

***Digital Forensics***

**Michael Sowemimo**

**White Paper**

**Abertay University**

**School Arts, Media, and Computer Games**

**\* Year E.g. 2016/2017\***

Contents

[1 Executive Summary 3](#_Toc468828463)

[2 Description of the crime 4](#_Toc468828464)

[3 Description of the investigation 5](#_Toc468828465)

[3.1 Job description and instructions 5](#_Toc468828466)

[3.2 Description of Recovered /Examined Items 6](#_Toc468828467)

[3.3 Methodology 7](#_Toc468828468)

[3.3.1 Acquisition 7](#_Toc468828469)

[3.3.2 Perseveration 7](#_Toc468828470)

[3.3.3 logical searching 7](#_Toc468828471)

[3.3.4 Production List and Associated Description 8](#_Toc468828472)

[4 Analysis 9](#_Toc468828473)

[4.1.1 Operating System 9](#_Toc468828474)

[4.1.2 System time and dates 9](#_Toc468828475)

[4.1.3 Unallocated space 9](#_Toc468828476)

[5 conclusion 10](#_Toc468828477)

[5.1 Equipment Required for Court Proceedings 11](#_Toc468828478)

[6 Appendices 12](#_Toc468828479)

[6.1 Appendix A – Images 12](#_Toc468828480)

[6.2 Appendix B - Documents 17](#_Toc468828481)

[6.3 Appendix C - Checklists 19](#_Toc468828482)

[6.4 Appendix D – Browser History 20](#_Toc468828483)

[6.5 Appendix E – user accounts 22](#_Toc468828484)

[6.6 Appendix F – installed Programs 22](#_Toc468828485)

[6.7 Appendix G - Operating System information 23](#_Toc468828486)

[6.8 Appendix H - Autopsy Timeline 24](#_Toc468828487)

[6.9 Appendix I - Altered file format 25](#_Toc468828488)

[6.10 Appendix J -Removeable Disk Drives 25](#_Toc468828489)

[6.11 Appendix K - Registry Files 26](#_Toc468828490)

[6.12 Appendix L – Verification 27](#_Toc468828491)

[6.13 Appendix M – Aggressive Bird Sound 27](#_Toc468828492)

# Executive Summary

Mr John Doe is known to have attributed in an absence act of birdwatching. The suspect has visited a web site in which related to the event of “chick sex”. The appropriate event has summoned the Abertay forensic team to assess the suspect hard drive and reimage the entire volume allocated. During the investigation, evidence eludes that the suspect has viewed a web page relating to abuse of natural wildlife. The evidence to support this statement is located at **Appendix D – browser history**.

An event with this magnitude should be brought forward to court, since the crime pertains to interactions online, the suspect is the owner of a windows server which can be found in **Appendix G – Perating System.** The crime could suggest that not only has partaken in illegal bird watching but the suspect could be planning to host birdwatching with the windows server.

# Description of the crime

John Doe is deemed susceptible to birdwatching and as a source of evidence the forensic team has sized the suspect Desktop. Many sources indicate that indeed john doe has partaken in some form of illegal birdwatching. The forensic team has obtained the suspect Desktop and implemented an internal inspect of the hardware and recorded the condition of the evidence**. Appendix A**- **Images** illustrates the state of evidence as soon as the alleged crime has taken place. Subsequently, the forensic team has obtained the hidden contents of the suspect hard drive by copying the whole disk drive to an image file.

The obtained image file was forensically assessed and based on the information gathered, the intelligence eludes that not only john doe is guilty of intense birdwatching but the suspect has co-workers that are working in connection to the malicious event. The following evidence defines many occasions whereas the suspect has implemented an indigenous amount of birdwatching, the malicious events are listed as followed:

* **Incident 1 –** between 16:25 and 16:51 on 2nd of February 2005, (unacceptable images of birdwatching) was deleted from the suspect drive and was found in the vol 3 unallocated space on john doe machine. The image can be obtained from **Appendix B logical search** – “*Volume 3 Unallocated – Recycle Bin”*
* **Incident 2 –**  On the 2nd of February 2005 (an email was sent relating to possible images of birdwatching and was found in the suspect thunderbird inbox. The image can be obtained from **Appendix B Logical Search –** “Email Messages”
* **Incident 3-** on the 2nd of February 2005 at 16:25 (inappropriate images of birds) was in the policy folder. The image can be found in **Appendix B logical search** – “winSxS”
* **Incident 4 -** On the 3rd February at 15:03 (an image of a bird offspring was identified) The image can be obtained from **Appendix B logical search** – “Images”
* **Incident 5 –** a record of a bird image was in the carved file folder which is in the unallocated volume but no access time was given, the image can be gathered from **Appendix B logical – “**Carved Files”
* **Incident 6 –** a download of a bird image was in bobs music folder on the 3rd of February 3rd 2005 at 15:46, the image can be verified from **appendix B logical search** – “my music folder”
* **Incident 7 –** between 15:04 and 16:57 the on 2nd and 3rd of February 2005 the main suspect has been watching inappropriate images of bird offspring. The image can be viewed in **appendix B** **logical search** – “my pictures”

# Description of the investigation

## Job description and instructions

I have been summoned to investigate a critical cyber case involving multiple events of extreme birdwatching. The case is very critical in the sense that the suspect has made many attempts to delete any significant evidence relating to birdwatching. As part of the forensic team at Abertay investigation department, my role in the investigation is to uncover may clues that will bring the cybercriminal into Justice. Bearing in mind that the seriousness of the case should not be overlooked since the cybercriminal has implemented of arbitrary of malicious events that should be brought forward to the court of law.

Consequently, Dr Ian Ferguson an experienced detective has asked for my professional assistance in relation to examining the suspect computer. To analyse and inspect any sensitive intelligence that will be apparent to the case at hand. Also, the investigation will address the position that john doe had during the events of birdwatching and allocating a plentiful amount of evidence supporting the injustice of john doe.

## Description of Recovered /Examined Items

**Altered extensions**

An unallocated space was removed from the suspect storage device but no records of time in which the unallocated device was deleted. The suspect tried to change the extension of the file to a format that may hide the suspects explicit birdwatching. The image could not be accessed by the Ubuntu operating system, although the image was accessed by mounting the whole Disk image as an external drive. The image appeared to be an executable but the mounted drive could revile the bird image which was in John does unallocated space. Evidence proves that john has modified the image/executable on the **9th of February 2005 at 11:28**, the image can be viewed in **Appendix J -Altered file format.**

**Base64**

An image was found in Joe Doe Inbox; it appears that there have been many images of exotic birds but each image is encoded with a base64. The suspect appears send images to another suspect named Bob Forbes, the email was received on the 9th February, 2005 at 11:08 and the evidence can have accessed in **Appendix D- browser history**.

**Access to suspect browser**

The suspect has been involved with some direct searching in relation to bird sex, this could infiltrate the reasoning behind the suspect intentions. Since this image could not open using a default browser. The image could be viewed using osforsencis and the web page was accessed, which can open the suspect web page in an internal browser, the source of the event can be accessed in **Appendix D -Browser history**. There is no information regarding the time and date in which the browser was accessed. The suspect may have used a facility to change created/Modified/Accessed dates.

**Suspect Operating System**

The suspect operating system was retrieved from the suspects storage drive, but was proven to be cumbersome in relation to the extracting sources of additional evidence that may prove any other bird watching events that the suspect may have contributed. Instead the windows operating system image was mounted as a hard drive and from there it was possible to revile the suspect internal assets. The suspect has made an additional user called James bond. Although the user account appears to be locked, this could be since john doe may be hiding secret operations that could be an expansion of birdwatching. The source can be accessed in **Append E – installed programs.**

## Methodology

### Acquisition

Since the crime relates to bird watching of some degree, the investigative process needed more intelligence on the configuration of the hardware during the crime. Screenshots was taken to remove any false positives that may weaken the validity of the crime. While the suspect’s Desktop was turned off, forensic copy was extracted from the suspect drive. A write blocker is used to gain a read only copy of the suspects drive without damaging the contents. The suspect appeared to have internet connection, since the Desktop is connected to another port on a specific network. The evidence can be **Appendix A – images.**

The connection to the port may be the suspect source of medium of accessing the illicit content of birdwatching. Moreover, the suspect could have used the connected port to host the windows NT server. This could also suggest maybe the suspect may have downloaded the bird images just so that each image could be hosted on a server, this justifies possible business plans to share images with an unknown source for commercial use.

### Perseveration

The forensic copy of the Suspect Disk Drive was converted to a Raw image to which the internal elements of the suspect Disk Drive can be accessed. A hash verification was initiated to check that the image is the exact copy of the original. The screenshot can be accessed in **Appendix L – verification.**

### logical searching

The logical search involves mounting the image as associative device of the operating system. The suspect operating system was mounted as a hard drive. The operating system appears to have another user names James bond. Although evidence illustrates the operating systems belongs to the accused suspect. Furthermore, evidence eludes that the suspect hard drive contains a substantial amount of bird images. The logical search also provides answers to the segregation of the operating system and the remaining file system. With that been said, the suspect has encrypted the “james bond” account with trycrypt . The suspect could be hiding hidden images bird watching or any other malicious activity surrounding Birds.

### Brute force Search

Once the image was mounted, a structured search was initiated to allocate file extensions such as jpeg, pdf, and audios. That could uncover the suspect criminal activity, as well as providing a better standpoint that will enhance the effectiveness of the evidence. During the search, there has been signs of birdwatching in the browser history. The brute force indicates that the most of the images have been downloaded from the browser. Also, the suspect has appeared to have used a Trojan horse which could have been used to erase component on the file system, to mask additional event in relation to bird watching. This evidence can be viewed in **appendix M -Trojan horse**.

### Production List and Associated Description

|  |  |
| --- | --- |
| Digital Item | Descriptions |
| Images in the unallocated Space - **Appendix A – Carved Files** | Explicit images were in the unallocated space, the suspect may have tried to conceal any evidence relating to the suspect bird watching. The defence argument can be ordered as followed:   1. The fact the images was in volume 3 of the hard drive which was unallocated. This could suggest the suspect tried to delete the allocated space containing the explicit bird images. 2. The fact that there is no recorded time of when the allocated space was deleted. 3. The hard drive seems to have unallocated space, which could question what other evidence the suspect could be hiding |
| History relating to suspect viewing inappropriate images in local browser - **Appendix D - Browser** | No access time was given for the malicious event, the suspect appears to have some interest relating to “Chick sex”, arguments could be made to suggest that the suspect have “chick sex” in mind. |
| Advanced registry – **Appendix E – User Accounts** | The suspect may have used to clean the computers clock, many occurrences that some retrieved evidence has no access time recorded. The suspect may have tweaked registry to remove any traces that could deduce possible start up times for the suspects software. |
| Aggressive Bird sounds – **Appendix M- Aggressive Sound** | The suspect appears to have downloaded an “Aggressive Bird” from msn.com on the 9th of February at 17:01 pm. The sound contains a screeching voice of what appears to be a young bird. |

# Analysis

### Operating System

John Doe Appears to be the owner of the operating system, this can be shown in **appendix D**- Operating System. Although most of the images was in the suspect unallocated space, questions are directed towards the possible motive behind why the suspect did not delete the operating along with the unallocated space that was examined. The operating system appears to be constructed as a client/server podium. The reason that the signs indicate that the suspect could have removed the operating system from the third partition of the main drive, to preserve any other bird images that may be stored on the operating system.

With that been said, the evidence is concrete in response to the fact that the suspect tried to delete access points to the operating system on the suspect Disk Drive. This proves the suspect intents to keep the bird images secure and systemically hindering any access to the malicious images. The evidence exposes the arbitrary amount of bird images found in the suspect Carved files folder located in volume 2 of the suspect operating system. Strong evidence concludes that john doe was watching illegal images of birds using his operating system and may have used his machine, also using the suspect may have used an optimized registry Optimizer to eradicate system clock during the explicit birdwatching event. The question remains to the motive behind changing the system clock, it may be possible that the suspect has secret motives behind the recollected images.

### System time and dates

It is apparent during the investigation that the suspect has used a registry optimizer to change the dates of the system. This has proven to be a problematic scenario, since there is structured time analysis of how the images found on the suspect operating during the time of the suspect browsing history. There is no correlation to when the suspect accessed the browser. The suspect may have used the optimized registry tool, to relinquish any other browsing history that may have contributed to the suspects extreme bird watching, **Appendix D-Browser History**.

### Unallocated space

The suspect drive has deleted multiple volumes of the allocated space of the suspects storage device, in which the suspect has adhered to multiple events of birdwatching. As mentioned earlier the windows operating system may have been part of the suspects storage drive and maybe deleted the operating systems partition as a method to break any chains that may summarize the main objectives behind the deletion of the allocated space that operating system was hoarding. The unallocated space has series of birdwatching images and documents, this evidence can be in **appendix -A images**.

# conclusion

The forensic investigation has proven that john doe has performed several events of birdwatching, the suspect has used many avenues to procedures to obscure any inequalities of the suspect filesystem. As mentioned the suspect has used registry optimizing tools to change the system time of the system time of the suspect drive. Changing the system time questions the if the suspect may have endeavoured a chain of malicious events that contain additional data relating to the computerized crime. Although, the forensic evidence eludes that john doe is liable for the inpatriate Images of birdwatching.

The methodology reflects that the medium that was used during the event is forensically sound and there were no alterations to contaminate the evidence. The evidence supplied in **Appendix -A – Images** conveys that the suspect has an unusual liking to bird watching and seems to derive an addiction to their existence. Furthermore, there evidence that the suspect seems to enjoy the chirping of birds, the evidence can be deduced in **Appendix M –** **Aggressive Bird Sound**. Further investigation is required to address the encrypted folder found in suspect windows account, although an astronomical amount of evidence eludes that the suspect has secret intensions for the vast supply of bird images.

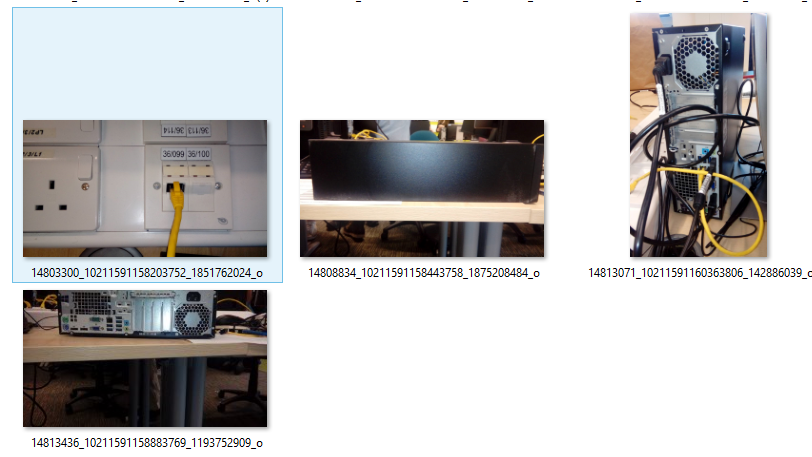
## Equipment Required for Court Proceedings

|  |  |
| --- | --- |
| **Equipment** | **Function** |
| Desktop Computer | Digital hardware to install forensic tools |
| Suspect Hard Drive | Source of evidence for the case |
| Write Blocker | permits read only access to data to the suspect device without damaging the integrity |
| Osfmount | Forensic tool used to mount disk images |
| OSForensics | Forensic tool used to extract forensic data or retrieve information from computers |
| Regviewer | Platform for examining registry files from any platform |
| Autopsy 4 | Forensic Ultity used to investigate disk images |

# Appendices

## Appendix A – Images

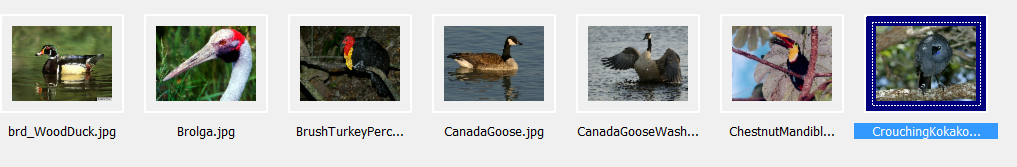




*Volume 3 Unallocated – Recycle Bin*



*WinSxS*

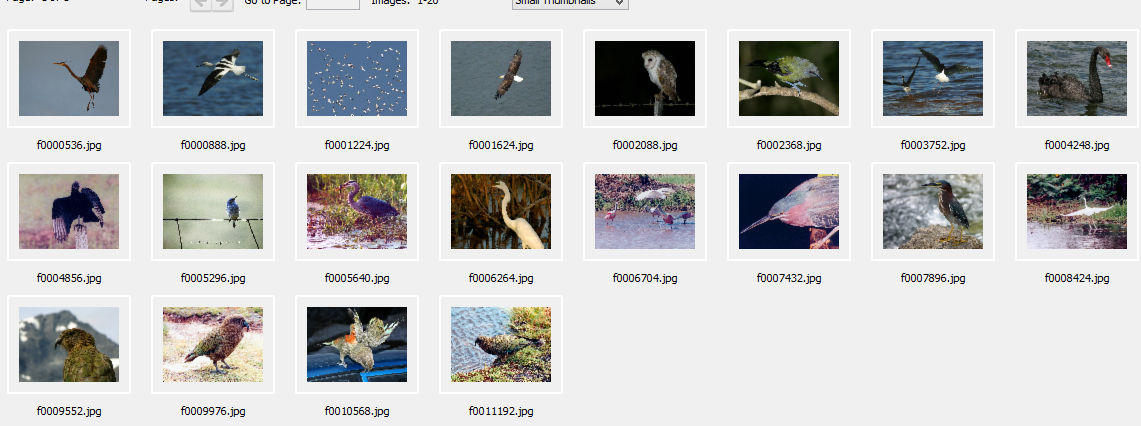


*Images*



*Carved Files*

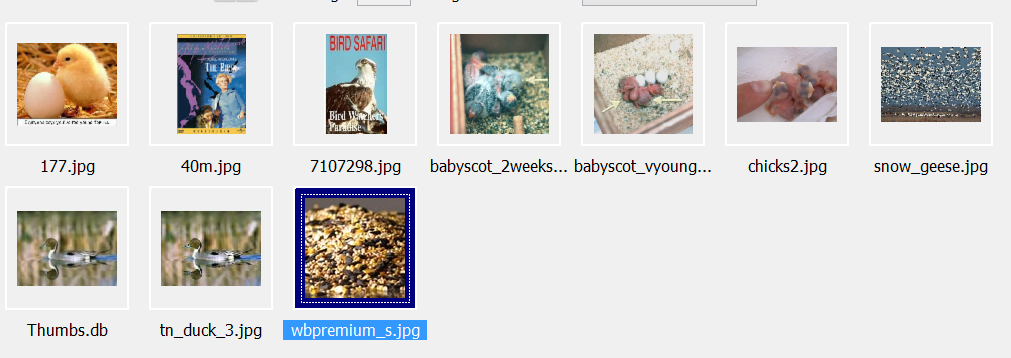




*Bobs My music Folder*



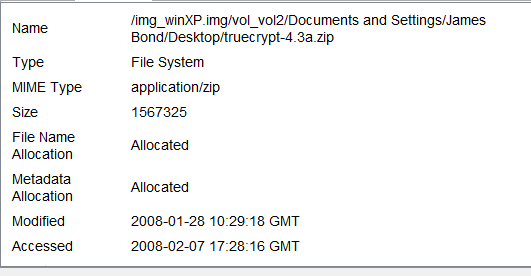
*John Doe Picture Folder*



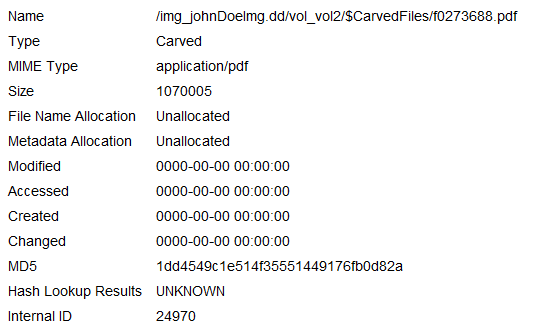
*John Doe browser Bookmark*



## Appendix B - Documents



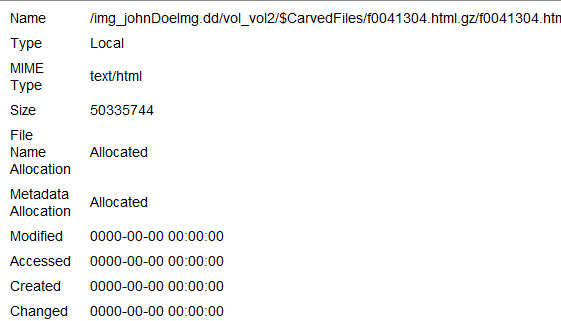


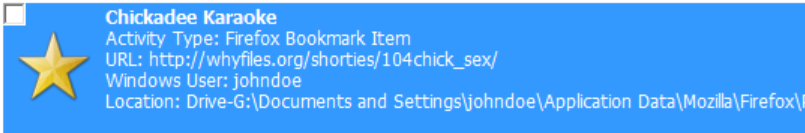


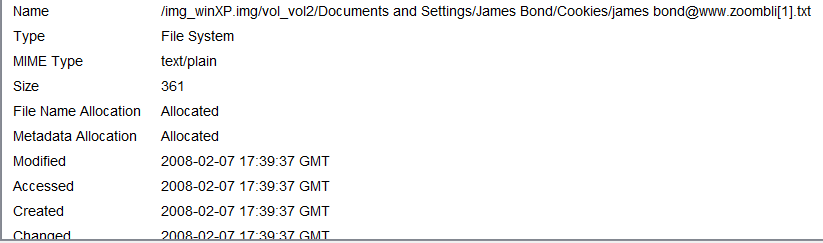
## Appendix C - Checklists

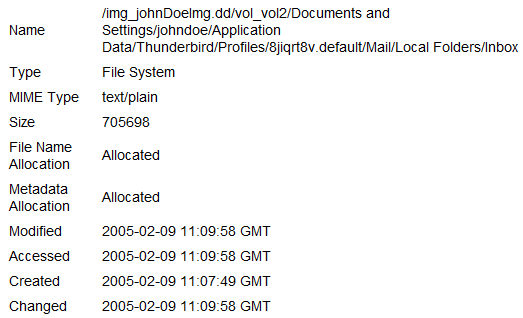
## Appendix D – Browser History

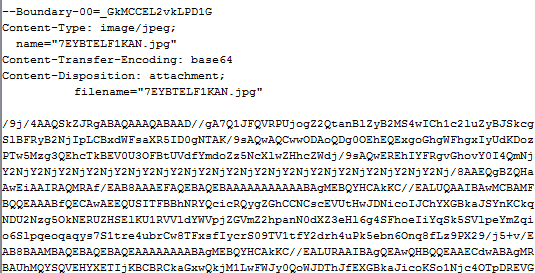




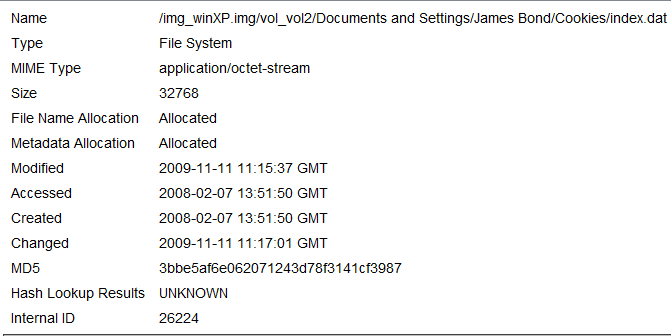




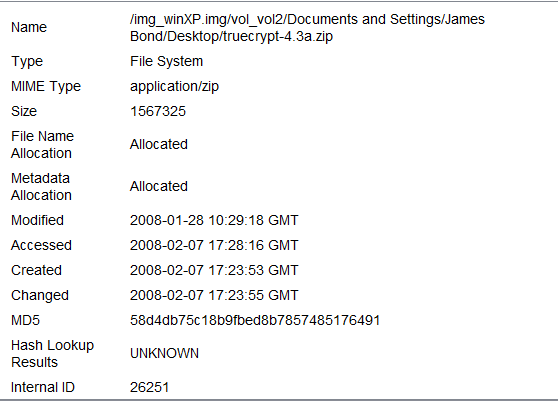




## Appendix E – user accounts

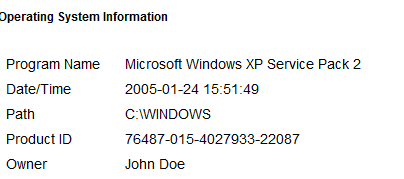


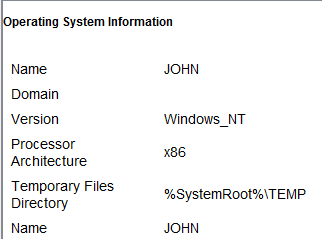
## Appendix F – installed Programs



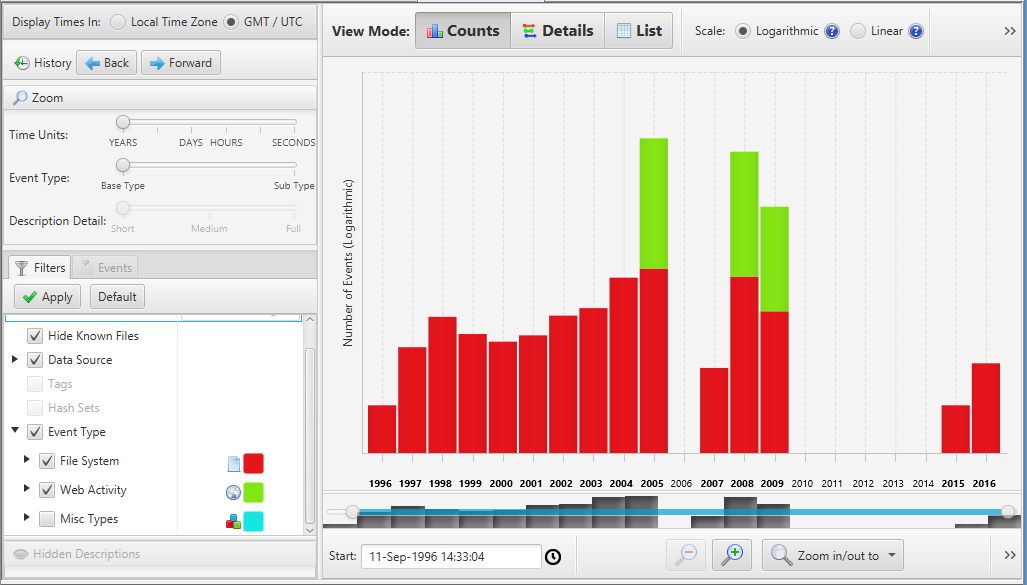


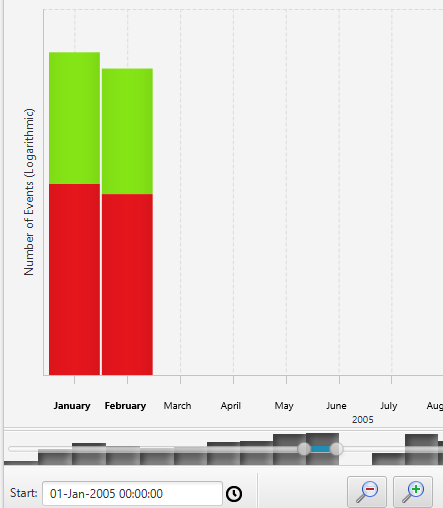
## Appendix G - Operating System information



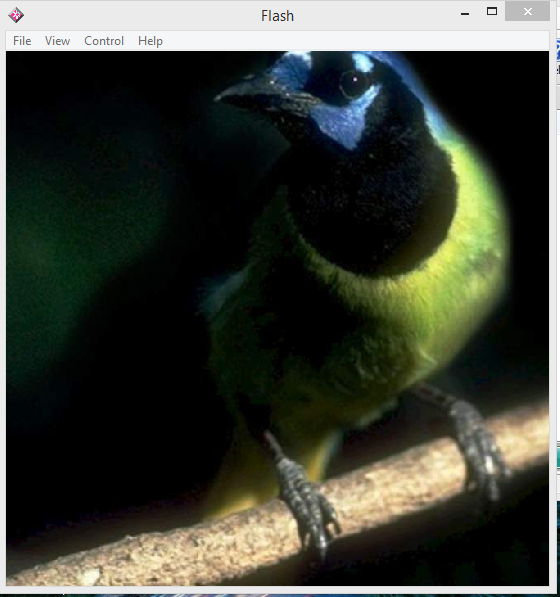


## Appendix H - Autopsy Timeline

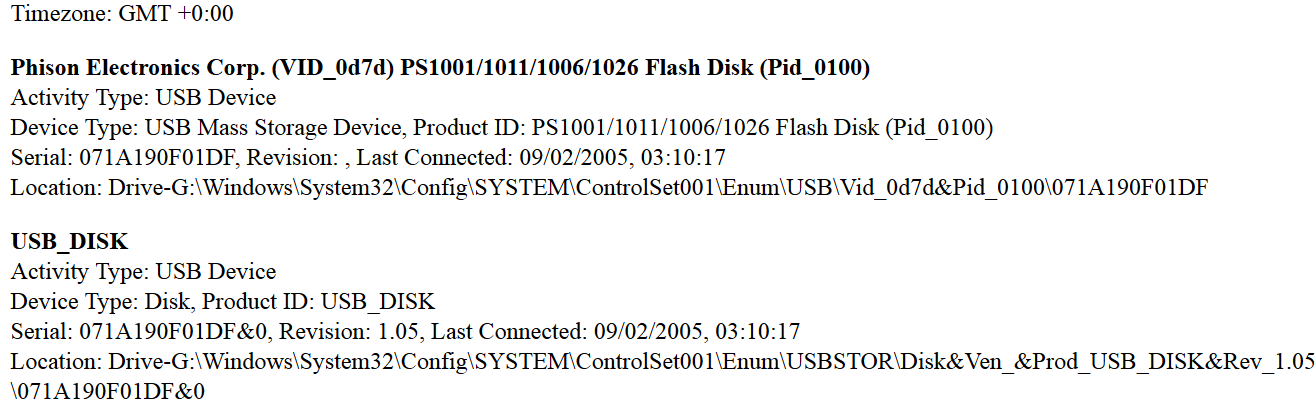




## Appendix I - Altered file format

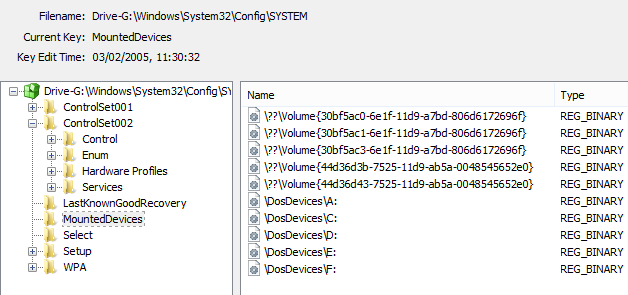


## Appendix J -Removeable Disk Drives

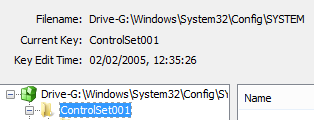


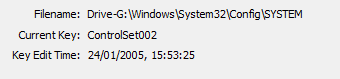
## Appendix K - Registry Files

Mounted Devices

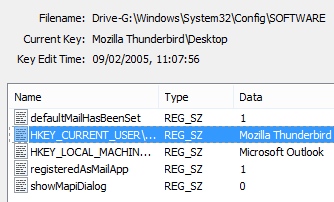


Usb Devices



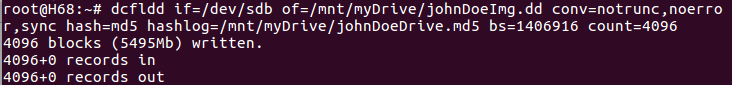


Thunderbird

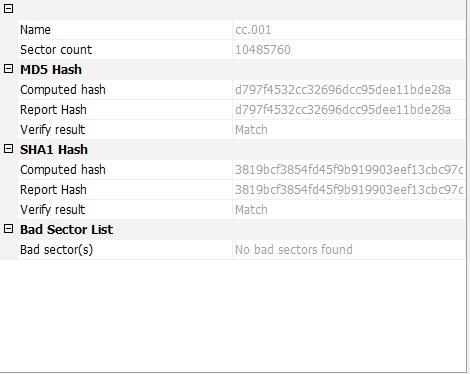


## Appendix L – Verification

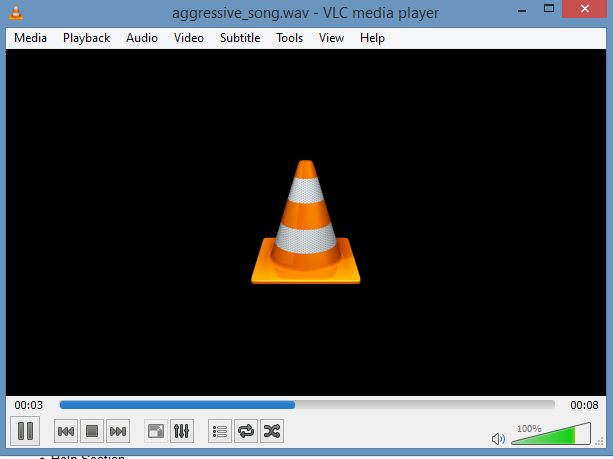
### Imaging



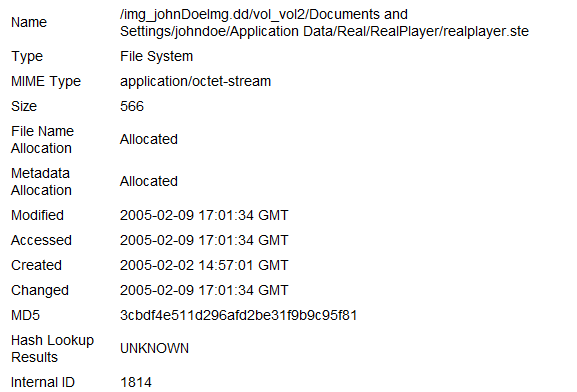
### Hashing



## Appendix M – Aggressive Bird Sound







## Appendix n -Trojan Horse

