John Doe Case: Court Report

Ben Gilmour, Mairi McQueer, Sam Heney

January 22, 2022

Contents

1 Job Description and Instructions

In this case the analysts collected hardware belonging to the suspect named ”John Doe” who is accused of possessing illicit images of birds. The analysts; Sam Heney, Mairi McQueer and Ben Gilmour, were tasked with investigating the device to locate and present any files or information that may be incriminating. The methodology and results of such are detailed in the following sections. The analysts have some experience in this field from a Digital Forensics module taken as a part of a Bachelor of science degree in Ethical Hacking.

2 Description of Recovered / Examined Physical Evidence

2.1 John Doe's Hard Drive

The Hard Drive Disk (HDD) acquired was 5.4 Gigabytes (GB), with the primary partition(NTFS/exFAT) being 2.9 GB in size. The items recovered are labelled as 'Devices C, E and F'.

Device C Being the primary partition contains the vast majority of the files that were uncovered as well as the Operating System (OS) for John Doe's computer.

Device E A removable drive. Evidence of this drive was discovered, but the analysis team did not have access to this drive.

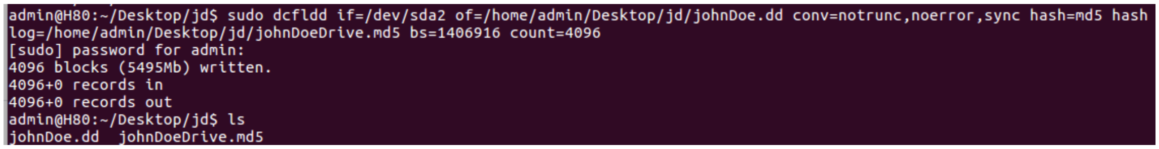
Device F A deleted partition, which contained a large collection of illicit files which will be presented later in the document.

3 Analysis Methodology

3.1 Disk imaging

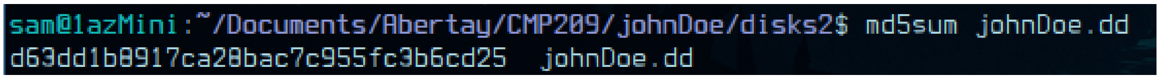
In order to preserve the data on the original, physical HDD retrieved from ”John Doe’s” hardware, disk images were created, so that none of the evidence on the original HDD will be tampered with or altered. Initially when the HDD was given to the analysts to investigate, their first step was to create a number of disk images.

An image was created using the following steps; first was connecting the suspect drive to a computer in the analysis lab, ensuring the disk permissions were read-only as to keep the integrity of the evidence, so the original was not changed in any form. Then dcfldd was used to make an image of the disk and then md5sum calculated the MD5 hash of the original image. Finally the integrity of the copy was verified by comparing the hashes of the original to the new image. The output of the commands are shown in the following figures.



```
admin@H80:~/Desktop/jd$ sudo dcfldd if=/dev/sda2 of=/home/admin/Desktop/jd/johnDoe.dd conv=notrunc,noerror,sync hash=md5 hash
log=/home/admin/Desktop/jd/johnDoeDrive.md5 bs=1406916 count=4096
[sudo] password for admin:
4096 blocks (5495Mb) written.
4096+0 records in
4096+0 records out
admin@H80:~/Desktop/jd$ ls
johnDoe.dd  johnDoeDrive.md5
```

Figure 1: Creating the disk image of the Hard Drive Disk



```
sam@1azMini:~/Documents/Abertay/CMP209/johnDoe/disks2$ md5sum johnDoe.dd
d63dd1b8917ca28bac7c955fc3b6cd25  johnDoe.dd
```

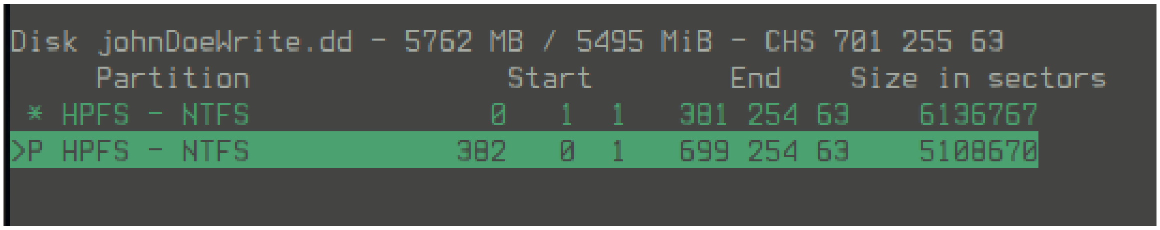
Figure 2: MD5 hash of John Doe disk image

3.2 Physical Searching

Physical searching is treating the whole disk image as a file while searching for data. This reveals deleted files and file segments that have been partially overwritten in memory.

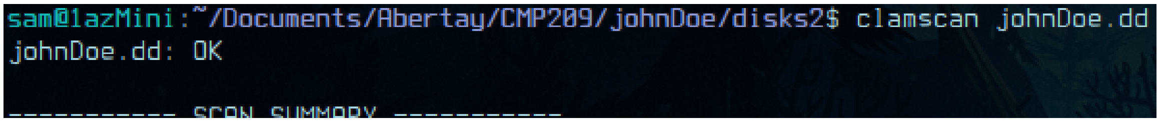
3.2.1 Disk Analysis

First the investigators decided to run clamscan in order to check for any viruses or infected files. The Sleuthkit mmls and img_stat commands identified the partitions as well as the disk image file size and type, as seen in the figure five. As there was a few Kilobytes (KB) of unallocated space after the recovered partition, so the investigators decided to use Hexdump to reveal any bytes that may indicate a hidden file. As there was also an unallocated partition fsstat was ran, in order to gather any information that could be determined from it. *(Figure 5)* Then the software TestDisk was used in order to retrieve the deleted partition so the investigators could examine the contents. *(Figure 3)* Foremost, was used to search for bit patterns and identify specific patterns that match different file types, allow the viewing of the file metadata and searching for specific file types. On the deleted partition was a encrypted file



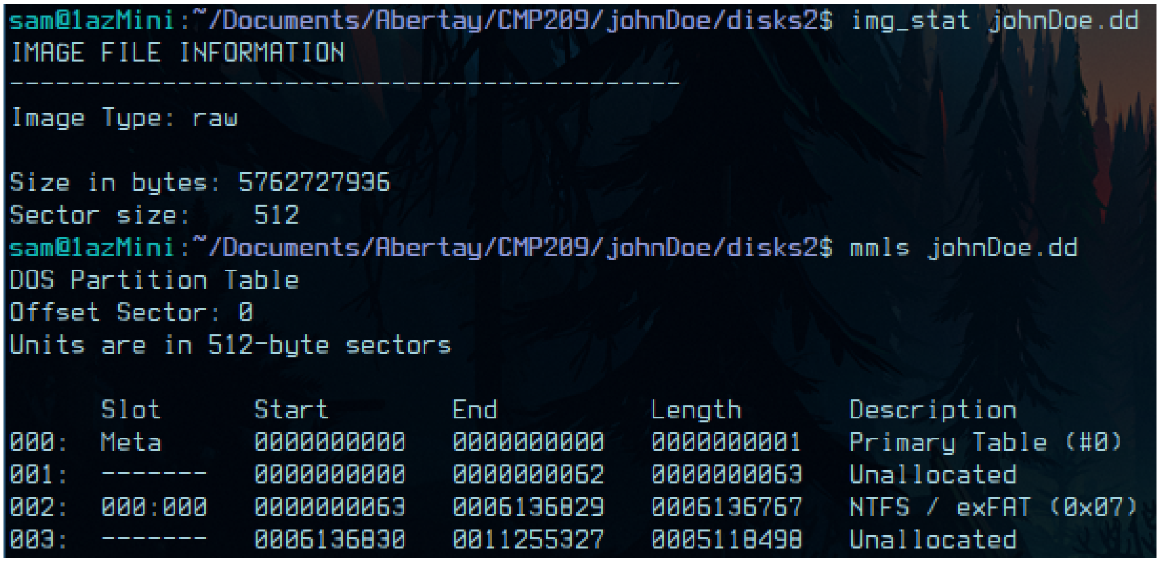
```
Disk johnDoeWrite.dd - 5762 MB / 5495 MiB - CHS 701 255 63
     Partition                  Start        End    Size in sectors
 * HPFS - NTFS                0   1  1   381 254 63    6136767
>P HPFS - NTFS              382   0  1   699 254 63    5108670
```

Figure 3: Testdisk retrieving deleted partition



```
sam@1azMini:~/Documents/Abertay/CMP209/johnDoe/disks2$ clamscan johnDoe.dd
johnDoe.dd: OK

----------- SCAN SUMMARY -----------
```

Figure 4: Clamscan on John Doe disk image

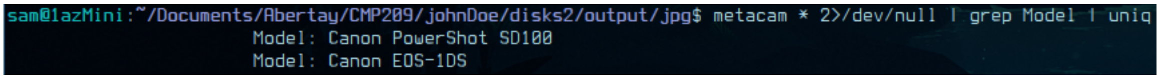


```
sam@1azMini:~/Documents/Abertay/CMP209/johnDoe/disks2$ img_stat johnDoe.dd
IMAGE FILE INFORMATION
--------------------------------------------
Image Type: raw

Size in bytes: 5762727936
Sector size:    512
sam@1azMini:~/Documents/Abertay/CMP209/johnDoe/disks2$ 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:  -------   0006136830   0011255327   0005118498   Unallocated
```

Figure 5: Sleuthkit commands on John Doe disk image

3.2.2 Images

Once images were found from the Foremost search, Metacam was used to display the metadata of each image. This is information about the image stored within the image itself, such as the camera used to take the photo, GPS coordinates of where the photo was taken, the time the photo was taken etc. This metadata was used for a number of operations; Firstly, Grep which searches for patterns in files was used to find if there was information about the cameras that took the photos, seen at *(Figure 6)*. Then another grep command was used to find the images taken by the discovered cameras and copy them to a folder.



```
sam@1azMini:~/Documents/Abertay/CMP209/johnDoe/disks2/output/jpg$ metacam * 2>/dev/null | grep Model | uniq
                        Model: Canon PowerShot SD100
                        Model: Canon EOS-1DS
```

Figure 6: Using Metacam and grep to locate camera data

3.3 Prefetch Analysis

Windows, in order to load commonly used programs faster, keeps a record of all programs that have been run recently. This can be used by the investigators to see what programs have been run by the user. Each file represents the running of a program. There can be multiple files for the same executable if it was moved and run from a different location.

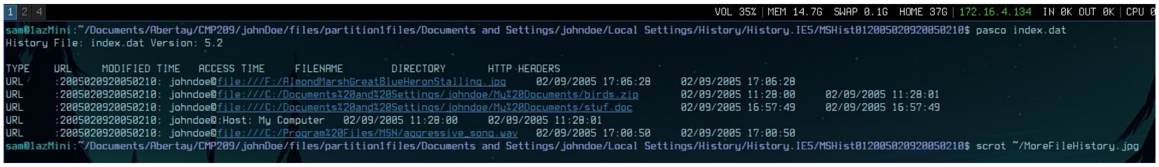
The time that these files were created is also useful for building a timeline of events, seeing as they are created at the last time the program was run.

3.4 Registry Examination

Then the analysts examined entries in the registry that relate to; the users on the machine, the devices that have been connected to it, what networks it has been connected to, last write times of files and log files that the machine itself created automatically. Anything that the machine automatically logs is called ”accidental evidence” as the creation of it has not been purposeful by the user.

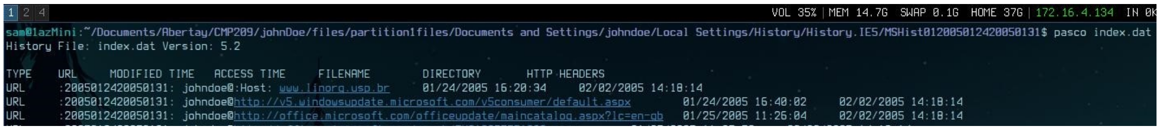
3.5 Browser Analysis

In order to search the file and web histories the tool Pasco was used to search the index.dat files from the browser, in this case the browser was Mozilla Firefox. *(Figures 8 & 9)*


1 2 4
VOL 35% | MEM 14.7G SWAP 0.1G HOME 37G | 172.16.4.134 IN 0K OUT 0K | CPU 0

```
sam@1azMini:~/Documents/Abertay/CMP209/johnDoe/files/partition1files/Documents and Settings/johndoe/Local Settings/History/History.IE5/MSHist012005020920050210$ pasco index.dat
History File: index.dat Version: 5.2

TYPE    URL     MODIFIED TIME   ACCESS TIME     FILENAME        DIRECTORY       HTTP HEADERS
URL     :2005020920050210: johndoe@file:///F:/AlmondMarshGreatBlueHeronStalling.jpg     02/09/2005 17:06:28     02/09/2005 17:06:28
URL     :2005020920050210: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/birds.zip       02/09/2005 11:28:00     02/09/2005 11:28:01
URL     :2005020920050210: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/stuf.doc        02/09/2005 16:57:49     02/09/2005 16:57:49
URL     :2005020920050210: johndoe@:Host: My Computer   02/09/2005 11:28:00     02/09/2005 11:28:01
URL     :2005020920050210: johndoe@file:///C:/Program%20Files/MSN/aggressive_song.wav   02/09/2005 17:00:50     02/09/2005 17:00:50
sam@1azMini:~/Documents/Abertay/CMP209/johnDoe/files/partition1files/Documents and Settings/johndoe/Local Settings/History/History.IE5/MSHist012005020920050210$ scrot ~/MoreFileHistory.jpg
```

Figure 7: File history index.dat

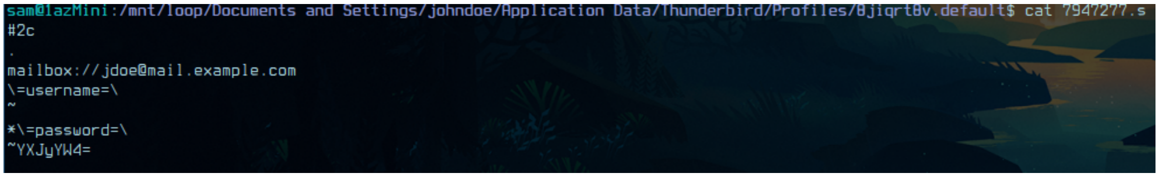


```
sam@1azMini:~/Documents/Abertay/CMP209/johnDoe/files/partition1files/Documents and Settings/johndoe/Local Settings/History/History.IE5/MSHist012005012420050131$ pasco index.dat
History File: index.dat Version: 5.2

TYPE    URL     MODIFIED TIME   ACCESS TIME     FILENAME        DIRECTORY       HTTP HEADERS
URL     :2005012420050131: johndoe@:Host: www.linorg.usp.br     01/24/2005 16:20:34     02/02/2005 14:18:14
URL     :2005012420050131: johndoe@http://v5.windowsupdate.microsoft.com/v5consumer/default.aspx        01/24/2005 16:40:02     02/02/2005 14:18:14
URL     :2005012420050131: johndoe@http://office.microsoft.com/officeupdate/maincatalog.aspx?lc=en-gb   01/25/2005 11:26:04     02/02/2005 14:18:14
```

Figure 8: Web history index.dat

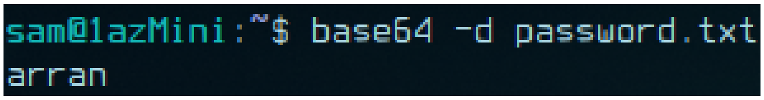
3.6 E-mail analysis

From browser analysis the analysts inferred the accused's e-mail client, Thunderbird, and from the client files their username and password were uncovered. The password was then decoded using a base64 decoder command.



```
sam@1azMini:/mnt/loop/Documents and Settings/johndoe/Application Data/Thunderbird/Profiles/8jiqrt8v.default$ cat 7947277.s
#2c
.
mailbox://jdoe@mail.example.com
\=username=\
~
*\=password=\
~YXJyYW4=
```

Figure 9: Retrieving password for jdoe@mail.example.com



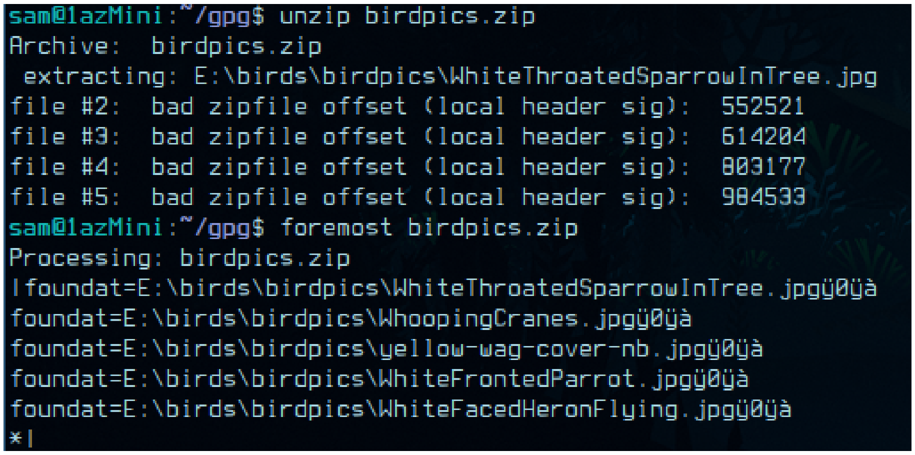
```
sam@1azMini:~$ base64 -d password.txt
arran
```

Figure 10: Decoding password for jdoe@mail.example.com

3.7 Encrypted Archive

In the main partition was a gpg encrypted file called birdpics.zip and the analysts attempted to decompress it, which unfortunately did not work.

Cryptographic keys secring.gpg and pubring.gpg were found in "Documents and Settings/johndoe/Application Data/GnuPG". The password used to decrypt the files was found earlier in the Thunderbird email client files, as the same password is used for both. Then the tool Foremost was used to recover the files. *(Figure 12)*



```
sam@1azMini:~/gpg$ unzip birdpics.zip
Archive:  birdpics.zip
 extracting: E:\birds\birdpics\WhiteThroatedSparrowInTree.jpg
file #2:  bad zipfile offset (local header sig):  552521
file #3:  bad zipfile offset (local header sig):  614204
file #4:  bad zipfile offset (local header sig):  803177
file #5:  bad zipfile offset (local header sig):  984533
sam@1azMini:~/gpg$ foremost birdpics.zip
Processing: birdpics.zip
|foundat=E:\birds\birdpics\WhiteThroatedSparrowInTree.jpgÿ0ÿà
foundat=E:\birds\birdpics\WhoopingCranes.jpgÿ0ÿà
foundat=E:\birds\birdpics\yellow-wag-cover-nb.jpgÿ0ÿà
foundat=E:\birds\birdpics\WhiteFrontedParrot.jpgÿ0ÿà
foundat=E:\birds\birdpics\WhiteFacedHeronFlying.jpgÿ0ÿà
*|
```

Figure 11: Attempting to unzip file and using Foremost on birdpics.zip

4 Analysis

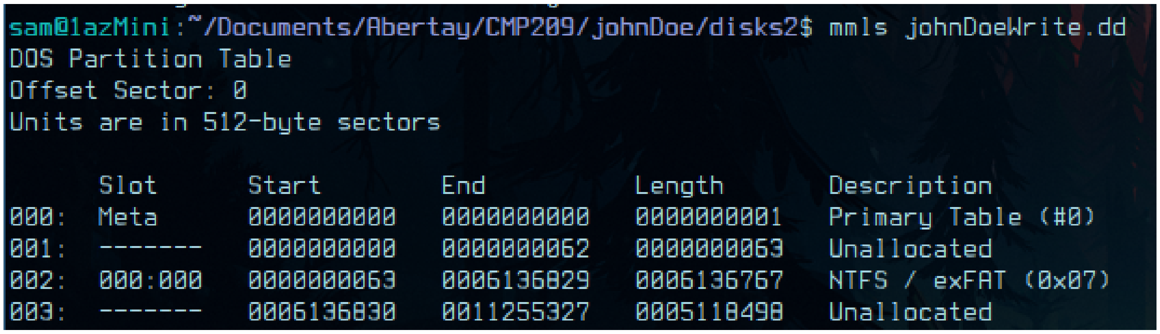
4.1 Physical Searching

4.1.1 Disk Analysis

Fsstat revealed the opperating system is Windows XP and the file system is NTFS. There was initially only one partition listed, but there was a lot of unallocated space on the HDD *(Figure 13)*. After further investigation using Testdisk *(Figure 3)*, a second partition that had been removed from the Master Boot Record (MBR) was found *(Figure 14)*.

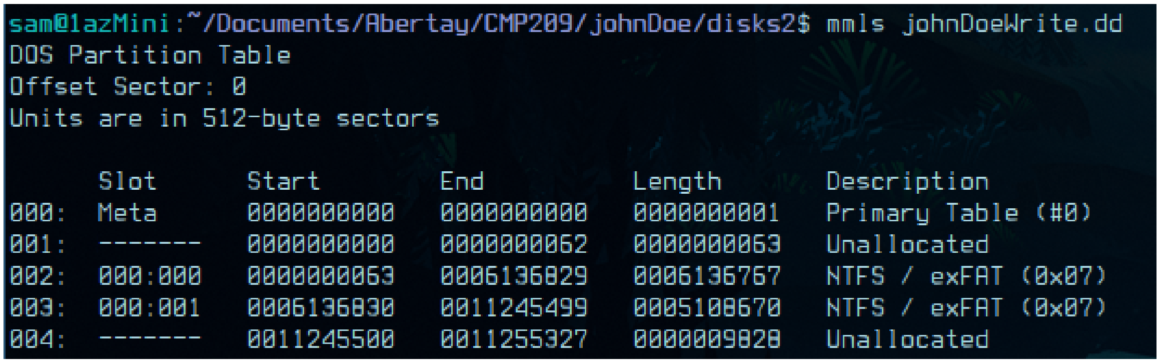
4.1.2 Summary of the partition table

- 512 bytes for the partition table
- 32.256 KB of unallocated space
- Partition 1 - 3.142GB - Main partition with a Windows XP installation
- Partition 2 - 2.62GB - Undeclared partition with bird images and birdwatching guide
- 5.032 Megabytes (MB) of unallocated space



```
sam@1azMini:~/Documents/Abertay/CMP209/johnDoe/disks2$ mmls johnDoeWrite.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:  -------   0006136830   0011255327   0005118498   Unallocated
```

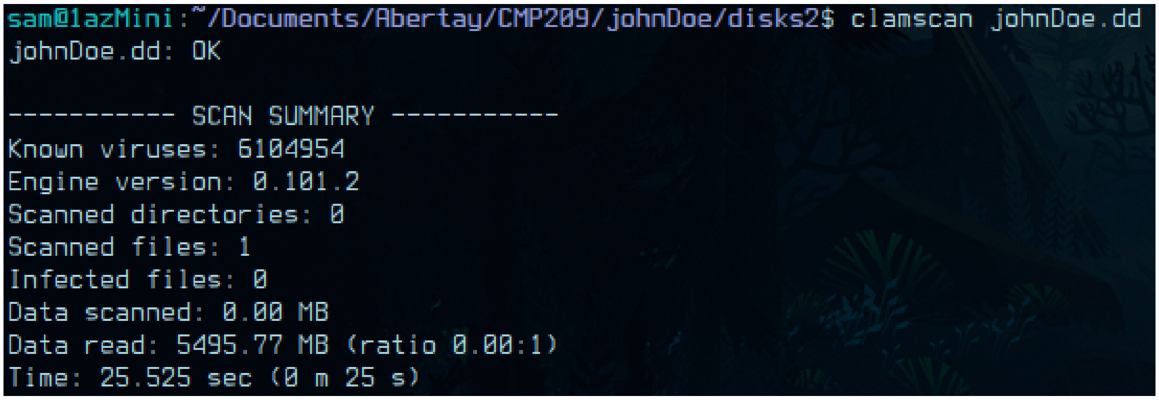
Figure 12: Original partition table of John Doe disk image



```
sam@1azMini:~/Documents/Abertay/CMP209/johnDoe/disks2$ mmls johnDoeWrite.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:  000:001   0006136830   0011245499   0005108670   NTFS / exFAT (0x07)
004:  -------   0011245500   0011255327   0000009828   Unallocated
```

Figure 13: Partition table of John Doe disk image - with uncovered partition

The Clamscan revealed that there was no malware or infected files on the HDD. This was important to know for the analysts so they would not unintentionally infect the lab machine with anything from the image. *(Figure 15)* Hexdump was used to manually search through the remaining unallocated space on the drive for hidden files, but nothing was found. On the unallocated partition Foremost retrieved twenty-three illicit images of an array of bird species, in various environments and positions, as well as a guide to birdwatching in Thailand. *Appendices 1a-w*



```
sam@1azMini:~/Documents/Abertay/CMP209/johnDoe/disks2$ clamscan johnDoe.dd
johnDoe.dd: OK

----------- SCAN SUMMARY -----------
Known viruses: 6104954
Engine version: 0.101.2
Scanned directories: 0
Scanned files: 1
Infected files: 0
Data scanned: 0.00 MB
Data read: 5495.77 MB (ratio 0.00:1)
Time: 25.525 sec (0 m 25 s)
```

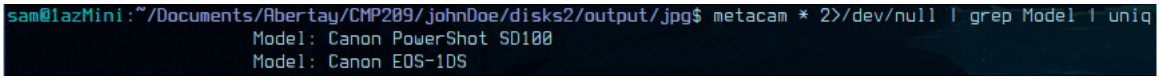
Figure 14: Clamscan results

4.1.3 Images

When the encrypted birds.gpg file was located in the primary partition. The analysts tried, unsuccessfully, to decompress it and retrieve the image files inside. Instead, foremost was used again to carve the files out of the zip file but due to the retrieval method all of the original names were removed. *(Figure 12)* In the appendices the original names have been inferred from the original list created by the attempted unzipping. *Appendices 2a-e*

The cameras that were used to take the images from the original Foremost scan are: *(Figure 16)*

- Canon PowerShot SD100
- Canon EOS-1DS



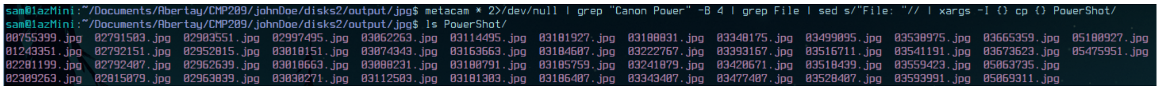
```
sam@1azMini:~/Documents/Abertay/CMP209/johnDoe/disks2/output/jpg$ metacam * 2>/dev/null | grep Model | uniq
                  Model: Canon PowerShot SD100
                  Model: Canon EOS-1DS
```

Figure 15: List of cameras from image metadata

From the Canon PowerShot there were 51 images total, 16 of which contained birds.*(Figure 17)* From the Canon EOS-1DS there was 1 image which contained a bird. *Appendices 3a-q*

The metadata revealed that The Canon PowerShot photos were all taken between 2004:06:09 19:05:11 (9th June 2004 7:05pm) and 2004:06:27 18:28:34 (27th June 2004 6:28pm)

The Canon EOS-1DS photo was taken at 2003:01:29 16:14:10 (29th January 2003 4:14pm)



```
sam@1azMini:~/Documents/Abertay/CMP209/johnDoe/disks2/output/jpg$ metacam * 2>/dev/null | grep "Canon Power" -B 4 | grep File | sed s/"File: "// | xargs -I {} cp {} PowerShot/
sam@1azMini:~/Documents/Abertay/CMP209/johnDoe/disks2/output/jpg$ ls PowerShot/
00755399.jpg  02791503.jpg  02903551.jpg  02997495.jpg  03062263.jpg  03114495.jpg  03181927.jpg  03188031.jpg  03348175.jpg  03499095.jpg  03530975.jpg  03665359.jpg  05180927.jpg
01243351.jpg  02792151.jpg  02952815.jpg  03018151.jpg  03074343.jpg  03163663.jpg  03184607.jpg  03222767.jpg  03393167.jpg  03516711.jpg  03541191.jpg  03673623.jpg  05475951.jpg
02281199.jpg  02792407.jpg  02962639.jpg  03018663.jpg  03088231.jpg  03180791.jpg  03185759.jpg  03241879.jpg  03420671.jpg  03518439.jpg  03559423.jpg  05063735.jpg
02309263.jpg  02815079.jpg  02963839.jpg  03030271.jpg  03112503.jpg  03181303.jpg  03186407.jpg  03343407.jpg  03477407.jpg  03528407.jpg  03593991.jpg  05069311.jpg
```

Figure 16: Listing the images found from the Cannon PowerShot

4.1.4 PDFs

A physical search for PDFs revealed 4 meaningful PDFs. Three of these PDFs were related to bird-watching. These included information about birding sites around Perth, a University of California Botanical Garden newsletter and a Birding Guide. *Appendices 4-6* The fourth PDF is a guide to using WinPT. WinPT stands for Windows Privacy Tools, a collection of tools used for encrypting files. This indicates the potential encryption of some files on the HDD or intent to do so.

There were other passworded pdfs found. The passwords were brute forced using John the Ripper (a password cracking tool) but the pdfs only contained unrelated material.

4.2 Logical Search

4.2.1 Miscellaneous Documents

In John Doe's documents folder there are a few different files relating to birds.

Firstly, there's a saved webpage called aa010703a.htm and saved assets from said webpage in a folder called aa010703a_files. This webpage is a guide to building a Bluebird nest box. A screenshot of this website can be seen at *Appendix 7a*.

Second is a text file called nestboxtips.txt with content describing how to maintain a nest box during summer. A screenshot of the contents can be seen at *Appendix 7b*.

There is a file called kakapo.ram linking to audio.pbs.org/songs/kakapo.rmd. .ram files are used to stream audio from the internet. Unfortunately this site is no longer active and there are no archives of the website so the analysts could not view it in order to ascertain its contents. Kakapo is a species of bird, so it can be inferred that the file was a birdsong.

Under "My Music" there is a document called Doc1.doc. This file contained an image of a bird, but half of the image was offscreen. A screenshot of the document can be seen at *Appendix 8*. Libreoffice was used to open the document and save the embedded image. The image can be seen at *Appendix 9*.

Also present is an encrypted file, which is covered in the next section.

Finally, there are also 9 images relating to birds. These can be seen at *Appendix 10a-i*

4.2.2 E-mails

All of these are communications to and from the accused from their private e-mail address via the Thunderbird e-mail client. In two of the emails from a Ben Forbes, Doe receives seven attachments, containing six images of birds. These images can be described as; Two red parrots in a white cage, a kingfisher in a tree, a balloon animal in the shape of a penguin, a flying seagull with a chip in its mouth with a male hand in the corner of the image, baby birds being fed by an older bird, three green parrots on grass and a female duck floating in water.

9th February 2005 - 11:08am

To: John Doe (jdoe@mail.example.com)
From: Ben Forbes (ben@example.com)
Subject: good pics
Main body:
Hi thought you'd like these
enjoy
Attachments: 7EYBTELF1KAN.jpg, IMG_3937_filtered.jpg and cute_penguin.jpg
Appendices 11a-c

To: John Doe (jdoe@mail.example.com)
From: Bird Fanciers (mailinglist@birds.example.com)
Subject: How to Identify Birds
Main body:
How to Identify Birds

Are you amazed at how quickly birders can identify birds? Actually, it's just like getting to know your human neighbours. When you move into a new neighbourhood 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 neighbour 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.
Attachments: none

To: John Doe (jdoe@mail.example.com)
From: Ben Forbes (ben@example.com)
Subject: some more good ones
Main body:
Thanks for the pics you sent me here are some I really like
Attachments: BC7 feeding the birds.jpg, glfs-storm-birds.jpg, colorful-birds.jpg, IMG_3937_filtered.jpg and gawall8.jpg
Appendices 11a, b, e &f

To: John Doe (jdoe@mail.example.com)
From: Ben Forbes (ben@example.com)

Subject: expensive birds
Main body:
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?”

Attachments: none

4.2.3 Registry Analysis: Recent Docs

Here are the documents found in `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer` These are recently accessed documents that were recorded by the registry.

This is proof that John Doe recently accessed all of these Documents

- My Pictures - John Doe’s images folder
- newbies2.jpg - Bird picture
- ready2fledge.jpg - Bird picture
- aa010703a.htm - Bird related website *Appendix 7a*
- birdwatching.doc - Birdwatching related document
- nestboxtips.txt - Bird box information *Appendix 7b*
- Prac4.gif - Unknown
- Prac4(2) - Unknown
- Q3 Thread (Statechart) - Unknown
- AlmondMarshGreatBlueHeronStalling.jpg - Bird picture *Appendix 1v*
- kakapo.ram - Previously discussed audio streaming file
- BirdingGuide.pdf - One of the recovered PDFs *Appendices 4a-b*
- non images - Unknown
- cookies.txt - Evidence of tampering with internet files
- bookmarks.html - Evidence of tampering with internet files
- aggresive_song.wav - Bird song
- audio - Unknown

- EvanstonWoodpecker.jpg - Bird picture
- Local Disk (C:) - The main partition
- Doc1.doc - Contains an image of a bird as previously discussed *Appendices 8 and 9*
- Sample Music - Files were hidden in here
- Killdeer.jpg - Bird picture
- birds - A folder on the E: drive
- babyscot_vyoung.jpg - Bird picture *Appendix 10e*
- babyscot_2weeks1.jpg - Bird picture *Appendix 10d*
- 117.jpg - Bird picture
- ostbk2b2.htm
- birdtrans2.jpg - Bird picture
- My Music - Files were hidden in here as previously discussed
- Booklist.doc
- ODBC.INI - Text was hidden in this file describing bird life in Lake Michigan
- WINDOWS
- birds.zip - The unencrypted birdpics.gpg file *Appendices 2a-e*
- stuf.doc - A letter informing the recipient that some tasks have been carried out according to previously discussed instructions
- MSN
- New Volume (F:) - The deleted partition

The only document discovered by this process that wasn't previously found was the ODBC.INI file, a windows config file that John Doe has used to hide text in. This is a method of obfuscation, intended to make it harder for investigators to find the text.

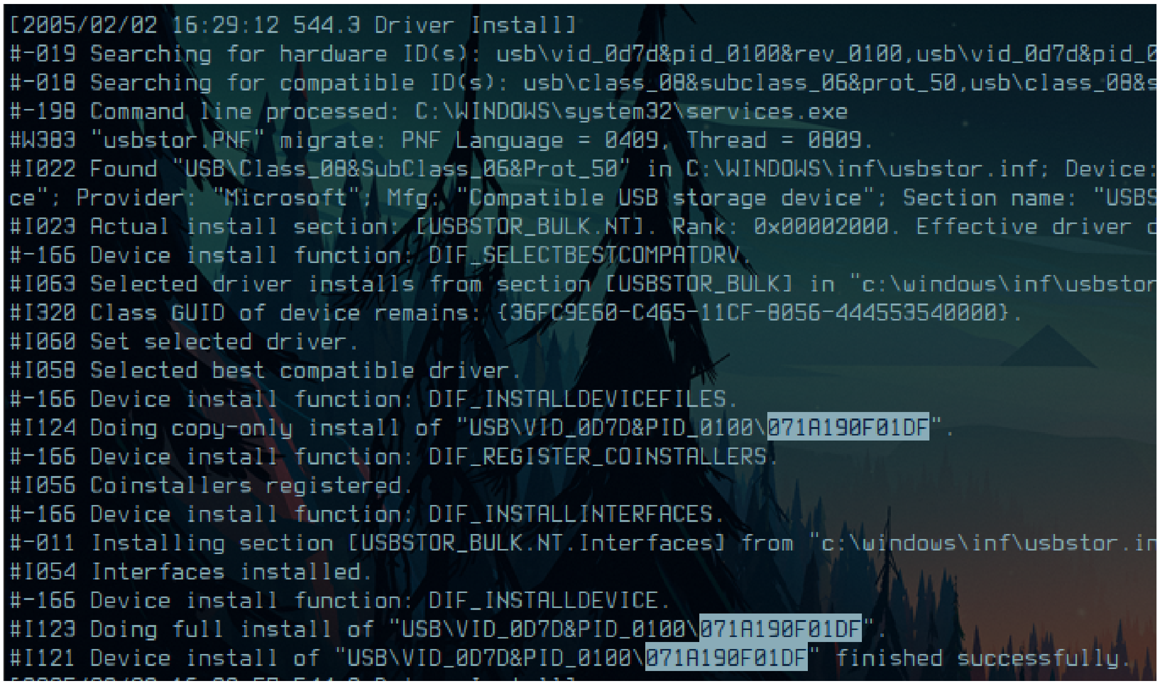
4.2.4 Registry Analysis: USB Drive

Evidence from the registry confirms the presence of a USB device.

The serial number was found at `HKCU\SOFTWARE\ControlSet001\Enum\USBSTOR\[classID]\[serial]`

The serial number is 071A190F01DF

This was then used to search through the event log at `C:\Windows\setupapi.log`



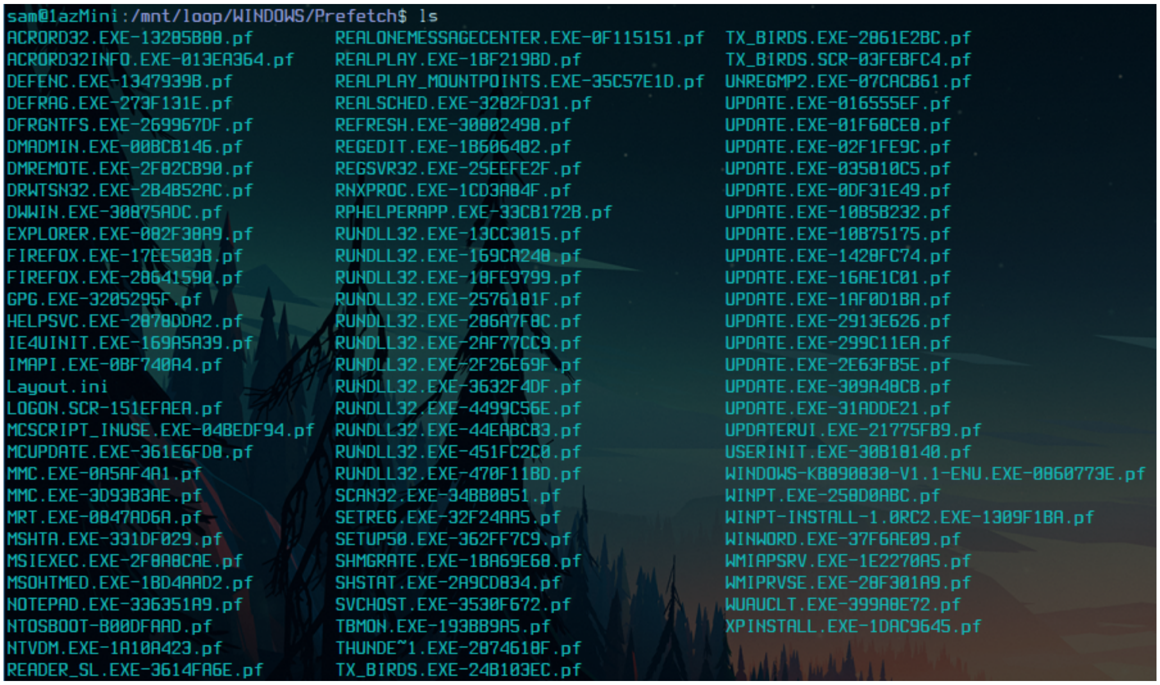
```
[2005/02/02 16:29:12 544.3 Driver Install]
#-019 Searching for hardware ID(s): usb\vid_0d7d&pid_0100&rev_0100,usb\vid_0d7d&pid_0
#-018 Searching for compatible ID(s): usb\class_08&subclass_06&prot_50,usb\class_08&s
#-198 Command line processed: C:\WINDOWS\system32\services.exe
#W383 "usbstor.PNF" migrate: PNF Language = 0409, Thread = 0809.
#I022 Found "USB\Class_08&SubClass_06&Prot_50" in C:\WINDOWS\inf\usbstor.inf; Device:
ce"; Provider: "Microsoft"; Mfg: "Compatible USB storage device"; Section name: "USBS
#I023 Actual install section: [USBSTOR_BULK.NT]. Rank: 0x00002000. Effective driver d
#-166 Device install function: DIF_SELECTBESTCOMPATDRV.
#I063 Selected driver installs from section [USBSTOR_BULK] in "c:\windows\inf\usbstor
#I320 Class GUID of device remains: {36FC9E60-C465-11CF-8056-444553540000}.
#I060 Set selected driver.
#I058 Selected best compatible driver.
#-166 Device install function: DIF_INSTALLDEVICEFILES.
#I124 Doing copy-only install of "USB\VID_0D7D&PID_0100\071A190F01DF".
#-166 Device install function: DIF_REGISTER_COINSTALLERS.
#I056 Coinstallers registered.
#-166 Device install function: DIF_INSTALLINTERFACES.
#-011 Installing section [USBSTOR_BULK.NT.Interfaces] from "c:\windows\inf\usbstor.in
#I054 Interfaces installed.
#-166 Device install function: DIF_INSTALLDEVICE.
#I123 Doing full install of "USB\VID_0D7D&PID_0100\071A190F01DF".
#I121 Device install of "USB\VID_0D7D&PID_0100\071A190F01DF" finished successfully.
```

Figure 17: setupapi.log search

This log entry proves that the device was first plugged into the computer at 2005/02/02 16:29:12

This serial number can also be used to identify the device if it's ever found in the future.

4.2.5 Prefetch Analysis



```
sam@1azMini:/mnt/loop/WINDOWS/Prefetch$ ls
ACRORD32.EXE-13285B88.pf        REALONEMESSAGECENTER.EXE-0F115151.pf  TX_BIRDS.EXE-2861E2BC.pf
ACRORD32INFO.EXE-013EA364.pf    REALPLAY.EXE-1BF219BD.pf              TX_BIRDS.SCR-03FEBFC4.pf
DEFENC.EXE-1347939B.pf          REALPLAY_MOUNTPOINTS.EXE-35C57E1D.pf  UNREGMP2.EXE-07CACB61.pf
DEFRAG.EXE-273F131E.pf          REALSCHED.EXE-3282FD31.pf             UPDATE.EXE-016555EF.pf
DFRGNTFS.EXE-269967DF.pf        REFRESH.EXE-30802498.pf               UPDATE.EXE-01F68CE8.pf
DMADMIN.EXE-00BCB146.pf         REGEDIT.EXE-1B606482.pf               UPDATE.EXE-02F1FE9C.pf
DMREMOTE.EXE-2F82CB90.pf        REGSVR32.EXE-25EEFE2F.pf              UPDATE.EXE-035810C5.pf
DRWTSN32.EXE-2B4B52AC.pf        RNXPROC.EXE-1CD3A84F.pf               UPDATE.EXE-0DF31E49.pf
DWWIN.EXE-30875ADC.pf           RPHELPERAPP.EXE-33CB172B.pf           UPDATE.EXE-10B5B232.pf
EXPLORER.EXE-082F38A9.pf        RUNDLL32.EXE-13CC3015.pf              UPDATE.EXE-10B75175.pf
FIREFOX.EXE-17EE503B.pf         RUNDLL32.EXE-169CA248.pf              UPDATE.EXE-1428FC74.pf
FIREFOX.EXE-28641590.pf         RUNDLL32.EXE-18FE9799.pf              UPDATE.EXE-16AE1C01.pf
GPG.EXE-3205295F.pf             RUNDLL32.EXE-2576181F.pf              UPDATE.EXE-1AF0D1BA.pf
HELPSVC.EXE-2878DDA2.pf         RUNDLL32.EXE-286A7F8C.pf              UPDATE.EXE-2913E626.pf
IE4UINIT.EXE-169A5A39.pf        RUNDLL32.EXE-2AF77CC9.pf              UPDATE.EXE-299C11EA.pf
IMAPI.EXE-0BF740A4.pf           RUNDLL32.EXE-2F26E69F.pf              UPDATE.EXE-2E63FB5E.pf
Layout.ini                      RUNDLL32.EXE-3632F4DF.pf              UPDATE.EXE-309A48CB.pf
LOGON.SCR-151EFAEA.pf           RUNDLL32.EXE-4499C56E.pf              UPDATE.EXE-31ADDE21.pf
MCSCRIPT_INUSE.EXE-04BEDF94.pf  RUNDLL32.EXE-44EABCB3.pf              UPDATERUI.EXE-21775FB9.pf
MCUPDATE.EXE-361E6FD8.pf        RUNDLL32.EXE-451FC2C8.pf              USERINIT.EXE-30B18140.pf
MMC.EXE-0A5AF4A1.pf             RUNDLL32.EXE-470F11BD.pf              WINDOWS-KB890830-V1.1-ENU.EXE-0860773E.pf
MMC.EXE-3D93B3AE.pf             SCAN32.EXE-34BB0851.pf                WINPT.EXE-258D0ABC.pf
MRT.EXE-0847AD6A.pf             SETREG.EXE-32F24AA5.pf                WINPT-INSTALL-1.0RC2.EXE-1309F1BA.pf
MSHTA.EXE-331DF029.pf           SETUP50.EXE-362FF7C9.pf               WINWORD.EXE-37F6AE09.pf
MSIEXEC.EXE-2F8A8CAE.pf         SHMGRATE.EXE-1BA69E68.pf              WMIAPSRV.EXE-1E2270A5.pf
MSOHTMED.EXE-1BD4AAD2.pf        SHSTAT.EXE-2A9CD834.pf                WMIPRVSE.EXE-28F301A9.pf
NOTEPAD.EXE-336351A9.pf         SVCHOST.EXE-3530F672.pf               WUAUCLT.EXE-399A8E72.pf
NTOSBOOT-B00DFAAD.pf            TBMON.EXE-193BB9A5.pf                 XPINSTALL.EXE-1DAC9645.pf
NTVDM.EXE-1A10A423.pf           THUNDE~1.EXE-2874618F.pf
READER_SL.EXE-3614FA6E.pf       TX_BIRDS.EXE-24B103EC.pf
```

Figure 18: prefetch files

The prefetch files reveal some interesting evidence.

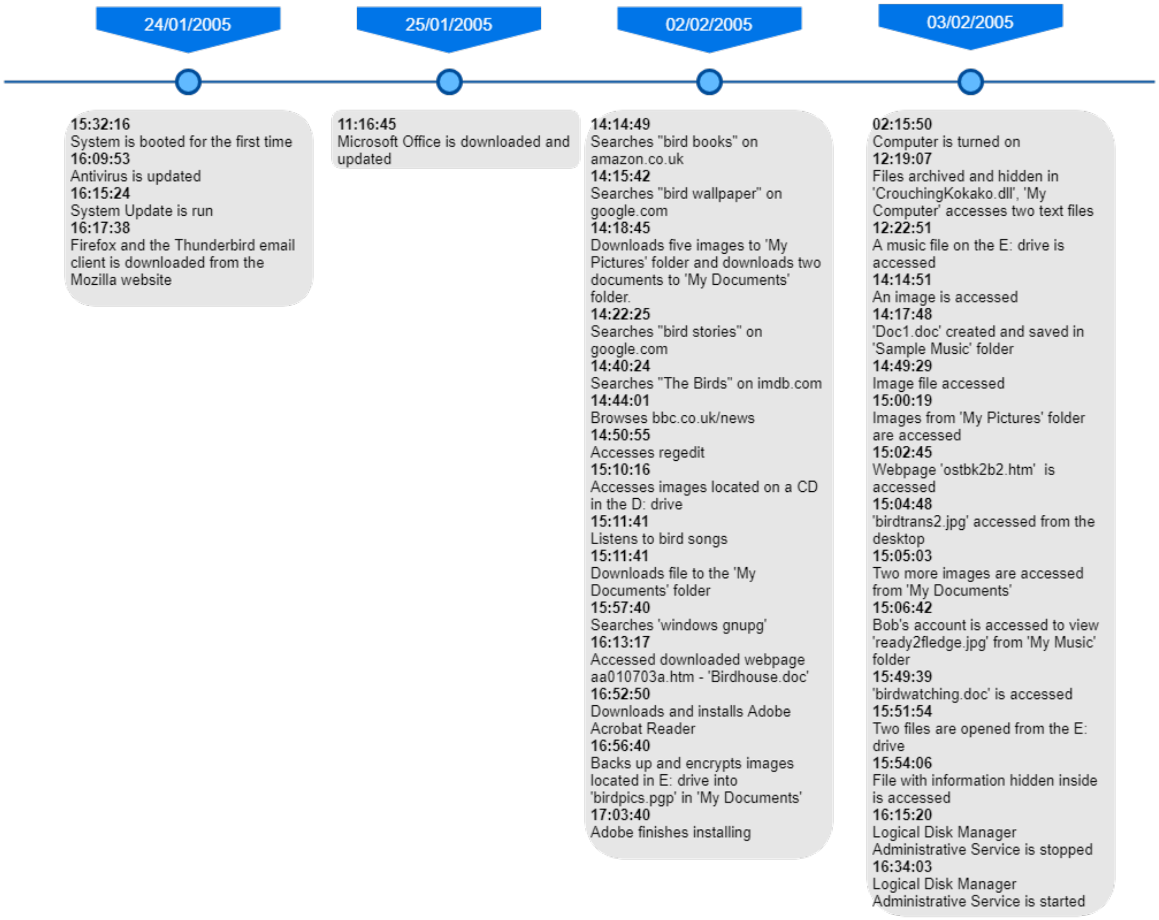
Realplay was used. This is an audio player and was most likely used to listen to bird songs since that is the only significant audio present on the HDD.

Regedit was used. This is a tool used to edit registry keys. This indicates that John Doe tampered with the registry somehow. It is unclear how it was tampered with, since editing the registry is not logged.

tx_birds.exe was run from a few different locations, indicated by the presence of multiple prefetch files for the same executable. This executable is a screensaver with a slideshow of several images of birds.

Other notable evidence from the prefetch files are covered in the time-lines presented in section 4.3.

4.3 Computer time-lines



24/01/2005

15:32:16
System is booted for the first time
16:09:53
Antivirus is updated
16:15:24
System Update is run
16:17:38
Firefox and the Thunderbird email client is downloaded from the Mozilla website

25/01/2005

11:16:45
Microsoft Office is downloaded and updated

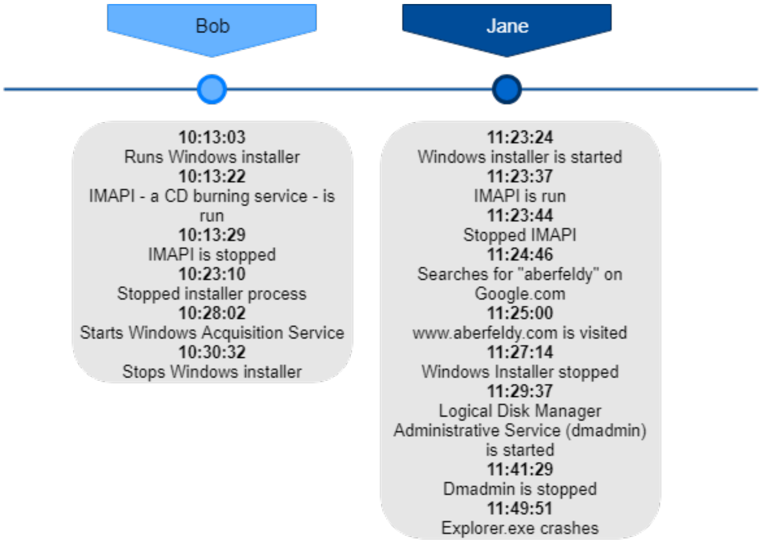
02/02/2005

14:14:49
Searches "bird books" on amazon.co.uk
14:15:42
Searches "bird wallpaper" on google.com
14:18:45
Downloads five images to 'My Pictures' folder and downloads two documents to 'My Documents' folder.
14:22:25
Searches "bird stories" on google.com
14:40:24
Searches "The Birds" on imdb.com
14:44:01
Browses bbc.co.uk/news
14:50:55
Accesses regedit
15:10:16
Accesses images located on a CD in the D: drive
15:11:41
Listens to bird songs
15:11:41
Downloads file to the 'My Documents' folder
15:57:40
Searches 'windows gnupg'
16:13:17
Accessed downloaded webpage aa010703a.htm - 'Birdhouse.doc'
16:52:50
Downloads and installs Adobe Acrobat Reader
16:56:40
Backs up and encrypts images located in E: drive into 'birdpics.pgp' in 'My Documents'
17:03:40
Adobe finishes installing

03/02/2005

02:15:50
Computer is turned on
12:19:07
Files archived and hidden in 'CrouchingKokako.dll', 'My Computer' accesses two text files
12:22:51
A music file on the E: drive is accessed
14:14:51
An image is accessed
14:17:48
'Doc1.doc' created and saved in 'Sample Music' folder
14:49:29
Image file accessed
15:00:19
Images from 'My Pictures' folder are accessed
15:02:45
Webpage 'ostbk2b2.htm' is accessed
15:04:48
'birdtrans2.jpg' accessed from the desktop
15:05:03
Two more images are accessed from 'My Documents'
15:06:42
Bob's account is accessed to view 'ready2fledge.jpg' from 'My Music' folder
15:49:39
'birdwatching.doc' is accessed
15:51:54
Two files are opened from the E: drive
15:54:06
File with information hidden inside is accessed
16:15:20
Logical Disk Manager Administrative Service is stopped
16:34:03
Logical Disk Manager Administrative Service is started

Figure 19: Timeline for John Doe



10:13:03
Runs Windows installer
10:13:22
IMAPI - a CD burning service - is run
10:13:29
IMAPI is stopped
10:23:10
Stopped installer process
10:28:02
Starts Windows Acquisition Service
10:30:32
Stops Windows installer

11:23:24
Windows installer is started
11:23:37
IMAPI is run
11:23:44
Stopped IMAPI
11:24:46
Searches for "aberfeldy" on Google.com
11:25:00
www.aberfeldy.com is visited
11:27:14
Windows Installer stopped
11:29:37
Logical Disk Manager Administrative Service (dmadmin) is started
11:41:29
Dmadmin is stopped
11:49:51
Explorer.exe crashes

Figure 20: Timeline for Bob and Jane

4.3.1 John Doe

Key items *Appendices 12-14*

Day one: 24th January 2005 **3:32pm**: According to the computers event log the accused boots up their computer for the first time, implying that this is the first time this computer has been used.
4:17pm: The e-mail client Thunderbird is installed, this is used later to receive bird images.

Day three: 2nd February 2005
2:15pm: Searches for books about birds on the online marketplace Amazon.
2:18pm: Searches Google images for bird wallpapers and downloads five images.
At the same time downloads an HTM file that contains instructions on how to build a birdhouse and a text document called 'nestboxtips.txt', which offers advice on how to attract birds. *Appendices 9a and b*
2:22pm: Google search history from Firefox shows that 'bird stories' was searched for.
2:50pm: Accesses the regedit tool. This tool is used to view or edit, such as deleting, items in the Windows registry. These items include registry keys their values and the value data.
3:10pm: Accesses images located on a CD, that has been inserted into the D: drive. The contents of this CD is unknown to the digital forensic analysts.
3:11pm: Listens to bird songs online and downloads a music file called 'kakapo.ram', this file is used to stream music from the internet but the host it's targeting is unresolvable. It's worth noting that Kakapo is a type of bird.
4:13pm: Accesses the webpage that was downloaded at 2:18pm.
4:31pm: Installs GNUP, software that allows the user to encrypt files.
4:56pm: Backs up and encrypts images from the E: drive into 'birdpics.gpg' in an attempt to obfuscate the files. *Appendices 2a-e*

Day four: 3rd February 2005

12:19pm: Seven image files archived and hidden in 'CrouchingKokado.dll' these images are. *Appendices 15a-g*
12:22pm: Music file titled 'aggressive_song.wav' is accessed from the 'audio' folder within the folder 'birds' on the E: drive.
2:14pm: 'EvanstonWoodpecker.jpg' is accessed from C: drive. **2:17pm**: 'Doc1.doc' is created and stored in 'Sample music'. The document contains an image of a bird *Appendix 9*
2:49pm: 'Killdeer.jpg' is accessed from the E: drive. **3:00pm**: Three images from 'My pictures' are accessed. **3:02pm**: 'ostbk2b2.htm' is accessed, this webpage contains . **3:04pm**: 'birdtrans2.jpg' is accessed from the desktop. **3:05pm**: 'chicks2.jpg' and 'newbies.jpg' are viewed. **3:06pm**: The suspect views another image titled 'ready2fledge.jpg'. **3:49pm**: The document 'birdwatching.doc' was accessed.
3:51pm: 'BookList.doc' and the PDF 'BirdingGuide.pdf' were opened
.

4.3.2 Bob and Jane (Day four: 3rd February 2005)

Bob

10:13am: IMAPI CD-burning service is run on windows and stopped seven seconds later, it is feasible for the person running the software to have burned files onto a disk but they would have to be small.
10:28am: Windows Image Acquisition Service (WIP) is run, implying that images are transferred either to or from an external piece of hardware such as a camera or scanner.

Jane

11:23am: IMAPI is run again for another seven seconds.
11:25am: A website called 'aberfeldys.com' is visited, this website contains numerous images of birds.
11:29am:Logical Disk Manager Administrative Service is run for twelve minutes, this service is used to configure hard drive disk partitions.

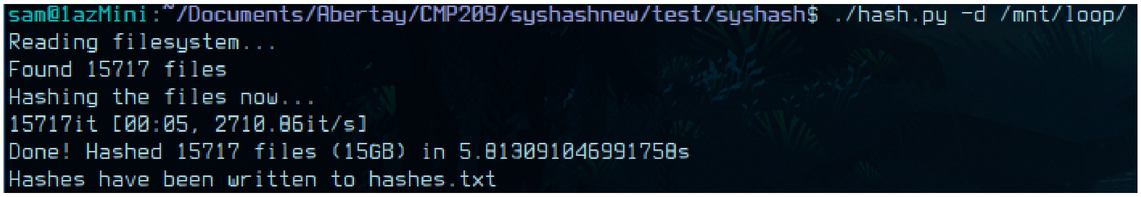
5 Production List and Associated Description

5.1 Syshash

A custom python script was written to create hashes of John Doe's entire filesystem. This was used to verify the integrity of the files throughout the investigation.

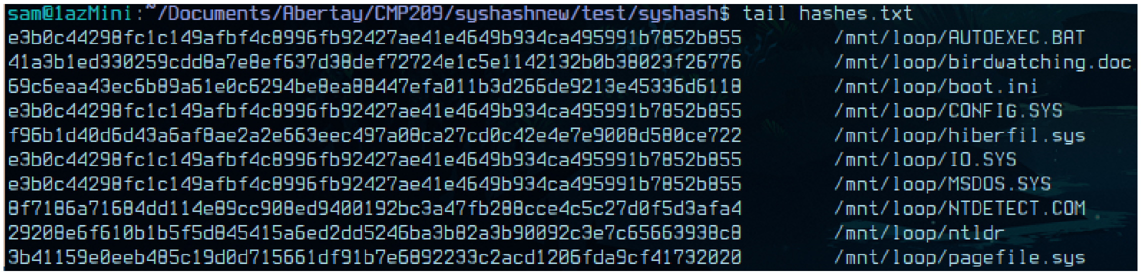
The script is in the attached files as hash.py.

To use the program, type "./hash.py -d [dir to hash]". For example: "./hash.py -d /mnt/loop/". This would hash the filesystem of a device that is loopback mounted.



```
sam@1azMini:~/Documents/Abertay/CMP209/syshashnew/test/syshash$ ./hash.py -d /mnt/loop/
Reading filesystem...
Found 15717 files
Hashing the files now...
15717it [00:05, 2710.86it/s]
Done! Hashed 15717 files (15GB) in 5.813091046991758s
Hashes have been written to hashes.txt
```

Figure 21: Running the script



```
sam@1azMini:~/Documents/Abertay/CMP209/syshashnew/test/syshash$ tail hashes.txt
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855        /mnt/loop/AUTOEXEC.BAT
41a3b1ed330259cdd8a7e8ef637d38def72724e1c5e1142132b0b38023f26776        /mnt/loop/birdwatching.doc
69c6eaa43ec6b89a61e0c6294be8ea88447efa011b3d266de9213e45336d6118        /mnt/loop/boot.ini
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855        /mnt/loop/CONFIG.SYS
f96b1d40d6d43a6af8ae2a2e663eec497a08ca27cd0c42e4e7e9008d580ce722        /mnt/loop/hiberfil.sys
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855        /mnt/loop/IO.SYS
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855        /mnt/loop/MSDOS.SYS
8f7186a71684dd114e89cc908ed9400192bc3a47fb288cce4c5c27d0f5d3afa4        /mnt/loop/NTDETECT.COM
29208e6f610b1b5f5d845415a6ed2dd5246ba3b82a3b90092c3e7c65663938c8        /mnt/loop/ntldr
3b41159e0eeb485c19d0d715661df91b7e6892233c2acd1206fda9cf41732020        /mnt/loop/pagefile.sys
```

Figure 22: A sample of the script's output file

6 Conclusions

There was a partition that was not initially present in the MBR, this is a result of a partition being deleted, since the contents were images and files related to birds and birdwatching, this potentially was an effort to hide the contents present there.

On the main partition itself numerous bird images were found and an audio that potentially contained birdsongs. In the browser and file histories, multiple websites related to bird watching and viewing bird related images were accessed, images and files were also downloaded over this four day period by John Doe.

Bob and Jane also used the computer in question but but it cannot be proven, from the digital evidence alone, that they assisted the accused even if they also accessed bird related websites.

Many efforts were made to conceal images and bird-related information. This includes hiding text in windows files, changing file extensions and hiding files in unusual places.

The e-mails received by John Doe's account contain a fairly substantial amount of bird images. The conversations had in the email also suggested that John Doe has previously distributed bird images over email.

There were a large collection of photos that were all taken by the same camera and within the same timeframe. They appear to be from a birdwatching trip.

Since the malware scan returned that there are no viruses, the images could not possibly have been put on John Doe's computer by malware or virus.

7 Contributions

Sam Heney:

Carried out every task in the analysis section, Got all of the screenshots in that section and wrote up the initial drafts of that section. Discovered and acquired all of the images and evidence used in the report. Used the evidence along with system time information and registry investigation to create the written timeline of events. Wrote the conclusions section. Wrote the description of items and the production list. Wrote the syshash python program that was used to generate hashes of all of the files.

Mairi McQueer:

Wrote the Job Description, most of analysis and conclusions, some of equipment required and also rewrote almost all of analysis methodology. Formatted and included appendices 1-3, as well as organising them in analysis and methodology. Implemented almost all of the design and aesthetic decisions in the formatting of the report.

Ben Gilmour:

Gathered some of the early screenshots that were missed. Wrote up some of the analysis methodology and added, formatted and organised the majority of the appendices.

8 Equipment Required for Court Proceedings

In order to present the evidence discovered the following items are required:

- A perfect image of John Doe's HDD
- A machine with a Linux distribution installed, in the report Debian was used. The machine will also require the following software and libraries:
    - Testdisk
    - Sleuthkit library
    - Metacam
    - Pasco
    - Foremost
    - chntpw
    - reged
    - syshash (written for this project)

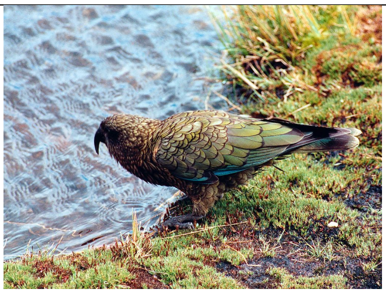
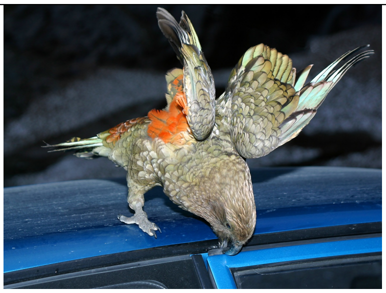
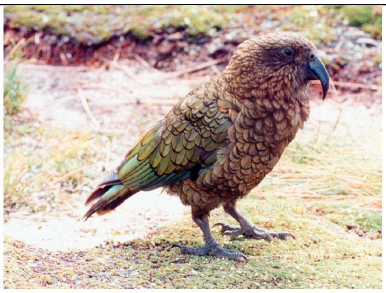
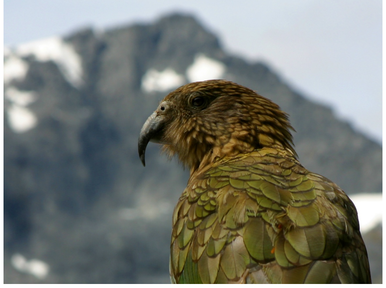
9 Acronyms used

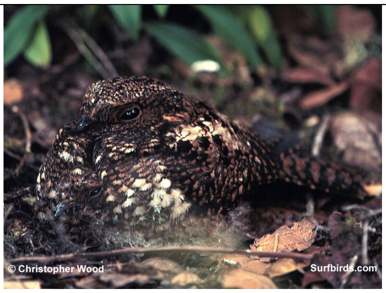
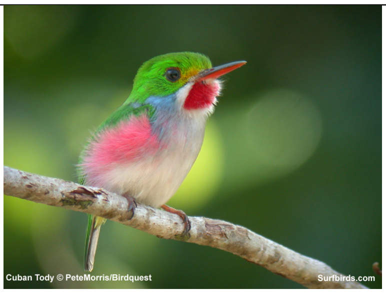
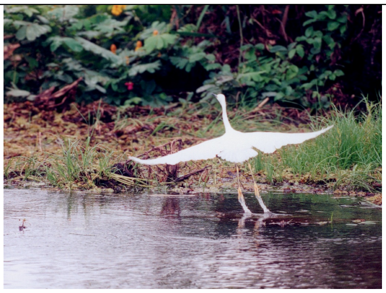
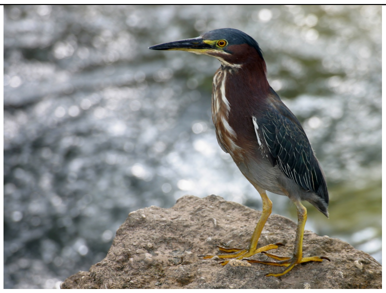
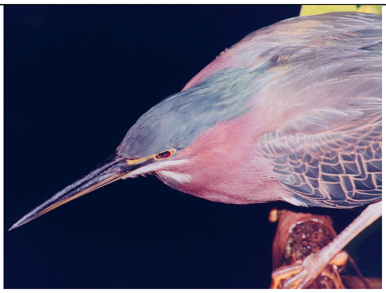
Hard Drive Disk (HDD)
Kilobytes (KB)
Megabytes (MB)
Gigabytes (GB)
Operating System (OS)
Media Access Control (MAC)
Windows Image Acquisition Service (WIP)
Master Boot Record (MBR)

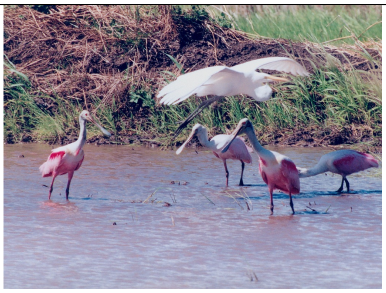
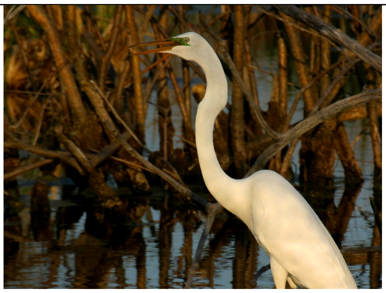
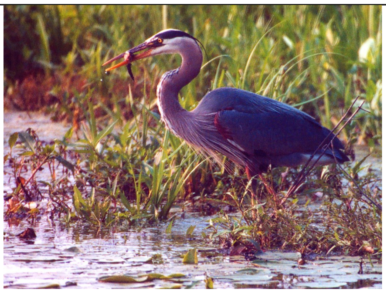
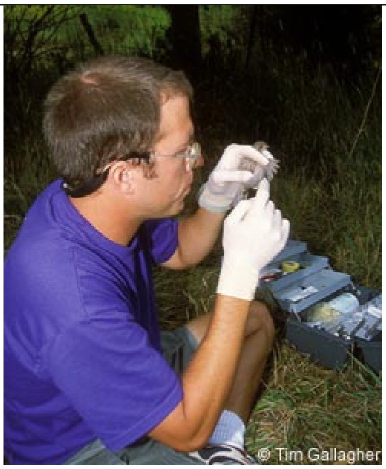
List of Figures

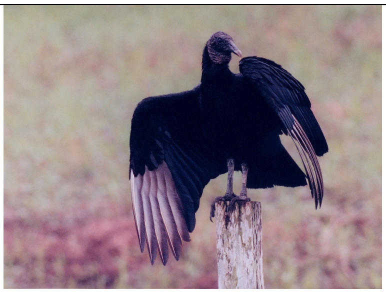
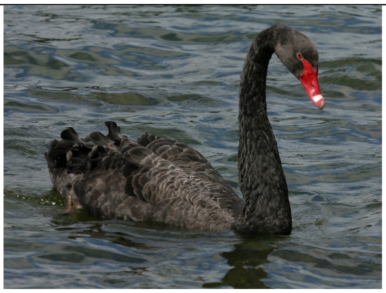
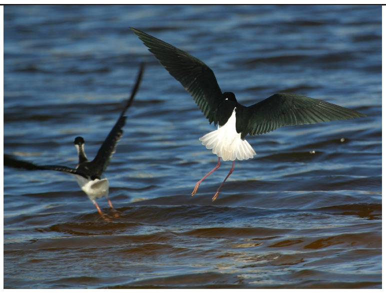
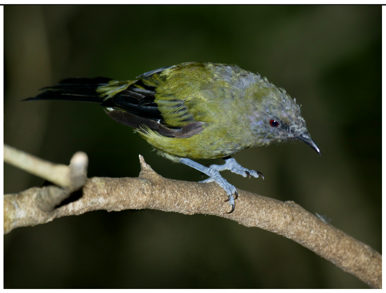
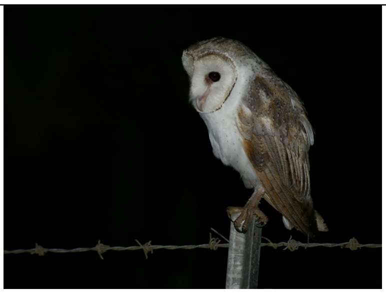
10 Appendices

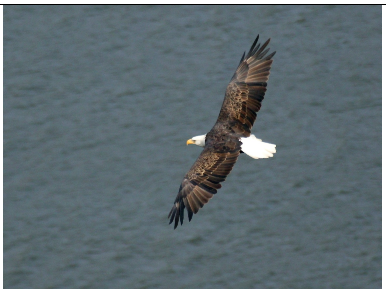
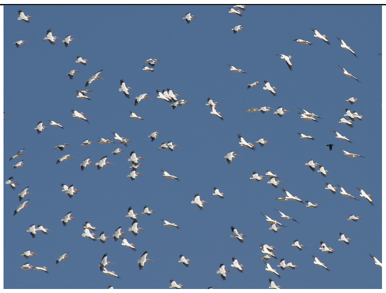
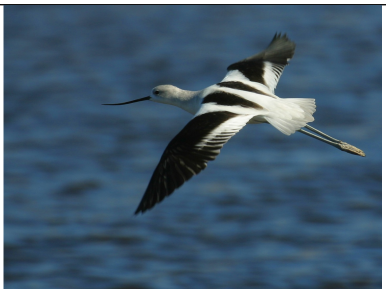
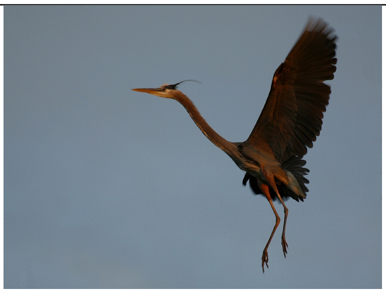
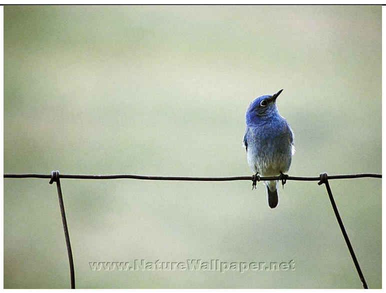
10.1 Images From Recovered Partition

Appendix Number.	Image	Image Name
1a		KeaRetrievingBakedBeanCanFromTarn.jpg
1b		KeaEatingRentalCar.jpg
1c		KeaAtTopOfMacKinnonPass0930.jpg
1d		KeaAndMountain.jpg

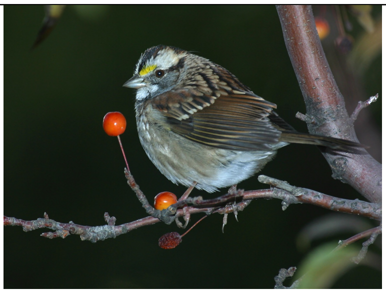
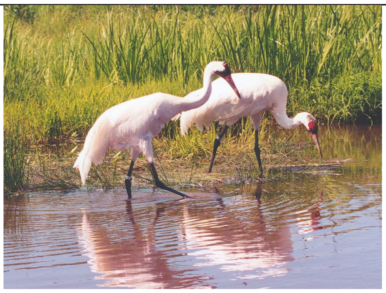
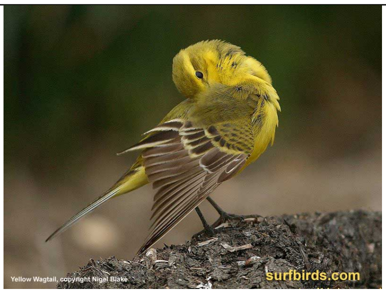
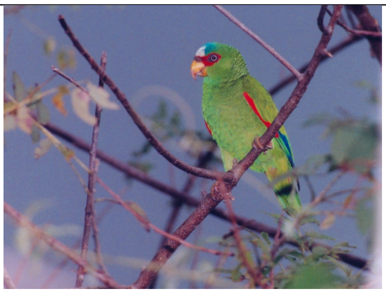
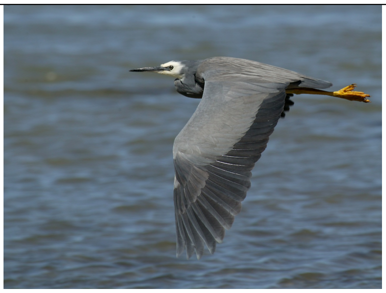
1e	 	junescreen01.jpg
1f	 	june03screen.jpg
1g		ImmatureSnowyEgretTakingOff.jpg
1h		GreenHeronOnChicagoLakeshore.jpg
1i		GreenHeronCloseup.jpg

1j		GreatEgretOverflyingRoseateSpoonbills.jpg
1k		GreatEgretInVoloBog.jpg
1l		GreatBlueHeronWithFish.jpg
1m		brd_Ornithologist_TWG.jpg

1n		BlackVultureSunningOnPost.jpg
1o		BlackSwan.jpg
1p		BlackNeckedStiltsFromBehind.jpg
1q		BellbirdJumpingOffBranch.jpg
1r		BarnOwl.jpg

1s		BaldEagle7oClock.jpg
1t		AmericanWhitePelicansCircling.jpg
1u		AmericanAvocetWinterPlumage.jpg
1v		AlmondMarshGreatBlueHeronStalling.jpg
1w		Df1.jpg

10.2 Images obtained from birdpics.gpg

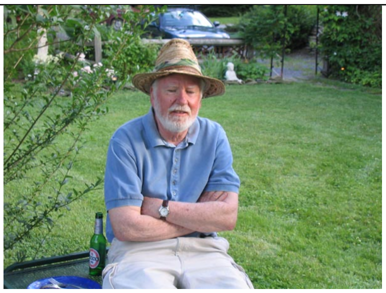
Appendix Number.	Image	Image Name
2a		00000000.jpg
2b		00000482.jpg
2c		00001079.jpg
2d		00001199.jpg
2e		00001568.jpg

10.3 Photos taken from Cannon Powershot

Appendix Number.	Image	Image Name
3a		05475951.jpg
3b		05180927.jpg
3c		05069311.jpg
3d		05063735.jpg
3e		03673623.jpg

3f		03665359.jpg
3g		03593991.jpg
3h		03559423.jpg
3i		03541191.jpg

3j		03538975.jpg
3k		03528407.jpg
3l		03518439.jpg
3m		03516711.jpg

3n		03499095.jpg
3o		03477407.jpg
3p		03420671.jpg
3q		03393167.jpg
3r		03348175.jpg

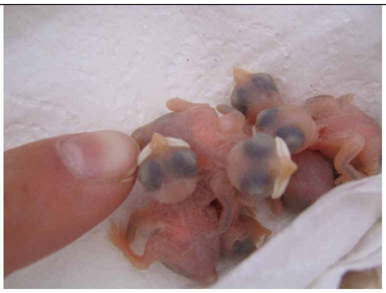
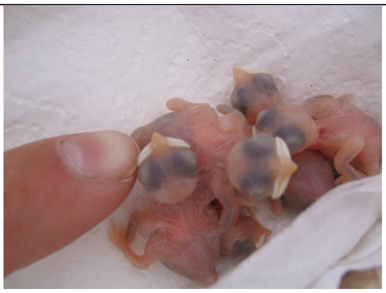
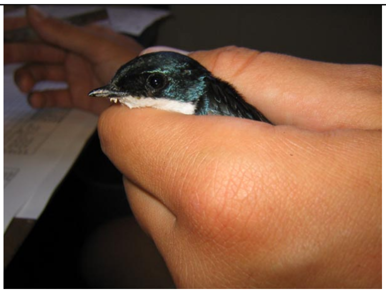
3s		03343407.jpg
3t		03241879.jpg
3u		03222767.jpg
3v		03188831.jpg
3w		03186407.jpg

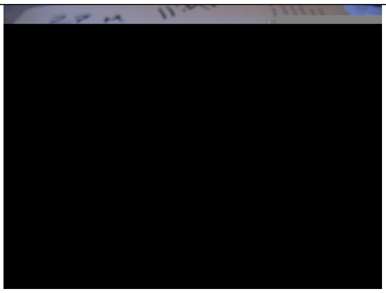
3x		03185759.jpg
3y		03184607.jpg
3z		03181927.jpg
3aa		03181303.jpg
3ab		03180791.jpg

3ac		03163663.jpg
3ad		03114495.jpg
3ae		03112503.jpg
3af		03088231.jpg
3ag		03074343.jpg

3ah		03062263.jpg
3ai		03030271.jpg
3aj		03018663.jpg
3ak		03018151.jpg

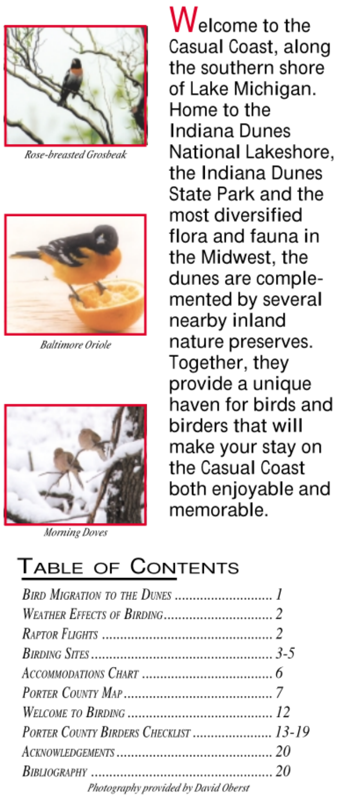
3al		02997495.jpg
3am		02963839.jpg
3an		02952815.jpg
3ao		02903551.jpg
3ap		02815079.jpg

3aq		02792407.jpg
3ar		02792151.jpg
3as		02791503.jpg
3at		02309263.jpg

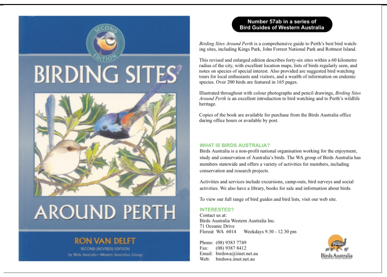
3au	 [redacted]	02281199.jpg
3av		01243351.jpg

10.4 Birding Guide PDF

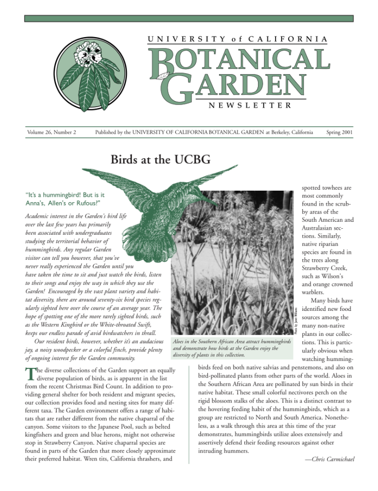
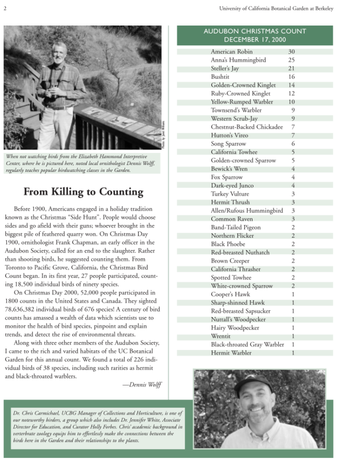
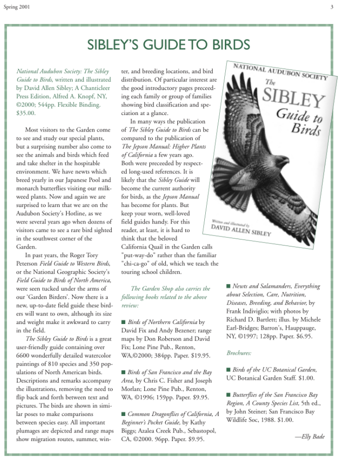
Appendix Number.	Image	Image Name
4a	 The Porter County Birding Guide Indiana Dunes The Casual Coast	Birding_guide_01.png

4b	 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. *Rose-breasted Grosbeak* *Baltimore Oriole* *Morning Doves* TABLE OF CONTENTS *Photography provided by David Oberst*	Birding_guide_02.png

10.5 Birding Sites around Perth PDF

Appendix Number.	Image	Image Name
5	 SECOND EDITION BIRDING SITES AROUND PERTH RON VAN DELFT SECOND (REVISED) EDITION by Birds Australia—Western Australian Group 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: birdswa@iinet.net.au Web: birdswa.iinet.net.au Birds Australia	Birding_sites_around_perth.png

10.6 California Botanical Garden newsletter PDF

Appendix Number.	Image	Image Name
6a		Cali_letter_01.png
6b		Cali_letter_02.png
6c		Cali_letter_03.png

UNIVERSITY of CALIFORNIA
BOTANICAL 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 the territorial behavior of hummingbirds. Any regular Garden visitor can tell you however, 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.

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

Photo by Janet Williams

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 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.

Many birds have identified new food sources among the many non-native plants in our collections. This is particularly obvious when watching hummingbirds feed on both native salvias and penstemons, and also on bird-pollinated plants from other parts of the world. Aloes in the Southern African Area are pollinated by sun birds in their native habitat. These small colorful nectivores perch on the rigid blossom stalks of the aloes. This is a distinct contrast to the hovering feeding habit of the hummingbirds, 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, hummingbirds utilize aloes extensively and assertively defend their feeding resources against other intruding hummers.

—Chris Carmichael

2 University of California Botanical Garden at Berkeley

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.

Photos by Janet Williams

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
Bushtit	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.

Spring 2001 3

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, winter, and breeding locations, and bird distribution. Of particular interest are the good introductory pages preceeding 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* a few years ago. Both were preceeded 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 your 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.

NATIONAL AUDUBON SOCIETY
The SIBLEY Guide to Birds
Written and illustrated by
DAVID ALLEN SIBLEY

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.

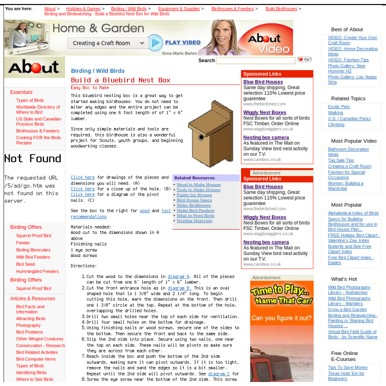
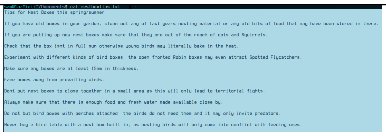
Brochures:

■ *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

10.7 Nestboxing Website images

Appendix Number.	Image	Image Name
7a		aa010703a.png
7b		nestboxtips.png

You are here: About > Hobbies & Games > Birding / Wild Birds > Equipment & Supplies > Birdhouses & Feeders > Build Birdhouses >
Birding and Birdwatching - Build a Bluebird Nest Box for Wild Birds

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

Not Found

The requested URL /5/ad/go.htm was not found on this server.

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

Birding Offers
- Squirrel Proof Bird

Articles & 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

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 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

Related Resources
- Wood to Make Houses
- Tools to Make Houses
- Paints for Houses
- Bird House Specs
- Make Birdhouses
- Make Bird Feeders
- What to Feed Birds
- Nesting Materials

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 nails 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

Sponsored Links

Blue Bird Houses
Same day shipping, Great selection 110% Lowest price guarentee
www.thebirdshed.com

Wiggly Nest Boxes
Nest Boxes for all sorts of birds FSC Timber, Order Online
www.wigglywigglers.co.uk

Nesting box camera
As featured in The Mail on Sunday View bird nest activity on our T.V.
www.cambox.co.uk

Advertisement
Sponsored Links

Blue Bird Houses
Same day shipping, Great selection 110% Lowest price guarentee
www.thebirdshed.com

Wiggly Nest Boxes
Nest Boxes for all sorts of birds FSC Timber, Order Online
www.wigglywigglers.co.uk

Nesting box camera
As featured in The Mail on Sunday View bird nest activity on our T.V.
www.cambox.co.uk

Advertisement

Best of About
- VIDEO: Create Your Own Craft Room
- VIDEO: Home Decorating Ideas
- VIDEO: Fashion Tips
- Photo Gallery: New Hummer H2
- Photo Gallery: Las Vegas Strip

Related Topics
- Exotic Pets
- Walking
- U.S. / Canadian Parks
- Climbing

Most Popular Video
- Bathroom Decoration Ideas
- Tag Sale Tips
- Creating a Craft Room
- Fashion for Special Occasions
- Women: Building a Wardrobe

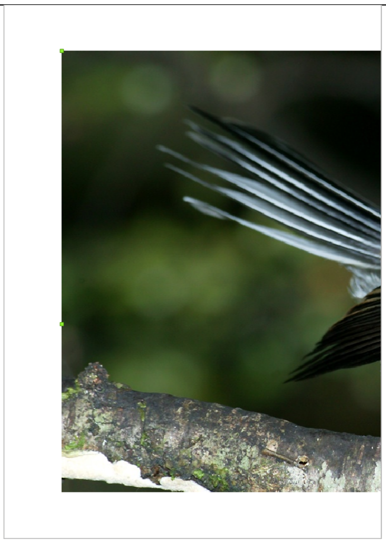
Most Popular
- Alphabetical Index of Birds
- Specs for Building Birdhouses and for use in Bird House Plan...
- FREE Holiday Bird Clipart - Valentine's Day Index
- Butterfly and Bee Free Clipart Index
- Free Bird Clipart Index - Eagles

What's Hot
- Wild Bird Photography Library - Nuthatches
- Wild Bird Photography Library - Warblers
- Grow a Bird Garden
- Birding and Birdwatching - Painting or Staining Bird Houses ...
- Virtual Bird Field Guide of Birds - by Scientific Name

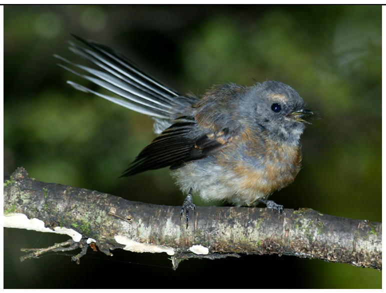
Free Online E-Courses
- Tips To Save Money
- Texas Hold 'Em for Beginners

```
sam@lazMini:~/Documents$ cat nestboxtips.txt
Tips for Nest Boxes this spring/summer

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

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

Check that the box isnt 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.

Dont put nest boxes to close together in a small area as this will only lead to territorial fights.

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

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

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

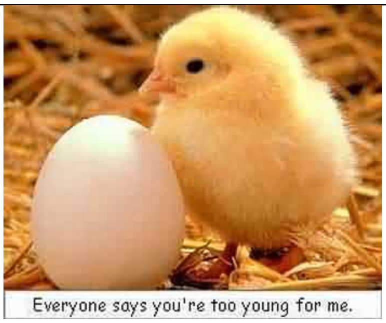
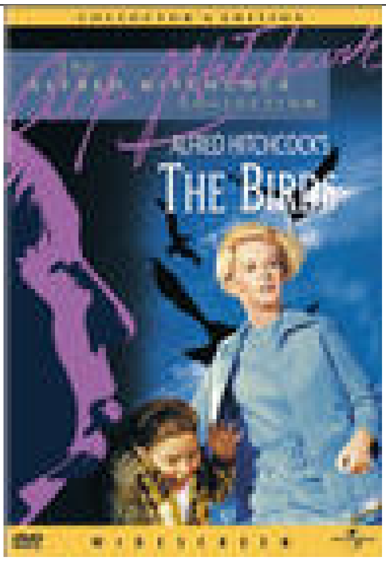
10.8 Screenshot of Doc1.doc

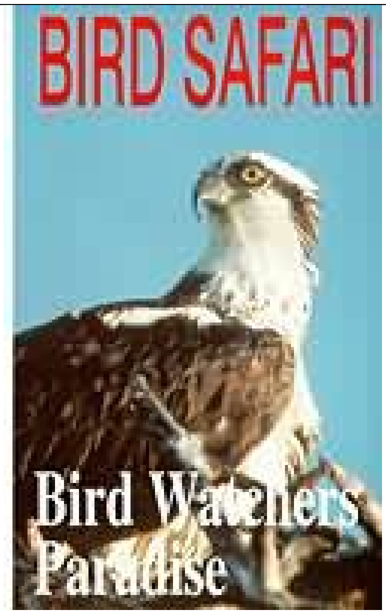
Appendix Number.	Image	Image Name
8		screenshot.png

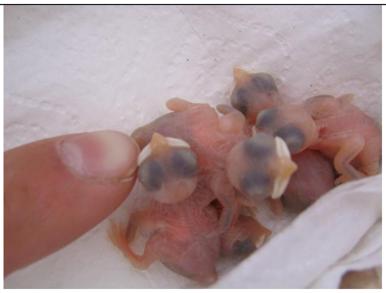
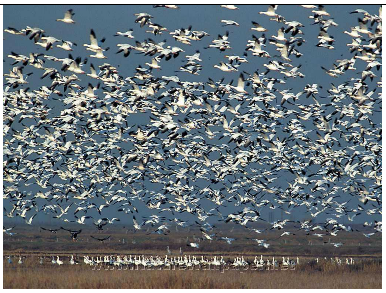
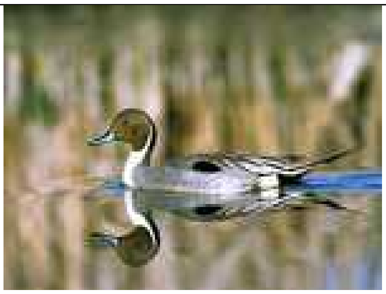
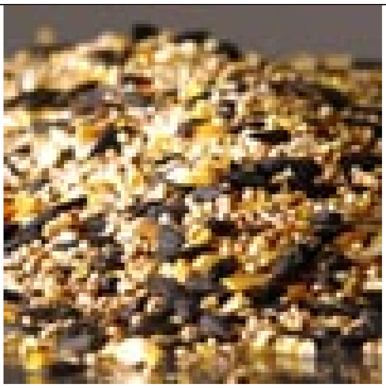
10.9 Image from Doc1.doc

Appendix Number.	Image	Image Name
9		Doc1Image.jpg

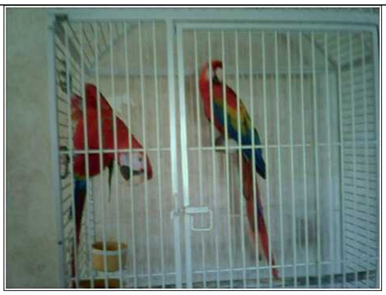
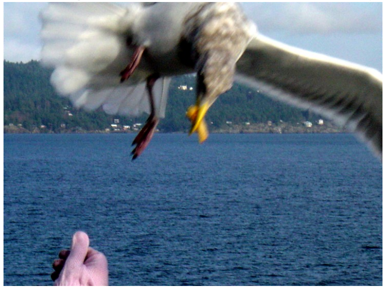
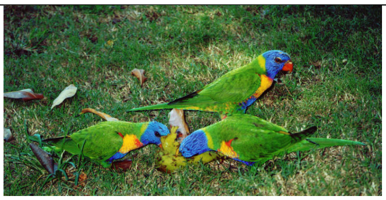
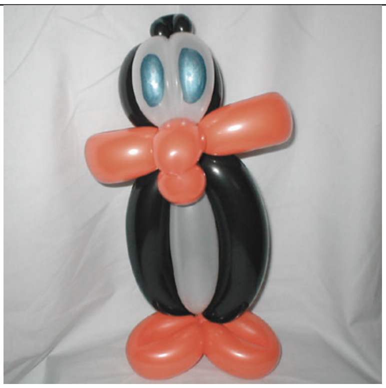
10.10 Images from John Doe's documents

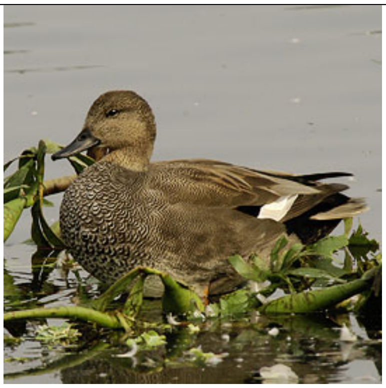
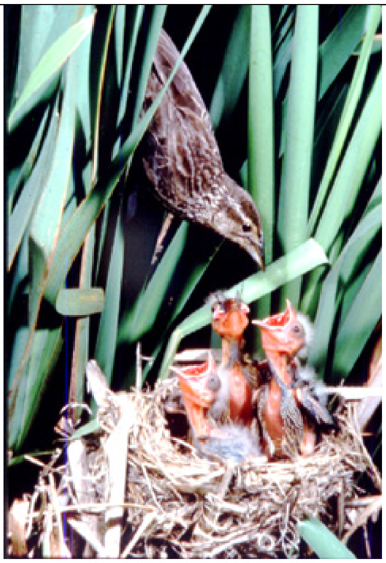
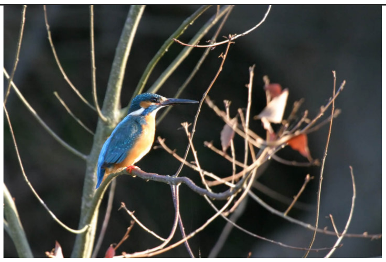
Appendix Number.	Image	Image Name
10a		177.jpg
10b		40m.jpg

10c		7107298.jpg
10d		babyscot_2week1.jpg
10e		babyscot_vyoung.jpg

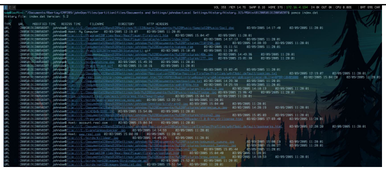
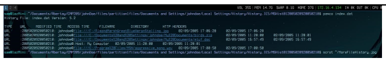
10f		chicks2.jpg
10g		snow_geese.jpg
10h		tn_duck_3.jpg
10i		wbpremium_s.jpg

10.11 Email Pictures

Appendix Number.	Image	Image Name
11a		7EYBTELF1KAN.jpg
11b	feeding the birds.jpg 	BC7 feeding the birds.jpg
11c		colorful-birds.jpg
11d		cute_penguin.jpg

11e		gawall8.jpg
11f	 *Nesting red-winged blackbird/* *Carouge à épaulettes en cours de nidification* *Mike Hopiak / Cornell Lab of Ornithology*	glfs-storm-birds.jpg
11g		IMG_3937_filtered.jpg

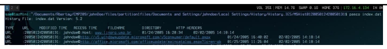
10.12 Event Log

Appendix Number.	Image	Image Name
12a		FileHistory.jpg
12b		MoreFileHistoryCrop.jpg

```
1 2 4                                VOL 35% | MEM 14.7G  SWAP 0.1G  HOME 37G | 172.16.4.134  IN 0K OUT 0K | CPU 0.00%   | BAT 89% CHR
sam@lazMini:~/Documents/Abertay/CMP209/johnDoe/files/partition1files/Documents and Settings/johndoe/Local Settings/History/History.IE5/MSHist012005013120050207$ pasco index.dat
History File: index.dat Version: 5.2

TYPE    URL     MODIFIED TIME   ACCESS TIME     FILENAME        DIRECTORY       HTTP HEADERS
URL     :2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/All%20Users/Documents/My%20Music/Sample%20Music/Doc1.doc      02/03/2005 14:17:40     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@:Host: My Computer   02/03/2005 12:19:07     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///C:/Program%20Files/Real/RealPlayer/Firstrun/1.htm    02/02/2005 15:04:47     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///C:/Program%20Files/Real/RealPlayer/DataCache/Login/index.html        02/02/2005 14:57:13     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/7107298.jpg       02/02/2005 14:20:33     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/kakapo.ram      02/02/2005 15:11:51     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///D:/Prac5/Q3%20Thread%20(Statechart).gif      02/02/2005 15:10:49     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/40m.jpg   02/02/2005 14:43:36     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/177.jpg   02/03/2005 15:01:30     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///C:/birdwatching.doc  02/03/2005 15:49:39     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///D:/Prac4/Prac4.gif   02/02/2005 15:10:16     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/pstbk2b2.htm    02/03/2005 15:02:45     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/Application%20Data/Mozilla/Firefox/Profiles/w4nf3obl.default/cookies.txt       02/03/2005 12:19:07     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@http://www.real.com/intro/index_upsell_manager.html?DC=NSP01C&optin=true&country=gb&language=en-gb&icon=tiscali&LI=en&PBR=10485000     02/02/2005 15:04:20     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/nestboxtips.txt 02/02/2005 14:29:30     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/aa010703a.htm   02/02/2005 14:25:59     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/tn_duck_3.jpg     02/02/2005 14:10:13     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/bob/My%20Documents/My%20Music/ready2fledge.jpg 02/03/2005 15:06:42     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@https://account.real.com/acct/intro/msg.html?msg=fryeur      02/02/2005 15:04:34     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///E:/birds/audio/aggressive_song.wav   02/03/2005 12:22:51     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/Desktop/birdtrans2.jpg 02/03/2005 15:04:40     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/wbpremium_s.jpg   02/02/2005 14:20:19     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///C:/WINDOWS/ODBC.INI  02/03/2005 15:54:06     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/chicks2.jpg       02/03/2005 15:05:03     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///C:/Program%20Files/Adobe/Acrobat%207.0/Reader/Legal/Adobe%20Reader/7.0.0/en_US/license.html  02/02/2005 17:03:40     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@:Host: account.real.com      02/02/2005 15:04:34     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/Application%20Data/Mozilla/Firefox/Profiles/w4nf3obl.default/bookmarks.html     02/03/2005 12:20:20     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///C:/EvanstonWoodpecker.jpg    02/03/2005 14:14:59     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@:Host: www.real.com  02/02/2005 15:04:20     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///E:/birds/Killdeer.jpg        02/03/2005 14:49:29     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/babyscot_young.jpg        02/03/2005 15:00:19     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/babyscot_2weeks1.jpg      02/03/2005 15:00:27     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/newbies2.jpg    02/03/2005 15:05:44     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///C:/Program%20Files/Real/RealPlayer/Firstrun/context.htm      02/02/2005 15:04:40     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/snow_goose.jpg    02/02/2005 14:10:53     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///E:/birds/non%20images/BirdingGuide.pdf       02/03/2005 15:52:01     02/09/2005 11:20:01
URL     :2005013120050207: johndoe@file:///E:/birds/non%20images/BookList.doc   02/03/2005 15:51:54     02/09/2005 11:20:01
```

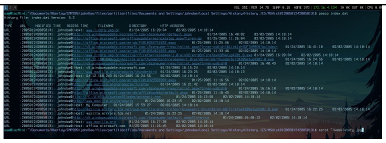
```
1 2 4                                VOL 35% | MEM 14.7G  SWAP 0.1G  HOME 37G | 172.16.4.134  IN 0K OUT 0K | CPU 0
sam@lazMini:~/Documents/Abertay/CMP209/johnDoe/files/partition1files/Documents and Settings/johndoe/Local Settings/History/History.IE5/MSHist012005020920050210$ pasco index.dat
History File: index.dat Version: 5.2

TYPE    URL     MODIFIED TIME   ACCESS TIME     FILENAME        DIRECTORY       HTTP HEADERS
URL     :2005020920050210: johndoe@file:///F:/AlmondMarshGreatBlueHeronStalling.jpg     02/09/2005 17:06:20     02/09/2005 17:06:20
URL     :2005020920050210: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/birds.zip       02/09/2005 11:20:00     02/09/2005 11:20:01
URL     :2005020920050210: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/stuf.doc        02/09/2005 16:57:49     02/09/2005 16:57:49
URL     :2005020920050210: johndoe@:Host: My Computer   02/09/2005 11:20:00     02/09/2005 11:20:01
URL     :2005020920050210: johndoe@file:///C:/Program%20Files/MSN/aggressive_song.wav   02/09/2005 17:00:50     02/09/2005 17:00:50
sam@lazMini:~/Documents/Abertay/CMP209/johnDoe/files/partition1files/Documents and Settings/johndoe/Local Settings/History/History.IE5/MSHist012005020920050210$ scrot ~/MoreFileHistory.jpg
```

10.13 Internet Explorer History

Appendix Number.	Image	Image Name
13		WebHistoryCommand.jpg

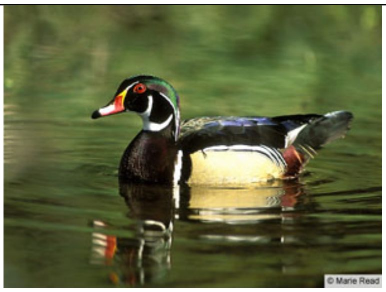
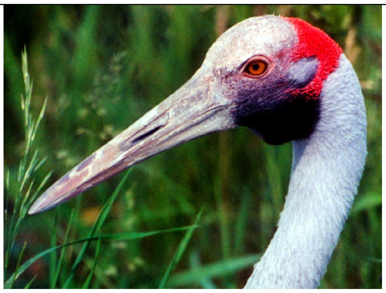
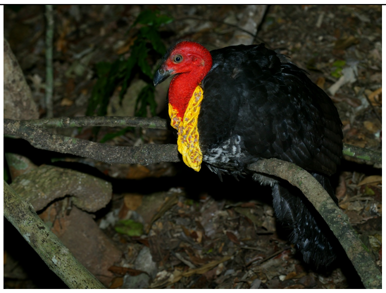
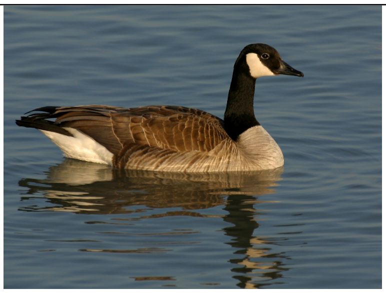
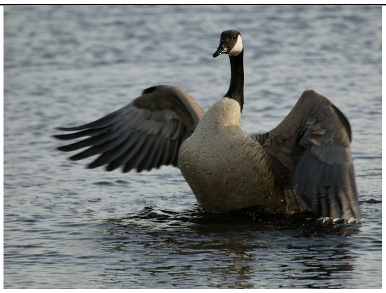
```
1 2 4                                                    VOL 35% | MEM 14.7G  SWAP 0.1G  HOME 37G | 172.16.4.134  IN 0K
sam@lazMini:~/Documents/Abertay/CMP209/johnDoe/files/partition1files/Documents and Settings/johndoe/Local Settings/History/History.IE5/MSHist012005012420050131$ pasco index.dat
History File: index.dat Version: 5.2

TYPE    URL     MODIFIED TIME   ACCESS TIME     FILENAME        DIRECTORY       HTTP HEADERS
URL     :2005012420050131: johndoe@:Host: www.linorg.usp.br     01/24/2005 16:20:34     02/02/2005 14:10:14
URL     :2005012420050131: johndoe@http://v5.windowsupdate.microsoft.com/v5consumer/default.aspx        01/24/2005 16:40:02     02/02/2005 14:10:14
URL     :2005012420050131: johndoe@http://office.microsoft.com/officeupdate/maincatalog.aspx?lc=en-gb   01/25/2005 11:26:04     02/02/2005 14:10:14
```

10.14 Firefox History

Appendix Number.	Image	Image Name
14		WebHistoryCrop.jpg

```
1 2 4                                           VOL 35% | MEM 14.7G  SWAP 0.1G  HOME 37G | 172.16.4.134  IN 0K OUT 0K | CPU 0.0
sam@lazMini:~/Documents/Abertay/CMP209/johnDoe/files/partition1files/Documents and Settings/johndoe/Local Settings/History/History.IE5/MSHist012005012420050131$ pasco index.dat
History File: index.dat Version: 5.2

TYPE    URL     MODIFIED TIME   ACCESS TIME     FILENAME        DIRECTORY       HTTP HEADERS
URL     :2005012420050131: johndoe@:Host: www.linorg.usp.br     01/24/2005 16:20:34     02/02/2005 14:10:14
URL     :2005012420050131: johndoe@http://v5.windowsupdate.microsoft.com/v5consumer/default.aspx        01/24/2005 16:40:02     02/02/2005 14:10:14
URL     :2005012420050131: johndoe@http://office.microsoft.com/officeupdate/maincatalog.aspx?lc=en-gb  01/25/2005 11:26:04     02/02/2005 14:10:14
URL     :2005012420050131: johndoe@http://office.microsoft.com/en-gb/FX010355751033.aspx        01/25/2005 11:25:56     02/02/2005 14:10:14
URL     :2005012420050131: johndoe@http://v5.windowsupdate.microsoft.com/v5consumer/resultslist.aspx?ln=en-us&id=1&LinkId=SOFTWARE&TocIndex=    01/24/2005 16:41:10     02/02/2005 14:10:14
URL     :2005012420050131: johndoe@http://office.microsoft.com/en-gb/FX010354621033.aspx        01/25/2005 11:33:46     02/02/2005 14:10:14
URL     :2005012420050131: johndoe@http://www.linorg.usp.br/mozilla//firefox/releases/1.0/win32/en-GB/Firefox%20Setup%201.0.exe 01/24/2005 16:20:34     02/02/2005 14:10:14
URL     :2005012420050131: johndoe@http://64.12.168.243/pub/mozilla.org/thunderbird/releases/1.0/win32/en-US/Thunderbird%20Setup%201.0.exe      01/24/2005 16:24:56     02/02/2005 14:10:14
URL     :2005012420050131: johndoe@http://v5.windowsupdate.microsoft.com/v5consumer/resultslist.aspx?ln=en-us&id=0      01/24/2005 16:40:43     02/02/2005 14:10:14
URL     :2005012420050131: johndoe@:Host: v5.windowsupdate.microsoft.com        01/24/2005 16:15:24     02/02/2005 14:10:14
URL     :2005012420050131: johndoe@http://www.mozilla.org/products/thunderbird  01/24/2005 16:23:25     02/02/2005 14:10:13
URL     :2005012420050131: johndoe@:Host: 64.12.168.243 01/24/2005 16:24:56     02/02/2005 14:10:14
URL     :2005012420050131: johndoe@http://office.microsoft.com/en-gb/FX010329501033.aspx        01/25/2005 11:16:56     02/02/2005 14:10:14
URL     :2005012420050131: johndoe@http://www.mozilla.org/products/firefox      01/24/2005 16:21:42     02/02/2005 14:10:14
URL     :2005012420050131: johndoe@http://v5.windowsupdate.microsoft.com/v5consumer/resultslist.aspx?ln=en-us&id=6      01/24/2005 16:16:10     02/02/2005 14:10:14
URL     :2005012420050131: johndoe@http://office.microsoft.com/en-gb/officeupdate/default.aspx  01/25/2005 11:16:45     02/02/2005 14:10:14
URL     :2005012420050131: johndoe@file:///C:/WINDOWS/system32/oobe/actshell.htm        01/24/2005 16:13:56     02/02/2005 14:10:14
URL     :2005012420050131: johndoe@http://www.mozilla.org/products      01/24/2005 16:23:15     02/02/2005 14:10:14
URL     :2005012420050131: johndoe@:Host: My Computer   01/24/2005 15:59:27     02/02/2005 14:10:14
URL     :2005012420050131: johndoe@http://mozilla.mirrors.tds.net/pub/mozilla.org/firefox/releases/1.0/win32/en-GB/Firefox%20Setup%201.0.exe    01/24/2005 16:22:25     02/02/2005 14:10:14
URL     :2005012420050131: johndoe@:Host: mozilla.mirrors.tds.net       01/24/2005 16:22:25     02/02/2005 14:10:14
URL     :2005012420050131: johndoe@http://v5.windowsupdate.microsoft.com/v5consumer/default.aspx?ln=en-us       01/24/2005 16:40:12     02/02/2005 14:10:14
URL     :2005012420050131: johndoe@:Host: www.mozilla.org       01/24/2005 16:17:30     02/02/2005 14:10:14
URL     :2005012420050131: johndoe@:Host: office.microsoft.com  01/25/2005 11:16:45     02/02/2005 14:10:14
sam@lazMini:~/Documents/Abertay/CMP209/johnDoe/files/partition1files/Documents and Settings/johndoe/Local Settings/History/History.IE5/MSHist012005012420050131$ scrot ~/WebHistory.jpg
```

10.15 Contents of CrouchingKokako.dll

Appendix Number.	Image	Image Name
15a		brd_WoodDuck.jpg
15b		Brolga.jpg
15c		BrushTurkeyPerching.jpg
15d		CanadaGoose.jpg
15e		CanadaGooseWashing,jpg

15f		ChestnutMandibledToucan.jpg
15g		CrouchingKokako.jpg