Forensic Investigation-Illegal Materials

Name

Institutional Affiliation

Forensic Investigation-Illegal Materials

**Executive Summary**

Forensic investigation involves gathering all crime-related evidence to provide a comprehensive conclusion about a suspicious activity. Ideally, in forensic investigation especially based on the case study provided, investigators will be concerned with performing (Delp et al., 2009) investigation and analysis on the hard drive and computer to establish how crime took place. In providing a brief description of the event with reference to the case study provided, it can be noted that the workstation purchased by Mr. Aaron Green was previously owned by m57.biz, which had not erased its data from the drive. By Mr. Aron Green purchasing this computer with suspicious data on the disk seems to pose cybersecurity questions, which require a though forensic investigation using the disk image, to ascertain the nature and security of data in the disk.

In ensuring that the whole process of forensic investigation has been completed successfully, the methodology used in this process was digital forensic analysis methodology. This methodology apply scientifically derived and proven approaches in the preservation, collection, validation, identifying, analyzing, documenting, and presenting digital evidence deduced from the digital sources with the aim of furthering the reconstruction of events found to be crime-related. Concerning the methods of evidence collection and preservation as applied in this forensic investigation included drive imaging, harsh values, and chain of custody. The three methods are known to be effective in digital forensic investigation and are critical in ensuring that legal admissibility while to engage a forensic analyst.

 Ideally, in this paper the goal is to ensuring a comprehensive forensic investigation has been undertaken with the aim of presenting digital evidence on the reported suspicious activity and data in the disk. In summary, the following are the key issues addressed in this paper:

* Preparation for digital forensic evidence collection.
* Analysis and identification of digital evidence.
* Preservation of the data by performing system boot-stream image capture of data.
* Selecting potential copy of the available data upon verification of the copy of the available data.
* Other things that need to be checked on include examining, classifying, analyzing and presenting forensic investigation report.

**Introduction**

Notably, in the case study provided there is one personality involved in the investigation process whose name is Joe, and she is considered to be the main suspect as well as subject of this investigation. It is worth noting that the primary offence being investigated in this case is the possession of drugs based on the suspicious documents and videos as found by Mr. Aaron Greene in his newly purchased workstation. Additionally, there are other suspects in this case, who include the rest of the employees who in one way or the other are connected to Jo through the network configuration of the company, who include Charlie, Pat McGoo, the CEO, as well as Terry, the system administrator. Additionally, apart from investigating based on illegal drug use, there are other possible crimes that are notable in this case, which include tampering with evidence and negligence by the police staff.

Based on the case background, the case that revolves around m57.biz involving Jo, who is an employee of this company, who used this workstation as part of her job as a patent researcher for the organization. Ideally, workstation is purported to have been replaced with another computing device, and therefore sold off, which was later bought by Mr. Aaron Greene, who did report about the suspicious issues about the workstation. Due to this, the police arrived at the scene to assist in carrying out investigation. All these operations were authorized by the company CEO, Mr. Pat McGoo . In this case, images of the original machine are presented in the presence of forensic experts witnessing it having a data format with E01 extensions. Additionally, two other available formats provided in this case include AD1-ADn. The stated formats are purported to be of the same computer; however, there is suspicions of negligence or foul-play that is under siege and being investigated by the forensic experts to see if there will be the basis of conviction for drug usage or possession

**Main Character Profile**

 As mentioned earlier, Jo is the main character under investigation. Below is his profile.

|  |  |
| --- | --- |
| Character Name | Jo |
| Profession | Patent Researcher |
| Organization  | M57.biz |
| Applications used | Outlook, Python, and Firefox |

**Relationship Diagram**

The diagram below shows the network configuration of M57.biz organization, which also forms the basis of forensic investigation.



Figure 1: Network Configuration

**Methodology Details**

As mentioned earlier, this forensic investigation adopted digital forensic analysis methodology. Digital forensic analysis methodology is an approach that apply scientifically derived and proven approaches in the preservation, collection, validation, identifying, analyzing, documenting, and presenting digital evidence deduced from the digital sources with the aim of furthering the reconstruction of events found to be crime-related. Understandably, digital forensic analysis methodology is based on various key elements, which include the use of scientific methods, collection and preservation of data and digital evidence, validation, identification, analysis and interpretation, and documentation and presentation (Delp et al., 2009). Based on this methodology, its process overview comprises of various steps, which include obtaining and imaging forensic data, forensic investigation, preparation/ extraction, identification, analysis, forensic reporting, and case level analysis.

 Based on the case under consideration, the investigator and forensic examiner must decide how much of the process is to be completed in every stage. Ideally, the whole process is iterative in nature hence the investigator and examiner must put this into consideration and decide how many times to repeat this process.

**Investigation Tools**

In this assignment, the main tool used to undertake forensic investigation is known as FTK imager as well as OS forensics. The main reason for using FTK imager is to help in gaining access to hard drive images that are under consideration (Sutherland et al., 2009). Additionally, this would be useful in making it possible to identify documents and media pertaining to the case at hard. With the application of FTK imager, all the suspicious files were identified and extracted which was used to do investigation using other tools and applications depending on specific files being investigated. Based on the investigation undertaken, the files that were identified included video files, image files, mail logs, and browser history as used in the past. Additionally, with the application of OS forensics, we were to perform indexing of the hard drive and then identifying suspicious files with ease through serial sequential searching. With DB browsing for SQlite was applied to further perform investigation of internet and web browsing history.

In the investigation process, one suspicious file was identified. The operations done to identified its contents involved decoding as well as decrypting. Ideally, steganography master was used to detect and decode image as well as wav files encoded in steganography.

**Recovery of Deleted Files**

After undertaking inspection of the thumb drive grasped from Jo with FTK Imager, several files that were deleted were identified whereby large amount of those files were inform of images and media. Such files were extracted and restored under the inkling that they could be directly associated with the case at hand. Notably, most of the deleted files had an indication of the last date modified at an earlier date that the first date created, indicating tampering of such files through the changes of timezone. The screenshot below show over 300 files deleted from the drive. These files were recovered using FTK imager.

Figure 2: Deleted Files

**Suspicious Crime Involvement with Drugs**

Ideally, the main crime being investigated in this case is the involvement and possession of the drugs. In this case, the main suspect being investigated is Joe. The reason of him being the main suspect is based on the inspection carried out on Mozilla Firefox history in her current computer/ workstation at m57.biz. Past searches by her shows things like instructions on how to take drugs were found in his browser, leading to a higher suspicion on drug involvement. Additionally, there is a reason of suspecting that Jo is not only the person involved in this case. With reference to the mails sent by other employees, it appears that there is a higher possibility that Jo and Pat McGoo, the CEO may have been collaborated in using and possession of drugs. Such conclusions were deduced based on a number of reasons, particularly from the email threads sent between the employees. Based on the investigation carried out, some emails retrieved purport that their CEO appear to be weird with both Charlie and Terry having commented on this to the rest of the employees in the past. Nevertheless, Jo has never done such a thing despite having such thoughts. It appears Pat behaved in a weird manner when under the influence of drugs, leading to such opinions from his subordinates. Additionally, there is no genuine reason for Jo not providing comments to his weirdness to her colleagues, meaning that Jo could be knowing the reasons for Pat acting in a peculiar manner

Figure 3: Charlie Commenting on Pat

 **Figure 4: Terry Commenting on Pat**

Based on the screenshots provided Pat appears to be spending quite a lot of time with Jo than any other employee in the organization, sending her “coffee runs” and requesting to meet on regular basis. Ideally, this means that the two may not have regular working relationship, but it appears they could be doing other things, based on their conversation as obtained from the disk. When telling Jo to purchase coffee, Pat provides a description of his flavor that he prefers in a very peculiar manner. Additionally, one of the employees by name Terry gives comments on the farcicality of the flavor. With this descriptions, it gives suspicion on the nature of coffee. It is highly possible that the form of coffee being described is meant for disguising the fact that it is depicting drugs. This is a speculation that is evident, that Pat always appear to request Jo to assist in refilling “coffee” which implies that Jo might have been going to attend errands not relating to fetching real coffee based on the preference of her boss.



Figure 5: Suspicious Coffee Ordering



Figure 6: Individual meetings with Jo.

Conceivably, the most convincing evidence identified in the investigation process is based on the email logs between Jo and her friend namely Jordan. Based on this evidence and as per the mail sent, Jo appears to be in a panicking mode because of the previous hard drive with the information on it. Additionally, Terry promised the hard drive properly and to never disclose any information and sensitive data. This is accompanied by a response from Jordan stating that Joe should be very careful. With this information, it clearly indicate that Jo has something that she is hiding, which forms the basis of this investigation on any files that could have been deleted from the disk. This narrative is boosted by the evidence learning on the mechanism of doing steganography, which is a well-known form of encryption based on an encoding of message via innocuous images.



Figure 7: Close Call by Jo

Figure 8: Jo’s Interest on Steganography

 Accordingly, the evidence provided above clearly provides a suggesting and point out on the issue of drug possession and use considering the browser history as used by Jo. Nevertheless, there is no explicit mentioning of drugs on the whole conversation, the main drug and suspect in this case and without such evidence, it is not possible to accuse the accused person because of drug question. It also appears not possible that based on the search history there seemed to have several links on the browser history, and that this was that it was done by Jo to pass time, and that the email conversation actually referred to as coffee and not drugs.

 Arguably, some people may claim that most of the pictures that are under suspicion do not exist in the hard drive of the computer purchased by Mr. Greene, pointing the possibility of no drug involvement. Nevertheless, as depicted in figure 7 above, one of the main reasons why it is hard to come across supporting and substantiated evidence in the hard drive copy is because Terry would have deleted such files to not be included in the FTK Imager. Additionally, on the side of defense for Jo, it is claimed that even if there were drug involvements, it appears that this could have be committed unintentionally or that it was done unknowingly that this action was not legal. Whereas this may sound possible, it is highly not likely that such an event would have occurred because of the nature of email conversations involved as retrieved from email log and as depicted in figure 7. Ideally, it is good to say the extent of nervousness and relieve in as seen in writing of her email with Jordan, implying that Jo would want to keep her activities and operations under cover. Additionally, the implication of this is that she must have an idea of the substance of her actions if they were to be found out meaning that this actions were unintentional.

**Evidence of Tampering**

 Based on what is depicted in figure 8, the images that were found on the hard drive, there is high possibility that such images are likely to have been tampered with via steganography with her friend Jordan. Notably, there is an observation that Jordan would have sent Jo a toolkit known as Digital Invisible Ink Toolkit. Notably, in this section it appears that Jo approached the instructions provided in the email as it appears below and hence is highly likely that the images in the Hidden folder have been encoded via steganography.

Figure 9: Testing of Steganography

 Based on the alternate disks images provided in the format of .AD1-And, it seems to be the same image as the one provided in the hard drive that is with the format of .E01. In having a clear insights on the effects of tampering, it is important to have an understanding of the disk imaging (Burke & Craiger, 2007). Additionally, there are several approaches of disk imaging in different formats. Ideally, disk imaging can come in various formats and just like file compression, disk imaging is connected to compression of the entire disk into an image. Therefore, it is worth noting that disk imaging may not provide 100% files recoverability. Additionally, it is important for such disk images to be in form of carbon copy for the disk under consideration. In evaluating if there is any tampering done in any particular image, the difficulty involved in preserving image should put under consideration. Naturally, with the imaging of the hard drive into many files, it is not imaged simultaneously. It is important to note that memory units tends to be tricky, and the presence of body traps for data may prevail. In such a case, specific aspects of the disk may become inaccessible as a result of destructive operations that may be involved when data is tried to be accessed leading to unrecoverable data loss. With this challenge of trying to attain consistent disk images in turn has an implication on the reliability aspects of tampering tests on disk images since it becomes practically impossible to attain actual copies of the same disk when trying to image it.

Nevertheless, there are specific mechanisms for detecting the tempering of the disks, with no regard of its similarity to the original disk. In the process of detecting tampering of the files in the disk, there are several tools available to complete this (Köhn et al., 2006). Such tools such as forensic droplets are applicable for commercial applications, which include Photoshop which can operate in allowing quick analysis and examination of images which is critical in identifying different changes in files if any (Newmann, 2013). Nonetheless, it is practically possible to achieve this only in micro-scale where tampering is detected. Ideally, it is clear that the whole disk images can be tampered with when making changes to the file systems and hence it becomes hard to detect (Davies et al., 2009). The rationale behind this is that standard forensic software are not able to access “bad” areas of the hard disk, thus providing an overview of how tampering and manipulation of the operations of the disk images (Sutherland.et al., 20019). Additionally, it is important to understand that disk image creation is not 100% perfect process, and what matters most is the tampering of the image, which makes it hard in determining whether foul-play was involved or not (Agarwal et al., 2011). Options available in non-tampering would be analyzing the original data from the media which is not an ideal solution in either way and may lead to dilemma on the best possible solution (Kim & Ross, 2012). Ideally, in such a case, it would be an ideal option to give the police the benefit of doubt and use the provided disk images.

**Conclusion**

 In summary, the available evidence does not clearly show about the drug traffic usage as well as the possession. Additionally, there is no adequate evidence based on the analysis and investigation carried out that could provide an explicit prove about the allegations. In ensuring that Jo and Pat are properly convicted and charge with drug usage and possession crimes proper prove beyond reasonable doubt must be proved or any other physical evidence, which must be presented and be substantiated for the conviction of the two or any other person to occur in this case.

References

Agarwal, A., Gupta, M., Gupta, S., & Gupta, S. C. (2011). Systematic digital forensic investigation model. *International Journal of Computer Science and Security (IJCSS)*, *5*(1), 118-131.

Beebe, N. (2009, January). Digital forensic research: The good, the bad and the unaddressed. In *IFIP International conference on digital forensics* (pp. 17-36). Springer, Berlin, Heidelberg.

Burke, P. K., & Craiger, P. (2007). Xbox forensics. *Journal of Digital Forensic Practice*, *1*(4), 275-282.

Cohen, F. B. (2012). *Digital forensic evidence examination*. Livermore: Fred Cohen & Associates.

Davies, G., Pringle, N., & Blyth, A. (2009). The Impact of Hard Disk Firmware Steganography on Computer Forensics. *Journal of Digital Forensics, Security & Law*, *4*(2).

Delp, E., Memon, N., & Wu, M. (2009). Digital forensics. *IEEE Signal Processing Magazine*, *26*(2), 14-15.

Kim, Y., & Ross, S. (2012). Digital forensics formats: seeking a digital preservation storage container format for web archiving. *International Journal of Digital Curation*, *7*(2), 21-39.

Köhn, M., Olivier, M. S., & Eloff, J. H. (2006, July). Framework for a Digital Forensic Investigation. In *ISSA* (pp. 1-7).

Newman, A. (2013). The art of detecting data and image manipulation. *Elsevier Editors Update*, *41*.

Phillips, A., Godfrey, R., Steuart, C., & Brown, C. (2013). *E-discovery: an introduction to digital evidence*. Cengage Learning.

Sutherland, I., Davies, G., Pringle, N., & Blyth, A. (2009). The impact of hard disk firmware steganography on computer forensics. *Journal of Digital Forensics, Security and Law*, *4*(2), 5.