Strategy:

Our investigative team would begin by meeting with senior management and the legal team to discuss which devices and systems may contain relevant evidence. This would prevent the unnecessary examination of unrelated devices and systems, reducing operational impact. To minimize any potential downtime and the effect on the organization, John Smiths workstation and any devices involved should be imaged after business hours, and network traffic monitoring and log collection should be performed passively.

Each device or piece of evidence collected must follow a strict chain of custody protocol to ensure data is secured and not altered during this process. This will make the data and evidence admissible in court should any legal action be pursued. The collection of evidence, devices, and data should adhere to corporate policies and legal requirements such as the Electronic Communications Privacy Act (ECPA) and the Computer Fraud and Abuse Act (CFAA).

Multiple copies of forensic images should be created to ensure redundancy; one copy will be used for examination, while the other will remain securely stored in an evidence locker. This will reduce the need to access the original devices, decreasing the chances of evidence being changed on the original devices. Integrity checks will also be performed, preferably using SHA-256 hashing to ensure each copy of the data remains the same and unchanged from the original device. All actions taken during this investigation should be documented and benchmarked against the NIST SP 800-86 or ISO/IEC 27037 recommended procedures.

Tools and Techniques:

Evidence-gathering tools and techniques will include using FTK Imager to create forensic images of hard drives, removable media, and volumes of suspect devices. Write Blockers will also prevent any changes to the original devices when collected, ensuring that all the source evidence remains untouched and unchanged. SHA-256 hashes will also be generated by FTK Imager for each device during and after imaging to make sure data has not changed between images, ensuring data integrity.

Evidence preparation tools and techniques include the use of hashing and chain of custody documentation and logs. This ensures that all data handled remains unchanged throughout the entire process and that it is known precisely who handles data, when it was handled, and for what purpose. Hashing must occur before and after data transfer, preferably with SHA-256, to verify that none of it has been tampered with or corrupted. Hashing can be accomplished with the FTK Imager tool during and after the imaging process. This step maintains a clear history of evidence handling and ensures legal defensibility.

Evidence analysis tools and techniques will help to analyze the data and search for any unauthorized collection or transfers of proprietary information and policy violations. Autopsy, Encase, Wireshark, and NetworkMiner are four tools that can be used for analysis. According to ISO/IEC 27037, forensic tools must be validated for reliability and repeatability, ensuring that evidence gathered is admissible in legal proceedings (ISO, 2012). Autopsy is an open-source tool that can recover deleted files, create a timeline of events, and identify suspect artifacts. Encase is a commercial product that can analyze browser history, email artifacts, and file metadata. Wireshark and NetworkMiner are network analysis tools that examine network logs and packets to help trace and suspect file transfers or unauthorized external connections. Techniques will include metadata examination, registry key review, and file carving.

Collection and Preservation of Evidence:

All potential sources of digital evidence relating to John Smith must be identified before any collection takes place. Possible sources include John Smiths workstation or company-issued laptop and mobile devices, corporate email, and external storage devices. Volatile data should be collected first before a system is shut down. Encase will be used to create at least two full disk images of hard drives and any external storage, while write blockers will be used during the imaging process to prevent any changes to the original devices. A strict chain of custody protocol will be followed, and each piece of evidence will be tagged, labeled, and logged in a digital forensics case management system. Every interaction with the evidence should also be recorded and logged, including who handled the evidence, when, and why. All images should be mounted as read-only during the analysis to prevent any changes from occurring. Audit logs will be created to track the actions of the investigators and any changes made to the case file. Lastly, when not in use, the original devices should be stored in a separate evidence locker away from the copies, with only authorized personnel having access to them, and the copies should be securely stored to prevent tampering and ensure the integrity of all the data.

Examination of Evidence:

The examination phase will help determine whether John Smith violated company policy, had unauthorized access to proprietary data, and if he took it. We will begin with creating a timeline of events using Encase. Having a timeline will help identify periods of unusual activity on the devices, and these timestamps can be cross-referenced with logs and any suspect artifacts. This will allow investigators to match suspicious behavior with specific timeframes and devices. Next, the team will search the imaged drives for proprietary information by analyzing metadata using Encase. This analysis will help investigators determine if files were renamed or relocated and if they were copied to external drives or uploaded to cloud storage. The team can find and recover any deleted or hidden files using Encase. Encase will also allow the team to identify

USB devices that were connected to the source machine based on the stored serial numbers; they can then cross-reference the identified devices with the timeline created earlier to review data transfers.

John Smiths internet activity will also be investigated and reviewed. Encase will allow the team to search through the browser history and cookies of the imaged device. Access to personal email and file-sharing platforms will be uncovered, and keyword searches can be used to find files or data with proprietary information. Wireshark can then inspect packet capture data from the company's network logs to determine if any unauthorized external connections were made. The team will also analyze the logs and search for suspicious data uploads or traffic spikes from the source device. To maintain integrity, all findings and actions will be documented and logged with screenshots, hash values, and time stamps.

Approach to Drawing Conclusions:

The team will draw an accurate conclusion based on digital evidence acquired throughout the forensic investigation. This will include timeline artifacts and anomalies compared against file access records to confirm if sensitive proprietary data was accessed, copied, and transferred. According to the company policy, John Smith was not authorized to access proprietary information; if he did access the information, that alone is a breach of company policy. USB usage can be compared against file copy operations to help determine if data was copied or transferred. Network Traffic will also help determine if any data left the corporate network.

The timeline, combined with the actions mentioned above, will reconstruct John Smiths digital behavior. The team can compare John Smiths standard usage patterns in the context of his role against the usage found in the investigation to distinguish legitimate authorized access from potential abuse. This will help identify any key moments for the investigation that will ultimately help the team conclude. Any decisions will follow internal company policies, such as non-disclosure agreements (NDAs) and acceptable use policies (AUPs), as well as NIST SP 800-86. Following NIST guidance, conclusions will be based solely on verifiable evidence collected in a repeatable, standards-based manner (NIST, 2006).

Before our team finalizes our conclusions, the findings will be presented to at least one other certified forensic analyst for peer review. This will further validate the findings, ensure that all the evidence has been analyzed consistently and reproducibly, and show that no biases have influenced the conclusion. The final decision will be evidence-backed and either support or refute the claim that John Smith violated company policies.

Presentation of Details and Conclusions:

The findings will be presented to senior management clearly and professionally to ensure that they and the legal team can make an informed decision based on the results of the findings. The report should be accessible to both technical and non-technical stakeholders. The presentation should include a summary of objectives, methods used, key findings, and conclusions that should be tailored for executives who won't need the full technical details. The full report will contain all the technical information, and a presentation version will be created for senior management and legal review, which will use clear, jargon-free language and include visual aids like timelines and evidence flow diagrams. Supporting materials should be included as attachments, such as chain of custody logs and forms, screenshots of all key findings, and hash logs to ensure integrity. The tone of the report should remain objective and evidence-driven throughout. Senior management will have everything they need to make a properly informed decision in the case of John Smith.

Sources:

ISO. (2012). *ISO/IEC 27037:2012: Guidelines for identification, collection, acquisition, and preservation of digital evidence*. International Organization for Standardization. https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027037-2012.pdf

NIST. (2006). *Guide to integrating forensic techniques into incident response (NIST SP 800-86)*. National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/800/86/final