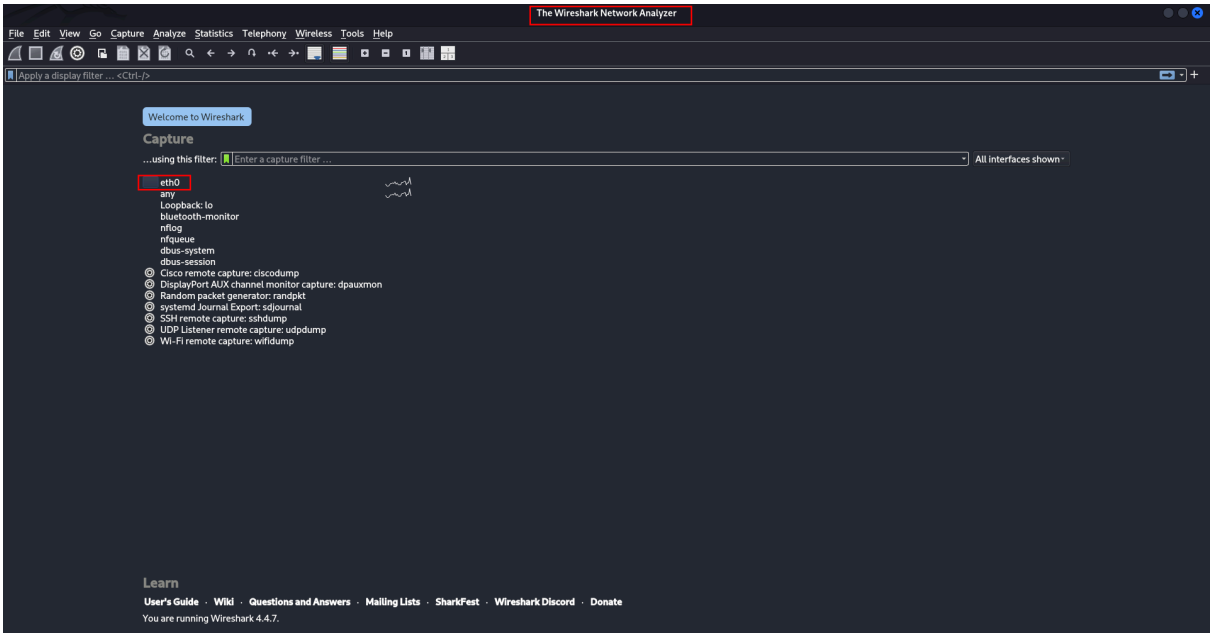
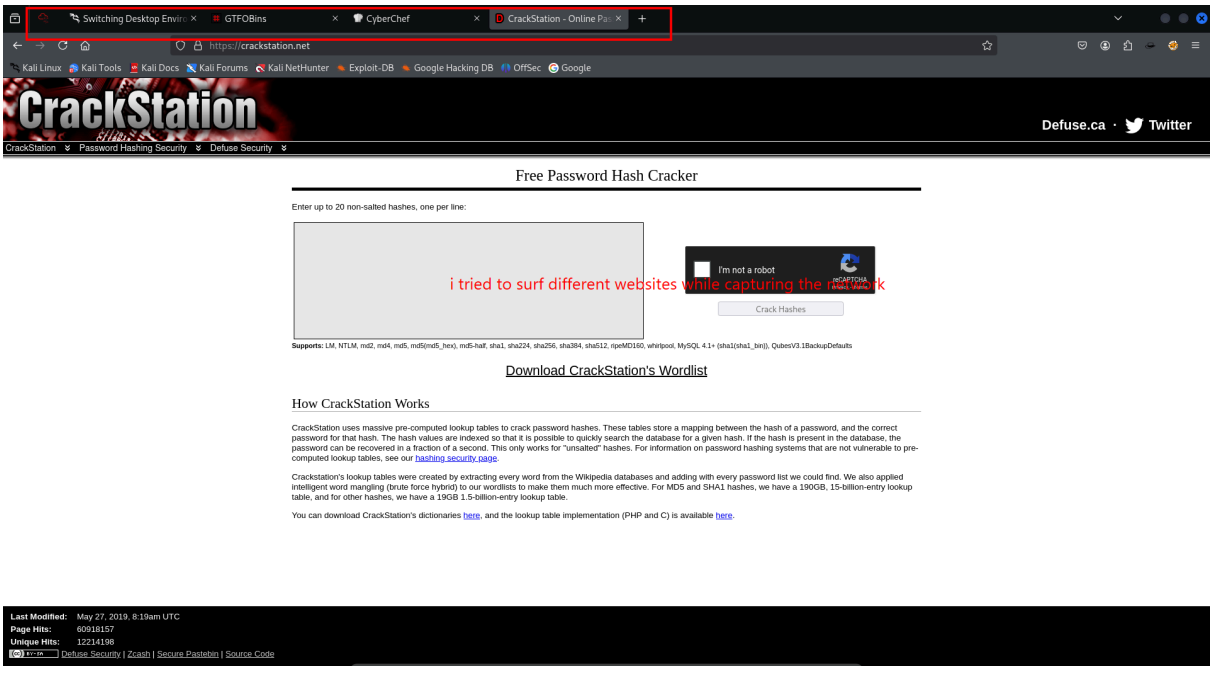
Task_5

Status	In progress

Wireshark : used to capture the network traffic.

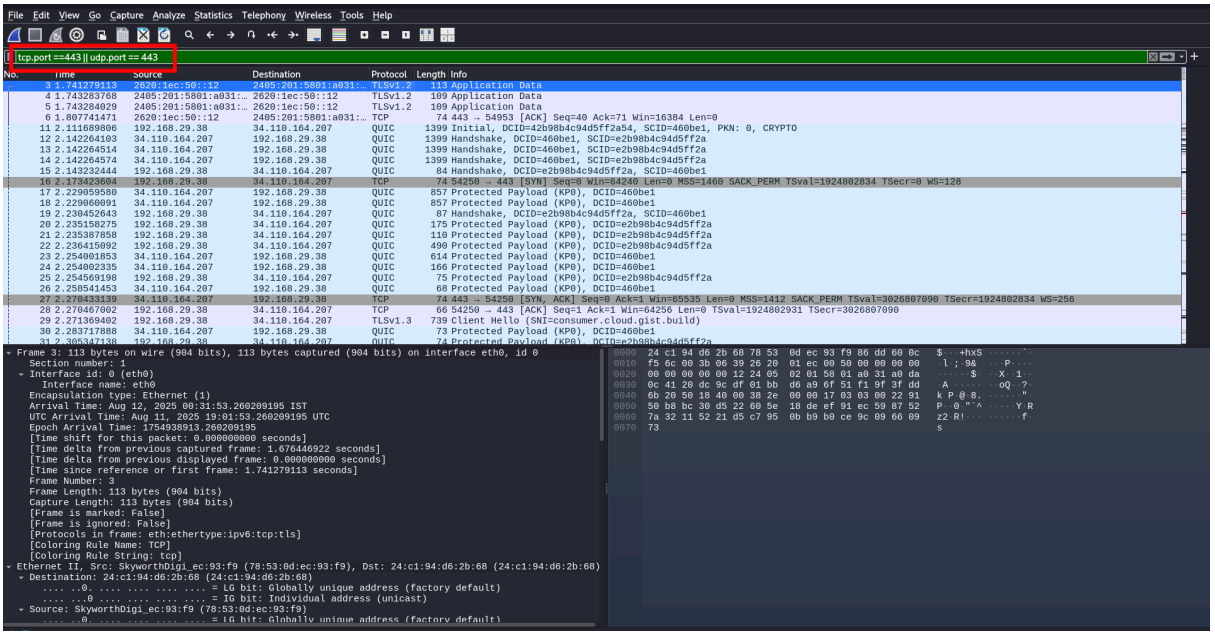
Here i will use eth0 interface to capture the network traffic.

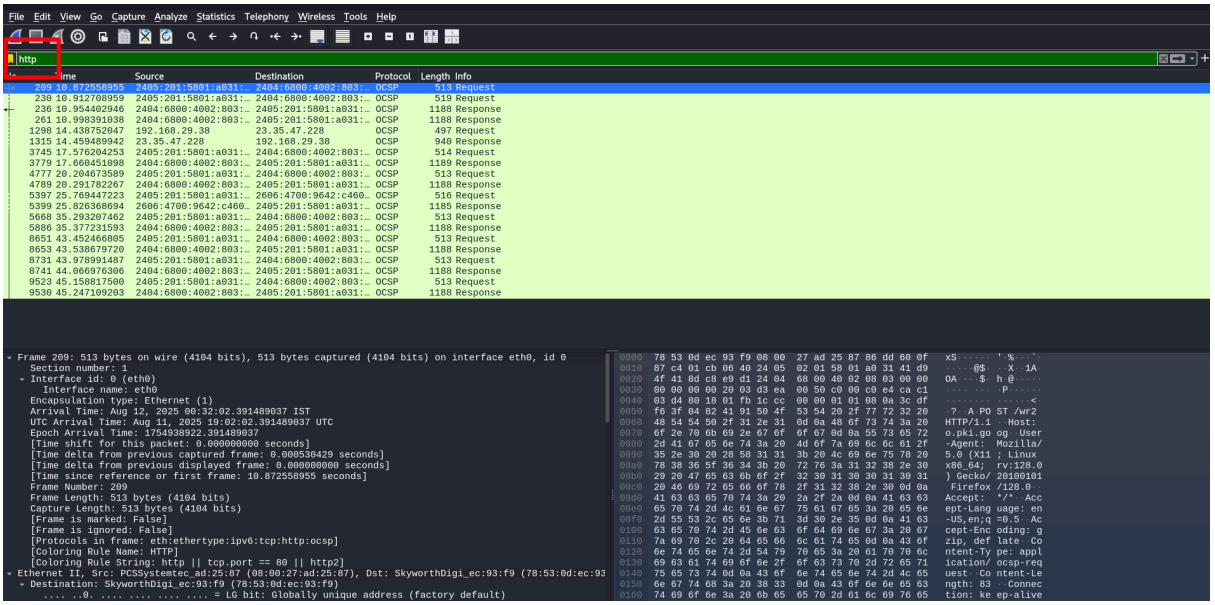


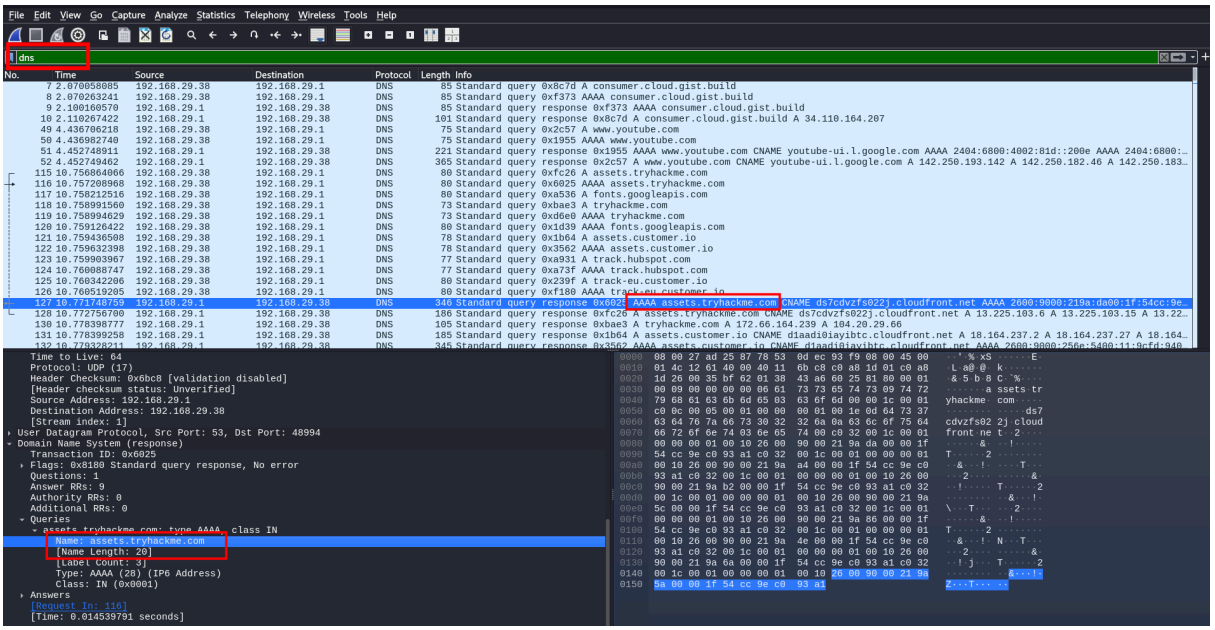


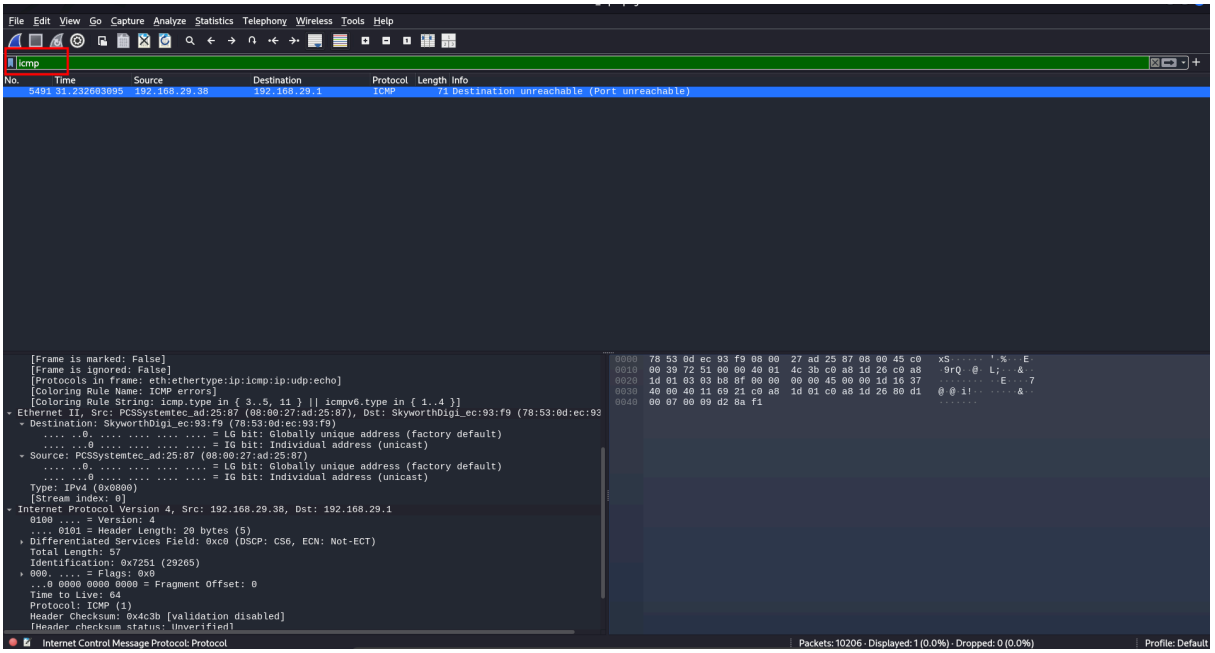
```
┌──(kali㉿kali)-[~]
└─$ ping google.com
PING google.com (2404:6800:4002:827::200e) 56 data bytes
64 bytes from tzdelb-bg-in-x0e.1e100.net (2404:6800:4002:827::200e): icmp_seq=1 ttl=118 time=44.6 ms
64 bytes from tzdelb-bg-in-x0e.1e100.net (2404:6800:4002:827::200e): icmp_seq=2 ttl=118 time=85.0 ms
64 bytes from tzdelb-bg-in-x0e.1e100.net (2404:6800:4002:827::200e): icmp_seq=3 ttl=118 time=42.1 ms
64 bytes from tzdelb-bg-in-x0e.1e100.net (2404:6800:4002:827::200e): icmp_seq=4 ttl=118 time=41.3 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4009ms
rtt min/avg/max/mdev = 41.329/53.246/85.007/18.376 ms

┌──(kali㉿kali)-[~]
└─$ nslookup tryhackme.com
Server:         192.168.29.1
Address:        192.168.29.1#53

Non-authoritative answer:
Name:   tryhackme.com
Address: 104.20.29.66
Name:   tryhackme.com
Address: 172.66.164.239
Name:   tryhackme.com
Address: 2606:4700:9646:d299:d3a6:b62:ae35:d89c


┌──(kali㉿kali)-[~]
└─$ nslookup google.com
Server:         192.168.29.1
Address:        192.168.29.1#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.77.206
Name:   google.com
Address: 2404:6800:4002:827::200e
```

I perform this while capturing the network




File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
209 10.872558955 2405:201:5801:a031:… 2404:6800:4002:803:… OCSP 513 Request
230 10.912708959 2405:201:5801:a031:… 2404:6800:4002:803:… OCSP 519 Request
236 10.954402946 2404:6800:4002:803:… 2405:201:5801:a031:… OCSP 1188 Response
261 10.998391038 2404:6800:4002:803:… 2405:201:5801:a031:… OCSP 1188 Response
1298 14.438752047 192.168.29.38 23.35.47.228 OCSP 497 Request
1315 14.459489942 23.35.47.228 192.168.29.38 OCSP 940 Response
3745 17.576204253 2405:201:5801:a031:… 2404:6800:4002:803:… OCSP 514 Request
3779 17.660451098 2404:6800:4002:803:… 2405:201:5801:a031:… OCSP 1189 Response
4777 20.204673589 2405:201:5801:a031:… 2404:6800:4002:803:… OCSP 513 Request
4789 20.291782267 2404:6800:4002:803:… 2405:201:5801:a031:… OCSP 1188 Response
5397 25.769447223 2405:201:5801:a031:… 2606:4700:9642:c460… OCSP 516 Request
5399 25.826368694 2606:4700:9642:c460… 2405:201:5801:a031:… OCSP 1185 Response
5668 35.293207462 2405:201:5801:a031:… 2404:6800:4002:803:… OCSP 513 Request
5886 35.377231593 2404:6800:4002:803:… 2405:201:5801:a031:… OCSP 1188 Response
8651 43.452466805 2405:201:5801:a031:… 2404:6800:4002:803:… OCSP 513 Request
8653 43.538679720 2404:6800:4002:803:… 2405:201:5801:a031:… OCSP 1188 Response
8731 43.978991487 2405:201:5801:a031:… 2404:6800:4002:803:… OCSP 513 Request
8741 44.066976306 2404:6800:4002:803:… 2405:201:5801:a031:… OCSP 1188 Response
9523 45.158817500 2405:201:5801:a031:… 2404:6800:4002:803:… OCSP 513 Request
9530 45.247109203 2404:6800:4002:803:… 2405:201:5801:a031:… OCSP 1188 Response
Frame 209: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits) on interface eth0, id 0
Section number: 1
Interface id: 0 (eth0)
Interface name: eth0
Encapsulation type: Ethernet (1)
Arrival Time: Aug 12, 2025 00:32:02.391489037 IST
UTC Arrival Time: Aug 11, 2025 19:02:02.391489037 UTC
Epoch Arrival Time: 1754938922.391489037
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.000530429 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 10.872558955 seconds]
Frame Number: 209
Frame Length: 513 bytes (4104 bits)
Capture Length: 513 bytes (4104 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ipv6:tcp:http:ocsp]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: PCSSystemtec_ad:25:87 (08:00:27:ad:25:87), Dst: SkyworthDigi_ec:93:f9 (78:53:0d:ec:93
Destination: SkyworthDigi_ec:93:f9 (78:53:0d:ec:93:f9)
.... ..0. .... = LG bit: Globally unique address (factory default)
0000 78 53 0d ec 93 f9 08 00 27 ad 25 87 86 dd 60 0f xS····· ' %···`
0010 87 c4 01 cb 06 40 24 05 02 01 58 01 a0 31 41 d9 ·····@$· ··X··1A
0020 4f 41 8d c8 e9 d1 24 04 68 00 40 02 08 03 00 00 OA····$· h·@·····
0030 00 00 00 00 20 03 d3 ea 00 50 c0 00 c0 e4 ca c1 ···· ···· ·P·····
0040 03 d4 80 18 01 fb 1c cc 00 00 01 01 08 0a 3c df ·····<·
0050 f6 3f 64 82 41 91 50 4f 53 54 20 2f 77 72 32 20 ·?·A·PO ST /wr2
0060 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 HTTP/1.1 ··Host:
0070 6f 2e 70 6b 69 2e 67 6f 6f 67 0d 0a 55 73 65 72 o.pki.go og··User
0080 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f -Agent: Mozilla/
0090 35 2e 30 20 28 58 31 31 3b 20 4c 69 6e 75 78 20 5.0 (X11 ; Linux
00a0 78 38 36 5f 36 34 3b 20 72 76 3a 31 32 38 2e 30 x86_64; rv:128.0
00b0 29 20 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31) Gecko/ 20100101
00c0 20 46 69 72 65 66 6f 78 2f 31 32 38 2e 30 0d 0a Firefox /128.0··
00d0 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 41 63 63 Accept: */*··Acc
00e0 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e ept-Lang uage: en
00f0 2d 55 53 2c 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63 -US,en;q =0.5··Ac
0100 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 cept-Enc oding: g
0110 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 43 6f zip, def late··Co
0120 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c ntent-Ty pe: appl
0130 69 63 61 74 69 6f 6e 2f 6f 63 73 70 2d 72 65 71 ication/ ocsp-req
0140 75 65 73 74 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 uest··Co ntent-Le
0150 6e 67 74 68 3a 20 38 33 0d 0a 43 6f 6e 6e 65 63 ngth: 83 ··Connec
0160 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 tion: ke ep-alive


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
7 2.070058085 192.168.29.38 192.168.29.1 DNS 85 Standard query 0x8c7d A consumer.cloud.gist.build
8 2.070263241 192.168.29.38 192.168.29.1 DNS 85 Standard query 0xf373 AAAA consumer.cloud.gist.build
9 2.100160570 192.168.29.1 192.168.29.38 DNS 85 Standard query response 0xf373 AAAA consumer.cloud.gist.build
10 2.110267422 192.168.29.1 192.168.29.38 DNS 101 Standard query response 0x8c7d A consumer.cloud.gist.build A 34.110.164.207
49 4.436706218 192.168.29.38 192.168.29.1 DNS 75 Standard query 0x2c57 A www.youtube.com
50 4.436982740 192.168.29.38 192.168.29.1 DNS 75 Standard query 0x1955 AAAA www.youtube.com
51 4.452748911 192.168.29.1 192.168.29.38 DNS 221 Standard query response 0x1955 AAAA www.youtube.com CNAME youtube-ui.l.google.com AAAA 2404:6800:4002:81d::200e AAAA 2404:6800:…
52 4.452749402 192.168.29.1 192.168.29.38 DNS 365 Standard query response 0x2c57 A www.youtube.com CNAME youtube-ui.l.google.com A 142.250.193.142 A 142.250.182.46 A 142.250.183…
115 10.756864066 192.168.29.38 192.168.29.1 DNS 80 Standard query 0xfc26 A assets.tryhackme.com
116 10.757208968 192.168.29.38 192.168.29.1 DNS 80 Standard query 0x6025 AAAA assets.tryhackme.com
117 10.758212516 192.168.29.38 192.168.29.1 DNS 80 Standard query 0xa536 A fonts.googleapis.com
118 10.758991560 192.168.29.38 192.168.29.1 DNS 73 Standard query 0xbae3 A tryhackme.com
119 10.758994629 192.168.29.38 192.168.29.1 DNS 73 Standard query 0xd6e0 AAAA tryhackme.com
120 10.759126422 192.168.29.38 192.168.29.1 DNS 80 Standard query 0x1d39 AAAA fonts.googleapis.com
121 10.759436508 192.168.29.38 192.168.29.1 DNS 78 Standard query 0x1b64 A assets.customer.io
122 10.759632398 192.168.29.38 192.168.29.1 DNS 78 Standard query 0x3562 AAAA assets.customer.io
123 10.759903967 192.168.29.38 192.168.29.1 DNS 77 Standard query 0xa931 A track.hubspot.com
124 10.760088747 192.168.29.38 192.168.29.1 DNS 77 Standard query 0xa73f AAAA track.hubspot.com
125 10.760342206 192.168.29.38 192.168.29.1 DNS 80 Standard query 0x239f A track-eu.customer.io
126 10.760519205 192.168.29.38 192.168.29.1 DNS 80 Standard query 0xf180 AAAA track-eu.customer.io
127 10.771478759 192.168.29.1 192.168.29.38 DNS 346 Standard query response 0x6025 AAAA assets.tryhackme.com CNAME ds7cdvzfs022j.cloudfront.net AAAA 2600:9000:219a:da00:1f:54cc:9e…
128 10.772756700 192.168.29.1 192.168.29.38 DNS 186 Standard query response 0xfc26 A assets.tryhackme.com CNAME ds7cdvzfs022j.cloudfront.net A 13.225.103.6 A 13.225.103.15 A 13.22…
130 10.778398777 192.168.29.1 192.168.29.38 DNS 105 Standard query response 0xbae3 A tryhackme.com A 172.66.164.239 A 104.20.29.66
131 10.778399258 192.168.29.1 192.168.29.38 DNS 185 Standard query response 0x1b64 A assets.customer.io CNAME d1aadi0iayibtc.cloudfront.net A 18.164.237.2 A 18.164.237.27 A 18.164…
132 10.779329211 192.168.29.1 192.168.29.38 DNS 345 Standard query response 0x3562 AAAA assets.customer.io CNAME d1aadi0iayibtc.cloudfront.net AAAA 2600:9000:256e:5400:11:9cf1:340…
Time to Live: 64
Protocol: UDP (17)
Header Checksum: 0x6bc8 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.29.1
Destination Address: 192.168.29.38
[Stream index: 1]
User Datagram Protocol, Src Port: 53, Dst Port: 48994
Domain Name System (response)
Transaction ID: 0x6025
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 9
Authority RRs: 0
Additional RRs: 0
Queries
assets.tryhackme.com: type AAAA, class IN
Name: assets.tryhackme.com
[Name Length: 20]
[Label Count: 3]
Type: AAAA (28) (IP6 Address)
Class: IN (0x0001)
Answers
[Request In: 116]
[Time: 0.014539791 seconds]
0000 08 00 27 ad 25 87 78 53 0d ec 93 f9 08 00 45 00 ··'·%·xS ····· E·
0010 01 4c 12 61 40 00 40 11 6b c8 c0 a8 1d 01 c0 a8 ·L·a@·@· k·····
0020 1d 26 00 35 bf 62 01 38 43 a6 60 25 81 80 00 01 ·&·5·b·8 C·`%····
0030 00 09 00 00 00 00 06 61 73 73 65 74 73 09 74 72 ·····a ssets·tr
0040 79 68 61 63 6b 6d 65 03 63 6f 6d 00 00 1c 00 01 yhackme· com·····
0050 c0 0c 00 05 00 01 00 00 00 01 00 1e 0d 64 73 37 ····· ····· ·····ds7
0060 63 64 76 7a 66 73 30 32 32 6a 0a 63 6c 6f 75 64 cdvzfs02 2j·cloud
0070 66 72 6f 6e 74 03 6e 65 74 00 c0 32 00 1c 00 01 front·ne t··2····
0080 00 00 00 01 00 10 26 00 90 00 21 9a da 00 00 1f ····· &· ··!·····
0090 54 cc 9e c0 93 a1 c0 32 00 1c 00 01 00 00 00 01 T····· 2·· ·····
00a0 00 10 26 00 90 00 21 9a a4 00 00 1f 54 cc 9e c0 ··&··· !· ····T···
00b0 93 a1 c0 32 00 1c 00 01 00 00 00 01 00 10 26 00 ···2···· ····· &·
00c0 90 00 21 9a b2 00 00 1f 54 cc 9e c0 93 a1 c0 32 ··!····· T····· 2
00d0 00 1c 00 01 00 00 00 01 00 10 26 00 90 00 21 9a ····· ····· &···!·
00e0 5c 00 00 1f 54 cc 9e c0 93 a1 c0 32 00 1c 00 01 \···T··· ···2····
00f0 00 00 00 01 00 10 26 00 90 00 21 9a 86 00 00 1f ····· &· ··!·····
0100 54 cc 9e c0 93 a1 c0 32 00 1c 00 01 00 00 00 01 T····· 2 ·····
0110 00 10 26 00 90 00 21 9a 4e 00 00 1f 54 cc 9e c0 ··&··· !· N···T···
0120 93 a1 c0 32 00 1c 00 01 00 00 00 01 00 10 26 00 ···2···· ····· &·
0130 90 00 21 9a 6a 00 00 1f 54 cc 9e c0 93 a1 c0 32 ··!·j··· T····· 2
0140 00 1c 00 01 00 00 00 01 00 10 26 00 90 00 21 9a ····· ····· &···!·
0150 5a 00 00 1f 54 cc 9e c0 93 a1 Z···T··· ··


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
5491 31.232603095 192.168.29.38 192.168.29.1 ICMP 71 Destination unreachable (Port unreachable)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:icmp:ip:udp:echo]
[Coloring Rule Name: ICMP errors]
[Coloring Rule String: icmp.type in { 3..5, 11 } || icmpv6.type in { 1..4 }]
Ethernet II, Src: PCSSystemtec_ad:25:87 (08:00:27:ad:25:87), Dst: SkyworthDigi_ec:93:f9 (78:53:0d:ec:93
Destination: SkyworthDigi_ec:93:f9 (78:53:0d:ec:93:f9)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: PCSSystemtec_ad:25:87 (08:00:27:ad:25:87)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
[Stream index: 0]
Internet Protocol Version 4, Src: 192.168.29.38, Dst: 192.168.29.1
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
Total Length: 57
Identification: 0x7251 (29265)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: ICMP (1)
Header Checksum: 0x4c3b [validation disabled]
[Header checksum status: Unverified]
0000 78 53 0d ec 93 f9 08 00 27 ad 25 87 08 00 45 c0
0010 00 39 72 51 00 00 40 01 4c 3b c0 a8 1d 26 c0 a8
0020 1d 01 03 03 b8 0f 00 00 00 00 45 00 00 1d 16 37
0030 40 00 40 11 69 21 c0 a8 1d 01 c0 a8 1d 26 80 d1
0040 00 07 00 09 d2 8a f1
Internet Control Message Protocol: Protocol
Packets: 10206 · Displayed: 1 (0.0%) · Dropped: 0 (0.0%)
Profile: Default