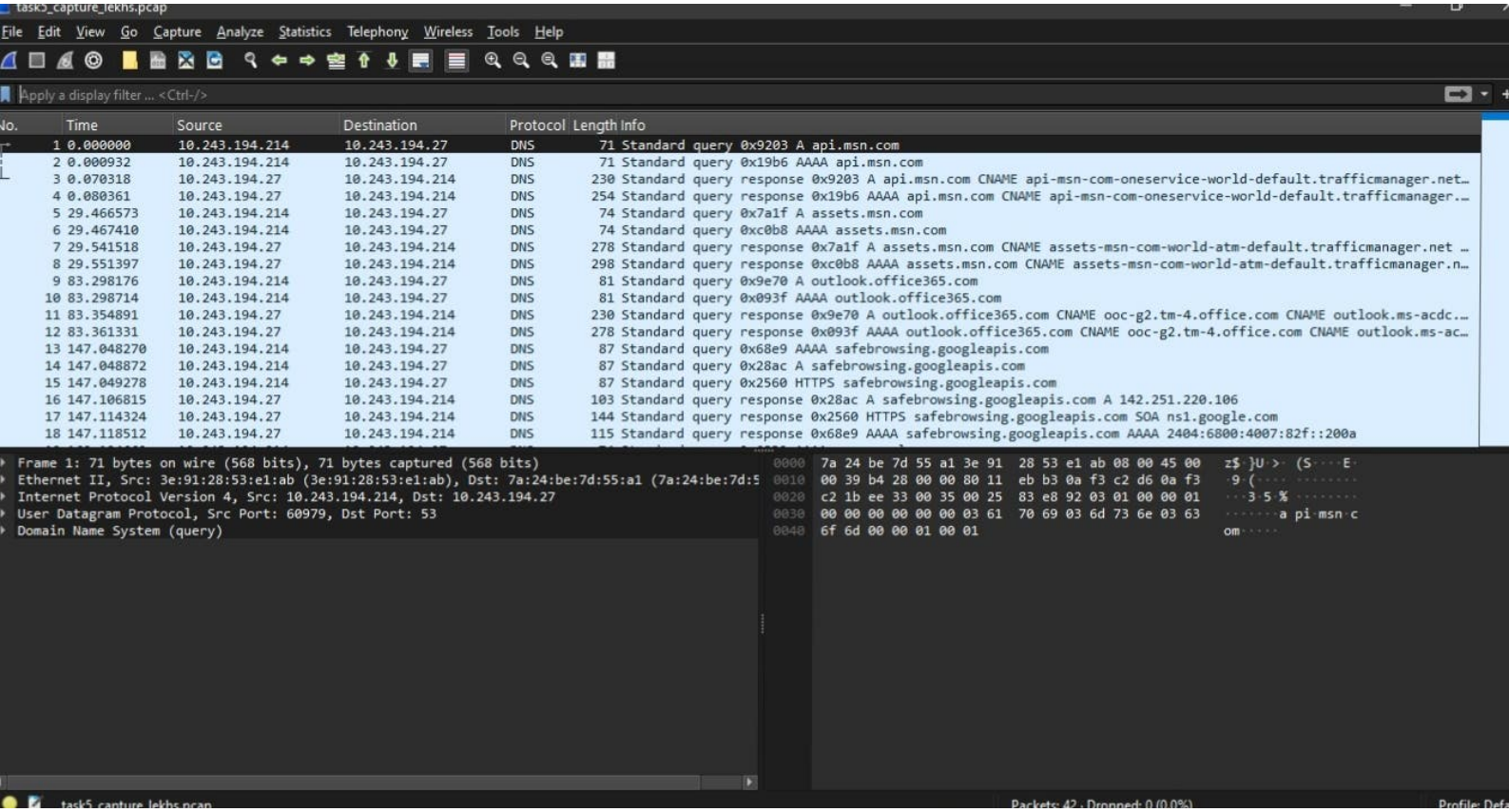
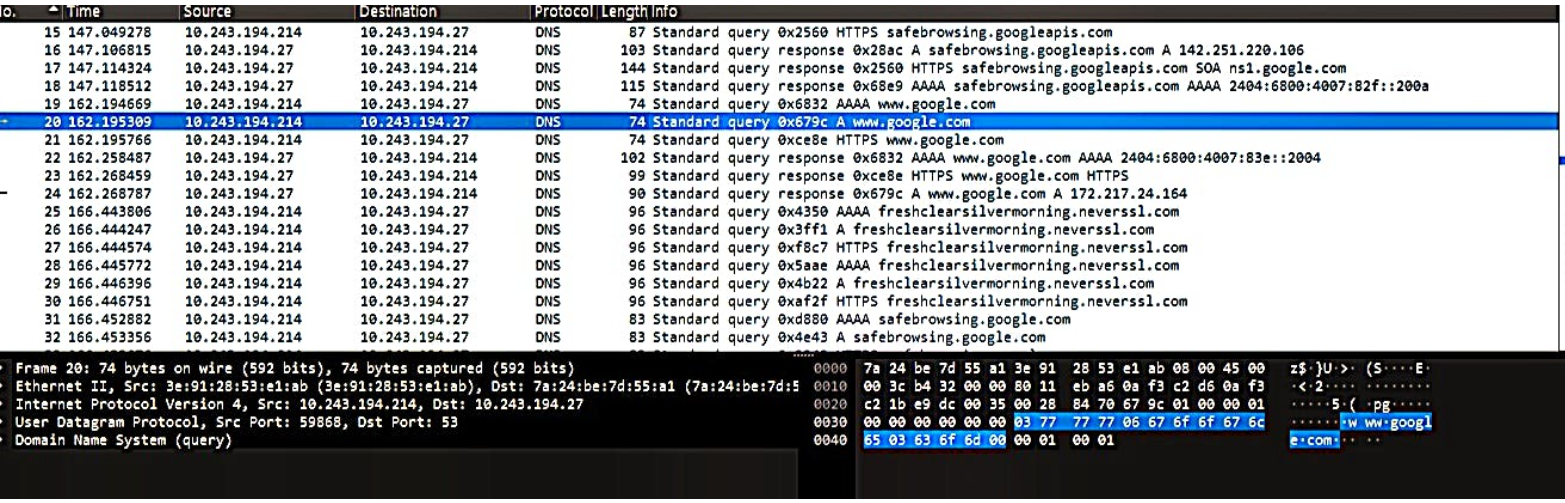
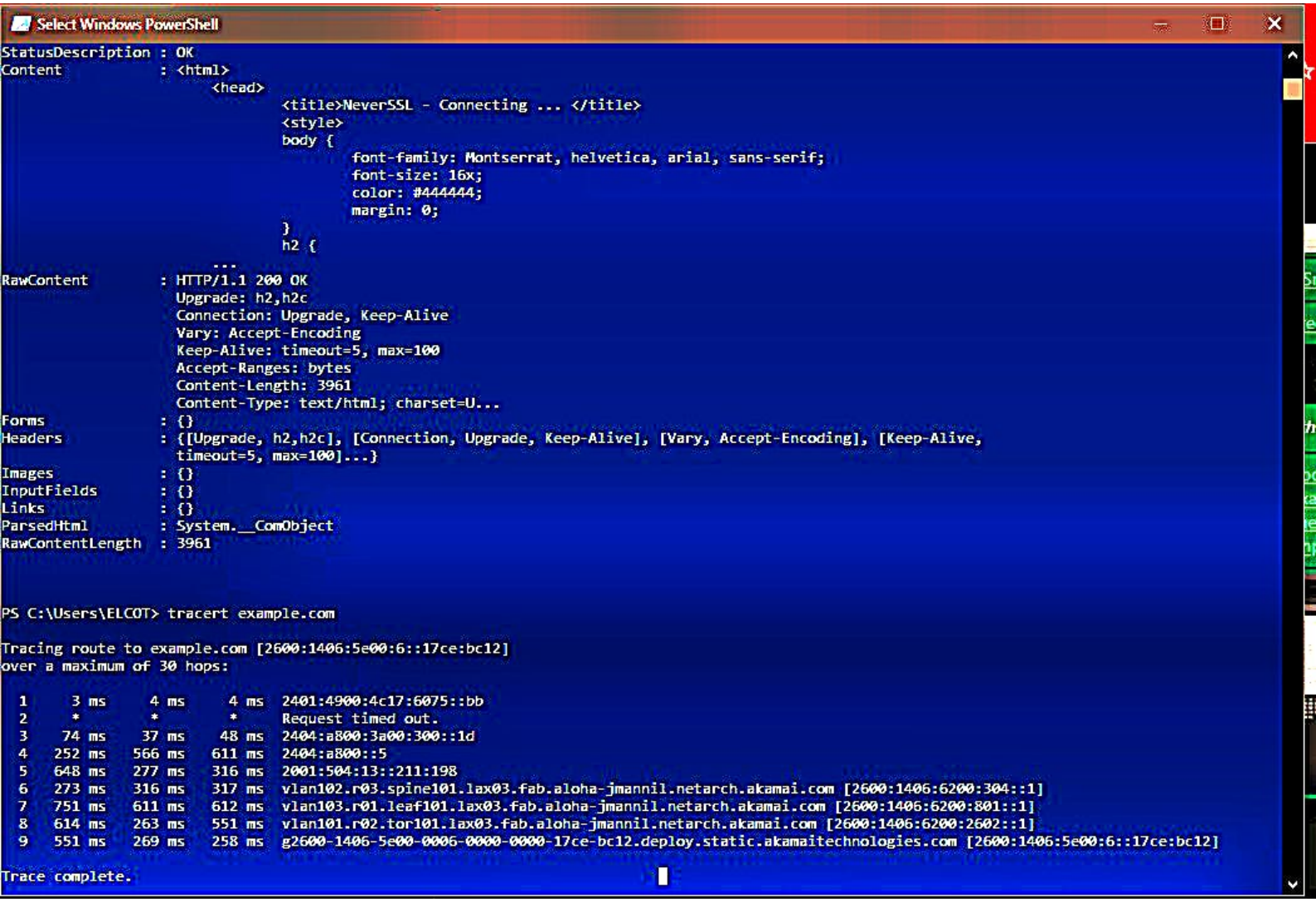
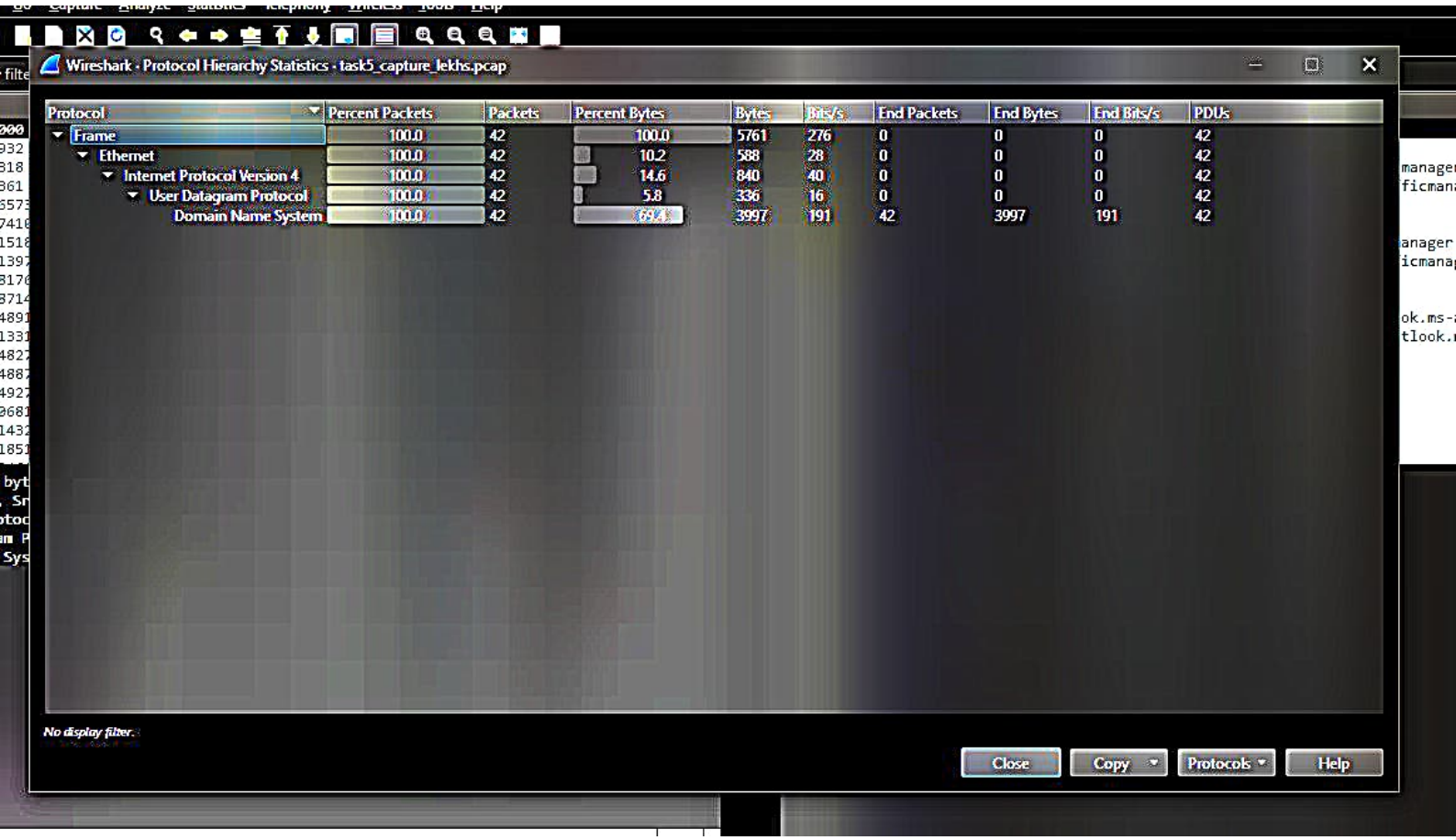
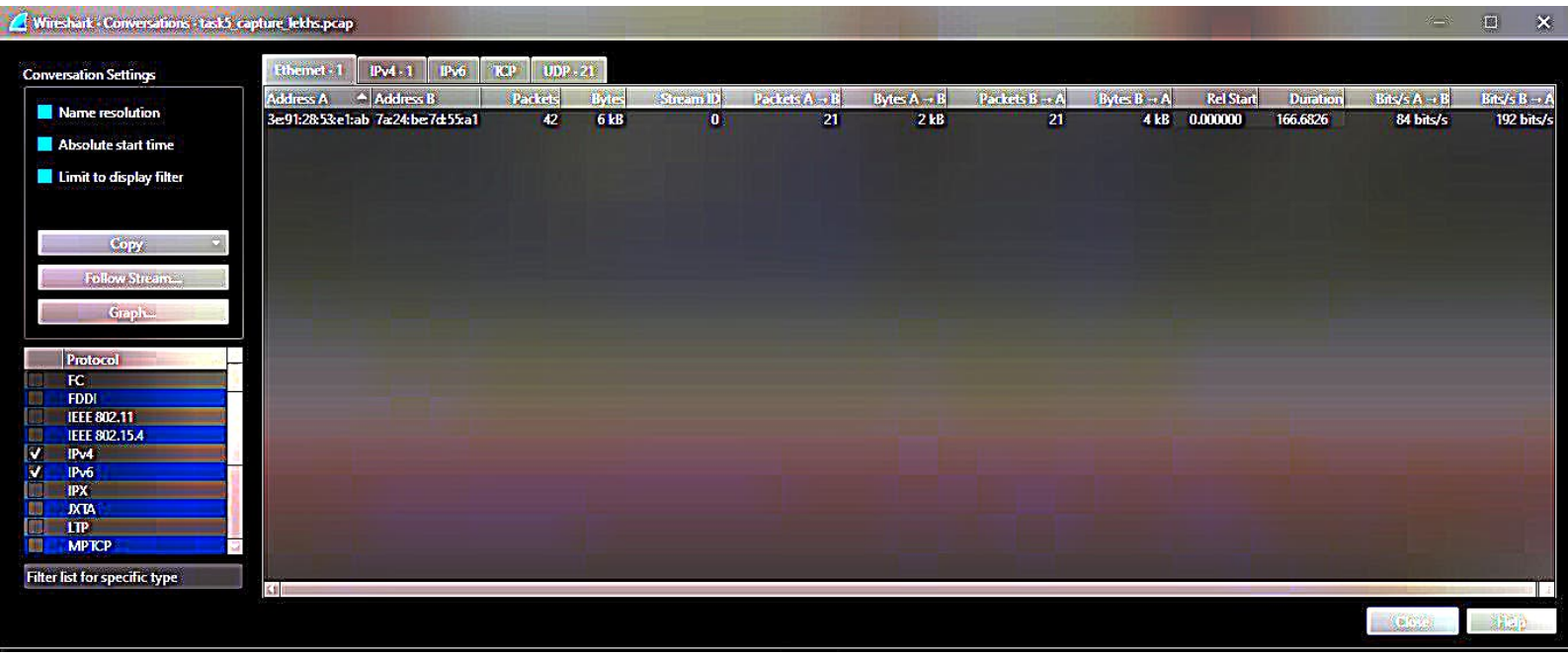
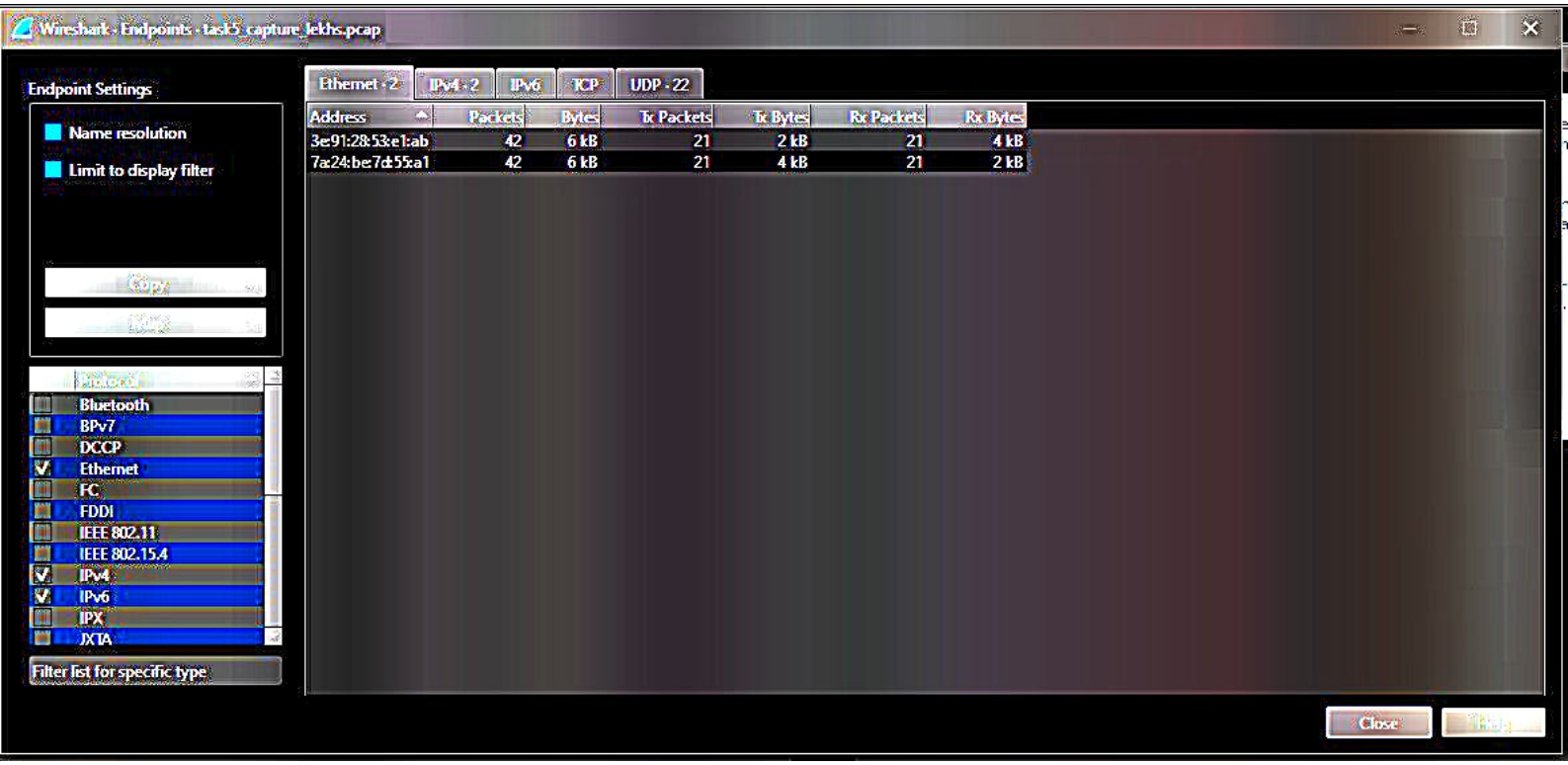

task5_capture_lekhs.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 10.243.194.214 10.243.194.27 DNS 71 Standard query 0x9203 A api.msn.com
2 0.000932 10.243.194.214 10.243.194.27 DNS 71 Standard query 0x19b6 AAAA api.msn.com
3 0.070318 10.243.194.27 10.243.194.214 DNS 230 Standard query response 0x9203 A api.msn.com CNAME api-msn-com-oneservice-world-default.trafficmanager.net
4 0.080361 10.243.194.27 10.243.194.214 DNS 254 Standard query response 0x19b6 AAAA api.msn.com CNAME api-msn-com-oneservice-world-default.trafficmanager.
5 29.466573 10.243.194.214 10.243.194.27 DNS 74 Standard query 0x7a1f A assets.msn.com
6 29.467410 10.243.194.214 10.243.194.27 DNS 74 Standard query 0xc0b8 AAAA assets.msn.com
7 29.541518 10.243.194.27 10.243.194.214 DNS 278 Standard query response 0x7a1f A assets.msn.com CNAME assets-msn-com-world-atm-default.trafficmanager.net
8 29.551397 10.243.194.27 10.243.194.214 DNS 298 Standard query response 0xc0b8 AAAA assets.msn.com CNAME assets-msn-com-world-atm-default.trafficmanager.n
9 83.298176 10.243.194.214 10.243.194.27 DNS 81 Standard query 0x9e70 A outlook.office365.com
10 83.298714 10.243.194.214 10.243.194.27 DNS 81 Standard query 0x093f AAAA outlook.office365.com
11 83.354891 10.243.194.27 10.243.194.214 DNS 230 Standard query response 0x9e70 A outlook.office365.com CNAME ooc-g2.tm-4.office.com CNAME outlook.ms-acdc.
12 83.361331 10.243.194.27 10.243.194.214 DNS 278 Standard query response 0x093f AAAA outlook.office365.com CNAME ooc-g2.tm-4.office.com CNAME outlook.ms-ac
13 147.048270 10.243.194.214 10.243.194.27 DNS 87 Standard query 0x68e9 AAAA safebrowsing.googleapis.com
14 147.048872 10.243.194.214 10.243.194.27 DNS 87 Standard query 0x28ac A safebrowsing.googleapis.com
15 147.049278 10.243.194.214 10.243.194.27 DNS 87 Standard query 0x2560 HTTPS safebrowsing.googleapis.com
16 147.106815 10.243.194.27 10.243.194.214 DNS 103 Standard query response 0x28ac A safebrowsing.googleapis.com A 142.251.220.106
17 147.114324 10.243.194.27 10.243.194.214 DNS 144 Standard query response 0x2560 HTTPS safebrowsing.googleapis.com SOA ns1.google.com
18 147.118512 10.243.194.27 10.243.194.214 DNS 115 Standard query response 0x68e9 AAAA safebrowsing.googleapis.com AAAA 2404:6800:4007:82f::200a
Frame 1: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)
Ethernet II, Src: 3e:91:28:53:e1:ab (3e:91:28:53:e1:ab), Dst: 7a:24:be:7d:55:a1 (7a:24:be:7d:5
Internet Protocol Version 4, Src: 10.243.194.214, Dst: 10.243.194.27
User Datagram Protocol, Src Port: 60979, Dst Port: 53
Domain Name System (query)
0000 7a 24 be 7d 55 a1 3e 91 28 53 e1 ab 08 00 45 00
0010 00 39 b4 28 00 00 80 11 eb b3 0a f3 c2 d6 0a f3
0020 c2 1b ee 33 00 35 00 25 83 e8 92 03 01 00 00 01
0030 00 00 00 00 00 00 03 61 70 69 03 6d 73 6e 03 63
0040 6f 6d 00 00 01 00 01
task5_capture_lekhs.pcap
Packets: 42 · Dropped: 0 (0.0%)


No. Time Source Destination Protocol Length Info
15 147.049278 10.243.194.214 10.243.194.27 DNS 87 Standard query 0x2560 HTTPS safebrowsing.googleapis.com
16 147.106815 10.243.194.27 10.243.194.214 DNS 103 Standard query response 0x28ac A safebrowsing.googleapis.com A 142.251.220.106
17 147.114324 10.243.194.27 10.243.194.214 DNS 144 Standard query response 0x2560 HTTPS safebrowsing.googleapis.com SOA ns1.google.com
18 147.118512 10.243.194.27 10.243.194.214 DNS 115 Standard query response 0x68e9 AAAA safebrowsing.googleapis.com AAAA 2404:6800:4007:82f::200a
19 162.194669 10.243.194.214 10.243.194.27 DNS 74 Standard query 0x6832 AAAA www.google.com
20 162.195309 10.243.194.214 10.243.194.27 DNS 74 Standard query 0x679c A www.google.com
21 162.195766 10.243.194.214 10.243.194.27 DNS 74 Standard query 0xce8e HTTPS www.google.com
22 162.258487 10.243.194.27 10.243.194.214 DNS 102 Standard query response 0x6832 AAAA www.google.com AAAA 2404:6800:4007:83e::2004
23 162.268459 10.243.194.27 10.243.194.214 DNS 99 Standard query response 0xce8e HTTPS www.google.com HTTPS
24 162.268787 10.243.194.27 10.243.194.214 DNS 90 Standard query response 0x679c A www.google.com A 172.217.24.164
25 166.443806 10.243.194.214 10.243.194.27 DNS 96 Standard query 0x4350 AAAA freshclearsilvermorning.neverssl.com
26 166.444247 10.243.194.214 10.243.194.27 DNS 96 Standard query 0x3ff1 A freshclearsilvermorning.neverssl.com
27 166.444574 10.243.194.214 10.243.194.27 DNS 96 Standard query 0xf8c7 HTTPS freshclearsilvermorning.neverssl.com
28 166.445772 10.243.194.214 10.243.194.27 DNS 96 Standard query 0x5aae AAAA freshclearsilvermorning.neverssl.com
29 166.446396 10.243.194.214 10.243.194.27 DNS 96 Standard query 0x4b22 A freshclearsilvermorning.neverssl.com
30 166.446751 10.243.194.214 10.243.194.27 DNS 96 Standard query 0xaf2f HTTPS freshclearsilvermorning.neverssl.com
31 166.452882 10.243.194.214 10.243.194.27 DNS 83 Standard query 0xd880 AAAA safebrowsing.google.com
32 166.453356 10.243.194.214 10.243.194.27 DNS 83 Standard query 0x4e43 A safebrowsing.google.com
Frame 20: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: 3e:91:28:53:e1:ab (3e:91:28:53:e1:ab), Dst: 7a:24:be:7d:55:a1 (7a:24:be:7d:5
Internet Protocol Version 4, Src: 10.243.194.214, Dst: 10.243.194.27
User Datagram Protocol, Src Port: 59868, Dst Port: 53
Domain Name System (query)
0000 7a 24 be 7d 55 a1 3e 91 28 53 e1 ab 08 00 45 00 z$·}U·>· (S····E·
0010 00 3c b4 32 00 00 80 11 eb a6 0a f3 c2 d6 0a f3 ·<·2···· ········
0020 c2 1b e9 dc 00 35 00 28 84 70 67 9c 01 00 00 01 ·····5·(·pg·····
0030 00 00 00 00 00 00 03 77 77 77 06 67 6f 6f 67 6c ·······w ww·googl
0040 65 03 63 6f 6d 00 00 01 00 01 e·com··· ··


Select Windows PowerShell
StatusDescription : OK
Content : <html>
<head>
<title>NeverSSL - Connecting ... </title>
<style>
body {
font-family: Montserrat, helvetica, arial, sans-serif;
font-size: 16x;
color: #444444;
margin: 0;
}
h2 {
...
RawContent : HTTP/1.1 200 OK
Upgrade: h2,h2c
Connection: Upgrade, Keep-Alive
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Accept-Ranges: bytes
Content-Length: 3961
Content-Type: text/html; charset=U...
Forms : {}
Headers : {[Upgrade, h2,h2c], [Connection, Upgrade, Keep-Alive], [Vary, Accept-Encoding], [Keep-Alive,
timeout=5, max=100]...}
Images : {}
InputFields : {}
Links : {}
ParsedHtml : System.__ComObject
RawContentLength : 3961
PS C:\Users\ELCOT> tracert example.com
Tracing route to example.com [2600:1406:5e00:6::17ce:bc12]
over a maximum of 30 hops:
1 3 ms 4 ms 4 ms 2401:4900:4c17:6075::bb
2 * * * Request timed out.
3 74 ms 37 ms 48 ms 2404:a800:3a00:300::1d
4 252 ms 566 ms 611 ms 2404:a800::5
5 648 ms 277 ms 316 ms 2001:504:13::211:198
6 273 ms 316 ms 317 ms vlan102.r03.spine101.lax03.fab.aloha-jmannil.netarch.akamai.com [2600:1406:6200:304::1]
7 751 ms 611 ms 612 ms vlan103.r01.leaf101.lax03.fab.aloha-jmannil.netarch.akamai.com [2600:1406:6200:801::1]
8 614 ms 263 ms 551 ms vlan101.r02.tor101.lax03.fab.aloha-jmannil.netarch.akamai.com [2600:1406:6200:2602::1]
9 551 ms 269 ms 258 ms g2600-1406-5e00-0006-0000-0000-17ce-bc12.deploy.static.akamaitechnologies.com [2600:1406:5e00:6::17ce:bc12]
Trace complete.


Wireshark · Protocol Hierarchy Statistics · task5_capture_lekhs.pcap
Protocol
Percent Packets
Packets
Percent Bytes
Bytes
Bits/s
End Packets
End Bytes
End Bits/s
PDUs
Frame 100.0 42 100.0 5761 276 0 0 0 42
Ethernet 100.0 42 10.2 588 28 0 0 0 42
Internet Protocol Version 4 100.0 42 14.6 840 40 0 0 0 42
User Datagram Protocol 100.0 42 5.8 336 16 0 0 0 42
Domain Name System 100.0 42 69.4 3997 191 42 3997 191 42
No display filter.
Close
Copy
Protocols
Help


Wireshark · Conversations · task3_capture_lekhs.pcap
Conversation Settings
Name resolution
Absolute start time
Limit to display filter
Copy
Follow Stream...
Graph...
Protocol
FC
FDDI
IEEE 802.11
IEEE 802.15.4
IPv4
IPv6
IPX
JXTA
LTP
MPTCP
Filter list for specific type
Ethernet · 1
IPv4 · 1
IPv6
TCP
UDP · 21
Address A
Address B
Packets
Bytes
Stream ID
Packets A → B
Bytes A → B
Packets B → A
Bytes B → A
Rel Start
Duration
Bits/s A → B
Bits/s B → A
3e91:28:53e1:ab
7a24:be7d:55a1
42
6 kB
0
21
2 kB
21
4 kB
0.000000
166.6826
84 bits/s
192 bits/s


Wireshark · Endpoints · task5_capture_lekhs.pcap
Endpoint Settings
Name resolution
Limit to display filter
Bluetooth
BPv7
DCCP
Ethernet
FC
FDDI
IEEE 802.11
IEEE 802.15.4
IPv4
IPv6
IPX
JXTA
Filter list for specific type
Ethernet · 2
IPv4 · 2
IPv6
TCP
UDP · 22
Address
Packets
Bytes
Tx Packets
Tx Bytes
Rx Packets
Rx Bytes
3e:91:28:53:e1:ab
42
6 kB
21
2 kB
21
4 kB
7a:24:be:7d:55:a1
42
6 kB
21
4 kB
21
2 kB
Close