

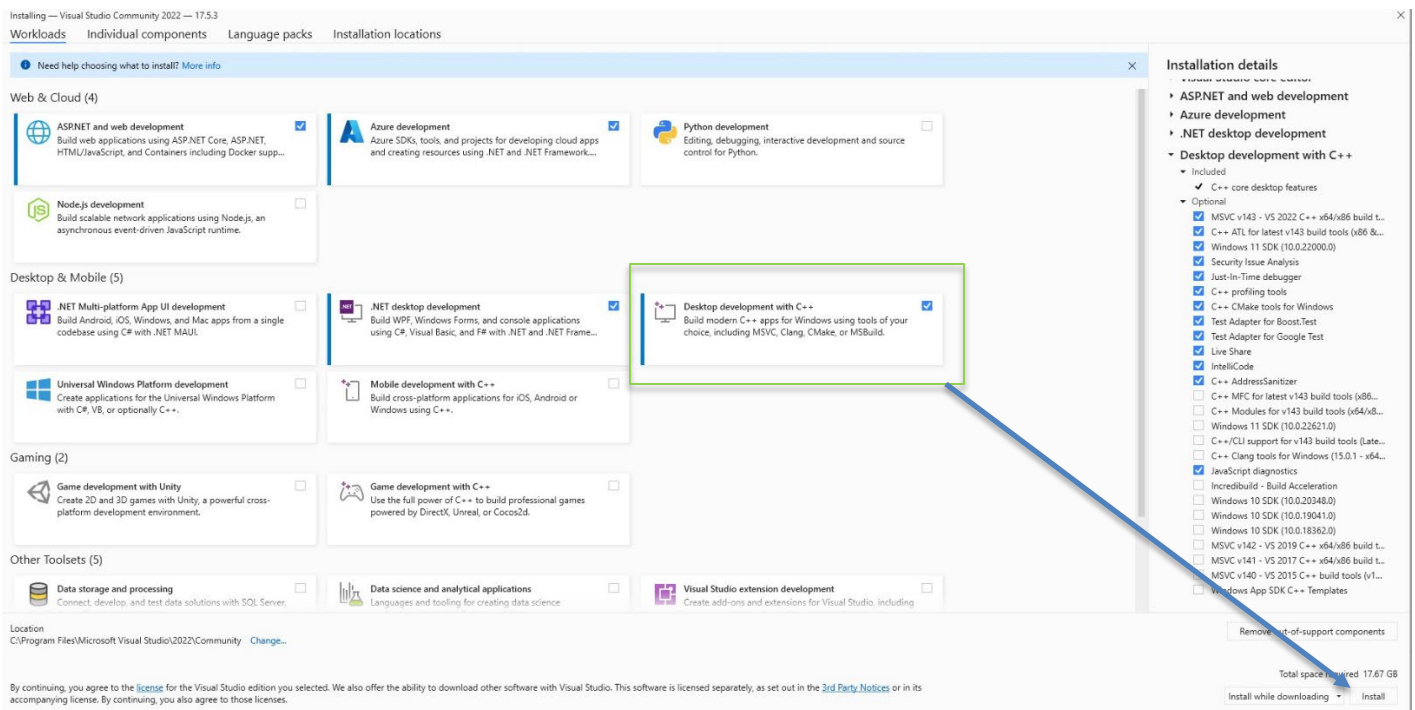


iLEAPP GUIDED EXERCISE

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 <https://visualstudio.microsoft.com/downloads/>, (there is a free community version) and “select” Desktop development with C++ and then click “install”.



After Microsoft Visual Studio with C++ has been installed, please download iLEAPP from

<https://github.com/abrignoni/iLEAPP>.

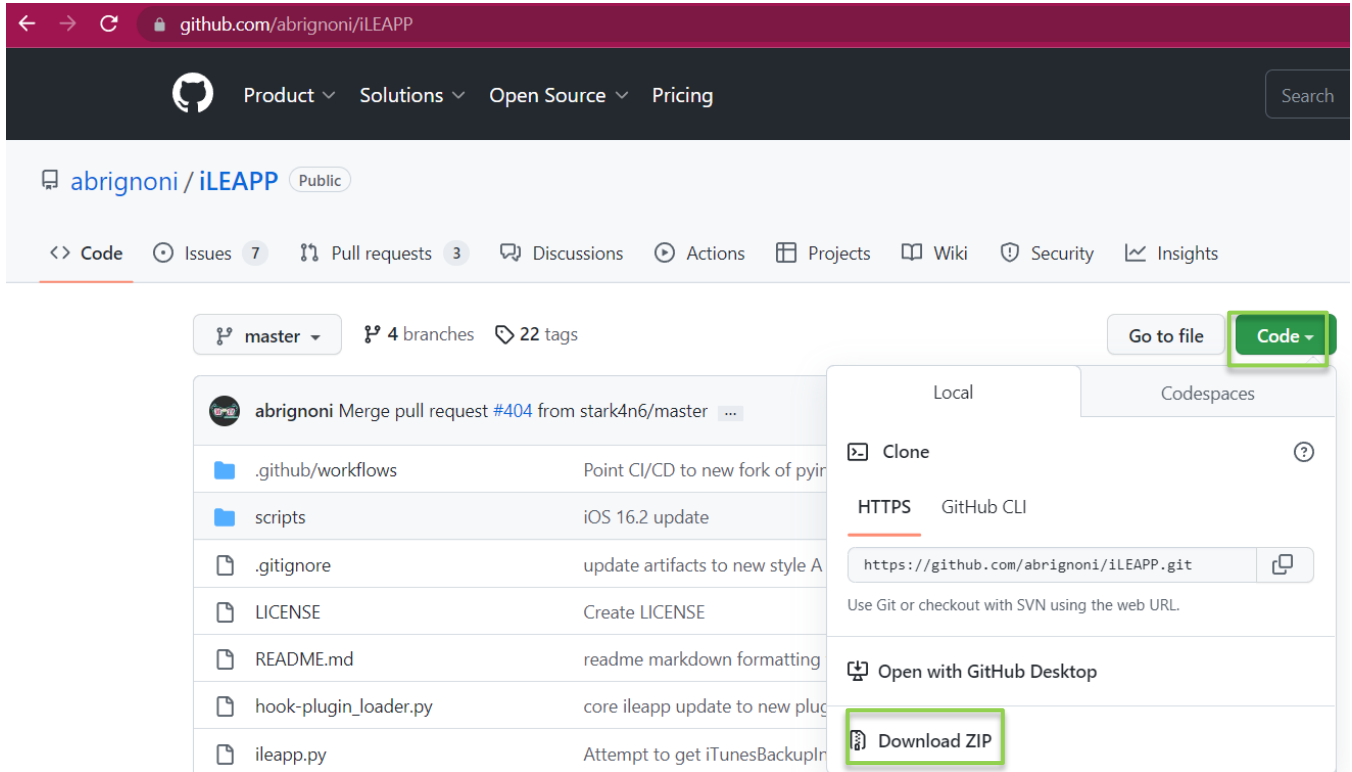
Prior to installation, verify the hash value to the known good from the syllabus for students enrolled in the HMFA Virtual Live course. The MD5 hash value for the iLEAPP-main.zip version 1.18.4 is e474ce96e04b3e2a12f18a5575b6f875.

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



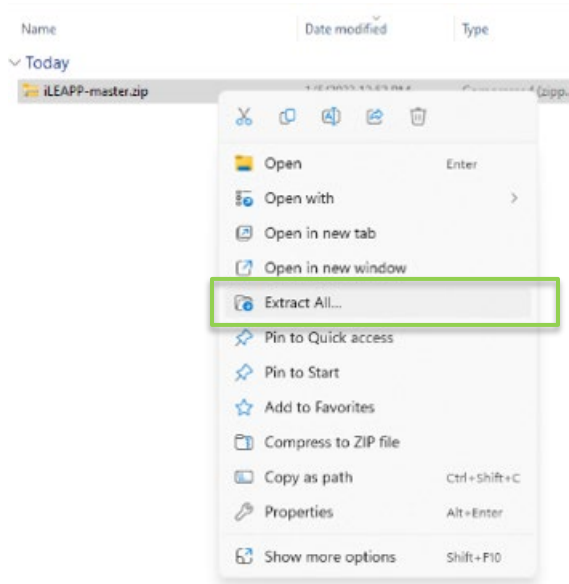
INSTALLATION

Select “Code” and then “Download Zip.”

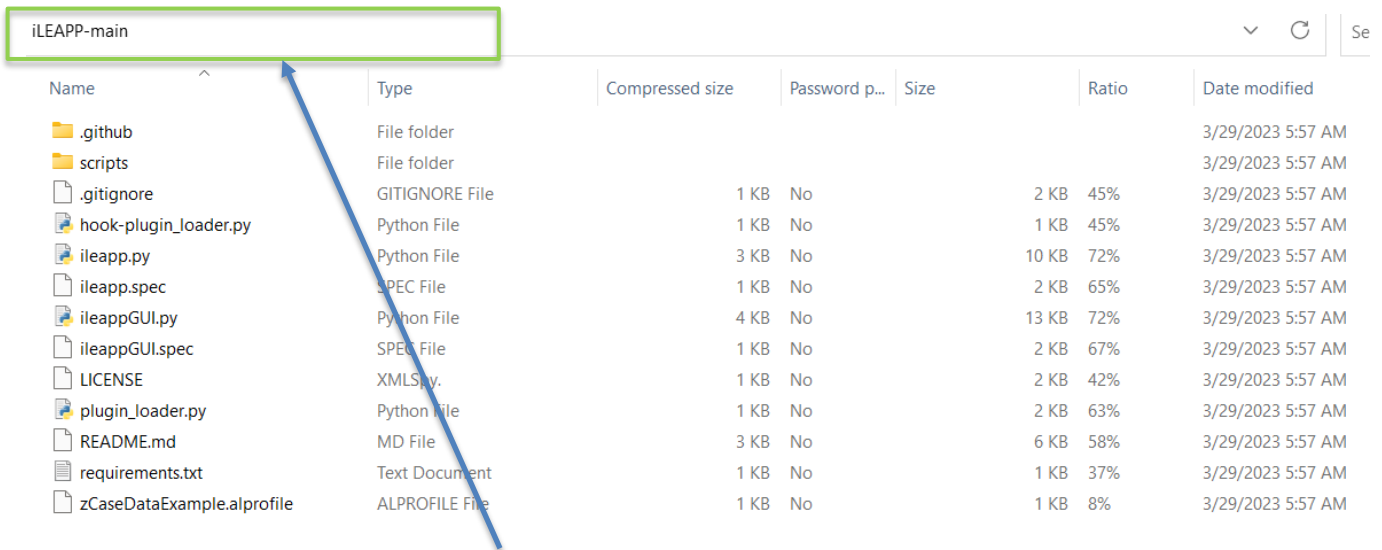




Once downloaded, extract the file, save it to a location of choice.



The output should look like the file below.



In the toolbar you are going to type CMD

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



Result:

```
C:\Windows\System32\cmd.e x + v
Microsoft Windows [Version 10.0.22621.1413]
(c) Microsoft Corporation. All rights reserved.

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

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  x  +  v
Requirement already satisfied: beautifulsoup4 in c:\users\sarah\AppData\Local\Programs\Python\Python311\lib\site-packages (from bs4->-r requirements.txt (line 4)) (4.8.2)
Requirement already satisfied: cryptography>=3.3.2 in c:\users\sarah\AppData\Local\Programs\Python\Python311\lib\site-packages (from PGPpy->-r requirements.txt (line 8)) (40.0.1)
Requirement already satisfied: pyasn1 in c:\users\sarah\AppData\Local\Programs\Python\Python311\lib\site-packages (from PGPpy->-r requirements.txt (line 8)) (0.4.8)
Requirement already satisfied: setuptools>=42.0.0 in c:\users\sarah\AppData\Local\Programs\Python\Python311\lib\site-packages (from pyinstaller->-r requirements.txt (line 10)) (65.5.0)
Requirement already satisfied: altgraph in c:\users\sarah\AppData\Local\Programs\Python\Python311\lib\site-packages (from pyinstaller->-r requirements.txt (line 10)) (0.17.3)
Requirement already satisfied: pyinstaller-hooks-contrib>=2021.4 in c:\users\sarah\AppData\Local\Programs\Python\Python311\lib\site-packages (from pyinstaller->-r requirements.txt (line 10)) (2023.1)
Requirement already satisfied: pefile>=2022.5.30 in c:\users\sarah\AppData\Local\Programs\Python\Python311\lib\site-packages (from pyinstaller->-r requirements.txt (line 10)) (2023.2.7)
Requirement already satisfied: pywin32-ctypes>=0.2.0 in c:\users\sarah\AppData\Local\Programs\Python\Python311\lib\site-packages (from pyinstaller->-r requirements.txt (line 10)) (0.2.0)
Requirement already satisfied: protobuf==3.10.0 in c:\users\sarah\AppData\Local\Programs\Python\Python311\lib\site-packages (from blackboxprotobuf->-r requirements.txt (line 12)) (3.10.0)
Requirement already satisfied: python-dateutil>=2.8.1 in c:\users\sarah\AppData\Local\Programs\Python\Python311\lib\site-packages (from pandas->-r requirements.txt (line 15)) (2.8.2)
Requirement already satisfied: pytz>=2020.1 in c:\users\sarah\AppData\Local\Programs\Python\Python311\lib\site-packages (from pandas->-r requirements.txt (line 15)) (2023.3)
Requirement already satisfied: cffi>=1.12 in c:\users\sarah\AppData\Local\Programs\Python\Python311\lib\site-packages (from cryptography>=3.3.2->PGPpy->-r requirements.txt (line 8)) (1.15.1)
Requirement already satisfied: soupsieve>=1.2 in c:\users\sarah\AppData\Local\Programs\Python\Python311\lib\site-packages (from beautifulsoup4->bs4->-r requirements.txt (line 4)) (2.4)
Requirement already satisfied: pycparser in c:\users\sarah\AppData\Local\Programs\Python\Python311\lib\site-packages (from cffi>=1.12->cryptography>=3.3.2->PGPpy->-r requirements.txt (line 8)) (2.21)
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
```

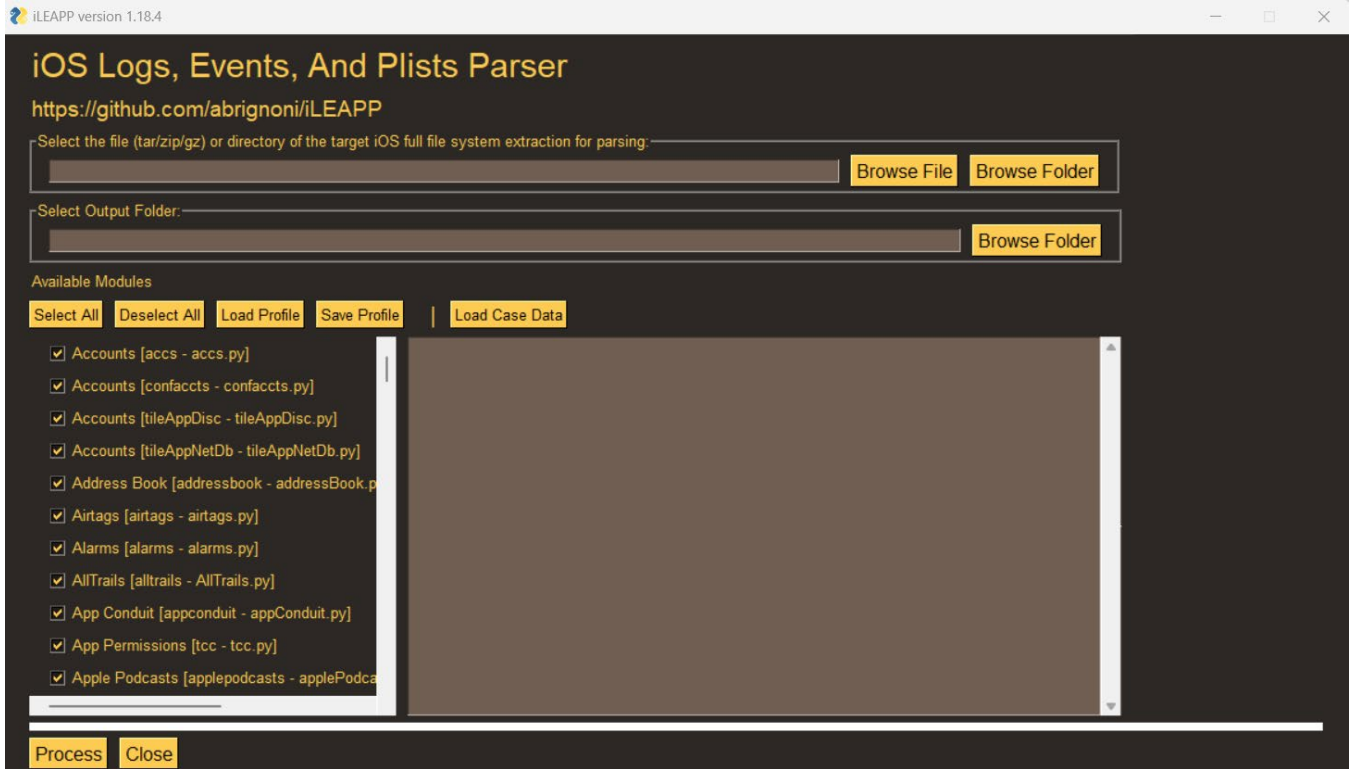
Help

```
$ python ileapp.py --help
```



SET UP AND USE

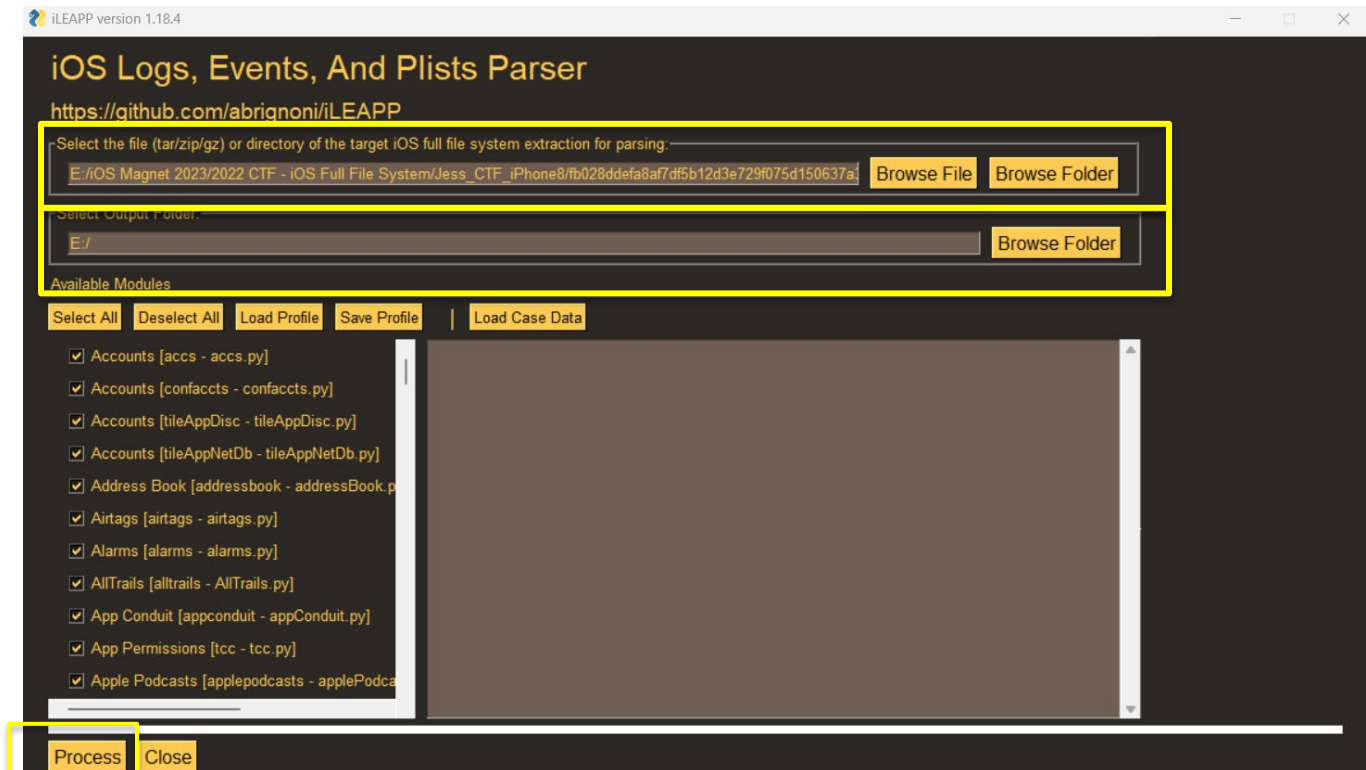
Once the GUI command is ran, the iLEAPP screen will pop up and should look like this.





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.



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 screenshot displays the iLEAPP version 1.18.4 application window. The main interface is titled "iOS Logs, Events, And Plists Parser" and includes a GitHub link. It features input fields for selecting a file or directory and an output folder. A list of available modules is shown on the left, with various checkboxes. The right side of the window displays a log of processing activities, including "sms [sms] artifact started", "applewifiplist [appleWifiPlist] artifact started", and "Report generation Completed". A "Processing completed" dialog box is overlaid on the main window, showing the report name "D:\iLEAPP_Reports_2023-03-29_Wednesday_112533\index.html" and an "OK" button. At the bottom of the application window, there are "Process" and "Close" buttons.



The index.html will automatically load.

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.














> iLEAPP_Reports_2023-03-29_Wednesday_174216

Name	Date modified	Type	Size
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
App 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

Name	Date modified	Type	Size
 Files App - iCloud Server Items.html	3/29/2023 5:44 PM	Chrome HTML Document	27 KB
 fsChachedData.html	3/29/2023 5:44 PM	Chrome HTML Document	596 KB
 Gmail - Offline Search.html	3/29/2023 5:44 PM	Chrome HTML Document	1,010 KB
 Health - Provenances.html	3/29/2023 5:44 PM	Chrome HTML Document	27 KB
 Identity.html	3/29/2023 5:44 PM	Chrome HTML Document	27 KB
 index.html	3/29/2023 5:44 PM	Chrome HTML Document	949 KB
 Intents - 663528486816806.html	3/29/2023 5:44 PM	Chrome HTML Document	40 KB
 iOS Notifications.html	3/29/2023 5:44 PM	Chrome HTML Document	329 KB
 Items.html	3/29/2023 5:44 PM	Chrome HTML Document	51 KB
 iTunes Backup Information.html	3/29/2023 5:44 PM	Chrome HTML Document	27 KB
 Keyboard Application Usage.html	3/29/2023 5:44 PM	Chrome HTML Document	29 KB
 Keyboard Dynamic Lexicon.html	3/29/2023 5:44 PM	Chrome HTML Document	27 KB
 List.html	3/29/2023 5:44 PM	Chrome HTML Document	28 KB