Digital Forensic Examination

Posted on September 17, 2018

Case Scenario

The present forensic case emphasizes investigating alleged contact between Russian officials and the US. The task involves forensic analysis of a laptop and cell phone of a high-ranked US government official. Investigation reveals some evidence that confirms ongoing suspicious activities between the parties involved. Initial investigations conducted on the phone depict a text confirming a lunch meeting on a particular day (2/15/2016), while the contact list displayed a phone number with the label 'Red Ralph.' Investigations on the laptop reveal the deletion of several zipped files containing classified materials, such as a weblog showing uploading to a file-sharing site. The official report provides pieces of evidence that can help the prosecutor to solve the case and identify if something illegal is going on.

Digital Forensic Examination

A digital forensic examination is a standard methodology adopted for retrieving important information that can help the crime department in investigations. Its role became more evident in the twentieth century due to the use of technology in various criminal activities. It involves assessing computers, electronic devices and IT infrastructures used by people in suspicious activities. The process focuses on examining the devices and equipment used in data transfer. Investigation searches the system files, devices, warbles,

Recovery of deleted files, internet and cloud storage. A standardized framework to address the issue, including increasing the volume of the data. Forensic examinations are capable of revealing securely erased files and making them usable for criminal investigations. Computer forensic analysts play a vital role in revering evidence that is deliberate removes from the systems or corrupted (Garfinkel & Shelat, 2003).

Case Identifier

Case identification is part of pre-preparation involving detection and identification of incidents and vulnerabilities associated with the event under analysis. Following are the steps involved in this stage;

- Identification of preliminary assignments before reaching the scene and identifying experienced search experts (Brian & Spafford, 2003).
- Identifying the person in charge with his name and details, assigned responsibility for handling

search operation.

- Developing legal activities and the coordination plan
- Initial case assessment mentions investigators involved in performing initial investigations related to the case. The activities included asking questions related to the computer rule and evidence (O'Seomus, 2004).
- Identification of case requirements involves outlining details in a systematic manner, such as;

Case Situation

Recognizing is the case represents a violation of company policies or legal rules.

Nature of the case

It identifies if the suspicious activity is at an individual level, organizational level or associated with the person in question (Reith, Carr, & Gunsch, 2002).

Specifications

Determining the role of the person or devices in question.

1. Determining the type of devices categorized as a hard disk, floppy, CD, USB or memory card.
2. Mentioning the case number for the operating system suspected of its involvement in the criminal incident.
3. Clearly labeling the disk format as FAT16, FAT32 etc.
4. Stating the motive behind the conduction of criminal activity.
5. Determination of the resources, private or public, is mentioned in the case.
6. Identification of the submitter of the information and his involvement in the case.
7. Estimating time, resources and money involved in the examination.
8. It includes the date of receipt when the case was forwarded for investigations (Brian & Spafford, 2003).

Descriptive list

- Reporting the name of the agency and data
- Submission number or case identifier
- Date of receipt and reporting
- Identification and names of submitter, examiners and investigators
- Details of examination and collection procedures
- Items such as serial number, make and model
- Titles and names of log files

- The inclusion of specific files requested and other files, such as deleted files, that support investigations (Garfinkel & Shelat, 2003).
- The inclusion of string searches, keyword searches
- Numbers and specifications of cache files, chat logs and e-mails
- Mentioning the model used for forensic examination
- Identifying techniques of encryption, hidden attributes and file name anomalies
- Listing supporting materials, including reports, particular items on evidence, number of digital copies and custody of documentation.

The primary focus of the forensic analysts is on recovering the lost information. Through the utilization of accredited tools such as the Association of Chief Police Officers (ACPO), they search for missing pieces that could make the information meaningful. The technicians, in the process, uncover and restore damaged and deleted parts and search for traces that reveal the time of its use before deletion (Agarwal, Gupta, & Gupta, 2011).

Types Of Attempts In Erasing Files

The forensic team identifies the type of attempts involved in damaging the files.

When the data is deleted permanently from the system the forensic investigator will use commercial recovery tools. The evidence that can be useful for examinations involves contact lists, audio files, browser histories, calendars, compressed archives (RAR, Zip etc.), cookies, databases, login files and system files (Brian & Spafford, 2003).

Level	Location	Description
Level 0	Regular files	The details include file name, attributes and contents. Direct access is possible.
Level 1	Temporary files	Include browser cache files, helper applications, print spooler files and the ones sent to the recycle bin. Users think that the systems automatically delete the file.
Level 2	Deleted files	When the file is deleted operating systems do not overwrite blocks on hard disk. Traditional undelete tools are useful in recovering these files such as Norton utilities.

Level 3	Data blocks retained	Recovering data from a disc is possible; however, it does not belong to a named file. The information is in slack space storing data in virtual memory. Using the Windows format command can help in recovering data.
Level 4	Vendor-hidden blocks	Vendor-specific commands are efficient in accessing data blocks that contain the deleted files.
Level 5	Data overwrote	If the information is overwritten, retrieving it from the hard drive is still possible.

Identification Of Recovery Techniques

The second step involves the identification of the recovery technique that is most useful for forensic investigations. Identification of the recovery technique is vital in forensic examinations as it provides details about the most suitable tool for retrieving lost data. To recover hard disk information forensic investigations use tools for analyzing images obtained from different operating systems. Explorer style interface allows a reading variety of files (Garfinkel & Shelat, 2003).

Tools	Platform	Details
Drive spy [22]	DOS/ windows	Inspection of slack space and deleted files from the metadata.
Encase [21]	Windows	Featuring sophisticated drive imaging, error checking, validation and preview mode.
Forensic toolkit [23]	Windows	Preview of forensic information, graphics searches such as JPEG images and internet texts.
I look [25]	Windows	Capable of handling multiple file systems at a time. Generating hashes and filtering functionality.
Norton Utilities	Windows	Containing tools useful for recovering lost files. Examining the hard disk of the computer.
The coroner’s toolkit [26]	Unix	Collected programs used in the analysis of the retrieved data.

XWays [20]	Windows	Requires native support of FAT, CDFS and NTFS. Data cloning and imaging of the files.
TASK [24]	Unix	Operating on disk images and created with the help of dd.

A Digital Forensic Process Model

Forensic analysts explain the process of forensic investigation and also identify the steps involved in the investigation process. Depending on the nature of the case, the forensic analysts adopt the Refining Digital Forensic Process Model. The reason for choosing the model is that it provides improved specific steps for investigations. It is more effective in dealing with the laptops and mobile devices. Agarwal's model Systematical Digital Forensic Model (2011) provides an effective approach to reveal the concealed data. The model is useful as it addresses the shortcomings of the previous models (Agarwal, Gupta, & Gupta, 2011).

Phase I: Preparation

Phase one of the model is preparation occurring prior to the conduction of investigation. The step involves understanding the nature of the crime, circumstances and activities linked to the incident. The step emphasizes relating circumstances to the crime. The team adopts an appropriate strategy covering the legal and technical factors.

Phase II: securing a scene

The second step of the investigation focuses on securing the scene from unauthorized access and preserving the original evidence. Adoption of a formal protocol is more useful in this phase as it ensures that custody is followed properly. All people involved in the investigation maintain integrity and cause no harm to the data (O'Seomus, 2004).

Phase III: survey and recognition

The initial survey allows investigators to evaluate the scene and determine potential sources, leading to the formulation of an appropriate plan. Assessment of power adapter, memory card and cables remains an essential part of the phase. Evaluation of electronic types of equipment is also crucial as it helps in the identification of people and scenes (Agarwal, Gupta, & Gupta, 2011).

Phase IV: documenting the scene

The next step involves documentation of the scene that includes photographing, sketching and mapping of the crime scene. Investigators generate photographic evidence of the devices, power adapters, cradles and accessories. Graphical record allows recreating the scene and using it for in-depth analysis. Date and time related to the incident are also documented (Agarwal, Gupta, & Gupta, 2011).

Phase V: communication shielding

The step blocks the option of possible communications even if the devices appear in off-state mode. The purpose is to secure the information and eliminate the chances of overwriting.

Phase VI: evidence collection

It involves a collection of;

Volatile evidence

Mobile devices are volatile in nature and exist in ROM. To save the information, an efficient solution is to replace the power adapter or recharging. Installation of malicious software also remains part of the investigations (Garfinkel & Shelat, 2003).

Non-volatile evidence

It focuses on a collection of information from external storage supported by various devices, including compact flash cards, memory sticks and USB. The selection of useful forensic tools helps in presenting the evidence in court. Mechanisms such as hashing and write protection are used to authenticate the evidence collected. It is also vital to view the evidence that is of a non-electronic nature, including passwords and hardware manuals (Agarwal, Gupta, & Gupta, 2011).

Phase VII: preservation

The investigation team adopts adequate procedures that ensure that the movement of evidence does not destroy the devices. Proper labeling of all potential sources is crucial in this phase. Radiofrequency isolation is used to keep the evidence bag safe and prevent further communications.

Phase VIII: the examination

The phase is most technical as it involves examining the evidence and the content obtained from investigations. An appropriate strategy is to create multiple backups and convert evidence to manageable sizes. Filtration of data, validation and matching of patterns remains part of the phase. Attempts for system tampering and deletion are highlighted (Agarwal, Gupta, & Gupta, 2011).

Phase IX: analysis

Conduction of technical review and teams of experts analyze the evidence for uncovering useful information. It involves the identification of an association between fragments of information. Timeframe analysis is the most efficient solution, leading to sound results. File analysis is conducted for the extraction of data. Documenting results is the final part of the phase.

Phase X: presentation

Presenting results is the next step of the phase, starting after the extraction of the information. The presentation involves appropriate corporate management, as it is possible to discard and allege a particular crime. Presenting a report is important as it contains a detailed summary of the steps involved in the examination and inquiry (Garfinkel & Shelat, 2003). The features of the good report include;

- Use of proper grammar and readable language
- The absence of errors or ambiguities that make the report unreadable
- Explaining results in brief with a focus on central information
- Including details of log files generated by forensic tools
- Enhances chances of convincing the jury, thus leading to a winning situation

Phase XI: results and review

Reviewing results is a crucial step of the examinations as it leads to sound details regarding the suspicious event. It involves interpretation and evaluation of the results obtained throughout the examination process. The information is helpful in identifying the nature of a crime and finding the involved persons (Agarwal, Gupta, & Gupta, 2011). The process involves;

- Review of the process and investigation techniques
- Collection and preservation of information associated with the incident
- Eradication of system information and prevention of crimes

Results

Results of the forensic investigation are presented in a comprehensive report format that provides clear details about the case. The report includes a description of the activities involved throughout the investigation process. The results lead to the formulation of opinions that help in the resolution of the case. Results of the digital forensic investigation depict the need for guidance that helps experts perform investigations with integrity and present evidence collected under the adoption of the forensic model. The selection of the digital forensic process model suggested by Agarwal helps in retrieving lost files from the metadata. The team looked for specific clues to detect the suspicious files helping in performing cluster comparisons. Handling huge amounts of data provided by the forensic teams is often daunting. To overcome the problem, an appropriate strategy involves determining suspicions associated with the file names, paths, size, extensions, fragmentation, hash codes and status. Evaluation of the contents reveals the clues that are useful for the investigation. Automated analysis of suspiciousness is more efficient for generating consistent valuations compared to manual analysis. Through metadata, the analysis provides more sophisticated methods for inquiring, but these are rare in criminal investigations. Suspicion determined through forensic examinations involved two types; anomalousness that focuses on determining the degree of object variation from its norm (Buchholz & Spafford, 2004). The second type includes deceptiveness indicating a degree of perceiving facts other than the truth. Deceptiveness is more common in concealing information or hiding facts. In forensic investigations, the measurement of anomalousness depends on comparing statistics in the drive.

The Main Findings Of The Investigation Reflect:

- One copy containing at least 200 images across 100 files.
- Drives are purchased and classified differently for computer disks and portable devices.
- The metadata revealed the file path, name, size and MAC times with NTS flags depicting information about encrypted, compressed, and empty.
- The total files exposed were at least 80000, while 2000 displayed unique paths.
- Among the collected files, 30 percent were unallocated or marked under the deletion category. Other 70 percent had the label of orphans. The discerning file name was not possible without information on the corresponding path.
- File carving was used to find the files that lost their metadata entirely.
- Correction of the file path names helped in marking useful files in so many deleted files from the data repository.
- Assigning files to semantically meaningful groups such as pictures, word documents and spreadsheets was useful in data classification.
- Searching parent directories for the meaningless immediate directories allowed mapping files into groups under expert system methodology. Searching extension names and different terms of software on the web also proves a great help.

- Matching the extensions and the directory names permits filtering and getting rid of the useless data.
- Finding anomalies involved the assessment of large JPEG images and specialized applications.

Extensions		MS OS		Graphics		None	
Configurations	11%	Camera images	7%	Web	6%	Non-readable	4%
Links	3%	Word	3%	Audio	2%	Unknown	3%
Encoded	1%	Sources	1%	XML	1%	Integers	2%
Copies	1%	Questions	0.9%	Excel	0.5%	Disk images	1%
Database	0.5%	Current actions	0.5%	Video	0.2%	Images	1%

The results acquired for the devices of the US official include;

Analysis of Drive 121

- Operating system Windows (60% non-deleted content and 40% temporary content).
- Time behavior: personal user

Analysis of Drive 129

- Operating system Windows (70% non-deleted content and 30% temporary content).
- Time behavior: personal user

Association between files

Clustering allowed the finding of an association between paired files and their quantification. The possible factors identified are;

- Temporal association: modification and creation of time leading to causal relationships.
- Filename association: files existing with the same names and excludes extensions.
- Content-hash association: files depicting cryptographical hashes referring to the specific identity of the content.

Conclusion

The assessment of the investigation report presented by the forensic investigation team will lead to the evaluation of contents. Forensic team adopts adequate procedures that result in meaningful outcomes and help in the determination of crime and its nature. A digital forensic process model provides benefits and ensures gaining sound interpretations. The evidence obtained through the process will assist in reconstructing events and uncovering the association between the US officials and the Russians. It also leads to the development of generalized solutions.

References

Agarwal, A., Gupta, M., & Gupta, S. (2011). Systematic Digital Forensic Investigation Model. *International Journal of Computer Science and Security, 5* (1).

Buchholz, F., & Spafford, E. (2004). On the Role of File System Metadata in Digital Forensics. *Digital Investigation, 1*, 298-309.

Brian, C., & Spafford. (2003). Getting Physical with the Digital Investigation Process", International Journal of Digital Evidence, 2 (2).

Garfinkel, S. L., & Shelat, A. (2003). Remembrance of Data Passed: A Study of Disk Sanitization Practices. IEEE Security & Privacy, 1, 17-27.

O'Seomus, C. (2004). An Extended Model of Cybercrime Investigations. *International Journal of Digital Evidence, 3* (1).

Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. *International Journal of Digital Evidence, 1* (3).