2017

JOINT REPORT OF

DARREN SHERRATT AND IAN FERGUSON

CASE AGAINST

MR JOHN DOE

ABERTAY UNIVERSITY FORENSIC INVESTIGATORS: MSDSJM
ABERTAY UNIVERSITY – ORNITHOLOGITS UNIT
Dundee

Contents

1. Summary

The accused, Mr John Doe, was found to be in possession of a sizeable number of illegal images of birds (IIOB) as well as material relating to bird watching, and bird house construction. The images were accumulated through means of the internet and from other ornithologists by email with whom Mr Doe has been communicating with. Mr Doe's internet history was examined and shows the accused has previously viewed information pertaining to the creation of bird houses and other sites used to listen to bird song.

2. Description of Crime

John Doe was found to be in possession of 78 illegal images of birds. Several of these images had been hidden, or deleted.

To analyse the suspects computer, a copy of the hard drive was taken, and various tools were used to determine the actions of the accused.

2.1. Incidents

2.1.1. Incident 1

Found of the hard drive images taken with a Canon Powershot SD100 camera, these images show several people on a camping trip, during which time they are shown birdwatching, holding birds of various age, measuring birds and tagging the birds. These images originated on the computer of John Doe on 03/02/2005. The source of these images could not be established.

Of these images, 13 were found be to illegal. (Appendix A: 3- 8, 10-14, 18, and 31), these images had been deleted.

2.1.2. Incident 2

On the 2nd of February, the accused downloaded and used tools to encrypt a file containing five IIOB.

The images can be found in Appendix A: 65-69.

See appendix E rows 107-113 for the internet history and appendix F for a detailed breakdown. Further information pertaining to the encrypted file can be found in appendix M.

2.1.3. Incident 3

Also on the 2nd of February, John Doe viewed a considerable number of websites pertaining to birding, more information can be found in the Firefox history breakdown in appendix F.

Included in this is the download of file aa010703a.htm, and the folder aa010703a_files. These files encompass a full webpage, in this case, a guide on building a bluebird nest box. More details can be found in appendix F.

2.1.4. Incident 4

John Doe partitioned his hard drive into two partitions (sections). A Windows operating system would only see the first partition, allowing the accused to hide files in the second partition for recovery with a specialized program or tool.

23 images were recovered from the second partition, these images are found in appendix A as numbers, 15 – 17, 19-24, 34 - 39, 41 - 44, 54, 55, 59, and 60.

Also on this hidden partition was a document “guide.doc”, a guide to “Enjoying Your First Birding Field Trip”. This document can be found in appendix L.

15-17, 19-24, and 54 were created on the 3rd of February and accessed on the 9th of February at the same time the other 12 were created. Further details on the location and information on when the files were created and accessed can be found in appendix B and appendix C, row 5.

2.1.5. Incident 5

The file ready2fledge.jpg is created in Bob's file directory on the 3rd of February at 1506. Evidence would suggest however that this image was placed there by Mr. Doe. At 1503, user account johndoe is conducting a Google image search for "chick2.jpg" as shown in appendix E, row 138. At 1506, johndoe is accessing the image ready2fledge.jpg with internet explorer as shown in appendix S, row 59.

2.1.6. Incident 6

The file CrouchingKokako.dll was created on the 3rd of February 2005 and is a renamed zip file. Due to the renamed file extension, Windows would not have seen the file as a zip file. The file contains seven IIOB, found in appendix A, 25-30, and 56. This file would have been manually changed to disguise it. See appendix C, row 3 for information on the file.

2.1.7. Incident 7

The file "birdwatching.doc" is created on the HDD at the root directory (C:\). This document details birdwatching in Thailand.

The document can be found in appendix U.

2.1.8. Incident 8

John Doe received two emails from "Ben Forbes – ben@example.com" to his personal email address, jdoe@example.com on the 8th of February 2005.

The first of these emails was received at 1413, and contained three attachments, two of which were IIOB. These images can be found in appendix A as image no's 45 and 47.

The second email was received at 1435 and contained four attachments, all four were classified as IIOB, these images can be found as the following: 46, 48, 49, and 50.

The content of the second email is as follows:

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

This would suggest that Ben Forbes and John Doe have exchanged IIOB at least once, however no sent emails could be recovered.

All information relating to these emails can be found in appendix D, rows 2 and 3.

2.1.9. Incident 8

On the 9th of February 2005, John Doe looked for bird wallpapers online (further details can be found in appendix F). An exe file was then selected and downloaded in order to set a slideshow of bird pictures as the screensaver. These images were captured and can be found in appendix A, numbers 70 – 78.

3. Description of Investigation

3.1. Job Description and Instructions

On the 7th of February 2017, the digital forensics examiner was summoned by Police Scotland to the home of John Doe to seize all computer equipment for investigation. Under suspicion of possessing and distributing inappropriate images of birds, any seized equipment would be investigated.

3.2. Description of Recovered/Examined Items

ITEM ID	NAME	DESCRIPTION	SERIAL NUMBER
MSDSJM/01	Tower	HP EliteDesk 800 G2	CZC624990T
MSDSJM/02	Monitor	Elitedisplay E202 Monitor	6CM6090GDN
MSDSJM/03	Keyboard	HP HQ-TRE 71025 Keyboard	CT-BEXHQ0AQR296JB
MSDSJM/04	Mouse	Black Optical Mouse	CT-FCMHH0AHD9VIBV
MSDSJM/05	Cables	Ethernet Cable Power Cable – Tower Power Cable – Monitor Display Port Cable	N/A

Table 1 – Recovered/Examined Items

See Appendix G for images of the initial entry and seizure of equipment.

The equipment was found on the desk in the home of the accused. As the images show, the USB ports were empty in both the tower and the monitor. The tower was connected to an ethernet jack and both the monitor and the tower were plugged in, with the sockets on. The computer was in a powered off state when found. Once categorised, the computer was booted into the BIOS to establish clock skew. The clock on the computer was found to be correct to within one minute, this establishes that the times on the incidents is accurate. The clock skew can be found in Appendix H.

Once seized, all items were moved to the evidence locker and possession was transferred to the desk sergeant. The chain of custody record can be found in Appendix I.

The tower (item MSDSJM /01) was signed back of the evidence locker to remove the hard drive (HDD). The details of the HDD are as follows:

ITEM ID	NAME	DESCRIPTION	SERIAL NUMBER
MSDSJM /06	HDD	Western Digital 20GB	WMAC82390427

Table 2 - Removed Items

3.3. Methodology

Once the hard drive was extracted from the pc the drive was connected to a computer running the Linux operating system to create a physical image of the disk. The HDD was connected to the analysis workstation using a SATA/IDE/USB cable. To prevent changing any of the data on the HDD, a write blocker was used so the workstation could read from the HDD but could not write to the HDD of John Doe – maintaining the state of the drive. The drive was copied with the "dcfldd" tool and the md5 hash generated so the integrity of the drive image could be verified. An md5 hash of the newly created image was compared to the hash of the drive and was found to be identical – verifying the image was a perfect copy of the drive. See appendix N for the hash comparison. To establish integrity throughout the investigation, the file permissions of the disk image and the md5 hashes were changed to read only – preventing changes from being made. This check was undertaken every time the image was mounted.

Once a verified disk image was obtained, the Linux tools fdisk and mmls were used to analyse the disk space. It was discovered the hard drive had a total capacity of 5.36GB with two partitions. Partition one was formatted to ntfs and was 2.93GB in size, this is the partition windows is installed on. Partition two was 2.44GB in size and is unallocated – this means it cannot be accessed from within Windows. During the investigation, a virtual machine was created from the John Doe image – this allows for the machine to be used as if it was John Doe's pc. From here, the disk partition information was confirmed – see appendix Q.

Once it became possible to mount the HDD image, a malware scan was undertaken to check for malicious software. The scan returned negative for viruses, the scan results can be found in appendix T.

3.4. Analysis

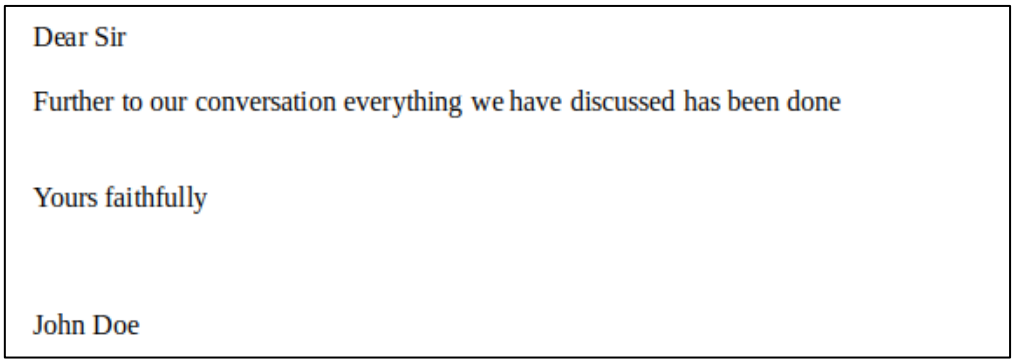
In order to view any images that had been deleted, hidden within other files, or stored on unallocated areas of the hard drive, autopsy 4.3.0 was used to carve – extract data – from the disk image. These images were then manually checked to ascertain if they contained any illegal content. Autopsy was used to also extract the locations and information for each file on the system and any emails John Doe received. This information can be viewed at appendices B and C, and D respectively.

Once any illegal or suspicious images had been extracted, the windows tool exiftool was used to extract data within the images. This data contains any information on the camera used to take the picture along with the camera settings used if applicable. From this information the file name, size, type, creation and last modified date and the name of the camera used to take the image - if applicable - was selected – this information can be found in appendix K. However, due to the inability to check the camera's time and date settings, the date set on the camera could not be confirmed therefore the creation dates in the EXIF data cannot be confirmed.

To examine the internet history of the users, the Windows program Web Historian was used to generate spreadsheets of information for each installed browser. The internet browsing history for johndoe can be found in E. From this information, it becomes possible to follow John Doe's tracks online.

3.4.1. Ownership

A document (stuf.doc) was found on the hard drive which indicates that the computer was owned by the accused. The document in question appears to be a typed letter which is signed with the accused's name. This document can be seen below.


Dear Sir

Further to our conversation everything we have discussed has been done

Yours faithfully

John Doe

Figure 1 - stuf.doc

The Linux tool regripper was installed to extract data from the registry files (system files) on the John Doe image. Using regripper, it is possible to extract the information containing the name of computer, "JOHN", suggesting further that the owner of the pc is John Doe.
This file can be found in appendix O.

Regripper can also be used to ascertain the account types of each user. This data shows three users on the machine, johndoe, bob, and jane. Of these, johndoe is the only user with administrator level privileges – the other user accounts are limited. This information also shows johndoe has logged in 21 times over the time the account has been active while the other accounts have only been logged in once. The regripper results can be found in appendix P.

3.5. Production List and Associated Description

TITLE	DESCRIPTION	LOCATION
IMAGES	Images recovered from the disk found to be in breach of the law	Appendix A
IMAGE INFORMATION	Spreadsheet showing names, locations, creation dates, last accessed dates and capture devices for the images used in this investigation	Appendix B
FILE INFORMATION	Spreadsheet containing file names, locations, file types, creation dates and last accessed dates for files used in the investigation	Appendix C
EMAIL INFORMATION	Subject, from and to addresses, attachment names, received date and content of any emails used in this investigation	Appendix D
JOHN DOE HISTORY – FIREFOX	Internet history from Mozilla Firefox for the user johndoe with highlighted entries of interest, colour coded by day	Appendix E
JOHN DOE HISTORY – FIREFOX - BREAKDOWN	Breakdown of the Firefox history, sectioned by time	Appendix F
SEIZURE IMAGES	Images from the initial seizure of the equipment from the home of John doe	Appendix G
CLOCK SKEW PROOF	Image of the bios of the computer of John Doe alongside an accurate clock to access clock skew	Appendix H
CHAIN OF CUSTODY DOCUMENT	Exhibit movement list for the investigation	Appendix I
INITIAL EXAMINATION CHECKLIST		Appendix J
EXIF DATA	Exif data for each image found in appendix A	Appendix K
GUIDE.DOC	Recovered file	Appendix L
GPG FILE DECRYPT	Explanation of the gpg format and explanation of the decryption process	Appendix M
HASH COMPARISON	Comparison of the md5 hashes of the hard drive and the initial image	Appendix N
EVENTLOGS.TXT	Regripper result for the event log settings	Appendix O
SAM USERS	Regripper result for the user information extracted from the SAM file	Appendix P
DISK PARTITIONS	Disk partition screenshot from the John Doe VM	Appendix Q
DOWNLOADS	Firefox downloads screenshot from the John Doe VM	Appendix R
JOHN DOE HISTORY – INTERNET EXPLORER	Internet explorer history information for the user johndoe	Appendix S
MALWARE SCAN	Images showing the mounting of the John Doe image and the malware scan of the files	Appendix T
BIRDWATCHING.DOC	Recovered file	Appendix U

Table 3 - Production Lis

4. Conclusions

From the equipment seized from the home of Mr John Doe, 81 law breaching files related to birds and birdwatching were recovered.

The investigation revealed multiple links to the accused. From the techniques used to hide some of the, it cannot be denied the accused was aware of the files in his possession, and made substantial efforts to hide them.

These files can only have been intentionally acquired by John Doe, as the virus scan shows there is no malware on the system which could have been the cause of the files on the system.

It is the advice of the digital forensics examiner that based on the evidence found during this investigation John Doe should be charged with possession of illegal images of birds. In addition, based on the email exchanges with Ben Forbes, it is recommended Mr Doe be charged with suspected distribution of IIOB.

5. Equipment Required for Court Proceedings

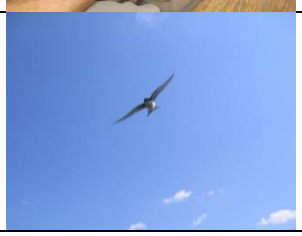
In order to present any evidence in a court of law, the following equipment need to be made available:

- The John Doe image, or HDD, from which an image will me made
- A digital forensics workstation, with the ability to run both Windows and Linux Ubuntu programs
- The following programs:
    - Anti-virus - Windows
    - Autopsy - Windows
    - Exiftool - Windows
    - Md5sum - Linux
    - Gpg - Linux
    - WinRAR/7zip - Windows

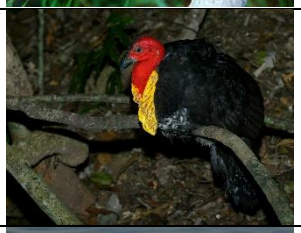
Appendices

Appendix A - Images

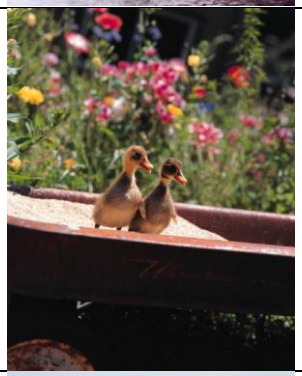
No.	Image	Name	Is Deleted
1.		0.jpg	
2.		117.jpg	
3.		3E8162AFd01	yes
4.		3E8262AFd01	yes
5.		3E8462AFd01	yes
6.		3E8662AFd01	yes

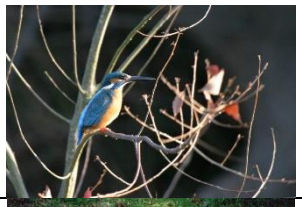
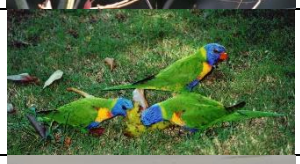
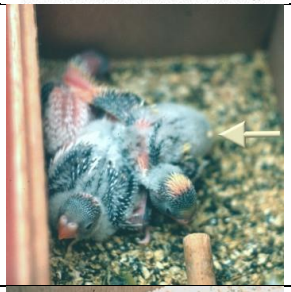
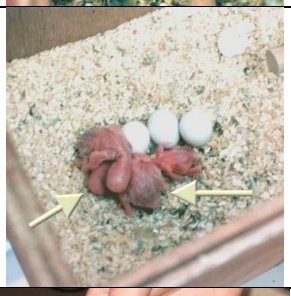
7.		3E8C62AFd01	yes
8.		4C3E89C6d01	yes
9.		67BAEB46d01	yes
10.		6A161D2Fd01	yes
11.		978D14DDd01	yes
12.		A0016363d01	yes
13.		A2E5F216d01	yes
14.		A3D4DDDDd01	yes

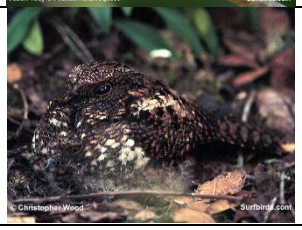
15.		AlmondMarshGreatBlueHeronStalling.jpg	
16.		AmericanAvocetWinterPlumage.jpg	
17.		AmericanWhitePelicansCircling.jpg	
18.		BF5BE9D9d01	yes
19.		BaldEagle7oClock.jpg	
20.		BarnOwl.jpg	
21.		BellbirdJumpingOffBranch.jpg	
22.		BlackNeckedStiltsFromBehind.jpg	

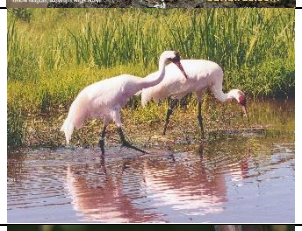
23.		BlackSwan.jpg	
24.		BlackVultureSunningOnPost.jpg	
25.		Brolga.jpg	
26.		BrushTurkeyPerching.jpg	
27.		CanadaGoose.jpg	
28.		CanadaGooseWashing.jpg	
29.		ChestnutMandibledToucan.jpg	
30.		CrouchingKokako.jpg	

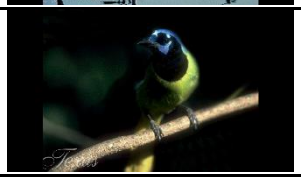
31.		EF29AEAEd01	yes
32.		FantailFrontView.exe	
33.		Firefox Wallpaper.bmp	
34.		GreatBlueHeronWithFish.jpg	
35.		GreatEgretInVoloBog.jpg	
36.		GreatEgretOverflyingRoseateSpoonbills.jpg	
37.		GreenHeronCloseup.jpg	
38.		GreenHeronOnChicagoLakeshore.jpg	

39.		ImmatureSnowyEgretTakingOff.jpg	
40.		J0178932.JPG	
41.		KeaAndMountain.jpg	
42.		KeaAtTopOfMacKinnonPass0930.jpg	
43.		KeaEatingRentalCar.jpg	
44.		KeaRetrievingBakedBeanCanFromTarn.jpg	
45.		_7_E_Y_B_T_E_L_F_1_K_A_N_._j_p_g_	
46.		_B_C_7_ _f_e_e_d_i_n_g_ _t_h_e_ _b_i_r_d_s_._j_p_g_	

47.		_I_M_G___3_9_3_7___f_i_l_t_e_r_e_d_._j_p_g_	
48.		_c_o_l_o_r_f_u_l_-_b_i_r_d_s_._j_p_g_	
49.		_g_a_w_a_l_l_8_._j_p_g_	
50.	 *Nesting red-winged blackbird/ Carouge à épaulettes en cours de nidification Mike Hopiak / Cornell Lab of Ornithology*	_g_l_f_s_-_s_t_o_r_m_-_b_i_r_d_s_._j_p_g_	
51.		babyscot_2weeks1.jpg	
52.		babyscot_vyoung.jpg	
53.		birdtrans2.jpg	

54.		blue_bird2.jpg	
55.		brd_Ornithologist_TWG.jpg	
56.		brd_WoodDuck.jpg	
57.		chicks2.jpg	
58.		f0526960.jpg	yes
59.		june03screen.jpg	
60.		junescreen01.jpg	

61.		newbies2.jpg	
62.		ready2fledge.jpg	
63.		snow_geese.jpg	
64.		tn_duck_3.jpg	
65.		yellow-wag-cover-nb.jpg	
66.		WhoopingCranes.jpg	
67.		WhiteThroatedSparrowInTree.jpg	
68.		WhiteFrontedParrot.jpg	

69.		WhiteFacedHeronFlying.jpg	
70.		Screensaver 1	
71.		Screensaver 2	
72.		Screensaver 3	
73.		Screensaver 4	
74.		Screensaver 5	
75.		Screensaver 6	
76.		Screensaver 7	
77.		Screensaver 8	
78.		Screensaver 9	

Appendix B – Image Information

No.	Name	Location	Creation date	Last accessed	Device
1.	_7_E_Y_B_T_E_L_F_1_K_A_N_._j_p_g_	johndoe/Application Data/Thunderbird/Profiles/8jiqrt8v.default/Mail/Local Folders/Inbox/	**Unknown**	**Unknown**	
2.	_B_C_7_ _f_e_e_d_i_n_g_ _t_h_e_ _b_i_r_d_s_._j_p_g_	johndoe/Application Data/Thunderbird/Profiles/8jiqrt8v.default/Mail/Local Folders/Inbox/	**Unknown**	**Unknown**	CyberShot
3.	_c_o_l_o_r_f_u_l_-_b_i_r_d_s_._j_p_g_	johndoe/Application Data/Thunderbird/Profiles/8jiqrt8v.default/Mail/Local Folders/Inbox/	**Unknown**	**Unknown**	
4.	_c_u_t_e___p_e_n_g_u_i_n_._j_p_g_	johndoe/Application Data/Thunderbird/Profiles/8jiqrt8v.default/Mail/Local Folders/Inbox/	**Unknown**	**Unknown**	
5.	_g_a_w_a_l_l_8_._j_p_g_	johndoe/Application Data/Thunderbird/Profiles/8jiqrt8v.default/Mail/Local Folders/Inbox/	**Unknown**	**Unknown**	
6.	_g_l_f_s_-_s_t_o_r_m_-_b_i_r_d_s_._j_p_g_	johndoe/Application Data/Thunderbird/Profiles/8jiqrt8v.default/Mail/Local Folders/Inbox/	**Unknown**	**Unknown**	
7.	_I_M_G___3_9_3_7___f_i_l_t_e_r_e_d_._j_p_g_	johndoe/Application Data/Thunderbird/Profiles/8jiqrt8v.default/Mail/Local Folders/Inbox/	**Unknown**	**Unknown**	
8.	_I_M_G___3_9_3_7___f_i_l_t_e_r_e_d_._j_p_g_	johndoe/Application Data/Thunderbird/Profiles/8jiqrt8v.default/Mail/Local Folders/Inbox/	**Unknown**	**Unknown**	
9.	0.jpg	johndoe/My Documents/My Music/ Doc1.doc/0.jpg	**Unknown**	**Unknown**	
10.	1238C212d01	vol_vol2/$OrphanFiles/	03-02-05 15:04	03-02-05 15:05	Canon PowerShot SD100
11.	177.jpg	johndoe/My Documents/My Pictures	03-02-05 15:01	03-02-05 15:05	Canon PowerShot SD100
12.	3328DD4Ed01	johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/Cache/	09-02-05 11:27	09-02-05 11:27	FireFox cache
13.	3E8162AFd01	vol_vol2/$OrphanFiles/	03-02-05 15:04	03-02-05 15:04	Canon PowerShot SD100
14.	3E8262AFd01	vol_vol2/$OrphanFiles/	03-02-05 15:04	03-02-05 15:04	Canon PowerShot SD100
15.	3E8462AFd01	vol_vol2/$OrphanFiles/	03-02-05 15:04	03-02-05 15:04	Canon PowerShot SD100
16.	3E8662AFd01	vol_vol2/$OrphanFiles/	03-02-05 15:04	03-02-05 15:04	Canon PowerShot SD100
17.	3E8762AFd01	vol_vol2/$OrphanFiles/	03-02-05 15:04	03-02-05 15:04	Canon PowerShot SD100
18.	3E8C62AFd01	vol_vol2/$OrphanFiles/	03-02-05 15:04	03-02-05 15:04	Canon PowerShot SD100
19.	40m.jpg	johndoe/My Documents/My Pictures	02-02-05 14:43	03-02-05 15:00	Canon PowerShot SD100
20.	4C3E89C6d01	vol_vol2/$OrphanFiles/	03-02-05 15:04	03-02-05 15:04	Canon PowerShot SD100
21.	67BAEB46d01	vol_vol2/$OrphanFiles/	03-02-05 15:01	03-02-05 15:01	Canon PowerShot SD100
22.	6A161D2Fd01	vol_vol2/$OrphanFiles/	03-02-05 15:04	03-02-05 15:04	Canon PowerShot SD100
23.	7107298.jpg	johndoe/My Documents/My Pictures	02-02-05 14:20	03-02-05 11:49	Canon PowerShot SD100
24.	83E8FA9Dd01	johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/Cache/	09-02-05 11:27	09-02-05 11:27	FireFox cache
25.	8FF8EA93d01	johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/Cache/	09-02-05 11:27	09-02-05 11:27	FireFox cache
26.	93C4F412d01	vol_vol2/$OrphanFiles/	03-02-05 15:04	03-02-05 15:05	Canon PowerShot SD100
27.	978D14DDd01	vol_vol2/$OrphanFiles/	03-02-05 15:04	03-02-05 15:04	Canon PowerShot SD100
28.	A0016363d01	vol_vol2/$OrphanFiles/	03-02-05 15:04	03-02-05 15:04	Canon PowerShot SD100

29.	A2E5F216d01	vol_vol2/$OrphanFiles/	03-02-05 15:04	03-02-05 15:04	
30.	A3D4DDDDd01	vol_vol2/$OrphanFiles/	03-02-05 15:04	03-02-05 15:04	Canon PowerShot SD100
31.	AA784519d01	vol_vol2/$OrphanFiles/AA784519d01	03-02-05 15:04	03-02-05 15:04	Canon PowerShot SD100
32.	AlmondMarshGreatBlueHeronStalling.jpg	vol_vol3/	03-02-05 11:42	09-02-05 17:06	Canon PowerShot SD100
33.	AmericanAvocetWinterPlumage.jpg	vol_vol3/	03-02-05 11:42	09-02-05 17:05	
34.	AmericanWhitePelicansCircling.jpg	vol_vol3/	03-02-05 11:42	09-02-05 17:05	Canon EOS-1DS
35.	B2906B79d01	johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/Cache/	09-02-05 11:27	09-02-05 11:27	FireFox cache
36.	B6E0589Dd01	johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/Cache/	09-02-05 11:27	09-02-05 11:27	FireFox cache
37.	B6E058BDd01	johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/Cache/	09-02-05 11:27	09-02-05 11:27	FireFox cache
38.	B76BD0AEd01	vol_vol2/$OrphanFiles/B76BD0AEd01	03-02-05 15:04	03-02-05 15:04	Canon PowerShot SD100
39.	babyscot_2weeks1.jpg	johndoe/My Documents/My Pictures	03-02-05 15:00	03-02-05 15:01	Canon PowerShot SD100
40.	babyscot_vyoung.jpg	johndoe/My Documents/My Pictures	03-02-05 15:00	03-02-05 15:00	
41.	BaldEagle7oClock.jpg	vol_vol3/	03-02-05 11:42	09-02-05 17:05	
42.	BarnOwl.jpg	vol_vol3/	03-02-05 11:42	09-02-05 17:05	
43.	BellbirdJumpingOffBranch.jpg	vol_vol3/	03-02-05 11:42	09-02-05 17:05	
44.	BF5BE9D9d01	vol_vol3/	03-02-05 15:04	03-02-05 15:04	Canon PowerShot SD100
45.	birdtrans2.jpg	johndoe/Desktop	03-02-05 15:04	03-02-05 15:04	Canon PowerShot SD100
46.	BlackNeckedStiltsFromBehind.jpg	vol_vol3/	03-02-05 11:42	09-02-05 17:05	
47.	BlackSwan.jpg	vol_vol3/	03-02-05 11:42	09-02-05 17:05	
48.	BlackVultureSunningOnPost.jpg	vol_vol3/	03-02-05 11:42	09-02-05 17:05	
49.	blue_bird2.jpg	vol_vol3/	03-02-05 11:42	09-02-05 16:51	
50.	brd_Ornithologist_TWG.jpg	vol_vol3/	03-02-05 11:42	09-02-05 17:05	
51.	chicks2.jpg	johndoe/My Documents/My Pictures	03-02-05 15:05	03-02-05 15:05	Canon PowerShot SD100
52.	E1663DDEd01	vol_vol2/$OrphanFiles/	03-02-05 15:04	03-02-05 15:04	Canon PowerShot SD100
53.	EF29AEAEd01	vol_vol2/$OrphanFiles/	03-02-05 15:04	03-02-05 15:04	Canon PowerShot SD100
54.	FB4EDA00d01	vol_vol2/$OrphanFiles/FB4EDA00d01	03-02-05 15:04	03-02-05 15:04	Canon PowerShot SD100
55.	Firefox Wallpaper.bmp	vol_vol2/WINDOWS/	02-02-05 14:16	03-02-05 11:51	
56.	frankbeecostume_1827_34457581	vol_vol2/Program Files/	03-02-05 15:42	03-02-05 15:42	
57.	frankbeecostume_1827_84985892	vol_vol2/Program Files/	03-02-05 15:42	03-02-05 15:42	
58.	frankbeecostume_1827_96360352	vol_vol2/Program Files/	03-02-05 15:42	03-02-05 15:42	
59.	GreatBlueHeronWithFish.jpg	vol_vol3/	09-02-05 17:05	09-02-05 17:05	

60.	GreatEgretInVoloBog.jpg	vol_vol3/	09-02-05 17:05	09-02-05 17:05	
61.	GreatEgretOverflyingRoseateSpoonbills.jpg	vol_vol3/	09-02-05 17:05	09-02-05 17:05	
62.	GreenHeronCloseup.jpg	vol_vol3/	09-02-05 17:05	09-02-05 17:05	
63.	GreenHeronOnChicagoLakeshore.jpg	vol_vol3/	09-02-05 17:05	09-02-05 17:05	
64.	ImmatureSnowyEgretTakingOff.jpg	vol_vol3/	09-02-05 17:05	09-02-05 17:05	
65.	june03screen.jpg	vol_vol3/	09-02-05 17:05	09-02-05 17:05	
66.	junescreen01.jpg	vol_vol3/	09-02-05 17:05	09-02-05 17:05	
67.	KeaAndMountain.jpg	vol_vol3/	09-02-05 17:05	09-02-05 17:05	FireFox cache
68.	KeaAtTopOfMacKinnonPass0930.jpg	vol_vol3/	09-02-05 17:05	09-02-05 17:05	
69.	KeaEatingRentalCar.jpg	vol_vol3/	09-02-05 17:05	09-02-05 17:05	
70.	KeaRetrievingBakedBeanCanFromTarn.jpg	vol_vol3/	09-02-05 17:05	09-02-05 17:05	
71.	newbies2.jpg	johndoe/My Documents/My Pictures	03-02-05 15:05	09-02-05 16:57	Canon PowerShot SD100
72.	ready2fledge.jpg	bob/My Documents/My Music/	03-02-05 15:06	03-02-05 15:06	Canon PowerShot SD100
73.	snow_geese.jpg	johndoe/My Documents/My Pictures	02-02-05 14:18	03-02-05 11:49	Canon PowerShot SD100
74.	tn_duck_3.jpg	johndoe/My Documents/My Pictures	02-02-05 14:18	03-02-05 11:49	
75.	WhiteFacedHeronFlying.jpg	johndoe/My Documents/birdpics.gpg	**Unknown**	**Unknown**	
76.	WhiteFrontedParrot.jpg	johndoe/My Documents/birdpics.gpg	**Unknown**	**Unknown**	
77.	WhiteThroatedSparrowInTree.jpg	johndoe/My Documents/birdpics.gpg	**Unknown**	**Unknown**	
78.	WhoopingCranes.jpg	johndoe/My Documents/birdpics.gpg	**Unknown**	**Unknown**	
79.	yellow-wag-cover-nb.jpg	johndoe/My Documents/birdpics.gpg	**Unknown**	**Unknown**	
80.	Screensaver 1	WINDOWS/tx_birds.exe	09-02-05 13:50	**Unknown**	
81.	Screensaver 2	WINDOWS/tx_birds.exe	10-02-05 13:50	**Unknown**	
82.	Screensaver 3	WINDOWS/tx_birds.exe	11-02-05 13:50	**Unknown**	
83.	Screensaver 4	WINDOWS/tx_birds.exe	12-02-05 13:50	**Unknown**	
84.	Screensaver 5	WINDOWS/tx_birds.exe	13-02-05 13:50	**Unknown**	
85.	Screensaver 6	WINDOWS/tx_birds.exe	14-02-05 13:50	**Unknown**	
86.	Screensaver 7	WINDOWS/tx_birds.exe	15-02-05 13:50	**Unknown**	
87.	Screensaver 8	WINDOWS/tx_birds.exe	16-02-05 13:50	**Unknown**	
88.	Screensaver 9	WINDOWS/tx_birds.exe	17-02-05 13:50	**Unknown**	

Table 4 - Image Information

89. Appendix C – File Information

No.	Name	Location	File Type	Creation date	Last accessed
1.	birdpics.gpg	vol_vol2/Documents and Settings/bob/My Documents/	gpg	02-02-05 16:46	03-02-05 11:45
2.	birdwatching.doc	vol_vol2/	doc	03-02-05 15:49	03-02-05 15:49
3.	CrouchingKokako.dll	Vol_vol2/WINDOWS	Zip	02-02-05 14:16	03-02-05 12:11
4.	Dear Fred.doc	vol_vol2/Documents and Settings/bob/My Documents/	doc	03-02-05 10:30	03-02-05 10:30
5.	guide.doc	vol_vol3/	doc	03-02-05 15:44	03-02-05 15:44
6.	stuf.doc	vol_vol2/Documents and Settings/johndoe/My Documents/	doc	09-02-05 16:56	09-02-05 16:57
7.	tx_birds.exe	vol_vol2/WINDOWS/	exe	09-02-05 11:28	09-02-05 13:50

Table 5 - File Information

8. Appendix D – Email Information

No.	Subject	From	To	Attachments	Received	Content
1.	How to Identify Birds	from: Bird Fanciers <mailinglist@birds.example.com>	jdoe@example.com		16-10-04 15:20	
2.	good pics	from: Ben Forbes <ben@example.org>	jdoe@example.com	7EYBTELF1KAN.jpg, img_3937_filtered.jpg, cute_penguin.jpg	08-02-05 14:13	Hi thought you'd like these enjoy
3.	some more good ones	from: Bird Fanciers <mailinglist@birds.example.com>	jdoe@example.com	BC7 feeding the birds.jpg, glfs-storm-birds.jpg, colorful-birds.jpg, gawall8.jpg	08-02-05 14:35	Thanks for the pics you sent me here are some I really like

Table 6 - Email Information

Appendix E – John Doe History – Firefox

	Mandiant: Web Historian - 1 - C:\Users\amg\Desktop\johndoe\Application Data\Mozilla\Firefox\Profiles\w4nf3obl.default\history.dat			
	Name	**URL Address**	**First Visit**	**Visits**
1.		http://www.google.co.uk/cxfer?c=PREF%3D:TM%3D1106584100:S%3DmHsHVdKldLZ9yvE_&prev=/firefox%3Fclient%3Dfirefox-a%26rls%3Dorg.mozilla:en-GB:official	1-24-05 16:28	1
2.	Mozilla Firefox Start Page	http://www.google.co.uk/cxfer?c=PREF%3D:TM%3D1106584100:S%3DmHsHVdKldLZ9yvE_&prev=/firefox%3Fclient%3Dfirefox-a%26rls%3Dorg.mozilla:en-GB:official	1-24-05 16:28	2
3.		http://www.google.com/firefox?client=firefox-a&rls=org.mozilla:en-GB:official	1-24-05 16:28	2
4.		http://start.mozilla.org/firefox?client=firefox-a&rls=org.mozilla:en-GB:official	1-24-05 16:28	3
5.		http://www.google.com/firefox?client=firefox-a&rls=org.mozilla:en-GB:official	1-24-05 16:28	3
6.	Mozilla Firefox Start Page	http://www.google.co.uk/firefox?client=firefox-a&rls=org.mozilla:en-GB:official	1-24-05 16:28	5
7.		http://www.google.com/firefox?client=firefox-a&rls=org.mozilla:en-GB:official	1-24-05 16:28	5
8.		http://start.mozilla.org/firefox?client=firefox-a&rls=org.mozilla:en-GB:official	1-24-05 16:28	5
9.	About Mozilla	http://www.mozilla.org/about/	1-24-05 16:28	1
10.	Mozilla Products	http://www.mozilla.org/products/	1-24-05 16:28	1
11.	Thunderbird - Reclaim Your Inbox	http://www.mozilla.org/products/thunderbird/	1-24-05 16:28	1
12.		http://download.mozilla.org/?product=thunderbird&os=win&lang=en-US	1-24-05 16:28	1
13.		ftp://ftp.scarlet.be/pub/mozilla.org/thunderbird/releases/1.0/win32/en-US/Thunderbird%20Setup%201.0.exe	1-24-05 16:28	1
14.		http://r.office.microsoft.com/r/rlidOfficeUpdate?clid=1033	1-25-05 11:15	1
15.		http://office.microsoft.com/officeupdate	1-25-05 11:15	1
16.	Microsoft Office Downloads Home Page	http://office.microsoft.com/en-gb/officeupdate/default.aspx	1-25-05 11:15	1
17.		http://office.microsoft.com/officeupdate/	1-25-05 11:15	1
18.	Microsoft Office Online: Internet Explorer version 5.0 or later is required	http://office.microsoft.com/en-gb/FX010532551033.aspx	1-25-05 11:15	1
19.		http://office.microsoft.com/officeupdate/maincatalog.aspx?lc=en-gb	1-25-05 11:15	1
20.		http://office.microsoft.com/search/redir.aspx?AssetID=ES790020331033&Origin=HH010704921033&CTT=5	1-25-05 11:15	1
21.	Microsoft Office Downloads: Office Download Catalog	http://office.microsoft.com/en-gb/officeupdate/CD010200271033.aspx	1-25-05 11:15	1
22.		http://office.microsoft.com/search/redir.aspx?AssetID=CD010200271033&CTT=5&Origin=HA010704291033	1-25-05 11:15	1
23.	Google Search: birds	http://www.google.co.uk/search?client=firefox-a&rls=org.mozilla%3Aen-GB%3Aofficial_s&hl=en&q=birds&meta=&btnG=Google+Search	2-2-05 14:11	1
24.	The Life of Birds	http://www.pbs.org/lifeofbirds/	2-2-05 14:11	2
25.	The Life of Birds | Songs	http://www.pbs.org/lifeofbirds/songs/index.html	2-2-05 14:12	2
26.		http://www.googleadservices.com/pagead/adclick?adurl=http://www.amazon.co.uk/exec/obidos/external-search%3Ftag%3Droscosolutions%26keyword%3Dbirds%26mode%3Dbooks-uk&sa=L&ai=BW2r0o98AQvKADLuuQbHk9JwHhtWFCMrNsqsBt7bCBaCNBhAEGAQgtlQoBTgAQIoWSLs5oAHVtMD_A6oBHG9yZy5tb3ppbGxhOmVuLUdCOm9mZmljaWFsX3PIAQE&num=4	2-2-05 14:14	1
27.	Amazon.co.uk: Search Results Books: birds	http://www.amazon.co.uk/exec/obidos/external-search/026-5665785-2744400?tag=roscosolutions&keyword=birds&mode=books-uk	2-2-05 14:14	1
28.		http://www.google.co.uk/pagead/iclk?adurl=http://www.amazon.co.uk/exec/obidos/external-search%3Ftag%3Droscosolutions%26keyword%3Dbirds%26mode%3Dbooks-uk&sa=l&ai=BW2r0o98AQvKADLuuQbHk9JwHhtWFCMrNsqsBt7bCBaCNBhAEGAQgtlQoBTgAQIoWSLs5oAHVtMD_A6oBHG9yZy5tb3ppbGxhOmVuLUdCOm9mZmljaWFsX3PIAQE&num=4	2-2-05 14:14	1

29.		http://www.amazon.co.uk/exec/obidos/external-search?tag=roscosolutions&keyword=birds&mode=books-uk	2-2-05 14:14	1
30.	Amazon.co.uk: Books: Garden Birds (Collins Gem S.)	http://www.amazon.co.uk/exec/obidos/ASIN/0007176147/qid=1107353690/sr=2-1/ref=sr_2_11_1/026-5665785-2744400	2-2-05 14:14	1
31.	Amazon.co.uk: Books: The Secret Lives of Garden Birds	http://www.amazon.co.uk/exec/obidos/ASIN/0713666161/qid=1107353690/sr=2-3/ref=sr_2_11_3/026-5665785-2744400	2-2-05 14:15	1
32.	Google Search: bird wallpaper	http://www.google.co.uk/search?q=bird+wallpaper&sourceid=mozilla-search&start=0&start=0&ie=utf-8&oe=utf-8&client=firefox-a&rls=org.mozilla:en-GB:official	2-2-05 14:15	1
33.	Free Bird Wallpaper - Bald Eagle Albatross Owl Falcon 1024x768	http://www.naturewallpaper.net/birds_L.html	2-2-05 14:15	1
34.		http://as.casalemedia.com/s?s=53524&u=http%3A//www.naturewallpaper.net/birds_L.html&f=2&id=5780266264.517584	2-2-05 14:15	1
35.	3-Home	http://isg10.casalemedia.com/V2/40842/43608/	2-2-05 14:15	1
36.		http://pagead2.googlesyndication.com/pagead/ads?client=ca-pub-0241683974610684&dt=1107353756202&lmt=1107353751&format=468x60_as&output=html&url=http%3A%2F%2Fwww.naturewallpaper.net%2Fbirds_L.html&ref=http%3A%2F%2Fwww.google.co.uk%2Fsearch%3Fq%3Dbird%2Bwallpaper%26sourceid%3Dmozilla-search%26start%3D0%26start%3D0%26ie%3Dutf-8%26oe%3Dutf-8%26client%3Dfirefox-a%26rls%3Dorg.mozilla%3Aen-GB%3Aofficial&u_h=768&u_w=1024&u_ah=738&u_aw=1024&u_cd=24&u_his=5&u_nplug=5&u_nmime=13	2-2-05 14:15	1
37.		http://asg36.casalemedia.com/s?s=53524&u=http%3A//www.naturewallpaper.net/birds_L.html&f=2&id=5780266264.517584	2-2-05 14:15	1
38.		http://isg10.casalemedia.com/V2/40842/43608	2-2-05 14:15	1
39.	bald_eagle3.jpg	http://www.naturewallpaper.net/birdsLpages/image4.html	2-2-05 14:16	1
40.	Winner !!!!	http://media.fastclick.net/w/get.media?t=n&sid=11194&m=1&f=b&v=1.4&c=1495&r=http%3A//www.naturewallpaper.net/birds_L.html&d=f	2-2-05 14:16	1
41.		http://pagead2.googlesyndication.com/pagead/ads?client=ca-pub-0241683974610684&dt=1107353782360&lmt=1107353781&format=468x60_as&output=html&url=http%3A%2F%2Fwww.naturewallpaper.net%2FbirdsLpages%2Fimage4.html&ref=http%3A%2F%2Fwww.naturewallpaper.net%2Fbirds_L.html&u_h=768&u_w=1024&u_ah=738&u_aw=1024&u_cd=24&u_his=6&u_nplug=5&u_nmime=13	2-2-05 14:16	1
42.	Winner !!!!	http://media.fastclick.net/w/get.media?t=n&sid=11194&m=1&f=b&v=1.4&c=7262&r=http%3A//www.naturewallpaper.net/birds_L.html&d=f	2-2-05 14:18	1
43.	snow_geese.jpg	http://www.naturewallpaper.net/birdsLpages/image21.html	2-2-05 14:18	1
44.	SHOP.COM - Search results for bald eagle	http://uk.shop.com/amos/cc/main/ccn_search_catsa/st/bald+eagle/sy/products/ccsyn/518/SourceID/30	2-2-05 14:19	1
45.	SHOP.COM - Bird Safari - Bird Watcher's Paradise from Choices Direct - Movies is available in Documentary	http://amos.shop.com/amos/cc/main/catalog/pcd/7107298/prd/10187717/ccsyn/518/_x_/Choices-Direct---Movies-Bird-Safari---Bird-Watcher's-Paradise-(VIDEO)	2-2-05 14:20	1
46.	Google Search: bird stories	http://www.google.co.uk/search?hl=en&client=firefox-a&rls=org.mozilla%3Aen-GB%3Aofficial&q=bird+stories&btnG=Search&meta=	2-2-05 14:22	1
47.	Click Here!	http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding;svc=;site=birding;t=14;pc=1;fd=0;fs=0;a=;sbj=pid512;kw=;chan=hobbies;syn=about;tile=1;r=0;dcopt=ist;sz=728x90;ord=1522EMf0O20SA1B0c43	2-2-05 14:22	1
48.	Bird Stories and Tales	http://birding.about.com/od/storie1/	2-2-05 14:22	1
49.	Untitled Document	http://z.about.com/0/ip/496/0.htm	2-2-05 14:22	8
50.		http://z.about.com/0/ip/512/6.htm	2-2-05 14:22	8
51.		http://z.about.com/0/ip/512/12.htm	2-2-05 14:22	8
52.	Google Offers	http://z.about.com/5/ad/go.htm?gs=birding	2-2-05 14:22	8
53.		http://z.about.com/0/ip/417/5.htm?CDN=hobbies	2-2-05 14:22	8
54.	Click Here!	http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding;svc=;site=birding;t=14;pc=1;fd=0;fs=0;a=;sbj=pid512;kw=;chan=hobbies;syn=about;tile=4;r=0;sz=728x91;ord=1522EMf0O20SA1B0c43	2-2-05 14:22	1
55.	Audience Match Data Agent	http://z.about.com/5/ad/am.htm?pid=about	2-2-05 14:22	8
56.	Current Headlines	http://z.about.com/6/o/b.htm?gs=birding	2-2-05 14:22	7
57.	Wings of Terror - avian humor article for people interesting in birdwatching and others interested in birds	http://birding.about.com/library/weekly/aa102598.htm	2-2-05 14:23	1
58.		http://z.about.com/7/o/cw.htm?gs=birding	2-2-05 14:23	6
59.	Related Articles	http://z.about.com/5/o/c.htm?gs=birding	2-2-05 14:23	6

60.	Click Here!	http://n479ad.doubleclick.net/adi/abt.hobbies/hobbies_birding;svc=;site=birding;t=0;pc=3;fd=0;fs=0;a=;sbj=pid512;kw=;chan=hobbies;syn=about;tile=4;r=0;u=0mfh7s21101oie;sz=728x91;ord=1522ENr0N20SA0T0C668	2-2-05 14:23	1
61.	Alphabetical Index of Birds	http://birding.about.com/library/blalphatypeofbird.htm	2-2-05 14:23	1
62.		http://clk.about.com/?zi=18/yV&sdn=hobbies_birding&tm=51&f=00&su=p512.6.140.ip_p512.12.140.ip_&tt=0&zu=http%3A//birding.about.com/library/blalphatypeofbird.htm	2-2-05 14:23	1
63.		http://clk.about.com/?zi=18/yV&sdn=hobbies_birding&tm=20&f=00&su=p512.6.140.ip_p512.12.140.ip_&tt=0&zu=http%3A//birding.about.com/library/blhousespecs.htm	2-2-05 14:24	1
64.	Specs for Building Birdhouses and for use in Bird House Plans	http://birding.about.com/library/blhousespecs.htm	2-2-05 14:24	1
65.	How to Build Bird Houses and Nest Boxes	http://birding.about.com/od/buildhouses/	2-2-05 14:24	1
66.	Free Feeder and Birdhouse Plans Index	http://birding.about.com/cs/birdhousesfeeders/a/buildingindex.htm	2-2-05 14:24	1
67.	vonage_vpart_gothrubiz_336	http://view.atdmt.com/VON/iview/btcmxvon0260000015von/direct/01?click=http://n479ad.doubleclick.net/click%3Bh=v4|3213|3|0|%2a|q%3B12023409%3B0-0%3B0%3B7596722%3B4252-336|280%3B8795737|8813633|1%3Bu%3D0mfh7s21101oie%3B%7Eaopt%3D0|ff373b%3B%7Esscs%3D%3f	2-2-05 14:24	1
68.	Birding and Birdwatching - Build a Bluebird Nest Box for Wild Birds	http://birding.about.com/library/weekly/aa010703a.htm	2-2-05 14:24	1
69.	Birding and Birdwatching - Painting or Staining Bird Houses and Feeders	http://birding.about.com/library/blhousefeederpaint.htm	2-2-05 14:26	1
70.	Haith's Wild Bird Foods & Bill Oddie's tips and advice also bird feeder, peanut, birdseed, bird, garden birds, wildlife, nest box, bird table, birdcare, binocular, bird bath, squirrel, robin, books, videos & wildflower seeds,	http://www.haiths.com/	2-2-05 14:27	1
71.	Haith's Wild Bird Foods & Bill Oddie's tips and advice also bird feeder, peanut, birdseed, bird, garden birds, wildlife, nest box, bird table, birdcare, binocular, bird bath, squirrel, robin, books, videos & wildflower seeds,	http://www.haiths.com/Features.asp?lookup=0&brand=1&article_id=features_1&customer_id=PAA0219022305524FFFKSRSZKKXZGRWU	2-2-05 14:28	1
72.	The Birds (1963)	http://www.imdb.com/title/tt0056869/	2-2-05 14:40	1
73.		http://www.imdb.com/google/box?num=3;k=power100-withsc;placement=midbucket;rnd=45504;sid=7845;referer=%2Ftitle%2Ftt0056869%2F;slot=GOOGLE	2-2-05 14:40	1
74.	Trailers for The Birds (1963)	http://www.imdb.com/title/tt0056869/trailers	2-2-05 14:40	1
75.		http://www.imdb.com/google/box?num=3;k=power100-withsc;placement=midbucket;rnd=83932;sid=8055;referer=%2Ftitle%2Ftt0056869%2Ftrailers;slot=BOTTOM_CENTER	2-2-05 14:40	1
76.		http://rcm.amazon.com/e/cm?f=ifr&t=imdb-rec-banner-20&l=st1&search=widescreen&mode=dvd&p=13&o=1	2-2-05 14:40	1
77.		http://www.imdb.com/rg/title-tease/trailers/title/tt0056869/trailers	2-2-05 14:40	1
78.		http://www.imdb.com/google/box?num=5;k=maxww-sky;placement=2;rnd=872225854982059300;sid=-123;referer=maxww;slot=TOP_RHS	2-2-05 14:40	1
79.		http://www.imdb.com/rg/TITLETRA_VIDDET//http://videodetective.com/home.asp?PublishedID=1843	2-2-05 14:41	1
80.	VideoDetective.com - Movie Trailers, Entertainment Previews, Streaming Video Samples.	http://videodetective.com/home.asp?PublishedID=1843	2-2-05 14:41	1
81.		http://videodetective.com/test.asp?List=307629|838353&PublishedID=1843&ListID=&New=&CustomerId=97135&refreshed=TRUE	2-2-05 14:41	1
82.		http://videodetective.com/test.asp?List=307629|838353&PublishedID=1843&ListID=&New=&CustomerId=97135	2-2-05 14:41	1
83.		http://videodetective.com/player.asp?PublishedId=1843&List=307629|838353&Customerid=97135	2-2-05 14:41	1
84.	Video Detective Player	http://videodetective.com/choosespeed.asp?BrowserSupportActiveX=false&ActiveXPlayerInstalled=false&plugin=true&List=307629|838353&PublishedID=1843&ListID=&New=&CustomerId=97135&refreshed=TRUE	2-2-05 14:42	1
85.		http://videodetective.com/Playlist.asp?	2-2-05 14:42	1
86.		http://videodetective.com/titleinfo.asp	2-2-05 14:42	1
87.	Videodetective.com - Player	http://videodetective.com/player.asp?PublishedId=1843&List=307629|838353&CustomerID=97135&videokbrate=300	2-2-05 14:42	1
88.		http://videodetective.com/play.asp?New=True&List=307629|838353&PublishedId=1843&VideoKbrate=300&ListID=&CustomerId=97135&HasPlayer=	2-2-05 14:42	1

89.	BBC NEWS | News Front Page	http://news.bbc.co.uk/	2-2-05 14:44	2
90.		http://news.bbc.co.uk/nol/ukfs_news/hi/front_page/ticker.stm	2-2-05 14:44	1
91.	BBC NEWS | Politics | Blair defends house arrest plans	http://news.bbc.co.uk/1/hi/uk_politics/4227829.stm	2-2-05 14:44	1
92.	BBC Media Selector	http://www.bbc.co.uk/mediaselector/check/nolavconsole/ukfs_news/hi?redirect=fs.stm&news=1&bbram=1&bbwm=1&nbram=1&nbwm=1&nol_storyid=4229711	2-2-05 14:45	1
93.		http://news.bbc.co.uk/1/hi/uk_politics/4227829.stm#	2-2-05 14:45	1
94.	BBC NEWS | UK | Blair defends house arrest plans	http://news.bbc.co.uk/nolavconsole/ukfs_news/hi/newsid_4220000/newsid_4229700/bb_rm_4229711.stm	2-2-05 14:45	1
95.	Untitled	http://news.bbc.co.uk/nolavconsole/shared/player/player.stm?clipurl=http://news.bbc.co.uk/media/news_web/video/40545000/bb/40545855_bb_16x9.ram&bw=bb	2-2-05 14:45	1
96.		http://news.bbc.co.uk/nolavconsole/ukfs_news/hi/front_page/bb_rm_promo.stm	2-2-05 14:45	1
97.		http://news.bbc.co.uk/nolavconsole/ukfs_news/hi/front_page/bb_rm_banner.stm	2-2-05 14:45	1
98.	BBC Media Selector	http://www.bbc.co.uk/cgi-perl/mediaselector/app.pl?action=sc&alreadySeen=1&m=%2Fnolavconsole%2Fukfs_news%2Fhi&q=nbram%3D1%26redirect%3Dfs.stm%26news%3D1%26nbwm%3D1%26bbwm%3D1%26bbram%3D1%26nol_storyid%3D4229711&quality=HiQuality&player=RealPlayer&frm_Submit=OK	2-2-05 14:45	1
99.		http://www.bbc.co.uk/mediaselector/check/nolavconsole/ukfs_news/hi?redirect=fs.stm&nbram=1&news=1&bbwm=1&nbwm=1&bbram=1&nol_storyid=4229711&checkedBandwidth=bb&checkedMedia=ram&alreadySeen=1	2-2-05 14:45	1
100.	BBC News Player	http://news.bbc.co.uk/nolavconsole/ukfs_news/hi/bb_rm_fs.stm?checkedBandwidth=bb&nbram=1&checkedMedia=ram&news=1&nbwm=1&bbwm=1&bbram=1&nol_storyid=4229711	2-2-05 14:45	1
101.	Untitled	http://news.bbc.co.uk/nolavconsole/ukfs_news/hi/uk/bb_rm_promo.stm	2-2-05 14:45	2
102.	Untitled	http://news.bbc.co.uk/nolavconsole/shared/player/player.stm?title=Blair%20defends%20house%20arrest%20plans&clipurl=http://news.bbc.co.uk/media/news_web/video/40786000/bb/40786999_bb_16x9.ram&cs=news	2-2-05 14:45	2
103.		http://news.bbc.co.uk/nolavconsole/ukfs_news/hi/uk/bb_rm_banner.stm	2-2-05 14:45	2
104.	BBC NEWS | Scotland	http://news.bbc.co.uk/1/hi/scotland/default.stm	2-2-05 15:11	1
105.		http://www.pbs.org/lifeofbirds/songs/kakapo.ram	2-2-05 15:11	1
106.		http://www.pbs.org/lifeofbirds/songs/dawn.ram	2-2-05 15:12	1
107.	Google Search: windows gnupg	http://www.google.co.uk/search?q=windows+gnupg&sourceid=mozilla-search&start=0&start=0&ie=utf-8&oe=utf-8&client=firefox-a&rls=org.mozilla:en-GB:official	2-2-05 15:57	1
108.		http://www.gnupg.org/download.html	2-2-05 15:57	1
109.	Download - GnuPG.org	http://www.gnupg.org/download/	2-2-05 15:57	1
110.	WinPT	http://www.winpt.org/	2-2-05 15:58	1
111.		http://www.stud.uni-hannover.de/~twoaday/winpt.html	2-2-05 15:58	1
112.	Google Search: windows gnupg	http://www.google.co.uk/search?q=windows+gnupg&hl=en&lr=&client=firefox-a&rls=org.mozilla:en-GB:official&start=10&sa=N	2-2-05 15:58	1
113.	GnuPG Windows	http://openpgp.vie-privee.org/wingpg.html	2-2-05 15:58	1
114.	Microsoft Application Search	http://shell.windows.com/fileassoc/0409/xml/redir.asp?Ext=pdf	2-2-05 16:51	1
115.		http://shell.windows.com/fileassoc/0409/SearchEngine.asp	2-2-05 16:51	1
116.	Adobe Reader - Download	http://www.adobe.com/products/acrobat/readstep2.html	2-2-05 16:52	1
117.	Adobe Reader - Download Thank you	http://www.adobe.com/products/acrobat/readstep_servefile.html?hasjavascript=1&esdcanbeused=1&esdcanhandle=0&language=English&platform=WinXP&connectionspeed=broadband&option=full&nodlm=1&x=27&y=5	2-2-05 16:52	1
118.		http://ardownload.adobe.com/pub/adobe/reader/win/7x/7.0/enu/AdbeRdr70_enu_full.exe	2-2-05 16:53	1
119.	Google Search: bird mating calls	http://www.google.co.uk/search?client=firefox-a&rls=org.mozilla%3Aen-GB%3Aofficial_s&hl=en&q=bird+mating+calls&meta=&btnG=Google+Search	2-3-05 12:21	1
120.	Chickadee Karaoke	http://whyfiles.org/shorties/104chick_sex/	2-3-05 12:21	1
121.	Google Image Search	http://www.google.co.uk/imghp?hl=en&tab=wi&client=firefox-a&rls=org.mozilla:en-GB:official_s&q=	2-3-05 14:59	1
122.	Google Search: young chicks	http://images.google.co.uk/images?client=firefox-a&rls=org.mozilla%3Aen-GB%3Aofficial_s&q=young+chicks&hl=en&btnG=Google+Search	2-3-05 14:59	1
123.	Google Image Result for http://freespace.virgin.net/cobber.budgies/images/babyscot_vyoung.jpg	http://images.google.co.uk/imgres?imgurl=http://freespace.virgin.net/cobber.budgies/images/babyscot_vyoung.jpg&imgrefurl=http://freespace.virgin.net/cobber.budgies/stories/scottie_a.html&h=353&w=350&sz=38&tbnid=4jg3dcJYAeIJ:&tbnh=116&tbnw=115&start=5&prev=/images%3Fq%3Dyoung%2Bchicks%26hl%3Den%26lr%3D%26client%3Dfirefox-a%26rls%3Dorg.mozilla:en-GB:official_s%26sa%3DG	2-3-05 14:59	1

124.		http://images.google.co.uk/imgres?imgurl=http://freespace.virgin.net/cobber.budgies/images/babyscot_vyoung.jpg&imgrefurl=http://freespace.virgin.net/cobber.budgies/stories/scottie_a.html&h=353&w=350&sz=38&tbnid=4jg3dcJYAeIJ:&tbnh=116&tbnw=115&prev=/images%3Fq%3Dyoung%2Bchicks%26hl%3Den%26lr%3D%26client%3Dfirefox-a%26rls%3Dorg.mozilla:en-GB:official_s%26sa%3DG&frame=small	2-3-05 14:59	1
125.	Scottie's Baby Pictures - 1	http://freespace.virgin.net/cobber.budgies/stories/scottie_a.html	2-3-05 14:59	1
126.	Google Image Result for http://www.insaneanimals.com/items/177.jpg	http://images.google.co.uk/imgres?imgurl=http://www.insaneanimals.com/items/177.jpg&imgrefurl=http://www.insaneanimals.com/funny-animals/177.html%3Fsort%3Ddate&h=290&w=350&sz=10&tbnid=97SA3_pw84UJ:&tbnh=96&tbnw=116&start=6&prev=/images%3Fq%3Dyoung%2Bchicks%26hl%3Den%26lr%3D%26client%3Dfirefox-a%26rls%3Dorg.mozilla:en-GB:official_s%26sa%3DG	2-3-05 15:01	1
127.		Error! Hyperlink reference not valid.	2-3-05 15:01	1
128.	Young Chicks - Funny Animals, Pets, Cats and Dogs Pictures - Insane Animals	http://www.insaneanimals.com/funny-animals/177.html?sort=date	2-3-05 15:01	1
129.		http://pagead2.googlesyndication.com/pagead/ads?client=ca-pub-2066660325911329&dt=1107442877733&format=120x600_as&output=html&url=http%3A%2F%2Fimages.google.co.uk%2Fimgres%3Fimgurl%3Dhttp%3A%2F%2Fwww.insaneanimals.com%2Fitems%2F177.jpg%26imgrefurl%3Dhttp%3A%2F%2Fwww.insaneanimals.com%2Ffunny-animals%2F177.html%253Fsort%253Ddate%26h%3D290%26w%3D350%26sz%3D10%26tbnid%3D97SA3_pw84UJ%3A%26tbnh%3D96%26tbnw%3D116%26start%3D6%26prev%3D%2Fimages%253Fq%253Dyoung%252Bchicks%2526hl%253Den%2526lr%253D%2526client%253Dfirefox-a%2526rls%253Dorg.mozilla%3Aen-GB%3Aofficial_s%2526sa%253DG&u_h=768&u_w=1024&u_ah=738&u_aw=1024&u_cd=24&u_his=4&u_nplug=9&u_nmime=21	2-3-05 15:01	1
130.		http://media.fastclick.net/w/get.media?t=n&sid=13470&m=3&f=b&v=1.4&c=7098&r=http%3A//images.google.co.uk/imgres%3Fimgurl%3Dhttp%3A//www.insaneanimals.com/items/177.jpg%26imgrefurl%3Dhttp%3A//www.insaneanimals.com/funny-animals/177.html%253Fsort%253Ddate%26h%3D290%26w%3D350%26sz%3D10%26tbnid%3D97SA3_pw84UJ%3A%26tbnh%3D96%26tbnw%3D116%26start%3D6%26prev%3D/images%253Fq%253Dyoung%252Bchicks%2526hl%253Den%2526lr%253D%2526client%253Dfirefox-a%2526rls%253Dorg.mozilla%3Aen-GB%3Aofficial_s%2526sa%253DG&d=f	2-3-05 15:01	1
131.	Google Search: young chicks	http://images.google.co.uk/images?q=young+chicks&hl=en&lr=&client=firefox-a&rls=org.mozilla:en-GB:official_s&start=20&sa=N	2-3-05 15:01	1
132.		http://www.cvm.okstate.edu/instruction/kocan/ostrich/ostbk2b2.htm	2-3-05 15:02	1
133.		http://images.google.co.uk/imgres?imgurl=http://www.cvm.okstate.edu/instruction/kocan/disk2/images/img0056.jpg&imgrefurl=http://www.cvm.okstate.edu/instruction/kocan/ostrich/ostbk2b2.htm&h=768&w=512&sz=108&tbnid=xe9EaVDii1EJ:&tbnh=141&tbnw=94&prev=/images%3Fq%3Dyoung%2Bchicks%26start%3D20%26hl%3Den%26lr%3D%26client%3Dfirefox-a%26rls%3Dorg.mozilla:en-GB:official_s%26sa%3DN&frame=small	2-3-05 15:02	1
134.	Google Image Result for http://www.cvm.okstate.edu/instruction/kocan/disk2/images/img0056.jpg	http://images.google.co.uk/imgres?imgurl=http://www.cvm.okstate.edu/instruction/kocan/disk2/images/img0056.jpg&imgrefurl=http://www.cvm.okstate.edu/instruction/kocan/ostrich/ostbk2b2.htm&h=768&w=512&sz=108&tbnid=xe9EaVDii1EJ:&tbnh=141&tbnw=94&start=24&prev=/images%3Fq%3Dyoung%2Bchicks%26start%3D20%26hl%3Den%26lr%3D%26client%3Dfirefox-a%26rls%3Dorg.mozilla:en-GB:official_s%26sa%3DN	2-3-05 15:02	1
135.	Google Search: young chicks	http://images.google.co.uk/images?q=young+chicks&hl=en&lr=&client=firefox-a&rls=org.mozilla:en-GB:official_s&start=40&sa=N	2-3-05 15:03	1
136.		http://images.google.co.uk/imgres?imgurl=http://people.cornell.edu/pages/sah67/chicks2.jpg&imgrefurl=http://people.cornell.edu/pages/sah67/summer.html&h=450&w=600&sz=39&tbnid=7SZWO4nGCbYJ:&tbnh=99&tbnw=132&prev=/images%3Fq%3Dyoung%2Bchicks%26start%3D40%26hl%3Den%26lr%3D%26client%3Dfirefox-a%26rls%3Dorg.mozilla:en-GB:official_s%26sa%3DN&frame=small	2-3-05 15:03	1
137.	Eco Gallery '04	http://people.cornell.edu/pages/sah67/summer.html	2-3-05 15:03	1
138.	Google Image Result for http://people.cornell.edu/pages/sah67/chicks2.jpg	http://images.google.co.uk/imgres?imgurl=http://people.cornell.edu/pages/sah67/chicks2.jpg&imgrefurl=http://people.cornell.edu/pages/sah67/summer.html&h=450&w=600&sz=39&tbnid=7SZWO4nGCbYJ:&tbnh=99&tbnw=132&start=59&prev=/images%3Fq%3Dyoung%2Bchicks%26start%3D40%26hl%3Den%26lr%3D%26client%3Dfirefox-a%26rls%3Dorg.mozilla:en-GB:official_s%26sa%3DN	2-3-05 15:03	1
139.	Google Search: bird screensavers	http://www.google.co.uk/search?client=firefox-a&rls=org.mozilla%3Aen-GB%3Aofficial_s&hl=en&q=bird+screensavers&meta=&btnG=Google+Search	2-9-05 11:27	1
140.	Screensavers	http://www.traveltex.com/screen.asp?SN=6245300&LS=0&SS=1	2-9-05 11:27	1
141.	Screensavers	http://www.traveltex.com/screen.asp?SN=6245300&LS=0&SS=1	2-9-05 11:27	2
142.		http://www.traveltex.com/downloads/screensavers/birds.zip	2-9-05 11:27	1

Table 7 - Firefox History

Appendix F – John Doe History – Firefox – Breakdown

02/02/2005

1411
John Doe goes online and searches Google for “birds” before visiting pbs.org/lifeofbirds to look at a page featuring bird songs. At 1414 John Doe shops for books pertaining to birds, searching Amazon for “bird books” – he goes on to look at two books, “Garden Birds (Collins Gem S.)”, and “The Secret Lives of Garden Birds”.

1415
Mr Doe searched Google for “bird wallpaper” and would spend the next three minutes browsing for images. One image, “snow_geese.jpg” would be downloaded.

1422
John Doe made Google search for “bird stories” then spent five minutes on about.com viewing articles on building bird houses and bird feeders.

1424
John Doe downloads all assets for the page “Building a Bluebird Nest Box”, see figure 2 for the available webpage.

Figure 2- aa010703a.htm

1427
John Doe visits haiths.com – a site specializing in wild bird food and tips and advice from notorious bird lover Bill Oddie.

1511
john Doe revisits pbs.com/lifeofbirds to listen to two bird songs (kakapo.ram, and dawn.ram).

1557
John Doe searches for, and downloads tools which he would use to encrypt a file containing five illegal images of birds at 1646 the same day.

03/02/2005

1221
John Doe makes a Google search for bird mating calls, this leads to an article on whyfiles.org about bird songs with links to samples of birdsongs throughout the article.

1459
John Doe searches Google for "young chicks", from here, he visits a site with images of young birds, and finds a blog following the growth of a baby bird – Scottie. From here, John Doe downloads "babyscot_vyoung.jpg" and "babyscot_2weeks1.jpg", this is shown from the images being sourced to the website John Doe was visiting when the images were downloaded to the computer.
(See Appendix E, rows 123-125 and Appendix B, rows 39 and 40).

1501
Further image searchers for "young chicks" are made and sites are visited pertaining to the search.

09/02/05

1127
John Doe makes a Google search for "bird wallpapers" and finds a website designed for tourist information for Texas. On this website are premade galleries downloaded as executable (.exe) files. Once run, these exe files set the gallery of images as a slideshow screensaver. From here, the accused downloaded tx_birds.exe at 1128, and ran it sometime between 1128 and 1350.

Appendix G – Images – Seizure

Image 1 - Pc on desk on entry

Image 2 – Monitor USB ports empty

Image 3 – PC USB ports empty

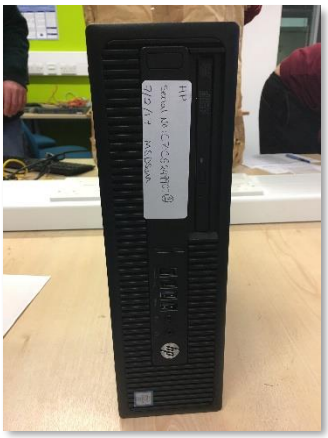


Image 4 – Tower – View 1

Image 5 – Tower – View 2

Image 6 – Tower – View 3

Image 7 – Tower – View 4

Image 8 – Tower – View 5

Image 9 – Tower – View 6

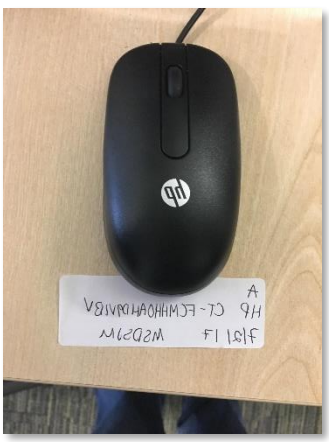


Image 10 - Mouse

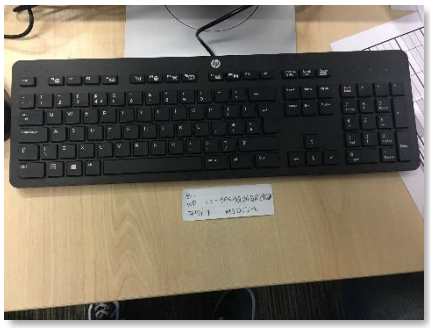


Image 11 - Keyboard

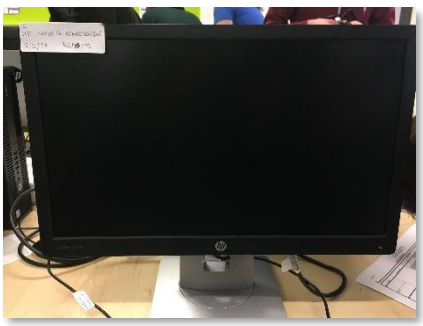


Image 12 - Monitor

Image 13 – Ethernet Socket

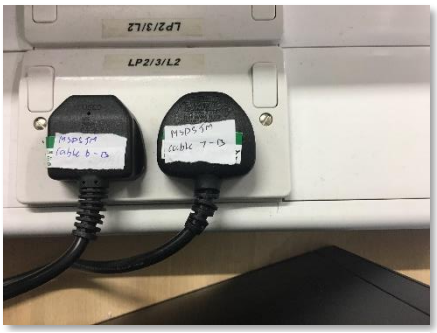


Image 14 – Monitor and tower plugged in

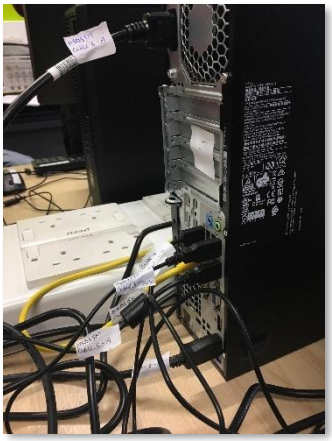


Image 15 – Tower – cables marked

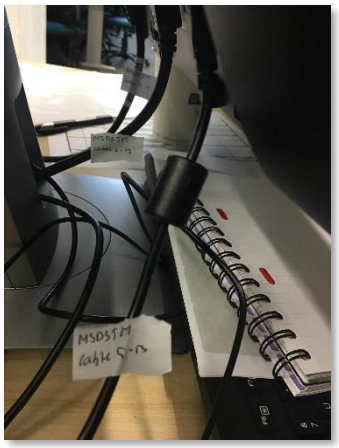


Image 16 – Monitor – cables marked

Image 17 – HDD Removed

Appendix H – Clock Skew

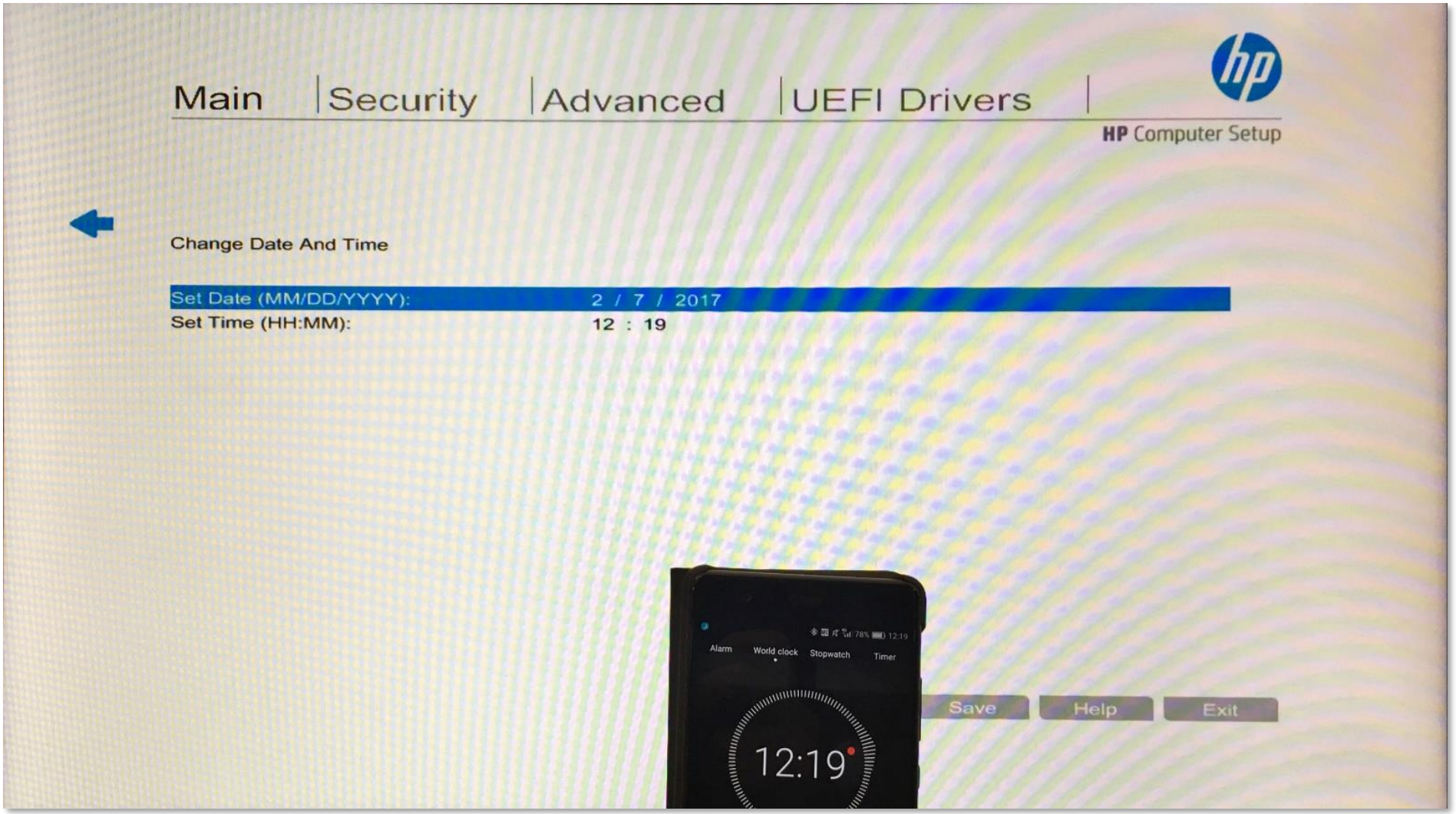


Figure 18 – Clock Skew

Appendix I – Chain of Custody

Case No:

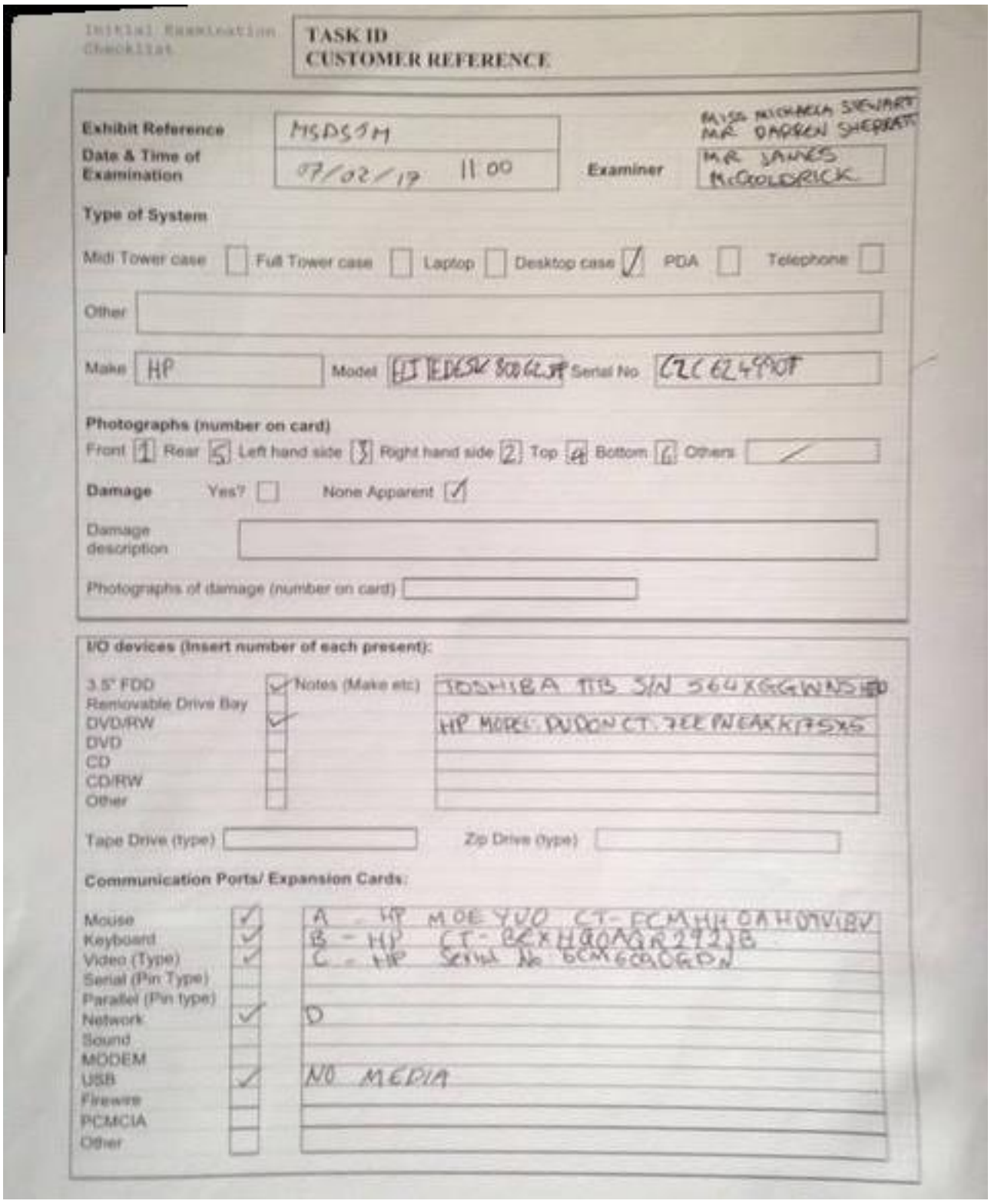
Investigation in Confidence
EXHIBIT MOVEMENT LIST

Exhibit	Description	Seal Number In	Seal Number Out	Date	Time	Initials
MSDSJM -1	Cables Mouse (HP) Keyboard (HP)			7/2/17	12:12	XH
				7/2/17	12:13	MS
MSDSJM-2	Monitor (HP)			7/2/17	12:12	XH
				7/2/17	12:13	MS
MSDSJM-3	Tower (HP)			7/2/17	12:12	XH
				7/2/17	12:13	MS
				14/2/17	OUT 11:58 IN 13:00	DCS
				28/2/17	OUT 10:30 IN 13:00	DCS

Investigation in Confidence

Figure 3 - Chain of Custody Document

[Appendix J – Initial Examination Checklist]



Initial Examination Checklist

TASK ID
CUSTOMER REFERENCE

Exhibit Reference: MSDSJM
Date & Time of Examination: 07/02/17 11:00
Examiner: MR JAMES McCOLDRICK
MISS MICHAELA STEWART MR DARREN SHERRATT

Type of System

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

Other

Make: HP Model: HJ TEDESK 800 GL3# Serial No: CZC624990T

Photographs (number on card)
Front [1] Rear [5] Left hand side [3] Right hand side [2] Top [4] Bottom [6] Others [/]

Damage Yes? ☐ None Apparent ☑

Damage description

Photographs of damage (number on card)

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

		Notes (Make etc)
3.5" FDD	☑	TOSHIBA 1TB S/N 564XGGWNS
Removable Drive Bay		
DVD/RW	☑	HP MODEL DUDON CT. TEEPNEAKK/75X5
DVD		
CD		
CD/RW		
Other		

Tape Drive (type) Zip Drive (type)

Communication Ports/ Expansion Cards:

Mouse	☑	A - HP MOE YUO CT-FCMHHOAHOTVIBV
Keyboard	☑	B - HP CT-BCXHGOAGR292JB
Video (Type)	☑	C - HP SERIAL No 6CM6COLOGDN
Serial (Pin Type)		
Parallel (Pin type)		
Network	☑	D
Sound		
MODEM		
USB	☑	NO MEDIA
Firewire		
PCMCIA		
Other		

Figure 4 - Initial Examination Checklist

Appendix K – Exif Data

File Name	1176-ready2fledge.jpg
File Size	77 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Camera Model Name	Canon PowerShot SD100
Modify Date	2004:07:02 17:29:18
Create Date	2004:06:20 18:01:44
File Source	Digital Camera

File Name	2501-birdtrans2.jpg
File Size	58 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Camera Model Name	Canon PowerShot SD100
Modify Date	2004:07:02 17:46:10
Create Date	2004:06:17 18:42:34
File Source	Digital Camera

File Name	26066-Firefox Wallpaper.bmp
File Size	2.3 MB
File Type	BMP
File Type Extension	bmp
MIME Type	image/bmp

File Name	31307-FantailFrontView.exe.jpg
File Size	304 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	31788-67BAEB46d01.jpg
File Size	18 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Modify Date	2004:07:13 18:36:45
Create Date	2004:07:13 18:36:45-08:00

File Name	31814-A0016363d01.jpg
File Size	44 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Camera Model Name	Canon PowerShot SD100

Modify Date	2004:07:02 17:30:41
Create Date	2004:06:13 19:44:11
File Source	Digital Camera

File Name	31816-3E8462AFd01.jpg
File Size	52 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Camera Model Name	Canon PowerShot SD100
Modify Date	2004:07:02 17:49:33
Create Date	2004:06:17 18:43:03
File Source	Digital Camera

File Name	31820-3E8662AFd01.jpg
File Size	52 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Camera Model Name	Canon PowerShot SD100
Modify Date	2004:07:02 17:46:36
Create Date	2004:06:18 23:31:50
File Source	Digital Camera

File Name	31822-3E8162AFd01.jpg
File Size	44 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Camera Model Name	Canon PowerShot SD100
Modify Date	2004:07:02 17:49:50
Create Date	2004:06:18 23:31:56
File Source	Digital Camera

File Name	31824-3E8262AFd01.jpg
File Size	55 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Camera Model Name	Canon PowerShot SD100
Modify Date	2004:07:02 17:50:06
Create Date	2004:06:18 23:32:28
File Source	Digital Camera

File Name	31826-3E8C62AFd01.jpg
File Size	100 kB
File Type	JPEG
File Type Extension	jpg

MIME Type	image/jpeg
Camera Model Name	Canon PowerShot SD100
Modify Date	2004:07:02 17:47:07
Create Date	2004:06:18 23:49:04
File Source	Digital Camera

File Name	31830-EF29AEAEd01.jpg
File Size	60 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Camera Model Name	Canon PowerShot SD100
Modify Date	2004:07:02 17:27:29
Create Date	2004:06:13 20:39:11
File Source	Digital Camera

File Name	31834-6A161D2Fd01.jpg
File Size	107 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Camera Model Name	Canon PowerShot SD100
Modify Date	2004:07:02 17:28:27
Create Date	2004:06:13 21:34:00
File Source	Digital Camera

File Name	31840-4C3E89C6d01.jpg
File Size	65 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Camera Model Name	Canon PowerShot SD100
Modify Date	2004:07:02 17:47:26
Create Date	2004:06:18 23:33:33
File Source	Digital Camera

File Name	31844-A2E5F216d01.jpg
File Size	59 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Camera Model Name	Canon PowerShot SD100
Modify Date	2004:07:02 17:57:42
Create Date	2004:06:19 19:49:58
File Source	Digital Camera

File Name	31850-978D14DDd01.jpg
File Size	54 kB

File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Camera Model Name	Canon PowerShot SD100
Modify Date	2004:07:02 17:31:09
Create Date	2004:06:09 20:14:06
File Source	Digital Camera

File Name	31902-A3D4DDDDd01.jpg
File Size	22 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Camera Model Name	Canon PowerShot SD100
Modify Date	2004:07:02 17:41:45
Create Date	2004:06:22 18:56:18
File Source	Digital Camera

File Name	31908-BF5BE9D9d01.jpg
File Size	67 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Camera Model Name	Canon PowerShot SD100
Modify Date	2004:07:02 17:57:10
Create Date	2004:06:18 23:28:19
File Source	Digital Camera

File Name	32010-BaldEagle7oClock.jpg
File Size	231 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	32012-GreatEgretOverflyingRoseateSpoonbills.jpg
File Size	362 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	32035-AlmondMarshGreatBlueHeronStalling.jpg
File Size	173 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	32037-AmericanAvocetWinterPlumage.jpg
File Size	165 kB

File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	32039-AmericanWhitePelicansCircling.jpg
File Size	197 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	32041-BellbirdJumpingOffBranch.jpg
File Size	692 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Camera Model Name	Canon EOS-1DS
Modify Date	2003:01:29 16:14:10
Create Date	2003:01:29 16:14:10
Control Mode	Camera Local Control
Camera Type	EOS High-end

File Name	32043-BlackNeckedStiltsFromBehind.jpg
File Size	245 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	32045-BlackSwan.jpg
File Size	301 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	32047-BlackVultureSunningOnPost.jpg
File Size	220 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	32051-brd_Ornithologist_TWG.jpg
File Size	20 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	32066-BarnOwl.jpg
File Size	138 kB
File Type	JPEG

File Type Extension	jpg
MIME Type	image/jpeg

File Name	32068-GreatBlueHeronWithFish.jpg
File Size	309 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	32070-GreatEgretInVoloBog.jpg
File Size	217 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	32073-GreenHeronCloseup.jpg
File Size	232 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	32075-GreenHeronOnChicagoLakeshore.jpg
File Size	262 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	32079-ImmatureSnowyEgretTakingOff.jpg
File Size	312 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	32081-june03screen.jpg
File Size	60 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	32083-junescreen01.jpg
File Size	189 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	32085-KeaAndMountain.jpg
File Size	211 kB
File Type	JPEG

File Type Extension	jpg
MIME Type	image/jpeg

File Name	32094-Df1.jpg
File Size	61 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	32098-KeaAtTopOfMacKinnonPass0930.jpg
File Size	295 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	32100-KeaEatingRentalCar.jpg
File Size	311 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	32102-KeaRetrievingBakedBeanCanFromTarn.jpg
File Size	295 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	3217-babyscot_2weeks1.jpg
File Size	33 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	3219-babyscot_vyoung.jpg
File Size	38 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	3221-chicks2.jpg
File Size	38 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Camera Model Name	Canon PowerShot SD100
Modify Date	2004:07:02 17:27:53
Create Date	2004:06:27 18:28:34
File Source	Digital Camera

File Name	3226-snow_geese.jpg
File Size	146 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	3237-newbies2.jpg
File Size	54 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Camera Model Name	Canon PowerShot SD100
Modify Date	2004:07:02 17:28:49
Create Date	2004:06:22 21:10:50
File Source	Digital Camera

File Name	33053-CrouchingKokako.jpg
File Size	282 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	33054-brd_WoodDuck.jpg
File Size	41 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Modify Date	2003:10:01 14:31:09

File Name	33055-Brolga.jpg
File Size	279 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	33056-BrushTurkeyPerching.jpg
File Size	277 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	33057-CanadaGoose.jpg
File Size	177 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	33058-CanadaGooseWashing.jpg
File Size	264 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	33059-ChestnutMandibledToucan.jpg
File Size	305 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	34175-f0526960.jpg
File Size	100 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Camera Model Name	Canon PowerShot SD100
Modify Date	2004:07:02 17:47:07
Create Date	2004:06:18 23:49:04
File Source	Digital Camera

File Name	35605-E^%@%birds@%birdpics@%WhiteFacedHeronFlying.jpg
File Size	177 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	35606-E^%@%birds@%birdpics@%WhiteFrontedParrot.jpg
File Size	184 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	35607-E^%@%birds@%birdpics@%WhiteThroatedSparrowInTree.jpg
File Size	241 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	35608-E^%@%birds@%birdpics@%WhoopingCranes.jpg
File Size	298 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	35609-E^%@%birds@%birdpics@%yellow-wag-cover-nb.jpg
File Size	60 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	35612-Wallpaper1.png
File Size	916 kB
File Type	PNG
File Type Extension	png
MIME Type	image/png

File Name	35613-Wallpaper2.png
File Size	513 kB
File Type	PNG
File Type Extension	png
MIME Type	image/png

File Name	35614-Wallpaper3.png
File Size	686 kB
File Type	PNG
File Type Extension	png
MIME Type	image/png

File Name	35615-Wallpaper4.png
File Size	977 kB
File Type	PNG
File Type Extension	png
MIME Type	image/png

File Name	35616-Wallpaper5.png
File Size	1305 kB
File Type	PNG
File Type Extension	png
MIME Type	image/png

File Name	35617-Wallpaper6.png
File Size	810 kB
File Type	PNG
File Type Extension	png
MIME Type	image/png

File Name	35618-Wallpaper7.png
File Size	949 kB
File Type	PNG
File Type Extension	png
MIME Type	image/png

File Name	35619-Wallpaper8.png
File Size	1480 kB
File Type	PNG
File Type Extension	png
MIME Type	image/png

File Name	35620-Wallpaper9.png
File Size	742 kB
File Type	PNG
File Type Extension	png
MIME Type	image/png

File Name	6864-J0178932.JPG
File Size	35 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

File Name	tn_duck_3.jpg
File Size	3.2 kB
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg

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

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

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

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

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

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

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

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

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

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

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

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

• Rule 7 - Speak Softly.
Human voices put wildlife on alert. Talking may also prevent a leader from hearing songs or calls and keep you from

hearing instructions. Field trips are social and conversation is part of the field trip experience. If you want to converse, do so in whispers or stand away from the group.

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

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

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

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

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

Appendix M – gpg File Decrypt

The accused, looking for a tool to encrypt data, downloaded two programs on the 2nd of February. The first was the program GnuPG – this program allows the use to encrypt data using the OpenPGP standard. The second, WinPT, is a taskbar front-end for GnuPG which includes key management.

GnuPG uses a private key along with a passphrase to securely encrypt data. It was possible through use of tools in Linux to extract the hash from John Doe's private key (registered to the email address jdoe@example.com) and extract the passphrase. From here it was possible to extract the five IIOB from the file.

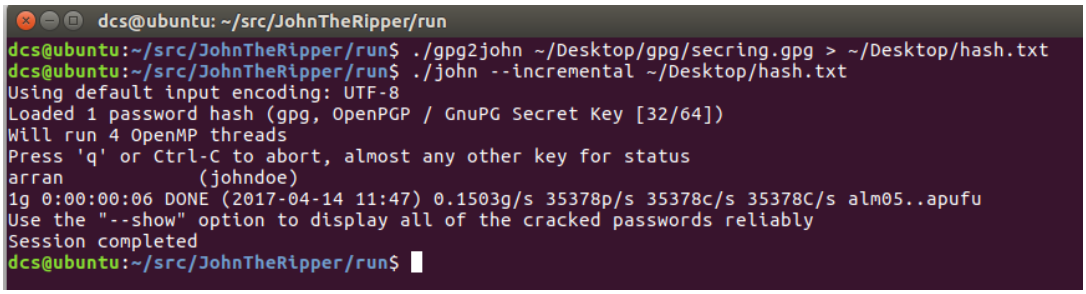


Figure 5 – GPG key crack

To gain access to the files contained in the encrypted .gpg file, John the Ripper was used to get the passphrase from John Doe's secret key found on the hard drive. The community version of John the Ripper – "Jumbo John" – contained the necessary program to allow John the Ripper to crack the passphrase for the key. Jumbo John's gpg2john was first used to extract the hash from the secret key, and John the Ripper was used to brute force the hash, revealing the password "arran".

From here, Linux's gpg tools were used to decrypt the file, revealing a zip file. Attempting extraction with zip tools proved to only extract one file despite the other four files existing in the file. The jar tools for Linux were installed and used to extract all five files.

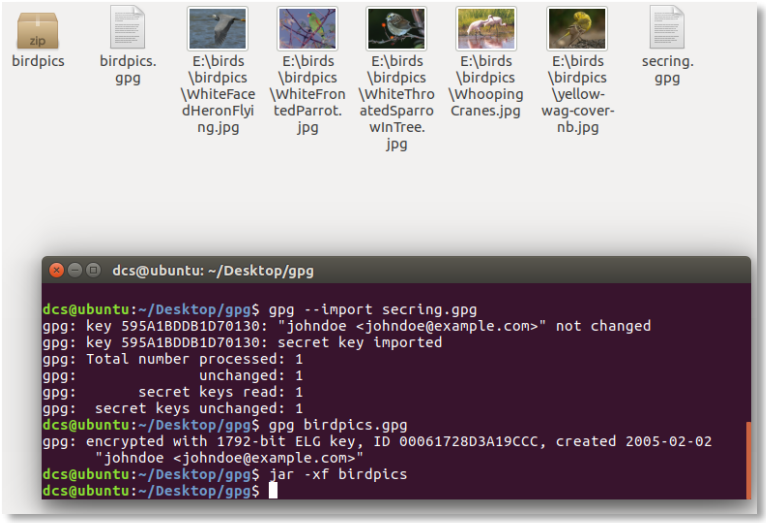


Figure 6 – GPG extraction

Appendix N – Hash Comparison

HDD md5 hash

Total (md5): d63dd1b8917ca28bac7c955fc3b6cd25

Image md5 hash

d63dd1b8917ca28bac7c955fc3b6cd25 johnDoe.dd

Appendix O – EventLogs.txt

eventlogs v.20081219

(System) Gets Event Log settings from System hive

EventLog Configuration
ControlSet001\Services\Eventlog
LastWrite Time Mon Jan 24 15:31:55 2005 (UTC)
ComputerName = JOHN

Application EventLog
ControlSet001\Services\Eventlog\Application
LastWrite Time Fri Jan 28 15:50:28 2005 (UTC)
Configuration Settings

Log location: %SystemRoot%\system32\config\AppEvent.Evt
Log Size: 524288 Bytes
AutoBackupLogFiles is Disabled

Security EventLog
ControlSet001\Services\Eventlog\Security
LastWrite Time Mon Jan 24 15:43:53 2005 (UTC)
Configuration Settings

Log location: %SystemRoot%\System32\config\SecEvent.Evt
Log Size: 524288 Bytes
AutoBackupLogFiles is Disabled

System EventLog
ControlSet001\Services\Eventlog\System
LastWrite Time Mon Jan 24 16:34:25 2005 (UTC)
Configuration Settings

Log location: %SystemRoot%\system32\config\SysEvent.Evt
Log Size: 524288 Bytes
AutoBackupLogFiles is Disabled

Appendix P – SAM Users

User Information

Username: johndoe [1003]
Full Name:
User Comment:
Account Type: Default Admin User
Account Created: Mon Jan 24 15:56:49 2005 Z
Last Login Date: Wed Feb 9 16:49:18 2005 Z
Pwd Reset Date: Mon Jan 24 16:36:30 2005 Z
Pwd Fail Date: Wed Feb 2 15:08:27 2005 Z
Login Count: 21
--> Password does not expire
--> Normal user account

Username: jane [1004]
Full Name: jane
User Comment:
Account Type: Custom Limited Acct
Account Created: Wed Feb 2 12:36:29 2005 Z
Last Login Date: Thu Feb 3 11:23:04 2005 Z
Pwd Reset Date: Wed Feb 2 12:37:25 2005 Z
Pwd Fail Date: Wed Feb 2 15:08:27 2005 Z
Login Count: 1
--> Password does not expire
--> Normal user account

Username: bob [1005]
Full Name: bob
User Comment:
Account Type: Custom Limited Acct
Account Created: Wed Feb 2 15:08:39 2005 Z
Last Login Date: Thu Feb 3 10:12:34 2005 Z
Pwd Reset Date: Wed Feb 2 15:08:54 2005 Z
Pwd Fail Date: Never
Login Count: 1
--> Password does not expire
--> Normal user account

Appendix Q – Disk Partitions

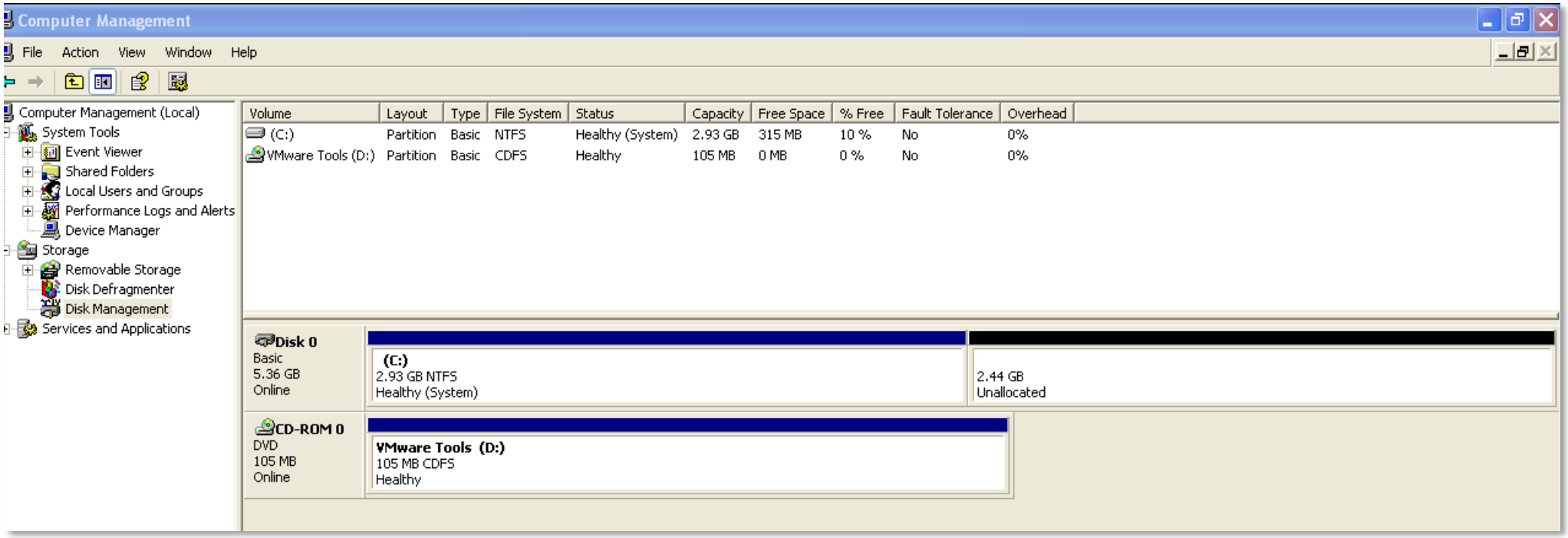


Figure 7 – Disk Partitions

Appendix R – Downloads

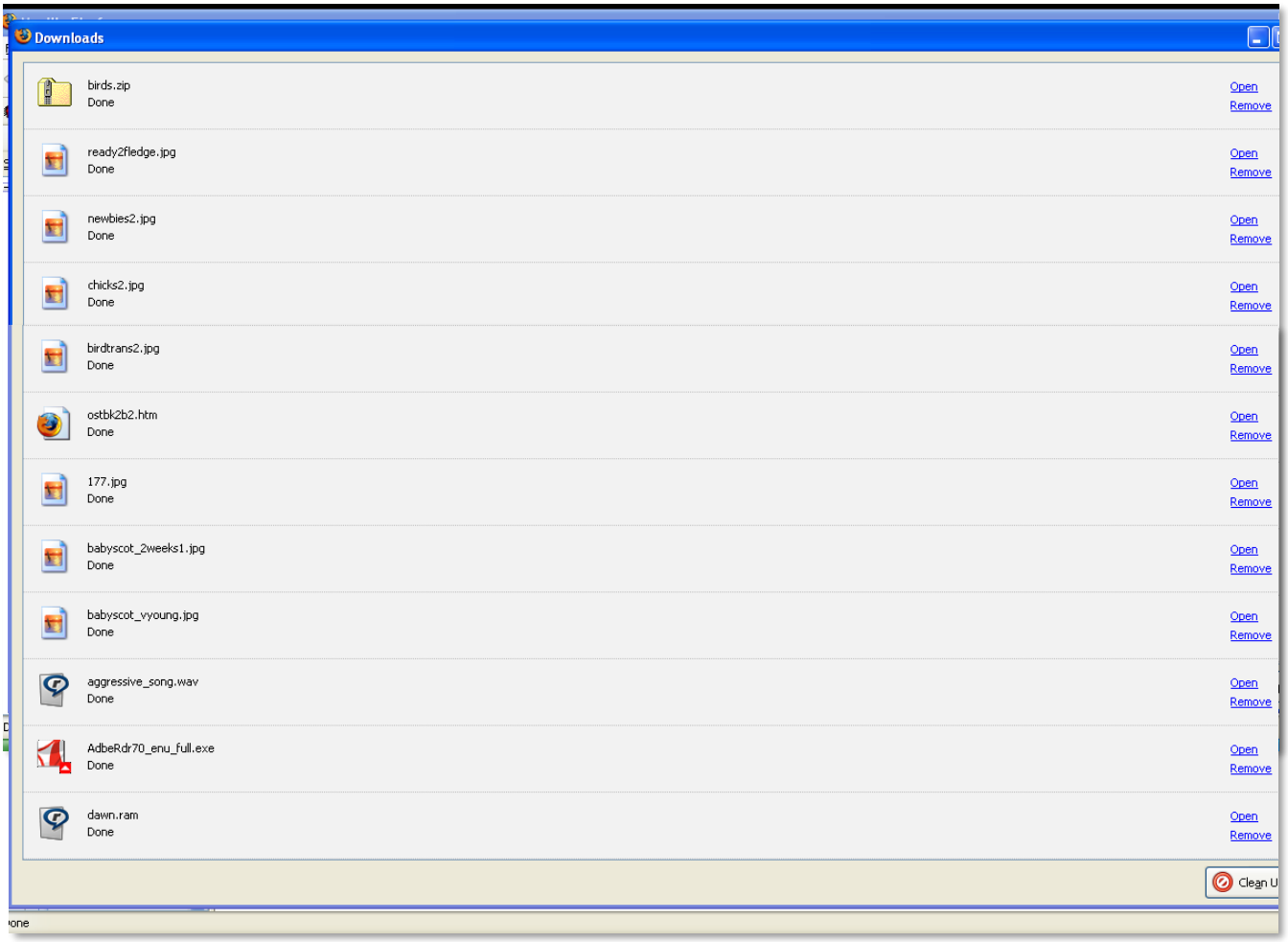


Figure 8 – Firefox downloads

Appendix S – John Doe History – Internet Explorer

	Mandiant: Web Historian - 1 - C:\Users\amg\Desktop\johndoe\Local Settings\History\History.IE5\index.dat		
No.	**URL Address**	**Modified Time**	**Accessed Time**
1.	Visited: johndoe@about:Home	24-01-05 15:57	24-01-05 15:57
2.	Visited: johndoe@res://C:\WINDOWS\system32\shdoclc.dll/dnserror.htm	24-01-05 16:13	24-01-05 16:13
3.	Visited: johndoe@file:///C:/WINDOWS/system32/oobe/actshell.htm	24-01-05 16:13	24-01-05 16:13
4.	Visited: johndoe@javascript:parent.fnExpressScan();	24-01-05 16:15	24-01-05 16:15
5.	Visited: johndoe@http://v5.windowsupdate.microsoft.com/v5consumer/resultslist.aspx?ln=en-us&id=6	24-01-05 16:16	24-01-05 16:16
6.	Visited: johndoe@http://www.linorg.usp.br/mozilla//firefox/releases/1.0/win32/en-GB/Firefox%20Setup%201.0.exe	24-01-05 16:20	24-01-05 16:20
7.	Visited: johndoe@http://www.mozilla.org/products/firefox	24-01-05 16:21	24-01-05 16:21
8.	Visited: johndoe@http://download.mozilla.org/?product=firefox&os=win&lang=en-GB	24-01-05 16:21	24-01-05 16:21
9.	Visited: johndoe@http://mozilla.mirrors.tds.net/pub/mozilla.org/firefox/releases/1.0/win32/en-GB/Firefox%20Setup%201.0.exe	24-01-05 16:22	24-01-05 16:22
10.	Visited: johndoe@http://www.mozilla.org/products	24-01-05 16:23	24-01-05 16:23
11.	Visited: johndoe@http://www.mozilla.org/products/thunderbird	24-01-05 16:23	24-01-05 16:23
12.	Visited: johndoe@http://download.mozilla.org/?product=thunderbird&os=win&lang=en-US	24-01-05 16:23	24-01-05 16:23
13.	Visited: johndoe@http://64.12.168.243/pub/mozilla.org/thunderbird/releases/1.0/win32/en-US/Thunderbird%20Setup%201.0.exe	24-01-05 16:24	24-01-05 16:24
14.	Visited: johndoe@http://windowsupdate.microsoft.com	24-01-05 16:39	24-01-05 16:39
15.	Visited: johndoe@http://v5.windowsupdate.microsoft.com/v5consumer/default.aspx	24-01-05 16:40	24-01-05 16:40
16.	Visited: johndoe@http://v5.windowsupdate.microsoft.com/v5consumer/default.aspx?ln=en-us	24-01-05 16:40	24-01-05 16:40
17.	Visited: johndoe@javascript:parent.fnScan();	24-01-05 16:40	24-01-05 16:40
18.	Visited: johndoe@http://v5.windowsupdate.microsoft.com/v5consumer/resultslist.aspx?ln=en-us&id=0	24-01-05 16:40	24-01-05 16:40
19.	Visited: johndoe@http://v5.windowsupdate.microsoft.com/v5consumer/resultslist.aspx?ln=en-us&id=1&LinkId=SOFTWARE&TocIndex=	24-01-05 16:41	24-01-05 16:41
20.	Visited: johndoe@about:blank	25-01-05 11:16	25-01-05 11:16
21.	Visited: johndoe@http://office.microsoft.com/en-gb/officeupdate/default.aspx	25-01-05 11:16	25-01-05 11:16
22.	Visited: johndoe@http://office.microsoft.com/search/redir.aspx?AssetID=ES790020331033&Origin=HH010704921033&CTT=5	25-01-05 11:16	25-01-05 11:16
23.	Visited: johndoe@http://office.microsoft.com/en-gb/FX010329501033.aspx	25-01-05 11:16	25-01-05 11:16
24.	Visited: johndoe@http://office.microsoft.com/en-gb/FX010355751033.aspx	25-01-05 11:25	25-01-05 11:25
25.	Visited: johndoe@http://office.microsoft.com/search/redir.aspx?AssetID=ES790020331033&CTT=5&Origin=HA010492041033	25-01-05 11:26	25-01-05 11:26
26.	Visited: johndoe@http://office.microsoft.com/officeupdate/maincatalog.aspx?lc=en-gb	25-01-05 11:26	25-01-05 11:26
27.	Visited: johndoe@http://office.microsoft.com/en-gb/FX010354621033.aspx	25-01-05 11:33	25-01-05 11:33
28.	Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/tn_duck_3.jpg	02-02-05 14:18	02-02-05 14:18
29.	Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/snow_geese.jpg	02-02-05 14:18	02-02-05 14:18
30.	Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/7107298.jpg	02-02-05 14:20	02-02-05 14:20
31.	Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/aa010703a.htm	02-02-05 14:25	02-02-05 14:25
32.	Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/wbpremium_s.jpg	02-02-05 14:28	02-02-05 14:28
33.	Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/nestboxtips.txt	02-02-05 14:29	02-02-05 14:29
34.	Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/40m.jpg	02-02-05 14:43	02-02-05 14:43
35.	Visited: johndoe@file:///C:/Program%20Files/Real/RealPlayer/DataCache/Login/index.html	02-02-05 14:57	02-02-05 14:57

36.	Visited: johndoe@http://www.real.com/intro/index_upsell_manager.html?DC=NSP01D&optin=true&country=gb&language=en-gb&icon=tiscali&LI=en&PBR=10485800	02-02-05 15:04	02-02-05 15:04
37.	Visited: johndoe@https://account.real.com/acct/intro/msg.html?msg=frweur	02-02-05 15:04	02-02-05 15:04
38.	Visited: johndoe@javascript:catchEvent('continue');	02-02-05 15:04	02-02-05 15:04
39.	Visited: johndoe@res://C:\Program%20Files\Real\RealPlayer\rpplugins\rpmn3260.dll/black.html	02-02-05 15:04	02-02-05 15:04
40.	Visited: johndoe@file:///C:/Program%20Files/Real/RealPlayer/Firstrun/1.htm	02-02-05 15:04	02-02-05 15:04
41.	Visited: johndoe@file:///C:/Program%20Files/Real/RealPlayer/Firstrun/context.htm	02-02-05 15:04	02-02-05 15:04
42.	Visited: johndoe@file:///D:/Prac4/Prac4.gif	02-02-05 15:10	02-02-05 15:10
43.	Visited: johndoe@file:///D:/Prac5/Q3%20Thread%20(Statechart).gif	02-02-05 15:10	02-02-05 15:10
44.	Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/kakapo.ram	02-02-05 15:11	02-02-05 15:11
45.	Visited: johndoe@file:///C:/Program%20Files/Adobe/Acrobat%207.0/Reader/Legal/Adobe%20Reader/7.0.0/en_US/license.html	02-02-05 17:03	02-02-05 17:03
46.	Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/Application%20Data/Mozilla/Firefox/Profiles/w4nf3obl.default/cookies.txt	03-02-05 12:19	03-02-05 12:19
47.	Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/Application%20Data/Mozilla/Firefox/Profiles/w4nf3obl.default/bookmarks.html	03-02-05 12:20	03-02-05 12:20
48.	Visited: johndoe@file:///E:/birds/audio/aggressive_song.wav	03-02-05 12:22	03-02-05 12:22
49.	Visited: johndoe@file:///C:/EvanstonWoodpecker.jpg	03-02-05 14:14	03-02-05 14:14
50.	Visited: johndoe@file:///C:/Documents%20and%20Settings/All%20Users/Documents/My%20Music/Sample%20Music/Doc1.doc	03-02-05 14:17	03-02-05 14:17
51.	Visited: johndoe@file:///E:/birds/Killdeer.jpg	03-02-05 14:49	03-02-05 14:49
52.	Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/babyscot_vyoung.jpg	03-02-05 15:00	03-02-05 15:00
53.	Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/babyscot_2weeks1.jpg	03-02-05 15:00	03-02-05 15:00
54.	Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/177.jpg	03-02-05 15:01	03-02-05 15:01
55.	Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/ostbk2b2.htm	03-02-05 15:02	03-02-05 15:02
56.	Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/Desktop/birdtrans2.jpg	03-02-05 15:04	03-02-05 15:04
57.	Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/chicks2.jpg	03-02-05 15:05	03-02-05 15:05
58.	Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/newbies2.jpg	03-02-05 15:05	03-02-05 15:05
59.	Visited: johndoe@file:///C:/Documents%20and%20Settings/bob/My%20Documents/My%20Music/ready2fledge.jpg	03-02-05 15:06	03-02-05 15:06
60.	Visited: johndoe@file:///C:/birdwatching.doc	03-02-05 15:49	03-02-05 15:49
61.	Visited: johndoe@file:///E:/birds/non%20images/BookList.doc	03-02-05 15:51	03-02-05 15:51
62.	Visited: johndoe@file:///E:/birds/non%20images/BirdingGuide.pdf	03-02-05 15:52	03-02-05 15:52
63.	Visited: johndoe@file:///C:/WINDOWS/ODBC.INI	03-02-05 15:54	03-02-05 15:54
64.	Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/birds.zip	09-02-05 11:28	09-02-05 11:28
65.	Visited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/stuf.doc	09-02-05 16:57	09-02-05 16:57
66.	Visited: johndoe@file:///C:/Program%20Files/MSN/aggressive_song.wav	09-02-05 17:00	09-02-05 17:00
67.	Visited: johndoe@file:///F:/AlmondMarshGreatBlueHeronStalling.jpg	09-02-05 17:06	09-02-05 17:06

Table 8 – Internet Explorer history

Appendix T – Malware Scan

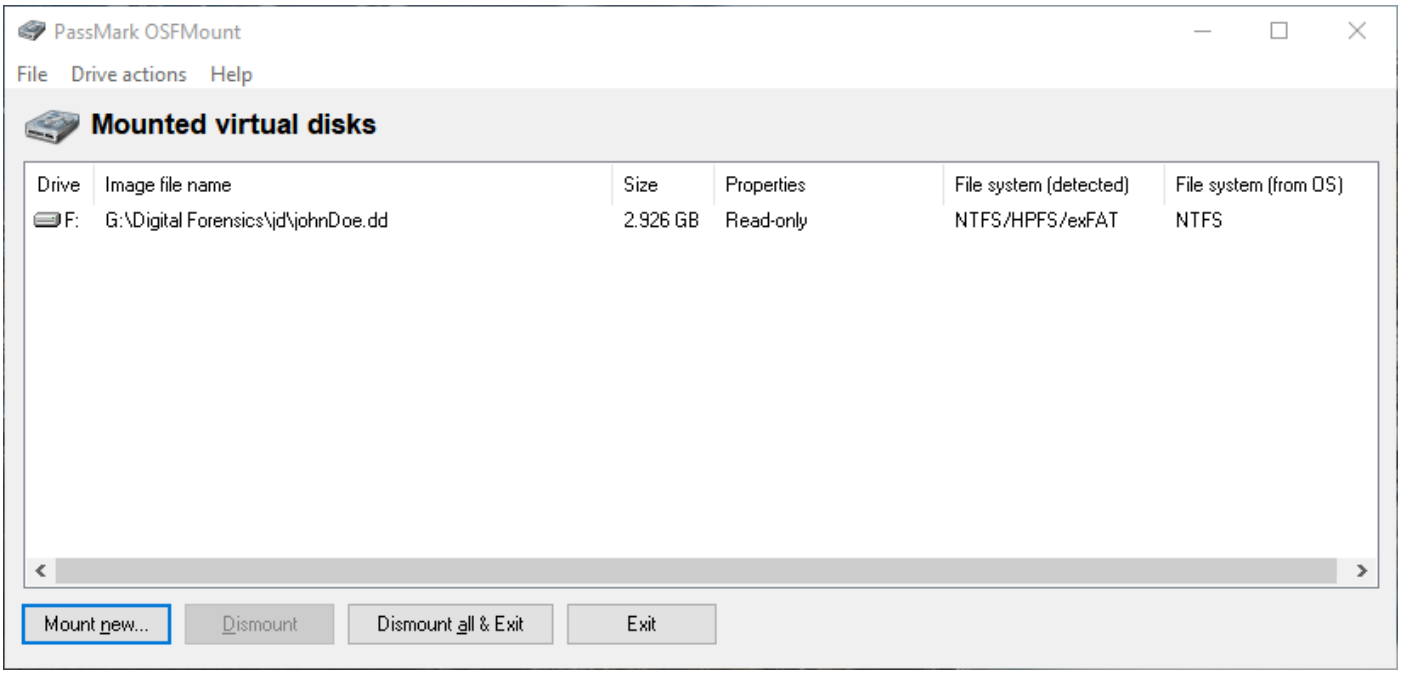


Figure 9 – Windows John Doe image mount

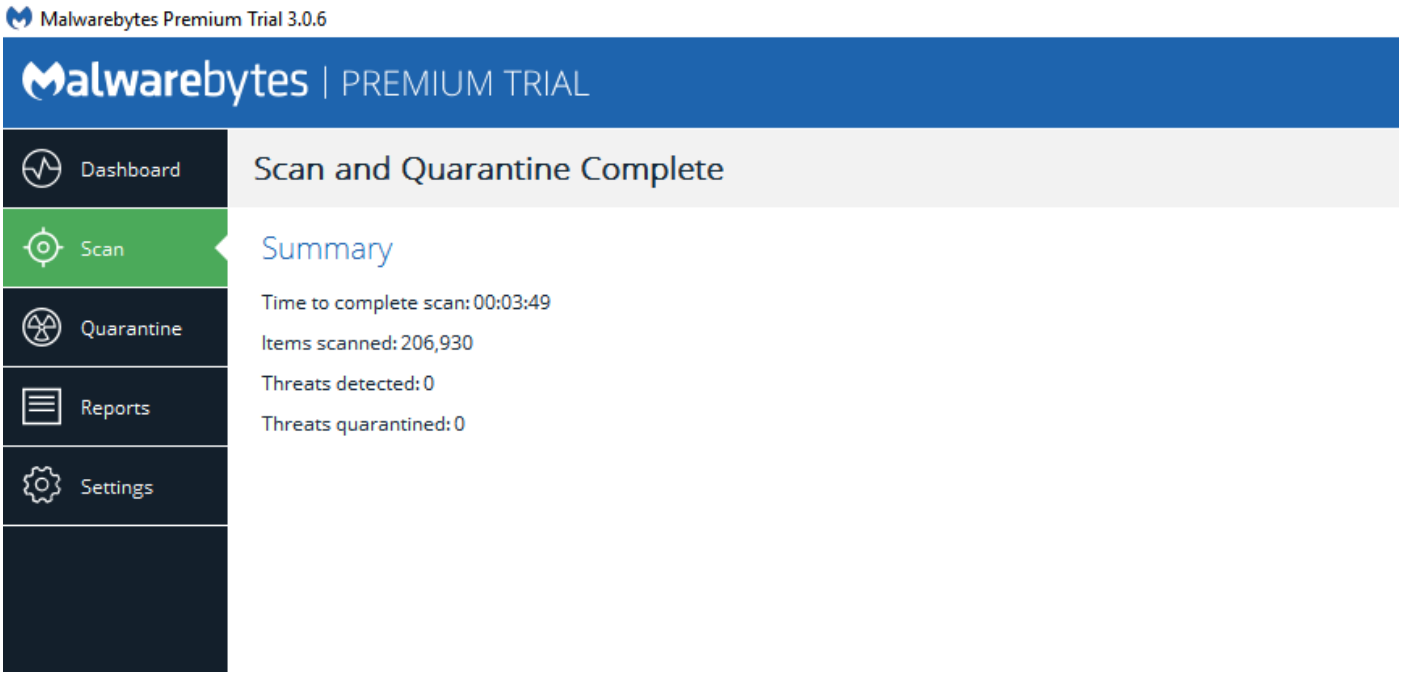


Figure 10 – Malwarebytes malware scan

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

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

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

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

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

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

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

BEST TIMES TO SEE BIRDS
The nesting season is a good time to be watching birds. During this most active time in a bird's life a variety of vocalizations and behaviours are exhibited. In Thailand, as in other tropical countries, the nesting season coincides with the period when food is in abundant supply. A bird expends much energy in courting, mating, incubating eggs, defending a nest and feeding offspring. Most birds nest during the transition between dry and wet seasons when new leaves and grass shoots sprout. This occurs from February to June. Certain birds depend on the availability of water and nest throughout the rainy season.

Migrants are best observed during their passage into or out of the country, or as they pass through on their way to other places. Most conspicuously, half a million ducks spend their winter in Thailand,

feeding and resting in watery roosts from Chiang Saen to Thale Noi. Thousands of garganey and Lesser treeduck flock during January and February.

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

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

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

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

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

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

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

SANDY BEACHES, MANGROVE AND TIDAL FLATS
Sandy beaches are attractive to tourists but are barren habitats for birds, while little-visited mangroves and tidal flats that are rich in nutrients and microorganisms, are favoured feeding haunts for migrant waders. Some birds like the Brown-winged kingfisher and Mangrove pitta, are entirely restricted to mangroves while Mangrove whistlers and flyeaters rarely leave the area.
Key sites: *Samut Sakhon, Ban Laem in Petchburi,* and *Krabi*.

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

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

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

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

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

Contact information:
Bird Conservation Society of Thailand (BCST)*
69/12 Soi Ramindra 24, Joorakaebau, Ladprao, Bangkok 10230, Thailand
Email: bcst@box1.a-net.net.th
Tel: 66-(0)-2943-5965
Web sites:
www.bcst.org/index_ebird.html
www.thai.net/bcst
* The Bird Conservation Society of Thailand (BCST) is a BirdLife Partner

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

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

Reference information:
Field guide
Robson, C. 2002.
A field guide to the birds of Thailand.
Asia Books, Bangkok. 272pp.

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

- KHAO YAI: DONG PHAYA YEN FOREST RANGE
  ISBN 974-8252-70-1
- KAENG KRACHAN:
  Amazing Forest of Phetchburi River
  ISBN 974-8252-72-8
- KHAO SOK
  Fascinating Limestone Mountains Amid The Verdant Forest of Surat Thani, Thailand
  ISBN 974-679-099-4

- DOI INTHANON - DOI SUTHEP
  The Himalayan Springs of Thailand
  SBN 974-8252-67-1
- PHU LUANG
  The Kingdom of Plants
  ISBN 974-8252-73-6

BIRDWATCHING TIPS

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

CONSERVING BIRD DIVERSITY

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

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

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

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

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

HOW YOU CAN HELP IN THE CONSERVATION OF BIRDS

Visitors to Thailand can assist efforts to preserve and maintain the diversity of birds and their habitats simply by visiting national parks and other wilderness areas. Bird enthusiasts can report the species

they observe to authorities. Checklists are now available at many popular national parks. Tourists can report evidence of suspicious activity that might lead to the arrest of unscrupulous individuals trapping or hunting birds and can also participate as volunteers in habitat conservation programmes. In these ways, tourists can help reduce the threats to birds, and at the same time enjoy Thailand's birdwatching paradise.

Contact information:

TO REPORT BIRD SPECIES OBSERVED

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

- **TO REPORT EVIDENCE OF SUSPICIOUS ACTIVITY**
  Please contact
  Willdife Protection and Suppression Office
  Department of National Parks, Wildlife, and Plant Conservation
  61 Paholyothin Road, Chatuchak, Bangkok 10900
  Tel: 66-(0)-2579-5266

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

  FAMILIES OF BIRDS IN THAILAND UNDER THREAT
  The following bird species are under threat because there is a high demand for them and they are hunted for the local, regional and global bird trade. To help preserve the species, please refrain from purchasing any of the following birds as pets, and if you happen to witness any of the following birds being sold or traded, or note any suspicious activities involving them, please contact:
  The Willdife Protection and Suppression Office
  Department of National Parks, Wildlife, and Plant Conservation
  61 Paholyothin Road, Chatuchak, Bangkok 10900
  Tel: 66-(0)-2579-5266

1. Phasianidae (wood partridges and pheasants) - 4 species
2. Anatidae (White-winged duck) - 1 species
3. Picidae (woodpeckers and barbets) - 3 species
4. Bucerotidae (hornbills) - 7 species
5. Upupidae (Common hoopoe) - 1 species
6. Cuculidae (Coral-billed ground cuckoo) - 1 species
7. Psittacidae (parrots and parakeets) - 4 species
8. Columbidae (pigeons) - 12 species
9. Accipitridae (birds of prey) - 9 species
10. Threskiornithidae (White-shouldered ibis) - 1 species

11. Ciconiidae (Lesser adjutant) - 1 species
12. Pittidae (pittas) - 3 species
13. Irenidae (Asian fairy bluebird and leafbirds) - 6 species
14. Corvidae (jays, crows, magpies, orioles and minivets) - 14 species
15. Muscicapidae (thrushes, robins, and sharmas) - 3 species
16. Sturnidae (starlings and mynas) - 3 species
17. Paridae (Yellow-cheeked tit) - 1 species
18. Pycnonotidae (bulbuls) - 7 species
19. Zosteropidae (Japanese white-eye) - 1 species
20. Sylvidae (laughing thrushes, mesias, minlas and sibias) - 8 species
21. Nectariniidae (Scarlet-backed flowerpecker) - 1 species
22. Passeridae (weavers and munias) - 7 species
23. Fringillidae (grosbeaks and buntings) - 3 species

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

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