Digital evidence preservation: Techniques and best practices

So far, you've learned that security professionals and their teams must preserve evidence to ensure accurate investigations, and maintain legal and ethical best practices. It's a team's responsibility to keep clear, accurate, and complete records of any incident investigations. In this reading, you'll learn more about digital evidence preservation, along with some techniques to help you preserve digital evidence.

Please note, the following reading should not be considered legal advice. If there's an investigation in your workplace, reach out to your organization's legal council.

Digital evidence preservation techniques

Here are some best practices you can use when preserving digital evidence:

- Use disk imaging to maintain an original file. Create a bit-by-bit duplication of an evidence file. This lets you keep the original evidence file.
- Avoid doing any analysis on the original artifact, and the system as a whole by implementing write-blocking techniques. This will prevent data modifications on the original device and ensure data integrity during analysis. Anything done to the original artifact may prevent it from being accepted as legal evidence.
- During imaging, cryptographic hash values are created. A hash is a digital checksum. Your files can be identified by their hashes. If you change the file, the hash will also change. A changed hash can tell you if there's been a change to the file. So, you can use the hash to ensure the integrity of the file as evidence.
- When comparing cloud storage and local storage, cloud storage has additional layers of security, so it's more secure, and also safeguards your digital evidence files.
- Document the chain of custody by maintaining a detailed record of the device's possession and handling to ensure its traceability.
- Document all preservation procedures, including the tools used, timestamps, and any relevant observations to provide transparency and support admissibility in court.

Identifying and preserving volatile evidence

Improper handling of digital evidence can alter evidence. It's important to follow protocols when handling evidence because it can be volatile and fragile.

Here are a few questions you need to be able to answer when collecting your evidence:

- Who was involved with the cybercrime?
- What happened in the cybercrime?
- When did the cybercrime happen?
- Where did the cybercrime happen?
- How did the cybercrime happen?

When you preserve evidence, your goal is to protect digital evidence and maintain its integrity in every phase. You also want to ensure it's not modified. This involves establishing a clear chain of custody, which includes documenting and preserving evidence in a way that maintains its integrity, and establishes a clear timeline for handling. This also includes confirming the names, titles, and contact information of everyone who identified, collected, and acquired the evidence. It's helpful to document any relevant information, including the recipients of the transferred evidence, specific details about the evidence itself, the precise time and date of the transfer, and the reasons behind the transfer.

Digital evidence considerations for cloud-based storage

There are security vulnerabilities that come along with storing and transferring data to the cloud. So, you need to use strong security, including multi-factor authentication. For example, suppose you implement two-factor authentication. With two-factor authentication, an individual logs in on a computer, then gets a text on their phone with a code. They then put this code into the computer for a second authentication.

If you encrypt the data before you store it in the cloud, you need to make sure the encryption keys can be retrieved when you need them in the future. It's helpful to have a strategy to move the data in case something happens with the provider, like a change in their services.

Key takeaways

When preserving digital evidence, security professionals should follow common best practices to ensure accurate investigations. They should also ask questions about the evidence to gain a better understanding of the issue, when it occurred, and who was involved. And remember, it's critical to follow protocols when handling evidence because it can be volatile and fragile. The more information security professionals have, the better they can preserve the evidence, and appropriately handle the situation.