Presentation Script

Slide 1

The global statistics of internet usage in 2020 is 50.88%, gradually increasing to 56% for this year compared to a desktop which is 46.39% and tablets at 2.74%.

Slide 2

Evidence collection from smartphones is very crucial. Examiners are extracting data, preserving them, building hypotheses or examining and presenting digital evidence can all aid in solving legal cases. They use sam brother's forensic tool classification.

Going from below to the top

Manual extraction: Requires human intervention to acquire the data from the mobile device.

Logical extraction: examiners use a wired connection like a USB or a wireless connection like IrDA, WiFi or Bluetooth to extract data.

Hex Dump/Physical extraction: Deals with the basic information stored in the flash memory of the mobile device.

The most promising part of this method is the tool's ability to parse and decode the captured image and make this information available to the examiner with the logical view of the file system.

Chip-Off: requires physical removal of the flash memory to acquire the data directly from the mobile phone. After extracting the data, examiners create a binary image of the removed chip with the help of reverse engineering on the wear levelling algorithm. After this, data analysis helps with information gathering.

The biggest challenge of chip-off is that it requires extensive training.

Micro Read: This method requires recording the physical observation of the gates (NAND or NOR) on the chip using an electron microscope. It requires an extreme level of technicalities, and so it is used only for high-profile cases equivalent to the national security crisis.

slide 3

This presentation focuses on the comparison of 6 mobile forensic tools as stated in 3 papers from 2013, 2015 and 2021.

Slide 4

In 2013, Ali complained that his contact list received text messages from WhatsApp and as per the ISP report, his contact list received the messages, but there was no record of it on his phone.

With the help of tools Oxygen Forensic Suite and UFED Physical Analyzer cellebrite, Al-Hadadi and Alshidhani extracted the artifacts as shown in the table from the iPhone4 running ios 5.0.1 to recreate the scenario.

Slide5

The investigation with Oxygen forensic suite found the most valued information such as IMEI, IMSI and ICCID in such mobile that used in given crimes scenario, acted as primary evidence.

UFED Physical Analyzer cellebrite, interfaces logged in and have sent messages to WhatsApp gives more insight on the technique used, connection time and date can act as legal evidence.

Possibilities from facts obtained

1. The attacker removed the Subscriber Identity Module (SIM) card and used the WiFi network to deliver a WhatsApp message.
2. Ali sold his smartphone but did not delete the WhatsApp application, and the new owner used a WiFi network to deliver WhatsApp messages to Ali's contacts.

Slide 6

Similarly, in 2015 Ritika, Priya and Pooja used MOBILedit Lite and Autopsy 3.1.2, details such as SMS, Call registers, Images, Songs, Videos and Files for investigation, to understand how to take evidence from mobile phones and how to analyze them for information retrieval for crimes like the Mumbai terrorist attack.

MOBILedit Lite comes with a write blocker (read-only) feature to ensure the integrity and that the evidence is not contaminated.

MOBILedit Lite and Autopsy 3.1.2 alone are not sufficient to recover deleted items. Additional open source or commercial tools help with additional functions such as authentication bypass, SIM cloning and retrieving internet data browsing.

Slide 7

Using the Timeline Analysis report of Autopsy 3.1.2, the sequence of events can be established and useful in event reconstruction.

slide 8

Various criminal activities, such as child sexual abuse, often use chat application services.

In December 2021, Leonardo and Indrayani used MiChat and SayHi as materials for forensic investigations using three different tools, namely MOBILedit, Magnet Axiom, and Belkasoft.

For MiChat application

Added a rooting process as an option if data extraction is not optimal even when using these three applications on a Samsung device.

For both (with or without root access)

MiChat managed to find evidence in the form of 2 avatars, using the Magnet Axiom tool only.

Other shreds of evidence were in the form of database files and conversation activities accompanied by other supporting evidence.

For SayHi Chat

Without root access

especially for Magnet Axiom tools, authentic evidence was in the form of an image file (proof of transaction) and one video file (proof of transaction)

Slide 9

With root access

For MOBILedit, they could find authentic evidence in the form of 1 image file and two avatars of suspect and client accounts.

Other shreds of evidence were in the form of database files and conversation activities on three forensic tools.

Based on the facts presented, it concluded that the recommended tool according to the scenario is Magnet Axiom.