Joint Report of
Jack Wilson (1501838)
and
Dr Ian Ferguson

Digital Forensics 2, Abertay Forensics Dept.
Case Against: Mr John Doe

Police Reference Number: (if applicable)
Case Reference No: CDBIJW
PF Reference No: (if applicable)

Contents

List of Figures

1 Summary

As digital forensic examiners with Abertay Forensic Department, we have been requested to assist in evidence acquisition and analysis for any and all digital media seized from the house of Mr John Doe who is accused with possession of indecent images of birds and bird-related material.

We have been summoned to seize all electronic equipment that may hold evidence. Industry-standard digital forensic software and methodologies were used to retrieve evidence that may assist in proving the accused innocent or guilty.

2 Description of Investigation

2.1 Description of Crime(s) Taken Place

John Doe is accused of holding numerous indecent images of birds and bird-related materials including (but not limited to) accessing birdwatching websites, guides on birdwatching expeditions and tips on building and maintaining bird boxes. Despite recovering over 100 files of interest from the suspect's PC, most of the files were created within days of each other in separate 'episodes'. Each 'episode' is listed and described (in chronological order) below:

Episode 1 - Creation of Image Using Sony Cybershot Camera

This episode took place on 30/12/2002 and contained the creation of one image of a bird (titled 'BC7 feeding the birds.jpg' with underscores to obfuscate the file) that was created at 12:28:49 GMT using a Sony Cybershot camera. This image was also located in the Thunderbird Mail Client application folder.

Episode 2 - Creation of Image Using Canon EOS-1DS Camera

One image of a bird was created with the Canon EOS-1DS camera at 16:14:10 GMT on 29/01/2003. The same image exists in two locations on the computer under two different file names: *f0002368.jpg* and *BellbirdJumpingOffBranch.jpg.*

Episode 3 - Creation of Images Using Canon PowerShot SD100 Camera

A total of 102 images were recovered from a Canon PowerShot SD100 camera. A large majority of these images related directly to birds or birdwatching. This is discussed further in *Section 2.4.2* and the images are available to view in *Appendix 1, Section 6.1.2.* The date of creation for these images ranges from 09/06/2004 19:02:28 BST to 27/06/2004 18:28:34 BST and would indicate a birdwatching field trip.

Episode 4 - Internet Browsing Session/Creation of Several Files of Interest

Throughout 02/02/2005, between 14:18:53 GMT and 16:46:32 GMT, several files of interest were created and several files were viewed:

- A text file (nestboxtips.txt) was recovered from the johndoe user section of the hard drive that contained information on building and maintaining bird boxes. The file was created at 14:29:30 GMT on 02/02/2005. This artefact is discussed further in *Section 2.4.9* and the contents of the file can be viewed in *Appendix 6.1.9.*

- An audio file (kakapo.ram) that was within the johndoe section of the hard drive was created at 15:11:41 GMT on 02/02/2005. This was an audio file used to stream from a remote website. The remote website (at the time of the investigation) was not working, so the audio could not be streamed. Despite this, the filename (Kakapo) is also a known breed of bird.

- A word document (birdwatching.doc) was created at 16:25:10 GMT on 02/02/2005. This contained a comprehensive guide to preparing for a birdwatching trip. This artefact is discussed further in *Section 2.4.5.*

- An encrypted file (birdpics.gpg) that was found in johndoe's user account was created on 02/02/2005 at 16:46:32 GMT. This was found to contain several indecent images of birds when successfully decrypted. This artefact is discussed further in *Section 2.4.3* and the recovered images of birds can be viewed in *Section 6.1.5*.

- Web browser history revealed that several of the recovered indecent images of birds were viewed alongside the web page aa010703.htm during an internet browsing session. This is further discussed in *Section 2.4.4*.

Episode 5 - Creation of Several Files of Interest

Between 12:08:40 GMT and 14:45:17 GMT on 03/02/2005 several files of interest were created:

- A .dll file (CrouchingKokako.dll) was created at 12:08:40 GMT on 03/02/2005 that was actually a compressed .zip file with the extension changed to .dll as an attempt to hide the file from forensic recovery. The file contained several indecent images of birds. This artefact is discussed further in *Section 2.4.6* and the recovered images of birds can be viewed in *Section 6.1.6*.
- One audio file (aggressive_song.wav) was created on 03/02/2005 at 12:23:00 GMT.
- A Microsoft Word document (Doc1.doc) was located in the johndoe user account of the hard drive. This document was created on 03/02/2005 at 14:19:12 GMT and contained one indecent image of a bird within the document. This artefact is discussed further in *Section 2.4.10* and the contents of the document can be viewed in *Section 6.1.10*.
- An executable file (FantailFrontView.exe) was detected as having the wrong extension in Autopsy. The file extension was determined to be .jpg. Changing the extension revealed a single image of a bird. This was another attempt to hide an inappropriate image of a bird from forensic recovery. This file was created on 03/02/2005 at 14:45:17 GMT. This evidence artefact is discussed further in *Section 2.4.7* and the image recovered can be viewed in *Section 6.1.7*.

Episode 6 - Email Conversations

Several emails of interest involving the email address jdoe@example.com were discovered in the Thunderbird Email Client folder. All email conversations were received on 09/02/2005 at 11:08:01 GMT. There were four conversations with a person called ‘Ben Forbes’, and one email from a mailing list involving birds. The contents is discussed further in *Section 2.4.14* and the images of birds recovered from the email client can be viewed in *Section 6.1.12*.

2.2 Description and Recovered/Examined Files

2.2.1 Acquisition

During the raid of the Mr John Doe’s property, several items were seized for further investigation at the forensics lab. All seized items were located in one area, at a computer desk. The items were powered off, meaning no potential evidence existed in RAM or on the network. Live imaging of the disk was also unnecessary because of the powered-off state.

Photographs with evidence tags for all devices seized can be viewed in *Appendix 2*.

Table 1: Recovered Items

Exhibit Reference	Name/Model	Description	Serial Number
CDBIJW-DESKTOP	HP EliteDesk	HP Desktop Computer	CZC62498YL
CDBIJW-MONITOR	HP EliteDisplay E202	HP Computer Monitor	3CQ6103S2V
CDBIJW-KEYBOARD	HP Computer Keyboard	HP Computer Keyboard	n/a
CDBIJW-MOUSE	HP Computer Mouse	HP Computer Mouse	n/a
CDBIJW-PHOTOGRAPH	n/a	Photograph of boat	n/a

After seizure, all evidence was stored securely in an evidence locker within the Abertay Forensics Department building. The relevant chain of custody forms were also recorded to track the which police and forensic personnel handled the evidence throughout the investigation.

Following the relevant chain of custody process throughout the entire investigation ensures that the evidence was left pristine, and untampered. The chain of custody document can be viewed in *Figure 96* in *Appendix 5*.

2.3 Methodology

2.3.1 Preservation

After signing the evidence out from the evidence locker, the hard disk drive was removed from the HP computer, preventing any data from being modified. The computer was booted to the Basic Input/Output System (BIOS), and the date and time of the BIOS clock were cross-checked with the watch of the forensic investigator. This ensured that any dates/times presented alongside evidence were presented accurately, or the appropriate date/time offset was applied if there was any skew in date/time. The date and time were found to be accurate, as shown in Appendix 3.

The next stage of the process involved creating an MD5 checksum of the suspect's hard drive. This is a sequence of numbers and letters that uniquely identifies the hard drive's contents, as if one piece of information changes the checksum will change substantially.

Next, an exact clone of the suspect's hard disk drive was created as a .dd file. Creating this clone, and working exclusively from it ensured that the original hard drive (and the evidence on the drive) were left untouched and untampered. An MD5 checksum of the .dd file was taken. The two checksum's matched, confirming that the clone of the hard drive was perfectly accurate. The MD5 checksum for the suspect hard drive is:

d63dd1b8917ca28bac7c955fc3b6cd25

2.3.2 Antivirus Scan

An antivirus scan was conducted on the disk image after seizure, this was to ensure no malware was present on the drive that could potentially install or download indecent images of birds. Clamscan/ClamAV was used, and the scan results indicated that there was no malware or viruses present on the suspects hard drive. This is shown in *Figure 94* in *Appendix 4*.

2.3.3 Physical and Logical Search

Having a copy of the disk allows for different types of searching. The first search method is called a physical search, which searches the contents of the .dd file as one entire file. With this method, no filesystem exists, more complex searches can be undertaken and deleted files can be recovered with the digital forensic software *Autopsy*.

The second search method is a logical search. This involves treating the disk image as a hard drive, not as a single file. The file system and the registry can be explored to find devices previously connected to the computer.

Both methods require the use of a write blocker. This device prevents any data from being written to the hard drive, and prevents any evidence from being modified or tampered with, either purposefully or accidentally.

2.4 Analysis

2.4.1 Disk Information & Partition Table

The first stage of the analysis included examining the various partitions contained on the hard drive, as well as determining the user accounts on the operating system. The partitions included:

- Volume 1 (vol1): Unallocated Space (63 bytes)
- Volume 2 (vol2): NTFS/exFAT Formatted Partition (3.14GB)
- Volume 3 (vol3): Unallocated Space (2.62GB)

Despite showing as an unallocated partition (meaning that it was not intended to store any files), volume 3 contained numerous files including numerous indecent images of birds and a guide for bird watching. This would indicate an effort to conceal these files.

Three user accounts were also found on the Windows partition of the hard drive, the account names were:

- johndoe
- jane
- bob

2.4.2 Images From Cameras

Metadata revealed that images recovered from the suspect's computer were taken on three different cameras:

- Canon PowerShot SD100
- Canon EOS-1DS
- Sony Cybershot

Canon PowerShot SD100

A total of 29 images directly relating to birds, birdwatching and bird paraphernalia were found to be taken on a Canon PowerShot SD100 camera. These images are shown from *Figure 30* to *Figure 58* in *Section 6.1.2*. The majority of the images related directly to birds and birdwatching, however, further images of a group of people were discovered that may indicated a group birdwatching expedition. This can be proven by matching the date and time that the images of birds were taken with the date and time that the image of the people pictured in the photographs (using the date and time information contained within the photograph). These dates and times were mentioned in the description of *Episode 3*, above.

Canon EOS-1DS

Just one image was found that was taken on a Canon EOS-1DS, but was found in 2 different locations (with the same MD5 checksum). Both of the images were found in unallocated disk space, as an attempt to hide the files. *BellbirdJumpingOffbranch.jpg* was found in the root of vol3, and *f0002368.jpg* was found in vol3/$CarvedFiles. The images can be viewed in *Section 6.1.3*.

Sony Powershot

Just one image was found to be taken on a Sony Powershot camera, and the image was retrieved from the inbox folder under the Thunderbird Mail Client. There was also an attempt to hide the image from forensic recovery, by changing the file extension from .jpg to ._j_p_g_.

2.4.3 GPG File

An encrypted .GPG file was discovered in *Document and Settings/johndoe/My Documents*. The file was protected with both a public/private keypair, and a password. The public and private keys (pubring.gpg & secring.gpg) were found in *Documents and Settings/johndoe/Application Data/GnuPG*.

The password protecting the file was determined to be 'arran'. There was three potential ways to discover the password:

- Brute-force guess the password using a program such as *John The Ripper.* This method would make hundreds of guesses per second guessing every possible password until the correct password was found.
- The picture on the desk seized during the raid (shown in *Figure 92* in *Appendix 2*) was a photograph of the Isle of Arran.
- An email conversation was recovered which contained a word encoded in Base64 (a technique to obfuscate the word). This word decoded to 'arran'.

Entering the password released a compressed .tar.gz file. Uncompressing the file revealed five inappropriate images of birds (shown in *Section 6.1.5*).

2.4.4 Birds Website

A web page aa010703.htm was discovered in johndoe's user folder on the hard drive. This website contains numerous references to birds, birdwatching, bird photography and birdboxes. Browser history would indicate that the webpage was visited on during *Episode 4*, detailed above.

2.4.5 Birdwatching.doc

A file (birdwatching.doc) was discovered in the root directory of volume 2 (e.g. C:\). This document (shown in *Section 6.1.8*) is a comprehensive guide that includes details on going on a birdwatching expedition in Thailand, how to identify birds, the best times of day to watch for birds, tips for birdwatching and contact details for birdwatching associations. The same file was also discovered in volume 3 under a different name: *f0005504.doc.*

2.4.6 Birds Embedded in Fake .dll File

Every file on the operating system was hashed (which gives a unique identifier for each file). This was cross-referenced with a database of known 'good' hashes. This process highlights files which have previously remained unseen. A .dll file (CrouchingKokako.dll) was highlighted, which was an abnormality since most Windows dll files are in the list of known good hashes. The file was later determined to be a compressed .zip file, which when unzipped revealed seven inappropriate images of birds (shown in *Section 6.1.6*).

2.4.7 Image Hidden in Fake .exe file

Autopsy detected a file mismatch on a file called 'FantailFrontView.exe' file and suggested the file was actually a .jpg image file. Changing the file extension revealed another inappropriate image of a bird shown in *Section 6.1.7.*

2.4.8 kakapo.ram

A .ram file was discovered, titled *kakapo.ram.* This was determined to be an audio file which streams audio from a remote website, however, the file could not be played as the streaming source website was now inactive, and no archived copies of the website could be found. It is noteworthy that a kakapo is a known breed of bird

2.4.9 nestboxtips.txt

A text file *nestboxtips.txt* was discovered on the suspect drive which contained tips on placement of a nest box. This included advice such as cleaning and maintenance next boxes, as well as the positioning and common types of next boxes. A full screenshot of the document is available in *Section 6.1.9.*

2.4.10 Doc1.doc

A Microsoft Word document was recovered that contained a partial image of a bird, specifically the right wing. Opening the document in Microsoft Office allowed for the image to be scaled down, revealing the full image of a bird. A screenshot of the document is available under *6.1.10*.

2.4.11 PDF Files

Three PDF files were discovered in volume 2 of the suspect's hard drive. Due to the size of these documents they are included fully as a separate documents, however previews of the documents can be viewed in *Section 6.1.11*. These included details of birding sites around Perth, Western Australia (f0180344.pdf), a University of California newsletter which details birds spotted at the University of California Botanical Garden (f0273688.pdf), a birding guide (f0327896.pdf)

2.4.12 .wav File

A single .wav audio file (aggressive_song.wav) was discovered in a folder associated with MSN messenger. This audio file appeared to be a bird call/whistle. The file is attached as a separate exhibit, rather than in the appendices of this report.

2.4.13 Discovered Email Addresses

- jdoe@mail.example.com
- jdoe@example.com
- jdoe@netscape.net
- johndoe@example.com
- johndoe@microsoft.com
- johndoe@netscape.net
- johndoe@office.microsoft.com
- johndoe@real.com
- johndoejohndoe@example.com

2.4.14 Email Account Contents

Four emails were received from ben@example.org that included a total of seven inappropriate images of birds and one email was received from mailinglist@birds.example.com which included several paragraphs explaining how to identify birds. Ben Forbes was also observed to thank jdoe@example.com for sending some pictures. Removing the obfuscation from the file names, the images recovered from the suspect's hard drive (shown in *Section 6.1.12*) would match the files referred to in the email metadata. These filenames were:

- 7EYBTELKF1KAN.jpg
- IMG\3937\filtered.jpg
- cute\penguin.jpg
- BC7 feeding the birds.jpg
- glfs-storm-birds.jpg

- colorful-birds.jpg
- gawall8.jpg

2.4.15 Removable Drive

Throughout the investigation, references were made to files on the E:\drive, which was a removable drive (such as a USB thumb drive or external hard drive). Further evidence of inappropriate images of birds may exist on this drive, but it could not be determined without direct access to the drive.

2.4.16 Registry Examination

Registry examination offered further confirmation that the removable drive (assigned the drive letter E:\) was connected to the computer, however, without seizure of the drive it could not be fully examined. Registry analysis also showed John Doe as the registered owner of the computer that was seized.

3 Conclusion

In total, 74 images relating to birds and birdwatching were recovered from the suspect's hard drive. Additionally, three PDF files, two word documents and two audio files relating to birds were also recovered.

Registry examination showed that John Doe was the registered owner of the computer. A large percentage of the recovered evidence was discovered either within the suspect's user folders on the hard drive, or in association with email addresses that could belong to the suspect. Some files were recovered from unallocated hard drive space, and a minute amount of bird-related material was discovered in other user's directories.

An extensive effort was undertaken to hide certain files; including the encrypted file that was in the suspect's area of the hard drive, the files with names and extensions changed in an attempt to evade forensic recovery and the numerous images of birds recovered from the unallocated section of the hard drive.

An email conversation between John Doe and a person called 'Ben Forbes' further indicates the suspect's direct involvement with inappropriate images of birds, where the suspect willingly received inappropriate images of birds from Ben, and was thanked by Ben for sending images.

The antivirus/malware scan by ClamScan/ClamAV showed no presence of any malware or viruses, thus removing the probability of the inappropriate images of birds being inadvertently downloaded by a computer virus.

4 Glossary of Terms

BIOS
BIOS (Basic Input/Output System) is firmware installed on every computer. Loading to the BIOS does not load files from a hard drive, nor does it change the contents of a hard drive in any way. For this reason, loading to the BIOS to check time-skew on the computer is deemed safe.

RAM
RAM (Random Access Memory) is a form of computer storage that only contains data (such as open programs and files) when a computer is powered on. The RAM is cleared when a computer is powered off. In the case of a computer still being powered on when seizure takes place, it is important not to power off the computer immediately to preserve the contents of the RAM, as it could contain evidence.

Partition
A hard drive can be split into multiple sections called partitions. This can be for a variety of reasons

including installing multiple operating systems (one per partition) or to separate the files required for an operating system from a user's personal files. Having hidden partitions or partitions that have not been allocated space are techniques that are well known techniques to hide files.
Encryption
Encryption is the process of jumbling the contents of a file or hard drive, therefore making the contents of the file or hard drive unreadable without the decryption password. The decryption password can be guessed using a computer program, and the shorter and simpler the password is, the easier and faster it is to guess.

5 Equipment Required for Court Proceedings

The equipment and evidence listed below is required for the court proceedings:

- Evidence:

  The suspect's seized PC (Evidence Number: CDBIJW-Desktop) including the hard drive.

- Specialist Equipment

  A workstation with Ubuntu - allows the drive to be mounted through loopback mounting.

  A second partition on the workstation for Windows - required for specialist forensic software.

  Autopsy 4 - Specialist digital forensics program for evidence recovery.

  MD5deep - A program that verifies the checksum of the disk to verify integrity.

  GPG - Allows for decryption of birds.gpg file.

- A projector or large television for the courtroom to view evidence.

6 Appendices

6.1 Appendix 1 - Images of Birds

6.1.1 Miscellaneous Images Discovered on Suspect Computer

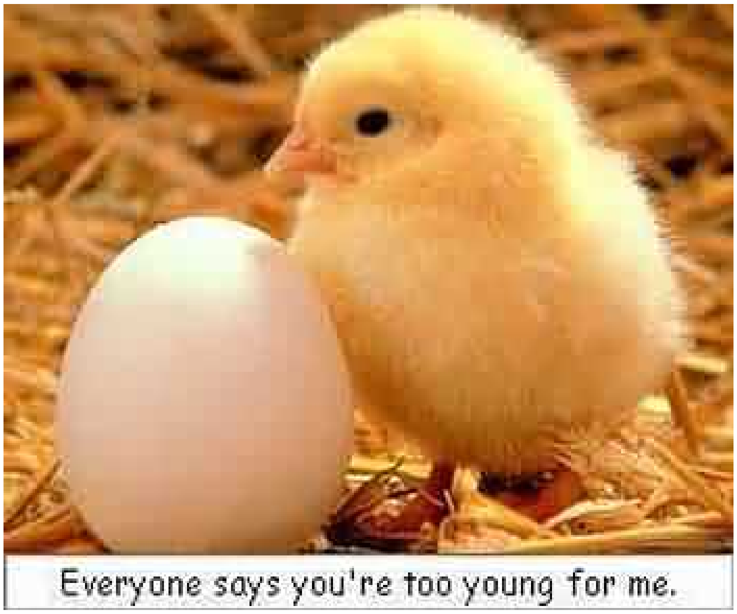


Figure 1: 177.jpg

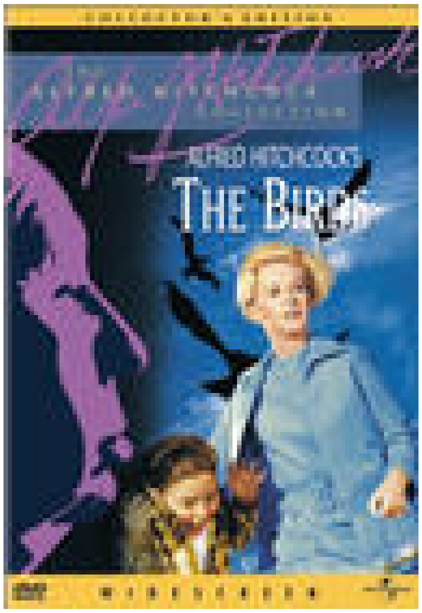


Figure 2: 40m.jpg

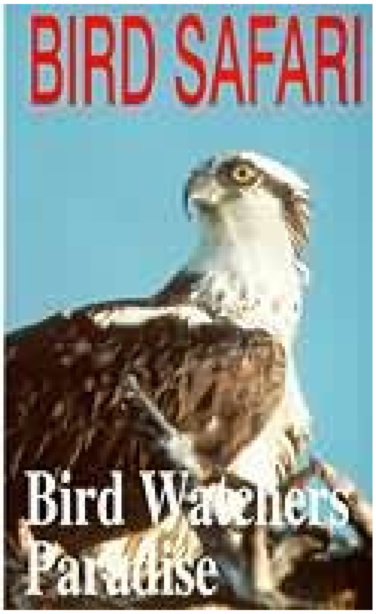


Figure 3: 7107298.jpg

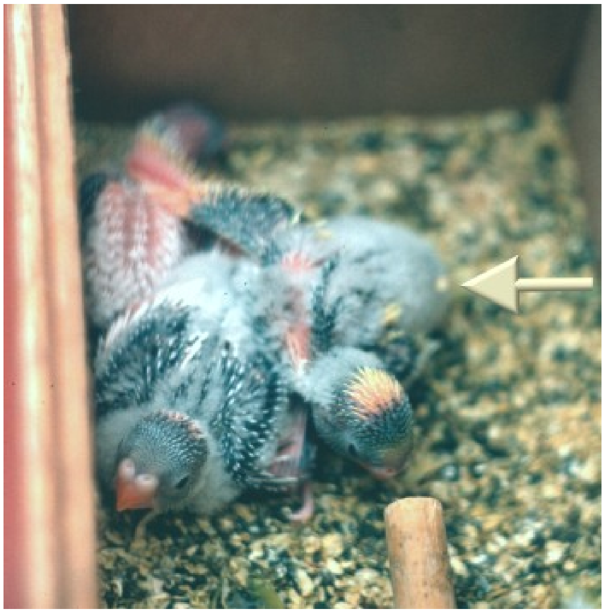


Figure 4: babyscot_2week1.jpg

Figure 5: babyscot_vyoung.jpg

Figure 6: tn_duck_3.jpg

Figure 7: wbpremium_s.jpg (Image of Bird Seed)

Figure 8: f0000536.jpg

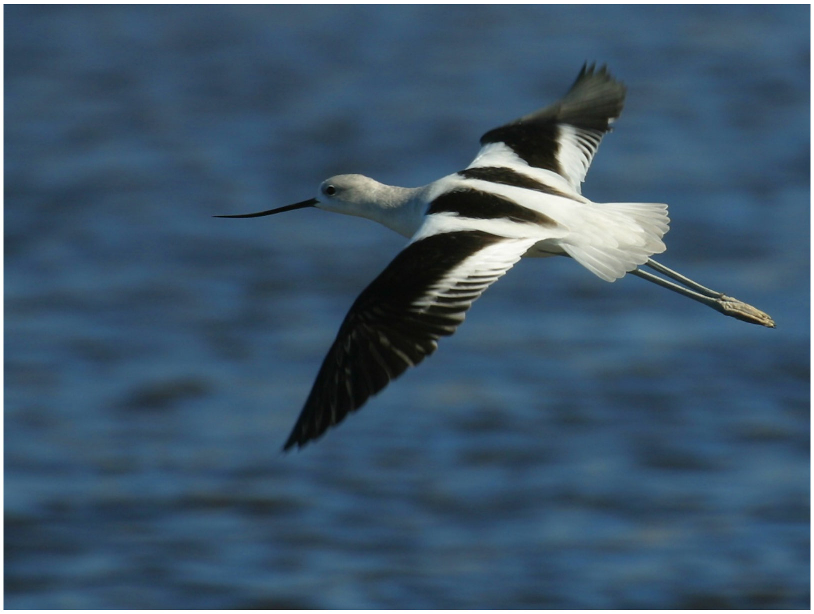


Figure 9: f0000888.jpg

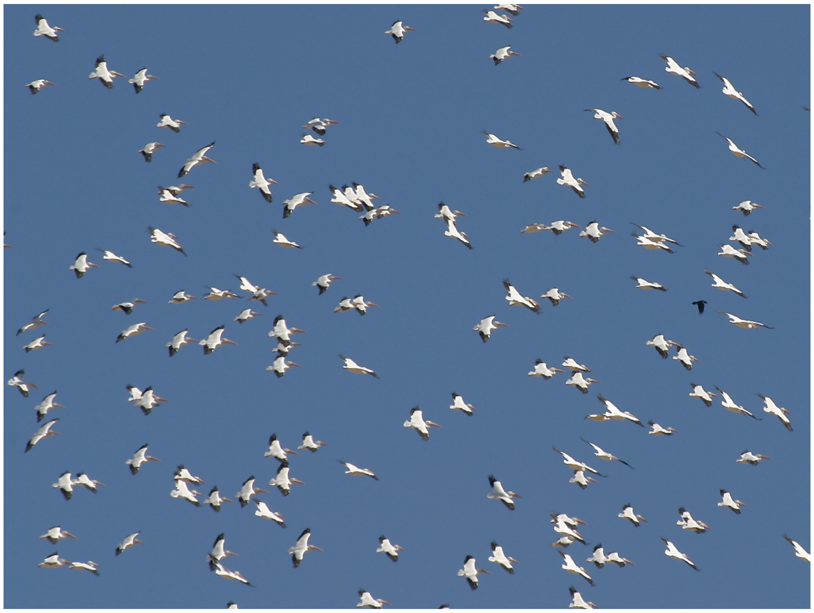


Figure 10: f0001224.jpg

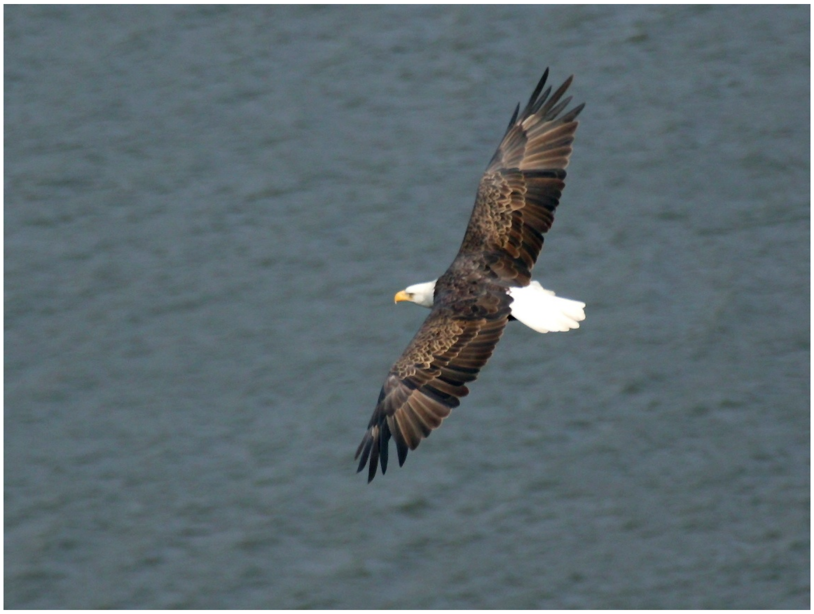


Figure 11: f0001624.jpg

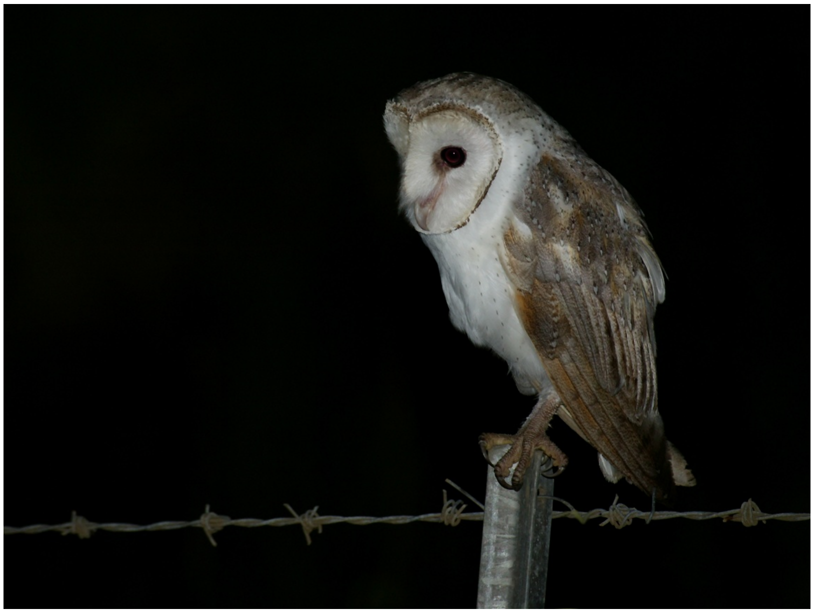


Figure 12: f0002088.jpg

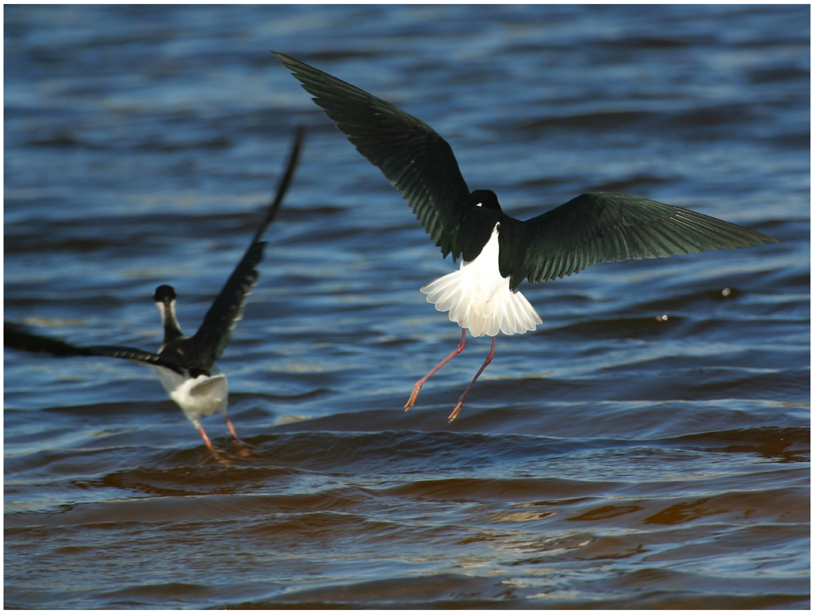


Figure 13: f0003752.jpg

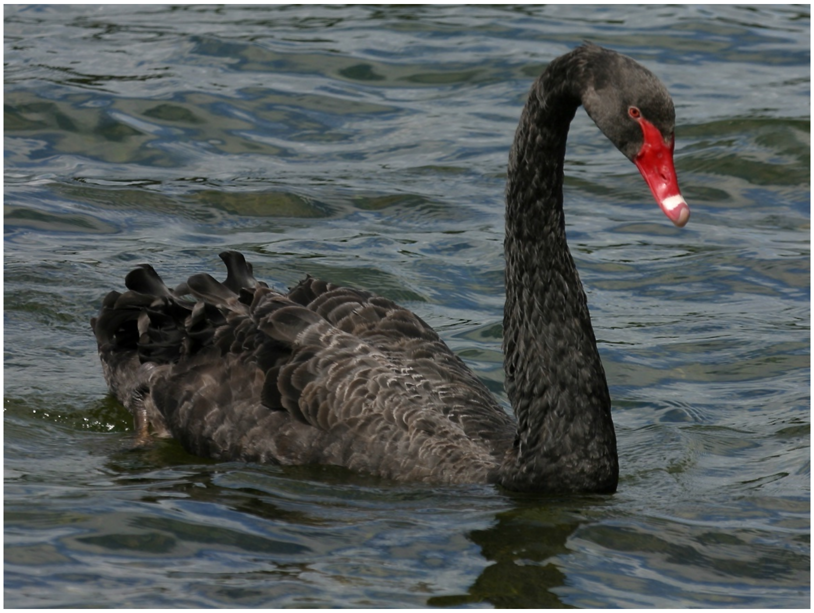


Figure 14: f0004248.jpg

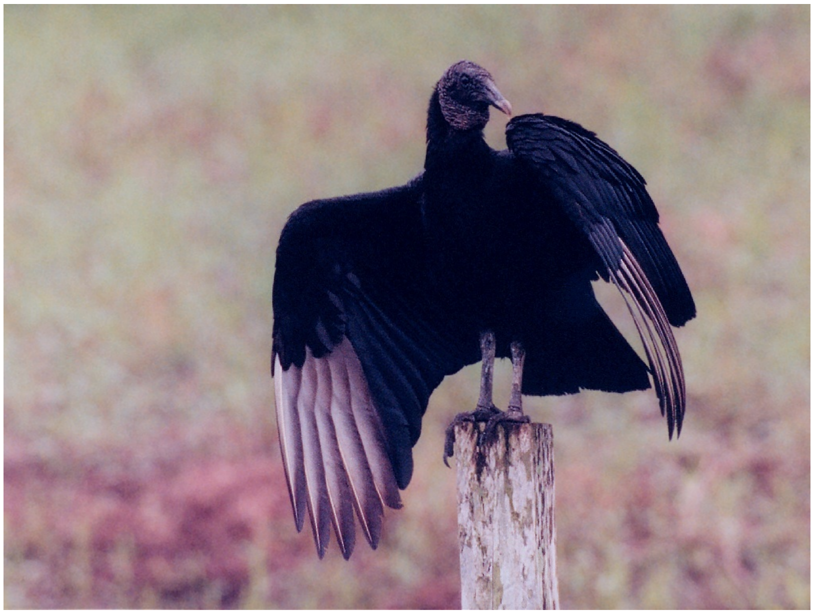


Figure 15: f0004856.jpg

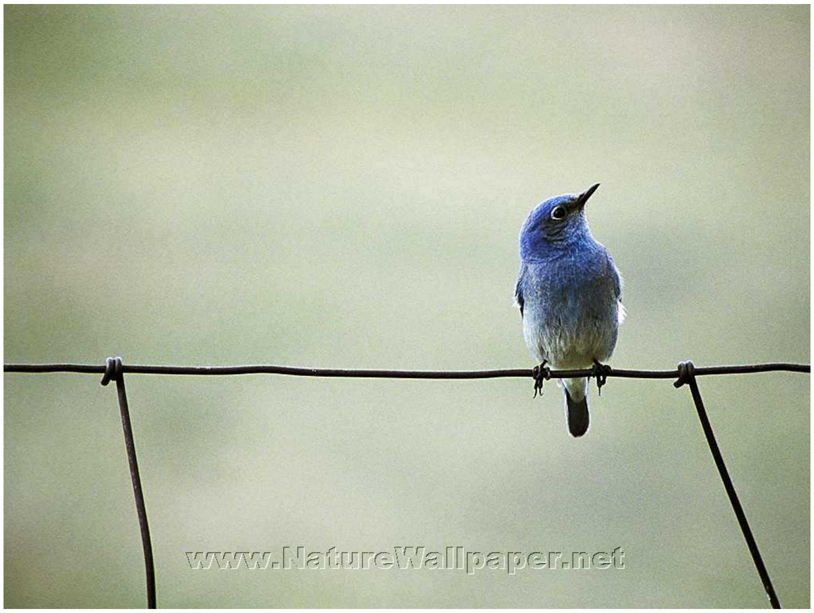


Figure 16: f0005296.jpg

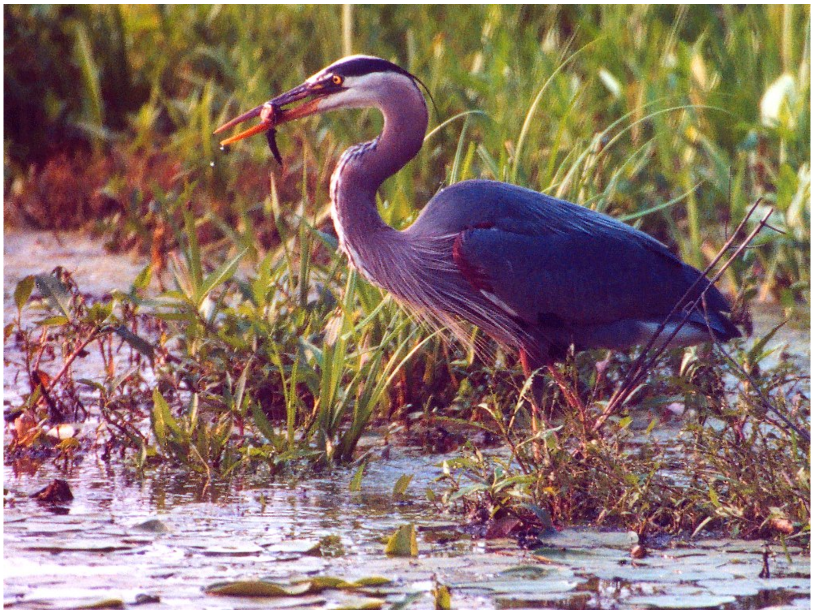


Figure 17: f0005640.jpg

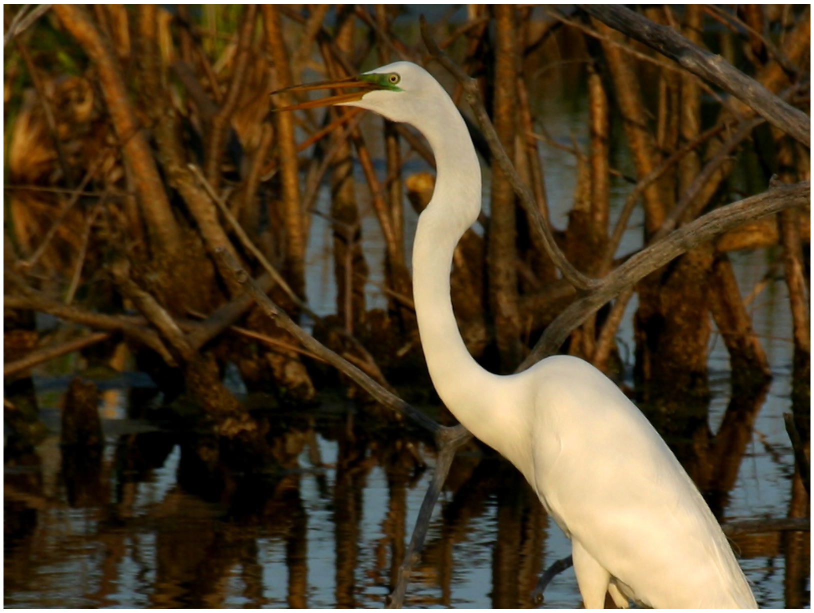


Figure 18: f0006264.jpg

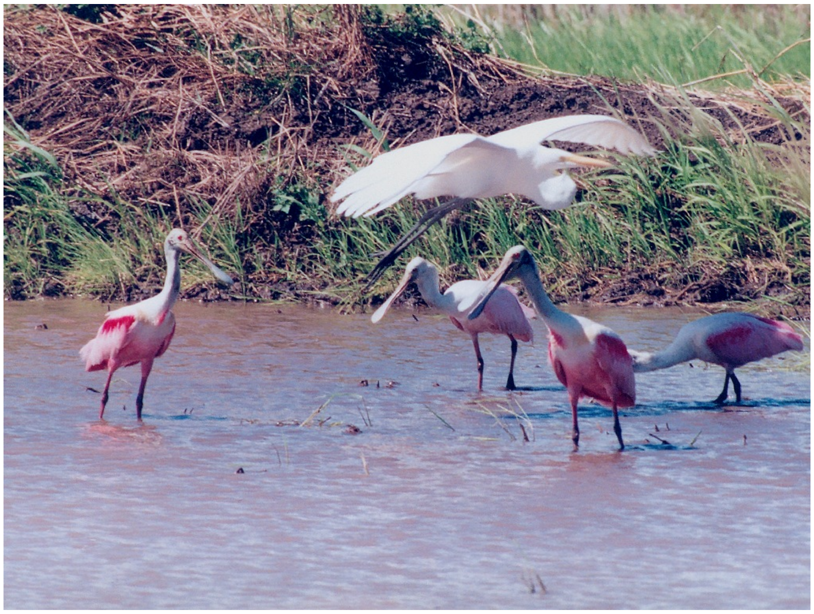


Figure 19: f0006704.jpg

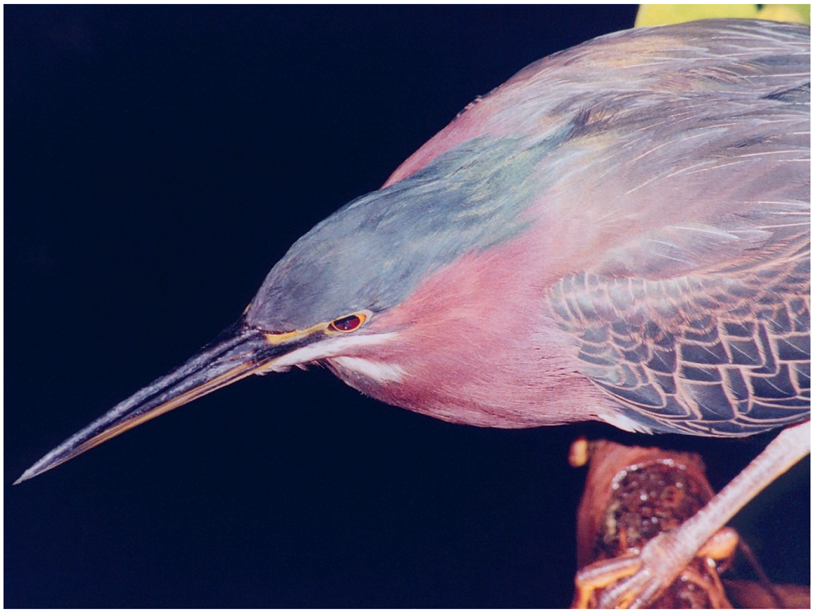


Figure 20: f0007432.jpg

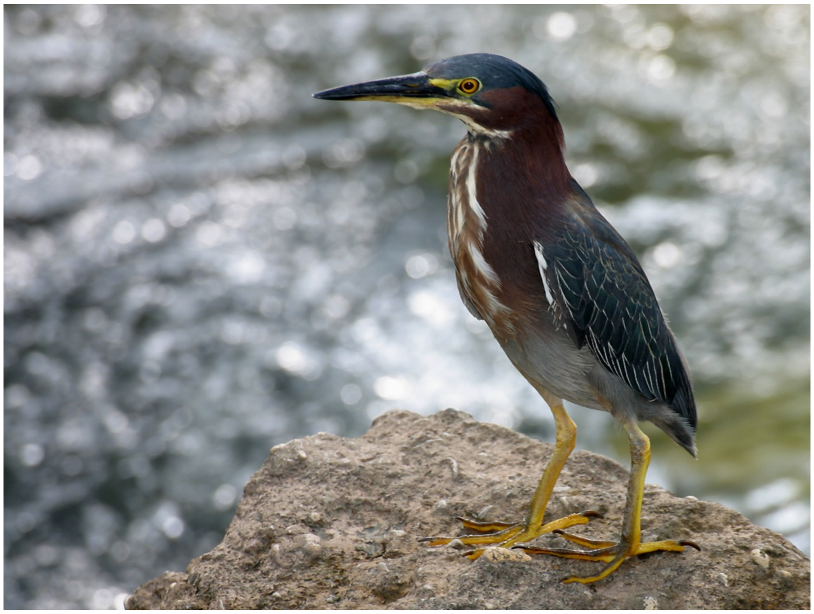


Figure 21: f0007896.jpg

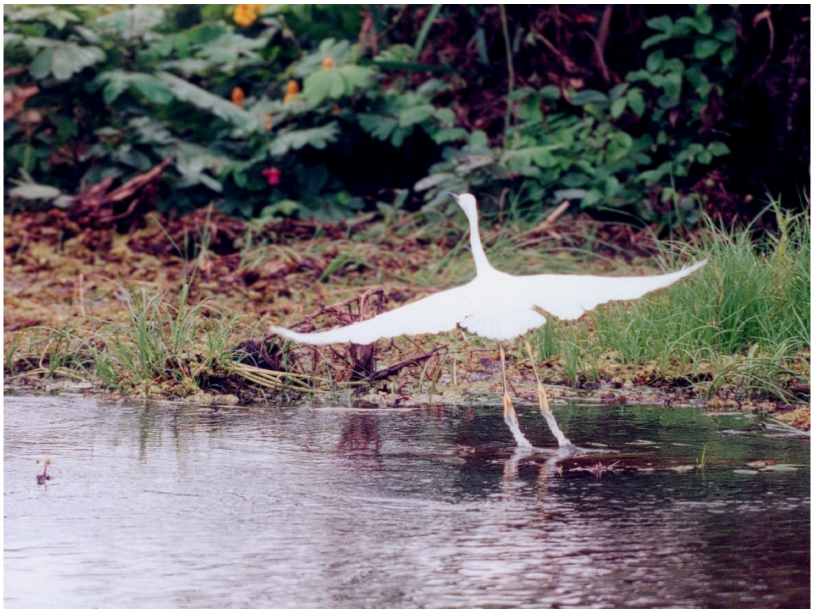


Figure 22: f0008424.jpg

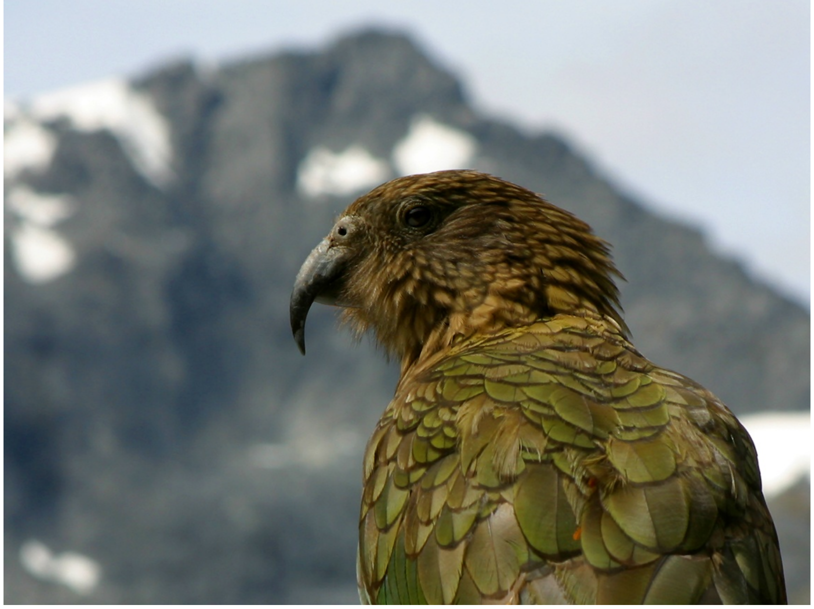


Figure 23: f0009552.jpg

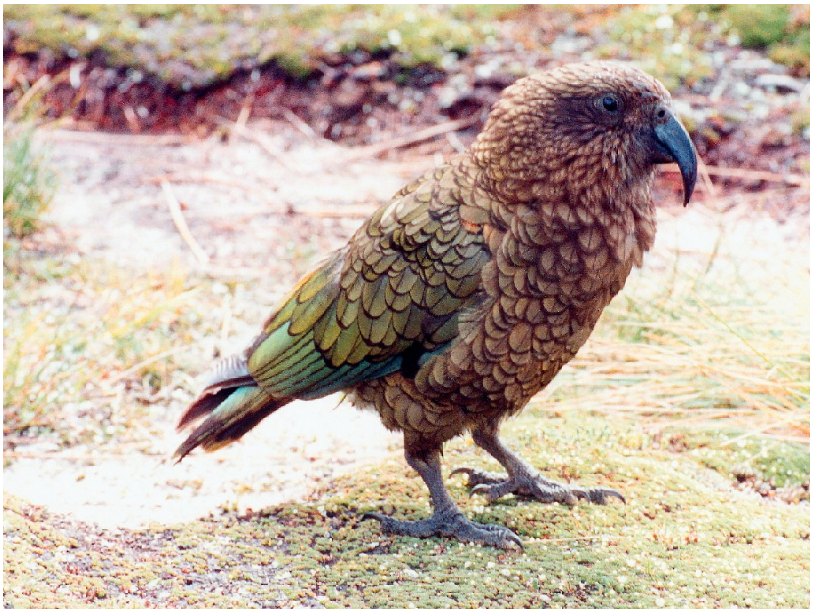


Figure 24: f0009976.jpg

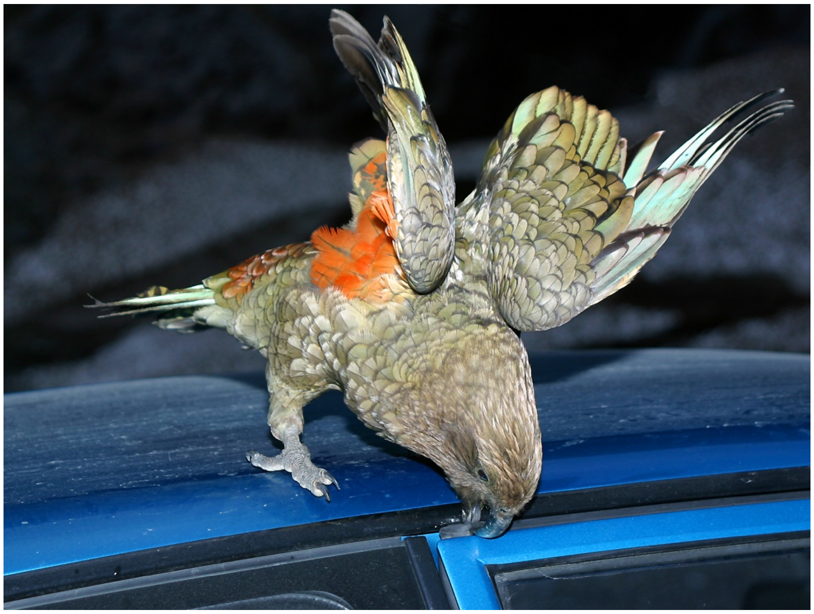


Figure 25: f0010568.jpg

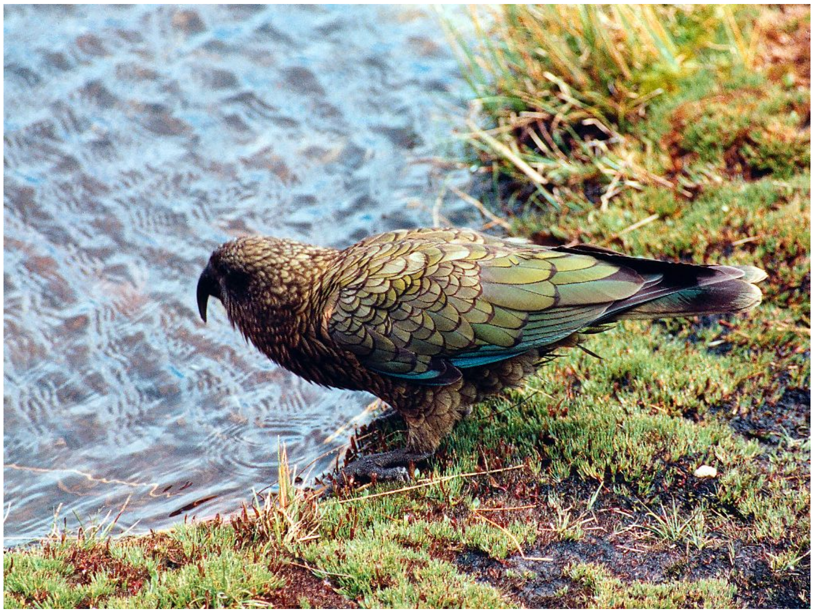


Figure 26: f0011192.jpg

Figure 27: BaldEagle7oClock.jpg

Figure 28: Df1.jpg

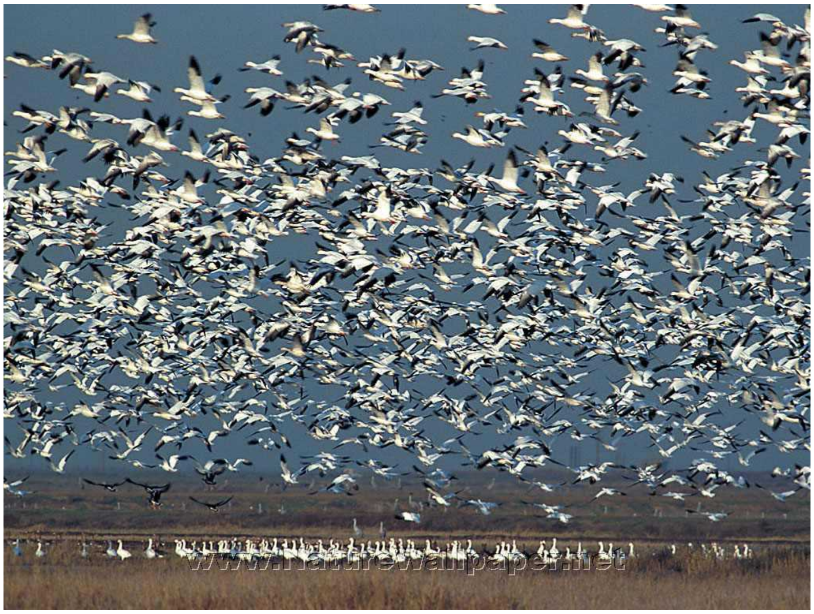


Figure 29: snow_geese.jpg

6.1.2 Images From Canon PowerShot SD100 Camera

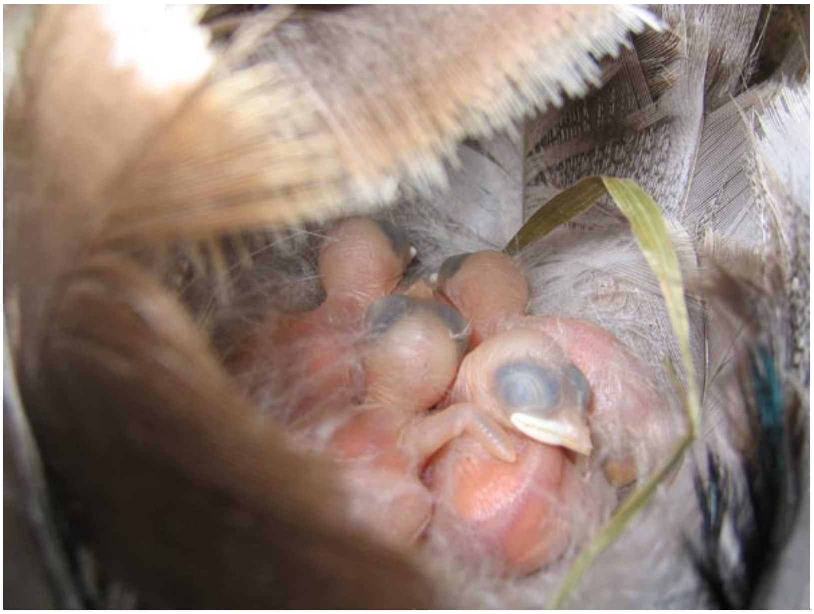


Figure 30: newbies2.jpg

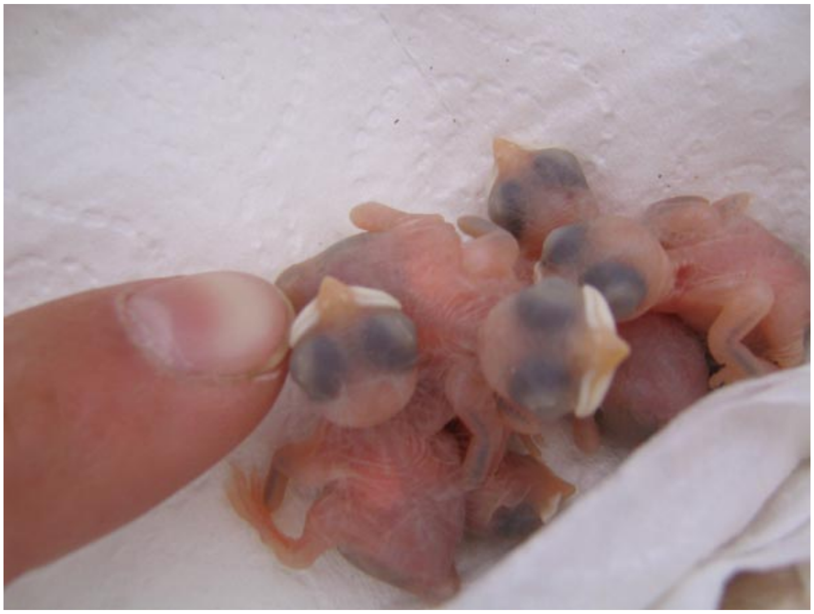


Figure 31: chicks2.jpg

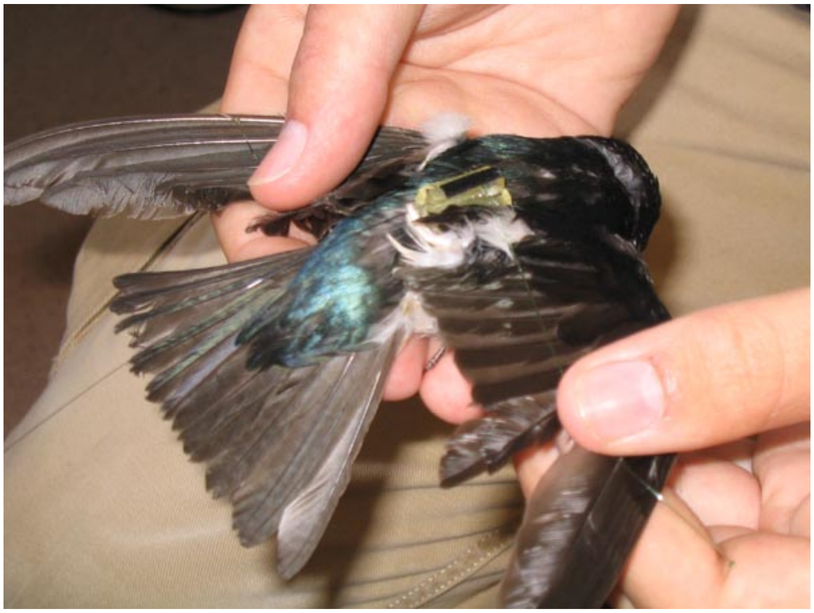


Figure 32: birdtrans2.jpg

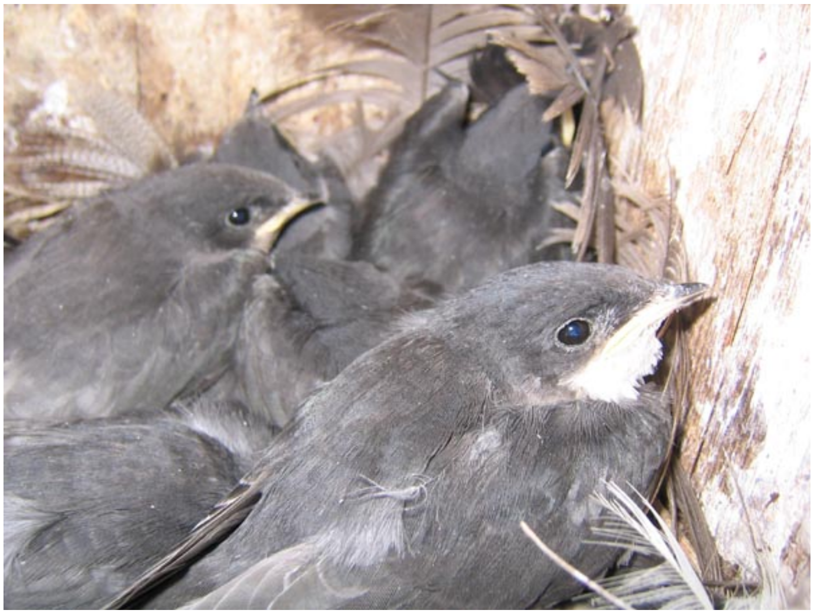


Figure 33: ready2fledge.jpg

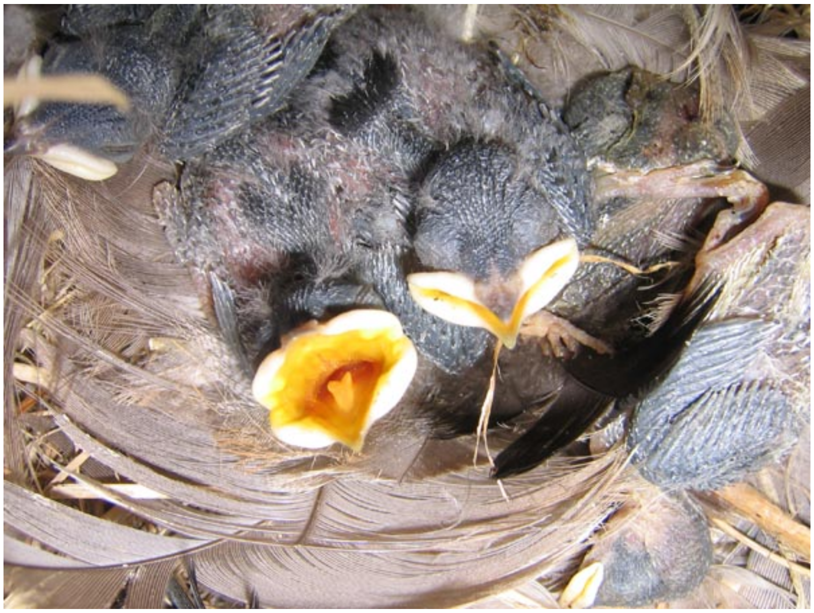


Figure 34: f0592136.jpg

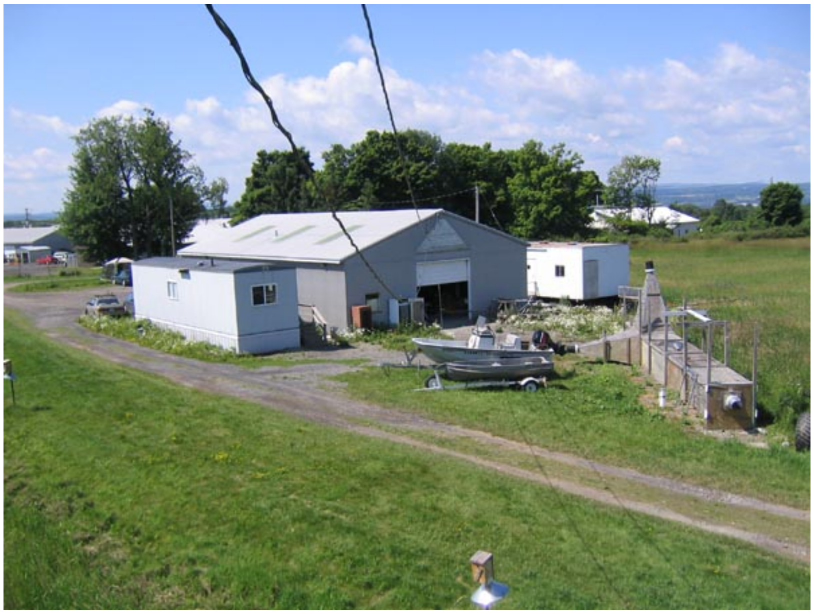


Figure 35: f0561264.jpg (Contains Bird Box in Image)

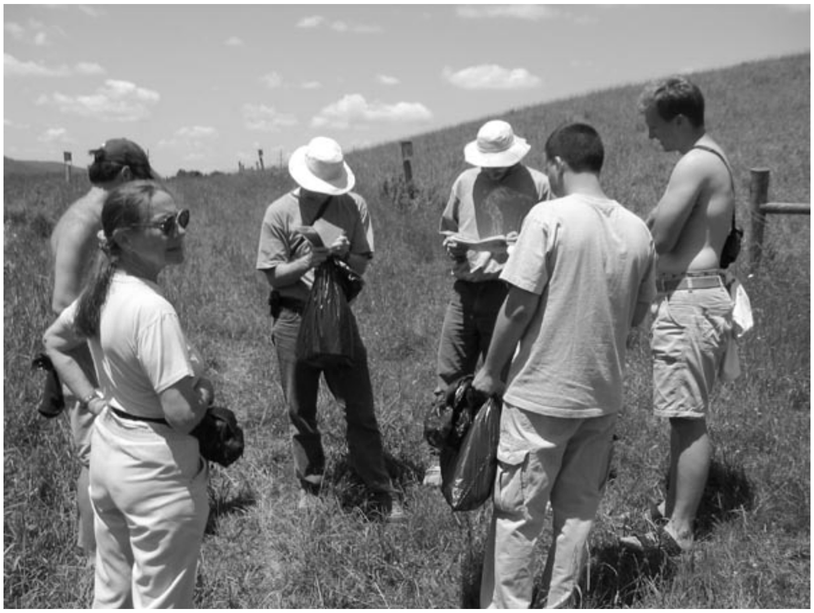


Figure 36: f0552688.jpg (Possible Evidence of a Birdwatching Trip)

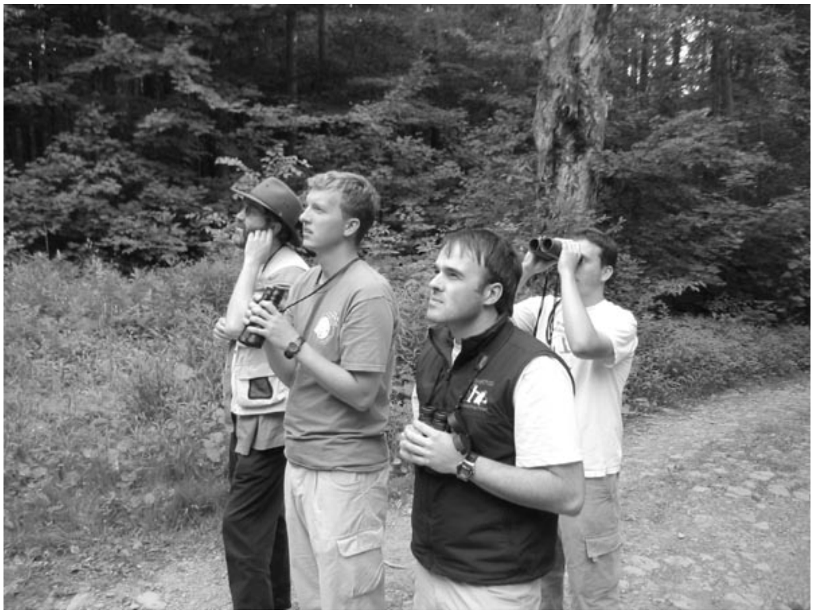


Figure 37: f0545184.jpg (Possible Evidence of a Birdwatching Trip)

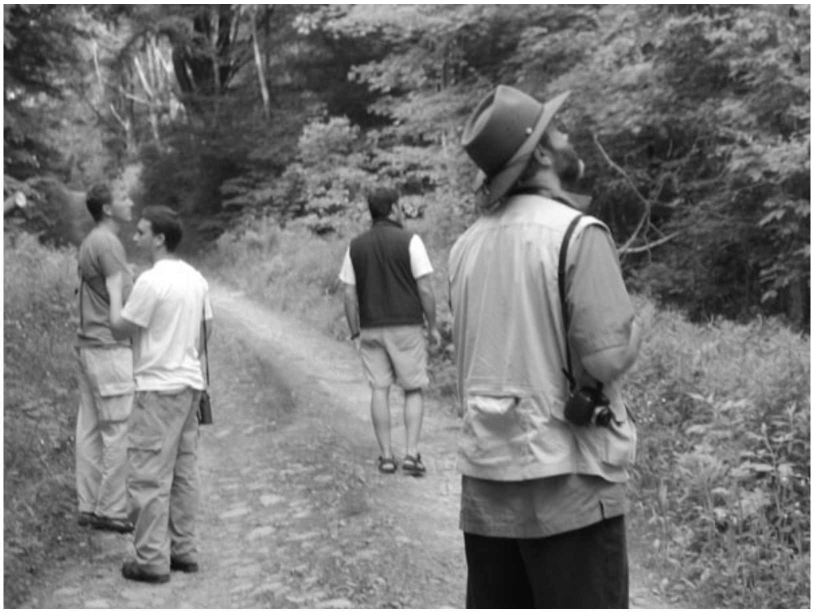


Figure 38: f0544152.jpg (Possible Evidence of a Birdwatching Trip)

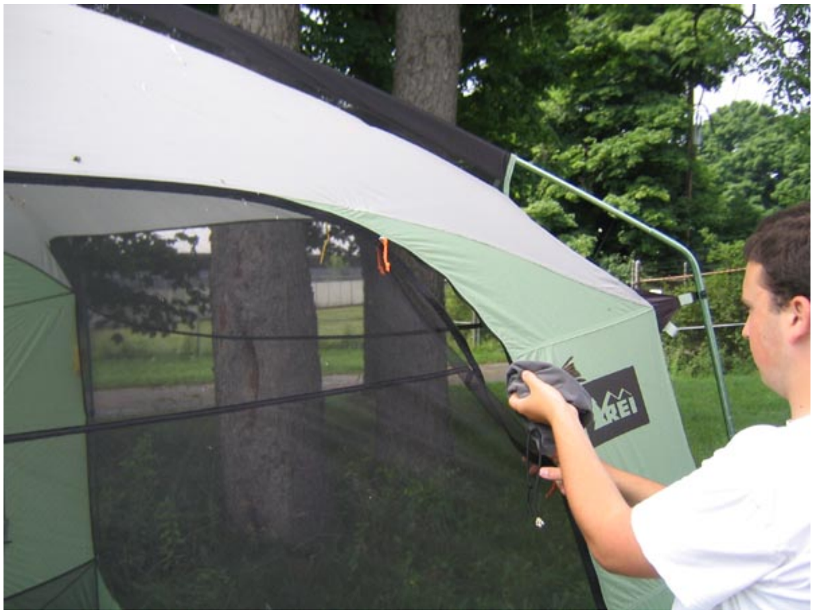


Figure 39: f0533600.jpg (Possible Evidence of a Birdwatching Trip)

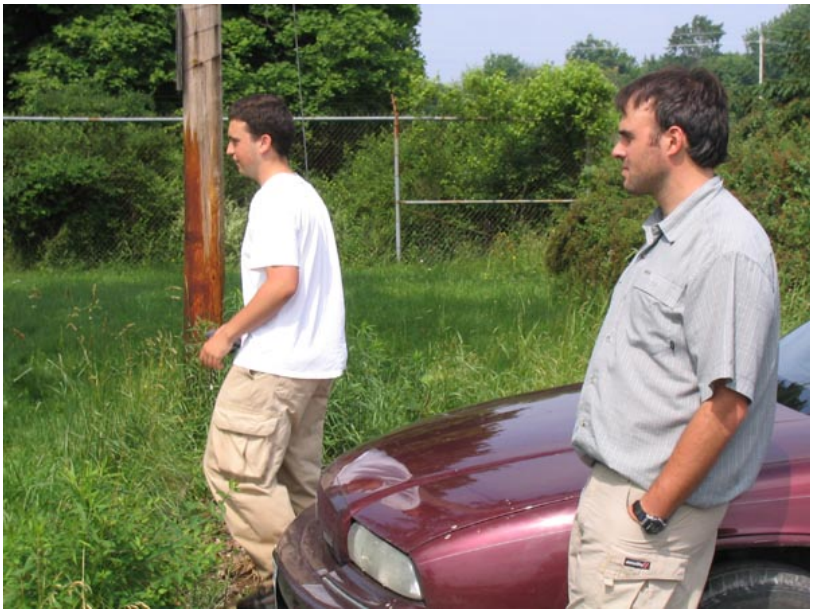


Figure 40: f0529544.jpg (Possible Evidence of a Birdwatching Trip)

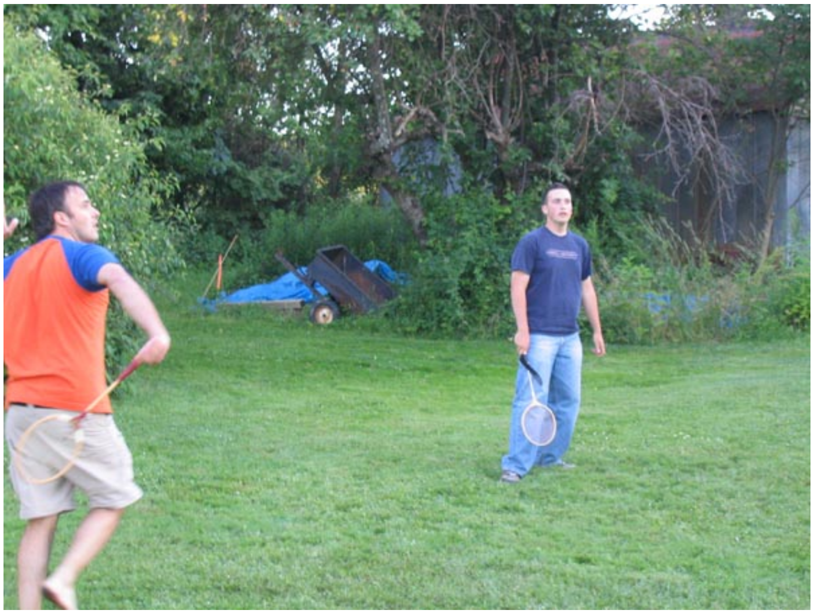


Figure 41: f0527448.jpg (Possible Evidence of a Birdwatching Trip)

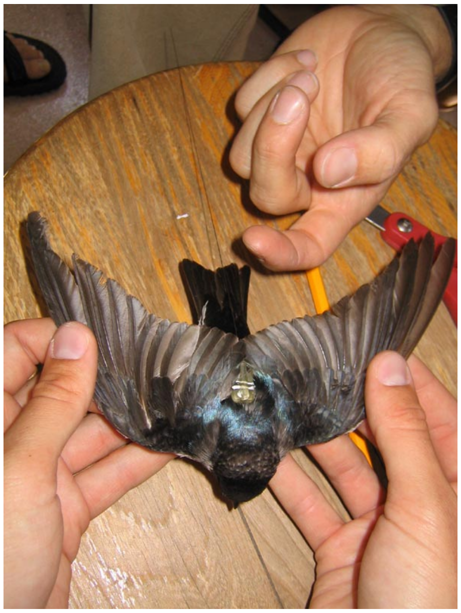


Figure 42: f0526960.jpg

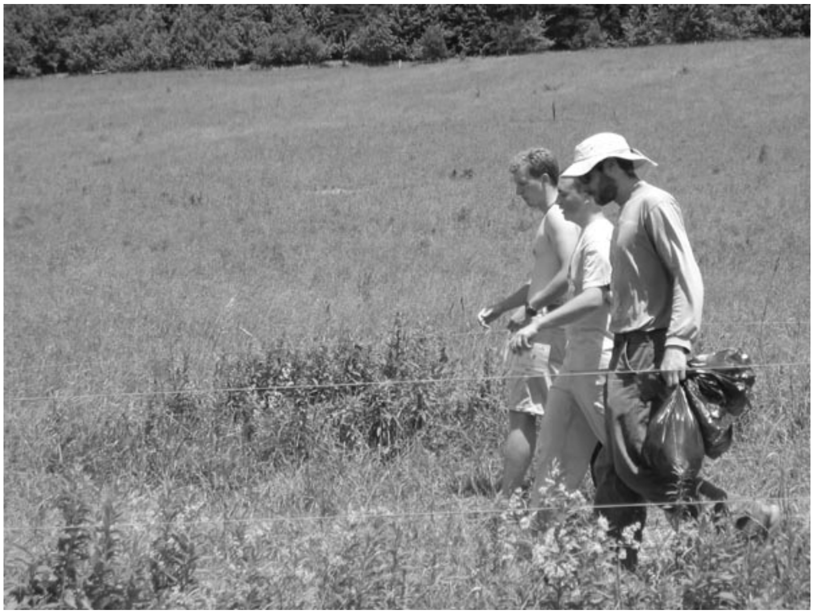


Figure 43: f0525016.jpg (Possible Evidence of a Birdwatching Trip)

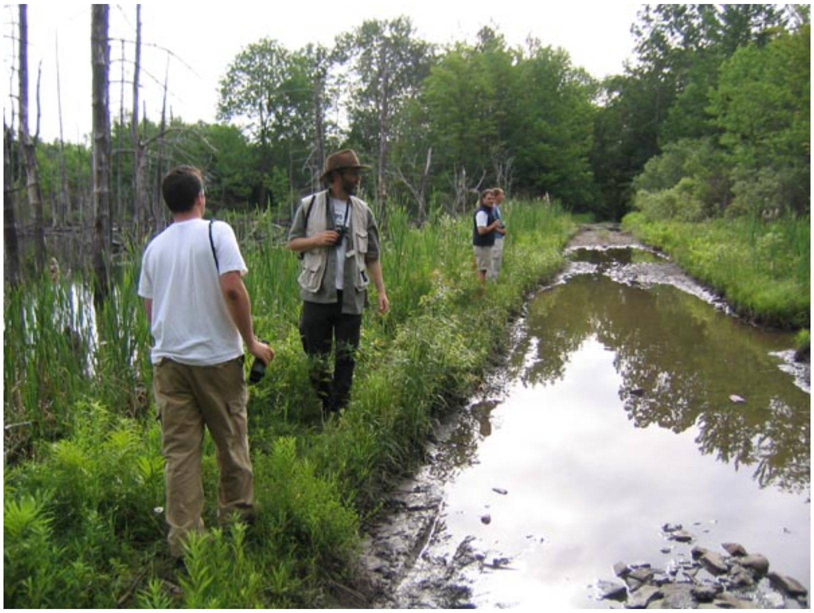


Figure 44: f0501184.jpg (Possible Evidence of a Birdwatching Trip)

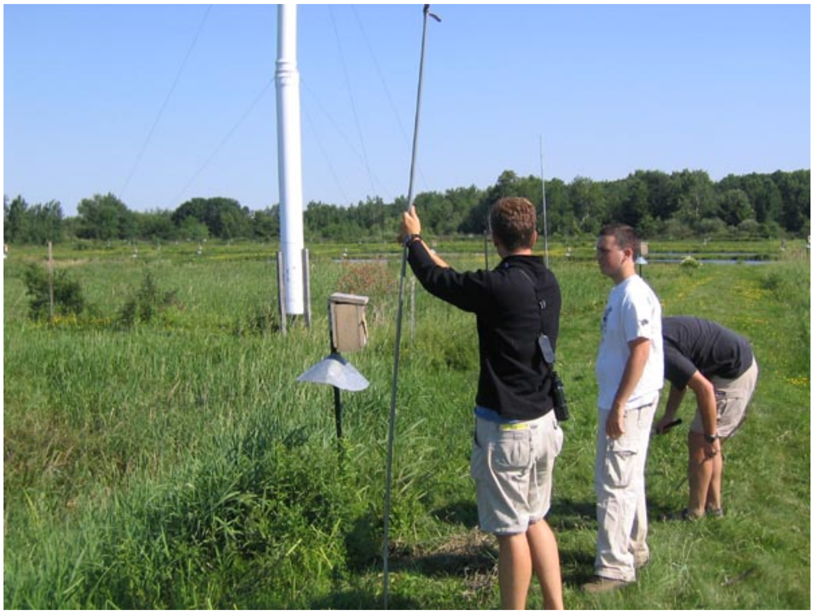


Figure 45: f0493176.jpg (Contains Image of Birdbox)

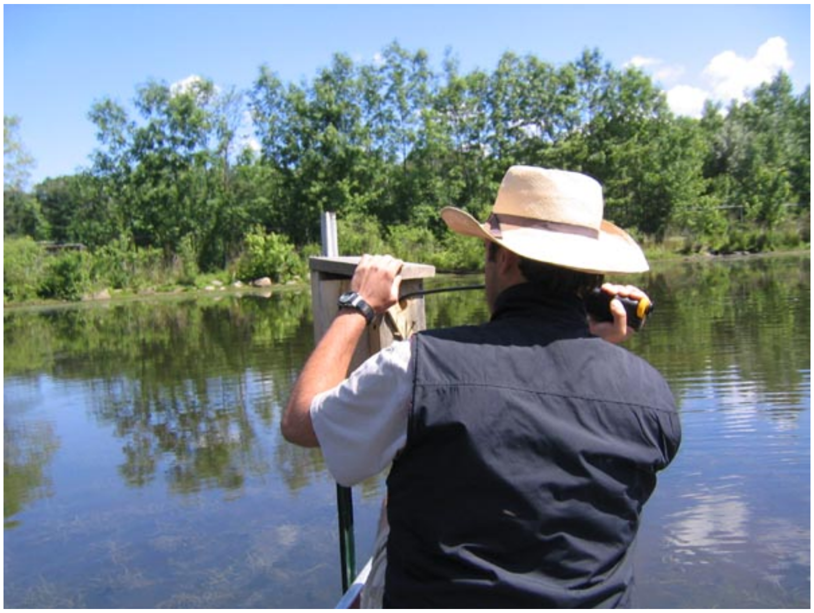


Figure 46: f0464568.jpg (Contains Proof of Tampering with Birdbox)

Figure 47: f0443520.jpg

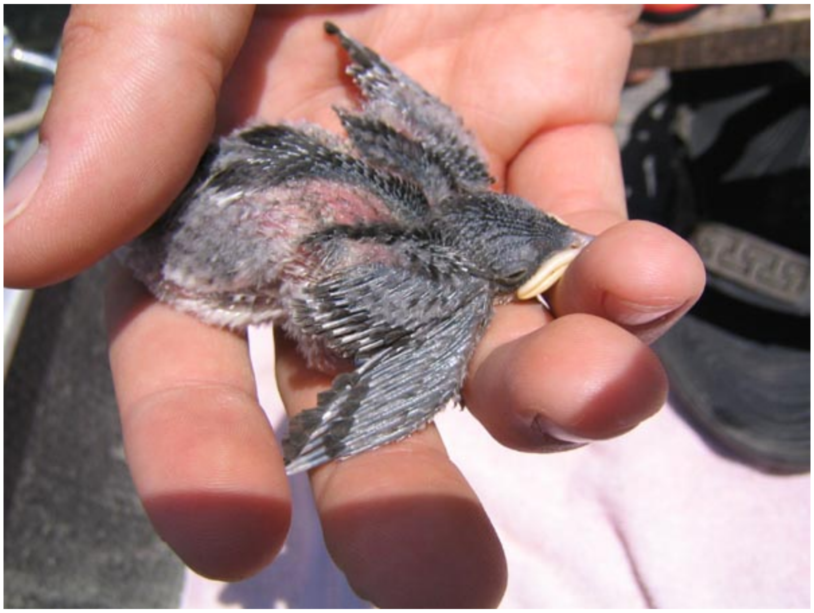


Figure 48: f0441536.jpg

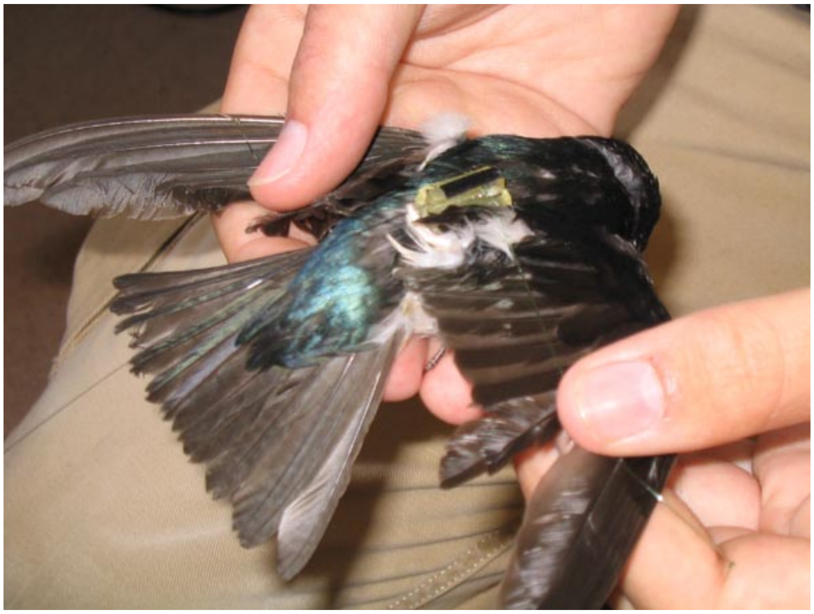


Figure 49: f0440944.jpg

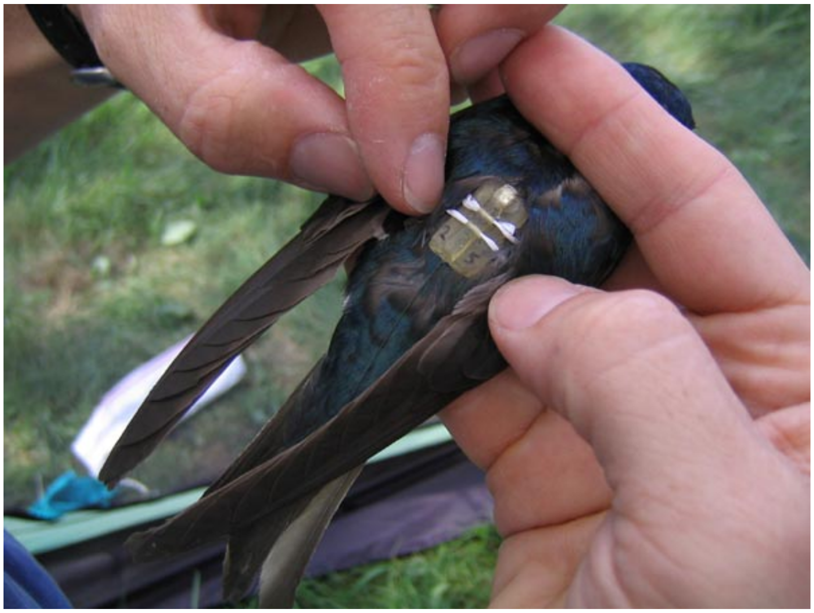


Figure 50: f0439400.jpg

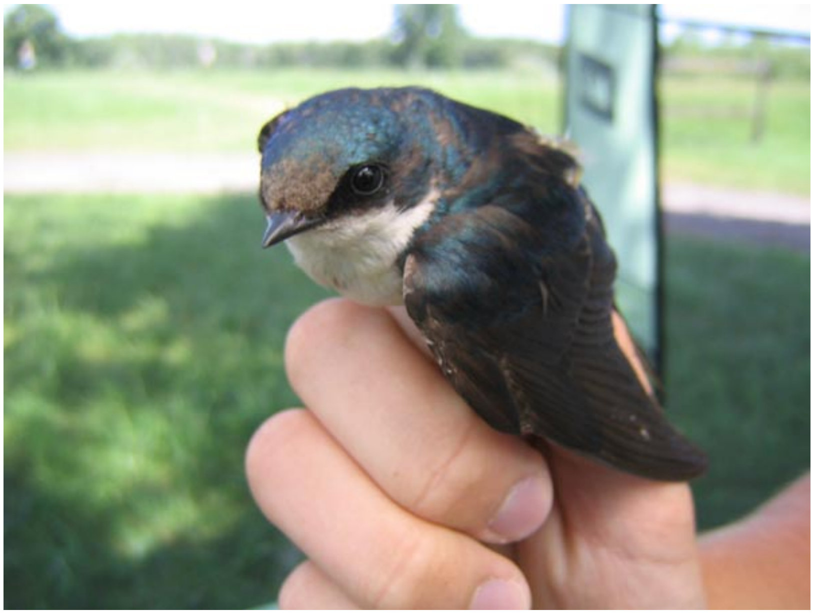


Figure 51: f0438640.jpg

Figure 52: f0416072.jpg

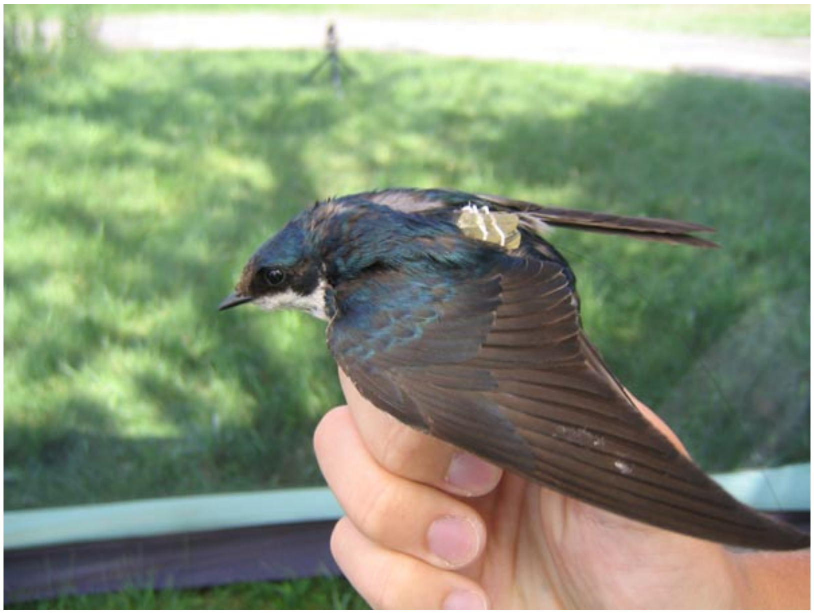


Figure 53: f0415008.jpg

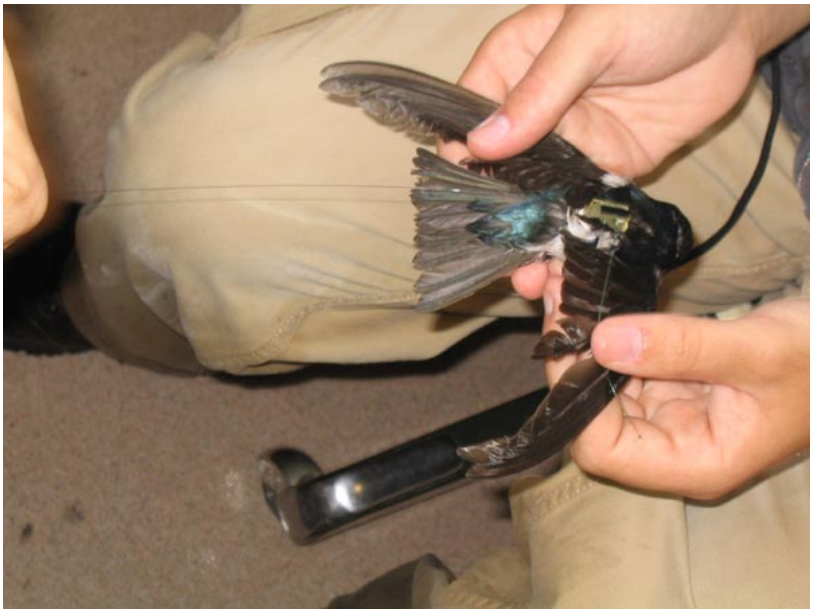


Figure 54: f0382464.jpg

Figure 55: f0360392.jpg

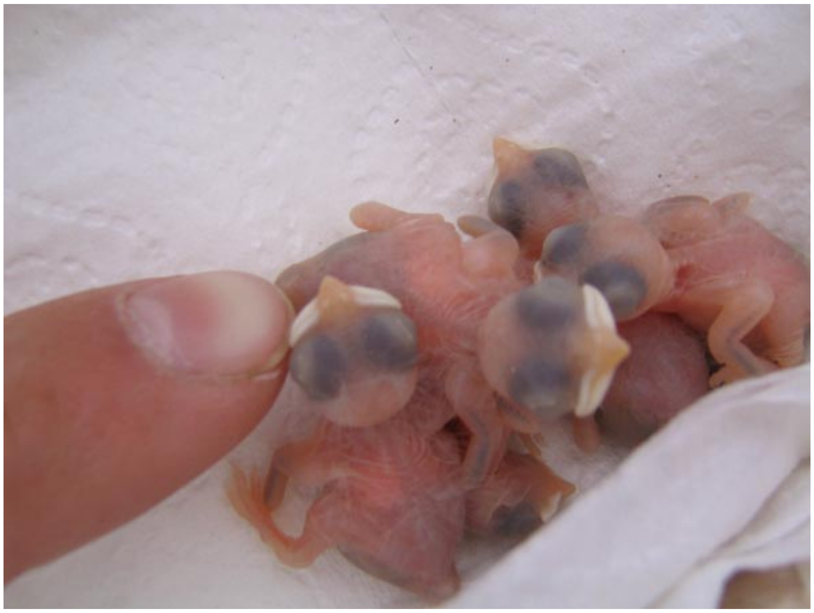


Figure 56: f0345832.jpg

Figure 57: f0345656.jpg

Figure 58: f0045880.jpg

6.1.3 Images From Canon EOS-1DS Camera

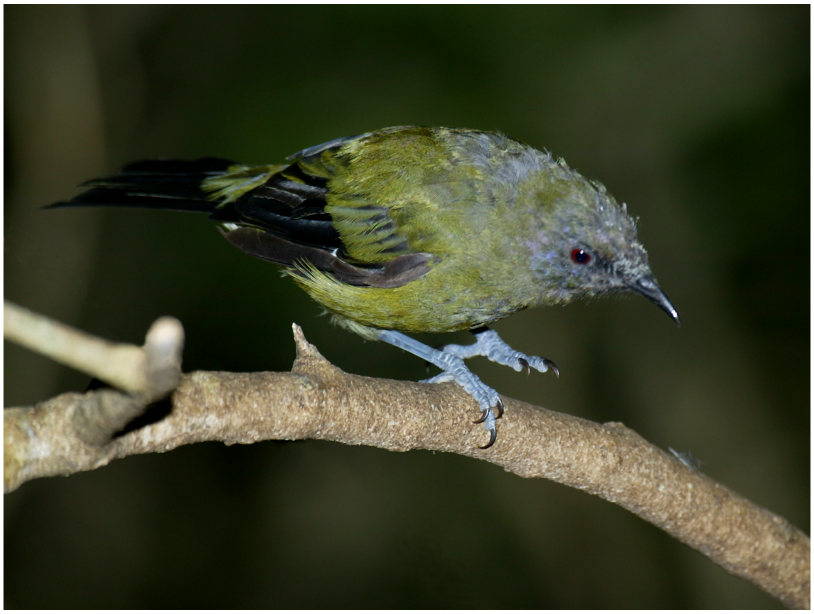


Figure 59: BellbirdJumpingOffBranch.jpg

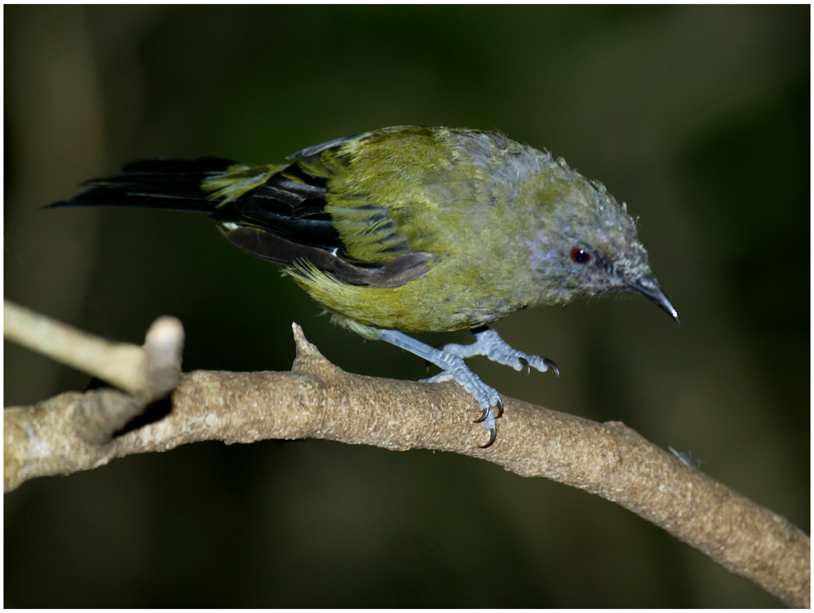


Figure 60: f0002368.jpg

6.1.4 Images From Sony Cybershot Camera

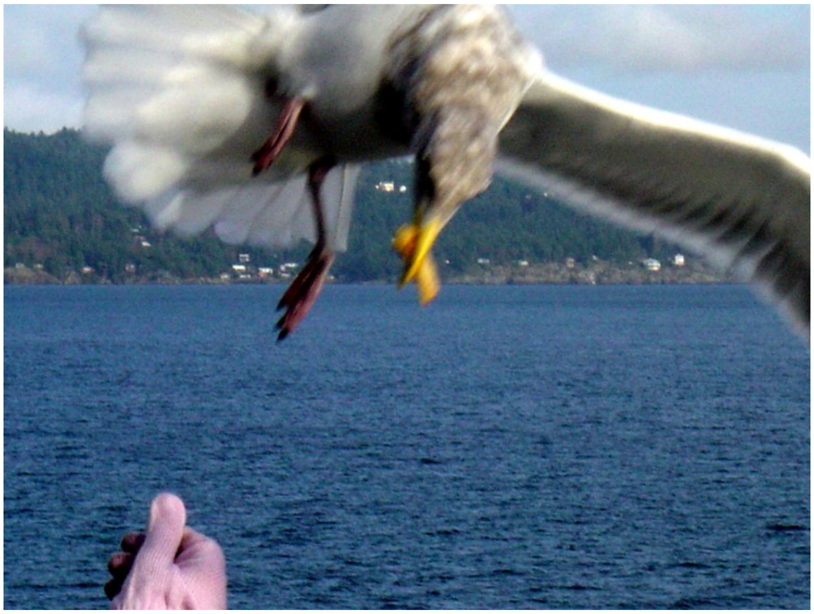


Figure 61: feedingthebirds.jpg (Title with Obfuscation Removed)

6.1.5 Images From Encrypted GPG File

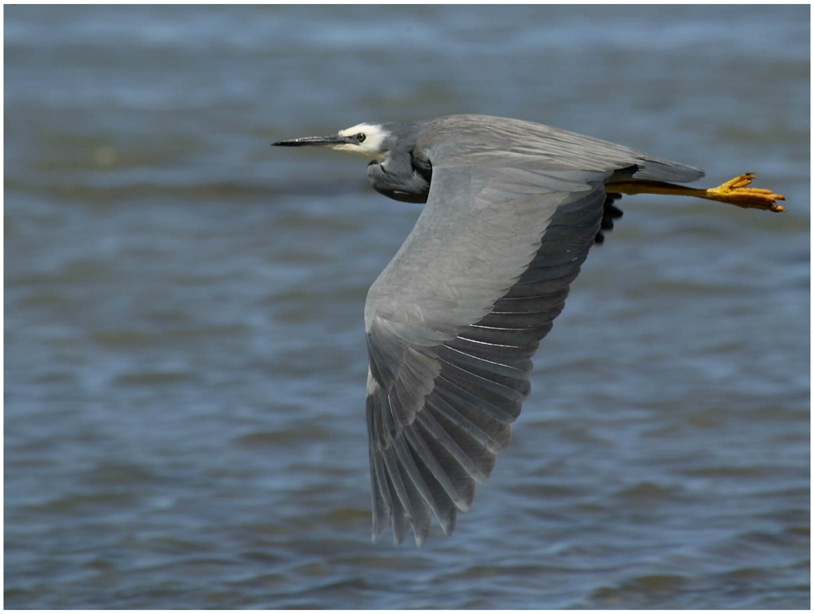


Figure 62: WhiteFacedHeronFlying.jpg

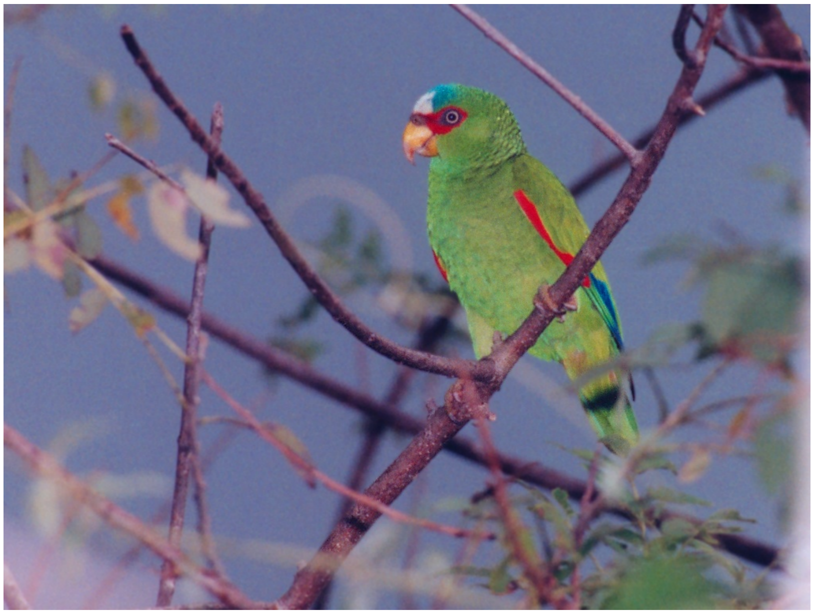


Figure 63: WhiteFrontedParrot.jpg

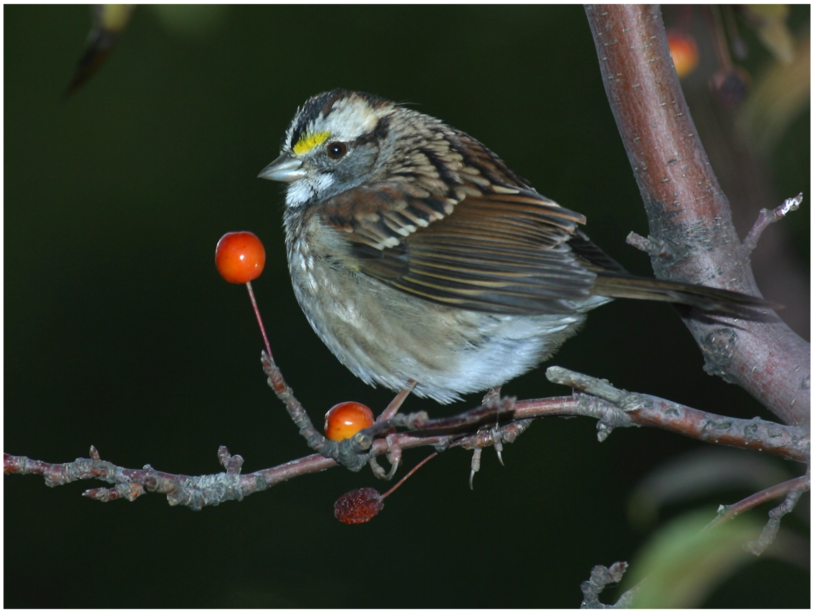


Figure 64: WhiteThroatedSparrowInTree.jpg

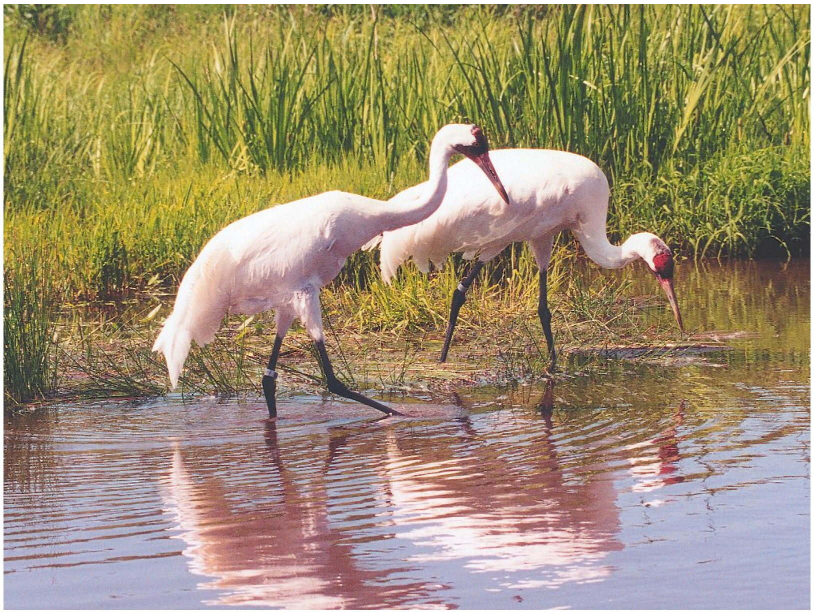


Figure 65: WhoopingCranes.jpg

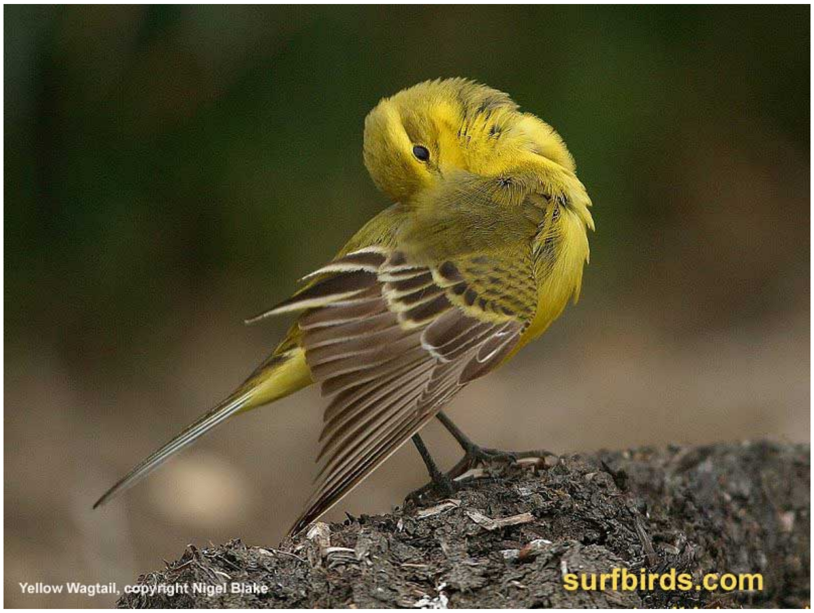


Figure 66: yellow-wag-cover-nb.jpg

6.1.6 Images From .dll File

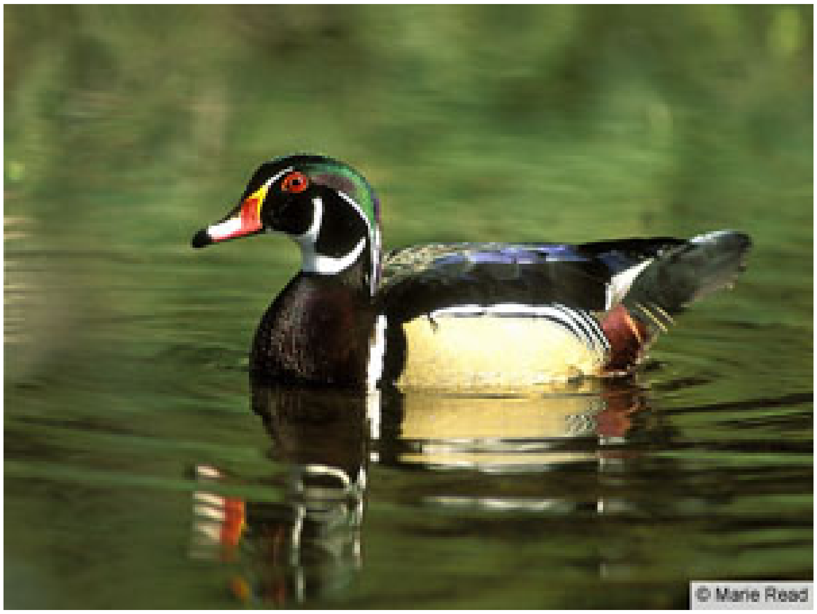


Figure 67: brdWoodDuck.jpg

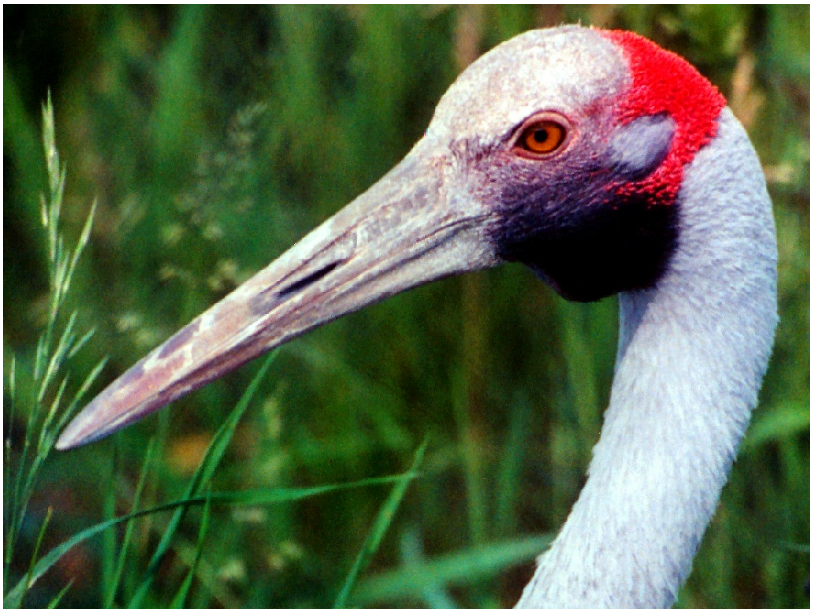


Figure 68: Brolga.jpg

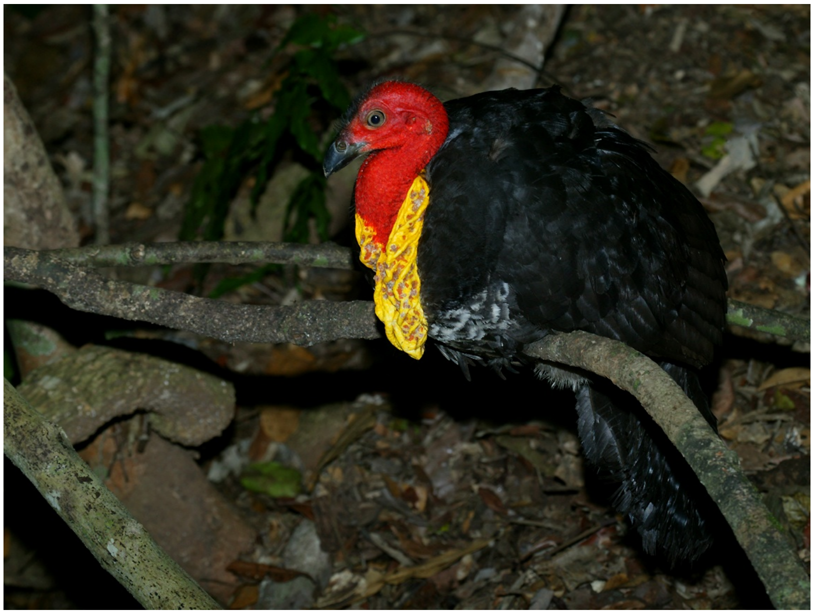


Figure 69: BrushTurkeyPerching.jpg

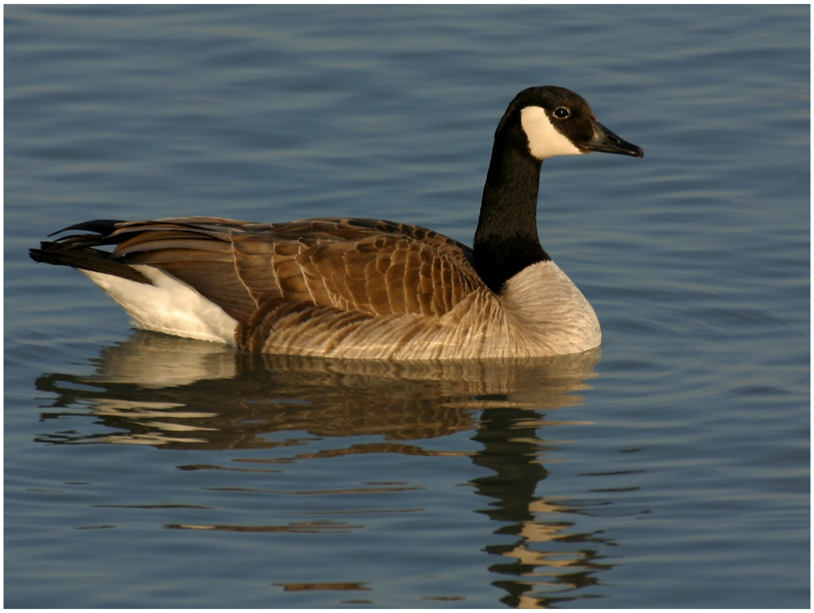


Figure 70: CanadaGoose.jpg

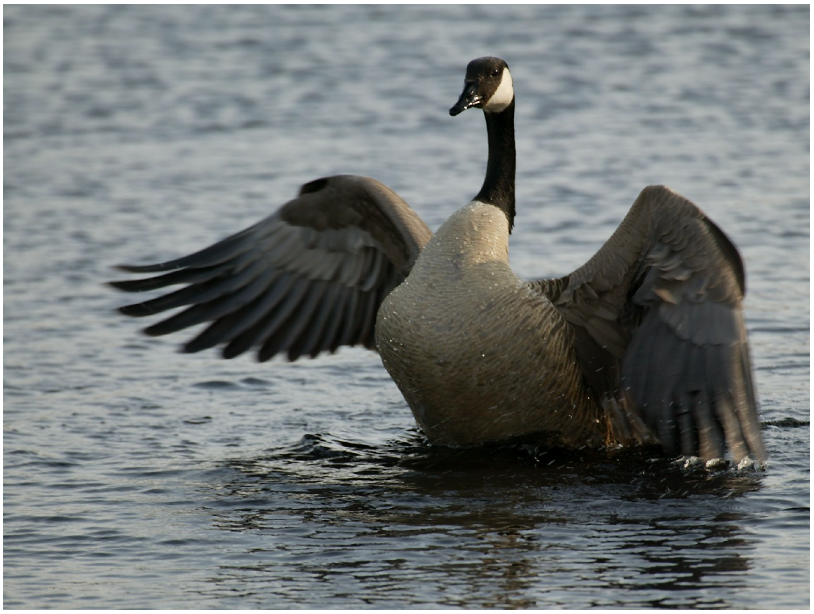


Figure 71: CanadaGooseWashing.jpg

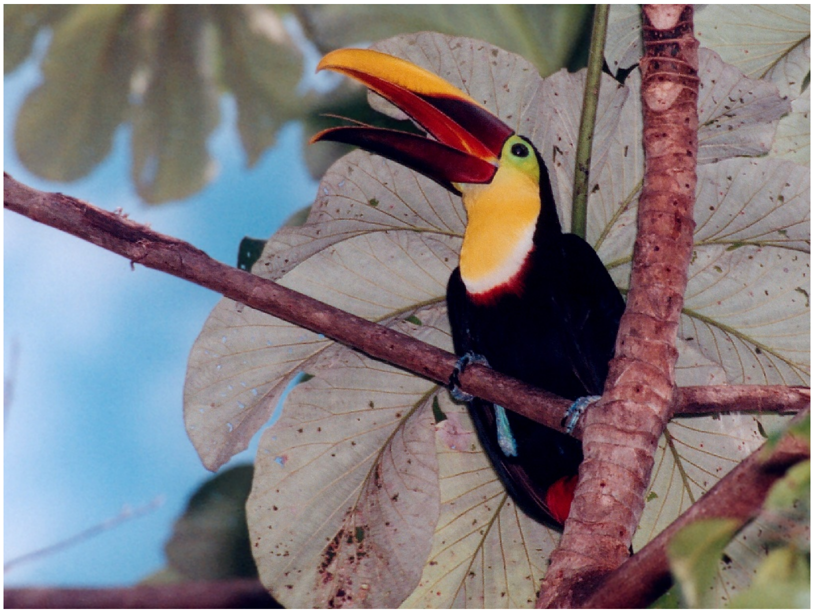


Figure 72: ChestnutMandibledToucan.jpg

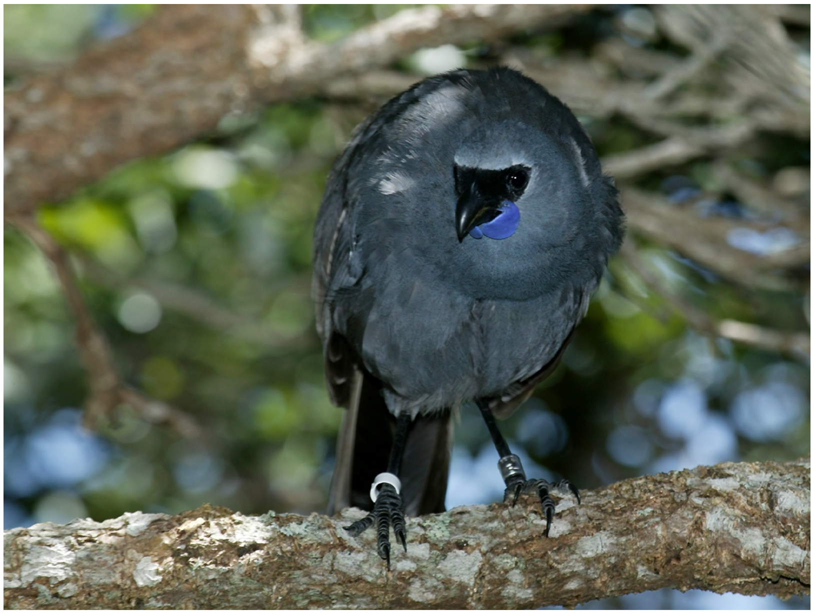


Figure 73: CrouchingKokako.jpg

6.1.7 Image From .exe File

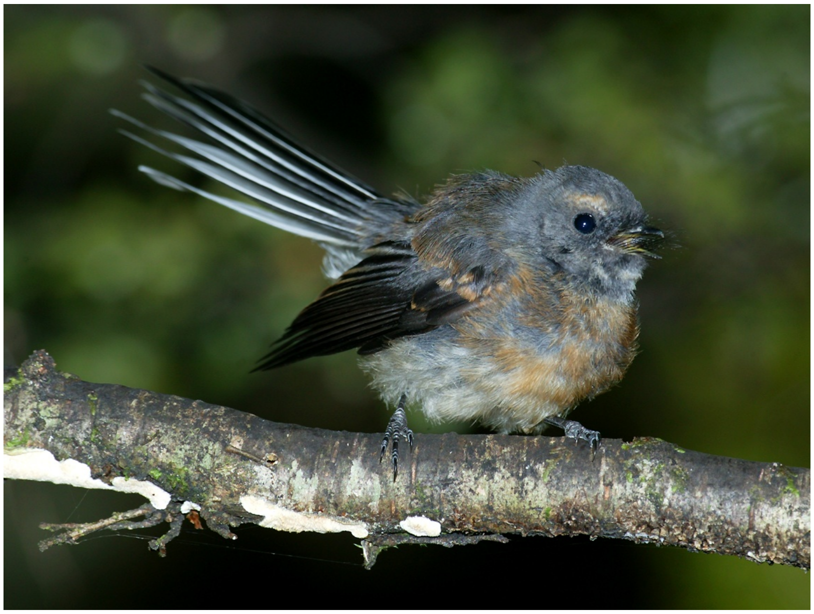
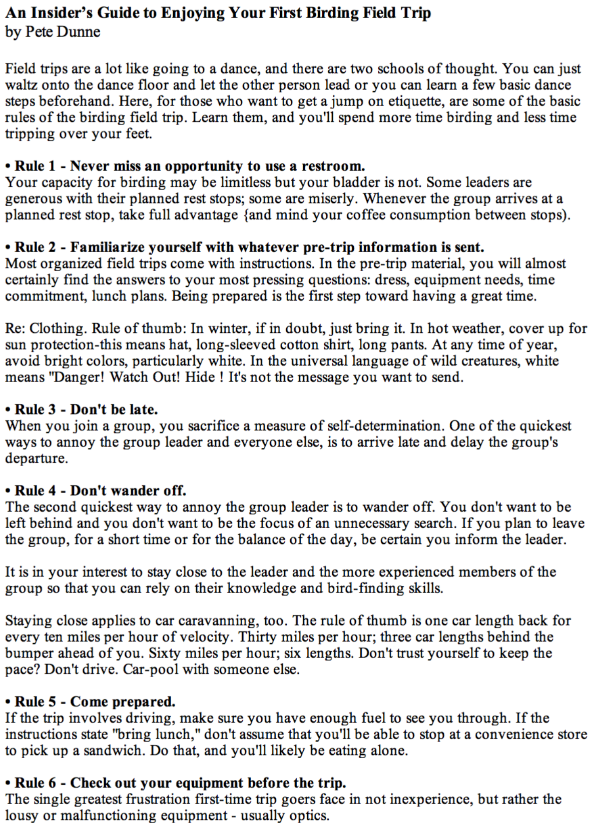


Figure 74: FantailFrontView.jpg

6.1.8 Screenshots of Birding Guide



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

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

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

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

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

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

• Rule 4 - Don't wander off.
The second quickest way to annoy the group leader is to wander off. You don't want to be left behind and you don't want to be the focus of an unnecessary search. If you plan to leave the group, for a short time or for the balance of the day, be certain you inform the leader.

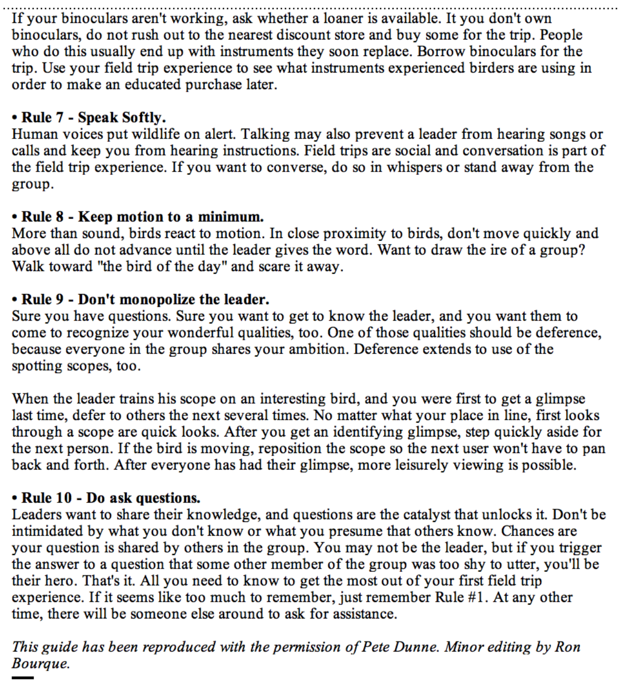
It is in your interest to stay close to the leader and the more experienced members of the group so that you can rely on their knowledge and bird-finding skills.

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

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

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

Figure 75: An Insider's Guide to Birdwatching 1/2



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

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

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

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

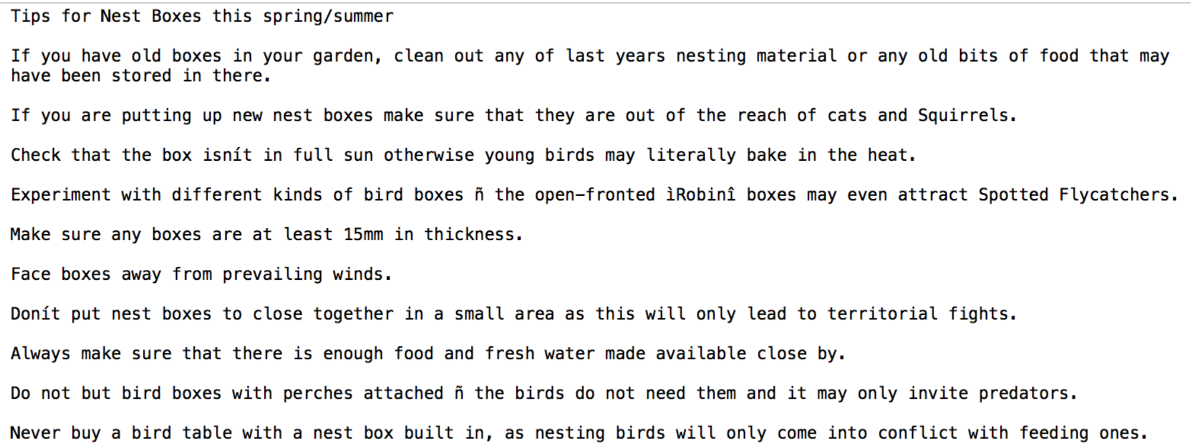
When the leader trains his scope on an interesting bird, and you were first to get a glimpse last time, defer to others the next several times. No matter what your place in line, first looks through a scope are quick looks. After you get an identifying glimpse, step quickly aside for the next person.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

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

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

Figure 76: An Insider's Guide to Birdwatching 2/2

6.1.9 Screenshot of 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 isnít in full sun otherwise young birds may literally bake in the heat.

Experiment with different kinds of bird boxes ñ the open-fronted ìRobinî boxes may even attract Spotted Flycatchers.

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

Face boxes away from prevailing winds.

Donít 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 ñ 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.
```

Figure 77: Screenshot of nestboxtips.txt

6.1.10 Screenshot of Doc1.doc

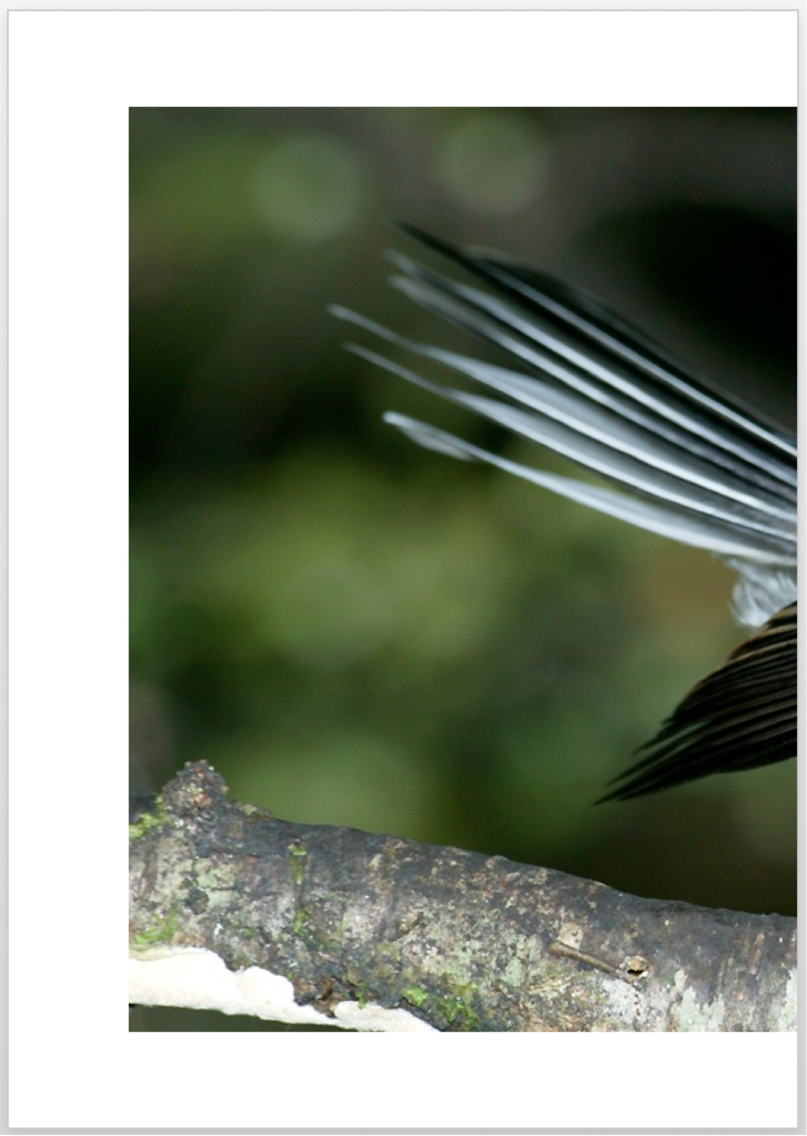
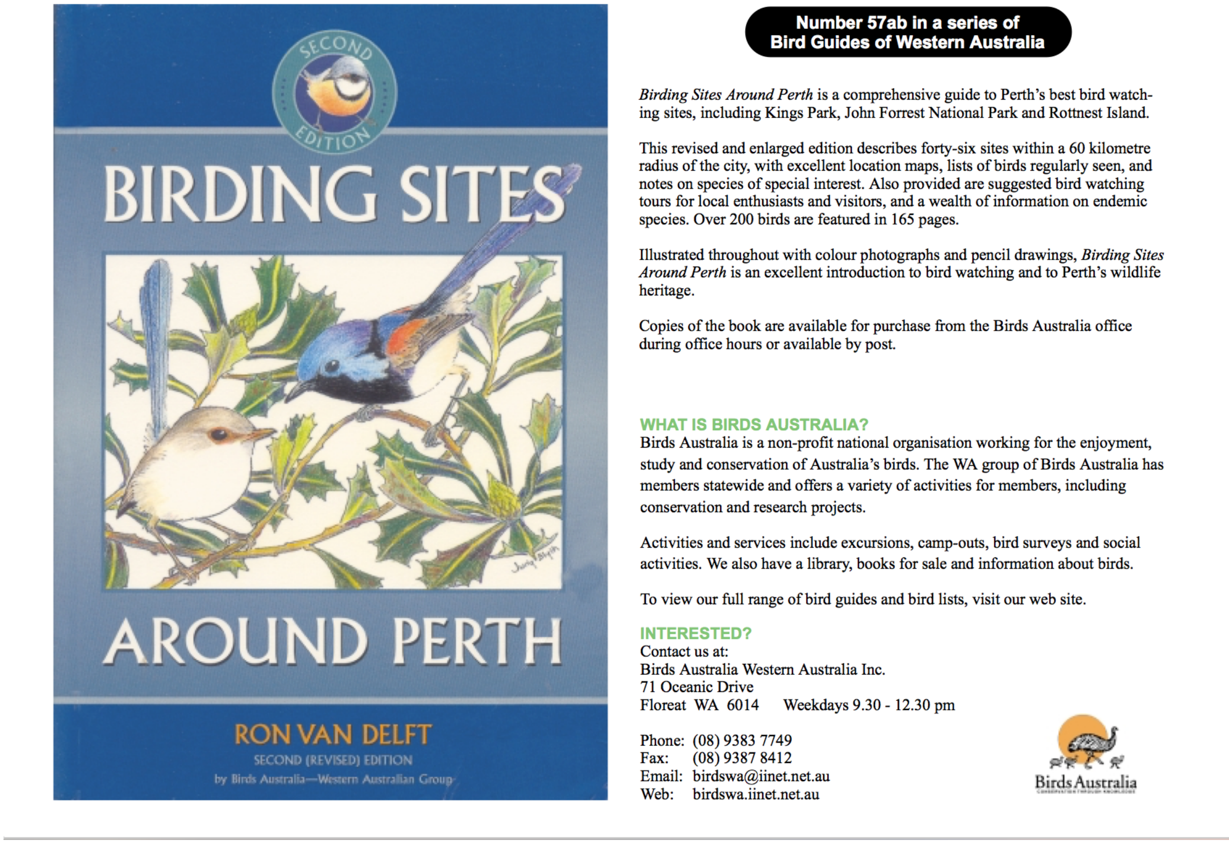


Figure 78: Screenshot of Doc1.doc

6.1.11 Screenshots of Recovered PDF's



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.

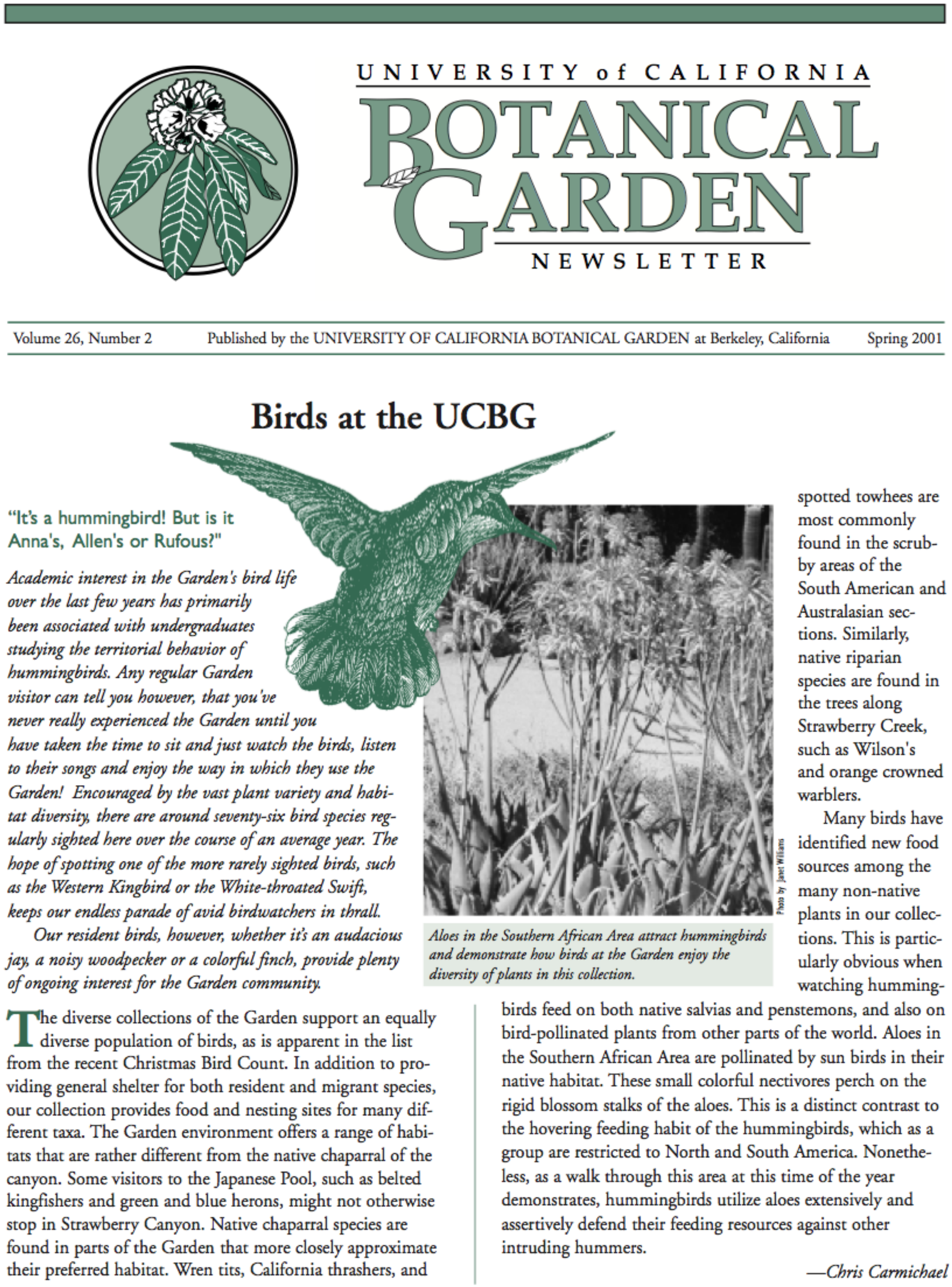
INTERESTED?

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

Figure 79: Screenshot of f0180344.pdf



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.

Photo by Janet Williams

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

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

Figure 80: Screenshot of f0273688.pdf

The Porter County
Birding Guide

Figure 81: Screenshot of f0327896.pdf

6.1.12 Images From Thunderbird Mail Client

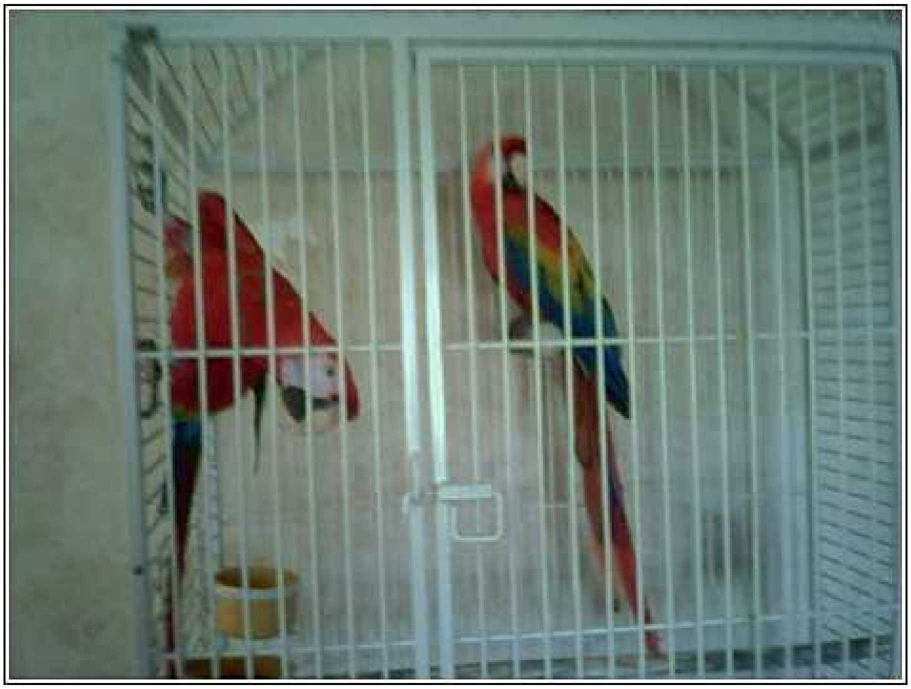


Figure 82: 7EYBTELF1KAN.jpg

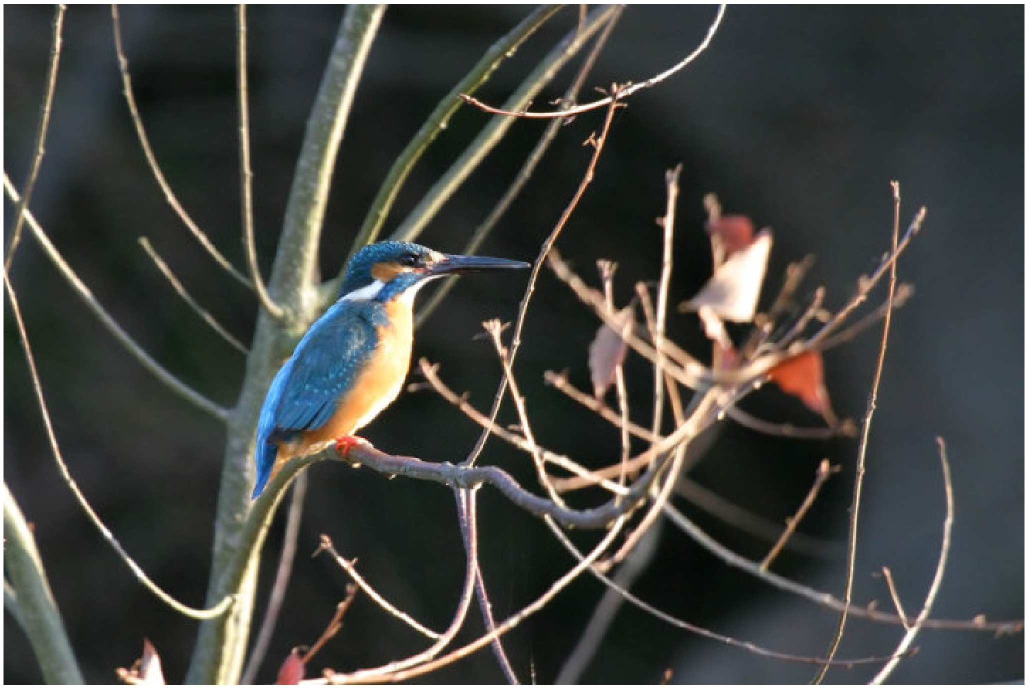


Figure 83: IMG3937filtered.jpg

Figure 84: cutepenguin.jpg

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

Figure 85: glfs-storm-birds.jpg

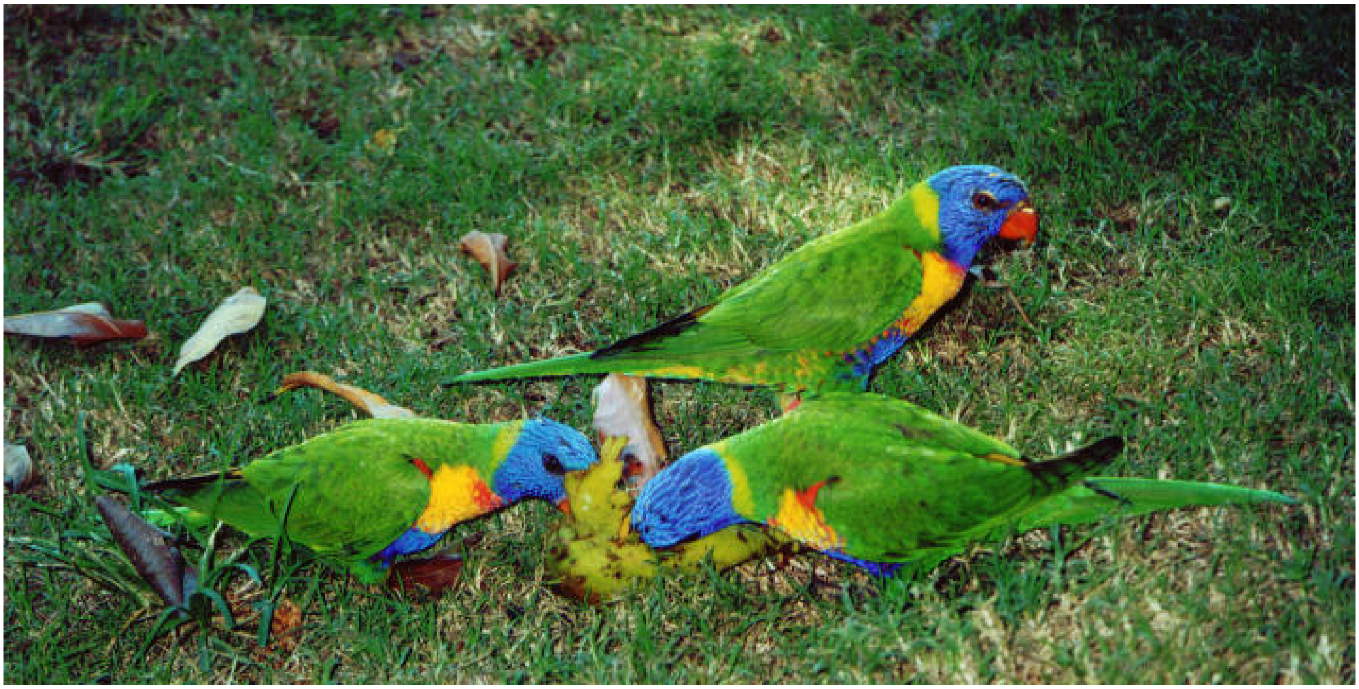


Figure 86: colorful-birds.jpg

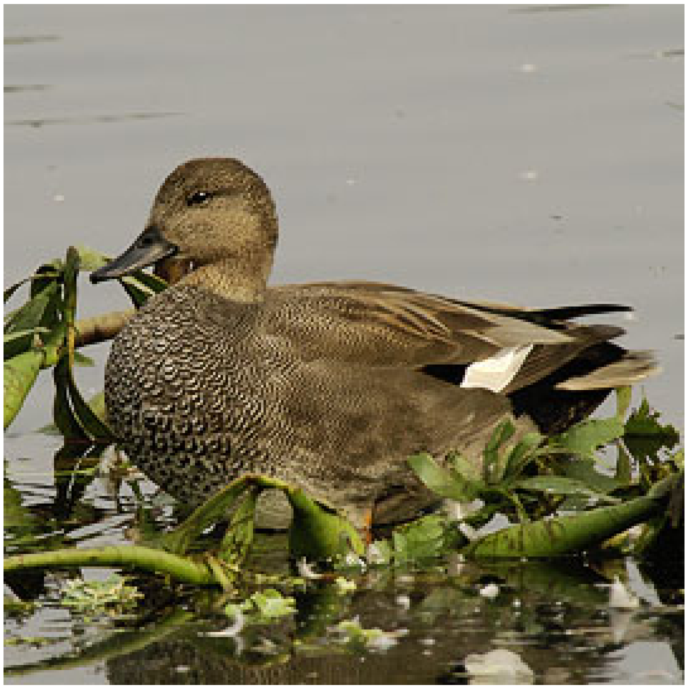


Figure 87: gawall8.jpg

6.2 Appendix 2 - Pictures of Evidence Seized

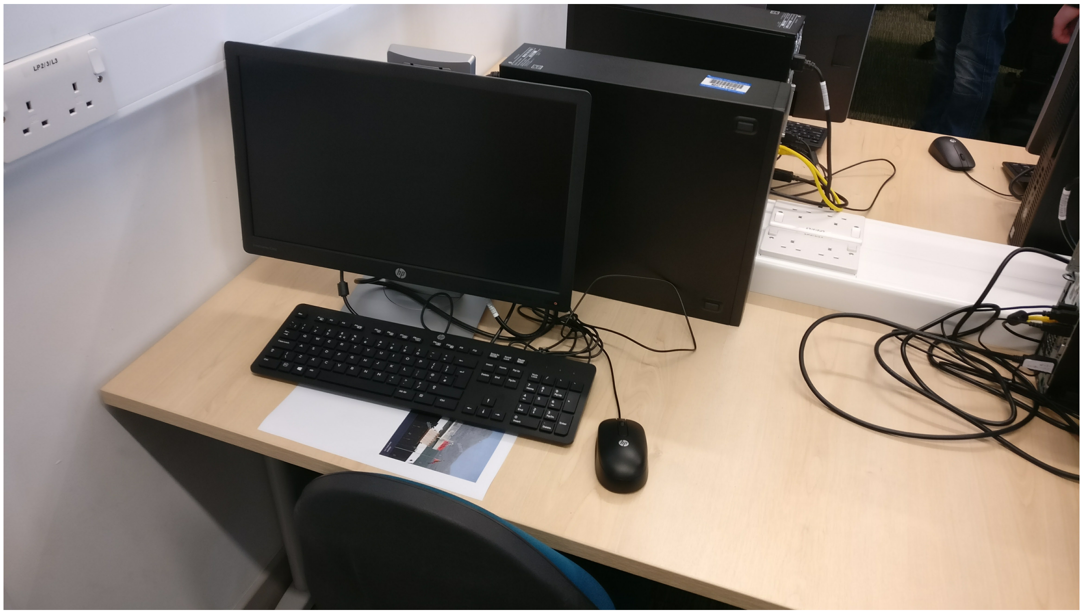


Figure 88: Overview of Crime Scene

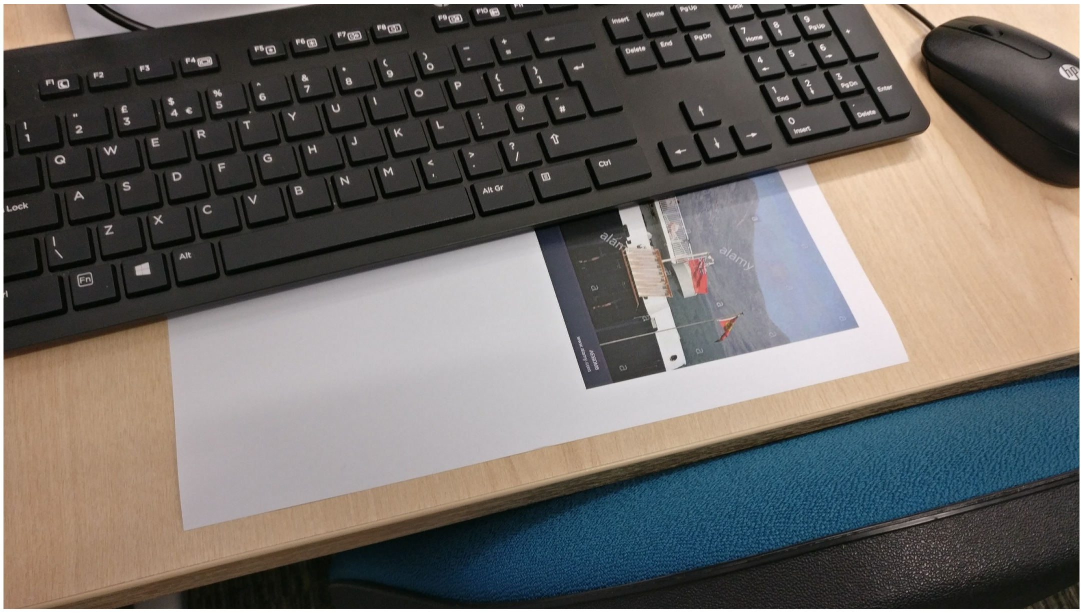


Figure 89: Photo Discovered on Desk

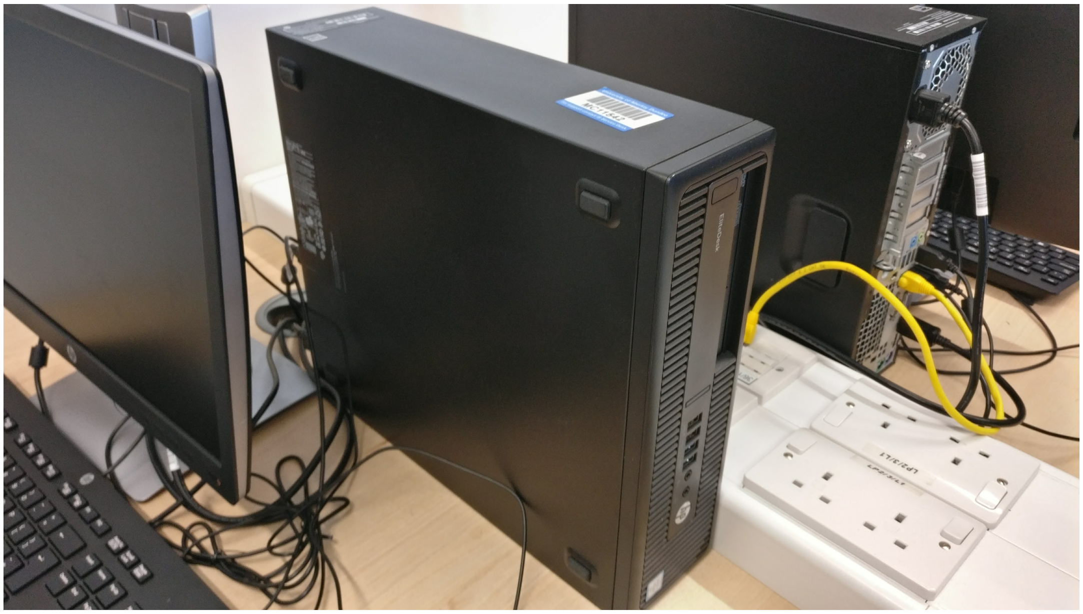


Figure 90: HP Computer

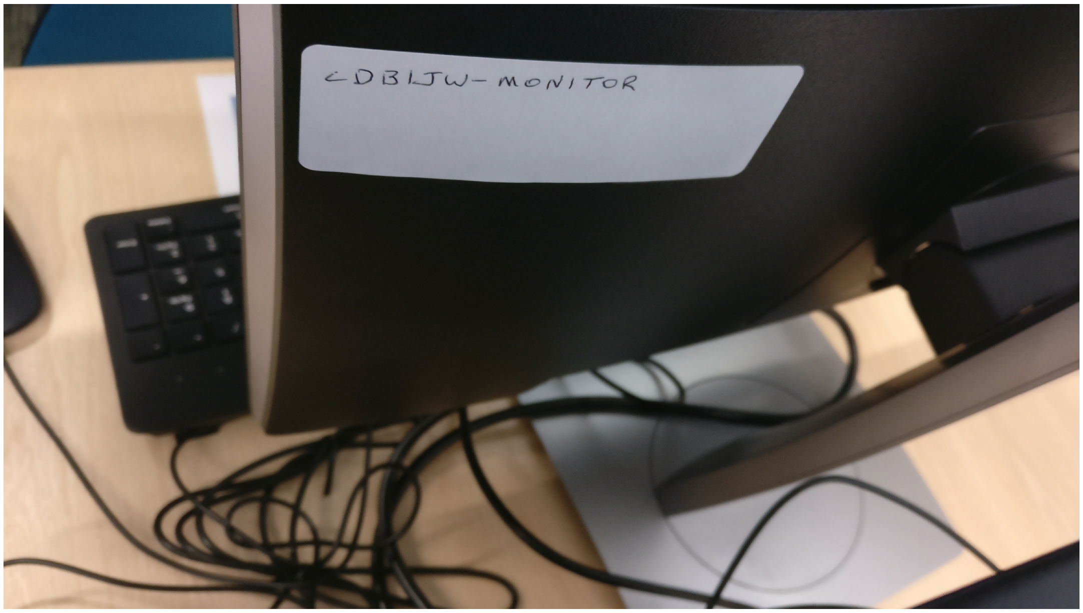


Figure 91: HP Monitor

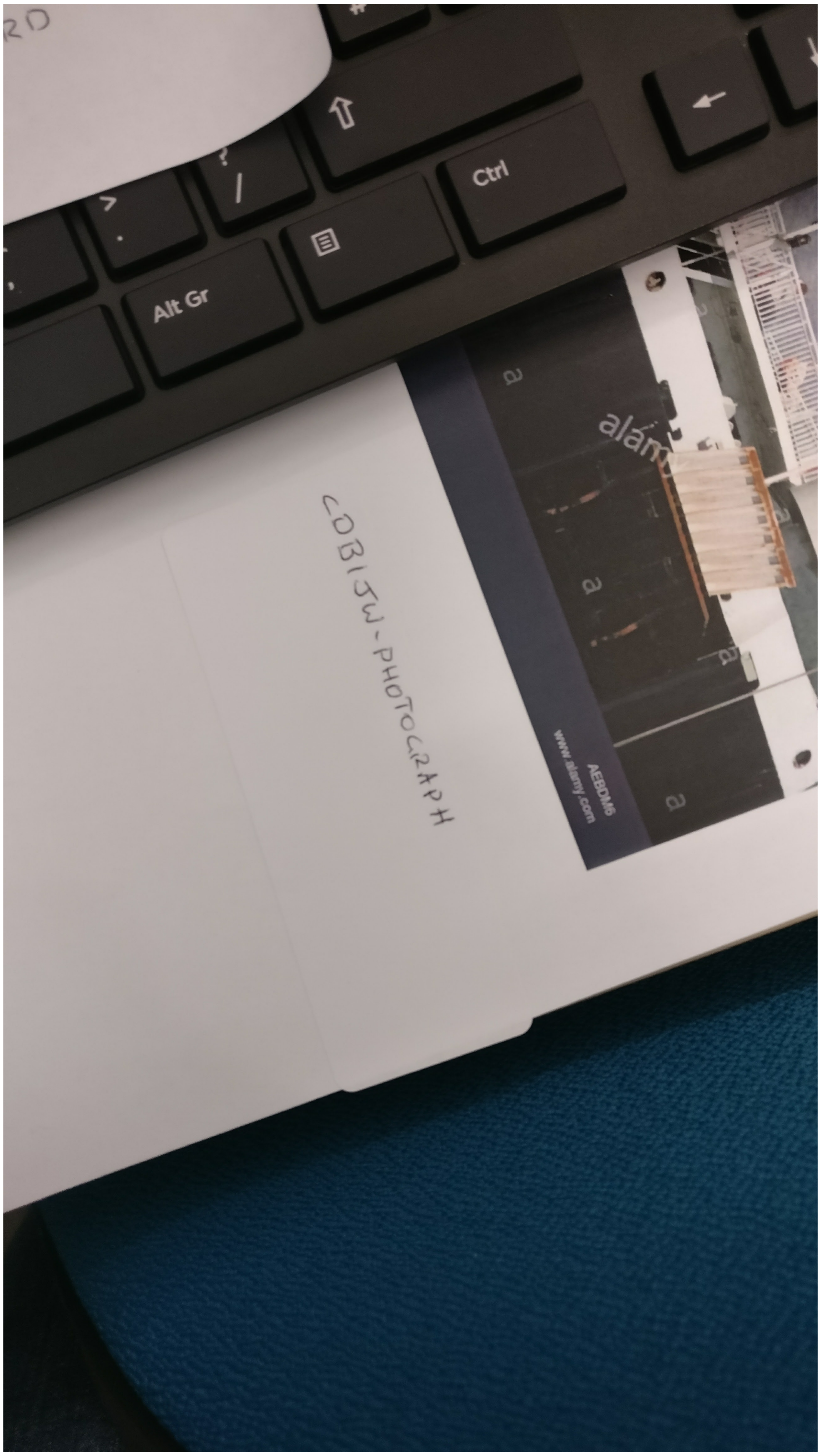
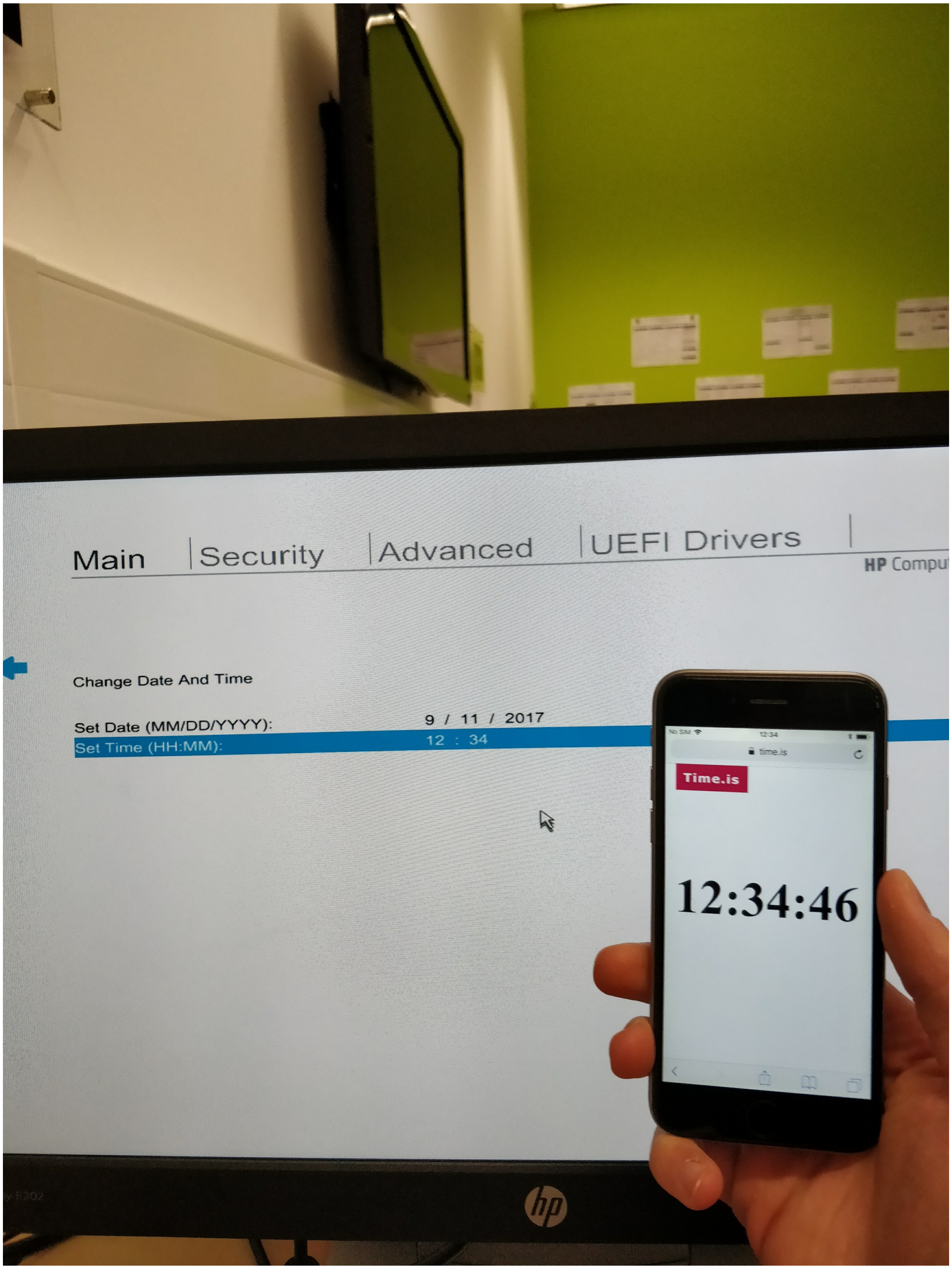


Figure 92: Picture Found on Desk

6.3 Appendix 3 - Picture of Clock Skew

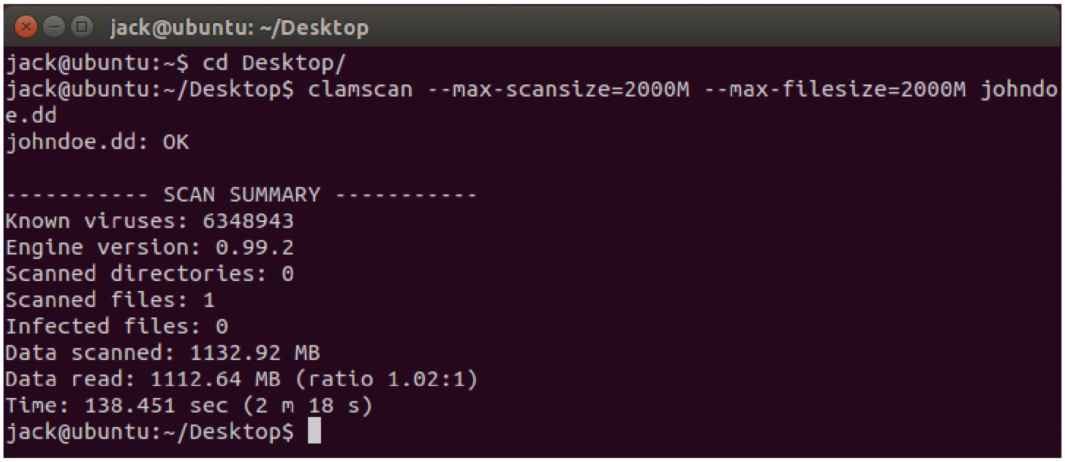


Set Date (MM/DD/YYYY): 9 / 11 / 2017

Set Time (HH:MM): 12 : 34

Figure 93: Check for Clock Skew

6.4 Appendix 4 - Screenshot of Antivirus Scan Results

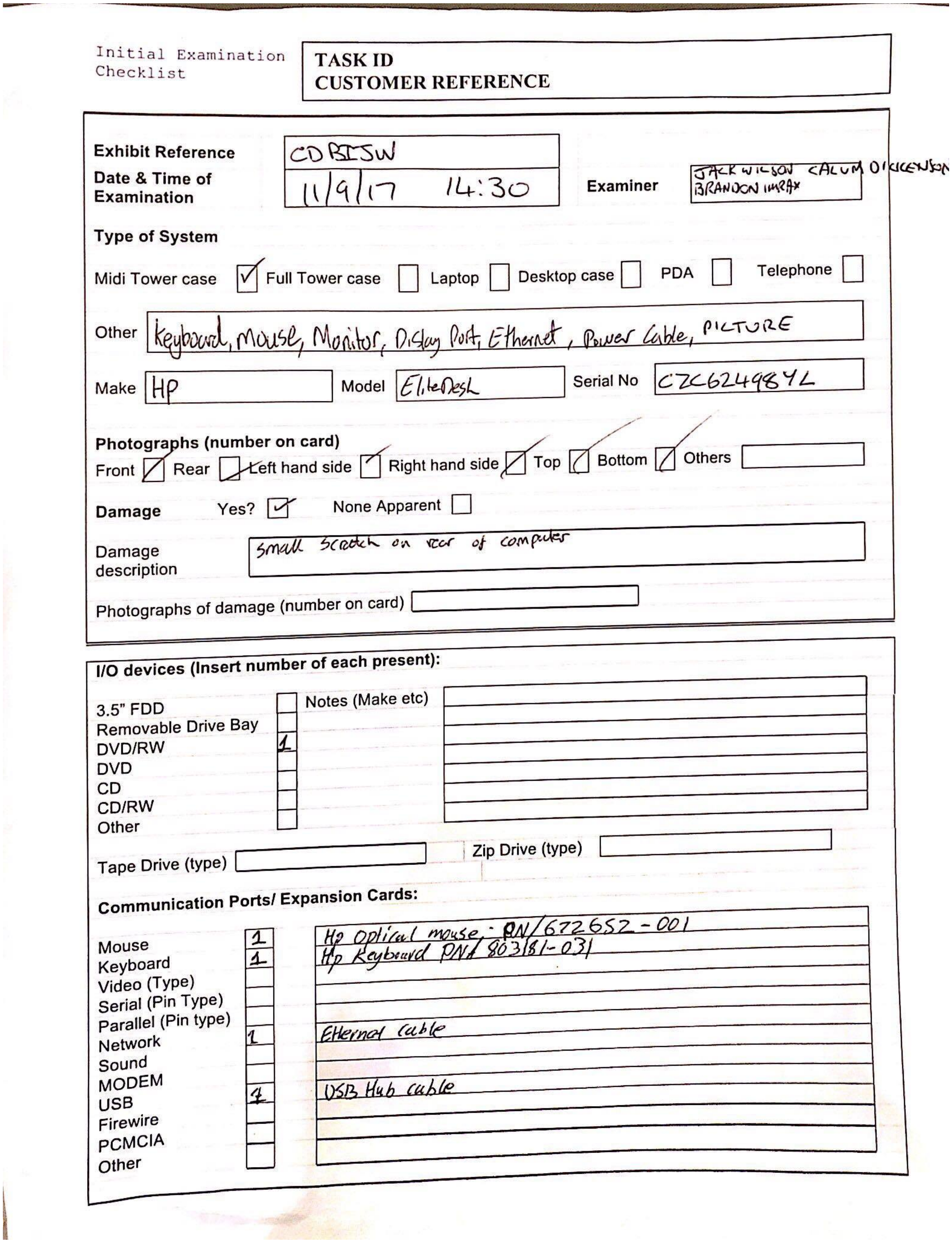


```
jack@ubuntu:~$ cd Desktop/
jack@ubuntu:~/Desktop$ clamscan --max-scansize=2000M --max-filesize=2000M johndo
e.dd
johndoe.dd: OK

----------- SCAN SUMMARY -----------
Known viruses: 6348943
Engine version: 0.99.2
Scanned directories: 0
Scanned files: 1
Infected files: 0
Data scanned: 1132.92 MB
Data read: 1112.64 MB (ratio 1.02:1)
Time: 138.451 sec (2 m 18 s)
jack@ubuntu:~/Desktop$
```

Figure 94: Antivirus Scan Results

6.5 Appendix 5 - Seizure Documents



Initial Examination Checklist

TASK ID
CUSTOMER REFERENCE

Exhibit Reference CDBISW

Date & Time of Examination 11/9/17 14:30

Examiner JACK WILSON CALUM DICKENSON BRANDON IMRAY

Type of System

Midi Tower case ☑ Full Tower case □ Laptop □ Desktop case □ PDA □ Telephone □

Other Keyboard, Mouse, Monitor, Display Port, Ethernet, Power Cable, PICTURE

Make HP Model EliteDesk Serial No CZC62498YL

Photographs (number on card)

Front ☑ Rear ☑ Left hand side ☑ Right hand side ☑ Top ☑ Bottom ☑ Others □

Damage Yes? ☑ None Apparent □

Damage description small scratch on rear of computer

Photographs of damage (number on card) □

I/O devices (Insert number of each present):

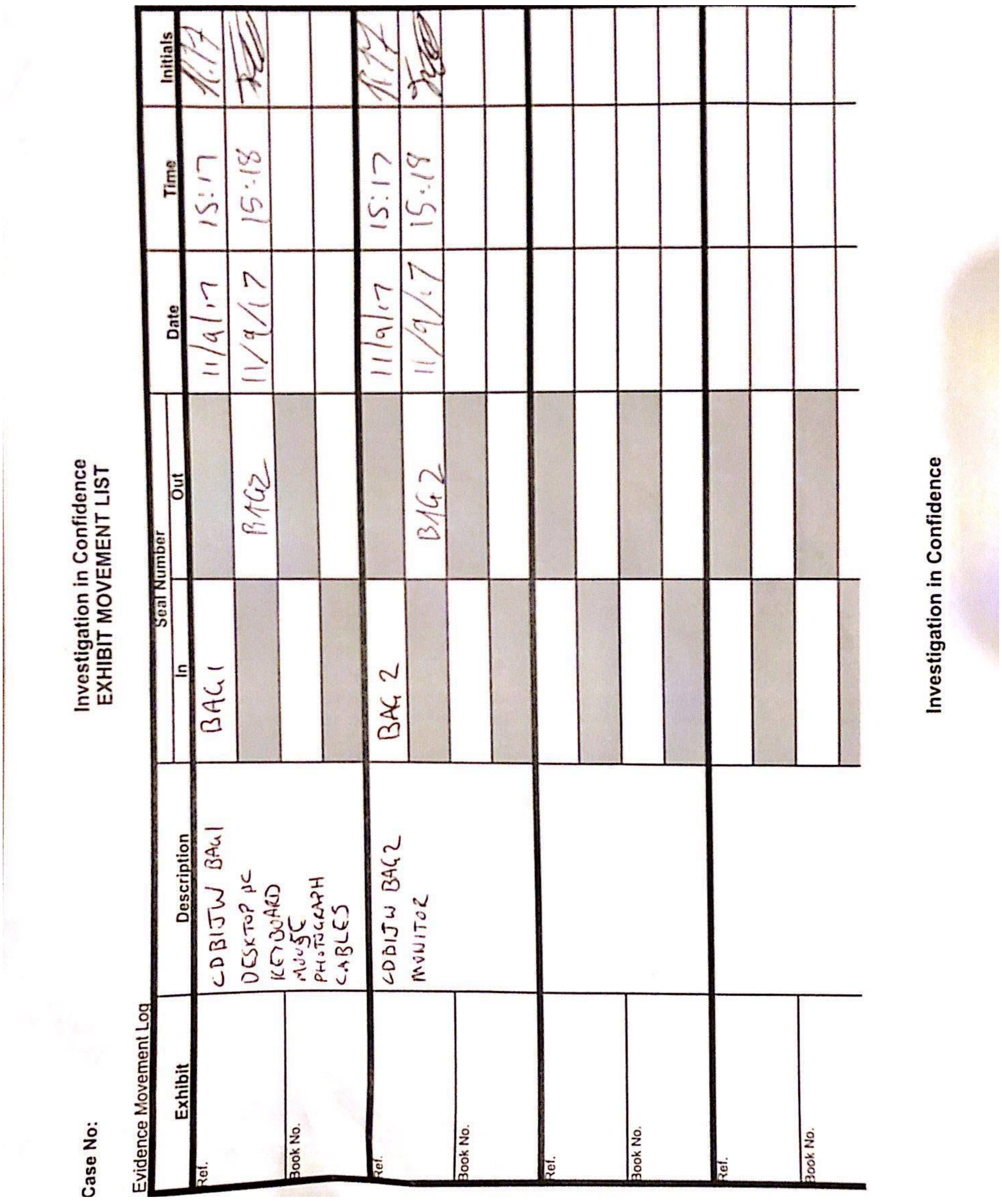
3.5" FDD	□	Notes (Make etc)
Removable Drive Bay	□	
DVD/RW	1	
DVD	□	
CD	□	
CD/RW	□	
Other	□	

Tape Drive (type) □ Zip Drive (type) □

Communication Ports/ Expansion Cards:

Mouse	1	Hp Optical mouse · PN/672652-001
Keyboard	1	Hp Keyboard PN/ 803181-031
Video (Type)		
Serial (Pin Type)		
Parallel (Pin type)		
Network	1	Ethernet cable
Sound		
MODEM		
USB	4	USB Hub cable
Firewire		
PCMCIA		
Other		

Figure 95: Initial Examination Checklist



Case No:

Investigation in Confidence
EXHIBIT MOVEMENT LIST

Evidence Movement Log

Exhibit	Description	Seal Number		Date	Time	Initials
		In	Out			
Ref.	CDBIJW BAG1 DESKTOP PC KEYBOARD MOUSE PHOTOGRAPH CABLES	BAG1		11/9/17	15:17	
			BAG2	11/9/17	15:18	
Book No.						
Ref.	CDBIJW BAG2 MONITOR	BAG 2		11/9/17	15:17	
			BAG2	11/9/17	15:19	
Book No.						
Ref.						
Book No.						
Ref.						
Book No.						

Investigation in Confidence

Figure 96: Chain of Custody Document