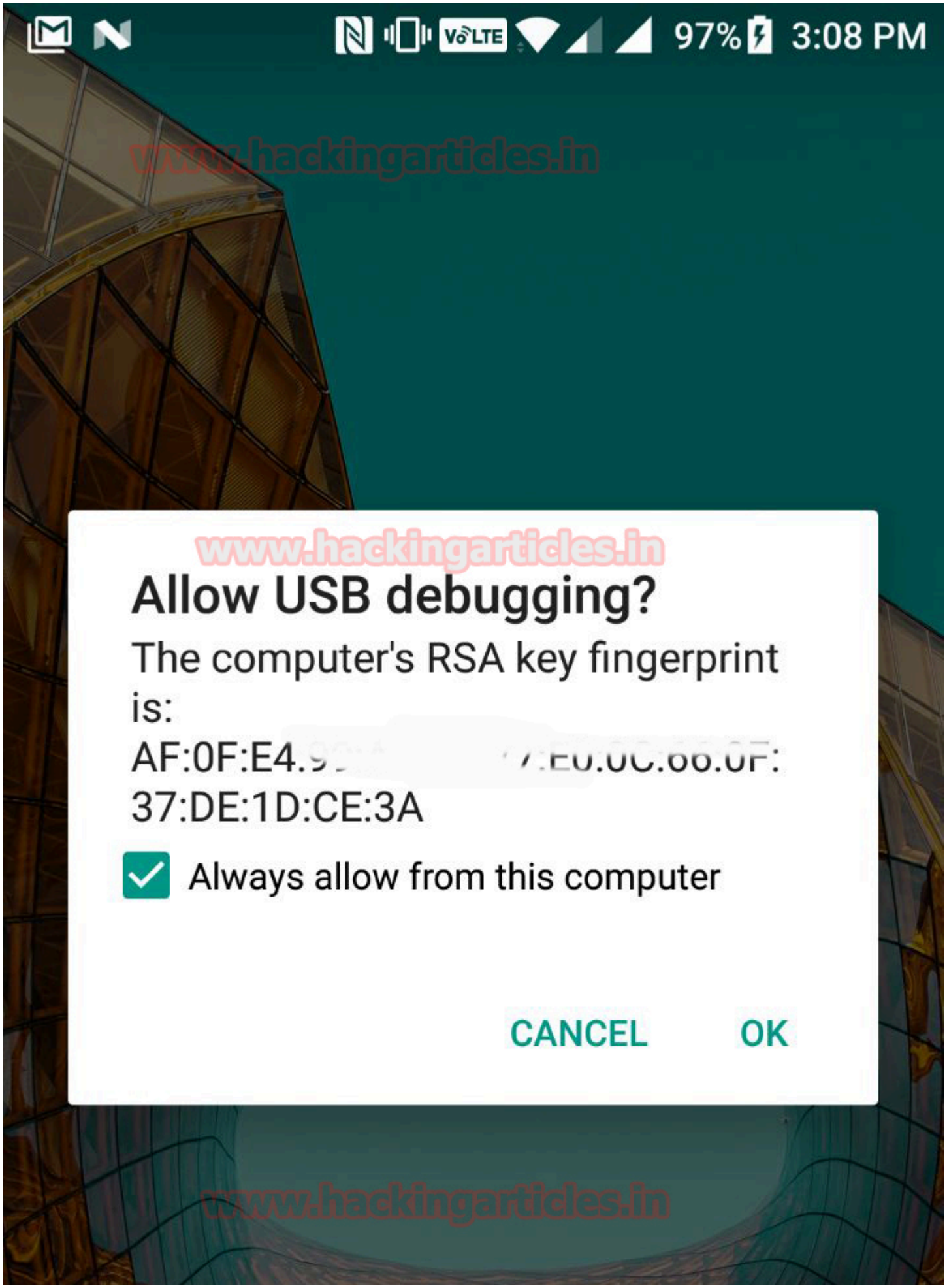
Mobile Forensics Investigation using Cellebrite UFED

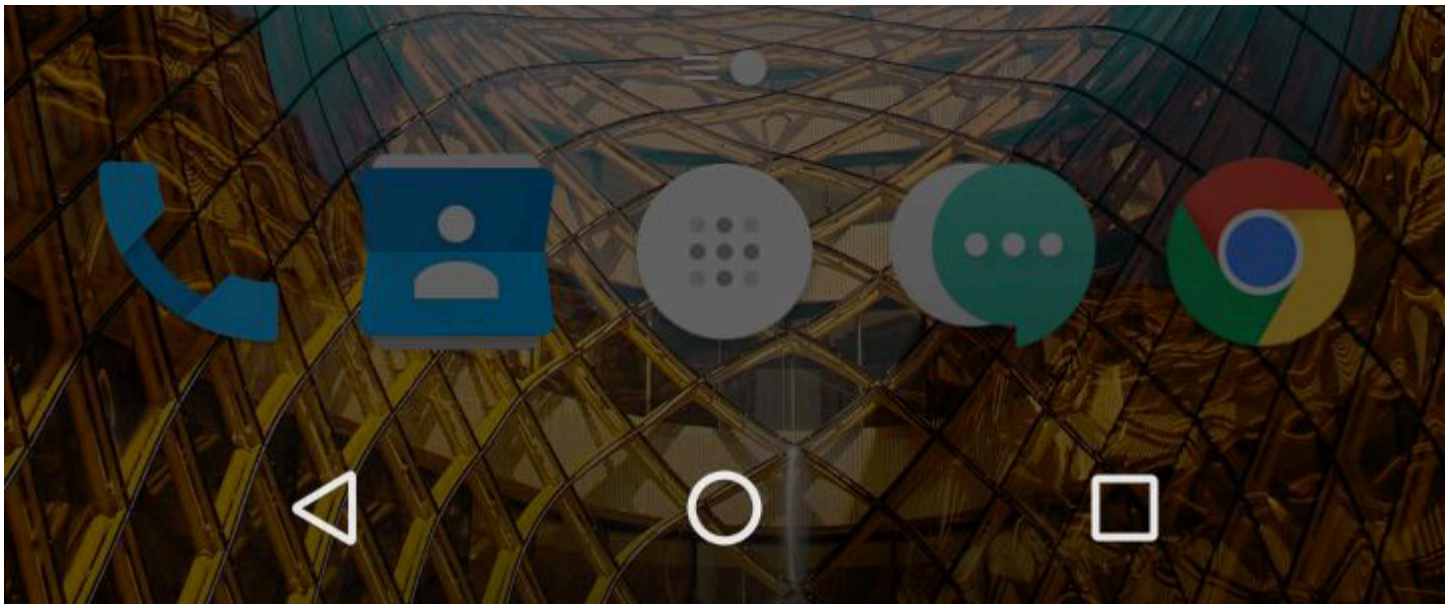
April 5, 2017 By Raj Chandel

The manifold increase in the mobile penetration amongst the world population has interested people from all works of life namely mobile manufactures, service providers, application developers and more to this industry. Thequantum jump inthe user base and its usage of mobile has even caught the eye of Forensic Experts.

In this article we will conduct a mobile investigation of ONE Plus mobile model by applying Cellebrite UFED software.

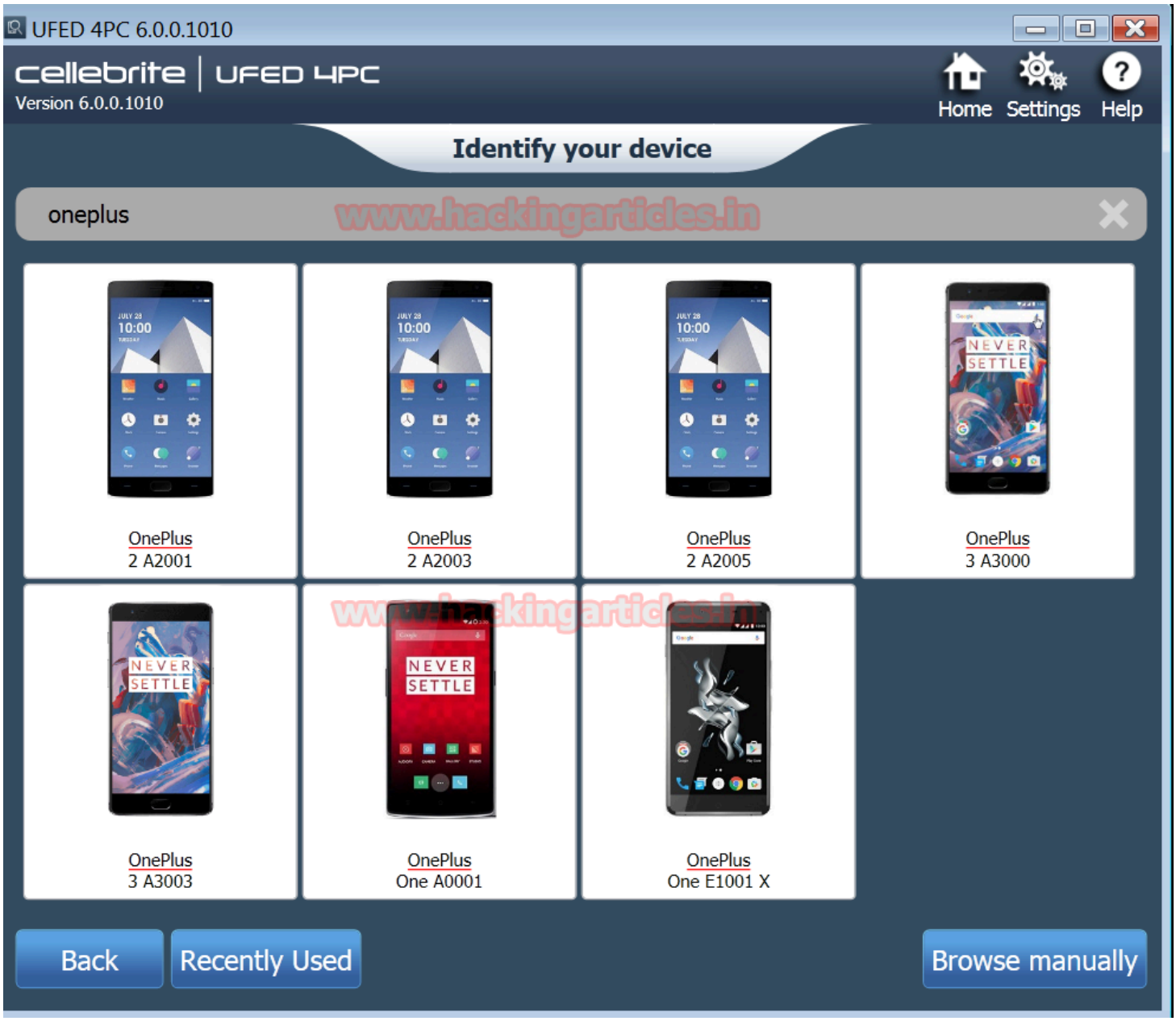
As a preliminary process, adjustments need to be undertaken on the mobile model under surveillance. The investigator attaches the mobile to his/her laptop through the phone cable.The investigator needs to open the 'About Phone' section under Setting and scroll down the various options till he reaches the 'Build Option', he needs to tap the 'Build Option' seven (7) times which opens a new section – the 'Developer Option'. Before commencing Cellebrite software, the investigator must check whether the mobile commands 'Stay Awake' and Debugging (USB debugging) are **ON.**


97% 3:08 PM
www.hackingarticles.in
Allow USB debugging?
The computer's RSA key fingerprint is:
AF:0F:E4.9
7:E0:0C:66:0F:
37:DE:1D:CE:3A
Always allow from this computer
CANCEL
OK
www.hackingarticles.in



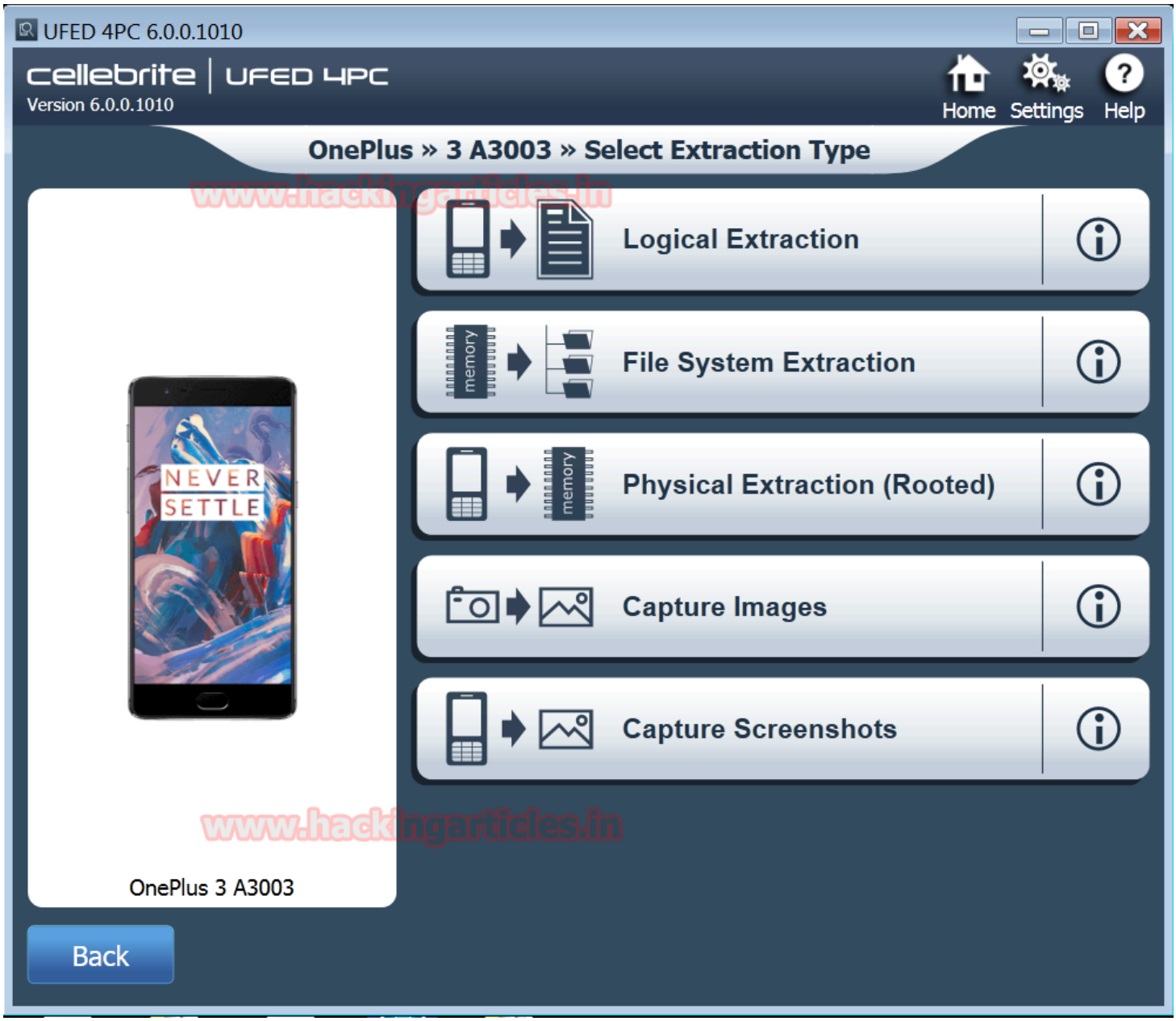
After completing the following steps, the investigator inserts the licensed Cellebrite USB Key in the laptop which displays five choices namely- Mobile device, SIM Card, USB device or Memory Card, UFED Camera and Device Tool.

We choose ONE Plus mobile model to demonstrate the Cellebrite software. After configuration the software on the laptop, the software displayed seven ONE Plus models to select our model.



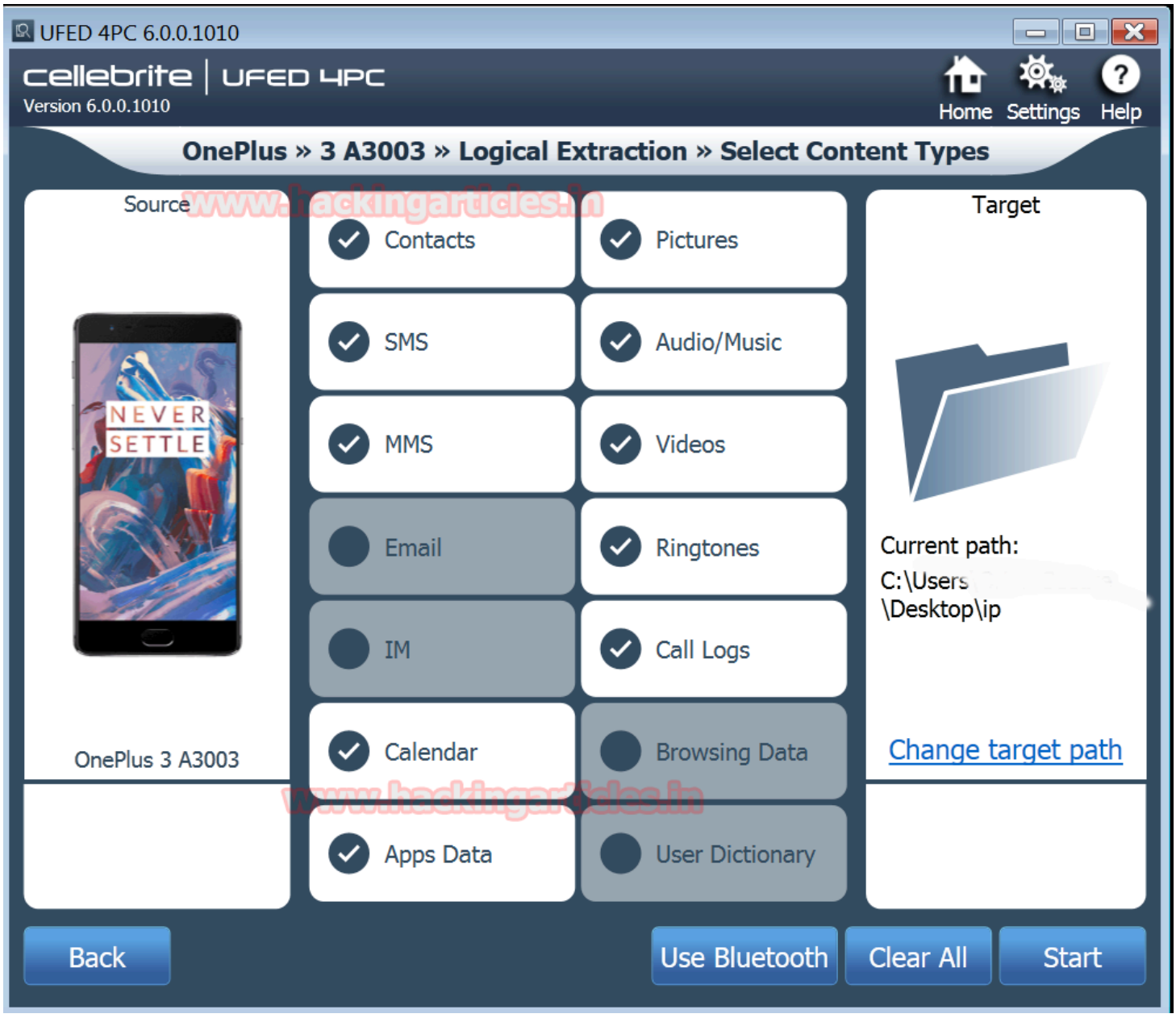
Since our mobile is ONE Plus 3 A3003 model, we put it for the forensic investigation. In order to gather information, the Cellebrite software provided us with five 'Extraction' choices ranging from Logical Extraction, File System Extraction, Physical Extraction (Root), Capture Images, Capture Screen Shots which are easy to understand and implement.

It is recommended that the investigator must click on Logical Extraction followed by Physical Extraction to gather information.

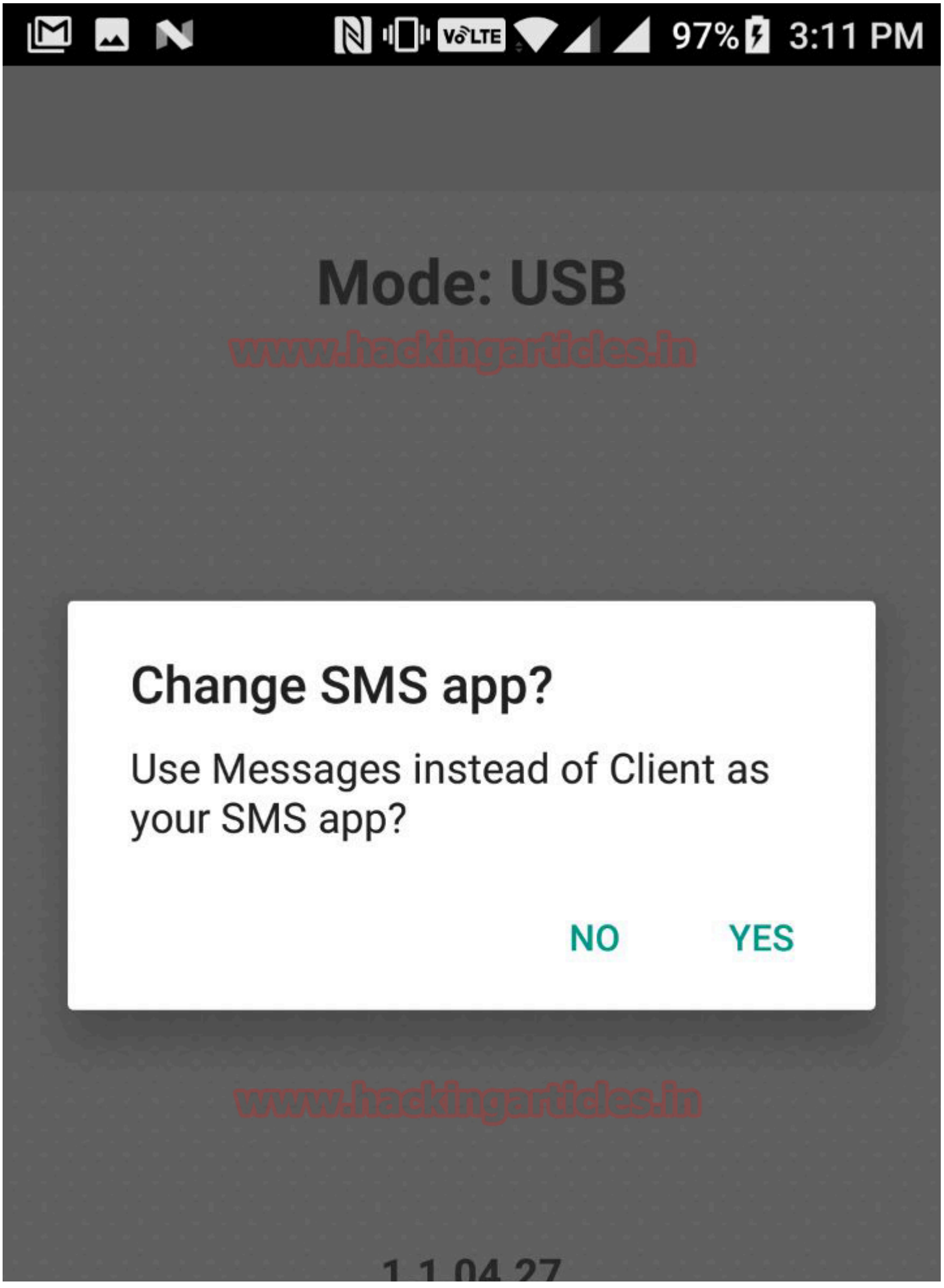


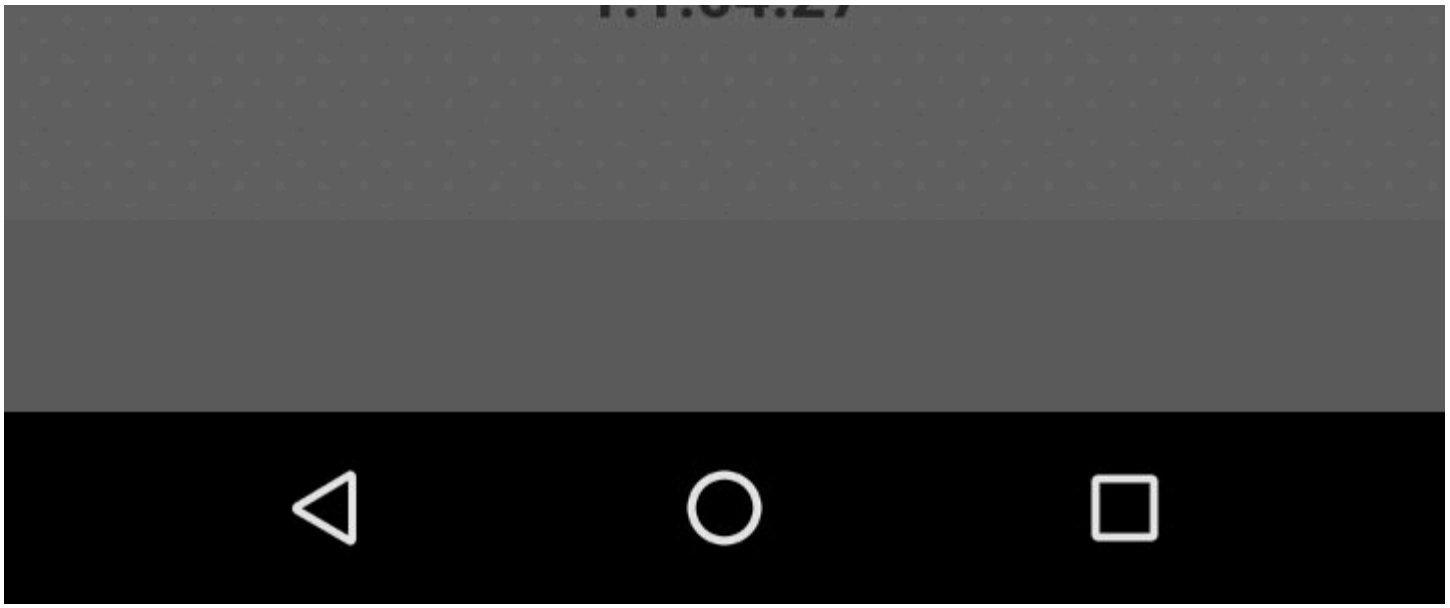
For our demonstration, we selected the Logical Extraction and selected three types of information from the Phone Memory likePhone (Phone Book), SIM (Phone Book) and Phone (Content) and press **Next**.

The Logical Extraction gave a further choice to select the type of information from the Phone Memory namely Contacts, SMS, MMS, Calendar, Apps Data, Pictures, Audio/Music, Videos, Ringtones and Call Logs.

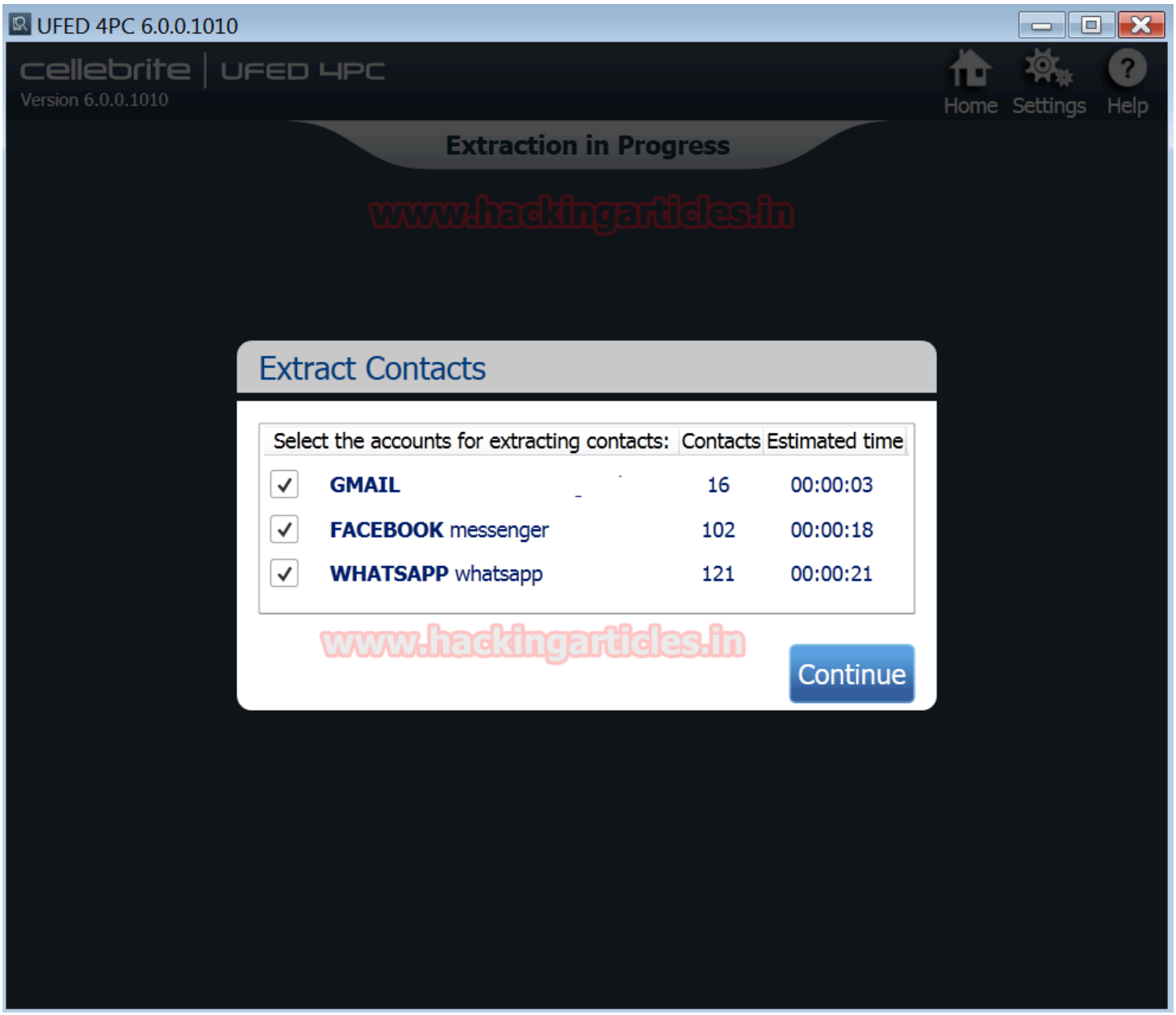


The software sends a ‘pop up’ message and in order to move further the investigator needs to click on YES.

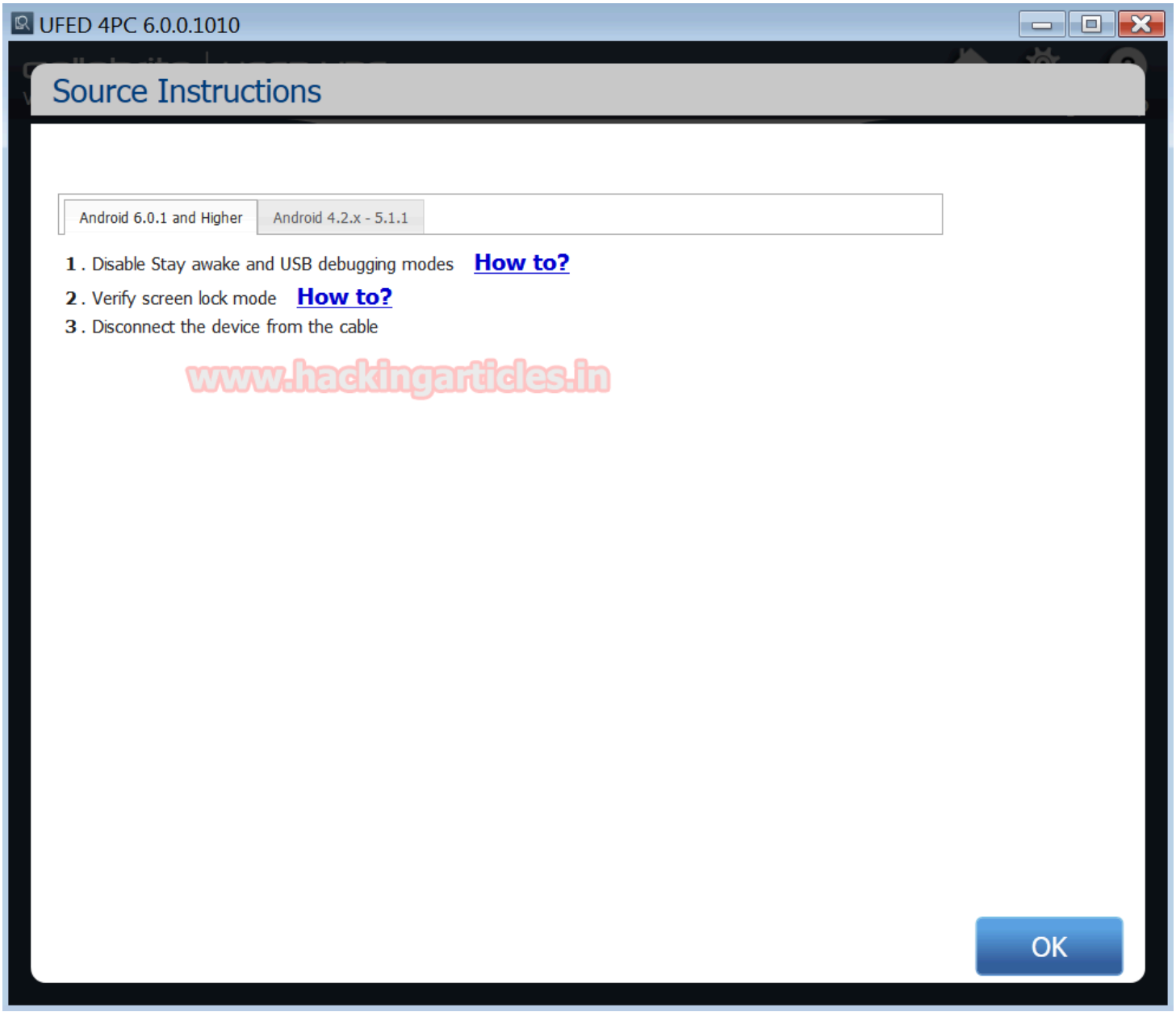

97% 3:11 PM
Mode: USB
www.hackingarticles.in
Change SMS app?
Use Messages instead of Client as your SMS app?
NO
YES
www.hackingarticles.in



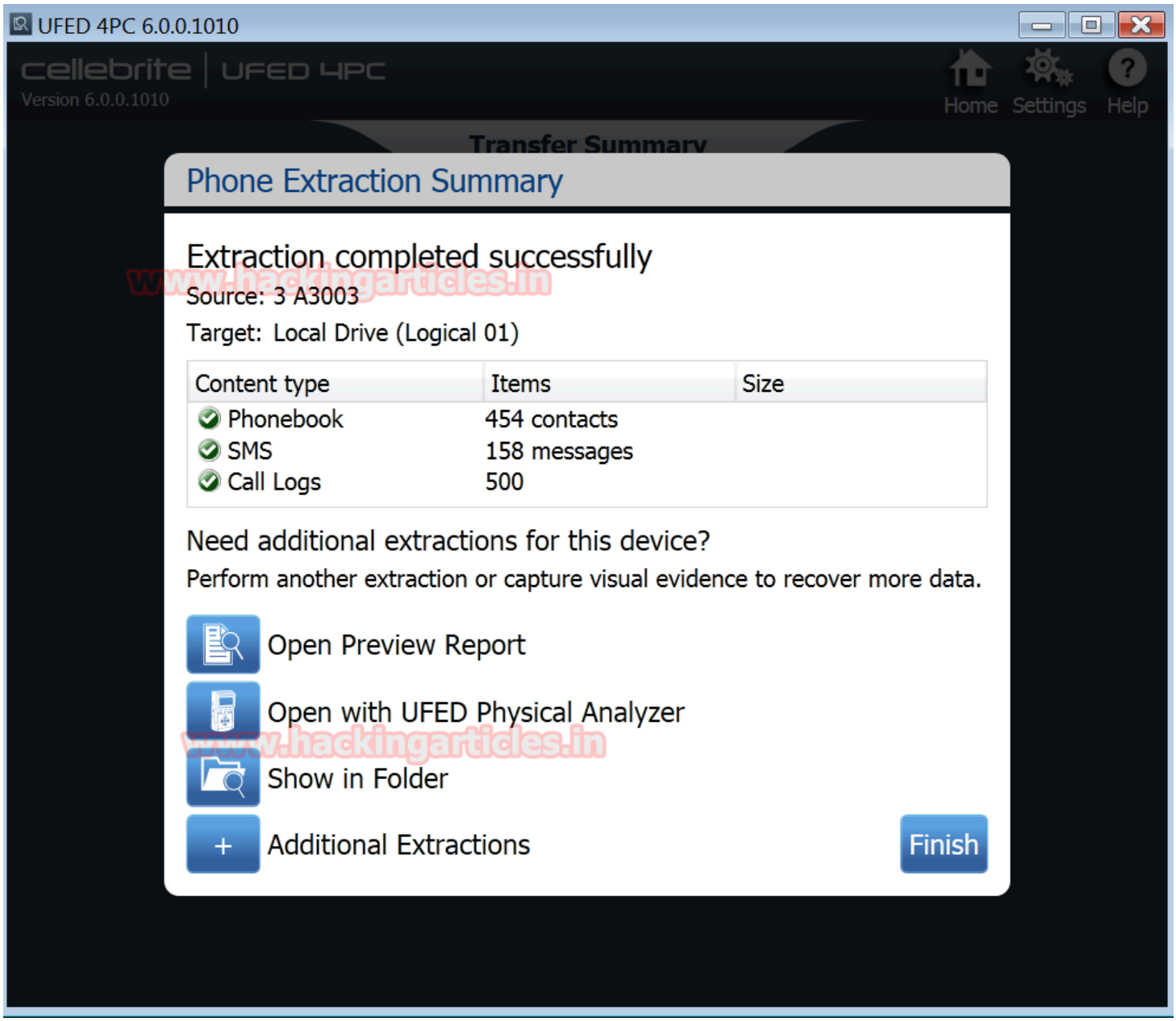
From the Contacts account we extracted contacts from Gmail, Face book messenger and Whatsapp as displayed below.



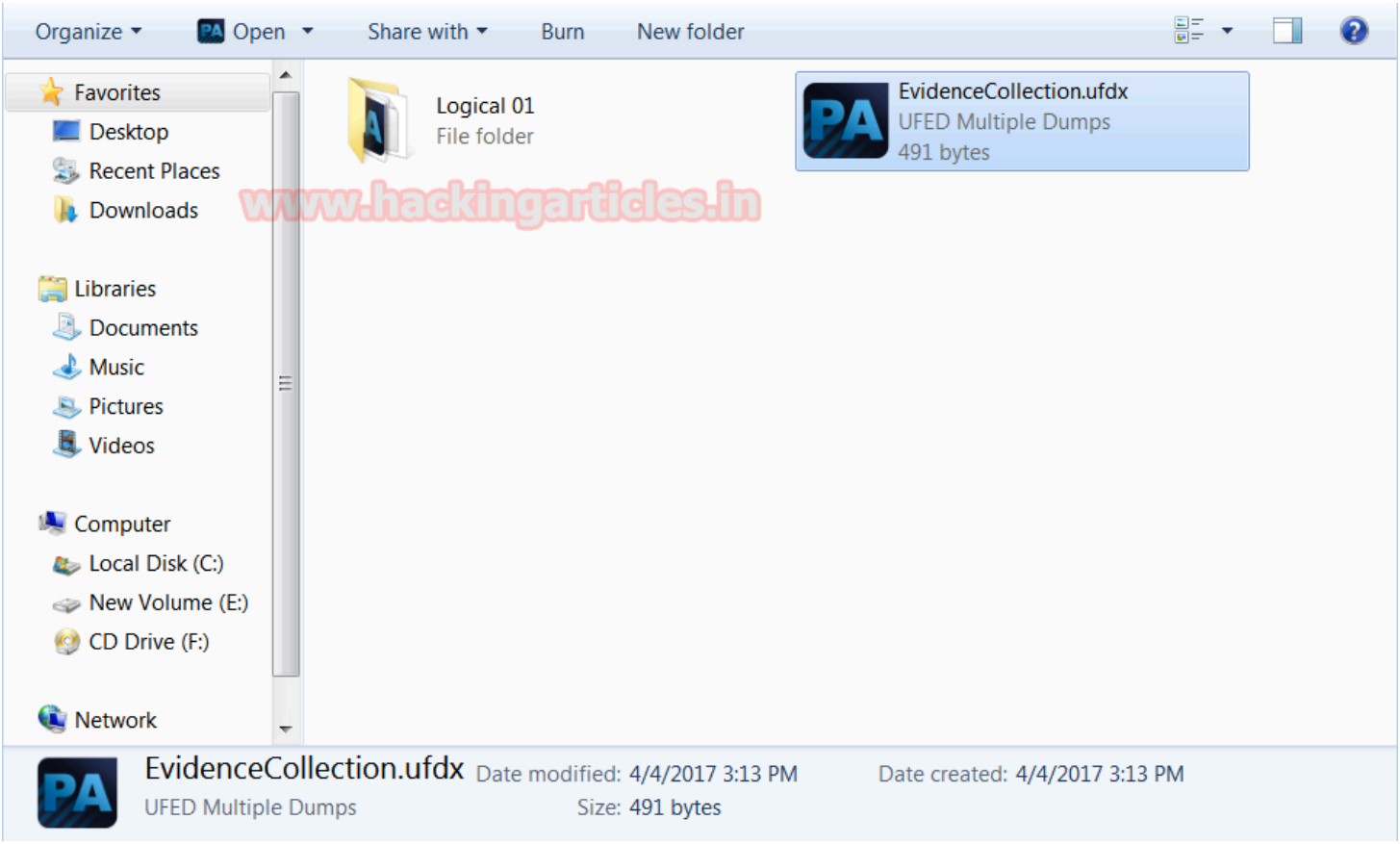
The Cellebrite software provides the investigator with source instructions to proceed further on the case by just clicking on the ‘How to?’



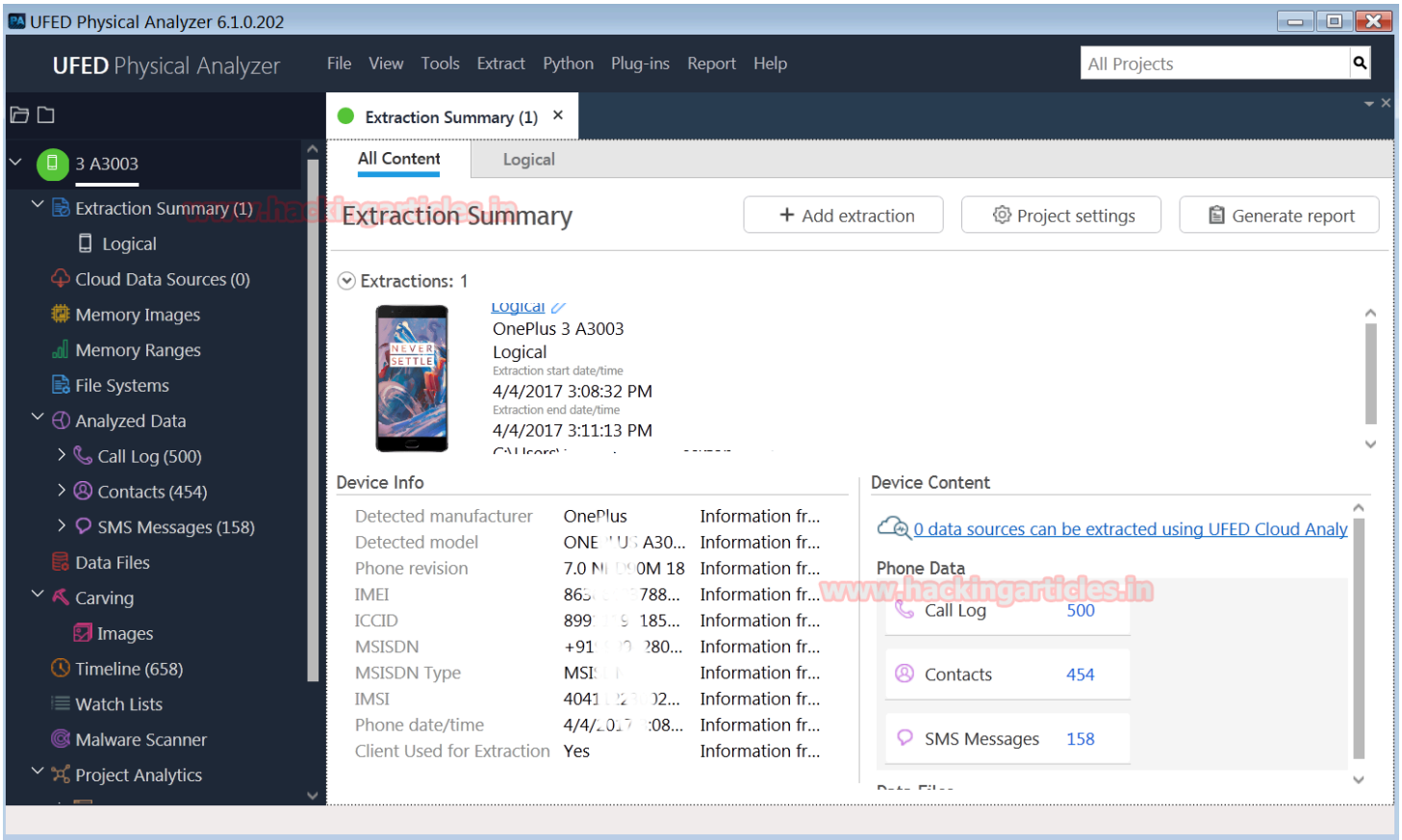
The Logical Phone Extraction was completed successfully. The details of the number of information gathered from Phonebook, SMS, and Call Logs from the mobile under forensic investigation is highlighted.



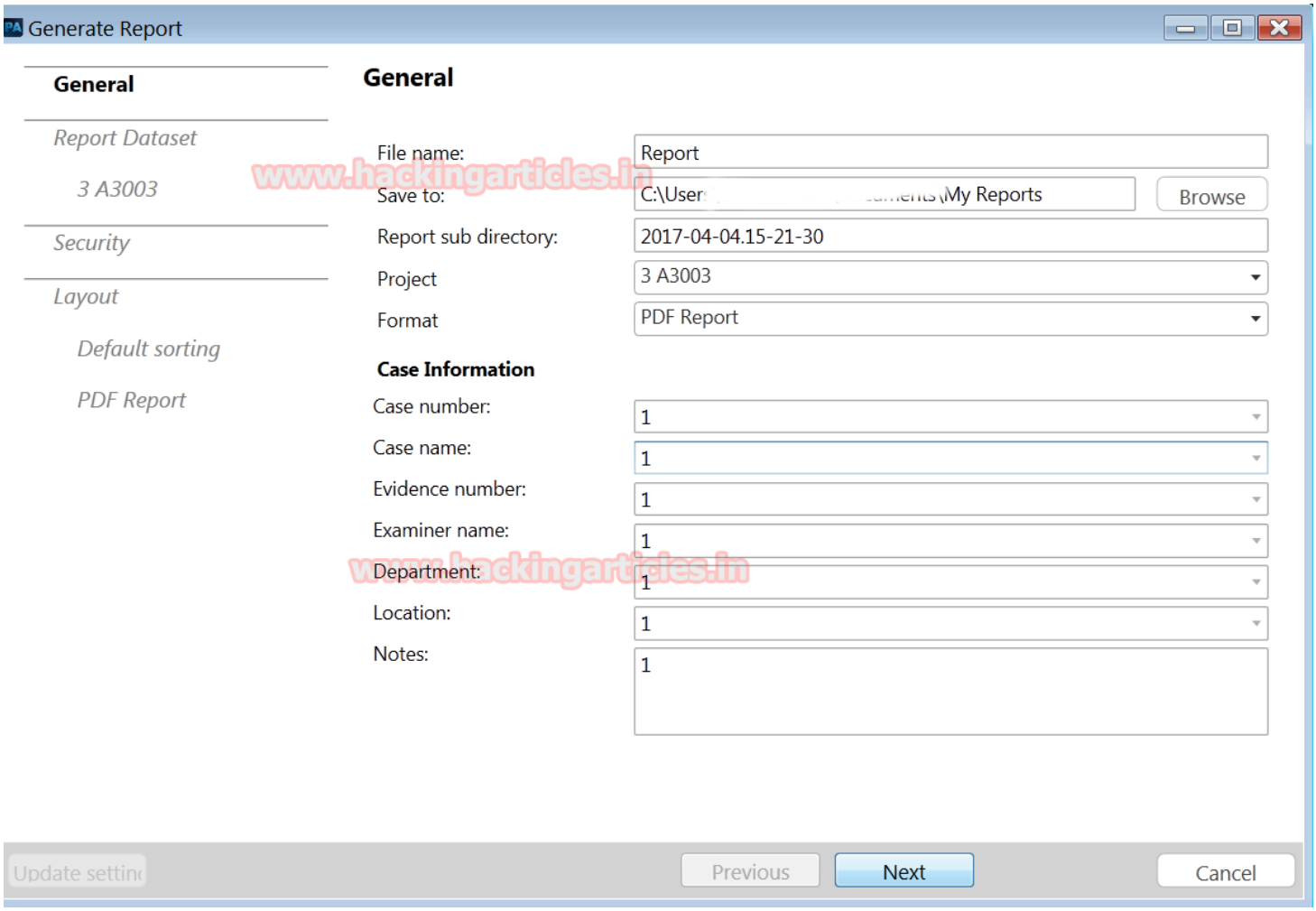
The software displays another pop up ‘PA Evidence Collection.ufdx’ along with the Logical 01 folder for the investigator



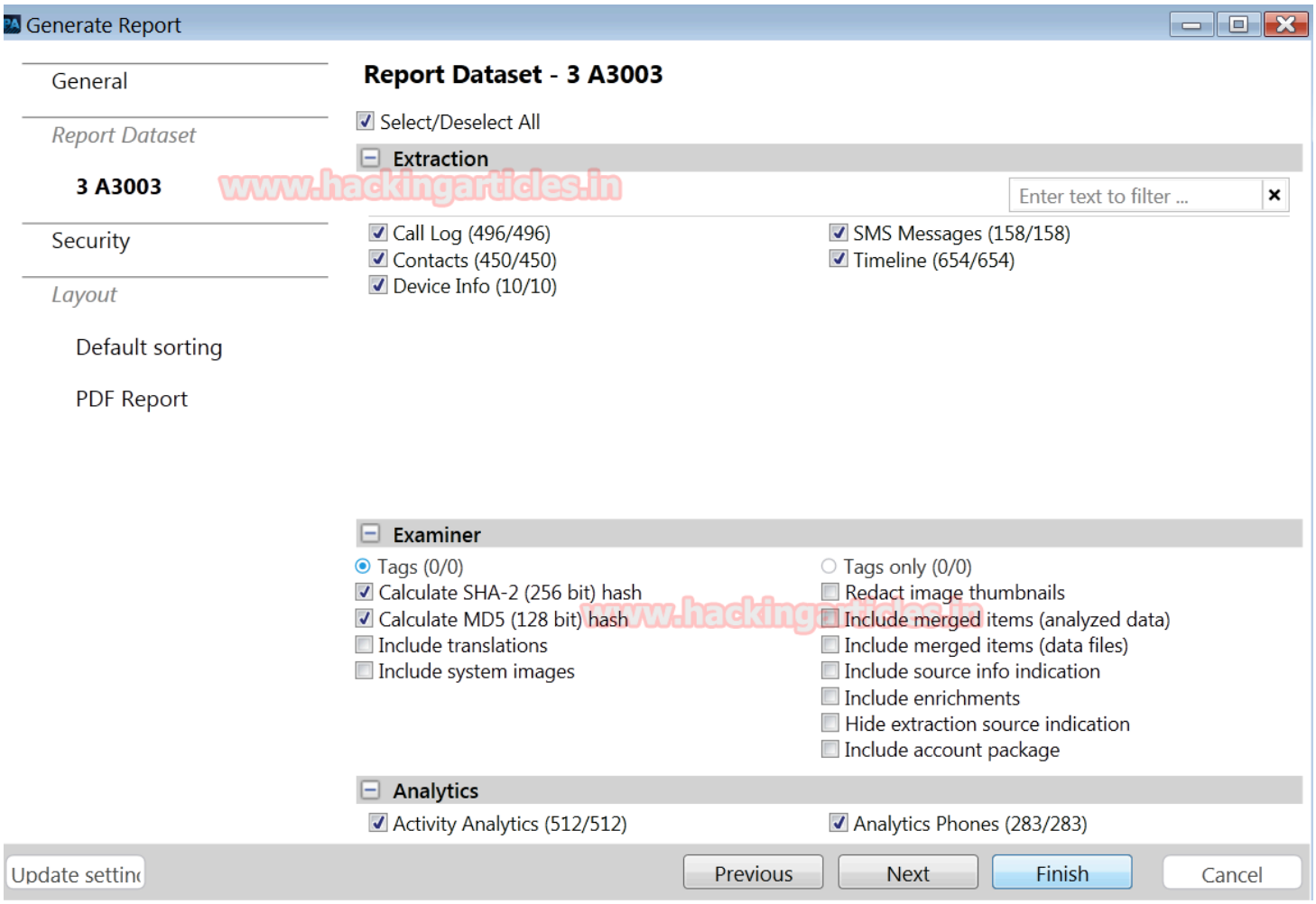
The UFED Physical Analyzer report of the mobile phone was captured by Cellebrite. The analyser captured content of the mobile model information ranging from the model name, IMEI, ICCID, MSISDN, IMSI to name a few.



Before making the final report, a case management form needs to be filled up by the investigator which provides –the case number, name, evidence number, examiner name, department, location, notes, name of the report, document details, project name as well as format. The report will be submitted in PDF or word or any other format. The final report is generated by pressing Next command.



Summary of the Cellebrite UFED report on mobile under forensic investigation.



Extraction Report

Cellebrite UFED Reports

Summary

UFED Physical Analyzer version	6.1.0.202
Report creation time	4/4/2017 3:25:26 PM +05:30
Time zone settings (UTC)	Original UTC value
Case number	1
Case name	1
Evidence number	1
Examiner name	1
Department	1
Location	1
Notes	1

Source Extraction

Logical	
Extraction start date/time	4/4/2017 3:08:32 PM
Extraction end date/time	4/4/2017 3:11:13 PM
UFED Version	6.0[illegible]1010
Internal Version	4.3.[illegible] 1010
Selected Manufacturer	OnePlus
Selected Device Name	3 A[illegible]
Connection Type	Cable No. 170
Extraction Type	Logical
Extraction ID	[illegible]
Report type	Phone
Unit Identifier	751[illegible]