

Windows:

```
c:\ Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.3930]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>date /t & time /t
Fri 02/02/2024
07:35 PM

C:\WINDOWS\system32>wmic os get LocalDateTime
LocalDateTime
20240202193555.164000+360

C:\WINDOWS\system32>query user
  USERNAME          SESSIONNAME      ID  STATE   IDLE TIME  LOGON TIME
>student           console            1  Active    none   2/2/2024 1:29 PM

C:\WINDOWS\system32>net sessions
There are no entries in the list.

C:\WINDOWS\system32>
```

```
C:\WINDOWS\system32>net file
There are no entries in the list.
```

```
C:\WINDOWS\system32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix . .
  Link-local IPv6 Address . . . . : fe80::7b78:9772:d9ef:d41f%6
  IPv4 Address. . . . . : 10.33.2.72
  Subnet Mask . . . . . : 255.255.255.192
  Default Gateway . . . . . : 10.33.2.126

Wireless LAN adapter Wi-Fi:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . .

Wireless LAN adapter Local Area Connection* 9:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . .

Wireless LAN adapter Local Area Connection* 10:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . .

Ethernet adapter Bluetooth Network Connection:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . .
```

```

C:\WINDOWS\system32>ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-7BET09L
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . . . . : Realtek PCIe GbE Family Controller
Description . . . . . : Realtek PCIe GbE Family Controller
Physical Address . . . . . : 1C-69-7A-43-DE-1F
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::7b78:9772:d9ef:d41f%6(PREFERRED)
IPv4 Address . . . . . : 10.33.2.72(Preferred)
Subnet Mask . . . . . : 255.255.255.192
Default Gateway . . . . . : 10.33.2.126
DHCPv6 IAID . . . . . : 438069626
DHCPv6 Client DUID. . . . . : 00-01-00-01-2A-95-56-49-1C-69-7A-43-DE-1F
DNS Servers . . . . . : 10.33.4.2
NetBIOS over Tcpip. . . . . : Enabled

Wireless LAN adapter Wi-Fi:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Intel(R) Dual Band Wireless-AC 3165
Physical Address . . . . . : C0-B8-83-CE-04-46
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Local Area Connection* 9:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address . . . . . : C0-B8-83-CE-04-47
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Local Area Connection* 10:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address . . . . . : C2-B8-83-CE-04-46
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Bluetooth Device (Personal Area Network)
Physical Address . . . . . : C0-B8-83-CE-04-4A
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

```

Image Name	PID	Session Name	Session#	Mem Usage	Status	User Name	CPU Time	Window Title
System Idle Process	0	Services	0	8 K	Unknown	NT AUTHORITY\SYSTEM	1:15:58	N/A
System	4	Services	0	824 K	Unknown	N/A	0:00:15	N/A
Registry	124	Services	0	74,912 K	Unknown	NT AUTHORITY\SYSTEM	0:00:08	N/A
sms.exe	476	Services	0	1,188 K	Unknown	NT AUTHORITY\SYSTEM	0:00:08	N/A
csrss.exe	656	Services	0	5,836 K	Unknown	NT AUTHORITY\SYSTEM	0:00:08	N/A
wininit.exe	876	Services	0	7,228 K	Unknown	NT AUTHORITY\SYSTEM	0:00:08	N/A
csrss.exe	884	Console	1	6,288 K	Running	NT AUTHORITY\SYSTEM	0:00:02	N/A
services.exe	956	Services	0	19,836 K	Unknown	NT AUTHORITY\SYSTEM	0:00:01	N/A
winlogon.exe	990	Console	1	1,912 K	Unknown	NT AUTHORITY\SYSTEM	0:00:01	N/A
lsass.exe	1080	Services	0	20,532 K	Unknown	NT AUTHORITY\SYSTEM	0:00:01	N/A
svchost.exe	768	Services	0	27,304 K	Unknown	NT AUTHORITY\SYSTEM	0:00:01	N/A
fontdrvhost.exe	784	Console	1	4,468 K	Unknown	Font Driver Host\UMFD-1	0:00:00	N/A
fontdrvhost.exe	788	Services	0	3,536 K	Unknown	Font Driver Host\UMFD-0	0:00:00	N/A
svchost.exe	524	Services	0	14,664 K	Unknown	NT AUTHORITY\NETWORK SERVICE	0:00:04	N/A
svchost.exe	1080	Services	0	5,696 K	Unknown	NT AUTHORITY\SYSTEM	0:00:04	N/A
diagram.exe	1144	Console	1	107,340 K	Running	Window Manager\DMW-1	0:00:03	DWM Notification Window
svchost.exe	1244	Services	0	15,284 K	Unknown	NT AUTHORITY\SYSTEM	0:00:01	N/A
svchost.exe	1336	Services	0	10,668 K	Unknown	NT AUTHORITY\SYSTEM	0:00:00	N/A

```
C:\WINDOWS\system32>tasklist
```

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	8 K
System	4	Services	0	824 K
Registry	124	Services	0	74,912 K
smss.exe	476	Services	0	1,108 K
csrss.exe	656	Services	0	5,836 K
wininit.exe	876	Services	0	7,228 K
csrss.exe	884	Console	1	6,280 K
services.exe	956	Services	0	10,824 K
winlogon.exe	984	Console	1	11,876 K
lsass.exe	1008	Services	0	20,532 K
svchost.exe	760	Services	0	27,304 K
fontdrvhost.exe	784	Console	1	4,460 K
fontdrvhost.exe	788	Services	0	3,536 K
svchost.exe	524	Services	0	14,684 K
svchost.exe	1088	Services	0	8,604 K

```
C:\WINDOWS\system32>arp -a
```

Interface: 10.33.2.72 --- 0x6	Internet Address	Physical Address	Type
	10.33.2.78	1c-69-7a-43-dd-c6	dynamic
	10.33.2.84	1c-69-7a-43-de-ba	dynamic
	10.33.2.91	1c-69-7a-43-dd-ae	dynamic
	10.33.2.110	8c-16-45-88-1f-b1	dynamic
	10.33.2.127	ff-ff-ff-ff-ff-ff	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
	239.255.255.250	01-00-5e-7f-ff-fa	static

```
nsic C:\WINDOWS\system32>route print
=====
Interface List
 6...1c 69 7a 43 de 1f .....Realtek PCIe GbE Family Controller
 3...c0 b8 83 ce 04 46 .....Intel(R) Dual Band Wireless-AC 3165
 17...c0 b8 83 ce 04 47 .....Microsoft Wi-Fi Direct Virtual Adapter
 18...c2 b8 83 ce 04 46 .....Microsoft Wi-Fi Direct Virtual Adapter #2
 16...c0 b8 83 ce 04 4a .....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    10.33.2.126   10.33.2.72    281
        10.33.2.64  255.255.255.192      On-link        10.33.2.72    281
        10.33.2.72  255.255.255.255      On-link        10.33.2.72    281
        10.33.2.127 255.255.255.255      On-link        10.33.2.72    281
          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
          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      10.33.2.72    281
        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      10.33.2.72    281
=====
Persistent Routes:
  Network Address      Netmask  Gateway Address Metric
          0.0.0.0        0.0.0.0  10.33.2.126 Default
=====

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
 1    331 ::1/128        On-link
 6    281 fe80:::/64        On-link
 6    281 fe80::7b78:9772:d9ef:d41f/128
          On-link
 1    331 ff00::/8        On-link
 6    281 ff00::/8        On-link
=====
Persistent Routes:
  None
```

| Forensic

```
C:\WINDOWS\system32>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.33.2.72:7680        10.33.2.78:60634      TIME_WAIT
  TCP    10.33.2.72:7680        10.33.2.78:60636      TIME_WAIT
  TCP    10.33.2.72:7680        10.33.2.78:60638      TIME_WAIT
  TCP    10.33.2.72:52470       74.125.24.188:5228  ESTABLISHED
  TCP    10.33.2.72:52649       74.125.68.84:443     CLOSE_WAIT
  TCP    10.33.2.72:52656       172.253.118.95:443  ESTABLISHED
  TCP    10.33.2.72:52660       96.17.182.215:443    ESTABLISHED
  TCP    10.33.2.72:52661       96.17.182.215:443    ESTABLISHED
  TCP    10.33.2.72:52662       96.17.182.215:443    ESTABLISHED
  TCP    10.33.2.72:52665       40.78.107.249:443   FIN_WAIT_1
  TCP    10.33.2.72:52667       13.107.42.16:443    ESTABLISHED
  TCP    10.33.2.72:52675       4.154.131.233:443   ESTABLISHED
  TCP    10.33.2.72:52676       20.231.121.79:80     ESTABLISHED
  TCP    10.33.2.72:62964       40.126.16.166:443   ESTABLISHED
  TCP    10.33.2.72:62965       13.107.21.200:443   ESTABLISHED
  TCP    10.33.2.72:62966       204.79.197.222:443  ESTABLISHED
  TCP    10.33.2.72:62967       117.18.232.200:443  ESTABLISHED
  TCP    10.33.2.72:62968       13.107.18.254:443  ESTABLISHED
  TCP    10.33.2.72:62969       13.107.13.254:443  ESTABLISHED
  TCP    10.33.2.72:62986       20.198.119.84:443  ESTABLISHED
  TCP    [fe80::7b78:9772:d9ef:d41f%6]:1521  [fe80::7b78:9772:d9ef:d41f%6]:49673  ESTABLISHED
  TCP    [fe80::7b78:9772:d9ef:d41f%6]:49673  [fe80::7b78:9772:d9ef:d41f%6]:1521  ESTABLISHED

C:\WINDOWS\system32>netstat -c

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

  -a      Displays all connections and listening ports.
  -b      Displays the executable involved in creating each connection or
         listening port. In some cases well-known executables host
         multiple independent components, and in these cases the
         sequence of components involved in creating the connection
         or listening port is displayed. In this case the executable
         name is in [] at the bottom, on top is the component it called,
         and so forth until TCP/IP was reached. Note that this option
         can be time-consuming and will fail unless you have sufficient
         permissions.
  -e      Displays Ethernet statistics. This may be combined with the -s
         option.
  -f      Displays Fully Qualified Domain Names (FQDN) for foreign
         addresses.
```

C:\WINDOWS\system32>netstat -ano

orensic Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	524
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:1521	0.0.0.0:0	LISTENING	3704
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	2228
TCP	0.0.0.0:8080	0.0.0.0:0	LISTENING	3704
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	876
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	1380
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING	1448
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	3180
TCP	0.0.0.0:49672	0.0.0.0:0	LISTENING	956
TCP	0.0.0.0:49674	0.0.0.0:0	LISTENING	3736
TCP	10.33.2.72:139	0.0.0.0:0	LISTENING	4
TCP	10.33.2.72:7680	10.33.2.78:60634	TIME_WAIT	0
TCP	10.33.2.72:7680	10.33.2.78:60636	TIME_WAIT	0
TCP	10.33.2.72:52470	74.125.24.188:5228	ESTABLISHED	8156
TCP	10.33.2.72:52649	74.125.68.84:443	ESTABLISHED	8156
TCP	10.33.2.72:52656	172.253.118.95:443	ESTABLISHED	9832
TCP	10.33.2.72:52660	96.17.182.215:443	ESTABLISHED	7456
TCP	10.33.2.72:52661	96.17.182.215:443	ESTABLISHED	7456
TCP	10.33.2.72:52662	96.17.182.215:443	ESTABLISHED	7456
TCP	10.33.2.72:52665	40.78.107.249:443	ESTABLISHED	10876
TCP	10.33.2.72:52667	13.107.42.16:443	ESTABLISHED	9832
TCP	10.33.2.72:52673	20.231.121.79:80	SYN_SENT	1244
TCP	10.33.2.72:62964	40.126.16.166:443	ESTABLISHED	7456
TCP	10.33.2.72:62965	13.107.21.200:443	ESTABLISHED	7456
TCP	10.33.2.72:62966	204.79.197.222:443	ESTABLISHED	7456
TCP	10.33.2.72:62967	117.18.232.200:443	ESTABLISHED	7456
TCP	10.33.2.72:62968	13.107.18.254:443	ESTABLISHED	7456
TCP	10.33.2.72:62969	13.107.13.254:443	ESTABLISHED	7456
TCP	10.33.2.72:62986	20.198.119.84:443	ESTABLISHED	3660
TCP	127.0.0.1:49670	0.0.0.0:0	LISTENING	3704
TCP	[::]:135	[::]:0	LISTENING	524
TCP	[::]:445	[::]:0	LISTENING	4
TCP	[::]:1521	[::]:0	LISTENING	3704
TCP	[::]:5357	[::]:0	LISTENING	4

Linux: