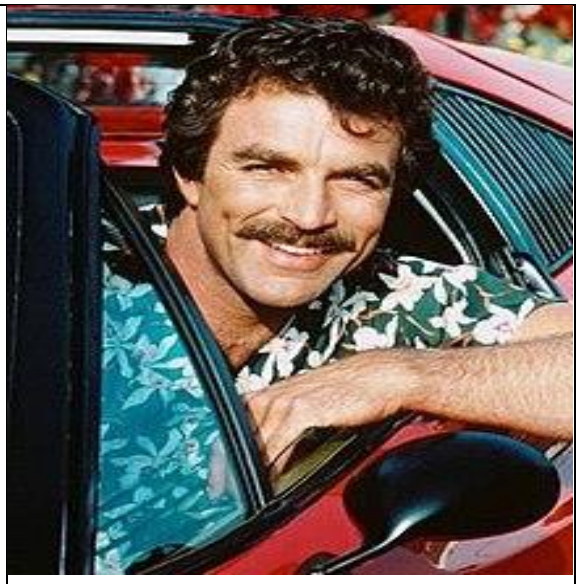
JOINT REPORT of

Analysist and investigators: Casey Donaldson, REMOVED

Unit name and Force: The Magnum P.I

Case against: John Doe

Police Reference No: 0069/23
Case Reference No: 69
PF Reference No: 4d/61/67/6e/75/6d/20/50/49



Magnum PI 1

Contents

Summary

The suspect was found to have over 200 separate illicit files pertaining to birds, that originated from the internet and two separate cameras, one of which was found and seized as part of the investigation.

The investigators have reasonable evidence to prove that John Doe was accessing illegal content from one of their email addresses and two browsers (Firefox, Internet Explorer) Further alert was caused when the investigators were able to identify illegal content hidden in a fake file, for example a jpeg image portraying an executable file.

1) Description of Crime

The suspect John Doe is accused of possessing illicit material of birds.

Incident 1 – Between 17:44 and 17:52 on 30th July 2002, 2 IIOB (Inappropriate Images of Birds) were downloaded to C:/Program Files/Microsoft Office/CLIPART/PUB60COR/ . These are numbers 109 and 110 in the Excel sheet contained in Appendix F.

Incident 2 – On the 8th July and 4th August 2004, 2 IIOB were downloaded into C:/Documents and Settings/johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/Cache/CE0AD533d01/ and C:/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/. These are numbers 113 and 114 within the Excel sheet contained in Appendix F.

Incident 3 – Between the 24th January and 9th February 2005, 127 IIOB were downloaded to various locations on the suspect's hard drive, including some hidden within system folders. These are file numbers 114 to 240 within the Excel sheet contained in Appendix F.

Incident 4 – At 11:08 on the 4th February 2005, 4 emails were found to have been received by the suspect. These including him receiving bird images as well as a bird identification guide. See Appendix B, figures 8 to 12.

There are also several items that do not contain valid timestamps, so we cannot attach them to an incident, however they are still included in the report as they are still illicit material. These are listed in the Excel sheet, items number 1 to 108.

A detailed timeline of these incidents is available in Appendix C.

2) Description of Investigation

2.1 Job Description and Instructions

Magnum P.I were tasked with investigating John Doe's hard drive. The task is to analyse the device for indecent bird images and videos and any other

evidence that can back up the accusations. The task was given to the team from Dr Ian Ferguson. The overall report writing, and sections of the report were all conducted as part of a collaborating team

We had to use a number of tools, at our disposal to extract the evidence from the digital device. Our first most important step was to create a forensically sound environment using a write blocker for imaging john doe's hard drive to prevent any changes to the data.

2.2 Description of Recovered / Examined Items

During the raid of john doe's house, Our team recovered a hard drive which may contain illicit images and videos of an ornithological nature and behaviour.

Barracuda 7200.2 80gb Seagate
Model number: ST380013AS
Date Code: 05405

Another piece of evidence was seized which is a canon camera which was broken upon capture. No SD card was in the camera.

Canon Camera
Model: Canon PowerShot SD100

2.3 Methodology

The magnum P.I's captured a virtual copy of John Doe's hard disk by using a write blocker. This produced an image file (johndoe.dd). This allowed the investigators to analyse the data, in a forensically sound environment.

The investigators created a md5sum of the John Doe disk image that could be used to verify the integrity of the created image to avoid corrupting or changing data during the analysis. The md5sum is:

d63dd1b8917ca28bac7c955fc3b6cd25

Each time that the disk image was accessed, its MD5 checksum was validated against the original.

The investigators then checked the time on the drive to test for clock skew on John Doe's machine to get accurate times. This was achieved by creating a replica image of John Doe's drive, that the magnums P.I's boated up to see if the time shown on the VM image was any different to the time displayed at the current moment. We were able to identify that there was no clock skew, and the timings were accurate.

Before investigating any further evidence, the analysist had to preform an anti-virus scan on John Doe's image. This was achieved by using a tool called FTK imager to mount a copy of the image to the E: and D: drive on a forensically safe environment before running an anti-virus scan on the drives.

The D: drive was used for the first partition and the E: drive was used for the recovered partition. This ensured no viruses were on any of the disk drive at the time. The results were no viruses found. See Appendix D

2.4 Analysis

Registry Analysis

Using a forensically safe drive image. The analysts were able to extract a list of users from the SAM database within the drive using an application called “chntpw”. The 4 main users of interest were as follows: ‘bob’ ‘jane’ ‘johndoe(admin)’ ‘Administrator(admin)’. The location of these records were found on the SAM hive.

The investigators were able to identify one USB connected. The USB was identified to be first used in January 2005 and last used in February 2005. The location was found on the system hive at: ControlSet002/Enum/USB

Number	Device Model	Device Make	Device ID
1	PS1001/1011/1006/1026 Flash Drive	Phison Electronics Corp	071A190F01DF

Table 1: Table of previously connected USBs

The usage period of this USB coincides with the file timestamps of the illicit images from Incident 3.

A type of software found to be useful for the investigation was called “VirusScan Enterprise”. Upon further analysis the investigators were able to identify that the program was set to auto scan which shows John Doe was protected against most malwares at the time. This program also was a paid version of the community VirusScan which indicates John Doe paid for this application. The location of this program was found in the software hive. See Appendix D.

These records were found using an application called “Fred”

Browser Analysis

The first browser the investigators analysed was Internet Explorer.
things of interest were:

- bird guide.pdf
  - Had images of birds with instructions on how to watch and view them, intent of grooming them and could be used for teaching bird watching. Originated from the internet.
- aggressive_song.wav,
  - A wav file containing bird noises was found. The investigators then consulted an expert by email and an application called “Picture Bird – Bird Identifier” was then used to find the type of bird to verify that it was illegal. The bird confirmed was Black-capped chickadee. File downloaded from the internet.
- several bird images,
  - Can be examined in appendix A

- software downloaded: Firefox, windows update, adobe, acrobat, Real player software,
    - This software can be used to for further analysis. real player, acrobat and adobe could've been used for illegal activity. The software itself was not illegal.

These were validated using autopsy. After internet explorer, the investigators then started analysing Firefox for further evidence.

During the examination of the Firefox history, the investigators came across, several websites most of them containing illegal images and/or audio. Some websites were advertising, digital marking, or an online marketplace.

These URL have been validated using the way back machine on the internet to verify the website during the time period of John Doe. See Appendix E.

1. URL:http://www.pbs.org/lifeofbirds
    - Illegal content, membership option which could be used to verify John Doe was using this service.
2. URL:https://www.naturewallpaper.net/birds
    - A website with illegal bird images.
3. URL:http://casalemedia.com
    - Digital marketing website. John Doe could've been looking to sell his content as evidence earlier shown he was looking at bird watching guides and he had a cannon camera himself. Login for this website should be noted as well.
4. URL:http://www.fastclick.com/
    - Another advertising website contains another logon option.
5. URL:http://uk.shop.com/amos/cc/main
    - Allows users to buy products from their account, the item John Doe searched for couldn't be found by the way back machine application.
6. URL: http://birding.about.com/od/storie1/Bird_Stories_and_Tales.htm
    - A website that contains stories, recommended cameras, and illegal content. The way back machine could not find any URL relating to this website before 2007. (The given time period)
7. URL:https://haiths.com/
    - This website contains information on bird feed, and this could show signs of John Doe grooming birds.
8. URL:http://www.imdb.com/title
    - A website for streaming movies. No snapshot of the website before 2005 however bird movies are held within this website.
9. URL:http://www.videodetective.com/
    - Another movie streaming website.
10. URL:https://whyfiles.org/shorties/104chick_sex
    - This website contains the origin of the aggressive_song.wav file. This site contains illegal content and audio files.

More searches were found including searches on Google Images.
In the location:

C:/Documents and Settings/johndoe/Application Data/Mozilla/Firefox/Profiles/w4nf3obl.default/Cache
There were 13 gif images and 5 out of 13 contained birds.

During the examination of a file called bookmarks.html we were able to find that 3 bookmarks were placed. Each of them taking the user to an illegal website. See Appendix E.

Password Protected Documents

Upon viewing the data collected the investigators were able to find 8 password protected files, made up of 7 pdf's and 1 .gpg file called "birdpics.gpg". Using a tool called john-the-ripper and two scripts. A python script called gpg2john.py for the .gpg file and a perl script called pdf2john.pl for the pdfs. The investigators were able to crack all the files.

The pdfs contained no illegal content however the "birdpics.gpg" contained an illegal image of a bird. Shown at appendix A.

Passwords found were:

- Arran – for gpg image file
    - To verify this an investigator used another tool called Kleopatra.
- 35703-f0279536.pdf password=561508, filed carved from autopsy
- 35847-f03396400.pdf password=561508, file carved from autopsy
- 35899-f0435336.pdf password=561508, file carved from autopsy
- Read006win_ENUyhoo0010.pdf, file found in program files/adobe/acrobat7.0/reader/message/ENU/
- Password=561508
- RdrMsgSplash.pdf, file found in program files/adobe/acrobat7.0/reader/message password=561508
- RdrMsgENU.pdf, file found in programs files/adobe/acrobat7.0/reader/message/ENU/ password=561508

Duplicated pdfs were found.

Emails Found

The investigators were able to find 3 email addresses in relation to this case. These email addresses were found in John Doe's mailbox located at:

C:/Documents and Settings/johndoe/Application Data/Thunderbird/Profiles

- ben@example.org

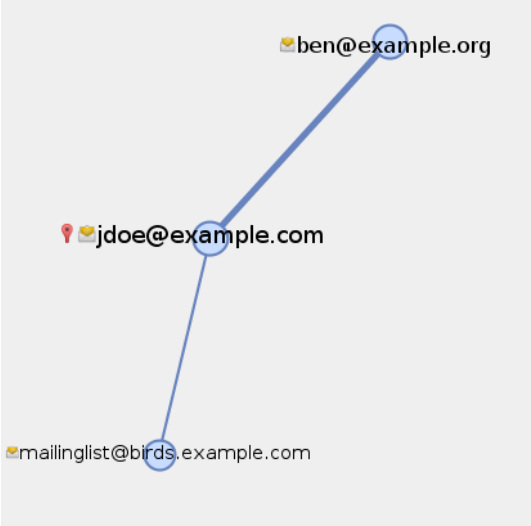
    The email was communicated with John Doe on 3 occasions, The times all appeared to be the same.

    - Email 1: Appears to be a story about exotic birds.
    - Email 2: Has 3 attachments with the caption that Ben thought John Doe would like the attachments which are illicit images.

    - Email 3:Is a thank you email to John Doe for apparent pictures. This email contains 5 attachments each of them containing illicit images.
    - Examining the emails on autopsy we found some data at an unallocated space relating to the images, on the drive. Upon further review we manage to find two URLs which have been accessed from John Doe's computer, Refer to browser analysis.
- jdoe@example.com
    - This email has only an input of received emails and none sent, believed to have been removed.
- mailinglist@birds.example.com
    - This email was found in John Doe's inbox and appears to be instructions on how to identify birds in lustful detail. E'g "their shape"
- The emails listed below appear to be different variants of Jdoe@example.com email, that could relate to the case or further investigation. These emails do not contain anything illegal but show that John doe has several email addresses in different formats.
    - jdoe@mail.example.com
    - jdoe@netscape.net
    - johndoe@example.com
    - johndoe@microsoft.com
    - johndoe@netscape.net
    - johndoe@office.microsoft.com
    - johndoe@real.com
    - johndoejohndoe@example.com

Shown at Appendix B.

Based on the emails we found the investigators created an entity relations diagram to show the relationships between the 3 email addresses. The thickness of the lines depicts the frequency of communication.



Relationship Diagram 1

2.5 Production List and Associated Description

Below is a table of all the production that will be brought to court to show physical evidence and where the digital evidence comes from.

Number	Item	Description
1	Canon PowerShot SD100 camera	This camera has been seized as a part of the raid; The investigators were able to prove that this camera has taken illegal images of birds.
2	John Doe's hard disk drive	This is the drive that the investigators used to create a forensically sound image for analysis.

Table 2:Table of court productions

3. Conclusions

The investigators were able to identify 255 unique illicit images of birds found on John Doe's drive. These were found in several different types of formats pdfs, jpg, gif, etc. 26 of these images were taken on a Canon PowerShot SD100, which was seized as evidence alongside the hard drive. 2 of the images were taken from an unfound Canon EOS-1SD camera. Duplicated images were not counted for these figures. The rest originated from the internet. Several illicit files were purposely obfuscated from the investigators, this shows intent to impede an investigation. Furthermore, emails pertaining information and images of birds were found that were in contact with two other personnel. The browser history for both Firefox and internet Explorer has been confirmed to have illegal activity visiting websites with illicit content.
A timeline of John Does activity has been displayed below in Appendix C. The earliest sign of illegal activity was found in 2001 and continued through until 2005. The timeline is based on modified time (2002 -2005) which the

investigators thought would be the most accurate because this shows John Doe was altering the data found.

4. Equipment Required for Court Proceedings

- Computer with USB port
- TV
- Speakers

Word dictionary

Forensically sound	The process of collecting data without altering any data to be used for examination.
Clock skew	This is the difference between the time that the machine holds, and the time used currently. For example, the time could be 20minutes before the current time, indicating that the file times are off by that much.
Admin	Admin is used as a shorter word for administrator and these accounts have the highest level of privileges on any windows computer. They are known as root on Linux operating systems.
Illicit images	An image containing unlawful or illegal content.

Table 3:Table of words that could help assist in the jury's understanding

Appendices

Appendix A – Images

Figure 1: John Doe's hard drive

Figure 2: John Doe's hard drive rear

Figure 2.1: John Doe's hard drive - connected to write blocker

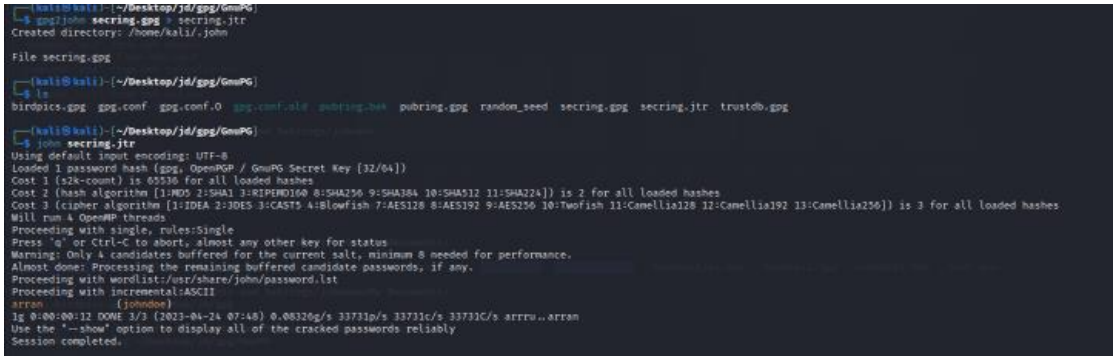


Figure 3: gpg2john – password

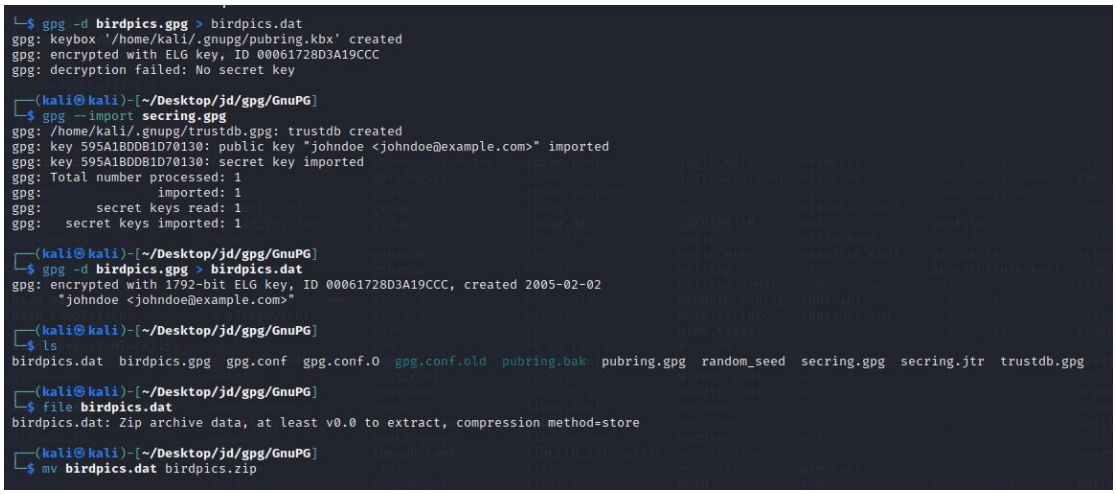


Figure 4:decrypting the file

Figure 5: showing the file as jpg

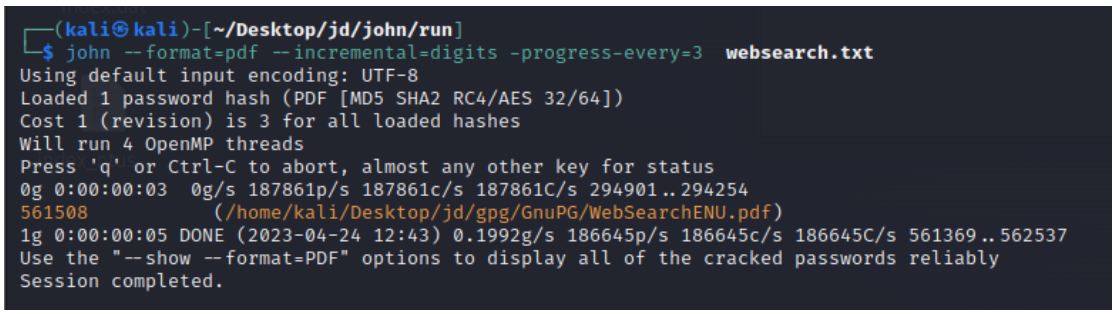


Figure 6:cracking pdfs

Figure 7: gpg encrypted image

Appendix B – Documents

Ben Forbes <ben@example.org> 09/02/2005 11:08

some more good ones

To : jdoe@example.com

BC7 feeding the birds.jpg	glfs-storm-birds.jpg	colorful-birds.jpg	IMG_3937_filtered.jpg	gawall8.jpg
107 KB	80 KB	98 KB	75 KB	24 KB

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

Figure 8:Email 1

Ben Forbes <ben@example.org> 09/02/2005 11:08

expensive birds

To : jdoe@example.com

A young woman was walking past a pet shop and saw an exotic, white cockatoo for sale. The price was $6000. She entered the store and asked the clerk why the bird was so expensive. The clerk told her that the bird spoke 6 different languages. "Does it speak English?" asked the woman. "Of course it does!" said the clerk.
The woman thought about her mother who was multi-lingual, a bit of a recluse and lived all alone.
She decided to purchase the bird and send it to her mother as a companion. She paid for the bird and made arrangements for it to be delivered. The following day, the woman telephoned her mother. "Mama, did you like the cockatoo that I sent you?" "Oh it was delicious!" she replied." "Mama, what do you mean delicious?" "I made soup out of it."
"But mama, that bird spoke six different languages!"
"Oh dear! Why didn't it say something?"

Figure 9:Email 2

Ben Forbes <ben@example.org> 09/02/2005 11:08

good pics

To : jdoe@example.com

7EYBTELF1KAN.jpg	IMG_3937_filtered.jpg	cute_penguin.jpg
18 KB	75 KB	18 KB

Hi thought you'd like these

enjoy

Figure 10: Email 3

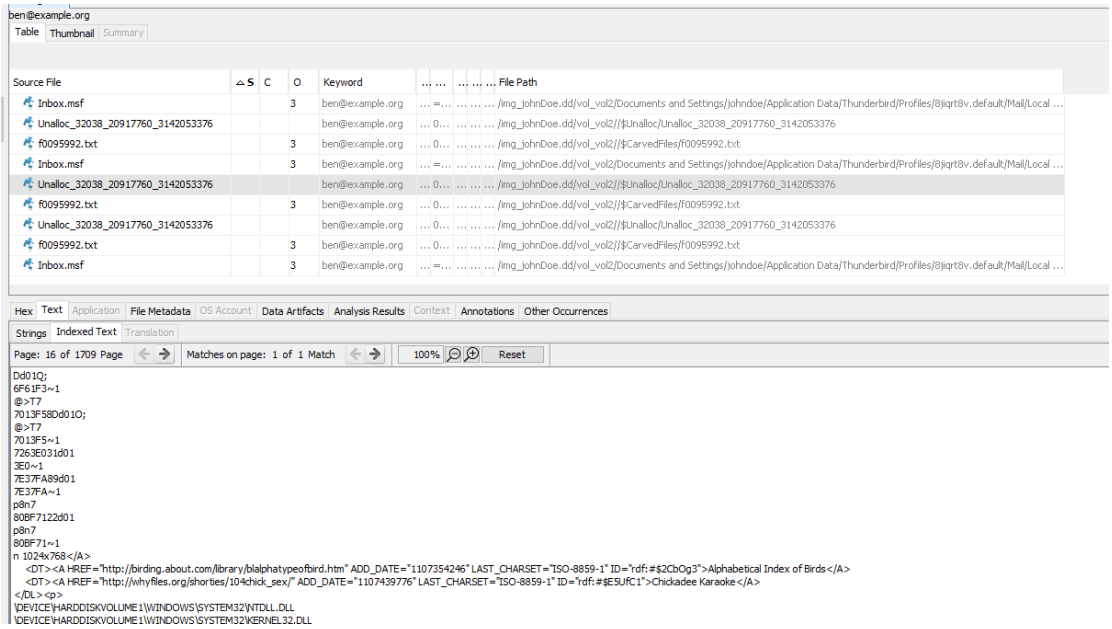


Figure 11:Email Data

Bird Fanciers <mailinglist@birds.example.com> 09/02/2005 11:08

How to Identify Birds

To : jdoe@example.com

How to Identify Birds

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

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

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

Figure 12: mailinglist@birds.example.com

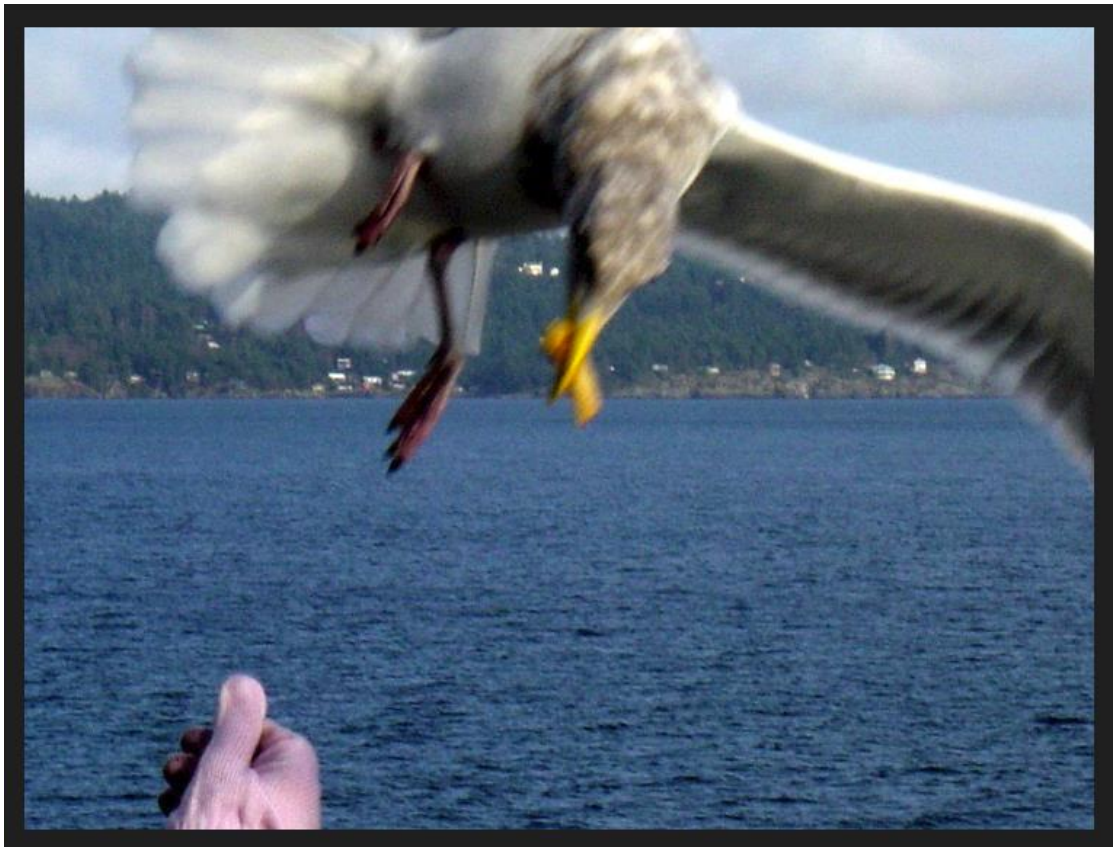


Figure 13: feeding the birds.jpg

Figure 14: glfs storm birds.jpg

Figure 15: colorful birds.jpg

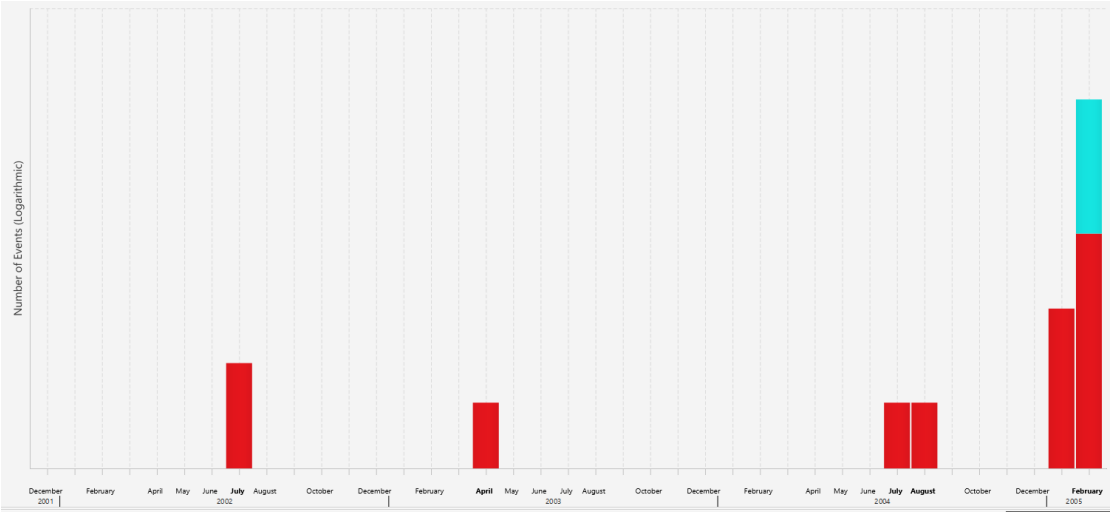
Figure 16: IMG 3937 filtered.jpg

Figure 17: gawall8.jpg

Figure 18: 7EYBTELF1KAN.jpg

Figure 19: cute penguin.jpg

Appendix C – Timeline



Timeline 1:2002 - 2005

Appendix D – Anti-virus

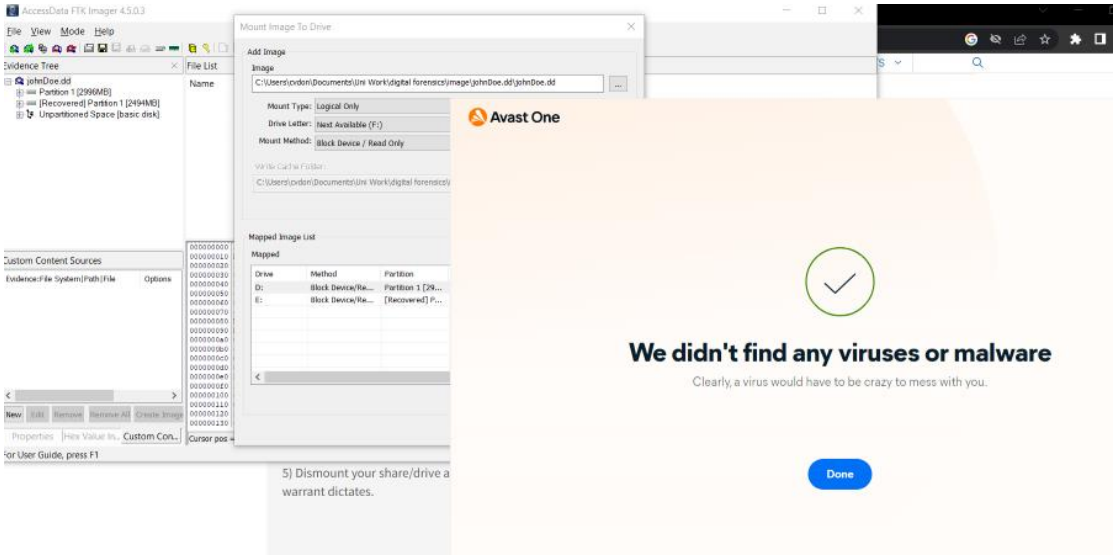


Figure 20: Anti-virus scan on John Doe's Image

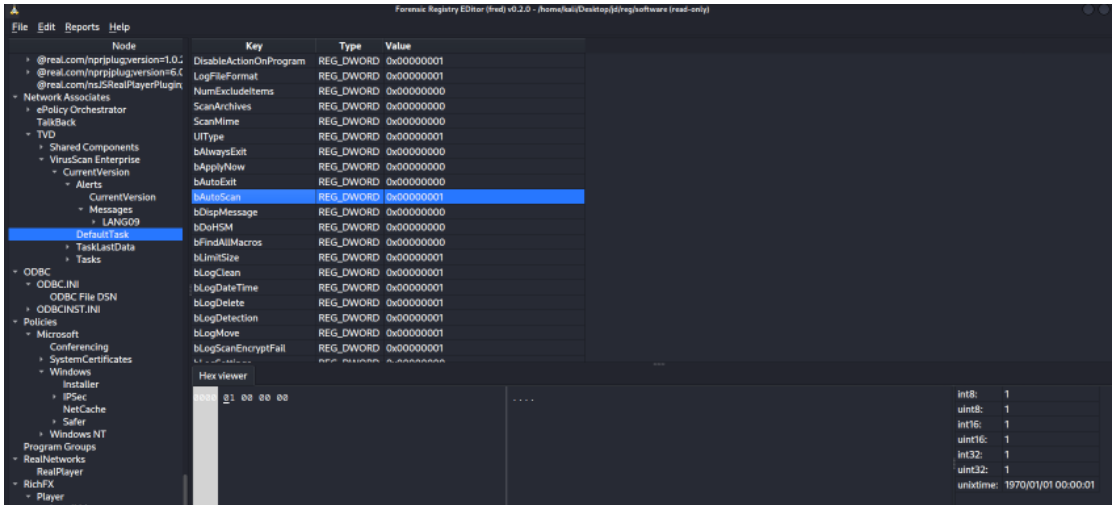


Figure 21: Software registry item shows VirusScan application and was set to auto scan.

Appendix E – Browser History

History File: index.dat Version: 5.2

TYPEURLMODIFIED TIMEACCESS TIMEFILENAMEDIRECTORYHTTP HEADERS
URL:2005020920050210: johndoe@file:///F:/AlmondMarshGreatBlueHeronStalling.jpg02/09/2005 12:06:2802/09/2005 12:06:28
URL:2005020920050210: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/birds.zip02/09/2005 06:28:0002/09/2005 06:28:01
URL:2005020920050210: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/stuf.doc02/09/2005 11:57:4902/09/2005 11:57:49
URL:2005020920050210: johndoe@:Host: My Computer02/09/2005 06:28:0002/09/2005 06:28:01
URL:2005020920050210: johndoe@file:///C:/Program%20Files/MSN/aggressive_song.wav02/09/2005 12:00:5002/09/2005 12:00:50

Figure 22: IE history temp file – John Doe

History File: index.dat Version: 5.2

TYPEURLMODIFIED TIMEACCESS TIMEFILENAMEDIRECTORYHTTP HEADERS
URL:2005012420050131: johndoe@:Host: www.linorg.usp.br01/24/2005 11:20:3402/02/2005 09:18:14
URL:2005012420050131: johndoe@http://v5.windowsupdate.microsoft.com/v5consumer/default.aspx01/24/2005 11:40:0202/02/2005 09:18:14
URL:2005012420050131: johndoe@http://office.microsoft.com/officeupdate/maincatalog.aspx?lc=en-gb01/25/2005 06:26:0402/02/2005 09:18:14
URL:2005012420050131: johndoe@http://office.microsoft.com/en-gb/FX010355751033.aspx01/25/2005 06:25:5602/02/2005 09:18:14
URL:2005012420050131: johndoe@http://v5.windowsupdate.microsoft.com/v5consumer/resultslist.aspx?ln=en-us&id=1&LinkId=SOFTWARE&TocIndex=01/24/2005 11:41:1002/02/2005 09:18:14
URL:2005012420050131: johndoe@http://office.microsoft.com/en-gb/FX010354621033.aspx01/25/2005 06:33:4602/02/2005 09:18:14
URL:2005012420050131: johndoe@http://www.linorg.usp.br/mozilla//firefox/releases/1.0/win32/en-GB/Firefox%20Setup%201.0.exe01/24/2005 11:20:3402/02/2005 09:18:14
URL:2005012420050131: johndoe@http://64.12.168.243/pub/mozilla.org/thunderbird/releases/1.0/win32/en-US/Thunderbird%20Setup%201.0.exe01/24/2005 11:24:5602/02/2005 09:18:14
URL:2005012420050131: johndoe@http://v5.windowsupdate.microsoft.com/v5consumer/resultslist.aspx?ln=en-us&id=001/24/2005 11:40:4302/02/2005 09:18:14
URL:2005012420050131: johndoe@:Host: v5.windowsupdate.microsoft.com01/24/2005 11:15:2402/02/2005 09:18:14
URL:2005012420050131: johndoe@http://www.mozilla.org/products/thunderbird01/24/2005 11:23:2502/02/2005 09:18:13
URL:2005012420050131: johndoe@:Host: 64.12.168.24301/24/2005 11:24:5602/02/2005 09:18:14
URL:2005012420050131: johndoe@http://office.microsoft.com/en-gb/FX010329501033.aspx01/25/2005 06:16:5602/02/2005 09:18:14
URL:2005012420050131: johndoe@http://www.mozilla.org/products/firefox01/24/2005 11:21:4202/02/2005 09:18:14
URL:2005012420050131: johndoe@http://v5.windowsupdate.microsoft.com/v5consumer/resultslist.aspx?ln=en-us&id=601/24/2005 11:16:1002/02/2005 09:18:14
URL:2005012420050131: johndoe@http://office.microsoft.com/en-gb/officeupdate/default.aspx01/25/2005 06:16:4502/02/2005 09:18:14
URL:2005012420050131: johndoe@file:///C:/WINDOWS/system32/oobe/actshell.htm01/24/2005 11:13:5602/02/2005 09:18:14
URL:2005012420050131: johndoe@http://www.mozilla.org/products01/24/2005 11:23:1502/02/2005 09:18:14
URL:2005012420050131: johndoe@:Host: My Computer01/24/2005 10:59:2702/02/2005 09:18:14
URL:2005012420050131: johndoe@http://mozilla.mirrors.tds.net/pub/mozilla.org/firefox/releases/1.0/win32/en-GB/Firefox%20Setup%201.0.exe01/24/2005 11:22:2502/02/2005 09:18:14
URL:2005012420050131: johndoe@:Host: mozilla.mirrors.tds.net01/24/2005 11:22:2502/02/2005 09:18:14
URL:2005012420050131: johndoe@http://v5.windowsupdate.microsoft.com/v5consumer/default.aspx?ln=en-us01/24/2005 11:40:1202/02/2005 09:18:14
URL:2005012420050131: johndoe@:Host: www.mozilla.org01/24/2005 11:17:3802/02/2005 09:18:14
URL:2005012420050131: johndoe@:Host: office.microsoft.com01/25/2005 06:16:4502/02/2005 09:18:14

Figure 23:IE history temp file - John Doe

History File: index.dat Version: 5.2

TYPEURLMODIFIED TIMEACCESS TIMEFILENAMEDIRECTORYHTTP HEADERS
URL:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/All%20Users/Documents/My%20Music/Sample%20Music/Doc1.doc02/03/2005 09:17:4802/09/2005 06:28:01
URL:2005013120050207: johndoe@:Host: My Computer02/03/2005 07:19:0702/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///C:/Program%20Files/Real/RealPlayer/Firstrun/1.htm02/02/2005 10:04:4702/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///C:/Program%20Files/Real/RealPlayer/DataCache/Login/index.html02/02/2005 09:57:1302/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/7107298.jpg02/02/2005 09:20:3302/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/kakapo.ram02/02/2005 10:11:5102/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///D:/Prac5/Q3%20Thread%20(Statechart).gif02/02/2005 10:10:4902/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/40m.jpg02/02/2005 09:43:3602/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/177.jpg02/03/2005 10:01:3802/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///C:/birdwatching.doc02/03/2005 10:49:3902/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///D:/Prac4/Prac4.gif02/02/2005 10:10:1602/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/ostbk2b2.htm02/03/2005 10:02:4502/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/Application%20Data/Mozilla/Firefox/Profiles/w4nf3obl.default/cookies.txt02/03/2005 07:19:0702/09/2005 06:28:01
URL:2005013120050207: johndoe@http://www.real.com/intro/index_upsell_manager.html?DC=NSP01D&optin=true&country=gb&language=en-gb&icon=tiscali&LI=en&PBR=1048580002/02/2005 10:04:2802/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/nestboxtips.txt02/02/2005 09:29:3002/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/aa010703a.htm02/02/2005 09:25:5902/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/tn_duck_3.jpg02/02/2005 09:18:1302/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/bob/My%20Documents/My%20Music/ready2fledge.jpg02/03/2005 10:06:4202/09/2005 06:28:01
URL:2005013120050207: johndoe@https://account.real.com/acct/intro/msg.html?msg=frweur02/02/2005 10:04:3402/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///E:/birds/audio/aggressive_song.wav02/03/2005 07:22:5102/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/Desktop/birdtrans2.jpg02/03/2005 10:04:4802/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/wbpremium_s.jpg02/02/2005 09:28:1902/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///C:/WINDOWS/ODBC.INI02/03/2005 10:54:0602/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/chicks2.jpg02/03/2005 10:05:0302/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///C:/Program%20Files/Adobe/Acrobat%207.0/Reader/Legal/Adobe%20Reader/7.0.0/en_US/license.html02/02/2005 12:03:4002/09/2005 06:28:01
URL:2005013120050207: johndoe@:Host: account.real.com02/02/2005 10:04:3402/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/Application%20Data/Mozilla/Firefox/Profiles/w4nf3obl.default/bookmarks.html02/03/2005 07:20:2002/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///C:/EvanstonWoodpecker.jpg02/03/2005 09:14:5902/09/2005 06:28:01
URL:2005013120050207: johndoe@:Host: www.real.com02/02/2005 10:04:2802/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///E:/birds/Killdeer.jpg02/03/2005 09:49:2902/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/babyscot_vyoung.jpg02/03/2005 10:00:1902/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/babyscot_2weeks1.jpg02/03/2005 10:00:2702/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/newbies2.jpg02/03/2005 10:05:4402/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///C:/Program%20Files/Real/RealPlayer/Firstrun/context.htm02/02/2005 10:04:4802/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/snow_geese.jpg02/02/2005 09:18:5302/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///E:/birds/non%20images/BirdingGuide.pdf02/03/2005 10:52:0102/09/2005 06:28:01
URL:2005013120050207: johndoe@file:///E:/birds/non%20images/BookList.doc02/03/2005 10:51:5402/09/2005 06:28:01

Figure 24: IE history temp file – John Doe

History File: index.dat Version: 5.2

TYPEURLMODIFIED TIMEACCESS TIMEFILENAMEDIRECTORYHTTP HEADERS
URLVisited: johndoe@about:Home01/24/2005 10:57:1001/24/2005 10:57:10
URLVisited: johndoe@http://office.microsoft.com/officeupdate/maincatalog.aspx?lc=en-gb01/25/2005 06:26:0401/25/2005 06:26:04
URLVisited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/Desktop/birdtrans2.jpg02/03/2005 10:04:4802/03/2005 10:04:48
URLVisited: johndoe@file:///C:/birdwatching.doc02/03/2005 10:49:3902/03/2005 10:49:39
URLVisited: johndoe@http://www.mozilla.org/products01/24/2005 11:23:1501/24/2005 11:23:15
URLVisited: johndoe@http://v5.windowsupdate.microsoft.com/v5consumer/default.aspx01/24/2005 11:40:0201/24/2005 11:40:02
URLVisited: johndoe@file:///C:/Program%20Files/Real/RealPlayer/Firstrun/context.htm02/02/2005 10:04:4802/02/2005 10:04:48
URLVisited: johndoe@http://download.mozilla.org/?product=firefox&os=win&lang=en-GB01/24/2005 11:21:4301/24/2005 11:21:43
URLVisited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/aa010703a.htm02/02/2005 09:25:5902/02/2005 09:25:59
URLVisited: johndoe@http://office.microsoft.com/en-gb/officeupdate/default.aspx01/25/2005 06:16:4501/25/2005 06:16:45
URLVisited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/babyscot_vyoung.jpg02/03/2005 10:00:1902/03/2005 10:00:19
URLVisited: johndoe@file:///E:/birds/Killdeer.jpg02/03/2005 09:49:2902/03/2005 09:49:29
URLVisited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/177.jpg02/03/2005 10:01:3802/03/2005 10:01:38
URLVisited: johndoe@file:///C:/Program%20Files/Real/RealPlayer/Firstrun/1.htm02/02/2005 10:04:4702/02/2005 10:04:47
URLVisited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/ostbk2b2.htm02/03/2005 10:02:4502/03/2005 10:02:45
URLVisited: johndoe@file:///D:/Prac5/Q3%20Thread%20(Statechart).gif02/02/2005 10:10:4802/02/2005 10:10:48
URLVisited: johndoe@res://C:\Program%20Files\Real\RealPlayer\rpplugins\rpmn3260.dll/black.html02/02/2005 10:04:4302/02/2005 10:04:43
URLVisited: johndoe@javascript:parent.fnScan();01/24/2005 11:40:2601/24/2005 11:40:26
URLVisited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/snow_geese.jpg02/02/2005 09:18:5302/02/2005 09:18:53
URLVisited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/Application%20Data/Mozilla/Firefox/Profiles/w4nf3obl.default/bookmarks.html02/03/2005 07:20:2002/03/2005 07:20:20
URLVisited: johndoe@res://C:\WINDOWS\system32\shdoclc.dll/dnserror.htm01/24/2005 11:13:0201/24/2005 11:13:02
URLVisited: johndoe@http://v5.windowsupdate.microsoft.com/v5consumer/resultslist.aspx?ln=en-us&id=001/24/2005 11:40:4301/24/2005 11:40:43
URLVisited: johndoe@file:///E:/birds/non%20images/BirdingGuide.pdf02/03/2005 10:52:0102/03/2005 10:52:01
URLVisited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/newbies2.jpg02/03/2005 10:05:4402/03/2005 10:05:44
URLVisited: johndoe@http://office.microsoft.com/en-gb/FX010354621033.aspx01/25/2005 06:33:4601/25/2005 06:33:46
URLVisited: johndoe@javascript:catchEvent('continue');02/02/2005 10:04:3402/02/2005 10:04:34
URLVisited: johndoe@http://v5.windowsupdate.microsoft.com/v5consumer/resultslist.aspx?ln=en-us&id=601/24/2005 11:16:1001/24/2005 11:16:10
URLVisited: johndoe@http://www.mozilla.org/products/thunderbird01/24/2005 11:23:2501/24/2005 11:23:25
URLVisited: johndoe@http://office.microsoft.com/search/redir.aspx?AssetID=ES790020331033&Origin=HH010704921033&CTT=501/25/2005 06:16:4701/25/2005 06:16:47
URLVisited: johndoe@file:///D:/Prac4/Prac4.gif02/02/2005 10:10:1602/02/2005 10:10:16
URLVisited: johndoe@file:///D:/Prac4/Prac4.gif02/02/2005 10:10:1602/02/2005 10:10:16
URLVisited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/7107298.jpg02/02/2005 09:20:3302/02/2005 09:20:33
URLVisited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/wbpremium_s.jpg02/02/2005 09:28:1902/02/2005 09:28:19
URLVisited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/birds.zip02/09/2005 06:28:0002/09/2005 06:28:00
URLVisited: johndoe@http://office.microsoft.com/en-gb/FX010329501033.aspx01/25/2005 06:16:5601/25/2005 06:16:56
URLVisited: johndoe@http://office.microsoft.com/search/redir.aspx?AssetID=ES790020331033&CTT=5&Origin=HA01049204103301/25/2005 06:26:0001/25/2005 06:26:00
URLVisited: johndoe@javascript:parent.fnExpressScan();01/24/2005 11:15:5401/24/2005 11:15:54
URLVisited: johndoe@http://www.mozilla.org/products/firefox01/24/2005 11:21:4201/24/2005 11:21:42
URLVisited: johndoe@file:///C:/Documents%20and%20Settings/bob/My%20Documents/My%20Music/ready2fledge.jpg02/03/2005 10:06:4202/03/2005 10:06:42
URLVisited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/stuf.doc02/09/2005 11:57:4902/09/2005 11:57:49
URLVisited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/tn_duck_3.jpg02/02/2005 09:18:1302/02/2005 09:18:13
URLVisited: johndoe@http://64.12.168.243/pub/mozilla.org/thunderbird/releases/1.0/win32/en-US/Thunderbird%20Setup%201.0.exe01/24/2005 11:24:5601/24/2005 11:24:56
URLVisited: johndoe@http://v5.windowsupdate.microsoft.com/v5consumer/resultslist.aspx?ln=en-us&id=1&LinkId=SOFTWARE&TocIndex=01/24/2005 11:41:1001/24/2005 11:41:10
URLVisited: johndoe@http://office.microsoft.com/en-gb/FX010355751033.aspx01/25/2005 06:25:5601/25/2005 06:25:56
URLVisited: johndoe@file:///C:/Program%20Files/Real/RealPlayer/DataCache/Login/index.html02/02/2005 09:57:1302/02/2005 09:57:13
URLVisited: johndoe@file:///E:/birds/audio/aggressive_song.wav02/03/2005 07:22:5102/03/2005 07:22:51
URLVisited: johndoe@file:///F:/AlmondMarshGreatBlueHeronStalling.jpg02/09/2005 12:06:2802/09/2005 12:06:28
URLVisited: johndoe@about:blank01/25/2005 06:16:3601/25/2005 06:16:36
URLVisited: johndoe@file:///C:/WINDOWS/ODBC.INI02/03/2005 10:54:0602/03/2005 10:54:06
URLVisited: johndoe@file:///C:/Program%20Files/MSN/aggressive_song.wav02/09/2005 12:00:5002/09/2005 12:00:50
URLVisited: johndoe@file:///C:/WINDOWS/system32/oobe/actshell.htm01/24/2005 11:13:5601/24/2005 11:13:56
URLVisited: johndoe@https://account.real.com/acct/intro/msg.html?msg=frweur02/02/2005 10:04:3402/02/2005 10:04:34
URLVisited: johndoe@file:///C:/EvanstonWoodpecker.jpg02/03/2005 09:14:5902/03/2005 09:14:59
URLVisited: johndoe@file:///E:/birds/non%20images/BookList.doc02/03/2005 10:51:5402/03/2005 10:51:54
URLVisited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/nestboxtips.txt02/02/2005 09:29:3002/02/2005 09:29:30
URLVisited: johndoe@http://v5.windowsupdate.microsoft.com/v5consumer/default.aspx?ln=en-us01/24/2005 11:40:1201/24/2005 11:40:12
URLVisited: johndoe@http://download.mozilla.org/?product=thunderbird&os=win&lang=en-US01/24/2005 11:23:2601/24/2005 11:23:26
URLVisited: johndoe@http://www.real.com/intro/index_upsell_manager.html?DC=NSP01D&optin=true&country=gb&language=en-gb&icon=tiscali&LI=en&PBR=1048580002/02/2005 10:04:2802/02/2005 10:04:28
URLVisited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/babyscot_2weeks1.jpg02/03/2005 10:00:2702/03/2005 10:00:27
URLVisited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/kakapo.ram02/02/2005 10:11:5102/02/2005 10:11:51
URLVisited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/Application%20Data/Mozilla/Firefox/Profiles/w4nf3obl.default/cookies.txt02/03/2005 07:19:0702/03/2005 07:19:07
URLVisited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/chicks2.jpg02/03/2005 10:05:0302/03/2005 10:05:03
URLVisited: johndoe@file:///C:/Documents%20and%20Settings/johndoe/My%20Documents/My%20Pictures/40m.jpg02/02/2005 09:43:3602/02/2005 09:43:36

URLVisited: johndoe@file:///C:/Program%20Files/Adobe/Acrobat%207.0/Reader/Legal/Adobe%20Reader/7.0.0/en_US/license.html02/02/2005 12:03:4002/02/2005 12:03:40
URLVisited: johndoe@http://windowsupdate.microsoft.com01/24/2005 11:39:5901/24/2005 11:39:59
URLVisited: johndoe@http://www.linorg.usp.br/mozilla//firefox/releases/1.0/win32/en-GB/Firefox%20Setup%201.0.exe01/24/2005 11:20:3401/24/2005 11:20:34
URLVisited: johndoe@http://mozilla.mirrors.tds.net/pub/mozilla.org/firefox/releases/1.0/win32/en-GB/Firefox%20Setup%201.0.exe01/24/2005 11:22:2501/24/2005 11:22:25
URLVisited: johndoe@file:///C:/Documents%20and%20Settings/All%20Users/Documents/My%20Music/Sample%20Music/Doc1.doc02/03/2005 09:17:4802/03/2005 09:17:48

Figure 25:IE history temp file – John Doe

All the above screenshots were found in /home/kali/mnt/drive/Documents and Settings/johndoe

```
d$00s$00)(AE=http://www.pbs.org/lifeofbirds/)(18A=1107357090607605)
  (AF=1107353514996128)(B0=pbs.org)(B1=T$00h$00e$00 $00L$00i$00f$00e$00 $00o$00\
f$00 $00B$00i$00r$00d$00s$00)(B2
     =http://www.pbs.org/lifeofbirds/songs/index.html)(18B=1107357094653422)
  (B3=1107353525280917)(B4
```

Figure 26: Lifeofbirds URL

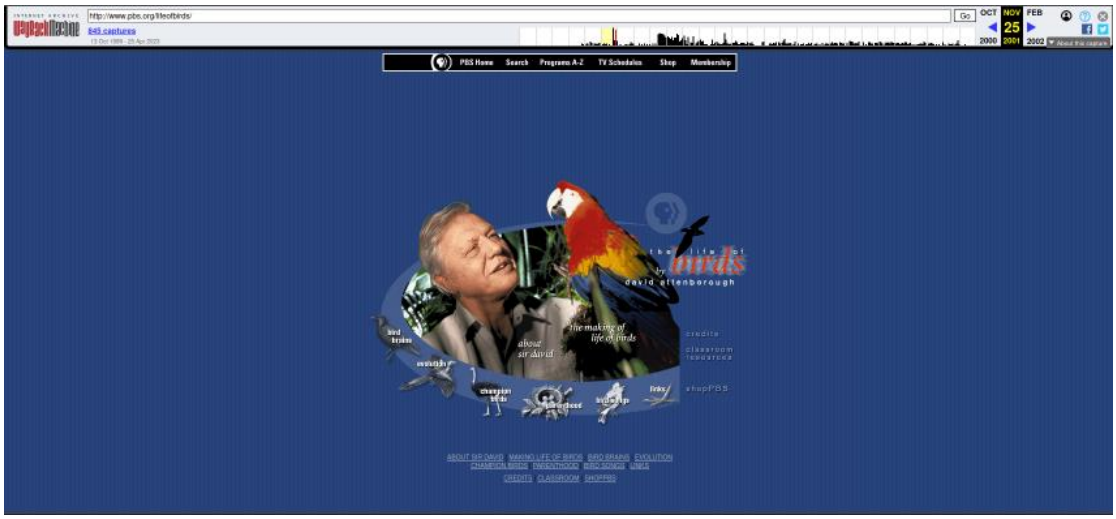


Figure 27:Lifeofbirds Website

Figure 28:Casalemedia website

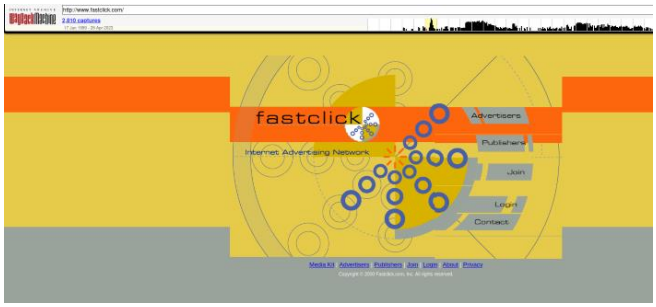


Figure 29: Fastclick website

Figure 30: Haiths website

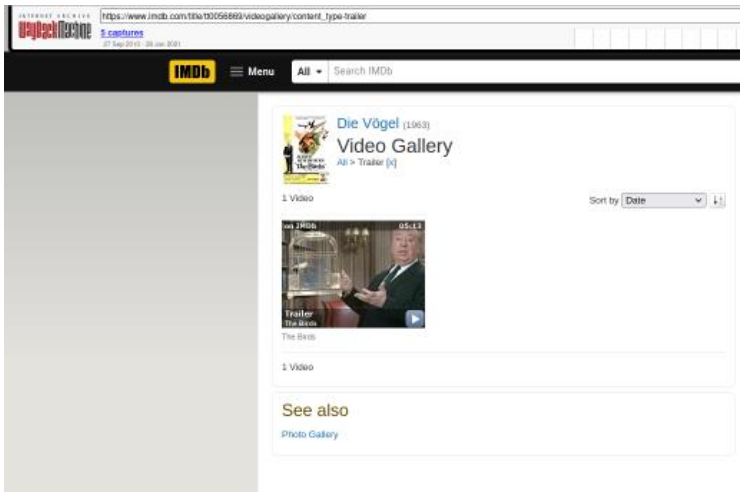


Figure 31:Imdb website

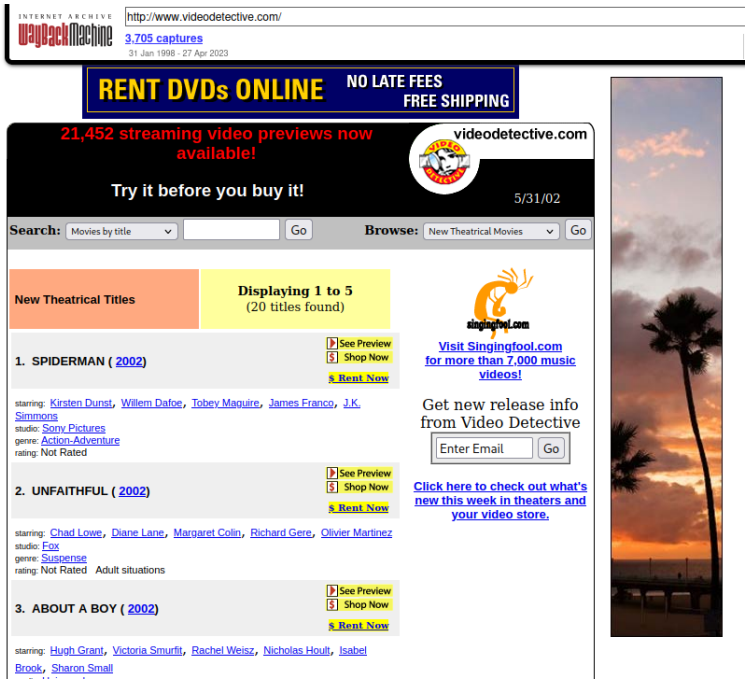


Figure 32: Videodetective website

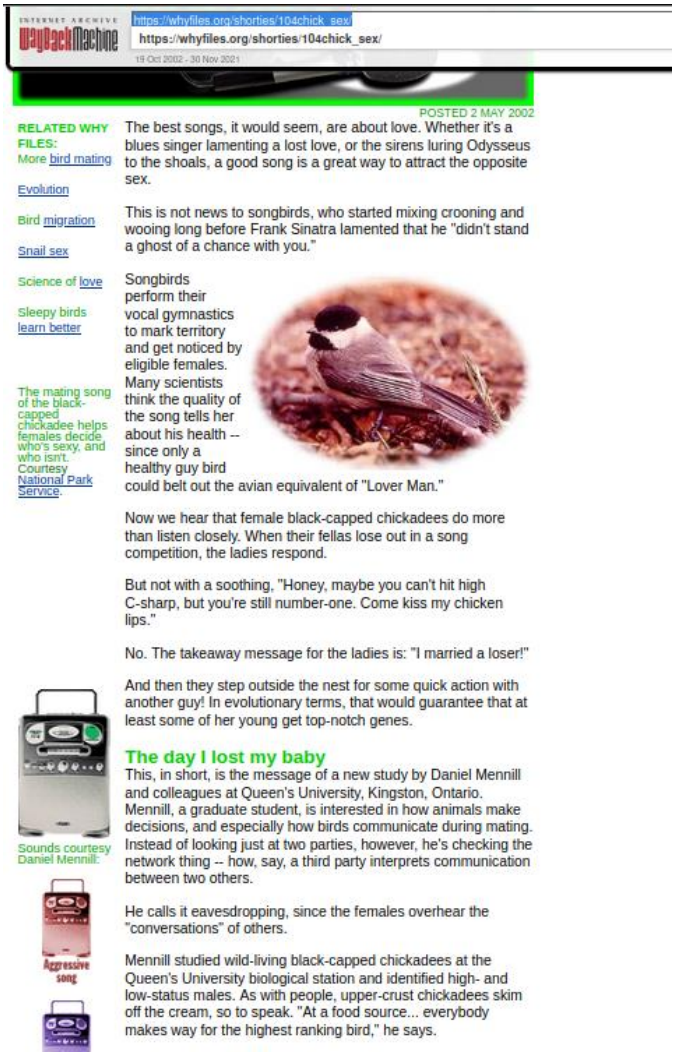


Figure 33: whyfiles website

```
    =http://ardownload.adobe.com/pub/adobe/reader/win/7x/7.0/enu/AdbeRdr70_enu\
_full.exe)(1B1=1107363193823598)(1B2=ardownload.adobe.com)>
```

Figure 34:Adobe Downloaded

```
</DL><p>
<DT><A HREF="http://www.naturewallpaper.net/birds_L.html" ADD_DATE="1107354119" ID="rdf:#$1CbOg3">Free Bird Wallpaper - Bald Eagle Albatross Owl Falcon 1024×768</A>
<DT><A HREF="http://birding.about.com/library/blalphatypeofbird.htm" ADD_DATE="1107354246" LAST_CHARSET="ISO-8859-1" ID="rdf:#$2CbOg3">Alphabetical Index of Birds</A>
<DT><A HREF="http://whyfiles.org/shorties/104chick_sex/" ADD_DATE="1107439776" LAST_CHARSET="ISO-8859-1" ID="rdf:#$E5UfC1">Chickadee Karaoke</A>
L><p>
```

Figure 35: Bookmarks

Appendix F – External evidence

REMOVED

Figure 36:: Evidence folder (Contains noteworthy files related to the investigation)

REMOVED
Figure 37: Excel spreadsheet (Contains table of recorded evidence)
REMOVED