

ILEAPP 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 Microsoft Visual Studio from <u>https://visualstudio.microsoft.com/downloads/</u>, (there is a free community version) and "select" Desktop development with C++ and then click "install".

Need help choosing what to install? More info			×	Installation details
b & Cloud (4)			1	ASP.NET and web development
ASP.NET and web development Build web applications using ASP.NET Core, ASP.NET, HTML/JavaScript, and Containers including Docker supp	Azure development Azure SDKs, tools, and projects for developing cloud apps and creating resources using .NET and .NET Framework	Python development Editing, debugging, interactive development and source control for Python.		 Azure development .NET desktop development Desktop development with C++ Included C++ core desktop features
Node.j: development Build scalable network applications using Node.jr, an asynchronous event-driven JavaScript runtime.				Optional MSVC v143 - VS 2022 C++ x64/x86 build C++ ATL for latest v143 build tools (x86 & Windows 11 SDK (100.22000.0) Sourch form Analytic
sktop & Mobile (5)			1 1	Just-In-Time debugger
INET Multi-platform App UI development Build Android, IOS, Windows, and Mac apps from a single codebase using C≢ with .NET MAUL	INET decktop development Build WPF, Windows Forms, and console applications using C#, Visual Basic, and F# with .NET and .NET Frame	Pesktop development with C++ Build modern C++ apps for Windows using tools of your choice, including MSVC, Clang, CMake, or MSBuild.		C++ profiling tools C++ Chake tools for Windows Test Adapter for Boost.Test Test Adapter for Google Test Live Share
Universal Windows Platform development Create applications for the Universal Windows Platform with C#, VB, or optionally C++.	* ■ Mobile development with C++ Build cross-platform applications for IOS, Android or Windows using C++.	,		IntellicOde C++ AddresSanitizer C++ AddresSanitizer C++ MFC for latest v143 build tools (x86, C++ Modules for v143 build tools (x64,x8 Windows 11 SDK (10.0.22621.0)
ming (2)				C++ Clang tools for Windows (15.0.1 - x6
Game development with Unity Create 2D and 3D games with Unity, a powerful cross- platform development environment.	Game development with C++ Use the full power of C++ to build professional games powered by DirectX, Unreal, or Cocos2d.			Jevascript diagnostics Incredibuild - Build Acceleration Windows 10 SDK (10.0.20348.0) Windows 10 SDK (10.0.19041.0) Windows 10 SDK (10.0.18362.0)
her Toolsets (5)				MSVC v142 - VS 2019 C++ x64/x86 build MSVC v141 - VS 2017 C++ x64/x86 build
Data storage and processing Connect, develop, and test data solutions with SQL Server,	Data science and analytical applications	Visual Studio extension development		MSVC v140 - VS 2015 C++ build tools (v1
ation rogram Files\Microsoft Visual Studio\2022\Community Change				Remove ut-of-support componer

After Microsoft Visual Studio with C++ has been installed, please download iLEAPP from https://github.com/abrignoni/iLEAPP.

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 iLEAPP-main.zip version 1.18.4 is e474ce96e04b3e2a12f18a5575b6f875.

**If you already have iLEAPP Installed, please move on to Set Up and Use.



INSTALLATION

Select "Code" and then "Download Zip."

\leftrightarrow \rightarrow G	github.com /abrignoni/iLEAPP					
	Product ~ Solutions ~ C	Dpen Source \vee Pricing		Search		
🛱 abrigno	abrignoni / iLEAPP Public					
<> Code	⊙ Issues 7 \$1 Pull requests 3	🖓 Discussions 💿 Actions 🖽 Pro	ojects 🖾 Wiki 🛈 Securit	ny 🗠 Insights		
	१९ master - १९ 4 branches	∑ 22 tags		Go to file Code -		
	abrignoni Merge pull request #	#404 from stark4n6/master	Local	Codespaces		
	.github/workflows	Point CI/CD to new fork of pyir	▶ Clone	3		
	scripts	iOS 16.2 update	HTTPS GitHub CLI			
	🗋 .gitignore	update artifacts to new style A	https://github.com/abrigno	ni/iLEAPP.git		
		Create LICENSE	Use Git or checkout with SVN using) the web URL.		
	README.md	readme markdown formatting	단 Open with GitHub Deskto	p		
	hook-plugin_loader.py	core ileapp update to new plug				
	🗋 ileapp.py	Attempt to get iTunesBackupIn	Download ZIP			



Once downloaded, extract the file, save it to a location of choice.



The output should look like the file below.

iLEAPP-main						∨ C Se
Name	Туре	Compressed size	Password p	Size	Ratio	Date modified
📒 .github	File folder					3/29/2023 5:57 AM
🚞 scripts	File folder					3/29/2023 5:57 AM
gitignore	GITIGNORE File	1 KB	No	2 KB	45%	3/29/2023 5:57 AM
📄 hook-plugin_loader.py	Python File	1 KB	No	1 KB	45%	3/29/2023 5:57 AM
📄 ileapp.py	Python File	3 KB	No	10 KB	72%	3/29/2023 5:57 AM
ileapp.spec	SPEC File	1 KB	No	2 KB	65%	3/29/2023 5:57 AM
📄 ileappGUI.py	Py hon File	4 KB	No	13 KB	72%	3/29/2023 5:57 AM
ileappGUI.spec	SPEC File	1 KB	No	2 KB	67%	3/29/2023 5:57 AM
LICENSE	XMLS, y.	1 KB	No	2 KB	42%	3/29/2023 5:57 AM
📄 plugin_loader.py	Python Vile	1 KB	No	2 KB	63%	3/29/2023 5:57 AM
README.md	MD File	3 KB	No	6 KB	58%	3/29/2023 5:57 AM
requirements.txt	Text Document	1 KB	No	1 KB	37%	3/29/2023 5:57 AM
ZCaseDataExample.alprofile	ALPROFILE File	1 KB	No	1 KB	8%	3/29/2023 5:57 AM

In the toolbar you are going to type CMD

In the toolbar you will want to type "CMD" for the command prompt.



MOBILE FORENSICS

Result:

Next, go back to the GitHub page and follow the Requirements and Dependencies.

Requirements

Python 3.9 to latest version (older versions of 3.x will also work with the exception of one or two modules) If on macOS (Intel) make sure Xcode is installed and have command line tools updated to be able to use Python 3.10 and above.

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



After running the dependencies, the command prompt should look similar to this. If errors are present, check the version of python installed and make sure the version is correct and pip updates are complete.

C:\Windows\System32\cmd.e × + ~			×
Requirement already satisfied: beautifulsoup4 in c:\users\sarah\appdata\local\programs\python\python311\lib\s s (from bs4->-r requirements.txt (line 4)) (4.8.2)	ite-pa	ackag	le
Requirement already satisfied: cryptography>=3.3.2 in c:\users\sarah\appdata\local\programs\python\python311\ ckages (from PGPy->-r requirements.txt (line 8)) (40.0.1)	lib\s:	ite-p	a
Requirement already satisfied: pyasn1 in c:\users\sarah\appdata\local\programs\python\python311\lib\site-pack PGPy->-r requirements.txt (line 8)) (0.4.8)	ages	(from	
Requirement already satisfied: setuptools>=42.0.0 in c:\users\sarah\appdata\local\programs\python\python311\l kages (from pyinstaller->-r requirements.txt (line 10)) (65.5.0)	ib\si	te-pa	۱C
Requirement already satisfied: altgraph in c:\users\sarah\appdata\local\programs\python\python311\lib\site-pa m pyinstaller->-r requirements.txt (line 10)) (0.17.3)	ckage	s (fr	0
Requirement already satisfied: pyinstaller-hooks-contrib>=2021.4 in c:\users\sarah\appdata\local\programs\pyt 11\lib\site-packages (from pyinstaller->-r requirements.txt (line 10)) (2023.1)	hon\p	ython	3
Requirement already satisfied: pefile>=2022.5.30 in c:\users\sarah\appdata\local\programs\python\python311\li ages (from pyinstaller->-r requirements.txt (line 10)) (2023.2.7)	b\sit(e-pac	:k
Requirement already satisfied: pywin32-ctypes>=0.2.0 in c:\users\sarah\appdata\local\programs\python\python31 packages (from pyinstaller->-r requirements.txt (line 10)) (0.2.0)	1∖lib`	\site	-
Requirement already satisfied: protobuf==3.10.0 in c:\users\sarah\appdata\local\programs\python\python311\lib ges (from blackboxprotobuf->-r requirements.txt (line 12)) (3.10.0)	\site	-pack	a
Requirement already satisfied: python-dateutil>=2.8.1 in c:\users\sarah\appdata\local\programs\python\python3 -packages (from pandas->-r requirements.txt (line 15)) (2.8.2)	11\lil	b\sit	.e
Requirement already satisfied: pytz>=2020.1 in c:\users\sarah\appdata\local\programs\python\python311\lib\sit (from pandas->-r requirements.txt (line 15)) (2023.3)	e-pacl	kages	
Requirement already satisfied: cffi>=1.12 in c:\users\sarah\appdata\local\programs\python\python311\lib\site- rom cryptography>=3.3.2->PGPy->-r requirements.txt (line 8)) (1.15.1)	packa	ges (f
Requirement already satisfied: soupsieve>=1.2 in c:\users\sarah\appdata\local\programs\python\python311\lib\s s (from beautifulsoup4->bs4->-r requirements.txt (line 4)) (2.4)	ite-pa	ackag	e
Requirement already satisfied: pycparser in c:\users\sarah\appdata\local\programs\python\python311\lib\site-p om cffi>=1.12->cryptography>=3.3.2->PGPy->-r requirements.txt (line 8)) (2.21)	ackage	es (f	r

C:\Users\sarah\Downloads\iLEAPP-main\iLEAPP-main>



Next, run the GUI command, for this exercise command iLEAPPGUI.py was used.

Usage

CLI

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

GUI

\$ python ileappGUI.py

Help

\$ python ileapp.py --help



SET UP AND USE

Once the GUI command is ran, the iLEAPP screen will pop up and should look like this.





Select "Browse File" to select an image or select "Browse folder" to add an entire folder. File types must be tar/zip/gz file.

Then under Select Output Folder: select "Browse Folder" this is where the results will save once ran. Available Modules: Select All or select Modules of interest.

iLEAPP version 1.18.4	-	×
iOS Logs, Events, And Plists Parser https://github.com/abrignoni/iLEAPP		
Select the file (tar/zip/gz) or directory of the target iOS full file system extraction for parsing: <u>E:/iOS Magnet 2023/2022 CTF - iOS Full File System/Jess_CTF_iPhone8/fb028ddefa8af7df5b12d3e729f075d150637a</u> Browse File Browse Folder		
E/ Browse Folder		
Available Modules Select All Deselect All Load Profile Save Profile Load Case Data		
 Accounts [accs - accs.py] Accounts [confaccts - confaccts.py] Accounts [tileAppDisc - tileAppDisc.py] Accounts [tileAppNetDb - tileAppNetDb.py] Address Book [addressbook - addressBook.p Adirtags [airtags - airtags.py] Alarms [alarms - alarms.py] AllTrails [alltrails - AllTrails.py] App Conduit [appconduit.py] Apple Podcasts [applepodcasts - applePodca 		
Process Close		

Once modules of choice are selected, click "Process". It will take a few minutes depending on the size of the file/folder. There should be a status bar running across the bottom of the Parser.



There will be a processing complete pop up. Select "OK."





The index.html will automatically load.

ileapp 1.18.4			Dark Switch
SAVED REPORTS Report Home ACCOUNTS	iOS Logs	Events And Protobuf Parser ce project that aims to parse every known iOS artifact for the purpose of forensic analysis.	
Account Data			
Account Configuration	Case Infor	mation	
ALARMS	Details Device of	Jetails Script run log Processed files list	
ALLTRAILS	Extraction location	E:/iOS Magnet 2023/2022 CTF - iOS Full File System/Jess_CTF_iPhone8/fb028ddefa8af7df5b12d3e729f075d150637a31_files_full.zip	
D AllTrails - Trail Details	Extraction type	zio	
AllTrails - User Info	Peport directory	· F\ii EADD Denorte 2022.02.20 Wednaeday 17/216	
APP PERMISSIONS	Processing time	00.02.00 (Total 120.52744209999219 seconds)	
BIOME BACKLIGHT	All dates and times a	are in UTC unless noted otherwise!	
Biome Backlight Public - 663201736571093			
BIOME INTENTS			
Intents - 663528486816806			
BIOME NOTIFICATIONS PUB			
Diama Natificationa Dublia			

From here utilizing the left side of the html file, navigate through the different modules. To get to the output, navigate to the selected output location from above. Each of these "folders" or "HTML" files can be opened and data may be available within.

Name	Date modified	Type Si	ize
_elements	3/29/2023 5:44 PM	File folder	
_KML Exports	3/29/2023 5:43 PM	File folder	
Timeline	3/29/2023 5:42 PM	File folder	
TSV Exports	3/29/2023 5:42 PM	File folder	
Address Book	3/29/2023 5:42 PM	File folder	
Apple Wallet	3/29/2023 5:42 PM	File folder	
Biome Intents	3/29/2023 5:42 PM	File folder	
Biome Notes	3/29/2023 5:42 PM	File folder	
📒 Cache Data	3/29/2023 5:42 PM	File folder	
Cloudkit	3/29/2023 5:43 PM	File folder	
iCloud Shared Albums	3/29/2023 5:43 PM	File folder	
Installed Apps	3/29/2023 5:43 PM	File folder	
iOS Mail	3/29/2023 5:43 PM	File folder	
Locations	3/29/2023 5:43 PM	File folder	
Mobile Installation Logs	3/29/2023 5:43 PM	File folder	
Mobile Software Update	3/29/2023 5:43 PM	File folder	
Photos	3/29/2023 5:43 PM	File folder	
Proton Mail	3/29/2023 5:43 PM	File folder	
Reminders	3/29/2023 5:43 PM	File folder	
Script Logs	3/29/2023 5:42 PM	File folder	
SQLite Journaling	3/29/2023 5:44 PM	File folder	
📜 temp	3/29/2023 5:42 PM	File folder	
Account Configuration.html	3/29/2023 5:44 PM	Chrome HTML Document	29 KB
Account Data.html	3/29/2023 5:44 PM	Chrome HTML Document	29 KB
💿 Alarms.html	3/29/2023 5:44 PM	Chrome HTML Document	27 KB
AllTrails - Trail Details.html	3/29/2023 5:44 PM	Chrome HTML Document	44 KB
💽 AllTrails - User Info.html	3/29/2023 5:44 PM	Chrome HTML Document	28 KB
Opp Snapshots.html	3/29/2023 5:44 PM	Chrome HTML Document	79 KB
Application State DB.html	3/29/2023 5:44 PM	Chrome HTML Document	43 KB



To get back the index.html, navigate through the saved output folder and select "index.html."

> iLEAPP_Reports_2023-03-29_Wednesday_174216						
Date modified	Туре	Size				
3/29/2023 5:44 PM	Chrome HTML Document	27 KB				
3/29/2023 5:44 PM	Chrome HTML Document	596 KB				
3/29/2023 5:44 PM	Chrome HTML Document	1,010 KB				
3/29/2023 5:44 PM	Chrome HTML Document	27 KB				
3/29/2023 5:44 PM	Chrome HTML Document	27 KB				
3/29/2023 5:44 PM	Chrome HTML Document	949 KB				
3/29/2023 5:44 PM	Chrome HTML Document	40 KB				
3/29/2023 5:44 PM	Chrome HTML Document	329 KB				
3/29/2023 5:44 PM	Chrome HTML Document	51 KB				
3/29/2023 5:44 PM	Chrome HTML Document	27 KB				
3/29/2023 5:44 PM	Chrome HTML Document	29 KB				
3/29/2023 5:44 PM	Chrome HTML Document	27 KB				
3/29/2023 5:44 PM	Chrome HTML Document	28 KB				
	Date modified 3/29/2023 5:44 PM 3/29/2023 5:44 PM	Date modifiedType3/29/2023 5:44 PMChrome HTML Document3/29/2023 5:44 PMChrome HTML Document </th <th>Date modifiedTypeSize3/29/2023 5:44 PMChrome HTML Document27 KB3/29/2023 5:44 PMChrome HTML Document596 KB3/29/2023 5:44 PMChrome HTML Document1,010 KB3/29/2023 5:44 PMChrome HTML Document27 KB3/29/2023 5:44 PMChrome HTML Document27 KB3/29/2023 5:44 PMChrome HTML Document27 KB3/29/2023 5:44 PMChrome HTML Document949 KB3/29/2023 5:44 PMChrome HTML Document40 KB3/29/2023 5:44 PMChrome HTML Document329 KB3/29/2023 5:44 PMChrome HTML Document51 KB3/29/2023 5:44 PMChrome HTML Document27 KB3/29/2023 5:44 PMChrome HTML Document28 KB3/29/2023 5:44 PMChrome HTML Document27 KB3/29/2023 5:44 PMChrome HTML Document28 KB</th>	Date modifiedTypeSize3/29/2023 5:44 PMChrome HTML Document27 KB3/29/2023 5:44 PMChrome HTML Document596 KB3/29/2023 5:44 PMChrome HTML Document1,010 KB3/29/2023 5:44 PMChrome HTML Document27 KB3/29/2023 5:44 PMChrome HTML Document27 KB3/29/2023 5:44 PMChrome HTML Document27 KB3/29/2023 5:44 PMChrome HTML Document949 KB3/29/2023 5:44 PMChrome HTML Document40 KB3/29/2023 5:44 PMChrome HTML Document329 KB3/29/2023 5:44 PMChrome HTML Document51 KB3/29/2023 5:44 PMChrome HTML Document27 KB3/29/2023 5:44 PMChrome HTML Document28 KB3/29/2023 5:44 PMChrome HTML Document27 KB3/29/2023 5:44 PMChrome HTML Document28 KB			