# EC-Council Digital Forensics Essentials (DFE) Practice Test (Sample)

## Study Guide


**Everything you need from our exam experts!**

# Questions

1. **What type of attack did Stetson commit when he secretly installed a sniffing device to listen to conversations on a network?**

   **A. Eavesdropping**

   **B. Ad-hoc connection attack**

   **C. Jamming attack**

   **D. Enumeration**

2. **What is the smallest physical storage unit on a hard-disk platter known as?**

   **A. Block**

   **B. Sector**

   **C. Cluster**

   **D. Byte**

3. **What does the term 'Sector' refer to in data storage terminology?**

   **A. A component of a file system**

   **B. A basic unit of storage on a disk**

   **C. A type of memory**

   **D. A data recovery method**

4. **What command did Zayn execute to view TCP and UDP network connections on a Windows machine?**

   **A. ipconfig**

   **B. netstat -ano**

   **C. tracert**

   **D. nslookup**

5. **In which phase does a forensic officer perform data acquisition and analysis of evidentiary data?**

   **A. Analysis phase**

   **B. Investigation phase**

   **C. Post-investigation phase**

   **D. Pre-investigation phase**

**6. Which command will help Eduardo retrieve the NetBIOS name-to-IP address mappings?**

**A. netstat**

**B. nbtstat**

**C. tracert**

**D. ipconfig**

**7. What information does the ID section of a sector contain?**

**A. Data block location**

**B. Sector number and location**

**C. Data checksum**

**D. Storage capacity**

**8. What type of data did Serin utilize to summarize conversations between two network devices?**

**A. Alert data**

**B. Session data**

**C. Event masking**

**D. Indicators of compromise**

**9. What technique refers to missing events related to systems downstream from a failed system?**

**A. Event correlation**

**B. Event masking**

**C. Root cause analysis**

**D. Payload correlation**

**10. Which NTFS system file contains definitions for all system and user-defined attributes of the volume?**

**A. $attrdef**

**B. $mft**

**C. $data**

**D. $standard_info**

# Answers

**1. A**
**2. B**
**3. B**
**4. B**
**5. B**
**6. B**
**7. B**
**8. B**
**9. B**
**10. A**

# Explanations

## 1. What type of attack did Stetson commit when he secretly installed a sniffing device to listen to conversations on a network?

**A. Eavesdropping**

**B. Ad-hoc connection attack**

**C. Jamming attack**

**D. Enumeration**

**The act of secretly installing a sniffing device to listen to conversations on a network is classified as eavesdropping. This type of attack involves intercepting and monitoring communications without the knowledge of the parties involved. Eavesdropping can take many forms, but in the context of network security, it typically refers to the unauthorized access of data packets traveling through a network. This can include listening to voice conversations, capturing emails, or stealing sensitive information. In this scenario, Stetson's actions demonstrate a clear intention to covertly gather information from network communications, which epitomizes eavesdropping. By using a sniffing device, he is effectively tapping into the data flows, thereby compromising the confidentiality and privacy of the communications that are intended to be secure. This distinguishes eavesdropping from the other types of attacks listed, which involve different tactics and objectives.**

## 2. What is the smallest physical storage unit on a hard-disk platter known as?

**A. Block**

**B. Sector**

**C. Cluster**

**D. Byte**

**The smallest physical storage unit on a hard-disk platter is referred to as a sector. Sectors are the fundamental building blocks of data storage on hard drives, with each sector typically containing 512 bytes of data. This organization allows for efficient reading and writing of data as the disk head moves across the surface of the platter. Understanding this concept is crucial for digital forensics, as sectors are the smallest identifiable units that can be accessed, read, and analyzed when recovering data. Forensic professionals often work with sectors to retrieve deleted files or analyze disk images, making a solid understanding of sectors and their function essential in the field. While blocks, clusters, and bytes represent data structures or counts, they do not specifically define the smallest unit on the physical disk surface. Blocks usually refer to larger groups of sectors used by file systems, clusters are combinations of sectors grouped together for storage management, and bytes are the individual units of data within these sectors.**

## 3. What does the term 'Sector' refer to in data storage terminology?

**A. A component of a file system**

**B. A basic unit of storage on a disk**

**C. A type of memory**

**D. A data recovery method**

**The term 'Sector' refers specifically to a basic unit of storage on a disk. In the architecture of a hard drive or other storage devices, a sector is the smallest addressable unit of storage that can be read from or written to. Typically, each sector holds a fixed amount of data, commonly 512 bytes or more in modern systems, which allows the operating system and applications to efficiently manage and access data. Understanding that a sector is a fundamental part of how data is organized on physical media helps clarify its role in data storage. It differs from a component of a file system, which involves higher-level organization of files and directories, or a type of memory, which could refer to various memory technologies that store data electronically. Additionally, a data recovery method refers to techniques used to retrieve lost or inaccessible data but does not define a sector itself.**

## 4. What command did Zayn execute to view TCP and UDP network connections on a Windows machine?

**A. ipconfig**

**B. netstat -ano**

**C. tracert**

**D. nslookup**

**The command that allows a user to view TCP and UDP network connections on a Windows machine is "netstat -ano." This command provides a comprehensive view of the current network connections and listening ports, along with their associated process IDs. The flags used in the command have specific functions: "a" displays all connections and listening ports, "n" shows the addresses and port numbers in numerical form, and "o" includes the process ID for each connection. This command is vital in network troubleshooting and security analysis, as it helps identify which applications are using network resources and can be used to detect any unauthorized connections or potential malicious activities. The ability to see active connections enables administrators or forensic analysts to monitor the state of network activity effectively. Other options like ipconfig are used for configuration information rather than active connections, tracert is meant for tracing network routers to a specific destination, and nslookup is designed for querying DNS records.**

## 5. In which phase does a forensic officer perform data acquisition and analysis of evidentiary data?

**A. Analysis phase**

**B. Investigation phase**

**C. Post-investigation phase**

**D. Pre-investigation phase**

**The investigation phase is where a forensic officer actively engages in the critical tasks of data acquisition and analysis of evidentiary data. During this phase, the officer systematically collects data from various sources such as computers, mobile devices, or networks, ensuring that the evidence is preserved in its original form to maintain its integrity for possible legal proceedings. Data acquisition in this context involves obtaining data without altering or damaging it, employing methods like disk imaging or copying files. Following this, analysis is conducted to examine the data for relevant information, patterns, or anomalies that can support the investigation. Forensic officers utilize specialized tools and methodologies during this phase to meticulously analyze the evidence in a way that adheres to legal standards and protocols. The other phases mentioned do not encompass the primary tasks of acquiring and analyzing data. The pre-investigation phase is focused on preparing for the investigation, while the analysis phase typically refers to the examination of data post-acquisition. The post-investigation phase centers on reporting findings and conclusions drawn from the analysis conducted earlier in the investigation phase.**

## 6. Which command will help Eduardo retrieve the NetBIOS name-to-IP address mappings?

**A. netstat**

**B. nbtstat**

**C. tracert**

**D. ipconfig**

**The command that allows Eduardo to retrieve the NetBIOS name-to-IP address mappings is "nbtstat." This command is specifically designed to provide information about the network and can display the NetBIOS over TCP/IP statistics. It helps in querying the NetBIOS name table to show the names registered on the local computer and their associated IP addresses. This functionality is crucial in diagnosing issues related to network protocols and can assist in identifying which computer (by its NetBIOS name) corresponds to which IP address on the network. This command is widely used in situations where there is a need to resolve a hostname to an IP address in a Windows environment, especially for applications that rely on NetBIOS names, which are often used in Windows networking. While other commands like "netstat," "tracert," and "ipconfig" serve different purposes, they do not specifically target NetBIOS name resolution. "Netstat" displays active connections and listening ports, "tracert" is used for tracing the path packets take to reach a network host, and "ipconfig" provides IP address configuration information without the focus on NetBIOS names. Therefore, "nbtstat" is the most appropriate choice for retrieving NetBIOS name-to**

## 7. What information does the ID section of a sector contain?

**A. Data block location**

**B. Sector number and location**

**C. Data checksum**

**D. Storage capacity**

**The ID section of a sector is responsible for storing important identifiers that help in organizing and accessing data within the storage medium. Specifically, it contains the sector number and the location information. This is crucial because it allows the operating system and applications to locate the data stored within a particular sector quickly and accurately. The sector number is a unique identifier for that sector, while the location helps in referencing where the sector is situated on the disk. Understanding this concept is critical for anyone involved in digital forensics or data recovery, as it relates to how data is structured on physical storage devices.**

## 8. What type of data did Serin utilize to summarize conversations between two network devices?

**A. Alert data**

**B. Session data**

**C. Event masking**

**D. Indicators of compromise**

**The correct answer is session data because this type of data encompasses the interaction between two network devices over a specific period. Session data includes information about established connections, including start and end times, protocols used, and the amount of data transferred. This makes it ideal for summarizing conversations since it captures the context and flow of communication between devices. By analyzing session data, one can gain insights into the patterns and behaviors of network applications, which is essential for understanding the overall interactions and for forensic investigations. It provides a comprehensive view of the sessions to ascertain what was communicated between devices during those periods. The other options, while relevant in network security contexts, do not serve the same purpose as session data. For example, alert data refers to notifications generated by security systems when suspicious activity is detected, which does not directly summarize the content of conversations between devices. Event masking involves hiding certain events or data points to streamline analysis, which does not provide the actual summary needed. Indicators of compromise represent artifacts or behaviors indicative of potential breaches but do not encapsulate the regular data flow between devices.**

## 9. What technique refers to missing events related to systems downstream from a failed system?

**A. Event correlation**

**B. Event masking**

**C. Root cause analysis**

**D. Payload correlation**

**The technique that refers to missing events related to systems downstream from a failed system is event masking. This occurs when the failure of one system prevents the logging or reporting of events from other dependent systems, effectively masking those events. In digital forensics or incident response, understanding this concept is crucial because it highlights the importance of tracing how failures in one area can obscure visibility into the impacts on other parts of the infrastructure. When a system fails, it may not only halt its own logging mechanisms but also disrupt the collection and transmission of events from systems that rely on the failed system, leading to gaps in the incident data that investigators need to analyze. While event correlation and payload correlation involve analyzing relationships and associations between events, they do not specifically address the phenomenon of events being hidden or missed due to a failure in another system. Root cause analysis focuses on identifying the underlying reason for a problem, which is related but distinct from observing the downstream impacts of system failures.**

## 10. Which NTFS system file contains definitions for all system and user-defined attributes of the volume?

**A. $attrdef**

**B. $mft**

**C. $data**

**D. $standard_info**

**The file that contains definitions for all system and user-defined attributes of the NTFS volume is the $attrdef file. This file is integral to the NTFS file system as it provides critical information regarding how attributes associated with filesystem objects are interpreted and managed. When a new attribute is created, it is defined within this file, allowing the file system to maintain consistency and understanding of various attributes across the volume. The $mft file, or Master File Table, is crucial as it contains metadata about every file and directory on the NTFS volume, but it does not specifically provide definitions of attributes. Instead, it utilizes the information contained within the $attrdef file to understand what those attributes mean. The $data file refers to the actual content of files stored on the NTFS volume, while $standard_info is a system file that holds standard information about a file, such as timestamps and file attributes, but again, it does not encompass attribute definitions as the $attrdef file does. Thus, the uniqueness of the $attrdef file in providing definitions makes it the correct answer in this context.**