

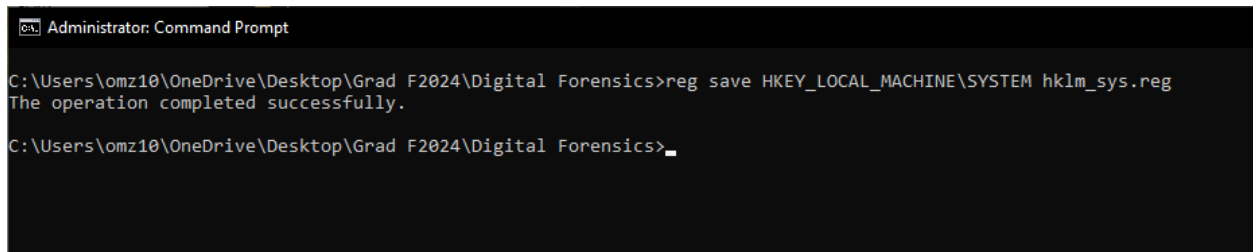
Windows Parsing Video Assignment

Hive: HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices

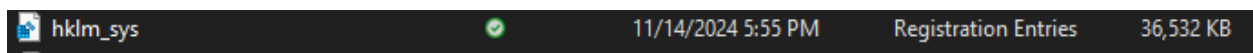
Tools: CMD (using reg save command), RegRipper

This hive contains important information on external drives that have been connected to the computer, including valuable timestamps that can reveal when each device was last mounted.

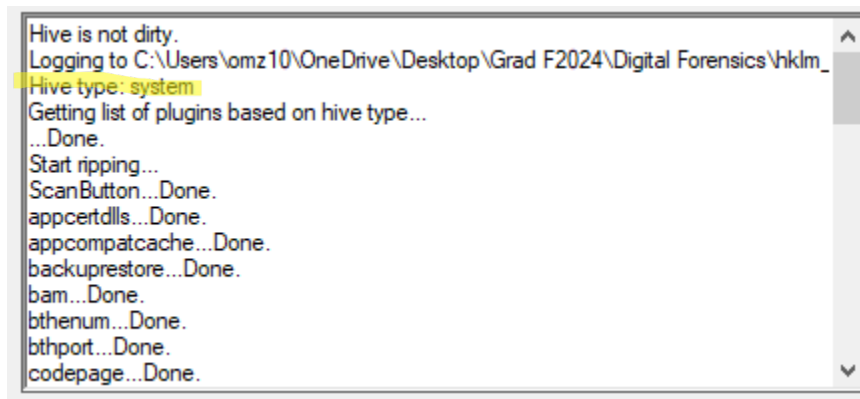
1. Using command prompt to export the registry to our desired folder using the “reg save” command to be parsed later.

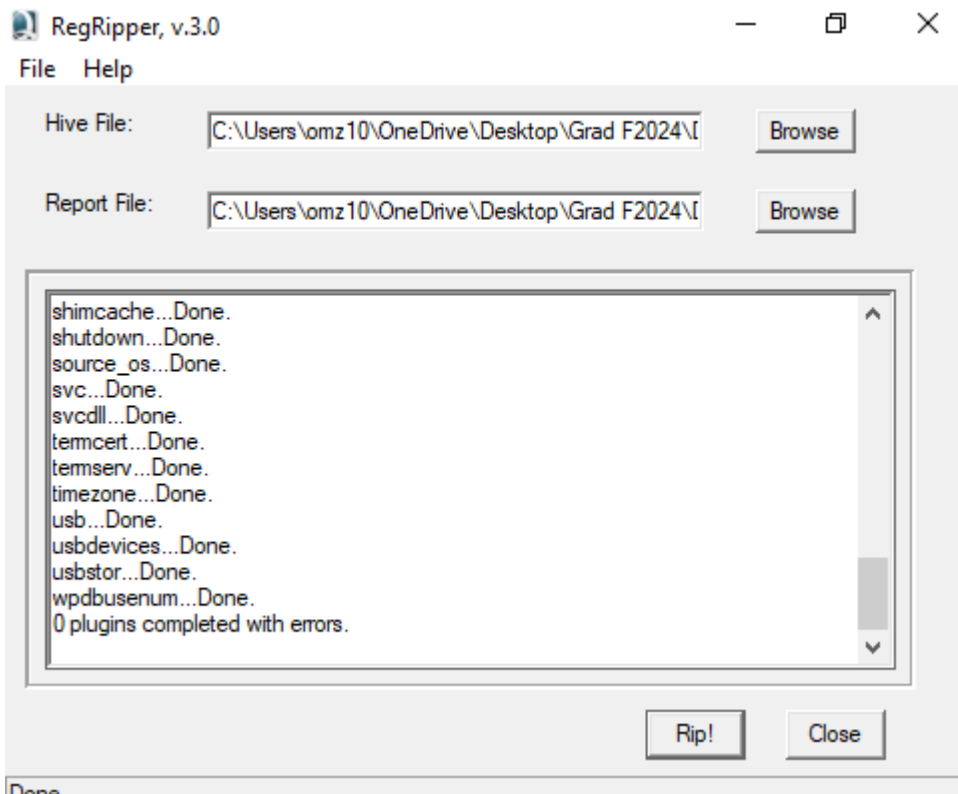


```
Administrator: Command Prompt
C:\Users\omz10\OneDrive\Desktop\Grad F2024\Digital Forensics>reg save HKEY_LOCAL_MACHINE\SYSTEM hklm_sys.reg
The operation completed successfully.
C:\Users\omz10\OneDrive\Desktop\Grad F2024\Digital Forensics>
```



2. Now that we have exported the HKLM\system registry, now time to parse it using RegRipper and search/ analyze the MountedDevices key. Here we upload our Hive file and the file where our report will be extracted to. It also specifies the hive type before it starts parsing.





- Here we analyze the txt file with all the keys in the HKLM_sys. Using the Find command, we search for the mounted devices section to locate the values.

