Forensic Investigation: Windows Registry Analysis

August 7, 2020 By Raj Chandel

In this article, we will learn how we can use RegRipper to analyze the windows registry in the forensic investigation environment.

Table of Content

Let’s begin the Forensic Investigation!!

Introduction to Regripper

RegRipper is an open-source tool, written in Perl. To extracting and parsing information like [keys, values, data] from the Registry and presenting it for analysis.

Its GUI version allows the analyst to select a hive to parse, an output file for the results. It also includes a command-line (CLI) tool called rip.

Rip can be pointed against a hive and can run either a profile (a list of plugins) or an individual plugin against that hive, with the results being sent to STDOUT.

Plugins are extremely valuable in the sense that they can be written to parse data in a manner that is useful to individual analysts.

To learn more about RegRipper click **here**.

We can download RegRipper for windows from **here**.

Creating a Registry Hives

A hive is a logical group of keys, subkeys, and values in the registry that has a set of supporting files loaded into memory when the OS is started or user login.

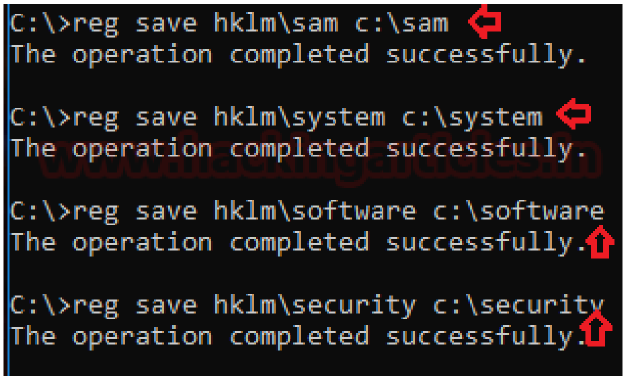
Each time a new user logs on a computer, a new hive file is created for that user with a separate file for the user profile hive.

A user's hive contains specific registry information about user's application settings, desktop, environment, network connections, and printers. User profile hives are located under the **HKEY_USERS key**.

We can learn more about **Registry Hives** from here.

Use these commands to save a copy of these Registry Hives [**SAM, System, Software, and Security**].

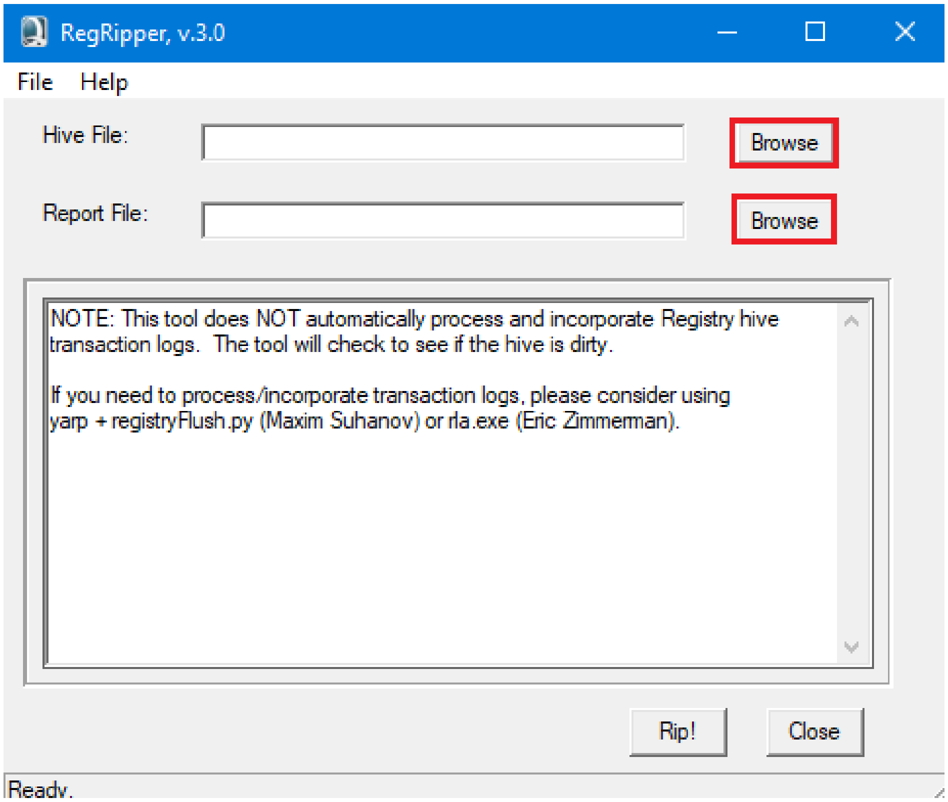
```
reg save hklm\sam c:\sam
reg save hklm\system c:\system
reg save hklm\software c:\software
reg save hklm\security c:\security
```



```
C:\>reg save hklm\sam c:\sam
The operation completed successfully.

C:\>reg save hklm\system c:\system
The operation completed successfully.

C:\>reg save hklm\software c:\software
The operation completed successfully.

C:\>reg save hklm\security c:\security
The operation completed successfully.
```

After saving all these Hive files, we can launch the RegRipper software.

In the **Hive file** tab, we need to select the location where we saved our Registry hive file. In the **Report file** tab, select that location where we want our report and log file both saved. Then click on a rip button to get the report and log file.



NOTE: This tool does NOT automatically process and incorporate Registry hive transaction logs. The tool will check to see if the hive is dirty.

If you need to process/incorporate transaction logs, please consider using yarp + registryFlush.py (Maxim Suhanov) or rla.exe (Eric Zimmerman).

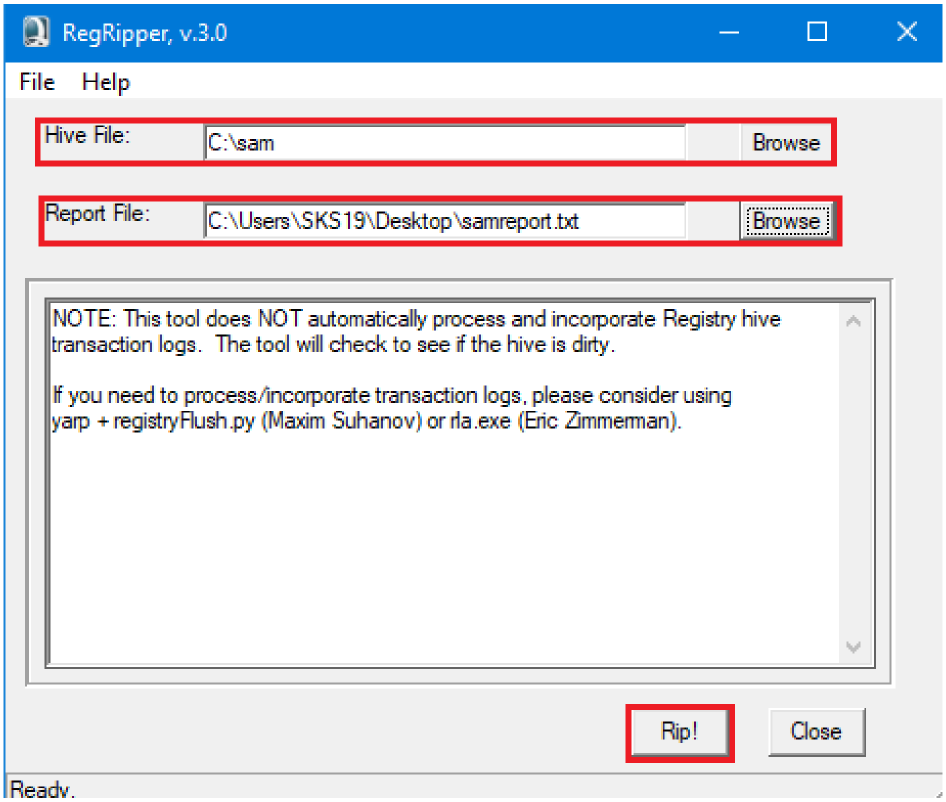
Now let us learn about all this file information.

SAM Hive

SAM stands for the **S**ecurity **A**ccount **M**anager is a database file in windows that **stores user's information**. The user passwords are stored in a hashed format in a Registry hive either as an LM hash or as an NTLM hash. This file can be found in "%SystemRoot%/system32/config/SAM" and is mounted on HKLM/SAM.

In an attempt to improve the security of the SAM database against offline software cracking, Microsoft introduced the SYSKEY function in Windows NT 4.0. When SYSKEY is enabled, the on-disk copy of the SAM file is partially encrypted, so that the password hash values for all local accounts stored in the SAM are encrypted with a key.

Now, open RegRipper and select the location of the **Hive file** and **Report file**. Then click on the **Rip**! Button to start the Investigation process.



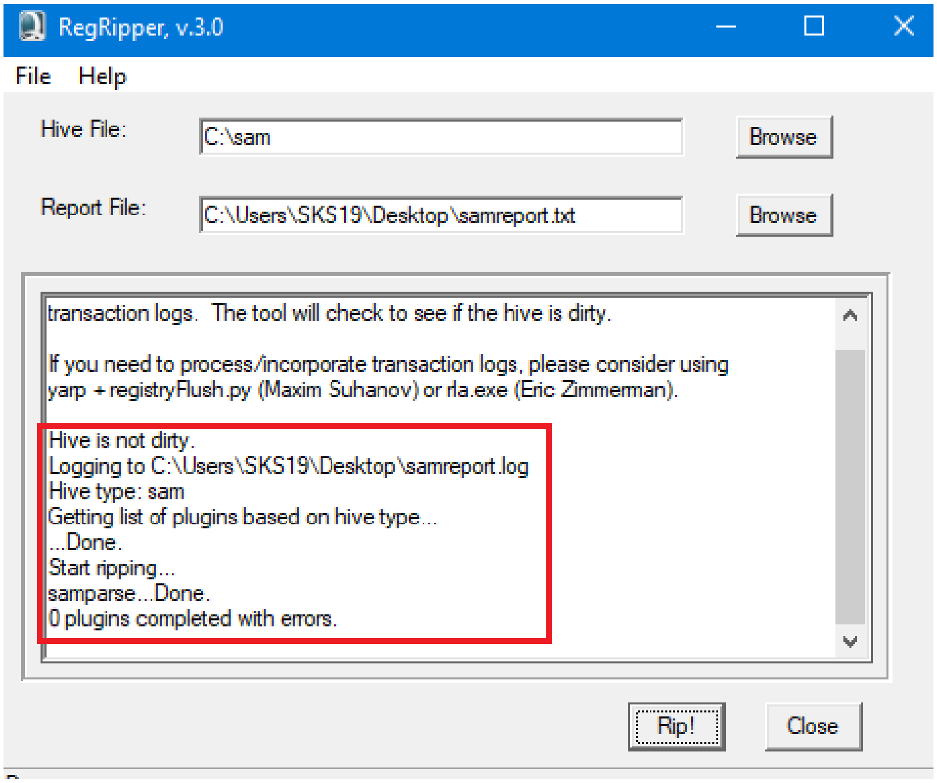
Hive File: C:\sam

Report File: C:\Users\SKS19\Desktop\samreport.txt

```
NOTE: This tool does NOT automatically process and incorporate Registry hive
transaction logs.  The tool will check to see if the hive is dirty.

If you need to process/incorporate transaction logs, please consider using
yarp + registryFlush.py (Maxim Suhanov) or rla.exe (Eric Zimmerman).
```

Ready.

After some time, it will showcase the message on the screen that our work for this investigation process is completed with zero plugins completed with errors.



Hive File: C:\sam

Report File: C:\Users\SKS19\Desktop\samreport.txt

```
transaction logs.  The tool will check to see if the hive is dirty.

If you need to process/incorporate transaction logs, please consider using
yarp + registryFlush.py (Maxim Suhanov) or rla.exe (Eric Zimmerman).

Hive is not dirty.
Logging to C:\Users\SKS19\Desktop\samreport.log
Hive type: sam
Getting list of plugins based on hive type...
...Done.
Start ripping...
samparse...Done.
0 plugins completed with errors.
```

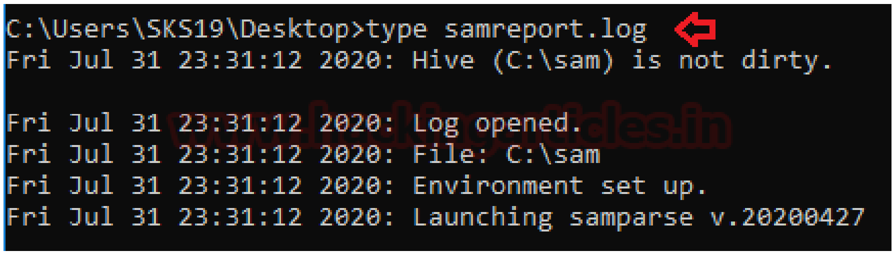
It will **create two files** one with **logs** of the investigation and Second with a **Report** of the investigation.

<u>Analyzing Log: SAM</u>

Now check the **log file** with this command.

```
type samreport.log
```

It will only tell about the environment of this hive file.



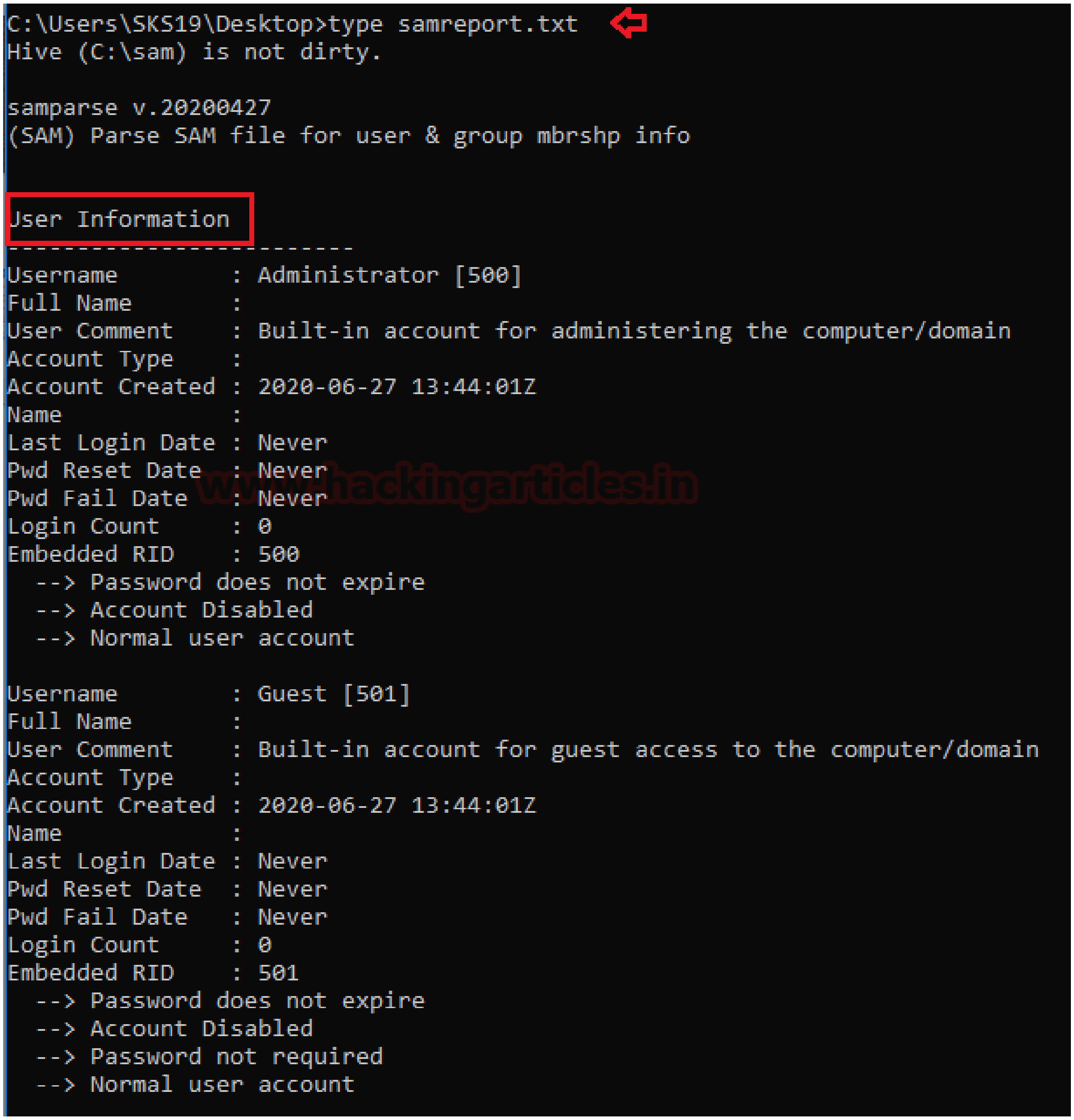
```
C:\Users\SKS19\Desktop>type samreport.log
Fri Jul 31 23:31:12 2020: Hive (C:\sam) is not dirty.

Fri Jul 31 23:31:12 2020: Log opened.
Fri Jul 31 23:31:12 2020: File: C:\sam
Fri Jul 31 23:31:12 2020: Environment set up.
Fri Jul 31 23:31:12 2020: Launching samparse v.20200427
```

Analyzing Report: SAM

Secondly now its Report time. we can access this file with the following commands.

```
type samreport.txt
```

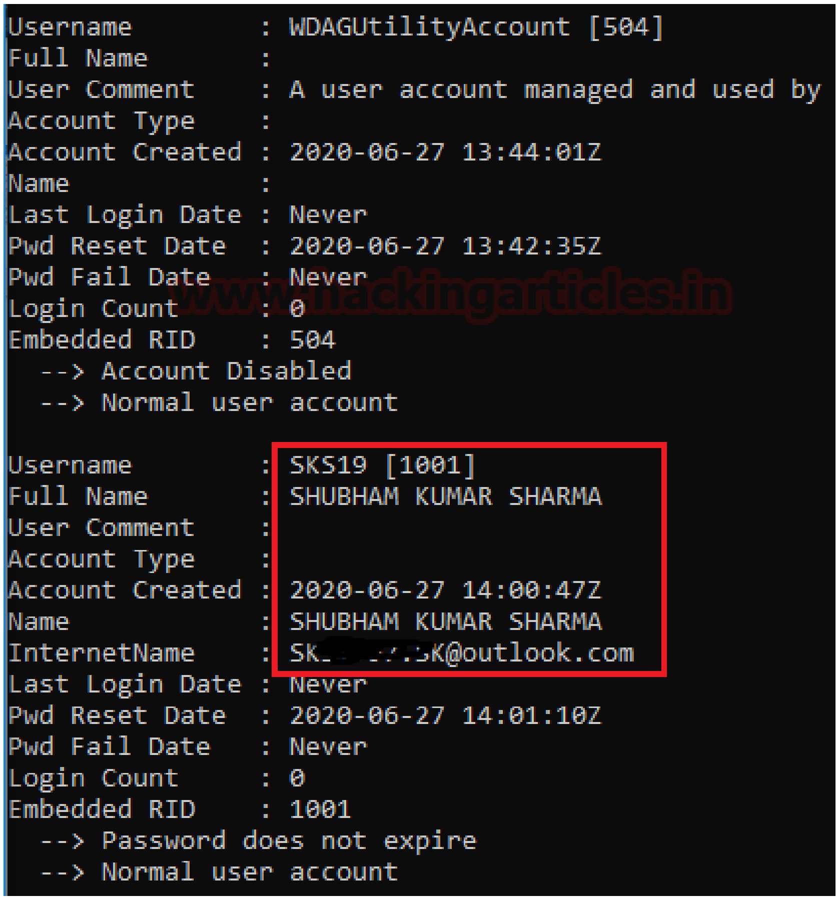
As we can see in the below screenshot it will tell about **SAM version** and **User information**.



```
C:\Users\SKS19\Desktop>type samreport.txt
Hive (C:\sam) is not dirty.

samparse v.20200427
(SAM) Parse SAM file for user & group mbrshp info


User Information
-------------------------
Username        : Administrator [500]
Full Name       :
User Comment    : Built-in account for administering the computer/domain
Account Type    :
Account Created : 2020-06-27 13:44:01Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Login Count     : 0
Embedded RID    : 500
  --> Password does not expire
  --> Account Disabled
  --> Normal user account

Username        : Guest [501]
Full Name       :
User Comment    : Built-in account for guest access to the computer/domain
Account Type    :
Account Created : 2020-06-27 13:44:01Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Login Count     : 0
Embedded RID    : 501
  --> Password does not expire
  --> Account Disabled
  --> Password not required
  --> Normal user account
```

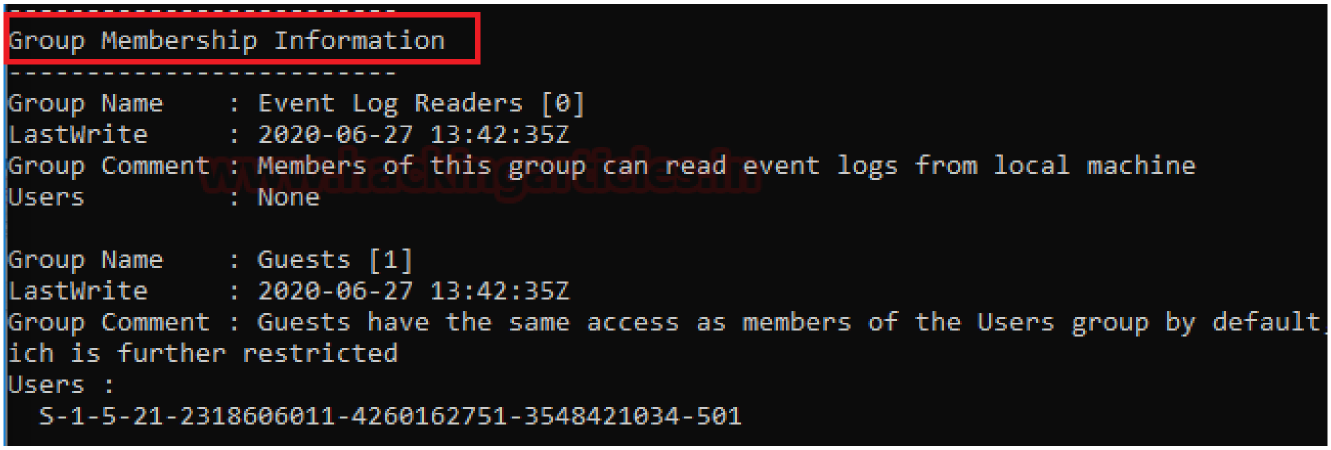
Now, as we can see the main user account got spotted with its major details like.

```
Username: SKS19 [1001]
Full Name: SHUBHAM KUMAR SHARMA
Account Created: 2020-06-27 14:00:47Z
Name: SHUBHAM KUMAR SHARMA
InternetName: S******.SK@outlook.com
Pwd Reset Date: 2020-06-27 14:01:10Z
Embedded RID: 1001
```



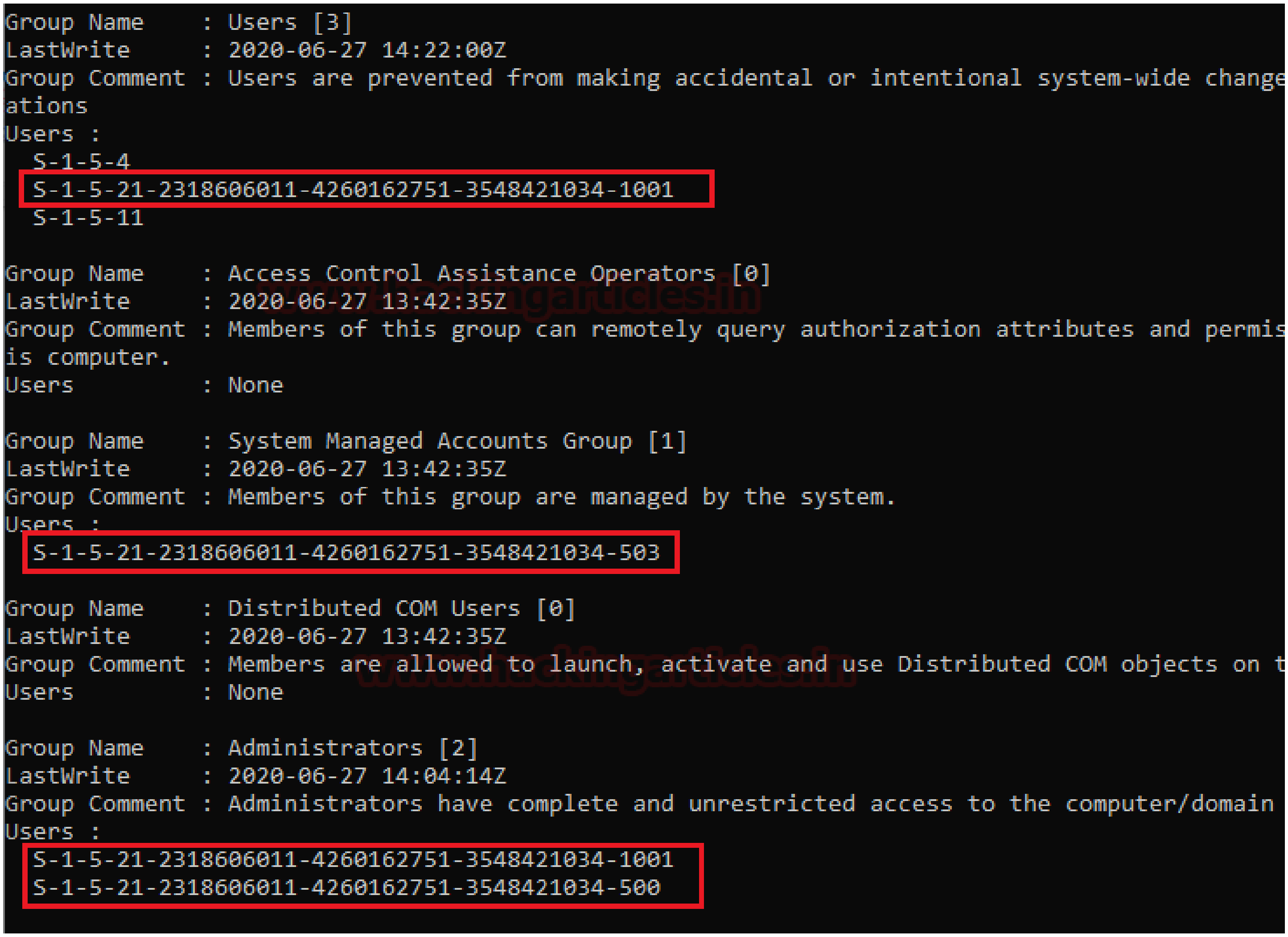
```
Username         : WDAGUtilityAccount [504]
Full Name        :
User Comment     : A user account managed and used by
Account Type     :
Account Created  : 2020-06-27 13:44:01Z
Name             :
Last Login Date  : Never
Pwd Reset Date   : 2020-06-27 13:42:35Z
Pwd Fail Date    : Never
Login Count      : 0
Embedded RID     : 504
  --> Account Disabled
  --> Normal user account

Username         : SKS19 [1001]
Full Name        : SHUBHAM KUMAR SHARMA
User Comment     :
Account Type     :
Account Created  : 2020-06-27 14:00:47Z
Name             : SHUBHAM KUMAR SHARMA
InternetName     : SK[redacted]K@outlook.com
Last Login Date  : Never
Pwd Reset Date   : 2020-06-27 14:01:10Z
Pwd Fail Date    : Never
Login Count      : 0
Embedded RID     : 1001
  --> Password does not expire
  --> Normal user account
```

Next, we have spotted **Group Membership Information.** With its group name Guests and its details.



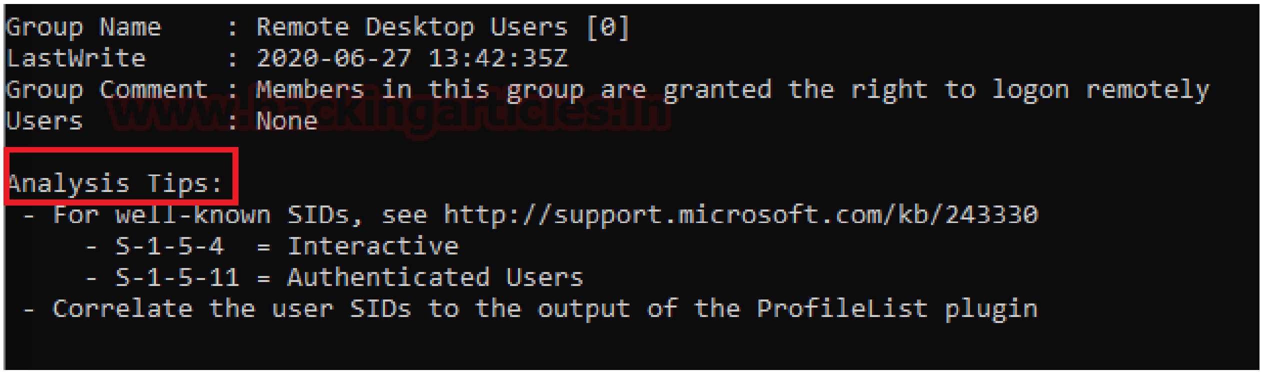
```
-------------------------
Group Membership Information
-------------------------
Group Name     : Event Log Readers [0]
LastWrite      : 2020-06-27 13:42:35Z
Group Comment  : Members of this group can read event logs from local machine
Users          : None

Group Name     : Guests [1]
LastWrite      : 2020-06-27 13:42:35Z
Group Comment  : Guests have the same access as members of the Users group by default
ich is further restricted
Users :
  S-1-5-21-2318606011-4260162751-3548421034-501
```

Some more group membership information, the group's name like Users, System Managed Accounts Group, and Administrators. Their details revel Lastwrite, Group Comment, and Its Users.



```
Group Name    : Users [3]
LastWrite     : 2020-06-27 14:22:00Z
Group Comment : Users are prevented from making accidental or intentional system-wide change
ations
Users :
  S-1-5-4
  S-1-5-21-2318606011-4260162751-3548421034-1001
  S-1-5-11

Group Name    : Access Control Assistance Operators [0]
LastWrite     : 2020-06-27 13:42:35Z
Group Comment : Members of this group can remotely query authorization attributes and permis
is computer.
Users         : None

Group Name    : System Managed Accounts Group [1]
LastWrite     : 2020-06-27 13:42:35Z
Group Comment : Members of this group are managed by the system.
Users :
  S-1-5-21-2318606011-4260162751-3548421034-503

Group Name    : Distributed COM Users [0]
LastWrite     : 2020-06-27 13:42:35Z
Group Comment : Members are allowed to launch, activate and use Distributed COM objects on t
Users         : None

Group Name    : Administrators [2]
LastWrite     : 2020-06-27 14:04:14Z
Group Comment : Administrators have complete and unrestricted access to the computer/domain
Users :
  S-1-5-21-2318606011-4260162751-3548421034-1001
  S-1-5-21-2318606011-4260162751-3548421034-500
```

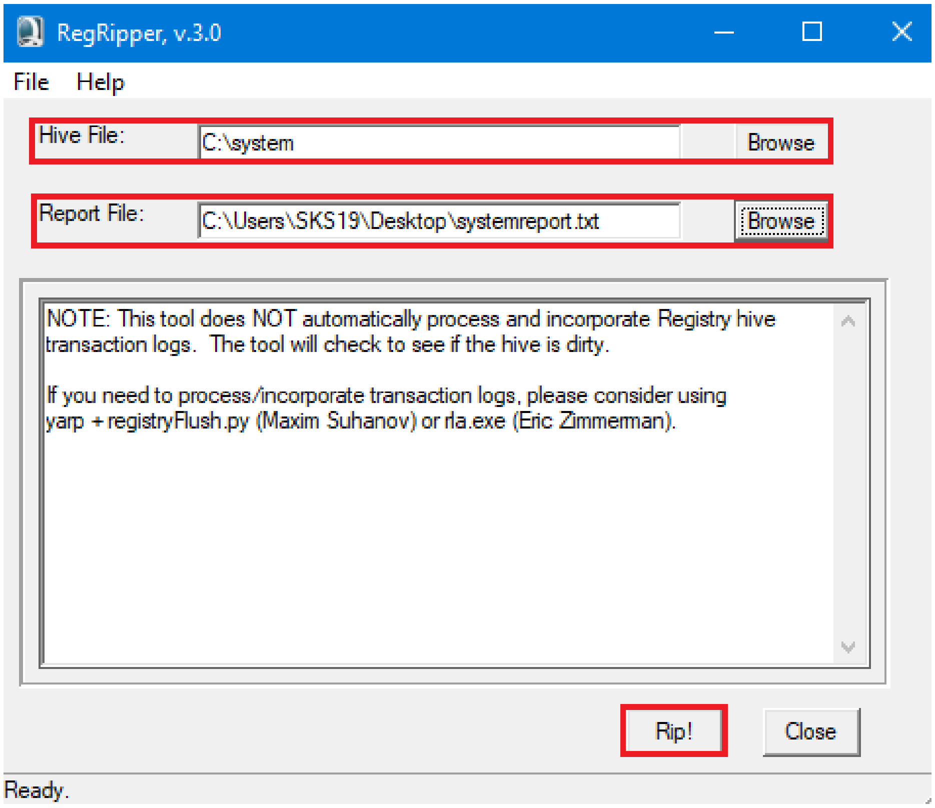
Lastly, RDP and some Analysis tips which would be handy for us in the Investigation.



```
Group Name    : Remote Desktop Users [0]
LastWrite     : 2020-06-27 13:42:35Z
Group Comment : Members in this group are granted the right to logon remotely
Users         : None

Analysis Tips:
 - For well-known SIDs, see http://support.microsoft.com/kb/243330
     - S-1-5-4  = Interactive
     - S-1-5-11 = Authenticated Users
 - Correlate the user SIDs to the output of the ProfileList plugin
```

System Hive

The system hive file consists of all basic information regarding the system information. Now, repeat the same steps for RegRipper and select the location of the **Hive file** and **Report file**. Then click on the **Rip**! Button to start the Investigation process.



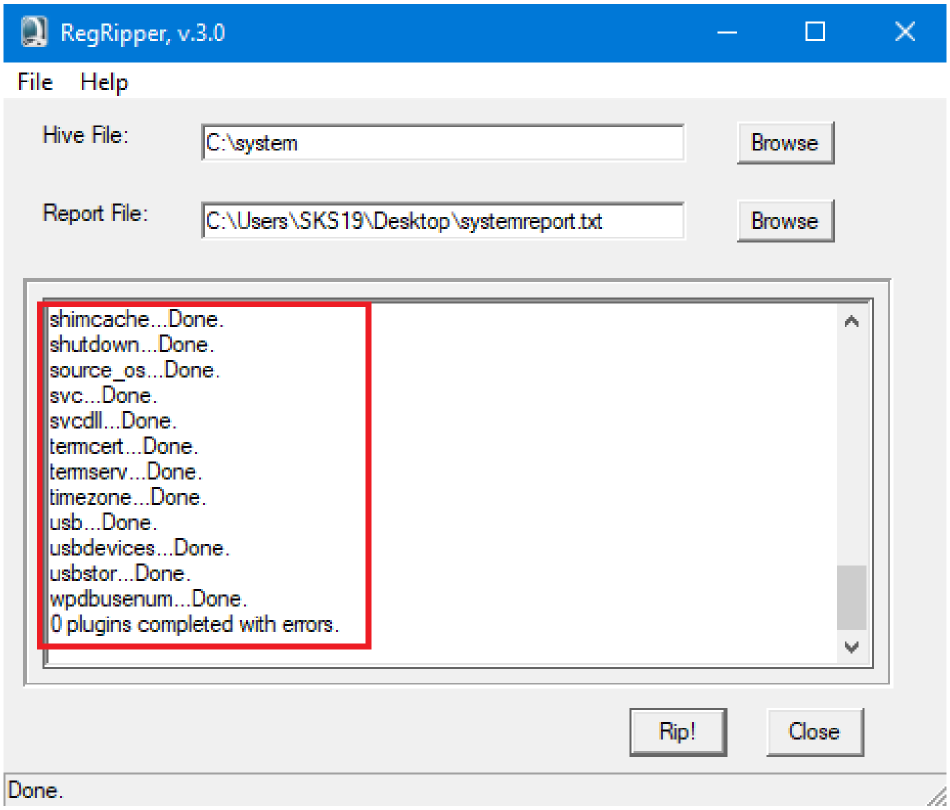
Hive File: C:\system

Report File: C:\Users\SKS19\Desktop\systemreport.txt

```
NOTE: This tool does NOT automatically process and incorporate Registry hive
transaction logs.  The tool will check to see if the hive is dirty.

If you need to process/incorporate transaction logs, please consider using
yarp + registryFlush.py (Maxim Suhanov) or rla.exe (Eric Zimmerman).
```

Ready.

After some time, it will showcase the message on the screen that our work for this investigation process is completed with zero plugins completed with errors. As we mentioned earlier it will create two files: Log and Report.



Hive File: C:\system

Report File: C:\Users\SKS19\Desktop\systemreport.txt

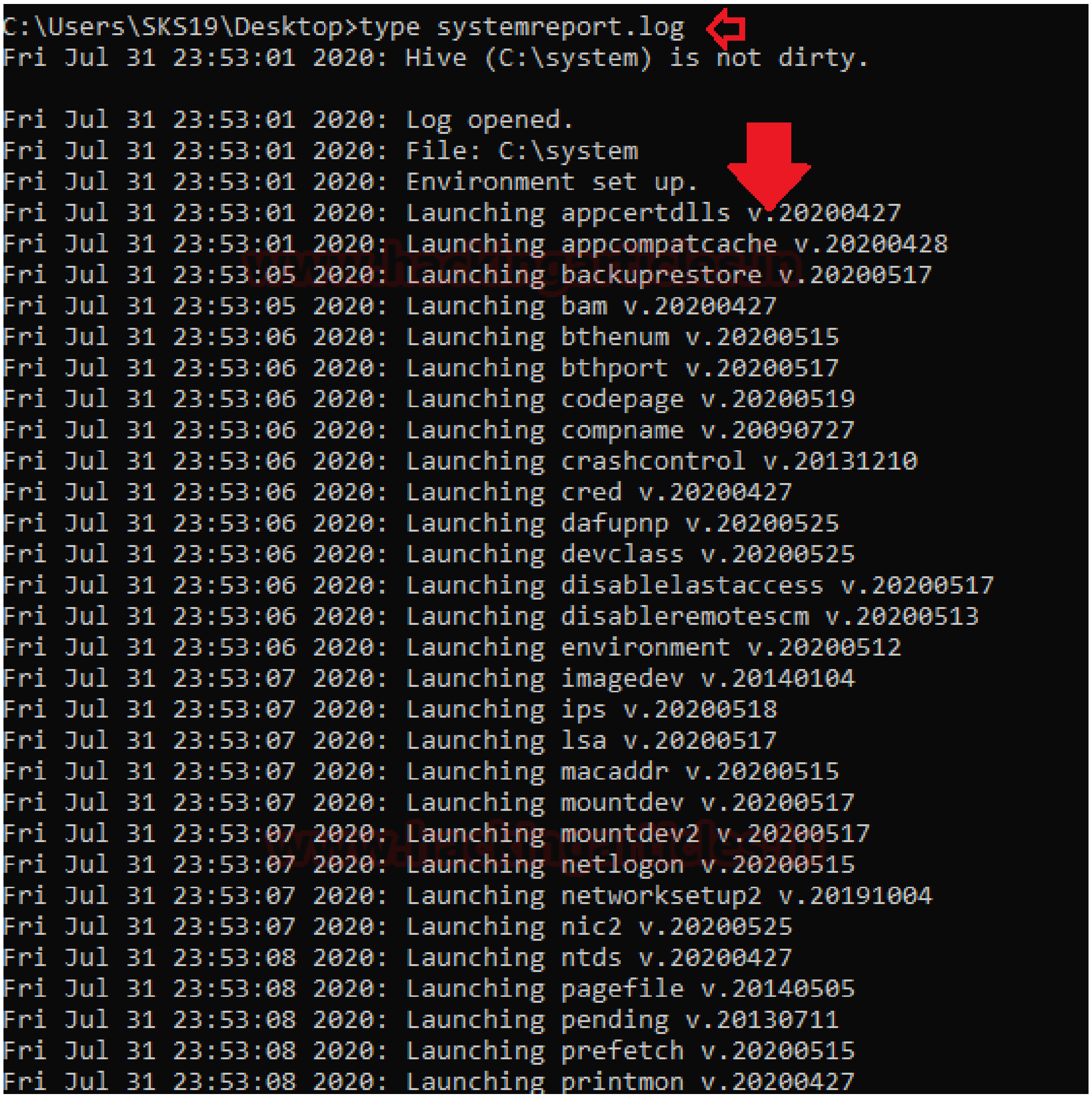
```
shimcache...Done.
shutdown...Done.
source_os...Done.
svc...Done.
svcdll...Done.
termcert...Done.
termserv...Done.
timezone...Done.
usb...Done.
usbdevices...Done.
usbstor...Done.
wpdbusenum...Done.
0 plugins completed with errors.
```

Done.

Analyzing Log: System

The first file is the **log file** regarding gathering information from that directory. After seeing the logs regarding system information.

```
type systemreport.log
```



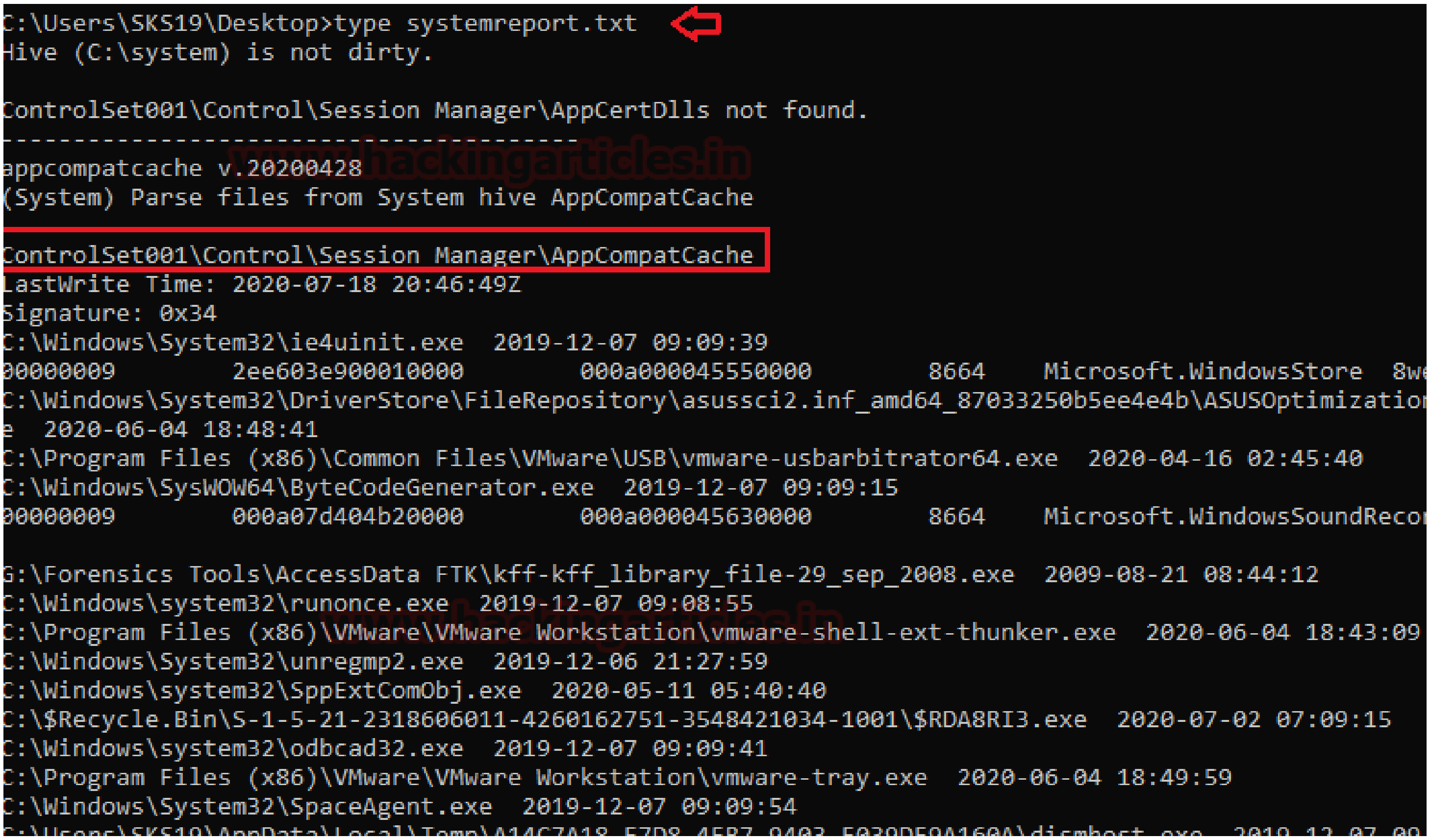
```
C:\Users\SKS19\Desktop>type systemreport.log
Fri Jul 31 23:53:01 2020: Hive (C:\system) is not dirty.

Fri Jul 31 23:53:01 2020: Log opened.
Fri Jul 31 23:53:01 2020: File: C:\system
Fri Jul 31 23:53:01 2020: Environment set up.
Fri Jul 31 23:53:01 2020: Launching appcertdlls v.20200427
Fri Jul 31 23:53:01 2020: Launching appcompatcache v.20200428
Fri Jul 31 23:53:05 2020: Launching backuprestore v.20200517
Fri Jul 31 23:53:05 2020: Launching bam v.20200427
Fri Jul 31 23:53:06 2020: Launching bthenum v.20200515
Fri Jul 31 23:53:06 2020: Launching bthport v.20200517
Fri Jul 31 23:53:06 2020: Launching codepage v.20200519
Fri Jul 31 23:53:06 2020: Launching compname v.20090727
Fri Jul 31 23:53:06 2020: Launching crashcontrol v.20131210
Fri Jul 31 23:53:06 2020: Launching cred v.20200427
Fri Jul 31 23:53:06 2020: Launching dafupnp v.20200525
Fri Jul 31 23:53:06 2020: Launching devclass v.20200525
Fri Jul 31 23:53:06 2020: Launching disablelastaccess v.20200517
Fri Jul 31 23:53:06 2020: Launching disableremotescm v.20200513
Fri Jul 31 23:53:06 2020: Launching environment v.20200512
Fri Jul 31 23:53:07 2020: Launching imagedev v.20140104
Fri Jul 31 23:53:07 2020: Launching ips v.20200518
Fri Jul 31 23:53:07 2020: Launching lsa v.20200517
Fri Jul 31 23:53:07 2020: Launching macaddr v.20200515
Fri Jul 31 23:53:07 2020: Launching mountdev v.20200517
Fri Jul 31 23:53:07 2020: Launching mountdev2 v.20200517
Fri Jul 31 23:53:07 2020: Launching netlogon v.20200515
Fri Jul 31 23:53:07 2020: Launching networksetup2 v.20191004
Fri Jul 31 23:53:07 2020: Launching nic2 v.20200525
Fri Jul 31 23:53:08 2020: Launching ntds v.20200427
Fri Jul 31 23:53:08 2020: Launching pagefile v.20140505
Fri Jul 31 23:53:08 2020: Launching pending v.20130711
Fri Jul 31 23:53:08 2020: Launching prefetch v.20200515
Fri Jul 31 23:53:08 2020: Launching printmon v.20200427
```

<u>Analyzing Report: System</u>

we have opened its **report** with these commands.

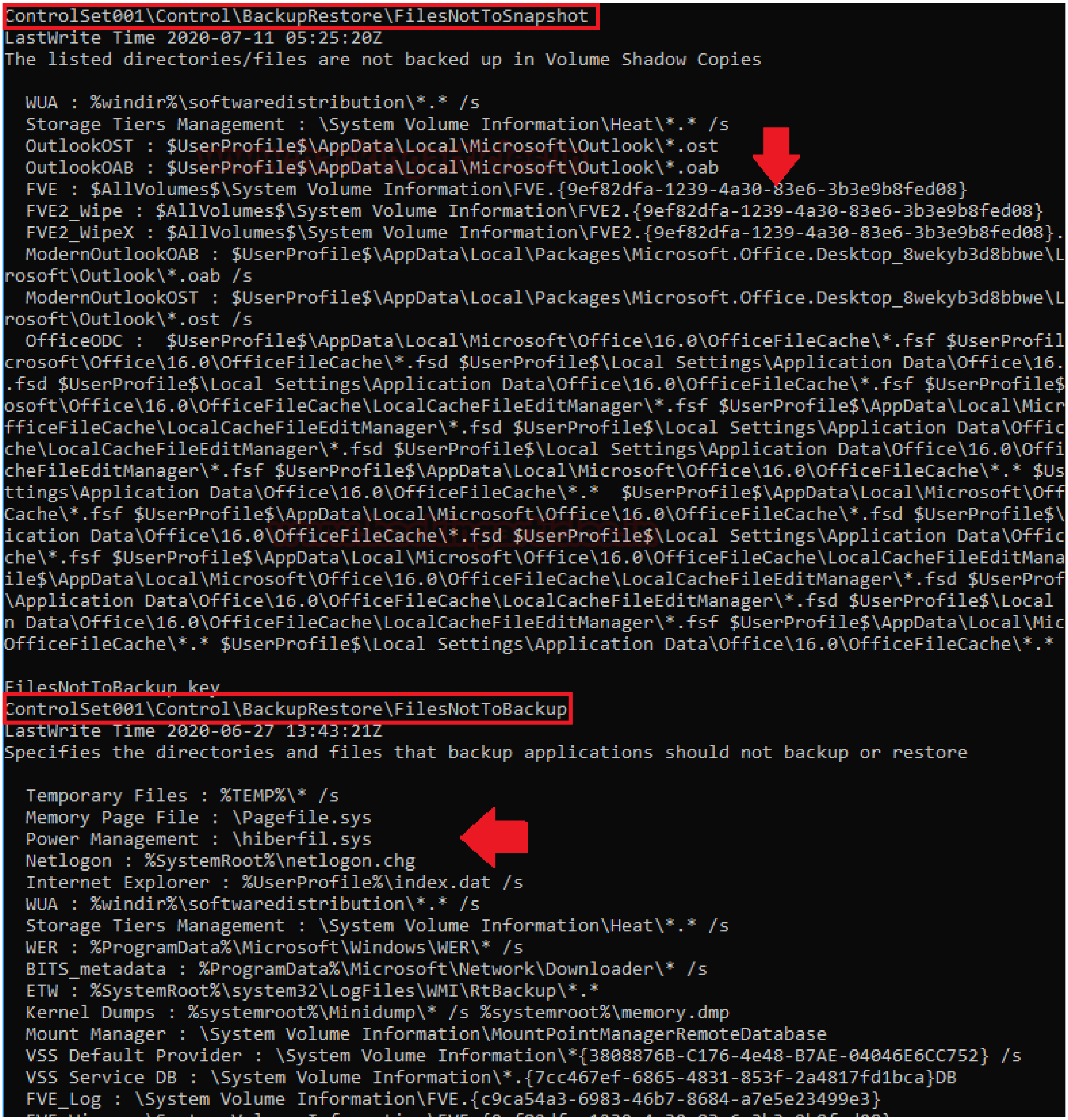
```
type systemreport.txt
```

The below screenshot tells about all the **software installed** with their default directory along with its path.



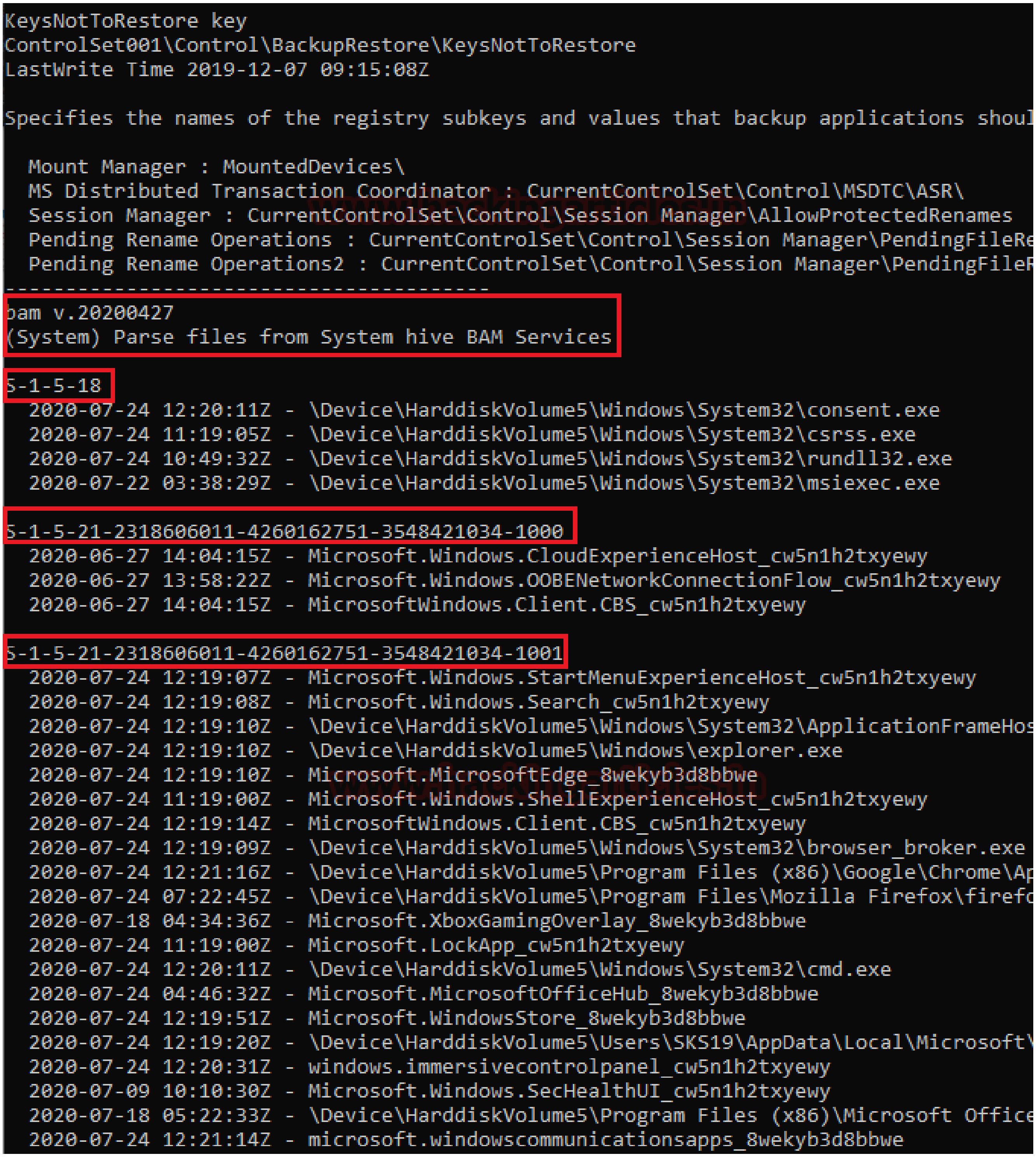
```
C:\Users\SKS19\Desktop>type systemreport.txt
Hive (C:\system) is not dirty.

ControlSet001\Control\Session Manager\AppCertDlls not found.
----------------------------------------
appcompatcache v.20200428
(System) Parse files from System hive AppCompatCache

ControlSet001\Control\Session Manager\AppCompatCache
LastWrite Time: 2020-07-18 20:46:49Z
Signature: 0x34
C:\Windows\System32\ie4uinit.exe  2019-12-07 09:09:39
00000009        2ee603e900010000        000a000045550000        8664    Microsoft.WindowsStore  8we
C:\Windows\System32\DriverStore\FileRepository\asussci2.inf_amd64_87033250b5ee4e4b\ASUSOptimizatio
e  2020-06-04 18:48:41
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe  2020-04-16 02:45:40
C:\Windows\SysWOW64\ByteCodeGenerator.exe  2019-12-07 09:09:15
00000009        000a07d404b20000        000a000045630000        8664    Microsoft.WindowsSoundReco

G:\Forensics Tools\AccessData FTK\kff-kff_library_file-29_sep_2008.exe  2009-08-21 08:44:12
C:\Windows\system32\runonce.exe  2019-12-07 09:08:55
C:\Program Files (x86)\VMware\VMware Workstation\vmware-shell-ext-thunker.exe  2020-06-04 18:43:09
C:\Windows\System32\unregmp2.exe  2019-12-06 21:27:59
C:\Windows\system32\SppExtComObj.exe  2020-05-11 05:40:40
C:\$Recycle.Bin\S-1-5-21-2318606011-4260162751-3548421034-1001\$RDA8RI3.exe  2020-07-02 07:09:15
C:\Windows\system32\odbcad32.exe  2019-12-07 09:09:41
C:\Program Files (x86)\VMware\VMware Workstation\vmware-tray.exe  2020-06-04 18:49:59
C:\Windows\System32\SpaceAgent.exe  2019-12-07 09:09:54
C:\Users\SKS19\AppData\Local\Temp\A14C7A18-E7D8-45B7-9403-E039D59A160A\dismhost.exe  2019-12-07 09
```

After that, we found out control set **backups** details in the victim’s system. Along with **temp** file details.



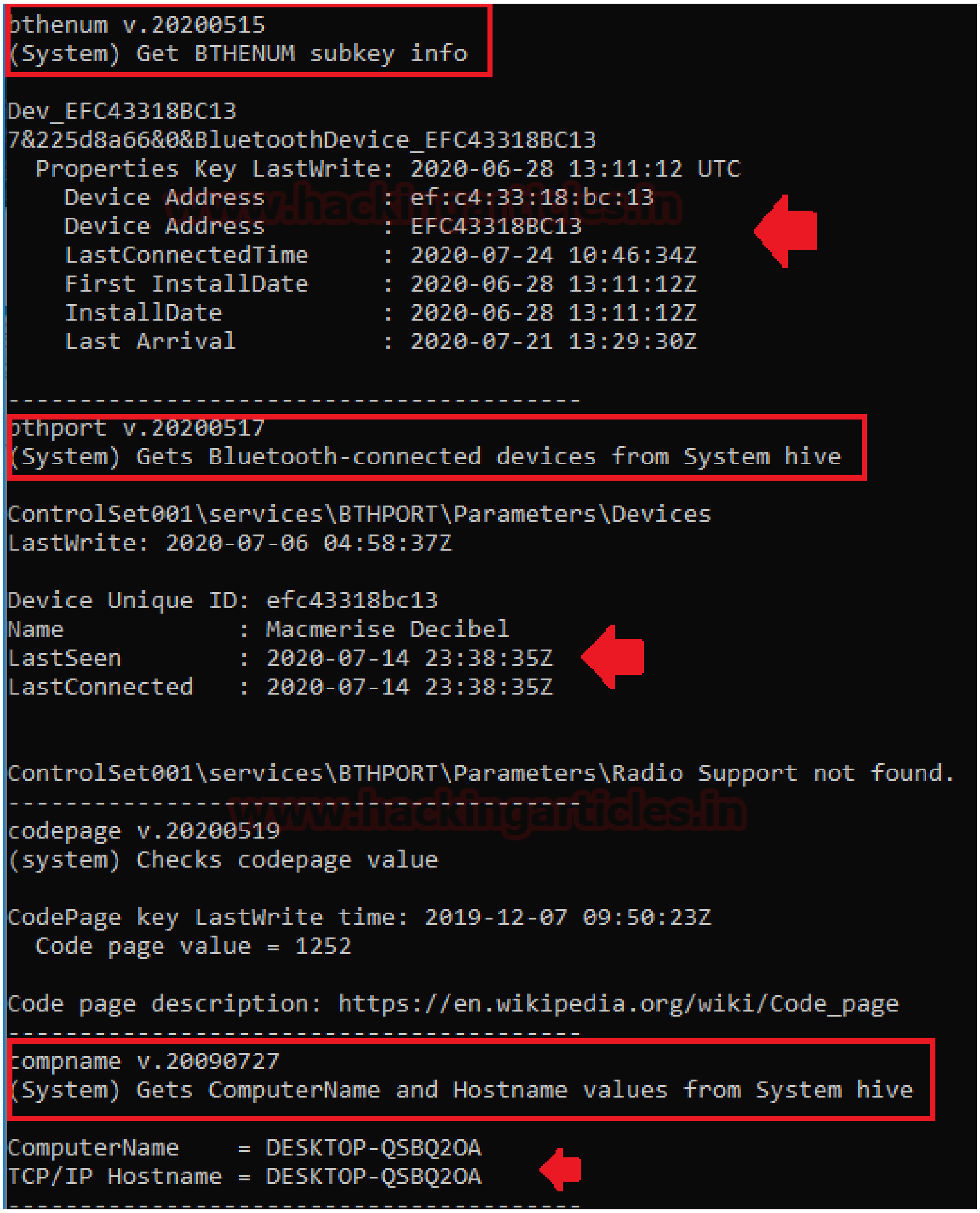
```
ControlSet001\Control\BackupRestore\FilesNotToSnapshot
LastWrite Time 2020-07-11 05:25:20Z
The listed directories/files are not backed up in Volume Shadow Copies

  WUA : %windir%\softwaredistribution\*.* /s
  Storage Tiers Management : \System Volume Information\Heat\*.* /s
  OutlookOST : $UserProfile$\AppData\Local\Microsoft\Outlook\*.ost
  OutlookOAB : $UserProfile$\AppData\Local\Microsoft\Outlook\*.oab
  FVE : $AllVolumes$\System Volume Information\FVE.{9ef82dfa-1239-4a30-83e6-3b3e9b8fed08}
  FVE2_Wipe : $AllVolumes$\System Volume Information\FVE2.{9ef82dfa-1239-4a30-83e6-3b3e9b8fed08}
  FVE2_WipeX : $AllVolumes$\System Volume Information\FVE2.{9ef82dfa-1239-4a30-83e6-3b3e9b8fed08}.
  ModernOutlookOAB : $UserProfile$\AppData\Local\Packages\Microsoft.Office.Desktop_8wekyb3d8bbwe\L
rosoft\Outlook\*.oab /s
  ModernOutlookOST : $UserProfile$\AppData\Local\Packages\Microsoft.Office.Desktop_8wekyb3d8bbwe\L
rosoft\Outlook\*.ost /s
  OfficeODC :  $UserProfile$\AppData\Local\Microsoft\Office\16.0\OfficeFileCache\*.fsf $UserProfil
crosoft\Office\16.0\OfficeFileCache\*.fsd $UserProfile$\Local Settings\Application Data\Office\16.
.fsd $UserProfile$\Local Settings\Application Data\Office\16.0\OfficeFileCache\*.fsf $UserProfile$
osoft\Office\16.0\OfficeFileCache\LocalCacheFileEditManager\*.fsf $UserProfile$\AppData\Local\Micr
fficeFileCache\LocalCacheFileEditManager\*.fsd $UserProfile$\Local Settings\Application Data\Offic
che\LocalCacheFileEditManager\*.fsd $UserProfile$\Local Settings\Application Data\Office\16.0\Offi
cheFileEditManager\*.fsf $UserProfile$\AppData\Local\Microsoft\Office\16.0\OfficeFileCache\*.* $Us
ttings\Application Data\Office\16.0\OfficeFileCache\*.*  $UserProfile$\AppData\Local\Microsoft\Off
Cache\*.fsf $UserProfile$\AppData\Local\Microsoft\Office\16.0\OfficeFileCache\*.fsd $UserProfile$\
ication Data\Office\16.0\OfficeFileCache\*.fsd $UserProfile$\Local Settings\Application Data\Offic
che\*.fsf $UserProfile$\AppData\Local\Microsoft\Office\16.0\OfficeFileCache\LocalCacheFileEditMana
ile$\AppData\Local\Microsoft\Office\16.0\OfficeFileCache\LocalCacheFileEditManager\*.fsd $UserProf
\Application Data\Office\16.0\OfficeFileCache\LocalCacheFileEditManager\*.fsd $UserProfile$\Local
n Data\Office\16.0\OfficeFileCache\LocalCacheFileEditManager\*.fsf $UserProfile$\AppData\Local\Mic
OfficeFileCache\*.* $UserProfile$\Local Settings\Application Data\Office\16.0\OfficeFileCache\*.*

FilesNotToBackup key
ControlSet001\Control\BackupRestore\FilesNotToBackup
LastWrite Time 2020-06-27 13:43:21Z
Specifies the directories and files that backup applications should not backup or restore

  Temporary Files : %TEMP%\* /s
  Memory Page File : \Pagefile.sys
  Power Management : \hiberfil.sys
  Netlogon : %SystemRoot%\netlogon.chg
  Internet Explorer : %UserProfile%\index.dat /s
  WUA : %windir%\softwaredistribution\*.* /s
  Storage Tiers Management : \System Volume Information\Heat\*.* /s
  WER : %ProgramData%\Microsoft\Windows\WER\* /s
  BITS_metadata : %ProgramData%\Microsoft\Network\Downloader\* /s
  ETW : %SystemRoot%\system32\LogFiles\WMI\RtBackup\*.*
  Kernel Dumps : %systemroot%\Minidump\* /s %systemroot%\memory.dmp
  Mount Manager : \System Volume Information\MountPointManagerRemoteDatabase
  VSS Default Provider : \System Volume Information\*{3808876B-C176-4e48-B7AE-04046E6CC752} /s
  VSS Service DB : \System Volume Information\*.{7cc467ef-6865-4831-853f-2a4817fd1bca}DB
  FVE_Log : \System Volume Information\FVE.{c9ca54a3-6983-46b7-8684-a7e5e23499e3}
```

Now, this result is showing us about the HKLM [HKEY_LOCAL_MACHINE] user’s BAM. It is a user-specific application.



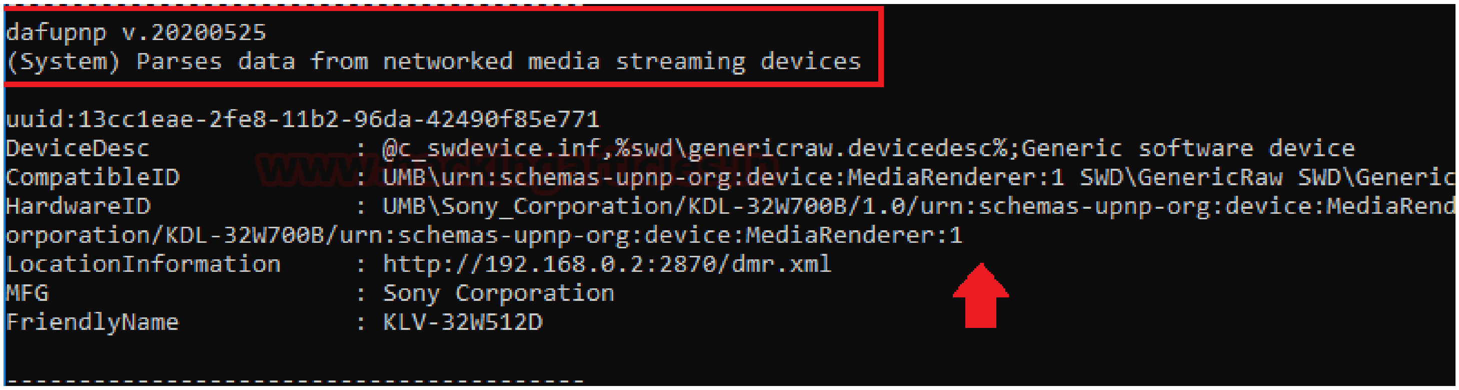
```
KeysNotToRestore key
ControlSet001\Control\BackupRestore\KeysNotToRestore
LastWrite Time 2019-12-07 09:15:08Z

Specifies the names of the registry subkeys and values that backup applications shoul

  Mount Manager : MountedDevices\
  MS Distributed Transaction Coordinator : CurrentControlSet\Control\MSDTC\ASR\
  Session Manager : CurrentControlSet\Control\Session Manager\AllowProtectedRenames
  Pending Rename Operations : CurrentControlSet\Control\Session Manager\PendingFileRe
  Pending Rename Operations2 : CurrentControlSet\Control\Session Manager\PendingFileR
----------------------------------------
bam v.20200427
(System) Parse files from System hive BAM Services

S-1-5-18
  2020-07-24 12:20:11Z - \Device\HarddiskVolume5\Windows\System32\consent.exe
  2020-07-24 11:19:05Z - \Device\HarddiskVolume5\Windows\System32\csrss.exe
  2020-07-24 10:49:32Z - \Device\HarddiskVolume5\Windows\System32\rundll32.exe
  2020-07-22 03:38:29Z - \Device\HarddiskVolume5\Windows\System32\msiexec.exe

S-1-5-21-2318606011-4260162751-3548421034-1000
  2020-06-27 14:04:15Z - Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy
  2020-06-27 13:58:22Z - Microsoft.Windows.OOBENetworkConnectionFlow_cw5n1h2txyewy
  2020-06-27 14:04:15Z - MicrosoftWindows.Client.CBS_cw5n1h2txyewy

S-1-5-21-2318606011-4260162751-3548421034-1001
  2020-07-24 12:19:07Z - Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy
  2020-07-24 12:19:08Z - Microsoft.Windows.Search_cw5n1h2txyewy
  2020-07-24 12:19:10Z - \Device\HarddiskVolume5\Windows\System32\ApplicationFrameHos
  2020-07-24 12:19:10Z - \Device\HarddiskVolume5\Windows\explorer.exe
  2020-07-24 12:19:10Z - Microsoft.MicrosoftEdge_8wekyb3d8bbwe
  2020-07-24 11:19:00Z - Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy
  2020-07-24 12:19:14Z - MicrosoftWindows.Client.CBS_cw5n1h2txyewy
  2020-07-24 12:19:09Z - \Device\HarddiskVolume5\Windows\System32\browser_broker.exe
  2020-07-24 12:21:16Z - \Device\HarddiskVolume5\Program Files (x86)\Google\Chrome\Ap
  2020-07-24 07:22:45Z - \Device\HarddiskVolume5\Program Files\Mozilla Firefox\firefo
  2020-07-18 04:34:36Z - Microsoft.XboxGamingOverlay_8wekyb3d8bbwe
  2020-07-24 11:19:00Z - Microsoft.LockApp_cw5n1h2txyewy
  2020-07-24 12:20:11Z - \Device\HarddiskVolume5\Windows\System32\cmd.exe
  2020-07-24 04:46:32Z - Microsoft.MicrosoftOfficeHub_8wekyb3d8bbwe
  2020-07-24 12:19:51Z - Microsoft.WindowsStore_8wekyb3d8bbwe
  2020-07-24 12:19:20Z - \Device\HarddiskVolume5\Users\SKS19\AppData\Local\Microsoft\
  2020-07-24 12:20:31Z - windows.immersivecontrolpanel_cw5n1h2txyewy
  2020-07-09 10:10:30Z - Microsoft.Windows.SecHealthUI_cw5n1h2txyewy
  2020-07-18 05:22:33Z - \Device\HarddiskVolume5\Program Files (x86)\Microsoft Office
  2020-07-24 12:21:14Z - microsoft.windowscommunicationsapps_8wekyb3d8bbwe
```

Now it shows, Some device details, Computer name on diff-diff instances and crash control information.



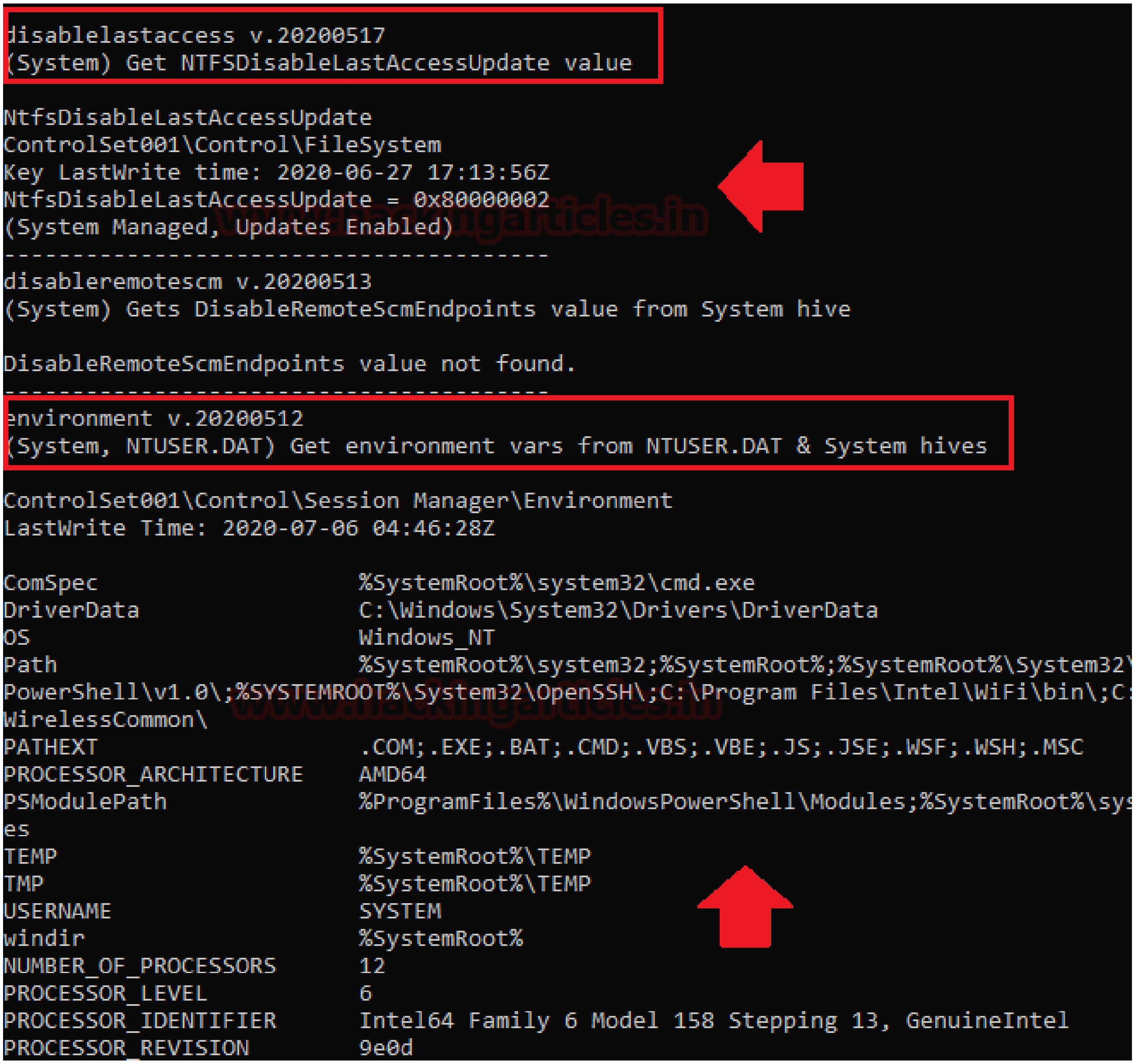
```
bthenum v.20200515
(System) Get BTHENUM subkey info

Dev_EFC43318BC13
7&225d8a66&0&BluetoothDevice_EFC43318BC13
  Properties Key LastWrite: 2020-06-28 13:11:12 UTC
    Device Address         : ef:c4:33:18:bc:13
    Device Address         : EFC43318BC13
    LastConnectedTime      : 2020-07-24 10:46:34Z
    First InstallDate      : 2020-06-28 13:11:12Z
    InstallDate            : 2020-06-28 13:11:12Z
    Last Arrival           : 2020-07-21 13:29:30Z

----------------------------------------
bthport v.20200517
(System) Gets Bluetooth-connected devices from System hive

ControlSet001\services\BTHPORT\Parameters\Devices
LastWrite: 2020-07-06 04:58:37Z

Device Unique ID: efc43318bc13
Name            : Macmerise Decibel
LastSeen        : 2020-07-14 23:38:35Z
LastConnected   : 2020-07-14 23:38:35Z


ControlSet001\services\BTHPORT\Parameters\Radio Support not found.
----------------------------------------
codepage v.20200519
(system) Checks codepage value

CodePage key LastWrite time: 2019-12-07 09:50:23Z
  Code page value = 1252

Code page description: https://en.wikipedia.org/wiki/Code_page
----------------------------------------
compname v.20090727
(System) Gets ComputerName and Hostname values from System hive

ComputerName     = DESKTOP-QSBQ2OA
TCP/IP Hostname = DESKTOP-QSBQ2OA
----------------------------------------
```

Now the network media streaming devices connected with the system. In our case, it is from a Sony corporation. We can get along some interesting details with its hardware ID. It also gets some details regarding the connected USB devices no matter their currently connected or not.



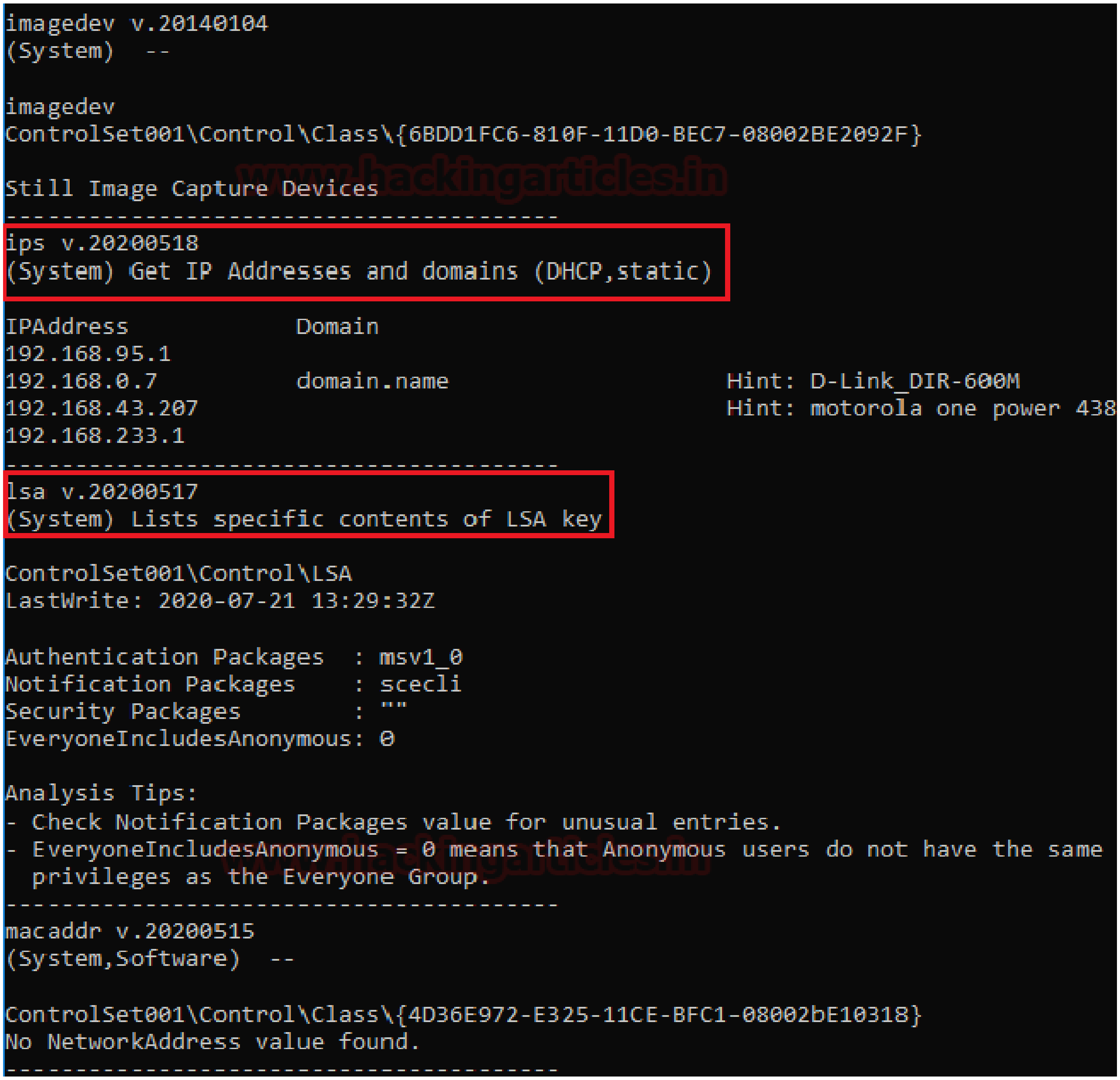
```
----------------------------------------
dafupnp v.20200525
(System) Parses data from networked media streaming devices

uuid:13cc1eae-2fe8-11b2-96da-42490f85e771
DeviceDesc               : @c_swdevice.inf,%swd\genericraw.devicedesc%;Generic software device
CompatibleID             : UMB\urn:schemas-upnp-org:device:MediaRenderer:1 SWD\GenericRaw SWD\Generic
HardwareID               : UMB\Sony_Corporation/KDL-32W700B/1.0/urn:schemas-upnp-org:device:MediaRend
orporation/KDL-32W700B/urn:schemas-upnp-org:device:MediaRenderer:1
LocationInformation      : http://192.168.0.2:2870/dmr.xml
MFG                      : Sony Corporation
FriendlyName             : KLV-32W512D

----------------------------------------
```

After this, it will cover the hardware details along with NTFS disable the last access update. Like, ControlSet001\Control\Session Manager\Environment, **Hardware details**.



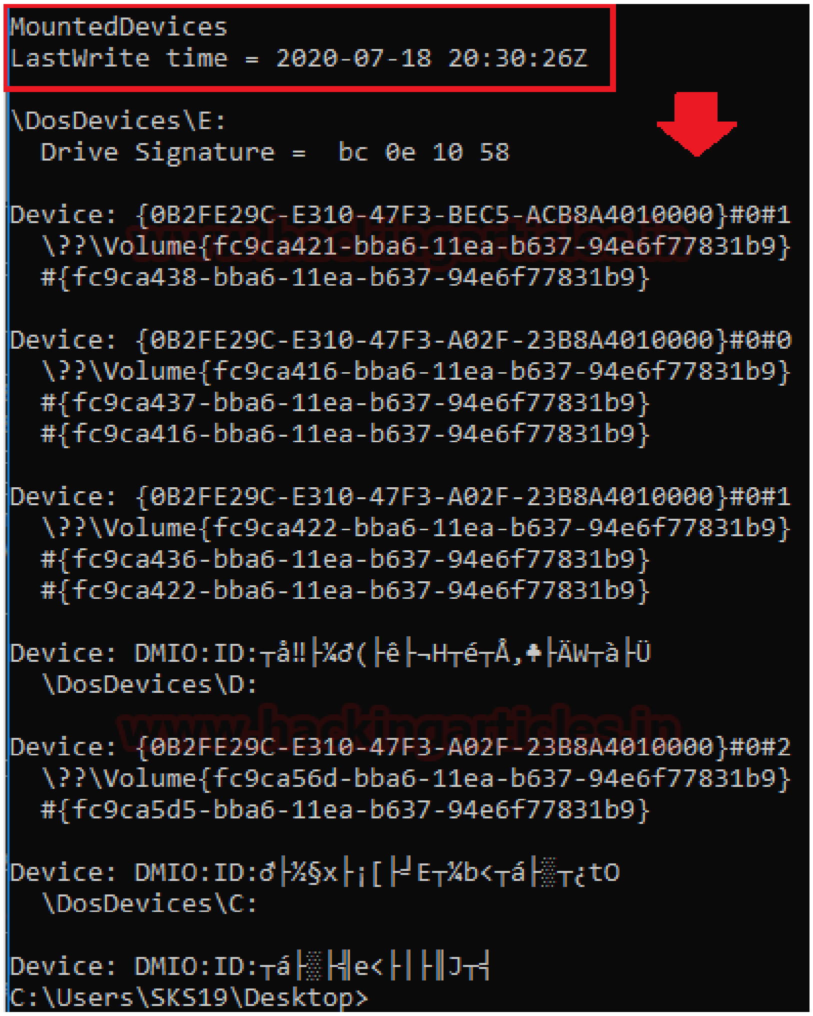
```
disablelastaccess v.20200517
(System) Get NTFSDisableLastAccessUpdate value

NtfsDisableLastAccessUpdate
ControlSet001\Control\FileSystem
Key LastWrite time: 2020-06-27 17:13:56Z
NtfsDisableLastAccessUpdate = 0x80000002
(System Managed, Updates Enabled)
----------------------------------------
disableremotescm v.20200513
(System) Gets DisableRemoteScmEndpoints value from System hive

DisableRemoteScmEndpoints value not found.
----------------------------------------
environment v.20200512
(System, NTUSER.DAT) Get environment vars from NTUSER.DAT & System hives

ControlSet001\Control\Session Manager\Environment
LastWrite Time: 2020-07-06 04:46:28Z

ComSpec                    %SystemRoot%\system32\cmd.exe
DriverData                 C:\Windows\System32\Drivers\DriverData
OS                         Windows_NT
Path                       %SystemRoot%\system32;%SystemRoot%;%SystemRoot%\System32\
PowerShell\v1.0\;%SYSTEMROOT%\System32\OpenSSH\;C:\Program Files\Intel\WiFi\bin\;C:
WirelessCommon\
PATHEXT                    .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE     AMD64
PSModulePath               %ProgramFiles%\WindowsPowerShell\Modules;%SystemRoot%\sys
es
TEMP                       %SystemRoot%\TEMP
TMP                        %SystemRoot%\TEMP
USERNAME                   SYSTEM
windir                     %SystemRoot%
NUMBER_OF_PROCESSORS       12
PROCESSOR_LEVEL            6
PROCESSOR_IDENTIFIER       Intel64 Family 6 Model 158 Stepping 13, GenuineIntel
PROCESSOR_REVISION         9e0d
```

After this **IP address** and **Domain name** details with Hint. Analysis Tips and Mounted devices.



```
imagedev v.20140104
(System)  --

imagedev
ControlSet001\Control\Class\{6BDD1FC6-810F-11D0-BEC7-08002BE2092F}

Still Image Capture Devices
----------------------------------------
ips v.20200518
(System) Get IP Addresses and domains (DHCP,static)

IPAddress            Domain
192.168.95.1
192.168.0.7          domain.name                    Hint: D-Link_DIR-600M
192.168.43.207                                      Hint: motorola one power 438
192.168.233.1
----------------------------------------
lsa v.20200517
(System) Lists specific contents of LSA key

ControlSet001\Control\LSA
LastWrite: 2020-07-21 13:29:32Z

Authentication Packages  : msv1_0
Notification Packages    : scecli
Security Packages        : ""
EveryoneIncludesAnonymous: 0

Analysis Tips:
- Check Notification Packages value for unusual entries.
- EveryoneIncludesAnonymous = 0 means that Anonymous users do not have the same
  privileges as the Everyone Group.
----------------------------------------
macaddr v.20200515
(System,Software)  --

ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002bE10318}
No NetworkAddress value found.
----------------------------------------
```

Now Finally in the System file, we got details regarding mounted devices details. It gets all details whether they are currently mounted or not.

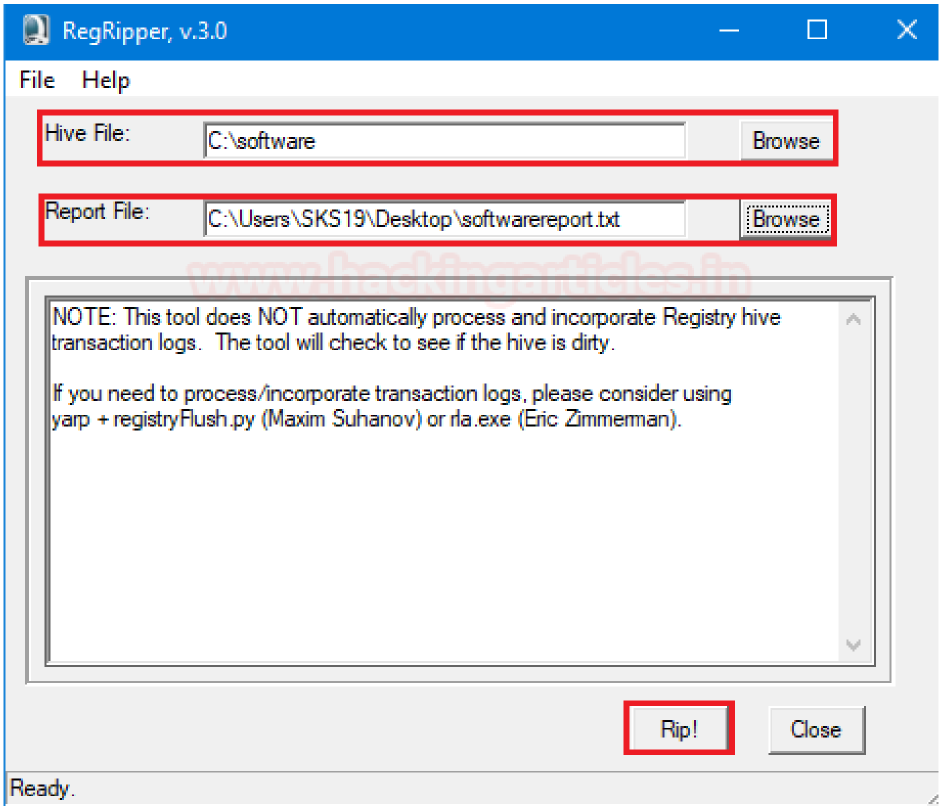


```
MountedDevices
LastWrite time = 2020-07-18 20:30:26Z

\DosDevices\E:
  Drive Signature =  bc 0e 10 58

Device: {0B2FE29C-E310-47F3-BEC5-ACB8A4010000}#0#1
  \??\Volume{fc9ca421-bba6-11ea-b637-94e6f77831b9}
  #{fc9ca438-bba6-11ea-b637-94e6f77831b9}

Device: {0B2FE29C-E310-47F3-A02F-23B8A4010000}#0#0
  \??\Volume{fc9ca416-bba6-11ea-b637-94e6f77831b9}
  #{fc9ca437-bba6-11ea-b637-94e6f77831b9}
  #{fc9ca416-bba6-11ea-b637-94e6f77831b9}

Device: {0B2FE29C-E310-47F3-A02F-23B8A4010000}#0#1
  \??\Volume{fc9ca422-bba6-11ea-b637-94e6f77831b9}
  #{fc9ca436-bba6-11ea-b637-94e6f77831b9}
  #{fc9ca422-bba6-11ea-b637-94e6f77831b9}

Device: DMIO:ID:┬å‼├%♂(├ê├¬H┬é┬Å,♣├ÄW┬à├Ü
  \DosDevices\D:

Device: {0B2FE29C-E310-47F3-A02F-23B8A4010000}#0#2
  \??\Volume{fc9ca56d-bba6-11ea-b637-94e6f77831b9}
  #{fc9ca5d5-bba6-11ea-b637-94e6f77831b9}

Device: DMIO:ID:♂├%§x├¡[├╛E┬%b<┬á├▒┬¿tO
  \DosDevices\C:

Device: DMIO:ID:┬á├▒╟e<├│├║J┬┤
C:\Users\SKS19\Desktop>
```

Software Hive

Software Hive file consists, all the information regarding the software installed in this system.

Now, follow the previous steps for RegRipper and select the location of the **Hive file** and **Report file**. Then click on the **Rip**! Button to start the Investigation process.



Hive File: C:\software

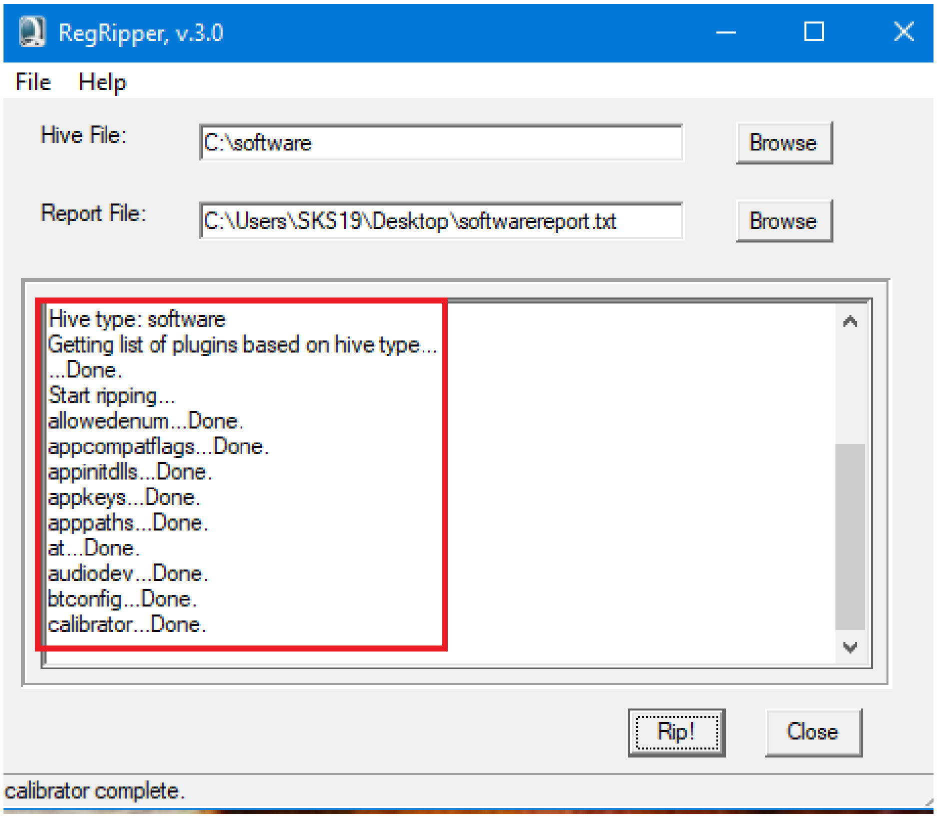
Report File: C:\Users\SKS19\Desktop\softwarereport.txt

NOTE: This tool does NOT automatically process and incorporate Registry hive transaction logs. The tool will check to see if the hive is dirty.

If you need to process/incorporate transaction logs, please consider using yarp + registryFlush.py (Maxim Suhanov) or rla.exe (Eric Zimmerman).

Ready.

After some time, it will showcase the message on the screen that our work for this investigation process is completed with zero plugins completed with errors.



Hive File: C:\software

Report File: C:\Users\SKS19\Desktop\softwarereport.txt

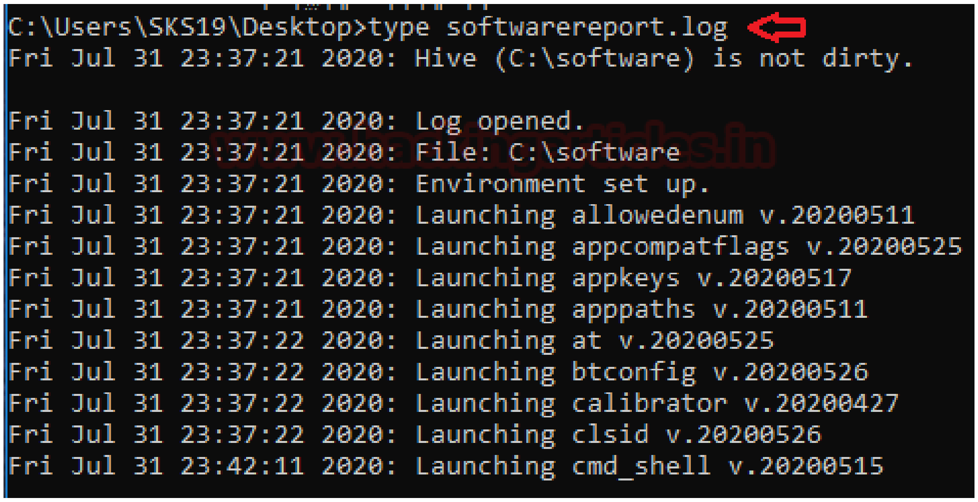
```
Hive type: software
Getting list of plugins based on hive type...
...Done.
Start ripping...
allowedenum...Done.
appcompatflags...Done.
appinitdlls...Done.
appkeys...Done.
apppaths...Done.
at...Done.
audiodev...Done.
btconfig...Done.
calibrator...Done.
```

calibrator complete.

Analyzing Log: Software

As usual, we opened the **logfile** first to check its log to understand through which file it is detecting to create an Investigation report for this file. Now run this command to view this file.

```
type softwarereport.log
```



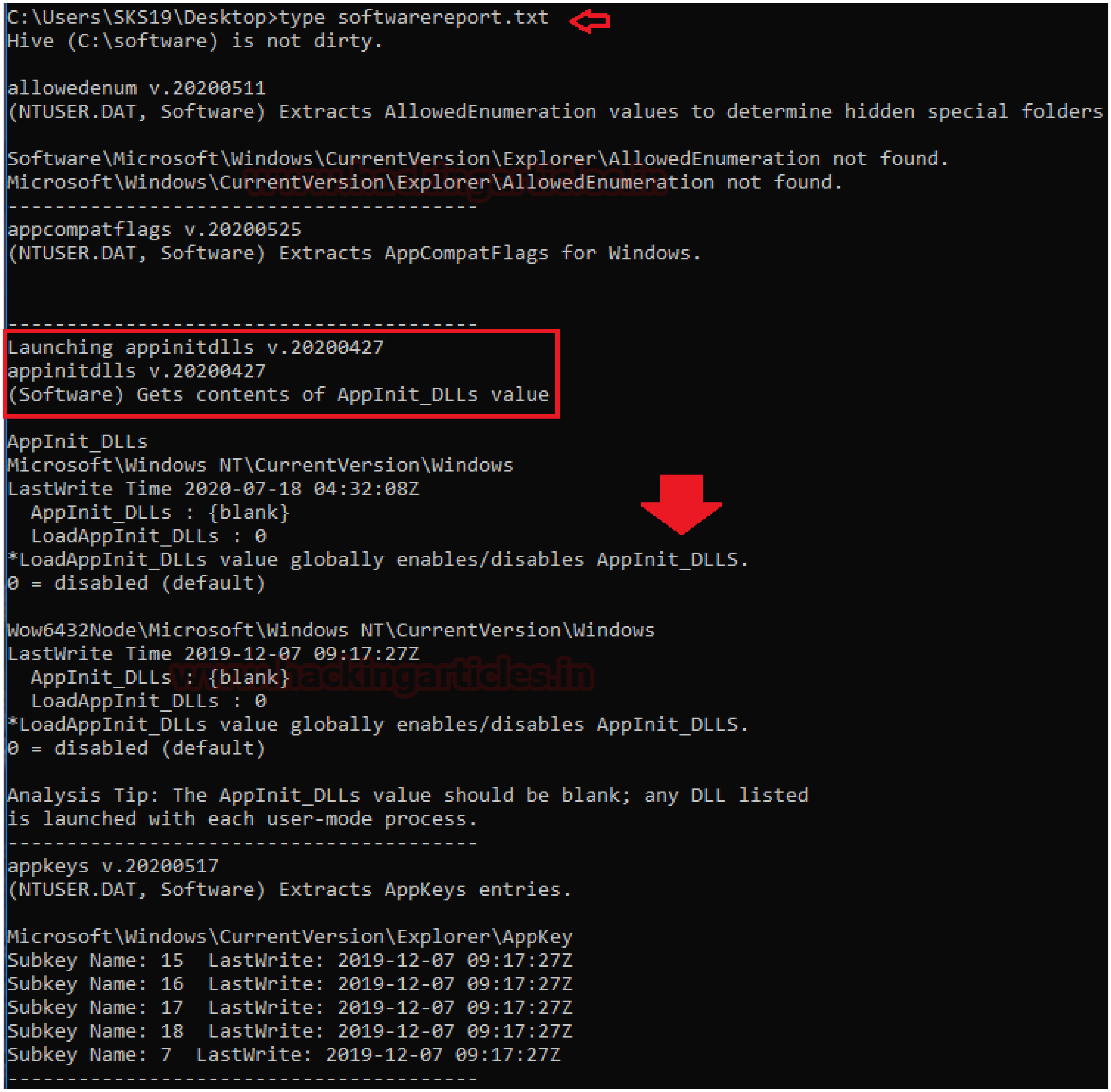
```
C:\Users\SKS19\Desktop>type softwarereport.log
Fri Jul 31 23:37:21 2020: Hive (C:\software) is not dirty.

Fri Jul 31 23:37:21 2020: Log opened.
Fri Jul 31 23:37:21 2020: File: C:\software
Fri Jul 31 23:37:21 2020: Environment set up.
Fri Jul 31 23:37:21 2020: Launching allowedenum v.20200511
Fri Jul 31 23:37:21 2020: Launching appcompatflags v.20200525
Fri Jul 31 23:37:21 2020: Launching appkeys v.20200517
Fri Jul 31 23:37:21 2020: Launching apppaths v.20200511
Fri Jul 31 23:37:22 2020: Launching at v.20200525
Fri Jul 31 23:37:22 2020: Launching btconfig v.20200526
Fri Jul 31 23:37:22 2020: Launching calibrator v.20200427
Fri Jul 31 23:37:22 2020: Launching clsid v.20200526
Fri Jul 31 23:42:11 2020: Launching cmd_shell v.20200515
```

Analyzing Report: Software

Now we need to view the **report file** of the software hive file. So, run this command to get this file.

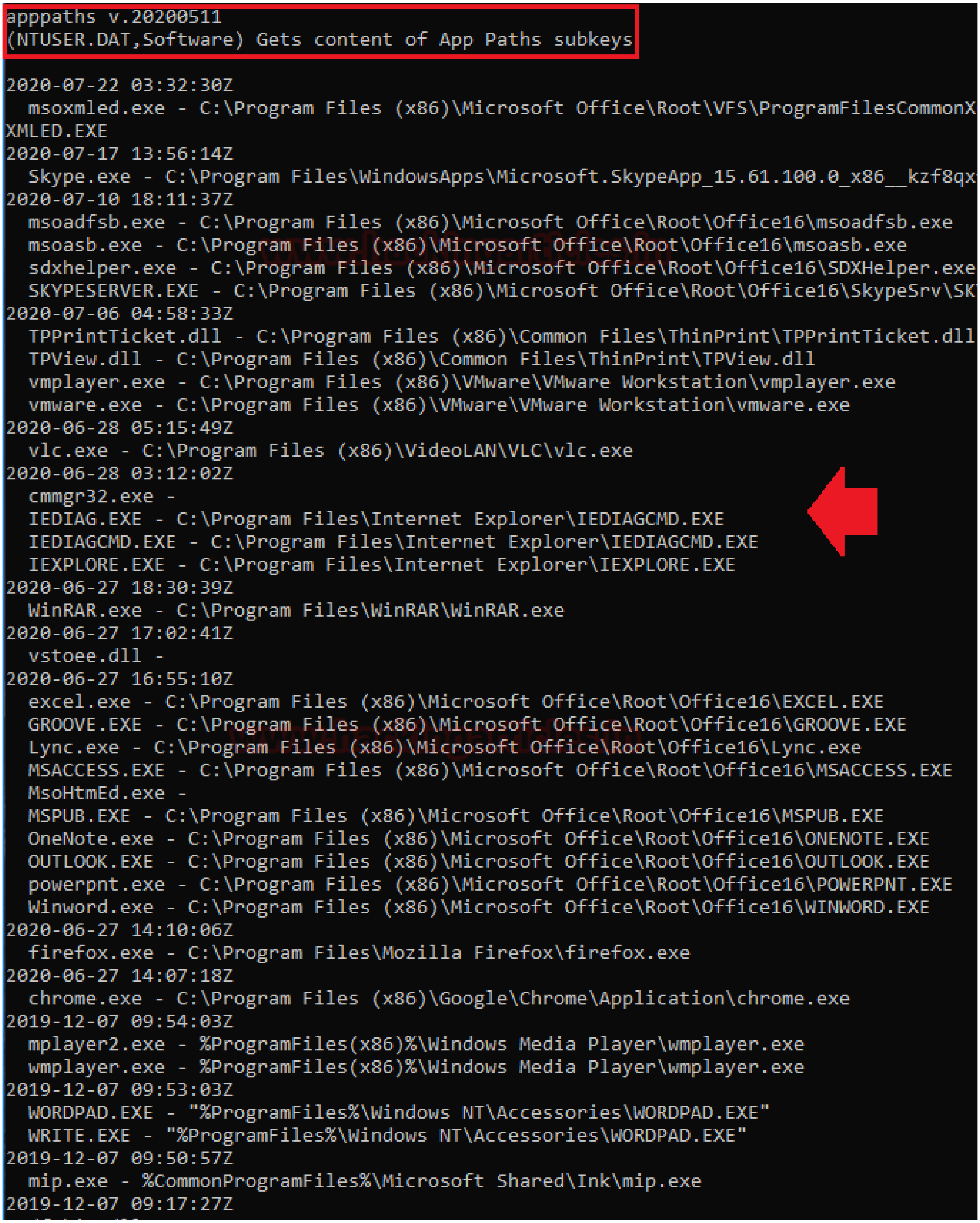
```
type softwarereport.txt
```

In this **report**, the first page shows details regarding AppInit DLLs values. AppInit DLLs is a mechanism that allows an arbitrary list of DLLs to be loaded into each user-mode process on the system.



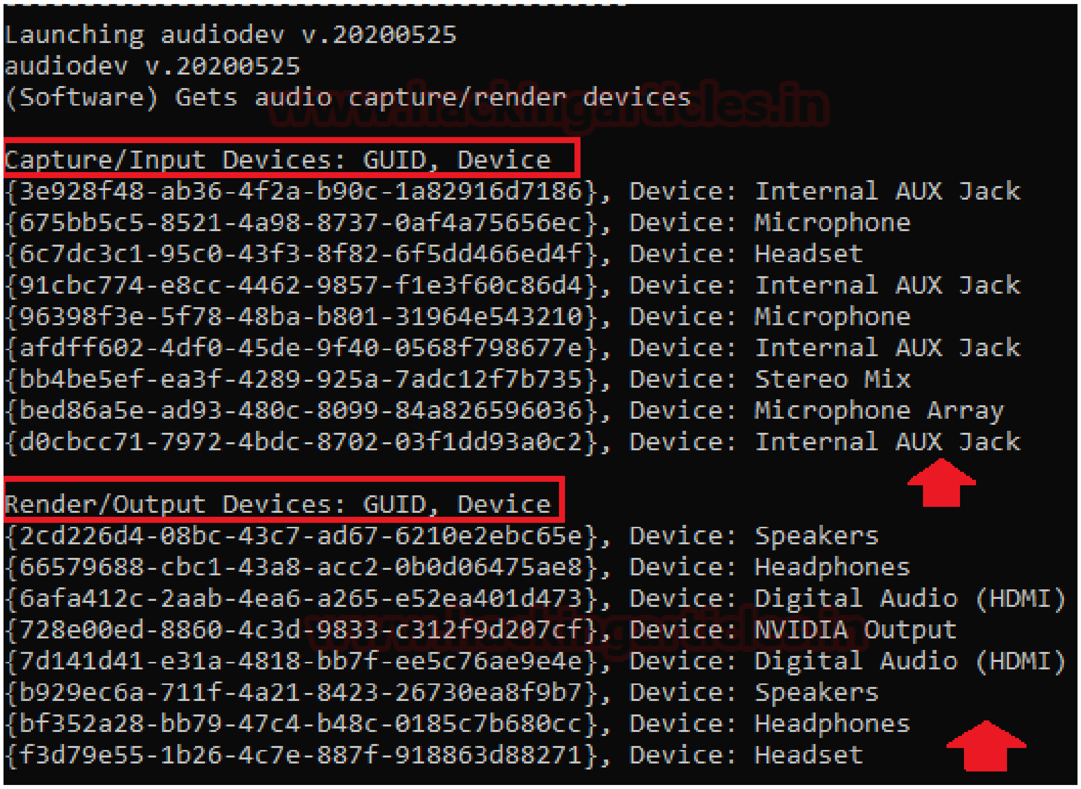
```
C:\Users\SKS19\Desktop>type softwarereport.txt
Hive (C:\software) is not dirty.

allowedenum v.20200511
(NTUSER.DAT, Software) Extracts AllowedEnumeration values to determine hidden special folders

Software\Microsoft\Windows\CurrentVersion\Explorer\AllowedEnumeration not found.
Microsoft\Windows\CurrentVersion\Explorer\AllowedEnumeration not found.
----------------------------------------
appcompatflags v.20200525
(NTUSER.DAT, Software) Extracts AppCompatFlags for Windows.


----------------------------------------
Launching appinitdlls v.20200427
appinitdlls v.20200427
(Software) Gets contents of AppInit_DLLs value

AppInit_DLLs
Microsoft\Windows NT\CurrentVersion\Windows
LastWrite Time 2020-07-18 04:32:08Z
  AppInit_DLLs : {blank}
  LoadAppInit_DLLs : 0
*LoadAppInit_DLLs value globally enables/disables AppInit_DLLS.
0 = disabled (default)

Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows
LastWrite Time 2019-12-07 09:17:27Z
  AppInit_DLLs : {blank}
  LoadAppInit_DLLs : 0
*LoadAppInit_DLLs value globally enables/disables AppInit_DLLS.
0 = disabled (default)

Analysis Tip: The AppInit_DLLs value should be blank; any DLL listed
is launched with each user-mode process.
----------------------------------------
appkeys v.20200517
(NTUSER.DAT, Software) Extracts AppKeys entries.

Microsoft\Windows\CurrentVersion\Explorer\AppKey
Subkey Name: 15  LastWrite: 2019-12-07 09:17:27Z
Subkey Name: 16  LastWrite: 2019-12-07 09:17:27Z
Subkey Name: 17  LastWrite: 2019-12-07 09:17:27Z
Subkey Name: 18  LastWrite: 2019-12-07 09:17:27Z
Subkey Name: 7  LastWrite: 2019-12-07 09:17:27Z
----------------------------------------
```

The next page shows us the details regarding **application details** and the **App Paths subkeys**.



```
apppaths v.20200511
(NTUSER.DAT,Software) Gets content of App Paths subkeys

2020-07-22 03:32:30Z
  msoxmled.exe - C:\Program Files (x86)\Microsoft Office\Root\VFS\ProgramFilesCommonX
XMLED.EXE
2020-07-17 13:56:14Z
  Skype.exe - C:\Program Files\WindowsApps\Microsoft.SkypeApp_15.61.100.0_x86__kzf8qx
2020-07-10 18:11:37Z
  msoadfsb.exe - C:\Program Files (x86)\Microsoft Office\Root\Office16\msoadfsb.exe
  msoasb.exe - C:\Program Files (x86)\Microsoft Office\Root\Office16\msoasb.exe
  sdxhelper.exe - C:\Program Files (x86)\Microsoft Office\Root\Office16\SDXHelper.exe
  SKYPESERVER.EXE - C:\Program Files (x86)\Microsoft Office\Root\Office16\SkypeSrv\SK
2020-07-06 04:58:33Z
  TPPrintTicket.dll - C:\Program Files (x86)\Common Files\ThinPrint\TPPrintTicket.dll
  TPView.dll - C:\Program Files (x86)\Common Files\ThinPrint\TPView.dll
  vmplayer.exe - C:\Program Files (x86)\VMware\VMware Workstation\vmplayer.exe
  vmware.exe - C:\Program Files (x86)\VMware\VMware Workstation\vmware.exe
2020-06-28 05:15:49Z
  vlc.exe - C:\Program Files (x86)\VideoLAN\VLC\vlc.exe
2020-06-28 03:12:02Z
  cmmgr32.exe -
  IEDIAG.EXE - C:\Program Files\Internet Explorer\IEDIAGCMD.EXE
  IEDIAGCMD.EXE - C:\Program Files\Internet Explorer\IEDIAGCMD.EXE
  IEXPLORE.EXE - C:\Program Files\Internet Explorer\IEXPLORE.EXE
2020-06-27 18:30:39Z
  WinRAR.exe - C:\Program Files\WinRAR\WinRAR.exe
2020-06-27 17:02:41Z
  vstoee.dll -
2020-06-27 16:55:10Z
  excel.exe - C:\Program Files (x86)\Microsoft Office\Root\Office16\EXCEL.EXE
  GROOVE.EXE - C:\Program Files (x86)\Microsoft Office\Root\Office16\GROOVE.EXE
  Lync.exe - C:\Program Files (x86)\Microsoft Office\Root\Office16\Lync.exe
  MSACCESS.EXE - C:\Program Files (x86)\Microsoft Office\Root\Office16\MSACCESS.EXE
  MsoHtmEd.exe -
  MSPUB.EXE - C:\Program Files (x86)\Microsoft Office\Root\Office16\MSPUB.EXE
  OneNote.exe - C:\Program Files (x86)\Microsoft Office\Root\Office16\ONENOTE.EXE
  OUTLOOK.EXE - C:\Program Files (x86)\Microsoft Office\Root\Office16\OUTLOOK.EXE
  powerpnt.exe - C:\Program Files (x86)\Microsoft Office\Root\Office16\POWERPNT.EXE
  Winword.exe - C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE
2020-06-27 14:10:06Z
  firefox.exe - C:\Program Files\Mozilla Firefox\firefox.exe
2020-06-27 14:07:18Z
  chrome.exe - C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
2019-12-07 09:54:03Z
  mplayer2.exe - %ProgramFiles(x86)%\Windows Media Player\wmplayer.exe
  wmplayer.exe - %ProgramFiles(x86)%\Windows Media Player\wmplayer.exe
2019-12-07 09:53:03Z
  WORDPAD.EXE - "%ProgramFiles%\Windows NT\Accessories\WORDPAD.EXE"
  WRITE.EXE - "%ProgramFiles%\Windows NT\Accessories\WORDPAD.EXE"
2019-12-07 09:50:57Z
  mip.exe - %CommonProgramFiles%\Microsoft Shared\Ink\mip.exe
2019-12-07 09:17:27Z
```

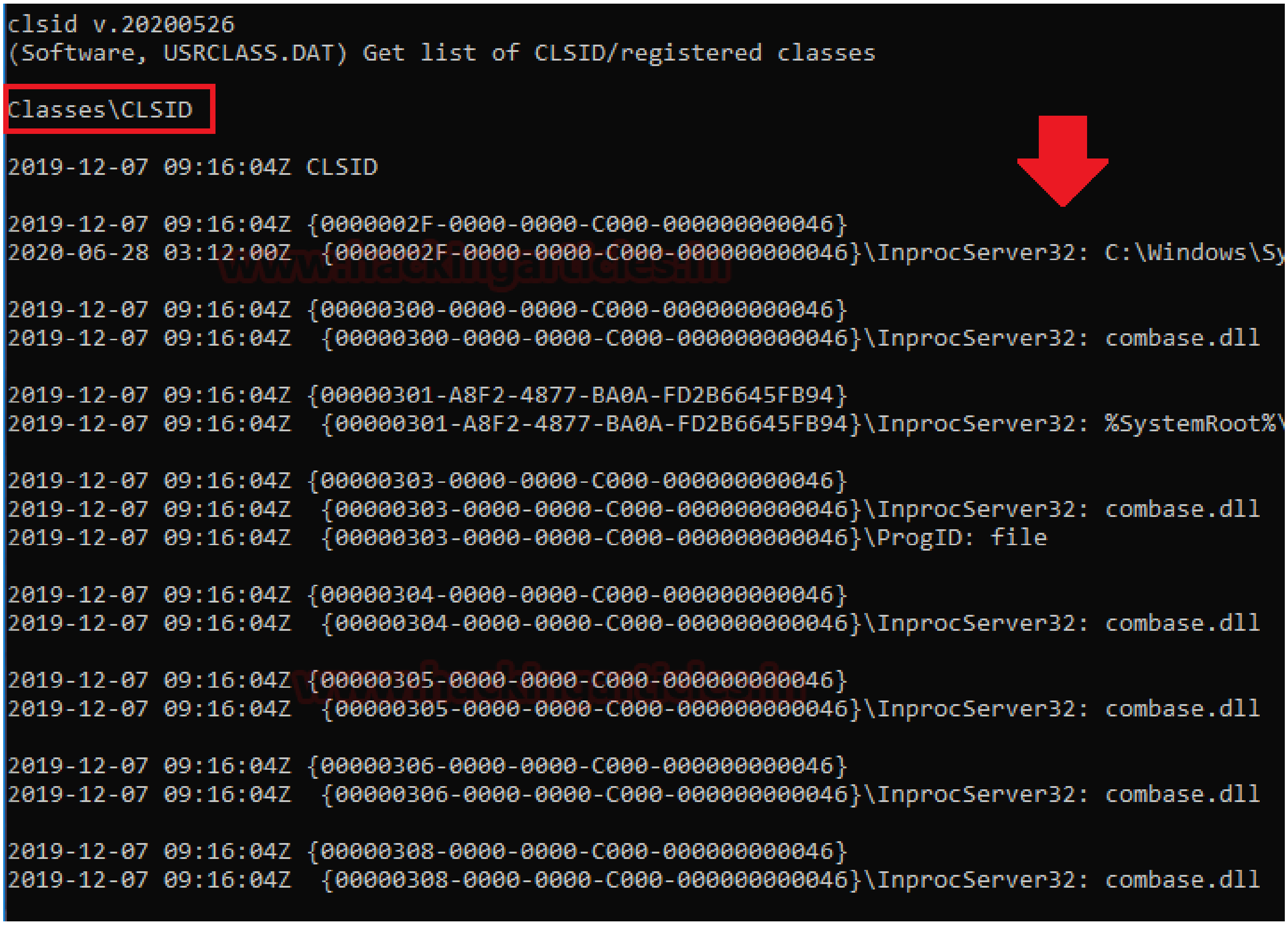
After this, it will showcase all the drivers regarding **Input and output devices** installed in the victim's system. It will show us **Bluetooth driver** details and the system doesn't have a webcam in the system.



```
Launching audiodev v.20200525
audiodev v.20200525
(Software) Gets audio capture/render devices

Capture/Input Devices: GUID, Device
{3e928f48-ab36-4f2a-b90c-1a82916d7186}, Device: Internal AUX Jack
{675bb5c5-8521-4a98-8737-0af4a75656ec}, Device: Microphone
{6c7dc3c1-95c0-43f3-8f82-6f5dd466ed4f}, Device: Headset
{91cbc774-e8cc-4462-9857-f1e3f60c86d4}, Device: Internal AUX Jack
{96398f3e-5f78-48ba-b801-31964e543210}, Device: Microphone
{afdff602-4df0-45de-9f40-0568f798677e}, Device: Internal AUX Jack
{bb4be5ef-ea3f-4289-925a-7adc12f7b735}, Device: Stereo Mix
{bed86a5e-ad93-480c-8099-84a826596036}, Device: Microphone Array
{d0cbcc71-7972-4bdc-8702-03f1dd93a0c2}, Device: Internal AUX Jack

Render/Output Devices: GUID, Device
{2cd226d4-08bc-43c7-ad67-6210e2ebc65e}, Device: Speakers
{66579688-cbc1-43a8-acc2-0b0d06475ae8}, Device: Headphones
{6afa412c-2aab-4ea6-a265-e52ea401d473}, Device: Digital Audio (HDMI)
{728e00ed-8860-4c3d-9833-c312f9d207cf}, Device: NVIDIA Output
{7d141d41-e31a-4818-bb7f-ee5c76ae9e4e}, Device: Digital Audio (HDMI)
{b929ec6a-711f-4a21-8423-26730ea8f9b7}, Device: Speakers
{bf352a28-bb79-47c4-b48c-0185c7b680cc}, Device: Headphones
{f3d79e55-1b26-4c7e-887f-918863d88271}, Device: Headset
```

Last page of this report regarding the **CLSID** key. Where CLSID is a globally unique identifier that identifies a COM class object. If your server or container allows linking to its embedded objects, you need to register a CLSID for each supported class of objects.

The CLSID key contains information used by the default COM handler to return information about a class when it is running. The CLSID is a 128-bit number, in hex, within a pair of curly braces.

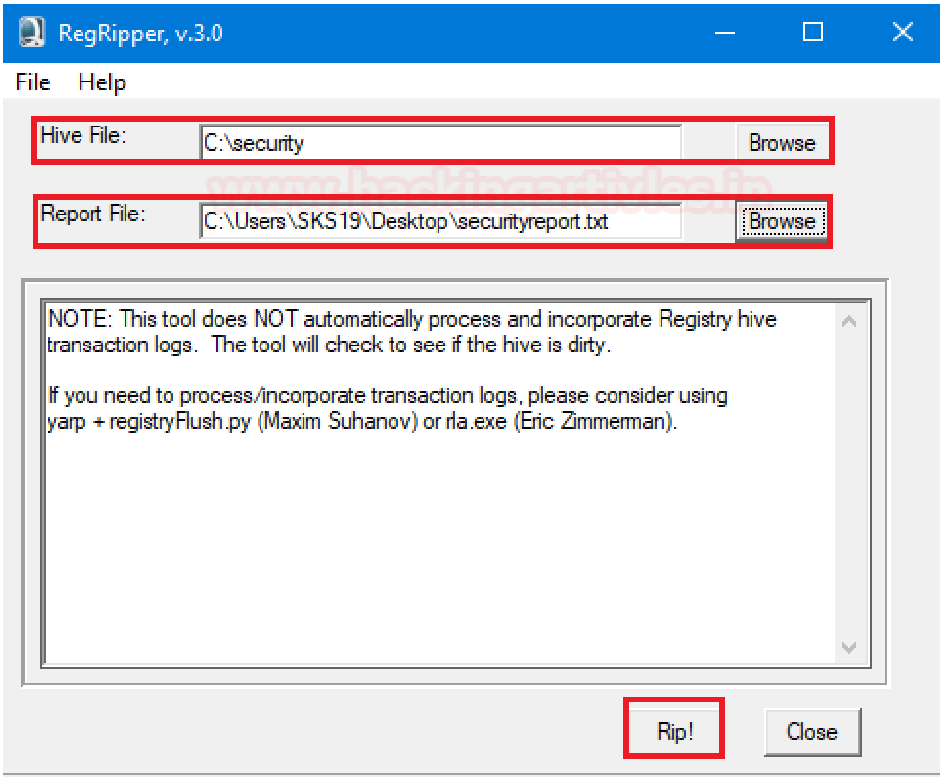


```
clsid v.20200526
(Software, USRCLASS.DAT) Get list of CLSID/registered classes

Classes\CLSID

2019-12-07 09:16:04Z CLSID

2019-12-07 09:16:04Z {0000002F-0000-0000-C000-000000000046}
2020-06-28 03:12:00Z  {0000002F-0000-0000-C000-000000000046}\InprocServer32: C:\Windows\Sy

2019-12-07 09:16:04Z {00000300-0000-0000-C000-000000000046}
2019-12-07 09:16:04Z  {00000300-0000-0000-C000-000000000046}\InprocServer32: combase.dll

2019-12-07 09:16:04Z {00000301-A8F2-4877-BA0A-FD2B6645FB94}
2019-12-07 09:16:04Z  {00000301-A8F2-4877-BA0A-FD2B6645FB94}\InprocServer32: %SystemRoot%\

2019-12-07 09:16:04Z {00000303-0000-0000-C000-000000000046}
2019-12-07 09:16:04Z  {00000303-0000-0000-C000-000000000046}\InprocServer32: combase.dll
2019-12-07 09:16:04Z  {00000303-0000-0000-C000-000000000046}\ProgID: file

2019-12-07 09:16:04Z {00000304-0000-0000-C000-000000000046}
2019-12-07 09:16:04Z  {00000304-0000-0000-C000-000000000046}\InprocServer32: combase.dll

2019-12-07 09:16:04Z {00000305-0000-0000-C000-000000000046}
2019-12-07 09:16:04Z  {00000305-0000-0000-C000-000000000046}\InprocServer32: combase.dll

2019-12-07 09:16:04Z {00000306-0000-0000-C000-000000000046}
2019-12-07 09:16:04Z  {00000306-0000-0000-C000-000000000046}\InprocServer32: combase.dll

2019-12-07 09:16:04Z {00000308-0000-0000-C000-000000000046}
2019-12-07 09:16:04Z  {00000308-0000-0000-C000-000000000046}\InprocServer32: combase.dll
```

Security Hive

Security hive helps us to understand the security measures of the victim's system in the Forensic Investigation process.

Now, follow the previous steps for RegRipper and select the location of the **Hive file** and **Report file**. Then click on the **Rip**! Button to start the Investigation process.

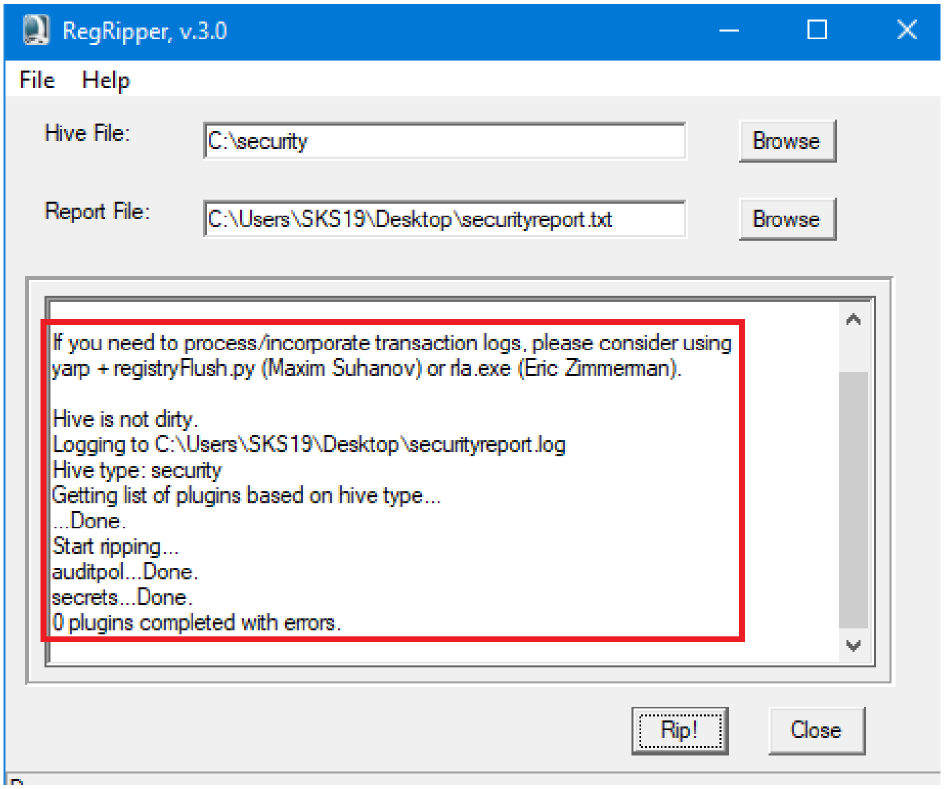


Hive File: C:\security

Report File: C:\Users\SKS19\Desktop\securityreport.txt

```
NOTE: This tool does NOT automatically process and incorporate Registry hive
transaction logs.  The tool will check to see if the hive is dirty.

If you need to process/incorporate transaction logs, please consider using
yarp + registryFlush.py (Maxim Suhanov) or rla.exe (Eric Zimmerman).
```

After some time, it will showcase the message on the screen that our work for this investigation process is completed with zero plugins completed with errors.



Hive File: C:\security

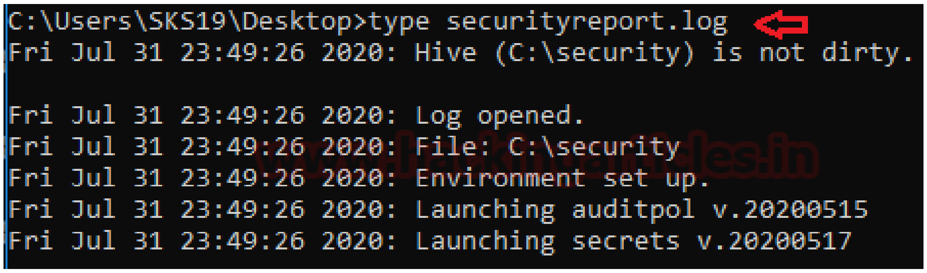
Report File: C:\Users\SKS19\Desktop\securityreport.txt

```
If you need to process/incorporate transaction logs, please consider using
yarp + registryFlush.py (Maxim Suhanov) or rla.exe (Eric Zimmerman).

Hive is not dirty.
Logging to C:\Users\SKS19\Desktop\securityreport.log
Hive type: security
Getting list of plugins based on hive type...
...Done.
Start ripping...
auditpol...Done.
secrets...Done.
0 plugins completed with errors.
```

Analyzing Log: Security

Now we checked its **log file** to deeply understand our Investigation report. Run these commands to view the log file in the command prompt.

```
type securityreport.log
```



```
C:\Users\SKS19\Desktop>type securityreport.log
Fri Jul 31 23:49:26 2020: Hive (C:\security) is not dirty.

Fri Jul 31 23:49:26 2020: Log opened.
Fri Jul 31 23:49:26 2020: File: C:\security
Fri Jul 31 23:49:26 2020: Environment set up.
Fri Jul 31 23:49:26 2020: Launching auditpol v.20200515
Fri Jul 31 23:49:26 2020: Launching secrets v.20200517
```

Analyzing Report: Security

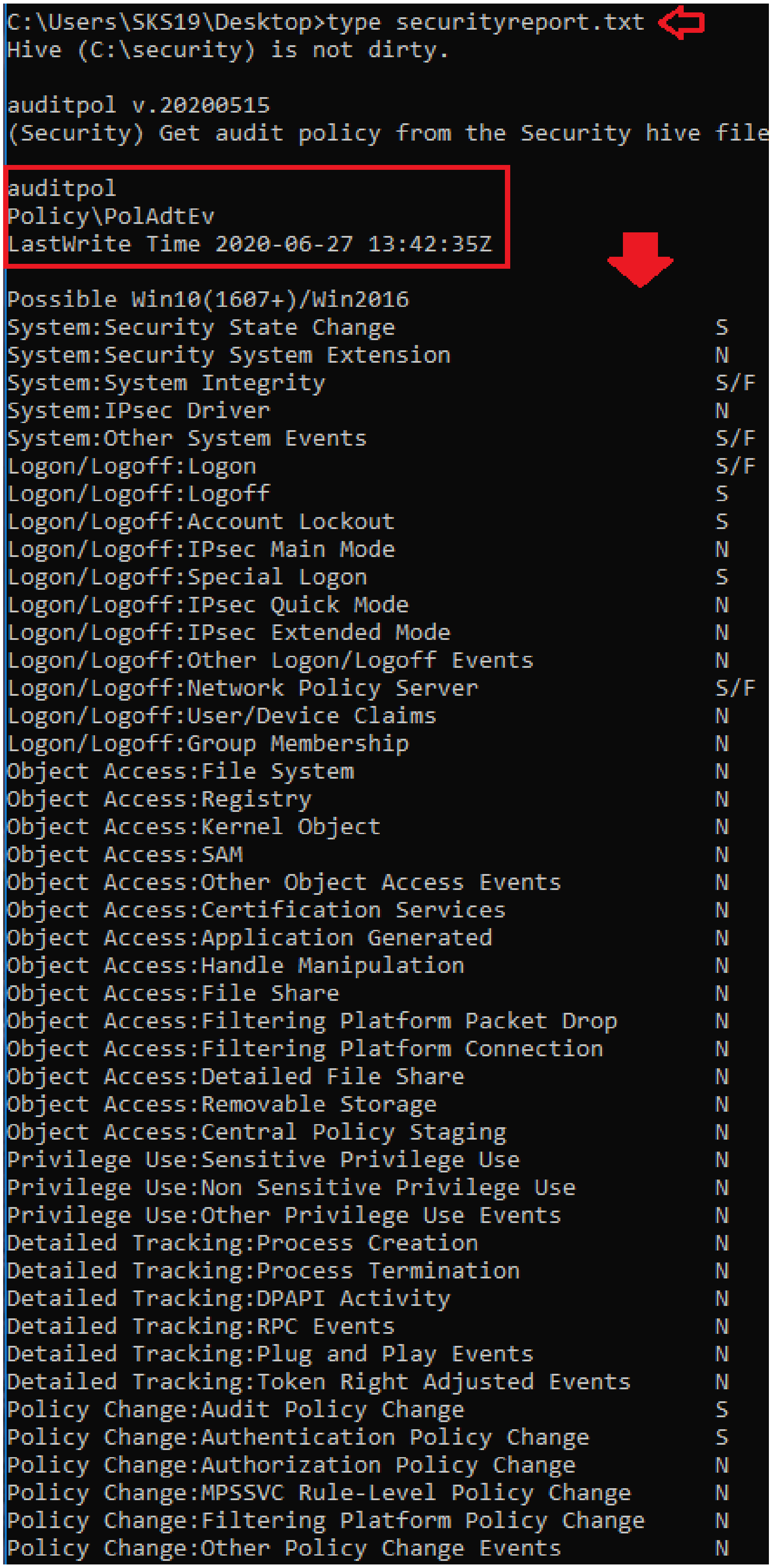
To view, the security hive file **report** follows this command.

```
type securityreport.txt
```

This report page is all about the security hive file audit policy. An audit policy specifies account limits of one or multiple resources for a group of users.

This contains guidelines that establish policy limitations and workflows for processing breaches after they occur.

Where **N** means No audit, **S** means Success, and **F** means failure.



```
C:\Users\SKS19\Desktop>type securityreport.txt
Hive (C:\security) is not dirty.

auditpol v.20200515
(Security) Get audit policy from the Security hive file

auditpol
Policy\PolAdtEv
LastWrite Time 2020-06-27 13:42:35Z

Possible Win10(1607+)/Win2016
System:Security State Change                       S
System:Security System Extension                   N
System:System Integrity                            S/F
System:IPsec Driver                                N
System:Other System Events                         S/F
Logon/Logoff:Logon                                 S/F
Logon/Logoff:Logoff                                S
Logon/Logoff:Account Lockout                       S
Logon/Logoff:IPsec Main Mode                       N
Logon/Logoff:Special Logon                         S
Logon/Logoff:IPsec Quick Mode                      N
Logon/Logoff:IPsec Extended Mode                   N
Logon/Logoff:Other Logon/Logoff Events             N
Logon/Logoff:Network Policy Server                 S/F
Logon/Logoff:User/Device Claims                    N
Logon/Logoff:Group Membership                      N
Object Access:File System                          N
Object Access:Registry                             N
Object Access:Kernel Object                        N
Object Access:SAM                                  N
Object Access:Other Object Access Events           N
Object Access:Certification Services               N
Object Access:Application Generated                N
Object Access:Handle Manipulation                  N
Object Access:File Share                           N
Object Access:Filtering Platform Packet Drop       N
Object Access:Filtering Platform Connection        N
Object Access:Detailed File Share                  N
Object Access:Removable Storage                    N
Object Access:Central Policy Staging               N
Privilege Use:Sensitive Privilege Use              N
Privilege Use:Non Sensitive Privilege Use          N
Privilege Use:Other Privilege Use Events           N
Detailed Tracking:Process Creation                 N
Detailed Tracking:Process Termination              N
Detailed Tracking:DPAPI Activity                   N
Detailed Tracking:RPC Events                       N
Detailed Tracking:Plug and Play Events             N
Detailed Tracking:Token Right Adjusted Events      N
Policy Change:Audit Policy Change                  S
Policy Change:Authentication Policy Change         S
Policy Change:Authorization Policy Change          N
Policy Change:MPSSVC Rule-Level Policy Change      N
Policy Change:Filtering Platform Policy Change     N
Policy Change:Other Policy Change Events           N
```

Conclusion

The Windows Registry is a hierarchical database that stores low-level settings for the operating system of Microsoft Windows and for programs choosing to use the registry. The register also offers access to counters for results in profiling systems. In other terms, on all models of Microsoft Windows operating systems, the registry or Windows registry contains information, settings, options, and other values for programs and hardware installed.

These details can be extracted with RegRipper to get a better result in the Forensic Investigation.