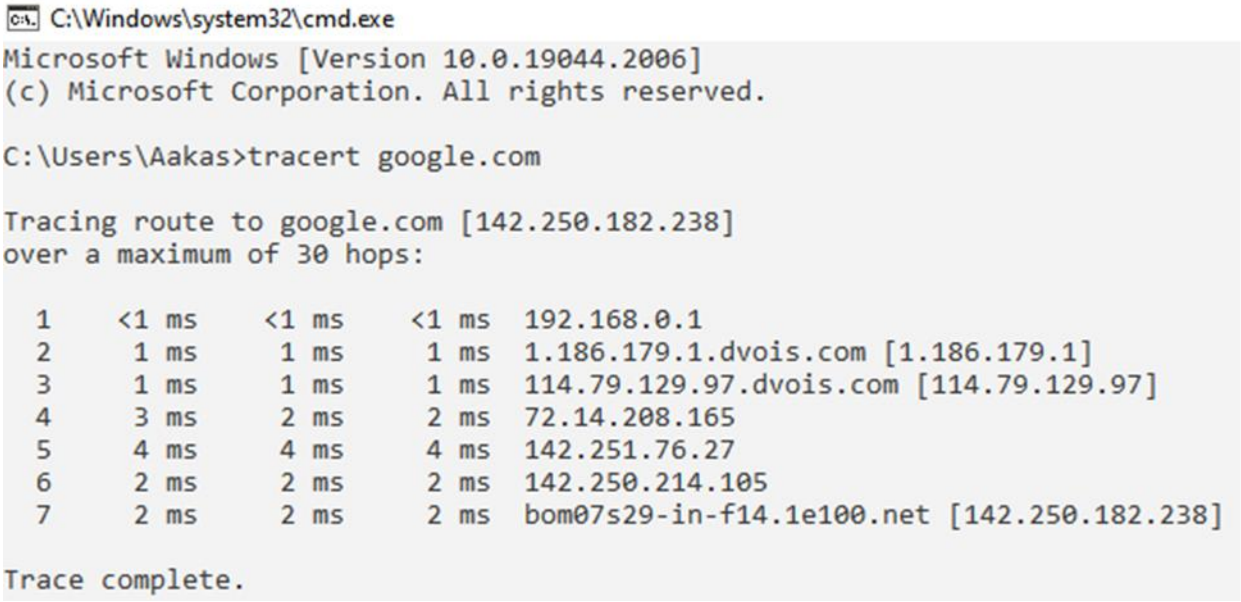
7. Study the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registrars

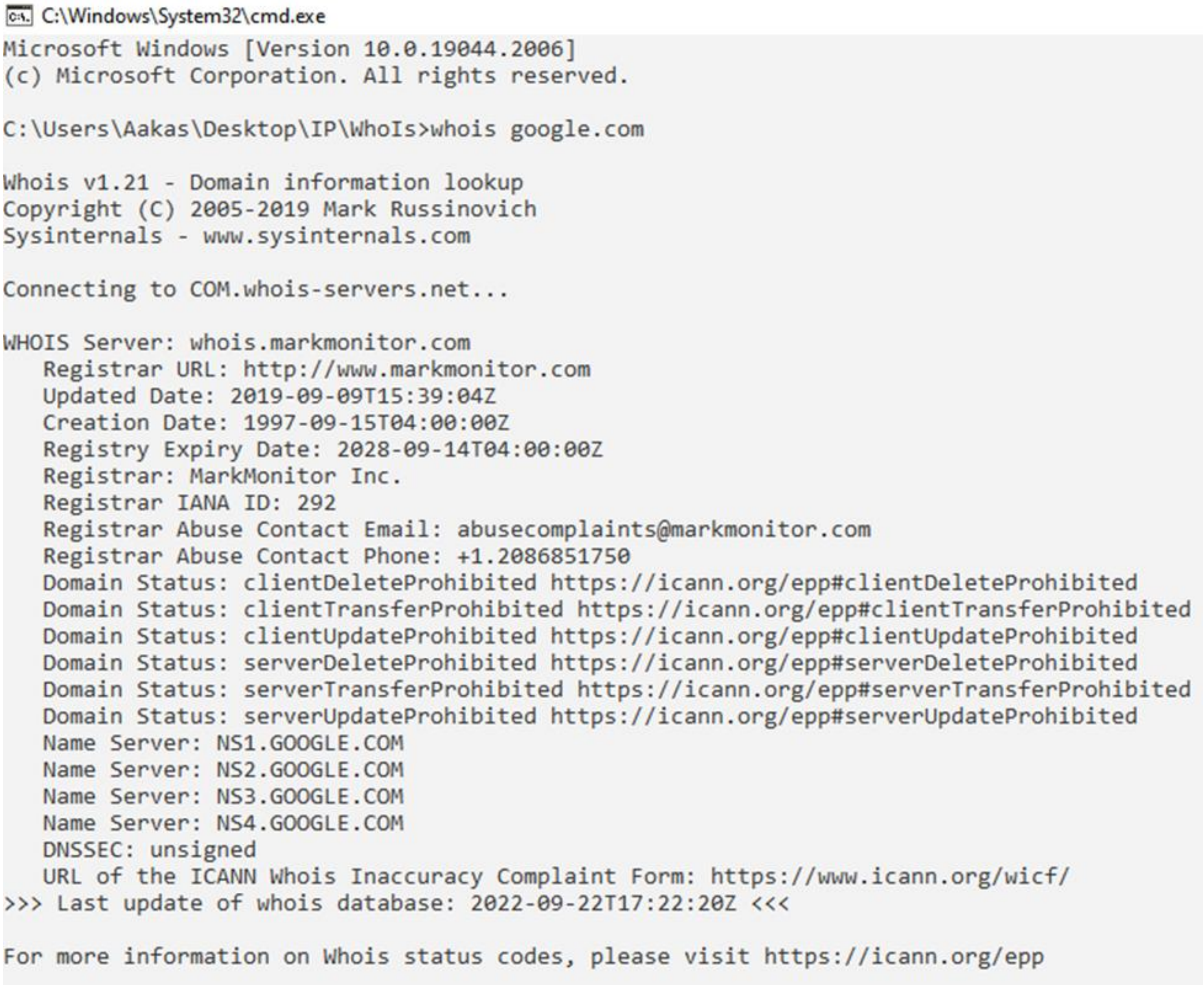
i. tracert google.com



```
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Aakas>tracert google.com

Tracing route to google.com [142.250.182.238]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.0.1
  2     1 ms     1 ms     1 ms  1.186.179.1.dvois.com [1.186.179.1]
  3     1 ms     1 ms     1 ms  114.79.129.97.dvois.com [114.79.129.97]
  4     3 ms     2 ms     2 ms  72.14.208.165
  5     4 ms     4 ms     4 ms  142.251.76.27
  6     2 ms     2 ms     2 ms  142.250.214.105
  7     2 ms     2 ms     2 ms  bom07s29-in-f14.1e100.net [142.250.182.238]

Trace complete.
```

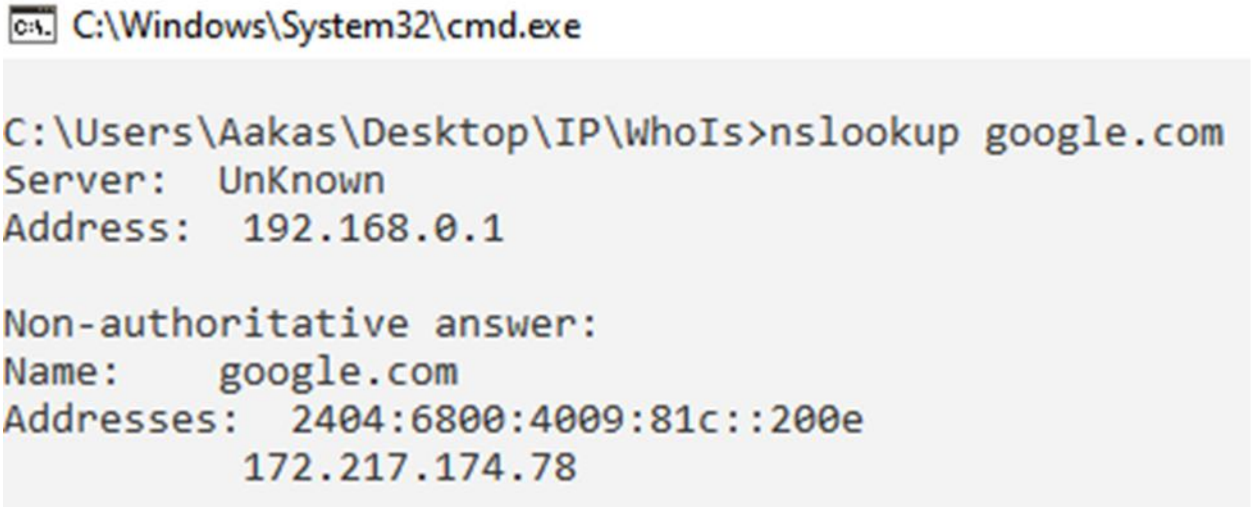
ii. Download whois and run in that whois folder

whois google.com



```
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Aakas\Desktop\IP\WhoIs>whois google.com

Whois v1.21 - Domain information lookup
Copyright (C) 2005-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting to COM.whois-servers.net...

WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry Expiry Date: 2028-09-14T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS1.GOOGLE.COM
   Name Server: NS2.GOOGLE.COM
   Name Server: NS3.GOOGLE.COM
   Name Server: NS4.GOOGLE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-09-22T17:22:20Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

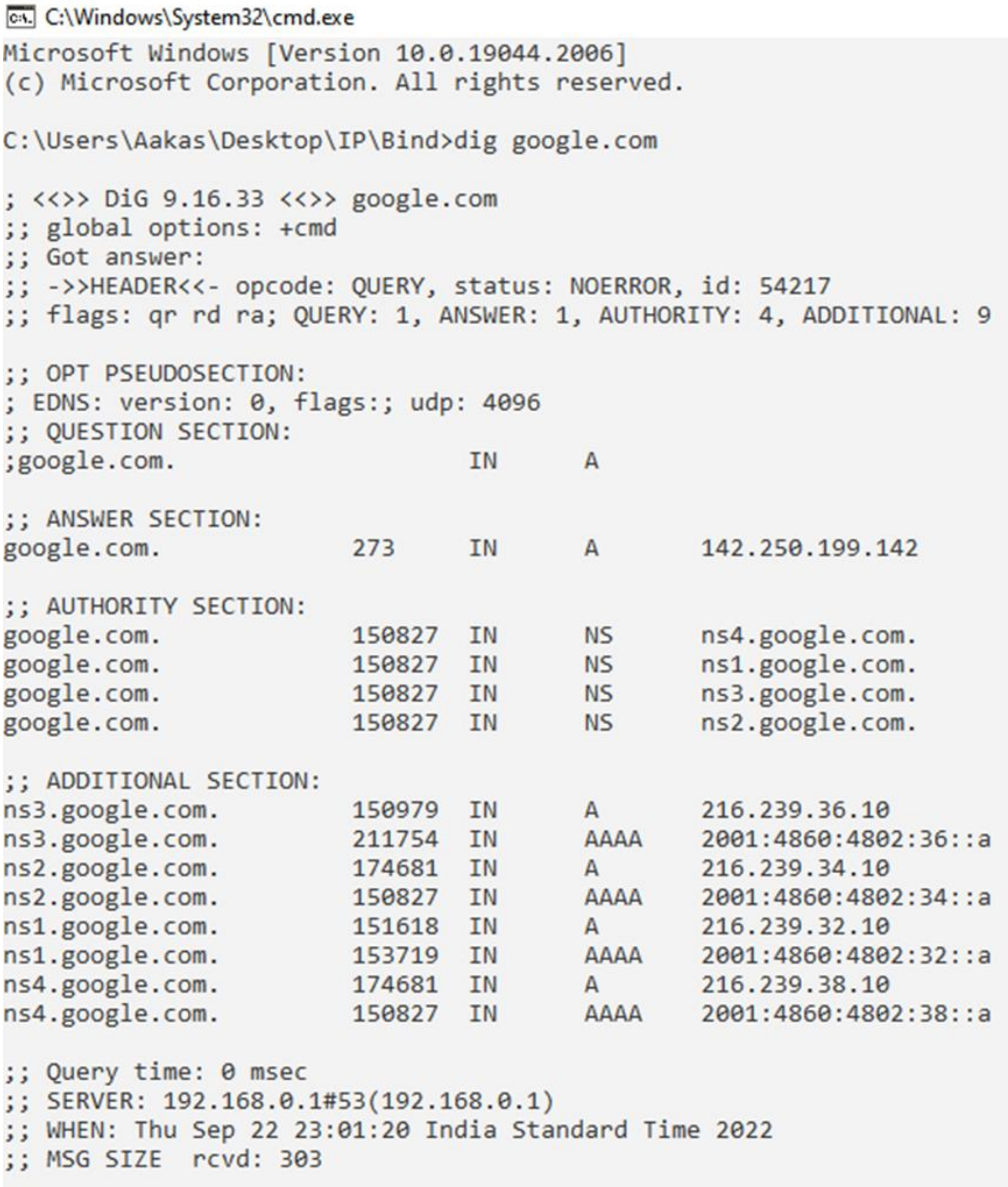
iii. nslookup google.com



C:\Windows\System32\cmd.exe

```
C:\Users\Aakas\Desktop\IP\WhoIs>nslookup google.com
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4009:81c::200e
          172.217.174.78
```

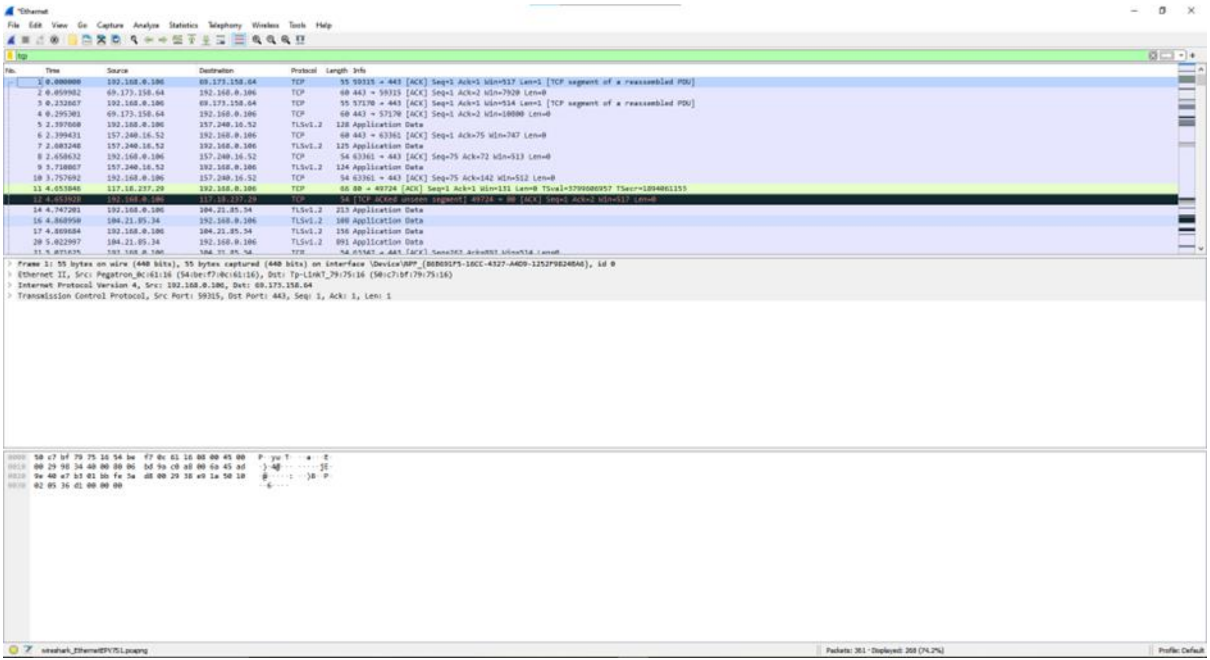
iv. Download bind and run in that bind folder
dig google.com



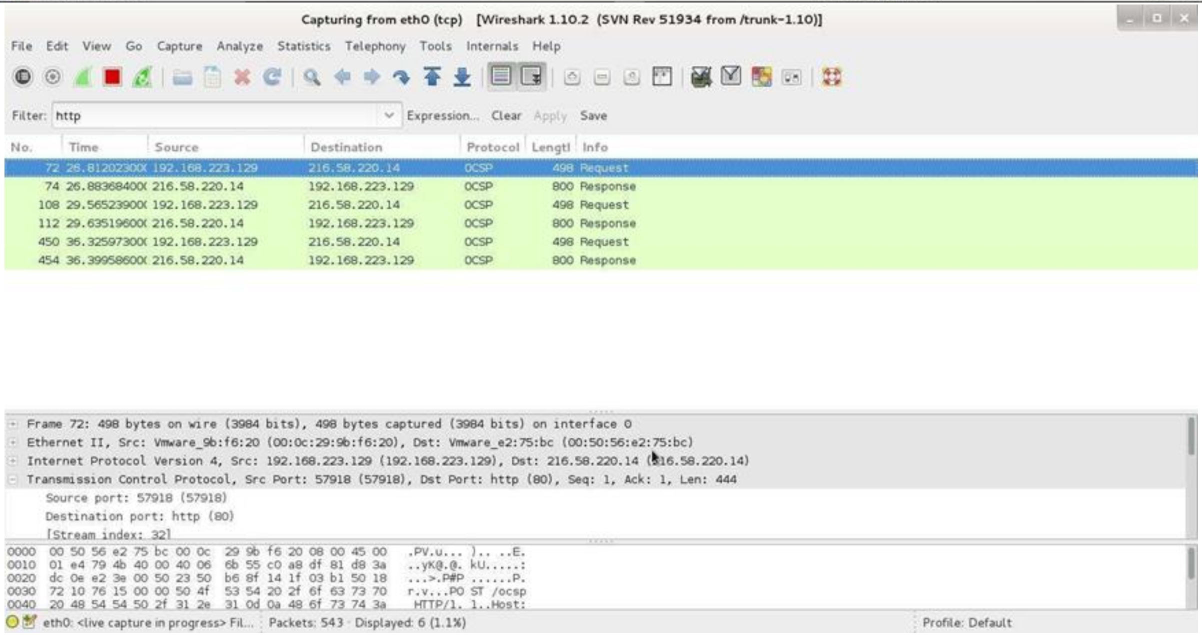
C:\Windows\System32\cmd.exe

```
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Aakas\Desktop\IP\Bind>dig google.com

; <<>> DiG 9.16.33 <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54217
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             273     IN      A       142.250.199.142

;; AUTHORITY SECTION:
google.com.             150827  IN      NS      ns4.google.com.
google.com.             150827  IN      NS      ns1.google.com.
google.com.             150827  IN      NS      ns3.google.com.
google.com.             150827  IN      NS      ns2.google.com.

;; ADDITIONAL SECTION:
ns3.google.com.         150979  IN      A       216.239.36.10
ns3.google.com.         211754  IN      AAAA    2001:4860:4802:36::a
ns2.google.com.         174681  IN      A       216.239.34.10
ns2.google.com.         150827  IN      AAAA    2001:4860:4802:34::a
ns1.google.com.         151618  IN      A       216.239.32.10
ns1.google.com.         153719  IN      AAAA    2001:4860:4802:32::a
ns4.google.com.         174681  IN      A       216.239.38.10
ns4.google.com.         150827  IN      AAAA    2001:4860:4802:38::a

;; Query time: 0 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Thu Sep 22 23:01:20 India Standard Time 2022
;; MSG SIZE  rcvd: 303
```

8. Study of packet sniffer tools Wireshark: Show the packets can be traced based on different filters.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp

No.  Time        Source          Destination     Protocol Length Info
   1 0.000000    192.168.0.106   69.173.158.64   TCP       55 59315 → 443 [ACK] Seq=1 Ack=1 Win=517 Len=1 [TCP segment of a reassembled PDU]
   2 0.059982    69.173.158.64   192.168.0.106   TCP       60 443 → 59315 [ACK] Seq=1 Ack=2 Win=7920 Len=0
   3 0.232667    192.168.0.106   69.173.158.64   TCP       55 57170 → 443 [ACK] Seq=1 Ack=1 Win=514 Len=1 [TCP segment of a reassembled PDU]
   4 0.295301    69.173.158.64   192.168.0.106   TCP       60 443 → 57170 [ACK] Seq=1 Ack=2 Win=10000 Len=0
   5 2.397660    192.168.0.106   157.240.16.52   TLSv1.2  128 Application Data
   6 2.399431    157.240.16.52   192.168.0.106   TCP       60 443 → 63361 [ACK] Seq=1 Ack=75 Win=747 Len=0
   7 2.603248    157.240.16.52   192.168.0.106   TLSv1.2  125 Application Data
   8 2.650632    192.168.0.106   157.240.16.52   TCP       54 63361 → 443 [ACK] Seq=75 Ack=72 Win=513 Len=0
   9 3.710067    157.240.16.52   192.168.0.106   TLSv1.2  124 Application Data
  10 3.757692    192.168.0.106   157.240.16.52   TCP       54 63361 → 443 [ACK] Seq=75 Ack=142 Win=512 Len=0
  11 4.653846    117.18.237.29   192.168.0.106   TCP       66 80 → 49724 [ACK] Seq=1 Ack=1 Win=131 Len=0 TSval=3799606957 TSecr=1894061155
  12 4.653928    192.168.0.106   117.18.237.29   TCP       54 [TCP ACKed unseen segment] 49724 → 80 [ACK] Seq=1 Ack=2 Win=517 Len=0
  14 4.747201    192.168.0.106   104.21.85.34    TLSv1.2  213 Application Data
  16 4.860950    104.21.85.34    192.168.0.106   TLSv1.2  100 Application Data
  17 4.869684    192.168.0.106   104.21.85.34    TLSv1.2  156 Application Data
  20 5.022997    104.21.85.34    192.168.0.106   TLSv1.2  891 Application Data
  21 5.071625    192.168.0.106   104.21.85.34    TCP       54 63362 → 443 [ACK] Seq=267 Ack=897 Win=514 Len=0

> Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{B6B691F5-16CC-4327-A4D9-1252F98248A6}, id 0
> Ethernet II, Src: Pegatron_0c:61:16 (54:be:f7:0c:61:16), Dst: Tp-LinkT_79:75:16 (50:c7:bf:79:75:16)
> Internet Protocol Version 4, Src: 192.168.0.106, Dst: 69.173.158.64
> Transmission Control Protocol, Src Port: 59315, Dst Port: 443, Seq: 1, Ack: 1, Len: 1

0000  50 c7 bf 79 75 16 54 be  f7 0c 61 16 08 00 45 00   P·yu·T· ··a···E·
0010  00 29 98 34 40 00 80 06  bd 9a c0 a8 00 6a 45 ad   ·)·4@··· ·····jE·
0020  9e 40 e7 b3 01 bb fe 3a  d8 00 29 38 e9 1a 50 10   ·@·····: ··)8··P·
0030  02 05 36 d1 00 00 00                               ··6····

wireshark_EthernetEPY75L.pcapng          Packets: 361 · Displayed: 268 (74.2%)          Profile: Default
```


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

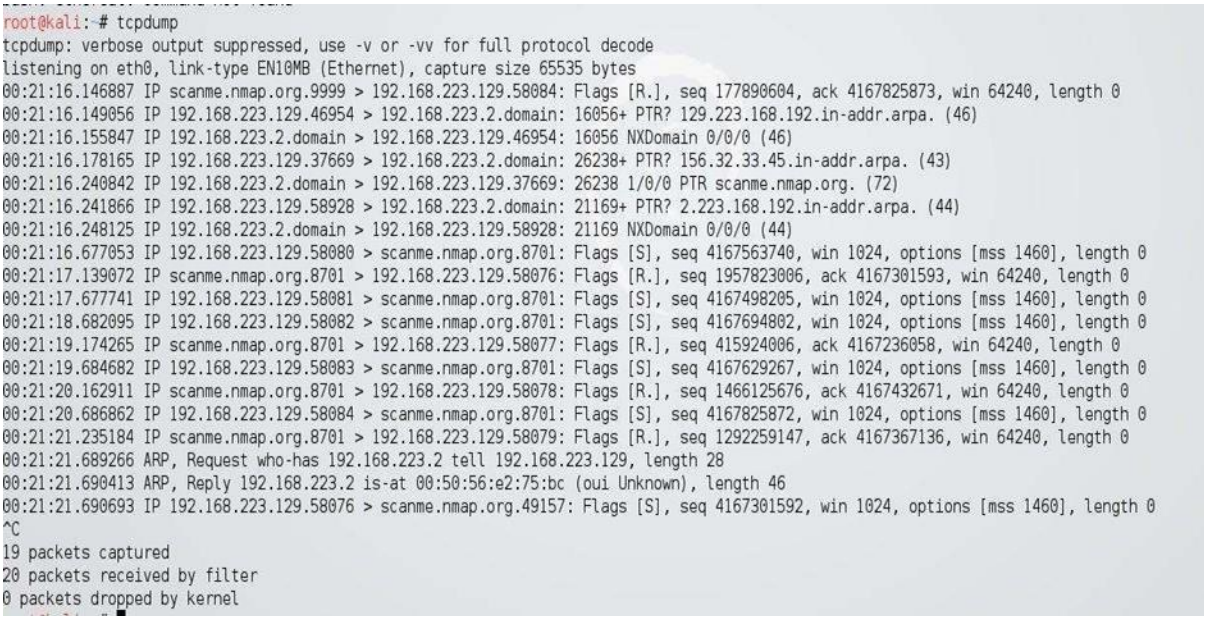
```
Capturing from eth0 (tcp)   [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]

Filter: http

No.  Time          Source            Destination       Protocol Length Info
  72 26.81202300(  192.168.223.129   216.58.220.14     OCSP       498 Request
  74 26.88368400(  216.58.220.14     192.168.223.129   OCSP       800 Response
 108 29.56523900(  192.168.223.129   216.58.220.14     OCSP       498 Request
 112 29.63519600(  216.58.220.14     192.168.223.129   OCSP       800 Response
 450 36.32597300(  192.168.223.129   216.58.220.14     OCSP       498 Request
 454 36.39958600(  216.58.220.14     192.168.223.129   OCSP       800 Response

+ Frame 72: 498 bytes on wire (3984 bits), 498 bytes captured (3984 bits) on interface 0
+ Ethernet II, Src: Vmware_9b:f6:20 (00:0c:29:9b:f6:20), Dst: Vmware_e2:75:bc (00:50:56:e2:75:bc)
+ Internet Protocol Version 4, Src: 192.168.223.129 (192.168.223.129), Dst: 216.58.220.14 (216.58.220.14)
- Transmission Control Protocol, Src Port: 57918 (57918), Dst Port: http (80), Seq: 1, Ack: 1, Len: 444
    Source port: 57918 (57918)
    Destination port: http (80)
    [Stream index: 32]
0000  00 50 56 e2 75 bc 00 0c  29 9b f6 20 08 00 45 00   .PV.u... ).. ..E.
0010  01 e4 79 4b 40 00 40 06  6b 55 c0 a8 df 81 d8 3a   ..yK@.@. kU.....:
0020  dc 0e e2 3e 00 50 23 50  b6 8f 14 1f 03 b1 50 18   ...>.P#P ......P.
0030  72 10 76 15 00 00 50 4f  53 54 20 2f 6f 63 73 70   r.v...PO ST /ocsp
0040  20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f 73 74 3a    HTTP/1. 1..Host:
eth0: <live capture in progress> Fil...   Packets: 543 · Displayed: 6 (1.1%)          Profile: Default
```

Tcpdump :

tcpdump is a common packet analyzer that runs under the command line.

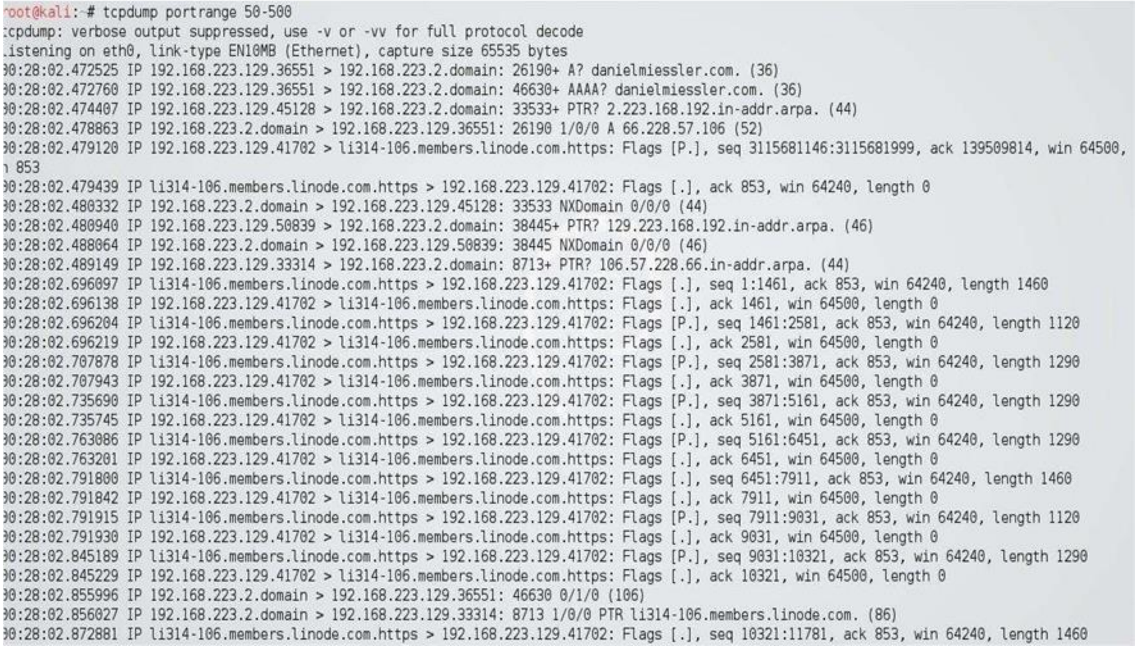
The port of tcpdump for Windows is called WinDump; it uses WinPcap, the Windows port of libpcap.

tcpdump



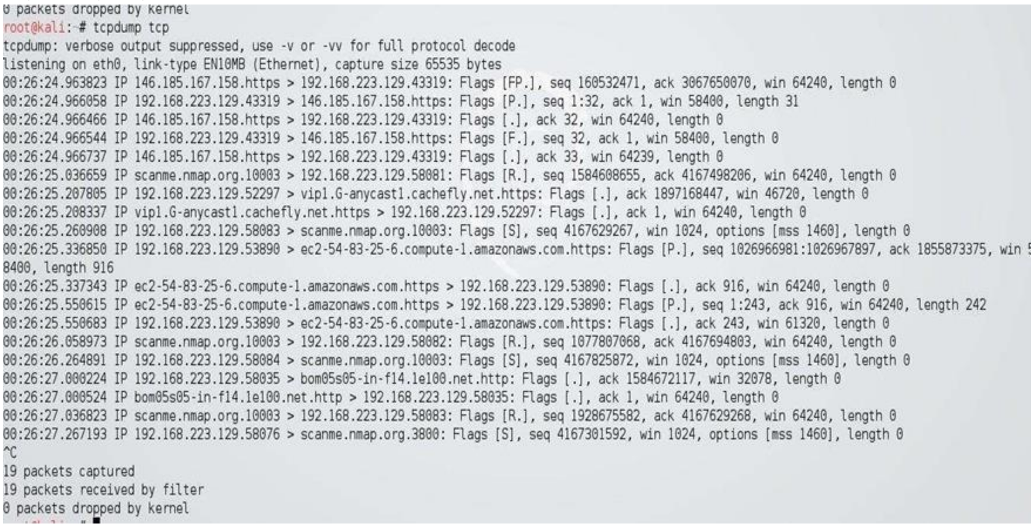
```
root@kali:~# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
00:21:16.146887 IP scanme.nmap.org.9999 > 192.168.223.129.58084: Flags [R.], seq 177890604, ack 4167825873, win 64240, length 0
00:21:16.149056 IP 192.168.223.129.46954 > 192.168.223.2.domain: 16056+ PTR? 129.223.168.192.in-addr.arpa. (46)
00:21:16.155847 IP 192.168.223.2.domain > 192.168.223.129.46954: 16056 NXDomain 0/0/0 (46)
00:21:16.178165 IP 192.168.223.129.37669 > 192.168.223.2.domain: 26238+ PTR? 156.32.33.45.in-addr.arpa. (43)
00:21:16.240842 IP 192.168.223.2.domain > 192.168.223.129.37669: 26238 1/0/0 PTR scanme.nmap.org. (72)
00:21:16.241866 IP 192.168.223.129.58928 > 192.168.223.2.domain: 21169+ PTR? 2.223.168.192.in-addr.arpa. (44)
00:21:16.248125 IP 192.168.223.2.domain > 192.168.223.129.58928: 21169 NXDomain 0/0/0 (44)
00:21:16.677053 IP 192.168.223.129.58080 > scanme.nmap.org.8701: Flags [S], seq 4167563740, win 1024, options [mss 1460], length 0
00:21:17.139072 IP scanme.nmap.org.8701 > 192.168.223.129.58076: Flags [R.], seq 1957823006, ack 4167301593, win 64240, length 0
00:21:17.677741 IP 192.168.223.129.58081 > scanme.nmap.org.8701: Flags [S], seq 4167498205, win 1024, options [mss 1460], length 0
00:21:18.682095 IP 192.168.223.129.58082 > scanme.nmap.org.8701: Flags [S], seq 4167694802, win 1024, options [mss 1460], length 0
00:21:19.174265 IP scanme.nmap.org.8701 > 192.168.223.129.58077: Flags [R.], seq 415924006, ack 4167236058, win 64240, length 0
00:21:19.684682 IP 192.168.223.129.58083 > scanme.nmap.org.8701: Flags [S], seq 4167629267, win 1024, options [mss 1460], length 0
00:21:20.162911 IP scanme.nmap.org.8701 > 192.168.223.129.58078: Flags [R.], seq 1466125676, ack 4167432671, win 64240, length 0
00:21:20.686862 IP 192.168.223.129.58084 > scanme.nmap.org.8701: Flags [S], seq 4167825872, win 1024, options [mss 1460], length 0
00:21:21.235184 IP scanme.nmap.org.8701 > 192.168.223.129.58079: Flags [R.], seq 1292259147, ack 4167367136, win 64240, length 0
00:21:21.689266 ARP, Request who-has 192.168.223.2 tell 192.168.223.129, length 28
00:21:21.690413 ARP, Reply 192.168.223.2 is-at 00:50:56:e2:75:bc (oui Unknown), length 46
00:21:21.690693 IP 192.168.223.129.58076 > scanme.nmap.org.49157: Flags [S], seq 4167301592, win 1024, options [mss 1460], length 0
^C
19 packets captured
20 packets received by filter
0 packets dropped by kernel
```

tcpdump portrange 50-500



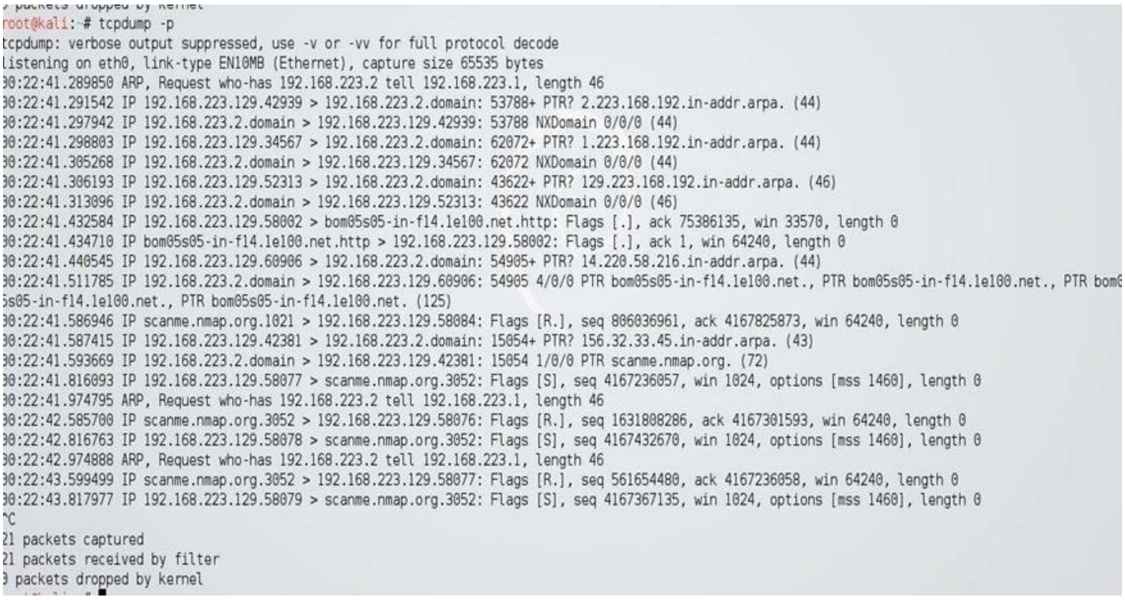
```
oot@kali:~# tcpdump portrange 50-500
cpdump: verbose output suppressed, use -v or -vv for full protocol decode
istening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
0:28:02.472525 IP 192.168.223.129.36551 > 192.168.223.2.domain: 26190+ A? danielmiessler.com. (36)
0:28:02.472760 IP 192.168.223.129.36551 > 192.168.223.2.domain: 46630+ AAAA? danielmiessler.com. (36)
0:28:02.474407 IP 192.168.223.129.45128 > 192.168.223.2.domain: 33533+ PTR? 2.223.168.192.in-addr.arpa. (44)
0:28:02.478863 IP 192.168.223.2.domain > 192.168.223.129.36551: 26190 1/0/0 A 66.228.57.106 (52)
0:28:02.479120 IP 192.168.223.129.41702 > li314-106.members.linode.com.https: Flags [P.], seq 3115681146:3115681999, ack 139509814, win 64500,
 853
0:28:02.479439 IP li314-106.members.linode.com.https > 192.168.223.129.41702: Flags [.], ack 853, win 64240, length 0
0:28:02.480332 IP 192.168.223.2.domain > 192.168.223.129.45128: 33533 NXDomain 0/0/0 (44)
0:28:02.480940 IP 192.168.223.129.50839 > 192.168.223.2.domain: 38445+ PTR? 129.223.168.192.in-addr.arpa. (46)
0:28:02.488064 IP 192.168.223.2.domain > 192.168.223.129.50839: 38445 NXDomain 0/0/0 (46)
0:28:02.489149 IP 192.168.223.129.33314 > 192.168.223.2.domain: 8713+ PTR? 106.57.228.66.in-addr.arpa. (44)
0:28:02.696097 IP li314-106.members.linode.com.https > 192.168.223.129.41702: Flags [.], seq 1:1461, ack 853, win 64240, length 1460
0:28:02.696138 IP 192.168.223.129.41702 > li314-106.members.linode.com.https: Flags [.], ack 1461, win 64500, length 0
0:28:02.696204 IP li314-106.members.linode.com.https > 192.168.223.129.41702: Flags [P.], seq 1461:2581, ack 853, win 64240, length 1120
0:28:02.696219 IP 192.168.223.129.41702 > li314-106.members.linode.com.https: Flags [.], ack 2581, win 64500, length 0
0:28:02.707878 IP li314-106.members.linode.com.https > 192.168.223.129.41702: Flags [P.], seq 2581:3871, ack 853, win 64240, length 1290
0:28:02.707943 IP 192.168.223.129.41702 > li314-106.members.linode.com.https: Flags [.], ack 3871, win 64500, length 0
0:28:02.735690 IP li314-106.members.linode.com.https > 192.168.223.129.41702: Flags [P.], seq 3871:5161, ack 853, win 64240, length 1290
0:28:02.735745 IP 192.168.223.129.41702 > li314-106.members.linode.com.https: Flags [.], ack 5161, win 64500, length 0
0:28:02.763086 IP li314-106.members.linode.com.https > 192.168.223.129.41702: Flags [P.], seq 5161:6451, ack 853, win 64240, length 1290
0:28:02.763201 IP 192.168.223.129.41702 > li314-106.members.linode.com.https: Flags [.], ack 6451, win 64500, length 0
0:28:02.791800 IP li314-106.members.linode.com.https > 192.168.223.129.41702: Flags [.], seq 6451:7911, ack 853, win 64240, length 1460
0:28:02.791842 IP 192.168.223.129.41702 > li314-106.members.linode.com.https: Flags [.], ack 7911, win 64500, length 0
0:28:02.791915 IP li314-106.members.linode.com.https > 192.168.223.129.41702: Flags [P.], seq 7911:9031, ack 853, win 64240, length 1120
0:28:02.791930 IP 192.168.223.129.41702 > li314-106.members.linode.com.https: Flags [.], ack 9031, win 64500, length 0
0:28:02.845189 IP li314-106.members.linode.com.https > 192.168.223.129.41702: Flags [P.], seq 9031:10321, ack 853, win 64240, length 1290
0:28:02.845229 IP 192.168.223.129.41702 > li314-106.members.linode.com.https: Flags [.], ack 10321, win 64500, length 0
0:28:02.855996 IP 192.168.223.2.domain > 192.168.223.129.36551: 46630 0/1/0 (106)
0:28:02.856027 IP 192.168.223.2.domain > 192.168.223.129.33314: 8713 1/0/0 PTR li314-106.members.linode.com. (86)
0:28:02.872881 IP li314-106.members.linode.com.https > 192.168.223.129.41702: Flags [.], seq 10321:11781, ack 853, win 64240, length 1460
```

tcpdump tcp



```
0 packets dropped by kernel
root@kali:~# tcpdump tcp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
00:26:24.963823 IP 146.185.167.158.https > 192.168.223.129.43319: Flags [FP.], seq 160532471, ack 3067650070, win 64240, length 0
00:26:24.966058 IP 192.168.223.129.43319 > 146.185.167.158.https: Flags [P.], seq 1:32, ack 1, win 58400, length 31
00:26:24.966466 IP 146.185.167.158.https > 192.168.223.129.43319: Flags [.], ack 32, win 64240, length 0
00:26:24.966544 IP 192.168.223.129.43319 > 146.185.167.158.https: Flags [F.], seq 32, ack 1, win 58400, length 0
00:26:24.966737 IP 146.185.167.158.https > 192.168.223.129.43319: Flags [.], ack 33, win 64239, length 0
00:26:25.036659 IP scanme.nmap.org.10003 > 192.168.223.129.58081: Flags [R.], seq 1584608655, ack 4167498206, win 64240, length 0
00:26:25.207805 IP 192.168.223.129.52297 > vip1.G-anycast1.cachefly.net.https: Flags [.], ack 1897168447, win 46720, length 0
00:26:25.208337 IP vip1.G-anycast1.cachefly.net.https > 192.168.223.129.52297: Flags [.], ack 1, win 64240, length 0
00:26:25.260908 IP 192.168.223.129.58083 > scanme.nmap.org.10003: Flags [S], seq 4167629267, win 1024, options [mss 1460], length 0
00:26:25.336850 IP 192.168.223.129.53890 > ec2-54-83-25-6.compute-1.amazonaws.com.https: Flags [P.], seq 1026966981:1026967897, ack 1855873375, win 5
8400, length 916
00:26:25.337343 IP ec2-54-83-25-6.compute-1.amazonaws.com.https > 192.168.223.129.53890: Flags [.], ack 916, win 64240, length 0
00:26:25.550615 IP ec2-54-83-25-6.compute-1.amazonaws.com.https > 192.168.223.129.53890: Flags [P.], seq 1:243, ack 916, win 64240, length 242
00:26:25.550683 IP 192.168.223.129.53890 > ec2-54-83-25-6.compute-1.amazonaws.com.https: Flags [.], ack 243, win 61320, length 0
00:26:26.058973 IP scanme.nmap.org.10003 > 192.168.223.129.58082: Flags [R.], seq 1077807068, ack 4167694803, win 64240, length 0
00:26:26.264891 IP 192.168.223.129.58084 > scanme.nmap.org.10003: Flags [S], seq 4167825872, win 1024, options [mss 1460], length 0
00:26:27.000224 IP 192.168.223.129.58035 > bom05s05-in-f14.1e100.net.http: Flags [.], ack 1584672117, win 32078, length 0
00:26:27.000524 IP bom05s05-in-f14.1e100.net.http > 192.168.223.129.58035: Flags [.], ack 1, win 64240, length 0
00:26:27.036823 IP scanme.nmap.org.10003 > 192.168.223.129.58083: Flags [R.], seq 1928675582, ack 4167629268, win 64240, length 0
00:26:27.267193 IP 192.168.223.129.58076 > scanme.nmap.org.3800: Flags [S], seq 4167301592, win 1024, options [mss 1460], length 0
^C
19 packets captured
19 packets received by filter
0 packets dropped by kernel
```
]

tcpdump -p



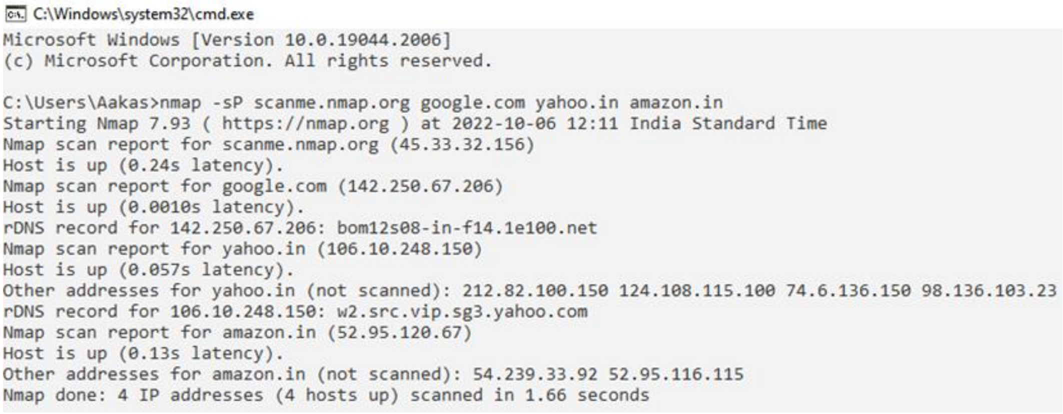
```
  packets dropped by kernel
root@kali:~# tcpdump -p
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
30:22:41.289850 ARP, Request who-has 192.168.223.2 tell 192.168.223.1, length 46
30:22:41.291542 IP 192.168.223.129.42939 > 192.168.223.2.domain: 53788+ PTR? 2.223.168.192.in-addr.arpa. (44)
30:22:41.297942 IP 192.168.223.2.domain > 192.168.223.129.42939: 53788 NXDomain 0/0/0 (44)
30:22:41.298803 IP 192.168.223.129.34567 > 192.168.223.2.domain: 62072+ PTR? 1.223.168.192.in-addr.arpa. (44)
30:22:41.305268 IP 192.168.223.2.domain > 192.168.223.129.34567: 62072 NXDomain 0/0/0 (44)
30:22:41.306193 IP 192.168.223.129.52313 > 192.168.223.2.domain: 43622+ PTR? 129.223.168.192.in-addr.arpa. (46)
30:22:41.313096 IP 192.168.223.2.domain > 192.168.223.129.52313: 43622 NXDomain 0/0/0 (46)
30:22:41.432584 IP 192.168.223.129.58002 > bom05s05-in-f14.1e100.net.http: Flags [.], ack 75386135, win 33570, length 0
30:22:41.434710 IP bom05s05-in-f14.1e100.net.http > 192.168.223.129.58002: Flags [.], ack 1, win 64240, length 0
30:22:41.440545 IP 192.168.223.129.60906 > 192.168.223.2.domain: 54905+ PTR? 14.220.58.216.in-addr.arpa. (44)
30:22:41.511785 IP 192.168.223.2.domain > 192.168.223.129.60906: 54905 4/0/0 PTR bom05s05-in-f14.1e100.net., PTR bom05s05-in-f14.1e100.net., PTR bom0
5s05-in-f14.1e100.net., PTR bom05s05-in-f14.1e100.net. (125)
30:22:41.586946 IP scanme.nmap.org.1021 > 192.168.223.129.58084: Flags [R.], seq 806036961, ack 4167825873, win 64240, length 0
30:22:41.587415 IP 192.168.223.129.42381 > 192.168.223.2.domain: 15054+ PTR? 156.32.33.45.in-addr.arpa. (43)
30:22:41.593669 IP 192.168.223.2.domain > 192.168.223.129.42381: 15054 1/0/0 PTR scanme.nmap.org. (72)
30:22:41.816093 IP 192.168.223.129.58077 > scanme.nmap.org.3052: Flags [S], seq 4167236057, win 1024, options [mss 1460], length 0
30:22:41.974795 ARP, Request who-has 192.168.223.2 tell 192.168.223.1, length 46
30:22:42.585700 IP scanme.nmap.org.3052 > 192.168.223.129.58076: Flags [R.], seq 1631808286, ack 4167301593, win 64240, length 0
30:22:42.816763 IP 192.168.223.129.58078 > scanme.nmap.org.3052: Flags [S], seq 4167432670, win 1024, options [mss 1460], length 0
30:22:42.974888 ARP, Request who-has 192.168.223.2 tell 192.168.223.1, length 46
30:22:43.599499 IP scanme.nmap.org.3052 > 192.168.223.129.58077: Flags [R.], seq 561654480, ack 4167236058, win 64240, length 0
30:22:43.817977 IP 192.168.223.129.58079 > scanme.nmap.org.3052: Flags [S], seq 4167367135, win 1024, options [mss 1460], length 0
^C
21 packets captured
21 packets received by filter
3 packets dropped by kernel
```

9. To study and implement various scanning techniques using Nmap.

Download nmap for windows.

I. Port scanning:

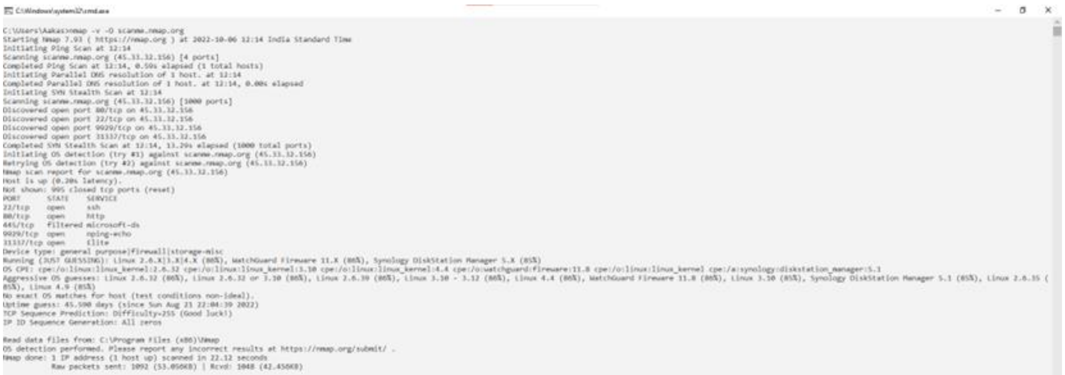
nmap -sP scanme.nmap.org google.com yahoo.in amazon.in



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Aakas>nmap -sP scanme.nmap.org google.com yahoo.in amazon.in
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-06 12:11 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.24s latency).
Nmap scan report for google.com (142.250.67.206)
Host is up (0.0010s latency).
rDNS record for 142.250.67.206: bom12s08-in-f14.1e100.net
Nmap scan report for yahoo.in (106.10.248.150)
Host is up (0.057s latency).
Other addresses for yahoo.in (not scanned): 212.82.100.150 124.108.115.100 74.6.136.150 98.136.103.23
rDNS record for 106.10.248.150: w2.src.vip.sg3.yahoo.com
Nmap scan report for amazon.in (52.95.120.67)
Host is up (0.13s latency).
Other addresses for amazon.in (not scanned): 54.239.33.92 52.95.116.115
Nmap done: 4 IP addresses (4 hosts up) scanned in 1.66 seconds
```

ii. Os fingerprinting:

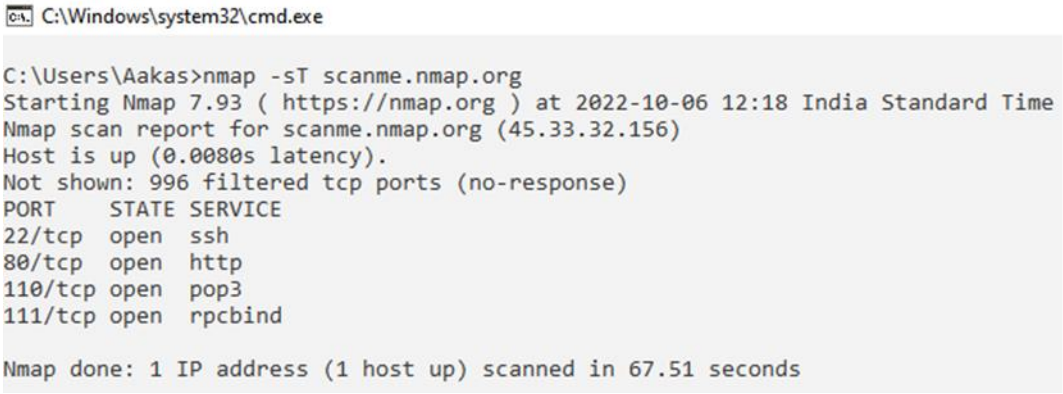
nmap -v -O scanme.nmap.org



```
C:\Windows\system32\cmd.exe
C:\Users\Aakas>nmap -v -O scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-06 12:14 India Standard Time
Initiating Ping Scan at 12:14
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 12:14, 0.59s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:14
Completed Parallel DNS resolution of 1 host. at 12:14, 0.00s elapsed
Initiating SYN Stealth Scan at 12:14
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Completed SYN Stealth Scan at 12:14, 13.29s elapsed (1000 total ports)
Initiating OS detection (try #1) against scanme.nmap.org (45.33.32.156)
Retrying OS detection (try #2) against scanme.nmap.org (45.33.32.156)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.20s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo
31337/tcp open     Elite
Device type: general purpose|firewall|storage-misc
Running (JUST GUESSING): Linux 2.6.X|3.X|4.X (86%), WatchGuard Fireware 11.X (86%), Synology DiskStation Manager 5.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3.10 cpe:/o:linux:linux_kernel:4.4 cpe:/o:watchguard:fireware:11.8 cpe:/o:linux:linux_kernel cpe:/a:synology:diskstation_manager:5.1
Aggressive OS guesses: Linux 2.6.32 (86%), Linux 2.6.32 or 3.10 (86%), Linux 2.6.39 (86%), Linux 3.10 - 3.12 (86%), Linux 4.4 (86%), WatchGuard Fireware 11.8 (86%), Linux 3.10 (85%), Synology DiskStation Manager 5.1 (85%), Linux 2.6.35 (
85%), Linux 4.9 (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 45.590 days (since Sun Aug 21 22:04:39 2022)
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: C:\Program Files (x86)\Nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.12 seconds
           Raw packets sent: 1092 (53.056KB) | Rcvd: 1048 (42.456KB)
```

iii. tcp scan:

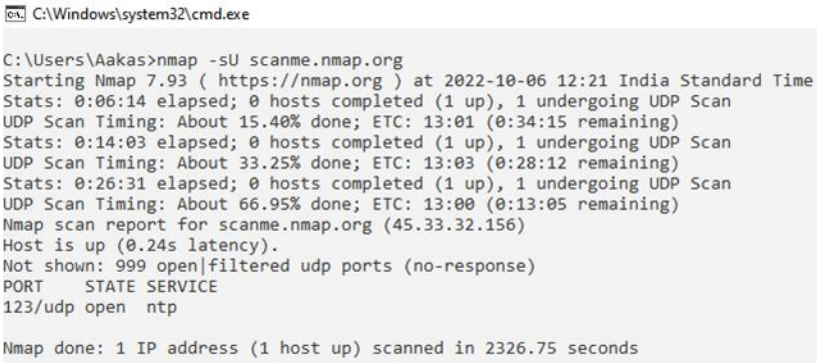
nmap -sT scanme.nmap.org



```
C:\Users\Aakas>nmap -sT scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-06 12:18 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0080s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
110/tcp open  pop3
111/tcp open  rpcbind

Nmap done: 1 IP address (1 host up) scanned in 67.51 seconds
```

iv. Udp scan:

nmap -sU scanme.nmap.org



```
C:\Users\Aakas>nmap -sU scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-06 12:21 India Standard Time
Stats: 0:06:14 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 15.40% done; ETC: 13:01 (0:34:15 remaining)
Stats: 0:14:03 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 33.25% done; ETC: 13:03 (0:28:12 remaining)
Stats: 0:26:31 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 66.95% done; ETC: 13:00 (0:13:05 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.24s latency).
Not shown: 999 open|filtered udp ports (no-response)
PORT    STATE SERVICE
123/udp open  ntp

Nmap done: 1 IP address (1 host up) scanned in 2326.75 seconds
```

10. Study of malicious software using different tools: Use the NESSUS/ISO Kali Linux tool to scan the network for vulnerabilities

Installation & Configuration:

i. You can download the Nessus home feed (free) or professional feed from Nessus website.

ii. Once you download the Nessus home tool, you need to register for generating an activation key. The activation key will be sent to your email id.

iii. Install the tool (Installation of nessus tool will be quite confusing and the installation guide comes handy).

iv. Open the Nessus in the browser, normally it runs on the port 8834 – http://localhost:8834/WelcomeToNessus-Install/welcome and follow the screen.

v. Create an account with Nessus.

vi. Enter the activation code you have obtained by registering with the Nessus website. Also, you can configure the proxy if needed by giving proxy hostname, proxy username and password.

vii. Then scanner gets registered and creates the user account.

viii. Then downloads the necessary plugins (It takes some time for downloading the plugins).

ix. Once the plug-ins are downloaded then it will automatically redirect you to a login screen.

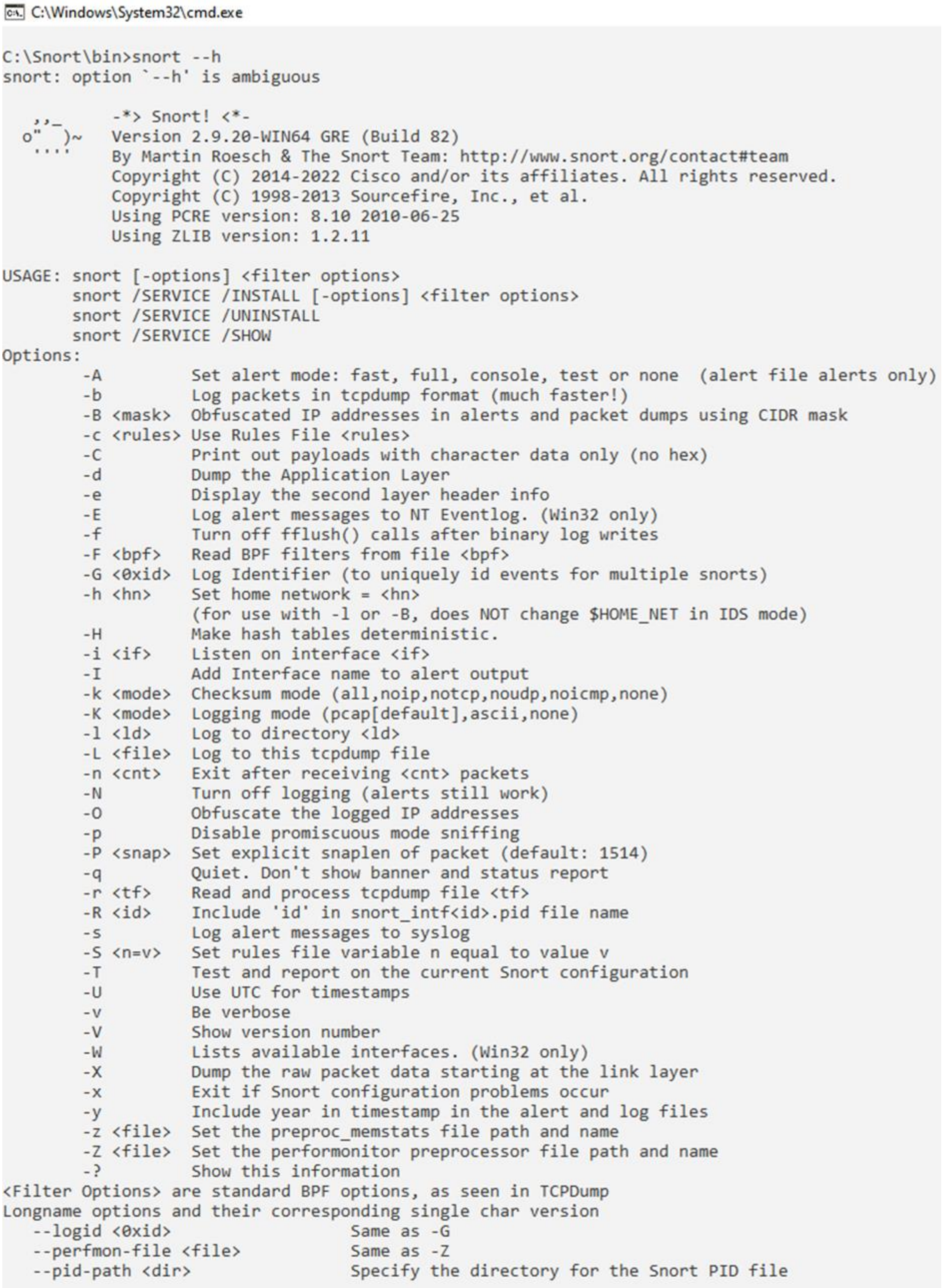
11. Study of Network security by: Set up Snort and study the logs.

Download snort and run in that folder.

Set the path in command prompt

Run the following commands.

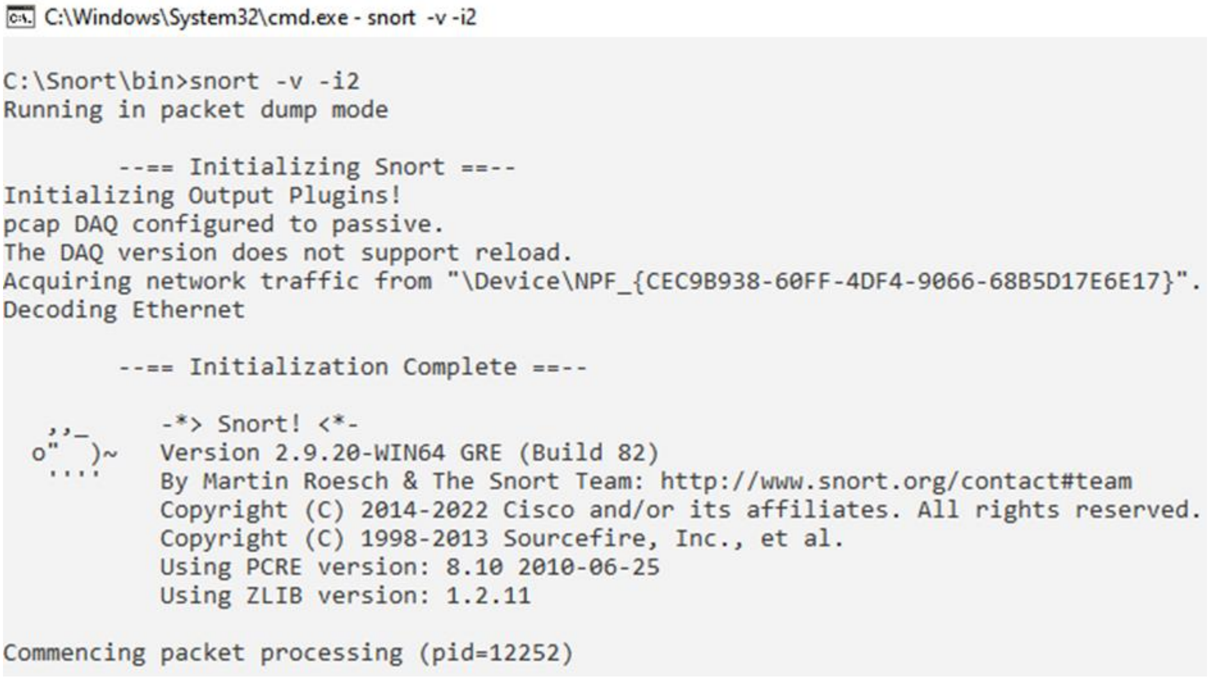
1. dir
2. snort.exe
3. snort --h



```
C:\Snort\bin>snort --h
snort: option `--h' is ambiguous

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20-WIN64 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

USAGE: snort [-options] <filter options>
       snort /SERVICE /INSTALL [-options] <filter options>
       snort /SERVICE /UNINSTALL
       snort /SERVICE /SHOW
Options:
        -A         Set alert mode: fast, full, console, test or none  (alert file alerts only)
        -b         Log packets in tcpdump format (much faster!)
        -B <mask>  Obfuscated IP addresses in alerts and packet dumps using CIDR mask
        -c <rules> Use Rules File <rules>
        -C         Print out payloads with character data only (no hex)
        -d         Dump the Application Layer
        -e         Display the second layer header info
        -E         Log alert messages to NT Eventlog. (Win32 only)
        -f         Turn off fflush() calls after binary log writes
        -F <bpf>   Read BPF filters from file <bpf>
        -G <0xid>  Log Identifier (to uniquely id events for multiple snorts)
        -h <hn>    Set home network = <hn>
                   (for use with -l or -B, does NOT change $HOME_NET in IDS mode)
        -H         Make hash tables deterministic.
        -i <if>    Listen on interface <if>
        -I         Add Interface name to alert output
        -k <mode>  Checksum mode (all,noip,notcp,noudp,noicmp,none)
        -K <mode>  Logging mode (pcap[default],ascii,none)
        -l <ld>    Log to directory <ld>
        -L <file>  Log to this tcpdump file
        -n <cnt>   Exit after receiving <cnt> packets
        -N         Turn off logging (alerts still work)
        -O         Obfuscate the logged IP addresses
        -p         Disable promiscuous mode sniffing
        -P <snap>  Set explicit snaplen of packet (default: 1514)
        -q         Quiet. Don't show banner and status report
        -r <tf>    Read and process tcpdump file <tf>
        -R <id>    Include 'id' in snort_intf<id>.pid file name
        -s         Log alert messages to syslog
        -S <n=v>   Set rules file variable n equal to value v
        -T         Test and report on the current Snort configuration
        -U         Use UTC for timestamps
        -v         Be verbose
        -V         Show version number
        -W         Lists available interfaces. (Win32 only)
        -X         Dump the raw packet data starting at the link layer
        -x         Exit if Snort configuration problems occur
        -y         Include year in timestamp in the alert and log files
        -z <file>  Set the preproc_memstats file path and name
        -Z <file>  Set the performonitor preprocessor file path and name
        -?         Show this information
<Filter Options> are standard BPF options, as seen in TCPDump
Longname options and their corresponding single char version
   --logid <0xid>                 Same as -G
   --perfmon-file <file>          Same as -Z
   --pid-path <dir>               Specify the directory for the Snort PID file
```

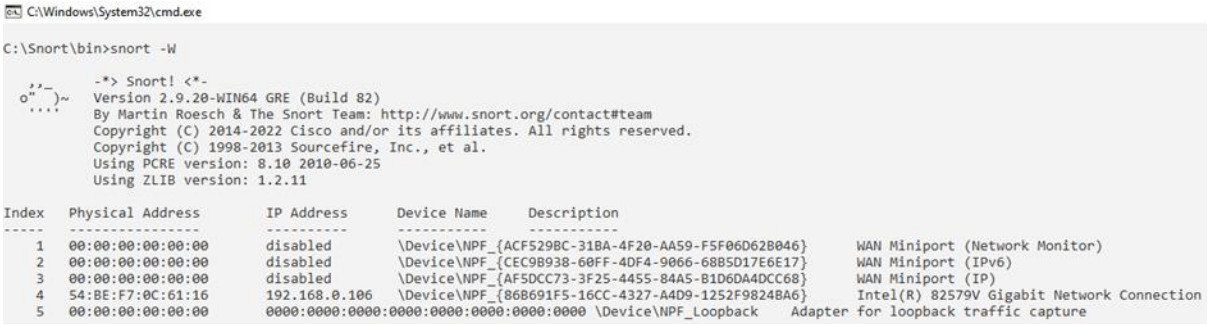
i. Snort in Sniffer mode

snort -v -i2



```
C:\Snort\bin>snort -v -i2
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{CEC9B938-60FF-4DF4-9066-68B5D17E6E17}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20-WIN64 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

Commencing packet processing (pid=12252)
```

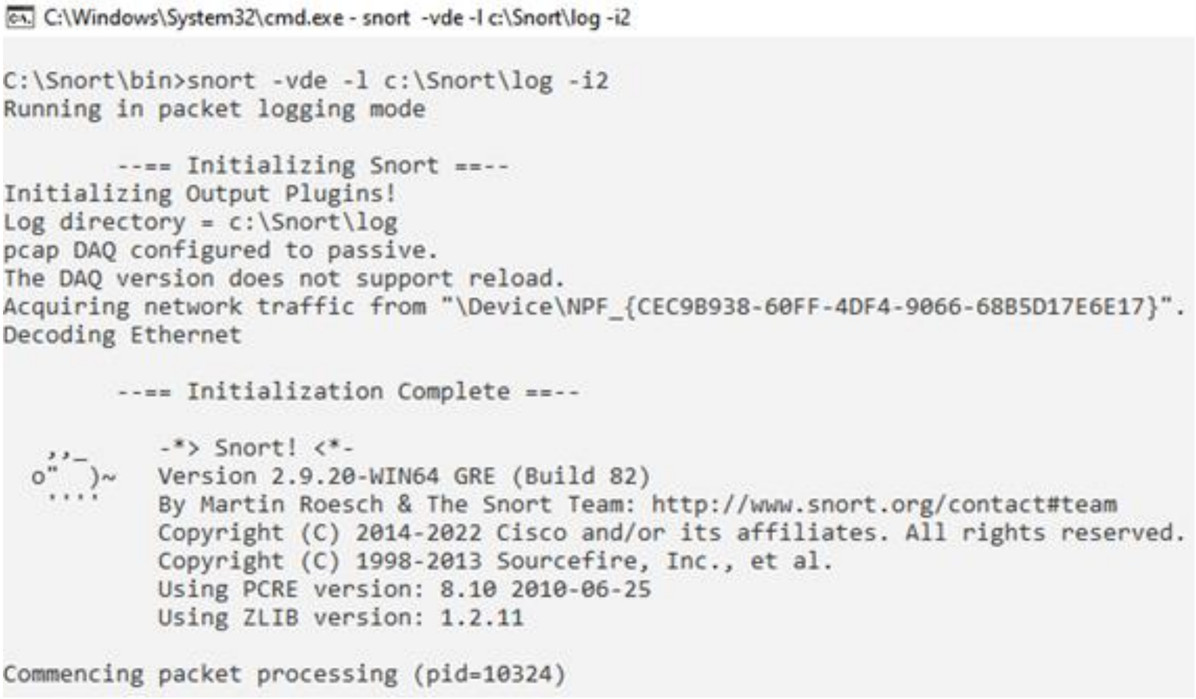
snort -W



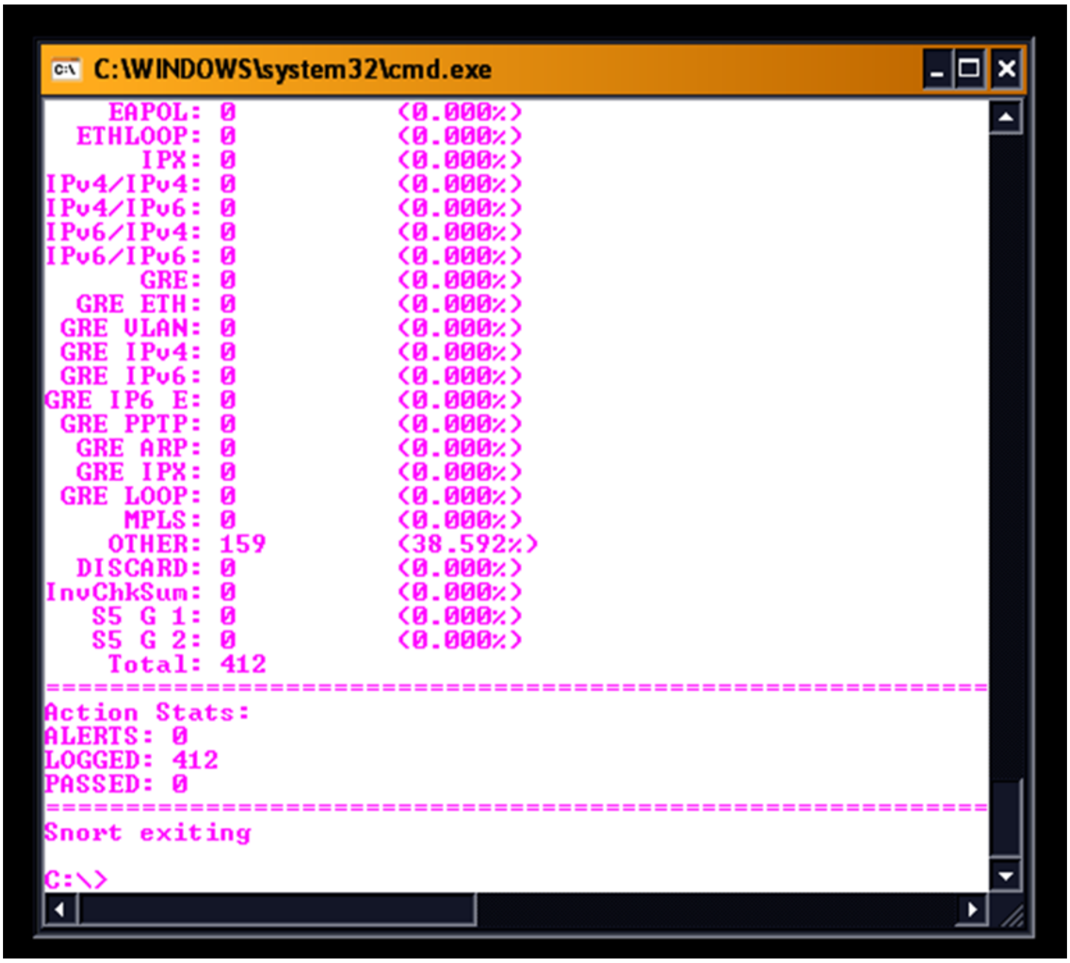
```
C:\Snort\bin>snort -W

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20-WIN64 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   00:00:00:00:00:00       disabled        \Device\NPF_{ACF529BC-31BA-4F20-AA59-F5F06D62B046}      WAN Miniport (Network Monitor)
    2   00:00:00:00:00:00       disabled        \Device\NPF_{CEC9B938-60FF-4DF4-9066-68B5D17E6E17}      WAN Miniport (IPv6)
    3   00:00:00:00:00:00       disabled        \Device\NPF_{AF5DCC73-3F25-4455-84A5-B1D6DA4DCC68}      WAN Miniport (IP)
    4   54:BE:F7:0C:61:16       192.168.0.106   \Device\NPF_{86B691F5-16CC-4327-A4D9-1252F9824BA6}      Intel(R) 82579V Gigabit Network Connection
    5   00:00:00:00:00:00       0000:0000:0000:0000:0000:0000:0000:0000 \Device\NPF_Loopback    Adapter for loopback traffic capture
```

ii. Snort as Packet Logger

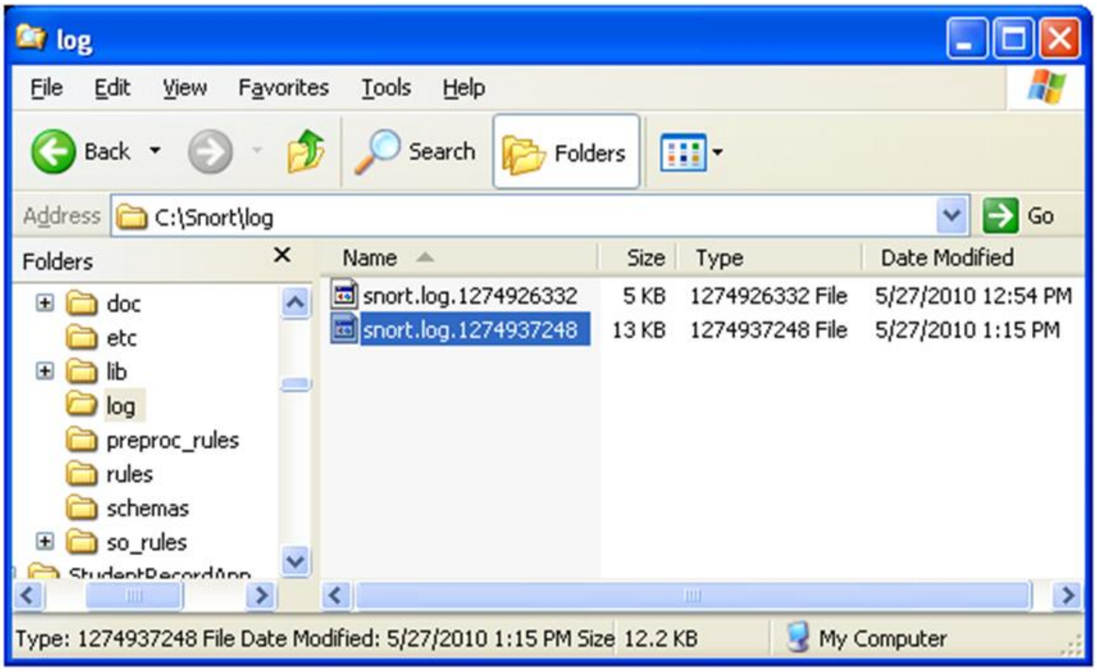
snort -vde -l c:\Snort\log -i2


C:\Windows\System32\cmd.exe - snort -vde -l c:\Snort\log -i2

```
C:\Snort\bin>snort -vde -l c:\Snort\log -i2
Running in packet logging mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Log directory = c:\Snort\log
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{CEC9B938-60FF-4DF4-9066-68B5D17E6E17}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20-WIN64 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

Commencing packet processing (pid=10324)
```



```
    EAPOL: 0          (0.000%)
  ETHLOOP: 0          (0.000%)
      IPX: 0          (0.000%)
IPv4/IPv4: 0          (0.000%)
IPv4/IPv6: 0          (0.000%)
IPv6/IPv4: 0          (0.000%)
IPv6/IPv6: 0          (0.000%)
      GRE: 0          (0.000%)
  GRE ETH: 0          (0.000%)
 GRE VLAN: 0          (0.000%)
 GRE IPv4: 0          (0.000%)
 GRE IPv6: 0          (0.000%)
GRE IP6 E: 0          (0.000%)
 GRE PPTP: 0          (0.000%)
  GRE ARP: 0          (0.000%)
  GRE IPX: 0          (0.000%)
 GRE LOOP: 0          (0.000%)
     MPLS: 0          (0.000%)
    OTHER: 159        (38.592%)
  DISCARD: 0          (0.000%)
InvChkSum: 0          (0.000%)
   S5 G 1: 0          (0.000%)
   S5 G 2: 0          (0.000%)
    Total: 412
============================================================
Action Stats:
ALERTS: 0
LOGGED: 412
PASSED: 0
============================================================
Snort exiting

C:\>
```



Address: C:\Snort\log

Name	Size	Type	Date Modified
snort.log.1274926332	5 KB	1274926332 File	5/27/2010 12:54 PM
snort.log.1274937248	13 KB	1274937248 File	5/27/2010 1:15 PM

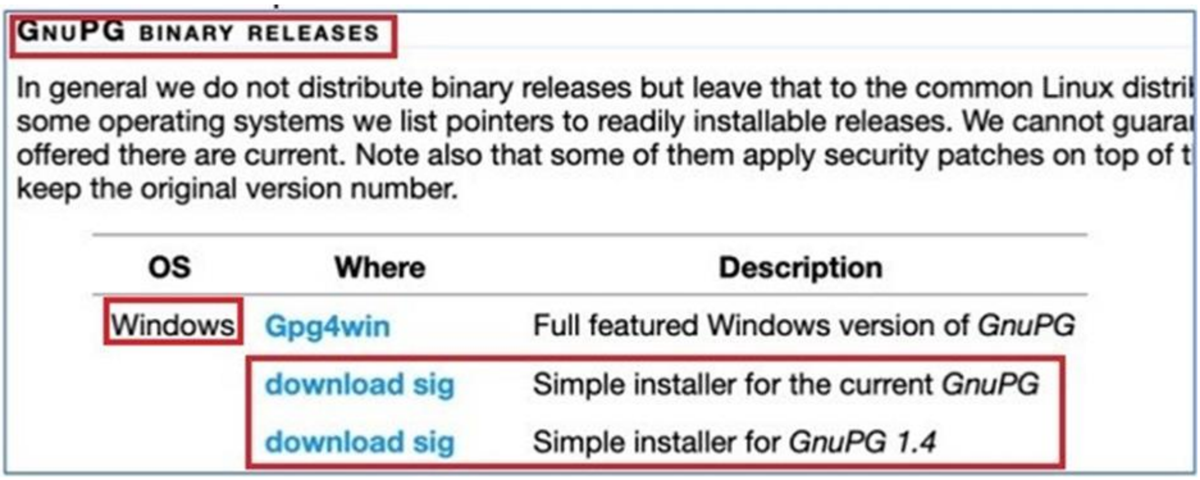
Type: 1274937248 File Date Modified: 5/27/2010 1:15 PM Size 12.2 KB

12. Explore the GPG tool to implement email security

STEP 1 - DOWNLOAD AND INSTALL GNUPG

1. Go to the GnuPG website to download the software: https://gnupg.org/download/index.html.

2. Scroll to GnuPG Binary Releases.



GNUPG BINARY RELEASES

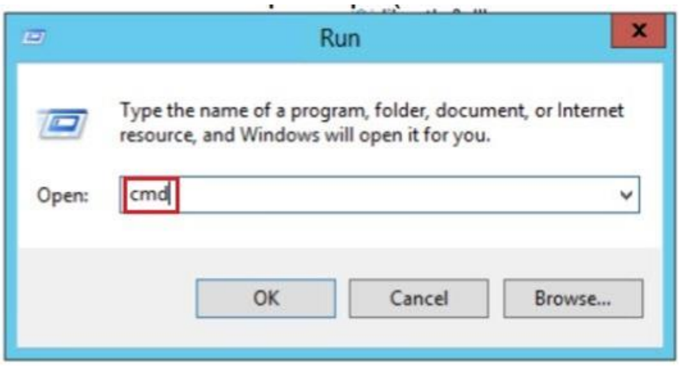
In general we do not distribute binary releases but leave that to the common Linux distri
some operating systems we list pointers to readily installable releases. We cannot guara
offered there are current. Note also that some of them apply security patches on top of t
keep the original version number.

OS	Where	Description
Windows	Gpg4win	Full featured Windows version of *GnuPG*
	download sig	Simple installer for the current *GnuPG*
	download sig	Simple installer for *GnuPG 1.4*

3. For the Windows OS, select the Download Sig link either for Simple Installer for the Current GnuPG or Simple Installer for GnuPG 1.4.

4. Select Run and follow the steps to install the software.

5. Open a command prompt (Windows > Run > cmd > OK or Enter key).

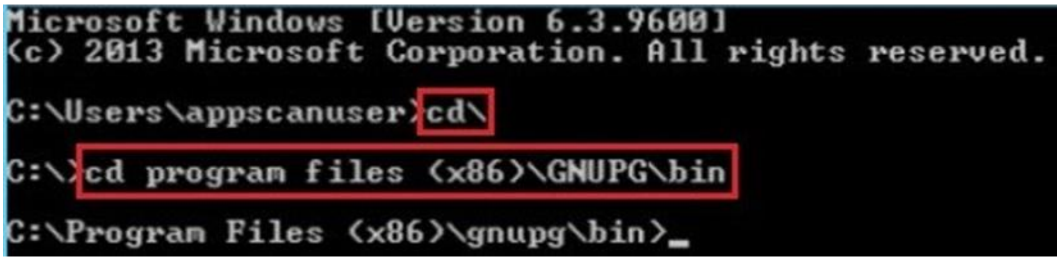


Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

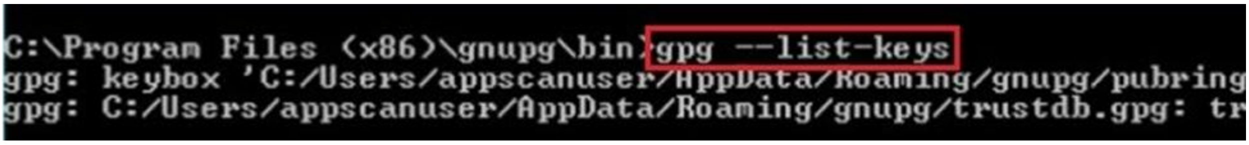
6. Enter command cd\ and press the Enter key to move to the root directory (for example, enter: C:\).



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\appscanuser>cd\

C:\>cd program files (x86)\GNUPG\bin

C:\Program Files (x86)\gnupg\bin>_
```

7. Change the directory where GNUPG is installed by entering a command like cd Program Files (x86)\gnupg\bin\.

Enter gpg --list-keys to initialize and create trustdb (trust database) before first time use.



```
C:\Program Files (x86)\gnupg\bin>gpg --list-keys
gpg: keybox 'C:/Users/appscanuser/AppData/Roaming/gnupg/pubring
gpg: C:/Users/appscanuser/AppData/Roaming/gnupg/trustdb.gpg: tr
```

STEP 2 - FINISH INSTALL FOR OPERATING SYSTEM

The following shows what you enter in a Command Prompt window for each operating system. This assumes you already went to the GnuPG website and downloaded/installed the software.

In all the operating systems, to check if your software installed correctly, enter gpg --help in the command line.

STEP 3 - IMPORT PUBLIC PGP KEY AND ENCRYPT ZIP FILE