Project overview for portfolio upload

Project Title:

Digital Forensic Investigation of Disk Image

Project Description

This project involved a mock digital forensic investigation of a suspect, 'John Doe.' As part of this coursework, we were tasked with 'seizing' John Doe's computer and conducting a comprehensive analysis. The focus was on digital forensics, and we analysed an imaged file representing John Doe's machine. Although we learned the process using physical hard drives, the imaged file was provided for this exercise.

Tooling used (But not limited to):

- Autopsy
- John The Ripper
- Registry Spry
- Okteta
- Mork.PL
- CLI tools: grep, strings, binwalk, exiftool, foremost, dd, etc

Processes and Techniques used (but not limited to):

- Disk imaging
- File carving
- Whitelisting
- Registry Analysis
- Browser Analysis
- Password cracking (Bruteforce, Dictionary)
- Timeline analysis

Grade: A

Appendices have been removed to avoid plagiarism from future students, however I am happy to provide additional information or discuss the work further if desired. ***Disclaimer****: I do not give permission for this work to be copied, those who do may be liable for plagiarism.*

Table of Contents

Executive Summary

The following report outlines the techniques carried out by Digital Forensic Analyst who has been tasked by Tayside Police to locate Illicit Ornithological Material found on Mr John Doe’s seized hard drive. In carrying out these techniques, many pieces of Illicit Ornithological Material were found on the hard drive within the system that was seized from Mr John Does residence on arrest.

This report is a comprehensive look at this evidence found and the corresponding activities that were carried out on the system belonging to John Doe. A timeline has been generated to allow the reader to understand the listed activities and how this applies to John Doe. The 2nd – 9th of February 2005 was when the highest level of IOM activity was taking place and as a result this period is the focus of the timeline and will further guide the presentation of evidence. An extensive methodology section has been created by the digital forensic analyst to provide context to the investigation and to help provide a universal understanding to the techniques used so that the reader is clear on how the evidence has been obtained and analysed. Additionally, it will provide information on how the evidence was stored & handled throughout the investigation.

These findings of this report show clear intent from an individual who was the user of the profile named ‘johndoe’. It is not for this report to decide who the user was but to simply show a pattern in the activities carried out by this user account on the seized machine. Logs discovered from two web browsers on the machine was used with crucial registry information to provide a comprehensive picture of the user's activities, detailing what had gone on in the system.

This report will not set out to determine whether John Doe should be considered guilty for the activities that are listed but to allow the reader to be informed of the activities taken place.

1) Description of Crime

Description of reconstructed events

Incident 1 – Bird pictures taken with Canon Power Shot

Between 9th and 27th of June 2004, 17 pictures related to Illicit Ornithological Material (IOM) were captured using a Canon PowerShot camera (see Appendix 1). These pictures were discovered on the recovered hard drive seized from Mr John Doe. Evidence of these files lying on John Does computer (see Appendix 2). Notably, one of these collected images is of an unidentified man holding a bird (see Appendix 2).

Incident 2 – Suspected Bird Trip & User

Upon further analysis of the Canon PowerShot photos obtained on John Doe's hard drive, there is images of a group of individuals partaking in outdoor activities (See Appendix 2) from the same dates as the previous incident (9th-27th of June). Five of these images were created between the 15th and 22nd of June have been given bird related "*names*" suggesting involvement in 'IOM'(See Appendix 19).

Incident 3 – Initial Web Browser Activity

On analysis of John Doe' hard drive, web browsing activity involving 'IOM' begins taking place on February 2nd, 2005 at 14:18. User 'johndoe' begins browsing by looking at local images that he has stored on his computer (on the path *C:/Documents and Settings/johndoe/My Documents/My Pictures)* through web browser Internet Explorer (See Appendix 18). On Mozilla Firefox (another web browser) the user johndoe proceeds to visit more 'IOM' related websites repeatedly for the next 30 minutes until the browsing material changes at 14:40 (Appendix 13). View appendix 13 for a full breakdown of websites visited and search terms used during this time. At 15:11 user johndoe visited the PBS website where they downloaded two audio files with IOM related titles. (See Appendix 12).

Incident 4 – Browsing Encryption Software Online

During Incident 3 (February 2nd) at 15:47 the user 'johndoe 'performs a google search for the search term "windows gnupg" on Mozilla Firefox web browser (Appendix XX). Through the Firefox history logs the user's activity can then be followed to the download page of GnuPG. GnuPG is a known encryption software (See glossary for encryption definition) and is often use to create password protected files. Whilst downloading encryption software is not illegal, as this report will outline in section 2.4.3 a file containing IOM had '.gpg' encryption proving its use in illegal activities. After this browsing of GnuPG, user johndoe visits the website of WinPT a tool that provides a more user-friendly interface for encryption tools such as GnuPG. This is suggestive in showing the clear path the user johndoe takes to download encryption software.

Incident 5 - Usage of Encryption Software on System

It is important to note that no download logs were found documenting the download of WinPT or GnuPG when looking at the retrieved download history log in Firefox (See Appendix 13). However, indication of the software being installed can be obtained through analysis of the disk's registry (*See glossary for defining registry*). When looking at the corresponding registry key for WINPT and GnuPG on NTUSER.dat it shows there was a modification to the key on February 2nd 16:32 for GnuPG and 16:32 for WinPT (Appendix 15). Additionally, when observing the creation time of the encrypted file entitled 'birdpics.gpg' that was later retrieved in evidence, it was created at 16:46 in '*C:\Documents and Settings\johndoe\My Documents*' (Appendix XX) shortly after the browsing to the website & registry key modification. There is also the download of adobe reader (a pdf reading software) shortly after at 16:52 on the same web browser, this is relevant due to a handbook on WinPT being found in a PDF format showing there is another clear activity taking place around the encryption software.

Incident 6 – viewing and downloading 'IOM' files online

On February 3rd, 2005, the johndoe user account can be seen once again browsing for IOM online. This is carried out between 12:21 and 15:04 on this day. The user begins the search by searching into google 'bird mating calls' (Appendix 13). This day is prominent for the substantial amounts of downloads that take place on the Firefox browser (See Appendix 12). There were several distinct types of files that were downloaded on the date including audio files (.wav), images (.jgp) and webpages (.htm) (See Appendix 12). These files were all labelled with some variation of an IOM related title. The files were downloaded to variety of places on the disk within user johndoe. However, one file, 'ready2fledge.jpg' was downloaded to the user bob directory, this file was later viewed on the machine.

Incident 7 – Searching for screensavers & downloading ZIP

On February 9th at 11:27, the user of the 'johndoe' account enters the search term into Google 'bird screensavers. He then proceeds to download a file entitled birds.zip to C:\Documents and Settings\johndoe\My Documents\. This file continued to be browsed by the user johndone once it was on the system. This can be seen by observing the Most Recently Used (MRU) hive in the registry detailing all the files which were previously used just before the hardisk was seized (see Appendix 15).

Incident 8 – Emails being sent with images

On 9th February 2005 at 11:08am, four emails were sent to an email address titled 'jdoe@example.com'. Notably, three of which are from the email address; 'ben@example.org'. Amongst these, two of them contain 'IOM' images. One email has three images, and another has five. The email that contains five IOM images also contains suggestive text which could imply that whoever the email was meant for (at the address jdoe@example.com) had previously sent some of their own images over. However, this is currently speculation. Another email from 'Ben@example' has text discussing a 'white cockatoo' – more IOM related correspondence. Finally, the other email comes from an email address 'mailinglist@birds.example.com' this can suggest that the user is also part of a bird mailing list.

2) Description of Investigation

2.1 – Job Description and Instructions

Upon the arrest of Mr John Doe, Police Scotland investigators carry out a search of his home for potentially incriminating items. One of these items, a Hard Disk Drive, was alleged to have evidence which could contribute to the prosecution of John Doe.

The evidence that investigators are concerned with fall under the categorisation of Illicit Ornithological Material (IOM). Any items of an ornithological nature are considered illicit, this includes documentation, files on disk, communication between suspects regarding ornithology and a variety of media such as images, audio files & videos. Additionally, investigators involved in the prosecution of John Doe are looking to identify any intent shown by John Doe in the viewing, distribution, or creation of IOM. Therefore, to perform a correct analysis of the hard disk, Police Scotland have given the hard disk over to a digital forensic analyst that is trained to perform industry standard digital forensics techniques, processes & procedures.

It is the responsibility of the digital forensic analyst authoring this report to present all relevant evidence that falls under the previously outlined specification of IOM. Additionally, the examiner has been tasked with determining key events (known as incidents) that can form the foundation of a timeline of evidence to create a procedural viewpoint that non-technical literate individuals can understand. In creating a report that can be read and understood by a variety of individuals, it will allow the document to be used in a court of law, presenting extra information, and providing a deeper context to the case of Mr. John Doe for a Jury, should the case go to trial.

2.2 - Description of Recovered / Examined Items

Table

Images	94
Documents	11
Audio files	3
Miscellaneous files	6
Correspondence	3
Logs	26

2.3 Methodology

2.3.1 - Acquisition & Preservation of disk

2.3.1.1 – Clock Skew

To provide an accurate and reliable account of the activity that has taken place on John Doe's machine it is important that correct validation has been given to the time that is stored within the BIOS of John Doe's machine. This then must be cross referenced with a known reliable source of time to ensure there is no dramatic variation with what the suspects system reads regarding the valid time.

2.3.1.2 Imaging

After receiving John Doe's disk drive from the evidence storage, an image of the disk must be created so that the digital forensics analyst is able to work on a separate copy without risk of damaging the original evidence. Therefore, a rigid process must be followed when creating an image of the disk. Firstly, ensuring a safe space on the workstation used by the digital forensic analyst will prevent unwanted change in the date. Secondly a SATA cable will be connected to the drive and to the forensic workstation being used. It was important to ensure this was done in a particular order of SATA cable (a data transfer cable for hard drives), power cable, power activation, USB cable link to the workstation. This was vital to prevent damage to the data on the hard drive. Once the examiner has reached this step, commands within Kali Linux (the Operating System used by the analyst on their workstation) will allow the analyst to create a mirror image of the data on the disk.

2.3.1.3 Investigating the drive.

At this point of the investigation the examiner has a file, of which its contents will have the suspects entire hard drive. It is important for the examiner to carry out forensic processes on this file to learn a bit more about how the disk will operate. Firstly, finding out the entire size, secondly, having a look at all the partitions that exist on the drive. Partitions are sections of the hard drive that allow users to store files and information in them. Sometimes those who wish to hide files can create unallocated partitions (secret partitions not available to see from a regular operating system). It is important to ensure that if there are unallocated partitions that the analyst is aware so they can ensure they are checked within their investigation. With this hard drive, there is a large section of unallocated space in one partition (2.42gb) indicating that there might be further information regarding this drive. Evidence found in the unallocated partition (see Appendix 22).

2.3.2.4 Malware Scan

When obtaining an image of disk for investigation, there is a possibility that the suspect installed potential *malware (See glossary for definition)* on the disk to protect their sensitive and potentially incriminating information on the disk. Often, this is so the malware will make files unreadable or try to deter the digital forensic analyst from searching the disk altogether. The existence of malware can also have legal consequences as the suspect can claim for a 'Trojan Horse Defence', where the suspect claims that the incriminating evidence (in this case IOM) got on the disk through unknowingly clicking on some downloaded malware. To circumvent all these potential issues, it is best practice for the analyst to produce a malware scan before proceeding to search the disk further. In the case of John Doe, Malware Scanner 'Clam Av' was used due to its reliable reputation (see Appendix 23) for results. During examination of Prefetch files (files which hold information about commonly used applications) there is reference to malware scanners already on JohnDoes machine (See Appendix 23)

2.3.2.5 – Ensuring validity of the disk

It is important that there is a way for the digital forensic analyst to verify the data is unchanged and to protect the integrity of the investigation (what is known as the validity of the disk). This is done by producing a MD5 checksum of the file (a checksum is producing a passphrase that is unique to the file in question that will change if the data on the disk has been altered.

By carrying out this operation on the file, the verification code can then be used at various points to ensure the validity of the search. The checksum (unique code) of the John Doe disk is “*d63dd1b8917ca28bac7c955fc3b6cd25*”.

2.3.2.6 – Who was using the computer.

Understanding the users of the machine can help with the ‘bums on seat’ problem that is often faced with this type of investigation. The ‘bums on seat’ problem is one where it can be exceedingly difficult to prove who is using the machine at the time of the offence being made. An indication for who was using the machine can be made judging by the user that is logged into the machine at the time of the offence. This is not concrete however as there is always the chance that someone else could be logged in as that user to help redirect suspicious activity. This can be countered by analysing the usage patterns of users online and on the operating system. For this investigation, the three users on John Doe’s machine are as follows: *johndoe, ‘bob’* and ‘*jane’.* Deciphering who has done what comes down to correctly analysing the registry & web browser activity logs to piece together the activities taken place.

2.3.2 – Reconnaissance (Initial Search)

Once an image of the disk has been obtained by the digital forensic analyst, the search for evidence can begin. There are multiple ways to search a disk and each analyst will have their own method, however the methodology detailed in this report is how the hard disk drive belonging to John Doe was searched. To provide some guidance to the investigation it is important to do some reconnaissance on the disk. This can include figuring out where some files of interest could lie. This involves a method called File Carving. The technical details are not important, what is important is the ability to understand how evidence was produced.

2.3.2.1 – File Carving

File carving is the process of searching for incriminating files using a files inbuilt information that each file can hold – known as ‘Meta Data’. Each file is different, and it is important for the analyst to understand what is relevant to the current investigation. File Carving is the process in which the Canon PowerShot images were obtained and is the evidence provided for Incident 1 in the timeline of events. These images carry information about the make and model of the camera which has allowed the analyst to perform a search on the disk to which numerous results have returned (see appendix 21) for a list of all the evidence that has been taken with a Canon Power Shot camera.

The process of this can be replicated for file types and by using a tool called ‘Foremost’ an initial search through the disk for several different file types (image files, such as jpg, png, gif, document files such as pdf or word files) can be executed. During this search, password protected PDF’s and one corrupted (unopenable) PDF is discovered, refer to the section 2.4 below for the information received from these files. File Carving provides many files which are no use to this investigation, therefore other methods have been implemented to help narrow down the scoop of the investigation such as Whitelisting.

2.3.2.2- Whitelisting

Whitelisting is the process of filtering out all the standard files that come pre-packaged with the operating system. This process can help narrow the scope of an analysts search and provide a quicker way to search through storage. This process is completed by comparing a list of all the known files of a fresh windows install to the suspects device (which has had its windows operating system altered due to the functionality of operating systems) and filtering out those that are known to be innocent. This process was carried out in this investigation to help filter down to just files of interest. It is a beneficial technique that when combined with File Carving can produce reliable results to finding the evidence required for an investigation. However, one problem still exists that is determining what exactly happened on the machine. For this, a directed search towards the registry is crucial.

2.3.2.3 - Searching the Operating System (Registry Analysis)

As outlined in the incidents in section 1, to prove that activity has taken place on a system, it is essential to analyse timestamps within the registry. The registry can be defined as a hierarchical database of configuration files that record the ongoings of an operating system such as installed programs or most recently used files. It is through looking at the timestamp of encryption software that Incidents 5 & 6 can be proved correct. Often individuals can alter files on the disk to cover up potential wrongdoing, however many forget to tamper with the registry, allowing for it to be a fantastic source of evidence & information. Registry analysis does however have its limits, it cannot view user activity online, which means that it cannot track a user's communication outside of the operating system. That is where browser analysis will fill in missing gaps in evidence.

2.3.3.4 – Searching the Network (Browser Analysis)

Through the previous searching of the operating system, there is evidence of two browsers, Mozilla Firefox & Internet Explorer. Each of these browsers has its own method of logging and its own way of retrieving these logs. The logs will inform investigators of the user's online activity and help provide more evidence where appropriate. Each browser can inform the investigator of web history, web caches, web downloads, cookies and finally if they have used the web browser to open local images (as mentioned in incident 3). Internet explorer stores its logs within files titled 'index.dat' and can be opened universally by a program called 'pasco' which then allows for them to be analysed within a spreadsheet. Firefox files must be opened a separate way. For this report a specific program (Mork.pl) has been used to open and read the information with the Firefox history & download history.

2.4 Analysis

This section will detail extra pieces of information acquired across the investigation through using the techniques carried out in the methodology, whilst making note of any extra techniques that are required to understand this new evidence. The evidence outlined here have also contributed to the creation of the incidents in section 1 as there is extra information that can strengthen proof of the incidents taking place.

2.4.1 Autopsy

A large part of this investigation was carried out through bash (see glossary) commands in Kali Linux (operating system). This involves large amounts of inputs and results being typically displayed to text files or within the terminal (input / output box for user commands). However, Autopsy a digital forensics platform has been used as a graphical interface to guide the investigation. Autopsy was the primary source for recovering the email correspondence outlined in section 8. Autopsy has been used as a point of reference throughout this investigation to cross reference information learnt from retrieved files in evidence.

2.4.2 Locally stored HTML Files

Found in C:\Documents and Settings\johndoe\My Documents were 2 HTML documents that when selected will open the browser two to IOM related pages. The First file entitled *aa010703a.html* takes the user to a crafting guide for bird box with the title page “Build a Bluebird Nest Box” and can be seen in appendix XX. The second page has a file called ostbk2b2.html and takes the user to page that describes how to best look after young birds.

Further analysis into the web browser revealed a bookmarks.html file that has a 3 incriminating bookmarks. These bookmarks belong to the user account john and have the following titles “Free Bird Wallpaper - Bald Eagle Albatross Owl Falcon 1024x768” , “Alphabetical Index of Birds” & Chicakdee Karaoke” all of which can be considered ‘IOM’. See appendix XX for a full view of these bookmarks.

2.4.3 Encryption

2.4.3.1 Birds.gpg

Encryption is found in multiple locations on the disk seized from JohhDoe. Encryption enables the contents of a folder to be hidden to those without the password. This use of encryption is outlined in Incident 5 & 6 from section 1, whereby observing browser activity logs & the registry provides definitive evidence of use of this software on the system. When decrypting the file 'birds.gpg', the method chosen was 'Brute Force Password Cracking' this is where a program will systematically try every password combination with hope of obtaining the password. The password obtained for this folder was 'arran' (Appendix XX). Inside this .zip folder were several bird photos. Unfortunately, all but one photo (WhiteThroatedSparrowInTree.jpg) was corrupted. However, the file names are suggestive of IOM. (See Appendix XX for corrupted files & file names) .

2.4.3.2 PDF Hashes & Dictionary Attack

As previously described, there is several PDFs on the system which have a password. The method of breaking this password was slightly different. To obtain the password for these files, a dictionary attack was carried out. This involves knowing the hash of the PDF (As mentioned earlier consider a hash of a file as a unique identifiable code) and using this combined with a list of commonly used passphrases to try creating a match. This process returned the correct password of 561508 (see Appendix 16)

2.4.4 Miscellaneous Files

Corrupted PDF & IOM

In discovering the password protected PDF's a corrupted pdf was uncovered, this PDF (01254615.pdf) was unable to be opened. When looking at the metadata of this file there was an obvious error with the structure of the file (Xfer Table – see glossary) Therefore an extraction was necessary by using a command in Linux called 'Binwalk'. This command allowed for the images that were inside to be separated from the corrupted file.

Extension Mismatch of .dll & .exe files

Autopsy has a built-in mismatch detection that provided to be very useful for this investigation as it provided a good reference for these types of files. This is where a file of one type can be masked by another for it to avoid detection by command searches such as use of strings and grep which was used a large amount in this investigation (Definition in glossary). Refer to Appendix XX for the images that were found in these masked files. The files that were masked includes.

2.4.5 Additional Events

Canon PowerShot Camera – User Connection

On the 27th of June 2004 an Image was created referencing 'Bob1'. As previously mentioned, Bob Is a shared name of a user on John Doe's system. This is open to being coincidental, however the data stored within the image of this individual shares a lot of commonalities with those containing IOM. This is something to consider later, however it does not directly affect the activities outlined in this report.

Photos examined on removable storage device.

The following analysis was done through Autopsy's inbuilt registry analysis. On February 3rd at 15:51 Internet Explorer was used to view files which were stored on an E: drive. These files were labelled *'E:/birds/non%20images/BirdingGuide.*pdf' and '*E:/birds/non%20images/BookList.doc'* (See Appendix XX) . These names show that the content viewed was in-fact more 'IOM'. To ensure that this is indeed a removable storage device, analysis of the system registry was required. In performing this analysis, there is confirmation that this E:\ drive is labelled as a removable storage device.

3. Conclusion

The large quantity if incriminating evidence regarding IOM on the Hard drive seized from the home of John Doe is striking. There is a large enough pile of evidence to suggest that this was a repeated occurrence, and that this collection would have continued to grow if the hard drive was not seized.

By analysing the ongoings on the computer, through web browser logs, and in-depth registry analysis it is clear there is regular visits to IOM related websites, where downloads have taken place. There were clear indicators that whoever was accessing the machines at the time in question made some attempt to cover their tracks through using removable USB devices & tyring to utilise encryption software.

Email correspondence is perhaps one of the most important pieces of evidence of showing intent regarding the crime. There is what looks like the back and forth between the user and another party in which a thread containing IOM was found.

This report has outlined the importance for thorough and correct digital forensic analysis and it should be treated this was if another party would try to recreate the evidence for a court of law. Below is an outline of how this can be done to the best of someone's ability .

4. Equipment Required for Court Proceedings

The following equipment is what has been deemed necessary by the digital forensic analysts to carry out correct court procedures.

Evidence

The hard drive belonging to John Doe or a suitably validated image of the hard drive.

Specialised Equipment

- Equipped workstation
  - With Kali Linux or a version of Ubuntu which has many forensic tools already installed. This includes.
- Registry Spy
  - A registry viewer that allows the investigator to open windows registry hives finding out more about the system in question.
- Okteta
  - Hex editor used to ensure file signatures are corrected when looking for mismatches manually over relying on Autopsy. Also, very helpful in other areas such as analysing a broken file – such in the case of the corrupted PDF.
- Autopsy –
  - General purpose digital forensics tool that will enable whoever conducts research to load a previously worked on case. This will allow all previous information logged in autopsy to carry over providing a succinct and unified investigation.
- Mork.Pl –
  - For converting the Firefox web browser logs to a readable format
- John The Ripper
  - For Brute Force & Dictionary Led Attacks on the encrypted files out the

Documentation

- This report to enable clarification & provide a timeline to the events carried out by johnDoe

5. Glossary

(Terms generated by an online tool and have been adjusted by digital forensic analyst to ensure they are correct)

Illegal Ornithological Material (IOM):

- Any content pertaining to birds, especially if it contains sensitive or improper information.

Digital Forensic Analyst

- A specialist who investigates and examines digital devices and data to find evidence for legal purposes is known as a digital forensic analyst.

Hard Drive

- The hard drive is a computer's main storage component that is used to store data permanently.

Registry:

- Configuration settings and options are stored in a hierarchical database found in Windows operating systems.

Encryption

- Information is transformed into a code through the process of encryption to prevent unauthorised access.

GnuPG:

- GNU Privacy Guard, an encryption programme available for free online

Windows Privacy Tools (WinPT):

- An user interface for encryption programmes such as GnuPG.

NTUSER.dat:

- A Windows registry file that holds configuration data unique to a single user.

Web browser Download History Log:

- A record of the programmes and files that have been downloaded.

Adobe Reader: A programme to read and work with PDF files.

(MRU) Hive

- is a section that records files that have been visited lately.

ZIP:

- A file format for combining several files into a single package by compression.