

ANALIZA PIXEL 3

Pliki telefonu zostały wypakowane na systemie linux, na którym przeprowadzę analizę

Proste wyszukanie plików .sqlite oraz .db za pomocą find

```
(kali㉿kali)-[~/sledcza/pixel/Pixel 3]
$ find . -name *.sqlite
./data/data/org.torproject.torbrowser/files/mozilla/us8lv7tc.default/formhistory.sqlite
./data/data/org.torproject.torbrowser/files/mozilla/us8lv7tc.default/storage-sync.sqlite
./data/data/org.torproject.torbrowser/files/mozilla/us8lv7tc.default/content-prefs.sqlite
./data/data/org.torproject.torbrowser/files/mozilla/us8lv7tc.default/cookies.sqlite
./data/data/org.torproject.torbrowser/files/mozilla/us8lv7tc.default/storage.sqlite
./data/data/org.torproject.torbrowser/files/mozilla/us8lv7tc.default/webappsstore.sqlite
./data/data/org.torproject.torbrowser/files/mozilla/us8lv7tc.default/storage/permanent/chrome/idb/3870112724rsegmnoittet-es.sqlite
./data/data/org.torproject.torbrowser/files/mozilla/us8lv7tc.default/storage/permanent/chrome/idb/3945951496arbeoduate%r3A.sqlite
./data/data/org.torproject.torbrowser/files/mozilla/us8lv7tc.default/signons.sqlite
./data/data/jp.naver.line.android/databases/search.sqlite
./data/data/com.venmo/databases/venmo.sqlite
./data/vendor/location/nvparam.sqlite
./data/vendor/location/xtra/xtra.sqlite
./sbin/.magisk/mirror/data/data/org.torproject.torbrowser/files/mozilla/us8lv7tc.default/formhistory.sqlite
./sbin/.magisk/mirror/data/data/org.torproject.torbrowser/files/mozilla/us8lv7tc.default/storage-sync.sqlite
./sbin/.magisk/mirror/data/data/org.torproject.torbrowser/files/mozilla/us8lv7tc.default/content-prefs.sqlite
./sbin/.magisk/mirror/data/data/org.torproject.torbrowser/files/mozilla/us8lv7tc.default/cookies.sqlite
./sbin/.magisk/mirror/data/data/org.torproject.torbrowser/files/mozilla/us8lv7tc.default/storage.sqlite
./sbin/.magisk/mirror/data/data/org.torproject.torbrowser/files/mozilla/us8lv7tc.default/webappsstore.sqlite
./sbin/.magisk/mirror/data/data/org.torproject.torbrowser/files/mozilla/us8lv7tc.default/storage/permanent/chrome/idb/3870112724rsegmnoittet-es.sqlite
./sbin/.magisk/mirror/data/data/org.torproject.torbrowser/files/mozilla/us8lv7tc.default/storage/permanent/chrome/idb/3945951496arbeoduate%r3A.sqlite
./sbin/.magisk/mirror/data/data/org.torproject.torbrowser/files/mozilla/us8lv7tc.default/signons.sqlite
./sbin/.magisk/mirror/data/data/jp.naver.line.android/databases/search.sqlite
./sbin/.magisk/mirror/data/data/com.venmo/databases/venmo.sqlite
./sbin/.magisk/mirror/data/vendor/location/nvparam.sqlite
./sbin/.magisk/mirror/data/vendor/location/xtra/xtra.sqlite

(kali㉿kali)-[~/sledcza/pixel/Pixel 3]
$ find . -name *.db
```

Przeanalizuję przykładowy plik, aby zobaczyć czy są w nim przydatne informacje:

```
(kali㉿kali)-[~/sledcza/pixel/Pixel 3]
$ sqlite3 ./sbin/.magisk/mirror/data/system_de/0/accounts_de.db
SQLite version 3.40.1 2022-12-28 14:03:47
Enter ".help" for usage hints.
sqlite>

sqlite> .table
accounts          debug_table      meta             visibility
android_metadata  grants          shared_accounts

sqlite> .schema accounts --indent
CREATE TABLE accounts(
  _id INTEGER PRIMARY KEY,
  name TEXT NOT NULL,
  type TEXT NOT NULL,
  previous_name TEXT,
  last_password_entry_time_millis_epoch INTEGER DEFAULT 0,
  UNIQUE(name,type)
);
```

```

sqlite> SELECT * FROM accounts;
1|thisisdfr@gmail.com|com.google||1580312467984
2|858233690|org.telegram.messenger||1580322664981
3|Signal|org.thoughtcrime.securesms||1580322700050
4|imo HD|com.imo.android.imoous||1580322720395
5|TikTok|com.zhiliaoapp.musically||1580323396517
6|Messenger|com.facebook.messenger||1580323862026
7|TDfir|com.twitter.android.auth.login||1580326971888
8|WhatsApp|com.whatsapp||1580332202948
10|thisisdfr|com.silentcircle.account||1580589691083
11|Skype|com.skype.raider||1580591300780
12|TextNow|com.enflick.android.TextNow.account||1581191692330
13|+19195794674|com.viber.voip||1581192938951
14|Duo|com.google.android.apps.tachyon||1581643155834

```

Od razu znalazłem dużo informacji na temat właściciela urządzenia:

email: thisisdfr@gmail.com

Numer telefonu: +19195794674

Czas od ostatniego podania hasła do aplikacji z listy (W sekundach od 1 stycznia 1970)

```

CREATE TABLE shared_accounts(
  _id INTEGER PRIMARY KEY AUTOINCREMENT
  name TEXT NOT NULL,
  type TEXT NOT NULL,
  UNIQUE(name,type)
);
sqlite> SELECT * FROM SHARED_ACCOUNTS;
sqlite> SELECT * FROM shared_accounts;

```

Tablica shared_accounts jest pusta

```

sqlite> .schema visibility --indent
CREATE TABLE visibility(
  accounts_id INTEGER NOT NULL,
  _package TEXT NOT NULL,
  value INTEGER,
  PRIMARY KEY(accounts_id,_package)
);
sqlite> SELECT * FROM visibility;
1|com.google.android.apps.docs|2
1|com.google.android.apps.docs.editors.docs|2
1|com.thinkyeah.galleryvault|2

```

Nic ciekawego

```

(kali@kali)-[~/sledcza/pixel/Pixel 3]
$ sqlite3 ./data/data/org.torproject.torbrowser/files/mozilla/us8lv7tc.default/signons.sqlite
SQLite version 3.40.1 2022-12-28 14:03:47
Enter ".help" for usage hints.
sqlite> .tables
moz_deleted_logins  moz_disabledHosts  moz_logins
sqlite> .schema moz_logins --indent
CREATE TABLE moz_logins(
  id INTEGER PRIMARY KEY,
  hostname TEXT NOT NULL,
  httpRealm TEXT,
  formSubmitURL TEXT,
  usernameField TEXT NOT NULL,
  passwordField TEXT NOT NULL,
  encryptedUsername TEXT NOT NULL,
  encryptedPassword TEXT NOT NULL,
  guid TEXT,
  encType INTEGER,
  timeCreated INTEGER,
  timeLastUsed INTEGER,
  timePasswordChanged INTEGER,
  timesUsed INTEGER
);

```

Kolejny plik, który przykuł moją uwagę

Widnieją tu informacje na temat hostname, username, może nawet hasło. Informacje należą do aplikacji torbrowser

```

sqlite> SELECT * FROM moz_logins;
sqlite> SELECT * FROM moz_disabledHosts;
sqlite> SELECT * FROM moz_deleted_logins;

```

Niestety nic się w nich nie znajduje

Kolejna baza pusta:

```

(kali@kali)-[~/sledcza/pixel/Pixel 3]
$ sqlite3 ./data/data/org.torproject.torbrowser/files/mozilla/us8lv7tc.default/formhistory.sqlite
SQLite version 3.40.1 2022-12-28 14:03:47
Enter ".help" for usage hints.
sqlite> .tables
moz_deleted_formhistory  moz_formhistory
sqlite> SELECT * FROM moz_formhistory;
sqlite>

```

Sprawdziłem więcej baz .sqlite i nic ciekawego nie znalazłem

Przeszukując pliki .db natknąłem się na plik direct.db powiązany z aplikacją instagram

Direct w domyśle oznacza direct messages

I tak, znajdują się tu wiadomości:

```

(kali@kali)-[~/sledcza/pixel/Pixel 3]
$ sqlite3 ./data/data/com.instagram.android/databases/direct.db
SQLite version 3.40.1 2022-12-28 14:03:47
Enter ".help" for usage hints.
sqlite> .tables
android_metadata  mutations  threads
messages          session

```

```

sqlite> SELECT user_id,text FROM messages;
9368974384|Thanks!
9368974384|No problem. You need photos.
9368974384|
9368974384|
9368974384|So what appears here does not show up in Instagram?
9368974384|No it does. Only the chats with people you identify as "close friends" will appear here.
9368974384|
9368974384|
9368974384|
9368974384|

```

Widać tu jednak wiadomości tylko jednej osoby

Ale do tego znamy id właściciela: 9368974384

Oraz odbiorcy: 22824420

```

sqlite> SELECT user_id, recipient_ids FROM threads;
9368974384|22824420

```

XML

Tak jak na iOS znajdują się pliki plist, tak na androidzie znajdują się zwykłe pliki xml

Niestety jest ich bardzo dużo i ciężko się w nich odnaleźć, dlatego spróbuję odczytać ważniejsze z nich

```

(kali@kali)-[~/sledcza/pixel/Pixel 3]
$ find . -name account*.xml
./data/data/com.google.android.apps.photos/shared_prefs/accounts.xml
./data/data/com.google.android.apps.chromecast.app/shared_prefs/accountmenu.AccountSelectionRestorer.selectedAccount.xml
./data/data/com.google.android.settings.intelligence/shared_prefs/account_feature_provider.xml
./data/data/com.google.android.apps.docs.editors.docs/shared_prefs/accountFlagsthisdfir@gmail.com.xml
./data/data/com.google.android.apps.docs.editors.docs/shared_prefs/accountmenu.AccountSelectionRestorer.selectedAccount.xml
./data/data/com.google.android.apps.docs/shared_prefs/accountFlagsthisdfir@gmail.com.xml
./data/system/sync/accounts.xml
./sbin/.magisk/mirror/data/data/com.google.android.apps.photos/shared_prefs/accounts.xml
./sbin/.magisk/mirror/data/data/com.google.android.apps.chromecast.app/shared_prefs/accountmenu.AccountSelectionRestorer.selectedAccount.xml
./sbin/.magisk/mirror/data/data/com.google.android.settings.intelligence/shared_prefs/account_feature_provider.xml
./sbin/.magisk/mirror/data/data/com.google.android.apps.docs.editors.docs/shared_prefs/accountFlagsthisdfir@gmail.com.xml
./sbin/.magisk/mirror/data/data/com.google.android.apps.docs.editors.docs/shared_prefs/accountmenu.AccountSelectionRestorer.selectedAccount.xml
./sbin/.magisk/mirror/data/data/com.google.android.apps.docs/shared_prefs/accountFlagsthisdfir@gmail.com.xml
./sbin/.magisk/mirror/data/system/sync/accounts.xml

```

```

(kali@kali)-[~/sledcza/pixel/Pixel 3]
$ cat ./sbin/.magisk/mirror/data/system/sync/accounts.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<accounts version="3" nextAuthorityId="66" offsetInSeconds="22752">
  <listenForTickles user="0" enabled="true" />
  <authority id="0" user="0" enabled="true" account="thisisdfir@gmail.com" type="com.google" authority="com.google.android.gms.chromesync" syncable="1" />
  <authority id="1" user="0" enabled="true" account="thisisdfir@gmail.com" type="com.google" authority="com.google.android.gms.plus.action" syncable="1" />
  <authority id="3" user="0" enabled="true" account="thisisdfir@gmail.com" type="com.google" authority="subscribed feeds" syncable="1" />
  <authority id="4" user="0" enabled="true" account="thisisdfir@gmail.com" type="com.google" authority="com.google.android.gms.auth.accountstate" syncable="1" />
  <authority id="5" user="0" enabled="true" account="thisisdfir@gmail.com" type="com.google" authority="com.google.android.location.reporting" syncable="1" />
  <authority id="6" user="0" enabled="true" account="thisisdfir@gmail.com" type="com.google" authority="com.google.android.gms.reminders" syncable="1" />
  <authority id="7" user="0" enabled="false" account="thisisdfir@gmail.com" type="com.google" authority="com.google.android.gms.games" syncable="-1" />
  <authority id="8" user="0" enabled="false" account="thisisdfir@gmail.com" type="com.google" authority="com.google.android.gms.appstate" syncable="-1" />
  <authority id="9" user="0" enabled="true" account="thisisdfir@gmail.com" type="com.google" authority="com.google

```

W tym pliku widać do jakich aplikacji został podpięty mail właściciela


```
(kali㉿kali)-[~/sledcza/pixel/Pixel 3]
$ find . -path "**/system/**/*.*.xml"
./data/system/users/0/registered_services/android.content.SyncAdapter.xml
./data/system/users/0/registered_services/android.accounts.AccountAuthenticator.xml
./data/system/users/0/settings_secure.xml
./data/system/users/0/appwidgets.xml
./data/system/users/0/roles.xml
./data/system/users/0/app_idle_stats.xml
./data/system/users/0/settings_system.xml
./data/system/users/0/package-restrictions.xml
./data/system/users/0/runtime-permissions.xml
./data/system/users/0/settings_config.xml
./data/system/users/0/settings_ssaid.xml
./data/system/users/0/settings_global.xml
./data/system/users/0/wallpaper_info.xml
./data/system/users/11.xml
./data/system/users/0.xml
./data/system/users/userlist.xml
./data/system/users/11/registered_services/android.content.SyncAdapter.xml
./data/system/users/11/registered_services/android.accounts.AccountAuthenticator.xml
./data/system/users/11/settings_secure.xml
./data/system/users/11/appwidgets.xml
./data/system/users/11/roles.xml
./data/system/users/11/app_idle_stats.xml
./data/system/users/11/settings_system.xml
```

Wyszukanie plików systemowych

Jest tu między innymi plik z usatwieniami globalnymi telefonu

```
(kali㉿kali)-[~/sledcza/pixel/Pixel 3]
$ cat ./sbin/.magisk/mirror/data/system/users/0/settings_global.xml
<?xml version='1.0' encoding='UTF-8' standalone='yes' ?>
<settings version="183">
  <setting id="43" name="low_battery_sound_timeout" value="0" package="android" defaultValue="0" defaultSysSet="true" />
  <setting id="34" name="car_undock_sound" value="/product/media/audio/ui/Undock.ogg" package="android" defaultValue="/product/media/audio/ui/Undock.ogg" defaultSysSet="true" />
  <setting id="6011" name="Phenotype_boot_count" value="5" package="com.google.android.gms" />
  <setting id="6152" name="time_remaining_estimate_based_on_usage" value="1" package="com.android.systemui" defaultValue="1" defaultSysSet="true" />
  <setting id="110" name="Phenotype_flags" value="activity_starts_logging_enabled:alarm_manager_constants:alarm_manager_dummy_flags:always_on_display_constants:anomaly_config:anomaly_config_version:anomaly_detection_constants:app_idle_constants:app_standby_enabled:appop_history_parameters:backup_agent_timeout_parameters:battery_saver_constants:battery_stats_constants:battery_tip_constants:binder_calls_stats:ble_scan_low_power_interval_ms:ble_scan_low_power_window_ms:blocking_helper_dismiss_to_view_ratio:blocking_helper_streak_limit:device_idle_constants:emergency_call_codes_data:gnsatellite_blacklist:hybrid_sysui_battery_warning_flags:job_scheduler_constants:job_scheduler_quota_controller_constants:job_scheduler_time_controller_constants:location_background_throttle_interval_ms:network_watchlist_enabled:night_display_forced_auto_mode_available:notification_snooze_options:phenotype_test_setting:settings_use_external_provider_api:settings_use_psd_api:smart_replies_in_notifications_flags:sqlite_compatibility_wal_flags:sys_uidcpu_power:text_classifier_constants:zram_enabled" package="com.google.android.gms" />
  <setting id="199" name="development_settings_enabled" value="1" package="com.android.settings" defaultValue="1" defaultSysSet="true" />
  <setting id="10" name="window_animation_scale" value="1.0" package="android" defaultValue="1.0" defaultSysSet="true" />
  <setting id="90" name="_boot_Phenotype_flags" value="" package="com.google.android.gms" />
  <setting id="123" name="battery_stats_constants" value="track_cpu_times_by_proc_state=false" package="com.google.android.gms" />
  <setting id="129" name="blocking_helper_streak_limit" package="com.google.android.gms" />
  <setting id="103" name="autofill_compat_allowed_packages" value="" package="com.google.android.gsf" />
  <setting id="101" name="lang_id_content_url" value="https://www.gstatic.com/android/text_classifier/langid/q/v1/mo del.smfb" package="com.google.android.gsf" />
  <setting id="143" name="settings_use_psd_api" value="1" package="com.google.android.gms" />
  <setting id="4346" name="multi_sim_data_call" value="2" package="com.android.phone" defaultValue="2" defaultSysSet="true" />
```

Oraz plik z użytkownikami

```
(kali㉿kali)-[~/sledcza/pixel/Pixel 3]
$ cat ./data/system/users/0.xml

<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<user id="0" serialNumber="0" flags="19" created="0" lastLoggedIn="1581695517124" lastLoggedInFingerprint="google/blueline/blueline:10/QQ1A.200105.003/6079943:user/release-keys" icon="/data/system/users/0/photo.png" profileBadge="0"
>
  <name>This Is</name>
  <restrictions />
</user>

(kali㉿kali)-[~/sledcza/pixel/Pixel 3]
$ cat ./data/system/users/11.xml

<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<user id="11" serialNumber="11" flags="16" created="1581644358241" lastLoggedIn="1581684601922" lastLoggedInFingerprint="google/blueline/blueline:10/QQ1A.200105.003/6079943:user/release-keys" icon="/data/system/users/11/photo.png" profileBadge="0">
  <name>User 2</name>
  <restrictions />
</user>
```

Pojawił się tutaj User 2

Więcej informacji i szybciej znajdzie aplikacja ALEAPP

ALEAPP

Tak jak w wcześniej pokazałem jest tu tylko jeden mail widoczny:

Accounts_de report

Total number of entries: 1

Accounts_de located at: /home/kali/sledcza/pixel/Pixel 3/data/system_de/11/accounts_de.db

Show 15 entries

Last password entry	Name
2020-02-14 12:54:28	thisisdirtwo@gmail.com
Last password entry	Name

Total number of entries: 13

Accounts_de located at: /home/kali/sledcza/pixel/Pixel 3/data/system_de/0/accounts_de.db

Show 15 entries

Last password entry	Name	Type
2020-01-29 15:41:07	thisisdirt@gmail.com	com.google
2020-01-29 18:31:04	858233690	org.telegram.messenger
2020-01-29 18:31:40	Signal	org.thoughtcrime.securesms
2020-01-29 18:32:00	imo HD	com.imo.android.imoous
2020-01-29 18:43:16	TikTok	com.zhiliaoapp.musically
2020-01-29 18:51:02	Messenger	com.facebook.messenger
2020-01-29 19:42:51	TDfirt	com.twitter.android.auth.login
2020-01-29 21:10:02	WhatsApp	com.whatsapp
2020-02-01 20:41:31	thisisdirt	com.silencircle.account
2020-02-01 21:08:20	Skype	com.skype.raider
2020-02-08 19:54:52	TextNow	com.enflick.android.TextNow.account
2020-02-08 20:15:38	+19195794674	com.viber.voip
2020-02-14 01:19:15	Duo	com.google.android.apps.tachyon
Last password entry	Name	Type

Informacje na temat Bluetooth:

Klucze

Sól

Adres

Bluetooth Adapter Information report

Total number of entries: 10

Bluetooth Adapter Information located at: /home/kali/sledcza/pixel/Pixel 3/data/misc/bluedroid/bt_config.

Show 15 entries

Key	Value
Address	7c:d9:5c:ac:a2:ce
DiscoveryTimeout	120
FileSource	Empty
LE_LOCAL_KEY_DHK	e506ba23332577b905649764bcd9e248
LE_LOCAL_KEY_ER	f6fdc1e629635e0d40e479d02694a0ab
LE_LOCAL_KEY_IR	6aec03cd0258857111ffe969e845ec72
LE_LOCAL_KEY_IRK	195d5c0827a16e7e95b8780cc4243049
Salt256Bit	8c68fa3461653b701e23f6bac4ae6fa71e56f7610758288c0fc27eb7228379ba
ScanMode	0
TimeCreated	2020-01-29 15:38:12
Key	Value

Połączone urządzenia

Bluetooth Connections report

Total number of entries: 1

Bluetooth Connections located at: /home/kali/sledcza/pixel/Pixel 3/data/misc/bluedroid/bt_config.conf

Show 15 entries

First Connected Timestamp	Device Name	MAC Address	Link Key
	Rouge	B4:EC:02:73:FF:93	acf8f79b5ecf1b517c84fa2c0fc57d15
First Connected Timestamp	Device Name	MAC Address	Link Key

Pokazane jest tylko jedno o nazwie Rouge

Rouge oznacza po angielsku czerwony. Nie wiem więc co to za urządzenie

Ciekawe rzeczy pojawiają się w historii połączeń

2020-02-14 01:29:01	9032684955	9195790479	Outgoing 📞	11	North Carolina	US
2020-02-14 01:30:24	9032684955	+19195790479	Incoming 📞	65	North Carolina	US
2020-02-14 13:05:57	9032684955	9195790479	Outgoing 📞	86	North Carolina	US
2020-02-14 14:41:18	9032684955	9195790479	Incoming 📞	91	North Carolina	US

Widzimy tu numer na który właściciel dzwonił: 903 268 4955

Pozostałe połączenia widnieją jako nieodebrane

Właściciel użył także Cast do urządzenia Office speaker. Prawdopodobnie do słuchania muzyki

2020-02-14 23:42:19	4c39777295c6314fcb2877f671b25a5	198660	5	Office speaker	Google Home	C12549866E269585
2020-02-14 23:42:19	f782d122cd23946e20c5770a5bab47e7	233477	5	Office display	Google Nest Hub	87CF4BACBBC707B5

Znalazłem również Imię, Nazwisko oraz Adres właściciela:

Imię: Joshua K Hickman

Adres 1: 120 Braxberry Way, Holly Springs, North Carolina, USA, Zip Code: 27540

Adres 2: 152 Sweet Vista Lane, Holly Springs, North Carolina, USA, Zip Code: 27540

Zakładki w przeglądarce

Chrome - Bookmarks report

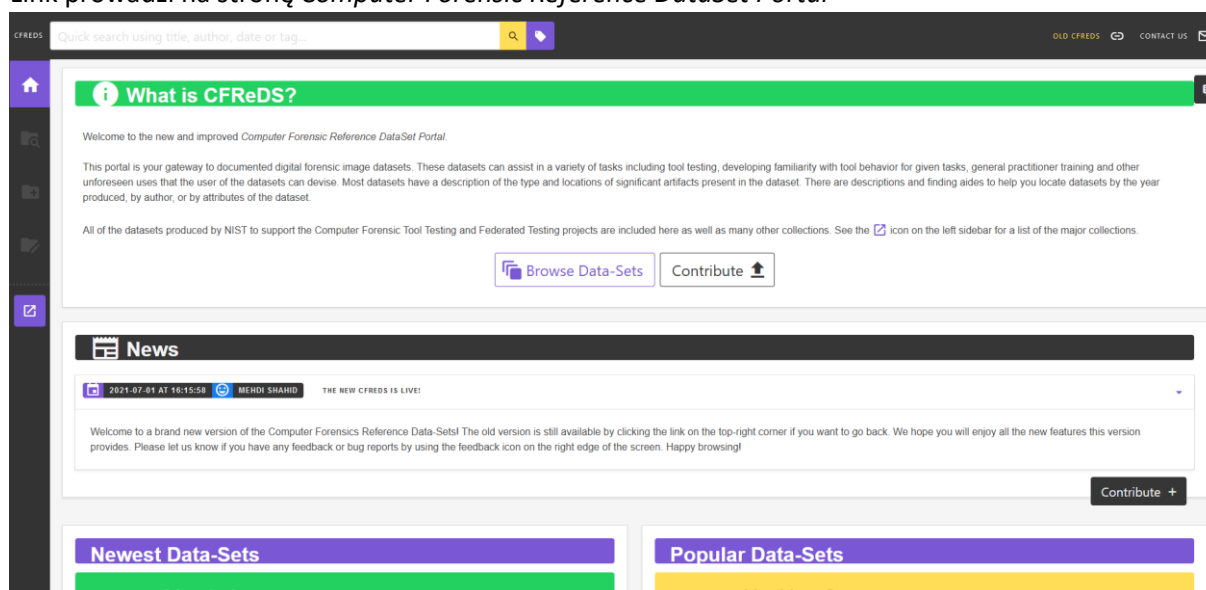
Total number of entries: 1

Chrome - Bookmarks located at: /home/kali/sledcza/pixel/Pixel 3/data/data/com.android.chrome/app_chrome/Default/Bookma

Show 15 entries

Added Date	URL	Name
2018-12-04 13:49:23.188162	https://www.cfreds.nist.gov/	The CFReDS Project

Link prowadzi na stronę *Computer Forensic Reference DataSet Portal*



Mogę po tym wywnioskować, że osoba interesuje się/pracuje w kryminalistyce

Na podstronie <https://cfreds.nist.gov/all/JoshuaHickman/Android12> znajduje się nawet obraz analizowanego właśnie urządzenia

Na urządzenie była również aplikacja Magisk Manager

Chrome - Downloads report

Total number of entries: 2

Chrome - Downloads located at: /home/kali/sledcza/pixel/Pixel 3/data/data/com.android.chrome/app_chrome

Show 15 entries

Start Time	End Time	Last Access Time	URL	Target Path	State
2020-02-01 02:11:22			https://magiskmanager.com/downloading-magisk-manager		Canceled
2020-02-14 21:58:20			https://magiskmanager.com/downloading-magisk-manager		Canceled

Narzędzie służy do zmieniania ustawień systemowych, bez wprowadzania zmian do systemu plików

Znalazłem również dane logowania twittera

Chrome - Login Data report

Total number of entries: 5

Chrome - Login Data located at: /home/kali/sledcza/pixel/Pixel 3/data/data/com.android.chrome/app_chrome/Default/Login Data

Show 15 entries

Search:

Created Time	Username	Password	Origin URL	Blacklisted by User
			android://MYExu9Tv3m412N_fvXcwEbwxtpfSUPdfpHW2_T7J9J97gmKXF3ScYJC-tD2gevgUg91h842hB8cP3SEYwuHTQ==@com.imgur.mobile/	1
2018-11-29 19:51:20	9197580276	w(vZFB867zBwh\$(pathH6Es:@v8z8fyZh	android://u0A-07lvuokjnmf1ciagiykwxsLSrXA9ZzyIb4yGEVu5tPRfhJbn8REHGmDAUKJCGf71TqwUowStwFobRssA==@com.twitter.android/	0
2018-11-30 16:29:09			android://EPqVUnC72PJefEbZr7tpXasZ5RamDixdGHwu1-4wrgoQSwitZ2vLNRvCSFsKVIpuNMukMUNTEFFowYZe-p0zrpA==@com.enflick.android.TextNow/	1
2019-02-07 21:03:10			android://79xEc7TXh3cNp5rV9kciB6AYyfPq8BmRomGIIiNpLTXCAx3qy5RICnOQLbMJaQ1UNGV_N7sSK1dLpTmEZQ8csg==@com.spotify.music/	1
2019-04-05 13:34:13			https://accounts.silentcircle.com/	1

Nie można się jednak zalogować na to konto, ponieważ konto nie istnieje

Informacje o urządzeniu:

Build Info report

Total number of entries: 5
Build Info located at: /home/kali/sledcza/pixel/Pixel 3/vendor/build.prop

Show 15 entries

Key	Value
Android Version	10
Brand	google
Device	blueline
Model	Pixel 3
SDK	29

Informacje o karcie SIM

Device Info report

Total number of entries: 2
Device Info located at: /home/kali/sledcza/pixel/Pixel 3/data/user_de/0/com.android.providers.telephony/databases/telephony.db

Show 15 entries

Search:

Number	IMSI	Display Name	Carrier Name	ISO Code	Carrier ID	ICC ID
6513381146	310260974867669	Google Fi		us	1989	8901260971148676693
+19195794674	310120405730709	Google Fi	Google Fi	us	1989	89011203004056803842

Zapis z konwersacji na Messengerze

Timestamp	Sender Name	Sender ID	Thread Key	Message	Snippet	Attachment Name	Share Name	Share Description
2020-02-01 18:49:07	ThisIs Dfir	100046799400843	ONE_TO_ONE:100030845613112:100046799400843	Hi there!				
2020-02-01 18:50:24	Josh Hickman	100030845613112	ONE_TO_ONE:100030845613112:100046799400843	Hey, how are you?				
2020-02-01 18:50:24	Josh Hickman	100030845613112	ONE_TO_ONE:100030845613112:100046799400843	You can now call each other and see information like Active Status and when you've read messages.				
2020-02-01 18:51:18	ThisIs Dfir	100046799400843	ONE_TO_ONE:100030845613112:100046799400843	Good. Hope you are.				
2020-02-01 18:52:05	Josh Hickman	100030845613112	ONE_TO_ONE:100030845613112:100046799400843	I am. Thanks!				
2020-02-01 18:57:46	Josh Hickman	100030845613112	ONE_TO_ONE:100030845613112:100046799400843		Josh sent a photo.	image-517951378846562		
2020-02-01 18:59:43	ThisIs Dfir	100046799400843	ONE_TO_ONE:100030845613112:100046799400843		You sent a photo.	image-486276645606085		
2020-02-09 18:10:03	ThisIs Dfir	100046799400843	ONE_TO_ONE:100030845613112:100046799400843		You sent a live location.		Holly Springs, North Carolina	Sharing for 60 minutes.

Widoczna jest udostępniona lokalizacja

ID użytkownika

Facebook - User ID report

Total number of entries: 1

Facebook - User ID located at: /home/kali/sledcza/pixel,

Show 15 entries

User ID

100046799400843

Historia wyszukiwania na google maps

Google Search History Maps report

Total number of entries: 2

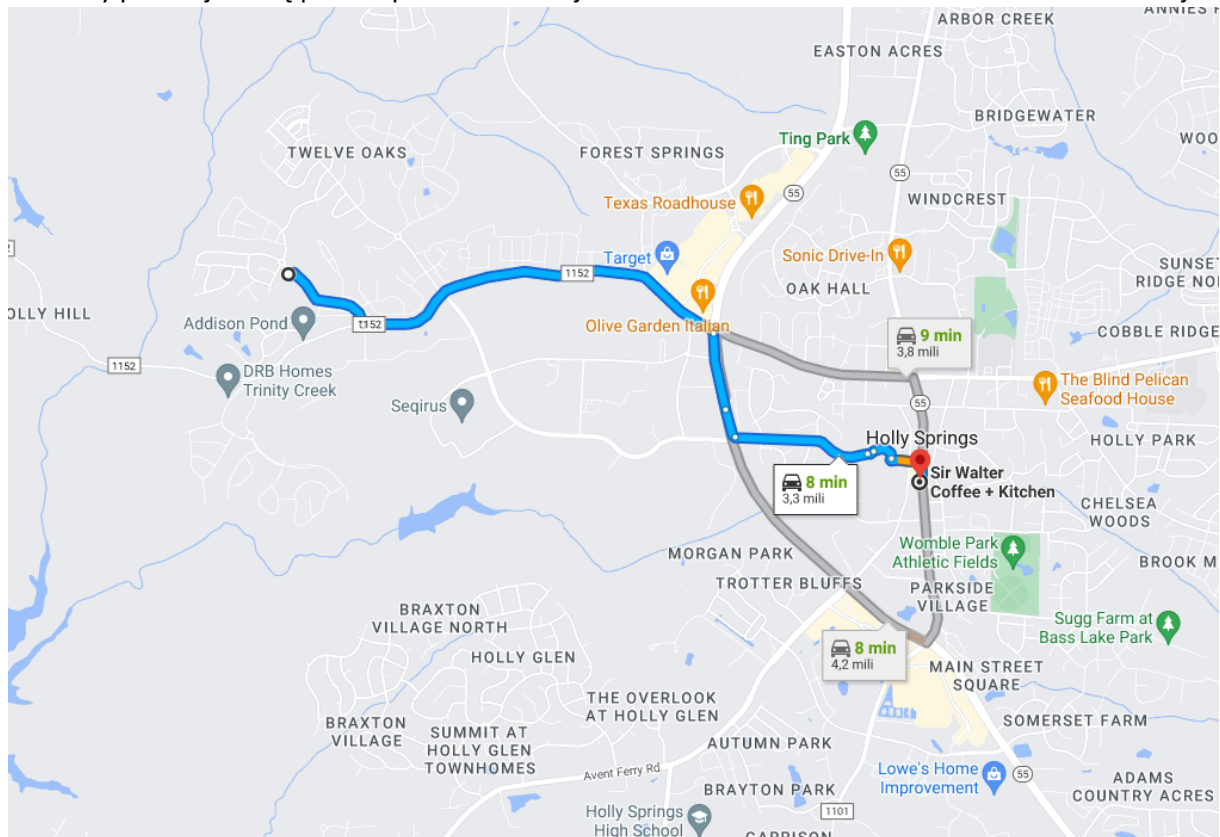
Google Search History Maps located at: /home/kali/sledcza/pixel/Pixel 3/sbin/.magisk/mirror/data/data/com.google.android.apps.maps/databases/gmm_storage.db

Show 15 entries

Search:

Directions	Latitude	Longitude	To Latitude	To Longitude	Row ID	Type
https://google.com/maps/dir/35.660825,-78.8792315/Sir+Walter+Coffee+%2B+Kitchen,+242+S+Main+St+Suite+118,+Holly+Springs,+NC+27540/data=!4m13!4m12!1m14e11m5!1m11s0x89ac8f3c54a4655d:0x8973bbf479866718!2m2!1d-78.83383479999999!2d35.64874572m2!6e0!7e2!3e0	35.660825	-78.8792315	35.6487457	-78.83383479999999	19	uri
https://google.com/maps/dir/35.660825,-78.8792315/Sir+Walter+Coffee+%2B+Kitchen,+242+S+Main+St+Suite+118,+Holly+Springs,+NC+27540/data=!4m13!4m12!1m14e11m5!1m11s0x89ac8f3c54a4655d:0x8973bbf479866718!2m2!1d-78.83383479999999!2d35.64874572m2!6e0!7e2!3e0	35.660825	-78.8792315	35.6487457	-78.83383479999999	19	uri
Directions	Latitude	Longitude	To Latitude	To Longitude	Row ID	Type

Pierwszy pokazuje trasę prawdopodobnie z miejsca zamieszkania właściciela telefonu do restauracji



Drugi link pokazuje dokładnie to samo

Pamięć klawiatury Gboard

Pojawia się tu dużo napisanych wiadomości w różnych aplikacjach

Gboard Keystroke cache - trainingcache2.db report

Keystrokes typed by the user in various input fields of apps, that have been temporarily cached by the Gboard keyboard app are seen here.

Total number of entries: 103

Gboard Keystroke cache - trainingcache2.db located at: /home/kali/sledcza/pixel/Pixel 3/data/data/com.google.android.inputmethod.latin/databases/trainingcache2.db

Show **All** entries

Search:

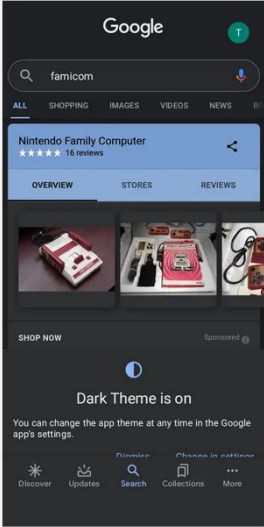
Event Timestamp	ID	Text	App	Input Name	Input ID
2020-01-29 18:49:30	25	oma	com.android.chrome		
2020-01-29 18:56:29	26	ThisIsTim	com.tencent.mm	John Appleseed	
2020-01-29 19:46:45	27	T	com.twitter.android		
2020-01-29 19:46:45	28	TDfir	com.twitter.android		
2020-01-29 20:19:32	29	thisisdfr@gmail.com	com.imgur.mobile	email	
2020-01-29 20:19:32	31	thisisdfr2718	com.imgur.mobile	username	
2020-02-09 18:54:08	222	sir walter coffee	com.google.android.projection.gearhead	Search	
2020-02-09 19:56:11	223	This is a test document . ctest tdocument is cwas created on 020/09/2020 at 14:51	com.google.android.apps.docs.editors.docs		
2020-02-09 19:56:11	224	This test document was created on 02-09-2020 at 14-51Test Document 11	com.google.android.apps.docs.editors.docs		
2020-02-09 19:56:11	225	TEST tTest Folder 2	com.google.android.documentsui	Folder name	
2020-02-14 01:02:52	227	Thanks! Almost done .	com.snapchat.android	Send a chat	
2020-02-14 01:13:15	229	Whats's up?!	com.mywickr.wickr2	Expires in 6 Days	
2020-02-14 01:13:15	230	Word .	com.mywickr.wickr2	Expires in 6 Days	
2020-02-14 01:13:15	231	Ok .	com.mywickr.wickr2	Expires in 6 Days	
2020-02-14 01:50:58	233	Android 10 image .	com.venmo	What's it for?	
2020-02-14 01:50:58	234	Android 10 imahge .	com.venmo	What's it for?	
2020-02-14 01:50:58	235	Thank you .	com.venmo	Leave a comment...	
2020-02-14 02:25:29	237	Super sSecret mMessage Apps	com.google.android.apps.nexuslauncher	Unnamed Folder	

Wiadomości jest bardzo dużo

Pojawiły się 2 wejścia dla Username oraz jedno dla emaila

Nie widać wejść dla haseł

Właściciel był zainteresowany famiconami

Timestamp	Screenshot Path	Search Query	Screenshot	Protobuf Data
2020-02-01 02:13:41	/home/kali/sledcza/pixel/Pixel 3/sbin/.magisk/mirror/data/data/com.google.android.googlequicksearchbox/files/recently/thisisdfr@gmail.com-6982875141504110754.jpg	famicon		{ "id": 8680340539682314510, "z": 0, "timestamp1": 1580523221380, "search-query": "famicon", "search": { "category": "web", "engine": "google.com" }, "screenshot-id": 6982875141504110754, "timestamp2": 1580523221120 }

Wyszukiwanie za pomocą głosu/asystenta google

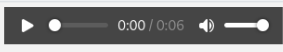
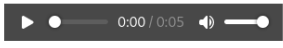
Google App & Quick Search queries report

Recently searched terms from the Google Search widget and any interaction with the Google Personal Assistant / app (previously known as 'Google Now') appear here. This can include g
another device too!

Total number of entries: 4

Google App & Quick Search queries located at: /home/kali/sledcza/pixel/Pixel 3/data/data/com.google.android.googlequicksearchbox/app_session

Show 15 entries

File Timestamp	Type	Queries	Response
2020-01-30 15:44:42	car_assistant	"I need directions to 7629 purfoy Road in Fuquay Varina"	
2020-02-01 02:16:50	search	"farni", "fami", "famicon"	
2020-02-09 18:43:14	opa	"send a text messag", "mobile", "I am on my way to the coffee shop. Do you want anything?", "send"	
2020-02-09 18:47:06	search	"give me directions to Sir Walter cof", "give me directions to Sir Walter coffee in Holly Springs North Carolina"	

Znalazłem kilka ciekawych zdjęć w Google Photos:


2020-02-01 01:46:36	0f6be04949801095a9dc917286ab10c397766771ea7b338dc893e9ddcc4b828a	<div><div>ME</div><div>This is a test message.</div><div>JOSH HICKMAN</div><div>Ok</div><div>ME</div><div>I will do one more.</div><div>JOSH HICKMAN</div><div>That's fine.</div></div>	12363
2020-02-01 01:46:36	b0dfd477c2e4ed30cfda6f56d98a1099ef5576103882300b4010d5f0b98e7f39	<div><div>5:03 PM</div><div>ME</div><div>My bad.</div><div>I can't get this phone to have any badges on the app icons.</div><div>TODAY</div><div>9:34 AM</div><div>ME</div><div>This is a test message.</div><div>JOSH HICKMAN</div><div>OK</div><div>9:34 AM</div><div>ME</div><div>I will do one more.</div><div>JOSH HICKMAN</div><div>That's fine.</div><div>9:35 AM</div><div>YOU TOOK A SCREENSHOT OF CHAT</div><div>9:35 AM</div><div>ME</div><div>Actually, let's do one or two more.</div><div>JOSH HICKMAN</div><div>That's fine. tnn</div></div>	27828

Screenshoty konwersacji

2020-02-01 02:24:58	9a0a7e36bbad3022e6349ae3d2be19d83cbf1a4878ad9572c26d8edf1fb43e29		
---------------------	--	--	--

Zdjęcie samochodu, bez tablicy rejestracyjnej

Screenshot lokalizacji

2020-02-01 02:28:03	7a51c66910dafdedbbfc3fe2b2398e5b5f7855a50af1453324e9c26269d8e4df		
---------------------	--	---	--

Właściciel uczy się/pracuje w kryminalistyce

2020-02-01 02:33:55

8d78825369a853f6950ecc4257a608fa51556f6e8248970dd5c0c00a4cee1a25

12:14

Josh Hickman

This is the test message for the digital forensic research Workshop presentation.

8:31 AM • SMS

Text message

Zapis konwersacji IMO:

IMO - Messages report

Total number of entries: 6

IMO - Messages located at: /home/kali/sledcza/pixel/Pixel 3/sbin/.magisk/mirror/data/data/com.imo.android.imoous/databases/imofriends.db

Show15entries

Search:

Timestamp	From ID	To ID	Last Message	Direction	Message Read	Attachment
2020-01-30 16:05:22	2001584915553829		is now on imo!	Incoming	1	
2020-02-01 14:17:02		2001584915553829	Hey there. How was Imgur?	Outgoing	1	
2020-02-01 14:18:07	2001584915553829		You tell me. You were there.	Incoming	1	
2020-02-01 14:19:30		2001584915553829	True. It was underwhelming.	Outgoing	1	
2020-02-01 14:21:45	2001584915553829		sent photo	Incoming	1	/storage/emulated/0/Download/trs_80.jpg
2020-02-01 14:23:33		2001584915553829	sent photo	Outgoing	1	/storage/emulated/0/Download/Imgur/dqXX3UK.jpg
Timestamp	From ID	To ID	Last Message	Direction	Message Read	Attachment

Lista wszystkich aplikacji:

Installed Apps (Library) report

Total number of entries: 116

Installed Apps (Library) located at: /home/kali/sledcza/pixel/Pixel 3/data/data/com.android.vending/databases/library.c

Show All entries

Purchase Time	Account	Doc ID
	thisisdfr@gmail.com	com.google.audio.hearing.visualization.accessibility.scribe
	thisisdfr@gmail.com	com.google.android.apps.safetyhub
	thisisdfr@gmail.com	com.google.android.apps.wallpaper
	thisisdfr@gmail.com	com.google.android.apps.wearables.maestro.companion
	thisisdfr@gmail.com	com.google.pixel.crosshatch.gamedriver
2018-11-29 18:03:30	thisisdfr@gmail.com	com.google.android.apps.plus
2018-11-29 18:04:07	thisisdfr@gmail.com	com.google.android.apps.docs.editors.docs
2018-11-29 18:05:50	thisisdfr@gmail.com	com.google.android.apps.docs.editors.sheets
2018-11-29 18:07:41	thisisdfr@gmail.com	com.google.android.apps.docs.editors.slides
2018-11-29 18:09:59	thisisdfr@gmail.com	com.google.android.keep
2018-11-29 18:10:19	thisisdfr@gmail.com	com.google.android.apps.books
2018-11-29 18:14:47	thisisdfr@gmail.com	com.google.android.gms
2018-11-29 18:17:31	thisisdfr@gmail.com	com.android.chrome
2018-11-29 18:22:01	thisisdfr@gmail.com	com.google.android.GoogleCamera
2018-11-29 18:22:27	thisisdfr@gmail.com	com.google.android.apps.cloudprint

Wszystkie SMS

Jest to domyślna aplikacja do SMS, ponieważ widać tu bardzo dużo kodów weryfikujących tożsamość

Wiadomości na SKOUT

Skout Messages report

Total number of entries: 7

Skout Messages located at: /home/kali/sledcza/pixel/Pixel 3/sbin/.magisk/mirror/data/data/com.skout.android/databases/skoutDatabase

Show 15 entries

Search:

Timestamp	User	Message	Type	Picture URL	Gift URL
2020-01-31 18:51:20.0	Skout Community	Hey there! If you're looking for something fun to do this weekend, don't forget to check out Live to find your next favorite streamer!	RICH		
2020-02-01 20:23:02.0	Micheal Curtis	Micheal Curtis just joined our local community - Be the first to welcome him!	AUTOINTRO		
2020-02-01 20:25:25.517	(local user)	Hi!	NORMAL		
2020-02-01 20:26:25.782	Josh	This is a terrible app.	NORMAL		
2020-02-01 20:27:17.762	(local user)	Agreed. At least there is no GPS capabilities.	NORMAL		
2020-02-01 20:32:20.402	(local user)	%TEMP% src="http://images-chat.skout.com/b2a008fab71c4dbd851f7d4dad830ea1_20151001"	PICTURE	http://images-chat.skout.com/b2a008fab71c4dbd851f7d4dad830ea1_20151001	
2020-02-01 20:35:31.189	Josh	<skout type="img" id="92804240670" src="http://images-chat.skout.com/d0f97008de374e84b6d34ad83e8aeb95_20151001" locked="true"/>	PICTURE	http://images-chat.skout.com/d0f97008de374e84b6d34ad83e8aeb95_20151001	

Wiadomości na snapchat

Snapchat - Messages report

Total number of entries: 9

Snapchat - Messages located at: /data/data/com.snapchat.android/databases/main.db

Show15entries

Search:

Creation Timestamp	Seen Timestamp	Sender ID	Sender Username	Sender Display Name	Message Type	Text
2018-12-01 17:03:42	2020-02-01 20:08:35	2	thisisdfr	This Is DFIR	text	My bad.
2018-12-01 17:05:16	2020-02-01 20:08:35	2	thisisdfr	This Is DFIR	text	I can't get this phone to have any badges over the app icons.
2020-02-13 19:51:33	2020-02-13 20:04:55	2	thisisdfr	This Is DFIR	snap	
2020-02-13 19:57:31	2020-02-13 20:12:32	1	hickdawg957	Josh Hickman	text	Got it. Nice!
2020-02-13 19:58:05	2020-02-13 19:58:39	2	thisisdfr	This Is DFIR	text	Thanks. Almost done.
2020-02-13 19:59:14	2020-02-13 20:12:32	1	hickdawg957	Josh Hickman	text	I know. Pretty exciting.
2020-02-13 19:59:46	2020-02-13 20:12:32	1	hickdawg957	Josh Hickman	media_v4	
2020-02-13 20:04:40	2020-02-13 20:04:41	1	hickdawg957	Josh Hickman	media_v4	
2020-02-14 13:03:39	UNREAD	3	teamsnapchat	Team Snapchat	snap	

Wiadomości Text now

Text Now - Messages report

Total number of entries: 8

Text Now - Messages located at: /home/kali/sledcza/pixel/Pixel 3/sbin/.magisk/mirror/data/data/com.enflick.android.TextNow/databases/textnow_data.db

Show15entries

Search:

Send Timestamp	Message ID	From ID	To ID	Direction	Message
2020-02-08 15:00:46		+19842032223		Incoming	Hi there!
2020-02-08 15:01:27			+19842032223	Outgoing	Back at it again, I see.
2020-02-08 15:03:06		+19842032223		Incoming	Yep! Have to keep generating data.
2020-02-08 15:05:41			+19842032223	Outgoing	
2020-02-08 15:08:22		+19842032223		Incoming	Missed call from +19842032223
2020-02-08 15:09:16		+19842032223		Incoming	https://media.textnow.com/?t=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6InRoXNpc2RmaXIlLCJrZXkiOiI4YjNmZjg2NC1YzY2LTU2OWltYWMwZi02NTdhNzZmMDh8B3ff864-ec66-569b-ac0f-657a76f05b8b
2020-02-08 15:10:25			+19842032223	Outgoing	https://media.textnow.com/?t=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6InRoXNpc2RmaXIlLCJrZXkiOiI3ODE3YmU2MS1kZTg0LTZhZn0xqqTBZ6t-MIECekWve4Y2u6ihM&h=7817be61-de84-Safc-9321-5df84b02285b
2020-02-08		+19842032223		Incoming	I wonder why I can't call you or send you pictures.

Wersja systemu

OS Version report

Total number of entries: 3

OS Version located at: /home/kali/sledcza/pixel/Pixel 3/data/system/usagestats/0/version

Show15entries

Key	Value
Android Version	10
Build version	6079943
Codename	REL

To wszystkie ciekawe informacje na urzędzeniu Joshua Hickmana