**Vijayamurugan Saravanan**

**A20563170**

**Cyber Forensics**

**ITMS 538**

**Project Part 1: Preparing for a Digital Forensic Investigation**

**Scenario**

Your manager has just scheduled a meeting with an important prospective client, and she has asked you to be part of the team that is preparing for the meeting. The prospective client is Brendan Oliver, a well-known celebrity. Last night, Mr. Oliver’s public relations team discovered that someone obtained three photos that were shot on his smartphone and tried to sell the photos to the media. Due to the sensitive nature of the photos, Mr. Oliver and his team have not yet contacted law enforcement. They would like to know if D&B can provide any guidance or support related to the investigation—or, at the very least, if D&B can help them prevent similar incidents from occurring in the future.

At this time, they do not know how the photos were acquired. The public relations team is wondering if a friend, family member, or employee could have gained direct access to Mr. Oliver’s phone and obtained the photos that way, although the phone is usually locked with a passcode when Mr. Oliver is not using it. In addition, Mr. Oliver emailed the photos to one other person several months ago. He has not spoken with that person in the last few weeks, but he does not believe that person would have shared the photos with anyone else.

Your manager plans to use this initial meeting with Mr. Oliver and his public relations team to establish rapport, learn more about the case, and demonstrate the firm’s expertise. The company sees this as an opportunity to build future business, regardless of whether they are retained to help with the investigation of this case.

**Discussion :**

1. What is the nature of the alleged crime, and how does the nature of the crime influence a prospective investigation?

* The nature of the alleged crime is the unauthorized acquisition of three photos from Mr. Brenden Oliver’s smartphone to sell these photos online. Prospective investigation can be influenced in several ways:
* Since it involves a smartphone, it focuses on digital forensics where investigating the device for any signs of unauthorized access, or malware along with how the device was compromised and identifying potential vulnerabilities are needed to understand how the image was accessed.
* Tracing communication channels is necessary to determine the origin of the attempt to sell the images to the media. Examining any emails, messages, or other correspondence about the sale of the pictures is part of this.
* To find out if any of them had direct access to the phone or if they might have unintentionally shared the pictures, interviews with Mr. Oliver's friends, family, and coworkers are crucial.

1. Based on the limited information provided in the scenario, what is the rationale for launching an investigation that uses computer forensic activities? Would D&B and/or law enforcement need additional information to determine if they should proceed with an investigation? Why or why not?

* The sensitive nature of the stated crime—the unapproved acquisition of images from Brendan Oliver's smartphone—justifies the opening of an inquiry that includes computer forensic activities. In this situation, computer forensics is essential for a few reasons:
* Computer Forensics could allow for a detailed examination of Mr. Oliver's smartphone and can uncover any evidence or digital traces that may indicate how the image was obtained. It can also determine if there were any breaches in security, if the phone was physically compromised, or if any vulnerability that allowed unauthorized access.
* D&B and/or law enforcement would likely need additional information to determine if they should proceed with the investigation. This may include:
* A more precise timeline of the event and security measures in place on Mr. Oliver's smartphone, such as the type of passcode used, any biometric authentication, or other security features is also needed.

1. What would you share with the client about how investigators prepare for and conduct a computer forensics investigation? Identify three to five key points that are most relevant to this case.

* Investigators will take measures to ensure that the data on Mr. Oliver's smartphone remains unchanged during the investigation. Create forensic copies of relevant data to avoid contamination or loss.
* Investigators will seek relevant information, such as additional details on recent interactions, the recipient of the emailed photos, and any other contextual information that could aid in the investigation.
* Examining security features, passcodes, and any biometric authentication methods. The goal is to identify any vulnerabilities or unauthorized access points that may have contributed to the incident.
* Emails, texts, and any other digital correspondence on the endeavor to sell the images will be examined. This procedure aids in locating possible participants and the source of the unlawful distribution.

1. What sources of evidence would investigators likely examine in this case? Provide concrete examples and explain your rationale.

* **Mobile Forensics:**
* Examples: Mr. Oliver's smartphone
* Rationale: The smartphone is the primary source of the alleged crime. Investigators would conduct a comprehensive examination of the device using forensic tools to extract data, including photos, call logs, text messages, app usage, and any other relevant information.
* **Access Logs and Security Settings:**
* Examples: Smartphone access logs, security settings
* Rationale: Examining access logs helps reconstruct a timeline of when the smartphone was accessed. Investigators would analyze security settings, passcodes, and biometric authentication methods to identify any vulnerabilities or unauthorized access points that could have been exploited.
* **Communication Records:**
* Examples: Email accounts, messaging apps
* Rationale: Tracing communication channels is crucial. Investigators would examine email accounts associated with Mr. Oliver, looking for any messages related to the attempt to sell the photos.

1. What should the client, investigators, and others do—or not do—to ensure that evidence could be used in a court of law? Using layman’s terms, explain laws and legal concepts that should be taken into account during the collection, analysis, and presentation of evidence.

* **Preservation of Evidence:**
* **Do:** Preserve the integrity of any potential evidence. Avoid altering, deleting, or tampering with data on Mr. Oliver's smartphone or any related communication channels. Make forensic copies to ensure that the original evidence remains unchanged.
* **Why:** Courts require evidence to be authentic and unaltered. Tampering with or mishandling evidence can raise doubts about its credibility.
* **Admissibility Rules:**
* **Do:** Follow legal procedures and rules for evidence admissibility. Ensure that the evidence was obtained legally and ethically.
* **Do Not:** Collect evidence through illegal means, such as unauthorized access to private accounts or hacking.
* **Why:** Illegally obtained evidence may be deemed inadmissible in court, and its use could lead to legal consequences.
* **Expert Testimony:**
* Do: Seek expert testimony when presenting technical evidence. Experts can explain complex concepts to the court.
* Why: In cases involving digital evidence, having an expert testify helps the court understand the technical aspects and lends credibility to the evidence.
* **Documentation:**
* Do: Maintain thorough documentation of the investigative process, findings, and any challenges faced.
* Why: Courts rely on clear documentation to understand how evidence was collected, analyzed, and preserved. Well-documented procedures enhance the reliability of the evidence.

1. What questions and concerns do you think the client will have?

* The client could ask the forensic investigator if more details about how the photos were accessed without authorization could be provided to him.
* The potential impact of this incident on the client's reputation?
* Is it possible to identify who was responsible for obtaining and attempting to sell the photos?
* The client may question whether the sensitive information remains confidential throughout the investigation.
* What is the expected timeline for the investigation, and how will the clients be updated on its progress?
* Should we involve law enforcement in this matter, and what are the implications?
* What security measures can be implemented to prevent similar incidents in the future?

1. What questions should the team ask the client to learn more about the case and determine the next steps?

* What are the client's primary goals or desired outcomes from the investigation?
* Are there specific objectives or milestones that Mr. Oliver hopes to achieve through this process?
* How does Mr. Oliver plan to address the incident publicly, if at all?
* Has Mr. Oliver consulted with legal counsel regarding the incident?
* Are there specific legal concerns or considerations that the team should be aware of during the investigation?
* How did Mr. Oliver become aware of the attempt to sell the photos to the media?
  + Is there any information on the individuals or entities involved in this attempt?
* Are there any individuals or groups that Mr. Oliver suspects might be involved in this incident?
* What specific details can you provide about the sensitive photos that were obtained without authorization?
* Can you share any information about the content or context of the photos that might be relevant to the investigation?
* What security measures are currently in place on Mr. Oliver's smartphone and other digital devices?
* Has there been any recent change or update to the security settings or passwords?