

Digitalna forenzika

Forenzika mobilnih uređaja:
Implementacija alata zasnovanog na ADB alat za
forenziku android uređaja

Uvod

Mobilna forenzika se najviše razvila i sledećeg razloga:

- Kršenje zakona i razvoj kriminala
- Mobilni forenzičari mogu oporaviti izbrisane podatke i na taj način detektovati kriminalne radnje.

Forenzika mobilnih telefona

- Zaplena – proces zaplene uređaja i zaštita od spoljašnjih uticaja
- Pribavljanje podataka – ekstrakcija podataka sa uređaja i pribavljanje istih
- Analiza i izveštaj – analiza podataka

Tehnike pribavljanje podataka

- Ručna(Direktna ekstrakcija) podataka
- Fizička ekstrakcija podataka
- Logička ekstrakcija podataka
- Nasilna ekstrakcija podataka

Memorija telefona

- Interna – boot, system, data, misc, cache
- Eksterna - sdcard

Particije telefona

- Boot - interna
- Device - interna
- Data - interna
- System - interna
- Sdcard - eksterna
- Misc – interna

U nastavku će se vršiti ekstrakcija podataka sa data particije

ADB (Android debug bridge)

- Client – server alat koji omogućava komunikaciju sa android uređajem
- Kopiranje fajlova sa telefona, na telefon
- Instaliranje, debug aplikacija
- Pristup provajderima sadržaja
- Pristup shell-u

Adb komande

- Adb install <source> <dest>
- Adb push <source> <dest>
- Adb pull <source> <dest>
- Adb devices
- Adb shell – pristup shellu

```
C:\platform-tools>adb shell ls /system
apex
app
bin
build.prop
cust
data-app
etc
fonts
framework
lib
lib64
media
operator
priv-app
product
ro.prop
rw.prop
system_ext
usr
vendor
xbin
```


ADB shell

- Adb shell command
- `adb shell content query --uri <URI> [--projection <PROJECTION>] [--where <WHERE>] [--sort <SORT_ORDER>]`
- Primer: `adb shell content query --uri content://com.android.contacts/contacts`

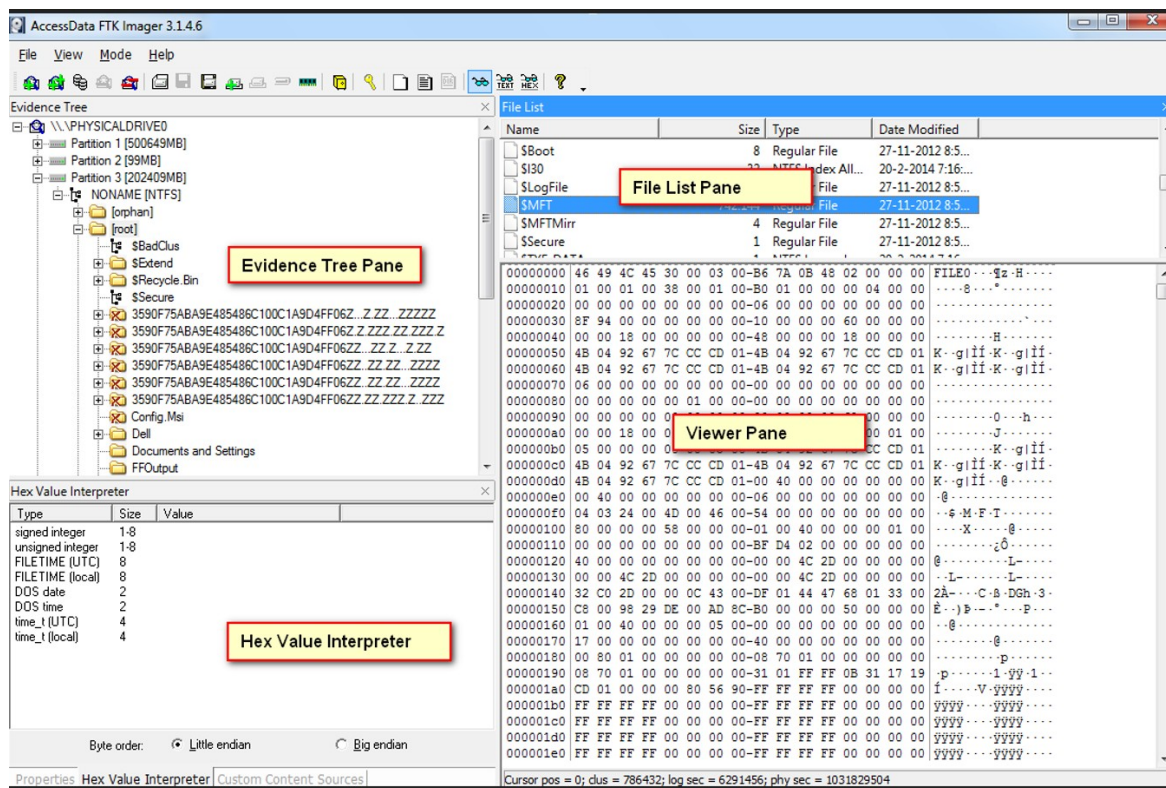
Provajderi sadržaja

- Kalendar
- Kontakti
- Poruke

Svaki kontent provajder izlaže javni URI (upakovan kao Uri objekat) koji jedinstveno identifikuje njegov skup podataka. Provajder sadržaja koji kontroliše više skupova podataka (više tabela) ima poseban URI za svaki od njih. Svi URI-ovi za provajdere počinju nizom content://. Na ovaj način se identifikuju podaci koje kontroliše provajder sadržaja. Takođe moguće je mnogi provajderi omogućavaju pristup jednom redu, samo dodavanjem ID-a na kraj putanje.

Alati za mobilnu forenziku

- Oxygen forensic detective
- MobileEdit
- ADEL (koristi adb)
- FTK imager



Oxygen forensics

Oxygen Forensic® Detective

Search - Apple iPhone 8 | Timeline - Apple iPhone 8

Extraction info | Export | Reset filters | View | Maps

Filters: Accounts (1), Groups (10), Contacts (248), Sources (47)

- Apple Messages (87)
- Apple Notes (20)
- Azar Messenger (20)
- Booking.com (33)
- Calendar (131)
- CoverMe (74)
- Endomondo (876)
- Event Log (53)
- FaceApp (1)
- Files (233)
- Firefox (14)
- Fitbit (301)
- Fly Delta (1)
- Google Chrome (17)
- Google Duo (4)
- Google Keep (7)
- Google Maps (1)
- Google Translate (21)
- Health (20 387)
- HeyTell (3)
- ICQ (18)
- Imo (13)
- Kakao Talk (1)
- Kik Messenger (998)
- KYMS - Keep your media safe (4)
- Line (27)
- Mail.Ru - Email App (44)
- Opera Mini Web Browser (13)
- OS Artifacts (272)
- Safari Browser (31)

All records (27 224) | Messages (4 494) | Calls (88) | Geolocations (1 037) | Web activity (61)

Find text...

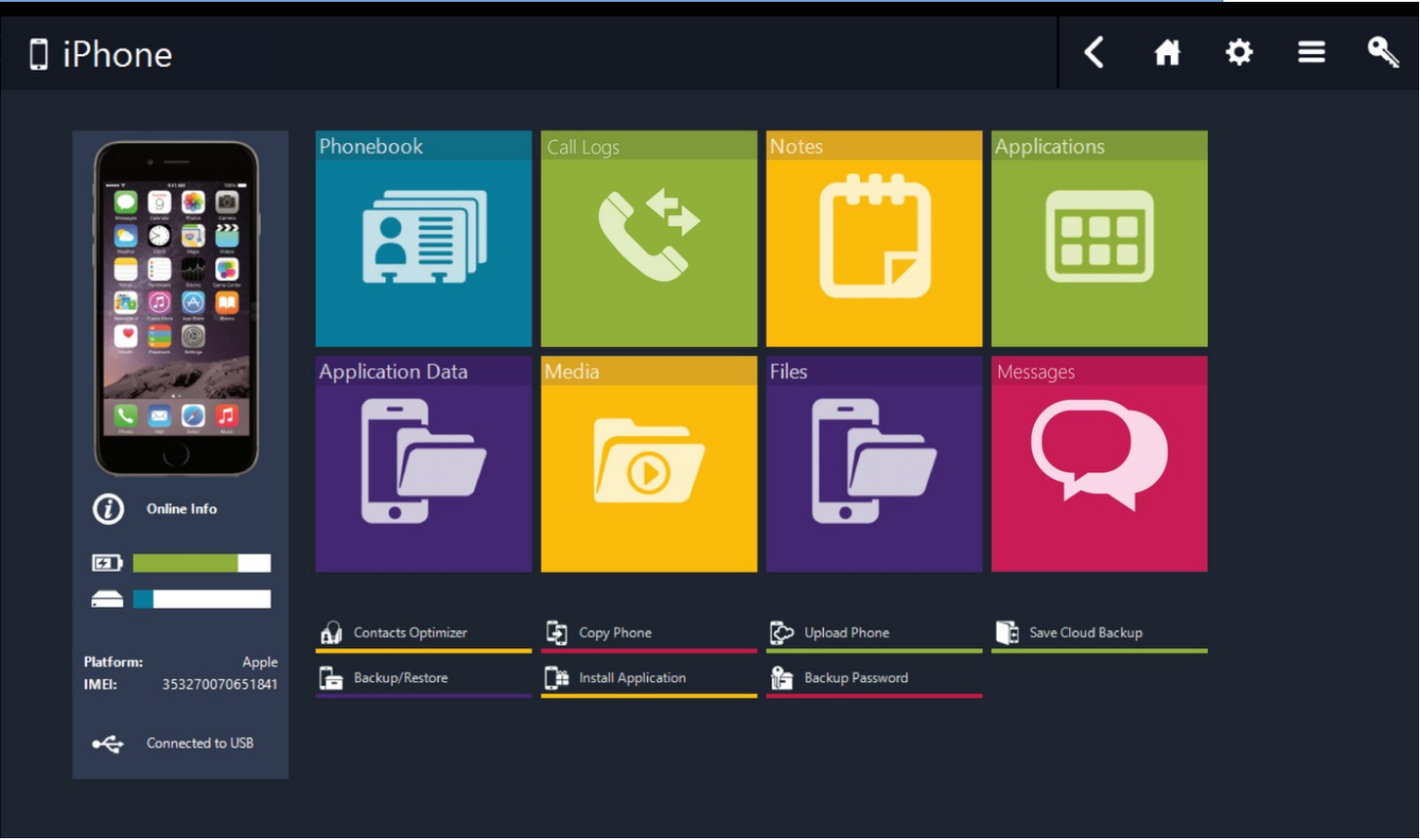
Type	Time stamp (GMT+9)	Description
Video file "MOV"	26.06.2018 09:40:12 (U...)	N 41.8954000, E 12.4844000 IMG_0131.MOV
Image file "HEIC"	26.06.2018 09:40:08 (U...)	N 41.8953861, E 12.4843778 IMG_0130.HEIC
Image file "HEIC"	26.06.2018 09:40:05 (U...)	N 41.8953889, E 12.4843722 IMG_0129.HEIC
Image file "HEIC"	26.06.2018 09:40:03 (U...)	N 41.8953861, E 12.4843444 IMG_0128.HEIC
Image file "HEIC"	26.06.2018 09:36:23 (U...)	N 41.8937639, E 12.4864611 IMG_0127.HEIC
Video file "MOV"	26.06.2018 09:34:43 (U...)	N 41.8938000, E 12.4865000 IMG_0126.MOV
Image file "HEIC"	26.06.2018 09:34:31 (U...)	N 41.8937944, E 12.4865139 IMG_0125.HEIC
Image file "HEIC"	26.06.2018 09:34:28 (U...)	N 41.8936806, E 12.4865000 IMG_0124.HEIC
Video file "MOV"	26.06.2018 09:31:43 (U...)	N 41.8948000, E 12.4862000 IMG_0123.MOV
Image file "HEIC"	26.06.2018 09:31:02 (U...)	N 41.8943528, E 12.4861083 IMG_0122.HEIC
Video file "MOV"	26.06.2018 09:29:30 (U...)	N 41.8940000, E 12.4866000 IMG_0121.MOV
Image file "HEIC"	26.06.2018 09:28:00 (U...)	N 41.8936667, E 12.4869861 IMG_0120.HEIC
Image file "HEIC"	26.06.2018 09:27:57 (U...)	N 41.8936806, E 12.4869917 IMG_0119.HEIC
Image file "HEIC"	26.06.2018 09:27:55 (U...)	N 41.8936944, E 12.4869778 IMG_0118.HEIC
Image file "HEIC"	26.06.2018 09:20:13 (U...)	N 41.8910778, E 12.4914111 IMG_0117.HEIC
Workout point	26.06.2018 09:34:24 (U...)	N 41.8968775, E 12.4829135 Coordinates: 41.8968774887553;12.48291346...
Workout point	26.06.2018 09:34:16 (U...)	N 41.8968767, E 12.4829131 Coordinates: 41.8968767162886;12.48291310...
Workout point	26.06.2018 09:34:08 (U...)	N 41.8968731, E 12.4829197 Coordinates: 41.8968730792062;12.48291970...
Workout point	26.06.2018 09:33:56 (U...)	N 41.8968907, E 12.4829391 Coordinates: 41.8968906716587;12.48293913...
Workout point	26.06.2018 09:33:42 (U...)	N 41.8969319, E 12.4829181 Coordinates: 41.8969319447037;12.48291809...
Workout point	26.06.2018 09:33:31 (U...)	N 41.8969111, E 12.4829092 Coordinates: 41.8969110703956;12.48290916...
Workout point	26.06.2018 09:33:14 (U...)	N 41.8968079, E 12.4829723 Coordinates: 41.8968078866991;12.48297225...
Workout point	26.06.2018 09:33:04 (U...)	N 41.8969152, E 12.4832201 Coordinates: 41.8969151750597;12.48322010...
Workout point	26.06.2018 09:32:44 (U...)	N 41.8968492, E 12.4830551 Coordinates: 41.8968491675722;12.48305507...
Workout point	26.06.2018 09:32:34 (U...)	N 41.8970279, E 12.4828956 Coordinates: 41.8970278697479;12.48289564...
Workout point	26.06.2018 09:32:11 (U...)	N 41.8969132, E 12.4828601 Coordinates: 41.8969132053125;12.48286010...
Workout point	26.06.2018 09:32:07 (U...)	N 41.8969132, E 12.4827912 Coordinates: 41.896913247222;12.482791207...
Workout point	26.06.2018 09:32:03 (U...)	N 41.8969125, E 12.4827273 Coordinates: 41.8969124928507;12.48272725...
Workout point	26.06.2018 09:32:00 (U...)	N 41.8969347, E 12.4826552 Coordinates: 41.8969347468036;12.48265516...

Group by: Year | Month | Day

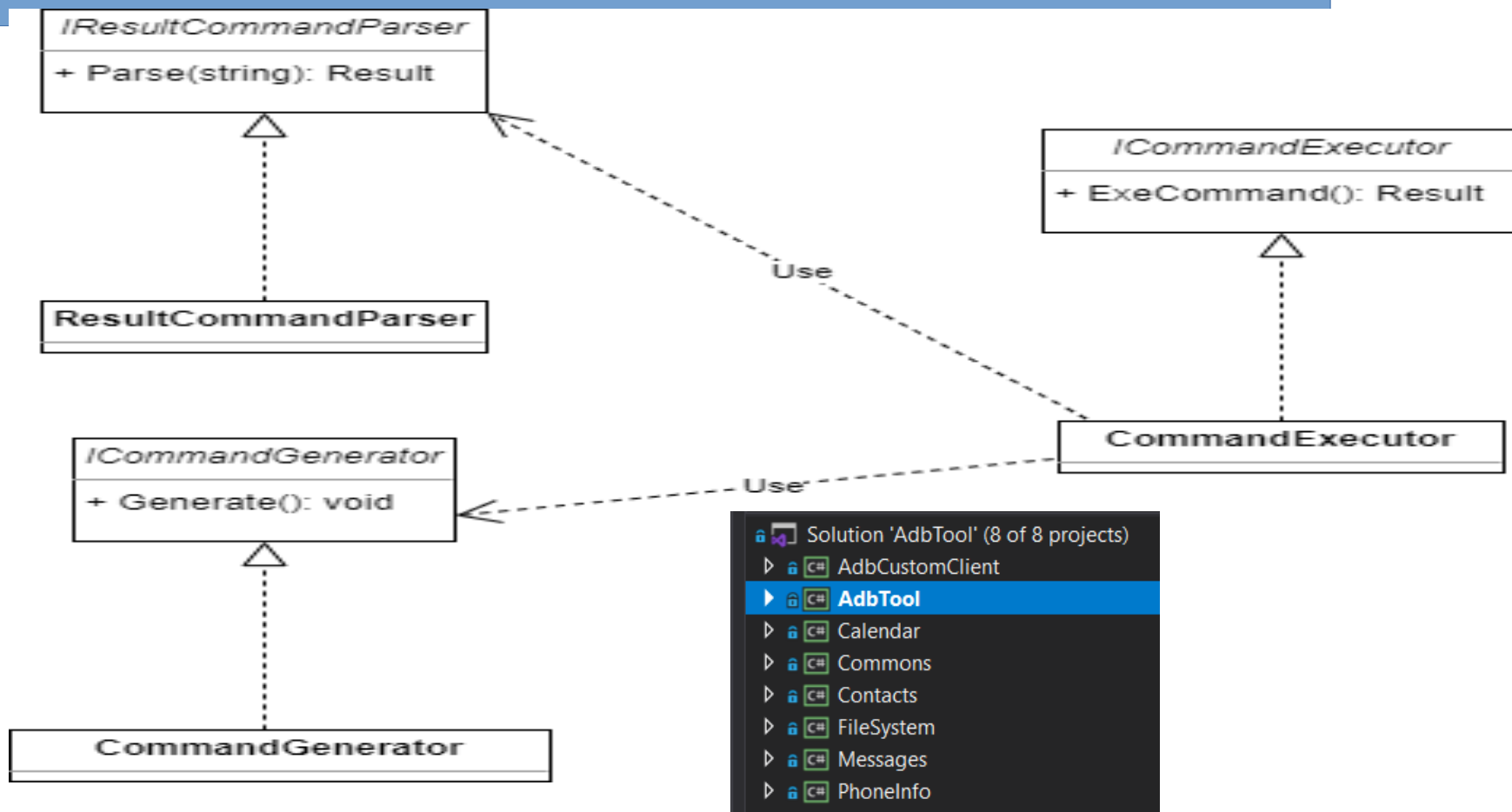
Version: 12.0.0.127 Total: 27 224 Filtered: 1 037 Selected: 1

You have 1 new notification

MobilEdit



Aplikacija



AF

Calendar/Events

Phone Info

Messages

Calendar/Events

Contacts

File System

Events

Calendar

Attendees

Export

eventTi...	account...	attende...	attende...	attende...	attende...	attende...	hasAlarm	calenda...
Europe/...	com.go...	#cetvrt...	cetvrta...	2	1	1	1	7
Europe/...	com.go...	Bratisla...	Bratisla...	1	NULL	1	1	7
Europe/...	com.go...	Emilija ...	emilija....	1	NULL	2	1	7
Europe/...	com.go...	Milos B...	Milos....	1	NULL	2	1	7
Europe/...	com.go...	Branko ...	branko....	1	NULL	2	1	7
Europe/...	com.go...	Mirjana...	mirjana...	1	NULL	2	1	7
Europe/...	com.go...	bogosav...	bogosav...	1	NULL	2	1	7
Europe/...	com.go...	Dunja C...	dunja.c...	1	NULL	2	1	7
Europe/...	com.go...	Marija ...	marija....	1	NULL	2	1	7
Europe/...	com.go...	stefan.t...	stefan.t...	1	NULL	2	1	7
Europe/...	com.go...	dragan....	dragan....	1	NULL	2	1	7
Europe/...	com.go...	Zoran ...	Zoran.P...	1	NULL	2	1	7
Europe/...	com.go...	Jovana ...	jovana...	1	NULL	2	1	7

AF

File System

Phone Info

Download

Messages

Calendar/Events

Contacts

File System

- oem
- proc
- product
- res
- sdcard
- storage
 - 9016-4EF8
 - emulated
 - self
 - primary
 - Alarms
 - Android
 - Audiobooks
 - DCIM
 - Documents
 - Download