



Факултет техничких наука
Лабораторија за дигиталну форензику

ФОРЕНЗИКА МОБИЛНИХ УРЕЂАЈА

Увод у дигиталну форензику
Милица Матијевић, Светлана Антешевић

Преглед области

Чиме се бави форензика мобилних уређаја?

Форензика мобилних уређаја је грана дигиталне форензике чији предмет су докази ускладиштени на мобилним уређајима или преношени путем целуларне мреже.



Преглед области

Које све доказе можемо прикупити?

- Дневници комуникација и листе контаката
- Календари и подсетници
- SMS, MMS, инстант поруке (Viber, WhatsApp, Messenger итд.)
- Електронска пошта
- Прегледање интернета
- Фотографије и видео снимци
- Документа
- Локација и кретање корисника итд.

Преглед области

Зашто је значајна?

- Мобилни уређаји су увек поред корисника,
- преносиви су,
- користе целуларну мрежу,
- користе се интимније и чешће него рачунари,
- користе се за шири спектар потреба,
- већа заступљеност,
- новији телефони представљају компактне рачунаре,
- садрже велику количину информација ...

Преглед области

Шта представља изазов?

- Мноштво хардверских архитектура, оперативних система, апликација, произвођача
- Безбедносне функције мобилне платформе
- Криптографска заштита на различитим слојевима архитектуре
- Удаљено брисање или измена података (уређај је бежично повезан са интернетом)
- Закључавање екрана
- Комуникација преко целуларне мреже (подаци се уз наредбу суда могу добити од мобилног оператора)

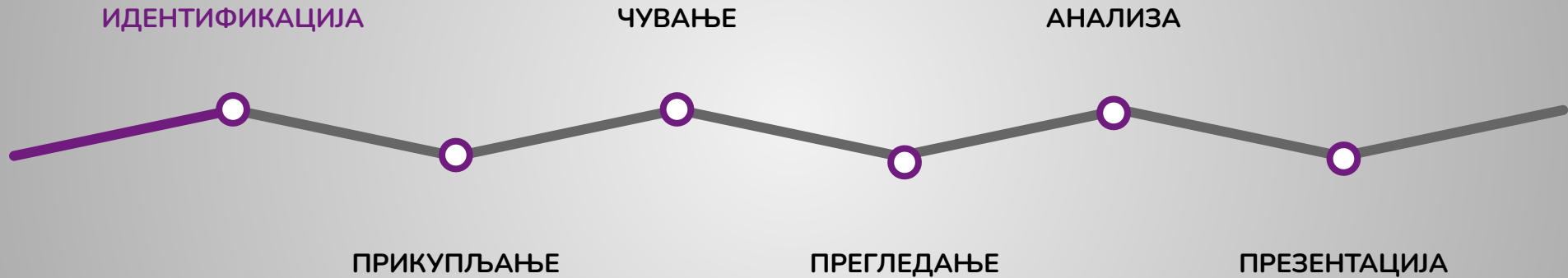
Преглед области

Како можемо идентификовати мобилне уређаје?

Mobile Equipment Identifier (MEID) – глобално јединствен идентификатор за уређаје у CDMA мрежи или

International Mobile Station Equipment Identity (IMEI) – глобално јединствен идентификатор за уређаје у GSM, UMTS, LTE мрежи.

Процес форензичке истраге



Напомена – етапе форензичке истраге не одвијају се секвенцијално. Често су репетитивне.

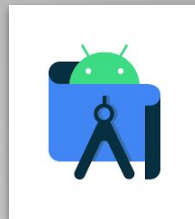
Идентификација

Односи се на детектовање, препознавање и одређивање дигиталних уређаја које треба истражити.

Под идентификацијом се подразумева и читавање идентификатора дигиталних уређаја, који се истражују (произвођач, модел, серијски број, IMEI).

Примери: мобилни уређај, таблет, SIM картица, SD картица, документација о месту догађаја (фотографије, видео снимци, гласовни снимак), просторија у којој се налази уређај, стање уређаја, књиге, белешке, каблови...

Идентификација



Android Studio

Интегрисано развојно окружење за Google-ов оперативни систем Android. Креиран од стране JetBrains' IntelliJ IDEA. Дизајнирано посебно за прављење Android апликација.

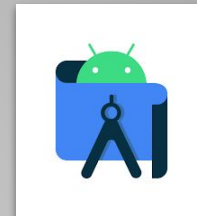
Android SDK

Комплет за развој софтвера који укључује свеобухватан скуп развојних алата. Ово укључује програм за отклањање грешака, библиотеке, емулатор телефона, документацију, пример кода и упутства.

Напомена: Демонстрација је везана за Android оперативни систем.

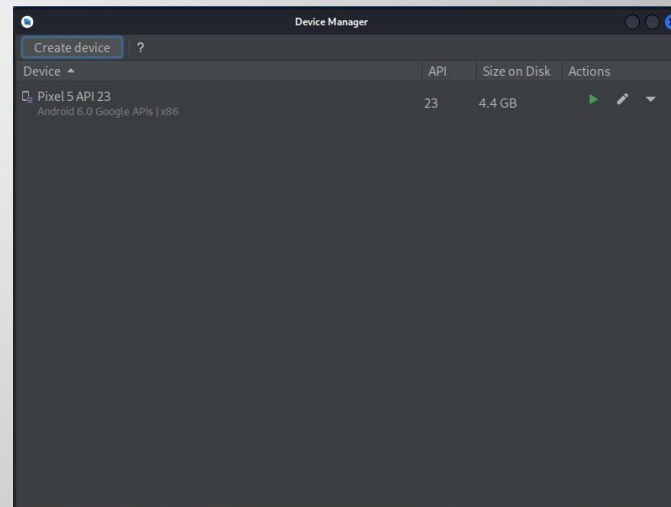
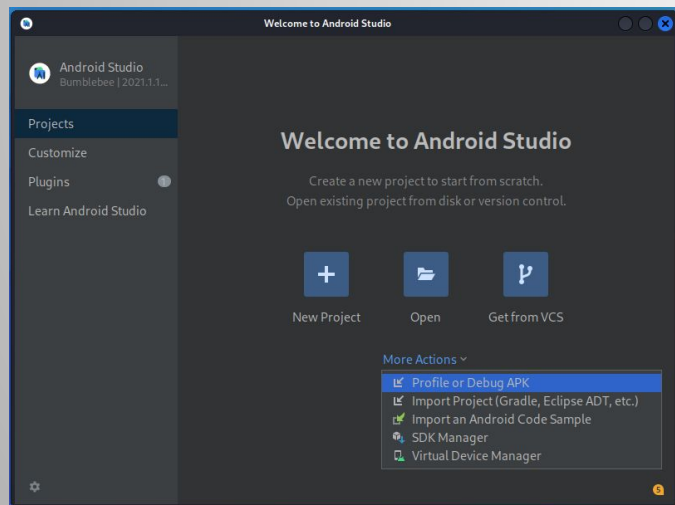
За потребе вежби користићемо Android Emulator како бисмо симулирали мобилни уређај.

Идентификација



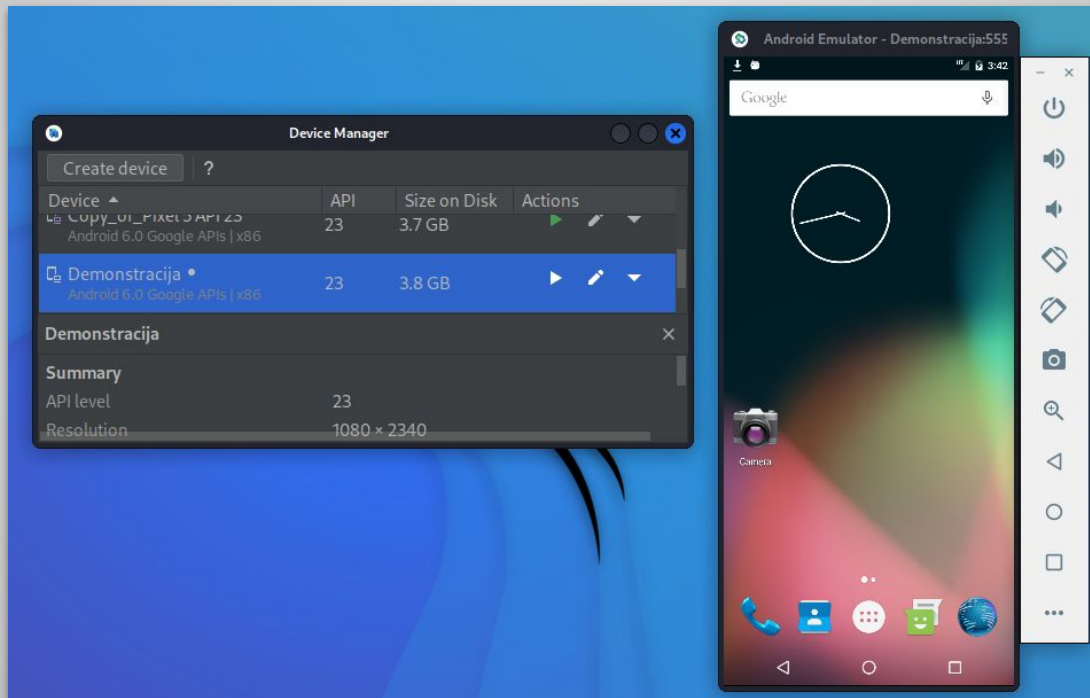
Android Emulator - покретање преко GUI-а Android Studio-а

1. У оквиру менија куцамо Android Studio и покренемо
2. Одаберемо опцију MoreActions, па одаберемо опцију Virtual Device Manager
3. Креирамо уређај и покренемо га на зелену стрелицу

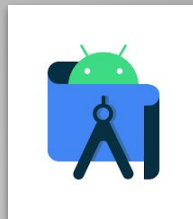


Идентификација

Android Emulator - покретање преко GUI-а Android Studio-а



Идентификација



Android Emulator - покретање помоћу терминала

\$ cd /home/kali/Android/Sdk/emulator - позиционирање у фолдер где се налази емулатор

\$./emulator -list-avds - излиставање свих емулираних уређаја

\$./emulator -avd <naziv> - покретање једног помоћу његовог назива

Идентификација

Произвођач: Google

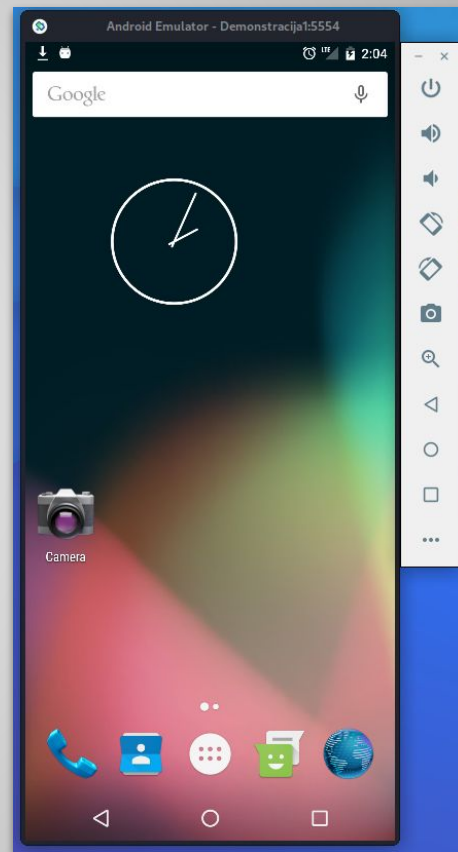
Модел: Pixel 5

Оперативни систем: Android

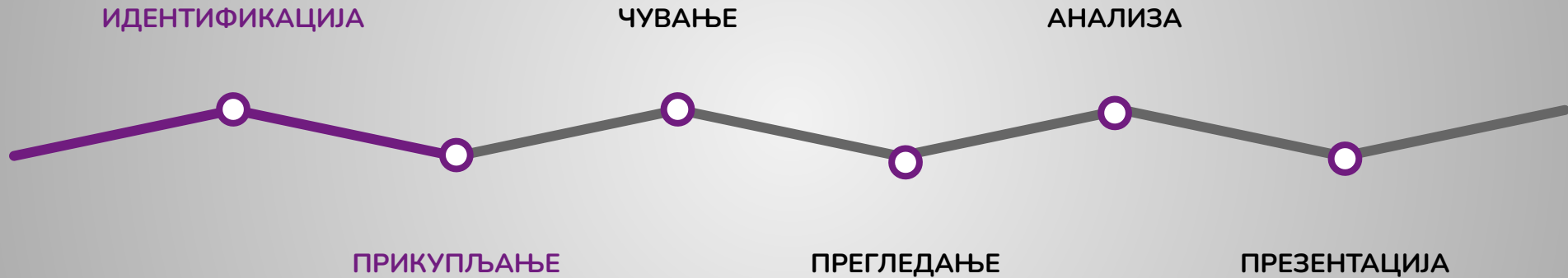
Верзија ОС: 6.0

Серијски број: EMULATOR31X2X8X0

IMEI: 358240005111110



Процес форензичке истраге



Напомена – етапе форензичке истраге не одвијају се секвенцијално. Често су репетитивне.

Прикупљање

Идентификоване доказе је потребно прикупити коришћењем научно и правно ваљаних метода.

Прављење форензичке копије мобилног уређаја, SIM картице, SD картице.

Потребно је припремити медије на којима се прави форензичка копија.

Опрема:

- Фарадејева врећа
- Dongle
- JTAG, ISP, ChipOff
- Читачи SD картица
- SIM клонер
- Каблови и адаптери

Прикупљање

Припрема

- Овлашћења (правна надлежност)
- Тренутно стање уређаја
- Битни/тражени подаци за истрагу
- Подаци о произвођачу, моделу уређаја
- Идентификација других потенцијалних извора доказа: SD, SIM, отисци прситију, сигурносне копије података у облаку...



Прикупљање

Изоловање

→ Мрежна изолација

- ◆ Фарадејева врећа
- ◆ Режим летења
- ◆ Лабораторије које су изоловане
- ◆ Откључавање у зависности од локације
- ◆ Клонирање SIM картице

→ Повезати уређај на извор напајања

→ Онеспособити закључавање уређаја

- ◆ Уређај који симулира додиривање екрана - **Dongle**
- ◆ Омогућити опцију да телефон увек остане будан **Settings/Display & brightness/Sleep - never**



Прикупљање

Откључавање мобилних уређаја

Реконструкција или погађање кода, обрасца, лозинке итд.

Промена конфигурационих датотека или брисање датотека са подацима за аутентификацију (ако је приступ интерном складишту података омогућен)

Откључавање помоћу мрежних сервиса (Google, Samsung..)

Примена специјалних софтверских алата (често није могућа са новијим верзијама Androida и iOS-a)

Прикупљање

Методе екстракције података

РУЧНО

ЛОГИЧКИ

ФИЗИЧКИ

ПРИКУПЉАЊЕ ИЗ
ОБЛАКА

ПРИКУПЉАЊЕ ИЗ
ЦЕЛУЛАРНЕ МРЕЖЕ



Факултет техничких наука
Лабораторија за дигиталну форензику

РУЧНО ПРИКУПЉАЊЕ

Увод у дигиталну форензику
Милица Матијевић, Светлана Антешевић

Ручно прикупљање

- Прикупљање коришћењем корисничког интерфејса мобилног уређаја.
- Докази се прикупљају на највишем нивоу апстракције.
- Приступамо само оним подацима које нам ОС дозвољава да прегледамо.
- Услов: да је уређај функционалан и отључан.
- Неопходно је да снимимо процес.
- Једноставно је интерпретирати податке.
- Поступак може да промени стање уређаја.



Факултет техничких наука
Лабораторија за дигиталну форензику

ЛОГИЧКО ПРИКУПЉАЊЕ

Увод у дигиталну форензику
Милица Матијевић, Светлана Антешевић

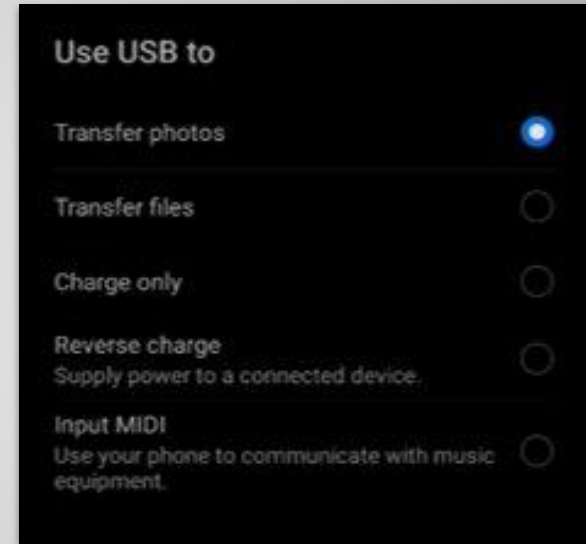
Логичко прикупљање - MTP

Media Transfer Protocol (MTP)

1. Потребно је повезати рачунар и мобилни уређај USB каблом
2. Пребацити уређај у „мод за пренос мултимедијалног садржаја" или „мод за пренос фотографија"
3. Добићемо приступ фолдерима, чији садржај је могуће преузети:

`/sdcard/DCIM`

`/sccard/Pictures`

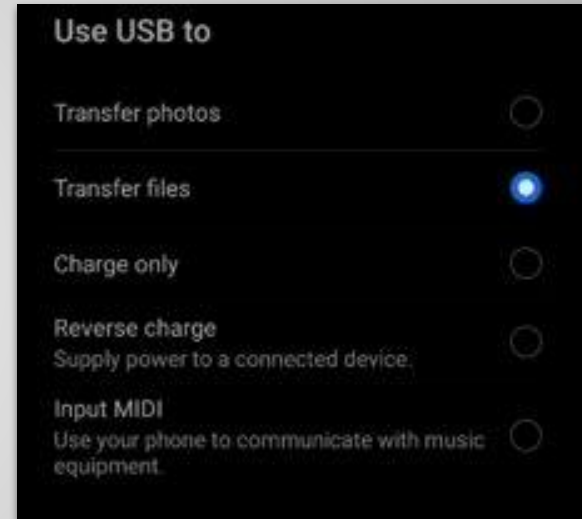


Логичко прикупљање - UMS

USB Mass Storage (UMS)

1. Потребно је повезати рачунар и мобилни уређај USB каблом
2. Пребацити уређај у „мод за пренос датотека“
3. Добићемо приступ само једном делу интерног складишта података

/sdcard

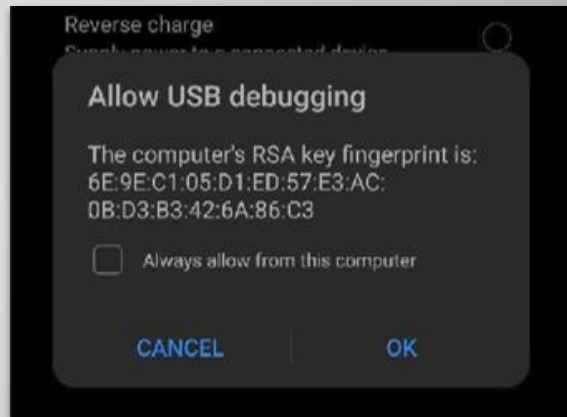


Логичко прикупљање - ADB

Android Debugging Bridge (ADB)

Софтверски алат за комуникацију са Android уређајима. Служи углавном за отклањање грешака на Android уређајима приликом програмирања.

1. Потребно је укључити „USB проналажење грешака“ (енг. USB debugging)
2. Потребно је повезати рачунар и мобилни уређај USB каблом
3. Пребацити уређај у „мод за пренос датотека“
4. Могуће је из терминала уносом команди преузети податке са уређаја.
 - а. Да бисмо могли да преузмемо цело складиште података потребан је **root** приступ.



Логичко прикупљање - ADB

Android Debugging Bridge (ADB) - команде

Да бисмо добили листу повезаних мобилних уређаја који су повезани на рачунар користимо следећу команду:

```
$ adb devices
```

Помоћу наредне команде можемо приступити интерном складишту података преко терминала на рачунару и прегледати га:

```
$ adb shell
```

Приказ информација о доступном, искоришћеном и укупном простору на уређају можемо добити помоћу команде disk free (df)

```
$ [adb shell] df
```

Логичко прикупљање - ADB

Android Debugging Bridge (ADB) - команде

Листу апликација које су инсталиране можемо добити командом:

```
$ adb shell pm list packages
```

Да бисмо преузели цело или део интерног складишта података користимо следећу команду:

```
$ adb pull [source path] [destination path]
```

Остале команде могу се наћи на [линку](#).

Логичко прикупљање - ADB

Android Debugging Bridge (ADB) - команде

У оквиру ADB-а постоји **dumpsys** команда која пружа информације о системским услугама које се користе (није потребан root приступ), а које нам могу дати корисне информације.

Можемо добити информације о RAM меморији, батерији, дијагностици мреже...

Покреће се над тренутно повезаним уређајем.

Листа свих активних системских услуга: **\$ adb shell dumpsys [-l]**

- `adb shell dumpsys procstats --hours 3`
- `adb shell dumpsys batterystats`
- `adb shell dumpsys netstats detail`
- `adb shell dumpsys backup`
- `adb shell dumpsys wifi`

Логичко прикупљање - Content Providers

Добављачи садржаја (енг. Content Providers)

Могуће је добити одређене информације о добављачима садржаја помоћу ADB алата, помоћу команде:

```
$ adb shell dumpsys package providers
```

AF Logical OSE - Android форензичка апликација и оквир отвореног кода. Омогућава испитивачу да издвоји позиве из евиденције позива, телефоне контаката, MMS поруке и SMS поруке са Android уређаја

Инсталирати апликацију на телефон командом

```
$ adb install AFLogical-OSE_1.5.2.apk
```

Преузети податке са телефона на рачунар командом

```
$ adb pull /sdcard/forensics/ [destination]
```



Логичко прикупљање - Backup

Сигурносне копије података (енг. backup)

Могу бити ускладиштене на SD картици, на РС рачунарима повезаним са мобилним уређајем или у облаку. Обично су шифроване.

Може им се приступити коришћењем стандардних софтверских алата за рад са сигурносним копијама или специјализованим форензичким алатима уз познавање криптографског кључа.

Могуће је помоћу ADB-а направити сигурносне копије података које не захтевају root приступ и помоћу одређених алата за рад са сигурносним копијама прегледати садржај.

Логичко прикупљање - Backup

Сигурносне копије података (енг. backup)

Команда за прављење сигурносне копије је следећа:

```
$ adb backup [-f <file>] [-apk|-noapk] [-shared|-noshared] [-all] [-system|-nosystem]
[<packages...>]
```

- **-f** : путања *.ab датотеке која ће бити сачувана на рачунару.
- **-apk|-noapk** : означава да ли треба направити резервну копију *.apk датотека (default is -noapk)
- **-obb|-noobb** : омогући/ономогући резервну копију било које инсталиране арк датотеке повезане са сваком апликацијом (default is -noobb)
- **-shared|-noshared**: омогући/ономогући резервну копију дељене меморије уређаја, садржаја SD картице (default is -noshared)
- **-all** : означава да желите да направите резервну копију целог система. Можете користити филтер пакета само да направите резервну копију одређених пакета или користите -all за потпуну резервну копију система.
- **-system|-nosystem**: показује да ли су све системске апликације и подаци укључени приликом прављења резервне копије. (default is -system)
- **<packages>** : овде можете навести одређене пакете за резервну копију. Користите их ако желите да направите резервну копију само одређених апликација. Ако користите -all, не морате да наводите пакете.

Пример: \$ adb backup -apk -shared -all -nosystem -f backup.ab

Биће тражено на уређају да унесете лозинку (користи се због шифровања резервне копије)

Логичко прикупљање

Меморијске картице (енг. Secure Digital - SD)

Користе преносни уређаји: фотоапарати, камере, паметни телефони..

Постоје различите физичке димензије: standard, mini, micro

Постоје различите класе

Ако су подаци ускладиштени на SD картици и нису шифровани, могуће их је прикупити читачем SD картица.

Новији модели SD могу да шифрују податке.



Логичко прикупљање

Рутовање (енг. rooting)

Рутовање је процес стицања привилегованог приступа на Android уређају.

Root приступ уређају омогућава приступ партицијама и директоријумима којима се не може приступити преко UMS, MTP, ADB.

Метод за преузимање целог интерног складишта података искоришћавањем рањивости оперативног система са циљем да се добије root приступ уређају.

Конкретне рањивости које се могу искористити у великој мери зависе од верзије ОС.

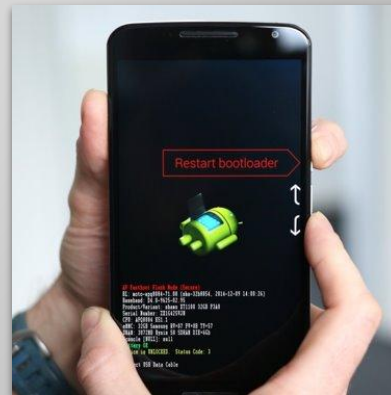
Логичко прикупљање

Boot-овање (енг. booting)

Други метод за преузимање целог интерног складишта података је учитавање наменског оперативног система уместо Android-а или iOS-а.

Наменски оперативни систем омогућава директан приступ складишту података и партицијама.

Учитавање наменског оперативног система није могуће ако уређај користи безбедно учитавање оперативног система.





Факултет техничких наука
Лабораторија за дигиталну форензику

ФИЗИЧКО ПРИКУПЉАЊЕ

Увод у дигиталну форензику
Милица Матијевић, Светлана Антешевић

Физичко прикупљање

Joint Test Action Group (JTAG)

Индустријски стандард за тестирање штампаних плоча.

Може да се користи за задавање инструкција процесору да прикупи сирове податке ускладиштене у флеш (полупроводничка меморија) меморијском чипу на штампаној плочи како би се направила слика целе интерне меморије уређаја.

Није деструктивни процес ако се изведе без грешке, у супротном се може уништити мобилни уређај.

Проблем представља енкрипција података, на нивоу партиција или појединачних датотека.



Физичко прикупљање

In-System Programming (ISP)

Представља својство неких уграђених уређаја да могу да се програмирају и када су инсталирани у крајњем систему.

Слична JTAG техници, али не може на свим уређајима. Само неки садрже протокол да се чипови програмирају док се налазе на крајњем систему тј. залемљени за штампану плочу.

Није деструктиван процес ако се изведе без грешке.



Физичко прикупљање

ChipOff

Најкомплекснија и најскупља метода.

Процес у коме се меморијски чип уклања са уређаја/матичне плоче да би се прочитао читачем, да би се направила слика целе интерне меморије.

Деструктивни процес, уређај више неће радити после примене овог поступка.

Потребно је залемити пинове на матичну плочу, а то захтева одређене вештине.





Факултет техничких наука
Лабораторија за дигиталну форензику

ПРИКУПЉАЊЕ ИЗ ОБЛАКА

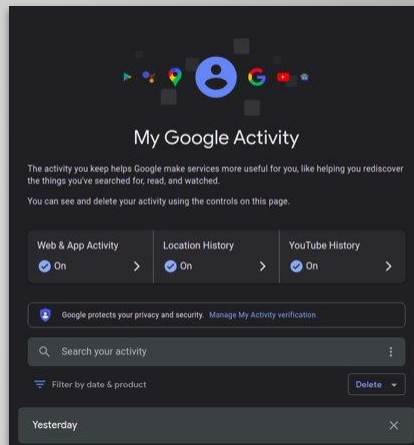
Увод у дигиталну форензику
Милица Матијевић, Светлана Антешевић

Прикупљање из облака

Неки докази могу бити ускладиштени у облаку тј. на неком серверу на интернету.

Google, Apple, Huawei нуде мрежне сервисе који омогућавају синхронизацију података између два мобилна уређаја или мобилног уређаја и рачунара.

Уз познавање корисничког имена и лозинке могуће је приступити тим сервисима и преузети податке.





Факултет техничких наука
Лабораторија за дигиталну форензику

ПРИКУПЉАЊЕ ИЗ ЦЕЛУЛАРНЕ МРЕЖЕ

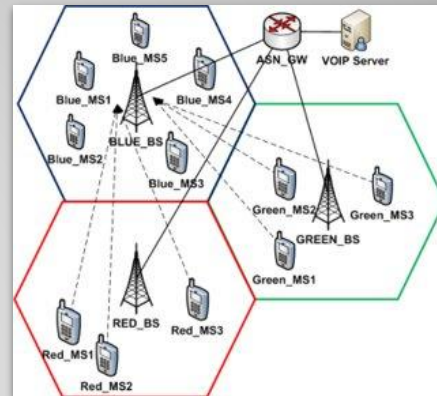
Увод у дигиталну форензику
Милица Матијевић, Светлана Антешевић

Прикупљање из целуларне мреже

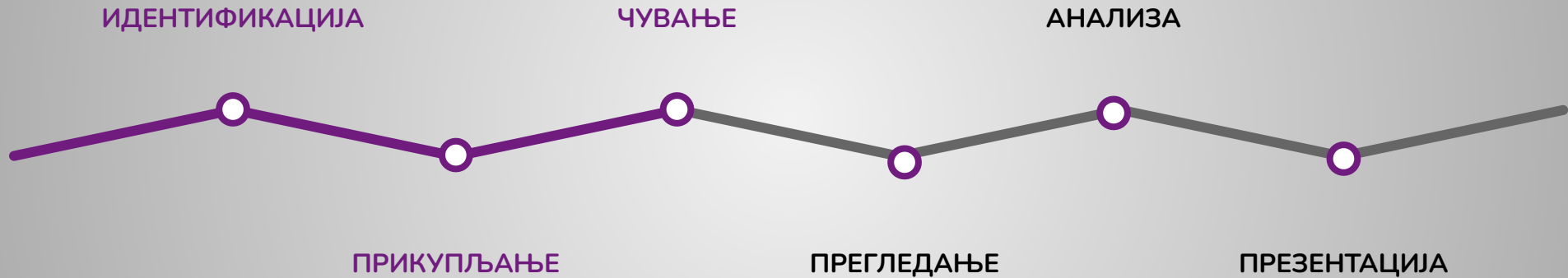
Могуће добити од телекомуникационих оператора уз наредбу суда, задржане податке call detail record (CDR).

На основу задржаних података је могуће реконструисати комуникације између претплатника, локације претплатника, али не и садржај комуникације.

Могуће је клонирати SIM картицу помоћу клонера SIM картица и прикупити потенцијалне податке: сачувани контакти, позиви, поруке..



Процес форензичке истраге



Напомена – етапе форензичке истраге не одвијају се секвенцијално. Често су репетитивне.

Чување

Прикупљени докази морају се сачувати коришћењем физичких, техничких и организационих контрола.

Верификација прикупљених података спроводи се помоћу рачунања хеш вредности (са неким од алгоритама: sha1, sha256, md5) да би се обезбедио интегритет доказа.

Рачунање хеш вредности:

- MD5 алгоритам: **\$ [sudo] md5sum [path]**
- SHA1 алгоритам: **\$ [sudo] sha1sum [path]**

Чување

Ланац доказа - евиденција о томе када и ко је имао приступ доказима.

Факултет техничких наука, Лабораторија за дигиталну форензику, Трг Доситеја Обрадовића 6, 21102 Нови Сад,
+381 214854565, +381 66 8211617, digfor@uns.ac.rs, <https://digfor.ftn.uns.ac.rs/>

ОБРАЗАЦ ЕВИДЕНЦИЈЕ РУКОВАЊА ДОКАЗНИМ МАТЕРИЈАЛОМ

Идентификатор предмета:
Идентификатор доказног материјала:
Произвођач:
Модел:
Серијски број:

Бр.	Датум	Име и презиме	Опис радње	Потпис
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Чување

Докази се чувају у одговарајућем формату датотека који омогућавају компресију података, поделу датотека на више датотека и шифровање датотека.

- XRY - власнички формат датотека (XRY)
- DD, ISO - сирови формати датотека
- AB - формат сигурносне копије направљене помоћу ADB-a

Процес форензичке истраге



Напомена – етапе форензичке истраге не одвијају се секвенцијално. Често су репетитивне.

Прегледање и анализа

Android partition layout

Изглед партиција варира између произвођача и верзија, али неколико партиција је присутно на свим Android уређајима

```
1|generic_x86:/ $ svetlana@svetlana:~$ adb shell
generic_x86:/ $ df -h

```

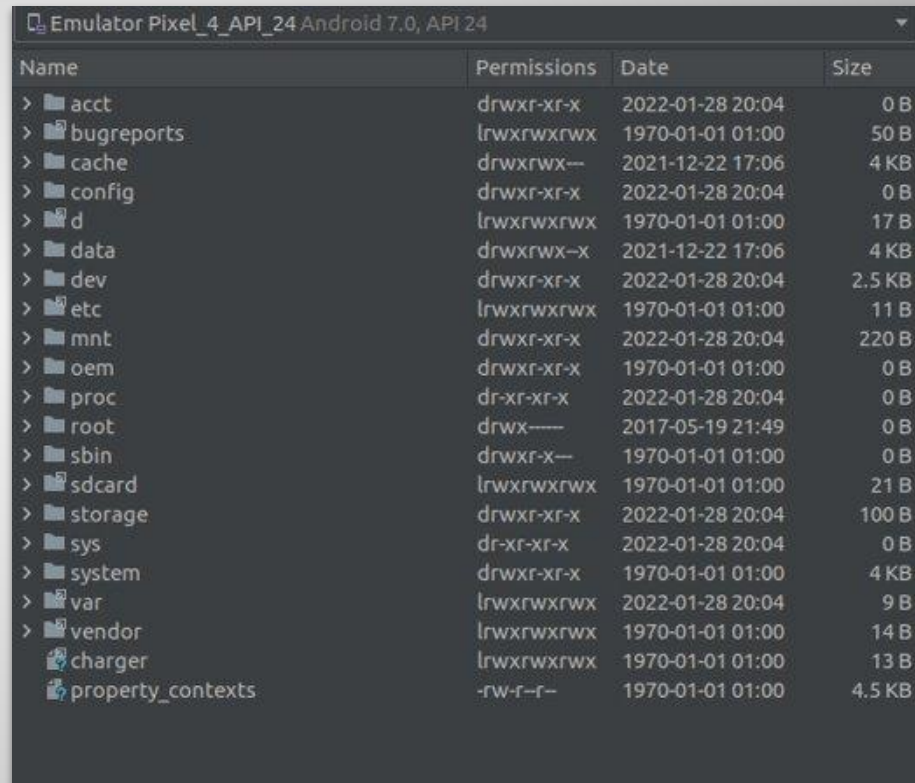
Filesystem	Size	Used	Avail	Use%	Mounted on
tmpfs	757M	460K	757M	1%	/dev
tmpfs	757M	0	757M	0%	/mnt
/dev/block/vda	1.9G	1.6G	244M	88%	/system
/dev/block/vdb	61M	68K	60M	1%	/cache
tmpfs	757M	0	757M	0%	/storage
/dev/block/dm-0	5.8G	1.1G	4.6G	20%	/data
/dev/fuse	5.8G	1.1G	4.6G	20%	/storage/emulated
/dev/fuse	510M	88K	510M	1%	/storage/160E-1716

```
svetlana@svetlana:~$
```


Прегледање и анализа

Android file hierarchy

Основно разумевање начина на који Android организује своје податке у датотеке и фасцикле помаже форензичком аналитичару да сузи своје истраживање на одређене локације.



Name	Permissions	Date	Size
> /acct	drwxr-xr-x	2022-01-28 20:04	0 B
> /bugreports	lrwxrwxrwx	1970-01-01 01:00	50 B
> /cache	drwxrwx---	2021-12-22 17:06	4 KB
> /config	drwxr-xr-x	2022-01-28 20:04	0 B
> /d	lrwxrwxrwx	1970-01-01 01:00	17 B
> /data	drwxrwx-x	2021-12-22 17:06	4 KB
> /dev	drwxr-xr-x	2022-01-28 20:04	2.5 KB
> /etc	lrwxrwxrwx	1970-01-01 01:00	11 B
> /mnt	drwxr-xr-x	2022-01-28 20:04	220 B
> /oem	drwxr-xr-x	1970-01-01 01:00	0 B
> /proc	dr-xr-xr-x	2022-01-28 20:04	0 B
> /root	drwx-----	2017-05-19 21:49	0 B
> /sbin	drwxr-x---	1970-01-01 01:00	0 B
> /sdcard	lrwxrwxrwx	1970-01-01 01:00	21 B
> /storage	drwxr-xr-x	2022-01-28 20:04	100 B
> /sys	dr-xr-xr-x	2022-01-28 20:04	0 B
> /system	drwxr-xr-x	1970-01-01 01:00	4 KB
> /var	lrwxrwxrwx	2022-01-28 20:04	9 B
> /vendor	lrwxrwxrwx	1970-01-01 01:00	14 B
> /charger	lrwxrwxrwx	1970-01-01 01:00	13 B
> /property_contexts	-rw-r--r--	1970-01-01 01:00	4.5 KB

Autopsy & The Sleuth Kit

Autopsy модули за преглед података са мобилних уређаја:

```
$ cd /opt/ALEAPP-3.1.6
$ python aleappGUI.py
```

→ **iLeapp** модул везан за преглед података прикупљених са iOS телефона.



Прегледање и анализа



DB Browser for SQLite

Софтверски алат који служи за прегледање и анализу SQLite база података.

Омогућава да истражите датотеке базе података са следећим екстензијама: .sqlite, .sqlite3, .sqlitedb, .db, и .db3.

Подаци се углавном налазе у оквиру **/data/data** секције код мобилних уређаја.

Прегледање и анализа



Andriller

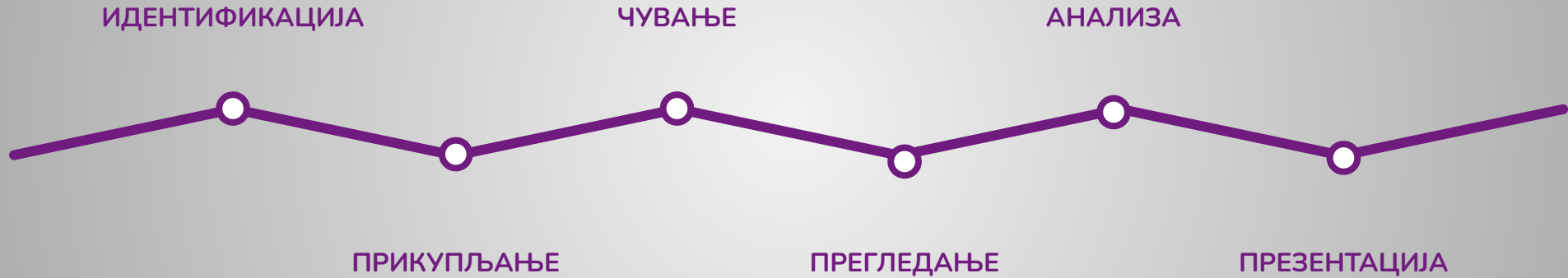
Andriller је софтверски услужни програм са колекцијом форензичких алата за паметне телефоне.

- Прикупљање доказа на повезаним телефонима.
- Креирање backup (ab) датотека.
- Прегледање и анализа Android фајл система.
- Подржава распакивање Android backup датотека.
- Прегледање и анализа Android backup datoteka.

Прегледање и анализа

Прегледање и анализа .csv датотека добијених помоћу AFLogical OSE алата помоћу LibreOffice Calc софтвера.

Процес форензичке истраге



Напомена – етапе форензичке истраге не одвијају се секвенцијално. Често су репетитивне.

Презентација

Резултати анализе доказа се презентују у писменом облику.

Односи се на процес којим форензичар дели резултате фазе анализе у облику извештаја заинтересованим странама.

Форензичар обично сачињава налаз и мишљење и усмено га брани одговарајући на питања на главном судском претресу.

Корисни линкови и књиге

Линкови:

- <https://www.kali.org/docs/>
- <https://github.com/abrignoni/ALEAPP>
- <https://github.com/den4uk/andriller>
- <https://developer.android.com/studio>
- <https://sqlitebrowser.org/>

Књиге:

- *Digital Forensics with Kali Linux*
- *Digital forensics : an academic introduction*
- *Learning Android Forensics*
- *Learning iOS Forensics*
- *Practical Mobile Forensics*

