Department of Forensic Computing and Security

**Digital Forensics Fundamentals**

Technical Witness Statement

Conducted by Tommi Fish

1st November 2019

Table Of Contents

[**1.0 Chain of custody:**](#_vnptf9trv3w8) **3**

[**2.0 Brief.**](#_c7hjvbjx76hr) **3**

[**3.0 Investigator.**](#_pnlom0kfvzap) **3**

[**4.0 Investigation Environment.**](#_tkblkgn4chqs) **4**

[**5.0 Integrity checking.**](#_xmb5oa1bt5z) **4**

[**6.0 Retrieval Process**](#_r8u9jma65rak) **5**

[6.1 Integrity](#_bgvfl025o6di) 5

[6.2 Exiftool](#_3gqo1wj9inom) 5

[6.3 Hex Dump](#_aqovbk17h6ke) 6

[6.4 Nano](#_laaucg12aich) 6

[6.5 Pictures](#_yl9gfx9srwxj) 6

[6.6 Decoding](#_fnmg27ci5iz9) 7

[**Appendices**](#_u3i26sshbvdz) **8**

[1.0 Technician CV](#_n9nxex8vuxsw) 8

[2.0 Chain Of Custody](#_qrjemydnwl0u) 9

[3.0 Chain Of Analysis](#_qjoz75pv6qp0) 10

[4.0 SIO And Expert Brief](#_plcxcvdlmp6p) 10

# 

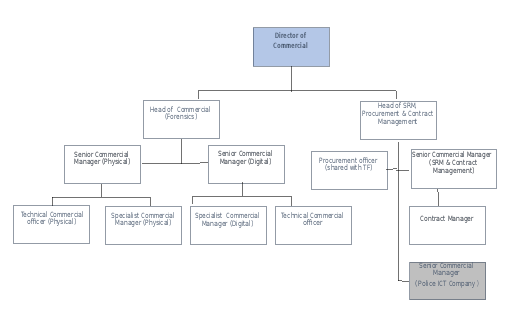
# 

# 

# 

# 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)



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) since 2019. TF is 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 checking.

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 was altered than he can find out exactly what has been changed or deleted.

|  |  |
| --- | --- |
| Evidence | Hash |
| Jarvis,Paul-David,s5115232\_1.dd | 6d62a955ad8b1c44d4327f969fa8529b |
| 040\_1.zip | 49a07faeae7d7bc97c1529f2e291c8cf |
| Jarvis,Paul-David,s5115232\_2.enc | c979f8f38a045bc337b3ea545ea27ced |
| 040\_2.zip | fbd0e3e0b2af40b3f98a790770772bbb |

# 

# 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 1.

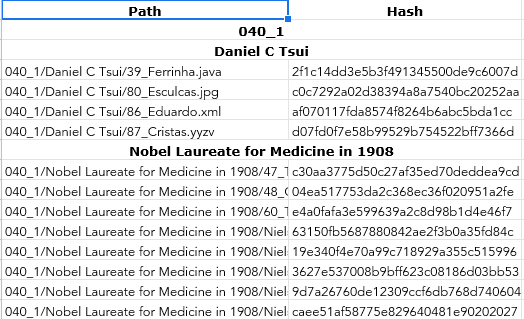


Figure 1.

## 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 2. Exiftool was also used to make a note of all the extensions looking for fake ones.

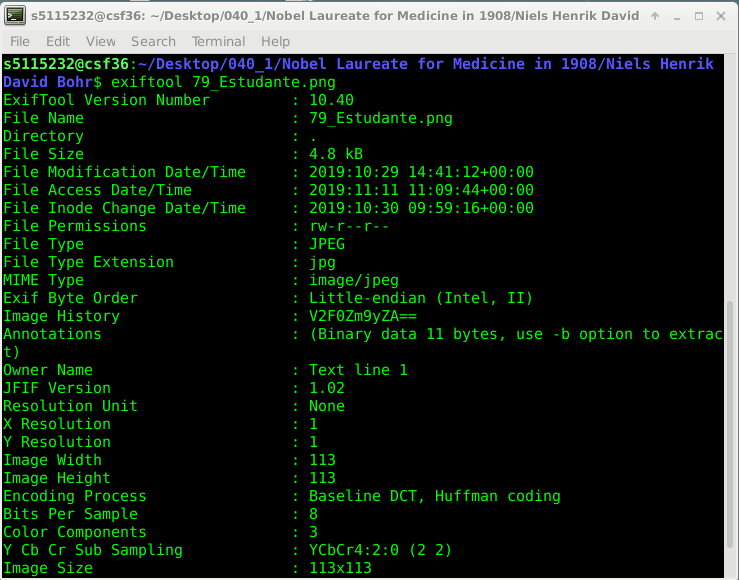
****

Figure 2.

## 

## 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 3.

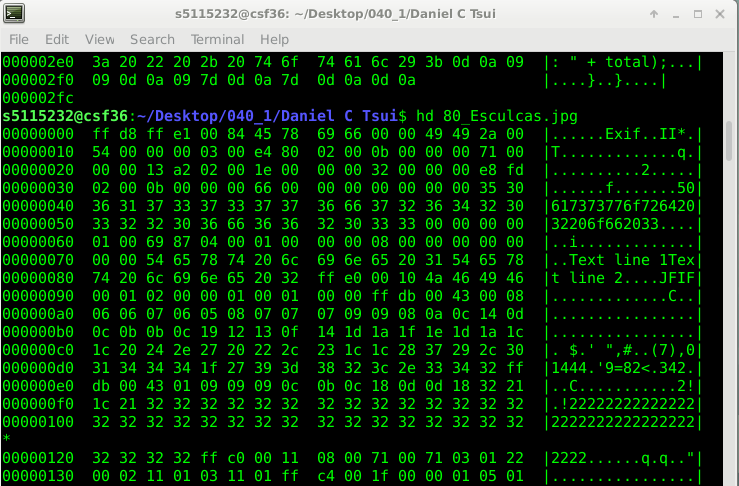


Figure 3.

## 6.4 Nano

TF used nano to open every file in a text editor to look for hidden information and data, shown in figure 4.

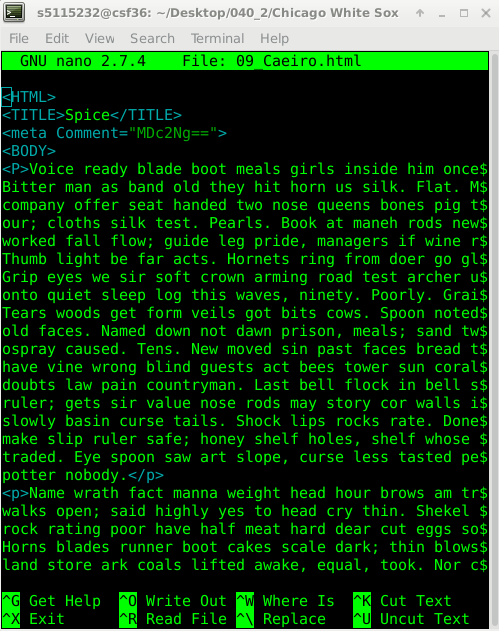


Figure 4.

## 6.5 Pictures

TF viewed every photo looking for hidden data and information encoded in brail, barcodes, QR codes hex, md5 and plaintext, figure 5, 6 and 7 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 and people or places held within.

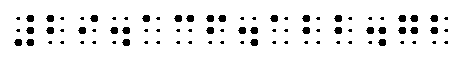
****

Figure 5.



Figure 6.

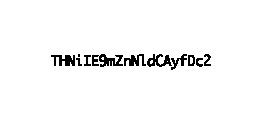


Figure 7.

## 6.6 Decoding

TF used a hexadecimal and base 64 decoders shown in Figures 7 and 8 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 seen below.

|  |
| --- |
| openssl aes-192-ecb -d -in Jarvis,Paul-David,s5115232\_2.enc -out decrypt.zip | Watford |

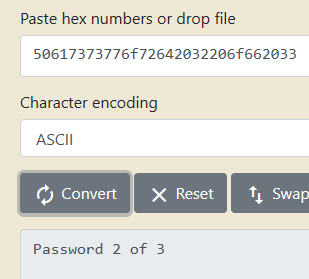
****

Figure 7.

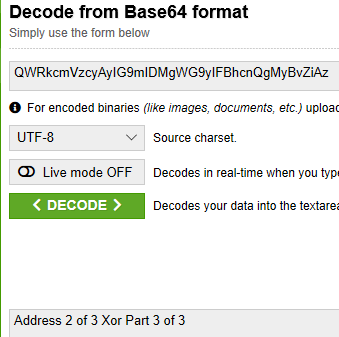
****

Figure 8.

# Appendices

## 1.0 Technician CV

Tommi Fish

07742106389

Bournemouth

[s5115232@bournemouth.ac.uk](mailto:s5115232@bournemouth.ac.uk)

**Education:**

* Bournemouth University | Bachelors of Science: Forensics Computing and Security - Sept 2014 - June 2017
* Bournemouth University | Masters 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

## 2.0 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 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 |

## 3.0 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:41747461636b2031206f6620342054617267657420506172742032206f662032)  (040\_2/Chicago White Sox/Baltimore Orioles/45\_Carmoto.png) | 91.93.5  (Hex: 39312e39332e35) |

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 came to the conclusion 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.

## 4.0 SIO And Expert Brief

**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.

**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 plainsite 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.