RESTRICTED

# Digital Forensics Examination Court Report


**Suspect Name: John Doe**

**Investigation Team: Imogen Rose**

**Patrick Collins**

**Riccardo Raso**

**Vanessa-Maria Ispas-Sava**


## CMP209: Digital Forensics 1

## 2020/21

RESTRICTED

# Table of Contents

## Case Summary

The SPEKTOR investigation team was assigned the case of Mr. John Doe with the purpose of collecting and examining evidence in order to prove that the suspect was in possession of unlawful material related to birds. Upon examining a copy of his computer's hard drive's storage, multiple illicit files were found, including images, email messages, audio files, and text files.

In order to perform this investigation, a copy of the hard drive's storage was obtained, which was compiled into a file named johnDoe.dd and placed into a zip file to maintain its integrity. The following sections present the process and results of the analysis of this copy.

## Description of Crime and Timeline of Events

The defendant, Mister John Doe, has been accused of browsing, storing, and attempting to hide and destroy files associated with birds. In order to establish a behavioural pattern, the unlawful actions discovered during the investigation were compiled into a timeline. The following figure presents a brief timeline of the major incidents.

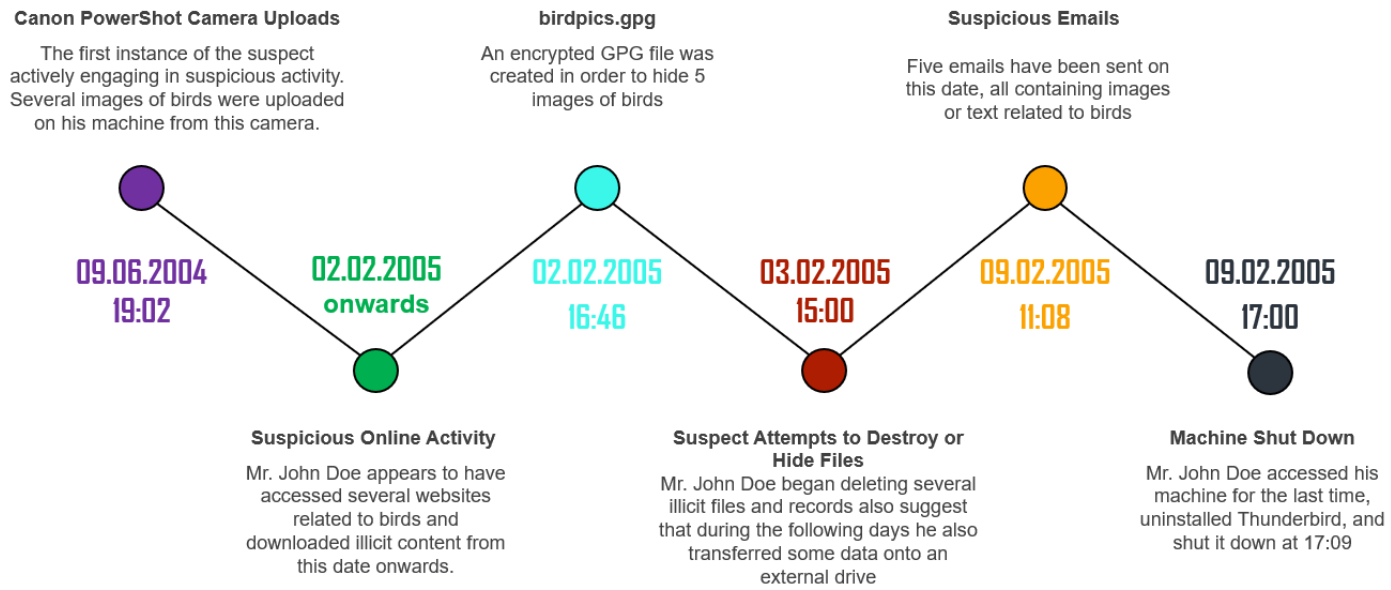



Figure 1. Main Incidents Timeline

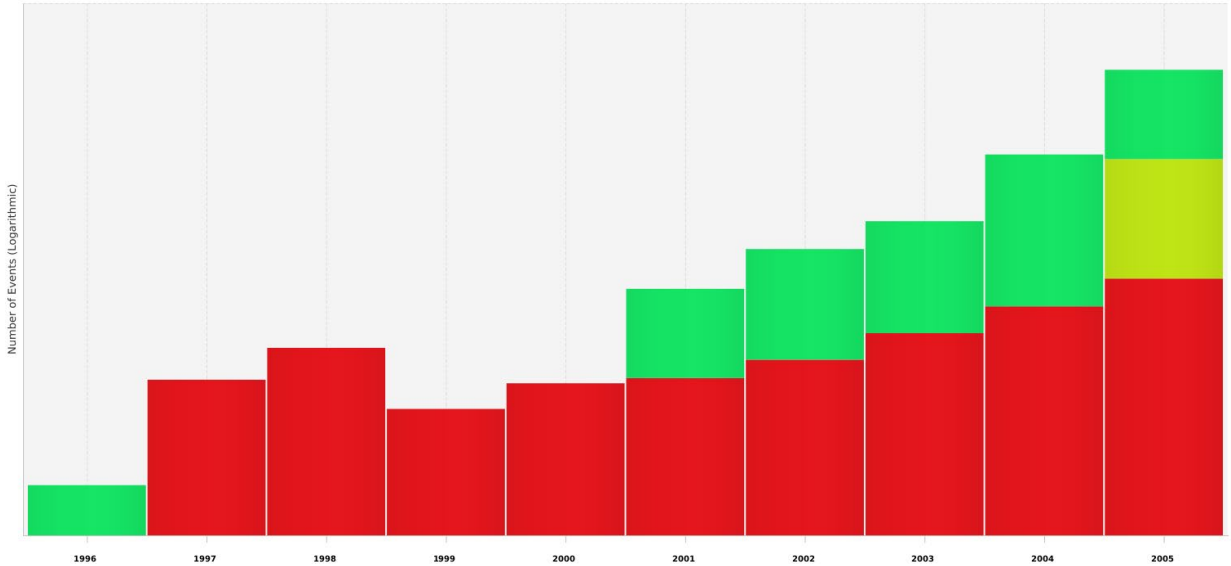


Figure 2. Autopsy Timeline Graph. Number of events steadily increased from 2001 to 2005

The following graph was created using the Autopsy tool, and it displays the frequency of events on the suspect's computer every year. The johnDoe.dd file was loaded into Autopsy, and the timeline option was selected. This resulted in a total of 11,424 events, which can be viewed in detail in Appendix 1.

Zeitline tool was also used for timelining events by merging all Pasco files from the machine's browser history into one final Pasco file. This file was then loaded into Zeitline, and the data was filtered by Pasco. The Zeitline tool ordered all dates chronologically to facilitate examining 350 events. Significant moments of these events are seen in Appendix 1, Figure 26.

## Investigation Process

The following sections detail the steps taken in order to examine the hard drive copy and extract evidence from it. It must be noted that there are seven users in total on the disk, with the most notable being ben, jane and johndoe, with the johndoe account being the focus of the investigation.

## Preparation

Tasks were divided among the team members in order to perform a thorough search and maximise time efficiency. Upon commencing the investigation, all members needed to comply with ACPO guidelines at every stage, and so the first step in handling the johnDoe.dd file was to change its permission to read-only using chmod 400. This was done in order to maintain the file's integrity and avoid changing any data on it.

## Antivirus Scan

The suspect had an anti-virus program installed called “McAfee AntiVirus”. The suspect ran regular malware scans, such as on 2005-01-24 5:03:54 GMT. This can be found in the evidence folder.

Before proceeding further with the investigation, an antivirus scan of the johnDoe.dd file was performed in order to determine if there was any malware present that could have planted incriminating evidence. The scan was performed using ClamAV, as seen in Appendix 2, and resulted in discovering an infected file, realplay.exe located at /home/student/mnt/suspectDrive/Program Files/Real/RealPlayer/realplay.exe on the suspect's system. ClamAV suggests this file is a Trojan virus, which usually acts as a practical application that could modify the computer's files when run.

There is a possibility that this might have caused some perturbance by changing files on the suspect system; however, this file has been on the computer from 02.02.2005 onwards. While files that suggest an inappropriate infatuation with birds have been present on the drive since 2004, starting with the pictures uploaded from the suspect's Canon PowerShot camera.

## Camera Images

A bash file was created to automate the process of extracting all images that only had file extension "jpg" and generating a copy of those images that had their EXIF header containing "Canon PowerShot" as for make and model of the assumed camera.

The bash file generated the hash sum value of johnDoe.dd, a crucial precautionary step to verify its integrity, then collected all JPG images and stored them into a folder. Following this, whitelists of the EXIF-headers were produced for copying the images taken by the camera into a subdirectory. Other bash files were generated for other repetitive tasks, such as mounting and unmounting the suspect's drive. The whole script is available in Appendix 4 and its scan results in Appendix 5. A similar method was also used in order to acquire most of the other images on the drive.

According to the JPG files with a valid EXIF header, 48 photos were produced with a Canon PowerShot SD100; two images were produced with a Canon EOS-1DS and one with a Sony Cybershot. However, not all JPG files recovered by the SPEKTOR Team had or contained a valid EXIF header.

Foremost -all and Autopsy were used for extracting all the other accessible files contained into the suspect's drive before mounting it.

## Checklists

After mounting johnDoe.dd, a hash list was created for all files on the disk. The exact process was applied to a fresh WindowsXP image. Text files were created containing only JPEG or BMP extensions from both disk images. A part of the WindowsXP text files were deleted to only contain JPEG or BMP hashes. Finally, these text files were used to compare which JPEG and BMP images were added since the suspect first started using the system. The results are included in the evidence folder provided.

# Internet Activity

Using Autopsy, several files related to the suspect's activity on the internet were extracted and analysed, including search history, cache, cookies and emails. The following sections detail the findings relevant to this case.

## Search History

The browser analysis procedure commenced with the analysis of the machine's browsing history, which can be viewed in full in Appendix 6. It must be noted that the suspect had two browsers installed on his machine, Internet Explorer and Mozilla Firefox, which he used to access websites related to birds. These web pages were found by examining the browser history, searching for HTM files or analysing cache and cookies. Some examples of the websites accessed, as well as other collected data, can be found in Appendix 9.

## Downloaded Files

The suspect downloaded several files related to birds through his browser, this activity being recorded into a file named download.rdf, which is available in Appendix 7. The content downloaded includes a zip file, an audio file and 8 pictures. Using the name of the files, Autopsy's search function was used in order to locate and extract them.

## Emails

The suspect was using Mozilla Thunderbird in order to send and receive email messages. He later uninstalled the email application and attempted to erase all messages, perhaps in order to destroy evidence. Four email messages were found in total, three of them sent by Ben, who not only sent John some pictures and other bird related materials, but he also appears to have received some pictures from John himself at some point according to Email #3 (see Appendix 8).

The other email, Email #4, was received from a subscription service named Bird Fanciers, and it contains information on how to identify birds. This suggests that John had a keen interest in birds as he deliberately subscribed to receive these emails.

## Birdpics.gpg

A GPG file called 'birdpics.gpg' was found in the directory 'C:/Documents and Settings/johndoe/My Documents/' on the suspect drive. GPG files are encrypted, and password protected and by creating a file of this type it indicates that the suspect was trying to hide its contents.

The file containing the key was found in the directory' C:/Documents and Settings/johndoe/Application Data/GnuPG', named 'secring.gpg', and was created on 02-02-2005. This file was converted to a JTR file that the John the Ripper dictionary could use. A hash file was then created from this file and then the hash compared to a wordlist containing any of the passwords on the suspect drive. The password was discovered to be 'arran'.

The password was then entered into the secring.gpg file, when it was opened, which decrypted then opened the birdpics.gpg file. The birdpics.gpg file was converted to a .dat file. The file was then found to be a zip folder, so was converted to a .zip file, that when unzipped, contained 5 images – all images have names that are related to birds. However, only one of the images, WhiteThroatedSparrowInTree.jpg, was recovered due to a file error. This image, as well as the names of the other images contained in this file, can be seen in Appendix 10.

As these files were found in directories that had the suspect's name, this implies that it was the suspect who created this file.

## Registry Analysis

The first phase of the stage, Fred was used for examining the registry files; further analysis was then conducted with Autopsy. Registry files over a Windows machine can be located in the default directory under *%SYSTEMROOT%\system32\config*. The files contained in the directory mentioned above are also known as hives. These can contain generic information about the local machine, such as *HKEY_LOCAL_MACHINE* found in SAM, or information regarding single users and their settings, such as NTUSER.DAT, which corresponds to the hive named *HKEY_CURRENT_USER.* Removing NTUSER.DAT would corrupt the user profile and make Windows prompting to not sign into the account. NTUSER.DAT hives were found among the deleted files together with SAM, SECURITY, SOFTWARE, and SYSTEM; this could therefore be an attempt of preventing the forensic staff from recovering critical information. However, NTUSER.DAT hives were analysed, bringing the investigative team to confirm some results and highlight some more. The scan result files can be found in the Evidence folder provided.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 706 | OBJECTS.DATA | 2005-02-02 16:35:33 GMT | 2005-02-02 16:35:33 GMT | 2005-02-02 16:59:11 GMT | 2005-02-02 16:59:10 GMT | 0 | Unallocated | U |
| 707 | OBJECTS.MAP | 2005-02-02 16:59:02 GMT | 2005-02-02 16:59:02 GMT | 2005-02-02 16:59:11 GMT | 2005-02-02 16:59:11 GMT | 2492 | Unallocated | U |
| 708 | _REGISTRY_MACHINE_SAM | 2005-02-02 16:59:09 GMT | 2005-02-02 16:59:09 GMT | 2005-02-02 16:59:09 GMT | 2005-02-02 16:59:09 GMT | 28672 | Unallocated | U |
| 709 | _REGISTRY_MACHINE_SECURITY | 2005-02-02 16:59:03 GMT | 2005-02-02 16:59:03 GMT | 2005-02-02 16:59:03 GMT | 2005-02-02 16:59:03 GMT | 45056 | Unallocated | U |
| 710 | _REGISTRY_MACHINE_SOFTWARE | 2005-02-02 16:59:08 GMT | 2005-02-02 16:59:08 GMT | 2005-02-02 16:59:08 GMT | 2005-02-02 16:59:04 GMT | 0 | Unallocated | U |
| 711 | _REGISTRY_MACHINE_SYSTEM | 2005-02-02 16:59:09 GMT | 2005-02-02 16:59:09 GMT | 2005-02-02 16:59:09 GMT | 2005-02-02 16:59:08 GMT | 3518464 | Unallocated | U |
| 712 | _REGISTRY_USER_.DEFAULT | 2005-02-02 16:59:03 GMT | 2005-02-02 16:59:03 GMT | 2005-02-02 16:59:03 GMT | 2005-02-02 16:59:03 GMT | 237568 | Unallocated | U |
| 713 | _REGISTRY_USER_NTUSER_S-1-5-18 | 2005-01-24 16:21:37 GMT | 2005-02-02 16:59:02 GMT | 2005-02-02 16:59:02 GMT | 2005-01-24 16:21:37 GMT | 262144 | Unallocated | U |
| 714 | _REGISTRY_USER_NTUSER_S-1-5-19 | 2005-02-02 16:59:02 GMT | 2005-02-02 16:59:02 GMT | 2005-02-02 16:59:02 GMT | 2005-02-02 16:59:02 GMT | 229376 | Unallocated | U |
| 715 | _REGISTRY_USER_NTUSER_S-1-5-20 | 2005-02-02 16:59:02 GMT | 2005-02-02 16:59:02 GMT | 2005-02-02 16:59:02 GMT | 2005-02-02 16:59:02 GMT | 225280 | Unallocated | U |
| 716 | _REGISTRY_USER_NTUSER_S-1-5-21-725345543-854245398-1202660629-1003 | 2005-02-02 16:59:03 GMT | 2005-02-02 16:59:03 GMT | 2005-02-02 16:59:03 GMT | 2005-02-02 16:59:03 GMT | 757760 | Unallocated | U |
| 717 | _REGISTRY_USER_USRCLASS_S-1-5-19 | 2005-02-02 16:59:02 GMT | 2005-02-02 16:59:02 GMT | 2005-02-02 16:59:02 GMT | 2005-02-02 16:59:02 GMT | 8192 | Unallocated | U |
| 718 | _REGISTRY_USER_USRCLASS_S-1-5-20 | 2005-02-02 16:59:03 GMT | 2005-02-02 16:59:03 GMT | 2005-02-02 16:59:03 GMT | 2005-02-02 16:59:02 GMT | 8192 | Unallocated | U |
| 719 | _REGISTRY_USER_USRCLASS_S-1-5-21-725345543-854245398-1202660629-1003 | 2005-02-02 16:59:03 GMT | 2005-02-02 16:59:03 GMT | 2005-02-02 16:59:03 GMT | 2005-02-02 16:59:03 GMT | 8192 | Unallocated | U |
| 720 | change.log.1 | 2005-02-03 15:54:06 GMT | 2005-02-03 17:43:21 GMT | 2005-02-03 15:54:06 GMT | 2005-02-02 16:59:10 GMT | 182386 | Unallocated | U |
| 721 | RestorePointSize | 2005-02-03 18:43:25 GMT | 2005-02-03 18:43:25 GMT | 2005-02-09 11:03:31 GMT | 2005-02-02 16:59:11 GMT | 8 | Unallocated | U |

deleted files | desktop shortcuts | email accounts | email addresses | email messages | encryption detected | encryption suspected

RegRipper was also used in order to analyse the NTUSER.DAT file from the johndoe account in order to view his settings, registry, and other relevant information stored in this file. The results also showed which files were accessed last, revealing that he did access some missing files before deleting and overwriting them. The full results are displayed in Appendix 11.

The data found demonstrates the suspect accessing sensitive content, confirmed the presence of the programs ran and installed on the machine, system rights of each user together with operating system information and the presence of external drives. The complete list of all actions with dates and timings are reported in the excel spreadsheet included.

## Other Findings

This section covers other findings relevant to the case that were retrieved during the investigation, which can be found at Appendix 13 or in the evidence folder provided. These include an audio file named aggressive_song.wav, which was found in /img_johnDoe.dd/vol_vol2/Program Files/MSN/aggressive_song.wav.

A total of four guides containing instructions on how to observe, interact or groom birds were discovered. Also, a document titled "Dear Fred.doc" was found among Bob's files, which appears to be a letter addressed to his friend Fred. While this information is not directly linked with the case, it could imply that Fred might enjoy birds as well.

Some images were hidden in files that seem to contain a different kind of content. For example, Doc1 contains a picture of an adult bird. FantailFrontView.exe was also another file that, by changing the .exe extension to .jpg, revealed another picture of a bird. One image was found inside a Music directory, suggesting that the suspect attempted to hide it there.

## Conclusion

The team was able to retrieve 49 pictures from the cameras, 1 image from Birdpics.gpg, 7 images from the emails and 57 other images. Bringing this to a total of 114 images. On top of that, several other files were extracted including 4 text files,1 audio file, over 430 web pages, 4 emails and several other files from the suspect's disk, most of which are irrefutably related to birds.

By analysing this evidence, it may be concluded that some individuals, such as Ben and Jane, may be involved in the gathering and distribution of such material. This suggest that Mr. John Doe was likely engaging into bird watching with other people, probably as part of a circle of individuals who share an infatuation for birds. The fact that he deliberately attempted to hide, encrypt or delete many of these files suggests that he was aware of the culpability of his obsessive tendencies in the face of law and the existence of such material on his computer was not just a ploy to incriminate him.

## Tools

- Autopsy 4.18.0
- ClamAV
- Fred (Forensic Registry Editor)
- RegRipper 3.0
- Zeitline
- Bash scripts
- Ubuntu Virtual Machines

# Appendices

## Appendix 1 – Complete Timeline of Events

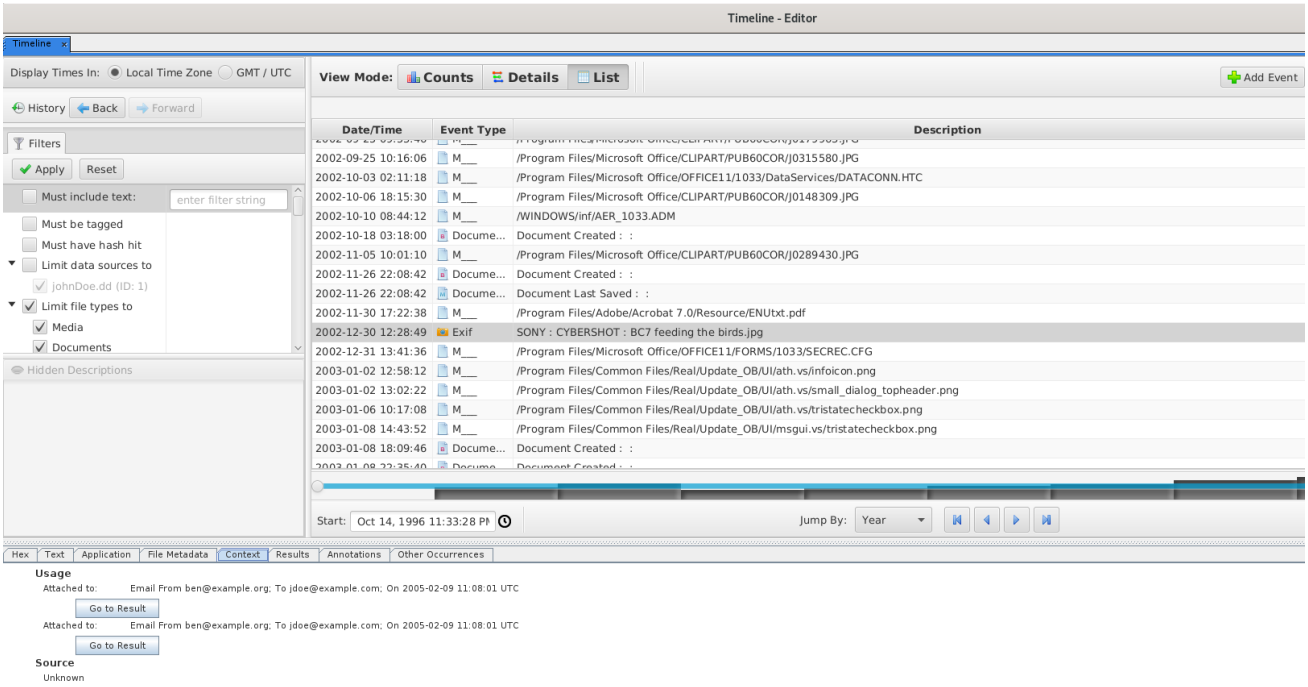



Figure 3. Ben Forbes' email image dates to 30.11.2002 at 12:28:49

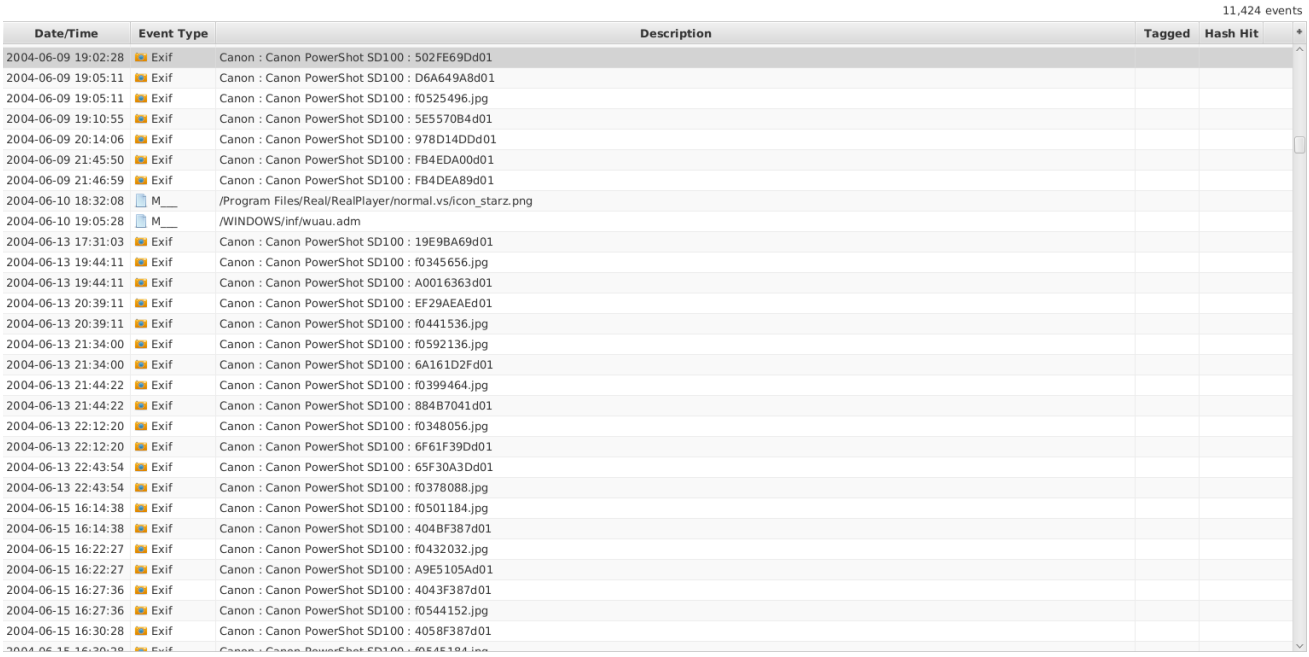



Figure 4.1. – First appearance of Canon Powershot's on John Doe's system on 09.06.2004 19:02:28

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2004-06-15 16:30:28 | Exif | Canon : Canon PowerShot SD100 : 4058F387d01 | | |
| 2004-06-15 16:30:28 | Exif | Canon : Canon PowerShot SD100 : f0545184.jpg | | |
| 2004-06-17 18:42:34 | Exif | Canon : Canon PowerShot SD100 : 3E8762AFd01 | | |
| 2004-06-17 18:42:34 | Exif | Canon : Canon PowerShot SD100 : f0440944.jpg | | |
| 2004-06-17 18:42:34 | Exif | Canon : Canon PowerShot SD100 : birdtrans2.jpg | | |
| 2004-06-17 18:43:03 | Exif | Canon : Canon PowerShot SD100 : 3E8462AFd01 | | |
| 2004-06-17 18:43:03 | Exif | Canon : Canon PowerShot SD100 : f0382464.jpg | | |
| 2004-06-17 18:46:20 | Exif | Canon : Canon PowerShot SD100 : f0533600.jpg | | |
| 2004-06-17 18:46:20 | Exif | Canon : Canon PowerShot SD100 : AA784519d01 | | |
| 2004-06-17 18:46:49 | Exif | Canon : Canon PowerShot SD100 : 8F5F3282d01 | | |
| 2004-06-17 18:48:53 | Exif | Canon : Canon PowerShot SD100 : D8829E69d01 | | |
| 2004-06-17 18:48:53 | Exif | Canon : Canon PowerShot SD100 : f0529544.jpg | | |
| 2004-06-18 23:28:19 | Exif | Canon : Canon PowerShot SD100 : BF5BE9D9d01 | | |
| 2004-06-18 23:29:36 | Exif | Canon : Canon PowerShot SD100 : BF4BE9D9d01 | | |
| 2004-06-18 23:31:50 | Exif | Canon : Canon PowerShot SD100 : 3E8662AFd01 | | |
| 2004-06-18 23:31:50 | Exif | Canon : Canon PowerShot SD100 : f0415008.jpg | | |
| 2004-06-18 23:31:56 | Exif | Canon : Canon PowerShot SD100 : 3E8162AFd01 | | |
| 2004-06-18 23:31:56 | Exif | Canon : Canon PowerShot SD100 : f0438640.jpg | | |
| 2004-06-18 23:32:28 | Exif | Canon : Canon PowerShot SD100 : f0439400.jpg | | |
| 2004-06-18 23:32:28 | Exif | Canon : Canon PowerShot SD100 : 3E8262AFd01 | | |
| 2004-06-18 23:33:33 | Exif | Canon : Canon PowerShot SD100 : f0360392.jpg | | |
| 2004-06-18 23:33:33 | Exif | Canon : Canon PowerShot SD100 : 4C3E89C6d01 | | |
| 2004-06-18 23:49:04 | Exif | Canon : Canon PowerShot SD100 : f0526960.jpg | | |
| 2004-06-18 23:49:04 | Exif | Canon : Canon PowerShot SD100 : 3E8C62AFd01 | | |
| 2004-06-19 17:24:05 | Exif | Canon : Canon PowerShot SD100 : D5FDCB9Ad01 | | |
| 2004-06-19 18:34:15 | Exif | Canon : Canon PowerShot SD100 : D19FCBF6d01 | | |
| 2004-06-19 18:34:15 | Exif | Canon : Canon PowerShot SD100 : f0526232.jpg | | |
| 2004-06-19 19:13:42 | Exif | Canon : Canon PowerShot SD100 : B76BD0AEd01 | | |
| 2004-06-19 19:13:42 | Exif | Canon : Canon PowerShot SD100 : f0464568.jpg | | |
| 2004-06-19 19:49:58 | Exif | Canon : Canon PowerShot SD100 : A2E5F216d01 | | |

Figure 4.2. – Further record of the Canon PowerShot pictures from 15 – 19.06.2004

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2004-06-19 19:49:58 | Exif | Canon : Canon PowerShot SD100 : f0443520.jpg | | |
| 2004-06-20 18:01:44 | Exif | Canon : Canon PowerShot SD100 : ready2fledge.jpg | | |
| 2004-06-20 20:25:34 | Exif | Canon : Canon PowerShot SD100 : f0438992.jpg | | |
| 2004-06-20 20:25:34 | Exif | Canon : Canon PowerShot SD100 : 426147D8d01 | | |
| 2004-06-22 18:50:52 | Exif | Canon : Canon PowerShot SD100 : f0561264.jpg | | |
| 2004-06-22 18:50:52 | Exif | Canon : Canon PowerShot SD100 : 5C1E7D60d01 | | |
| 2004-06-22 18:56:18 | Exif | Canon : Canon PowerShot SD100 : f0416072.jpg | | |
| 2004-06-22 18:56:18 | Exif | Canon : Canon PowerShot SD100 : A3D4DDDDd01 | | |
| 2004-06-22 21:10:50 | Exif | Canon : Canon PowerShot SD100 : 0E47C6DFd01 | | |
| 2004-06-22 21:10:50 | Exif | Canon : Canon PowerShot SD100 : newbies2.jpg | | |
| 2004-06-22 21:18:16 | Exif | Canon : Canon PowerShot SD100 : B9D470B5d01 | | |
| 2004-06-22 21:18:16 | Exif | Canon : Canon PowerShot SD100 : f0552688.jpg | | |
| 2004-06-22 21:23:00 | Exif | Canon : Canon PowerShot SD100 : D192AAB2d01 | | |
| 2004-06-22 21:23:00 | Exif | Canon : Canon PowerShot SD100 : f0525016.jpg | | |
| 2004-06-23 10:15:48 | M_B_ | /Program Files/Adobe/Acrobat 7.0/Reader/HowTo/ENU/Images/zoomintool.gif | | |
| 2004-06-23 17:16:02 | Exif | Canon : Canon PowerShot SD100 : E319CFC2d01 | | |
| 2004-06-23 17:16:02 | Exif | Canon : Canon PowerShot SD100 : f0522304.jpg | | |
| 2004-06-23 17:37:06 | Exif | Canon : Canon PowerShot SD100 : f0493176.jpg | | |
| 2004-06-23 17:37:06 | Exif | Canon : Canon PowerShot SD100 : 7E37FA89d01 | | |
| 2004-06-23 20:15:05 | Exif | Canon : Canon PowerShot SD100 : 848752E7d01 | | |
| 2004-06-26 23:42:59 | Exif | Canon : Canon PowerShot SD100 : 42626CDDd01 | | |
| 2004-06-26 23:42:59 | Exif | Canon : Canon PowerShot SD100 : f0457096.jpg | | |
| 2004-06-26 23:44:08 | Exif | Canon : Canon PowerShot SD100 : f0520464.jpg | | |
| 2004-06-26 23:44:08 | Exif | Canon : Canon PowerShot SD100 : 7013F58Dd01 | | |
| 2004-06-26 23:55:03 | Exif | Canon : Canon PowerShot SD100 : FA73DB84d01 | | |
| 2004-06-26 23:55:03 | Exif | Canon : Canon PowerShot SD100 : f0417336.jpg | | |
| 2004-06-27 00:16:07 | Exif | Canon : Canon PowerShot SD100 : f0415616.jpg | | |
| 2004-06-27 00:16:07 | Exif | Canon : Canon PowerShot SD100 : D1D1775Fd01 | | |
| 2004-06-27 00:58:13 | Exif | Canon : Canon PowerShot SD100 : 61C27B40d01 | | |

Figure 4.3. – Further record of the Canon PowerShot pictures from 15 – 19.06.2004

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2004-06-27 00:58:13 | Exif | Canon : Canon PowerShot SD100 : f0413632.jpg | | |
| 2004-06-27 00:58:26 | Exif | Canon : Canon PowerShot SD100 : 1CE0A8AEd01 | | |
| 2004-06-27 00:58:26 | Exif | Canon : Canon PowerShot SD100 : f0494144.jpg | | |
| 2004-06-27 00:58:39 | Exif | Canon : Canon PowerShot SD100 : f0395576.jpg | | |
| 2004-06-27 00:58:39 | Exif | Canon : Canon PowerShot SD100 : A8331696d01 | | |
| 2004-06-27 02:39:21 | Exif | Canon : Canon PowerShot SD100 : f0395928.jpg | | |
| 2004-06-27 02:39:21 | Exif | Canon : Canon PowerShot SD100 : FC6938FDd01 | | |
| 2004-06-27 02:39:44 | Exif | Canon : Canon PowerShot SD100 : 80BF7122d01 | | |
| 2004-06-27 02:39:44 | Exif | Canon : Canon PowerShot SD100 : f0508024.jpg | | |
| 2004-06-27 03:29:11 | Exif | Canon : Canon PowerShot SD100 : f0391728.jpg | | |
| 2004-06-27 03:29:11 | Exif | Canon : Canon PowerShot SD100 : 661C3843d01 | | |
| 2004-06-27 03:52:20 | Exif | Canon : Canon PowerShot SD100 : f0527448.jpg | | |
| 2004-06-27 03:52:20 | Exif | Canon : Canon PowerShot SD100 : 3FB68809d01 | | |
| 2004-06-27 18:28:34 | Exif | Canon : Canon PowerShot SD100 : 93C4F412d01 | | |
| 2004-06-27 18:28:34 | Exif | Canon : Canon PowerShot SD100 : chicks2.jpg | | |
| 2004-06-27 18:28:34 | Exif | Canon : Canon PowerShot SD100 : f0345832.jpg | | |
| 2004-06-27 18:28:34 | Exif | Canon : Canon PowerShot SD100 : f0045880.jpg | | |
| 2004-06-28 13:11:34 | M_B_ | /Program Files/Adobe/Acrobat 7.0/Reader/HowTo/ENU/Images/C_UpOneLevel_Lg_N.png | | |
| 2004-06-28 13:33:24 | M_B_ | /Program Files/Adobe/Acrobat 7.0/Reader/HowTo/ENU/Images/bkgrnd_art.gif | | |
| 2004-07-17 11:44:24 | M___ | /Program Files/Windows Media Player/Skins/Revert.wmz/pl_restoremin_btngrp_disabled.bmp | | |
| 2004-07-17 11:44:24 | M___ | /Program Files/Windows Media Player/Skins/Revert.wmz/volume_thumb_hover.bmp | | |
| 2004-07-17 11:44:24 | M___ | /Program Files/Windows Media Player/Skins/Revert.wmz/pl_tr.bmp | | |
| 2004-07-17 11:44:24 | M___ | /Program Files/Windows Media Player/Skins/Revert.wmz/pause_down.bmp | | |
| 2004-07-17 11:44:24 | M___ | /Program Files/Windows Media Player/Skins/Revert.wmz/player_up.bmp | | |
| 2004-07-17 11:44:24 | M___ | /Program Files/Windows Media Player/Skins/Revert.wmz/pause_hover.bmp | | |
| 2004-07-17 11:44:24 | M___ | /Program Files/Windows Media Player/Skins/Revert.wmz/player_down.bmp | | |
| 2004-07-17 11:44:24 | M___ | /Program Files/Windows Media Player/Skins/Revert.wmz/pl_r.bmp | | |
| 2004-07-17 11:44:24 | M___ | /Program Files/Windows Media Player/Skins/Revert.wmz/eq_vslider_thumb_disabled.bmp | | |
| 2004-07-17 11:44:24 | M___ | /Program Files/Windows Media Player/Skins/Revert.wmz/pl_bl.bmp | | |
| 2004-07-17 11:44:24 | M___ | /Program Files/Windows Media Player/Skins/Revert.wmz/player_disable.bmp | | |

Figure 4.4. – Further record of the Canon PowerShot pictures from 15 – 19.06.2004

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2005-01-24 16:23:23 | __B_ | /Program Files/Mozilla Firefox/res/table-add-column-after-active.gif | | |
| 2005-01-24 16:23:23 | MABC | /Documents and Settings/johndoe/Local Settings/Temporary Internet Files/Content.IE5/456NWTMR/thunderbird[1].htm | | |
| 2005-01-24 16:23:23 | _A__ | /Documents and Settings/johndoe/Local Settings/Temporary Internet Files/Content.IE5/CLABK1AB/template[1].css | | |
| 2005-01-24 16:23:23 | _A__ | /Documents and Settings/johndoe/Local Settings/Temporary Internet Files/Content.IE5/OH6F8TA3/content[1].css | | |
| 2005-01-24 16:23:23 | __B_ | /Program Files/Mozilla Firefox/res/html/gopher-image.gif | | |
| 2005-01-24 16:23:23 | _A__ | /Documents and Settings/johndoe/Local Settings/Temporary Internet Files/Content.IE5/4963KDYV/print[1].css | | |
| 2005-01-24 16:23:23 | _A__ | /Documents and Settings/johndoe/Local Settings/Temporary Internet Files/Content.IE5/CLABK1AB/template[2].css | | |
| 2005-01-24 16:23:24 | _A__ | /Documents and Settings/johndoe/Local Settings/Temporary Internet Files/Content.IE5/OH6F8TA3/download_back[1].gif | | |
| 2005-01-24 16:23:24 | _A__ | /Documents and Settings/johndoe/Local Settings/Temporary Internet Files/Content.IE5/456NWTMR/header_bl[1].png | | |
| 2005-01-24 16:23:24 | __B_ | /Program Files/Mozilla Firefox/res/html/gopher-menu.gif | | |
| 2005-01-24 16:23:24 | MABC | /Documents and Settings/johndoe/Local Settings/Temporary Internet Files/Content.IE5/4963KDYV/moz_shirt[1].jpg | | |
| 2005-01-24 16:23:24 | __B_ | /Documents and Settings/johndoe/Local Settings/Temporary Internet Files/Content.IE5/CLABK1AB/product-thunderbird-screen[1].png | | |
| 2005-01-24 16:23:24 | MABC | /Documents and Settings/johndoe/Local Settings/Temporary Internet Files/Content.IE5/OH6F8TA3/award_softpediapick[1].gif | | |
| 2005-01-24 16:23:24 | _A__ | /Documents and Settings/johndoe/Local Settings/Temporary Internet Files/Content.IE5/CLABK1AB/shop_back[1].gif | | |
| 2005-01-24 16:23:24 | __B_ | /Program Files/Mozilla Firefox/components/jsconsole-clhandler.js | | |
| 2005-01-24 16:23:24 | _A__ | /Documents and Settings/johndoe/Local Settings/Temporary Internet Files/Content.IE5/OH6F8TA3/header_tab[1].gif | | |
| 2005-01-24 16:23:24 | __B_ | /Program Files/Mozilla Firefox/res/builtin/platformHTMLBindings.xml | | |
| 2005-01-24 16:23:25 | __B_ | /Program Files/Mozilla Firefox/components/nsSetDefaultBrowser.js | | |
| 2005-01-24 16:23:25 | MA_C | /Documents and Settings/johndoe/Local Settings/Temporary Internet Files/Content.IE5/CLABK1AB/product-thunderbird-screen[1].png | | |
| 2005-01-24 16:23:25 | __B_ | /Program Files/Mozilla Firefox/res/table-remove-column-hover.gif | | |
| 2005-01-24 16:23:25 | __B_ | /Program Files/Mozilla Firefox/res/table-remove-column.new | | |

Figure 5. John searching for thunderbird in IE5 internet browser

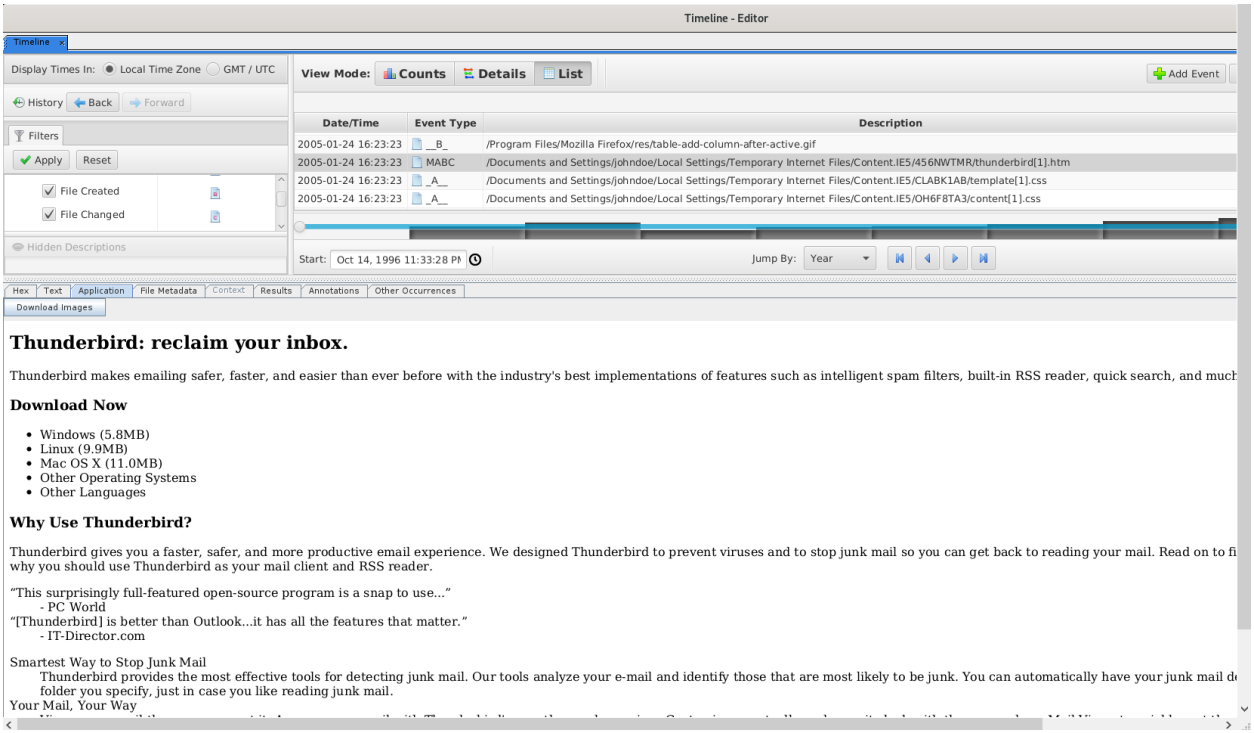



Figure 6. John visiting the thunderbird website

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2005-01-24 16:21:27 | _AB_ | /WINDOWS/$hf_mig$/KB885836/update/updatebr.inf | | |
| 2005-01-24 16:21:30 | MABC | /Documents and Settings/johndoe/Local Settings/Temporary Internet Files/Content.IE5/456NWTMR/product-camino[1].png | | |
| 2005-01-24 16:21:30 | __B_ | /Documents and Settings/johndoe/Local Settings/Temporary Internet Files/Content.IE5/4963KDYV/product-firefox[1].png | | |
| 2005-01-24 16:21:30 | MABC | /Documents and Settings/johndoe/Local Settings/Temporary Internet Files/Content.IE5/456NWTMR/product-calendar[1].png | | |
| 2005-01-24 16:21:30 | M_BC | /Documents and Settings/johndoe/Local Settings/Temporary Internet Files/Content.IE5/CLABK1AB/products[1].htm | | |
| 2005-01-24 16:21:31 | MA_C | /Documents and Settings/johndoe/Local Settings/Temporary Internet Files/Content.IE5/4963KDYV/product-firefox[1].png | | |
| 2005-01-24 16:21:31 | MABC | /Documents and Settings/johndoe/Local Settings/Temporary Internet Files/Content.IE5/OH6F8TA3/product-bugzilla[1].png | | |
| 2005-01-24 16:21:31 | MA_C | /WINDOWS/$NtUninstallKB885836$/spuninst/spuninst.inf | | |
| 2005-01-24 16:21:31 | MABC | /Documents and Settings/johndoe/Local Settings/Temporary Internet Files/Content.IE5/CLABK1AB/product-thunderbird[1].png | | |
| 2005-01-24 16:21:31 | MABC | /Documents and Settings/johndoe/Local Settings/Temporary Internet Files/Content.IE5/4963KDYV/product-mozilla[1].png | | |
| 2005-01-24 16:21:32 | MA_C | /WINDOWS/KB885836.log | | |
| 2005-01-24 16:21:36 | __B_ | /WINDOWS/Debug/mrt.log | | |
| 2005-01-24 16:21:41 | _A__ | /Documents and Settings/johndoe/Local Settings/Temporary Internet Files/Content.IE5/456NWTMR/firefox[1].htm | | |
| 2005-01-24 16:21:44 | __B_ | /Documents and Settings/johndoe/Local Settings/Temporary Internet Files/Content.IE5/CLABK1AB/Firefox%20Setup%201.0[1].exe:Zone.Identifier | | |
| 2005-01-24 16:21:52 | ___C | /System Volume Information/_restore{F551F22F-0FBF-41E1-AE7D-8B7BB8E7F937}/RP13/A0000616.inf | | |
| 2005-01-24 16:21:52 | __B_ | /WINDOWS/$NtUninstallKB890175$/spuninst/spuninst.inf | | |
| 2005-01-24 16:21:52 | MABC | /WINDOWS/$NtUninstallKB890175$/spuninst/spuninst.txt | | |
| 2005-01-24 16:21:56 | _AB_ | /WINDOWS/$hf_mig$/KB890175/update/update_SP2QFE.inf | | |
| 2005-01-24 16:21:56 | _AB_ | /WINDOWS/$hf_mig$/KB890175/update/eula.txt | | |

Figure 7. Thunderbird website, download section snippet

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2005-01-24 16:24:55 | M___ | /Documents and Settings/johndoe/Local Settings/Temporary Internet Files/Content.IE5/456NWTMR/Thunderbird%20Setup%201.0[1].exe:Zone.Identifier | | |
| 2005-01-24 16:24:55 | ___C | /Program Files/Mozilla Firefox/defaults/profile/search.rdf | | |
| 2005-01-24 16:24:55 | ___C | /Documents and Settings/johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/chrome/userChrome-example.css | | |
| 2005-01-24 16:24:55 | ___C | /Program Files/Mozilla Firefox/defaults/pref/firefox-l10n.js | | |
| 2005-01-24 16:24:55 | ___C | /Program Files/Mozilla Firefox/defaults/profile/search-2.new | | |
| 2005-01-24 16:24:55 | ___C | /Program Files/Mozilla Firefox/defaults/profile/chrome/userContent-example.css | | |
| 2005-01-24 16:24:55 | ___C | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/extensions/Extensions.rdf | | |
| 2005-01-24 16:24:56 | ___C | /Program Files/Mozilla Firefox/defaults/profile/localstore.rdf | | |
| 2005-01-24 16:24:56 | _A_C | /Documents and Settings/johndoe/Local Settings/Temporary Internet Files/Content.IE5/456NWTMR/Thunderbird%20Setup%201.0[1].exe:Zone.Identifier | | |
| 2005-01-24 16:24:57 | ___C | /Program Files/Mozilla Firefox/defaults/profile/prefs.js | | |
| 2005-01-24 16:24:57 | ___C | /Program Files/Mozilla Firefox/defaults/profile/prefs-2.new | | |
| 2005-01-24 16:24:58 | ___C | /Documents and Settings/johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/extensions/installed-extensions.txt | | |
| 2005-01-24 16:24:58 | ___C | /Documents and Settings/jane/Application Data/Mozilla/Firefox/Profiles/hcdost7f.default/extensions/installed-extensions.txt | | |
| 2005-01-24 16:24:58 | ___C | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/extensions/installed-extensions.txt | | |
| 2005-01-24 16:24:58 | ___C | /Program Files/Mozilla Firefox/defaults/profile/extensions/installed-extensions.txt | | |
| 2005-01-24 16:25:00 | ___C | /Program Files/Mozilla Firefox/searchplugins/eBay.src | | |
| 2005-01-24 16:25:07 | ___C | /Program Files/Mozilla Firefox/searchplugins/yahoo.gif | | |
| 2005-01-24 16:25:08 | ___C | /Program Files/Mozilla Firefox/searchplugins/dictionary-3.new | | |
| 2005-01-24 16:25:08 | ___C | /Program Files/Mozilla Firefox/searchplugins/dictionary.src | | |

Figure 8. John has installed thunderbird and has run the "Thunderbird Setup.exe"

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2005-02-02 14:16:36 | __B_ | /WINDOWS/Firefox Wallpaper.bmp | | |
| 2005-02-02 14:16:37 | M__C | /WINDOWS/Firefox Wallpaper.bmp | | |
| 2005-02-02 14:18:07 | MAB_ | /Documents and Settings/All Users/Documents/My Pictures/Sample Pictures/Thumbs.db | | |
| 2005-02-02 14:18:08 | ___C | /Documents and Settings/All Users/Documents/My Pictures/Sample Pictures/Thumbs.db | | |
| 2005-02-02 14:18:10 | __B_ | /Documents and Settings/johndoe/My Documents/My Pictures/tn_duck_3.jpg | | |
| 2005-02-02 14:18:11 | M___ | /Documents and Settings/johndoe/My Documents/My Pictures/tn_duck_3.jpg | | |
| 2005-02-02 14:18:12 | ___C | /Documents and Settings/johndoe/My Documents/My Pictures/tn_duck_3.jpg | | |
| 2005-02-02 14:18:50 | __B_ | /Documents and Settings/johndoe/My Documents/My Pictures/Thumbs.db | | |
| 2005-02-02 14:18:52 | __B_ | /Documents and Settings/johndoe/My Documents/My Pictures/snow_geese.jpg | | |
| 2005-02-02 14:18:53 | M__C | /Documents and Settings/johndoe/My Documents/My Pictures/snow_geese.jpg | | |
| 2005-02-02 14:20:33 | M_BC | /Documents and Settings/johndoe/My Documents/My Pictures/7107298.jpg | | |
| 2005-02-02 14:25:59 | __B_ | /Documents and Settings/johndoe/My Documents/aa010703a.htm | | |
| 2005-02-02 14:26:00 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/xml.gif | | |
| 2005-02-02 14:26:00 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/hobbies_birding_data_003/business_entrepreneurs_mostadmiredpoll1_leaderboard.jpg | | |
| 2005-02-02 14:26:00 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/vhg1.jpg | | |
| 2005-02-02 14:26:00 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/birding.gif | | |
| 2005-02-02 14:26:00 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/tfm.gif | | |
| 2005-02-02 14:26:00 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/fl00.gif | | |
| 2005-02-02 14:26:00 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/abSb.gif | | |
| 2005-02-02 14:26:00 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/bluebirdhousepic.jpg | | |
| 2005-02-02 14:26:00 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/abT.gif | | |
| 2005-02-02 14:26:00 | MABC | /Documents and Settings/johndoe/My Documents/aa010703a_files/ads | | |
| 2005-02-02 14:26:00 | MABC | /Documents and Settings/johndoe/My Documents/aa010703a_files/5_data/gs03.css | | |
| 2005-02-02 14:26:00 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/bxbr.gif | | |
| 2005-02-02 14:26:00 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/5_data/goR.gif | | |
| 2005-02-02 14:26:00 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/hobbies_birding_data/a.gif | | |
| 2005-02-02 14:26:00 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/su.gif | | |
| 2005-02-02 14:26:00 | MABC | /Documents and Settings/johndoe/My Documents/aa010703a_files/cj017x14t207.js | | |
| 2005-02-02 14:26:00 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/bxtl.gif | | |
| 2005-02-02 14:26:00 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/y1.gif | | |

Figure 9. Start of John accessing bird images

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2005-02-02 14:26:02 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/12.htm | | |
| 2005-02-02 14:26:02 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/hobbies_birding_002.htm | | |
| 2005-02-02 14:26:02 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/5.htm | | |
| 2005-02-02 14:26:02 | M__C | /Documents and Settings/johndoe/My Documents/aa010703a_files/hobbies_birding.htm | | |
| 2005-02-02 14:26:02 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/6.htm | | |
| 2005-02-02 14:26:02 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/go.htm | | |
| 2005-02-02 14:28:19 | M_BC | /Documents and Settings/johndoe/My Documents/My Pictures/wbpremium_s.jpg | | |
| 2005-02-02 14:29:30 | MABC | /Documents and Settings/johndoe/My Documents/nestboxtips.txt | | |
| 2005-02-02 14:41:32 | M_BC | /Documents and Settings/johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/hostperm.1 | | |
| 2005-02-02 14:42:31 | _A__ | /Program Files/Mozilla Firefox/res/viewsource.css | | |
| 2005-02-02 14:43:35 | __B_ | /Documents and Settings/johndoe/My Documents/My Pictures/40m.jpg | | |
| 2005-02-02 14:43:36 | M__C | /Documents and Settings/johndoe/My Documents/My Pictures/40m.jpg | | |
| 2005-02-02 14:47:04 | __B_ | /Program Files/Mozilla Firefox/install.log | | |
| 2005-02-02 14:47:14 | __B_ | /Program Files/Internet Explorer/PLUGINS/RichFX/Player/nprfxins_EULA.txt | | |
| 2005-02-02 14:49:56 | __B_ | /Program Files/Common Files/Real/Update_OB/RealPlayer-log.txt | | |
| 2005-02-02 14:49:59 | MABC | /Program Files/Common Files/Real/Update_OB/UI/msgoff.htm | | |
| 2005-02-02 14:49:59 | MABC | /Program Files/Common Files/Real/Update_OB/UI/Images/real_logo_93x44.gif | | |
| 2005-02-02 14:49:59 | MABC | /Program Files/Common Files/Real/Update_OB/UI/default.png | | |

Figure 10. More images

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2005-02-02 16:25:10 | M___ | /WINDOWS/mui/FantailFrontView.exe | | |
| 2005-02-02 16:25:10 | M___ | /AmericanAvocetWinterPlumage.jpg | | |
| 2005-02-02 16:25:10 | M___ | /BellbirdJumpingOffBranch.jpg | | |
| 2005-02-02 16:25:10 | M___ | /KeaAndMountain.jpg | | |
| 2005-02-02 16:25:10 | M___ | /brd_Ornithologist_TWG.jpg | | |
| 2005-02-02 16:25:10 | M___ | /WINDOWS/CrouchingKokako.dll/CanadaGooseWashing.jpg | | |
| 2005-02-02 16:25:10 | M___ | /AmericanWhitePelicansCircling.jpg | | |
| 2005-02-02 16:25:10 | M___ | /Program Files/frankbeecostume_1827_34457581 | | |
| 2005-02-02 16:25:10 | M___ | /Program Files/frankbeecostume_1827_96360352 | | |
| 2005-02-02 16:25:10 | M___ | /WINDOWS/CrouchingKokako.dll/ChestnutMandibledToucan.jpg | | |
| 2005-02-02 16:25:10 | M___ | /WINDOWS/CrouchingKokako.dll/BrushTurkeyPerching.jpg | | |
| 2005-02-02 16:25:10 | M___ | /KeaAtTopOfMacKinnonPass0930.jpg | | |
| 2005-02-02 16:25:10 | M___ | /WINDOWS/CrouchingKokako.dll/brd_WoodDuck.jpg | | |
| 2005-02-02 16:25:10 | M___ | /Program Files/frankbeecostume_1827_84985892 | | |
| 2005-02-02 16:25:10 | M___ | /BlackNeckedStiltsFromBehind.jpg | | |
| 2005-02-02 16:25:10 | M___ | /birdwatching.doc | | |
| 2005-02-02 16:25:10 | M___ | /KeaRetrievingBakedBeanCanFromTarn.jpg | | |
| 2005-02-02 16:25:10 | M___ | /GreatEgretOverflyingRoseateSpoonbills.jpg | | |
| 2005-02-02 16:25:10 | M___ | /GreatBlueHeronWithFish.jpg | | |
| 2005-02-02 16:25:10 | M___ | /KeaEatingRentalCar.jpg | | |
| 2005-02-02 16:25:10 | M___ | /AlmondMarshGreatBlueHeronStalling.jpg | | |
| 2005-02-02 16:25:10 | M___ | /BlackSwan.jpg | | |
| 2005-02-02 16:25:10 | M___ | /WINDOWS/CrouchingKokako.dll/Brolga.jpg | | |
| 2005-02-02 16:25:10 | M___ | /guide.doc | | |
| 2005-02-02 16:25:10 | M___ | /BarnOwl.jpg | | |
| 2005-02-02 16:25:10 | M___ | /junescreen01.jpg | | |
| 2005-02-02 16:25:10 | M___ | /RECYCLER/S-1-5-21-725345543-854245398-1202660629-1003/Df1.jpg | | |
| 2005-02-02 16:25:10 | M___ | /june03screen.jpg | | |
| 2005-02-02 16:25:10 | M___ | /GreenHeronOnChicagoLakeshore.jpg | | |
| 2005-02-02 16:25:10 | M___ | /WINDOWS/CrouchingKokako.dll/CanadaGoose.jpg | | |

Figure 11. FantailFrontView.exe among bird images

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2005-02-02 16:25:10 | M___ | /RECYCLER/S-1-5-21-725345543-854245398-1202660629-1003/Df1.jpg | | |
| 2005-02-02 16:25:10 | M___ | /june03screen.jpg | | |
| 2005-02-02 16:25:10 | M___ | /GreenHeronOnChicagoLakeshore.jpg | | |
| 2005-02-02 16:25:10 | M___ | /WINDOWS/CrouchingKokako.dll/CanadaGoose.jpg | | |
| 2005-02-02 16:25:10 | M___ | /BaldEagle7oClock.jpg | | |
| 2005-02-02 16:25:10 | M___ | /blue_bird2.jpg | | |
| 2005-02-02 16:25:10 | M___ | /BlackVultureSunningOnPost.jpg | | |
| 2005-02-02 16:25:10 | M___ | /ImmatureSnowyEgretTakingOff.jpg | | |
| 2005-02-02 16:25:10 | M___ | /GreenHeronCloseup.jpg | | |
| 2005-02-02 16:25:10 | M___ | /GreatEgretInVoloBog.jpg | | |
| 2005-02-02 16:25:10 | M___ | /WINDOWS/CrouchingKokako.dll/CrouchingKokako.jpg | | |
| 2005-02-02 16:29:57 | _A__ | /WINDOWS/inf/syssetup.inf | | |
| 2005-02-02 16:31:58 | _A_C | /Program Files/Windows Privacy Tools/Readme.txt | | |
| 2005-02-02 16:32:03 | ___C | /Program Files/Windows Privacy Tools/GnuPG/CVS/Root | | |
| 2005-02-02 16:32:03 | ___C | /Program Files/Windows Privacy Tools/GnuPG/CVS/Entries | | |
| 2005-02-02 16:32:03 | ___C | /Program Files/Windows Privacy Tools/GnuPG/CVS/Repository | | |

Figure 12. More images

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2005-02-03 15:04:12 | MA__ | /$OrphanFiles/D6A649A8d01 | | |
| 2005-02-03 15:04:12 | MAB_ | /$OrphanFiles/426147D8d01 | | |
| 2005-02-03 15:04:48 | _A__ | /$OrphanFiles/3E8762AFd01 | | |
| 2005-02-03 15:04:48 | MABC | /Documents and Settings/johndoe/Desktop/birdtrans2.jpg | | |
| 2005-02-03 15:05:01 | _A__ | /Documents and Settings/johndoe/My Documents/My Pictures/177.jpg | | |
| 2005-02-03 15:05:03 | _A__ | /$OrphanFiles/93C4F412d01 | | |
| 2005-02-03 15:05:03 | M_BC | /Documents and Settings/johndoe/My Documents/My Pictures/chicks2.jpg | | |
| 2005-02-03 15:05:38 | MA_C | /Documents and Settings/johndoe/My Documents/My Pictures/Thumbs.db | | |
| 2005-02-03 15:05:38 | _A__ | /Documents and Settings/johndoe/My Documents/My Pictures/chicks2.jpg | | |
| 2005-02-03 15:05:44 | M_BC | /Documents and Settings/johndoe/My Documents/newbies2.jpg | | |
| 2005-02-03 15:05:44 | _A__ | /$OrphanFiles/0E47C6DFd01 | | |
| 2005-02-03 15:06:42 | MABC | /Documents and Settings/bob/My Documents/My Music/ready2fledge.jpg | | |
| 2005-02-03 15:42:16 | _ABC | /Program Files/frankbeecostume_1827_34457581 | | |
| 2005-02-03 15:42:16 | _ABC | /Program Files/frankbeecostume_1827_96360352 | | |
| 2005-02-03 15:42:16 | _ABC | /Program Files/frankbeecostume_1827_84985892 | | |
| 2005-02-03 15:43:48 | ___C | /blue_bird2.jpg | | |
| 2005-02-03 15:43:48 | ___C | /RECYCLER/S-1-5-21-725345543-854245398-1202660629-1003/Df1.jpg | | |

Figure 13. End of John accessing large volume of bird images

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2005-01-24 16:27:05 | __B_ | /Documents and Settings/johndoe/Application Data/Mozilla/Firefox/pluginreg.dat | | |
| 2005-01-24 16:27:11 | _ABC | /Program Files/Mozilla Firefox/extensions/installed-extensions-processed.txt | | |
| 2005-01-24 16:27:11 | _AB_ | /Program Files/Mozilla Firefox/extensions/{972ce4c6-7e08-4474-a285-3208198ce6fd}/install.rdf | | |
| 2005-01-24 16:27:11 | M_BC | /Program Files/Mozilla Firefox/extensions/Extensions.rdf | | |
| 2005-01-24 16:27:13 | M__C | /Documents and Settings/johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/compreg.dat | | |
| 2005-01-24 16:27:15 | M__C | /Documents and Settings/johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/search.rdf | | |
| 2005-01-24 16:28:20 | __B_ | /Documents and Settings/johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/history.dat | | |

Figure 14. John's history.dat

| | | |
|---|---|---|
| 2005-01-24 16:28:25 | __B_ | /Documents and Settings/johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/cookies.txt |
| 2005-01-24 16:28:55 | __B_ | /Documents and Settings/johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/downloads.rdf |
| 2005-01-24 16:30:03 | __B_ | /Program Files/Mozilla Thunderbird/install_status.log |
| 2005-01-24 16:30:03 | __B_ | /Program Files/Mozilla Thunderbird/install_wizard.log |
| 2005-01-24 16:30:13 | __B_ | /Program Files/Mozilla Thunderbird/res/builtin/platformHTMLBindings.xml |
| 2005-01-24 16:30:13 | __B_ | /Program Files/Mozilla Thunderbird/res/table-add-column-after-active.gif |
| 2005-01-24 16:30:13 | __B_ | /Program Files/Mozilla Thunderbird/res/forms.css |
| 2005-01-24 16:30:13 | __B_ | /Program Files/Mozilla Thunderbird/components/jsconsole-clhandler.js |
| 2005-01-24 16:30:13 | __B_ | /Program Files/Mozilla Thunderbird/res/langGroups-1.new |
| 2005-01-24 16:30:13 | __B_ | /Program Files/Mozilla Thunderbird/res/forms-1.new |
| 2005-01-24 16:30:20 | __B_ | /Program Files/Mozilla Thunderbird/defaults/pref/composer.js |

Figure 15. John's downloads.rdf

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2005-02-02 14:20:33 | M_BC | /Documents and Settings/johndoe/My Documents/My Pictures/7107298.jpg | | |
| 2005-02-02 14:25:59 | __B_ | /Documents and Settings/johndoe/My Documents/aa010703a.htm | | |
| 2005-02-02 14:26:00 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/xml.gif | | |
| 2005-02-02 14:26:00 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/hobbies_birding_data_003/business_entrepreneurs_mostadmiredpoll1_leaderboard.jpg | | |
| 2005-02-02 14:26:00 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/vhg1.jpg | | |
| 2005-02-02 14:26:00 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/birding.gif | | |
| 2005-02-02 14:26:00 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/tfm.gif | | |
| 2005-02-02 14:26:00 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/fl00.gif | | |
| 2005-02-02 14:26:00 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/abSb.gif | | |
| 2005-02-02 14:26:00 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/bluebirdhousepic.jpg | | |
| 2005-02-02 14:26:00 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/abT.gif | | |
| 2005-02-02 14:26:00 | MABC | /Documents and Settings/johndoe/My Documents/aa010703a_files/ads | | |
| 2005-02-02 14:26:00 | MABC | /Documents and Settings/johndoe/My Documents/aa010703a_files/5_data/gs03.css | | |
| 2005-02-02 14:26:00 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/bxbr.gif | | |
| 2005-02-02 14:26:00 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/5_data/goR.gif | | |
| 2005-02-02 14:26:00 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/hobbies_birding_data/a.gif | | |

Figure 16. Advertisements

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2005-02-02 14:26:01 | __B_ | /Documents and Settings/johndoe/My Documents/aa010703a_files/hobbies_birding.htm | | |
| 2005-02-02 14:26:01 | M__C | /Documents and Settings/johndoe/My Documents/aa010703a.htm | | |
| 2005-02-02 14:26:01 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/5_data/B1342877.gif | | |
| 2005-02-02 14:26:01 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/5_data/lg2.gif | | |
| 2005-02-02 14:26:02 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/c.htm | | |
| 2005-02-02 14:26:02 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/b.htm | | |
| 2005-02-02 14:26:02 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/0.htm | | |
| 2005-02-02 14:26:02 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/hobbies_birding_003.htm | | |
| 2005-02-02 14:26:02 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/cw.htm | | |
| 2005-02-02 14:26:02 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/am.htm | | |
| 2005-02-02 14:26:02 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/12.htm | | |
| 2005-02-02 14:26:02 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/hobbies_birding_002.htm | | |
| 2005-02-02 14:26:02 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/5.htm | | |
| 2005-02-02 14:26:02 | M__C | /Documents and Settings/johndoe/My Documents/aa010703a_files/hobbies_birding.htm | | |
| 2005-02-02 14:26:02 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/6.htm | | |
| 2005-02-02 14:26:02 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/go.htm | | |
| 2005-02-02 14:28:19 | M_BC | /Documents and Settings/johndoe/My Documents/My Pictures/wbpremium_s.jpg | | |
| 2005-02-02 14:29:30 | MABC | /Documents and Settings/johndoe/My Documents/nestboxtips.txt | | |

Figure 17. Visiting bird hobby website

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2005-02-02 16:13:20 | _A__ | /Documents and Settings/johndoe/My Documents/aa010703a_files/su.gif | | |
| 2005-02-02 16:13:20 | _A__ | /Documents and Settings/johndoe/My Documents/aa010703a_files/y1.gif | | |
| 2005-02-02 16:13:20 | _A__ | /Documents and Settings/johndoe/My Documents/aa010703a_files/tfp.gif | | |
| 2005-02-02 16:13:20 | _A__ | /Documents and Settings/johndoe/My Documents/aa010703a_files/su_002.gif | | |
| 2005-02-02 16:13:20 | _A__ | /Documents and Settings/johndoe/My Documents/aa010703a_files/tfm.gif | | |
| 2005-02-02 16:13:20 | _A__ | /Documents and Settings/johndoe/My Documents/aa010703a_files/vhg1.jpg | | |
| 2005-02-02 16:13:20 | _A__ | /Documents and Settings/johndoe/My Documents/aa010703a_files/te.gif | | |
| 2005-02-02 16:13:22 | _A__ | /Documents and Settings/johndoe/My Documents/aa010703a_files/bxbr.gif | | |
| 2005-02-02 16:13:22 | _A__ | /Documents and Settings/johndoe/My Documents/aa010703a_files/bg.gif | | |
| 2005-02-02 16:13:22 | _A__ | /Documents and Settings/johndoe/My Documents/aa010703a_files/am.htm | | |
| 2005-02-02 16:13:22 | _A__ | /Documents and Settings/johndoe/My Documents/aa010703a_files/b.htm | | |
| 2005-02-02 16:13:22 | _A__ | /Documents and Settings/johndoe/My Documents/aa010703a_files/bxtl.gif | | |
| 2005-02-02 16:13:22 | _A__ | /Documents and Settings/johndoe/My Documents/aa010703a_files/abT.gif | | |
| 2005-02-02 16:13:23 | _A__ | /Documents and Settings/johndoe/My Documents/aa010703a_files/bluebirdhousepic.jpg | | |
| 2005-02-02 16:13:23 | _A__ | /Documents and Settings/johndoe/My Documents/aa010703a_files/birding_002.gif | | |
| 2005-02-02 16:13:23 | _A__ | /Documents and Settings/johndoe/My Documents/aa010703a_files/birding.gif | | |
| 2005-02-02 16:13:23 | _A__ | /Documents and Settings/johndoe/My Documents/aa010703a_files/c.htm | | |
| 2005-02-02 16:13:23 | _A__ | /Documents and Settings/johndoe/My Documents/aa010703a_files/bxbm.gif | | |

Figure 18. b.htm date

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2005-02-02 16:25:10 | M___ | /BellbirdJumpingOffBranch.jpg | | |
| 2005-02-02 16:25:10 | M___ | /KeaAndMountain.jpg | | |
| 2005-02-02 16:25:10 | M___ | /brd_Ornithologist_TWG.jpg | | |
| 2005-02-02 16:25:10 | M___ | /WINDOWS/CrouchingKokako.dll/CanadaGooseWashing.jpg | | |
| 2005-02-02 16:25:10 | M___ | /AmericanWhitePelicansCircling.jpg | | |
| 2005-02-02 16:25:10 | M___ | /Program Files/frankbeecostume_1827_34457581 | | |
| 2005-02-02 16:25:10 | M___ | /Program Files/frankbeecostume_1827_96360352 | | |
| 2005-02-02 16:25:10 | M___ | /WINDOWS/CrouchingKokako.dll/ChestnutMandibledToucan.jpg | | |
| 2005-02-02 16:25:10 | M___ | /WINDOWS/CrouchingKokako.dll/BrushTurkeyPerching.jpg | | |
| 2005-02-02 16:25:10 | M___ | /KeaAtTopOfMacKinnonPass0930.jpg | | |
| 2005-02-02 16:25:10 | M___ | /WINDOWS/CrouchingKokako.dll/brd_WoodDuck.jpg | | |
| 2005-02-02 16:25:10 | M___ | /Program Files/frankbeecostume_1827_84985892 | | |
| 2005-02-02 16:25:10 | M___ | /BlackNeckedStiltsFromBehind.jpg | | |
| 2005-02-02 16:25:10 | M___ | /birdwatching.doc | | |
| 2005-02-02 16:25:10 | M___ | /KeaRetrievingBakedBeanCanFromTarn.jpg | | |
| 2005-02-02 16:25:10 | M___ | /GreatEgretOverflyingRoseateSpoonbills.jpg | | |
| 2005-02-02 16:25:10 | M___ | /GreatBlueHeronWithFish.jpg | | |
| 2005-02-02 16:25:10 | M___ | /KeaEatingRentalCar.jpg | | |
| 2005-02-02 16:25:10 | M___ | /AlmondMarshGreatBlueHeronStalling.jpg | | |
| 2005-02-02 16:25:10 | M___ | /BlackSwan.jpg | | |

Figure 19. birdwatching.doc creation date on John's system

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2005-02-02 16:25:10 | M___ | /KeaAtTopOfMacKinnonPass0930.jpg | | |
| 2005-02-02 16:25:10 | M___ | /WINDOWS/CrouchingKokako.dll/brd_WoodDuck.jpg | | |
| 2005-02-02 16:25:10 | M___ | /Program Files/frankbeecostume_1827_84985892 | | |
| 2005-02-02 16:25:10 | M___ | /BlackNeckedStiltsFromBehind.jpg | | |
| 2005-02-02 16:25:10 | M___ | /birdwatching.doc | | |
| 2005-02-02 16:25:10 | M___ | /KeaRetrievingBakedBeanCanFromTarn.jpg | | |
| 2005-02-02 16:25:10 | M___ | /GreatEgretOverflyingRoseateSpoonbills.jpg | | |
| 2005-02-02 16:25:10 | M___ | /GreatBlueHeronWithFish.jpg | | |
| 2005-02-02 16:25:10 | M___ | /KeaEatingRentalCar.jpg | | |
| 2005-02-02 16:25:10 | M___ | /AlmondMarshGreatBlueHeronStalling.jpg | | |
| 2005-02-02 16:25:10 | M___ | /BlackSwan.jpg | | |
| 2005-02-02 16:25:10 | M___ | /WINDOWS/CrouchingKokako.dll/Brolga.jpg | | |
| 2005-02-02 16:25:10 | M___ | /guide.doc | | |
| 2005-02-02 16:25:10 | M___ | /BarnOwl.jpg | | |
| 2005-02-02 16:25:10 | M___ | /junescreen01.jpg | | |
| 2005-02-02 16:25:10 | M___ | /RECYCLER/S-1-5-21-725345543-854245398-1202660629-1003/Df1.jpg | | |
| 2005-02-02 16:25:10 | M___ | /june03screen.jpg | | |
| 2005-02-02 16:25:10 | M___ | /GreenHeronOnChicagoLakeshore.jpg | | |
| 2005-02-02 16:25:10 | M___ | /WINDOWS/CrouchingKokako.dll/CanadaGoose.jpg | | |

Figure 20. guide.doc creation date on John's system

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2005-02-02 14:26:02 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/cw.htm | | |
| 2005-02-02 14:26:02 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/am.htm | | |
| 2005-02-02 14:26:02 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/12.htm | | |
| 2005-02-02 14:26:02 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/hobbies_birding_002.htm | | |
| 2005-02-02 14:26:02 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/5.htm | | |
| 2005-02-02 14:26:02 | M__C | /Documents and Settings/johndoe/My Documents/aa010703a_files/hobbies_birding.htm | | |
| 2005-02-02 14:26:02 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/6.htm | | |
| 2005-02-02 14:26:02 | M_BC | /Documents and Settings/johndoe/My Documents/aa010703a_files/go.htm | | |
| 2005-02-02 14:28:19 | M_BC | /Documents and Settings/johndoe/My Documents/My Pictures/wbpremium_s.jpg | | |
| 2005-02-02 14:29:30 | MABC | /Documents and Settings/johndoe/My Documents/nestboxtips.txt | | |
| 2005-02-02 14:41:32 | M_BC | /Documents and Settings/johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/hostperm.1 | | |
| 2005-02-02 14:42:31 | _A__ | /Program Files/Mozilla Firefox/res/viewsource.css | | |
| 2005-02-02 14:43:35 | __B_ | /Documents and Settings/johndoe/My Documents/My Pictures/40m.jpg | | |
| 2005-02-02 14:43:36 | M__C | /Documents and Settings/johndoe/My Documents/My Pictures/40m.jpg | | |
| 2005-02-02 14:47:04 | __B_ | /Program Files/Mozilla Firefox/install.log | | |
| 2005-02-02 14:47:14 | __B_ | /Program Files/Internet Explorer/PLUGINS/RichFX/Player/nprfxins_EULA.txt | | |
| 2005-02-02 14:49:56 | __B_ | /Program Files/Common Files/Real/Update_OB/RealPlayer-log.txt | | |
| 2005-02-02 14:49:59 | MABC | /Program Files/Common Files/Real/Update_OB/UI/msgoff.htm | | |

Figure 21. nestboxtips.txt creation date on John's system

| Date/Time | Event Type | Description |
|---|---|---|
| 2005-02-03 15:52:01 | Recent ... | E:\birds\non images\BirdingGuide.pdf |
| 2005-02-03 15:52:01 | Web His... | file/birds/non%20images/BirdingGuide.pdf |
| 2005-02-03 15:52:01 | MABC | /Documents and Settings/johndoe/Recent/BirdingGuide.pdf.lnk |

Figure 22. Birdingguide.pdf date

| Date/Time | Event Type | Description |
|---|---|---|
| 2005-02-03 15:02:45 | Web His... | file/Documents%20and%20Settings/johndoe/My%20Documents/ostbk2b2.htm |
| 2005-02-03 15:02:45 | M_BC | /Documents and Settings/johndoe/My Documents/ostbk2b2.htm |
| 2005-02-03 15:02:45 | Recent ... | C:\Documents and Settings\johndoe\My Documents\ostbk2b2.htm |
| 2005-02-03 15:02:45 | MABC | /Documents and Settings/johndoe/Recent/ostbk2b2.htm.lnk |
| 2005-02-09 11:28:01 | Web His... | file/Documents%20and%20Settings/johndoe/My%20Documents/ostbk2b2.htm |
| 2005-02-09 11:28:01 | Web His... | file/Documents%20and%20Settings/johndoe/My%20Documents/ostbk2b2.htm |
| 2005-02-09 11:28:21 | _A__ | /Documents and Settings/johndoe/My Documents/ostbk2b2.htm |

Figure 23. ostbk2b2.htm date

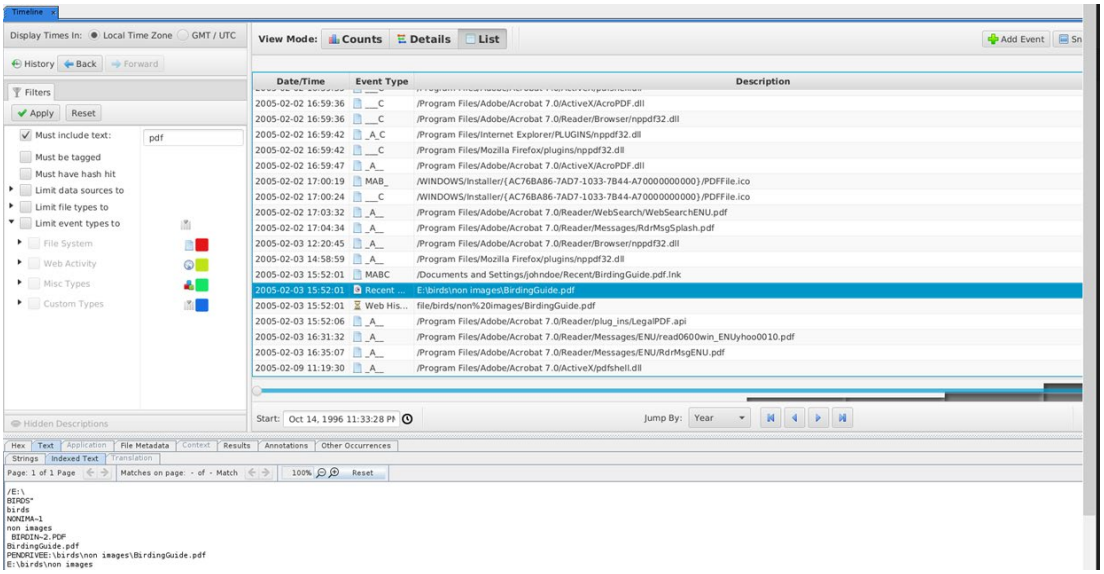



Figure 24. Clearly a USB drive E

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2005-02-03 13:21:05 | _A__ | /Program Files/Mozilla Firefox/extensions/Extensions.rdf | | |
| 2005-02-03 14:16:00 | Docume... | Document Created : : | | |
| 2005-02-03 14:16:22 | ___C | /Program Files/MSN/MSNCoreFiles/Install/msnms.ico | | |
| 2005-02-03 14:17:00 | Docume... | Document Last Saved : : | | |
| 2005-02-03 14:17:42 | __B_ | /Documents and Settings/johndoe/My Documents/My Music/Doc1.doc | | |
| 2005-02-03 14:17:43 | M___ | /Documents and Settings/johndoe/My Documents/My Music/Doc1.doc | | |
| 2005-02-03 14:18:43 | _A__ | /Documents and Settings/All Users/Documents/My Music/Sample Music/New Stories (Highway Blues).wma | | |
| 2005-02-03 14:18:43 | _A__ | /Documents and Settings/All Users/Documents/My Music/Sample Music/Beethoven's Symphony No. 9 (Scherzo).wma | | |
| 2005-02-03 14:18:54 | ___C | /Documents and Settings/johndoe/My Documents/My Music/Doc1.doc | | |
| 2005-02-03 14:19:12 | _A__ | /Documents and Settings/johndoe/My Documents/My Music/Doc1.doc | | |
| 2005-02-03 14:37:47 | M___ | /Documents and Settings/johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/prefs.js.moztmp | | |
| 2005-02-03 14:40:13 | _A__ | /WINDOWS/Media/Windows XP Exclamation.wav | | |
| 2005-02-03 14:40:40 | __B_ | /WINDOWS/mui/FantailFrontView.exe | | |
| 2005-02-03 14:41:57 | _A__ | /Documents and Settings/johndoe/Favorites/Radio Station Guide.url | | |
| 2005-02-03 14:41:57 | _A__ | /Documents and Settings/johndoe/Favorites/MSN.com.url | | |
| 2005-02-03 14:42:52 | ___C | /WINDOWS/mui/FantailFrontView.exe | | |
| 2005-02-03 14:43:34 | _A__ | /WINDOWS/Media/Windows XP Recycle.wav | | |
| 2005-02-03 14:45:17 | _A__ | /WINDOWS/mui/FantailFrontView.exe | | |
| 2005-02-03 14:58:59 | M__C | /Documents and Settings/johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/xpti.dat | | |
| 2005-02-03 14:59:00 | M__C | /Documents and Settings/johndoe/Application Data/Mozilla/Firefox/pluginreg.dat | | |

Figure 25. Doc1 created 2005-2-03 21:05

```
5-02-02 15:04:43.0 MA. Visited: johndoe@res://C:\Program%20Files\Real\RealPlayer\rpplugins\rpmn3260.dll/black.html
5-02-02 15:04:47.0 MA. Visited: johndoe@file:///C:/Program%20Files/Real/RealPlayer/Firstrun/1.htm
5-02-02 15:04:48.0 MA. Visited: johndoe@file:///C:/Program%20Files/Real/RealPlayer/Firstrun/context.htm
5-02-02 15:10:16.0 MA. Visited: johndoe@file:///D:/Prac4/Prac4.gif
5-02-02 15:10:48.0 MA. Visited: johndoe@file:///D:/Prac5/Q3%20Thread%20(Statechart).gif
5-02-02 15:11:51.0 MA. Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/kakapo.ram
5-02-02 17:03:40.0 MA. Visited: johndoe@file:///C:/Program%20Files/Adobe/Acrobat%207.0/Reader/Legal/Adobe%20Reader/7.0.0/en_US/license.html
5-03-02 11:50:10.0 .A. http://www-config.strath.ac.uk/proxy.config
5-03-02 12:19:07.0 MA. Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/Application%20Data/Mozilla/Firefox/Profiles/w4nf3obl.default/cookies.txt
5-03-02 12:20:20.0 MA. Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/Application%20Data/Mozilla/Firefox/Profiles/w4nf3obl.default/bookmarks.html
5-03-02 12:22:51.0 MA. Visited: johndoe@file:///E:/birds/audio/aggressive_song.wav
5-03-02 14:14:59.0 MA. Visited: johndoe@file:///C:/EvanstonWoodpecker.jpg
5-03-02 14:17:48.0 MA. Visited: johndoe@file:///C:/Documents%20and%20Settings/All%20Users/Documents/My%20Music/Sample%20Music/Doc1.doc
```

Figure 26. aggressive_song.wav on USB drive E as noted previously. Contains birds chirping

| Date/Time | Event Type | Description |
|---|---|---|
| 2005-02-03 12:22:51 | __B_ | /Documents and Settings/johndoe/Recent/aggressive_song.wav.lnk |
| 2005-02-03 12:22:51 | Web His... | file/birds/audio/aggressive_song.wav |
| 2005-02-03 12:22:51 | Recent ... | C:\Program Files\MSN\aggressive_song.wav |
| 2005-02-03 12:23:00 | M___ | /Program Files/MSN/aggressive_song.wav |
| 2005-02-09 11:28:01 | Web His... | file/birds/audio/aggressive_song.wav |
| 2005-02-09 11:28:01 | Web His... | file/birds/audio/aggressive_song.wav |
| 2005-02-09 17:00:20 | __B_ | /Program Files/MSN/aggressive_song.wav |
| 2005-02-09 17:00:21 | _A__ | /Program Files/MSN/aggressive_song.wav |
| 2005-02-09 17:00:50 | ___C | /Program Files/MSN/aggressive_song.wav |
| 2005-02-09 17:00:50 | MA_C | /Documents and Settings/johndoe/Recent/aggressive_song.wav.lnk |
| 2005-02-09 17:01:19 | MABC | /Documents and Settings/johndoe/Application Data/Real/RealPlayer/History/aggressive_song.lnk |

Figure 27. All aggressive songs dates on John's system

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2005-02-03 11:24:09 | MA_C | /Documents and Settings/jane/Application Data/Mozilla/Firefox/Profiles/hcdost7f.default/search.rdf | | |
| 2005-02-03 11:24:36 | __B_ | /Documents and Settings/jane/Application Data/Mozilla/Firefox/Profiles/hcdost7f.default/history.dat | | |
| 2005-02-03 11:24:36 | MABC | /Documents and Settings/jane/Application Data/Mozilla/Firefox/Profiles/hcdost7f.default/Cache/2FB68356d01 | | |
| 2005-02-03 11:24:44 | __B_ | /Documents and Settings/jane/Application Data/Mozilla/Firefox/Profiles/hcdost7f.default/formhistory.dat | | |
| 2005-02-03 11:24:51 | MABC | /Documents and Settings/jane/Application Data/Mozilla/Firefox/Profiles/hcdost7f.default/cookies.txt | | |
| 2005-02-03 11:25:10 | __B_ | /Documents and Settings/jane/Application Data/Mozilla/Firefox/Profiles/hcdost7f.default/Cache/86A6C463d01 | | |
| 2005-02-03 11:25:11 | MA_C | /Documents and Settings/jane/Application Data/Mozilla/Firefox/Profiles/hcdost7f.default/Cache/86A6C463d01 | | |
| 2005-02-03 11:26:29 | __B_ | /Documents and Settings/jane/Application Data/Mozilla/Firefox/Profiles/hcdost7f.default/Cache/55072A23d01 | | |
| 2005-02-03 11:26:30 | MA_C | /Documents and Settings/jane/Application Data/Mozilla/Firefox/Profiles/hcdost7f.default/Cache/55072A23d01 | | |
| 2005-02-03 11:26:37 | MABC | /Documents and Settings/jane/Application Data/Mozilla/Firefox/Profiles/hcdost7f.default/Cache/55042A23d01 | | |
| 2005-02-03 11:26:39 | MABC | /Documents and Settings/jane/Application Data/Mozilla/Firefox/Profiles/hcdost7f.default/Cache/55022A23d01 | | |
| 2005-02-03 11:26:43 | MABC | /Documents and Settings/jane/Application Data/Mozilla/Firefox/Profiles/hcdost7f.default/Cache/55052A23d01 | | |
| 2005-02-03 11:26:47 | MABC | /Documents and Settings/jane/Application Data/Mozilla/Firefox/Profiles/hcdost7f.default/Cache/55032A23d01 | | |
| 2005-02-03 11:26:49 | MABC | /Documents and Settings/jane/Application Data/Mozilla/Firefox/Profiles/hcdost7f.default/Cache/55002A23d01 | | |
| 2005-02-03 11:26:51 | MABC | /Documents and Settings/jane/Application Data/Mozilla/Firefox/Profiles/hcdost7f.default/Cache/550E2A23d01 | | |
| 2005-02-03 11:26:58 | MABC | /Documents and Settings/jane/Application Data/Mozilla/Firefox/Profiles/hcdost7f.default/Cache/55012A23d01 | | |

Figure 28. Jane's cache images. Maybe Jane herself

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2005-02-03 11:26:47 | MABC | /Documents and Settings/jane/Application Data/Mozilla/Firefox/Profiles/hcdost7f.default/Cache/55032A23d01 | | |
| 2005-02-03 11:26:49 | MABC | /Documents and Settings/jane/Application Data/Mozilla/Firefox/Profiles/hcdost7f.default/Cache/55002A23d01 | | |
| 2005-02-03 11:26:51 | MABC | /Documents and Settings/jane/Application Data/Mozilla/Firefox/Profiles/hcdost7f.default/Cache/550E2A23d01 | | |
| 2005-02-03 11:26:58 | MABC | /Documents and Settings/jane/Application Data/Mozilla/Firefox/Profiles/hcdost7f.default/Cache/55012A23d01 | | |
| 2005-02-03 11:27:09 | M___ | /Documents and Settings/jane/Application Data/Mozilla/Firefox/Profiles/hcdost7f.default/bookmarks.bak | | |
| 2005-02-03 11:27:10 | MA_C | /Documents and Settings/jane/Application Data/Mozilla/Firefox/Profiles/hcdost7f.default/history.dat | | |
| 2005-02-03 11:27:10 | MA_C | /Documents and Settings/jane/Application Data/Mozilla/Firefox/Profiles/hcdost7f.default/localstore.rdf | | |
| 2005-02-03 11:27:10 | _ABC | /Documents and Settings/jane/Application Data/Mozilla/Firefox/Profiles/hcdost7f.default/bookmarks.bak | | |
| 2005-02-03 11:27:10 | MA_C | /Documents and Settings/jane/Application Data/Mozilla/Firefox/Profiles/hcdost7f.default/prefs.js | | |
| 2005-02-03 11:27:10 | MA_C | /Documents and Settings/jane/Application Data/Mozilla/Firefox/Profiles/hcdost7f.default/formhistory.dat | | |
| 2005-02-03 11:27:10 | MA_C | /Documents and Settings/jane/Application Data/Mozilla/Firefox/Profiles/hcdost7f.default/bookmarks.html | | |

Figure 29. Jane's history.dat date

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2005-02-03 10:22:08 | M_BC | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/Cache/B92526AFd01 | | |
| 2005-02-03 10:22:09 | MABC | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/Cache/1777BFA0d01 | | |
| 2005-02-03 10:22:28 | M_BC | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/Cache/CFF688E3d01 | | |
| 2005-02-03 10:23:38 | MABC | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/Cache/78E1DD2Ed01 | | |
| 2005-02-03 10:25:04 | _A__ | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/Cache/CFF688E3d01 | | |
| 2005-02-03 10:25:06 | _A__ | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/Cache/B92526AFd01 | | |
| 2005-02-03 10:26:08 | MA_C | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/Cache/D392FC32d01 | | |
| 2005-02-03 10:26:16 | MABC | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/Cache/BC8EF547d01 | | |
| 2005-02-03 10:26:31 | MABC | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/Cache/D5F652F7d01 | | |
| 2005-02-03 10:26:37 | MA_C | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/cookies.txt | | |
| 2005-02-03 10:26:58 | MA_C | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/prefs.js | | |
| 2005-02-03 10:26:58 | MA_C | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/bookmarks.html | | |
| 2005-02-03 10:26:58 | MABC | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/bookmarks.bak | | |
| 2005-02-03 10:26:58 | MA_C | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/localstore.rdf | | |
| 2005-02-03 10:26:58 | MA_C | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/history.dat | | |
| 2005-02-03 10:26:59 | MA_C | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/formhistory.dat | | |

Figure 30. Bob's history.dat date

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2005-02-03 10:22:09 | MABC | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/Cache/1777BFA0d01 | | |
| 2005-02-03 10:22:28 | M_BC | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/Cache/CFF688E3d01 | | |
| 2005-02-03 10:23:38 | MABC | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/Cache/78E1DD2Ed01 | | |
| 2005-02-03 10:25:04 | _A__ | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/Cache/CFF688E3d01 | | |
| 2005-02-03 10:25:06 | _A__ | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/Cache/B92526AFd01 | | |
| 2005-02-03 10:26:08 | MA_C | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/Cache/D392FC32d01 | | |
| 2005-02-03 10:26:16 | MABC | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/Cache/BC8EF547d01 | | |
| 2005-02-03 10:26:31 | MABC | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/Cache/D5F652F7d01 | | |
| 2005-02-03 10:26:37 | MA_C | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/cookies.txt | | |
| 2005-02-03 10:26:58 | MA_C | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/prefs.js | | |
| 2005-02-03 10:26:58 | MA_C | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/bookmarks.html | | |
| 2005-02-03 10:26:58 | MABC | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/bookmarks.bak | | |
| 2005-02-03 10:26:58 | MA_C | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/localstore.rdf | | |
| 2005-02-03 10:26:58 | MA_C | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/history.dat | | |
| 2005-02-03 10:26:59 | MA_C | /Documents and Settings/bob/Application Data/Mozilla/Firefox/Profiles/ktrx3s9f.default/formhistory.dat | | |
| 2005-02-03 10:27:00 | Docume... | Document Created : : | | |
| 2005-02-03 10:27:51 | MA_C | /WINDOWS/Installer/{90110409-6000-11D3-8CFE-0150048383C9}/graph.ico | | |
| 2005-02-03 10:27:51 | _A__ | /System Volume Information/_restore{F551F22F-0FBF-41E1-AE7D-8B7BB8E7F937}/Fifoed/A0000563.rbf | | |
| 2005-02-03 10:27:51 | _A__ | /System Volume Information/_restore{F551F22F-0FBF-41E1-AE7D-8B7BB8E7F937}/Fifoed/A0000564.rbf | | |
| 2005-02-03 10:27:55 | ___C | /System Volume Information/_restore{F551F22F-0FBF-41E1-AE7D-8B7BB8E7F937}/Fifoed/A0000563.rbf | | |

Figure 31. Bob creating document for Fred ( titled "Dear Fred")

| | | | | |
|---|---|---|---|---|
| 2005-02-03 10:27:00 | Docume... | Document Created : : | | |
| 2005-02-03 10:27:51 | MA_C | /WINDOWS/Installer/{90110409-6000-11D3-8CFE-0150048383C9}/graph.ico | | |
| 2005-02-03 10:27:51 | _A__ | /System Volume Information/_restore{F551F22F-0FBF-41E1-AE7D-8B7BB8E7F937}/Fifoed/A0000563.rbf | | |
| 2005-02-03 10:27:51 | _A__ | /System Volume Information/_restore{F551F22F-0FBF-41E1-AE7D-8B7BB8E7F937}/Fifoed/A0000564.rbf | | |
| 2005-02-03 10:27:55 | ___C | /System Volume Information/_restore{F551F22F-0FBF-41E1-AE7D-8B7BB8E7F937}/Fifoed/A0000563.rbf | | |
| 2005-02-03 10:27:55 | ___C | /System Volume Information/_restore{F551F22F-0FBF-41E1-AE7D-8B7BB8E7F937}/Fifoed/A0000564.rbf | | |
| 2005-02-03 10:28:17 | MABC | /Documents and Settings/bob/Application Data/Microsoft/Proof/CUSTOM.DIC | | |
| 2005-02-03 10:30:00 | Docume... | Document Last Saved : : | | |
| 2005-02-03 10:30:24 | __B_ | /Documents and Settings/bob/My Documents/Dear Fred.doc | | |
| 2005-02-03 10:30:25 | MA_C | /Documents and Settings/bob/My Documents/Dear Fred.doc | | |
| 2005-02-03 10:30:25 | __B_ | /Documents and Settings/bob/Application Data/Microsoft/Office/Recent/index.dat | | |
| 2005-02-03 10:30:27 | _AB_ | /Documents and Settings/bob/Application Data/Microsoft/Templates/Normal.dot | | |

Figure 32. Bob's custom Microsoft dictionary

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2005-02-03 15:04:12 | MA__ | /$OrphanFiles/D6A649A8d01 | | |
| 2005-02-03 15:04:12 | MAB_ | /$OrphanFiles/426147D8d01 | | |
| 2005-02-03 15:04:48 | _A__ | /$OrphanFiles/3E8762AFd01 | | |
| 2005-02-03 15:04:48 | MABC | /Documents and Settings/johndoe/Desktop/birdtrans2.jpg | | |
| 2005-02-03 15:05:01 | _A__ | /Documents and Settings/johndoe/My Documents/My Pictures/177.jpg | | |
| 2005-02-03 15:05:03 | _A__ | /$OrphanFiles/93C4F412d01 | | |
| 2005-02-03 15:05:03 | M_BC | /Documents and Settings/johndoe/My Documents/My Pictures/chicks2.jpg | | |
| 2005-02-03 15:05:38 | MA_C | /Documents and Settings/johndoe/My Documents/My Pictures/Thumbs.db | | |
| 2005-02-03 15:05:38 | _A__ | /Documents and Settings/johndoe/My Documents/My Pictures/chicks2.jpg | | |
| 2005-02-03 15:05:44 | M_BC | /Documents and Settings/johndoe/My Documents/newbies2.jpg | | |
| 2005-02-03 15:05:44 | _A__ | /$OrphanFiles/0E47C6DFd01 | | |
| 2005-02-03 15:06:42 | MABC | /Documents and Settings/bob/My Documents/My Music/ready2fledge.jpg | | |
| 2005-02-03 15:42:16 | _ABC | /Program Files/frankbeecostume_1827_34457581 | | |
| 2005-02-03 15:42:16 | _ABC | /Program Files/frankbeecostume_1827_96360352 | | |
| 2005-02-03 15:42:16 | _ABC | /Program Files/frankbeecostume_1827_84985892 | | |
| 2005-02-03 15:43:48 | ___C | /blue_bird2.jpg | | |
| 2005-02-03 15:43:48 | ___C | /RECYCLER/S-1-5-21-725345543-854245398-1202660629-1003/Df1.jpg | | |
| 2005-02-03 15:44:05 | _ABC | /guide.doc | | |
| 2005-02-03 15:49:19 | __B_ | /birdwatching.doc | | |
| 2005-02-03 15:49:26 | ___C | /birdwatching.doc | | |
| 2005-02-03 15:49:27 | _A__ | /birdwatching.doc | | |
| 2005-02-03 15:52:13 | _A__ | /Program Files/Adobe/Acrobat 7.0/Reader/Javascripts/WebSearch.js | | |
| 2005-02-03 15:52:39 | _A__ | /Program Files/Adobe/Acrobat 7.0/Reader/Updater/bootstrap.js | | |
| 2005-02-03 16:15:11 | _A__ | /WINDOWS/system32/compmgmt.msc | | |

Figure 33. Bob having bird image ready2fledge.jpg on his account and accessing

| | | |
|---|---|---|
| 2005-02-09 11:08:01 | Email | ben@example.org; to jdoe@example.com; : some more good ones : Thanks for the pics you sent me here are some I really like |
| 2005-02-09 11:08:01 | Email | ben@example.org; to jdoe@example.com; : expensive birds : A young woman was ... o for sale. The price was $6000. She entered the store and asked the |
| 2005-02-09 11:08:01 | Email | ben@example.org; to jdoe@example.com; : good pics : Hi thought you'd like these<br><br>enjoy |
| 2005-02-09 11:08:01 | Email | ben@example.org; to jdoe@example.com; : good pics : Hi thought you'd like these<br><br>enjoy |

Figure 34. Email conversations with John and Ben.

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2005-02-03 14:16:22 | ___C | /Program Files/MSN/MSNCoreFiles/Install/msnms.ico | | |
| 2005-02-03 14:17:00 | Docume... | Document Last Saved : : | | |
| 2005-02-03 14:17:42 | __B_ | /Documents and Settings/johndoe/My Documents/My Music/Doc1.doc | | |
| 2005-02-03 14:17:43 | M___ | /Documents and Settings/johndoe/My Documents/My Music/Doc1.doc | | |
| 2005-02-03 14:18:43 | _A__ | /Documents and Settings/All Users/Documents/My Music/Sample Music/New Stories (Highway Blues).wma | | |
| 2005-02-03 14:18:43 | _A__ | /Documents and Settings/All Users/Documents/My Music/Sample Music/Beethoven's Symphony No. 9 (Scherzo).wma | | |
| 2005-02-03 14:18:54 | ___C | /Documents and Settings/johndoe/My Documents/My Music/Doc1.doc | | |
| 2005-02-03 14:19:12 | _A__ | /Documents and Settings/johndoe/My Documents/My Music/Doc1.doc | | |
| 2005-02-03 14:37:47 | M___ | /Documents and Settings/johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/prefs.js.moztmp | | |
| 2005-02-03 14:40:13 | _A__ | /WINDOWS/Media/Windows XP Exclamation.wav | | |
| 2005-02-03 14:40:40 | __B_ | /WINDOWS/mui/FantailFrontView.exe | | |
| 2005-02-03 14:41:57 | _A__ | /Documents and Settings/johndoe/Favorites/Radio Station Guide.url | | |
| 2005-02-03 14:41:57 | _A__ | /Documents and Settings/johndoe/Favorites/MSN.com.url | | |
| 2005-02-03 14:42:52 | ___C | /WINDOWS/mui/FantailFrontView.exe | | |
| 2005-02-03 14:43:34 | _A__ | /WINDOWS/Media/Windows XP Recycle.wav | | |
| 2005-02-03 14:45:17 | _A__ | /WINDOWS/mui/FantailFrontView.exe | | |
| 2005-02-03 14:58:59 | M__C | /Documents and Settings/johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/xpti.dat | | |
| 2005-02-03 14:59:00 | M__C | /Documents and Settings/johndoe/Application Data/Mozilla/Firefox/pluginreg.dat | | |
| 2005-02-03 15:00:00 | M_B_ | /$OrphanFiles/1238C212d01 | | |
| 2005-02-03 15:00:00 | M_B_ | /$OrphanFiles/E1663DDEd01 | | |
| 2005-02-03 15:00:17 | _A__ | /Documents and Settings/johndoe/My Documents/My Pictures/40m.jpg | | |
| 2005-02-03 15:00:18 | _A__ | /Documents and Settings/johndoe/My Documents/My Pictures/wbpremium_s.jpg | | |
| 2005-02-03 15:00:19 | _A__ | /$OrphanFiles/E1663DDEd01 | | |
| 2005-02-03 15:00:19 | M_BC | /Documents and Settings/johndoe/My Documents/My Pictures/babyscot_vyoung.jpg | | |

Figure 35. John begins deleting images as indicated by $OrphanFiles

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2005-02-03 16:35:07 | _A__ | /Program Files/Adobe/Acrobat 7.0/Reader/Messages/ENU/RdrMsgENU.pdf | | |
| 2005-02-03 16:35:08 | MA_C | /Documents and Settings/johndoe/Application Data/Adobe/Acrobat/7.0/Collab/RSS | | |
| 2005-02-03 17:43:28 | MABC | /System Volume Information/_restore{F551F22F-0FBF-41E1-AE7D-8B7BB8E7F937}/RP7/snapshot/domain.txt | | |
| 2005-02-03 17:43:28 | MABC | /System Volume Information/_restore{F551F22F-0FBF-41E1-AE7D-8B7BB8E7F937}/Fifoed/drivetable.txt | | |
| 2005-02-04 12:44:05 | M_BC | /WINDOWS/pchealth/helpctr/DataColl/CollectedData_57.xml | | |
| 2005-02-04 18:43:28 | MABC | /System Volume Information/_restore{F551F22F-0FBF-41E1-AE7D-8B7BB8E7F937}/RP8/snapshot/domain.txt | | |
| 2005-02-04 18:43:29 | MABC | /System Volume Information/_restore{F551F22F-0FBF-41E1-AE7D-8B7BB8E7F937}/RP7/drivetable.txt | | |
| 2005-02-05 12:47:53 | M_BC | /WINDOWS/pchealth/helpctr/DataColl/CollectedData_87.xml | | |
| 2005-02-05 19:43:29 | MABC | /System Volume Information/_restore{F551F22F-0FBF-41E1-AE7D-8B7BB8E7F937}/RP9/snapshot/domain.txt | | |
| 2005-02-05 19:43:29 | MABC | /System Volume Information/_restore{F551F22F-0FBF-41E1-AE7D-8B7BB8E7F937}/RP8/drivetable.txt | | |
| 2005-02-06 12:51:38 | M_BC | /WINDOWS/pchealth/helpctr/DataColl/CollectedData_117.xml | | |
| 2005-02-06 20:43:27 | MABC | /System Volume Information/_restore{F551F22F-0FBF-41E1-AE7D-8B7BB8E7F937}/RP9/drivetable.txt | | |
| 2005-02-06 20:43:27 | MABC | /System Volume Information/_restore{F551F22F-0FBF-41E1-AE7D-8B7BB8E7F937}/RP10/snapshot/domain.txt | | |
| 2005-02-07 12:55:24 | M_BC | /WINDOWS/pchealth/helpctr/DataColl/CollectedData_147.xml | | |
| 2005-02-07 21:43:27 | MABC | /System Volume Information/_restore{F551F22F-0FBF-41E1-AE7D-8B7BB8E7F937}/RP11/snapshot/domain.txt | | |
| 2005-02-07 21:43:27 | MABC | /System Volume Information/_restore{F551F22F-0FBF-41E1-AE7D-8B7BB8E7F937}/RP10/drivetable.txt | | |
| 2005-02-08 12:59:07 | M_B_ | /WINDOWS/pchealth/helpctr/DataColl/CollectedData_166.xml | | |
| 2005-02-08 12:59:08 | M_BC | /WINDOWS/pchealth/helpctr/DataColl/CollectedData_177.xml | | |
| 2005-02-08 22:43:28 | _A__ | /WINDOWS/system32/Restore/filelist.xml | | |
| 2005-02-08 22:43:28 | MABC | /System Volume Information/_restore{F551F22F-0FBF-41E1-AE7D-8B7BB8E7F937}/RP11/drivetable.txt | | |
| 2005-02-08 22:43:28 | MABC | /System Volume Information/_restore{F551F22F-0FBF-41E1-AE7D-8B7BB8E7F937}/RP12/snapshot/domain.txt | | |
| 2005-02-08 22:43:29 | ___C | /WINDOWS/system32/Restore/filelist.xml | | |
| 2005-02-09 02:04:50 | _A_C | /WINDOWS/SoftwareDistribution/SelfUpdate/wuident.txt | | |
| 2005-02-09 02:04:51 | _A_C | /WINDOWS/SoftwareDistribution/SelfUpdate/wusetup.inf | | |

Figure 36. John possibly transferring data over to a USB or activating system restore as shown by multiple system volume changes

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2005-02-09 03:00:32 | _AB_ | /WINDOWS/$hf_mig$/KB888302/update/branches.inf | | |
| 2005-02-09 03:00:32 | _AB_ | /WINDOWS/$hf_mig$/KB888302/update/updatebr.inf | | |
| 2005-02-09 03:00:32 | _AB_ | /WINDOWS/$hf_mig$/KB888302/update/update.ver | | |
| 2005-02-09 03:00:32 | _AB_ | /WINDOWS/$hf_mig$/KB888302/update/eula.txt | | |
| 2005-02-09 03:00:32 | _AB_ | /WINDOWS/$hf_mig$/KB888302/update/update_SP2QFE.inf | | |
| 2005-02-09 03:00:42 | MA_C | /WINDOWS/$NtUninstallKB888302$/spuninst/spuninst.inf | | |
| 2005-02-09 03:00:42 | MA_C | /WINDOWS/KB888302.log | | |
| 2005-02-09 03:00:43 | _A__ | /WINDOWS/SoftwareDistribution/Download/e85f60fa51e40d03873c40d08cf4725c/_file_to_execute_.txt | | |
| 2005-02-09 03:00:50 | _A__ | /WINDOWS/SoftwareDistribution/Download/e85f60fa51e40d03873c40d08cf4725c/update/branches.inf | | |
| 2005-02-09 03:00:55 | MABC | /WINDOWS/$NtUninstallKB890047$/spuninst/spuninst.txt | | |
| 2005-02-09 03:00:55 | __B_ | /WINDOWS/$NtUninstallKB890047$/spuninst/spuninst.inf | | |
| 2005-02-09 03:00:57 | _AB_ | /WINDOWS/$hf_mig$/KB890047/update/eula.txt | | |
| 2005-02-09 03:00:57 | _AB_ | /WINDOWS/$hf_mig$/KB890047/update/update_SP2QFE.inf | | |
| 2005-02-09 03:00:57 | _AB_ | /WINDOWS/$hf_mig$/KB890047/update/update.ver | | |
| 2005-02-09 03:00:57 | _AB_ | /WINDOWS/$hf_mig$/KB890047/update/updatebr.inf | | |
| 2005-02-09 03:00:57 | _AB_ | /WINDOWS/$hf_mig$/KB890047/update/branches.inf | | |
| 2005-02-09 03:01:18 | MA_C | /WINDOWS/$NtUninstallKB890047$/spuninst/spuninst.inf | | |
| 2005-02-09 03:01:18 | MA_C | /WINDOWS/KB890047.log | | |
| 2005-02-09 03:01:19 | _A__ | /WINDOWS/SoftwareDistribution/Download/191c899196624d7a81a735dad2332655/_file_to_execute_.txt | | |
| 2005-02-09 03:01:24 | _A__ | /WINDOWS/SoftwareDistribution/Download/191c899196624d7a81a735dad2332655/update/branches.inf | | |
| 2005-02-09 03:01:25 | __B_ | /WINDOWS/$NtUninstallKB873333$/spuninst/spuninst.inf | | |
| 2005-02-09 03:01:25 | MABC | /WINDOWS/$NtUninstallKB873333$/spuninst/spuninst.txt | | |
| 2005-02-09 03:01:27 | _AB_ | /WINDOWS/$hf_mig$/KB873333/update/update_SP2QFE.inf | | |
| 2005-02-09 03:01:28 | _AB_ | /WINDOWS/$hf_mig$/KB873333/update/branches.inf | | |

Figure 37. A lot of updates running on John's system

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2005-02-09 11:07:49 | __B_ | /Documents and Settings/johndoe/Application Data/Thunderbird/Profiles/8jiqrt8v.default/Mail/Local Folders/Templates.msf | | |
| 2005-02-09 11:07:49 | __B_ | /Documents and Settings/johndoe/Application Data/Thunderbird/Profiles/8jiqrt8v.default/Mail/Local Folders/Drafts.msf | | |
| 2005-02-09 11:07:49 | __B_ | /Documents and Settings/johndoe/Application Data/Thunderbird/Profiles/8jiqrt8v.default/Mail/mail.example.com/Junk.msf | | |
| 2005-02-09 11:07:49 | __B_ | /Documents and Settings/johndoe/Application Data/Thunderbird/Profiles/8jiqrt8v.default/Mail/mail.example.com/Trash.msf | | |
| 2005-02-09 11:07:50 | __B_ | /Documents and Settings/johndoe/Application Data/Thunderbird/Profiles/8jiqrt8v.default/Mail/Local Folders/Inbox.msf | | |
| 2005-02-09 11:08:07 | MABC | /Documents and Settings/johndoe/Application Data/Thunderbird/Profiles/8jiqrt8v.default/Mail/mail.example.com/msgFilterRules.dat | | |
| 2005-02-09 11:08:08 | __B_ | /Documents and Settings/johndoe/Application Data/Thunderbird/Profiles/8jiqrt8v.default/Mail/mail.example.com/popstate.dat | | |
| 2005-02-09 11:08:08 | _A__ | /WINDOWS/Media/Windows XP Notify.wav | | |
| 2005-02-09 11:08:09 | MA_C | /Documents and Settings/johndoe/Application Data/Thunderbird/Profiles/8jiqrt8v.default/Mail/mail.example.com/popstate.dat | | |
| 2005-02-09 11:09:54 | _A__ | /Documents and Settings/johndoe/Application Data/Thunderbird/Profiles/8jiqrt8v.default/mimeTypes.rdf | | |
| 2005-02-09 11:11:06 | _A__ | /Program Files/Mozilla Thunderbird/components/newsblog.js | | |
| 2005-02-09 11:11:06 | _A__ | /Program Files/Mozilla Thunderbird/components/smime-service.js | | |
| 2005-02-09 11:11:06 | _A__ | /Program Files/Mozilla Thunderbird/components/mdn-service.js | | |
| 2005-02-09 11:11:13 | MA_C | /Documents and Settings/johndoe/Application Data/Thunderbird/Profiles/8jiqrt8v.default/localstore.rdf | | |
| 2005-02-09 11:11:21 | MA_C | /Documents and Settings/johndoe/Application Data/Thunderbird/Profiles/8jiqrt8v.default/prefs.js | | |
| 2005-02-09 11:11:31 | MA_C | /Documents and Settings/johndoe/Application Data/Thunderbird/Profiles/8jiqrt8v.default/Mail/mail.example.com/Inbox.msf | | |
| 2005-02-09 11:11:31 | MA_C | /Documents and Settings/johndoe/Application Data/Thunderbird/Profiles/8jiqrt8v.default/Mail/Local Folders/Templates.msf | | |
| 2005-02-09 11:11:31 | MA_C | /Documents and Settings/johndoe/Application Data/Thunderbird/Profiles/8jiqrt8v.default/Mail/mail.example.com/Trash.msf | | |
| 2005-02-09 11:11:31 | MA_C | /Documents and Settings/johndoe/Application Data/Thunderbird/Profiles/8jiqrt8v.default/Mail/mail.example.com/Junk.msf | | |
| 2005-02-09 11:11:31 | _A__ | /Program Files/Mozilla Thunderbird/components/nsCloseAllWindows.js | | |
| 2005-02-09 11:11:31 | _A__ | /Program Files/Mozilla Thunderbird/components/nsCloseAllWindows-1.new | | |
| 2005-02-09 11:11:31 | MA_C | /Documents and Settings/johndoe/Application Data/Thunderbird/Profiles/8jiqrt8v.default/Mail/Local Folders/Junk.msf | | |
| 2005-02-09 11:11:31 | _A__ | /Documents and Settings/johndoe/Application Data/Thunderbird/Profiles/8jiqrt8v.default/abook.mab | | |
| 2005-02-09 11:11:31 | MA_C | /Documents and Settings/johndoe/Application Data/Thunderbird/Profiles/8jiqrt8v.default/panacea.dat | | |

Figure 38. John starting process of uninstalling thunderbird email application

11,424 events

| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2005-02-09 11:26:37 | ___C | /$OrphanFiles/B76BD0AEd01 | | |
| 2005-02-09 11:26:37 | ___C | /$OrphanFiles/D6A649A8d01 | | |
| 2005-02-09 11:26:38 | ___C | /$OrphanFiles/FA73DB84d01 | | |
| 2005-02-09 11:26:38 | _A__ | /Program Files/Mozilla Firefox/res/html.css | | |
| 2005-02-09 11:26:38 | ___C | /$OrphanFiles/E319CFC2d01 | | |
| 2005-02-09 11:26:38 | ___C | /$OrphanFiles/FC6938FDd01 | | |
| 2005-02-09 11:26:38 | ___C | /$OrphanFiles/FB4EDA00d01 | | |
| 2005-02-09 11:26:38 | ___C | /$OrphanFiles/FB4DEA89d01 | | |
| 2005-02-09 11:26:38 | ___C | /$OrphanFiles/EF29AEAEd01 | | |
| 2005-02-09 11:26:43 | _A__ | /Program Files/Mozilla Firefox/res/ua.css | | |
| 2005-02-09 11:26:43 | _A__ | /Program Files/Mozilla Firefox/res/quirk.css | | |
| 2005-02-09 11:26:45 | _A__ | /Program Files/Mozilla Firefox/res/platform-forms.css | | |
| 2005-02-09 11:26:45 | _A__ | /Program Files/Mozilla Firefox/res/forms.css | | |
| 2005-02-09 11:26:48 | _A__ | /Program Files/Mozilla Firefox/chrome/overlayinfo/browser/content/overlays.rdf | | |
| 2005-02-09 11:26:49 | _A__ | /Program Files/Mozilla Firefox/searchplugins/eBay.src | | |
| 2005-02-09 11:26:49 | _A__ | /Program Files/Mozilla Firefox/searchplugins/dictionary.src | | |
| 2005-02-09 11:26:49 | _A__ | /Program Files/Mozilla Firefox/searchplugins/yahoo.src | | |
| 2005-02-09 11:26:49 | _A__ | /Documents and Settings/johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/search.rdf | | |
| 2005-02-09 11:26:49 | _A__ | /Program Files/Mozilla Firefox/searchplugins/google-uk.src | | |
| 2005-02-09 11:26:49 | _A__ | /Program Files/Mozilla Firefox/searchplugins/amazondotcom-uk.src | | |
| 2005-02-09 11:26:49 | _A__ | /Program Files/Mozilla Firefox/searchplugins/dictionary-3.new | | |
| 2005-02-09 11:26:49 | _A__ | /Program Files/Mozilla Firefox/res/builtin/platformHTMLBindings.xml | | |
| 2005-02-09 11:26:50 | _A__ | /Program Files/Mozilla Firefox/searchplugins/google-uk.gif | | |
| 2005-02-09 11:26:50 | _A__ | /Program Files/Mozilla Firefox/components/nsUpdateService.js | | |

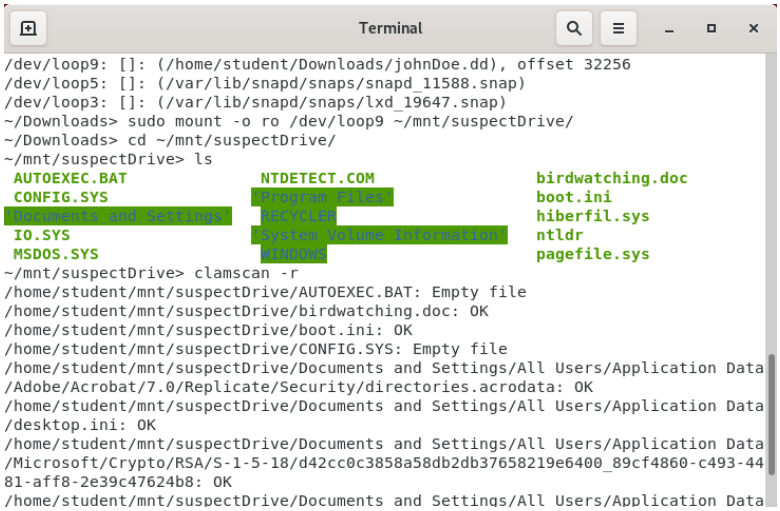
Figure 39. End of Deleting images 2005-02-09

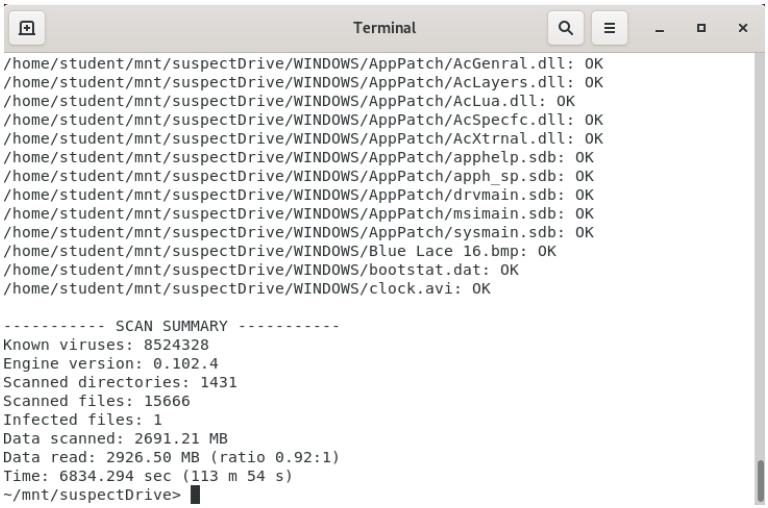
11,424 events

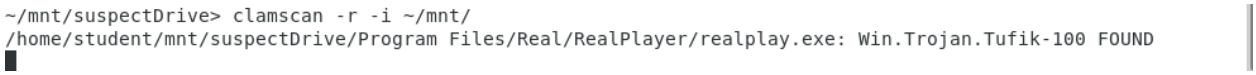
| Date/Time | Event Type | Description | Tagged | Hash Hit |
|---|---|---|---|---|
| 2005-02-09 17:09:16 | MA_C | /Documents and Settings/johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/localstore.rdf | | |
| 2005-02-09 17:09:18 | _A__ | /Documents and Settings/johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/bookmarks.bak | | |
| 2005-02-09 17:09:18 | MA_C | /Documents and Settings/johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/history.dat | | |
| 2005-02-09 17:09:18 | MA_C | /Documents and Settings/johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/bookmarks.html | | |
| 2005-02-09 17:09:19 | MA_C | /Documents and Settings/johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/prefs.js | | |
| 2005-02-09 17:09:19 | __C | /Documents and Settings/johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/prefs.js.moztmp | | |
| 2005-02-09 17:09:21 | MA_C | /Documents and Settings/johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/formhistory.dat | | |
| 2005-02-09 17:09:28 | _A__ | /WINDOWS/Media/Windows XP Shutdown.wav | | |
| 2005-02-09 17:09:33 | _A__ | /WINDOWS/WinSxS/Policies/x86_policy.5.2.Microsoft.Windows.Networking.Rtcdll_6595b64144ccf1df_x-ww_c7b7206f/5.2.2.3.Policy | | |
| 2005-02-09 17:09:33 | _A__ | /WINDOWS/WinSxS/Policies/x86_policy.5.2.Microsoft.Windows.Networking.Dxmrtp_6595b64144ccf1df_x-ww_362e60dd/5.2.2.3.Policy | | |
| 2005-02-09 17:09:33 | _A__ | /WINDOWS/WinSxS/Policies/x86_policy.1.0.Microsoft.Windows.GdiPlus_6595b64144ccf1df_x-ww_4e8510ac/1.0.2600.2180.Policy | | |
| 2005-02-09 17:09:34 | _A__ | /WINDOWS/WinSxS/Manifests/x86_Microsoft.Windows.Networking.RtcRes_6595b64144ccf1df_5.2.2.3_en_16a24bc0.Manifest | | |
| 2005-02-09 17:09:34 | _A__ | /WINDOWS/WinSxS/Manifests/x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.2180_x-ww_522f9f82.Manifest | | |
| 2005-02-09 17:09:34 | _A__ | /WINDOWS/WinSxS/Manifests/x86_Microsoft.Windows.SystemCompatible_6595b64144ccf1df_5.1.2600.2000_x-ww_bcc9a281.Manifest | | |
| 2005-02-09 17:09:34 | _A__ | /WINDOWS/WinSxS/Manifests/x86_Microsoft.Windows.Networking.Dxmrtp_6595b64144ccf1df_5.2.2.3_x-ww_468466a7.Manifest | | |
| 2005-02-09 17:09:34 | _A__ | /WINDOWS/WinSxS/Manifests/x86_Microsoft.Windows.Networking.RtcDll_6595b64144ccf1df_5.2.2.3_x-ww_d6bd8b95.Manifest | | |
| 2005-02-09 17:09:39 | MA_C | /Documents and Settings/All Users/Application Data/Network Associates/VirusScan/OnAccessScanLog.txt | | |
| 2005-02-09 17:09:41 | MA_C | /Documents and Settings/All Users/Application Data/Network Associates/Common Framework/Db/Agent_JOHN.log | | |
| 2005-02-09 17:09:45 | MA_C | /System Volume Information/_restore{F551F22F-0FBF-41E1-AE7D-8B7BB8E7F937}/drivetable.txt | | |
| 2005-02-09 17:09:46 | MA_C | /WINDOWS/system32/wbem/Logs/wbemess.log | | |
| 2005-02-09 17:09:46 | MA_C | /WINDOWS/SchedLgU.Txt | | |
| 2005-02-09 17:09:49 | MA_C | /WINDOWS/WindowsUpdate.log | | |
| 2005-02-09 17:09:54 | MA_C | /Documents and Settings/All Users/Application Data/Network Associates/VirusScan/BufferOverflowProtectionLog.txt | | |
| 2005-02-09 17:09:54 | MA_C | /Documents and Settings/All Users/Application Data/Network Associates/VirusScan/AccessProtectionLog.txt | | |

Figure 40. Finally, john shuts down his Windows XP machine and no other records after this. Possibly the last time john used his system before seizure

## Appendix 2. Virus scan results

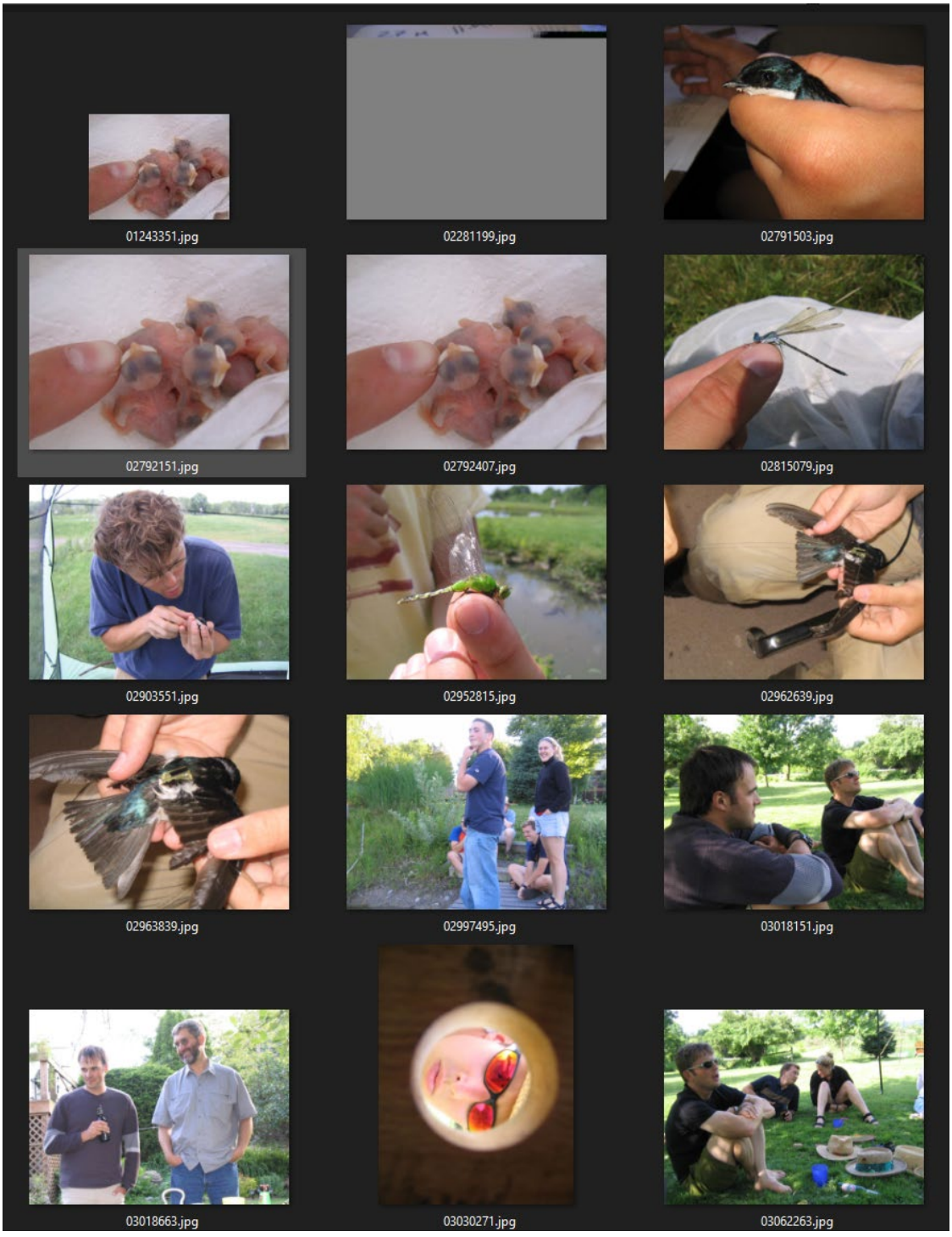


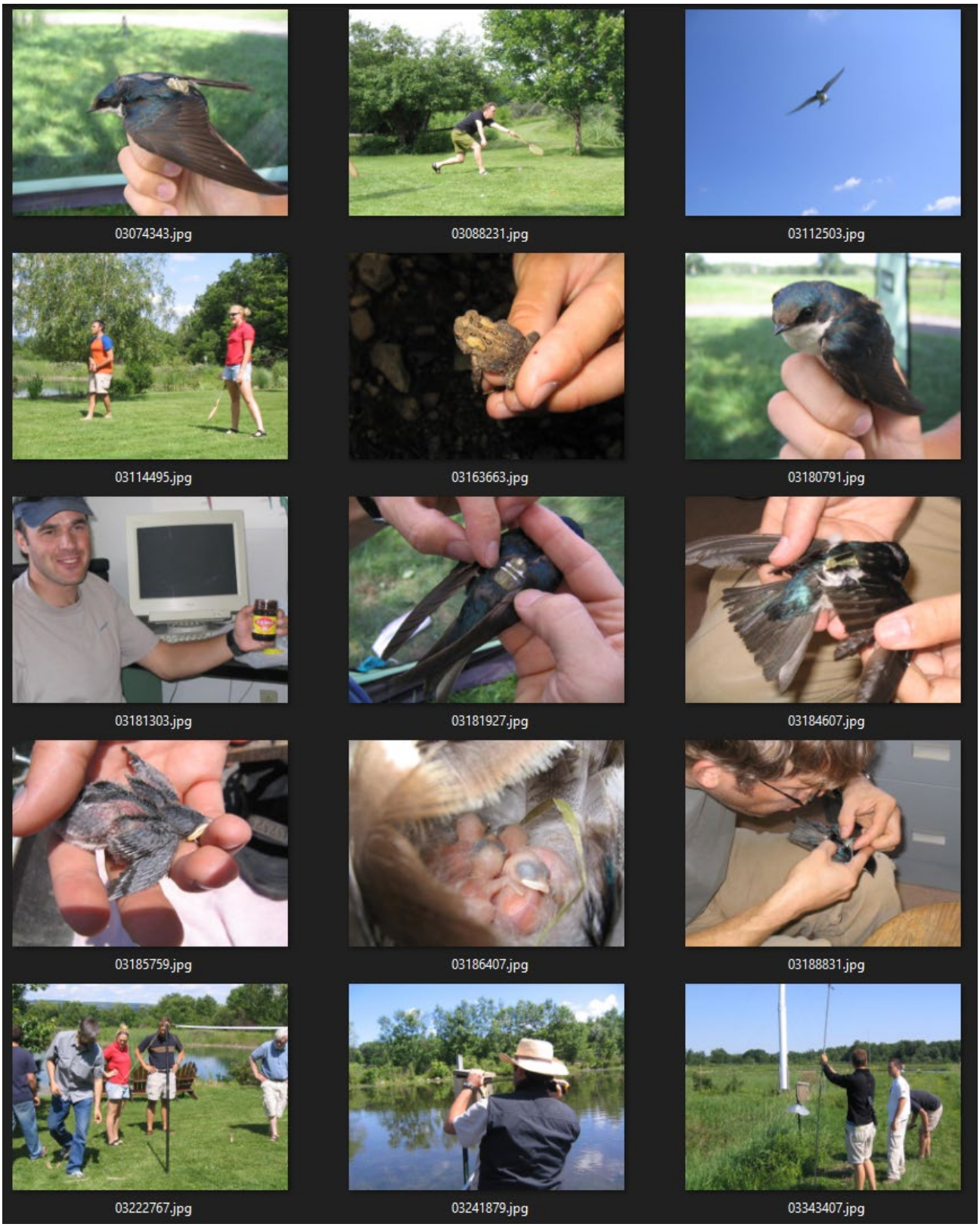



# Appendix 3 – Canon Cameras Images

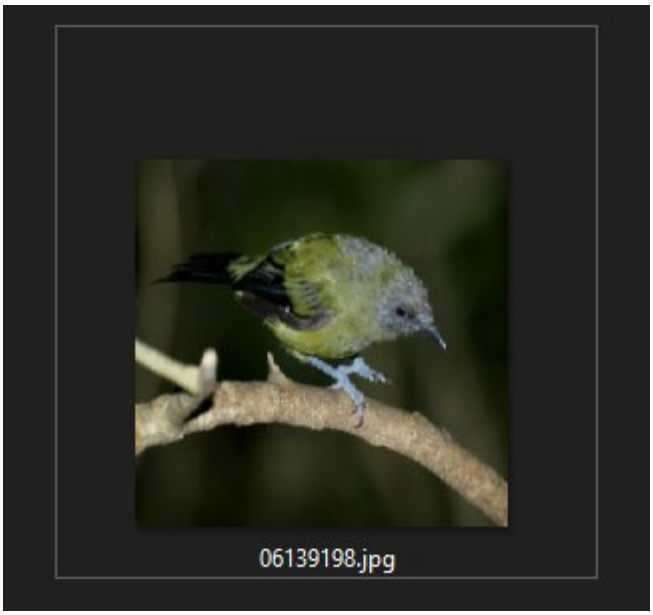
## 3.1. Canon PowerShot




03074343.jpg
03088231.jpg
03112503.jpg
03114495.jpg
03163663.jpg
03180791.jpg
03181303.jpg
03181927.jpg
03184607.jpg
03185759.jpg
03186407.jpg
03188831.jpg
03222767.jpg
03241879.jpg
03343407.jpg


03348175.jpg
03393167.jpg
03420671.jpg
03477407.jpg
03499095.jpg
03516711.jpg
03518439.jpg
03528407.jpg
03538975.jpg
03541191.jpg
03559423.jpg
03593991.jpg
03665359.jpg
03673623.jpg
05063735.jpg
05069311.jpg
05180927.jpg
05475951.jpg

### 3.2. Canon EOS-1DS




## Appendix 4 – Bash Script Code

```
#!/bin/bash

#Riccardo Raso - 1902091@uad.ac.uk

#defining STRING variables

dwn_dir="/home/student/Downloads"

Desktop="/home/student/Desktop"

jd_dir="/home/student/Desktop/jd"


john_img="/home/student/Downloads/johnDoe.dd.gz"

john_dd="/home/student/Downloads/johnDoe.dd"

john_dd2="/home/student/Desktop/jd/johnDoe.dd"


now=$(date +"%m%d_%H%M")
```

```
#-----------------------------------------------------------------------------------------------------------

ls_dirs(){
ls -F -1 -l --time-style=full-iso
}

#defining FUNCTION variables
stage3_echo(){
echo -e "
\e[7m|-------------------------------------------------------------|
|-----------------\e[1m|STAGE #3 - PHYSICAL SEARCH|\e[0m\e[7m-----------------|
|-------------------------------------------------------------|\n\e[0m"
}

terms_use(){
echo -e "\e[96m\e[1mThank you for agreeing to our terms of use by running this\nbash script after choosing to give read/write rights.\n\n\tWe give it as granted your Linux machine is up to date and\n\tthat the tool' foremost' is already installed and blah blah blah.\n\tOtherwise, please end this program and install that first.\e[0m"
}

anykey(){
```

```
echo -e "\n\n\e[100mPress any key to continue\e[0m\v\n\n"

}


anykey_again(){

echo -e "\n\n\e[100mPress any key, then try again\e[0m\v\n\n"

}


anykey2(){

echo -e "\n\n\e[100mSUCCESS!! Press any key to continue\e[0m\v\n\n"

}


parag1(){

echo -e "\nThe aim of STAGE 3 is to start searching the contents of the

disk image from the John Doe case that come from the previous
sections.\e[0m\n\n\n\n"

}


verifyecho(){

echo -e "\n\n\t\t\t\e[7m----------SECTION 3.A----------\e[0m\n\nPlease, let us verify
whether the compressed or uncompressed\nfile of interest exists or not:
\n\t\t\e[34mjohnDoe.dd.gz\n\t\e[0mor \n\t\t\e[34mjohnDoe.dd\n\t\e[0mThese (or even
just one of the two) should be placed\n\tin the Download folder under:
\n\t\t\e[0m\e[93m/home/student/Downloads\e[0m...\n\n\t...hit\e[0m \e[42mY+enter\e[0m
to continue or \e[41mN+enter\e[0m to abort.\v"
```

```
}

permissions(){

echo -e "\n\n Please, allow us to check the presence of the concerning file
by entering one\nof the two following options:\vY --> YES,  check this for me\n\v\vN -->
NO,  abort."

}

exists(){

echo -e "AWESOME!\nThe uncompressed version of the file exists!...\n\n\e[5mPRESS
ENTER TO CONTINUE\e[25m...\e[0m\n\n"

}

dwn_johnDoe(){

echo -e "OH NO! --> None of the two files was found.\nYou may want to
\e]8;;https://liveabertayac-
my.sharepoint.com/:u:/r/personal/1902091_uad_ac_uk/Documents/bash_analysis-
backup/johnDoe.dd.gz?csf=1&web=1&e=c1fv2v\a \e[44mdownload\e[0m the
compressed version (1.6gb)\e]8;;\a\n\n"

echo "(once downloaded press enter to continue)"

}

perm2_echo(){

echo -e "\n\n\t\t\t\e[7m----------SECTION 3.B----------\e[0m\n\n\e[0m\n\nWe now need
to work with that image.\nIn order to do so, we'll need to ensure the correct rights to that
```

file.\n\tCan we assign it \e[43mchmod 400\e[0m permissions?(for this step, password\n\t may be required for action 'sudo chmod')\n\n ...hit\e[0m \e[42mY+enter\e[0m to approve or \e[41mCTRL+Z\e[0m to abort.\v"

}

perm2(){

sudo chmod 400 "$john_dd" && echo -e "\n\t\t\t\e[43mchmod 400 granted!\e[0m \n\nNow \e[1mpress enter\e[0m to continue..."

}

lab5_echo0(){

echo -e "\n\n\t\t\t\e[7m----------SECTION 3.C----------\e[0m\n\n\e[0m\n\nThe next steps of our investigation include:\n\t1)grabbing the \e[32mmd5 hash \e[97m of the \e[34mjohnDoe.dd\e[39m file\n\t2)finding all \e[95mJPG files\e[0m first;\n\t3)filtering all JPG images taken with a \e[95mCanon PowerShot\e[0m camera.\n\n\tYou will be prompt for confirmation before each step; but if you wish\n\tto proceed in a different way, you'll then need to terminate\n\tthis program \e[41mCTRL+Z\e[0m.\n\n\tOtherwise, please press \e[42mY+enter\e[0m to continue.    "

}

lab5_f1_e0(){

echo -e "\n\n\t\t\t\e[7m--------SECTION 3.C.0-TIDINESS-------\e[0m\n\n\tFirst of all, some tidiness.\n\tLet's begin from creating a working dir if it does not exist yet,\n\tnamed: <\e[36m/home/student/Desktop/\e[1mjd\e[0m>.\n\tAfterwards, let's move <\e[34mjohnDoe.dd\e[0m> from <\e[36m../Downloads\e[0m> to the

```
newly\n\tcreated one...\n\t(...for this step, password may be required for action 'sudo mv').\n\n\t\t\t\t\e[90m(press enter to continue...)\e[0m\n\n"

}


lab5_f1_f0(){

cd "$Desktop" ; mkdir -p "$jd_dir" ; sudo mv "$john_dd" "$jd_dir" ; echo -e "\n\n\t\t\e[46mNew directory successfully created!\e[0m\n\t\t\e[46m   JOHNDOE.dd successfully moved!  \e[0m\n\n\t\t\t\t\e[90m(press enter to continue...)\e[0m\n\n"

}


lab5_f1_e1(){

echo -e "\n\n\t\t\t\e[7m--------SECTION 3.C.1-MD5 HASH-------\e[0m\n\n\tWe are about to \e[32mcheck the HASH\e[0m of johnDoe.dd file \e[42musing md5sum\e[0m.\n\tThis will generate a txt file named:\n\t\t <\e[36m[date (mmdd)]_[time (hhmm)]-md5hash_johnDoe.txt\e[0m>\n\tin your newly created working dir (where <\e[34mjohnDoe.dd\e[0m> is supposed to be).\n\n\tThe file md5hash_johnDoe.txt is prompt ('cat') in the terminal afterwards.\n\n\t...please be patient, it could take quite a while (up to 11 min)."

}


lab5_f1_f1(){

cd "$jd_dir" ; md5sum johnDoe.dd >> $now-md5sum_johnDoe.txt ; cat $now-md5sum_johnDoe.txt ; echo -e "\n\n\t\t\t\e[90m(press enter to continue...)\e[0m\n\n"

}
```

```
lab5_f1_e2(){

echo -e "\n\n\t\t\t\e[7m--------SECTION 3.C.2-JPG FILEs----------\e[0m\n\n\tWe are about to collect all \e[95mJPG files\e[0m \e[105musing foremost\e[0m.\n\tThis will generate a new folder-path <\e[36m./fileCarving/jpg\e[0m> inside\n\tthe current working dir, which is going to be the same as\n\tin the previous step:\n\t\t<\e[36m/home/student/Desktop/jd\e[0m>.\n\n---->\tInside the first of the two new folders, a txt file named:\n\t\t<\e[36m./fileCarving/audit.txt\e[0m>\n\twill report the findings of each single element\n\n\t...please be patient, it could take quite a while (up to 5 min).\n\n\t\t\t\t\e[90m(press enter to continue...)\e[0m\n\n"

}


lab5_f1_f2(){

cd "$jd_dir" ; foremost -T -t jpg -i johnDoe.dd -o fileCarving ; cd */jpg ; echo -e "\n\n\t\t\t\t\e[90m(press enter to continue...)\e[0m\n\n"

}


lab5_f1_e3(){

echo -e "\n\n\t\t\t\e[7m--------SECTION 3.C.3-CANON JPG----------\e[0m\n\n\tThis stage will be further divided in other smaller steps.\n\tFirst of all, we need to find out which of the JPG files \n\tdiscovered in the step before were produced by a Canon\n\tPowerShot camera. \n\n\tFor this stage, we will attempt to gain the exif header of each\n\tJPG file (if there's any).\n\n\tThe program may output some 'warnings': no worries. After the\n\twarnings, you should be prompted about the satus of the program.\n\n\tA new folder named <\e[36m./fileCarving/jpg/Powershot\e[0m> will include\n\tthe photos johnDoes took with a Powershot camera.\n\n\t\t\\e[90m(please be patient, it could take up to 2 min)\e[0m\n\n"

}
```

```
lab5_f1_f3_f1(){
cd /home/student/Desktop/jd/*/jpg/ ; identify -verbose * | egrep "Image:|exif:Model" | tr "\n" "-" | sed "s/Image:/\n/g" >> ../exifh1.txt
}
lab5_f1_f3_f1_e1(){
echo -e "\n\n\t\t\t\t\e[90m(press enter to continue...)\e[0m\n\n"
}

lab5_f1_f3_f2(){
cd /home/student/Desktop/jd/*/ ; grep 'PowerShot' -C 0 exifh1.txt  >> exifh2.txt; echo -e "\n\tgenerating exifh2.txt\n\n\t\t\t\t\e[90m(press enter to continue...)\e[0m\n\n"
}

lab5_f1_f3_f3(){
cd /home/student/Desktop/jd/*/ ; awk '{print $1}' exifh2.txt >> exifh3.txt ; tr -d '-' < exifh3.txt > exifh.txt ; cp exifh.txt ./jpg ; echo -e "\n\tgenerating exifh.txt\n\n\t\t\t\t\e[90m(press enter to continue...)\e[0m\n\n"
}

lab5_f1_f3_f4(){
cd /home/student/Desktop/jd/*/jpg ; mkdir -p ./Powershot ; xargs -a exifh.txt cp -t ./Powershot ; echo -e "\n\tJPG files moved to Powershot dir.\n\n\t\t\t\t\e[90m(press enter to continue...)\e[0m\n\n"
```

```
}

lab5_f1_f3(){
read -p "$(lab5_f1_f3_f1)"

read -p "$(lab5_f1_f3_f2)"

read -p "$(lab5_f1_f3_f3)"

read -p "$(lab5_f1_f3_f4)"

}

lab5_f1(){
read -p "$(lab5_f1_e0)"

read -p "$(lab5_f1_f0)"

read -p "$(lab5_f1_e1)"

read -p "$(lab5_f1_f1)"
```

```
read -p "$(lab5_f1_e2)"

read -p "$(lab5_f1_f2)"

read -p "$(lab5_f1_e3)"

read -p "$(lab5_f1_f3)"

}

lab5(){
while true; do
read -p "$(lab5_echo0)" yn
case $yn in

[Yy]* ) read -p "$(lab5_f1)" && echo "PHYSICAL SEARCH DONE!" && break;;
[Nn]* ) exit;;

esac
done
}
```

```
permission2(){
  while true; do
   read -p "$(perm2_echo)" yn
   case $yn in

   [Yy]* ) read -p "$(perm2)" && read -p "$(lab5)" && break;;
   [Nn]* ) exit;;

   esac
  done
}

ucomp_echo(){
echo -e "\n\nWE'VE FOUND \e[34mjohnDoe.dd.gz\e[0m.\nDo you want to \e[1muncompress\e[0m the disk image of John Doe's disk?\nhit\e[0m \e[42mY+enter\e[0m to continue or \e[41mN+enter\e[0m to abort.\n\n afterwards, please wait some minutes (shouldn't be more than 4 min)\n\n\e[90mplease press\e[0m \e[41mCTRL+Z\e[0m\e[90m at any time to abort.\e[0m\v"
}

ucomp_echo2(){
echo -e "uncompression successfully terminated\n\n\e[100mPress any key to continue\e[0m\v\n\n"
```

```
}

ucomp(){
cd "$dwn_dir" && gunzip johnDoe.dd.gz

read -n 1 -s -r -p "$(anykey2)"

#rm -r "$john_img"

read -p "$(ucomp_echo2)"

read -p "$(permission2)"

read -p "$(img_existence)"

}

ucompress(){
  while true; do
   read -p "$(ucomp_echo)" yn
   case $yn in
```

```
   [Yy]* ) read -p "$(ucomp)" && break;;

   [Nn]* ) exit;;


   esac

  done

}


img_existence(){

  if [ -f "$john_dd" ] || [ -f "$john_dd2" ] ; then

   read -p "$(exists)" && read -p "$(permission2)"


    elif  [ -f "$john_img" ]; then

     echo -e "johnDoe.dd.gz exists and it's still compressed...\v...giving it chmod -R 777 permissions so to work with that\n\e[5mPRESS ENTER TO CONTINUE\e[25m.\e[0m\n\n" && chmod u+x "$john_img" && read -p "$(ucompress)" && exit


   else

   echo -e "The file of interest does not exist.\n\t\tPlease, try again later by running again the script.\n\t\e"

   read -p  "$(dwn_johnDoe)"

   read -n 1 -s -r -p "$(anykey_again)"

  fi

}
```

```
#////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////

#main-SCRIPT

echo -e "$(stage3_echo)"


echo -e "$(terms_use)"


read -n 1 -s -r -p "$(anykey)"


echo -e "$(parag1)"


read -n 1 -s -r -p "$(anykey)"


while true; do

read -p "$(verifyecho)" yn

case $yn in


[Yy]* ) read -p "$(img_existence)" && break;; #https://linuxize.com/post/bash-break-continue/

[Nn]* ) exit;;


esac

done
```

## Appendix 5 – Bash Script Search Results

01243351.jpg- exif:Model: Canon PowerShot SD100-

02281199.jpg- exif:Model: Canon PowerShot SD100-

02791503.jpg- exif:Model: Canon PowerShot SD100-

02792151.jpg- exif:Model: Canon PowerShot SD100-

02792407.jpg- exif:Model: Canon PowerShot SD100-

02815079.jpg- exif:Model: Canon PowerShot SD100-

02903551.jpg- exif:Model: Canon PowerShot SD100-

02952815.jpg- exif:Model: Canon PowerShot SD100-

02962639.jpg- exif:Model: Canon PowerShot SD100-

02963839.jpg- exif:Model: Canon PowerShot SD100-

02997495.jpg- exif:Model: Canon PowerShot SD100-

03018151.jpg- exif:Model: Canon PowerShot SD100-

03018663.jpg- exif:Model: Canon PowerShot SD100-

03030271.jpg- exif:Model: Canon PowerShot SD100-

03062263.jpg- exif:Model: Canon PowerShot SD100-

03074343.jpg- exif:Model: Canon PowerShot SD100-

03088231.jpg- exif:Model: Canon PowerShot SD100-

03112503.jpg- exif:Model: Canon PowerShot SD100-

03114495.jpg- exif:Model: Canon PowerShot SD100-

03163663.jpg- exif:Model: Canon PowerShot SD100-

03180791.jpg- exif:Model: Canon PowerShot SD100-

03181303.jpg- exif:Model: Canon PowerShot SD100-

03181927.jpg- exif:Model: Canon PowerShot SD100-

03184607.jpg- exif:Model: Canon PowerShot SD100-

03185759.jpg- exif:Model: Canon PowerShot SD100-

03186407.jpg- exif:Model: Canon PowerShot SD100-

03188831.jpg- exif:Model: Canon PowerShot SD100-

03222767.jpg- exif:Model: Canon PowerShot SD100-

03241879.jpg- exif:Model: Canon PowerShot SD100-

03343407.jpg- exif:Model: Canon PowerShot SD100-

03348175.jpg- exif:Model: Canon PowerShot SD100-

03393167.jpg- exif:Model: Canon PowerShot SD100-

03420671.jpg- exif:Model: Canon PowerShot SD100-

03477407.jpg- exif:Model: Canon PowerShot SD100-

03499095.jpg- exif:Model: Canon PowerShot SD100-

03516711.jpg- exif:Model: Canon PowerShot SD100-

03518439.jpg- exif:Model: Canon PowerShot SD100-

03528407.jpg- exif:Model: Canon PowerShot SD100-

03538975.jpg- exif:Model: Canon PowerShot SD100-

03541191.jpg- exif:Model: Canon PowerShot SD100-

03559423.jpg- exif:Model: Canon PowerShot SD100-

03593991.jpg- exif:Model: Canon PowerShot SD100-

03665359.jpg- exif:Model: Canon PowerShot SD100-

03673623.jpg- exif:Model: Canon PowerShot SD100-

05063735.jpg- exif:Model: Canon PowerShot SD100-

05069311.jpg- exif:Model: Canon PowerShot SD100-

05180927.jpg- exif:Model: Canon PowerShot SD100-

05475951.jpg- exif:Model: Canon PowerShot SD100-

06139198.jpg- exif:Model: Canon EOS-1DS-

## Appendix 6 – johndoe Web History

| | | | |
|---|---|---|---|
| about:Home | 2005-01-24 23:57:10 GMT | Internet Explorer | |
| res\WINDOWS\system32\shdoclc.dll/dnserror.htm | 2005-01-25 00:13:02 GMT | Internet Explorer | res\WINDOWS\system32\s |
| file/WINDOWS/system32/oobe/actshell.htm | 2005-01-25 00:13:56 GMT | Internet Explorer | |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/js/tgar.js?1/24/2005%208:15:21%20AM | 2005-01-25 00:15:25 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/js/redirect.js?1/24/2005%208:15:21%20AM | 2005-01-25 00:15:26 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/js/commontop.js?1/24/2005%208:15:21%20AM | 2005-01-25 00:15:27 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/js/spupdateids.js?1/24/2005%208:15:21%20AM | 2005-01-25 00:15:29 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/js/webcomtop.js?1/24/2005%208:15:21%20AM | 2005-01-25 00:15:29 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/js/survey.js?632421512922307396 | 2005-01-25 00:15:34 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/SelfUpdate/wuident.cab?0501241615 | 2005-01-25 00:15:40 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/SelfUpdate/AU/x86/XP/en/wusetup.cab?0501241615 | 2005-01-25 00:15:41 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/js/survey.js?632421512871551603 | 2005-01-25 00:15:46 GMT | Internet Explorer | microsoft.com |
| javascript:parent.fnExpressScan(); | 2005-01-25 00:15:54 GMT | Internet Explorer | |
| http://v5.windowsupdate.microsoft.com/v5consumer/resultslist.aspx?ln=en-us&id=612e66c8b | 2005-01-25 00:16:07 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/resultslist.aspx?ln=en-us&id=6 | 2005-01-25 00:16:10 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/js/resultslist.js?1/24/2005%208:16:07%20AM | 2005-01-25 00:16:10 GMT | Internet Explorer | microsoft.com |
| http://www.linorg.usp.br/mozilla//firefox/releases/1.0/win32/en-GB/Firefox%20Setup%201.0.exe | 2005-01-25 00:19:35 GMT | Internet Explorer | usp.br |
| http://www.linorg.usp.br/mozilla//firefox/releases/1.0/win32/en-GB/Firefox%20Setup%201.0.exe | 2005-01-25 00:20:34 GMT | Internet Explorer | usp.br |
| http://i.i.com.com/cnwk.1d/i/cobd/ec/EC_nov04_39x72.gif | 2005-01-25 00:21:41 GMT | Internet Explorer | com.com |
| http://www.mozilla.org/images/ff_shirt.jpg | 2005-01-25 00:21:41 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/images/product-firefox-screen.png | 2005-01-25 00:21:41 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/products/firefox/ | 2005-01-25 00:21:41 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/products/firefox/featuring-flash.gif | 2005-01-25 00:21:41 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/products/firefox/featuring-java.gif | 2005-01-25 00:21:41 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/products/firefox/featuring-realplayer.gif | 2005-01-25 00:21:41 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/products/firefox/featuring-shockwave.gif | 2005-01-25 00:21:41 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/products/firefox | 2005-01-25 00:21:42 GMT | Internet Explorer | mozilla.org |
| http://download.mozilla.org/?product=firefox&os=win&lang=en-GB | 2005-01-25 00:21:43 GMT | Internet Explorer | mozilla.org |
| http://mozilla.mirrors.tds.net/pub/mozilla.org/firefox/releases/1.0/win32/en-GB/Firefox%20Setup%201.0.exe | 2005-01-25 00:22:19 GMT | Internet Explorer | tds.net |
| http://mozilla.mirrors.tds.net/pub/mozilla.org/firefox/releases/1.0/win32/en-GB/Firefox%20Setup%201.0.exe | 2005-01-25 00:22:25 GMT | Internet Explorer | tds.net |
| http://v5.windowsupdate.microsoft.com/v5consumer/InstallStatus.aspx?page=0&ln=en-us | 2005-01-25 00:22:56 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/info_16x.gif | 2005-01-25 00:22:57 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/ok.gif | 2005-01-25 00:22:57 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/warning.gif | 2005-01-25 00:22:57 GMT | Internet Explorer | microsoft.com |
| http://c.microsoft.com/trans_pixel.asp?source=v5.windowsupdate&TYPE=PV&p=v5consumer_InstallStatus.aspx& | 2005-01-25 00:22:58 GMT | Internet Explorer | microsoft.com |
| http://www.mozilla.org/images/product-bugzilla.png | 2005-01-25 00:23:13 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/images/product-calendar.png | 2005-01-25 00:23:13 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/images/product-camino.png | 2005-01-25 00:23:13 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/images/product-firefox.png | 2005-01-25 00:23:13 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/images/product-mozilla.png | 2005-01-25 00:23:13 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/images/product-thunderbird.png | 2005-01-25 00:23:13 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/products/ | 2005-01-25 00:23:13 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/products | 2005-01-25 00:23:15 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/css/base/content.css | 2005-01-25 00:23:23 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/css/base/template.css | 2005-01-25 00:23:23 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/css/cavendish/content.css | 2005-01-25 00:23:23 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/css/cavendish/template.css | 2005-01-25 00:23:23 GMT | Internet Explorer | mozilla.org |

| | | | |
|---|---|---|---|
| http://www.mozilla.org/css/print.css | 2005-01-25 00:23:23 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/images/body_back.gif | 2005-01-25 00:23:23 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/images/header_bl.png | 2005-01-25 00:23:23 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/images/header_br.gif | 2005-01-25 00:23:23 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/images/header_tr.gif | 2005-01-25 00:23:23 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/products/thunderbird/ | 2005-01-25 00:23:23 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/images/download_back.gif | 2005-01-25 00:23:24 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/images/header_logo.gif | 2005-01-25 00:23:24 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/images/header_tl.gif | 2005-01-25 00:23:24 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/images/key-point_back.gif | 2005-01-25 00:23:24 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/images/moz_shirt.jpg | 2005-01-25 00:23:24 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/images/shop_back.gif | 2005-01-25 00:23:24 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/products/thunderbird/award_softpediapick.gif | 2005-01-25 00:23:24 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/images/product-thunderbird-screen.png | 2005-01-25 00:23:25 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/products/thunderbird | 2005-01-25 00:23:25 GMT | Internet Explorer | mozilla.org |
| http://download.mozilla.org/?product=thunderbird&os=win&lang=en-US | 2005-01-25 00:23:26 GMT | Internet Explorer | mozilla.org |
| http://64.12.168.243/pub/mozilla.org/thunderbird/releases/1.0/win32/en-US/Thunderbird%20Setup%201.0.exe | 2005-01-25 00:24:24 GMT | Internet Explorer | 64.12.168.243 |
| http://64.12.168.243/pub/mozilla.org/thunderbird/releases/1.0/win32/en-US/Thunderbird%20Setup%201.0.exe | 2005-01-25 00:24:56 GMT | Internet Explorer | 64.12.168.243 |
| http://www.mozilla.org/images/header_tab.gif | 2005-01-25 00:26:10 GMT | Internet Explorer | mozilla.org |
| http://windowsupdate.microsoft.com/ | 2005-01-25 00:39:57 GMT | Internet Explorer | microsoft.com |
| http://windowsupdate.microsoft.com | 2005-01-25 00:39:59 GMT | Internet Explorer | microsoft.com |
| http://windowsupdate.microsoft.com/redirect.js | 2005-01-25 00:39:59 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/default.aspx | 2005-01-25 00:40:01 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/default.aspx | 2005-01-25 00:40:02 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/default.aspx?ln=en-us | 2005-01-25 00:40:03 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/js/redirect.js?1/24/2005%208:40:03%20AM | 2005-01-25 00:40:03 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/js/tgar.js?1/24/2005%208:40:03%20AM | 2005-01-25 00:40:03 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/js/commontop.js?1/24/2005%208:40:03%20AM | 2005-01-25 00:40:05 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/js/webcomtop.js?1/24/2005%208:40:03%20AM | 2005-01-25 00:40:06 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/js/spupdateids.js?1/24/2005%208:40:03%20AM | 2005-01-25 00:40:07 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/library/toolbar/3.0/images/banners/windows_masthead_ltr.gif | 2005-01-25 00:40:08 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/mstoolbar.aspx?ln=en-us | 2005-01-25 00:40:08 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/library/toolbar/3.0/css.aspx?c=/v5consumer/Config/en/shell.config | 2005-01-25 00:40:09 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/library/toolbar/3.0/subbanner.aspx?t=V2luZG93cyBVcGRhdGU%3d&f=F | 2005-01-25 00:40:09 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/footer.aspx?ln=en-us | 2005-01-25 00:40:09 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/splash.aspx?page=0&ln=en-us | 2005-01-25 00:40:09 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/toc.aspx?ln=en-us | 2005-01-25 00:40:09 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/library/toolbar/3.0/text.aspx?t=TQ%3d%3d&f=FFFFFF&b=6487DB&font | 2005-01-25 00:40:10 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/js/toc.js | 2005-01-25 00:40:10 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/css/toc.css | 2005-01-25 00:40:11 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/icon_wu_installnow_16x.gif | 2005-01-25 00:40:11 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/default.aspx?ln=en-us | 2005-01-25 00:40:12 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/js/survey.js?632421527970738072 | 2005-01-25 00:40:12 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/SelfUpdate/AU/x86/XP/en/wusetup.cab?0501241640 | 2005-01-25 00:40:15 GMT | Internet Explorer | microsoft.com |
| http://c.microsoft.com/trans_pixel.asp?source=v5.windowsupdate&TYPE=PV&p=v5consumer_default.aspx | 2005-01-25 00:40:16 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/splash.aspx?page=3&cpuClass=x86&auenabled=false&ln=e | 2005-01-25 00:40:16 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/AU_Button_Left.gif | 2005-01-25 00:40:17 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/AU_Button_Right.gif | 2005-01-25 00:40:17 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/AU_ShieldYellow.gif | 2005-01-25 00:40:17 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/AU_bg_LeftBottom.gif | 2005-01-25 00:40:17 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/AU_bg_LeftTop.gif | 2005-01-25 00:40:17 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/AU_bg_RightBottom.gif | 2005-01-25 00:40:17 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/AU_bg_RightTop.gif | 2005-01-25 00:40:17 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/AU_bg_TopMiddle.gif | 2005-01-25 00:40:17 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/Banners/en/Hdr_Welcome.jpg | 2005-01-25 00:40:17 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/Hdr_Tall_Middle.gif | 2005-01-25 00:40:17 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/Hdr_Tall_Right.jpg | 2005-01-25 00:40:17 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/arrow.gif | 2005-01-25 00:40:17 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/js/survey.js?632421528169176842 | 2005-01-25 00:40:17 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/news.aspx?ln=en | 2005-01-25 00:40:18 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/AU_Button_Middle.gif | 2005-01-25 00:40:18 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/AU_ShieldGreen.gif | 2005-01-25 00:40:18 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/AU_bg_BottomMiddle.gif | 2005-01-25 00:40:18 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/AU_bg_LeftMiddle.gif | 2005-01-25 00:40:18 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/AU_bg_LeftTop_Green.gif | 2005-01-25 00:40:18 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/AU_bg_RightMiddle.gif | 2005-01-25 00:40:18 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/AU_bg_RightTop_Green.gif | 2005-01-25 00:40:18 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/AU_bg_TopMiddle_Green.gif | 2005-01-25 00:40:18 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/News_Info.gif | 2005-01-25 00:40:18 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/News_bg_BottomMiddle.gif | 2005-01-25 00:40:18 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/News_bg_LeftBottom.gif | 2005-01-25 00:40:18 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/News_bg_LeftMiddle.gif | 2005-01-25 00:40:18 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/News_bg_LeftTop.gif | 2005-01-25 00:40:18 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/News_bg_RightBottom.gif | 2005-01-25 00:40:18 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/News_bg_RightMiddle.gif | 2005-01-25 00:40:18 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/News_bg_RightTop.gif | 2005-01-25 00:40:18 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/News_bg_TopMiddle.gif | 2005-01-25 00:40:18 GMT | Internet Explorer | microsoft.com |
| http://c.microsoft.com/trans_pixel.asp?source=v5.windowsupdate&TYPE=PV&p=v5consumer_splash.aspx&r=htt | 2005-01-25 00:40:19 GMT | Internet Explorer | microsoft.com |
| javascript:parent.fnScan(); | 2005-01-25 00:40:26 GMT | Internet Explorer | |
| http://v5.windowsupdate.microsoft.com/v5consumer/resultslist.aspx?ln=en-us&id=060cadd56 | 2005-01-25 00:40:41 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/toc_collapsed.gif | 2005-01-25 00:40:41 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/toc_endnode.gif | 2005-01-25 00:40:41 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/js/resultslist.js?1/24/2005%208:40:14%20AM | 2005-01-25 00:40:42 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/resultslist.aspx?ln=en-us&id=0 | 2005-01-25 00:40:43 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/resultslist.aspx?ln=en-us&id=1&LinkId=SOFTWARE&TocIn | 2005-01-25 00:41:09 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/css/content.css | 2005-01-25 00:41:09 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/css/hcp.css | 2005-01-25 00:41:09 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/toc_expanded.gif | 2005-01-25 00:41:09 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/js/content.js | 2005-01-25 00:41:09 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/js/resultslist.js?1/24/2005%208:41:09%20AM | 2005-01-25 00:41:09 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/js/tgar.js | 2005-01-25 00:41:09 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/blank.aspx | 2005-01-25 00:41:10 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/resultslist.aspx?ln=en-us&id=1&LinkId=SOFTWARE&TocIn | 2005-01-25 00:41:10 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/Banners/en/Hdr_CustomInstall.jpg | 2005-01-25 00:41:10 GMT | Internet Explorer | microsoft.com |

| | | | |
|---|---|---|---|
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/Banners/en/Hdr_ExpressInstall.jpg | 2005-01-25 00:41:10 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/Banners/en/Hdr_InstallBasket.jpg | 2005-01-25 00:41:10 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/Hdr_Shrt_Middle.jpg | 2005-01-25 00:41:10 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/shared/images/Hdr_Shrt_Right.jpg | 2005-01-25 00:41:10 GMT | Internet Explorer | microsoft.com |
| http://c.microsoft.com/trans_pixel.asp?source=v5.windowsupdate&TYPE=PV&p=v5consumer_resultslist.aspx&r= | 2005-01-25 00:41:12 GMT | Internet Explorer | microsoft.com |
| about:blank | 2005-01-25 19:16:36 GMT | Internet Explorer | |
| http://office.microsoft.com/global/images/1ptrans_ZA06047535.gif | 2005-01-25 19:16:44 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/global/images/default.aspx?assetid=ZA010499831033 | 2005-01-25 19:16:44 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/global/images/default.aspx?assetid=ZA011158451033 | 2005-01-25 19:16:44 GMT | Internet Explorer | microsoft.com |
| http://c.microsoft.com/trans_pixel.aspx?TYPE=SSPV&SOURCE=OFFICE&guid=1f4fc18c-f71e-47fb-8fc9-612f8ee59 | 2005-01-25 19:16:45 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/_Services/Ont/images/BulletLN.gif | 2005-01-25 19:16:45 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/_Services/Ont/images/RghtArrBlt.gif | 2005-01-25 19:16:45 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/en-gb/officeupdate/default.aspx | 2005-01-25 19:16:45 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/global/images/default.aspx?assetid=HX010492821033 | 2005-01-25 19:16:45 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/global/images/default.aspx?assetid=ZA011035021033 | 2005-01-25 19:16:45 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/global/images/default.aspx?assetid=ZA011708901033 | 2005-01-25 19:16:45 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/search/redir.aspx?AssetID=ES790020331033&Origin=HH010704921033&CTT=5 | 2005-01-25 19:16:47 GMT | Internet Explorer | microsoft.com |
| ?CodeDownloadErrorLog!name={3E68E405-C6DE-49FF-83AE-41EE9F4C36CE} | 2005-01-25 19:16:54 GMT | Internet Explorer | |
| http://office.microsoft.com/en-gb/FX010329501033.aspx | 2005-01-25 19:16:54 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/global/images/default.aspx?AssetID=ZA011357811033 | 2005-01-25 19:16:55 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/global/images/default.aspx?AssetID=ZA011357821033 | 2005-01-25 19:16:55 GMT | Internet Explorer | microsoft.com |
| http://c.microsoft.com/trans_pixel.aspx?TYPE=SSPV&SOURCE=OFFICE&guid=1f4fc18c-f71e-47fb-8fc9-612f8ee59 | 2005-01-25 19:16:56 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/en-gb/FX010329501033.aspx | 2005-01-25 19:16:56 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/officeupdate/content/opuc.cab | 2005-01-25 19:17:25 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/officeupdate/catalog/xml/1033/SP1_11_1033.xml?632422172995214127 | 2005-01-25 19:17:40 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/officeupdate/catalog/xml/1033/OLKFTR_0.xml?632422172995214127 | 2005-01-25 19:17:42 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/en-gb/FX010355751033.aspx | 2005-01-25 19:25:53 GMT | Internet Explorer | microsoft.com |
| http://c.microsoft.com/trans_pixel.aspx?TYPE=SSPV&SOURCE=OFFICE&guid=1f4fc18c-f71e-47fb-8fc9-612f8ee59 | 2005-01-25 19:25:56 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/en-gb/FX010355751033.aspx | 2005-01-25 19:25:56 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/search/redir.aspx?AssetID=ES790020331033&CTT=5&Origin=HA010492041033 | 2005-01-25 19:26:00 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/officeupdate/maincatalog.aspx?lc=en-gb | 2005-01-25 19:26:01 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/_Services/ont/images/WWGlobe.gif | 2005-01-25 19:26:02 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/officeupdate/arrowright.gif | 2005-01-25 19:26:02 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/officeupdate/mainsc.js?11,0,6412,0 | 2005-01-25 19:26:02 GMT | Internet Explorer | microsoft.com |
| http://c.microsoft.com/trans_pixel.aspx?TYPE=SSPV&SOURCE=OFFICE&guid=1f4fc18c-f71e-47fb-8fc9-612f8ee59 | 2005-01-25 19:26:03 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/officeupdate/catalog/SiteBaselines.xml?632422172995214127 | 2005-01-25 19:26:03 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/officeupdate/catalog/ActiveBundles.xml?632422172995214127 | 2005-01-25 19:26:04 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/officeupdate/maincatalog.aspx?lc=en-gb | 2005-01-25 19:26:04 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/officeupdate/catalog/xml/1033/FGC11_0.xml?632422172995214127 | 2005-01-25 19:26:14 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/officeupdate/catalog/xml/1033/INFPXSN11_1033.xml?632422172995214127 | 2005-01-25 19:26:14 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/_Services/Ont/images/ONTLogoLt.gif | 2005-01-25 19:26:22 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/officeupdate/wizardFrame.aspx | 2005-01-25 19:26:22 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/officeupdate/wizardUpdate.aspx | 2005-01-25 19:26:22 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/officeupdate/bang.gif | 2005-01-25 19:26:23 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/officeupdate/check.gif | 2005-01-25 19:26:23 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/officeupdate/disk.gif | 2005-01-25 19:26:23 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/officeupdate/timer.gif | 2005-01-25 19:26:23 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/_Services/Ont/images/TBGradient.gif | 2005-01-25 19:27:44 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/_Services/Ont/images/bulletl.gif | 2005-01-25 19:27:44 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/_Services/Ont/oo.js | 2005-01-25 19:33:44 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/_Services/Ont/images/ONLBulCol.gif | 2005-01-25 19:33:45 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/_Services/Ont/images/ONLHorzSpcrTail.gif | 2005-01-25 19:33:45 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/_Services/Ont/images/ONLItemBk.gif | 2005-01-25 19:33:45 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/_Services/Ont/images/ONLPlCellSpcr2.gif | 2005-01-25 19:33:45 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/_Services/Ont/images/ONTLogo.gif | 2005-01-25 19:33:45 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/_Services/Ont/images/WWGlobe.gif | 2005-01-25 19:33:45 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/_Services/Ont/images/cg2057.gif | 2005-01-25 19:33:45 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/_Services/Ont/images/footerMSlogo.gif | 2005-01-25 19:33:45 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/_Services/Ont/images/footerl.gif | 2005-01-25 19:33:45 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/_Services/Ont/images/topnav2m.gif | 2005-01-25 19:33:45 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/_Services/Ont/images/topnav2r.gif | 2005-01-25 19:33:45 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/_Services/Ont/images/topnav3r.gif | 2005-01-25 19:33:45 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/en-gb/FX010354621033.aspx | 2005-01-25 19:33:45 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/global/images/default.aspx?AssetID=ZA010499831033 | 2005-01-25 19:33:45 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/global/images/default.aspx?assetid=ZA011153081033 | 2005-01-25 19:33:45 GMT | Internet Explorer | microsoft.com |
| http://c.microsoft.com/trans_pixel.aspx?TYPE=SSPV&SOURCE=OFFICE&guid=1f4fc18c-f71e-47fb-8fc9-612f8ee59 | 2005-01-25 19:33:46 GMT | Internet Explorer | microsoft.com |
| http://office.microsoft.com/en-gb/FX010354621033.aspx | 2005-01-25 19:33:46 GMT | Internet Explorer | microsoft.com |
| file/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/tn_duck_3.jpg | 2005-02-02 22:18:13 GMT | Internet Explorer | |
| http://www.mozilla.org/products/thunderbird | 2005-02-02 22:18:13 GMT | Internet Explorer | mozilla.org |
| 64.12.168.243 | 2005-02-02 22:18:14 GMT | Internet Explorer | 64.12.168.243 |
| My Computer | 2005-02-02 22:18:14 GMT | Internet Explorer | |
| file/WINDOWS/system32/oobe/actshell.htm | 2005-02-02 22:18:14 GMT | Internet Explorer | |
| http://v5.windowsupdate.microsoft.com/v5consumer/default.aspx | 2005-02-02 22:18:14 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/default.aspx?ln=en-us | 2005-02-02 22:18:14 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/resultslist.aspx?ln=en-us&id=0 | 2005-02-02 22:18:14 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/resultslist.aspx?ln=en-us&id=1&LinkId=SOFTWARE&TocIn | 2005-02-02 22:18:14 GMT | Internet Explorer | microsoft.com |
| http://v5.windowsupdate.microsoft.com/v5consumer/resultslist.aspx?ln=en-us&id=6 | 2005-02-02 22:18:14 GMT | Internet Explorer | microsoft.com |
| http://www.linorg.usp.br/mozilla//firefox/releases/1.0/win32/en-GB/Firefox%20Setup%201.0.exe | 2005-02-02 22:18:14 GMT | Internet Explorer | usp.br |
| http://www.mozilla.org/products | 2005-02-02 22:18:14 GMT | Internet Explorer | mozilla.org |
| http://www.mozilla.org/products/firefox | 2005-02-02 22:18:14 GMT | Internet Explorer | mozilla.org |
| mozilla.mirrors.tds.net | 2005-02-02 22:18:14 GMT | Internet Explorer | tds.net |
| v5.windowsupdate.microsoft.com | 2005-02-02 22:18:14 GMT | Internet Explorer | microsoft.com |
| www.linorg.usp.br | 2005-02-02 22:18:14 GMT | Internet Explorer | usp.br |
| www.mozilla.org | 2005-02-02 22:18:14 GMT | Internet Explorer | mozilla.org |
| file/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/snow_geese.jpg | 2005-02-02 22:18:53 GMT | Internet Explorer | |
| file/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/7107298.jpg | 2005-02-02 22:20:33 GMT | Internet Explorer | |
| file/Documents%20and%20Settings/johndoe/My%20Documents/aa010703a.htm | 2005-02-02 22:25:59 GMT | Internet Explorer | |
| file/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/wbpremium_s.jpg | 2005-02-02 22:28:19 GMT | Internet Explorer | |
| file/Documents%20and%20Settings/johndoe/My%20Documents/nestboxtips.txt | 2005-02-02 22:29:30 GMT | Internet Explorer | |
| file/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/40m.jpg | 2005-02-02 22:43:36 GMT | Internet Explorer | |
| file/Program%20Files/Real/RealPlayer/DataCache/Login/index.html | 2005-02-02 22:57:13 GMT | Internet Explorer | |
| http://home.real.com/signin/3.0/loader.html?cd=firstrun_acct&loader=2.0&LI=en&PV=6.0.12.1053 | 2005-02-02 22:57:19 GMT | Internet Explorer | real.com |
| http://home.real.com/signin/common/log/log.html?configcount=1&distcode=NSP01D&build=6.0.12.1053&overi | 2005-02-02 22:57:20 GMT | Internet Explorer | real.com |
| ?CodeDownloadErrorLog!name={00EF2092-6AC5-47C0-BD25-CF2D5D657FEB} | 2005-02-02 22:57:24 GMT | Internet Explorer | |

| | | | |
|---|---|---|---|
| http://home.real.com/signin/common/log/log.html?toolbar=Google&action=istoolbarregistered%20error&code= | 2005-02-02 22:57:24 GMT | Internet Explorer | real.com |
| http://i.real.com/g/pics/space.gif | 2005-02-02 23:04:16 GMT | Internet Explorer | real.com |
| http://www.real.com/intro/index.html?DC=NSP01D&optin=true&country=gb&language=en-gb&icon=tiscali | 2005-02-02 23:04:24 GMT | Internet Explorer | real.com |
| http://realguide.real.com/4plus/main_.js | 2005-02-02 23:04:25 GMT | Internet Explorer | real.com |
| http://www.real.com/4plus/trinity_.css | 2005-02-02 23:04:25 GMT | Internet Explorer | real.com |
| http://www.real.com/intro/index_upsell_manager.html?DC=NSP01D&optin=true&country=gb&language=en-gb& | 2005-02-02 23:04:25 GMT | Internet Explorer | real.com |
| http://i.real.com/pics/real/intro/bttn_disabled.gif | 2005-02-02 23:04:26 GMT | Internet Explorer | real.com |
| http://images.real.com//pics/real/common/bull_tri.gif | 2005-02-02 23:04:27 GMT | Internet Explorer | real.com |
| http://images.real.com//pics/space.gif | 2005-02-02 23:04:27 GMT | Internet Explorer | real.com |
| http://www.real.com/intro/index_upsell_manager.html?DC=NSP01D&optin=true&country=gb&language=en-gb& | 2005-02-02 23:04:28 GMT | Internet Explorer | real.com |
| http://i.real.com/pics/real/intro/bttn_enabled.gif | 2005-02-02 23:04:30 GMT | Internet Explorer | real.com |
| http://i.real.com/pics/real/intro/bttn_down.gif | 2005-02-02 23:04:34 GMT | Internet Explorer | real.com |
| http://i.real.com/pics/real/intro/bttn_over.gif | 2005-02-02 23:04:34 GMT | Internet Explorer | real.com |
| https://account.real.com/acct/intro/msg.html?msg=frweur | 2005-02-02 23:04:34 GMT | Internet Explorer | real.com |
| https://account.real.com/acct/intro/msg.html?msg=frweur | 2005-02-02 23:04:34 GMT | Internet Explorer | real.com |
| javascript:catchEvent('continue'); | 2005-02-02 23:04:34 GMT | Internet Explorer | |
| res\Program%20Files\Real\RealPlayer\rpplugins\rpmn3260.dll/black.html | 2005-02-02 23:04:43 GMT | Internet Explorer | |
| file/Program%20Files/Real/RealPlayer/Firstrun/1.htm | 2005-02-02 23:04:47 GMT | Internet Explorer | |
| file/Program%20Files/Adobe/Acrobat%207.0/Reader/Legal/Adobe%20Reader/7.0.0/en_US/license.html | 2005-02-03 01:03:40 GMT | Internet Explorer | |
| http://www-config.strath.ac.uk/proxy.config | 2005-02-03 19:50:10 GMT | Internet Explorer | strath.ac.uk |
| file/Documents%20and%20Settings/johndoe/Application%20Data/Mozilla/Firefox/Profiles/w4nf3obl.default/boc | 2005-02-03 20:20:20 GMT | Internet Explorer | |
| file/birds/audio/aggressive_song.wav | 2005-02-03 20:22:51 GMT | Internet Explorer | |
| file/EvanstonWoodpecker.jpg | 2005-02-03 22:14:59 GMT | Internet Explorer | |
| file/Documents%20and%20Settings/All%20Users/Documents/My%20Music/Sample%20Music/Doc1.doc | 2005-02-03 22:17:48 GMT | Internet Explorer | |
| file/birds/Killdeer.jpg | 2005-02-03 22:49:29 GMT | Internet Explorer | |
| file/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/babyscot_vyoung.jpg | 2005-02-03 23:00:19 GMT | Internet Explorer | |
| file/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/babyscot_2weeks1.jpg | 2005-02-03 23:00:27 GMT | Internet Explorer | |
| file/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/177.jpg | 2005-02-03 23:01:38 GMT | Internet Explorer | |
| file/Documents%20and%20Settings/johndoe/My%20Documents/ostbk2b2.htm | 2005-02-03 23:02:45 GMT | Internet Explorer | |
| file/Documents%20and%20Settings/johndoe/Desktop/birdtrans2.jpg | 2005-02-03 23:04:48 GMT | Internet Explorer | |
| file/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/chicks2.jpg | 2005-02-03 23:05:03 GMT | Internet Explorer | |
| file/Documents%20and%20Settings/johndoe/My%20Documents/newbies2.jpg | 2005-02-03 23:05:44 GMT | Internet Explorer | |
| file/Documents%20and%20Settings/bob/My%20Documents/My%20Music/ready2fledge.jpg | 2005-02-03 23:06:42 GMT | Internet Explorer | |
| file/birdwatching.doc | 2005-02-03 23:49:39 GMT | Internet Explorer | |
| file/birds/non%20images/BookList.doc | 2005-02-03 23:51:54 GMT | Internet Explorer | |
| file/birds/non%20images/BirdingGuide.pdf | 2005-02-03 23:52:01 GMT | Internet Explorer | |
| file/Documents%20and%20Settings/johndoe/My%20Documents/birds.zip | 2005-02-09 19:28:00 GMT | Internet Explorer | |
| My Computer | 2005-02-09 19:28:01 GMT | Internet Explorer | |
| My Computer | 2005-02-09 19:28:01 GMT | Internet Explorer | |
| account.real.com | 2005-02-09 19:28:01 GMT | Internet Explorer | real.com |
| account.real.com | 2005-02-09 19:28:01 GMT | Internet Explorer | real.com |
| file/Documents%20and%20Settings/All%20Users/Documents/My%20Music/Sample%20Music/Doc1.doc | 2005-02-09 19:28:01 GMT | Internet Explorer | |
| file/Documents%20and%20Settings/All%20Users/Documents/My%20Music/Sample%20Music/Doc1.doc | 2005-02-09 19:28:01 GMT | Internet Explorer | |
| file/Documents%20and%20Settings/johndoe/Application%20Data/Mozilla/Firefox/Profiles/w4nf3obl.default/coo | 2005-02-09 19:28:01 GMT | Internet Explorer | |
| file/Documents%20and%20Settings/johndoe/Application%20Data/Mozilla/Firefox/Profiles/w4nf3obl.default/coo | 2005-02-09 19:28:01 GMT | Internet Explorer | |
| file/Documents%20and%20Settings/johndoe/Desktop/birdtrans2.jpg | 2005-02-09 19:28:01 GMT | Internet Explorer | |
| file/Documents%20and%20Settings/johndoe/Desktop/birdtrans2.jpg | 2005-02-09 19:28:01 GMT | Internet Explorer | |

| | | |
|---|---|---|
| file/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/177.jpg | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/177.jpg | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/40m.jpg | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/40m.jpg | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/7107298.jpg | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/7107298.jpg | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/babyscot_2weeks1.jpg | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/babyscot_2weeks1.jpg | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/babyscot_vyoung.jpg | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/babyscot_vyoung.jpg | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/snow_geese.jpg | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/snow_geese.jpg | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/tn_duck_3.jpg | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/tn_duck_3.jpg | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/wbpremium_s.jpg | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/wbpremium_s.jpg | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Documents%20and%20Settings/johndoe/My%20Documents/aa010703a.htm | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Documents%20and%20Settings/johndoe/My%20Documents/aa010703a.htm | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Documents%20and%20Settings/johndoe/My%20Documents/kakapo.ram | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Documents%20and%20Settings/johndoe/My%20Documents/kakapo.ram | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Documents%20and%20Settings/johndoe/My%20Documents/nestboxtips.txt | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Documents%20and%20Settings/johndoe/My%20Documents/nestboxtips.txt | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Documents%20and%20Settings/johndoe/My%20Documents/newbies2.jpg | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Documents%20and%20Settings/johndoe/My%20Documents/newbies2.jpg | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Documents%20and%20Settings/johndoe/My%20Documents/ostbk2b2.htm | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Documents%20and%20Settings/johndoe/My%20Documents/ostbk2b2.htm | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/EvanstonWoodpecker.jpg | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/EvanstonWoodpecker.jpg | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Prac4/Prac4.gif | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Prac4/Prac4.gif | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Prac5/Q3%20Thread%20(Statechart).gif | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Prac5/Q3%20Thread%20(Statechart).gif | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Program%20Files/Adobe/Acrobat%207.0/Reader/Legal/Adobe%20Reader/7.0.0/en_US/license.html | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Program%20Files/Adobe/Acrobat%207.0/Reader/Legal/Adobe%20Reader/7.0.0/en_US/license.html | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Program%20Files/Real/RealPlayer/DataCache/Login/index.html | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Program%20Files/Real/RealPlayer/DataCache/Login/index.html | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Program%20Files/Real/RealPlayer/Firstrun/1.htm | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Program%20Files/Real/RealPlayer/Firstrun/1.htm | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Program%20Files/Real/RealPlayer/Firstrun/context.htm | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/Program%20Files/Real/RealPlayer/Firstrun/context.htm | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/WINDOWS/ODBC.INI | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/WINDOWS/ODBC.INI | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/birds/audio/aggressive_song.wav | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/birds/audio/aggressive_song.wav | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/birds/non%20images/BookList.doc | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/birds/non%20images/BookList.doc | 2005-02-09 19:28:01 GMT | Internet Explorer |
| file/birdwatching.doc | 2005-02-09 19:28:01 GMT | Internet Explorer |

| | | | |
|---|---|---|---|
| file/birdwatching.doc | 2005-02-09 19:28:01 GMT | Internet Explorer | |
| http://www.real.com/intro/index_upsell_manager.html?DC=NSP01D&optin=true&country=gb&language=en-gb8 | 2005-02-09 19:28:01 GMT | Internet Explorer | real.com |
| http://www.real.com/intro/index_upsell_manager.html?DC=NSP01D&optin=true&country=gb&language=en-gb8 | 2005-02-09 19:28:01 GMT | Internet Explorer | real.com |
| https://account.real.com/acct/intro/msg.html?msg=frweur | 2005-02-09 19:28:01 GMT | Internet Explorer | real.com |
| https://account.real.com/acct/intro/msg.html?msg=frweur | 2005-02-09 19:28:01 GMT | Internet Explorer | real.com |
| www.real.com | 2005-02-09 19:28:01 GMT | Internet Explorer | real.com |
| www.real.com | 2005-02-09 19:28:01 GMT | Internet Explorer | real.com |
| file/Documents%20and%20Settings/johndoe/My%20Documents/stuf.doc | 2005-02-10 00:57:49 GMT | Internet Explorer | |

## Appendix 7 – downloads.rdf Data


```
−<RDF:Description RDF:about="C:\DOCUME~1\JOHNDOE\LOCALS~1\TEMP\dawn.ram" NC:Name="dawn.ram" NC:Transferred="1kB of 1kB">
    <NC:URL RDF:resource="http://www.pbs.org/lifeofbirds/songs/dawn.ram"/>
    <NC:File RDF:resource="C:\DOCUME~1\JOHNDOE\LOCALS~1\TEMP\dawn.ram"/>
    <NC:DateStarted NC:parseType="Date">Wed Feb 02 15:12:09 GMT Standard Time 2005 +573635</NC:DateStarted>
    <NC:DateEnded NC:parseType="Date">Wed Feb 02 15:12:09 GMT Standard Time 2005 +593664</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\Desktop\AdbeRdr70_enu_full.exe" NC:Name="AdbeRdr70_enu_full.exe" NC:Transferred="20311kB of 20311kB">
    <NC:URL RDF:resource="http://ardownload.adobe.com/pub/adobe/reader/win/7x/7.0/enu/AdbeRdr70_enu_full.exe"/>
    <NC:File RDF:resource="C:\Documents and Settings\johndoe\Desktop\AdbeRdr70_enu_full.exe"/>
    <NC:DateStarted NC:parseType="Date">Wed Feb 02 16:53:20 GMT Standard Time 2005 +553275</NC:DateStarted>
    <NC:DateEnded NC:parseType="Date">Wed Feb 02 16:54:42 GMT Standard Time 2005 +150606</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_vyoung.jpg" NC:Name="babyscot_vyoung.jpg" NC:Transferred="38kB of 38kB">
    <NC:URL RDF:resource="http://freespace.virgin.net/cobber.budgies/images/babyscot_vyoung.jpg"/>
    <NC:File RDF:resource="C:\Documents and Settings\johndoe\My Documents\My Pictures\babyscot_vyoung.jpg"/>
    <NC:DateStarted NC:parseType="Date">Thu Feb 03 15:00:19 GMT Standard Time 2005 +779785</NC:DateStarted>
    <NC:DateEnded NC:parseType="Date">Thu Feb 03 15:00:19 GMT Standard Time 2005 +819843</NC:DateEnded>
    <NC:DownloadState NC:parseType="Integer">1</NC:DownloadState>
    <NC:ProgressPercent NC:parseType="Integer">100</NC:ProgressPercent>
  </RDF:Description>
−<RDF:Description RDF:about="E:\birds\audio\aggressive_song.wav" NC:Name="aggressive_song.wav" NC:Transferred="716kB of 716kB">
    <NC:URL RDF:resource="http://whyfiles.org/shorties/104chick_sex/images/aggressive_song.wav"/>
    <NC:File RDF:resource="E:\birds\audio\aggressive_song.wav"/>
    <NC:DateStarted NC:parseType="Date">Thu Feb 03 12:22:52 GMT Standard Time 2005 +164782</NC:DateStarted>
    <NC:DateEnded NC:parseType="Date">Thu Feb 03 12:23:00 GMT Standard Time 2005 +466720</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\ostbk2b2.htm" NC:Name="ostbk2b2.htm" NC:Transferred="4kB of 4kB">
    <NC:URL RDF:resource="http://www.cvm.okstate.edu/instruction/kocan/ostrich/ostbk2b2.htm"/>
    <NC:File RDF:resource="C:\Documents and Settings\johndoe\My Documents\ostbk2b2.htm"/>
    <NC:DateStarted NC:parseType="Date">Thu Feb 03 15:02:45 GMT Standard Time 2005 +499320</NC:DateStarted>
    <NC:DateEnded NC:parseType="Date">Thu Feb 03 15:02:45 GMT Standard Time 2005 +579435</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\newbies2.jpg" NC:Name="newbies2.jpg" NC:Transferred="54kB of 54kB">
    <NC:URL RDF:resource="http://people.cornell.edu/pages/sah67/newbies2.jpg"/>
    <NC:File RDF:resource="C:\Documents and Settings\johndoe\My Documents\newbies2.jpg"/>
    <NC:DateStarted NC:parseType="Date">Thu Feb 03 15:05:44 GMT Standard Time 2005 +376532</NC:DateStarted>
    <NC:DateEnded NC:parseType="Date">Thu Feb 03 15:05:44 GMT Standard Time 2005 +456648</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\chicks2.jpg" NC:Name="chicks2.jpg" NC:Transferred="38kB of 38kB">
    <NC:URL RDF:resource="http://people.cornell.edu/pages/sah67/chicks2.jpg"/>
    <NC:File RDF:resource="C:\Documents and Settings\johndoe\My Documents\My Pictures\chicks2.jpg"/>
    <NC:DateStarted NC:parseType="Date">Thu Feb 03 15:05:03 GMT Standard Time 2005 +698040</NC:DateStarted>
    <NC:DateEnded NC:parseType="Date">Thu Feb 03 15:05:03 GMT Standard Time 2005 +748112</NC:DateEnded>
    <NC:DownloadState NC:parseType="Integer">1</NC:DownloadState>
    <NC:ProgressPercent NC:parseType="Integer">100</NC:ProgressPercent>
  </RDF:Description>
</RDF:RDF>
```

```
-<RDF:RDF>
 -<RDF:Description RDF:about="C:\Documents and Settings\johndoe\My Documents\birds.zip" NC:Name="birds.zip" NC:Transferred="1028kB of 1028kB">
    <NC:URL RDF:resource="http://www.traveltex.com/downloads/screensavers/birds.zip"/>
    <NC:File RDF:resource="C:\Documents and Settings\johndoe\My Documents\birds.zip"/>
    <NC:DateStarted NC:parseType="Date">Wed Feb 09 11:28:00 GMT Standard Time 2005 +345172</NC:DateStarted>
    <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>
    <NC:ProgressPercent NC:parseType="Integer">100</NC:ProgressPercent>
  </RDF:Description>
 -<RDF:Description RDF:about="C:\Documents and Settings\johndoe\My Documents\My Pictures\177.jpg" NC:Name="177.jpg" NC:Transferred="9kB of 9kB">
    <NC:URL RDF:resource="http://www.insaneanimals.com/items/177.jpg"/>
    <NC:File RDF:resource="C:\Documents and Settings\johndoe\My Documents\My Pictures\177.jpg"/>
    <NC:DateStarted NC:parseType="Date">Thu Feb 03 15:01:38 GMT Standard Time 2005 +983675</NC:DateStarted>
    <NC:DateEnded NC:parseType="Date">Thu Feb 03 15:01:39 GMT Standard Time 2005 +033747</NC:DateEnded>
    <NC:DownloadState NC:parseType="Integer">1</NC:DownloadState>
    <NC:ProgressPercent NC:parseType="Integer">100</NC:ProgressPercent>
  </RDF:Description>
```


## Appendix 8 – Email Content

### Email #1 Text

To: jdoe@example.com;  From: ben@example.org;

Subject: expensive birds

Date: 2005-02-09 11:08:01 GMT  /Local Folders/Inbox

A young woman was walking past a pet shop and saw an exotic, white cockatoo for sale.  The price was $6000.  She entered the store and asked the clerk why the bird was so expensive.  The clerk told her that the bird spoke 6 different languages. "Does it speak English?" asked the woman. "Of course it does!" said the clerk.

The woman thought about her mother who was multi-lingual, a bit of a recluse and lived all alone.

She decided to purchase the bird and send it to her mother as a companion. She paid for the bird and made arrangements for it to be delivered. The following day, the woman telephoned her mother. "Mama, did you like the cockatoo that I sent you?" "Oh it was delicious!" she replied." "Mama, what do you mean delicious?" "I made soup out of it."

"But mama, that bird spoke six different languages!"

"Oh dear! Why didn't it say something?"

**Email #2 Text**

To: jdoe@example.com; From: ben@example.org;

Subject: good pics

Date: 2005-02-09 11:08:01 GMT /Local Folders/Inbox

Hi thought you'd like these

enjoy

**Email #3 Text**

To: jdoe@example.com; From: ben@example.org;

Subject: some more good ones

Date: 2005-02-09 11:08:01 GMT /Local Folders/Inbox

Thanks for the pics you sent me here are some I really like

**Email #4 Text**

To: jdoe@example.com; From: Bird Fanciers

Subject: How to Identify Birds How to Identify

Date: 2005-02-09 11:08:01 GMT  /Local Folders/Inbox

How to Identify Birds

Are you amazed at how quickly birders can identify birds? Actually, it's just like getting to know your human neighbors. When you move into a new neighborhood everyone is a stranger, but soon you learn to tell people apart as you unconsciously catalog their characteristics. Their habits, shape, styles of walking, and "habitats" become familiar enough that you can recognise each neighbor immediately, even at a distance.

Paying attention to individual differences can help you identify birds, too. You can recognise many birds simply by noting their shapes, even if seen only in silhouette. Other useful characteristics are a bird's posture, size (easiest to judge if you use familiar birds as a size reference), flight pattern and/or head-on flight profile, and the kind of habitat in which the bird was seen.

Start by learning to identify general groups of birds- warblers, flycatchers, hawks, owls, wrens- whose members all share certain similarities. As your observation skills improve, familiarise yourself with the field marks- colored or patterned areas on the bird's body, head, and wings- that help distinguish species.

**Email Images**

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

glfs-storm-birds.jpg

7EYBTELF1KAN.jpg

IMG_3937_filtered.jpg

cute_penguin.jpg

BC7 feeding the birds.jpg

gawall8.jpg

colorful-birds.jpg

# Appendix 9 – Other Browser Files

## 9.1. Bookmarks

| | Source File | URL | Title | Date Created | Program Name | Domain | Data Source |
|---|---|---|---|---|---|---|---|
| 2 | Customize Links.url | http://www.microsoft.com/isapi/redir.dll?prd=ie&pver= | Customize Links.url | 2005-02-03 10:13:14 GMT | Internet Explorer | microsoft.com | johnDoe.dd |
| 3 | Free Hotmail.url | http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=h | Free Hotmail.url | 2005-02-03 10:13:14 GMT | Internet Explorer | microsoft.com | johnDoe.dd |
| 4 | Windows Marketplace.url | http://go.microsoft.com/fwlink/?LinkId=30857&clcid=0 | Windows Marketplace.url | 2005-02-03 10:13:03 GMT | Internet Explorer | microsoft.com | johnDoe.dd |
| 5 | Windows Media.url | http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=w | Windows Media.url | 2005-02-03 10:13:14 GMT | Internet Explorer | microsoft.com | johnDoe.dd |
| 6 | Windows.url | http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=w | Windows.url | 2005-02-03 10:13:14 GMT | Internet Explorer | microsoft.com | johnDoe.dd |
| 7 | MSN.com.url | http://www.microsoft.com/isapi/redir.dll?prd=ie&pver= | MSN.com.url | 2005-02-03 10:13:14 GMT | Internet Explorer | microsoft.com | johnDoe.dd |
| 8 | Radio Station Guide.url | http://www.microsoft.com/isapi/redir.dll?prd=windows | Radio Station Guide.url | 2005-02-03 10:13:14 GMT | Internet Explorer | microsoft.com | johnDoe.dd |
| 9 | Customize Links.url | http://www.microsoft.com/isapi/redir.dll?prd=ie&pver= | Customize Links.url | 2005-02-03 11:23:31 GMT | Internet Explorer | microsoft.com | johnDoe.dd |
| 10 | Free Hotmail.url | http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=h | Free Hotmail.url | 2005-02-03 11:23:31 GMT | Internet Explorer | microsoft.com | johnDoe.dd |
| 11 | Windows Marketplace.url | http://go.microsoft.com/fwlink/?LinkId=30857&clcid=0 | Windows Marketplace.url | 2005-02-03 11:23:22 GMT | Internet Explorer | microsoft.com | johnDoe.dd |
| 12 | Windows Media.url | http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=w | Windows Media.url | 2005-02-03 11:23:31 GMT | Internet Explorer | microsoft.com | johnDoe.dd |
| 13 | Windows.url | http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=w | Windows.url | 2005-02-03 11:23:31 GMT | Internet Explorer | microsoft.com | johnDoe.dd |
| 14 | MSN.com.url | http://www.microsoft.com/isapi/redir.dll?prd=ie&pver= | MSN.com.url | 2005-02-03 11:23:30 GMT | Internet Explorer | microsoft.com | johnDoe.dd |
| 15 | Radio Station Guide.url | http://www.microsoft.com/isapi/redir.dll?prd=windows | Radio Station Guide.url | 2005-02-03 11:23:30 GMT | Internet Explorer | microsoft.com | johnDoe.dd |
| 16 | Customize Links.url | http://www.microsoft.com/isapi/redir.dll?prd=ie&pver= | Customize Links.url | 2005-01-24 15:57:33 GMT | Internet Explorer | microsoft.com | johnDoe.dd |
| 17 | Free Hotmail.url | http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=h | Free Hotmail.url | 2005-01-24 15:57:33 GMT | Internet Explorer | microsoft.com | johnDoe.dd |
| 18 | Windows Marketplace.url | http://go.microsoft.com/fwlink/?LinkId=30857&clcid=0 | Windows Marketplace.url | 2005-01-24 15:57:15 GMT | Internet Explorer | microsoft.com | johnDoe.dd |
| 19 | Windows Media.url | http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=w | Windows Media.url | 2005-01-24 15:57:33 GMT | Internet Explorer | microsoft.com | johnDoe.dd |
| 20 | Windows.url | http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=w | Windows.url | 2005-01-24 15:57:33 GMT | Internet Explorer | microsoft.com | johnDoe.dd |
| 21 | MSN.com.url | http://www.microsoft.com/isapi/redir.dll?prd=ie&pver= | MSN.com.url | 2005-01-24 15:57:33 GMT | Internet Explorer | microsoft.com | johnDoe.dd |
| 22 | Radio Station Guide.url | http://www.microsoft.com/isapi/redir.dll?prd=windows | Radio Station Guide.url | 2005-01-24 15:57:33 GMT | Internet Explorer | microsoft.com | johnDoe.dd |

## 9.2. Cookies

```
.birding.about.com      TRUE    /       FALSE   7107440743      zFS     52280520810500801
.audiencematch.net      TRUE    /       FALSE   1138458167      TID     0mfh7s21101pog
.doubleclick.net        TRUE    /       FALSE   1201962166      id      8000004c8c97582
.atdmt.com      TRUE    /       FALSE   1264982398      AA002   001107354287-989877906/1108563887
.shop.com       TRUE    /       FALSE   2145916801      AMID    319429603
.casalemedia.com        TRUE    /       FALSE   1109927756      CMX2    40842&1107353757%53524%43608
.casalemedia.com        TRUE    /       FALSE   1138094156      CMID    41WW9kU5iDMAAGZqItgAAAAN
www.relmaxtop.com       FALSE   /       FALSE   1422713927      visitor_id      96988879
.amazon.co.uk   TRUE    /       FALSE   2082758401      ubid-acbuk      432-0491950-8565500
www.googleadservices.com        FALSE   /pagead/conversion/1072699989/  FALSE   1109945507      Conversion
```

Figure 41.1. Accessing bird websites

```
MC1
GUID=5b275fd64a540a428f547642b683a212&HASH=d65f&LV=20051&V=3
microsoft.com/
1024
2330023936
29812409
4096274368
29688367
*
```

Figure 41.2. 2721-johndoe@microsoft

### 9.3. b.js

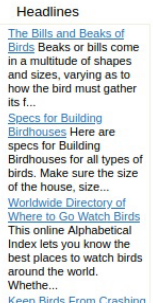
b.js zIBlg=new Array("Birding/Wild Birds","http://birding.about.com/","Birding/Wild Birds","Thu, 27 Jan 2005 11:50:29 -0500"); zIBlgI=new Array("The Bills and Beaks of Birds","http://birding.about.com/b/a/142335.htm","Beaks or bills come in a multitude of shapes and sizes, varying as to how the bird must gather its food as well as to what food he eats. Click here to learn all about them....","Specs for Building Birdhouses","http://birding.about.com/b/a/142333.htm","Here are specs for Building Birdhouses for all types of birds. Make sure the size of the house, size and placement of the entrance hole is for the type of bird you want to attract. Click here....","Worldwide Directory of Where to Go Watch Birds","http://birding.about.com/b/a/142329.htm","This online Alphabetical Index lets you know the best places to watch birds around the world. Whether you want a place nearby or somewhere exotic, this index is what you need. Click here!...","Keep Birds From Crashing into Windows","http://birding.about.com/b/a/141702.htm","Here are some handy tips for keeping wild birds from flying and crashing into windows. Click here for these excellent tips....","Birdie Fast Food for Feeding Backyard Birds","http://birding.about.com/b/a/141699.htm","What the heck do you do when your bird feeders are empty and you have no more seed or suet? Simply fix the birds some birdie fast food, of course! Click here to read about it and get easy recipes!...","Valentine\'s Day Bird Clipart","http://birding.about.com/b/a/139106.htm","Valentine\'s Day is just around the corner! Here are NEW clipart images of Valentine\'s and BIRDS!!New Bird Valentines Day Clipart...","All the Specs for Building Birdhouses","http://birding.about.com/b/a/139105.htm","To attract a particular bird to your backyard, you need to know the type of feeder and food they prefer. Check these lists to determine what type of feeders you need in your yard. Click here for the specs by...","Food and Feeder Preferences for Feeding and Attracting Birds","http://birding.about.com/b/a/139104.htm","To attract a particular bird to your backyard, you need to know the type of feeder and food they prefer. Check these lists to determine what type of feeders you need in your yard. Read about it here....","Build a Winter Roosting Box","http://birding.about.com/b/a/135422.htm","When very cold

weather descends upon your area, how do the birds survive? This roosting box will protect many birds from extreme winter conditions. Here are the plans, directions, and information about this box you can build today....","Thailand Birds","http://birding.about.com/b/a/135420.htm","With the recent disasters in Thailand, obviously the birds of the area are affected. Click here to learn about the birds of Thailand as well as hot spots to view them....","Cold Weather vs Birds","http://birding.about.com/b/a/135418.htm","Cold winter weather complete with snow and ice poses many life-threatening problems for birds. First, their normal natural food sources may be covered up under a layer of ice or snow. How will they eat?? Then cold temperatures outside and...","Sweet Tweets!","http://birding.about.com/b/a/132903.htm","Sugar and spice and everything nice. Making holiday cookies? Why not get the kids together and make some delicious and easy

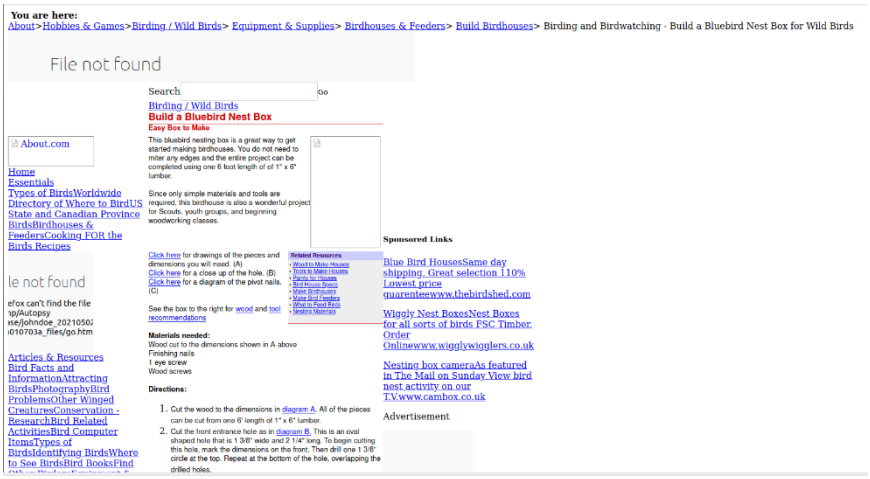
cookies shaped like cardinals, doves, and penguins?...Recipes, patterns and more...","Free Holiday Clipart!","http://birding.about.com/b/a/132902.htm","Holiday Bird Clipart - Winter, Christmas, Hanukkah Index - all free, all for you to use! Get it here!...","Penguins of the World","http://birding.about.com/b/a/132900.htm","Read about the Tuxedoed Birds of the world!...Where do they live, how many species are there, what do they look like and much more! Click here...","Between Heaven and Earth","http://birding.about.com/b/a/129694.htm","What happens when a renowned author and folklore translator and an award-winning pair of children's book illustrators collaborate on a book? An extraordinary flight of fancy, in this case!...read more...","")

### 9.4. Websites


go.htm




b.htm




aa010703a.htm

*ostbk2b2.htm*

CHICKS

Young chicks can be maintained in a variety of suitable facilities. A small portable pen, 12 feet long, 4 feet wide and 2 foot high can be adequate for a number of chicks. The pen is placed on short cut grass and moved daily. Chicks are brought out to the pen after the temperature reaches above 60 F and the sun is shining. Birds can be maintained in this type of facility until the temperature drops or until weather is prohibitive. Include some type of shade and wind break as young birds are sensitive to extreme sun and wind.

Young birds should be brought indoors in the evening and maintained in a heated environment until at least 2 to 3 months of age. Temperature in indoor shelters should be maintained at least 65 F and enough room to allow the birds to exercise should be provided. In areas where weather is more severe, this period may need to be extended.

Do not provide feed at night but available water is acceptable. Feed the young birds as outlined in CARE OF YOUNG BIRDS section, prior to turning them out in the morning.

---

JUVENILES

Juvenile birds between 3 and 10 months of age can be maintained in a similar, but larger facility as young birds. For convenience, access to the indoor facility should be available directly from the outdoor pens. However, shelter is not needed except in extremely cold areas. The amount of space per bird, for both indoor and outdoor facilities should be increased for this age bird as compared to that available for younger chicks. Outdoor pens can be of any type of substrate but ground cover such as grass, clover, or alfalfa is ideal. Grass should be kept at a closely mowed level, especially when grass begins to dry out or turn to seed, as impactions are more common at this time. Daily mowing may be necessary during some periods of the year.

---

ADULTS

Pens and facilities for adults vary considerably. Most ranchers maintain adult pairs or trios in facilities that range from five thousand square feet to an acre or more. In general, the more room that can be provided, the better the situation. Common fences and line of sight access to neighboring pairs is often desirable but may not be practicable with overly aggressive males.

Housing or shade is usually provided although not always utilised. If birds are accustomed to being fed and watered in a shed they will be more easily confined when necessary and may build the nest and lay indoors. Alley-ways for movement of birds from pen to pen, access for haling, and provisions for confinement for veterinary care should be considered at the time of construction. Although suprising, most ratites do not require indoor shelter once over 6 months of age and often refuse to use such structures, independent of weather.

Fencing is dependent on personal preference and economics. Chain link is good but may result in problems related to leg and foot injures and is not easily climbed if escape from the pen by egg gatherers is necessary. Tubular "cattle" type fence is suitable and offer some benefits and others types of woven wire fencing are routinely used.

Many ranchers are now utilising group pens consisting of several males and numerous females in larger acreage. This appears to provide some benefits and is more nearly similar to a natural situation. Early results indicate that increased fertility, more egg numbers, and extended laying periods can be expected in this type of set up. Several acres of enclosed pasture are needed for this type of operation.

Difficulties with a group breeding situation include the inability to determine exactly the resultant chicks parentage.

Ostrich Book

# Appendix 10 – birdpics.gpg Examination Results

## 10.1. Recovered Image

## 10.2. The other image files

| Name | Size | Type | Modified |
|---|---|---|---|
| E:\birds\birdpics\WhiteFacedH... | 181.3 kB | JPEG image | 02 February... |
| E:\birds\birdpics\WhiteFronted... | 188.9 kB | JPEG image | 02 February... |
| E:\birds\birdpics\WhiteThroate... | 247.0 kB | JPEG image | 02 February... |
| E:\birds\birdpics\WhoopingCra... | 305.5 kB | JPEG image | 02 February... |
| E:\birds\birdpics\yellow-wag-c... | 61.6 kB | JPEG image | 02 February... |

# Appendix 11 – Fred Results from NTUSER.DAT

adobe v.20200522

(NTUSER.DAT) Gets user's Adobe app cRecentFiles values

Could not access Software\Adobe\Adobe Acrobat\\AVGeneral\cRecentFiles

Software\Adobe\Acrobat Reader\7.0\AVGeneral\cRecentFiles

Key name,file name,sDate,uFileSize,uPageCount

c1,/E/birds/non images/BirdingGuide.pdf ,,,

---

allowedenum v.20200511

(NTUSER.DAT, Software) Extracts AllowedEnumeration values to determine hidden special folders

Software\Microsoft\Windows\CurrentVersion\Explorer\AllowedEnumeration not found.

Microsoft\Windows\CurrentVersion\Explorer\AllowedEnumeration not found.

---

appassoc v.20200515

- Gets contents of user's ApplicationAssociationToasts key

Software\Microsoft\Windows\CurrentVersion\ApplicationAssociationToasts not found.

---

appcompatflags v.20200525

(NTUSER.DAT, Software) Extracts AppCompatFlags for Windows.

---

appkeys v.20200517

(NTUSER.DAT, Software) Extracts AppKeys entries.

---

applets v.20200525

(NTUSER.DAT) Gets contents of user's Applets key

Applets

Software\Microsoft\Windows\CurrentVersion\Applets

LastWrite Time 2005-01-24 15:57:40Z

Software\Microsoft\Windows\CurrentVersion\Applets\Paint\Recent File List not found.

---

apppaths v.20200511

(NTUSER.DAT,Software) Gets content of App Paths subkeys

---

Software\Microsoft\IntelliPoint\AppSpecific not found.

---

appx v.20200427

(NTUSER.DAT, USRCLASS.DAT) Checks for persistence via Universal Windows Platform Apps

---

arpcache v.20200515

(NTUSER.DAT) Retrieves CurrentVersion\App Management\ARPCache entries

Software\Microsoft\Windows\CurrentVersion\App Management\ARPCache not found.

---

attachmgr v.20200525

(NTUSER.DAT) Checks user's keys that manage the Attachment Manager functionality

Software\Microsoft\Windows\CurrentVersion\Policies\Associations not found.

Software\Microsoft\Windows\CurrentVersion\Policies\Attachments not found.

---

cached v.20200525

(NTUSER.DAT) Gets cached Shell Extensions from NTUSER.DAT hive

Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached not found.

---

cmdproc v.20200515

(NTUSER.DAT) Autostart - get Command Processor\AutoRun value from NTUSER.DAT hive

Software\Microsoft\Command Processor

LastWrite Time 2005-01-24 15:56:58Z

AutoRun value not found.

---

comdlg32 v.20200517

Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32

LastWrite Time 2005-02-02 14:18:10Z

LastVisitedMRU

LastWrite: 2005-02-09 11:28:00Z

MRUList = acb

a -> EXE: firefox.exe

-> Last Dir: C:\Documents and Settings\johndoe\My Documents

c -> EXE: WinPT.exe

-> Last Dir: C:\Documents and Settings\johndoe\My Documents

b -> EXE: notepad.exe

-> Last Dir: C:\Documents and Settings\johndoe\My Documents

OpenSaveMRU

LastWrite: 2005-02-09 11:28:00Z

OpenSaveMRU\OpenSaveMRU

LastWrite time: 2005-02-09 11:28:00Z

MRUList = a

a -> C:\Documents and Settings\johndoe\My Documents\birdpics

OpenSaveMRU*

LastWrite time: 2005-02-09 11:28:00Z

MRUList = jihgfedcba

j -> C:\Documents and Settings\johndoe\My Documents\birds.zip

i -> C:\Documents and Settings\bob\My Documents\My Music\ready2fledge.jpg

h -> C:\Documents and Settings\johndoe\My Documents\newbies2.jpg

g -> C:\Documents and Settings\johndoe\My Documents\My Pictures\chicks2.jpg

f -> C:\Documents and Settings\johndoe\Desktop\birdtrans2.jpg

e -> C:\Documents and Settings\johndoe\My Documents\ostbk2b2.htm

d -> C:\Documents and Settings\johndoe\My Documents\My Pictures\177.jpg

c -> C:\Documents and Settings\johndoe\My Documents\My Pictures\babyscot_2weeks1.jpg

b -> C:\Documents and Settings\johndoe\My Documents\My Pictures\babyscot_vyoung.jpg

a -> E:\birds\audio\aggressive_song.wav

OpenSaveMRU\exe

LastWrite time: 2005-02-02 16:53:20Z

MRUList = a

a -> C:\Documents and Settings\johndoe\Desktop\AdbeRdr70_enu_full.exe

OpenSaveMRU\htm

LastWrite time: 2005-02-03 15:02:45Z

MRUList = ba

b -> C:\Documents and Settings\johndoe\My Documents\ostbk2b2.htm

a -> C:\Documents and Settings\johndoe\My Documents\aa010703a.htm

OpenSaveMRU\jpg

LastWrite time: 2005-02-03 15:06:42Z

MRUList = bajihgfedc

b -> C:\Documents and Settings\bob\My Documents\My Music\ready2fledge.jpg

a -> C:\Documents and Settings\johndoe\My Documents\newbies2.jpg

j -> C:\Documents and Settings\johndoe\My Documents\My Pictures\chicks2.jpg

i -> C:\Documents and Settings\johndoe\Desktop\birdtrans2.jpg

h -> C:\Documents and Settings\johndoe\My Documents\My Pictures\177.jpg

g -> C:\Documents and Settings\johndoe\My Documents\My Pictures\babyscot_2weeks1.jpg

f -> C:\Documents and Settings\johndoe\My Documents\My Pictures\babyscot_vyoung.jpg

e -> C:\Documents and Settings\johndoe\My Documents\My Pictures\40m.jpg

d -> C:\Documents and Settings\johndoe\My Documents\My Pictures\wbpremium_s.jpg

c -> C:\Documents and Settings\johndoe\My Documents\My Pictures\7107298.jpg

OpenSaveMRU\ram

LastWrite time: 2005-02-02 15:11:51Z

MRUList = a

a -> C:\Documents and Settings\johndoe\My Documents\kakapo.ram

OpenSaveMRU\txt

LastWrite time: 2005-02-02 14:29:30Z

MRUList = a

a -> C:\Documents and Settings\johndoe\My Documents\nestboxtips.txt

OpenSaveMRU\wav

LastWrite time: 2005-02-03 12:22:51Z

MRUList = a

a -> E:\birds\audio\aggressive_song.wav

OpenSaveMRU\zip

LastWrite time: 2005-02-09 11:28:00Z

MRUList = a

a -> C:\Documents and Settings\johndoe\My Documents\birds.zip

---

compdesc v.20200511

(NTUSER.DAT) Gets contents of user's ComputerDescriptions key

ComputerDescriptions

Software\Microsoft\Windows\CurrentVersion\Explorer\ComputerDescriptions

LastWrite Time 2005-01-24 16:10:00Z

pcsrcfs Samba 2.2.8a

PC-FABIO

ARNOTT Samba 3.0.10-Debian

DEWAR Samba 2.2.8a

GUESTSHARES Samba 2.2.8a

KELVIN Samba 2.2.8a

LAP-DAVIDM Staff XP PC

LAP-EFOCS3

LAP-FABIO XP SP2 LAPTOP

PC-AN

PC-CAROLANN

PC-DCE Staff XP PC

PC-DOUG

PC-EFOCS2

PC-EVELIN Staff XP PC

PC-FABIOC Fabio's new Sony

---

DDO v.20140414

(NTUSER.DAT) Gets user's DeviceDisplayObjects key contents

Software\Microsoft\Windows NT\CurrentVersion\DeviceDisplayObjects not found.

---

disablemru v.20190924

(NTUSER.DAT, Software) Checks settings disabling user's MRUs

---

environment v.20200512

(System, NTUSER.DAT) Get environment vars from NTUSER.DAT & System hives

Environment

LastWrite Time: 2005-01-24 15:56:58Z

TEMP %USERPROFILE%\Local Settings\Temp

TMP %USERPROFILE%\Local Settings\Temp

---

featureusage v.20200511

(NTUSER.DAT) Extracts user's FeatureUsage data.

Software\Microsoft\Windows\CurrentVersion\Explorer\FeatureUsage not found.

---

[-] SOFTWARE\HeidiSQL not found.

[-] SOFTWARE\HeidiSQL\Servers not found.

---

identities v.20200525

(NTUSER.DAT) Extracts values from Identities key; NTUSER.DAT

Identities

LastWrite Time 2005-01-24 15:57:13Z

| | |
|---|---|
| Identity Ordinal | 1 |
| Migrated5 | 1 |
| Last Username | Main Identity |
| Last User ID | {9F5A55BB-7A6C-41C4-9559-B06794935BE1} |
| Identity Login | 622675 |
| Default User ID | {9F5A55BB-7A6C-41C4-9559-B06794935BE1} |

---

injectdll64 v.20200427

(NTUSER.DAT, Software) Retrieve values set to weaken Chrome security

Software\Policies\Google\Chrome\CertificateTransparencyEnforcementDisabledForUrls not found.

Policies\Google\Chrome\CertificateTransparencyEnforcementDisabledForUrls not found.

---

jumplistdata v.20200517

Gets contents of user's JumpListData key

Software\Microsoft\Windows\CurrentVersion\Search\JumpListData not found.

---

knowndev v.20200515

(NTUSER.DAT) Gets user's KnownDevices key contents

Software\Microsoft\Windows\CurrentVersion\Explorer\AutoplayHandlers\KnownDevices not found.

---

listsoft v.20200517

(NTUSER.DAT) Lists contents of user's Software key

List the contents of the Software key in the NTUSER.DAT hive

file, in order by LastWrite time.

2005-02-02 17:03:31Z Microsoft

2005-02-02 16:59:47Z Adobe

2005-02-02 16:32:22Z WinPT

2005-02-02 16:32:07Z GNU

2005-02-02 15:04:41Z RealNetworks

2005-01-25 10:50:39Z ODBC

2005-01-24 16:47:05Z Clients

2005-01-24 16:31:47Z Mozilla

2005-01-24 15:56:58Z Intel

2005-01-24 15:56:58Z Netscape

2005-01-24 15:56:58Z Policies

---

load v.20200517

(NTUSER.DAT) Gets load and run values from user hive

load

Software\Microsoft\Windows NT\CurrentVersion\Windows

LastWrite Time 2005-01-24 15:56:58Z

load =

run value not found.

---

logonstats v.20200517

Gets contents of user's LogonStats key

Software\Microsoft\Windows\CurrentVersion\Explorer\LogonStats not found.

---

lxss v.20200511

(NTUSER.DAT) Gets WSL config.

Software\Microsoft\Windows\CurrentVersion\Lxss not found.

---

mixer v.20200517

(NTUSER.DAT) Checks user's audio mixer settings

---

mmc v.20200517

(NTUSER.DAT) Get contents of user's MMC\Recent File List key

MMC - Recent File List

Software\Microsoft\Microsoft Management Console\Recent File List

LastWrite Time 2005-02-09 11:20:04Z

  File1 -> C:\WINDOWS\system32\eventvwr.msc

  File2 -> C:\WINDOWS\system32\compmgmt.msc

---

mmo v.20200517

(NTUSER.DAT) Checks NTUSER for Multimedia\Other values [malware]

Software\Microsoft\Multimedia\Other not found.

Software\Microsoft\CTF\LangBarAddIn not found.

---

mndmru v.20200517

(NTUSER.DAT) Get contents of user's Map Network Drive MRU

Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU not found.

---

mp2 v.20200526

(NTUSER.DAT) Gets user's MountPoints2 key contents

MountPoints2

Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2

LastWrite Time 2005-02-09 11:03:40Z

Remote Drives:

Volumes:

2005-02-09 16:50:51Z

{44d36d3b-7525-11d9-ab5a-0048545652e0}

2005-02-03 11:36:05Z

{44d36d43-7525-11d9-ab5a-0048545652e0}

2005-02-02 15:11:00Z

{30bf5ac1-6e1f-11d9-a7bd-806d6172696f}

2005-01-24 15:57:34Z

{30bf5ac0-6e1f-11d9-a7bd-806d6172696f}

{30bf5ac3-6e1f-11d9-a7bd-806d6172696f}

Drives:

2005-02-02 16:30:03Z - E

2005-01-24 15:56:58Z - A,C,D

Unique MAC Addresses:

80:6D:61:72:69:6F

00:48:54:56:52:E0

Analysis Tip: Correlate the Volume entries to those found in the MountedDevices entries that begin with "\??\Volume".

---

mpmru v.20200517

(NTUSER.DAT) Gets user's Media Player RecentFileList values

Software\Microsoft\MediaPlayer\Player\RecentFileList not found.

---

msoffice v.20200518

---

muicache v.20200525

(NTUSER.DAT,USRCLASS.DAT) Gets EXEs from user's MUICache key

Software\Microsoft\Windows\ShellNoRoam\MUICache

LastWrite Time 2005-02-09 17:09:26Z

C:\Program Files\Real\RealPlayer\realplay.exe (RealPlayer)

C:\Program Files\Windows Media Player\wmplayer.exe (Windows Media Player)

C:\PROGRA~1\MOZILL~1\FIREFOX.EXE (Firefox)

C:\Program Files\Adobe\Acrobat 7.0\Reader\AcroRd32.exe (Adobe Reader 7.0)

C:\WINDOWS\system32\shimgvw.dll (Windows Picture and Fax Viewer)

C:\WINDOWS\system32\mspaint.exe (Paint)

C:\WINDOWS\Explorer.EXE (Windows Explorer)

Local Settings\Software\Microsoft\Windows\Shell\MUICache not found.

---

nation v.20200517

(ntuser.dat) Gets region information from HKCU

Nation Information Check

Control Panel\International\Geo

LastWrite time: 2005-01-24 15:56:58Z

The Region value is : 242

The Country Is: United Kingdom

For more information please visit the link below:

https://msdn.microsoft.com/en-us/library/aa723531.aspx

---

oisc v.20091125

(NTUSER.DAT) Gets contents of user's Office Internet Server Cache

Office Version:

Software\Microsoft\Office\\Common\Internet\Server Cache not found.

---

onedrive v.20200515

(NTUSER.DAT) Gets contents of user's OneDrive key

Software\Microsoft\OneDrive not found.

---

OSVersion

Software\Microsoft

LastWrite Time 2005-02-02 17:03:31Z

OSVersion value not found.

---

outlookhomepage v.20201002

(NTUSER.DAT, Software) Retrieve values set to attack Outlook WebView Homepage

Looking for webview homepage modifications. If this value is pointing

to a URL outside the corporate domain it may be a malicious site.

Looking for key values associated with security.

If you see:

[Example]  EnableRoamingFolderHomepages : 1

[Example]  NonDefaultStoreScript : 1

[Example]  EnableUnsafeClientMailRules : 1

You may have a security vulnerability that allows attackers to hijack the URL

Software\Microsoft\Office\11.0\Outlook\Security

LastWrite Time 2005-01-25 10:49:37Z

Level : 3

UseCRLChasing : 1

---

pendinggpos v.20200427

NTUSER.DAT - Gets contents of user's PendingGPOs key

Software\Microsoft\IEAK\GroupPolicy\PendingGPOs not found.

---

profiler v.20200525

(NTUSER.DAT, System) Environment profiler information

Environment

LastWrite Time 2005-01-24 15:56:58Z

TEMP -> %USERPROFILE%\Local Settings\Temp

TMP -> %USERPROFILE%\Local Settings\Temp

---

pslogging v.20200515

(NTUSER.DAT, Software) Extracts PowerShell logging settings

Software\Policies\Microsoft\Windows\PowerShell not found.

Policies\Microsoft\Windows\PowerShell not found.

---

---

putty v.20200515

(NTUSER.DAT) Extracts the saved SshHostKeys for PuTTY.

Software\SimonTatham\PuTTY\SshHostKeys not found.

---

recentapps v.20200515

- Gets contents of user's RecentApps key

Software\Microsoft\Windows\CurrentVersion\Search\RecentApps not found.

---

recentdocs v.20200427

(NTUSER.DAT) Gets contents of user's RecentDocs key

RecentDocs

**All values printed in MRUList\MRUListEx order.

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

LastWrite Time: 2005-02-09 17:06:28Z

38 = New Volume (F:)

11 = AlmondMarshGreatBlueHeronStalling.jpg

37 = MSN

18 = aggressive_song.wav

36 = stuf.doc

35 = birds.zip

34 = WINDOWS

33 = ODBC.INI

14 = non images

13 = BirdingGuide.pdf

32 = BookList.doc

21 = Local Disk (C:)

5 = birdwatching.doc

31 = My Music

3 = ready2fledge.jpg

2 = newbies2.jpg

1 = My Pictures

0 = chicks2.jpg

30 = birdtrans2.jpg

29 = ostbk2b2.htm

28 = 177.jpg

27 = babyscot_2weeks1.jpg

26 = babyscot_vyoung.jpg

25 = birds

24 = Killdeer.jpg

23 = Sample Music

22 = Doc1.doc

20 = EvanstonWoodpecker.jpg

19 = audio

17 = bookmarks.html

15 = cookies.txt

12 = kakapo.ram

10 = Q3 Thread (Statechart).gif

9 = Prac4

8 = Prac4.gif

6 = nestboxtips.txt

4 = aa010703a.htm

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.doc

LastWrite Time 2005-02-09 16:57:49Z

MRUListEx = 1,3,2,0

1 = stuf.doc

3 = BookList.doc

2 = birdwatching.doc

0 = Doc1.doc

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.gif

LastWrite Time 2005-02-02 15:10:48Z

MRUListEx = 1,0

1 = Q3 Thread (Statechart).gif

0 = Prac4.gif

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.htm

LastWrite Time 2005-02-03 15:02:45Z

MRUListEx = 1,0

1 = ostbk2b2.htm

0 = aa010703a.htm

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.html

LastWrite Time 2005-02-03 12:20:20Z

MRUListEx = 0

0 = bookmarks.html

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.INI

LastWrite Time 2005-02-03 15:54:06Z

MRUListEx = 0

0 = ODBC.INI

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.jpg

LastWrite Time 2005-02-09 17:06:28Z

MRUListEx = 4,3,2,1,0,9,8,7,6,5

4 = AlmondMarshGreatBlueHeronStalling.jpg

3 = ready2fledge.jpg

2 = newbies2.jpg

1 = chicks2.jpg

0 = birdtrans2.jpg

9 = 177.jpg

8 = babyscot_2weeks1.jpg

7 = babyscot_vyoung.jpg

6 = Killdeer.jpg

5 = EvanstonWoodpecker.jpg

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.pdf

LastWrite Time 2005-02-03 15:52:01Z

MRUListEx = 0

0 = BirdingGuide.pdf

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.ram

LastWrite Time 2005-02-02 15:11:51Z

MRUListEx = 0

0 = kakapo.ram

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt

LastWrite Time 2005-02-03 12:19:07Z

MRUListEx = 1,0

1 = cookies.txt

0 = nestboxtips.txt

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.wav

LastWrite Time 2005-02-09 17:00:50Z

MRUListEx = 0

0 = aggressive_song.wav

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.zip

LastWrite Time 2005-02-09 11:28:00Z

MRUListEx = 0

0 = birds.zip

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder

LastWrite Time 2005-02-09 17:06:28Z

MRUListEx = 4,2,3,1,6,9,0,8,7,5

4 = New Volume (F:)

2 = MSN

3 = WINDOWS

1 = non images

6 = Local Disk (C:)

9 = My Music

0 = My Pictures

8 = birds

7 = Sample Music

5 = audio

---

run v.20200511

(Software, NTUSER.DAT) [Autostart] Get autostart key contents from Software hive

Software\Microsoft\Windows\CurrentVersion\Run

LastWrite Time 2005-01-24 15:56:58Z

Software\Microsoft\Windows\CurrentVersion\Run has no values.

Software\Microsoft\Windows\CurrentVersion\Run has no subkeys.

Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run not found.

Software\Microsoft\Windows\CurrentVersion\RunOnce not found.

Software\Microsoft\Windows\CurrentVersion\RunServices not found.

Software\Microsoft\Windows\CurrentVersion\RunServicesOnce not found.

Software\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run not found.

Software\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\RunOnce not found.

Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not found.

Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not found.

Software\Microsoft\Windows\CurrentVersion\StartupApproved\Run not found.

Software\Microsoft\Windows\CurrentVersion\StartupApproved\Run32 not found.

Software\Microsoft\Windows\CurrentVersion\StartupApproved\StartupFolder not found.

---

runmru v.20200525

(NTUSER.DAT) Gets contents of user's RunMRU key

RunMru

Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

LastWrite Time 2005-02-02 14:29:06Z

MRUList = a

a   notepad\1

---

runvirtual v.20200427

(NTUSER.DAT, Software) Gets RunVirtual entries

---

searchscopes v.20200517

- Gets contents of user's SearchScopes key

Software\Microsoft\Internet Explorer\SearchScopes not found.

---

sevenzip v.20210329

- Gets records of histories from 7-Zip keys

Software\7-Zip not found.

Software\Wow6432Node\7-Zip not found.

---

shc v.20200427

(NTUSER.DAT) Gets SHC entries from user hive

Software\Microsoft\Windows\CurrentVersion\UFH\SHC not found.

---

shellfolders v.20200515

Gets user's shell folders values

Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders

LastWrite Time 2005-02-02 16:59:48Z

StartUp folder : C:\Documents and Settings\johndoe\Start Menu\Programs\Startup

Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders

LastWrite Time 2005-01-28 16:51:42Z

StartUp folder : %USERPROFILE%\Start Menu\Programs\Startup

---

speech v.20200427

(NTUSER.DAT) Get values from user's Speech key

Software\Microsoft\Speech not found.

---

Software\SysInternals not found.

---

Launching tsclient v.20200518

(NTUSER.DAT) Displays contents of user's Terminal Server Client\Default key

Software\Microsoft\Terminal Server Client\Default not found.

Software\Microsoft\Terminal Server Client\Servers not found.

---

typedpaths v.20200526

(NTUSER.DAT) Gets contents of user's typedpaths key

Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths not found.

---

typedurls v.20200526

(NTUSER.DAT) Returns contents of user's TypedURLs key.

TypedURLs

Software\Microsoft\Internet Explorer\TypedURLs

LastWrite Time 2005-02-09 13:40:14Z

url1 -> e:

url2 -> e:\

---

typedurlstime v.20200526

(NTUSER.DAT) Returns contents of user's TypedURLsTime key.

Software\Microsoft\Internet Explorer\TypedURLsTime not found.

---

uninstall v.20200525

(Software, NTUSER.DAT) Gets contents of Uninstall keys from Software, NTUSER.DAT hives

Uninstall

---

UserAssist

Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

LastWrite Time 2005-01-24 15:57:05Z

{5E6AB780-7743-11CF-A12B-00AA004AE837}

2005-02-09 11:28:58Z

UEME_UITOOLBAR (28)

UEME_UITOOLBAR:0x1,130 (19)

2005-02-03 16:34:56Z

UEME_UITOOLBAR:0x1,123 (2)

2005-02-03 12:11:09Z

UEME_UITOOLBAR:0x1,133 (3)

2005-02-03 12:09:40Z

UEME_UITOOLBAR:0x4,7031 (2)

2005-01-24 16:07:37Z

UEME_UITOOLBAR:0x1,120 (2)

Value names with no time stamps:

HRZR_PGYPHNPbhag:pgbe

{75048700-EF1F-11D0-9888-006097DEACF9}

2005-02-09 17:04:04Z

UEME_UISCUT (8)

UEME_RUNPATH (33)

UEME_RUNPATH:::{645FF040-5081-101B-9F08-00AA002F954E} (3)

2005-02-09 17:00:50Z

UEME_RUNPATH:C:\Program Files\Real\RealPlayer\RealPlay.exe (1)

2005-02-09 16:51:54Z

UEME_RUNPIDL (13)

UEME_RUNPIDL:%csidl2%\Microsoft Office\Microsoft Office Word 2003.lnk (2)

UEME_RUNPATH:C:\Program Files\Microsoft Office\OFFICE11\WINWORD.EXE (4)

UEME_RUNPATH:{90110409-6000-11D3-8CFE-0150048383C9} (2)

2005-02-09 16:49:17Z

UEME_RUNPIDL:C:\Documents and Settings\All Users\Desktop\Mozilla Firefox.lnk (4)

UEME_RUNPIDL:C:\Documents and Settings\All Users\Desktop (4)

2005-02-09 11:29:35Z

UEME_RUNCPL (4)

UEME_RUNCPL:desk.cpl (2)

2005-02-09 11:26:11Z

UEME_RUNPATH:C:\Program Files\Mozilla Firefox\firefox.exe (3)

2005-02-09 11:26:10Z

UEME_RUNPATH:Mozilla Firefox.lnk (3)

2005-02-09 11:19:35Z

UEME_RUNPATH:C:\WINDOWS\system32\mmc.exe (3)

2005-02-09 11:04:35Z

UEME_RUNPATH:C:\PROGRA~1\MOZILL~2\THUNDE~1.EXE (1)

UEME_RUNPIDL:::{2559A1F5-21D7-11D4-BDAF-00C04F60B9F0} (1)

2005-02-03 15:54:06Z

UEME_RUNPATH:C:\WINDOWS\system32\notepad.exe (4)

2005-02-03 15:52:00Z

UEME_RUNPATH:C:\Program Files\Adobe\Acrobat 7.0\Reader\AcroRd32.exe (2)

2005-02-03 14:45:16Z

UEME_RUNPATH:C:\WINDOWS\mui\FantailFrontView.exe (1)

2005-02-03 14:16:31Z

UEME_RUNPIDL:%csidl2%\Microsoft Office (1)

2005-02-03 12:20:41Z

UEME_RUNPATH:C:\PROGRA~1\MOZILL~1\FIREFOX.EXE (1)

UEME_RUNPIDL:::{2559A1F4-21D7-11D4-BDAF-00C04F60B9F0} (1)

2005-02-03 12:19:59Z

UEME_RUNPATH:C:\Program Files\Microsoft Office\OFFICE11\msohtmed.exe (1)

2005-02-02 16:55:49Z

UEME_RUNPATH:C:\Documents and Settings\johndoe\Desktop\AdbeRdr70_enu_full.exe (1)

2005-02-02 16:53:33Z

UEME_RUNPATH:C:\WINDOWS\system32\rundll32.exe (2)

2005-02-02 16:31:07Z

UEME_RUNPATH:E:\winpt-install-1.0rc2.exe (1)

2005-02-02 15:08:22Z

UEME_RUNCPL:"C:\WINDOWS\system32\nusrmgr.cpl",User Accounts (2)

Value names with no time stamps:

HRZR_PGYPHNPbhag:pgbe

---

wc_shares v.20200515

- Gets contents of user's WorkgroupCrawler/Shares subkeys

Software\Microsoft\Windows\CurrentVersion\Explorer\WorkgroupCrawler\Shares not found.

---

winrar v.20200526

(NTUSER.DAT) Get WinRAR\ArcHistory entries

Software\WinRAR\ArcHistory not found.

---

winscp v.20201227

(NTUSER.DAT) Gets user's WinSCP 2 data

Software\Martin Prikryl\WinSCP 2 not found.

---

winzip v.20200526

(NTUSER.DAT) Get WinZip extract and filemenu values

Software\Nico Mak Computing\WinZip not found.

---

wordwheelquery v.20200823

(NTUSER.DAT) Gets contents of user's WordWheelQuery key

Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery not found.

---

# Appendix 12 – SAM report

**User accounts**

| Name | RID | Full name | Last login | Last PW change | Last failed login | Account expiry | Total logins | Failed logins | Flags | Password hint | Home drive and dir | Logon script path | Profile path | Comment |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Administrator | 500 (0x000001f4) | | n/a | 2005/01/24 16:31:26 | n/a | 1975/01/22 22:55:33 | 0 | 0 | NoPwExpiry | | | | | Built-in account for administering the computer/domain |
| Guest | 501 (0x000001f5) | | n/a | n/a | n/a | 1975/01/22 22:55:33 | 0 | 0 | NoPwExpiry Disabled PwNotReq | | | | | Built-in account for guest access to the computer/domain |
| HelpAssistant | 1000 (0x0003e8) | Remote Desktop Help Assistant Account | n/a | 2005/01/24 15:37:21 | n/a | n/a | 0 | 0 | NoPwExpiry Disabled | | | | | Account for Providing Remote Assistance |
| SUPPORT_388945a0 | 1002 (0x0003ea) | CN=Microsoft Corporation,L=Redmond,S=Washington,C=US | n/a | 2005/01/24 15:42:04 | n/a | n/a | 0 | 0 | NoPwExpiry Disabled | | | | | This is a vendor's account for the Help and Support Service |
| bob | 1005 (0x0003ed) | bob | 2005/02/03 10:12:34 | 2005/02/02 15:08:54 | n/a | 1975/01/22 22:55:33 | 1 | 0 | NoPwExpiry | | | | | |
| jane | 1004 (0x0003ec) | jane | 2005/02/03 11:23:04 | 2005/02/02 12:37:25 | 2005/02/02 15:08:27 | 1975/01/22 22:55:33 | 1 | 0 | NoPwExpiry | | | | | |
| johndoe | 1003 (0x0003eb) | | 2005/02/09 16:49:18 | 2005/01/24 16:36:30 | 2005/02/02 15:08:27 | 1975/01/22 22:55:33 | 21 | 0 | NoPwExpiry | | | | | |

# Appendix 13 – Other Evidence Files

## Doc1.doc image

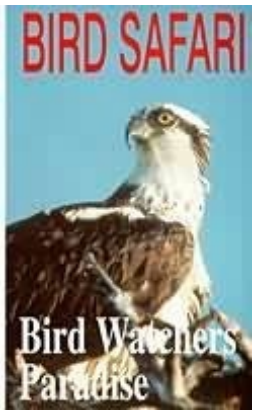
FantailFrontView.jpg

**Other images of birds**

ready2fledge.jpg

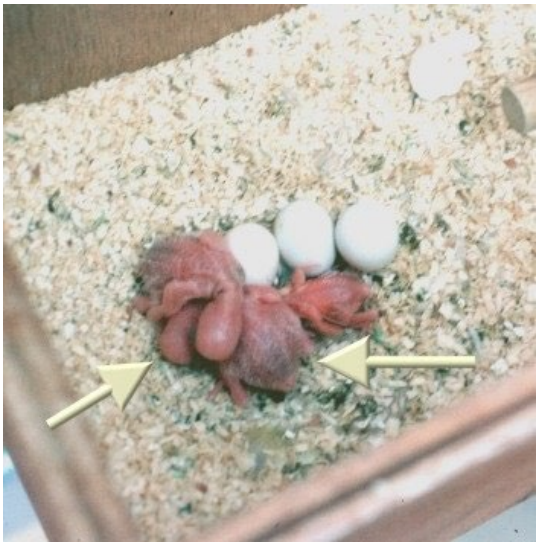
birdtrans2.jpg


177.jpg




7107298.jpg

babyscot_2weeks.jpg



babyscot_vyoung.jpg

chicks2.jpg

BaldEagle7oClock.jpg

GreatEgretOverflyingRoseateSpoonbills.jpg

AlmondMarshGreatBlueHeronStalling.jpg

AmericanAvocetWinterPlumage.jpg

AmericanWhitePelicansCircling.jpg

BellbirdJumpingOffBranch.jpg

BlackNeckedStiltsFromBehind.jpg

BlackSwan.jpg

BlackVultureSunningOnPost.jpg

snow_geese.jpg


blue_bird2.jpg


brd_Ornithologist_TWG.jpg

BarnOwl.jpg

GreatBlueHeronWithFish.jpg

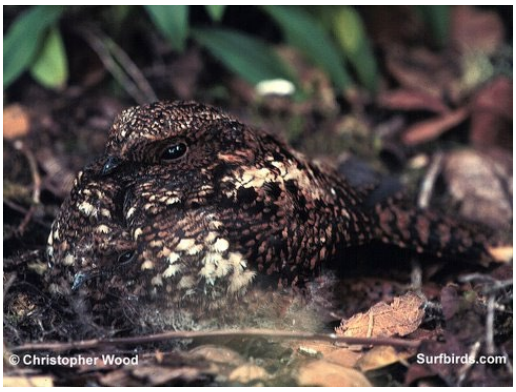
GreatEgretInVoloBog.jpg

GreenHeronCloseup.jpg

GreenHeronOnChicagoLakeshore.jpg

ImmatureSnowyEgretTakingOff.jpg


june03screen.jpg




junescreen01.jpg

KeaAndMountain.jpg


Df1.jpg

tn_duck_3.jpg

newbies2.jpg

KeaAtTopOfMacKinnonPass0930.jpg

KeaEatingRentalCar.jpg

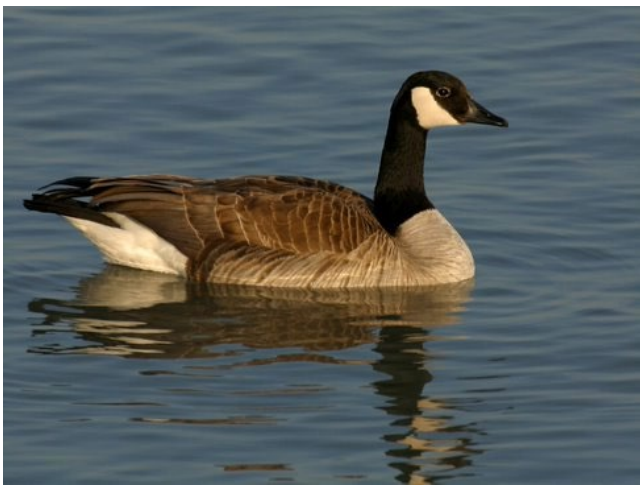
KeaRetrievingBakedBeanCanFromTarn.jpg

CrouchingKokako.jpg


brd_WoodDuck.jpg

Brolga.jpg

BrushTurkeyPerching.jpg



CanadaGoose.jpg

CanadaGooseWashing.jpg

ChestnutMandibledToucan.jpg

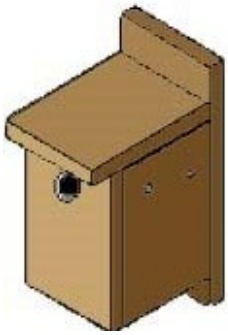

40m.jpg

frankbeecostume_1827_96360352.jpg

frankbeecostume_1827_34457581.jpg

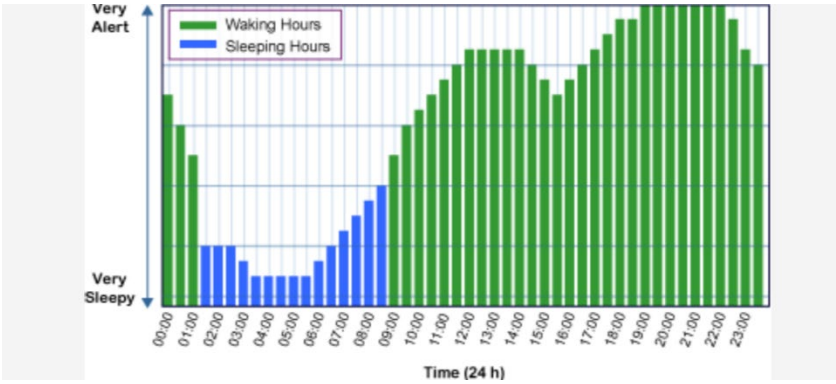
frankbeecostume_1827_84985892.jpg

birding.gif



bluebirdhousepic.jpg

Firefox Wallpaper.bmp




birdSchedule.jpg


business_entrepreneurs_mostadmiredpoll1_leaderboard.jpg

## Text files

*Guide.doc*

**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 group, for a short time or for the balance of the day, be certain you inform the leader.

It is in your interest to stay close to the leader and the more experienced members of the group so that you can rely on their knowledge and bird-finding skills.

Staying close applies to car caravanning, too. The rule of thumb is one car length back for every ten miles per hour of velocity. Thirty miles per hour; three car lengths behind the bumper ahead of you. Sixty miles per hour; six lengths. Don't trust yourself to keep the pace? Don't drive. Car-pool with someone else.

**• Rule 5 - Come prepared.**
If the trip involves driving, make sure you have enough fuel to see you through. If the instructions state "bring lunch," don't assume that you'll be able to stop at a convenience store to pick up a sandwich. Do that, and you'll likely be eating alone.

**• Rule 6 - Check out your equipment before the trip.**
The single greatest frustration first-time trip goers face in not inexperience, but rather the lousy or malfunctioning equipment - usually optics.

If your binoculars aren't working, ask whether a loaner is available. It you don't own binoculars, do not rush out to the nearest discount store and buy some for the trip. People who do this usually end up with instruments they soon replace. Borrow binoculars for the trip. Use your field trip experience to see what instruments experienced birders are using in order to make an educated purchase later.

**• Rule 7 - Speak Softly.**
Human voices put wildlife on alert. Talking may also prevent a leader from hearing songs or calls and keep you from hearing instructions. Field trips are social and conversation is part of the field trip experience. If you want to converse, do so in whispers or stand away from the group.

**• Rule 8 - Keep motion to a minimum.**
More than sound, birds react to motion. In close proximity to birds, don't move quickly and above all do not advance until the leader gives the word. Want to draw the ire of a group? Walk toward "the bird of the day" and scare it away.

**• Rule 9 - Don't monopolize the leader.**
Sure you have questions. Sure you want to get to know the leader, and you want them to come to recognize your wonderful qualities, too. One of those qualities should be deference, because everyone in the group shares your ambition. Deference extends to use of the spotting scopes, too.

When the leader trains his scope on an interesting bird, and you were first to get a glimpse last time, defer to others the next several times. No matter what your place in line, first looks through a scope are quick looks. After you get an identifying glimpse, step quickly aside for the next person. If the bird is moving, reposition the scope so the next user won't have to pan back and forth. After everyone has had their glimpse, more leisurely viewing is possible.

**• Rule 10 - Do ask questions.**
Leaders want to share their knowledge, and questions are the catalyst that unlocks it. Don't be intimidated by what you don't know or what you presume that others know. Chances are your question is shared by others in the group. You may not be the leader, but if you trigger the answer to a question that some other member of the group was too shy to utter, you'll be their hero. That's it. All you need to know to get the most out of your first field trip experience. If it seems like too much to remember, just remember Rule #1. At any other time, there will be someone else around to ask for assistance.

*This guide has been reproduced with the permission of Pete Dunne. Minor editing by Ron Bourque.*

*nestboxtips.txt*

Tips for Nest Boxes this spring/summer

If you have old boxes in your garden, clean out any of last years nesting material or any old bits of food that may have been stored in there.

If you are putting up new nest boxes make sure that they are out of the reach of cats and Squirrels.

Check that the box isn't in full sun otherwise young birds may literally bake in the heat.

Experiment with different kinds of bird boxes – the open-fronted "Robin" boxes may even attract Spotted Flycatchers.

Make sure any boxes are at least 15mm in thickness.

Face boxes away from prevailing winds.

Don't put nest boxes to close together in a small area as this will only lead to territorial fights.

Always make sure that there is enough food and fresh water made available close by.

Do not but bird boxes with perches attached – the birds do not need them and it may only invite predators.

Never buy a bird table with a nest box built in, as nesting birds will only come into conflict with feeding ones.

*Letter to Fred*

Dear Fred,

Hi haven't seen you in ages been meaning to write to you for a while but never got round to it.

How have you been?  Still working at the library?

We should meet up next time you are up here, my phone number is still 435 7862

Yours truly,

Bob