

## **Expert Witness Report**

Title of the action: **Fred Basset, Defendant v West Midlands Police, Plaintiff**

Court reference number: **0012345**

---

Final report of [2286790] for the *West Midlands Police*

---

|   |   |
|---|---|
| <b>Dated</b>  | <b>9<sup>th</sup> November 2015</b>   |
| <b>Specialist field:</b>  | <b>Computer and Mobile Forensics</b>  |
| <b>On behalf of the<br/>Claimant/<br/>Defendant (or both if<br/>single<br/>joint expert):</b> | <b>Joint Expert</b>   |
| <b>On the instructions of:</b>  | <b>John Doe<br/>Senior Officer and Case Manager<br/>(West Midlands Police)</b>  |
| <b>Subject matter:</b>  | <b>Expert Opinion report for the exhibit IMK/1 to refute or<br/>corroborate Fred abusing Internet for browsing and<br/>distributing illegal pictures of Mickey Mouse.</b> |

**Your Name- 2286790**

**Address- Blackstone Avenue, Coventry, CV3 6FZ**

**Telephone number- 09757068485**

**Fax number/Email- 2286790@live.west-midlands.ac.uk**

**Reference**

## **Contents**

| Paragraph number | Paragraph contents                                   | Page number |
|------------------|--|-------------|
| 1                | Introduction   | 4           |
| 2                | Data Acquisition Procedures                          | 5           |
| 3                | The issues addressed and a statement of instructions | 5           |
| 4                | My investigation of the facts                        | 6           |
| 5                | My opinion   | 10          |
| 6                | Conclusion   | 10          |
| 7                | Statement of compliance                              | 11          |
| 8                | Statement of conflicts                               | 11          |
| 9                | Statement of truth                                   | 11          |
| Appendices       |  |             |
| 1                | My experience and qualifications                     | 12          |
| 2                | Supporting Evidence                                  | 12          |

**List of Tables**

| Table No. | Table Name              | Page No. |
|-----------|-------------------------|----------|
| 1         | Table of Exhibits       | 4        |
| 2         | Table of Tools Used     | 4        |
| 3         | Table of MD5 Hash Match | 9        |

**List of Figures**

| Figure No. | Figure Name                                   | Page No. |
|------------|---|----------|
| 1          | Images of Mickey Mouse on the suspect's drive | 5        |
| 2          | URLs Typed by the User                        | 6        |
| 3          | Web Searches of the User                      | 6        |
| 4          | Website from where Images were Downloaded     | 7        |
| 5          | Evidence of Distribution of Images            | 8        |
| 6          | Evidence of E-mail sent                       | 8        |

## 1 Introduction

### 1.1 The writer

I am #2286790. I am a Certified Electronic Evidence Collection Specialist, and my expertise is in Computer Forensics, Mobile Forensics, and Data Recovery. I have been working in the digital forensic industry for 12 years and have completed more than 1,500 forensic examinations, including many complicated cases.

Appendix 1 contains full details of my qualifications and experience entitling me to give expert opinion evidence.

### 1.2 Summary background of the case

The case concerns Fred Basset, who is suspected to be engaged in downloading, keeping, and distributing pictures of Mickey Mouse. Handling or accessing any kind of files (online or offline) related to Mickey Mouse is made illegal since 2005. On 9<sup>th</sup> October 2015 at 6:10 am, the suspect was brought in for interrogation according to the intelligence that links the suspect to the crime, and a desktop computer (IMK/1) was seized.

### 1.3 Those involved

Those involved in the case are as follows:

- a. Fred Basset – The suspect who is brought in for investigation.
- b. Hampsterman - To whom the suspect distributed the images through attachments.
- c. Chris Gibson – The person whose website the suspect accessed to download images. He also holds the copyright to the website and maintains it.

### 1.4 Technical terms and explanations

The technical terms used in the report are highlighted in **BOLD** letters. These terms are explained here when first used and are included in the glossary.

1. **Digital Forensic Image:** It is a bit-by-bit replication of the original drive.
2. **Write Blocker:** Prevents data being written in the evidence subject.
3. **Message Direct (MD5) Hash:** A file's hash value serves as a digital signature and is particular to each file. The integrity of the file cannot be guaranteed if the hash value does not match because the data is altered within the file.
4. **Connection Manager:** Remote Access Software for windows
5. **Autopsy:** Digital Forensic Tool used for investigation
6. **Virtual Machine:** Secondary Machine which is virtual within a machine
7. **ACPO<sup>1</sup>:** There are 4 principles for good digital forensic practices.
8. **Net Meeting:** PC to Pc Screen Sharing Software

## 2 Data Acquisition Procedures

At 6:10 am on October 9, 2015, an artefact was taken from the suspect's home. The artefact was a computer called (IMK/1) that was discovered under the stairs with its power off.

---

<sup>1</sup> Dr Harjinder Singh Allie "First Principles" Lecture Notes for DFI 13/21 University of Warwick October 9, 2022

Senior Officer and Case Manager John Doe was given the computer's original hard drive, and a chain of custody was upheld. The case manager made a **Digital Forensic Image (DFI)** by attaching the original drive to a **Write Blocker**. The software used is **Pro Discover** Image Acquiring Tool. I created a second copy to work on ("BCS Fred.E01") after receiving the DFI.

The copy image was loaded on a new clean forensic workstation, which was checked for virus beforehand. **Message Direct (MD5) Hash** of the file was checked using FTK Imager for data integrity, which was matched. The SHA-1 Hash shows a mismatch because when the DFI file was created, it did not calculate the SHA-1 Hash but only MD5 hash. So there is no possible hash to compare with.

The investigation is performed according to the **ACPO** principles and reference image for MD5 Hash is in the Appendix 2 (Figure 1).

| Exhibit Devices  | Serial Number                        | Description |
|------------------|--------------------------------------|-------------|
| Desktop Computer | 5df4b63c-b603-4127-9f5b-b0e9e8eb7bc9 | Windows XP  |

*Table 1: Table of Exhibits*

| Tools Used and Result        | Description            | Version |
|------------------------------|------------------------|---------|
| Avast Antivirus (Software)   | No Threat found        | 2015    |
| Pro Discover (Software)      | Image Acquiring Tool   | 2015    |
| FTK Imager (Software)        | Hash Integrity Checker | 4.1.1.2 |
| Ultra Dock (Hardware)        | Write Blocker          | -       |
| Autopsy (Software)           | Digital Forensic Tool  | 4.19.3  |
| Registry Explorer (Software) | Tool                   | 2.0.0.0 |

*Table 2: Table of Tools Used*

### 3 The issues to be addressed and a statement of instructions

The issues to be addressed in this report includes the statements provided by the suspect and verifying it. This report includes a review of the data discovered on the hard drive of the computer named FREDDY which was in the hands of the suspect FRED. After examining it with industry-standard forensic tools and techniques, the purpose of is to provide an expert opinion with supporting evidence.

#### 3.1 The purpose of the report:

I have been instructed by John Doe, to examine and investigate the exhibit for evidence and provide an expert report independent of the parties included for the following objectives:

- To determine if there are any occurrences of illegal images of Mickey Mouse.
- If the occurrences are discovered, look for evidence linking the suspect to the distribution of these illegal images.
- Identify any evidence to corroborate or refute the statements provided by the suspect.
- Provide supporting evidence of either *actus reus* or *mens rea* for each of the objectives.

#### 4 My investigation of the facts:

The DFI has three partitions (Volumes). Using Autopsy (v 4.19.3), I discovered five images of Mickey Mouse during my preliminary manual investigation in the second partition (img BCS Fred.E01/vol vol2/Document and Settings/Fred/My Documents/My Pictures/). There are other occurrences of mickey mouse in the drive which is due to data stored in the temporary files by the system.

Figure 1 shows these images, which were accessed on June 8, 2006. Extraction of the system registry file and examination of the most recently used documents in Registry Explorer (version 2.0.0.0), i.e. (Software/Microsoft/Windows/Current Version/Explorer/RecentDocs), can be used to confirm this fact. The reference image is in Appendix 2 (Figure 2).

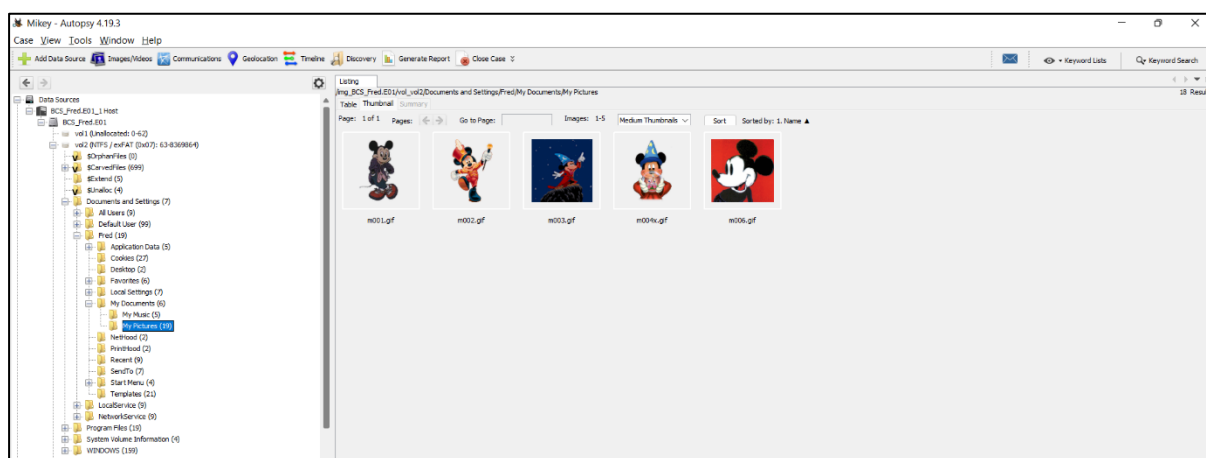


Figure 1: Images of Mickey Mouse on the suspect's drive

I discovered a registry of URLs that the user had entered, in the NTUSER.DAT file, which was extracted using Autopsy. This registry entry reveals that the user entered the URL manually <http://mickeymouse.com/>. (Software/Microsoft/Internet Explorer/TypedURLs)

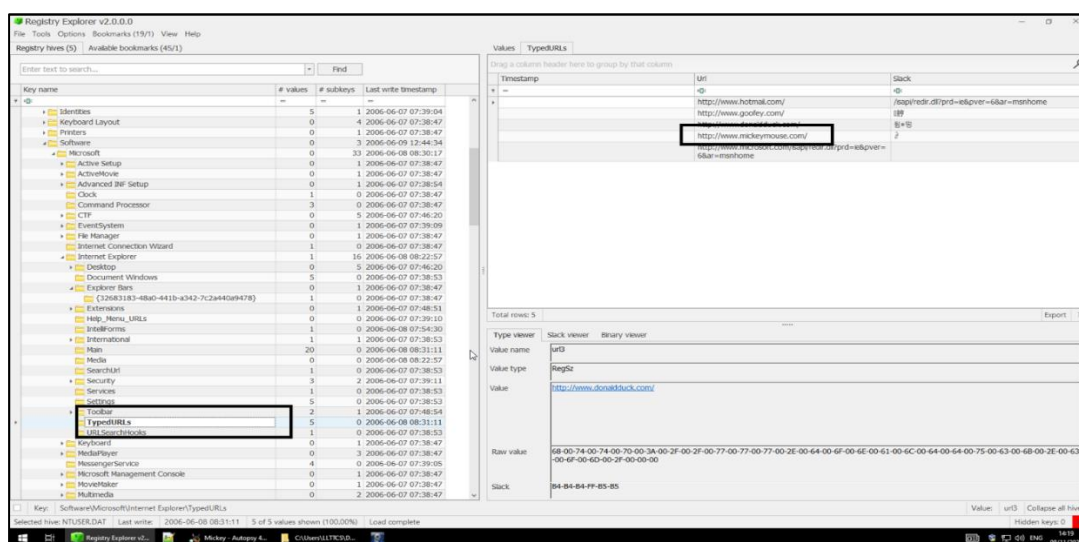
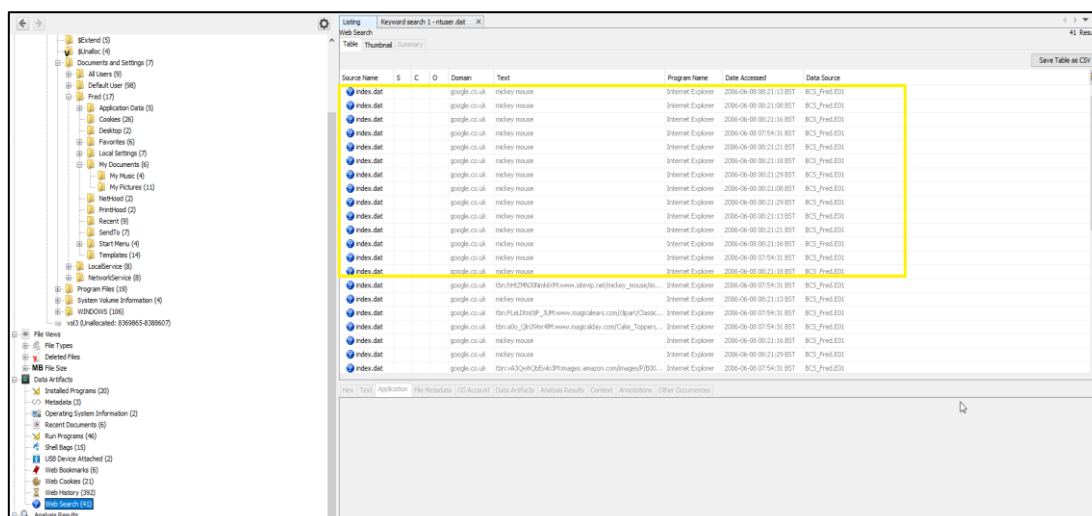


Figure 2: URLs Typed by the User

This fact can be further confirmed by looking into Web Searches column in Autopsy. This shows that the user typed the keyword “mickey mouse” on the domain [www.google.co.uk](http://www.google.co.uk).



| Source Name | S | C | O | Domain       | Text         | Program Name      | Date Accessed           | Data Source  |
|-------------|---|---|---|--------------|--------------|-------------------|-------------------------|--------------|
| index.dat   |   |   |   | google.co.uk | mickey mouse | Internet Explorer | 2006-06-09 09:21:10 BST | ICS_Pred.E01 |
| index.dat   |   |   |   | google.co.uk | mickey mouse | Internet Explorer | 2006-06-09 09:21:08 BST | ICS_Pred.E01 |
| index.dat   |   |   |   | google.co.uk | mickey mouse | Internet Explorer | 2006-06-09 09:21:04 BST | ICS_Pred.E01 |
| index.dat   |   |   |   | google.co.uk | mickey mouse | Internet Explorer | 2006-06-09 07:54:31 BST | ICS_Pred.E01 |
| index.dat   |   |   |   | google.co.uk | mickey mouse | Internet Explorer | 2006-06-09 09:21:01 BST | ICS_Pred.E01 |
| index.dat   |   |   |   | google.co.uk | mickey mouse | Internet Explorer | 2006-06-09 09:21:08 BST | ICS_Pred.E01 |
| index.dat   |   |   |   | google.co.uk | mickey mouse | Internet Explorer | 2006-06-09 09:21:29 BST | ICS_Pred.E01 |
| index.dat   |   |   |   | google.co.uk | mickey mouse | Internet Explorer | 2006-06-09 09:21:13 BST | ICS_Pred.E01 |
| index.dat   |   |   |   | google.co.uk | mickey mouse | Internet Explorer | 2006-06-09 09:21:01 BST | ICS_Pred.E01 |
| index.dat   |   |   |   | google.co.uk | mickey mouse | Internet Explorer | 2006-06-09 07:54:31 BST | ICS_Pred.E01 |

Figure 3: Web Searches of the User

The user also browsed a web page, from where he looked through many images of mickey mouse and downloaded 5 of them. The copyright to this website is maintained by Chris Brown and the email associated with this name is [webmaster@mickey-mouse.com](mailto:webmaster@mickey-mouse.com).

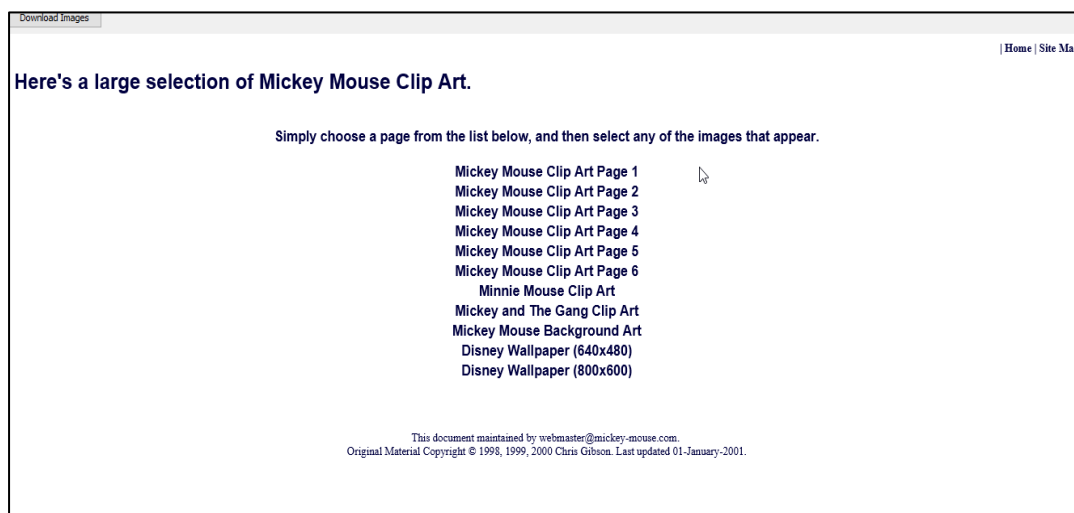


Figure 4: Website from where images were downloaded

Moreover, I discovered an email from [mickeyfan@hotmail.com](mailto:mickeyfan@hotmail.com) on August 6, 2006, to [Hampsterman@animalhouse.com](mailto:Hampsterman@animalhouse.com), with the subject line "Here are those pics you asked for ;)" and images of Mickey Mouse attached.

Fred owns the email [mickeyfan@hotmail.com](mailto:mickeyfan@hotmail.com) and likely used it to conceal his identity. This can be inferred because there is only one user on the computer and Fred's operating system account was used to access the website. Appendix 2 (Figure 3) contains evidence demonstrating that Fred used this Hotmail account on his own operating system.

2286790

## Joint Expert Witness

### West Midlands Police

Further, I found a temporary file that proves the Fred distributed the images and sent it.(/img\_BCS\_Fred.E01/vol\_vol2/Documents and Settings/Fred/Local Settings/Temporary Internet Files/Content.IE5/K9Y055DX/compose [2]) using Autopsy.

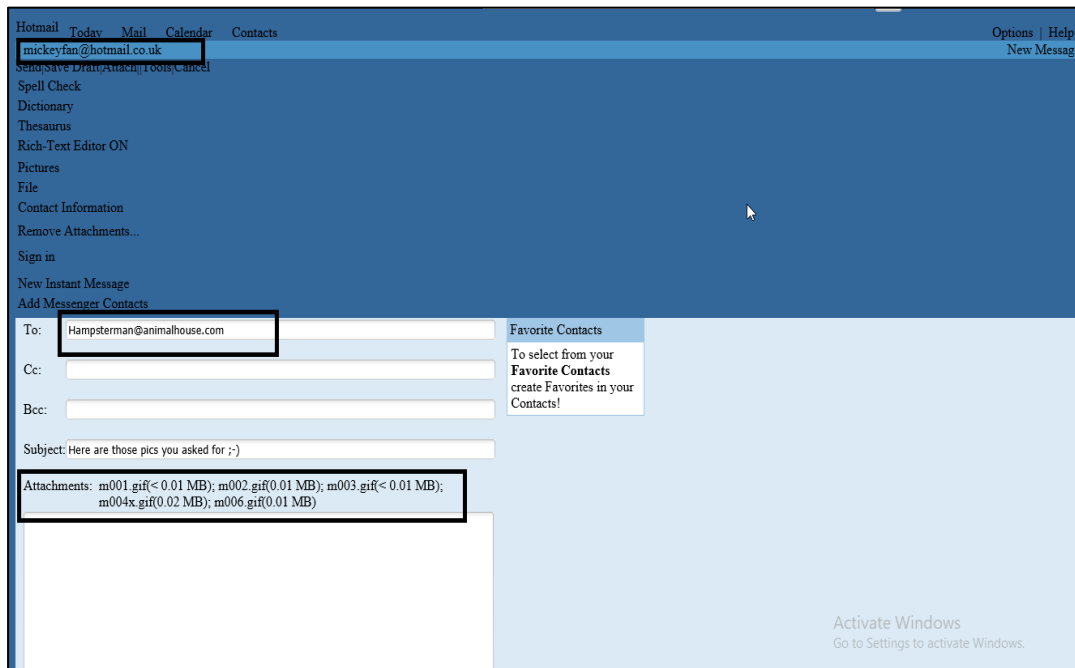


Figure 5: Evidence for distribution of Images (actus reus)

Using Autopsy, the proof of sent mails is below and can be found at:

(/img\_BCS\_Fred.E01/vol\_vol2/Documents and Settings/Fred/Local Settings/Temporary Internet Files/Content.IE5/BUETOYP0/5955[1])

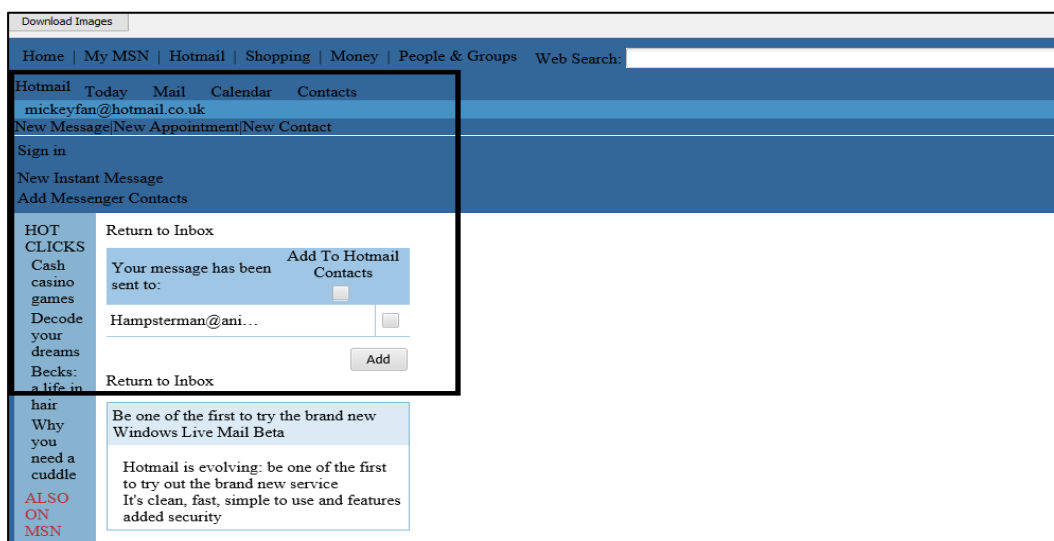


Figure 6: The confirmation of email sent (mens rea)



#### 4.1 Assumed facts

There is only one user of this device called FREDY, who is assumed to be FRED (Appendix 2 Figure 5). Additionally, it is assumed that the user's access to the www.disney.com website gave him the access to the Mickey Mouse images as well. It is assumed that he deleted the images right away and did not have any intentions or interest in these pictures.

#### 4.2 Enquiries/investigation into facts by the expert

In the course of my initial research, I discovered that the images of Mickey Mouse had a hash match with images from a different location in the temporary internet files, which are used to store all cache (temporary) data while browsing or surfing the internet.

| Hash                             | Location   |
|----------------------------------|--|
| 83ca13e6218f6fe7efd1c5b78587215e | img_BCS_Fred.E01/vol_vol2/Document and Settings/Fred/My Documents/My Pictures                            |
| 83ca13e6218f6fe7efd1c5b78587215e | img_BCS_Fred.E01/vol_vol2/Document and Settings/Fred/Local Settings/Temporary Internet Files/Content.IE5 |

Figure 3: Table of MD5 Hash Match

Given that the hash of the downloaded images and the browsed images are the same, these two files demonstrate that the suspect downloaded the images from the same website that he was browsing on 08-06-2006. Another inference is that the images did not appear as a result of cookies, and even if they had, it was because he had repeatedly searched the internet for Mickey Mouse and had viewed the images on various Mickey Mouse websites.

In addition, before accessing the images, the suspect installed Connection Manager, tried to connect with Remote Assistance and created a VMware (v.3.1.0000) in order to establish a remote access connection online. The appendix 2 (figure 4) contains the reference image for the events. He already accessed and installed the virtual machine on his computer on 16-12-2005 and installed connection manager on 7-06-2006 (The day he accessed the illegal images).

#### 4.3 Documents

With this Expert Witness Report, there are three other documents attached:

1. Documents of intake of exhibits (Chain of custody form)
2. Document stating assignment of evidence exhibit to me
3. Pictures, videos, and notes taken on the scene and during investigation

#### 4.4 Interview and examination

When interviewed, the suspect reportedly stated that he has no interest in pictures like that and he did not keep them. He further stated that the pictures may have appeared through the website cookies and that he deleted them straight away from the computer.

**5 My Opinion:**

It can be observed that the suspect was aware that searching for and downloading images is prohibited by reviewing the timeline of events that took place in the system using Autopsy. He made several attempts to hide the fact that he had personally accessed them. To only be able to access his own desktop remotely, he created a virtual machine. The suspect also claimed that "the pictures may have appeared from cookies," but this is untrue because cookie files store data about websites visited. At (/img BCS Fred.E01/vol vol2/Documents and Settings/Fred/Cookies/), 21 cookie files were discovered, of which two were linked to Mickey Mouse. One cookie file named fred@disney.go[1].txt was created when the website disney.go.com/ was accessed. The other cookie file fred@login.live[2].txt contains the username (mickeyfan@hotmail.com) and website domain login.live.com/.

In my opinion, the suspect was interested in these images and did his best to cover up his wrongdoing. All the evidence found during my investigation can be considered as exculpatory.

According to his statement, he had no intention to keep those images and deleted them right away, but there were no traces of any images in the deleted files. Although it is possible if the data is overwritten after being deleted, he only downloaded 5 images, and they were all present on the drive. Thus, he deleted nothing. The suspect also seemed to have some technical knowledge as he tried to connect remotely to his own computer several times. Additionally, he sent the pictures via email and made an effort to conceal his identity by using a different name (mickeyfan). This action shows that he knew what he was doing and had every intention of doing it.

Besides that, the desktop computer was discovered under the stairs, powered off. The user's account has logged in only 10 times since the last logout time of 18:19:50 on June 9, 2006 (Appendix 2 figure 5). This shows that the suspect used the computer only for acquiring, accessing, and distributing the images and then stopped using it afterwards, clearly shows his intentions to use it solely for this purpose.

**3.6 Limitations:**

On 07/06/2006, the suspect installed a piece of malware called Fontcore. It is hard to ascertain why he put this malware on his system. He also installed **NetMeeting**, which is PC to PC screen sharing software. The intention as to why he installed a screen sharing software cannot be confirmed.

(/img\_BCS\_Fred.E01/vol\_vol2/WINDOWS/system32/config/software)

One other limitation is the Virtual Machine created by the suspect. At the moment not much can be retrieved from the virtual machine logs as it is a whole separate system.

**3.6 My Conclusions:**

The goal of this investigation was to find exculpatory or inculpatory evidence supporting or contradicting the statements reported by the suspect Fred Basset. All conclusions drawn here are supported by the circumstantial, logical, and exculpatory evidence mentioned above.

It is possible to infer from the interpretation of the aforementioned data that the suspect, Fred Basset, had a strong interest in illegal Mickey Mouse images. He consciously distributed these images through his Hotmail account which can be considered as direct

**2286790**

**Joint Expert Witness**

**West Midlands Police**

evidence linking the suspect to his crime. The evidence found in my investigation was exculpatory and contradicting Fred's original statements.

Finally, I can conclude that the digital forensic investigation for the exhibit IMK/4 is successfully completed, and an expert witness report was made.

**Statement of compliance**

I understand my duty as an expert witness to the court to provide independent assistance by way of objective unbiased opinion in relation to matters within my expertise. I have complied with that duty and will continue to comply with it. I will inform all parties and where appropriate the court and in the event that my opinion changes on any material issues. I further understand that my duty to the court overrides any obligation to the party from whom I received instructions. Parts 33.2 (1), (2) and (3) and 33.4(j) Criminal Procedure Rules

**Declaration of Truth**

This statement consisting of..... pages, is true to the best of my knowledge and belief and I make it knowing that, if it is tendered in evidence, I shall be liable to prosecution if I have wilfully stated in it anything which I know to be false or do not believe to be true.

**Statement of conflicts**

I confirm that I have no conflict of interest of any kind, other than any which I have already set out in this report. I do not consider that any interest which I have disclosed affects my suitability to give expert evidence on any issue on which I have given evidence and I will advise the party by whom I am instructed if, between the date of this report and the trial, there is any change in circumstances which affects this statement.

**Signature**



**Date...09-Nov-2015.....**

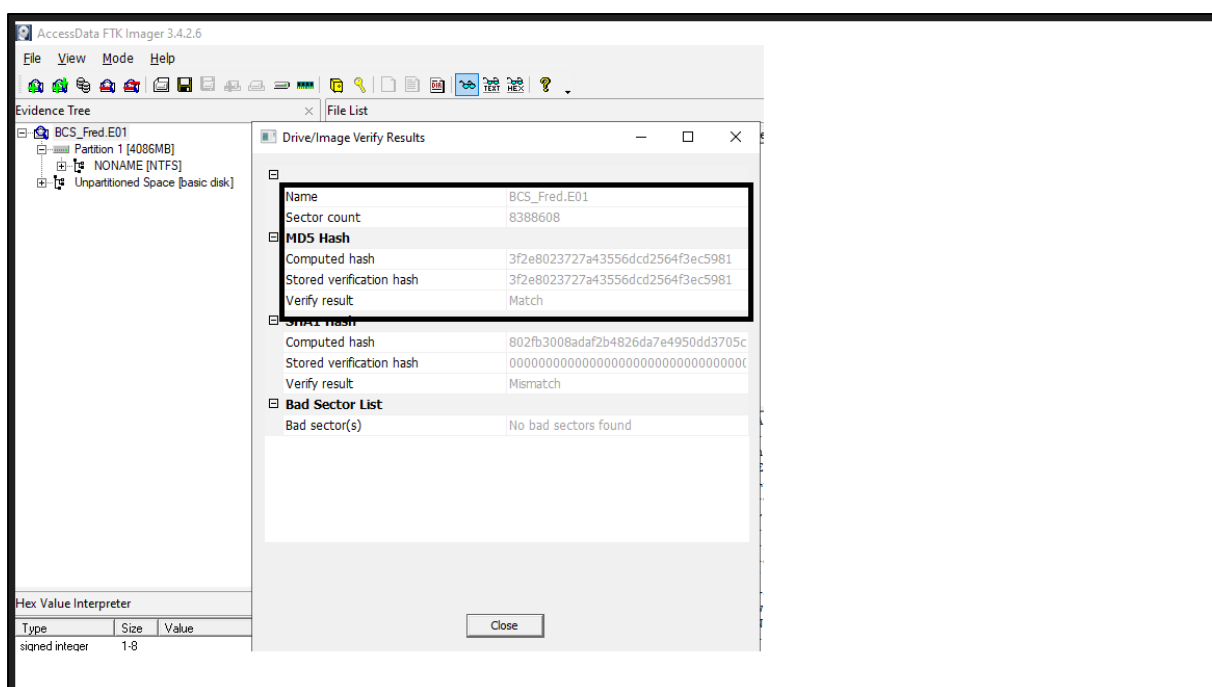
## Appendix 1

I have completed my Bachelor's in Computer Science from University of Warwick and Master's in Digital Forensics from The University of Birmingham. I have attended several training sessions and have attended to and investigated many high profile cases since the past 12 years. I have been working with the west midlands police for 7 years now. Before that, I was working with The Police Service of Northern Ireland.

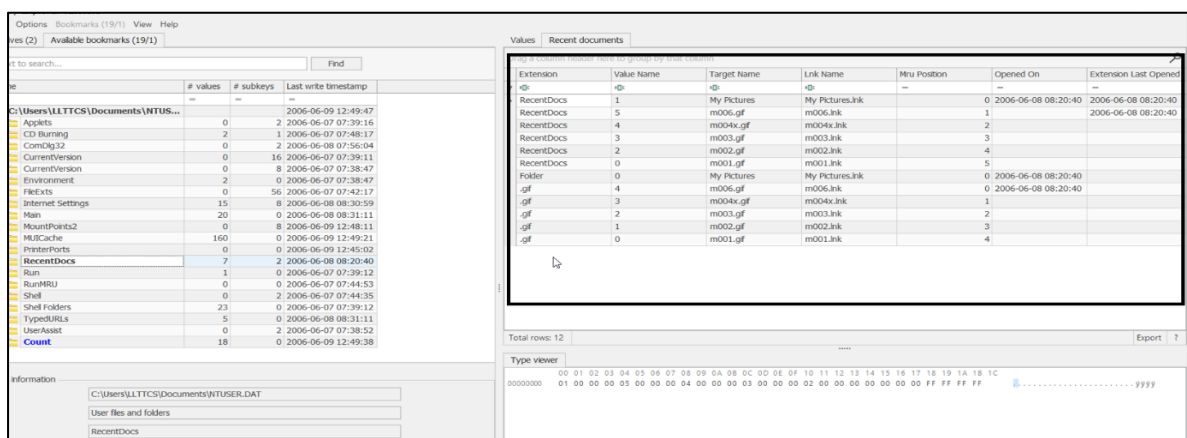
## Appendix 2

### Supporting Evidence

#### 1. Hash Match of the copy of DFI file



#### 2. Recent Documents accessed in Registry Explorer





2286790

**Joint Expert Witness  
West Midlands Police**

5. Proof that Fred is the only user of the computer:

Registry Explorer V2.0.0.0

File Tools Options Bookmarks (2/0) View Help

Values User accounts

Drag a column header here to group by that column

|                                     | Total Login Count | Created On          | Last Login Time     | Last ... | Last ... | Expir... | User Name        | Pro...  | Pas... | Gr...          | Comment   | Us... | Ho... | Int... | Re... | Ac...                               | Ho...                    | Pa...                               | Te...                    | No...                               | Mh...                    | Int...                   | W...                     | ...                      | Password Does Not Expire            | Auto Locked              |
|-------------------------------------|-------------------|---------------------|---------------------|----------|----------|----------|------------------|---|--------|----------------|---|-------|-------|--------|-------|-------------------------------------|--------------------------|-------------------------------------|--------------------------|-------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|-------------------------------------|--------------------------|
| <input checked="" type="checkbox"/> | 0                 | 2006-06-07 08:22:43 |                     | 200...   |          |          | Administrator    |   |        | Administrators | Built-in account for administering the computer/domain      |       |       |        |       |                                     | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| <input checked="" type="checkbox"/> | 0                 | 2006-06-07 08:22:43 |                     |          |          |          | Guest            |   |        | Guests         | Built-in account for guest access to the computer/domain    |       |       |        |       | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| <input checked="" type="checkbox"/> | 0                 | 2006-06-07 07:31:15 |                     | 200...   |          |          | HelpAssistant    | Remote Desktop Help Assistant Account           |        |                | Account for Providing Remote Assistance                     |       |       |        |       | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| <input checked="" type="checkbox"/> | 0                 | 2006-06-07 07:33:18 |                     | 200...   |          |          | SUPPORT_38894540 | CN=Microsoft Corporation Remote Support Service |        |                | This is a vendor's account for the Help and Support Service |       |       |        |       | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| <input checked="" type="checkbox"/> | 10                | 2006-06-07 07:38:41 | 2006-06-09 12:44:34 | 200...   |          |          | Fred             | Administrator                                   |        |                |   |       |       |        |       | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |