Bhuvaneshwar-Naidu Update Exp_7_AFLogical_OSE.md 4a12dba · 1 minute ago

208 lines (158 loc) · 5.35 KB

Ex.No.7: Use AFLogical OSE to Extract Data from an Android Device

Aim

To extract logical data such as contacts, messages, call logs, and other user information from an Android device using **AFLogical OSE (Open Source Edition)** as part of digital forensic analysis.

STEP 1 — Initial Setup & File Extraction

Required Files (Pre-requisites)

- **Android Platform Tools (ADB):** For device communication
- **AFLogical OSE ZIP (Source/APK):** Core forensic extraction tool
- **Google USB Driver (Windows):** For PC-device connectivity

Instructions

1. Create the main lab directory:

```
C:\DF
```

2. Extract all downloaded ZIP archives into this folder:

```
C:\DF\platform-tools\
C:\DF\aflogical-ose\
C:\DF\usb-driver\
```

3. **Note:**
   If `AFLogical-OSE.apk` is missing, use **Santoku Linux** or another forensic OS to build or extract it from the source.

STEP 2 — Configure System Environment (PATH)

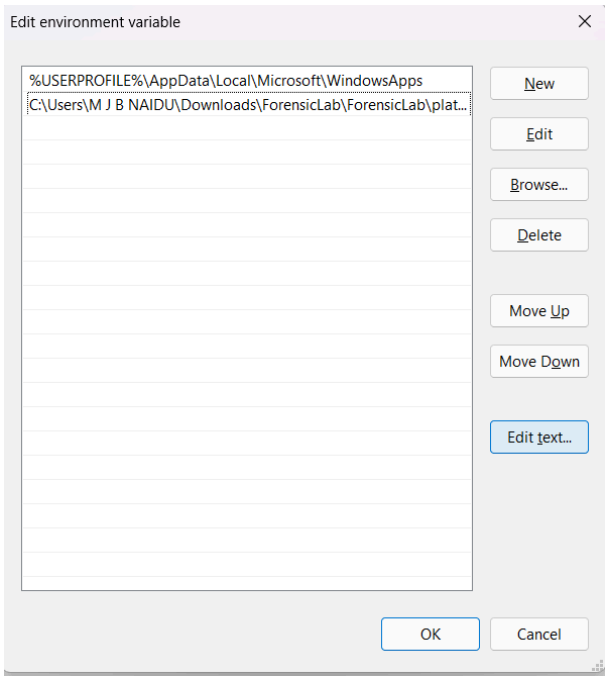
Purpose

To make `adb` commands accessible from any terminal or command prompt without specifying the full path.

Steps

1. Open:
   Control Panel → System → Advanced system settings → Environment Variables
2. Under *User Variables*, select **Path → Edit → New**.
3. Add:

```
C:\DF\platform-tools
```

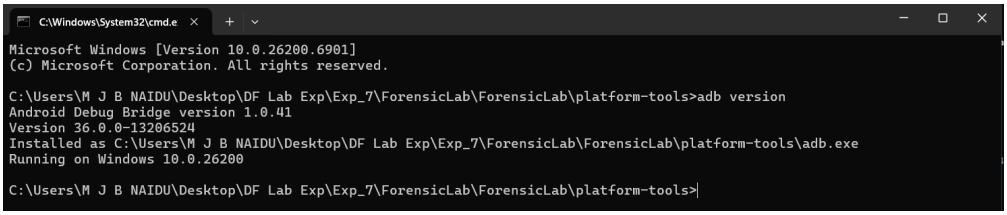


4. Click **OK** to apply.

Verification

Run:

```
adb version
```



Expected Output:
Displays the installed **Android Debug Bridge version**.

STEP 3 — Install Google USB Driver (Windows Specific)

Purpose

To ensure the Windows system can identify and communicate with the connected Android device.

Steps

1. Connect the Android phone via USB.
2. Open **Device Manager** → Locate your phone.
3. Right-click → **Update Driver** → **Browse my computer for drivers**.
4. Specify path:

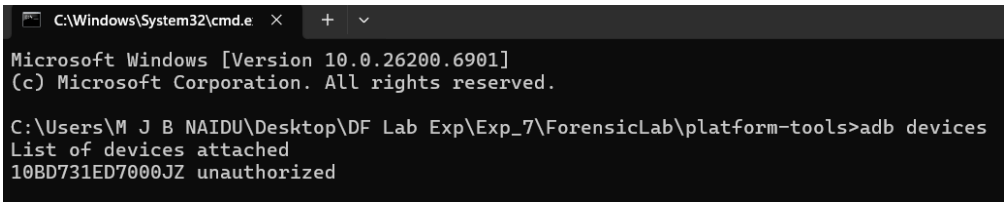
   ```
   C:\DF\usb-driver
   ```

5. Click **Next** to complete installation.

Verification

Run:

```
adb devices
```



Device should be listed as "**device**", not *offline* or *unauthorized*.

STEP 4 — Prepare the Android Device (Developer Options)

Steps

1. Go to **Settings → About Phone → Tap "Build Number" 7 times**.
2. Return to **Settings → Developer Options**.
3. Enable:
   - USB Debugging
   - Install via USB (if available)

STEP 5 — Establish and Verify ADB Connection

Purpose

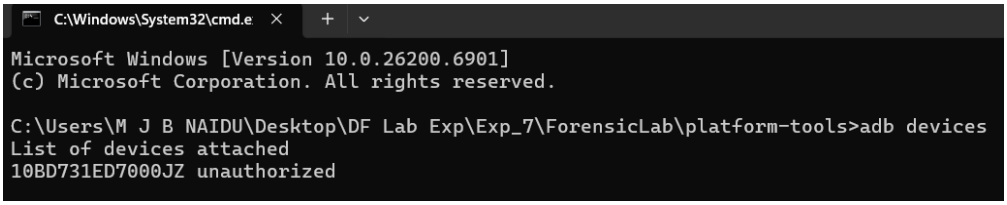
To confirm a stable and authorized link between your computer and the Android device.

Steps

1. Connect your phone via USB.
2. Run:

```
adb devices
```

3. Tap **Allow** on the phone if prompted for debugging authorization.



Troubleshooting

If the device shows as *unauthorized*, replug it and reauthorize USB debugging.

STEP 6 — Deploy AFLogical OSE to the Device

Purpose

To install the AFLogical forensic application on the Android device.

Steps

1. Confirm APK location:

```
C:\DF\aflogical-ose\AFLogical-OSE.apk
```

2. Install using ADB:

```
adb install --bypass-low-target-sdk-block "C:\Users\Manya\Downloads\DF\
```

STEP 7 — Execute Logical Data Extraction

Purpose

To perform the actual data extraction from the Android device using AFLogical.

Steps

1. Open **AFLogical** on the Android device.
2. Grant all necessary permissions (Contacts, SMS, Call Logs, Storage).
3. Select the data types to extract:
   - Contacts
   - SMS
   - Call Logs
   - MMS
   - Calendar
4. Tap **Start Extraction**.
5. Wait for extraction to finish.

Default Save Location

```
/sdcard/aflogical/
```

or

```
/storage/emulated/0/aflogical/
```

STEP 8 — Collect Extracted Data (Pull to PC)

Purpose

To transfer the extracted `.csv` data from the Android device to your computer.

Command

```
adb pull /sdcard/aflogical C:\Users\Manya\Downloads
```

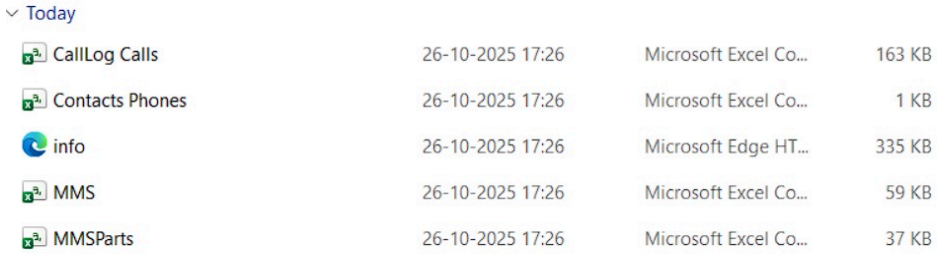
Verification

Extracted files will be saved in:

```
C:\Users\Manya\Downloads
```

The folder should contain files like:

- `contacts.csv`
- `sms.csv`
- `calllogs.csv`
- `calendar.csv`



Rubrics

Criteria	Mark Allotted	Mark Awarded
1. GitHub Activity & Submission Regularity	3	
2. Application of Forensic Tools & Practical Execution	3	
3. Documentation & Reporting	2	
4. Engagement, Problem-Solving & Team Collaboration	2	
Total	10	

Result

Successfully extracted logical data (Contacts, SMS, Call Logs, etc.) from an Android device using **AFLogical OSE**, transferred it to the computer using ADB, and analyzed the extracted `.csv` files for forensic investigation.