

CYFI 330-700 HTC Desire Assignment

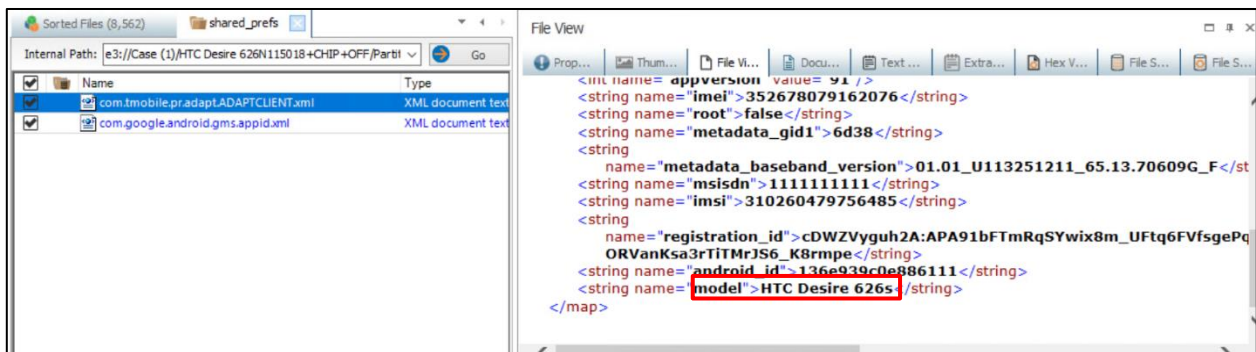
The HTC Desire mobile device's contents have been imaged and extracted and you uploaded it to your OneDrive. You are back at the office and ready to begin the tedious process of recovering evidence for your extortion case. The evidence file is named HTS Desire 626 N115018 CHIPOFF.001. This file size 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: **HTC Desire 626s**

Location: e3://Case (1)/HTC Desire 626N115018+CHIP+OFF/Partition

Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.tmobile.pr.adapt_114777/shared_prefs_115191?item=com.tmobile.pr.adapt.ADAPTCLIENT.xml_116137



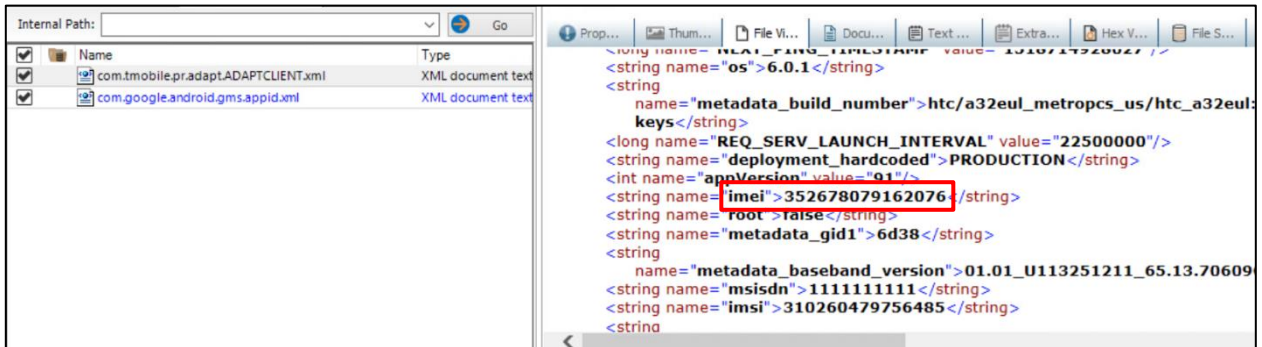
Reason: The *com.tmobile.pr.adapt.ADAPTCLIENT.xml* file is part of the shared preferences of the **T-Mobile Adapt** app. These types of files are typically generated and managed by the system or the app itself. Since this file stores important app-specific information, including device metadata, it's a reliable source for details like the IMEI, model, and Google account status.

2. What is the IMEI of this device

Answer: 352678079162076

Location: e3://Case (1)/HTC Desire 626N115018+CHIP+OFF/Partition

Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.tmobile.pr.adapt_11477/shared_prefs_115191?item=com.tmobile.pr.adapt.ADAPTCLIENT.xml_116137



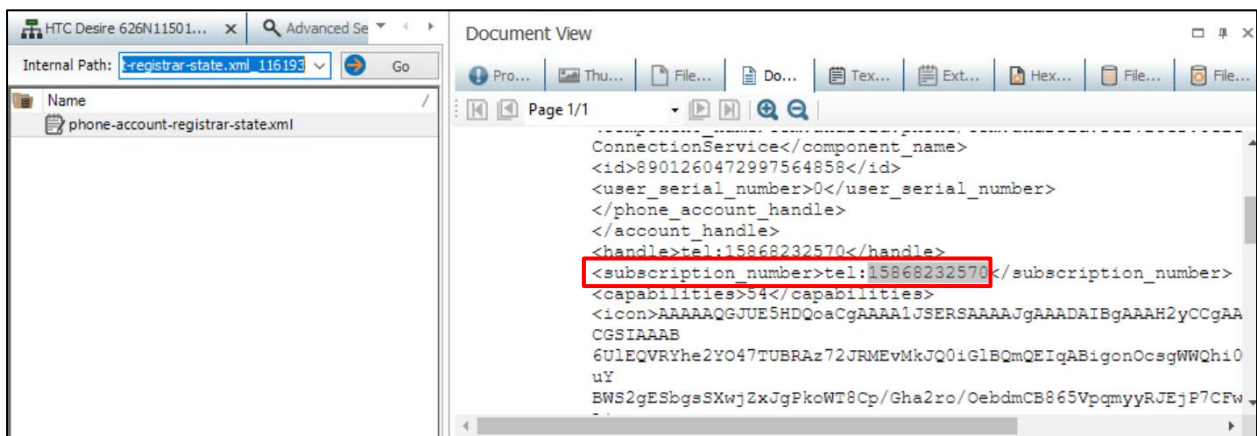
Reason: The *com.tmobile.pr.adapt.ADAPTCLIENT.xml* file is part of the shared preferences of the **T-Mobile Adapt** app. These types of files are typically generated and managed by the system or the app itself. Since this file stores important app-specific information, including device metadata

3. What is the telephone number of this device?

Answer: 15868232570

Location: e3://Case (1)/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



Reason: The *phone-account-registrar-state.xml* file is part of the Telecom system service in Android. It's used by the Android OS to manage phone account registrations, handle calls, and store important telephony data such as phone numbers and subscription information.

4. State the two famous persons name, telephone number, email, address and telephone number (the internal memory locations may not give you all of this info)

Answer:

Contact 1: Stevie Ray Vaughn / Stevie Ray Vaughan

Phone Number: 1234567890

Email: stevie@srv.com

Address: Home: 1234 Main Street, Dallas, TX

Location: HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.google.android.gms\databases\icing_contacts.db

Artifacts

COMMUNICATION

Android Call Logs

Android Contacts

Android Facebook Messages

Android SMS/MMS

Facebook Messenger Messages

Facebook Messenger Users

TextPlus Calls

SOCIAL NETWORKING

EVIDENCE (21)

Column view

ARTIFACTS	MOBILE	Display Name	Phone Number(s)	Email Address(es)	Address	Website	Status
		Customer Care	7691234560	hendrix@experienced.com		www.jimihendrix.com	Yes
		Jimi Hendrix	Mobile: 7691234560	Home: hendrix@experienced.com			
		John Bonham	(987) 876-7654				No
		John Jacob Jingle Heimer Schmidt That's My Name T...	8988675309				No
		John Jacob Jingle Heimer Schmidt That's My Name T...	Mobile: 8988675309				
		Stevie Ray Vaughn	1234567890	stevie@srv.com	Home: 1234 Main Street, Dallas, TX		Yes
		Stevie Ray Vaughn	Mobile: 1234567890	Work: stevie@srv.com			
		Voice Mail	+18056377243				No
		Voice Mail	Mobile: +18056377243				No
		阿惡哈拉	+86 35 8 763 30 07				No
		阿惡哈拉	Mobile: +86 35 8 763 30 07				No

Contact 2: Jimi Hendrix

Phone Number: 7691234560

Email: [Hendrix@experienced.com](mailto:hendrix@experienced.com)

Location: HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.android.providers.contacts\databases\contacts2.db

Artifacts

ARTIFACTS

MOBILE

RECENT

COMMUNICATION

Android Call Logs

Android Contacts

EVIDENCE (21)

Column view

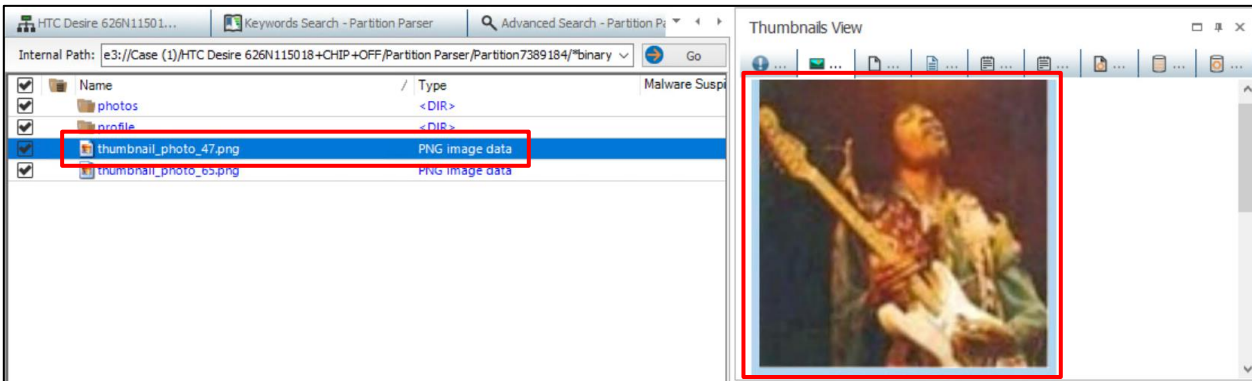
Display Name	Phone Number(s)	Email Address(es)	Address	Website	St
Jimi Hendrix	7691234560	hendrix@experienced.com		www.jimihendrix.com	Yes
Jimi Hendrix	Mobile: 7691234560	Home: hendrix@experienced.com			
John Bonham	(987) 876-7654				No
John Jacob Jingle Heimer Schmidt That's My Name T...	8988675309				No
John Jacob Jingle Heimer Schmidt That's My Name T...	Mobile: 8988675309				

5. Show images of two famous persons

Answer:

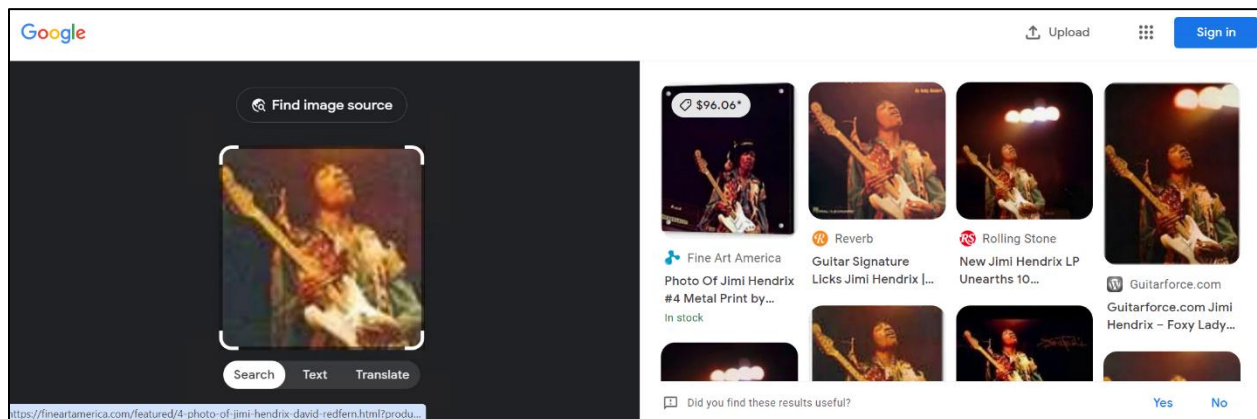
Person 1: Jimi Hendrix

Location: e3://Case (1)/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.android.providers.contacts_114710/files_115004?item=thumbnail_photo_47.png_116024



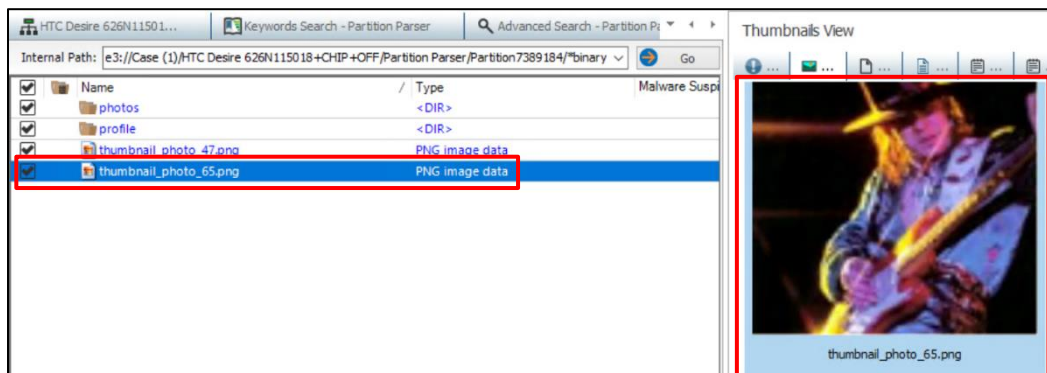
Verifying personality:

Searching on Google by Image Search.



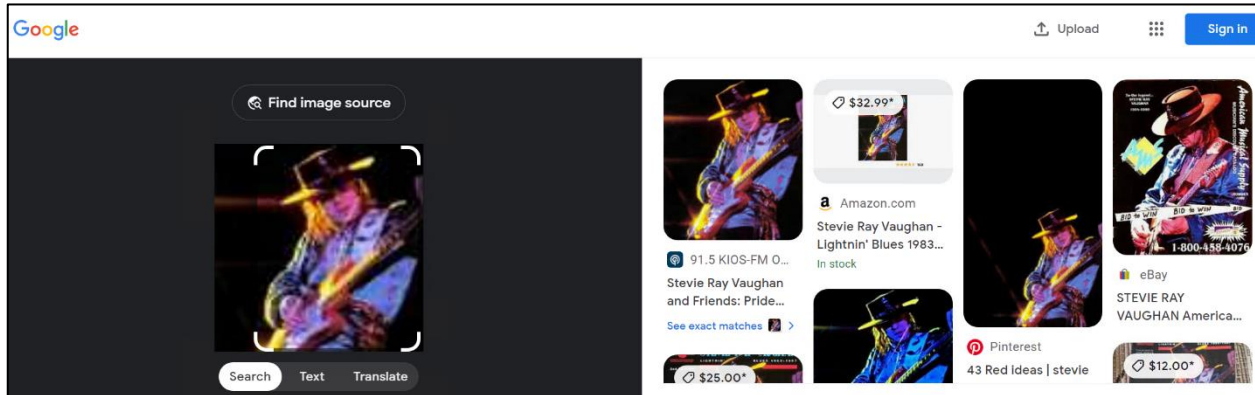
Person 2: Stevie Ray Vaughan

Location: e3://Case (1)/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.android.providers.contacts_114710/files_115004?item=thumbnail_photo_65.png_116026



Verifying personality:

Searching on Google by Image Search.

**6. What are the telephone numbers without names?**

Answer: 8785551111, 8887771212 and 3019754971

Location: e3://Case (1)/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/contact s/7-21?item=row_8

- 2 Numbers Found Through Contact database:**

display_name	given_names	times_contacted	score	emails	nickname	note / organization	phone_numbers	postal_a
411 & More	411	1					411	
Customer Care	Customer	1					611	
Voice Mail	Voice	1					+18056377243	
John Jacob Jingle Heimer Sch John	John	1					8988675309	
阿恶哈拉	哈拉	1					+86 35 8 763 30 07	
Aurélien	Aurélien	1					+33 22 6 555 20 20	
Jimi Hendrix	Jimi	1		hendrix@expe			7691234560	
8785551111		1					8785551111	
Stevie Ray Vaughn	Stevie	1		stevie@srv.cor			1234567890	1234 Ma
Voice Mail	Voice	1					+18056377243	
411 & More	411	1					411	
Customer Care	Customer	1					611	
*	*	1			W Zno		8887771212	

- 1 Number found through Call Log:**

Location: HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.android.providers.contacts\databases\contacts2.db

EVIDENCE (1)							Column view
Local User	Partner	Partner Name	Dire...	Call...	Call Date/Ti		
15868232570	3019754971		Outgoing	Unanswered	2/15/2018 4:3		

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

Answer:

Name: John Bonham

Contact Number: (987) 876-7654

Location: e3://Case (1)/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

dirty	deleted	contact_id	aggregation_id	aggr_cust	send_t	times	last_t	starr	pinne	display_name	display_name_alt	displ	pho	phoneti	sort_key	phone	phon	sort_key_al	phonebo
0	0	15	0	0	0	0	0	0	0	*	*	40	0	*	*	0	*	*	*
0	0	13	0	0	0	0	0	0	0	阿恶哈拉	阿恶哈拉	40	0	A 阿 E 恶 HA 哈 LA 拉	A	1	A 阿 E 恶 HA A	A	
0	0	12	0	0	0	0	0	0	0	Aurélien	Aurélien	40	0	Aurélien	A	4	Aurélien	A	
1	1	3	1	0	0	0	0	0	0	John Bonham	Bonham, John	40	0	John Bonham	J	10	Bonham, Joh	B	
1	0	18	3	1	0	0	0	0	0	Customer Care	Care, Customer	40	0	Customer Care	C	3	Care, Custom	C	
0	0	14	0	0	0	0	0	1	0	Jimi Hendrix	Hendrix, Jimi	40	0	Jimi Hendrix	J	10	Hendrix, Jimi	H	
1	0	20	3	1	0	0	0	0	0	411 & More	More, 411 &	40	0	411 & More	#	213	More, 411 &	M	
1	0	19	3	1	0	0	0	0	0	Voice Mail	Mail, Voice	40	0	Voice Mail	V	22	Mail, Voice	M	
0	0	11	0	0	0	0	0	0	0	John Jacob Jingle Heimer Sch	Schmidt, John Jacob Jingle H	40	0	John Jacob Jingle Heimer Sch	J	10	Schmidt, Joh	S	
0	0	16	0	0	0	0	0	1	0	Stevie Ray Vaughn	Vaughn, Stevie Ray	40	0	Stevie Ray Vaughn	S	19	Vaughn, Stev	V	
0	0	10	0	0	0	0	0	0	0	8785551111	8785551111	20	0	8785551111	#	213	8785551111	#	

Display Name	Phone Number(s)	Email Ad...	A...	We...	Star...	Deleted
*	8887771212				No	No
John Jacob Jingle Heimer Schmidt That's My Name T...	8988675309				No	No
Jimi Hendrix	7691234560	hendrix@experi...		www.jimi...	Yes	No
Aurélien	+33 22 6 555 20 20				No	No
Stevie Ray Vaughn	1234567890	stevie@srv.com	Home:...		Yes	No
John Bonham	(987) 876-7654				No	Yes
8785551111	8785551111				No	No
阿恶哈拉	+86 35 8 763 30 07				No	No
411 & More	411				No	No
Customer Care	611				No	No
Voice Mail	+18056377243				No	No
Customer Care	Mobile: 611					

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

Answer:

Contact 1

Name: Aurélien

Phone Number: +33 22 6 555 20 20

Country Code: +33 is for France

Location: HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.android.providers.contacts\databases\contacts2.db

Contact 2**Name:** 阿恶哈拉**Phone Number:** +86 35 8 763 30 07**Country Code:** +86 is for China

Location: HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.android.providers.contacts\databases\contacts2.db

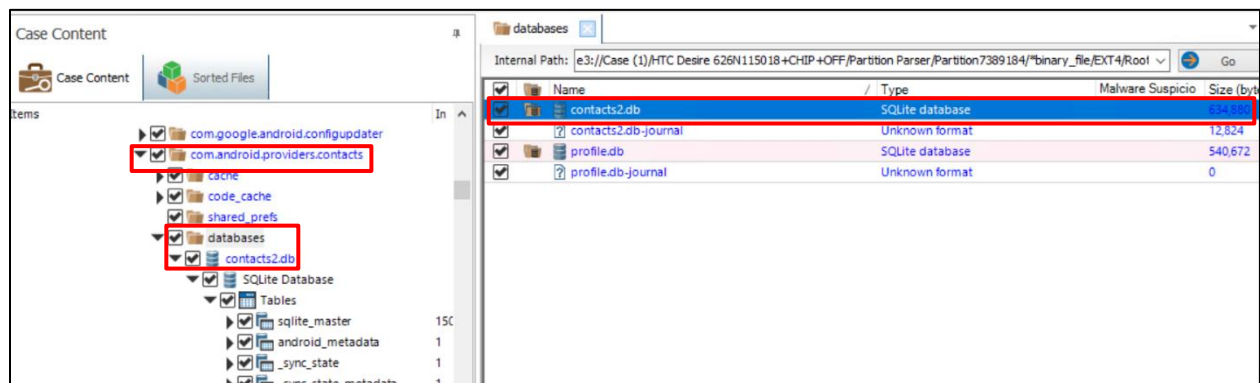
Display Name	Phone Number(s)	Email Ad...	A...	We...	Star...	Deleted	Last...	Num...
*	8887771212				No	No		0
John Jacob Jingle Heimer Schmidt That's My Name T...	8988675309				No	No		0
Jimi Hendrix	7691234560	hendrix@experi...		www.jimi...	Yes	No		0
Aurélien	+33 22 6 555 20 20				No	No		0
Stevie Ray Vaughn	1234567890	stevie@srv.com	Home:...		Yes	No		0
John Bonham	(987) 876-7654				No	Yes		0
8785551111	8785551111				No	No		0
阿恶哈拉	+86 35 8 763 30 07				No	No		0
411 & More	411				No	No		0
Customer Care	611				No	No		0
Voice Mail	+18056377243				No	No		0

9. What is contained in the group contact?

Answer: 27 Club and Starred in Android created by User and Group name My Contacts created by System.

Step 1: Identifying the contacts2.db Database

Location: e3://Case (1)/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.android.providers.contacts_114710/databases_114958?item=contacts2.db_114959



Exported data base to local system and start analyzing them.

Step 2: Identifying Key Tables

> data	CREATE TABLE data (_id INTEGER PRIMARY KEY AUTOINCREMENT,package_id INTEGER REFERENCES package(_id),r
> data_usage_stat	CREATE TABLE data_usage_stat(stat_id INTEGER PRIMARY KEY AUTOINCREMENT, data_id INTEGER NOT NULL, usag
> default_directory	CREATE TABLE default_directory (_id INTEGER PRIMARY KEY)
> deleted_contacts	CREATE TABLE deleted_contacts (contact_id INTEGER PRIMARY KEY,contact_deleted_timestamp INTEGER NOT NULL
> directories	CREATE TABLE directories(_id INTEGER PRIMARY KEY AUTOINCREMENT,packageName TEXT NOT NULL,authority TEX
> email_lookup	CREATE TABLE email_lookup (data_id INTEGER PRIMARY KEY REFERENCES data(_id) NOT NULL,raw_contact_id INTE
> event_instance	CREATE TABLE event_instance (_id INTEGER PRIMARY KEY AUTOINCREMENT,data_ref_id INTEGER REFERENCES dat
> frequency	CREATE TABLE frequency (_id INTEGER PRIMARY KEY AUTOINCREMENT, raw_contact_id INTEGER REFERENCES raw
> group_ext_table	CREATE TABLE group_ext_table(group_id INTEGER PRIMARY KEY,group_led TEXT)
> groups	CREATE TABLE groups (_id INTEGER PRIMARY KEY AUTOINCREMENT,package_id INTEGER REFERENCES package(_id
> ip_dial	CREATE TABLE ip_dial (_id INTEGER PRIMARY KEY AUTOINCREMENT,number TEXT, state INTEGER NOT NULL DEFAU
> mimetypes	CREATE TABLE mimetypes (_id INTEGER PRIMARY KEY AUTOINCREMENT,mimetype TEXT NOT NULL)
> name_lookup	CREATE TABLE name_lookup (data_id INTEGER REFERENCES data(_id) NOT NULL,raw_contact_id INTEGER REFEREN
> nickname_lookup	CREATE TABLE nickname_lookup (name TEXT,cluster TEXT)
> orderships	CREATE TABLE orderships(group_id Integer DEFAULT (-1),raw_contact_id INTEGER NOT NULL DEFAULT 0 ,display_or

> photo_files	CREATE TABLE photo_files (_id INTEGER PRIMARY KEY AUTOINCREMENT, height INTEGER NOT NULL, width INTEGE
> pre_authorized_uris	CREATE TABLE pre_authorized_uris (_id INTEGER PRIMARY KEY AUTOINCREMENT, uri STRING NOT NULL, expiration
> properties	CREATE TABLE properties (property_key TEXT PRIMARY KEY, property_value TEXT)
> raw_contacts	CREATE TABLE raw_contacts (_id INTEGER PRIMARY KEY AUTOINCREMENT,account_id INTEGER REFERENCES accou
> search_index	CREATE VIRTUAL TABLE search_index USING FTS4 (contact_id INTEGER REFERENCES contacts(_id) NOT NULL,conten

Step 3: Understanding the *mimetypes* Table

Export mimetypes table.

Location: e3://Case (1)/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/mimetypes/1-17

Include in	Attachme	rowid	_id	mimetype
TRUE	No	1	1	vnd.android.cursor.item/email_v2
TRUE	No	2	2	vnd.android.cursor.item/im
TRUE	No	3	3	vnd.android.cursor.item/nickname
TRUE	No	4	4	vnd.android.cursor.item/organization
TRUE	No	5	5	vnd.android.cursor.item/phone_v2
TRUE	No	6	6	vnd.android.cursor.item/sip_address
TRUE	No	7	7	vnd.android.cursor.item/name
TRUE	No	8	8	vnd.android.cursor.item/postal-address_v2
TRUE	No	9	9	vnd.android.cursor.item/identity
TRUE	No	10	10	vnd.android.cursor.item/photo
TRUE	No	11	11	vnd.android.cursor.item/note
TRUE	No	12	12	com.htc.htccontacts/htc_data_ext
TRUE	No	13	13	vnd.android.cursor.item/contact_event
TRUE	No	14	14	vnd.android.cursor.item/group_membership
TRUE	No	15	15	vnd.com.google.cursor.item/contact_misc
TRUE	No	16	16	vnd.android.cursor.item/website

- To understand the structure of the **data** table and how to retrieve group membership, we first inspect the **mimetypes** table. The mimetypes table helps us understand what type of data each entry in the data table represents.
- The key value for **group membership** is **mimetype_id = 14**, which corresponds to vnd.android.cursor.item/group_membership.

Step 4: Retrieving Group Membership from the data Table

Include in Attachme	rowid	id	package	mimetype_id	row_content_hash_id	is_read_o	is_primary	is_super	data1	data2	data3	data4	data5	data6	data7	data8	data9	data
TRUE	No	20	20	7	10	0	0	0	1	*	*							
TRUE	No	21	21	11	10	0	0	0	1	W Z_nova an	AuyoGpxqxl ix Of, vi.	Gcy SMS	, o aglrhp wackos S. u.	Fan ad waz l, j7 b htv ads. U.ufe				
TRUE	No	22	22	3	10	0	0	0	1									
TRUE	No	24	24	14	10	0	0	0	1	7								
TRUE	No	25	25	3	10	0	1	1	4	8.89E+09	2		1.89E+10					
TRUE	No	27	27	7	11	0	0	0	1									
TRUE	No	28	28	11	11	0	0	0	1									
TRUE	No	29	29	3	11	0	0	0	1		1							
TRUE	No	31	31	14	11	0	0	0	1	7								
TRUE	No	32	32	5	11	0	1	1	4	8.79E+09	2		1.88E+10					
TRUE	No	34	34	7	12	0	0	0	1	阿恶哈拉 哈拉	阿恶							
TRUE	No	35	35	11	12	0	0	0	1									
TRUE	No	36	36	3	12	0	0	0	1		1							
TRUE	No	38	38	14	12	0	0	0	1	7								
TRUE	No	39	39	5	12	0	1	1	4	+86 35 8 7	2		8.64E+11					

- Now that we know **group membership** is stored in the data table where **mimetype_id = 14**, we query the data table to retrieve all entries related to group membership.

Step 5: Cross-Referencing the groups Table to Get Group Names

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD
Include in Attachme	rowid	id	package	account_id	sourceid	version	dirty	title	title_res	notes	system_id	deleted	group_visi	should_sync	auto_add	favorites	group_is_f	sync1	sync2	sync3	sync4	photo	sortorder	display_tit	is_hide	display_or_is	attribute_set		
TRUE	No	1	1		3 HTC_01			Favorite_86150684	47252476	Favorite_8	0	1	1	1	0	0	1							5 Favorites	2.15E+09	0			
TRUE	No	2	2		3 HTC_01			VIP			VIP	0	1	1	0	0	1							5 VIP	2.15E+09	0			
TRUE	No	3	3		3 HTC_01			Family			Family	0	1	1	0	0	1							0 Family	2.15E+09	0			
TRUE	No	4	4		3 HTC_01			Friends			Friends	0	1	1	0	0	1							0 Friends	2.15E+09	0			
TRUE	No	5	5		3 HTC_01			Coworkers			Coworkers	0	1	1	0	0	1							0 Co-workers	2.15E+09	0			
TRUE	No	6	6		3 HTC_01			Frequent Contacts			Frequent C	0	1	0	0	0	0	1						0 Frequent	2.15E+09	1			
TRUE	No	7	7		5	6		My Contacts			System Grn Contacts	0	1	1	1	0	1							0 My Contacts	2.15E+09	0			
TRUE	No	8	8		5	4842a3a90818269b		Starred in Android			Starred in Android	0	1	1	0	1	1	https://ww8Ux7Zpjp	1.39E+15					0 Starred in Android	2.15E+09	0			
TRUE	No	9	9		5 d			Friends			System Grn Friends	0	1	1	0	0	1							0 Friends	2.15E+09	0			
TRUE	No	10	10		5 e			Family			System Grn Family	0	1	1	0	0	1							0 Family	2.15E+09	0			
TRUE	No	11	11		5 f			Coworkers			System Grn Coworkers	0	1	1	0	0	1							0 Co-workers	2.15E+09	0			
TRUE	No	12	12		5	252c105b8f0870ba		27 Club			27 Club	0	1	1	0	0	1	https://wwOI2IMExnE	1.45E+15					0 27 Club	2.15E+09	0			

Key Information in the groups Table:

- _id (Column D):** The unique identifier for each group. This ID is used to link contacts to their respective groups.
- title (Column J):** The **name of the group** (e.g., "Family," "Friends," "My Contacts," "Starred in Android").
- system_id (Column L):** This column helps determine if the group is **system-generated** or **user-created**:
 - If the **system_id** is populated, the group is likely **system-generated** (e.g., "Starred in Android").
 - If the **system_id** is **NULL**, the group is **user-created** (e.g., "Family," "Friends").
- notes (Column K):** This column may provide additional information about the group. For example, system groups often have notes like "System Group: Friends."
- favorites (Column R):** Indicates whether the group is marked as a favorite.

The group information is crucial because it allows us to:

- Identify the **group names** that contacts belong to.
- Determine if the group was **system-generated** or **user-created**, which will be reflected in the final query.

Step 6: Joining Contacts with Group Information and Adding Phone Numbers

In **Step 6**, we use the information from the **groups** table and join it with the **raw_contacts** and **data** tables to display the group names alongside each contact. We also retrieve phone numbers from the data table where mimetype_id = 5.

```
SELECT rc.display_name, g.title AS group_name,
       CASE
         WHEN g.system_id IS NOT NULL THEN 'System-Generated'
         ELSE 'User-Created'
       END AS group_origin,
       p.data1 AS phone_number
FROM data d
JOIN raw_contacts rc ON d.raw_contact_id = rc._id
JOIN groups g ON d.data1 = g._id
LEFT JOIN data p ON rc._id = p.raw_contact_id AND p.mimetype_id = 5 -- 5 is the mimetype for phone numbers
WHERE d.mimetype_id = 14;
```

Result:

	display_name	group_name	group_origin	phone_number
1	Jimi Hendrix	27 Club	User-Created	7691234560
2	Stevie Ray Vaughn	27 Club	User-Created	1234567890
3	*	My Contacts	System-Generated	8887771212
4	8785551111	My Contacts	System-Generated	8785551111
5	阿恶哈拉	My Contacts	System-Generated	+86 35 8 763 30 07
6	John Jacob Jingle Heimer Schmidt ...	My Contacts	System-Generated	8988675309
7	Jimi Hendrix	My Contacts	System-Generated	7691234560
8	Aurélien	My Contacts	System-Generated	+33 22 6 555 20 20
9	Stevie Ray Vaughn	My Contacts	System-Generated	1234567890
10	John Bonham	My Contacts	System-Generated	(987) 876-7654
11	Jimi Hendrix	Starred in Android	User-Created	7691234560
12	Stevie Ray Vaughn	Starred in Android	User-Created	1234567890

A **group contact** contains the following:

1. **Contact names:** The names of the individuals in the group.
2. **Phone numbers:** The phone numbers associated with each contact in the group.
3. **Group names:** The name of the group the contacts belong to (e.g., "Family," "Friends").
4. **Group origin:** Indicates whether the group is **User-Created** or **System-Generated**.

10. Provide all details of the datebook/Calendar**Answer:**

Title	Original Start	Instance Start	Instance End
Van halen were scheduled to perform forty shows on their 2007 tour with David lee Roth after much success in the early 80s with David lee Roth as their front man for van halen!!	1393804800000	1488499200000	1488585600000
Van halen were scheduled to perform forty shows on their 2007 tour with David lee Roth after much success in the early 80s with David lee Roth as their front man for van halen!!	1393804800000	1520035200000	1520121600000
Van halen were scheduled to perform forty shows on their 2007 tour with David lee Roth after much success in the early 80s with David lee Roth as their front man for van halen!!	1393804800000	1551571200000	1551657600000
Rush Concert	1461398400000	1492934400000	1492938000000
Rush Concert	1461398400000	1524470400000	1524474000000
	1476108000000	1507644000000	1507647600000
	1476108000000	1539180000000	1539183600000
!	1482307200000	1513843200000	1513846800000
!	1482307200000	1545379200000	1545382800000
Independence Day	1499126400000	1499126400000	1499212800000
Halloween	1509408000000	1509408000000	1509494400000
Thanksgiving Day	1511395200000	1511395200000	1511481600000
Independence Day	1530662400000	1530662400000	1530748800000
Valentine's Day	1550102400000	1550102400000	1550188800000
Thomas Jefferson's Birthday	1492041600000	1492041600000	1492128000000
Easter Sunday	1492300800000	1492300800000	1492387200000
Labor Day	1504483200000	1504483200000	1504569600000
Veterans Day	1510358400000	1510358400000	1510444800000
Christmas Day	1514160000000	1514160000000	1514246400000

New Year's Eve	1514678400000	1514678400000	1514764800000
Valentine's Day	1518566400000	1518566400000	1518652800000
Thomas Jefferson's Birthday	1523577600000	1523577600000	1523664000000
Labor Day	1535932800000	1535932800000	1536019200000
Halloween	1540944000000	1540944000000	1541030400000
Veterans Day	1541894400000	1541894400000	1541980800000
Thanksgiving Day	1542844800000	1542844800000	1542931200000
Christmas Eve	1545609600000	1545609600000	1545696000000
Christmas Day	1545696000000	1545696000000	1545782400000
New Year's Eve	1546214400000	1546214400000	1546300800000
New Year's Day	1546300800000	1546300800000	1546387200000
Memorial Day	1496016000000	1496016000000	1496102400000
Christmas Eve	1514073600000	1514073600000	1514160000000
New Year's Day	1514764800000	1514764800000	1514851200000
Easter Sunday	1522540800000	1522540800000	1522627200000
Memorial Day	1527465600000	1527465600000	1527552000000
Daylight Saving Time starts	1489276800000	1489276800000	1489363200000
Daylight Saving Time ends	1509840000000	1509840000000	1509926400000
Daylight Saving Time starts	1520726400000	1520726400000	1520812800000
Daylight Saving Time ends	1541289600000	1541289600000	1541376000000
Daylight Saving Time starts	1552176000000	1552176000000	1552262400000
Mother's Day	1494720000000	1494720000000	1494806400000
Father's Day	1497744000000	1497744000000	1497830400000
Mother's Day	1526169600000	1526169600000	1526256000000
Father's Day	1529193600000	1529193600000	1529280000000
Martin Luther King Jr. Day	1515974400000	1515974400000	1516060800000
Martin Luther King Jr. Day	1548028800000	1548028800000	1548115200000

Veterans Day observed	1510272000000	1510272000000	1510358400000
Veterans Day observed	1541980800000	1541980800000	1542067200000
Columbus Day (regional holiday)	1507507200000	1507507200000	1507593600000
Columbus Day (regional holiday)	1538956800000	1538956800000	1539043200000
Presidents' Day (regional holiday)	1487548800000	1487548800000	1487635200000
Presidents' Day (regional holiday)	1518998400000	1518998400000	1519084800000
Presidents' Day (regional holiday)	1550448000000	1550448000000	1550534400000

We are using data from 4 tables: Events, Reminders, Instances and Calendars.

- **Location 1:** e3://Case (1)/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
- **Location 2:** e3://Case (1)/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/Instances/1-59
- **Location 3:** e3://Case (1)/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/Reminders/1-5
- **Location 4:** e3://Case (1)/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/Calendars/1-5

Method:

We have extracted and open DB file and Explored tables. After going through tables we got 4 tables that provide this information Events, Reminders, Instances and Calendars.

```
SELECT e.title, e.dtstart AS original_start, i.begin AS instance_start, i.end AS instance_end
FROM events e
JOIN instances i ON e._id = i.event_id;
```

We are running this query to **link events** with their **specific instances**. The **events** table contains the main event details, while the **instances** table stores the **actual occurrences** of the events, especially useful for recurring events. **events._id** is the unique identifier for each event. **instances.event_id** links each instance back to its main event by referencing the **events._id**.

11. Provide the outgoing telephone numbers in the call log

Answer: 3019754971

Location: HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.android.providers.contacts\databases\contacts2.db

ARTIFACTS	MOBILE
Android Call Logs	1
Android Contacts	21
Android Facebook Messenger Attachments	63
Android SMS/MMS	7
Facebook Messenger Messages	20
Facebook Messenger Users Contacted	2
TextPlus Calls	8

Local User	Partner	Partner Name	Dire...	Call...	Call Date/Time
15868232570	3019754971		Outgoing	Unanswered	2/15/2018 4:34:09.711 PM

Local User	15868232570
Partner	3019754971
Direction	Outgoing
Call Status	Unanswered
Call Date/Time	2/15/2018 4:34:09.711 PM
Call End Date/Time	2/15/2018 4:34:09.000 PM
Partner Location	Maryland
Service Provider Country Code	US
ICCID	8901260472997564858
Artifact type	Android Call Logs
Item ID	46354

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

Answer: Yes, there are outgoing SMS messages. 2 outgoing messages were found:

- The first was sent to 3014011239 on 2/21/2018 at 2:07:34 PM, with the content: "The following SMS message is an active outgoing message sent to another device."
- The second was sent to the same recipient on 2/15/2018 at 4:58:42 PM, with the content: "Outgoing active extended SMS message. This is an outgoing SMS message that exceeds 160 characters."

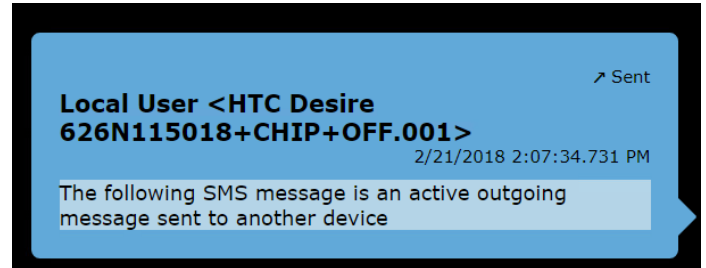
Both messages were in **queued** status at the time of recording.

Location: HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.android.providers.telephony\databases\mmssms.db

Evidence:

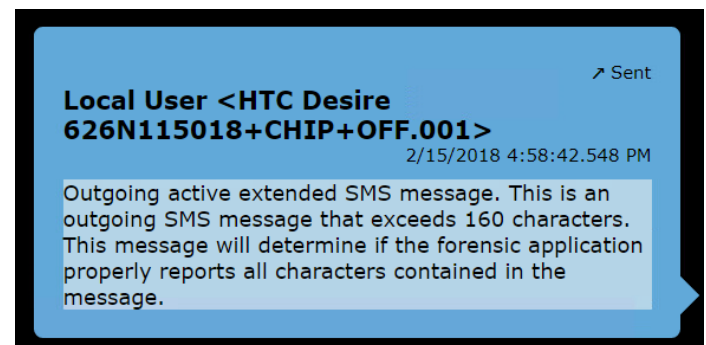
For Outgoing SMS 1:

Sender	Local User <HTC Desire 626N115018+CHIP+OFF.001>
Recipient(s)	3014011239
Message	The following SMS message is an active outgoing message sent to another device
Sent Date/Time	2/21/2018 2:07:34.731 PM
Direction	Queued
Type	SMS
Application	com.htc.sense.mms
Date/Time	2/21/2018 2:07:34.731 PM
Artifact type	Android SMS/MMS
Item ID	46580



For Outgoing SMS 2:

Sender	Local User <HTC Desire 626N115018+CHIP+OFF.001>
Recipient(s)	3014011239
Message	Outgoing active extended SMS message. This is an outgoing SMS message that exceeds 160 characters. This message will determine if the forensic application properly reports all characters contained in the message.
Sent Date/Time	2/15/2018 4:58:42.548 PM
Direction	Queued
Type	SMS
Application	com.htc.sense.mms
Date/Time	2/15/2018 4:58:42.548 PM
Artifact type	Android SMS/MMS
Item ID	46582



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

Answer: **Yes**

Location: HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.android.providers.telephony\databases\mmssms.db

Evidence:

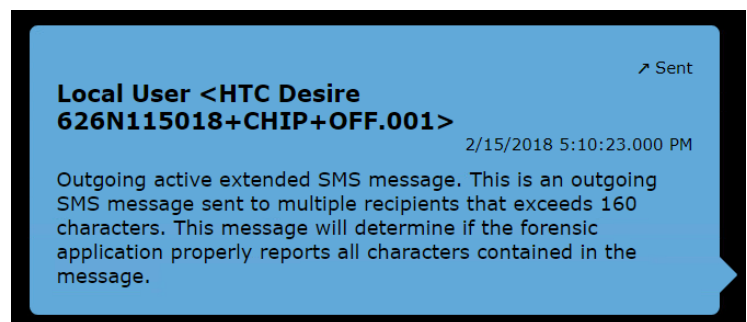
MMS 1:

Sender	Local User <HTC Desire 626N115018+CHIP+OFF.001>
Recipient(s)	Stevie Ray Vaughn (1234567890), 3014011239, Jimi Hendrix (7691234560)
Message	The following SMS message is an active outgoing group message sent to multiple recipients
Sent Date/Time	2/15/2018 5:00:54.000 PM
Received Date/Time	2/15/2018 5:00:54.000 PM
Direction	Outbox
Type	MMS
Attachment Data Recovered	n/a
Application	com.htc.sense.mms
Date/Time	2/15/2018 5:00:54.000 PM
Artifact type	Android SMS/MMS



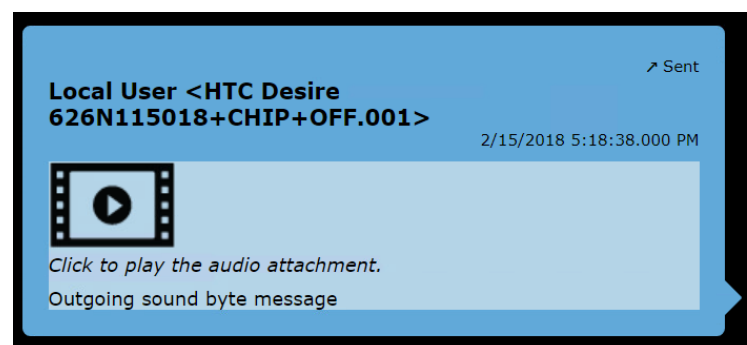
MMS 2:

Sender	Local User <HTC Desire 626N115018+CHIP+OFF.001>
Recipient(s)	Stevie Ray Vaughn (1234567890), 3014011239, Jimi Hendrix (7691234560)
Message	Outgoing active extended SMS message. This is an outgoing SMS message sent to multiple recipients that exceeds 160 characters. This message will determine if the forensic application properly reports all characters contained in the message.
Sent Date/Time	2/15/2018 5:10:23.000 PM
Received Date/Time	2/15/2018 5:10:23.000 PM
Direction	Outbox
Type	MMS
Attachment Data Recovered	n/a
Application	com.htc.sense.mms
Date/Time	2/15/2018 5:10:23.000 PM
Artifact type	Android SMS/MMS



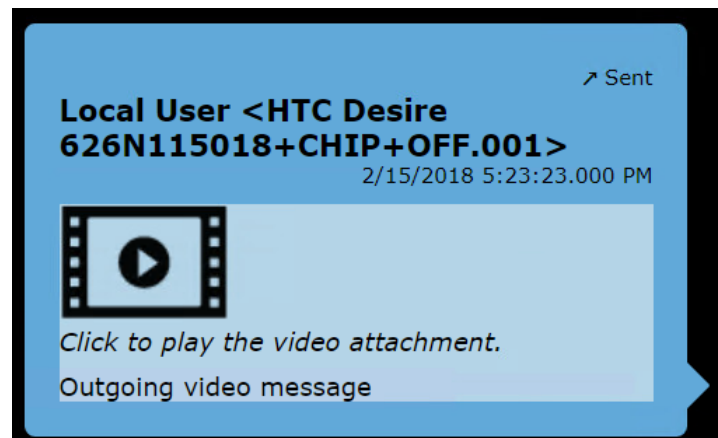
MMS 3:

Sender	Local User <HTC Desire 626N115018+CHIP+OFF.001>
Recipient(s)	3014011239
Message	Outgoing sound byte message
Sent Date/Time	2/15/2018 5:18:38.000 PM
Received Date/Time	2/15/2018 5:18:38.000 PM
Direction	Outbox
Type	MMS
Attachments	/data/user/0/com.android.providers.telephony/app_parts/PART_1518714275688_Voice0001.aac
Attachment Data Recovered	Yes
Application	com.htc.sense.mms
Date/Time	2/15/2018 5:18:38.000 PM
Artifact type	Android SMS/MMS
Item ID	46587

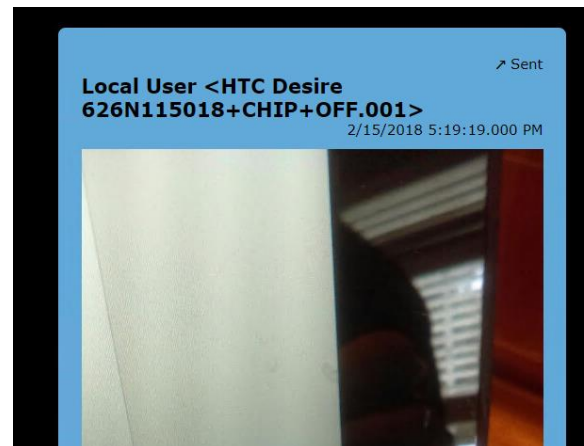


MMS 4:

Sender	Local User <HTC Desire 626N115018+CHIP+OFF.001>
Recipient(s)	3014011239
Message	Outgoing video message
Sent Date/Time	2/15/2018 5:23:23.000 PM
Received Date/Time	2/15/2018 5:23:23.000 PM
Direction	Outbox
Type	MMS
Attachments	/data/user/0/com.android.providers.telephony/app_parts/ PART_1518714463219_VIDEO0004.3gp
Attachment Data Recovered	Yes
Application	com.htc.sense.mms
Date/Time	2/15/2018 5:23:23.000 PM
Artifact type	Android SMS/MMS
Item ID	46588

**MMS 5:**

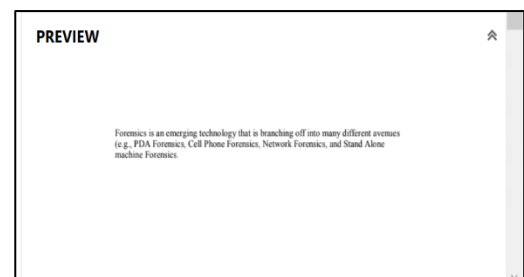
Sender	Local User <HTC Desire 626N115018+CHIP+OFF.001>
Recipient(s)	3014011239
Message	Outgoing image MMS message
Sent Date/Time	2/15/2018 5:19:19.000 PM
Received Date/Time	2/15/2018 5:19:19.000 PM
Direction	Outbox
Type	MMS
Attachments	/data/user/0/com.android.providers.telephony/app_parts/ PART_1518714343199_IMAGE0001.jpg
Attachment Data Recovered	Yes
Application	com.htc.sense.mms
Date/Time	2/15/2018 5:19:19.000 PM
Artifact type	Android SMS/MMS
Item ID	46589

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

In digital forensics, a **stand-alone file** refers to any file that exists independently on a device, not linked to a specific program or application. It's not part of a system or app's usual data but is simply stored on the device, like a photo, document, or video that someone saved. These files can be analyzed for evidence during an investigation.

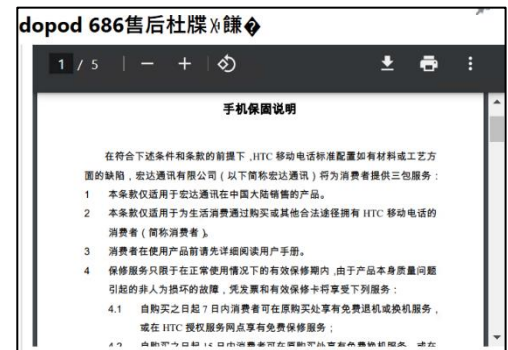
There are a lot of file location but below are few locations of this files:

Location: HTC Desire 626N115018+CHIP+OFF.001 -
Partition 63 (EXT-family, 3.75
GB)\media\0\Download\forensics.pdf



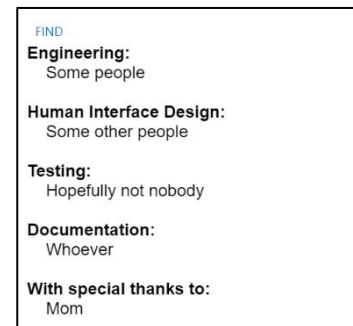
Location: HTC Desire 626N115018+CHIP+OFF.001 - Partition 60 (EXT-family, 2.5 GB)\priv-app\HTCAdvantage\HTCAdvantage.apk

Explanation: Despite being part of the system's privileged app directory, the APK itself is a stand-alone application package and can be considered a stand-alone file. It contains everything necessary for the app to function independently.



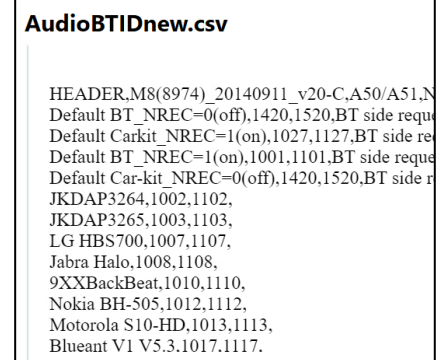
Location: HTC Desire 626N115018+CHIP+OFF.001 - Partition 60 (EXT-family, 2.5 GB)\etc\PCTOOL.ISO

Explanation: Despite its unusual location in the /etc/ folder, the .ISO file is a stand-alone file by nature. It can be extracted, mounted, or opened independently, without relying on other system components.



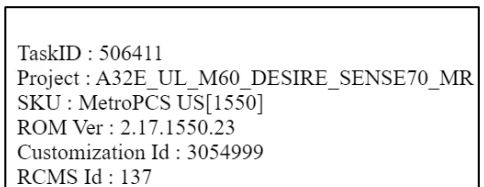
Location: HTC Desire 626N115018+CHIP+OFF.001 - Partition 60 (EXT-family, 2.5 GB)\etc\AudioBTIDnew.csv

Explanation: Despite being stored in a system configuration folder, a .csv file is inherently a stand-alone file that can be opened, viewed, and analyzed independently. The data it contains could be used for further analysis, but it is self-contained.



Location: HTC Desire 626N115018+CHIP+OFF.001 - Partition 60 (EXT-family, 2.5 GB)\customize\AAInfo.txt

Explanation: This file can be considered stand-alone, as it is a plain text file that does not rely on other files to function. Even though it might contain information related to system customization, it can be opened and analyzed on its own.



- There are more Stand-alone files on the system image. These are just few files to show the evidence of existence of stand-alone file on system.

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

Answer: **Yes**

Common Location has most of the files:

Location: e3://Case (1)/HTC Desire 626N115018+CHIP+OFF/Partition

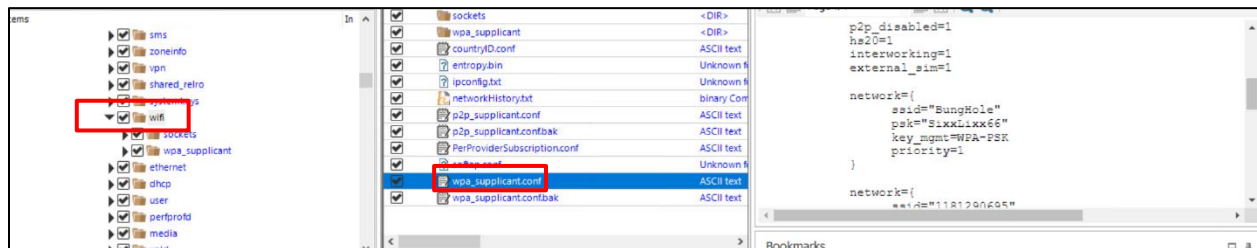
Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.android.chrome_114840/cache_123007/Cache_124580

ARTIFACTS	MOBILE	URL	Web...	First...	Last
WEB RELATED	1,240				
Chrome Bookmarks	2	http://www.metropcs.mobi/styles/app-af92276d84.css			2/15/
Chrome Cache Records	470	http://assets-lib.mobileposse.mobi/js/lib-utility/0.1.7...			2/15/
Chrome Cookies	136	http://www.metropcs.mobi/			2/15/
Chrome FavIcons	13	http://assets-lib.mobileposse.mobi/js/lib-posse-ad/3...			2/15/
Chrome Tab History	1	http://www.metropcs.mobi/scripts/app-en-cb0d22f2...			2/15/
Chrome Top Sites	6	http://www.metropcs.mobi/images/sprite-main-596...			2/15/
Chrome Web History	12	https://www.google-analytics.com/analytics.js			2/15/
Chrome Web Visits	14	https://www.google.com/complete/search?client=ch...			2/15/
Potential Browser Activity	586	http://www.googletagmanager.com/gtm.js?id=GTM...			2/15/
		http://www.googletagservices.com/tag/js/gpt.js			2/15/
		https://www.google.com/complete/search?client=ch...			2/15/

Another Internet Data:

Location: e3://Case (1)/HTC Desire 626N115018+CHIP+OFF/Partition

Parser/Partition7389184/*binary_file/EXT4/Root/misc_155649/wifi_155663?item=wpa_supplicant.conf_155722



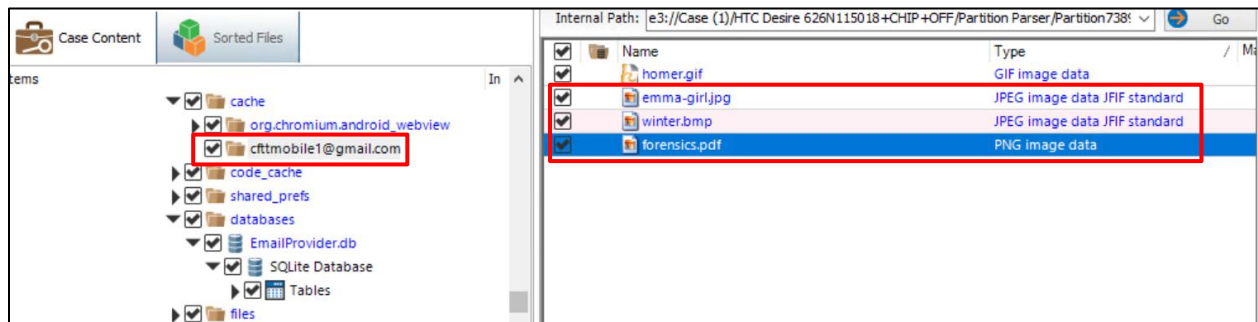
Below All the Social medias and internet based services consider as Internet data:

Facebook URLs	99	https://m.facebook.com/profile/questions/view/100...	Potential Activity	Unknown
Google Analytics First Visit Cookies	2	https://www.facebook.com/help/messenger-app/94...	Artifact type	Facebook URLs
Google Analytics Referral Cookies	2	https://www.facebook.com/help/messenger-app/94...	Item ID	46632
Google Analytics Session Cookies	2	https://staticxx.facebook.com/connect/xd_arbiter/r/...	Original artifact	Potential Browser Activity
Google Searches	1	http://staticxx.facebook.com/connect/xd_arbiter/r/...		
Identifiers - Device	10	https://m.facebook.com/jennifer.vasquezdeayala?n...		
Identifiers - People	202	https://m.facebook.com/profile/questions/view/100...		
Passwords and Tokens	39	https://m.facebook.com/story.php?story_fbid=1982...		
Rebuilt Webpages	25	https://m.facebook.com/photo.php?fbid=19829854...		
Social Media URLs	4	https://m.facebook.com/story.php?story_fbid=1983...		

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

Answer: **Yes Set up email found.**

Location: e3://Case (1)/HTC Desire 626N115018+CHIP+OFF/Partition Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.google.android.gm_114860/cache_115012?item=cfttmobile1@gmail.com_124408




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

Answer: **Yes**

Location: HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\data\com.google.android.apps.maps\databases\gmm_storage.db

Evidence:

Search Query	The White House, 1600 Pennsylvania Ave NW, Washington, DC 20500
URL	http://www.google.com/search?q=The+White+House,+1600+Pennsylvania+Ave+NW,+Washington,+DC+20500&ludocid=8167675777476425407#lrd=0x89b7b7bcdecbb1df:0x715969d86d0b76bf
CID	8167675777476425407
FID	0x89b7b7bcdecbb1df:0x715969d86d0b76bf
Artifact type	 Android Google Maps
Item ID	46797

Wi-Fi Evidence:

Location: HTC Desire 626N115018+CHIP+OFF.001 - Partition 63 (EXT-family, 3.75 GB)\misc\wifi\wpa_supplicant.conf

Net...	Security Mo...	Net...	User...	WEP...	MAC...
BungHole	WPA-PSK	SixxLixx66			
1181290695	WPA-EAP IEEE8021X				

DETAILS

ARTIFACT INFORMATION

Network Name (SSID) **BungHole**

Security Mode **WPA-PSK**

Network Password **SixxLixx66**

Artifact type Android Wi-Fi Profiles

Item ID **34578**

Net...	Security Mo...	Net...	User...	WEP...	MAC...
BungHole	WPA-PSK	SixxLixx66			
1181290695	WPA-EAP IEEE8021X				

DETAILS

ARTIFACT INFORMATION

Network Name (SSID) **1181290695**

Security Mode **WPA-EAP IEEE8021X**

Artifact type Android Wi-Fi Profiles

Item ID **34582**

There are many location data we can get from Magnet Axiom Examiner's data extraction:

LOCATION & TRAVEL		34
	Android Google Maps	1
	Android Wi-Fi Profiles	2
	Google Maps	27
	Google Maps Directions	1
	Google Maps Saved Locations	2
	Google Maps Tiles	1

18. Is there any social media data? If so, provide evidence

Answer: **Yes**

Facebook

Location: e3://Case (1)/HTC Desire 626N115018+CHIP+OFF/Partition

Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.facebook.katana_114855

ARTIFACTS	MOBILE	Auth...	Com...	Com...	Post ID	Artifact type	Source
Facebook Comments	1				2067826459900117	Facebook Comments	HTC Desire 626
Facebook Contacts	2						
Facebook User/Friends	2						

Instagram

Location: e3://Case (1)/HTC Desire 626N115018+CHIP+OFF/Partition

Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.instagram.android_12428

0

ARTIFACTS	MOBILE	Pict...	MIM...	Created Date/Time	Last Accessed Dat...	Last Modified
Instagram Direct Messages	3		image/jpeg	2/15/2018 5:36:59.000 PM	2/15/2018 5:36:59.000 PM	2/15/2018 5:36
Instagram Media	88		image/jpeg	2/15/2018 5:37:04.000 PM	2/15/2018 5:37:04.000 PM	2/15/2018 5:37
			image/jpeg	2/15/2018 5:39:36.000 PM	2/15/2018 5:39:36.000 PM	2/15/2018 5:39

LinkedIn

Location: e3://Case (1)/HTC Desire 626N115018+CHIP+OFF/Partition

Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.linkedin.android_139400

ARTIFACTS	MOBILE	UserName	First...	Last...	Full...	Summary	Art
LinkedIn Profile	1	cftmobile1@gmail.com	John	Smith	John Smith	Computer Scientist at TSIN	Linke

Twitter

Location: e3://Case (1)/HTC Desire 626N115018+CHIP+OFF/Partition

Parser/Partition7389184/*binary_file/EXT4/Root/data_114689/com.twitter.android_123734

ARTIFACTS	MOBILE	Text	Sen...	Reci...	Sent/Received Da
Twitter Direct Messages	10	Now g4 is here	2249111010	2249114522	3/2/2016 8:32:59.00
Twitter Tweets	105	Hey Jane this is s4s brother	2249111010	2249114522	8/30/2016 3:35:46.0
Twitter Users	27		2249111010	2249114522	8/30/2016 3:37:37.0
			2249111010	2249114522	8/30/2016 3:37:40.0