CREATING MOBILE FORENSICS LABS FOR EDUCATIONAL PURPOSES

Ahmed Elgazar

A Capstone Project Submitted to the
University of North Carolina Wilmington in Partial Fulfillment
of the Requirements for the Degree of
Master of Science

Department of Computer Science
Congdon School of Supply Chain, Business Analytics, and Information Systems

University of North Carolina Wilmington

2023

Approved by

Advisory Committee

_____	_____
Ulku Clark	Geoffrey Stoker

_____
Ronald J. Vetter, Chair

TABLE OF CONTENTS
(Insert Automatic Table of Contents)

ABSTRACT

Creating Mobile Forensics Labs for Educational Purposes. Elgazar, Ahmed, 2023. Capstone Paper, University of North Carolina Wilmington.

Mobile forensics has become heavily relied on in legal cases especially since the rise of smartphones. The amount and nature of data stored on them makes the forensics process feel almost like a time travel experience. Many forensics tools and course materials were developed to improve the forensics process. In this paper, I discuss the process of creating a similar experience. A new Canvas module was created to train UNCW students on advanced mobile forensics techniques. Students are walked through the thought process of a digital investigator to find hidden artifacts in seized smartphones to collect incriminating evidence. The Canvas module has 3 labs, including their scenarios and deliverables, along with a quiz to guide students during their investigations.

LIST OF FIGURES

Figure Page

CHAPTER 1: INTRODUCTION

In Spring 2022, a Digital Forensics Course was offered at UNCW. The course covered multiple chapters from the textbook 'Digital Forensics, Investigation, and Response.'. While the course was taught face-to-face, the material itself and the training labs were accessible online. The course material covered a variety of Digital Forensics topics to give students a solid idea about the field, from where to start as a Digital Forensics Investigator to where to go as a professional in the field. It did this by exercising the principles and concepts covered in the book in an online virtual environment. Although the book covered almost all concentrations of Digital Forensics, it did not offer much hands-on practice on Mobile Forensics.

I address such needs in my project by offering educational labs which include the following capabilities and features:

1) Online availability using Horizon as a hosting environment.
2) Application of Mobile Forensics techniques using the Cellebrite Software Suite.
3) Lab instructions, including learning objectives, tools used, and deliverables.
4) Progression of difficulty, Easy, Medium, and Advanced, to cover different skill levels.

The benefits of such project include:

1) Supplementing the courseware of the Digital Forensics course offered at UNCW.
2) Avoiding security risk by installing certified software on the campus network.

CHAPTER 2: REVIEW OF LITERATURE REVIEW AND ANALYSIS

2.1 Researching Vendor Solutions

Digital Forensics, D.F, is a cyber security field that is categorized under the defensive security domain. It is more on the reactive than proactive side of cyber security and is an integral part of the Incident Response process in which security teams respond to or investigate security incidents such as data breaches. Mobile forensics is but one part of that bigger field of digital forensics. It has become a more wanted skill in the job market since smart phones became more involved in security incidents and are considered as valuable pieces of evidence in legal cases.

JB Learning. In Spring 2022, A Digital Forensics course was offered at UNCW that utilized an online learning platform called 'JB Learning' which was launched in 2010. On such platform, users are offered the opportunity to learn and practice DF techniques by selecting one of two plans, either buy a bundle that includes a digital copy of a book and access to their online virtual labs, or just buy access to the labs to practice D.F techniques. This is a traditional approach of online learning platforms which gives students some flexibility with the options available (see Figure 1).

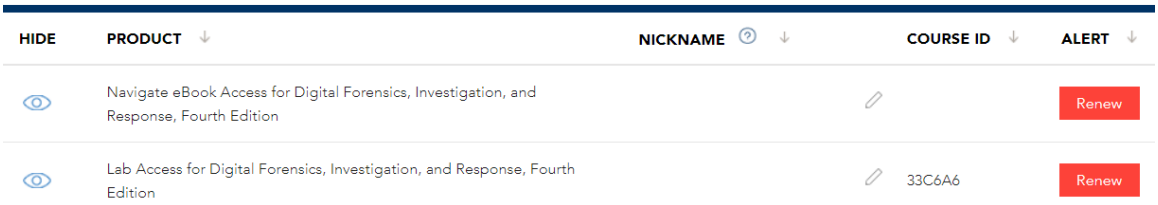


Figure 1. JB Learning's eBook & Lab access plans

After being granted access to the virtual labs, a student would open a dedicated virtual session over RDP (remote desktop protocol) and a lab guide that includes the lab's objectives, walkthrough instructions, and deliverables (see Figure 2).

After completing a module, the student should have learned new concepts and techniques, applied them in a guided manner, and submitted the deliverables of each module as they finish each step of the lab instructions. The last deliverable of each lab would be an unguided task to test the skills of students and how much they learned. The content was targeting beginners' level in D.F and did not dive deep into advanced techniques.

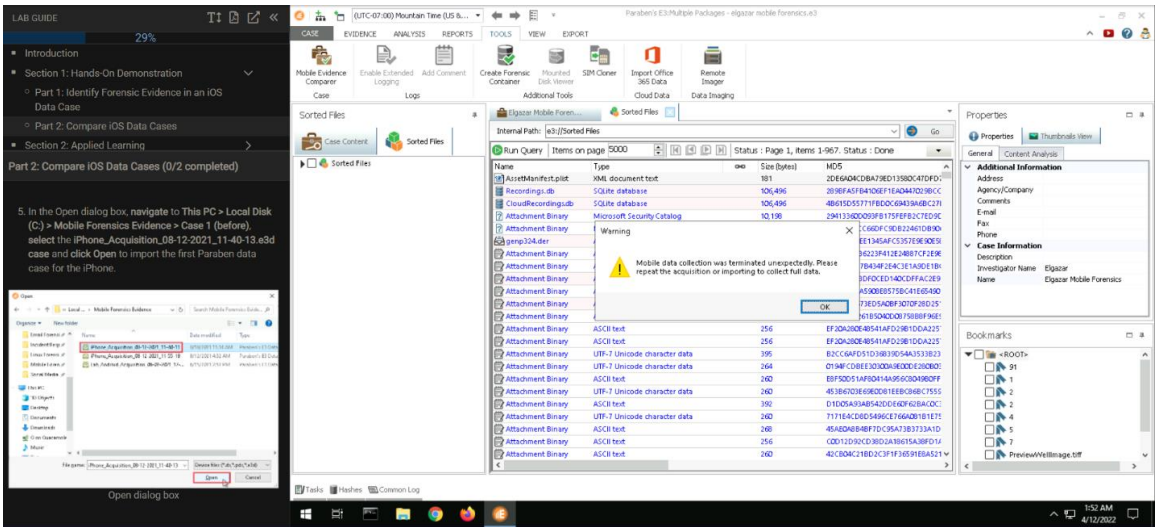


Figure 2. Example of lab instructions on JB Learning.

TryHackMe.com. In 2018, TryHackMe (THM) was launched by two cyber security enthusiasts, Ashu Savani and Ben Spring, as a personal training project and later expanded to become one of the biggest cyber security training platforms with a community of more than 1 million security enthusiasts. Their approach is to teach cyber security through short, gamified real-world labs. They host more than 500 virtual labs that cover most cybersecurity domains and all skill levels. The labs are hosted on their servers and are accessed either through an RDP session from the web browser, or if the user prefers to connect to the lab from their local machine, THM's VPN (Virtual Private Network) servers. The labs use a gamified approach to keep the whole experience

interactive and fun. A user would go through the labs following a step-by-step instructions web page and as soon as they finish a task, the user would submit their answer and receive streak points followed by another challenge or task (see Figure 3).

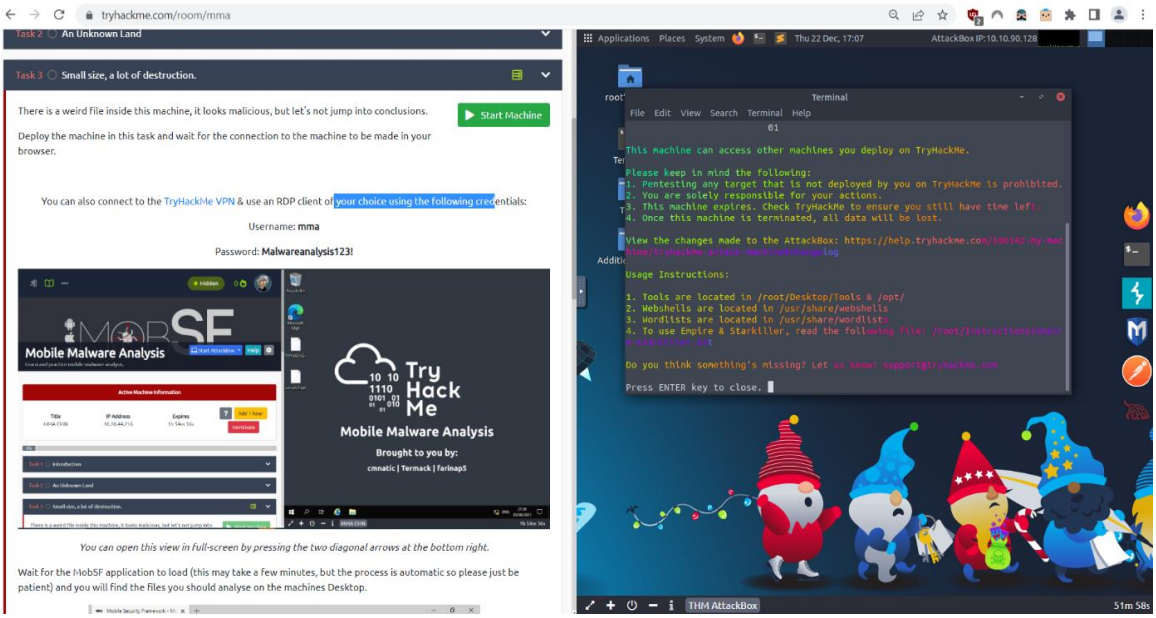


Figure 3. An example of a mobile forensics challenge on TryHackMe.

Also, there are ‘Blackbox’ challenges for which users do not receive many instructions to test users with advanced skills. In addition to the online hosted labs, they offer downloadable challenges in which the user downloads a compressed file and runs it locally. They allow community members to submit and share with the community their own challenges on the platform. They have ‘Learning Paths’ to teach different cybersecurity domains from beginner to Intermediate and advanced levels. Also, they host ‘Capture The Flag’ competitions, CTFs, with big prize pools to encourage beginners in the field to join. One new feature they added is to allow college instructors to host their cybersecurity classes on their platform. They offer them full access to the platform’s features, which makes teaching a hassle-free and a fun experience for the teacher and the

students alike (see Figure 4).

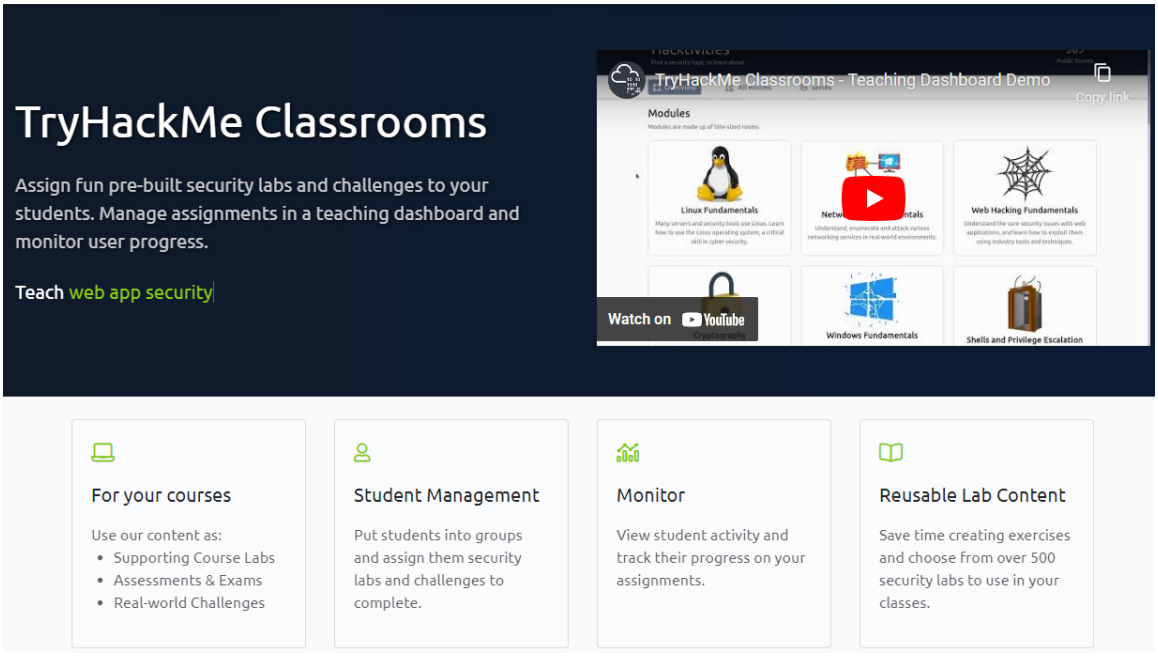


Figure 4. THM's Classroom features for educational institutions

Although they cover many cybersecurity domains in the training labs, they heavily lack labs on Mobile Forensics. Only 2 labs on the platform cover Mobile Forensics.

*CyberDefenders.org***.** CyberDefenders was found in 2019, by Muhammad Alharmeel and Ahmed Shawky because they noticed the absence of user-friendly training platform for 'Blue Teams'. Blue Teams refers to the security teams that focus on defensive rather than offensive security, which is the focus of Red Teams. So, unlike TryHackMe and JB Learning, CyberDefenders' content is focused only on the defensive side of cybersecurity. The challenges offered cover topics such as Mobile Forensics, Linux Forensics, Malware Analysis, Threat Intelligence, etc. Also, CyberDefenders's labs are not accessed online, rather users download the challenges, decompress, and start their analysis journey locally on their machines, then they are asked to provide answers to questions posted on the platform to receive points, like THM. Included with every task, a

simple scenario, a few instructions, and the tools which a Security Analyst in a real-world scenario would use. Also, write-ups are provided by other users who have solved that challenge already, but points are not given if the user decided to read the write-up (see Figure 5).

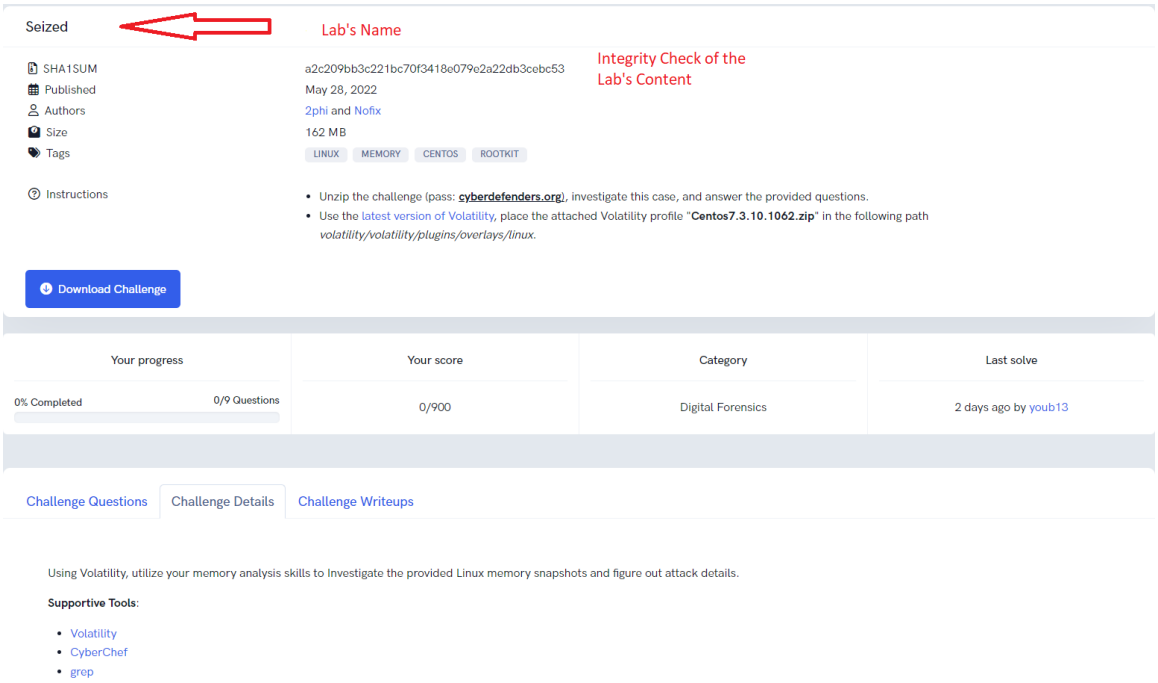


Figure 5. An example of a downloadable challenge on CyberDefenders

The platform offers one course, Certified CyberDefender, for almost $400, which covers the basics of DF and goes even more in depth on other topics such as Threat Hunting and Emulation. Finally, they offer security enthusiasts to host their own CTFs on another platform of theirs called BlueRing, dedicated exclusively for CTF competitions. Also, BlueRing is free for educational institutions.

HackTheBox.com. HackTheBox (HTB), is probably the biggest online platform for cyber security training. It was founded in 2017 and now after 5 years they have gained over 1.5 million users and offer over 450 training labs. Now, there are professors from 853 universities around the world who register their students for HTB training. So

far, they have supported and co-hosted more than 150 Capture the Flags events. Their labs model is remarkably like TryHackMe's in that they offer both online challenges and the opportunity to download and solve tasks locally. Users can either access their online labs or connect to their VPN servers and use their personal machines. The labs take a gamified approach to encourage users to solve more challenging tasks. After completing a task, the user would submit 'flags' found inside the virtual labs.

Until recently, to join the platform users had to hack their way in to prove that they have the basics of web security, which was like a Hollywood movie experience. Just last year, they removed that challenge and allowed user to register the normal way and later created their own HackTheBox Academy to offer different learning paths, which cover multiple cyber security domains, to fill in the knowledge gap of their own users and expand their project to beginners who felt intimidated.

Although HackTheBox offers training for most cybersecurity domains, it has a lack of training materials when it comes to mobile forensics. They lean more towards offensive security and offer training labs on how to break the security of mobile phone technologies.

2.2 Challenges and Opportunities

From previous research, I could not find many online platforms that offered us what we want for the lab environment of the new Digital Forensics course. In addition to the lack of labs on mobile forensics, the tools used in them are either open-source tools such as Autopsy, or its command line alternative, the Sleuth kit, or commercial tools like Paraben's E3 Forensics kit. What I could utilize in a future upgrade of the project is to host the labs on one of these platforms, but that would require more rigorous work to solve the problem of licensing, because the Cellebrite's software suite is dependent on

network dongles and software license to work. This obstacle would stand in the way of such a future update. Another possible update is to create a course webpage with submission forms like what is found on the other platforms, instead of students submitting their answers in a pdf form, or on Canvas.

CHAPTER 3: METHODOLOGY

3.1 Project Setup and Solution Approach

For the project to be effective and to avoid the limitations of the other solutions, the labs must be accessible online to allow students to work on assignments and submit them at their own pace. For this reason, the setup of my project is going to leverage the existence of a university's hosted virtualization solution such as Horizon to host the training materials and the labs.

1) Using Group Access Controls, students enrolled in the Digital Forensics class would automatically gain access to the labs and can access it outside of class and from off campus.
2) Labs' updates can be applied uniformly.
3) Any maintenance requests will be assisted and performed by the IT team on campus.

In this project, I am using 3 tools from Cellebrite's Forensics Suite which consists of the following:

1) UFED4PC: is used to access, extract, and collect data extensively from almost all types of smart phones and categorize it for later use by investigators. The extraction process is depicted in Appendix A.
2) Physical Analyzer: is used for analysis and examination. Also, by using a plugin such as "Virtual Analyzer" a student can emulate the smartphone from which the evidence was extracted and can browse as if they were using the original smartphone. A demonstration of Physical Analyzer is shown in Appendix B.
3) Inspector: is used for analyzing and correlating artifacts, media

categorization, Optical Character Recognition, etc. A student can create a case using evidence extracted from UFED4PC and further analyze the files, filter artifacts, look for hidden evidence in images using OCR, create timelines of events, and share the case with peers using the 'Portable Case' feature.

3.2 Labs Objectives, Instructions, and Deliverables

Delivery Method:

- Included with each lab, a pdf that contains the lab's objectives, instructions on how to approach the task, and the deliverables to guarantee that the student can get the most benefit out of the experience.

Scenario Design:

- Easy tasks should be straightforward and do not need more than 2 steps to complete. Flags in this category will be given 5 points.
- Medium tasks may require more steps to complete and the combination of more than 1 tool or technique. Additionally, hints would be provided. Flags in this category will be given 10 - 15 points.
- Hard tasks may include rabbit holes and more advanced techniques should be researched online. Flags in this category will be given 20 - 30 points.
- One important practice to keep in mind while designing the scenarios is to not include rabbit holes in the easy tasks, and to keep the unnecessary rabbit holes to the minimum in the hard ones.

3.3 Evaluation

There are two main stakeholders for my project, the instructor of the Digital Forensics course and the students of the course. To make sure that the project's results

fulfill the requirements and are acceptable to the stakeholders I listed an example of user stories which if met successfully that means the completion of such requirements.

1) Instructor's stories:
    a. As an instructor, I want to give my students the opportunity to access, extract, and analyze hidden information on smart phones, so that I would expand the domain of the course.
    b. As an instructor, I want to give my students access to the labs throughout the semester, so that they work at their own pace.
2) Students' stories:
    a. As a student, I want to follow a set of instructions to guide me through the labs, so that I can learn the basics of Mobile Forensics.
    b. As a student, I want to access the labs online from my home network, so that I do not have to use up space on my local machine.

This guarantees the prioritization of the features which I want to include in my project and be able to set a clear criterion of which requirement is completed successfully and which is not. After setting up the labs, they will be uploaded to Horizon and access will be granted to the instructor and students of the Digital Forensics course for feedback and final updates.

CHAPTER 4: RESULTS AND DISCUSSION

4.1 Final Product

The final product of the supplementary course material is very promising and meets most of the proposed features. As proposed, a new module was added to Canvas which includes a 'tools overview' section to demonstrate the capabilities of each Cellebrite tool, 3 lab pages, each includes a level of difficulty, learning objectives, brief scenario, tasks, skills earned, list of deliverables, helping references, and a grading rubric, 3 quizzes which students can use to navigate and analyze the extracted evidence and look for flags to submit, 3 solution walkthrough videos which would be published after students solve the 3 quizzes, a 'Resources' page to help students in their search for answers and to improve their techniques, and finally a 'Setup Technical Instructions' page that includes instructional videos of how to configure the network settings to run Cellebrite's products using a network dongle and fully utilize the products' available 30 licenses in a class setting. The new Canvas module is depicted in Appendix D.

4.2 Lessons Learned

Creating educational materials takes a lot of time and mental effort, especially if the material requested is technical in nature and relatively new to the instructors themselves. Personally, I had to learn a lot about the tools and techniques I present in the videos to deliver it in an understandable manner. Also, the material should be up to date and presented in a fun and engaging way to improve students' learning process. That is why I changed the delivery method from pdf files to video walkthroughs. While developing "lab 1," I understood how hard the process is. I used an old iPhone 6, and had to populate the phone with dummy settings, applications, images, etc. to make the scenario as believable as possible. The laborious process and the nature of the content

made me choose the option of utilizing previously used datasets, for “lab 2,” medium difficulty, and “lab 3,” hard difficulty, such as Cellebrite’s own CTF’s datasets from 2021 and 2022.

In learning the tools, I learned how thorough and powerful forensics techniques are. I was amazed by the amount and nature of data saved on my personal phone. From associated user accounts to system and applications’ notifications, this data is very persistent on smartphones. For example: UFED4PC extracted a phone number I previously used even after performing a factory reset for the sake of building the labs. When I was researching “lab 2” solutions, I learned that this level of data persistence is also possible for Android phones (Hickman, n.d.). An investigator can find the same data saved across multiple applications’ databases, and “plist,” property list, files. So, it is almost impossible to permanently delete data related to an event in the phone’s timeline without leaving a trace.

Another takeaway is the computing resources required to perform both extraction and analysis of data. At least a half terabyte of disk space is needed to save the extracted datasets, at least 4-cores processor, and 16GB of RAM is preferred when using examination tools such as “Carve locations” and enrichment engines such as “Media Classification” and “Cryptocurrency” in Physical Analyzer. Computing resources consumption is shown in Appendix E.

4.3 Limitations

The Cellebrite toolkit for this project included 1 network dongle to license both UFED4PC and Physical Analyzer, and 1 network dongle to license Inspector. Each with 30 licenses available. So, I planned to host the final product on Horizon to fulfill the availability requirements, but I had it, Cellebrite tools and extracted datasets, hosted

locally on university-owned laptops, because Cellebrite's network dongles do not support licensing over virtual servers. The second option was to attach the dongle to a physical host in the on-campus Datacenter, but this would be a security risk and would affect the stability of the virtual machines running on that physical host. Shown in Appendix F.

Another obstacle was the lack of clear instructions on how to configure the dongles network-wide to allow multiple users to run the tools, so I had to contact Cellebrite's technical support to work with to configure the dongles in my home network first before deploying it on campus. Even after receiving Inspector's network configuration instructions, they were not accurate and I troubleshooted the issue myself until I solved it. Depending in Appendix F Inspector's license server instructions.

While Cellebrite keeps adding helpful features and updates to their tools, it is not efficient to have to uninstall the previous version and download a whole latest version and install it from scratch each update. For example, UFED4PC V7.60.0.222_ 202212061156's zip file is 5.625 GB.

A personal limitation is that I have not developed educational materials before, so I looked for inspiration in the courses that I enrolled in previously. Starting by understanding the topics covered, then understanding the students' needs and skills, then defining the learning objectives, then choosing the delivery format, and finally developing the content and refining it, and that helped me know where to begin.

The use of Cellebrite's datasets comes with its own challenges. Given that the datasets are from a CTF, it had many tricky questions which required advanced knowledge. This inspired me to study the official write-ups, solutions, and other write-ups by the digital forensics community members of the challenges to be able to explain the thought process behind each answer in the walkthrough videos. (Pagano, n.d.).

CHAPTER 5: CONCLUSIONS AND FUTURE WORK

5.1 Conclusions

Overall, the project was a great learning experience both in technical and academic aspects. It utilized a collection of commercial, high-grade software used by law enforcement agencies in real cases. This offers cybersecurity students at UNCW the opportunity to be job-ready if they wish to work as digital forensics investigators. Its effectiveness is yet to be known until it is offered with main course material in the upcoming semester, Fall 2023, and only then updates to the labs' materials can be done.

5.2 Future Work

There is enormous potential for this project to outgrow the digital forensics course and be its own stand-alone course where students can be Cellebrite certified. This can be possible by incorporating more Cellebrite tools into the labs' material such as Cellebrite Reader and Virtual Analyzer, which does not require a separate license and easily integrated with other tools such as Physical Analyzer. The utilization of the hardware toolkit, such as cables and adapters, included with the software products to develop more real-world scenarios. Depicted in Appendix G is the content of the toolkit bag.

Online deployment of the labs on Horizon would give more flexibility and access to students to solve the challenges as a medium or hard challenge can easily take more than the class time to solve, depending on the student's skills. So, dedicating a physical host in the Datacenter, or a dedicated server in Congdon Hall building to which students connect over UNCW's VPN would solve the issue, but more experimenting is needed.

Utilizing on-campus resources such as the Office of Distance Education and eLearning to improve the content and delivery method of the labs. Additionally, I registered for a Faculty Fellowship Program sponsored by the National Cybersecurity

Training & Education Center, NCYTE, to learn more on creating educational academic material.

REFERENCES

Blue Team CTF Challenges. CyberDefenders. (n.d.). Retrieved December 9, 2022, from https://cyberdefenders.org/

"Cellebrite 2021 CTF - Google Drive." *Drive.google.com*, drive.google.com/drive/folders/1aPuq-c1U1txOBJQIA688u6bFzdz59FJ6.

"Cellebrite Reader | Share Digital Intelligence Reports across Departments." *Cellebrite.com*, cellebrite.com/en/reader/.

"CFReDS Portal." *Cfreds.nist.gov*, cfreds.nist.gov/all.

Cyber security training. TryHackMe. (n.d.). Retrieved December 8, 2022, from https://tryhackme.com/

Easttom. Chuck, PhD, DSc, Med. (2022). Digital Forensics, Investigation, and Response.

Hacking Training. Hack The Box. (n.d.). Retrieved December 8, 2022, from https://www.hackthebox.com/

Jones & Bartlett Learning. Main. (n.d.). Retrieved December 9, 2022, from https://www.jblearning.com/

link, Get, et al. *Cellebrite CTF 2021 - Beth's IPhone*. www.stark4n6.com/2021/10/cellebrite-ctf-2021-beths-iphone.html.

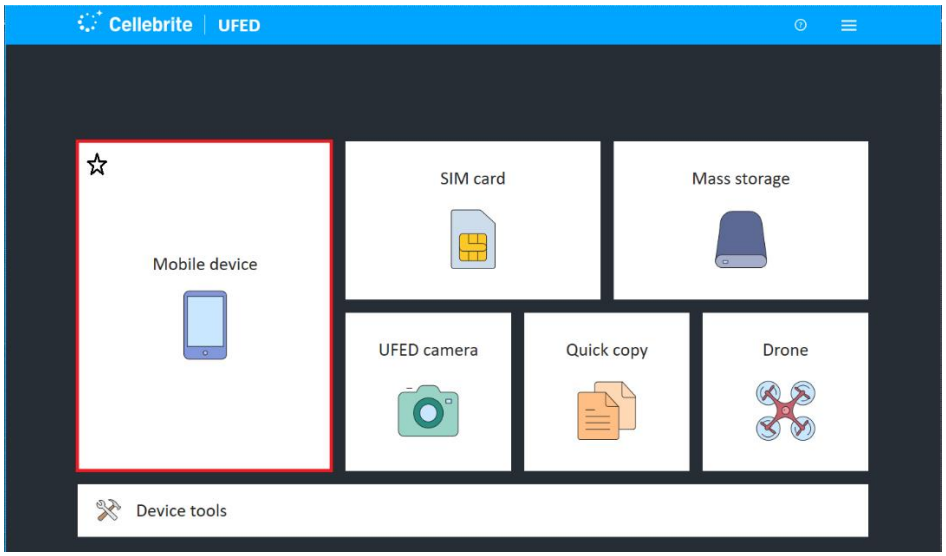
"NCyTE Center - Faculty Fellowship Program: Orientation Workshop." *Ncytecenter.wildapricot.org*, ncytecenter.wildapricot.org/event-5153124.

"New to Online Teaching: DEeL: UNCW." *Uncw.edu*, uncw.edu/oel/new/index.html.

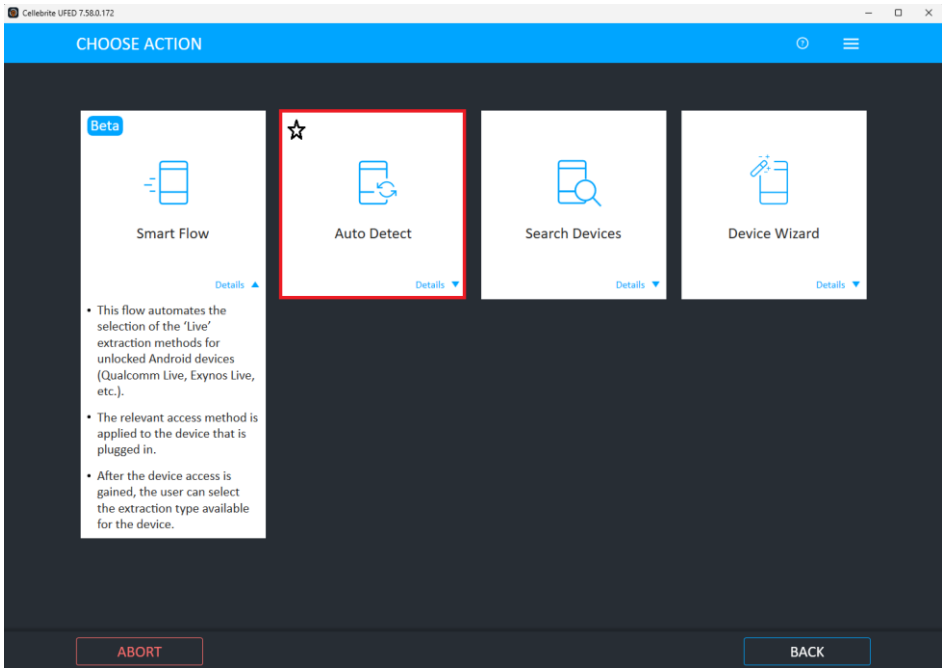
Thoughts From a Digital Forensics Practitioner. TheBinaryHick. (n.d.). Retrieved March 26, 2023, from https://thebinaryhick.blog

APPENDIX A

UFED4PC's Extraction Process:

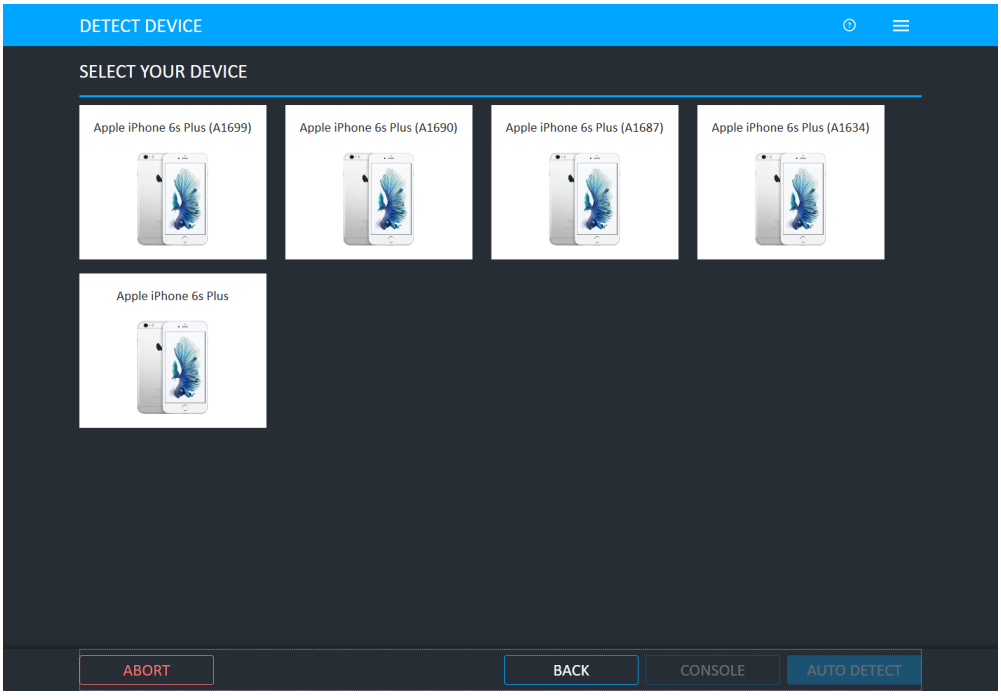


Selecting Mobile device extraction to start the process.

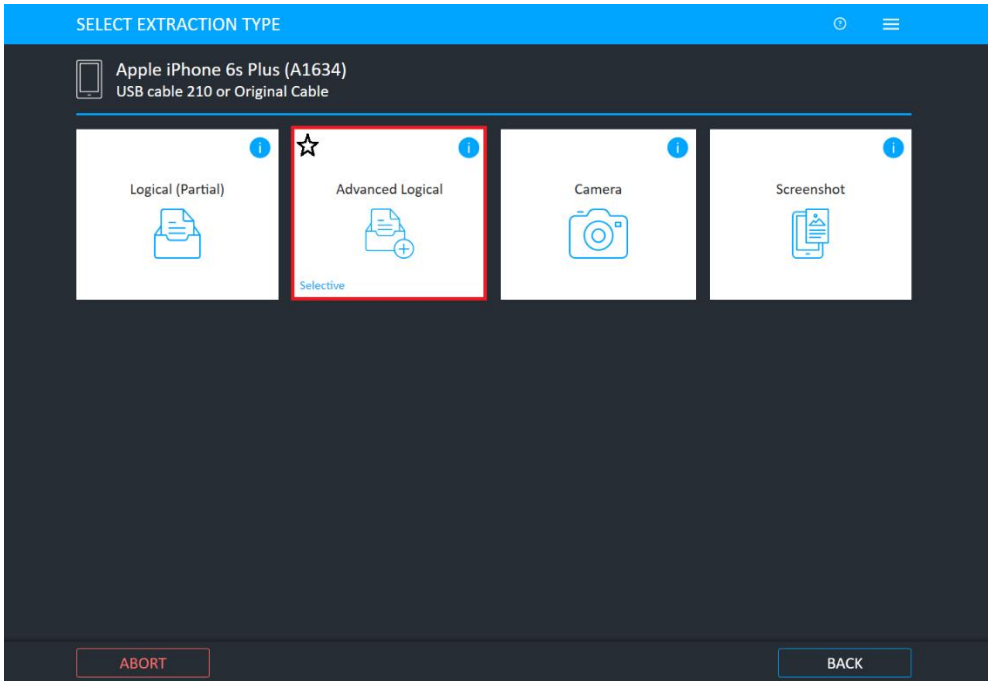


Selecting the suitable detection method.

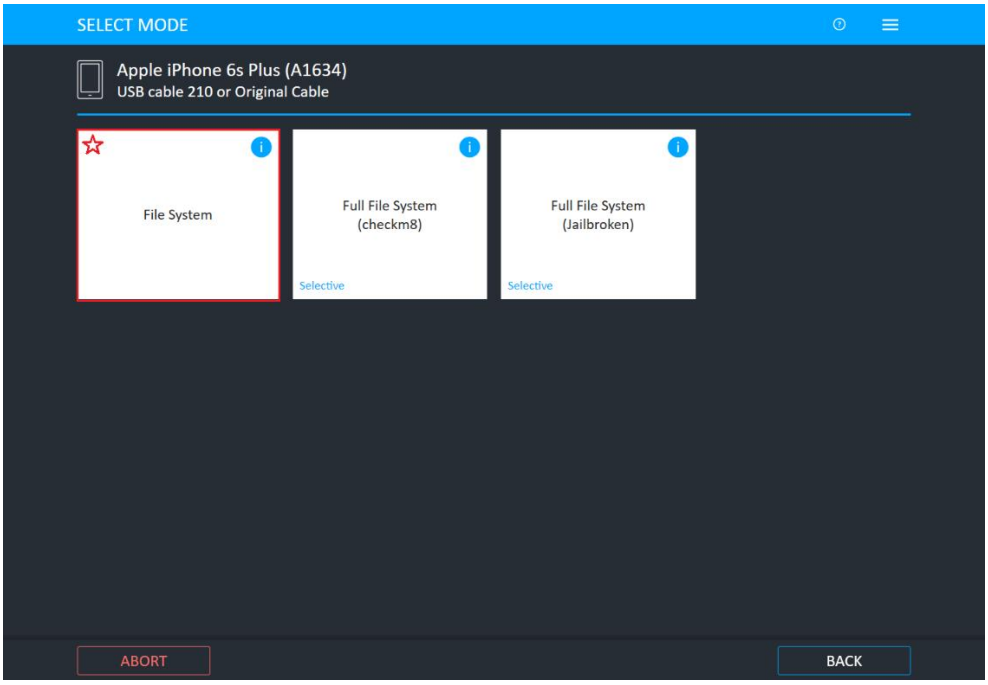
Auto detection instructions.



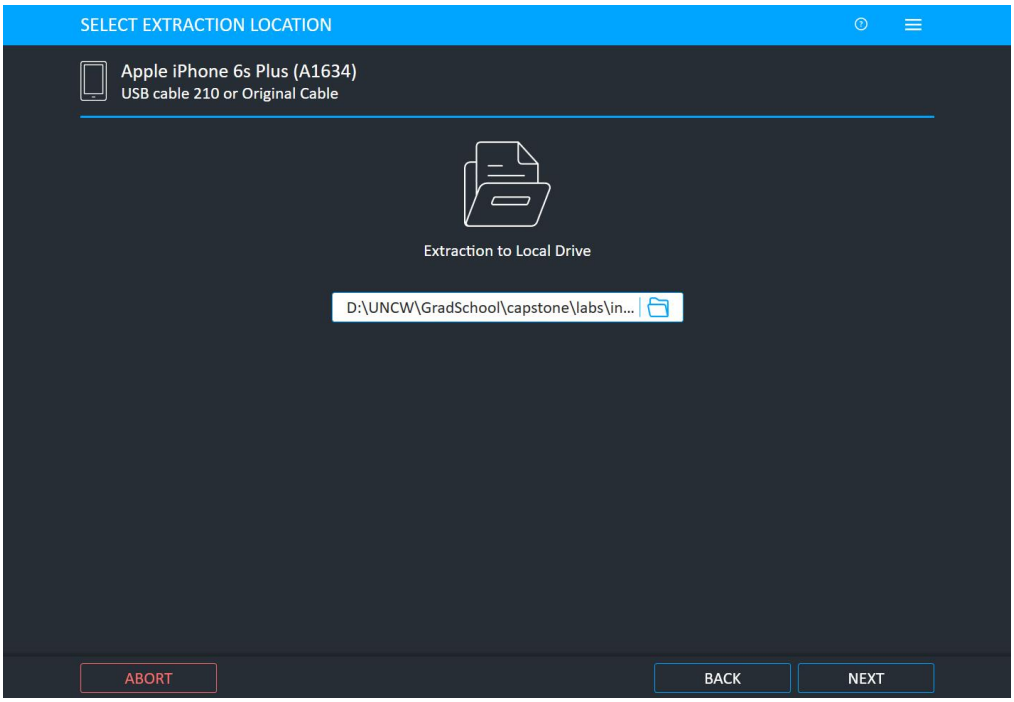
Selecting the proper model number.



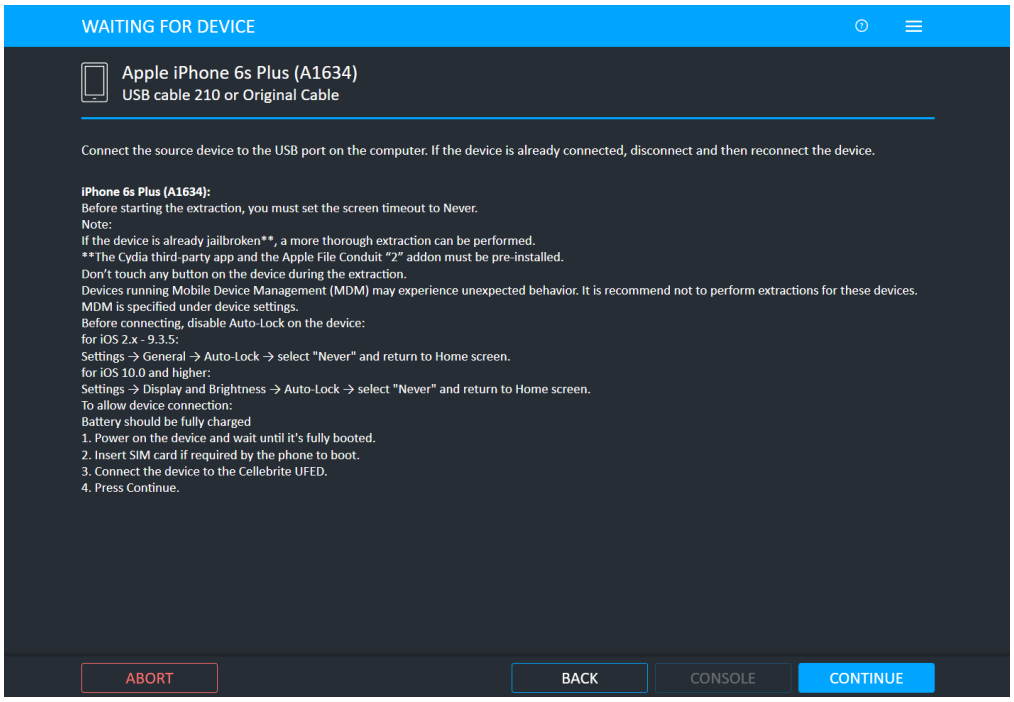
Selecting Advanced Logical to extract the most amount of data.



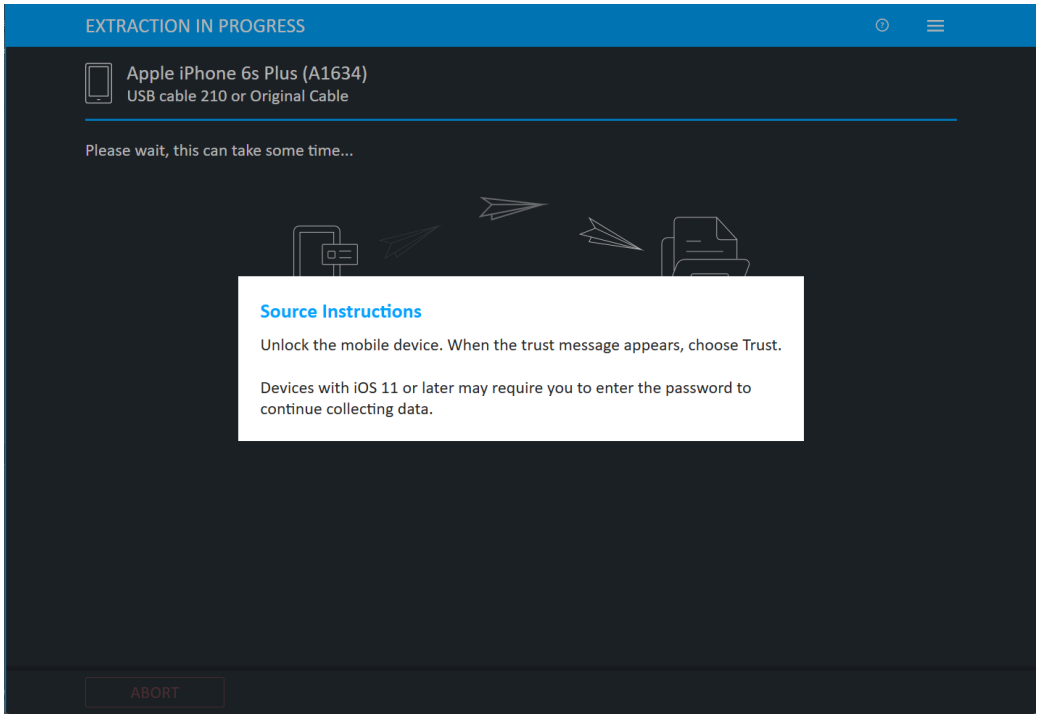
Selecting the suitable extraction method.

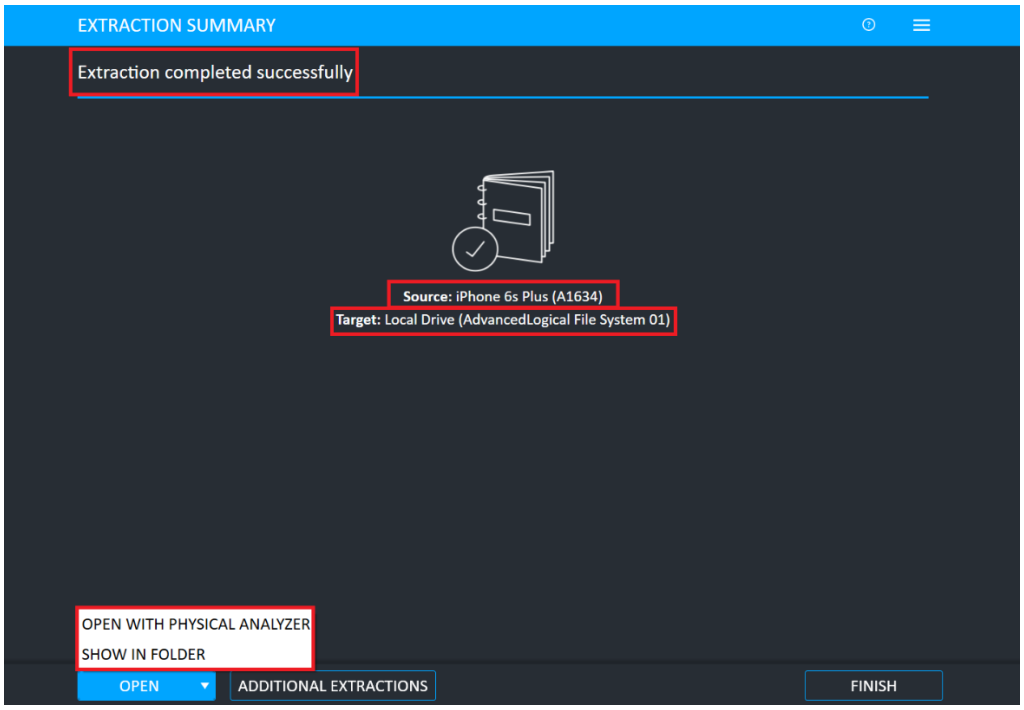


Selecting extraction location.



Connection establishing instructions.

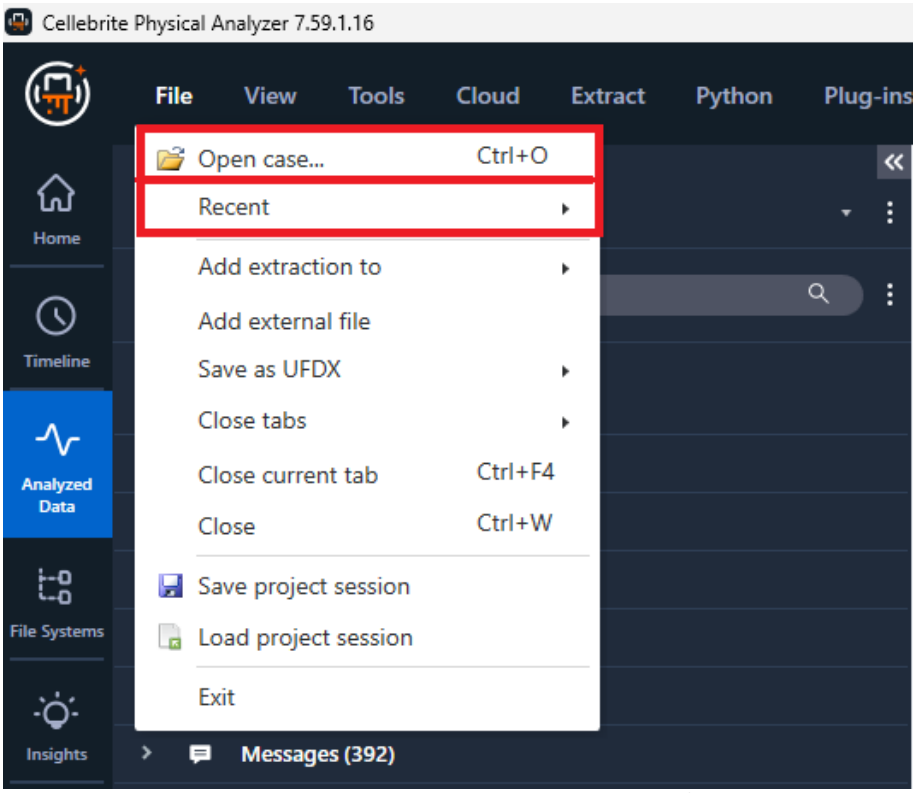




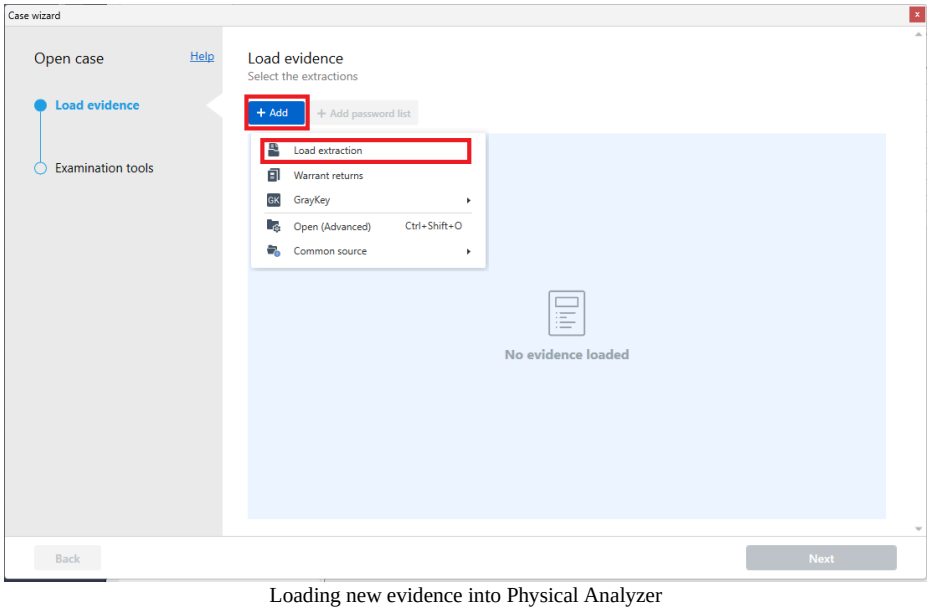
Investigators can either choose to load extracted evidence into Physical Analyzer or Extract more evidence from the same device.

APPENDIX B

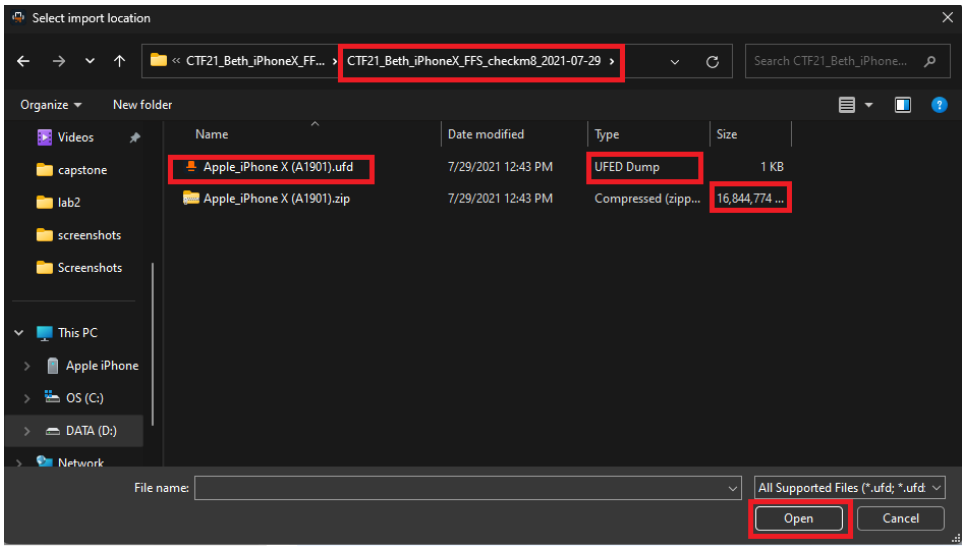
Physical Analyzer Demo



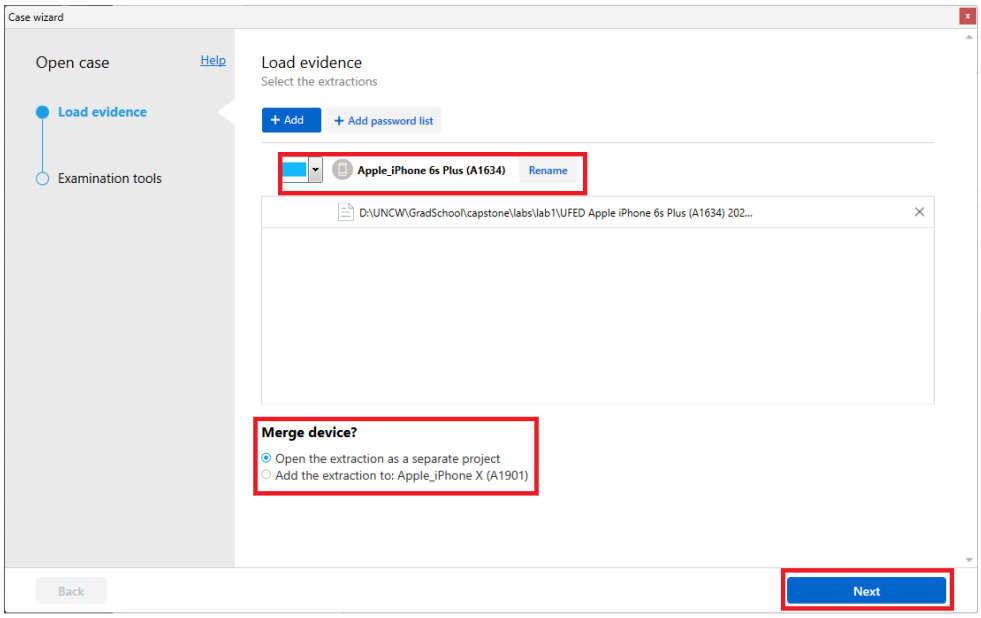
Investigators can either choose to load new evidence or load evidence from recent cases



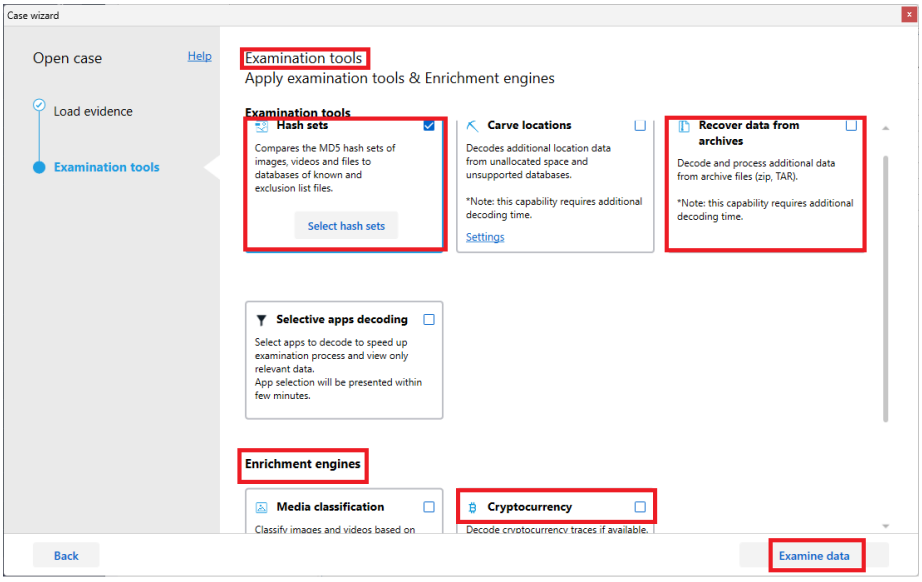
Loading new evidence into Physical Analyzer



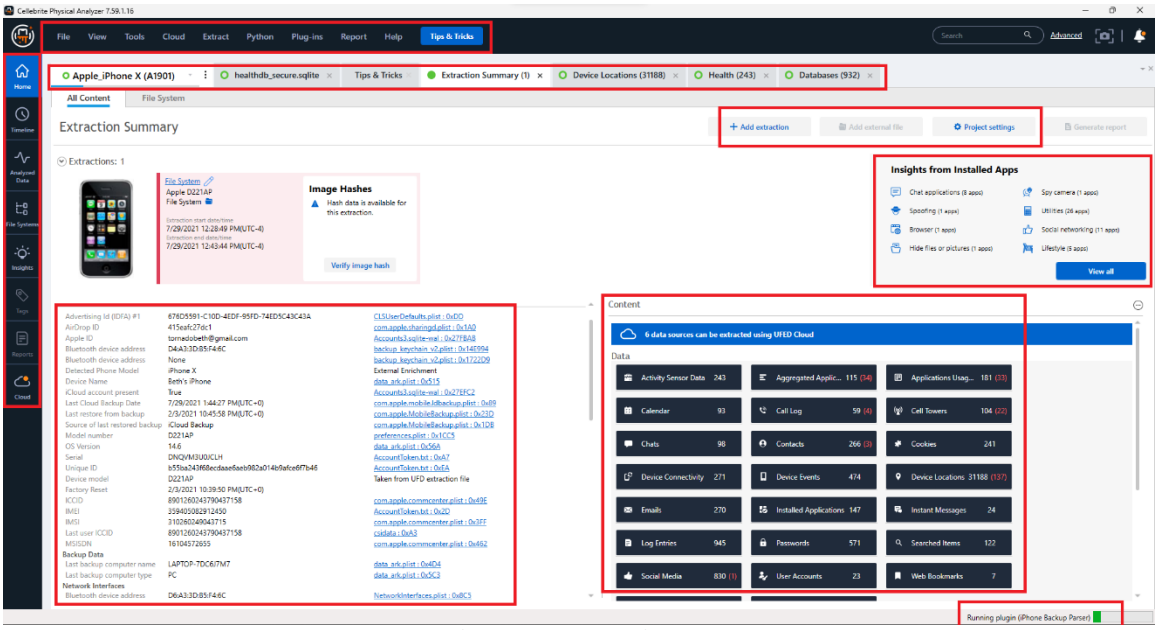
Loading UFED extraction



Evidence Configuration



Examination tools and enrichment engines

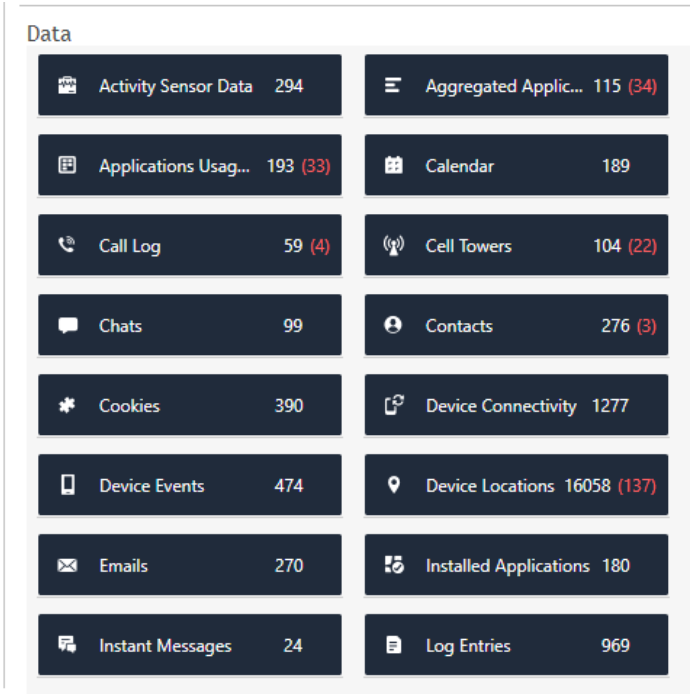


Main Screen of Physical Analyzer after loading evidence.

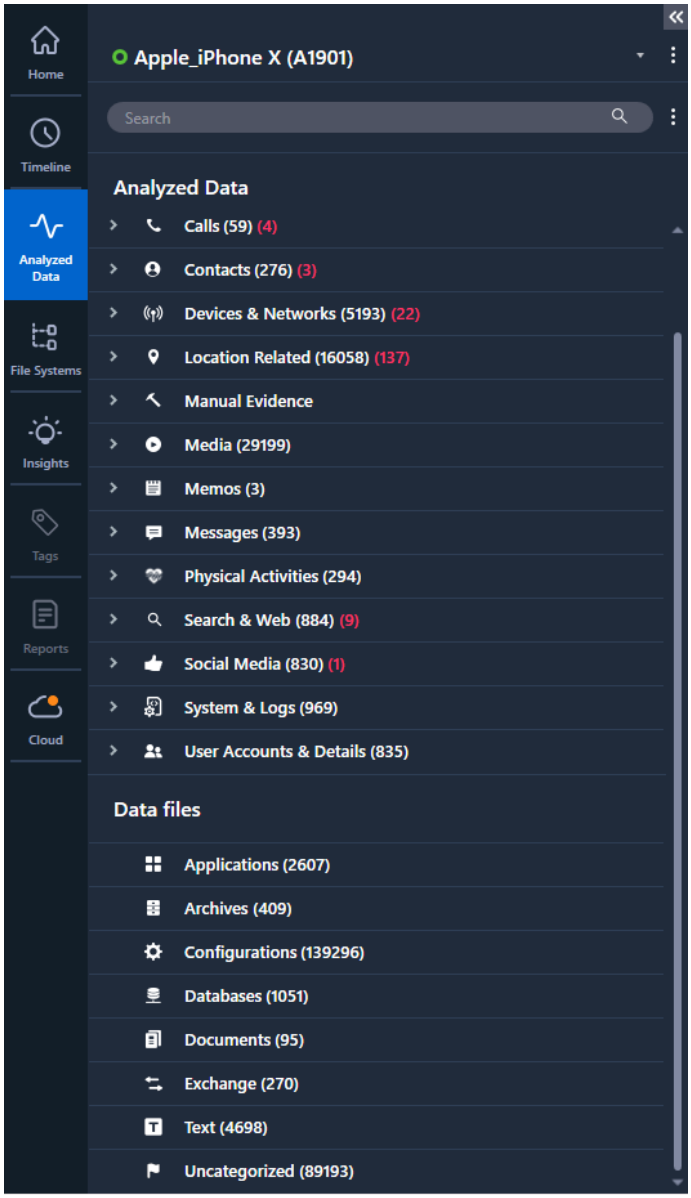
File System

Advertising Id (IDFA) #1	676D5591-C10D-4EDF-95FD-74ED5C43C43A	CLSUserDefaults.plist : 0xDD
AirDrop ID	415eafc27dc1	com.apple.sharingd.plist : 0x1A0
Apple ID	tornadobeth@gmail.com	Accounts3.sqlite-wal : 0x27FBAB
Bluetooth device address	D4:A3:3D:B5:F4:6C	backup_keychain_v2.plist : 0x14E994
Bluetooth device address	None	backup_keychain_v2.plist : 0x1722D9
Detected Phone Model	iPhone X	External Enrichment
Device Name	Beth's iPhone	data_ark.plist : 0x515
iCloud account present	True	Accounts3.sqlite-wal : 0x27EFC2
Last Cloud Backup Date	7/29/2021 9:44:27 AM(UTC-4)	com.apple.mobile.ldbackup.plist : 0x89
Last restore from backup	2/3/2021 5:45:58 PM(UTC-5)	com.apple.MobileBackup.plist : 0x23D
Source of last restored backup	iCloud Backup	com.apple.MobileBackup.plist : 0x1DB
Model number	D221AP	preferences.plist : 0x1CC5
OS Version	14.6	data_ark.plist : 0x56A
Serial	DNQVM3U0JCLH	AccountToken.txt : 0xA7
Unique ID	b55ba243f68ecdaae6aeb982a014b9afce6f7b46	AccountToken.txt : 0xEA
Device model	D221AP	Taken from UFD extraction file
Factory Reset	2/3/2021 5:39:50 PM(UTC-5)	
ICCID	8901260243790437158	com.apple.commcenter.plist : 0x49E
IMEI	359405082912450	AccountToken.txt : 0x2D
IMSI	310260249043715	com.apple.commcenter.plist : 0x3FF
Last user ICCID	8901260243790437158	csidata : 0xA3
MSISDN	16104572655	com.apple.commcenter.plist : 0x462
Backup Data		
Last backup computer name	LAPTOP-7DC6J7M7	data_ark.plist : 0x4D4
Last backup computer type	PC	data_ark.plist : 0x5C3
Network Interfaces		

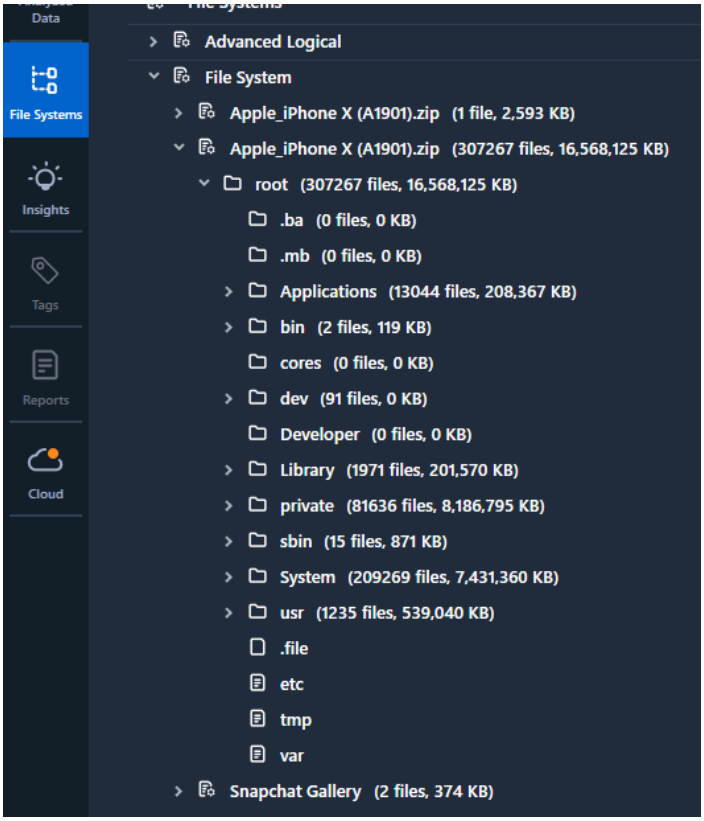
Summary of phone's information.



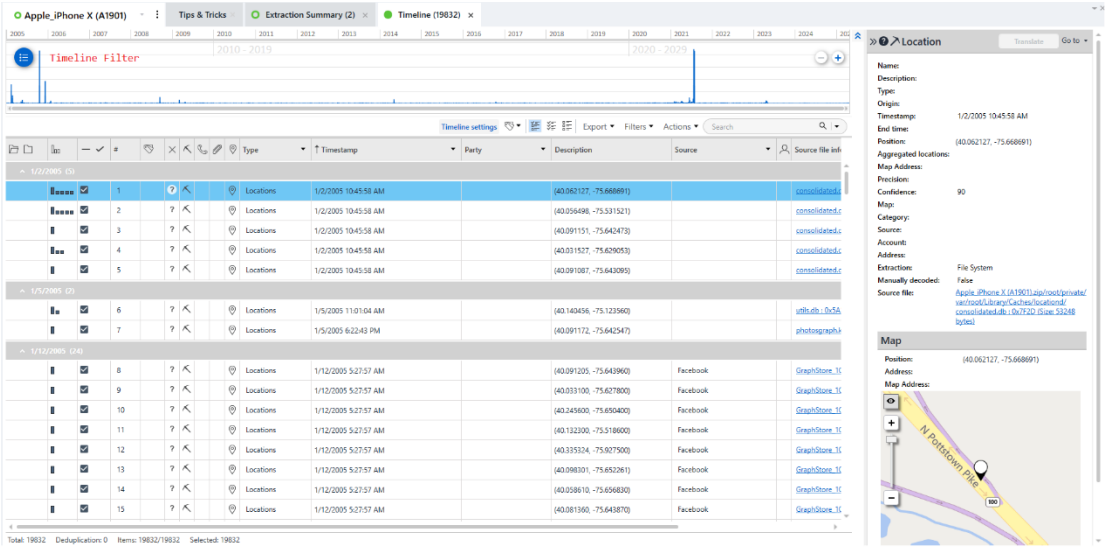
Analyzed data.



Another look at analyzed data.



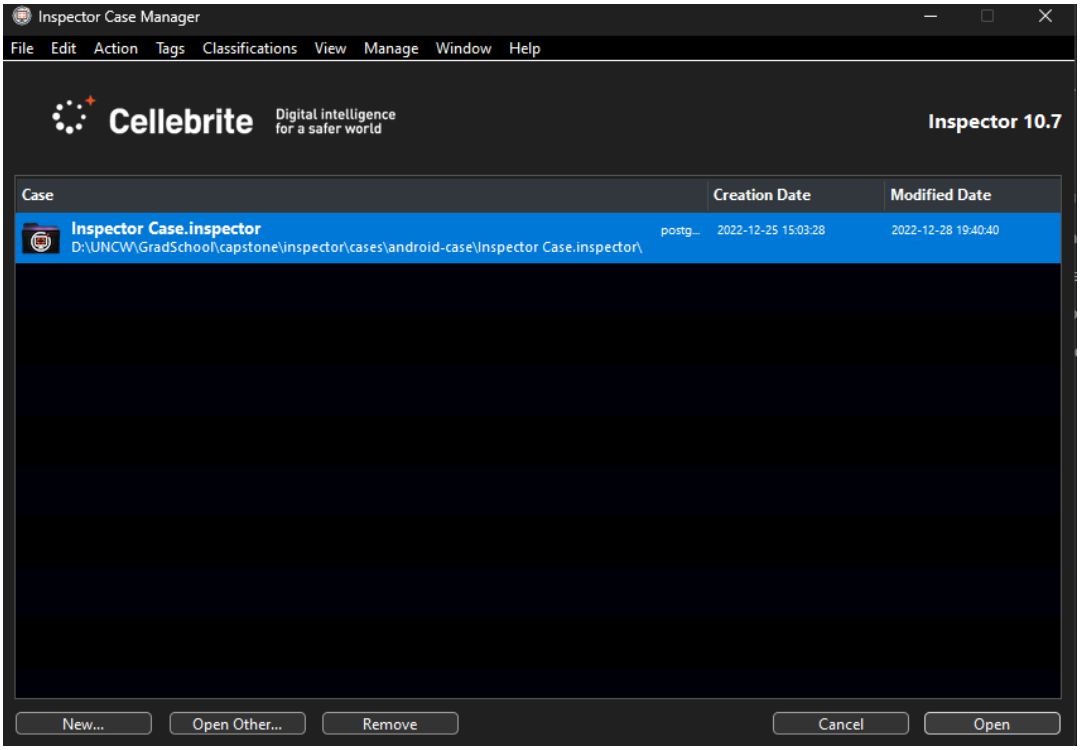
iOS File System.



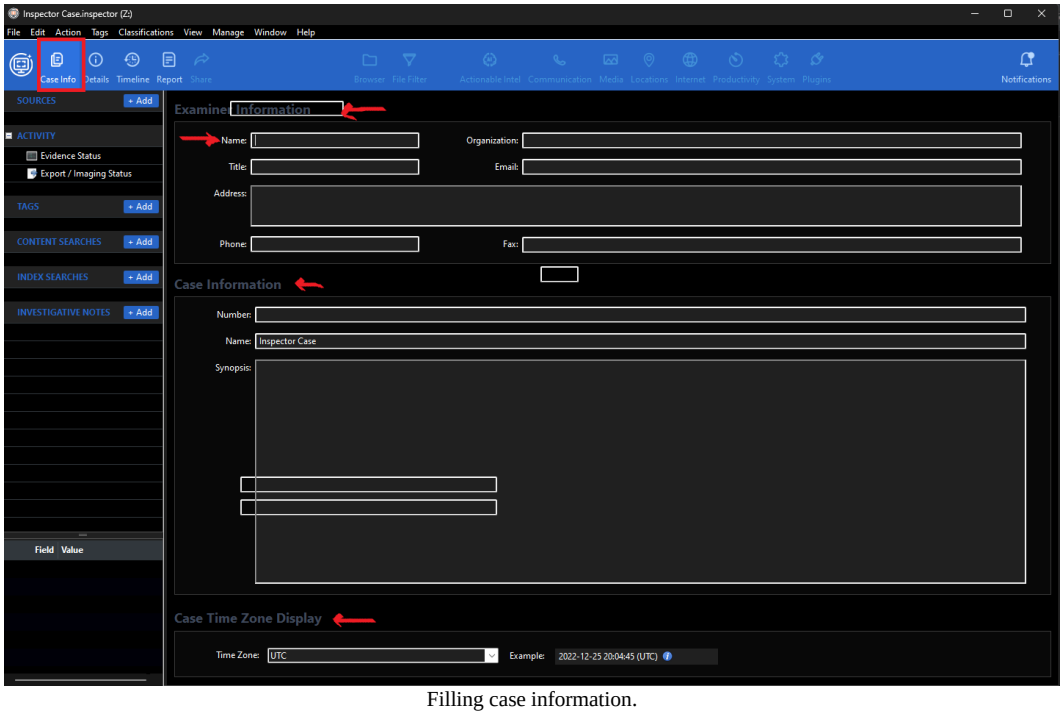
Device's Timeline.

APPENDIX C

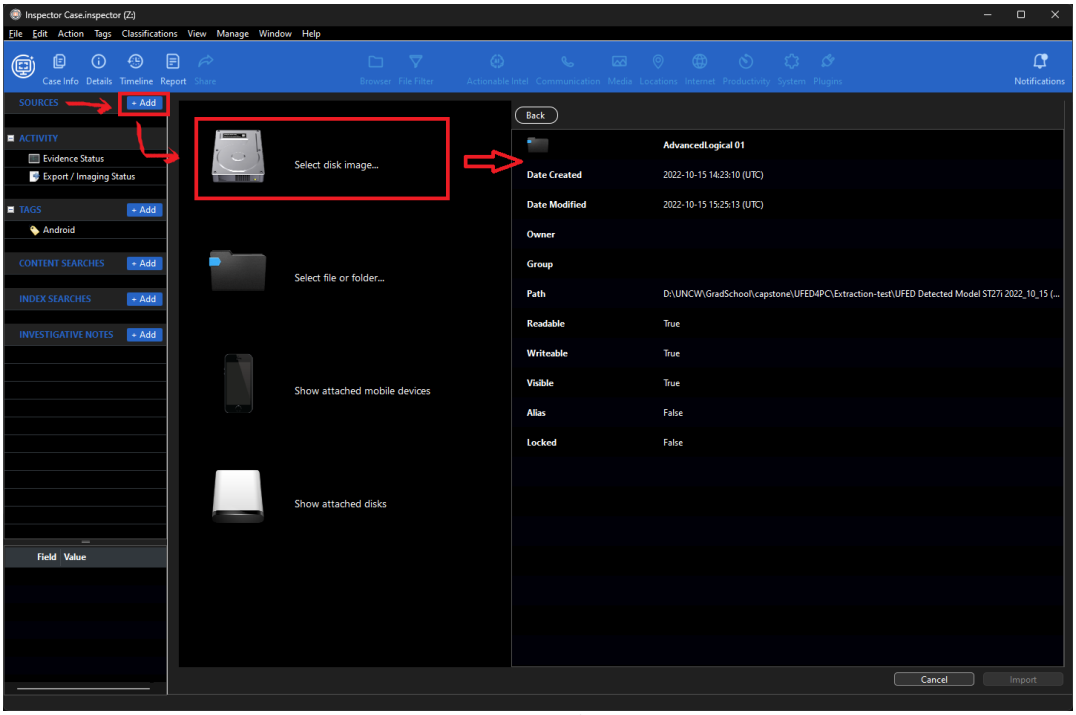
Inspector Demo



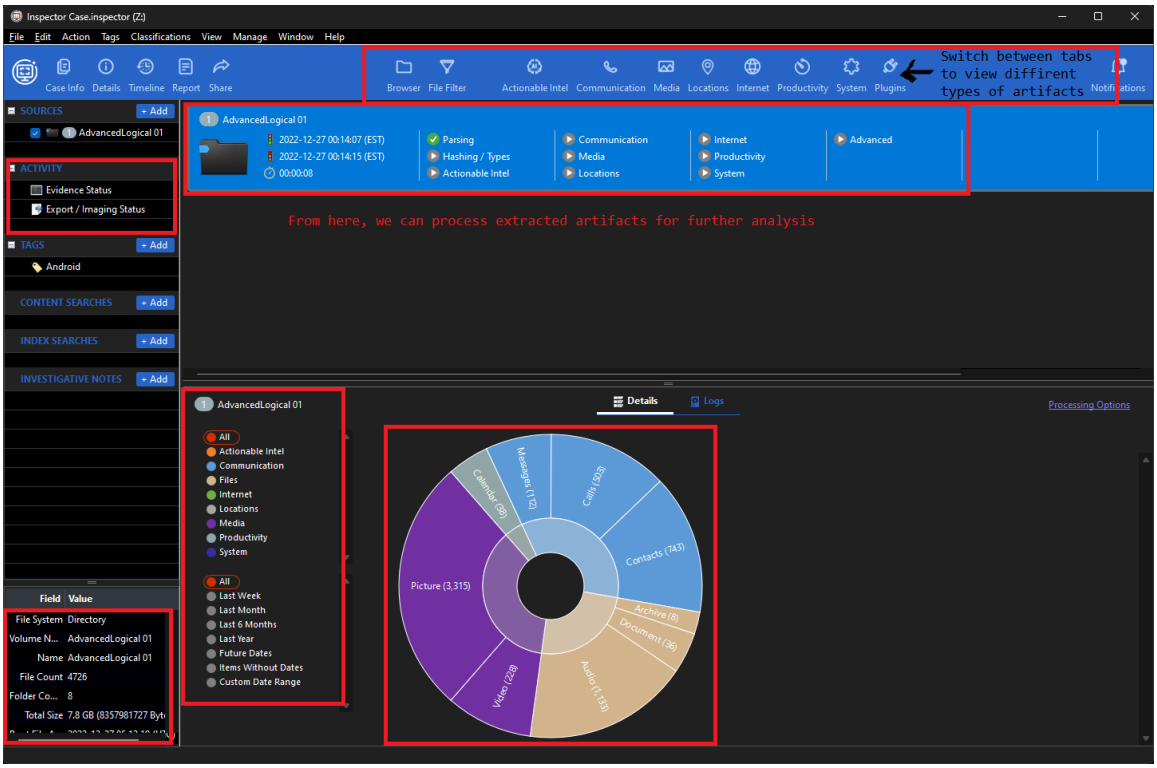
Opening a new case in Inspector.



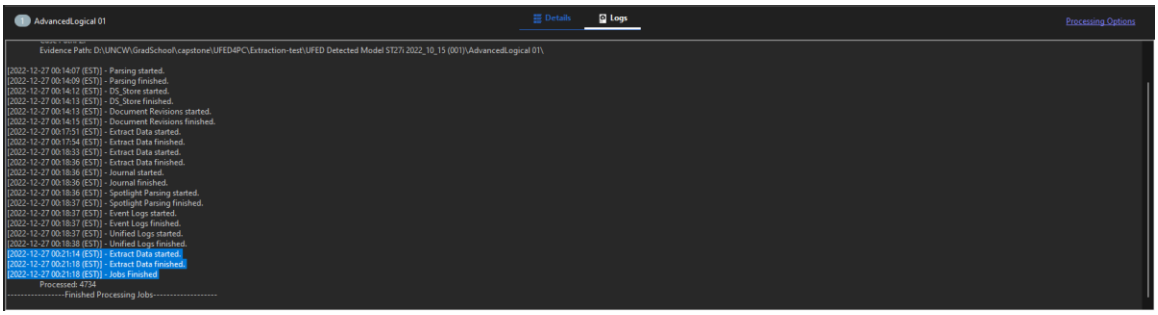
Filling case information.



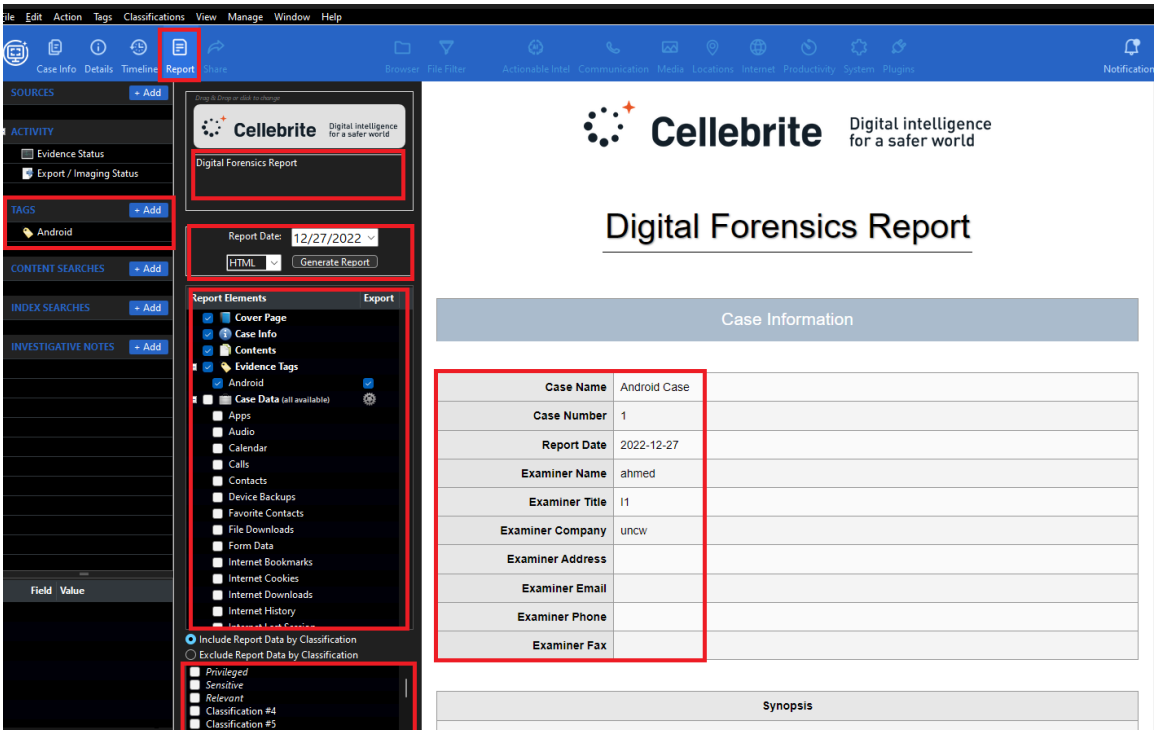
Selecting a source image for the new case.



Main screen where we can see a summary of the artifacts extracted.



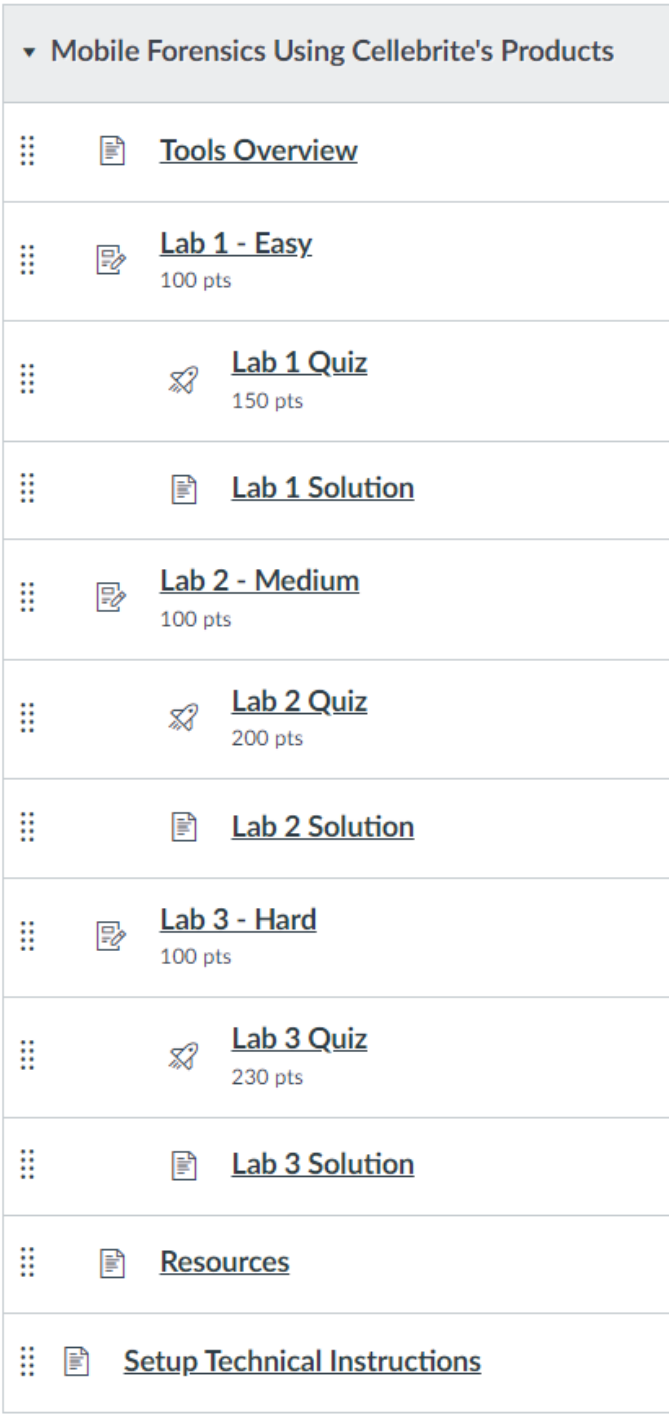
Logs of tasks started by Inspector.



Building a case report. Tags can be used to selectively generate reports.

APPENDIX D

New Canvas Module



Mobile Forensics Module's Content.

APPENDIX E

Tools Overview Page

Tools Overview

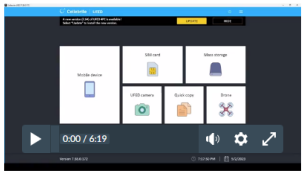
Introduction to Cellebrite Mobile Forensics Suite

Welcome to the introduction to Cellebrite's UFED4PC, Physical Analyzer, and Inspector. This guide is designed to provide a comprehensive introduction to Cellebrite's digital forensic tools for cybersecurity students. By the end of this guide, students will understand the basics of UFED4PC, Physical Analyzer, and Inspector, and how to use these tools to conduct digital forensics investigations.

Cellebrite's UFED4PC

Cellebrite's UFED4PC is a powerful digital forensic tool used by law enforcement agencies, military organizations, and private investigators to extract, decode, and analyze data from mobile devices. UFED4PC supports a wide range of devices, including smartphones, tablets, GPS devices, and drones. The tool's intuitive user interface allows investigators to quickly and easily extract and analyze data from a wide range of sources, including deleted data, call logs, text messages, emails, and social media activity.

UFED Overview:

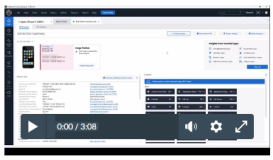


Tools Overview - UFED4PC.

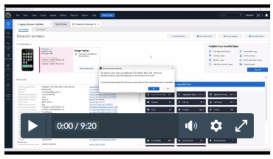
Physical Analyzer

Cellebrite's Physical Analyzer is a complementary tool to UFED4PC that allows investigators to conduct in-depth analysis of extracted data. Physical Analyzer provides a range of advanced analytical tools, including timeline analysis, social network analysis, and keyword searching. The tool also includes a range of visualization options, including charts and graphs, to help investigators better understand complex data sets.

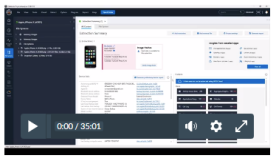
Physical Analyzer - Loading an Extraction (.ufd):



PA Overview:



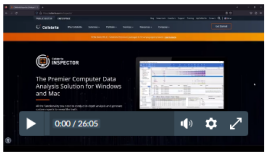
PA Demo:



Tools Overview – Physical Analyzer.

Inspector

Cellebrite's Inspector is a cloud-based tool that allows investigators to analyze and collaborate on digital evidence in real-time. Inspector provides a range of advanced analytical tools, including timeline analysis, data categorization, keyword searching, data visualization, optical character recognition, and facial recognition. The tool also allows investigators to collaborate with other team members in real-time, making it an ideal tool for complex investigations.



Tools Overview – Inspector.

APPENDIX F

Lab 1

Lab 1 - Easy

Publish | Edit

Difficulty: Easy. No rabbit holes, very straightforward.

Learning Objectives:

1. Use Cellebrite UFED4PC to extract data from an iOS mobile device.
2. Understand how to analyze extracted data using Cellebrite Physical Analyzer.
3. Identify common types of evidence that can be extracted from a smartphone.
4. Explain the limitations of mobile device forensics and the ethical considerations that must be considered.

Scenario:

A smartphone has been recovered from a suspect in a criminal investigation. The main suspect's name is Elmer Fudd. He along with one more partner are planning to execute an evil plan. Luckly he was caught before fully executing the plan, but he is facing some charges. As the lead digital investigator in this criminal case, extract and analyze the extracted data to identify evidence of criminal activity and uncover their plot.

Tasks:

Extract data from the smartphone,

Analyze and follow the leads,

Generate a report using Inspector and submit it,

Create a Portable Case using Inspector and exchange it with your assigned peer to compare your results,

Answer questions in 'Lab 1 Flags' quiz as you go to solve the case.

Skills:

Extracting evidence using UFED4PC,

Basic analysis of artifacts recovered from the phone using Physical Analyzer,

Data categorization and files analysis using Inspector.

Deliverables:

Physical Analyzer report of flags (.PDF),

Inspector report of artifacts (.PDF),

Shared Portable Case.

Lab 1 – Content.

References:

SANS' Advanced Smartphone Forensics Poster

SANS' iOS 3rd Part Apps Poster

Solution: Solution will be unlocked after the assignment is submitted.

Points 100
Submitting a text entry box, a media recording, or a file upload
File Types pdf

Due	For	Available from	Until
-	Everyone	-	-

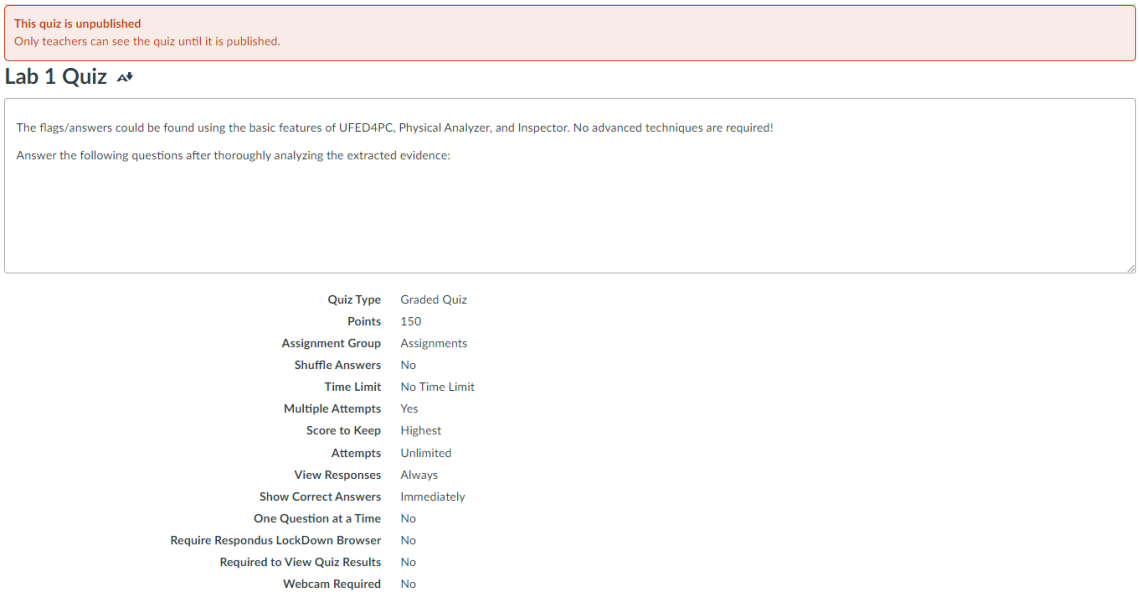
lab 1

Criteria	Ratings		Pts
Report incriminating evidence using Inspector	25 pts Full Marks	0 pts No Marks	25 pts
Share a Portable Case with your peer for evaluation	25 pts Full Marks	0 pts No Marks	25 pts
Proper use of extraction method	25 pts Full Marks	0 pts No Marks	25 pts
Physical Analyzer Report Generate a report using Physical Analyzer which includes a your quiz answers/flags found.	25 pts Full Marks	0 pts No Marks	25 pts
			Total Points: 100

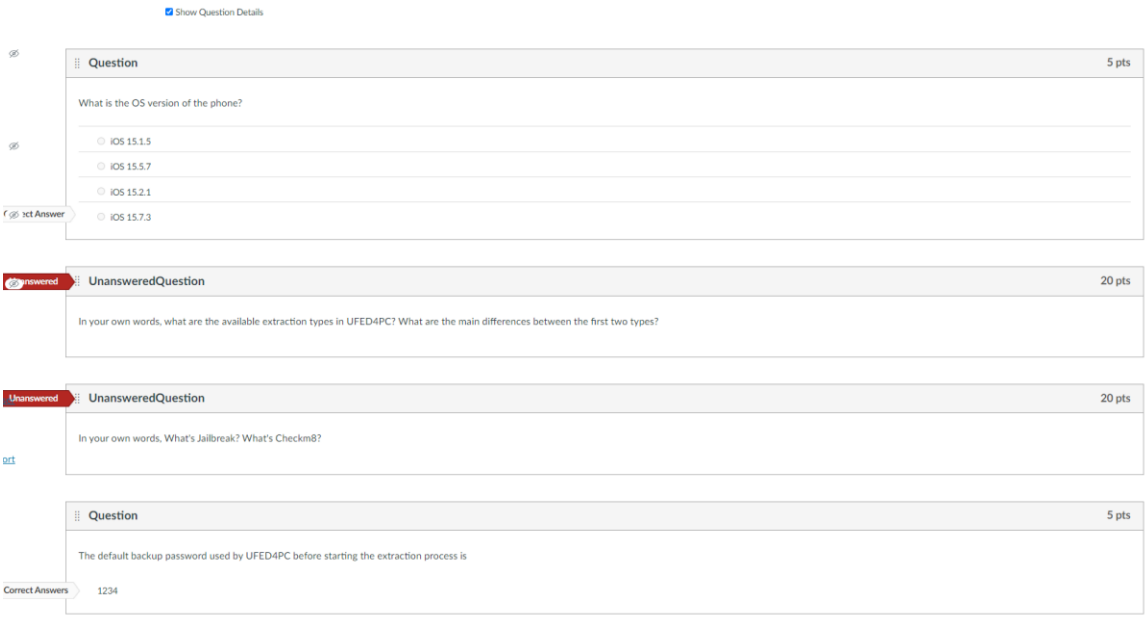
Lab 1 – Rubric.

APPENDIX G

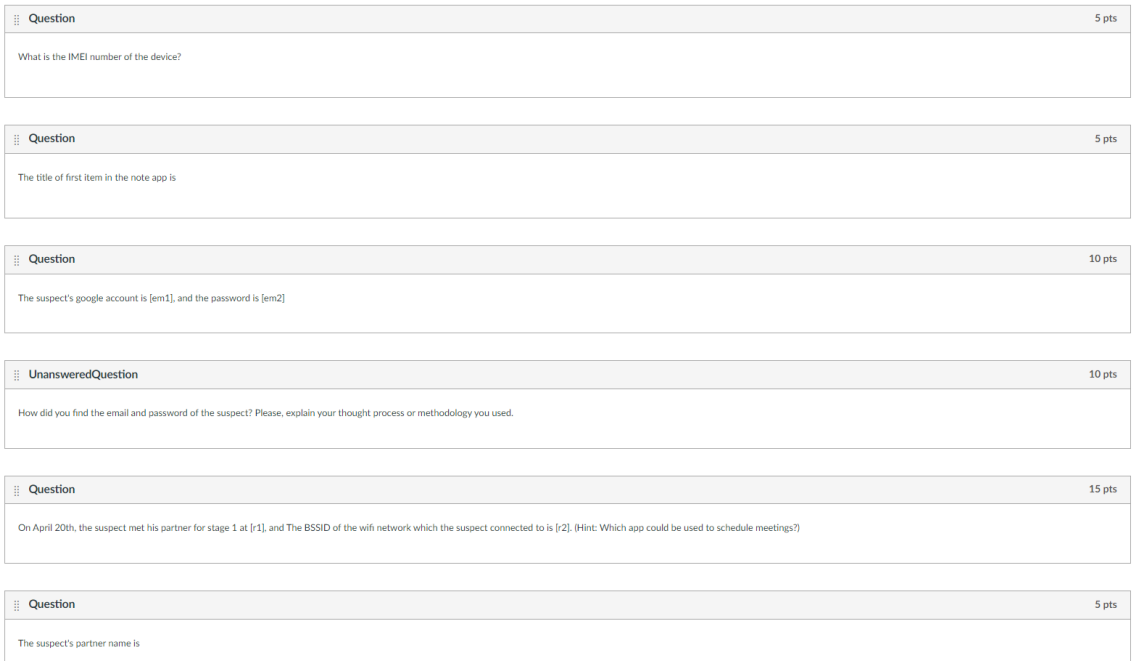
Quiz 1 & Solution



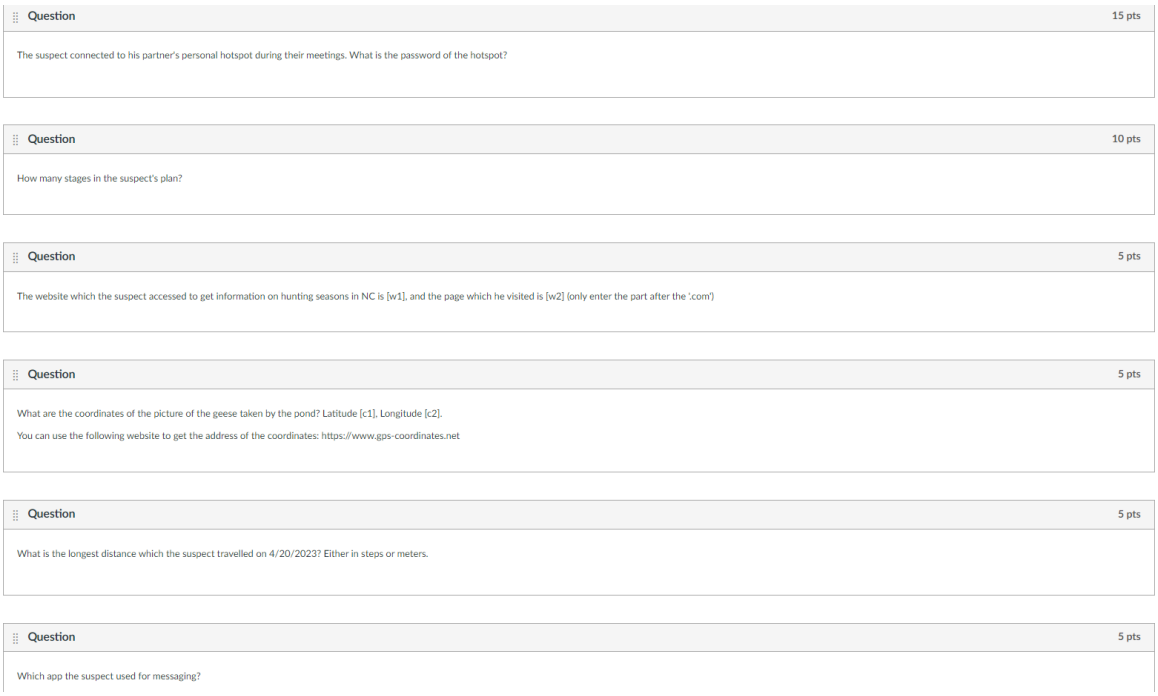
Lab 1 – Quiz 1.



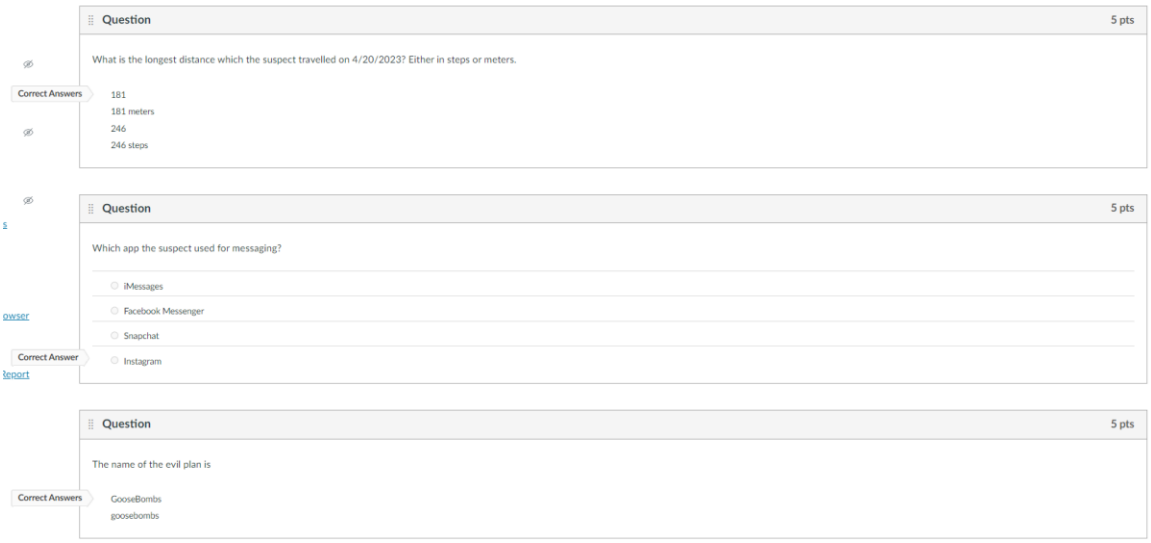
Example 1- questions from Quiz 1.



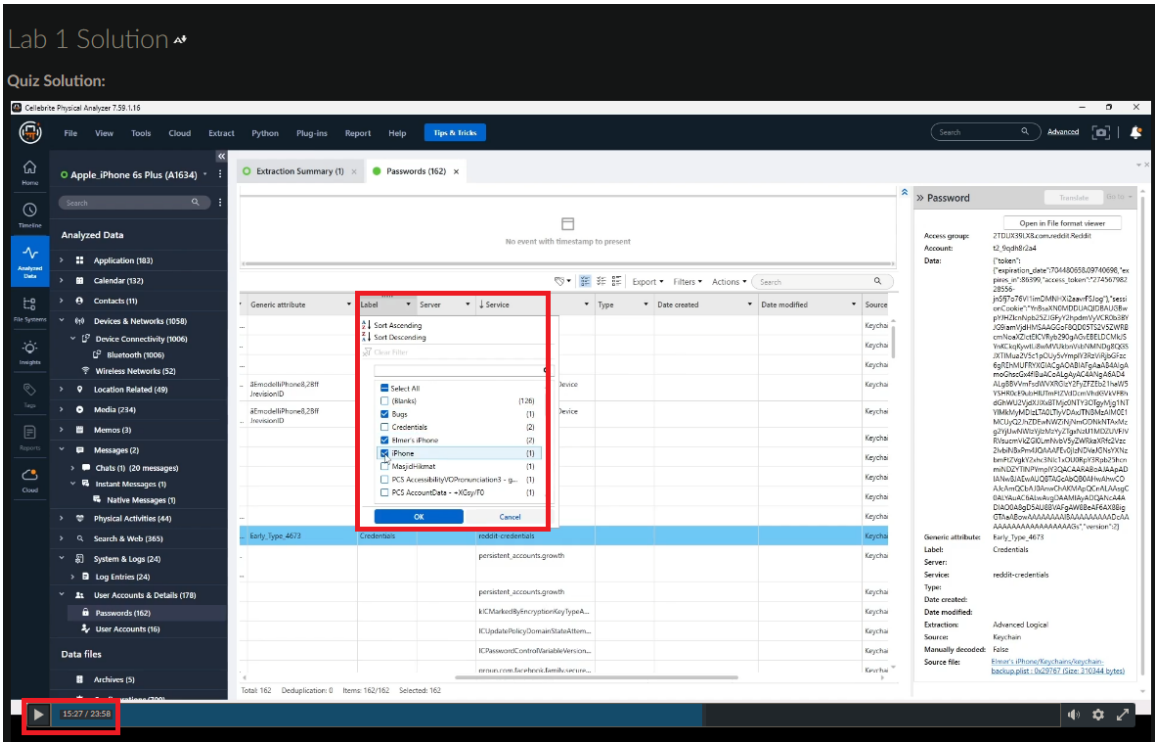
Example 2 – questions from quiz 1.



Example 3 of questions from quiz 1.



Example 4 of questions from quiz 1.



Example of walkthrough solution video for lab 1 where I am filtering through saved passwords to look for a personal hotspot's password.

APPENDIX H

Lab 2

Lab 2 - Medium

Publish | Edit

Difficulty: Medium. A combination of straightforward techniques and manual digging in Android's File System.

Learning Objectives:

1. Understand how to analyze extracted data using Cellebrite Physical Analyzer.
2. Understand how to navigate Android's File System.
3. Identify common types of evidence that can be extracted from an Android.
4. Explain the limitations of mobile device forensics and the ethical considerations that must be considered.

Scenario:

A smartphone has been recovered from a suspect named Heisenberg. He's being held for auto theft crimes. He along with two more partner sell stolen cars in the black market. As the lead digital investigator in this criminal case, analyze the extracted data to identify evidence of criminal activity and uncover their plot.

Tasks:

Analyze and follow the leads,

Tag your leads/flags as you solve quiz 2,

Generate a report of the tagged artifacts using Physical Analyzer and submit it,

Create a Portable Case using Inspector and exchange it with your assigned peer to compare your results,

Answer questions in 'Lab 2 Flags' quiz as you go to solve the case.

Skills:

Familiarity of Android's File System,

Analysis of artifacts recovered from the phone using Physical Analyzer,

Data categorization and files analysis using Inspector.

Deliverables:

Physical Analyzer report of flags (.PDF),

Shared Portable Case.

References:

SANS' Advanced Smartphone Forensics Poster

Android's 3rd Party Apps Poster

Solution: Solution will be unlocked after the assignment is submitted.

Points 100
Submitting a media recording or a file upload
File Types pdf

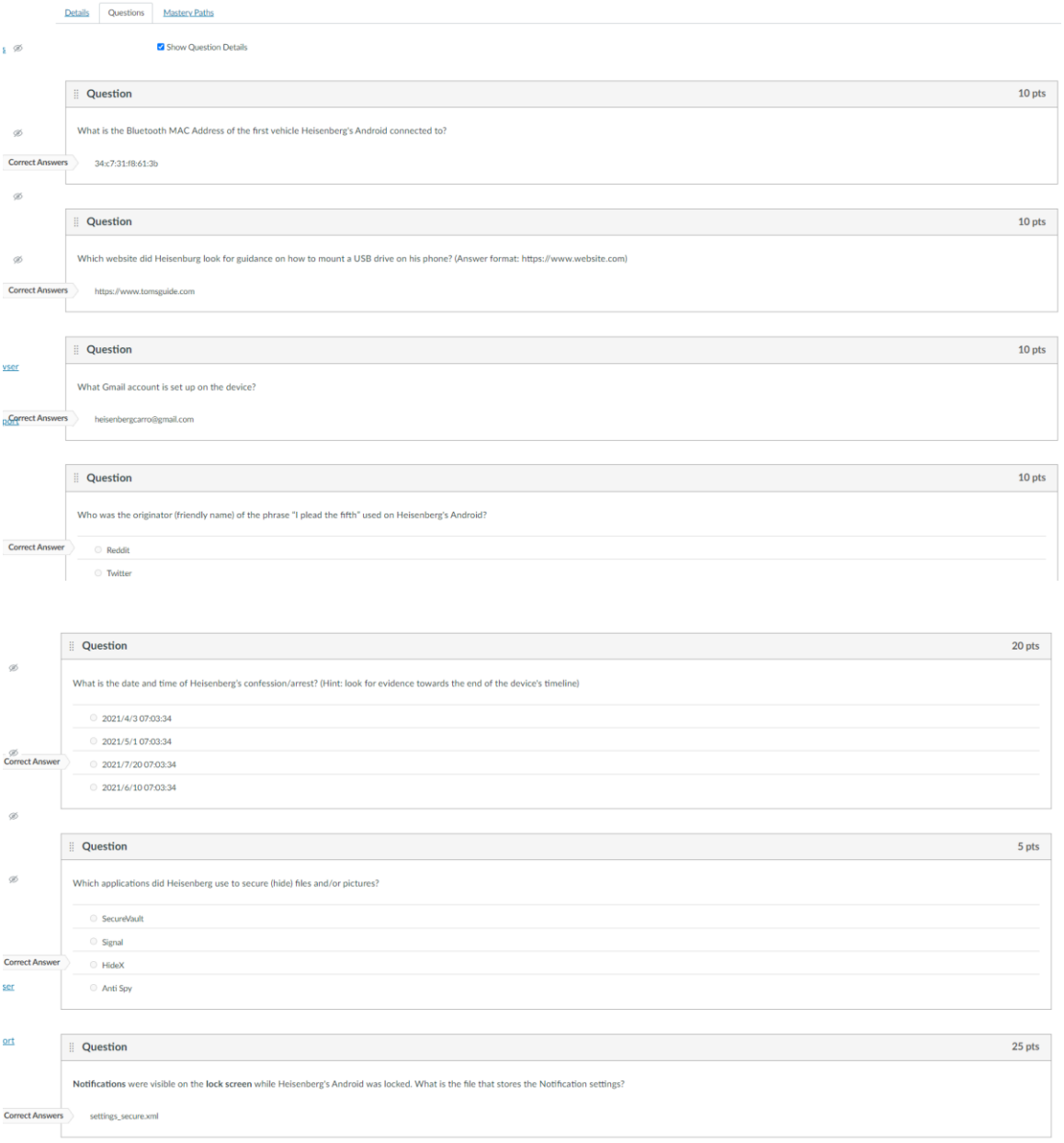
Due	For	Available from	Until
-	Everyone	-	-

lab 2 (1)

Criteria	Ratings		Pts
Physical Analyzer's Report	**50 to >0.0 pts** **Report Completeness** All flags/answers from the quiz are included in the report	**0 pts** **No Marks**	50 pts
Inspector's Portable Case	**50 to >0.0 pts** **Portable Case** Portable Case includes the right artifacts exported from Inspector	**0 pts** **No Marks**	50 pts
			Total Points: 100

APPENDIX I

Quiz 2 & Solution



Question 15 pts

Which website appears in the **false postives** table in DuckDuckGo's DB?

Question 20 pts

When and in which city did Heisenberg **search for rental** properties on his Android? (Answer Format: YYYY-MM-DD **HH:MM:SS** NameOfCity)

Date - Time:[d]

City:[c]

Question 15 pts

Heinsenberg has a clear interest in Crypto Currency. What is the **Topic ID Hash** for **$ETH** on his Android device? (Hint: which cryptocurrency is $ETH?)

Question 15 pts

On Heisenberg's Android, where else can you find the IMSI number on the device, other than the Checkin.xml file?

Question 15 pts

Heisenberg was looking for cars. Which vehicle did he not search for? (Hint: search in car related apps' databases such as CarFax and CarGuru)

Question 15 pts

Heinsenberg has a clear interest in Crypto Currency. What is the **Topic ID Hash** for **$ETH** on his Android device? (Hint: which cryptocurrency is $ETH?)

Question 15 pts

On Heisenberg's Android, where else can you find the IMSI number on the device, other than the Checkin.xml file?

Question 15 pts

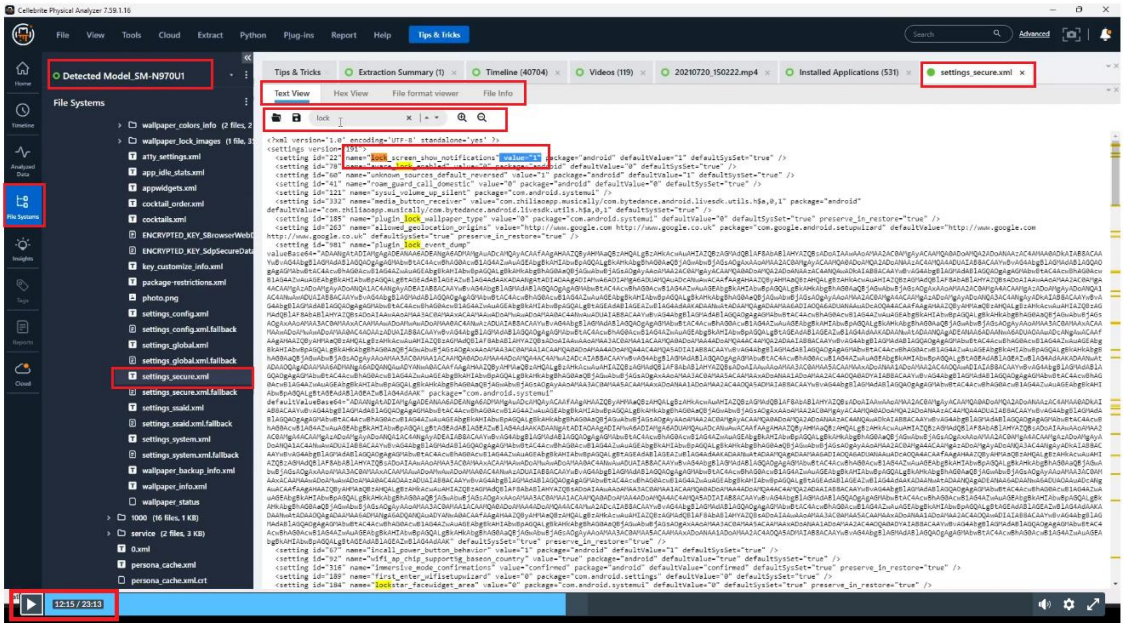
Heisenberg was looking for cars. Which vehicle did he not search for? (Hint: search in car related apps' databases such as CarFax and CarGuru)

Question 30 pts

How many times did Heisenberg's Android power off due to the battery being fully depleted between May and August? The answer must be an integer (i.e 4).

Lab 2 Solution

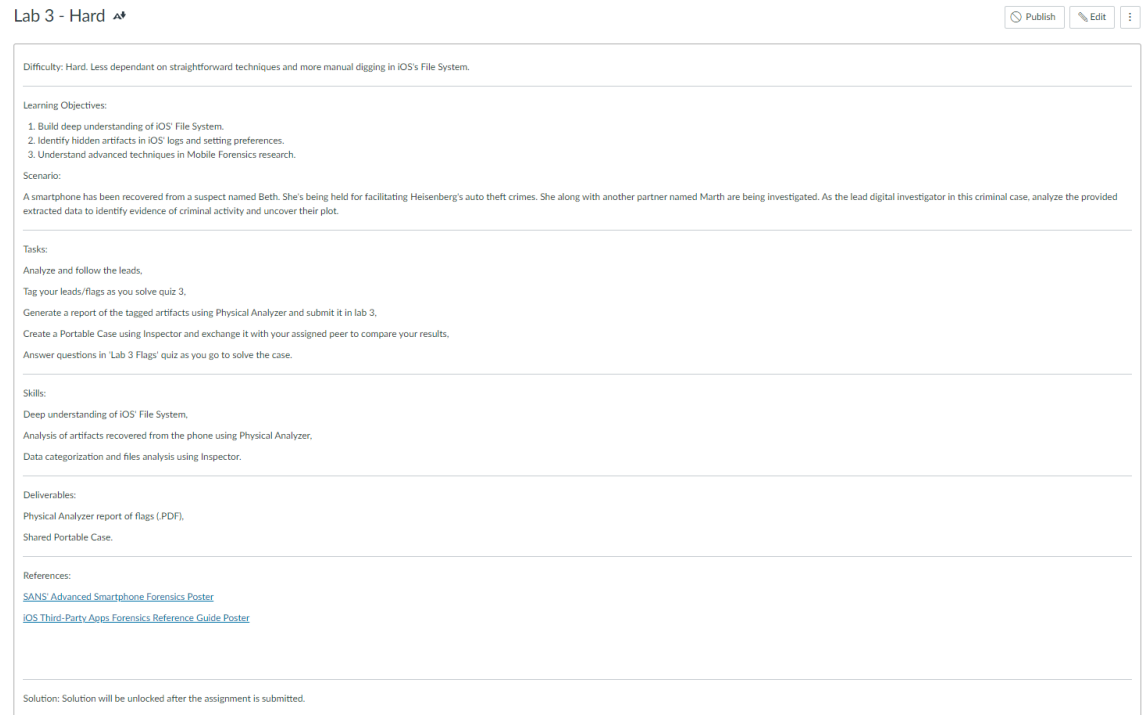
Quiz Solution:



Walkthough of a quiz 3 question where students have to find whether the suspect's phone shows notifications on lock screen or not. In this case the value was '1', meaning that it shows notifications.

APPENDIX J

Lab 3



Lab 3 - Hard

Publish Edit

Difficulty: Hard. Less dependant on straightforward techniques and more manual digging in iOS's File System.

Learning Objectives:

1. Build deep understanding of iOS' File System.
2. Identify hidden artifacts in iOS' logs and setting preferences.
3. Understand advanced techniques in Mobile Forensics research.

Scenario:

A smartphone has been recovered from a suspect named Beth. She's being held for facilitating Heisenberg's auto theft crimes. She along with another partner named Marth are being investigated. As the lead digital investigator in this criminal case, analyze the provided extracted data to identify evidence of criminal activity and uncover their plot.

Tasks:

Analyze and follow the leads,

Tag your leads/flags as you solve quiz 3,

Generate a report of the tagged artifacts using Physical Analyzer and submit it in lab 3,

Create a Portable Case using Inspector and exchange it with your assigned peer to compare your results,

Answer questions in 'Lab 3 Flags' quiz as you go to solve the case.

Skills:

Deep understanding of iOS' File System,

Analysis of artifacts recovered from the phone using Physical Analyzer,

Data categorization and files analysis using Inspector.

Deliverables:

Physical Analyzer report of flags (.PDF),

Shared Portable Case.

References:

SANS' Advanced Smartphone Forensics Poster

iOS Third-Party Apps Forensics Reference Guide Poster

Solution: Solution will be unlocked after the assignment is submitted.

References:

SANS' Advanced Smartphone Forensics Poster

iOS Third-Party Apps Forensics Reference Guide Poster

Solution: Solution will be unlocked after the assignment is submitted.

Points 100
Submitting a media recording or a file upload
File Types pdf

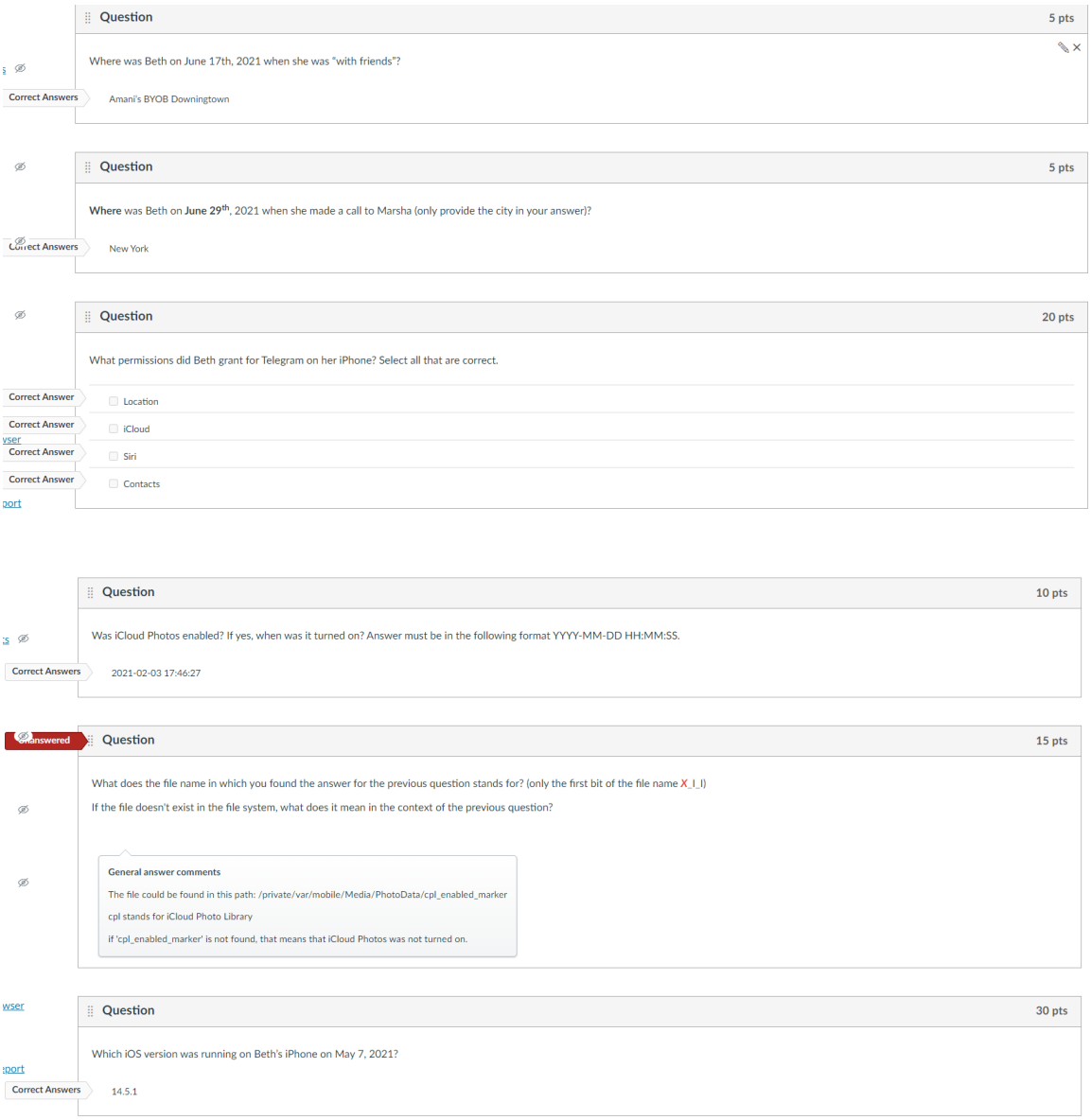
Due	For	Available from	Until
-	Everyone	-	-

lab 3

Criteria	Ratings		Pts
Physical Analyzer's Report	**50 to >0.0 pts** **Report Completeness** All flags/answers from the quiz are included in the report	**0 pts** **No Marks**	50 pts
Inspector's Portable Case	**50 to >0.0 pts** **Portable Case** Portable Case includes the right artifacts exported from Inspector	**0 pts** **No Marks**	50 pts
			Total Points: 100

APPENDIX K

Quiz 3 & Solution



Question 5 pts

Where was Beth on June 17th, 2021 when she was "with friends"?

Correct Answers: Amani's BYOB Downingtown

Question 5 pts

Where was Beth on **June 29th**, 2021 when she made a call to Marsha (only provide the city in your answer)?

Correct Answers: New York

Question 20 pts

What permissions did Beth grant for Telegram on her iPhone? Select all that are correct.

Correct Answer: Location

Correct Answer: iCloud

Correct Answer: Siri

Correct Answer: Contacts

Question 10 pts

Was iCloud Photos enabled? If yes, when was it turned on? Answer must be in the following format YYYY-MM-DD HH:MM:SS.

Correct Answers: 2021-02-03 17:46:27

Unanswered

Question 15 pts

What does the file name in which you found the answer for the previous question stands for? (only the first bit of the file name X_I_I)

If the file doesn't exist in the file system, what does it mean in the context of the previous question?

General answer comments

The file could be found in this path: /private/var/mobile/Media/PhotoData/cpl_enabled_marker

cpl stands for iCloud Photo Library

if 'cpl_enabled_marker' is not found, that means that iCloud Photos was not turned on.

Question 30 pts

Which iOS version was running on Beth's iPhone on May 7, 2021?

Correct Answers: 14.5.1

Question 25 pts

Which time zones were visited while the device was on iOS 14.4.

Correct Answer — Central

Correct Answer — Eastern

Correct Answer — Mountain

Pacific

Question 30 pts

On July 20th, 2021 at 20:06 PM **local time**, Beth's iPhone received a System message regarding the **thermal** state of the device. What is the name of the file that contains this information? (Hint: Search how apple processes and stores **system logs**. You can use Inspector's filter!)

Correct Answers: 0000000000000393.tracev3

Question 15 pts

What was the search query in the open tab of the DuckDuckGo Privacy Browser?

Correct Answers: daphne bridgerton actress

Question 20 pts

A Visa card ends in 4483 was saved in the Apple Wallet?

Correct Answer — True

False

No cards were saved in the Apple wallet.

Question 20 pts

How long does Beth's phone need to be inactive for the screen to auto-lock? (Answer: integer value)

Correct Answers: 0

Question 5 pts

An analyst generated a list of the codes used by the gang members. 'f0x' is one of the code names. You think you know what f0x is? Provide the name that appears on one of f0x related images.

Correct Answers: Werner

Question 5 pts

Beth wanted to meet her partner in an isolated place in the mountains to close a deal. Which email address did she send to?

Question 5 pts

Beth wanted to meet her partner in an isolated place in the mountains to close a deal. Which email address did she send to?

orrect Answers livingstonhank11@gmail.com

Question 5 pts

Two of the suspects use the same app to facilitate money transfers without handling fees. Who are they? Provide first names separated by a comma: [AAA],[BBB]

orrect Answers Marsha,Beth

Question 10 pts

What is the version of the extraction container format in the provided evidence file?

orrect Answers CLBX-0.3.1

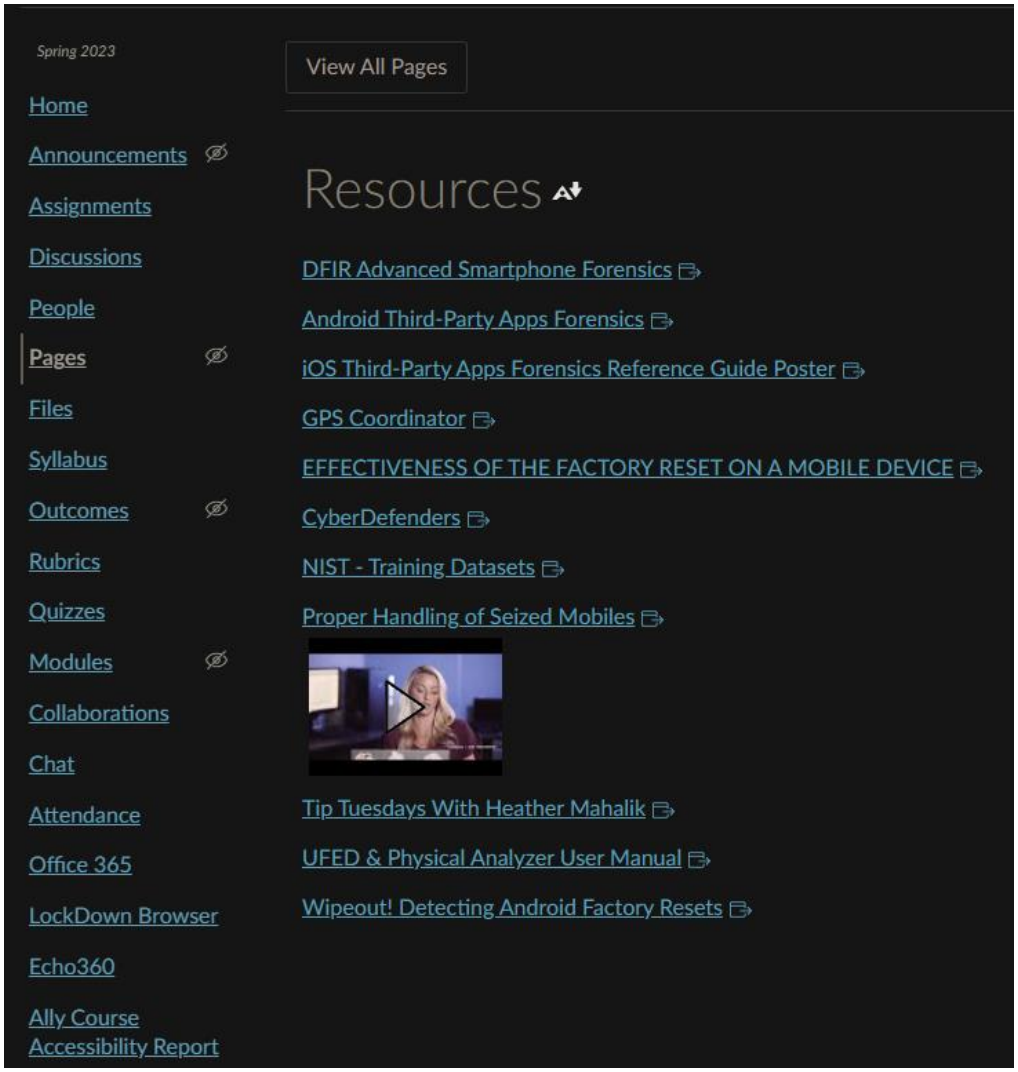
Question 10 pts

What is the Exclusive Chip Identification (ECID) of the mobile device?

orrect Answers 000469E20847002E

APPENDIX L

Resources Page



Content of Resources page where students can look for more tips and techniques to apply in the labs.

APPENDIX M

Computing Resources Consumption

Name	Status	100% CPU	79% Memory	19% Disk	0% Network
Cellebrite Physical Analyzer (7)		56.8%	4,011.6 MB	35.2 MB/s	0 Mbps
Cellebrite Physical Analyzer		56.8%	3,963.1 MB	35.2 MB/s	0 Mbps
CefSharp.BrowserSubprocess		0%	23.7 MB	0 MB/s	0 Mbps
CefSharp.BrowserSubprocess		0%	11.8 MB	0 MB/s	0 Mbps
CefSharp.BrowserSubprocess		0%	6.9 MB	0 MB/s	0 Mbps
External License Manager (32 bit)		0%	2.1 MB	0 MB/s	0 Mbps
External License Manager (32 bit)		0%	2.0 MB	0 MB/s	0 Mbps
External License Manager (32 bit)		0%	1.9 MB	0 MB/s	0 Mbps

Computer Consumption while Physical Analyzer's Hash set Examination tool is processing lab 3's dataset.

Name	Status	74% CPU	93% Memory	61% Disk	0% Network
Cellebrite Physical Analyzer (7)		0.2%	6,528.2 MB	3.6 MB/s	0 Mbps
Cellebrite Physical Analyzer		0.2%	6,520.0 MB	3.5 MB/s	0 Mbps
CefSharp.BrowserSubprocess		0%	2.5 MB	0 MB/s	0 Mbps
CefSharp.BrowserSubprocess		0%	1.9 MB	0 MB/s	0 Mbps
External License Manager (32 bit)		0%	1.0 MB	0.1 MB/s	0 Mbps
CefSharp.BrowserSubprocess		0%	1.0 MB	0 MB/s	0 Mbps
External License Manager (32 bit)		0%	0.9 MB	0.1 MB/s	0 Mbps
External License Manager (32 bit)		0%	0.7 MB	0 MB/s	0 Mbps
OpenJDK Platform binary		73.1%	1,187.3 MB	26.3 MB/s	0 Mbps

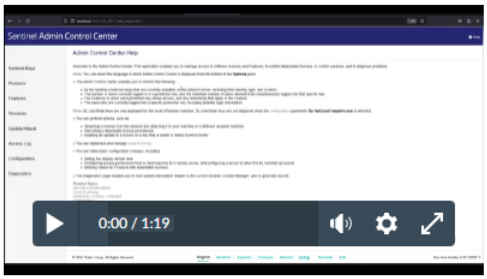
Computer Consumption while running Physical Analyzer's Hash set Extraction tool + other Enrichment engines such as 'Cryptocurrency'.

APPENDIX N

UFED4PC & Physical Analyzer Network Dongle Configuration

Setup Technical Instructions

UFED4PC & Physical Analyzer's Dongle:



Client Machines:

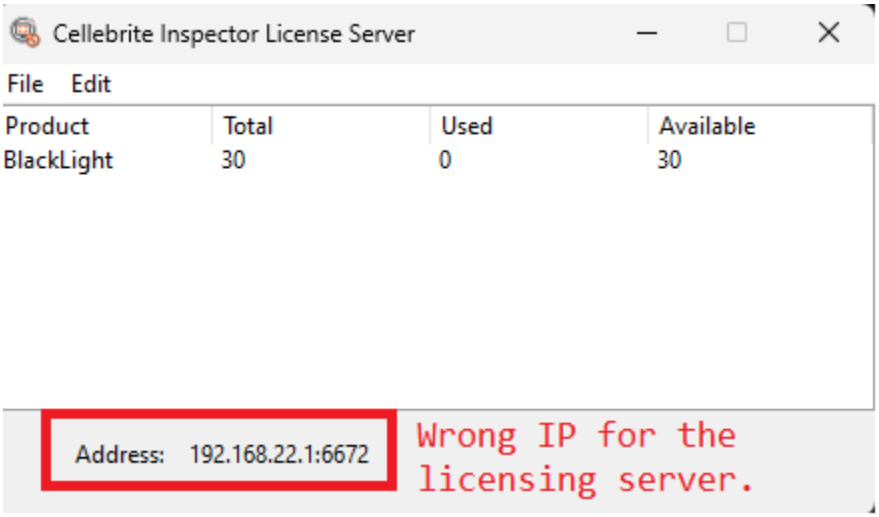
1. Navigate to Localhost:1947 -> Configuration -> Access to Remote License Managers -> check Allow Access to Remote Licenses
2. Enter the IP address of the server hosting the dongle in the Remote License Search Parameters and click submit.
3. Next Navigate to Localhost:1947 -> Configuration -> Network
4. Check the radial bubble for all network interfaces and click submit.

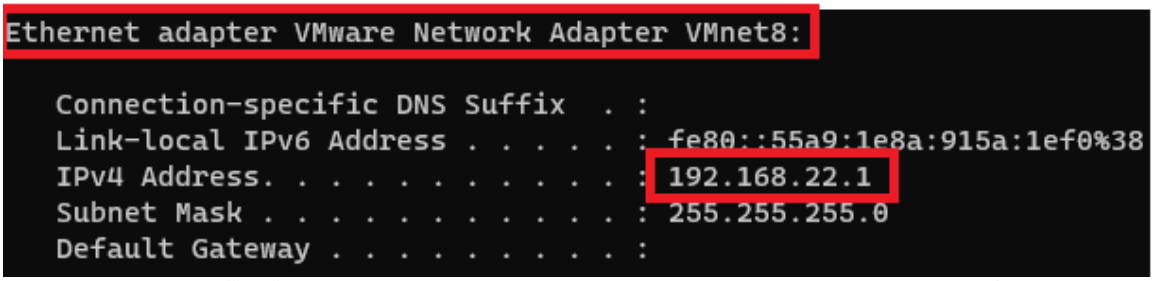
Server hosting the dongle:

1. Navigate to Localhost:1947 -> Configuration -> Access from Remote Clients
2. Check the radial button for All licenses are accessible without need of identity and click submit.
3. Next Navigate to Localhost:1947 -> Configuration -> Network
4. Check the radial bubble for all network interfaces and click submit.

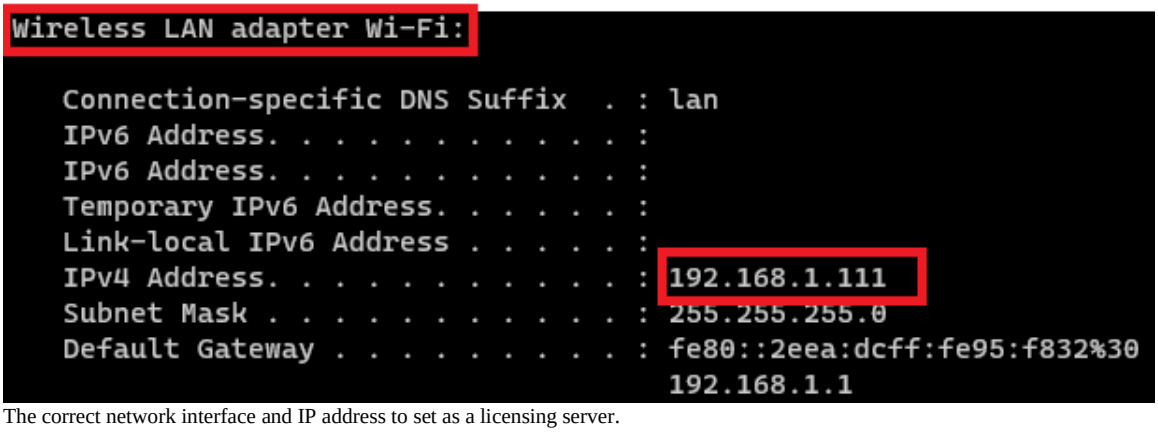
APPENDIX O

Inspector Network Dongle Configuration

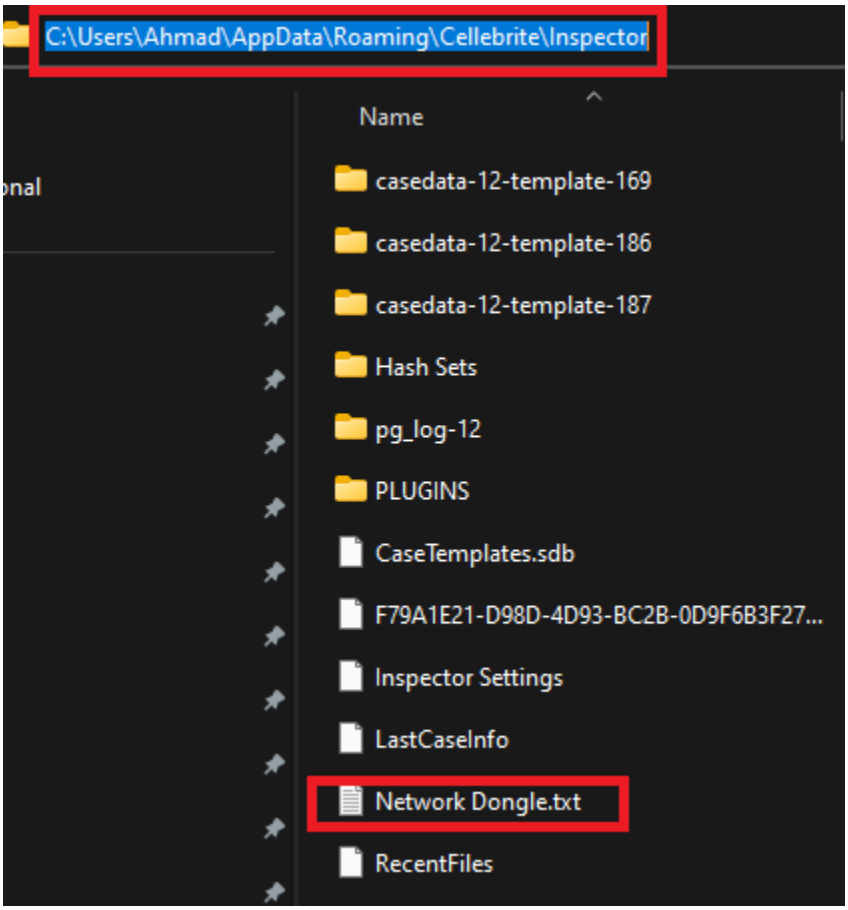




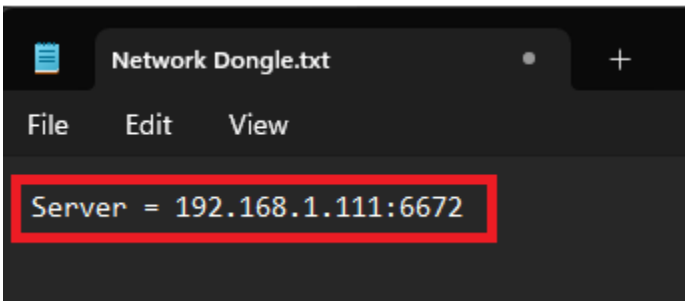
Inspector's licensing server, where the dongle will be connected, is detecting the wrong network interface.



The correct network interface and IP address to set as a licensing server.



Create ‘Network Dongle.txt’ in the location highlighted on the hosts which students will be using and do the following edit inside this file.



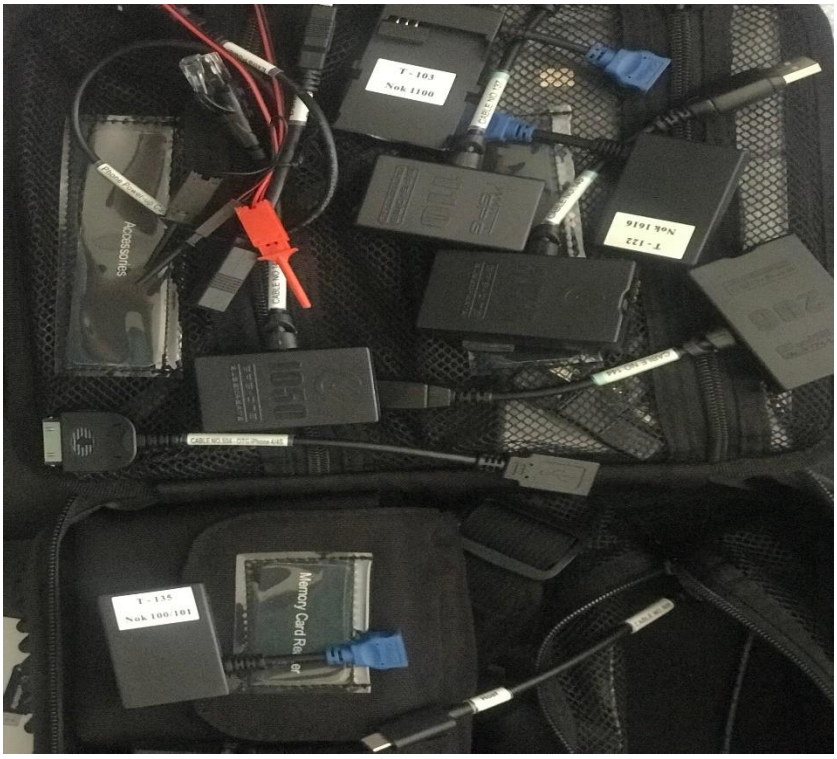
The licensing server’s correct IP address.

APPENDIX P

Toolkit Bag Content

SIM cards cloning kit.

Cable collection for multiple mobile phone vendors.



Another cable collection for multiple mobile phone vendors.