

# Zabezpieczanie i Analiza Danych z Urządzeń Mobilnych

## **Wykład #4 – Identyfikacja danych istotnych z punktu widzenia informatyki śledczej**



# Plan wykładu

- Istotne dane
- Możliwe metody ustalania lokalizacji istotnych danych
- Lokalizacje
  - Karta SIM
  - Pamięć telefonu
  - Nośniki zewnętrzne
  - Zdalne (chmury, konta w serwisach, metadane przechowywane przez operatora)

# Istotne dane

- IMEI, ICCID, numer telefonu, tożsamość, używane konta
- Lista kontaktów
- Komunikacja
  - Historia połączeń (w tym nieodebrane)
  - SMS-y
  - E-maile
  - Logi komunikatorów
- Historia przeglądania, cache
- Dokumenty, obrazy, nagrania
- Dane lokalizacyjne
  - GPS
  - Wi-Fi
  - Exif-data
  - GSM
- Kalendarz, budzik, stoper etc.
- Metadane
- Dane z innych aplikacji
- Nagrania, dane z sensorów, inne dane wskazujące na aktywność
- Nerozpoznane pliki
- Ślady włamań, obecność malware
- Dane wskazujące na zewnętrzne lokalizacje (chmura, synchronizacja z komputerem etc.)
- Ślady fizyczne

# Istotne dane - IMEI

15-cyfrowy identyfikator urządzenia mobilnego

- 2 cyfry – kod producenta
  - 4 cyfry – kod modelu telefonu
  - 2 cyfry – kod kraju
  - 6 cyfr-numer seryjny
  - Ostatnia cyfra – suma kontrolna
- 
- Pierwsze 6 cyfr (kod producenta + kod modelu telefonu) często określa się TAC (TAC number)
  - IMEI można odczytać z każdego włączonego telefonu klikając \*#06#

W wielu urządzeniach z Androidem IMEI jest przechowywany w pliku /efs/.nv\_data (wymagane uprawnienia roota).

# Karta SIM



**ICCID** – numer karty SIM, zawiera również kod abonenta

**IMSI** - zawierający dane operatora i kod abonenta (część wspólna z ICCID)

**MSISDN** (Mobile Station ISDN, numer telefonu)

**LAI** (Local Area Identity) – adres ostatniego BTS-a

**LP** (Language Preferences) - ustawienia językowe; ten rekord może zawierać jeden lub więcej rekordów

**PUCT** (Price Per Unit and Currency) - Informacja o walucie (np. liczniki opłat za połączenia

**ADN** (Abbreviated Dial Numbers) - Książka adresowa (kontakty)

**SMS** (w niektórych przypadkach da się odczytać usunięte SMS-y, np. jeśli został nadpisany tylko pierwszy bit (gdyż nie jest używany, 7-bitowe kodowanie))

**LND** (Last Numbers Dialed) – lista 10 ostatnio wybranych numerów

Z uwagi na ograniczoną pojemność kart SIM oraz rozpowszechnienie się nowoczesnych metod synchronizacji, współczesne telefony nie korzystają z karty SIM do przechowywania kontaktów, SMS-ów czy historii połączeń – rekordy te w kartach z takich telefonów zazwyczaj będą puste.

# Nokia - OS40, OS40 - PM tables

Lokalizacje najważniejszych informacji w rekordach PM records występujących w najpopularniejszych OS-ach Nokii

PM records/

5 - IMEI

35 - Security Code

58 - Kontakty

59 - Wybierane numery

60 - Połączenia nieodebrane

61 - Połączenia odebrane

84 - Historia www

91 - Tekst słownika

117 - Informacje o poprzednio włożonej karcie SIM

140 - SMS

150 - „SMS Cache”\*

202 - Informacje Bluetooth

# Możliwe metody ustalania lokalizacji

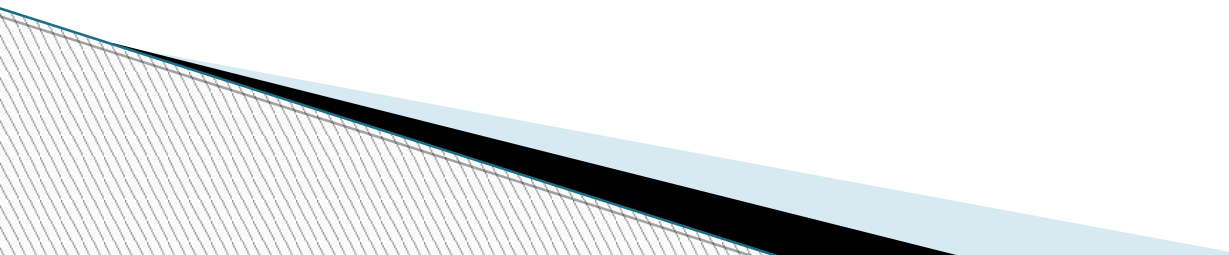
Metoda	Wady	Zalety
Dokumentacja/specyfikacja	Żmudna	Skuteczna (o ile istnieje dokumentacja)
Wyszukiwanie informacji w Internecie	Żmudna	Skuteczna (o ile ktoś zamieścił takie informacje)
Analiza kodu źródłowego/analiza wsteczna oprogramowania	Żmudna i trudna, czasami nielegalna	Pozwala odkryć rzeczy bardzo trudne do odkrycia innymi metodami
Samodzielne eksperymentowanie na testowych urządzeniach	Żmudna	Praktyczna, uniwersalna, interesująca i bardzo skuteczna

# Możliwe metody ustalania lokalizacji - eksperymenty

## Metoda 1:

- Stworzenie akwizycji logicznej NAND/SD
- Włączenie przechwytywania ruchu sieciowego (Wi-Fi)
- Wykonanie określonej akcji
- Ponowne wykonanie akwizycji logicznej NAND/SD
- Wyszukanie plików, które się różnią (bądź których w którymś ze zbiorów brakuje)

## Metoda 2:

- Wyszukanie plików zmodyfikowanych w ciągu ostatnich kilkunastu minut
  - Wykonanie określonej akcji
  - Ponowne wyszukiwanie plików zmodyfikowanych w czasie niekrótszym niż teraz+czas wykonywania akcji
  - Porównanie wyników
- 



# Możliwe metody ustalania lokalizacji - eksperymenty - RAM

Aby sprawdzić, do jakich procesów trafiają poszczególne dane, można zastosować metodę „igły i stosu”:

1. Wygenerować losowy ciąg znaków
2. Wprowadzić go na wejście do badanej aplikacji/usługi
3. Zrzucić pamięć wszystkich procesów+jądra, obszar każdego zrzutu przeszukując pod kątem tego ciągu

Przykładowy skrypt dla GNU/Linux: <https://github.com/ewilded/memplunge>

- Do akwizycji pamięci w systemach Android konieczne jest zainstalowanie (umieszczenie w filesystemie) i załadowanie (insmod) specjalnego modułu ([LIME FORENSICS]).
- Moduł należy skompilować w sposób dostosowany do dokładnej wersji jądra (Linux, kernel) [LIME FORENSICS]

# UNIX – konieczne komendy

<b>ls</b>	wyświetla zawartość bieżącego katalogu
<b>ls &lt;katalog&gt;</b>	wyświetla listę katalogu podanego jako argument
<b>ls -la</b>	wyświetla zawartość bieżącego katalogu wraz z plikami ukrytymi i rozmiarami oraz datami modyfikacji
<b>pwd</b>	wyświetla obecny katalog roboczy
<b>cd &lt;katalog&gt;</b>	zmienia obecny katalog roboczy na <katalog>
<b>md5sum</b>	oblicza sumę kontrolną md5 z zawartości
<b>&lt;plik&gt;</b>	wskazanego pliku
<b>file &lt;plik&gt;</b>	rozpoznaje typ pliku poprzez inspekcję zawartości (bez względu na nazwę/rozszerzenie)
<b>du -hs &lt;plik&gt;</b>	wyświetla rozmiar pliku w czytelnej formie (KB/MB/GB)
<b>cat &lt;plik&gt;</b>	wyświetla zawartość pliku
<b>head &lt;plik&gt;</b>	wyświetla początek pliku
<b>tail &lt;plik&gt;</b>	wyświetla koniec pliku
<b>diff &lt;plik1&gt;</b>	wyświetla różnice między plikami
<b>&lt;plik2&gt;</b>	
<b>cp &lt;plik&gt;</b>	kopiuje plik do nowej ścieżki
<b>&lt;nowa_sciezka&gt;</b>	
<b>&gt;</b>	
<b>grep &lt;fraza&gt;</b>	przeszukuje plik pod względem wystąpień danej frazy
<b>&lt;plik&gt;</b>	
<b>find &lt;katalog&gt;</b>	wyświetla pełną listę plików w danym katalogu i podkatalogach (pozwala na stosowanie zaawansowanych kryteriów oraz wykonywanie określonych komend na każdym z odnalezionych plików z osobna)

Szersza lista: <http://newbie.linux.pl/wydruk.php?wydruk=15&show=artykul>

# adb shell - czas aktywności urządzenia

Rezultat komendy *uptime*

```
/data/data # uptime  
22:14:34 up 1:44, load average: 7.00, 7.00, 6.97  
/data/data #
```

# adb shell - lista uruchomionych procesów

```
150 root      0 SW    [cfg80211]
165 root      0 SW    [wl12xx_wq]
166 root      0 SW    [irq/275-wl1271]
169 root      0 SW    [phy0]
171 shell      652 S    /system/bin/sh
172 root      4352 S    /sbin/adbd
219 system    355m S    system_server
294 system    284m S    {ndroid.systemui} com.android.systemui
347 app_22     270m S    {d.process.media} android.process.media
361 app_52     325m S    {e.process.gapps} com.google.process.gapps
383 app_26     268m S    {putmethod.latin} com.android.inputmethod.latin
396 radio     286m S    {m.android.phone} com.android.phone
408 app_7      331m S    {enmod.trebuchet} com.cyanogenmod.trebuchet
464 app_2      266m S    {android.smspush} com.android.smspush
496 app_58     269m S    {id.partnersetup} com.google.android.partnersetup
601 app_36     267m S    {roid.dspmanager} com.bel.android.dspmanager
618 app_49     277m S    {le.android.talk} com.google.android.talk
705 system    277m S    {ndroid.settings} com.android.settings
757 app_62     273m S    {nie.geniewidget} com.google.android.apps.genie.geni
779 app_31     272m S    {ndroid.exchange} com.android.exchange
792 app_32     278m S    {m.android.email} com.android.email
813 app_34     269m S    {droid.deskclock} com.android.deskclock
843 app_39     269m S    {viders.calendar} com.android.providers.calendar
858 app_48     298m S    {android.vending} com.android.vending
893 app_61     284m S    {ogle.android.gm} com.google.android.gm
922 app_52     271m S    {droid.gsf.login} com.google.android.gsf.login
938 app_52     411m S    {gle.android.gms} com.google.android.gms
955 app_14     269m S    {utta.rommanager} com.koushikdutta.rommanager
009 app_52     298m S    {rocess.location} com.google.process.location
024 app_40     271m S    {ndroid.calendar} com.android.calendar
060 app_6      313m S    {d.process.acore} android.process.acore
214 root      0 SW    [irq/179-bma250]
215 radio     16692 S    /system/bin/rild
224 root      1760 S    /sbin/sh -
229 root      1752 R    ps
# ps
```

Rezultat komendy  
*ps*

# adb shell - lista załadowanych modułów kernela

```
~ # lsmod
wl12xx_sdio 3359 0 - Live 0x7f09c000
wl12xx 130886 1 wl12xx_sdio, Live 0x7f073000
mac80211 195103 1 wl12xx, Live 0x7f038000
cfg80211 133322 2 wl12xx,mac80211, Live 0x7f00e000
compat_firmware_class 341 0 - Live 0x7f008000 (P)
compat 11181 3 wl12xx,mac80211,cfg80211, Live 0x7f000000
~ # █
```

Rezultat komendy *lsmod* - lista aktywnych modułów kernela - wiele rootkitów i złośliwych programów działa pod postacią modułów - daje im to pełen dostęp do pamięci jądra, co pozwala na oszukiwanie wyższych warstw architektury (wyników wywołań systemowych itd.)

# Wyszukiwanie - grep

O ile dostępne pliki nie są dodatkowo zakodowane, można bez problemu przeszukać rekursywnie całe katalogi pod kątem odpowiednio dobranych fraz celem np. poznania kolejnych interesujących lokalizacji (w ten sposób, znając jedynie imię właściciela urządzenia odkryliśmy np. lokalizację z historią przeglądania i ciastkami):

```
root@kali:~/MOBILE/playground/kamil# grep -ri kamil .
Binary file ./com.android.chrome/app_chrome/Default/Favicons matches
Binary file ./com.android.chrome/app_chrome/Default/History matches
Binary file ./com.android.chrome/app_chrome/Default/History Index 2014-03 matches
Binary file ./com.android.chrome/app_chrome/Default/History-journal matches
Binary file ./com.android.providers.contacts/databases/profile.db matches
root@kali:~/MOBILE/playground/kamil#
```

# Wyszukiwanie - find

Wyszukanie plików zmodyfikowanych co najmniej 10 minut temu:

```
/data # find . -mmin -10
./system/throttle/1652762375
/data # find . -mmin -30
./system
./system/batterystats.bin
./system/throttle/1652762375
./system/dropbox
./system/dropbox/event_data@1400875271901.txt
./data/com.google.android.gms/shared_prefs
./data/com.google.android.gms/shared_prefs/EventLogService.xml
./data/com.google.android.gms/shared_prefs/DownloadService.xml
/data #
```

# Przeglądanie baz sqlite

Polecenie `sqlite3 <nazwa pliku>` wczytuje bazę sqlite  
Wewnętrzne polecenie `.tables` wyświetla listę tabel:

```
root@kali:~/FORENSIC/playground/w0rm# sqlite3 contacts2.db
SQLite version 3.7.16.2 2013-04-12 11:52:43
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> .tables
_sync_state           phone_lookup          view_data_usage_stat
_sync_state_metadata  photo_files           view_entities
accounts              properties            view_groups
activities            raw_contacts          view_raw_contacts
agg_exceptions        search_index           view_raw_entities
android_metadata      search_index_content  view_stream_items
calls                 search_index_docsize  view_vl_contact_methods
contacts              search_index_segdir   view_vl_extensions
data                  search_index_segments view_vl_group_membership
data_usage_stat       search_index_stat     view_vl_groups
default_directory     settings              view_vl_organizations
directories            status_updates        view_vl_people
groups                stream_item_photos    view_vl_phones
mimetypes             stream_items          view_vl_photos
name_lookup           vl_settings           visible_contacts
nickname_lookup       view_contacts         voicemail_status
packages              view_data
sqlite> 
```

Bardzo szczegółowy opis struktury baz  
sqlite [CHEEKY4N6MONKEY]



# Przeglądanie baz sqlite

Wewnętrzne polecenie `pragma table_info(<nazwa_tabeli>)` wyświetla strukturę tabeli (typy i nazwy kolumn; pozwala to ustalić ich przeznaczenie). Poniżej struktura kolumny `calls` (23 kolumny):

```
sqlite> pragma table_info(calls);
0|_id|INTEGER|0||1
1|number|TEXT|0||0
2|date|INTEGER|0||0
3|duration|INTEGER|0||0
4|type|INTEGER|0||0
5|new|INTEGER|0||0
6|name|TEXT|0||0
7|numbertype|INTEGER|0||0
8|numberlabel|TEXT|0||0
9|countryiso|TEXT|0||0
10|voicemail_uri|TEXT|0||0
11|is_read|INTEGER|0||0
12|geocoded_location|TEXT|0||0
13|lookup_uri|TEXT|0||0
14|matched_number|TEXT|0||0
15|normalized_number|TEXT|0||0
16|photo_id|INTEGER|1||0
17|formatted_number|TEXT|0||0
18|_data|TEXT|0||0
19|has_content|INTEGER|0||0
20|mime_type|TEXT|0||0
21|source_data|TEXT|0||0
22|source_package|TEXT|0||0
23|state|INTEGER|0||0
sqlite>
```

# Przeglądanie baz sqlite

Jedynym poleceniem potrzebnym do przeglądania zawartości tabel w bazie danych jest kwerenda *select* (standard SQL), np.:

`SELECT * FROM <nazwa_tabeli>;`

```
sqlite> select * from calls;
1|519499144|1392927528940|0|0|PL||Poland|||0|519 499 144|1|||
2|+48533744867|1393236575378|0|3|0|Cool People|2|PL||1|Poland|content://com.android.contacts/contacts/lookup/0r1-2B43433D452F43453D2F/1||+48533744867|0|+48 533 744 867|1|||
3|+48533744867|1393238340368|0|2|0|Cool People|2|PL||Poland|content://com.android.contacts/contacts/lookup/0r1-2B43433D452F43453D2F/1||+48533744867|0|+48 533 744 867|1|||
4|+48533744867|1393238403092|0|2|0|Cool People|2|PL||Poland|content://com.android.contacts/contacts/lookup/0r1-2B43433D452F43453D2F/1||+48533744867|0|+48 533 744 867|1|||
5|+48533744867|1393238462237|0|2|0|Cool People|2|PL||Poland|content://com.android.contacts/contacts/lookup/0r1-2B43433D452F43453D2F/1||+48533744867|0|+48 533 744 867|1|||
6|+48533744867|1393238543797|0|2|0|Cool People|2|PL||Poland|content://com.android.contacts/contacts/lookup/0r1-2B43433D452F43453D2F/1||+48533744867|0|+48 533 744 867|1|||
7|+48533744867|1393238651058|0|2|0|Cool People|2|PL||Poland|content://com.android.contacts/contacts/lookup/0r1-2B43433D452F43453D2F/1||+48533744867|0|+48 533 744 867|1|||
8|+48533744867|1393238666666|0|2|0|Cool People|2|PL||Poland|content://com.android.contacts/contacts/lookup/0r1-2B43433D452F43453D2F/1||+48533744867|0|+48 533 744 867|1|||
9|+48533744867|1393238695459|321|1|0|Cool People|2|PL||Poland|content://com.android.contacts/contacts/lookup/0r1-2B43433D452F43453D2F/1||+48533744867|0|+48 533 744 867|1|||
10|608491839|1393416201550|0|2|0|0|PL||Poland|||0|608 491 839|1|||
11|608491839|1393416358952|19|2|0|0|PL||Poland|||0|608 491 839|1|||The quieter you become, the more you are able to hear.
12|+48794761902|1393495573325|0|3|0|0|PL||1|Poland|||0|+48 794 761 902|1|||
13|334979888|1393760531723|54|2|0|0|PL||Poland|||0|33 497 98 88|1|||
14|+48794761902|1394034276397|0|3|0|0|PL||1|Poland|||0|+48 794 761 902|1|||
15|608491839|1394306680008|0|2|0|0|PL||Poland|||0|608 491 839|1|||
16|726839511|1394306729982|13|2|0|0|PL||Poland|||0|726 839 511|1|||
17|726839511|1394306764008|383|2|0|0|PL||Poland|||0|726 839 511|1|||
18|+48726839511|1397889144316|207|1|1|0|PL||Poland|||0|1|||
sqlite> █
```

Możemy zauważyć, że data jest wyrażona liczbą całkowitą (a nie formatem typu *datetime/timestamp/date* itd). Jest to tzw. unix timestamp (oznacza ilość sekund, jaką należy dodać do daty 01.01.1970, aby otrzymać właściwą datę).

# Przeglądanie baz sqlite

Aby łatwo przekonwertować tak zapisany czas na czytelny format, można posłużyć się wbudowaną komendą linuxową *date -d*:

```
root@kali:~/FORENSIC/playground/w0rm# date -d 1392927528940
date: invalid date `1392927528940'
```

Wiele aplikacji przechowuje datę z dokładnością milisekund, gdy komenda *date* operuje na sekundach, w takim wypadku pomijamy 3 ostatnie cyfry:

```
root@kali:~/FORENSIC/playground/w0rm# date -d @1392927528
Thu Feb 20 21:18:48 CET 2014
root@kali:~/FORENSIC/playground/w0rm#
```

# Analiza - rozpoznawanie typów plików

Komenda file:

```
root@kali:~/MOBILE/playground/w0rm/dbs/com.android.providers.contacts/databases# adb pull /data/data/com.google.android.gms/.z@gmail.com/~4/-TtZ8a2i9KsM/UYFKqR5KewI/AAAAAAAAABiI/Vvu0Y_VEJQc/default_cover_2_ae125d34a6150400a2a97f22e218a904158 KB/s (15992 bytes in 0.098s)
root@kali:~/MOBILE/playground/w0rm/dbs/com.android.providers.contacts/databases# qiv 3
bash: qiv: command not found
root@kali:~/MOBILE/playground/w0rm/dbs/com.android.providers.contacts/databases# vim 320
root@kali:~/MOBILE/playground/w0rm/dbs/com.android.providers.contacts/databases# firefox 32
^C
root@kali:~/MOBILE/playground/w0rm/dbs/com.android.providers.contacts/databases# firefox .
root@kali:~/MOBILE/playground/w0rm/dbs/com.android.providers.contacts/databases# file 320
320: JPEG image data, JFIF standard 1.01
root@kali:~/MOBILE/playground/w0rm/dbs/com.android.providers.contacts/databases#
```

*file* stosuje trzy metody diagnostyczne:

1. Rozróżnienie po obecności znaków drukowalnych (plik txt|plik wykonywalny|inny plik)
2. Inspekcja rezultatu wywołania systemowego *stat* (czy np. jest to plik specjalny, jak pipe czy unix socket)
3. Rozpoznanie po unikalnych dla znanych formatów sekwencji bajtów (tzw. *magic numbers*) [FILE]

# Android - używane konta

Znalezienie listy w systemie jest stosunkowo intuicyjne:

```
~ # find / -iname '*accounts*'
/data/system/sync/accounts.xml
/data/system/accounts.db-journal
/data/system/accounts.db
/data/system/registered_services/android.accounts.AccountAuthenticator.xml
```

Pobieramy, przeglądamy (poza identyfikatorami kont są również hashe haseł ☹):

```
root@kali:~/MOBILE/playground/w0rm/dbs/com.android.providers.contacts/databases# adb pull /data/system/accounts.d
296 KB/s (38912 bytes in 0.128s)
root@kali:~/MOBILE/playground/w0rm/dbs/com.android.providers.contacts/databases# sqlite3 accounts.db
SQLite version 3.7.16.2 2013-04-12 11:52:43
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> .tables
accounts          authtokens        grants
android_metadata  extras            meta
sqlite> select * from accounts;
1|julian.horoszkiewicz@gmail.com|com.google|1/Pqw6QJwaJMIxvoxKp_xBrL2Y0ofVDIJj ru7jAnt7kI4 fFrTdVy0TpQhCerxsghnCc1
sqlite> pragma table_info(accounts);
0|_id|INTEGER|0||1
1|name|TEXT|1||0
2|type|TEXT|1||0
3|password|TEXT|0||0
sqlite> 
```

Dane o posiadanych kontach gmail w Androidzie można znaleźć w kilku innych lokalizacjach, np. można wykorzystać fakt, że system tworzy katalog dla avatarów:

```
~ # ls /data/data/com.google.android.gms/files/images/people-cover-photos/
julian.horoszkiewicz@gmail.com
~ #
```

# Android - lista kontaktów

Lista kontaktów znajduje się w

/data/data/com.android.providers.contacts/databases/contacts2.db (widok view\_contactas):

```
root@kali:~/MOBILE/playground/w0rm/dbs/com.android.providers.contacts/databases# ls
contacts2.db  contacts2.db-journal  profile.db  profile.db-journal
```

```
sqlite> select * from view_Contacts;
```

```
1|40|Cool People|People, Cool||3|Cool People|People, Cool|1|1|2299i6352da958ae42a6b||1|0|0|0|0|0|0
2|10|lukspl@gmail.com|lukspl@gmail.com|0|lukspl@gmail.com|lukspl@gmail.com|0|2|2299i5e67e2c18f3d4206||0|0|0|
3|10|info@e-system.biz|info@e-system.biz|0|info@e-system.biz|info@e-system.biz|0|3|2299i7bdaec4b0d04e7c5||0|0|
4|10|ewilded@gmail.pl|ewilded@gmail.pl|0|ewilded@gmail.pl|ewilded@gmail.pl|0|4|2299i7a4b91c70f42610f||0|0|0|
5|10|acid@ewil.pl|acid@ewil.pl|0|acid@ewil.pl|acid@ewil.pl|0|5|2299i4a0903409ff07d0||0|0|0|0|0|0|0
6|10|asterisk@itathome.com.pl|asterisk@itathome.com.pl|0|asterisk@itathome.com.pl|asterisk@itathome.com.pl|0|
7|10|info@econren.com|info@econren.com|0|info@econren.com|info@econren.com|0|7|2299i7c8fb6f00ee0c3d4||0|0|0|
8|10|admin@econren.pl|admin@econren.pl|0|admin@econren.pl|admin@econren.pl|0|8|2299ib5e5f0288b57e10||0|0|0|0|
9|10|ssladmin@econren.com.pl|ssladmin@econren.com.pl|0|ssladmin@econren.com.pl|ssladmin@econren.com.pl|0|9|2
10|10|acid@econren.eu|acid@econren.eu|0|acid@econren.eu|acid@econren.eu|0|10|2299i52cad8f88ffc4eab||0|0|0|0|
11|10|info@econren.net|info@econren.net|0|info@econren.net|info@econren.net|0|11|2299i5416116b0f3bbfcd||0|0|
12|10|info@econren.info|info@econren.info|0|info@econren.info|info@econren.info|0|12|2299i76257bed0b3d0a41||
13|10|info@econren.nazwa.pl|info@econren.nazwa.pl|0|info@econren.nazwa.pl|info@econren.nazwa.pl|0|13|2299i40
14|10|info@poolseklusseniers.com|info@poolseklusseniers.com|0|info@poolseklusseniers.com|info@poolseklusseniers.com|0|
15|10|root@econren.com|root@econren.com|0|root@econren.com|root@econren.com|0|15|2299i582d3ba88b678b65||0|0|
16|10|acid@infolinia.org|acid@infolinia.org|0|acid@infolinia.org|acid@infolinia.org|0|17|2299i13e3cefc0ca65b
17|10|ewilded@psychodela.pl|ewilded@psychodela.pl|0|ewilded@psychodela.pl|ewilded@psychodela.pl|0|16|2299i63
18|10|acid@niepowinnotakbyc.pl|acid@niepowinnotakbyc.pl|0|acid@niepowinnotakbyc.pl|acid@niepowinnotakbyc.pl|0|
19|10|acid@grubeimprezy.pl|acid@grubeimprezy.pl|0|acid@grubeimprezy.pl|acid@grubeimprezy.pl|0|18|2299i1d1fb5
20|40|LEWEL - Usługi Reklamowe|Reklamowe, LEWEL - Usługi||3|LEWEL - Usługi Reklamowe|Reklamowe, LEWEL - Usługi
```



# Android - historia połączeń

Spis połączeń również znajduje się w

/data/data/com.android.providers.contacts/databases/contacts2.db (tabela calls, kolumna type określa, czy połączenie było wychodzące/przychodzące/odebrane/niedebrane). Ważną cechą jest tutaj zawartość połączeń nieodebranych, gdyż te nie są przechowywane w billingach operatorów).

```
sqlite> select * from calls;
1|519499144|1392927528940|0|2|0|0|PL||Poland|||0|519 499 144|)|||
2|+48533744867|1393236575378|0|3|0|Cool People|2|PL||1|Poland|content://com.android.c
3|+48533744867|1393238340368|0|2|0|Cool People|2|PL||Poland|content://com.android.co
4|+48533744867|1393238403092|0|2|0|Cool People|2|PL||Poland|content://com.android.co
5|+48533744867|1393238462237|0|2|0|Cool People|2|PL||Poland|content://com.android.co
6|+48533744867|1393238543797|0|2|0|Cool People|2|PL||Poland|content://com.android.co
7|+48533744867|1393238651058|0|2|0|Cool People|2|PL||Poland|content://com.android.co
8|+48533744867|1393238666666|4|2|0|Cool People|2|PL||Poland|content://com.android.co
9|+48533744867|1393238695459|321|1|0|Cool People|2|PL||Poland|content://com.android.
10|608491839|1393416261956|0|2|0|0|PL||Poland|||0|608 491 839|)|||
11|608491839|1393416358952|19|2|0|0|PL||Poland|||0|608 491 839|)|||
12|+48794761902|1393495573325|0|3|0|0|PL||1|Poland|||0|+48 794 761 902|)|||
13|334979888|1393760531723|54|2|0|0|PL||Poland|||0|33 497 98 88|)|||
14|+48794761902|1394034276397|0|3|0|0|PL||1|Poland|||0|+48 794 761 902|)|||
15|608491839|1394306680008|0|2|0|0|PL||Poland|||0|608 491 839|)|||
16|726839511|1394306729982|13|2|0|0|PL||Poland|||0|726 839 511|)|||
17|726839511|1394306764008|383|2|0|0|PL||Poland|||0|726 839 511|)|||
18|+48726839511|1397889144316|207|1|1|0|PL||Poland|||0|)|||
sqlite> pragma table_info(calls);
0|_id|INTEGER|0||1
1|number|TEXT|0||0
2|date|INTEGER|0||0
3|duration|INTEGER|0||0
4|type|INTEGER|0||0
5|new|INTEGER|0||0
6|name|TEXT|0||0
7|numbertype|INTEGER|0||0
8|numberlabel|TEXT|0||0
```

# Android - SMS-y

Spis połączeń również znajduje się w  
/data/data/com.android.providers.telephony/databases/mmssms.db (odnaleziono  
poprzez przeszukanie rekursywne pod kątem frazy; polecenie *grep -ri czytnik /data/data*):

```
./com.android.providers.telephony/databases/mmssms.db:01 01 %To czytnik kart, z  
./com.android.providers.telephony/databases/mmssms.db:01 01 %To czytnik kart, z
```

Struktura bazy:

```
~ # cd /data/data/com.android.providers.telephony/databases/  
/data/data/com.android.providers.telephony/databases # sqlite3 mmssms.db  
SQLite version 3.7.4  
Enter ".help" for instructions  
Enter SQL statements terminated with a ";"  
sqlite> .tables  
addr                pdu                threads  
android_metadata    pending_msgs       words  
attachments         rate              words_content  
canonical_addresses raw                words_segdir  
drm                 sms                words_segments  
part                sr_pending  
sqlite>
```

SMS-y:

```
sqlite> select * from sms;  
1|1|100||1392926867691|1392926865000|0|1|-1|1|0||Korzystasz z Internetu w Play bez obaw o wysokie rachunki. Jes  
dz uzycie kodem *111*55*5#|+48790998250|0|0|1  
2|2|ING||1393238209617|1393238207000|0|1|-1|1|0||ING Bank informuje, ze nie odnotowalismy platnosci w kwocie 48  
atnosci. Dziekujemy|+48790998600|0|0|1  
12|4|2279||1393397743566|1393397739000|0|1|-1|1|0||mBank: Informujemy, ze pisemna dyspozycja wypowiedzenia Umov  
ji pod nr AXP026465787|+48790998250|0|0|1  
26|2|ING||1393527540231|1393527538000|0|1|-1|1|0||ING Bank. Sprawdź KWOTE i RACHUNEK. Kod autoryzacyjny dla pr  
.02.27 ** 19:58:57.|+48790998600|0|0|1  
03|0|ING||1393507676601|1393507676600|0|1|-1|1|0||ING Bank. Sprawdź KWOTE i RACHUNEK. Kod autoryzacyjny dla pr
```



# Android - email

Wiadomości z aplikacji gmail można odnaleźć w lokalizacji:  
/data/data/com.google.android.gm/databases/mailstore<nazwa\_konta>.db

```
/data/data/com.google.android.gm/databases # sqlite3 mailstore.julian.horoszkiewicz@gmail.com.db
SQLite version 3.7.4
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> .tables
ads
android_metadata
attachments
conversation_labels
conversations
conversations_to_fetch
custom_from_prefs
custom_label_color_prefs
dasher_info
engine_settings
labels
message_labels
messages
messages_to_fetch
operations
search_sequence
search_status
send_without_sync_conversations_to_fetch
server_preferences
sync_settings
sqlite> .
```

```
sqlite> select * from messages limit 1;
1|1468386293371541585|1468386293371541585|"Facebook" <update+zj4y6j99s4f9@facebookmail.com>|"Ewil Ded" <julian.horoszkiewicz@gmail.com>|""|"noreply" <noreply@facebookmail.com>|1400362294000|1400362294732|Masz na Facebooku więcej znajomych niż myślisz. |Najszybszym sposobem na znalezienie wszystkich Twoich znajomych na Facebooku ...|2||1||1||0|0|0|0|0|x00ZYs0000+00T00||0|-1||1||
sqlite>
```

# Android - historia przeglądarki

Lokalizacja: /data/data/com.android.chrome/app\_chrome/Default/History:

```
root@kali:~/MOBILE/playground/kamil/com.android.chrome/app_chrome/Default# sqlite3 History
SQLite version 3.7.16.2 2013-04-12 11:52:43
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> .tables
android_urls      presentation      visit_source
downloads         segment_usage    visits
keyword_search_terms  segments
meta              urls
sqlite> select * from urls;
1|http://fb.com/|Witamy na Facebooku. Zaloguj się, zarejestruj się lub dowiedz się więcej|1|1|13038163653111621
2|http://www.facebook.com/|Witryna http://www.facebook.com/ jest niedostępna|1|0|13038163653111621|0|0
3|https://www.facebook.com/|Facebook|4|0|13038497845116364|0|0
4|https://play.google.com/store/apps/details?id=com.google.android.youtube&hl=pl|YouTube - Aplikacje Android w
5|http://fb.pl/|...|2|1|13038252198680003|0|0
6|http://ogito.pl/|ogito.pl|1|0|13038246814874620|0|0
7|http://pl-pl.facebook.com/|Witryna http://pl-pl.facebook.com/ jest niedostępna|3|1|13038497763523081|0|0
8|https://pl-pl.facebook.com/|Witamy na Facebooku. Zaloguj się, zarejestruj się lub dowiedz się więcej|2|0|1303
9|https://www.facebook.com/login.php?login_attempt=1|Facebook|2|0|13038497817833298|0|0
10|https://www.facebook.com/mobile/ipad|Facebook dla urządzeń iPad|1|0|13038246911541986|0|0
```

# Android - cookies

Cookies są kolejnym źródłem informacji o odwiedzanych stronach  
(/data/data/com.android.chrome/app\_chrome/Default/Cookies):

```
root@kali:~/MOBILE/playground/kamil/com.android.chrome/app_chrome/Default# sqlite3 Cookies
SQLite version 3.7.16.2 2013-04-12 11:52:43
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> .tables
cookies  meta
sqlite> select * from cookies;
13038163851537377|play.google.com|PLAY_PREFS|CgJQTBDprJPzxyg:S:AN01ljIGrKSYgNeH|/|13039373451543539|1|1|13038163851537
13038163851544112|.google.com|NID|67=i17F9AI0s_maq1Dd9nfZZtEEG-txAlcMj-xlf0-Fr1X27VIPkVUtXg46ST-R4s4L_P5NhYf4wkdb3hd0B
741000000|0|1|13038498385256798|1|1
13038246814854293|.ogito.pl|osclass|295cc1008avpjtsn098fjmmbf3|/|13039456414854382|0|1|13038246814854293|1|1
13038246823350519|.ogito.pl|__utma|82444936.642966581.1393773223.1393773223.1393773223.1|/|13101318823000000|0|0|13038
13038246823353829|.ogito.pl|__utmb|82444936.1.10.1393773223|/|13038248623000000|0|0|13038246823353829|1|1
13038246823360414|.ogito.pl|__utmc|82444936|/|13039456423360501|0|0|13038246823360414|1|1
13038246823371468|.ogito.pl|__utmz|82444936.1393773223.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)|/|13054014823
13038246960531235|.atdmt.com|AA003|AXxbBg2LHts0HoLLAi6836TXKxq38H1CA1TQwtLqMCm3-Wv0fDKoypsYSdMdDUTTTWorXfccZLBxHSnABnf
8981000000|0|0|13038246960531235|1|1
13038247232716195|.facebook.com|locale|pl_PL|/|13038852054000000|0|0|13038498062301783|1|1
13038254771417589|.google.pl|NID|67=LN1INtMudiNsZNYMfol6lti6IPGxURz9LkMkdLj9QWL4WNl4q5jELGrsQRHphss2X0WM2Ntsilztv3Ut8
95000000|0|1|13038498421503949|1|1
13038254796682036|.youtube.com|VISITOR_INFO1_LIVE|54HfSrPkj0Y|/|13059292800000000|0|0|13038498384458872|1|1
13038254796682445|.youtube.com|YSC|naw6lgsfl3A|/|13039464396682505|0|1|13038498384458872|1|1
13038254798591694|.youtube.com|PREF|f1=500000000&fms2=10000&fms1=10000|/|13059292802000000|0|0|13038498384458872|1|1
13038254804225707|accounts.google.com|GoogleAccountsLocale_session|pl|/|13039464404225817|1|0|13038254804225707|1|1
13038254804226046|accounts.google.com|GAPS|1:EMM8Lsmc03TinVFQIOaiEZKi6EIXDA:3yvGTQv27Pr80VPH|/|13101326828000000|1|1|1
13038254804226326|accounts.google.com|GALX|6Nlby2AyBOM|/|13039464404226374|1|0|13038254804226326|1|1
13038489295099132|wifi.orange.pl|JSESSIONID|A73FBE8832AA81EC547877449A1C7A65|/|13039698895099266|1|1|13038489407711823
13038497591284598|.youtube.com|GPS|1|/|13038499386000000|0|0|13038498384458872|1|1
13038497593916523|.google.pl|PREF|ID=a1285c7fb8eb1ba3:U=da9f5a87b8c7b805:FF=0:TM=1393781195:LM=1394023989:S=0QZvaeo_J9
13038497599641724|www.google.pl|MRES|bd7037fdf1b637:c403f1276dae3108:514f757a381c2ceb:f110f01e28a3451b|/search|1304108
13038497604419555|.youtube.com|s_gl|da31afa91505e36f8d5ab291d88e299dcwIAAABQTA==|/|13039707204419672|0|0|1303849838445
13038497817096916|.facebook.com|fr|0ufvdoeQ6lsPcqHrH.AWU5-9-nIepXERoHykr9fMz5rz0.BTE0sU.cE.FMT.AWWUNj6n|/|130410898120
13038497817101381|.facebook.com|datr|jQQSU9gSGSpZxP0jn8Kmm0_r|/|13101569811000000|0|1|13038498045493974|1|1
```

# Android - cache przeglądarki

Typy plików rozpoznane w katalogu cache (/data/data/com.android.chrome/cache/Cache):

```
root@kali:~/MOBILE/playground/kamil/com.android.chrome/cache/Cache# file *
data_2:      data
data_3:      data
f_000001:    gzip compressed data
f_000002:    gzip compressed data
f_000003:    gzip compressed data, from FAT filesystem (MS-DOS, OS/2, NT)
f_000004:    gzip compressed data, from FAT filesystem (MS-DOS, OS/2, NT)
f_000005:    PNG image data, 472 x 432, 8-bit/color RGBA, non-interlaced
f_000006:    gzip compressed data
f_000007:    PNG image data, 201 x 310, 8-bit/color RGB, non-interlaced
f_000008:    PNG image data, 201 x 310, 8-bit/color RGB, non-interlaced
f_000009:    PNG image data, 206 x 310, 8-bit/color RGB, non-interlaced
f_00000a:    PNG image data, 201 x 310, 8-bit/color RGB, non-interlaced
f_00000b:    PNG image data, 206 x 310, 8-bit/color RGB, non-interlaced
f_00000c:    PNG image data, 206 x 310, 8-bit/color RGB, non-interlaced
f_00000d:    PNG image data, 584 x 900, 8-bit/color RGB, non-interlaced
f_00000e:    PNG image data, 584 x 900, 8-bit/color RGB, non-interlaced
f_00000f:    PNG image data, 201 x 310, 8-bit/color RGB, non-interlaced
f_000010:    PNG image data, 206 x 310, 8-bit/color RGB, non-interlaced
f_000011:    PNG image data, 206 x 310, 8-bit/color RGB, non-interlaced
f_000012:    PNG image data, 584 x 900, 8-bit/color RGB, non-interlaced
f_000013:    PNG image data, 598 x 900, 8-bit/color RGB, non-interlaced
f_000014:    PNG image data, 206 x 310, 8-bit/color RGB, non-interlaced
f_000015:    PNG image data, 206 x 310, 8-bit/color RGB, non-interlaced
f_000016:    PNG image data, 584 x 900, 8-bit/color RGB, non-interlaced
f_000017:    PNG image data, 598 x 900, 8-bit/color RGB, non-interlaced
f_000018:    PNG image data, 598 x 900, 8-bit/color RGB, non-interlaced
f_000019:    PNG image data, 206 x 310, 8-bit/color RGB, non-interlaced
f_00001a:    PNG image data, 598 x 900, 8-bit/color RGB, non-interlaced
f_00001b:    PNG image data, 598 x 900, 8-bit/color RGB, non-interlaced
f_00001c:    UTF-8 Unicode text, with very long lines
f_00001d:    ASCII text, with very long lines
f_00001e:    ASCII text, with very long lines
f_00001f:    ASCII text, with very long lines
```

- Fragmenty stron (style, skrypty, HTML, grafika)
- Pobrane pliki
- Skompresowana zawartość stron



# Android - cache przeglądarki

Dane skompresowane z pomocą gzip można bez trudu rozpakować (poniżej kod JavaScript):

```
root@kali:~/MOBILE/playground/kamil/com.android.chrome/cache/Cache# cp f_000097 /tmp/f.gz
root@kali:~/MOBILE/playground/kamil/com.android.chrome/cache/Cache# cd /tmp/
root@kali:/tmp# gunzip f.gz
root@kali:/tmp# less f
root@kali:/tmp# head f
/*!CK:2191352267!*//*1393854406,178127443*/

if (self.CavalryLogger) { CavalryLogger.start_js(["MT1v3"]); }

_d("ImageUtils",["UserAgent"],function(a,b,c,d,e,f,g){var h={hasLoaded:function(i){if(i.naturalWidth!==undefined){return
==20&&i.complete){return false;}else if(i.complete===undefined&&g.webkit()<500){var j=new Image();j.src=i.src;return j
_d("PhotoEverstoreLogger",["Event","AsyncRequest","copyProperties","ImageUtils"],function(a,b,c,d,e,f,g,h,i,j){var k=
: function(n){k.storedLog.push(n);if(k.storedLog.length==1)setTimeout(m,k.BATCH_WINDOW_MS);},logImmediately:function(n
.getElementById(n);if(o!=null)if(j.hasLoaded(o)){l._log(o.src);}else g.listen(o,'load',function(event){l._log(o.src);})
```

# Android - kalendarz

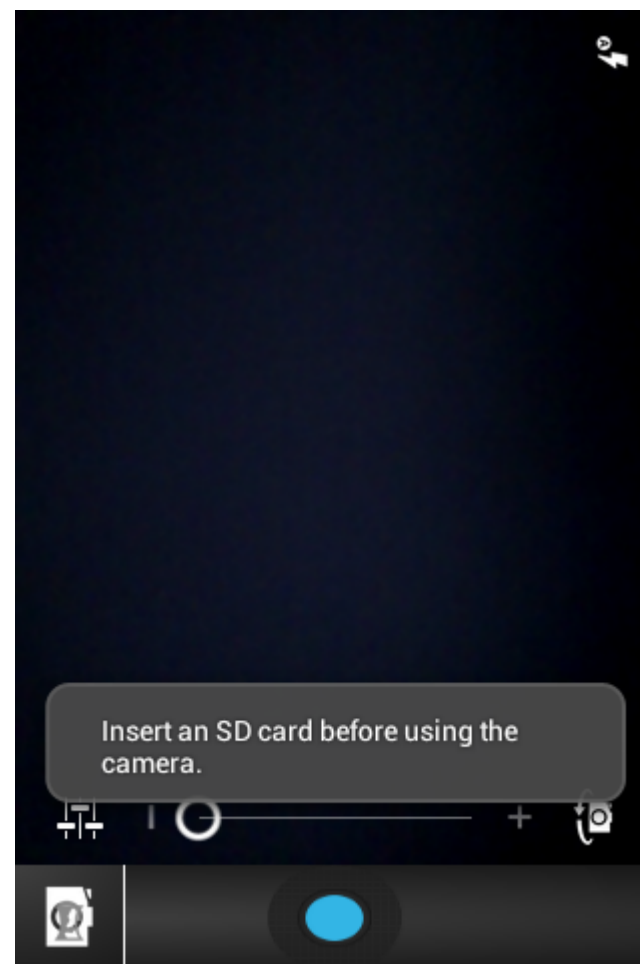
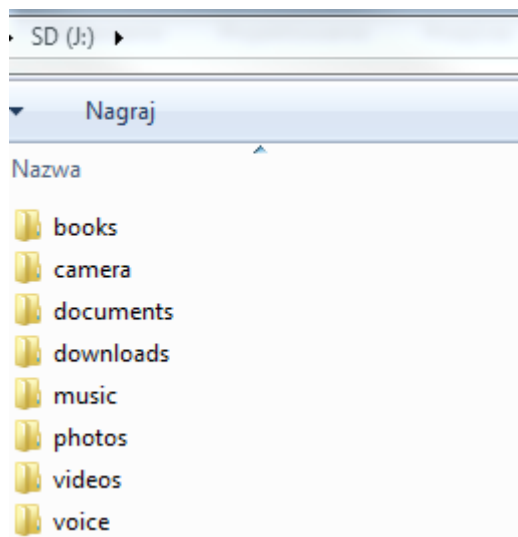
Zdarzenia z kalendarza (dodane samodzielnie jak i predefiniowane przez google, jak np. święta) znajdziemy w  
/data/data/com.android.providers.calendar/databases/calendar.db:

```
30|Testing||Bielsko||0|1|1400752800000|1400756400000||Europe/Warsaw|0|0|0|1|0|||||||1400756400000|1|1|1|0|1|1|
wicz@gmail.com|com.google|Europe/Warsaw|julian.horoszkiewicz@gmail.com|1|-14069085||700|5|0,1,2|0,1,2,3|0,1|1|1|
gmail.com/private/full|https://www.google.com/calendar/feeds/default/allcalendars/full/julian.horoszkiewicz%40gm
rs/full/julian.horoszkiewicz%40gmail.com|1|0||1397918924378||julian.horoszkiewicz@gmail.com|1
sqlite> .quit
/data/data/com.android.providers.calendar/databases # sqlite3 calendar.db
```

```
SQLite version 3.7.4
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> .tables
Attendees          Colors             Reminders
CalendarAlerts     Events            _sync_state
CalendarCache      EventsRawTimes    _sync_state_metadata
CalendarMetaData   ExtendedProperties android_metadata
Calendars           Instances         view_events
sqlite>
```

# Android - dokumenty

Dokumenty przechowywane są domyślnie na karcie SD (np. aplikacja do obsługi kamery odmawia wykonania zdjęcia bez włożonej karty SD)



# SQLite - usunięte rekordy

- Bardzo często usunięcie rekordu z tabeli sqlite (*delete from <table> where id=<id>*) nie powoduje faktycznego usunięcia rekordu z pliku, a, podobnie jak w przypadku filesystemów, oznaczenie obszaru zajmowanego przez ten rekord jako wolnego (zapomnienie poprzez skasowanie jedynie metadanych)
- Wykrycie takich rekordów w najprostszy sposób jest możliwe poprzez podejrzenie pliku/przeszukanie pod kątem pożądanых fraz
- Istnieją rozwiązania pozwalające na (w mniej lub bardziej skuteczny i uniwersalny sposób) czytelny odzysk tych rekordów

**[CHEEKY4N6MONKEY] [REVERSE ENGIN SQLITE] [OXYGEN SQLITE VIEWER]  
[SQLITE]**

- Ewidentną oznaką zapomnianych rekordów jest baza sqlite, która nie posiada tabel/posiada tabele puste, mając jednocześnie niezerowy rozmiar pliku



# Android - inne lokalizacje

```
~ # mount
rootfs on / type rootfs (ro,relatime)
tmpfs on /dev type tmpfs (rw,nosuid,relatime,mode=755)
devpts on /dev/pts type devpts (rw,relatime,mode=600)
proc on /proc type proc (rw,relatime)
sysfs on /sys type sysfs (rw,relatime)
none on /acct type cgroup (rw,relatime,cpuacct)
tmpfs on /mnt/asec type tmpfs (rw,relatime,mode=755,gid=1000)
tmpfs on /mnt/obb type tmpfs (rw,relatime,mode=755,gid=1000)
none on /dev/cpuctl type cgroup (rw,relatime,cpu)
/dev/block/mtdblock0 on /system type yaffs2 (ro,relatime)
/dev/block/mtdblock3 on /data type yaffs2 (rw,nosuid,nodev,relatime)
/dev/block/mtdblock2 on /cache type yaffs2 (rw,nosuid,nodev,relatime)
```

*rootfs on /* – katalog główny /

*tmpfs on /dev* – katalog podsystemu dev (urządzenia, faktyczne i wirtualne)

*devpts on /dev/pts* – katalog podsystemu pts (deskryptory pseudoterminali, można tak ustalić aktywne sesje powłoki) – podczas inspekcji z adb powinien tam widnieć tylko jeden deskryptor o nazwie 0

*proc on /proc* – pseudofilesystem /proc – lista wszystkich procesów i ich deskryptory

*sysfs on /sys* – pseudofilesystem /sys

*none on /acct* – cgroups (pseudofilesystem kontroli limitów zużycia zasobów)

*/dev/cpuctl* – jak wyżej, z tym, że dla CPU

*/mnt/asec* – obsługa DRM dla aplikacji (opcja forward lock) [FORWARD LOCK]

*tmpfs on /mnt/obb* – pliki tymczasowe aplikacji przekraczające 50 MB

[ANDROID FILE STRUCTURE]

# Android - inne lokalizacje - /etc

*/etc, /system/etc* – pliki konfiguracyjne usług (nie aplikacji działających w maszynie Dalvik)

Np. */system/etc/hosts* (modyfikacja lokalnego rozwiązywania domen)

```
~ # cat /system/etc/hosts
127.0.0.1          localhost
~ #
```

*/cache, /data/dalvik-cache* – cache maszyny wirtualnej Dalvik (zawiera pliki wykonywalne dex aplikacji, które były uruchamiane):

```
~ # ls /cache/dalvik-cache/
system@app@AntHalService.apk@classes.dex
system@app@Apollo.apk@classes.dex
system@app@ApplicationsProvider.apk@classes.dex
system@app@BackupRestoreConfirmation.apk@classes.dex
system@app@Bluetooth.apk@classes.dex
system@app@Browser.apk@classes.dex
system@app@CMWallpapers.apk@classes.dex
system@app@Calculator.apk@classes.dex
system@app@Calendar.apk@classes.dex
```

# Android - lista zapamiętanych sieci Wi-Fi

*/data/wifi/bcm\_supp.conf,/data/misc/wifi/wpa\_supplicant.conf*

Zawiera nawet hasła do WEP/WPA w czystej postaci ☐

```
/data/data # cat /data/misc/wifi/wpa_supplicant.conf
ctrl_interface=wlan0
update_config=1
device_type=0-00000000-0


network={
    ssid="AbraMakabra"
    psk="[REDACTED]lesniczegoboruty"
    key_mgmt=WPA-PSK
    priority=1
}
/data/data #
```

Gdzie i od której wersji jest przechowywany BSSID?

**[OPEN SSID BROADCAST VULN]**

# Android - inne lokalizacje - /etc

```
~ # ls /system/etc/security/cacerts/
00673b5b.0  27af790d.0  4fbd6bfa.0  72fa7371.0  9339512a.0  bf64f35b.0  e8651083.0
03e16f6c.0  2afc57aa.0  5021a0a2.0  74c26bd0.0  95aff9e3.0  c215bc69.0  ea169617.0
08aef7bb.0  2e8714cb.0  5046c355.0  75680d2e.0  9685a493.0  c33a80d4.0  eb375c3e.0
0d188d89.0  2fa87019.0  524d9b43.0  7651b327.0  9772ca32.0  c527e4ab.0  ed049835.0
10531352.0  2fb1850a.0  56b8a0b6.0  76579174.0  9d6523ce.0  c7e2a638.0  ed524cf5.0
111e6273.0  33815e15.0  57692373.0  7999be0d.0  9dbefe7b.0  c8763593.0  ee7cd6fb.0
1155c94b.0  343eb6cb.0  58a44af1.0  7a481e66.0  9f533518.0  ccc52f49.0  f4996e82.0
119afc2e.0  399e7759.0  594f1775.0  7a819ef2.0  a0bc6fbb.0  cdaebb72.0  f58a60fe.0
11a09b38.0  3a3b02ce.0  5a3f0ff8.0  7d3cd826.0  a15b3b6b.0  cf701eeb.0  f61bff45.0
12d55845.0  3ad48a91.0  5a5372fc.0  7d453d8f.0  a3896b44.0  d16a5865.0  f80cc7f6.0
17b51fe6.0  3c58f906.0  5cf9d536.0  81b9768f.0  a7605362.0  d537fba6.0  fac084d7.0
1920cacb.0  3c860d51.0  5e4e69e7.0  8470719d.0  a7d2cf64.0  d64f06f3.0  facacbc6.0
1dac3003.0  3d441de8.0  60afe812.0  84cba82f.0  ab5346f4.0  d777342d.0  fde84897.0
1dbdda5b.0  3e7271e8.0  635ccfd5.0  85cde254.0  add67345.0  d8274e24.0  ff783690.0
1dc6d6f4.0  418595b9.0  67495436.0  86212b19.0  b0f3e76e.0  dbc54cab.0
1df5ec47.0  455f1b52.0  69105f4f.0  87753b0d.0  b7db1890.0  ddc328ff.0
1e8e7201.0  46b2fd3b.0  6adf0799.0  882de061.0  bc3f2570.0  e48193cf.0
1eb37bdf.0  48478734.0  6e8bf996.0  895cad1a.0  bcdd5959.0  e60bf0c0.0
219d9499.0  4d654d1d.0  6fcc125d.0  89c02a45.0  bda4cc84.0  e775ed2d.0
23f4c490.0  4e18c148.0  72f369af.0  8f7b96c4.0  bdacca6f.0  e7b8d656.0
~ # cat /system/etc/security/cacerts/e7b8d656.0
-----BEGIN CERTIFICATE-----
MIICGjCCAeugAwIBAgIBBDANBgkqhkiG9w0BAQQFADBTMQswCQYDVQQGEwJVUzEc
MBoGA1UEChMTZXFlaWZheCBTZWN1cmUgSW5jLjEjEmMCQGA1UEAxMdRXFlaWZheCBT
ZWN1cmUgZUJ1c2luZXNzIENBLTEwHhcNOTkwNjIxMDQwMDAwWhcNMjAwNjIxMDQw
MDAwWjBTMQswCQYDVQQGEwJVUzEcMBoGA1UEChMTZXFlaWZheCBTZWN1cmUgSW5j
LjEjEmMCQGA1UEAxMdRXFlaWZheCBTZWN1cmUgZUJ1c2luZXNzIENBLTEwZ8wDQYJ
-----
```



The quieter yo

# Android - inne lokalizacje - lista aplikacji

*/data/system/packages.xml , /data/system/packages.list*- lista zainstalowanych aplikacji

```
com.google.android.location 10052 0 /data/data/com.google.android.location
com.andrew.apollo 10046 0 /data/data/com.andrew.apollo
com.android.soundrecorder 10012 0 /data/data/com.android.soundrecorder
com.android.voicedialer 10003 0 /data/data/com.android.voicedialer
com.android.defcontainer 10035 0 /data/data/com.android.defcontainer
com.dsi.ant.service.socket 10001 0 /data/data/com.dsi.ant.service.socket
com.android.contacts 10006 0 /data/data/com.android.contacts
com.android.vending.updater 10055 0 /data/data/com.android.vending.updater
com.android.inputmethod.latin 10026 0 /data/data/com.android.inputmethod.lati
com.google.android.onetimeinitializer 10051 0 /data/data/com.google.android.o
timeinitializer
com.google.android.partnersetup 10058 0 /data/data/com.google.android.partner
tup
com.android.calculator2 10041 0 /data/data/com.android.calculator2
net.cactii.flash2 10008 0 /data/data/net.cactii.flash2
com.android.htmlviewer 10028 0 /data/data/com.android.htmlviewer
com.google.android.voicesearch 10047 0 /data/data/com.google.android.voicesea
h
com.google.android.gsf.login 10052 0 /data/data/com.google.android.gsf.login
com.android.providers.calendar 10039 0 /data/data/com.android.providers.calen
r
com.android.bluetooth 10044 0 /data/data/com.android.bluetooth
com.bel.android.dspmanager 10036 0 /data/data/com.bel.android.dspmanager
packages.list
```

# Android - logcat

```
/Finsky ( 858): [1] CheckWifiAndAutoUpdate.cancelCheck: Cancelling auto-update with check.
/Finsky ( 858): [1] 2.onErrorResponse: Update check failed: com.android.volley.NoConnectionError: java.net.UnknownHostException: "google.com": No address associated with hostname
/Finsky ( 858): [1] DailyHygiene.flushEventLogsAndContinue: Flushing event logs for [_KyebirDRh_MKkgCk3ixdv-yo
/Finsky ( 858): [1] DailyHygiene.reschedule: Scheduling new run in 29 minutes (failures=2)
/Finsky ( 858): [1] 5.onFinished: Installation state replication succeeded.
/ActivityManager( 219): Timeout of broadcast BroadcastRecord{2bd14740 com.android.server.action.NETWORK_STATS_F
Receiver@2ba0cef8, started 10004ms ago
/ActivityManager( 219): Receiver during timeout: BroadcastFilter{2b9e9398 ReceiverList{2b9f48c8 219 system/1000
/PlayEventListener( 858): Upload failed class java.net.UnknownHostException(Unable to resolve host "play.googleap
/ThrottleService( 219): unable to find stats for iface rmnet0
/ActivityManager( 219): finishReceiver called but no pending broadcasts
/PlayEventListener( 858): Upload failed class java.net.UnknownHostException(Unable to resolve host "play.googleap
/ThrottleService( 219): unable to find stats for iface rmnet0
/PlayEventListener( 858): Upload failed class java.net.UnknownHostException(Unable to resolve host "play.googleap
/ActivityManager( 219): No longer want com.android.email (pid 792): hidden #16
/ActivityManager( 219): No longer want com.bel.android.dspmanager (pid 601): hidden #17
/ActivityManager( 219): Scheduling restart of crashed service com.bel.android.dspmanager/.service.HeadsetService
/ActivityManager( 219): No longer want com.android.exchange (pid 779): hidden #16
/EventLogService( 938): Aggregate from 1400869871286 (log), 1400869871286 (data)
/ActivityManager( 219): Start proc com.bel.android.dspmanager for service com.bel.android.dspmanager/.service.H
/HeadsetService( 1288): Starting service.
```



# Android - dmesg

```
<6>cyttsp-spi spi0.0: cyttsp_resume: Enter
<6>cyttsp-spi spi0.0: cyttsp_resume: Waking ...
<6>cyttsp_wakeup: wakeup
<6>cyttsp-spi spi0.0: cyttsp_resume: hst_mode 00
<6>cyttsp-spi spi0.0: cyttsp_resume: hst_mode 00
<6>as3676 0-0040: as3676_late_resume
<6>cyttsp-spi spi0.0: chg_status_work: Set charger mode to reg: 0x0
<6>msm_hsusd msm_hsusd: reset
<6>msm_hsusd msm_hsusd: reset
<6>msm_hsusd msm_hsusd: reset
<6>msm_hsusd msm_hsusd: reset
<6>android_usb gadget: high speed config #1: android
<6>bq24185 0-006b: Turning on charger. USB-Host mode
<6>bq24185 0-006b: Set init values
<6>bq24185 0-006b: Disabling charger
<6>bq24185 0-006b: Setting input charger current to 500 mA
<6>bq24185 0-006b: Setting charger voltage to 4200 mV
<6>bq24185 0-006b: Setting charger current to 850 mA
<6>bq24185 0-006b: Enabling charger
<6>bq27520 0-0055: bq27520_handle_soc_worker() capacity=96 (96) flags=0x138 ctrl_status=0x28b sc
<6>request_suspend_state: sleep (0->3) at 434253166593 (2014-05-23 18:37:34.431427032 UTC)
<6>as3676 0-0040: as3676_early_suspend
<6>cyttsp-spi spi0.0: cyttsp_suspend: Enter
<6>bq27520 0-0055: bq27520_handle_soc_worker() capacity=97 (97) flags=0x138 ctrl_status=0x28b sc
<6>bq27520 0-0055: bq27520_handle_soc_worker() capacity=98 (98) flags=0x138 ctrl_status=0x28b sc
<6>bq27520 0-0055: bq27520_handle_soc_worker() capacity=99 (99) flags=0x38 ctrl_status=0x28b soh
<6>bq27520 0-0055: Fully charged (SOC=99%)
<6>chargalg chargalg: Battery fully charged says fuelgauge!
<6>bq24185 0-006b: Disabling charger
<6>bq27520 0-0055: bq27520_handle_soc_worker() capacity=100 (100) flags=0x239 ctrl_status=0x28b
```

# iOS/Android - cache klawiatury/słownik

- w iOS cache klawiatury  
/var/mobile/Application/<APPNAME>/Library/Keyboard/en\_GB-dynamic-text.dat [iphone-keyboard-cache]
- W urządzeniach z systemem Android (i prawdopodobnie wielu innych) warto zwrócić uwagę na słownik użytkownika (user dictionary).

```
root@kali:~# adb shell
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
~ # find / -iname '*dictionary*'
/cache/dalvik-cache/system@app@UserDictionaryProvider.apk@classes.dex
/system/usr/srec/config/en.us/dictionary
/system/app/UserDictionaryProvider.apk
/data/backup/com.google.android.backup.BackupTransportService/com.android.providers.userdictionary
/data/data/com.android.providers.userdictionary
~ # cd /data/data/com.android.providers.userdictionary/
/data/data/com.android.providers.userdictionary # ls
databases lib
/data/data/com.android.providers.userdictionary # cd databases/
/data/data/com.android.providers.userdictionary/databases # ls
user_dict.db          user_dict.db-journal
/data/data/com.android.providers.userdictionary/databases #
```

```
/data/data/com.android.providers.userdictionary/databases # sqlite3 user_dict.db
SQLite version 3.7.4
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> .tables
android_metadata  words
sqlite> select * from words limit 2;
sqlite> .quit
/data/data/com.android.providers.userdictionary/databases # du -hs
6.0K      .
/data/data/com.android.providers.userdictionary/databases # du -hs *
4.0K      user_dict.db
0         user_dict.db-journal
/data/data/com.android.providers.userdictionary/databases #
```



# Zdjęcia - dane z GPS (geotagging)

- Wiele Smartfonów z włączonym GPS zapisuje bieżące koordynaty w metadanych graficznych plików wynikowych wykonanych zdjęć (np. w BlackBerry 10 jest to zależne od włączenia tzw. usług lokalizacyjnych)
- Informacja ta trafia do metadanych graficznych (exif data)
- Z łatwością można je odczytać przy pomocy linuksowego narzędzia exiftool (jak i wielu okienkowych aplikacjach przeznaczonych do przeglądania plików graficznych)
- Polecenie exiftool -l wyświetla wszystkie metatagi

```
micha@hayun-820:~$ exiftool -l /media/data/pix/ExifTool/P1000034.JPG |  
grep "GPS"  
....  
GPS Satellites  
....  
GPS Latitude  
GPS Longitude
```

[GEOTAGGING]

```
micha@hayun-820:~$ exiftool -GPSLongitude -GPSLatitude  
/media/data/pix/ExifTool/P1000034.JPG  
GPS Longitude           : 35 deg 11' 9.27" E  
GPS Latitude            : 30 deg 36' 51.73" N
```

# Zdjęcia - exif data - inne parametry

- Poza GPS, z exif data można wyciągnąć też inne wartościowe metadane (szczególnie przydatne przy odzyskiwaniu usuniętych plików, gdy nie ma dostępu do metadanych OS) – jest to również przydatne w weryfikacji, czy zdjęcie nie zostało nieudolnie spreparowane

Czas utworzenia, marka i model urządzenia w wyjściu z komendy

`exiftool -I IMG_20140524_081106.jpg`

```
ExifTool Version Number
  8.60
File Name
  IMG_20140524_081106.jpg
Directory
  .
File Size
  535 kB
File Modification Date/Time
  2014:05:24 08:18:26+02:00
File Permissions
  rwxrwxrwx
File Type
  JPEG
MIME Type
  image/jpeg
Exif Byte Order
  Big-endian (Motorola, MM)
Make
  BlackBerry
Camera Model Name
  BlackBerry Z10
```

# Android - nierozpoznane pliki

- Zaszyfrowane dane
- Ukryte dane (steganografia)
- Umyślnie częściowo uszkodzone dane
- Uszkodzone dane
- ?

# iOS - interesujące lokalizacje

/media/DCIM - zdjęcia

/var/mobile/Library

- /Address Book/
  - AddressBook.sqlitedb - książka adresowa
  - AddressBookImages.sqlitedb - obrazy przypisane do kontaktów
- Calendar/Calendar.sqlitedb - kalendarz
- Call History /call\_history.db - historia połączeń
- Installer/LocalPackages.plist - lista zainstalowanych aplikacji
- Keyboard/Dynamic\_text.dat - słownik użytkownika
- Mail
  - Accounts.plist - ustawienia kont pocztowych
  - Envelope/Index - spis maili
- SMS/sms.db - baza SMS
- Safari
  - Bookmarks.plist - ulubione
  - History.plist - historia przeglądarki
- Voicemail/voicemail.db - poczta głosowa

# iOS - interesujące lokalizacje

- /private/var/root/Library/Caches/locationd/cache\_encryptedA.db
- /private/var/root/Library/Caches/locationd/cache\_encryptedC.db
- /private/var/root/Library/Caches/locationd/lockCache\_encryptedA.db
- /var/preferences/SystemConfiguration/com.apple.wifi.plist
- /private/var/wireless/Library/CallHistory/call\_history.db
- /var/mobile/Application/<APPNAME>/Library/Keyboard/en\_GB-dynamic-text.dat

[iOS full ls] [https://wikileaks.org/ciav7p1/cms/files/full\\_ls.txt](https://wikileaks.org/ciav7p1/cms/files/full_ls.txt)

# Zdalne lokalizacje

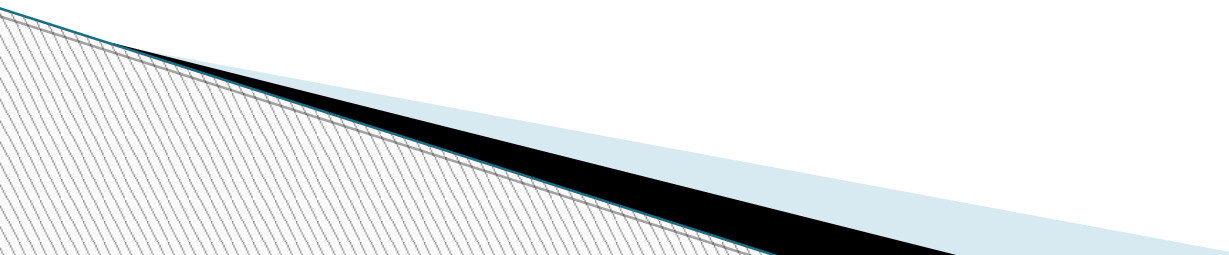
- Dropbox
- Googledrive
- iCloud
- Zasoby NFS/CIFS
- Zewnętrzne konta shell, e-mail, FTP

[Does Google know all the WiFi passwords in the world]  
[3 sposoby FBI na shackowanie zablokowanego iPhone'a]

# Ślady włamań, obecność malware

- W poważniejszych przypadkach sprawdzenie pod kątem obecności malware może mieć kluczowe znaczenie dla charakteru dowodu (obciążający/uniewinniający) – obecność pewnych obciążających danych może być wynikiem włamania;
- Ślady włamania podważają podstawowe założenie pozwalające na wykorzystanie dowodu elektronicznego – tzn. założenie, że to użytkownik urządzenia wykonał dane akcje

## Poszlaki sugerujące włamanie/wysokie ryzyko włamania

- Zrootowane urządzenie
  - Nieaktualizowane urządzenie
  - Urządzenie posiadające zainstalowane aplikacje o złośliwym charakterze (faktycznie nadużywające uprawnień do providerów) [ANDROID MALWARE ANALYSIS]
- 

# Dane przechowywane przez operatora - metadane

Pojęcie metadanych stosuje się do określenia danych na temat danych, np:

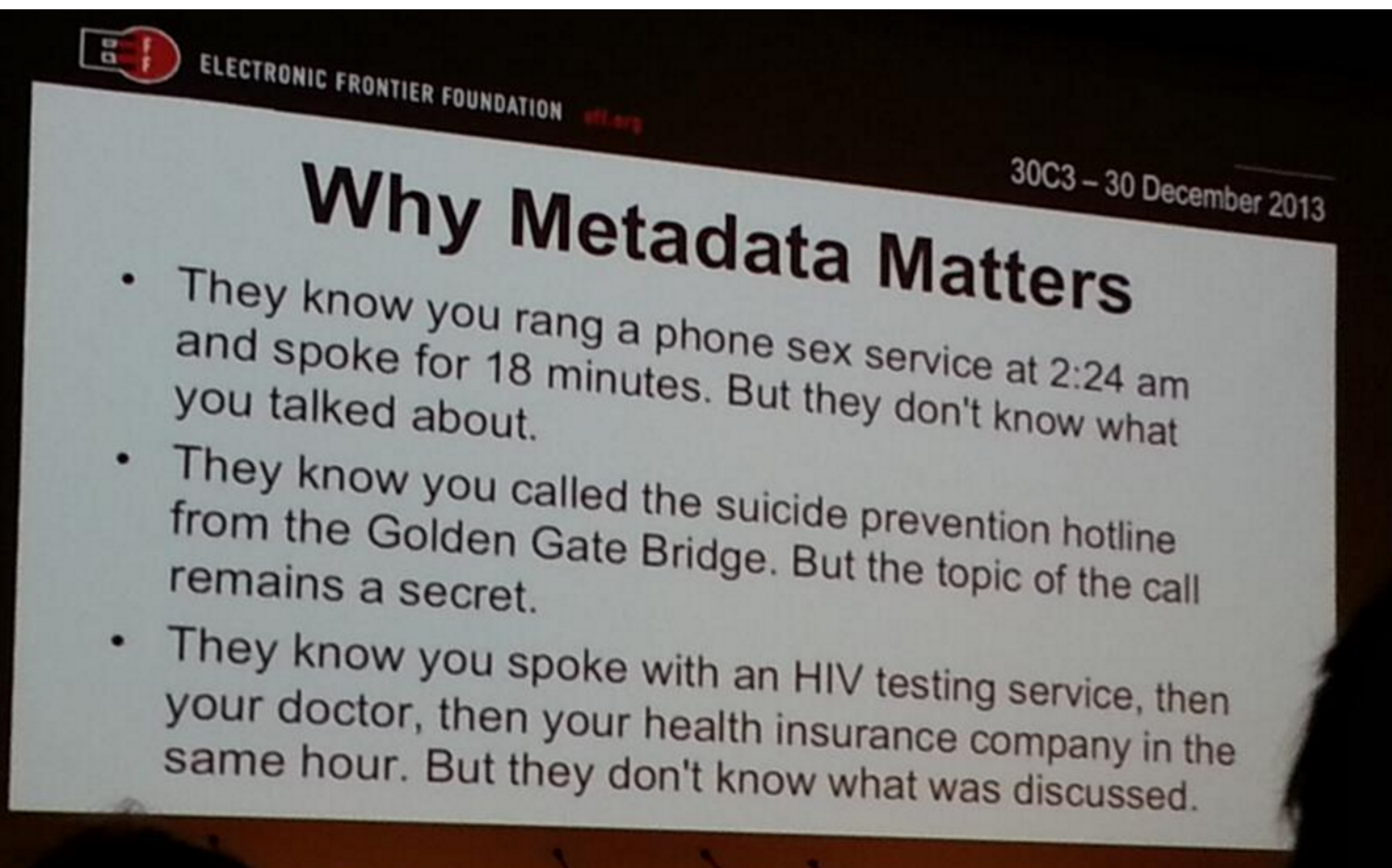
- Nazwy plików, ich rozmiary, daty utworzenia/dostępu/modyfikacji
- Billingi telefoniczne (numery telefonów, czas połączeń)


**Metadane są czasami bardziej przydatne w inwigilacji niż same dane (łatwość przeszukiwania i wykrywania wzorców)**



# Dane przechowywane przez operatora - metadane

Slajd z prezentacji EFF na 30C3:



 ELECTRONIC FRONTIER FOUNDATION [eff.org](http://eff.org)

30C3 – 30 December 2013

## Why Metadata Matters

- They know you rang a phone sex service at 2:24 am and spoke for 18 minutes. But they don't know what you talked about.
- They know you called the suicide prevention hotline from the Golden Gate Bridge. But the topic of the call remains a secret.
- They know you spoke with an HIV testing service, then your doctor, then your health insurance company in the same hour. But they don't know what was discussed.

# Dane przechowywane przez operatora

Dane przechowywane w ramach obowiązkowych przepisów o retencji danych telekomunikacyjnych (do 2 lat).

- Billingi wykonanych rozmów (nie zawierają połączeń nieodebranych, mogą jednak zawierać połączenia do poczty głosowej)
- Billingi wiadomości SMS (sama treść wiadomości SMS nie jest przechowywana przez operatorów, choć istnieje taka techniczna możliwość – treść SMS-ów nie zalicza się do metadanych i podlega ochronie tajemnicą korespondencji – podobnie z treścią (nagraniami rozmów))
- Data, godzina oraz numer stacji bazowej BTS, do której zalogowany był telefon (ICCID + IMEI) → **historia przybliżonych fizycznych lokalizacji**

# GSM – śledzenie lokalizacji

LAI precyzyjnie (do fizycznego BTS-a, do kilkuset, czasami kilkudziesięciu metrów) określa lokalizację geograficzną aktywnego abonenta

LAI składa się z 3 elementów:

MCC (Mobile Country Code), 260 dla PL

MNC (Mobile Network Operator), 03 dla Orange

LAC (Location Area Code), do 5 cyfr, identyfikuje komórkę GSM (komórka GSM składa się z co najmniej jednego BTS-a; stąd też nazwa telefonii komórkowej)

CID – identyfikator BTS-a w komórce

Informacje o BTS-ach i ich lokalizacjach są publicznie dostępne, istnieją nawet aplikacje oferujące usługę lokalizacyjną w oparciu o dane z GSM (alternatywa dla GPS) [HACKADAY]

# GSM - btsearch.pl

btsearch.pl

## BTSearch v2 beta - zapraszamy!



Wyszukiwarka stacji bazowych telefonii komórkowej GSM i UMTS

» Ostatnia aktualizacja: 2014-05-17 10:57:21 » Pobierz wykaz w formacie .csv  
» Liczba stacji bazowych: 28590 » Liczba wpisów (wierszy) w bazie: 84218

QuickBT Search:

Dodaj BTS

Newsletter

Statystyki

Linki

Eksport CLF

Galeria BTS

Mapa BTS

Tutorial

Szukaj:

Wartość szesnastkową wpisz z literą *h* na końcu, np. A3E0h

Sieć:

Rodzaj szukania:

©2000-2014 Krzysztof Niemczyk & Dawid Lorenz & Dominik Boryś » O serwisie » Napisz do nas » Eksport CLF [for Celltrack...] [strona główna](#) | [do góry](#) ^

# GSM - przykład

LAI: 104 03 0CF6D (wyekstraktowany z karty SIM i odkodowany)

104 - dziesiętnie 260, MCC (kod kraju - PL)


03 - MNC (kod operatora, Orange)

0CF6D - dziesiętnie 53101, LAC

Wpisujemy dziesiętną reprezentację LAC do wyszukiwarki (w przypadku wielu BTS-ów w komórce lokalizacja jest mało precyzyjna bez znajomości CID):

[btsearch.pl/szukaj.php?search=53101&siec=2&mode=std](http://btsearch.pl/szukaj.php?search=53101&siec=2&mode=std)

## BTSearch v2 beta - zapraszamy!



Wyszukiwarka stacji bazowych telefonii komórkowej GSM i UMTS

» Ostatnia aktualizacja: 2014-05-19 00:14:11 » Pobierz wykaz w formacie .csv  
» Liczba stacji bazowych: 28597 » Liczba wpisów (wierszy) w bazie: 84293

QuickBT Search:

[Strona główna](#)  
[Dodaj BTS](#)  
[Newsletter](#)  
[Statystyki](#)  
[Linki](#)  
[Eksport CLF](#)  
[Galeria BTS](#)  
[Mapa BTS](#)  
[Tutorial](#)

Kryterium szukania: 53101, sieć: Orange; Znalezione: 1793 | [1] 2 3 4 5 ...

Sieć	Lokalizacja	Pasmo	LAC	CID	RNC	UC-Id	StationID	Uwagi Data akt.
Orange	Bielsko-Biała, Śląskie al. Armii Krajowej 101 - Szpital Wojewódzki - kratownica na dachu	GSM 1800	53101	42147 42148 42149			?	NetWorkSI! 2012-09-29
Orange	Bielsko-Biała, Śląskie al. Armii Krajowej 101 - Szpital Wojewódzki - kratownica na dachu	GSM 900	53101	42141 42142 42143			?	NetWorkSI! 2012-09-29
Orange	Bielsko-Biała, Śląskie al. Armii Krajowej 101 - Szpital Wojewódzki - kratownica na dachu	UMTS 2100	53101	42153 42154 42155	900	59024553 59024554 59024555	?	nośna 10564 NetWorkSI! 2012-09-29
Orange	Bielsko-Biała, Śląskie al. Armii Krajowej 101 - Szpital Wojewódzki - kratownica na dachu	UMTS 2100	53101	42156 42157 42158	900	59024556 59024557 59024558	?	nośna 10589 NetWorkSI! 2012-09-29

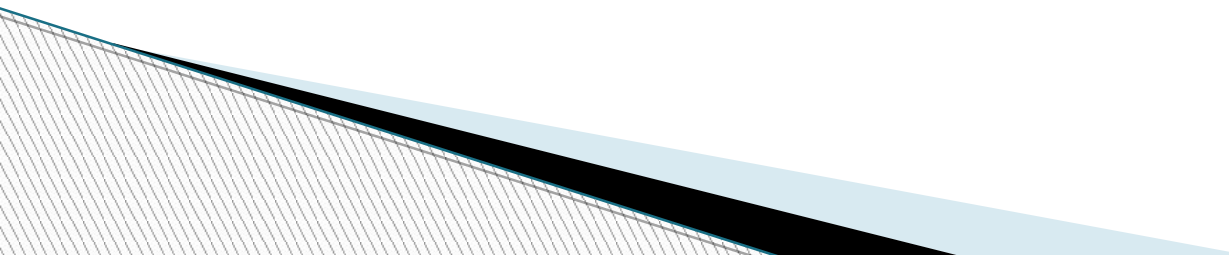
# GSM - btsearch.pl

Istnieje możliwość wyeksportowania całej bazy do pliku .csv:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
1	id	siec_id	wojewod	miestow	lokalizacja	standard	pasmo	lac	btsid	cid1	cid2	cid3	cid4	cid5	cid6	cid7	cid8	cid9	cid0	uwagi	aktualizac	StationId	RNC	carrier
2	1	Plus	Lubuskie	Krosno Oc	maszt Ora	GSM	900	34131	1695	1	2	3									#####	31695		
3	2	T-Mobile	Pomorskie	Rumia	ul. Mickie	UMTS	2100	47104	1346	1	2	3									#####	30885	3050	
4	3	T-Mobile	Wielkopo	Bolewice	ul. Szkoln	GSM	900	48285	4200	1	2	3	4								#####	42006		
5	4	Plus	MaŁopols	Kraków	ul. Skarbo	GSM	900	21500	2966	1	2	3									#####	22966		
6	5	T-Mobile	DolnoŁ	Ł	Chocian	strunob	GSM	900	48270	4848	1	2	3								#####	48121		
7	6	T-Mobile	Lubuskie	Chocie	Chocie	GSM	900	48290	4123	1	2	3									#####	41024		
8	7	T-Mobile	DolnoŁ	Ł	Chojn	ul. Okrzei	GSM	900	48277	4822	1	2	3								#####	48022		
9	8	T-Mobile	Lubuskie	Cybinka	ul. Mickie	GSM	900	48290	4155	1	2	3									#####	41121		
10	9	T-Mobile	Lubuskie	CzerwieŁ	ul. SkŁad	GSM	900	48275	4122	1	2	3									#####	41122		
11	10	T-Mobile	DolnoŁ	Ł	Dobromil	betonowy	GSM	900	48270	4806	1	2	3								#####	48006		
12	11	T-Mobile	Lubuskie	Drezdenk	al. Piast	GSM	900	56210	5515	1	2	3								NetWorks	#####	42025		
13	12	T-Mobile	DolnoŁ	Ł	Gaworzyc	betonowy	GSM	900	48270	4807	1	2	3								#####	48007		
14	13	T-Mobile	Lubuskie	GÅłstow	maszt PTK	GSM	900	48290	4132	1	2	3									#####	41023		
15	14	T-Mobile	DolnoŁ	Ł	GŁog	ul. Merku	GSM	900/1800	48270	4821	1	2	3			7	8	9			#####	48017		
16	15	T-Mobile	DolnoŁ	Ł	GŁog	ul. Skargi	GSM	900/1800	48270	4803	1	2	3			7		9			#####	48003		
17	16	T-Mobile	DolnoŁ	Ł	GŁog	ul. Rudno	GSM	900/1800	48270	4818	1	2	3			7	8	9			#####	48018		
18	17	T-Mobile	DolnoŁ	Ł	Golnice	Golnice 1	GSM	900	56910	6346	1	2	3							NetWorks	#####	49028		
19	18	T-Mobile	Lubuskie	Gorz	ul. Szwale	GSM	900/1800	48300	4208	1	2	3				7	8	9			#####	42012		
20	19	T-Mobile	Lubuskie	Gorz	ul. Energe	GSM	900	48300	4209	1	2	3									#####	42020		
21	20	T-Mobile	Lubuskie	Gorz	ul. Sikorsk	GSM	900/1800	48300	4210	1	2	3				7	8	9			#####	42010		
22	21	T-Mobile	Lubuskie	Gorz	ul. Zubrzy	GSM	900	48300	4211	1	2	3									#####	42011		
23	22	T-Mobile	Lubuskie	Gorz	ul. Matejk	GSM	900/1800	48300	4213	1	2	3				7	8	9			#####	42013		
24	23	T-Mobile	Lubuskie	Gorz	ul. GwiaŁ	GSM	900	48300	4214	1	2	3									#####	42014		

## Dane przechowywane przez operatora - sieć korelacji ICCID ↔ IMEI

Należy pamiętać, iż:

- każda karta SIM (identyfikowana numerem IMSI) mogła być używana z więcej niż jednym telefonem
  - każdy telefon (identyfikowany numerem IMEI) mógł być używany z więcej niż jedną kartą SIM
  - Potencjalnie łańcuch korelacji może być dość długi
- 



# Dane przechowywane przez operatora - sieć korelacji IMSI ↔ IMEI

Przykład 1 (2 telefony, 2 karty SIM, wymieniane stopniowo):

- Po miesiącu użytkowania przestępca kasuje dane z telefonu A i sprzedaje go w lombardzie, a kartę SIM Y umieszcza w nowym telefonie B
- Po tygodniu przestępca wyrzuca kartę SIM Y i zastępuje ją nową Z
- Następnie telefon B wraz z kartą SIM Z zostaje zabezpieczony
- Zabezpieczona zostaje historia połączeń zapisana w telefonie B + operator dostarcza billingi i lokalizacje na podstawie IMSI (karta Z)
- Po odpytaniu operatorów okazuje się, że zabezpieczony telefon B (IMEI) był wcześniej używany z inną kartą SIM Y
- Uzyskany zostaje billing i lokalizacje powiązane z poprzednią kartą SIM Y
- Ponownie, ustalone zostaje, że wcześniej dany IMSI był używany z innym numerem IMEI (telefon A)
- Aktualnie telefon A używany jest aktywnie przez osobę, która zakupiła go w lombardzie i umieściła w nim kartę SIM X... :)

## Dane przechowywane przez operatora - sieć korelacji ICCID ↔ IMEI + korelacja lokalizacyjna

Przykład 2 (2 telefony, 2 karty SIM, od początku używane osobno) – często spotykany scenariusz:

- Przestępca zakupuje nowy “lewy” telefon wraz z kartą SIM (zarejestrowaną przez bezdomnego) i używa go do popełniania przestępstwa
- Przez cały czas nosi ze sobą również swój prywatny telefon z prywatną kartą SIM, wykorzystywany na co dzień do wszystkich pozostałych celów
- Przestępca porzuca “lewy” telefon
- Telefon, wraz z bilingami i danymi lokalizacyjnymi zostaje zabezpieczony
- Analiza historii lokalizacji po stronie operatorów wykazuje, że istnieje drugi telefon (prywatny telefon przestępcy), który przez cały czas podróżował w te same lokalizacje
- Przestępca zostaje zidentyfikowany

Ciekawostka: “lewe” telefony dość łatwo jest zidentyfikować na podstawie anomalii w billingu (wykonywane są połączenia na tylko jeden/dwa numery, + ewentualnie telefon bywa długo niezalogowany do sieci (wyłączony))

# Dane znajdujące się na innych urządzeniach

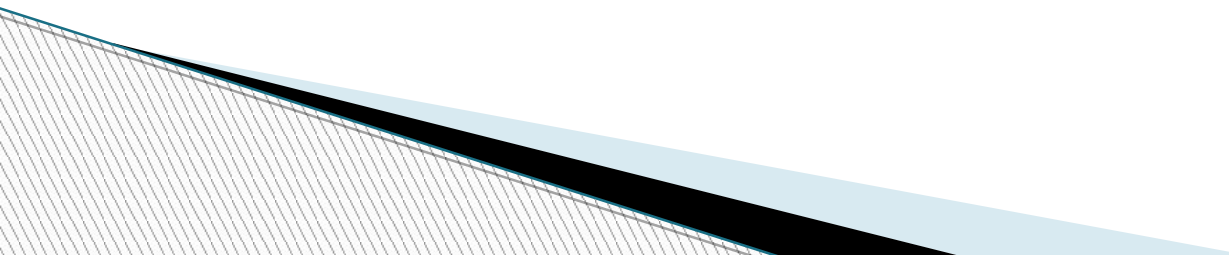
## Scenariusz

1) Cel = historia konwersacji Skype

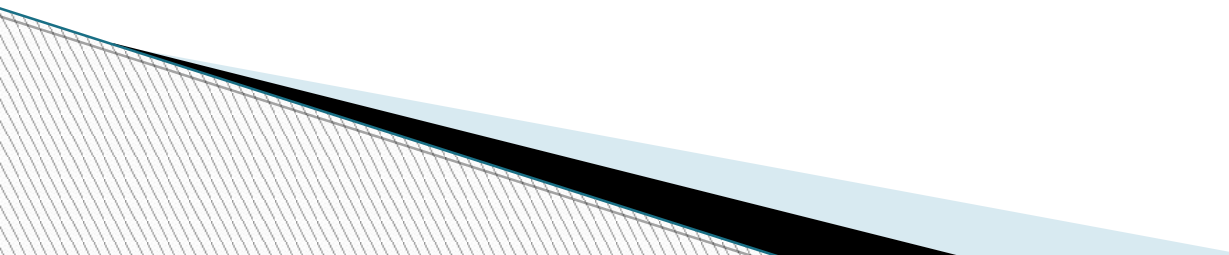
2) Okoliczności:

- Brak możliwości odszyfrowania telefonu
- Brak współpracy ze strony Microsoftu
- Brak możliwości odgadnięcia hasła do konta

3) Potencjalne rozwiązania:

- Inne urządzenia, z których korzystano z danego konta Skype (obecność historii lub poświadczeń (zapisane hasło/token uwierzytelniający → dostęp do historii online)
  - Dostęp do urządzeń/kont rozmówców
- 

# Podsumowanie źródeł informacji o fizycznej lokalizacji urządzenia

- Dane z odbiornika GPS (np. exif data)
  - Dane o logowaniach do stacji BTS posiadane przez operatorów
  - Korelacja informacji o zapamiętanych sieciach bezprzewodowych
  - Korelacja informacji o poborze mocy [Pobór mocy a lokalizacja]
  - Korelacja informacji z akcelerometru
- 

# Dane przechowywane przez operatora - połączenia Internetowe

Jak kwestia retencji wygląda w przypadku metadanych internetowych?

- adresy IP+numery portów?
- URL-e w przypadku braku SSL?
- Ewidencja żądań ICMP?
- Zapytania DNS?

## Odnośniki

Lista odnośników pod adresem:

[https://github.com/ewilded/mobile/W4\\_URLs.txt](https://github.com/ewilded/mobile/W4_URLs.txt)