6/14/2025

Forensics of Mobile Phone (Andorid) with ADB Tool

Digital Forensics

Student Name(s): Shahmeer Khan-24109115, DeepChand-24109105

Teacher Name: Muhammad Waqar

Course Name: Digital Forensics

Introduction:

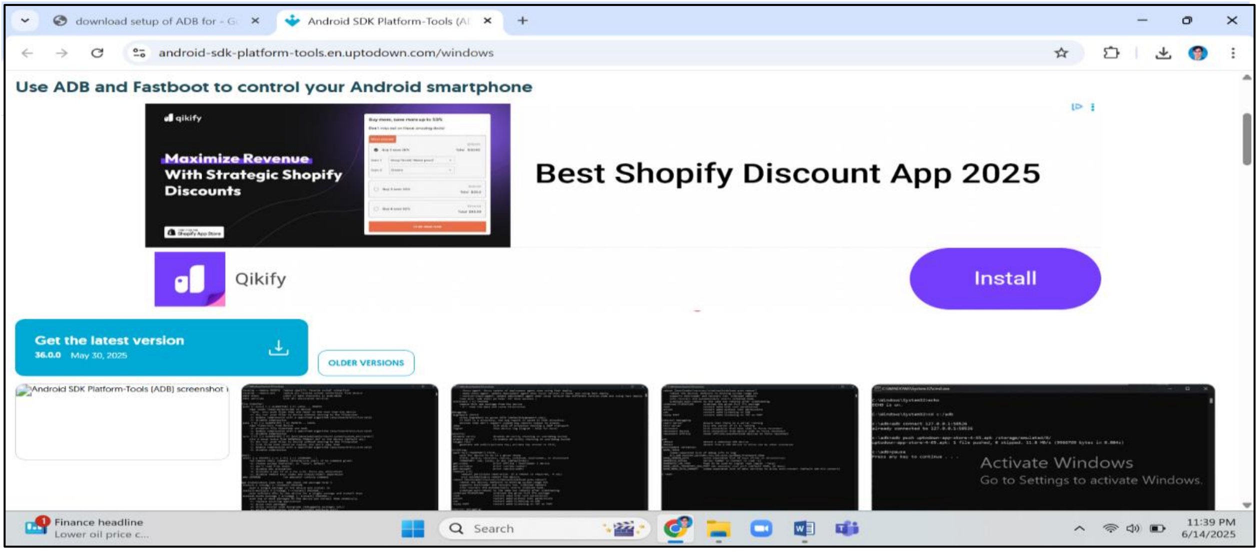
Peform the forensics of mobile phone (Android) to get the records as an evidence of data movement from mobile device to the windwos OS. Additionally, to check the mobile phone hardware detaisl, software details, versions, and repositries including the folders existance in the mobile phone.

Project Execution details:

We have pefomred the forensics of the project 'Forensics of Mobile Phone (Android) with ADB tool', in which intilally we have execute the project by downloading and installation of tools and then perfomed the activities, later in the end to gather the evidences performed the forensics of all activities which were requried record purspose.

Executions Steps:

- Downloading and Installation of the software **ADB**



download setup of ADB for - G | Android SDK Platform-Tools (A

android-sdk-platform-tools.en.uptodown.com/windows

Use ADB and Fastboot to control your Android smartphone

qikify
Maximize Revenue With Strategic Shopify Discounts
Best Shopify Discount App 2025
Qikify
Install

Get the latest version
36.0.0 May 30, 2025

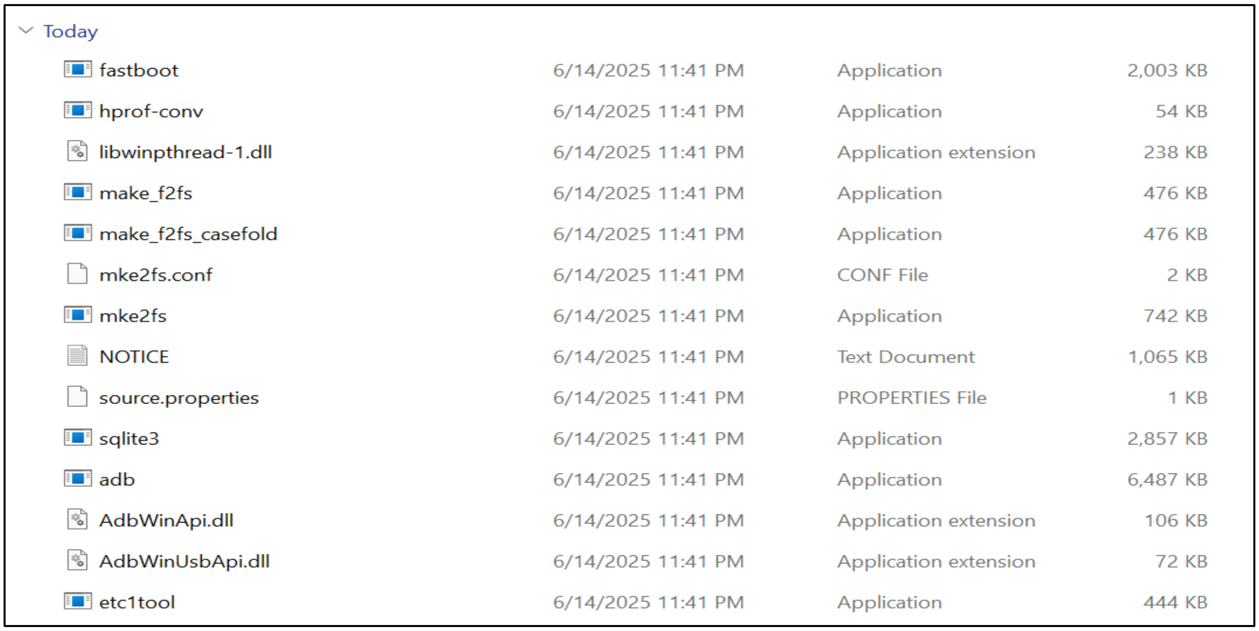
OLDER VERSIONS

Android SDK Platform-Tools (ADB) screenshot 1

Activate Windows
Go to Settings to activate Windows.

Finance headline
Lower oil price c...
Search
11:39 PM
6/14/2025

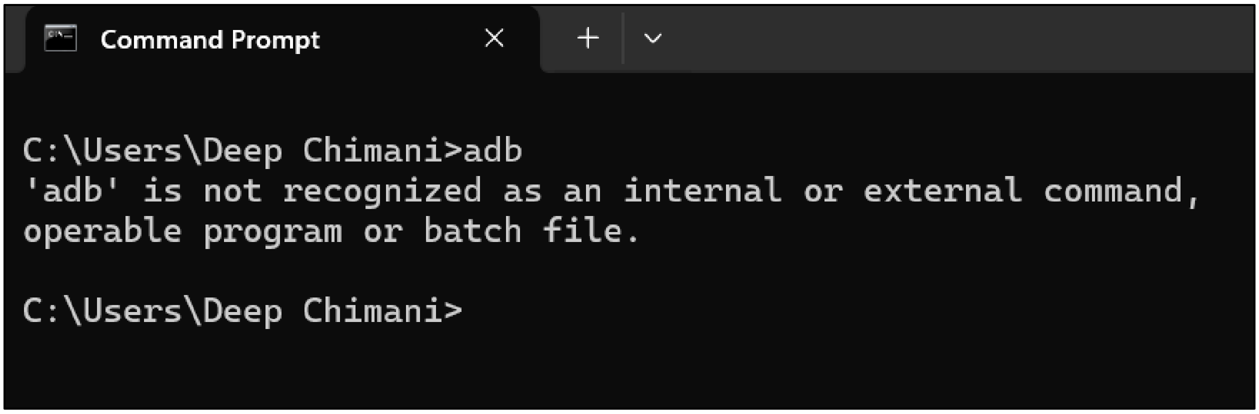
- After downloading the folder containing the file of ADB.



Today

fastboot	6/14/2025 11:41 PM	Application	2,003 KB
hprof-conv	6/14/2025 11:41 PM	Application	54 KB
libwinpthread-1.dll	6/14/2025 11:41 PM	Application extension	238 KB
make_f2fs	6/14/2025 11:41 PM	Application	476 KB
make_f2fs_casefold	6/14/2025 11:41 PM	Application	476 KB
mke2fs.conf	6/14/2025 11:41 PM	CONF File	2 KB
mke2fs	6/14/2025 11:41 PM	Application	742 KB
NOTICE	6/14/2025 11:41 PM	Text Document	1,065 KB
source.properties	6/14/2025 11:41 PM	PROPERTIES File	1 KB
sqlite3	6/14/2025 11:41 PM	Application	2,857 KB
adb	6/14/2025 11:41 PM	Application	6,487 KB
AdbWinApi.dll	6/14/2025 11:41 PM	Application extension	106 KB
AdbWinUsbApi.dll	6/14/2025 11:41 PM	Application extension	72 KB
etc1tool	6/14/2025 11:41 PM	Application	444 KB

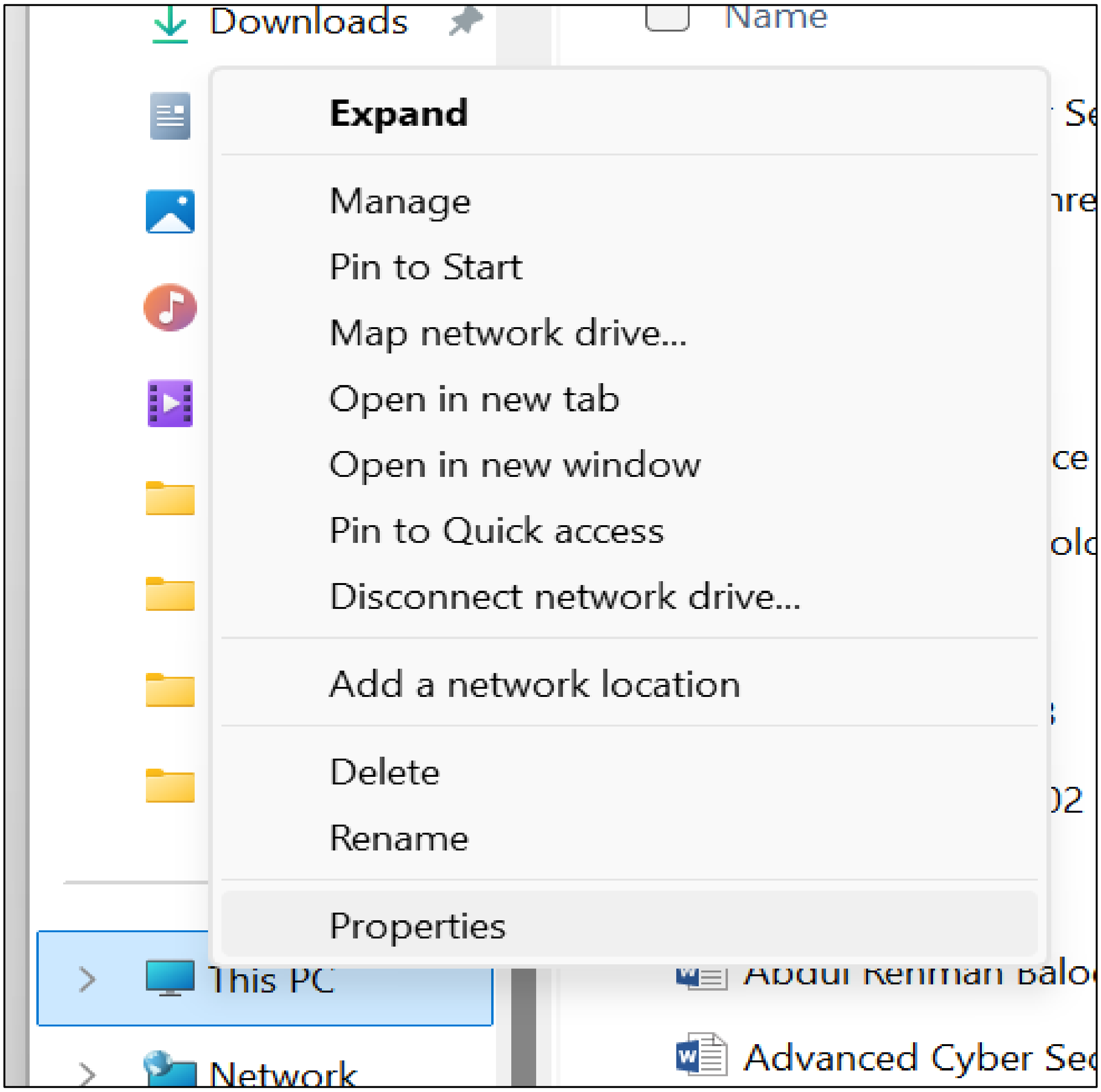
- Run the CMD with Administrator rights and type ‘**adb**’ to check the adb existance status.

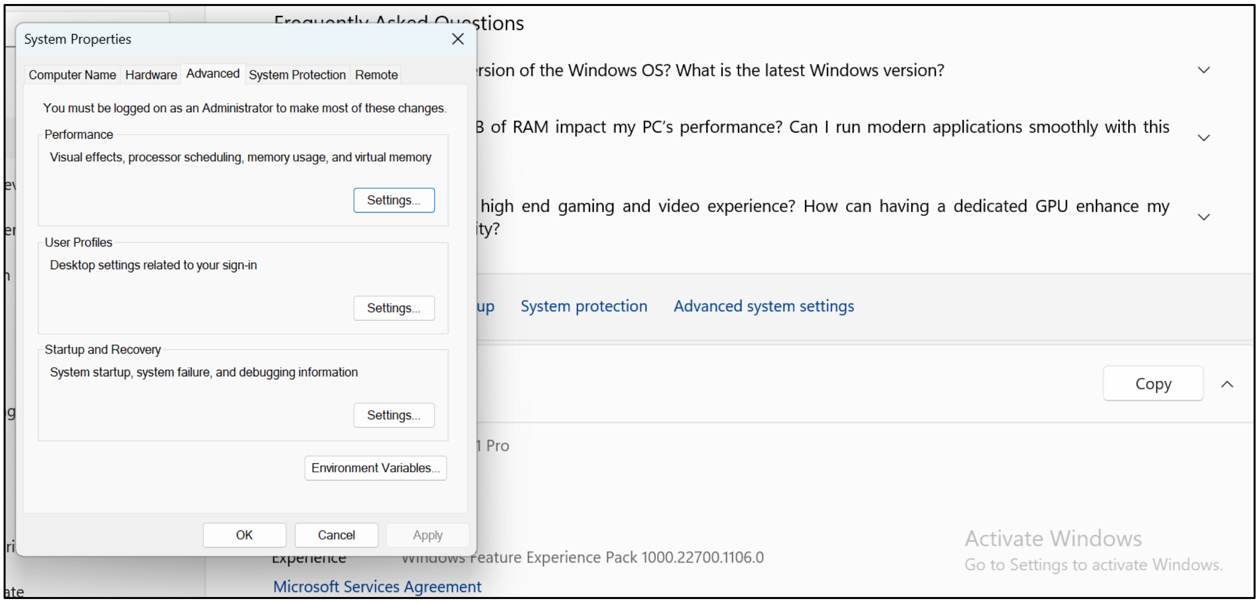


```
C:\Users\Deep Chimani>adb
'adb' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Deep Chimani>
```

When this msg is arrived, it means the ADB is not working, now we have to open the computer properties and go in the enviroment variables.

Then go to the **Path** click the **edit**
add the address where ADB setup is exist.





System Properties

You must be logged on as an Administrator to make most of these changes.

Performance

Visual effects, processor scheduling, memory usage, and virtual memory

User Profiles

Desktop settings related to your sign-in

Startup and Recovery

System startup, system failure, and debugging information

Frequently Asked Questions

rsion of the Windows OS? What is the latest Windows version?

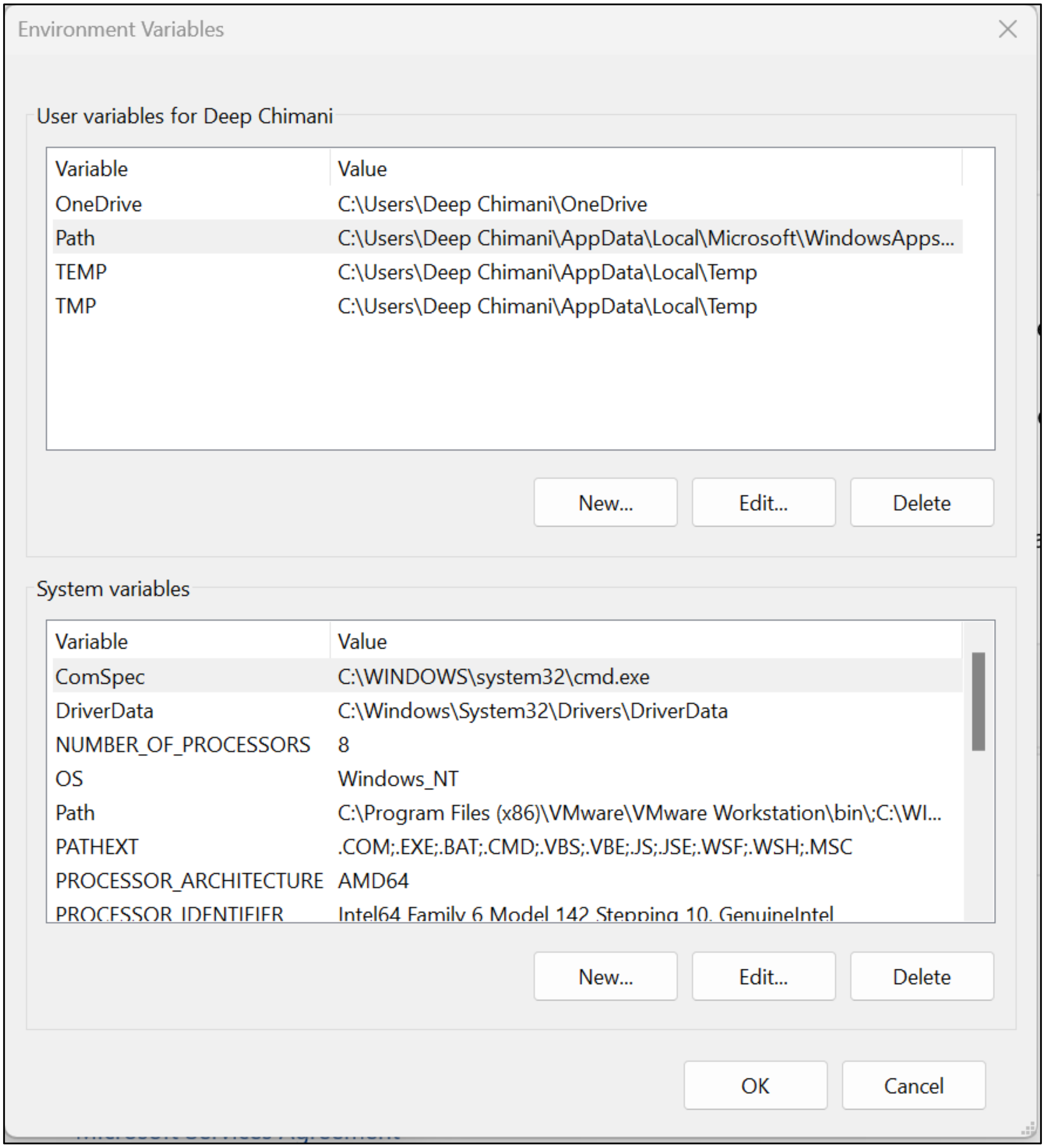
B of RAM impact my PC's performance? Can I run modern applications smoothly with this

high end gaming and video experience? How can having a dedicated GPU enhance my ity?

1 Pro

Experience Windows Feature Experience Pack 1000.22700.1106.0

Activate Windows
Go to Settings to activate Windows.

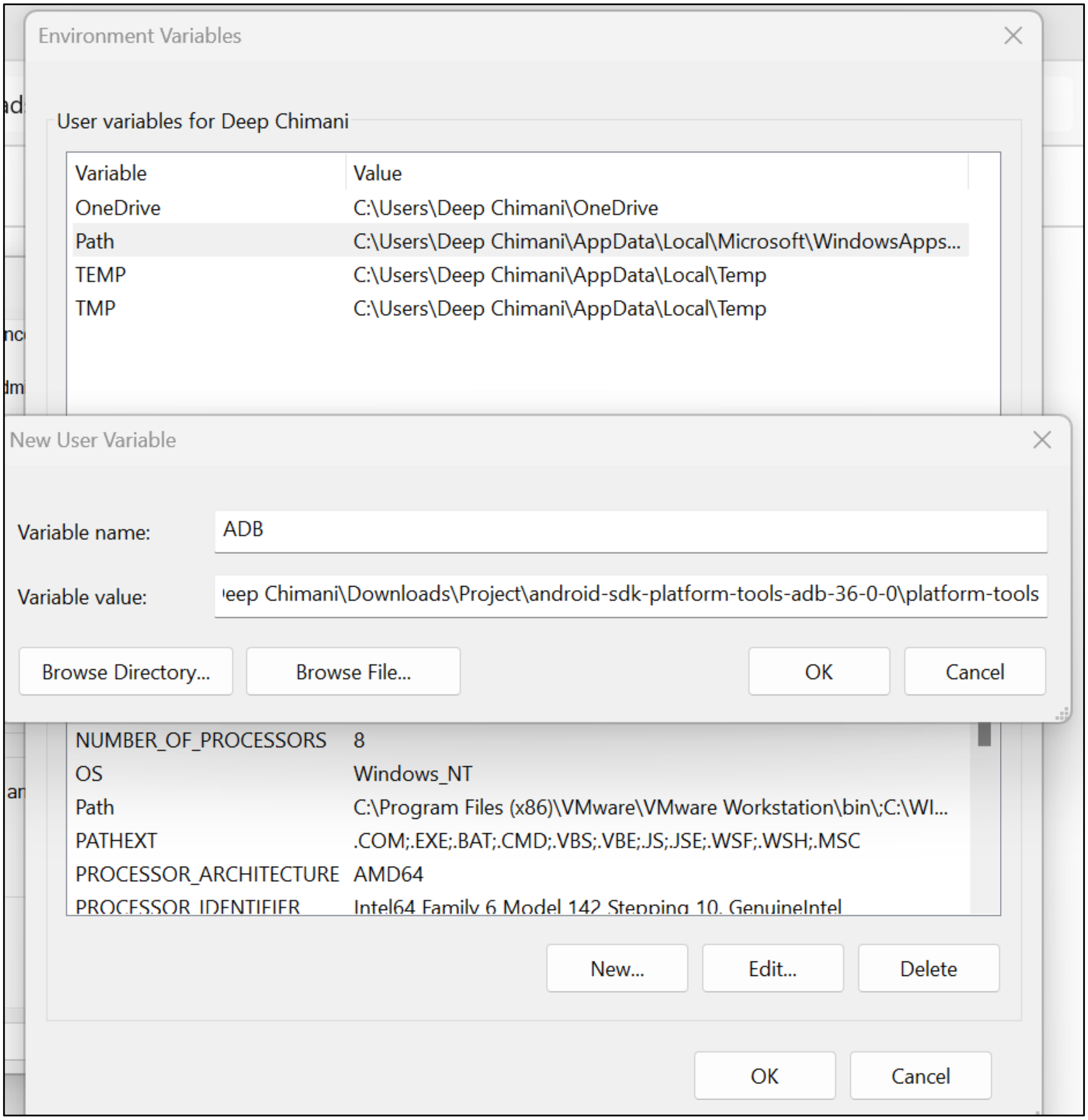


User variables for Deep Chimani

Variable	Value
OneDrive	C:\Users\Deep Chimani\OneDrive
Path	C:\Users\Deep Chimani\AppData\Local\Microsoft\WindowsApps...
TEMP	C:\Users\Deep Chimani\AppData\Local\Temp
TMP	C:\Users\Deep Chimani\AppData\Local\Temp

System variables

Variable	Value
ComSpec	C:\WINDOWS\system32\cmd.exe
DriverData	C:\Windows\System32\Drivers\DriverData
NUMBER_OF_PROCESSORS	8
OS	Windows_NT
Path	C:\Program Files (x86)\VMware\VMware Workstation\bin\;C:\WI...
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE	AMD64
PROCESSOR_IDENTIFIER	Intel64 Family 6 Model 142 Stepping 10, GenuineIntel



User variables for Deep Chimani

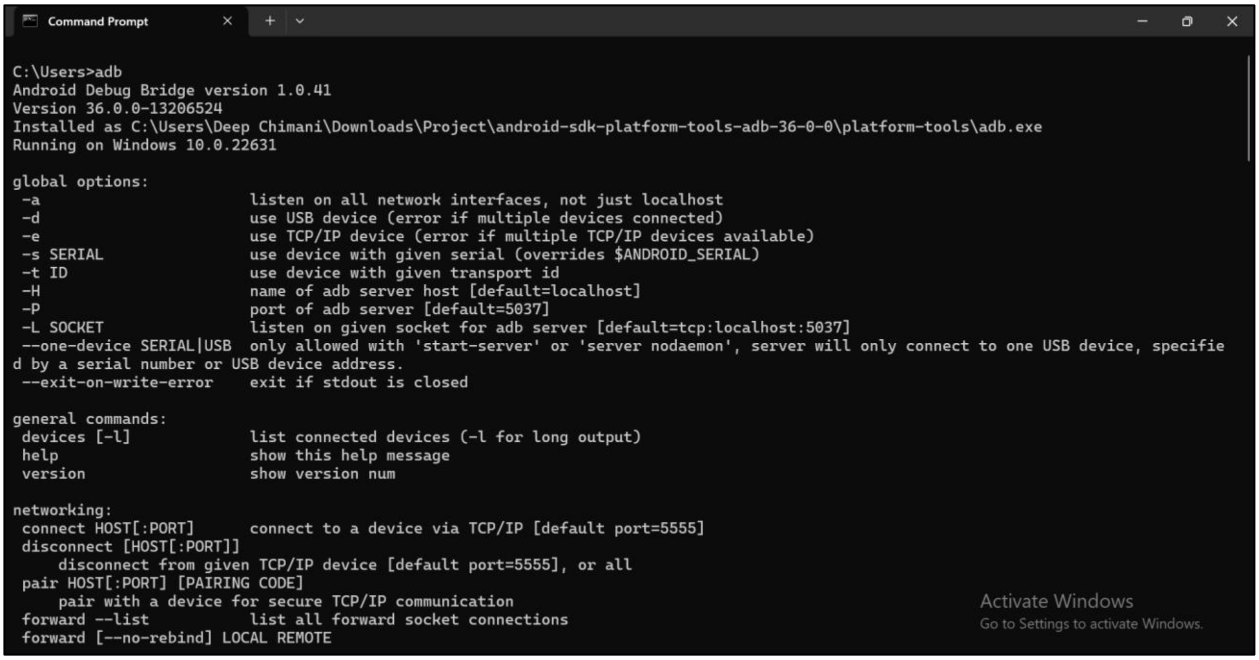
Variable	Value
OneDrive	C:\Users\Deep Chimani\OneDrive
Path	C:\Users\Deep Chimani\AppData\Local\Microsoft\WindowsApps...
TEMP	C:\Users\Deep Chimani\AppData\Local\Temp
TMP	C:\Users\Deep Chimani\AppData\Local\Temp

Variable name: ADB

Variable value: eep Chimani\Downloads\Project\android-sdk-platform-tools-adb-36-0-0\platform-tools

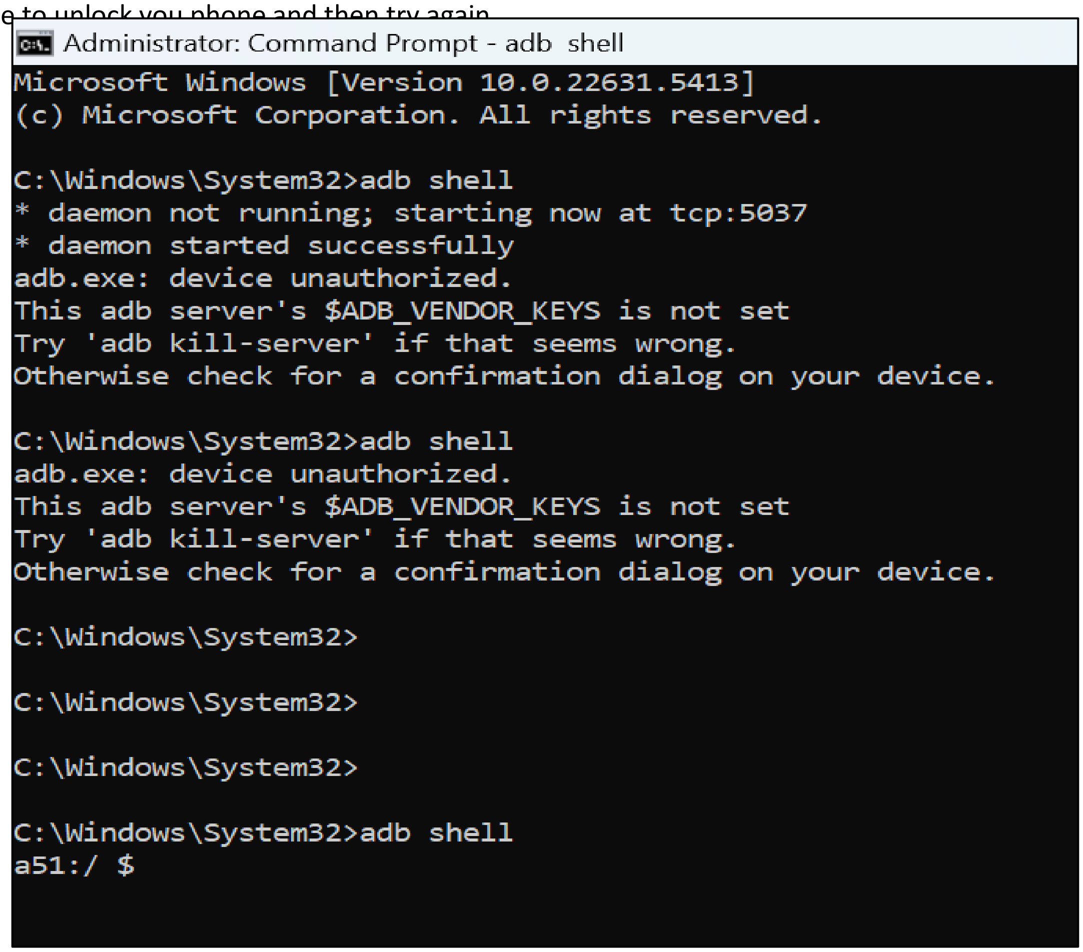
NUMBER_OF_PROCESSORS	8
OS	Windows_NT
Path	C:\Program Files (x86)\VMware\VMware Workstation\bin\;C:\WI...
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE	AMD64
PROCESSOR_IDENTIFIER	Intel64 Family 6 Model 142 Stepping 10, GenuineIntel

- Reopen the CMD with administrator rights after changing the path and type ‘adb’, we will get below sanpped result which shows adb is working with success status.



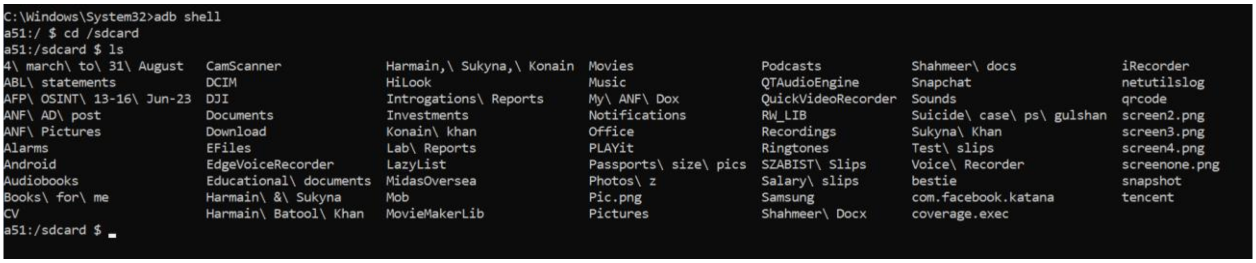
```
C:\Users>adb
Android Debug Bridge version 1.0.41
Version 36.0.0-13206524
Installed as C:\Users\Deep Chimani\Downloads\Project\android-sdk-platform-tools-adb-36-0-0\platform-tools\adb.exe
Running on Windows 10.0.22631

global options:
 -a                       listen on all network interfaces, not just localhost
 -d                       use USB device (error if multiple devices connected)
 -e                       use TCP/IP device (error if multiple TCP/IP devices available)
 -s SERIAL                use device with given serial (overrides $ANDROID_SERIAL)
 -t ID                    use device with given transport id
 -H                       name of adb server host [default=localhost]
 -P                       port of adb server [default=5037]
 -L SOCKET                listen on given socket for adb server [default=tcp:localhost:5037]
 --one-device SERIAL|USB  only allowed with 'start-server' or 'server nodaemon', server will only connect to one USB device, specifie
d by a serial number or USB device address.
 --exit-on-write-error    exit if stdout is closed

general commands:
 devices [-l]             list connected devices (-l for long output)
 help                     show this help message
 version                  show version num

networking:
 connect HOST[:PORT]      connect to a device via TCP/IP [default port=5555]
 disconnect [HOST[:PORT]]
     disconnect from given TCP/IP device [default port=5555], or all
 pair HOST[:PORT] [PAIRING CODE]
     pair with a device for secure TCP/IP communication
 forward --list           list all forward socket connections
 forward [--no-rebind] LOCAL REMOTE
```

When ADB is working good, and we want to access mobile phone and if this error accurs then it means we have to unlock you phone and then try again.



```
Microsoft Windows [Version 10.0.22631.5413]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>adb shell
* daemon not running; starting now at tcp:5037
* daemon started successfully
adb.exe: device unauthorized.
This adb server's $ADB_VENDOR_KEYS is not set
Try 'adb kill-server' if that seems wrong.
Otherwise check for a confirmation dialog on your device.

C:\Windows\System32>adb shell
adb.exe: device unauthorized.
This adb server's $ADB_VENDOR_KEYS is not set
Try 'adb kill-server' if that seems wrong.
Otherwise check for a confirmation dialog on your device.

C:\Windows\System32>

C:\Windows\System32>

C:\Windows\System32>

C:\Windows\System32>adb shell
a51:/ $
```

- Type ADB Shell for access the phone, the go to the your memory for checking your files in mobile.



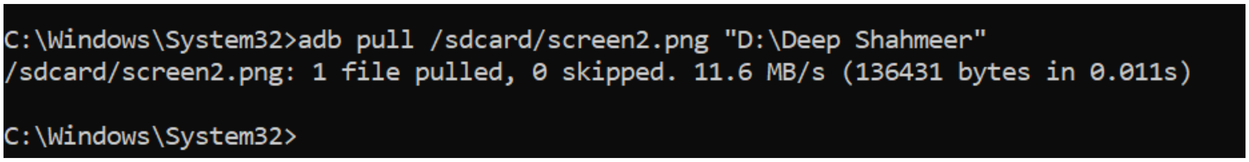
```
C:\Windows\System32>adb shell
a51:/ $ cd /sdcard
a51:/sdcard $ ls
4\ march\ to\ 31\ August   CamScanner              Harmain,\ Sukyna,\ Konain  Movies                 Podcasts            Shahmeer\ docs              iRecorder
ABL\ statements            DCIM                    HiLook                     Music                  QTAudioEngine       Snapchat                    netutilslog
AFP\ OSINT\ 13-16\ Jun-23  DJI                     Introgations\ Reports      My\ ANF\ Dox           QuickVideoRecorder  Sounds                      qrcode
ANF\ AD\ post              Documents               Investments                Notifications          RW_LIB              Suicide\ case\ ps\ gulshan  screen2.png
ANF\ Pictures              Download                Konain\ khan               Office                 Recordings          Sukyna\ Khan                screen3.png
Alarms                     EFiles                  Lab\ Reports               PLAYit                 Ringtones           Test\ slips                 screen4.png
Android                    EdgeVoiceRecorder       LazyList                   Passports\ size\ pics  SZABIST\ Slips      Voice\ Recorder             screenone.png
Audiobooks                 Educational\ documents  MidasOversea               Photos\ z              Salary\ slips       bestie                      snapshot
Books\ for\ me             Harmain\ &\ Sukyna      Mob                        Pic.png                Samsung             com.facebook.katana         tencent
CV                         Harmain\ Batool\ Khan   MovieMakerLib              Pictures               Shahmeer\ Docx      coverage.exec
a51:/sdcard $ _
```

In this list of the mobile there is PNG file with name “screen2.png”.

- Type pull command to move the data from Mobile Phone to PC.

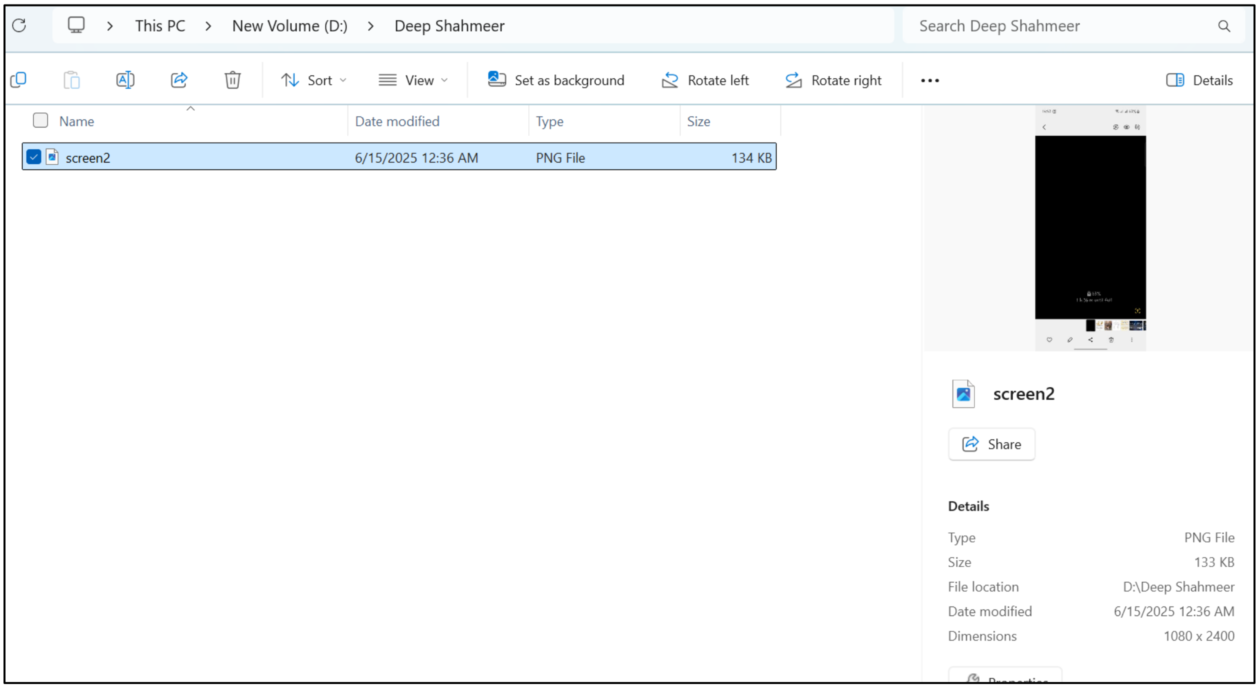
And adb pull command is for the copy that data from mobile to PC (given address of PC)

Below snapped is the folder where we given the address to copy the data.



```
C:\Windows\System32>adb pull /sdcard/screen2.png "D:\Deep Shahmeer"
/sdcard/screen2.png: 1 file pulled, 0 skipped. 11.6 MB/s (136431 bytes in 0.011s)

C:\Windows\System32>
```

- You saw the file which we copied from mobile.



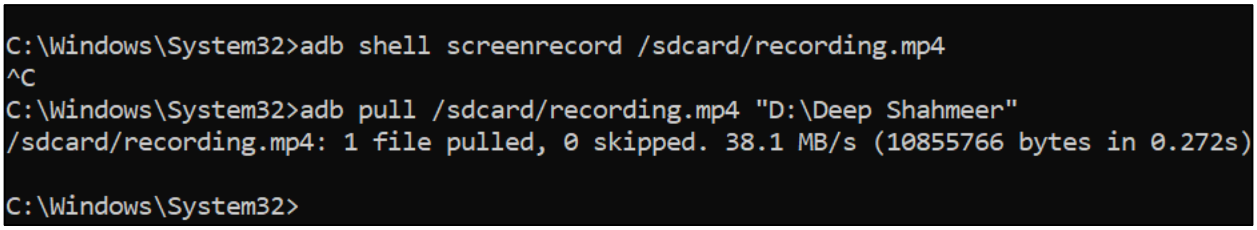
Name	Date modified	Type	Size
☑ screen2	6/15/2025 12:36 AM	PNG File	134 KB

screen2

Details

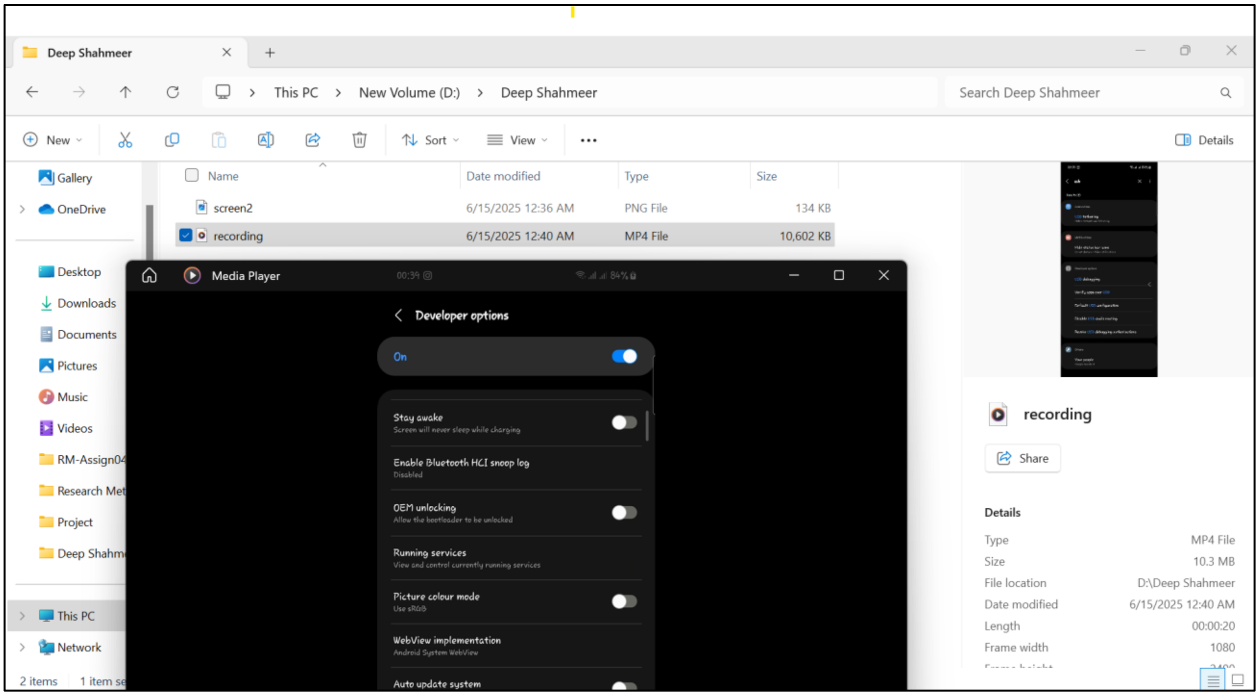
Type	PNG File
Size	133 KB
File location	D:\Deep Shahmeer
Date modified	6/15/2025 12:36 AM
Dimensions	1080 x 2400

This command for record mobile phone screen that and copy data file to the PC.



```
C:\Windows\System32>adb shell screenrecord /sdcard/recording.mp4
^C
C:\Windows\System32>adb pull /sdcard/recording.mp4 "D:\Deep Shahmeer"
/sdcard/recording.mp4: 1 file pulled, 0 skipped. 38.1 MB/s (10855766 bytes in 0.272s)

C:\Windows\System32>
```

This is the MP4 file which screen recorded.



Name	Date modified	Type	Size
screen2	6/15/2025 12:36 AM	PNG File	134 KB
☑ recording	6/15/2025 12:40 AM	MP4 File	10,602 KB

Developer options

On

Stay awake
Screen will never sleep while charging

Enable Bluetooth HCI snoop log
Disabled

OEM unlocking
Allow the bootloader to be unlocked

Running services
View and control currently running services

Picture colour mode
Use sRGB

WebView implementation
Android System WebView

Auto update system

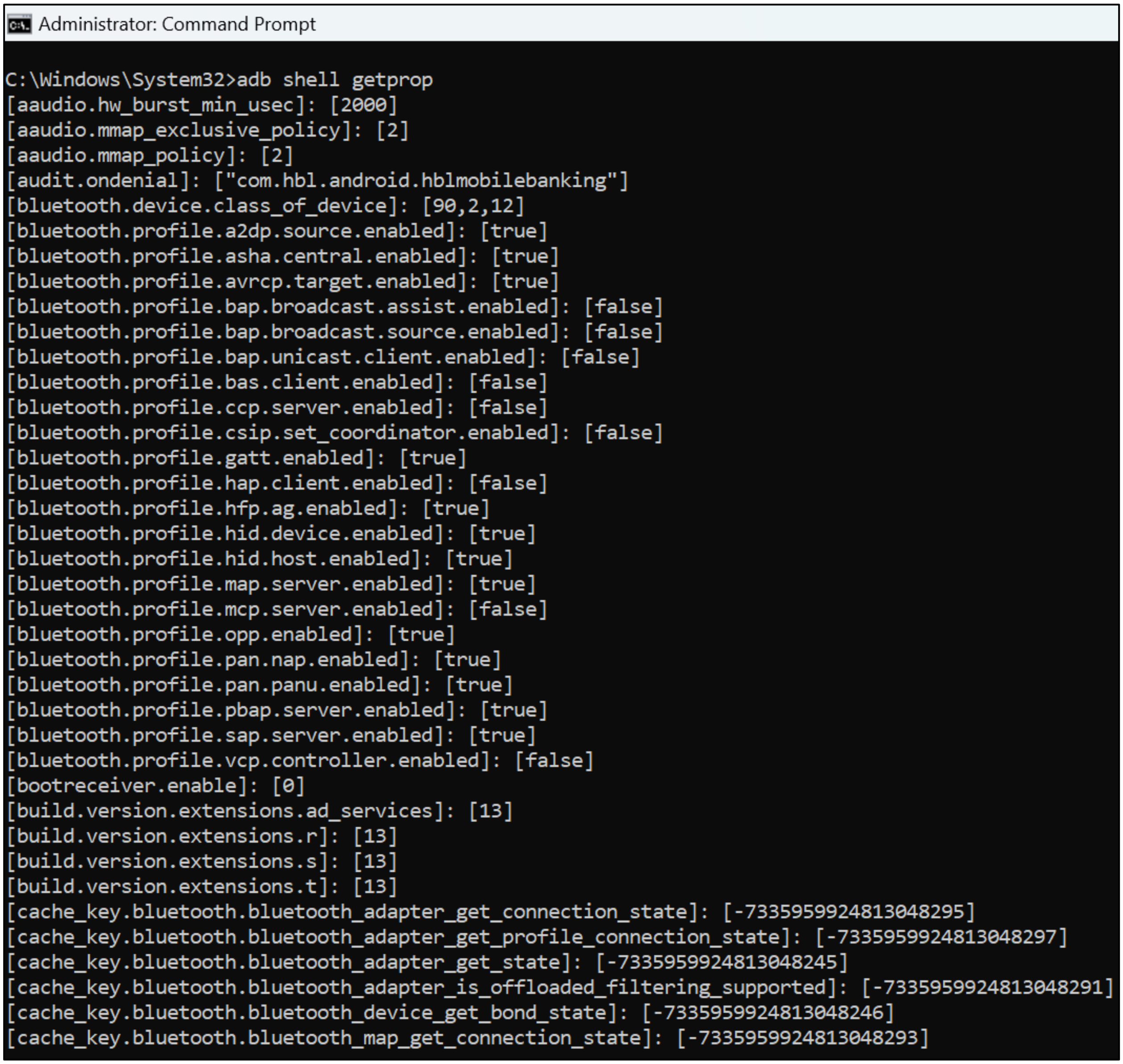
recording

Share

Details

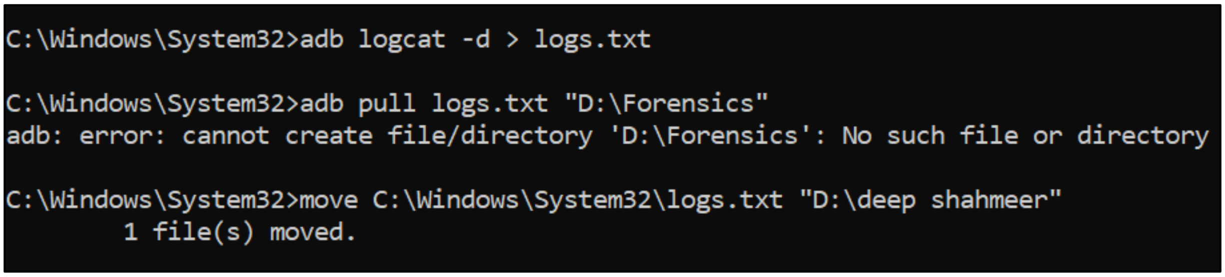
Type	MP4 File
Size	10.3 MB
File location	D:\Deep Shahmeer
Date modified	6/15/2025 12:40 AM
Length	00:00:20
Frame width	1080

Here we are geting the details about the mobile (System Details).



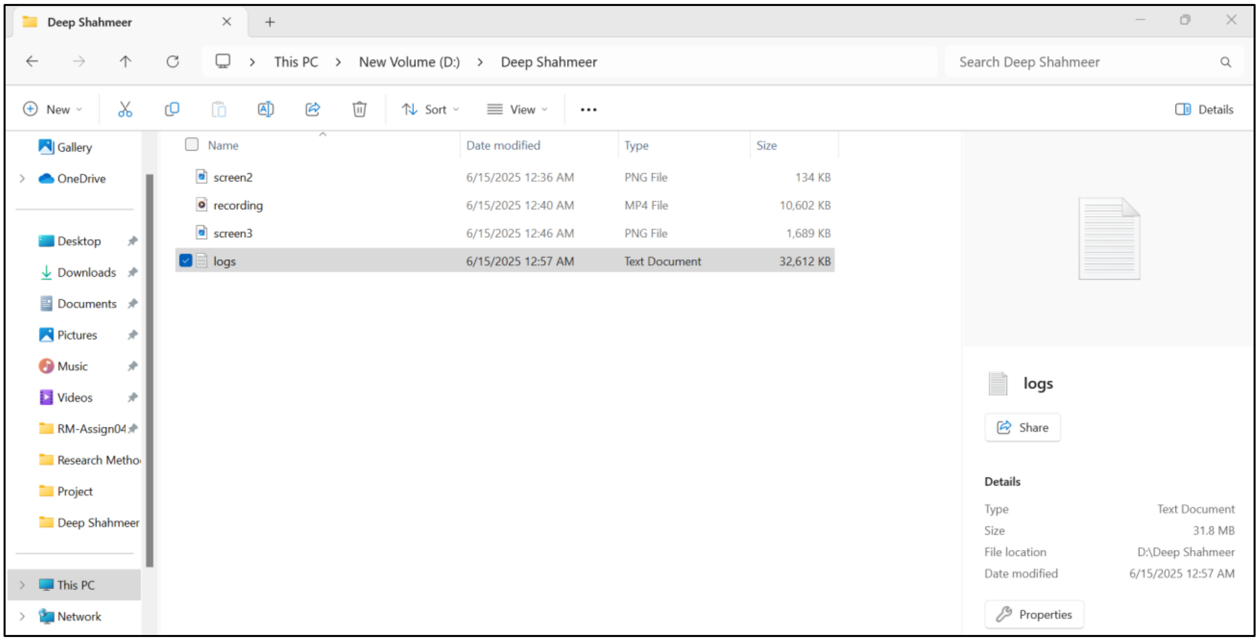
```
C:\Windows\System32>adb shell getprop
[aaudio.hw_burst_min_usec]: [2000]
[aaudio.mmap_exclusive_policy]: [2]
[aaudio.mmap_policy]: [2]
[audit.ondenial]: ["com.hbl.android.hblmobilebanking"]
[bluetooth.device.class_of_device]: [90,2,12]
[bluetooth.profile.a2dp.source.enabled]: [true]
[bluetooth.profile.asha.central.enabled]: [true]
[bluetooth.profile.avrcp.target.enabled]: [true]
[bluetooth.profile.bap.broadcast.assist.enabled]: [false]
[bluetooth.profile.bap.broadcast.source.enabled]: [false]
[bluetooth.profile.bap.unicast.client.enabled]: [false]
[bluetooth.profile.bas.client.enabled]: [false]
[bluetooth.profile.ccp.server.enabled]: [false]
[bluetooth.profile.csip.set_coordinator.enabled]: [false]
[bluetooth.profile.gatt.enabled]: [true]
[bluetooth.profile.hap.client.enabled]: [false]
[bluetooth.profile.hfp.ag.enabled]: [true]
[bluetooth.profile.hid.device.enabled]: [true]
[bluetooth.profile.hid.host.enabled]: [true]
[bluetooth.profile.map.server.enabled]: [true]
[bluetooth.profile.mcp.server.enabled]: [false]
[bluetooth.profile.opp.enabled]: [true]
[bluetooth.profile.pan.nap.enabled]: [true]
[bluetooth.profile.pan.panu.enabled]: [true]
[bluetooth.profile.pbap.server.enabled]: [true]
[bluetooth.profile.sap.server.enabled]: [true]
[bluetooth.profile.vcp.controller.enabled]: [false]
[bootreceiver.enable]: [0]
[build.version.extensions.ad_services]: [13]
[build.version.extensions.r]: [13]
[build.version.extensions.s]: [13]
[build.version.extensions.t]: [13]
[cache_key.bluetooth.bluetooth_adapter_get_connection_state]: [-7335959924813048295]
[cache_key.bluetooth.bluetooth_adapter_get_profile_connection_state]: [-7335959924813048297]
[cache_key.bluetooth.bluetooth_adapter_get_state]: [-7335959924813048245]
[cache_key.bluetooth.bluetooth_adapter_is_offloaded_filtering_supported]: [-7335959924813048291]
[cache_key.bluetooth.bluetooth_device_get_bond_state]: [-7335959924813048246]
[cache_key.bluetooth.bluetooth_map_get_connection_state]: [-7335959924813048293]
```

From this command we grap the log file of the mobile that tells about each and every change in mobile



```
C:\Windows\System32>adb logcat -d > logs.txt

C:\Windows\System32>adb pull logs.txt "D:\Forensics"
adb: error: cannot create file/directory 'D:\Forensics': No such file or directory

C:\Windows\System32>move C:\Windows\System32\logs.txt "D:\deep shahmeer"
        1 file(s) moved.
```

This is the file in PC



Name	Date modified	Type	Size
screen2	6/15/2025 12:36 AM	PNG File	134 KB
recording	6/15/2025 12:40 AM	MP4 File	10,602 KB
screen3	6/15/2025 12:46 AM	PNG File	1,689 KB
☑ logs	6/15/2025 12:57 AM	Text Document	32,612 KB

logs

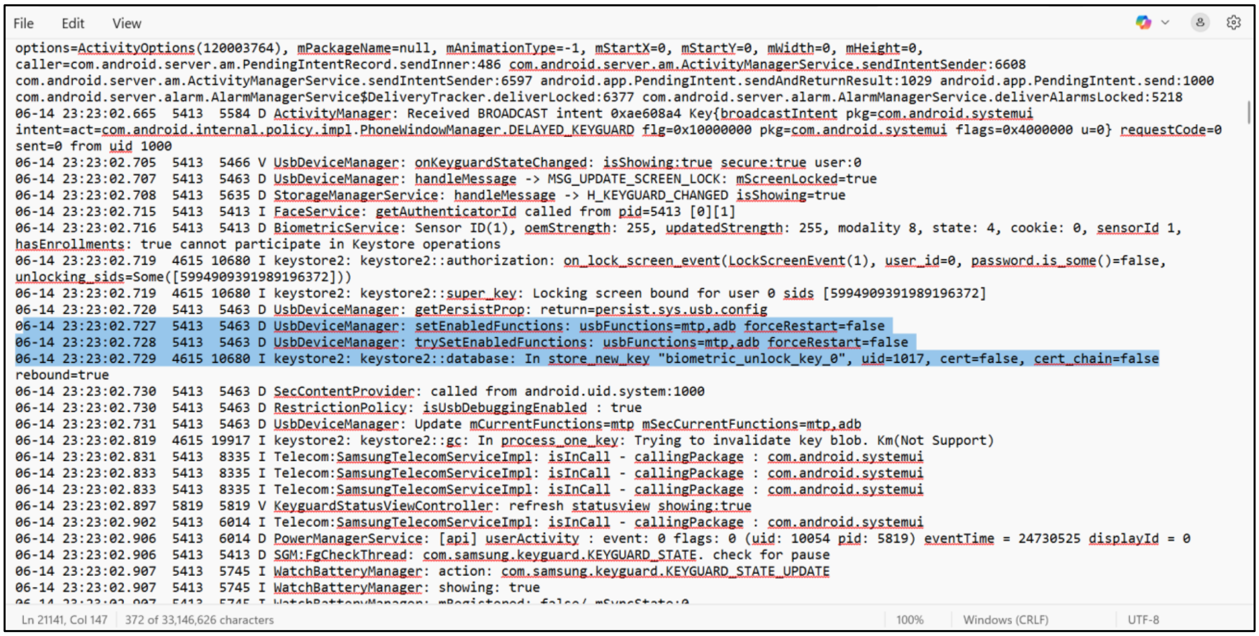
Share

Details

Type	Text Document
Size	31.8 MB
File location	D:\Deep Shahmeer
Date modified	6/15/2025 12:57 AM

Properties

Here is the file, where i search for the ADB in logs file of mobile



```
options=ActivityOptions(120003764), mPackageName=null, mAnimationType=-1, mStartX=0, mStartY=0, mWidth=0, mHeight=0,
caller=com.android.server.am.PendingIntentRecord.sendInner:486 com.android.server.am.ActivityManagerService.sendIntentSender:6608
com.android.server.am.ActivityManagerService.sendIntentSender:6597 android.app.PendingIntent.sendAndReturnResult:1029 android.app.PendingIntent.send:1000
com.android.server.alarm.AlarmManagerService$DeliveryTracker.deliverLocked:6377 com.android.server.alarm.AlarmManagerService.deliverAlarmsLocked:5218
06-14 23:23:02.665  5413  5584 D ActivityManager: Received BROADCAST intent 0xae608a4 Key{broadcastIntent pkg=com.android.systemui
intent=act=com.android.internal.policy.impl.PhoneWindowManager.DELAYED_KEYGUARD flg=0x10000000 pkg=com.android.systemui flags=0x4000000 u=0} requestCode=0
sent=0 from uid 1000
06-14 23:23:02.705  5413  5466 V UsbDeviceManager: onKeyguardStateChanged: isShowing:true secure:true user:0
06-14 23:23:02.707  5413  5463 D UsbDeviceManager: handleMessage -> MSG_UPDATE_SCREEN_LOCK: mScreenLocked=true
06-14 23:23:02.708  5413  5635 D StorageManagerService: handleMessage -> H_KEYGUARD_CHANGED isShowing=true
06-14 23:23:02.715  5413  5413 I FaceService: getAuthenticatorId called from pid=5413 [0][1]
06-14 23:23:02.716  5413  5413 D BiometricService: Sensor ID(1), oemStrength: 255, updatedStrength: 255, modality 8, state: 4, cookie: 0, sensorId 1,
hasEnrollments: true cannot participate in Keystore operations
06-14 23:23:02.719  4615 10680 I keystore2: keystore2::authorization: on_lock_screen_event(LockScreenEvent(1), user_id=0, password.is_some()=false,
unlocking_sids=Some([5994909391989196372]))
06-14 23:23:02.719  4615 10680 I keystore2: keystore2::super_key: Locking screen bound for user 0 sids [5994909391989196372]
06-14 23:23:02.720  5413  5463 D UsbDeviceManager: getPersistProp: return=persist.sys.usb.config
06-14 23:23:02.727  5413  5463 D UsbDeviceManager: setEnabledFunctions: usbFunctions=mtp,adb forceRestart=false
06-14 23:23:02.728  5413  5463 D UsbDeviceManager: trySetEnabledFunctions: usbFunctions=mtp,adb forceRestart=false
06-14 23:23:02.729  4615 10680 I keystore2: keystore2::database: In store_new_key "biometric_unlock_key_0", uid=1017, cert=false, cert_chain=false
rebound=true
06-14 23:23:02.730  5413  5463 D SecContentProvider: called from android.uid.system:1000
06-14 23:23:02.730  5413  5463 D RestrictionPolicy: isUsbDebuggingEnabled : true
06-14 23:23:02.731  5413  5463 D UsbDeviceManager: Update mCurrentFunctions=mtp mSecCurrentFunctions=mtp,adb
06-14 23:23:02.819  4615 19917 I keystore2: keystore2::gc: In process_one_key: Trying to invalidate key blob. Km(Not Support)
06-14 23:23:02.831  5413  8335 I Telecom:SamsungTelecomServiceImpl: isInCall - callingPackage : com.android.systemui
06-14 23:23:02.833  5413  8335 I Telecom:SamsungTelecomServiceImpl: isInCall - callingPackage : com.android.systemui
06-14 23:23:02.833  5413  8335 I Telecom:SamsungTelecomServiceImpl: isInCall - callingPackage : com.android.systemui
06-14 23:23:02.897  5819  5819 V KeyguardStatusViewController: refresh statusview showing:true
06-14 23:23:02.902  5413  6014 I Telecom:SamsungTelecomServiceImpl: isInCall - callingPackage : com.android.systemui
06-14 23:23:02.906  5413  6014 D PowerManagerService: [api] userActivity : event: 0 flags: 0 (uid: 10054 pid: 5819) eventTime = 24730525 displayId = 0
06-14 23:23:02.906  5413  5413 D SGM:FgCheckThread: com.samsung.keyguard.KEYGUARD_STATE. check for pause
06-14 23:23:02.907  5413  5745 I WatchBatteryManager: action: com.samsung.keyguard.KEYGUARD_STATE_UPDATE
06-14 23:23:02.907  5413  5745 I WatchBatteryManager: showing: true
06-14 23:23:02.907  5413  5745 I WatchBatteryManager: mRegistered: false/ mSyncState:0
```

Thank you