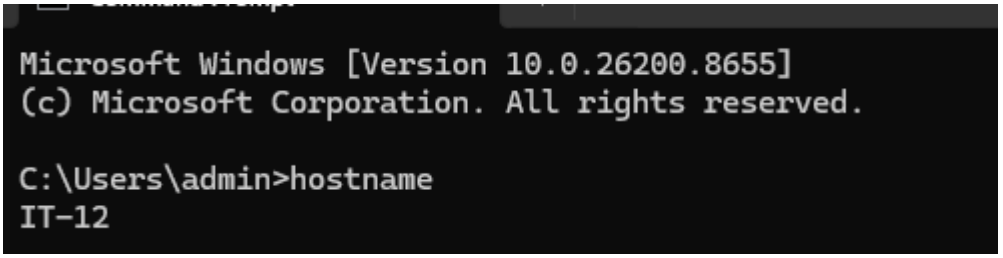
Practical No.4

Step 1: Find the Computer Name

What it does: Displays the specific name of your computer as it is identified on your local network.
Why it is useful: When troubleshooting network issues, mapping network drives, or trying to connect to a specific machine remotely, you need to know its exact network identifier.



Step 2: Display Windows Version

What it does: Short for "version," this outputs the specific version and build number of the Windows Operating System currently running.
Why it is useful: It helps verify if your system is fully updated, which is important for security patching or checking if your OS meets the minimum requirements to install specific software.

Step 3: Display Detailed System Information

What it does: Pulls a comprehensive, readable summary of your computer's hardware and software configuration. This includes the OS version, system boot time (uptime), computer manufacturer, processor details, total RAM, and a list of installed Windows updates (hotfixes).

Why it is useful: It acts as a one-stop command for gathering foundational diagnostic information about a PC without needing to click through multiple graphical menus.

```
Host Name:                 IT-12
OS Name:                   Microsoft Windows 11 Pro
OS Version:                10.0.26200 N/A Build 26200
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          admin
Registered Organization:
Product ID:                00330-80000-00000-AA898
Original Install Date:     3/9/2026, 4:49:59 PM
System Boot Time:          7/9/2026, 10:15:43 AM
System Manufacturer:       Gigabyte Technology Co., Ltd.
System Model:              H610M K DDR4
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 151 Stepping 2 GenuineIntel ~2100 Mhz
BIOS Version:              American Megatrends International, LLC. FC, 12/14/2023
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+05:30) Sri Jayawardenepura
Total Physical Memory:     32,537 MB
Available Physical Memory: 23,714 MB
Virtual Memory: Max Size:  34,585 MB
Virtual Memory: Available: 24,883 MB
Virtual Memory: In Use:    9,702 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\IT-12
Hotfix(s):                 4 Hotfix(s) Installed.
                           [01]: KB5087051
                           [02]: KB5054156
```

Step 4: Display Network Configuration

What it does: Displays the complete network configuration for all network adapters (Wi-Fi, Ethernet, virtual adapters) on your machine. The `/all` switch reveals details beyond just your basic IP address, including your MAC address (Physical Address), DNS servers, and whether DHCP is enabled.
Why it is useful: This is the most essential command for troubleshooting internet or local network connectivity issues.

```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : IT-12
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : 10-FF-E0-29-A7-7D
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::7d74:1cd2:e4e2:615c%9(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.2.22(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.2.1
   DHCPv6 IAID . . . . . . . . . . . : 68222944
   DHCPv6 Client DUID. . . . . . . . : 00-01-01-00-31-45-63-FE-10-FF-E0-29-A7-7D
   DNS Servers . . . . . . . . . . . : 8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-0E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::b275:4abc:a3c2:cc52%14(Preferred)
   Autoconfiguration IPv4 Address. . : 169.254.42.12(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :
```

Options

ipconfig/flushdns : command used to clear the DNS cache on a Windows computer, helping to resolve network connectivity issues by discarding outdated

```
C:\Users\admin>ipconfig/flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

ipconfig/registerdns : command that refreshes and updates the DNS (Domain Name System) registration for a computer's network interface.

(Perform in administrative mode)

```
Successfully flushed the DNS Resolver Cache.

C:\Users\admin>ipconfig/registerdns
The requested operation requires elevation.
```

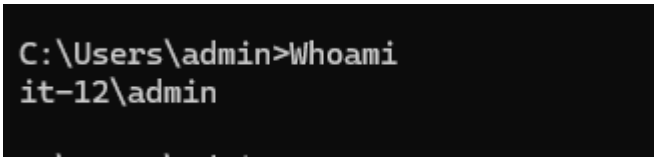
ipconfig/release : command that releases the IP address assigned to a network interface.

```
Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::7d74:1cd2:e4e2:615c%9
   IPv4 Address. . . . . . . . . . . : 192.168.2.22
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.2.1

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b275:4abc:a3c2:cc52%14
   Autoconfiguration IPv4 Address. . : 169.254.42.12
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b8cc:ba6e:7588:88e5%8
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::75e0:b8c:960b:9e57%11
   Default Gateway . . . . . . . . . :
```

ipconfig/renew : command used to renew the IP address assigned to a computer or network interface.

Step 5: Find Logged-in User

What it does: Displays the exact username and domain of the user currently logged into the active command prompt session.
Why it is useful: In corporate environments, servers, or home PCs with multiple accounts, this confirms exactly which user profile (and associated security permissions) you are operating under.



Step 6: View Running Processes

What it does: Generates a list of all currently running applications and background services. It shows the image name (e.g., `chrome.exe`), its unique Process ID (PID), and how much system memory it is currently consuming.
Why it is useful: It is the command-line equivalent of the Windows Task Manager. It helps identify frozen programs, rogue background processes, or applications that are eating up system resources.

```
C:\Users\admin>tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0      4,732 K
Registry                       320 Services                   0     65,544 K
smss.exe                       928 Services                   0      1,780 K
csrss.exe                     1288 Services                   0      8,708 K
wininit.exe                   1376 Services                   0     10,420 K
csrss.exe                     1384 Console                    1      8,892 K
winlogon.exe                  1476 Console                    1     16,984 K
services.exe                  1496 Services                   0     12,788 K
lsass.exe                     1540 Services                   0     27,576 K
svchost.exe                   1676 Services                   0     36,628 K
fontdrvhost.exe               1708 Services                   0      5,732 K
fontdrvhost.exe               1716 Console                    1      8,732 K
svchost.exe                   1804 Services                   0     20,008 K
svchost.exe                   1852 Services                   0     13,592 K
dwm.exe                       1916 Console                    1    208,792 K
svchost.exe                   1228 Services                   0      7,504 K
svchost.exe                   1240 Services                   0      8,500 K
svchost.exe                   2052 Services                   0     18,192 K
svchost.exe                   2096 Services                   0     14,736 K
svchost.exe                   2104 Services                   0     14,104 K
svchost.exe                   2112 Services                   0     15,924 K
IntelCpHDCPSvc.exe            2216 Services                   0      8,464 K
svchost.exe                   2240 Services                   0     22,112 K
svchost.exe                   2256 Services                   0      7,924 K
svchost.exe                   2320 Services                   0     10,948 K
svchost.exe                   2424 Services                   0     21,664 K
svchost.exe                   2580 Services                   0     23,132 K
svchost.exe                   2612 Services                   0      7,940 K
svchost.exe                   2620 Services                   0     11,244 K
svchost.exe                   2628 Services                   0     19,160 K
Memory Compression            2768 Services                   0          N/A
```

Step 7: View Active Network Connections

What it does: Displays active network connections and listening ports on your machine.

- `-a`: Displays all active connections and listening ports.

- `-n`: Displays addresses and port numbers in numerical form (speeding up the command by skipping DNS lookups).
- `-o`: Includes the Process ID (PID) responsible for each connection.

Why it is useful: It is a crucial tool for security and network monitoring. If you suspect malware or unauthorized access, this shows exactly what external servers your computer is talking to, and allows you to trace that connection back to a specific program using the PID.

```
C:\Users\admin>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1804
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:796            0.0.0.0:0              LISTENING       11488
  TCP    0.0.0.0:903            0.0.0.0:0              LISTENING       4892
  TCP    0.0.0.0:913            0.0.0.0:0              LISTENING       4892
  TCP    0.0.0.0:2383           0.0.0.0:0              LISTENING       5808
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING       4332
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       8384
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       10752
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       1540
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1376
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       2052
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       2580
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       3536
  TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING       3708
  TCP    0.0.0.0:49672          0.0.0.0:0              LISTENING       1496
  TCP    127.0.0.1:1434         0.0.0.0:0              LISTENING       5428
  TCP    127.0.0.1:8991         0.0.0.0:0              LISTENING       17280
  TCP    127.0.0.1:9009         0.0.0.0:0              LISTENING       4
  TCP    192.168.2.158:139      0.0.0.0:0              LISTENING       4
  TCP    192.168.2.158:796      192.168.2.3:60112      TIME_WAIT       0
  TCP    192.168.2.158:796      192.168.2.3:60166      TIME_WAIT       0
  TCP    192.168.2.158:796      192.168.2.3:60218      TIME_WAIT       0
  TCP    192.168.2.158:796      192.168.2.3:60270      TIME_WAIT       0
  TCP    192.168.2.158:796      192.168.2.3:60323      TIME_WAIT       0
  TCP    192.168.2.158:796      192.168.2.3:60375      TIME_WAIT       0
  TCP    192.168.2.158:7680     10.0.0.125:59341       ESTABLISHED     10752
  TCP    192.168.2.158:7680     10.0.0.239:64088       ESTABLISHED     10752
```

2. Netstat and its options.
Description :
● Stands for network statistics
● Monitors incoming and outgoing network connections.
● Helps in network troubleshooting and performance measurement.

```
C:\Users\admin>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.2.158:796      192:64607              TIME_WAIT
  TCP    192.168.2.158:796      192:64660              TIME_WAIT
  TCP    192.168.2.158:796      192:64715              TIME_WAIT
  TCP    192.168.2.158:796      192:64765              TIME_WAIT
  TCP    192.168.2.158:796      192:64814              TIME_WAIT
  TCP    192.168.2.158:7680     10:59341               ESTABLISHED
  TCP    192.168.2.158:7680     192:41325              TIME_WAIT
  TCP    192.168.2.158:7680     192:41327              TIME_WAIT
  TCP    192.168.2.158:7680     192:60390              TIME_WAIT
  TCP    192.168.2.158:7680     192:54233              ESTABLISHED
  TCP    192.168.2.158:7680     192:63524              TIME_WAIT
  TCP    192.168.2.158:7680     192:63526              TIME_WAIT
  TCP    192.168.2.158:7680     192:63533              TIME_WAIT
  TCP    192.168.2.158:7680     192:63422              ESTABLISHED
  TCP    192.168.2.158:7680     192:63542              ESTABLISHED
  TCP    192.168.2.158:7680     192:65100              ESTABLISHED
  TCP    192.168.2.158:7680     192:52244              ESTABLISHED
  TCP    192.168.2.158:7680     192:56760              TIME_WAIT
  TCP    192.168.2.158:7680     192:56767              TIME_WAIT
  TCP    192.168.2.158:7680     192:56775              TIME_WAIT
  TCP    192.168.2.158:7680     192:59555              ESTABLISHED
  TCP    192.168.2.158:7680     192:49694              ESTABLISHED
  TCP    192.168.2.158:7680     192:49695              ESTABLISHED
  TCP    192.168.2.158:7680     192:52414              TIME_WAIT
  TCP    192.168.2.158:7680     192:52416              TIME_WAIT
  TCP    192.168.2.158:7680     192:58194              ESTABLISHED
  TCP    192.168.2.158:7680     192:58204              ESTABLISHED
  TCP    192.168.2.158:7680     192:55763              TIME_WAIT
  TCP    192.168.2.158:7680     192:56100              TIME_WAIT
  TCP    192.168.2.158:7680     192:62076              ESTABLISHED
```

Options :
● netstat-a : enlists all active network connections and listening ports.

```
C:\Users\admin>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             IT-11:0                LISTENING
  TCP    0.0.0.0:135            IT-11:0                LISTENING
  TCP    0.0.0.0:445            IT-11:0                LISTENING
  TCP    0.0.0.0:796            IT-11:0                LISTENING
  TCP    0.0.0.0:903            IT-11:0                LISTENING
  TCP    0.0.0.0:913            IT-11:0                LISTENING
  TCP    0.0.0.0:2383           IT-11:0                LISTENING
  TCP    0.0.0.0:3306           IT-11:0                LISTENING
  TCP    0.0.0.0:5040           IT-11:0                LISTENING
  TCP    0.0.0.0:7680           IT-11:0                LISTENING
  TCP    0.0.0.0:49664          IT-11:0                LISTENING
  TCP    0.0.0.0:49665          IT-11:0                LISTENING
  TCP    0.0.0.0:49666          IT-11:0                LISTENING
  TCP    0.0.0.0:49667          IT-11:0                LISTENING
  TCP    0.0.0.0:49668          IT-11:0                LISTENING
  TCP    0.0.0.0:49671          IT-11:0                LISTENING
  TCP    0.0.0.0:49672          IT-11:0                LISTENING
  TCP    127.0.0.1:1434         IT-11:0                LISTENING
  TCP    127.0.0.1:8991         IT-11:0                LISTENING
  TCP    127.0.0.1:9009         IT-11:0                LISTENING
  TCP    192.168.2.158:139      IT-11:0                LISTENING
  TCP    192.168.2.158:796      192:64863              TIME_WAIT
  TCP    192.168.2.158:796      192:64913              TIME_WAIT
  TCP    192.168.2.158:796      192:64963              TIME_WAIT
  TCP    192.168.2.158:796      192:65014              TIME_WAIT
  TCP    192.168.2.158:7680     10:59341               ESTABLISHED
  TCP    192.168.2.158:7680     192:41336              TIME_WAIT
  TCP    192.168.2.158:7680     192:41340              TIME_WAIT
  TCP    192.168.2.158:7680     192:64804              TIME_WAIT
  TCP    192.168.2.158:7680     192:54233              ESTABLISHED
```

netstat -s: Give statistics of all the ports

```
C:\Users\admin>netstat -s

IPv4 Statistics

  Packets Received                   = 1422866
  Received Header Errors             = 0
  Received Address Errors            = 17
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 1120700
  Received Packets Delivered         = 337687
  Output Requests                    = 220923
  Routing Discards                   = 0
  Discarded Output Packets           = 1141
  Output Packet No Route             = 37
  Reassembly Required                = 40805
  Reassembly Successful              = 9065
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0

IPv6 Statistics

  Packets Received                   = 86762
  Received Header Errors             = 0
  Received Address Errors            = 1465
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 5866
  Received Packets Delivered         = 94025
  Output Requests                    = 995
  Routing Discards                   = 0
  Discarded Output Packets           = 0
  Output Packet No Route             = 0
```

netstat-r : giveskernel routingtableand information regarding it.

```
C:\Users\admin>netstat -r
===========================================================================
Interface List
  8...10 ff e0 58 e6 95 ......Realtek PCIe GbE Family Controller
 17...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
  9...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.2.1    192.168.2.158     25
        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
      192.168.2.0    255.255.255.0         On-link     192.168.2.158    281
    192.168.2.158  255.255.255.255         On-link     192.168.2.158    281
    192.168.2.255  255.255.255.255         On-link     192.168.2.158    281
    192.168.177.0    255.255.255.0         On-link     192.168.177.1    291
    192.168.177.1  255.255.255.255         On-link     192.168.177.1    291
  192.168.177.255  255.255.255.255         On-link     192.168.177.1    291
    192.168.220.0    255.255.255.0         On-link     192.168.220.1    291
    192.168.220.1  255.255.255.255         On-link     192.168.220.1    291
  192.168.220.255  255.255.255.255         On-link     192.168.220.1    291
        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     192.168.177.1    291
        224.0.0.0        240.0.0.0         On-link     192.168.220.1    291
        224.0.0.0        240.0.0.0         On-link     192.168.2.158    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     192.168.177.1    291
  255.255.255.255  255.255.255.255         On-link     192.168.220.1    291
  255.255.255.255  255.255.255.255         On-link     192.168.2.158    281
===========================================================================
Persistent Routes:
  None
```

netstat-i : gives list of networking interface.

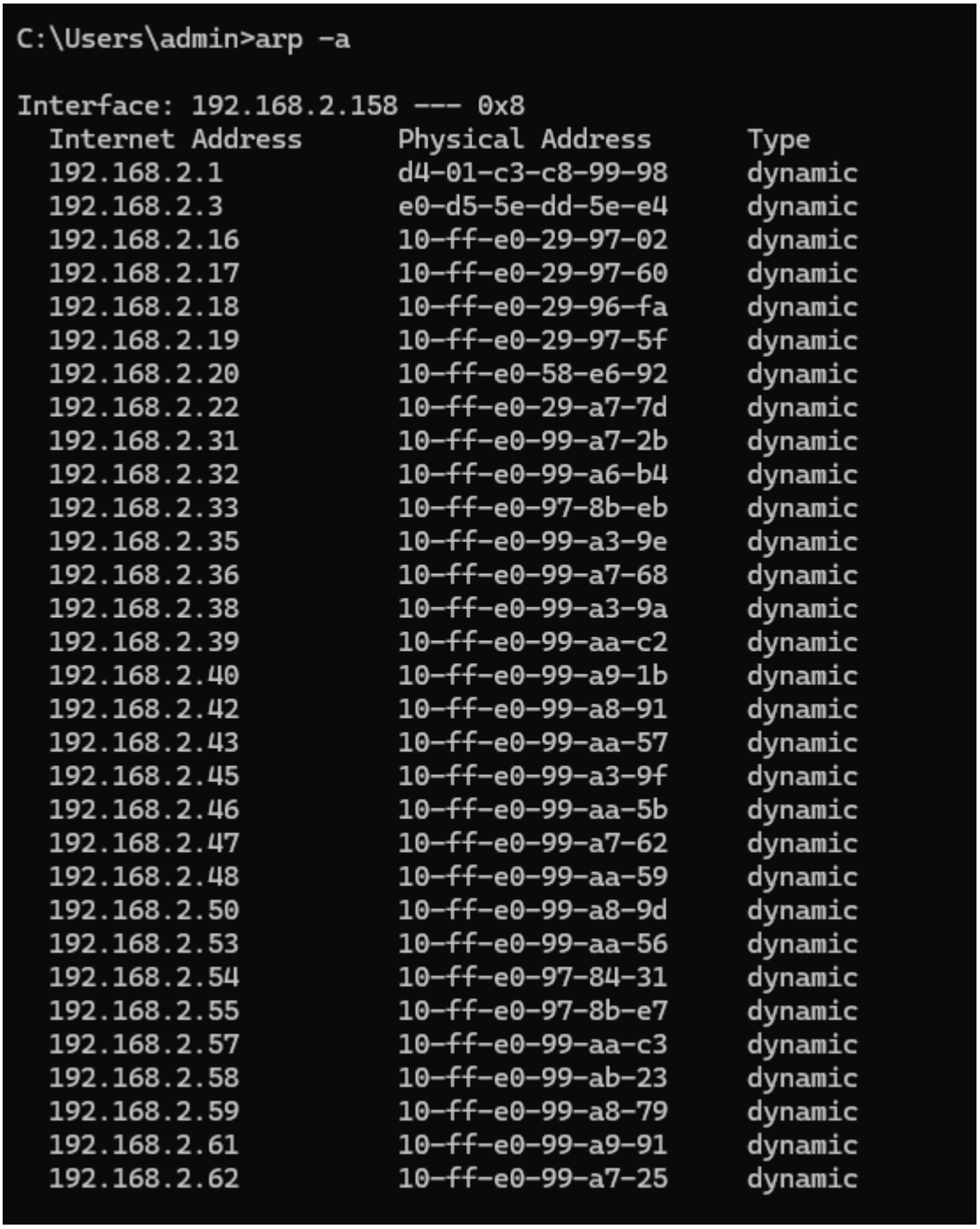
```
C:\Users\admin>netstat -i

Active Connections

  Proto  Local Address          Foreign Address        State           Time in State (ms)
TCP    192.168.2.158:796      192.168.2.3:49173      TIME_WAIT           18898
TCP    192.168.2.158:796      192.168.2.3:65406      TIME_WAIT           99533
TCP    192.168.2.158:796      192:65456              TIME_WAIT           79504
TCP    192.168.2.158:796      192:65505              TIME_WAIT           59641
TCP    192.168.2.158:7680     192:1509               TIME_WAIT           35618
TCP    192.168.2.158:7680     192:8052               ESTABLISHED         1652937
TCP    192.168.2.158:7680     192:8620               TIME_WAIT           98653
TCP    192.168.2.158:7680     192:8885               ESTABLISHED         7561291
TCP    192.168.2.158:7680     192:24732              ESTABLISHED         6705893
TCP    192.168.2.158:7680     192:25038              ESTABLISHED         7372306
TCP    192.168.2.158:7680     192:26929              ESTABLISHED         7280390
TCP    192.168.2.158:7680     192:46969              TIME_WAIT           31056
TCP    192.168.2.158:7680     192:46970              ESTABLISHED         22993
TCP    192.168.2.158:7680     192:48107              ESTABLISHED         7581069
TCP    192.168.2.158:7680     192:48129              ESTABLISHED         7422206
TCP    192.168.2.158:7680     192:49694              ESTABLISHED         7506803
TCP    192.168.2.158:7680     192:49695              ESTABLISHED         7502676
TCP    192.168.2.158:7680     192:50411              TIME_WAIT           80438
TCP    192.168.2.158:7680     192:51113              TIME_WAIT           50389
TCP    192.168.2.158:7680     192:51711              ESTABLISHED         6887569
TCP    192.168.2.158:7680     192:52183              ESTABLISHED         7364451
TCP    192.168.2.158:7680     192:52244              ESTABLISHED         7344790
TCP    192.168.2.158:7680     192:52291              TIME_WAIT           96502
TCP    192.168.2.158:7680     192:52498              TIME_WAIT           56618
TCP    192.168.2.158:7680     192:52874              ESTABLISHED         7365500
TCP    192.168.2.158:7680     192:52875              ESTABLISHED         7356621
TCP    192.168.2.158:7680     192:52875              ESTABLISHED         1
TCP    192.168.2.158:7680     192:53329              TIME_WAIT           102619
TCP    192.168.2.158:7680     192:53548              TIME_WAIT           77406
```

netstat-f : Displays Fully Qualified Domain Names (FQDN) for foreign addresses.

```
C:\Users\admin>netstat -f

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.2.158:796      192.168.2.3:49173      TIME_WAIT
  TCP    192.168.2.158:796      192.168.2.3:49221      TIME_WAIT
  TCP    192.168.2.158:796      192.168.2.3:49271      TIME_WAIT
  TCP    192.168.2.158:796      192.168.2.3:49320      TIME_WAIT
  TCP    192.168.2.158:796      192.168.2.3:65505      TIME_WAIT
  TCP    192.168.2.158:7680     10.0.0.125:59341       ESTABLISHED
  TCP    192.168.2.158:7680     192.168.2.20:60922     TIME_WAIT
  TCP    192.168.2.158:7680     192.168.2.31:54233     ESTABLISHED
  TCP    192.168.2.158:7680     192.168.2.31:63573     TIME_WAIT
  TCP    192.168.2.158:7680     192.168.2.32:63422     ESTABLISHED
  TCP    192.168.2.158:7680     192.168.2.32:63542     ESTABLISHED
  TCP    192.168.2.158:7680     192.168.2.32:65100     ESTABLISHED
  TCP    192.168.2.158:7680     192.168.2.35:52244     ESTABLISHED
  TCP    192.168.2.158:7680     192.168.2.35:55515     TIME_WAIT
  TCP    192.168.2.158:7680     192.168.2.35:55522     TIME_WAIT
  TCP    192.168.2.158:7680     192.168.2.35:55531     TIME_WAIT
  TCP    192.168.2.158:7680     192.168.2.35:59555     ESTABLISHED
  TCP    192.168.2.158:7680     192.168.2.36:49694     ESTABLISHED
  TCP    192.168.2.158:7680     192.168.2.36:49695     ESTABLISHED
  TCP    192.168.2.158:7680     192.168.2.36:56685     TIME_WAIT
  TCP    192.168.2.158:7680     192.168.2.36:63760     TIME_WAIT
  TCP    192.168.2.158:7680     192.168.2.36:63761     TIME_WAIT
  TCP    192.168.2.158:7680     192.168.2.36:63762     TIME_WAIT
  TCP    192.168.2.158:7680     192.168.2.38:56579     TIME_WAIT
  TCP    192.168.2.158:7680     192.168.2.39:51113     TIME_WAIT
  TCP    192.168.2.158:7680     192.168.2.39:58194     ESTABLISHED
  TCP    192.168.2.158:7680     192.168.2.39:58204     ESTABLISHED
  TCP    192.168.2.158:7680     192.168.2.39:58314     TIME_WAIT
  TCP    192.168.2.158:7680     192.168.2.39:65443     TIME_WAIT
  TCP    192.168.2.158:7680     192.168.2.40:56525     TIME_WAIT
  TCP    192.168.2.158:7680     192.168.2.40:56535     TIME_WAIT
  TCP    192.168.2.158:7680     192.168.2.40:56540     TIME_WAIT
```

Step 8: Display ARP Cache

What it does: Displays the Address Resolution Protocol (ARP) cache. This table maps IP addresses (like `192.168.1.5`) to physical device MAC addresses (like `00-14-22-01-23-45`) for devices on your immediate local network.
Why it is useful: It maps out the devices currently communicating with your PC on the local network, which is useful for diagnosing local connection drops, finding hidden devices, or identifying IP conflicts.



Step 9: Display Routing Table

What it does: Displays the IP routing table for your computer. This table contains the rules that dictate exactly where network traffic should be sent based on its destination IP address.
Why it is useful: Primarily used by network administrators, it helps diagnose complex networking issues, such as figuring out why you can reach a local network printer but cannot access the internet, or verifying that a VPN is routing your traffic correctly.

```
C:\Users\admin>route print
===========================================================================
Interface List
  8...10 ff e0 58 e6 95 ......Realtek PCIe GbE Family Controller
 17...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
  9...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.2.1    192.168.2.158     25
        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
      192.168.2.0    255.255.255.0         On-link     192.168.2.158    281
    192.168.2.158  255.255.255.255         On-link     192.168.2.158    281
    192.168.2.255  255.255.255.255         On-link     192.168.2.158    281
    192.168.177.0    255.255.255.0         On-link     192.168.177.1    291
    192.168.177.1  255.255.255.255         On-link     192.168.177.1    291
  192.168.177.255  255.255.255.255         On-link     192.168.177.1    291
    192.168.220.0    255.255.255.0         On-link     192.168.220.1    291
    192.168.220.1  255.255.255.255         On-link     192.168.220.1    291
  192.168.220.255  255.255.255.255         On-link     192.168.220.1    291
        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     192.168.177.1    291
        224.0.0.0        240.0.0.0         On-link     192.168.220.1    291
        224.0.0.0        240.0.0.0         On-link     192.168.2.158    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     192.168.177.1    291
  255.255.255.255  255.255.255.255         On-link     192.168.220.1    291
  255.255.255.255  255.255.255.255         On-link     192.168.2.158    281
===========================================================================
Persistent Routes:
  None
```

Step 10: Display Shared Folders

What it does: Lists all the folders, storage drives, and printers on your computer that are currently configured to be shared with other users on the network.
Why it is useful: It allows you to quickly audit what resources you are making publicly accessible to other network users, ensuring you aren't accidentally sharing sensitive data or exposing your file system unnecessarily.

```
  None

C:\Users\admin>net share

Share name   Resource                        Remark

-------------------------------------------------------------------------------
C$           C:\                             Default share
IPC$                                         Remote IPC
ADMIN$       C:\Windows                      Remote Admin
The command completed successfully.
```

3. ping

Description :

- Stands for Packet Internet Groper.
- Checks if source device is connected to destination device.

```
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

Options :

● ping -i : Change the interval between two ping packets. Default interval is 1ms. It can be increases or decreased by using this option by giving values greater than 1 and less than 0 respectively (-i 2 or -i 0.5)

```
C:\Users\admin>ping -i 2 www.google.com

Pinging www.google.com [142.251.153.119] with 32 bytes of data:
Reply from 115.117.107.149: TTL expired in transit.
Reply from 115.117.107.149: TTL expired in transit.
Reply from 115.117.107.149: TTL expired in transit.
Reply from 115.117.107.149: TTL expired in transit.

Ping statistics for 142.251.153.119:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

ping -s : Change the packet size while communication. Default size is 56 bytes + 28 bytes header (84 bytes)

```
C:\Users\admin>ping -s 2 www.google.com

Pinging www.google.com [142.251.157.119] with 32 bytes of data:
Reply from 142.251.157.119: bytes=32 time=120ms TTL=119
Reply from 142.251.157.119: bytes=32 time=43ms TTL=119
Reply from 142.251.157.119: bytes=32 time=343ms TTL=119
Reply from 142.251.157.119: bytes=32 time=98ms TTL=119

Ping statistics for 142.251.157.119:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 43ms, Maximum = 343ms, Average = 151ms
```

ping- c : Limit the number of ping packets being sent. Thus, if we give -c 2, transmission stops after transmitting 2 packets. (run on administrative mode)

```
C:\Windows\System32>ping -c 1 www.google.com

Pinging www.google.com [142.251.154.119] with 32 bytes of data:
Reply from 142.251.154.119: bytes=32 time=1ms TTL=119
Reply from 142.251.154.119: bytes=32 time=1ms TTL=119
Reply from 142.251.154.119: bytes=32 time=1ms TTL=119
Reply from 142.251.154.119: bytes=32 time=1ms TTL=119

Ping statistics for 142.251.154.119:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

ping -w : sets time (in seconds) for the
transmission after which transmission stops.

```
C:\Windows\System32>ping -w 2 www.google.com

Pinging www.google.com [142.251.154.119] with 32 bytes of data:
Reply from 142.251.154.119: bytes=32 time=1ms TTL=119
Reply from 142.251.154.119: bytes=32 time=1ms TTL=119
Reply from 142.251.154.119: bytes=32 time=1ms TTL=119
Reply from 142.251.154.119: bytes=32 time=1ms TTL=119

Ping statistics for 142.251.154.119:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

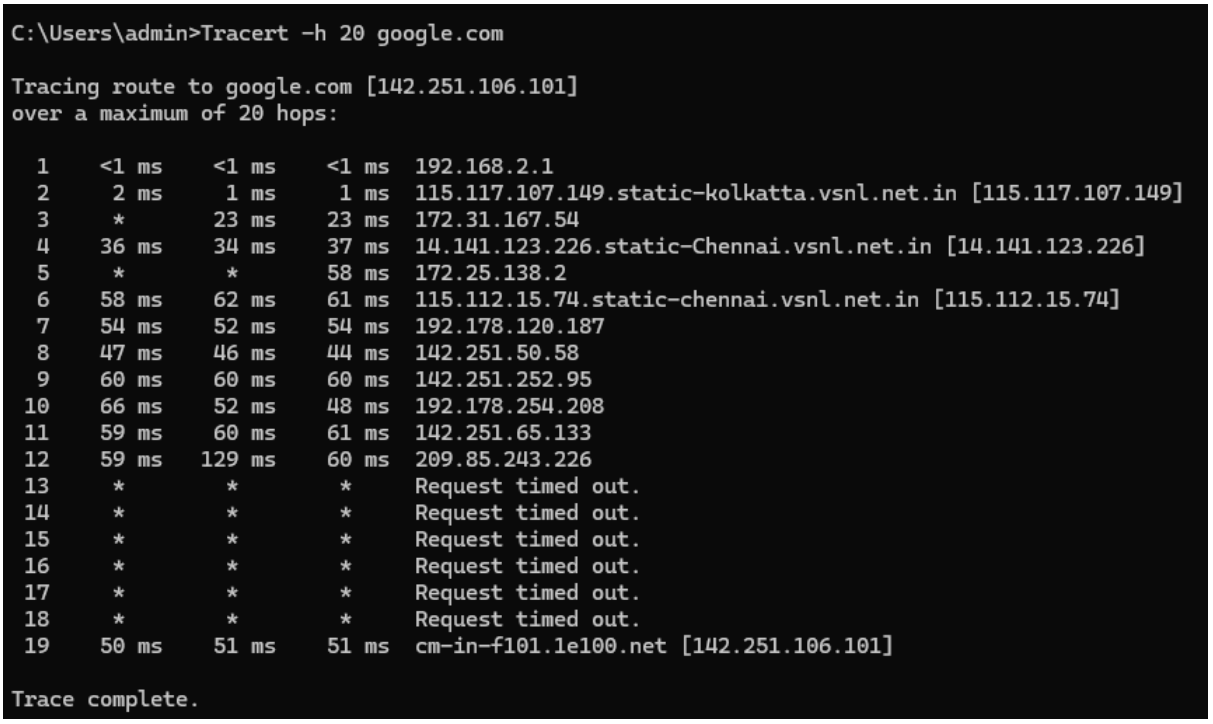
4. Tracert

Description :

- Stands for trace route.
- Shows details about the path that data packets follow from the source to the destination.

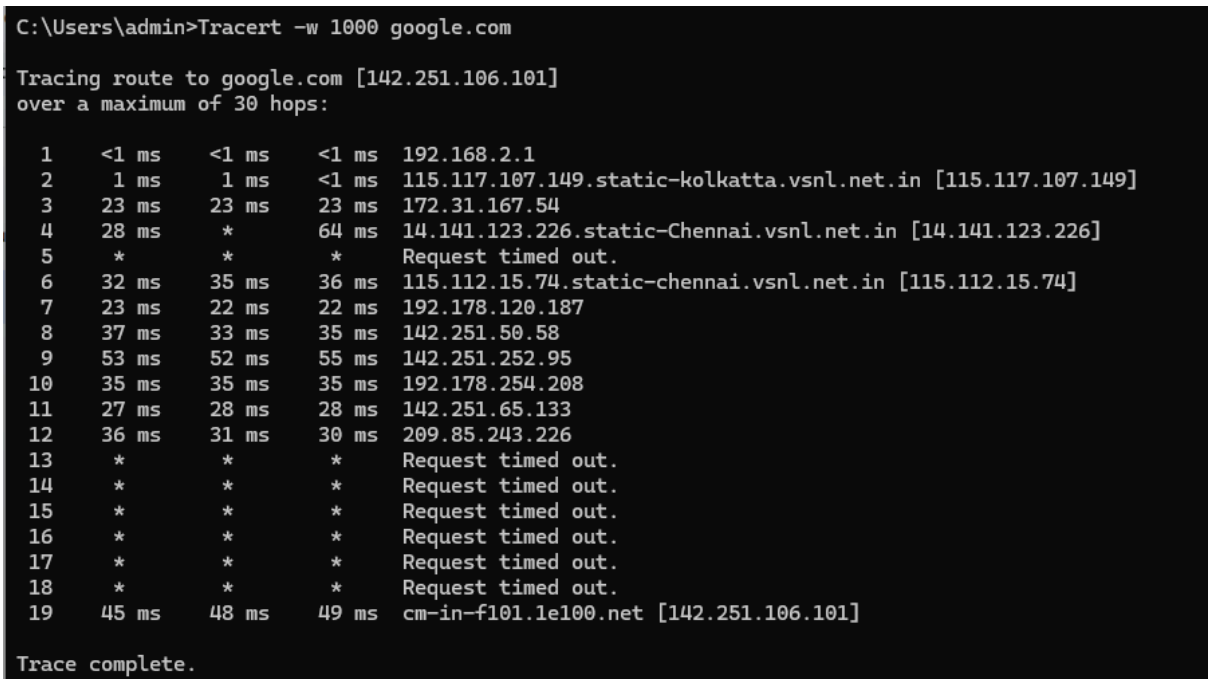
Options :

● **Tracert -h** : Specify a number after -h and only 2 hops taking to trace the route of data packets will be displayed.



```
C:\Users\admin>Tracert -h 20 google.com

Tracing route to google.com [142.251.106.101]
over a maximum of 20 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.2.1
  2     2 ms     1 ms     1 ms  115.117.107.149.static-kolkatta.vsnl.net.in [115.117.107.149]
  3     *       23 ms    23 ms  172.31.167.54
  4    36 ms    34 ms    37 ms  14.141.123.226.static-Chennai.vsnl.net.in [14.141.123.226]
  5     *        *       58 ms  172.25.138.2
  6    58 ms    62 ms    61 ms  115.112.15.74.static-chennai.vsnl.net.in [115.112.15.74]
  7    54 ms    52 ms    54 ms  192.178.120.187
  8    47 ms    46 ms    44 ms  142.251.50.58
  9    60 ms    60 ms    60 ms  142.251.252.95
 10    66 ms    52 ms    48 ms  192.178.254.208
 11    59 ms    60 ms    61 ms  142.251.65.133
 12    59 ms   129 ms    60 ms  209.85.243.226
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19    50 ms    51 ms    51 ms  cm-in-f101.1e100.net [142.251.106.101]

Trace complete.
```

● Tracert -w : specify the time (in milliseconds) to allow reply before time out.



```
C:\Users\admin>Tracert -w 1000 google.com

Tracing route to google.com [142.251.106.101]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.2.1
  2     1 ms     1 ms    <1 ms  115.117.107.149.static-kolkatta.vsnl.net.in [115.117.107.149]
  3    23 ms    23 ms    23 ms  172.31.167.54
  4    28 ms     *       64 ms  14.141.123.226.static-Chennai.vsnl.net.in [14.141.123.226]
  5     *        *        *     Request timed out.
  6    32 ms    35 ms    36 ms  115.112.15.74.static-chennai.vsnl.net.in [115.112.15.74]
  7    23 ms    22 ms    22 ms  192.178.120.187
  8    37 ms    33 ms    35 ms  142.251.50.58
  9    53 ms    52 ms    55 ms  142.251.252.95
 10    35 ms    35 ms    35 ms  192.178.254.208
 11    27 ms    28 ms    28 ms  142.251.65.133
 12    36 ms    31 ms    30 ms  209.85.243.226
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19    45 ms    48 ms    49 ms  cm-in-f101.1e100.net [142.251.106.101]

Trace complete.
```

● Tracert – 4 : Forces tracert to use only ip4 addresses for transmission.

8. Gpupdate

Description :

● Updates Group Policy settings manually.

Example: gpupdate /force.

```
C:\Users\admin>systeminfo

Host Name:                 IT-11
OS Name:                   Microsoft Windows 11 Pro
OS Version:                10.0.26200 N/A Build 26200
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          admin
Registered Organization:
Product ID:                00330-80000-00000-AA898
Original Install Date:     3/9/2026, 4:49:59 PM
System Boot Time:          7/9/2026, 10:14:30 AM
System Manufacturer:       Gigabyte Technology Co., Ltd.
System Model:              H610M K DDR4
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 151 Stepping 2 GenuineIntel ~2100 Mhz
BIOS Version:              American Megatrends International, LLC. FC, 12/14/2023
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+05:30) Sri Jayawardenepura
Total Physical Memory:     32,537 MB
Available Physical Memory: 23,284 MB
Virtual Memory: Max Size:  34,585 MB
Virtual Memory: Available: 24,386 MB
Virtual Memory: In Use:    10,199 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\IT-11
Hotfix(s):                 4 Hotfix(s) Installed.
```

9. Chkdsk

Description :

● Checks a disk for errors and attempts to fix them.

Example: chkdsk C: /f

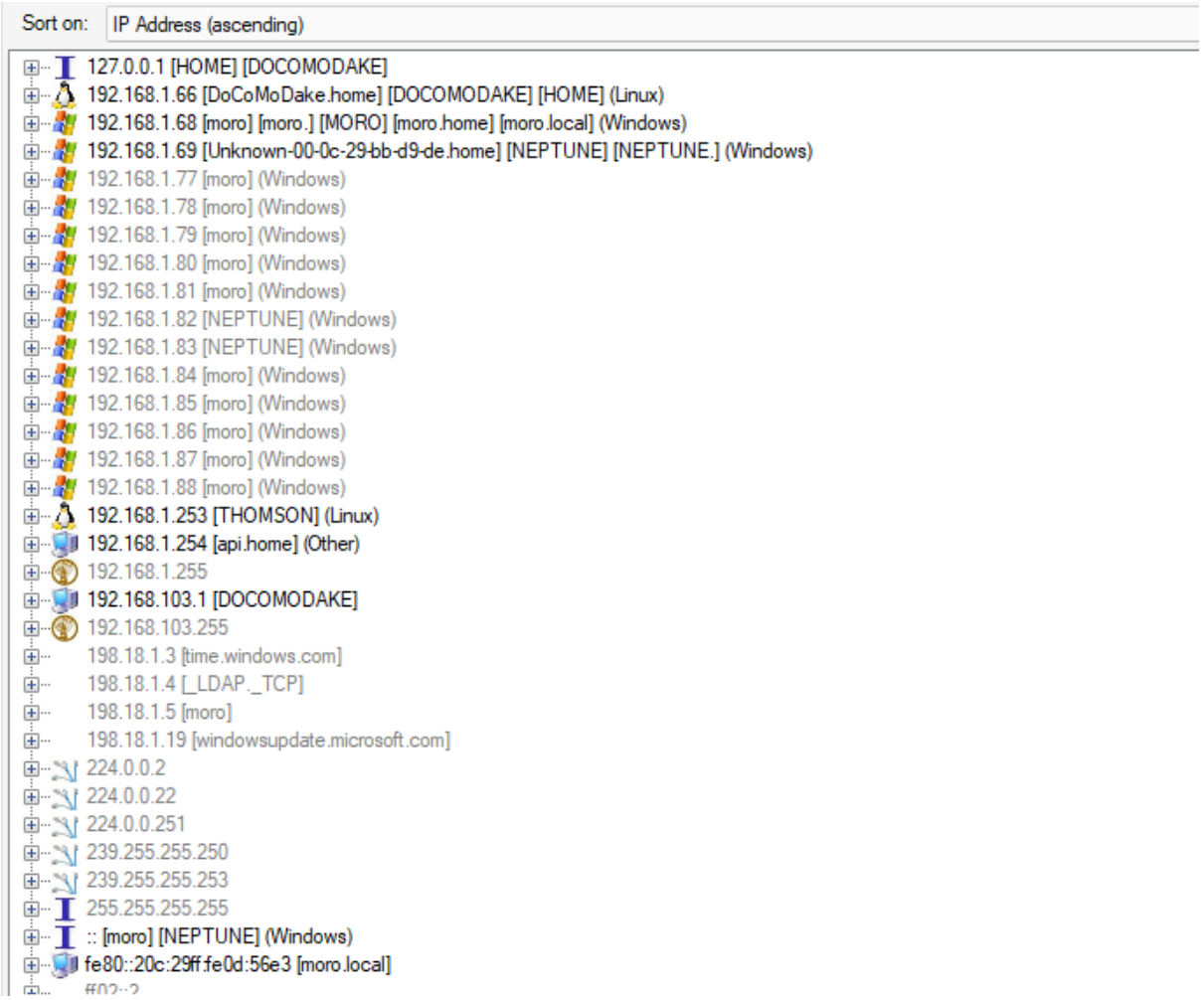
```
C:\Windows\System32>chkdsk
The type of the file system is NTFS.

WARNING!  /F parameter not specified.
Running CHKDSK in read-only mode.

Stage 1: Examining basic file system structure ...
  1403648 file records processed.
File verification completed.
 Phase duration (File record verification): 15.74 seconds.
  30497 large file records processed.
 Phase duration (Orphan file record recovery): 8.15 milliseconds.
  0 bad file records processed.
 Phase duration (Bad file record checking): 0.10 milliseconds.

Stage 2: Examining file name linkage ...
  520 reparse records processed.
  1928442 index entries processed.
Index verification completed.
 Phase duration (Index verification): 22.89 seconds.
  0 unindexed files scanned.
 Phase duration (Orphan reconnection): 5.60 seconds.
  0 unindexed files recovered to lost and found.
 Phase duration (Orphan recovery to lost and found): 0.11 milliseconds.
  520 reparse records processed.
 Phase duration (Reparse point and Object ID verification): 3.25 milliseconds.

Stage 3: Examining security descriptors ...
Security descriptor verification completed.
 Phase duration (Security descriptor verification): 16.59 milliseconds.
  262398 data files processed.
 Phase duration (Data attribute verification): 0.31 milliseconds.
CHKDSK is verifying Usn Journal...
  36996120 USN bytes processed.
Usn Journal verification completed.
 Phase duration (USN journal verification): 88.76 milliseconds.

Windows has scanned the file system and found no problems.
No further action is required.

 999276543 KB total disk space.
 239675192 KB in 1102099 files.
    750928 KB in 262399 indexes.
         0 KB in bad sectors.
   1541463 KB in use by the system.
     65536 KB occupied by the log file.
```

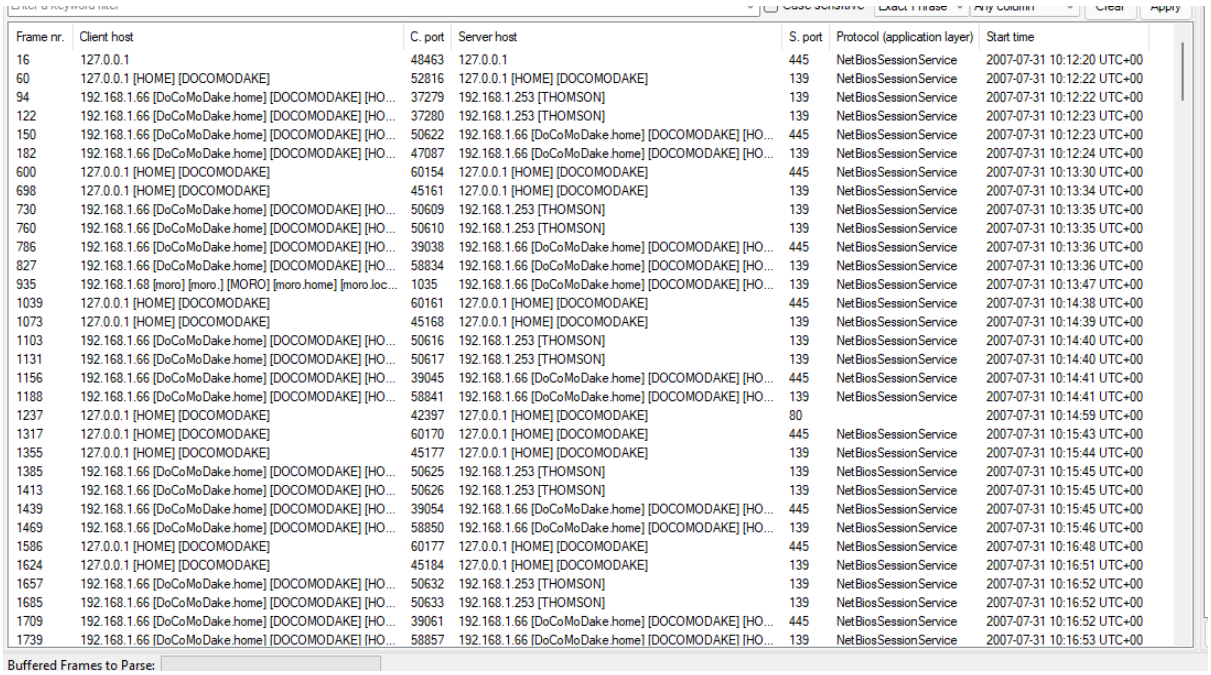
Tool : Network Miner

Use:

NetworkMiner is an open-source Network

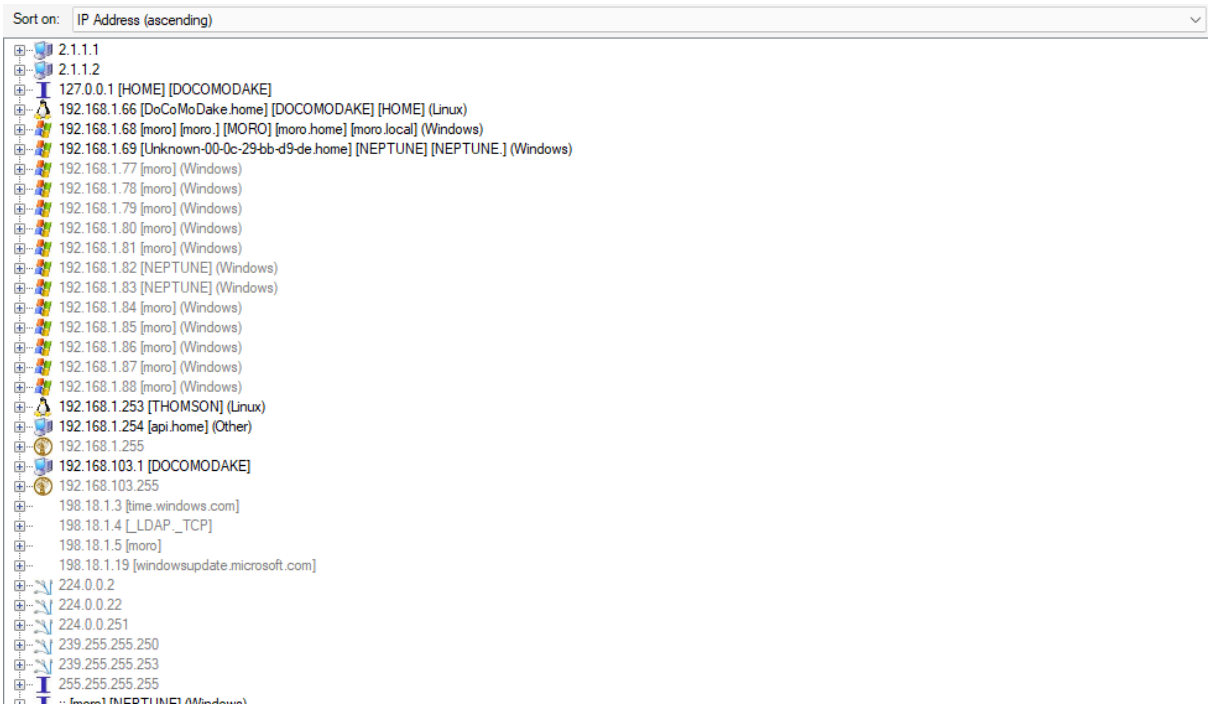
Forensic Analysis Tool (NFAT). While tools like Wireshark are designed to look at network traffic packet-by-packet, NetworkMiner is designed to be

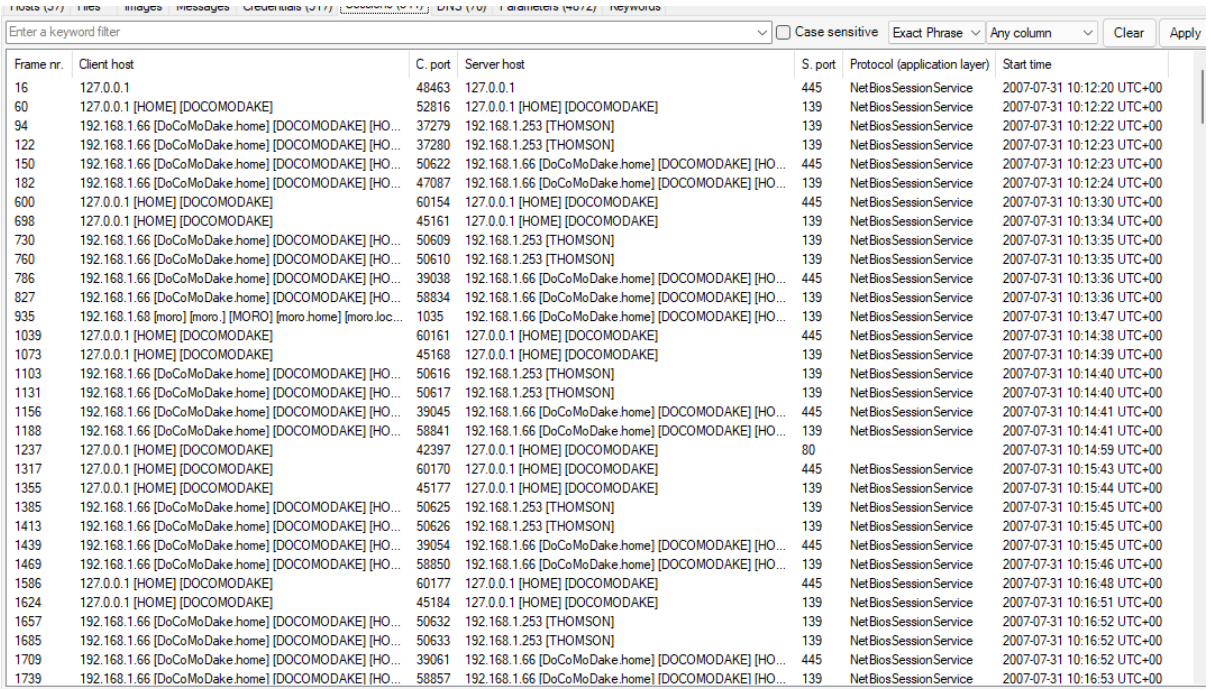




Frame nr.	Client host	C. port	Server host	S. port	Protocol (application layer)	Start time
16	127.0.0.1	48463	127.0.0.1	445	NetBiosSessionService	2007-07-31 10:12:20 UTC+00
60	127.0.0.1 [HOME] [DOCOMODAKE]	52816	127.0.0.1 [HOME] [DOCOMODAKE]	139	NetBiosSessionService	2007-07-31 10:12:22 UTC+00
94	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	37279	192.168.1.253 [THOMSON]	139	NetBiosSessionService	2007-07-31 10:12:22 UTC+00
122	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	37280	192.168.1.253 [THOMSON]	139	NetBiosSessionService	2007-07-31 10:12:23 UTC+00
150	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	50622	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	445	NetBiosSessionService	2007-07-31 10:12:23 UTC+00
182	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	47087	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	139	NetBiosSessionService	2007-07-31 10:12:24 UTC+00
600	127.0.0.1 [HOME] [DOCOMODAKE]	60154	127.0.0.1 [HOME] [DOCOMODAKE]	445	NetBiosSessionService	2007-07-31 10:13:30 UTC+00
698	127.0.0.1 [HOME] [DOCOMODAKE]	45161	127.0.0.1 [HOME] [DOCOMODAKE]	139	NetBiosSessionService	2007-07-31 10:13:34 UTC+00
730	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	50609	192.168.1.253 [THOMSON]	139	NetBiosSessionService	2007-07-31 10:13:35 UTC+00
760	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	50610	192.168.1.253 [THOMSON]	139	NetBiosSessionService	2007-07-31 10:13:35 UTC+00
786	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	39038	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	445	NetBiosSessionService	2007-07-31 10:13:36 UTC+00
827	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	58834	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	139	NetBiosSessionService	2007-07-31 10:13:36 UTC+00
935	192.168.1.68 [moro] [moro.] [MORO] [moro.home] [moro.loc...	1035	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	139	NetBiosSessionService	2007-07-31 10:13:47 UTC+00
1039	127.0.0.1 [HOME] [DOCOMODAKE]	60161	127.0.0.1 [HOME] [DOCOMODAKE]	445	NetBiosSessionService	2007-07-31 10:14:38 UTC+00
1073	127.0.0.1 [HOME] [DOCOMODAKE]	45168	127.0.0.1 [HOME] [DOCOMODAKE]	139	NetBiosSessionService	2007-07-31 10:14:39 UTC+00
1103	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	50616	192.168.1.253 [THOMSON]	139	NetBiosSessionService	2007-07-31 10:14:40 UTC+00
1131	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	50617	192.168.1.253 [THOMSON]	139	NetBiosSessionService	2007-07-31 10:14:40 UTC+00
1156	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	39045	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	445	NetBiosSessionService	2007-07-31 10:14:41 UTC+00
1188	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	58841	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	139	NetBiosSessionService	2007-07-31 10:14:41 UTC+00
1237	127.0.0.1 [HOME] [DOCOMODAKE]	42397	127.0.0.1 [HOME] [DOCOMODAKE]	80		2007-07-31 10:14:59 UTC+00
1317	127.0.0.1 [HOME] [DOCOMODAKE]	60170	127.0.0.1 [HOME] [DOCOMODAKE]	445	NetBiosSessionService	2007-07-31 10:15:43 UTC+00
1355	127.0.0.1 [HOME] [DOCOMODAKE]	45177	127.0.0.1 [HOME] [DOCOMODAKE]	139	NetBiosSessionService	2007-07-31 10:15:44 UTC+00
1385	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	50625	192.168.1.253 [THOMSON]	139	NetBiosSessionService	2007-07-31 10:15:45 UTC+00
1413	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	50626	192.168.1.253 [THOMSON]	139	NetBiosSessionService	2007-07-31 10:15:45 UTC+00
1439	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	39054	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	445	NetBiosSessionService	2007-07-31 10:15:45 UTC+00
1469	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	58850	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	139	NetBiosSessionService	2007-07-31 10:15:46 UTC+00
1586	127.0.0.1 [HOME] [DOCOMODAKE]	60177	127.0.0.1 [HOME] [DOCOMODAKE]	445	NetBiosSessionService	2007-07-31 10:16:48 UTC+00
1624	127.0.0.1 [HOME] [DOCOMODAKE]	45184	127.0.0.1 [HOME] [DOCOMODAKE]	139	NetBiosSessionService	2007-07-31 10:16:51 UTC+00
1657	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	50632	192.168.1.253 [THOMSON]	139	NetBiosSessionService	2007-07-31 10:16:52 UTC+00
1685	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	50633	192.168.1.253 [THOMSON]	139	NetBiosSessionService	2007-07-31 10:16:52 UTC+00
1709	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	39061	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	445	NetBiosSessionService	2007-07-31 10:16:52 UTC+00
1739	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	58857	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	139	NetBiosSessionService	2007-07-31 10:16:53 UTC+00

Buffered Frames to Parse:





Hosts (37) Files Images Messages Credentials (317) Sessions (211) DNS (70) Parameters (4072) Keywords

Enter a keyword filter | Case sensitive | Exact Phrase | Any column | Clear | Apply

Frame nr.	Client host	C. port	Server host	S. port	Protocol (application layer)	Start time
16	127.0.0.1	48463	127.0.0.1	445	NetBiosSessionService	2007-07-31 10:12:20 UTC+00
60	127.0.0.1 [HOME] [DOCOMODAKE]	52816	127.0.0.1 [HOME] [DOCOMODAKE]	139	NetBiosSessionService	2007-07-31 10:12:22 UTC+00
94	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	37279	192.168.1.253 [THOMSON]	139	NetBiosSessionService	2007-07-31 10:12:22 UTC+00
122	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	37280	192.168.1.253 [THOMSON]	139	NetBiosSessionService	2007-07-31 10:12:23 UTC+00
150	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	50622	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	445	NetBiosSessionService	2007-07-31 10:12:23 UTC+00
182	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	47087	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	139	NetBiosSessionService	2007-07-31 10:12:24 UTC+00
600	127.0.0.1 [HOME] [DOCOMODAKE]	60154	127.0.0.1 [HOME] [DOCOMODAKE]	445	NetBiosSessionService	2007-07-31 10:13:30 UTC+00
698	127.0.0.1 [HOME] [DOCOMODAKE]	45161	127.0.0.1 [HOME] [DOCOMODAKE]	139	NetBiosSessionService	2007-07-31 10:13:34 UTC+00
730	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	50609	192.168.1.253 [THOMSON]	139	NetBiosSessionService	2007-07-31 10:13:35 UTC+00
760	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	50610	192.168.1.253 [THOMSON]	139	NetBiosSessionService	2007-07-31 10:13:35 UTC+00
786	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	39038	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	445	NetBiosSessionService	2007-07-31 10:13:36 UTC+00
827	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	58834	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	139	NetBiosSessionService	2007-07-31 10:13:36 UTC+00
935	192.168.1.68 [moro] [moro.] [MORO] [moro.home] [moro.loc...	1035	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	139	NetBiosSessionService	2007-07-31 10:13:47 UTC+00
1039	127.0.0.1 [HOME] [DOCOMODAKE]	60161	127.0.0.1 [HOME] [DOCOMODAKE]	445	NetBiosSessionService	2007-07-31 10:14:38 UTC+00
1073	127.0.0.1 [HOME] [DOCOMODAKE]	45168	127.0.0.1 [HOME] [DOCOMODAKE]	139	NetBiosSessionService	2007-07-31 10:14:39 UTC+00
1103	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	50616	192.168.1.253 [THOMSON]	139	NetBiosSessionService	2007-07-31 10:14:40 UTC+00
1131	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	50617	192.168.1.253 [THOMSON]	139	NetBiosSessionService	2007-07-31 10:14:40 UTC+00
1156	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	39045	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	445	NetBiosSessionService	2007-07-31 10:14:41 UTC+00
1188	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	58841	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	139	NetBiosSessionService	2007-07-31 10:14:41 UTC+00
1237	127.0.0.1 [HOME] [DOCOMODAKE]	42397	127.0.0.1 [HOME] [DOCOMODAKE]	80		2007-07-31 10:14:59 UTC+00
1317	127.0.0.1 [HOME] [DOCOMODAKE]	60170	127.0.0.1 [HOME] [DOCOMODAKE]	445	NetBiosSessionService	2007-07-31 10:15:43 UTC+00
1355	127.0.0.1 [HOME] [DOCOMODAKE]	45177	127.0.0.1 [HOME] [DOCOMODAKE]	139	NetBiosSessionService	2007-07-31 10:15:44 UTC+00
1385	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	50625	192.168.1.253 [THOMSON]	139	NetBiosSessionService	2007-07-31 10:15:45 UTC+00
1413	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	50626	192.168.1.253 [THOMSON]	139	NetBiosSessionService	2007-07-31 10:15:45 UTC+00
1439	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	39054	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	445	NetBiosSessionService	2007-07-31 10:15:45 UTC+00
1469	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	58850	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	139	NetBiosSessionService	2007-07-31 10:15:46 UTC+00
1586	127.0.0.1 [HOME] [DOCOMODAKE]	60177	127.0.0.1 [HOME] [DOCOMODAKE]	445	NetBiosSessionService	2007-07-31 10:16:48 UTC+00
1624	127.0.0.1 [HOME] [DOCOMODAKE]	45184	127.0.0.1 [HOME] [DOCOMODAKE]	139	NetBiosSessionService	2007-07-31 10:16:51 UTC+00
1657	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	50632	192.168.1.253 [THOMSON]	139	NetBiosSessionService	2007-07-31 10:16:52 UTC+00
1685	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	50633	192.168.1.253 [THOMSON]	139	NetBiosSessionService	2007-07-31 10:16:52 UTC+00
1709	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	39061	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	445	NetBiosSessionService	2007-07-31 10:16:52 UTC+00
1739	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	58857	192.168.1.66 [DoCoMoDake.home] [DOCOMODAKE] [HO...	139	NetBiosSessionService	2007-07-31 10:16:53 UTC+00