

REPORT of [REDACTED]

Forensic Analyst
DFMsc, Abertay

Case against: John Doe

Police Reference No: N/A
Case Reference No: CMP507JKPJD
PF Reference No: N/A



Summary

An image was acquired of the hard drive of a PC belonging to John Doe (the suspect) following his arrest on charges of suspicion of possession and distribution of material of an ornithological nature. The arrest was made at 17:30 on 9th February 2005.

Between 14:11 on 2nd February 2005 and 17:09 on 9th February 2005, the user “johndoe” used a personal computer (“PC”) to engage with material of an ornithological nature, some of which was subjected to concealment techniques. E-mails with ornithological content were also received in an e-mail account belonging to johndoe@example.com prior to the installation of an operating system on the PC.

The PC activity can be broken into seventeen distinct episodes of activity (“incidents”). A further three incidents without a specific time period have been identified. A summary of the materials recovered on the PC can be found in the table below:

Type of material	Number of occurrences
Image	104
Document	16
Email	4
Website visit	12
Internet search	49
Audio	3
Internet bookmark	3

Contents

1	Description of Crime	1
1.1	Incident #1.....	1
1.2	Incident #2.....	1
1.3	Incident #3.....	1
1.4	Incident #4.....	2
1.5	Incident #5.....	2
1.6	Incident #6.....	3
1.7	Incident #7.....	3
1.8	Incident #8.....	3
1.9	Incident #9.....	3
1.10	Incident #10.....	4
1.11	Incident #11.....	4
1.12	Incident #12.....	4
1.13	Incident #13.....	5
1.14	Incident #14.....	5
1.15	Incident #15.....	6
1.16	Incident #16.....	6
1.17	Incident #17.....	6
1.18	Incident #18.....	7
1.19	Incident #19.....	7
1.20	Incident #20.....	8
2	Description of Investigation	9
2.1	Job Description and Instructions.....	9
2.2	Description of Examined Item	9
2.3	Methodology.....	9
2.3.1	File integrity.....	9
2.3.2	Disk audit.....	9
2.3.3	Antivirus scan (including mounting of image file).....	10
2.3.4	Evidence discovery/extraction	10
2.4	Analysis.....	10
2.4.1	Disk audit.....	10

2.4.2	Antivirus scan.....	12
2.4.3	Autopsy Data Extraction	14
2.4.4	Internet history analysis.....	18
2.4.5	Registry Analysis.....	23
2.4.6	Event Log Analysis	27
2.4.7	Printer Spool File Analysis	27
2.4.8	Pagefile.sys Analysis	28
2.4.9	Recent Documents analysis.....	28
2.4.10	Prefetch analysis.....	29
2.4.11	Recycling Bin examination	30
2.4.12	Timeline creation.....	31
2.4.13	Steganography analysis.....	33
2.4.14	File header analysis	33
2.5	Production List and Associated Description.....	33
3	Conclusions.....	34
	Appendices.....	35
	Appendix A - Recovered Images.....	35
	Appendix B - Recovered Documents.....	70
	Appendix C - Metadata	111
	Appendix D - E-mail Analysis.....	112
	Appendix E - Internet History Analysis.....	115
	Appendix F - Registry Analysis.....	144
	Appendix G - Recent Documents Analysis	155
	Appendix H - Prefetch Analysis	163
	Appendix I - Recycling Bin Analysis	165
	Appendix J - Graphical Representation of Timeline	166
	Appendix K - Glossary	168
	Appendix L - List of Evidentiary Files with MD5 Hashes.....	172
	Appendix M - List of Software/Tools Used to Conduct Analysis	177

1 DESCRIPTION OF CRIME

A detailed breakdown of incidents can be found below. A graphical representation of the incidents can be found in Appendix J - Graphical Representation of Timeline. A glossary of terms can be found in Appendix K - Glossary.

1.1 INCIDENT #1

At 18:51 on 16th October 2004, an e-mail with the subject line “How to Identify Birds” with a sender e-mail address of mailinglist@birds.example.com and a recipient e-mail address of jdoe@example.com was received. The e-mail was found in the Inbox file associated with the Thunderbird profile located in the profile folder for user “johndoe”. The sender’s e-mail display name was “Bird Fanciers”. The contents of the e-mail body were ornithological in nature (text only). The e-mail contents and its headers are produced as exhibit 1.1 and 1.2 (respectively) in Appendix D - E-mail Analysis.

1.2 INCIDENT #2

At 19:51 on 17th November 2004, an e-mail with the subject line “expensive birds” with a sender e-mail address of ben@example.org and a recipient e-mail address of jdoe@example.com was received. The e-mail was found in the Inbox file associated with the Thunderbird profile located in the user profile folder for user “johndoe”. The contents of the e-mail body were ornithological in nature (text only). The e-mail contents and its headers are produced as exhibit 2.1 and 2.2 (respectively) in Appendix D - E-mail Analysis.

1.3 INCIDENT #3

Between 14:11 and 15:12 on 2nd February 2005, the user “johndoe” used Firefox to search for and visit websites containing material of an ornithological nature. A breakdown of the internet activity can be found in Table 1 below. The accompanying browser history log can be found in exhibits 3.1 and 3.2 in Appendix A - Recovered Images, which also includes details of subject-specific advertisements found in the internet history for this time period.

Table 1: Breakdown of internet activity for Incident #3

Activity type	Number of occurrences
Search	8
Website visits	34

During this time, four IIOB (Inappropriate Images of Birds) were saved to the "My Pictures" directory within the profile folder belonging to user “johndoe”. A further IIOB was saved to C:\Windows. The

images are included in Appendix A - Recovered Images as exhibits 3.3 to 3.7. The accompanying browser activity log can be found in exhibit 3.8 of Appendix E - Internet History Analysis.

A further three items that contained ornithological material were downloaded to the "My Documents" directory within the profile folder belonging to user "johndoe". The first of these items was a web page entitled "Birding and Birdwatching - Build a Bluebird Nest Box for Wild Birds" and was saved as aa010703a.htm at 14:25. A screenshot of this web page is included as exhibit 3.9 in Appendix B - Recovered Documents. At 14:29, a text file named "nestboxtips.txt" was downloaded. The contents of this file are produced as exhibit 3.10 in Appendix B - Recovered Documents. The accompanying browser activity log for these two items can be found in exhibit 3.8 of Appendix E - Internet History Analysis. At 15:11, an audio file named "kakapo.ram" was downloaded. The accompanying browser activity log for this item can be found in exhibits 3.1 and 3.2 of Appendix E - Internet History Analysis. Further evidence of file access for the aa010703a.htm and kakapo.ram files was found in the Recent folder in the profile folder for user "johndoe" (provided as exhibits 3.11 and 3.12 in Appendix F - Registry Analysis) and in the Recent Documents key entries from the registry (provided as exhibits 3.13 and 3.14 in Appendix G - Recent Documents Analysis).

A second audio file named "dawn.ram" was downloaded to the Local Settings/Temp directory in the profile folder belonging to user "johndoe" at 15:12. The download log for this file is produced as exhibit 3.15 in Appendix E - Internet History Analysis. The accompanying browser activity log for this item can be found in exhibits 3.1 and 3.2 of Appendix E - Internet History Analysis.

Two URLs for websites containing ornithological material were added to the Firefox Bookmarks for the user "johndoe" at 14:21 and 14:24. The bookmark file is produced as exhibits 3.16 and 3.17 in Appendix E - Internet History Analysis. The accompanying browser activity log for this item can be found in exhibits 3.1 and 3.2 of Appendix E - Internet History Analysis.

1.4 INCIDENT #4

At 16:46 on 2nd February 2005, an encrypted file called "birdpics.gpg" was created and saved to the "My Documents" directory within the profile folder belonging to user "johndoe". The file contained an archive file called "birdpics.zip", containing five IIOB, which were downloaded from an external USB drive, mounted as E:\. The images are included in Appendix A - Recovered Images as exhibits 4.1 - 4.5. Evidence of file access for the birds.zip file was found in the Recent Documents key entries from the registry (provided as exhibits 4.6 and 4.7 in Appendix F - Registry Analysis). Further evidence of the connected USB drive was found in the system registry hive and is provided as exhibit 4.8 in Appendix F - Registry Analysis.

1.5 INCIDENT #5

Between 11:42 and 11:51 on 3rd February 2005, the user "johndoe" had a period of file interaction on the PC, during which time eleven IIOB were saved to a hidden volume (mounted as F:\) on the hard drive. The images are included in Appendix A - Recovered Images as exhibits 5.1 - 5.11. Evidence of the mounted volume was found in the system registry hive, provided as exhibit 5.12 in Appendix F - Registry Analysis.

At 11:45, the birdpics.gpg file was accessed. At 11:46, the directories containing the files associated with the aa010703a.htm file were also accessed. Furthermore, at 11:51, the “Firefox wallpaper.bmp” IIOB was accessed. The accompanying time stamps are shown in exhibit 5.14 In Appendix G - Recent Documents Analysis.

1.6 INCIDENT #6

At 12:08 on 3rd February 2005, the user “johndoe” created an archive file called “CrouchingKokako.dll”, containing seven IIOB using an irregular file extension (.dll). The file was saved in a common location for these types of files not usually used for personal data (C:\WINDOWS). The images contained with the archive file are included in Appendix A - Recovered Images as exhibits 6.1 - 6.7.

1.7 INCIDENT #7

Between 12:21 and 12:23 on 3rd February 2005, the user “johndoe” conducted an internet search for “bird mating calls”, and then visited a website of ornithological nature. An audio file entitled “aggressive_song.wav” was downloaded to the external USB drive, mounted as E:\. The accompanying browser activity and download logs for this item can be found in exhibits 7.1 and 7.2 of Appendix E - Internet History Analysis, respectively. Further evidence demonstrating that the file was accessed once it had been downloaded is provided in exhibits 7.3 and 7.4 of Appendix F - Registry Analysis.

1.8 INCIDENT #8

At 14:09 on 3rd February 2005, a URL for a website containing ornithological material was added to the Firefox Bookmarks for the user “johndoe”. The bookmark file is produced as exhibits 8.1 and 8.2 in Appendix E - Internet History Analysis.

1.9 INCIDENT #9

Between 14:14 and 14:19, the user “johndoe” had a period of file interaction on the PC, during which time an IIOB entitled “EvanstonWoodpecker.jpg” was viewed. This image could not be located within the image, however the accompanying file access logs are provided in exhibits 9.1 (Appendix E - Internet History Analysis), 9.2 & 9.3 (Appendix G - Recent Documents Analysis), and 9.4 & 9.5 (Appendix F - Registry Analysis).

A document called “Doc1.doc” was created and saved to the “My Music” directory within the profile folder belonging to user “johndoe” at 14:17. The document contains a single oversized IIOB. Screenshots of this document and its contents are included as exhibits 9.6 and 9.7 in Appendix B - Recovered Documents. The accompanying file access logs are provided in exhibits 9.8 (Appendix E - Internet History Analysis), 9.9 - 9.12 (Appendix G - Recent Documents Analysis), and 9.13 & 9.14 (Appendix F - Registry Analysis).

1.10 INCIDENT #10

At 14:40 on 3rd February 2005, the user “johndoe” created an IIOB called “FantailFrontView.exe”, using an irregular file extension (.exe). The file was saved in a location not usually used for personal data (C:\WINDOWS\mui). The image, which appears to be the same as that inserted into Doc1.doc, is included in Appendix A - Recovered Images as exhibit 10.1. The accompanying file access log is provided in exhibits 10.2 of Appendix F - Registry Analysis.

1.11 INCIDENT #11

At 14:49 on 3rd February 2005, the user “johndoe” interacted with some files on the PC, during which time an image was viewed entitled “Killdeer.jpg” on an external USB drive. It is believed the file was an IIOB, based on its file name. This image could not be located however the accompanying file access logs are provided in exhibits 11.1 (Appendix E - Internet History Analysis), 11.2 & 11.3 (Appendix G - Recent Documents Analysis), and 11.4 & 11.5 (Appendix F - Registry Analysis).

1.12 INCIDENT #12

Between 14:59 and 15:06 on 3rd February 2005, the user “johndoe” used Firefox to search for and visit websites containing material of an ornithological nature. A breakdown of the internet activity can be found in Table 2 below. The accompanying browser history log can be found in exhibits 12.1 and 12.2 in Appendix E - Internet History Analysis, which also includes details of subject-specific advertisements found in the internet history for this time period.

Table 2: Breakdown of internet activity for Incident #12

Activity type	Number of occurrences
Search	3
Website visits	12

During this time, four IIOB were saved to the “My Pictures” directory, one IIOB was saved to the “Desktop” directory, and one IIOB was saved to the “My Documents” directory, all within the profile folder belonging to user “johndoe”. A further IIOB was saved to the “My Music” directory within the profile folder belonging to user “bob”, though this activity can be seen in the downloads log for the Firefox profile for the user “johndoe”. The images are included in Appendix A - Recovered Images as exhibits 12.3 - 12.9. A web page document that contained ornithological material was also downloaded to the “My Documents” directory within the profile folder belonging to user “johndoe”. A screenshot of this web page is included as exhibit 12.10 in Appendix B - Recovered Documents. The accompanying download logs for these files can be found in exhibit 12.11 of Appendix E - Internet History Analysis. Further evidence of file access for the files was found in the index.dat file (provided as exhibit 12.12 in Appendix E - Internet History Analysis), in the Recent folder in the profile folder for user “johndoe” (provided as exhibits 12.13 and 12.14 in Appendix G - Recent Documents Analysis), and in the Recent Documents key entries from the registry (provided as exhibits 12.15 and 12.16 in Appendix F - Registry Analysis).

1.13 INCIDENT #13

Between 15:42 and 15:55 on 3rd February 2005, the user “johndoe” had a period of file interaction on the PC. During this time three IIOB images were saved to a location not usually used for personal data (C:\Program Files) without any file extension. The images are included in Appendix A - Recovered Images as exhibits 13.1 - 13.3.

During this time period, a file (blue_bird2.jpg) was renamed to Df1.jpg and subsequently deleted at 15:43 as shown in the INFO2 file found in the Recycling Bin on the hidden volume, provided as exhibit 13.4 in Appendix I - Recycling Bin Analysis.

At 15:44, the user “johndoe” saved a document entitled “guide.doc”, originally authored by “Paul Teddy” to the hidden volume. The contents of the document are ornithological in nature. The document is included as exhibit 13.5 in Appendix B - Recovered Documents. The accompanying metadata information is provided as exhibit 13.6 in Appendix C - Metadata.

Between 15:49 and 15:52, the user “johndoe” viewed three documents containing material of an ornithological nature. Of these three documents, only one has been retrieved, with the title “birdwatching.doc”. This is provided as exhibit 13.7 in Appendix B - Recovered Documents. The other two documents were accessed from the external USB drive. Evidence of file access for all three files was found in the index.dat file (provided as exhibit 13.8 in Appendix E - Internet History Analysis), the Recent folder in the profile folder for user “johndoe” (provided as exhibits 13.9 and 13.10 in Appendix G - Recent Documents Analysis), and in the Recent Documents key entries from the registry (provided as exhibits 13.11 and 13.12 in Appendix F - Registry Analysis). Further evidence of access to both “.doc” files was found in the Office Recent documents folder of the profile folder belonging to the user “johndoe” and is presented in exhibits 13.13 and 13.14 of Appendix G - Recent Documents Analysis.

At 15:54, the user “johndoe” edited a system configuration file named “ODBC.ini”, using commenting to include text with a subject of ornithological nature. The document is included as exhibit 13.15 in Appendix B - Recovered Documents. Further evidence of this file was found in the Recent documents folder of the profile folder belonging to the user “johndoe” and is presented in exhibits 13.16 and 13.17 of Appendix G - Recent Documents Analysis.

1.14 INCIDENT #14

Between 11:04 and 11:08 on 9th February 2005, the Thunderbird client installed on the PC was used to access the Thunderbird e-mail profile for the user “johndoe”. Two e-mails with a sender e-mail address of ben@example.org and a recipient e-mail address of jdoe@example.com were received since the installation of Windows XP on the PC and were found in the Inbox. Both e-mails have IIOB as attached files. One of the e-mails contains text in the message body that suggests the sender has previously received IIOB originating from john@example.com. A breakdown of the e-mails can be seen in Table 3 below.

Table 3: Breakdown of e-mail activity for Incident #14

Subject line	Received time	Number of attachments
good pics	08/02/2005 11:08	2
some more good ones	08/02/2005 11:08	5

The e-mail contents and its headers (both of which appear corrupted) are produced as exhibit 14.1 and 14.2 (respectively) in Appendix D - E-mail Analysis. The IIOB attachments are included in Appendix A - Recovered Images as exhibits 14.3 - 14.9. The accompanying prefetch file entry is provided in exhibit 14.10 of Appendix H - Prefetch Analysis.

1.15 INCIDENT #15

Between 11:27 and 11:28 on 9th February 2005, the user “johndoe” conducted an internet search for “bird screensavers”, and then visited two websites of ornithological nature. An archive file entitled “birds.zip” was downloaded to the “My Documents” directory within the profile folder belonging to user “johndoe”. The accompanying browser activity for this activity can be found in exhibits 15.1 - 15.3 of Appendix E - Internet History Analysis. The download log for the “birds.zip” can be found in exhibit 15.4 of Appendix E - Internet History Analysis. This file could not be located, however evidence demonstrating that the file was accessed once it had been downloaded is provided in exhibits 15.5 and 15.6 of Appendix G - Recent Documents Analysis. Furthermore, the prefetch analysis, provided in exhibits 15.7 and 15.8 of Appendix H - Prefetch Analysis, evidences that this file was used as the source for the installation of a program named “TX_BIRDS.EXE” at 11:28. Three other files relating to this executable were created at 11:28, namely tx_birds.dat, tx_birds.dll, and tx_birds.scr (a screensaver file), all contained within the C:\WINDOWS directory.

1.16 INCIDENT #16

At 13:50 on 9th February 2005, the user “johndoe” accessed the “TX_BIRDS.EXE” file as evidenced by the prefetch analysis, provided as exhibit 16.1 in Appendix H - Prefetch Analysis.

1.17 INCIDENT #17

Between 16:51 and 17:09 on 9th February 2005, the user “johndoe” had a period of file interaction on the PC. During this time, a file originally named “birds to find” was renamed and saved as “stuf.doc” in the “My Documents” directory within the profile folder belonging to user “johndoe” at 16:51. The document is signed off by “John Doe”. The document is included as exhibit 17.1 in Appendix B - Recovered Documents. The accompanying metadata information is provided as exhibit 17.2 in Appendix C - Metadata. Evidence of access for this file was found in the Recent folder in the profile folder for user “johndoe” (provided as exhibits 17.3 and 17.4 in Appendix G - Recent Documents Analysis), and in the Recent Documents key entries from the registry (provided as exhibits 17.5 and 17.6 in Appendix F - Registry Analysis). Further evidence of access to this file was

found in the Office Recent documents folder of the profile folder belonging to the user “johndoe” and is presented in exhibits 17.7 and 17.8 of Appendix G - Recent Documents Analysis.

During this time period (specifically between 17:05 and 17:06), the user “johndoe” also created and accessed 22 IIOB on the hidden volume, ten of which had been created during Incident #5. Their details are shown in Table 4 below and are provided as exhibits in Appendix A - Recovered Images.

Table 4: Listing of image files for Incident #17

Image name	Image reference number
AlmondMarshGreatBlueHeronStalling.jpg	5.1
BaldEagle7oClock.jpg	5.2
AmericanAvocetWinterPlumage.jpg	5.3
AmericanWhitePelicansCircling.jpg	5.4
BellbirdJumpingOffBranch.jpg	5.5
BarnOwl.jpg	5.6
BlackNeckedStiltsFromBehind.jpg	5.7
BlackSwan.jpg	5.8
BlackVultureSunningOnPost.jpg	5.9
brd_Ornithologist_TWG.jpg	5.11

The remaining twelve IIOB are included in Appendix A - Recovered Images as exhibits 17.7 - 18. Evidence of file access for one of these files specifically (“AlmondMarshGreatBlueHeronStalling.jpg”) was found in the Recent folder in the profile folder for user “johndoe” (provided as exhibits 17.19 and 17.20 in Appendix G - Recent Documents Analysis), and in the Recent Documents key entries from the registry (provided as exhibits 17.21 and 17.22 in Appendix F - Registry Analysis).

1.18 INCIDENT #18

In addition to the activities detailed in the timeline, eighteen IIOB were discovered in the allocated space on the hard drive. It is not known where these files originated from. They have been retrieved (“carved”) by the Autopsy forensic tool used by the analyst and are included as exhibits 18.1 - 18.18 in Appendix A - Recovered Images.

Two further files were discovered in this fashion, both appearing to depict a cached web page showing internet searches for ornithological material. They are included as exhibits 18.19 and 18.20 in Appendix B - Recovered Documents.

1.19 INCIDENT #19

In addition to the activities detailed in the timeline, 24 IIOB were discovered in the unallocated space on the hard drive. It is not known where these files originated from. They have been retrieved by the Autopsy forensic tool used by the analyst and are included as exhibits 19.1 - 19.24 in Appendix A - Recovered Images.

Two cached web pages showing material of ornithological content were discovered in this fashion. They are included as exhibits 19.25 - 19.27 in Appendix B - Recovered Documents. A breakdown of the file content per file can be found in Table 5 below:

Table 5: Table 4: Listing of image files for Incident #19

File name	Content description
f0005672_Related_Articles.html	List of related articles for ornithological material
f0033288.html	List of books containing ornithological material
f0041304.html	Internet search for “bird mating calls”

A further three PDF files showing material of ornithological content (which appear to be the source of the images discovered in Incident #18) were discovered in this fashion. They are included as exhibits 19.28 - 19.30 in Appendix B - Recovered Documents.

1.20 INCIDENT #20

In addition to the activities detailed in the timeline, five IIOB were discovered as “orphaned” files on the hard drive. One of these images has been recovered only in part (“0E47C6DFd01”). It is not known where these files originated from. They have been retrieved by the Autopsy forensic tool used by the analyst and are included as exhibits 20.1 - 20.05 in Appendix A - Recovered Images.

2 DESCRIPTION OF INVESTIGATION

2.1 JOB DESCRIPTION AND INSTRUCTIONS

The analyst was tasked with analysing an acquired image of a home PC belonging to John Doe (hereon referred to as “the suspect”), an employee of Strathclyde University. The instructions, received from Dr. Ian Ferguson, were issued to assist with an investigation into the suspect’s alleged possession and distribution of material of an ornithological nature, with which he had been charged. It was the analyst’s responsibility to discover any data pertinent to the charges within the acquired image. Any such discovered data was to be extracted and detailed in a report suitable for court presentation, should the charges against the suspect be taken to prosecution.

2.2 DESCRIPTION OF EXAMINED ITEM

The analyst was provided with an image file (hereon referred to as “the image”) of the hard drive of a PC that had been acquired by a first responder at the suspect’s home address. The PC was powered off at the time of the acquisition. The image was provided to the analyst in the .dd file format with a name of “johndoe.dd”. The first responder confirmed that there was no time skew present on the PC during the seizure of the hard drive. The image file was provided to the analyst in password-protected cloud storage and was compressed as a .zip file. File integrity (after the file had been downloaded and decompressed) was ensured by way of MD5 hash verification.

2.3 METHODOLOGY

The analyst used two forensic workstations to conduct the investigation into the image - a Windows 11 laptop (for any tools with a graphical interface) and a Kali (Linux) virtual machine (for any command-line driven tools), hosted on the same Windows 11 laptop. The image file was downloaded using a secure internet connection and decompressed using 7Zip. After extraction, the johnDoe.dd was copied from the Windows 11 host to the Kali forensic machine using VirtualBox File Manager. Details of the tool/software versions used can be found in Appendix M - List of Software/Tools Used to Conduct Analysis.

2.3.1 File integrity

After extraction the john.dd file was set as read-only on both the Windows 11 laptop (using the file properties available) and on the Kali virtual machine (using the chmod tool). The MD5 hash was verified using HashCalc (on the Windows 11 laptop) and the md5sum tool (on the Kali virtual machine). Both versions of the file were found to have the same MD5 hash value as had been provided by the first responder who performed the file acquisition.

2.3.2 Disk audit

The analyst performed a preliminary disk audit to ensure that there were no inconsistencies between the data contained in the raw data and the data analysed by the analyst. The audit was conducted

using a number of command-line tools detailed in Appendix M - List of Software/Tools Used to Conduct Analysis.

2.3.3 Antivirus scan (including mounting of image file)

The image was mounted in the Kali virtual machine, enabling the analyst to perform an antivirus scan on the file system using ClamAV.

2.3.4 Evidence discovery/extraction

The main tool used to perform the discovery and extraction of evidence was Autopsy (for Windows), under the case number “CMP507JKPD”. All ingested modules, including the Plaso module for timeline analysis, were applied at the time of import. Three new tags were created for categorising of potentially pertinent material:

- Ornithological (for material found in allocated space).
- Unallocated Ornithological material.
- Orphaned Ornithological material.

The Autopsy platform enabled the analyst to discover and extract images, documents, audio files, e-mails, and browser activity pertinent to the charges. It further enabled analysis of the registry and prefetch data found within the image. Keyword searching allowed the analyst to identify several items of interest, which in turn allowed the keyword list in use to be expanded, yielding further results. A number of context-specific tools were used to analyse some data discovered in proprietary formats (e.g. the Firefox cache). A list of all tools used, with a description of their purpose, can be found in Appendix M - List of Software/Tools Used to Conduct Analysis.

2.4 ANALYSIS

A list of all tools used for the analysis of the image, along with a description of their purpose, can be found in Appendix M - List of Software/Tools Used to Conduct Analysis.

2.4.1 Disk audit

fdisk was used to initiate the disk audit. The output can be seen in Figure 1 below and showed a single NTFS partition with 512-byte sectors.

```
$ fdisk -l johnDoe.dd
Disk johnDoe.dd: 5.37 GiB, 5762727936 bytes, 11255328 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0ddb8ddb8

Device      Boot Start     End Sectors  Size Id Type
johnDoe.dd1 *        63 6136829 6136767  2.9G  7 HPFS/NTFS/exFAT
```

Figure 1: Output from fdisk tool for disk audit

The analyst sought to validate these findings using mmls. The output can be seen in Figure 2:

```
└$ mmls johnDoe.dd
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End        Length      Description
000: Meta    0000000000  0000000000  0000000001  Primary Table (#0)
001: _____  0000000000  0000000062  0000000063  Unallocated
002: 000:000  0000000063  0006136829  0006136767  NTFS / exFAT (0x07)
003: Sect lists 0006136830  0011255327  0005118498  Unallocated
```

Figure 2: Output from mmls tool for disk audit

Whilst the output from the second tool validated the findings from fdisk in terms of sector and disk size, it also revealed a hidden partition in the unallocated space on the disk. This was confirmed with the use of the parted tool, whose output can be seen in Figure 3:

```
└$ sudo parted johnDoe.dd print free
Model: (file)
Disk /home/osboxes/cmp507/johnDoe.dd: 5763MB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:

Number  Start   End     Size   Type      File system  Flags
 1       32.3kB  3142MB  3142MB  primary    ntfs         boot
                  3142MB  5763MB  2621MB          Free Space
```

Figure 3: Output from parted tool for disk audit

For the final part of the disk audit, fsstat was used to confirm the operating system in place in the image. The output from this tool, which suggests that the operating system was Windows XP, can be seen in Figure 4 below:

```
└$ fsstat -o 6136830 johnDoe.dd
FILE SYSTEM INFORMATION
_____
File System Type: NTFS
Volume Serial Number: 64708B6C708B43B0
OEM Name: NTFS
Volume Name: New Volume
Version: Windows XP

METADATA INFORMATION
_____
First Cluster of MFT: 262144
First Cluster of MFT Mirror: 319291
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 64
Root Directory: 5

CONTENT INFORMATION
_____
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 638582
Total Sector Range: 0 - 5108668

$AttrDef Attribute Values:
$STANDARD_INFORMATION (16)  Size: 48-72  Flags: Resident
$ATTRIBUTE_LIST (32)  Size: No Limit  Flags: Non-resident
$FILE_NAME (48)  Size: 68-578  Flags: Resident,Index
$OBJECT_ID (64)  Size: 0-256  Flags: Resident
$SECURITY_DESCRIPTOR (80)  Size: No Limit  Flags: Non-resident
$VOLUME_NAME (96)  Size: 2-256  Flags: Resident
$VOLUME_INFORMATION (112)  Size: 12-12  Flags: Resident
$DATA (128)  Size: No Limit  Flags:
$INDEX_ROOT (144)  Size: No Limit  Flags: Resident
$INDEX_ALLOCATION (160)  Size: No Limit  Flags: Non-resident
$BITMAP (176)  Size: No Limit  Flags: Non-resident
$REPARSE_POINT (192)  Size: 0-16384  Flags: Non-resident
$EA_INFORMATION (208)  Size: 8-8  Flags: Resident
$EA (224)  Size: 0-65536  Flags:
$LOGGED.Utility_Stream (256)  Size: 0-65536  Flags: Non-resident
```

Figure 4: Output from fsstat tool for disk audit

2.4.2 Antivirus scan

After mounting the image at the appropriate offset, an antivirus scan was run on the first partition identified in the disk audit. The output of the scan can be seen in Figure 5 below:

```
└$ cat johnDoe.dd.o32256.clamscan.log
_____
/mnt/suspectDrive/Program Files/Real/RealPlayer/realplay.exe: Win.Trojan.Tufik-100 FOUND

____ SCAN SUMMARY ____
Known viruses: 8699041
Engine version: 1.4.1
Scanned directories: 1431
Scanned files: 15666
Infected files: 1
Data scanned: 3125.94 MB
Data read: 2926.50 MB (ratio 1.07:1)
Time: 3674.266 sec (61 m 14 s)
Start Date: 2024:10:14 16:23:20
End Date: 2024:10:14 17:24:34
```

Figure 5: Output from ClamAV scan for visible partition

This process was repeated with the hidden partition identified in the disk audit (after “unmounting” the first partition). The output of this scan can be seen in Figure 6:

```
$ clamscan -ri /mnt/suspectDrive/ -l johnDoe.dd.o3142056960.clamscan.log
____ SCAN SUMMARY _____
Known viruses: 8699850
Engine version: 1.4.1
Scanned directories: 6
Scanned files: 28
Infected files: 0
Data scanned: 5.66 MB
Data read: 5.36 MB (ratio 1.06:1)
Time: 16.835 sec (0 m 16 s)
Start Date: 2024:11:21 13:39:59
End Date: 2024:11:21 13:40:16
```

Figure 6: Output from ClamAV scan for hidden partition

Upon the discovery of a trojan in the first partition, the analyst extracted the potentially malicious file identified from the image so that the MD5 hash could be generated and sent to VirusTotal for further analysis. The VirusTotal results can be seen in Figures 7 and 8 below:

Vendor	Detection	Details	Notes
Bkav Pro	W32.AIDetectMalware	ClamAV	Win.Trojan.Tufik-100
Google	Detected	SecureAge	Malicious

Figure 7: VirusTotal results for MD5 hash of alleged malicious file summary page

Property	Value
MD5	8b0334f36476e0cf754186ca5c20e2ba
SHA-1	91bb9675e3a00ba6e01175ef4644cd03670a81b
SHA-256	35514d52a5dc1da3e977898f056c56a1b27cd1849330f951de9bdd8ff4d04e24
Vhash	025046655d1550e521003672zcz1202dz
Authentihash	823c704e2fa544f69f15dcf8e52ac20feb2236f806e8537b19c81fa445b7517
Impfhash	3eeffd519db605c37b59e86fb6aa61
Rich PE header hash	f5a8109e5b5d919c424461967977257c
SSDEEP	3072:MNK5jqV5tzkrmuUh5nG0gZtYkgZfYnpW+W1M:MNKY5TqmUuH5GHZwpZwNHWi
TSLH	T168141813F604C498D6884831C9AAAF80470FC56D045566BF3BD0FF6F3C76993AA0B25E
File type	Win32 EXE
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Win32 Executable MS Visual C++ (generic) (47.3%) Win64 Executable (generic) (15.9%) Win32 Dynamic Link Library (generic) (9.9%) Win16 NE executable (generic) (7...)
DetectItEasy	PE32 Compiler: EP:Microsoft Visual C/C++ (5.0-6.0 (1720-9049)) [EXE32] Compiler: Microsoft Visual C/C++ (6.0) Compiler: Microsoft Visual C/C++ (12.00.8966) [C++]
File size	200.04 KB (204845 bytes)
PEiD packer	Microsoft Visual C++
History	
Creation Time	2004-08-19 22:05:34 UTC
First Seen In The Wild	2019-03-18 23:05:26 UTC
First Submission	2009-06-13 23:02:45 UTC
Last Submission	2024-11-08 18:57:07 UTC
Last Analysis	2023-12-01 11:29:01 UTC

Figure 8: VirusTotal results for MD5 hash of alleged malicious file properties page

Furthermore, this particular MD5 hash has been identified by SpywareRemove.com as being a legitimate file from the supplier, and Microsoft's advice regarding this Trojan variant suggests that it was not in circulation until 2009, corroborating the results from VirusTotal. Given the incidents being investigated happened several years prior to this (in 2004 and 2005), the analyst concluded that this result from ClamAV was a false positive, caused by the time disparity between the date of the image file and the date that the antivirus scan was run against the image.

No malicious files were detected in the second (hidden) partition.

2.4.3 Autopsy Data Extraction

Prior to opening the image with Autopsy for further analysis, the analyst confirmed that list of known good hashes (the hash values for files that are known to be part of the Windows XP operating system, and therefore "good") had been imported into Autopsy.

2.4.3.1 System information

Using the software registry hive (extracted using Autopsy) and Registry Viewer, the analyst conducted a preliminary investigation to ascertain some basic facts about the system that had been installed on the suspect's hard drive. The results of this preliminary investigation can be seen in Figures 9 and 10 below, which show that the operating system was confirmed as a licensed version of Windows XP Service Pack 2, which had been installed at 15:51 on 24th January 2005. The registered owner was confirmed as "John Doe".

SubVersionN...	REG_SZ	(value not set)
CurrentBuild	REG_SZ	1.511.1 () (Obsolete data - do not use)
InstallDate	REG_DWORD	0x41F51995 (1106581909)
ProductName	REG_SZ	Microsoft Windows XP
RegDone	REG_SZ	(value not set)
RegisteredO...	REG_SZ	(value not set)
RegisteredO...	REG_SZ	John Doe
SoftwareType	REG_SZ	SYSTEM
CurrentVersi...	REG_SZ	5.1
CurrentBuild...	REG_SZ	2600
BuildLab	REG_SZ	2600.xpsp_sp2_rtm.040803-2158
CurrentType	REG_SZ	Uniprocessor Free
CSDVersion	REG_SZ	Service Pack 2
SystemRoot	REG_SZ	C:\WINDOWS
SourcePath	REG_SZ	D:\I386
PathName	REG_SZ	C:\WINDOWS
ProductId	REG_SZ	76487-015-4027933-22087
DigitalProdu...	REG_BINARY	A4 00 00 00 03 00 00 00 37 36 34 38 37 2D 30 31 35 2D ...
LicensesInfo	REG_BINARY	33 B7 21 85 38 A9 F7 32 0E C1 08 AB 4F F4 A5 9D 1B F...

Figure 9: software registry hive OS information

Key Properties	
Last Written Time	09/02/2005 11:03:33 UTC
OS Install Date (UTC)	Mon Jan 24 15:51:49 2005
OS Install Date (Local)	Mon Jan 24 15:51:49 2005

Figure 10: software registry hive OS installation date

The software registry hive was furthermore used to populate a list of installed software, which would help guide the investigation. These results from Registry Viewer can be seen in exhibits 0.1 and 0.2 of Appendix F - Registry Analysis.

Lastly, the analyst used the system registry hive to confirm the time zone in use for the PC, which can be seen as “GMT” in Figure 11.

Name	Type	Data
Bias	REG_DWORD	0x00000000 (0)
StandardName	REG_SZ	GMT Standard Time
StandardBias	REG_DWORD	0x00000000 (0)
StandardStart	REG_BINARY	00 00 0A 00 05 00 02 00 00 00 00 00 00 00 00 00
DaylightName	REG_SZ	GMT Standard Time
DaylightBias	REG_DWORD	0xFFFFFC4 (4294967236)
DaylightStart	REG_BINARY	00 00 03 00 05 00 01 00 00 00 00 00 00 00 00 00
ActiveTimeBias	REG_DWORD	0x00000000 (0)

Figure 11: system registry hive OS effective time zone

2.4.3.2 User profiles information

A preliminary investigation into the Users folder identified three user profiles that had been created on the PC, detailed in Table 6 below:

Table 6: Summary of user profiles discovered

Username	Creation date/time
johndoe	24/01/05 15:56
bob	03/02/05 10:12
jane	03/02/05 11:23

2.4.3.3 Images

The built-in functionality of the Autopsy platform identified 1422 images within the johndoe.dd image file. The analyst was able to view these images from within the Autopsy Image/Video Gallery tool to assess their content, marking them as pertinent to the investigation where appropriate. Of note, Autopsy identified 101 photos that had been taken with a Canon Powershot Sd100, but no such camera was found during the property search of the suspect’s residence.

Through the use of the known good hashes file, which lists any .dll files that are to be expected within an operating system, Autopsy was able to identify a suspicious .dll file found in the WINDOWS directory. Upon further inspection, this file (“CrouchingKokako.dll”) was found to be an archive containing seven IIOB. Furthermore, the list of known good hashes enabled Autopsy to identify three non-standard files, none of which had a file extension, residing in a system directory (C:\Program Files) that upon investigation showed content of an ornithological nature.

Manual searching of the profile folder with the same name as the suspect uncovered an encrypted file named “birdpics.gpg”. Public and private encryption keys were found in the GPG program’s default location and were extracted from the image along with the encrypted file. Once the password for the private key (“arran”) was obtained using a password cracking suite installed on the Kali virtual machine, the encrypted file was able to be decrypted and was found to house an archive file containing five IIOB. The analyst noted that both keys had a creation date of 01:37 on 1st April 2003, suggesting that these keys had been used for encryption purposes prior to the installation of Windows of this PC.

Manual searching of the profile folders for the two other user profiles discovered on the PC (“bob” and “jane”) failed to uncover any further incriminating evidence.

The built-in functionality of the Autopsy platform identified a file (“FantailFrontView.exe”) with a mismatched extension that, upon investigation, proved to be an image of ornithological nature.

Manual searching of the orphaned files identified by Autopsy revealed a further 24 IIOB.

All images discovered by the processes detailed above were extracted from the johndoe.dd image, along with their MD5 hash values. The analyst used Microsoft Excel to remove any duplicate image files using the hashes. A total of 104 unique IIOB were discovered, which are presented in Appendix A - Recovered Images. Their MD5 hash values are presented in Appendix L - List of Evidentiary Files with MD5 Hashes. The contents of the IIOB could be categorised as follows:

- Images of adult birds.
- Images of baby birds
- Animated images of birds.
- Images of people and birds.
- Images of people touching birds.
- Images of people wearing bird costumes.
- Images of bird-adjacent objects (e.g. a nesting box).

2.4.3.4 Videos

There were five video files identified by the Autopsy platform. None of these files contained any suspicious content.

2.4.3.5 Documents

The built-in functionality of the Autopsy platform identified a total of 438 documents within the johndoe.dd image file, broken down into categories as detailed in Table 7 below:

Table 7: Summary of document types discovered by Autopsy

Type of file	Number of occurrences
HTML	224
Office	17
PDF	17
Plain Text	480

The analyst was able to view these documents from within Autopsy to assess their content, marking them as pertinent to the investigation where appropriate. The metadata was also examined for any Microsoft Word documents (.doc files), uncovering an original file title of “Birds To Find” for a document named “stuf.doc”.

A keyword search was initiated using a list generated partially from the data discovered during the image discovery phase. The resulting list can be seen in Figure 12 below:

Keyword
bird
brd
kea
frank
sibley
bc7
christine
scot
ben
wing
warbler
flycatcher
hawk
owl
wren
cockatoo
birds

Figure 12: list of terms used for keyword search

Within the results of this keyword search, a system file (ODBC.INI) was marked as matching one of the search terms. Upon further investigation (possible from within the Autopsy platform), the file contents showed material of an ornithological nature.

A total of 16 pertinent documents were discovered, which are presented in Appendix B - Documents. Their MD5 hash values are presented in Appendix L - List of Evidentiary Files with MD5 Hashes. The accompanying metadata discoveries can be found in Appendix C - Metadata.

2.4.3.6 E-mails

The built-in functionality of the Autopsy platform identified a total of 4 unique e-mail messages within the johndoe.dd image file, summarised in Table 8 below:

Table 8: Summary of e-mails discovered by Autopsy

Sender e-mail	Recipient e-mail	Date received	Subject line
mailinglist@birds.example.com	johndoe@example.com	16/10/04 15:20	How to Identify Birds
ben@example.org	johndoe@example.com	17/11/04 19:20	expensive birds
ben@example.org	johndoe@example.com	09/02/05 11:08	good pics
ben@example.org	johndoe@example.com	09/02/05 11:08	some more good ones

The analyst was able to view these E-mails from within the Autopsy Communications tool to assess their content, finding all of them to be pertinent to the investigation. Both e-mails received on 9th February were found to contain IIOB attachments. The analyst chose to corroborate the findings from Autopsy by importing the mailbox file from the image into a Thunderbird client. The profile file was found in the default program location within the user profile folder for a user with the suspect's name.

Two of the e-mails received displayed a delivery date that falls prior to the installation of the operating system for the suspect's PC. This can be explained with an understanding that the Thunderbird e-mail client used to interact with the e-mails acts solely as a conduit for viewing the contents of an e-mail mailbox hosted in the cloud, rather than on a PC itself.

The e-mails are presented in Appendix D - E-mails, with the images presented within Appendix A - Recovered Images. Any relevant MD5 values can be found in Appendix L - List of Evidentiary Files with MD5 Hashes.

2.4.3.7 Audio files

The built-in functionality of the Autopsy platform identified 42 audio files within the johndoe.dd image file. The analyst was able to analyse these images from within the Autopsy tool to assess their content, marking them as pertinent to the investigation where appropriate. Of the 42 files identified, the analyst deemed one as relevant to the charges levied against the suspect ("aggressive_song.wav"). The MD5 value for this file can be found in Appendix L - List of Evidentiary Files with MD5 Hashes.

2.4.4 Internet history analysis

With the knowledge that there were two internet browsers (Internet Explorer and Firefox) installed on the suspect's PC, the analyst investigated the browsing history of each in turn.

2.4.4.1 Internet Explorer

The cache, history, and cookies index.dat files were extracted using Autopsy from their default locations within the profile folder with the name of the suspect. The analyst then used Pasco (in undelete mode to ensure that any deleted history would be captured) to extract the information from these files into a human-readable format.

There was evidence in the history index.dat file that the suspect had used Internet Explorer to search for and download software that would support the incidents detailed in the Description of Crime. Between 15:57 and 16:41 on 24th January 2005, a period of browsing activity shows that the suspect searched for Microsoft Updates. During this time, he also searched for and downloaded the installation files for Firefox and Thunderbird. A summary of these actions can be seen exhibit 0.3 of Appendix E - Internet History Analysis.

The analyst noted another period of internet activity between 14:18 and 15:04 on 2nd February 2005, this time showing evidence that the suspect had navigated to the RealPlayer website, as shown in Figure 13 below:

2005-02-02 14:57:24	http://home.real.com/signin/common/log/log.html?toolbar=Google&action=istool...
2005-02-02 15:04:16	http://i.real.com/g/pics/space.gif
2005-02-02 15:04:19	real.com/
2005-02-02 15:04:24	http://www.real.com/intro/index.html?DC=NSP01D&optin=true&country=gb&lang...
2005-02-02 15:04:25	http://realguide.real.com/4plus/main_.js
2005-02-02 15:04:25	http://www.real.com/intro/index_upsell_manager.html?DC=NSP01D&optin=true&c...
2005-02-02 15:04:25	http://www.real.com/4plus/trinity_.css
2005-02-02 15:04:26	http://i.real.com/pics/real/intro/btn_disabled.gif
2005-02-02 15:04:27	http://images.real.com//pics/space.gif
2005-02-02 15:04:27	http://images.real.com//pics/real/common/bull_tri.gif
2005-02-02 15:04:28	http://www.real.com/intro/index_upsell_manager.html?DC=NSP01D&optin=true&c...
2005-02-02 15:04:30	http://i.real.com/pics/real/intro/btn_enabled.gif
2005-02-02 15:04:34	javascript:catchEvent('continue');
2005-02-02 15:04:34	https://account.real.com/acct/intro/msg.html?msg=frweur
2005-02-02 15:04:34	http://i.real.com/pics/real/intro/btn_down.gif
2005-02-02 15:04:34	http://i.real.com/pics/real/intro/btn_over.gif
2005-02-02 15:04:34	https://account.real.com/acct/intro/msg.html?msg=frweur

Figure 13: Entries from IE index.dat file showing visits to the RealPlayer website

There was no incriminating evidence found in the cache and cookies index.dat files, nor in the Favorites folder or auto-complete data for this same profile. All relevant findings from the history index.dat file are presented in Appendix E - Internet History Analysis. Any relevant MD5 values can be found in Appendix L - List of Evidentiary Files with MD5 Hashes.

The cache, history, and cookies index.dat files belonging to the two other user profiles discovered on the PC (“bob” and “jane”) did not contain any incriminating evidence.

The analyst then utilised the find command on the Kali virtual machine to locate any other “index.dat” files present within the image. Any discovered index.dat files were enumerated using Pasco in undelete mode as before. No incriminating evidence was found in any of these files.

2.4.4.2 Firefox

The cache files were extracted using Autopsy from their default location within the profile folder with the name of the suspect. The analyst then used MZCacheView to view the information from these files in a graphical format and make a note of any items pertinent to the investigation. This process was repeated with the history and cookies files, using MZHistoryView and MZCookieView respectively.

There was evidence in the history file that the suspect had used Firefox to search for and download software that would support the incidents detailed in the Description of Crime. Between 14:10 and 16:52 on 2nd February 2005, a period of browsing activity shows that the suspect searched for and downloaded the installation files for PGP and Adobe Reader, as demonstrated in Figure 14 below:

http://www.google.co.uk/search?q=windows+gnupg&sourceid=mozilla-search&start=0&start=0&ie=utf-8&oe=utf-8&client=firefox-a&rls=org.mozilla:en-GB:official	02/02/2005 15:57:40
http://www.gnupg.org/download.html	02/02/2005 15:57:51
http://www.gnupg.org/download/	02/02/2005 15:57:51
http://www.winpt.org/	02/02/2005 15:58:23
http://www.stud.uni-hannover.de/~twoaday/winpt.html	02/02/2005 15:58:23
http://www.google.co.uk/search?q=windows+gnupg&hl=en&lr=&client=firefox-a&rls=org.mozilla:en-GB:official&start=10&sa=N	02/02/2005 15:58:48
http://openpgp.vie-privee.org/wingpg.html	02/02/2005 15:58:58
http://shell.windows.com/fileassoc/0409/xml/redir.asp?Ext=pdf	02/02/2005 16:51:54
http://shell.windows.com/fileassoc/0409/SearchEngine.asp	02/02/2005 16:51:54
http://www.adobe.com/products/acrobat/readstep2.html	02/02/2005 16:52:06
http://www.adobe.com/products/acrobat/readstep_serverfile.html?hasjavascript=1&esdcanbeused=1&esdcanhandle=0&language=English&platform=WinXP&connectio...	02/02/2005 16:52:50
http://ardownload.adobe.com/pub/adobe/reader/win/7x/7.0/enu/AdbeRdr70_enu_full.exe	02/02/2005 16:53:13

Figure 14: MZHistory view of Firefox history.dat file showing search and download of GPG and Adobe Reader

All further relevant findings to the incidents as detailed in the Description of Crime from the cache and history files are presented in Appendix E - Internet History Analysis. Any relevant MD5 values can be found in Appendix L - List of Evidentiary Files with MD5 Hashes.

Whilst there were a number of cookies within the cookies file that pertain to suspicious activity, the date of creation of these cookie files is not retained within the cookie file, as can be seen in Figure 15.

Domain/Host	Path	Name	Value	Last Accessed	Created Time
112.20.7.net	/	s_viihenx7Cxxhd7Ex60	[CS]v4 4200E7360006854-A000BA400000001 4200E735[CE]		
about.com	/	Amnc	N		
about.com	/	gs	birding		
about.com	/	zFD	52280520810500801		
about.com	/	referrer	http://about.com		
about.com	/	trailblazer	referrer=<http://birding.about.com/library/weekly/aa010703a.htm>		
about.com	/	TID	0mfh7z21101oe		
about.com	/	jsc	13		
about.com	/	TMog	522EM0020SA1B0c		
advertising.com	/	ROLL	ciZBMGzb1BT4K3vhdMSXYioZoz+TN3K!		
advertising.com	/	ACID	bb090011073552260010!		
advertising.com	/	BASE	ms1gBNakPyPLDr+eQSXr/cjb/wrU5feDqZS1N!		
amazon.co.uk	/	ubid-acbuk	432-0491950-8565500		
atdm.com	/	AA002	001107354287-989877906/1108563887		
audiencematch.net	/	TID	0mfh7z21101peg		
bbc.co.uk	/	BBC-UID	24a239f0ec70333475fdcd4a188e366767cf3377010c018a002cab072...		
bbc.co.uk	/	BBCMediaSelector	murmRbb		
birding.about.com	/	zFS	52280520810500801		
casalemedia.com	/	CMX2	40842&107333757524C608		
casalemedia.com	/	CMID	41WW9kUsIDMAAGqltgAAAN		
doubleclick.net	/	id	800004c8c7982		
fastclick.net	/	pluto	663483068 66b5a384-3d2e-44e2-9a8b-44094f4503db		
fastclick.net	/	m2	18809-1:45368:8:1107442877		
focalex.com	/	focalex_aa_p	o8&8&dAaa9m8CeURksdMKW65C2A		
google.co.uk	/	PREF	ID=61669b956c7ef5a1D=en TM=1106584100 LM=1106584100 S=...		
google.com	/	PREF	ID=ad3ac92f040d59a CR=1 TM=1106584100 LM=1106584100 S=...		
imdb.com	/	uu	0N3KNlgbcjldC08GFBcwgCVHxv2w+1NhZNNe/QGrj5VQN3bp...		
maxserving.com	/	uu	en92jGpVnRYT		
microsoft.com	/	MC1	GUID=31d3ee23c79ae349abcf98b8e27574b&HASH=23ee&LV=20...		
office.microsoft.com	/	awususerid	guid=45a3ad6c-4fa0-4e1b-b6a4-eed3400df84c		
office.microsoft.com	/	_DetectCookies	Y		
real.com	/	RNates	forms03-00kC8Y:3		
serveby.advertising.com	/	65413475	_4200e6a5,6431706035,684689^223368_		
serveby.advertising.com	/	19410806	_4200e65a,3229376194,689639^244838_		
serveby.advertising.com	/	80141706	_4200e65a,2726379568,689642^233315_		
serveby.advertising.com	/	8208981	_4200e684,9079152656,604689^242879_		
serveby.advertising.com	/	15326566	_4200e70c,5539309421,689991^232484_		
serveby.advertising.com	/	72136016	_4200e709,9535359602,689991^242222_		
serveby.advertising.com	/	23536105	_4200e70b,2209937515,689989^244838_		
shop.com	/	AMID	319429603		
office.microsoft.com	/	_DetectCookies	Y		
videodetective.com	/	videokrate	300		
www.adobe.com	/	AWID	130.159.248.44.175491107363127998		
www.googleadservices.com	/pagead/conversion/107269998/	Conversion	CnxCVz/MG850EFdkBREx1d/Fi5Gg55ndlaHRXRkNNck5zcYNC...		
www.hauths.com	/	session	first_visited_referer_id=BIRDING.ABOUT.COM&referer_id=BIRDIN...		
www.hauths.com	/	session%5Fsrc	src=		
www.remaxtop.com	/	visitor_id	9698879		

Figure 15: MZCookies showing contents of Firefox cookies file

The analyst extracted the data for the bookmarks file, located within the profile folder with the name of the suspect, using the Extracted Text feature of Autopsy. As the bookmarks file stores date/time information (for bookmark creation) in Epoch time, the analyst used an online converter (<https://www.epochconverter.com/>) to convert these values into a human-readable format. The analyst discovered three bookmarks pertinent to the investigation, which are presented in Appendix E - Internet History Analysis. Any relevant MD5 values can be found in Appendix L - List of Evidentiary Files with MD5 Hashes.

The downloads file was extracted using Autopsy from its default location within the profile folder with the name of the suspect. The analyst then used Firefox to view the information from this file in a graphical format and make a note of any items pertinent to the investigation. A total of eleven downloaded files with ornithological content were discovered, summarised in Table 9 below, with detailed findings presented in Appendix E - Internet History Analysis. The downloaded images are presented in Appendix A - Recovered Images. Any relevant MD5 values can be found in Appendix L - List of Evidentiary Files with MD5 Hashes.

Table 9: Breakdown of downloads discovered

Type of file	Number of occurrences
Image	8
Audio	2
Archive (.zip)	1

One of the audio files downloaded, “dawn.ram”, allowed the analyst to identify a second file with this extension type that had also been downloaded. This second file was located within the image and whilst it was not possible to play the discovered file, the file name (“kakapo.ram”) would suggest the contents were of an ornithological nature, a kakapo being a species of bird. Similarly, the analyst was not able to play the contents of the discovered “dawn.ram” file, however its contents (a URL for the streaming media located at audio.pbs.org/songs/dawn.rmd) would suggest that this file was also of an ornithological nature.

There were no SQLite files (for holding information of any typed URLs) available for inspection or any incriminating evidence found in the auto-complete data for this same profile.

The Firefox files belonging to the two other user profiles discovered on the PC (“bob” and “jane”) did not contain any incriminating evidence.

Whilst the pertinence of the majority of the internet history was obvious by way of naming conventions (e.g. birding.about.com), there were a number of URLs whose content was not obvious from their description or wording. Furthermore, these websites were no longer live at the time of the investigation, specifically those of [VideoDetective.com](http://videodetective.com). In these instances, the Analyst utilised an online resource, the Wayback Machine, to determine what the content of these URLs would have been at the time they were visited. An example of the result of this practice can be seen in Figure 16 below, which shows the website contained material of an ornithological nature.

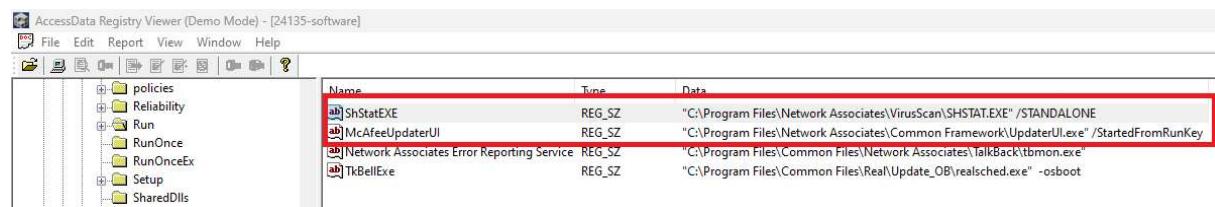
The screenshot shows a Wayback Machine archive of a VideoDetective.com page. At the top, it says "INTERNET ARCHIVE Wayback Machine https://videodetective.com/home.asp?PublishedID=1843 15 captures 14 Nov 2003 - 15 Nov 2024". Below this is a search bar with "SEARCH the largest preview archive on the web!" and dropdown menus for "Movie by title" and "go". A red box highlights the search bar and the date range. The main content area has a large blue banner saying "CLICK HERE TO WATCH PREVIEW". To the right, there's a movie card for "THE BIRDS (1963)" with details: director Alfred Hitchcock, cast Veronica Cartwright, Ethel Griffies, Jessica Tandy, Tippi Hedren, Suzanne Pleshette, Rod Taylor. It lists genres: Mystery-Suspense, studio: MCA Universal Home Video, and MPAA Rating: Not Rated. Below the movie card is a sidebar with "Related titles by genre" listing CRACKER (2003), PRIME SUSPECT (2003), LAW & ORDER: CRIMINAL INTENT SEASON 14 (2004), LAW & ORDER: CRIMINAL INTENT SEASON 3 (2004), and SOHO SQUARE (2002). At the bottom are buttons for "Rent DVDs Online", "FREE TRIAL", "Keywords", "SHOWTIMES IN JUST ONE CLICK", and "Buy from amazon.com". A small note "(advertisement)" is at the bottom left of the main content area.

Figure 16: Wayback Machine archived result for VideoDetective.com

2.4.5 Registry Analysis

The analyst used Registry Viewer to analyse the software, system, and SAM registry hives (including those belonging to any registry shadow copies), paying particular attention to registry keys outlined in guidance provided by the HackTricks and Hackers-Arise websites, making a note of any information pertinent to the investigation as it was discovered.

Upon inspection of the system registry hive, the analyst noted that an antivirus product and its auto-update mechanism were installed on the suspect's PC, and were scheduled to start automatically at start-up, as demonstrated in Figure 17 below. This would suggest that there were no malicious files detected on the suspect's computer at the time of its use.

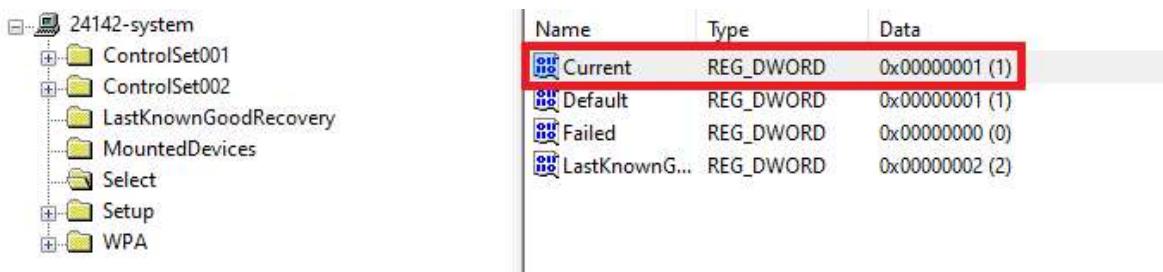


A screenshot of the AccessData Registry Viewer interface. The title bar reads "AccessData Registry Viewer (Demo Mode) - [24135-software]". The menu bar includes File, Edit, Report, View, Window, Help. The left pane shows a tree view of registry keys under "24142-system": policies, Reliability, Run, RunOnce, RunOnceEx, Setup, SharedDlIs. The right pane displays a table of registry keys under the "Run" key:

Name	Type	Data
ShStatEXE	REG_SZ	"C:\Program Files\Network Associates\VirusScan\SHSTAT.EXE" /STANDALONE
McAfeeUpdaterUI	REG_SZ	"C:\Program Files\Network Associates\Common Framework\UpdaterUI.exe" /StartedFromRunKey
Network Associates Error Reporting Service	REG_SZ	"C:\Program Files\Common Files\Network Associates\talkBack\btmon.exe"
TkBellExe	REG_SZ	"C:\Program Files\Common Files\Real\Update_OB\realshed.exe" -osboot

Figure 17: Run key from software hive showing auto-start programs

For any keys being investigated in the ControlSet key, the analyst confirmed that the control set in use was "001", as can be seen in Figure 18. Both available ControlSet keys were analysed, with the analyst noting that those keys in the 001 set were the effective keys at the time of acquisition.



A screenshot of the AccessData Registry Viewer interface. The title bar reads "AccessData Registry Viewer (Demo Mode) - [24142-system]". The left pane shows a tree view of registry keys under "24142-system": ControlSet001, ControlSet002, LastKnownGoodRecovery, MountedDevices, Select, Setup, WPA. The right pane displays a table of registry keys under the "ControlSet001" key:

Name	Type	Data
Current	REG_DWORD	0x00000001 (1)
Default	REG_DWORD	0x00000001 (1)
Failed	REG_DWORD	0x00000000 (0)
LastKnownG...	REG_DWORD	0x00000002 (2)

Figure 18: Registry Viewer showing selected ControlSet at time of acquisition

Upon inspection of the system registry hive, the analyst discovered that the PC had previously been connected to the "strath.ac.uk" domain, as can be seen in Figure 19. Using an online DNS resolution service (<https://whois.com>), the analyst was able to ascertain that this domain was registered to The University of Strathclyde and as such provides a link between the PC and the suspect. The output from whois.com can be in Figure 20.

Interfaces	UncpServer	REG_SZ	130.159.184.9
{0417D2B7-A391-4CA4-89D15DAF-5CD5-4E57-\}	Lease	REG_DWORD	0x00003840 (14400)
{A4BE5220-C76D-4E74-\}	LeaseObtain...	REG_DWORD	0x420A27EA (1107961834)
PersistentRoutes	T1	REG_DWORD	0x420A440A (1107969034)
Winsock	T2	REG_DWORD	0x420A5922 (1107974434)
Performance	LeaseTermin...	REG_DWORD	0x420A602A (1107976234)
Security	IPAutoconfi...	REG_SZ	0.0.0.0
ServiceProvider	IPAutoconfi...	REG_SZ	255.255.0.0
TDPIPE	IPAutoconfi...	REG_DWORD	0x00000000 (0)
TDTCP	AddressType	REG_DWORD	0x00000000 (0)
TermDD	DhcpIpAddr...	REG_SZ	130.159.184.252
TermService	DhcpSubnet...	REG_SZ	255.255.254.0
Themes	DhcpNameS...	REG_SZ	130.159.185.254 130.159.196.92
TlntSvr	DhcpDefault...	REG_MULTI_SZ	130.159.185.254
Toslde	DhcpDomain	REG_SZ	cis.strath.ac.uk
	DhcpSubnet...	REG_MULTI_SZ	255.255.254.0

Figure 19: Network adapter information from the system registry hive

strath.ac.uk

Domain:
strath.ac.uk

Registered For:
The University of Strathclyde

Domain Owner:
University of Strathclyde

Registered By:
Jisc Services Limited

Servers:
dns0.strath.ac.uk 130.159.248.11
dns1.strath.ac.uk 130.159.248.9
ns4.ja.net

Registrant Contact:
Hostmaster

Registrant Address:
Information Services
100, Cathedral St
Glasgow
G4 0LN
+44 141 548 4444 (Phone)
hostmaster@strath.ac.uk

Renewal date:
Monday 11th May 2026

Entry updated:
Wednesday 13th November 2024

Entry created:
Wednesday 17th September 2003

Figure 20: whois.com DNS results for strath.ac.uk

The system hive also provided evidence of the use of five “drives” on the PC, as evidenced in Figure 21 below:

Name	Type	Data
\??\Volume{30bf5ac0-6e1f-11d9-a7bd-806d6172696f}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 46 00 44 00 43 00 23 00 47 00 ...
\??\Volume{30bf5ac1-6e1f-11d9-a7bd-806d6172696f}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 49 00 44 00 45 00 23 00 43 00 ...
\DosDevices\A:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 46 00 44 00 43 00 23 00 47 00 ...
\DosDevices\B:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 49 00 44 00 45 00 23 00 43 00 ...
\??\Volume{30bf5ac3-6e1f-11d9-a7bd-806d6172696f}	REG_BINARY	B8 DD B8 DD 00 7E 00 00 00 00 00 00
\DosDevices\C:	REG_BINARY	B8 DD B8 DD 00 7E 00 00 00 00 00 00
\??\Volume{44d36d3b-7525-11d9-ab5a-0048545652e0}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 53 00 54 00 4F 00 52 00 41 00 ...
\DosDevices\E:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 53 00 54 00 4F 00 52 00 41 00 ...
\??\Volume{44d36d43-7525-11d9-ab5a-0048545652e0}	REG_BINARY	B8 DD B8 DD 00 FC 47 BB 00 00 00 00
\DosDevices\F:	REG_BINARY	B8 DD B8 DD 00 FC 47 BB 00 00 00 00

Figure 21: Utilised drives shown in the system hive

Of these, drives A:, C:, and D: are commonly used in Windows computing, usually designated as a floppy disk drive, CD drive, and system drive, respectively. There is further evidence in the system hive that the E: drive letter was allocated to a removable USB drive, demonstrated by the presence of the same ParentIdPrefix shown in Figures 20 and 21. No such USB drive was located during the search at the suspect’s residence.

\DosDevices\E:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 53 00 54 00 4F 00 52 00 41 00 ...
\??\Volume{44d36d43-7525-11d9-ab5a-0048545652e0}	REG_BINARY	B8 DD B8 DD 00 FC 47 BB 00 00 00 00
\DosDevices\F:	REG_BINARY	B8 DD B8 DD 00 FC 47 BB 00 00 00 00

00	5C 00 3F 00 3F 00 5C 00-53 00 54 00 4F 00 52 00	\-2-?-S-T-O-R-
10	41 00 47 00 45 00 23 00-52 00 65 00 6D 00 6F 00	A-G-E-#-R-e-m-o-
20	76 00 61 00 62 00 6C 00-65 00 4D 00 65 00 64 00	v-a-b-1-e-M-e-d-
30	69 00 61 00 23 00 37 00-26 00 32 00 66 00 62 00	i-a-#-7-&2-f-b-
40	34 00 32 00 37 00 64 00-63 00 26 00 30 00 26 00	4-2-7-d-c-&-0-g-
50	52 00 4D 00 23 00 7B 00-35 00 33 00 66 00 35 00	R-M-#-(1-5-3-f-5-
60	36 00 33 00 30 00 64 00-2D 00 62 00 36 00 62 00	6-3-0-d--b-6-b-
70	66 00 2D 00 31 00 31 00-64 00 30 00 2D 00 39 00	f--1-1-d-0--9-
80	34 00 66 00 32 00 2D 00-30 00 30 00 61 00 30 00	4-f-2--0-0-a-0-
90	63 00 39 00 31 00 65 00-66 00 62 00 38 00 62 00	c-9-1-e-f-b-8-b-
a0	7D 00	1.

Figure 22: E: drive mount details

AccessData Registry Viewer (Demo Mode) - [24142-system]

Name	Type	Data
DeviceDesc	REG_SZ	Disk drive
Capabilities	REG_DWORD	0x00000010 (16)
UINumber	REG_DWORD	0x00000000 (0)
HardwareID	REG_MULTI_SZ	USBSTOR\Disk_____USB_DISK_____1.05 USBSTOR...
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW
ClassGUID	REG_SZ	{4D36E967-E325-11CE-BFC1-08002BE10318}
Service	REG_SZ	disk
ConfigFlags	REG_DWORD	0x00000000 (0)
ParentIdPrefix	REG_SZ	7&2fb427dc&0
Driver	REG_SZ	{4D36E967-E325-11CE-BFC1-08002BE10318}\0002
Class	REG_SZ	DiskDrive
Mfq	REG_SZ	(Standard disk drives)
FriendlyName	REG_SZ	USB DISK USB Device

Figure 23: E: ParentIdPrefix matching and device description

The system hive entry for the F: drive was absent of any information regarding the device it had been attached to, as shown in Figure 24. This suggests that the drive was not actively mounted to the F: drive at the time the acquisition was made.

AccessData Registry Viewer (Demo Mode) - [24142-system]

Name	Type	Data
??\Volume{30bf5ac0-6e1f-11d9-a7bd-806d6172696f}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 46 00 44 00 43 00 23 00 47 00 ...
??\Volume{30bf5ac1-6e1f-11d9-a7bd-806d6172696f}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 49 00 44 00 45 00 23 00 43 00 ...
(DosDevices)\A:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 46 00 44 00 43 00 23 00 47 00 ...
(DosDevices)\B:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 49 00 44 00 45 00 23 00 43 00 ...
??\Volume{30bf5ac3-6e1f-11d9-a7bd-806d6172696f}	REG_BINARY	B8 DD B8 DD 00 7E 00 00 00 00 00 00
(DosDevices)\C:	REG_BINARY	B8 DD B8 DD 00 7E 00 00 00 00 00 00
??\Volume{44d36d3b-7525-11d9-ab5a-0048545652e0}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 53 00 54 00 4F 00 52 00 41 00 ...
(DosDevices)\E:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 53 00 54 00 4F 00 52 00 41 00 ...
??\Volume{44d36d43-7525-11d9-ab5a-0048545652e0}	REG_BINARY	B8 DD B8 DD 00 FC 47 BB 00 00 00 00
(DosDevices)\F:	REG_BINARY	B8 DD B8 DD 00 FC 47 BB 00 00 00 00

Figure 24: F: drive mount details

Any further findings from the system registry hive relevant to the incidents as detailed in the Description of the Crime are presented in Appendix F - Registry Analysis. Any relevant MD5 values can be found in Appendix L - List of Evidentiary Files with MD5 Hashes.

The NTUSER.DAT hives for all three user profiles discovered on the PC (“bob”, “jane”, and “johndoe”) were inspected using Autopsy. The analyst made a note of any information pertinent to the investigation as it was discovered. No incriminating evidence was discovered in the files belonging to the “bob” or “jane” profiles. All findings from the NTUSER.DAT file belonging to the “johndoe” user relevant to the incidents as detailed in the Description of the Crime are presented in Appendix F - Registry Analysis. Any relevant MD5 values can be found in Appendix L - List of Evidentiary Files with MD5 Hashes.

2.4.5.1 Password enumeration

The analyst used Registry Viewer with the SAM and system registry hives to extract the NT hashes for each of the user profiles discovered on the PC (“bob”, “jane”, and “johndoe”). These were then entered into an online password cracking tool, the results of which can be found in Table 10 below:

Table 10: Cracked passwords for user profiles

Username	NT hash	Password
bob	8132FD27546995C4DC43D50C554705A8	bob
jane	4114F17BA8142A1B4093367031A58A83	jane
johndoe	B7C899154197E8A2A33121D76A240AB5	doe

The analyst noted that whilst the discovery that all three user accounts were protected with a password, the passwords chosen were of a very weak standard, being absent of a mixture of alphanumeric characters and symbols, having very short lengths, and all being easily to guess when taking the username into account.

2.4.6 Event Log Analysis

After extracting the event log files from the image using Autopsy, Event Viewer was used to view their contents. Most of the logs were corrupted, as can be seen in Figure 25. No incriminating evidence was found in the logs that were readable.

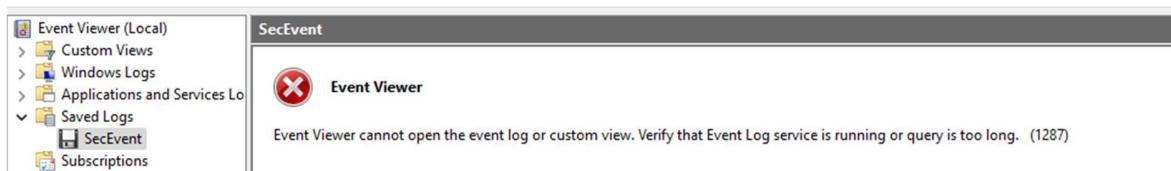


Figure 25: Event Viewer error message when trying to open event log files

2.4.7 Printer Spool File Analysis

The analyst attempted to enumerate any available printer spool files from within Autopsy but none were available, as can be seen in Figure 26 below:

/img_johnDoe.dd/vol_vol2/WINDOWS/system32/spool/PRINTERS							
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
[current folder]				2005-01-24 15:32:34 GMT	2005-01-24 15:32:34 GMT	2005-02-09 08:18:13 GMT	2005-01-24 15:32:34 GMT
[parent folder]				2005-01-24 15:32:34 GMT	2005-01-24 15:32:34 GMT	2005-02-09 08:18:13 GMT	2005-01-24 15:56:28 GMT

Figure 26: Autopsy file view showing absence of printer spool files

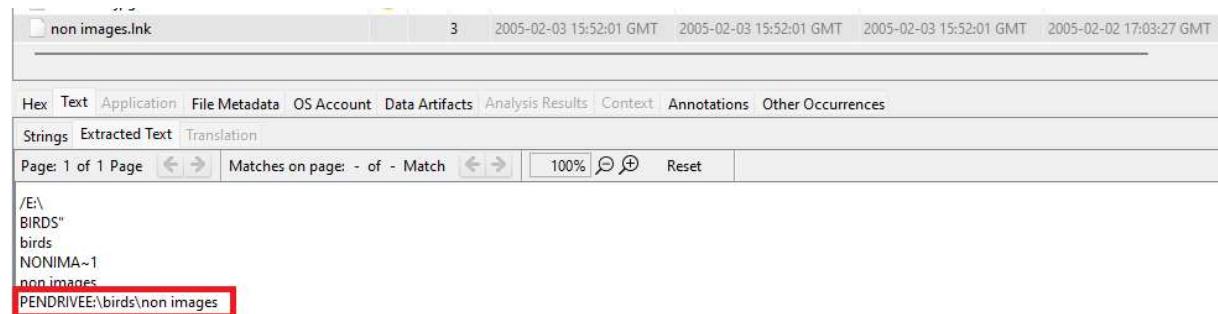
2.4.8 Pagefile.sys Analysis

After extracting the pagefile.sys file from the image using Autopsy, Notepad++ was used to view its contents. The analyst noted what whilst the file contained a large number of pieces of pertinent information to the charges levied against the suspect, the file (by its very nature) was devoid of any date/time information.

2.4.9 Recent Documents analysis

In addition to the evidence found in the Recent Documents key in the NTUSER.DAT registry hive belonging to the user “johndoe”, the analyst used the file browser within Autopsy to analyse the contents of two “recent documents” directories, making a note of any pertinent information as it was discovered. Both directories were found at the default locations within the profile folder with the name of the suspect.

Upon inspection of the “Recent” folder belonging to the suspect, the analyst found further evidence of a removable drive being accessed, as can be seen in Figure 27 below:



The screenshot shows the Notepad++ interface with the file 'non images.lnk' open. The search results pane displays the following text:
/E:\
BIRDS"
birds
NONIMA~1
non images
PENDRIVEE\birds\non images

Figure 27: Evidence of a removable drive found in the "Recent" directory

Furthermore, the analyst found evidence that files had been accessed from a CD, as demonstrated in Figure 28. The files could not be located within the image and their file names do not allow for determination of their content. No such CD was found during the search at the suspect's premises.

<input type="checkbox"/> Prac4.lnk	▼	2	2005-02-02 15:10:16 GMT	2005-02-02 15:10:16 GMT	2005-02-03 14:49:57 GMT	2005-02-02 15:10:16 GMT
<input type="checkbox"/> Q3 Thread (Statechart).lnk		2	2005-02-02 15:10:48 GMT	2005-02-02 15:10:48 GMT	2005-02-03 14:49:59 GMT	2005-02-02 15:10:48 GMT
<input type="checkbox"/> ready2fledge.jpg.lnk		2	2005-02-03 15:06:42 GMT	2005-02-03 15:06:42 GMT	2005-02-03 15:06:42 GMT	2005-02-03 15:06:42 GMT
<input type="checkbox"/> Sample Music.lnk		2	2005-02-03 14:17:48 GMT	2005-02-03 14:17:48 GMT	2005-02-03 14:49:38 GMT	2005-02-03 14:17:48 GMT
<input type="checkbox"/> stuf.doc.lnk	▼	2	2005-02-09 16:57:49 GMT	2005-02-09 16:57:49 GMT	2005-02-09 16:57:49 GMT	2005-02-09 16:57:49 GMT
<input type="checkbox"/> WINDOWS.lnk		2	2005-02-03 15:54:06 GMT	2005-02-03 15:54:06 GMT	2005-02-03 15:54:06 GMT	2005-02-03 15:54:06 GMT

<input type="checkbox"/> Q3 Thread (Statechart).lnk	2	2005-02-02 15:10:48 GMT	2005-02-02 15:10:48 GMT	2005-02-03 14:49:59 GMT	2005-02-02 15:10:48 GMT
<input type="checkbox"/> ready2fledge.jpg.lnk	2	2005-02-03 15:06:42 GMT	2005-02-03 15:06:42 GMT	2005-02-03 15:06:42 GMT	2005-02-03 15:06:42 GMT
<input type="checkbox"/> Sample Music.lnk	2	2005-02-03 14:17:48 GMT	2005-02-03 14:17:48 GMT	2005-02-03 14:49:38 GMT	2005-02-03 14:17:48 GMT
<input type="checkbox"/> stuf.doc.lnk	▼	2	2005-02-09 16:57:49 GMT	2005-02-09 16:57:49 GMT	2005-02-09 16:57:49 GMT
<input type="checkbox"/> WINDOWS.lnk		2	2005-02-03 15:54:06 GMT	2005-02-03 15:54:06 GMT	2005-02-03 15:54:06 GMT

<input type="checkbox"/> Q3 Thread (Statechart).lnk	2	2005-02-02 15:10:48 GMT	2005-02-02 15:10:48 GMT	2005-02-03 14:49:59 GMT	2005-02-02 15:10:48 GMT
<input type="checkbox"/> ready2fledge.jpg.lnk	2	2005-02-03 15:06:42 GMT	2005-02-03 15:06:42 GMT	2005-02-03 15:06:42 GMT	2005-02-03 15:06:42 GMT
<input type="checkbox"/> Sample Music.lnk	2	2005-02-03 14:17:48 GMT	2005-02-03 14:17:48 GMT	2005-02-03 14:49:38 GMT	2005-02-03 14:17:48 GMT
<input type="checkbox"/> stuf.doc.lnk	▼	2	2005-02-09 16:57:49 GMT	2005-02-09 16:57:49 GMT	2005-02-09 16:57:49 GMT
<input type="checkbox"/> WINDOWS.lnk		2	2005-02-03 15:54:06 GMT	2005-02-03 15:54:06 GMT	2005-02-03 15:54:06 GMT

Figure 28: Evidence of a CD found in the "Recent" directory

No incriminating evidence was discovered in the directories belonging to the “bob” or “jane” profiles. All relevant findings to the incidents as detailed in the Description of the Crime from the “recent documents” directories are presented in Appendix G - Recent Documents Analysis.

2.4.10 Prefetch analysis

After extracting the prefetch files (located within the default location for files of this type on Windows XP) from the image using Autopsy, WinPrefetchView was used to view their contents, with the analyst noting any pertinent information as it was discovered.

Upon inspection of the prefetch files, the analyst noted that the cookies.txt file contained within the Firefox profile belonging to the user “johndoe” had been opened with Notepad, as evidenced in Figure 29. It is not possible to determine what changes, if any, were made to the cookies.txt file.

	NOTEPAD.EXE-336351...	03/11/2024 20:44...	03/11/2024 20:44...	18,204	NOTEPAD.EXE	\DEVICE\HARDDISKVOLUME1\WINDOWS\...	4	03/02/2005 15:54:06	No
	NTOSBOOT-B00DFAA...	03/11/2024 20:44...	03/11/2024 20:44...	479,216	NTVDM.EXE	\DEVICE\HARDDISKVOLUME1\WINDOWS\...	6	09/02/2005 03:09:55	No
	NTVDM.EXE-1A10A42...	03/11/2024 20:44...	03/11/2024 20:44...	14,684	NTVDM.EXE	\DEVICE\HARDDISKVOLUME1\WINDOWS\...	1	03/02/2005 14:45:16	No
	READER_SELXE-3614F...	03/11/2024 20:44...	03/11/2024 20:44...	12,768	READER_SELXE	\DEVICE\HARDDISKVOLUME1\PROGRAM F...	4	09/02/2005 11:03:50	No
	REALONMESSAGECE...	03/11/2024 20:44...	03/11/2024 20:44...	16,688	REALONMESSAGEC...	\DEVICE\HARDDISKVOLUME1\PROGRAM F...	7	09/02/2005 17:01:34	No
	REALPLAY.EXE-1BF21...	03/11/2024 20:44...	03/11/2024 20:44...	65,982	REALPLAY.EXE	\DEVICE\HARDDISKVOLUME1\PROGRAM F...	296	09/02/2005 17:03:54	No
	REALPLAY_MOUNTP...	03/11/2024 20:44...	03/11/2024 20:44...	36,128	REALPLAY_MOUNTP...	\DEVICE\HARDDISKVOLUME1\PROGRAM F...	1	02/02/2005 14:51:05	No
	REALSCHED.EXE-3282...	03/11/2024 20:44...	03/11/2024 20:44...	22,638	REALSCHED.EXE	\DEVICE\HARDDISKVOLUME1\PROGRAM F...	15	09/02/2005 11:03:47	No
	REGSVR32.EXE-3080249...	03/11/2024 20:44...	03/11/2024 20:44...	9,468	REGSVR32.EXE	\DEVICE\HARDDISKVOLUME1\DOCUMENT...	1	02/02/2005 16:32:06	No
	REGEDIT.EXE-1B60648...	03/11/2024 20:44...	03/11/2024 20:44...	18,788	REGEDIT.EXE	\DEVICE\HARDDISKVOLUME1\WINDOWS\...	7	02/02/2005 14:50:55	No
	REGSVR32.EXE-25EFFE...	03/11/2024 20:44...	03/11/2024 20:44...	52,070	REGSVR32.EXE	\DEVICE\HARDDISKVOLUME1\WINDOWS\...	14	03/02/2005 11:23:17	No
	RNXPROC.EXE-1CD9A...	03/11/2024 20:44...	03/11/2024 20:44...	13,872	RNXPROC.EXE	\DEVICE\HARDDISKVOLUME1\PROGRAM F...	1	02/02/2005 15:04:21	No
	RPHelperApp.exe-33...	03/11/2024 20:44...	03/11/2024 20:44...	24,448	RPHelperApp.exe	\DEVICE\HARDDISKVOLUME1\PROGRAM F...	7	09/02/2005 17:01:19	No
	RUNDLL32.EXE-13C3...	03/11/2024 20:44...	03/11/2024 20:44...	16,352	RUNDLL32.EXE	\DEVICE\HARDDISKVOLUME1\WINDOWS\...	2	02/02/2005 15:08:22	No
	RUNDLL32.EXE-155CD...	03/11/2024 20:44...	03/11/2024 20:44...	0			0		No

Filename /	Full Path	Device Path	Index
		\DEVICE\HARDDISKVOLUME1\\$MFT	39
		\DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\ALL USERS\APPLICATION DATA\NETWORK ASSOCIATES\BOPDATA_DATE-20050202_TIME-123526620_ENTERCEPTE...	32
		\DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\ALL USERS\APPLICATION DATA\NETWORK ASSOCIATES\BOPDATA_DATE-20050202_TIME-123526620_ENTERCEPTR...	33
		\DEVICE\HARDDISKVOLUME1\WINDOWS\APPATCH\AGGENERAL.DLL	18
		\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\ADVAPI32.DLL	10
		\DEVICE\HARDDISKVOLUME1\WINDOWS\WIN32SX\86_MICROSOFT.WINDOWS.COMMON-CONTROLS_6595B64144CCF1DF_6.0.2600.2180_X-WW_A84F1FF9\COMCTL32.DLL	12
		\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\COMDI32.DLL	5
		\DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\JHNDOB\APPLICATION DATA\Mozilla\FIREFOX\PROFILES\W4NF3BL.DEFAULT\COOKIES.TXT	38

Figure 29: WinPrefetchView displaying use of Notepad to open cookies.txt

There was also evidence to suggest that the registry had been edited using the built-in Windows tool, Registry Editor, as shown in Figure 30. As with the cookies.txt file, it is not possible to ascertain what changes, if any, were made to the registry at the time.

	REGEDIT.EXE-1B60648...	03/11/2024 20:44...	03/11/2024 20:44...	18,788	REGEDIT.EXE	\DEVICE\HARDDISKVOLUME1\WINDOWS\...	7	02/02/2005 14:50:55	No
--	------------------------	---------------------	---------------------	--------	-------------	-------------------------------------	---	---------------------	----

Figure 30: WinPrefetchView displaying opening of Registry Editor

All further relevant findings to the incidents as detailed in the Description of the Crime from the prefetch files are presented in Appendix H - Prefetch Analysis. Any relevant MD5 values can be found in Appendix L - List of Evidentiary Files with MD5 Hashes.

2.4.11 Recycling Bin examination

The analyst used the file explorer within Autopsy to analyse the contents of both Recycling Bin instances (one for each partition). Upon inspection of the Recycling Bin attached to the partition in the allocated space, the analyst noted that there was evidence of some files that would have been pertinent to the investigation being deleted, but this could not be verified with any date/time information. This finding can be seen in Figure 31 below. Whilst there were traces of all three of these documents found in other sources (pagefile.sys and the prefetch files), no files of these names could be found within the image.

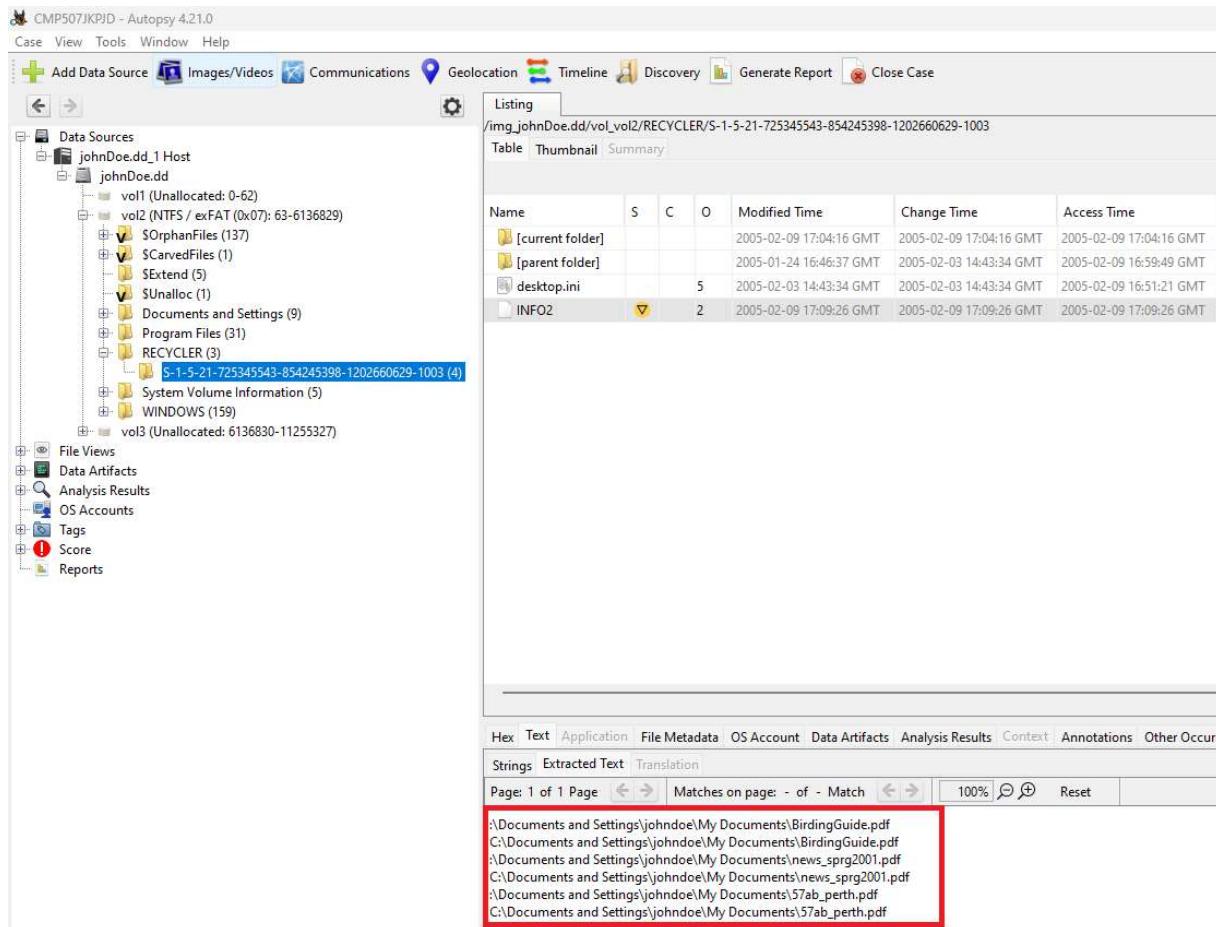


Figure 31: Contents of the INFO2 file from the Recycling Bin in the allocated space partition

All further relevant findings to the incidents as detailed in the Description of the Crime are presented in Appendix I - Recycling Bin Analysis. Any relevant MD5 values can be found in Appendix L - List of Evidentiary Files with MD5 Hashes.

2.4.12 Timeline creation

Along with the findings discovered during the investigation, the analyst used the Timeline feature of Autopsy guide and inform the creation of the timeline, a summary image of which can be found in Figure 32 below, which shows periods of user inactivity (characterised by a lack of blue or green areas on the chart) and PC inactivity (characterised by an absence of red, blue, or green areas of the chart):

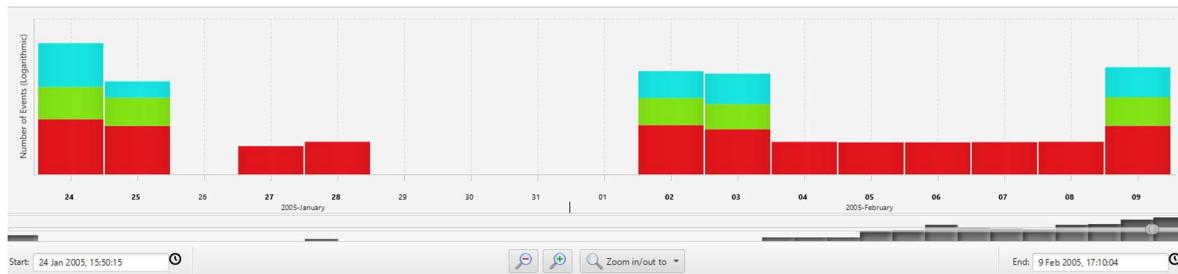


Figure 32: Timeline created by Autopsy

Using the timeline produced by Autopsy, the analyst was able to note when the programs that the suspect had previously searched for and downloaded the installation media for had been installed. All of the installations concerned occurred a short time after the search for the product had been conducted, as summarised in Table 11, with the relevant entries from the Timeline shown in Figure 33.

Table 11: Summary of programs installed

Name of program	Date/time of internet activity	Date/time of installation
Firefox	16:21 24/01/05	16:26 24/01/05
Thunderbird	16:23 24/01/05	16:32 24/01/05
RealPlayer	14:57 02/02/05*	14:50 02/02/05
PGP	15:58 02/02/05	16:32 02/02/05
Adobe Reader	16:53 02/02/05	17:00 02/02/05

⚡	2005-01-24 16:26:04	Mozilla Firefox (1.0) v.1.0 (en-GB) : :	Program Installed
⚡	2005-01-24 16:32:28	Mozilla Thunderbird (1.0) v.1.0 (en) : :	Program Installed
⚡	2005-02-02 14:50:04	RealPlayer : :	Program Installed
⚡	2005-02-02 14:50:49	RealJukebox 1.0 : :	Program Installed
⚡	2005-02-02 16:32:02	Windows Privacy Tools v.1.0rc2 : :	Program Installed
⚡	2005-02-02 17:00:18	Adobe Reader 7.0 v.7.0.0 : :	Program Installed

Figure 33: Program installation entries from Autopsy Timeline

The analyst was further able to determine that Microsoft Word 2003 was installed at 10:27 on 3rd February 2005, shortly before the creation of a Word document entitled “Dear Fred.doc” (saved in the “My Documents” folder for the user “bob”, this file contains no incriminating evidence). The installation entry for this program can be seen in Figure 34 below:

⚡	2005-02-03 10:27:51	Microsoft Office Professional Edition 2003 v.11.0.6361....	Program Installed
---	---------------------	--	-------------------

Figure 34: Microsoft Word installation entry from Autopsy Timeline

Furthermore, the Timeline allowed the analyst to identify a period of activity indicating that Windows Updates had been configured to apply automatically, as demonstrated in Figure 35, suggesting that the suspect was taking appropriate precautions to ensure that the PC was receiving security patches.

2005-02-09 03:00:33	Windows XP Hotfix - KB888302 v.20041207.111426 : :	Program Installed
2005-02-09 03:01:16	Windows XP Hotfix - KB890047 v.20041221.124506 : :	Program Installed
2005-02-09 03:01:33	Windows XP Hotfix - KB873333 v.20050114.005213 : :	Program Installed
2005-02-09 03:02:06	Windows XP Hotfix - KB867282 v.20050127.090417 : :	Program Installed
2005-02-09 03:02:18	Windows XP Hotfix - KB891781 v.20050110.165439 : :	Program Installed
2005-02-09 03:02:31	Windows XP Hotfix - KB887472 v.20041014.162858 : :	Program Installed
2005-02-09 03:02:42	Windows XP Hotfix - KB888113 v.20041116.131036 : :	Program Installed
2005-02-09 03:02:55	Windows XP Hotfix - KB885250 v.20050118.202711 : :	Program Installed

Figure 35: Installation of Microsoft Updates from Autopsy Timeline

* Upon inspection of the Firefox browser history relating to RealPlayer, it would appear that communication to the website did not commence until after installation of the program. This would suggest that the installation media was not obtained from the internet; possibly it was included within the Windows XP installation.

2.4.13 Steganography analysis

No evidence of any steganography tools was found within the image. As such, the analyst deemed steganography analysis unnecessary for the investigation.

2.4.14 File header analysis

No evidence of any hex editing tools was found within the image. As such, the analyst deemed header analysis unnecessary for the investigation.

2.5 PRODUCTION LIST AND ASSOCIATED DESCRIPTION

A list of productions can be found in Appendix L - List of Evidentiary Files with MD5 Hashes, along with details of the relevant containing Appendix and the MD5 hash of the original file.

3 CONCLUSIONS

A total of 104 images were recovered from the acquired image of the hard drive belonging to the suspect, as well as sixteen documents and four e-mails with ornithological content. Three audio files were also recovered. Investigation into the suspect's internet history uncovered twelve visits and three bookmarks to websites hosting ornithological material, as well as 49 searches for bird-related matter.

Evidence of interactions with the material concerned was found in the analysis of the registry and the recent documents directories of the PC. Furthermore, the internet history and timeline analysis provided evidence to show that these interactions were not accidental, intent being shown through the use of internet searches to find and download suitable software to interact with documents and audio files.

There was evidence showing that the suspect had saved an image to a user profile belonging to a user other than himself. The evidence also showed a number of other methods used to attempt to conceal the evidence, listed below:

- Encryption.
- Use of archive files.
- Use of a removable USB drive.
- Use of unallocated ("hidden") disk space.
- Mismatched file extensions.
- Absent file extensions.
- Non-standard data save locations.
- File deletion.

The internet history and timeline analysis provided evidence to show that the use of encryption was knowledgeable, being shown through the use of internet searches to find and download suitable software to perform the encryption. Furthermore, the creation date for the security keys used to perform the encryption showed that the suspect had a history of using encryption tools prior to his possession of the PC being analysed.

One of the e-mails recovered indicated that the suspect had previously sent material of an ornithological nature to a third party. Furthermore, the delivery date for two of the recovered e-mails showed that the suspect had a history of corresponding with other parties about ornithological matters prior to his possession of the PC being analysed.

Evidence linking the suspect, an employee of the University of Strathclyde, with the user account "johndoe" was found in document signed off by the suspect and in the details of a network connection used.

There was no evidence discovered of any malicious software present on the PC. Furthermore, there was evidence of antivirus software being active and updated on the PC, and that the Windows Update auto-update mechanism was enabled, ensuring that the system received the relevant security patches in a timely manner.

APPENDICES

APPENDIX A - RECOVERED IMAGES

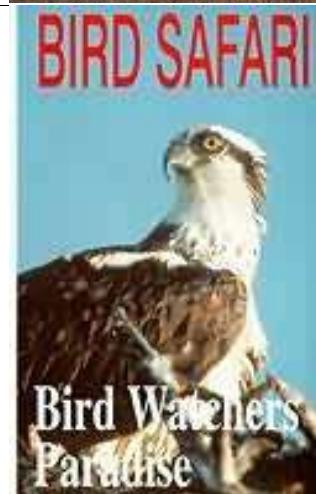
Incident #3

3.3 <i>Firefox wallpaper.bmp</i>	 A photograph showing two fluffy, downy bird chicks, likely penguins or albatrosses, nestled together in a nest made of dry grass and twigs. They have white feathers and dark, hooked beaks. The image is watermarked with "www.natureWallpaper.net".
3.4 <i>tn_duck_3.jpg</i>	 A photograph of a duck swimming on the surface of water. The duck has a dark head and neck with a distinctive white patch near its eye, and a light-colored body. Its reflection is clearly visible in the water.

3.5
snow_geese.jpg



3.6
7107298.jpg



3.7
40m.jpg



Incident #4 (birdpics.gpg/birdpics.zip contents)

4.1 <i>WhiteFacedHeronFlying.jpg</i>	 A white-faced heron is captured in mid-flight against a backdrop of blue water. The bird has long legs and a long neck, with its wings partially spread.	
4.2 <i>WhiteFrontedParrot.jpg</i>	 A white-fronted parrot is perched on a brown, thorny branch. The bird has vibrant green feathers with blue and yellow accents on its wings and a distinct red patch on its wing.	
4.3 <i>WhiteThroatedSparrowInTree.jpg</i>	 A white-throated sparrow is perched on a thin, bare branch. It is surrounded by small, round, orange-red berries. The bird has a white patch on its wing and a yellow patch on its side.	

4.4

WhoopingCranes.jpg



4.5

yellow-wag-cover-nb.jpg



surfbirds.com

Incident #5

5.1

AlmondMarshGreatBlueHeronStalling.jpg



5.2

BaldEagle7oClock.jpg



5.3

AmericanAvocetWinterPlumage.jpg



5.4

AmericanWhitePelicansCircling.jpg



5.5

BellbirdJumpingOffBranch.jpg



5.6

BarnOwl.jpg



5.7

BlackNeckedStiltsFromBehind.jpg



5.8

BlackSwan.jpg



5.9

BlackVultureSunningOnPost.jpg



5.10

blue_bird2.jpg



5.11

brd_Ornithologist_TWG.jpg



© Tim Gallagher

Incident #6 (crouchingkokako.dll contents)

6.1

brd_WoodDuck.jpg



© Marie Read

6.2

Brolga.jpg



6.3

BrushTurkeyPerching.jpg



6.4

CanadaGoose.jpg



6.5

CanadaGooseWashing.jpg



6.6

ChestnutMandibledToucan.jpg



6.7

CrouchingKokako.dll



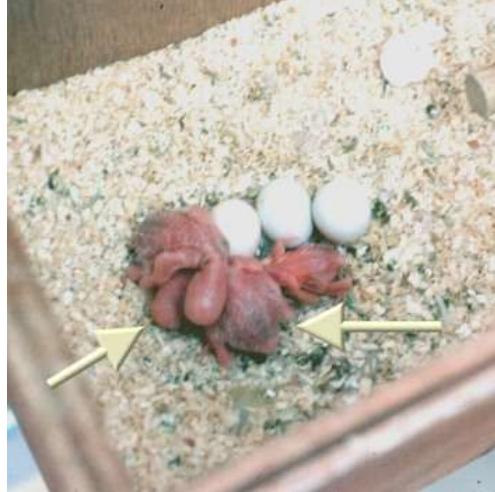
Incident #12

12.3

babyscot_2weeks.jpg



12.4
babyscot_vyoung.jpg



12.5
177.jpg



Everyone says you're too young for me.

12.6
birdtrans2.jpg



12.7
newbies2.jpg



12.8
chicks2.jpg



12.9
ready2fledge.jpg



Incident 13

13.1 <i>frankbeecostume_1827_34457581</i>		
13.2 <i>frankbeecostume_1827_84985892</i>		
13.3 <i>frankbeecostume_1827_96360352</i>		

Incident #14

14.3 <i>7EYBTELF1KAN.jpg</i>	 A photograph showing two parrots inside a large metal cage. One parrot is red and yellow, while the other is more multi-colored with blue, green, and yellow feathers. They are perched on branches or toys within the cage.	
14.4 <i>cute_penguin.jpg</i>	 A photograph of a balloon sculpture shaped like a penguin. The sculpture is primarily black with orange feet and a white belly. It has large, expressive blue eyes on its black head. The body is made of black balloons, and the feet are orange.	
14.5 <i>colorful-birds.jpg</i>	 A photograph of three vibrant lorikeets feeding on the ground. The birds have bright green bodies with distinct blue, yellow, and orange patches around their eyes and on their wings. They are eating from a pile of fallen fruit or seeds on a patch of green grass.	

14.6
*IMG_3937_filtered.j
pg*



14.7
gawall8.jpg



14.8
*BC7 feeding the
birds.jpg*



14.9

glfs-storm-birds.jpg



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

Incident #17

17.7

GreatBlueHeronWithFish.jpg



17.8

GreatEgretInVoloBog.jpg



17.9

GreatEgretOverflyingRoseateSpoonbills.jpg



17.10

GreenHeronCloseup.jpg



17.11

GreenHeronOnChicagoLakeshore.jpg



17.12

ImmatureSnowyEgretTakingOff.jpg



17.13

KeaAndMountain.jpg



17.14

KeaAtTopOfMacKinnonPass0930.jpg



17.15

KeaEatingRentalCar.jpg



17.16

KeaRetrievingBakedBeanCanFromTarn.jpg



17.17

june03screen.jpg



Cuban Tody © Pete Morris/Birdquest

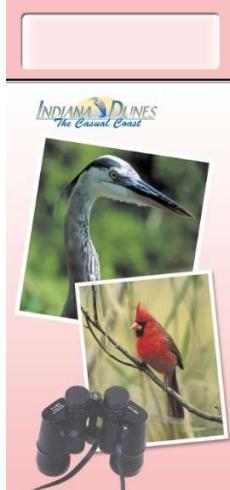
Surfbirds.com

17.18
junescreen01.jpg

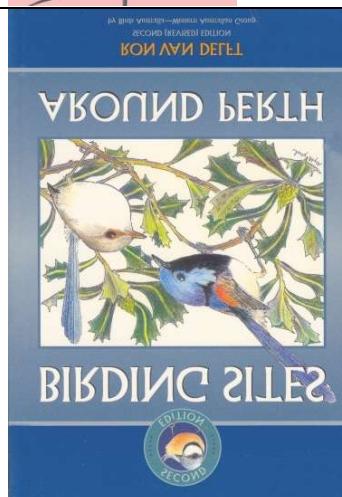


Incident #18

18.1
image0.jpg (1)



18.2
image0.jpg (2)



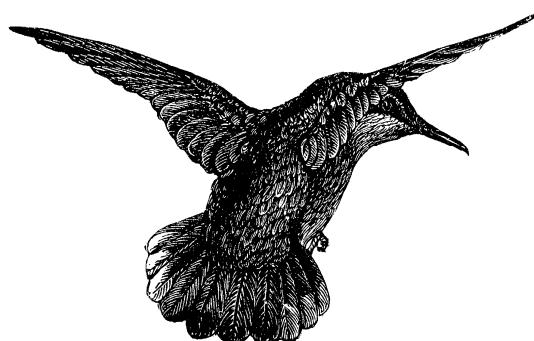
18.3
image1.jpg (1)



18.4
image1.jpg (1)



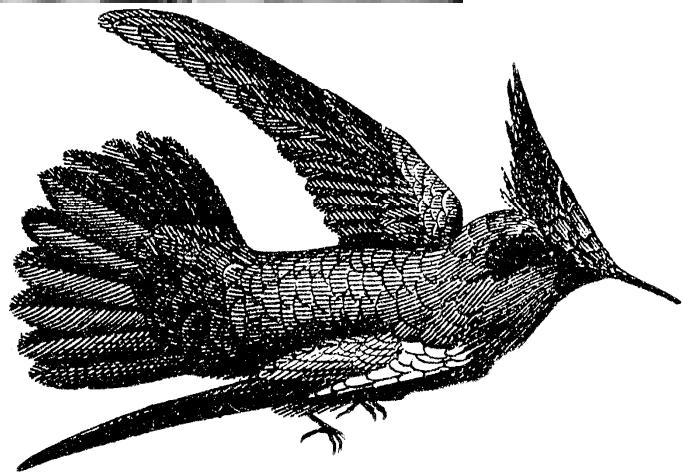
18.5
image1.tif



18.6
image12.jpg



18.7
image12.tif



18.8
image14.jpg



18.9
image15.jpg



Area Attractions:

• Miles from the shores of Lake Michigan
• Woodland Park (1 minute)
• 35 miles East of Chicago
• Variety of restaurants nearby

Amenities include:

- Manager's Reception (Mon-Thurs 5-7pm)
- Unique Spa Suites with Overized Jacuzzi Tubs
- Expanded Continental Breakfast
- Heated Indoor Pool and Fitness Center
- "Wildsuited" - Perfect for Families with Children
- Cable TV with HBO, CNN, ESPN
- "Snoopy" Movie Room
- Meeting and Banquet Facilities
- In-room Iron and Ironing Board

18.10
image16.jpg



18.11
image2.jpg



18.12
image26.jpg



18.13
image3.jpg



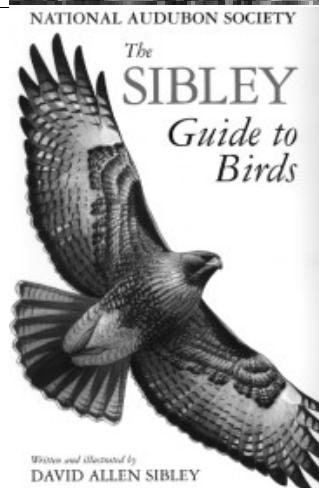
18.14
image33.jpg



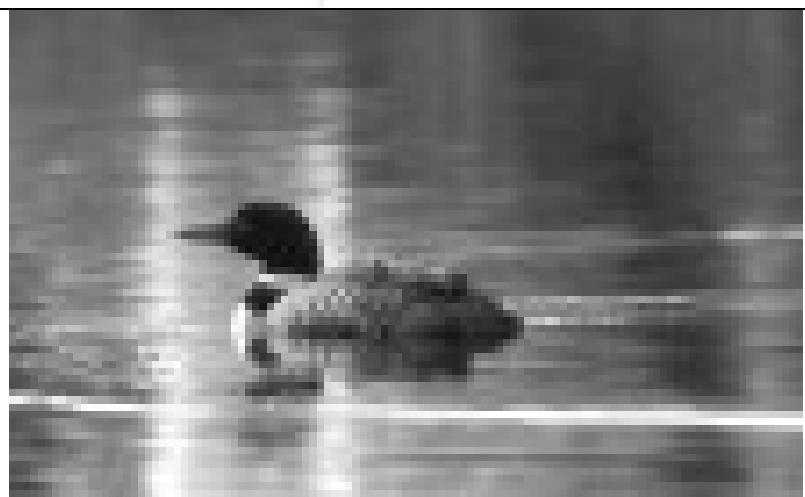
18.15
image4.jpg (1)



18.16
image4.jpg (2)



18.17
image5.jpg



18.18
image6.jpg



Incident #19

19.1
f0056920.jpg



19.2
f0438640.jpg



19.3
f0045880.jpg



19.4
f0056976.jpg



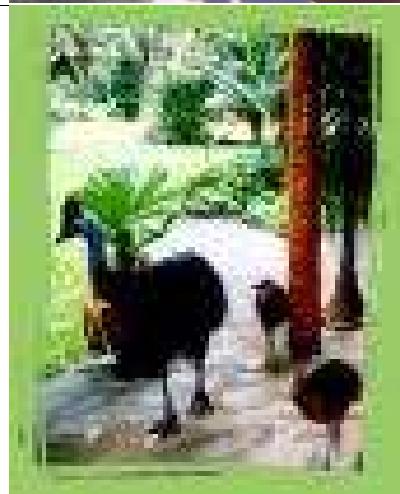
19.5
f0415008.jpg



19.6
f0441536.jpg



19.7
f0033912.jpg



19.8
f0310480.jpg



19.9
f0056944.jpg



19.10
f0056952.jpg



19.11
f0493176.jpg



19.12
f0443520.jpg



19.13
f0345656.jpg



19.14
f0592136.jpg



19.15
f0526960.jpg



19.16
f0387624.jpg



19.17
f0033928.jpg



19.18
f0533600.jpg



19.19
f0464568.jpg



19.20
f0416072.jpg



19.21
f0382464.jpg



19.22
f0439400.jpg



19.23
f0056936.jpg



19.24
f0360392.jpg



Incident #20

20.1
0E47C6DFd01



20.2
5C1E7D60d01



20.3
5E5570B4d01



20.4
BF5BE9D9d01



20.5
FB4EDA00d01



APPENDIX B - RECOVERED DOCUMENTS

Incident #3

3.9
aa010703a.h
tm

You are here: [About](#) > [Hobbies & Games](#) > [Birding / Wild Birds](#) > [Entertainment & Recreation](#) > [Birdhouses & Feeders](#) > [Build Birdhouses](#) >

Creating a Craft Room

About

Home

Essentials

- Types of Birds
- Birdhouse Directory of Where to Bird
- US State and Canadian Province Birds
- Birdhouses & Feeders
- Cooking FOR the Birds
- Recipes

Birding Offers

- Squirrel Proof Bird Feeder
- Birding Binoculars
- Wild Bird Feeders
- Bird Seed
- Hummingbird Feeders

Birds & Resources

- Bird Facts and Information
- Attracting Birds
- Photography
- Bird Problems
- Other Winged Creatures
- Conservation - Research
- Bird Related Activities
- Bird Computer Items
- Types of Birds
- Identifying Birds
- Where to See Birds
- Bird Books
- Find Other Birders
- Equipment & Supplies
- Extinct Birds

Buyer's Guide

- Before You Buy
- Top Photo
- Great Digital Cameras
- Bird Feeders
- Bird Stories to Read
- Product Reviews

Articles

Forums

Help

Birding / Wild Birds

Build a Bluebird Nest Box

Easy Box to Make

This bluebird nesting box is a great way to get started making birdhouses. You do not need to miter any edges and the entire project can be completed using one 6 foot length of 1" x 6" lumber.

Since only simple materials and tools are required, this birdhouse is also a wonderful project for Scouts, youth groups, and beginning woodworking classes.

[Click here](#) for drawings of the pieces and dimensions you will need. (A)
[Click here](#) for a close up of the hole. (B)
[Click here](#) for a diagram of the pivot nails. (C)

See the box to the right for wood and tool recommendations

Materials needed:

Wood cut to the dimensions shown in A above

Finishing nails
1 eye screw
Wood screws

Directions:

1. Cut the wood to the dimensions in [diagram A](#). All of the pieces can be cut from one 6' length of 1" x 6" lumber.
2. Cut the front entrance hole as in [diagram B](#). This is an oval shaped hole that is 1 3/8" wide and 2 1/4" long. To begin cutting this hole, mark the dimensions on the front. Then drill one 1 3/8" circle at the top. Repeat at the bottom of the hole, overlapping the drilled holes.
3. Drill two small holes near the top of each side for ventilation.
4. Drill four small holes on the bottom for drainage.
5. Using finishing nails or wood screws, secure one of the sides to the bottom. Then secure the front and back to the same side.
6. Slip the 2nd side into place. Secure using two nails, one near the top on each side. These nails will be pivots so make sure they are across from each other.
7. Reach inside the box and push the bottom of the 2nd side outwards, making sure it can pivot outwards. If it is too tight, remove the nail and sand the edges so it is a bit smaller. Repeat until the 2nd side will pivot outwards. See [diagram C](#) for
8. Screw the eye screw near the bottom of the 2nd side. This screw is to make it easier for you to open the box occasionally to monitor it as well as to clean it out at the end of the season.
9. Drill a small hole through the front near the bottom into the 2nd side. Push a bent nail (I have a few by this point) into the hole to keep the 2nd side closed. If you wish, use a small wood screw instead of the nail.
10. Nail or screw the roof to the nest box.
11. Mount the bluebird nest box to a pole, fence post, or tree. Be sure to use some type of predator guard to keep squirrels, snakes, raccoons, and other creatures from harming the nestlings. See the [Birdhouse Spec](#) page for the correct mounting height.

May you always hear the whisper of wings...
Christine

Sponsored Links

Blue Bird Houses
Same day shipping, Great selection, 110% Lowest price guarantee
[www.thebirdshed.com](#)

Woolly Nest Boxes
Nest Boxes for all sorts of birds FSC Timber, Order Online
[www.wigglwigglers.co.uk](#)

Nestling box camera
As featured in The Mail on Sunday View bird nest activity on our TV.
[www.cambox.co.uk](#)

Related Topics

- Exotic Pets
- Walking
- Wild / Canadian Parks
- Wildlife

Most Popular Video

- Bathroom Decoration Ideas
- Makeup Tips
- Create a Craft Room
- Fashion for Special Occasions
- Women Building a Website

Most Popular

- Alphabetical Index of Birds
- Books for Birding
- Birdhouses and Bruges In
- Birdhouses
- BIRD Houses And Clips
- Valentine's Day Ideas
- Butterfly and Bee Free
- Cloud Index
- Free Bird Count Index
- Events

What's Hot

- Wild Bird Photography
- Mail Order Pet Supplies
- Mail Order Photography
- Leaves - Warblers
- Glow in the Dark
- Books and Reference
- Mountain or Mountain Bird
- Books
- Virtual Bird Field Guide of Birds - by Scientific Name

Free Online E-Courses

- The To Save Money
- Texas Hold 'Em for Beginners
- How To Find The Best Credit Cards
- How To Get Your Credit Score
- How To Eliminate All Debt
- Break For Success
- More E-Courses

Advertisement

Advertisement

 From [Christine Teresi](#)
Your Guide to [Birds](#) / [Wild Birds](#).
FREE Newsletter: [Sign Up Now!](#)

 **EarthLink**
Dial-Up, High Speed &
Wireless Internet
access for all your
needs!
[Learn More](#)

 **VONAGE**
Save lots of
money on your
phone service.
[Learn More](#)
[Sign Up Now!](#)

FREE Newsletter
[Sign Up Now!](#) for the Birding / Wild Birds newsletter!
Enter email address:
[Sign Up](#) [See Online Courses](#)

Related Articles

- [Birds and Birdhouses - Build a Wren Roosting Box](#)
- [How to Make a Coffee Can Feeder](#)
- [Fire Truck Costumes](#)
- [Birds and Birdhouses - Tools Needed for Building Birds](#)
- [Birds and Birdhouses - Build a Remote Platform Feeder](#)

Most Popular Video

- [Bell Tower Decoration Ideas](#)
- [Tall Spires](#)
- [Creating a Craft Room](#)
- [Fashion for Special Occasions](#)
- [Women Building a Wardrobe](#)

[See other videos at About.com](#)

Sponsored Links

[Feed The Birds](#)
Bill Oddie's favourite bird foods delivered direct to your door.
[www.halts.com](#)

[Bluebird Houses](#)
Discount new & used items. aff! Search for bluebird houses now!
[www.eBay.com](#)

[Your Own Wildlife Channel](#)
A Bird Nesting Box with a built in TV Camera. Just £59.
[www.feathervision.co.uk](#)

[Bird & Parrot Breeding](#)
Birds, cages, nest boxes, vitamins, incubators, brooders, accessories.
[www.parrotsupplies.co.uk](#)

[Smart bird box cameras](#)
Wireless nest box camera colour Images to PC or TV
[www.enjoybirdsmore.co.uk](#)

Featured Content:

- [Dating / Relationships](#)
- [Entertainment](#)
- [Gifs](#)
- [Show Your Best](#)
- [Romantic Getaways](#)
- [Ways to Celebrate](#)

All you need to know about Super Bowl XXXIX.

Featured Content:

- [The Game](#)
- [Off the Field](#)
- [Parties and Food](#)

[Topic Index](#) | [XML](#) | [MY YAHOO!](#) | [back to top](#)

About Poll

	<p>Which Entrepreneur Do You Admire Most?</p> <div style="display: flex; justify-content: space-around; align-items: center;"> <div style="flex: 1;"> <input type="radio"/> Oprah Winfrey <input type="radio"/> Bill Gates <input type="radio"/> Martha Stewart </div> <div style="flex: 1;"> <input type="radio"/> Donald Trump <input type="radio"/> Richard Branson <input type="radio"/> None of Above </div> <div style="flex: 1;"> See Results  </div> </div>
Email to a friend Font size	

[Our Story](#) | [Be a Guide](#) | [Advertising Info](#) | [Investor Relations](#) | [Work at About](#) | [Site Map](#) | [Icons](#) | [Help](#)
 ©2005 About, Inc. All rights reserved. A PRIMEDIA Company.
[User Agreement](#) | [Privacy Policy](#) | [Kids' Privacy Policy](#)

71 | Page

3.10 *nestboxtips.txt*

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 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 buy 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.

Ln 1, Col 1 997 characters

100% Windows (CRLF)

Incident #9

9.6 *Doc1.doc*



9.7

Extracted image from Doc1.doc



Incident #12

12.10
[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 utilized. 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 hailing, and provisions for confinement for veterinary care should be considered at the time of construction. Although surprising, most raptors 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 injuries 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 other types of woven wire fencing are routinely used.

Many ranchers are now utilizing 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](#)

Incident #13

13.5 guide.doc	<p>An Insider's Guide to Enjoying Your First Birding Field Trip by Pete Dunne</p> <p>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.</p> <ul style="list-style-type: none">• 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. <p>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.</p> <ul style="list-style-type: none">• 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. <p>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.</p> <p>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. Carpool with someone else.</p> <ul style="list-style-type: none">• 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 is not inexperience, but rather the lousy or malfunctioning equipment - usually optics.
-------------------	---

If your binoculars aren't working, ask whether a loaner is available. If 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.

BIRDWATCHING IN THAILAND Feathered Magic from Mangroves to Mountaintops by Antony Lynam

One of the great attractions for nature tourists visiting Thailand is the diversity of environments extending across mountain peaks, lowland rainforests, mangroves, coral reefs, farmland and urban jungles. Within a day, or even a few hours travel, one can easily make the transition between these places and witness natural marvels large and small.

For wildlife enthusiasts no group maintains interest and pleasure more than birds. While special efforts are required to see in the wild charismatic species such as elephants and primates, birds are found across the entire spectrum of environments from pristine to severely degraded areas.

Part of the attraction for birds lies in their diversity. Nine hundred and seventy eight bird species have been recorded in Thailand, approximately 10% of the world's total. At the Isthmus of Kra between latitudes 11° and 13°N, a major biogeographic transition between Indochinese and Sundaic forests produces a special diversity of birds with a total of 152 species of birds reaching the northern or southern range limits of their geographic ranges.

Two-thirds of Thai birds are residents, the remainder are seasonal visitors. Locations where migrants congregate, often in large numbers, are highly accessible making Thailand a special destination for birdwatchers.

Many birds are susceptible to human disturbance because they have small geographic ranges, a result of specific habitat requirements. For example, Deignan's babbler - a non-descript forest bird is found on Doi Chiang Dao and nowhere else in the world. Gurney's pitta are only found in lowland rainforests. Fewer than 30 birds remain in the last known population in Thailand at Khao Nor Chuchi, Krabi. Efforts by local and international conservation agencies strive to increase protection efforts and reforest areas encroached by rubber farmers, though time is running out. With approximately 20% of the birds found in Thailand being globally or regionally endangered species, this makes the country a birdwatching haven for bird enthusiasts.

IDENTIFYING BIRDS

Birds are distinguished first by their size and shape. They range from diminutive flowerpeckers, sunbirds and white-eyes, about the size of your index finger, to lanky storks and egrets that stand almost a metre tall, and Green peafowl with its spectacular 2m tail. The form of the beak offers vital clues about the bird's diet. For example a thin curved tube for sipping nectar or a sharp hook for tearing flesh. The pattern and colour of plumage can tell apart the sexes as in pheasants where males are bright and striking, and females are drab and dowdy. By far the most useful character for identification is a bird's voice. This is especially true in forests where on average 90% of birds are hidden from view. The most experienced birdwatchers in the tropics know their songs and calls.

BEST TIMES TO SEE BIRDS

The nesting season is a good time to be watching birds. During this most active time in a bird's life a variety of vocalizations and behaviours are exhibited. In Thailand, as in other tropical countries, the nesting season coincides with the period when food is in abundant supply. A bird expends much energy in courting, mating, incubating eggs, defending a nest and feeding offspring. Most birds nest during the transition between dry and wet seasons when new leaves and grass

mangroves while Mangrove whistlers and flyeaters rarely leave the area.
Key sites: *Samut Sakhon*, *Ban Laem* in *Petchburi*, and *Krabi*.

OFFSHORE ISLANDS

Offshore islands such as *Phi Phi*, *Libong*, *Surin* and the *Similans* support fewer species than similar sized mainland habitats but some such as Nicobar and Pied Imperial pigeon are entirely restricted to these refuges.

SEASCAPES

While there are fewer seabirds in the warm Thai waters compared with those in the northern and southern hemispheres, frigate birds, skuas, boobies, and terns are among the rewards for marine birders.

FORESTS

Most resident Thai birds depend upon forests for their survival. Rainforests in the extreme south support the greatest avian diversity, while seasonally dry dipterocarp, mixed deciduous and evergreen forests in the centre and north. Key sites: *Khao Yai National Park*, *Kaeng Krachan National Park*, *Khao Soi Dao*, *Nam Nao National Park*, *Khao Nor Chuchi*, *Ban Nai Chong*, and *Hala Bala Wildlife Sanctuary*.

MOUNTAINS

Sibias, minlas, and laughing thrushes are relatives of species found in the Himalayas and southern China, and can only be found in mountain forests. Following surveys of high mountain peaks in the last decade, at least 20 new species or 2% of the total have been added to the lists for Thailand. Key sites: *Doi Pha Hom Pok*, *Doi Chiang Dao*, *Doi Inthanon*, *Doi Ang Khang*, and *Doi Suthep*.

By visiting these enchanting destinations, travellers can appreciate the avian wonders that Thailand offers and better understand the importance of the wild and not so wild areas that preserve them.

Contact information:

Bird Conservation Society of Thailand (BCST)*
69/12 Soi Ramindra 24, Joorakaebau, Ladprao, Bangkok 10230, Thailand
Email: bcst@box1.a-net.net.th

Tel: 66-(0)-2943-5965

Web sites:

www.bcst.org/index_ebird.html

www.thai.net/bcst

* The Bird Conservation Society of Thailand (BCST) is a BirdLife Partner

Oriental Bird Club (OBC)
c/o Uthai Treesucon, 723/1 Mu 2 Soi Ram Intra, Joorakhaebua, Bangkok 10230.
E-mail:
utree@loxinfo.co.th
mail@orientalbirdclub.org
Web site: www.orientalbirdclub.org

Wildlife Conservation Society - Thailand Programme

P.O. Box 170, Laksi, Bangkok 10210

Tel: +662-503 4478, +662-503 4479

Fax: +662-503 4096

Email: thailand@wcs.org

Reference information:

Field guide

Robson, C. 2002.

A field guide to the birds of Thailand.

Asia Books, Bangkok. 272pp.

TAT PUBLICATIONS ON NATURE TOURISM

For more information on birdwatching in Thailand, please refer to the following nature tourism guide books in the "National Park" series published by the Tourism Authority of Thailand as part of the Tourism and Employment Creation Plan implemented under the Social Investment Project.

- KHAO YAI: DONG PHAYA YEN FOREST RANGE
ISBN 974-8252-70-1
- KAENG KRACHAN:
Amazing Forest of Phetchburi River
ISBN 974-8252-72-8
- KHAO SOK
Fascinating Limestone Mountains Amid The Verdant Forest of Surat Thani, Thailand
ISBN 974-679-099-4
- DOI INTHONON - DOI SUTHEP
The Himalayan Springs of Thailand
SBN 974-8252-67-1
- PHU LUANG
The Kingdom of Plants
ISBN 974-8252-73-6

BIRDWATCHING TIPS

- Consult field guides, checklists, and maps prior to arriving at the birdwatching destination.
- Dress in colours that blend in with the surroundings.
- Bring appropriate equipment such as telescope, bird guide, and a notebook.
- Plan to arrive at the destination at sunrise when birds are first out in search for food and are most active.
- Walk slowly stopping at intervals to listen for calling birds.
- Look for the birds in thickets, on the branches of trees, and on the ground.
- Avoid talking, smoking, or walking on dry leaves, all of which will scare birds away.

CONSERVING BIRD DIVERSITY

Across the world, humans coexist with birds but human activities often affect the survival prospects for birds. Forty-eight species of birds found in Thailand (5% of the total) are globally threatened by the loss or disturbance of their habitats, food resources, and breeding areas, and by other human actions, and so require special conservation attention. A further 97 species (10%) are potentially threatened if current trends persist.

In Thailand, 101 species (10% of the total) are hunted as pests, for food or for the pet trade and are directly threatened by humans. The list of hunted species includes waterbirds, birds of prey, pheasants, parakeets, pigeons, hornbills, pitta weavers, bulbuls, and other forest birds. Worldwide the trade in birds includes 2,600 species and several million birds each year. Ten percent of threatened bird worldwide are affected by the bird trade.

shoots sprout. This occurs from February to June. Certain birds depend on the availability of water and nest throughout the rainy season.

Migrants are best observed during their passage into or out of the country, or as they pass through on their way to other places. Most conspicuously, half a million ducks spend their winter in Thailand, feeding and resting in watery roosts from Chiang Saen to Thale Noi. Thousands of garganey and Lesser treeduck flock during January and February.

Shorebirds like sandpipers, stints and plovers migrate long-distances between nesting grounds in Eurasia and tropical Asia and wintering grounds in Australasia. They stop to feed in Thailand's mudflats and mangroves during September to May where they stock up on invertebrates and crustaceans. During October, the southward migration of hawks over peninsular Thailand is an avian spectacle. Chinese goshawks, Japanese sparrowhawks, crested honey buzzards, black bazas, and others are seen coasting on thermals in their thousands daily. Less conspicuous is the blue-winged pitta, a ground dwelling bird that arrives with the rains to nest in deciduous and bamboo forests, and escapes the hot season for the wetter forests of Malaysia and Sumatra.

WHERE TO FIND BIRDS

Given that many birds are denizens of certain times, places, habitats or seasons, the amateur naturalist can remember them by association.

PARKS, TEMPLES AND GARDENS

Some species like barn swallows, magpie robins, mynas and starlings can be found around Bangkok and environs. *Lumphini Park*, a heavily-used green area in the city centre supports a variety of birds with over 90 species having been recorded there. Temples near Bangkok and Ayutthaya preserve pockets of the natural landscape including birds such as black kites, parakeets and woodland birds that are characteristic of the habitats.

RICE PADDIES, MARSHES AND PONDS

Rice paddies, marshes and ponds away from built-up areas support breeding populations of Asian openbill stork and many other waterbirds.
Key sites: *Suphan Buri-Ayutthaya* and *Beung Borapet*.

PEAT SWAMP FORESTS

Almost the last vestige of Thailand's peat swamp forest at *Phru To Daeng* or *Chalerm Phrakiat Wildlife Sanctuary* in Narathiwat supports Lesser adjutants, a kind of stork, along with several birds characteristic of Sundanic forests.

LAKES, RIVER SANDBANKS AND REEDBEDS

Lakes, river sandbanks and reedbeds preserve unique assemblages of wintering waterfowl and perching birds.
Key sites: *Chiang Saen*, *Fang Hot Springs*, and *Thaton*.

AGRICULTURAL LANDSCAPES

Agricultural landscapes across the country support species that tolerate human presence and include kites, rollers, bee-eaters, coucals, weavers and bulbuls.

SANDY BEACHES, MANGROVE AND TIDAL FLATS

Sandy beaches are attractive to tourists but are barren habitats for birds, while little-visited mangroves and tidal flats that are rich in nutrients and microorganisms, are favoured feeding haunts for migrant waders. Some birds like the Brown-winged kingfisher and Mangrove pitta, are entirely restricted to

There are a number of ways in which the numbers and distribution of threatened birds are being restored. Habitat conservation programmes are an important mechanism. Feeding habitats for seasonal migrants are being preserved by incorporating mangroves and coastal tidal areas in marine protected areas. Lowland forests that support Gurney's pitta and other diversity are being protected and a reafforestation programme planned. Preventing encroachment around the edges of parks maintains the integrity of forest blocks used by the majority of native birds, including migrant raptors and songbirds.

In most cases, preserving and protecting natural habitats can bring back even highly endangered populations of rare birds. These measures are relatively cost effective to implement. As an example, a 3-year Khao Yai Conservation Project preserved over 2,000 sq km of wildlife habitat, discouraged poaching, and provided employment alternatives for local forest resource users, at an annual cost of 7 million baht (US\$171,000).

For critically endangered species, whose populations are extremely small, and whose survival in the wild is uncertain due to factors that simply cannot be controlled, other more costly measures such as captive breeding, are being considered. Captive breeding is risky because birds need to be recovered from the wild to establish breeding populations, and injury is possible. Some species do not breed well in captivity because their natural courting and nesting behaviours are no longer possible. Strict controls on who is allowed to breed endangered species, registration of individuals, and enforcement of laws so that commercial sale is not possible, need to be adopted. Without these controls, captive breeding programmes cannot succeed.

HOW YOU CAN HELP IN THE CONSERVATION OF BIRDS

Visitors to Thailand can assist efforts to preserve and maintain the diversity of birds and their habitats simply by visiting national parks and other wilderness areas. Bird enthusiasts can report the species they observe to authorities. Checklists are now available at many popular national parks. Tourists can report evidence of suspicious activity that might lead to the arrest of unscrupulous individuals trapping or hunting birds and can also participate as volunteers in habitat conservation programmes. In these ways, tourists can help reduce the threats to birds, and at the same time enjoy Thailand's birdwatching paradise.

Contact information:

TO REPORT BIRD SPECIES OBSERVED

- TO REPORT BIRD SPECIES OBSERVED**

Please contact the Park Visitor Centre of the National Park
or
Bird Conservation Society of Thailand (BCST)*
69/12 Soi Ramindra 24, Joorakaebau, Ladprao, Bangkok 10230, Thailand
Email: bcst@box1.a-net.net.th
Tel: 66-(0)-2943-5965
Web sites:
www.bcst.org/index_ebird.html
www.thai.net/bcst

* The Bird Conservation Society of Thailand (BCST) is a BirdLife Partner

- TO REPORT EVIDENCE OF SUSPICIOUS ACTIVITY**

Please contact

Wildlife Protection and Suppression Office
Department of National Parks, Wildlife, and Plant Conservation
61 Paholyothin Road, Chatuchak, Bangkok 10900
Tel: 66-(0)-2579-5266

• **HABITAT CONSERVATION VOLUNTEER PROGRAMMES**

Please contact
Wildlife Conservation Society - Thailand Programme
P.O. Box 170, Laksi, Bangkok 10210
Tel: +662-503 4478, +662-503 4479
Fax: +662-503 4096
Email: thailand@wcs.org

FAMILIES OF BIRDS IN THAILAND UNDER THREAT

The following bird species are under threat because there is a high demand for them and they are hunted for the local, regional and global bird trade. To help preserve the species, please refrain from purchasing any of the following birds as pets, and if you happen to witness any of the following birds being sold or traded, or note any suspicious activities involving them, please contact:

The Wildlife Protection and Suppression Office
Department of National Parks, Wildlife, and Plant Conservation
61 Paholyothin Road, Chatuchak, Bangkok 10900
Tel: 66-(0)-2579-5266

1. Phasianidae (wood partridges and pheasants) - 4 species
2. Anatidae (White-winged duck) - 1 species
3. Picidae (woodpeckers and barbets) - 3 species
4. Bucerotidae (hornbills) - 7 species
5. Upupidae (Common hoopoe) - 1 species
6. Cuculidae (Coral-billed ground cuckoo) - 1 species
7. Psittacidae (parrots and parakeets) - 4 species
8. Columbidae (pigeons) - 12 species
9. Accipitridae (birds of prey) - 9 species
10. Threskiornithidae (White-shouldered ibis) - 1 species
11. Ciconiidae (Lesser adjutant) - 1 species
12. Pittidae (pittas) - 3 species
13. Irenidae (Asian fairy bluebird and leafbirds) - 6 species
14. Corvidae (jays, crows, magpies, orioles and minivets) - 14 species
15. Muscicapidae (thrushes, robins, and sharmas) - 3 species
16. Sturnidae (starlings and mynas) - 3 species
17. Paridae (Yellow-cheeked tit) - 1 species
18. Pycnonotidae (bulbuls) - 7 species
19. Zosteropidae (Japanese white-eye) - 1 species
20. Sylviidae (laughing thrushes, mesias, minlas and sibias) - 8 species
21. Nectariniidae (Scarlet-backed flowerpecker) - 1 species
22. Passeridae (weavers and munias) - 7 species
23. Fringillidae (grosbeaks and buntings) - 3 species

About The Author

ANTONY LYNAM

Antony Lynam (Ph.D.), Wildlife Conservation Society (WCS)- Thailand Programme Director and conservation scientist, works with the Thailand Department of National Parks, Wildlife and Plants to develop programmes for the conservation of the country's endangered species, park resources management, and the design and conduct of training curriculum for park rangers.

An Australian citizen, he has authored a number of technical papers and popular articles concerning conservation issues in Australia, North America, and Thailand, and was a contributor to the seminal volume on habitat fragmentation "Tropical Forest Remnants: Ecology, Conservation and Management". He writes frequently on natural history for magazines, journals and newspapers including Wildlife Conservation, The Nation, The Bangkok Post, and The Natural History Bulletin of The Siam Society.

13.15
ODBC.INI

ODBC.INI

File Edit View

```
[ODBC 32 bit Data Sources]
MS Access Database=Microsoft Access Driver (*.mdb) (32 bit)
Excel Files=Microsoft Excel Driver (*.xls) (32 bit)
dBASE Files=Microsoft dBase Driver (*.dbf) (32 bit)
[MS Access Database]
Driver32=C:\WINDOWS\system32\odbcjt32.dll
[Excel Files]
Driver32=C:\WINDOWS\system32\odbcjt32.dll
[dBASE Files]
Driver32=C:\WINDOWS\system32\odbcjt32.dll
;"Without doubt the presence of Lake Michigan affects the
;movement and distribution of birdlife in the Dunes more than
;any other single factor. The shores of this enormous lake provide
;leading lines that control flight paths of numerous migrants, and
;the vast open waters draw legions of transitory and wintering birds.
;During autumn the elongate north-south boundaries of the lake become
;airways along which thousands of migrants navigate toward
;wintering areas. Southbound birds following the shores are ultimately
;guided into the
;Dunes Area, at the toe of
;the lake. This avian convergence
;at the bottom of
;Lake Michigan is termed
;the funneling effect."
;The funneling effect explains
;the unusually high
;diversity of autumn birds
;in northwest Indiana.
;"Lake Michigan also provides
;two important avian habitats that are otherwise quite rare in the
;Midwest: the deep lake and the beach. Waters of the lake attract
;large numbers of bay and sea ducks, many of which are virtually
;unrecorded at inland sites in the Midwest. Additionally, the lake
;attracts a number of rare periodic transients, including the Purple
;Sandpiper, Red Phalarope, Pomarine Jaeger, Parasitic Jaeger, Great
;Black-backed Gull, Glaucous Gull, Iceland Gull, Thayer's Gull,
;Sabine's Gull, Little Gull, Black-legged Kittiwake. Extensive beaches
;provide resting and feeding areas for shorebirds, especially those
;species preferring sand rather than mudflats, e.g., Sanderling, Red
;Knot, and Baird's Sandpiper.
;"The deep waters of Lake Michigan also constitute a significant
;obstacle to migrants. During nocturnal flights many north-bound
;passerines overfly land's end and daybreak finds them over the lake.
;When landfall is visible, they often fly directly to the shore, where
;they immediately land for rest and feeding.
;This effect generates an anomalously high concentration of passerines
;in parks and woodlands immediately adjacent to the lake"
;(Brock 5).
```

Incident #17

17.1 <i>stuf.doc</i>	<p>Dear Sir</p> <p>Further to our conversation everything we have discussed has been done</p> <p>Yours faithfully</p> <p>John Doe</p>
-------------------------	---

Incident #18

18.19 <i>f0201904.html</i>	<p>Go to Google Home Web Images Groups News more Search Advanced Search Preferences</p> <p>Search: <input checked="" type="radio"/> web <input type="radio"/> pages from the UK</p> <p>Results 1 - 10 of about 28,800,000 for birds [definition] (0.11 seconds)</p> <p>Sponsored Links</p> <p>Pictures Express your talent Stimulate your artistic potential www.takingglobal.org/express/gall</p> <p>Birds Birds for sale aff Check out the deals now! www.eBay.com</p> <p>Birds Aff. Everything to do with Birds eBay.co.uk</p> <p>Birds and Bird Watching Popular books about birds, great Discounts, fast UK Delivery aff www.englishbooks.co.uk/birds</p> <p>Wild Woods Go wild around Britain with our can-see, must-see wildlife guide. www.forestry.gov.uk/wildwoods</p> <p>Result Page: 1 2 3 4 5 6 7 8 9 10 Next</p> <p>Free! Google Desktop Search: Search your own computer.</p> <p>Search within results Language Tools Search Tutorials Dissatisfied? Help us improve</p>
-------------------------------	---

18.20
f0496112.html

Results 1 - 10 of about 176,000 for [bird screensavers](#) (0.46 seconds)

[Sponsored Link](#)

[Free Screensavers](#)
The Only Screensaver That Guarantees No Spyware. Be Original. [www.screensavers.com](#)

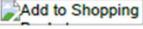
[Free Desktop Screensavers](#)
Hundreds of Screensavers to choose from. Download your favorite today! [www.webssearch.com](#)

[All Free Screensavers](#)
Screensavers For All Occasions. Get Yours For Free Today! [www.screen saver.com](#)

Incident #19

<p>19.25 f0005672_Related_Articles.html</p>	<p>Related Topics</p> <p>Bird Problems Other Winged Creatures Conservation - Research Bird Related Activities</p> <p>Related Articles</p> <p>BIRDING AND BIRDWATCHING HOW TO MAKE A COFFEE</p>
---	--

19.26
f0033288.html

- 5785-2744400 > 
5.  [The Very Worst Thing](#)
~Torey L. Hayden
HarperCollins Publishers
Hardcover - June 1, 2003
Avg. Customer Review: 5.0 out of 5
Usually dispatched within 8 to 10 days
- US List Price:** \$15.99
UK Equivalent: £8.54
Our Price: £7.69
You Save: £0.85 (9%)
[Used & New](#) from £5.86
6.  [Garden Birds \(Collins Gem S.\)](#)
~Stephen Moss
Collins
Paperback - November 1, 2004
Avg. Customer Review: 4.0 out of 5
Usually dispatched within 24 hours
- Our Price:** £4.99
[Used & New](#) from £2.37
7.  [Birds Without Wings](#)
~Louis De Bernieres
Secker & Warburg
Hardcover - July 1, 2004
Avg. Customer Review: 3.6 out of 5
Usually dispatched within 24 hours
- List Price:** £17.99
Our Price: £12.59
You Save: £5.40 (30%)
[Used & New](#) from £9.50
8.  [Collins Field Guide: Bird Songs and Calls of Britain and Northern Europe \(Contains 2 accompaniment CDs\)](#)
~Geoff Sample
Collins
Hardcover - February 1, 1999
Avg. Customer Review: 4.6 out of 5
Usually dispatched within 24 hours

19.27
f0041304.html

[Go to Google Home](#)

Web Images Groups News more > Search Advanced Search Preferences

Search: the web pages from the UK

Results 1

Web

Chickadee Karaoke
... During mating season, Mennill hung out in the woods with a laptop and a speaker. He gathered the birds by playing the familiar chickadee call. ... www.ihns.uic.edu/shories/104chick_sex/ - 11k - Cached - Similar pages

Teacher's Guide - Bird Banter
... other and rejoin the group through a gathering call. ... other types of communications are used by birds. ... and American woodcocks have elaborate mating dances and ... www.ihns.uic.edu/cifc/pub/virtualbird/teacher/lesp10.html - 5k - Cached - Similar pages

Bird Banter
... to attract mates and mark the territory necessary to raise young. Each species has its own specific song or songs. Some birds have over a dozen calls and songs ... www.ihns.uic.edu/cifc/pub/virtualbird/student/les0.html - 3k - Cached - Similar pages
[More results from www.ihns.uic.edu]

Rainforest Birds I Photo, lists & guides, Far North Queensland
... the spring you can hear the rasping mating calls of the ... the birds of paradise and their mating display is one of the most precious bird watching sightings ... rainforest-australia.com/bird.htm - 12k - Cached - Similar pages

Sound Ideas Just Birds and Animals II Complete Track and Index
File Format: PDF/Adobe Acrobat - [View as HTML](#)
... 02 JBA03 52-04 BIRD, TURKEY FEMALE WILD TURKEY: MATING CALL. 03 JBA03 53-01 BIRD, WOODPECKER LESSER SPOTTED WOODPECKER: CALLING. 03 ... www.sound-ideas.com/pdf/jba2.pdf - Similar pages

LYREBIRDS MATING
... Rituals in all of the bird world. First, he builds a platform out of a mound of dirt. And then, mounting his stage, the lyrebird lets out his mating call. ... www.pulseplanet.com/archive/May97/1400.html - 14k - Cached - Similar pages

About The Bird Mating
... Because the female is the larger bird, the male needs ... her back and balances precariously during mating - with no ... The kiwi female calls the shots during mating ... www.kiwirecover.org.nz/AboutTheBird/KiwiLifeCycle/Mating.htm - 28k - 1 Feb 2005 - Cached - Similar pages

NPR - The Call of the Wild Car Alarm
... She got the basic bird sounds from the Macaulay Library of Natural Sounds at Cornell University. Her sonic avairy includes the mating call of the Three-Wattled ... www.npr.org/programs/ato/features/2002/july/car_alarm - 34k - Cached - Similar pages

Scientific American Frontiers - Calls of the Wild - Songs of Love
... But as they release the newly-banded bird, everyone hears a warbler's "pleased-pleased-pleased to MEET-ya" mating call coming from another male a few feet away ... www.pbs.org/saf/1308/segments/1308-1.htm - 16k - Cached - Similar pages

2986 Birds-1
File Format: PDF/Adobe Acrobat - [View as HTML](#)
... territory or attract a mate, you might break out in song. Birds call out to alert others of danger. Read the following instructions to play this bird song game ... dnr.state.il.us/lands/education/CLASRM/birds/unit2_lesson2.pdf - Similar pages

Result Page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [Next](#)

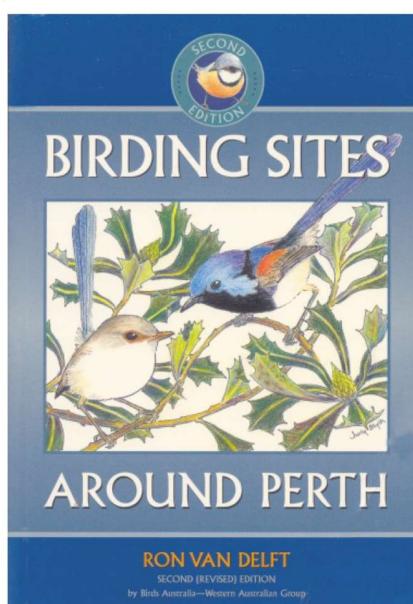
 [Free!](#) [Google Desktop Search](#): Search your own computer.

bird mating calls

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied? Help us improve](#)

[Google Home](#) · [Advertising Programmes](#) · [About Google](#)

19.28
f0180344.pdf



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

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

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

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

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

WHAT IS BIRDS AUSTRALIA?

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

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

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

INTERESTED?

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

Phone: (08) 9383 7749
Fax: (08) 9387 8412
Email: birdsawa@inet.net.au
Web: birdsawa.inet.net.au



BOTANICAL

UNIVERSITY OF CALIFORNIA

GARDEN

NEWSLETTER

Volume 26, Number 2 Published by the UNIVERSITY OF CALIFORNIA BOTANICAL GARDEN at Berkeley, California Spring 2001

Birds at the UCBG

"It's a hummingbird! But is it Anna's, Allen's or Rufous?"

Academic interest in the Garden's bird life over the last few years has primarily been associated with undergraduates studying territorial behavior of hummingbirds. A regular Garden visitor can tell you how odd that you've never really experienced the Garden until you have taken the time to sit and just watch the birds, listen to their songs and enjoy the way in which they use the Garden! Encouraged by the vast plant variety and habitat diversity, there are around seventy-six bird species regularly sighted here over the course of an average year. The hope of spotting one of the more rarely sighted birds, such as the Western Kingbird or the White-throated Swift, keeps our endless parade of avid birdwatchers in thrall. Our resident birds, however, whether it's an audacious jay, a noisy woodpecker or a colorful finch, provide plenty of ongoing interest for the Garden community.

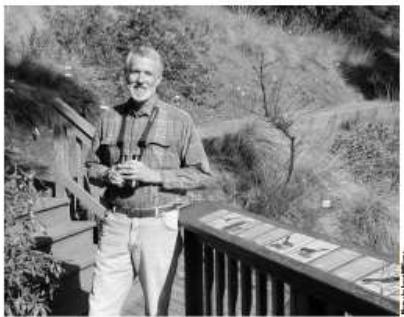
The diverse collections of the Garden support an equally diverse population of birds, as is apparent in the list from the recent Christmas Bird Count. In addition to providing general shelter for both resident and migrant species, our collection provides food and nesting sites for many different taxa. The Garden environment offers a range of habitats that are rather different from the native chaparral of the canyon. Some visitors to the Japanese Pool, such as belted kingfishers and green and blue herons, might not otherwise stop in Strawberry Canyon. Native chaparral species are found in parts of the Garden that more closely approximate their preferred habitat. Wren tits, California thrashers, and



Aloes in the Southern African Area attract hummingbirds and demonstrate how birds at the Garden enjoy the diversity of plants in this collection.

spotted towhees are most commonly found in the scrubby areas of the South American and Australasian sections. Similarly, native riparian species are found in the trees along Strawberry Creek, such as Wilson's and orange crowned warblers. Sources among the This is hummers feed on, and also on parts of the world. Aloes limited by sun birds in orful nectivores perch oes. This is a distinct contrast to the hovering feeding habit of the hummers, which as a group are restricted to North and South America. Nonetheless, as a walk through this area at this time of the year demonstrates, hummers utilize aloes extensively and assertively defend their feeding resources against other intruding hummers.

—Chris Carmichael



When not watching birds from the Elizabeth Hammond Interpretive Center, where he is pictured here, noted local ornithologist Dennis Wolff, regularly teaches popular birdwatching classes in the Garden.

From Killing to Counting

Before 1900, Americans engaged in a holiday tradition known as the Christmas "Side Hunt". People would choose sides and go afield with their guns; whoever brought in the biggest pile of feathered quarry won. On Christmas Day 1900, ornithologist Frank Chapman, an early officer in the Audubon Society, called for an end to the slaughter. Rather than shooting birds, he suggested counting them. From Toronto to Pacific Grove, California, the Christmas Bird Count began. In its first year, 27 people participated, counting 18,500 individual birds of ninety species.

On Christmas Day 2000, 52,000 people participated in 1800 counts in the United States and Canada. They sighted 78,636,382 individual birds of 676 species! A century of bird counts has amassed a wealth of data which scientists use to monitor the health of bird species, pinpoint and explain trends, and detect the rise of environmental threats.

Along with three other members of the Audubon Society, I came to the rich and varied habitats of the UC Botanical Garden for this annual count. We found a total of 226 individual birds of 38 species, including such rarities as hermit and black-throated warblers.

—Dennis Wolff

AUDUBON CHRISTMAS COUNT DECEMBER 17, 2000

American Robin	30
Anna's Hummingbird	25
Steller's Jay	21
Bush-tit	16
Golden-Crowned Kinglet	14
Ruby-Crowned Kinglet	12
Yellow-Rumped Warbler	10
Townsend's Warbler	9
Western Scrub-Jay	9
Chestnut-Backed Chickadee	7
Hutton's Vireo	7
Song Sparrow	6
California Towhee	5
Golden-crowned Sparrow	5
Bewick's Wren	4
Fox Sparrow	4
Dark-eyed Junco	4
Turkey Vulture	3
Hermit Thrush	3
Allen/Rufous Hummingbird	3
Common Raven	3
Band-Tailed Pigeon	2
Northern Flicker	2
Black Phoebe	2
Red-breasted Nuthatch	2
Brown Creeper	2
California Thrasher	2
Spotted Towhee	2
White-crowned Sparrow	2
Cooper's Hawk	1
Sharp-shinned Hawk	1
Red-breasted Sapsucker	1
Nuttall's Woodpecker	1
Hairy Woodpecker	1
Wrentit	1
Black-throated Gray Warbler	1
Hermit Warbler	1



Dr. Chris Carmichael, UCBG Manager of Collections and Horticulture, is one of our noteworthy birders, a group which also includes Dr. Jennifer White, Associate Director for Education, and Curator Holly Forbes. Chris' academic background in vertebrate zoology equips him to effortlessly make the connections between the birds here in the Garden and their relationships to the plants.

SIBLEY'S GUIDE TO BIRDS

National Audubon Society: The Sibley Guide to Birds, written and illustrated by David Allen Sibley; A Chanticleer Press Edition, Alfred A. Knopf, NY, ©2000; 544pp. Flexible Binding. \$35.00.

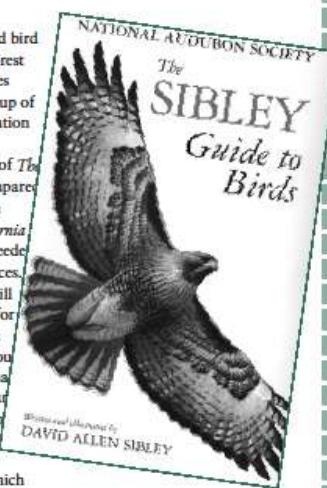
Most visitors to the Garden come to see and study our special plants, but a surprising number also come to see the animals and birds which feed and take shelter in the hospitable environment. We have newts which breed yearly in our Japanese Pool and monarch butterflies visiting our milkweed plants. Now and again we are surprised to learn that we are on the Audubon Society's Hotline, as we were several years ago when dozens of visitors came to see a rare bird sighted in the southwest corner of the Garden.

In past years, the Roger Tory Peterson *Field Guide to Western Birds*, or the National Geographic Society's *Field Guide to Birds of North America*, were seen tucked under the arms of our "Garden Birders". Now there is a new, up-to-date field guide these birders will want to own, although its size and weight make it awkward to carry in the field. *The Sibley Guide to Birds* is a great user-friendly guide containing over 6600 wonderfully detailed watercolor paintings of 810 species and 350 populations of North American birds. Descriptions and remarks accompany the illustrations, removing the need to flip back and forth between text and pictures. The birds are shown in similar poses to make comparisons between species easy. All important plumages are depicted and range maps show migration routes, summer, win-

ter, and breeding locations, and bird distribution. Of particular interest are the good introductory pages preceding each family or group of families showing bird classification and speciation at a glance. In many ways the publication of *The Sibley Guide to Birds* can be compared to the publication of *The Jepson Manual: Higher Plants of California* few years ago. Both were preceded by respected long-used references, it is likely that the *Sibley Guide* will become the current authority for birds, as the *Jepson Manual* has become for plants. But keep you worn, well-loved field guides handy. For this reader, at least, it is hard to think that the beloved California Quail in the Garden calls "put-way-do" rather than the familiar "chi-ca-go" of old, which we teach the touring school children.

The Garden Shop also carries the following books related to the above review:

Birds of Northern California by David Fix and Andy Bezener; range maps by Don Roberson and David Fix; Lone Pine Pub., Renton, WA, ©2000; 384pp. Paper. \$19.95.
Birds of San Francisco and the Bay Area, by Chris C. Fisher and Joseph Morlan; Lone Pine Pub., Renton, WA, ©1996; 159pp. Paper. \$9.95.
Common Dragonflies of California, A Beginner's Pocket Guide, by Kathy Biggs; Azalea Creek Pub., Sebastopol, CA, ©2000. 96pp. Paper. \$9.95.



Newts and Salamanders, Everything about Selection, Care, Nutrition, Diseases, Breeding, and Behavior, by Frank Indiviglio; with photos by Richard D. Bartlett; illus. by Michele Earl-Bridges; Barron's, Hauppauge, NY, ©1997; 128pp. Paper. \$6.95.
Brochures:

Birds of the UC Botanical Garden, UC Botanical Garden Staff. \$1.00.

Butterflies of the San Francisco Bay Region, A County Species List, 5th ed., by John Steiner; San Francisco Bay Wildlife Soc, 1988. \$1.00.

—Elly Bade

DIRECTOR'S COLUMN

Celebrating the Garden

Spring is here again! The hills are green and spangled with flowers. The wind is whipping across the coastal bluffs, and anyone with even the slightest inclination toward gardening has their hands in the soil. As I watch the seasons march across the landscape and think back to the past year, I'm amazed at the amount of progress we have to celebrate here at the Garden.

The living collection is in superior condition. Over the years, the horticultural staff has done an inspired job of maintaining and building the collection. However, with leadership by Manager of Collections and Horticulture, Chris Carmichael, and better access to materials and supplies, they have added new shine to the Garden. I invite you to push past the construction sites in the entrance to get a better look!

Ah, yes, those construction sites. We were so excited when they started. Now, we look forward eagerly to their completion. The Garden has not been a peaceful place to work or visit this year. Staff and volunteers have been wonderful, carrying out their work over the din of jackhammers, dump trucks, cement mixers, and more. From all this dust, mud, and upset, the Garden is gaining many physical improvements. Some, like the utility upgrades, make our jobs easier but are invisible to visitors. Others, such as renovated bathrooms and FEMA restoration of pathways in the Mexican and Central American area, are essential but not sensational. Many projects, though, are downright sensational!

Master rock garden creator, Phil Johnson, has just completed a spectacular hardscape in the Southern African section, and horticulturist Lawrence Lee will soon begin planting it with material obtained during his collecting trips to South Africa. This garden will feature the natural beauty of bulbs and succulents from the winter rainfall areas of the Karoo and Fynbos semi-arid and desert habitats. It also provides an opportunity to inform visitors about the precarious situation these habitats in the face of regional development and global climate change.

Our new Arid House is also nearing completion. The name has recently been changed to Arid House from Desert Greenhouse — Arid House being more appropriate for that collection, though we are still making the name transition. This structure will house a substantial number of the most biologically and scientifically valuable plants in our collection, including many living "type" specimens. Type specimens are the exemplar individuals a taxonomist uses to describe a new species. Other specimens belong to species that are now extinct in the wild, and are therefore irreplace-

able. The new house provides the public with excellent visual access to the exciting and unusual plant forms in this collection while ensuring their security. UC researchers are anxiously awaiting opening of the Center for the Study of Plant Conservation (CSPC) at the Garden. Although the lab is not yet finished, scientists associated with this center are already exploring a diversity of questions related to plant conservation. Richard Shefferson, a graduate student at the Center, writes in this issue about his research devoted to discovering the types of fungi that sustain terrestrial orchids. Another graduate student, Jessica Riquetti, recently established a major field experiment to determine whether soil-borne organisms can limit the spread of European beach grass, an invasive species that reduces native plant diversity in sand dunes along the Pacific coast of North America. Work by these students and other scholars will be greatly facilitated by the new Center.

In preparation for our next round of construction, we have just begun design of the Jane Gray Research Greenhouse, which will be an important adjunct of Garden research in plant conservation and ethnobotany. This house will be erected in the place currently occupied by the temporary arid house and will serve researchers from both the CSPC and elsewhere on the Cal campus. Although construction is the most visible sign of progress that visitors can see, the Garden has many other achievements to celebrate as well. Our educational outreach programs are receiving national recognition. Many partners are joining our Math in the Garden initiative. Beginning this spring staff at the UC Davis Arboretum, Brooklyn Botanic Garden, Missouri Botanical Garden, Morris Arboretum, and Atlanta Botanical Garden become active partners in the development process of the 'Math in the Garden' project as they try out the activities in their own programs. San Francisco Girl Scout Council troops and 4-H programs across California are also partners in this effort. Over the next year their evaluations of the effectiveness of the project's activities will provide crucial information to ensure that the final published materials will fit into different informal settings and programs and work in gardens throughout the country. Collaborations with these, and other partners, provide audiences diverse program opportunities that strengthen this and other aspects of the Garden's Education Programs.

Cactus drawings by UCBG horticulturist, Judith Finn. Above: Gymnocalycium saglionii and at right: Euphorbia cf. leuconeura.

Our collaboration with East Bay Municipal Utility District, which resulted in our spectacular and innovative contribution to last year's San Francisco Flower and Garden Show, is now producing exciting new Garden interpretation materials. Garden staff and dedicated volunteers worked with EBMUD staff to develop an extensive and well-received tour of Plants for Water-wise Gardening. (See the Education Director's column for more information about this tour.) The tour takes advantage of our diverse and outstanding collection to illustrate landscape uses of water-conserving plants. Most species highlighted in the tour are available in the horticultural trade, but some are not, which puts the tour on the leading edge of horticultural innovation.

Through all of these changes, the Garden continues to expand its primary mission of support for botanical research. New molecular tools are allowing exciting discoveries in evo-lutionary biology and plant systematics. These tools work best on DNA extracted from live tissues, which makes living collections such as ours ever more important scientifically. Important new studies that have used UC Botanical Garden specimens are finding exciting and sometimes disturbing results. For example, Olmstead, DePamphilis, Young, and colleagues report this spring in the *American Journal of Botany*, (Vol. 88: 348-361, 2001) that the snapdragon family (Scrophulariaceae) is not a natural evolutionary grouping. In their new interpretation, which was based in part on samples from the UC Botanical Garden, the only member of this family in the California flora that will remain in the Scrophulariaceae is the eponymous *Scrophularia californica*! Even the snapdragons (*Antirrhinum*) will no longer be in the "snapdragon" family.

Although living tissue is the *sine qua non* for molecular phylogenetics, it is still essential that every plant used in such research be vouchered. Vouchering, which involves removing a sample of the plant to produce a herbarium specimen, creates a permanent record that persists after death of the plant itself. It is essential that Garden material be vouchered so that future scientists can examine the specimen that today's botanists are using to classify plants and understand their evolutionary relationships. Thus, an important goal of the Garden is to voucher all accessioned plants in our collection. This academic year, our graduate student assistant, Rich Shefferson, has helped to voucher 274 plants in our collection.

With all this happening this year, one might ask whether Garden staff has had time to plan very far into the future. In fact, we have embarked on the early stages of strategic planning and, as the first round of construction nears completion, we will continue to move forward on this very important project.

—Ellen Simms



Garden Visitors

(left to right). Horticulturist Elaine Sellack accompanied Mark Flanagan, "keeper of the gardens" at Windsor Great Park, and William McNamara, director of Quarryhill Botanical Garden in Glen Ellen, CA, during their visit on April 16th. Mr. Flanagan was the April speaker for the California Horticultural Society meeting.

Gardening Tips

The larvae of the diamond back moth can be a serious pest for members of the cabbage family, including cabbage, broccoli, collards, kale and others. The insects are becoming resistant to Bt, which has been used widely to control the insect. A researcher in Florida found the larvae of the moths prefer feeding on high-bolting collards more than on any other member of the family. Fields of crucifers to be protected are sprayed with a crop of specially treated collards, resulting in a reduction of spray from 75 to 100%. In addition, a naturally occurring parasitic insect of diamond backs built up on the collards, and this helped control them in the desired crop. *Agricultural Research* 47 (3): 26.



The old world fern, (*Lycopodium microphyllum*), introduced into Florida in 1950, now covers over 40,000 acres. In the last 6 years, there has been a 100 fold increase. A single leaf can be 100 feet long. Fortunately, it is believed that the plant will not move farther north than central Florida. *American Nurseryman* 191 (3): 10.

Euphorbia esula, an introduced species in the northern midwestern states, has colonized vast areas of marginal and non-agricultural land, displacing many beneficial plant species. In addition, it is toxic to sheep, cattle and horses. Recently, a gall midge was released which produced galls on the stem tips resulting in their destruction, thus preventing flowering and seed production. The insect may produce 3 or 4 generations in a season though the first generation produces the largest number of adults. It is these that can be harvested and used for new releases. *Biological Control* 16(2): 128-132.

—Robert D. Raabe

The Overlooked Equation

When I was an undergraduate living in Chicago, I volunteered at local county nature preserves to help restore Illinois' endangered prairies, savannas, and wetlands. Very often, my work involved monitoring the endangered plants that grew in the area, especially the imperiled populations of native, wild lady's slippers. The lady's slippers we all know and love (*Paphiopedilum spp.*) are tropical, and have been propagated and hybridized for many years. Should you ever see a lady's slipper of the genus *Cypripedium* on display at a nursery, be warned – it was most likely stolen from the wild. Cypripedioid lady's slippers grow on the wild lands of North and Central America, Europe, and Asia, and have not been propagated successfully at all. Yet, as we have seen in other endangered plants, propagation is very often integral to successful restoration.

Why has propagation been so unsuccessful? The biology of orchids, especially the rare terrestrial orchids that evolved in the temperate regions of the world, is very complex. In fruiting structures known as pods, they produce thousands to millions of seeds no longer than a single millimeter, and half that in width. These seeds very rarely survive to produce a mature plant, and this seems to be why they have evolved to produce so many seeds all at once. The seeds scatter in the wind and find a new place to settle in the soil. Once the winter snows and rains are over, they imbibe water, and then they just sit. Why? Because they cannot progress any further.



This Cypripedium californicum in the Garden was collected by Garden horticulturist, Roger Raiche.

in their development without the aid of a soil-inhabiting fungus. The orchid family is one of the few plant families that depends completely on soil fungi for germination. This kind of interaction is called "mycorrhizal," and requires some more explanation. A mycorrhiza is an interface of two organisms – a plant and a fungus. The fungus, which can be one of many different species, grows through the soil as a mass of tiny filaments known individually as hyphae, forming a hyphal network called a mycelium. The fungus grows outward, looking

GARDEN NOTES

SUDDEN OAK DEATH...Horticulturists Judith Finn and Jerry Parsons attended an all day symposium, "Combating the Sudden Oak Death *Phytophthora*: a new disease", in Marin County, hosted by UC Cooperative Extension on March 9th.

CHANNEL ISLAND VIST...Horticulturist Nathan Smith accompanied Steven Junak, of the Santa Barbara Botanic Garden, on a three-day visit to San Nicolas Island in late March. This island is part of the southern group of Channel Islands off the coast of southern California. They were conducting plant surveys and removing exotic plants. Nathan was able to collect several plants for the Garden's Californian Area.

GARDEN SHARING...Curator Holly Forbes, distributed duplicates of the Garden's epiphytic cactus collection to the

Huntington Botanical Gardens in San Marino and to Gamma Walske Lotusland in Santa Barbara. It is common practice among gardens to share duplicates of collections, providing some protection against loss in any one location. John Trager, Curator of Desert Collections at the Huntington, donated several collections of South African material for the Garden's African Area.

RESEARCH GRANT...We are pleased to report that the Genetic Resources Conservation Program at UC Davis funded a grant proposal by Dr. Jason Koontz and Holly Forbes to study the genetic variability of Baker's Larkspur, *Delphinium bakeri*. The research will seek to determine the genetic diversity of this species to obtain base-line data for future research and conservation efforts. The grant money will pay for the cost of DNA analyses to be performed by Dr. Koontz. Baker's

for new patches of resources to digest and absorb. Part of the mycelium grows into the root system of a plant, penetrating the root tissue itself, and "colonizes" it. Other parts of the same mycelium grow far beyond the range of the plant's root system, and collect nutrients such as phosphorus and calcium.

Amazingly, the mycelium then gives the plant vast quantities of these nutrients, which are very often limiting to the plant's growth. But the fungus does not do this out of the goodness of its fungal heart! It gets a very valuable commodity from the plant: carbon. The plant produces sugar in its photosynthetic leaves, and it now appears that, on average, at least 20% of all the sugar produced by the plant goes to the fungus. This makes sense: the plant is limited much more by phosphorus, calcium, and other nutrients than carbon. Hence, the fungus and the plant seem to exist in a mutually beneficial system.

The importance of mycorrhizae is evident in the fossil record, which shows that the first land plants (now thought to be *Rhynia* species), growing roughly 500 million years ago, actually had mycorrhizal structures in their roots. Indeed, current estimates suggest that 90% of plants are mycorrhizal – a situation that clearly displays the importance of this unusual interaction.

Which brings us back to the orchid. Orchids are unlike any other plants. We are discovering that this is true in their biology as well as in their aesthetics. Orchids break all the rules. With most plants, germination and growth are possible

without fungi, although the plant will generally be stunted throughout its life. But orchids do not appear to grow without these organisms. Although some orchids can be cultivatable in the lab under very specific conditions, these orchids generally grow poorly relative to their wild-grown kin. More and more we find that most orchids cannot even germinate without a fungus.

Why should this concern us? The kind of interaction that orchids exhibit with mycorrhizal fungi is very different from what we are used to, and this has important ramifications for propagation, and ultimately restoration. First of all, we have as yet not seen any evidence that orchids donate carbon to the fungus. Second, we have found that as seedlings, and in the case of the non-photosynthetic "ghost" and "phantom" orchids, orchids even extract sugar from the fungus! Third, orchids are very particular about which fungi they will associate with, and it appears that they choose fungi that are mycorrhizal, or sometimes even pathogenic, on local trees and other plants. So, these unusual plants indirectly acquire their sugar from other plants in the ecosystem. Fourth, orchids native to the northern temperate latitudes generally stay within the soil as seedlings for many years without developing any leaves, relying on mycorrhizae for complete nourishment. Finally, even mature, photosynthetic orchids choose not to break the surface and sprout leaves in some growing seasons. This happens particularly often in lady's slipper populations. In my Midwestern study sites, I have found that lady's slippers can stay belowground like this for many years without interruption, while still growing more root and rhizome tissue. Other researchers have found very solid evidence that this "dormant" condition can last for 25 years or more. Considering that lady's slippers have very low sugar reserves, this is an amazing feat.

The key, then, to understanding what can be done to restore native orchid populations, which are in decline all over the world, is to explore this overlooked equation: orchid + appropriate fungus + appropriate conditions = successful growth.

It is an exciting topic. We are now beginning to understand the nature of this puzzling interaction, and modern scientific methods and tools, including molecular techniques, genetic sequencing, carbon-isotopes, and mathematical and statistical theory, are helping us in tackling major environmental questions. My research is an example of the conservation issues which will be investigated by Cal scientists and graduate students at the Garden's new Center for the Study of Plant Conservation.

—Richard P. Shefferson

larkspur is one of several endangered and rare California native plants the Garden is committed to helping conserve through its participation in the Center for Plant Conservation. Dr. Koontz studied the genus *Delphinium* for his dissertation project. He is now at the Center for Biodiversity of the Illinois Natural History Survey.

NEW STAFF MEMBER...
We extend a warm welcome to Ms. Leslie Wozniak who has joined the staff at the Garden in the capacity of Visitor Services Specialist. Leslie is a long time fan of the Garden and brings a wealth of work skills to the new position.





EDUCATION AT THE GARDEN

One goal of the Education Program is to encourage visitors to discover the Garden's magnificent collection and to look at plants from new perspectives. While our seasonal self-guided tours showcase different plants in their peak flowering or display seasons, other brochures focus on ethnobotanical (Chinese medicinal herbs) or special collections.



The shining silver leaves of Leucadendron argenteum make it an interesting choice for water conserving landscaping in the Bay Area. Threatened in its native habitats in South Africa it can be seen in the Garden in the Southern African Area, where it is just one of the 125 exciting plants in the new Water-Wise Gardening Tour.

(serpentine plants). Building on the interest generated through our successful collaboration at last year's San Francisco Flower and Garden Show, the Botanical Garden and the East Bay Municipal Utility District (EBMUD) have teamed up again, this time to develop a self-guided tour in the Garden. This interpretive tour of the collection focuses on plants that grow successfully in the Bay Area, but use little water. Most people have no idea how much water their garden needs. The typical Bay Area residential landscape is irrigated enough each year to flood it six feet deep. This is at least twice as much as plants need for healthy growth. Using water-efficient plants and creative design, local gardeners can create a garden that thrives on little more than natural rainfall. Properly designed, a water-efficient garden is easier to maintain than one that is over-watered. It requires less weeding, pruning, mowing, fertilizing, and pest control. It is better adapted to fluctuations in rainfall and seasonal changes. There is no one way to create a water-efficient garden. The Botanical Garden is filled with a plethora of exciting possibilities from around the world.

This walking tour of the Garden introduces you to some of these beautiful plants that thrive in the Bay Area. California's chaparral is our local community of drought tolerant plants. The climate and plant communities in Chile's matorral, South Africa's fynbos, and the

Mediterranean maquis, with their winter rains and summer drought, are but a few of the parts of the world that have water-conserving plants similar to California's chaparral. Most of the plants on this tour have been in our collection for many years.

They will give you a good idea of what that seedling in the local nursery will look like once it gets established in your garden.

This new publication is the collaboration of the Garden's horticultural, educational and communications staff working with three knowledgeable and dedicated docents — Barbara Lyss, Kathryn Welch and Alison Mills. After hours of walking through the Garden and conversations with horticulturists, Barbara, Kathy and Alison wove fascinating plant histories, horticultural information, name derivations and ethnobotanical information into stories for more than 100 plants. A lot of give and take occurred as the Garden staff vetted the information from different perspectives. Weeding out some plants that we all loved but which did not fit all the criteria was one of our biggest problems. Plants included on the tour use little water, are available (or could be available) in the horticulture trade, and are not weedy or endangered.

Ten thousand preview versions of the tour are available this Spring: in the Garden, at this year's San Francisco Flower and Garden Show and at Earth Day events. Over the next several months, Education staff will be collecting evaluations from visitors. This information will be used to improve the final version of the brochure. I invite you to come to the Garden, go on the tour, and give us your feedback.

We are grateful for EBMUD's participation and support of the process and production of this new exciting self-guided tour of the Garden.

—Jennifer Meux White

Research at the Garden

The Garden recently provided research materials to these individuals:

Ms. Eden Abram, dissertation student with Prof. Donald Kaplan, UCB Dept. of Plant Biology launched her study of comparative morphology of succulent, drought-tolerant plants. She will be using the desert collections for illustration purposes.

Prof. David D. Ackerly, Stanford University, again visited to collect many species in the Rhamnaceae (buckthorn family). He is looking at the evolution of the "evergreen sclero-phyll" strategy in California chaparral. The project is to examine each of the major taxa in comparison with their close relatives from non-chaparral habitats, employing a phylogenetic approach where possible.

Dr. Stephen Burgess, post-doc, UCB Dept. of Environmental Science, Policy, and Management, used the Mather Grove for an investigation of the basic physiological ecology of redwoods with the aim of relating climatic and hydrological factors with the growth and distribution of *Sequoia sempervirens* (Coast Redwood). They are particularly interested in quantifying direct foliar absorption of fog water by redwoods and determining its role in mitigating drought and allowing redwoods to grow to extreme heights. This study will principally involve the use of sensitive xylem sap flow meters to gauge patterns and amounts of water transport in branches and stems of redwoods.

Prof. Todd Dawson's class, Physiological Plant Ecology, used several Garden plants for measurements of photosynthesis under sun and shade conditions during the Spring Semester.

Prof. James Eckenwalder, University of Toronto, received leaf bases of *Zamia integrifolia*. These were plants used by Dr. Robert Ornduff for a study published in 1996: Gender performance in a cultivated cohort of the cycad *Zamia integrifolia* (Zamiaceae). *Amer. J. Bot.* 83: 1006-1015.

Mr. Taylor Field, dissertation student at Harvard, visited to take cuttings of primitive angiosperms for his project (*Chloranthus*, *Illicium mexicanum*, *Illicium simonsii*, *Schisandra berryi*).



Ms. Ruth Kirkpatrick, dissertation student with Prof. Brent Mishler, UCB Dept. of Integrative Biology, received fronds of several xerophytic ferns for a course project on dessication tolerance.

Ms. Nancy Kiang, dissertation student with Prof. Dennis Baldocchi, UCB Dept. of Environmental Science, Policy, and Management, tested a sap flow sensor on a Garden oak for several weeks prior to using it in the field.

Ms. Jessica Messmer McAbee, graduate student at UC Davis with Prof. Charles Gasser, visited to obtain cuttings of *Impatiens boqueriana* and *Impatiens balsaminaeflora* for her graduate studies in ovule diversification in the angiosperms.

Dr. Susana Magallon, UC Davis, post-doc with Profs. Michael Sanderson and James Doyle, received a wide range of species for their study of seed plant phylogeny, the age of angiosperms, and the evolution of pentamery among basal eudicots.

Ms. Jodi McGraw, dissertation student with Prof. Wayne Sousa, in Integrative Biology completed her soil seed bank study in the Garden's research greenhouse.

Prof. Rei Rasmussen, Oregon Graduate Institute in Beaverton, Oregon, visited the Garden to collect emissions from several oak species for his study on ter-pene release by oaks.

Mr. Andrew Salywon, dissertation student at Arizona State University, is working on the molecular systematics of the Myrtaceae family. He received cuttings of *Eugenia capuli*, *Austromyrtus dulcis*, *Myrcengenia chrysocarpa*, *Syzygium jambos*, and *Ugni molinae*.

Ms. Caroline Stromberg, dissertation student at UC Berkeley, Department of Integrative Biology, received dozens of specimens and associated herbarium vouchers for development of a phytolith reference collection.

Dr. Nori Yoshikawa, a post-doc at the University of Washington in Seattle, visited to collect *Hibbertia scandens*, *Dillenia*, and *Aextoxicon punctatum*. His main object is to find where in the phylogeny of angiosperms particular genes (the RPB2) are duplicated.

—Holly Forbes

Recognition Contributions received from 2/01/2001 up to and including 4/15/2001.

New Members

The Garden wishes to thank our new Individual and Family Members:

Mrs. Shellie Albright & Mr. Scott Emmett
Mrs. Monica Baldzikowski
Ms. Marge W. Barry
Mrs. Wendy S. Bergman & Mr. Robert G. Bergman
Ms. Barbara Bister
Ms. Suzanne M. Briley
Ms. Michaela Brockstedt
Dr. and Mrs. Daniel Callahan
Ms. Dwyn Daniels Robbie
Mr. and Mrs. Randy Davis
Mrs. Lou De Domenico
Mr. Bob Deloria
Ms. Carmel Drudy
Ms. Anna Eastwood
Ms. J. M. B. Edwards
Dr. and Mrs. Ray Ergas
Mr. Raymond Ford
Ms. Sam Foushee
Ms. Gloria Galindo
Ms. Judith E. Garvens
Mr. Kent N. Garvens
Mr. Patrick Gavin Duffy
Ms. Penelope E. Gordon
Ms. Anna Greenwood
Ms. Alix Greenwood
Ms. Jeane Hamblin-Lecky
Mr. and Mrs. Alan Hoben
Ms. Lynne Hosdey
Mr. and Mrs. David Huang
Ms. Laura J. Kainik
Ms. Gretchen Kell
Ms. Sydney Katsu
Ms. Marie C. Lagarde
Ms. A. Lim & Mr. K. Henderson
Ms. Kiamara Ludwig
Ms. Caren Maghrebian
Ms. Pradeep & Mr. Karek Mathew
Ms. Helen McKinley
Mrs. Laura Miller & Mr. Dave Miller
Mr. Charles L. Moreau
Ms. Alexandra Moss
Ms. Phyllis Peacock
Ms. Phyllis Potter & Ms. Nora Underwood
Ms. Delaine Renard & Mr. Bruce Bedortha
Ms. Janet A. Rudolph
Ms. Jeanine Sidran
Mr. Steve Siver
Ms. Jean Smith
Ms. Laura Sueoka
Ms. Anita L. Thomas
Mr. Dan Vierra
Ms. Virginia C. von Colditz

Grateful Thanks

The Garden thanks these new members for their substantial gifts over and above membership:

Ms. Patti Barker
Mr. and Mrs. David Benning
Ms. Beth Burnside
Mr. and Mrs. Ronald Clendenen
Mr. and Mrs. Fred Dengler
Mr. and Mrs. John Dolbinow
Dr. and Mrs. James E. Dryden
Ms. Fonda Kallio
Mr. and Mrs. Ron Ladd
Mr. Jim Lovekin & Priti
Mr. and Mrs. Geoff Machin
Mr. and Mrs. Robert McDonald

Ms. Eleanor Mulkey
Ms. Mildred J. O'Connor
Ms. Jean Portello
Ms. Jacqueline Woodfill & Mr. John Woodfill
(Myrtle Wolf Library)

James Harrold Van Sickler from:
Mr. and Mrs. Richard Amundsen
Mr. and Mrs. Bill Bade
(Entrance Improvement)
Mr. Michael Gilmore & Family
Mr. Bruce Hayes
Mr. & Mrs. R. Sheldon Milligan, Jr.
Mr. John P. Stock

Gifts In Kind

The Garden offers appreciation and thanks for gifts in kind:

Ms. B. Sonja Altena
Ms. Mary Lynn Cox
Louise Dutton
Myrtle Wolf

In Appreciation

The Garden offers appreciation and thanks for gifts from these donors in memory of:

Shih Ning Chen from:
Mr. & Mrs. Kenneth Palladino
(Chinese Medicinal Herb Garden)

Jean & Earl Hyde from:
Mr. & Mrs. Harry Heckman
(Myrtle Wolf Library)

Josephine Tonge Larson from:
Mr. and Mrs. Bill Bade
(Myrtle Wolf Library)

Ms. Ellen Felker

WISHLIST

The Garden particularly thanks Dr. and Mrs. David Reiffel for their contributions of a sofa and a projector for the new Center for the Study of Plant Conservation.

This issue we are asking our readers if they could support us by donating:

A "point and shoot" camera
Card tables

If you can donate, please call (510) 643-2937—we would appreciate the help.



Pictured after receiving their awards from the Director at the recent ceremony are: (Back, left to right) John Domzalski, Judith Finn, Jerry Parsons, Peter Klement, Gerald Ford. (Front, left to right) Elaine Sedlack, Nancy Swarengen, Holly Forbes and Dr. Ellen Simms, Garden Director.

Staff Members Honored

Various members of the Garden staff were recently recognized and applauded for their many years of service. Director Ellen Simms commented that the Garden is the envy of many campus units for the longevity of its staff! University service award pins were given to Holly Forbes, Gerald Ford, Jerry Parsons and Nancy Swarengen for 10+ years of service; to Elaine Sedlack for 15+ years; to Peter Klement and Roger Raiche for 20+; and to John Domzalski for 25. Judith Finn had already received her 25-year pin! Congratulations to all you long-timers!

Noteworthy Donations...

The Garden Library received several donations of books and journals. Mrs. Mary Lynn Cox donated over 130 books on garden design, horticulture, and botanical subjects. Mrs. Myrtle Wolf, donated a complete run of *Pacific Horticulture Magazine*, many issues of the *Journal of the California Horticultural Society*, several volumes of the *Bulletin of the American Rock Garden Society*, the early issues of *The Four Seasons* (journal of the Regional Parks Botanic Garden), and *Fremontia* (journal of the California Native Plant Society), among others. Additional donations of books for the library were made by Mrs. Sonja Altena and Ms. Louise Dutton. Thank you very much indeed!

GARDEN STAFF

Dr. Ellen Simms, *Garden Director*

ADMINISTRATION

Afroz Navid, *Administrative Assistant*
Margaret Richardson, *Tour & Rentals Coordinator*
Michael Rumar, *Administrative Assistant*
Candice Schott, *Business Operations Supervisor*
Nancy Swarengen, *Volunteer Services Coordinator*
Janet Williams, *Marketing & Development Officer*
Leslie Wozniak, *Visitor Services Specialist*

COLLECTIONS & HORTICULTURE

Dr. Christopher Carmichael,
Manager of Collections and Horticulture
Holly Forbes, *Curator*
Barbara Keller, *Curatorial Assistant*
Anthony Garza,
Supervisor of Horticulture and Grounds
John Domzalski, *Propagator*
Judith Finn, *Horticulturist*
Peter Klement, *Horticulturist*
Lawrence Lee, *Horticulturist*
Jerry Parsons, *Horticulturist*
Dr. Robert Raiche, *Garden Pathologist*
Roger Raiche, *Horticulturist*
Eric Schultz, *Horticulturist*
Elaine Sedlack, *Horticulturist*
Nathan Smith, *Horticulturist*
Gerald Ford, *Building and Grounds Maintenance*

EDUCATION

Dr. Jennifer White, *Associate Director for Education*
Christine Manoux, *Program Assistant*

FACULTY ADVISORY COMMITTEE

Dr. Nan Crystal Arens, *Integrative Biology*
Dr. Lewis Feldman, *Plant Biology*
Dr. Joe McIlrath, *Environmental Science, Policy, & Management*
Dr. Brent Mishler, *Integrative Biology*
Dr. Vincent Resh, *Environmental Science, Policy, & Management*
Dr. Alan Smith, *Herbarium*

NEWSLETTER

Janet Williams, *Editor*

Administration 642-0849

Development 643-2937

Director's Office 643-8999

Education 495-2803

Entrance Kiosk 643-2735

The Garden Shop 642-3343

Plant Collections 643-8040

Tours/Rentals 642-3352

Volunteers 643-1924

Fax 642-5045

E-mail: garden@clink4.berkeley.edu

Web Site: <http://www.mip.berkeley.edu/garden/>

The Newsletter is published by the University of California Botanical Garden with support from memberships. © UC Regents 2001
Articles may be reprinted with credit to the authors and the UC Botanical Garden.

CALENDAR OF EVENTS

TREES AND SHRUBS OF CALIFORNIA

We are pleased to help launch a new book from University of California Press, Trees and Shrubs of California by two distinguished faculty members from Humboldt State University, John Stuart, Professor of Forestry and John Stewart, Professor of Botany. Both authors will be with us, to share highlights of their research, and to sign copies of their book. Also on hand will be their illustrator, Andrea Pickart, exhibiting samples of her work.

Wednesday, June 13, 7:30 pm

Free

Registration requested

TWILIGHT TOURS

Celebrate the long evenings of summer with us in the Garden. Members of our horticulture staff will share their favorite spots and special insights about the Garden on Wednesday evenings at 5:30 pm. Each walk will be different, so plan to come every week during July, beginning July 11, and every week during August.

Free with Garden admission.

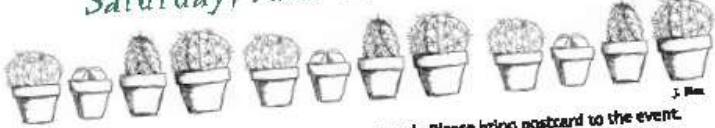
University of California Botanical Garden

Second Annual Garden Party

Please Join Us!

Enjoy fabulous food, wine and music,
stroll around the Garden at the peak of its glory,
and tour the newly renovated South African Desert Habitat.
At 4 PM we'll celebrate the opening of
the new Desert Greenhouse!

Saturday, June 16, 2001, 3 - 6 PM



Your reservation will be acknowledged by postcard. Please bring postcard to the event.

To register for any program or event*, call 510-643-2755.

University of California Botanical Garden
200 Centennial Drive, #5045
Berkeley, California 94720-5045

Address Service Requested

Nonprofit Org.
U.S. Postage
PAID

University of California

Plants are for sale at *The Garden Shop* all year. Call 510-642-3343

The Porter County
Birding Guide

INDIANA DUNES
The Casual Coast



Rose breasted Grosbeak



Baltimore Oriole



Mourning Doves

Welcome to the Casual Coast, along the southern shore of Lake Michigan. Home to the Indiana Dunes National Lakeshore, the Indiana Dunes State Park and the most diversified flora and fauna in the Midwest, the dunes are complemented by several nearby inland nature preserves. Together, they provide a unique haven for birds and birders that will make your stay on the Casual Coast both enjoyable and memorable.

TABLE OF CONTENTS

BIRD MIGRATION TO THE DUNES	1
WEATHER EFFECTS OF BIRDING	2
RAPTOR FLIGHTS	2
BIRDING SITES	35
ACCOMMODATIONS CHART	6
PORTER COUNTY MAP	7
WELCOME TO BIRDING	12
PORTER COUNTY BIRDERS CHECKLIST	13-19
ACKNOWLEDGEMENTS	20
BIBLIOGRAPHY	20

Photography provided by David Oberst

1

BIRD MIGRATION TO THE DUNES

Without doubt the presence of Lake Michigan affects the movement and distribution of birdlife in the Dunes more than any other single factor. The shores of this enormous lake provide leading lines that control flight paths of numerous migrants, and the vast open waters draw legions of transient and wintering birds. During autumn the elongate north-south boundaries of the lake become airways along which thousands of migrants navigate toward wintering areas. Southbound birds following the shores are ultimately guided into the Dunes Area, at the toe of the lake.

This avian convergence at the bottom of Lake Michigan is termed the funneling effect. • The funneling effect explains the unusually high diversity of autumn birds in northwest Indiana.



Wood Duck

Lake Michigan also provides two important avian habitats that are otherwise quite rare in the Midwest: the deep lake and the beach. Waters of the lake attract large numbers of bay and sea ducks, many of which are virtually unrecorded at inland sites in the Midwest. Additionally, the lake attracts a number of rare periodic transients, including the Purple Sandpiper, Red Phalarope, Pomarine Jaeger, Parasitic Jaeger, Great Black-backed Gull, Glaucous Gull, Iceland Gull, Thayer's Gull, Sabine's Gull, Little Gull, Black-legged Kittiwake. Extensive beaches provide resting and feeding areas for shorebirds, especially those species preferring sand rather than mudflats, e.g., Sanderling, Red Knot, and Baird's Sandpiper.

The deep waters of Lake Michigan also constitute a significant obstacle to migrants. During nocturnal flights many north-bound passersines overfly land and by daybreak finds them over the lake. When landfall is visible, they often fly directly to the shore, where they immediately land for rest and feeding.

This effect generates an anomalously high concentration of passerines in parks and woodlands immediately adjacent to the lake. (Brock 5).

1

2

WEATHER EFFECTS ON BIRDING

That most migrants fly during fair weather when trailing winds are available is well documented in ornithology textbooks. Along the shores of southern Lake Michigan this principle is most clearly evident during

Photo by Bird Count



Common Loon

the fall. Bennett (1952) discovered that the number of fall passage migrants along the Chicago lakefront tripled (compared to numbers on the day immediately prior to frontal passage) on the days immediately following passage of cold fronts.

Similarly, the most exciting autumn birding in the Dunes occurs during or immediately following the passage of cold fronts. In addition to the passerine waves that follow the fronts, northerly winds stimulate a general longshore movement of water birds.

On such occasions, an endless stream of loons, ducks, gulls, and terns often flows along the lakefront. (Brock 6).

RAPTOR FLIGHTS

Soaring hawk flights along the High Dunes must be attributed to the presence of Lake Michigan. Northern hawks, especially buteos, enjoy a leisurely spring migration, wafting effortlessly over the Midwest on balmy southerly winds. These soaring raptors, however, display a marked aversion to flying over large bodies of water. Consequently, upon encountering Lake Michigan the northerly movement is abruptly halted. Hawks turn to a course paralleling the shoreline. Thus, the migrating hawks are concentrated in a belt immediately adjacent to the lake. In effect, therefore, the High Dunes rest directly below a narrow flight corridor that extends along the lake's southern margin. (Brock 8).



Cooper's Hawk

During March and April, the major flight months, good daily flights can consist of 100 to 300 birds. Fall flights are limited; the most notable species observed is the Peregrine Falcon, with flight peaks in early October.

2



BIRDING SITES

BEVERLY SHORES A

Whether you drive or walk, Beverly Shores will produce a number of species, seen or heard, that will delight the birder. This •island• in the National Lakeshore supports habitats such as an interdunal marsh, lake, beach and wooded dune. The interdunal marsh offers excellent habitat for passerines as well as nesting species. Beverly Drive produces many opportunities to see and hear several species of birds. Best observation time is all year.

Types of migration birds seen are loons, waterfowl and gulls. Birds seen and heard in late spring and summer are Willow Flycatcher and warblers.

COFFEE CREEK WATERSHED PRESERVE B

The preserve is a 167 acre home to over 500 native plants, trees, sedges and forbs as well as over 4 miles of trails. Wetlands can be found throughout the landscape including swamps, marshes, wet prairies and fens. Birds of Coffee Creek include several species of woodpeckers such as Downy and Hairy Woodpeckers. Herons, hawks, and state endangered marsh wren can be seen in their respective habitats. Bridge 5, near the southern end of the trail, see Cardinals, Indigo Buntings and the Tufted Titmouse. From the Water Plaza, at the northern area of the preserve, Belted Kingfishers can be seen fluttering near the wetlands. Don't miss the Killdeer who often nests near Phillips Pond.



COWLES BOG C

Wooded alders, savannah, marshes and wooded swamp

Photo: K. Morris

provide ideal habitats for Common Yellowthroat, Sora,

general. For more information call 219/926-7561 ext. 225.

Virginia Rail, Blue Grosbeak, Woodcock, Scaly-breasted

S



BIRDING SITES

PORTER BEACH HAWK WATCH D

Formerly known as the Johnson Beach hawk watch, this stabilized dune allows prime viewing of several hawk flights, especially in the spring.

WEST BEACH & LONG LAKE E

Following the West Beach trails which take you by the beach, an interdunal pond, and wooded dune, one may discover a Hairy Woodpecker or two and perhaps a Common Yellowthroat. Long Lake may grace one with the presence of Least Bitterns, warblers and scores of waterfowl. A parking fee is required in the summer.



INDIANA DUNES STATE PARK F

Indiana Dunes State Park encompasses a variety of habitats including savannah, marshy grass covered dunes, bluffs, beaches and ponds. Several trails run through these areas, providing opportunities for field sparrows, flycatchers, thrushes, warblers, hawks, owls and more. Observation areas would include the forest and the marsh woods along with trails 2 and 10. Trail 9 allows for eye level bird watching because of its higher elevation. Wilson Shelter also attracts several birds during spring migration. Entrance fee.



PORT OF INDIANA G

During winter one can best observe the Horned Larks, Lapland Longspurs, Snow Buntings, Common Mergansers and bay ducks from the public access area of the Port of Indiana. On windy days, birds fly almost directly over the public access area.

SUNSET HILL FARM COUNTY PARK H

Porter County's ongoing commitment to ecological integrity

dairy farm is filled with woods, meadows, and three ponds. Part-time naturalists are

available during three seasons of the year to offer a wide range of opportunities

including natural science projects on ponds, trees, birds, wildflowers or fields. With

over ten miles of trails, bird watchers, nature photographers, or woods walk observers



BIRDING TRAIL

TALTREE ARBORETUM & GARDENS

Taltree Arboretum & Gardens offers the bird enthusiast a chance to explore. Prairie, Savanna, Woods, Wooded Edge, and Wetland can all be easily observed at this 300-acre trail. Taltree is a special place to bird. For more birding opportunities visit them at www.taltree.org (Mondays)



ROGERS LAKWOOD PARK

A 122 acre facility of the Valparaiso Park Department, it is home to hiking trails, a beach, fishing, boating, and swimming. Birds commonly seen at Rogers Lakewood Park include: native waterfowl such as Canada geese and mallard ducks, herons, hawks, and common songbirds. Daily entry fees are collected from Memorial Day through Labor Day and are charged by the carload.

JASPER-PULASKI FISH AND WILDLIFE AREA

The Jasper-Pulaski Fish and Wildlife Area has long been the sight of the annual migration of Sandhill Cranes. View this awesome spectacle during the fall to see thousands of these birds as they rest from their journey and feed. Springtime also brings the cranes, but in a lesser amount. Don't forget the binoculars or a scope! During the spring and summer, the area boasts ducks, geese, and egrets that are viewable from the observation trail. Jasper-Pulaski Fish and Wildlife Area is also a public hunting area. Please check in at the headquarters to obtain information about the affected areas before setting out.

Photo by National Geographic



HERON ROOKERY

Observe the Great Blue Heron in the spring and summer at this mature woodland located along the Little Calumet River. Migrant warblers are present in the spring along the channel among other species.



ACCOMMODATIONS GUIDE

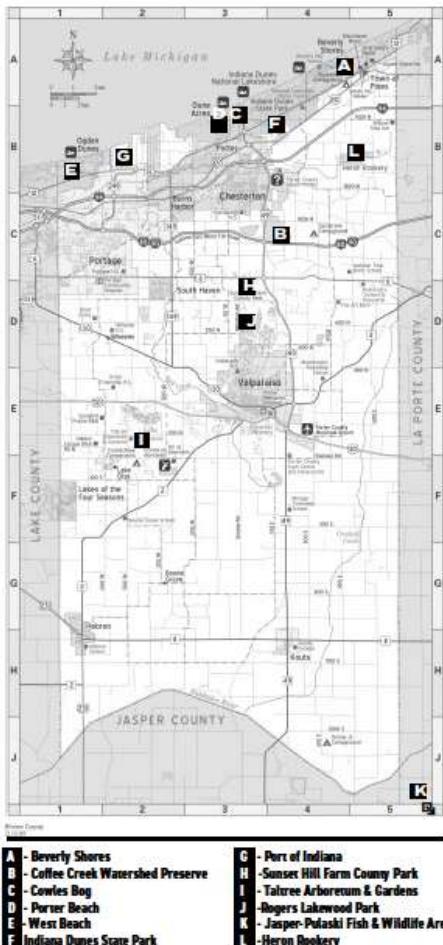
Classification	Portage	Valparaiso	Bed & Breakfast	Campgrounds
\$	\$20-\$40 price per room	\$5	\$40-\$60 price per room	
\$\$	\$60+ price per room	\$\$\$\$	\$80+ price per room	
55	Eaton Lodge State Road 40 and Indiana Boundary Road Hillside Campground State Road 40 and U.S. Highway 20 Indiana State Resort & Spa, State Road 40 and Indiana Boundary Road	219/745-4428 or 800-99-9999 219/745-5000 or 800-724-1200 219/745-2200 or 800-826-4202 219/745-8500 or 800-826-8500 219/745-4224		
55+	Concordia Motel State Road 300 and U.S. Highway 20 Clement Inn State Road 300 and I-90/I-94 Days Inn State Road 210 and U.S. Highway 20 Dove Inn State Road 300 and U.S. Highway 20 Dove's Motel State Road 300 and U.S. Highway 20 Hampton Inn State Road 300 and U.S. Highway 20 Holiday Inn Express State Road 300 and I-90/I-94 Homestead Inn State Road 300 and U.S. Highway 20 Inn & Suites State Road 300 and U.S. Highway 20 Jewell House Inn U.S. Highway 20 and Illinois Springs Road	219/745-2277 or 800-626-8118 219/745-2220 or 800-822-0200 219/745-2230 or 800-822-0200 219/745-4901 219/745-4227 219/745-4227 219/745-2200 or 800-826-8118 219/745-7777 or 800-410-1117 219/745-8840 or 800-827-8840 219/745-4267 or 800-826-8260 219/745-2200 and U.S. Highway 20		
56	Elk Ridge Motel U.S. Highway 20 Elkhorn Motel U.S. Highway 20 Family Inn Motel U.S. Highway 20 and State Road 300	219/745-2116 219/745-2000 or 800-826-8260 219/745-4727		
56+	Empire City Motel State Road 40 and U.S. Highway 20 Foothills Inn State Road 40 and U.S. Highway 20 Hampton Inn & Suites State Road 40 and U.S. Highway 20 Holiday Inn Express U.S. Highway 20 and State Road 2 Inn & Suites State Road 300 and State Road 2 Vanderbilt Motel U.S. Highway 20 and State Road 2	219/745-2700 or 800-822-2222 219/745-8200 or 800-826-2344 219/745-2000 or 800-826-2000 219/745-2000 or 800-826-2000 219/745-4688 or 800-826-8268 219/745-0000 or 800-826-8000 219/745-2702		
57	Emma Shores Inn U.S. Highway 20, Indiana Dunes Foggy Harbor Inn State Road 40 and Indiana Boundary Road, Munster Hidden Harbor Perry Road 10 North, Valparaiso, Indiana The Inn at Abberley State Road 2, Valparaiso, Indiana Roughneck Motel County Road 100 North, Valparaiso, Indiana Tin Top Inn County Road 200 North, Tin Top	219/745-4429 219/745-4701 219/745-4701 219/745-4701 219/745-2705 219/745-4874 or 877-808-8080 219/745-4200		
57+	Country Inn & Cottages Wabash Road, Valparaiso, Indiana Dunes Inn County Road 200 East, Munster Domestic Encampment U.S. Highway 22, Indiana National Lakeshore, Munster, Indiana Sand Groves Campground County Road 200 East, Munster State Park Campground State Road 40, Indiana State Park, Munster Valley Deer's Polyester Camp Resort Old River Road, Munster	219/745-8764 219/745-4234 219/745-4234 219/745-7401 or 800-826-8704 219/745-9822 219/745-4220 219/745-4220 219/745-7707		

5 \$20-\$40 price per room \$5 \$40-\$60 price per room
55 \$60+ price per room \$\$\$\$ \$80+ price per room

5



Potawatamie County Map



Custom Seed Blends • Garden Accents • Binoculars
Birdhouses • Feeders • Bird Baths • Nature Gifts

Wild Birds Unlimited
Your Backyard Birdfeeding Specialist®
Visit our website at www.wbu.com

We Bring People and Nature Together
(219) 465-0508
4205 Calumet Avenue
Valparaiso, IN

**Holiday Inn
EXPRESS**
Bird Watching Extravaganza

2525 Wabashaw Road
Portage, IN 46368
(219) 782-1439
I-94 Exit 23, 1/4 mile
South of Exit 9, 1-88
800-95-POCI8
www.holidayinnexpress.com

Area Attractions:

Minutes from the shores of Lake Michigan
Woodland Park (1 minute)
3½ miles East of Chicago
Variety of restaurants nearby

Amenities Include:

- Manager's Reception (Yankee-Pines 5-7pm)
- Unique Spa Suites with Over-sized Whirlpool Tub
- Expanded Commercial Kitchen
- Heated Indoor Pool and Fitness Center
- Kidzuh!™ - Perfect for Families with Children
- Color TV with HBO, CNN, ESPN
- Sealy® Mattresses
- Meeting and Banquet Facilities
- In-room Iron and Ironing Board

**Chesterton Feed
Garden Center, Inc.**

- N.W. Indiana's premier garden center
- Patio Gift Shop - Unique & beautiful products for home & garden
- Happy Pet Place complete line of pet foods & pet supplies
- Always the finest variety of wild bird seed & bird feeders

400 Locust Street • Chesterton, IN
www.duneland.com/cfgc.html
Open everyday all year: Call (219) 926-2700

**Williams Creek
Accommodations**

Williams Creek Accommodations
812-526-2700 or 800-334-2700
www.williams creek.com

• A Lodge & Wicker Room
Whisper of Pineapple Specialty Room

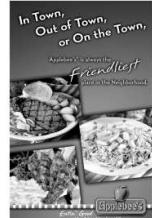
• Full Service Spa & Salon

• Awarded Meeting of Banquet Center
Capacity of Special Events up to 140 people

Come Out and Play

The Banana Golf Club is a large, rugged, wooded course that contains over 18 holes of challenging golf. The facility is owned by Jim Miller and has an experienced and local head professional on hand to assist you with an exceptional experience.

For More Information,
Please Call 219-921-1192



We're Ready to Welcome You!

VALPARAISO

Fairfield Inn
U.S. 30 & State Road 49
CALL 800-28-FAIR or
219-464-2800 ext. 101 or
www.fairfieldinn.com/VPIPC

Courtyard
U.S. 30 & State Road 49
CALL 800-28-COUR or
219-464-1700 ext. 101 or
www.courtyard.com/VPIPC

Davy likes just anywhere. There are two great hotels in Valparaiso have for you, the Courtyard and Fairfield Inn by Marriott. Both friendly staff members are always offering the best rates and services to make your stay enjoyable.

- Easy access from Route #4 and I-80
- Restaurants, shopping, and more shopping
- Indoor pool, whirlpool and exercise rooms

Country Charm in the Heart of the Dunes

Nestled amid the woodlands and wildflowers of the Indiana Dunes, Springhouse Inn offers a comfortable atmosphere complemented by thoughtful amenities and attentive service. You can enjoy the cozy warmth of a bed & breakfast inn, with the clean, friendly service of a hotel, featuring...

**SPRING
HOUSE
INN**
the perfect getaway.
ASK ABOUT OUR WHIRLPOOL ROOMS!

Call 219-929-4600 or 866-DUNES-00
or visit www.springhouseinn.com
303 Mineral Springs Road Porter, IN 46304

Accommodations & Services

- 30 beautifully appointed, oversized country rooms, each with private bath, and balcony or porch
- Many rooms offer woodland views
- Indoor swimming pool
- Dry sauna & oversized whirlpool, exercise room
- Computer room, complimentary breakfast served daily in our Main House library
- Picturesque sitting rooms
- Two meeting rooms with audio visual training boards
- Four meeting rooms for up to 16 people

Located just 40 minutes from Chicago, Springhouse Inn, one of Chesterton's finest hotels, provides a lodging and dining respite option only 2 miles from the Indiana Dunes.

**Escape at...
Hidden Escape
Bed & Breakfast**

An Intimate Getaway in the Country

**A Private Bungalow
Deep in the Woods**

Gazebo • Hot Tub • Sunroom
Whirlpool • Living Room • Master Bedroom

*Birthdays, Anniversaries,
Weddings, Honeymoons
A Great Getaway - Weekend Packages*

We Accept:

219-759-4701
www.hiddenescape.com

A Great Gift Making Time for Each Other



Welcome to Birding!

WELCOME TO THE WONDERFUL WORLD OF BIRDING!
If you like watching birds in your backyard or you want to travel the world to see all 10,000 bird species, use these ten tips to get started! You might also want to visit WildBirds.com, a great site for newer birders!



Hint #1: You need a field guide for your area. A field guide is a book with pictures of the birds and tips for identifying them.

Hint #2: You need a binocular to see the birds. (Hint: you need four eyes to use binoculars.)

Hint #3: You need to know what to expect in your area. Checklists of birds in your area will tell you this. See pages 13-19 for the Porter County Bird Checklist. **Hint #4:** You need to be able to find the birds. To do this, you should learn about the habitat each species of bird prefers. See page 13 for Habitat information and the Bird Checklist for where to spot each species.

Hint #5: Join a group of other birders. Birders are very friendly and helpful. They are always willing to share their knowledge. We were all beginners once.

Hint #6: Try a birding trip or tour. Local bird trips are sometimes advertised in the newspapers. Check out the Birding Sites information on pages 3-5 for information on local bird treks.

Hint #7: Read about birds. There are many good magazines about birds and birding. For North American birds: *Birders World*, *Bird Watcher's Digest*, *Birding* and *WildBird* are magazines you might like.

Hint #8: Bring the birds to you. You can attract birds to your yard with just a little work. Planting the right flowers will attract hummingbirds. Sunflower seeds will bring lots of new birds to your house. You might even want to build a bluebird house.

Hint #9: Record your bird sightings. You might want to keep a diary or list of the birds you see in your yard. You can also keep a list of birds you see in your town or on your vacation. Birders often keep lists for their county, state or country. The Porter County Bird Checklist can be found in this guide on pages •

**Hint #10: HAVE FUN. ASK LOTS OF QUESTIONS.
BE KIND TO BIRDS.**

These hints are from the popular birding website - Birding.com

12



Porter County Birding Checklist

SEASONAL ABUNDANCE CODES:

A = ABUNDANT: Often observed and widespread throughout county

C = COMMON: Frequent in appropriate habitat

U = UNCOMMON: Infrequent in appropriate habitat

R = RARE: Unlikely, but possible in county

HABITAT TYPES & LOCATIONS

I-LAKE; B-BEACH: Lake Michigan and its beachfront including: Beverly Shores, Indiana Dunes State Park, Indiana Dunes National Lakeshore

D-DUNES: Indiana Dunes State Park, Indiana Dunes National Lakeshore

F-FIELDS: Cultivated and roadside fields, open areas and prairies such as those found at Tidbit Arboretum & Gardens, Indiana Dunes National Lakeshore, Sunset Hill Farm County Park and Coffee Creek Watershed Preserve

FL-FLIGHT: Observed in flight

M-MARSH: Areas regularly inundated by shallow water for much of the year. Intertidal marshes are found along Lake Michigan at Beverly Shores, Indiana Dunes National Lakeshore & Indiana Dunes State Park. Marshes are also found along county rivers, the most notable being the Kankakee River at the southern border of the county and at Kankakee Fish & Wildlife Area in neighboring Stark County

P-PONDS: Permanent bodies of water that include small lakes, ponds and wetlands: Long Lake, Tidbit Arboretum & Gardens, Rogers Lakewood Park, Coffee Creek Watershed Preserve, Sunset Hill Farm County Park and Indiana Dunes National Lakeshore S-SWAMPS: Wetlands that are poorly drained with trees growing throughout. There are numerous types of swamps in the county and they can be found at: Indiana Dunes State Park, Indiana Dunes National Lakeshore, Beverly Shores (along Beverly Drive), Coffee Creek Watershed Preserve, Tidbit Arboretum & Gardens and the Kankakee River Floodplain

W-WOODS: Beverly Shores, Indiana Dunes National Lakeshore, Sunset Hill Farm County Park, Tidbit Arboretum & Gardens, Indiana Dunes State Park, Coffee Creek Watershed Preserve WE-WOODED EDGES: Coffee Creek Watershed Preserve, Tidbit Arboretum & Gardens, Sunset Hill Farm County Park, Indiana Dunes National Lakeshore, and Indiana Dunes State Park

U-URBAN: Urban areas throughout the county

13

1 Northern Country Bird Lists

Bird	Seasons					Habitat
	SP	S	F	W		
Loon & Grebes						
*Common Loon	C	R	C	R	L	
*Pied-billed Grebe	C	C	C	R	M,P	
*Horned Grebe	U	C	C	R	L,H	
Cormorants						
*Double-crested Cormorant	C	U	C	R	L	
Bitterns & Herons						
American Bittern	U	U	U	R	M	
Least Bittern	R	R	R	R	M	
*Great Blue Heron	A	A	A	R	M,P	
*Great Egret	C	U	C	R	M	
*Green Heron	C	C	C	R	M,P	
Black-crowned Night Heron	U	U	U	R	M	
Yellow-crowned Night Heron	U	U	U	R	M	
Swans, Geese & Ducks						
*Mute Swan	C	C	C	C	L,P	
*Tundra Swan	U	U	R	R	L	
*Canada Goose	A	A	A	A	L,M,P	
*Wood Duck	A	A	C	R	P,S	
*Green-winged Teal	C	R	UR	R	M,P	
*Black Duck	C	R	C	U	L,M	
*Mallard	A	A	A	C	L,P,M,	
*Northern Pintail	U	R	U	R	M,P	
*Blue-winged Teal	C	U	C	R	M,P	
*Northern Shoveler	C	R	U	R	M,P	
*Gadwall	C	R	C	R	M,P	
*American Wigeon	C	R	C	R	M,P	
*Canvasback	U	R	R	U	M,P	
*Redhead	C	R	U	R	L,P	
*Ring-necked Duck	C R C R M,P	*Greater Scaup	U R U U L,P			
*Lesser Scaup	C R C U L,P	*Black Scoter	R R U R L			

* State endangered

W

2 Northern Country Bird Lists

Bird	Seasons					Habitat
	SP	S	F	W		
Pred-tailed Hawk						
*Rough-legged Hawk	U	U	U	U	U	F,WE,F,M
Osprey & Falcons						
Osprey	U	R	U	R	L	
*American Kestrel	C	C	C	C	F	
Peregrine Falcon	U	U	U	U	FL	
Quail, Pheasant, Turkey						
*Northern Bobwhite	U	U	U	U	F,WE	
*Ring-necked Pheasant	U	U	U	U	F	
*Wild Turkey	U	U	U	U	F,W	
Rails & Coots						
Virginia Rail	U	U	U	U	M	
*Sora Rail	C	U	U	U	M	
*Common Moorhen	R	R	R	R	M	
*American Coot	A	A	A	A	M,P,L	
Crane						
*Sandhill Crane (Jasper-Pulaski Site)	C	U	C	U	F,M	
Plovers						
*Black-bellied Plover	U	R	U	R	B,P	
*American Golden Plover	C	R	U	R	B,P	
*Semipalmated Plover	U	R	U	R	B,P	
Piping Plover	R	R	R	R	B	
*Killdeer	A	A	C	R	M,D,F	
Sandpipers & other Shorebirds						
*Greater Yellowlegs	U	R	R	R	M,P	
*Lesser Yellowlegs	U	U	U	U	M,P	
*Solitary Sandpiper	C	U	U	U	M	
*Spotted Sandpiper	C	C	U	U	M,S	
*Semipalmated Sandpiper	U	R	C	R	B,P	
*Least Sandpiper	U	U	U	U	B,P	
*Pectoral Sandpiper	C	R	U	U	M,P	
*Baird's Sandpiper	R	R	U	U	B	
*Ruddy Turnstone	U	R	U	U	B	
*Sanderling	R	C	C	C	B	
*Dunlin	U	R	U	U	B,P	
*Red Knot	R	R	R	R	B	
*Purple Sandpiper	R	R	R	R	B	
*Short-billed Dowitcher	R	R	R	R	P	
*Ruddy Turnstone	U	U	U	U	LB	
*Common Snipe	U	R	U	U	M,P	
*American Woodcock	C	C	C	R	S,W	
Jaegers						
*Parasitic Jaeger					LB	
*Pomarine Jaeger					LB	
Gulls						
*Little Gull	R	R	U	R	L	
*Bonaparte's Gull	C	R	C	U	LB	
*Laughing Gull	U	R	R	R	L	
*Ring-billed Gull	A	C	A	C	LB	

* State endangered

W



Northeastern Birders

CANADA **Seasons**

Bird	SP	S	F	W	Habitat
*Herring Gull	A	U	A	A	LB
*Thayer's Gull	R	R	U	U	LB
Iceland Gull	U	R	R	L	L
*Glaucous Gull	R	R	U	U	LB
*Great Black-backed Gull	U	R	R	U	L
*Sabine's Gull	R	U	R	U	L
*Black-legged Kittiwake	R	R	U	R	L
Terres					
*Caspian Tern	C	U	R	R	LB
*Common Tern	C	R	R	U	LB
*Forster's Tern	U	R	U	U	LB
Black Tern	R	U	R		M,B
Doves					
*Rock Dove	C	C	C	C	U
*Mourning Dove	A	A	A	A	FW
Cuckoos					
*Black-billed Cuckoo	U	U	U		WE
*Yellow-billed Cuckoo	U	U	U		WE
Owls					
*Short-eared Owl	R	R	R	U	FM
*Great Horned Owl	C	C	C	C	W
*Snowy Owl		R	R	B	B
*Barred Owl	C	C	C	C	S
*Northern Saw-whet Owl	R		R	W	
*Eastern Screech Owl	C	C	C	C	W
Goatsuckers					
*Common Nighthawk	C	A	C		WE,F
*Whip-poor-will	C	U	U		W
Swifts					
*Chimney Swift	A	A	A		U
Hummingbirds					
*Ruby-throated Hummingbird	C	C	C		FW,WE
Kingfishers					
*Belted Kingfisher	C	C	C	R	MP
Woodpeckers					
*Red-headed Woodpecker	C	C	C	C	W
*Red-bellied Woodpecker	C	C	C	C	W
*Yellow-bellied Sapsucker	C	R	U	R	W
*Downy Woodpecker	C	C	C	C	W,WE
*Hairy Woodpecker	U	U	U	U	W
*Northern Flicker	C	C	C	U	W
*Pileated Woodpecker	U	U	U	U	W

* State endangered

16



Northeastern Birders

CANADA **Seasons**

Bird	SP	S	F	W	Habitat
Flycatchers					
*Olive-sided Flycatcher	U	R	U		S
*Eastern Wood Pewee	C	C	C		W
*Yellow-bellied Flycatcher	U	R	R		W
*Acadian Flycatcher	C	C	R		W
*Alder Flycatcher	U	U	R		M
*Willow Flycatcher	C	U	R		M
*Least Flycatcher	C	R	C		W,WE
*Eastern Phoebe	C	C	U		F,W,WE
*Great-crested Flycatcher	C	C	U		W
*Eastern Kingbird	C	C	U		FM
Larks					
*Horned Lark	C	U	U		F
Swallows					
*Purple Martin	C	C	C		FP
*Tree Swallow	C	A	C		FM
*Rough-winged Swallow	U	U	U		FM
*Bank Swallow	C	C	C		BD
*Cliff Swallow	R	R	R		F
*Barn Swallow	C	A	C		F
Jays & Crows					
*Blue Jay	A	A	A	A	W,WE
*American Crow	A	A	A	A	ALL
Titmice					
*Black-capped Chickadee	C	C	C	C	W
*Tufted Titmouse	C	C	C	C	W
Nuthatches					
*Red-breasted Nuthatch	U	R	U	U	W
*White-breasted Nuthatch	C	C	C	C	W
Creepers					
*Brown Creeper	C	R	C	U	W
Wrens					
*Carolina Wren	U	U	U	U	WE,U
*House Wren	C	C	C	U	WE,U
*Winter Wren	U	R	U	R	W
Marsh Wren	U	U	U	U	M
Sedge Wren	U	R	R	R	FM
Old World Warblers, Thrushes & Allies					
*Golden-crowned Kinglet	C	R	C	R	W
*Ruby-crowned Kinglet	C	R	C	R	W
*Blue-gray Gnatcatcher	C	U	R		W
*Eastern Bluebird	C	C	C	U	F,WE
*Veery	U	U	U	U	W
*Gray-cheeked Thrush	U	U	U	U	W

* State endangered

17

⑦ Norman County Birds

Bird	SP	Seasons				Habitat
		S	F	W	E	
*Swainson's Thrush	U		C	R		W
*Hermit Thrush	C		C	R		W
*Wood Thrush	U	U	U	R		W
*American Robin	A	A	A	U		F,W
Thrashers						
*Gray Catbird	C	C	C	R		WE
*Northern Mockingbird	U	U	U	R		F,W,E
*Brown Thrasher	C	C	C	R		WE
Waxwings						
*Cedar Waxwing	C	U	C	U		W,M
Starlings						
*European Starling	A	A	A	A		ALL
Vireos						
*White-eyed Vireo	U	R	U			W
*Solitary Vireo	U	R	U			W
*Yellow-throated Vireo	C	U	U			W
*Warbling Vireo	C	C	U			WE,P
*Philadelphia Vireo	U	R	U			W
*Red-eyed Vireo	C	C	C			W
Warblers						
*Blue-winged Warbler	C	U	U			WE
Golden-winged	R	R	R			WE
Warbler						
*Tennessee Warbler	C	R	C			W
*Nashville Warbler	C	R	C			W
*Northern Parula	U	R	R			W
Warbler						
*Orange-crowned	U	R	U			W
Warble						
*Yellow Warbler	C	C	R			WE,M
*Chestnut-sided	C	R	U			W,WE
Warbler						
*Magnolia Warbler	C	R	C			W
*Cape May Warbler	C	R	C			W
*Yellow-rumped	C	R	C			W,M
Warbler						
*Black-throated	C	R	C			W
Green Warbler						
*Blackburnian	C	R	C			W
Warbler						
*Prairie Warbler	U	U	R		D	
*Palm Warbler	C	R	C			WE,M
*Bay-breasted	C	R	C			W
Warbler						
*Blackpoll Warbler	C	R	C			W
*Cerulean Warbler	C	C	R			W
*Black and White	C	R	C			W
Warbler						
*American Redstart	C	U	C			W
*Ovenbird	C	C	U			W
*Northern	U	R	U			WE,M
Waterthrush						
*Louisiana	U	R	U			S
Waterthrush						
*Mourning Warbler	R	R	R			WE

* State endangered

18

⑦ Norman County Birds

Bird	SP	Seasons				Habitat
		S	F	W	E	
*Common Yellowthroat	C	C	C			M
*Hooded Warbler	U	R	R			S
*Wilson's Warbler	C	R	C			W
*Canada Warbler	C	R	C			W
*Yellow-breasted Chat	U	R	R			M,WE
Tanagers						
*Scarlet Tanager	C	C	U			W
Cardinals & Buntings						
*Northern Cardinal	A	A	A	A		F,WE
*Rose-breasted Grosbeak	C	C	C			W
*Indigo Bunting	C	C	C			F,WE
*Dickcissel	U	U	U			F
Sparrows						
*Eastern Towhee	C	C	C	R		WE
*Tree Sparrow	C	C	C			F,WE,D
*Chipping Sparrow	C	C	C			F,D,M
*Field Sparrow	C	C	C	U		F,D
*Vesper Sparrow	U	U	U	U		F,D
*Savannah Sparrow		U	U	U		F,D
*Grasshopper Sparrow	U	U	U			F
*Fox Sparrow	C	C	C	R		WE
*Song Sparrow	C	C	C	U		M,WE
*Lincoln's Sparrow	U	U	U	U		W
*Swamp Sparrow	C	C	C	R		M,S
*White-throated Sparrow	C	C	C	R		WE
*White-crowned Sparrow	C	C	C	R		WE
*Dark-eyed Junco	C	C	R	A		WE
*Lapland Longspur	R	R	R	R		B
*Snow Bunting	R	R	R	U		F,B
Blackbirds & Orioles						
*Bobolink	C	C	R	A		F
*Red-winged Blackbird	A	A	A	A		F,M,S
*Eastern Meadowlark	C	C	C			F
*Western Meadowlark	R	R	R			F
Yellow-headed Blackbird	R	R	R			M
*Rusty Blackbird	U	R	U	R		S
*Common Grackle	C	C	C	U		M,F
*Brown-headed Cowbird	C	C	C	U		W,WE
*Baltimore Oriole	C	C	U	U		W,WE
*Orchard Oriole	U	U	U	U		W,WE
Finches						
*Purple Finch	U	U	U	U		W
*House Finch	A	A	A	A		U
*Common Redpoll	R	R	R	U		WE
*Pine Siskin	R	R	R	U		WE
*American Goldfinch	A	A	A	A		F,WE,U
*Evening Grosbeak	R	R	R	U		WE
Old World Sparrows						
*House Sparrow	A	A	A	A		U

* State endangered

9



ACROSS THE GARDEN STATE

The Porter County Convention, Recreation & Visitors Commission (PCCRVC) would like to give special thanks to David Oberst, Director of Education and Naturalist at Taltree Arboretum & Gardens, and Taltree board member, Laurie Eberhardt, Ph.D., for their help in creating this guide. The PCCRVC is truly grateful for their help.

TALTREE ARBORETUM & GARDENS: A SPECIAL PLACE TO BIRD*

Taltree offers the birder a wide variety of habitat at one location: Prairie, Savanna, Woods, Wooded Edges, Swamp, Pond and open Wetland, can all be easily observed at this 300+ acre site. More than 60 species of birds have been identified on Taltree's property. The Bluebird Trail derives its name from the numerous Bluebird nesting boxes along its route. Eastern Bluebirds are a common site at Taltree. The trail directs visitors along the perimeter of the prairie in an effort to reduce disturbance to wildlife and restore habitat to natural nesting conditions. As a result grassland nesting birds, such as the Bobolink, that need a large area of undisturbed habitat for survival have abundantly returned. This trail also traverses a 7 acre open wetland, which holds abundant migratory waterfowl in the spring. Wood Ducks are a common site as they utilize nesting boxes in the wetland. In 2002, a Hooded Merganser successfully nested at Taltree. Migrating spring warblers can be viewed in abundance along the Heron Pond Woodlands and Owl Trails. Taltree is an excellent site to view raptors. Red tailed, Cooper's and Sharp shinned Hawks are year round residents. During the winter and early spring months a pair of Northern Harrier Hawks regularly patrol the open space at the arboretum. Wild Turkey, Ring necked Pheasant and Bobwhite Quail are also present. Other birds of particular interest are American Woodcocks, Eastern Meadowlarks, Dickcissels, Indigo Buntings, Rose breasted Grosbeaks, Baltimore Orioles and the Savanna and Grasshopper Sparrows. Taltree Arboretum & Gardens: A Natural Inspiration.

Bibliography

Brock, Kenneth J. *Birds of the Indiana Dunes*. (Revised Edition) Shirley Heinz Environmental Fund, 1997.

Sibley, David A. *Memorable Sibley Guide to Birds*

United States. *Birds of the Indiana Dunes National Lakeshore*. (Revised Edition) Indiana Dunes National Lakeshore, 1991.

Special thanks to Ken Brock for permission to use information about birding in the Indiana Dunes directly from his book, *Birds of the Indiana Dunes*.

20



There's still more...

to see and do at the Casual Coast. There are several more specialty guides, each geared to people's special interests!



Call, write, or visit our website to
request your free specialty guides.

INDIANA DUNES
The Casual Coast

Produced by the Porter County Convention,
Recreation, & Visitor Commission
800 Indian Boundary Road Chesterton, Indiana 46304
219/926-2255 • 800/288-8687
www.indianadunes.com • www.casualcoast.com

APPENDIX C - METADATA

13.6 Author metadata for F:\guide.doc

Properties ▾

Size	51.7KB
Pages	2
Words	983
Total Editing Time	2 Minutes
Title	An Insiders Guide to Enjoyi...
Tags	Add a tag
Comments	Add comments

Related Dates

Last Modified	15/09/2002 16:17
Created	15/09/2002 16:09
Last Printed	

Related People

Author

 Paul Teddy
Add an author

Last Modified By

 Paul Teddy

17.2 File name metadata for stuf.doc

Properties ▾

Size	41.7KB
Pages	1
Words	17
Total Editing Time	6 Minutes
Title	Birds To Find
Tags	Add a tag
Comments	Add comments

Related Dates

Last Modified	09/02/2005 16:57
Created	09/02/2005 16:51
Last Printed	

Related People

Author

 John Doe
Add an author

Last Modified By

 John Doe

APPENDIX D - E-MAIL ANALYSIS

1.2 E-mail received 16/10/04 contents

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 recognize each neighbor immediately, even at a distance.

Paying attention to individual differences can help you identify birds, too. You can recognize 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, familiarize yourself with the field marks- colored or patterned areas on the bird's body, head, and wings- that help distinguish species.

1.2 E-mail received 16/10/04 headers

-----HEADERS-----

```
-Account-Key: account2
X-UIDL: vmyLTMZm6jBNjghPvFqQ
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
Message-Id: <WnifxIWJ4fCUPH80kr3g@fakepop.invalid>
Date: Wed, 09 Feb 2005 11:08:01 +0000
X-UIDL: vmyLTMZm6jBNjghPvFqQ
X-fakepop-version: 7
X-fakepop-build: Dec 4 2004 17:08:02
X-fakepop-url: http://vztech.com.br/software/fakepop/
X-Message-Flag: message delivered by fakepop - http://vztech.com.br/software/fakepop/
Envelope-to: jdoe@example.com
Delivery-date: Sat, 16 Oct 2004 18:51:39 +0100
Received: from outgoing.birds.com ([192.168.231.26] helo=outgoing2.birds.example.com) by mail.example.com with esmtp (Exim 4.34) id 1CIWEs-0005v3-7o for jdoe@example.com; Sat, 16 Oct 2004 18:51:39 +0100
Received: (qmail 23682 invoked from network); 16 Oct 2004 07:08:32 -0000
Date: Sat, 16 Oct 2004 15:20:15 +0200
From: Bird Fanciers <mailinglist@birds.example.com>
To: jdoe@example.com
Subject: How to Identify Birds
```

---END HEADERS--

2.1 E-mail received 17/11/04 contents

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?"

2.2 E-mail received 17/11/04 headers

-----HEADERS-----

-Account-Key: account2
X-UIDL: ml9vNXPVmE7PpsleLfhS
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
Message-Id: <FcJjpiktBLDJt7QctR1@fakepop.invalid>
Date: Wed, 09 Feb 2005 11:08:01 +0000
X-UIDL: ml9vNXPVmE7PpsleLfhS
X-fakepop-version: 7
X-fakepop-build: Dec 4 2004 17:08:02
X-fakepop-url: http://vztech.com.br/software/fakepop/
X-Message-Flag: message delivered by fakepop - http://vztech.com.br/software/fakepop/
Envelope-to: jdoe@example.com
Delivery-date: Wed, 17 Nov 2004 19:51:39 +0100
Received: from example.org ([192.168.231.26] helo=example.org) by mail.example.com with esmtp (Exim 4.34) id 1CIWES-0005v3-7o for jdoe@example.com; Fri, 15 Oct 2004 18:51:39 +0100
Received: (qmail 23682 invoked from network); 15 Oct 2004 07:08:32 -0000
Date: Wed, 17 Nov 2004 19:20:15 +0200
From: Ben Forbes <ben@example.org>
To: jdoe@example.com
Subject: expensive birds

--END HEADERS--

14.1 E-mails received 09/02/05 contents

From: ben@example.org; To: jdoe@example.com; CC: Subject: good pics 2005-02-09 11:08:01 GMT

Headers Text HTML RTF Attachments (1) Accounts Original Text

Hi thought you'd like these

enjoy

From: ben@example.org; 2005-02-09 11:08:01 GMT
To: jdoe@example.com;
CC:
Subject: some more good ones

Headers Text HTML RTF Attachments (5) Accounts Original Text

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

14.2 E-mails received 09/02/05 headers

From: ben@example.org; 2005-02-09 11:08:01 GMT
To: jdoe@example.com;
CC:
Subject: good pics

Headers Text HTML RTF Attachments (1) Accounts

-----HEADERS-----
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline
---END HEADERS--

From: ben@example.org; 2005-02-09 11:08:01 GMT
To: jdoe@example.com;
CC:
Subject: some more good ones

Headers Text HTML RTF Attachments (5) Accounts

-----HEADERS-----
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline
---END HEADERS--

APPENDIX E - INTERNET HISTORY ANALYSIS

0.3 Extracted data from IE history index.dat showing search and download of Microsoft updates, Firefox and Thunderbird installation files

1	2005-01-24 16:15:25	http://v5.windowsupdate.microsoft.com/v5consumer...	Web History
2	2005-01-24 16:15:26	http://v5.windowsupdate.microsoft.com/v5consumer...	Web History
3	2005-01-24 16:15:27	http://v5.windowsupdate.microsoft.com/v5consumer...	Web History
4	2005-01-24 16:15:29	http://v5.windowsupdate.microsoft.com/v5consumer...	Web History
5	2005-01-24 16:15:29	http://v5.windowsupdate.microsoft.com/v5consumer...	Web History
6	2005-01-24 16:15:34	http://v5.windowsupdate.microsoft.com/v5consumer...	Web History
7	2005-01-24 16:15:40	http://v5.windowsupdate.microsoft.com/SelfUpdate/...	Web History
8	2005-01-24 16:15:41	http://v5.windowsupdate.microsoft.com/SelfUpdate/...	Web History
9	2005-01-24 16:21:43	http://download.mozilla.org/?product=firefox&os=win&lang=en-GB	Web History
10	2005-01-24 16:23:26	http://download.mozilla.org/?product=thunderbird&os=win&lang=en-US	Web History

3.1 Extracted data from Firefox history.dat file (14:11 - 15:12 02/02/05)

=====

URL : http://www.google.co.uk/search?client=firefox-a&rls=org.mozilla%3Aen-GB%3Aofficial_s&hl=en&q=birds&meta=&btnG=Google+Search

First Visit Date : 02/02/2005 14:11:46

=====

URL : http://www.pbs.org/lifeofbirds/

First Visit Date : 02/02/2005 14:11:54

=====

URL : http://www.pbs.org/lifeofbirds/songs/index.html

First Visit Date : 02/02/2005 14:12:05

=====

URL : http://www.amazon.co.uk/exec/obidos/external-search/026-5665785-2744400?tag=roscosolutions&keyword=birds&mode=books-uk

First Visit Date : 02/02/2005 14:14:49

```
=====
URL : http://www.amazon.co.uk/exec/obidos/external-
search?tag=roscosolutions&keyword=birds&mode=books-uk

First Visit Date : 02/02/2005 14:14:49
=====

=====

URL :
http://www.google.co.uk/pagead/iclk?adurl=http://www.amazon.co.uk/exec/obidos/external-
search%3Ftag%3Droscosolutions%26keyword%3Dbirds%26mode%3Dbooks-
uk&sa=l&ai=BW2r0o98AqvKADLuuQbHk9JwHhtWFCMrNsqsBt7bCBaCNBhAEGAQgtlQoBTgAQIoWSLs5oAHVtMD_A6oBHG9yZ
y5tb3ppbGxh0mVuLUDCOM9mZmljaWFsX3PIAQE&num=4

First Visit Date : 02/02/2005 14:14:49
=====

=====

URL :
http://www.googleadservices.com/pagead/adclick?adurl=http://www.amazon.co.uk/exec/obidos/external-
-search%3Ftag%3Droscosolutions%26keyword%3Dbirds%26mode%3Dbooks-
uk&sa=L&ai=BW2r0o98AqvKADLuuQbHk9JwHhtWFCMrNsqsBt7bCBaCNBhAEGAQgtlQoBTgAQIoWSLs5oAHVtMD_A6oBHG9yZ
y5tb3ppbGxh0mVuLUDCOM9mZmljaWFsX3PIAQE&num=4

First Visit Date : 02/02/2005 14:14:49
=====

=====

URL : http://www.amazon.co.uk/exec/obidos/ASIN/0007176147/qid=1107353690/sr=2-
1/ref=sr_2_11_1/026-5665785-2744400

First Visit Date : 02/02/2005 14:14:59
=====

=====

URL : http://www.amazon.co.uk/exec/obidos/ASIN/0713666161/qid=1107353690/sr=2-
3/ref=sr_2_11_3/026-5665785-2744400

First Visit Date : 02/02/2005 14:15:29
=====

=====

URL : http://www.google.co.uk/search?q=bird+wallpaper&sourceid=mozilla-
search&start=0&start=0&ie=utf-8&oe=utf-8&client=firefox-a&rls=org.mozilla:en-GB:official
```

First Visit Date : 02/02/2005 14:15:42

=====

=====

URL :
http://as.casalemedia.com/s?s=53524&u=http%3A//www.naturewallpaper.net/birds_L.html&f=2&id=578026
6264.517584

First Visit Date : 02/02/2005 14:15:51

=====

=====

URL : http://www.naturewallpaper.net/birds_L.html

First Visit Date : 02/02/2005 14:15:51

=====

=====

URL :
http://asg36.casalemedia.com/s?s=53524&u=http%3A//www.naturewallpaper.net/birds_L.html&f=2&id=578
0266264.517584

First Visit Date : 02/02/2005 14:15:56

=====

=====

URL : http://isg10.casalemedia.com/V2/40842/43608

First Visit Date : 02/02/2005 14:15:56

=====

=====

URL : http://isg10.casalemedia.com/V2/40842/43608/

First Visit Date : 02/02/2005 14:15:56

=====

=====

URL : http://pagead2.googlesyndication.com/pagead/ads?client=ca-pub-
0241683974610684&dt=1107353756202&lmt=1107353751&format=468x60_as&output=html&url=http%3A%2F%2Fww
w.naturewallpaper.net%2Fbirds_L.html&ref=http%3A%2F%2Fwww.google.co.uk%2Fsearch%3Fq%3Dbird%2Bwall
paper%26sourceid%3Dmozilla-search%26start%3D0%26start%3D0%26ie%3Dutf-8%26oe%3Dutf-
8%26client%3Dfirefox-a%26rls%3Dorg.mozilla%3Aen-
GB%3Aofficial&u_h=768&u_w=1024&u_ah=738&u_aw=1024&u_cd=24&u_his=5&u_nplug=5&u_nmime=13

First Visit Date : 02/02/2005 14:15:56

=====

=====

URL :
http://media.fastclick.net/w/get.media?t=n&sid=11194&m=1&f=b&v=1.4&c=1495&r=http%3A//www.naturewallpaper.net/birds_L.html&d=f

First Visit Date : 02/02/2005 14:16:21

=====

=====

URL : http://pagead2.googlesyndication.com/pagead/ads?client=ca-pub-0241683974610684&dt=1107353782360&lmt=1107353781&format=468x60_as&output=html&url=http%3A%2F%2Fwww.naturewallpaper.net%2FbirdsLpages%2Fimage4.html&ref=http%3A%2F%2Fwww.naturewallpaper.net%2Fbirds_L.html&u_h=768&u_w=1024&u_ah=738&u_aw=1024&u_cd=24&u_his=6&u_nplug=5&u_nmime=13

First Visit Date : 02/02/2005 14:16:21

=====

=====

URL : <http://www.naturewallpaper.net/birdsLpages/image4.html>

First Visit Date : 02/02/2005 14:16:21

=====

=====

URL :
http://media.fastclick.net/w/get.media?t=n&sid=11194&m=1&f=b&v=1.4&c=7262&r=http%3A//www.naturewallpaper.net/birds_L.html&d=f

First Visit Date : 02/02/2005 14:18:45

=====

=====

URL : http://pagead2.googlesyndication.com/pagead/ads?client=ca-pub-0241683974610684&dt=1107353925746&lmt=1107353925&format=468x60_as&output=html&url=http%3A%2F%2Fwww.naturewallpaper.net%2FbirdsLpages%2Fimage21.html&ref=http%3A%2F%2Fwww.naturewallpaper.net%2Fbirds_L.html&u_h=768&u_w=1024&u_ah=738&u_aw=1024&u_cd=24&u_his=6&u_nplug=5&u_nmime=13

First Visit Date : 02/02/2005 14:18:45

=====

=====

URL : <http://www.naturewallpaper.net/birdsLpages/image21.html>

First Visit Date : 02/02/2005 14:18:45

=====

=====

URL : http://pagead2.googlesyndication.com/pagead/adclick?sa=L&ai=Bv4uhneAAQrfmAqX-QcmCpMoK0MuACPLnwJwBwI23AcC4AhACGAIg05r2ASgCQIoWSIo5sgEXd3d3Lm5hdHVyZXdhbGxwYXBlc15uZXS6AQk0Njh4NjBFYXPIAQHaAStodHRwOi8vd3d3Lm5hdHVyZXdhbGxwYXBlc15uZQvYmlyZHNfTC5odG1s&num=2&adurl=http://uk.shop.com/amos/cc/main/ccn_search_catsa/st/bald%2Beagle/sy/products/ccsyn/518/SourceID/30&client=ca-pub-0241683974610684

First Visit Date : 02/02/2005 14:19:48

=====

=====

URL : http://pagead2.googlesyndication.com/pagead/iclk?sa=l&ai=Bv4uhneAAQrfmAqX-QcmCpMoK0MuACPLnwJwBwI23AcC4AhACGAIg05r2ASgCQIoWSIo5sgEXd3d3Lm5hdHVyZXdhbGxwYXBlc15uZXS6AQk0Njh4NjBFYXPIAQHaAStodHRwOi8vd3d3Lm5hdHVyZXdhbGxwYXBlc15uZQvYmlyZHNfTC5odG1s&num=2&adurl=http://uk.shop.com/amos/cc/main/ccn_search_catsa/st/bald%2Beagle/sy/products/ccsyn/518/SourceID/30&client=ca-pub-0241683974610684

First Visit Date : 02/02/2005 14:19:48

=====

=====

URL : http://uk.shop.com/amos/cc/main/ccn_search_catsa/st/bald+eagle/sy/products/ccsyn/518/SourceID/30

First Visit Date : 02/02/2005 14:19:56

=====

=====

URL : http://amos.shop.com/amos/cc/main/catalog/pcd/7107298/prd/10187717/ccsyn/518/_x_/Choices-Direct--Movies-Bird-Safari---Bird-Watcher's-Paradise-VIDEO\

First Visit Date : 02/02/2005 14:20:19

=====

=====

URL : <http://www.google.co.uk/search?hl=en&client=firefox-a&rls=org.mozilla%3Aen-GB%3Aofficial&q=bird+stories&btnG=Search&meta=>

First Visit Date : 02/02/2005 14:22:25

=====

```
=====
URL : http://birding.about.com/od/storie1/
First Visit Date : 02/02/2005 14:22:38
=====

=====
URL :
http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding;svc=;site=birding;t=14;pc=1;fd=0;fs=0;a=;sbj=pid512;kw=;chan=hobbies;syn=about;tile=1;r=0;dcopt=ist;sz=728x90;ord=1522EMf0020SA1B0c43
First Visit Date : 02/02/2005 14:22:38
=====

=====
URL : http://z.about.com/0/ip/417/5.htm?CDN=hobbies
First Visit Date : 02/02/2005 14:22:38
=====

=====
URL : http://z.about.com/0/ip/496/0.htm
First Visit Date : 02/02/2005 14:22:38
=====

=====
URL : http://z.about.com/0/ip/512/12.htm
First Visit Date : 02/02/2005 14:22:38
=====

=====
URL : http://z.about.com/0/ip/512/6.htm
First Visit Date : 02/02/2005 14:22:38
=====

=====
URL : http://z.about.com/5/ad/go.htm?gs=birding
```

First Visit Date : 02/02/2005 14:22:38

=====

=====

URL :
http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding;svc=;site=birding;t=14;pc=1;fd=0;fs=0;a=;sbj=pid512;kw=;chan=hobbies;syn=about;tile=4;r=0;sz=728x91;ord=1522EMf0020SA1B0c43

First Visit Date : 02/02/2005 14:22:45

=====

=====

URL : http://z.about.com/5/ad/am.htm?pid=about

First Visit Date : 02/02/2005 14:22:45

=====

=====

URL : http://z.about.com/6/o/b.htm?gs=birding

First Visit Date : 02/02/2005 14:22:45

=====

=====

URL : http://birding.about.com/library/weekly/aa102598.htm

First Visit Date : 02/02/2005 14:23:04

=====

=====

URL :
http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding;svc=;site=birding;t=0;pc=2;fd=0;fs=0;a=;sbj=pid512;kw=;chan=hobbies;syn=about;tile=1;r=0;dcopt=ist;sz=728x90;ord=1522EN50L20SA0d1843

First Visit Date : 02/02/2005 14:23:04

=====

=====

URL :
http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding;svc=;site=birding;t=0;pc=2;fd=0;fs=0;a=;sbj=pid512;kw=;chan=hobbies;syn=about;tile=2;r=0;sz=120x600;ord=1522EN50L20SA0d1843

First Visit Date : 02/02/2005 14:23:04

=====

```
=====
URL : http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding;svc=;site=birding;t=0;pc=2;fd=0;fs=0;a=;sbj=pid512;kw=;chan=hobbies;syn=about;tile=4;r=0;sz=728x91;ord=1522EN50L20SA0d1843
First Visit Date : 02/02/2005 14:23:04
=====

=====
URL : http://z.about.com/5/o/c.htm?gs=birding
First Visit Date : 02/02/2005 14:23:04
=====

=====
URL : http://z.about.com/7/o/cw.htm?gs=birding
First Visit Date : 02/02/2005 14:23:04
=====

=====
URL : http://birding.about.com/library/blalphatypeofbird.htm
First Visit Date : 02/02/2005 14:23:56
=====

=====
URL : http://clk.about.com/?zi=18/yV&sdn=hobbies_birding&tm=51&f=00&su=p512.6.140.ip_p512.12.140.ip_&tt=0&zu=http%3A//birding.about.com/library/blalphatypeofbird.htm
First Visit Date : 02/02/2005 14:23:56
=====

=====
URL :
http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding;svc=;site=birding;t=0;pc=3;fd=0;fs=0;a=;sbj=pid512;kw=;chan=hobbies;syn=about;tile=1;r=0;u=0mfh7s21101oie;dcopt=ist;sz=728x90;ord=1522ENr0N20SA0T0C668
First Visit Date : 02/02/2005 14:23:56
=====
```

=====

URL :
http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding;svc=;site=birding;t=0;pc=3;fd=0;fs=0;a=;sbj=pid512;kw=;chan=hobbies;syn=about;tile=2;r=0;u=0mfh7s21101oie;sz=120x600;ord=1522ENr0N20SA0T0C668

First Visit Date : 02/02/2005 14:23:56

=====

=====

URL :
http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding;svc=;site=birding;t=0;pc=3;fd=0;fs=0;a=;sbj=pid512;kw=;chan=hobbies;syn=about;tile=4;r=0;u=0mfh7s21101oie;sz=728x91;ord=1522ENr0N20SA0T0C668

First Visit Date : 02/02/2005 14:23:56

=====

=====

URL : http://birding.about.com/library/blhousespecs.htm

First Visit Date : 02/02/2005 14:24:18

=====

=====

URL :
http://clk.about.com/?zi=18/yV&sdn=hobbies_birding&tm=208f=00&su=p512.6.140.ip_p512.12.140.ip_8tt=0&zu=http%3A//birding.about.com/library/blhousespecs.htm

First Visit Date : 02/02/2005 14:24:18

=====

=====

URL :
http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding;svc=;site=birding;t=0;pc=4;fd=0;fs=0;a=;sbj=pid512;kw=;chan=hobbies;syn=about;tile=1;r=0;u=0mfh7s21101oie;dcopt=ist;sz=728x90;ord=1522EOJ0E20SA2k0X896

First Visit Date : 02/02/2005 14:24:18

=====

=====

URL :
http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding;svc=;site=birding;t=0;pc=4;fd=0;fs=0;a=;sbj=pid512;kw=;chan=hobbies;syn=about;tile=2;r=0;u=0mfh7s21101oie;sz=120x600;ord=1522EOJ0E20SA2k0X896

First Visit Date : 02/02/2005 14:24:18

=====

=====

URL :
http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding;svc=;site=birding;t=0;pc=4;fd=0;fs=0;a=;sbj=pid512;kw=;chan=hobbies;syn=about;tile=4;r=0;u=0mfh7s21101oie;sz=728x91;ord=1522E0J0E20SA2k0X896

First Visit Date : 02/02/2005 14:24:18

=====

=====

URL : http://birding.about.com/cs/buildhouses/index.htm

First Visit Date : 02/02/2005 14:24:32

=====

=====

URL : http://birding.about.com/od/buildhouses/

First Visit Date : 02/02/2005 14:24:32

=====

=====

URL :
http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding;svc=;site=birding;t=14;pc=5;fd=0;fs=0;a=;sbj=pid512;kw=;chan=hobbies;syn=about;tile=1;r=0;u=0mfh7s21101oie;dcopt=ist;sz=468x60;ord=1522E0V0N20SA0G0P124

First Visit Date : 02/02/2005 14:24:32

=====

=====

URL :
http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding;svc=;site=birding;t=14;pc=5;fd=0;fs=0;a=;sbj=pid512;kw=;chan=hobbies;syn=about;tile=3;r=0;u=0mfh7s21101oie;sz=336x280;ord=1522E0V0N20SA0G0P124

First Visit Date : 02/02/2005 14:24:32

=====

=====

URL :
http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding;svc=;site=birding;t=14;pc=5;fd=0;fs=0;a=;sbj=pid512;kw=;chan=hobbies;syn=about;tile=4;r=0;u=0mfh7s21101oie;sz=728x91;ord=1522E0V0N20SA0G0P124

First Visit Date : 02/02/2005 14:24:32

=====

=====

URL : http://birding.about.com/cs/birdhousesfeeders/a/buildingindex.htm

First Visit Date : 02/02/2005 14:24:42

=====

=====

URL :
http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding;svc=;site=birding;t=2;pc=6;fd=0;fs=0;a=;sbj=pid512;kw=;chan=hobbies;syn=about;tile=2;r=0;u=0mfh7s21101oie;sz=120x600;ord=1522E0b0P20SA3M0A64

First Visit Date : 02/02/2005 14:24:42

=====

=====

URL :
http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding;svc=;site=birding;t=2;pc=6;fd=0;fs=0;a=;sbj=pid512;kw=;chan=hobbies;syn=about;tile=3;r=0;u=0mfh7s21101oie;dcopt=ist;sz=336x280;ord=2522E0b0P20SA3M0A64

First Visit Date : 02/02/2005 14:24:42

=====

=====

URL :
http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding;svc=;site=birding;t=2;pc=6;fd=0;fs=0;a=;sbj=pid512;kw=;chan=hobbies;syn=about;tile=4;r=0;u=0mfh7s21101oie;sz=728x91;ord=1522E0b0P20SA3M0A64

First Visit Date : 02/02/2005 14:24:42

=====

=====

URL :
http://view.atdmt.com/VON/iview/btcmxvon0260000015von/direct/01?click=http://n479ad.doubleclick.net/click%3Bh=v4|3213|3|0|%2a|q%3B12023409%3B0-0%3B0%3B7596722%3B4252-336|280%3B8795737|8813633|1%3Bu%3D0mfh7s21101oie%3B%7Eaopt%3D0|ff373b%3B%7Esscs%3D%3f

First Visit Date : 02/02/2005 14:24:42

=====

=====

URL : http://birding.about.com/library/weekly/aa010703a.htm

First Visit Date : 02/02/2005 14:24:55

=====

=====

URL :
http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding;svc=;site=birding;t=0;pc=7;fd=0;fs=0;a=;sbj=pid512;kw=;chan=hobbies;syn=about;tile=1;r=0;u=0mfh7s21101oie;dcopt=ist;sz=728x90;ord=1522E0v0I20SA2e0F480

First Visit Date : 02/02/2005 14:24:55

=====

=====

URL :
http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding;svc=;site=birding;t=0;pc=7;fd=0;fs=0;a=;sbj=pid512;kw=;chan=hobbies;syn=about;tile=2;r=0;u=0mfh7s21101oie;sz=160x600;ord=1522E0v0I20SA2e0F480

First Visit Date : 02/02/2005 14:24:55

=====

=====

URL :
http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding;svc=;site=birding;t=0;pc=7;fd=0;fs=0;a=;sbj=pid512;kw=;chan=hobbies;syn=about;tile=4;r=0;u=0mfh7s21101oie;sz=728x91;ord=1522E0v0I20SA2e0F480

First Visit Date : 02/02/2005 14:24:55

=====

=====

URL : http://birding.about.com/library/blhousefeederpaint.htm

First Visit Date : 02/02/2005 14:26:43

=====

=====

URL :
http://clk.about.com/?zi=18/yW&sdn=hobbies_birding&tm=107&f=00&su=p512.6.140.ip_p512.12.140.ip_&t=0&zu=http%3A//birding.about.com/library/blhousefeederpaint.htm

First Visit Date : 02/02/2005 14:26:43

=====

=====

URL :
http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding;svc=;site=birding;t=0;pc=8;fd=0;fs=0;a=;sbj=pid512;kw=;chan=hobbies;syn=about;tile=1;r=0;u=0mfh7s21101oie;dcopt=ist;sz=728x90;ord=1522EQi0B20SA1x0N820

First Visit Date : 02/02/2005 14:26:43

=====

=====

URL :
http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding;svc=;site=birding;t=0;pc=8;fd=0;fs=0;a=;sbj=pid512;kw=;chan=hobbies;syn=about;tile=2;r=0;u=0mfh7s21101oie;sz=160x600;ord=1522EQi0B20SA1x0N820

First Visit Date : 02/02/2005 14:26:43

=====

=====

URL :
http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding;svc=;site=birding;t=0;pc=8;fd=0;fs=0;a=;sbj=pid512;kw=;chan=hobbies;syn=about;tile=4;r=0;u=0mfh7s21101oie;sz=728x91;ord=1522EQi0B20SA1x0N820

First Visit Date : 02/02/2005 14:26:43

=====

=====

URL : http://pagead2.googlesyndication.com/pagead/adclick?sa=L&ai=BiW5-JeMAQviVFI7YQa3yjJsK_PzSBq7nwZQBwI23AaCzIxABGAEgvKX3ASgIQIoWSJQ5mAGcSqdBEHByaW1lZGlhX2JpcmRpmbeyARFiaXJkaW5nLmFib3V0LmNvbcbgBADoBN2h0dHA6Ly9iaXJkaW5nLmFib3V0LmNvbS9saWJyYXJ5L2JsaG91c2VmZWVkJwYWludC5odG0&num=1&adurl=http://www.haiths.com&client=ca-primedia-basic_js

First Visit Date : 02/02/2005 14:27:01

=====

=====

URL : http://pagead2.googlesyndication.com/pagead/iclk?sa=l&ai=BiW5-JeMAQviVFI7YQa3yjJsK_PzSBq7nwZQBwI23AaCzIxABGAEgvKX3ASgIQIoWSJQ5mAGcSqdBEHByaW1lZGlhX2JpcmRpmbeyA

RFiaXJkaW5nLmFib3V0LmNvbcbAdoBN2h0dHA6Ly9iaXJkaW5nLmFib3V0LmNvbS9saWJyYXJ5L2JsaG91c2VmZWVkJwYW
ludC5odG0&num=1&adurl=http://www.haiths.com&client=ca-primedia-basic_js

First Visit Date : 02/02/2005 14:27:01

=====

=====

URL : http://www.haiths.com/

First Visit Date : 02/02/2005 14:27:07

=====

=====

URL :
http://www.haiths.com/Features.asp?lookup=0&brand=1&article_id=features_1&customer_id=PAA02190223
05524FFFKSRSZKKXZGRWU

First Visit Date : 02/02/2005 14:28:31

=====

=====

URL : http://www.imdb.com/title/tt0056869/

First Visit Date : 02/02/2005 14:40:24

=====

=====

URL : http://www.imdb.com/google/box?num=3;k=power100-
withsc;placement=midbucket;rnd=45504;sid=7845;referer=%2Ftitle%2Ftt0056869%2F;slot=GOOGLE

First Visit Date : 02/02/2005 14:40:30

=====

=====

URL : http://rcm.amazon.com/e/cm?f=ifr&t=imdb-rec-banner-
20&l=st1&search=widescreen&mode=dvd&p=13&o=1

First Visit Date : 02/02/2005 14:40:46

=====

=====

URL : http://www.imdb.com/google/box?num=3;k=power100-
withsc;placement=midbucket;rnd=83932;sid=8055;referer=%2Ftitle%2Ftt0056869%2Ftrailers;slot=BOTTOM
_CENTER

First Visit Date : 02/02/2005 14:40:46

=====

=====

URL : http://www.imdb.com/rg/title-tease/trailers/title/tt0056869/trailers

First Visit Date : 02/02/2005 14:40:46

=====

=====

URL : http://www.imdb.com/title/tt0056869/trailers

First Visit Date : 02/02/2005 14:40:46

=====

=====

URL : http://www.imdb.com/google/box?num=5;k=maxww-sky;placement=2;rnd=872225854982059300;sid=-123;referer=maxww;slot=TOP_RHS

First Visit Date : 02/02/2005 14:40:49

=====

=====

URL : http://videodetective.com/home.asp?PublishedID=1843

First Visit Date : 02/02/2005 14:41:00

=====

=====

URL : http://www.imdb.com/rg/TITLETRA_VIDDET//http://videodetective.com/home.asp?PublishedID=1843

First Visit Date : 02/02/2005 14:41:00

=====

=====

URL : http://videodetective.com/player.asp?PublishedId=1843&List=307629|838353&Customerid=97135

First Visit Date : 02/02/2005 14:41:56

=====

```
=====
URL      :
http://videodetective.com/test.asp?List=307629|838353&PublishedID=1843&ListID=&New=&CustomerId=97135
First Visit Date : 02/02/2005 14:41:56
=====

=====
URL      :
http://videodetective.com/test.asp?List=307629|838353&PublishedID=1843&ListID=&New=&CustomerId=97135&refreshed=TRUE
First Visit Date : 02/02/2005 14:41:56
=====

=====
URL      :
http://videodetective.com/choosespeed.asp?BrowserSupportActiveX=false&ActiveXPlayerInstalled=false&plugin=true&List=307629|838353&PublishedID=1843&ListID=&New=&CustomerId=97135&refreshed=TRUE
First Visit Date : 02/02/2005 14:42:00
=====

=====
URL      :
http://videodetective.com/play.asp?New=True&List=307629|838353&PublishedId=1843&VideoKbrate=300&ListID=&CustomerId=97135&HasPlayer=
First Visit Date : 02/02/2005 14:42:09
=====

=====
URL      :
http://videodetective.com/player.asp?PublishedId=1843&List=307629|838353&CustomerID=97135&videokbrate=300
First Visit Date : 02/02/2005 14:42:09
=====

=====
URL      : http://videodetective.com/Playlist.asp?
First Visit Date : 02/02/2005 14:42:09
=====
```

```
=====
URL : http://videodetective.com/titleinfo.asp
First Visit Date : 02/02/2005 14:42:09
=====

=====
URL : http://news.bbc.co.uk/
First Visit Date : 02/02/2005 14:44:01
=====

=====
URL : http://news.bbc.co.uk/nol/ukfs_news/hi/front_page/ticker.stm
First Visit Date : 02/02/2005 14:44:01
=====

=====
URL : http://news.bbc.co.uk/1/hi/uk_politics/4227829.stm
First Visit Date : 02/02/2005 14:44:12
=====

=====
URL : http://news.bbc.co.uk/1/hi/uk_politics/4227829.stm#
First Visit Date : 02/02/2005 14:45:28
=====

=====
URL :
http://www.bbc.co.uk/mediaselector/check/nolavconsole/ukfs_news/hi?redirect=fs.stm&news=1&bbram=1
&bbwm=1&nbram=1&nbwm=1&nol_storyid=4229711
First Visit Date : 02/02/2005 14:45:28
=====

=====
URL :
http://news.bbc.co.uk/nolavconsole/shared/player/player.stm?clipurl=http://news.bbc.co.uk/media/news_web/video/40545000/bb/40545855_bb_16x9.ram&bw=bb
```

First Visit Date : 02/02/2005 14:45:37

=====

=====

URL :
http://news.bbc.co.uk/nolavconsole/shared/player/player.stm?title=Blair%20defends%20house%20arrest%20plans&clipurl=http://news.bbc.co.uk/media/news_web/video/40786000/bb/40786999_bb_16x9.ram&cs=news

First Visit Date : 02/02/2005 14:45:37

=====

=====

URL :
http://news.bbc.co.uk/nolavconsole/ukfs_news/hi/bb_rm_fs.stm?checkedBandwidth=bb&nbram=1&checkedMedia=ram&news=1&nbwm=1&bbwm=1&bram=1&nol_storyid=4229711

First Visit Date : 02/02/2005 14:45:37

=====

=====

URL : http://news.bbc.co.uk/nolavconsole/ukfs_news/hi/front_page/bb_rm_banner.stm

First Visit Date : 02/02/2005 14:45:37

=====

=====

URL : http://news.bbc.co.uk/nolavconsole/ukfs_news/hi/front_page/bb_rm_promo.stm

First Visit Date : 02/02/2005 14:45:37

=====

=====

URL : http://news.bbc.co.uk/nolavconsole/ukfs_news/hi/newsid_4220000/newsid_4229700/bb_rm_4229711.stm

First Visit Date : 02/02/2005 14:45:37

=====

=====

URL : http://news.bbc.co.uk/nolavconsole/ukfs_news/hi/uk/bb_rm_banner.stm

First Visit Date : 02/02/2005 14:45:37

=====

```
=====
URL : http://news.bbc.co.uk/nolavconsole/ukfs_news/hi/uk/bb_rm_promo.stm
First Visit Date : 02/02/2005 14:45:37
=====

=====
URL : http://www.bbc.co.uk/cgi-perl/mediaselector/app.pl?action=sc&alreadySeen=1&m=%2Fnolavconsole%2Fukfs_news%2Fhi&q=nbram%3D1%26redirect%3Dfs.stm%26news%3D1%26nbwm%3D1%26bbwm%3D1%26bbram%3D1%26nol_storyid%3D4229711&quality=HiQuality&player=RealPlayer&frm_Submit=OK
First Visit Date : 02/02/2005 14:45:37
=====

=====
URL :
http://www.bbc.co.uk/mediaselector/check/nolavconsole/ukfs_news/hi?redirect=fs.stm&nbram=1&news=1&bbwm=1&nbwm=1&bbram=1&nol_storyid=4229711&checkedBandwidth=bb&checkedMedia=ram&alreadySeen=1
First Visit Date : 02/02/2005 14:45:37
=====

=====
URL : http://news.bbc.co.uk/1/hi/scotland/default.stm
First Visit Date : 02/02/2005 15:11:19
=====

=====
URL : http://www.pbs.org/lifeofbirds/songs/kakapo.ram
First Visit Date : 02/02/2005 15:11:41
=====

=====
URL : http://www.pbs.org/lifeofbirds/songs/dawn.ram
First Visit Date : 02/02/2005 15:12:06
=====
```


3.16 bookmarks.html file



The screenshot shows a browser window displaying the source code of a bookmarks.html file. The code is an XML document with various entries for bookmarks. A specific entry is highlighted with a red box:

```
<DT><A href="http://www.naturewallpaper.net/birds_1.html" add_date="1107354119" id="rdf:$1Cb0g3">Free Bird Wallpaper - Bald Eagle Albatross Owl Falcon 1024x768</A>
```

3.17 Conversion of epoch time to human-readable time

Convert epoch to human-readable date and vice versa

1107354119 [batch convert]

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

Assuming that this timestamp is in **seconds**:

GMT : Wednesday, February 2, 2005 2:21:59 PM

Your time zone : Wednesday, February 2, 2005 2:21:59 PM **GMT+00:00**

Relative : 20 years ago

Convert epoch to human-readable date and vice versa

1107354246 [batch convert]

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

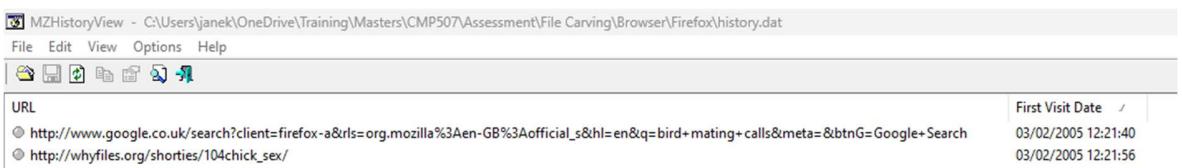
Assuming that this timestamp is in **seconds**:

GMT : Wednesday, February 2, 2005 2:24:06 PM

Your time zone : Wednesday, February 2, 2005 2:24:06 PM **GMT+00:00**

Relative : 20 years ago

7.1 Firefox history.dat file (12:21 03/02/05)



The screenshot shows the MZHistoryView application interface. It displays a list of URLs visited by the user. Two entries are highlighted with red boxes:

URL	First Visit Date
http://www.google.co.uk/search?client=firefox-a&rls=org.mozilla%3Aen-GB%3Aofficial_s&hl=en&q=bird+mating+calls&meta=&btnG=Google+Search	03/02/2005 12:21:40
http://whyfiles.org/shorties/104chick_sex/	03/02/2005 12:21:56

7.2 Aggressive_song.wav download from downloads.rdf

```
<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 12:30:00 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>
```

7.3 Extracted summary data from internet explorer index.dat (12:22 03/02/05)

URL	Access timestamp
Visited: john Doe@file:///E:/birds/audio/aggressive_song.wav	03/02/2005 12:22

8.1 bookmarks.html file



```
<!DOCTYPE NETSCAPE-Bookmark-file-1>
<!-- This is an automatically generated file.
     It will be read and overwritten.
     DO NOT EDIT! -->
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=UTF-8">
<TITLE>Bookmarks</TITLE>
<H1>LAST_MODIFIED="1107439776">Bookmarks</H1>
<DL><p>
<DT><H3>PERSONAL_TOOLBAR_FOLDER="true" ID="rdf:#$vPhC3">Bookmarks Toolbar Folder</H3>
<DD>Add bookmarks to this folder to see them displayed on the Bookmarks Toolbar
<DL><p>
<DT><A HREF="http://www.mozilla.org/products/firefox/index.html" ICON="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAABAAAAQCAVAAAf8/9hAAAABgdBTUEAK/INwvK6QAAAb10RVh0U29ndhcmUAQhRvYm>">Dictionary.com Quicksearch</A>
<DT><A HREF="http://fxfeeds.mozillaazine.org/" LAST_MODIFIED="1107966483" FEEDURL="http://fxfeeds.mozillaazine.org/rss20.xml" ID="rdf:#$vPhC3">Latest Headlines</A>
</DL><p>
<H3>Quick Searches</H3>
<DD>Handy searches that can be performed in the addressbar
<DL><p>
<DT><A HREF="http://www.google.co.uk/search?q=%s" SHORTCUTURL="google" ICON="data:image/x-icon;base64,AABAAEAEBAAAAAAABoBQAAfGAACgAAAQAAAAIAAAAECAAAAAAAAAAAAAAAQAAAAAAA" >Google Search</A>
<DT><A HREF="http://dictionary.reference.com/search?q=%s" SHORTCUTURL="dict" ID="rdf:#$vPhC3">Dictionary.com Quicksearch</A>
<DT><A HREF="http://www.google.co.uk/search?q=%s" SHORTCUTURL="q" ICON="data:image/x-icon;base64,AABAAEAEBAAAAAAABoBQAAfGAACgAAAQAAAAIAAAAECAAAAAAAAAAAAAAAQAAAAAAA" >Google Search</A>
<DT><A HREF="http://www.google.co.uk/search?q=%s" SHORTCUTURL="q" ICON="data:image/x-icon;base64,AABAAEAEBAAAAAAABoBQAAfGAACgAAAQAAAAIAAAAECAAAAAAAAAAAAAAAQAAAAAAA" >Google Search</A>
<DT><A HREF="http://en.wikipedia.org/wiki/Special:Search?search=%s" SHORTCUTURL="wp" ID="rdf:#$vPhC3">Wikipedia Quicksearch</A>
<DT><A HREF="http://www.urbandictionary.com/define.php?term=%s" SHORTCUTURL="slang" ID="rdf:#$vPhC3">Urban Dictionary</A>
<DT><A HREF="http://www.urbandictionary.com/define.php?term=%s" SHORTCUTURL="slang" ID="rdf:#$vPhC3">Urban Dictionary</A>
<DT><A HREF="http://www.mozilla.org/irc" SHORTCUTURL="irc" ID="rdf:#$vPhC3">Mozilla Links</A>
<DT><A HREF="http://start.mozilla.org/firefox/" ICON="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAABAAAQCAVAAAf8/9hAAAABgdBTUEAK/INwvK6QAAAb10RVh0U29ndhcmUAQhRvYm>">Firefox and Mozilla Links</A>
<DT><A HREF="http://start.mozilla.org/firefox-central.html" ICON="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAABAAAQCAVAAAf8/9hAAAABgdBTUEAK/INwvK6QAAAb10RVh0U29ndhcmUAQhRvYm>">Firefox Central</A>
<DT><A HREF="http://update.mozilla.org/?application=firefox" ICON="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAABAAAQCAVAAAf8/9hAAAABgdBTUEAK/INwvK6QAAAb10RVh0U29ndhcmUAQhRvYm>">Mozilla Application Update</A>
<DT><A HREF="http://getfirefox.com/" ICON="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAABAAAQCAVAAAf8/9hAAAABgdBTUEAK/INwvK6QAAAb10RVh0U29ndhcmUAQhRvYm>">Get Firefox</A>
<DT><A HREF="http://www.mozilla.org/" ICON="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAABAAAQCAVAAAf8/9hAAAABgdBTUEAK/INwvK6QAAAb10RVh0U29ndhcmUAQhRvYm>">Mozilla.org</A>
<DT><A HREF="http://www.mozillaireland.org/" ICON="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAABAAAQCAVAAAf8/9hAAAABgdBTUEAK/INwvK6QAAAb10RVh0U29ndhcmUAQhRvYm>">Mozilla Ireland</A>
<DT><A HREF="http://www.mozillastore.com/" ICON="data:image/x-icon;base64,AABAAEAEBAAAAAT1ABCBAAA" ID="rdf:#$vPhC3">Get Involved - Help spread Firefox</A>
<DT><A HREF="http://www.naturewallpaper.net/birds_L.html" ADD_DATE="1107354119" ID="rdf:#$1ChOp3">Free Bird Wallpapers - Bald Eagle Albatross Owl Falcon 1024x768</A>
<DT><A HREF="http://birdsintheheadlands.com/birds/birds.htm" ADD_DATE="1107354266" ID="rdf:#$vPhC3">Birds Index</A>
<DT><A HREF="http://whyfiles.org/shorties/104chick_sex/" ADD_DATE="1107439776" LAST_CHARSET="ISO-8859-1" ID="rdf:#$vPhC1">Chickadee Karaoke</A>
</DL>
```

8.2 Conversion of epoch time to human-readable time

Convert epoch to human-readable date and vice versa

1107439776 [Timestamp to Human date](#) [batch convert]

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

Assuming that this timestamp is in **seconds**:

GMT : Thursday, February 3, 2005 2:09:36 PM

Your time zone : Thursday, February 3, 2005 2:09:36 PM **GMT+00:00**

Relative : 20 years ago

9.11 Extracted summary data from internet explorer index.dat (14:14 03/02/05)

URL	Access timestamp
Visited: john Doe@file:///C:/EvanstonWoodpecker.jpg	03/02/2005 14:14

9.8 Extracted summary data from IE index.dat (14:14 03/02/05)

URL	Access timestamp
Visited: johndoe@file:///C:/Documents%20and%20Settings/All%20Users/Documents/My%20Music/Sample%20Music/Doc1.doc	03/02/2005 14:17

11.1 Extracted summary data from IE index.dat (14:49 03/02/05)

URL	Access timestamp
Visited: johndoe@file:///E:/birds/Killdeer.jpg	03/02/2005 14:49

12.1 extracted data from Firefox history.dat file (14:59-15:106 03/02/05)

```
=====
URL : http://www.google.co.uk/imghp?hl=en&tab=wi&client=firefox-
a&rls=org.mozilla:en-GB:official_s&q=
First Visit Date : 03/02/2005 14:59:29
=====

=====
URL : http://images.google.co.uk/images?client=firefox-a&rls=org.mozilla%3Aen-
GB%3Aofficial_s&q=young+chicks&hl=en&btnG=Google+Search
First Visit Date : 03/02/2005 14:59:40
=====

=====
URL :
http://images.google.co.uk/imgres?imgurl=http://freespace.virgin.net/cobber.budgies/images/babysc
ot_vyoung.jpg&imgrefurl=http://freespace.virgin.net/cobber.budgies/stories/scottie_a.html&h=353&w
=350&sz=38&tbnid=4jg3dcJYAeIJ:&tbnh=116&tbnw=115&start=5&prev=/images%3Fq%3Dyoung%2Bchicks%26hl%3
Den%26lr%3D%26client%3Dfirefox-a%26rls%3Dorg.mozilla:en-GB:official_s%26sa%3DG
First Visit Date : 03/02/2005 14:59:56
=====

=====
URL :
http://images.google.co.uk/imgres?imgurl=http://freespace.virgin.net/cobber.budgies/images/babysc
ot_vyoung.jpg&imgrefurl=http://freespace.virgin.net/cobber.budgies/stories/scottie_a.html&h=353&w
=350&sz=38&tbnid=4jg3dcJYAeIJ:&tbnh=116&tbnw=115&prev=/images%3Fq%3Dyoung%2Bchicks%26hl%3Den%26lr
%3D%26client%3Dfirefox-a%26rls%3Dorg.mozilla:en-GB:official_s%26sa%3DG&frame=small
First Visit Date : 03/02/2005 14:59:56
=====
```

URL : http://freespace.virgin.net/cobber.budgies/stories/scottie_a.html

First Visit Date : 03/02/2005 14:59:56

=====

=====

URL :
http://images.google.co.uk/imgres?imgurl=http://www.insaneanimals.com/items/177.jpg&imgrefurl=htt
p://www.insaneanimals.com/funny-
animals/177.html%3Fsort%3Ddate&h=290&w=350&sz=10&tbnid=97SA3_pw84UJ:&tbnh=96&tbnw=116&start=6&pre
v=/images%3Fq%3Dyoung%2Bchicks%26hl%3Den%26lr%3D%26client%3Dfirefox-a%26rls%3Dorg.mozilla:en-
GB:official_s%26sa%3DG

First Visit Date : 03/02/2005 15:01:02

=====

=====

URL :
http://images.google.co.uk/imgres?imgurl=http://www.insaneanimals.com/items/177.jpg&imgrefurl=htt
p://www.insaneanimals.com/funny-
animals/177.html%3Fsort%3Ddate&h=290&w=350&sz=10&tbnid=97SA3_pw84UJ:&tbnh=96&tbnw=116&prev=/image
s%3Fq%3Dyoung%2Bchicks%26hl%3Den%26lr%3D%26client%3Dfirefox-a%26rls%3Dorg.mozilla:en-
GB:official_s%26sa%3DG&frame=small

First Visit Date : 03/02/2005 15:01:02

=====

=====

URL : http://www.insaneanimals.com/funny-animals/177.html?sort=date

First Visit Date : 03/02/2005 15:01:08

=====

=====

URL :
http://media.fastclick.net/w/get.media?t=n&sid=13470&m=3&f=b&v=1.4&c=7098&r=http%3A//images.googl
e.co.uk/imgres%3Fimgurl%3Dhttp%3A//www.insaneanimals.com/items/177.jpg%26imgrefurl%3Dhttp%3A//www
.insaneanimals.com/funny-
animals/177.html%253Fsort%253Ddate%26h%3D290%26w%3D350%26sz%3D10%26tbnid%3D97SA3_pw84UJ%3A%26tbnh
%3D96%26tbnw%3D116%26start%3D6%26prev%3D/images%253Fq%253Dyoung%252Bchicks%2526hl%253Den%2526lr%2
53D%2526client%253Dfirefox-a%2526rls%253Dorg.mozilla%3Aen-GB%3Aofficial_s%2526sa%253DG&d=f

First Visit Date : 03/02/2005 15:01:17

=====

=====

URL : http://pagead2.googlesyndication.com/pagead/ads?client=ca-pub-2066660325911329&dt=1107442877733&format=120x600_as&output=html&url=http%3A%2F%2Fimages.google.co.uk%2Fimgres%3Fimgurl%3Dhttp%3A%2F%2Fwww.insaneanimals.com%2Fitems%2F177.jpg%26imgrefurl%3Dhttp%3A%2F%2Fwww.insaneanimals.com%2Ffunny-animals%2F177.html%253Fsort%253Ddate%26h%3D290%26w%3D350%26sz%3D10%26tbnid%3D97SA3_pw84UJ%3A%26tbnh%3D96%26tbnw%3D116%26start%3D6%26prev%3D%2Fimages%253Fq%253Dyoung%252Bchicks%2526hl%253Den%2526lr%253D%2526client%253Dfirefox-a%2526rls%253Dorg.mozilla%3Aen-GB%3Aofficial_s%2526sa%253DG&u_h=768&u_w=1024&u_ah=738&u_aw=1024&u_cd=24&u_hi=4&u_nplug=9&u_nmime=21

First Visit Date : 03/02/2005 15:01:17

=====

=====

URL : http://images.google.co.uk/images?q=young+chicks&hl=en&lr=&client=firefox-a&rls=org.mozilla:en-GB:official_s&start=20&sa=N

First Visit Date : 03/02/2005 15:01:53

=====

=====

URL : http://images.google.co.uk/imgres?imgurl=http://www.cvm.okstate.edu/instruction/kocan/disk2/images/img0056.jpg&imgrefurl=http://www.cvm.okstate.edu/instruction/kocan/ostrich/ostbk2b2.htm&h=768&w=512&sz=108&tbnid=x9EaVDii1EJ:&tbnh=141&tbnw=94&start=24&prev=/images%3Fq%3Dyoung%2Bchicks%26start%3D20%26hl%3Den%26lr%3D%26client%3Dfirefox-a%26rls%3Dorg.mozilla:en-GB:official_s%26sa%3DN

First Visit Date : 03/02/2005 15:02:14

=====

=====

URL : http://images.google.co.uk/imgres?imgurl=http://www.cvm.okstate.edu/instruction/kocan/disk2/images/img0056.jpg&imgrefurl=http://www.cvm.okstate.edu/instruction/kocan/ostrich/ostbk2b2.htm&h=768&w=512&sz=108&tbnid=x9EaVDii1EJ:&tbnh=141&tbnw=94&prev=/images%3Fq%3Dyoung%2Bchicks%26start%3D20%26hl%3Den%26lr%3D%26client%3Dfirefox-a%26rls%3Dorg.mozilla:en-GB:official_s%26sa%3DN&frame=small

First Visit Date : 03/02/2005 15:02:14

=====

=====

URL : http://www.cvm.okstate.edu/instruction/kocan/ostrich/ostbk2b2.htm

First Visit Date : 03/02/2005 15:02:14

=====

URL : http://images.google.co.uk/images?q=young+chicks&hl=en&lr=&client=firefox-a&rls=org.mozilla:en-GB:official_s&start=40&sa=N

First Visit Date : 03/02/2005 15:03:32

=====

=====

URL :
http://images.google.co.uk/imgres?imgurl=http://people.cornell.edu/pages/sah67/chicks2.jpg&imgrefurl=http://people.cornell.edu/pages/sah67/summer.html&h=450&w=600&sz=39&tbnid=7SW04nGCbYJ:&tbnh=99&tbnw=132&start=59&prev=/images%3Fq%3Dyoung%2Bchicks%26start%3D40%26hl%3Den%26lr%3D%26client%3Dfirefox-a%26rls%3Dorg.mozilla:en-GB:official_s%26sa%3DN

First Visit Date : 03/02/2005 15:03:54

=====

=====

URL :
http://images.google.co.uk/imgres?imgurl=http://people.cornell.edu/pages/sah67/chicks2.jpg&imgrefurl=http://people.cornell.edu/pages/sah67/summer.html&h=450&w=600&sz=39&tbnid=7SW04nGCbYJ:&tbnh=99&tbnw=132&prev=/images%3Fq%3Dyoung%2Bchicks%26start%3D40%26hl%3Den%26lr%3D%26client%3Dfirefox-a%26rls%3Dorg.mozilla:en-GB:official_s%26sa%3DN&frame=small

First Visit Date : 03/02/2005 15:03:54

=====

=====

URL : http://people.cornell.edu/pages/sah67/summer.html

First Visit Date : 03/02/2005 15:03:54

=====

12.2 Extracted summary data from Firefox history file (14:59 -15:06 03/02/05)

URL	Title	First Visit Date	Last Visit Date
http://images.google.co.uk/images?client=firefox-a&rls=org.mozilla%3Aen-GB%3Aofficial_s&q=young+chicks&hl=	Google Search: young chicks	03/02/2005 14:59	03/02/2005 14:59
http://freespace.virgin.net/cobber.budgies/stories/scottie_a.html	Scottie's Baby Pictures - 1	03/02/2005 14:59	03/02/2005 14:59
http://images.google.co.uk/imgres?imgurl=http://freespace.virgin.net/cobber.budgies/images/babyscot_yyoung.jpg&imgrefurl=http://freespace.virgin.net/cobber.budgies/stories/scottie_a.html		03/02/2005 14:59	03/02/2005 14:59
http://images.google.co.uk/imgres?imgurl=http://freespace.virgin.net/cobber.budgies/images/babyscot_yyoung.jpg	Google Image Result for http://freespace.virgin.net/cobber.budgies/in	03/02/2005 14:59	03/02/2005 14:59
http://images.google.co.uk/imgres?imgurl=http://www.insaneanimals.com/items/177.jpg&imgrefurl=http://www.insaneanimals.com/funny-animals/177.htm?sort%3Ddate&h=290&rls=org.mozilla:en-GB:official_s%26sa%3DN		03/02/2005 15:01	03/02/2005 15:01
http://images.google.co.uk/imgres?imgurl=http://www.insaneanimals.com/items/177.jpg&imgrefurl=http://www.Google Image Result for http://www.insaneanimals.com/items/177.htm?sort%3Ddate&h=290&rls=org.mozilla:en-GB:official_s%26sa%3DN		03/02/2005 15:01	03/02/2005 15:01
http://www.insaneanimals.com/funny-animals/177.htm?sort=date&h=290&rls=org.mozilla:en-GB:official_s%26sa%3DN	Young Chicks - Funny Animals, Pets, Cats and Dogs Pictures - Insane Animals	03/02/2005 15:01	03/02/2005 15:01
http://media.fastclick.net/w/get.media?i=&sid=13470&m=3&fb=w&l=1.4&c=7098&r=http%3A//images.google.co.uk/imgres?imgurl%3Dhttp%3A//www.insaneanimals.com/items/177.jpg&imgrefurl%3Dhttp%3A//www.insaneanimals.com/items/177.jpg&imgrefurl=http://www.Google Image Result for http://www.insaneanimals.com/items/177.htm?sort%3Ddate&h=290&rls=org.mozilla:en-GB:official_s%26sa%3DN		03/02/2005 15:01	03/02/2005 15:01
http://images.google.co.uk/images?q=young+chicks&hl=en&lr=&client=firefox-a&rls=org.mozilla:en-GB:official_s&start=20&sa=N		03/02/2005 15:01	03/02/2005 15:01
http://images.google.co.uk/imgres?imgurl=http://www.cvm.okstate.edu/instruction/kocan/disk2/images/img0056.jpg&imgrefurl=http://www.cvm.okstate.edu/instruction/kocan/ostrik		03/02/2005 15:02	03/02/2005 15:02
http://images.google.co.uk/imgres?imgurl=http://www.cvm.okstate.edu/instruction/kocan/disk2/images/img005 Google Image Result for http://www.cvm.okstate.edu/instruction/kocan/ostrik		03/02/2005 15:02	03/02/2005 15:02
http://www.cvm.okstate.edu/instruction/kocan/ostrik/ostrik2b.htm		03/02/2005 15:02	03/02/2005 15:02
http://images.google.co.uk/images?q=young+chicks&hl=en&lr=&client=firefox-a&rls=org.mozilla:en-GB:official_s&start=40&sa=N		03/02/2005 15:03	03/02/2005 15:03
http://images.google.co.uk/imgres?imgurl=http://people.cornell.edu/pages/sah67/chicks2.jpg&imgrefurl=http://people.cornell.edu/pages/sah67/summer.html&h=450&w=600&sz=39&rls=org.mozilla:en-GB:official_s%26sa%3DN		03/02/2005 15:03	03/02/2005 15:03
http://images.google.co.uk/imgres?imgurl=http://people.cornell.edu/pages/sah67/chicks2.jpg&imgrefurl=http://people.cornell.edu/pages/sah67/summer.html&h=450&w=600&sz=39&rls=org.mozilla:en-GB:official_s%26sa%3DN		03/02/2005 15:03	03/02/2005 15:03
http://people.cornell.edu/pages/sah67/summer.html	Eco Gallery '04	03/02/2005 15:03	03/02/2005 15:03

12.11 Extracted data from Firefox downloads.rdf file (14:59-15:106 03/02/05)

```
--<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\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="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>

--<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\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: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: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/ostrik/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>
```

12.12 Extracted summary data from IE index.dat (14:59 - 15:06 03/02/05)

URL	Access timestamp
Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/babyscot_vyoung.jpg	03/02/2005 15:00
Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/babyscot_2weeks1.jpg	03/02/2005 15:00
Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/177.jpg	03/02/2005 15:01
Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/ostbk2b2.htm	03/02/2005 15:02
Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/Desktop/birdtrans2.jpg	03/02/2005 15:04
Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/chicks2.jpg	03/02/2005 15:05
Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/newbies2.jpg	03/02/2005 15:05
Visited: johndoe@file:///C:/Documents%20and%20Settings/bob/My%20Documents/My%20Music/ready2fledge.jpg	03/02/2005 15:06

13.8 Extracted summary data from IE index.dat (15:42 - 15:55 03/02/05)

URL	Access timestamp
Visited: johndoe@file:///C:/birdwatching.doc	03/02/2005 15:49
Visited: johndoe@file:///E:/birds/non%20images/BookList.doc	03/02/2005 15:51
Visited: johndoe@file:///E:/birds/non%20images/BirdingGuide.pdf	03/02/2005 15:52

15.1 Extracted data from Firefox history.dat file (11:27 - 11:28 09/02/05)

=====

URL : http://www.google.co.uk/search?client=firefox-a&rls=org.mozilla%3Aen-GB%3Aofficial_s&hl=en&q=bird+screensavers&meta=&btnG=Google+Search

First Visit Date : 09/02/2005 11:27:00

=====

=====

URL : http://www.traveltex.com/screen.asp?SN=6245300&LS=0&SS=1

First Visit Date : 09/02/2005 11:27:12

=====

=====

URL : http://www.traveltex.com/downloads/screensavers/birds.zip

First Visit Date : 09/02/2005 11:27:48

=====

15.2 Extracted summary data from Firefox history file (11:27 - 11:28 09/02/05)

URL	Title	First Visit Date
http://www.google.co.uk/search?client=firefox-a&rls=org.mozilla%3Aen-GB%3Aofficial_s&hl=en&q=bird+screensavers&meta=&btnG=Google+Search	Google Search: bird screensavers	09/02/2005 11:27
http://www.traveltex.com/screen.asp?SN=6245300&LS=0&SS=1	Screensavers	09/02/2005 11:27
http://www.traveltex.com/downloads/screensavers/birds.zip		09/02/2005 11:27

15.3 Extracted data from Firefox cache directory (11:27 - 11:28 09/02/05)

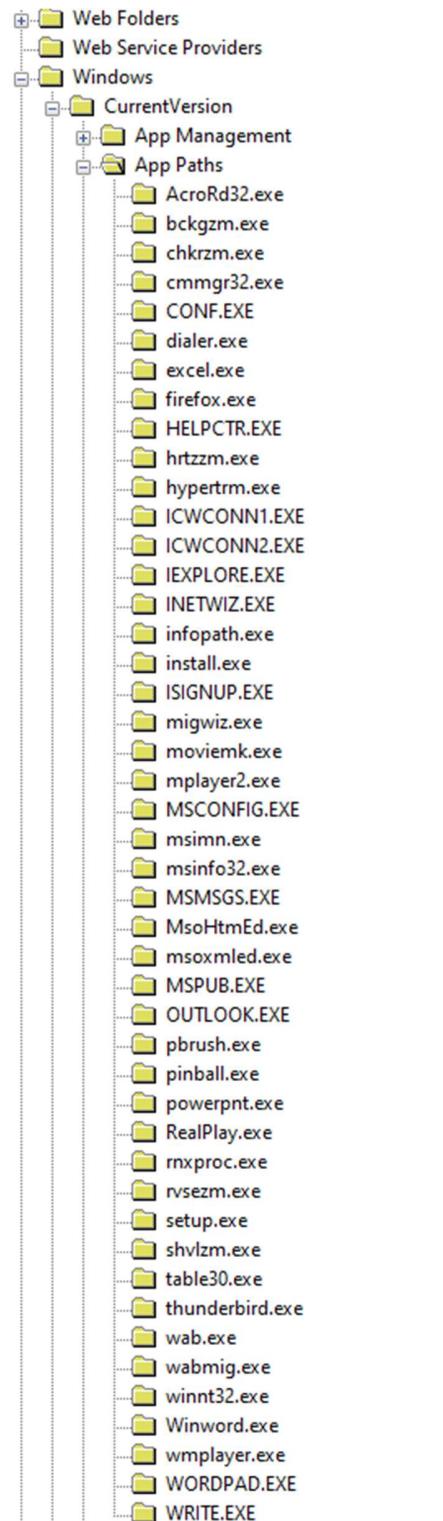
File Name	Content Type	URL	Fetch Count	Last Fetched	Server Response
5723.gif	image/gif	http://0b.bluestreak.com/ix.ebb&t=5723	2	09/02/2005 11:27:30	HTTP/1.0 200 OK
Attractions.gif	image/gif	http://www.traveltex.com/images/sc_savers/Attractions.gif	1	09/02/2005 11:27:13	HTTP/1.0 200 OK
attractions_icon.jpg	image/jpeg	http://www.traveltex.com/images/sc_savers/attractions_icon.jpg	1	09/02/2005 11:27:13	HTTP/1.0 200 OK
Beeches.gif	image/gif	http://www.traveltex.com/images/sc_savers/Beeches.gif	1	09/02/2005 11:27:13	HTTP/1.0 200 OK
beeches_icon.jpg	image/jpeg	http://www.traveltex.com/images/sc_savers/beeches_icon.jpg	1	09/02/2005 11:27:13	HTTP/1.0 200 OK
bg_tile.gif	image/gif	http://www.traveltex.com/images/bg_tile.gif	1	09/02/2005 11:27:13	HTTP/1.0 200 OK
Birds.gif	image/gif	http://www.traveltex.com/images/sc_savers/Birds.gif	1	09/02/2005 11:27:13	HTTP/1.0 200 OK
birds.gif	image/gif	http://www.traveltex.com/images/sc_savers/birds.gif	1	09/02/2005 11:27:13	HTTP/1.0 200 OK
birds.zip	application/x-zip-compressed	http://www.traveltex.com/downloads/screensavers/birds.zip	1	09/02/2005 11:27:47	HTTP/1.0 200 OK
birds_icon.jpg	image/jpeg	http://www.traveltex.com/images/sc_savers/birds_icon.jpg	1	09/02/2005 11:27:13	HTTP/1.0 200 OK
clear.gif	image/gif	http://www.google.co.uk/images/firefox/clear.gif	1	09/02/2005 11:28:59	HTTP/1.0 200 OK
client=firefox-a&rls=org.mozilla%3Aen-GB%3Aofficial_s&hl=en&q=b.htm	text/html	http://www.google.co.uk/search?client=firefox-a&rls=org.mozilla%3Aen-GB%3Aofficial_s&hl=en&q=bird+screensaver&...	1	09/02/2005 11:27:00	HTTP/1.0 200 OK
client=firefox-a&rls=org.mozilla_en-GB_official.htm	text/html	http://start.mozilla.org/firefox/client=firefox-a&rls=org.mozilla:en-GB:official	1	09/02/2005 11:28:49	HTTP/1.0 301 Mov...

15.4 birds.zip download from downloads.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>
```

APPENDIX F - REGISTRY ANALYSIS

0.1 software registry hive installed programs



0.2 Extracted installed programs summary data from software hive

Product name	Executable path
Adobe Acrobat 7	C:\Program Files\Adobe\Acrobat 7.0\Reader\AcroRd32.exe
MS Backgammon	C:\Program Files\MSN Gaming Zone\Windows\bckgzm.exe
MS Checkers	C:\Program Files\MSN Gaming Zone\Windows\chkrzm.exe
MS Connection Manager	C:\WINDOWS\system32\cmmgr32.exe
MS NetMeeting	C:\Program Files\NetMeeting\conf.exe
MS Dialer	C:\Program Files\Windows NT\dialer.exe
Excel	C:\PROGRA~1\MICROS~2\OFFICE11\EXCEL.EXE
Firefox	C:\Program Files\Mozilla Firefox\firefox.exe
Help Center	C:\WINDOWS\PCHealth\HelpCtr\Binaries\HelpCtr.exe
MS Hearts	C:\Program Files\MSN Gaming Zone\Windows\hrtzzm.exe
HyperTerminal	C:\Program Files\Windows NT\hypertrm.exe
MS Internet Connection Wizard	C:\Program Files\Internet Explorer\Connection Wizard\ICWCONN1.EXE
MS Internet Connection Wizard	C:\Program Files\Internet Explorer\Connection Wizard\ICWCONN2.EXE
Internet Explorer	C:\Program Files\Internet Explorer\iexplore.exe
MS Internet Connection Wizard	C:\Program Files\Internet Explorer\Connection Wizard\INETWIZ.EXE
Infopath	C:\Program Files\Microsoft Office\OFFICE11\INFOPATH.EXE
MS Internet Connection Wizard	C:\Program Files\Internet Explorer\Connection Wizard\ISIGNUP.EXE
Windows Easy Transfer	%SystemRoot%\system32\usmt\migwiz.exe
Movie Maker	C:\Program Files\Movie Maker\moviemk.exe
Windows Media Player	C:\Program Files\Windows Media Player\mplayer2.exe
System Configuration utility	C:\WINDOWS\PCHealth\HelpCtr\Binaries\MSConfig.exe
Outlook Express	%ProgramFiles%\Outlook Express\msimn.exe
MS System Information	C:\Program Files\Common Files\Microsoft Shared\MSInfo\MSInfo32.exe
MSN Messenger	C:\Program Files\Messenger\msmsgs.exe
Office XML Handler	C:\Program Files\Common Files\Microsoft Shared\OFFICE11\MSOXMLED.EXE
Publisher	C:\PROGRA~1\MICROS~2\OFFICE11\MSPUB.EXE
Outlook	C:\PROGRA~1\MICROS~2\OFFICE11\OUTLOOK.EXE
MS Paint	%SystemRoot%\system32\mspaint.exe
Pinball	C:\Program Files\Windows NT\Pinball\pinball.exe
Powerpoint	C:\PROGRA~1\MICROS~2\OFFICE11\POWERPNT.EXE
RealPlayer	C:\Program Files\Real\RealPlayer\realplay.exe
RNX File Processor	C:\Program Files\Common Files\Real\Update_OB\rnxproc.exe
Reversi	C:\Program Files\MSN Gaming Zone\Windows\rvsezm.exe
MSN Gaming Zone	C:\Program Files\MSN Gaming Zone\Windows\shvlzm.exe
Thunderbird	C:\Program Files\Mozilla Thunderbird\thunderbird.exe
Windows Address Book	C:\Program Files\Mozilla Thunderbird\thunderbird.exe
Windows Contacts Import Tool	%ProgramFiles%\Outlook Express\wabmig.exe

Word	C:\PROGRA~1\MICROS~2\OFFICE11\WINWORD.EXE
Windows Media Player	C:\Program Files\Windows Media Player\wmplayer.exe
Wordpad	%ProgramFiles%\Windows NT\Accessories\WORDPAD.EXE

3.11 NTUSER.DAT (johndoe) Recent Documents key

Metadata		
Name:	4	Type: REG_BIN
Value		
0x0	61 00 61 00 30 00 31 00 30 00 37 00 30 00 33 00	a.a.0.1.0.7.0.3.
0x10	61 00 2E 00 68 00 74 00 6D 00 00 00 4E 00 32 00	a...h.t.m...N.2.
0x20	00 00 00 00 00 00 00 00 00 00 61 61 30 31 30 37aa0107
0x30	30 33 61 2E 6C 6E 6B 00 32 00 03 00 04 00 EF BE	03a.lnk.2.....
0x40	00 00 00 00 00 00 00 00 14 00 00 00 61 00 61 00a.a.
0x50	30 00 31 00 30 00 37 00 30 00 33 00 61 00 2E 00	0.1.0.7.0.3.a...
0x60	6C 00 6E 00 6B 00 00 00 1C 00 00 00	l.n.k.....
Value		
Name:	6	
Type:	REG_BIN	
Value		
0x0	6E 00 65 00 73 00 74 00 62 00 6F 00 78 00 74 00	n.e.s.t.b.o.x.t.
0x10	65 00 70 00 73 00 2E 00 74 00 78 00 74 00 00 00	i.p.s...t.x.t...
0x20	54 00 32 00 00 00 00 00 00 00 00 00 00 6E 65	T.2.....ne
0x30	73 74 62 6F 78 74 69 70 73 2E 6C 6E 6B 00 36 00	stboxtips.lnk.6.
0x40	03 00 04 00 EF BE 00 00 00 00 00 00 00 00 14 00
0x50	00 00 6E 00 65 00 73 00 74 00 62 00 6F 00 78 00	..n.e.s.t.b.o.x.
0x60	74 00 69 00 70 00 73 00 2E 00 6C 00 6E 00 6B 00	t.i.p.s...l.n.k.
0x70	00 00 1E 00 00 00
Value		
Name:	12	
Type:	REG_BIN	
Value		
0x0	6B 00 61 00 6B 00 61 00 70 00 6F 00 2E 00 72 00	k.a.k.a.p.o....r.
0x10	61 00 6D 00 00 00 46 00 32 00 00 00 00 00 00 00	a.m...F.2.....
0x20	00 00 00 00 6B 61 6B 61 70 6F 2E 6C 6E 6B 00 00kakapo.lnk..
0x30	2C 00 03 00 04 00 EF BE 00 00 00 00 00 00 00 00 00	,.....
0x40	14 00 00 00 6B 00 61 00 6B 00 61 00 70 00 6F 00k.a.k.a.p.o.
0x50	2E 00 6C 00 6E 00 6B 00 00 00 1A 00 00 00	..l.n.k.....

3.12 Extracted summary data from Firefox NTUSER.DAT (johndoe) Recent Documents key

Key	Value	Value Data
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	4	aa010703a.htm
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	6	nestboxtips.txt
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	12	kakapo.ram

4.6 NTUSER.DAT (johndoe) Recent Documents key

Metadata		
Name:	35	
Type:	REG_BIN	
Value		
0x0	62 00 69 00 72 00 64 00 73 00 2E 00 7A 00 69 00	
0x10	70 00 00 00 4E 00 32 00 00 00 00 00 00 00 00 00	b.i.r.d.s...z.i. p...N.2.....
0x20	00 00 62 69 72 64 73 2E 7A 69 70 2E 6C 6E 6B 00	.birds.zip.lnk.
0x30	32 00 03 00 04 00 EF BE 00 00 00 00 00 00 00 00	2.....
0x40	14 00 00 00 62 00 69 00 72 00 64 00 73 00 2E 00b.i.r.d.s...
0x50	7A 00 69 00 70 00 2E 00 6C 00 6E 00 6B 00 00 00	z.i.p...l.n.k...
0x60	1C 00 00 00	

4.7 Extracted summary data from NTUSER.DAT (johndoe) Recent Documents key

Key	Value	Value Data
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	35	birds.zip

4.8 USB drive details from system hive

Name	Type	Data
DeviceDesc	REG_SZ	Disk drive
Capabilities	REG_DWORD	0x00000010 (16)
UINumber	REG_DWORD	0x00000000 (0)
HardwareID	REG_MULTI_SZ	USBSTOR\Disk_____USB_DISK_____1.05 USBSTOR...
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW
ClassGUID	REG_SZ	{4D36E967-E325-11CE-BFC1-08002BE10318}
Service	REG_SZ	disk
ConfigFlags	REG_DWORD	0x00000000 (0)
ParentIdPrefix	REG_SZ	7&2fb427dc&0
Driver	REG_SZ	{4D36E967-E325-11CE-BFC1-08002BE10318}\0002
Class	REG_SZ	DiskDrive
Mfg	REG_SZ	(Standard disk drives)
FriendlyName	REG_SZ	USB DISK USB Device

24142-system		
Name	Type	Data
??\Volume{30bf5ac0-6e1f-11d9-a7bd-806d6172696f}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 46 00 44 00 43 00 23 00 47 00 ...
??\Volume{30bf5ac1-6e1f-11d9-a7bd-806d6172696f}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 49 00 44 00 45 00 23 00 43 00 ...
\DosDevices\A:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 46 00 44 00 43 00 23 00 47 00 ...
\DosDevices\D:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 49 00 44 00 45 00 23 00 43 00 ...
\??\Volume{30bf5ac3-6e1f-11d9-a7bd-806d6172696f}	REG_BINARY	B8 DD B8 DD 00 7E 00 00 00 00 00 00
\DosDevices\C:	REG_BINARY	B8 DD B8 DD 00 7E 00 00 00 00 00 00
\??\Volume{44d36d3b-7525-11d9-ab5a-0048545652e0}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 53 00 54 00 4F 00 52 00 41 00 ...
\DosDevices\E:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 53 00 54 00 4F 00 52 00 41 00 ...
\??\Volume{44d36d43-7525-11d9-ab5a-0048545652e0}	REG_BINARY	B8 DD B8 DD 00 FC 47 BB 00 00 00 00 00
\DosDevices\F:	REG_BINARY	B8 DD B8 DD 00 FC 47 BB 00 00 00 00 00

Key Properties		
Last Written Time	03/02/2005 11:30:32 UTC	
00	5C 00 3F 00 3F 00 5C 00-53 00 54 00 4F 00 52 00 \-\?\-\?\-\S-T-O-R-	
10	41 00 47 00 45 00 23 00-52 00 65 00 6D 00 6F 00 A-G-E-\#-R-e-m-o-	
20	76 00 61 00 62 00 6C 00-65 00 4D 00 65 00 64 00 v-a-b-l-e-M-e-d-	
30	69 00 61 00 23 00 37 00-26 00 32 00 66 00 62 00 i-a-\#-7-a-2-f-b-	
40	34 00 32 00 37 00 64 00-63 00 26 00 30 00 26 00 4\2\7\o-c\c\o\z\	
50	52 00 4D 00 23 00 7B 00-35 00 33 00 66 00 35 00 R-M-\#-(5-3-f-5-	
60	36 00 33 00 30 00 64 00-2D 00 62 00 36 00 62 00 6-3-0-d-\#-b-6-b-	
70	66 00 2D 00 31 00 31 00-64 00 30 00 2D 00 39 00 f-\#-1-d-0-\#-9-	
80	34 00 66 00 32 00 2D 00-30 00 30 00 61 00 30 00 4\#-2-\#-0\#-a\#-	
90	63 00 39 00 31 00 65 00-66 00 62 00 38 00 62 00 c\#-1-e\#-b\#-8-b-	
a0	7D 00 }	

5.12 Mounted volume details from system hive

AccessData Registry Viewer (Demo Mode) - [24142-system]		
File Edit Report View Window Help		
Name	Type	Data
??\Volume{30bf5ac0-6e1f-11d9-a7bd-806d6172696f}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 46 00 44 00 43 00 23 00 47 00 ...
??\Volume{30bf5ac1-6e1f-11d9-a7bd-806d6172696f}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 49 00 44 00 45 00 23 00 43 00 ...
\DosDevices\A:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 46 00 44 00 43 00 23 00 47 00 ...
\DosDevices\D:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 49 00 44 00 45 00 23 00 43 00 ...
\??\Volume{30bf5ac3-6e1f-11d9-a7bd-806d6172696f}	REG_BINARY	B8 DD B8 DD 00 7E 00 00 00 00 00 00
\DosDevices\C:	REG_BINARY	B8 DD B8 DD 00 7E 00 00 00 00 00 00
\??\Volume{44d36d3b-7525-11d9-ab5a-0048545652e0}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 53 00 54 00 4F 00 52 00 41 00 ...
\DosDevices\E:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 53 00 54 00 4F 00 52 00 41 00 ...
\??\Volume{44d36d43-7525-11d9-ab5a-0048545652e0}	REG_BINARY	B8 DD B8 DD 00 FC 47 BB 00 00 00 00 00
\DosDevices\F:	REG_BINARY	B8 DD B8 DD 00 FC 47 BB 00 00 00 00 00

7.3 NTUSER.DAT (johndoe) Recent Documents key

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
					Metadata Name: 18 Type: REG_BIN				
					Value 0x0 61 00 67 00 67 00 72 00 65 00 73 00 73 00 69 00 0x10 76 00 65 00 5F 00 73 00 6F 00 6E 00 67 00 2E 00 0x20 77 00 61 00 76 00 00 00 6C 00 32 00 00 00 00 00 0x30 00 00 00 00 61 67 67 72 65 73 73 69 76 65 0x40 5F 73 6F 6E 67 2E 77 61 76 2E 6C 6E 6B 00 46 00 0x50 03 00 04 00 EF BE 00 00 00 00 00 00 00 14 00 0x60 00 00 61 00 67 00 67 00 72 00 65 00 73 00 73 00 0x70 69 00 76 00 65 00 5F 00 73 00 6F 00 6E 00 67 00 0x80 2E 00 77 00 61 00 76 00 2E 00 6C 00 6E 00 6B 00 0x90 00 00 2E 00 00 00				a.g.g.r.e.s.s.i. v.e._s.o.n.g... w.a.v...1.2....aggressive _song.wav.lnk.F.g.g.r.e.s.s. i.v.e._s.o.n.g. ..w.a.v...l.n.n.k. ...g...

7.4 Extracted summary data from NTUSER.DAT (johndoe) Recent Documents key

Key	Value	Value Data
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	18	aggressive_song.wav

9.4 NTUSER.DAT (johndoe) Recent Documents key

Key	Value	Value Data
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	20	EvanstonWoodpecker.jpg

9.5 Extracted summary data from NTUSER.DAT (johndoe) Recent Documents key

Key	Value	Value Data
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	20	EvanstonWoodpecker.jpg

9.13 NTUSER.DAT (johndoe) Recent Documents key

Key	Value	Value Data
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	22	Doc1.doc

9.14 Extracted summary data from NTUSER.DAT (johndoe) Recent Documents key

Key	Value	Value Data
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	22	Doc1.doc

10.2 NTUSER.DAT (johndoe) UserAssist key

	Name	Type	Data
	HRZR_EHACNGU:P\Cebtenz_Svyr\Zbmvyyn Sversbk\sversbk.rkr	REG_BINARY	08 00 00 00 08 00 00 E0 36 3D 28 9A 0E C5 01
	HRZR_EHACNGU:P\VAQBI\F\ffgrz32\abrgncng.rkr	REG_BINARY	06 00 00 09 00 00 00 D0 AE 33 97 08 04 C5 01
	HRZR_EHACNGU:\vagc-vafgnry-1.0ep2.rkr	REG_BINARY	05 00 00 06 00 00 00 F7 AB 98 44 09 C5 01
	HRZR_EHACNGU:P\VAQBI\F\ffgrz32\ehqgy32.rkr	REG_BINARY	05 00 00 07 00 00 00 54 1A BB 47 09 C5 01
	HRZR_EHACNGU:P\Qbphzrafl naq Frggvat\wbuagbr\Qrfxgb\NqorEge70_zah_shyy.rkr	REG_BINARY	05 00 00 06 00 00 A0 1F E0 0B 48 09 C5 01
	HRZR_EHACVOY:\Cebtenz_Svyr\Nqbri\Npeborg 7.0\Emqre\NpebbEq32.rkr	REG_BINARY	06 00 00 07 00 00 E0 53 6A 4C 08 04 C5 01
	HRZR_EHACVOY	REG_BINARY	08 00 00 12 00 00 20 1A B7 A8 C7 0E C5 01
	HRZR_EHACVOY:\P\Opbphzrafl naq Frggvat\Nyy Href\Qrfxgb\Zbmvyyn Sversbk.yax	REG_BINARY	08 00 00 09 00 00 F0 99 60 4B C7 0E C5 01
	HRZR_EHACVOY:\P\Opbphzrafl naq Frggvat\Nyy Href\Qrfxgb	REG_BINARY	08 00 00 08 00 00 E0 C9 0F 3C 99 0E C5 01
	HRZR_EHACVOY:\P\VAQBI\F\ffgrz32\zzp.rkr	REG_BINARY	08 00 00 07 00 00 60 C2 22 A2 9A 0E C5 01
	HRZR_EHAPCY:qfx.pcy	REG_BINARY	08 00 00 06 00 00 E0 F4 FD AD EA 09 C5 01
	HRZR_EHACNGU:P\Cebtenz_Svyr\Zvpebfbsg Bssvp\BSSVPR11\zfbuzqrz.rkr	REG_BINARY	06 00 00 06 00 00 30 79 10 C7 EA 09 C5 01
	HRZR_EHACNGU:P\CEBTEN-1\ZBMVYY-1\VERSBR.KRR	REG_BINARY	06 00 00 06 00 00 FF 11 C7 EA 09 C5 01
	HRZR_EHACVOY:(2559N154-2107-11C4-Q0NS-000P04560950)	REG_BINARY	08 00 00 07 00 00 20 1A B7 A8 C7 0E C5 01
	HRZR_EHACVOY:\SpfVqy2%Z\Zvpebfbsg Bssvp\Zvpebfbsg Bssvp\Jbeq 2003.yax	REG_BINARY	06 00 00 06 00 00 50 F6 3A F5 FA 09 C5 01
	HRZR_EHACVOY:\SpfVqy2%Z\Zvpebfbsg Bssvp	REG_BINARY	08 00 00 09 00 00 80 93 B5 A8 C7 0E C5 01
	HRZR_EHACNGU:P\Cebtenz_Svyr\Zvpebfbsg Bssvp\BSSVPR11\UVAJBEQ.RKR	REG_BINARY	08 00 00 07 00 00 20 1A B7 A8 C7 0E C5 01
	HRZR_EHACNGU:P\VAQBI\Fvhv\SnagmySebag\vjri.rkr	REG_BINARY	06 00 00 06 00 00 7A BF F9 FE 09 C5 01
	HRZR_EHACNGU:P\CEBTEN-1\ZBMVYY-1\GUHQCR-1.RKR	REG_BINARY	08 00 00 06 00 00 40 CF AB 23 97 0E C5 01
	HRZR_EHACVOY:(2559N155-2107-11C4-Q0NS-000P04560950)	REG_BINARY	08 00 00 06 00 00 80 DC AE 23 97 0E C5 01
	HRZR_EHACNGU:(6455040-5081-1010-9508-00NNN002594R)	REG_BINARY	08 00 00 08 00 00 E0 6A DD 5B C9 0E C5 01

11.4 NTUSER.DAT (johndoe) Recent Documents key

RecentDocs	Name: 24	Type: REG_BIN																								
.doc .gif .htm .html .INI .jpg .pdf .ram .txt .wav .zip Folder	Value	<table border="1"> <tr><td>0x0</td><td>4B 00 69 00 6C 00 6C 00 64 00 65 00 65 00 72 00</td><td>K.i.l.l.d.e.e.r..</td></tr> <tr><td>0x10</td><td>2E 00 6A 00 70 00 67 00 00 58 00 32 00 00 00</td><td>..j.p.g...X.2...</td></tr> <tr><td>0x20</td><td>00 00 00 00 00 00 00 00 4B 69 6C 6C 64 65 65 72</td><td>.....Killdeer</td></tr> <tr><td>0x30</td><td>2E 6A 70 67 2E 6C 6E 6B 00 38 00 03 00 04 00</td><td>.Jpg.Ink.8....</td></tr> <tr><td>0x40</td><td>EF BE 00 00 00 00 00 00 00 14 00 00 00 4B 00</td><td>.....K.</td></tr> <tr><td>0x50</td><td>69 00 6C 00 6C 00 64 00 65 00 65 00 72 00 2E 00</td><td>i.l.l.d.e.e.r...</td></tr> <tr><td>0x60</td><td>6A 00 70 00 67 00 2E 00 6C 00 6E 00 6B 00 00 00</td><td>J.p.g...l.n.k...</td></tr> <tr><td>0x70</td><td>20 00 00 00</td><td>...</td></tr> </table>	0x0	4B 00 69 00 6C 00 6C 00 64 00 65 00 65 00 72 00	K.i.l.l.d.e.e.r..	0x10	2E 00 6A 00 70 00 67 00 00 58 00 32 00 00 00	..j.p.g...X.2...	0x20	00 00 00 00 00 00 00 00 4B 69 6C 6C 64 65 65 72Killdeer	0x30	2E 6A 70 67 2E 6C 6E 6B 00 38 00 03 00 04 00	.Jpg.Ink.8....	0x40	EF BE 00 00 00 00 00 00 00 14 00 00 00 4B 00K.	0x50	69 00 6C 00 6C 00 64 00 65 00 65 00 72 00 2E 00	i.l.l.d.e.e.r...	0x60	6A 00 70 00 67 00 2E 00 6C 00 6E 00 6B 00 00 00	J.p.g...l.n.k...	0x70	20 00 00 00	...
0x0	4B 00 69 00 6C 00 6C 00 64 00 65 00 65 00 72 00	K.i.l.l.d.e.e.r..																								
0x10	2E 00 6A 00 70 00 67 00 00 58 00 32 00 00 00	..j.p.g...X.2...																								
0x20	00 00 00 00 00 00 00 00 4B 69 6C 6C 64 65 65 72Killdeer																								
0x30	2E 6A 70 67 2E 6C 6E 6B 00 38 00 03 00 04 00	.Jpg.Ink.8....																								
0x40	EF BE 00 00 00 00 00 00 00 14 00 00 00 4B 00K.																								
0x50	69 00 6C 00 6C 00 64 00 65 00 65 00 72 00 2E 00	i.l.l.d.e.e.r...																								
0x60	6A 00 70 00 67 00 2E 00 6C 00 6E 00 6B 00 00 00	J.p.g...l.n.k...																								
0x70	20 00 00 00	...																								

11.5 Extracted summary data from NTUSER.DAT (johndoe) Recent Documents key

Key	Value	Value Data
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	24	Killdeer.jpg

12.15 NTUSER.DAT (johndoe) Recent Documents key

RecentDocs	Name: 27	Type: REG_BIN																														
.doc .gif .htm .html .INI .jpg .pdf .ram .txt .wav .zip Folder 1 MRUListEx 4	Value	<table border="1"> <tr><td>0x0</td><td>62 00 61 00 62 00 79 00 73 00 63 00 6F 00 74 00</td><td>b.a.b.y.s.c.o.t.</td></tr> <tr><td>0x10</td><td>5F 00 32 00 77 00 65 00 65 00 6B 00 73 00 31 00</td><td>_2.w.e.e.k.s.l.</td></tr> <tr><td>0x20</td><td>2E 00 6A 00 70 00 67 00 00 70 00 32 00 00</td><td>.J.p.g...p.2...</td></tr> <tr><td>0x30</td><td>00 00 00 00 00 00 00 00 62 61 62 79 73 63 EF 74</td><td>.....babyscot</td></tr> <tr><td>0x40</td><td>5F 32 77 65 65 6B 73 31 2E 6A 70 67 2E 6C 6E 6B</td><td>_2weeksl.jpg.lnk</td></tr> <tr><td>0x50</td><td>00 00 48 00 03 00 04 00 EF BE 00 00 00 00 00</td><td>_H.....</td></tr> <tr><td>0x60</td><td>00 00 14 00 00 00 62 00 61 00 62 00 79 00 73 00</td><td>.....b.a.b.y.s.</td></tr> <tr><td>0x70</td><td>63 00 6F 00 74 00 5F 00 32 00 77 00 65 00 65 00</td><td>c.o.t._2.w.e.e.</td></tr> <tr><td>0x80</td><td>6B 00 73 00 31 00 2E 00 6A 00 70 00 67 00 2E 00</td><td>k.s.l...j.p.g...</td></tr> <tr><td>0x90</td><td>6C 00 6E 00 6B 00 00 00 28 00 00 00</td><td>l.n.k....</td></tr> </table>	0x0	62 00 61 00 62 00 79 00 73 00 63 00 6F 00 74 00	b.a.b.y.s.c.o.t.	0x10	5F 00 32 00 77 00 65 00 65 00 6B 00 73 00 31 00	_2.w.e.e.k.s.l.	0x20	2E 00 6A 00 70 00 67 00 00 70 00 32 00 00	.J.p.g...p.2...	0x30	00 00 00 00 00 00 00 00 62 61 62 79 73 63 EF 74babyscot	0x40	5F 32 77 65 65 6B 73 31 2E 6A 70 67 2E 6C 6E 6B	_2weeksl.jpg.lnk	0x50	00 00 48 00 03 00 04 00 EF BE 00 00 00 00 00	_H.....	0x60	00 00 14 00 00 00 62 00 61 00 62 00 79 00 73 00b.a.b.y.s.	0x70	63 00 6F 00 74 00 5F 00 32 00 77 00 65 00 65 00	c.o.t._2.w.e.e.	0x80	6B 00 73 00 31 00 2E 00 6A 00 70 00 67 00 2E 00	k.s.l...j.p.g...	0x90	6C 00 6E 00 6B 00 00 00 28 00 00 00	l.n.k....
0x0	62 00 61 00 62 00 79 00 73 00 63 00 6F 00 74 00	b.a.b.y.s.c.o.t.																														
0x10	5F 00 32 00 77 00 65 00 65 00 6B 00 73 00 31 00	_2.w.e.e.k.s.l.																														
0x20	2E 00 6A 00 70 00 67 00 00 70 00 32 00 00	.J.p.g...p.2...																														
0x30	00 00 00 00 00 00 00 00 62 61 62 79 73 63 EF 74babyscot																														
0x40	5F 32 77 65 65 6B 73 31 2E 6A 70 67 2E 6C 6E 6B	_2weeksl.jpg.lnk																														
0x50	00 00 48 00 03 00 04 00 EF BE 00 00 00 00 00	_H.....																														
0x60	00 00 14 00 00 00 62 00 61 00 62 00 79 00 73 00b.a.b.y.s.																														
0x70	63 00 6F 00 74 00 5F 00 32 00 77 00 65 00 65 00	c.o.t._2.w.e.e.																														
0x80	6B 00 73 00 31 00 2E 00 6A 00 70 00 67 00 2E 00	k.s.l...j.p.g...																														
0x90	6C 00 6E 00 6B 00 00 00 28 00 00 00	l.n.k....																														

Name: 26		
Type: REG_BIN		
Value		
0x0	62 00 61 00 62 00 79 00 73 00 63 00 6F 00 74 00	b.a.b.y.s.c.o.t.
0x10	5F 00 76 00 79 00 6F 00 75 00 6E 00 67 00 2E 00	_.v.y.o.u.n.g...
0x20	6A 00 70 00 67 00 00 00 6C 00 32 00 00 00 00 00	j.p.g...1.2.....
0x30	00 00 00 00 00 00 62 61 62 79 73 63 6F 74 5F 76babyscot_v
0x40	79 6F 75 6E 67 2E 6A 70 67 2E 6C 6E 6B 00 46 00	young.jpg.lnk.F.
0x50	03 00 04 00 EF BE 00 00 00 00 00 00 00 00 14 00
0x60	00 00 62 00 61 00 62 00 79 00 73 00 63 00 6F 00	..b.a.b.y.s.c.o.
0x70	74 00 5F 00 76 00 79 00 6F 00 75 00 6E 00 67 00	t._v.y.o.u.n.g.
0x80	2E 00 6A 00 70 00 67 00 2E 00 6C 00 6E 00 6B 00	..j.p.g...l.n.k.
0x90	00 00 26 00 00 00	...&...
Metadata		
Name: 28		
Type: REG_BIN		
Value		
0x0	31 00 37 00 37 00 2E 00 6A 00 70 00 67 00 00 00	1.7.7...j.p.g...
0x10	48 00 32 00 00 00 00 00 00 00 00 00 00 00 31 37	H.2.....17
0x20	37 2E 6A 70 67 2E 6C 6E 6B 00 2E 00 03 00 04 00	7.jpg.lnk.....
0x30	EF BE 00 00 00 00 00 00 00 00 14 00 00 00 31 001.
0x40	37 00 37 00 2E 00 6A 00 70 00 67 00 2E 00 6C 00	7.7...j.p.g...1.
0x50	6E 00 6B 00 00 00 1A 00 00 00	n.k.....
Metadata		
Name: 32		
Type: REG_BIN		
Value		
0x0	42 00 6F 00 6F 00 6B 00 4C 00 69 00 73 00 74 00	B.o.o.k.L.i.s.t.
0x10	2E 00 64 00 6F 00 63 00 00 00 58 00 32 00 00 00	..d.o.c...X.2...
0x20	00 00 00 00 00 00 00 00 42 6F 6F 6B 4C 69 73 74BookList
0x30	2E 64 6F 63 2E 6C 6E 6B 00 00 38 00 03 00 04 00	.doc.lnk..8.....
0x40	EF BE 00 00 00 00 00 00 00 14 00 00 00 42 00B.
0x50	6F 00 6F 00 6B 00 4C 00 69 00 73 00 74 00 2E 00	o.o.k.L.i.s.t...
0x60	64 00 6F 00 63 00 2E 00 6C 00 6E 00 6B 00 00 00	d.o.c...l.n.k...
0x70	20 00 00 00	...
Metadata		
Name: 2		
Type: REG_BIN		
Value		
0x0	6E 00 65 00 77 00 62 00 69 00 65 00 73 00 32 00	n.e.w.b.i.e.s.2.
0x10	2E 00 6A 00 70 00 67 00 00 00 58 00 32 00 00 00	..j.p.g...X.2...
0x20	00 00 00 00 00 00 00 00 6E 65 77 62 69 65 73 32newbies2
0x30	2E 6A 70 67 2E 6C 6E 6B 00 00 38 00 03 00 04 00	.jpg.lnk..8.....
0x40	EF BE 00 00 00 00 00 00 00 14 00 00 00 6E 00n.
0x50	65 00 77 00 62 00 69 00 65 00 73 00 32 00 2E 00	e.w.b.i.e.s.2...
0x60	6A 00 70 00 67 00 2E 00 6C 00 6E 00 6B 00 00 00	j.p.g...l.n.k...
0x70	20 00 00 00	...
Metadata		
Name: 0		
Type: REG_BIN		
Value		
0x0	63 00 68 00 69 00 63 00 6B 00 73 00 32 00 2E 00	c.h.i.c.k.s.2...
0x10	6A 00 70 00 67 00 00 00 54 00 32 00 00 00 00 00	j.p.g...T.2.....
0x20	00 00 00 00 00 00 63 68 69 63 6B 73 32 2E 6A 70chicks2.jp
0x30	67 2E 6C 6E 6B 00 36 00 03 00 04 00 EF BE 00 00	g.lnk.6.....
0x40	00 00 00 00 00 00 14 00 00 00 63 00 68 00 69 00c.h.i.
0x50	63 00 6B 00 73 00 32 00 2E 00 6A 00 70 00 67 00	c.k.s.2...j.p.g.
0x60	2E 00 6C 00 6E 00 6B 00 00 00 1E 00 00 00	..l.n.k.....

Metadata		
Name:	3	Type: REG_BIN
Value		
0x0	72 00 65 00 61 00 64 00 79 00 32 00 66 00 6C 00	r.e.a.d.y.2.f.l.
0x10	65 00 64 00 67 00 65 00 2E 00 6A 00 70 00 67 00	e.d.g.e...j.p.g.
0x20	00 00 64 00 32 00 00 00 00 00 00 00 00 00 00 00	..d.2.....
0x30	72 65 61 64 79 32 66 6C 65 64 67 65 2E 6A 70 67	ready2fledge.jpg
0x40	2E 6C 6E 6B 00 00 40 00 03 00 04 00 EF BE 00 00	.lnk..@.....
0x50	00 00 00 00 00 00 14 00 00 00 72 00 65 00 61 00r.e.a.
0x60	64 00 79 00 32 00 66 00 6C 00 65 00 64 00 67 00	d.y.2.f.l.e.d.g.
0x70	65 00 2E 00 6A 00 70 00 67 00 2E 00 6C 00 6E 00	e...j.p.g...l.n.
0x80	6B 00 00 00 24 00 00 00	k...\$...

Metadata		
Name:	29	Type: REG_BIN
Value		
0x0	6F 00 73 00 74 00 62 00 6B 00 32 00 62 00 32 00	o.s.t.b.k.2.b.2.
0x10	2E 00 68 00 74 00 6D 00 00 00 58 00 32 00 00 00	..h.t.m...X.2...
0x20	00 00 00 00 00 00 00 00 6F 73 74 62 6B 32 62 32ostbk2b2
0x30	2E 68 74 6D 2E 6C 6E 6B 00 00 38 00 03 00 04 00	.htm.lnk..8....
0x40	EF BE 00 00 00 00 00 00 00 14 00 00 00 6F 000...
0x50	73 00 74 00 62 00 6B 00 32 00 62 00 32 00 2E 00	s.t.b.k.2.b.2...
0x60	68 00 74 00 6D 00 2E 00 6C 00 6E 00 6B 00 00 00	h.t.m...l.n.k...
0x70	20 00 00 00	...

12.16 Extracted summary data from NTUSER.DAT (johndoe) Recent Documents key

Key	Value	Value Data
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	0	chicks2.jpg
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	2	newbies2.jpg
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	3	ready2fledge.jpg
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	26	babyscot_v young.jpg
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	27	babyscot_2weeks1.jpg
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	28	177.jpg
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	29	ostbk2b2.htm
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	30	birdtrans2.jpg

13.11 NTUSER.DAT (johndoe) Recent Documents key

RecentDocs		Name: 5	Type: REG_BIN
Value			
0x0	62 00 69 00 72 00 64 00 77 00 61 00 74 00 63 00	b.i.r.d.w.a.t.c.	
0x10	68 00 69 00 6E 00 67 00 2E 00 64 00 6F 00 63 00	h.i.n.g...d.o.c.	
0x20	00 00 64 00 32 00 00 00 00 00 00 00 00 00 00 00	..d.2.....	
0x30	62 69 72 64 77 61 74 63 68 69 6E 67 2E 64 6F 63	birdwatching.doc	
0x40	2E 6C 6E 6B 00 00 40 00 03 00 04 00 EF BE 00 00	.lnk..@.....	
0x50	00 00 00 00 00 00 14 00 00 00 62 00 69 00 72 00b.i.r.	
0x60	64 00 77 00 61 00 74 00 63 00 68 00 69 00 6E 00	d.w.a.t.c.h.i.n.	
0x70	67 00 2E 00 64 00 6F 00 63 00 2E 00 6C 00 6E 00	g...d.o.c...l.n.	
0x80	6B 00 00 00 24 00 00 00	k...\$...	

Name: 32																								
Type: REG_BIN																								
Value																								
<table border="1"> <tr><td>0x0</td><td>42 00 6F 00 6F 00 6B 00 4C 00 69 00 73 00 74 00</td><td>B.o.o.k.L.i.s.t.</td></tr> <tr><td>0x10</td><td>2E 00 64 00 6F 00 63 00 00 00 58 00 32 00 00 00</td><td>..d.o.c...X.2...</td></tr> <tr><td>0x20</td><td>00 00 00 00 00 00 00 00 42 6F 6B 4C 69 73 74</td><td>.....BookList</td></tr> <tr><td>0x30</td><td>2E 64 6F 63 2E 6C 6E 6B 00 00 38 00 03 00 04 00</td><td>.doc.lnk..8....</td></tr> <tr><td>0x40</td><td>EF BE 00 00 00 00 00 00 14 00 00 00 42 00</td><td>.....B.</td></tr> <tr><td>0x50</td><td>6F 00 6F 00 6B 00 4C 00 69 00 73 00 74 00 2E 00</td><td>o.o.k.L.i.s.t...</td></tr> <tr><td>0x60</td><td>64 00 6F 00 63 00 2E 00 6C 00 6E 00 6B 00 00 00</td><td>d.o.c...l.n.k...</td></tr> <tr><td>0x70</td><td>20 00 00 00</td><td>...</td></tr> </table>	0x0	42 00 6F 00 6F 00 6B 00 4C 00 69 00 73 00 74 00	B.o.o.k.L.i.s.t.	0x10	2E 00 64 00 6F 00 63 00 00 00 58 00 32 00 00 00	..d.o.c...X.2...	0x20	00 00 00 00 00 00 00 00 42 6F 6B 4C 69 73 74BookList	0x30	2E 64 6F 63 2E 6C 6E 6B 00 00 38 00 03 00 04 00	.doc.lnk..8....	0x40	EF BE 00 00 00 00 00 00 14 00 00 00 42 00B.	0x50	6F 00 6F 00 6B 00 4C 00 69 00 73 00 74 00 2E 00	o.o.k.L.i.s.t...	0x60	64 00 6F 00 63 00 2E 00 6C 00 6E 00 6B 00 00 00	d.o.c...l.n.k...	0x70	20 00 00 00	...
0x0	42 00 6F 00 6F 00 6B 00 4C 00 69 00 73 00 74 00	B.o.o.k.L.i.s.t.																						
0x10	2E 00 64 00 6F 00 63 00 00 00 58 00 32 00 00 00	..d.o.c...X.2...																						
0x20	00 00 00 00 00 00 00 00 42 6F 6B 4C 69 73 74BookList																						
0x30	2E 64 6F 63 2E 6C 6E 6B 00 00 38 00 03 00 04 00	.doc.lnk..8....																						
0x40	EF BE 00 00 00 00 00 00 14 00 00 00 42 00B.																						
0x50	6F 00 6F 00 6B 00 4C 00 69 00 73 00 74 00 2E 00	o.o.k.L.i.s.t...																						
0x60	64 00 6F 00 63 00 2E 00 6C 00 6E 00 6B 00 00 00	d.o.c...l.n.k...																						
0x70	20 00 00 00	...																						

Name: 13																								
Type: REG_BIN																								
Value																								
<table border="1"> <tr><td>0x0</td><td>42 00 69 00 72 00 64 00 69 00 6E 00 67 00 47 00</td><td>B.i.r.d.i.n.g.G.</td></tr> <tr><td>0x10</td><td>75 00 69 00 64 00 65 00 2E 00 70 00 64 00 66 00</td><td>u.i.d.e...p.d.f.</td></tr> <tr><td>0x20</td><td>00 00 58 00 32 00 00 00 00 00 00 00 00 00 00 00</td><td>..X.2.....</td></tr> <tr><td>0x30</td><td>42 69 72 64 69 6E 67 47 75 69 64 65 2E 6C 6E 6B</td><td>BirdingGuide.lnk</td></tr> <tr><td>0x40</td><td>00 00 38 00 03 00 04 00 EF BE 00 00 00 00 00 00 00</td><td>..8.....</td></tr> <tr><td>0x50</td><td>00 00 14 00 00 00 42 00 69 00 72 00 64 00 69 00</td><td>.....B.i.r.d.i.</td></tr> <tr><td>0x60</td><td>6E 00 67 00 47 00 75 00 69 00 64 00 65 00 2E 00</td><td>n.g.G.u.i.d.e...</td></tr> <tr><td>0x70</td><td>6C 00 6E 00 6B 00 00 00 20 00 00 00</td><td>l.n.k... ...</td></tr> </table>	0x0	42 00 69 00 72 00 64 00 69 00 6E 00 67 00 47 00	B.i.r.d.i.n.g.G.	0x10	75 00 69 00 64 00 65 00 2E 00 70 00 64 00 66 00	u.i.d.e...p.d.f.	0x20	00 00 58 00 32 00 00 00 00 00 00 00 00 00 00 00	..X.2.....	0x30	42 69 72 64 69 6E 67 47 75 69 64 65 2E 6C 6E 6B	BirdingGuide.lnk	0x40	00 00 38 00 03 00 04 00 EF BE 00 00 00 00 00 00 00	..8.....	0x50	00 00 14 00 00 00 42 00 69 00 72 00 64 00 69 00B.i.r.d.i.	0x60	6E 00 67 00 47 00 75 00 69 00 64 00 65 00 2E 00	n.g.G.u.i.d.e...	0x70	6C 00 6E 00 6B 00 00 00 20 00 00 00	l.n.k... ...
0x0	42 00 69 00 72 00 64 00 69 00 6E 00 67 00 47 00	B.i.r.d.i.n.g.G.																						
0x10	75 00 69 00 64 00 65 00 2E 00 70 00 64 00 66 00	u.i.d.e...p.d.f.																						
0x20	00 00 58 00 32 00 00 00 00 00 00 00 00 00 00 00	..X.2.....																						
0x30	42 69 72 64 69 6E 67 47 75 69 64 65 2E 6C 6E 6B	BirdingGuide.lnk																						
0x40	00 00 38 00 03 00 04 00 EF BE 00 00 00 00 00 00 00	..8.....																						
0x50	00 00 14 00 00 00 42 00 69 00 72 00 64 00 69 00B.i.r.d.i.																						
0x60	6E 00 67 00 47 00 75 00 69 00 64 00 65 00 2E 00	n.g.G.u.i.d.e...																						
0x70	6C 00 6E 00 6B 00 00 00 20 00 00 00	l.n.k... ...																						

13.12 Extracted summary data from NTUSER.DAT (johndoe) Recent Documents key

Key	Value	Value Data
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	5	birdwatching.doc
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	13	BirdingGuide.pdf
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	32	BookList.doc

17.5 NTUSER.DAT (johndoe) Recent Documents key

	<table border="1"> <tr> <td>Metadata</td></tr> <tr> <td>Name: 36</td></tr> <tr> <td>Type: REG_BIN</td></tr> <tr> <td>Value</td></tr> <tr> <td> <table border="1"> <tr><td>0x0</td><td>73 00 74 00 75 00 66 00 2E 00 64 00 6F 00 63 00</td><td>s.t.u.f...d.o.c.</td></tr> <tr><td>0x10</td><td>00 00 4C 00 32 00 00 00 00 00 00 00 00 00 00 00</td><td>..L.2.....</td></tr> <tr><td>0x20</td><td>73 74 75 66 2E 64 6F 63 2E 6C 6E 6B 00 00 30 00</td><td>stuf.doc.lnk..0.</td></tr> <tr><td>0x30</td><td>03 00 04 00 EF BE 00 00 00 00 00 00 00 00 14 00</td><td>.....</td></tr> <tr><td>0x40</td><td>00 00 73 00 74 00 75 00 66 00 2E 00 64 00 6F 00</td><td>..s.t.u.f...d.o.</td></tr> <tr><td>0x50</td><td>63 00 2E 00 6C 00 6E 00 6B 00 00 00 00 00 00 00</td><td>c...l.n.k.....</td></tr> </table> </td></tr> </table>	Metadata	Name: 36	Type: REG_BIN	Value	<table border="1"> <tr><td>0x0</td><td>73 00 74 00 75 00 66 00 2E 00 64 00 6F 00 63 00</td><td>s.t.u.f...d.o.c.</td></tr> <tr><td>0x10</td><td>00 00 4C 00 32 00 00 00 00 00 00 00 00 00 00 00</td><td>..L.2.....</td></tr> <tr><td>0x20</td><td>73 74 75 66 2E 64 6F 63 2E 6C 6E 6B 00 00 30 00</td><td>stuf.doc.lnk..0.</td></tr> <tr><td>0x30</td><td>03 00 04 00 EF BE 00 00 00 00 00 00 00 00 14 00</td><td>.....</td></tr> <tr><td>0x40</td><td>00 00 73 00 74 00 75 00 66 00 2E 00 64 00 6F 00</td><td>..s.t.u.f...d.o.</td></tr> <tr><td>0x50</td><td>63 00 2E 00 6C 00 6E 00 6B 00 00 00 00 00 00 00</td><td>c...l.n.k.....</td></tr> </table>	0x0	73 00 74 00 75 00 66 00 2E 00 64 00 6F 00 63 00	s.t.u.f...d.o.c.	0x10	00 00 4C 00 32 00 00 00 00 00 00 00 00 00 00 00	..L.2.....	0x20	73 74 75 66 2E 64 6F 63 2E 6C 6E 6B 00 00 30 00	stuf.doc.lnk..0.	0x30	03 00 04 00 EF BE 00 00 00 00 00 00 00 00 14 00	0x40	00 00 73 00 74 00 75 00 66 00 2E 00 64 00 6F 00	..s.t.u.f...d.o.	0x50	63 00 2E 00 6C 00 6E 00 6B 00 00 00 00 00 00 00	c...l.n.k.....
Metadata																								
Name: 36																								
Type: REG_BIN																								
Value																								
<table border="1"> <tr><td>0x0</td><td>73 00 74 00 75 00 66 00 2E 00 64 00 6F 00 63 00</td><td>s.t.u.f...d.o.c.</td></tr> <tr><td>0x10</td><td>00 00 4C 00 32 00 00 00 00 00 00 00 00 00 00 00</td><td>..L.2.....</td></tr> <tr><td>0x20</td><td>73 74 75 66 2E 64 6F 63 2E 6C 6E 6B 00 00 30 00</td><td>stuf.doc.lnk..0.</td></tr> <tr><td>0x30</td><td>03 00 04 00 EF BE 00 00 00 00 00 00 00 00 14 00</td><td>.....</td></tr> <tr><td>0x40</td><td>00 00 73 00 74 00 75 00 66 00 2E 00 64 00 6F 00</td><td>..s.t.u.f...d.o.</td></tr> <tr><td>0x50</td><td>63 00 2E 00 6C 00 6E 00 6B 00 00 00 00 00 00 00</td><td>c...l.n.k.....</td></tr> </table>	0x0	73 00 74 00 75 00 66 00 2E 00 64 00 6F 00 63 00	s.t.u.f...d.o.c.	0x10	00 00 4C 00 32 00 00 00 00 00 00 00 00 00 00 00	..L.2.....	0x20	73 74 75 66 2E 64 6F 63 2E 6C 6E 6B 00 00 30 00	stuf.doc.lnk..0.	0x30	03 00 04 00 EF BE 00 00 00 00 00 00 00 00 14 00	0x40	00 00 73 00 74 00 75 00 66 00 2E 00 64 00 6F 00	..s.t.u.f...d.o.	0x50	63 00 2E 00 6C 00 6E 00 6B 00 00 00 00 00 00 00	c...l.n.k.....						
0x0	73 00 74 00 75 00 66 00 2E 00 64 00 6F 00 63 00	s.t.u.f...d.o.c.																						
0x10	00 00 4C 00 32 00 00 00 00 00 00 00 00 00 00 00	..L.2.....																						
0x20	73 74 75 66 2E 64 6F 63 2E 6C 6E 6B 00 00 30 00	stuf.doc.lnk..0.																						
0x30	03 00 04 00 EF BE 00 00 00 00 00 00 00 00 14 00																						
0x40	00 00 73 00 74 00 75 00 66 00 2E 00 64 00 6F 00	..s.t.u.f...d.o.																						
0x50	63 00 2E 00 6C 00 6E 00 6B 00 00 00 00 00 00 00	c...l.n.k.....																						

17.6 Extracted summary data from NTUSER.DAT (johndoe) Recent Documents key

Key	Value	Value Data
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	36	stuf.doc

17.21 NTUSER.DAT (johndoe) Recent Documents key

RecentDocs		Name: 11	Type: REG_BIN	
[+]	.doc	0x0	41 00 6C 00 6D 00 6F 00 6E 00 64 00 4D 00 61 00	{A.l.m.o.n.d.M.a.
[+]	.gif	0x10	72 00 73 00 68 00 47 00 72 00 65 00 61 00 74 00	r.s.h.G.r.e.a.t.
[+]	.htm	0x20	42 00 6C 00 75 00 65 00 48 00 65 00 72 00 6F 00	B.l.u.e.H.e.r.o.
[+]	.html	0x30	6E 00 53 00 74 00 61 00 6C 00 65 00 6E 00	n.S.t.a.l.l.i.n.
[+]	.INI	0x40	67 00 2E 00 6A 00 70 00 67 00 00 00 A2 00 32 00	g...J.p.g.....2.
[+]	.jpg	0x50	00 00 00 00 00 00 00 00 00 41 6C 6D 6F 6E 64Almond
[+]	.pdf	0x60	6D 61 72 73 68 47 72 65 61 74 42 6C 75 65 48 65	MarshGreatBlueHe
[+]	.ram	0x70	72 6F 6E 53 74 61 6C 69 6E 67 2E 6A 70 67 2E	ronStalling.jpg.
[+]	.txt	0x80	6C 6E 6B 00 6A 00 03 00 04 00 EE BE 00 00 00 00	lnk.j.....
[+]	.wav	0x90	00 00 00 00 14 00 00 00 41 00 6C 00 6D 00 6F 00A.l.m.o.
[+]	.zip	0xa0	6E 00 64 00 4D 00 61 00 72 00 73 00 65 00 47 00	n.d.M.a.r.s.h.G.
[+]	Folder	0xb0	72 00 65 00 61 00 74 00 42 00 6C 00 75 00 65 00	r.e.a.t.B.l.u.e.
●	1	0xc0	48 00 65 00 72 00 6F 00 6E 00 53 00 74 00 61 00	H.e.r.o.n.S.t.a.
●	MRUListEx	0xd0	6C 00 6C 00 69 00 6E 00 67 00 2E 00 6A 00 70 00	l.l.i.n.g..j.p.
●	4	0xe0	67 00 2E 00 6C 00 6E 00 6B 00 00 00 38 00 00 00	g...l.n.k...8...
●	6			
●	8			
●	9			

17.22 Extracted summary data from NTUSER.DAT (johndoe) Recent Documents key

Key	Value	Value Data
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	11	AlmondMarshGreatBlueHeronStalling.jpg

APPENDIX G - RECENT DOCUMENTS ANALYSIS

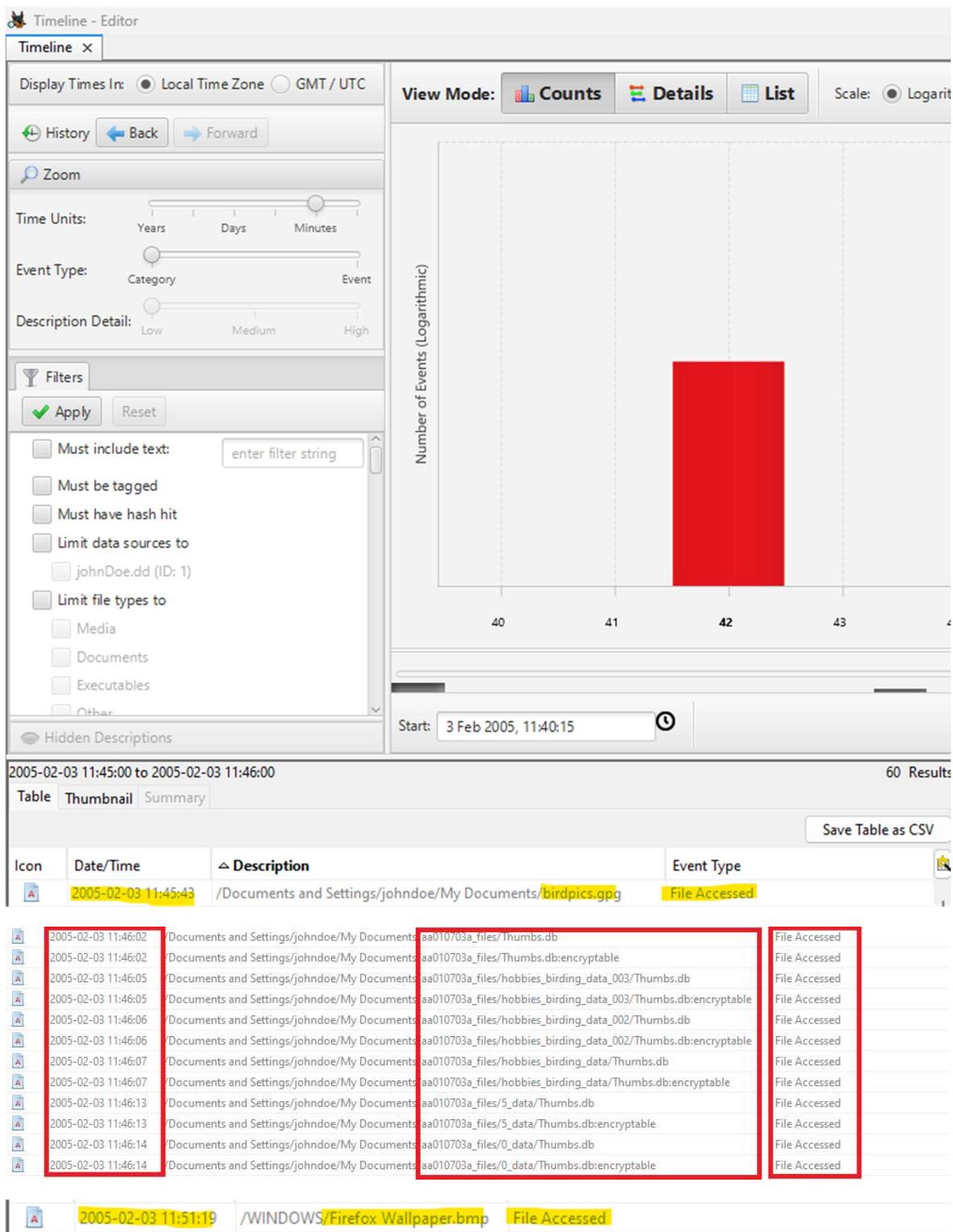
3.13 Recent folder (johndoe profile) entries

/img_johnDoe.dd/vol_vo2/Documents and Settings/johndoe/Recent							
	Table	Thumbnail	Summary				
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
[current folder]				2005-02-09 17:06:28 GMT	2005-02-09 17:06:28 GMT	2005-02-09 17:06:28 GMT	2005-01-28 16:51:42 GMT
[parent folder]				2005-01-28 16:51:42 GMT	2005-01-28 16:51:42 GMT	2005-02-09 16:51:54 GMT	2005-01-24 15:56:56 GMT
177.jpg.lnk		▼	2	2005-02-03 15:01:38 GMT	2005-02-03 15:01:38 GMT	2005-02-03 15:01:38 GMT	2005-02-03 15:01:38 GMT
aa010703a.htm		▼	2	2005-02-02 14:25:59 GMT	2005-02-02 14:25:59 GMT	2005-02-03 14:49:39 GMT	2005-02-02 14:25:59 GMT
aggressive_song.wav.lnk			2	2005-02-09 17:00:50 GMT	2005-02-09 17:00:50 GMT	2005-02-09 17:00:50 GMT	2005-02-03 12:22:51 GMT
AlmondMarshGreatBlueHeronStalling.jpg.lnk			2	2005-02-09 17:06:28 GMT	2005-02-09 17:06:28 GMT	2005-02-09 17:06:28 GMT	2005-02-09 17:06:28 GMT
audio.lnk			2	2005-02-03 12:22:51 GMT	2005-02-03 12:22:51 GMT	2005-02-03 14:49:38 GMT	2005-02-03 12:22:51 GMT
babyscot_2weeks1.jpg.lnk		▼	2	2005-02-03 15:00:27 GMT	2005-02-03 15:00:27 GMT	2005-02-03 15:00:27 GMT	2005-02-03 15:00:27 GMT
babyscot_vyoung.jpg.lnk		▼	2	2005-02-03 15:00:19 GMT	2005-02-03 15:00:19 GMT	2005-02-03 15:00:19 GMT	2005-02-03 15:00:19 GMT
BirdingGuide.pdf.lnk			2	2005-02-03 15:52:01 GMT	2005-02-03 15:52:01 GMT	2005-02-03 15:52:01 GMT	2005-02-03 15:52:01 GMT
birds.lnk			2	2005-02-03 14:49:29 GMT	2005-02-03 14:49:29 GMT	2005-02-03 14:49:38 GMT	2005-02-03 14:49:29 GMT
birds.zip.lnk		▼	2	2005-02-09 11:28:00 GMT	2005-02-09 11:28:00 GMT	2005-02-09 11:28:00 GMT	2005-02-09 11:28:00 GMT
birdtrans2.jpg.lnk		▼	2	2005-02-03 15:04:48 GMT	2005-02-03 15:04:48 GMT	2005-02-03 15:04:48 GMT	2005-02-03 15:04:48 GMT
birdwatching.doc.lnk			2	2005-02-03 15:49:39 GMT	2005-02-03 15:49:39 GMT	2005-02-03 15:49:39 GMT	2005-02-03 15:49:26 GMT
BookList.doc.lnk			2	2005-02-03 15:51:54 GMT	2005-02-03 15:51:54 GMT	2005-02-03 15:51:54 GMT	2005-02-03 15:51:43 GMT
bookmarks.html.lnk		▼	2	2005-02-03 12:20:20 GMT	2005-02-03 12:20:20 GMT	2005-02-03 14:49:39 GMT	2005-02-03 12:19:59 GMT
chicks2.jpg.lnk		▼	2	2005-02-03 15:05:03 GMT	2005-02-03 15:05:03 GMT	2005-02-03 15:05:03 GMT	2005-02-03 15:05:03 GMT
cookies.txt.lnk		▼	2	2005-02-03 12:19:07 GMT	2005-02-03 12:19:07 GMT	2005-02-03 14:49:51 GMT	2005-02-03 12:19:07 GMT
Desktop.ini			2	2005-01-28 16:51:42 GMT	2005-01-28 16:51:42 GMT	2005-02-09 11:27:53 GMT	2005-01-28 16:51:42 GMT
Doc1.doc.lnk			2	2005-02-03 14:17:47 GMT	2005-02-03 14:17:47 GMT	2005-02-03 14:49:39 GMT	2005-02-03 14:17:47 GMT
EvanstonWoodpecker.jpg.lnk			2	2005-02-03 14:14:59 GMT	2005-02-03 14:14:59 GMT	2005-02-03 14:49:52 GMT	2005-02-03 14:14:59 GMT
kakapo.lnk		▼	2	2005-02-02 15:11:51 GMT	2005-02-02 15:11:51 GMT	2005-02-03 14:49:54 GMT	2005-02-02 15:11:51 GMT

3.14 Extracted summary for Recent folder (johndoe profile) entries

File name	File location	Date first accessed	Date last accessed
aa010703a.htm	C:\Documents and Settings\johndoe\My Documents\	02/02/2005 14:25	03/02/2005 14:39
kakapo.ram	C:\Documents and Settings\johndoe\My Documents\	02/02/2005 15:11	03/02/2005 14:49

5.14 Accessed file timestamps



9.2 Recent folder (johndoe profile) entry

/img_johnDoe.dd/vol_vol2/Documents and Settings/johndoe/Recent							
Table		Thumbnail		Summary			
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
Desktop.ini		2		2005-01-28 16:51:42 GMT	2005-01-28 16:51:42 GMT	2005-02-09 11:27:53 GMT	2005-01-28 16:51:42 GMT
Doc1.doc.lnk		2		2005-02-03 14:17:47 GMT	2005-02-03 14:17:47 GMT	2005-02-03 14:49:39 GMT	2005-02-03 14:17:47 GMT
EvanstonWoodpecker.jpg.lnk		2		2005-02-03 14:14:59 GMT	2005-02-03 14:14:59 GMT	2005-02-03 14:49:52 GMT	2005-02-03 14:14:59 GMT
kakapo.lnk		2		2005-02-02 15:11:51 GMT	2005-02-02 15:11:51 GMT	2005-02-03 14:49:54 GMT	2005-02-02 15:11:51 GMT

9.3 Extracted summary for Recent folder (johndoe profile) entry

File name	File location	Date first accessed	Date last accessed
EvanstonWoodpecker.jpg	C:\	03/02/2005 14:14	03/02/2005 14:49

9.9 Recent folder (johndoe profile) entry

/img_johnDoe.dd/vol_vol2/Documents and Settings/johndoe/Recent							
Table		Thumbnail		Summary			
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
Desktop.ini		2		2005-01-28 16:51:42 GMT	2005-01-28 16:51:42 GMT	2005-02-09 11:27:53 GMT	2005-01-28 16:51:42 GMT
Doc1.doc.lnk		2		2005-02-03 14:17:47 GMT	2005-02-03 14:17:47 GMT	2005-02-03 14:49:39 GMT	2005-02-03 14:17:47 GMT
EvanstonWoodpecker.jpg.lnk		2		2005-02-03 14:14:59 GMT	2005-02-03 14:14:59 GMT	2005-02-03 14:49:52 GMT	2005-02-03 14:14:59 GMT

9.10 Extracted summary for Recent folder (johndoe profile) entry

File name	File location	Date first accessed	Date last accessed
Doc1.doc	C:\Documents and Settings\All Users\Documents\My Music\Sample Music\	03/02/2005 14:17	03/02/2005 14:49

9.11 Extracted summary for Office/Recent folder (johndoe profile) entry

/img_johnDoe.dd/vol_vol2/Documents and Settings/johndoe/Application Data/Microsoft/Office/Recent							
Table		Thumbnail		Summary			
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
[current folder]				2005-02-09 16:57:46 GMT	2005-02-09 16:57:46 GMT	2005-02-09 16:57:46 GMT	2005-01-25 11:35:54 GMT
[parent folder]				2005-01-25 11:35:54 GMT	2005-01-25 11:35:54 GMT	2005-02-09 16:51:54 GMT	2005-01-25 11:35:30 GMT
birdwatching.doc.LNK		2		2005-02-03 15:49:31 GMT	2005-02-03 15:49:31 GMT	2005-02-03 15:49:31 GMT	2005-02-03 15:49:31 GMT
BookList.doc.LNK		2		2005-02-03 15:51:45 GMT	2005-02-03 15:51:45 GMT	2005-02-03 15:51:45 GMT	2005-02-03 15:51:45 GMT
bookmarks.html.LNK		2		2005-02-03 12:20:06 GMT	2005-02-03 12:20:06 GMT	2005-02-03 12:20:06 GMT	2005-02-03 12:20:06 GMT
Desktop.ini		3		2005-02-03 14:17:24 GMT	2005-02-03 14:17:24 GMT	2005-02-09 16:57:46 GMT	2005-02-03 14:17:24 GMT
Doc1.doc.LNK		2		2005-02-03 14:17:43 GMT	2005-02-03 14:17:43 GMT	2005-02-03 14:17:43 GMT	2005-02-03 14:17:43 GMT

9.12 Extracted summary for Recent folder (johndoe profile) entry

File name	File location	Date first accessed	Date last accessed
Doc1.doc	C:\Documents and Settings\All Users\Documents\My Music\Sample Music\	03/02/2005 14:17	03/02/2005 14:17

11.2 Recent folder (johndoe profile) entry

/img_johnDoe.dd/vol_vol2/Documents and Settings/johndoe/Recent							
Table		Thumbnail		Summary			
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
177.jpg.lnk		2		2005-02-03 15:01:38 GMT	2005-02-03 15:01:38 GMT	2005-02-03 15:01:38 GMT	2005-02-03 15:01:38 GMT
AlmondMarshGreatBlueHeronStalling.jpg.lnk		2		2005-02-09 17:06:28 GMT	2005-02-09 17:06:28 GMT	2005-02-09 17:06:28 GMT	2005-02-09 17:06:28 GMT
BirdingGuide.pdf.lnk		2		2005-02-03 15:52:01 GMT	2005-02-03 15:52:01 GMT	2005-02-03 15:52:01 GMT	2005-02-03 15:52:01 GMT
BookList.doc.lnk		2		2005-02-03 15:51:54 GMT	2005-02-03 15:51:54 GMT	2005-02-03 15:51:54 GMT	2005-02-03 15:51:43 GMT
Desktop.ini		2		2005-01-28 16:51:42 GMT	2005-01-28 16:51:42 GMT	2005-02-09 11:27:53 GMT	2005-01-28 16:51:42 GMT
Doc1.doc.lnk		2		2005-02-03 14:17:47 GMT	2005-02-03 14:17:47 GMT	2005-02-03 14:49:39 GMT	2005-02-03 14:17:47 GMT
EvanstonWoodpecker.jpg.lnk		2		2005-02-03 14:14:59 GMT	2005-02-03 14:14:59 GMT	2005-02-03 14:49:52 GMT	2005-02-03 14:14:59 GMT
Killdeer.jpg.lnk		2		2005-02-03 14:49:29 GMT	2005-02-03 14:49:29 GMT	2005-02-03 14:49:55 GMT	2005-02-03 14:49:29 GMT

11.3 Extracted summary for Recent folder (johndoe profile) entry

File name	File location	Date first accessed	Date last accessed
Killdeer.jpg	E:\birds\Killdeer.jpg	03/02/2005 14:49	03/02/2005 14:49

12.13 Recent folder (johndoe profile) entries

/img_johnDoe.dd/vol_vol2/Documents and Settings/johndoe/Recent							
Table		Thumbnail		Summary			
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
177.jpg.lnk		2		2005-02-03 15:01:38 GMT	2005-02-03 15:01:38 GMT	2005-02-03 15:01:38 GMT	2005-02-03 15:01:38 GMT
aa010703a.lnk		2		2005-02-02 14:25:59 GMT	2005-02-02 14:25:59 GMT	2005-02-03 14:49:39 GMT	2005-02-02 14:25:59 GMT
aggressive_song.wav.lnk		2		2005-02-09 17:00:50 GMT	2005-02-09 17:00:50 GMT	2005-02-09 17:00:50 GMT	2005-02-03 12:22:51 GMT
AlmondMarshGreatBlueHeronStalling.jpg.lnk		2		2005-02-09 17:06:28 GMT	2005-02-09 17:06:28 GMT	2005-02-09 17:06:28 GMT	2005-02-09 17:06:28 GMT
audio.lnk		2		2005-02-03 12:22:51 GMT	2005-02-03 12:22:51 GMT	2005-02-03 14:49:38 GMT	2005-02-03 12:22:51 GMT
babyscot_2weeks1.jpg.lnk		2		2005-02-03 15:00:27 GMT	2005-02-03 15:00:27 GMT	2005-02-03 15:00:27 GMT	2005-02-03 15:00:27 GMT
babyscot_vyoung.jpg.lnk		2		2005-02-03 15:00:19 GMT	2005-02-03 15:00:19 GMT	2005-02-03 15:00:19 GMT	2005-02-03 15:00:19 GMT
BirdingGuide.pdf.lnk		2		2005-02-03 15:52:01 GMT	2005-02-03 15:52:01 GMT	2005-02-03 15:52:01 GMT	2005-02-03 15:52:01 GMT
birds.lnk		2		2005-02-03 14:49:29 GMT	2005-02-03 14:49:29 GMT	2005-02-03 14:49:38 GMT	2005-02-03 14:49:29 GMT
birds.zip.lnk		2		2005-02-09 11:28:00 GMT	2005-02-09 11:28:00 GMT	2005-02-09 11:28:00 GMT	2005-02-09 11:28:00 GMT
birdtrans2.jpg.lnk		2		2005-02-03 15:04:48 GMT	2005-02-03 15:04:48 GMT	2005-02-03 15:04:48 GMT	2005-02-03 15:04:48 GMT
birdwatching.doc.lnk		2		2005-02-03 15:49:39 GMT	2005-02-03 15:49:39 GMT	2005-02-03 15:49:39 GMT	2005-02-03 15:49:26 GMT
BookList.doc.lnk		2		2005-02-03 15:51:54 GMT	2005-02-03 15:51:54 GMT	2005-02-03 15:51:43 GMT	2005-02-03 15:51:43 GMT
bookmarks.html.lnk		2		2005-02-03 12:20:20 GMT	2005-02-03 12:20:20 GMT	2005-02-03 14:49:39 GMT	2005-02-03 12:19:59 GMT
chicks2.jpg.lnk		2		2005-02-03 15:05:03 GMT	2005-02-03 15:05:03 GMT	2005-02-03 15:05:03 GMT	2005-02-03 15:05:03 GMT
cookies.txt.lnk		2		2005-02-03 12:19:07 GMT	2005-02-03 12:19:07 GMT	2005-02-03 14:49:51 GMT	2005-02-03 12:19:07 GMT
Desktop.ini		2		2005-01-28 16:51:42 GMT	2005-01-28 16:51:42 GMT	2005-02-09 11:27:53 GMT	2005-01-28 16:51:42 GMT
Doc1.doc.lnk		2		2005-02-03 14:17:47 GMT	2005-02-03 14:17:47 GMT	2005-02-03 14:49:39 GMT	2005-02-03 14:17:47 GMT
EvanstonWoodpecker.jpg.lnk		2		2005-02-03 14:14:59 GMT	2005-02-03 14:14:59 GMT	2005-02-03 14:49:52 GMT	2005-02-03 14:14:59 GMT
kakapo.lnk		2		2005-02-02 15:11:51 GMT	2005-02-02 15:11:51 GMT	2005-02-03 14:49:54 GMT	2005-02-02 15:11:51 GMT
Killdeer.jpg.lnk		2		2005-02-03 14:49:29 GMT	2005-02-03 14:49:29 GMT	2005-02-03 14:49:55 GMT	2005-02-03 14:49:29 GMT
Local Disk (C).lnk		2		2005-02-03 15:49:39 GMT	2005-02-03 15:49:39 GMT	2005-02-03 15:49:39 GMT	2005-02-03 14:14:59 GMT
MSN.lnk		2		2005-02-09 17:00:50 GMT	2005-02-09 17:00:50 GMT	2005-02-09 17:00:50 GMT	2005-02-09 17:00:50 GMT
My Music.lnk		2		2005-02-03 15:06:42 GMT	2005-02-03 15:06:42 GMT	2005-02-03 15:06:42 GMT	2005-02-03 15:06:42 GMT
My Pictures.lnk		2		2005-02-03 15:05:03 GMT	2005-02-03 15:05:03 GMT	2005-02-03 15:05:03 GMT	2005-02-02 14:18:14 GMT
nestboxtips.lnk		2		2005-02-02 14:29:30 GMT	2005-02-02 14:29:30 GMT	2005-02-03 14:49:56 GMT	2005-02-02 14:29:30 GMT
New Volume (F).lnk		2		2005-02-09 17:06:28 GMT	2005-02-09 17:06:28 GMT	2005-02-09 17:06:28 GMT	2005-02-09 17:06:28 GMT
newbies2.jpg.lnk		2		2005-02-03 15:05:44 GMT	2005-02-03 15:05:44 GMT	2005-02-03 15:05:44 GMT	2005-02-03 15:05:44 GMT
non_images.lnk		3		2005-02-03 15:52:01 GMT	2005-02-03 15:52:01 GMT	2005-02-03 15:52:01 GMT	2005-02-02 17:03:27 GMT
ODBC.INI.lnk		2		2005-02-03 15:54:06 GMT	2005-02-03 15:54:06 GMT	2005-02-03 15:54:06 GMT	2005-02-03 15:54:06 GMT
ostbk2b2.htm.lnk		2		2005-02-03 15:02:45 GMT	2005-02-03 15:02:45 GMT	2005-02-03 15:02:45 GMT	2005-02-03 15:02:45 GMT
Prac4 (2).lnk		2		2005-02-02 15:10:16 GMT	2005-02-02 15:10:16 GMT	2005-02-03 14:49:38 GMT	2005-02-02 15:10:16 GMT
Prac4.lnk		2		2005-02-02 15:10:16 GMT	2005-02-02 15:10:16 GMT	2005-02-03 14:49:57 GMT	2005-02-02 15:10:16 GMT
Q3 Thread (Statechart).lnk		2		2005-02-02 15:10:48 GMT	2005-02-02 15:10:48 GMT	2005-02-03 14:49:59 GMT	2005-02-02 15:10:48 GMT
ready2fledge.jpg.lnk		2		2005-02-03 15:06:42 GMT	2005-02-03 15:06:42 GMT	2005-02-03 15:06:42 GMT	2005-02-03 15:06:42 GMT

12.14 Extracted summary for Recent folder (johndoe profile) entries

File name	File location	Date first accessed	Date last accessed
babyscot_2weeks1.jpg	C:\Documents and Settings\johndoe\My Documents\My Pictures\	03/02/2005 15:00	03/02/2005 15:00
babyscot_vyoung.jpg	C:\Documents and Settings\johndoe\My Documents\My Pictures\	03/02/2005 15:00	03/02/2005 15:00
177.jpg	C:\Documents and Settings\johndoe\My Documents\My Pictures\	03/02/2005 15:01	03/02/2005 15:01
ostbk2b2.htm	C:\Documents and Settings\johndoe\My Documents\	03/02/2005 15:02	03/02/2005 15:02
birdtrans2.jpg	C:\Documents and Settings\johndoe\Desktop\	03/02/2005 15:04	03/02/2005 15:04
chicks2.jpg	C:\Documents and Settings\johndoe\My Documents\My Pictures\	03/02/2005 15:05	03/02/2005 15:05
newbies2.jpg	C:\Documents and Settings\johndoe\My Documents\	03/02/2005 15:05	03/02/2005 15:05
ready2fledge.jpg	C:\Documents and Settings\bob\My Documents\My Music\	03/02/2005 15:06	03/02/2005 15:06

13.09 Recent folder (johndoe profile) entries

/img_johnDoe.dd/vol_vol2/Documents and Settings/johndoe/Recent							
Table Thumbnail Summary							
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
chicks2.jpg.lnk	▼	2		2005-02-03 15:05:03 GMT	2005-02-03 15:05:03 GMT	2005-02-03 15:05:03 GMT	
My Pictures.lnk	▼	2		2005-02-03 15:05:03 GMT	2005-02-03 15:05:03 GMT	2005-02-02 14:18:14 GMT	
newbies2.jpg.lnk	▼	2		2005-02-03 15:05:44 GMT	2005-02-03 15:05:44 GMT	2005-02-03 15:05:44 GMT	
My Music.lnk		2		2005-02-03 15:06:42 GMT	2005-02-03 15:06:42 GMT	2005-02-03 15:06:42 GMT	
ready2fledge.jpg.lnk		2		2005-02-03 15:06:42 GMT	2005-02-03 15:06:42 GMT	2005-02-03 15:06:42 GMT	
birdwatching.doc.lnk		2		2005-02-03 15:49:39 GMT	2005-02-03 15:49:39 GMT	2005-02-03 15:49:39 GMT	2005-02-03 15:49:26 GMT
Local Disk (C).lnk		2		2005-02-03 15:49:39 GMT	2005-02-03 15:49:39 GMT	2005-02-03 15:49:39 GMT	2005-02-03 14:14:59 GMT
BookList.doc.lnk		2		2005-02-03 15:51:54 GMT	2005-02-03 15:51:54 GMT	2005-02-03 15:51:54 GMT	2005-02-03 15:51:43 GMT
BirdingGuide.pdf.lnk		2		2005-02-03 15:52:01 GMT	2005-02-03 15:52:01 GMT	2005-02-03 15:52:01 GMT	2005-02-03 15:52:01 GMT
non images.lnk		3		2005-02-03 15:52:01 GMT	2005-02-03 15:52:01 GMT	2005-02-03 15:52:01 GMT	2005-02-02 17:03:27 GMT

13.10 Extracted summary for Recent folder (johndoe profile) entries

File name	File location	Date first accessed	Date last accessed
birdwatching.doc	C:\	03/02/2005 15:49	03/02/2005 15:49
BookList.doc	E:\birds\non images\	03/02/2005 15:51	03/02/2005 15:51
BirdingGuide.pdf	E:\birds\non images\	03/02/2005 15:52	03/02/2005 15:52

13.13 Office/Recent folder (johndoe profile) entries

/img_johnDoe.dd/vol_vol2/Documents and Settings/johndoe/Application Data/Microsoft/Office/Recent							
Table Thumbnail Summary							
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
BookList.doc.LNK	2			2005-02-03 15:51:45 GMT	2005-02-03 15:51:45 GMT	2005-02-03 15:51:45 GMT	2005-02-03 15:51:45 GMT
Desktop.ini	3			2005-02-03 14:17:24 GMT	2005-02-03 14:17:24 GMT	2005-02-09 16:57:46 GMT	2005-02-03 14:17:24 GMT
Doc1.doc.LNK	2			2005-02-03 14:17:43 GMT	2005-02-03 14:17:43 GMT	2005-02-03 14:17:43 GMT	2005-02-03 14:17:43 GMT
Local Disk (C).LNK	2			2005-02-03 15:49:31 GMT	2005-02-03 15:49:31 GMT	2005-02-03 15:49:31 GMT	2005-02-03 15:49:31 GMT
My Documents.LNK	▼	2		2005-02-09 16:57:46 GMT	2005-02-09 16:57:46 GMT	2005-02-09 16:57:46 GMT	2005-02-09 16:56:51 GMT
Sample Music.LNK	2			2005-02-03 14:17:43 GMT	2005-02-03 14:17:43 GMT	2005-02-03 14:17:43 GMT	2005-02-03 14:17:43 GMT
Templates.LNK	▼	2		2005-01-25 11:35:55 GMT	2005-01-25 11:35:55 GMT	2005-01-25 11:35:55 GMT	2005-01-25 11:35:55 GMT
[current folder]				2005-02-09 16:57:46 GMT	2005-02-09 16:57:46 GMT	2005-02-09 16:57:46 GMT	2005-01-25 11:35:54 GMT
[parent folder]				2005-01-25 11:35:54 GMT	2005-01-25 11:35:54 GMT	2005-02-09 16:51:54 GMT	2005-01-25 11:35:30 GMT
birdwatching.doc.LNK	2			2005-02-03 15:49:31 GMT	2005-02-03 15:49:31 GMT	2005-02-03 15:49:31 GMT	2005-02-03 15:49:31 GMT

13.14 Extracted summary for Office/Recent folder (johndoe profile) entries

File name	File location	Date first accessed	Date last accessed
birdwatching.doc	C:\	03/02/2005 15:49	03/02/2005 15:49
BookList.doc	E:\birds\non images\	03/02/2005 15:51	03/02/2005 15:51

13.16 Recent folder (johndoe profile) entry

/img_johnDoe.dd/vol_vol2/Documents and Settings/johndoe/Recent							
Table Thumbnail Summary							
△ Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
New Volume (F).lnk			2	2005-02-09 17:06:28 GMT	2005-02-09 17:06:28 GMT	2005-02-09 17:06:28 GMT	2005-02-09 17:06:28 GMT
ODBC.INI.lnk			2	2005-02-03 15:54:06 GMT	2005-02-03 15:54:06 GMT	2005-02-03 15:54:06 GMT	2005-02-03 15:54:06 GMT
Prac4 (2).lnk			2	2005-02-02 15:10:16 GMT	2005-02-02 15:10:16 GMT	2005-02-03 14:49:38 GMT	2005-02-02 15:10:16 GMT

13.17 Extracted summary for Recent folder (johndoe profile) entry

File name	File location	Date first accessed	Date last accessed
ODBC.INI	C:\WINDOWS	03/02/2005 15:46	03/02/2005 15:46

15.5 Recent folder (johndoe profile) entry

/img_johnDoe.dd/vol_vol2/Documents and Settings/johndoe/Recent							
Table Thumbnail Summary							
△ Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
aa010703a.lnk			2	2005-02-02 14:25:59 GMT	2005-02-02 14:25:59 GMT	2005-02-03 14:49:39 GMT	2005-02-02 14:25:59 GMT
aggressive_song.wav.lnk			2	2005-02-09 17:00:50 GMT	2005-02-09 17:00:50 GMT	2005-02-09 17:00:50 GMT	2005-02-03 12:22:51 GMT
audio.lnk			2	2005-02-03 12:22:51 GMT	2005-02-03 12:22:51 GMT	2005-02-03 14:49:38 GMT	2005-02-03 12:22:51 GMT
babyscot_2weeks1.jpg.lnk			2	2005-02-03 15:00:27 GMT	2005-02-03 15:00:27 GMT	2005-02-03 15:00:27 GMT	2005-02-03 15:00:27 GMT
babyscot_vyoung.jpg.lnk			2	2005-02-03 15:00:19 GMT	2005-02-03 15:00:19 GMT	2005-02-03 15:00:19 GMT	2005-02-03 15:00:19 GMT
birds.lnk			2	2005-02-03 14:49:29 GMT	2005-02-03 14:49:29 GMT	2005-02-03 14:49:38 GMT	2005-02-03 14:49:29 GMT
birds.zip.lnk			2	2005-02-09 11:28:00 GMT	2005-02-09 11:28:00 GMT	2005-02-09 11:28:00 GMT	2005-02-09 11:28:00 GMT
birdtrans2.jpg.lnk			2	2005-02-03 15:04:48 GMT	2005-02-03 15:04:48 GMT	2005-02-03 15:04:48 GMT	2005-02-03 15:04:48 GMT

15.6 Extracted summary for Recent folder (johndoe profile) entry

File name	File location	Date first accessed	Date last accessed
birds.zip	C:\Documents and Settings\johndoe\My Documents\	09/02/2005 11:28	09/02/2005 11:28

17.3 Recent folder (johndoe profile) entry

/img_johnDoe.dd/vol_vol2/Documents and Settings/johndoe/Recent							
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
❑ kakapo.lnk	▼		2	2005-02-02 15:11:51 GMT	2005-02-02 15:11:51 GMT	2005-02-03 14:49:54 GMT	2005-02-02 15:11:51 GMT
❑ Killdeer.jpg.lnk			2	2005-02-03 14:49:29 GMT	2005-02-03 14:49:29 GMT	2005-02-03 14:49:29 GMT	2005-02-03 14:49:29 GMT
❑ Local Disk (C).lnk			2	2005-02-03 15:49:39 GMT	2005-02-03 15:49:39 GMT	2005-02-03 15:49:39 GMT	2005-02-03 14:14:59 GMT
❑ MSN.lnk			2	2005-02-09 17:00:50 GMT	2005-02-09 17:00:50 GMT	2005-02-09 17:00:50 GMT	2005-02-09 17:00:50 GMT
❑ My Music.lnk			2	2005-02-03 15:06:42 GMT	2005-02-03 15:06:42 GMT	2005-02-03 15:06:42 GMT	2005-02-03 15:06:42 GMT
❑ My Pictures.lnk		▼	2	2005-02-03 15:05:03 GMT	2005-02-03 15:05:03 GMT	2005-02-03 15:05:03 GMT	2005-02-02 14:18:14 GMT
❑ nestboxtips.lnk		▼	2	2005-02-02 14:29:30 GMT	2005-02-02 14:29:30 GMT	2005-02-03 14:49:56 GMT	2005-02-02 14:29:30 GMT
❑ New Volume (F).lnk			2	2005-02-09 17:06:28 GMT	2005-02-09 17:06:28 GMT	2005-02-09 17:06:28 GMT	2005-02-09 17:06:28 GMT
❑ newbies2.jpg.lnk		▼	2	2005-02-03 15:05:44 GMT	2005-02-03 15:05:44 GMT	2005-02-03 15:05:44 GMT	2005-02-03 15:05:44 GMT
❑ non_images.lnk			3	2005-02-03 15:52:01 GMT	2005-02-03 15:52:01 GMT	2005-02-03 15:52:01 GMT	2005-02-02 17:03:27 GMT
❑ ODBC.INI.lnk			2	2005-02-03 15:54:06 GMT	2005-02-03 15:54:06 GMT	2005-02-03 15:54:06 GMT	2005-02-03 15:54:06 GMT
❑ ostbk2b2.htm.lnk		▼	2	2005-02-03 15:02:45 GMT	2005-02-03 15:02:45 GMT	2005-02-03 15:02:45 GMT	2005-02-03 15:02:45 GMT
❑ Prac4 (2).lnk		▼	2	2005-02-02 15:10:16 GMT	2005-02-02 15:10:16 GMT	2005-02-03 14:49:38 GMT	2005-02-02 15:10:16 GMT
❑ Prac4.lnk		▼	2	2005-02-02 15:10:16 GMT	2005-02-02 15:10:16 GMT	2005-02-03 14:49:57 GMT	2005-02-02 15:10:16 GMT
❑ Q3 Thread (Statechart).lnk			2	2005-02-02 15:10:48 GMT	2005-02-02 15:10:48 GMT	2005-02-03 14:49:59 GMT	2005-02-02 15:10:48 GMT
❑ ready2fledge.jpg.lnk			2	2005-02-03 15:06:42 GMT	2005-02-03 15:06:42 GMT	2005-02-03 15:06:42 GMT	2005-02-03 15:06:42 GMT
❑ Sample Music.lnk			2	2005-02-03 14:17:48 GMT	2005-02-03 14:17:48 GMT	2005-02-03 14:49:38 GMT	2005-02-03 14:17:48 GMT
❑ stuf.doc.lnk		▼	2	2005-02-09 16:57:49 GMT	2005-02-09 16:57:49 GMT	2005-02-09 16:57:49 GMT	2005-02-09 16:57:49 GMT

17.4 Extracted summary for Recent folder (johndoe profile) entry

File name	File location	Date first accessed	Date last accessed
stuf.doc	C:\Documents and Settings\johndoe\My Documents\	09/02/2005 16:57	09/02/2005 16:57

17.7 Office/Recent folder (johndoe profile) entry

/img_johnDoe.dd/vol_vol2/Documents and Settings/johndoe/Application Data/Microsoft/Office/Recent							
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
❑ [current folder]				2005-02-09 16:57:46 GMT	2005-02-09 16:57:46 GMT	2005-02-09 16:57:46 GMT	2005-01-25 11:35:54 GMT
❑ [parent folder]				2005-01-25 11:35:54 GMT	2005-01-25 11:35:54 GMT	2005-02-09 16:51:54 GMT	2005-01-25 11:35:30 GMT
❑ birdwatching.doc.LNK			2	2005-02-03 15:49:31 GMT	2005-02-03 15:49:31 GMT	2005-02-03 15:49:31 GMT	2005-02-03 15:49:31 GMT
❑ BookList.doc.LNK			2	2005-02-03 15:51:45 GMT	2005-02-03 15:51:45 GMT	2005-02-03 15:51:45 GMT	2005-02-03 15:51:45 GMT
❑ bookmarks.html.LNK	▼		2	2005-02-03 12:20:06 GMT	2005-02-03 12:20:06 GMT	2005-02-03 12:20:06 GMT	2005-02-03 12:20:06 GMT
❑ Desktop.ini			3	2005-02-03 14:17:24 GMT	2005-02-03 14:17:24 GMT	2005-02-09 16:57:46 GMT	2005-02-03 14:17:24 GMT
❑ Doc1.doc.LNK			2	2005-02-03 14:17:43 GMT	2005-02-03 14:17:43 GMT	2005-02-03 14:17:43 GMT	2005-02-03 14:17:43 GMT
❑ index.dat	▼		2	2005-02-09 16:57:47 GMT	2005-02-09 16:57:47 GMT	2005-02-09 16:57:47 GMT	2005-01-25 11:35:55 GMT
❑ Local Disk (C).LNK			2	2005-02-03 15:49:31 GMT	2005-02-03 15:49:31 GMT	2005-02-03 15:49:31 GMT	2005-02-03 15:49:31 GMT
❑ My Documents.LNK	▼		2	2005-02-09 16:57:46 GMT	2005-02-09 16:57:46 GMT	2005-02-09 16:57:46 GMT	2005-02-09 16:56:51 GMT
❑ non_images.LNK			3	2005-02-03 15:51:46 GMT	2005-02-03 15:51:46 GMT	2005-02-03 15:51:46 GMT	2005-02-03 15:51:46 GMT
❑ Sample Music.LNK			2	2005-02-03 14:17:43 GMT	2005-02-03 14:17:43 GMT	2005-02-03 14:17:43 GMT	2005-02-03 14:17:43 GMT
❑ stuf.doc.LNK	▼		2	2005-02-09 16:57:46 GMT	2005-02-09 16:57:46 GMT	2005-02-09 16:57:46 GMT	2005-02-09 16:56:52 GMT
❑ Templates.LNK	▼		2	2005-01-25 11:35:55 GMT	2005-01-25 11:35:55 GMT	2005-01-25 11:35:55 GMT	2005-01-25 11:35:55 GMT

17.8 Extracted summary for Office/Recent folder (johndoe profile) entry

File name	File location	Date first accessed	Date last accessed
stuf.doc	C:\Documents and Settings\johndoe\My Documents\	09/02/2005 16:56	09/02/2005 16:57

17.19 Recent folder (johndoe profile) entry

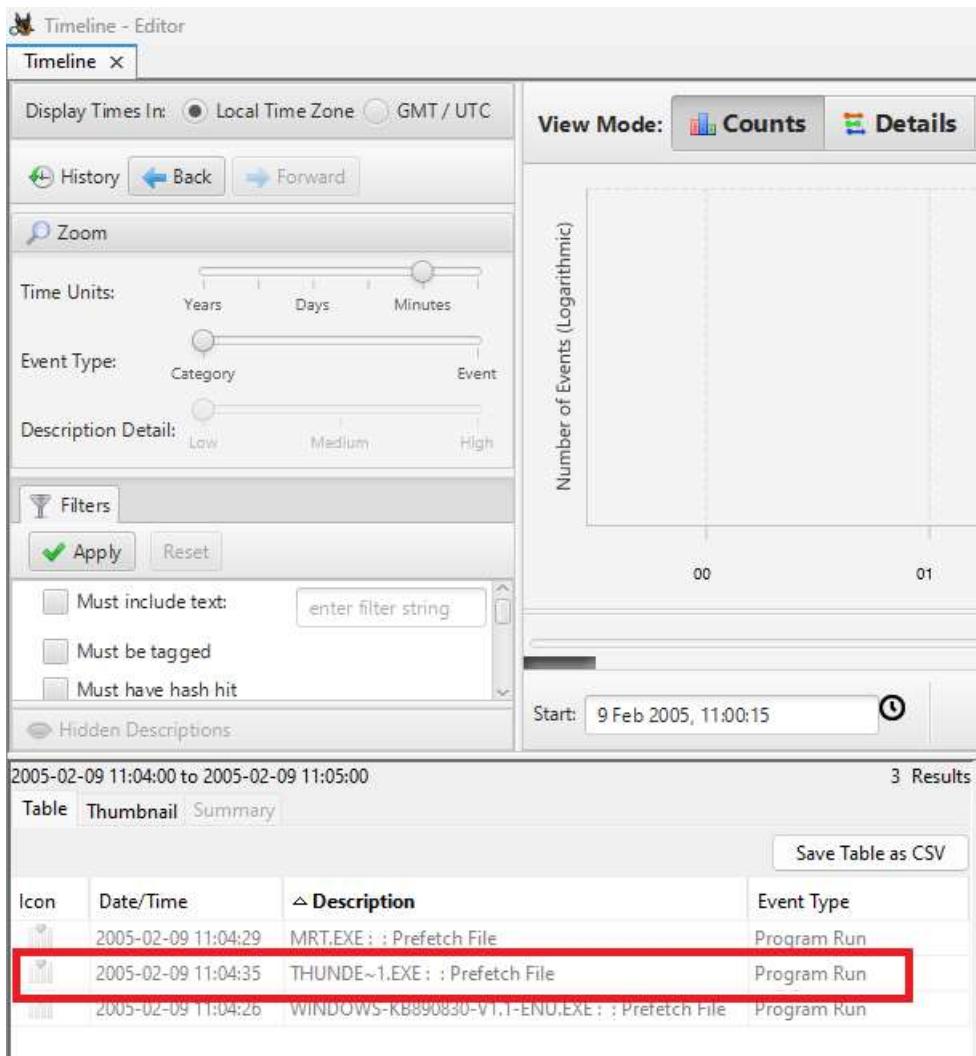
/img.johnDoe.dd/vol_vol2/Documents and Settings/johndoe/Recent							
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
[current folder]				2005-02-09 17:06:28 GMT	2005-02-09 17:06:28 GMT	2005-02-09 17:06:28 GMT	2005-01-28 16:51:42 GMT
[parent folder]				2005-01-28 16:51:42 GMT	2005-01-28 16:51:42 GMT	2005-02-09 16:51:54 GMT	2005-01-24 15:56:56 GMT
177.jpg.lnk	▼		2	2005-02-03 15:01:38 GMT	2005-02-03 15:01:38 GMT	2005-02-03 15:01:38 GMT	2005-02-03 15:01:38 GMT
aa010703a.lnk	▼		2	2005-02-02 14:25:59 GMT	2005-02-02 14:25:59 GMT	2005-02-03 14:49:39 GMT	2005-02-02 14:25:59 GMT
aggressive_song.wav.lnk			2	2005-02-09 17:00:50 GMT	2005-02-09 17:00:50 GMT	2005-02-09 17:00:50 GMT	2005-02-03 12:22:51 GMT
AlmondMarshGreatBlueHeronStalling.jpg.lnk			2	2005-02-09 17:06:28 GMT	2005-02-09 17:06:28 GMT	2005-02-09 17:06:28 GMT	2005-02-09 17:06:28 GMT
audio.lnk			2	2005-02-03 12:22:51 GMT	2005-02-03 12:22:51 GMT	2005-02-03 14:49:38 GMT	2005-02-03 12:22:51 GMT

17.20 Extracted summary for Recent folder (johndoe profile) entry

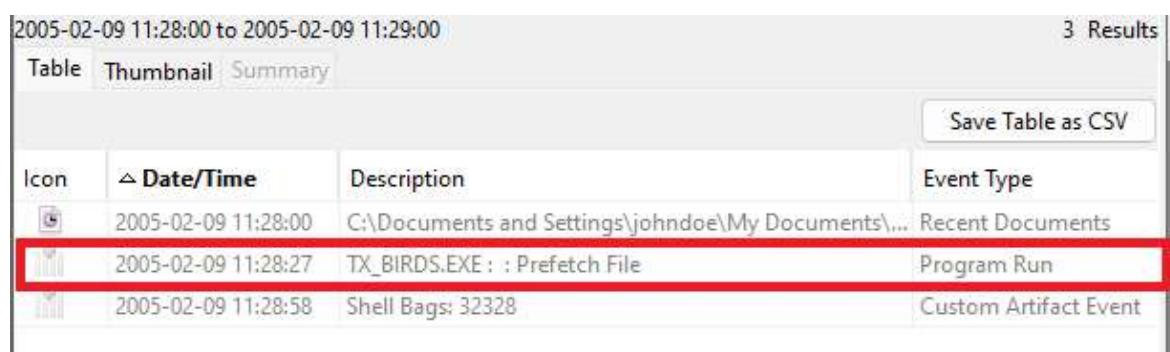
File name	File location	Date first accesse	Date last accesse
AlmondMarshGreatBlueHeronStalling.jpg	F:\	09/02/2005 17:06	09/02/2005 17:06

APPENDIX H - PREFETCH ANALYSIS

14.10 - THUNDE~1.EXE-2874618F.PF file creation



15.7 TX_BIRDS.EXE-2861E2BC.PF file creation



15.8 Extracted data for TX_BIRDS.EXE-2861E2BC.PF file creation

Prefetch file TX_BIRDS.EXE-2861E2BC.pf Process EXE Process path TX_BIRDS.EXE\DEVICE\HARDDISKVOLUME1\DOCUMENTS\JOHNDOE\LOCALS~1\TEMP\TEMPORARY DIRECTORY 1 FOR BIRDS.ZIP\TX_BIRDS.EXE Last run time 09/02/2005 11:28 File name TX_BIRDS.EXE

16.1 TX_BIRDS.EXE-24B103EC.PF AND TX_BIRDS.SCR-03FEBFC4.PF file creation

2 Results			
Icon	△ Date/Time	Description	Event Type
File	2005-02-09 13:50:27	TX_BIRDS.EXE : : Prefetch File	Program Run
File	2005-02-09 13:50:27	TX_BIRDS.SCR : : Prefetch File	Program Run

Save Table as CSV

APPENDIX I - RECYCLING BIN ANALYSIS

13.4 F:\ Recycling Bin

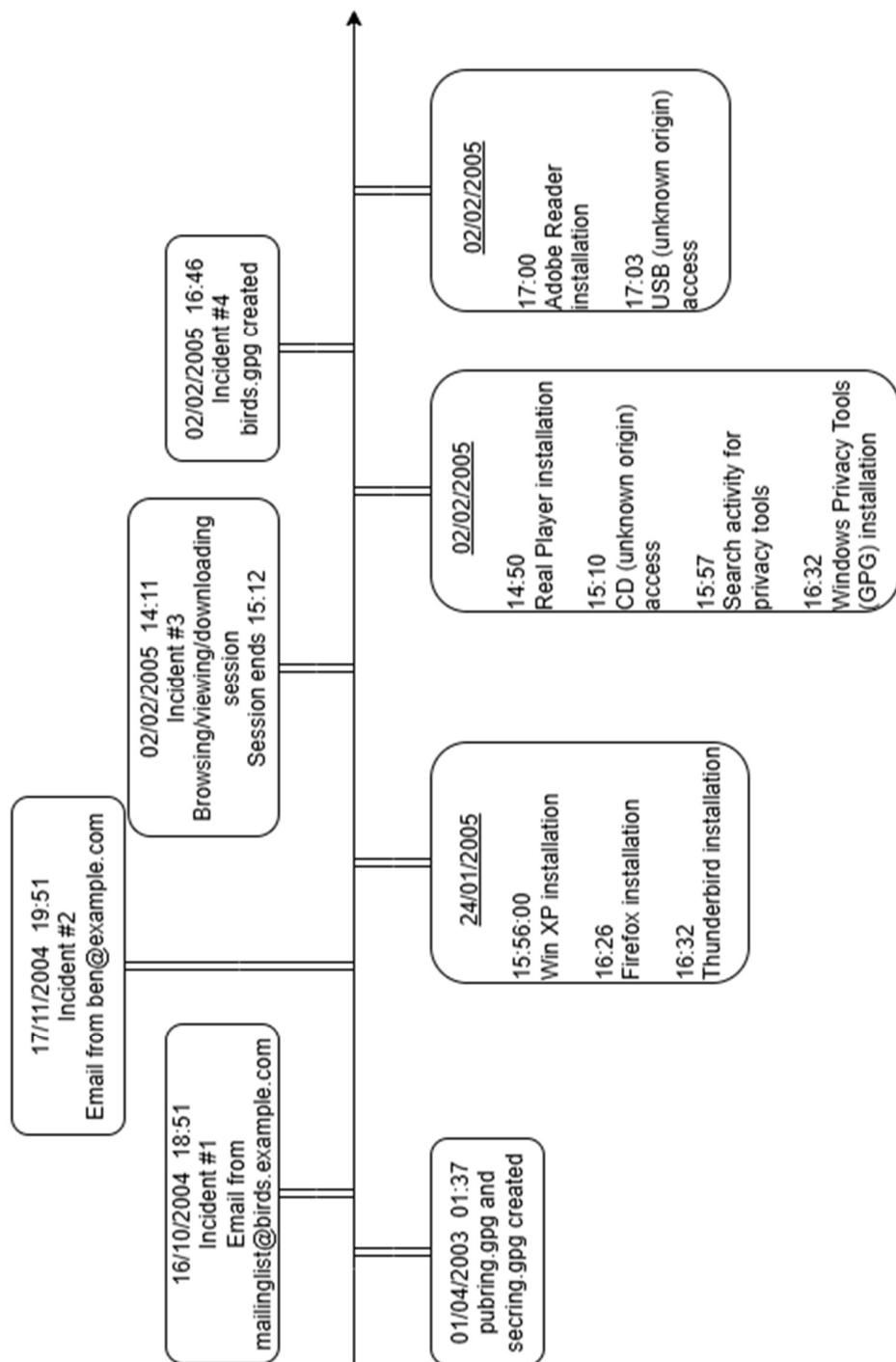
The screenshot shows the Autopsy 4.21.0 interface. The left sidebar displays 'Data Sources' with 'johnDoe.dd_1 Host' selected, showing its contents: 'johnDoe.dd' (containing 'vol1' (Unallocated: 0-62), 'vol2 (NTFS / exFAT (0x07): 63-6136829), 'vol3 (Unallocated: 6136830-11255327) with sub-folders '\$OrphanFiles (0)', '\$Extend (5)', '\$Unalloc (3)', 'RECYCLER (3)', and '\$-1-5-21-725345543-854245398-1202660629-1003 (5)'; and 'System Volume Information (5)' and '\$CarvedFiles (1)'). Other options in the sidebar include 'File Views', 'Data Artifacts', 'Analysis Results', 'OS Accounts', 'Tags', 'Score', and 'Reports'. The main pane shows a 'Listing' table with the following data:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
[current folder]				2005-02-03 15:43:48 GMT	2005-02-03 15:43:48 GMT	2005-02-09 16:51:22 GMT	2005-02-03 11:50:22 GMT
[parent folder]				2005-02-03 11:50:22 GMT	2005-02-03 14:43:34 GMT	2005-02-09 16:51:21 GMT	2005-02-03 11:50:22 GMT
desktop.ini	6			2005-02-03 14:43:34 GMT	2005-02-03 14:43:34 GMT	2005-02-09 16:51:21 GMT	2005-02-03 11:50:22 GMT
Df1.jpg	3			2005-02-02 16:25:10 GMT	2005-02-03 15:43:48 GMT	2005-02-09 16:51:22 GMT	2005-02-03 11:42:20 GMT
INFO2	2			2005-02-09 17:09:26 GMT	2005-02-09 17:09:26 GMT	2005-02-09 17:09:26 GMT	2005-02-03 11:50:22 GMT

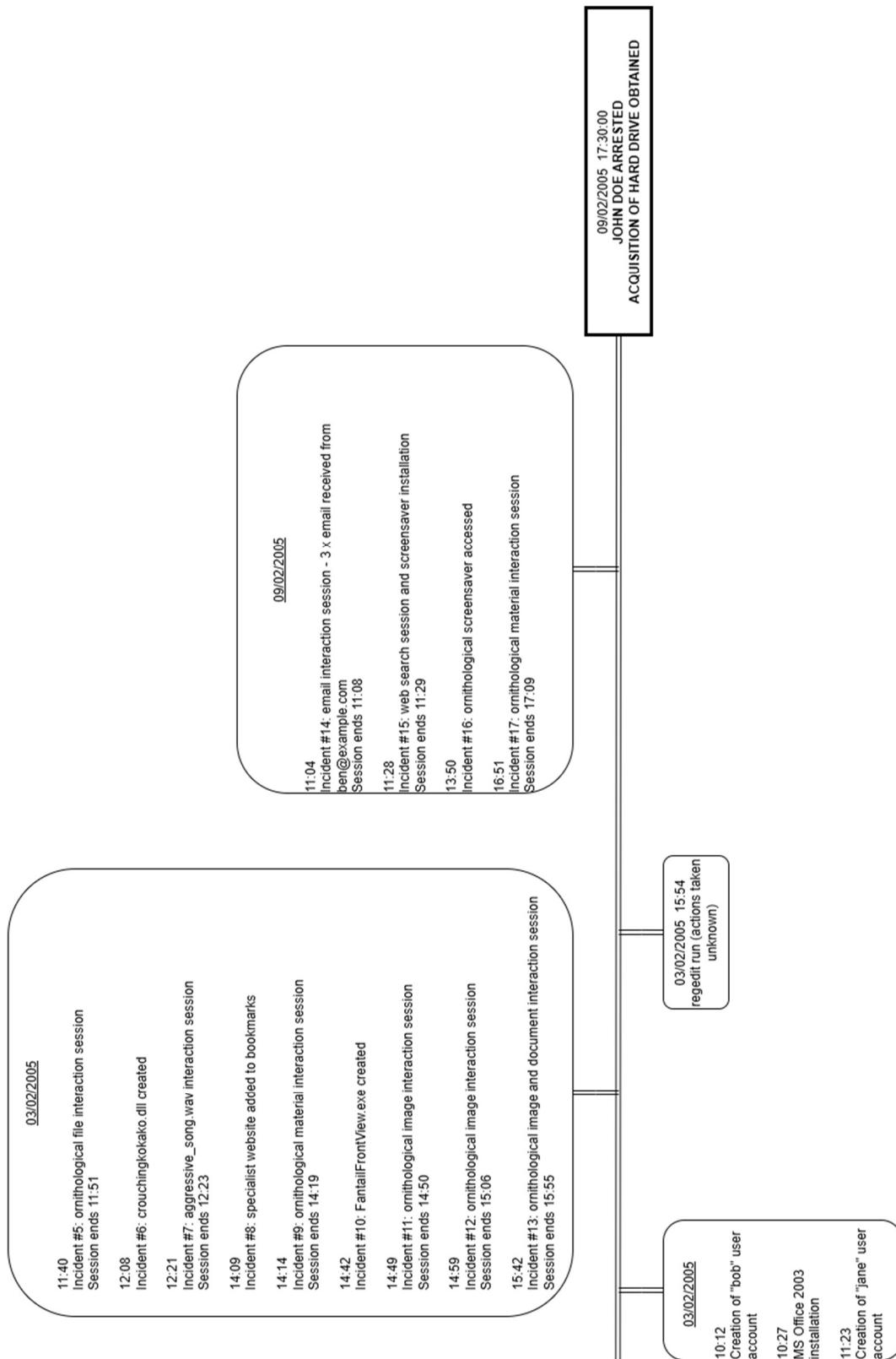
Below the table, the 'Hex' tab of the file viewer is active, showing the file content: F:\blue_bird2.jpg, P:, F:\blue_bird2.jpg.

APPENDIX J - GRAPHICAL REPRESENTATION OF TIMELINE

Part 1 - 01/04/03 - 02/02/05



Part 1 - 03/02/03 - 09/02/05



APPENDIX K - GLOSSARY

.dll file	Compiled library of functions, data, and other resources needed by Windows programs
.doc file	Microsoft Word document file format
.exe file	Executable file format
.gif file	Image file format
.pdf file	Adobe Reader document file format
.scr file	Screen saver file format
.wav file	Audio file format
Absent file extension	A file with no file extension specified
Accessed time	Most recent time that a file has been opened
Acquisition	Practice of forensically copying a hard drive/storage device for analysis
Antivirus	Utility used for scanning and removing malicious content from a computer
Archive (.zip) file	File format that enables the compression of data and can combine multiple files into a single file archive
Autopsy (forensic tool)	Open-source digital forensics platform for device and file system analysis
Bookmark	Saved shortcut to a specific webpage
Carved files	Damaged file that has been recovered from its fragments
CD drive	Drive for reading CDs, a form of removable media
CLI (Command Line Interface)	User interface that runs exclusively from a command line (text-based)
Clock skew	The difference in time between two active clock elements in a system e.g. the BIOS and the Windows operating system
Cloud	Resource on a computer not physically accessible by a user. Can only be accessed through the internet
Commenting	Human-readable notes contained within program source code. Any data added to the file as a comment is ignored by the program that uses the file
Cookie(s)	Small amount of data generated by a website and saved by a web browser. Contains information specific to the user that accessed the webpage in that particular browser
DNS	Services to enable the use of memorable names for websites and other internet-based services
Domain	Network under corporate control
Download log	Record of files downloaded within a browser
Drive	Computer component used to store data
E-mail header	Hidden section of an e-mail containing technical details about the message
Encryption	Process of converting data into an unrecognisable format. Used to transmit sensitive information ensuring that only authorised persons can access the data
Epoch time	Method for representing dates and times
Executable file	File that contains a program that can run on a computer

File compression	Process of reducing the size of a file to remove redundant data
File decompression	Process of restoring a compressed file to its original state
File extension	Suffix attached to a file indicating the file type. Windows systems are not able to open files without an appropriate file extension
File header	Small amount of information at the beginning of a file that defines the content of the file and lists file attributes
Firefox	Internet browser software by Mozilla
Floppy disk drive	Drive for reading floppy disks, a form of removable media
GUI (Graphical User Interface)	User interface that includes graphical elements. Microsoft Windows XP is an example of a GUI operating system
Hash(ing)	Used to create checksums, validating the integrity of a file. If the hash of two files matches, the two files are identical
Hex editing	Changing the binary data that makes up a computer file
history.dat	One of the internet history files for Internet Explorer
ILOB	Inappropriate Images of Birds
Image (of a PC/disk)	Result of an acquisition - the forensic copy of a hard drive/storage device
Inbox	Default folder within an e-mail account for receiving e-mail messages
index.dat	Database file that stores information about user activity
INFO2 file	Stores metadata about deleted files
Internet cache	Temporary storage area that saves copies of information accessed on the internet
Internet history	Set of files and folders holding information about a user's browsing history
Local settings	Settings that are specific to a profile on a specific computer
MD5	Hashing algorithm
Mismatched extension	file Mismatch between a file extension and the file headers of a file (e.g. a file has a file header indicating it is a .jpg file but has a name ending in ".bmp")
Mounting	Process of activating a volume on a drive, making it accessible to the operating system
Notepad	Graphical text editor installed on Windows systems
NT hash	Hashing algorithm used to obfuscate Windows login passwords
NTUSER.DAT	File for storing user-specific preferences and settings. Used by the registry
ODBC.INI	Configuration file storing information about data sources
Operating system	Software that controls a computer's core functions
Orphaned files	File stored on a computer but no longer associated with an application or process
Prefetch	Performance improving technique used by computer systems to load programs quicker by using cached data
Private key	Cryptographic key used to encrypt and decrypt messages. The private key is used to encrypt data before sending the encrypted data to an authorised person
Proxy	Intermediary server through which other computers access the internet

Public key	Cryptographic key used to encrypt and decrypt messages. The public key can be provided to recipients of data that has been encrypted with the sender's private key
RAM (.ram) file	Proprietary audio format developed for use with RealPlayer
Recent (documents)	Directory that holds information about recently opened documents
Recycling bin	Area on the hard drive where files are placed before being fully deleted
Registry	Database of settings used by Windows operating systems
Registry hive	A purpose-specific collection of settings within the registry
Registry key	Individual setting within the registry
SAM hive	Group of registry keys that stores user login information
Security patches	Software update that fixes security vulnerabilities in a program or operating system
Server Response	Action taken by a server in response to a request from a client (web browser)
Shadow copy (of a registry)	Snapshot of the registry duplicating the data held by the registry at a specific point in time
software hive	Group of registry keys that stores important software information
SpywareRemove.com	Security research centre providing information on spyware and malware
SQLite file	Single file that contains an entire database
Steganography	Technique for hiding data within a message or file. Similar to encryption
System drive	Storage area on a hard drive where the operating system files are stored
system hive	Group of registry keys that stores important system information
Temp directory	Folder for storing temporary data. Usually emptied automatically on a schedule
Thunderbird	E-mail client by Mozilla
Timestamp	Specific date and time added to a file showing creation, access, and modification times
Trojan (horse)	Software that masquerades as legitimate software but contains a malicious program
Unallocated space	Portion of storage that has not been assigned within a computer. May appear empty yet contain data
Unmount	Process of deactivating a disk volume. Once unmounted, the operating system is no longer able to access any data held on the volume
URL	Address of a specific webpage or file
USB drive	Storage device that can be connected to a computer using a USB connection
User profile	Collection of data, information, preferences and settings for a particular user on a system
UserAssist key	Registry key that records which programs have been run by a user, when, and how often
Users folder	Directory containing all the user profiles for a computer
Virtual machine	Computer that runs as software on another physical computer
VirusTotal	Online platform that analyses files and URLs for malicious content

Volume	Section of a storage device or a specific storage area
Wayback Machine	Digital archive of the World Wide Web allowing users to view past versions of websites
Windows Updates	Microsoft service that automates the downloading and installation of Microsoft update files

APPENDIX L - LIST OF EVIDENTIARY FILES WITH MD5 HASHES

MD5 hash for johndoe.dd: d63dd1b8917ca28bac7c955fc3b6cd25

File name	File type	Reference	Appendix	MD5 hash
0E47C6DFd01	Image (partial)	20.1	A	596368518f3c4afc85e08fd03e97bd72
177.jpg	Image	12.5	A	ac192837bda3a7b224fd259ddad99be5
40m.jpg	Image	3.7	A	b4f567dead60a8292931e12ead7911c9
5C1E7D60d01	Image	20.2	A	83a171d89d6476445fa3e3adca06854c
5E5570B4d01	Image	20.3	A	fe1f3a53e513da312f6e03768cd7db4a
7107298.jpg	Image	3.6	A	f095a5eee85aa81de775e45e481bab94
7EYBTELF1KAN.jpg	Image	14.3	A	87cfa58be4bdc094db96d9f94d2905e5
aa010703a.htm	Saved web page	3.9	B	4ab04de423f60bc5e2ff230b5a4f9ced
Aggressive_song.wav	Audio	N/A	N/A	87e0a9e129a8c887458a2f5d2af7aebe
AlmondMarshGreatBlueHeronStalling.jpg	Image	5.1	A	ed2b7f661974455399f9d083f01c19fe
AmericanAvocetWithPlumage.jpg	Image	5.3	A	7addf538b2781a0d44d2ef0d4649e680
AmericanWhitePelicansCircling.jpg	Image	5.4	A	9e637c4b39b94f2eb72a8ebc81684652
babyscot_2weeks.jpg	Image	12.3	A	c14916d4a3c790e80e65232dc8e9a707
babyscot_vyoung.jpg	Image	12.4	A	e3273c1494f601e2e4378580ca76a1ec
BaldEagle7oClock.jpg	Image	5.2	A	7c3be8176820e88dcb1f89f6d2ddbab5
BarnOwl.jpg	Image	5.6	A	35c82564737216998e3d051f286bb728
BC7 feeding the birds.jpg	Image	14.8	A	f23c5e544e08726e9228ca915882976f
BellbirdJumpingOffBranch.jpg	Image	5.5	A	44d0a2dc29c52a8656bd4bdcb12d794c
BF5BE9D9d01	Image	20.4	A	ff0ace5e6f7f467f9c0bf9f840f5d561
birdpics.gpg	Encrypted file	N/A	N/A	11e7a23a9422ecc0b2a5f39c3f388f5b
birdpics.zip	Archive	N/A	N/A	0a4f6220a8abedac1ac8641c3bc38166
birdtrans2.jpg	Image	12.6	A	25f12c1dbb64575b56a92bdcadc88ade
birdwatching.doc	Document	13.7	B	c6108e60db66aa588543657c4f656847
BlackNeckedStiltsFromBehind.jpg	Image	5.7	A	e08381661fdb2f06e0c15b599dcad571
BlackSwan.jpg	Image	5.8	A	64302e831dc5ddb8c9a0e75781d5c76f
BlackVultureSunningOnPost.jpg	Image	5.9	A	6257f2b469c8820c6a8cf7703b9dd7c8
blue_bird2.jpg	Image	5.10	A	91e2843f48162ac7a12a777d5e4226f5
bookmarks.html	Firefox bookmarks	3.16 8.1	E	9e1e34b2b5daa52c476c3d8220f41c07
brd_Ornithologist_TWG.jpg	Image	5.11	A	beaaaf73518d8e49e58f116fb834f537
brd_WoodDuck.jpg	Image	6.1	A	296531879159ce77999f1c8af6d1e92a
Brolga.jpg	Image	6.2	A	e44460b1be9072794611dbdd64d319c9
BrushTurkeyPerching.jpg	Image	6.3	A	55bd5a13fd9663b481bce7f066cbb32c
Cache (directory)	Firefox cache	15.3	F	N/A

CanadaGoose.jpg	Image	6.4	A	b7a84aa1ed0763fbeb8d52b386c3d13e
CanadaGooseWashing.jpg	Image	6.5	A	7cace0aee77031856c1dc628b4c0c826
ChestnutMandibledToucan.jpg	Image	6.6	A	db5480ccb1dbbad7ad245629c0fa80e0
chicks2.jpg	Image	12.8	A	5b3fa4e2e40a5b50e7563612725e19ea
colorful-birds.jpg	Image	14.5	A	b1e81a55793382729364646680d51010
CrouchingKokako.dll	Archive	N/A	N/A	b945f685ea4d7e6b3882ed7cb61e7830
CrouchingKokako.jpg	Image	6.7	A	fa463d5035f0ed111ac59c7f8856d404
cute_penguin.jpg	Image	14.4	A	915b8be5369cccd6b7cc1278eed00b413
dawn.ram	Audio	N/A	N/A	64f24a34376b201e8823cff99fea1b41
Doc1.doc	Document	9.6	B	9860f16826698f3c38f7486b16aa5e2e
downloads.rdf	Firefox downloads	3.15 7.2 12.11 15.4	E	a98744e309dec5b86407f0e2ba29e179
f0005672_Related_Articles.html	Web page	19.25	B	e17c68d2f5d1053b8774a702b7bb7dbe
f0033288.html	Web page	19.26	B	78d676ce04fc12abc49be640b490c6e4
f0033912.jpg	Image	19.7	A	880b9bafbd139aafb30fb2ecdf373d7
f0033928.jpg	Image	19.17	A	c8556706fc11c2a717f49ee20c1e3292
f0041304.html	Web page	19.27	B	9613c2658998a4b7eb96e48c813efea1
f0045880.jpg	Image	19.3	A	502bd8d15da3091618ac3cf483bd1654
f0056920.jpg	Image	19.1	A	9e43274bd8374867674f15ffa67be052
f0056936.jpg	Image	19.23	A	b12a067c033a94b290f89a733f6ca72a
f0056944.jpg	Image	19.9	A	aea86094a7a46fa0b8ff889e9da32ef9
f0056952.jpg	Image	19.10	A	dcf99efec7a00d28ed11c8923eb96e95
f0056976.jpg	Image	19.4	A	65f9489e302828bbf65639075646a1ec
f0180344.pdf	Document	19.28	B	26a49cca77de541139f5ab718d672e99
f0201904.html	Web page	18.19	B	11e1f3c817b17d312225408cf0924931
f0273688_Newsletter_Win_2001_q.pdf	Document	19.29	B	1dd4549c1e514f35551449176fb0d82a
f0310480.jpg	Image	19.8	A	2ebf36f3124138f584112ddc07e5118b
f0327896.pdf	Document	19.30	B	a717b5167cde89d2ffb520b4d85b2233
f0345656.jpg	Image	19.13	A	a47d625cba6895455d099442bad55a3c
f0360392.jpg	Image	19.24	A	37d60053d5e9336516887a24bc735edc
f0382464.jpg	Image	19.21	A	041a23c317560764d11f1003dc82e2f
f0387624.jpg	Image	19.16	A	7bc7bee527e4bed1af3f00d328824d27
f0415008.jpg	Image	19.5	A	cfffb68753718298750d0b5b130e9c372
f0416072.jpg	Image	19.20	A	884104db790c715174c2ceffff97546
f0438640.jpg	Image	19.2	A	84ab7a6f4f27a1e8b93433e5b279e68c
f0439400.jpg	Image	19.22	A	056347a7d67d714fb535c01b9667c4cf
f0441536.jpg	Image	19.6	A	5ad002eddc616855099b47323c463a98
f0443520.jpg	Image	19.12	A	6ec584061dc3fc527b2d5d419a696c94
f0464568.jpg	Image	19.19	A	c8bde2f6fcf8d842d503968504872db3
f0493176.jpg	Image	19.11	A	66b5167365db72e85039c52b85ff90c7
f0496112.html	Web page	18.20	B	bdbfb2f705953b7a7f7bcba4dc86917e
f0526960.jpg	Image	19.15	A	b887686b7bfa6e4da155ef302a3e04b7
f0533600.jpg	Image	19.18	A	448697f1928ebc380f619d8e061ae04e

f0592136.jpg	Image	19.14	A	65cd3c59f03ab229bd34c3a20d8bf43a
FantailFrontView.exe	Image	10.1	A	864459aedb0450e30cf384c81d470153
FB4EDA00d01	Image	20.5	A	5ff1ada80635ebc04f5722a88e4f4d9d
Firefox wallpaper.bmp	Image	3.3	A	c57ffe125adaa520c26be8a410ba9421
frankbeecostume_1827_34457581	Image	13.1	A	210527d0c5ff1214b78f95a72b49f512
frankbeecostume_1827_84985892	Image	13.2	A	75d03c25d9397282689016b0a3d7bbc5
frankbeecostume_1827_96360352	Image	13.3	A	7dc714fe905bafbcaca1c333f4aa35fb
gawall8.jpg	Image	14.7	A	80bcd2179290c3e87c8505b1d1d991a5
glfs-storm- birds.jpg	Image	14.9	A	e1e504e73c0c2944fafc2f45db0ded37
GreatBlueHeron WithFish.jpg	Image	17.7	A	5db35478fd169cf7487b1a62ec872ac4
GreatEgretInVol oBog.jpg	Image	17.8	A	798a2db6f5695328bf8d116f2a76f99f
GreatEgretOverfl yingRoseateSpo onbills.jpg	Image	17.9	A	ca239de832cf2a1f6084a6939ee3d405
GreenHeronClos eup.jpg	Image	17.10	A	acbcef7efb3a148e050d6fe3340b4bd
GreenHeronOnC hicagoLakeshore .jpg	Image	17.11	A	f393ebd21e9f30d4a75e4db4bf10dc5b
guide.doc	Document	13.5	B	08c4123261ed8ebb648ba7bcf25788aa
history.dat	Firefox history	3.1, 3.2 7.1 12.1, 12.2 15.1, 15.2	E	2918ffe38ad701afb3543da42c842f3f
image0.jpg	Image	18.1	A	ca0ee720504806e4fb8d27a8b4ef4c87
image0.jpg	Image	18.2	A	d83bfed1cb6ddae3894b8e2a31421b56
image1.jpg	Image	18.3	A	df289b9b97460dc4841ef8cdff99f6e6
image1.jpg	Image	18.4	A	ae0224250379a9947ab7b0c662403634
image1.tif	Image	18.5	A	f7ff305701449584379f73ae31973959
image12.jpg	Image	18.6	A	adab3ef8244801d70550a9b6dd7378b8
image12.tif	Image	18.7	A	41de35e072b3a6104d638f58686cc0be
image14.jpg	Image	18.8	A	931ad1eaa65a63baf83feacf58bcbd3b
image15.jpg	Image	18.9	A	675ae2666d572b1a0e1e5c2e4135e659
image16.jpg	Image	18.10	A	00373ae0e2967c5458acc57f3fedff20
image2.jpg	Image	18.11	A	4e7a41349cf80f8ce4abf74aabbc5815
image26.jpg	Image	18.12	A	17a9c739e3734d10e7f43b138f9c5aa6
image3.jpg	Image	18.13	A	fb5d2adc39b4e01f638eda55200ce380
image33.jpg	Image	18.14	A	d01c67d39f700e4d264abb770cfcaa9de
image4.jpg	Image	18.15	A	f07b9ddacd6675848058af7732ff8596
image4.jpg	Image	18.16	A	122255b261e779a3659d84a5569afce4
image5.jpg	Image	18.17	A	e7e8a371afc6c15ac1502dc3b7b7046
image6.jpg	Image	18.18	A	48650701309fdf4d709d5ac7e7e5d710
IMG_3937_filtered. jpg	Image	14.6	A	7da33af8e6ba203e1a4f52f960b7151e

ImmatureSnowyEgretTakingOff.jpg	Image	17.12	A	eb09aea7a30842db52a3bb6acf23442b
Inbox	Mailbox file	1.1, 1.2 2.1, 2.2 14.1, 14.2	D	a9865bf00f6e97f613834dc445c60d78
index.dat	IE history	3.8 7.3 9.1, 9.8 11.1 12.12 13.8	F	9b694700c19e90658824ff23db1f961f
INFO2	Recycler info	13.4	I	55c0ed33d7b695991d65d8667d545673
june03screen.jpg	Image	17.17	A	26ea3ed3b63821dd6ed5d0828696d741
junescreen01.jpg	Image	17.18	A	b86ddb90a6902c83c0e516d0aaa32f31
kakapo.ram	Audio	N/A	N/A	836112e9d5fc24471923a5016364ef20
KeaAndMountain.jpg	Image	17.13	A	a46cef1fd7b9735372e7fa07d5f05457
KeaAtTopOfMacKinnonPass0930.jpg	Image	17.14	A	6070cdc8e0c059ad72fd782ac8b7f161
KeaEatingRentalCar.jpg	Image	17.15	A	3db5fb16b446ea0e92447cf6399709e9
KeaRetrievingBakedBeanCanFromTarn.jpg	Image	17.16	A	cc51364cd95f021f7422ab2a219966ef
nestboxtips.txt	Text document	3.10	B	333fc58042a410d453c22984c4b55e3d
newbies2.jpg	Image	12.7	A	a2ef1f75882f955a1e41b77e8a593a0e
NTUSER.DAT	Registry hive	3.11 4.6 7.4 9.4, 9.13 10.2 11.4 12.15 13.11 17.5, 17.22	F	282ac586e5e25bb72f51836e717f5249
ODBC.INI	System file	13.15	B	e30b740ff551da8061405499ae9ad8c9
ostbk2b2.htm	Web page	12.10	B	b8dc8422fe0551e1c1eca78f99e7b9c9
ready2fledge.jpg	Image	12.9	A	25ba487aeb9ae11a3adb64e4fb32414b
snow_geese.jpg	Image	3.5	A	55cc22374ddd67183a02b2b17d343386
stuf.doc	Document	17.1, 17.2	B	c8873d36266916c20bd2f3ebb89a800e
system	Registry hive	4.8 5.12	F	0dbe3b9ca1dbf85794063edef5c04884
THUNDE~1.EXE-2874618F_pf	Prefetch file	14.10	H	d5f3ca830a04d80a99cfea8098133556
tn_duck_3.jpg	Image	3.4	A	526e5d096bbfc21f593dd2f0b5bcfd6e
tx_birds.dat	System file	N/A	N/A	b3d22a483875a61cb2060c7d518effc2
tx_birds.dll	System file	N/A	N/A	0409b45f5f6eec43651dd7a62bb6d5d1

tx_birds.exe	Executable file	N/A	N/A	178928fc03e3c6ee8ab686e81844f957
TX_BIRDS.EXE-24B103EC(pf	Prefetch file	16.1	H	fe71abf3fbb7d2f89ffb9869907db2f1
TX_BIRDS.EXE-2861E2BC(pf	Prefetch file	15.7	H	74a76bde8b187d319de205db092ceccc
tx_birds.scr	Screensaver file	N/A	N/A	a6d2f96e533d293726ac17116b610875
TX_BIRDS.SCR-03FEBFC4(pf	Prefetch file	16.1	H	cb818dab272ae89f9da928973a3513cc
WhiteFacedHeron Flying.jpg	Image	4.1	A	b32e0bec9e1c301cf826d4ef5a13d7c
WhiteFrontedParr ot.jpg	Image	4.2	A	501dfcb0677fe10e7cbd4e25373c23b1
WhiteThroatedSparrowInTree.jpg	Image	4.3	A	ae5099b0789f67b971e846ea3be71cef
WhoopingCranes.jpg	Image	4.4	A	4d2c8828ae6ec294c9a234dc81d7adab
yellow-wag-cover-nb.jpg	Image	4.5	A	a3695fa7e971d3583083002107faa650

APPENDIX M - LIST OF SOFTWARE/TOOLS USED TO CONDUCT ANALYSIS

Tool/software name	Purpose	Version
7Zip	Decompression of image file	22.01
Autopsy	Platform for evidence analysis/extraction	4.21.0
chmod	Set files to read-only (Kali virtual machine)	9.4
clamscan	Antivirus scanner	1.4.1/27427
cp	Copying of files from the mounted image	9.4
Event Viewer	Viewing Event Log files	1.0
fdisk	Enumeration of partition table	2.40.2
find	Locating files of potential interest in image	4.10.0
Firefox	Viewing of Firefox bookmarks and download data	132.0
fsstat	Enumeration of image operating system	TSK versioning
Google Chrome	Browser to access cloud storage	129.0.6668.58
gpg	Tool for encrypting/decrypting files	2.2.4
gpg2john	John the Ripper feature for processing GPG private keys	John versioning
HashCalc	MD5 hash calculation (Windows 11 laptop)	2.02.00337
ImportExportTools NG	Thunderbird add-on for importing profile folders	14.1.2
jar	Used to extract images from bird.zip	17.0.13
John the Ripper	Password cracking tool	1.9.0-jumbo-1+bleeding-aec1328d6c
Kali (Linux)	Hosting of CLI tools	6.10.9-amd64
losetup	Tool for mounting image file	2.40.2
md5sum	MD5 hash calculation (Kali virtual machine)	9.4
Microsoft Excel	Comparison of hash values to identify unique files	2409
mmls	Enumeration of disk size	The Sleuth Kit (TSK) 4.12.1
Mount	Attaching image file to a mount point	2.40.2
MZCacheView	Viewing of Firefox cache data	2.22
MZCookiesView	Viewing of Firefox cookies data	1.6
MZHistoryView	Viewing of Firefox history data	1.7
Notepad++	Inspection of pagefile.sys content	8.7
Oracle Virtual Box	Hosting of kali virtual machine	7.0.20 r163906
parted	Enumeration of free disk space	3.6
Pasco	Extraction of data from Internet Explorer cache, history, and cookies files	1
Registry Viewer	Graphical tool for registry analysis	2.0.0.7
sudo	Builtin Linux tool required to use some tools	1.9.15p5

Thunderbird	E-mail client	128.2.0esr
Windows 11	Hosting of GUI tools	23H2 22631.4169
WinPrefetchView	Viewing of prefetch files	1.37