12. Acquisition of Mobile Data

Objective: To learn the methods for acquiring data from mobile devices

Tools: Android Debug Bridge

Acquiring mobile data using Android Debug Bridge (ADB) involves using ADB commands to access and extract data from an Android device. This is often done for digital forensics, security audits, or to back up data and it requires enabling Developer Options and USB Debugging on the device.

Acquisition of Mobile Data using ADB on Linux OS

Here are the steps tailored specifically for Linux users for acquiring mobile data using Android Debug Bridge (ADB):

Pre-requisites for Linux:

1. Install ADB on Linux:

ADB can be installed easily via the terminal.

- **Open a terminal** and run the following command to install ADB:

```
sudo apt update
sudo apt install android-tools-adb
sudo apt install android-tools-fastboot
```

Alternatively, for **Fedora-based** distributions:

```
sudodnf install android-tools
```

- To **verify ADB installation**, check the version:

```
adb version
```

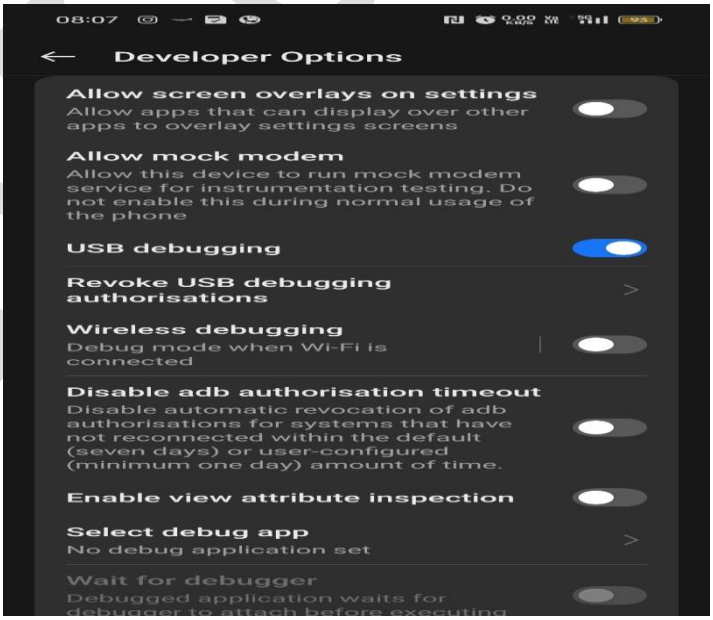
```
┌──(root㉿kalieverything)-[/home/kalieverything]
└─# apt-get install android-tools-adb
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'adb' instead of 'android-tools-adb'
adb is already the newest version (1:34.0.4-1).
The following packages were automatically installed and are no longer required:
  golang-1.21-go golang-1.21-src libatk-adaptor libboost-dev libopenblas-dev libopenblas-pthread-dev libopenblas0 libpython3-all-dev libpython3.12 libpython3.12-dev libxsimd-dev python3-all-dev
  python3-anyjson python3-beniget python3-certvalidator python3-endesive python3-gast python3-pyatspi python3-pykcs11 python3-pythran python3.12-dev xtl-dev
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 562 not upgraded.

┌──(root㉿kalieverything)-[/home/kalieverything]
└─# apt-get install android-tools-fastboot
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'fastboot' instead of 'android-tools-fastboot'
fastboot is already the newest version (1:34.0.4-1).
The following packages were automatically installed and are no longer required:
  golang-1.21-go golang-1.21-src libatk-adaptor libboost-dev libopenblas-dev libopenblas-pthread-dev libopenblas0 libpython3-all-dev libpython3.12 libpython3.12-dev libxsimd-dev python3-all-dev
  python3-anyjson python3-beniget python3-certvalidator python3-endesive python3-gast python3-pyatspi python3-pykcs11 python3-pythran python3.12-dev xtl-dev
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 562 not upgraded.

┌──(root㉿kalieverything)-[/home/kalieverything]
└─# adb start
adb: unknown command start

┌──(root㉿kalieverything)-[/home/kalieverything]
└─# adb start-server

┌──(root㉿kalieverything)-[/home/kalieverything]
└─#
```

2. Enable Developer Mode and USB Debugging on Android:

1. On your Android device, go to `Settings > About Phone`.
2. Tap on the **Build Number** seven times to unlock Developer Mode.
3. Navigate to `Settings > Developer Options`.
4. Enable **USB Debugging**.

3. Connect the Android Device:

1. Connect your Android device to your Linux machine using a USB cable.
2. On the phone, when prompted to select a connection type, choose **File Transfer (MTP)**.



3. Allow the computer to access the device by granting USB Debugging permissions.

Steps for Data Acquisition on Linux:

Step 1: Verify ADB connection

1. Open your terminal.
2. Run the following command to check if the Android device is recognized.

   adb devices

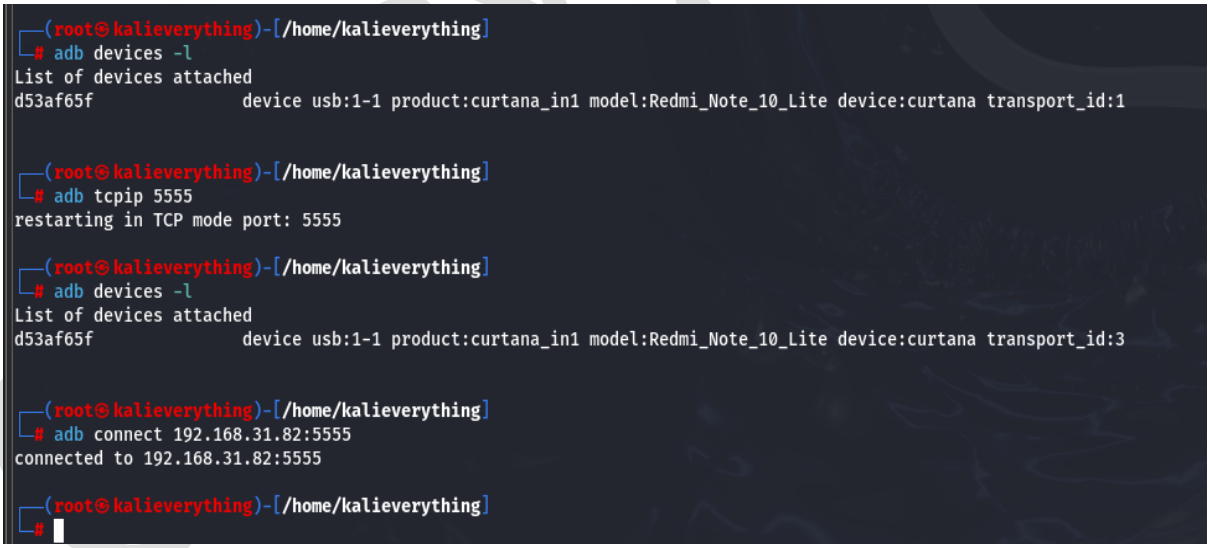
   - You should see a device ID listed with a "device" status. If the status says "unauthorized," check your phone and approve the connection.

3. To connect mobile device wireless run the following command before that note down the IP address of your mobile from – About device/Status/IP address.

   adbtcpip 5555

   adb connect 192.168.31.82:5555

   - Note: The IP address in above command is 192.168.31.82
   - Now you can unplug your mobile device and both internet should be **ON** on in your mobile phone and you can now use adb commands wirelessly.



Step 2: Retrieve Basic Device Information

To gather basic information about the device (useful for forensic documentation):

```
adb shell getprop
```

This will output system properties such as OS version, model, and build details.

Step 3: Pull Specific Data from Device

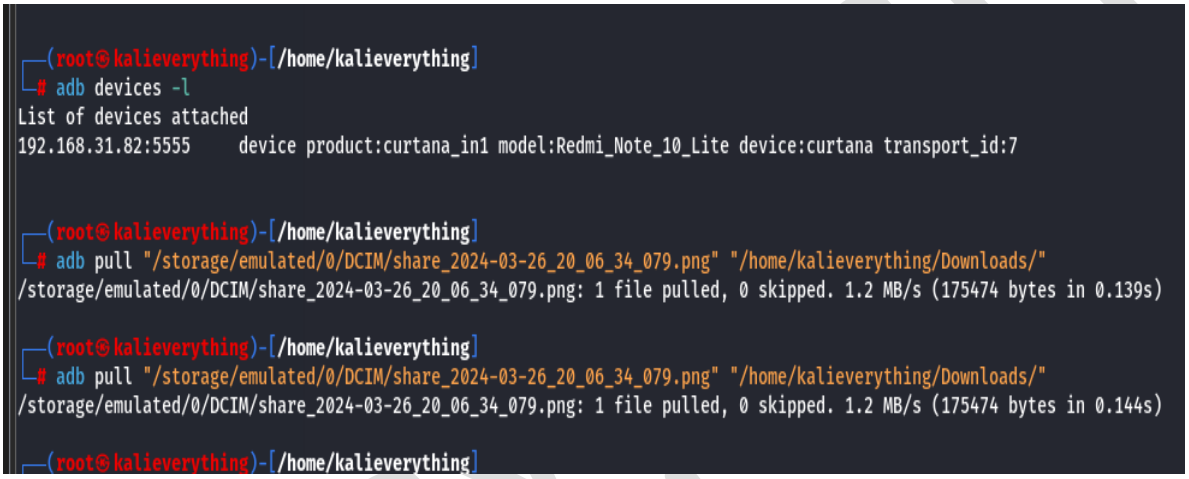
1. **Extract Photos (from DCIM directory):** To pull photos from the DCIM folder:

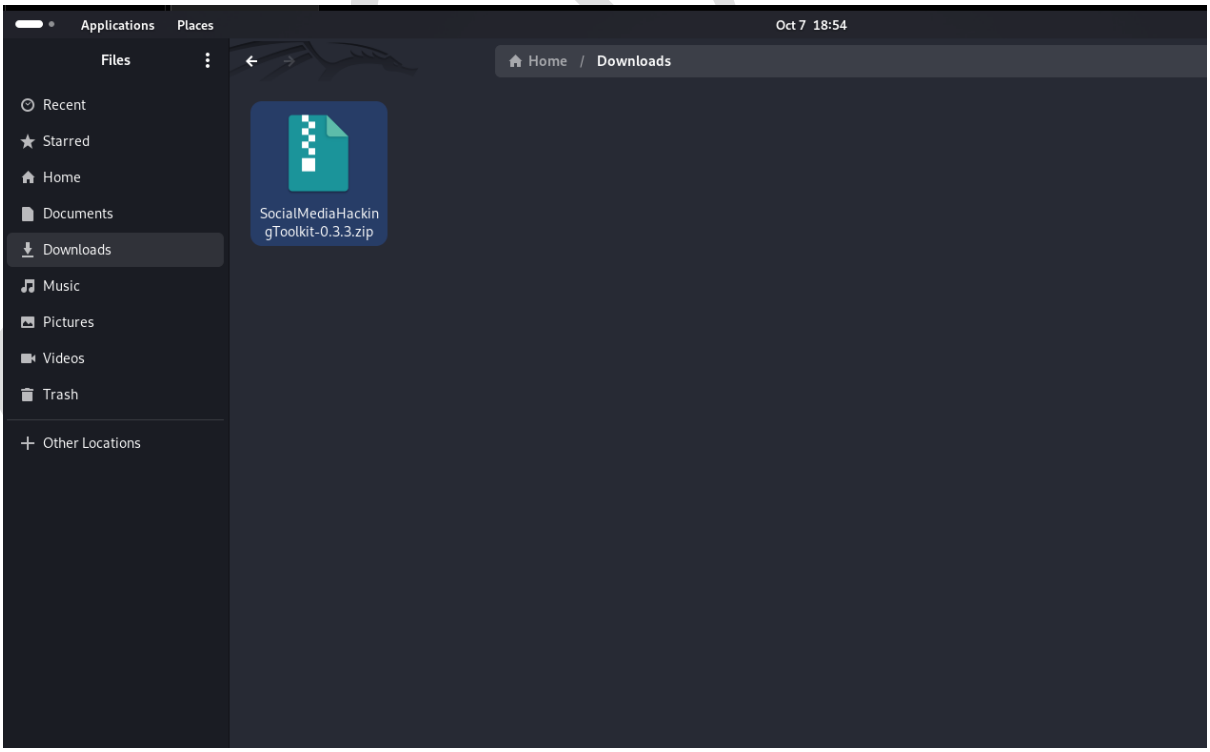
   ```
   adb pull /sdcard/DCIM/ ~/Desktop/mobile_data/photos
   ```

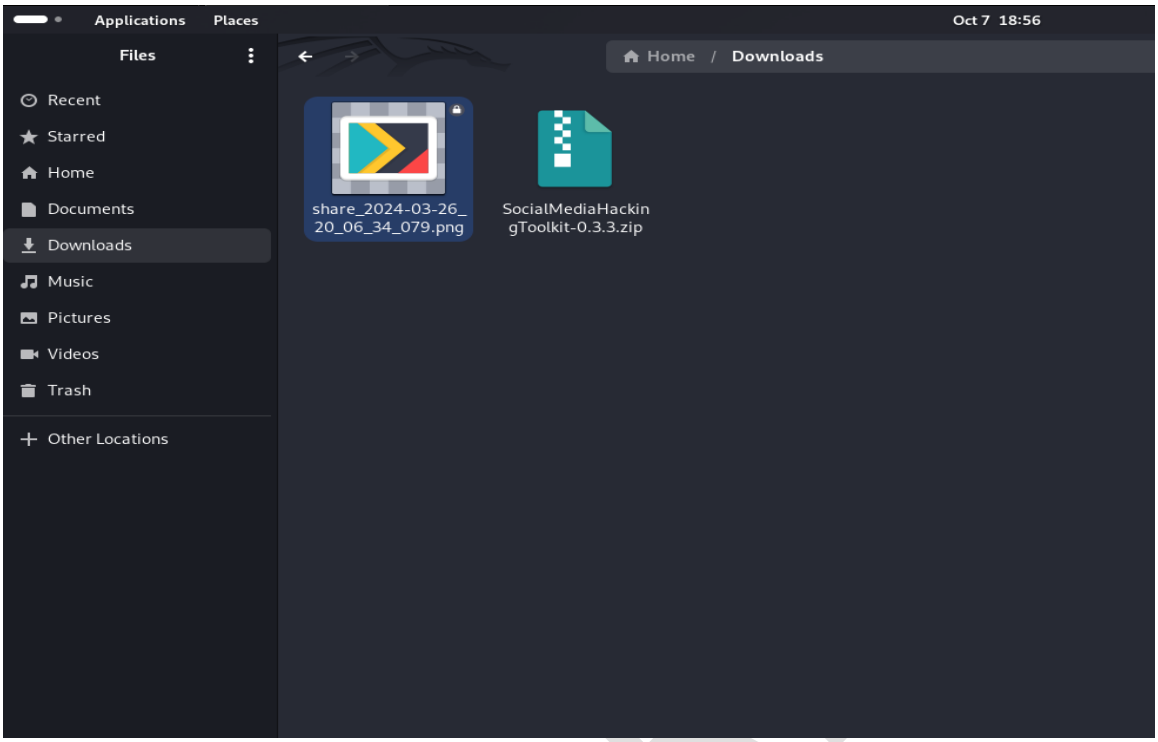
   This will transfer the photos to the `~/Desktop/mobile_data/photos` directory on your Linux machine.

2. **Extract Entire SD Card:** To copy the entire contents of the SD card:

   ```
   adb pull /sdcard/ ~/Desktop/mobile_data/sdcard
   ```






Applications
Places
Oct 7 18:56
Files
Recent
Starred
Home
Documents
Downloads
Music
Pictures
Videos
Trash
Other Locations
Home / Downloads
share_2024-03-26_20_06_34_079.png
SocialMediaHackingToolkit-0.3.3.zip