Autopsy 4.10.0 - Evidence Consolidation with File Tags

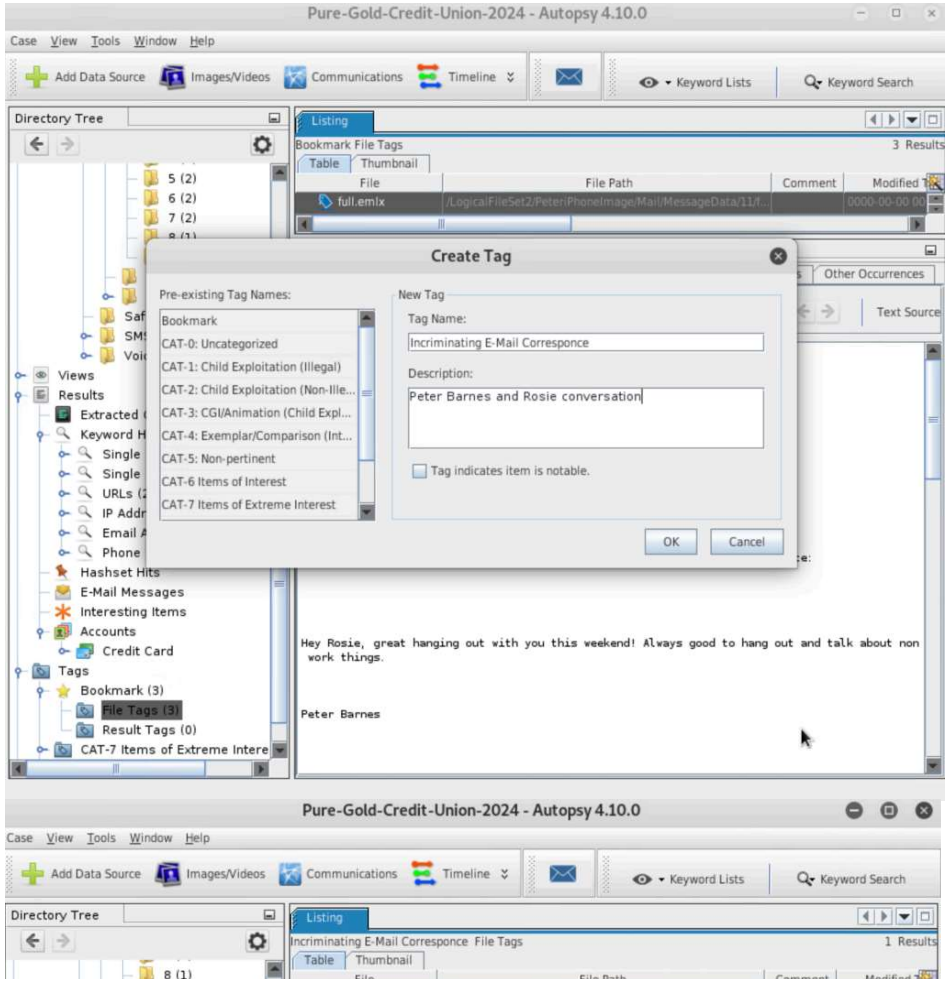
Wednesday, November 20, 2024 8:14 PM

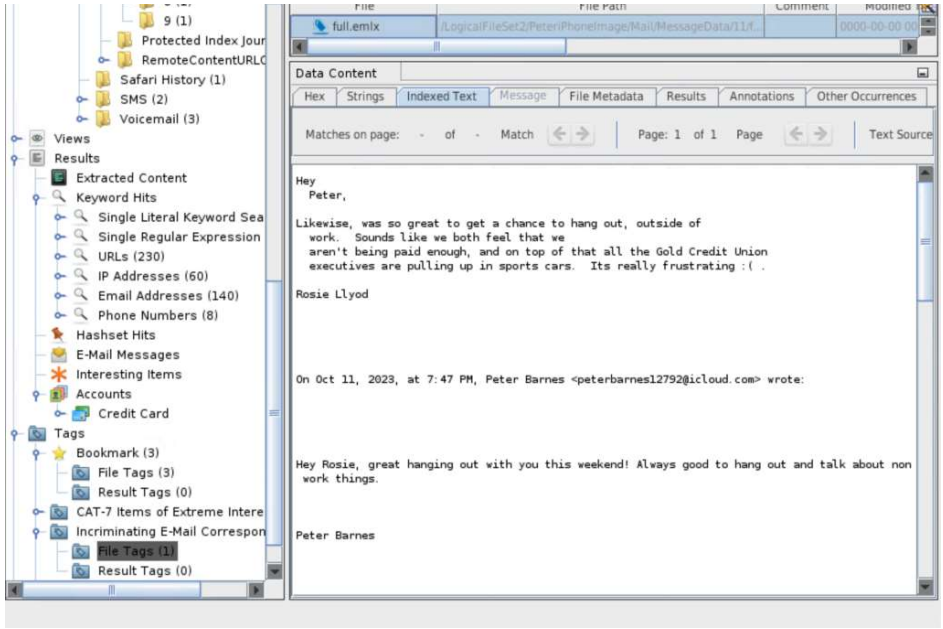
In this activity, you will continue your role as a digital forensics investigator working on the Pure Gold CU case.

- As part of your daily routine, you regularly tag all evidence that you consider critical to the investigation.
- To help speed up your workflow, you will use default and custom tags to categorize and organize all files and folders.
- This will allow other team members to sort through large amounts of data quickly and prevent double work.

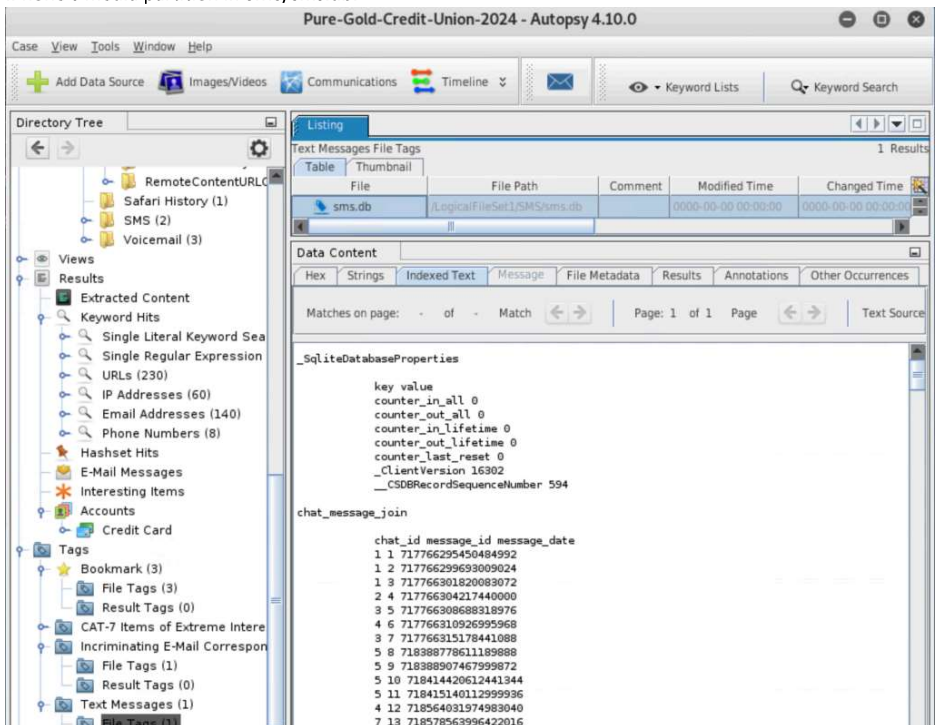
Evidence I bookmarked that I found to be of importance are as followed.

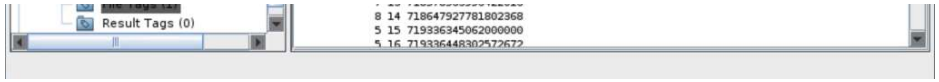
1. E-Mail correspondence showing incriminating evidence.



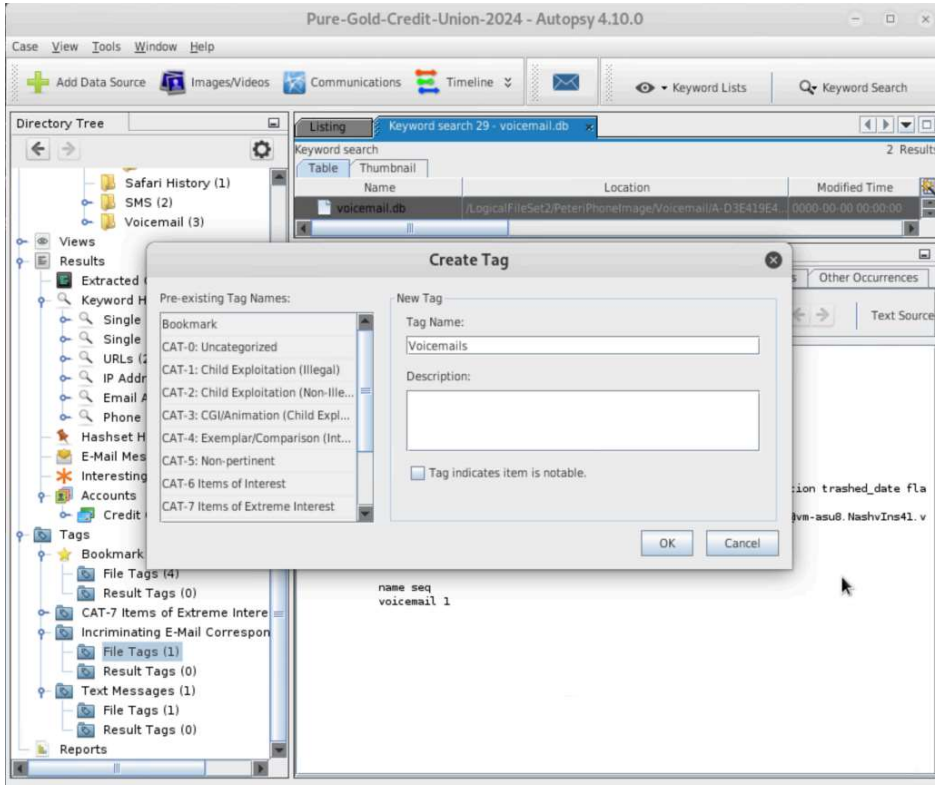


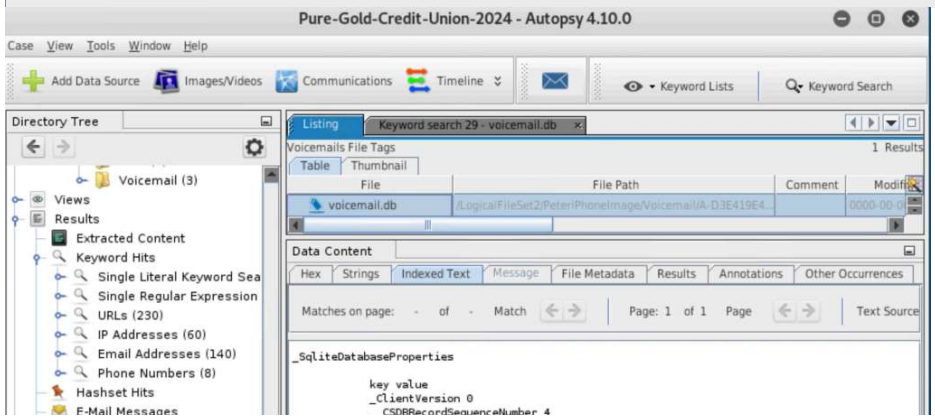
2. Text Message Correspondence - The SMS message database contains information about SMS messages sent and received on the device. This includes the phone number of the remote party, timestamp, actual text, and various carrier information. The file can be found on the iPhone's media partition in SMS/sms.db.

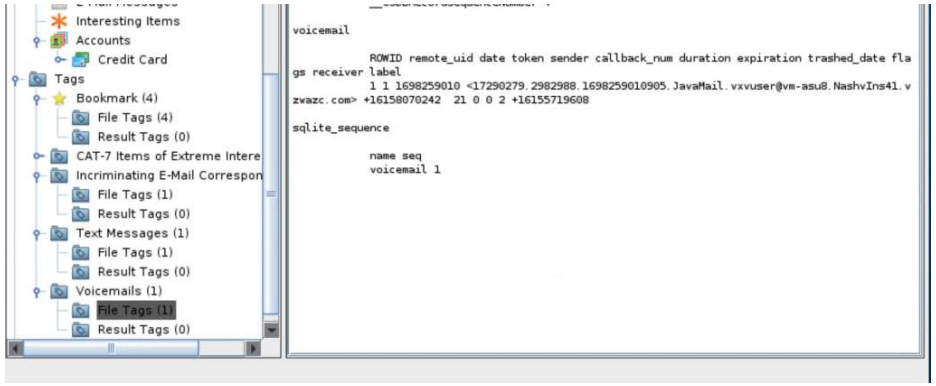




3. Voicemails- The voicemail database contains information about each voicemail stored on the device and includes the sender's phone number and callback number, timestamp, the message duration, the expiration date of the message, and the timestamp (if any) denoting when the message was moved to the trash. The voicemail database is located in Voicemail/voicemail.db, while the voicemail recordings themselves are stored as AMR codec audio files in the directory Voicemail/.

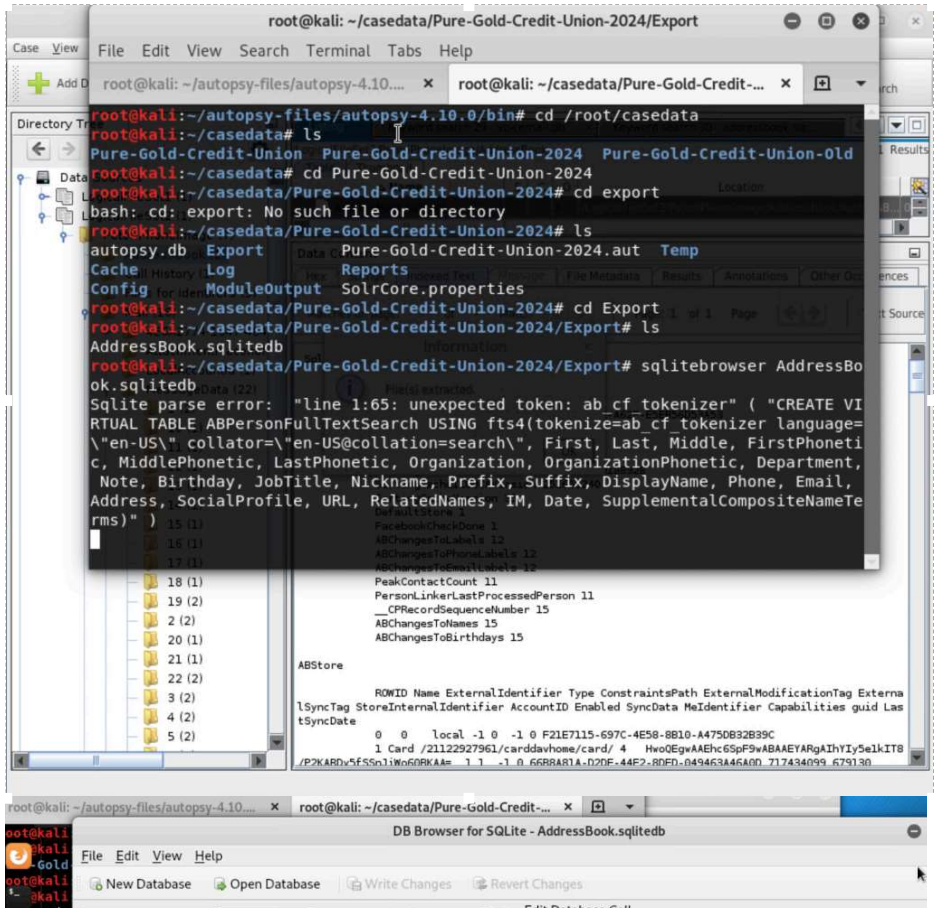


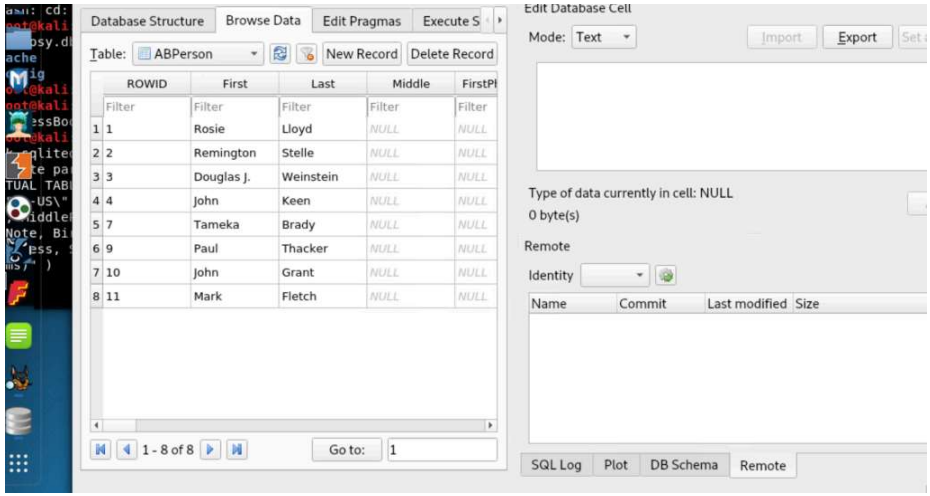




4. Address Book- The address book contains individual contact entries for all of the contacts stored on the iPhone. The address book database can be found at AddressBook/AddressBook.sqlitedb. The following tables are primarily used:

-ABPerson to filter results into cohesive results. This shows information like: Name, Organization, Department, and other general information about each individual contact.




Database Structure
Browse Data
Edit Pragmas
Execute S
Table: ABPerson
New Record
Delete Record
ROWID
First
Last
Middle
FirstPl
Filter
1 1 Rosie Lloyd NULL NULL
2 2 Remington Stelle NULL NULL
3 3 Douglas J. Weinstein NULL NULL
4 4 John Keen NULL NULL
5 7 Tameka Brady NULL NULL
6 9 Paul Thacker NULL NULL
7 10 John Grant NULL NULL
8 11 Mark Fletch NULL NULL
1 - 8 of 8
Go to: 1
Edit Database Cell
Mode: Text
Import
Export
Type of data currently in cell: NULL
0 byte(s)
Remote
Identity
Name
Commit
Last modified
Size
SQL Log
Plot
DB Schema
Remote