Joint Report of

Matthew Allan (1702675)

And

Ekku Jokinen (1703641)

CMP209 Digital Forensics

Case Against: John Doe

Case Reference Number: EJMA

Contents

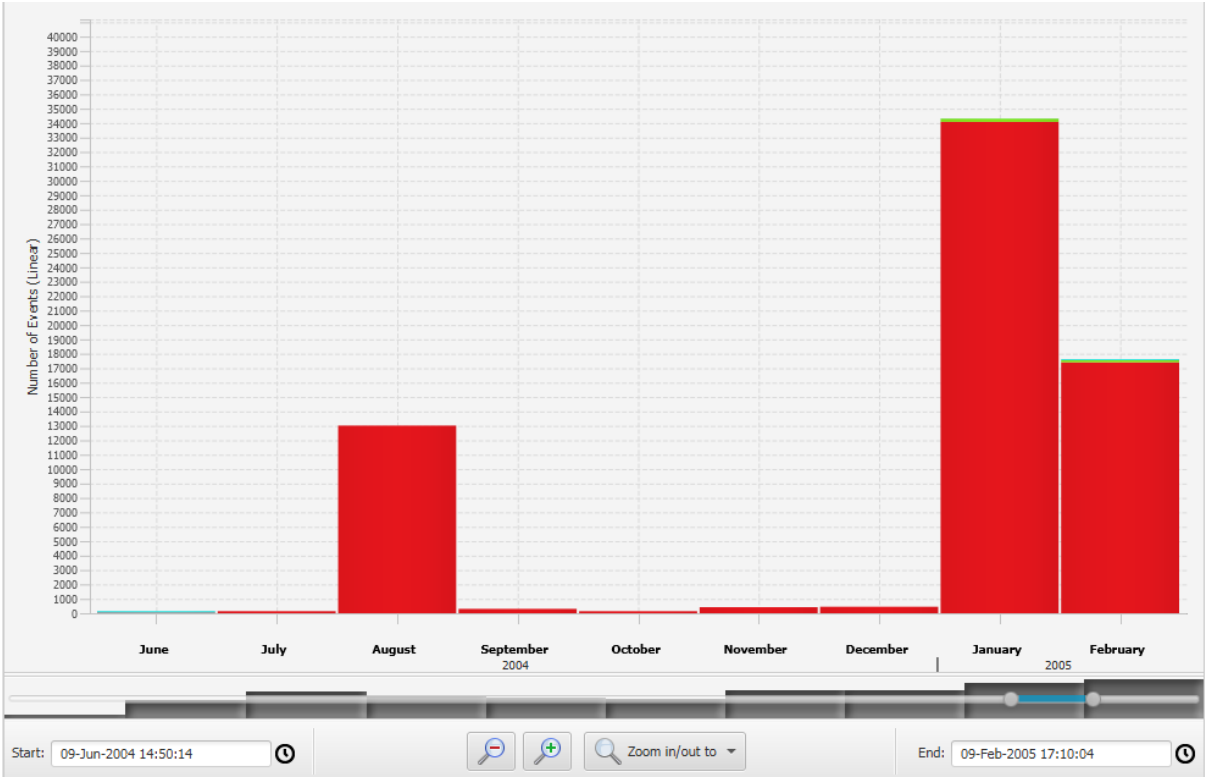
1. Summary

The hard drive of the suspect John Doe was seized and handed over to be forensically investigated. The hard drive was suspected to contain illicit images and material relating to birds. The goal was to recover any illicit material that was present or removed and determine the ownership of that material. The hard drive was analyzed and contained multiple images and documents relating to birds, including websites that had been visited which contained bird guides. Two E-mail conversations were recovered containing multiple exchanged bird images.

A total of 133 bird related images were recovered from the suspect hard drive, of which 123 had unique hashes.

2. Description of Crime

2.1. Timeline of events



The timeline above shows the three major episodes of events when user activity was high in relation to the investigation.

2.2. Notable Incidents

2.2.1. Incident 1 – Creation of images using cameras

Between 30th Dec 2002 12:28 and 27th June 2004 18:29, 102 Images were created using Sony & Cannon cameras, of which 47 of them were unique. The majority of these images were of ornithological nature (see *Appendix 1).*

2.2.2. Incident 2 – Illicit material is deleted

On 2nd Feb 2005 at 11:03, three documents previously located at 'C:\Documents and Settings\johndoe\My Documents\', were deleted from the machine (see *Appendix 11 Figure 2).*

2.2.3. Incident 3 – Downloading of illicit bird material

Between 2nd Feb 2005 15:12 and 3rd Feb 2005 15:06, multiple websites of illicit nature were visited and files were downloaded (see *Appendix 7 Figure 3)*. The user also performed multiple google image searches (see *Appendix 7 Figure 4).*

2.2.4. Incident 4 – Creation of encrypted file

On the 2nd Feb 2005 at 16:46 an encrypted file called birdpics.gpg was created, it contained a zipped file with 5 bird images inside (see *Appendix 1 Section 1.6.7).*

2.2.5. Incident 5 – Use of removable media

Between 3rd Feb 2005 15:06 – 15:43. A removeable storage device was used to hold a downloaded audio file (aggressive_song.wav), and a separate file (blue_bird2.jpg) was deleted from the storage device which was later recovered from the recycling bin from the unallocated space under a new name (Df1). (see *Appendix 11*).

2.2.6. Incident 6 – E-mail conversation

On the 9th Feb 2005 at 11:08am, an email exchange between Ben Forbes - ben@example.org and jdoe@example.com consisting of 3 emails all containing bird related material, of which 2 emails contained a combined total of 8 bird images, one being a duplicate. There was also a second email exchange between Bird Fanciers – mailinglist@birds.example.com and jdoe@example.com, which was a subscription mailing list (see *Appendix 10* for E-mail contents).

2.2.7. Incident 7 – Viewing of illicit materials

On the 9th Feb 2005 between 11:28 – 17:07, Bird materials stored on the machine at location 'C:/Documents and Settings/johndoe/My Documents/' were accessed via Internet Explorer. (see *Section 2.3.4).*

2.3. Description of Investigation

2.3.1. Job Description and Instructions

We were tasked with assisting Abertay Forensics on the case of John Doe. We were provided with a single Hard Disk Drive (HDD) which had been seized from a computer within John Does' premises. The HDD was suspected to contain illicit material of an ornithological nature, and we were tasked investigating ownership of the material.

2.4. Methodology

2.4.1. Acquisition & Preservation

The evidence HDD was handed to us in our forensics lab and photographed for evidence. It was a Seagate 40 gigabyte HDD (see *Appendix 3).*

The first step was to calculate a MD5 checksum of the suspect hard drive. This is a sequence of letters and numbers that will uniquely identify the drive based on its contents. If any information changes the MD5 hash will also change. As the hardware was presented in a powered off state, live imaging was not required. Static imaging was used to create a .dd file of the exact contents of the drive. By using a write blocker, it was assured that no data would be modified during this process.

Creating this exact copy allows investigations to be carried out on the drive without ever modifying the original evidence. Once the imaging process was complete, an MD5 checksum of the image was calculated to validate its integrity and forensic soundness (see *Appendix 4).* The checksum of the hard drive was compared to newly calculated checksums of the forensic image throughout the investigation.

2.4.2. Anti-Virus Scan

A virus scan was conducted to determine if any malware existed which could potentially be used to infect the host with the illicit material. Anti-Virus software called clamAV was used for the scan. The scan results showed three files were infected, which were thought to be false positives as the related files were all a part of a media suite called Real Player (see *Appendix 2).*

2.4.3. Physical & Logical Searching

Two different types of searching can be performed with the forensic image of the drive.

2.4.3.1. Physical

A physical search can be performed using the forensic image produced as a single file, using software called Autopsy 4 a search can be performed without the knowledge of filesystems and partitions. This type of search allows for more complex searching to be performed and the possible recovery of deleted/hidden data (see *Appendix 6 Figure 1).*

2.4.3.2. Logical

Logical searching involves treating the forensic image as a drive and mounting its filesystem. This allows partitions and registry files to be viewed. We calculated a MD5 checksum of every file mounted in the partition. The next step was to find out which operating system was active on the drive; this was done by navigating the software registry file using a tool called RegViewer. It was discovered the active operating system was Microsoft Windows XP Service Pack 2 (see *Appendix 5 Section 6.5.2).*

With the operating system information known, an MD5 checksum was calculated of every file in a clean install of Windows XP and compared to the list of files on the suspect drive. A new list was produced of all files which did not match standard Windows XP files, this is any modified or newly created files since install (see *Appendix 6 Figure 2).*

2.5. Search & Analysis

2.5.1. Disk Analysis

The first step of analysing the disk was examining the partition table, using autopsy provided a list of partitions labelled:
Volume 1 (vol1) – Unallocated: 0-62
Volume 2 (vol2) – NTFS/exFAT (0x07): 63-6136829
Volume 3 (vol3) – Unallocated: 6136830-11255327
See *Appendix 6 Figure 1.*

Even though Volume 3 shows a large amount of unallocated space (meaning no filesystem is present and no files are intended to be stored), there are numerous illicit bird images inside that space, (see *Appendix 1 Section 6.1.4)*. These images could have been purposely concealed at this location in an attempt to hide evidence.

2.5.2. Camera Images

Examining metadata on the suspect drive revealed that the images were taken using three models of cameras:

- Sony Cybershot
- Cannon EOS-1DS

- Cannon PowerShot SD100

2.5.2.1. Sony Cybershot

There was only one image taken using the Sony Cybershot camera. The image was recovered through the inbox of the Thunderbird Mail Client. The image name was obfuscated in attempts to hide it from forensic analysis, the file extension was changed from '.jpg' to '. _J_P_G_'. Image can be viewed at *Appendix 1 Section 6.1.1.*

2.5.2.2. Cannon EOS-1DS

There was only one image taken using the Cannon EOS-1DS camera. The image was recovered from two different locations on the disk, both inside the unallocated space. Image can be viewed at *Appendix 1 Section 6.1.2.*

2.5.2.3. Cannon PowerShot SD100

There were 45 images taken using the Cannon PowerShot SD100. They were recovered from both the allocated partition and the unallocated space using a tool called Foremost. 27 out of the 45 images directly related to birds and birdwatching. The other photos include groups of people indicating they were there for a group birdwatching expedition. Images can be viewed at *Appendix 1 Section 6.1.3.*

2.5.3. Registry Analysis & User Accounts

Registry analysis is a vital part of any investigation, each registry file holds valuable information regarding user accounts, ownership and general information on what happened on the computer. A tool named RegRipper was used to convert each registry hive into readable formats for easier examination.

The Security Accounts Manager (SAM) file hold all information regarding user accounts and login information, including timestamps of previous logins. Analysis of the file revealed three user accounts registered;

- johndoe
- jane
- bob

The user accounts jane and bob were both created on Wednesday 2nd Feb 2005 between 12:30-15:30. Both accounts' last recorded login was the day after creation within a two hour window of each other, this was the only login ever recorded for these two accounts. The johndoe administrator account was created Mon 24th Jan 2005 at 15:56, the account since that time has been logged in 21 times which indicates johndoe is the main user account of this computer. (see *Appendix 5 Section 6.5.1)*.

The Software file holds information about recently installed software packages and windows information. Analysing this file revealed John Doe is the registered owner of the computer, adding to the indication that johndoe was the main user account (see *Appendix 5 Section 6.5.1).*

Out of all the installed software packages there was a number of interesting ones, which are listed below;

- NetMeeting (Skype Style Video Chats)
- RealPlayer 6.0 (Movie Player)

- Mplayer2 (Movie Player)
- RealJukeBox 1.0 (media file organizer, part of RealPlayer software)
- Anti-Virus MacAfee (anti-virus software)
- GnuPG (used for encrypting files)

The software file also showed a timestamp for the last time each user account wrote to disk, (see *Appendix 5 Section 6.5.1 Figure 3).*

The system file holds information related to device data. Searching this file revealed there was a removable storage device removed from the computer which was mapped as the 'E' Drive. It was later discovered that this removable drive held illicit bird images which were encrypted using GPG encryption in attempts to hide the evidence. No further analysis of the drive could be performed as it was not recovered from the crime scene.

The NTUSER.DAT registry file shows recently viewed documents by the most recently active user account, in this case it was johndoe. Several of the illicit files which were recovered from the drive were seen to have been accessed by the user account johndoe (See *Appendix 5 Section 6.5.2).*

2.5.4. Browser History Reconstruction

2.5.4.1. Internet Explorer

Analysing the web browsing history of the user accounts resulted in many interesting findings. The history files for the Internet Explorer browser are formatted as .dat files named index and can be found in 'C:\Documents and Settings\<username>Local Settings\Temporary Internet Files\Content.IE5'. The tool Pasco was then used to convert the content into a readable format.

For the user account bob there was only one entry, it was a word document called "Dear Fred.doc" but it doesn't seem suspicious (see *Appendix 7 Figure 5)*. The user account jane had no entries in their .dat file. The user account for johndoe had multiple entries, there was only a few external URLs, the majority of entries were windows file paths to locations on the drive containing illicit material (see *Appendix 7 Figure 2).*

2.5.4.2. Mozilla Firefox

Firefox's history and downloads file can be found in 'C:\Documents and Settings\<username>\Application Data\Mozilla\Firefox\Profiles'. The history logs are stored as .dat files and were converted into a text files for analysis. Inside the log there were multiple entries of visits to websites with illicit material. (See *Appendix 7 Figure 4* for URLs).

The download logs are stored as .rdf files and contained information about file downloads and the URLs from which they had been downloaded from (See *Appendix 7 Figure 3* for URLs).

Based on the data shown it seems as if the johndoe user account was using Firefox to download and browse for illicit material and Internet Explorer to view the material.

Also, a total of 13 unique bird images were discovered inside the Firefox cache file. They were embedded inside of multiple .gif files stored while browsing bird related websites (see *Appendix 1 Section 6.1.12).*

2.5.5. Email

Throughout the investigation multiple E-Mail addresses were discovered, many had no significance with regards to the case. Below is a list of the interesting ones related to the case;

- ben@example.org
- ben@mozilla.org
- ben@netscape.com
- jdoe@example.com
- jdoe@mail.example.com
- jdoe@netscape.net
- johndoe@example.com
- johndoe@microsoft.com
- johndoe@netscape.net
- johndoe@office.microsoft.com
- johndoe@real.com
- mailinglist@birds.example.com
- mail@orientalbirdclub.org

There were multiple E-mail conversations as described above in Incident 6 which involve some of the above E-mail addresses (see *Appendix 10).*

2.5.6. GPG Encrypted File

A .GPG file was located at 'C:\Documents and Settings\johndoe\My Documents' named birdpics.gpg. The file was encrypted using a public/private key and a password. Because the HDD recovered contained both the public and private key files (pubring.gpg & secring.gpg), we were able to obtain the password, these files were located at 'C:\Documents and Settings\johndoe\Application Data\GnuPG'. The password turned out to be 'arran' (shown in *Appendix 11 Figure 3)*.
There was 3 different ways to obtain the password:

- Brute Force: The secring.gpg file's password can be guessed by using a tool called John the Ripper which tries every possible combination of characters and numbers together.
- Dictionary: A wordlist was created using the forensic image by running it through a command called strings which extracts all ascii words present in the image. The output file is used as a dictionary to perform password attempts using John the Ripper.
- Thunderbird Mail: The password was hidden inside a file located in johndoes thunderbird mail client. The password was encoded using Base64. Decoding it reveals the password.

Entering the recovered password, revealed a .tar.gz file, once it was uncompressed 5 illicit bird images were found (shown in *Appendix 1 Section 6.1.7).*

2.5.7. Fake .dll actually .zip archive

While searching the mounted filesystem, inside the C:\WINDOWS folder a number of illicit materials was discovered. Among the discovered files there was an unusual .dll file which was named after a bird. We ran the command 'file' to gather metadata and identify the real file type, the output was a .zip archive (as shown in *Appendix 1 Section 6.1.8 Figure 8).* After changing the file extension to '.zip', an archive containing 7 illicit bird images was revealed (See *Appendix 1 Section 6.1.8).*

2.5.8. Image Hidden Inside .exe File

Using Autopsy revealed multiple mismatch file extensions, one of particular interest was a .exe file which was being recognized as a jpeg image. The location of this exe file was

'C:\WINDOWS\mui\FantailFrontView.exe'. Simply changing the file extension to '.jpg' revealed a hidden image (Shown in *Appendix 1 Section 6.1.9).*

2.5.9. ODBC.ini has hidden text inside using comments

There was a .ini file mentioned in multiple logs including recently accessed documents and Internet Explorer (IE) history. The IE history logs revealed a file path which we were able to navigate to and view the contents of this file in a text editor. The file was a Windows configuration file by default but included in the file was hidden text about bird material which was written using comments so it could remain undetected (See *Appendix 8* Section 6.8.1).

2.5.10. Kakapo.ram & dawn.ram

There was a .ram file was located at 'C:\Documents and Settings\johndoe\My Documents' which was named after a bird. The file contained a link to an audio file stored on a website about birds. The file is used by the Real Media Player. The URL was invalid during the time of investigation, the website was available to view through a new URL but unfortunately the audio file was unavailable (See *Appendix 9 Figure 1 & 2).*

Dawn.ram was discovered in the Mozilla Firefox downloads log, the website which hosted the file is no longer accessible. There was no archived copy available to recover the file (see *Appendix 9 Figure 4).*

2.5.11. Aggressive_song.wav

A .wav audio file was discovered at 'C:\Program Files\MSN\' containing sounds of a bird singing (see *Appendix 9 Figure 3)*, it had been referenced in multiple log files including IE history log and a registry file that details the most recently viewed documents.

2.5.12. Birds.zip

Birds.zip was mentioned in multiple locations through the drive and there was a .lnk file linking to Birds.zip. The original location was 'C:\Documents and Settings\johndoe\My Documents' but the archive had been deleted and was unrecoverable through the drive. While searching through browser logs for Mozilla Firefox the download link was recovered (see *Appendix 7*, however it was unavailable at the time of the investigation. An archived version of the .zip file was successfully downloaded using a cached version of the website. Inside the archive was a .exe file named tx_birds.exe, which could also be located on the drive at 'C:\WINDOWS' under the same name. Before obtaining the archived .zip file there was no way of connecting the two together. Running the .exe file revealed a flash slideshow consisting of 9 illicit images of birds (as shown in *Appendix 1 Section 6.1.10*).

2.5.13. Documents

2.5.13.1. Doc1.doc

A Microsoft Word document was recovered which contained an image of a bird which had been zoomed in. Opening the word document allowed for the image to be zoomed out and the full bird image viewed (see *Appendix 8 Section 6.8.2 Figure 1).*

2.5.13.2. Birdwatching.doc

A Microsoft Word Document was found located at the root of the NTFS partition called birdwatching.doc. This document contained detailed information regarding birdwatching trips to Thailand. The information included contact details of other bird related organisations (see Appendix 8 Section 6.8.2 Figure 2).

2.5.13.3. Guide.doc

A Microsoft Word Document which was recovered from the unallocated space (Volume 3) named guide.doc. Its contents are a guide for beginners in birdwatching and how to have fun doing it. The guide was written by another birdwatcher by the name of 'Pete Dunne' (see *Appendix 8 Section 6.8.2 Figure 3).*

2.5.13.4. PDF

Using the file carving tool 'Foremost', three bird related PDFs were recovered from the drive. The contents of these PDFs were different bird related guides. One was about Birding sites around Perth, one was about Birds at the University of California Botanical Gardens (UCBG) and the third was about Birds in Porter County (see *Appendix 8 Section 6.8.3).*

2.5.13.5. TXT

One .txt file named nestboxtips.txt was discovered at 'C:\Documents and Settings\johndoe\My Documents'. It contained information on bird nests such as how to maintain them and prime locations for them (see *Appendix 8 Section 6.8.4).*

2.5.14. Website pages

2.5.14.1. aa010703a.htm

A saved offline copy of a website which contains detailed instructions on how to build a bluebird nest box (see *Appendix 8 Section 6.8.5 Figure 1)*. The URL was listed in the Mozilla Firefox history logs.

2.5.14.2. ostbk2b2.htm

A saved offline copy of a website which contains information about caring for birds of different ages (see *Appendix 8 Section 6.8.5 Figure 2).* The source URL was listed in Mozilla Firefox history logs.

3. Conclusion

In total there was 150 illicit files of varying severity recovered. From those files there was 133 images, three audio related files, seven text documents and seven miscellaneous files of different types.

The registry files showed the computer is registered under the same name as the accused John Doe. Many of the recovered files were located inside folders belonging to the johndoe user account. More files of birds were discovered in an unallocated space on the hard drive and some were recovered after being deleted. Other files were discovered in various locations throughout the filesystem.

There was extensive evidence showing multiple visits to bird related websites, as well as material being downloaded onto the johndoe user account which was recovered through Mozilla Firefox and Internet Explorer history logs.

Significant effort was made to conceal bird images using a variety of methods including renaming files, hiding material inside regular files and encrypting a zip archive of images.

Based on the timestamps of the user accounts, johndoe was used to search, download, access, move and delete files of illicit nature. The same user account is evidently the main user of the computer based on the significant number of logins when compared to the single logins of the other two user

accounts, it is also the only administrator account present. The other two user accounts showed no suspicious activity.

It is very unlikely that malware was the cause of the illicit material being present on the hard drive as the anti-virus scan showed no significant threats.

4. Equipment Required for Court Proceedings

- **Evidence**

  The seized hard drive

- **Specialist Equipment**

  A forensic workstation with several tools & operating systems installed.

  - Linux Distribution – Create and mount a forensic image of the hard drive

    GPG – Allows for the GPG files to be decrypted

    Clam Anti-virus – For running an initial scan of the file system

    RegRipper – Allows for registry files to be in a readable format

    Pasco – Allows for .dat browser history files to be in a readable format

  - Windows Operating System

    Autopsy 4 – A specialist digital forensic software used for evidence recovery using the forensic image file

    Web Historian – For viewing browser history files

- **Equipment**

  Keyboard, Mouse, Monitor

5. Terms

Encryption: The conversion of a readable file into an unreadable one. Used for preventing unauthorized access.

File system: The way files are organized into locations and folders in an operating system.

GPG file: An encrypted file generated by GnuPG. Can be opened using a private key and password.

Mounting: A disk image can be mounted after which it is accessible as a storage partition on the file system.

MD5 checksum: a 128-bit hash value calculated using the common MD5 hashing function. The unique value can be used to identify a file and if it's modified even slightly, the hash value changes.

Metadata: Data about the file. Can include last access time, file owner information, file type and various other bits of information.

Partition: An independently formatted area of storage.

Unallocated space: Space on a hard drive that isn't used as storage space on the active file system.

6. Appendices

6.1. Appendix 1 – Images of Birds

6.1.1. Image from Sony Cybershot Camera

Figure 1: feedingthebirds.jpg | Obfuscation Removed
_B_C_7_ _f_e_e_d_i_n_g_ _t_h_e_ _b_i_r_d_s_._J_P_G_ | Original File Name

6.1.2. Image from Cannon EOS-1DS Camera

Figure 1: BellbirdJumpingOffBranch.jpg | First recovered name f0002368.jpg | Second recovered name

6.1.3. Images from Cannon PowerShot SD100 Camera

Figure 1: 02791503.jpg

Figure 2: 02792407.jpg

Figure 3: 02815079.jpg

Figure 4: 02903551.jpg

Figure 5: 02952815.jpg

Figure 6: 02962639.jpg

Figure 7: 02963839.jpg

Figure 8: 02997495.jpg

Figure 9: 03018151.jpg

Figure 10: 03018663.jpg

Figure 11: 03030271.jpg

Figure 12: 03062263.jpg

Figure 13: 03074343.jpg

Figure 14: 03088231.jpg

Figure 15: 03112503.jpg

Figure 16: 03114495.jpg

Figure 17: 03163663.jpg

Figure 18: 03180791.jpg

Figure 19: 03181303.jpg

Figure 20: 03181927.jpg

Figure 21: 03184607.jpg

Figure 22: 03185759.jpg

Figure 23: 03186407.jpg

Figure 24: 03188831.jpg

Figure 25: 03222767.jpg

Figure 26: 03241879.jpg

Figure 27: 03343407.jpg

Figure 28: 03348175.jpg

Figure 29: 03393167.jpg

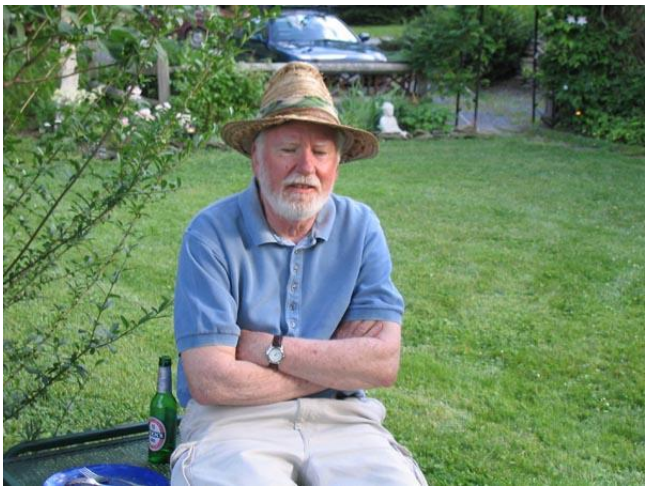


Figure 30: 03420671.jpg

Figure 31: 03477407.jpg

Figure 32: 03499095.jpg

Figure 33: 03516711.jpg

Figure 34: 03518439.jpg

Figure 35: 03528407.jpg

Figure 36: 03538975.jpg

Figure 37: 03541191.jpg

Figure 38: 03559423.jpg

Figure 39: 03593991.jpg

Figure 40: 03665359.jpg

Figure 41: 03673623.jpg

Figure 42: 05063735.jpg

Figure 43: 05069311.jpg

Figure 44: 05180927.jpg

Figure 45: 05475951.jpg

6.1.4. Images from Unallocated Space

Figure 1: AlmondMarshGreatBlueHeronStalling.jpg

Figure 2: AmericanAvocetWinterPlumage.jpg

Figure 3: AmericanWhitePelicansCircling.jpg

Figure 4: BaldEagle7oClock.jpg

Figure 5: BarnOwl.jpg

Figure 6: BellbirdJumpingOffBranch.jpg

Figure 7: BlackNeckedStiltsFromBehind.jpg

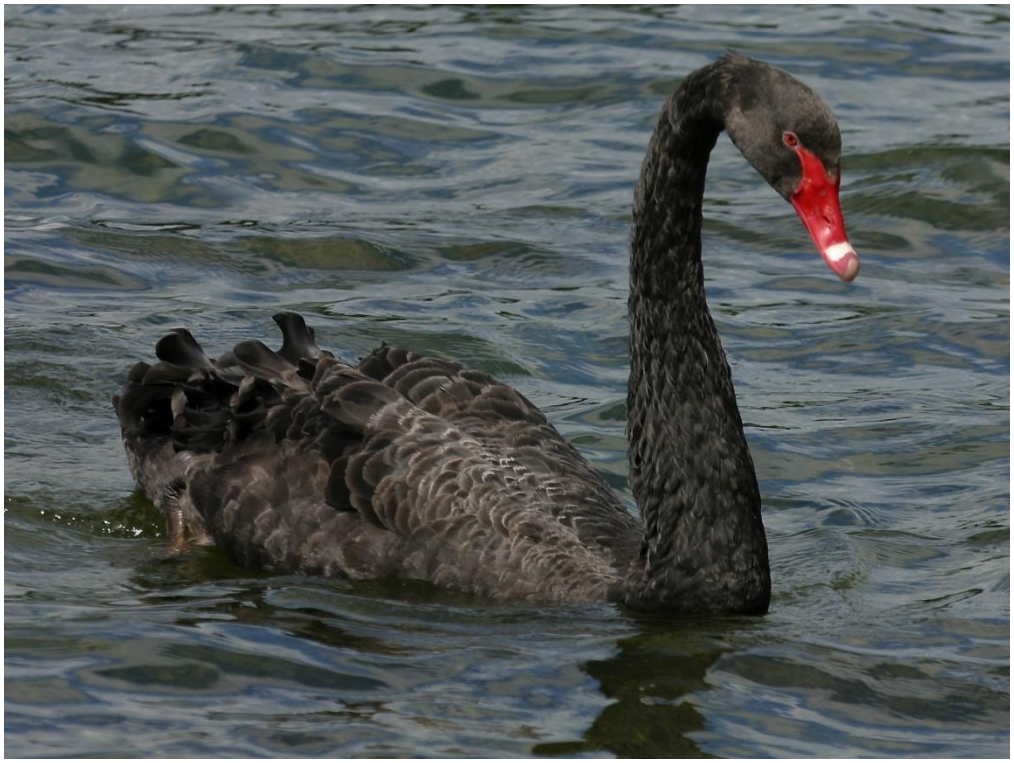


Figure 8: BlackSwan.jpg

Figure 9: BlackVultureSunningOnPost.jpg

Figure 10: brd_Ornithologist_TWG.jpg


Figure 11: GreatBlueHeronWithFish.jpg

Figure 12: GreatEgretInVoloBog.jpg

Figure 13: GreatEgretOverflyingRoseateSpoonbills.jpg

Figure 14: GreenHeronCloseup.jpg

Figure 15: GreenHeronOnChicagoLakeshore.jpg

Figure 16: ImmatureSnowyEgretTakingOff.jpg

Figure 17: june03screen.jpg

Figure 18: junescreen01.jpg


Figure 19: KeaAndMountain.jpg

Figure 20: KeaAtTopOfMacKinnonPass0930.jpg

Figure 21: KeaEatingRentalCar.jpg

Figure 22: KeaRetrievingBakedBeanCanFromTarn.jpg

Figure 23: Df1.jpg

6.1.5. Recovered Deleted Images from Volume 2 (NTFS Partition)

Figure 1: 0E47C6DFd01.jpg

Figure 2: 1CE0A8AEd01.jpg

Figure 3: 3E8C62AFd01.jpg

Figure 4: 3E8162AFd01.jpg

Figure 5: 3E8262AFd01.jpg

Figure 6: 3E8462AFd01.jpg

Figure 7: 3E8662AFd01.jpg

Figure 8: 3E8762AFd01.jpg

Figure 9: 3FB68809d01.jpg

Figure 10: 4C3E89C6d01.jpg

Figure 11: 5C1E7D60d01.jpg

Figure 12: 5E5570B4d01.jpg

Figure 13: 6A161D2Fd01.jpg

Figure 14: 6F61F39Dd01.jpg

Figure 15: 7E37FA89d01.jpg

Figure 16: 19E9BA69d01.jpg

Figure 17: 61C27B40d01.jpg

Figure 18: 65F30A3Dd01.jpg

Figure 19: 67BAEB46d01.jpg

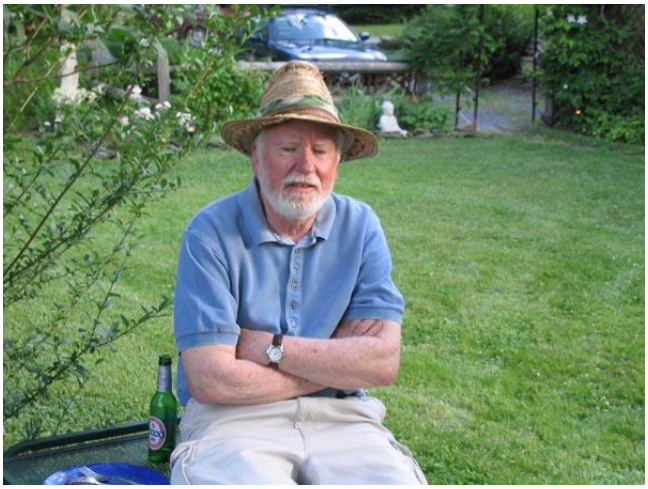


Figure 20: 80BF7122d01.jpg

Figure 21: 93C4F412d01.jpg

Figure 22: 404BF387d01.jpg

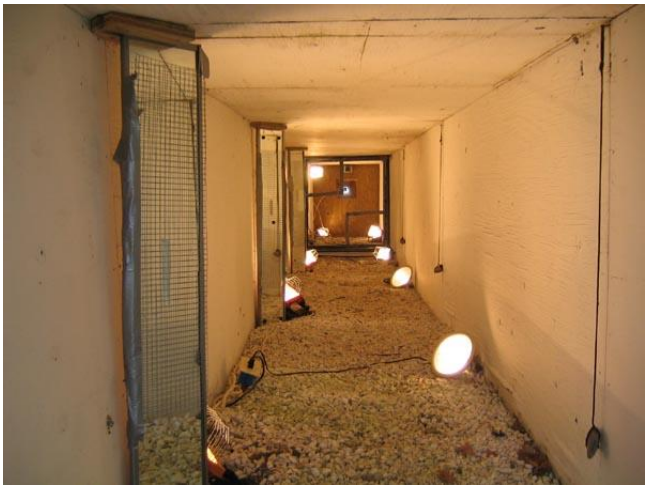


Figure 23: 502FE69Dd01.jpg

Figure 24: 661C3843d01.jpg

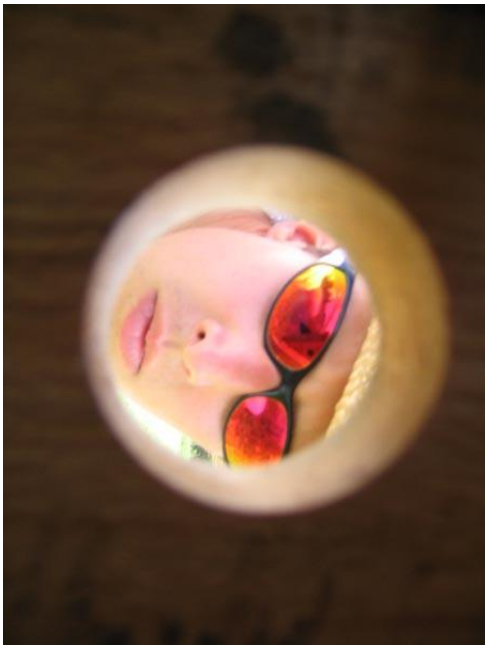


Figure 25: 884B7041d01.jpg

Figure 26: 978D14DDd01.jpg

Figure 27: 1238C212d01.jpg

Figure 28: 4043F387d01.jpg

Figure 29: 4058F387d01.jpg

Figure 30: 7013F58Dd01.jpg

Figure 31: 42626CDDd01.jpg

Figure 32: 426147D8d01.jpg

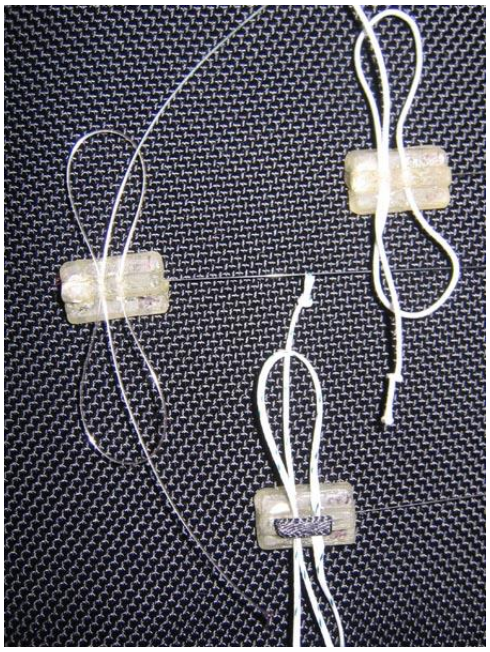


Figure 33: 848752E7d01.jpg


Figure 34: A2E5F216d01.jpg

Figure 35: A3D4DDDDd01.jpg

Figure 36: A9E5105Ad01.jpg

Figure 37: A0016363d01.jpg

Figure 38: A8331696d01.jpg

Figure 39: AA784519d01.jpg

Figure 40: B9D470B5d01.jpg

Figure 41: B76BD0AEd01.jpg

Figure 42: BF5BE9D9d01.jpg

Figure 43: D1D1775Fd01.jpg

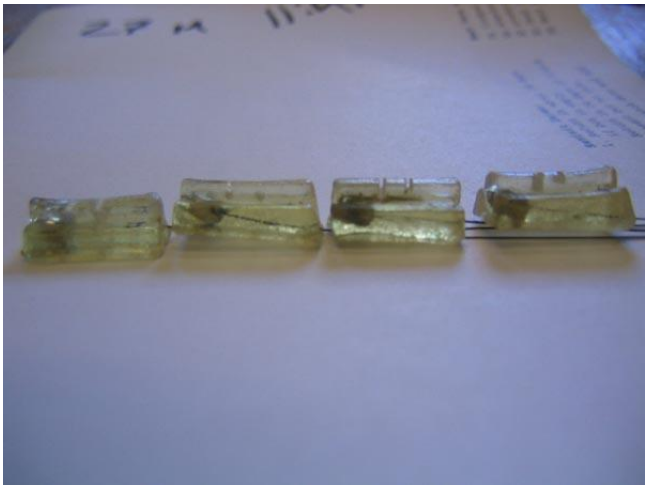


Figure 44: D5FDCB9Ad01.jpg

Figure 45: D6A649A8d01.jpg

Figure 46: D19FCBF6d01.jpg

Figure 47: D192AAB2d01.jpg

Figure 48: D8829E69d01.jpg

Figure 49: E319CFC2d01.jpg

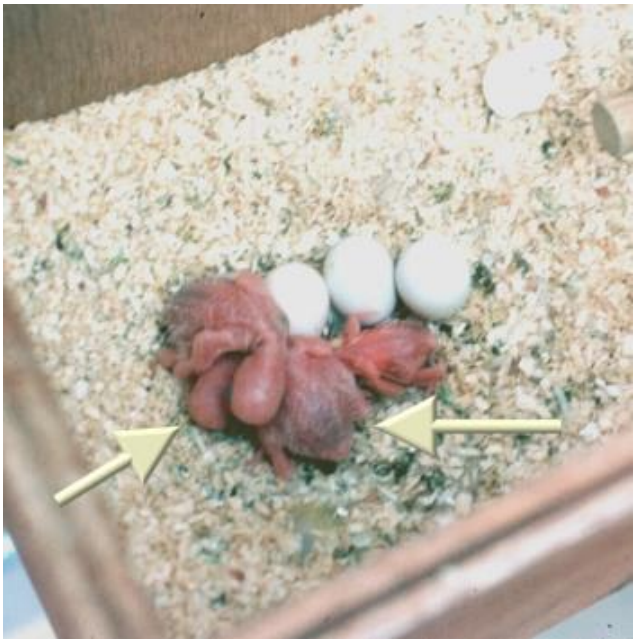


Figure 50: E1663DDEd01.jpg

Figure 51: EF29AEAEd01.jpg

Figure 52: FA73DB84d01.jpg

Figure 53: FB4DEA89d01.jpg

Figure 54: FB4EDA00d01.jpg

Figure 55: FC6938FDd01.jpg

6.1.6. Other images found in various locations on filesystem

Figure 1: 40m.jpg

Figure 2: 177.jpg

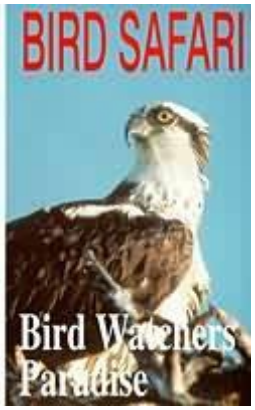


Figure 3: 7107298.jpg

Figure 4: babyscot_2weeks1.jpg

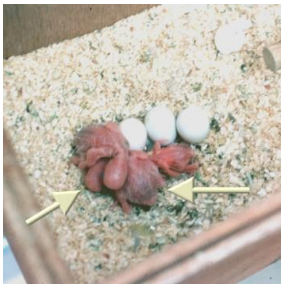


Figure 5: babyscot_vyoung.jpg

Figure 6: birdtrans2.jpg

Figure 7: chicks2.jpg

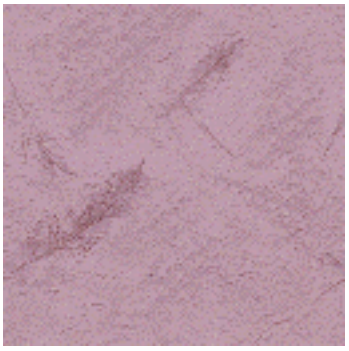


Figure 8: FeatherTexture.bmp

Figure 9: Firefox Wallpaper.bmp

Figure 10: newbies2.jpg

Figure 11: ready2fledge.jpg

Figure 12: snow_geese.jpg

Figure 13: tn_duck_3.jpg

Figure 14: wbpremium_s.jpg

6.1.7. Images from Encrypted GPG File

Figure 1: WhiteFacedHeronFlying.jpg

Figure 2: WhiteFrontedParrot.jpg

Figure 3: WhiteThroatedSparrowInTree.jpg

Figure 4: WhoopingCranes.jpg

Figure 5: yellow-wag-cover-nb.jpg

6.1.8. Images hidden inside Kokako.dll

Figure 1: brd_WoodDuck.jpg

Figure 2: Brolga.jpg

Figure 3: BrushTurkeyPerching.jpg

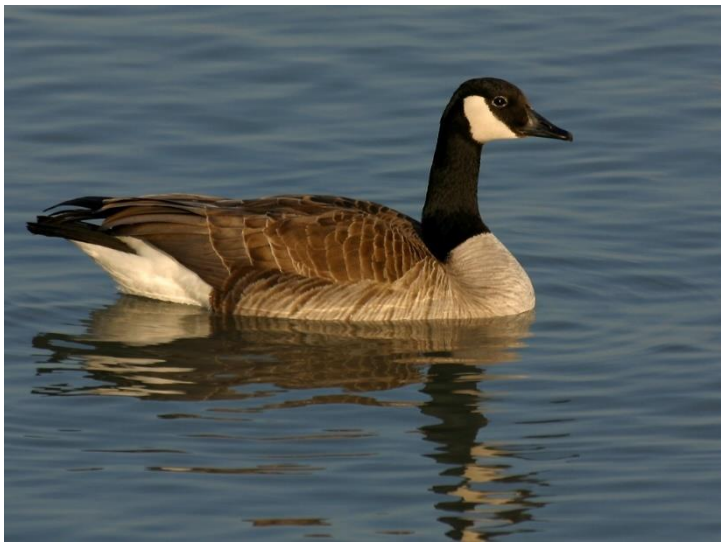


Figure 4: CanadaGoose.jpg

Figure 5: CanadaGooseWashing.jpg

Figure 6: ChestnutMandibledToucan.jpg

Figure 7: CrouchingKokako.jpg

```
admin@H38:/mnt/suspectDrive/WINDOWS$ file CrouchingKokako.dll
CrouchingKokako.dll: Zip archive data, at least v2.0 to extract
admin@H38:/mnt/suspectDrive/WINDOWS$
```

Figure 8: Output from file type discovery

6.1.9. Image hidden inside FantailFrontView.exe

Figure 1: FantailFrontView.jpg

```
Terminal
admin@H38:~$ cd Desktop
admin@H38:~/Desktop$ file FantailFrontView.exe
FantailFrontView.exe: JPEG image data, JFIF standard 1.01, resolution (DPI), den
sity 72x72, segment length 16, comment: "Created with The GIMP", baseline, preci
sion 8, 1152x864, frames 3
admin@H38:~/Desktop$
```

Figure 2: Evidence of jpeg metadata inside the .exe

6.1.10. Birds.zip Contents

Original file names for these images were un-recoverable.

Figure 1: Slideshow Image 1

Figure 2: Slideshow Image 2

Figure 3: Slideshow Image 3

Figure 4: Slideshow Image 4

Figure 5: Slideshow Image 5

Figure 6: Slideshow Image 6

Figure 7: Slideshow Image 7

Figure 8: Slideshow Image 8

Figure 9: Slideshow Image 9

6.1.11. Images recovered from E-mail conversations

Figure 1: 7EYBTELF1KAN.jpg

Figure 2: BC7 feeding the birds.jpg

Figure 3: colorful-birds.jpg

Figure 4: cute_penguin.jpg

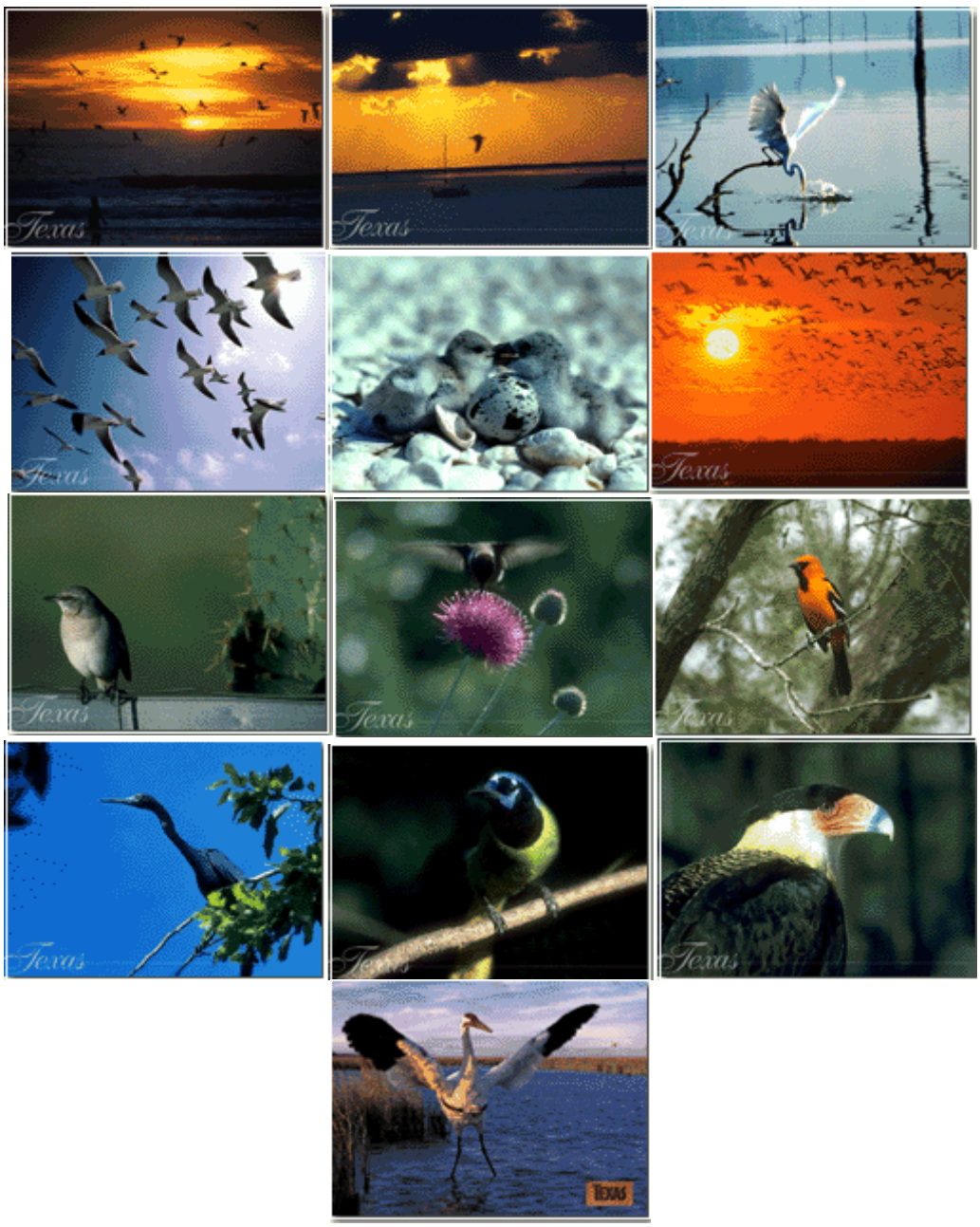
Figure 5: gawall8.jpg

Nesting red-winged blackbird/
Carouge à épaulettes en cours de nidification
Mike Hopiak / Cornell Lab of Ornithology

Figure 6: glfs-storm-birds.jpg

Figure 7: IMG_3937_filtered.jpg | This image was sent twice over 2 separate emails

6.1.12. Recovered Images from Mozilla Firefox Cache



6.2. Appendix 2 – Anti-Virus Scan Results

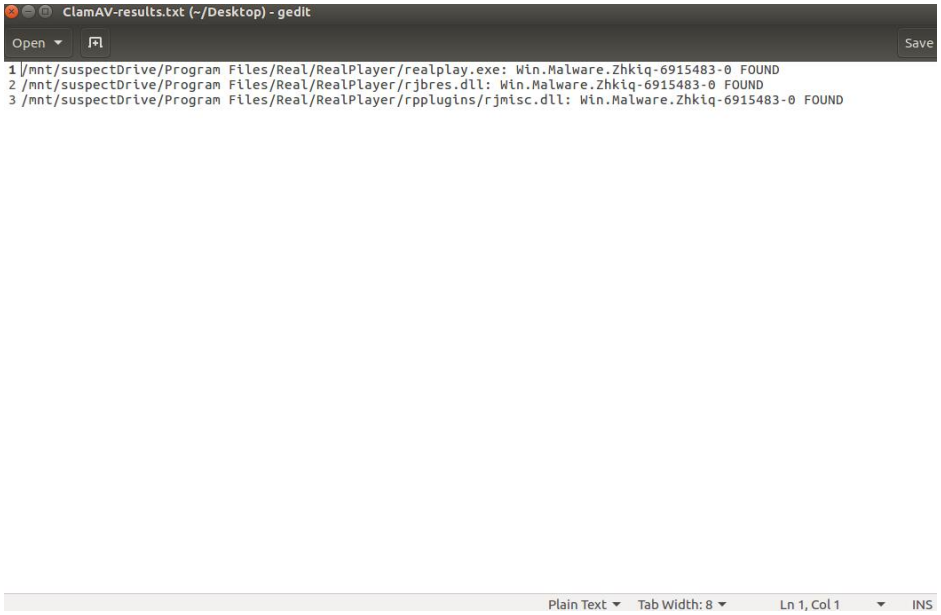


Figure 1: clamav-found.png
List of found malware files

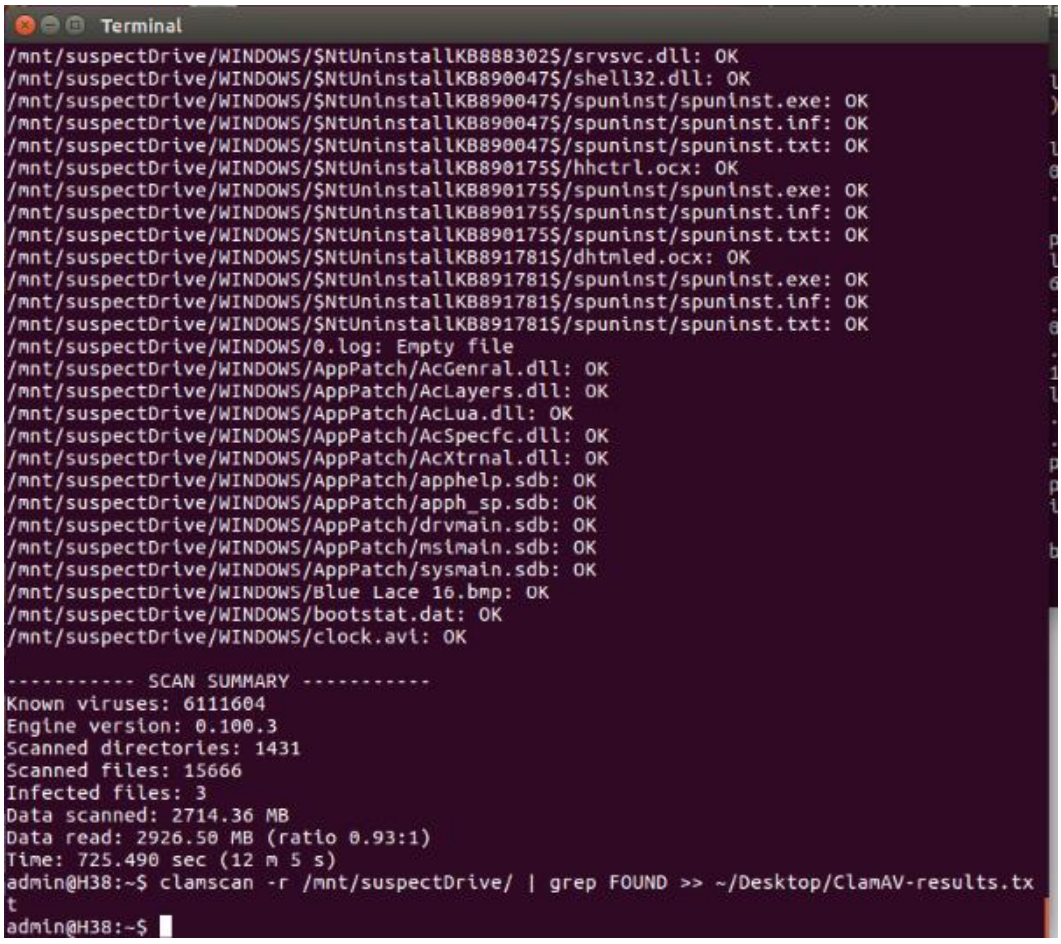


Figure 2: clamav-scan.png
Anti-Virus Result Summary

6.3. Appendix 3- Images of Recovered Hardware

Figure 1: IMG_20190417_092210.jpg
Front of John Doe Hard Drive

Figure 2: IMG_20190417_092238.jpg
Back of John Doe Hard Drive

Figure 3: IMG_20190417_093640.jpg
Hard Drive connected using a write blocker ready for forensic imaging

6.4. Appendix 4 – MD5 Checksum of Forensic Image

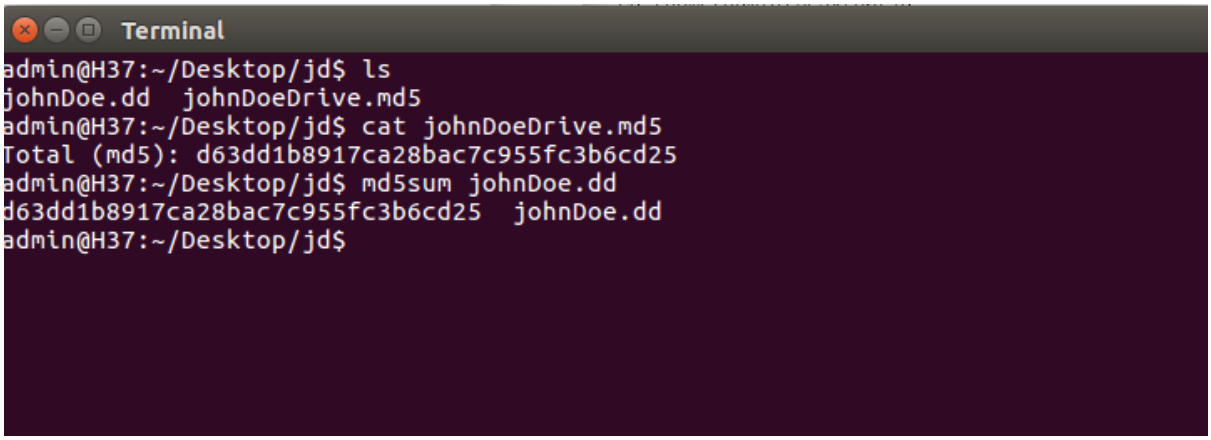


Figure 1: Top hash | MD5 Checksum of Hard Drive Before Imaging
Bottom Hash | MD5 Checksum of Forensic Image After Imaging

6.5. Appendix 5 – Information from Registry Files

6.5.1. User Information

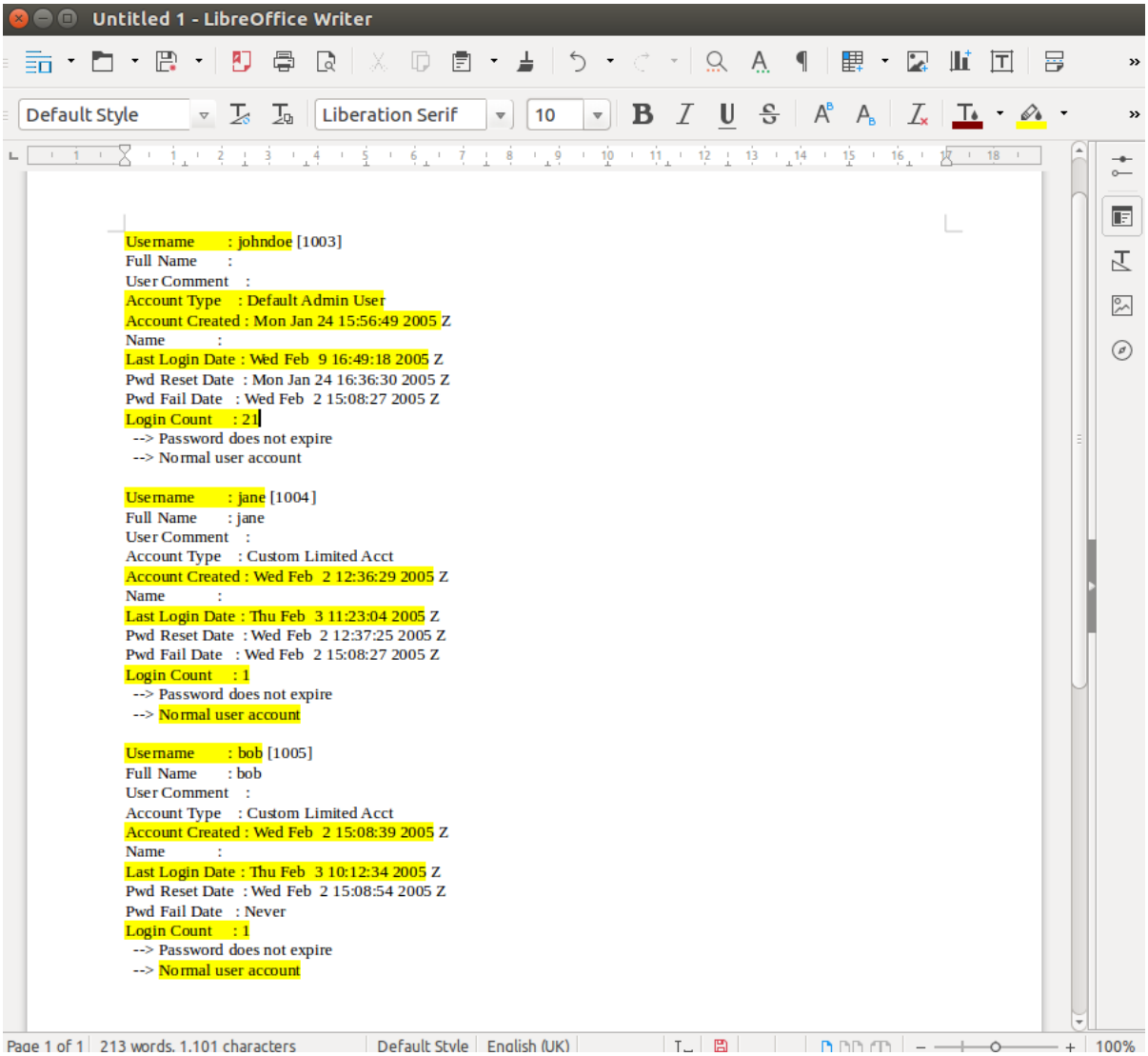


Figure 1: User Accounts & Login Timestamps – SAM File Results

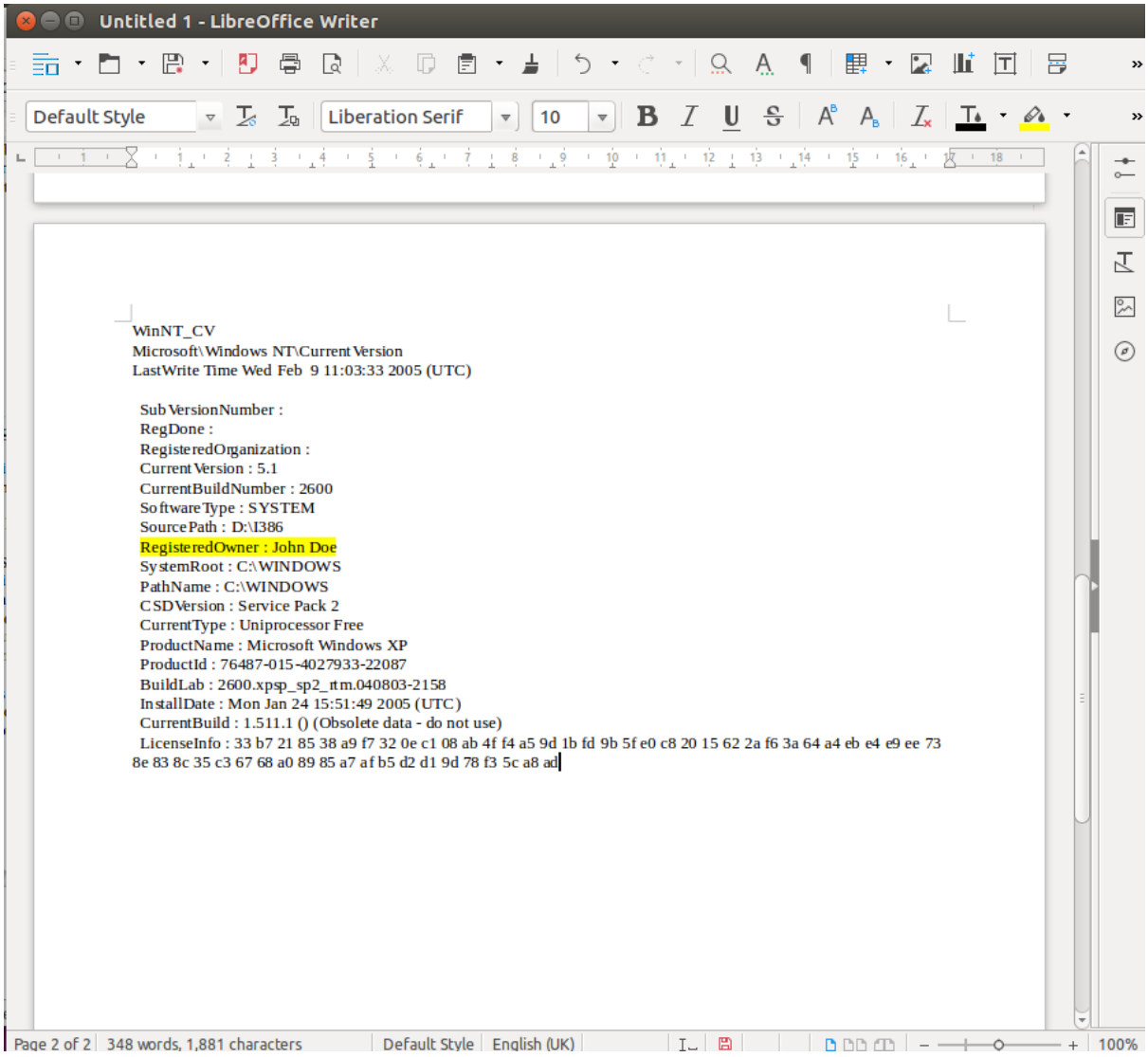


Figure 2: Registered Owner of PC – Software File Results

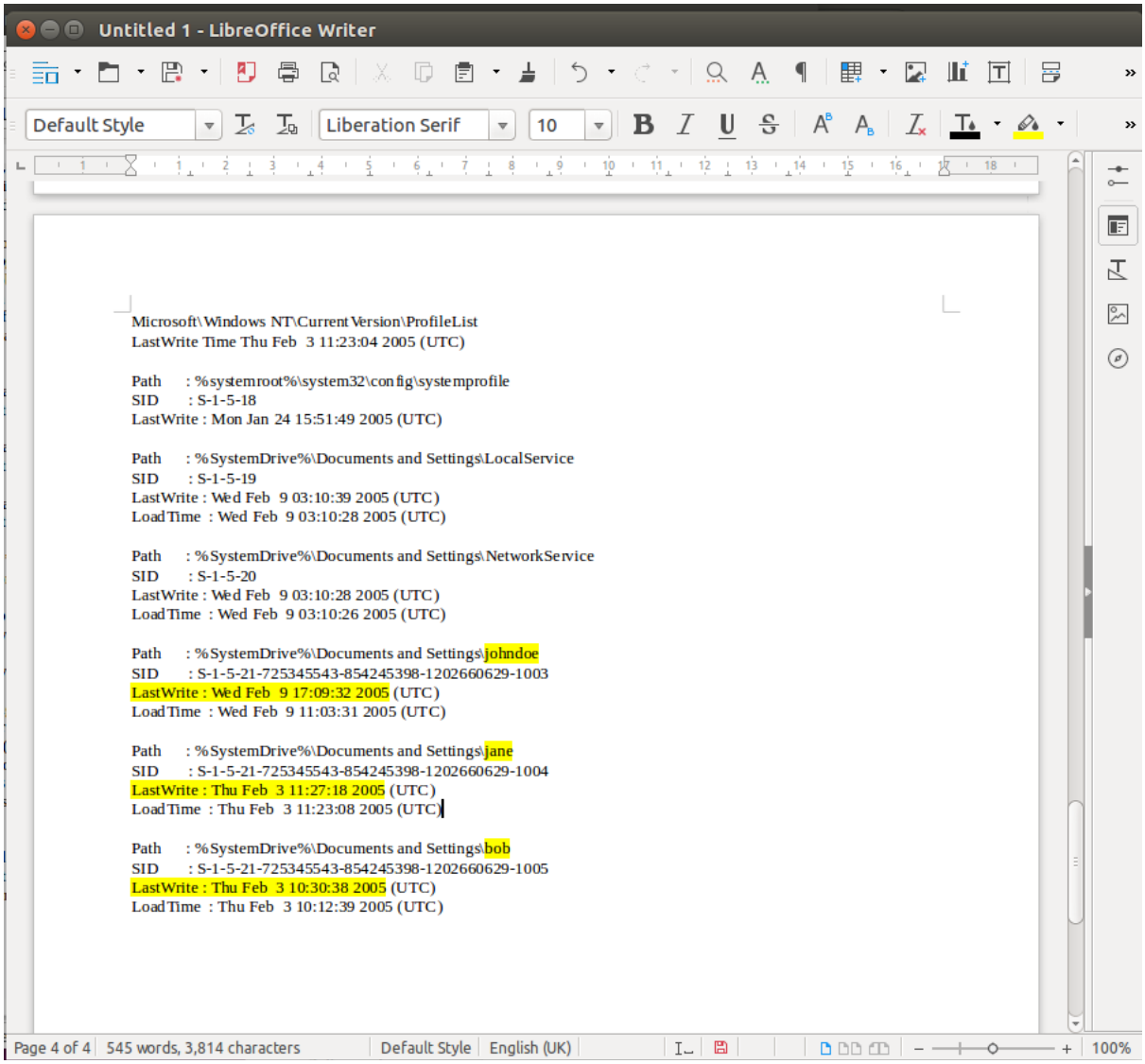


Figure 3: Last Write time of each user account – Software File Results

6.5.2. System Information

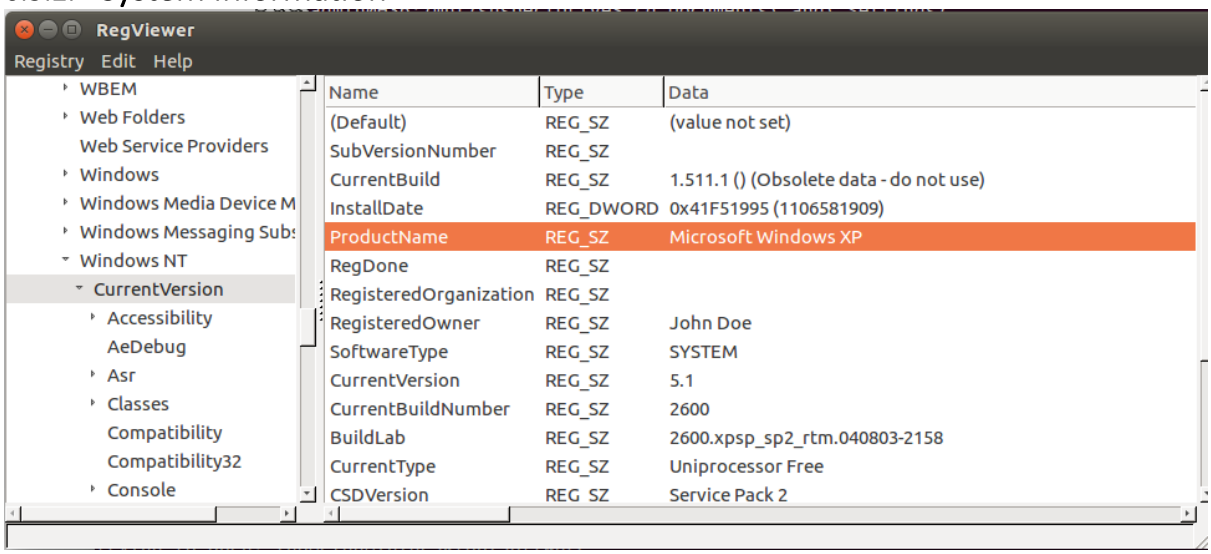


Figure 1: Operating System Information

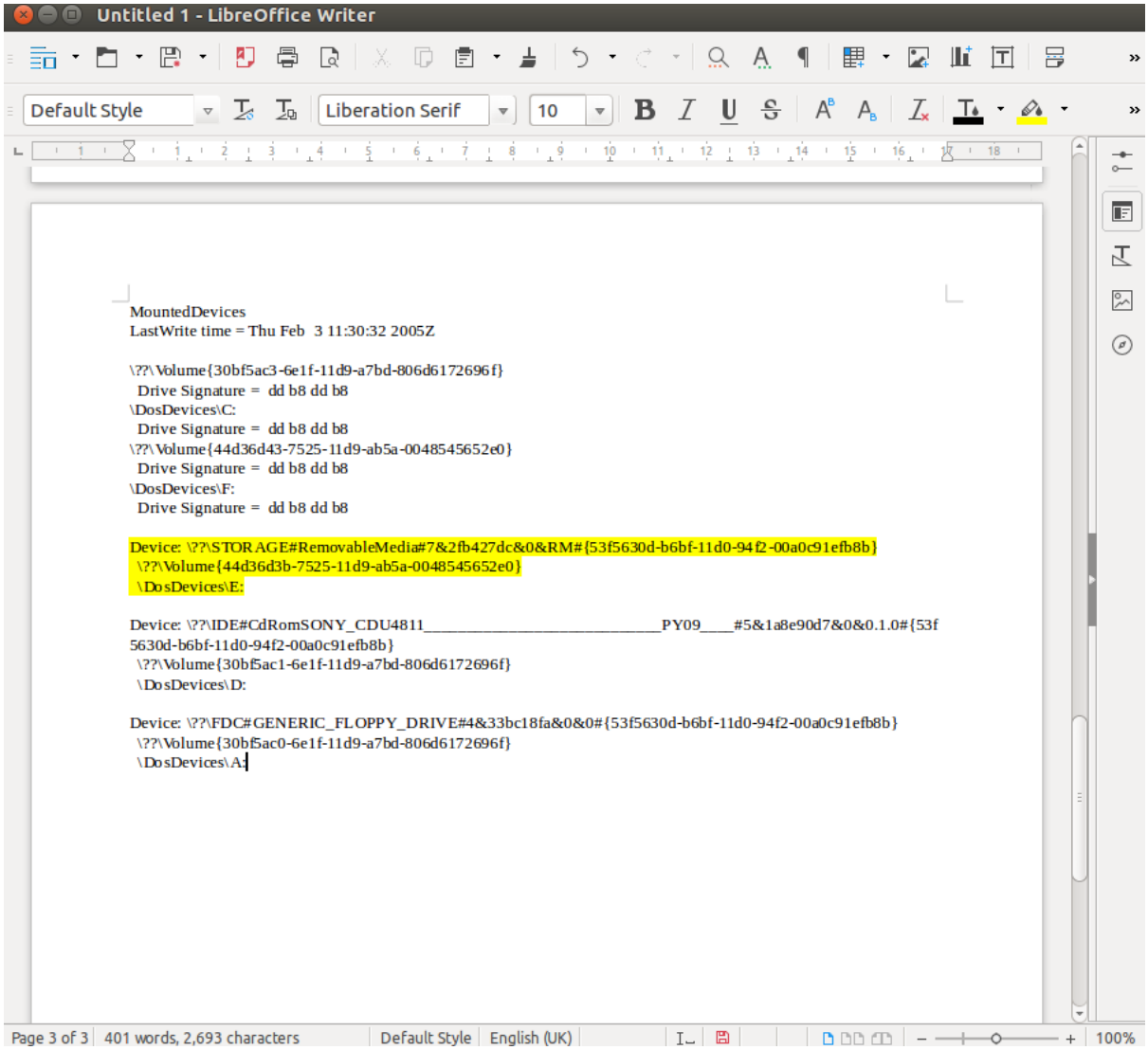


Figure 2: Removable media drive labelled ‘E’

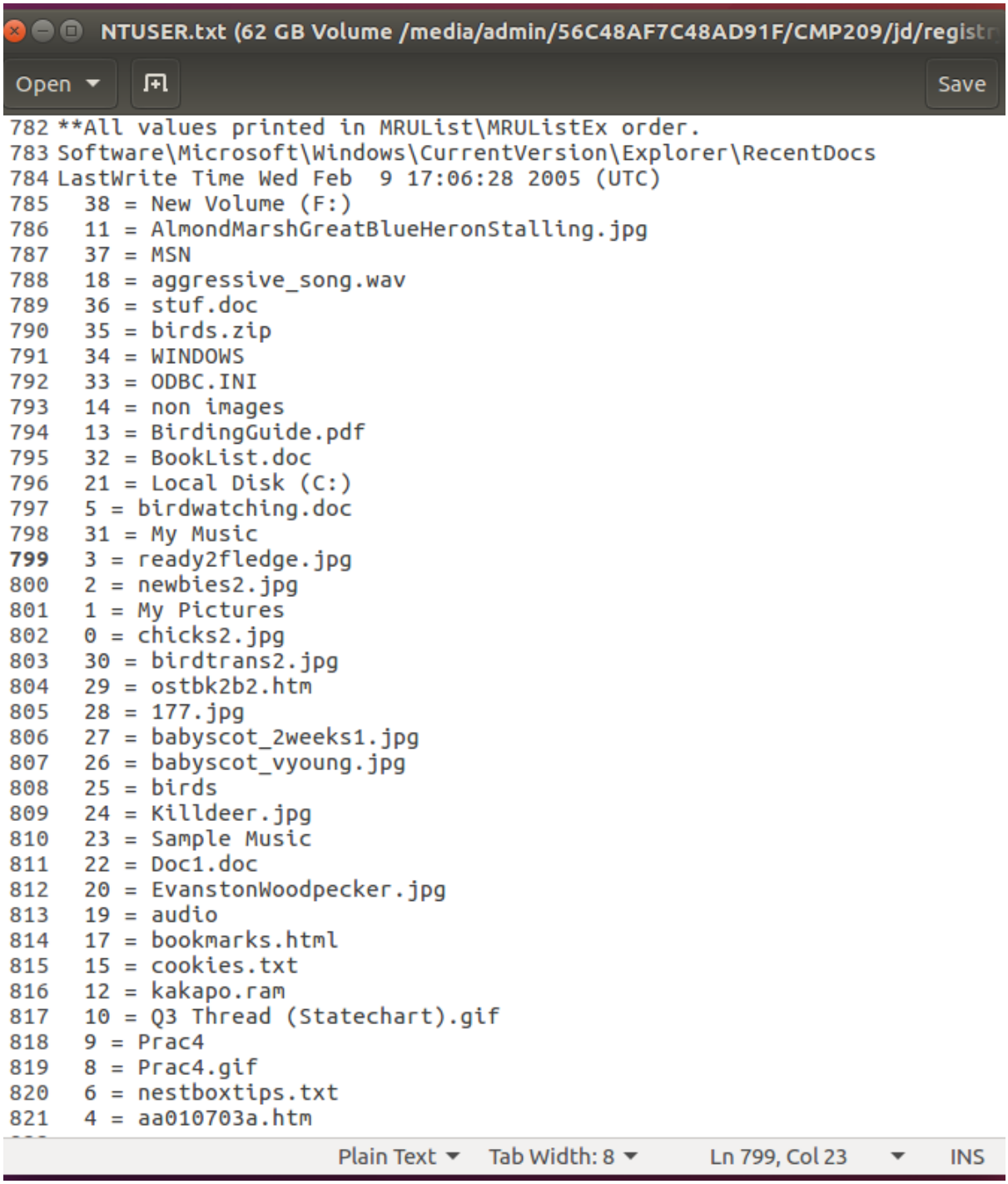


Figure 3: Accessed files by johndoe user account.

6.6. Appendix 6 – Physical & Logical Search Results

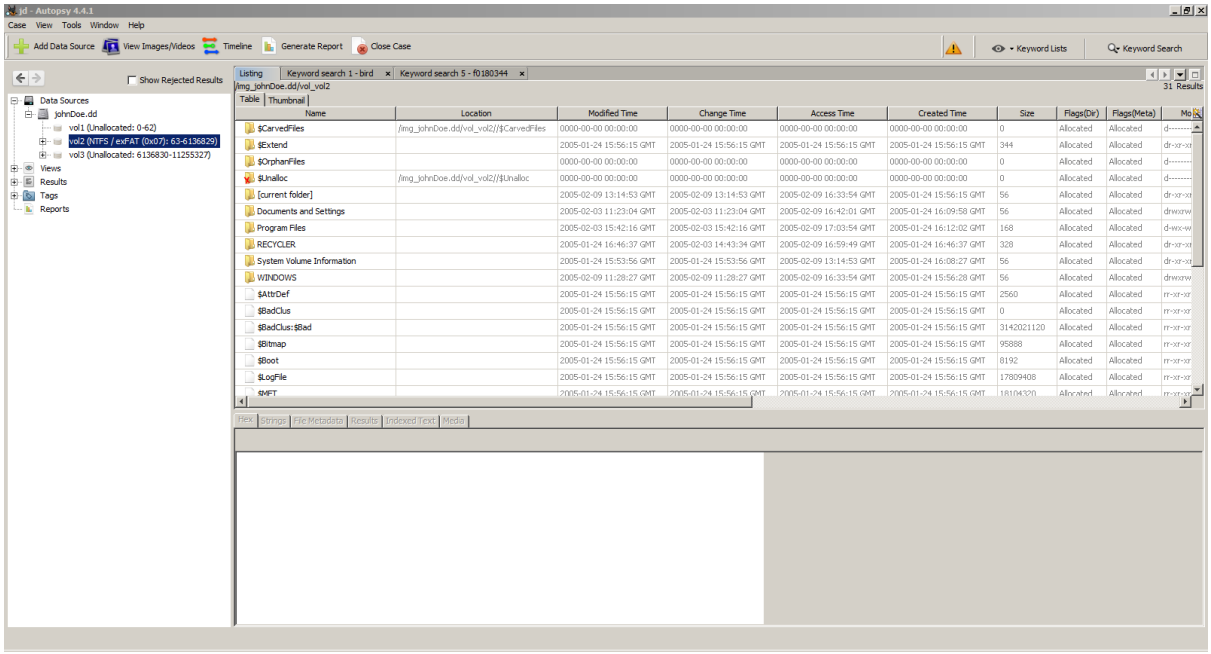


Figure 1: Autopsy.png
Results from Autopsy Physical search showing partition & filesystem with lots of files

jd-cleanhashesremoved.txt (62 GB Volume /media/sansforensics/56C48AF7C48AD

Open Save

```
c6108e60db66aa588543657c4f656847  ./birdwatching.doc
fa579938b0733b87066546afe951082c  ./boot.ini
3b5ee2412acd09d764ce26787e7f61c3  ./Documents and Settings/All Users/
Application Data/Adobe/Acrobat/7.0/Replicate/Security/directories.acrodata
c92d0ad32aa6992605bcd497df7719ed  ./Documents and Settings/All Users/
Application Data/Microsoft/Crypto/RSA/S-1-5-18/
d42cc0c3858a58db2db37658219e6400_89cf4860-c493-4481-aff8-2e39c47624b8
babaff5f2c7d4d60afb9b11bfb0e60e8  ./Documents and Settings/All Users/
Application Data/Microsoft/Dr Watson/drwtsn32.log
c2b34d84592259614494e2f79e1c0a54  ./Documents and Settings/All Users/
Application Data/Microsoft/Dr Watson/user.dmp
921ef84fd6ab08321f9f385776ef933d  ./Documents and Settings/All Users/
Application Data/Microsoft/Media Player/DefaultStore_59R.bin
921ef84fd6ab08321f9f385776ef933d  ./Documents and Settings/All Users/
Application Data/Microsoft/Media Player/UserMigratedStore_59R.bin
362e354c68513e8a09056c7978acf8bd  ./Documents and Settings/All Users/
Application Data/Microsoft/Network/Downloader/qmgr0.dat
2138cb92db34e0c16df1eb320198a0fa  ./Documents and Settings/All Users/
Application Data/Microsoft/Network/Downloader/qmgr1.dat
8b7a6fc84edbb9b9c2164f3227a8c945  ./Documents and Settings/All Users/
Application Data/Microsoft/OFFICE/DATA/OPA11.BAK
0e7e24ed21bd5da96b0d882d5a043ad4  ./Documents and Settings/All Users/
Application Data/Microsoft/OFFICE/DATA/opa11.dat
8987a8a938af9b0f4e46f34e3e8b3d5a  ./Documents and Settings/All Users/
Application Data/Microsoft/User Account Pictures/bob.bmp
f2139758e1ca788944e3d676ffdf569d  ./Documents and Settings/All Users/
Application Data/Microsoft/User Account Pictures/jane.bmp
851de535ebf2fecc9d6ca8c313f313a6  ./Documents and Settings/All Users/
```

Plain Text Tab Width: 8 Ln 7, Col 105 INS

Figure 2: Small view of the suspicious hashes list. The full file can be viewed as an external deliverable

6.7. Appendix 7 – Browser Analysis Logs

History File: index.dat Version: 5.2			
TYPE	URL	MODIFIED TIME	ACCESS TIME
URL	:2005020920050210: johndoe@file:///F:/AlmondMarshGreatBlueHeronStalling.jpg	02/09/2005 17:06	02/09/2005 17:06
URL	:2005020920050210: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/birds.zip	02/09/2005 11:28	02/09/2005 11:28
URL	:2005020920050210: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/stuf.doc	02/09/2005 16:57	02/09/2005 16:57
URL	:2005020920050210: johndoe@:Host: My Computer	02/09/2005 11:28	02/09/2005 11:28
URL	:2005020920050210: johndoe@file:///C:/Program%20Files/MSN/aggressive_song.wav	02/09/2005 17:00	02/09/2005 17:00

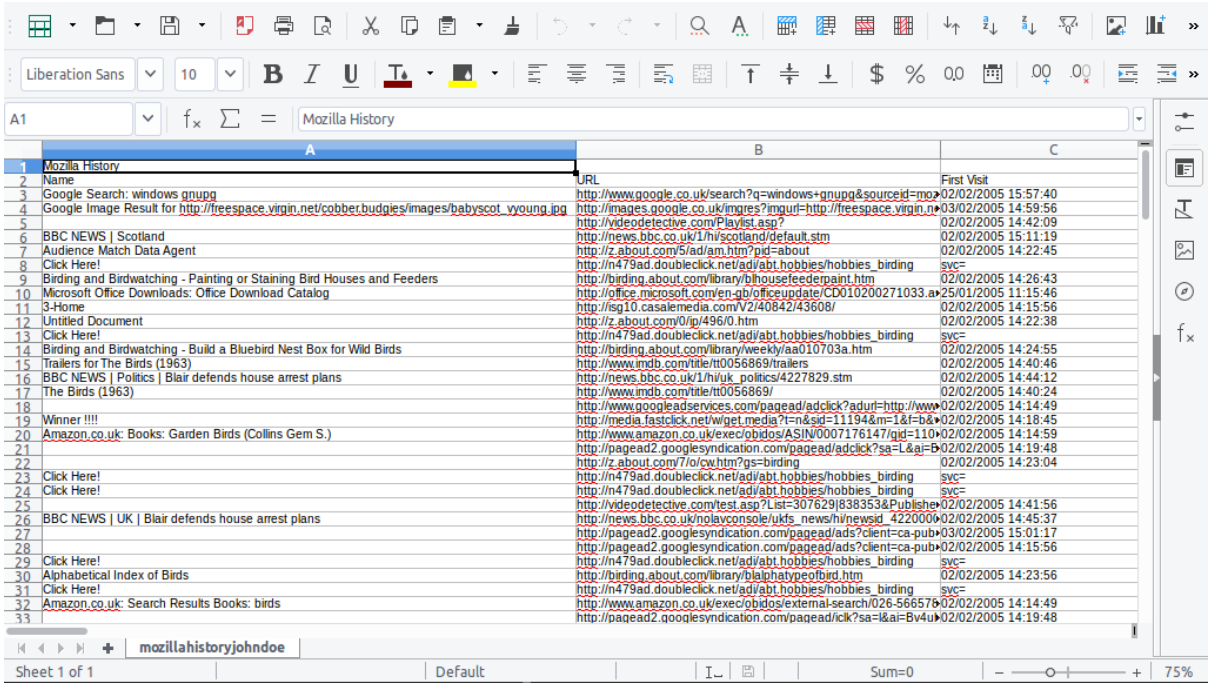
Figure 1: bob User Account | Internet Explorer History

History File: index.dat Version: 5.2			
TYPE	URL	MODIFIED TIME	ACCESS TIME
URL	:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/All%20Users/Documents/My%20Music/Sample%20Music/Doc1.doc	02/03/2005 14:17	02/09/2005 11:28
URL	:2005013120050207: johndoe@:Host: My Computer	02/03/2005 12:19	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///C:/Program%20Files/Real/RealPlayer/Firstrun/1.htm	02/02/2005 15:04	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///C:/Program%20Files/Real/RealPlayer/DataCache/Login/index.html	02/02/2005 14:57	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/7107298.jpg	02/02/2005 14:20	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/kakapo.ram	02/02/2005 15:11	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///D:/Prac5/Q3%20Thread%20(Statechart).gif	02/02/2005 15:10	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/40m.jpg	02/02/2005 14:43	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/177.jpg	02/03/2005 15:01	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///C:/birdwatching.doc	02/03/2005 15:49	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///D:/Prac4/Prac4.gif	02/02/2005 15:10	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/ostbk2b2.htm	02/03/2005 15:02	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/Application%20Data/Mozilla/Firefox/Profiles/w4nf3obl.default/cookies.txt	02/03/2005 12:19	02/09/2005 11:28
URL	:2005013120050207: johndoe@http://www.real.com/intro/index_upsell_manager.html?DC=NSP01D&optin=true&country=gb&language=en-gb&icon=tiscali&LI=en&PBR=10485E	02/02/2005 15:04	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/nestboxtips.txt	02/02/2005 14:29	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/aa010703a.htm	02/02/2005 14:25	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/tn_duck_3.jpg	02/02/2005 14:18	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/bob/My%20Documents/My%20Music/ready2fledge.jpg	02/03/2005 15:06	02/09/2005 11:28
URL	:2005013120050207: johndoe@https://account.real.com/acct/intro/msg.html?msg=frweur	02/02/2005 15:04	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///E:/birds/audio/aggressive_song.wav	02/03/2005 12:22	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/Desktop/birdtrans2.jpg	02/03/2005 15:04	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/wbpremium_s.jpg	02/02/2005 14:28	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///C:/WINDOWS/ODBC.INI	02/03/2005 15:54	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/chicks2.jpg	02/03/2005 15:05	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///C:/Program%20Files/Adobe/Acrobat%207.0/Reader/Legal/Adobe%20Reader/7.0.0/en_US/license.html	02/02/2005 17:03	02/09/2005 11:28
URL	:2005013120050207: johndoe@:Host: account.real.com	02/02/2005 15:04	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/Application%20Data/Mozilla/Firefox/Profiles/w4nf3obl.default/bookmarks.html	02/03/2005 12:20	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///C:/EvanstonWoodpecker.jpg	02/03/2005 14:14	02/09/2005 11:28
URL	:2005013120050207: johndoe@:Host: www.real.com	02/02/2005 15:04	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///E:/birds/Killdeer.jpg	02/03/2005 14:49	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/babyscot_yyoung.jpg	02/03/2005 15:00	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/babyscot_2weeks1.jpg	02/03/2005 15:00	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/newbies2.jpg	02/03/2005 15:05	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///C:/Program%20Files/Real/RealPlayer/Firstrun/context.htm	02/02/2005 15:04	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/snow_geese.jpg	02/02/2005 14:18	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///E:/birds/non%20images/BirdingGuide.pdf	02/03/2005 15:52	02/09/2005 11:28
URL	:2005013120050207: johndoe@file:///E:/birds/non%20images/BookList.doc	02/03/2005 15:51	02/09/2005 11:28

Figure 2: johndoe User Account | Internet Explorer History

```
    <NC:DateEnded NC:parseType="Date">Wed Feb 09 11:28:00 GMT Standard Time 2005 +415273</NC:DateEnded>
    <NC:DownloadState NC:parseType="Integer">1</NC:DownloadState>
    <NC:ProgressPercent NC:parseType="Integer">100</NC:ProgressPercent>
  </RDF:Description>
  <RDF:Description RDF:about="C:\Documents and Settings\johndoe\My Documents\My Pictures\babyscot_2weeks1.jpg"
                   NC:Name="babyscot_2weeks1.jpg"
                   NC:Transferred="33kB of 33kB">
    <NC:URL RDF:resource="http://freespace.virgin.net/cobber.budgies/images/babyscot_2weeks1.jpg"/>
    <NC:File RDF:resource="C:\Documents and Settings\johndoe\My Documents\My Pictures\babyscot_2weeks1.jpg"/>
    <NC:DateStarted NC:parseType="Date">Thu Feb 03 15:00:27 GMT Standard Time 2005 +761262</NC:DateStarted>
    <NC:DateEnded NC:parseType="Date">Thu Feb 03 15:00:27 GMT Standard Time 2005 +811334</NC:DateEnded>
    <NC:DownloadState NC:parseType="Integer">1</NC:DownloadState>
    <NC:ProgressPercent NC:parseType="Integer">100</NC:ProgressPercent>
  </RDF:Description>
  <RDF:Description RDF:about="C:\Documents and Settings\bob\My Documents\My Music\ready2fledge.jpg"
                   NC:Name="ready2fledge.jpg"
                   NC:Transferred="77kB of 77kB">
    <NC:URL RDF:resource="http://people.cornell.edu/pages/sah67/ready2fledge.jpg"/>
    <NC:File RDF:resource="C:\Documents and Settings\bob\My Documents\My Music\ready2fledge.jpg"/>
    <NC:DateStarted NC:parseType="Date">Thu Feb 03 15:06:42 GMT Standard Time 2005 +379937</NC:DateStarted>
    <NC:DateEnded NC:parseType="Date">Thu Feb 03 15:06:42 GMT Standard Time 2005 +440024</NC:DateEnded>
    <NC:DownloadState NC:parseType="Integer">1</NC:DownloadState>
    <NC:ProgressPercent NC:parseType="Integer">100</NC:ProgressPercent>
  </RDF:Description>
  <RDF:Seq RDF:about="NC:DownloadsRoot">
    <RDF:li RDF:resource="C:\Documents and Settings\johndoe\My Documents\birds.zip"/>
    <RDF:li RDF:resource="C:\Documents and Settings\bob\My Documents\My Music\ready2fledge.jpg"/>
    <RDF:li RDF:resource="C:\Documents and Settings\johndoe\My Documents\newbies2.jpg"/>
    <RDF:li RDF:resource="C:\Documents and Settings\johndoe\My Documents\My Pictures\chicks2.jpg"/>
    <RDF:li RDF:resource="C:\Documents and Settings\johndoe\Desktop\birdtrans2.jpg"/>
    <RDF:li RDF:resource="C:\Documents and Settings\johndoe\My Documents\ostbk2b2.htm"/>
    <RDF:li RDF:resource="C:\Documents and Settings\johndoe\My Documents\My Pictures\177.jpg"/>
    <RDF:li RDF:resource="C:\Documents and Settings\johndoe\My Documents\My Pictures\babyscot_2weeks1.jpg"/>
    <RDF:li RDF:resource="C:\Documents and Settings\johndoe\My Documents\My Pictures\babyscot_vyoung.jpg"/>
    <RDF:li RDF:resource="E:\birds\audio\aggressive_song.wav"/>
    <RDF:li RDF:resource="C:\Documents and Settings\johndoe\Desktop\AdbeRdr70_enu_full.exe"/>
    <RDF:li RDF:resource="C:\DOCUME~1\JOHNDOE\LOCALS~1\TEMP\dawn.ram"/>
  </RDF:Seq>
  <RDF:Description RDF:about="C:\Documents and Settings\johndoe\Desktop\birdtrans2.jpg"
                   NC:Name="birdtrans2.jpg"
                   NC:Transferred="58kB of 58kB">
    <NC:URL RDF:resource="http://people.cornell.edu/pages/sah67/birdtrans2.jpg"/>
    <NC:File RDF:resource="C:\Documents and Settings\johndoe\Desktop\birdtrans2.jpg"/>
    <NC:DateStarted NC:parseType="Date">Thu Feb 03 15:04:48 GMT Standard Time 2005 +235806</NC:DateStarted>
    <NC:DateEnded NC:parseType="Date">Thu Feb 03 15:04:48 GMT Standard Time 2005 +285878</NC:DateEnded>
    <NC:DownloadState NC:parseType="Integer">1</NC:DownloadState>
```

Figure 3: johndoe User Account | Mozilla Firefox Downloads Log



	A	B	C
1	Mozilla History		
2	Name	URL	First Visit
3	Google Search: windows gnupg	http://www.google.co.uk/search?q=windows+gnupg&sourceid=mo	02/02/2005 15:57:40
4	Google Image Result for http://freespace.virgin.net/cobber.budgies/images/babyscot_vyoung.jpg	http://images.google.co.uk/imgres?imgurl=http://freespace.virgin.n	03/02/2005 14:59:56
5		http://videodetective.com/Playlist.asp?	02/02/2005 14:42:09
6	BBC NEWS | Scotland	http://news.bbc.co.uk/1/hi/scotland/default.stm	02/02/2005 15:11:19
7	Audience Match Data Agent	http://z.about.com/5/ad/am.htm?pid=about	02/02/2005 14:22:45
8	Click Here!	http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding	svc=
9	Birding and Birdwatching - Painting or Staining Bird Houses and Feeders	http://birding.about.com/library/blhousefeederpaint.htm	02/02/2005 14:26:43
10	Microsoft Office Downloads: Office Download Catalog	http://office.microsoft.com/en-gb/officeupdate/CD010200271033.a	25/01/2005 11:15:46
11	3-Home	http://sg10.casalemedia.com/V2/40842/43608/	02/02/2005 14:15:56
12	Untitled Document	http://z.about.com/0/ip/496/0.htm	02/02/2005 14:22:38
13	Click Here!	http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding	svc=
14	Birding and Birdwatching - Build a Bluebird Nest Box for Wild Birds	http://birding.about.com/library/weekly/aa010703a.htm	02/02/2005 14:24:55
15	Trailers for The Birds (1963)	http://www.imdb.com/title/tt0056869/trailers	02/02/2005 14:40:46
16	BBC NEWS | Politics | Blair defends house arrest plans	http://news.bbc.co.uk/1/hi/uk_politics/4227829.stm	02/02/2005 14:44:12
17	The Birds (1963)	http://www.imdb.com/title/tt0056869/	02/02/2005 14:40:24
18		http://www.googleadservices.com/pagead/adclick?adurl=http://www	02/02/2005 14:14:49
19	Winner !!!!	http://media.fastclick.net/w/get.media?t=n&sid=11194&m=1&f=b&	02/02/2005 14:18:45
20	Amazon.co.uk: Books: Garden Birds (Collins Gem S.)	http://www.amazon.co.uk/exec/obidos/ASIN/0007176147/qid=110	02/02/2005 14:14:59
21		http://pagead2.googlesyndication.com/pagead/adclick?sa=L&ai=B	02/02/2005 14:19:48
22		http://z.about.com/7/o/cw.htm?gs=birding	02/02/2005 14:23:04
23	Click Here!	http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding	svc=
24	Click Here!	http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding	svc=
25		http://videodetective.com/test.asp?List=307629|838353&Publishe	02/02/2005 14:41:56
26	BBC NEWS | UK | Blair defends house arrest plans	http://news.bbc.co.uk/nolavconsole/ukfs_news/hi/newsid_422000	02/02/2005 14:45:37
27		http://pagead2.googlesyndication.com/pagead/ads?client=ca-pub	03/02/2005 15:01:17
28		http://pagead2.googlesyndication.com/pagead/ads?client=ca-pub	02/02/2005 14:15:56
29	Click Here!	http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding	svc=
30	Alphabetical Index of Birds	http://birding.about.com/library/blalphatypeofbird.htm	02/02/2005 14:23:56
31	Click Here!	http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding	svc=
32	Amazon.co.uk: Search Results Books: birds	http://www.amazon.co.uk/exec/obidos/external-search/026-56657	02/02/2005 14:14:49
33		http://pagead2.googlesyndication.com/pagead/iclk?sa=l&ai=Bv4u	02/02/2005 14:19:48

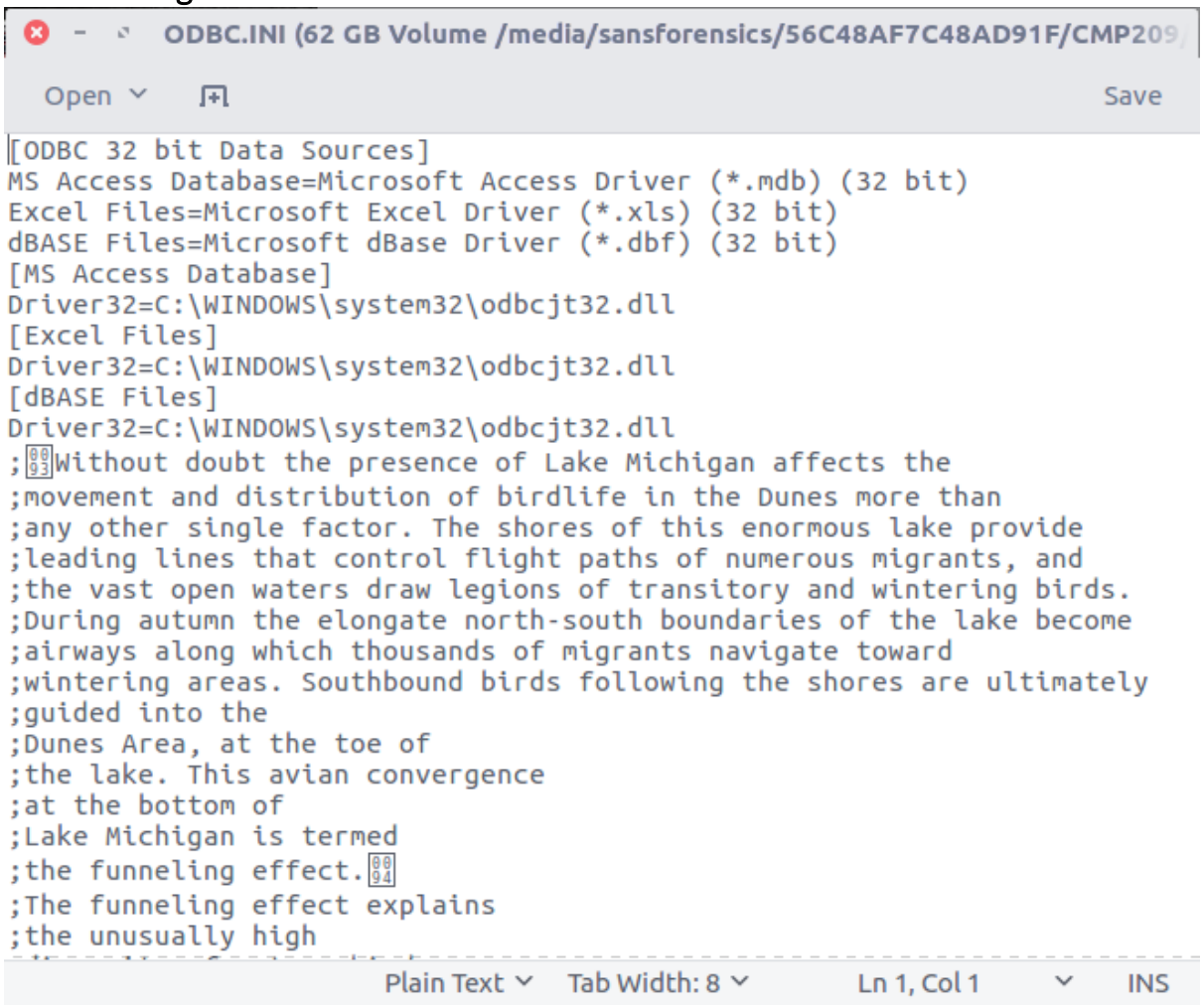
Figure 4: johndoe User Account | Mozilla Firefox History

History File: index.dat Version: 5.2			
TYPE	URL	MODIFIED TIME	ACCESS TIME
URL	Visited: bob@about:Home	02/03/2005 10:12	02/03/2005 10:12
URL	Visited: bob@file:///C:/Documents%20and%20Settings/bob/My%20Documents/Dear%20Fred.doc	02/03/2005 10:30	02/03/2005 10:30

Figure 5: bob User Account | Internet Explorer History

6.8. Appendix 8 – Bird related documents

6.8.1. Configuration File



6.8.2. Word Documents

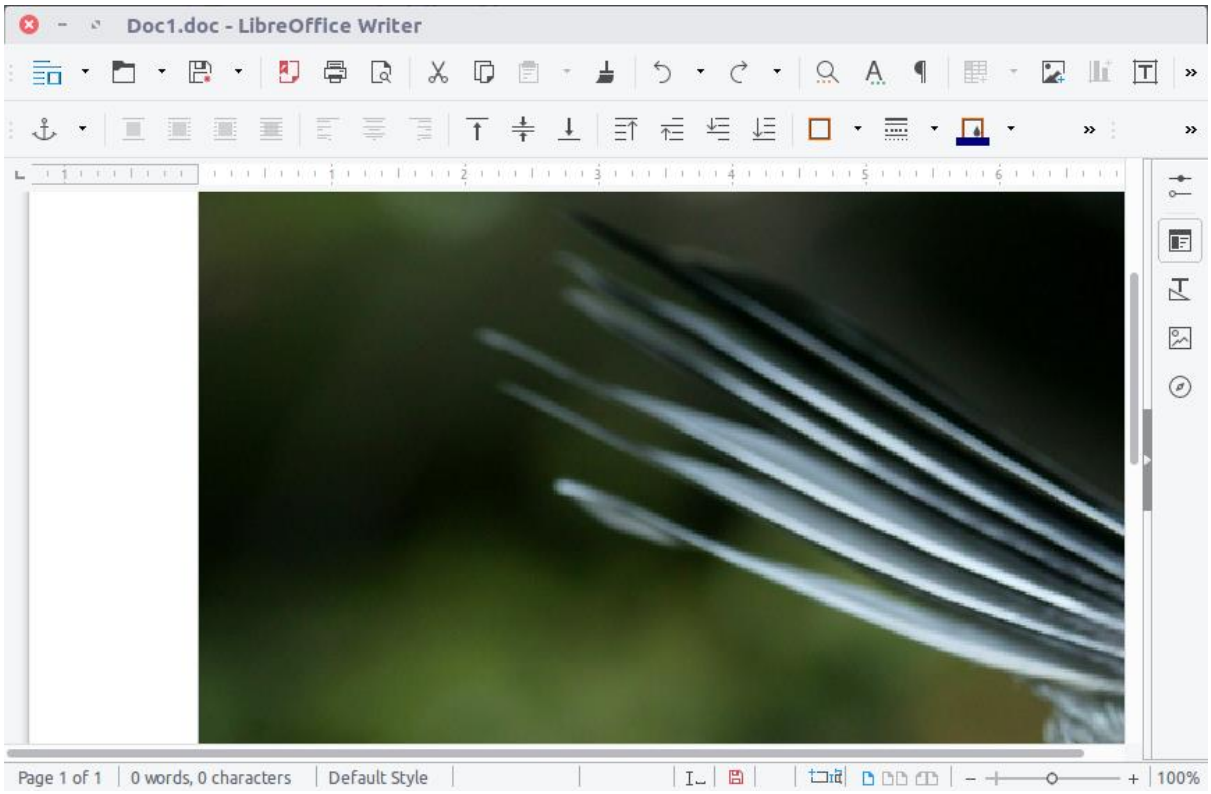


Figure 1: Image of Doc1.doc Contents

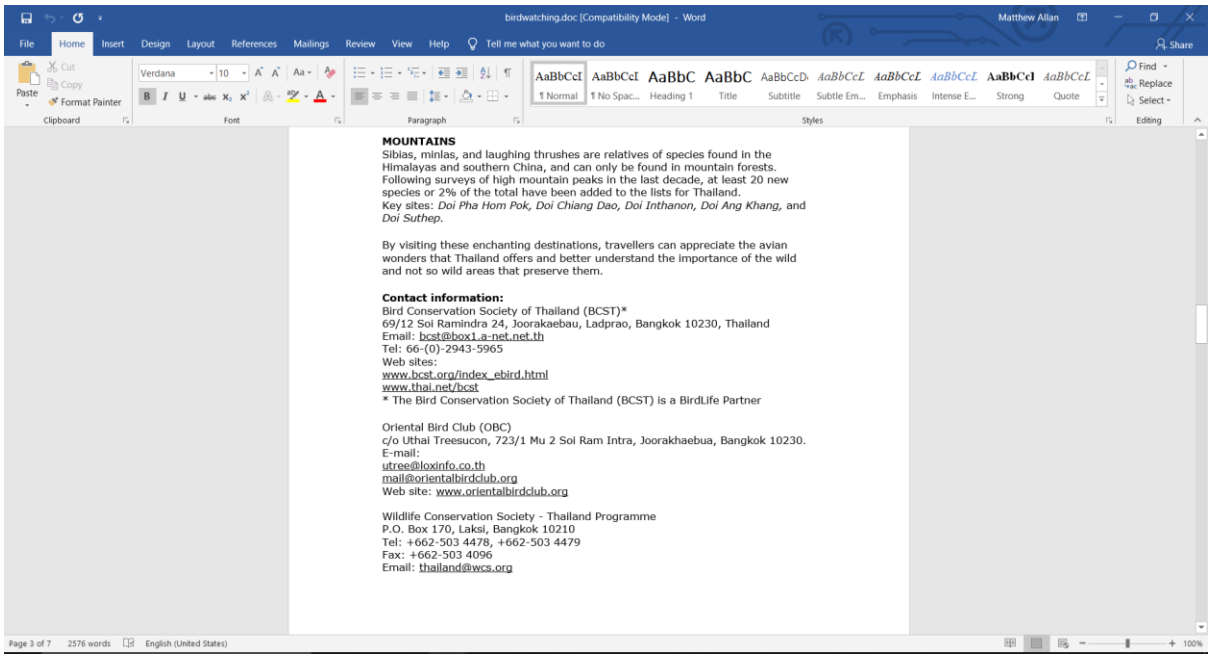
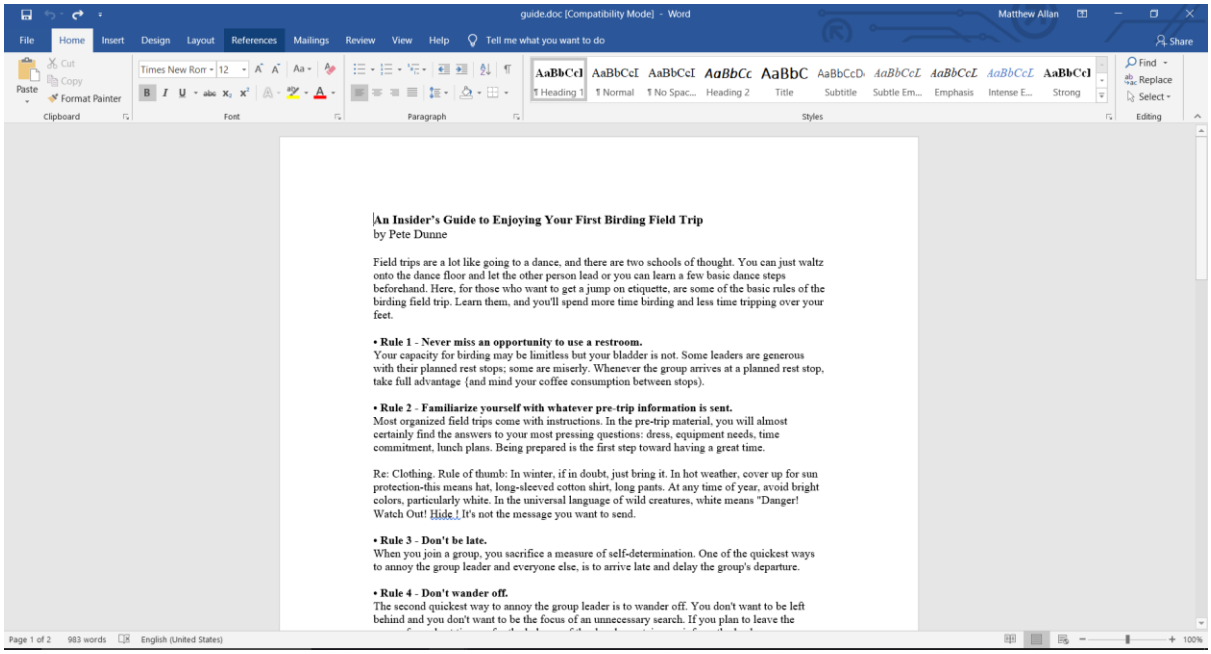


Figure 2: Snippet of birdwatching.doc showing contact information | Full file is available as a separate deliverable



An Insider's Guide to Enjoying Your First Birding Field Trip
by Pete Dunne

Field trips are a lot like going to a dance, and there are two schools of thought. You can just waltz onto the dance floor and let the other person lead or you can learn a few basic dance steps beforehand. Here, for those who want to get a jump on etiquette, are some of the basic rules of the birding field trip. Learn them, and you'll spend more time birding and less time tripping over your feet.

• **Rule 1 - Never miss an opportunity to use a restroom.**
Your capacity for birding may be limitless but your bladder is not. Some leaders are generous with their planned rest stops; some are miserly. Whenever the group arrives at a planned rest stop, take full advantage {and mind your coffee consumption between stops).

• **Rule 2 - Familiarize yourself with whatever pre-trip information is sent.**
Most organized field trips come with instructions. In the pre-trip material, you will almost certainly find the answers to your most pressing questions: dress, equipment needs, time commitment, lunch plans. Being prepared is the first step toward having a great time.

Re: Clothing. Rule of thumb: In winter, if in doubt, just bring it. In hot weather, cover up for sun protection-this means hat, long-sleeved cotton shirt, long pants. At any time of year, avoid bright colors, particularly white. In the universal language of wild creatures, white means "Danger! Watch Out! Hide ! It's not the message you want to send.

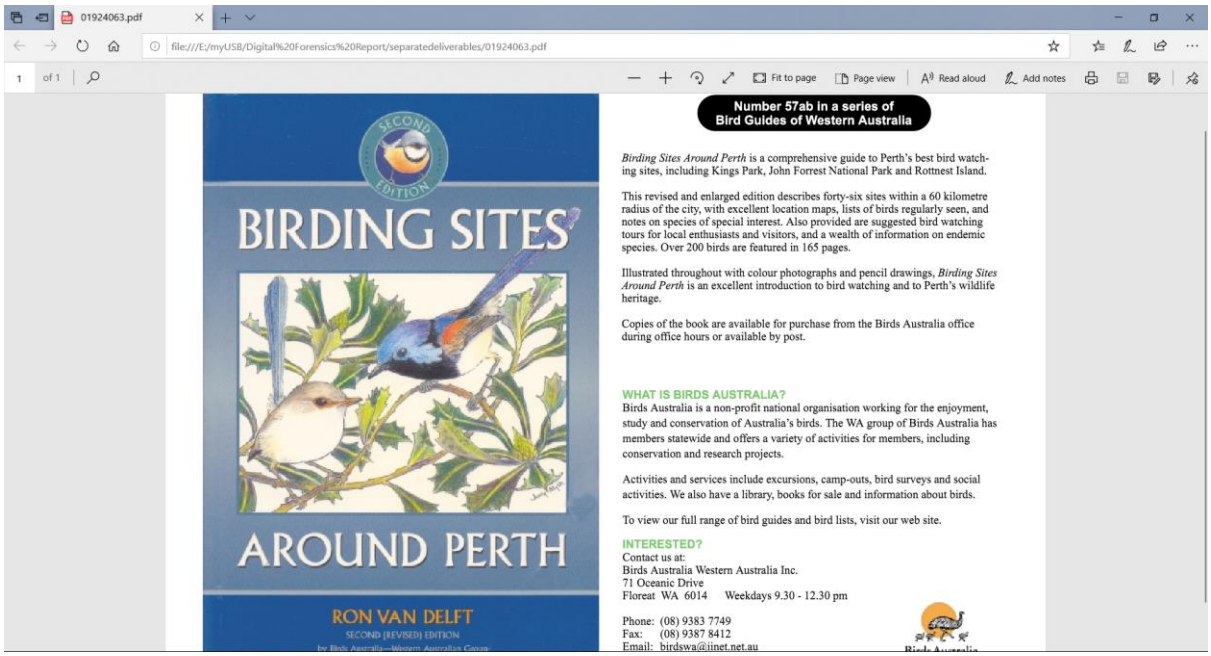
• **Rule 3 - Don't be late.**
When you join a group, you sacrifice a measure of self-determination. One of the quickest ways to annoy the group leader and everyone else, is to arrive late and delay the group's departure.

• **Rule 4 - Don't wander off.**
The second quickest way to annoy the group leader is to wander off. You don't want to be left behind and you don't want to be the focus of an unnecessary search. If you plan to leave the

Figure 3: Snippet of guide.doc | Full file is available as a separate deliverable

6.8.3. PDF Documents

Due to the size of these documents they have been included as separate deliverables, snapshots of each document can be viewed here.



Number 57ab in a series of
Bird Guides of Western Australia

BIRDING SITES
AROUND PERTH
RON VAN DELFT
SECOND (REVISED) EDITION

Birding Sites Around Perth is a comprehensive guide to Perth's best bird watching sites, including Kings Park, John Forrest National Park and Rottnest Island.

This revised and enlarged edition describes forty-six sites within a 60 kilometre radius of the city, with excellent location maps, lists of birds regularly seen, and notes on species of special interest. Also provided are suggested bird watching tours for local enthusiasts and visitors, and a wealth of information on endemic species. Over 200 birds are featured in 165 pages.

Illustrated throughout with colour photographs and pencil drawings, *Birding Sites Around Perth* is an excellent introduction to bird watching and to Perth's wildlife heritage.

Copies of the book are available for purchase from the Birds Australia office during office hours or available by post.

WHAT IS BIRDS AUSTRALIA?
Birds Australia is a non-profit national organisation working for the enjoyment, study and conservation of Australia's birds. The WA group of Birds Australia has members statewide and offers a variety of activities for members, including conservation and research projects.

Activities and services include excursions, camp-outs, bird surveys and social activities. We also have a library, books for sale and information about birds.

To view our full range of bird guides and bird lists, visit our web site.

INTERESTED?
Contact us at:
Birds Australia Western Australia Inc.
71 Oceanic Drive
Floreat WA 6014 Weekdays 9.30 - 12.30 pm

Phone: (08) 9383 7749
Fax: (08) 9387 8412
Email: birdswa@iinet.net.au

Figure 1: 01924063.pdf

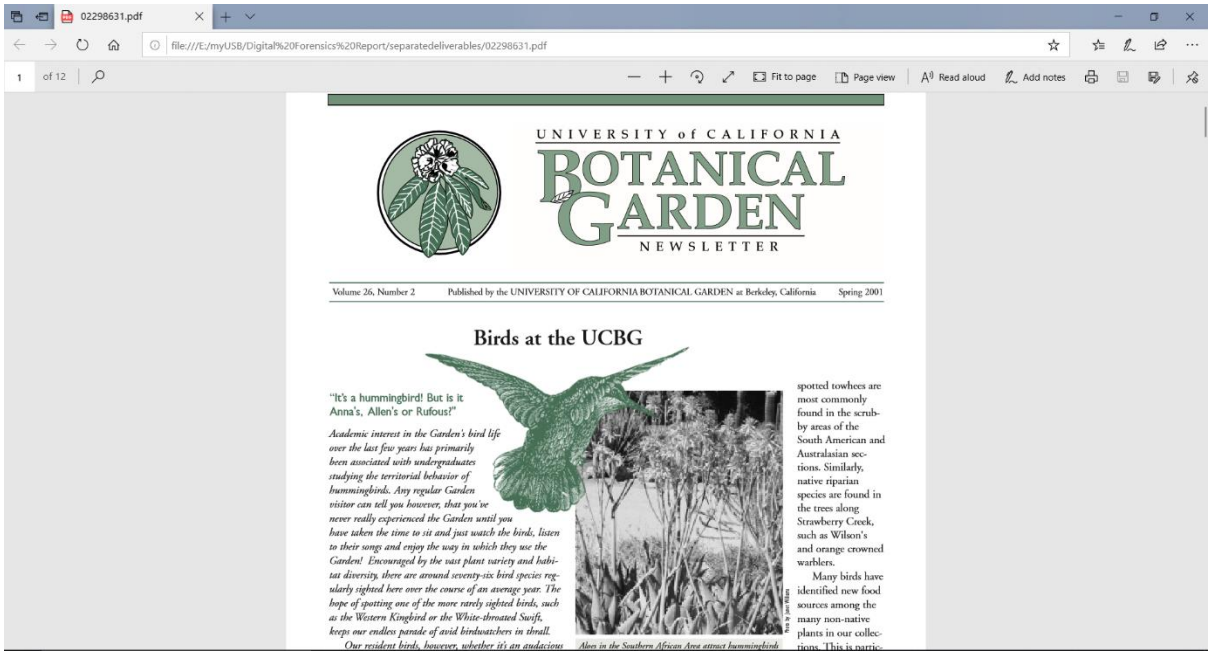


Figure 2: 02298631.pdf

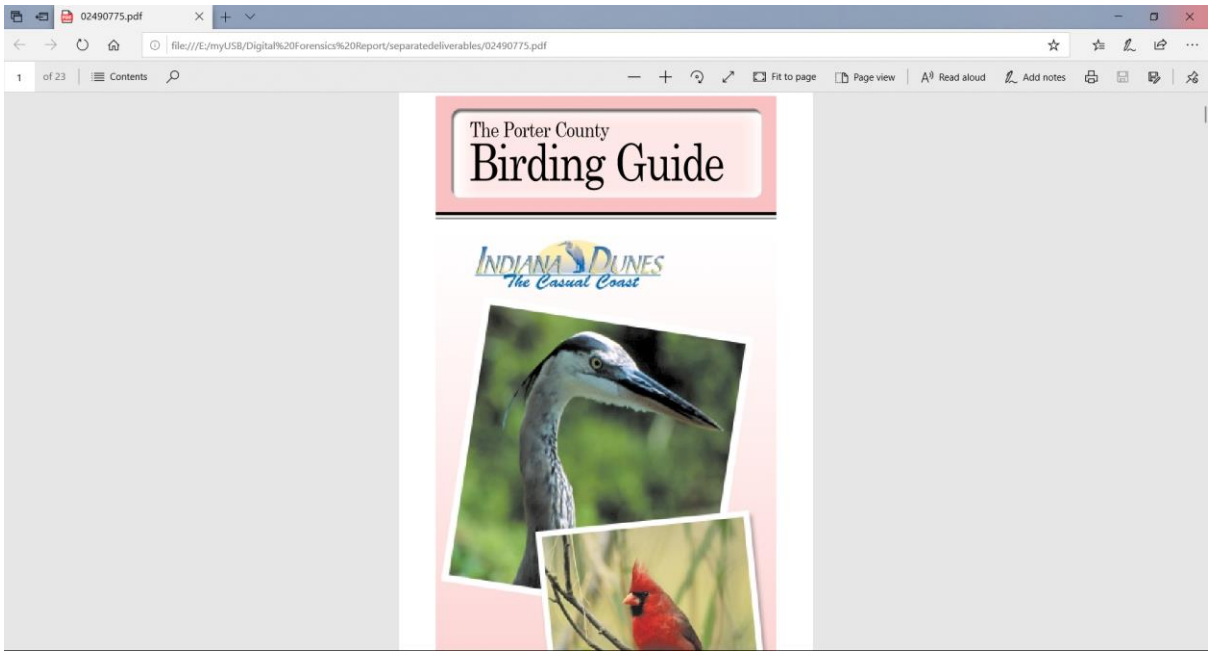


Figure 3: 02490775.pdf

6.8.4. TXT File

This file has been included as a separate deliverable; this is a snapshot of part of the document.

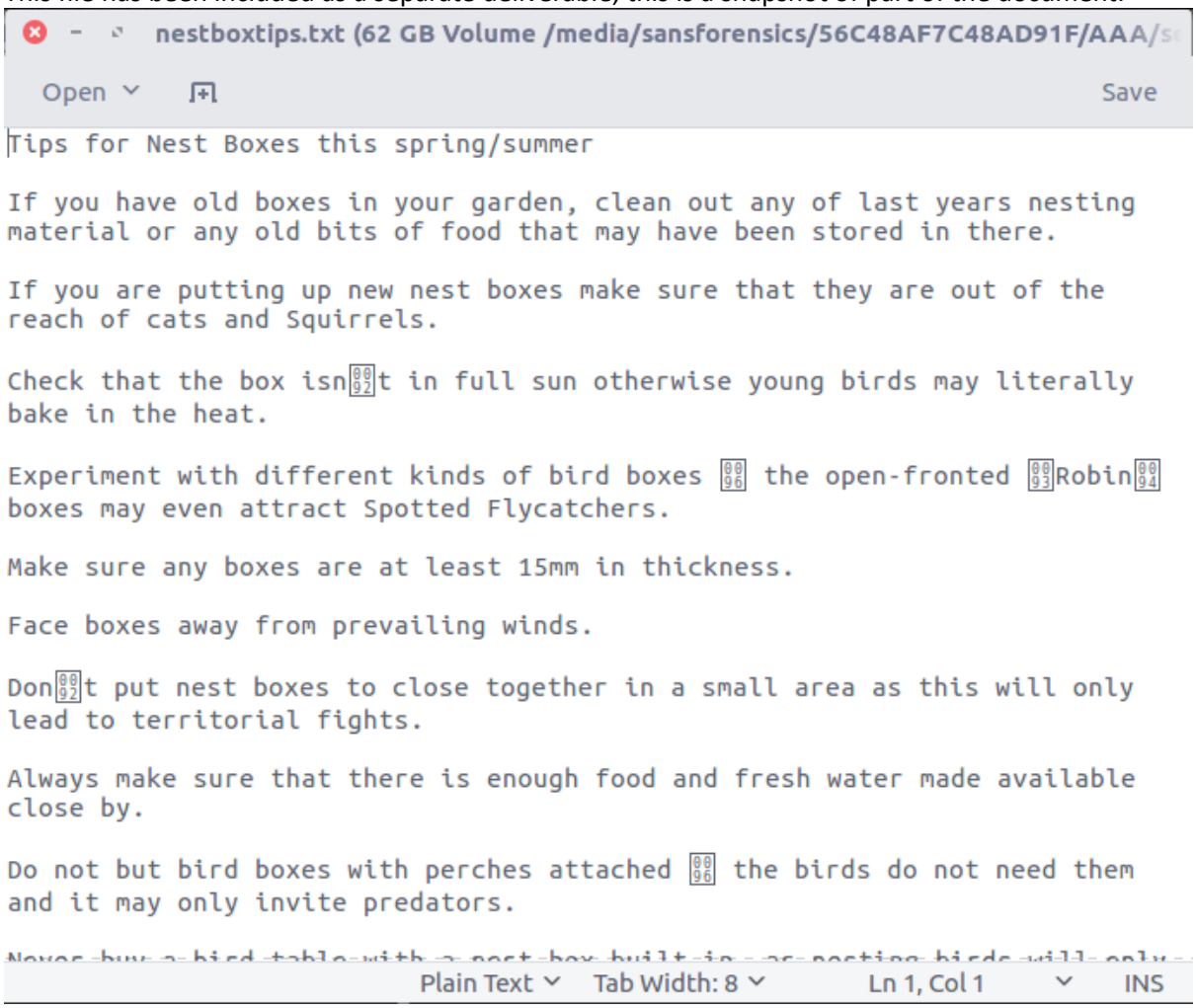


Figure 1: nextboxtips.txt

6.8.5. HTM Files

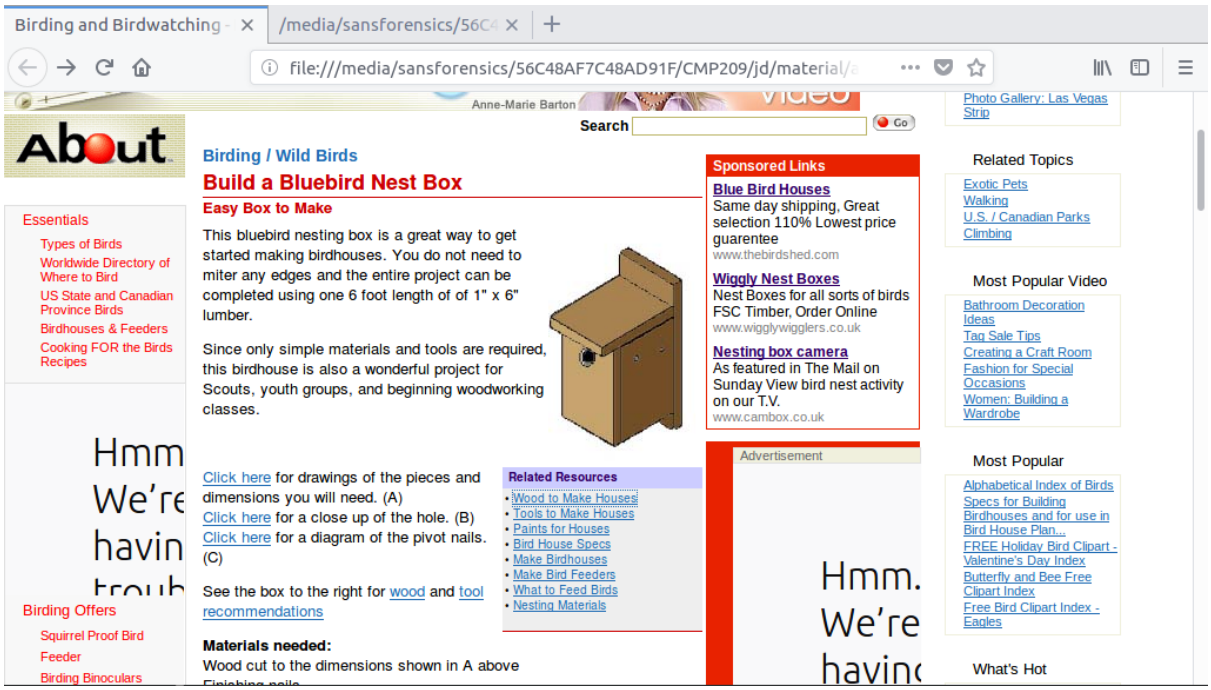


Figure 1: aa010703a.htm

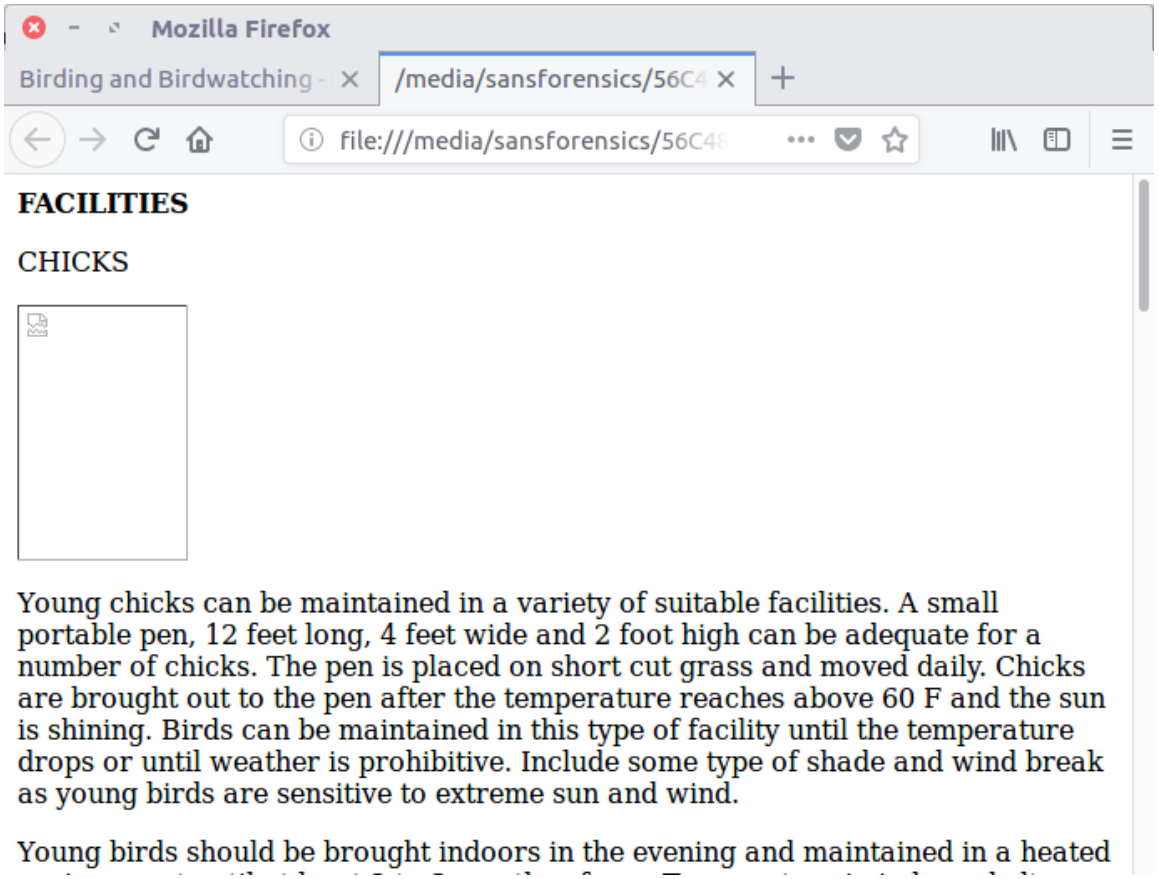


Figure 2: ostbk2b2.htm

6.9. Appendix 9 – Audio Related Bird Files

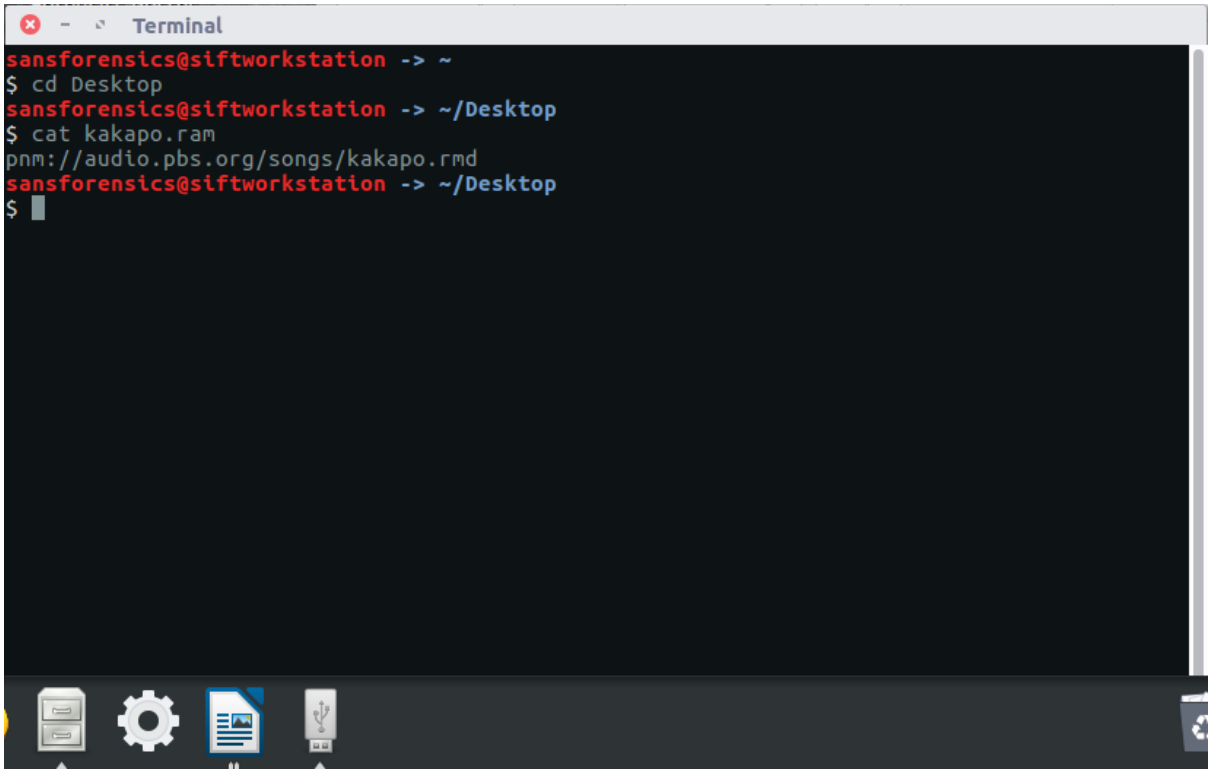


Figure 1: Contents of kakapo.ram file.

Figure 2: Website that kakapo.ram links to with a new URL

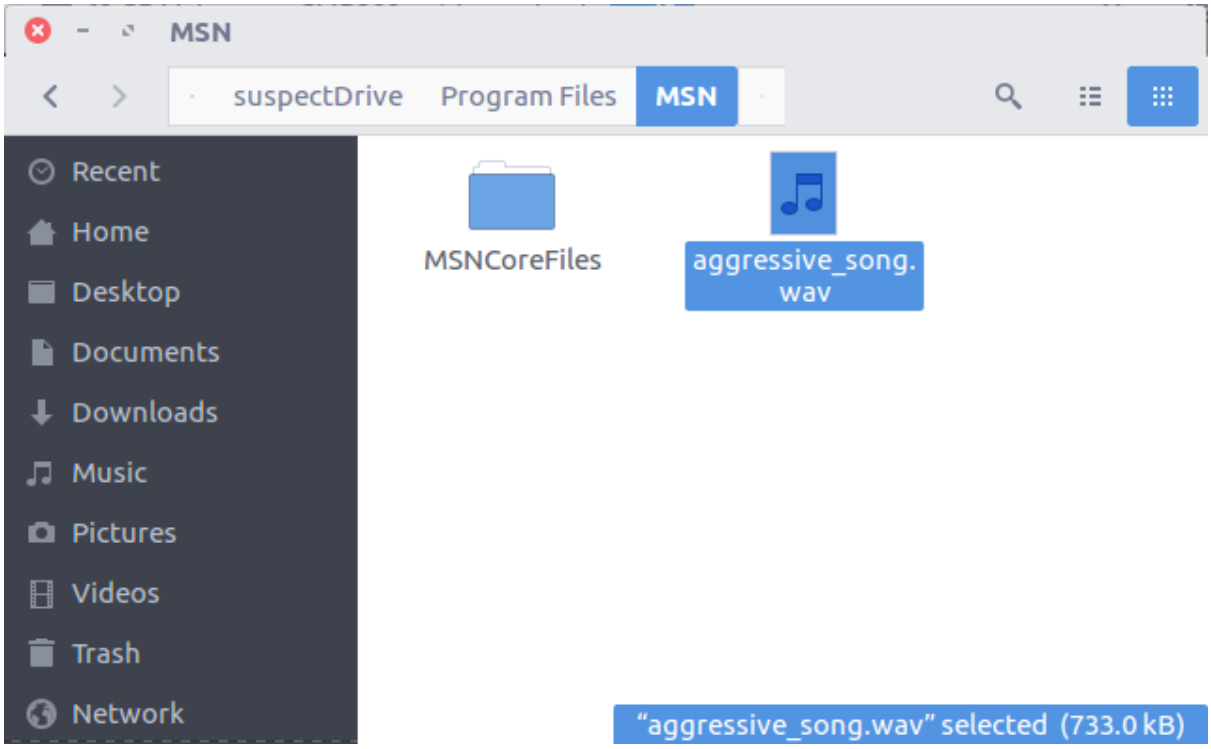


Figure 3: The audio file is available as an external deliverable named aggressive_song.wav

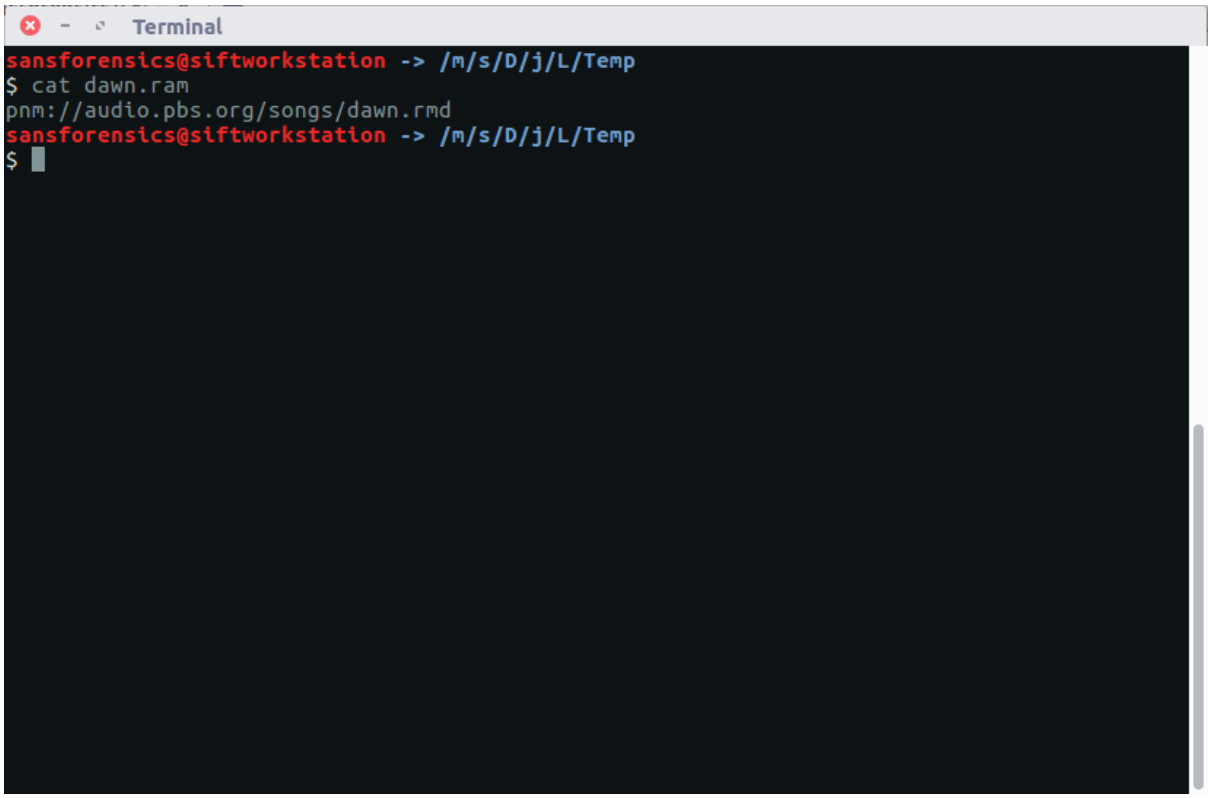


Figure 4: dawn.ram contents

6.10. Appendix 10 – E-mail

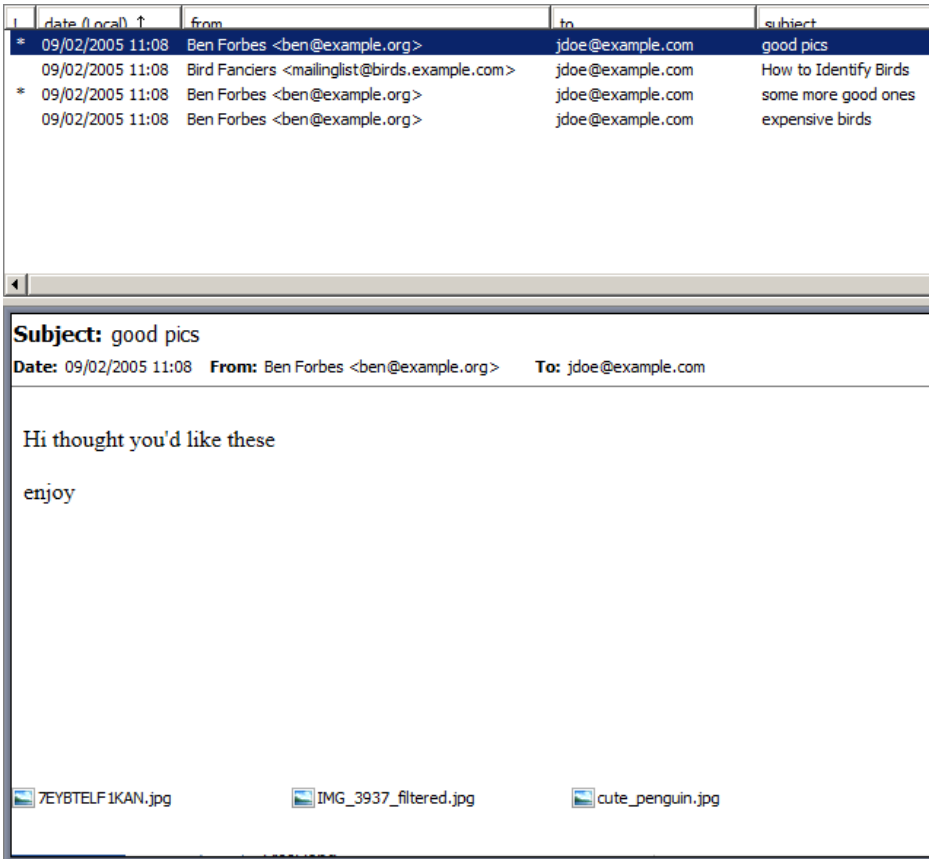


Figure 1: E-mail contents

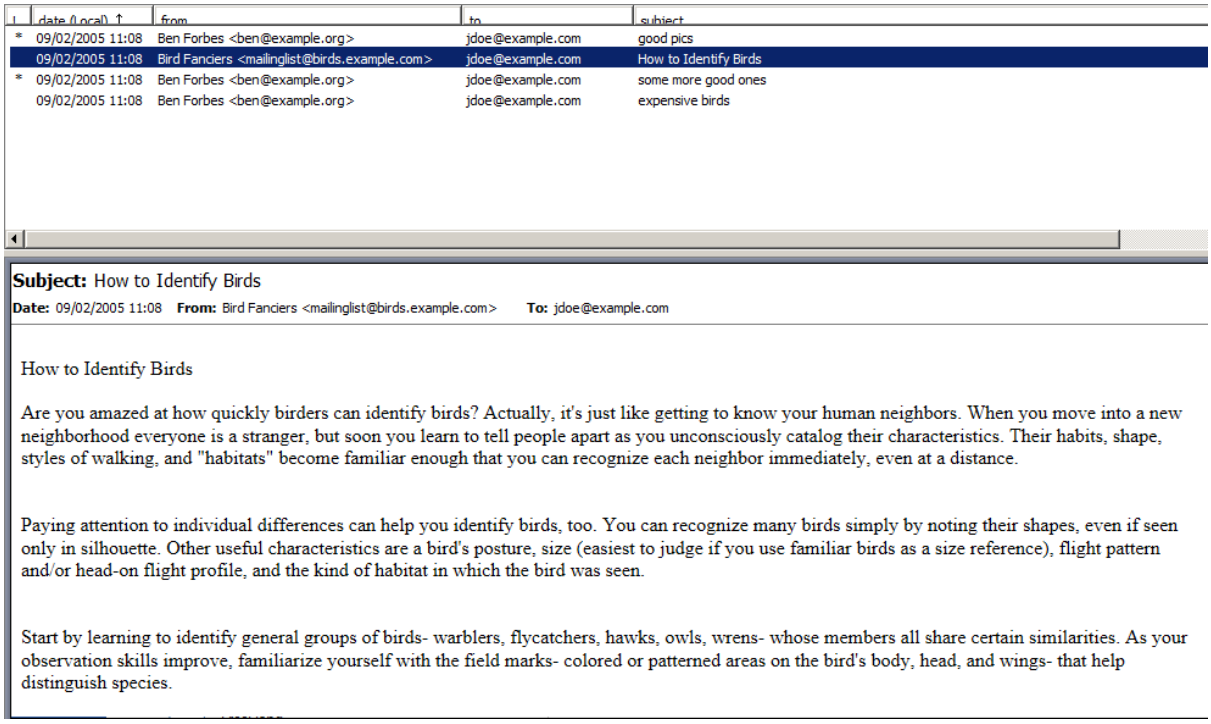


Figure 2: E-mail Contents

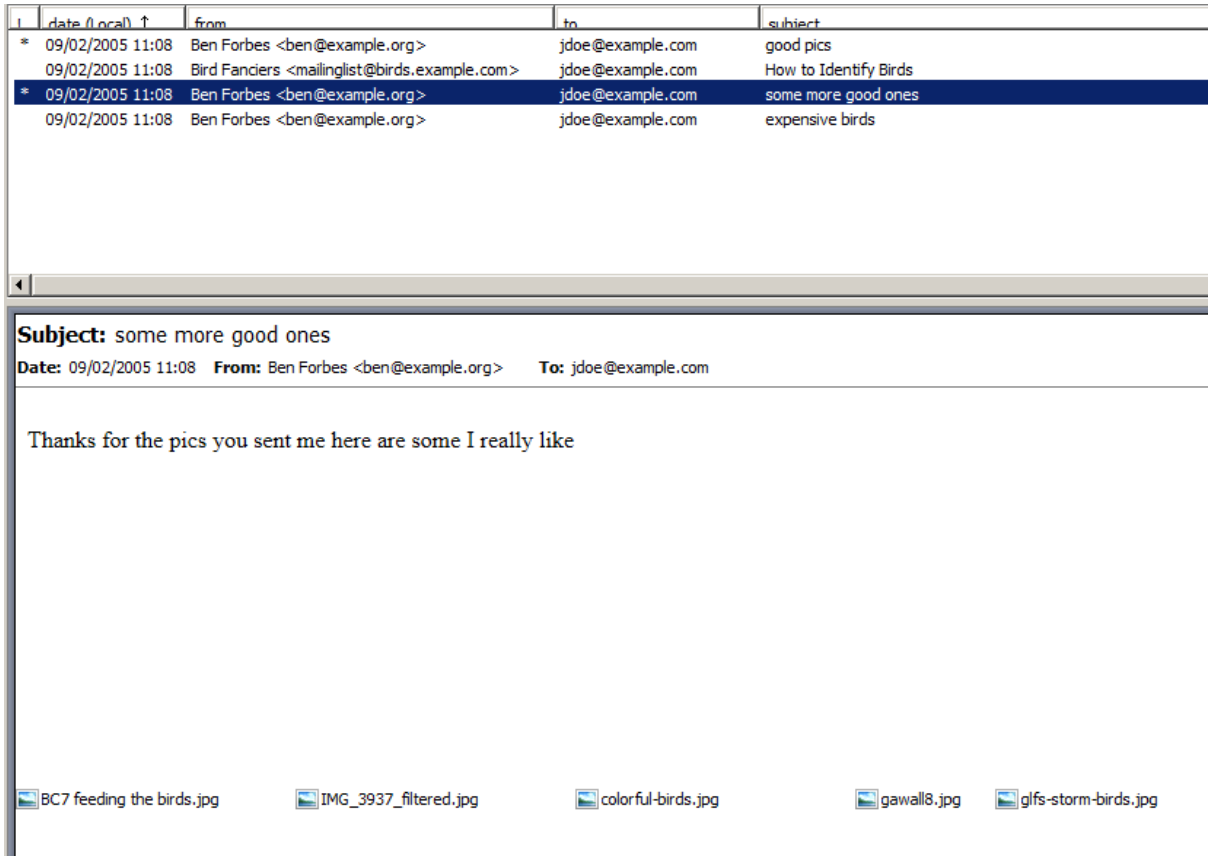


Figure 3: E-mail Contents

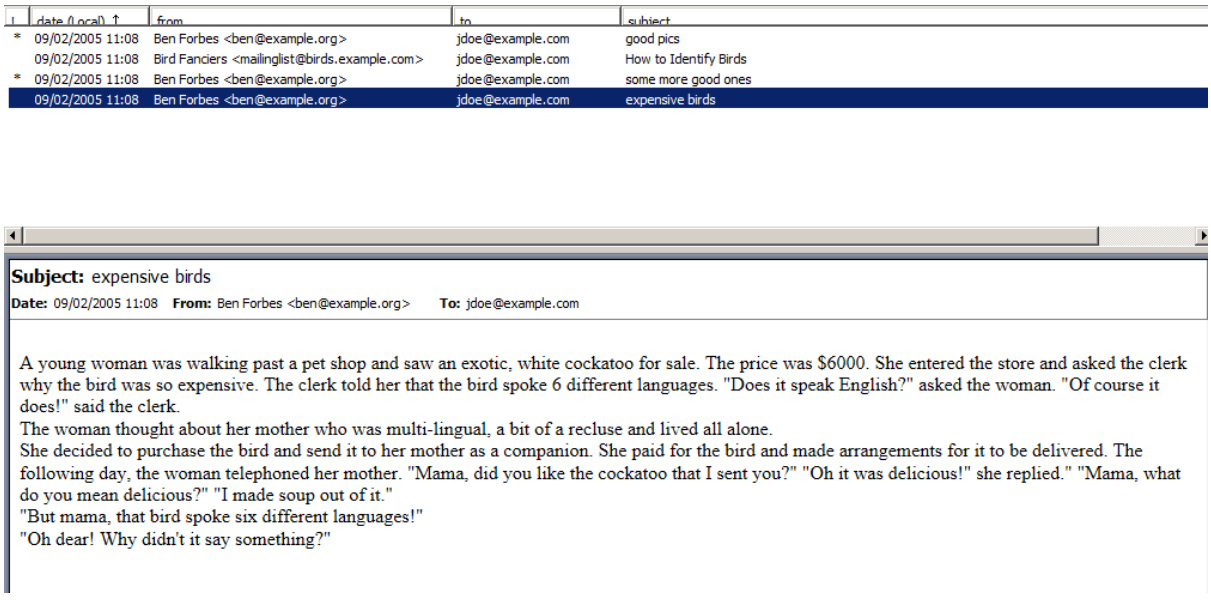
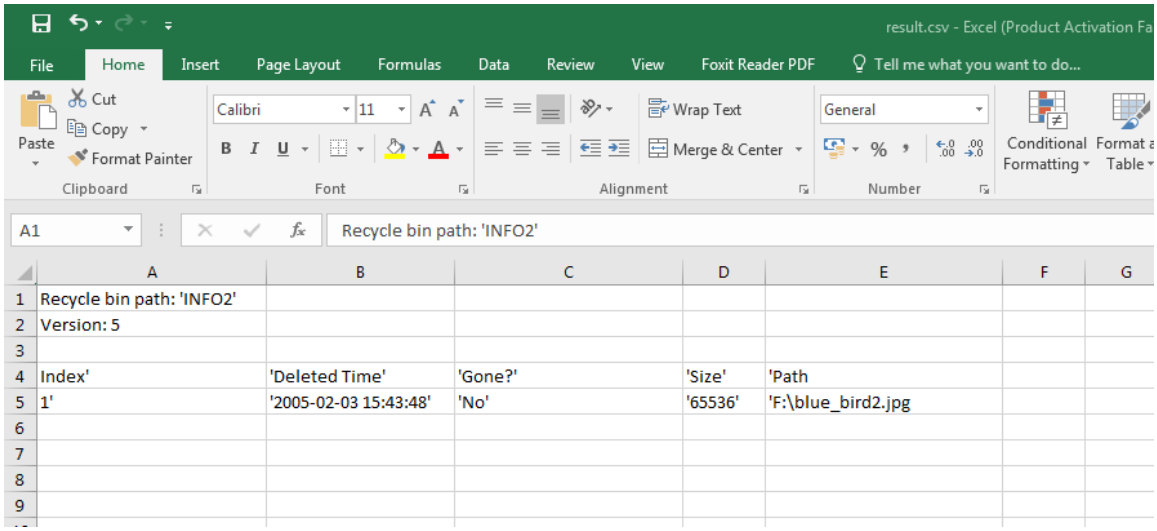


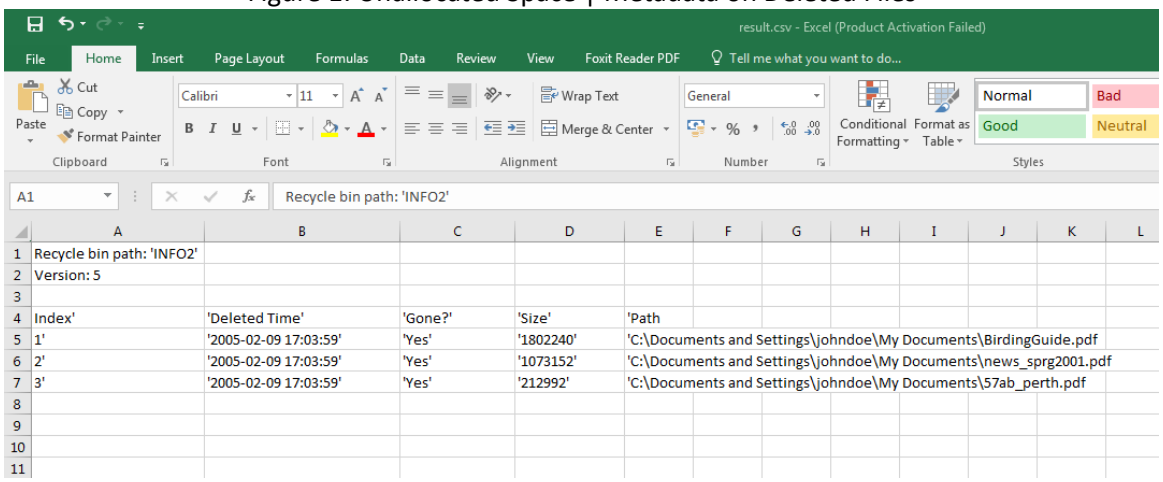
Figure 4: E-mail Contents

6.11. Appendix 11 – Miscellaneous



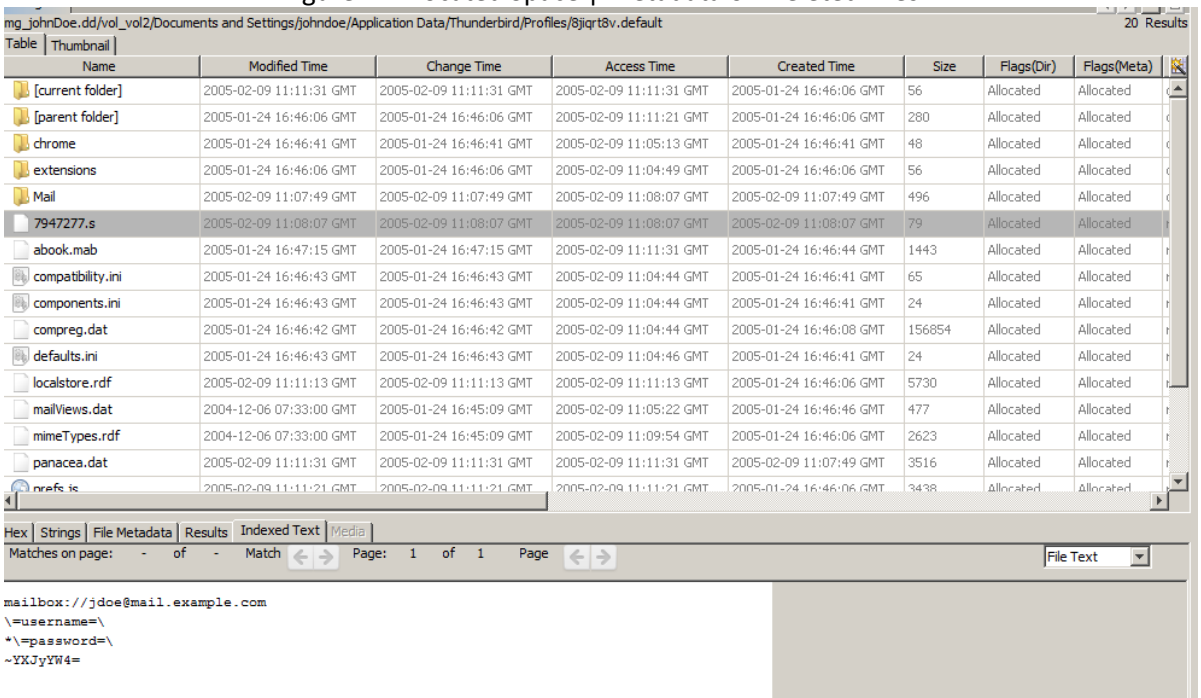
	A	B	C	D	E
1	Recycle bin path: 'INFO2'				
2	Version: 5				
3					
4	Index'	'Deleted Time'	'Gone?'	'Size'	'Path
5	1'	'2005-02-03 15:43:48'	'No'	'65536'	'F:\blue_bird2.jpg

Figure 1: Unallocated Space | Metadata on Deleted Files



	A	B	C	D	E
1	Recycle bin path: 'INFO2'				
2	Version: 5				
3					
4	Index'	'Deleted Time'	'Gone?'	'Size'	'Path
5	1'	'2005-02-09 17:03:59'	'Yes'	'1802240'	'C:\Documents and Settings\johndoe\My Documents\BirdingGuide.pdf
6	2'	'2005-02-09 17:03:59'	'Yes'	'1073152'	'C:\Documents and Settings\johndoe\My Documents\news_sprg2001.pdf
7	3'	'2005-02-09 17:03:59'	'Yes'	'212992'	'C:\Documents and Settings\johndoe\My Documents\57ab_perth.pdf

Figure 2: Allocated Space | Metadata on Deleted Files



Name	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
[current folder]	2005-02-09 11:11:31 GMT	2005-02-09 11:11:31 GMT	2005-02-09 11:11:31 GMT	2005-01-24 16:46:06 GMT	56	Allocated	Allocated
[parent folder]	2005-01-24 16:46:06 GMT	2005-01-24 16:46:06 GMT	2005-02-09 11:11:21 GMT	2005-01-24 16:46:06 GMT	280	Allocated	Allocated
chrome	2005-01-24 16:46:41 GMT	2005-01-24 16:46:41 GMT	2005-02-09 11:05:13 GMT	2005-01-24 16:46:41 GMT	48	Allocated	Allocated
extensions	2005-01-24 16:46:06 GMT	2005-01-24 16:46:06 GMT	2005-02-09 11:04:49 GMT	2005-01-24 16:46:06 GMT	56	Allocated	Allocated
Mail	2005-02-09 11:07:49 GMT	2005-02-09 11:07:49 GMT	2005-02-09 11:08:07 GMT	2005-02-09 11:07:49 GMT	496	Allocated	Allocated
7947277.s	2005-02-09 11:08:07 GMT	2005-02-09 11:08:07 GMT	2005-02-09 11:08:07 GMT	2005-02-09 11:08:07 GMT	79	Allocated	Allocated
abook.mab	2005-01-24 16:47:15 GMT	2005-01-24 16:47:15 GMT	2005-02-09 11:11:31 GMT	2005-01-24 16:46:44 GMT	1443	Allocated	Allocated
compatibility.ini	2005-01-24 16:46:43 GMT	2005-01-24 16:46:43 GMT	2005-02-09 11:04:44 GMT	2005-01-24 16:46:41 GMT	65	Allocated	Allocated
components.ini	2005-01-24 16:46:43 GMT	2005-01-24 16:46:43 GMT	2005-02-09 11:04:44 GMT	2005-01-24 16:46:41 GMT	24	Allocated	Allocated
compreg.dat	2005-01-24 16:46:42 GMT	2005-01-24 16:46:42 GMT	2005-02-09 11:04:44 GMT	2005-01-24 16:46:08 GMT	156854	Allocated	Allocated
defaults.ini	2005-01-24 16:46:43 GMT	2005-01-24 16:46:43 GMT	2005-02-09 11:04:46 GMT	2005-01-24 16:46:41 GMT	24	Allocated	Allocated
localstore.rdf	2005-02-09 11:11:13 GMT	2005-02-09 11:11:13 GMT	2005-02-09 11:11:13 GMT	2005-01-24 16:46:06 GMT	5730	Allocated	Allocated
mailViews.dat	2004-12-06 07:33:00 GMT	2005-01-24 16:45:09 GMT	2005-02-09 11:05:22 GMT	2005-01-24 16:46:46 GMT	477	Allocated	Allocated
mimeTypes.rdf	2004-12-06 07:33:00 GMT	2005-01-24 16:45:09 GMT	2005-02-09 11:09:54 GMT	2005-01-24 16:46:06 GMT	2623	Allocated	Allocated
panacea.dat	2005-02-09 11:11:31 GMT	2005-02-09 11:11:31 GMT	2005-02-09 11:11:31 GMT	2005-02-09 11:07:49 GMT	3516	Allocated	Allocated

```
mailbox://jdoe@mail.example.com
\=username=\
*\=password=\
~YXJyYW4=
```

Figure 3: John Doe GPG password in Base64 Format | Found inside Mozilla Thunderbird Client