Checkpoint Operations, Governance & Risk Management

In the presented video, the digital forensics analyst undertakes a comprehensive investigation with a focus on creating evidence from potentially infected sources.

To establish evidence from potentially infected sources:

I. Linux Disk Imaging

1. Objective: Given a scenario, use the appropriate tool to assess organizational security (4.1).

- Successfully logged into the PT1-Kali VM with root credentials.

- Identified the suspect 1 GB disk as `/dev/sbd1` using the `lsblk` and `df` commands.

- Utilized the powerful `dd` command to duplicate the suspect disk, resulting in the creation of a disk image named `suspect.img`.

- Confirmed the existence of the `suspect.img` file within the `/root` directory.

2. Objective: Explain the key aspects of digital forensics (4.5).

- Implemented the MD5 hashing technique to generate a unique checksum for the `suspect.img` file, enhancing data integrity verification.

- Appended hash results after introducing controlled changes to the original image, demonstrating the importance of preserving evidence.

- Rigorously verified hash values to ensure the integrity of the disk image and data consistency.

3. Cautionary Note:

- Emphasized the critical importance of using tools like `dd` to avoid accidental data destruction when working directly with evidence.

II. Autopsy Forensics

1. Objective: Use the appropriate tool to assess organizational security (4.1).

- Accessed the Windows environment and opened the "Forensics - Marketing" case in Autopsy.

- Conducted a thorough examination of critical disk components, including the Master Boot Record, system volume (`vol2`), and boot volume (`vol3`).

- Analyzed folders such as Users > Viral > Downloads for potential evidence of malicious activities.

2. Objective: Explain the key aspects of digital forensics (4.5).

- Delved into Autopsy's features, exploring EXIF Metadata, Encryption details, and Installed Programs for additional insights.

- Observed the absence of download files in the specified directory, indicating potential intentional data concealment or deletion.

The Linux-based imaging process involving the use of the `dd` command and MD5 hashing served as a robust methodology for securely duplicating and verifying the integrity of the suspect disk. The cautionary note highlighted the risks associated with direct manipulation of evidence without proper tools, reinforcing the importance of a meticulous forensic approach.

Autopsy on the Windows platform provided a comprehensive examination of the seized disk image, uncovering valuable insights into file structures, metadata, and potential malicious activities. The absence of download files raises questions about intentional data concealment, warranting further investigation.