ZAPiXWEB 1.5

Author: alberto.magno@gmail.com (https://github.com/kraftdenker)

Implementation of technique described in paper:
Soares, A. (2022). WhatsApp Web Client Live Forensics Technique. In Proceedings of the 8th International Conference on Information Systems Security and Privacy - ICISSP, ISBN 978-989-758-553-1, pages 629-636. DOI: 10.5220/0011006400003120
https://doi.org/10.5220/0011006400003120

ZAPiXWEB WhatsApp Extractor - 4 CHROME (TESTED), FIREFOX (TESTED), EDGE (TESTED), OPERA (It also works offline)

Goal

Describe the use of the ZAPiXWEB tool for extracting conversations from the WhatsApp Web messaging service and for importing the extracted data in the Cellebrite UFED Physical Analyser analysis application.

Motivation

During the activity of expertise in locations, often the expert is stun with a computer connected with section of the WhatsApp message service in operation in a web browser. The ZAPiXWEB tool features a *javascript* script to run in the browser to extract active conversations, even working if the computer is disconnected from the internet.

Features

It is a *javascript-based tool that* should be run in the web browser command console, accessible through development mode. For each browser, you must seek the activation of the developer mode and paste the script that will take action immediately after pressing the <enter>. The script is designed to work on all standard ECMAScript version 6 browsers as the most current versions of chrome, firefox, edge, opera and safari browsers. The script has been successfully tested in the first three, but still requires adaptations for use in the Safari browser. The extracted textual data is packaged by the script itself into a single ZIP file, including all attachments. Due to the large volume of possible conversation data, and often the large volume of attachments and the time required to download, the script does not extract all possible conversations, so if you focus on any specific conversation, you should navigate the specific conversation (through the respective scroll bar of the conversation) to where you are interested in copying the data.

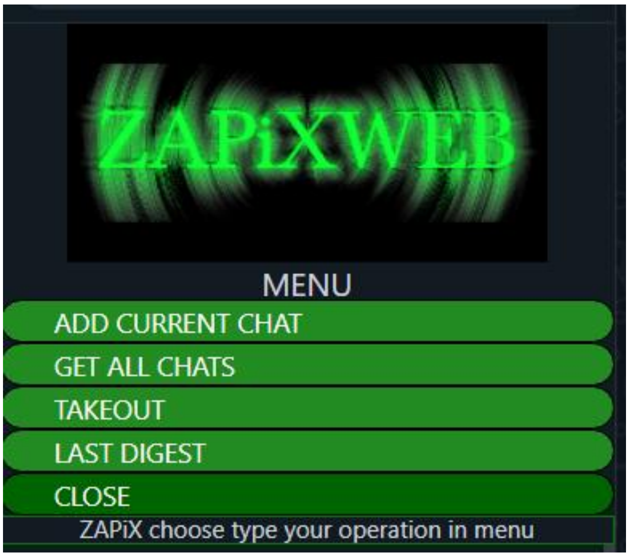
Use

Extraction

Windows Operating System

For use in the Windows operating system, you must first identify the browser with the WhatsApp Web window open, then you must scroll through the conversations of greatest interest "going up" with the scroll bar until the date of interest. Next, you must activate the developer mode, which usually takes place via the F12 hotkey. In the location where ZAPiXWEB script is stored, you should run the script "ZAPiXWEB_WIN. bat", which will automatically place the ZAPiXWEB code on the clipboard. In the browser, you must copy the script to the console and press <ENTER> to the beginning of the extract. Then wait for the script to start (it may take a few seconds). For the Firefox browser it is necessary to run a specific command to release the collage of the script in the console.

The commands available for extraction are:



ZAPiX choose type your operation in menu

`Add current chat`

(for extracting messages from an open chat – can be used more than one time)

`Get all chats`

(for extracting all chats)

`Takeout`

(to package what was extracted to ZIP file)

`Last Digest`

(to show last calculated digest)

Linux Operating System (under test)
For use in the Linux operating system, you must first identify the browser with the WhatsApp Web window open, and then you must scroll through the conversations of greatest interest "going up" with the scroll bar until the date of interest. Next, you must activate the developer mode, which usually takes place via the F12 hotkey. In the location where ZAPiXWEB script is stored, you should run the "ZAPiXWEB_LINUX. sh", which will automatically place the ZAPiXWEB code on the clipboard. In the browser, you must copy the script to the console and press <ENTER> to the beginning of the extract. Follow the same instructions presented to windows operations.

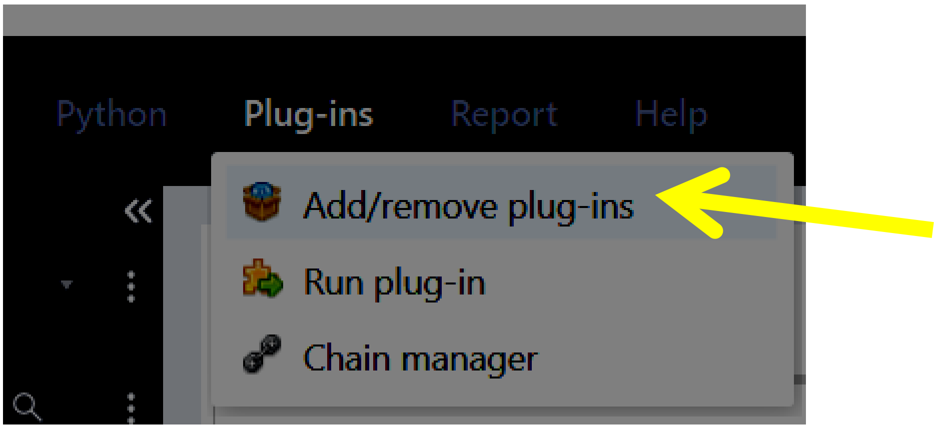
MacOS Operating System (not yet working for safari browser)
For use in the Windows operating system, you must first identify the browser with the WhatsApp Web window open, and then you must scroll through the conversations of greatest interest "going up" with the scroll bar until the date of interest. Next, you must activate the developer mode, which usually takes place via the F12 hotkey. In the location where ZAPiXWEB script is stored, you must run the "ZAPiXWEB_iOS.sh" script, which will

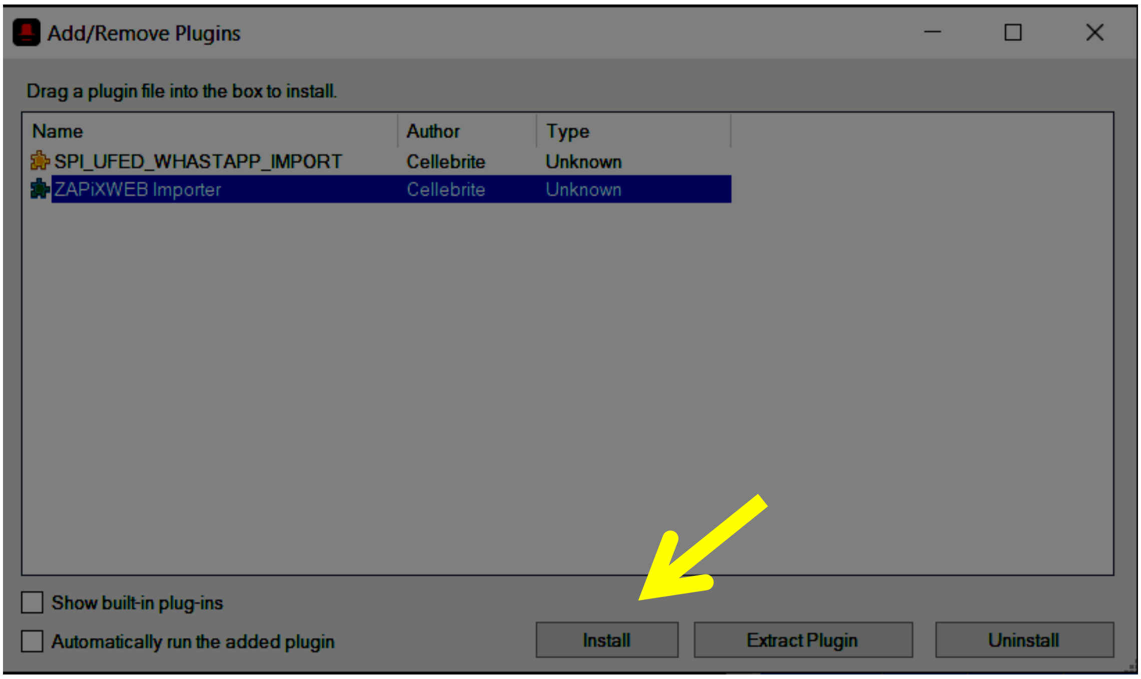
automatically place the ZAPiXWEB code on the clipboard. In the browser, you must copy the script to the console and press <ENTER> to the beginning of the extract. . Follow the same instructions presented to windows operations.

Importing

Cellebrite UFED Physical Analyser

PLUGIN instalation




Add/Remove Plugins

Drag a plugin file into the box to install.

Name	Author	Type
SPI_UFED_WHASTAPP_IMPORT	Cellebrite	Unknown
ZAPiXWEB Importer	Cellebrite	Unknown

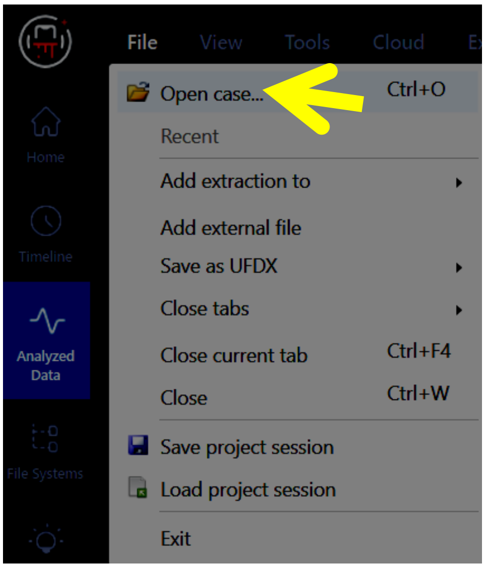
□ Show built-in plug-ins

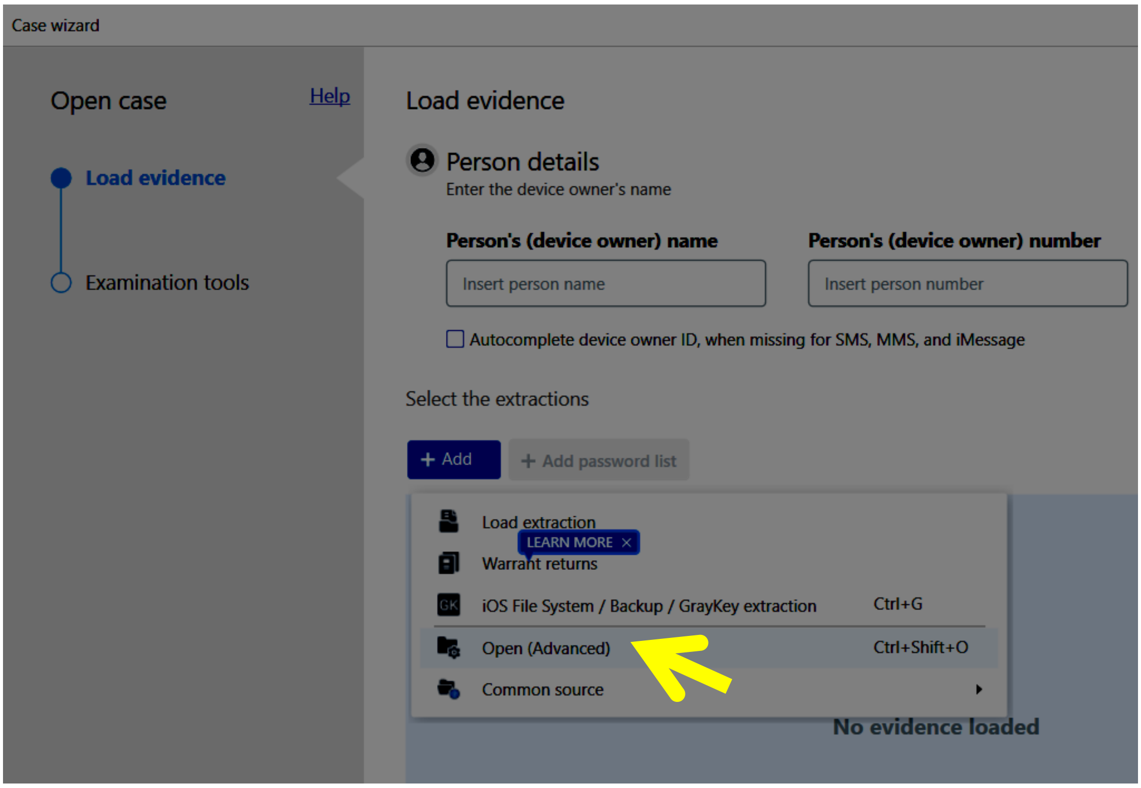
□ Automatically run the added plugin

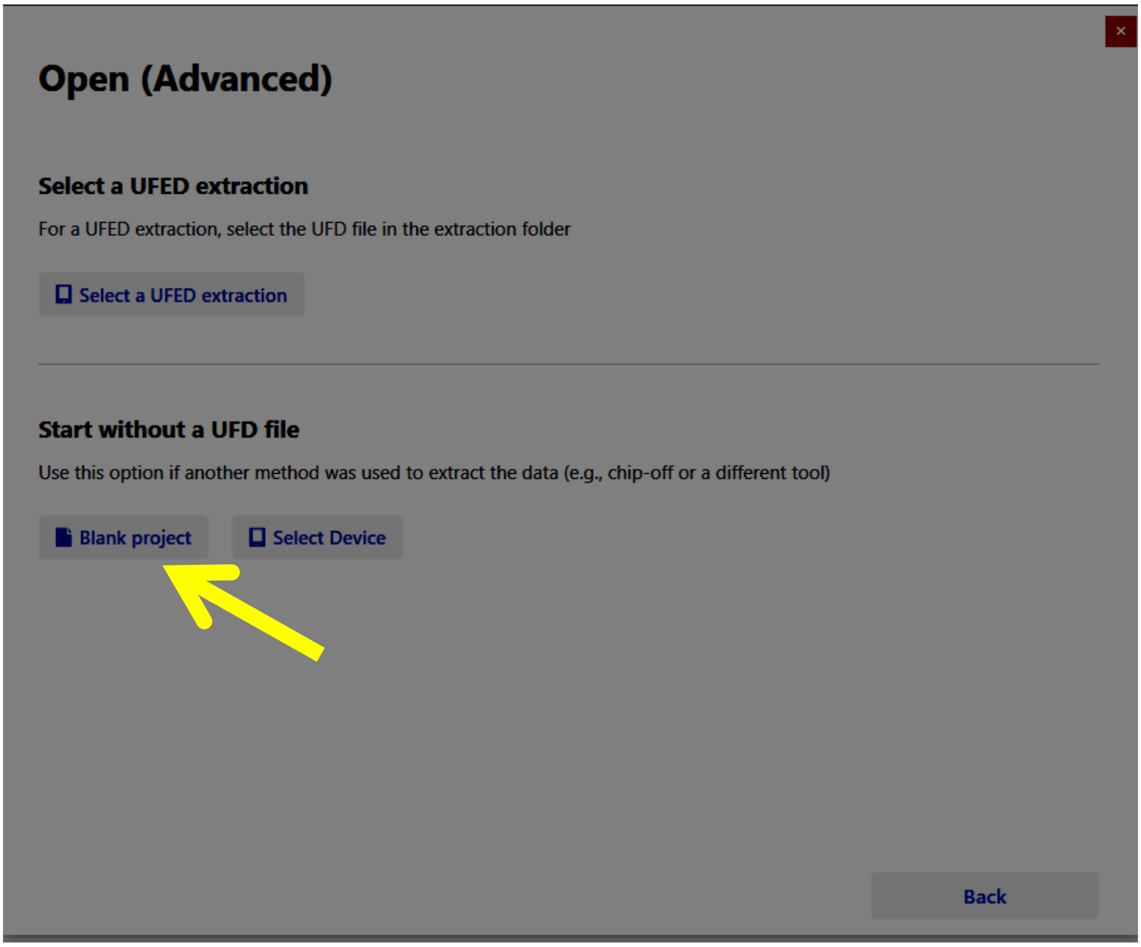
In installation process, "simplejson" directory must be in the same directory of the plugin's file.

Using plugin

Create or add a blank Project and import the zip file generated by ZAPiXWEB.


File
View
Tools
Cloud
Home
Timeline
Analyzed Data
File Systems
Open case... Ctrl+O
Recent
Add extraction to
Add external file
Save as UFDX
Close tabs
Close current tab Ctrl+F4
Close Ctrl+W
Save project session
Load project session
Exit


Case wizard
Open case
Help
Load evidence
Examination tools
Load evidence
Person details
Enter the device owner's name
Person's (device owner) name
Person's (device owner) number
Insert person name
Insert person number
□ Autocomplete device owner ID, when missing for SMS, MMS, and iMessage
Select the extractions
+ Add
+ Add password list
Load extraction
LEARN MORE ×
Warrant returns
iOS File System / Backup / GrayKey extraction Ctrl+G
Open (Advanced) Ctrl+Shift+O
Common source
No evidence loaded



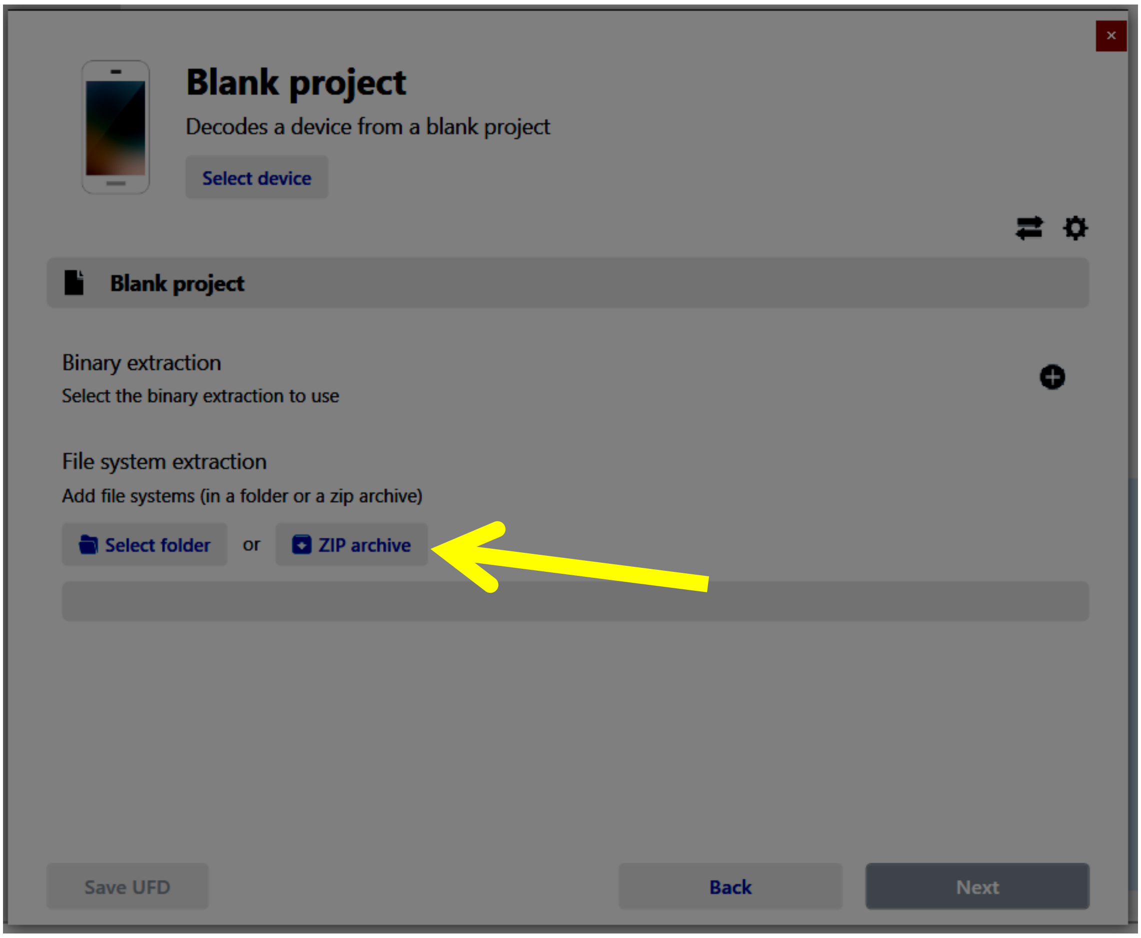
Open (Advanced)

Select a UFED extraction

For a UFED extraction, select the UFD file in the extraction folder

Start without a UFD file

Use this option if another method was used to extract the data (e.g., chip-off or a different tool)



Blank project

Decodes a device from a blank project

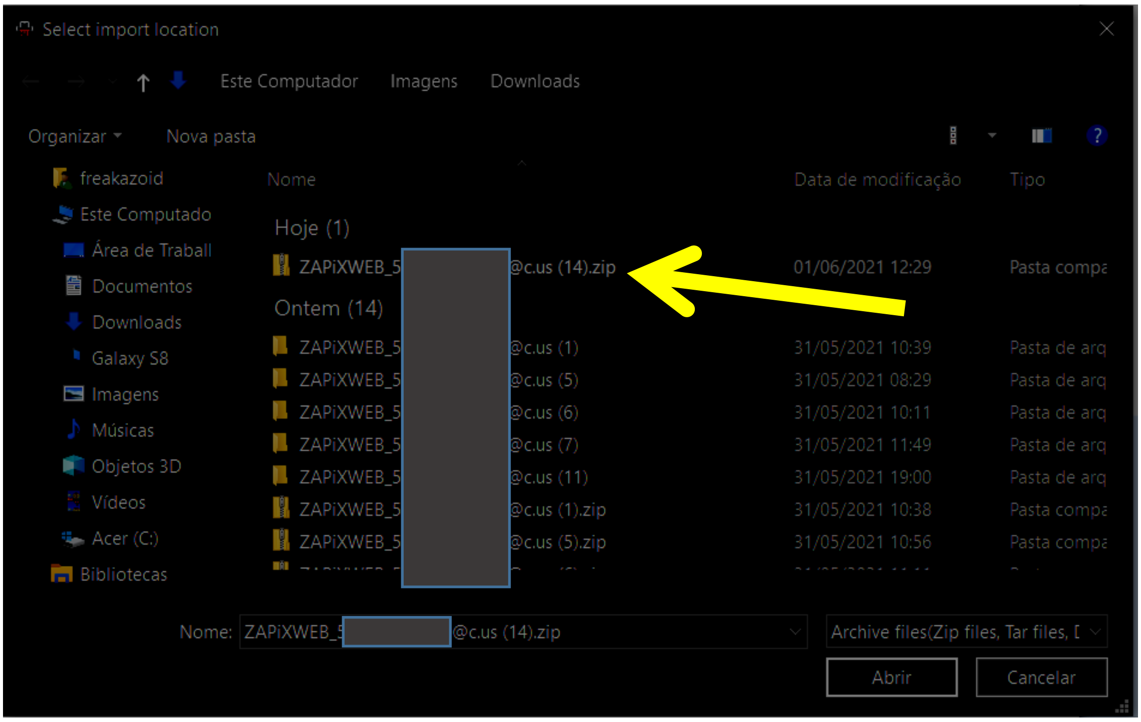
Blank project

Binary extraction

Select the binary extraction to use

File system extraction

Add file systems (in a folder or a zip archive)



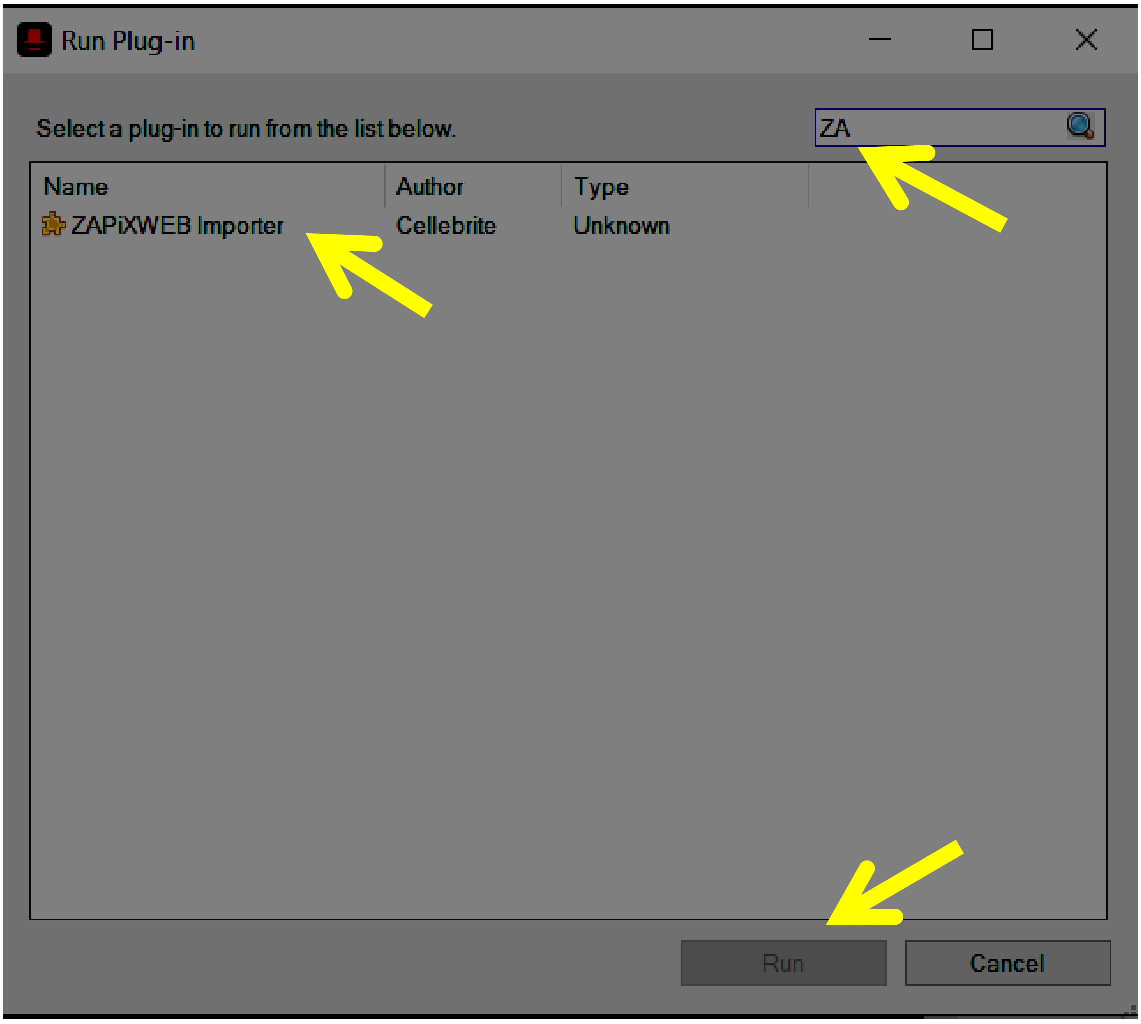
Select import location

Este Computador › Imagens › Downloads

Nome	Data de modificação	Tipo
Hoje (1)		
ZAPiXWEB_5[redacted]@c.us (14).zip	01/06/2021 12:29	Pasta compa
Ontem (14)		
ZAPiXWEB_5[redacted]@c.us (1)	31/05/2021 10:39	Pasta de arq
ZAPiXWEB_5[redacted]@c.us (5)	31/05/2021 08:29	Pasta de arq
ZAPiXWEB_5[redacted]@c.us (6)	31/05/2021 10:11	Pasta de arq
ZAPiXWEB_5[redacted]@c.us (7)	31/05/2021 11:49	Pasta de arq
ZAPiXWEB_5[redacted]@c.us (11)	31/05/2021 19:00	Pasta de arq
ZAPiXWEB_5[redacted]@c.us (1).zip	31/05/2021 10:38	Pasta compa
ZAPiXWEB_5[redacted]@c.us (5).zip	31/05/2021 10:56	Pasta compa

Nome: ZAPiXWEB_5[redacted]@c.us (14).zip

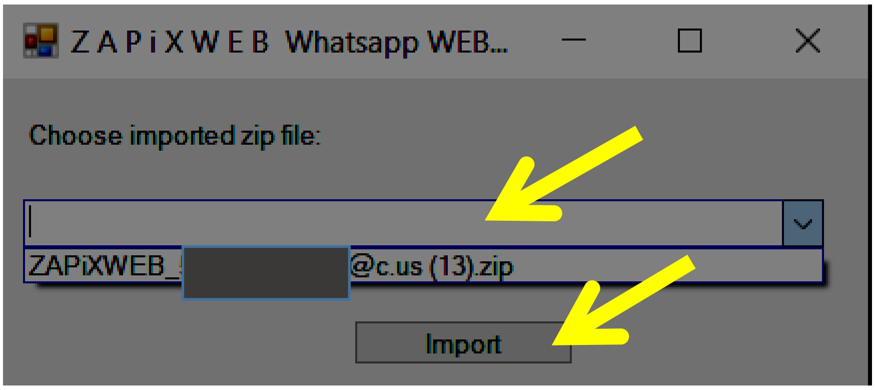
Archive files(Zip files, Tar files, [



Select a plug-in to run from the list below.

ZA

Name	Author	Type
ZAPiXWEB Importer	Cellebrite	Unknown



Choose imported zip file:

ZAPiXWEB_[redacted]@c.us (13).zip

Run the UFED plugin and select the imported ZIP file as the data source.

WARNING: Due to the use of window system, the appearance of the window for selecting the file .zip may take a few seconds. In case of error, close the window for unlocking the interface and reading the errors in the trace window.

Meta changes API frequently, so this code needs constant revisions.