D. B. J. COLLEGE, CHIPLUN

Page No. : _____

DEPARTMENT OF COMPUTER SCIENCE

Expt. No.

Name : Piyush Pandurang Burate Class : TYCS Roll No.: 523

Title of Experiment : Acquisition of phones and mobile devices

Date

Sub titles : Assignment/ Problem Solution, Flow chart/Algorithm, Problem Listing, Input Screen, Output Screen, Comments (If any)

Aim :- To study about acquisition of cell phones and mobile devices.

~~SoftW~~

SW/HW Requirements :- MoBILEdit, Forensic connector, printer, computer.

Theory :-

- Understanding Acquisition procedure for cell phones and mobile devices.
- The main concerns with mobile devices are loss of power, synchronization with cloud services and remote wiping.
- All mobile devices have volatile memory- making sure they don't lose power before you can retrieve ~~R~~ PAM data is critical
- Mobile devices attached to PC via a USB cable should be disconnected from the PC immediately.
- Helps prevent synchronization that might occur automatically and overwrite data.
- Depending on warrant or subpoena the time of seizure might be relavant.

Remark

Signature

- Messages might be received on the mobile device after seizure.
- One of the following options:
  - Place the device in airplane mode.
  - Place the device in a point can use the paraben wireless strong holdbag
  - Turn the device OFF.

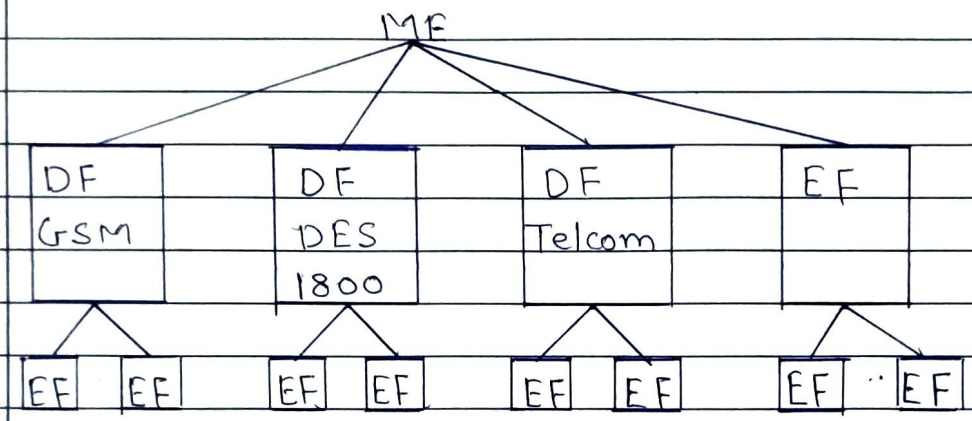
- The drawbace of using these isolating options is that the mobile device is put into roaming mode.

- Accelerate battery drainage -
SANS DFIR Forensics recommendations
- IF device is on and unlocked - isolates it from the network, disable the screen locks, remove passcode.
- IF the device is off - attempt a physical static acquisition and turn the device on
- Check these areas in forensic lab:
  - Internal memory
  - SIM card
  - Removable or external memory cards.

- Due to the growing problem of mobile devices being stolen service providers have started using remote wiping to remove a users personal info. stored on a stolen device.

- Memory storage on mobile device is usually a combination of volatile and non-volatile memory

- The File system for a SIM card is a heirarchical structure

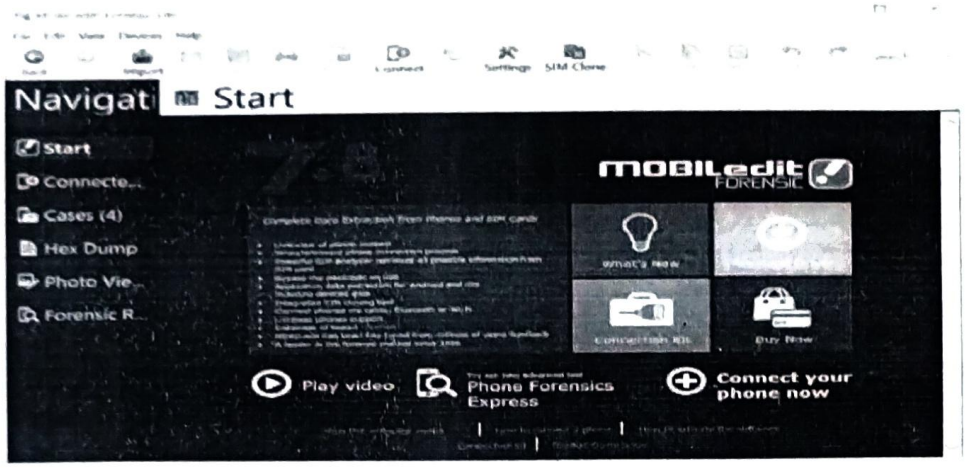


- Information that can be retrived falls into Four categories :-
  - Service-related data, such as identities For the SIM card the subscriber.
  - Call data, such as numbers dialed, message information.

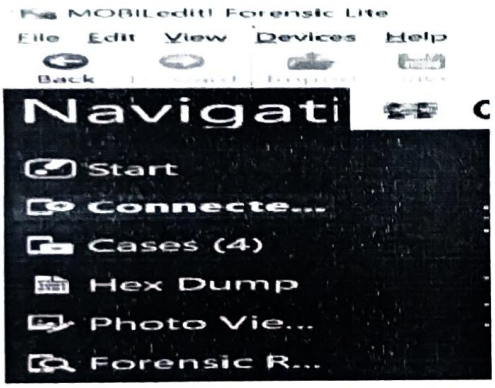
Practical 8: Acquisition of Cell phones and Mobile devices

Steps:

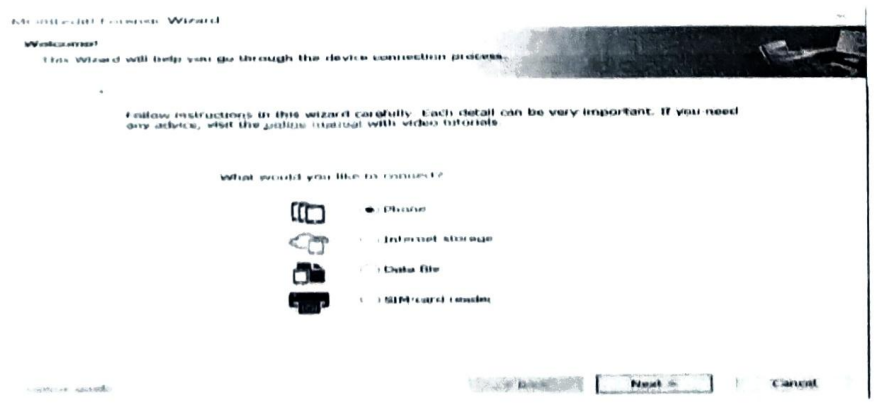
1. Download mobiledit forensic tool in mobile.
2. Open Mobiledit tool in PC.



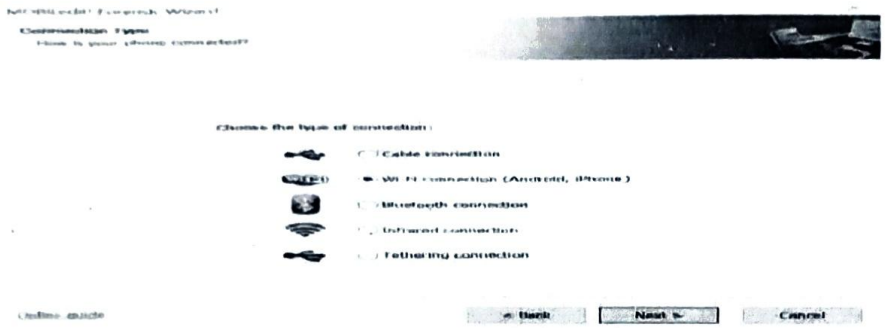
3. Click on connect.



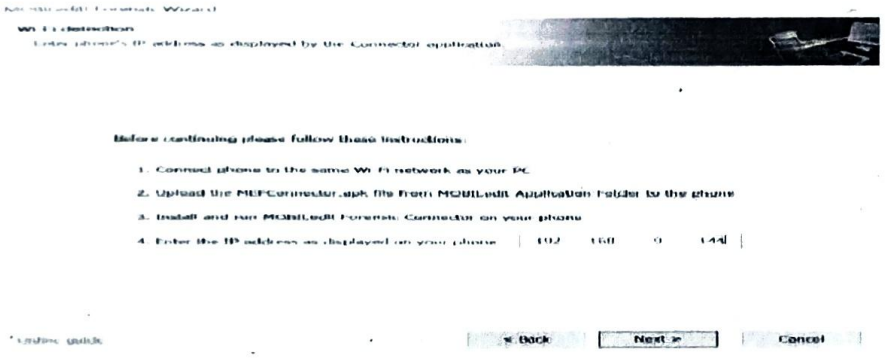
4. Connect your mobile device to the system. Click on phone > next.



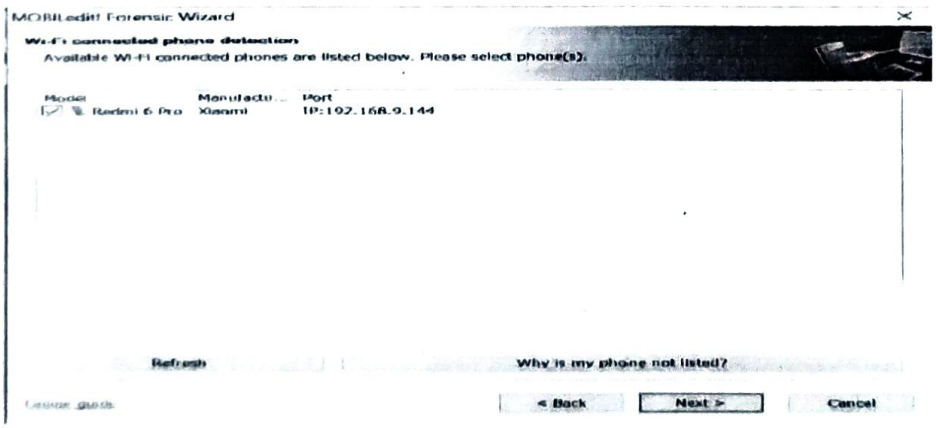
5. Click the connection



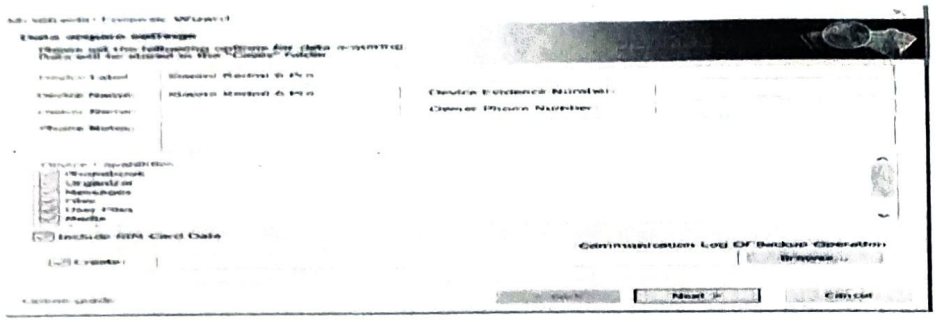
6. Open the mobiledit tool in phone and click on the type of connection (i.e Wifi) > Copy the IP address and enter it in the PC and click next.



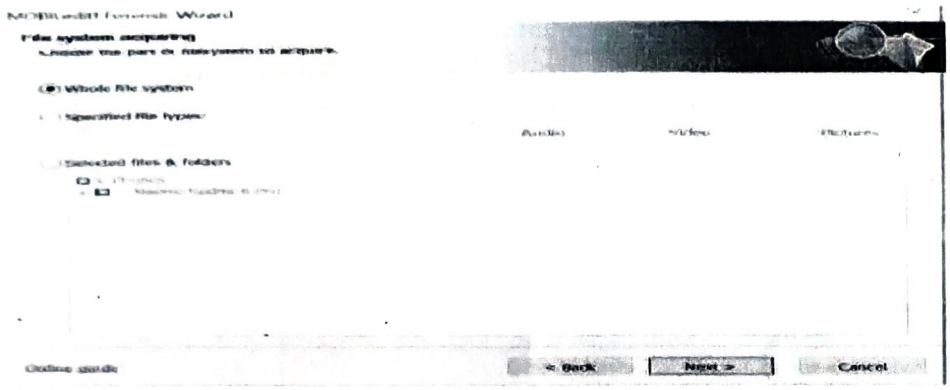
7. It shows the phone which is connected. Click on next.

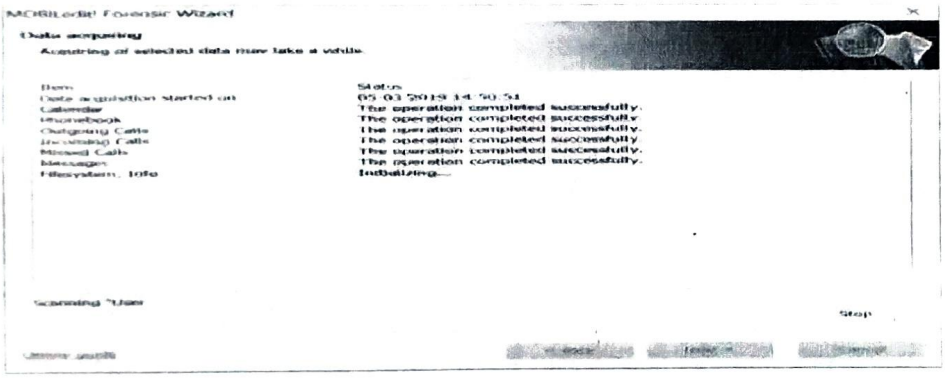


8. Click on next.

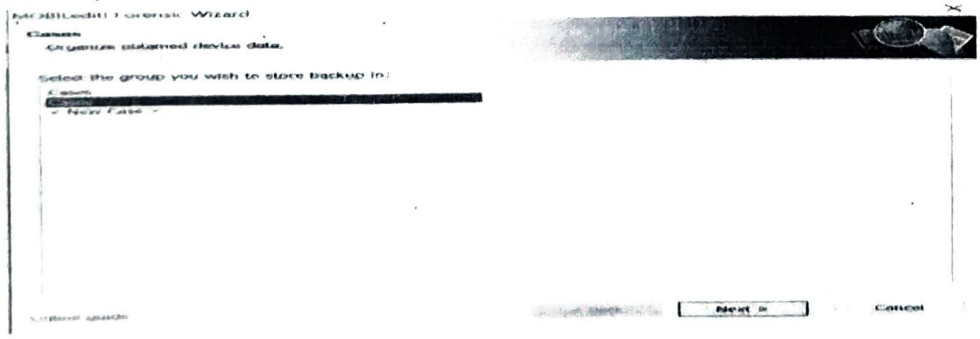


9. Click on whole system and click next.

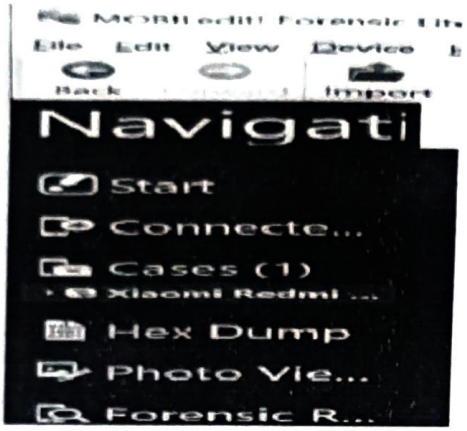




10. Click on case and click next.



11. Click on your device in the left panel.



12. You can see all the files.