

FILE SYSTEM ANALYSIS WITH AUTOPSY

Name: Alaoui Belghiti Hanaa

First thing I'll do is install autopsy and put the disk image into it in kali:

CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

2. **Description:** An optional, one line description of this case.

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a. <input type="text" value="Hanaa"/>	b. <input type="text"/>
c. <input type="text"/>	d. <input type="text"/>
e. <input type="text"/>	f. <input type="text"/>
g. <input type="text"/>	h. <input type="text"/>
i. <input type="text"/>	j. <input type="text"/>

Choosing the image I'm working on:

Select the case to open or create a new one

Name	Description	
<input checked="" type="radio"/> fat16	forensics	details
<input type="radio"/> rawimage	inage	details

Analysing It:

Select the host to open or create a new one

Name	Description	
<input checked="" type="radio"/> host1	crotian	details

Investigator (for reports only):

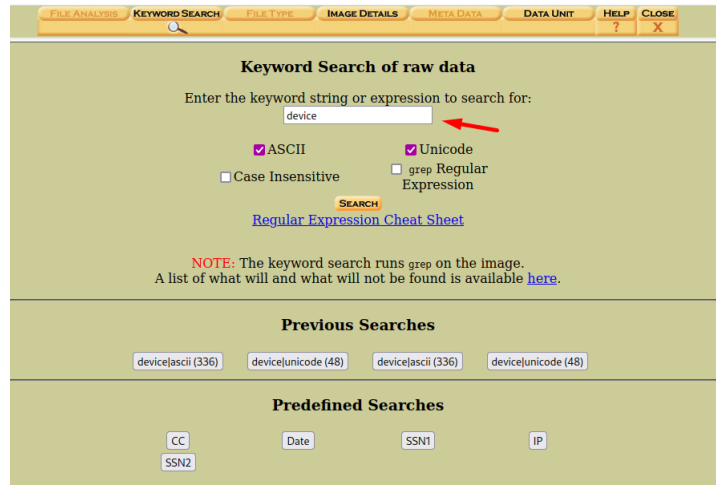
Select a volume to analyze or add a new image file.

mount	name	fs type	
<input checked="" type="radio"/> disk	deviceImageCorrupted.raw-disk	raw	details
<input type="radio"/> raw	deviceImageCorrupted.raw-63-144584	raw	details

I. What is the type and model of the device?


In order to determine the type and model of the device I'll try looking for keywords that include "device" "type" etc.

Here is my first try:



The screenshot shows the 'Keyword Search' tab of a forensic analysis tool. The search bar contains the word 'device'. Below the search bar, there are checkboxes for 'ASCII' (checked), 'Unicode' (checked), 'Case Insensitive' (unchecked), and 'grep Regular Expression' (unchecked). A 'SEARCH' button is located below these options. A note states: 'NOTE: The keyword search runs grep on the image. A list of what will and what will not be found is available [here](#).' Below the note, there are sections for 'Previous Searches' and 'Predefined Searches'. The 'Previous Searches' section shows four search terms: 'device|ascii (336)', 'device|unicode (48)', 'device|ascii (336)', and 'device|unicode (48)'. The 'Predefined Searches' section shows four search terms: 'CC', 'Date', 'SSN1', and 'IP'.

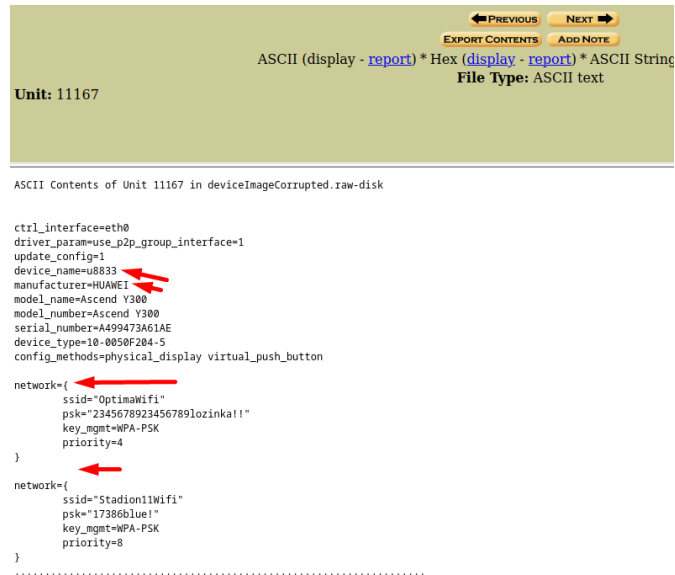
Result :



The screenshot shows the search results for the keyword 'device'. The results are listed as follows:

- Unit 11167 ([Hex](#) - [Ascii](#))
 - 1: 75 (device_name)
 - 2: 188 (device_type)
- Unit 12901 ([Hex](#) - [Ascii](#))
 - 3: 342 (help_devices.png)
- Unit 13092 ([Hex](#) - [Ascii](#))
 - 4: 222 (port_device.png)
- Unit 15065 ([Hex](#) - [Ascii](#))
 - 5: 135 (help_devices.png)
- Unit 15317 ([Hex](#) - [Ascii](#))
 - 6: 256 (port_device.png)
- Unit 18082 ([Hex](#) - [Ascii](#))
 - 7: 441 (help_devices.png)
- Unit 18429 ([Hex](#) - [Ascii](#))
 - 8: 420 (port_device.png)
- Unit 22384 ([Hex](#) - [Ascii](#))

Clicking on it:



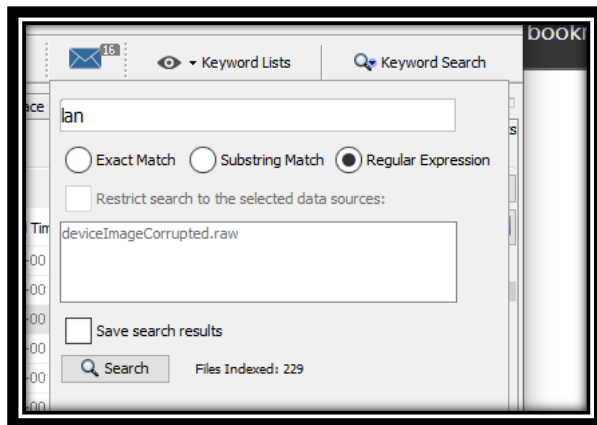
As you can see above, I found the info, therefore:

Device name	manufacturer	Model name
U8833	HUAWEI	Ascend Y300

II. What is the Mac address of the ethernet interface?

I switched to autopsy on windows for more convenience.

In order to detect the mac address of the internet interface, first I tried looking for keywords such as "mac" "interface" "Ethernet" etc, didn't find much info, so I searched for the keyword "Lan" and this is the result:



f0129363.txt	<?xml:lang="x-default">proba	/img_deviceImageCorrupted.raw/vol_vol2/\$CarvedFiles/1/...	0000-00-00 00:00:00
Unalloc_4_32256_74027520	pcc-eth0.pid smart.<lan=pubkey_blacklist.tx	/img_deviceImageCorrupted.raw/vol_vol2/Unalloc_4_3225...	0000-00-00 00:00:00
f0133536.txt	iro.product.locale.<lan=guage=enro.product,	/img_deviceImageCorrupted.raw/vol_vol2/\$CarvedFiles/1/...	0000-00-00 00:00:00
f0133696.elf	sizehistsizehostfile<lan=glc_alllc_collatcl_	/img_deviceImageCorrupted.raw/vol_vol2/\$CarvedFiles/1/...	0000-00-00 00:00:00
f0134576.kf	=fct=...<lan=blacklist_blacklist_blacklist...	/img_deviceImageCorrupted.raw/vol_vol2/\$CarvedFiles/1/...	0000-00-00 00:00:00

As you can see, I found multiple files that contains “Lan” keyword but I checked the unallocated one first:

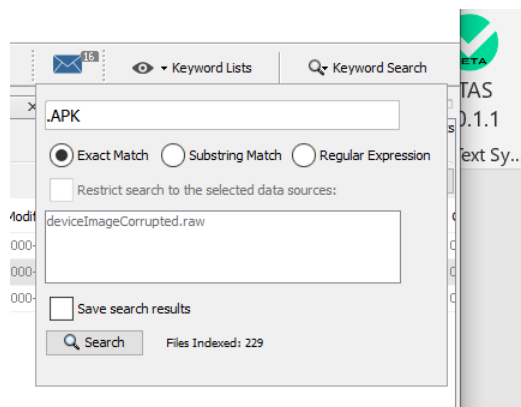
```
proxySettings
NONE
ids_
    AndroidAP
    12345678
    A4:99:47:3A:6D:C3 ←
    ctrl_interface=eth0
    driver_param=use_p2p_group_interface=1
    update_config=1
    device_name=u8833
    manufacturer=HUAWEI
    model_name=Ascend Y300
    model_number=Ascend Y300
    serial_number=A499473A61AE
    device_type=10-0050F204-5
    config_methods=physical_display virtual_push_button
    network={
        ssid="OptimaWifi"
        psk="2345678923456789lozinka!!"
        key_mgmt=WPA-PSK
        priority=4
    }
network=f
```

Thus:

interface	Mac address
Eth0	A4:99:47:3A:6D:C3

III. List 3 applications that were installed on the device:

In order to do so I looked up the extension .apk



Result :

[/system/app/ApplicationsProvider.apk](#)
[/system/app/Browser.apk](#)
[/system/app/Calculator.apk](#)
[/system/app/Calendar.apk](#)
[/system/app/CalendarProvider.apk](#)
[/system/app/CertInstaller.apk](#)
[/system/app/Contacts.apk](#)
[/system/app/ContactsProvider.apk](#)
[/system/app/DeskClock.apk](#)
[/system/app/Development.apk](#)
[/system/app/DownloadProvider.apk](#)
[/system/app/DrmProvider.apk](#)
[/system/app/FusedLocation.apk](#)

Therefore some three applications that were found on the device would be:

- Browser.apk
- Calculator.apk
- Contacts.apk

IV. Find the SSID network names and passwords for all the networks which the device ever connected to:

Looked up the word SSID and read the file and this was the result:

```
network={  
    ssid="OptimaWifi"  
    psk="2345678923456789lozinka!!"  
    key_mgmt=WPA-PSK  
    priority=4  
}  
  
network={  
    ssid="Stadion11Wifi"  
    psk="17386blue!"  
    key_mgmt=WPA-PSK  
    priority=8  
}  
.....
```

V. Find the SSID and the password of the WIFI hotspot of the device:

I looked for the host file since that's where network info is stored, and looked for SSID, and also "wpa" and this is the result:

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

```
f0011072.txt interface=eth0
ctrl_interface=/data/misc/wifi/hostapd
ssid=AndroidAP
auth_algs=1
max_num_sta=8
beacon_int=100
dtim_period=1
wpa=2
wpa_key_mgmt=WPA-PSK
wpa_pairwise=CCMP
wpa_passphrase=12345678
channel=6
driver=nl80211
hw_mode=g
```

VI. When was the contact Ivan BBB called and for how long did the call last?

Looked up the name of the contact:

Table calls4 entriesPage 1 of 1Export to CSV

_id	number	date	duration	type	new	name	numbert...	numbera...	countryiso	voicemail...	is_read	geocode...	lookup_uri	matched...	normaliz...	pl
1	+38513331000	1431725121112	0		0				HR		1	Croatia				0
2	+38513331000	1431790511455	86		0				HR		1	Croatia				0
3	+385981795597	1432147845356	25		0	Ivan BBB			HR		1	Croatia				0
4	+38514831483	1432143267849	66		0				HR		1	Croatia				0

As you can see the duration was 25 and the date is as follows:

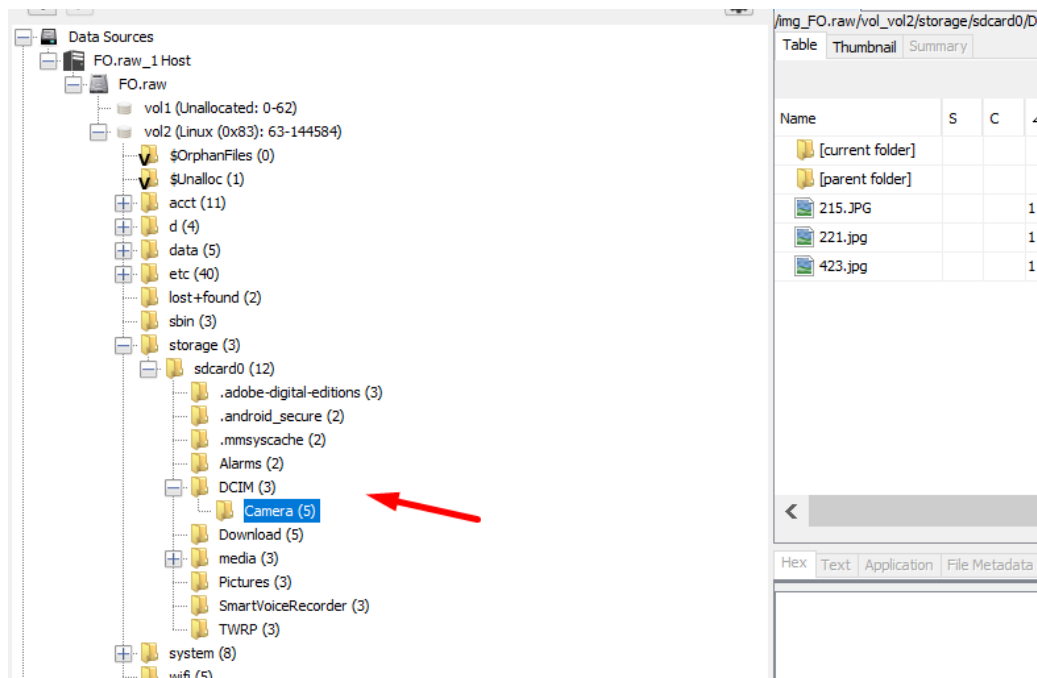
number	date	duration	type	new	name
+38513331000	1431790511455	86		0	
+385981795597	1432147845356	25		0	Ivan BBB
+38514831483	1432143267849				

Display as > Date
 Show only rows where > Raw Data

2	+38513331000	2015/05/16 16:35:11	86	
3	+385981795597	2015/05/20 19:50:45	25	
4	+38514831483	2015/05/20 18:34:27	66	

VII. Which movie did the user of the device search twice for on google?

The film is "American history x"



This is the image I found



Examining the EXIF metadata, I found no information regarding the location, no GPS coordinates, I also tried exiftool on kali Linux, but got same result.

However, I found this picture on the device:



Which indicates the football team name is west ham united, and since they're on same device I'm assuming the picture was taken in London.