My Network Project

INTRO TO CYCBER

STUDENT : MUHAMMAD FEROZ (S10)

Scope

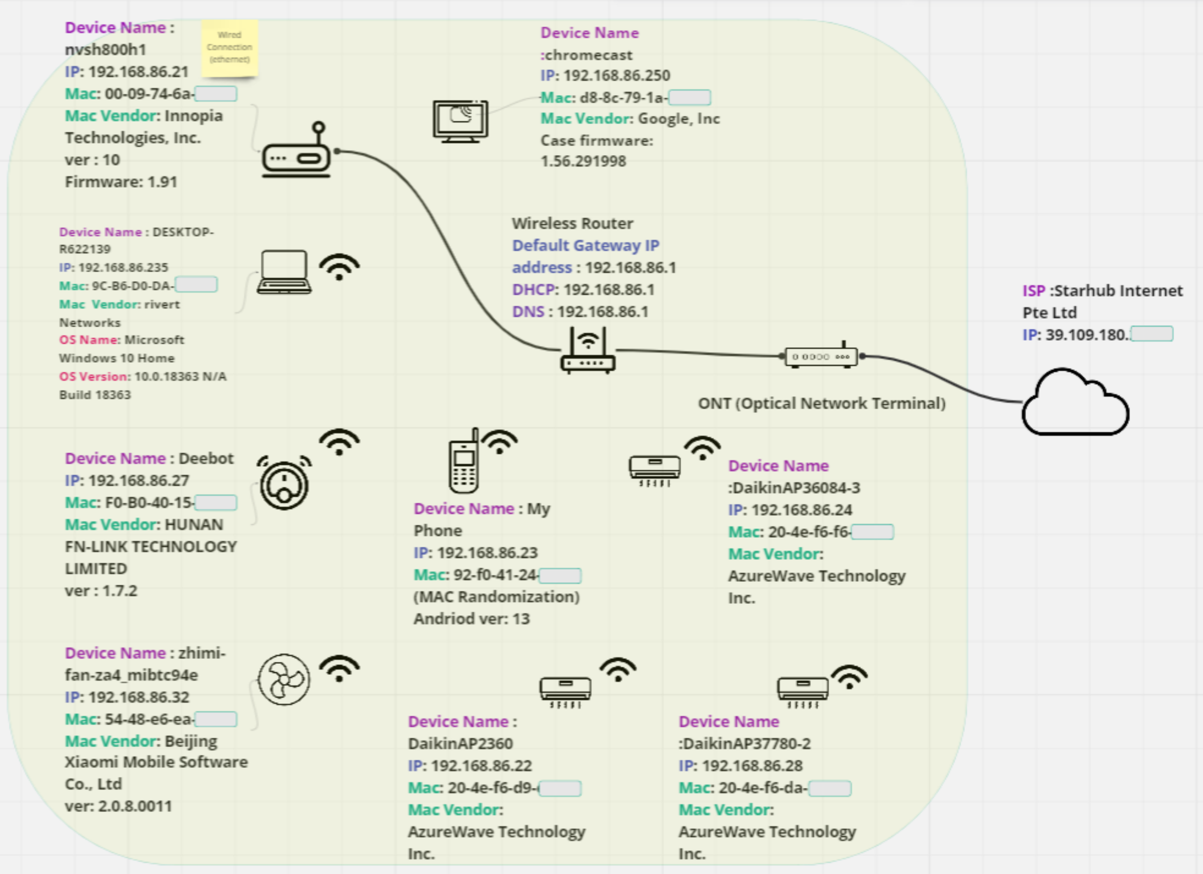
- Understanding the Basic Networking and Networking protocols
- Ability to map network devices within an internal network
- Comfortability to use Command prompt and other methods to discover internal networks
- Comfortability to use 3rd party tool (Wireshark) to analysis network traffic within the internal and external domains.

Content Page

Scope
Content Page
Home Network Map
Commands and Websites
    Internet Service Provider (ISP)
        Default Gateway
        DHCP and DNS
    Primary Device - Notebook
        Host and Network Details
        Host MAC Details
        Host Network Adaptor Vendor
    Devices within local network
    Other Device within local network (routing table)
        MAC Randomization
Wireshark
    Scenario 1 -

Home Network Map

Network diagram below depicts a setup of a home network, where internet service is provided by a ISP through an ONT. A router is used to manage the local area network (LAN) and simultaneously acting as a Default gateway to other networks outside the LAN. 8 out the 9 nodes shares data wirelessly and one node directly connected via ethernet to the router.



Device Name : nvsh800h1
IP: 192.168.86.21
Mac: 00-09-74-6a-[redacted]
Mac Vendor: Innopia Technologies, Inc.
ver : 10
Firmware: 1.91

Device Name :chromecast
IP: 192.168.86.250
Mac: d8-8c-79-1a-[redacted]
Mac Vendor: Google, Inc
Case firmware: 1.56.291998

Device Name : DESKTOP-R622139
IP: 192.168.86.235
Mac: 9C-B6-D0-DA-[redacted]
Mac Vendor: rivert Networks
OS Name: Microsoft Windows 10 Home
OS Version: 10.0.18363 N/A Build 18363

Wireless Router
Default Gateway IP address : 192.168.86.1
DHCP: 192.168.86.1
DNS : 192.168.86.1

ISP :Starhub Internet Pte Ltd
IP: 39.109.180.[redacted]

Device Name : Deebot
IP: 192.168.86.27
Mac: F0-B0-40-15-[redacted]
Mac Vendor: HUNAN FN-LINK TECHNOLOGY LIMITED
ver : 1.7.2

Device Name : My Phone
IP: 192.168.86.23
Mac: 92-f0-41-24-[redacted]
(MAC Randomization)
Andriod ver: 13

Device Name :DaikinAP36084-3
IP: 192.168.86.24
Mac: 20-4e-f6-f6-[redacted]
Mac Vendor: AzureWave Technology Inc.

Device Name : zhimi-fan-za4_mibtc94e
IP: 192.168.86.32
Mac: 54-48-e6-ea-[redacted]
Mac Vendor: Beijing Xiaomi Mobile Software Co., Ltd
ver: 2.0.8.0011

Device Name : DaikinAP2360
IP: 192.168.86.22
Mac: 20-4e-f6-d9-[redacted]
Mac Vendor: AzureWave Technology Inc.

Device Name :DaikinAP37780-2
IP: 192.168.86.28
Mac: 20-4e-f6-da-[redacted]
Mac Vendor: AzureWave Technology Inc.

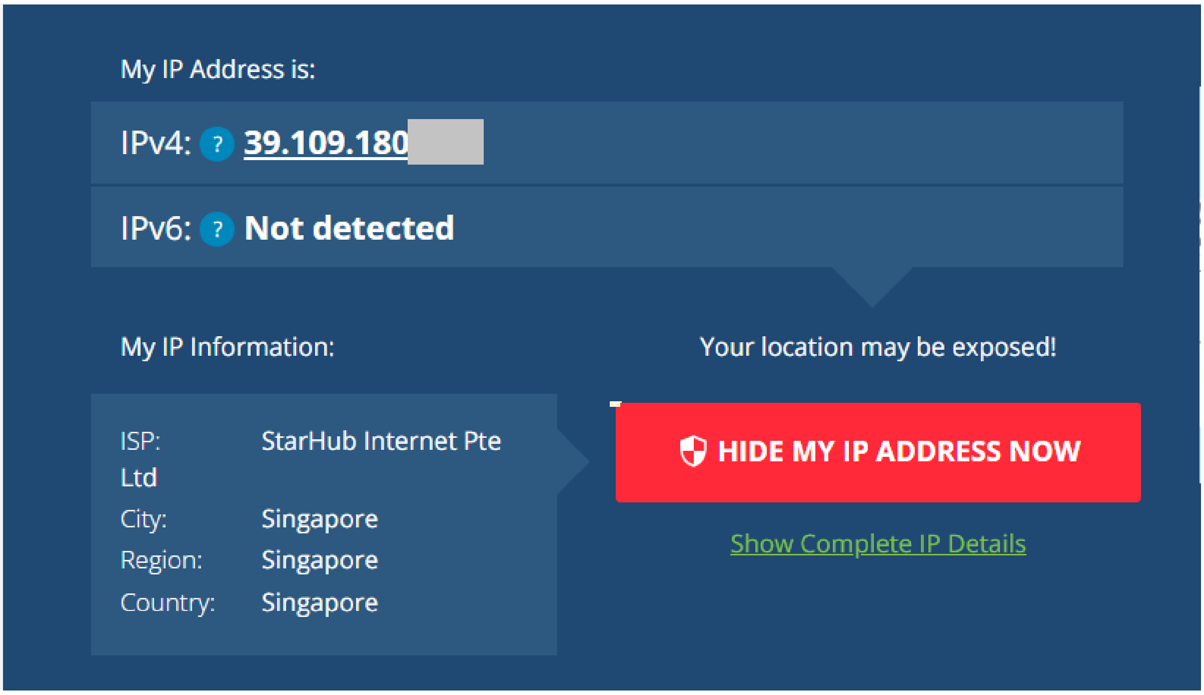
Credit : digram drawn in miro, icons obtained from Google Images

💡 MAC address last two bytes has been covered for privacy purpose as the Vendor details has been exposed.

Commands and Websites

Internet Service Provider (ISP)

External IP address which is the Internet Protocol address provided by the ISP. The following site was used to retrieve the IPv4 address and the service provider.



My IP Address is:

IPv4: ? 39.109.180[redacted]

IPv6: ? Not detected

My IP Information:

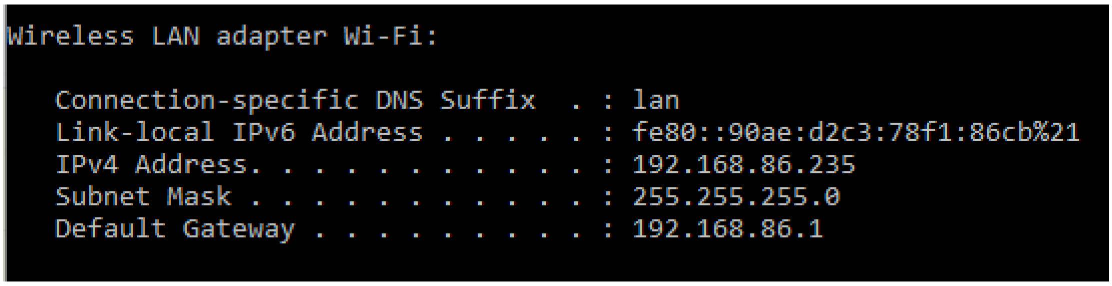
ISP: StarHub Internet Pte Ltd
City: Singapore
Region: Singapore
Country: Singapore

Your location may be exposed!

Link - https://whatismyipaddress.com/

Default Gateway

The default gateway is a physical hardware in this case the Home’s Wi-Fi router which separates the home network from the Internet (other networks). The command “**ipconfig**” is used to determine the IP address of the Default gateway.

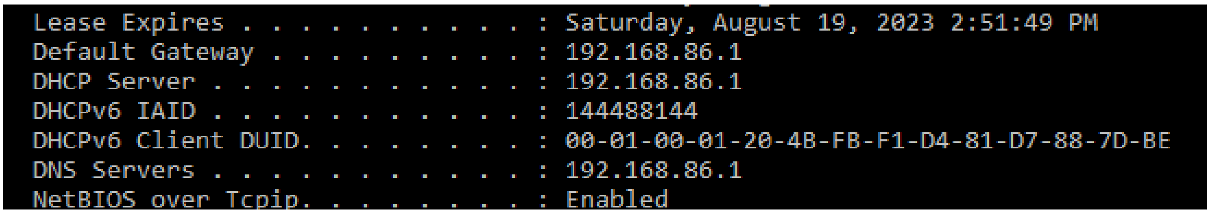


```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : lan
   Link-local IPv6 Address . . . . . : fe80::90ae:d2c3:78f1:86cb%21
   IPv4 Address. . . . . . . . . . . : 192.168.86.235
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.86.1
```

Credit - https://nordvpn.com/blog/what-is-a-default-gateway/#:~:text=Default gateway definition,is the Wi-Fi router.

DHCP and DNS

The DHCP (Dynamic Host Configuration Protocol) is a protocol that automatically provides a device /host with an unique IP address to identify itself within a network. The DNS (Domain Name System) assist to translate internet Domain names (understandable to end user) into IP address. Command "**ipconfig /all**" is is use to determine both DHCP and DNS



```
   Lease Expires . . . . . . . . . . : Saturday, August 19, 2023 2:51:49 PM
   Default Gateway . . . . . . . . . : 192.168.86.1
   DHCP Server . . . . . . . . . . . : 192.168.86.1
   DHCPv6 IAID . . . . . . . . . . . : 144488144
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-20-4B-FB-F1-D4-81-D7-88-7D-BE
   DNS Servers . . . . . . . . . . . : 192.168.86.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Credit :*https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top*

https://aws.amazon.com/route53/what-is-dns/

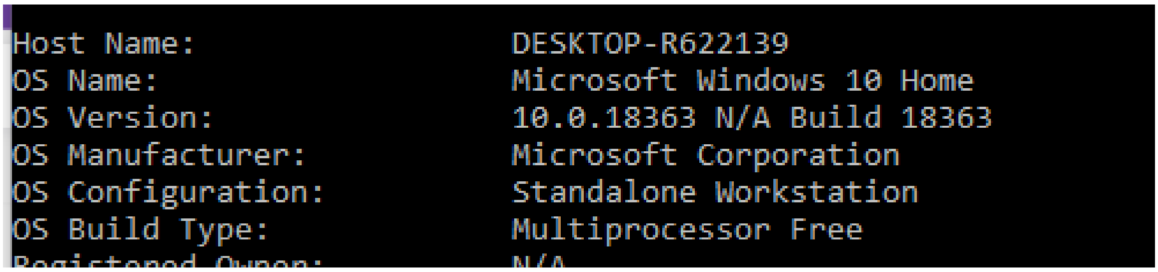
Primary Device - Notebook

Host and Network Details

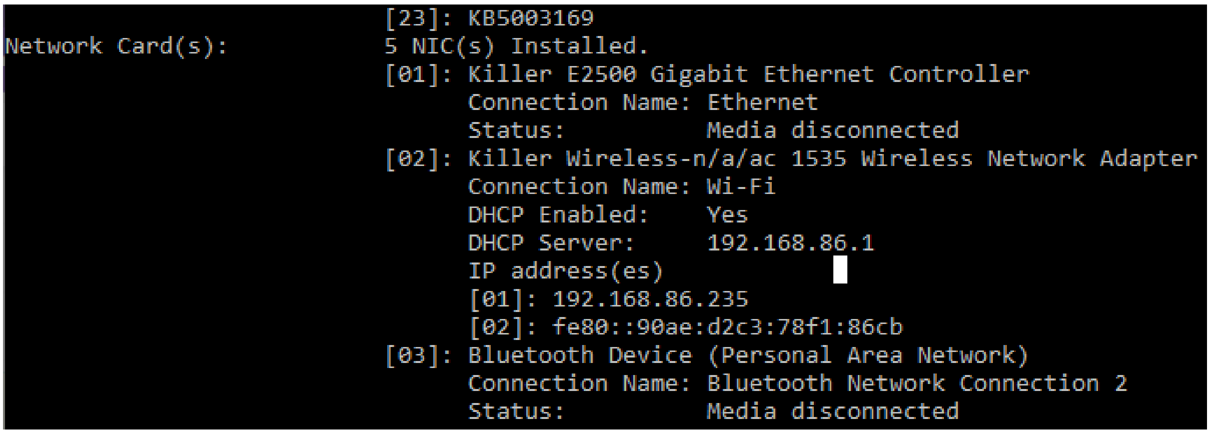
The following device was primarily used to discover the Home network. Details of the device can be retrieved using the command "systeminfo". Details such a computer name, operating system and hardware properties are listed for analysis.

Name	Values	Description
Host Name:	DESKTOP-R622139	Name of the host terminal where the command is executed from
OS Name	Microsoft Windows 10 Home	Operating System installed in host
OS Version	10.0.18363 N/A Build 18363	Version of OS in host

Name	Values	Description
Network Card(s):	Killer Wireless-n/a/ac 1535 Wireless Network Adapter	It provides information about the network card.
	Connection Name: Wi-Fi	Wireless Network adapter
	DHCP Enabled: Yes	Detection of enablement of DHCP
	DHCP Server: 192.168.86.1	DHCP IP
	IP address(es) [01]:192.168.86.235 [02]: fe80::90ae:d2c3:78f1:86cb	IP address assigned to the Host by DHCP



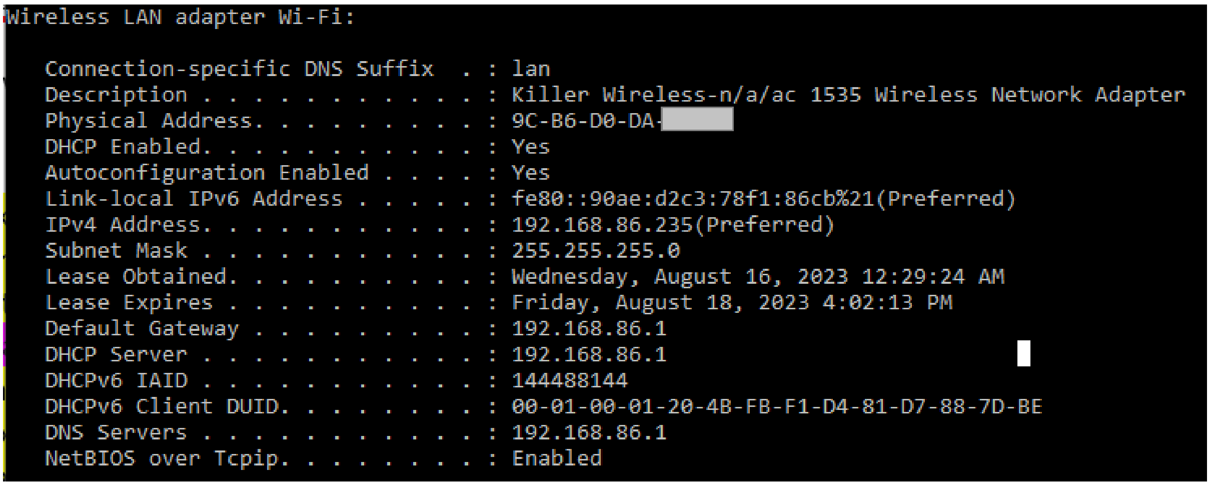
```
Host Name:                 DESKTOP-R622139
OS Name:                   Microsoft Windows 10 Home
OS Version:                10.0.18363 N/A Build 18363
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          N/A
```



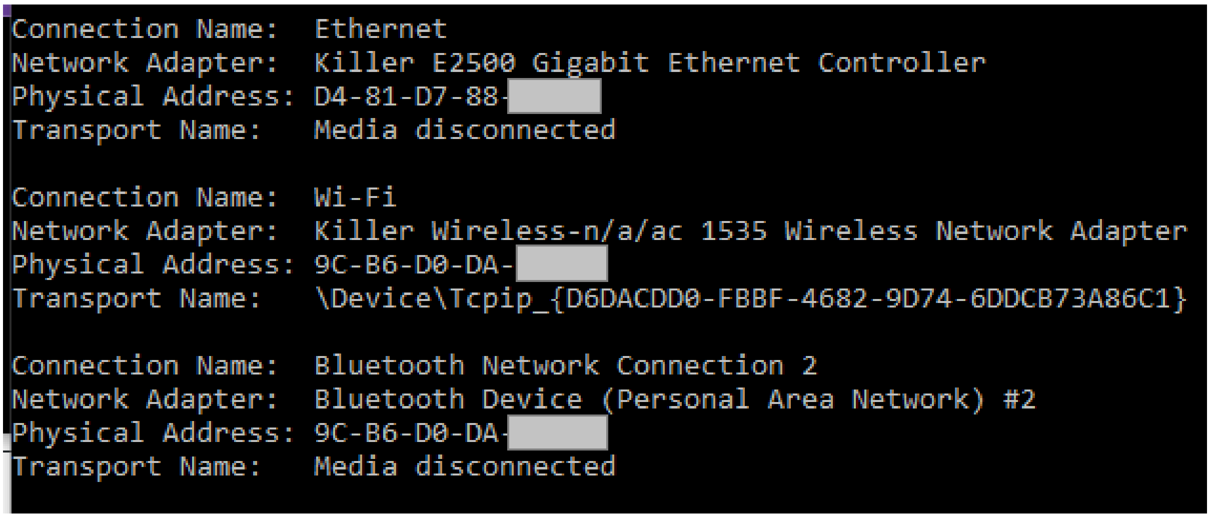
```
                           [23]: KB5003169
Network Card(s):           5 NIC(s) Installed.
                           [01]: Killer E2500 Gigabit Ethernet Controller
                                 Connection Name: Ethernet
                                 Status:          Media disconnected
                           [02]: Killer Wireless-n/a/ac 1535 Wireless Network Adapter
                                 Connection Name: Wi-Fi
                                 DHCP Enabled:    Yes
                                 DHCP Server:     192.168.86.1
                                 IP address(es)
                                 [01]: 192.168.86.235
                                 [02]: fe80::90ae:d2c3:78f1:86cb
                           [03]: Bluetooth Device (Personal Area Network)
                                 Connection Name: Bluetooth Network Connection 2
                                 Status:          Media disconnected
```

Host MAC Details

Command “**ipconfig /all**” provides the MAC address of the network adapter or a more comprehensive search with the command “**getmac /v /fo list**” to view all MAC addresses within the host system if one is not familiar with the Transport name with “**getmac**” command.



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : lan
   Description . . . . . . . . . . . : Killer Wireless-n/a/ac 1535 Wireless Network Adapter
   Physical Address. . . . . . . . . : 9C-B6-D0-DA-[redacted]
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::90ae:d2c3:78f1:86cb%21(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.86.235(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, August 16, 2023 12:29:24 AM
   Lease Expires . . . . . . . . . . : Friday, August 18, 2023 4:02:13 PM
   Default Gateway . . . . . . . . . : 192.168.86.1
   DHCP Server . . . . . . . . . . . : 192.168.86.1
   DHCPv6 IAID . . . . . . . . . . . : 144488144
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-20-4B-FB-F1-D4-81-D7-88-7D-BE
   DNS Servers . . . . . . . . . . . : 192.168.86.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```



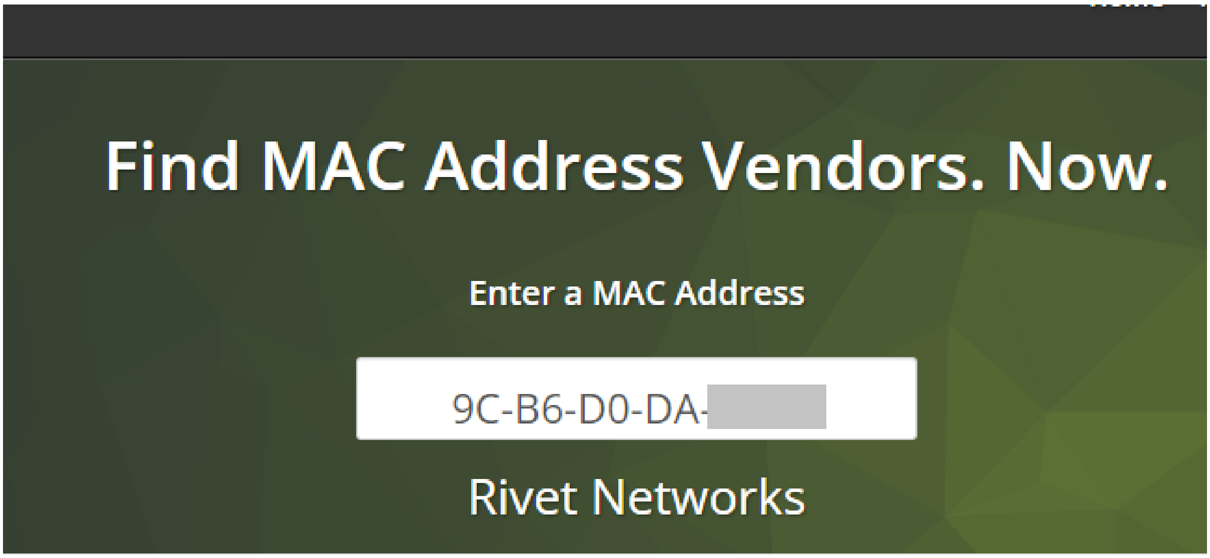
```
Connection Name:  Ethernet
Network Adapter:  Killer E2500 Gigabit Ethernet Controller
Physical Address: D4-81-D7-88-[redacted]
Transport Name:   Media disconnected

Connection Name:  Wi-Fi
Network Adapter:  Killer Wireless-n/a/ac 1535 Wireless Network Adapter
Physical Address: 9C-B6-D0-DA-[redacted]
Transport Name:   \Device\Tcpip_{D6DACDD0-FBBF-4682-9D74-6DDCB73A86C1}

Connection Name:  Bluetooth Network Connection 2
Network Adapter:  Bluetooth Device (Personal Area Network) #2
Physical Address: 9C-B6-D0-DA-[redacted]
Transport Name:   Media disconnected
```

Credit : https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/systeminfo

https://networking.grok.lsu.edu/article.aspx?articleid=15960

Host Network Adaptor Vendor

The vendor of the network card for above mentioned the MAC address can be determined via an online platform.



Find MAC Address Vendors. Now.

Enter a MAC Address

9C-B6-D0-DA-[redacted]

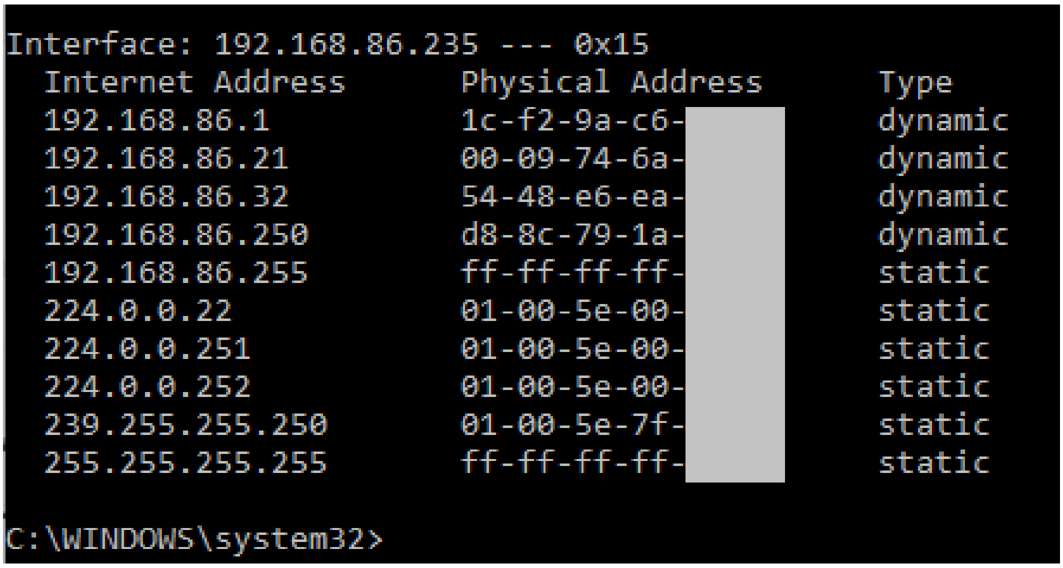
Rivet Networks

Credit : https://macvendors.com/

Devices within local network

ARP - Address Resolution Protocol is a networking protocol that is used to map a network address, such as an IP address, to a physical (MAC) address. ARP table is a cache that stores the mapping of IP addresses to their corresponding MAC addresses in the target system. Command “**arp -a**” displays IP address, MAC address and Type (Dynamic and Static)

The following list is available from the arp command.



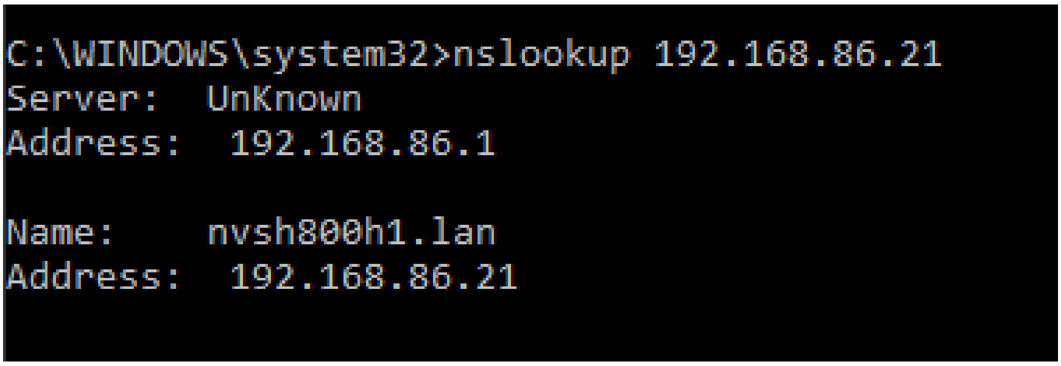
```
Interface: 192.168.86.235 --- 0x15
  Internet Address      Physical Address      Type
  192.168.86.1          1c-f2-9a-c6-[redacted]     dynamic
  192.168.86.21         00-09-74-6a-          dynamic
  192.168.86.32         54-48-e6-ea-          dynamic
  192.168.86.250        d8-8c-79-1a-          dynamic
  192.168.86.255        ff-ff-ff-ff-          static
  224.0.0.22            01-00-5e-00-          static
  224.0.0.251           01-00-5e-00-          static
  224.0.0.252           01-00-5e-00-          static
  239.255.255.250       01-00-5e-7f-          static
  255.255.255.255       ff-ff-ff-ff-          static

C:\WINDOWS\system32>
```

IP address	MAC	Note
192.168.86.1	**1c-f2-9a-c6**	Wireless router
192.168.86.21	**00-09-74-6a**	**nvsh800h1**
192.168.86.32	**54-48-e6-ea**	**zhimi-fan-za4_mibtc94e**
192.168.86.250	**d8-8c-79-1a**	**chromecast**

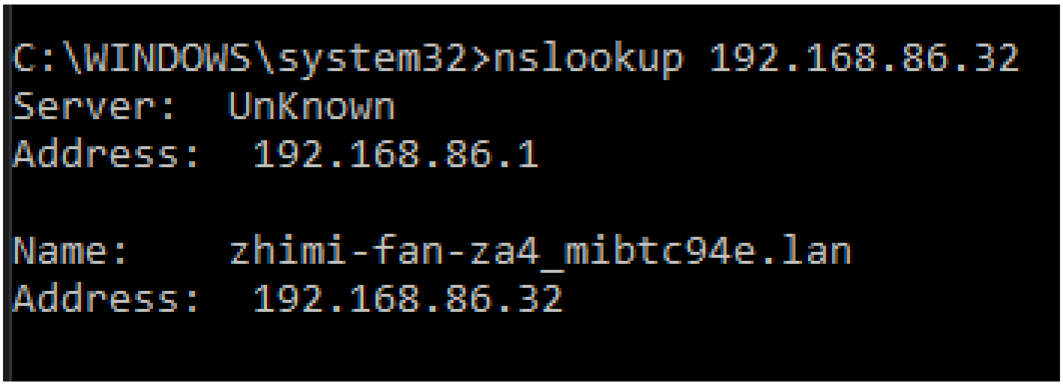
Note: IP addresses that are not retrieved via the arp command was manually crossed referenced from the vendor router's management page. OS version names are taken from respective application manually.

Credit : https://macvendors.com/ (MAC Vendor of individual devices are listed the network diagram)

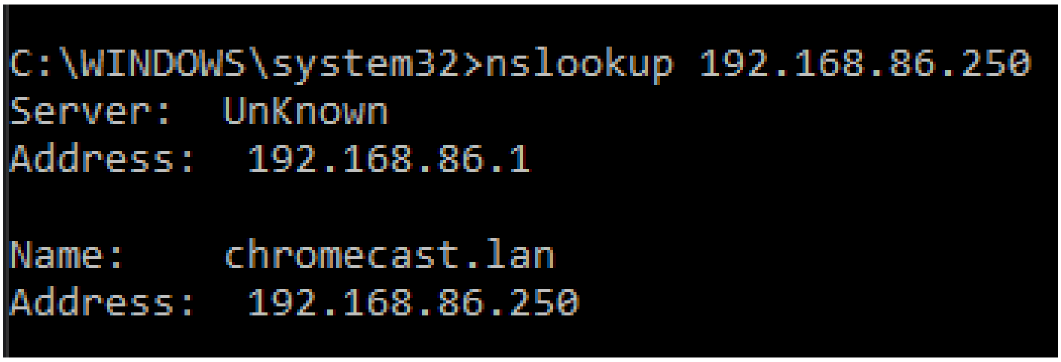
The "**nslookup <IP address>**" command is used to query Domain Name System (DNS) servers and retrieve information about a specific domain or IP address. This reverse DNS lookup command is used to discover the description of the device link to the IP address.



```
C:\WINDOWS\system32>nslookup 192.168.86.21
Server:  UnKnown
Address:  192.168.86.1

Name:    nvsh800h1.lan
Address:  192.168.86.21
```



```
C:\WINDOWS\system32>nslookup 192.168.86.32
Server:  UnKnown
Address:  192.168.86.1

Name:    zhimi-fan-za4_mibtc94e.lan
Address:  192.168.86.32
```



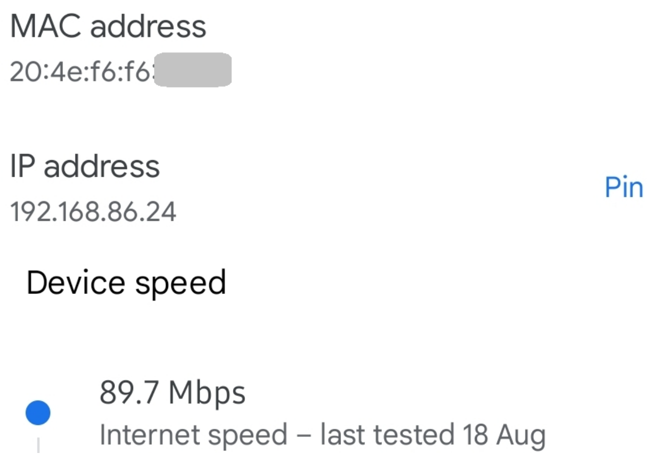
```
C:\WINDOWS\system32>nslookup 192.168.86.250
Server:  UnKnown
Address:  192.168.86.1

Name:    chromecast.lan
Address:  192.168.86.250
```

Other Device within local network (routing table)

The following list is generated via the vendor's router management app “Google Home” .

IP address	MAC	Note
192.168.86.27	**F0-B0-40-15**	Deebot
192.168.86.23	**92-f0-41-24**	My Phone (MAC Randomization)
192.168.86.22	**20-4e-f6-d9**	AP2360
192.168.86.28	**20-4e-f6-da**	AP37780-2
192.168.86.24	**20-4e-f6-f6**	AP36084-3
192.168.86.21	**00-09-74-6a**	nvsh800h1
192.168.86.32	**54-48-e6-ea**	zhimi-fan-za4_mibtc94e

Credit : https://macvendors.com/ (MAC Vendor of individual devices are listed the network diagram)

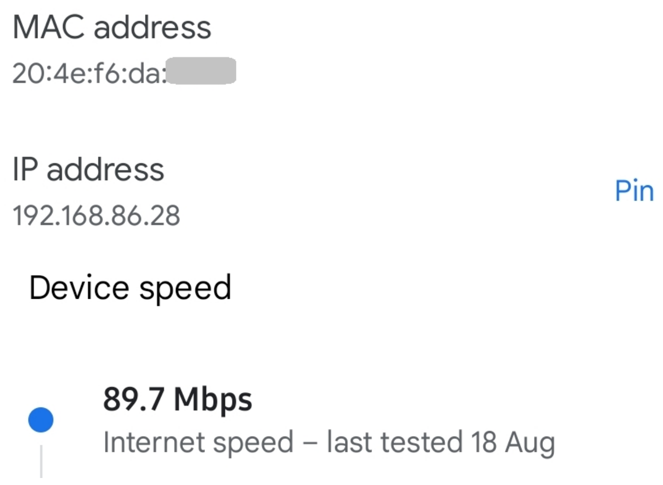


MAC address
20:4e:f6:f6[redacted]

IP address
192.168.86.24

Device speed

89.7 Mbps
Internet speed – last tested 18 Aug



MAC address

20:4e:f6:da:[redacted]

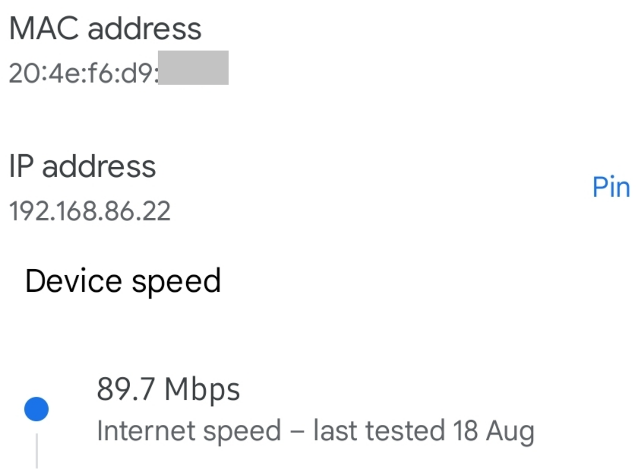
IP address

192.168.86.28

Device speed

89.7 Mbps

Internet speed – last tested 18 Aug



MAC address

20:4e:f6:d9:[redacted]

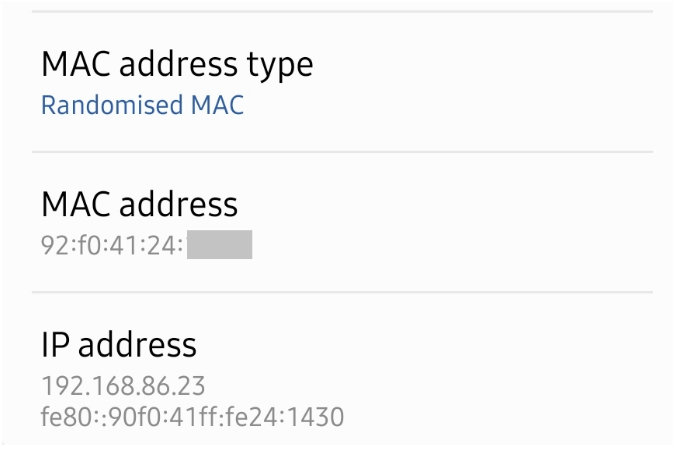
IP address

192.168.86.22

Device speed

89.7 Mbps

Internet speed – last tested 18 Aug



MAC address type

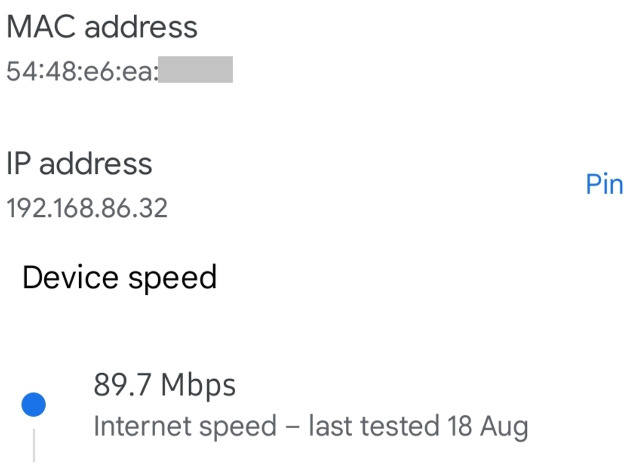
Randomised MAC

MAC address

92:f0:41:24:[redacted]

IP address

192.168.86.23
fe80::90f0:41ff:fe24:1430

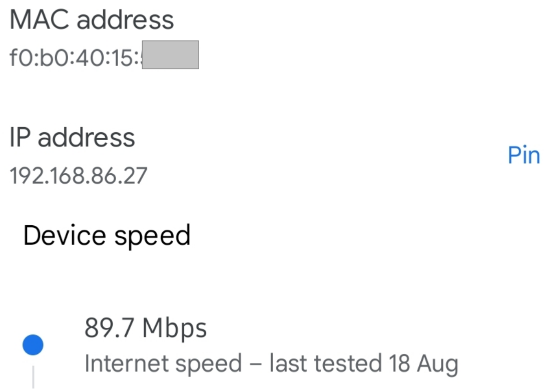


MAC address
54:48:e6:ea:[redacted]

IP address
192.168.86.32

Device speed

89.7 Mbps
Internet speed – last tested 18 Aug

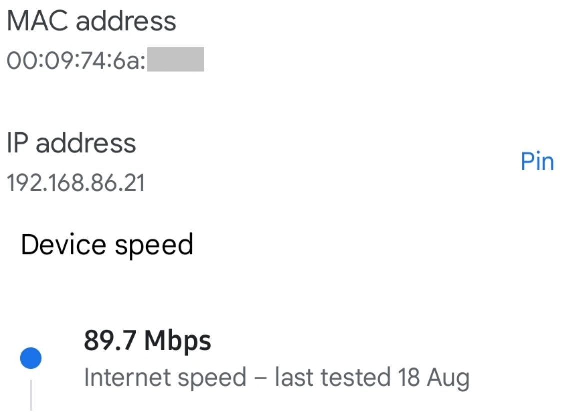


MAC address
f0:b0:40:15:[redacted]

IP address
192.168.86.27

Device speed

89.7 Mbps
Internet speed – last tested 18 Aug



MAC address
00:09:74:6a:[redacted]

IP address
192.168.86.21

Device speed

89.7 Mbps
Internet speed – last tested 18 Aug

MAC Randomization

Android devices using Android 10 OS (Android Q) have a new feature to randomizes the MAC address for different Wi-Fi connections. This help to prevent listeners from using MAC addresses to build a history of device or user activity, increasing user privacy and security. This feature is usually enabled by default but can be deactivated for specific Wi-Fi networks.

Credit : https://techzone.vmware.com/blog/how-control-mac-randomization-samsung-devices

Wireshark

This tool helps to capture network packages and allows an individual to analyse the network traffics, and inspect burst within the traffic and contents of network transactions.

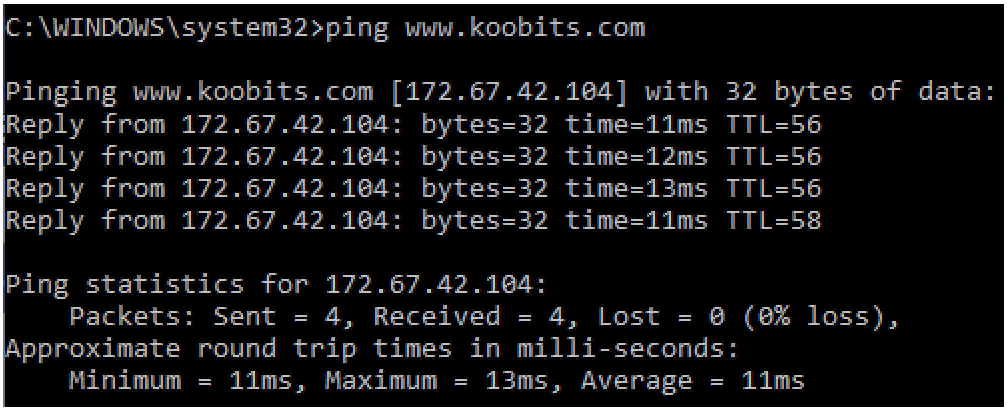
Scenario 1 -

Inspect a PCAP file to determine network traffic to www.koobits.com and the individual that has been accessing the site.

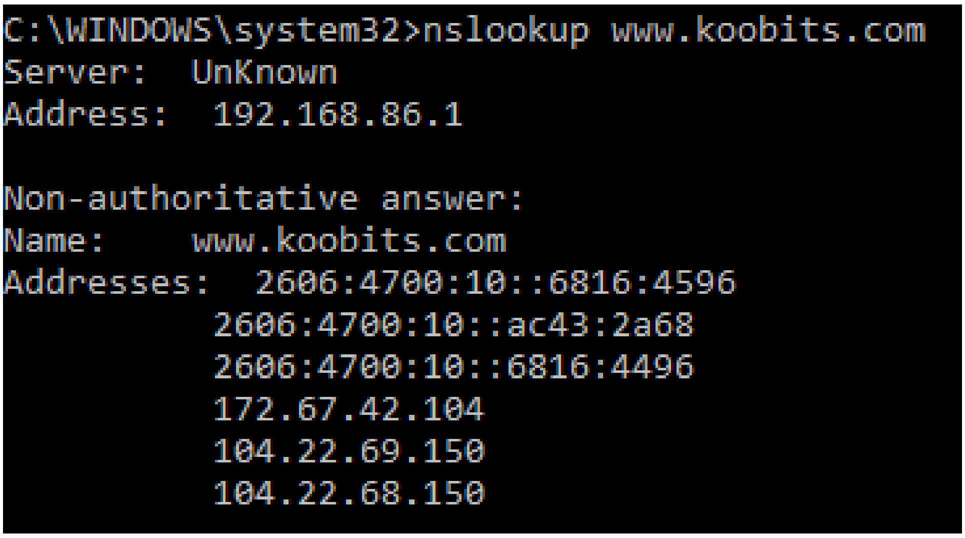
Step 1 - to determine the IP address of the Domain name “www.koobits.com”, command “**ping**” can be used to determine the address. The address would be “172.67.42.104”.

If the Domain has multiple addresses allocated, “**nslookup**” command can be used to retrieve the IP addresses

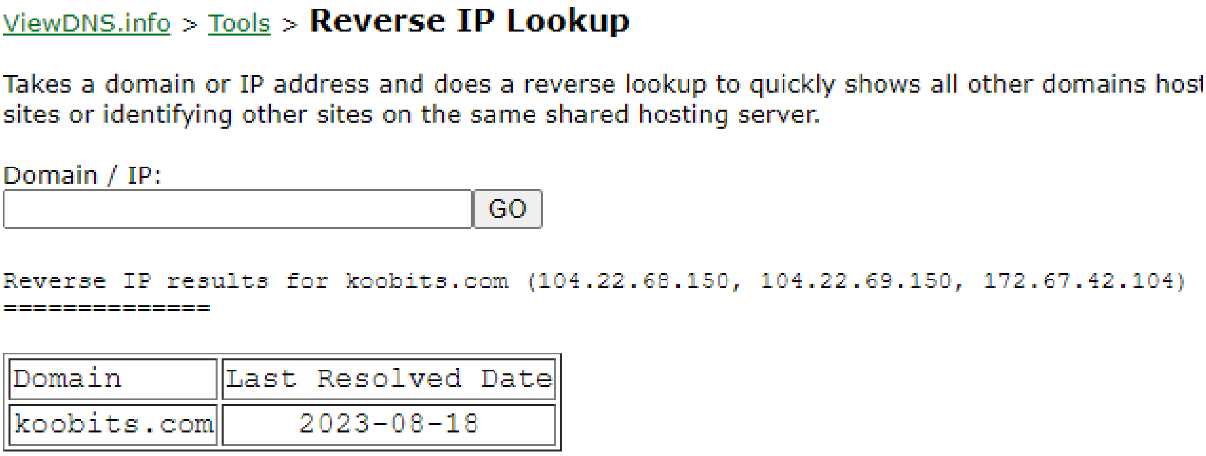
This can information can be reaffirmed via an online tool by searching for Reverse IP lookup (nslookup)



```
C:\WINDOWS\system32>ping www.koobits.com

Pinging www.koobits.com [172.67.42.104] with 32 bytes of data:
Reply from 172.67.42.104: bytes=32 time=11ms TTL=56
Reply from 172.67.42.104: bytes=32 time=12ms TTL=56
Reply from 172.67.42.104: bytes=32 time=13ms TTL=56
Reply from 172.67.42.104: bytes=32 time=11ms TTL=58

Ping statistics for 172.67.42.104:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 13ms, Average = 11ms
```



```
C:\WINDOWS\system32>nslookup www.koobits.com
Server:  UnKnown
Address:  192.168.86.1

Non-authoritative answer:
Name:    www.koobits.com
Addresses:  2606:4700:10::6816:4596
          2606:4700:10::ac43:2a68
          2606:4700:10::6816:4496
          172.67.42.104
          104.22.69.150
          104.22.68.150
```



ViewDNS.info > Tools > **Reverse IP Lookup**

Takes a domain or IP address and does a reverse lookup to quickly shows all other domains host
sites or identifying other sites on the same shared hosting server.

Domain / IP:

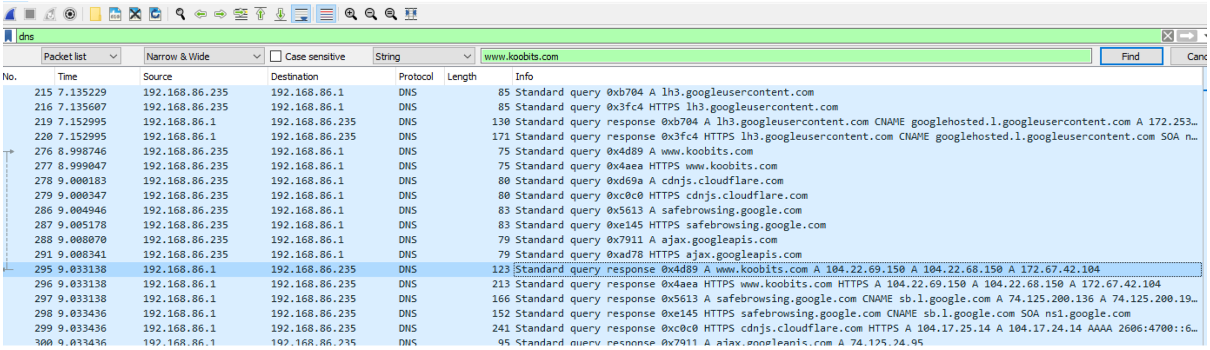
```
Reverse IP results for koobits.com (104.22.68.150, 104.22.69.150, 172.67.42.104)
==============
```

Domain	Last Resolved Date
koobits.com	2023-08-18

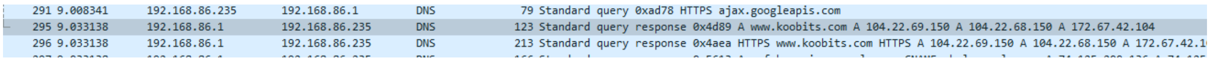
Credit : https://viewdns.info/

Step 2 - The above mention step can also be determined through the Wireshark tool, where filter set as “**dns**” and further drill down with a domain name search within a packet.

The tool gives opportunity to determine the DNS server and the target terminal where quires are being triggered form/to the DNS.

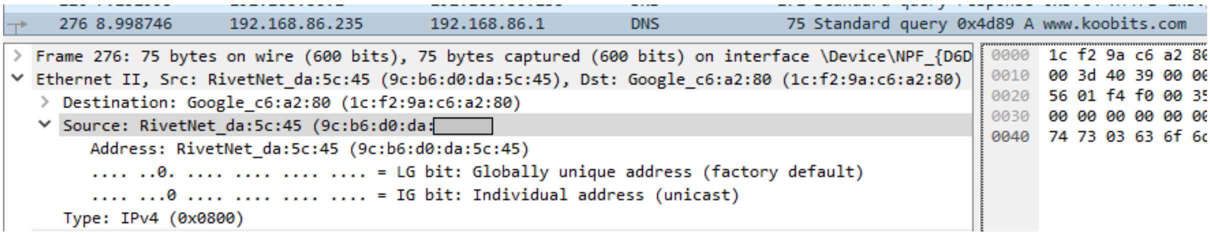


```
No.  Time      Source          Destination     Protocol Length Info
 215 7.135229  192.168.86.235  192.168.86.1    DNS       85 Standard query 0xb704 A lh3.googleusercontent.com
 216 7.135607  192.168.86.235  192.168.86.1    DNS       85 Standard query 0x3fc4 HTTPS lh3.googleusercontent.com
 219 7.152995  192.168.86.1    192.168.86.235  DNS      130 Standard query response 0xb704 A lh3.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A 172.253…
 220 7.152995  192.168.86.1    192.168.86.235  DNS      171 Standard query response 0x3fc4 HTTPS lh3.googleusercontent.com CNAME googlehosted.l.googleusercontent.com SOA n…
 276 8.998746  192.168.86.235  192.168.86.1    DNS       75 Standard query 0x4d89 A www.koobits.com
 277 8.999047  192.168.86.235  192.168.86.1    DNS       75 Standard query 0x4aea HTTPS www.koobits.com
 278 9.000183  192.168.86.235  192.168.86.1    DNS       80 Standard query 0xd69a A cdnjs.cloudflare.com
 279 9.000347  192.168.86.235  192.168.86.1    DNS       80 Standard query 0xc0c0 HTTPS cdnjs.cloudflare.com
 286 9.004946  192.168.86.235  192.168.86.1    DNS       83 Standard query 0x5613 A safebrowsing.google.com
 287 9.005178  192.168.86.235  192.168.86.1    DNS       83 Standard query 0xe145 HTTPS safebrowsing.google.com
 288 9.008070  192.168.86.235  192.168.86.1    DNS       79 Standard query 0x7911 A ajax.googleapis.com
 291 9.008341  192.168.86.235  192.168.86.1    DNS       79 Standard query 0xad78 HTTPS ajax.googleapis.com
 295 9.033138  192.168.86.1    192.168.86.235  DNS      123 Standard query response 0x4d89 A www.koobits.com A 104.22.69.150 A 104.22.68.150 A 172.67.42.104
 296 9.033138  192.168.86.1    192.168.86.235  DNS      213 Standard query response 0x4aea HTTPS www.koobits.com HTTPS A 104.22.69.150 A 104.22.68.150 A 172.67.42.104
 297 9.033138  192.168.86.1    192.168.86.235  DNS      166 Standard query response 0x5613 A safebrowsing.google.com CNAME sb.l.google.com A 74.125.200.136 A 74.125.200.19…
 298 9.033436  192.168.86.1    192.168.86.235  DNS      152 Standard query response 0xe145 HTTPS safebrowsing.google.com CNAME sb.l.google.com SOA ns1.google.com
 299 9.033436  192.168.86.1    192.168.86.235  DNS      241 Standard query response 0xc0c0 HTTPS cdnjs.cloudflare.com HTTPS A 104.17.25.14 A 104.17.24.14 AAAA 2606:4700::6…
 300 9.033436  192.168.86.1    192.168.86.235  DNS       95 Standard query response 0x7911 A ajax.googleapis.com A 74.125.24.95
```



```
 291 9.008341   192.168.86.235   192.168.86.1     DNS        79 Standard query 0xad78 HTTPS ajax.googleapis.com
 295 9.033138   192.168.86.1     192.168.86.235   DNS       123 Standard query response 0x4d89 A www.koobits.com A 104.22.69.150 A 104.22.68.150 A 172.67.42.104
 296 9.033138   192.168.86.1     192.168.86.235   DNS       213 Standard query response 0x4aea HTTPS www.koobits.com HTTPS A 104.22.69.150 A 104.22.68.150 A 172.67.42.1
```

Step 3 - Selecting targeted IP address as the source and further inspection of the packet in the ethernet header provides details for target system’s MAC address and manufacture (disregarding MAC address spoofing in this scenario).



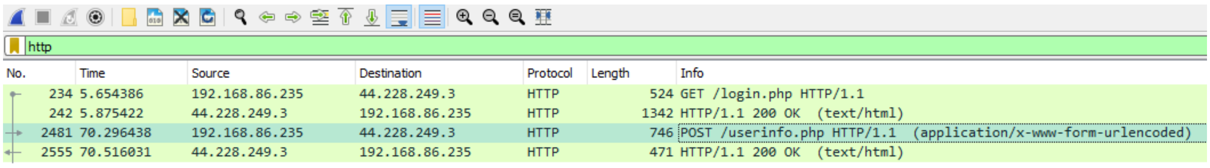
```
 276 8.998746   192.168.86.235   192.168.86.1   DNS   75 Standard query 0x4d89 A www.koobits.com

> Frame 276: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{D6D
v Ethernet II, Src: RivetNet_da:5c:45 (9c:b6:d0:da:5c:45), Dst: Google_c6:a2:80 (1c:f2:9a:c6:a2:80)
  > Destination: Google_c6:a2:80 (1c:f2:9a:c6:a2:80)
  v Source: RivetNet_da:5c:45 (9c:b6:d0:da:[redacted]
      Address: RivetNet_da:5c:45 (9c:b6:d0:da:5c:45)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)

0000  1c f2 9a c6 a2 80
0010  00 3d 40 39 00 00
0020  56 01 f4 f0 00 35
0030  00 00 00 00 00 00
0040  74 73 03 63 6f 6c
```

Scenario 2 -

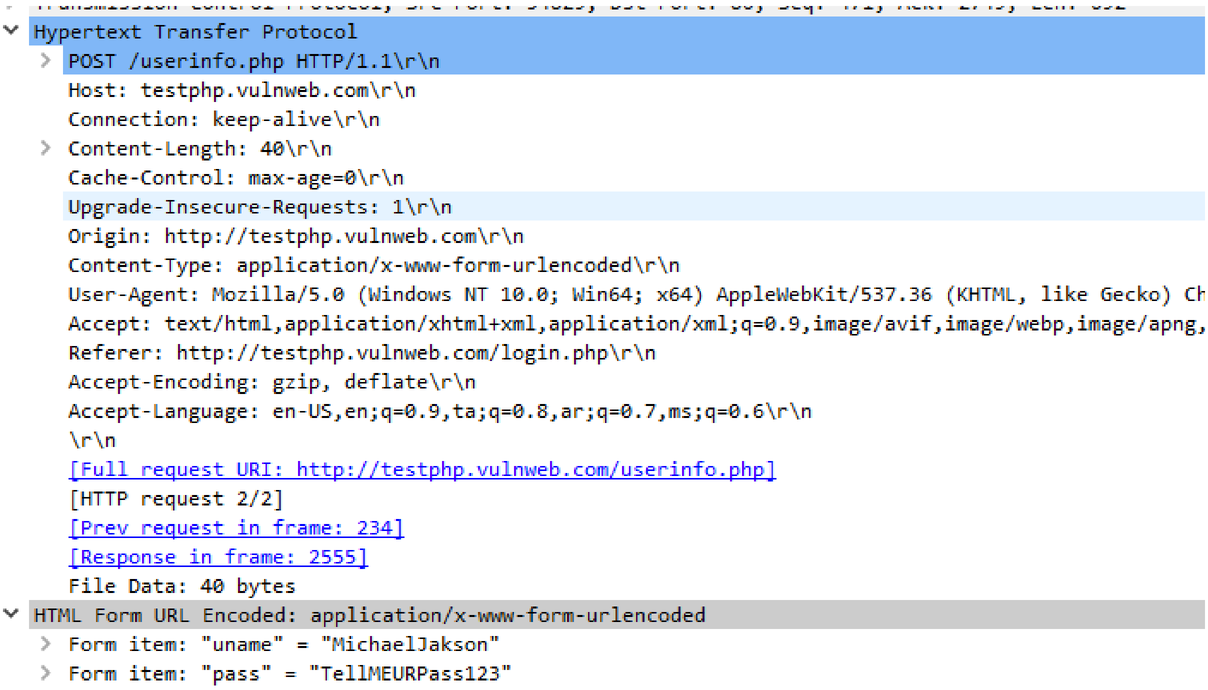
Inspect a PCAPNG file to determine network traffic to an unsecure site and the individual that has been accessing it.

Step 1- Set filter to “http” to search for an unsecure protocol. Result shows source IP address with the MAC address information of the targeted system accessing an unsecure site. Further to this, a POST msg was sent to targeted to domain.

Step 2 - Analyzing the HTTP Content, the packet shares information on the Host name referring too http://testphp.vulnweb.com/ and URI used to POST a msg to the host. From the HTML Form URL the tool also shares the Username and Password of the user trying to sign for a service on an unsecure site.



```
No.   Time        Source           Destination      Protocol Length Info
  234 5.654386    192.168.86.235   44.228.249.3     HTTP      524 GET /login.php HTTP/1.1
  242 5.875422    44.228.249.3     192.168.86.235   HTTP     1342 HTTP/1.1 200 OK  (text/html)
 2481 70.296438   192.168.86.235   44.228.249.3     HTTP      746 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
 2555 70.516031   44.228.249.3     192.168.86.235   HTTP      471 HTTP/1.1 200 OK  (text/html)
```



```
Transmission Control Protocol, Src Port: 51829, Dst Port: 80, Seq: 471, Ack: 2749, Len: 692
Hypertext Transfer Protocol
    POST /userinfo.php HTTP/1.1\r\n
    Host: testphp.vulnweb.com\r\n
    Connection: keep-alive\r\n
    Content-Length: 40\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Origin: http://testphp.vulnweb.com\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Ch
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
    Referer: http://testphp.vulnweb.com/login.php\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,ta;q=0.8,ar;q=0.7,ms;q=0.6\r\n
    \r\n
    [Full request URI: http://testphp.vulnweb.com/userinfo.php]
    [HTTP request 2/2]
    [Prev request in frame: 234]
    [Response in frame: 2555]
    File Data: 40 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
    Form item: "uname" = "MichaelJakson"
    Form item: "pass" = "TellMEURPass123"
```