Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 4/19/2022 7:29:42 pm • Time spent: 06:37

Score: 90%

Passing Score: 80%

Question 1: ✓ Correct

What is the most important element related to evidence in addition to the evidence itself?

○ Photographs of the crime scene

➡ ● Chain of custody document

○ Witness testimony

○ Completeness

EXPLANATION

The chain of custody document is the most important item related to the evidence.

Nothing is more important than the chain of custody document, including photographs. Witness testimony can be helpful, but it is not more important than the chain of custody document. Completeness of the evidence is beneficial, but it is not as beneficial as a reliable chain of custody document.

REFERENCES

12.5.9 Forensic Investigation Facts

q_for_invest_chain_01_secp7.question.fex

Question 2: ✓ Correct

The chain of custody is used for which purpose?

- ○ Retaining evidence integrity
- ➡ ● Listing people coming into contact with the evidence
- ○ Identifying the owner of the evidence
- ○ Detailing the timeline between creation and discovery of evidence

EXPLANATION

The chain of custody is used to track the people who came in contact with the evidence. The chain of custody starts at the moment evidence is discovered and lists the identity of the person who discovered, logged, gathered, protected, transported, stored, and presented the evidence. The chain of custody helps to ensure the admissibility of evidence in court.

REFERENCES

12.5.9 Forensic Investigation Facts

q_for_invest_chain_02_secp7.question.fex

Question 3: ✓ Correct

You have been asked to draft a document related to evidence-gathering that contains details about personnel in possession and control of evidence from the time of discovery up through the time of presentation in court. Which type of document is this?

○ Rules of evidence

➡ ● Chain of custody

○ FIPS-140

○ CPS (certificate practice statement)

EXPLANATION

The chain of custody is a document related to evidence-gathering that contains details about personnel in possession and control of evidence from the time of discovery up through the time of presentation in court.

A CPS (certificate practice statement) is a document written by a certificate authority outlining their certificate handling, management, and administration procedures. FIPS-140 is a government standard that defines procedures, hardware, and software that can be employed when performing forensic investigations of cybercrime. The rules of evidence are the restrictions that must be adhered to in order to ensure the admissibility of collected evidence.

REFERENCES

12.5.9 Forensic Investigation Facts

q_for_invest_chain_03_secp7.question.fex

Question 4: ✓ Correct

How can a criminal investigator ensure the integrity of a removable media device found while collecting evidence?

○ Reset the file attributes on the media to read-only

➡ ● Create a checksum using a hashing algorithm

○ Write a log file to the media

○ Enable write protection

EXPLANATION

To protect or ensure the integrity of collected digital evidence, an investigator should create a checksum using a hashing algorithm. In the future, the same hashing algorithm can be used to create another checksum. Then the two values are compared. If the checksums are identical, the media was not altered.

Not all removable media has write-protection switches, and it is possible for software to circumvent these physical restrictions. Writing a new file to the media or altering the settings on files on the media is a direct violation of integrity.

REFERENCES

12.5.9 Forensic Investigation Facts

q_for_invest_checksum_secp7.question.fex

Question 5: ✕ Incorrect

As a security analyst, you are configuring your environment to be able to properly gather digital forensic information. Which of the following must be set up to help create a timeline of events?

➡ ○ Make sure all client computers have their time set accurately by a time server.

○ Create a solid chain of custody that proves that no evidence-tampering has occurred.

○ Create a report template that helps you describe the incident, how the evidence was analyzed, and the conclusions you came to.

● ~~Create tags for all your IT assets so that they are easily identifiable and trackable.~~

EXPLANATION

You would choose to make sure that all client computers have their time set accurately by a time server. Event logs are only as reliable as the system they come from. These logs show exactly what happened on a specific computer and are also timestamped. These timestamps provide the backbone for a timeline of events, which allows the evidence to be admissible. You should also configure the correct time offset by setting the correct time zone.

REFERENCES

12.5.9 Forensic Investigation Facts

q_for_invest_eventlogs_secp7.question.fex

Question 6: ✓ Correct

You want to store your computer-generated audit logs in case they are needed in the future for examination or to be used as evidence in the event of a security incident. Which method can you use to ensure that the logs you put in storage have not been altered when you use them in the future?

- ○ Make two copies of each log and store each copy in a different location.
- ○ Store the logs in an offsite facility.
- ➡ ● Create a hash of each log.
- ○ Encrypt the logs.

EXPLANATION

Use a hash to verify that the contents of a log have not been altered. When you analyze the logs, take another hash and compare the new hash to the original one. If the hashes match, the logs have not been altered.

Storing logs offsite makes them harder to access and alter, and this prevents a disaster at your main location from destroying the logs. Encrypting the logs protects the log confidentiality but does not prevent them from being altered, nor can it prove that the logs have not been altered. Creating two copies of the logs ensures that a single disaster does not destroy the logs. Comparing both logs to make sure they match does not guarantee that someone didn't alter both copies. In addition, if a disaster destroys one copy of the logs, you would not have a way to verify that the remaining copy has not been altered.

REFERENCES

12.5.9 Forensic Investigation Facts

q_for_invest_hashing_01_secp7.question.fex

Question 7: ✓ Correct

What does the hashing of log files provide?

- ○ Prevention of log files being altered or overwritten
- ○ Prevention of the system running when the log files are full
- ➡ ● Proof that the files have not been altered
- ○ Sequencing of files and log entries to recreate a timeline of events
- ○ Confidentiality to prevent unauthorized reading of the files

EXPLANATION

Perform hashing of the log files to detect alteration. If a log file is altered, the hash of that file will be different. If the current hash is the same, you can assume that the file has not been altered.

Hashing can detect alteration, but does not prevent it; users can still alter or delete a file. Encryption prevents unauthorized users from viewing the file contents. Timestamps on logs and log entries identify when events occur so you can reconstruct a timeline of events. Audit policies and retention policies control how log files are saved and what the system does when a log cannot be created or when disk space is full.

REFERENCES

12.5.9 Forensic Investigation Facts

q_for_invest_hashing_02_secp7.question.fex

▼ Question 8: ✓ Correct

Which method can you use to verify that a bit-level image copy of a hard drive is an exact clone of the original hard drive collected as evidence?

- ➡ ● Hashing
- ○ Serial number notation
- ○ File directory listing
- ○ Photographs

EXPLANATION

Hashing is the method used to verify that a bit-level image copy of a hard drive is an exact clone of the original hard drive collected as evidence.

File directory listings, photographs, and serial number notation are not sufficient methods for verifying hard drive cloning.

REFERENCES

- 7.3.2 Hashing Algorithms
- 7.3.4 Using Hashes
- 7.3.5 Compare an MD5 Hash
- 12.5.9 Forensic Investigation Facts

q_for_invest_hashing_03_secp7.question.fex

▾ Question 9: ✓ Correct

Your company is about to begin litigation, and you need to gather information. You need to get emails, memos, invoices, and other electronic documents from employees. You'd also like to get printed, physical copies of documents. Which tool would you use to gather this information?

- ○ Timeline of events
- ○ Timestamps
- ➡ ● Legal hold
- ○ Chain of custody

EXPLANATION

You would use a legal hold. The purpose behind a legal hold is to help ease the burden of the IT and legal teams when it comes to gathering evidentiary documentation. This notice instructs employees to retain any electronically stored information, or ESI.

The chain of custody proves that no tampering has occurred in gathering evidence.

Timestamps provide an exact date and time of an event and must be accurate to be admissible.

A timeline of events is required for digital forensic evidence to be admissible and to prove who is most responsible for what occurred.

REFERENCES

12.5.9 Forensic Investigation Facts

q_for_invest_lglhold_secp7.question.fex

Question 10: ✓ Correct

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 said data.

Place the following items in the correct order of volatility in the gathering of potential evidence.

1

✓ Random Access Memory (RAM)

2

✓ Swap/page file

3

✓ Hard drive

4

✓ Remote logs

5

✓ Archived data

EXPLANATION

The correct order of volatility is:

1. Random Access Memory (RAM)
2. Swap/page file
3. Hard drive
4. Remote logs
5. Archived data

RAM is the most volatile of all computer data storage and is cleared when a computer is shut down.

Swap files or page files are a virtual extension of RAM.

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.

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 are documents, logs, etc. that are not used regularly and are stored on a device other than the device under forensic investigation.

REFERENCES

12.5.9 Forensic Investigation Facts

q_for_invest_volatility_secp7.question.fex