

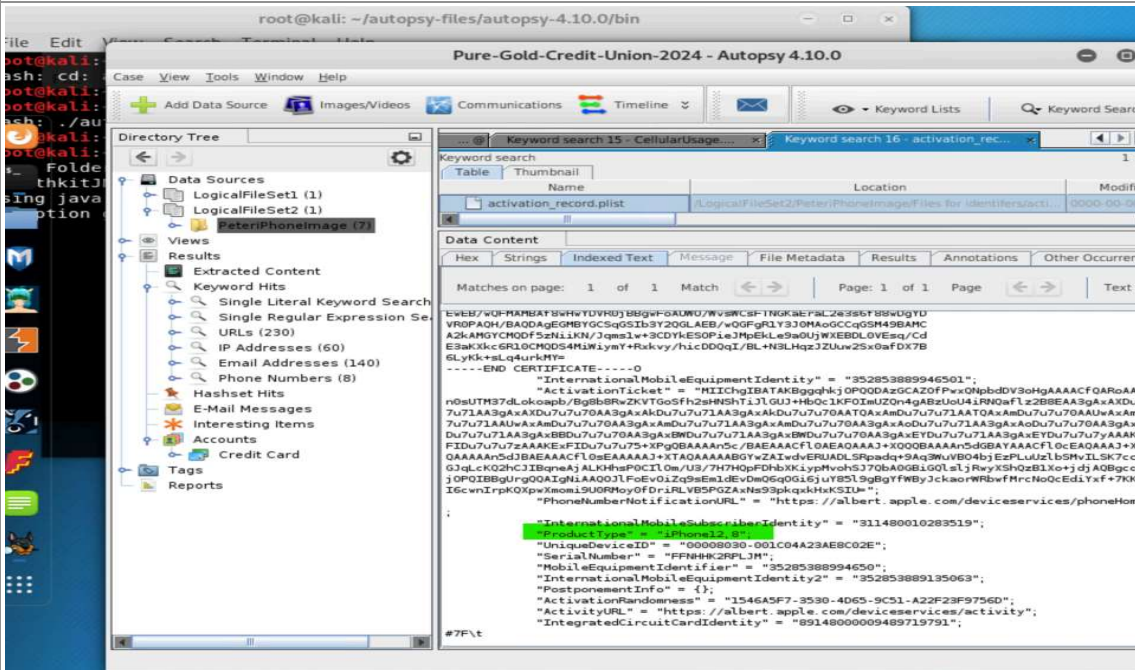
# Autopsy 4.10.0 - iPhone Mobile Evidence Analysis

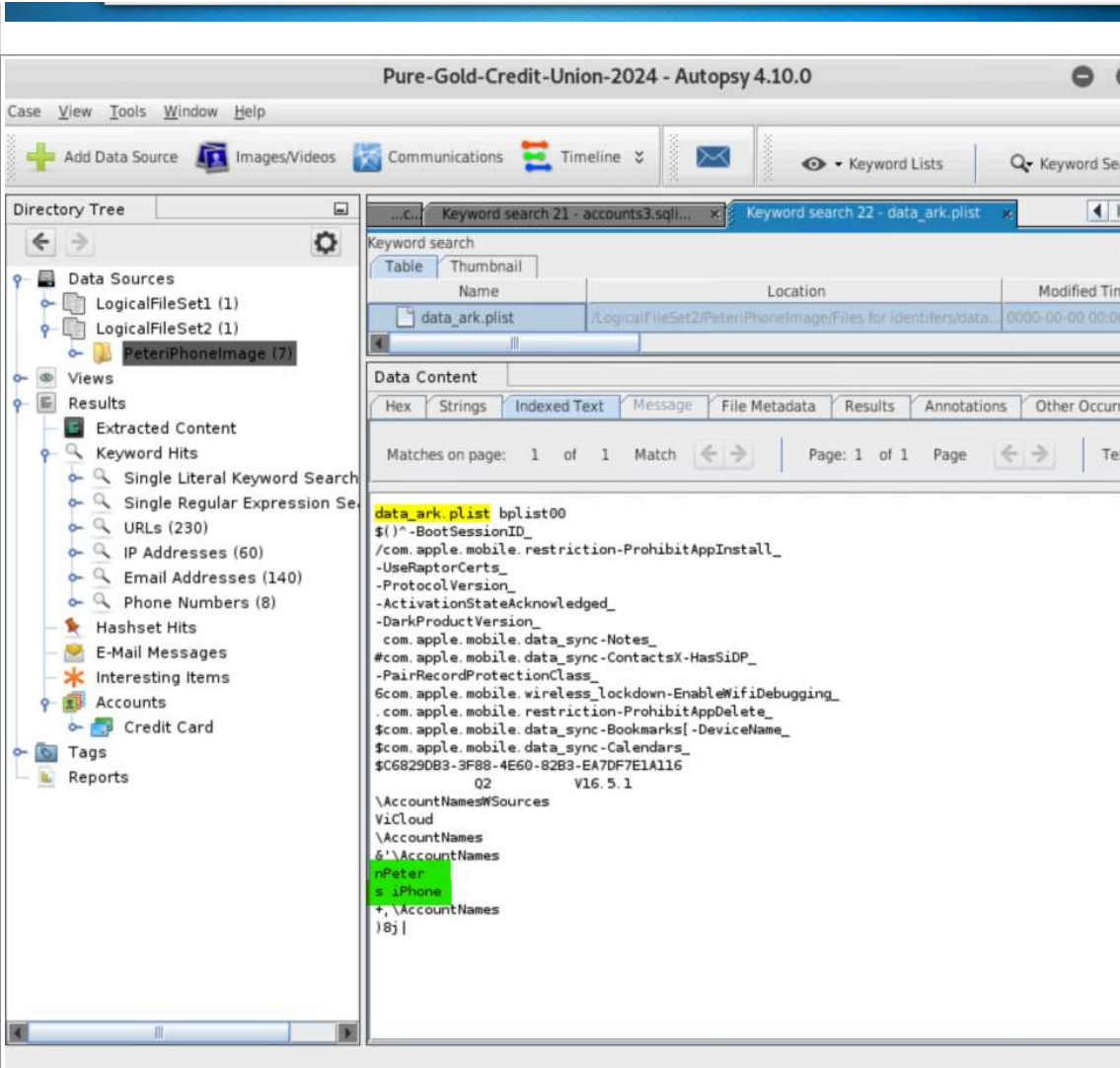
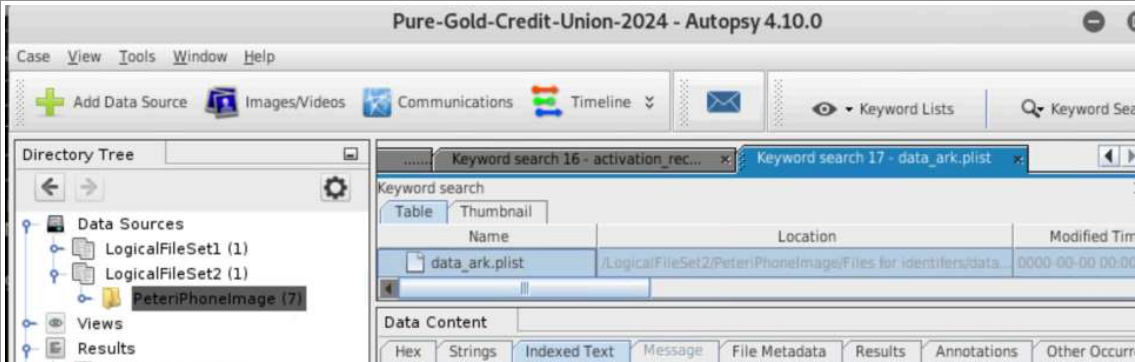
Wednesday, November 20, 2024 7:01 PM

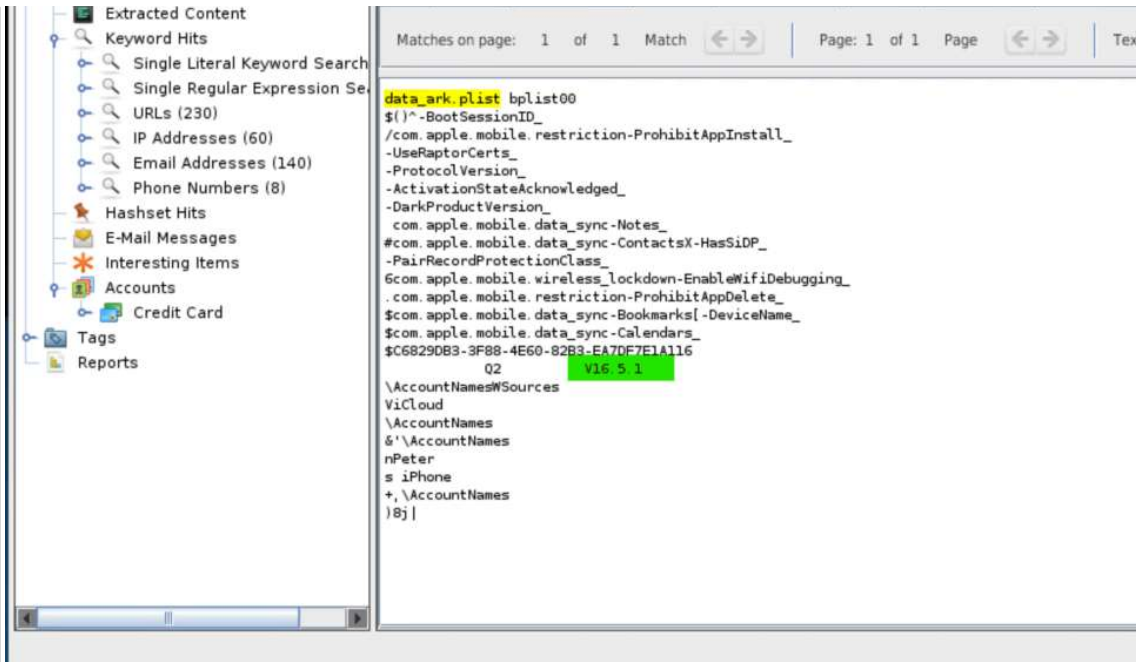
## Activity File: Mobile Evidence Analysis

- In this activity, you will play the role of a digital forensics investigator.
- You are tasked with analyzing evidence and creating a spreadsheet that profiles the details of Peter's iPhone.
- This will serve as your preliminary documentation for the remaining activities.
- To complete this task, you will need to use Autopsy's File Search by Attributes and Keyword Search functions.

## Details of Peter's iPhone

Name	Findings	Location/File in iPhone image file	Screenshot Findings
Model	iPhone 12, 8	activation_record.plist	

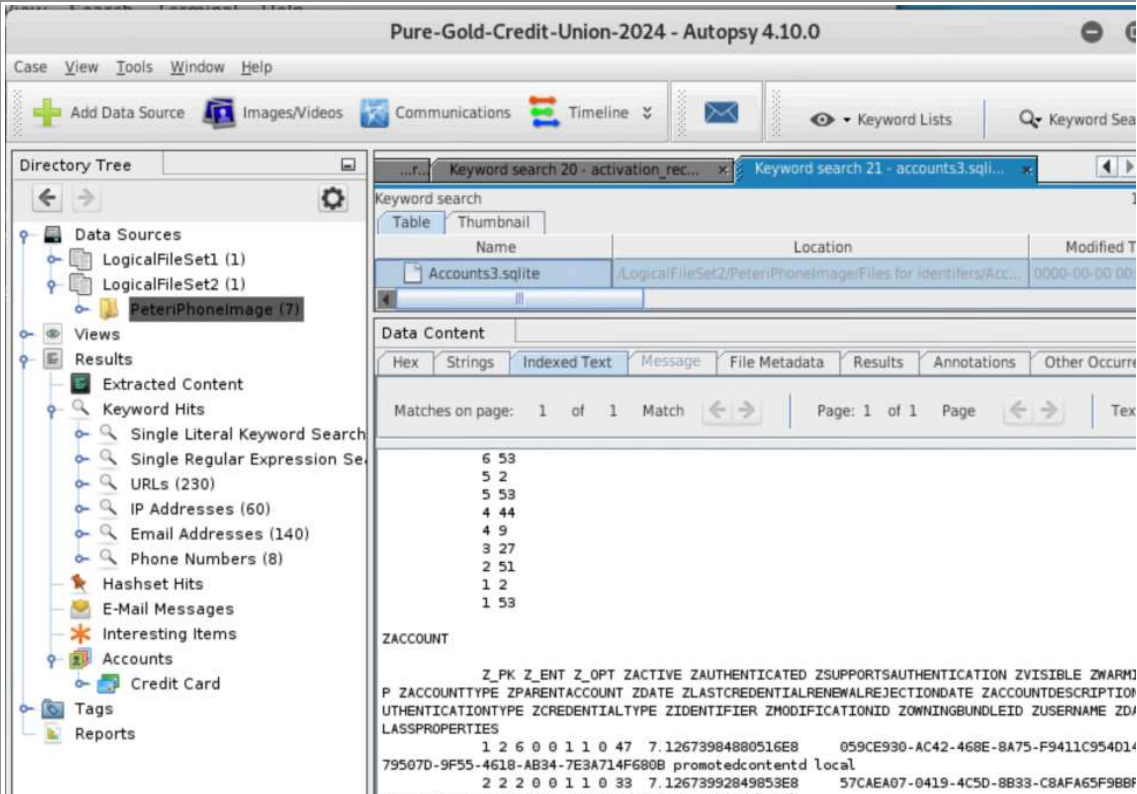
Host Name	Peters iPhone	data_ark.plist	 <p>The screenshot shows the Autopsy 4.10.0 interface. The 'Directory Tree' on the left highlights 'PeteriPhoneImage (7)'. The 'Keyword search' panel on the right shows a search for 'data_ark.plist' in the 'Indexed Text' view. The search results display the following content:</p> <pre>data_ark.plist bplist00 \$()^ -BootSessionID_ /com.apple.mobile.restriction-ProhibitAppInstall_ -UseRaptorCerts_ -ProtocolVersion_ -ActivationStateAcknowledged_ -DarkProductVersion_ com.apple.mobile.data_sync-Notes_ #com.apple.mobile.data_sync-ContactsX-HasSiDP_ -PairRecordProtectionClass_ 6com.apple.mobile.wireless_lockdown-EnableWifiDebugging_ .com.apple.mobile.restriction-ProhibitAppDelete_ \$com.apple.mobile.data_sync-Bookmarks -DeviceName_ \$com.apple.mobile.data_sync-Calendars_ \$C68290B3-3F88-4E60-82B3-EA7DF7E1A116 Q2 V16.5.1 \AccountNames\WSources ViCloud \AccountNames &amp;'\AccountNames nPeter s iPhone +,\AccountNames  8j </pre>
OS Version	16.5.1	data-ark.plist	 <p>The screenshot shows the Autopsy 4.10.0 interface. The 'Directory Tree' on the left highlights 'PeteriPhoneImage (7)'. The 'Keyword search' panel on the right shows a search for 'data-ark.plist' in the 'Indexed Text' view. The search results display the following content:</p> <pre>data-ark.plist bplist00 \$()^ -BootSessionID_ /com.apple.mobile.restriction-ProhibitAppInstall_ -UseRaptorCerts_ -ProtocolVersion_ -ActivationStateAcknowledged_ -DarkProductVersion_ com.apple.mobile.data_sync-Notes_ #com.apple.mobile.data_sync-ContactsX-HasSiDP_ -PairRecordProtectionClass_ 6com.apple.mobile.wireless_lockdown-EnableWifiDebugging_ .com.apple.mobile.restriction-ProhibitAppDelete_ \$com.apple.mobile.data_sync-Bookmarks -DeviceName_ \$com.apple.mobile.data_sync-Calendars_ \$C68290B3-3F88-4E60-82B3-EA7DF7E1A116 Q2 V16.5.1 \AccountNames\WSources ViCloud \AccountNames &amp;'\AccountNames nPeter s iPhone +,\AccountNames  8j </pre>



User Email

[peterbarnes12792@icloud.com](mailto:peterbarnes12792@icloud.com)

accounts3.sqlite



```
A317EB-C7B8-41D5-B04E-E0E35845A55B storekitd local
3 2 51 1 1 0 1 0 29 7.17433986180657E8 FB6A58FF-4B3D-4E21-BA4B-5578BC5527F
C004630-4ACD-48BA-A98C-C57AFA1E5CB4 com.apple.AuthKit peterbarnes12792@icloud.com
4 2 9 1 1 1 1 0 21 7.17433986246615E8 ACFDE5CB-6883-41F9-B349-74AC185585D0E
43F201-7079-4351-976C-F69A72D28DCF com.apple.AuthKit peterbarnes12792@icloud.com
5 2 35 1 1 1 1 0 6 7.17433988760136E8 3CB76625-F1E2-4500-9258-F273C6B1230X
797880-003F-426F-9B69-47112E514A72 com.apple.purplebuddy peterbarnes12792@icloud.com
6 2 8 1 1 1 1 27 7.17433988830666E8 8E148275-FC70-49AE-AFFF-E2750CA9515A
E7D0BB-4480-4775-9CF4-60AA033DC149 com.apple.accounts.accountsd peterbarnes12792@icloud.com
7 2 28 1 1 1 1 0 1 7.174339888308E8 iCloud A03F4501-0255-44BA-B1EA-F25E449E
0 3AD20059-BE77-49BA-8ED3-FC32C9DDC249 com.apple.purplebuddy peterbarnes12792@icloud.com
```

Phone  
Number

+1 (615) 551-9608

CellularUsage.db

Pure-Gold-Credit-Union-2024 - Autopsy 4.10.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Timeline Keyword Lists Keyword Search

Directory Tree

- Data Sources
  - LogicalFileSet1 (1)
  - LogicalFileSet2 (1)
  - PeteriPhoneImage (7)
- Views
  - Results
    - Extracted Content
      - Keyword Hits
        - Single Literal Keyword Search
        - Single Regular Expression Search
        - URLs (230)
        - IP Addresses (60)
        - Email Addresses (140)
        - Phone Numbers (8)
      - Hashset Hits
      - E-Mail Messages
      - Interesting Items
      - Accounts
        - Credit Card
      - Tags
      - Reports

Keyword search 15 - CellularUsage.db

Name	Location	Modified
CellularUsage.db	/LogicalFileSet2/PeteriPhoneImage/Files for identifiers/Cell...	0000-00-00

Data Content

Hex Strings Indexed Text Message File Metadata Results Annotations Other Occurrences

Matches on page: 1 of 1 Match Page: 1 of 1 Page

```
1 com.apple.ActivityMonitorApp 48
2 com.apple.NanoBooks 48
3 com.apple.NanoCalculator.watchkitapp 48
4 com.apple.NanoCalendar 48
5 com.apple.NanoCamera 48
6 com.apple.NanoCompass.watchkitapp 48
7 com.apple.NanoContacts 48
8 com.apple.NanoHome 48
9 com.apple.NanoMail 48
10 com.apple.NanoMaps 48
11 com.apple.NanoMusic 48
12 com.apple.NanoPassbook 48
13 com.apple.NanoPhone 48
14 com.apple.NanoPhotos 48
15 com.apple.NanoReminders 48
16 com.apple.NanoSettings 48
17 com.apple.NanoWorldClock 48
18 com.apple.nanoneews 48
19 com.apple.shortcuts.watch 48
20 com.apple.stocks.watchapp 48
21 com.apple.tincan 48
22 com.apple.weather.watchapp 48
23 com.apple.MobileReplayer 48

subscriber_info

ROWID subscriber_id subscriber_mdn tag last_update_time slot_id home_budget r
g_budget user_entered_bill_end_dom low_data_mode reliable_network_fallback smart_data_mod
erface_cost privacy_proxy
1 89148000009489719791 +16155719608 1 7.2105926717604E8 1
```

Serial Number

FFNHHK2RPLJM

activation\_record.plist

root@kali: ~/autopsy-files/autopsy-4.10.0/bin

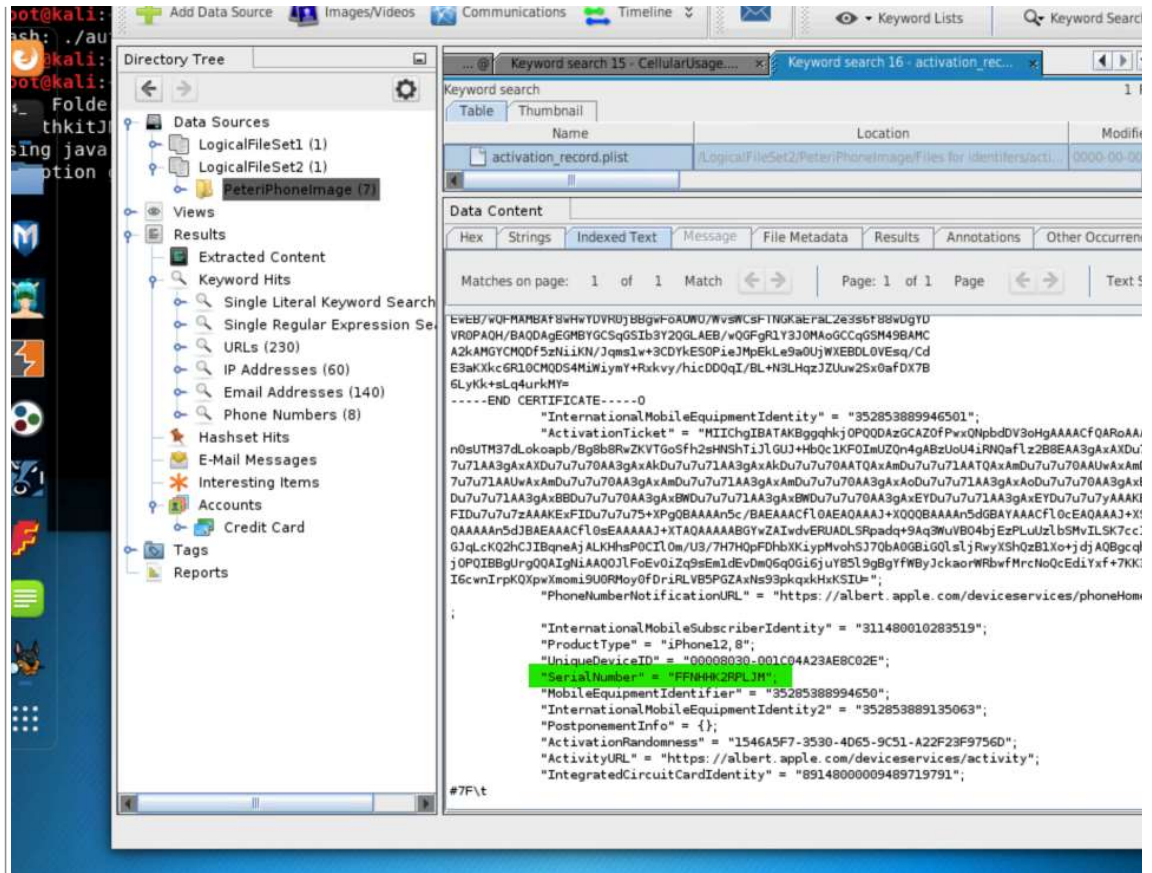
Pure-Gold-Credit-Union-2024 - Autopsy 4.10.0

file Edit View Search Timeline Help

Case View Tools Window Help

ash: cd: root@kali:

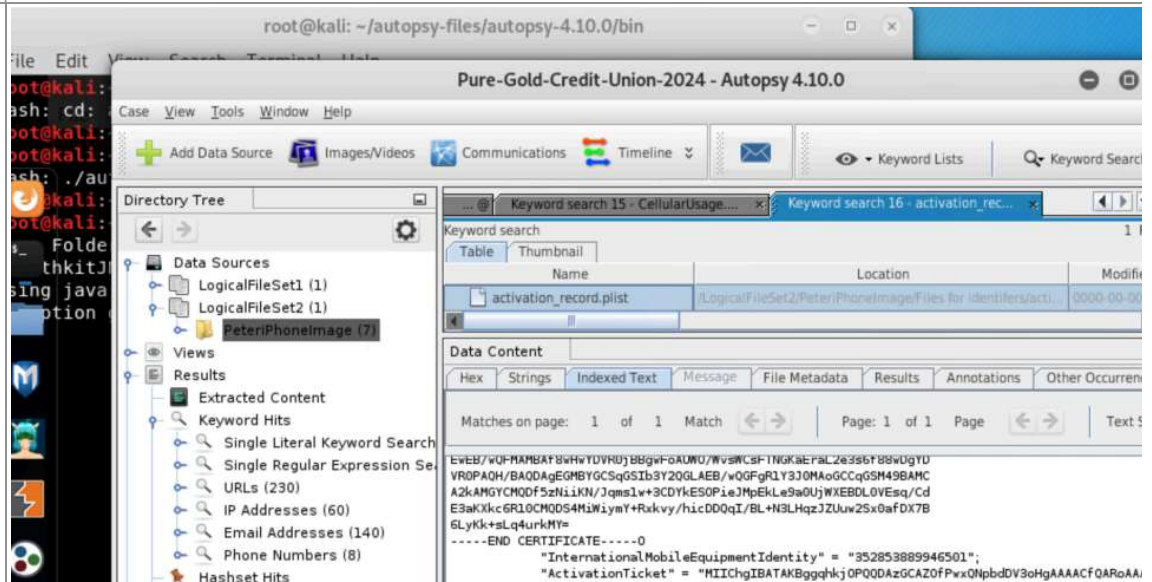




ICCID

8914800009489719791

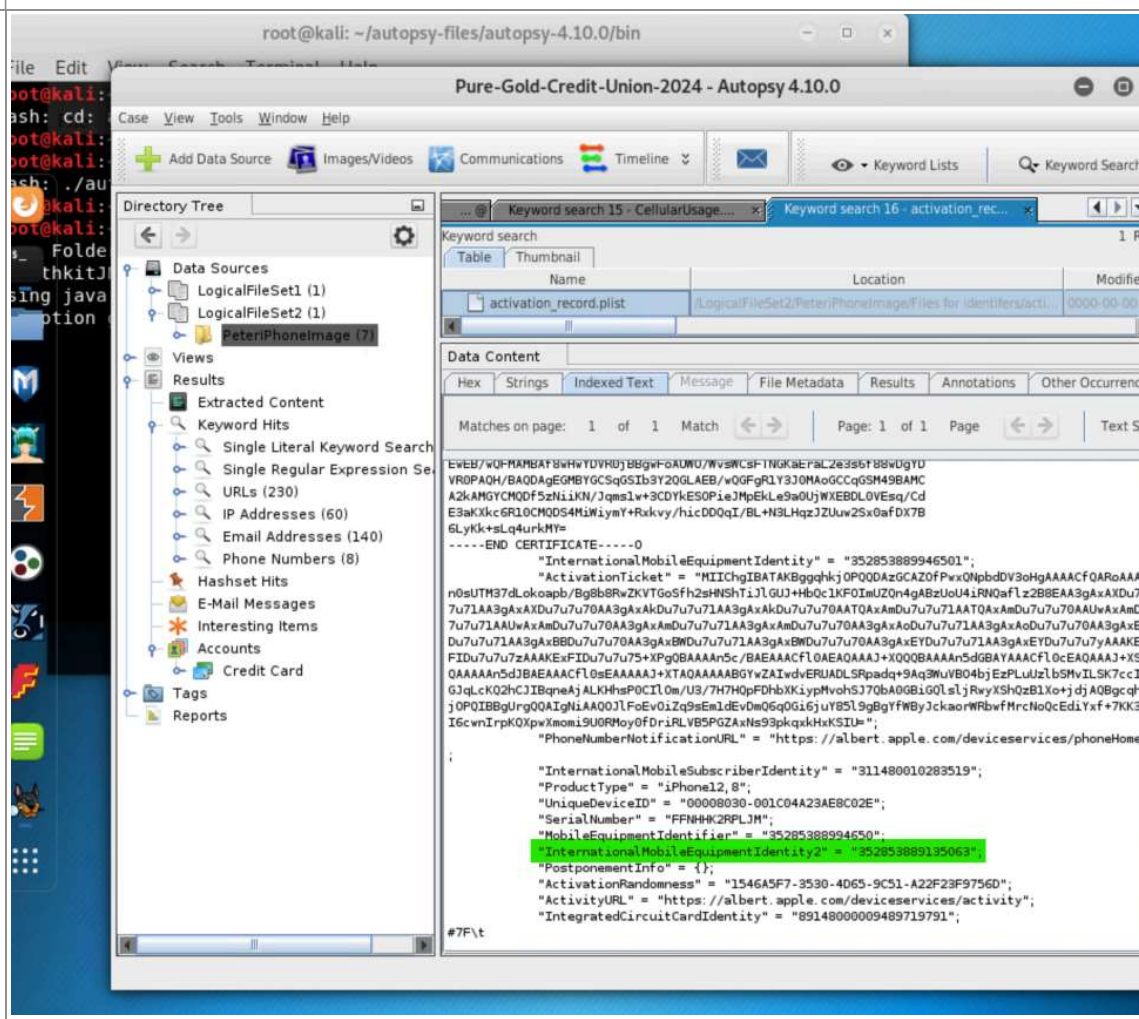
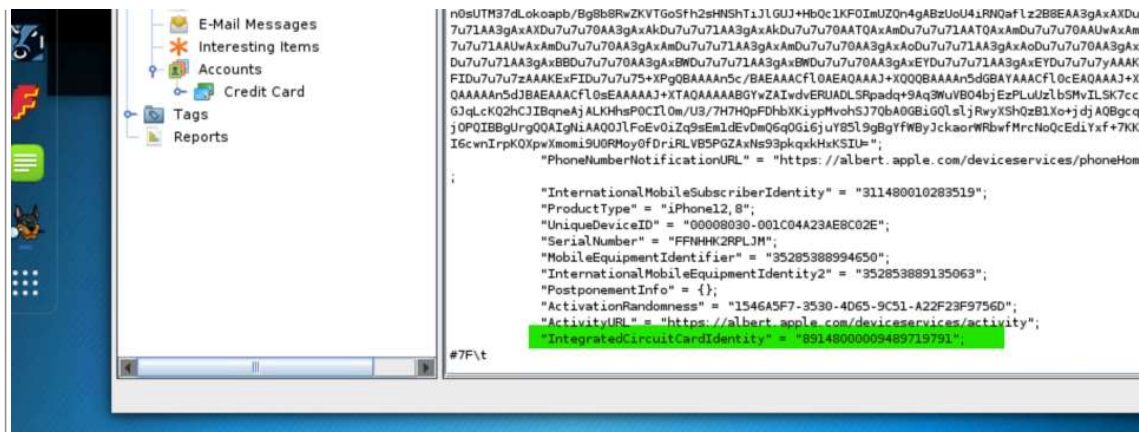
activation\_record.plist



IMEI

352853889135063

activation\_record.plist



MD5 Hash	34c4888f095dc3241330462923f6fea5	Provided	
SHA256 Hash	71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607	Provided	