

## ALEAPP GUIDED EXERCISE

Video walkthrough available on the Tool Walkthrough Playlist at <https://youtube.com/@hexordia>

Prior to going through this process please see the walkthrough on Python and pip updates.

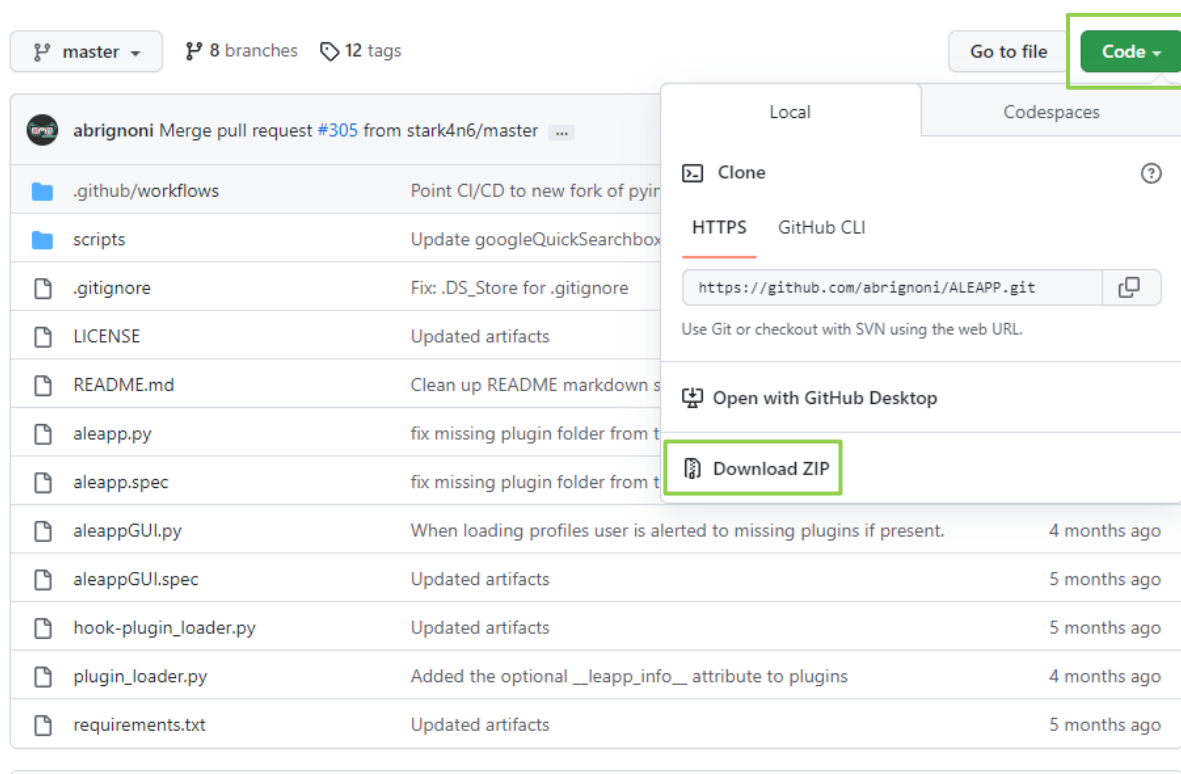
To get started, please download ALEAPP from <https://github.com/abrignoni/ALEAPP>

Prior to installation, verify the hash value to the known good from the syllabus for students enrolled in the HMFA Virtual Live course. The MD5 hash value for the ALEAPP-main.zip version 3.1.6 is eed3be30230346ed3271f0a6e8b06e58.

\*\*If you already have ALEAPP Installed, please move on to [Set Up and Use](#).















### INSTALLATION

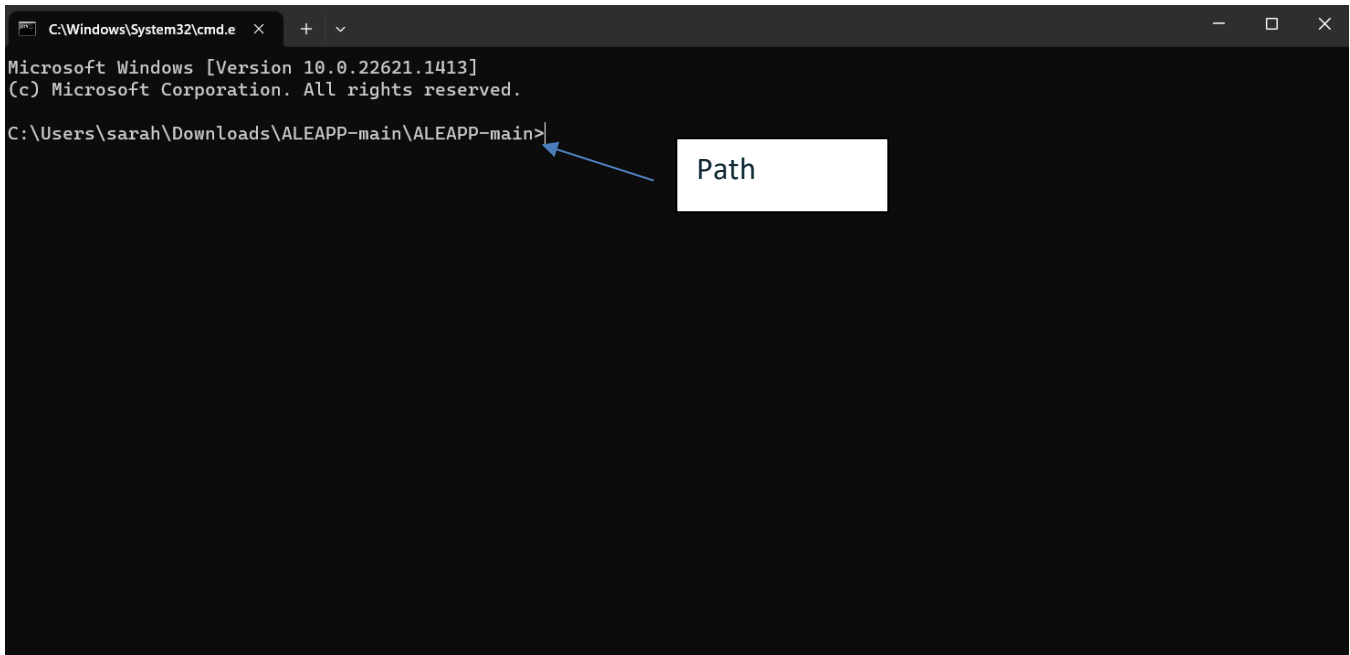
Once on the GitHub page, click “Code” and then “download zip”.



In the downloaded file, type “CMD” in the toolbar and this will pull up the command prompt.

oads > ALEAPP-main > ALEAPP-main

Name	Date modified	Type	Size
▼ Today			
 .gitignore	3/30/2023 10:34 AM	GITIGNORE File	2 KB
 aleapp.py	3/30/2023 10:34 AM	Python File	9 KB
 aleapp.spec	3/30/2023 10:34 AM	SPEC File	2 KB
 aleappGUI.py	3/30/2023 10:34 AM	Python File	13 KB
 aleappGUI.spec	3/30/2023 10:34 AM	SPEC File	2 KB
 hook-plugin_loader.py	3/30/2023 10:34 AM	Python File	1 KB
 LICENSE	3/30/2023 10:34 AM	XMLSpy.	2 KB
 plugin_loader.py	3/30/2023 10:34 AM	Python File	3 KB
 README.md	3/30/2023 10:34 AM	MD File	5 KB
 requirements.txt	3/30/2023 10:34 AM	Text Document	1 KB
 zCaseDataExample.alprofile	3/30/2023 10:34 AM	ALPROFILE File	1 KB
 __pycache__	3/30/2023 10:35 AM	File folder	
 scripts	3/30/2023 10:35 AM	File folder	
 .github	3/30/2023 10:33 AM	File folder	



```
C:\Windows\System32\cmd.e x + v
Microsoft Windows [Version 10.0.22621.1413]
(c) Microsoft Corporation. All rights reserved.
C:\Users\sarah\Downloads\ALEAPP-main\ALEAPP-main>
```

A blue arrow points from the text "Path" in a white box to the current directory path in the command prompt.



Follow the requirements and dependencies section. Follow whichever direction for the Operating system used.

## Requirements

Python 3.9 or above (older versions of 3.x will also work with the exception of one or two modules)

## Dependencies

Dependencies for your python environment are listed in `requirements.txt`. Install them using the below command. Ensure the `py` part is correct for your environment, eg `py`, `python`, or `python3`, etc.

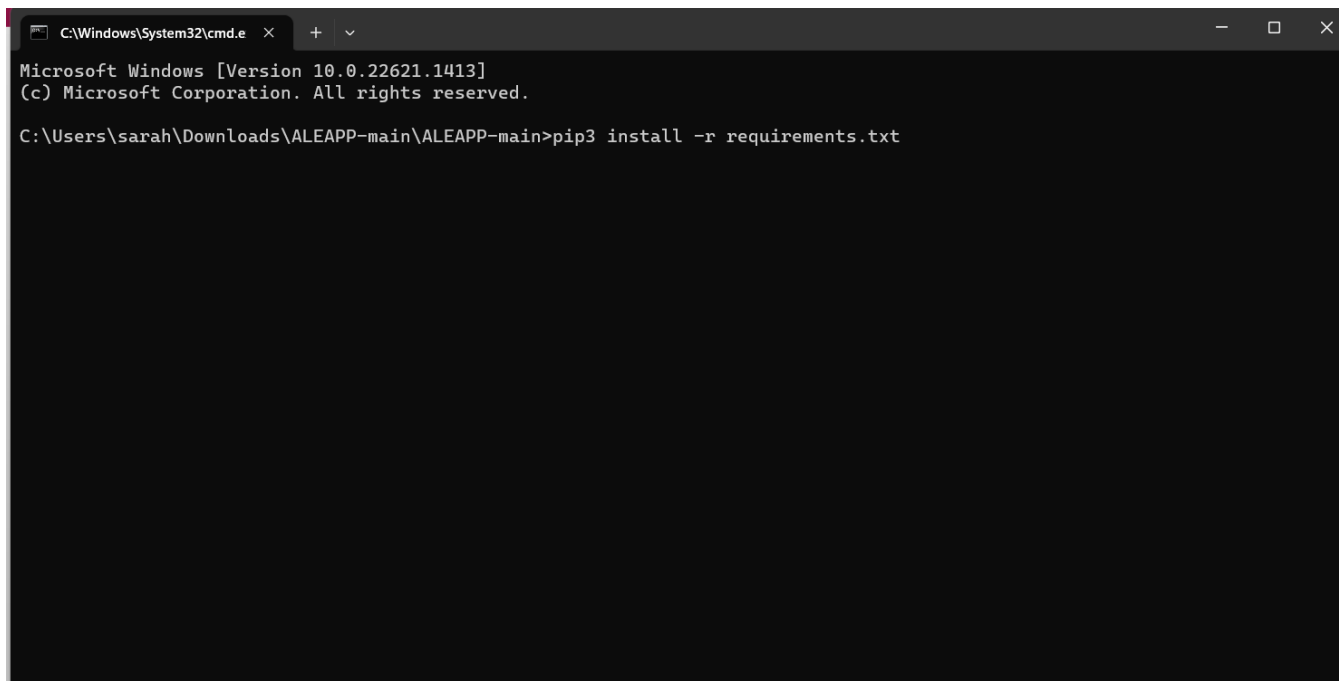
```
py -m pip install -r requirements.txt  
or  
pip3 install -r requirements.txt
```

To run on **Linux**, you will also need to install `tkinter` separately like so:

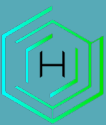
```
sudo apt-get install python3-tk
```

To install dependencies offline Troy Schnack has a neat process here:  
<https://twitter.com/TroySchnack/status/1266085323651444736?s=19>

CMD with windows command.

A screenshot of a Windows Command Prompt window. The title bar shows 'C:\Windows\System32\cmd.e'. The window content displays the following text: 'Microsoft Windows [Version 10.0.22621.1413] (c) Microsoft Corporation. All rights reserved. C:\Users\sarah\Downloads\ALEAPP-main\ALEAPP-main>pip3 install -r requirements.txt'. The prompt is at the end of the line, indicating the command has been entered but not yet executed.

```
C:\Windows\System32\cmd.e  
Microsoft Windows [Version 10.0.22621.1413]  
(c) Microsoft Corporation. All rights reserved.  
C:\Users\sarah\Downloads\ALEAPP-main\ALEAPP-main>pip3 install -r requirements.txt
```



## Results post pip3 install -r requirement.txt

```
C:\Windows\System32\cmd.e x + v
Requirement already satisfied: six>=1.4.1 in c:\users\sarah\appdata\local\programs\python\python311\lib\site-packages (f
rom bcrypt==3.2.0->-r requirements.txt (line 1)) (1.16.0)
Requirement already satisfied: soupsieve>=1.2 in c:\users\sarah\appdata\local\programs\python\python311\lib\site-packag
es (from beautifulsoup4==4.8.2->-r requirements.txt (line 2)) (2.4)
Requirement already satisfied: pyparsing>=2.0.2 in c:\users\sarah\appdata\local\programs\python\python311\lib\site-packa
ges (from packaging==20.1->-r requirements.txt (line 4)) (3.0.9)
Requirement already satisfied: setuptools in c:\users\sarah\appdata\local\programs\python\python311\lib\site-packages (f
rom protobuf==3.10.0->-r requirements.txt (line 5)) (65.5.0)
Requirement already satisfied: branca>=0.6.0 in c:\users\sarah\appdata\local\programs\python\python311\lib\site-packages
 (from folium==0.14.0->-r requirements.txt (line 17)) (0.6.0)
Requirement already satisfied: Jinja2>=2.9 in c:\users\sarah\appdata\local\programs\python\python311\lib\site-packages (
from folium==0.14.0->-r requirements.txt (line 17)) (3.1.2)
Requirement already satisfied: numpy in c:\users\sarah\appdata\local\programs\python\python311\lib\site-packages (from f
olium==0.14.0->-r requirements.txt (line 17)) (1.24.2)
Requirement already satisfied: requests in c:\users\sarah\appdata\local\programs\python\python311\lib\site-packages (fro
m folium==0.14.0->-r requirements.txt (line 17)) (2.28.2)
Requirement already satisfied: pycparser in c:\users\sarah\appdata\local\programs\python\python311\lib\site-packages (fr
om cffi>=1.1->bcrypt==3.2.0->-r requirements.txt (line 1)) (2.21)
Requirement already satisfied: MarkupSafe>=2.0 in c:\users\sarah\appdata\local\programs\python\python311\lib\site-packag
es (from Jinja2>=2.9->folium==0.14.0->-r requirements.txt (line 17)) (2.1.2)
Requirement already satisfied: charset-normalizer<4,>=2 in c:\users\sarah\appdata\local\programs\python\python311\lib\si
te-packages (from requests->folium==0.14.0->-r requirements.txt (line 17)) (3.1.0)
Requirement already satisfied: idna<4,>=2.5 in c:\users\sarah\appdata\local\programs\python\python311\lib\site-packages
 (from requests->folium==0.14.0->-r requirements.txt (line 17)) (3.4)
Requirement already satisfied: urllib3<1.27,>=1.21.1 in c:\users\sarah\appdata\local\programs\python\python311\lib\site-
packages (from requests->folium==0.14.0->-r requirements.txt (line 17)) (1.26.15)
Requirement already satisfied: certifi>=2017.4.17 in c:\users\sarah\appdata\local\programs\python\python311\lib\site-pac
kages (from requests->folium==0.14.0->-r requirements.txt (line 17)) (2022.12.7)

C:\Users\sarah\Downloads\ALEAPP-main\ALEAPP-main>
```



Next, select CLI command or GUI command based on the OS in use.

## Usage

### CLI

```
$ python aleapp.py -t <zip | tar | fs | gz> -i <path_to_extraction> -o <path_for_report_output>
```

### GUI

```
$ python aleappGUI.py
```

### Help

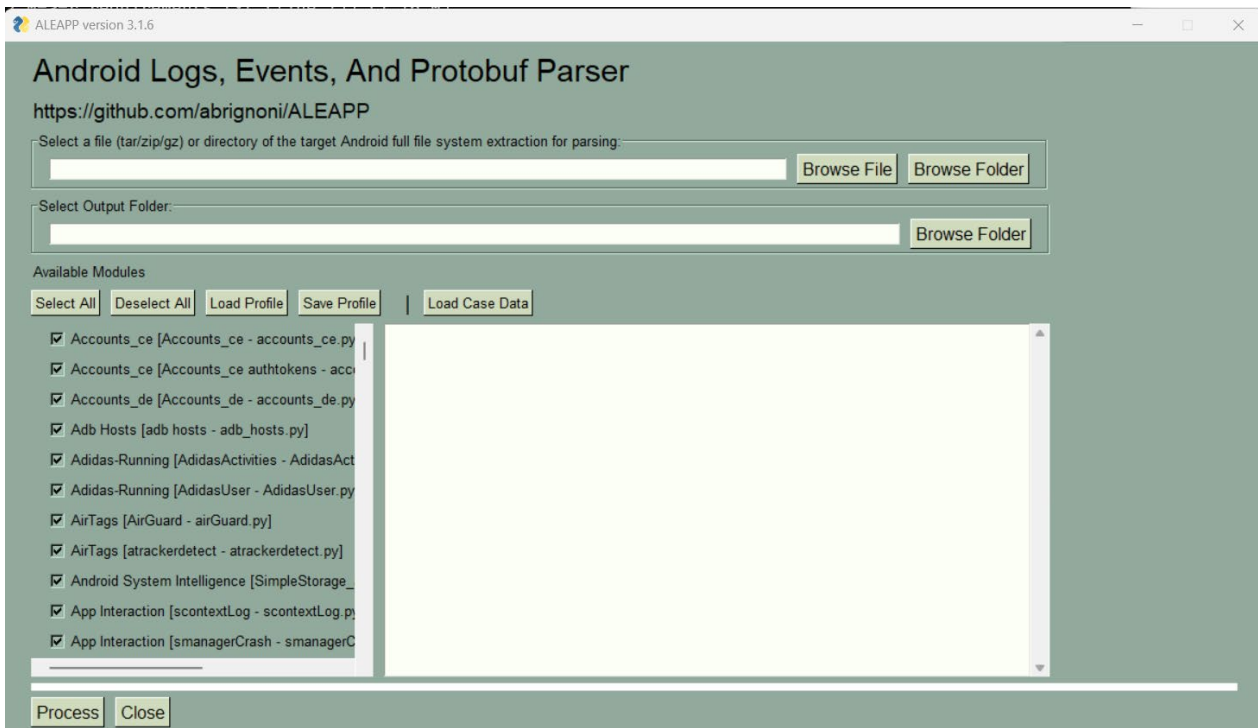
```
$ python aleapp.py --help
```

Example of “python aleappGUI.py”

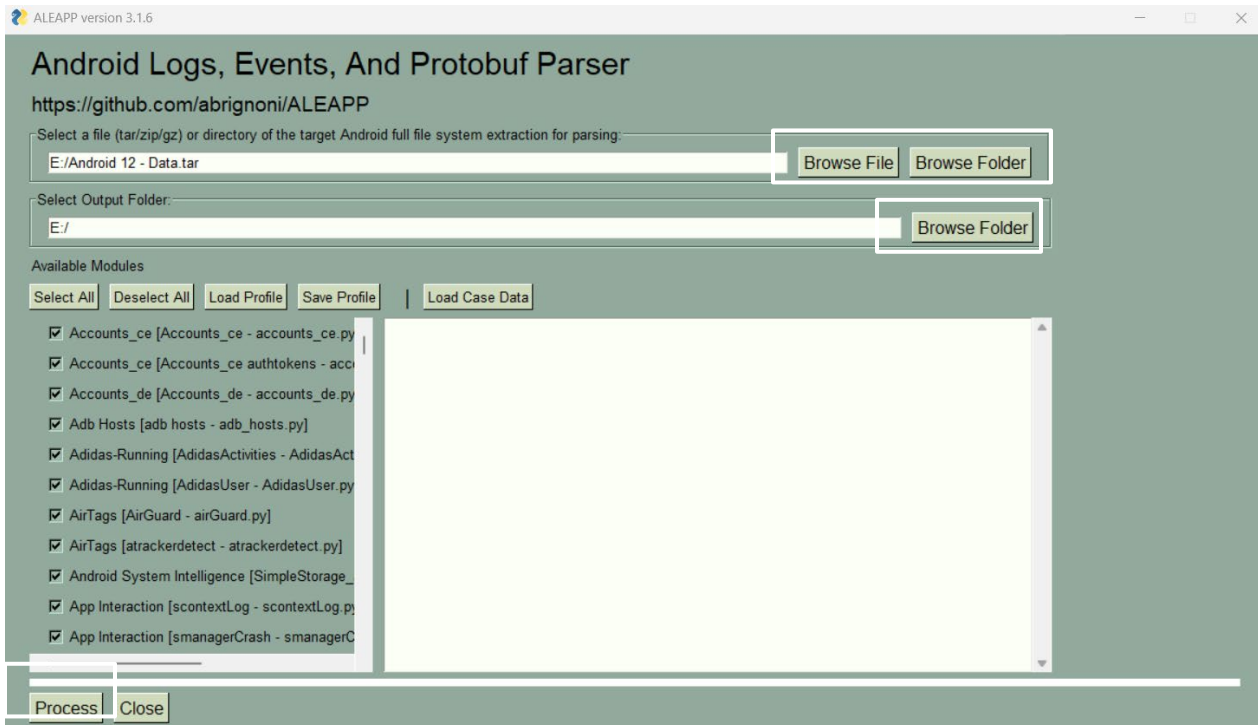
```
C:\Windows\System32\cmd.e x + v
Requirement already satisfied: six>=1.4.1 in c:\users\sarah\appdata\local\programs\python\python311\lib\site-packages (from bcrypt==3.2.0->r requirements.txt (line 1)) (1.16.0)
Requirement already satisfied: soupsieve>=1.2 in c:\users\sarah\appdata\local\programs\python\python311\lib\site-packages (from beautifulsoup4==4.8.2->r requirements.txt (line 2)) (2.4)
Requirement already satisfied: pyparsing>=2.0.2 in c:\users\sarah\appdata\local\programs\python\python311\lib\site-packages (from packaging==20.1->r requirements.txt (line 4)) (3.0.9)
Requirement already satisfied: setuptools in c:\users\sarah\appdata\local\programs\python\python311\lib\site-packages (from protobuf==3.10.0->r requirements.txt (line 5)) (65.5.0)
Requirement already satisfied: branca>=0.6.0 in c:\users\sarah\appdata\local\programs\python\python311\lib\site-packages (from folium==0.14.0->r requirements.txt (line 17)) (0.6.0)
Requirement already satisfied: Jinja2>=2.9 in c:\users\sarah\appdata\local\programs\python\python311\lib\site-packages (from folium==0.14.0->r requirements.txt (line 17)) (3.1.2)
Requirement already satisfied: numpy in c:\users\sarah\appdata\local\programs\python\python311\lib\site-packages (from folium==0.14.0->r requirements.txt (line 17)) (1.24.2)
Requirement already satisfied: requests in c:\users\sarah\appdata\local\programs\python\python311\lib\site-packages (from folium==0.14.0->r requirements.txt (line 17)) (2.28.2)
Requirement already satisfied: pycparser in c:\users\sarah\appdata\local\programs\python\python311\lib\site-packages (from cffi>=1.1->bcrypt==3.2.0->r requirements.txt (line 1)) (2.21)
Requirement already satisfied: MarkupSafe>=2.0 in c:\users\sarah\appdata\local\programs\python\python311\lib\site-packages (from Jinja2>=2.9->folium==0.14.0->r requirements.txt (line 17)) (2.1.2)
Requirement already satisfied: charset-normalizer<4,>=2 in c:\users\sarah\appdata\local\programs\python\python311\lib\site-packages (from requests->folium==0.14.0->r requirements.txt (line 17)) (3.1.0)
Requirement already satisfied: idna<4,>=2.5 in c:\users\sarah\appdata\local\programs\python\python311\lib\site-packages (from requests->folium==0.14.0->r requirements.txt (line 17)) (3.4)
Requirement already satisfied: urllib3<1.27,>=1.21.1 in c:\users\sarah\appdata\local\programs\python\python311\lib\site-packages (from requests->folium==0.14.0->r requirements.txt (line 17)) (1.26.15)
Requirement already satisfied: certifi>=2017.4.17 in c:\users\sarah\appdata\local\programs\python\python311\lib\site-packages (from requests->folium==0.14.0->r requirements.txt (line 17)) (2022.12.7)
C:\Users\sarah\Downloads\ALEAPP-main\ALEAPP-main>python aleappGUI.py
```

## SET UP AND USE

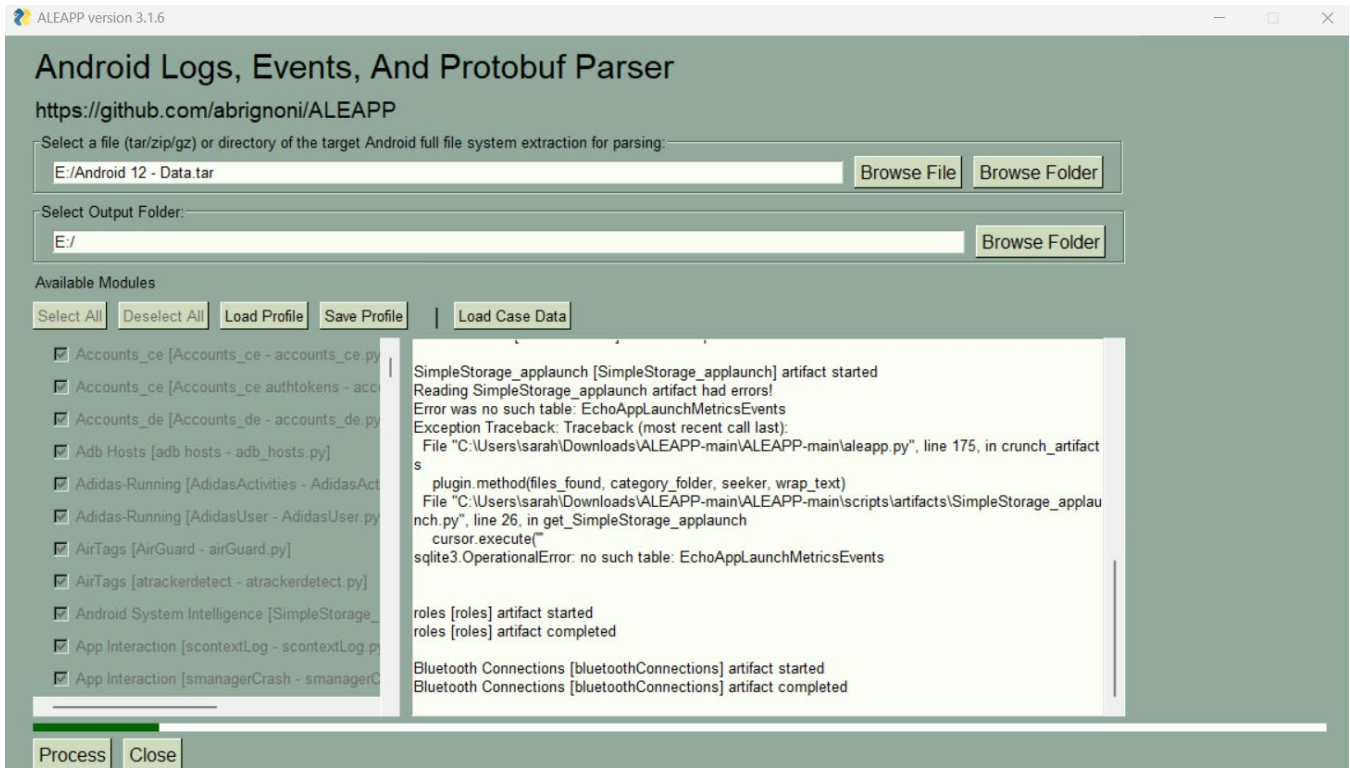




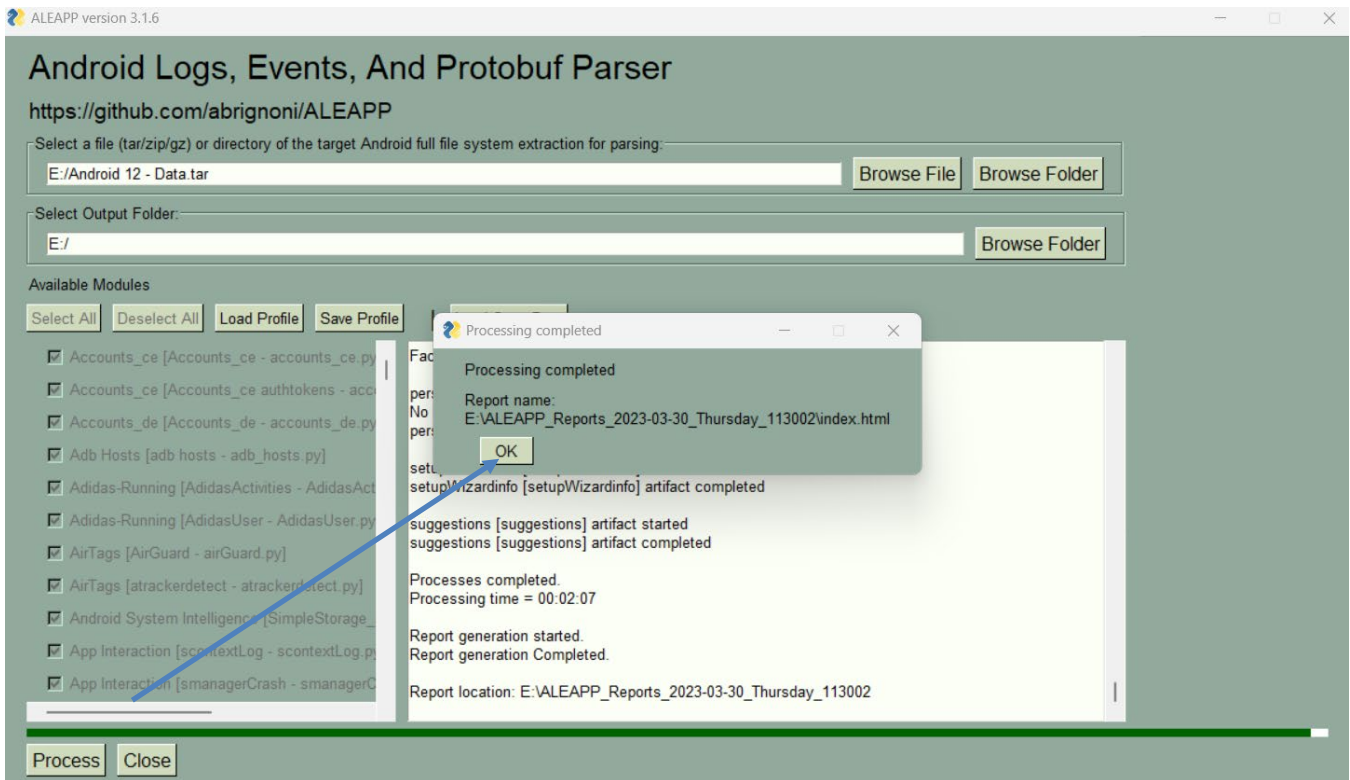
Next select “browse file” or “folder” and “select tar/zip/gz” file type. Select “output” and then “process”.



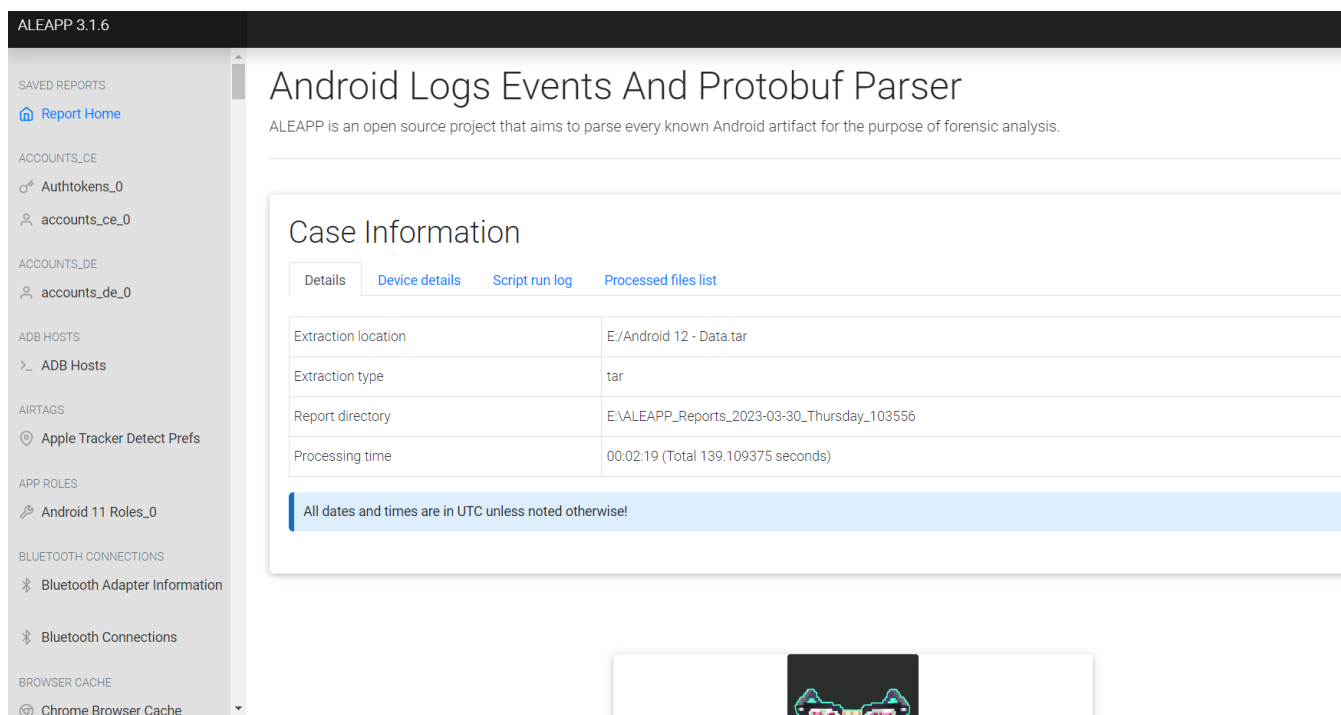
View of processing



Once "Ok" is selected an HTML file will pop up.



Expected output HTML file.



The screenshot shows the ALEAPP 3.1.6 web interface. The main heading is 'Android Logs Events And Protobuf Parser'. Below this, a 'Case Information' section is visible with tabs for 'Details', 'Device details', 'Script run log', and 'Processed files list'. The 'Details' tab is active, showing a table with the following data:

Extraction location	E:/Android 12 - Data.tar
Extraction type	tar
Report directory	E:\ALEAPP_Reports_2023-03-30_Thursday_103556
Processing time	00:02:19 (Total 139.109375 seconds)

Below the table, a blue banner states: 'All dates and times are in UTC unless noted otherwise!'

Post-closing out of the HTML file there will be a folder labelled ALEAPP\_Reports\_(date) saved to the output location.





































ALEAPP\_Reports\_2023-03-30\_Thursday  
\_113002





Open the “folders” or “HTML” files to access the data.

-  \_elements
-  \_Timeline
-  \_TSV Exports
-  Call Logs
-  Cast
-  Contacts
-  Google Chat
-  Google Fit (GMS)
-  Google Maps Voice Guidance
-  Google Photos
-  Image Manager Cache
-  RCS Chats
-  Recent Activity
-  Script Logs
-  SQLite Journaling
-  temp
-  TikTok
-  Usage Stats
-  User Dictionary
-  WiFi Profiles
-  Account Data.html
-  accounts\_ce\_0.html
-  accounts\_de\_0.html
-  ADB Hosts.html
-  App Icons.html
-  App Updates (Frosting.db).html
-  Authtokens\_0.html
-  Bluetooth Adapter Information.html
-  Bluetooth Connections.html
-  Bumble - Chat Messages.html
-  Bumble - Matches.html
-  Bumble - User Settings.html
-  Cello.html
-  Chrome - Autofill - Entries.html



FR5



Select "index.html" for the summary.html file.

ALEAPP\_Reports\_2023-03-30\_Thursday\_113002

Name	Date modified	Type	Size
Google Messages.html	3/30/2023 11:39 AM	Chrome HTML Do...	71 KB
Google Photos (gphotos0) - Cache.html	3/30/2023 11:39 AM	Chrome HTML Do...	503 KB
Google Photos (gphotos0) - Local Media...	3/30/2023 11:39 AM	Chrome HTML Do...	90 KB
Google Photos (gphotos0) - Remote Me...	3/30/2023 11:39 AM	Chrome HTML Do...	139 KB
Google Photos (gphotos0) - Shared Medi...	3/30/2023 11:39 AM	Chrome HTML Do...	68 KB
Google Photos (gphotos-1) - Local Medi...	3/30/2023 11:39 AM	Chrome HTML Do...	90 KB
Google Play Links for Apps.html	3/30/2023 11:39 AM	Chrome HTML Do...	148 KB
Google Play Searches.html	3/30/2023 11:39 AM	Chrome HTML Do...	64 KB
Google Search History Maps.html	3/30/2023 11:39 AM	Chrome HTML Do...	65 KB
Group Information.html	3/30/2023 11:39 AM	Chrome HTML Do...	65 KB
Image Manager Cache.html	3/30/2023 11:39 AM	Chrome HTML Do...	7,246 KB
IMO - Account ID.html	3/30/2023 11:39 AM	Chrome HTML Do...	64 KB
IMO - Messages.html	3/30/2023 11:39 AM	Chrome HTML Do...	66 KB
index.html	3/30/2023 11:39 AM	Chrome HTML Do...	5,119 KB
Installed Apps (GMS).html	3/30/2023 11:39 AM	Chrome HTML Do...	81 KB
Installed Apps (GMS)_0.html	3/30/2023 11:39 AM	Chrome HTML Do...	81 KB
Installed Apps (Library).html	3/30/2023 11:39 AM	Chrome HTML Do...	84 KB
Installed Apps (Vending).html	3/30/2023 11:39 AM	Chrome HTML Do...	87 KB
JSON Activities.html	3/30/2023 11:39 AM	Chrome HTML Do...	2,115 KB
JSON.html	3/30/2023 11:39 AM	Chrome HTML Do...	1,298 KB
Last Boot Time.html	3/30/2023 11:39 AM	Chrome HTML Do...	64 KB
Line - Call Logs.html	3/30/2023 11:39 AM	Chrome HTML Do...	64 KB
Line - Contacts.html	3/30/2023 11:39 AM	Chrome HTML Do...	64 KB
Line - Messages.html	3/30/2023 11:39 AM	Chrome HTML Do...	69 KB
Log.html	3/30/2023 11:39 AM	Chrome HTML Do...	64 KB
MEGA - Chat.html	3/30/2023 11:39 AM	Chrome HTML Do...	67 KB
MEGA - Files.html	3/30/2023 11:39 AM	Chrome HTML Do...	68 KB
MeWe - Chat.html	3/30/2023 11:39 AM	Chrome HTML Do...	72 KB
MeWe - SGSession.html	3/30/2023 11:39 AM	Chrome HTML Do...	70 KB

