

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".

🐉 master 🗸 🤔 8 branches 🔊 12 tag	s		Go to file	Code -
abrignoni Merge pull request #305 from	n stark4n6/master	Local	Codespa	aces
.github/workflows	Point CI/CD to new fork of pyir	>_ Clone		?
scripts	Update googleQuickSearchbox	HTTPS GitHub CLI		
🗋 .gitignore	Fix: .DS_Store for .gitignore	https://github.com/abrign	oni/ALEAPP.git	C
	Updated artifacts	Use Git or checkout with SVN usin	g the web URL.	
README.md	Clean up README markdown s	요. Open with GitHub Deskt	ор	
🗋 aleapp.py	fix missing plugin folder from t			
aleapp.spec	fix missing plugin folder from t	Download ZIP		
aleappGUI.py	When loading profiles user is al	erted to missing plugins if prese	ent. 4 i	months ago
aleappGUI.spec	Updated artifacts		5 1	months ago
hook-plugin_loader.py	Updated artifacts		5 (months ago
plugin_loader.py	Added the optionalleapp_info	oattribute to plugins	4 1	months ago
requirements.txt	Updated artifacts		5 (months ago

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



Name	Date modified	Туре	Size
∨ Today			
] .gitignore	3/30/2023 10:34 AM	GITIGNORE File	2 KB
澷 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	







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 python 3 , 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.





HIJ MOBILE FORENSICS

C:\Windows\System32\cmd.e × + ~			×
Requirement already satisfied: six>=1.4.1 in c:\users\sarah\appdata\local\programs\python\python311\lib\site rom bcrypt==3.2.0->-r requirements.txt (line 1)) (1.16.0)	-packa	ges	(f
Requirement already satisfied: soupsieve>=1.2 in c:\users\sarah\appdata\local\programs\python\python311\lib\s (from beautifulsoup4==4.8.2->-r requirements.txt (line 2)) (2.4)	site-p	ackag	ge
Requirement already satisfied: pyparsing>=2.0.2 in c:\users\sarah\appdata\local\programs\python\python311\lik ges (from packaging==20.1->-r requirements.txt (line 4)) (3.0.9)	⊳\site	-pacl	ka
Requirement already satisfied: setuptools in c:\users\sarah\appdata\local\programs\python\python311\lib\siterom protobuf==3.10.0->-r requirements.txt (line 5)) (65.5.0)	-packa	ges	(f
Requirement already satisfied: branca>=0.6.0 in c:\users\sarah\appdata\local\programs\python\python311\lib\s: (from folium==0.14.0->-r requirements.txt (line 17)) (0.6.0)	ite-pa	ckage	es
Requirement already satisfied: jinja2>=2.9 in c:\users\sarah\appdata\local\programs\python\python311\lib\site from folium==0.14.0->-r requirements.txt (line 17)) (3.1.2)	e-pack	ages	(
Requirement already satisfied: numpy in c:\users\sarah\appdata\local\programs\python\python311\lib\site-packa olium==0.14.0->-r requirements.txt (line 17)) (1.24.2)	ages (from	f
Requirement already satisfied: requests in c:\users\sarah\appdata\local\programs\python\python311\lib\site-pa m folium==0.14.0->-r requirements.txt (line 17)) (2.28.2)	ackage	s (fi	ro
Requirement already satisfied: pycparser in c:\users\sarah\appdata\local\programs\python\python311\lib\site- om cffi>=1.1->bcrypt==3.2.0->-r requirements.txt (line 1)) (2.21)	backag	es (·	fr
Requirement already satisfied: MarkupSafe>=2.0 in c:\users\sarah\appdata\local\programs\python\python311\lib' es (from jinja2>=2.9->folium==0.14.0->-r requirements.txt (line 17)) (2.1.2)	site-	packa	ag
Requirement already satisfied: charset-normalizer<4,>=2 in c:\users\sarah\appdata\local\programs\python\pythot te-packages (from requests->folium==0.14.0->-r requirements.txt (line 17)) (3.1.0)	on311\	lib\s	si
Requirement already satisfied: idna<4,>=2.5 in c:\users\sarah\appdata\local\programs\python\python311\lib\sit	ce-pac	kage	s
Requirement already satisfied: urllib3<1.27,>=1.21.1 in c:\users\sarah\appdata\local\programs\python\python3: packages (from requests->folium==0.14.0->-r requirements.txt (line 17)) (1.26.15)	l1\lib	\sit(e-
Requirement already satisfied: certifi>=2017.4.17 in c:\users\sarah\appdata\local\programs\python\python311\ kages (from requests->folium==0.14.0->-r requirements.txt (line 17)) (2022.12.7)	.ib\si	te-pa	ac
C:\Users\sarah\Downloads\ALEAPP-main\ALEAPP-main>			





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

Usage
CLI
<pre>\$ python aleapp.py -t <zip fs="" gz="" tar="" =""> -i <path_to_extraction> -o <path_for_report_output></path_for_report_output></path_to_extraction></zip></pre>
GUI
<pre>\$ python aleappGUI.py</pre>
Help
<pre>\$ python aleapp.pyhelp</pre>

Example of "python aleappGUI.py"

C:\Windows\System32\cmd.e × + v	-	o x
Requirement already satisfied: six>=1.4.1 in c:\users\sarah\appdata\local\programs\python\python311\lil rom bcrypt==3.2.0->-r requirements.txt (line 1)) (1.16.0)	o∖site-packa	ges (f
Requirement already satisfied: soupsieve>=1.2 in c:\users\sarah\appdata\local\programs\python\python31: s (from beautifulsoup4==4.8.2->-r requirements.txt (line 2)) (2.4)	l\lib\site-p	ackage
Requirement already satisfied: pyparsing>=2.0.2 in c:\users\sarah\appdata\local\programs\python\python' ges (from packaging==20.1->-r requirements.txt (line 4)) (3.0.9)	311\lib\site	-packa
Requirement already satisfied: setuptools in c:\users\sarah\appdata\local\programs\python\python311\lil rom protobuf==3.10.0->-r requirements.txt (line 5)) (65.5.0)	o∖site-packa	ges (f
Requirement already satisfied: branca>=0.6.0 in c:\users\sarah\appdata\local\programs\python\python311` (from folium==0.14.0->-r requirements.txt (line 17)) (0.6.0)	\lib\site-pa	ckages
Requirement already satisfied: jinja2>=2.9 in c:\users\sarah\appdata\local\programs\python\python311\l: from folium==0.14.0->-r requirements.txt (line 17)) (3.1.2)	ib\site-pack	ages (
Requirement already satisfied: numpy in c:\users\sarah\appdata\local\programs\python\python311\lib\site olium==0.14.0->-r requirements.txt (line 17)) (1.24.2)	e-packages (·	from f
Requirement already satisfied: requests in c:\users\sarah\appdata\local\programs\python\python311\lib\: m folium==0.14.0->-r requirements.txt (line 17)) (2.28.2)	site-package:	s (fro
Requirement already satisfied: pycparser in c:\users\sarah\appdata\local\programs\python\python311\lib` om cffi>=1.1->bcrypt==3.2.0->-r requirements.txt (line 1)) (2.21)	\site-packag	es (fr
Requirement already satisfied: MarkupSafe>=2.0 in c:\users\sarah\appdata\local\programs\python\python3: es (from jinja2>=2.9->folium==0.14.0->-r requirements.txt (line 17)) (2.1.2)	l1\lib\site-	packag
Requirement already satisfied: charset-normalizer<4,>=2 in c:\users\sarah\appdata\local\programs\pytho te-packages (from requests->folium==0.14.0->-r requirements.txt (line 17)) (3.1.0)	ı\python311\`	lib\si
Requirement already satisfied: idna<4,>=2.5 in c:\users\sarah\appdata\local\programs\python\python311\ (from requests->folium==0.14.0->-r requirements.txt (line 17)) (3.4)	Lib\site-pac	kages
Requirement already satisfied: urllib3<1.27,>=1.21.1 in c:\users\sarah\appdata\local\programs\python\py packages (from requests->folium==0.14.0->-r requirements.txt (line 17)) (1.26.15)	/thon311\lib	\site-
Requirement already satisfied: certifi>=2017.4.17 in c:\users\sarah\appdata\local\programs\python\pytho kages (from requests->folium==0.14.0->-r requirements.txt (line 17)) (2022.12.7)	on311\lib\si	te-pac
C:\Users\sarah\Downloads\ALEAPP-main\ALEAPP-main>python aleappGUI.py		

SET UP AND USE



ALEAPP version 3.1.6	- 0	×
Android Logs, Events, And Protobuf Parser https://github.com/abrignoni/ALEAPP		
Select a file (tar/zip/gz) or directory of the target Android full file system extraction for parsing: Browse File Browse Folder		
Select Output Folder: Browse Folder		
Available Modules Select All Load Profile Save Profile Load Case Data		
Image: Accounts_ce [Accounts_ce - accounts_ce.py] Image: Accounts_ce authtokens - accounts_de.py Image: Accounts_de [Accounts_de - accounts_de.py] Image: Add Hosts [adb hosts - adb_hosts.py] Image: Add Add Add Add Add Add Add Add Add Ad		
Process Close		

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

ALEAPP version 3.1.6			_	\times
Android Logs, Events, And Protobuf https://github.com/abrignoni/ALEAPP Select a file (tar/zip/gz) or directory of the target Android full file system extract E:/Android 12 - Data.tar	Parser	Browse File Browse Folder		
Select Output Folder:		Browse Folder		
Available Modules Select All Deselect All Load Profile Save Profile Load Case Data Image: Comparison of the second secon]			
 Accounts_ce [Accounts_ce - accounts_ce.py Accounts_ce [Accounts_ce authtokens - accounts_de.py Adcounts_de [Accounts_de - accounts_de.py Adb Hosts [adb hosts - adb_hosts.py] Adidas-Running [AdidasActivities - AdidasAct Adidas-Running [AdidasUser - AdidasUser.py AirTags [AirGuard - airGuard.py] AirTags [atrackerdetect - atrackerdetect.py] AirTags [atrackerdetect - atrackerdetect.py] Android System Intelligence [SimpleStorage_ App Interaction [scontextLog - scontextLog.p] App Interaction [smanagerCrash - smanagerC 				
Process				
View of processing	6			



ALEAPP version 3.1.6		-	
Android Logs, Events, An	d Protobuf Parser		
https://github.com/abrignoni/ALEAPP			
Select a file (tar/zip/gz) or directory of the target Androi	d full file system extraction for parsing:		
E:/Android 12 - Data.tar	Browse File Browse Folder		
Select Output Folder:			
E:/	Browse Folder		
Available Modules			
Select All Deselect All Load Profile Save Profile	Load Case Data		
Accounts ce [Accounts ce - accounts ce.py]			
Accounts ce Accounts ce authtokens - acco	SimpleStorage_applaunch [SimpleStorage_applaunch] artifact started Reading SimpleStorage_applaunch artifact had errors!		
Accounts de Accounts de - accounts de.py	Error was no such table: EchoAppLaunchMetricsEvents		
Adb Hosts [adb hosts - adb hosts.py]	Exception fraceback. fraceback (most recent call fast). File "C:\Users\sarah\Downloads\ALEAPP-main\ALEAPP-main\aleapp.py", line 175, in crunch_artifact		
Adidas-Running [AdidasActivities - AdidasAct	s plugin.method(files found, category folder, seeker, wrap text)		
Adidas-Running [AdidasUser - AdidasUser.pv	File "C:\Users\sarah\Downloads\ALEAPP-main\ALEAPP-main\scripts\artifacts\SimpleStorage_applau		
AirTags [AirGuard - airGuard pv]	cursor.execute("		
AirTaos fatrackerdetect - atrackerdetect pv]	sqlite3.OperationalError: no such table: EchoAppLaunchMetricsEvents		
Android System Intelligence [SimpleStorage	roles (roles) artifact started		
Ann Interaction (scontext) on a scontext) on m	roles [roles] artifact completed		
Ann Interaction [scontextEdg - scontextEdg.p]	Bluetooth Connections [bluetoothConnections] artifact started		
Abb interaction famanagerciasti - smanagerc	Bluetooth Connections [bluetoothConnections] artifact completed		

Process Close

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

2 ALEAPP version 3.1.6	- 🗆 X
Android Logs, Events, And Protobuf Parser https://github.com/abrignoni/ALEAPP	
E:/Android 12 - Data tar Browse File Browse Folder	
Select Output Folder: E:/ Browse Folder	
Available Modules	
Select All Deselect All Load Profile Save Profile ?Processing completed - X	
Image: Accounts_ce [Accounts_ce - accounts_ce:py] Fac Image: Accounts_ce [Accounts_ce authtokens - accounts_de:per: Processing completed Image: Accounts_de [Accounts_de - accounts_de:py] Per: Image: Report name: E:\ALEAPP_Reports_2023-03-30_Thursday_113002\index.html Image: Processing completed Processing completed Image: Processing completed Per: Image: Procesing completed Per: <td></td>	
Adidas-Running [AdidasActivities - AdidasAct setup1///zardinfo [setup1///zardinfo] artifact completed Suggestions] artifact started	
AirTags [AirGuard - airGuard py] suggestions] artifact completed AirTags [atrackerdetect - atrackerdetect.py] Processes completed. Processes to make a completed. Processes to make a completed. Processes to make a completed.	
Android System Intelligence [SimpleStorage_ App Interaction [scontextLog - scontextLog p] Report generation Started. Report generation Completed.	
Pape Interaction [smanagerCrash - smanagerC Report location: E:VALEAPP_Reports_2023-03-30_Thursday_113002	
Process Close	

Expected output HTML file.



ALEAPP 3.1.6		
SAVED REPORTS	Android Logs Event ALEAPP is an open source project that aims to p	arse every known Android artifact for the purpose of forensic analysis.
ACCOUNTS_CE		
o [∞] Authtokens_0		
	Case Information	
ACCOUNTS_DE		
A accounts_de_0	Details Device details Script run log	Processed files list
ADB HOSTS	Extraction location	E:/Android 12 - Data.tar
>_ ADB Hosts	Extraction type	tar
AIRTAGS	Report directory	E:\ALEAPP_Reports_2023-03-30_Thursday_103556
O Apple Tracker Detect Prefs	Processing time	00:02:19 (Total 139.109375 seconds)
APP ROLES		
Android 11 Roles_0	All dates and times are in UTC unless noted othe	erwise!
BLUETOOTH CONNECTIONS		
Bluetooth Adapter Information	·	
Bluetooth Connections		
BROWSER CACHE		
Chrome Browser Cache T		

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
- O ADB Hosts.html
- App Icons.html
- Opp Updates (Frosting.db).html
- O 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





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

ALEAPP_Reports_2023-03-30_Thursday_113002

Name	Date modified	Туре	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	
SON 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	

