SOFTWARICA COLLEGE OF IT AND E COMMERCE

DILLIBAZAR, KATHMANDU

ST4060CEM DIGITAL FORENSIC FUNDAMENTALS

SUBMITTED BY: PRABESH KUMAR YADAV

STUDENT ID: 220394

SUBMITTED TO:

MANOJ BHUSAL

A scenario

You are a digital forensics investigator assigned to investigate a cyber-attack on a local business. The company has reported that its computer systems were hacked, and sensitive customer information was stolen. As a digital forensics' investigator, your job is to identify and analyze the digital evidence related to the crime.

Using your knowledge of digital forensics, describe the steps you would take to identify and analyze the digital evidence in this case. Be sure to address the following questions:

Question1.What tools and techniques would you use to collect digital evidence from the affected systems?

Answer: Several technologies and procedures are utilized to gather digital evidence from impacted systems. To gather digital evidence, I would employ a variety of techniques, including:

1.Bit streaming tools (FTK Imager)

2.Hashing tools

3.Memory analysis tools

4. File carving tools

Question2.How would you ensure that the evidence you collect is admissible in court?

Answer:

I would ensure that the digital evidence I collected from the crime site in court in different ways. First I would be sure to click some photos of all the digital evidence in the place where the crime was committed and then in the office to make sure. And then I would a simple forensics report that could be readable and understandable by anyone in court. But before submitting the digital evidence, it should not be changed in any way including meta data of the evidence, to maintain integrity of such evidence I would always make one replica or bit streaming image of it and generate a hash of the digital evidence and keep backup of evidence safely.

Question3. What type of digital evidence would you expect to find in this case, and how would you analyze it to determine who was responsible for the cyber-attack?

Answer: At first, after I get in the site, In a cyber-attack investigation, digital evidence such as log files, network traffic data, system configuration files, malware samples, email headers, and user account information may be collected. Analysis techniques such as data recovery, file carving, metadata analysis, timeline analysis, and pattern recognition would be used to examine the evidence. Malware analysis would involve studying the code, behavior, and signatures of the malware samples, while network traffic data would be analyzed to identify attack source and vectors. Correlating evidence, identifying patterns, and conducting link analysis would help establish a timeline of events and determine the responsible party, following established digital forensic investigation methodologies and best practices.

Question4. How would you ensure the security and integrity of the digital evidence throughout the investigation process?

Answer: Digital evidence should be handled with care, stored securely, and tracked with proper chain of custody procedures. Forensic images should be created using write-protected tools, and original media should be preserved. Hashing or checksums should be generated and documented to ensure evidence integrity.

Access control and authentication measures should be implemented to restrict unauthorized access. Detailed documentation of all investigation actions should be maintained, including tools used, parameters, and changes made to evidence. Logging and auditing mechanisms should be implemented. Encryption and protection against malware should be in place to safeguard the evidence's integrity and confidentiality.

Question5. What steps would you take to document and report your findings to the relevant authorities?

Answer: Documenting and reporting findings in digital forensic investigations is critical. Steps include detailed documentation of actions, findings, and analysis results, including tools used and changes made. And the findings should be presented in a clear, concise, standardized format with relevant information. Maintaining a chain of custody to establish evidence integrity is important, as is compliance with legal requirements, such as privacy and data protection. Reports should be securely transmitted to relevant authorities with proper authentication measures. Digital forensic examiners may need to provide expert testimony in court or presentations to relevant parties. Confidentiality and security measures should be followed throughout the process to protect the integrity and confidentiality of the findings and evidence.