HEXORDIA MOBILE FORENSIC ANALYSIS (HMFA)

Dates and time: TBD

Location: TBD

Jessica Hyde	Jessica@Hexordia.com

General Information

DESCRIPTION

This course is designed to prepare students to conduct mobile forensic analysis. This course will cover fundamentals of mobile forensics including timestamp analysis, SQLite, PLists, and device preservation. The course will then look at Android and iOS analysis.

COURSE MATERIALS

System Requirements:

- Any computer with an internet connection capable of watching live stream video will be able to view the lectures in this class. Students will need a headset and microphone.
- We recommend systems with the latest Intel/AMD CPU, 8GB RAM, 250GB of disk space to participate in lab content.
- Some tools are Windows only; however, a Windows Virtual Machine will work.

DOWNLOADS:

The following forensic images will be needed by students for labs in the course. Please download these.

- Hickman Android 12 image
  - https://digitalcorpora.org/2022/09/06/new-android-10-and-11-images/
  - d9ded3a93b976fba38789cf81dffd114
- 2022 CTF – iOS Full File System.zip
  - https://cfreds.nist.gov/all/MagnetForensics/2022iOS15FullFileSystemMagnetCTF
  - md5 4FDC02C7104350B7086F0CEFD8937E52

The following tools will be necessary for the course. Additional tools of value are listed on the final page. Please download and install these prior to the course start. ***Please note that this course is using python version 3.11 due to restraints within iLEAPP.**

- autopsy-4.21 64bit.msi

  - https://www.autopsy.com/download/
  - Version 4.21 md5 17a89c39f978ed2cbe7dc15f5b4d382b
- ALEAPP-main.zip
  - https://github.com/abrignoni/ALEAPP
  - Version 3.1.8 md5 3cd3e524538a45ca98e2bec83e2e3787
- iLEAPP-main.zip
  - https://github.com/abrignoni/iLEAPP
  - Version 1.18.6 md5 d3b095069dff518d2f9e591cded38f74
- python-3.11.6 amd64.exe
  - https://www.python.org/downloads/
  - Version 3.11.6 md5 4a501c073d0d688c033d43f85e22d77e

LEARNING OBJECTIVES

- Understand different types of forensic images available from mobile devices.
- Understand critical elements of mobile device preservation.
- Decode common mobile timestamps by hand or with the use of freeware tools.
- Create mobile data test sets for purposes of verification and validation.
- Conduct analysis of Android and iOS devices to include multimedia, communications, geolocation, and system artifacts.
- Identify and analyze unsupported 3rd party applications from mobile devices.
- Conduct comparative analysis.

COURSE SCHEDULE

Subject to change based on individual class pacing needs

Day	Topic
Day 1 AM	Mobile Forensics Fundamentals
Day 1 PM	Mobile Device Preservation
Day 2 AM	Mobile Timestamp Fundamentals
Day 2 PM	SIM Analysis
Day 3 AM	SQLite Forensics and Android Analysis
Day 3 PM	Android Analysis continued
Day 4 AM	PList Forensics and iOS Analysis
Day 4 PM	iOS Analysis continued
Day 5 AM	Mobile Analysis Methodology and 3rd Party App Parsing
Day 5 PM	Comparative Analysis

TOPIC DETAILS

Mobile Forensic Fundamentals

Terminology of mobile forensics, basic components, identifiers, possible data sources, artifact types, mobile forensic image types, similarities, and differences between mobile and computer forensics.

MOBILE DEVICE PRESERVATION

Methods to maintain data integrity, network isolation, device states, and documentation.

MOBILE TIMESTAMP FUNDAMENTALS

Manual decoding of timestamps and fundamentals such as nibble swapping and endianness are covered as well as different timestamp formats a forensic examiner may encounter in their analysis of Android and iOS mobile devices. Includes multiple parsing and decoding exercises.

SIM Analysis

Basics about Subscriber Identity Module (SIM) cards. Discussed different formats, identifiers, SIM card clones, SIM card imaging and data found on SIM Cards. Includes multiple parsing and decoding exercises.

SQLite Analysis

Analysis of SQLite databases to include parsing of data from binary large objects (BLOBs) and the use of SQL queries.

ANDROID ANALYSIS

Understanding and location of Android artifacts to include multimedia locations, timestamps, communication applications, geolocation, and system artifacts. Includes hands-on labs.

PLIST FORENSICS

Analysis of PLists encountered in the analysis of iOS and Mac devices, including Binary PLists, XML PLists, NSKeyedArchive, and more.

iOS Analysis

Understanding and location of Android and Google Takeout artifacts to include multimedia locations, timestamps, communication applications, geolocation, and system artifacts. Includes hands-on labs.

MOBILE ANALYSIS METHODOLOGY AND 3RD PARTY APP ANALYSIS

Methodology for mobile forensic analysis of unsupported applications and artifacts. It teaches a 5-part methodology; Discover, Test, Parse, Find, and Script. These are necessary skills to parse 3rd party applications. Includes hands-on labs and exercises.

CREATING MOBILE TEST DATA

Methodology for creating mobile test data is taught to include use cases for data generation, data set development, pre-release activities, use of existing datasets, maintenance of data sets, and emulation.

COMPARATIVE ANALYSIS

Utilize comparative analysis tools to understand their function in app analysis and testing. Hands-on exercises to learn to detect changes in artifacts.

TOOLS

All tools utilized in this course are Open Source, Freeware, or trial versions of inexpensive (under $100) tools. It is intended that students learn concepts and techniques that are non-vendor specific. The analysis skills taught in this course can be replicated in commercial tools. As this course is not tool specific, utilities may be added or removed as new resources are available.

https://www.autopsy.com/download/	4.21.0	autopsy-4.20.0-64bit.msi
https://github.com/den4uk/andriller	3.6.3	andriller-master.zip
https://www.python.org/downloads/	3.11.3	python-3.11.2-amd64.exe
https://github.com/abrignoni/ALEAPP	3.1.8	ALEAPP-main.zip
https://github.com/abrignoni/iLEAPP	1.18.7	ILEAPP-main.zip
https://github.com/abrignoni/RLEAPP	1.0.4	RLEAPP-main.zip
https://www.doubleblak.com/Software/Epoch/Epoch_2_1_4_0.zip	2.1.4.0	Epoch 2_1_4_0.zip
https://www.digital-detective.net/dcode/	5.5.21194.40	DCode-x86-EN-5.5.21194.40.exe
https://sqlitebrowser.org/dl/	3.12.2	DB.Browser.for.SQLite-3.12.2-win64.msi
https://www.staff.hs-mittweida.de/~pawlaszc/fqlite/	2.0	FQlite.zip
https://download.cnet.com/HxD-Hex-Editor/3000-2352_4-10891068.html	2.4	HxDSetup.zip

https://www.slavasoft.com/hashcalc/	2.02	hashcalc.zip
https://sourceforge.net/projects/mbox-viewer/	1.0.3.38	mbox-viewer.exe-v1.0.3.36.zip

https://www.digital-detective.net/download/download.php?downcode=ae2znu5994j1lforlh03	5.5.21194.40	DCode-x86-EN-5.5.21194.40
https://download.mobiledit.com/mobiledit!/setup_SIMClone_3_3_1.exe	3.3.1	setup_SIMClone_3_3_1.exe
https://github.com/osmocom/pySIM	1	N/A
https://github.com/PicciMario/SIMBrush	0.1	N/A
https://vidstromlabs.com/freetools/simquery/	1.2	SIMquery.exe
https://vidstromlabs.com/freetools/undeletesms/	1.1	undeletesms.exe
http://www.mediafire.com/file/0e7zn8fiy2ahwr1/GSIMReaderApp_V1.0.7.2.rar/file	1.0.7.2	GSIMReaderApp_V1.0.7.2.rar
https://www.sublimetext.com/	4143	sublime_text_build_4143_x64_setup.exe
https://www.dekart.com/free_download	3.3	SIMManager.exe
https://developer.android.com/studio	2023-3.1.20	android-studio-2022.3.1.20-windows.exe
https://gsmusbdrivers.com/download/adb-fastboot-drivers/	1.4.3	adb-setup-1.4.3.zip
https://github.com/topjohnwu/Magisk/releases	25.2	N/A
https://github.com/topjohnwu/MagiskManager/releases	5.8.1	N/A
https://secure-appldnld.apple.com/QuickTime/031-43075-20160107-C0844134-B3CD-11E5-B1C0-43CA8D551951/QuickTimeInstaller.exe	7.7.9	QuickTimeInstaller.exe
http://www.ithmbconverter.com/plist/plistexplorer.zip	1	plistexplorer.zip
http://www.icopybot.com/plisteditor_setup.exe	2.5	plisteditor_setup.exe
https://github.com/ydkhatri/MacForensics/tree/master/Deserializer	N/A	MacForensics-master.zip
https://www.doubleblak.com/Software/Mushy/Mushy_2_5_0_0.zip	2.5	Mushy 2_5_0_0.zip
https://storage.googleapis.com/google-code-archive-downloads/v2/code.google.com/iphonebackupbrowser/iphonebackupbrowser-r38.zip	1.2.0.6	iphonebackupbrowser-r38.zip
https://github.com/ydkhatri/MacForensics/tree/master/IOS_KTX_TO_PNG		ios_ktx2png.exe
https://www.7-zip.org/download.html	23.01	7z2301-x64.exe

https://www.doubleblak.com/Software/ArtEx2/ArtEx2_2_7_4_0.zip	2.7.1.0	ArtEx2 2_7_1_0.zip
https://github.com/mdegrazia/SQLite-Deleted-Records-Parser	V1.1	SQLite-Deleted-Records-Parser-master.zip

ONLINE TOOLS AND SITES REFERENCED IN THIS COURSE:

https://www.imei.info
https://everymac.com/ultimate-mac-lookup/
https://www.epochconverter.com/
https://gchq.github.io/CyberChef/
https://www.dcode.fr
https://www.iban.com/dialing-codes
https://appledb.dev/device-selection/
https://ijailbreakguide.com/
https://canijailbreak.com/
https://ipsw.me
https://www.mockaroo.com/
https://generatedata.com/
https://proton.me/
https://www.unrealperson.com/
https://digitalcorpora.org/
https://cfreds.nist.gov/
https://discord.com/channels/820387839518441502/824317694714183710