FACULTY OF SCIENCE & TECHNOLOGY
Department of Computing & Informatics
Forensic Computing & Security

Digital Forensics Fundamentals

Paul-David Jarvis
s5115232@bournemouth.ac.uk

Technical Witness Statement

Table of Contents

List of Figures

List of Tables

1.0 Chain of Custody

The evidence was collected from the crime scene and then transported to Dorset Police Station at 399 Wimborne Road, BH92AS and then given to the director of commercial and then was given to the head of commercial (Forensics) who passed it down to the senior commercial manager (digital) and then finally to TF whose current role is the technical commercial officer (TF)

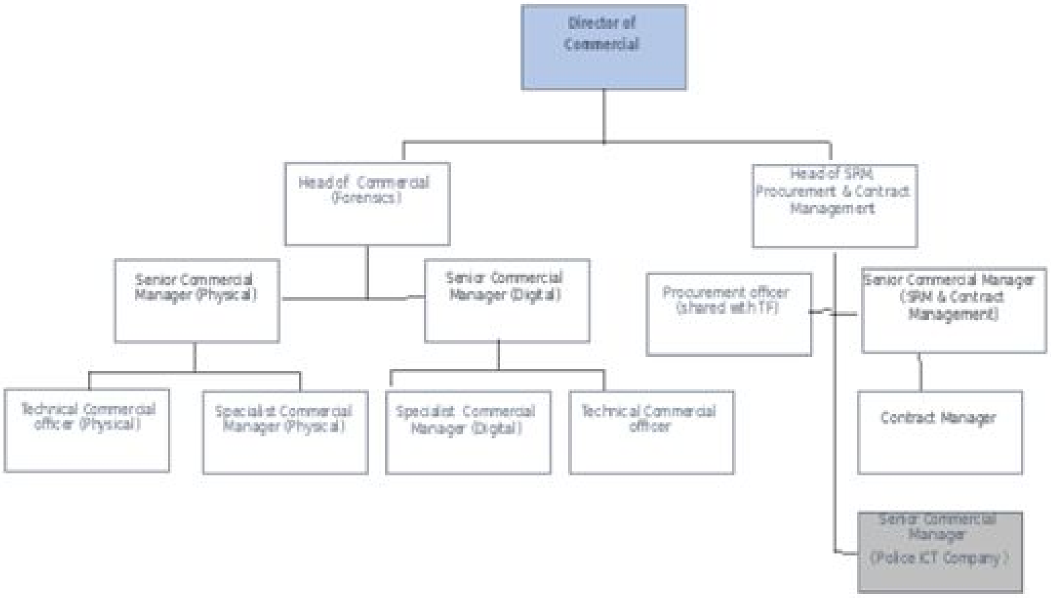

Director of Commercial
Head of Commercial (Forensics)
Head of SRM, Procurement & Contract Management
Senior Commercial Manager (Physical)
Senior Commercial Manager (Digital)
Procurement officer (shared with TF)
Senior Commercial Manager (SRM & Contract Management)
Technical Commercial officer (Physical)
Specialist Commercial Manager (Physical)
Specialist Commercial Manager (Digital)
Technical Commercial officer
Contract Manager
Senior Commercial Manager (Police ICT Company)

Figure 1: Police Hierarchy

The disk image was created from the possessions found on the individual who was arrested at the crime scene. The evidence referenced “40DDENC” was then handed over to the chief of police for the case referenced “FRTCR40” and then was given to the head of commercial (forensics) and finally to the technical commercial officer, that was TF.

2.0 Brief

TF was tasked with a thorough investigation of an image of a device that was recovered among the personal possessions of an individual who was arrested. This task came from the director of commercials and down the evidence was passed down the chain of command and is for the case “FRTCR40” and this image file is referred to as “40DDENC”.

3.0 Investigator

TF graduated with a bachelor's degree in 2017 and a master's degree in 2018 at Bournemouth University. TF is also a certified forensic computer examiner (CFCE) from 2019. TF has been working for Dorset police in their cybersecurity and computer forensics sector as a Technical Commercial Officer since 2019.

4.0 Investigation Environment

Dorset Police forensics lab was the environment where this investigation was conducted. A small number of people have access to these labs, they require an 8-digit pin code to enter the labs. The computers in these labs are running an Intel Core i7-8700 CPU and have 64GB of memory. They're also running a basic Linux Debian system. These computers all come with ExifTool, hex dump and nano pre-installed. The Debian version is 4.19.67-2, ExifTool version is Perl v5.24.1, nano is running version 2.7.4. They are all password protected and encrypted to make sure that there is no unauthorised access.

5.0 Integrity Check

TF took the hash of both the dd file and the enc file as well as a zip file that was retrieved after mounting the image file and the zip file that was retrieved after decoding the encrypted file. As well as maintaining the integrity of these two main files, TF also noted the hash of every single file in every single folder in case the folders were altered so he can find out exactly what has been changed or deleted.

Integrity Check	
Evidence	Hash
Jarvis,Paul-David,s5115232_1.dd	6d62a955ad8b1c44d4327f969fa8529b
040_1.zip	49a07faeae7d7bc97c1529f2e291c8cf
Jarvis,Paul-David,s5115232_2.enc	c979f8f38a045bc337b3ea545ea27ced

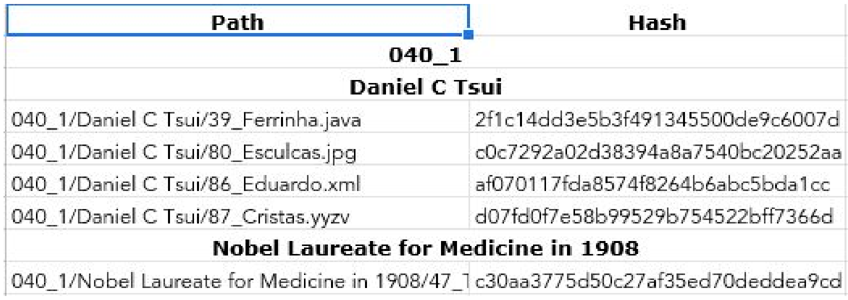
040_2.zip	fbd0e3e0b2af40b3f98a790770772bbb

Table 1: Integrity Check

6.0 Retrieval Process

6.1 Integrity

TF took a hash of every single file to maintain the integrity of every single file, these can be found in the hash table of the evidence summary spreadsheet. Seen in figure 2.

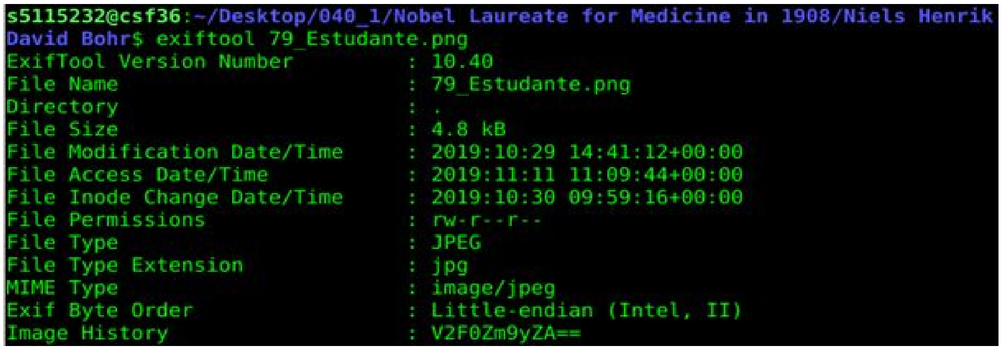


Path	Hash
040_1	
Daniel C Tsui	
040_1/Daniel C Tsui/39_Ferrinha.java	2f1c14dd3e5b3f491345500de9c6007d
040_1/Daniel C Tsui/80_Esculcas.jpg	c0c7292a02d38394a8a7540bc20252aa
040_1/Daniel C Tsui/86_Eduardo.xml	af070117fda8574f8264b6abc5bda1cc
040_1/Daniel C Tsui/87_Cristas.yyzv	d07fd0f7e58b99529b754522bff7366d
Nobel Laureate for Medicine in 1908	
040_1/Nobel Laureate for Medicine in 1908/47_1	c30aa3775d50c27af35ed70deddea9cd

Figure 2: File Path and Hash

6.2 Exiftool

TF used Exiftool to examine the metadata of every file looking for hidden information and data, this can be seen in figure 3. Exiftool was also used to make a note of all the extensions looking for fake ones.

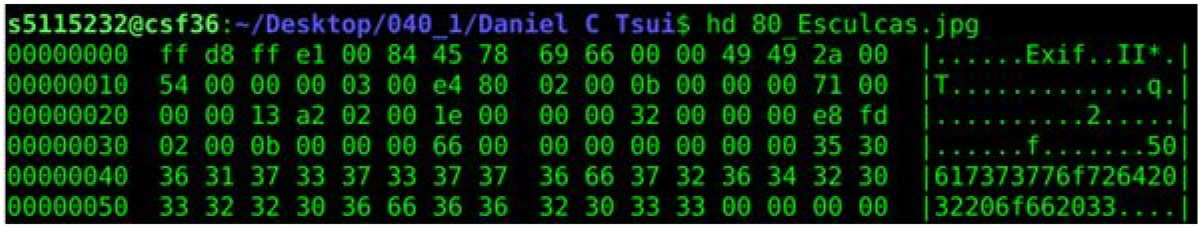


```
s5115232@csf36:~/Desktop/040_1/Nobel Laureate for Medicine in 1908/Niels Henrik
David Bohr$ exiftool 79_Estudante.png
ExifTool Version Number         : 10.40
File Name                       : 79_Estudante.png
Directory                       : .
File Size                       : 4.8 kB
File Modification Date/Time     : 2019:10:29 14:41:12+00:00
File Access Date/Time           : 2019:11:11 11:09:44+00:00
File Inode Change Date/Time     : 2019:10:30 09:59:16+00:00
File Permissions                : rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Little-endian (Intel, II)
Image History                   : V2F0Zm9yZA==
```

Figure 3: Exiftool

6.3 Hex Dump

TF hex dumped the files to examine the hex of every file looking for any appended information and data, as seen in figure 4.

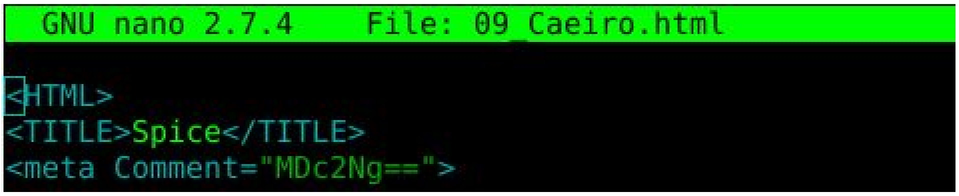


```
s5115232@csf36:~/Desktop/040_1/Daniel C Tsui$ hd 80_Esculcas.jpg
00000000  ff d8 ff e1 00 84 45 78  69 66 00 00 49 49 2a 00  |......Exif..II*.|
00000010  54 00 00 00 03 00 e4 80  02 00 0b 00 00 00 71 00  |T.............q.|
00000020  00 00 13 a2 02 00 1e 00  00 00 32 00 00 00 e8 fd  |..........2.....|
00000030  02 00 0b 00 00 00 66 00  00 00 00 00 00 00 35 30  |......f.......50|
00000040  36 31 37 33 37 33 37 37  36 66 37 32 36 34 32 30  |617373776f726420|
00000050  33 32 32 30 36 66 36 36  32 30 33 33 00 00 00 00  |32206f662033....|
```

Figure 4: Hex dump

6.4 Nano

TF used nano to open every file in a text editor to look for hidden information and data, shown in figure 5.



```
  GNU nano 2.7.4     File: 09_Caeiro.html

<HTML>
<TITLE>Spice</TITLE>
<meta Comment="MDc2Ng==">
```

Figure 5: Nano

6.5 Pictures

TF viewed every photo looking for hidden data and information encoded in braille, barcodes, QR codes hex, md5 and plaintext, figure 6, 7 and 8 shows a picture in Braille that is secretly a drone IP, a QR code that includes information for the attack port and a piece of data encoded in base 64 that was decoded to “Lsb Offset 2”. These pictures were also reversed image search to identify people or places held within.

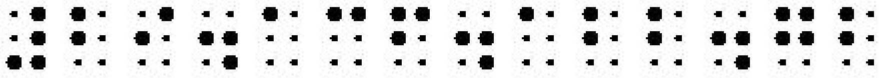
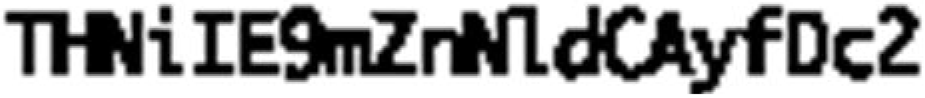


Figure 6: Braille

Figure 7: QR Code

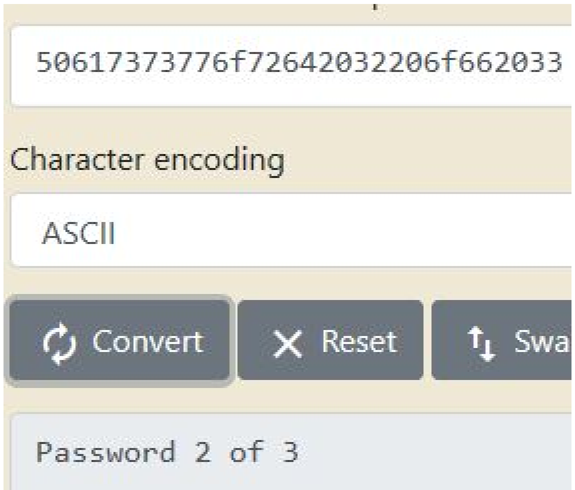


THNiIE9mZnNldCAyfDc2

Figure 8: Base 64

6.6 Decoding

TF used a hexadecimal and base 64 decoders shown in Figures 9 and 10 to decode any encoded information or data. TF retrieved 3 symmetric ciphers and 3 passwords. TF used these to decrypt an encrypted file that was recovered. The command that was used is “openssl aes-192-ecb -d -in Jarvis,Paul-David,s5115232_2.enc -out decrypt.zip | Watford”



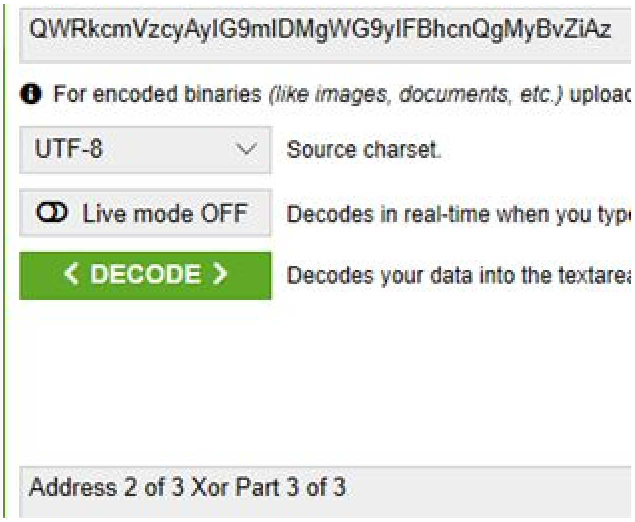
```
50617373776f72642032206f662033
```

Character encoding

ASCII

```
Password 2 of 3
```

Figure 9: Hex Decoding



QWRkcmVzcyAyIG9mIDMgWG9yIFBhcnQgMyBvZiAz

For encoded binaries *(like images, documents, etc.)* uploac

UTF-8 Source charset.

Live mode OFF Decodes in real-time when you typ

Decodes your data into the textare

Address 2 of 3 Xor Part 3 of 3

Figure 10: Base 64 Decoding

Appendices

Appendix A: Technician CV

T.F
07742106389
Bournemouth
s5115232@bournemouth.ac.uk

Education:

❏ Bournemouth University | Bachelor of Science: Forensics Computing and Security - Sept 2014 - June 2017

❏ Bournemouth University | Master of Science: Cyber Security & Human Factors - September 2017 - June 2018

Certifications:

❏ Certified Forensic Computer Examiner (CFCE) from The International Association of Computer Investigative Specialists (IACIS) - Aug 2019

Work History:

❏ Sept 2019 - Current | Technical Commercial Officer | Dorset Police

Skills:

❏ Knowledge of Linux
❏ Kali (Debian)
❏ Parrot Security (Debian)
❏ Manjaro (Arch)
❏ Knowledge of Digital Forensics & Tools
❏ Exiftool
❏ Hexdumps
❏ Autopsy
❏ COFEE
❏ EnCase
❏ FTK

Appendix B: Chain of Custody

Description of Evidence		
Item #	**Quantity**	**Description of Item**
1	1	Suspects memory stick
2	1	Encrypted File found on the suspects memory stick
3	1	A dd Image of the files found on the suspect's memory stick

Table 2: Evidence

Chain of Custody				
Item #	**Date/Time**	**Released By**	**Received By**	**Location**
2	11/11/19 - 4:55 PM	Forensics	Director of Commercial	Dorset Police Station
3	11/11/19 - 4:55 PM	Forensics	Director of Commercial	Dorset Police Station
2	11/11/19 - 5:10 PM	Director of Commercial	Head of commercial (forensics)	Dorset Police Station
3	11/11/19 - 5:10 PM	Director of Commercial	Head of commercial (forensics)	Dorset Police Station
2	11/11/19 - 5:20 PM	Head of commercial (forensics)	senior commercial manager (digital)	Dorset Police Station

3	11/11/19 - 5:20 PM	Head of commercial (forensics)	senior commercial manager (digital)	Dorset Police Station
2	11/11/19 - 5:25 PM	senior commercial manager (digital)	Technical commercial officer (TF)	Dorset Police Station
3	11/11/19 - 5:25 PM	senior commercial manager (digital)	Technical commercial officer (TF)	Dorset Police Station

Table 3: Chain of Custody

Appendix C: Chain of Analysis

Data Recovered	
Attribute	**Value**
Attack 1 of 4 Target Part 1 of 2 (Plaintext) (040_2/New York Yankees/Minnesota Twins/46_Isidoro.png)	167. (Hex: 3136372e)
Attack 1 of 4 Target Part 2 of 2 (Hex:41747461636b2031206f66203420546172676574205061727420 32 206f662032) (040_2/Chicago White Sox/Baltimore Orioles/45_Carmoto.png)	91.93.5 (Hex: 39312e39332e35)

Table 4: Recovered Data

TF found the data above in two different files and many like it. TF decoded all the encoded values using a hexadecimal to ascii text decoder. After seeing the attributes TF concluded that these two values belong together and saw that these two pieces of data were split up into two parts and putting them together produced the target for attack 1 of 4 attacks. He also saw and did the same with the two values he decoded and that produced the IP 167.91.93.5 for the target.

Appendix D: SIO and Expert Brief

Appendix D.1: CSI SIO Briefing

An individual has been arrested as a result of a lengthy serious crime investigation. A memory stick was among the personal possessions recovered during an authorised search of his home. The device has been imaged. You have been tasked with a thorough investigation of the image, and with producing a Technical Witness Statement and an Expert Witness Statement. The statements are to be produced for the SIO and CPS with a view to prosecuting the individual.

Appendix D.2: CSI SIO Expert Briefing

An individual that was arrested as a result of a lengthy serious crime investigation had in his possession a memory stick that was recovered during an authorised search of his home. The device was imaged into a dd file and an encrypted file that was also found on the memory stick. These files need to be thoroughly analysed with a range of forensics tools in order to locate any hidden data or information that the suspect attempted to hide from authorities. The individual had technical experience implying that information may not be in plain sight and rather appended to files, hidden in the meta data, placed into barcodes and encoded into a range of formats like hexadecimal and base 64.