Free research paper on plan for processing a potential crime scene

Law, Evidence

Plan for Processing a Potential Crime Scene

Identifying the Potential Digital Evidence

Processing a crime scene will involve following standard procedures used in assessing a digital crime scene. According to Wile and Reyes (2011), the process of identifying the potential digital evidence will require a series of investigations to be done. Thus, this will involve assessment of the case, asking the affected parties questions, locating the evidence and documenting the results with the goal of identifying where the crime was exactly committed. In this case, the first clue to potential evidence will be to assess the intrusion detection logs. Additionally, it is important to note that network intrusions may also come from employees within the same local network (Shinder and Tittel, 2002). Thus, the strange email from the Human Resources will have to be identified as evidence as it caused the HCC database administrator to act in a strange way and more to that it was benefits attachment document that was blank.

Preparation for Searching the Evidence

Preparations will require the team to have the necessary tool kits for assessing the network intrusion. Further, potential areas for evidence collection will be identified. According to the Ec-council (2009), when searching for evidence, one of the approaches for searching involves assessing the attack of the computer workstation and other intermediate computers. This evidence can be in the form of files, logs, tools, and ambient data. Further, the computer of the HCC database administrator will also be searched and the logs, files, configuration files, and remainders of Trojaned files such as the benefits attachment retrieved (Ec-Council, 2009). In addition, the firewalls of the system will have to be assessed to see if they were compromised by the benefits attachment and if so the firewall logs will be treated as evidence.

Steps in Seizing Digital Evidence

Seizing the digital evidence will require strict procedures to be followed. This is because the collection of digital evidence is expensive and any compromise in the collection process may damage the evidence, which may not be available for reuse (Vacca, 2005).

The first step will be to separate the evidence from other unnecessary data. This will require recognizing the workstation of the HCC administrator as the crime scene and establish where the email was sent from in the local network. This will assist in developing the best approach in retrieving and storing any evidence stored. The second step will require the preservation of the evidence collected. Precaution will be observed to ensure that the evidence remains in its original state. In cases any changes are made, documentation will be necessary and reasons for the alterations given. The third step will involve the developing of a list of volatility of the evidence. This will guide in knowing how to gather the evidence identified and will minimize chances of corrupting the evidence (Vacca, 2005). The fourth step will be to ensure that chances of external are attacks to the system are eliminated. This will prevent tampering of the evidence to be collected. Once these steps have been followed strictly, evidence will be seized applying recommended tools for evidence collection.

Documentation Processes to Support any Potential Legal Proceedings

The documentation processes begins from the time of arrival at the scene and is continuous up to the final reporting. The forms of documentation to be used will be photographic documentation and written documentation (Sheetz, 2007). Once at the scene, the first step will be to take photographs of the workstation arrangement in the HCC database administrator’s office. This will be important in providing information on the arrangement of the system setup if required by a court of law. Further, presence of such photographs will aid in reconstructing the scene. Labeling of all details such as wires, cables and other devices is significant. According to Sheetz (2007), this will aid in establishing the purpose of each cable and components of the workstation area. This provides the legal team an understanding of how a given computer environment functions. Since evidence will be collected when the system is, still running, step-by-step documentation will be done to assist in the reconstruction of the original state of the system at the time of evidence collection. Small alterations such as the movement of a mouse will be documented. In addition, a sketch representation of the scene will be done to act as an aid in understanding the photographs that were taken of the scene. Measurements on the sketches will be necessary to assist the litigators in constructing the crime scene. The documentation process will also be aided by the use of tools that have an in-built documentation system that record every action done during the gathering and acquiring of data. Moreover, the documents containing the description of the investigators experience will be of importance to a court of law in establishing the validity of the work or evidence provided (Sheetz, 2007).

Ensuring Chain of Evidences Processes

Ensuring the chain of evidence processes is followed will require few people to handle the evidence. In case the evidence will have to be transported to the laboratory for further analysis, the technician receiving the evidence will have to document the status of the evidence prior to transportation from the crime scene and the state it arrives in at the laboratory. This will be used to establish accountability in case the evidence is tampered (Shinder and Tittel, 2002).

Processing the Database Administrator’s Computer

Steps in Imaging the Drive

Imaging will be done using the FTK tool. This will assist in creating an evidence disk (Lewis, 2007).

FTK Imaging

- An evidence disk will be created by inserting a sanitized USB thumb drive into the administrator’s system. Then, a text file will be created using a notepad to include the name of the investigator.
- The FTK program will be installed in the thumb drive. According to Carvey and Kolde (2012), installing the FTK imager on a USB thumb drive provides the required storage space for acquired images and files. Once installed, the FTK image icon is double clicked to launch the program
- Next step will involve the selection of the image drive, which will provide

the option for selecting the local drive.

- The desired drive in the system where the evidence is to be extracted is selected.

- Then the desired image parameters are selected on the dialogue box that will appear. Then the next button is selected

- Verification of the summary image information is carried out to ensure they are correct. This will involve ensuring that the source, destination, and summary file information are all correct (Lewis, 2007).

- After this, the drive image process will start and when finished the dialogue box will be closed.

- The two files created in the destination folder, a text file, and the image file need to be stored on a sanitized drive or partition to prevent them from being contaminated.

Analyzing the image

Analysis of the image will be done using the FTK imager tool. After launching the FTK program, the option for starting a new case will be selected. Then when the new case wizard dialogue box emerges, it will be filled as per the required fields. This will include the investigators name, case number, case name, and the case path. Different case log options will be selected. In this case, the default settings will be selected. Additionally, different processes such as the MD5 hash tag function that can be performed using the FTL imager will be selected. In the refine case default dialogue box, the default selections will not be changed. Following the refine case default, the next dialogue box that appears will be the refine index where the default selections are left unchanged. In the adding evidence dialogue box, the option for acquired image of the drive is selected. The next button will be clicked and then press the finish button to begin processing the image file. Once the analysis is complete, a report will be generated by the imager, which can be used to view all the activities that were done on the drive. Potential areas analyzed in the system will be the memory usage and registry.

Network Analysis

Network analysis will be carried to determine the network traffic that occurred during the intrusion incident (Fichera and Bolt, 2012). Prior to this, the investigating team will familiarize themselves with the network environment to increase understanding of the physical and logical topology of the network.

Preserving the Evidence

It will be critical to preserve the evidence that will be collected. A number of approaches can be used in preserving digital evidence. In the preservation of the evidence, duplication and authentication will need to be observed (Mohay, 2003). According to Casey (2011), it will be important to place the database administrator’s computer system and the storage media in a secure storage for future use. Secondly, only the information that will contain evidence will be extracted. This will include memory logs and registry logs. According to Baggili (2011), log records contain a significant amount of information, which is normally used in evidence collection. Thirdly, all material from the database administrators system will have to be saved in an image format. Since the HCC organization is a top health care organization, which has a very large database, it will be more practical to extract specific data from the server.

It will be significant to filter out irrelevant and confidential data while analyzing the evidence. This process will involve the elimination of valid system files that have no bearing on the investigation. More time will be spent analyzing most user created data (Casey, 2011).

Processing the Database Server

The storage of data in the database ensures that no modifications can be made. The only probable action is to add information. According to Pavlou and Snodgrass (2008), this makes it easy to determine if the database is compromised. The process of acquiring the image from the server will have a similar approach to that of acquiring the image from the computer system, but with a few changes as will be outlined in the steps indicated

- An evidence disk will be created by inserting a sanitized USB thumb drive into the Windows Server 2003 system. Since it is a server, that contains a large volume of data, a sanitized 16-GB thumb drive will be used.
- The FTK program will be installed in the thumb drive. According to Carvey and Kolde (2012), installing the FTK imager on a USB thumb drive provides the required storage space for acquired images and files. Once installed, the FTK image icon is double clicked to launch the program
- Next step will involve the selection of the image drive, which will provide the option for selecting the local drive on the server.
- The desired drive in the system where the evidence is to be extracted is

selected.

- Then the desired image parameters are selected on the dialogue box that will appear. Then the next button is selected
- Verification of the summary image information is carried out to ensure they are correct. This will involve ensuring that the source, destination, and summary file information are all correct (Lewis, 2007).
- After this, the drive image process will start and when finished the dialogue box will be closed. The image can be stored in a variety of formats (Olivier and Shenoi, 2006).

Analyzing the image

Analysis of the image will be done using the FTK imager tool. After launching the FTK program, the option for starting a new case will be selected. Then when the new case wizard dialogue box emerges, it will be filled as per the required fields. This will include the investigators name, case number, case name, and the case path. Different case log options will be selected. In this case, the default settings will be selected. To reduce the data tampering the MD5 hash tag will be selected to ensure data integrity of the evidence is maintained. In the refine case default dialogue box, the default selections will not be changed. After selecting the options in the refine case default, the next dialogue box that appears will be the refine index where the default selections are left unchanged. In the adding evidence dialogue box, the option for acquired image of drive is selected. The next button will be clicked and then press the finish button to begin processing the image file. Once the analysis is complete, a report will be generated by the imager, which can be used to view all the activities that were done on the drive.

Additionally, after launching the FTK imager, the capture memory icon will be used to obtain data about the memory usage of the server (Anson, 2012). The capture memory icon will be used to save the RAM dump on the thumb drive. Analysis of RAM dump saved on the thumb drive will be used to reveal any compromise in the RAM. Further, analyzing the windows rrregistry of the server will help in tracking the location of any malicious activities on the server (Carvey, 2011).

Best Practices for Acquiring the Evidence

Investigations involving data collection are repeatedly several times to ensure that a valid decision can be made. Acquiring of evidence from a server that is still running is such a risky move, which if compromised can result in comprising the entire evidence (Adelstein, 2006). One of the keys ways to ensure that evidence is not compromised is to ensure that all the executable files for gathering the evidence will be from the investigators thumb drive. This is the case when using the FTK imager. To maintain the evidence in its original state, hashing is done. Secure hashes executed by the FTK imager include MD5 and the SHA-1 (Adelstein, 2006).

Risks that need to be observed in analyzing a live server system

During the live forensic analysis of the server, it will be important to appreciate that Trojan horse backdoor tools can exist in the system. According to Carrier (2006), Trojan horses are a very common source for creating false data. These activities by the Trojan horses can be eliminated by using tools that are complied statically to ensure they do not use the Trojan libraries. The Trojan horse in this case uses dynamic libraries.

Steps Taken in Documentation

Digital crimes, just like physical crimes have strategic steps that must be taken in the course of investigation. The first step, upon arrival at the digital crime scene, is to preserve the evidence as it is for future analysis. This is followed by the survey phase that involves transfer of the evidence to a controlled location to ensure it is not tampered. The documentation phase involves adept and efficient documenting of the digital evidence as it is found. The last step is usually the analysis phase that involves use of specific software to determine if there are hidden or deleted files in the digital evidence (Kruse and Heiser, 2001).

While documenting the digital crime scene, the investigator and his team should use photographing as a tool of representing the digital evidence as it was. They may also use the conventional crime scene mapping to indicate the location of different types of evidence in the scene. Clear labels should accompany these. In situations where photographing or crime scene mapping is not possible, they may settle for sketching to enable them to recreate the crime scene during the analysis phase of the investigation.

In order to ensure the documentation is thorough, the investors should photograph all electronic devices in the crime scene. This includes capturing these devices in their on-state. None of the devices should be shut down until the documentation phase is complete. This may help to capture computer activity prior to the start of the investigation. All digital data that is visible should be recorded. This is especially crucial in case the forensic investigation is expected to witness in a court of law concerning the case (Vacca, 2005).

The investigator should also include events surrounding the case. This may include noting the person who reported the crime, and the exact time and date that this was done. All the investigators or employees of the firm present at the crime should also be documented. It should also be noted why these people were present at the scene and what activities they did. All persons concerned with the case such as victims, witnesses and suspects should be noted . Their exact locations at the time of the beginning of the investigation noted (Maras, 2012).

Preparation for Court Testimony

All these steps must be carried out keenly since the court usually links the admissibility of digital evidence to the method of retrieval, collection, preservation, and presentation of the digital evidence. Before the court testimony, I would prepare my team by letting them know that the court will be seeking to find if there were any anomalies in the collection of data or if there are loopholes that might have led to tampering of the digital evidence (Clarke, 2010).

Therefore, the investigators should have all the documentation sheets and their copies on the due date. They should also use these documentation sheets to recall all the events that occurred while collecting data. This should be done before the court testimony. They should make sure that they have all the facts right to prevent the opposing counsel from misleading of the investigators. They should also be composed and relax as they answer any questions thrown their way. This will reassure the court of their honesty, and hence the credibility of the evidence being submitted (Wiles, Cardwell, and Reyes, 2007).

Ethical Responsibilities

Digital forensic investigators should exercise utmost care and scrutiny in their documentation of digital evidence to ensure that this evidence will be acceptable in a court of law. The investigators have an ethical responsibility to their profession and to the users of the digital forensic information to present all the facts of the case as they were. They should not omit or twist any facts according to their liking. They ought not to be biased in their presentation of the evidence they found.

References

Adelstein, F. (2006). Live Forensics: Diagnosing your System without Killing It

First. Communications of the ACM, 49(2), 63-66.

Anson, S. (2012). Mastering Windows network forensics and investigation.

Hoboken, N. J.:

Wiley.

Baggili, I. (2011). Digital forensics and cyber crime second international ICST

conference:

ICDF2C 2010, Abu Dhabi, United Arab Emirates, October 4-6, 2010: revised

selected

papers. New York: Springer.

Carvey, H. (2011). Windows Registry Forensics Advanced Digital Forensic Analysis of the

Windows Registry.. Burlington: Elsevier Science.

Carvey, H. A., & Kolde, J. (2012). Windows forensic analysis toolkit advanced analysis

Techniques for Windows 7 (3rd Ed.). Amsterdam: Elsevier/Syngress.

Carrier, B. D. (2006). Risk of Live Digital Forensic Analysis. Communications Of

The ACM, 49(2), 56-61

Casey, E. (2011). Digital evidence and computer crime forensic science, computers and the

Internet (3rd Ed.). Burlington, MA: Academic Press.

Clarke, N. (2010). Computer Forensics A Pocket Guide. Ely: IT Governance Pub.

Ec-Council, E. (2009). Computer forensics: investigating network intrusions and cybercrime.

Clifton Park: Course Technology/Cengage Learning.

Fichera, J., & Bolt, S. (2012). Network Intrusion Analysis Methodologies, Tools, and Techniques

For Incident Analysis and Response. Burlington: Elsevier Science.

Kruse, W. G., & Heiser, J. G. (2001). Computer Forensics: Incident Response Essentials.

Boston, MA: Addison-Wesley.

Lewis, J. (2007). Corporate Computer Forensics Training System Laboratory Manual, Volume

1. Michigan: Lulu. com.

Maras, M. (2012). Computer Forensics: Cybercriminals, Laws, and Evidence.

Sudbury, Mass.:

Jones & Bartlett Learning.

Mohay, G. M. (2003). Computer and intrusion forensics. Boston: Artech

House.

Olivier, M. S., & Shenoi, S. (2006). Advances in digital forensics II IFIP

International

Conference on Digital Forensics, National Center for Forensic Science,

Orlando, Florida, January 29-February 1, 2006. New York: Springer.

Pavlou, K. E., & Snodgrass, R. T. (2008). Forensic Analysis of Database

Tampering. ACM Transactions on Database Systems, 33(4), 30: 1-30: 47

Sheetz, M. (2007). Computer forensics: an essential guide for accountants,

lawyers, and

Managers. Hoboken, N. J.: John Wiley & Sons.

Shinder, D. L., & Tittel, E. (2002). Scene of the cybercrime computer

forensics handbook.

Rockland, MA: Syngress Pub.

Vacca, J. R. (2005). Computer forensics computer crime scene

investigation (2nd Ed.).

Hingham, Mass.: Charles River Media.

Wiles, J., & Reyes, A. (2007). The best damn cybercrime and digital forensics

book period.

Rockland, Mass.: Syngress