**Vendor:** EC-Council

**Exam Code:** 112-57

**Exam Name:** EC-Council Threat Intelligence Essentials (TIE)

**Version:** DEMO

**QUESTION 1**
Which of the following network protocols creates secure tunneling through which content obfuscation can be achieved?

A. SNMP
B. ARP
C. SSH
D. UDP

**Answer:** C
**Explanation:**
SSH (Secure Shell) is specifically designed to provide an encrypted channel over an untrusted network. In digital forensics and incident response, SSH is well known for supporting tunneling/port forwarding, where traffic for another protocol (for example, HTTP, database connections, or remote desktop) is encapsulated inside an SSH session. Because the SSH session encrypts payload data (and can also protect authentication and command content), the tunneled traffic becomes obfuscated to network monitoring tools that can only see metadata such as source/destination IPs, port numbers (often TCP/22), timing, and byte counts. This capability is frequently discussed in forensic references as a mechanism that can hinder content inspection and complicate attribution of user actions purely from packet payload analysis.

By contrast, SNMP is primarily for network management and monitoring, not secure tunneling. ARP resolves IP-to-MAC addresses on local networks and does not provide encryption or tunneling. UDP is a transport protocol that can carry data for many applications but provides no built-in security or tunneling features by itself. Therefore, the protocol that creates secure tunneling enabling content obfuscation is SSH (C).

**QUESTION 2**
Below are the elements included in the order of volatility for a typical computing system as per the RFC 3227 guidelines for evidence collection and archiving.

```
1. Archival media
2. Remote logging and monitoring data related to the target system
3. Routing table, process table, kernel statistics, and memory
4. Registers and processor cache
5. Physical configuration and network topology
6. Disk or other storage media
7. Temporary system files
```

Identify the correct sequence of order of volatility from the most to least volatile for a typical system.

A. 7-->5-->4-->3-->2-->6-->1
B. 4-->3-->7-->6-->2-->5-->1
C. 2-->1-->4-->3-->6-->5-->7
D. 4-->3-->7-->1-->2-->5-->6

**Answer:** B
**Explanation:**
RFC 3227's "order of volatility" principle guides responders to collect the most perishable evidence first because some data can disappear immediately when power is lost, processes terminate, or the system state changes during response actions. The most volatile items are CPU registers and processor cache (4) because they change continuously at instruction speed and are lost instantly on shutdown or context switching. Next are routing table, process table, kernel

statistics, and memory (3) because live RAM contents and active system tables can change within seconds and are lost if the machine is powered off or rebooted.

After volatile memory, temporary system files (7) are collected because they are frequently overwritten or cleaned by the OS, users, or malware. Then comes disk or other storage media (6) which is more persistent but still subject to modification, log rotation, and overwriting through normal activity; hence imaging should occur before extensive interaction.

Less volatile still are remote logging and monitoring data (2) since they may persist off-host, but can be rotated or altered by retention policies. Physical configuration and network topology (5) generally changes less frequently and can often be re-documented later. Finally, archival media (1) is the least volatile because it is typically write-once or preserved storage. Thus the correct sequence is 4376251 (Option B).

**QUESTION 3**
Wesley, a professional hacker, deleted a confidential file in a compromised system using the "/bin/rm/" command to deny access to forensic specialists.

Identify the operating system on which Don has performed the file carving act.

A. Windows
B. Android
C. Mac OS
D. Linux

**Answer:** D
**Explanation:**
The command path /bin/rm is a hallmark of UNIX/POSIX-style operating systems, where core userland utilities are commonly stored under directories such as /bin, /sbin, and /usr/bin. The utility rm (remove) is the standard UNIX command used to delete directory entries that reference a file's data blocks on disk. This layout and command structure do not match Windows, which uses different filesystem conventions (drive letters, backslashes, and Windows-native executables) and does not provide /bin/rm as a native path. Android, while Linux-kernel-based, typically exposes shell utilities through environments like /system/bin (and newer systems may use toybox/busybox variants), not the classic /bin hierarchy expected on general-purpose UNIX systems. Between the remaining options, both Linux and macOS are UNIX-like and can include an rm command; however, in digital forensics training and examination contexts, the explicit reference to /bin/rm is most commonly used to indicate a Linux/UNIX command-line environment on a compromised host.

**QUESTION 4**
A disk drive has 16,384 cylinders, 80 heads, and 63 sectors per track, and each sector can store 512 bytes of data.

What is the total size of the disk?

A. 42,278,584,320 bytes
B. 42,278,584,340 bytes
C. 42,279,584,320 bytes
D. 43,278,584,320 bytes

**Answer:** A
**Explanation:**

Sectors per track) multiplied by bytes per sector. Forensic examiners learn this because it helps validate whether an image acquisition size is consistent with the physical disk geometry and to spot anomalies caused by misreported device geometry or capture errors.

First compute total addressable sectors:
Then multiply by sectors per track:

This matches option A exactly. In practice, modern drives often use LBA and may report different logical geometries, but the forensic principle remains the same: capacity equals the number of logical blocks times the logical block size, and CHS-style values are a structured way to perform that verification.

**QUESTION 5**
Which of the following tools helps forensic experts analyze user activity in the Microsoft Edge browser?

A. MZHistoryView
B. BrowsingHistoryView
C. MZCacheView
D. ChromeHistoryView

**Answer:** B
**Explanation:**
In Windows forensics, analyzing Microsoft Edge user activity commonly involves extracting and correlating browser artifacts such as visited URLs, visit counts, timestamps, download references, and cached content indicators. A practical forensic approach is to use a tool that can parse and normalize history artifacts across multiple browsers, because investigations often require comparing activity between Edge and other installed browsers on the same workstation. BrowsingHistoryView is designed specifically for that purpose: it aggregates browsing history from different browsers and presents it in a unified timeline-style view, which supports rapid triage and cross-validation of user activity.

By contrast, MZHistoryView and MZCacheView are associated with Mozilla-family artifacts (history and cache), making them appropriate for Firefox-related examinations rather than Edge. ChromeHistoryView is specialized for Google Chrome history databases and does not target Edge artifacts as its primary source. In forensic workflow terms, a multi-browser history tool is valuable because it helps identify patterns such as repeated access to specific domains, time windows of browsing activity, and correlation with other Windows artifacts (prefetch, jump lists.

# Thank You for Trying Our Product

## Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

**10% Discount Coupon Code:** **ASTR14**