Design and Development of Hard Disk Images for use in Computer Forensics

S.Siddiqui and N.L.Clarke

Centre for Information Security and Network Research,
University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

Educating people in new domains on new technologies requires good practise. But educating people has its own limitation as forensic is a very sophisticated job and it will not be sufficient to make an untrained person part of an investigation in order to get him trained because his less technical skills might cost loss of important evidences. Here the questions arrives then how to train and educate people about collecting digital evidences without involving them in real scenario and even if they get trained but it remains doubtful that either they would be enough capable of handling real crime situations or not. This research paper has been made on behalf of the research & experiment conducted on designing a forensic bit level image which would be useful for educating people about forensic examination. People can benefit from the designed image by evaluating their skills through trying to recover all possible artefacts. One of the main priorities of the research was to design an image which should look much closer to the images captured from the actual drives found on real crime scenes in order to provide users a much practical and professional experience. Presence of anti forensics artefacts in crime case assures investigators that their job will not be easy this time or might be end up with failure as anti forensic utilities are used to thwart the crime investigations, That's why one of the most common crime has picked and also included essence of anti forensic to produce a list of artefacts which later practised on the experiment drive. A chronology of approx 80 artefacts has made which truly reflects a crime of employee conspiracy which is supposed to be one of the crucial issues in every next organization.

Keywords

Digital forensic, Security education, Hard disk imaging

1 Introduction

Rapid advancement in technology made the abusers more sophisticated which results involvement of computers in almost every next crime. Any level of involvement of computers in a crime makes it necessary to get examine by responsible officials who can identify what exactly went through the suspect machine. To convict the suspect requires evidence which brings the need of digital forensic which have the capability to dig further into all technology mediums in order to identify and preserve the digital evidence. Computer crimes are increasing rapidly day by day and for dealing them it requires a good number of experienced forensic experts which unfortunately departments does not have. Getting the inexperienced staff on crimes scenes and involving them on forensic examination creates a high risk of losing digital

evidences by making them tampered or overwritten which results prosecution to weaken the impact of the collected evidence against them.

Here is the question arrives that how to train and educate people about collecting digital evidences without involving them in real scenarios and even if they get trained but it remains doubtful that either they would be enough capable of handling real crime situations or not. On actual crime spots the very first thing an investigator does is to capture a bit level copy of found storage mediums and then begins analysing them. If a copy of those images provided to the beginners then it will hurt the privacy of the suspect as it is against the privacy legislation because passing drive images to people who are not directly connected to the investigation will become illegal as the suspect has the right of maintaining his privacy does not matter he is criminal or not (RFC 3227, 2002). Other than that passing actual crime images neither will it give a good platform in educating people as it will make them difficult to explore random huge GB drives because they really does not know the much background of the crime and the image, so that they will keep wasting time in searching different bits of the image. Therefore the best practise would be to design a smaller drive images which contains variety of suspicious stuff that makes the user familiar with all kind of common techniques used by abusers and they can learn the skill of differentiating casual activities among suspicious activities as well. In real world most of the times investigators come across those cases which based on sophisticated criminals who tries their best to thwart investigation process against them through using stegnography, encryption, overwriting recycle bin, and forensically wiping data. Along with simple illegal activities if the drive image contains above all anti forensics techniques as well that makes the image useful for all level of people who can utilize image according to their technical background. After playing with some special designed images people can get enough educated and they would be able to meet the level of real crime scenario investigation.

2 Research & Experiment Methodology

The initial phase of the methodology was to gain sufficient knowledge about digital forensic (mentioned above in the flow diagram), There are many technology products that can hold digital evidences such as hard drives, IPODS, network cards, floppy disks, memory sticks, magnetic tapes, firewalls, and routers. Exposure to all these hardware's and different kinds of computing environments is essential to develop expertise in dealing with digital evidences as different type of hardware might be encountered since different equipment and expertise is required for terabytes of storage versus miniature systems. Different crimes result in different types of digital evidences like cyber stalkers mostly use email to harass their victims, child pornographers sometimes have digitized images stored on their systems (Casey 2004, p.216). Increased work load on digital forensics has forced to form sub domains which includes specialised categories of System, Network, and Mobile forensics. It is apparent that single individual can not successfully handle crimes which based on different platforms as it is quite rare an investigator carries deep knowledge of each domain. But knowledge of operating system, artefacts and anti-forensic artefacts remain common in all domain of digital forensic.

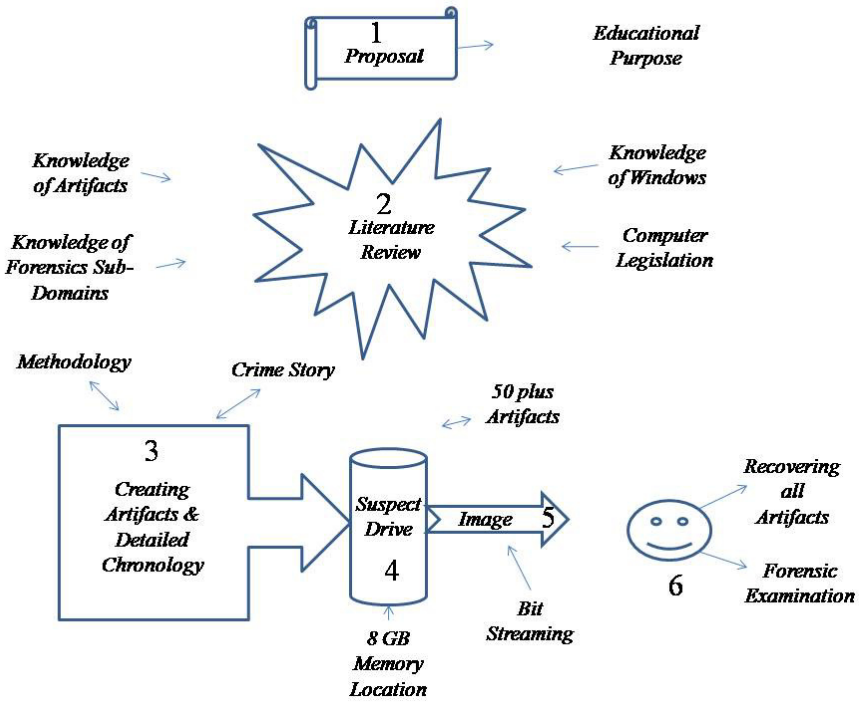

Figure 1: Research Methodology

An artefact is something created or shaped by human craft, Digital forensic artefacts are found on multiple locations of a storage medium which produced according to the behavioural activities of users. Several bits of a storage medium used to explore when investigators needs to identify the purpose behind the crime and if a nature of a crime is known than investigators remains focused on exploring only specific domain of artefacts.

Presence of anti forensics artefacts in crime case assures investigators that their job will not be easy this time or might be end up with failure as anti forensic utilities are used to thwart the crime investigations by overwriting, encrypting, and hiding their all possible foot marks (Hackaholic, n.d.).

After understanding the fundamentals of forensic, 3rd phase of the methodology (mentioned above in the flow diagram) includes a crime story in order to produce artefacts according to the scope of the crime. And In the last phase those artefacts will get perform on the 8 GB hard drive and makes the drive ready to get forensically imaged.

2.1 Crime Scenario for Designing Image

A practical crime scenario is the need for producing effective chronology, more effective chronology results broad range of artefacts which will make the image more interesting in analysing and useful for educating people. Crime of conspiracy

makes several things to look suspicious which bounds investigators to search for all emails, chats, history, documents, and hardware in order to find the digital evidences. In contrast to conspiracy with other destructive crimes like hacking, and spreading malwares that only makes the installed software and programming editors suspicious in the development of crime, which does not gives broad area to look for. Picking the crime scene below gives a broad range of artefacts which brings out variety of activities to add in crime chronology.

The Crime scenario is based on two employees who belongs to their competitor companies, Sid who is one of the trusty employees of Marine shipping meet John (Senior official of Titans) 1st time on a joint conference arranged by all shipping groups together. After having a general chit chat they exchanged their contacts details before leaving, later Sid received an informal email from John in order to plan a get together. John offered Sid a lucrative package which was way better to his current job at Marine Service but in condition he asked him to pass some confidential records of his company and offered him bribes for that conspiracy. Sid accepted his offer but to remain safe from all formal inquiries he opened a new back account to hide his additional income and studied about anti forensic techniques in order to thwart future investigations. Sid and John have made many conversations through Email and Instant Messengers and shared loads off confidential documents, to hide data exchanges and removing digital evidence Sid practised his anti-forensic skills by installing stegnography, virtual memory safe, and overwriting recycle bin software's. In addition to divert the attention of expected future investigation he added few random data including documents, images and tried deliberately to hide them suspiciously by encrypting or renaming file extensions. As his intentions were that even if someone examines his machine they will get busy in sorting and understanding the objective behind those suspicious files and that will lead the investigation towards wrong way and he will get safe from his actual crime.

2.2 Selected Artefacts

- ✓ Internet Explore
  Cookie, Cache, History
- ✓ Instant Messaging
  Chat logs, File transfer, webcam images
- ✓ Peer 2 Peer
  IP activity, connected hosts, host cache, file cache
- ✓ Email
  Text, Attachments, contacts lists
- ✓ Storage media
  Hard drive, USB, DVD, CD
- ✓ Router/Firewall
  Logs, ACLs
- ✓ Software's
  Hacking, Encryption, Stegnography
- ✓ Print
  Printing documents (RAW & EMF files)

2.2.1 Used Anti-Forensic Artefacts

Anti forensic artefacts have been used to made the drive look closer to the actual crimes happening around, which will prove more beneficial for users to get educated about forensic limitations.

Safebit software has been used in order to store documents in a virtual safe which are supposed to be in visible and un detectable in front of others and the most important thing that files stored in virtual safe never appears in any sort of search and it never occupies any level of memory which becomes more deceptive because of its ability of not increasing the memory consumption after storing documents in the safe (Download, 2007).

Stenography uses for hiding data onto files without making in notice to others. Hider software has been used for performing stenography on documents, through stenography text, jpeg, and other extension files can be embedded onto another file and later can be retrieved after entering the secret key (Lillard, 2003). The files first encrypted then embedded onto a carrier file after entering the secret key, even if the middle man sniffed the carrier file but he will not be able to identify that this file contains another file or in any case if someone has discovered that particular embedded file but still he needs the key to decrypt the original encrypted file to read. Such complex technology is supposed to be the most deadly utility of anti-forensic domain which hardly becomes detectable for investigators (Softaward, 2004).

Clean Disk Security software used for completely removing the traces of deleted files existence in recycle bin. Deleting files normally just removes the file directory index but the data itself remains stored on the memory mediums and by the use of data recovery software's the deleted file index can be restored which results in providing the access of the deleted file again. Use of this anti forensic software means assurance of vanishing all possible traces of the files (Clean Disk Security, n.d.).

2.3 Chronology of Conspiracy

Regrouping all activities according to their periods and forming a chronology helps investigators to understand the seriousness of a crime and it indeed plays a vital role in searching the smoke gun. Chronology is basically the sequential order in which past events occur, its basically a science of arranging time in periods and a reference work organized according to the dates of events.

A detailed chronology has made and practised on the experimental drive which leads the investigation towards crime of conspiracy. The developed chronology starts from 18th/Oct/2007 up till 30th/Oct/2007 which included variety of incidents relevant and irrelevant to selected crime. Below is the brief example of the incidents have made which were rich of criminal, suspicious, anti-forensic, and casual activities in order to design a drive image which is much closer to the actual suspect's drives.

Date/ Time	Description Of Artefact	Artefact	Tech.	Conspiracy
18/Oct/07	Image transfer from digital camera to my pictures in the folder 'conference 2007 ', These images were taken on the joint conference of all shipping groups held in Plymouth	Storage media	None	NO
24/Oct/07	Sid received an email from John, In which he offered him a lucrative package at Titans shipping which is a way better than his current job but in condition he has to pass some confidential information of his current company, They made this conversation through MS Outlook	Email attachment	None	YES
25/Oct/07	Sid sent a positive rely to john's offer of bribery	Email text	None	YES
26/Oct/07	Sid browsed Yahoo webpage	Web Cookies, Cache	None	NO
26/Oct/07	Instant Conversation b/w Sid and Sarah, Their conversation shows Sarah was Sid's girlfriend but she was not part of the conspiracy as no activities shows any involvement of her in the crime scene	Instant Messenger chat logs	None	NO
27/Oct/07	Sid browsed web page of HSBC to open a new account in order to hide his under the table benefits	Web Cookies, Cache	None	YES
27/Oct/07	Sid browsed some Anti-forensics pages which shows he was afraid of forensic investigation and he was looking for some way outs to avoid evidence collection. A "Anti Digital Forensic.pdf" was downloaded and copied to USB. Sid deleted that pdf on the same day when it was downloaded.	Web Cookies, Cache Storage media Deleted files	None None Deletion	YES
28/Oct/07	Online shopping of mobile phone through carphone warehouse web site	Web Cookies, Cache	None	NO
28/Oct/07	Three MS Excel files (confidential1.xls, confidential2.xls, confidential3.xls) which contains crucial information about the company has transferred to John through MS Outlook	Email attachment	None	YES
29/Oct/07	Sid created a word document "New word document.docx" which contains confidential information about the company, He encrypted the document before transferring through Instant Messenger as	Instant Messenger File transfer	Encryption	YES

	except john if any one else tries to access it would not become successful			
29/Oct/07	Sid browsed Google web page and it seems he was searching for a particular singer or song, As all pages belongs to a similar artist	Web Cookies, Cache	None	NO
29/Oct/07	Conversion of "sdsd.jpg" extension file into "sdsd.ppt", Although the files did not contain conspiracy stuff but this has been done to divert the attention of investigators	File Signatures	Changed extensions	YES
29/Oct/07	Browsed news paper websites	Web Cookies, Cache	None	NO
30/Oct/07	(a) Documents was scanned and then saved into a different file extension, Which makes the file open able but after opening it will show nothing except garbage values. (b) Sid installed stenography software and later those files were stegoed and sent through email attachment, Stego process will embed secret data in the file which remain invisible for others and that data can be recovered by entering a secret key.	Registry files File Signatures Installed Software's Email attachment	Changed extensions None Stego	YES
30/Oct/07	Couple of important documents (print1.doc, print2.doc) had been printed	Printing jobs (EMF, RAW files)	None	YES
30/Oct/07	Transferring Images from Digital cam to PC, These were just causal pics taken in the office cafeteria	Interconnecting Hardware	None	NO
30/Oct/07	Sid installed Safebit anti forensic software, Files hidden by software are highly unlikely to become traceable, Multiple files (asasasa.jpg, dasd.file, hellopak33) had stored in virtual memory by creating a virtual safe containing name "Mysafe"	File Signatures	Hiding data	YES

Table 1: Brief Sample of actual experiment chronology

3 Discussion on Designed Image

After analysing the image one can get a perfect start for becoming a System Forensic investigator which is the foundation of all forensic domains, as this image explores all the possible artefacts of an system including documents, web browser, email, printing, scanning, storage medium, and installed software's which leads individual to a solid foundation of systems forensic

Detecting stego files are a bit rear due to its nature of deception, The file that contains steganographically hidden information is somewhat proportional to the popularity of the software package. The software used in the experiment hard drive was not renowned and commonly available to masses, and if a new method formulated privately and used carefully then chances are that its existence would never become alerting (Caloyannides, p-246).

EMF & RAW print jobs will not be found in the print spool as they get deleted once the printing job has been done. Mostly these files are expected to be found in slack spaces and unallocated clusters but chances of tracing them become low with the passage of time as the data keep overwriting on slack spaces (Encase, p-381). So that could be the valid reason if one will not recover printing jobs as there were already just couple of printing activities made according to the chronology therefore couple of jobs will not take much time to get overwrite under slack space.

The designed image could also be very useful in performing a comprehensive evolution of tools, people if want to identify which forensic tool is more powerful than they can play with the same image by using different tools and can verify how many artefacts they managed to recover through each tool.

4 Conclusion

This designed hard drive image contains verity of colours of forensics & anti forensics and one could get extensive knowledge and practise while playing with this image. Various artefacts have been created in order to give broader scope to explore different areas of a hard drive and other than that anti forensic techniques has been used to improve the skill level by making them difficult in finding evidences and forcing them to think the way outs against them. The image created email traces by using both web based and software based email communication which indeed gives a useful exposure of discovering both the technologies, banking and many other web sites have browsed to give good exposure in sorting Cache & History between relevant and irrelevant sites to crime. Other than that the image contains the traces of existence of weird software's and un compatible file extensions which provides a better platform to learn more about difficulties in forensics investigations

5 Reference

Casey (2004), *Digital Evidence and Computer Crime*, Academic Press, Britain

Caloyannides (2004), *Privacy Protection and Computer Forensic*, Artech House, London

Disk cleaners n.d., http://www.diskcleaners.com/clndisk.html (accessed on 10/Nov/2007)

Download (2007), http://www.download.com/SafeBit-Disk-Encryption/3000-2092_4-10711654.html?tag=lst-1 (accessed on 10/Oct/2007)

Bunting, Wei (2006), Encase Computer Forensic, Wiley, USA

Hackaholic n.d., "Anti forensic", http://ws.hackaholic.org/slides/AntiForensics-CodeBreakers2006-Translation-To-English.pdf (accessed on 10/Oct/2007)

Lillard (2003), "Steganography-based techniques using Encase", http://www.cit.uws.edu.au/compsci/computerforensics/Online%20Materials/SteganographyEFE4.pdf (accessed on 29/05/2007)

RFC 3227 (2002), "Guidelines for Evidence Collection and Archiving", http://www.faqs.org/rfcs/rfc3227.html (accessed on 3/Dec/2007)

Softaward (2004), http://www.softaward.com/3519.html (accessed on 15/Dec/2007)