Analiza aplikacji Slack

Maciej Rak
Mateusz Tyl

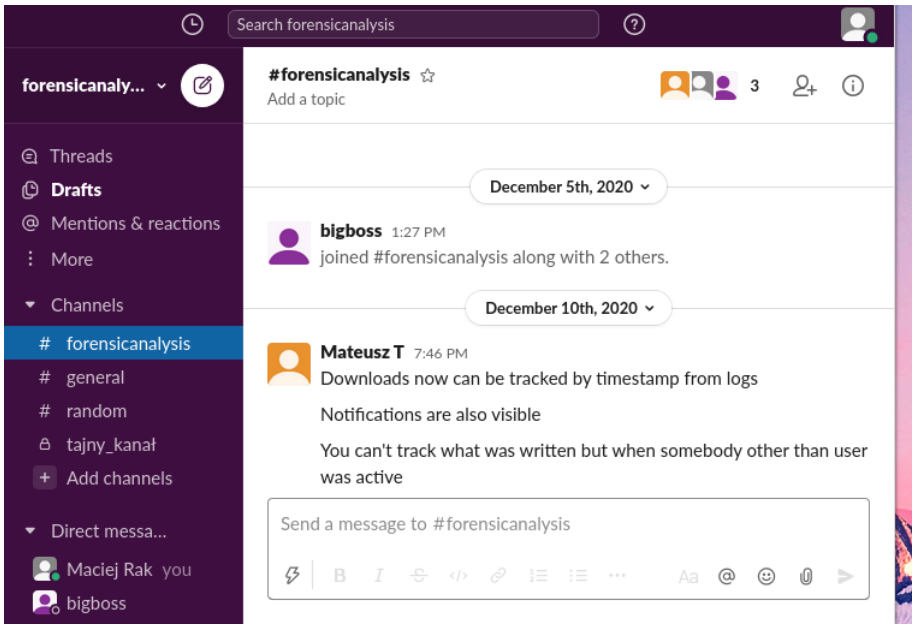
Styczeń 2021

Spis treści

1 Wstęp

1.1 Wysokopoziomowy opis aplikacji

Slack to darmowa usługa pozwalająca na komunikację w zespole w sposób przejrzysty i zorganizowany. Użytkownik dołącza do zespołu w obrębie którego pracuje, a następnie przełączając się między odpowiednimi kanałami może odpowiednio przeglądać zasoby zespołu, a także bezpośrednio skomunikować się z innymi członkami.



Zdjęcie 1: Example

1.2 Zastosowanie

Slack jest najczęściej stosowany w firmach oraz organizacjach w celu organizacji zadań. Z tego powodu często staje się miejscem wymiany danych o dużym znaczeniu biznesowym.

1.3 Z perspektywy Informatyki Śledczej

Slack przechowuje lokalnie ogromne ilości informacji ciekawych z perspektywy informatyki śledczej. Są to nie tylko wszystkie wiadomości wysłane prez uzytkownika w zespołach których jest członkiem, lecz także dokładne odciski wszystkich aktywności (logowanie, wysyłanie i odczytanie wiadomości etc.), tak samo jak historię odwiedzonych kanałów.

2 Analiza danych

W tej części omówimy system plików aplikacji, dane które przechowuje, oraz wskażemy które z nich zawierają interesujące dane.

2.1 Aplikacje desktopowe

Podczas analizy aplikacji desktopowych zauważyliśmy, że zdecydowana większość plików oraz folderów jest identyczna (zwłaszcza te, w których udało nam się znaleźć dane ciekawe z perspektywy informatyki śledczej). Z tego powodu analiza struktur danych jest dla obu aplikacji wspólna.

2.1.1 Środowisko testowe oraz metodologia

Aplikację Slack zainstalowano w wersji desktopowej na maszynach wirtualnych z systemami Windows 10 i Lubuntu 20.10.
Do zarządzania nimi wykorzystano oprogramowanie VMWare Workstation.
Wstępny przegląd danych aplikacji desktopowych przeprowadzono z wykorzystaniem programów **Autopsy**, a do dalszej analizy zamontowano dyski w trybie tylko do odczytu z użyciem narzędzia guestmount.

2.1.2 Lokalizacje plików

Aplikacja Slack zostawia dane w następujących katalogach:
Dla systemu Windows:
Pobrane pliki C:\\Users\nazwa użytkownika\Downloads
Dane aplikacji C:\Users\nazwa użytkownika\AppData\Roaming\Slack

Dla systemu Linux: **Pobrane pliki** /home/nazwa użytkownika/Downloads
Dane aplikacji /home/nazwa użytkownika/.config/Slack
Aplikacja Slack wykorzystuje framework Electron dzięki czemu pozostawiane dane mają bardzo zbliżoną strukturę.

2.1.3 Najciekawsze dane

Po wnikliwej analizie dla obu systemów uznano za najważniejsze z punktu widzenia informatyki śledczej następujące pliki znajdujące się w katalogu Slack:

- **storage/root-state.json** Plik zawiera informacje dotyczące pobranych plików i workspace do których należy użytkownik.
  Linux - workspaces


```
{
  "T01FTL4GPC7": {
    "domain": "forensicanalysis",
    "id": "T01FTL4GPC7",
    "icon": {
      "image_34": "https://a.slack-edge.com/80588/img/avatars-teams/ava_0010-34.png",
      "image_44": "https://a.slack-edge.com/80588/img/avatars-teams/ava_0010-44.png",
      "image_68": "https://a.slack-edge.com/80588/img/avatars-teams/ava_0010-68.png",
      "image_88": "https://a.slack-edge.com/80588/img/avatars-teams/ava_0010-88.png",
      "image_102": "https://a.slack-edge.com/80588/img/avatars-teams/ava_0010-102.png",
      "image_132": "https://a.slack-edge.com/80588/img/avatars-teams/ava_0010-132.png",
      "image_230": "https://a.slack-edge.com/80588/img/avatars-teams/ava_0010-230.png",
      "image_default": true
    },
    "name": "forensicanalysis",
    "order": 0
  }
}
```

Linux - downloads


```
{
  "T01FTL4GPC7": {
    "F01GEPSP4US": {
      "id": "F01GEPSP4US",
      "teamId": "T01FTL4GPC7",
      "url": "https://files.slack.com/files-pri/T01FTL4GPC7-F01GEPSP4US/download/se
      ↪  cret",
      "userId": "U01GM1MGD6D",
      "appVersion": "4.11.3",
      "downloadState": "completed",
      "startTime": 1607447192352,
      "progress": 1,
      "downloadPath": "/home/lubuntu/Downloads/secret",
      "endTime": 1607447192718
    },
    "F01GN823W5R": {
      "id": "F01GN823W5R",
      "teamId": "T01FTL4GPC7",
      "url": "https://files.slack.com/files-pri/T01FTL4GPC7-F01GN823W5R/download/9a
      ↪  5ba575.0",
      "userId": "U01GM1MGD6D",
      "appVersion": "4.11.3",
      "downloadState": "completed",
      "startTime": 1607629755408,
      "progress": 1,
      "downloadPath": "/home/lubuntu/Downloads/9a5ba575.0",
      "endTime": 1607629755679
    },
    "F01GN1YK7GA": {
      "id": "F01GN1YK7GA",
      "teamId": "T01FTL4GPC7",
      "url": "https://files.slack.com/files-pri/T01FTL4GPC7-F01GN1YK7GA/download/st
      ↪  ick__2_.png",
      "userId": "U01GM1MGD6D",
      "appVersion": "4.11.3",
      "downloadState": "completed",
      "startTime": 1607629757681,
      "progress": 1,
      "downloadPath": "/home/lubuntu/Downloads/Stick (2).png",
      "endTime": 1607629758062
    }
  }
}
```

Windows - workspaces


```
{
  "T01FTL4GPC7": {
    "domain": "forensicanalysis",
    "id": "T01FTL4GPC7",
    "icon": {
      "image_34":
      ↪  "https://a.slack-edge.com/80588/img/avatars-teams/ava_0010-34.png",
      "image_44":
      ↪  "https://a.slack-edge.com/80588/img/avatars-teams/ava_0010-44.png",
      "image_68":
      ↪  "https://a.slack-edge.com/80588/img/avatars-teams/ava_0010-68.png",
      "image_88":
      ↪  "https://a.slack-edge.com/80588/img/avatars-teams/ava_0010-88.png",
      "image_102":
      ↪  "https://a.slack-edge.com/80588/img/avatars-teams/ava_0010-102.png",
      "image_132":
      ↪  "https://a.slack-edge.com/80588/img/avatars-teams/ava_0010-132.png",
      "image_230":
      ↪  "https://a.slack-edge.com/80588/img/avatars-teams/ava_0010-230.png",
      "image_default": true
    },
    "name": "forensicanalysis",
    "order": 0
  }
}
```

Windows - downloads


```
{
  "T01FTL4GPC7": {
    "F01GEPSP4US": {
      "id": "F01GEPSP4US",
      "teamId": "T01FTL4GPC7",
      "url": "https://files.slack.com/files-pri/T01FTL4GPC7-F01GEPSP4US/download/se
      ↪  cret",
      "userId": "U01FTM99K7H",
      "appVersion": "4.11.3",
      "downloadState": "completed",
      "startTime": 1607447604865,
      "progress": 1,
      "downloadPath": "C:\\Users\\Mateusz\\Downloads\\secret",
      "endTime": 1607447605467
    },
    "F01GN823W5R": {
      "id": "F01GN823W5R",
      "teamId": "T01FTL4GPC7",
      "url": "https://files.slack.com/files-pri/T01FTL4GPC7-F01GN823W5R/download/9a
      ↪  5ba575.0",
      "userId": "U01FTM99K7H",
      "appVersion": "4.11.3",
      "downloadState": "completed",
      "startTime": 1607629750175,
      "progress": 1,
      "downloadPath": "C:\\Users\\Mateusz\\Downloads\\9a5ba575.0",
      "endTime": 1607629750788
    }
  }
}
```


Dostęp do pobranych plików poprzez link wymaga zalogowania. Nie dotyczy to avatarów. Już tutaj można znaleźć ID workspace, kanału z którego pobrano plik, lokalizację pliku i ID użytkownika. Dzięki informacjom z workspaces można ustalić nazwę subdomeny pod którą jest dostępny workspace i jego ID

- **logs/browser.log**
  Jeden z plików tekstowych z logami aplikacji. Można w nim znaleźć informacje o posiadanym systemie operacyjnym i jego wersji, dla Linuksa o jego dystrybucji i środowisku graficznym.

  Linux


```
{
  "resourcePath": "/usr/lib/slack/resources/app.asar",
  "bootFragments": [],
  "appVersion": "4.11.3",
  "is64Bit": true,
  "isGpuCompositionAvailable": true,
  "isTitleBarHidden": false,
  "platform": "linux",
  "platformVersion": {
    "major": 5,
    "minor": 8,
    "build": 0
  },
  "releaseChannel": "prod",
  "developerMenuOverride": false,
  "uuid": "843b9027-d73b-5e36-be0d-19d692d25c1b",
  "sessionId": "ODQzYjkwMjctZDczYi01ZTM2LWJlMGQtMTlkNjkyZDI1YzFiXzE2MDcxNzQyMDkwNzg=",
  "distribution": "DDL",
  "linux": {
    "os": "Ubuntu 20.10",
    "name": "20.10",
    "release": "groovy",
    "codename": "",
    "desktopEnvironment": "LXQt"
  }
}
```

Windows


```
{
  "resourcePath": "C:\\Users\\Mateusz\\AppData\\Local\\slack\\app-4.11.3\\resources\\app.asar",
  "bootFragments": [],
  "appVersion": "4.11.3",
  "is64Bit": true,
  "isGpuCompositionAvailable": true,
  "isTitleBarHidden": false,
  "platform": "win32",
  "platformVersion": {
    "major": 10,
    "minor": 0,
    "build": 17763
  },
  "releaseChannel": "prod",
  "developerMenuOverride": false,
  "uuid": "c883fc05-d992-5690-8994-dcaff590728b",
  "sessionId": "Yzg4M2ZjMDUtZDk5Mi01NjkwLTg5OTQtZGNhZmY1OTA3MjhiXzE2MDc0NDU1NDA5NzE=",
  "distribution": "DDL",
  "win32": {
    "isAeroGlassEnabled": true,
    "isWin10": true,
    "isStore": false
  }
}
```


Zawiera też informacje o języku aplikacji


```
{
  "locale": "en-US"
}
```

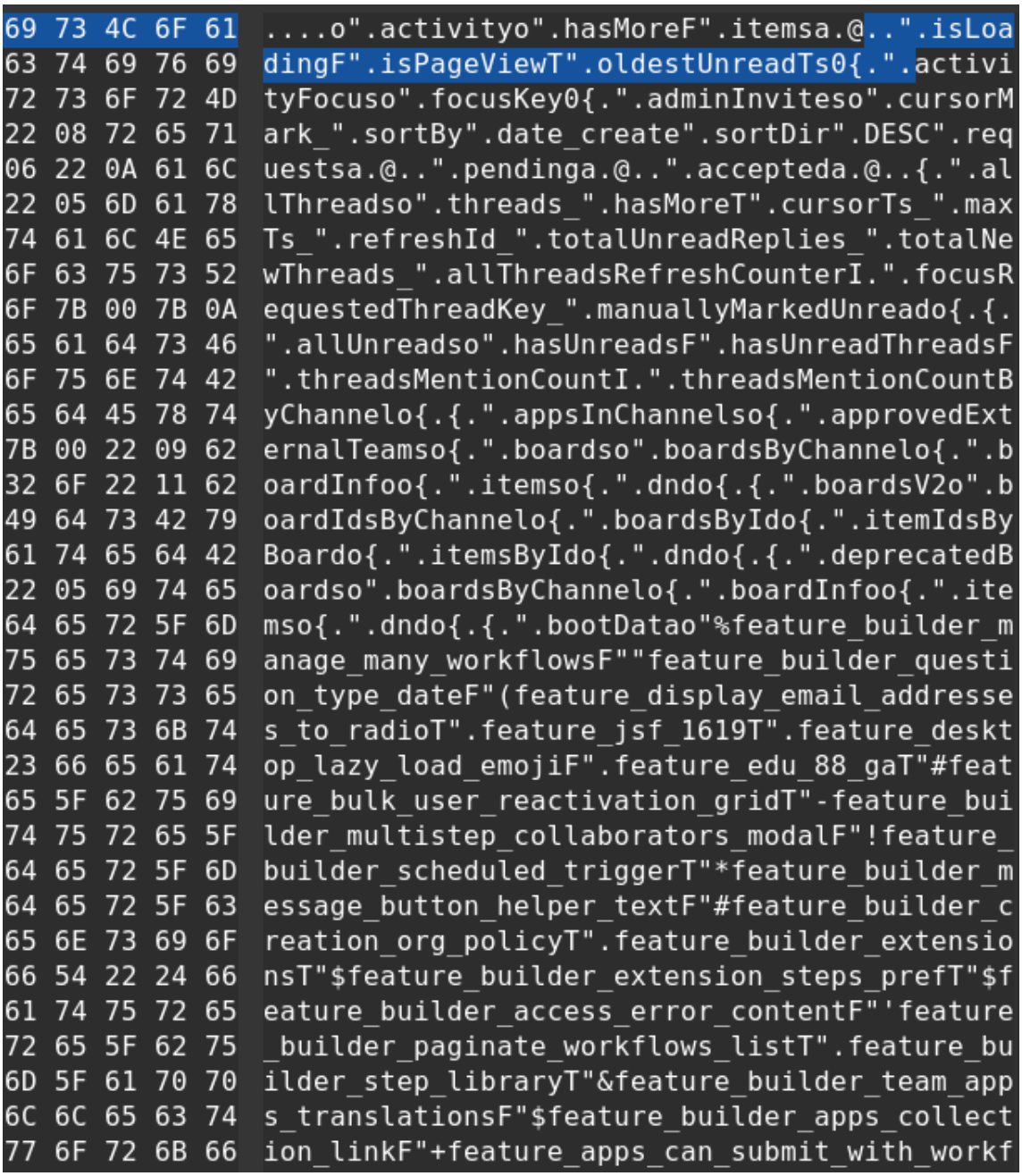
- **Cookies**
  Baza danych SQLite zawierająca dane wybranych ciasteczek

host_key	name	value	path	expires_utc	is_secure	is_httponly
Filtr	Filtr	Filtr	Filtr	Filtr	Filtr	Filtr
.slack.com	b	.jllope9lc5p2cvfh...	/	13567181218828310	1	0
.slack.com	d	vp%2BYhW41Rc...	/	13567185254017009	1	1
.slack.com	lc	1607178853	/	13254244454017065	1	0

root-state.json

Na szczególną uwagę zasługuje ciasteczko o nazwie ***d*** które pozwala na zalogowanie się na konto użytkownika bez znajomości hasła.

- **IndexedDB/https_app.slack.com_0.indexeddb.blob/1/00/** Zawartość katalogu stanowi jeden plik binarny. Przy użyciu programu ghex można zauważyć, że są to dane tekstowe. Wykorzystując program *strings*
  Ominiemy część danych, lecz będą one dużo czytelniejsze.



Blob w ghexie

Wynik polecenia *strings* na pliku.

```
type"    rich_text"
block_id"
tDZa"
elementsA
type"
rich_text_section"
elementsA
type"
text"
You know what's more unstable?{
client_msg_id"\$f5ddf1b1-ad84-4e2f-8052-6fbf56329064"
source_team_id"
T01FTL4GPC7"
type"
message"
1607630518.005600"
channel"
G01G8L00Z99"
no_displayF"
user"
U01G8KPNVGT"
_rxn_key"%message-1607630518.005600-G01G8L00Z99"
subtype_"
text"
You know what's more unstable?"
__meta__o"
lastUpdatedTs"    5708553.7{
1607630528.005900o"    thread_ts_"
slackbot_feels0"
_hidden_reply_"
reply_countI
replies_"
latest_reply_"
reply_users_"
reply_users_count_"
files_"
attachments_"
blocksA
U01G8KPNVGTo"
filesA
activityA
starsA
mentionsA
U01G8KPNVGT"
team_id"
T01FTL4GPC7"
```

```
name"    maciejrak"
deletedF"
color"
4bbe2e"    real_name"
Maciej Rak"
Europe/Warsaw"
tz_label"
Central European Time"    tz_offsetI
profileo"
title"
phone"
skype"
"    real_name"
Maciej Rak"
real_name_normalized"
Maciej Rak"
display_name"
display_name_normalized"
fieldso{
status_text"
status_emoji"
status_expirationI
avatar_hash"
gab5a63a6f22"
email"
maciejrak@student.agh.edu.pl"
status_text_canonical"
team"
T01FTL4GPC7"
image_32"Ahttps://ca.slack-edge.com/T01FTL4GPC7-U01G8KPNVGT-gab5a63a6f22-32"
image_72"Ahttps://ca.slack-edge.com/T01FTL4GPC7-U01G8KPNVGT-gab5a63a6f22-72"    image_192"Bhttps:
image_1024"Chttps://ca.slack-edge.com/T01FTL4GPC7-U01G8KPNVGT-gab5a63a6f22-1024"
is_custom_imageF{
is_adminF"
is_ownerF"
is_primary_ownerF"
is_restrictedF"
is_ultra_restrictedF"
is_botF"
is_app_userF"
updatedN
is_strangerF"
member_color"
4bbe2e"
is_invited_user_"
isExternalF"    isUnknownF"
isNonExistentF"
_name_lc"    maciejrak"
```

Po szczegółowej analizie wyjścia strings ustalono, że blok tekstu zaczynający się od type" rich text" a kończący na attachments" zawiera informacje dotyczące wybranych wiadomości. Poza treścią wiadomości przechowuje też ID workspace, ID kanału na którym została wysłana, ID użytkownika i czas wysłania w formie epoch.

Znając ID użytkownika łatwo znaleźć blok z informacjami o nim. Zaczyna się od ID po którym należy dopisać znaki o". Wśród nich można znaleźć imię i nazwisko podane przy rejestracji, email, nick i strefę czasową.

- **logs/webapp-console.log**

```
[12/10/20, 21:40:21:461] info: Store: NEW_NOTIFICATION

{
  "id": "T01FTL4GPC7_1607629219.001000",
  "title": "[REDACTED]",
  "subtitle": "[REDACTED]",
  "content": "[REDACTED]",
  "authorName": "[REDACTED]",
  "avatarImage": "[REDACTED]",
  "teamId": "T01FTL4GPC7",
  "userId": "U01FTM99K7H",
  "msg": "1607629219.001000",
  "channel": "C01FTL4GUQP",
  "channelName": "[REDACTED]",
  "launchUri": "slack://channel?id=C01FTL4GUQP&message=1607629219.001000&team=T01FTL4GPC7",
  "silent": true,
  "hasReply": true
}
```

Slack zapisuje tu informację za każdym razem kiedy pojawia się nowa wiadomość w czasie uruchomienia aplikacji.

```
[12/08/20, 19:13:03:712] info: [ACTION:MESSAGE] (T01FTL4GPC7) Sent a message to
↪  G01G8L00Z99 via HTTP, clientMsgId: 293722ed-7a32-4bcc-8c92-872323baa1cf
```

Nie można stąd odczytać treści wiadomości ale można poznać ID kanału na który została wysłana.
Gdy tworzony jest nowy kanał znajduje to swoje odzwierciedlenie w logu:

```
[12/05/20, 08:27:41:684] info: [CHANNEL-STATUS] (T01FTL4GPC7) Created channel
↪  C01G1LFLYG6
```

Pojawia się też informacja o dołączeniu do kanału:

```
[12/05/20, 08:27:41:849] info: [CHANNEL-STATUS] (T01FTL4GPC7) You joined channel
↪  C01G1LFLYG6
[12/05/20, 08:27:41:902] info: [API-Q] (T01FTL4GPC7) 2afa031b-1607174861.899
↪  channels.suggestions called with reason: channels-suggestions
[12/05/20, 08:27:41:903] info: [API-Q] (T01FTL4GPC7) 2afa031b-1607174861.899
↪  channels.suggestions is ENQUEUED
```

```
[12/05/20, 08:27:41:909] info: [API-Q] (T01FTL4GPC7) 2afa031b-1607174861.899
↪  channels.suggestions is ACTIVE
[12/05/20, 08:27:41:947] info: [(T01FTL4GPC7)] U01GM1MGD6D joined channel
↪  C01G1LFLYG6
```

Warto zwrócić uwagę na to, że dane ID można powiązać z danymi użytkownika z jednego z poprzednich plików.
W logu można też znaleźć ID zalogowanego użytkownika:

```
[12/05/20, 08:26:59:985] info: [LOCAL-CONFIG] ingestIncomingConfig(): teams before:
↪  (none), teams now: T01FTL4GPC7:U01GM1MGD6D
```

Są to miejsca z których możemy wyciągnąć pełne dane opisujące działanie użytkownika w aplikacji - wszystkie konwersacje, logi aktywności, jego uprawnienia oraz wykonane działania.

2.1.4 Analzia struktur danych

- **blob_storage**
  Katalog zawiera pusty katalog którego nazwa może być identyfikatorem.
- **Cache**
  Katalog zawiera pliki binarne których struktura wskazuje na wynik żądań aplikacji. Są zakodowane i forma zapisu różni się w zależności od systemu.
- **Code cache**
  Katalog zawiera kilka niewielkich plików binarnych w katalogach js oraz wasm.
- **Cookies-journal**
  Plik tekstowy bez zawartości. Jego nazwa może sugerować że umieszczane są w nim dane wygasłych ciasteczek.
- **Crash reports**
  Katalog istniejący tylko w wersji dla Linuksa zawierający plik tekstowy o nazwie client_id zawierający identyfikator. Prawdopodobnie umieszczane są w nim dane o błędach które spowodowały zatrzymanie aplikacji.
- **Crashpad**
  Katalog zawierający podkatalog plik binarny settings.dat, plik tekstowy metadata oraz katalog reports, w którym prawdopodobnie umieszczane są w nim dane o błędach które spowodowały zatrzymanie aplikacji.
- **Databases**
  Katalog występuje tylko dla Linuksa i zawiera plik bazy danych SQLite Databases.db i plik tekstowy Databases.db-journal. Nie zawierają one danych istotnych dla informatyki śledczej.
- **Dictionaries**
  Katalog zawierający dane wykorzystywanych słowników.
- **GPUCache**
  Katalog zawierający kilka plików binarnych. Podczas analizy były wypełnione głównie zerami.
- **Local Storage**
  Katalog zawierający podkatalog leveldb. Podczas analizy plików bazy danych LevelDB nie znaleziono interesujących danych
- **Sentry**
  Katalog zawierający plik scope_v2.json. Zawiera wybrane timestampy związane z pracą aplikacji
- **Installation**
  Plik tekstowy zawierający ID instalacji.
- **Preferences**
  Plik tekstowy zawierający preferencję języka.
- **Quota Manager**
  Niemalże pusta baza danych. Prawdopodobnie powiązany z nią QuotaManager-journal jest pusty.
- **Transport security**
  Plik tekstowy zawierający preferencje HTTPS

- **local-settings.json**
  Informacje o ostatniej wykorzystanej wersji Electrona
- **Network Persistent State**
  Lista adresów do komunikacji z serwerem w tym nazwa subdomeny właściwej dla workspace
- **Service Worker**
  Ma 3 podkatalogi: CacheStorage z danymi tymczasowymi w formie binarnej, Database z pustą bazą danych i ScriptCache z kilkoma plikami binarnymi
- **SingletonLock, SS, SingletonCookie**
  Tylko w systemie Linux: dowiązania symboliczne przechowujące krótką informację
- **IndexedDB**
  Katalog składa się z dwóch podkatalogów: jednego z bazą danych IndexedDB i drugiego z plikiem binarnym. Baza nie przechowuje interesujących danych w przeciwieństwie do pliku.
- **logs/**
  Katalog zawiera logi z działania aplikacji w formie plików tekstowych

2.1.5 Podsumowanie

Na przytoczonych przykładach można łatwo zauważyć, że analizując dane aplikacji desktopowej jesteśmy w stanie z łatwością powiązać wszystkie działania oferowane przez aplikację z odpowiednim zespołem, kanałem i użytkownikiem, wraz ze wskazaniem dokładnego czasu wykonania akcji. Poprzez analizę danych mamy także pełen dostęp do wszelkich konwersacji w których użytkownik wziął udział, nawet tych oznaczonych jako *"prywatny"*.

2.2 Aplikacje mobilne

2.2.1 Środowisko testowe oraz metodologia

Próba analizy została podjęta na dwóch fizycznych urządzeniach:

- Urządzenie z systemem iOS: ***iPhone 5***
- Urządzenie z systemem Android: ***Oppo A91***

Których dane analizowane były na komputerze z systemem ***Arch Linux***.

ANDROID
W celu przeprowadzenia poprawnej analizy, bez ograniczeń, pierwszym krokiem było uzyskanie najwyższych uprawnień (***root***).
W przypadku urządzenia z systemem Android wystarczyło pobrać aplikację KongoRoot:
`https://root-apk.kingoapp.com/`
Uruchomić ją na urządzeniu, a następnie postępować zgodnie z instrukcją na ekranie. Dodatkowo w celu komunikacji z urządzeniem został użyty program ADB [1].

iOS
W przypadku urządzenia z systeme iOS proces w teorii jest analogiczny - należy zainstalować aplikację H3lix:
`https://h3lix.tihmstar.net/`
A następnie postępując zgodnie z instrukcją na ekranie w prosty sposób dokonujemy *jailbreak-a*[2] Nie jest to jednak tak prosty proces jak w przypadku urządzenia z systemem Android z powodu dodatkowych zabezpieczeń zastosowanych przez firmę Apple.

Instalacja aplikacji wymaga podpisanego certyfikatu wydawcy, lub odpowiedniego oprogramowania na komputerze, które pozwoli dokonać *sideloadingu* [3]
Okazało się jednak, że najpopularniejsze narzędzie `http://www.cydiaimpactor.com/` przestało być wspierane i obecnie nie działa.
W tym wypadku postanowiliśmy skorzystać ze specjalnych *"sklepów"* z aplikacjami:

- Panda Helper
- taigone
- ftOS
- AppValey

Są to aplikacje udostępniające do pobrania tymczasowo podpisane aplikacje - w ten sposób nie musimy posiadać certyfikatu, ani dokonywać *sideloadingu*, wystarczy pobrać aplikację ze *"sklepu"*. Wadą jest to, że pobrane w ten sposób aplikację posiadają certyfikat tymczasowy, ważny 24h, lecz jest on wystarczający do wykonania *jailbreak-a*.

Okazało się jednak, iż ponieważ iPhone 5 jest ostatnim iPhonem z procesorem 32bitowym, wsparcie dla niego jest bardzo ograniczone, a certyfikaty aplikacji rzadko odświeżane.
Jednak po długim czasie regularnych prób, udało się wreszcie na jednym ze *"sklepów"* pobrać oraz zainstalować

[1] Android Debug Bridge
[2] Proces analogiczny do *rootowania* telefonu z Androidem - pozwala uzyskać najwyższe uprawnienia na urzadzeniu.
[3] Proces polegający na instalacji oprogramowania na urządzeniu nie bezpośrednio, a poprzez wykorzystanie innego urządzenia.

aplikację "H3lix" oraz wykonać *jailbreak*.

Niestety kolejnym problemem, tym razem niestety niemożliwym do obejścia, okazały się być wymagania aplikacji Slack dla systemu iOS - wymaga on systemu w wersji conajmniej 12.0, tyczasem najnowsza wersja ze wsparciem dla procesora 32bitowego jest 10.3.4.

Jesteśmy jednak niemal pewni, że aplikacja w wersji mobilnej zachowuje się podobnie na obu systemach, z jedyną wartą wspomnienia różnicą - bezpieczny katalog w którym aplikacja może przechowywać wrażliwe dane w systemie Android to **Shared Preferences**, a w systemie iOS jest to **Keychain**. Różnice będą też widocznie w użytych bibliotekach zewnętrznych, jednak wierzymy, że są to różnice o znikomej wadze z perspektywy naszej analizy.

Podejrzenie to, wynika z porównania innych aplikacji które udało nam się pobieżnie porównać, korzystając z oprogramowania ***Passionfruit***, pozwalającego na sprawną i dokładną analizę aplikacji w systemie iOS w sposób zarówno statyczny jak i dynamiczny.

2.2.2 Lokalizacja plików

W przypadku analizy aplikacji mobilnych, na naszą korzyść wpływa architektura aplikacji mobilnych - nacisk na konteneryzację sprawia, że wszystkie dane aplikacji znadują się w katalogu o ograniczonym dostępie: ***/data/data/nazwa_paczki*** (dla aplikacji Slack jest to ***/data/data/com.Slack***). Wszystkie interesujące nas dane znajdziemy w podkatalogach tej lokacji.

```
app_com_birbit_jobqueue_jobs  cache  code_cache  config  databases  files  lib  no_backup  oat  shared_prefs  var
```

Zawartość katalogu com.Slack

2.2.3 Najciekawsze dane

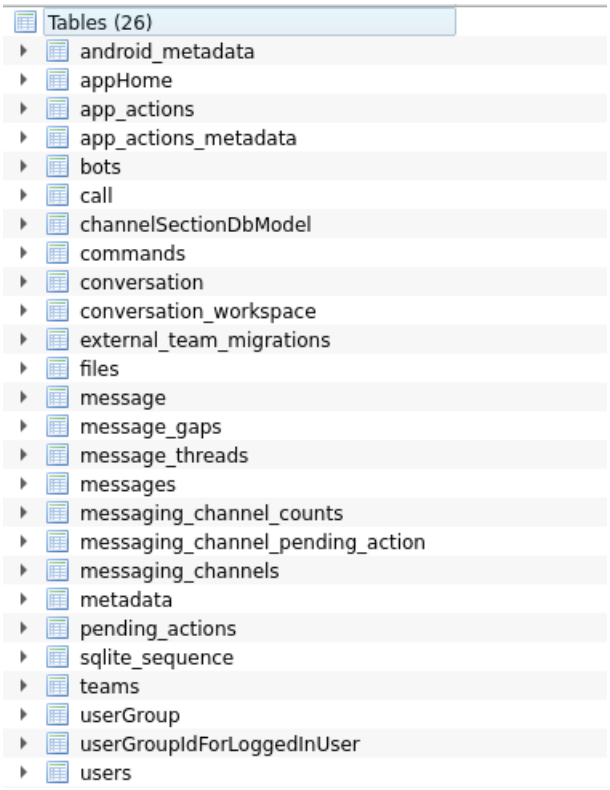
Najciekawszymi miejscami z perspektywy informatyki śledczej w aplikacjach mobilnych będą następujące miejsca:

1. **Katalog database**
   Zaiwera bazy danych, do przeglądania jego zawartości posłużymy się narzędziem sqlitebrowser.

```
❯ ls
T01FTL4GPC7      com.google.android.datatransport.events          db_default_job_manager          mixpanel-journal
T01FTL4GPC7-shm  com.google.android.datatransport.events-journal  db_default_job_manager-journal  org_T01FTL4GPC7
T01FTL4GPC7-wal  db_ChannelSyncJobManager_T01FTL4GPC7             log_sync
account_manager  db_ChannelSyncJobManager_T01FTL4GPC7-journal     mixpanel
```

Lista baz danych

   - **<team_id>**
     Dla każdego zespołu powstaje odpowienia baza danych, która jest niezwykle bogata w interesujące nas dane, takie jak między innymi:

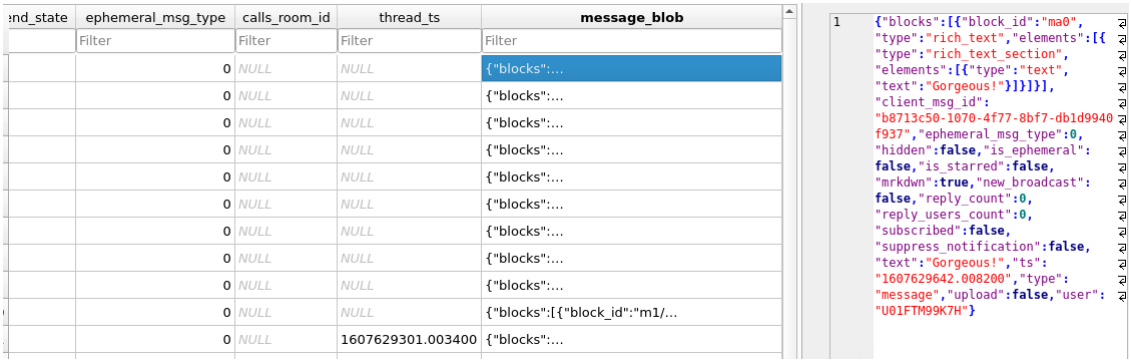


Baza danych <team_id>

- Wszystkie **wiadomości** wysłane w danym zespole, wraz z metadanymi
Możemy z niego odczytać nie tylko treść wiadomości, lecz także czy oraz kto na nią odpowiedział, ile odpowiedzi udzielono, kiedy nastąpiła ostatnia. Dodatkowo możemy zobaczyć czy wiadomość dla użytkownika była oflagowana jako "subskrybowa" (tzn. czy powinien o niej otrzymać powiadomienie) oraz czy może wyłączył akurat dla niej powiadomienia.

_id	local_id	ts	channel_id	client_msg_id
F...	Filter	Filter	Filter	Filter
1	a24c2b39-6303-4c3e-9bd2-4826be7ec9a0	1607629642.008200	C01FTL4GUQP	b8713c50-1070-4f77-8bf7-db1c
2	9504c949-7206-4bdd-8179-58a0d7c83719	1607629624.007900	C01FTL4GUQP	b404379f-2984-4dfe-be99-546c
3	59f6070f-9dff-40ea-bcab-8ab084586159	1607629616.007300	C01FTL4GUQP	c5db203c-4bba-4234-ab68-832
4	9039955a-d6ee-4ff1-bbef-da68862ed7c4	1607629415.005900	C01FTL4GUQP	f3dbd8b0-e9fe-4198-b46b-ff84c
5	a9a7bda0-7339-4a87-9d69-181abac1adc9	1607629401.005700	C01FTL4GUQP	29bdd6b0-9f7a-4785-a8a9-f3c3
6	f6573e53-411f-4cfc-8caa-2da1dec392a8	1607629375.005200	C01FTL4GUQP	717cd353-38e7-4deb-a54f-97cc
7	da88cdf6-7f0c-4f8a-8997-95f0ab0e9f67	1607629342.004600	C01FTL4GUQP	8a646656-b972-4dc2-bf74-b37
8	94b50758-4ce3-4d05-939e-783fd4d4a731	1607629338.004500	C01FTL4GUQP	89baf12e-39f9-4d7e-a803-ff7f1

Wiadomości



end_state	ephemeral_msg_type	calls_room_id	thread_ts	message_blob
	Filter	Filter	Filter	Filter
	0	NULL	NULL	{"blocks":...
	0	NULL	NULL	{"blocks":...
	0	NULL	NULL	{"blocks":...
	0	NULL	NULL	{"blocks":...
	0	NULL	NULL	{"blocks":...
	0	NULL	NULL	{"blocks":...
	0	NULL	NULL	{"blocks":...
	0	NULL	NULL	{"blocks":...
	0	NULL	NULL	{"blocks":[{"block_id":"m1/...
	0	NULL	1607629301.003400	{"blocks":...

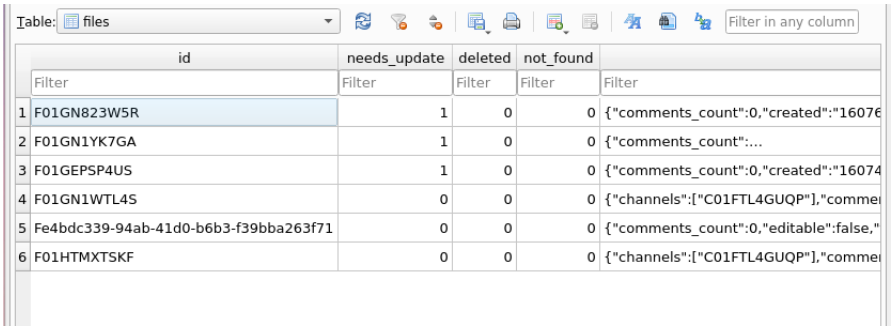

```
1  {"blocks":[{"block_id":"ma0",
   "type":"rich_text","elements":[{
   "type":"rich_text_section",
   "elements":[{"type":"text",
   "text":"Gorgeous!"}]}]}],
   "client_msg_id":
   "b8713c50-1070-4f77-8bf7-db1d9940
   f937","ephemeral_msg_type":0,
   "hidden":false,"is_ephemeral":
   false,"is_starred":false,
   "mrkdwn":true,"new_broadcast":
   false,"reply_count":0,
   "reply_users_count":0,
   "subscribed":false,
   "suppress_notification":false,
   "text":"Gorgeous!","ts":
   "1607629642.008200","type":
   "message","upload":false,"user":
   "U01FTM99K7H"}
```


Wiadomości

"Blob" wiadomości


```
{
   "blocks":[
      {
         "block_id":"pAdfb",
         "type":"rich_text",
         "elements":[
            {
               "type":"rich_text_section",
               "elements":[
                  {
                     "type":"text",
                     "text":"Memy to strata czasu wracać do pracy!"
                  }
               ]
            }
         ]
      }
   ],
   "client_msg_id":"74565990-bcf0-4438-a261-c91659a51688",
   "ephemeral_msg_type":0,
   "hidden":false,
   "is_ephemeral":false,
   "is_starred":false,
   "mrkdwn":true,
   "new_broadcast":false,
   "reply_count":0,
   "reply_users_count":0,
   "subscribed":false,
   "suppress_notification":false,
   "text":"Memy to strata czasu wracać do pracy!",
   "ts":"1607179812.001500",
   "type":"message",
   "upload":false,
   "user":"U01FTM99K7H"
}
```

- **Pliki** wysłane w obrębie zespołu, wraz z metadanymi



Pliki

"Blob" pliku


```
{
   "comments_count":0,
   "created":"1607629676",
   "edit_link":"https://forensicanalysis.slack.com/files/U01G8KPNVGT/F01GN823W5
   ↪  R/9a5ba575.0/edit",
   "editable":true,
   "external_type":"",
   "filetype":"text",
   "has_rich_preview":false,
   "id":"F01GN823W5R",
   "is_external":false,
   "is_public":false,
   "is_revoked":false,
   "is_starred":false,
   "lines":23,
   "lines_more":18,
   "mimetype":"text/plain",
   "mode":"snippet",
   "name":"9a5ba575.0",
   "num_stars":0,
   "permalink":"https://forensicanalysis.slack.com/files/U01G8KPNVGT/F01GN823W5
   ↪  R/9a5ba575.0",
   "pretty_type":"Plain Text",
   "preview":"-----BEGIN
   ↪  CERTIFICATE-----\nMIIDqDCCApCgAwIBAgIFAKcnDMswDQYJKoZIhvcNAQELBQAwgYoxFD
   ↪  ASBgNVBAYT\nC1BvcnRTd2lnZ2VyMRQwEgYDVQQIEwtQb3J0U3dpZ2dlcjEUMBIGA1UEBxML
   ↪  UG9y\ndFN3aWdnZXIxFDASBgNVBAoTC1BvcnRTd2lnZ2VyMRcwFQYDVQQLEw5Qb3J0U3dp\n
   ↪  Z2dlciBDQTEXMBUGA1UEAxMOUG9ydFN3aWdnZXIgQ0EwHhcNMTQwNzA2MTMzMTI3",
```

```
    "preview_highlight":"\u003cdiv class\u003d\"CodeMirror cm-s-default
    ↪ CodeMirrorServer\" oncopy\u003d\"if(event.clipboardData){event.clipboard
    ↪ Data.setData(\u0027text/plain\u0027,window.getSelection().toString().rep
    ↪ lace(/\\u200b/g,\u0027\u0027));event.preventDefault();event.stopPropagat
    ↪ ion();}\"\u003e\n\u003cdiv
    ↪ class\u003d\"CodeMirror-code\"\u003e\n\u003cdiv\u003e\u003cpre\u003e----
    ↪ -BEGIN
    ↪ CERTIFICATE-----\u003c/pre\u003e\u003c/div\u003e\n\u003cdiv\u003e\u003cp
    ↪ re\u003eMIIDqDCCApCgAwIBAgIFAKcnDMswDQYJKoZIhvcNAQELBQAwgYoxFDASBgNVBAYT
    ↪ \u003c/pre\u003e\u003c/div\u003e\n\u003cdiv\u003e\u003cpre\u003eC1BvcnRT
    ↪ d2lnZ2VyMRQwEgYDVQQIEwtQb3J0U3dpZ2dlcjEUMBIGA1UEBxMLUG9y\u003c/pre\u003e
    ↪ \u003c/div\u003e\n\u003cdiv\u003e\u003cpre\u003edFN3aWdnZXIxFDASBgNVBAoT
    ↪ C1BvcnRTd2lnZ2VyMRcwFQYDVQQLEw5Qb3J0U3dp\u003c/pre\u003e\u003c/div\u003e
    ↪ \n\u003cdiv\u003e\u003cpre\u003eZ2dlciBDQTEXMBUGA1UEAxMOUG9ydFN3aWdnZXIg
    ↪ Q0EwHhcNMTQwNzA2MTMzMTI3\u003c/pre\u003e\u003c/div\u003e\n\u003c/div\u00
    ↪ 3e\n\u003c/div\u003e\n",
    "public_url_shared":false,
    "size":1330,
    "thumb_360_h":0,
    "thumb_360_w":0,
    "thumb_720_h":0,
    "thumb_720_w":0,
    "thumb_800_h":0,
    "thumb_800_w":0,
    "thumb_pdf_h":0,
    "thumb_pdf_w":0,
    "timestamp":"1607629676",
    "title":"9a5ba575.0",
    "url_private":"https://files.slack.com/files-pri/T01FTL4GPC7-F01GN823W5R/9a5
    ↪ ba575.0",
    "url_private_download":"https://files.slack.com/files-pri/T01FTL4GPC7-F01GN8
    ↪ 23W5R/download/9a5ba575.0",
    "user":"U01G8KPNVGT"
}
```


Warto zwrócić uwagę na "preview_highlight" ponieważ zawiera kod javascript wykonywany w przypadku powiększenia obrazka przez użytkownika,
"[...] oncopy\u003dïf(event.clipboardData)event.clipboardData.setData(\u0027text/plain\u0027,window.getSelection().toString().replace(/\\u200b/g,\u0027\u0027)); event.preventDefault();event.stopPropagation(); [..]"
mógłby to być potencjalny wektor ataku na użytkownika.

- Informacje na temat **kanałów**

Table: messaging_channels

	_id	msg_channel_id	name_or_user	name_or_user_normalized	type	is_starred	is_open	is_member	lates
	F...	Filter	Filter	Filter	Fil...	Filter	Filter	Filter	Filter
1	1	C01FTL4GUQP	random	random	0	0	1	1	1609682791
2	2	C01G1LFLYG6	forensicanalysis	forensicanalysis	0	0	1	1	1609682791
3	3	C01G8JKK52P	general	general	0	0	1	1	1609682791
4	4	G01G8L00Z99	tajny_kanał	tajny_kanal	1	0	1	NULL	1609682791
5	5	D01G1MK4V5L	U01FTM99K7H	U01FTM99K7H	2	0	1	NULL	NULL
6	6	D01G8DMDU3U	USLACKBOT	USLACKBOT	2	0	0	NULL	NULL
7	7	D01GEJEEUA0	U01GM1MGD6D	U01GM1MGD6D	2	0	1	NULL	1607179534
8	8	D01GY8ZK400	U01G8KPNVGT	U01G8KPNVGT	2	0	1	NULL	NULL

Kanały

- Oraz bogaty zbiór informacji o **użytkownikach**

Table: users

	_id	id	name	deleted	updated	app_deleted_state	presence	color	tz	
	F...	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filt
1	1	U01G8KPNVGT	maciejrak	0	1609682589	2	NULL	4bbe2e	Africa/Monrovia	Gre
2	2	U01FTM99K7H	mtyl	0	1608817214	2	NULL	e7392d	Europe/Athens	Eas
3	3	U01GM1MGD6D	balhaim	0	1607179053	2	NULL	9f69e7	America/New_York	Eas
4	4	USLACKBOT	slackbot	0	0	2	active	757575	America/Los_Angeles	Pac

Użytkownicy

profile_real_name_normalized	profile_display_name_normalized	profile_email	
Filter	Filter	Filter	Fi
Maciej Rak		maciejrak@student.agh.edu.pl	
Mateusz T	Mateusz T	mtyl@student.agh.edu.pl	
bigboss		balhaim@protonmail.com	
Slackbot	Slackbot	NULL	

Użytkownicy

- **account_manager**
  Ta baza danych zawiera dane logowania użytkownika zarówno w wersji zaszyfrowanej jak i nie. Dzięki nim możemy zalogować się na konto użytkownika w danym zespole, nie znając jego hasła.

Table: accounts — Filter in any column

	user_id	team_id	token	token_encrypted	token_encrypted_ext1	token_encrypted_ext1_checksum
	Filter	Filter	Filter	Filter	Filter	Filter
1	U01G8KPNVGT	T01FTL4GPC7	xoxs-1537684567415-1552669777571-16...	AWO4B2a1tirpV0JtYerJERn4Y6TvpVMAN08f...	ARUp9BoCVs2edZac+f5oWZdhX+IN2HxB/...	7dee602773771d319978ff73a8273f4a082...

Tokeny

2. **Katalog cache**

   - Zawiera zdjęcia wysłane przez użytkownika, oraz zdjęcia oraz emotikony używane w ostatnim czasie przez użytkownika. W katalogu **image_manager_disk_cache** możemy także znaleźć plik **journal** który służy do zarządzania pamięcia cache w sposób optymalny.

```
./file-upload:
IMG_20210103_141534.jpg

./image_manager_disk_cache:
148b75b183d1797d2fa27aedb80f12a2903b0e464750724a6ab204bb5ac92cd4.0  752970f60160bd897bb7dc825d1be12d951fe3c9f9de7fdf620bf60f91ec8226.0
172cdf9e515e2d34caf21d9b3a1fc9cba971f44da19947a35323870e940bd846.0  7b0dc91d7417a14eec21b8e2d381843f1f518b2547584e423a25c00732b03bdc.0
27318a75c8b965364028b20e18bb11de589a341658a931937ba64ce31500ac61.0  83f64ae4254751d691a20a29a8fe9d7b2c60ebaae39c41a8b0721de79207a0b6.0
46657231067e26ac5512a293bb2b42441b76df42b98688e1cf8925f862331f4a.0  89981daaeaea328f6a53267d955c319e12f0175014375a6d2a249a0ce15a9125.0
4732ee66de320425fb539eaf5c06930a4d6ca2733d3006deeece09988220d1f6.0  8c6ca8d45e58dac005c70cdee77d040f6606fc95c738c2d97508a0e6f001c387.0
536068b2e21d9064379490f307422c2e61d3cdf63c0b8ec99e26b005d3e9bdfb.0  962c556c89620b1e0aee386d17b47a79570711f8a226d6be99365f734b071b18.0
58d0ae84d475e15c34248e809f84a74818714c57962840f72f76b826e660c6f9.0  97ac66ce46022b312b45576d4894c4327278ff363165c31f35a9376cbd70b65d.0
5bb43463b41225ffd3a291219e7bec9114b5bf897f36f9e16f745a8432c4e4b7.0  9e04f7257886017b1ae2cb90885bc478266ad3dfe4bedb91f4fee7e86851bee1.0
5ce63e33cdad1a97c5563505468c9c8ac6a8afa58ba98694e535eda58c302742.0  9e797892e617e6e3fe0be9af4281ab3ee34d6a170850bf8e172645d1e29ccbef.0
```

Zawartość katalogu cache (ciekawa część)

3. **Katalog files/**

   - Zawiera pliki **debug.log*** w których znajdziemy dane na temat aktywności użytkownika.

```
01-03 14:15:42:123 Process keyboard hidden action: SHOW_TAB_CONTENT.
01-03 14:15:42:123 Toggle tab content, show: true.
01-03 14:15:42:123 Should collapse send bar: false, input has focus: false, is file share or upload: false, hidden action: SHOW_T
AB_CONTENT, emoji picker visibility: 8, tab content visibility: 0, currentTab: PhotoTab(advancedMessageData=AnyFileData(files=[Ad
vancedMessageImageUploadPreviewData(intentData=Intent { act=android.intent.action.SEND typ=image/ (has extras) }, mimeType=image/
, size=Size(width=960, height=1280), ticketId=Fe4bdc339-94ab-41d0-b6b3-f39bba263f71, title=IMG_20210103_141534.jpg)], unfurls=nul
l, previewScrollIndex=0), fullscreen=false, showPermissionsScreen=false).
01-03 14:15:42:123 Should collapse send bar: false, input has focus: false, is file share or upload: false, hidden action: SHOW_T
AB_CONTENT, emoji picker visibility: 8, tab content visibility: 0, currentTab: PhotoTab(advancedMessageData=AnyFileData(files=[Ad
vancedMessageImageUploadPreviewData(intentData=Intent { act=android.intent.action.SEND typ=image/ (has extras) }, mimeType=image/
, size=Size(width=960, height=1280), ticketId=Fe4bdc339-94ab-41d0-b6b3-f39bba263f71, title=IMG_20210103_141534.jpg)], unfurls=nul
l, previewScrollIndex=0), fullscreen=false, showPermissionsScreen=false).
01-03 14:15:42:123 Updating send bar display to mode: FULL.
```

Debug log

Na przykładzie widać akcję użytkownika - wysłanie obrazka.

Podsumowanie

W podanych wyżej katalogach/plikach możemy znaleźć najciekawsze z perspektywy informatyki śledczej dane. Na ich podstawie możemy utworzyć bardzo dokładną, chronologiczną mapę aktywności nie tylko użytkownika, lecz całego zespołu.

2.2.4 Analzia struktur danych

- **app_com_birbit_jobqueue_jobs**
  katalog należący do modułu birbit - kolejki prac dla systemu android. Obecnie system jest przedawniony, nie zalecany do użycia.

  app_com_birbit_jobqueue_jobs/files_jobs_ChannelSyncJobManager_T01FTL4GPC7
  app_com_birbit_jobqueue_jobs/files_jobs_default_job_manager
  to podkatalogi modułu **birbit**, służą do zarządzania kolejką operacji na plikach. pierwszy jest przypisany do użytkownika (używajac jego identyfikatora jako ostatnia część nazwy), zaś drugi jest domyślny.

- **cache:**
  trzy podkatalogi bugsnag-*
  Należą do narzedzia moniturującego stabilność, nie zawierają danych interesujących nas z perspektywy informatyki śledczej `https://www.bugsnag.com/`

  cache/file_upload
  Zawiera zdjęcia które użytkownik wysłał za pomocą aplikacji

  cache/image_manager_disk_cache
  Zawiera ostatnio używane obrazki (bez kompresji, zgodne z orgyginałem) dodatkowo zawiera plik journal, który najprawdopodobniej jest częścią bilbioteki `https://github.com/google/iosched` - pomaga w zarządzaniu cachem - od niego zależy które pliki zostaną usunięte, tak by panować nad zajętym miejscem

- **code_cache**
  Pusty katalog, prawdopodobnie służy do przechowywania złożonych obiektów z kodu dla szybszego dostepu

- **config/Preferences/org/netbeans/modules/autoupdate.properties** Jest to plik konfiguracyjny modułu do IDE pozwalającego na proste auto-aktualizacje zawiera pola z identyfikatorami pozwalające jednoznacznie opisać źródło pochodzenia aktualizacji które zgodzimy się przyjąć.

- **config/Windows2Local**
  Kolejny framework pakietu netbeans - przechowuje dane na temat pozycji, oraz otwartych/zamkniętych okien

bottomSlidingSide	explorer	output	rightSlidingSide
bottomSlidingSide.wsmode	explorer.wsmode	output.wsmode	rightSlidingSide.wsmode
editor	leftSlidingSide	properties	topSlidingSide
editor.wsmode	leftSlidingSide.wsmode	properties.wsmode	topSlidingSide.wsmode

Menadżer okien

Po dogłębnej analizie nie znaleziono żadnych danych interesujących z perspektywy informatyki śledczej.

- **files/PersistedInstallation.W0RFRkFVTFRd+MTo1MDg3Njc0MDM0MjQ6YW5kcm9pZDo3YzI2MT**
  Jest to plik zawierający tokeny autoryzacji i refresh token do niektórych usług firebase.


```
{
   "Fid":"f85J-_Y-T3um-lRRYqjgx5",
   "Status":3,
   "AuthToken":"eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCJ9.eyJmaWQiOiJmODVKLV9ZLVQzdW0tbFJ
   SWXFqZ3g1IiwicHJvamVjdE51bWJlciI6NTA4NzY3NDAzNDI0LCJleHAiOjE2MTAyODczMTEsImFwcEl
   kIjoiMTo1MDg3Njc0MDM0MjQ6YW5kcm9pZDo3YzI2MTk3ODUyOTExMTFkIn0.AB2LPV8wRQIgDTTzNa3
   kf6h9XIbh-I7VEwgTJ7xuudbEr7q18yBxq8ECIQCoQoPvjudcxDTO598395bDxJ-kgvki6SmuLql416j
   ngQ",
   "RefreshToken":"2_YiTLVvEPVPAv2eexwQHX_zz22QFfp-mY2gYv7D56xnmfoXkDmoQsjhUPF7LFz_D4",
   "TokenCreationEpochInSecs":1609682511,
   "ExpiresInSecs":604800
}
```


  Według informacji znalezionych w internecie nie służą one do dostępu do poufnych lub w inaczej sposób ważnych danych, zatem nie jest on ciekawy z perspektywy informatyki śledczej

- **files/AFRequestCache**
  Pusty katalog, prawdopodobnie zawiera dane pozwalające przyspieszyć pewne funkcje zapewnione przez API.

- **lib**
  Pusty katalog, prawdopodobnie domyślny katalog w aplikacji przechowujący biblioteki wymagane przez aplikacje

- **no_backup**
  Katalog zawierający plik com.google.android.gms.appid-no-backup - o pliku nie ma wiele informacji w internecie, występuje w dwóch miejscach jako potencjalny plik tworzony przez szkodliwe oprogramowanie:
  `https://vms.drweb-av.de/virus/?i=17777965&lng=de`
  `https://vms.drweb-av.pl/virus/?i=17686290`

- **shared_prefs**
  Specjalnie wydzielone miejsce w pamięci do którego dostępu pod żadnym pozorem nie mają inne aplikacje - chyba że urządzenie posiada uprawnienia roota: Jest to miejsce wykorzystywane przez system android do przechowywania specjalnych map danych (w postaci <klucz, wartość>) które pozwalają na zdecydowanie szybszy dostęp do danych

  Pliki:
  CONV_MENTION_COUNT_PREF<team_id>.xml
  CONV_UNREAD_COUNT_PREF<team_id>.xml

  Zawierają kolejno dane na temat ilości wspomnień użytkownika, oraz nieprzeczytanych wiadomości (dotyczących danego zespołu).

  FirebaseAppHeartBeat.xml

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <long name="fire-global" value="1609682510492" />
    <long name="fire-iid" value="1609682511069" />
    <long name="fire-installations-id" value="1609682510492" />
</map>
```

  Zawiera dane identyfikacyjne instalacji (dla bazy danych firebase)

  GCM_PREFS.xml

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="KEY_DEVICE_ID">dcec31ffc4373d20</string>
    <string name="KEY_GCM_REG_ID">f85J-_Y-T3um-lRRYqjgx5:APA91bEMNpKwn1u2HkkTtZismy
    pc7XDwOUXfeqDb_Bqeppba_YBe-Gf3pbHOH2hCBmWD134dLVPWUAvsFZUHHSOr3XY47Xw4tjAzirH-K
    fIIkMqbFx2QV6UUmfFktnvvsoNsMkMF16a7</string>
</map>
```

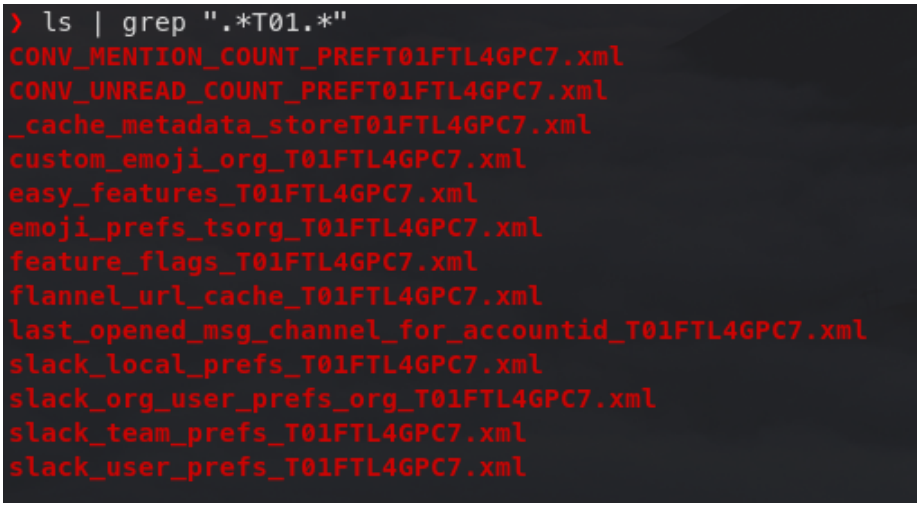
  Zawiera dane identyfikacyjne urządzenia oraz regionu geograficznego użytkownika. Dane są zaszyfrowane i nie udało nam się ich odczytać. Jednak mogą one pozwolić zidentyfikować konkretnego użytkownika

account_token_store.xml

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="__androidx_security_crypto_encrypted_prefs_key_keyset__">12a90164
    349d523eeaf832acd113d76a192c3f691f4c02b6fde26026aadbcd9d4de17328bfae106a46262e9
    46b810f07c790f2a601c9ed45ed30b077c918395eff3eb154c9503b2fa5a188cfd2bd515f9d11e5
    9ab3380c2253693393f2146210cc9a365f3960ab86d841c38d6747b51019a64884ac275baebed6d
    d6f89bf7becff1bcad7b181455f7f632b6b2471d2233f43de781441efb668e03354230528143635
    2b12e6b7f1b352db26651a4408ecdbe69c03123c0a30747970652e676f6f676c65617069732e636
    f6d2f676f6f676c652e63727970746f2e74696e6b2e4165735369764b6579100118ecdbe69c0320
    01</string>
    <string name="ATOZrezGCNmCuHwxCKerlWEQRSXG32jGW1J2s+MlsSs=">ATrOcM1vd1IFdxXANqv
    /4UUsy/LV27lg/YsqN9LixI21gDYKRgwYo7KwLGqC2KwKnFhQ0DLMmvBpCxTyLonJwfoSAaI4LqQYfJ
    4lliPm1uKO0/74ZYTtIPhgZ3+JPdx0tX2JbRcjPsJWKhM76UrwiuD9eWT8eRAQnCML4mifX7aH98H82
    jU5bwuWYIwhPc21ZnHd6HZtVgc=</string>
    <string name="__androidx_security_crypto_encrypted_prefs_value_keyset__">128801
    788dbb21aedd5af155d13227708b2878b01d96323cd1ae619b57bbe11d70138eea8734181d4ea57
    4ec5c7d7611ff9f64884d18da1a932b1be147dbb5a89bc9d71fbea40edc9ccd399114748facf9ba
    42fa733292a05b4799c7b1a5a5681620d0a5cd1d17d3c89247a30844654c17a14fbef600ff9212a
    8d71589281022e7d84a7c6f5ec7949cb3481a4408cde1b9d603123c0a30747970652e676f6f676c
    65617069732e636f6d2f676f6f676c652e63727970746f2e74696e6b2e41657347636d4b6579100
    118cde1b9d6032001</string>
</map>
```

Zawiera zaszyfrowane tokeny uwierzytelniające użytkownika

- **wszystkie pliki zakończone _<team_id>.xml**



Pliki

Zawierają konfigurację użytkownika związane z danym zespołem, z ciekawszych danych znajdują się tu między innymi historia otwieranych kanałów w zespole:
last_opened_msg_channel_for_accountid_<team_id>.xml

```
<map>
    <string name="last\_opened\_channel\_source">MESSAGES</string>
    <string name="channel\_history">D01G8DMDU3U,C01G1LFLYG6,C01G8JKK52P,C01FTL4
    GUQP</string>
</map>
```

A także informacje na temat uprawnień:
slack_team_prefs_<team_id>.xml

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
[...]
<string name="warn_before_at_channel">always</string>
<string name="who_can_create_channels">regular</string>
<string name="who_can_kick_channels">admin</string>
<boolean name="channel_email_addresses_enabled" value="true" />
<boolean name="commands_only_regular" value="false" />
<long name="compliance_export_start" value="0" />
[...]
```

Oraz preferencje dotyczące powiadomień:
slack_org_user_prefs_org_<team_id>.xml

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="dnd_after_thursday">22:00</string>
    <string name="dnd_before_sunday">8:00</string>
    <string name="dnd_after_sunday">22:00</string>
    <string name="dnd_enabled_wednesday">PARTIAL</string>
    <string name="dnd_enabled_saturday">PARTIAL</string>
    <string name="dnd_start_hour">22:00</string>
    <string name="dnd_after_friday">22:00</string>
    <string name="emoji_mode">DEFAULT</string>
    <string name="dnd_enabled_friday">PARTIAL</string>
    <boolean name="dnd_weekdays_off_allday" value="false" />
    <string name="dnd_after_wednesday">22:00</string>
    <string name="dnd_enabled_tuesday">PARTIAL</string>
    <string name="dnd_after_monday">22:00</string>
    <string name="preferred_skin_tone">1</string>
    <string name="dnd_after_tuesday">22:00</string>
    <string name="dnd_end_hour">8:00</string>
    <string name="dnd_enabled_sunday">PARTIAL</string>
    <boolean name="dnd_enabled" value="true" />
    <string name="dnd_enabled_monday">PARTIAL</string>
    <string name="dnd_before_thursday">8:00</string>
    <string name="dnd_before_wednesday">8:00</string>
    <string name="dnd_after_saturday">22:00</string>
```

```
    <string name="dnd_days">EVERY_DAY</string>
    <string name="dnd_before_saturday">8:00</string>
    <string name="dnd_enabled_thursday">PARTIAL</string>
    <string name="dnd_before_monday">8:00</string>
    <string name="dnd_before_friday">8:00</string>
    <string name="dnd_before_tuesday">8:00</string>
</map>
```

2.2.5 Podsumowanie

Analiza aplikacji mobilnej wskazała, że aplikacja Slack przechowuje lokalnie dane, które z powodzeniem można wykorzystać w informatyce śledczej, zgodne z tymi które można znaleźć w aplikacji desktopowej.