ITIS 4250 / 5250

Shivani Sathe

Lab # 4

24th October 2021

**Overview:**

On 24th October 2021, Detective Angela Lansbury, acting director of the UNCC forensics lab, provided me a ChatApp database extracted by one of the lab technicians with UNCC’s SIS created Mobile Electronics Technical Analysis Lab. I was asked to analyze the database and find who Rett has been talking to and what he’s been talking about.

For reference, Rett Harring is one of North Carolina’s best-known villains also known as

the “goon for hire”. Rett is known to work for several different super villains, including Malcom Monarch and Gene Poole. Occasionally Rett has been known to engage in petty thievery to earn a living in between acting as a minion.

**Forensic Acquisition & Exam Preparation**

To begin the analysis, Windows 10, 64-bit system was used, and the ChatApp Database was loaded in DB Browser for SQLite.

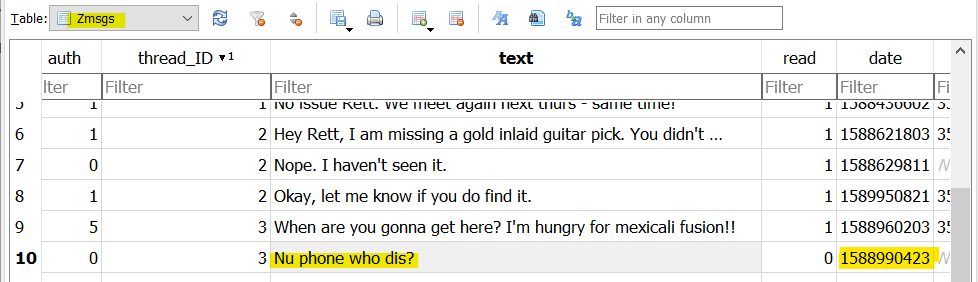
**Findings and Report (Forensic Analysis)**

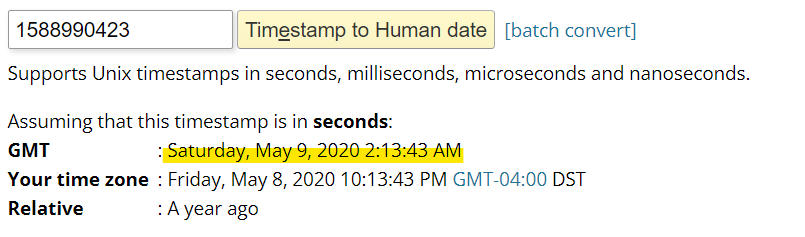
1. What was the date of contact for the user who replied “Nu phone who dis”.

The contact date can be found by selecting the table ‘Zmsgs’ under Browse Data tab. To

convert below highlighted epoch date, epochconverter.com site was used. Contact Date

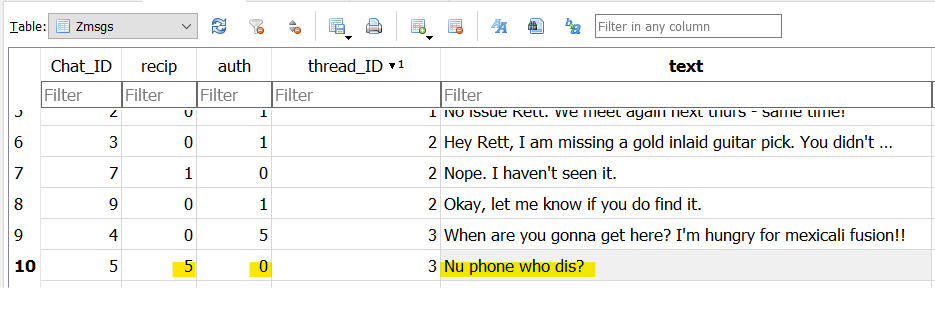
was - Saturday, May 9, 2020 2:13:43 AM.

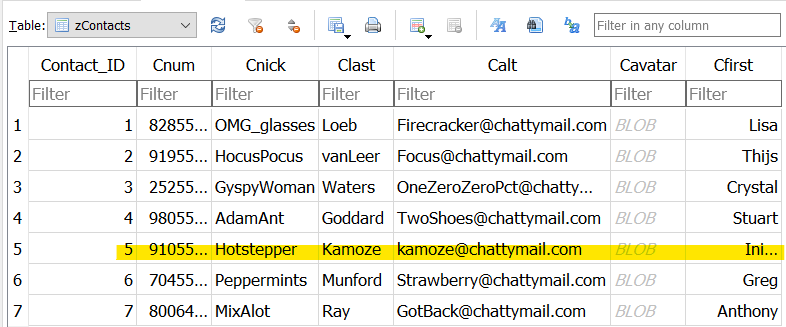




1. Which users (by their email address) were involved in that conversation?

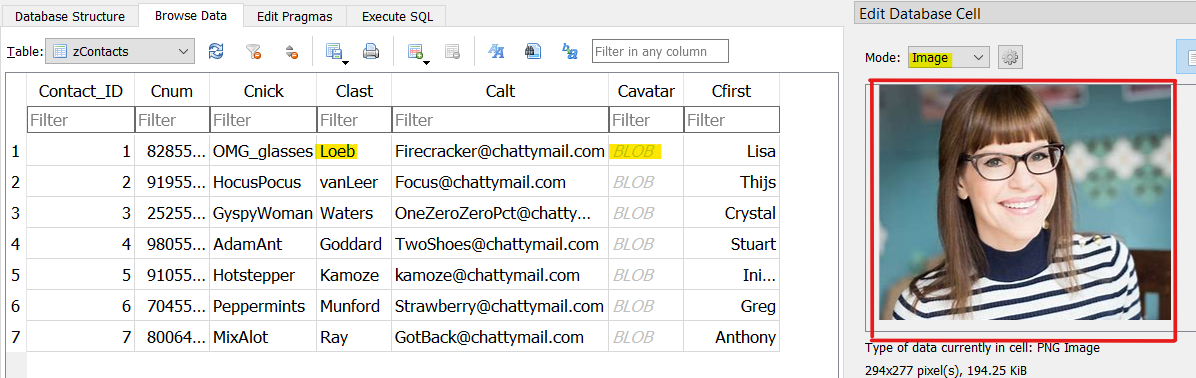
From the ‘Zmsgs’ table under Browse Data tab, the recipient id is 5 and author id is 0. Id 0 belongs to Rett Harring. Using ‘zContacts’ table under Browse Data tab, it was found that id 5 belongs to Kamoze. The users involved in the conversation were [kamoze@chattymail.com](mailto:kamoze@chattymail.com) and [rett.harring@outlook.com](mailto:rett.harring@outlook.com).





1. What does Ms. Loeb look like?

From the ‘zContacts’ table under Browse Data, when clicked on Cavatar cell for Loeb and selecting mode of database cell as Image, the image was found.

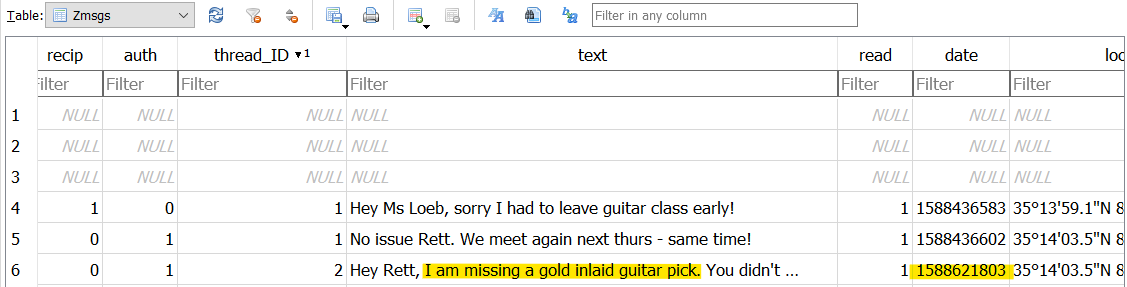


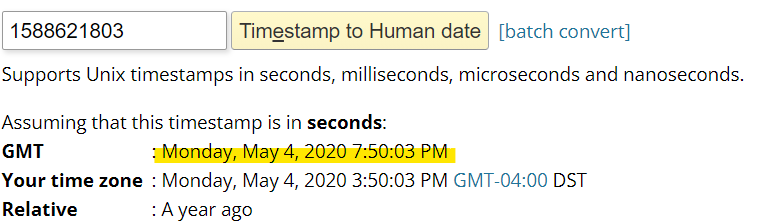
1. What is the item that appears to have been stolen and when was the message sent?

From Zmsgs table, looking at the conversation threads, Gold inlaid guitar pick appears to

have been stolen. Using epochconverter.com the message was sent on Monday, May 4,

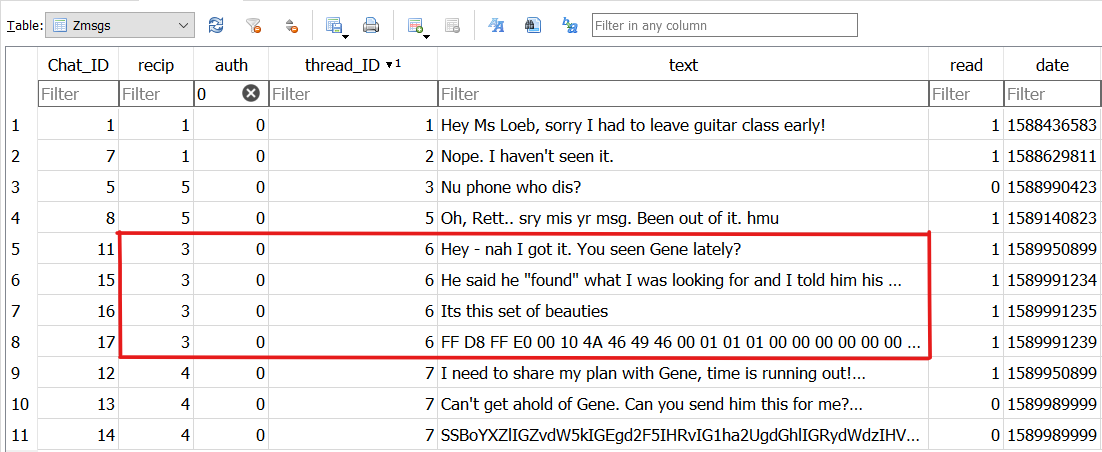
2020 7:50:03 PM.

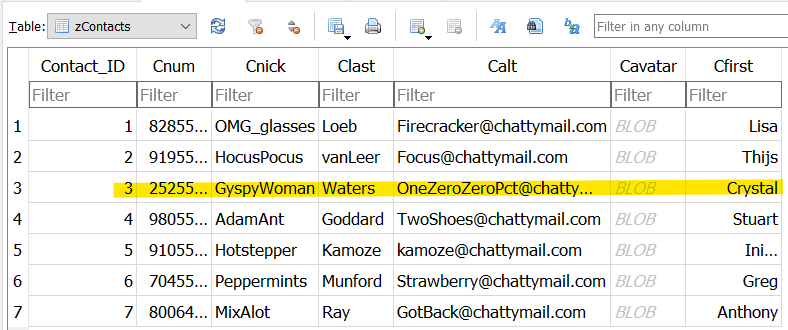




1. Who has Rett sent messages to most often (tell me their email)?

In the ‘Zmsgs’ table, filter 0 was applied under ‘auth’ column to see all messages sent from Rett. As per the message threads, Rett has messaged receipt ID 3 most often. Using ‘zContacts’ table, ID 3 belongs to Crystal whose mail id is OneZeroZeroPct@chattymail.com.





**Conclusion:**

Overall, in this lab I was asked to analyze the ChatApp database and determine who Rett has been talking to and what he’s been talking about. The database was extracted with UNCC’s SIS

created Mobile Electronics Technical Analysis Lab. To begin the analysis, the chat database was loaded in DB Browser for SQLite on a Windows 10 Machine. All the questions regarding this case were successfully answered with the help of DB Browser for SQLite. No evidence has been retained. The ChatApp database and answered questions regarding it, were returned to Detective Lansbury.