**ITIS 4250/5250**

**Pooja Haridasyam**

**Lab #4**

**Overview:**

Detective Lansbury provided me with a database from a Chat App that was extracted by a lab technician using UNCC's Mobile Electronics Technical Analysis Lab. Unfortunately, the technician was unable to analyze the database using METAL. As a result, I was tasked with identifying the individuals Rett has been communicating with and the topics they have been discussing.

**Forensic Acquisition & Exam Preparation:**

To carry out the examination, a Dell Latitude 3510 with 16 GB of RAM that operates on Windows 10 Home was utilized. The tool used for the analysis was DB Browser SQLite 3.12.2. Specifically, the database file named "ChattyMcChatFaceChats.db" was opened using this software for the purpose of inspection. After a comprehensive evaluation, I responded to all of Detective Lansbury's inquiries.

**Findings and Report (Forensic Analysis):**

1. What was the date of contact for the user who replied “Nu phone who dis”?

On the 9th of May 2020, GMT, contact was made with a user who replied with the message "Nu phone who dis". By clicking on "Browse Data" and selecting the "Zmsgs table", the conversations can be seen. The epoch date was converted into a format that can be read by humans using epochconverter.com.

Graphical user interface, text, application

Description automatically generated

*Fig: Zmsgs table with the message and epoch date*

Graphical user interface, text, application

Description automatically generated

*Fig: Converting the Epoch date to human-readable format*

1. Which users (by their email address) were involved in that conversation?

The conversation involved two users, namely Rett Harring and Kamoze, whose email addresses are rett.harring@outlook.com and kamoze@chattymail.com, respectively. By examining the Zmsgs table, the conversation with thread\_ID 3 was identified. The participants in the conversation were determined by analyzing the recip and auth columns in the Zmsgs table, which indicated that the conversation was between user IDs 0 and 5. According to the ZContacts table, the user with ID 5 corresponds to Kamoze.

Graphical user interface, text, application

Description automatically generated

*Fig: Zmsgs table with conversation with thread\_id 3*

Graphical user interface, text, application, email

Description automatically generated

*Fig: zConatcts table with recip\_id-5 shows Kamoze*

Graphical user interface, text, application

Description automatically generated

*Fig: zConstants table with Rett details*

1. What does Ms. Loeb look like?

In the zContacts table, I came across a picture of Lisa Loeb with Contact\_ID-1. The image depicts her wearing glasses. Her complete name is Lisa Loeb. By selecting the Cavatar BLOB with contact\_id-1 in the same table, an image is displayed in the Edit database cell on the right-hand side.

Graphical user interface, text

Description automatically generated

*Fig: zContacts table with Cavatar BLOB of Ms.Loeb*

Graphical user interface, text, application

Description automatically generated

*Fig: Image of Ms. Loeb*

1. What is the item that appears to have been stolen and when was the message sent?

By analyzing the conversation, I was able to identify the stolen item, which is a pair of jars, as shown in the image below. One of the messages in the conversation included a jpeg image file represented by a message starting with "FFD8". I converted the hexadecimal code to binary format using an online converter, and was able to retrieve the image.

Graphical user interface, text, application, email

Description automatically generated

*Fig: Zmsgs table- Hexadecimal message found with thread\_id-6*

Graphical user interface

Description automatically generated

I used an online converter to change the epoch date into a format that can be easily understood by people. The conversation occurred specifically on May 20th, 2020.

Graphical user interface, text, application

Description automatically generated

*Fig: Epoch date to human-readable format*

1. Who has Rett sent messages most often (tell me their email)?

Rett utilized the email addresses OneZeroZeroPct@chattymail.com and TwoShoes@chattymail.com to send the majority of their messages to Waters and Goddard, respectively. The Zmsgs table indicates that most of Rett's conversations are linked to thread\_id- 6 and 7. By examining the recip and auth id's of the messages, I discovered that these correspond to id's 3 and 4. Lastly, in the zConatcts table, the rows that correspond to id's 3 and 4 are associated with Waters and Goddard.

Table

Description automatically generated

*Fig: Zmsgs table - often sent messages with thread\_id- 6,7*

Table, calendar

Description automatically generated

*Fig: zContacts table- people to whom Rett has sent messages most often*

1. Bonus: Can you tell me what the text was in the secret message?

I have discovered a hidden message within the Zmsgs table with thread\_ID-7. I copied the encoded message in base 64 format and used an online base64 decoder to reveal the content. The resulting message is presented below.

**I have found a way to make the drugs undetectable by the dogs at the checkpoint. It’s my own special mix of sage, rosemary, thyme, vaporub and Carolina reaper oil!**

Graphical user interface, text, application, email

Description automatically generated

*Fig: Base64 encoded message in Zmsgs table*

Graphical user interface, text, application, email

Description automatically generated

*Fig: Decoding message using online base64 decoder.*

**Conclusion:**

After conducting an analysis, I discovered that Rett had been engaging in conversations with various individuals, with the most frequent communication being with Waters and Goddard. From the discussions, I was able to determine the stolen item, as well as information on how to make the drugs untraceable. Through a comprehensive investigation, I was able to provide answers to the questions posed by Det. Lansbury.