PassQueen
a.k.a dumpsqueen.com

EC-Council Digital Forensics Essentials (DFE)

ECCouncil 112-57

Version Demo

Total Demo Questions: 10

Total Premium Questions: 102

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Introduction to Digital Forensics	6
Topic 2, Computer Forensics Investigation Process	8
Topic 3, Understanding Hard Disks and File Systems	7
Topic 4, Data Acquisition and Duplication	11
Topic 5, Defeating Anti-Forensics Techniques	4
Topic 6, Windows Forensics	20
Topic 7, Linux and Mac Forensics	8
Topic 8, Network Forensics	9
Topic 9, Web Application Forensics	8
Topic 10, Dark Web Forensics	3
Topic 11, Malware Forensics	6
Topic 12, Cloud Forensics	1
Topic 13, Email Crime and Computer Forensics	8
Topic 14, Mobile Forensics	1
Topic 15, Mix Questions	2
Total	102

QUESTION NO: 1

David, a cybercriminal, targeted a community and initiated anti-social campaigns online. In this process, he used a layer of the web that allowed him to maintain anonymity during the campaign.

Which of the following layers of the web allowed David to hide his presence during the anti-social campaign?

A. Surface Web

B. World Wide Web

C. Dark Web

D. Deep Web

ANSWER: C

Explanation:

Dark Web is correct because it consists of intentionally concealed services and sites that operate through anonymity-focused overlay networks, most commonly Tor. Tor routes communications through multiple relays, helping conceal a user's originating IP address from the destination and making direct network-level attribution more difficult. Dark-web services can also be configured as onion services, which avoid exposing the service host's normal public IP address. These properties make the dark web a relevant environment for actors seeking to communicate, coordinate, publish material, or access services while reducing the visibility of their identity and location. In a digital-forensics context, this does not mean that attribution is impossible: investigators may still use endpoint evidence, seized systems, operational-security mistakes, service logs where available, financial records, and correlation of other artifacts. However, the defining purpose of dark-web infrastructure is to provide stronger privacy and anonymity characteristics than ordinary publicly indexed websites. The U.S. National Institute of Standards and Technology describes Tor as an anonymizing network designed to conceal users' network locations, while the Tor Project explains that onion services provide services without revealing their locations. See NIST: The Tor Anonymity Network and Tor Project: Onion Services.

QUESTION NO: 2

Which of the following acts was passed by the U.S. Congress in 2002 to protect investors from the possibility of fraudulent accounting activities by corporations?

A. The Electronic Communications Privacy Act

B. General Data Protection Regulation (GDPR)

C. Sarbanes–Oxley Act (SOX)

D. Information Privacy Act 2014

ANSWER: C

Explanation:

Sarbanes–Oxley Act (SOX) is correct. Congress enacted the Sarbanes-Oxley Act of 2002 in response to major corporate accounting scandals and to strengthen protections for investors who rely on public companies' financial reporting. SOX established significant requirements for publicly traded companies, their executives, auditors, and audit committees. Among its key measures, it requires chief executive and chief financial officers to certify the accuracy of financial reports, requires management to assess internal controls over financial reporting, and imposes rules intended to improve auditor independence and accountability. These controls help reduce the opportunity for material misstatements, concealment of financial information, and fraudulent accounting practices. From a digital-forensics and compliance perspective, SOX also increases the importance of preserving reliable electronic business records, maintaining audit trails, and applying controls that support the integrity and availability of financial data. The statutory text identifies the law as the Sarbanes-Oxley Act of 2002 and states its purpose is to protect investors by improving the accuracy and reliability of corporate disclosures. See the official Sarbanes-Oxley Act text and the U.S. Securities and Exchange Commission's SOX resource page.

QUESTION NO: 3

Bob, a forensic investigator, was instructed to review a Windows machine and identify any anonymous activities performed using it. In this process, Bob used the command “netstat -ano” to view all the active connections in the system and determined that the connections established by the Tor browser were closed.

Which of the following states of the connections established by Tor indicates that the Tor browser is closed?

A. CLOSE_WAIT

B. TIME_WAIT

C. ESTABLISHED

D. LISTENING

ANSWER: B

Explanation:

TIME_WAIT is the appropriate state indicating that a TCP connection formerly used by the Tor browser has been closed from the local endpoint's perspective and is completing the TCP shutdown process. When a program closes a TCP connection, Windows may retain the connection entry in the TIME_WAIT state temporarily. This waiting interval helps ensure that delayed packets associated with the previous connection are not confused with packets from a later connection using the same endpoint details. Therefore, during a forensic review using `netstat -ano`, Tor-related connections shown as TIME_WAIT are evidence of recently terminated rather than currently active sessions.

The `-a` parameter displays all active connections and listening ports, `-n` displays addresses and ports numerically, and `-o` includes the process identifier, allowing an investigator to correlate observed network entries with processes. Microsoft documents these parameters and the connection-state output in its Netstat command reference. The TCP specification also defines TIME-WAIT as the state entered after the active close, where the endpoint waits before fully removing the connection control information; see RFC 9293.

QUESTION NO: 4

A Windows user claims that a confidential document was never renamed before it was deleted. The investigator needs an artifact that can help identify file-system change events, including rename and deletion activity, on an NTFS volume.

Which artifact is most useful for this purpose?

A. $Bitmap

B. $LogFile

C. $UsnJrnl

D. $Secure

ANSWER: C

Explanation:

The NTFS change journal, `$UsnJrnl`, records change activity for files and directories, including events associated with creation, deletion, renaming, and data changes. Its records can help an examiner reconstruct a sequence of file-system activity and identify prior names or paths when the relevant entries remain available.

The $MFT provides essential file metadata, but it is not primarily a chronological journal of changes. $Bitmap records allocation status, while $LogFile is chiefly used by NTFS for transactional recovery and is less directly suited to identifying the requested file-change history.

QUESTION NO: 5

Below is an extracted Apache error log entry.

“[Wed Aug 28 13:35:38.878945 2020] [core:error] [pid 12356:tid 8689896234] [client 10.0.0.8] File not found: /images/folder/pic.jpg”

Identify the element in the Apache error log entry above that represents the IP address from which the request was made.

A. 13:35:38.878945

B. 12356

C. 10.0.0.8

D. 8689896234

ANSWER: C

Explanation:

10.0.0.8 is the client IP address recorded for the request. Apache HTTP Server error-log entries can include a client field in the form `[client address]`, where `address` identifies the remote client associated with the event. In this entry, the bracketed field `[client 10.0.0.8]` directly associates that IPv4 address with the failed attempt to retrieve `/images/folder/pic.jpg`. From a forensic perspective, this field is important for correlating web-server activity with network records, identifying the system that made a request, and determining whether repeated errors or suspicious requests originated from the same source. The value is an IPv4 address in dotted-decimal notation, consisting of four decimal octets separated by periods. Apache’s error-log documentation describes the error log as the location where the server records diagnostic information and explains that log formats may contain contextual information about the request and client. See the Apache HTTP Server error log documentation and the Apache core error-handling documentation for related logging and error-reporting context.

QUESTION NO: 6

Which of the following titles of The Electronic Communications Privacy Act protects the privacy of the contents of files stored by service providers and records held about the subscriber by service providers, such as subscriber name, billing records, and IP addresses?

A. Title II

B. Title IV

C. Title III

D. Title I

ANSWER: A

Explanation:

Title II is correct because it is the Stored Communications Act (SCA), the portion of the Electronic Communications Privacy Act that establishes privacy protections for electronic communications held in storage by service providers. Codified principally at 18 U.S.C. §§ 2701–2713, the SCA addresses both the contents of stored wire or electronic communications and specified non-content customer records maintained by providers. Those records can include subscriber identity, account information, billing details, session times, and assigned IP addresses. The law also defines the circumstances and legal process under which a provider may voluntarily disclose or may be compelled to disclose stored content and customer records to governmental entities. This distinction is especially important in digital-forensics investigations because data collected from an online provider is often governed by the SCA rather than solely by the technical ability to retrieve it. The statutory disclosure provisions, including the categories of subscriber and transactional information in 18 U.S.C. § 2703, directly support the description in the question. See the SCA text at Cornell Law School, 18 U.S.C. Chapter 121 and the U.S. Department of Justice’s Electronic Communications Privacy Act overview.

QUESTION NO: 7

Sam, a digital forensic expert, is working on a case related to file tampering in a system at the administrative department of an organization. In this process, Sam started performing the following steps to analyze the acquired data to draw conclusions related to the case.

1.Analyze the file content for data usage.

2.Analyze the date and time of file creation and modification.

3.Find the users associated with file creation, access, and file modification.

4.Determine the physical storage location of the file.

5.Generate a timeline.

6.Identify the root cause of the incident.

Identify the type of analysis performed by Sam in the above scenario.

A. Case analysis

B. Data analysis

C. Reporting

D. Search and seizure

ANSWER: B

Explanation:

Data analysis is correct because Sam is interpreting the artifacts obtained from an acquired system image in order to reconstruct events and reach a defensible conclusion about suspected file tampering. This work includes examining file contents and usage, evaluating file-system timestamps for creation and modification activity, associating actions with users, and identifying the file's location on the storage medium. These are core evidence-analysis activities because they turn raw acquired data into meaningful facts about what happened, when it happened, where the relevant artifact resides, and which account or user may be connected to the activity.

Creating a timeline is especially characteristic of data analysis. Examiners correlate timestamps and related artifacts to establish event sequence, detect inconsistencies, and determine whether activity supports the incident hypothesis. Identifying the root cause is the conclusion reached after this correlation and interpretation. NIST describes digital forensic analysis as examining collected data to identify and extract information relevant to an investigation, including using timelines and artifact correlation to understand events. EC-Council's Digital Forensics Essentials curriculum likewise treats the examination and analysis of acquired evidence as a central forensic activity. See NIST SP 800-86 and EC-Council Digital Forensics Essentials.

QUESTION NO: 8

An investigator wants to extract information about the status of the network interface cards (NICs) in an organizationâ€™s Windows-based systems. Identify the command-line utility that can help the investigator detect the network status.

A. ipconfig

B. PsLoggedOn

C. PsList

D. ifconfig

ANSWER: A

Explanation:

ipconfig is the appropriate Windows command-line utility for examining a system's current TCP/IP network configuration and the state of its network adapters. For a live forensic examination, its output helps establish the endpoint's connectivity context at the time of collection, including assigned IPv4 and IPv6 addresses, subnet masks, default gateways, and DNS server addresses. This information can be correlated with DHCP leases, firewall records, network-flow data, VPN records, and other organizational logs to determine how the system was connected to the network.

Investigators commonly use `ipconfig /all` because it provides more complete adapter-level information than the basic command. The expanded output includes each adapter's physical (MAC) address, description, DHCP status, DHCP server, DNS suffixes, and lease-obtained or lease-expiration details where applicable. These details are valuable for identifying the specific interface used by a host and documenting its active network configuration in a repeatable manner. Microsoft describes `ipconfig` as a tool for displaying the current TCP/IP configuration and refreshing DHCP/DNS-related settings. See Microsoft's ipconfig command reference and the Microsoft DHCP documentation.

QUESTION NO: 9

Which of the following files belonging to the Extensible Storage Engine (ESE) stores the mail data in Microsoft Exchange Server?

A. DataStore.edb

B. Mail.MSMessageStore

C. WLCalendarStore.edb

D. Database.edb

ANSWER: D

Explanation:

Database.edb is correct because Microsoft Exchange Server stores mailbox content in an Extensible Storage Engine (ESE) database with the `.edb` extension. This mailbox database is the persistent repository for Exchange mail data, including email messages, attachments, mailbox folders, contacts, calendar items, and the associated message properties and metadata. Although an administrator can assign a different filename to an Exchange mailbox database, the fundamental artifact remains an ESE `.edb` file; "Database.edb" represents that Exchange database file in this question.

For digital-forensics work, the Exchange ESE database is a key evidence source because it contains the structured records that represent mailbox objects and their relationships. Investigators may acquire and examine the database alongside its transaction logs, which record changes and can be relevant to recovery or timeline analysis. Microsoft's Exchange documentation identifies mailbox databases as the storage location for mailbox data and notes that each database has an ESE database file. The ESE technology itself is Microsoft's embedded database engine used by Exchange for this purpose. See Microsoft Learn: Mailbox databases in Exchange Server and Microsoft Learn: Extensible Storage Engine.

QUESTION NO: 10

An investigator is reviewing an Apache access log after a suspected web-shell upload. The log shows the following request:

```
192.0.2.45 - - [12/May/2024:14:20:18 +0000] "POST /upload.php HTTP/1.1" 200 318
```

Which conclusion can be drawn directly from the status code in this entry?

A. The uploaded file was confirmed to be a web shell

B. The client was confirmed to have authenticated successfully

C. The web shell was confirmed to have executed

D. The server reported a successful response to the HTTP request

ANSWER: D

Explanation:

The status code **200** indicates that the server reported a successful HTTP response to the POST request. It supports the conclusion that Apache processed the request without reporting an HTTP error for that transaction.

The status code alone does not prove that a malicious file was uploaded, that a web shell executed, or that the client authenticated successfully. The investigator must correlate the request with application logs, uploaded-file locations, file-system timestamps, and server-side artifacts to determine the result of the upload operation.