

Maria Valencia

Csc 153

Lab 12

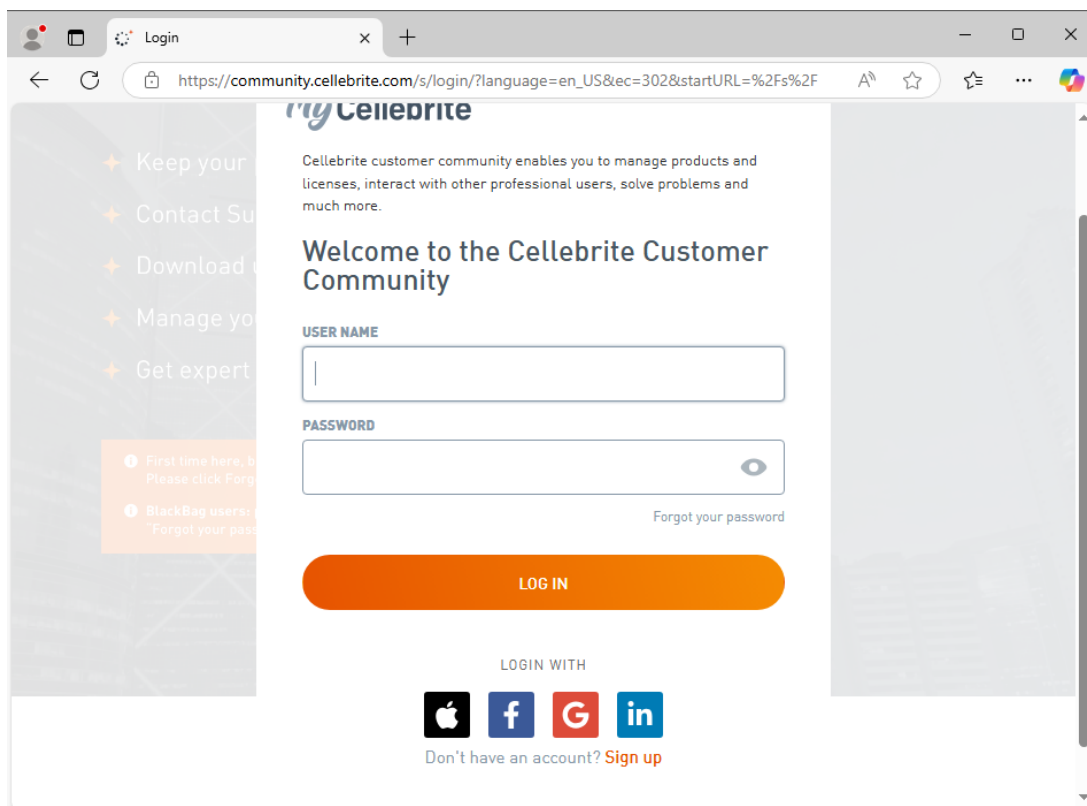
Mobile Device forensics and IoA

Task 1- Mobile Device Forensics

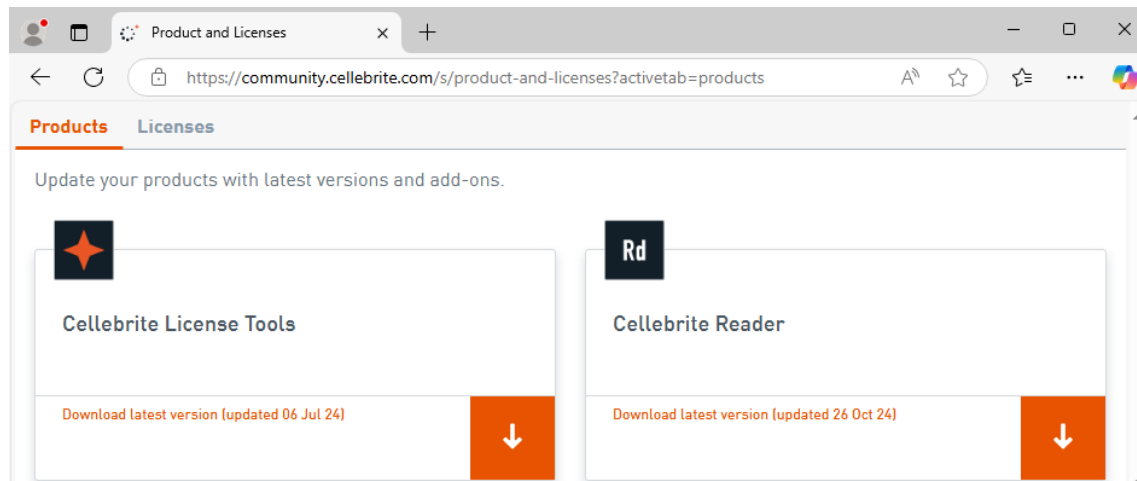
In this task, you will analyze a logical acquisition of a nokia device using Cellebrite Reader software.

Step 1: Signup and Download

In your windows VM, navigate to <https://community.cellebrite.com/> and follow the “Sign up” link.



Complete the registration form with your name and email to sign up. Observe a validation link is sent to your inbox. Follow the registration link in your inbox and complete the registration form selecting "Academic" for your profession. Once logged in, navigate to the "Products & Licenses" tab.



Cellebrite Reader Downloads



Get activation code

10.4

7.70

10.3

Released: 26/10/24



Welcome to Cellebrite Reader 7.70!


Here's what's new in the product:

- New support for Private Vault applications including Gallery Lock (Android & iOS) and KeepSafe Calculator (Android).
- New support for Secure Messaging application Skred (Android).
- Now supports Google Maps Timeline data stored locally on the device.
- Improvements include Safari data from additional profiles, new locations and updated Message Retention settings.
- Support Updated for Telegram, Signal, Facebook and GMX among others.

▼


Software Version

26/10/24 544.75 MB	MD5-	 Download
Cellebrite Reader 7.70	8A4AC37D089310CD1DBA8982AB67D191	

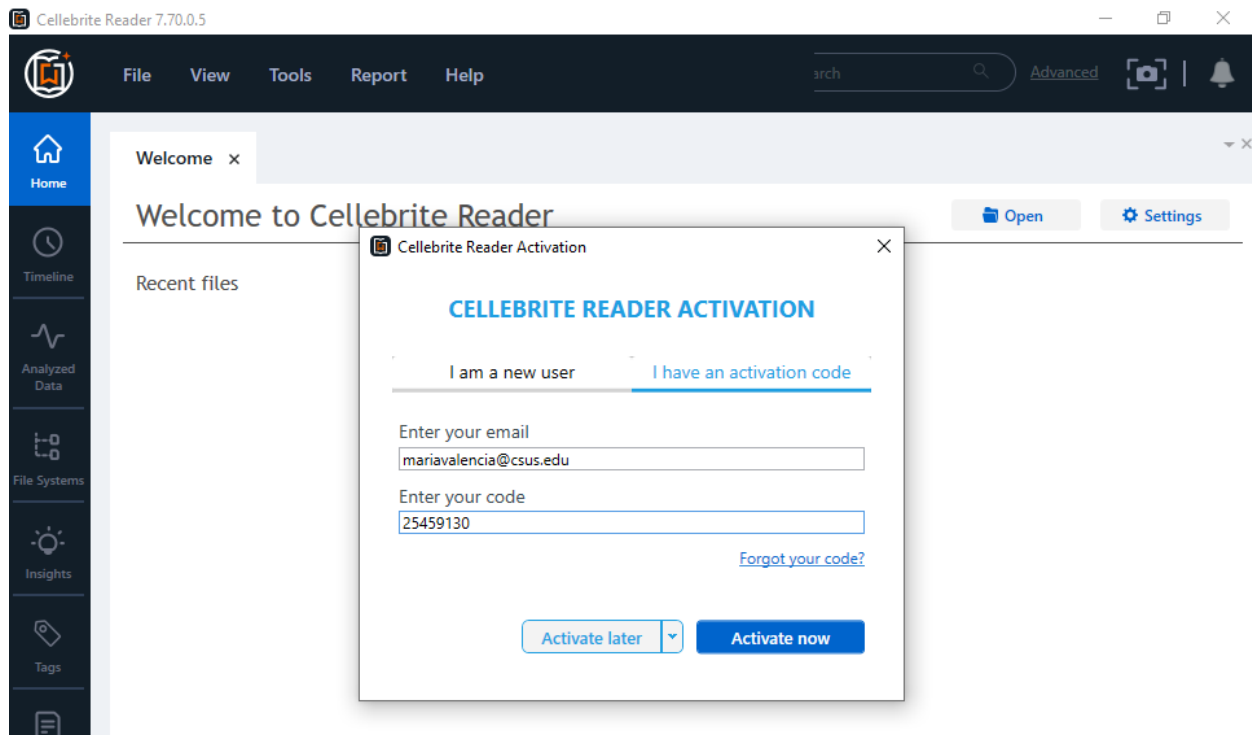
Download the software and write down the "Activation Code" when presented.

Step 2: Install Cellebrite Reader

With the Cellebrite Reader zip file downloaded, unzip and double click the EXE to start the installation.

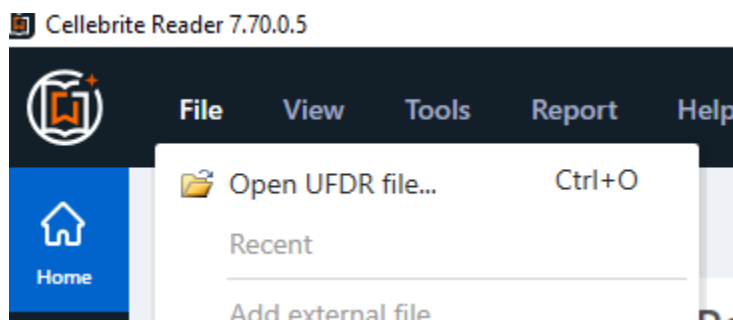
Name	Date modified	Type	Size
 CellebriteReader_7.70.0.5	11/19/2024 11:30 AM	Application	557,821 KB

Upon loading you are presented with an activation window. Enter the activation code presented to you after you downloaded the installer from the website. Note that you can re-retrieve this activation code from the "Get Activation Code" if needed.

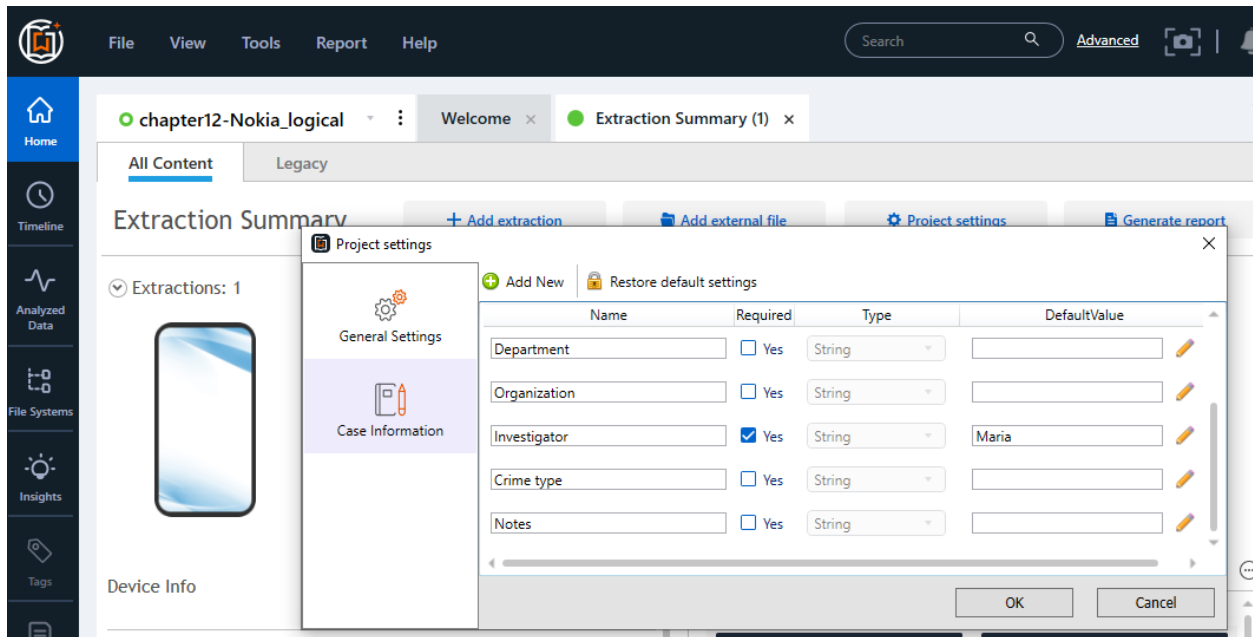


Step 3: Setup Case

With Cellebrite Reader installed and activated, download the "chapter12-nokia_logical.ufdr" file to your Windows VM. Open the "chapter12-Nokia_logical.ufdr" file in Cellebrite Reader by going to File and "Open UFDR file...". Select the logical UFDR file and allow a few seconds for the extraction to complete.

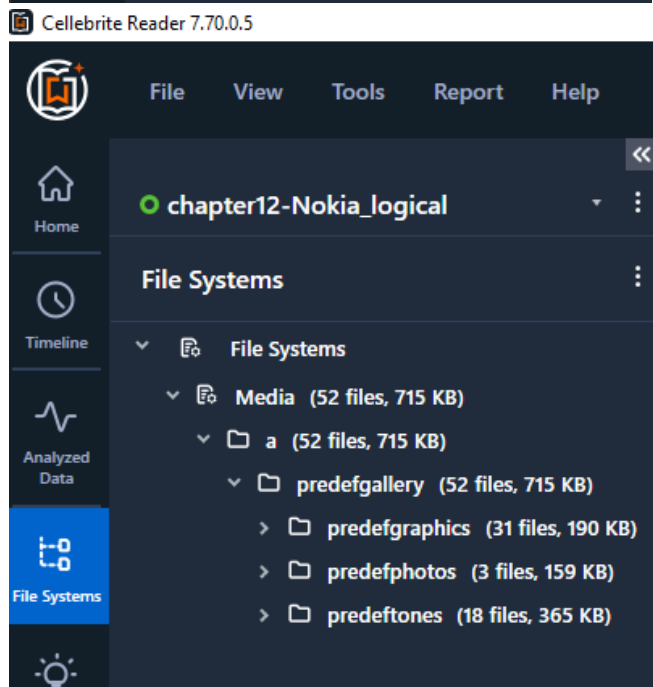
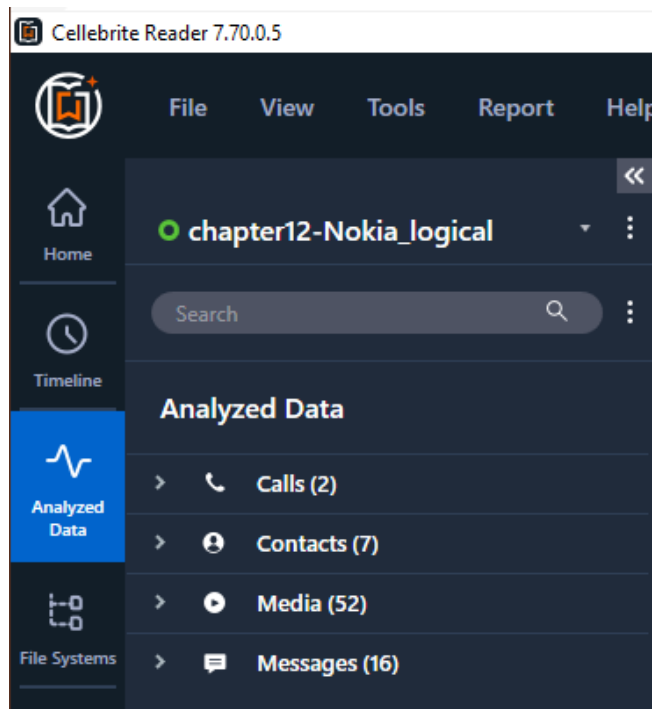


Select the "Project Settings" under the "Extraction Summary" and select Case Information. Make the Investigator field Required and enter the default value with your name. Newer versions of this software have the Project Settings under the Tools menu.



Step 4: Examine Logical Acquisition

Explore the content extracted, timeline, and File Systems.



Step 5: Generate Report

After you have analyzed the acquisition, write a 1-2 paragraph summary of your findings that considers the types of data analyzed and any relevant information that could be used to describe what happened on the device. In addition, use the "Generate report" feature to create a PDF of the case.

Using Cellebrite Reader, I uploaded a nokia to be extracted and analyzed. While looking at the data analyzed, I see that 2 calls were made, there's 7 contacts, 18 audio, 34 images, and 16 messages. When looking at the File Systems, I see there's 52 files in the media. This is a combination of audio and images from the media tab. After further inspection of the file systems, I come across a gallery which has 3 categories: graphics, photos and tones. There are 31 files in the graphics, 3 files in photos and 18 files in tones. Finally, there was no malware found in the phone.

Generate Report

General

Report Dataset

chapter12-Nokia...

Security

Formatting

Table Sorting

PDF Report

General

File name:chapter12-Nokia_logical_2024-11-19_Report

Save to:C:\Users\maria\Documents\My ReportsBrowse

Report sub directory:2024-11-19.11-49-39

Projectchapter12-Nokia_logical

FormatPDF Report

Case Information

Examiner name:Maria

Location:

Case number:

Case name:

Evidence number:

Department:

Organization:

Investigator:Maria

Crime type:

Notes:

combination of audio and images from the media tab. After further inspection of the file systems, I come across a gallery which has 3 categories: graphics, photos and tones. There are 31 files in the graphics, 3 files in photos and 18 files in tones. Finally, there was no malware found in the phone.

Update report settings

Previous

Next

Cancel

