PES1UG20S581
ROHITH H
J SEC

DIGITAL FORENSICS CASE STUDY ASSIGNMENT

CASE -01

Jonathan Simpson owns a construction company. One day a subcontractor calls him, saying that he needs a replacement check for the job he completed at 1437 West Maple Avenue. Jonathan looks up the job on his accounting program and agrees to reissue the check for $12,750. The subcontractor says that the original check was for only $10,750. Jonathan looks around the office but can't find the company check book or ledger. Only one other person has access to the Jonathan calls you to investigate. How would you proceed? Write a one-page report detailing the steps Jonathan needs to take to gather the necessary evidence and protect his company.

Answer:

Objectives:

The objective of this is to find out from which end the problem is occurred and who is the main culprit of the check issue and who is the one who had created this problem and where the error has occurred and what might be the possible

Or the potential reason for this issue and what might be the reason for the missing of the ledger in the company and who is the other person and what might be the reason for that and what have happened in the managing the account of the company.

Evidences Analysed:

- *Ledger book*
- *Account details*
- *Phone logs*
- *Checks*

PES1UG20S581
ROHITH H
J SEC

DIGITAL FORENSICS CASE STUDY ASSIGNMENT

- *Details of all the users in the system*
- *Jonathan Simpson computer with the hard disk containing the data of all the company accounts and details of all the transactions.*
- *Capturing all the digital forensics steps which involves copying all the data from the user computer and the mobile phone and the copying all the data including the deleted files and the unallocated storage in the disks and which may potentially may be the main reason for investigating the case.*

Investigating steps:

As a Investigator I would have tried to gather all the information of the worker and the check issued place and the work which was completed at the 1437 venue and try to collect all the information which would necessarily needed for the investigation process and tried to collect all the info from the nearby them to have a clear understanding and to have more info which might lead to the closer step to complete the investigation process and helps to find what happened exactly there.

Once we had the information on the our side we will try to investigate the internal members of the office and find all the persons who had the access to the Jonathan ledger book and the staff who are working under him

Then we have to investigate in the other way also and find out the reason for the failure of the check and why this happened and why for this check and to whom and all he called and where and all he travelled and whom and all he met.

the Jonathan should conduct an internal investigation to determine who else may have had access to the company checkbook and ledger. He should gather any relevant information such as security logs, computer activity logs, and any other records that may be relevant.

PES1UG20S581
ROHITH H
J SEC

DIGITAL FORENSICS CASE STUDY ASSIGNMENT

Jonathan should also check the bank records to see if the check was cashed or deposited, if so he should obtain copies of the check and deposit slip. This will help to determine if the check was altered or if it was an authorized transaction.

Jonathan should also conduct interviews with any employees or subcontractors who may have had access to the company checkbook and ledger. During these interviews, he should ask about any suspicious activity or behavior that may be related to the missing check.

Once all of this information has been gathered, Jonathan should analyze the evidence and make a determination about what happened to the check. This may include identifying any potential suspects, determining if any laws were broken, and making recommendations for future security measures.

To protect his company, Jonathan should also take steps to implement new security measures to prevent similar incidents from happening in the future. This may include implementing new security protocols, such as requiring multiple levels of approval for check issuance, implementing strict access controls for company financial records, and conducting regular internal audits.

Findings:

The potential findings are the

Find the missing check which was altered

The transactions which are unauthorized

The main culprit or the suspect in the case

The not proper functional of the security in the agency or the company.

Conclusion:

We have to gather the necessary evidence and protect his company, Jonathan should take several steps. This includes gathering as much information as

PES1UG20S581
ROHITH H
J SEC

DIGITAL FORENSICS CASE STUDY ASSIGNMENT

possible about the situation, conducting an internal investigation, checking bank records, conducting interviews, analysing the evidence, making a determination about what happened to the check, implementing new security measures, and documenting the entire process. By taking these steps, Jonathan can identify the cause of the missing check and take steps to prevent similar incidents from happening in the future. Additionally, by maintaining the evidence in a secure location, it can be used as reference in case the case is taken to court.

CASE-02:

You are the digital forensics investigator for a law firm. The firm acquired a new client, a young woman who was fired from her job for inappropriate files discovered on her computer. She swears she never accessed the files. What questions should you ask and how should you proceed? Write a one- to two-page report describing the computer the client used, who else had access to it, and any other relevant facts that should be investigated.

Answer:

Objectives:

The objective of the above question is to determine the cause of the inappropriate files found on the client's computer, as the client claims to have not accessed the files. The digital forensics investigator is asked to gather information about the computer, who had access to it, and any other relevant facts that should be investigated in order to determine how the files got onto the computer and who is responsible for it. The report will detail the steps and the findings of the investigation to provide evidence in the case and to help the law firm make a decision.

PES1UG20S581
ROHITH H
J SEC

DIGITAL FORENSICS CASE STUDY ASSIGNMENT

Evidences Analysed:

- *Computer file system to analyse the file in the client system*
- *Network logs to check whether any other person has accessed the computer remotely.*
- *Interviews with the client and the other IT staffs working in the company*
- *User activity to analyse how the user was during the job period*
- *Computer activity such as any malware is found in the computer of the client and check the browsing history and the emails and etc*
- *Hardware evidences: to gather the information of the physical devices that are used to store the info or the data that is pen drives and to check whether any tampering is done to them.*

Investigating steps:

Initial assessment: The investigator will first gather information about the computer in question, including its make and model, operating system, and any relevant software that is installed.

Collecting all the data required: The investigator will make a forensic image of the computer's hard drive to preserve the original state of the data. This will allow the investigator that is me to examine the data without altering the original data in the client system. Analysing the data found: The investigator will analyze the data collected, including the file system, network logs, and user activity, to identify any relevant information. The investigator will also check for malware and other malicious software.

PES1UG20S581
ROHITH H
J SEC

DIGITAL FORENSICS CASE STUDY ASSIGNMENT

Interviews: The investigator will conduct interviews with the client, as well as any relevant parties such as co-workers or IT staff, to gather additional information .Report preparation: The investigator will prepare a report detailing the steps taken during the investigation and the findings. This report will be used to present the evidence to the law firm. Presentation: The investigator will present the report and findings to the law firm and answer any questions they may have. Preservation of evidence: The investigator will ensure that all evidence is properly preserved and stored in case it needs to be used in court.

Conclusion:

The conclusion for the above case we have to analyse and come out with the conclusion that who has actually made this and why is the files present in the client computer and who is the one who actually did that and the purpose of the file present on her computer and what might be the potential reason to actually fire her is this actually done by her or is it done by the other person who is in the company premises or is it done by remotely accessing the client computer and finally produces all the evidences and the report of the case and have a video proof of the investigation process to show that the actual files are not tampered and all the task or the process done on the copied files from the client.