CMP6186 – Mobile Device Forensics

Contemporaneous Notes

Name: Umar Hussain

Student Number: 21183170

Contents

[1. Test Details 3](#_Toc163655068)

[1.1. Remit of Test 3](#_Toc163655069)

[2. Questions 3](#_Toc163655070)

# Test Details

## Remit of Test

# Questions

|  |  |
| --- | --- |
| **Question 1:**  Attribution of the mobile device to its owner. | |
| Answer | Ross Geller |
| Location of Answer | On Cellbrite, an extraction summary is presented after loading the ‘ufdr’ file into the environment. On the bottom right is a ‘content table’, in which is a ‘Device Users’ content header. The content header (screenshot 1) of ‘Device Users’ states 1 user, which can be reasonably assumed to be the owner of the device. Clicking on the header, reveals the name the mobile device is attributed to (screenshot 2 and screenshot 3) and the user type (screenshot 4) |
| Additional Notes | Screenshot 1    Screenshot 2    Screen shot 3    Screenshot 4 |

|  |  |
| --- | --- |
| **Question 2:**  Who added Ross to the conversation, in what application and when? | |
| Answer | Gunthur, Whatsapp, date: 03/09/2019, time:15:05:00(UTC+1) – 14:05:00 |
| Location of Answer | Within the content table, there is a content header called ‘Chat’ (screenshot 1). Clicking this, all 28 chats are presented in table format, where the user is present (screenshot 2), across platforms that include their phone number. From the ‘Participants’ section of the table, we can associate numbers used with names, and derive the number of ‘Ross’, the device owner (screenshot 3). Where participants are more than 2, indicates a group (screenshot 4). This shows all participants on this whatsapp group, and pairing this with the chat window (screenshot 5) it can be derived that ‘Gunthur’ created the group, naming it big bears, and then added ‘Ross’ at ‘15:05:00(UTC+1)’ on ‘03/09/2019’ |
| Additional Notes | Screenshot 1  Screenshot 2    Screenshot 3    Screenshot 4    Screenshot 5 |

|  |  |
| --- | --- |
| **Question 3:**  Who else is in this conversation? | |
| Answer | Janice, Phoebe Buffay, Gunthur, Rachael Green, Monica Geller, David, Joey Tribbiani and Chandler Bing |
| Location of Answer | The chats are presented on a table, in which is a column called ‘Participants’. We can see the numbers in the conversation named ‘Big Bears’ and the associated name (screenshot 1) |
| Additional Notes | Screenshot 1  All names are full names apart from David. Another chat with Rachael Green mentions ‘Minsk David’ which can be inferred as Davids full name: |

|  |  |
| --- | --- |
| **Question 4:**  What is the conversation called and when was it first created? | |
| Answer | Big Bear, 03/09/2019 15:05:00(UTC +1) – 14:05:00 |
| Location of Answer | In the chat window, presenting the messages sent, the name is presented as being set when the chat was established (screenshot 1). The established time is presented through the ‘Start Time’ column in the chats table (screenshot 2), and both times and dates are the same. |
| Additional Notes | Screenshot 1    Screenshot 2 |

|  |  |
| --- | --- |
| **Question 5:**  What time was the first image shared in the group and who sent it? | |
| Answer | 15:09:46(UTC+1) – 14:09:46, Gunthur sent it |
| Location of Answer | In the chat window, the chats can be traversed in the order they were sent and stored on whatsapp. Here, the first image sent can be seen (screenshot 1) with its ‘jpeg’ extension. Additionally, under the message we can view the sources associated with the message (screenshot 2) |
| Additional Notes | Screenshot 1  Screenshot 2 |

|  |  |
| --- | --- |
| **Question 6:**  To whom was the message sent to betray the group? | |
| Answer | Janice Litman-Goralnik |
| Location of Answer | Through the file path - \USERDATA(ExtX)\Root\data\com.google.android.gm\databases\EmailProvider.db. This will present emails between ‘Ross’ and ‘Janice’ where the messages potray their intention to betray the group and sell the ‘Porche Patent’ |
| Additional Notes | Screenshot 1  Sreenshot 2 |

|  |  |
| --- | --- |
| **Question 7:**  What application was used to search for information on ‘Vitality Blast’? | |
| Answer | Android Browser |
| Location of Answer | In the table of content, click on the ‘Web History’ content header. This will direct to the web history of the user. Here we see a table presenting this information, ‘Title’ and ‘URL’ being important. Here, the search containing ‘Vitality Blast’ can be found (screenshot 1). In the ‘Web History’ window on the right, we can see the souce of this search (screenshot 2) |
| Additional Notes | Screenshot 1    Screenshot 2  Screenshot 3 is the viewing of the source file, following this source file - \USERDATA (ExtX)\Root\data\com.sec.android.app.sbrowser\app\_sbrowser\Default\History - where the source is stated as ’android home’ |

|  |  |
| --- | --- |
| **Question 8:**  What time was the search for Amsterdam? | |
| Answer | 19:46:37 (UTC+1) – 18:46:47 |
| Location of Answer | From the file ‘History’ through the path - \USERDATA (ExtX)\Root\data\com.sec.android.app.sbrowser\app\_sbrowser\Default\History - (screenshot 1) suggests the search ‘amsterdam’ is connected to ‘lastminute.com’. Through ‘autposy’ -> ‘data artifacts’ -> ‘web history’ we find the search ‘amsterdam’ (screenshot 2) at time 19:46.37 BST. |
| Additional Notes | Screenshot 1  Screenshot 2 |

|  |  |
| --- | --- |
| **Question 9:**  With what password did Ross log in to the website? | |
| Answer | CentralPerk1994 |
| Location of Answer | Through traversing through the file system along this path - \USERDATA (ExtX)\Root\data\com.sec.android.app.sbrowser\app\_sbrowser\Default\Login Data – we can see ross the credentials used to logged into ‘www.lastminute.com’ (screenshot 1). Through Autopsy, the website and email can be verified (screenshot 2) |
| Additional Notes | Screenshot 1    Screenshot 2 |

|  |  |
| --- | --- |
| **Question 10:**  What is the name on the credit card used to purchase flight tickets? | |
| Answer | Rosstopher Geller |
| Location of Answer | Through the file path - \USERDATA (ExtX)\Root\data\com.sec.android.app.sbrowser\app\_sbrowser\Default\Web Data |
| Additional Notes |  |

|  |  |
| --- | --- |
| **Question 11:**  What date\time is the flight booked to leave? | |
| Answer | 06/09/2019 04:45:00 |
| Location of Answer | Through the file path - \USERDATA (ExtX)\Root\media\0\Download\Flight Confirmed.txt - the fllight details are listed (screenshot 1) |
| Additional Notes | Screenshot 1 |

|  |  |
| --- | --- |
| **Question 12:**  Is there any evidence the user planned any further criminal activity? | |
| Answer | Yes – the user planned to clone ‘Janice’s’ card, taking all her money. He plans to use her name to sneak onto a plane. |
| Location of Answer | Within the ‘notes’ application on the users phone (screenshot 1) where it can be viewed through - \USERDATA (ExtX)\Root\data\com.samsung.android.app.notes\personal\_notes.json. |
| Additional Notes |  |