# Zabezpieczanie i Analiza Danych z Urządzeń Mobilnych

## Wykład #6 – Proces identyfikacji, zabezpieczania, analizy i prezentacji danych z urządzeń mobilnych

[1]

# Plan wykładu

- Zarys metod akwizycji
- Poziomy akwizycji
  - Dokumentacja fotograficzna/pisemna
  - Akwizycja logiczna
  - Akwizycja fizyczna
- Zarys procesu
  - Identyfikacja
  - Przygotowanie
  - Zabezpieczenie
  - Akwizycja
  - Dokumentacja i raportowanie akwizycji
  - Analiza
  - Dokumentacja i raportowanie analizy
  - Prezentacja
  - Archiwizacja

# Zarys metod akwizycji

**Urządzenia mobilne nie były tworzone z myślą o informatyce śledczej,** dlatego mechanizmy wykorzystywane do zbierania z nich danych są kwestią oferowanych przez urządzenie (zamierzonych i nie) funkcjonalności oraz naszej inwencji.

Bardzo często wykorzystywane są (zarówno amatorsko, jak i przez profesjonalne narzędzia do mobile forensics) wbudowane narzędzia, protokoły i mechanizmy służące m.in. do:

- synchronizacji (kontaktów, plików etc.)
- wykonywania kopii bezpieczeństwa
- dokonywania napraw (tryb recovery w Androidzie)
- rozwijania oprogramowania (Android Debug Bridge)
- serwisowe (JTAG)

Do tego często stosuje się narzędzia do łamania zabezpieczeń (root exploity, łamacze kryptograficzne, znane metody obejścia blokady ekranu) itd.

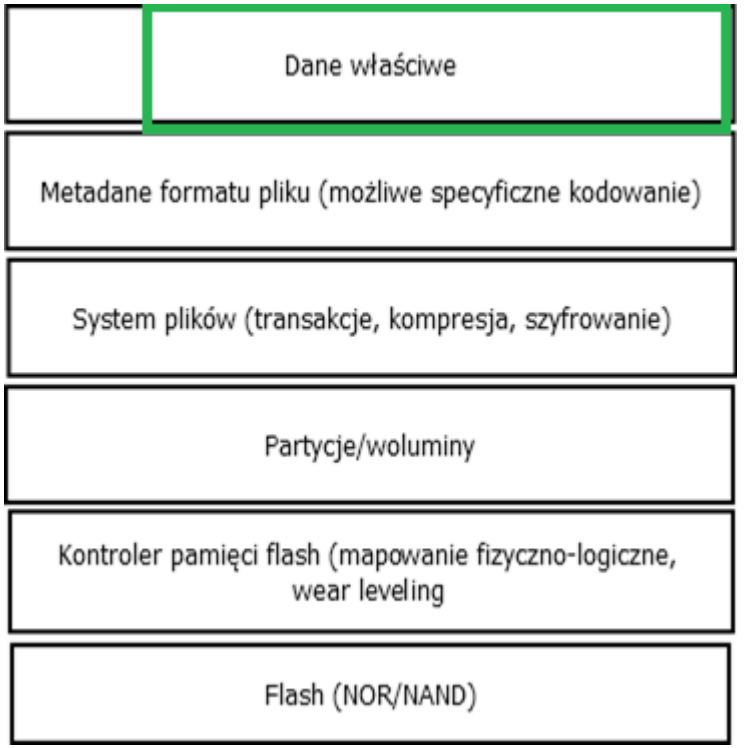
# Inwazyjność metod akwizycji a dowód elektroniczny

- Główną zasadą stosowaną w informatyce śledczej jest nieingerowanie w dane będące dowodem elektronicznym
- Szczególnie w przypadku urządzeń mobilnych ze względów praktycznych mamy do czynienia z umiarkowanym odstępstwem od tego założenia
- Dopuszczane jest ingerowanie w dowód w sposób wiarygodnie udokumentowany, z zastosowaniem minimum koniecznych do przeprowadzenia akwizycji zmian (rekonfiguracja urządzenia, przełamanie zabezpieczeń, modyfikacja oprogramowania itd.).

# Poziomy akwizycji – dokumentacja pisemna/fotograficzna

Metoda polegająca na **manualnym przejrzeniu zawartości urządzenia** (historia połączeń, SMS-y itd.), dokumentowana poprzez sporządzenie pisemnego protokołu (ręcznym przepisaniu danych) lub wykonywaniem fotografii ekranu urządzenia, powszechnie stosowana przed pojawieniem się narzędzi do mobile forensics jak i w przypadku niewspieranych modeli.

Ten typ akwizycji oferuje najbardziej skąpy zakres danych; **jedynie to, co uda się osobie egzaminującej wyświetlić na wyświetlaczu i sfotografować/przepisać.**

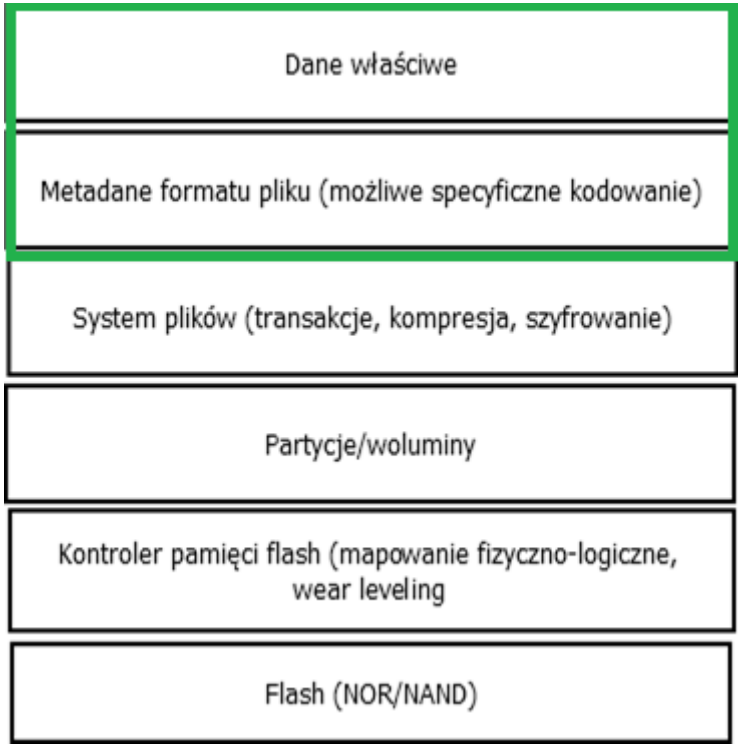


# Poziomy akwizycji – akwizycja logiczna

Metoda polegająca na wykonaniu kopii plików, które są **widoczne z poziomu systemu plików**/wbudowanej logiki urządzenia. Dane usunięte nie wchodzą zatem w zakres zebranych danych (z drobnymi wyjątkami).

Przy akwizycji logicznej plików tracone są również atrybuty nadawane przez dany system plików (np. właściciel, data utworzenia) o ile kopia nie jest wykonywana bezpośrednio na inny nośnik o tym samym systemie plików.

Nic nie stoi jednak na przeszkodzie, by przepisać odczyty atrybutów oryginalnych plików do oddzielnego loga.



# Akwizycja logiczna – adb pull

Przykład #1 – skopiowanie plików poprzez adb

Wymagania: włączone debugowanie USB+root/dostęp do trybu recovery

```
root@kali:~/FORENSIC/playground/w0rm# adb devices
List of devices attached
0123456789ABCDEF        device

root@kali:~/FORENSIC/playground/w0rm#
```

```
root@kali:~/FORENSIC/playground/w0rm# adb pull /data/data/com.android.providers.contacts/databases/contacts2.db
459 KB/s (321536 bytes in 0.683s)
root@kali:~/FORENSIC/playground/w0rm#
```

Pierwszy rzut oka pokazuje, że nie zachowały się atrybuty systemu plików:

```
root@kali:~/FORENSIC/playground/w0rm# adb shell ls /data/data/com.android.providers.contacts/databases/ -la
drwxrwx--x    1 app_6    app_6         2048 May 18 09:21 .
drwxr-x--x    1 app_6    app_6         2048 Jan  6  1980 ..
-rw-rw----    1 app_6    app_6       321536 May 18 09:20 contacts2.db
-rw-rw----    1 app_6    app_6            0 May 18 09:20 contacts2.db-journal
-rw-rw----    1 app_6    app_6       135168 Apr 19 16:48 profile.db
-rw-rw----    1 app_6    app_6            0 Apr 19 16:48 profile.db-journal
root@kali:~/FORENSIC/playground/w0rm# ls -la contacts2.db
-rwxrwxrwx 1 root root 321536 May 20 11:34 contacts2.db
root@kali:~/FORENSIC/playground/w0rm#
```

# Akwizycja logiczna – adb pull

Można również pobierać całe katalogi:

```
root@kali:~/MOBILE/playground/w0rm/dbs# adb pull /data/data/
pull: building file list...
skipping special file '.socket790'
pull: /data/data/com.andrew.apollo/shared_prefs/apollopreferences.xml -> ./com.andrew.apollo/shared_prefs/apollopref
pull: /data/data/com.andrew.apollo/shared_prefs/artistimage.xml -> ./com.andrew.apollo/shared_prefs/artistimage.xml
pull: /data/data/com.andrew.apollo/shared_prefs/albumimage.xml -> ./com.andrew.apollo/shared_prefs/albumimage.xml
pull: /data/data/com.andrew.apollo/shared_prefs/artistid.xml -> ./com.andrew.apollo/shared_prefs/artistid.xml
pull: /data/data/com.andrew.apollo/shared_prefs/artistimageoriginal.xml -> ./com.andrew.apollo/shared_prefs/artistimag
pull: /data/data/com.android.bluetooth/databases/btopp.db -> ./com.android.bluetooth/databases/btopp.db
pull: /data/data/com.android.bluetooth/databases/btopp.db-journal -> ./com.android.bluetooth/databases/btopp.db-journa
pull: /data/data/com.android.bluetooth/shared_prefs/OPPMGR.xml -> ./com.android.bluetooth/shared_prefs/OPPMGR.xml
pull: /data/data/com.android.browser/shared_prefs/com.android.browser_preferences.xml -> ./com.android.browser/shared_
pull: /data/data/com.android.browser/shared_prefs/browser_recovery_prefs.xml -> ./com.android.browser/shared_prefs/bro
pull: /data/data/com.android.browser/app_appcache/ApplicationCache.db -> ./com.android.browser/app_appcache/Applicatio
pull: /data/data/com.android.browser/databases/browser2.db -> ./com.android.browser/databases/browser2.db
pull: /data/data/com.android.browser/databases/webview.db -> ./com.android.browser/databases/webview.db
pull: /data/data/com.android.browser/databases/autofill.db -> ./com.android.browser/databases/autofill.db
pull: /data/data/com.android.browser/databases/webviewCookiesChromium.db -> ./com.android.browser/databases/webviewCoo
pull: /data/data/com.android.browser/databases/autofill.db-journal -> ./com.android.browser/databases/autofill.db-jour
pull: /data/data/com.android.browser/databases/webviewCookiesChromiumPrivate.db -> ./com.android.browser/databases/web
pull: /data/data/com.android.browser/databases/webview.db-wal -> ./com.android.browser/databases/webview.db-wal
pull: /data/data/com.android.browser/databases/webview.db-shm -> ./com.android.browser/databases/webview.db-shm
pull: /data/data/com.android.browser/databases/browser2.db-wal -> ./com.android.browser/databases/browser2.db-wal
pull: /data/data/com.android.browser/databases/browser2.db-shm -> ./com.android.browser/databases/browser2.db-shm
pull: /data/data/com.android.browser/cache/webviewCacheChromium/f_00002d -> ./com.android.browser/cache/webviewCacheCh
pull: /data/data/com.android.browser/cache/webviewCacheChromium/f_00002e -> ./com.android.browser/cache/webviewCacheCh
pull: /data/data/com.android.browser/cache/webviewCacheChromium/index -> ./com.android.browser/cache/webviewCacheChrom
pull: /data/data/com.android.browser/cache/webviewCacheChromium/data_0 -> ./com.android.browser/cache/webviewCacheChro
pull: /data/data/com.android.browser/cache/webviewCacheChromium/data_1 -> ./com.android.browser/cache/webviewCacheChro
pull: /data/data/com.android.browser/cache/webviewCacheChromium/data_2 -> ./com.android.browser/cache/webviewCacheChro
```

# Akwizycja logiczna - cp

Przykład #2 – skopiowanie plików poprzez cp na zamontowaną uprzednio kartę SD

Wymagania: włączone debugowanie USB+root/dostęp do trybu recovery

Pierwszy rzut oka pokazuje, że nie zachowały się atrybuty systemu plików:

```
root@kali:~/FORENSIC/playground/w0rm# adb shell
~ # cp /data/data/com.android.providers.contacts/databases/contacts2.db /sdcard
~ # ls -la /sdcard/contacts2.db
----rwxr-x    1 system   sdcard_r    321536 May 20 11:40 /sdcard/contacts2.db
~ # ls -la /data/data/com.android.providers.contacts/databases/contacts2.db
-rw-rw----    1 app 6    app 6       321536 May 18 09:20 /data/data/com.android.providers.contacts/databases/c
```

**Tracone przy zwykłym kopiowaniu atrybuty można oczywiście przepisać (wymusić ich wartości na docelowym nośniku), wymaga to jednak zastosowania tego samego systemu plików, precyzyjnego odczytywania atrybutów źródłowych i (wskazane) automatyzacji.**

# Akwizycja logiczna – instalacja aplikacji i dostęp przez provierów

Wymagania: USB debugging

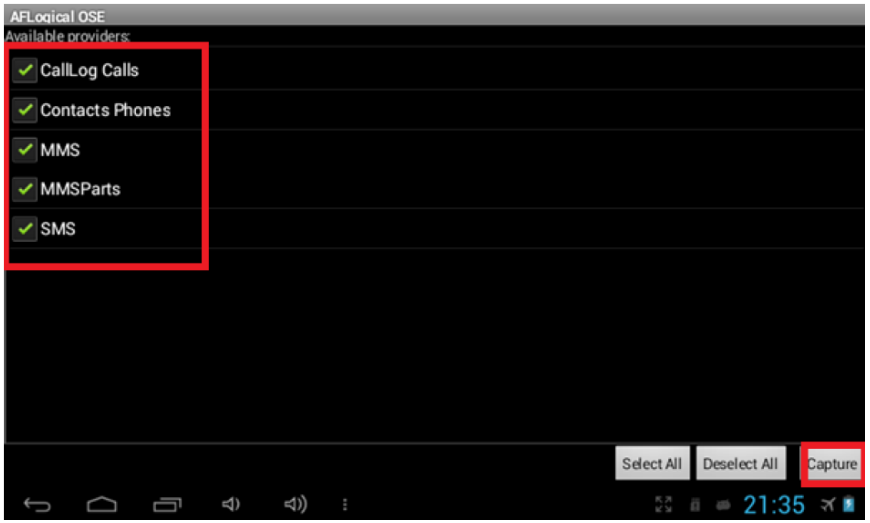
Instalacja i wywołanie z poziomu adb (przykład: AFLogical OSE)

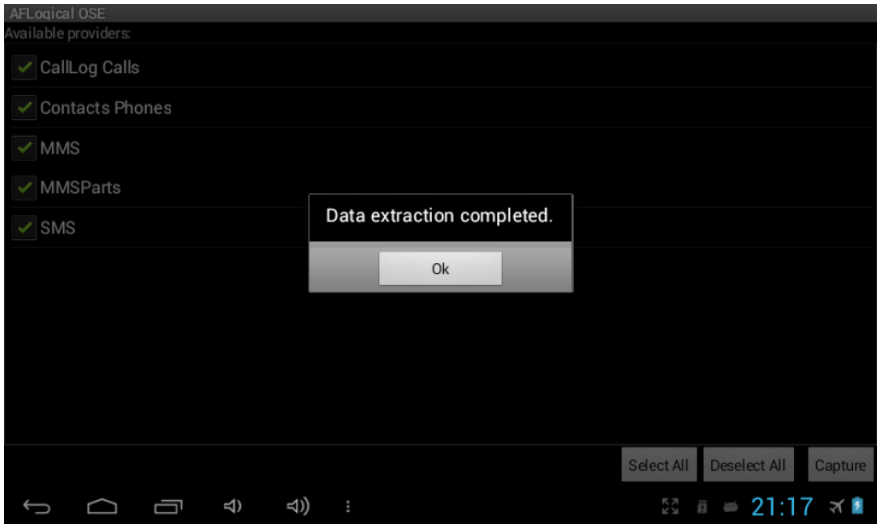
```
root@santoku-VirtualBox:/media/sf_FORENSIC# aflogical-ose
Make sure android device is connected to USB

334 KB/s (28794 bytes in 0.084s)
        pkg: /data/local/tmp/AFLogical-OSE_1.5.2.apk
Success
```

# Akwizycja logiczna – instalacja aplikacji i dostęp przez providerów

Instalacja i wywołanie z poziomu adb (przykład: AFLogical OSE)




```
Starting: Intent { cmp=com.viaforensics.android.aflogical_ose/com.viaforensics.android.ForensicsActivity }

Press enter to pull /sdcard/forensics into ~/aflogical-data/
```

```
pull: building file list...
pull: /sdcard/forensics/19700106.2113/SMS.csv -> /root/aflogical-data/19700106.2113/SMS.csv
pull: /sdcard/forensics/19700106.2113/MMS.csv -> /root/aflogical-data/19700106.2113/MMS.csv
pull: /sdcard/forensics/19700106.2113/MMSParts.csv -> /root/aflogical-data/19700106.2113/MMSParts.csv
pull: /sdcard/forensics/19700106.2113/Contacts Phones.csv -> /root/aflogical-data/19700106.2113/Contacts Phones.csv
pull: /sdcard/forensics/19700106.2113/CallLog Calls.csv -> /root/aflogical-data/19700106.2113/CallLog Calls.csv
pull: /sdcard/forensics/19700106.2113/info.xml -> /root/aflogical-data/19700106.2113/info.xml
pull: /sdcard/forensics/19700106.2134/Contacts Phones.csv -> /root/aflogical-data/19700106.2134/Contacts Phones.csv
pull: /sdcard/forensics/19700106.2134/CallLog Calls.csv -> /root/aflogical-data/19700106.2134/CallLog Calls.csv
pull: /sdcard/forensics/19700106.2134/MMSParts.csv -> /root/aflogical-data/19700106.2134/MMSParts.csv
pull: /sdcard/forensics/19700106.2134/MMS.csv -> /root/aflogical-data/19700106.2134/MMS.csv
pull: /sdcard/forensics/19700106.2134/SMS.csv -> /root/aflogical-data/19700106.2134/SMS.csv
pull: /sdcard/forensics/19700106.2134/info.xml -> /root/aflogical-data/19700106.2134/info.xml
12 files pulled. 0 files skipped.
103 KB/s (151346 bytes in 1.421s)

root@santoku-VirtualBox:/#
```

# Akwizycja fizyczna

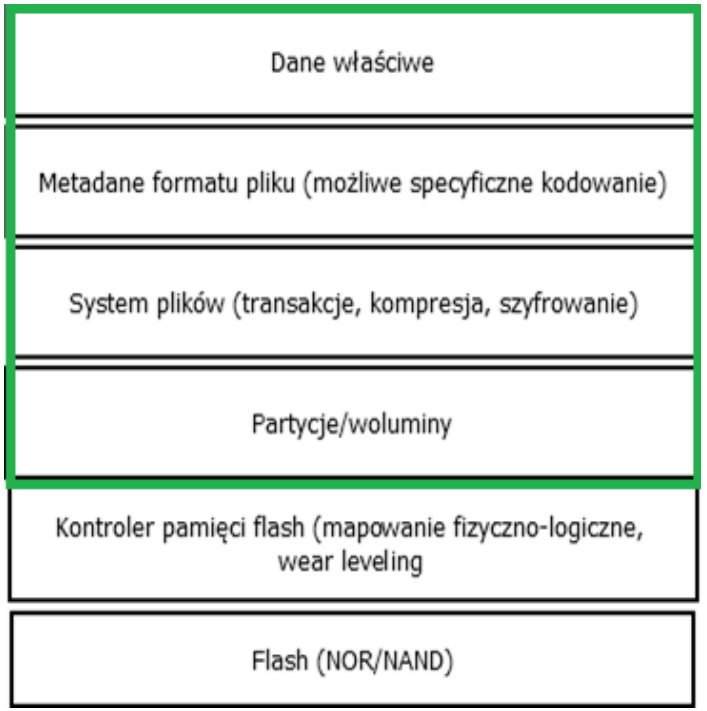
Metoda polegająca na wykonaniu kopii binarnej całych partycji/woluminów/nośnika, bit po bicie, bez żadnej modyfikacji, konwersji, kodowania, interpretacji etc.

Akwizycja fizyczna dostarcza pełnych informacji:

- Aktualnych plików
- Usuniętych plików
- Pełnych metadanych systemu plików
- Pełnych metadanych geometrii dysku (partycje, woluminy)

Powszechnie spotykane sposoby akwizycji fizycznej można sklasyfikować następująco:

- **Wbudowane funkcje urządzenia (backup, OBEX, mapowanie pamięci NAND jako USB-MS)**
- **JTAG**
- **Chip-Off**



# Akwizycja logiczna – wgląd w dane

Do akwizycji logicznej może dojść tylko i wyłącznie jeśli:

- Mamy bezpośredni dostęp do nośnika i mamy oprogramowanie do obsługi jego systemu plików
- Mamy pośredni dostęp do nośnika poprzez urządzenie mobilne, z którym komunikujemy się za pomocą wspieranego przez nie protokołu (obsługa systemu plików jest wykonywana przez OS urządzenia)

Prostym rozwiązaniem jest udostępnienie kopii zebranych danych w innym urządzeniu o tej samej konfiguracji sprzętowo-programowej.

Gdy akwizycja logiczna jest już przeprowadzona, do wglądu w dane konieczna jest:

- Obsługa ewentualnego kodowania, jakie zastosowano w danych (np. kodowanie GSM)

Nie zawsze konieczna (ale zawsze wygodna) jest:

- Obsługa formatu plików, które zebraliśmy

**Wynika to z faktu, że znajomość kodowania pozwala przeszukiwać nośnik pod kątem określonych przez nas wzorców, ignorując znajdujące się na w pliku metadane formatu pliku**

# Akwizycja fizyczna

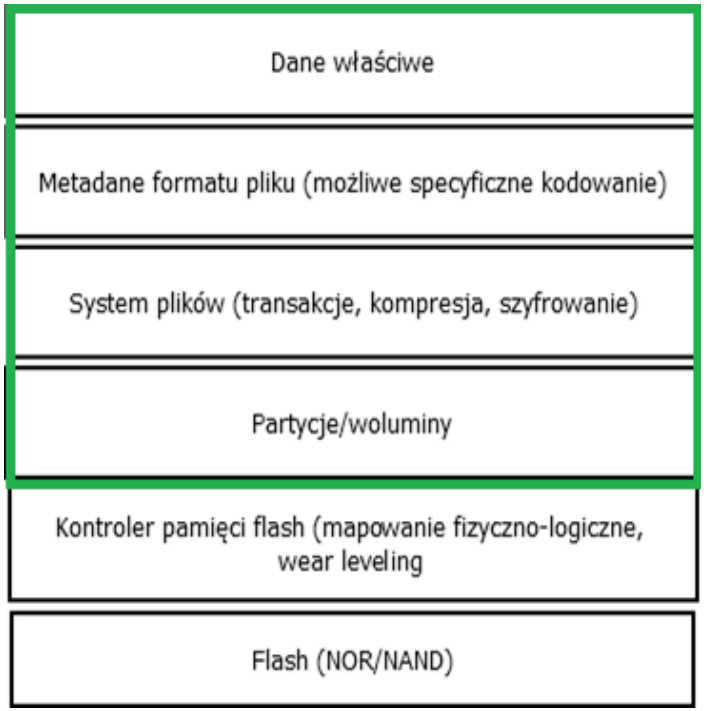
Metoda polegająca na wykonaniu kopii binarnej całych partycji/woluminów/nośnika, bit po bicie, bez żadnej modyfikacji, konwersji, kodowania, interpretacji etc.

Akwizycja fizyczna dostarcza pełnych informacji:

- Aktualnych plików
- Usuniętych plików
- Pełnych metadanych systemu plików
- Pełnych metadanych geometrii dysku (partycje, woluminy)

Powszechnie spotykane sposoby akwizycji fizycznej można sklasyfikować następująco:

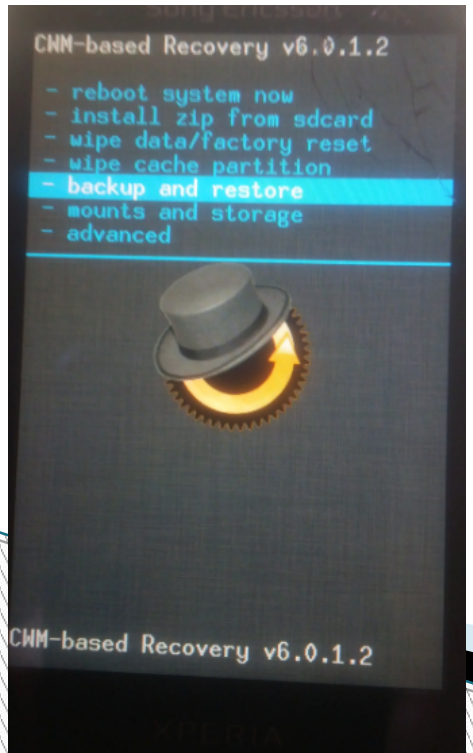
- **Wbudowane funkcje urządzenia (backup, OBEX, mapowanie pamięci NAND jako USB-MS)**
- **JTAG**
- **Chip-Off**

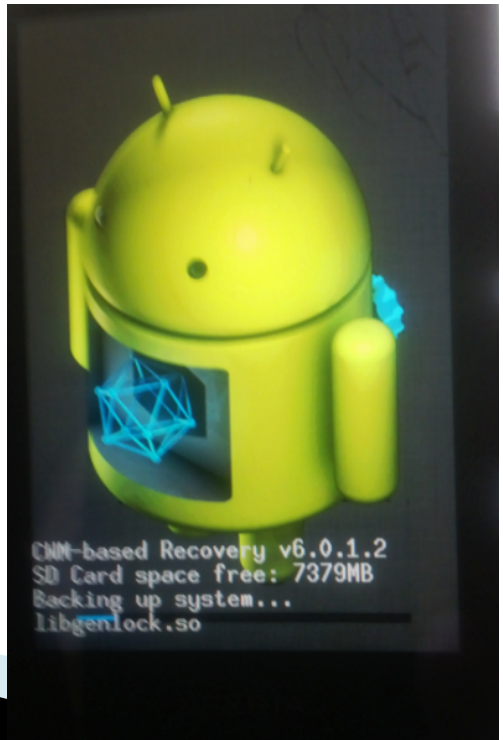


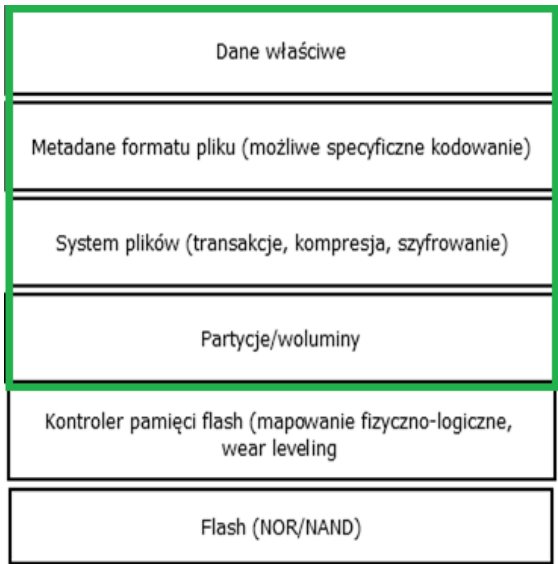
# Akwizycja  fizyczna – wbudowane funkcje –backup (clockworkmod)


Przykład: Android
Potrzebne: clockworkmod recovery, karta SD

1. Wkładamy kartę microSD
2. Uruchomiamy tryb recovery, wybieramy backup/restore
3. Na następnym ekranie wybieramy backup

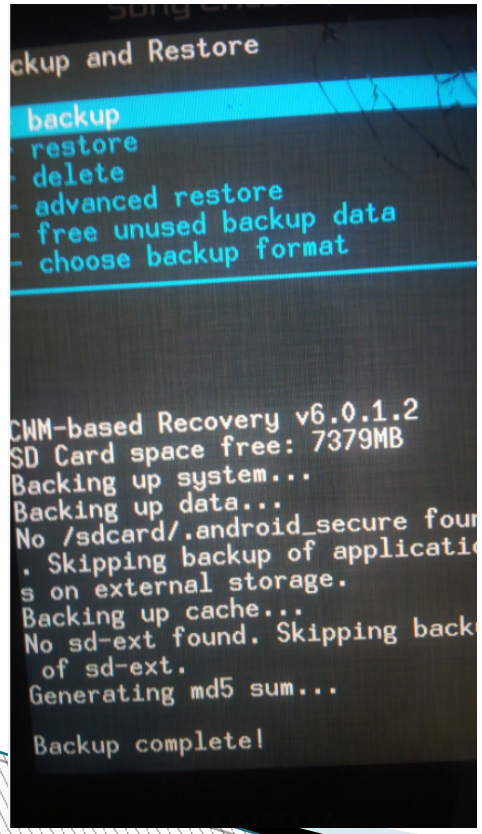


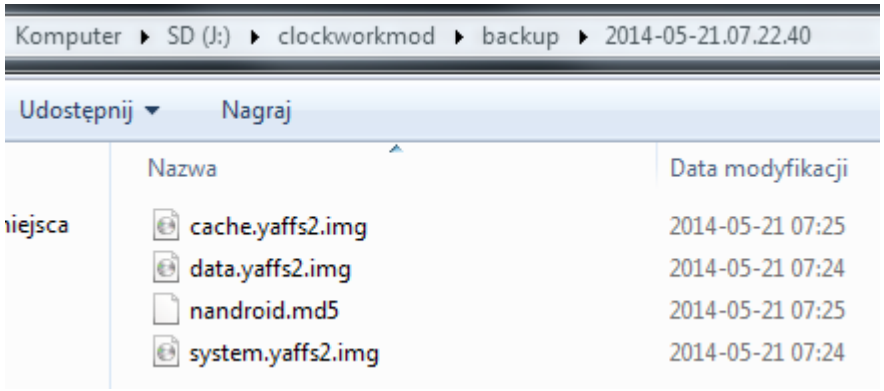



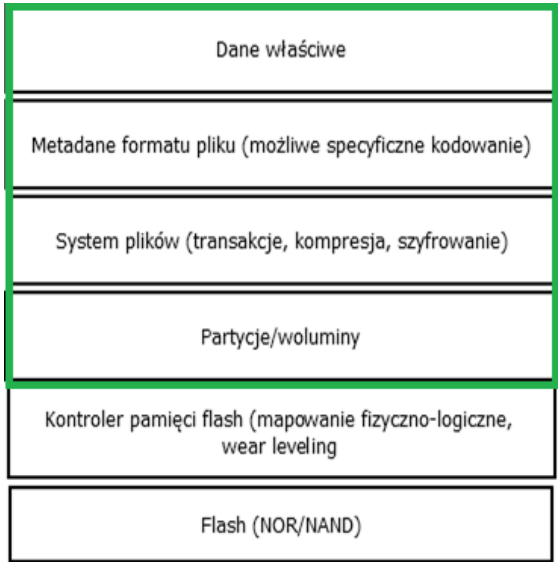



# Akwizycja  fizyczna – wbudowane funkcje –backup (clockworkmod)


Tworzony jest osobny obraz dla każdej partycji:



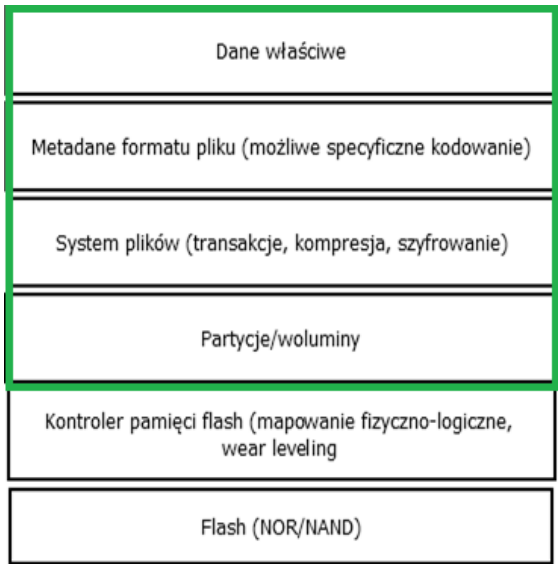
# Akwizycja fizyczna – Android - nandump/nandread/dd


Przykład: Android
Potrzebne: root

```
127|root@android:/mnt/extsd # dd if=/dev/block/mmcblk0p8 of=sys_manta
2097152+0 records in
2097152+0 records out
1073741824 bytes transferred in 243.856 secs (4403179 bytes/sec)
root@android:/mnt/extsd #
```

W przypadku partycji YAFFS zamiast dd należy użyć nandread/nandump.

W przypadku braku możliwości umieszczenia karty SD należy spróbować przesłać dane siecią (bluetooth, irda, Wi-Fi, USB? adb?).

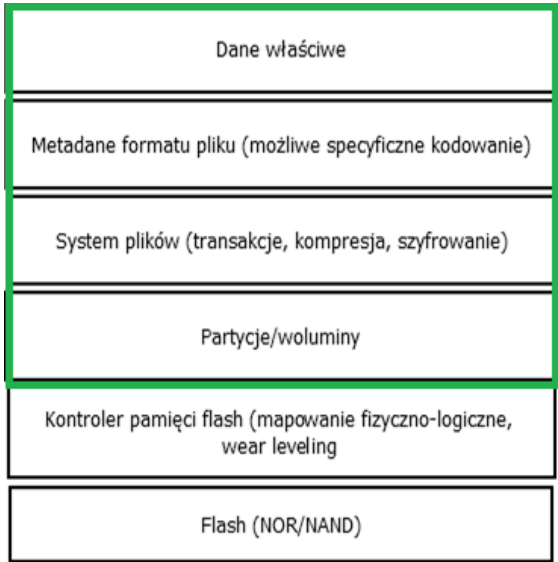


# Akwizycja fizyczna – mapowanie NAND

- Bardzo użyteczną i mało znaną metodą jest wykorzystanie funkcjonalności występującej w niektórych urządzeniach, np. **Nokia 6500 Classic, Sony Ericsson W300I i niektóre modele telefonów z Androidem**. Jeśli nie wiemy, czy dany model wspiera tę opcję, zawsze warto spróbować, jeśli możemy wyłączyć urządzenie **[RECOVERING FAT PARTITIONS]**

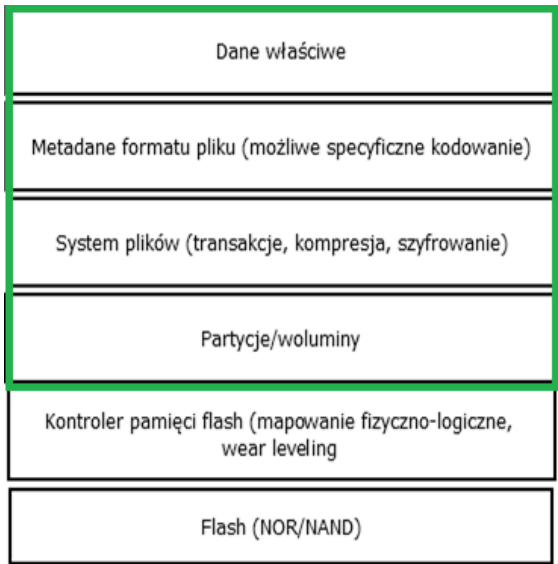
- Urządzenia te, będąc wyłączone, podłączeniu do komputera kablem USB udostępniają swoją pamięć główną jako urządzenie przenośne (USB Mass Storage Device).

  - **Pozwala to na dokonanie zupełnie nieinwazyjnej akwizycji fizycznej (poza restartem urządzenia OS nie zarejestruje żadnej aktywności z naszej strony).**



# Poziomy akwizycji – akwizycja fizyczna – mapowanie NAND

1. Należy upewnić się, że urządzenie jest wyłączone
2. Należy upewnić się, że karta SD jest wyjęta (wiele modeli w tym trybie udostępnia kartę SD, a tę można odczytać bez udziału urządzenia)
3. Podłączamy telefon kablem USB poprzez bloker zapisu (bądź do systemu skonfigurowanego w taki sposób, by montował nośniki w trybie tylko do odczytu)
4. Rozpoczynamy tworzenie obrazu

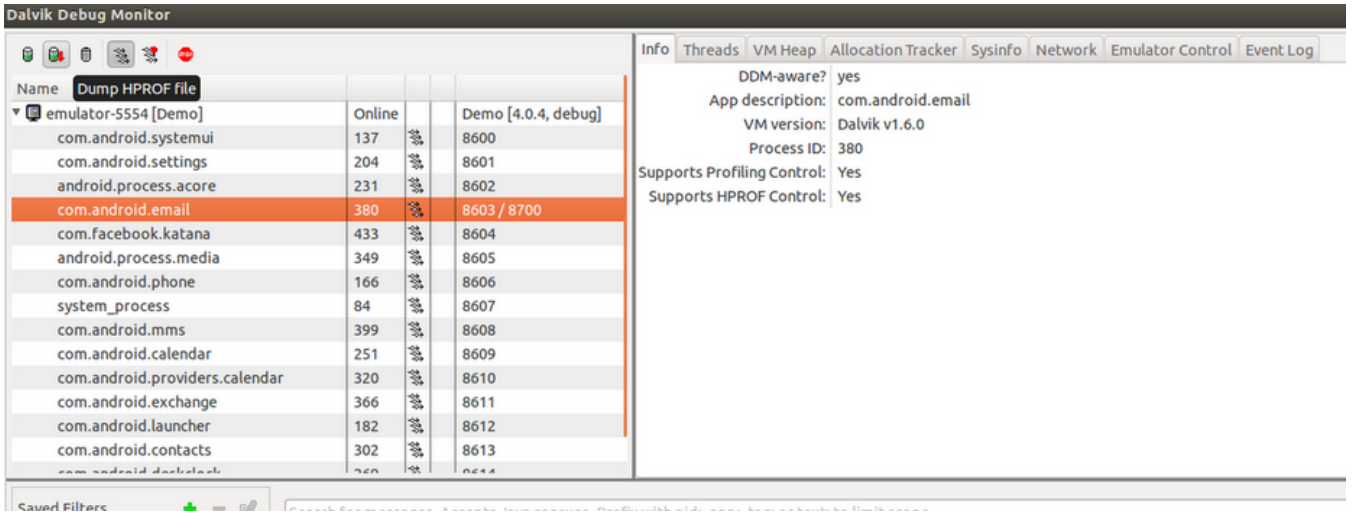


# Akwizycja RAM

Działa na Androidach przed 4.4 KitKat
Wymagania: adb+root

[VOLATILMEM]

Sposób 1 – zrzut pamięci poszczególnych procesów – DDMS (Dalvik Debug Monitor Server) [DDMS]




Sposób 2 – zrzut pamięci całego systemu – Foremost/LiME (moduł kernela) [LIME]

```
$ adb shell
root@android:/ # insmod /sdcard/lime.ko "path=/sdcard/lime.dump format=lime"
root@android:/ # ls -al /sdcard/lime.dump
----rwxr-x system   sdcard_rw 872415264 2013-02-25 16:48 lime.dump
```

# Poziomy akwizycji – akwizycja fizyczna – JTAG

JTAG (Joint Test Action Group) jest interfejsem występującym w układach scalonych, stworzonym z myślą o ich testowaniu i przeprogramowywaniu (wiele napraw serwisowych odbywa się poprzez użycie JTAG)
[EVIDENCEMAGAZINE]

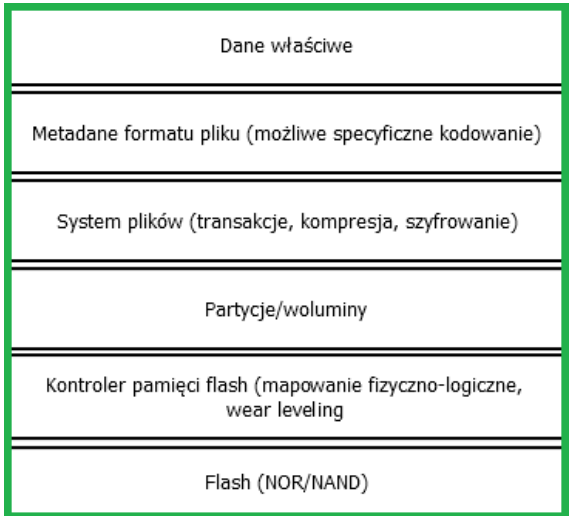
JTAG polega na wpięciu się za pośrednictwem płyty głównej urządzenia do jego chipu pamięci, **z pominięciem jego systemu operacyjnego i kontrolera pamięci flash**.

Nie wymaga więc usuwania czipa z płyty głównej.

Wymaga za to:

- Urządzenia z czipem wyposażonym w interfejs JTAG
- Urządzenie musi mieć sprawną elektronikę
- Odpowiedniego sprzętu i oprogramowania (Flasher Box, który zastąpi kontroler flash; obsługa FTL)

[EVIDENCEMAGAZINE]

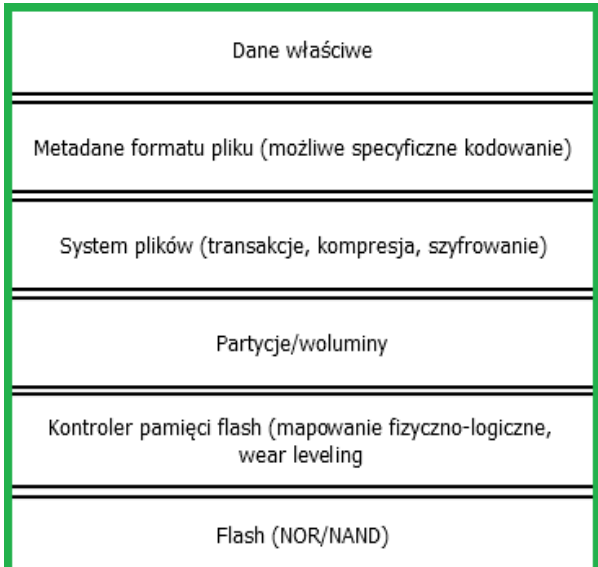


# Poziomy akwizycji – akwizycja fizyczna – chip-off

Metoda

- stosowana w ostateczności
- ryzykowna (ryzyko uszkodzenia czipa)
- podobnie jak JTAG wymaga specjalnego sprzętu  i oprogramowania
- dostarcza ten sam poziom abstrakcji co JTAG (najniższy możliwy)

[EVIDENCEMAGAZINE]



# Akwizycja ze zniszczonych urządzeń – chip swapping

W przypadku uszkodzeń elektroniki urządzenia chip-off nie musi być jedyną metodą (chip-swapping pozwala ominąć konieczność użycia specjalnego oprogramowania i sprzętu).

Często po prostu przekłada się czip pamięci wraz z kontrolerem (czasami są to dwa osobne czipy, czasami jeden scalony jak np. pamięci iNAND) do drugiego urządzenia „dawcy” tej samej marki i modelu 

[EXTRACTING DATA FROM DAMAGED DEVICES]

# Akwizycja fizyczna – wgląd w dane

Gdy akwizycja fizyczna jest już przeprowadzona, do wglądu w dane **zawsze konieczna jest** :

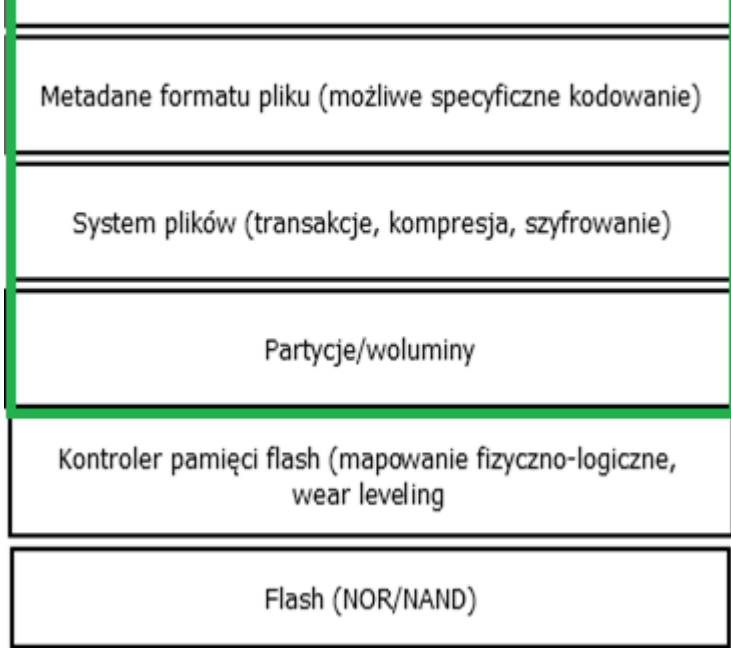
- Obsługa ewentualnego kodowania, jakie zastosowano w danych (np. kodowanie GSM), kompresja gzip,utf-8 itd.
- W przypadku chip-off dochodzi znajomość warstwy abstrakcji pamięci flash (FTL)

Nie zawsze konieczna (ale zawsze wygodna) jest:

- Obsługa formatu plików, które zebraliśmy
- Znajomość systemu plików
- Znajomość stosowanych partycji i woluminów

**Wynika to z faktu, że znajomość kodowania pozwala przeszukiwać nośnik pod kątem określonych przez nas wzorców, ignorując znajdujące się na nośniku metadane systemu plików** 

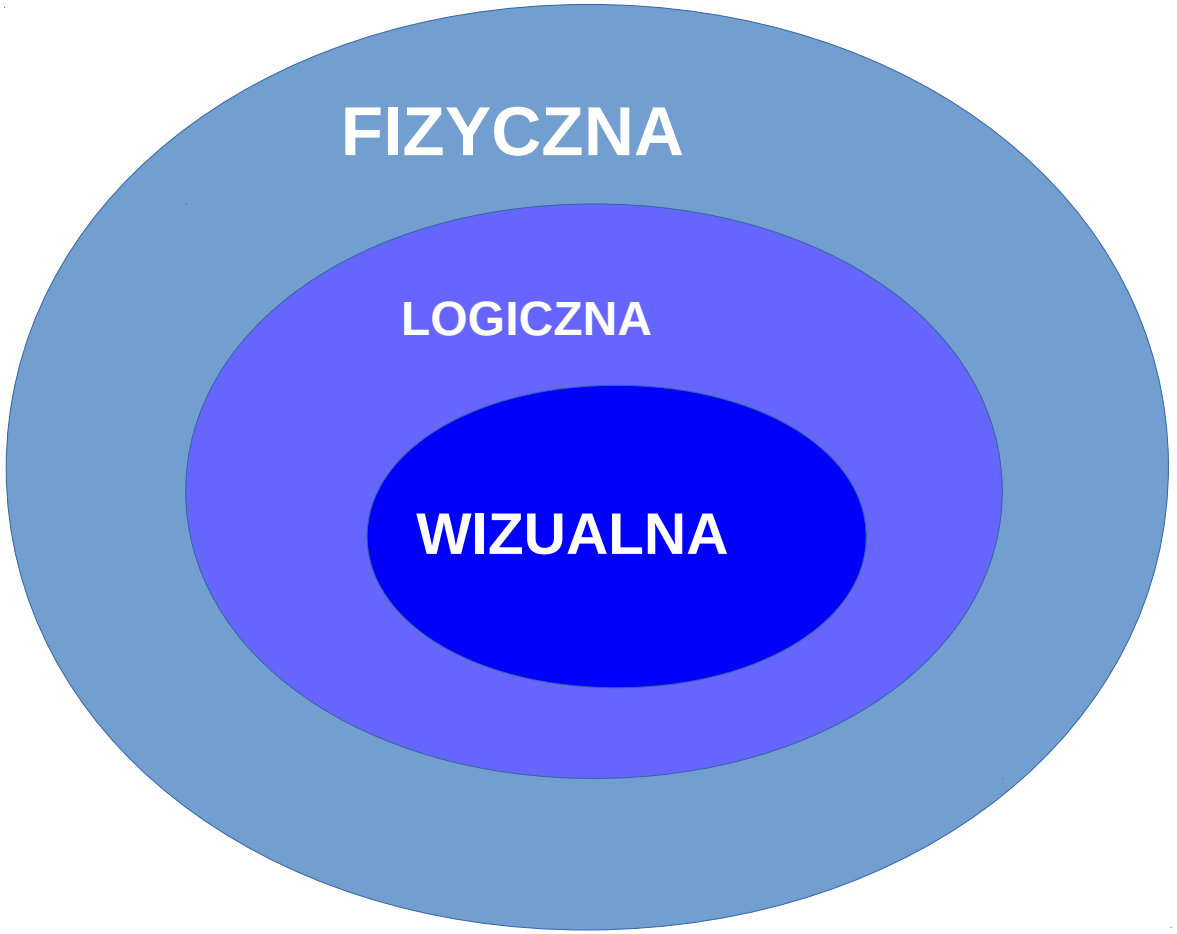
Prostym rozwiązaniem jest udostępnienie kopii zebranych danych w innym urządzeniu o tej samej konfiguracji sprzętowo-programowej.



# Poziomy akwizycji - relacja

Pomimo faktu, że akwizycja fizyczna obejmuje jednocześnie zakres akwizycji logicznej i wizualnej, dobrą praktyką jest, o ile to możliwe, **zastosowanie wszystkich dostępnych metod celem** porównania wyników.
Pozwala to:

- Wykryć anomalie wynikające z zastosowania niektórych technik antiforensics
- Ominąć niedociągnięcia niektórych narzędzi do mobile forensics (np. kodowanie)



# Klasyfikacja metod i stanów urządzenia

| Metoda | Typ metody | Urządzenie włączone |
|---|---|---|
| Manualne przejrzenie i dokumentacja fotograficzna/pisemna | Logiczna | Tak |
| Synchronizacja (SyncML/komendy AT/kopiowanie przez adb itd.) | Logiczna | Tak |
| Backup | Logiczna/Fizyczna | Tak |
| Mapowanie NAND | Fizyczna | Nie |
| OBEX | Fizyczna | Tak |
| JTAG | Fizyczna | Nie |
| Chip-Off | Fizyczna | Nie |
| Zrzut pamięci RAM | Logiczna/Fizyczna | Tak |

# Akwizycja selektywna

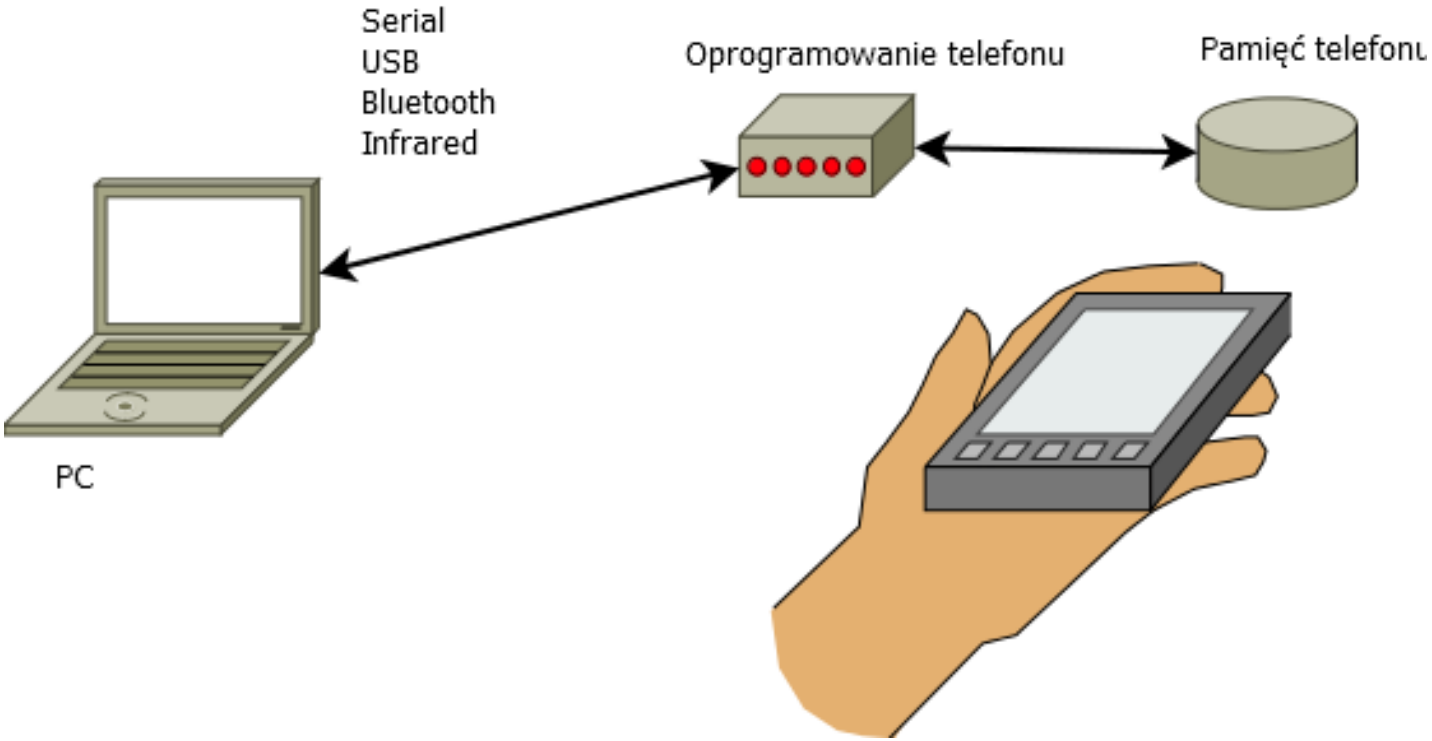
- Jeśli urządzenie zostało zabezpieczone w wyniku postanowienia o przeszukaniu, zebranie i analiza danych muszą mieścić się w zakresie ewentualnych ograniczeń postanowienia (np. zgoda wyłącznie na zabezpieczenie i analizę danych z określonego odcinka czasu)
- Jeśli urządzenie zostało oddane do analizy za zgodą właściciela, zebranie i analiza danych muszą mieścić się w zakresie ewentualnych ograniczeń tej zgody (np. zgoda wyłącznie na zabezpieczenie i analizę historii połączeń)
- W pewnych przypadkach ze względów praktycznych (np. brak czasu przy kilkudziesięciu GB zajętego miejsca w pamięci telefonu) zachodzi potrzeba akwizycji selektywnej
- Funkcjonalność tego typu można spotkać w niektórych narzędziach do mobile forensics (triage), np. w XRY

# Aspekty akwizycji danych z włączonych urządzeń

- Błędnym jest założenie, że sam proces zbierania nie zostawia śladów (zachodzą zmiany w niektórych plikach tymczasowych, logach itd. zależnie od systemu)
- Zakłada się (naiwnie), że oprogramowanie, z którym się komunikujemy, przekazuje pełne i prawdziwe informacje (flash firmware, OS telefonu)
- Bez chip-off nie da się udowodnić, iż dane pozyskane takimi metodami odzwierciedlają dokładnie dane oryginalne [AUSTRALIAN p 59]
- Wykorzystywanie OBEX, AT, SyncML, FBUS, nie istnieje żaden standard pozwalający na wyciągnięcie całej pamięci z telefonu [AUSTRALIAN p 59]

# Aspekty akwizycji danych z włączonych urządzeń

- Aplikacja na PC nie otrzymuje bezpośredniego dostępu do pamięci urządzenia, a jedynie polega i ufa wbudowanej w jego oprogramowanie logice
- Operacja taka wywołuje zmiany niektórych plików tymczasowych (logi etc.), co rodzi problemy natury ochrony integralności



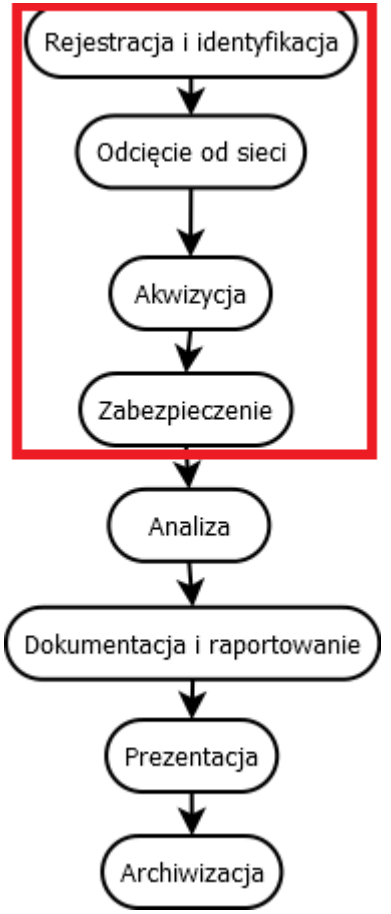
# Zarys procesu stosowania wymienionych metod

- **Rejestracja i identyfikacja** – rozpoczęcie fazy dokumentacji i ustalenie celu i zakresu czynności, stopniowe rozpoznanie sprzętu, oprogramowania, konfiguracji
- **Odcięcie od sieci** – zagwarantowanie braku jakiejkolwiek łączności z siecią
- **Akwizycja** – wykonanie kopii danych z nośników
- **Zabezpieczenie** – udokumentowanie poświadczeń nienaruszalności (sum kontrolnych)
- **Analiza** – praca z zabezpieczonymi danymi
- **Dokumentacja i raportowanie** – udokumentowanie interpretacji wyników analizy
- **Prezentacja** – przedstawienie wyników poprzednich etapów procesu
- **Archiwizacja** – ostatni etap cyklu życia wytworzonych w procesie danych (bezpieczne przechowanie/skasowanie)


[CYNTHIA MURPHY]

# Zarys procesu

Zgodnie z praktyką stosowaną w polskim prawie, od momentu przejęcia urządzenia do momentu wygenerowania sum kontrolnych z plików wynikowych przez cały czas muszą być obecne 3 osoby, których podpisy trafiają na protokół z zabezpieczenia zawierający dotychczasową dokumentację i sumy kontrolne (ich podpis jest poświadczeniem prawdziwości sekwencji dokonanych czynności i sum kontrolnych na raporcie). Od tego momentu proces analizy musi być  powtarzalny dla plików wynikowych (a niekoniecznie dla urządzenia).




Jest to szczególnie ważne zważywszy na fakt, że powtórna akwizycja z tego samego urządzenia najprawdopodobniej da inną sumę kontrolną pliku wynikowego.

Nic nie stoi na przeszkodzie, by jednocześnie stosować sumy kontrolne dwóch funkcji mieszających, np. md5 i sha1. w celu udaremnienia zarzutów wystąpienia rzekomej kolizji.

[CYNTHIA MURPHY]

# Rejestracja i identyfikacja

- Ustalenie podstawy przejęcia urządzenia
- Ustalenie celu i zakresu zabezpieczenia
- Umieszczenie danych zaangażowanych osób
- Ustalenie stanu operacyjnego urządzenia (włączone/wyłączone)
- Pożądany rodzaj akwizycji (pełna/selektywna?, fizyczna/logiczna/obydwie?)
- Formularz (początek tworzonej dokumentacji procesu)
  - Ustalenie numeru IMEI
  - Data i czas rozpoczęcia zabezpieczenia
  - Ustalenie marki i modelu urządzenia
  - Ustalenie stanu technicznego urządzenia (czy jest sprawne)
  - Ustalenie cech charakterystycznych (np. zadrapania)
  - Ustalenie, czy jest aktywny jakiś mechanizm blokady ekranu
  - Ustalenie, czy jest aktywne szyfrowanie (czasami można to ustalić po rodzaju blokady ekranu)
  - Ustalenie, jaka data, godzina i strefa czasowa jest ustawiona na urządzeniu
  - Ustalenie, jakie aplikacje są uruchomione
  - Ustalenie rodzaju i wersji oprogramowania

  **Jeśli którejś z powyższych informacji nie da się uzyskać bez zmiany stanu (włączenia/wyłączenia), uzyskanie tej informacji należy odłożyć do etapu akwizycji.**

# Odcięcie od sieci

Najlepszym sposobem jest uaktywnienie trybu lotu (wyłącza wszelkie nadajniki radiowe).
W przypadku braku takiej możliwości należy umieścić telefon w klatce Faradaya przy jednoczesnym zapewnieniu źródła zasilania
W przypadku braku klatki Faradaya zaleca się wyłączyć telefon, separując baterię, kartę SIM i telefon).

Co, jeśli nie ma dostępu do ekranu (i nie da się włączyć trybu lotu) i telefon jest zalogowany do GSM, a istnieje podejrzenie, że jest FDE (Full Disk Encryption)/cenne ulotne dane w RAM?

# Akwizycja z włączonym urządzeniem czy wyłączonym?

**Urządzenie nie ma prawa zalogować się do żadnej sieci od momentu jego zabezpieczenia, w innym przypadku dane będą podważone jako dowód (przynajmniej takie podejście ma miejsce w polskich sądach).**

Z technicznego punktu widzenia, zalogowany do sieci telefon to ryzyko:

- Nadpisania historycznych danych nowymi danymi
- Włamania/Sabotażu

**Istnieją różne, indywidualne scenariusze, niemniej ogólne zasady brzmią:**

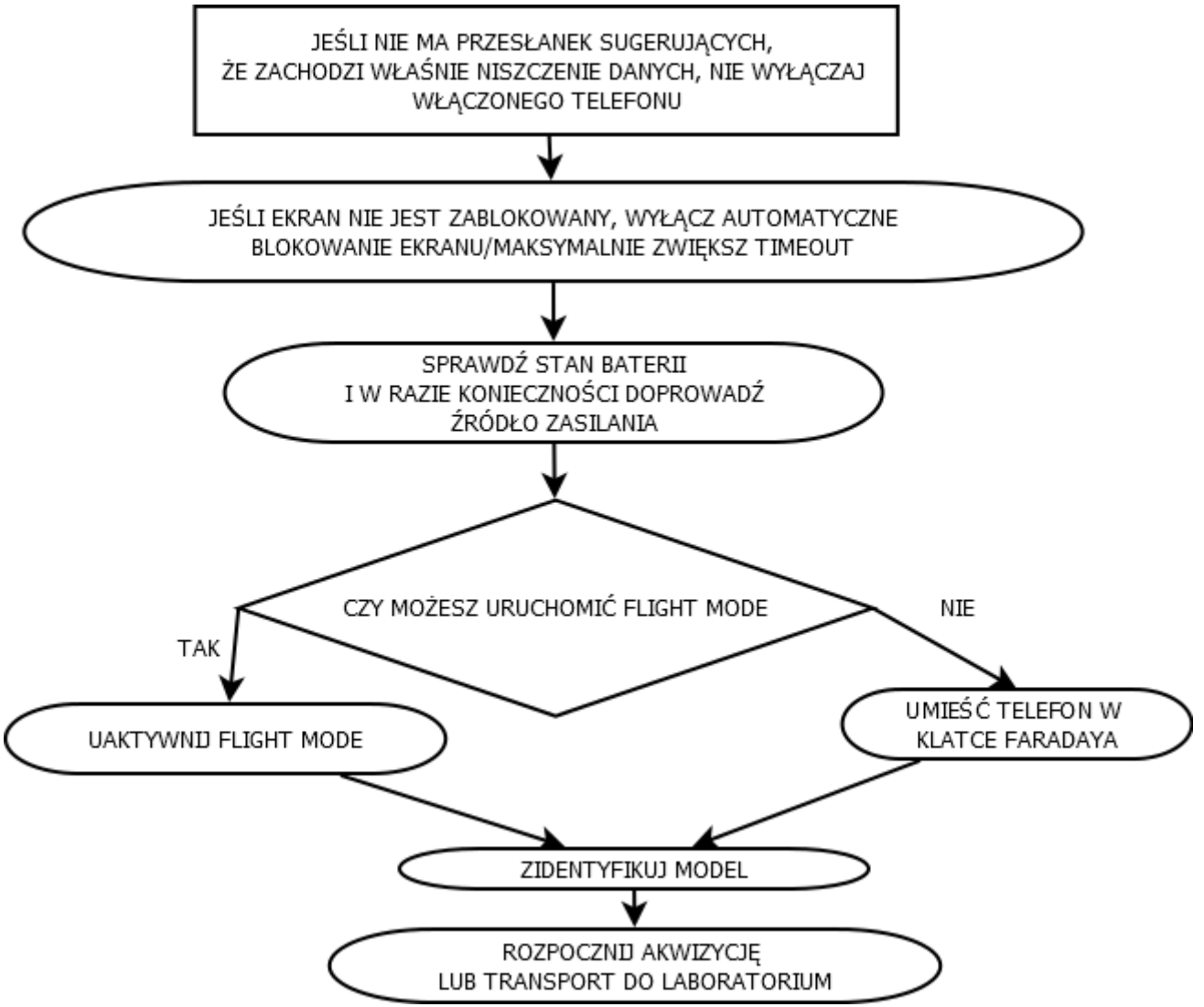
- Jeśli urządzenie jest wyłączone, odseparuj:
  - karty SIM
  - karty SD
  - urządzenie
  - baterię

- Jeśli urządzenie jest **włączone**, nie wyłączaj go (wiąże się to z utratą ulotnych śladów (RAM), w tym być może obecnych tam kluczy kryptograficznych dających w obecnym stanie dostęp do nośnika)

# Akwizycja – faza wstępna

- Upewniamy się, że mamy odpowiedni sprzęt (czytniki, kable, karty (SIM RW, czysta karta SD)
- Upewniamy się, że dysponujemy wymaganym oprogramowaniem (sterowniki do kabli, akwizycja danych)
- Zawsze upewniamy się, że złącza gniazd są suche i czyste

# Rejestracja i identyfikacja – jeśli urządzenie jest włączone



# Akwizycja – jeśli urządzenie jest włączone

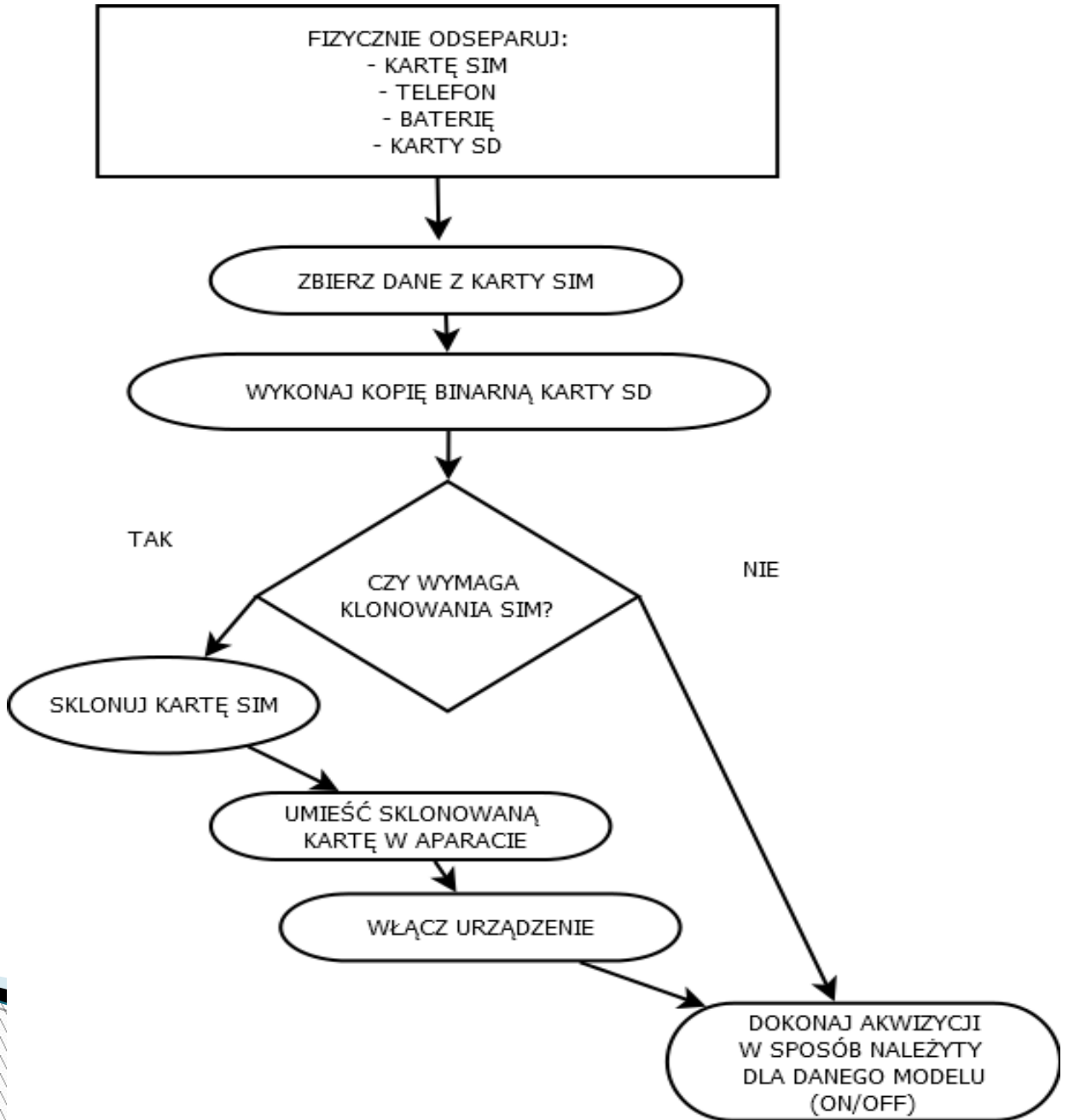
1. Manualna inspekcja:
- IMEI
- Obecność plików
- Obecność historii kontaktów
- Lista procesów
- Lista modułów
- Czas aktywności urządzenia
- Zawartość tymczasowych logów (np. dmesg, logcat)

2. Akwizycja logiczna metodą dostępną dla danego modelu (2 narzędzia) + weryfikacja, czy wynik ma sens

3. Akwizycja fizyczna metodą dostępną dla danego modelu (2 narzędzia) + weryfikacja, czy wynik ma sens
Np. sprawdzenie pod kątem plików graficznych, upewnienie się, że wyniki akwizycji logicznej mają mniejszą objętość itd.

4. Można wyłączyć urządzenie i dokonać akwizycji danych z karty SIM

# Zabezpieczenie – jeśli urządzenie jest wyłączone



# Klonowanie SIM

Ze względu
- na fakt, że niektóre telefony po wykryciu, że zostały uruchomione z nową kartą SIM/bez karty SIM (ICCID i IMSI jest przechowywany tymczasowo w pamięci stałej telefonu, głównie ze względów optymalizacyjnych) potrafią skasować/nadpisać dane
- fakt, że nie dopuszcza się ponownego zalogowania zabezpieczonego telefonu do sieci

Stosuje się tzw. SIM cloning.
- Polega to na przepisaniu numerów ICCID oraz IMSI na specjalną kartę SIM (SIM-RW, która różni się od GSM-owych kart SIM i służy tylko do tego, by zapisywać na niej wybrany zestaw ICCID+IMSI).
- Karta następnie zostaje umieszczona  w telefonie.
- Telefon przy włączeniu nie wykrywa zmiany w ICCID/IMSI, a jednocześnie nie potrafi zalogować się do sieci

Wiele telefonów nie wymaga klonowania SIM, zatem można je włączyć bez oryginalnej karty

# Zabezpieczenie

- Wygenerowanie sum kontrolnych z plików wynikowych (nie zaszkodzi dwiema różnymi funkcjami skrótu)
- Umieszczenie sum kontrolnych wraz z nazwami plików na raporcie
- Zachowanie wyników i ewentualne zachowanie urządzenia
- Podpisanie raportu przez komisję

# Analiza

- Montowanie obrazów
- http://www.liatsisfotis.com/2014/05/dump-memory-volatile-memory.html
- Przeszukiwanie atrybutów plików
- Przeszukiwanie zawartości plików
- Analiza aplikacji (reverse engineering)
- Data mining
- Daty (uwzględnienie różnic w ustawieniu daty i czasu na urządzeniu w stosunku do naszych ustawień daty i czasu; inna strefa czasowa/błędne ustawienie daty i godziny)
- Korelowanie wyników z różnych etapów akwizycji (np. w uzyskanych logicznie metadanych z odzyskanym usuniętym plikiem)
- Korelowanie i konfrontowanie wyników z wielu źródeł (wiele urządzeń, metadane od operatora)

# Archiwizacja

Bezpieczny sposób przechowywania i kasowania zebranych danych musi być elementem procesu (zapobieganie wyciekom).

# Odnośniki

Lista odnośników pod adresem:
https://github.com/ewilded/mobile/W6_URLs.txt