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

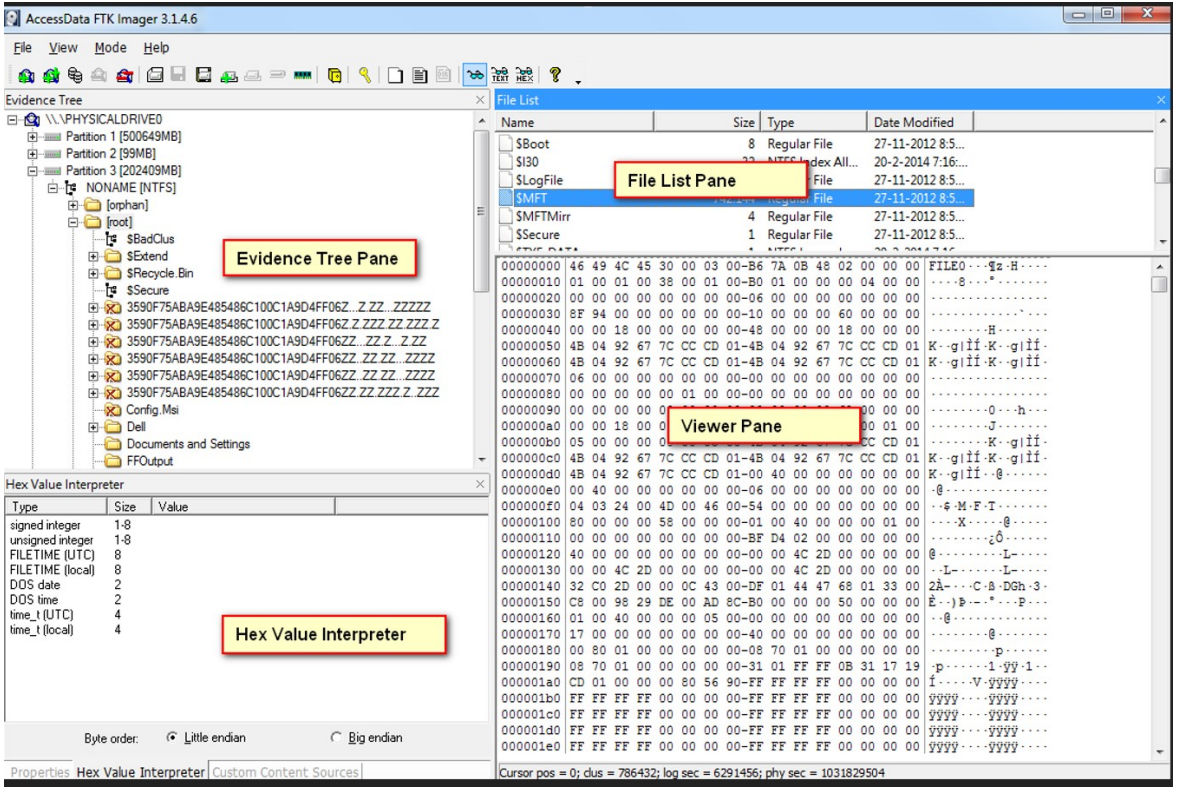
Provajderi sadrzaja

- Kalendar
- Kontakti
- Poruke

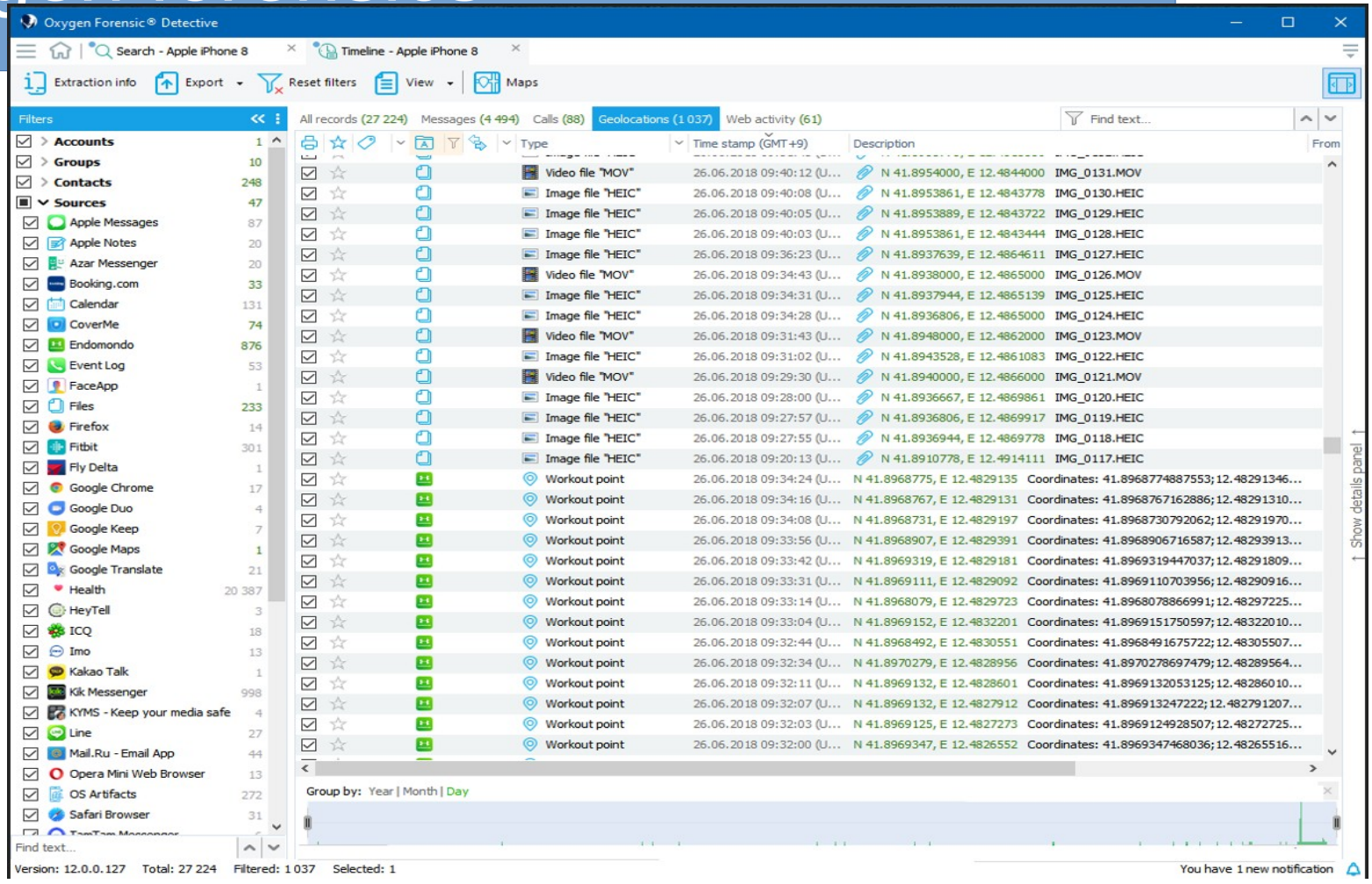
Svaki kontent provajder izlaže javni URI (upakovan kao Uri objekat) koji jedinstveno identifikuje njegov skup podataka. Provajder sadržaja koji kontroliše više skupova podataka (više tabela) ima poseban URI za svaki od njih. Svi URI-ovi za provajdere počinju nizom content://. Na ovaj način se identifikuju 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

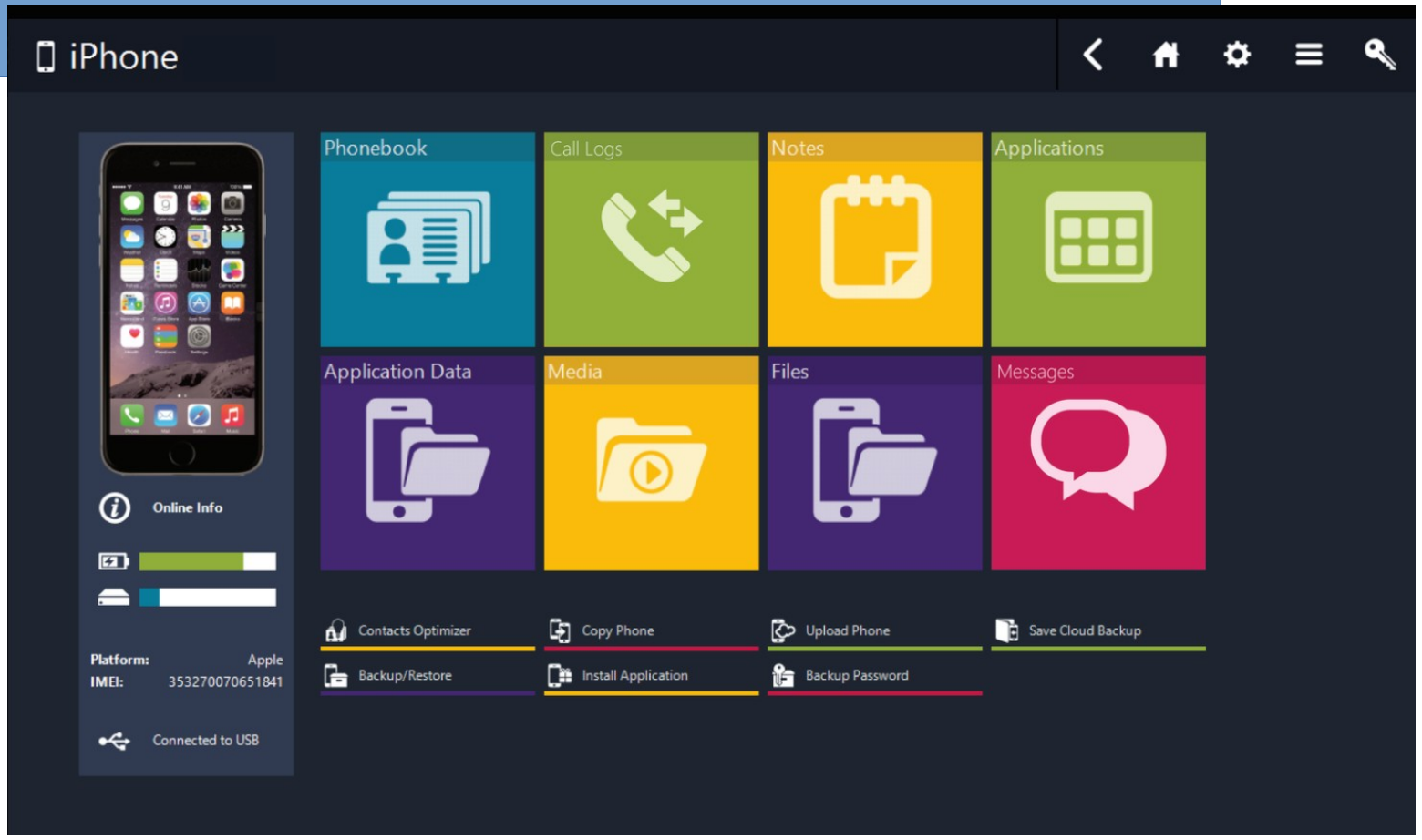
- Oxygen forensic detective
- MobileEdit
- ADEL (koristi adb)
- FTK imager



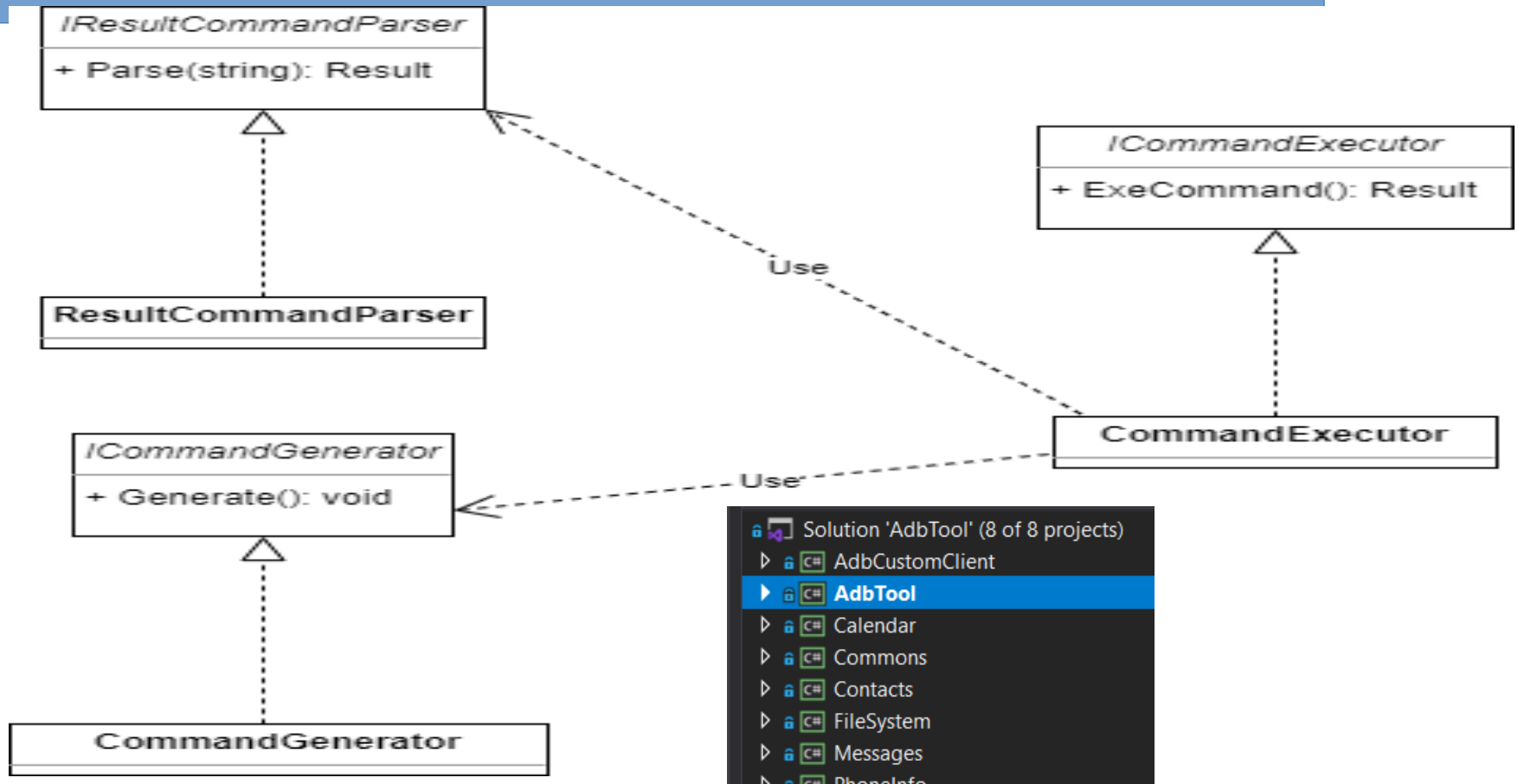
Oxygen forensics

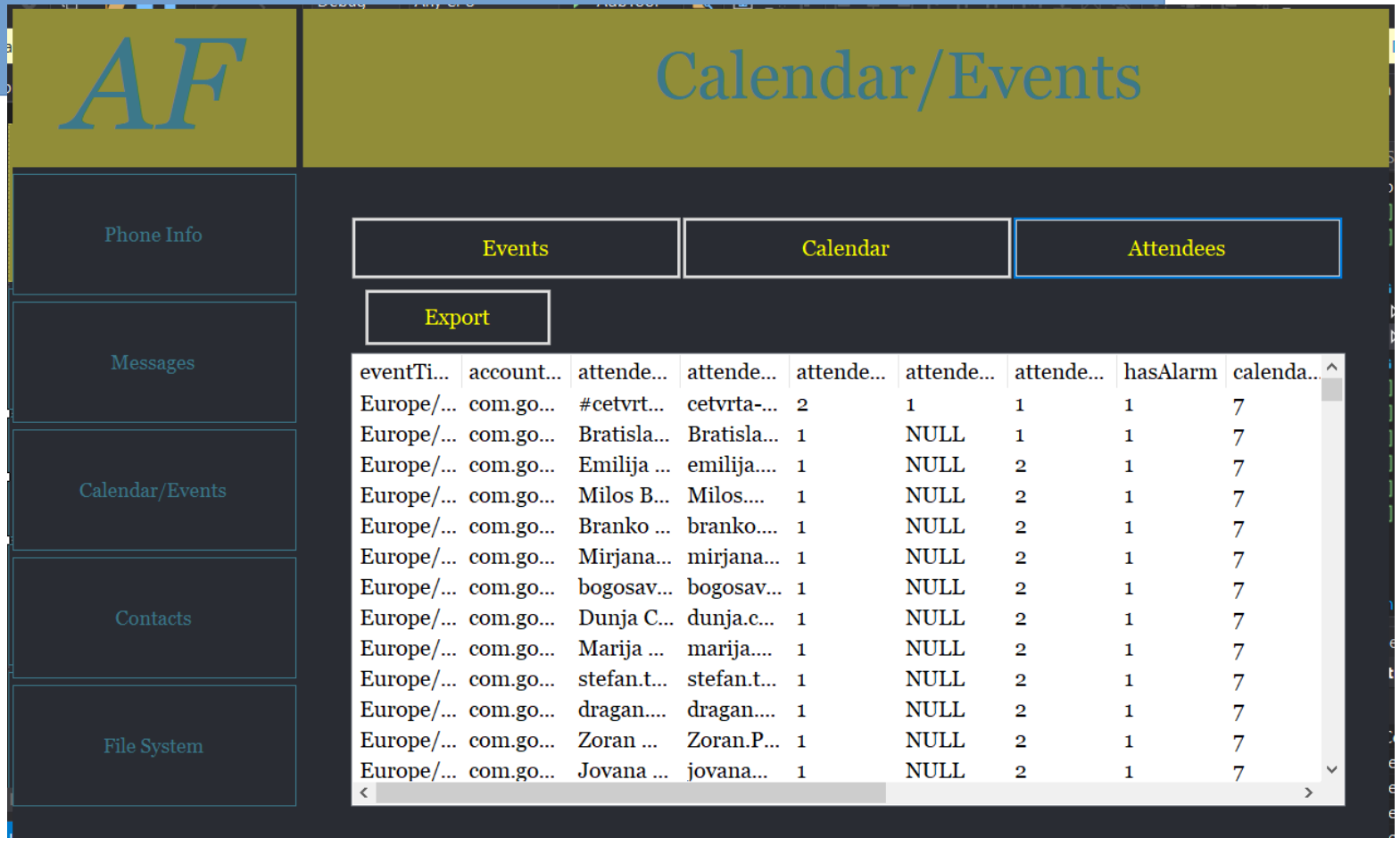


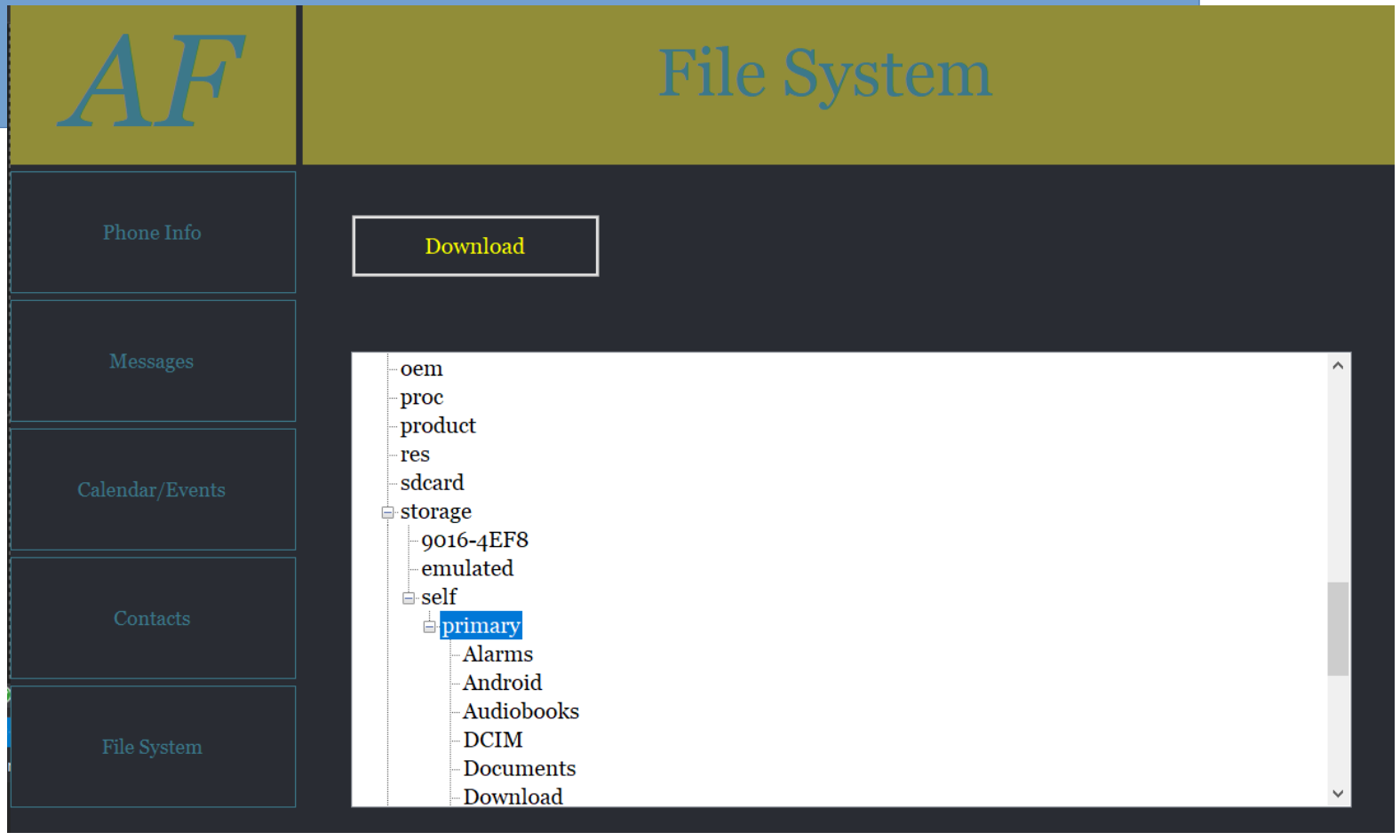
MobilEdit


iPhone
Online Info
Platform: Apple
IMEI: 353270070651841
Connected to USB
Phonebook
Call Logs
Notes
Applications
Application Data
Media
Files
Messages
Contacts Optimizer
Copy Phone
Upload Phone
Save Cloud Backup
Backup/Restore
Install Application
Backup Password

Aplikacija


IResultCommandParser
+ Parse(string): Result
ICommandExecutor
+ ExeCommand(): Result
Use
ResultCommandParser
CommandExecutor
ICommandGenerator
+ Generate(): void
Use
CommandGenerator
Solution 'AdbTool' (8 of 8 projects)
AdbCustomClient
AdbTool
Calendar
Commons
Contacts
FileSystem
Messages
PhoneInfo


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
Messages
Calendar/Events
Contacts
File System
Download
oem
proc
product
res
sdcard
storage
9016-4EF8
emulated
self
primary
Alarms
Android
Audiobooks
DCIM
Documents
Download