



3e Rendez-vous 4n6s

12 Mai 2020

Heather Mahalik Senior Director of Digital Intelligence at Cellebrite
Jean-Philippe Noat Senior Director of Intl training chez Cellebrite

Format des rendez-vous

- Votre rendez-vous d'échange
- Proposer les sujets qui vous intéressent
- Poser des questions techniques, si toutes ne peuvent être répondues elles le seront lors du prochain rendez-vous.
- Faites vous plaisir et échangez
- Mettre l'humain au coeur de la technique
- N'hésitez pas à présenter un sujet si vous le souhaitez



Que faire en cas de pépin ?

En cas de perturbation technique :

mon portable +33 6 08 98 08 94

Pour toute question sur le thème (et les thèmes à venir)

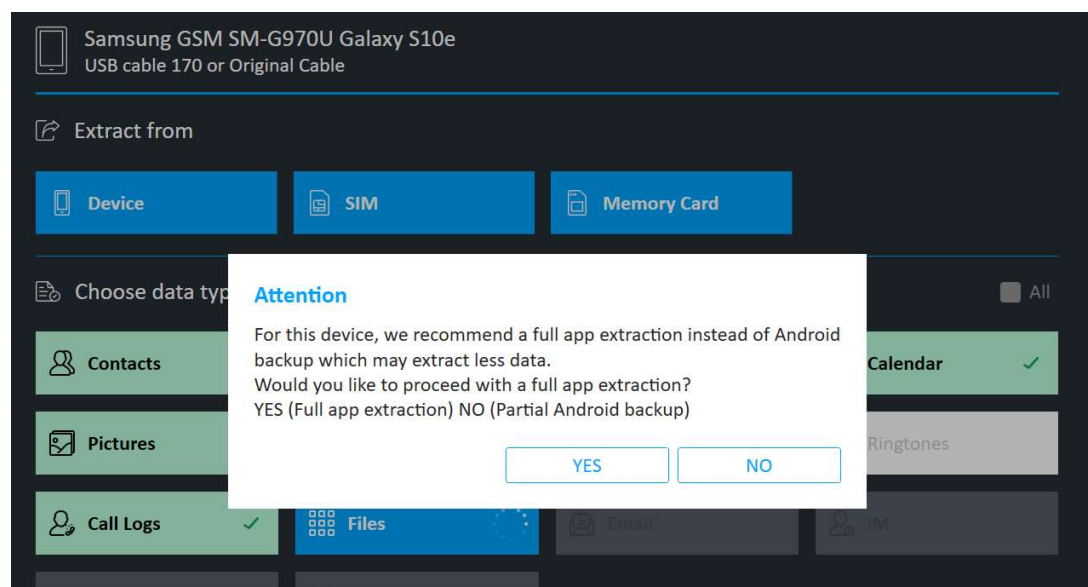
jean-philippe.noat@cellebrite.com

Heather@cellebrite.com

NEW FEATURES IN UFED

Nouvelles fonctionnalités Features de l'UFED

- Support checkm8 – version 13.4 supportée
- Samsung “Extract All Apps” - NOUVEAUTES





Mobile device



SIM card



Mass storage



UFED camera



Drone



Device tools





Search By: Name, Model, Chipset, IMEI, TAC, Manufacturer



CONNECT DEVICE TO AUTO DETECT

EXTRACTION FLOW



★ AUTO DETECTION TIPS

Android devices

1. Enable developer options (tap Build Number 7 times)
2. Enable USB debugging
3. Enable stay awake (if available)
4. Set USB connection to enable file transfers (MTP/Media)

iOS devices

1. Disable auto-lock

ABORT

BACK

CONSOLE

BROWSE DEVICES

AUTO DETECT

NOUVEAUX DEVELOPPEMENTS DANS PHYSICAL ANALYZER

Nouveautés dans Physical Analyzer

- Nouvelle Interface
- Un seul bouton pour les extractions iOS
- Regroupement des Applications
- App Genie
- Paramétrage du Timeline
- Géolocalisation
 - Carving
 - Playback








Regroupement des Applications

Insights from Installed Apps

- | | |
|---|--|
|  Chat applications (6 apps) |  Lifestyle (11 apps) |
|  Browser (5 apps) |  Social networking (5 apps) |
|  Hide files or pictures (1 apps) |  Entertainment (4 apps) |
|  Utilities (32 apps) |  Finance (2 apps) |

[View all](#)

Insights from Installed Apps

- | | |
|---|---|
|  Chat applications (23 apps) |  Social networking (31 apps) |
|  Hide files or pictures (3 apps) |  Developer tools (23 apps) |
|  Browser (2 apps) |  Lifestyle (9 apps) |
|  Secure wipe (1 apps) |  Utilities (7 apps) |

[View all](#)

Et toujours plus

Fuzzy Model

App Genie

BSSID

What is AppGenie?

AppGenie is a research tool that tries to automatically identify specific artifact types from device databases. The AppGenie analyzes databases based on past decoding support, heuristics and can provide additional app data such as Contacts, User accounts and Chats.

As a research tool, the suggested results **do not** replace native PA decoding and should be used as preliminary/triage results for manual review, because it may include false-positives and partial results. It's recommended to review results before including them in your reports.



Database View

Hex View

File Info

Hide

android_metadata

(1) (0)

bookmarks

(15) (0)

clients

(1)

deleted_logins

(0)

favicons

(6)

history

(13) (0)

logins

(0) (0)

logins_disabled_hosts

(0)

metadata

(6) (0)

numbers

(51) (0)

searchhistory

(2) (0)

sqlite_master

(47)

sqlite_sequence

(9)

tabs

(2) (0)

thumbnails

thumbnails (7) (488)

_id

url

data

9

https://support.mozilla.org/en-US/kb/private-browsing-use-firefox-without-history

PNG

8

https://www.google.com/search?q=private+tabs&ie=utf-8&oe=utf-8&client=firefox-b

PNG

7

http://smarterforensics.com/2016/09/a-glimpse-of-ios-10-from-a-smartphone-forensic-perspective/

PNG

6

http://smarterforensics.com/blog/

PNG

5

https://www.google.com/search?q=iphone+says+custom.jailbreak&ie=utf-8&oe=utf-8&client=firefox-b

PNG

4

http://m.mainlinehealth.org/

PNG

4

http://m.mainlinehealth.org/

PNG

2

http://www.google.com/

PNG

1

http://smarterforensics.com/

PNG

1

http://smarterforensics.com/

PNG

0

9[#####+&#####@

J

0

#####E#####Thhttp://m.mainlinehealth.org/

PNG

Trucs et Astuces

- Fuzzy Model
- App Genie
- “GoTo” Feature
- Carving
- Capture Vidéo – Comment l’utiliser ?

Exemple d'utilisation de la capture vidéo

The screenshot displays the UFED Physical Analyzer 7.30.0.206 interface. The top menu bar includes File, View, Tools, Extract, Python, Plug-ins, Report, and Help. The main window is titled 'WhatsApp Chat (9)' and shows a conversation between Karolina and Heather. The chat area includes a 'Participants (2)' section and a 'Conversation' section with a 'Select/Deselect all 9 messages' option. The right-hand pane shows details for an 'Instant Message', including Source, Subject, Timestamp, Status, Extraction, and Source file. The chat messages include text, images, and a video attachment.

UFED Physical Analyzer 7.30.0.206

File View Tools Extract Python Plug-ins Report Help

Send to Analytics

WhatsApp Chat (9)

Conversation View Messages View

Export Filters Actions Enter text to filter ...

Participants (2)

Karolina

Heather

Do you want me to do the voice first? I can do it early next week

2/6/2020 3:44:25 PM(UTC+0)

Sources (2)

Karolina

Yes I prefer it this way. it's easier for me to put the animation and the VO in one process. I will continue to DFU mode for now

2/6/2020 3:46:47 PM(UTC+0)

Sources (1)

Karolina

That means the same as "iTunes screen appears" as in other two videos? Or something else should happen o...

image/jpeg

02990760-c992-4e34-a804-79f545a62855.jpg

https://mmg-fna.whatsapp.net/d/t/AsTcKnFq4UkKSFzEFxVjNGaBQL_IvZBDVcmXmExw.enc

2/11/2020 2:36:10 PM(UTC+0)

Sources (2)

Heather

Yep. Same thing. :)

2/11/2020 3:10:49 PM(UTC+0)

Sources (2)

Instant Message

Translate Go to

Source: WhatsApp

Subject:

Timestamp: 1/29/2020 5:46:57 PM(UTC+0)

Status: Logical (1)

Extraction: Logical (1)

Source file: Heather's iPhone/mobile/Containers/Shared/AppGroup/group.net.whatsapp.WhatsApp.shared/ChatStorage.sqlite : 0xd6E37E (Table: ZWAMESSAGE_ZWAGROUPMEMBER_ZWACHATSESSION_ZWAMEDIAITEM_Size: 13023280 bytes)

Heather's iPhone/mobile/Containers/Shared/AppGroup/group.net.whatsapp.WhatsApp.shared/Message/Media/972546543913@s.whatsapp.net/8/0/8...

From: [redacted] whatsapp.net Karolina

Participants: [redacted] whatsapp.net Karolina [redacted] whatsapp.net Heather (owner)

Attachment: audio/ogg; codecs=opus 80abc02d-cb10-42a5-87bf-b18a06314522.op https://mmg.whatsapp.net/d/t/Am9DIzBenhw_L...

SharedContacts

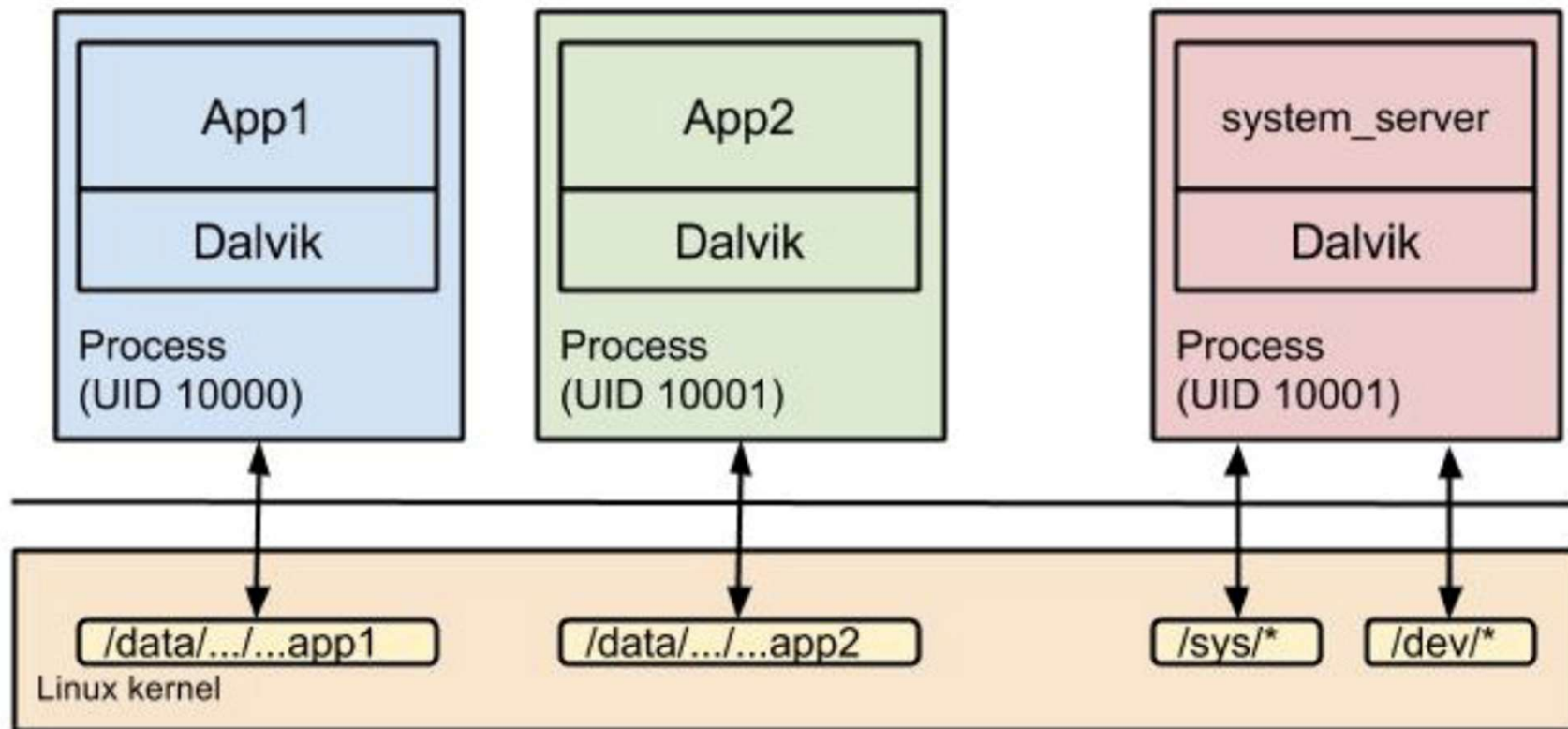
Body

Map

Position:

MALWARE SUR ANDROID

Le modèle de sécurité sous Android



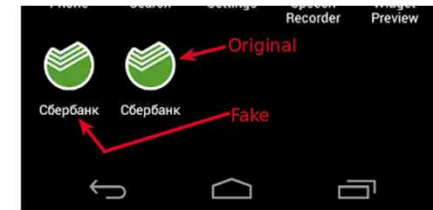
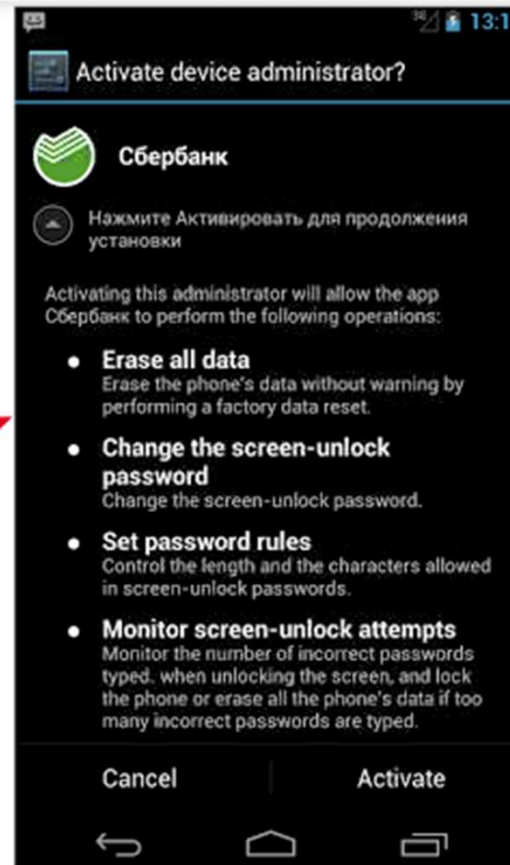
Méthodes analyses de malwares

STATIQUE ET DYNAMIQUE

Quelques outils nécessaires:







- JAD-X: <https://github.com/skylot/jadx>
- Apktool : <https://ibotpeaches.github.io/Apktool/> (décompilation APK)
- Dex2jar : <https://sourceforge.net/projects/dex2jar/>
- Jd-gui (visual interface) : <http://java-decompiler.github.io/>
- Android Studio : <http://developer.android.com/studio>

Effets d'un malware (en utilisant un émulateur)



Fake app and its permissions
Cellebrite

Exemple analyse de malware

Nom	Modifié le	Type	Taille
 assets	08/05/2020 11:52	Dossier de fichiers	
 original	08/05/2020 11:52	Dossier de fichiers	
 res	08/05/2020 11:52	Dossier de fichiers	
 smali	08/05/2020 11:52	Dossier de fichiers	
 AndroidManifest.xml	08/05/2020 11:52	Document XML	6 Ko
 apktool.yml	08/05/2020 11:52	Fichier YML	1 Ko

```
C:\test>apktool krep.itmtd.ywtjexf-1.apk
I: Using Apktool 2.4.1 on krep.itmtd.ywtjexf-1.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: C:\Users\jpnoa\AppData\Local\apktool\framework\1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...

C:\test>
```

Analyse de malware

```
new 1 README AndroidManifest.xml
1 <?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android"
2   <uses-permission android:name="android.permission.INTERNET"/>
3   <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
4   <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
5   <uses-permission android:name="android.permission.READ_SMS"/>
6   <uses-permission android:name="android.permission.SEND_SMS"/>
7   <uses-permission android:name="android.permission.WRITE_SMS"/>
8   <uses-permission android:name="android.permission.READ_CONTACTS"/>
9   <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
10  <uses-permission android:name="android.permission.READ_CALL_LOG"/>
11  <uses-permission android:name="com.android.browser.permission.READ_HISTORY_BOOKMARKS"/>
12  <uses-permission android:name="android.permission.READ_SYNC_SETTINGS"/>
13  <uses-permission android:name="android.permission.READ_CALENDAR"/>
14  <uses-permission android:name="android.permission.READ_LOGS"/>
15  <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
16  <uses-permission android:name="android.permission.READ_PROFILE"/>
17  <uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
18  <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
19  <uses-permission android:name="com.android.alarm.permission.SET_ALARM"/>
20  <uses-permission android:name="android.permission.RECEIVE_SMS"/>
21  <uses-permission android:name="android.permission.READ_SMS"/>
22  <uses-permission android:name="android.permission.SEND_SMS"/>
23  <uses-permission android:name="android.permission.VIBRATE"/>
24  <uses-permission android:name="android.permission.GET_TASKS"/>
25  <uses-permission android:name="android.permission.KILL_BACKGROUND_PROCESSES"/>
26  <uses-permission android:name="android.permission.RESTART_PACKAGES"/>
27  <uses-permission android:name="android.permission.GET_TASKS"/>
28  <uses-permission android:name="android.permission.CALL_PHONE"/>
29  <application android:icon="@drawable/ic_launcher" android:label="C6ep6aHk" android:screenOrientation="portrait" android:theme="@android:
30    <activity android:name="krep.itmtd.ywtjexf.SampleOverlayHideActivity"/>
31    <activity android:name="krep.itmtd.ywtjexf.MasterPage" android:theme="@android:style/Theme.Translucent.NoTitleBar"/>
32    <activity android:name="krep.itmtd.ywtjexf.MasterPage2" android:theme="@android:style/Theme.Translucent.NoTitleBar.Fullscreen"/>
33    <activity android:name="MasterNewTask"/>
34    <service android:name="krep.itmtd.ywtjexf.OverlayService"/>
35    <service android:name="krep.itmtd.ywtjexf.MasterInterceptor"/>
```

jadx-gui - evernote.zip

File View Navigation Tools Help

167a.CameraProxyCrash x com.evernote.android.camera.CameraEvent x

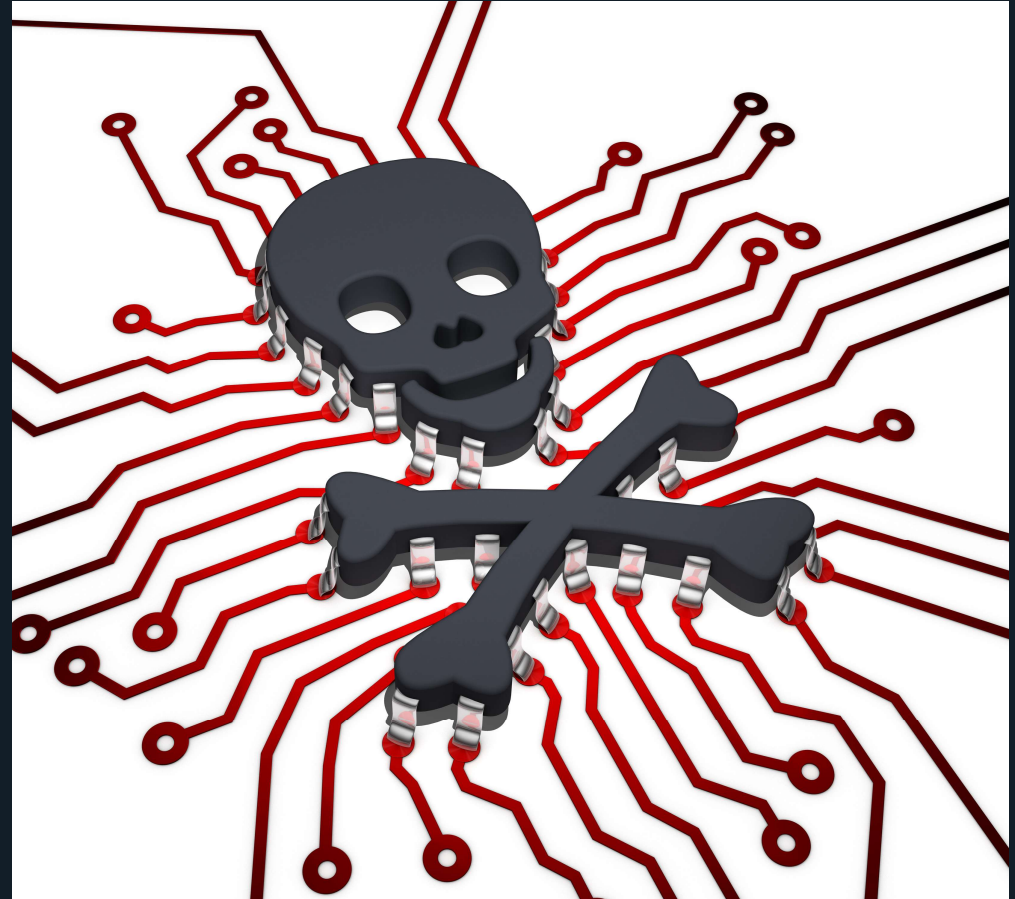
```
renamed from: com.evernote.android.camera.b ?
public class CameraEvent {
    /* renamed from: a ?
    private final C1042a f7114a;
    /* renamed from: b ?
    private final CameraException f7115b;

    /* compiled from: CameraEvent ?
    /* renamed from: com.evernote.android.camera.b$a ?
    public enum C1042a {
        CAMERA_OPENED,
        CAMERA_PREVIEW_STARTED,
        CAMERA_PREVIEW_STOPPED,
        CAMERA_RELEASED,
        CAMERA_AUTO_FOCUS,
        CAMERA_CANCEL_AUTO_FOCUS,
        CAMERA_TAKE_PICTURE,
        CAMERA_CHANGE_SETTINGS,
        CAMERA_ADD_FRAME_CALLBACK,
        CAMERA_REMOVE_FRAME_CALLBACK,
        CAMERA_UNEXPECTED_ERROR,
        CAMERA_EXCEPTION;

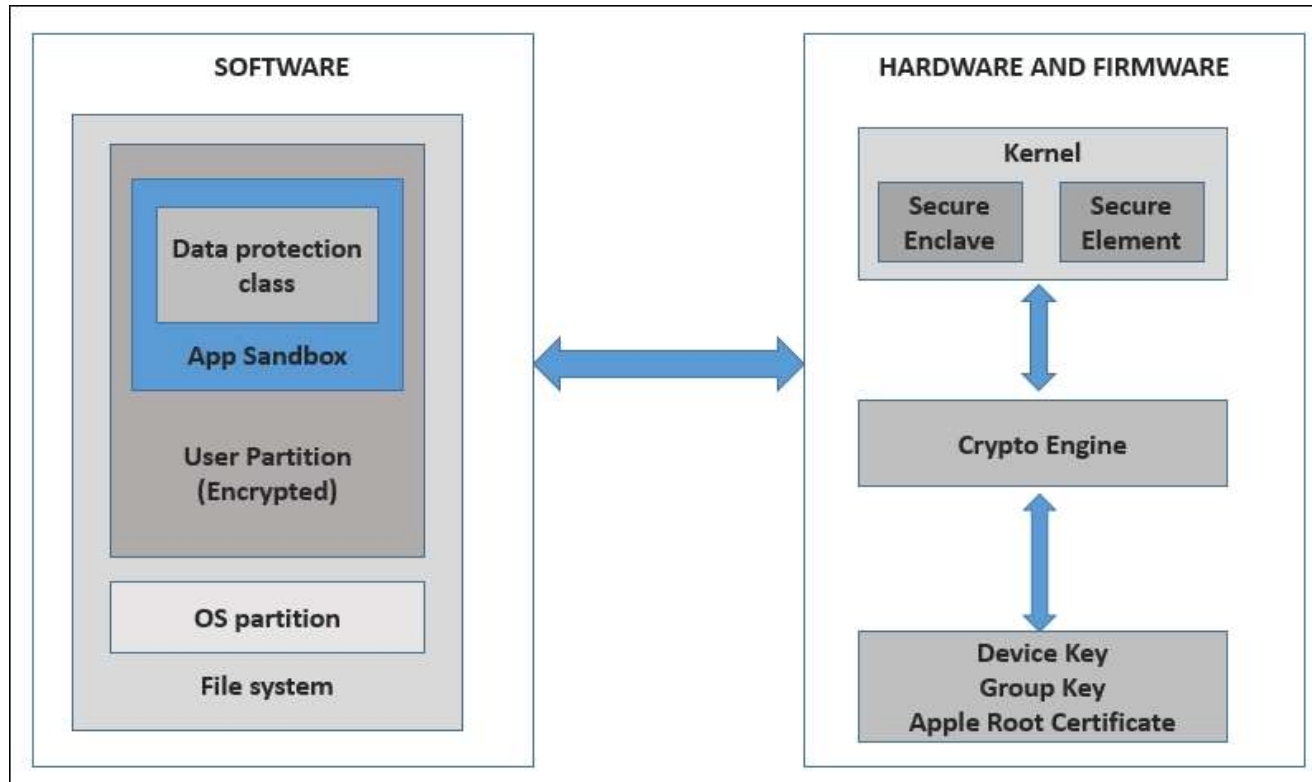
    /* renamed from: a ?
    public final boolean mo6137a() {
        return equals(CAMERA_OPENED) || equals(CAMERA_PREVIEW_STARTED) || equals(CAMERA_UNEXPECTED_ER
    }

    /* compiled from: CameraEvent ?
    /* renamed from: com.evernote.android.camera.b$b ?
    static class C1044b extends CameraEvent {
```

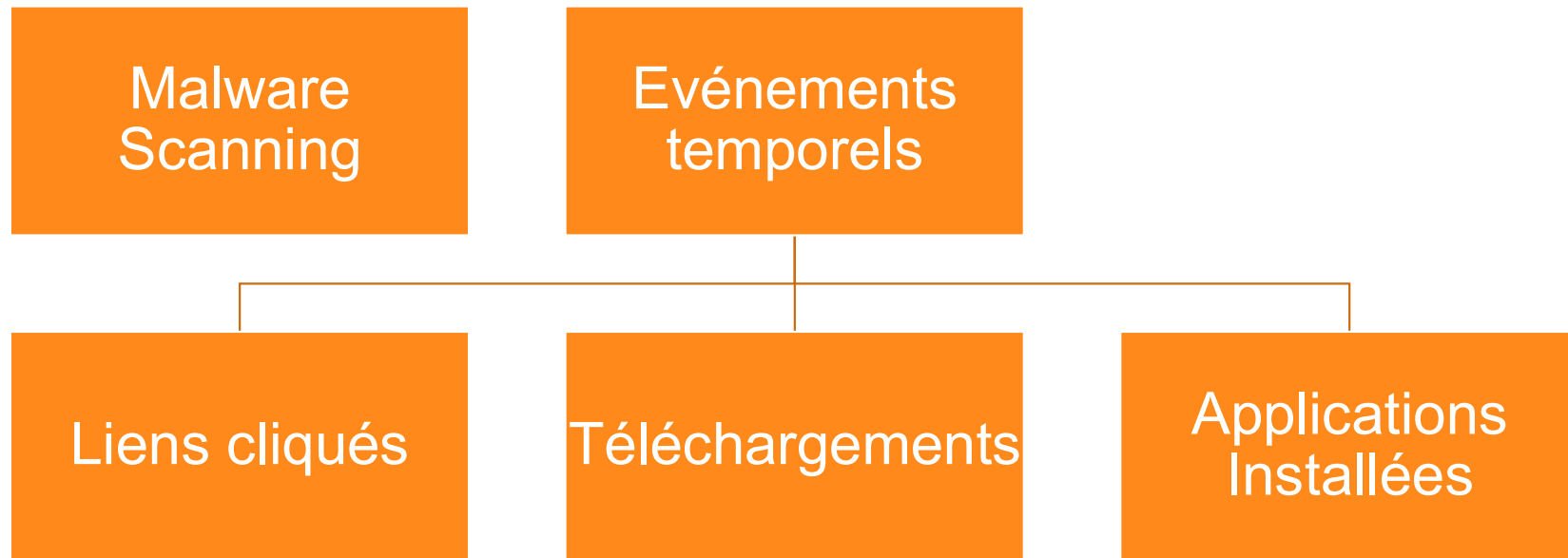
Les malwares sous iOS



Le modèle de sécurité de l'iOS

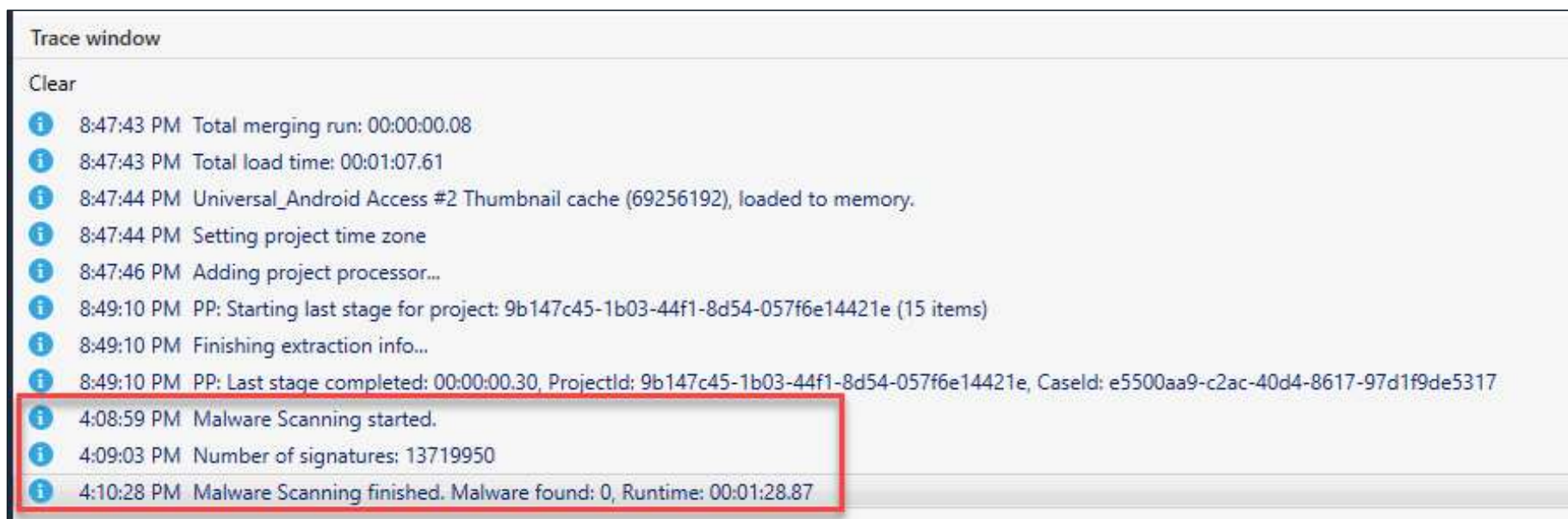


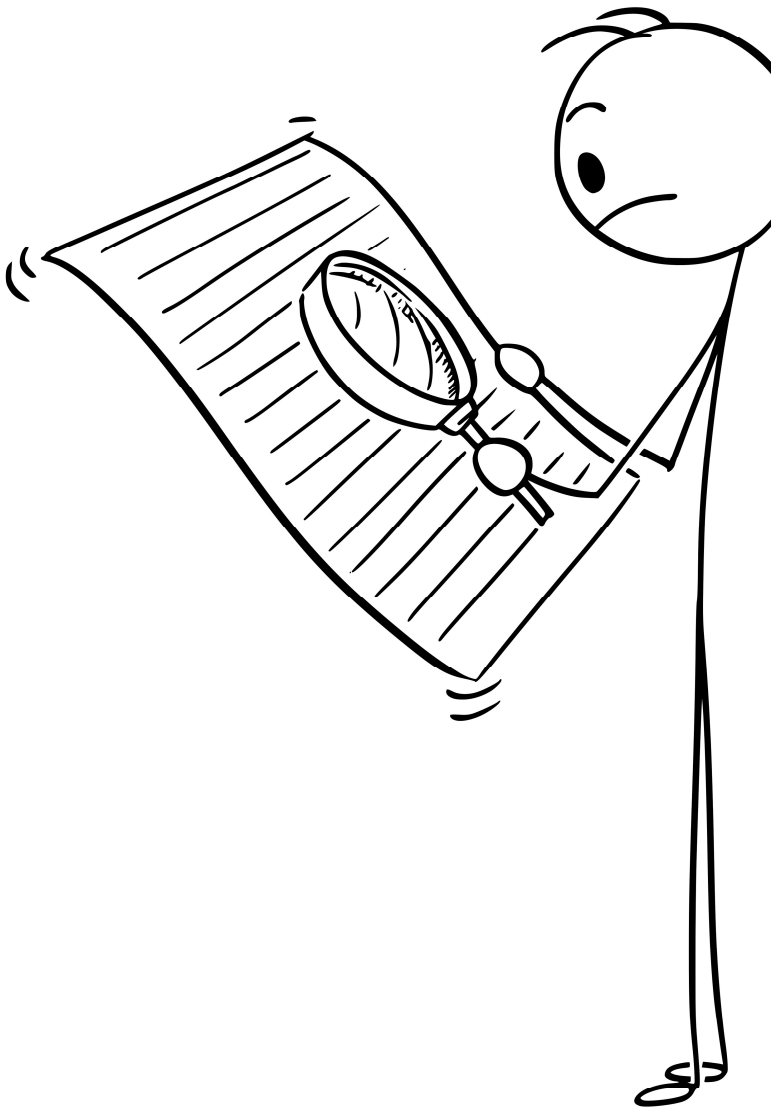
A la chasse aux malwares



Utilisation de la fenêtre de trace

DANS PA ALLER A VUE/VIEW >TRACE WINDOW

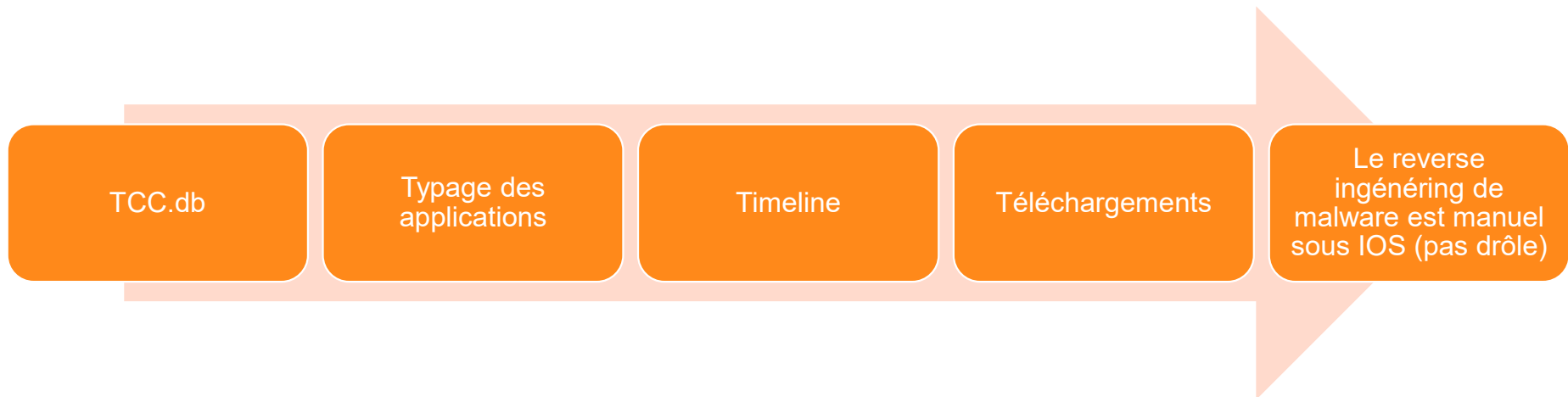




Pas de résultats – PAS VRAIMENT UNE SURPRISE

- Avez-vous vérifié la fenêtre de Trace ?
- Êtes vous sur Android ou iOS ?
- Avez-vous mis à jour vos signatures?
 - Pas commun d'avoir des signatures connues sous iOS
- Quelle version d'iOS avez vous ?
- Quelle type d'acquisition avez-vous ?
- Avez-vous une période precise ?

Etapes suivantes



TCC.db (1)

TCC.db x Learn more x Extraction Summary (1) x TCC.db x Extraction Summary (1) x

Database View Hex View File Info

Hide

access (136)

access (136)

access_overrides (0)

active_policy (0)

active_policy_id (0)

admin (1)

expired (0)

policies (0)

sqlite_master (13)

service	client	client_type	allowed
kTCCServiceAddressBook	org.whispersystems.signal	0	1
kTCCServiceBluetoothAlways	com.fitbit.FitbitMobile	0	1
kTCCServiceBluetoothAlways	com.signify.hue.blue	0	1
kTCCServiceBluetoothAlways	com.hammerandchisel.discord	0	1
kTCCServiceCalendar	us.zoom.videomeetings	0	1
kTCCServiceCamera	net.whatsapp.WhatsApp	0	1
kTCCServiceCamera	com.toyopagroup.picaboo	0	1
kTCCServiceCamera	com.facebook.Messenger	0	1
kTCCServiceCamera	com.skype.skype	0	1
kTCCServiceCamera	com.skout.SKOUT	0	1
kTCCServiceCamera	com.mywicks.wicks	0	1
kTCCServiceCamera	com.tinginteractive.usms	0	1
kTCCServiceCamera	com.herzick.houseparty	0	1
kTCCServiceCamera	com.viber	0	1
kTCCServiceCamera	com.zhiliaoapp.musically	0	1
kTCCServiceCamera	com.weareza.zclient.ios	0	1
kTCCServiceCamera	com.mentionmobile.cyberdust	0	1
kTCCServiceCamera	jp.naver.line	0	1
kTCCServiceCamera	co.babypenguin.imo	0	1
kTCCServiceCamera	com.coverme.covermeAdhoc	0	1
kTCCServiceCamera	org.whispersystems.signal	0	1
kTCCServiceCamera	com.burbn.threads	0	1
kTCCServiceCamera	com.mewe	0	1
kTCCServiceCamera	ph.telegra.Telegraph	0	1
kTCCServiceCamera	com.burbn.instagram	0	1
kTCCServiceCamera	us.zoom.videomeetings	0	1
kTCCServiceLiverpool	com.apple.TrustedPeersHelper	0	1
kTCCServiceLiverpool	com.apple.mobilenotes	0	1
kTCCServiceLiverpool	com.apple.mobilesafari	0	1
kTCCServiceLiverpool	com.apple.stocks	0	1
kTCCServiceLiverpool	com.apple.newsdaemon	0	1
kTCCServiceLiverpool	com.apple.VoiceShortcuts	0	1
kTCCServiceLiverpool	ph.telegra.Telegraph	0	1
kTCCServiceLiverpool	com.apple.Maps	0	1
kTCCServiceLiverpool	com.apple.news	0	1
kTCCServiceLiverpool	com.apple.iCloudNotification	0	1
kTCCServiceMicrophone	org.whispersystems.signal	0	1
kTCCServiceMicrophone	co.babypenguin.imo	0	1
kTCCServiceMicrophone	com.burbn.threads	0	1
kTCCServiceMicrophone	com.coverme.covermeAdhoc	0	1

TCC.db (2)

TCC.db x

Learn more

Extraction Summary (1) x

TCC.db x

Extraction Summary (1) x

Database View

Hex View

File Info

Hide

access (136)

access_overrides (0)

active_policy (0)

active_policy_id (0)

admin (1)

expired (0)

policies (0)

sqlite_master (13)

access (136)

service	client	client_type	allowed
kTCCServiceMicrophone	co.babypenguin.imo	0	1
kTCCServiceMicrophone	com.burbn.threads	0	1
kTCCServiceMicrophone	com.coverme.covermeAdhoc	0	1
kTCCServiceMicrophone	jp.naver.line	0	1
kTCCServiceMicrophone	com.silenticircle.SilentPhone	0	1
kTCCServiceMicrophone	com.viber	0	1
kTCCServiceMicrophone	ph.telegra.Telegraph	0	1
kTCCServiceMicrophone	com.burbn.instagram	0	1
kTCCServiceMicrophone	com.toyopagroup.picaboo	0	1
kTCCServiceMicrophone	net.whatsapp.WhatsApp	0	1
kTCCServiceMicrophone	com.mywickr.wickr	0	1
kTCCServiceMicrophone	com.wearezeta.zclient.ios	0	1
kTCCServiceMicrophone	com.skype.skype	0	1
kTCCServiceMicrophone	com.facebook.Messenger	0	1
kTCCServiceMicrophone	com.mewe	0	1
kTCCServiceMicrophone	com.skout.SKOUT	0	1
kTCCServiceMicrophone	com.tinginteractive.usms	0	1
kTCCServiceMicrophone	com.hammerandchisel.discord	0	1
kTCCServiceMicrophone	com.herzick.houseparty	0	1
kTCCServiceMicrophone	us.zoom.videomeetings	0	1
kTCCServiceMicrophone	com.zhiliaoapp.musically	0	1
kTCCServiceMotion	com.apple.Health	0	1
kTCCServicePhotos	com.atebits.Tweetie2	0	1
kTCCServicePhotos	de.tutao.tutanota	0	1
kTCCServicePhotos	com.tinginteractive.usms	0	1
kTCCServicePhotos	com.viber	0	1
kTCCServicePhotos	com.burbn.threads	0	1
kTCCServicePhotos	ch.protonmail.protonmail	0	1
kTCCServicePhotos	com.silenticircle.SilentPhone	0	1
kTCCServicePhotos	net.whatsapp.WhatsApp	0	1
kTCCServicePhotos	com.wearezeta.zclient.ios	0	1
kTCCServicePhotos	com.coverme.covermeAdhoc	0	1
kTCCServicePhotos	com.skout.SKOUT	0	1
kTCCServicePhotos	com.toyopagroup.picaboo	0	1
kTCCServicePhotos	us.zoom.videomeetings	0	1
kTCCServicePhotos	ph.telegra.Telegraph	0	1
kTCCServicePhotos	org.whispersystems.signal	0	1
kTCCServicePhotos	imgurmobile	0	1
kTCCServicePhotos	co.babypenguin.imo	0	1
kTCCServicePhotos	com.burbn.instagram	0	1

La chasse continue

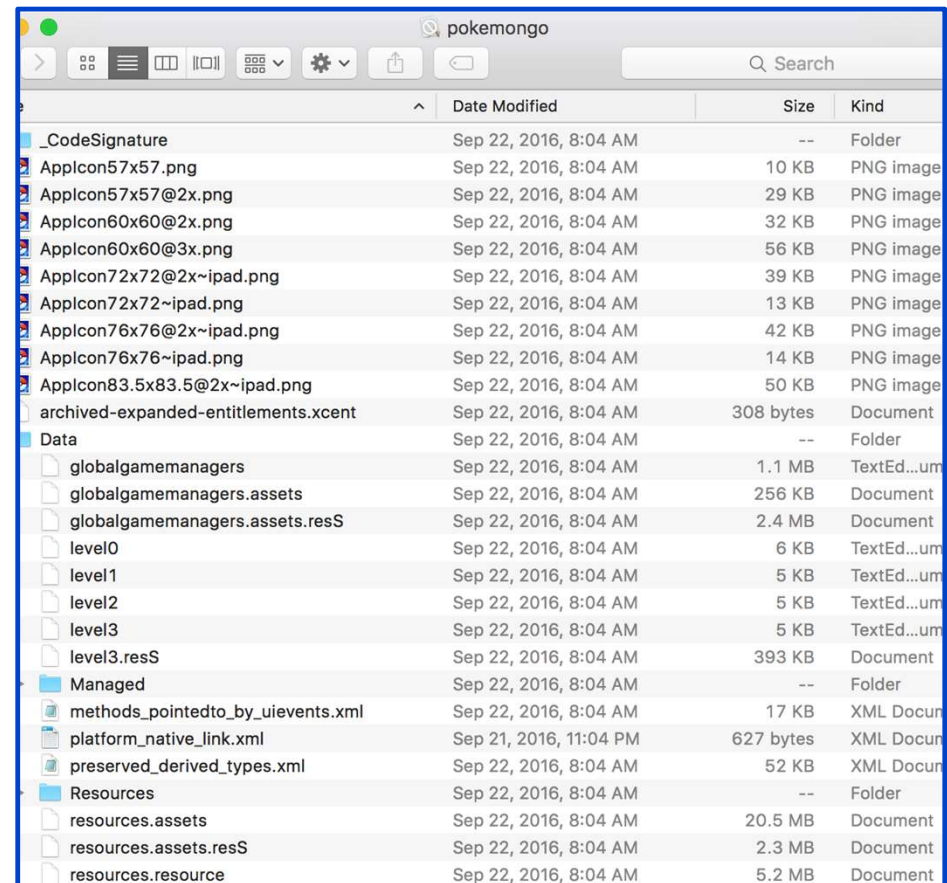
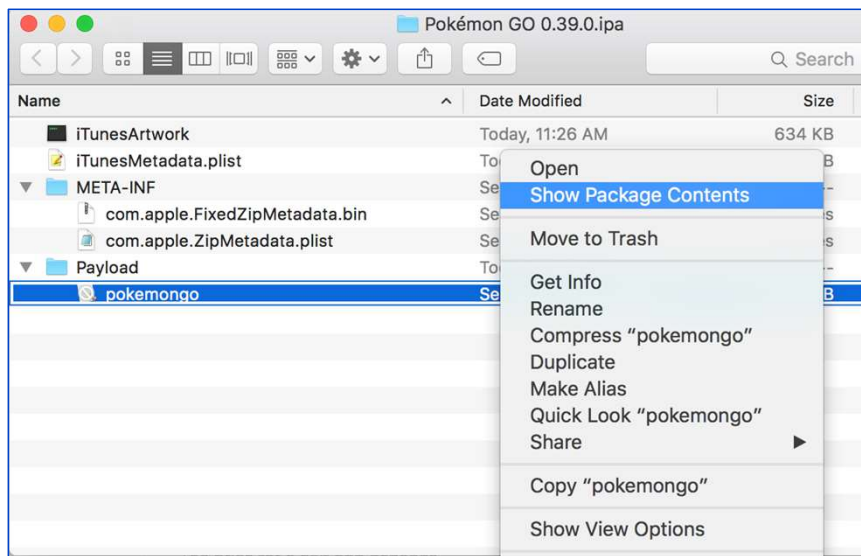
Timeline

Téléchargements

Browser et liens

Etudier toute trace

Analyse de malware



Références

SANS : www.for585.com/course and poster for585.com/poster

Practical Mobile Forensics: Heather Mahalik, Rohit Tamma 2nd Edition - for585.com/books (free copy for you of the 2nd edition)

Use the same images I showed in the webinar

- <https://thebinaryhick.blog/2020/02/15/android-10-image-now-available/>
- https://drive.google.com/file/d/1GQP_y1340LHcq8eiDOYKAma62Q8GEyN5/view?usp=sharing

La semaine prochaine...

Analyse du Timeline sous Windows 10

Prenez soin de vous et de ceux que vous aimez



La parole est à vous !