Presented by: -
Mohit Ajaykumar Dhabuwala
M.S. in Cyber Forensics

—

‘HTC Desire Android Device Analysis’

—

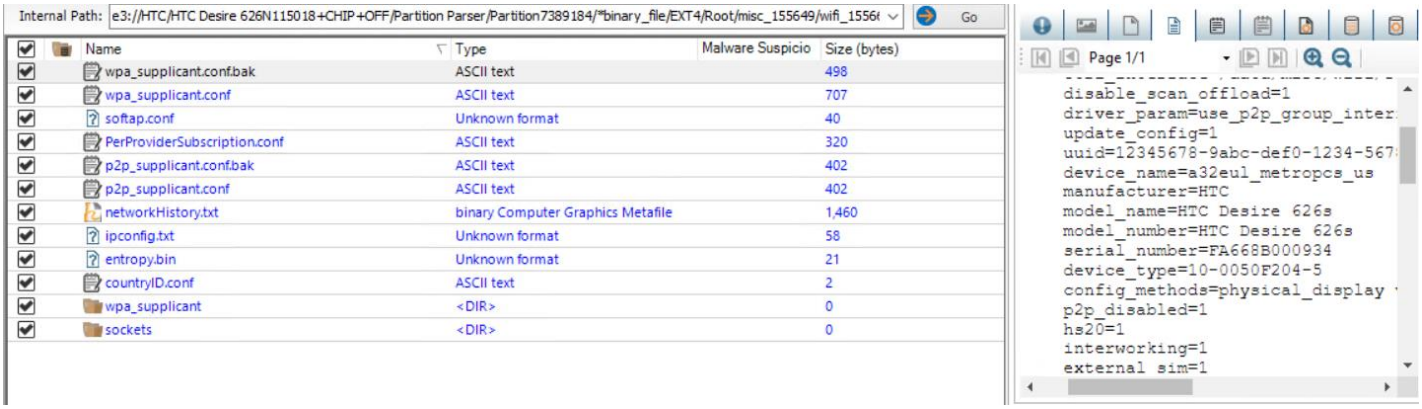
To: -
Prof. Melvin de la Cruz
(CYFI 700) Mobile Forensics

Aim: The HTC Desire mobile device’s contents have been imaged and extracted and you uploaded it to your OneDrive. You are back at the office and ready to begin the tedious process of recovering evidence for your extorsion case. The evidence file is named HTS Desire 626 N115018 CHIPOFF.001. This file size is 7GB so make sure you work on a VM, or you have sufficient space on your workstation to run multiple tools and handle the evidence. I have deliberately NOT provided you with any other information about the device or background of the case. Please give me a screenshot, a path and a written response for every question. Very basic responses are ok on this assignment. I am not looking for substance and quality. I am looking for your technical ability and know-how.

1. What is the model of this device

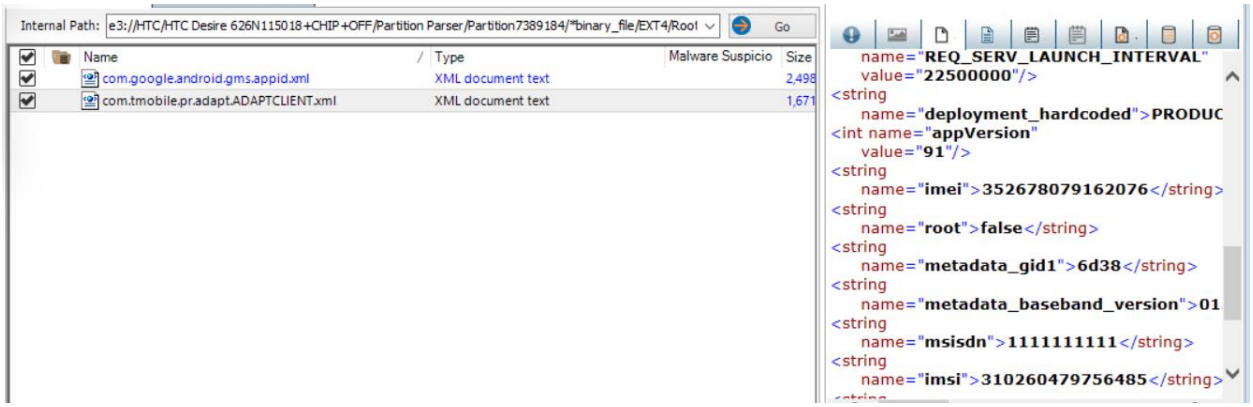
Answer: The model name of this device is “**HTC Desire 626s**”.

- **Path**: “e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/misc_155649/wifi_155663?item=wpa_supplicant.conf.bak_155725.”



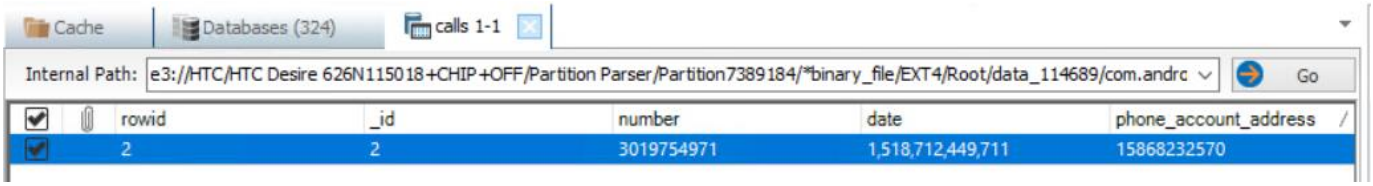
2. What is the IMEI of this device

Answer: The IMEI number is “**352678079162076”** found in the Path “ e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/misc_155649/wifi_155663 ?item=wpa_supplicant.conf.bak_155725”



3. What is the telephone number of this device?

Answer: The phone number of the device is +1 (586)823-2570" and it can be found from the SMS sent from the device. The evidence can be in "e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.android.providers.contacts_114710/databases_114958/contacts2.db_114959/*binary_file/database/tables/calls/2-3?item=row_2e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.android.providers.telephony_114811/databases_114987."



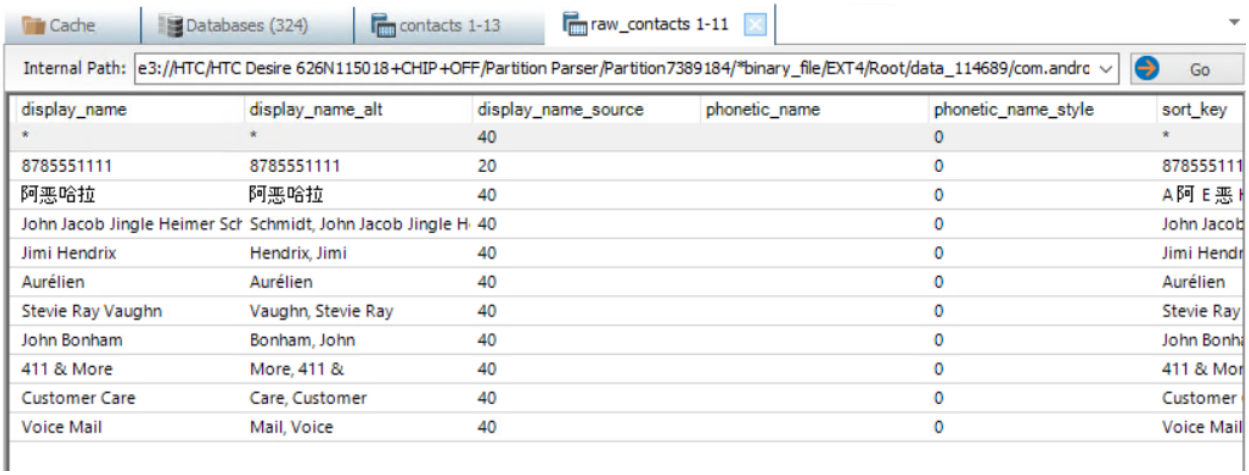
4. State the two famous person's name, telephone number, email, address and telephone number*(the internal memory Paths may not give you all of this info)*

Answer:

Person-1: Jimi Hendrix, 7691234560, hendrix@gmail.com,

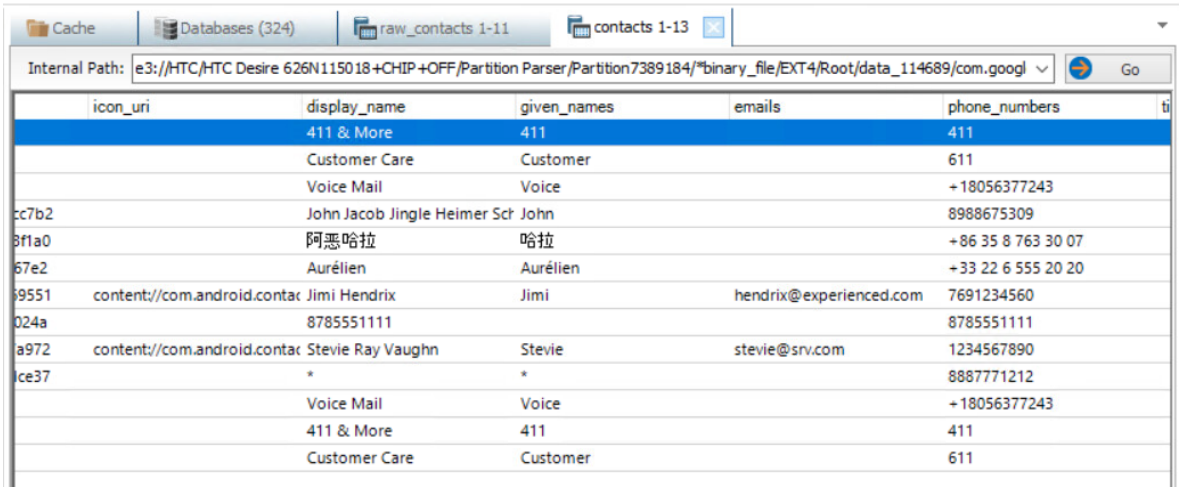
Person-2: Stevie Ray Vaughn, 1234567890, stevie@srv.com,

- **Path-1**: e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.google.android.gms_114726/databases_115144/icing_contacts.db_115492/*binary_file/database/tables/contacts/7-21. This could be from the synchronized phone data across devices having the same account.



display_name	display_name_alt	display_name_source	phonetic_name	phonetic_name_style	sort_key
*	*	40		0	*
8785551111	8785551111	20		0	878555111
阿恶哈拉	阿恶哈拉	40		0	A阿 E恶
John Jacob Jingle Heimer Sch	Schmidt, John Jacob Jingle H	40		0	John Jacob
Jimi Hendrix	Hendrix, Jimi	40		0	Jimi Hendr
Aurélien	Aurélien	40		0	Aurélien
Stevie Ray Vaughn	Vaughn, Stevie Ray	40		0	Stevie Ray
John Bonham	Bonham, John	40		0	John Bonh
411 & More	More, 411 &	40		0	411 & Mor
Customer Care	Care, Customer	40		0	Customer
Voice Mail	Mail, Voice	40		0	Voice Mail

- **Path-2**: e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.android.providers.contacts_114710/databases_114958/contacts2.db_114959/*binary_file/database/tables/calls/2-3?item=row_2e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.android.providers.telephony_114811/databases_114987. This is from the phone's local storage.



	icon_uri	display_name	given_names	emails	phone_numbers	ti
		411 & More	411		411	
		Customer Care	Customer		611	
		Voice Mail	Voice		+18056377243	
cc7b2		John Jacob Jingle Heimer Sch	John		8988675309	
3f1a0		阿恶哈拉	哈拉		+86 35 8 763 30 07	
67e2		Aurélien	Aurélien		+33 22 6 555 20 20	
9551	content://com.android.contac	Jimi Hendrix	Jimi	hendrix@experienced.com	7691234560	
024a		8785551111			8785551111	
a972	content://com.android.contac	Stevie Ray Vaughn	Stevie	stevie@srv.com	1234567890	
ce37		*	*		8887771212	
		Voice Mail	Voice		+18056377243	
		411 & More	411		411	
		Customer Care	Customer		611	

5. Show images of two famous persons

Answer: The 2 famous person whose photos are available on the device are:

- **Stephen Ray Vaughan**: an American musician, best known as the guitarist.
    - **Path**: “e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.htc.sense.mms_114785/cache_115100?item=1234567890_116212”

Stephen Ray Vaughan

- **Jimi Hendirx**: James Marshall "Jimi" Hendrix was an American guitarist, songwriter and singer. He is widely regarded as the greatest guitarist in history.
    - **Path**: “e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.htc.sense.mms_114785/cache_115100?item=1234567890_116212”.

Jimi Hendrix

6. What are telephone numbers without names?

Answer: There are 2 contacts without names. They are “8785551111”, “8887771212”.

- **Path**: “e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.google.android.gms_114726/databases_115144/icing_contacts.db_115492/*binary_file/database/tables/contacts/7-21?item=row_15”.

2171i73a99ba0bc9024a		8785551111		8785551111
2171i5e531bf20c07a972	content://com.android.contac	Stevie Ray Vaughn	Stevie	1234567890
2171i2d570efa0c4dce37		*	*	8887771212

7. What is the deleted contact name and telephone number?

Answer: The deleted contact name is “John Bonham”, and the telephone number is “(987)876-7654”.

- **Path:** e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.android.providers.contacts_114710/databases_114958/contacts2.db_114959/*binary_file/database/tables/raw_contacts/10-21?item=row_17

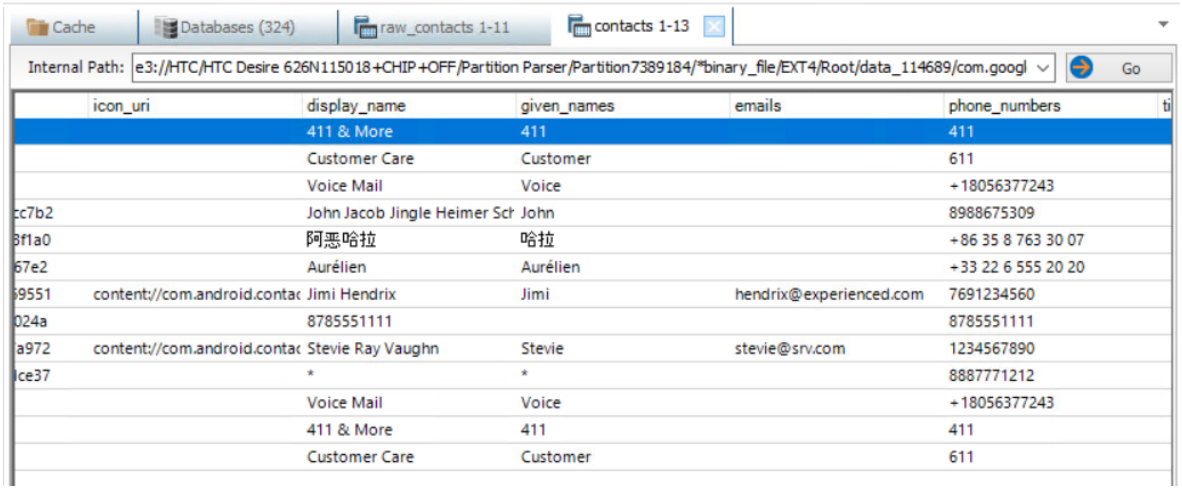
deleted	display_name	display_name_alt	display_name_source
1	John Bonham	Bonham, John	40
0	*	*	40
0	8785551111	8785551111	20
0	阿恶哈拉	阿恶哈拉	40
0	John Jacob Jingle Heimer Sch	Schmidt, John Jacob Jingle H	40
0	Jimi Hendrix	Hendrix, Jimi	40
0	Aurélien	Aurélien	40
0	Stevie Ray Vaughn	Vaughn, Stevie Ray	40
0	411 & More	More, 411 &	40
0	Customer Care	Care, Customer	40
0	Voice Mail	Mail, Voice	40

8. What are the two foreign contact names and telephone numbers?

Answer: The 2 foreign contact name and telephone number are:

- **Aurélien**: It is a French name and the number is: “+33 2265552020” and it has a telephone code “+33” which is the country code of France.
  - **Path**: e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.android.providers.contacts_114710/databases_114958/contacts2.db_114959/*binary_file/database/tables/raw_contacts/10-21

- **阿恶哈拉 (A E HA LA)**: It is a Chinese name and the number associated is: “+86 3587633007” and it also has a code “+86” which is the telephone code of China.
  - **Path:** e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.android.providers.contacts_114710/databases_114958/contacts2.db_114959/*binary_file/database/tables/raw_contacts/10-21



	icon_uri	display_name	given_names	emails	phone_numbers	ti
		411 & More	411		411	
		Customer Care	Customer		611	
		Voice Mail	Voice		+18056377243	
cc7b2		John Jacob Jingle Heimer Sch	John		8988675309	
8f1a0		阿恶哈拉	哈拉		+86 35 8 763 30 07	
67e2		Aurélien	Aurélien		+33 22 6 555 20 20	
69551	content://com.android.contac	Jimi Hendrix	Jimi	hendrix@experienced.com	7691234560	
024a		8785551111			8785551111	
a972	content://com.android.contac	Stevie Ray Vaughn	Stevie	stevie@srv.com	1234567890	
ce37		*	*		8887771212	
		Voice Mail	Voice		+18056377243	
		411 & More	411		411	
		Customer Care	Customer		611	

9. What is contained in group contact?

Answer: There is 1 SMS group between the user, Stevie Ray Vaughn (1234567890), 3014011239, and Jimi Hendrix (7691234560).

- **Path:** e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.android.providers.telephony_114811/databases_114987/mmssms.db_114995/*binary_file/database/tables/threads/1-3

recipient_ids	recipient_address	name	snippet	snippet_
1	3014011239	3014011239	The following SMS message is an active	0
1 2 3	3014011239;1234567890;7691234560	3014011239;Stevie Ray Vaughn;Jimi Hendrix		0

10. Provide all details of the datebook/Calendar

Answer: There is a total of 49 calendar events found in the device.

- **Path**: "e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.android.providers.calendar_114705/databases_115068/calendar.db_115079/*binary_file/database/tables/Events/1-50"

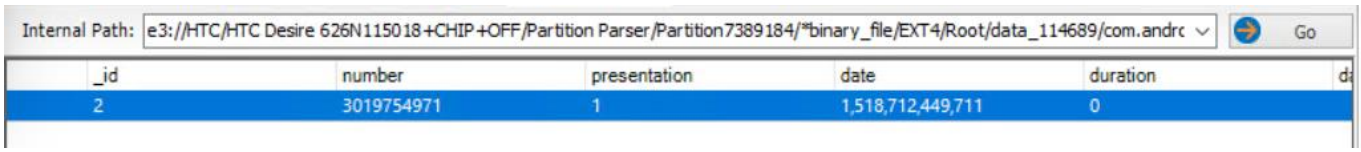
This calendar data represents a snapshot of calendar entries between 2014 and early 2019, with a concentration of activity in 2017 and 2018. It mixes personal events (like a Rush concert), American holidays, and practical reminders like Daylight Saving Time adjustments. This suggests it's a personal calendar, likely belonging to someone in the US, who also used it to track some individual interests. The abrupt end of entries in 2019 hints that either the data is incomplete, or the calendar stopped being used around that time.

_sync_id	title	calendar_id	dtstart	dtend	eventLocation
1n9asvs73me13m61o0ji8hkq	Rush Concert	2	1,461,398,400,000		Los angeles
_6d2jehhj6ss3iba36l2kcb9k8	Van halen were scheduled to	2	1,393,804,800,000		
9kf26dov637nnrm36ckmsvsn		2	1,476,108,000,000		
20170220_60o30dr570o30e1	Presidents' Day (regional hol	4	1,487,548,800,000	1,487,635,200,000	
20170312_60o30c9o60o30dp	Daylight Saving Time starts	4	1,489,276,800,000	1,489,363,200,000	
20170413_60o30o9lc8o30c1g	Thomas Jefferson's Birthday	4	1,492,041,600,000	1,492,128,000,000	
20170416_60o30dr660o30c1	Easter Sunday	4	1,492,300,800,000	1,492,387,200,000	
20170514_60o30dr560o30e1	Mother's Day	4	1,494,720,000,000	1,494,806,400,000	
20170529_60o30dr56co30e1	Memorial Day	4	1,496,016,000,000	1,496,102,400,000	
20170618_60o30dr564o30e1	Father's Day	4	1,497,744,000,000	1,497,830,400,000	
20180115_60o30dr56oo30c1	Martin Luther King Jr. Day	4	1,515,974,400,000	1,516,060,800,000	
20170704_60o30dr470o30c1	Independence Day	4	1,499,126,400,000	1,499,212,800,000	
20171009_60o30dr5c8o38e1	Columbus Day (regional holi	4	1,507,507,200,000	1,507,593,600,000	
20171031_60o30dr4cko30c1g	Halloween	4	1,509,408,000,000	1,509,494,400,000	
20171105_60o30c9o64o30dp	Daylight Saving Time ends	4	1,509,840,000,000	1,509,926,400,000	
20171110_60o30dr568o36c1	Veterans Day observed	4	1,510,272,000,000	1,510,358,400,000	
20171111_60o30dr568o30c1	Veterans Day	4	1,510,358,400,000	1,510,444,800,000	
20171123_60o30dr5cco30e1g	Thanksgiving Day	4	1,511,395,200,000	1,511,481,600,000	
20171224_60o30dr56ko30c1	Christmas Eve	4	1,514,073,600,000	1,514,160,000,000	
20171225_60o30dr56go30c1	Christmas Day	4	1,514,160,000,000	1,514,246,400,000	
20171231_60o30dr4coo30c1	New Year's Eve	4	1,514,678,400,000	1,514,764,800,000	
20170904_60o30dr5c4o30e1	Labor Day	4	1,504,483,200,000	1,504,569,600,000	
20180101_60o30dr46oo30c1	New Year's Day	4	1,514,764,800,000	1,514,851,200,000	
20190310_60o30c9o60o30dp	Daylight Saving Time starts	4	1,552,176,000,000	1,552,262,400,000	
20180214_60o30dr46so30c1g	Valentine's Day	4	1,518,566,400,000	1,518,652,800,000	
20180219_60o30dr570o30e1	Presidents' Day (regional hol	4	1,518,998,400,000	1,519,084,800,000	
20180311_60o30c9o60o30dp	Daylight Saving Time starts	4	1,520,726,400,000	1,520,812,800,000	

11. Provide the outgoing telephone numbers in the call log

Answer: The outgoing telephone number is "3019754971".

- **Path**: "e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.android.providers.contacts_114710/databases_114958/contacts2.db_114959/*binary_file/database/tables/calls/2-3?item=row_2" .



12. Are there any outgoing SMS messages? If so, give evidence of the content.

Answer: There are 2 outgoing SMS messages available.

- **Path:** "e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.android.providers.telephony_114811/databases_114987/mmssms.db_114995/*binary_file/database/tables/sms/1-4" and the Path of both the SMS is "Table: sms(_id: 1)" and "Table: sms(_id: 3)."

Local User <HTC Desire 626N11501...	3014011239	The following SMS message is an active outgoing message sent to an...	SMS	2/21/2018 2:07:34.731 PM
Local User <HTC Desire 626N11501...	3014011239	Outgoing active extended SMS message. This is an outgoing SMS m...	SMS	2/15/2018 4:58:42.548 PM

13. Are there any MMS messages? If so, give evidence of the content.

Answer: Yes, there are 5 MMS available on the device.

- **Path:** "e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.android.providers.telephony_114811/databases_114987/mmssms.db_114995/*binary_file/database/tables/part/1-16?item=row_6"

Sender	Recipient(s)	Message	Type	Sent Date/Time	Received Dat
Local User <HTC Desire 626N11501...	Stevie Ray Vaughn...	The following SMS message is an active outgoing group message sen...	MMS	2/15/2018 5:00:54.000 PM	2/15/2018 5:00:
Local User <HTC Desire 626N11501...	Stevie Ray Vaughn...	Outgoing active extended SMS message. This is an outgoing SMS m...	MMS	2/15/2018 5:10:23.000 PM	2/15/2018 5:10:
Local User <HTC Desire 626N11501...	3014011239	Outgoing sound byte message	MMS	2/15/2018 5:18:38.000 PM	2/15/2018 5:18:
Local User <HTC Desire 626N11501...	3014011239	Outgoing image MMS message	MMS	2/15/2018 5:19:19.000 PM	2/15/2018 5:19:
Local User <HTC Desire 626N11501...	3014011239	Outgoing video message	MMS	2/15/2018 5:23:23.000 PM	2/15/2018 5:23:

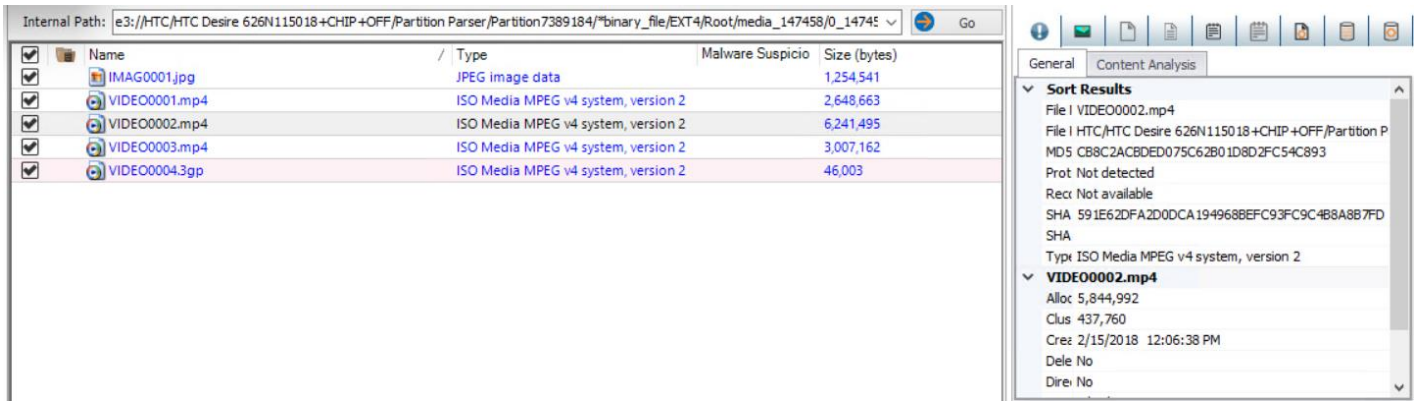
14. Are there any standalone data files? If so, give evidence of the content.

Answer: **Standalone data files** are the files that exist independently of a specific app or the operating system's main file structure. These files typically contain user-generated or app-generated data that is stored separately for various reasons. This data can be images(.jpeg/.jpg, .PNG), videos(.mp4, .mpeg), documents(.docx, .pdf, .txt, .xml), audio recordings(mp3) etc.

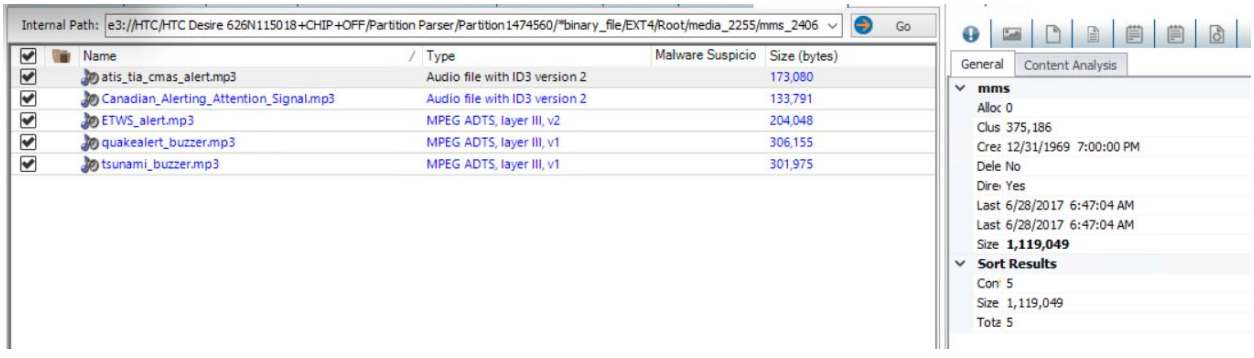
Yes, based on the provided information, there is strong evidence suggesting the presence of standalone data files. The category **"Media (48,697)" and "Documents (291)"** consist of a total of **48,938** files. Within this category, we have:

- **Pictures (48,223):** This substantial number strongly indicates the presence of image files, which could be standalone data files. These files would likely contain photographic images captured by the device's camera, downloaded from various sources or created/stored by some applications. These images are located at various locations.
    - **Path:** e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.instagram.android_124280/cache_131132/images_131162?item=91c00bf6.clean_131559

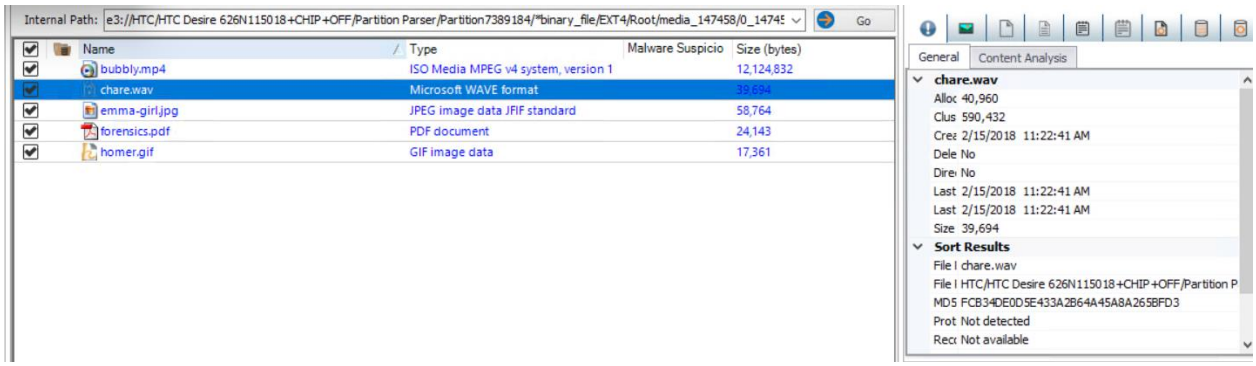
- **Videos (28):** This signifies the existence of video files, another type of standalone data. These files would likely contain video recordings or downloaded videos.
    - **Path:** e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/media_147458/0_147457/DCIM_147491/100MEDIA_147608?item=VIDEO0002.mp4_147519



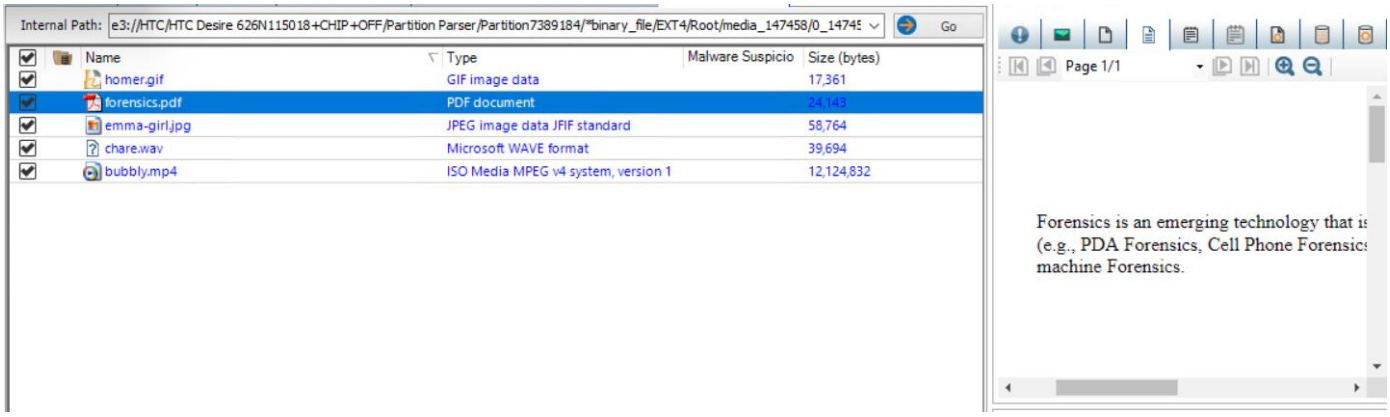
- **Audio (321):** This points towards standalone audio files, which could include music, voice recordings, or other sound clips.
    - **Path:** e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition1474560/*binary_file/EXT4/Root/media_2255/mms_2406



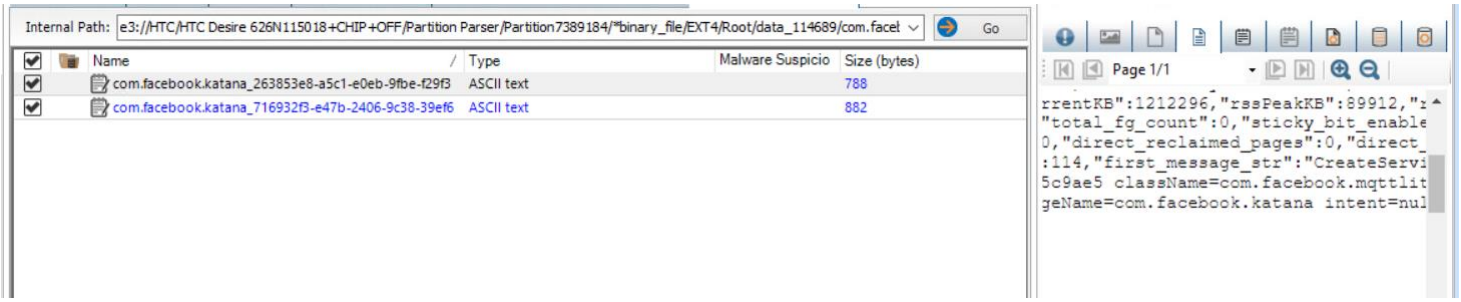
- **Carved Audio (115):** "Carved" audio suggests that these files were recovered through data carving techniques, possibly from unallocated space or fragmented data. These would also be standalone audio files.
    - **Path:** e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/media_147458/0_147457/Download_147490?item=chare.wav_147577



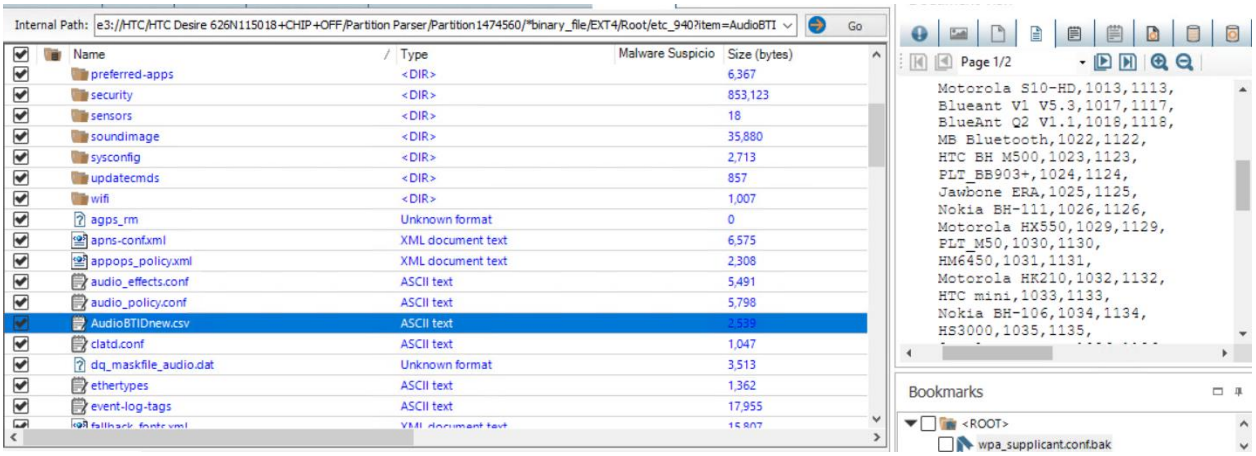
- **PDF Documents (14):** PDFs (Portable Document Format) are widely used for sharing documents and are inherently standalone files.
    - **Path:** e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/media_147458/0_147457/Download_147490?item=forensics.pdf_147575



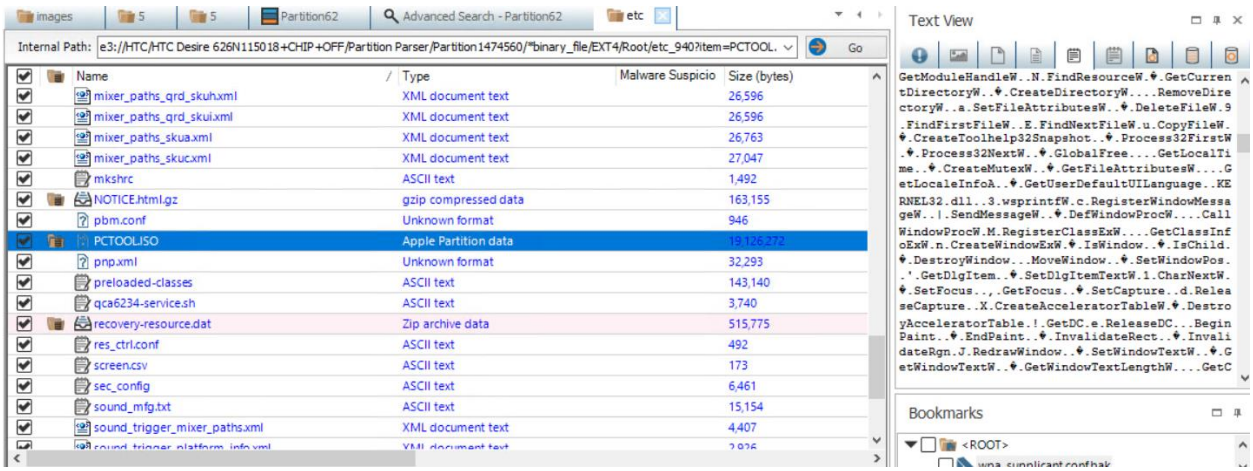
- **Text Documents (224):** This substantial number indicates the presence of plain text files, which are also standalone data files. These could contain notes, code, logs, or other textual information.
    - **Path:** e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.facebook.katana_114855/app_state_logs_124023?item=com.facebook.katana_263853e8-a5c1-e0eb-9fbe-f29f34f1bcd9.txt_123122



- **CSV Documents (2):** CSV (Comma Separated Values) files are commonly used for storing tabular data and can be considered standalone data files.
    - **Path:** e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition1474560/*binary_file/EXT4/Root/etc_940?item=AudioBTIDnew.csv_941



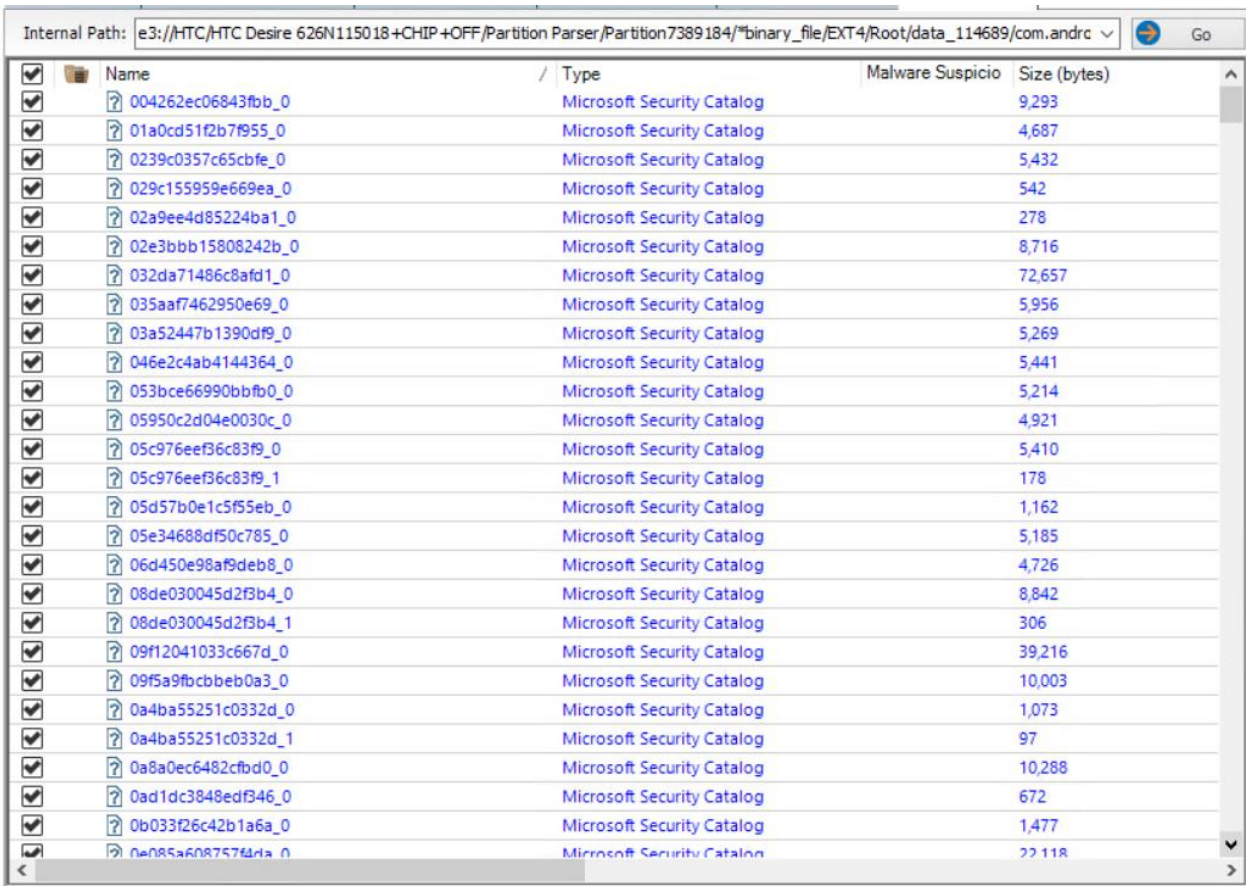
- **RTF Documents (1):** RTF (Rich Text Format) files are another type of document format that can store formatted text and images, and they are also standalone files.
    - **Path:** e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition1474560/*binary_file/EXT4/Root/etc_940?item=PCTOOL.ISO_953



15. Is there any internet data? If so, provide evidence.

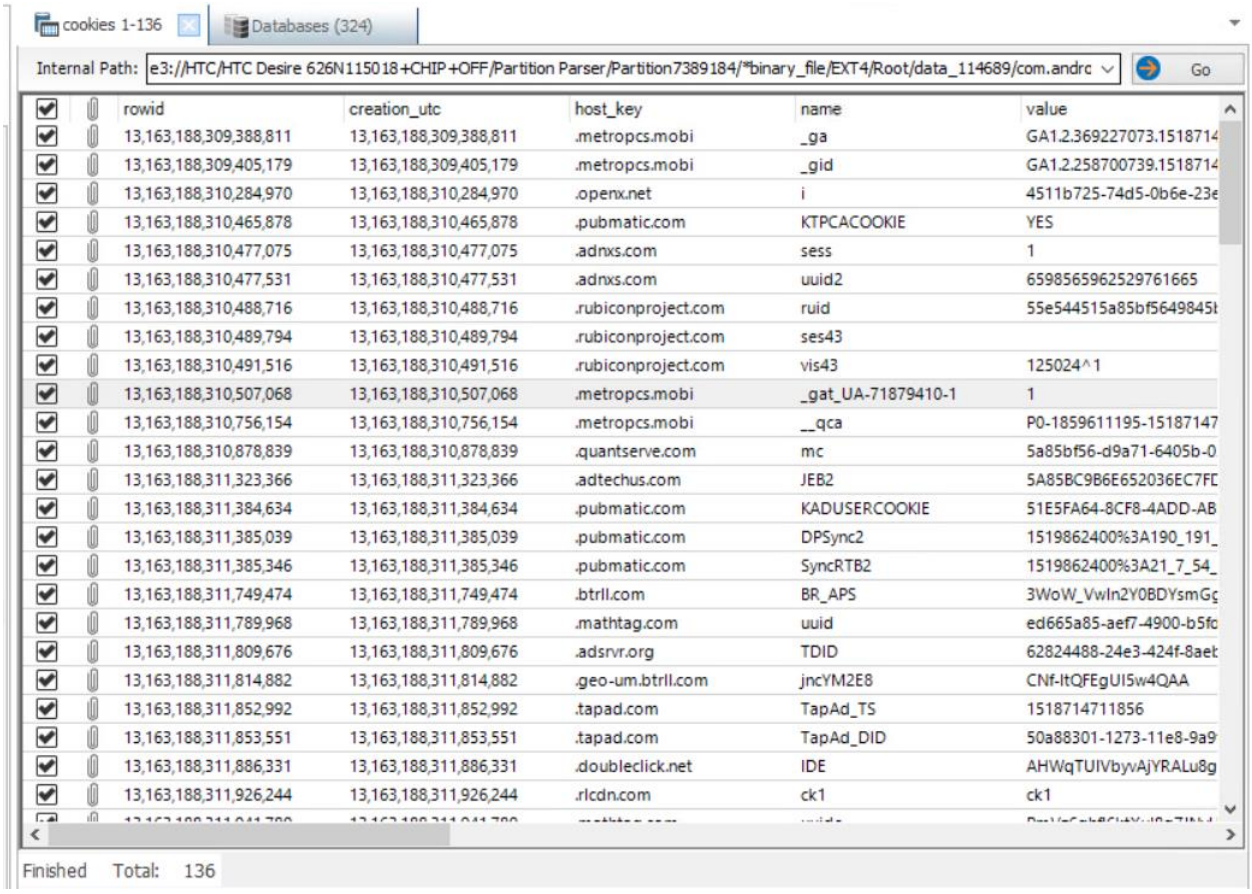
Answer: Yes, there is substantial evidence of internet data. The presence of "Chrome Bookmarks," "Chrome Cache Records," "Chrome Cookies," "Chrome Tab History," "Chrome Top Sites," "Chrome Web History," and "Chrome Web Visits" — coupled with a high number of "Potential Browser Activity" records — clearly indicates significant internet browsing activity.

- **Chrome Cache Records (576):** Temporary stored website data, revealing recently visited sites and content.
    - **Path:** “e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.android.chrome_114840/cache_123007/Cache_124580”

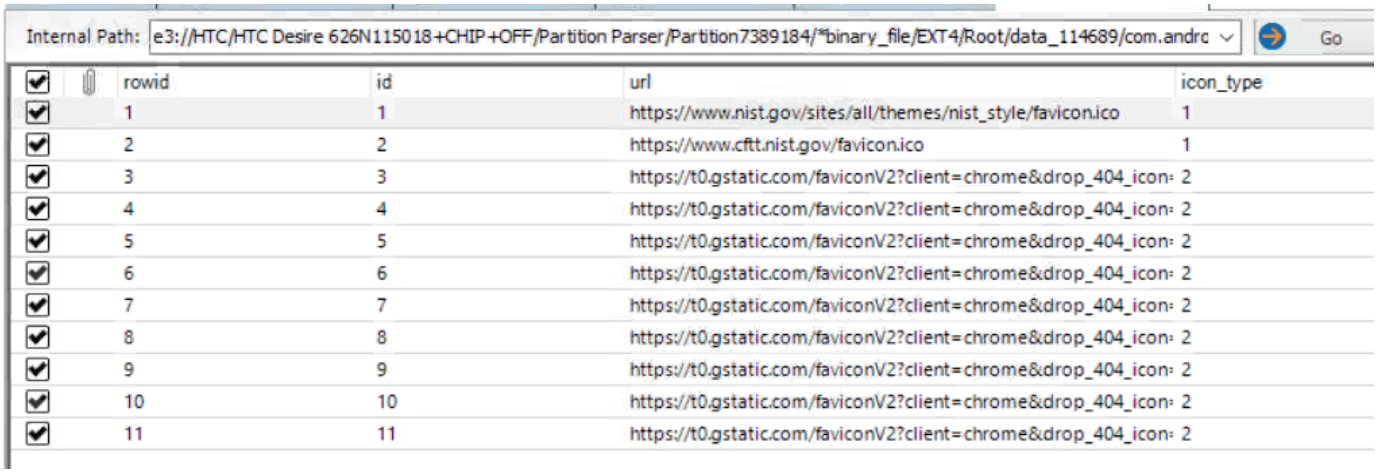


- **Chrome Cookies (136):** Small files stored by websites, tracking user activity and preferences. There are 136 of such cookies found in the device.

    - **Path**: e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.android.chrome_114840/app_chrome_124498/Default_124507/Cookies_124567/*binary_file/database/tables/cookies/131631883 09388811-13163188462121730?item=row_13163188310507068

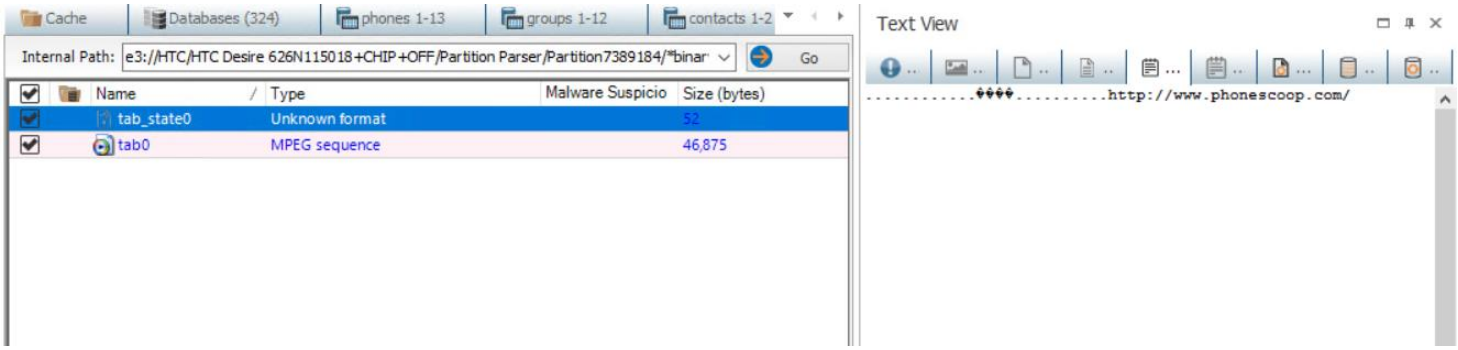


- **Chrome Favicons (11):** Website icons associated with bookmarks or history, aiding site identification. There are 11 such favicons recovered from device.
  - **Path:** e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.android.chrome_114840/app_chrome_124498/Default_124507/Favicons_124555/*binary_file/database/tables/favicons/1-12

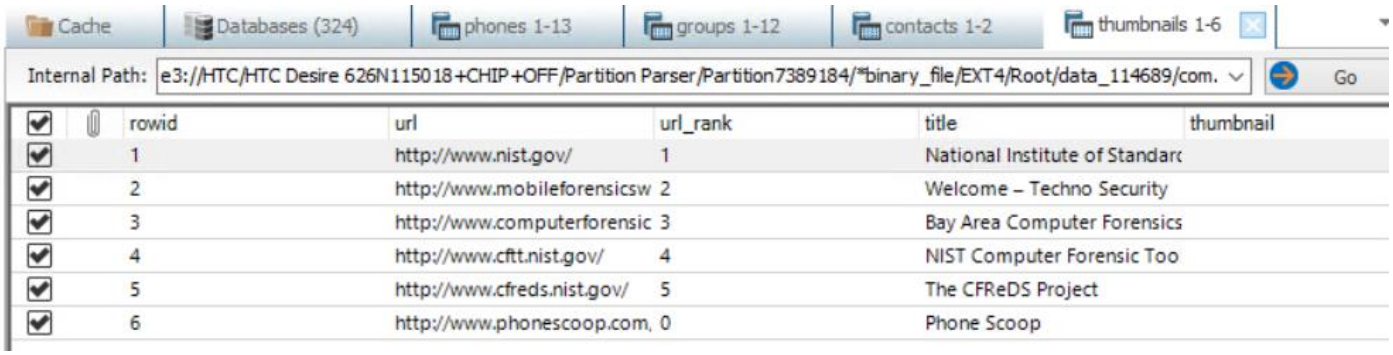


rowid	id	url	icon_type
1	1	https://www.nist.gov/sites/all/themes/nist_style/favicon.ico	1
2	2	https://www.cftt.nist.gov/favicon.ico	1
3	3	https://t0.gstatic.com/faviconV2?client=chrome&drop_404_icon=	2
4	4	https://t0.gstatic.com/faviconV2?client=chrome&drop_404_icon=	2
5	5	https://t0.gstatic.com/faviconV2?client=chrome&drop_404_icon=	2
6	6	https://t0.gstatic.com/faviconV2?client=chrome&drop_404_icon=	2
7	7	https://t0.gstatic.com/faviconV2?client=chrome&drop_404_icon=	2
8	8	https://t0.gstatic.com/faviconV2?client=chrome&drop_404_icon=	2
9	9	https://t0.gstatic.com/faviconV2?client=chrome&drop_404_icon=	2
10	10	https://t0.gstatic.com/faviconV2?client=chrome&drop_404_icon=	2
11	11	https://t0.gstatic.com/faviconV2?client=chrome&drop_404_icon=	2

- **Chrome Tab History (1):** The last open tab at the time of data collection, offering a glimpse into current activity. There is 1 one tab found in the android device.
  - **Path:** e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.android.chrome_114840/app_tabs_124569/0_124585?item=tab_state0_125294



- **Chrome Top Sites (6):** Most frequently visited websites, revealing user habits and interests. There are 6 websites featuring in the top sites list.
    - **Path:** e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.android.chrome_114840/app_chrome_124498/Default_124507/Top Sites_124561/*binary_file/database/tables/thumbnails/1-7



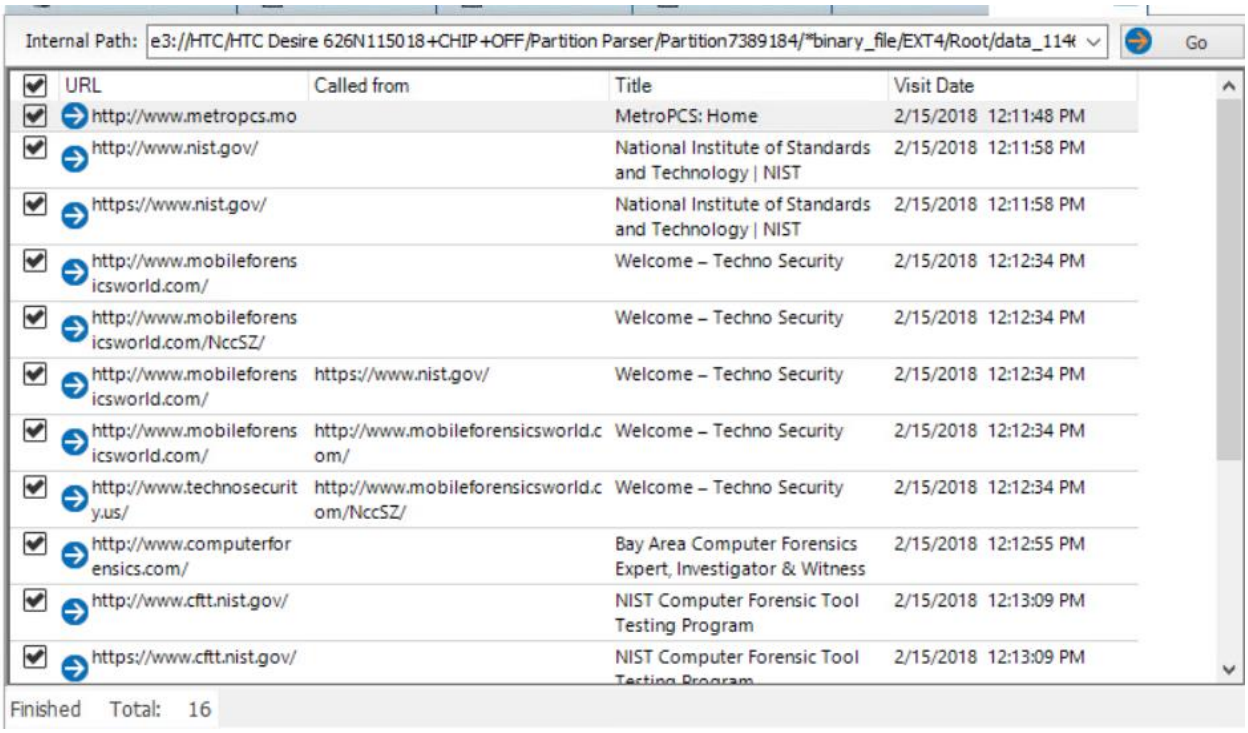
rowid	url	url_rank	title	thumbnail
1	http://www.nist.gov/	1	National Institute of Standarc	
2	http://www.mobileforensicsw	2	Welcome – Techno Security	
3	http://www.computerforensic	3	Bay Area Computer Forensics	
4	http://www.cftt.nist.gov/	4	NIST Computer Forensic Too	
5	http://www.cfreds.nist.gov/	5	The CFReDS Project	
6	http://www.phonescoop.com,	0	Phone Scoop	

- **Chrome Bookmarks (2):** Saved website links, indicating user interest or frequently accessed pages.

    - **Path**: e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.android.chrome_114840/app_chrome_124498/Default_124507/*VFM/Chrome_Storage_Manager/Bookmarks

Created Time	Title	URL	Visit Date	Folder
2/15/2018 12:13:15 PM	NIST Computer Forensic Tool Testing Program	https://www.cftt.nist.gov/	2/15/2018 12:13:15 PM	/Mobile bookmarks
2/15/2018 12:13:32 PM	The CFReDS Project	https://www.cfreds.nist.gov/	2/15/2018 12:13:32 PM	/Mobile bookmarks

- **Chrome Web History (16):** A record of websites visited, potentially revealing the user's browsing patterns. There is total 16 entries and 7 websites visited, and few have the different domain visits.
    - **Path:** e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.android.chrome_114840/app_chrome_124498/Default_124507/*VFM/Chrome_Storage_Manager/History



- **Chrome Web Visits (14):** Timestamped records of website visits, providing a more detailed browsing timeline.
    - **Path:** e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.android.chrome_114840/app_chrome_124498/Default_124507/*VFM/Chrome_Storage_Manager/History

URL	Called from	Title	Visit Date
http://www.metropcs.mo		MetroPCS: Home	2/15/2018 12:11:48 PM
http://www.nist.gov/		National Institute of Standards and Technology | NIST	2/15/2018 12:11:58 PM
https://www.nist.gov/		National Institute of Standards and Technology | NIST	2/15/2018 12:11:58 PM
http://www.mobileforensicsworld.com/		Welcome – Techno Security	2/15/2018 12:12:34 PM
http://www.mobileforensicsworld.com/NccSZ/		Welcome – Techno Security	2/15/2018 12:12:34 PM
http://www.mobileforensicsworld.com/	https://www.nist.gov/	Welcome – Techno Security	2/15/2018 12:12:34 PM
http://www.mobileforensicsworld.com/	http://www.mobileforensicsworld.com/	Welcome – Techno Security	2/15/2018 12:12:34 PM
http://www.technosecurity.us/	http://www.mobileforensicsworld.com/NccSZ/	Welcome – Techno Security	2/15/2018 12:12:34 PM
http://www.computerforensics.com/		Bay Area Computer Forensics Expert, Investigator & Witness	2/15/2018 12:12:55 PM
http://www.cftt.nist.gov/		NIST Computer Forensic Tool Testing Program	2/15/2018 12:13:09 PM
https://www.cftt.nist.gov/		NIST Computer Forensic Tool Testing Program	2/15/2018 12:13:09 PM

- **Potential Browser Activity (586):** Additional web-related data, possibly indicating further browsing activity or interactions. This are not available in one location rather there are several files and path.
  - **Path:**

EVIDENCE (586)

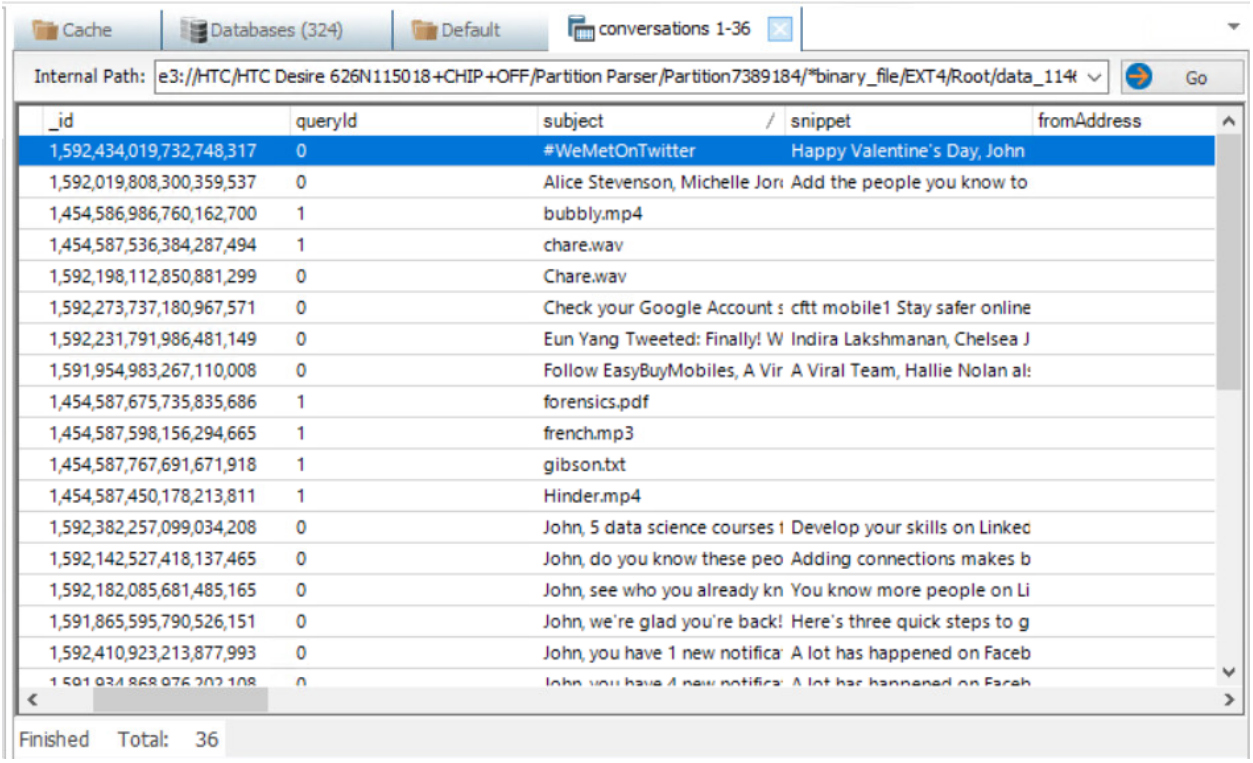
Column view

Artifact type	Source
Potential Browser Activity	HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.android.chrome\app_tabs\0\tab0
Potential Browser Activity	HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.android.chrome\app_tabs\0\tab0
Potential Browser Activity	HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.android.chrome\app_tabs\0\tab0
Potential Browser Activity	HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.android.chrome\app_tabs\0\tab0
Potential Browser Activity	HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.android.chrome\app_tabs\0\tab0
Potential Browser Activity	HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.android.chrome\app_tabs\0\tab0
Potential Browser Activity	HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.android.chrome\app_tabs\0\tab0
Potential Browser Activity	HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.android.chrome\app_tabs\0\tab0
Potential Browser Activity	HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.android.chrome\app_tabs\0\tab0
Potential Browser Activity	HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.android.chrome\app_tabs\0\tab0
Potential Browser Activity	HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.android.chrome\app_tabs\0\tab0
Potential Browser Activity	HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.android.chrome\app_tabs\0\tab0
Potential Browser Activity	HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.android.chrome\app_tabs\0\tab0
Potential Browser Activity	HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.android.chrome\cache\Cache\40ca592857545419_1
Potential Browser Activity	HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.android.chrome\cache\Cache\65612ec690fa7a7b_1
Potential Browser Activity	HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.android.chrome\cache\Cache\6b21d1da9ba0c759_1

16. Is there any email data? If so, provide evidence.

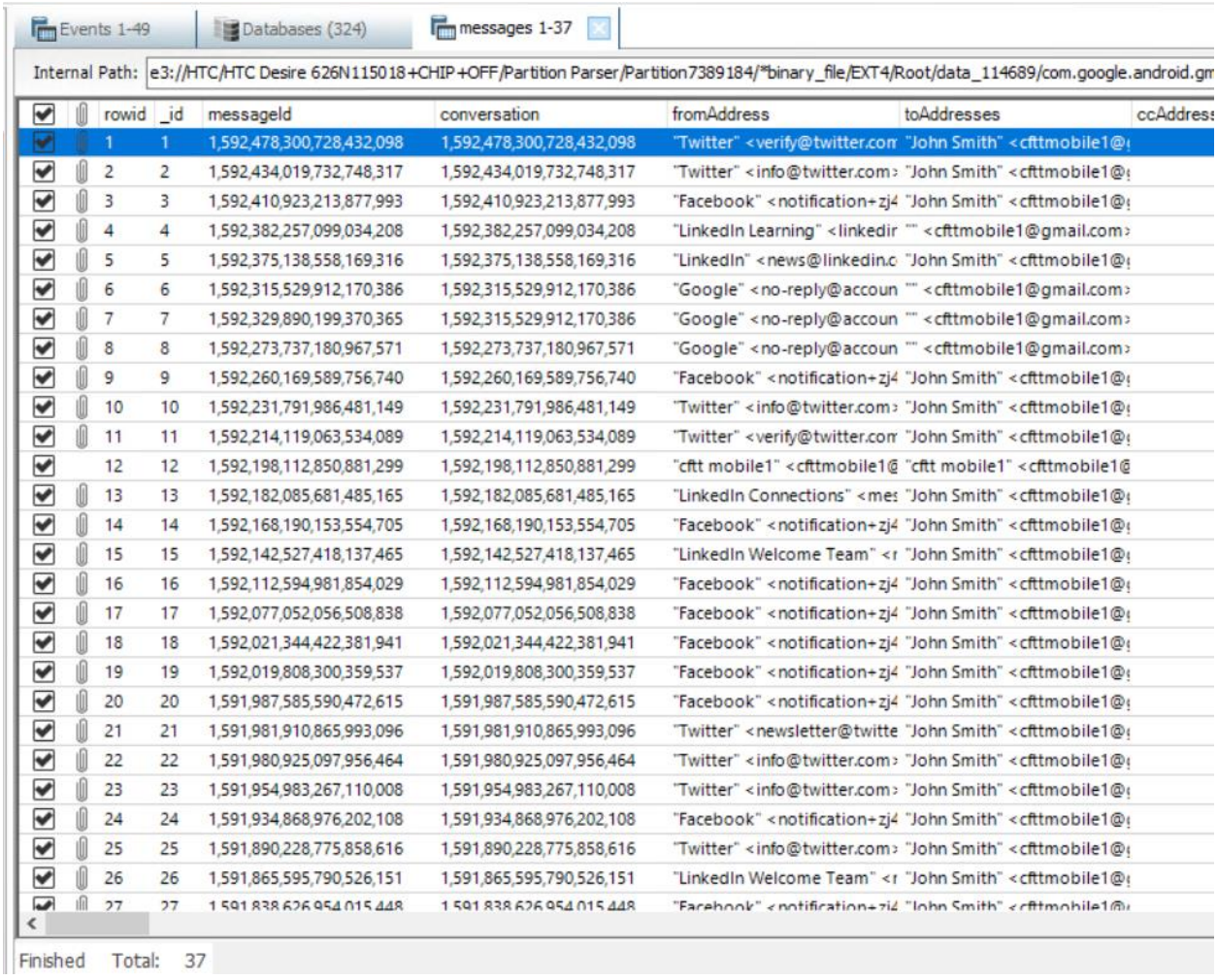
Answer: The image indicates the presence of 83 email-related items, comprised of:

- **36 Android Gmail Conversations:** These likely represent email threads or ongoing conversations within the Gmail app on an Android device.
    - **Path:** e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.google.android.gm_114860/databases_115024/mailstore.cfttmobile1@gmail.com.db_115862/*binary_file/database/tables/conversations/2-39



- **37 Gmail Emails:** These are most likely individual email messages within the Gmail account.
    - **Path:** e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.google.android.gm_114860/databases_115024/mailstore.cfttmobile1@gmail.com.db_115862/*binary_file/database/tables/messages/1-38

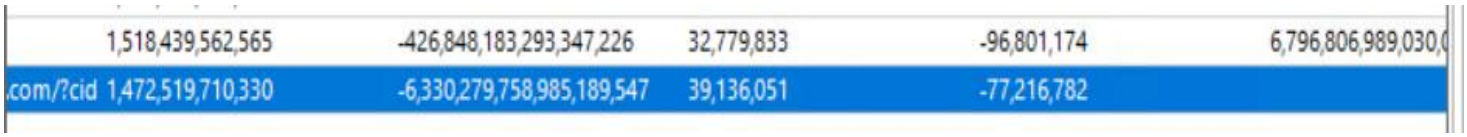
The symbol in the first column also suggests that there are attachments in every email.



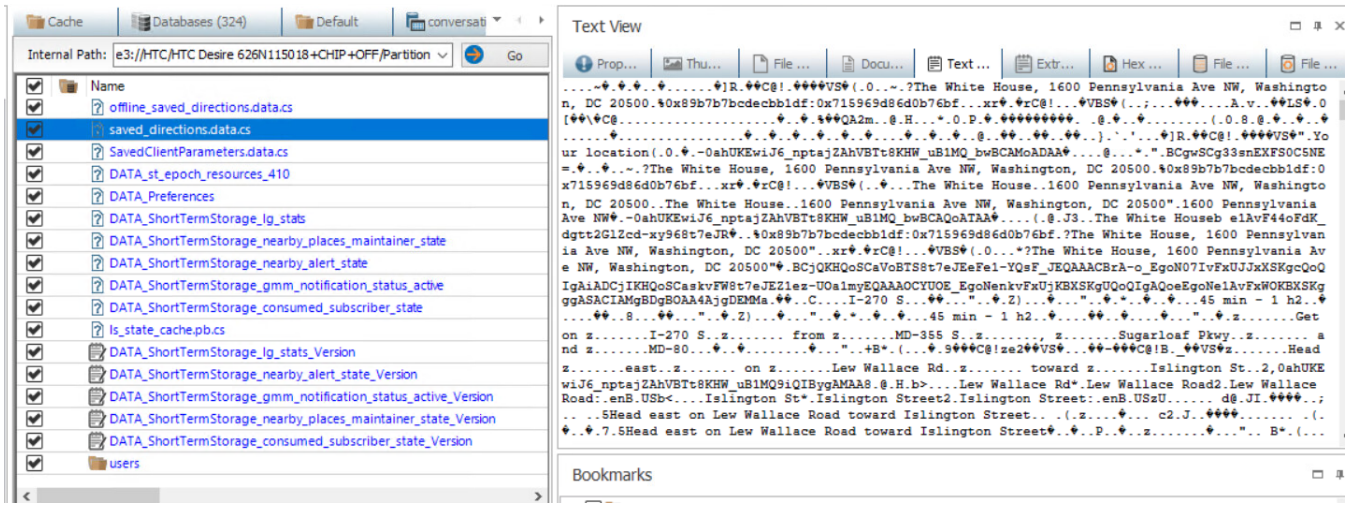
17. Is there any GPS data? If so, provide evidence.

Answer: Yes, there is evidence suggesting the presence of internet data, specifically related to Path and mapping services.

- **Location & travel (34)**: This item indicates data related to the user's movements and interactions with Path-based services.
    - **Google Maps**: The presence of "Google Maps" with 27 entries, along with "Google Maps Directions" and "Google Maps Saved Paths," strongly suggests the use of Google Maps for navigation and Path searches.
        - **Saved Location on Maps:** There are 2 map saved location found in the device.
        - **Path:** e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.google.android.apps.maps_114900/databases_123158/gmm_sync.db_124266/*binary_file/database/tables/sync_item_data/1-5
        - Both this latitude and longitude corresponds to 1234 Main street, Dallas, TX and 100 Bureau Dr, Gaithersburg, MD 20899



        - **Saved Map Directions (1)**: There is 1 evidence of saved data in the Maps app.
            - **Path**: e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.google.android.apps.maps_114900/files_123123?item=saved_directions.data.cs_123857



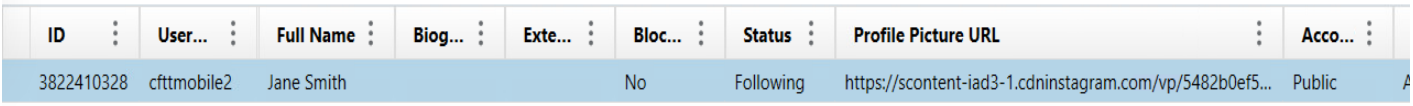
- **Google Maps Data(27): There are 27 google map search location**
  - **Path:** e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.google.android.apps.maps_114900/databases_123158/gmm_storage.db_124385/*binary_file/database/tables/gmm_storage_table/1-26

EVIDENCE (27)

Search Query	Start...	Latit...	Long...	Location Type
The+White+House+loc:+1600+Pennsylvania+Ave+z				
The+White+House+loc:+1600+Pennsylvania+Ave+NW,+Washington,+DC+20500,+USA		38.897676	-77.03653	Business
The+White+House+loc:+1600+Pennsylvania+Ave+NW,+Washington,+DC+20500,+USA		38.897676	-77.0365302	Business
The+White+House+loc:+1600+Pennsylvania+Ave+NW,+Washington,+DC+20500,+United+States		38.897676	-77.036529	Business
The+White+House+loc:+1600+Pennsylvania+Ave+NW,+Washington,+DC+20500		38.897676	-77.03653	Business
The White House loc: 1600 Pz				
The White House loc: 1600 Pennsylvania Ave NW, Washington, DC 20500, USA				Business
The White House loc: 1600 Pennsylvania Ave NW, Washington, DC 20500, United States				Business
The White House loc: 1600 Pennsylvania Ave NW, Washington, DC 20500				Business
The White House				Center of Map
The White H				
(%s,%s)				
'r a e','s'				Center of Map
'r a e','s'				Center of Map
'o'				
'o'				

18.Is there any social media data? If so, provide evidence.
Answer: Yes, there is social media data in the android device. This evidence is available in the list of items under the heading "SOCIAL NETWORKING," which shows presence of 245 artifacts in total. These items specifically reference data from various social media platforms:

- **Android Instagram Following** indicates about the account followed by user “cfttmobile2” whose name is “Jane Smith” on Instagram via an Android device. This piece of evidence can be found at the
  - **Path** “\data\com.instagram.android\shared_prefs\2922492216_usersBootstrapService.xml.”



ID	User...	Full Name	Biog...	Exte...	Bloc...	Status	Profile Picture URL	Acco...
3822410328	cfttmobile2	Jane Smith			No	Following	https://scontent-iad3-1.cdninstagram.com/vp/5482b0ef5...	Public

- **Android Instagram Posts** suggests that the user “cfttmobile1” whose name is “Jane cftt mobile” presence of data related to posts made by the user on Instagram from an Android device. The user has posted 4 images in total and the evidence can be found at the “\data\com.instagram.android\cache\MainFeed.json.0003 > json > feed_items[0] > media_or_ad > image_versions2 > candidates[0] > url, \data\com.instagram.android\cache\MainFeed.json.0003 > json > feed_items[0] > media_or_ad > taken_at, \data\com.instagram.android\cache\MainFeed.json.0003 > json > feed_items[0] > media_or_ad > device_timestamp, \data\com.instagram.android\cache\MainFeed.json.0003 > json > feed_items[0] > media_or_ad > user > username, \data\com.instagram.android\cache\MainFeed.json.0003 > json > feed_items[0] > media_or_ad > user > full_name, \data\com.instagram.android\cache\MainFeed.json.0003 > json > feed_items[0] > media_or_ad > user > profile_pic_url, \data\com.instagram.android\cache\MainFeed.json.0003 > json > feed_items[0] > media_or_ad > caption > text, \data\com.instagram.android\cache\MainFeed.json.0003 > json > feed_items[0] > media_or_ad > caption > pk, \data\com.instagram.android\cache\MainFeed.json.0003 > json >

feed_items[0] > media_or_ad > caption > user_id" having source at HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.instagram.android\cache\MainFeed.json.0003

Post ID	ID	User...	Full...	Com...	Text	Profile Picture URL	Dow...
17924235436053192	2922492216	cfttmobile1	cftt mobile		Jane	https://scontent-iad3-1.cdninstagram.com/vp/76e0...	
		cfttmobile1	cftt mobile			https://scontent-iad3-1.cdninstagram.com/vp/76e0...	
17896344211155635	2922492216	cfttmobile1	cftt mobile		Pic from Galaxy SIII mini - n115009	https://scontent-iad3-1.cdninstagram.com/vp/76e0...	
17864880064204439	2922492216	cfttmobile1	cftt mobile		Pic taken with Galaxy S III Mini :)	https://scontent-iad3-1.cdninstagram.com/vp/76e0...	

- **Android Instagram Users** likely refers to information about Instagram users the person interacted with or viewed on their Android device. There is only 1 such instance and the evidence's source is "HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.instagram.android\cache\MainFeed.json.0003"

ID	User...	Full...	Profile Picture URL	Dow...	Artifact type	Source
2922492216 (Last logged in)	cfttmobile1	cftt mobile	https://scontent-iad3-1.cdninstagram.com/vp/76e0...		Android Instagram Users	HTC Desire 626N115018+CH

- **Facebook Activity** point towards data associated with the user's Facebook activity, including their comments, contact list, and friends list.
    - **Facebook Comments:** There is once such evidence of the user commenting on Facebook whose evidence comes from Path "HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.instagram.android\cache\MainFeed.json.0003" and the source file is at "HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.facebook.katana\cache\graph_store_cache.08977bd0-be07-4b70-8308-fd386990c3a6.0\GraphStore.sqlite3"

Post ID	Artifact type	Source	Reco...	Dele...	Location	Evidence number
2067826459900117	Facebook Comments	HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (...	Parsing		Table: Objects(rowid: 3)	HTC Desire 626N115018+CHIP+OFF

- **Facebook Contacts:** There are 2 contacts found from the Facebook's contact list.
  - **Path:** "Table: contacts(internal_id: 1)" and "Table: contacts(internal_id: 2)" coming from the source file "e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/misc_155649/wifi_155663?item=wpa_supplicant.conf.bak_155725."

Profile ID	First...	Last...	Disp...	Picture URL	Pho...	Artifact type	Source
100007218342184	John	Smith	John Smith	https://scontent-iad3-1.xx.fbcdn.net/v/t1.0-1/c66.0.1...		Facebook Contacts	HTC Desire 626N115018+CHIP+OF
100007246184143	Jane	Smith	Jane Smith	https://scontent-iad3-1.xx.fbcdn.net/v/t1.0-1/c49.0.1...		Facebook Contacts	HTC Desire 626N115018+CHIP+OF

- **Facebook User/Friends:** There are 2 users found from the Facebook's friends/user list. Though both are the same users.
- **Path**: "HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.facebook.katana\app_light_prefs\com.facebook.katana\logged_in_100007218342184".

User ID	Frien...	Dis...	First...	Last...	Email(s)	User Image URL	I...	Ph...	Other
1000072183421...	User	John Smi...	John	Smith	cfttmobile1@gmail.com	https://scontent-iad3-1.xx.fbcdn.net/v/t1.0-1/...			
1000072183421...	User	John Smi...	John	Smith	cfttmobile1@gmail.com	https://scontent.xx.fbcdn.net/v/t1.0-1/c39.0.1...			

- **Instagram Direct Messages and Media** imply data from direct messages and media shared on Instagram. There are 3 direct messages recovered from Instagram.
  - **Path:** "Table: messages (_id: 6), Table: threads(_id: 6)", "Table: messages(_id: 7), Table: threads(_id: 6)" and "File Offset 63030" respectively. And Source "HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.instagram.android\databases\direct.db"

Sender	Artifact type	Message Date/Time	Type	Dire...	Location	Source
cfttmobile1	Instagram Direct Messages	2/15/2018 2:50:01.549 PM		Outgoing	Table: messages(_id: 6), Table: threads(_id: 6)	HTC Desire 626N115018+CHIP+OFF.00
cfttmobile1	Instagram Direct Messages	2/15/2018 5:39:44.111 PM	media_share	Outgoing	Table: messages(_id: 7), Table: threads(_id: 6)	HTC Desire 626N115018+CHIP+OFF.00
	Instagram Direct Messages	2/15/2018 5:39:44.111 PM	MEDIA_SHARE		File Offset 63030	HTC Desire 626N115018+CHIP+OFF.00

- **Instagram Media** imply to the media shared on Instagram. There are 88 media files recovered from Instagram. This evidence can be found in the source file “HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.instagram.android\cache\images\”, “HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.instagram.android\cache\images\”, “HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.instagram.android\cache\blur_icons”

Picture	MIM...	Created Date/Time	Last Accessed Dat...	Last Modified Dat...	Size...	Origi...	Origi...	Skin...
	image/jpeg	2/15/2018 5:36:59.000 PM	2/15/2018 5:36:59.000 PM	2/15/2018 5:36:59.000 PM	9,479	243	324	52.1
	image/jpeg	2/15/2018 5:37:04.000 PM	2/15/2018 5:37:04.000 PM	2/15/2018 5:37:05.000 PM	37,634	1080	1080	34.8
	image/jpeg	2/15/2018 5:39:36.000 PM	2/15/2018 5:39:36.000 PM	2/15/2018 5:39:36.000 PM	188,327	1458	1458	34.7
	image/jpeg	2/15/2018 5:36:28.000 PM	2/15/2018 5:36:28.000 PM	2/15/2018 5:36:28.000 PM	6,625	150	150	59.3
	image/jpeg	2/15/2018 5:36:29.000 PM	2/15/2018 5:36:29.000 PM	2/15/2018 5:36:29.000 PM	32,098	540	540	86.2
	image/jpeg	2/15/2018 5:36:29.000 PM	2/15/2018 5:36:29.000 PM	2/15/2018 5:36:29.000 PM	63,336	750	1248	31.4
	image/jpeg	2/15/2018 5:36:28.000 PM	2/15/2018 5:36:28.000 PM	2/15/2018 5:36:28.000 PM	35,204	750	750	13.8
	image/jpeg	2/15/2018 5:36:29.000 PM	2/15/2018 5:36:29.000 PM	2/15/2018 5:36:29.000 PM	51,268	750	750	88.5
	image/jpeg	2/15/2018 5:36:29.000 PM	2/15/2018 5:36:29.000 PM	2/15/2018 5:36:29.000 PM	50,741	750	750	0.0
	image/jpeg	2/15/2018 5:36:32.000 PM	2/15/2018 5:36:32.000 PM	2/15/2018 5:36:32.000 PM	10,598	240	216	0.8
	image/jpeg	2/15/2018 5:36:32.000 PM	2/15/2018 5:36:32.000 PM	2/15/2018 5:36:32.000 PM	12,348	240	240	20.1
	image/jpeg	2/15/2018 5:36:32.000 PM	2/15/2018 5:36:32.000 PM	2/15/2018 5:36:32.000 PM	7,427	240	240	0.0
	image/jpeg	2/15/2018 5:36:32.000 PM	2/15/2018 5:36:32.000 PM	2/15/2018 5:36:32.000 PM	9,653	240	240	22.3
	image/jpeg	2/15/2018 5:36:32.000 PM	2/15/2018 5:36:32.000 PM	2/15/2018 5:36:32.000 PM	11,808	240	240	16.8
	image/jpeg	2/15/2018 5:36:32.000 PM	2/15/2018 5:36:32.000 PM	2/15/2018 5:36:32.000 PM	6,207	240	240	88.8
	image/jpeg	2/15/2018 5:36:32.000 PM	2/15/2018 5:36:32.000 PM	2/15/2018 5:36:32.000 PM	9,174	240	240	86.3

- **LinkedIn Profile** signifies the presence of data from the user's LinkedIn profile. There is 1 LinkedIn profile available on the device.
  - **Path:** “HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.linkedin.android\shared_prefs\auth_library_prefs.xml”.

UserName	First...	Last...	Full...	Summary	Artifact...	Source	Reco...
cfttmobile1@gmail.com	John	Smith	John Smith	Computer Scientist at TSIN	LinkedIn Profile	HTC Desire 626N115018+CHIP+OFF.001 - Partition...	Parsing

- **Twitter Direct Messages, Tweets and Users** suggest the existence of data related to data such as direct messages, Users on device and tweets on Twitter.

    - **Twitter Direct Messages**: There are 10 evidence of direct messages which is a conversation between 2 users named “John Smith” and “Jane Smith”.
        - **Path:** “Table: conversations(rowid: 1), Table: conversation_entries(rowid: 1), Table: users(rowid: 1), Table: users(rowid: 2), Table: conversation_participants(rowid: 1)” at the source “HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.twitter.android\databases\2249111010-49.db”

Text	Send...	Reci...	Sent/Received Da...	Dire...	Send...	Send...	Reci...	Reci...
Now g4 is here	2249111010	2249114522	3/2/2016 8:32:59.000 PM	Sent	John Smith	cfttmobile1	Jane Smith	cfttmobile2
Hello geefour	2249114522	2249111010	3/2/2016 8:34:02.000 PM	Received	Jane Smith	cfttmobile2	John Smith	cfttmobile1
Hey Jane meet S4	2249111010	2249114522	8/30/2016 1:42:05.000 AM	Sent	John Smith	cfttmobile1	Jane Smith	cfttmobile2
https://t.co/TVwzxepgOP twitter.com/cfttmobile1/s...	2249111010	2249114522	8/30/2016 2:29:22.000 PM	Sent	John Smith	cfttmobile1	Jane Smith	cfttmobile2
Hey Jane this is s4s brother	2249111010	2249114522	8/30/2016 3:35:46.000 PM	Sent	John Smith	cfttmobile1	Jane Smith	cfttmobile2
	2249111010	2249114522	8/30/2016 3:37:37.000 PM	Sent	John Smith	cfttmobile1	Jane Smith	cfttmobile2
	2249111010	2249114522	8/30/2016 3:37:40.000 PM	Sent	John Smith	cfttmobile1	Jane Smith	cfttmobile2
	2249111010	2249114522	8/30/2016 3:37:43.000 PM	Sent	John Smith	cfttmobile1	Jane Smith	cfttmobile2
Hi Jane, texting from Galaxy SIII mini - n115016 this...	2249111010	2249114522	2/9/2018 12:41:34.000 AM	Sent	John Smith	cfttmobile1	Jane Smith	cfttmobile2
Cheers from Galaxy SIII mini-n115009	2249111010	2249114522	2/9/2018 1:34:08.000 AM	Sent	John Smith	cfttmobile1	Jane Smith	cfttmobile2

    - **Twitter Tweets:** There are 105 evidence of tweets found on the android device.
        - **Path**: “Table: statuses(_id: 1)” with different id starting from 1 to 10, having the source file at “HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.twitter.android\databases\2249111010-49.db”

Auth...	Status ID	Created Date/Time	Tweet	Source	Location
2249114522	464772515098017792	5/9/2014 2:22:57.000 PM	Happy Friday! From samsung convoy 3 5/5/2014	HTC Desire 626N115018+CHIP+OFF.0...	Table: statuses(_id: 1)
2249114522	697132702026194944	2/9/2016 6:59:22.000 PM	@cfttmobile1 nice to meet your brother	HTC Desire 626N115018+CHIP+OFF.0...	Table: statuses(_id: 2)
2249111010	463302524368601088	5/5/2014 1:01:44.000 PM	Happy cinco de mayo!!!	HTC Desire 626N115018+CHIP+OFF.0...	Table: statuses(_id: 3)
2249114522	415117281492889601	12/23/2013 1:50:47.000 PM	cfttmobile2 wondering whats up with this weather!	HTC Desire 626N115018+CHIP+OFF.0...	Table: statuses(_id: 4)
2249114522	774206070680018945	9/9/2016 11:21:25.000 AM	This is HTC One VX for JTAG! @cfttmobile1	HTC Desire 626N115018+CHIP+OFF.0...	Table: statuses(_id: 5)
2249111010	415118243368800256	12/23/2013 1:54:36.000 PM	@cfttmobile2 hey Jane - how are you today?	HTC Desire 626N115018+CHIP+OFF.0...	Table: statuses(_id: 6)
2249114522	463325747575525376	5/5/2014 2:34:01.000 PM	Today a bunch of people will be celebrating 5 de ma...	HTC Desire 626N115018+CHIP+OFF.0...	Table: statuses(_id: 7)
2249111010	700016934402813952	2/17/2016 6:00:17.000 PM	https://t.co/3tgrtfG1NI	HTC Desire 626N115018+CHIP+OFF.0...	Table: statuses(_id: 8)
2249111010	705052773075832832	3/2/2016 3:30:55.000 PM	@cfttmobile2 galaxy s6 edge on board	HTC Desire 626N115018+CHIP+OFF.0...	Table: statuses(_id: 9)
2249111010	462296770945744896	5/2/2014 6:25:13.000 PM	@cfttmobile2 Pontiacs are slow vehicles	HTC Desire 626N115018+CHIP+OFF.0...	Table: statuses(_id: 10)
2249111010	413381670423638016	12/18/2013 6:54:05.000 PM	Tweeting from HTC one	HTC Desire 626N115018+CHIP+OFF.0...	Table: statuses(_id: 11)
2249111010	462296639659864064	5/2/2014 6:24:42.000 PM	Today's date is may 2 2014	HTC Desire 626N115018+CHIP+OFF.0...	Table: statuses(_id: 12)
2249111010	692688247105912833	1/28/2016 12:38:42.000 PM	HTC sensation xp for jtag.	HTC Desire 626N115018+CHIP+OFF.0...	Table: statuses(_id: 13)
2249111010	692687852128198657	1/28/2016 12:37:08.000 PM	@cfttmobile2 hey Jane this is HTC sensation xp for j...	HTC Desire 626N115018+CHIP+OFF.0...	Table: statuses(_id: 14)
2249114522	699948998161997825	2/17/2016 1:30:20.000 PM	Hey @cfttmobile1 - nice iPad pro https://t.co/SG4Q...	HTC Desire 626N115018+CHIP+OFF.0...	Table: statuses(_id: 15)
2249114522	463376591239016449	5/5/2014 5:56:03.000 PM	White sheet of paper :) http://t.co/EvWhRjei0c	HTC Desire 626N115018+CHIP+OFF.0...	Table: statuses(_id: 16)

- **Twitter Users**: There are 27 instances of user activity on Twitter
  - **Path:** “Table: users(_id: 1)” having id starting from 1 till 27. The source file of this evidence is “HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.twitter.android\databases\2249111010-49.db”.

User ID	User Name	F...	Profile Created Date...	Description	Web URL
2249111010	cfttmobile1		12/16/2013 6:09:11.000 PM		
807095	nytimes		3/2/2007 8:41:42.000 PM	Where the conversation begins. Follow for breaking...	http://t.co/ahvuWqicF9
21001534	audible_com		2/16/2009 4:50:28.000 PM	The dedicated account for Audible—audiobooks &...	https://t.co/lkHFTpyYRM
19103481	Uber		1/17/2009 6:37:59.000 AM	Connecting you with the people, places, and things...	http://t.co/11elV5LX3Z
776196808909336577	madebygoogle		9/14/2016 11:11:55.000 PM	Devices that work together to make life run smooth...	https://t.co/BkJ1P3phme
12092012	VMware		1/11/2008 12:39:51.000 AM	#VMware, a global leader in cloud infrastructure and...	https://t.co/wfnvZi2IjU
18909186	TurkishAirlines		1/12/2009 6:15:16.000 PM	Thanks for visiting the airline that flies to more coun...	http://t.co/apWF0veYyu
895751473811791872			8/10/2017 8:59:28.000 PM		
14219877	Toyota		3/25/2008 9:45:13.000 PM	Official tweets from Toyota #LetsGoPlacesIIJj LetsGo...	https://t.co/6mtGimUaaK
76117579	SAP		9/21/2009 7:31:15.000 PM	Helping the world run better and improving people'...	http://t.co/Ukh9Sw9BIq
82382893	MandT_Bank		10/14/2009 3:17:15.000 PM	The official channel for news, community updates an...	https://t.co/qNJjuEFy4D
207647013	bittripfan		10/25/2010 7:05:38.000 PM		
769181159834071040	Arunodhaya62		8/26/2016 2:34:14.000 PM	#Msdian..... Lv u #mahii.... [lf][lf]#dhfm...l[tab]IJjMsdi...	
77682426	ahkaromi		9/27/2009 7:01:51.000 AM		
723126626	MileIQ		7/29/2012 1:17:41.000 AM	MileIQ automatically logs your drives and calculates...	http://t.co/5zGzgvx3kP
15991258	Xerox		8/26/2008 2:33:30.000 AM	#SetThePageFree IIJjSetThePageFreeXXIXXIIXI...	http://t.co/lvSrfHhpbE

Overall, this list clearly demonstrates the presence of social media data from various platforms, potentially offering insights into the user's online activities and connections.

CYFI 330 - 700 HTC Quiz (1)

The HTC Desire mobile device's contents have been imaged and extracted and you uploaded it to your OneDrive. You are back at the office and ready to begin the tedious process of recovering evidence for your extortion case. The evidence file is the same as the HTC pre-quiz you started last week. Please give me a written response, screenshot(s) and path(s) for every question. Don't even think about asking me for extension or turning this in late.

1. Show the email account and telephone number and profile pic for user account1

Answer: The telephone number of the account associated with the account is "**+1(888)777-1212**" and the email address is "**cfttmobile1@gmail.com**." and the profile picture is

- **Path:** e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.facebook.katana_114855/cache_115277/image_123449/v2.ols100.1_123450/39_131309?item=7FUyCoBGFRA2gBDvLp0O-y7nW-Q.cnt_131310

Based on the given hint for evidence related to "user account1" with the phone number +1...5551212 and the email address useraccount1@gmail.com.

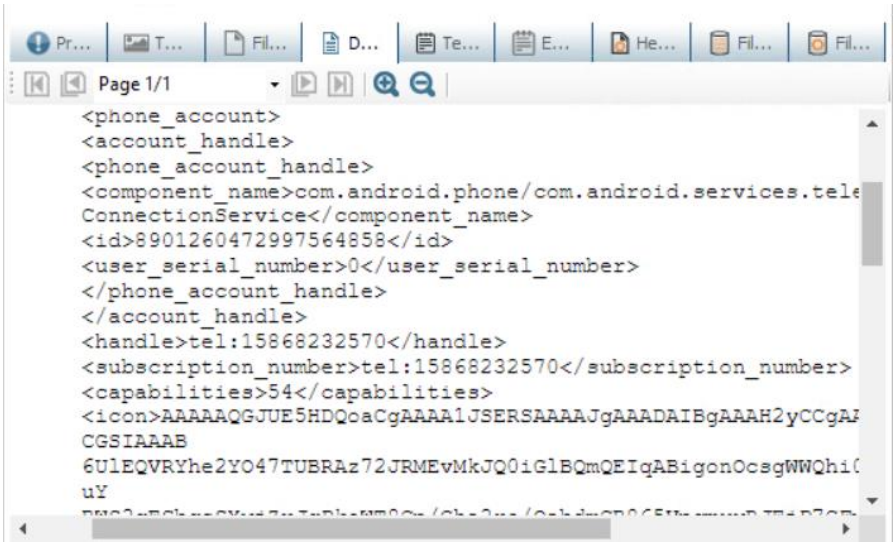
Approach:

- We will search for these identifiers within the extracted data, particularly in areas where account information is typically stored, such as databases or configuration files.
- Once we identify relevant entries, we'll attempt to locate any associated profile pictures.

2. What is the ICCID number of this device?

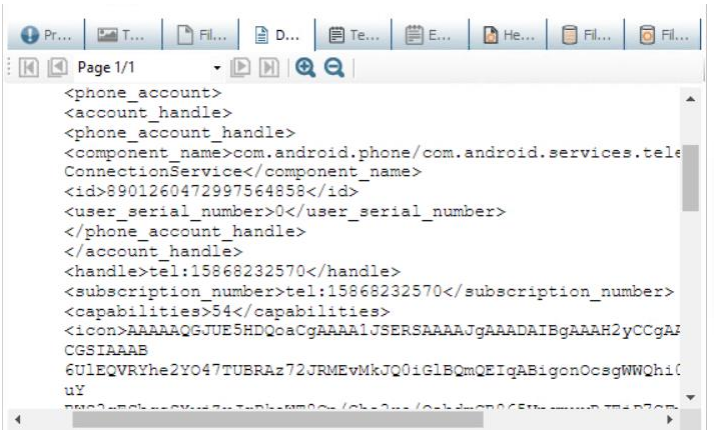
Answer: The ICCID of the device is "**8901260472997564858".** It can be found in a file named "**siminfo**" inside the "**telephony.db"** database. The **telephony.db** is an SQLite database that stores various information related to the device's telephony functions, including call logs, SMS messages, carrier settings, and SIM card details. And the **siminfo** table specifically holds information about the Subscriber Identity Module (SIM) card inserted in the device.

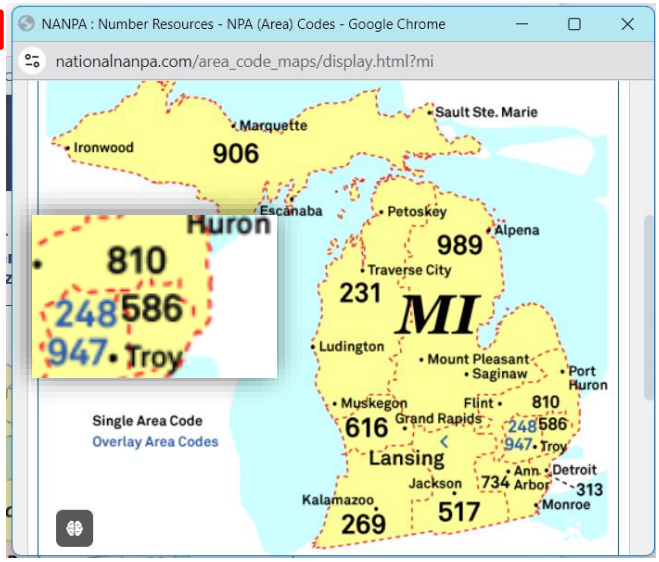
- **Path: e3**: //HTC/HTC Desire 626N115018+CHIP+OFF/Partition



Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.android.providers.telephony_114811/databases_114987/telephony.db_115129/*binary_file/database/tables/siminfo/1-2

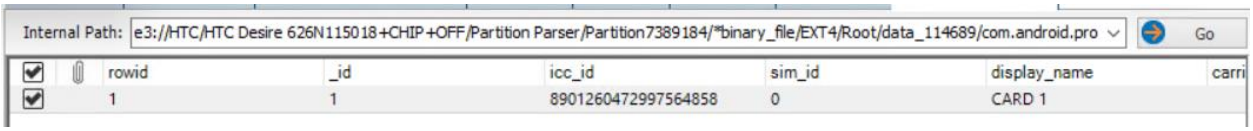
3. You indicated the telephone number of this device in the pre-quiz. What geographic area is the area code registered?





Answer: The phone number is "**+1 (586)823-2570**" and the geographic location is **Macomb County in Michigan, USA**. Some major cities within this area code include **Warren, Sterling Heights, and St. Clair Shores**. The phone number is recovered from the following location:

- **Path:** e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.android.server.telecom_114809/files_114982?item=phone-account-registrar-state.xml_116193

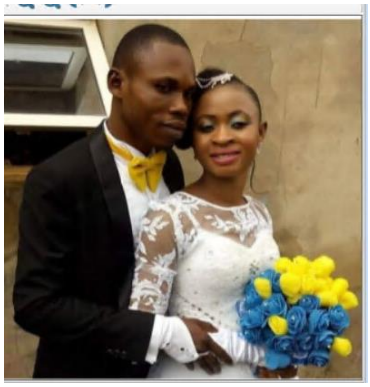
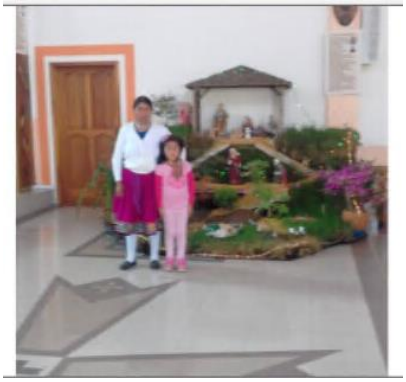


- **Area code verification from the website:** https://nationalnanpa.com/area_code_maps/display.html?mi

The telephone area code map of Michigan.

4. Show images of any three persons (do NOT use Jimi Hendrix or Steven Ray Vaugh)

Answer: The images of the person found in this device are not in **.jpg** format but they are in .clean format .A **.clean** file extension associated with an HTC Desire device typically relates to temporary or junk files created by the device's cleaning or optimization tools, such as the Boost+ app. These files are meant to help manage storage space by removing unnecessary data. he most plausible explanation is that it's a **proprietary or non-standard file format** specific to either:

A. **HTC's Image Processing:** HTC might have used the ".clean" extension for images that have undergone some form of processing or optimization within their camera app or gallery software. This could involve noise reduction, sharpening, or other enhancements applied before saving the image.
B. **Third-Party App:** It's also possible that a third-party app installed on the HTC Desire 626 used the ".clean" extension for its own image storage or processing.

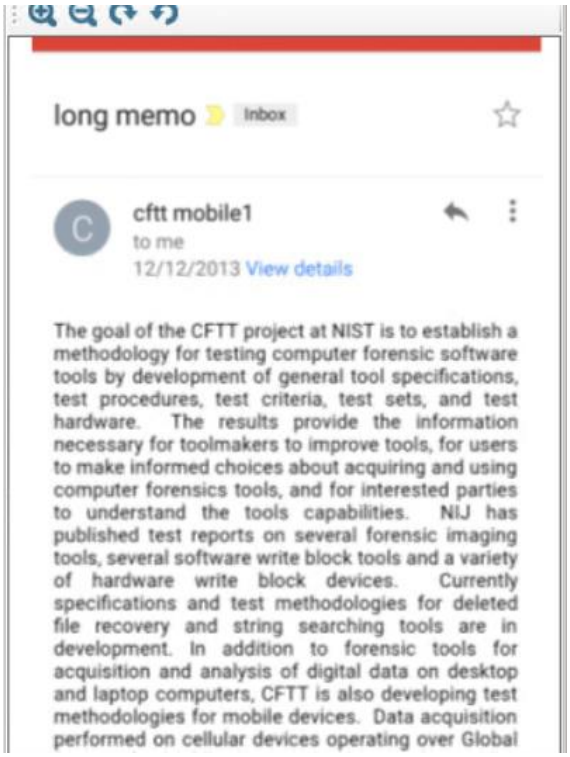
- **Path**: e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.facebook.katana_114855/cache_115277/image_123449/v2.ols100.1_123450/6_131261?item=E5cYwGzA3k0kfN6fxjc96XzXRuU.cnt_131323
- **Path**: e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.facebook.katana_114855/cache_115277/image_123449/v2.ols100.1_123450/6_131261?item=GfVMCuQL2Xk2FQATw22clKyHNKg.cnt_131313
- **Path**: e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.facebook.katana_114855/cache_115277/image_123449/v2.ols100.1_123450/62_131333?item=cKCHebSK6oZbJ-kuKEYpsqTHvTo.cnt_131334

5. There is a long memo in the evidence. Please show an excerpt of this memo
Answer: The excerpt of the memo found is "**The goal of the CFTT project at NIST is to establish a methodology for testin...**"

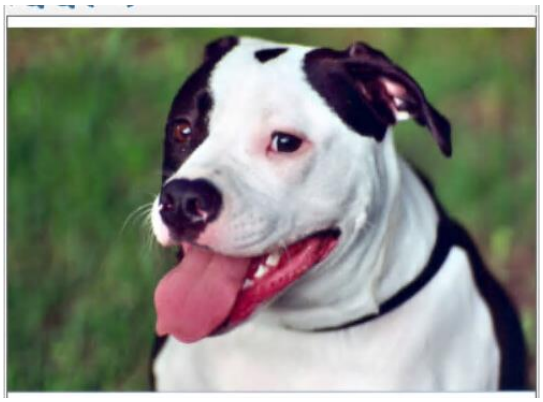
- **Path:** e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.google.android.gm_114860/databases_115024/mailstore.cfttmobile1@gmail.com.db_115862/*binary_file/database/tables/messages/1-38?item=row_35

6. There are some active images. Show two of these. Hint: one jpg and one gif
Answer: In the context of data acquired from an Android device, "active images" generally refer to **images that were recently accessed or viewed by the user**. These could be photos or animated GIFs that were opened in the device's gallery, image viewer app, or even within social media or messaging applications. This also means that these images are not deleted (i.e. have allocated space)and have a specific creation, access and modification time. The active images found in the device are:

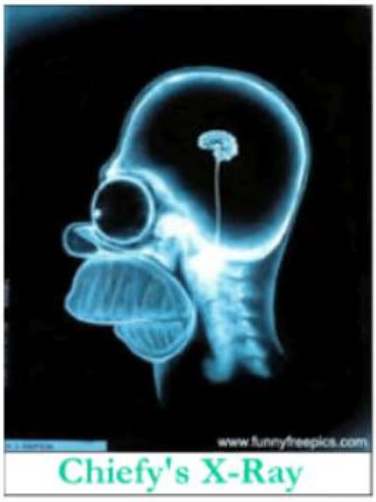
- **GIF image**:



  - **Name**: Homer.gif
  - **Path**: e3://HTC/HTC Desire



626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/media_147458/0_147457/Download_147490?item=homer.gif_147589



- **Verification:**

➢ **JPEG image**:

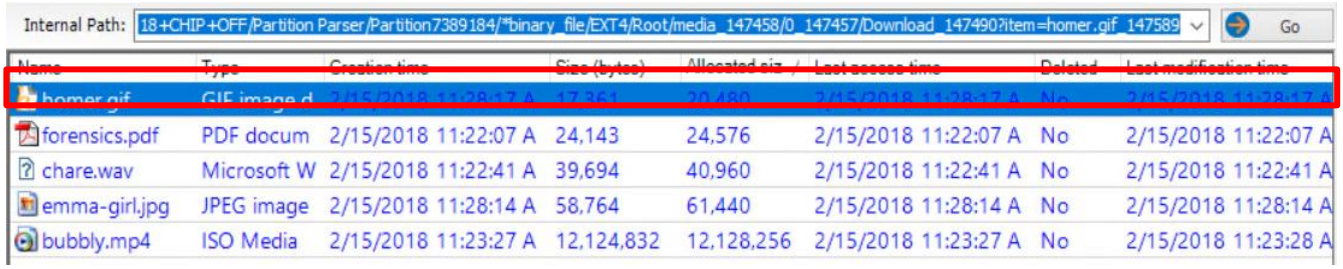
Internal Path: 18+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/media_147458/0_147457/Download_147490?item=homer.gif_147589 Go

Name	Type	Creation time	Size (bytes)	Allocated siz /	Last access time	Deleted	Last modification time
homer.gif	GIF image d	2/15/2018 11:28:17 A	17,361	20,480	2/15/2018 11:28:17 A	No	2/15/2018 11:28:17 A
forensics.pdf	PDF docum	2/15/2018 11:22:07 A	24,143	24,576	2/15/2018 11:22:07 A	No	2/15/2018 11:22:07 A
chare.wav	Microsoft W	2/15/2018 11:22:41 A	39,694	40,960	2/15/2018 11:22:41 A	No	2/15/2018 11:22:41 A
emma-girl.jpg	JPEG image	2/15/2018 11:28:14 A	58,764	61,440	2/15/2018 11:28:14 A	No	2/15/2018 11:28:14 A
bubbly.mp4	ISO Media	2/15/2018 11:23:27 A	12,124,832	12,128,256	2/15/2018 11:23:27 A	No	2/15/2018 11:23:28 A

- **Name**: emma-girl.jpg
- **Path**: e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/media_147458/0_147457/Download_147490?item=emma-girl.jpg_147588

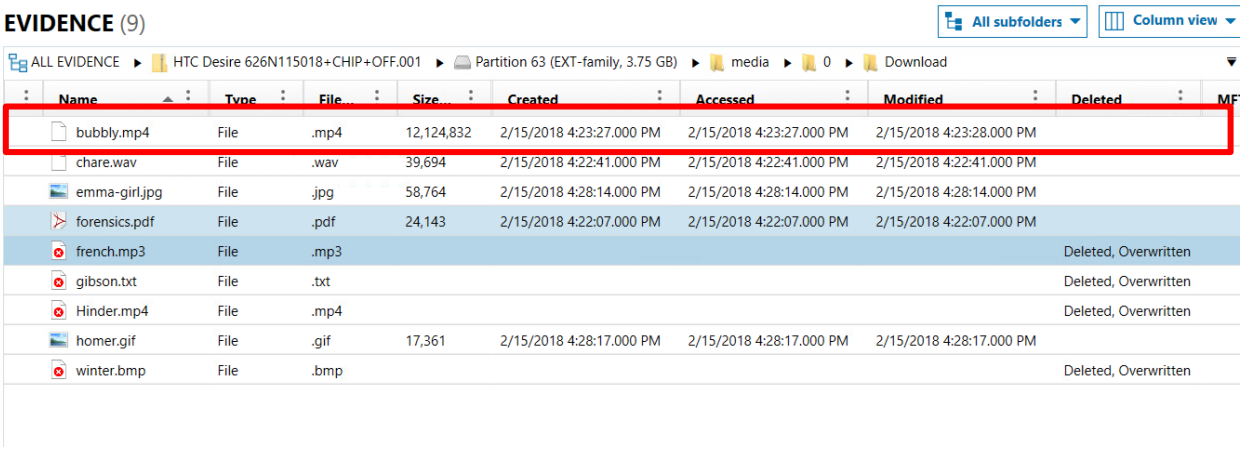
- **Verification**:

7. There is a deleted audio file. Show what type of file this is.



Answer: The name of the deleted audio file is "**French**", and it is in mp3 format. An **MP3** file is a digital audio file that uses a compression algorithm to reduce the size of the original audio data while maintaining acceptable sound quality. This compression makes MP3 files much smaller than uncompressed formats like WAV, allowing for easier storage and transfer.

- **Path:** HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\media\0\Download\french.mp3



8. There is a deleted image file in an 'old school' format i.e. NOT jpg format. Show this image and name the format.

Answer: "**Old school**" image formats generally refer to file formats that were popular in the early days of digital imaging but have since been largely replaced by more modern and efficient formats like JPEG and PNG. Some examples of these older formats are **BMP (Bitmap), GIF (Graphics Interchange Format), TIFF (Tagged Image File Format), PCX (Picture Exchange) and TGA (Truevision TGA).**
The images found in this device are BMP and GIF. During the analysis, a deleted image file named "**winter.bmp**" was recovered. This image utilized the **BMP** format, which is considered a legacy or "old-school" format compared to modern formats like JPEG. The specific file path where this image was found is:

- **Path:** HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\media\0\Download\winter.bmp

- **BMP**, which stands for Bitmap, is an uncompressed image format that stores pixel data directly. This results in high-quality images but also leads to larger file sizes compared to compressed formats. The presence of a BMP image in this case might suggest that the image is older or originated from a system that primarily used this format.

ALL EVIDENCE ▸ HTC Desire 626N115018+CHIP+OFF.001 ▸ Partition 63 (EXT-family, 3.75 GB) ▸ media ▸ 0 ▸ Download

Name	Type	File...	Size...	Created	Accessed	Modified	Deleted	MFT...
forensics.pdf	File	.pdf	24,143	2/15/2018 4:22:07.000 PM	2/15/2018 4:22:07.000 PM	2/15/2018 4:22:07.000 PM		
chare.wav	File	.wav	39,694	2/15/2018 4:22:41.000 PM	2/15/2018 4:22:41.000 PM	2/15/2018 4:22:41.000 PM		
bubbly.mp4	File	.mp4	12,124,832	2/15/2018 4:23:27.000 PM	2/15/2018 4:23:27.000 PM	2/15/2018 4:23:28.000 PM		
emma-girl.jpg	File	.jpg	58,764	2/15/2018 4:28:14.000 PM	2/15/2018 4:28:14.000 PM	2/15/2018 4:28:14.000 PM		
homer.gif	File	.gif	17,361	2/15/2018 4:28:17.000 PM	2/15/2018 4:28:17.000 PM	2/15/2018 4:28:17.000 PM		
gibson.txt	File	.txt					Deleted, Overwritten	
french.mp3	File	.mp3					Deleted, Overwritten	
Hinder.mp4	File	.mp4					Deleted, Overwritten	
winter.bmp	File	.bmp					Deleted, Overwritten	

9. A social media account belonging to John Doe is located in the evidence. Show the profile pic.

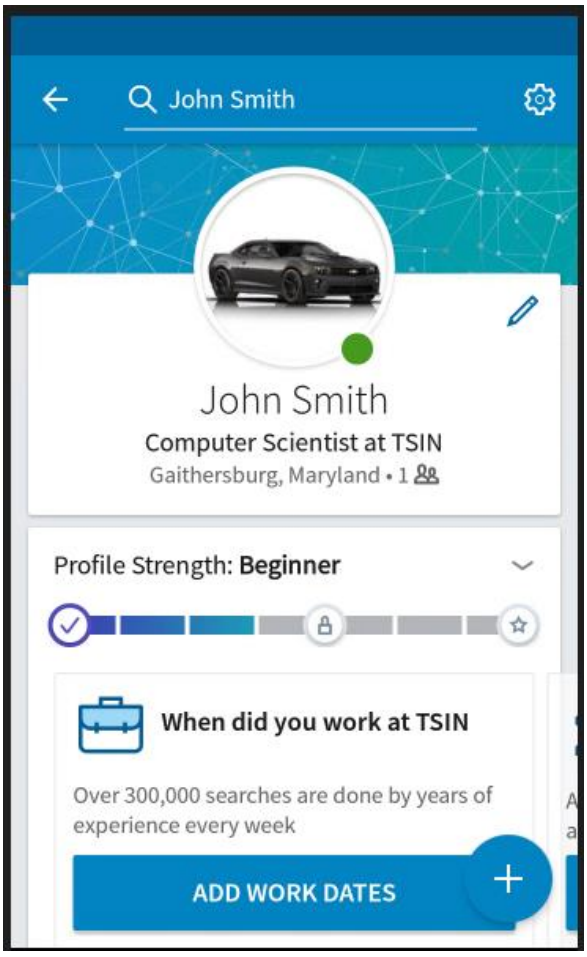
Answer: **John Doe (male)** and **Jane Doe (female)** are multiple-use placeholder names that are used in the United States when the true name of a person is unknown or is being intentionally concealed. In the context of law enforcement in the United States, such names are often used to refer to a corpse whose identity is unknown or cannot be confirmed. These names are also often used to refer to a hypothetical "everyman" in other contexts, like John Q. Public or "Joe Public". There are many variants to the above names, including **John (or Richard)/Jane Roe, John/Jane Smith, John/Jane Bloggs, and Johnie/Janie Doe or just Baby Doe for children.**

Thus, here John Doe and John Smith are being used to refer to the same person. The evidence of the social media login on **LinkedIn** points to an account belonging to John Smith, and the login activity log further strengthens the association of this account with the individual under investigation

- **Social media app**: LinkedIn
- **Login verification**
  - **File name**: linkedInPrefsName.xml
  - **Path**: e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.linkedin.android_139400/shared_prefs_140167?item=linkedInPrefsName.xml_140227

- **Profile photo name:** profile_pic.png
- **Path**: e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.linkedin.android_139400/files_140166/sso_140201?item=profile_pic.png_140203

- **Evidence of image being used as LinkedIn profile picture by John Smith**:



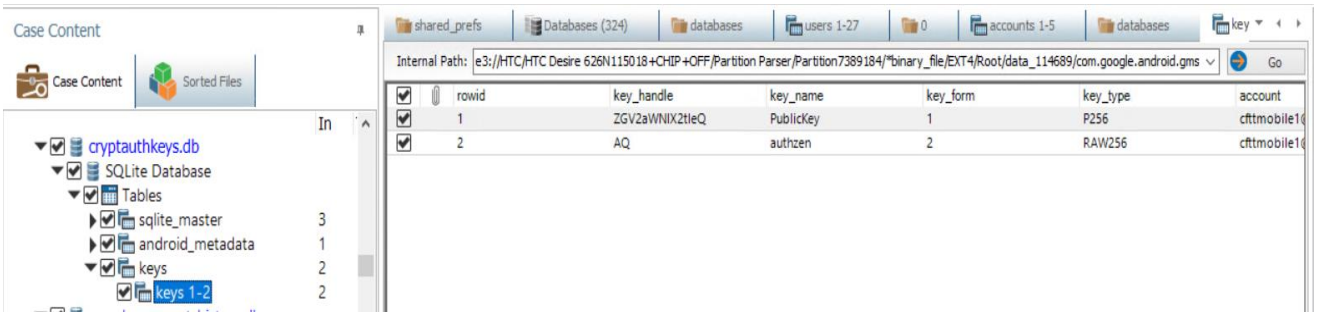
10. Your HTC evidence and all Android devices have two primary types of memory: 1. Volatile (RAM), 2. Non-Volatile (NAND flash) memory. From which of these two types of memory can I find things like passwords, encryption keys, usernames, or App data. Can you show an example of this in an exhibit? You must answer the question but if you can't show me an example you will still get full credit. *If you show me an example, then I may give you extra credit.*

Answer: You can find remnants of passwords, encryption keys, usernames, and app data in both volatile (RAM) and non-volatile (NAND flash) memory, although the likelihood and nature of the data differ between them.

1. **Volatile Memory (RAM)**
   - **RAM** is volatile, meaning its contents are lost when the device loses power. Capturing a live image or memory dump is crucial for preserving this type of evidence. Thus, it is more likely to contain remnants of sensitive data like passwords, encryption keys, and usernames, especially if the device was recently used or is in an active state. This is because RAM is the device's working memory where data is actively processed and stored temporarily.
   - **Example:** If a user recently entered a password, that password might still exist in plaintext within RAM until it is overwritten by other data. Similarly, encryption keys used to decrypt files might be temporarily present in memory while the device is actively using them.

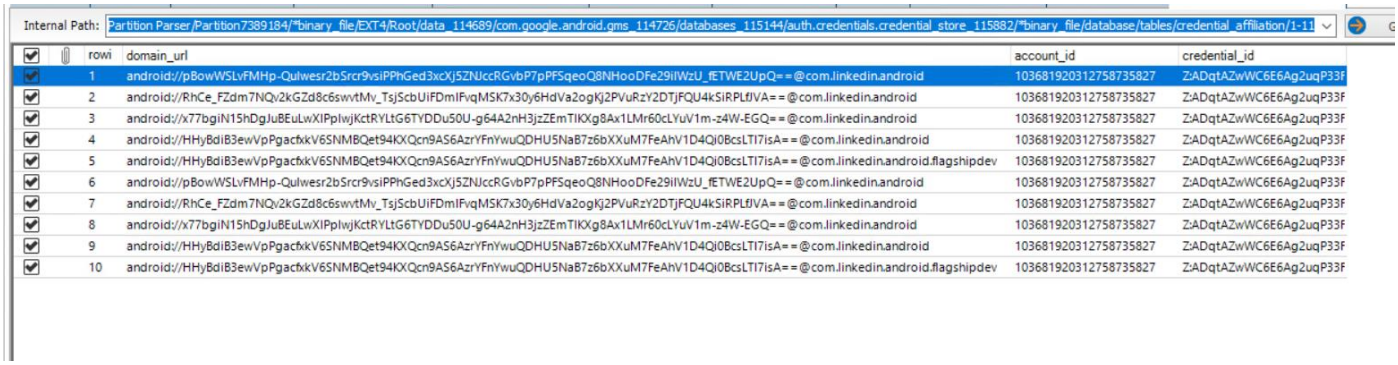
2. **Non-Volatile Memory (NAND flash)**

- **NAND flash** memory is the primary storage for user data, app installations, and system files. NAND flash memory is persistent, meaning it retains data even when the device is powered off. It's less likely to contain sensitive information in plaintext as passwords and encryption keys are usually stored in hashed or encrypted formats. However, remnants of these data types might still be found in unallocated space or through careful analysis of app data and system files.
- A forensic analysis of the /data/data directory on the HTC Desire 626 uncovers a database file belonging to a password manager app, containing encrypted passwords. While the passwords themselves are not directly accessible without the decryption key, their presence suggests the user stored sensitive login credentials.
- **Exhibit**: The forensic image of the HTC Desire 626 contains encryption keys *(master_key and public_key)* associated with the "**cfttmobile1@gmail.com**" account, found under the . These keys, if valid and accessible, could be used to decrypt data protected by the corresponding encryption schemes.



- **Path:** e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.google.android.gms_114726/databases_115144/cryptauthkeys.db_115513/*binary_file/database/tables/keys/1-3

The image provides a clear example of encryption keys found within the non-volatile storage of an Android device. These keys are crucial for protecting user data and accessing encrypted information.



- **Path:** e3://HTC/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.google.android.gms_114726/databases_115144/auth.credentials.credential_store_115882/*binary_file/database/tables/credential_affiliation/1-11

This image also contains a database table (credential within the affiliation folder) that stores information about user accounts and their associated credentials on various online services (like LinkedIn). While the actual passwords or keys might not be directly visible in this table, their presence indicates that the device stores sensitive authentication data in its non-volatile memory.