drive or solid-state drive whose main purpose is to interact with the Unified Extensible Firmware Interface (UEFI) . UEFI starts the OS and different utilities, drivers, kernel images, boot loaders, etc.
Understanding Linux processes	Paragraph	362	In Linux, there are two methods for starting a process—starting it in the foreground and starting it in the background. Processes can be viewed with the <code>ps ()</code> command.
What are Ext4 & the Linux file system	Paragraph	366	Ext4 - You should also become familiar with the Linux file system. Ext4 is one of the most used Linux file systems. It has several improvements over its predecessors Ext3 and Ext2. Ext4 not only supports journaling (covered in the next section) but also modifies important data structures of the file system, such as the ones destined to store the file data. This is done for better performance, reliability, and additional features. size. Ext4 supports a maximum of 1 exabyte (EB), which equals 1,048,576 TB. The maximum possible number of subdirectories contained in a single directory in Ext3 is 32,000. Ext4 allows an unlimited number of subdirectories. It uses a “multiblock allocator” (mballoc) to allocate many blocks in a single call, instead of a single block per call. This feature avoids a lot of overhead and improves system performance.

Aa Description	:≡ Element	▼ Page	≡ Summary
<u>What is journaling?</u>	Paragraph	366	<p>Journaling - A journaling file system maintains a record of changes not yet committed to its main part. This data structure is referred to as a journal, which is a circular log. One of the main features of a file system that supports journaling is that if the system crashes or experiences a power failure, it can be restored back online a lot more quickly while also avoiding system corruption. One of the features of Ext4 is that it checksums the journal data to know if the journal blocks are failing or becoming corrupted. Journaling ensures the integrity of the file system by keeping track of all disk changes, but it introduces a bit of overhead.</p>
<u>Linux MBR & the swap file system</u>	Paragraph	366	<p>The MBR includes instructions about how the logical partitions that have file systems are organized on the drive. It also has executable code to load the installed operating system. The most common boot loaders in Linux are Linux Loader (LILO), Load Linux (LOADLIN), and the Grand Unified Bootloader (GRUB).</p>