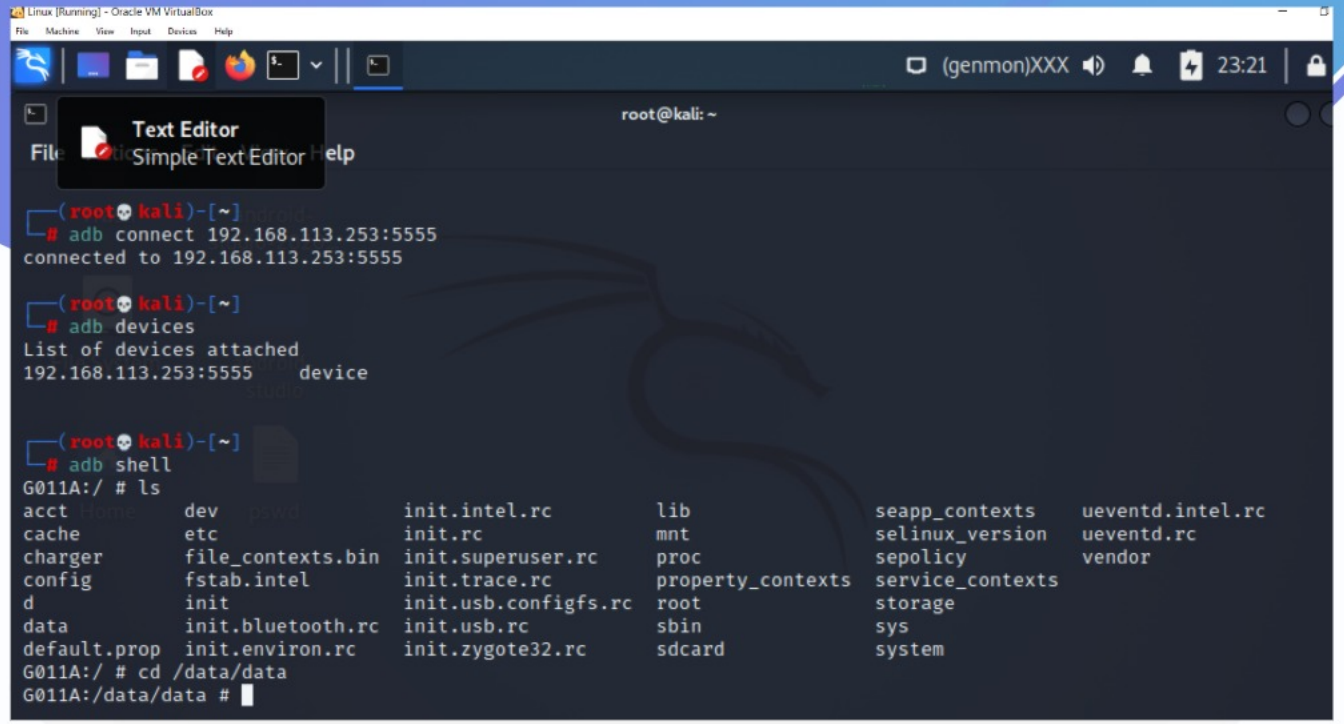
Android Forensics - Recovering Deleted Data

Recovering Deleted Data

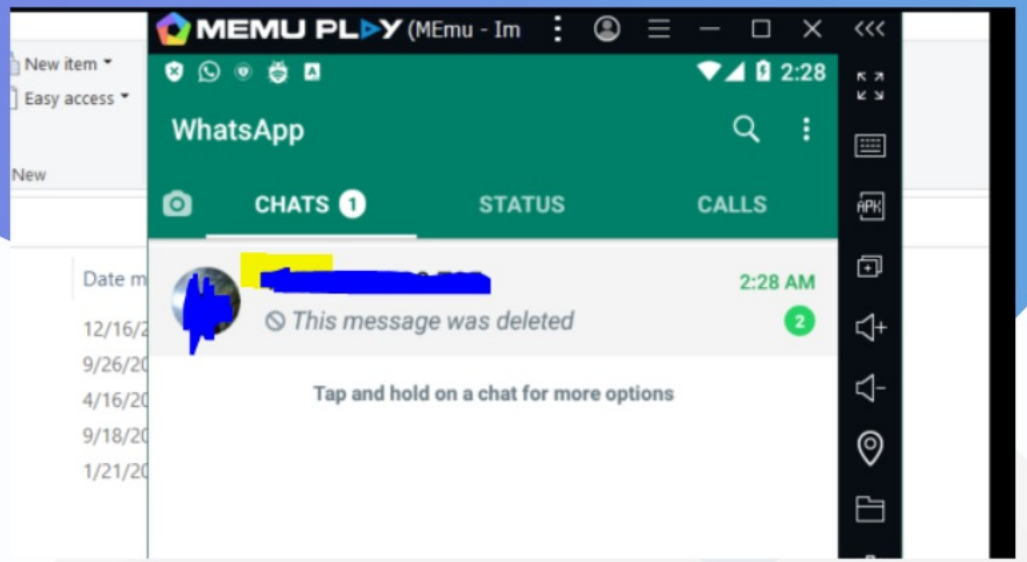
- Go to ADB Shell and then list the packages. Check for which package you want to recover deleted datas.
- When dealing with Android application data analysis, it is important to note that all the data associated with the user installed apps will be stored in /data/data/.

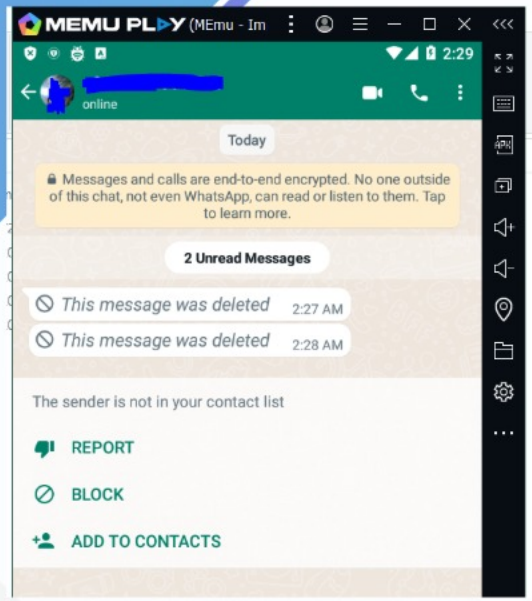
Example: Android browser is named com.android.browser, data files are stored at /data/data/com.android.browser

- As an example, I am using whatsapp Messages.
- Going under com.whatsapp under /data/data/com.whatsapp. It has many database, Now I am going to recover the deleted messages, messages will be stored under msgstore.db-wal (I am using this folder today to retrieve (unread deleted messages))
- You can use adb pull as shown in the below screenshot and you cannot read those messages. as it will be in non-human readable format. We can use the hex tools(I am using Hexer tool to check the messages which got deleted)




```
G011A:/data/data # pm list packages -f
package:/data/app/stericson.busybox-1/base.apk=stericson.busybox
package:/system/priv-app/GoogleExtServices/GoogleExtServices.apk=com.google.android.ext.services
package:/system/priv-app/TelephonyProvider/TelephonyProvider.apk=com.android.providers.telephony
package:/system/priv-app/CalendarProvider/CalendarProvider.apk=com.android.providers.calendar
package:/system/priv-app/MediaProvider/MediaProvider.apk=com.android.providers.media
package:/system/priv-app/GoogleOneTimeInitializer/GoogleOneTimeInitializer.apk=com.google.android.onetimeinitiali
r
package:/system/app/GoogleExtShared/GoogleExtShared.apk=com.google.android.ext.shared
package:/system/priv-app/WallpaperCropper/WallpaperCropper.apk=com.android.wallpapercropper
package:/data/app/com.diwa.xmodul-1/base.apk=com.diwa.xmodul
package:/system/priv-app/DocumentsUI/DocumentsUI.apk=com.android.documentsui
package:/system/priv-app/ExternalStorageProvider/ExternalStorageProvider.apk=com.android.externalstorage
package:/system/app/HTMLViewer/HTMLViewer.apk=com.android.htmlviewer
```






```
G011A:/data/data/com.whatsapp/databases # ls -l
total 3768
-rw-rw---- 1 u0_a68 u0_a68   16384 2022-01-22 02:27 _jobqueue-WhatsAppJobManager
-rw------- 1 u0_a68 u0_a68    8720 2022-01-22 02:27 _jobqueue-WhatsAppJobManager-journa
-rw-rw---- 1 u0_a68 u0_a68  262144 2022-01-22 02:27 axolotl.db
-rw------- 1 u0_a68 u0_a68   32768 2022-01-22 02:28 axolotl.db-shm
-rw------- 1 u0_a68 u0_a68  432632 2022-01-22 02:28 axolotl.db-wal
-rw-rw---- 1 u0_a68 u0_a68    4096 2022-01-22 02:27 chatsettings.db
-rw------- 1 u0_a68 u0_a68   32768 2022-01-22 02:29 chatsettings.db-shm
-rw------- 1 u0_a68 u0_a68   70072 2022-01-22 02:29 chatsettings.db-wal
-rw-rw---- 1 u0_a68 u0_a68    4096 2022-01-22 02:27 companion_devices.db
-rw------- 1 u0_a68 u0_a68   32768 2022-01-22 02:27 companion_devices.db-shm
-rw------- 1 u0_a68 u0_a68   37112 2022-01-22 02:27 companion_devices.db-wal
-rw-rw---- 1 u0_a68 u0_a68    4096 2022-01-22 02:28 location.db
-rw------- 1 u0_a68 u0_a68   32768 2022-01-22 02:28 location.db-shm
-rw------- 1 u0_a68 u0_a68   53592 2022-01-22 02:28 location.db-wal
-rw------- 1 u0_a68 u0_a68 1028096 2022-01-22 02:28 msgstore.db
-rw------- 1 u0_a68 u0_a68   32768 2022-01-22 02:29 msgstore.db-shm
-rw------- 1 u0_a68 u0_a68  524288 2022-01-22 02:29 msgstore.db-wal
-rw-rw---- 1 u0_a68 u0_a68    4096 2022-01-22 02:27 payments.db
-rw------- 1 u0_a68 u0_a68   32768 2022-01-22 02:28 payments.db-shm
```

```
┌──(root💀kali)-[~]
└─# adb pull /data/data/com.whatsapp/databases/msgstore.db-wal .
/data/data/com.whatsapp/databases/msgstore.db-wal: 1 file pulled. 26.6 MB/s (524288 bytes in 0.019s)
```

```
┌──(root💀kali)-[~]
└─# hexer msgstore.db-wal
```

```
00011d90:  36 35 44 34 41 32 30 41  38 37 35 44 36 33 35 32  65D4A20A875D6352
00011da0:  37 43 45 32 32 45 37 35  43 45 43 33 36 43 45 54  7CE22E75CEC36CET
00011db0:  65 73 74 69 6e 67 20 77  68 65 74 68 65 72 20 49  esting whether I
00011dc0:  20 63 61 6e 20 73 65 65  20 74 68 69 73 20 6d 65   can see this me
00011dd0:  73 73 61 67 65 20 6f 72  20 6e 6f 74 3f 01 7e 7d  ssage or not?.~}
00011de0:  e4 7f d0 30 01 7e 7d e4  82 76 ff ff ff 79 08 2c  ...0.~}..v...y.,
00011df0:  00 43 08 4d 08 08 11 05  00 00 0f 08 00 00 00 08  .C.M............
00011e00:  08 08 08 00 00 05 01 01  01 00 00 00 08 00 00 08  ................
```

> I have used Hexer tool to recover deleted data by using the phone no. and we were able to find the deleted message now.