**Project Part 2: Researching Forensic Best Practices and Creating Procedures**

**Scenario**

D&B has been engaged by a state crime forensics lab to assist them in refreshing their procedures manual and bringing it up to date. Part of the project will include researching best practices for performing investigations and collecting digital evidence, which will be incorporated into the procedure’s manual. You have been asked to be a part of the small team that is regularly meeting with the client to review the procedures manual provide revised and new information.

1. **A procedure for capturing video of a crime scene**.

In accordance with ethical and legal guidelines, the Crime Scene Video Capture Procedure attempts to record crime scenes methodically and accurately for forensic examination. First step is making sure everything is secure, making sure the equipment works, and getting the right authorization to record. A thorough approach is emphasized in the documentation phase, which begins with an overview, records close-ups of important pieces of evidence, and applies panning techniques to provide spatial context. A grid system, steady camera movement, and filming the complete crime scene are all part of the systematic video capture process, whereas setting baselines include documenting the layout, measurements, and important objects. Appropriate tracking is ensured by evidence marking and chain of custody documents. Post-recording processes concentrate on making backups, checking for completeness, and methodically organizing files. Assessing accuracy, working together to identify further needs, turning down audio to remove background noise, and minimizing needless lingering are all part of finalization and review. The procedure emphasizes compliance to legal and ethical standards and records any shortcomings. [1]

1. **What to take screenshots of during an investigation.**

Taking screenshots strategically is crucial to efficiently documenting and preserving evidence during a digital inquiry. Start with an overview screenshot of the desktop or home screen. Take note of system data, such as the hardware specifications, operating system version, and pertinent program information. To comprehend the present state of the system, record open apps, processes that are active, and the file directory structure. Network activity can be collected from screenshots of IP addresses, active ports, and network connections. To evaluate how much time is spent online, record bookmarks, open tabs, and browser history. Keep track of communications, chat logs, and important incident artifacts, including alarms or error messages. Provide console output, timestamps, and screenshots of the logs to create a chronological timeline of occurrences. Record file-related metadata, important user actions, and any security alerts or warnings. Documentation of user account details, such as usernames and permissions, is also necessary. [2]

1. **The significance of recording a computer’s time offset.**

Recording a computer's time offset is essential, especially when the computers in question might not be synchronized with "real" time. To create precise event timelines, time offsets must be calculated and recorded. Reconstructing the flow of events, assigning actions to users, and supplying a trustworthy chronological foundation for court cases are all made possible with the use of this data. It is stressed that to prevent losing the offset data, this operation must be completed before the machine is turned off. Investigators can improve the accuracy of forensic analysis and the comprehension of temporal features in the context of a cyber incident by being aware of and documenting time offsets, which preserves the integrity of digital evidence. [3]

1. **Three best practices in collecting digital evidence from a computer's memory and hard drive.**

To maintain integrity, digital evidence must be carefully gathered from a computer's memory and hard disk. Data in volatile memory should be captured first since it is subject to sudden changes and could be deleted if the system is shut down. Reduce how much you interact with the system to prevent changing volatile data. To ensure the preservation of original data and enable hash verification to verify data integrity, make forensic pictures for non-volatile data using specialized tools. Keep thorough records of all dates, times, locations, tools used, and observations made during the procedure. To guarantee that gathered evidence is admissible in court, clearly define the chain of custody for each item. The dependability and legitimacy of digital evidence gathered from a computer's memory and hard drive are increased when these best practices are followed. [4]

1. **Three high-level requirements for ediscovery.**

There are three fundamental needs for eDiscovery. These are:

***Defensibility and Legal Compliance:*** Procedures for eDiscovery must abide by legal constraints and norms. Maintaining adherence to pertinent laws, regulations, and court rules is essential to the process's defendability. This entails being aware of and abiding by the Federal Rules of Civil Procedure (FRCP) and other relevant legal frameworks' procedures.

***Data Gathering and Preservation:*** It is essential to preserve electronically stored information that may be relevant. Organizations need to have plans in place for locating, protecting, and gathering ESI while preserving the data's authenticity and integrity. This entails putting data under legal hold, stopping data spoliation, and using forensic methods to gather data in a way that adheres to forensic best practices.

***Effective Data Review and Processing:*** Effectively handling and processing massive amounts of electronic data is essential. The review process is streamlined by employing cutting-edge eDiscovery technologies and tools for data culling, deduplication, and early case assessment. By ensuring that legal teams can concentrate on pertinent material, this criterion helps them save time and money. [5]

1. **Three best practices to follow when interviewing witnesses.**

Several best practices are helpful in ensuring the efficacy and legitimacy of the investigative process when interviewing witnesses. In order to preserve credibility, a thorough preparation is necessary, requiring in-depth knowledge about the occurrence and specifics about the witness. A welcoming atmosphere is created by starting the conversation with appropriate introductions, defining authority, and highlighting voluntariness. It's critical to ensure the interviewee is comfortable, treat them with respect and dignity, and adopt a non-intimidating manner. Creating a well-organized outline helps keep the focus on the objectives of the investigation, and being flexible in the interview process and attending to the witness's demands improves efficacy. Gaining trustworthy information requires being able to communicate plainly by avoiding investigative jargon, letting the witness talk freely while maintaining control, and carefully listening. Furthermore, it is stressed to present a professional image by dressing appropriately, since this fosters respect, improves perceptions, and could influence the interview's result. In the context of an investigation or judicial proceeding, these collective norms establish a framework for carrying out in-depth and courteous witness interviews. [6]

1. **Three best practices to follow when testifying as an expert witness.**

***1.*** ***Dynamic Communication:*** Communicate dynamically by paying close attention to what others are saying, selecting your words wisely, and observing how the audience responds. Tess Neal of Arizona State University highlights the need of control and accuracy in responses. Expert testimony is more persuasive when this strategy is used during both direct and cross-examination.

***2.*** ***Good Body Language:*** Use open and receptive body language to communicate positivity. Make eye contact without being frightening, stay away from defensive stances like crossed arms, and utilize affirming gestures. Stanley L. Brodsky emphasizes the importance of eye contact and contends that making effective use of it in testifying requires awareness of it. Retaining a laid-back manner and speaking more slowly during testifying enhances ease and participation.

***3.* *Avoid Overconfidence:***Maintain a healthy mix between assurance and modesty. Although confidence fosters trust, excessive confidence may be interpreted unfavourably. When giving testimony, steer clear of absolutes and use qualifiers like "often" or "in some cases." Cite reliable sources and make it obvious that your thoughts are based on your experience. This subtle method guarantees the expert's testimony is regarded with credibility and improves believability.[7]

**References:**

1. <https://www.ojp.gov/ncjrs/virtual-library/abstracts/bringing-crime-scene-life>2. <https://www.adfsolutions.com/news/4-key-considerations-for-using-screenshots-in-digital-forensic-investigations#:~:text=There%20are%20several%20strong%20use,be%20relevant%20to%20a%20case>.3. <https://jaimelightfoot.com/blog/comptia-security-digital-forensics/#:~:text=Time%20Offsets&text=The%20computers%20in%20question%20might,might%20lose%20the%20offset%20data>.

4. <https://www.adfsolutions.com/news/5-tips-for-collecting-digital-evidence-properly>

5. <https://www.druva.com/glossary/what-is-ediscovery-definition-and-related-faqs>

6. <https://www.legaltranscriptionservice.com/blog/8-expert-tips-on-conducting-witness-interviews/>

7. <https://careercatalyst.asu.edu/newsroom/career/four-best-practices-for-effective-expert-testimony/>