

Forensic Investigation: Extract Volatile Data (Manually)

July 5, 2020 By Raj Chandel

In this article, we will run a couple of CLI commands that help a forensic investigator to gather volatile data from the system as much as possible. The commands which we use in this post are not the whole list of commands, but these are most commonly used once.

As per forensic investigator, create a folder on the desktop name “case” and inside create another subfolder named as “case01” and then use an empty document “volatile.txt” to save the output which you will extract.

Here I have saved all the output inside /SKS19/prac/notes.txt which help us creating an investigation report.

Table of Content

- **What is Volatile Data?**
- **System Information**
- **Currently available network connections**
- **Routing Configuration**
- **Date and Time**
- **System Variables**
- **Task List**
- **Task List with Modules**
- **Task List with Service**
- **Workstation Information**
- **MAC Address save in system ARP Cache**
- **System User Details**
- **DNS configuration**
- **System network shares**
- **Network configuration**

What is Volatile Data?

There are two types of data collected in Computer Forensics Persistent data and Volatile data. Persistent data is that data that is stored on a local hard drive and it is preserved when the computer is OFF. Volatile data is any kind of data that is stored in memory, which will be lost when computer power or OFF.

Volatile data resides in the registry’s cache and random access memory (RAM). This investigation of the volatile data is called “live forensics”.

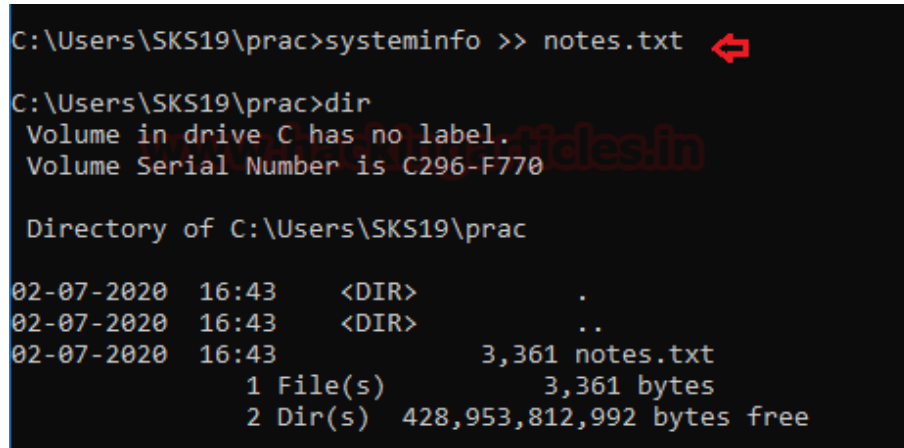
System Information

It is a system profiler included with Microsoft Windows that displays diagnostic and troubleshooting information related to the operating system, hardware, and software.

We can collect this volatile data with the help of commands. All we need is to type this command.

```
systeminfo >> notes.txt
```

It will save all the data in this text file. We check whether this file is created or not by [dir] command to compare the size of the file each time after executing every command.

A screenshot of a Windows command prompt window. The background is black, and the text is white. The prompt shows the user's location as C:\Users\SKS19\prac. The first command entered is 'systeminfo >> notes.txt', followed by a red arrow pointing to the right. The second command is 'dir'. The output of 'dir' shows the directory contents of C:\Users\SKS19\prac, including a file named 'notes.txt' with a size of 3,361 bytes. The output also shows the volume information for drive C, indicating it has no label and a serial number of C296-F770.

```
C:\Users\SKS19\prac>systeminfo >> notes.txt  
C:\Users\SKS19\prac>dir  
Volume in drive C has no label.  
Volume Serial Number is C296-F770  
  
Directory of C:\Users\SKS19\prac  
  
02-07-2020  16:43    <DIR>          .  
02-07-2020  16:43    <DIR>          ..  
02-07-2020  16:43                3,361 notes.txt  
               1 File(s)                3,361 bytes  
               2 Dir(s)  428,953,812,992 bytes free
```

Now, go to this location to see the results of this command. Where it will show all the system information about our system software and hardware.

```
notes - Notepad
File Edit Format View Help

Host Name:                DESKTOP-QSBQ20A
OS Name:                  Microsoft Windows 10 Pro
OS Version:               10.0.19041 N/A Build 19041
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:         SKS1997.SK@outlook.com
Registered Organization:
Product ID:                00331-10000-00001-AA187
Original Install Date:     27-06-2020, 19:14:02
System Boot Time:          01-07-2020, 19:57:26
System Manufacturer:       ASUSTeK COMPUTER INC.
System Model:              ROG Strix G731GT_G731GT
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 158 Stepping 13 GenuineIntel ~2592 Mhz
BIOS Version:              American Megatrends Inc. G731GT.306, 11-03-2020
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume3
System Locale:              en-us;English (United States)
Input Locale:              00004009
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     16,236 MB
Available Physical Memory: 9,942 MB
Virtual Memory: Max Size:  19,180 MB
Virtual Memory: Available: 10,736 MB
Virtual Memory: In Use:    8,444 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\DESKTOP-QSBQ20A
Hotfix(s):                 6 Hotfix(s) Installed.
                           [01]: KB4552925
                           [02]: KB4537759
                           [03]: KB4557968
                           [04]: KB4560366
                           [05]: KB4561600
                           [06]: KB4557957
Network Card(s):           4 NIC(s) Installed.
                           [01]: Intel(R) Wireless-AC 9560 160MHz
                               Connection Name: Wi-Fi
                               DHCP Enabled:    Yes
```

Currently Available Network Connections

Network connectivity describes the extensive process of connecting various parts of a network. With the help of routers, switches, and gateways.

We can check all the currently available network connections through the command line.

```
netstat -nao >> notes.txt
```

we can check whether it is created or not with the help of [dir] command as you can see, now the size of the get increased.

```
C:\Users\SKS19\prac>netstat -nao >> notes.txt ↵
C:\Users\SKS19\prac>dir
Volume in drive C has no label.
Volume Serial Number is C296-F770

Directory of C:\Users\SKS19\prac

02-07-2020  16:26    <DIR>          .
02-07-2020  16:26    <DIR>          ..
02-07-2020  16:26                11,771 notes.txt
               1 File(s)              11,771 bytes
               2 Dir(s)  428,961,267,712 bytes free

C:\Users\SKS19\prac>
```

Now, open that text file to see all active connections in the system right now. It will also provide us with some extra details like state, PID, address, protocol.

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	1244
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING	6544
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:7680	0.0.0.0:0	LISTENING	3692
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	1008
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	880
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	1736
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING	1792
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	3960
TCP	0.0.0.0:49670	0.0.0.0:0	LISTENING	992
TCP	127.0.0.1:5939	0.0.0.0:0	LISTENING	9636
TCP	127.0.0.1:5939	127.0.0.1:49379	ESTABLISHED	9636
TCP	127.0.0.1:5939	127.0.0.1:65464	ESTABLISHED	9636
TCP	127.0.0.1:43058	0.0.0.0:0	LISTENING	9008
TCP	127.0.0.1:49306	127.0.0.1:49307	ESTABLISHED	16764
TCP	127.0.0.1:49307	127.0.0.1:49306	ESTABLISHED	16764
TCP	127.0.0.1:49379	127.0.0.1:5939	ESTABLISHED	18912
TCP	127.0.0.1:59523	127.0.0.1:59524	ESTABLISHED	3552
TCP	127.0.0.1:59524	127.0.0.1:59523	ESTABLISHED	3552
TCP	127.0.0.1:59527	127.0.0.1:59528	ESTABLISHED	7680
TCP	127.0.0.1:59528	127.0.0.1:59527	ESTABLISHED	7680
TCP	127.0.0.1:59534	127.0.0.1:59535	ESTABLISHED	1892
TCP	127.0.0.1:59535	127.0.0.1:59534	ESTABLISHED	1892
TCP	127.0.0.1:61220	127.0.0.1:61221	ESTABLISHED	9008
TCP	127.0.0.1:61221	127.0.0.1:61220	ESTABLISHED	9008
TCP	127.0.0.1:64588	127.0.0.1:64589	ESTABLISHED	9636
TCP	127.0.0.1:64589	127.0.0.1:64588	ESTABLISHED	9636
TCP	127.0.0.1:64899	127.0.0.1:64900	ESTABLISHED	9280
TCP	127.0.0.1:64900	127.0.0.1:64899	ESTABLISHED	9280
TCP	127.0.0.1:65378	127.0.0.1:65379	ESTABLISHED	9572
TCP	127.0.0.1:65379	127.0.0.1:65378	ESTABLISHED	9572
TCP	127.0.0.1:65464	127.0.0.1:5939	ESTABLISHED	37504
TCP	127.0.0.1:65517	127.0.0.1:65518	ESTABLISHED	37504
TCP	127.0.0.1:65518	127.0.0.1:65517	ESTABLISHED	37504
TCP	192.168.0.6:139	0.0.0.0:0	LISTENING	4
TCP	192.168.0.6:43058	0.0.0.0:0	LISTENING	9008
TCP	192.168.0.6:43058	157.140.100.60:443	ESTABLISHED	30634

Routing Configuration

It specifies the correct IP addresses and router settings. Host configuration: sets up a network connection on a host computer or laptop by logging the default network settings, such as IP address, proxy, network name, and ID/password.

To know the Router configuration in our network follows this command.

```
route print >> notes.txt
```

We can check the file with [dir] command.

```
C:\Users\SKS19\prac>route print >> notes.txt ↵  
C:\Users\SKS19\prac>dir  
Volume in drive C has no label.  
Volume Serial Number is C296-F770  
  
Directory of C:\Users\SKS19\prac  
02-07-2020 16:32 <DIR> .  
02-07-2020 16:32 <DIR> ..  
02-07-2020 16:32      2,942 notes.txt  
               1 File(s)      2,942 bytes  
               2 Dir(s)  428,959,805,440 bytes free  
  
C:\Users\SKS19\prac>
```

Open the txt file to evaluate the results of this command. Like the Router table and its settings.

Interface List

```

5...04 d4 c4 e9 52 69 .....Realtek PCIe GbE Family Controller
14...0a 00 27 00 00 0e .....VirtualBox Host-Only Ethernet Adapter
4...94 e6 f7 78 31 b6 .....Microsoft Wi-Fi Direct Virtual Adapter
9...96 e6 f7 78 31 b5 .....Microsoft Wi-Fi Direct Virtual Adapter #2
10...94 e6 f7 78 31 b5 .....Intel(R) Wireless-AC 9560 160MHz
18...94 e6 f7 78 31 b9 .....Bluetooth Device (Personal Area Network)
1.....Software Loopback Interface 1

```

IPv4 Route Table

Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0		192.168.0.1	192.168.0.6	60
127.0.0.0	255.0.0.0		On-link	127.0.0.1	331
127.0.0.1	255.255.255.255		On-link	127.0.0.1	331
127.255.255.255	255.255.255.255		On-link	127.0.0.1	331
192.168.0.0	255.255.255.0		On-link	192.168.0.6	316
192.168.0.6	255.255.255.255		On-link	192.168.0.6	316
192.168.0.255	255.255.255.255		On-link	192.168.0.6	316
192.168.56.0	255.255.255.0		On-link	192.168.56.1	281
192.168.56.1	255.255.255.255		On-link	192.168.56.1	281
192.168.56.255	255.255.255.255		On-link	192.168.56.1	281
224.0.0.0	240.0.0.0		On-link	127.0.0.1	331
224.0.0.0	240.0.0.0		On-link	192.168.56.1	281
224.0.0.0	240.0.0.0		On-link	192.168.0.6	316
255.255.255.255	255.255.255.255		On-link	127.0.0.1	331
255.255.255.255	255.255.255.255		On-link	192.168.56.1	281
255.255.255.255	255.255.255.255		On-link	192.168.0.6	316

Persistent Routes:

None

IPv6 Route Table

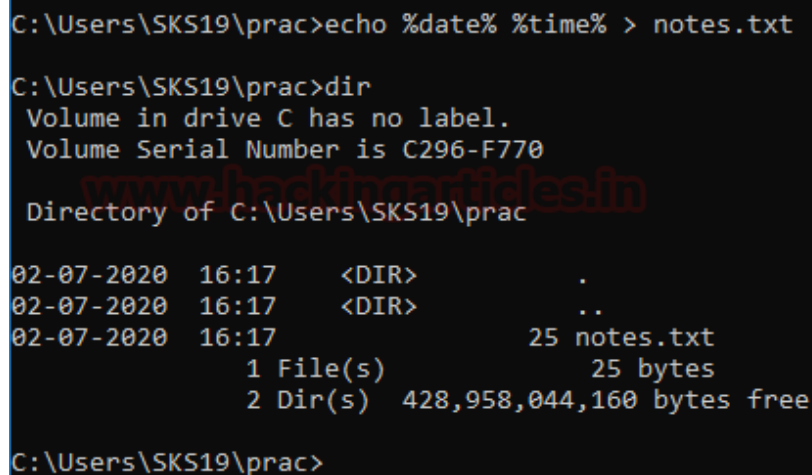
Active Routes:

If	Metric	Network	Destination	Gateway
10	316	::/0		fe80::1e5f:2bff:fe59:e124
1	331	::1/128		On-link
14	281	fe80::/64		On-link
10	316	fe80::/64		On-link

Date and Time

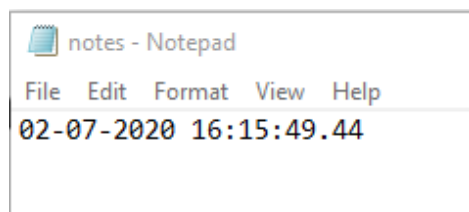
To know the date and time of the system we can follow this command. We can also check the file is created or not with the help of [dir] command.

```
echo %date% %time% > notes.txt  
dir
```



```
C:\Users\SKS19\prac>echo %date% %time% > notes.txt  
C:\Users\SKS19\prac>dir  
Volume in drive C has no label.  
Volume Serial Number is C296-F770  
Directory of C:\Users\SKS19\prac  
  
02-07-2020  16:17    <DIR>          .  
02-07-2020  16:17    <DIR>          ..  
02-07-2020  16:17                25 notes.txt  
               1 File(s)                25 bytes  
               2 Dir(s)  428,958,044,160 bytes free  
  
C:\Users\SKS19\prac>
```

Open that file to see the data gathered with the command.



System Variables

A System variable is a dynamic named value that can affect the way running processes will behave on the computer. They are part of the system in which processes are running. For Example, a running process can query the value of the TEMP environment variable to discover a suitable location to store temporary files.

We can check all system variable set in a system with a single command.

```
set >> notes.txt
```

We can check whether the file is created or not with [dir] command.

```
dir
```



```

C:\Users\SKS19\prac>set >> notes.txt
C:\Users\SKS19\prac>dir
Volume in drive C has no label.
Volume Serial Number is C296-F770

Directory of C:\Users\SKS19\prac

02-07-2020  16:34    <DIR>          .
02-07-2020  16:34    <DIR>          ..
02-07-2020  16:34                1,671 notes.txt
               1 File(s)                1,671 bytes
               2 Dir(s)  428,956,356,608 bytes free

C:\Users\SKS19\prac>_

```

Now, open the text file to see set system variables in the system.

```

notes - Notepad
File Edit Format View Help
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Users\SKS19\AppData\Roaming
CommonProgramFiles=C:\Program Files\Common Files
CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
CommonProgramW6432=C:\Program Files\Common Files
COMPUTERNAME=DESKTOP-QSBQ20A
ComSpec=C:\Windows\system32\cmd.exe
DriverData=C:\Windows\System32\Drivers\DriverData
HOMEDRIVE=C:
HOMEPATH=\Users\SKS19
LOCALAPPDATA=C:\Users\SKS19\AppData\Local
LOGONSERVER=\\DESKTOP-QSBQ20A
NUMBER_OF_PROCESSORS=12
OneDrive=C:\Users\SKS19\OneDrive
OneDriveConsumer=C:\Users\SKS19\OneDrive
OS=Windows_NT
Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Win
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE=AMD64
PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 158 Stepping 13, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=9e0d
ProgramData=C:\ProgramData
ProgramFiles=C:\Program Files
ProgramFiles(x86)=C:\Program Files (x86)
ProgramW6432=C:\Program Files
PROMPT=$P$G
PSModulePath=C:\Program Files\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules
PUBLIC=C:\Users\Public
SESSIONNAME=Console
SystemDrive=C:
SystemRoot=C:\Windows
TEMP=C:\Users\SKS19\AppData\Local\Temp
TMP=C:\Users\SKS19\AppData\Local\Temp
USERDOMAIN=DESKTOP-QSBQ20A
USERDOMAIN_ROAMINGPROFILE=DESKTOP-QSBQ20A
USERNAME=SKS19
USERPROFILE=C:\Users\SKS19
VBOX_MSI_INSTALL_PATH=C:\Program Files\Oracle\VirtualBox\
windir=C:\Windows

```

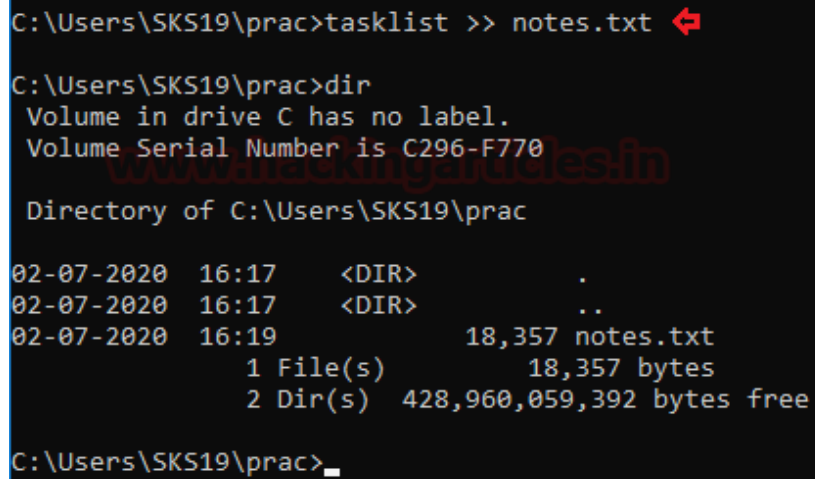
Task List

A Task list is a menu that appears in Microsoft Windows, It will provide a list of running applications in the system.

To get the task list of the system along with its process id and memory usage follow this command.

```
tasklist >> notes.txt
```

we can also check whether the text file is created or not with [dir] command.



```
C:\Users\SKS19\prac>tasklist >> notes.txt ↵
C:\Users\SKS19\prac>dir
Volume in drive C has no label.
Volume Serial Number is C296-F770

Directory of C:\Users\SKS19\prac

02-07-2020  16:17    <DIR>          .
02-07-2020  16:17    <DIR>          ..
02-07-2020  16:19                18,357 notes.txt
               1 File(s)                18,357 bytes
               2 Dir(s)  428,960,059,392 bytes free

C:\Users\SKS19\prac>_
```

Open the text file to evaluate the details.

notes - Notepad				
File Edit Format View Help				
Image Name	PID	Session Name	Session#	Mem Usage
=====	=====	=====	=====	=====
System Idle Process	0	Services	0	8 K
System	4	Services	0	1,048 K
Registry	148	Services	0	63,672 K
smss.exe	500	Services	0	1,232 K
csrss.exe	768	Services	0	5,616 K
wininit.exe	880	Services	0	6,868 K
services.exe	992	Services	0	11,136 K
lsass.exe	1008	Services	0	24,936 K
svchost.exe	1048	Services	0	3,104 K
svchost.exe	1080	Services	0	28,756 K
fontdrvhost.exe	1112	Services	0	4,420 K
WUDFHost.exe	1168	Services	0	17,124 K
svchost.exe	1244	Services	0	17,600 K
svchost.exe	1288	Services	0	8,456 K
svchost.exe	1540	Services	0	8,392 K
svchost.exe	1572	Services	0	9,512 K
svchost.exe	1588	Services	0	11,008 K
svchost.exe	1736	Services	0	17,640 K
svchost.exe	1792	Services	0	14,028 K
svchost.exe	1800	Services	0	12,576 K
svchost.exe	1808	Services	0	10,076 K
svchost.exe	1816	Services	0	8,056 K
svchost.exe	1968	Services	0	8,264 K
svchost.exe	2016	Services	0	12,776 K
svchost.exe	2024	Services	0	5,896 K
svchost.exe	2032	Services	0	7,360 K
svchost.exe	672	Services	0	10,488 K
svchost.exe	2112	Services	0	7,196 K
svchost.exe	2168	Services	0	7,312 K
svchost.exe	2180	Services	0	5,924 K
svchost.exe	2284	Services	0	8,020 K
igfxCUIService.exe	2396	Services	0	7,944 K
svchost.exe	2404	Services	0	9,836 K
svchost.exe	2492	Services	0	12,340 K
NVDisplay.Container.exe	2640	Services	0	11,012 K
svchost.exe	2676	Services	0	7,500 K
svchost.exe	2708	Services	0	9,700 K
dasHost.exe	2812	Services	0	18.024 K

Task List with Modules

With the help of task list modules, we can see the working of modules in terms of the particular task. We can see that results in our investigation with the help of the following command.

```
tasklist /m >> notes.txt
```

```
C:\Users\SKS19\prac>tasklist /m >> notes.txt ↵  
C:\Users\SKS19\prac>dir  
Volume in drive C has no label.  
Volume Serial Number is C296-F770  
  
Directory of C:\Users\SKS19\prac  
  
02-07-2020  16:22    <DIR>          .  
02-07-2020  16:22    <DIR>          ..  
02-07-2020  16:22                242,678 notes.txt  
               1 File(s)                242,678 bytes  
               2 Dir(s)  428,963,270,656 bytes free  
  
C:\Users\SKS19\prac>
```

we can check whether our result file is created or not with the help of [dir] command.

Open the text file to evaluate the command results.

```

NVDisplay.Container.exe          7344 N/A
AsusOptimizationStartupTa      12756 ntdll.dll, KERNEL32.DLL, KERNELBASE.dll,
                                     combase.dll, ucrtbase.dll, RPCRT4.dll,
                                     cfgmgr32.dll, kernel.appcore.dll,
                                     msvcrt.dll, HID.DLL, user32.dll,
                                     win32u.dll, GDI32.dll, gdi32full.dll,
                                     msvcp_win.dll, IMM32.DLL, uxtheme.dll,
                                     MSCTF.dll, OLEAUT32.dll, sechost.dll,
                                     Wtsapi32.dll, WINSTA.dll, powrprof.dll,
                                     UMPDC.dll, tv_x64.dll, SHELL32.dll,
                                     ole32.dll, VERSION.dll
sihost.exe                      11408 ntdll.dll, KERNEL32.DLL, KERNELBASE.dll,
                                     msvcp_win.dll, ucrtbase.dll, combase.dll,
                                     RPCRT4.dll, sechost.dll, advapi32.dll,
                                     msvcrt.dll, CoreMessaging.dll, WS2_32.dll,
                                     ntmarta.dll, kernel.appcore.dll,
                                     bcryptPrimitives.dll, user32.dll,
                                     win32u.dll, GDI32.dll, gdi32full.dll,
                                     IMM32.DLL, clbcatq.dll,
                                     desktopshellex.dll, shcore.dll,
                                     shlwapi.dll, wtsapi32.dll, WINSTA.dll,
                                     Windows.Shell.ServiceHostBuilder.dll,
                                     OneCoreUAPCommonProxyStub.dll, uxtheme.dll,
                                     ClipboardServer.dll, RMCLIENT.dll,
                                     activationmanager.dll, OLEAUT32.dll,
                                     AppXDeploymentClient.dll, wintypes.dll,
                                     MPR.dll, profapi.dll, twinapi.appcore.dll,
                                     AppointmentActivation.dll,
                                     windows.staterepositorycore.dll,
                                     modernexecserver.dll, usermgrproxy.dll,
                                     usermgrcli.dll, CoreUIComponents.dll,
                                     ExecModelClient.dll, PROPSYS.dll,
                                     windowmanagement.dll,
                                     OneCoreCommonProxyStub.dll,
                                     execmodelproxy.dll,

```

Task List with Services

It will showcase all the services taken by a particular task to operate its action. We get these results in our Forensic report by using this command.

```
tasklist /svc >> notes.txt
```

we check whether the text file is created or not with the help [dir] command.

```
C:\Users\SKS19\prac>tasklist /svc >> notes.txt ↩️  
  
C:\Users\SKS19\prac>dir  
Volume in drive C has no label.  
Volume Serial Number is C296-F770  
  
Directory of C:\Users\SKS19\prac  
02-07-2020  16:24    <DIR>          .  
02-07-2020  16:24    <DIR>          ..  
02-07-2020  16:24                19,199 notes.txt  
               1 File(s)              19,199 bytes  
               2 Dir(s)  428,963,123,200 bytes free  
  
C:\Users\SKS19\prac>
```

Open this text file to evaluate the results. It will showcase the services used by each task.

notes - Notepad		
File Edit Format View Help		
Image Name	PID	Services
=====		
System Idle Process	0	N/A
System	4	N/A
Registry	148	N/A
smss.exe	500	N/A
csrss.exe	768	N/A
wininit.exe	880	N/A
services.exe	992	N/A
lsass.exe	1008	EFS, KeyIso, SamSs, VaultSvc
svchost.exe	1048	PlugPlay
svchost.exe	1080	BrokerInfrastructure, DcomLaunch, Power, SystemEventsBroker
fontdrvhost.exe	1112	N/A
WUDFHost.exe	1168	N/A
svchost.exe	1244	RpcEptMapper, RpcSs
svchost.exe	1288	LSM
svchost.exe	1540	BTAGService
svchost.exe	1572	BthAvctpSvc
svchost.exe	1588	bthserv
svchost.exe	1736	EventLog
svchost.exe	1792	Schedule
svchost.exe	1800	ProfSvc
svchost.exe	1808	NcbService
svchost.exe	1816	TimeBrokerSvc
svchost.exe	1968	DisplayEnhancementService
svchost.exe	2016	UserManager
svchost.exe	2024	hidserv
svchost.exe	2032	EventSystem
svchost.exe	672	nsi
svchost.exe	2112	PhoneSvc
svchost.exe	2168	Dhcp
svchost.exe	2180	CoreMessagingRegistrar
svchost.exe	2284	SENS
igfxCUIService.exe	2396	igfxCUIService2.0.0.0
svchost.exe	2404	SEMgrSvc

Workstation Information

A workstation is known as a special computer designed for technical or scientific applications intended primarily to be used by one person at a time. They are commonly connected to a LAN and run multi-user operating systems. Follow these commands to get our workstation details.

```
net config workstation >> notes.txt
```

to check whether the file is created or not use [dir] command.

```

C:\Users\SKS19\prac>net config workstation >> notes.txt
C:\Users\SKS19\prac>dir
Volume in drive C has no label.
Volume Serial Number is C296-F770

Directory of C:\Users\SKS19\prac

02-07-2020  16:41    <DIR>          .
02-07-2020  16:41    <DIR>          ..
02-07-2020  16:41                604 notes.txt
               1 File(s)                604 bytes
               2 Dir(s)  428,953,464,832 bytes free

```

Now, open the text file to see the investigation results.

```

notes - Notepad
File Edit Format View Help
Computer name          \\DESKTOP-QSBQ20A
Full Computer name     DESKTOP-QSBQ20A
User name              sks1997.sk@outlook.com

Workstation active on
NetBT_Tcpip_{74C48C54-FB6B-421F-BBF9-19AB93B4AD2A} (0A002700000E)

Software version       Windows 10 Pro

Workstation domain     WORKGROUP
Logon domain           MicrosoftAccount

COM Open Timeout (sec) 0
COM Send Count (byte)  16
COM Send Timeout (msec) 250
The command completed successfully.

```

MAC Address saved in System ARP Cache

There are two types of ARP entries- static and dynamic. Most of the time, we will use the dynamic ARP entries. This means that the ARP entries kept on a device for some period of time, as long as it is being used.

The opposite of a dynamic, if ARP entry is the static entry we need to enter a manual link between the Ethernet MAC Address and IP Address. Because of management headaches and the lack of significant negatives. We use dynamic most of the time. To get that details in the investigation follow this command.

```
arp -a >> notes.txt
```

we can whether the text file is created or not with [dir] command.


```
C:\Users\SKS19\prac>arp -a >> notes.txt

C:\Users\SKS19\prac>dir
Volume in drive C has no label.
Volume Serial Number is C296-F770

Directory of C:\Users\SKS19\prac

02-07-2020  16:27    <DIR>          .
02-07-2020  16:27    <DIR>          ..
02-07-2020  16:27                1,159 notes.txt
               1 File(s)                1,159 bytes
               2 Dir(s)  428,958,384,128 bytes free

C:\Users\SKS19\prac>
```

Now, open the text file to see the investigation report.

```
notes - Notepad
File Edit Format View Help

Interface: 192.168.0.6 --- 0xa
  Internet Address      Physical Address      Type
  192.168.0.1           1c-5f-2b-59-e1-24    dynamic
  192.168.0.3           40-49-0f-85-e7-71    dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff    static
  224.0.0.2             01-00-5e-00-00-02    static
  224.0.0.22            01-00-5e-00-00-16    static
  224.0.0.251           01-00-5e-00-00-fb    static
  224.0.0.252           01-00-5e-00-00-fc    static
  239.192.152.143       01-00-5e-40-98-8f    static
  239.255.255.250       01-00-5e-7f-ff-fa    static
  255.255.255.255       ff-ff-ff-ff-ff-ff    static

Interface: 192.168.56.1 --- 0xe
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff    static
  224.0.0.2             01-00-5e-00-00-02    static
  224.0.0.22            01-00-5e-00-00-16    static
  224.0.0.251           01-00-5e-00-00-fb    static
  224.0.0.252           01-00-5e-00-00-fc    static
  239.192.152.143       01-00-5e-40-98-8f    static
  239.255.255.250       01-00-5e-7f-ff-fa    static
```

System User Details

A user is a person who is utilizing a computer or network service. Users of computer systems and software products generally lack the technical expertise required to fully understand how they work. To get that user details to follow this command.

```
net user %username% >> notes.txt
```

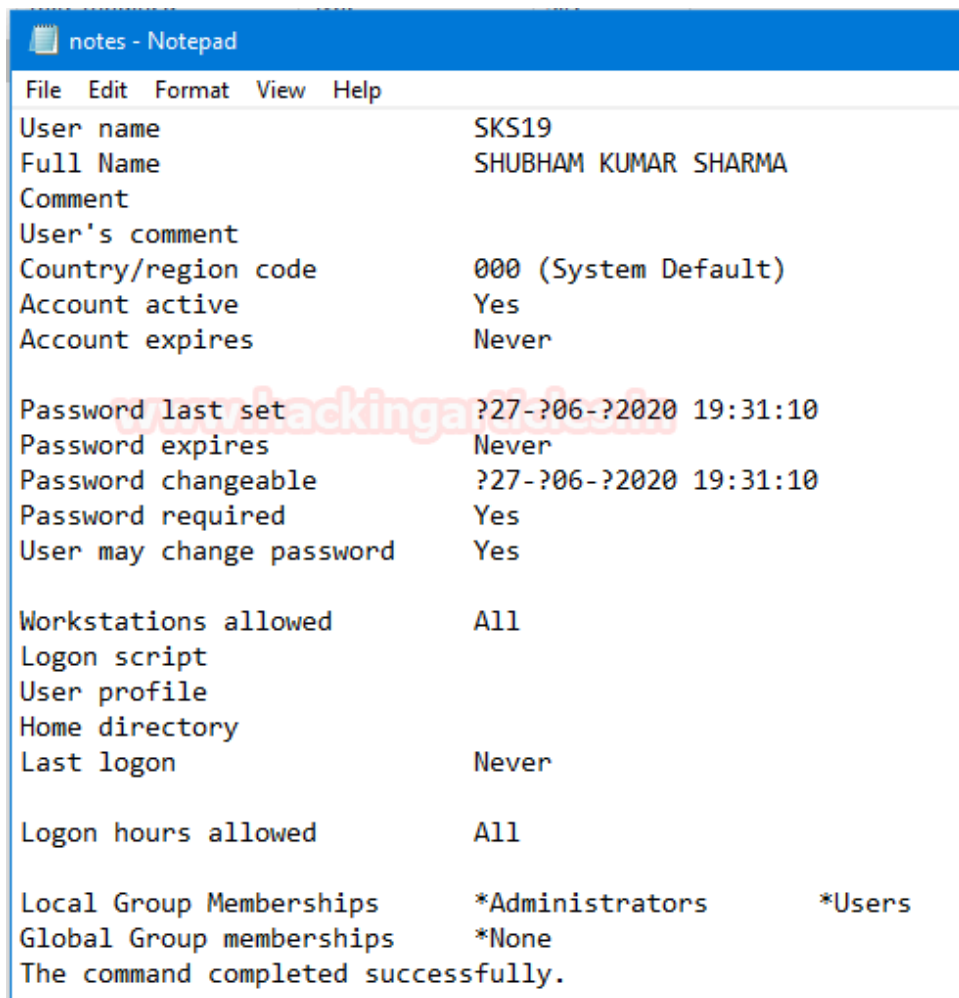
we can use [dir] command to check the file is created or not.

```
C:\Users\SKS19\prac>net user %username% >> notes.txt
C:\Users\SKS19\prac>dir
Volume in drive C has no label.
Volume Serial Number is C296-F770

Directory of C:\Users\SKS19\prac

02-07-2020  16:36    <DIR>          .
02-07-2020  16:36    <DIR>          ..
02-07-2020  16:36                852 notes.txt
               1 File(s)                852 bytes
               2 Dir(s)  428,958,584,832 bytes free
```

Now, open a text file to see the investigation report.



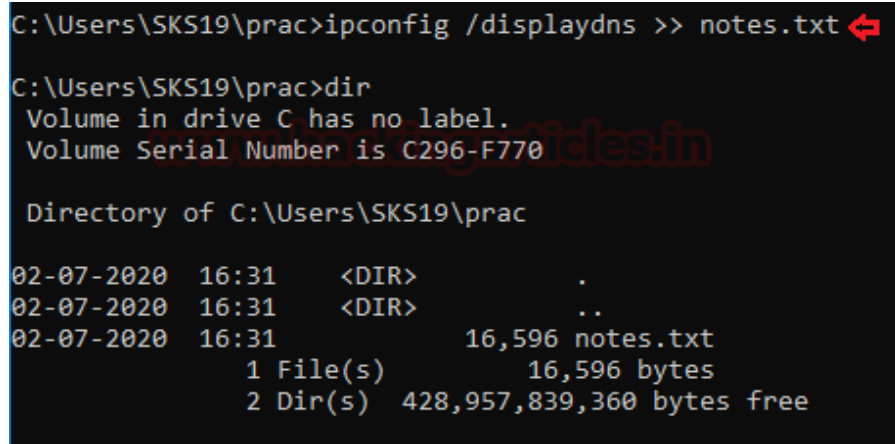
DNS Configuration

DNS is the internet system for converting alphabetic names into the numeric IP address. When a web address is typed into the browser, DNS servers return the IP address of the webserver associated with that name. To know the

system DNS configuration follow this command.

```
ipconfig /displaydns >> notes.txt
```

we can see the text report is created or not with [dir] command.



```
C:\Users\SKS19\prac>ipconfig /displaydns >> notes.txt ↵
C:\Users\SKS19\prac>dir
Volume in drive C has no label.
Volume Serial Number is C296-F770

Directory of C:\Users\SKS19\prac

02-07-2020  16:31    <DIR>          .
02-07-2020  16:31    <DIR>          ..
02-07-2020  16:31                16,596 notes.txt
               1 File(s)              16,596 bytes
               2 Dir(s)  428,957,839,360 bytes free
```

Now open the text file to see the text report.

```
notes - Notepad
File Edit Format View Help

Windows IP Configuration

pop-esp2.perf.linkedin.com
-----
Record Name . . . . . : pop-esp2.perf.linkedin.com
Record Type . . . . . : 1
Time To Live . . . . . : 1406
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 108.174.12.129

www.softwarecrew.com
-----
Record Name . . . . . : www.softwarecrew.com
Record Type . . . . . : 1
Time To Live . . . . . : 9447
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 109.104.89.128

ocsp.sectigo.com
-----
Record Name . . . . . : ocsp.sectigo.com
Record Type . . . . . : 28
Time To Live . . . . . : 761
Data Length . . . . . : 16
Section . . . . . : Answer
AAAA Record . . . . . : 2001:4de0:ac19::1:b:1b

Record Name . . . . . : ocsp.sectigo.com
Record Type . . . . . : 28
Time To Live . . . . . : 761
Data Length . . . . . : 16
Section . . . . . : Answer
AAAA Record . . . . . : 2001:4de0:ac19::1:b:2b
```

System network shares

A shared network would mean a common Wi-Fi or LAN connection. The same is possible for another folder on the system. By turning on network sharing and allowing certain or restricted rights, these folders can be viewed by other users/computers on the same network services. We can see these details by following this command.

```
net share >> notes.txt
```

we can also check the file it is created or not with [dir] command.

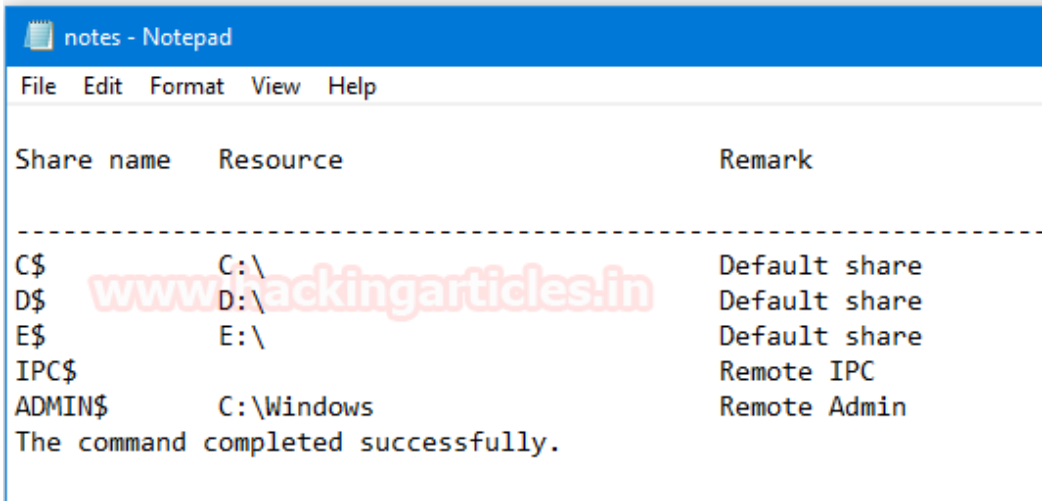
```
C:\Users\SKS19\prac>net share >> notes.txt ↵

C:\Users\SKS19\prac>dir
Volume in drive C has no label.
Volume Serial Number is C296-F770

Directory of C:\Users\SKS19\prac

02-07-2020  16:39    <DIR>          .
02-07-2020  16:39    <DIR>          ..
02-07-2020  16:39                582 notes.txt
               1 File(s)                582 bytes
               2 Dir(s)  428,954,308,608 bytes free
```

Now, open that text file to see the investigation report.



Network Configuration

Network configuration is the process of setting a network’s controls, flow, and operation to support the network communication of an organization and/or network owner. This term incorporates the multiple configurations and steps up processes on network hardware, software, and other supporting devices and components. To get the network details follow these commands.

```
ipconfig /all >> notes.txt
```

As usual, we can check the file is created or not with [dir] commands.

```
C:\Users\SKS19\prac>ipconfig /all >> notes.txt ↵  
C:\Users\SKS19\prac>dir  
Volume in drive C has no label.  
Volume Serial Number is C296-F770  
  
Directory of C:\Users\SKS19\prac  
  
02-07-2020  16:29    <DIR>          .  
02-07-2020  16:29    <DIR>          ..  
02-07-2020  16:29                3,790 notes.txt  
               1 File(s)                3,790 bytes  
               2 Dir(s)  428,960,899,072 bytes free  
  
C:\Users\SKS19\prac>
```

Now, open the text file to see the investigation report.

As we said earlier these are one of few commands which are commonly used. There are plenty of commands left in the Forensic Investigator's arsenal.

Windows IP Configuration

Host Name : DESKTOP-QSBQ20A
Primary Dns Suffix :
Node Type : Hybrid
IP Routing Enabled. : No
WINS Proxy Enabled. : No
DNS Suffix Search List. : domain.name

Ethernet adapter Ethernet:

Media State : Media disconnected
Connection-specific DNS Suffix . :
Description : Realtek PCIe GbE Family Controller
Physical Address. : 04-D4-C4-E9-52-69
DHCP Enabled. : Yes
Autoconfiguration Enabled : Yes

Ethernet adapter VirtualBox Host-Only Network:

Connection-specific DNS Suffix . :
Description : VirtualBox Host-Only Ethernet Adapter
Physical Address. : 0A-00-27-00-00-0E
DHCP Enabled. : No
Autoconfiguration Enabled : Yes
Link-local IPv6 Address : fe80::65e8:1f11:e0fc:aa83%14(Preferred)
IPv4 Address. : 192.168.56.1(Preferred)
Subnet Mask : 255.255.255.0
Default Gateway :
DHCPv6 IAID : 67764263
DHCPv6 Client DUID. : 00-01-00-01-26-89-08-AB-04-D4-C4-E9-52-69
DNS Servers : fec0:0:0:ffff::1%1
 fec0:0:0:ffff::2%1
 fec0:0:0:ffff::3%1
NetBIOS over Tcpip. : Enabled

... ..