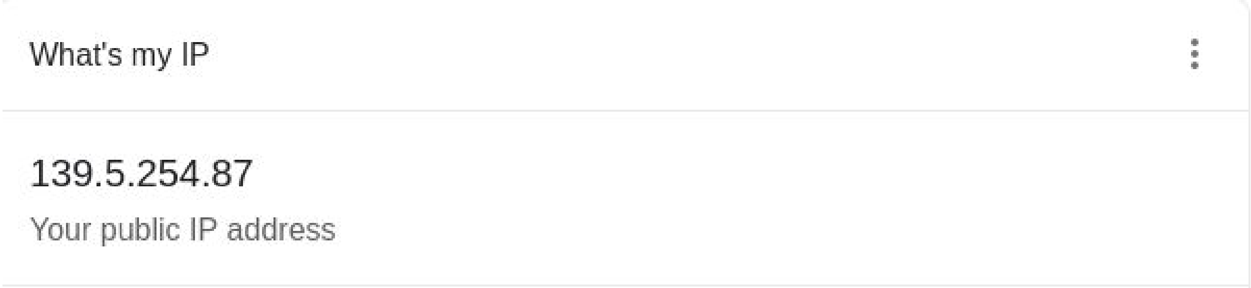
CN | HW5

Setu Gupta (2018190)

Q1.) ASN lookup

Source: https://securitytrails.com/blog/asn-lookup
I found my public ip:

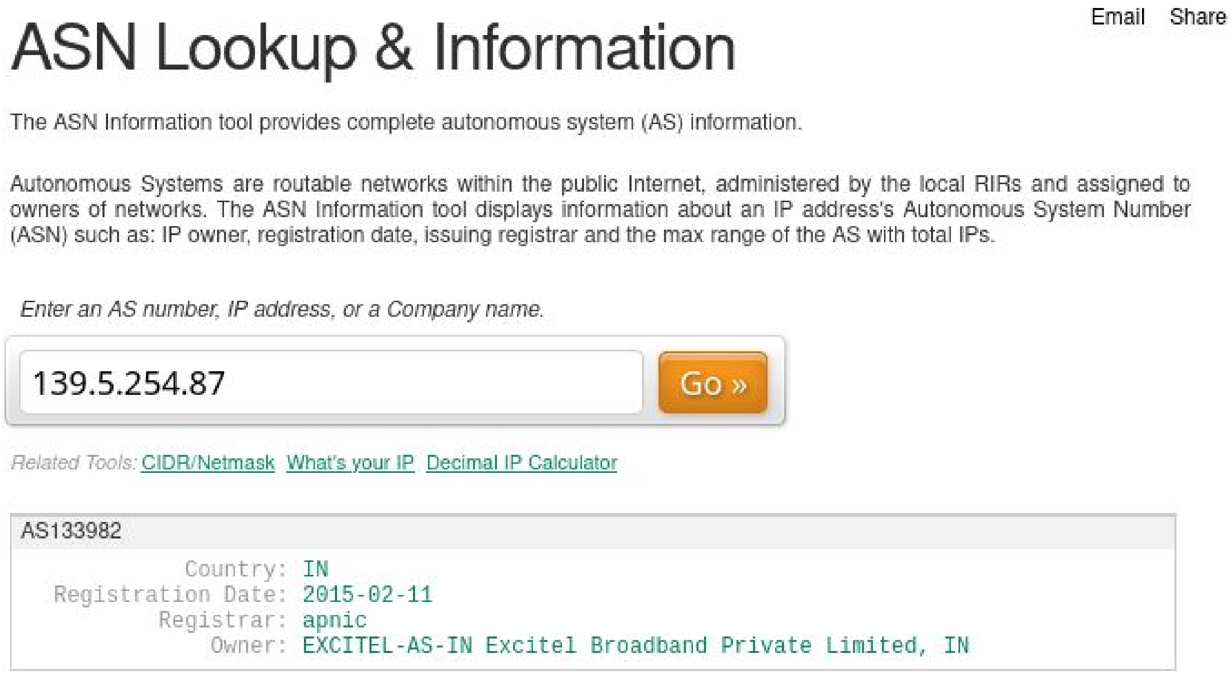


What's my IP

139.5.254.87

Your public IP address

Then I used an ASN lookup tool: https://www.ultratools.com/tools/asnInfo



ASN Lookup & Information

The ASN Information tool provides complete autonomous system (AS) information.

Autonomous Systems are routable networks within the public Internet, administered by the local RIRs and assigned to owners of networks. The ASN Information tool displays information about an IP address's Autonomous System Number (ASN) such as: IP owner, registration date, issuing registrar and the max range of the AS with total IPs.

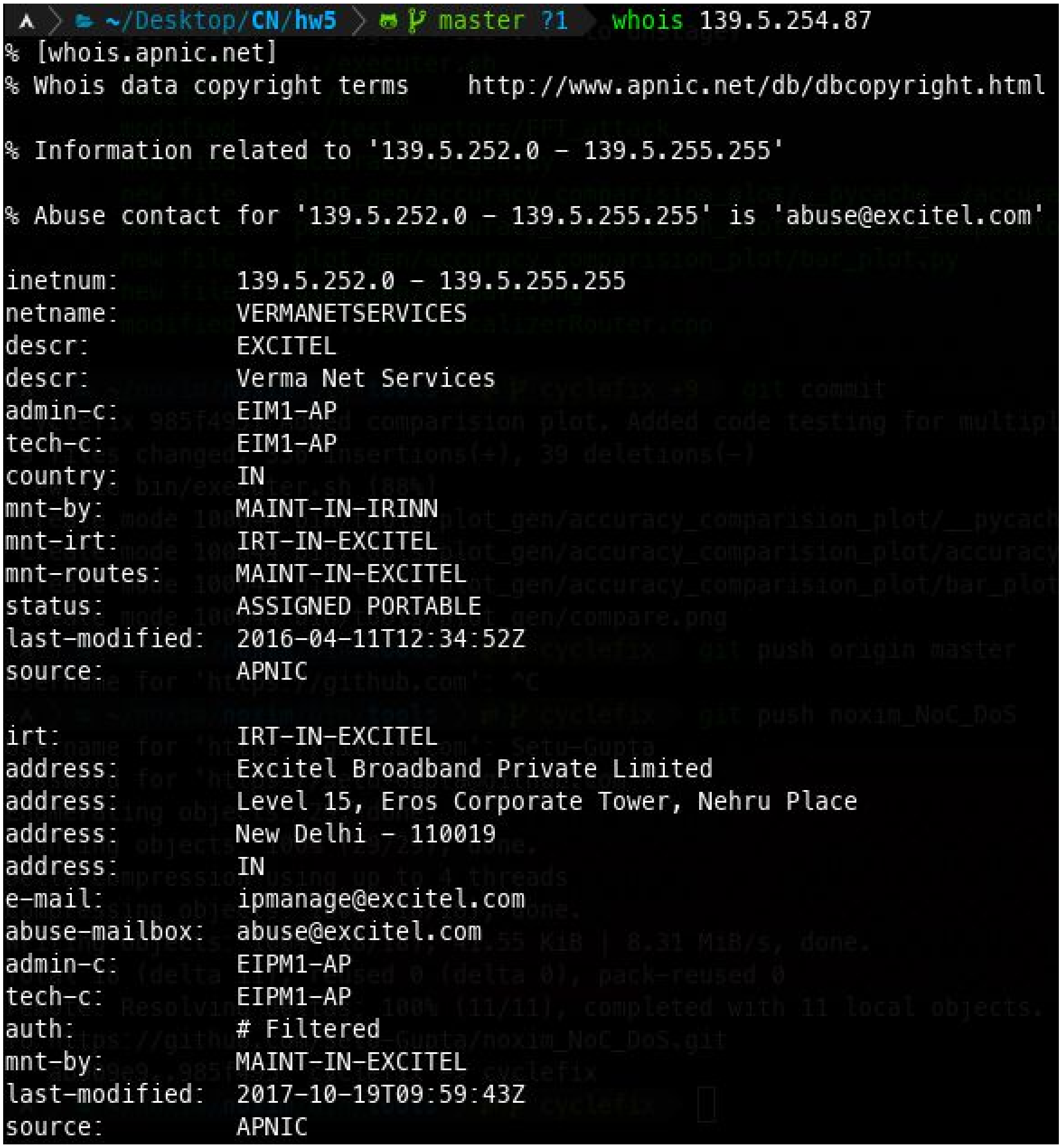
Enter an AS number, IP address, or a Company name.

139.5.254.87

Related Tools: CIDR/Netmask What's your IP Decimal IP Calculator

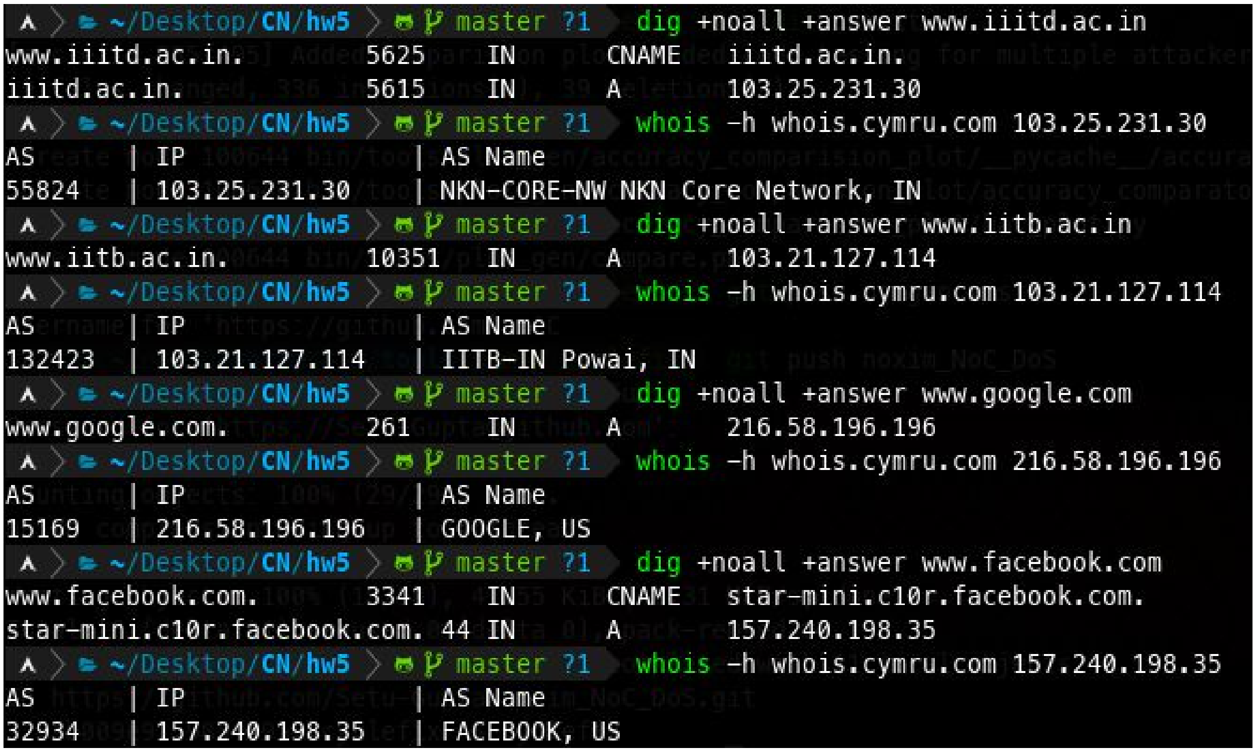
```
AS133982
            Country: IN
  Registration Date: 2015-02-11
          Registrar: apnic
              Owner: EXCITEL-AS-IN Excitel Broadband Private Limited, IN
```

I found other details using `whois` command:



```
~/Desktop/CN/hw5  master ?1  whois 139.5.254.87
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '139.5.252.0 - 139.5.255.255'

% Abuse contact for '139.5.252.0 - 139.5.255.255' is 'abuse@excitel.com'

inetnum:        139.5.252.0 - 139.5.255.255
netname:        VERMANETSERVICES
descr:          EXCITEL
descr:          Verma Net Services
admin-c:        EIM1-AP
tech-c:         EIM1-AP
country:        IN
mnt-by:         MAINT-IN-IRINN
mnt-irt:        IRT-IN-EXCITEL
mnt-routes:     MAINT-IN-EXCITEL
status:         ASSIGNED PORTABLE
last-modified:  2016-04-11T12:34:52Z
source:         APNIC

irt:            IRT-IN-EXCITEL
address:        Excitel Broadband Private Limited
address:        Level 15, Eros Corporate Tower, Nehru Place
address:        New Delhi - 110019
address:        IN
e-mail:         ipmanage@excitel.com
abuse-mailbox:  abuse@excitel.com
admin-c:        EIPM1-AP
tech-c:         EIPM1-AP
auth:           # Filtered
mnt-by:         MAINT-IN-EXCITEL
last-modified:  2017-10-19T09:59:43Z
source:         APNIC
```

a. ASN: 133982
b. Owner: Excitel
c. IPv4 address range: 139.5.252.0 - 139.5.255.255
d. I used `dig +noall +answer <url>` to find the IP. Then I called `whois -h whois.cymru.com <IP>` on it for ASN. The -h specified the service to use.

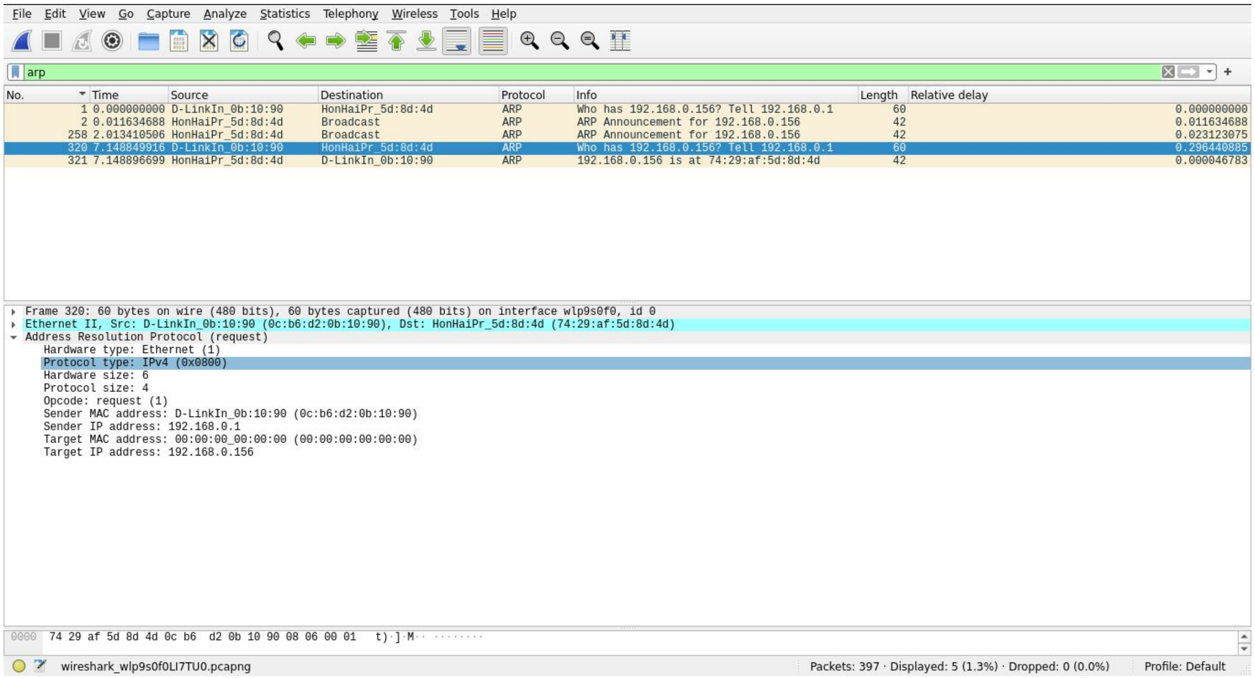


```
~/Desktop/CN/hw5 > master ?1   dig +noall +answer www.iiitd.ac.in
www.iiitd.ac.in.        5625    IN      CNAME   iiitd.ac.in.
iiitd.ac.in.            5615    IN      A       103.25.231.30
~/Desktop/CN/hw5 > master ?1   whois -h whois.cymru.com 103.25.231.30
AS      | IP               | AS Name
55824   | 103.25.231.30    | NKN-CORE-NW NKN Core Network, IN
~/Desktop/CN/hw5 > master ?1   dig +noall +answer www.iitb.ac.in
www.iitb.ac.in.         10351   IN      A       103.21.127.114
~/Desktop/CN/hw5 > master ?1   whois -h whois.cymru.com 103.21.127.114
AS      | IP               | AS Name
132423  | 103.21.127.114   | IITB-IN Powai, IN
~/Desktop/CN/hw5 > master ?1   dig +noall +answer www.google.com
www.google.com.         261     IN      A       216.58.196.196
~/Desktop/CN/hw5 > master ?1   whois -h whois.cymru.com 216.58.196.196
AS      | IP               | AS Name
15169   | 216.58.196.196   | GOOGLE, US
~/Desktop/CN/hw5 > master ?1   dig +noall +answer www.facebook.com
www.facebook.com.       3341    IN      CNAME   star-mini.c10r.facebook.com.
star-mini.c10r.facebook.com. 44 IN      A       157.240.198.35
~/Desktop/CN/hw5 > master ?1   whois -h whois.cymru.com 157.240.198.35
AS      | IP               | AS Name
32934   | 157.240.198.35   | FACEBOOK, US
```

i. www.iiitd.ac.in : 55824
ii. www.iitb.ac.in : 132423
iii. www.google.com : 15169
iv. www.facebook.com : 32934

Q2.)

a. Request:



arp

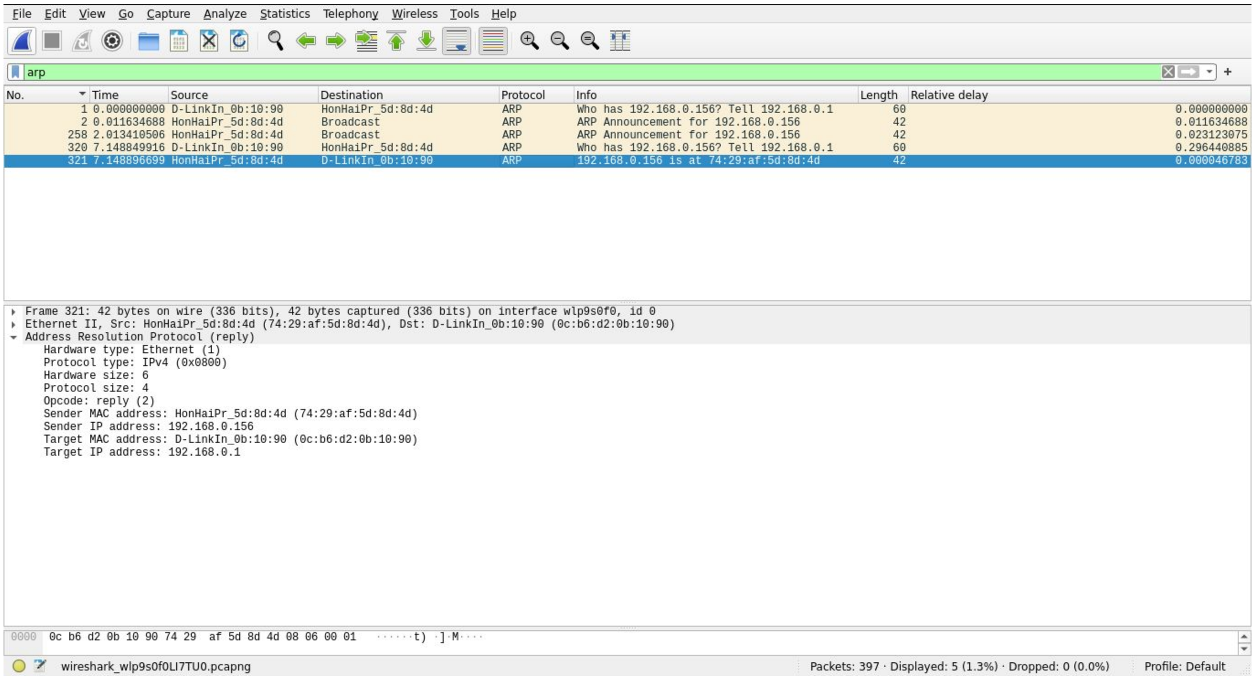
```
No.   Time        Source             Destination        Protocol  Info                                   Length  Relative delay
  1 0.000000000 D-LinkIn_0b:10:90  HonHaiPr_5d:8d:4d  ARP       Who has 192.168.0.156? Tell 192.168.0.1    60     0.000000000
  2 0.011634688 HonHaiPr_5d:8d:4d  Broadcast          ARP       ARP Announcement for 192.168.0.156         42     0.011634688
258 2.013410506 HonHaiPr_5d:8d:4d  Broadcast          ARP       ARP Announcement for 192.168.0.156         42     0.023123075
320 7.148849916 D-LinkIn_0b:10:90  HonHaiPr_5d:8d:4d  ARP       Who has 192.168.0.156? Tell 192.168.0.1    60     0.296440885
321 7.148896699 HonHaiPr_5d:8d:4d  D-LinkIn_0b:10:90  ARP       192.168.0.156 is at 74:29:af:5d:8d:4d      42     0.000046783
```

```
▸ Frame 320: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface wlp9s0f0, id 0
▸ Ethernet II, Src: D-LinkIn_0b:10:90 (0c:b6:d2:0b:10:90), Dst: HonHaiPr_5d:8d:4d (74:29:af:5d:8d:4d)
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: D-LinkIn_0b:10:90 (0c:b6:d2:0b:10:90)
    Sender IP address: 192.168.0.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.0.156
```

```
0000  74 29 af 5d 8d 4d 0c b6  d2 0b 10 90 08 06 00 01   t)·]·M·· ········
```

wireshark_wlp9s0f0LI7TU0.pcapng   Packets: 397 · Displayed: 5 (1.3%) · Dropped: 0 (0.0%)   Profile: Default

Reply:



arp

```
No.       Time        Source             Destination        Protocol  Info                                     Length  Relative delay
        1 0.000000000 D-LinkIn_0b:10:90  HonHaiPr_5d:8d:4d  ARP       Who has 192.168.0.156? Tell 192.168.0.1      60     0.000000000
        2 0.011634688 HonHaiPr_5d:8d:4d  Broadcast          ARP       ARP Announcement for 192.168.0.156           42     0.011634688
      258 2.013410506 HonHaiPr_5d:8d:4d  Broadcast          ARP       ARP Announcement for 192.168.0.156           42     0.023123075
      320 7.148849916 D-LinkIn_0b:10:90  HonHaiPr_5d:8d:4d  ARP       Who has 192.168.0.156? Tell 192.168.0.1      60     0.296440885
      321 7.148896699 HonHaiPr_5d:8d:4d  D-LinkIn_0b:10:90  ARP       192.168.0.156 is at 74:29:af:5d:8d:4d        42     0.000046783
```

```
▸ Frame 321: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlp9s0f0, id 0
▸ Ethernet II, Src: HonHaiPr_5d:8d:4d (74:29:af:5d:8d:4d), Dst: D-LinkIn_0b:10:90 (0c:b6:d2:0b:10:90)
▾ Address Resolution Protocol (reply)
     Hardware type: Ethernet (1)
     Protocol type: IPv4 (0x0800)
     Hardware size: 6
     Protocol size: 4
     Opcode: reply (2)
     Sender MAC address: HonHaiPr_5d:8d:4d (74:29:af:5d:8d:4d)
     Sender IP address: 192.168.0.156
     Target MAC address: D-LinkIn_0b:10:90 (0c:b6:d2:0b:10:90)
     Target IP address: 192.168.0.1
```

```
0000  0c b6 d2 0b 10 90 74 29  af 5d 8d 4d 08 06 00 01   ······t) ·]·M····
```

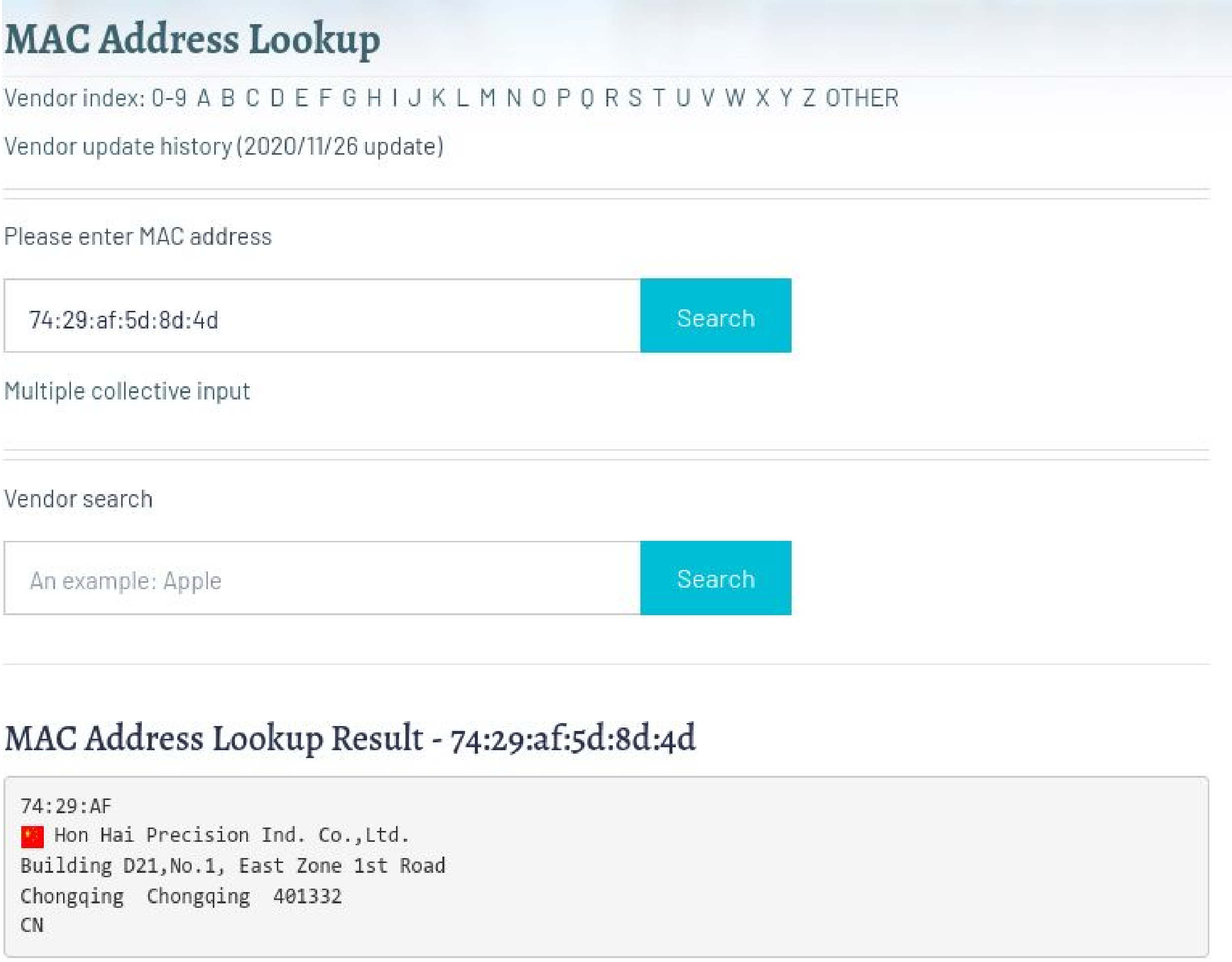
wireshark_wlp9s0f0LI7TU0.pcapng   Packets: 397 · Displayed: 5 (1.3%) · Dropped: 0 (0.0%)   Profile: Default

The source and destination IPs get flipped in request and reply. The target MAC is 00:00:00:00:00:00 in request. In reply the source MAC is of my laptop’s NIC and the target MAC is the previous source MAC.

b. 1 for request and 2 for reply

c. Ref: https://uic.win/en/mac/

i. 74:29:af:5d:8d:4d : Hon Hai Precision Ind. Co.,Ltd.



MAC Address Lookup

Vendor index: 0-9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z OTHER

Vendor update history (2020/11/26 update)

Please enter MAC address

74:29:af:5d:8d:4d

Multiple collective input

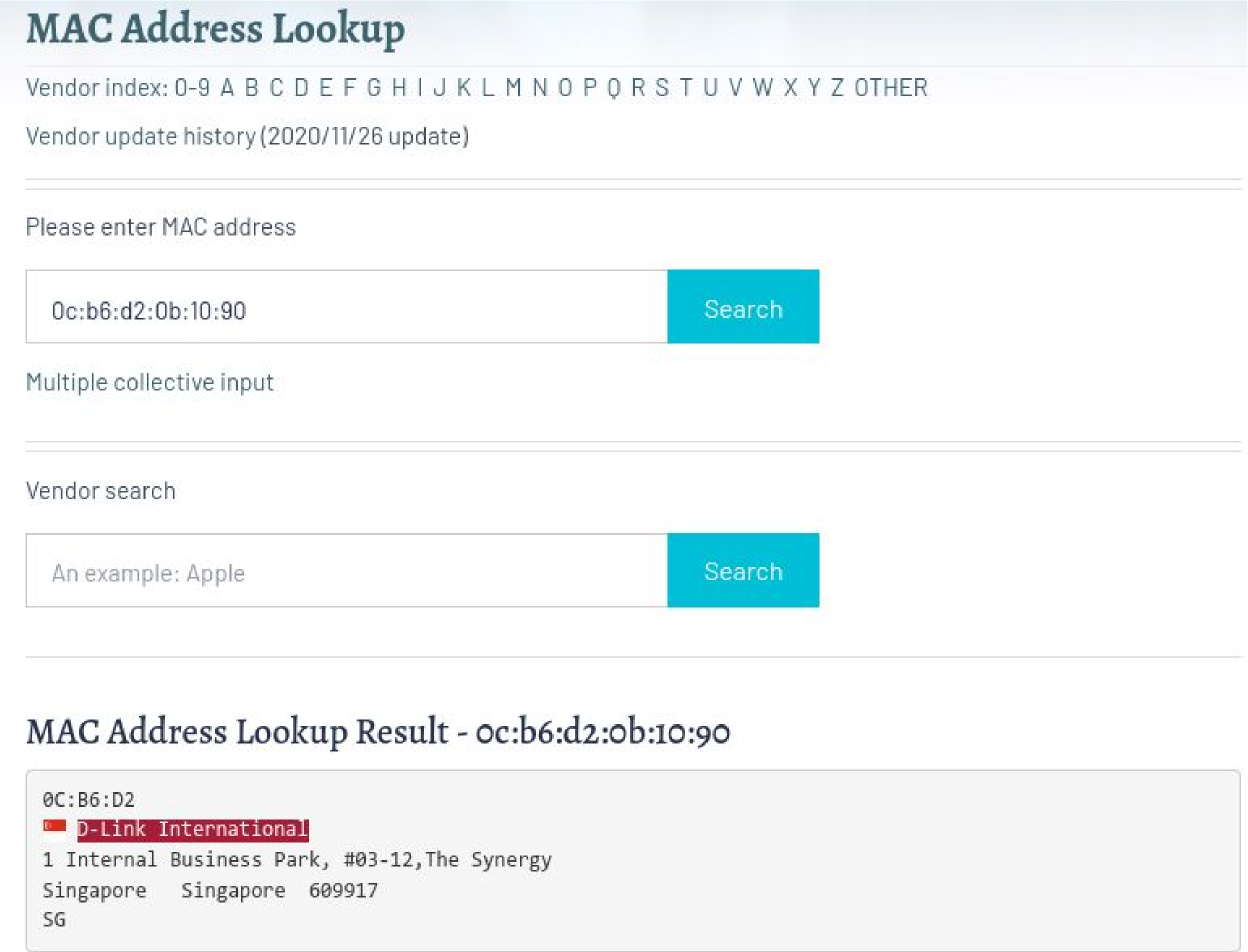
Vendor search

An example: Apple

MAC Address Lookup Result - 74:29:af:5d:8d:4d

```
74:29:AF
🇨🇳 Hon Hai Precision Ind. Co.,Ltd.
Building D21,No.1, East Zone 1st Road
Chongqing  Chongqing  401332
CN
```

ii. 0c:b6:d2:0b:10:90 : D-Link International



MAC Address Lookup

Vendor index: 0-9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z OTHER

Vendor update history (2020/11/26 update)

Please enter MAC address

0c:b6:d2:0b:10:90

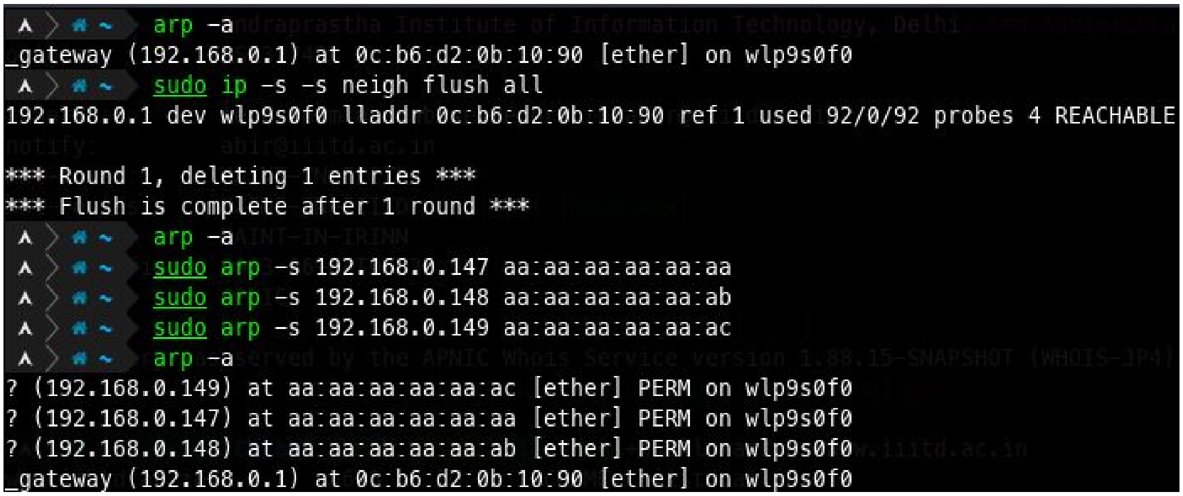
Multiple collective input

Vendor search

MAC Address Lookup Result - 0c:b6:d2:0b:10:90

```
0C:B6:D2
🇸🇬 D-Link International
1 Internal Business Park, #03-12,The Synergy
Singapore   Singapore   609917
SG
```

d. Source: https://linux-audit.com/how-to-clear-the-arp-cache-on-linux/
Source: https://www.linuxquestions.org/questions/linux-networking-3/arp-problem-w-subnet-20853/

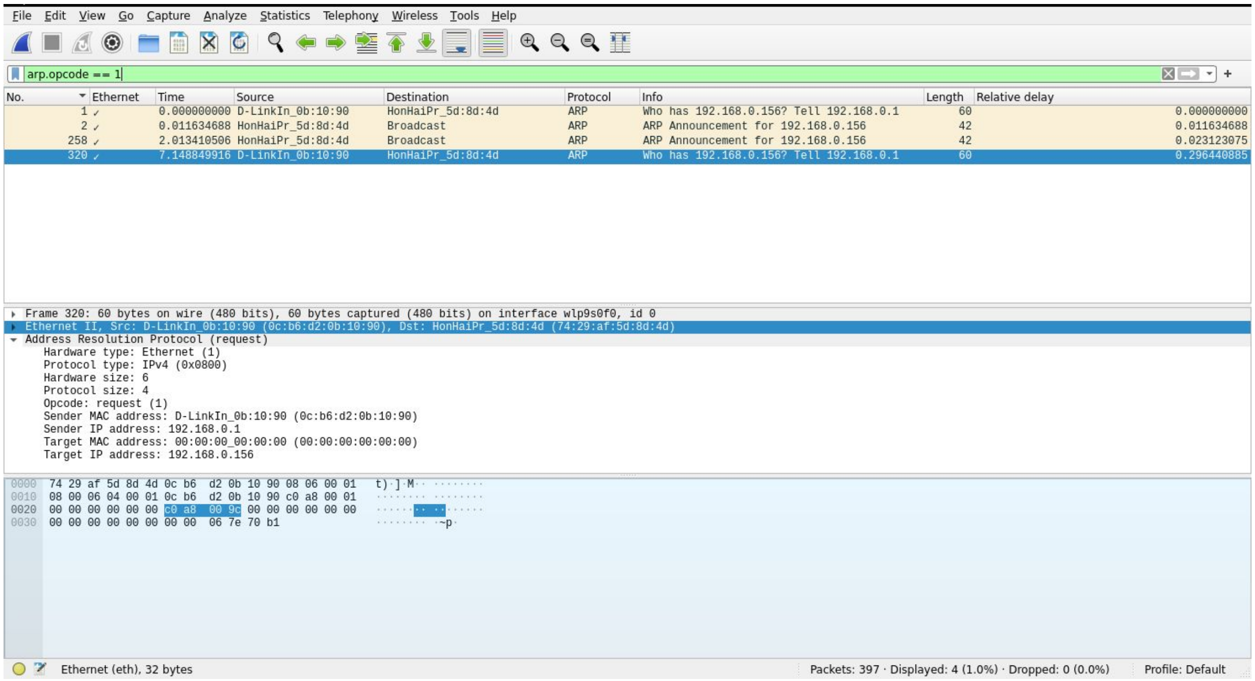


```
 Λ 〉 ⌂ ~  arp -a
_gateway (192.168.0.1) at 0c:b6:d2:0b:10:90 [ether] on wlp9s0f0
 Λ 〉 ⌂ ~  sudo ip -s -s neigh flush all
192.168.0.1 dev wlp9s0f0 lladdr 0c:b6:d2:0b:10:90 ref 1 used 92/0/92 probes 4 REACHABLE

*** Round 1, deleting 1 entries ***
*** Flush is complete after 1 round ***
 Λ 〉 ⌂ ~  arp -a
 Λ 〉 ⌂ ~  sudo arp -s 192.168.0.147 aa:aa:aa:aa:aa:aa
 Λ 〉 ⌂ ~  sudo arp -s 192.168.0.148 aa:aa:aa:aa:aa:ab
 Λ 〉 ⌂ ~  sudo arp -s 192.168.0.149 aa:aa:aa:aa:aa:ac
 Λ 〉 ⌂ ~  arp -a
? (192.168.0.149) at aa:aa:aa:aa:aa:ac [ether] PERM on wlp9s0f0
? (192.168.0.147) at aa:aa:aa:aa:aa:aa [ether] PERM on wlp9s0f0
? (192.168.0.148) at aa:aa:aa:aa:aa:ab [ether] PERM on wlp9s0f0
_gateway (192.168.0.1) at 0c:b6:d2:0b:10:90 [ether] on wlp9s0f0
```

Static entries are user added whereas dynamic entries are learned. Static entries for devices which are not connected can also exist.
Source:
http://docs.ruckuswireless.com/fastiron/08.0.70/fastiron-08070-l3guide/GUID-B5A197B6-5EB5-481E-8535-5DC9FD66CA14.html

Q3.)

a. The destination of request is not a real host. Everyone will receive this packet.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp.opcode == 1

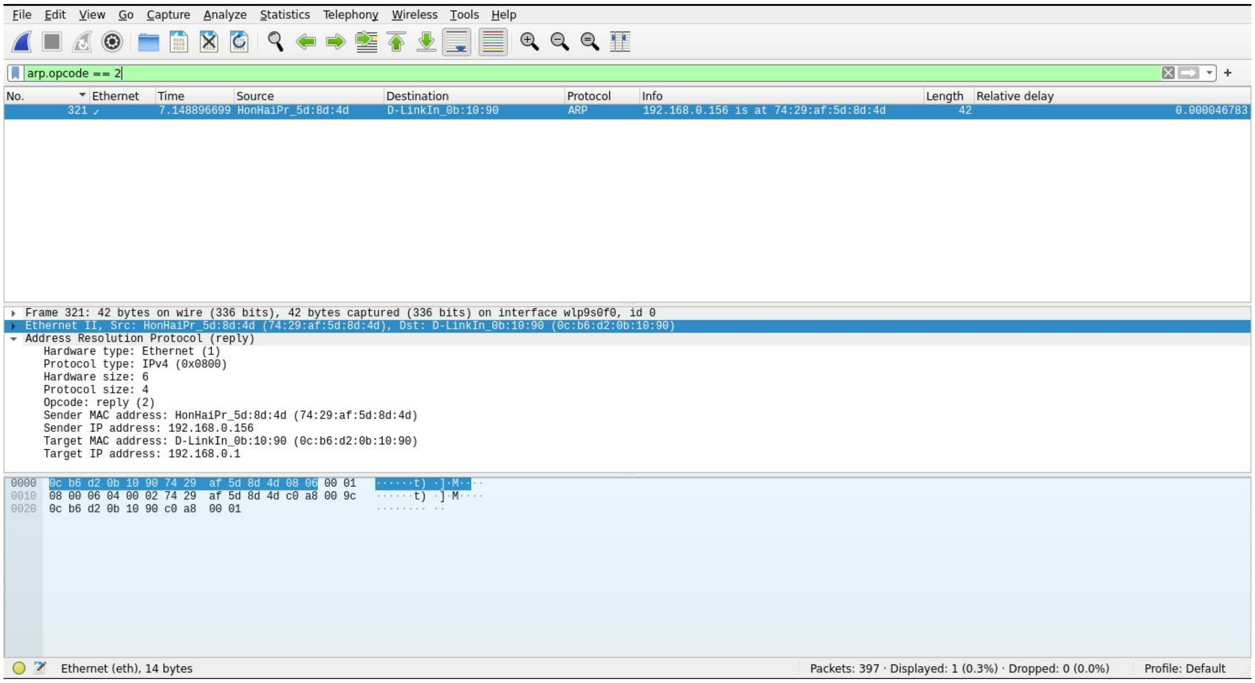
```
No.        Ethernet  Time        Source             Destination        Protocol  Info                                     Length  Relative delay
        1 ✓          0.000000000 D-LinkIn_0b:10:90  HonHaiPr_5d:8d:4d  ARP       Who has 192.168.0.156? Tell 192.168.0.1  60          0.000000000
        2 ✓          0.011634688 HonHaiPr_5d:8d:4d  Broadcast          ARP       ARP Announcement for 192.168.0.156       42          0.011634688
      258 ✓          2.013410506 HonHaiPr_5d:8d:4d  Broadcast          ARP       ARP Announcement for 192.168.0.156       42          0.023123075
      320 ✓          7.148849916 D-LinkIn_0b:10:90  HonHaiPr_5d:8d:4d  ARP       Who has 192.168.0.156? Tell 192.168.0.1  60          0.296440885
```

```
▸ Frame 320: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface wlp9s0f0, id 0
▸ Ethernet II, Src: D-LinkIn_0b:10:90 (0c:b6:d2:0b:10:90), Dst: HonHaiPr_5d:8d:4d (74:29:af:5d:8d:4d)
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: D-LinkIn_0b:10:90 (0c:b6:d2:0b:10:90)
    Sender IP address: 192.168.0.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.0.156
```

```
0000  74 29 af 5d 8d 4d 0c b6  d2 0b 10 90 08 06 00 01   t)·]·M·· ········
0010  08 00 06 04 00 01 0c b6  d2 0b 10 90 c0 a8 00 01   ········ ········
0020  00 00 00 00 00 00 c0 a8  00 9c 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 00 00 00  06 7e 70 b1               ········ ·~p·
```

Ethernet (eth), 32 bytes   Packets: 397 · Displayed: 4 (1.0%) · Dropped: 0 (0.0%)   Profile: Default

b. Yes it’s a real host. The device which made the request (0c:b6:d2:0b:10:90) will receive the packet.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp.opcode == 2

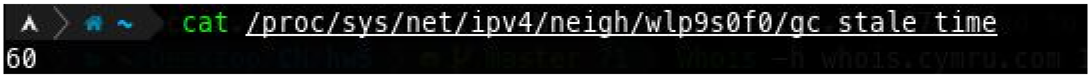
No.	Ethernet	Time	Source	Destination	Protocol	Info	Length	Relative delay
321	✓	7.148896699	HonHaiPr_5d:8d:4d	D-LinkIn_0b:10:90	ARP	192.168.0.156 is at 74:29:af:5d:8d:4d	42	0.000046783

```
▸ Frame 321: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlp9s0f0, id 0
▸ Ethernet II, Src: HonHaiPr_5d:8d:4d (74:29:af:5d:8d:4d), Dst: D-LinkIn_0b:10:90 (0c:b6:d2:0b:10:90)
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: HonHaiPr_5d:8d:4d (74:29:af:5d:8d:4d)
    Sender IP address: 192.168.0.156
    Target MAC address: D-LinkIn_0b:10:90 (0c:b6:d2:0b:10:90)
    Target IP address: 192.168.0.1
```

```
0000  0c b6 d2 0b 10 90 74 29  af 5d 8d 4d 08 06 00 01   ······t) ·]·M····
0010  08 00 06 04 00 02 74 29  af 5d 8d 4d c0 a8 00 9c   ······t) ·]·M····
0020  0c b6 d2 0b 10 90 c0 a8  00 01                     ········ ··
```

Ethernet (eth), 14 bytes   Packets: 397 · Displayed: 1 (0.3%) · Dropped: 0 (0.0%)   Profile: Default

c. 60 seconds.
Source: https://linux.die.net/man/7/arp
Source: https://serverfault.com/questions/684380/default-arp-cache-timeout



```
cat /proc/sys/net/ipv4/neigh/wlp9s0f0/gc_stale_time
60
```