Network Traffic Monitoring

Exercise 1: Capturing Network Traffic using Wireshark

Wireshark is a network packet analyzer that is used to capture network packets and display packet data in detail.

Lab Scenario

The traffic flowing through a network contains various kinds of data. Understanding the packets of data flowing through the network using command line applications is a tedious task, and it is difficult to sort out the required traffic from the live traffic that flows through the network. Hence, it is necessary to have an application with a graphical user interface that can capture the entire traffic in a network and help filter the traffic. As a network defender, you should have Wireshark installed to monitor and capture network traffic.

Lab Objectives

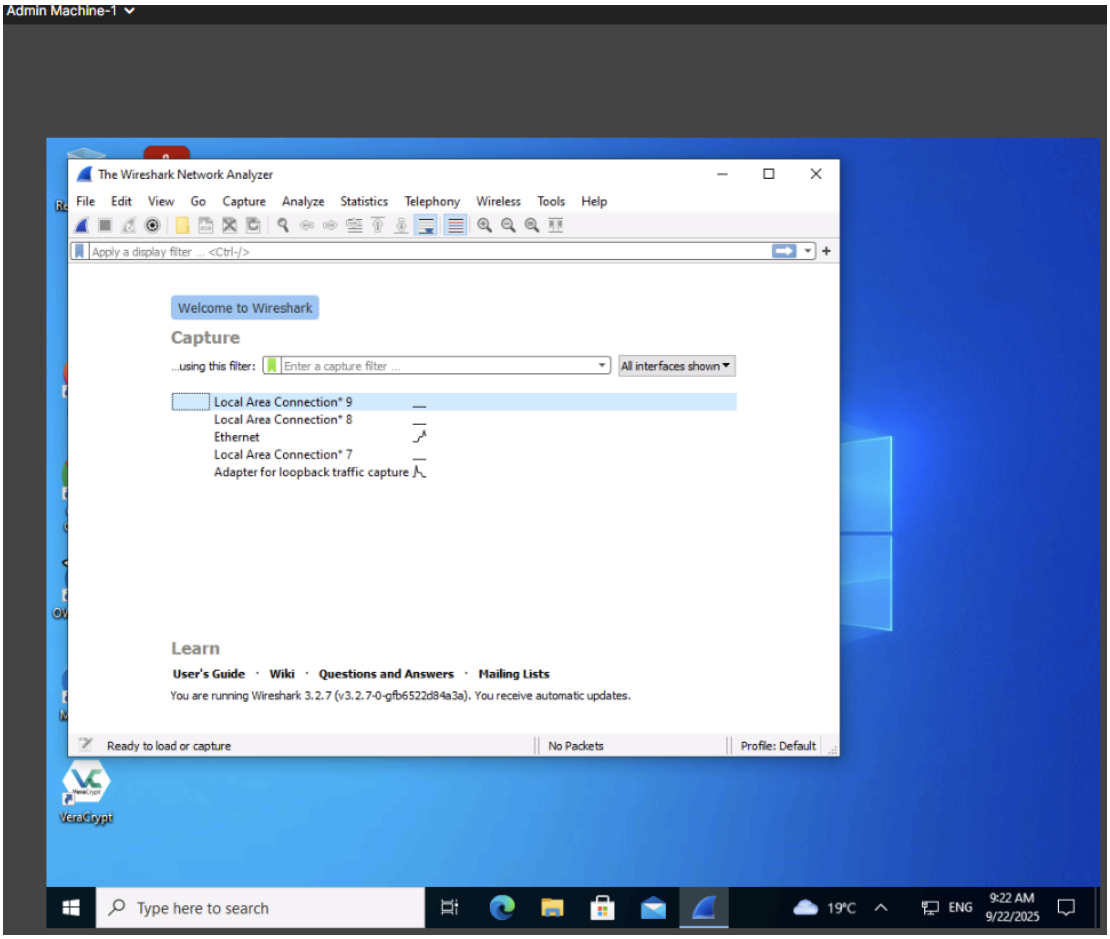
This lab will demonstrate how to capture network traffic.

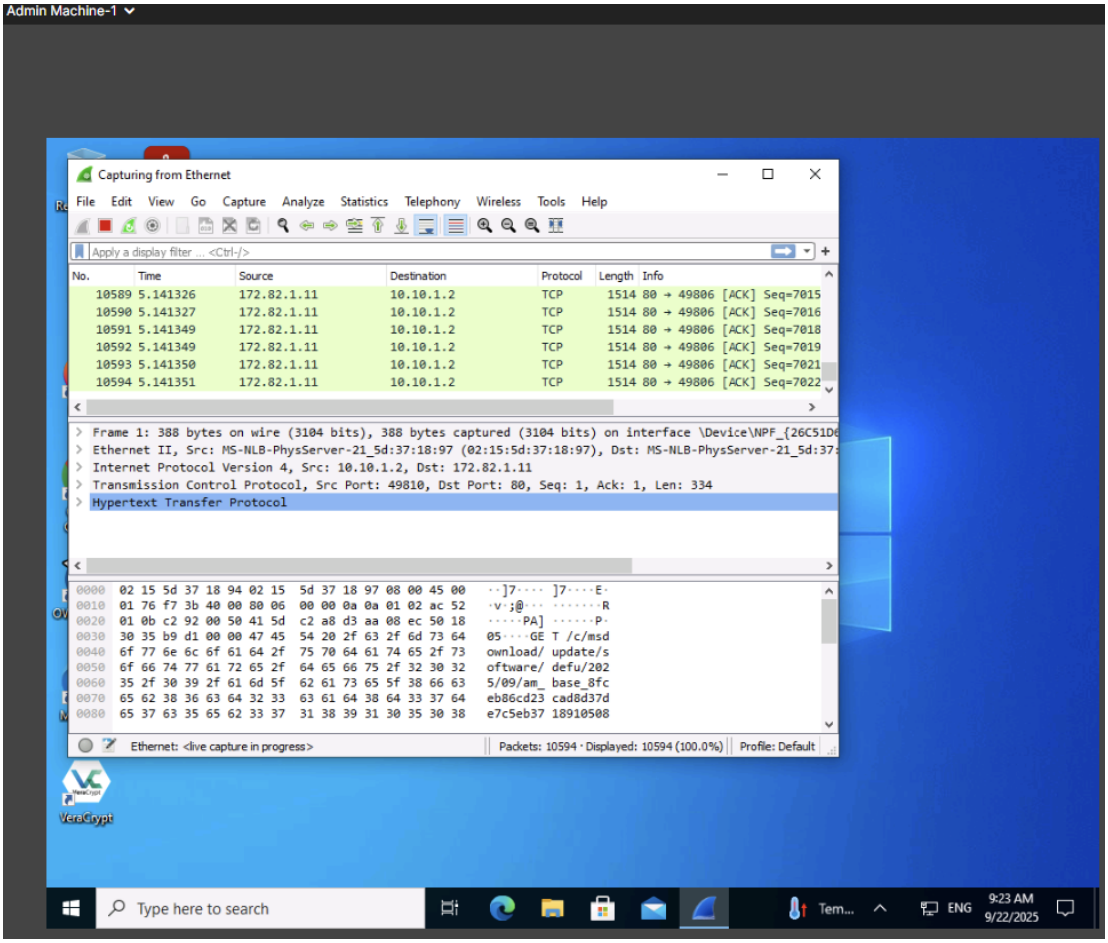
Lab Environment

Overview of Packet Capture

Packet capture refers to intercepting data packets traversing over a network using packet capture tools such as Wireshark. These captured packets are analyzed in order to determine whether appropriate network security policies are being followed.

Security Onion: Security Onion is a free open-source Linux distribution used for functions such as network monitoring, log analysis, and intrusion detection. Security Onion includes various inbuilt tools for network monitoring and detection such as Wireshark.


Admin Machine-1
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
Local Area Connection* 9
Local Area Connection* 8
Ethernet
Local Area Connection* 7
Adapter for loopback traffic capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.2.7 (v3.2.7-0-gfb6522d84a3a). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default
VeraCrypt
Type here to search
19°C
ENG
9:22 AM
9/22/2025



Exercise 2: Applying Various Filters in Wireshark

Wireshark provides numerous filters that can be applied to obtain only the required packets.

Lab Scenario

Wireshark filters traffic flowing through the entire network. This traffic contains various kinds of data packets associated with various protocols flowing between the source and destination. Therefore, searching for a specific packet, port, or an IP address manually is extremely difficult. In such cases, applying Wireshark filters helps a network defender track down a huge amount of traffic and discover the intended packets. As a network defender, it is essential to have a good knowledge of various Wireshark filters that help you narrow down the traffic and obtain the desired result.

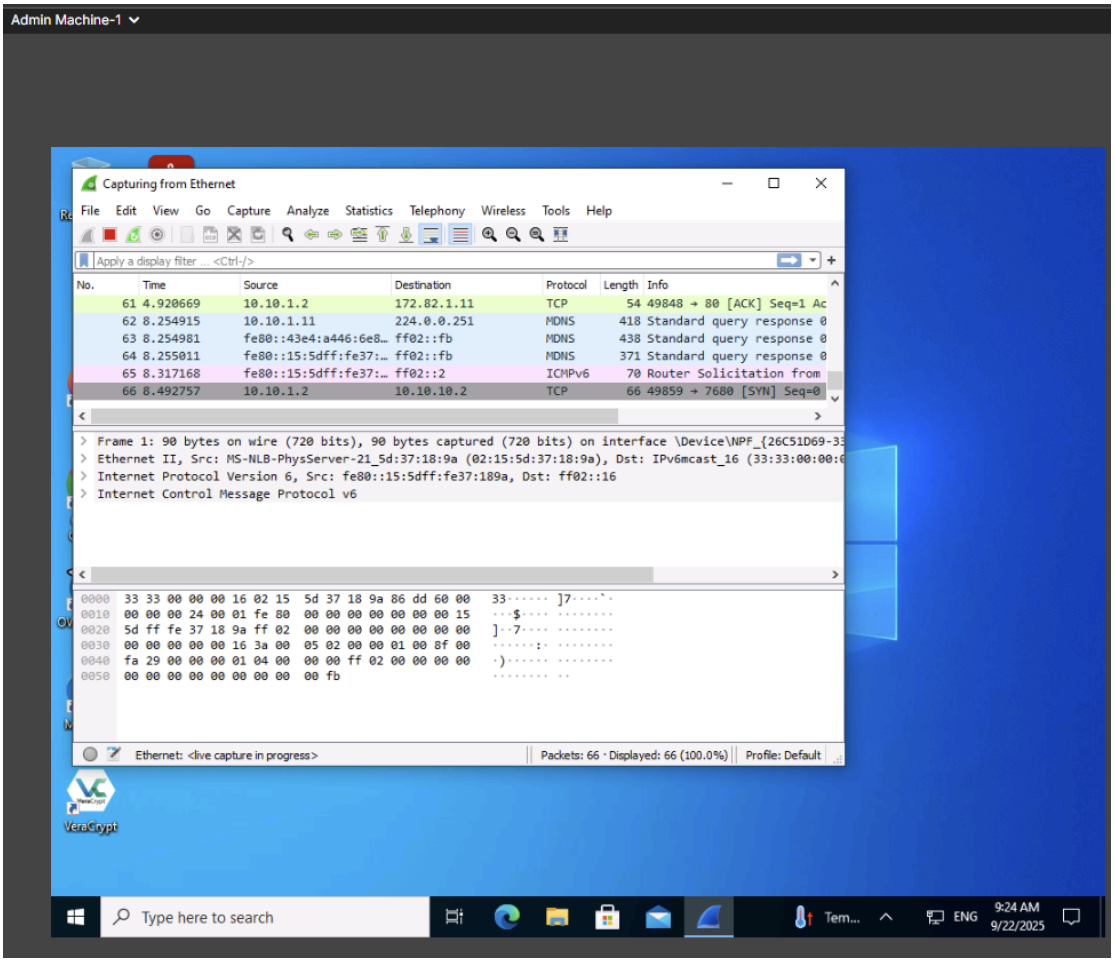
Lab Objectives

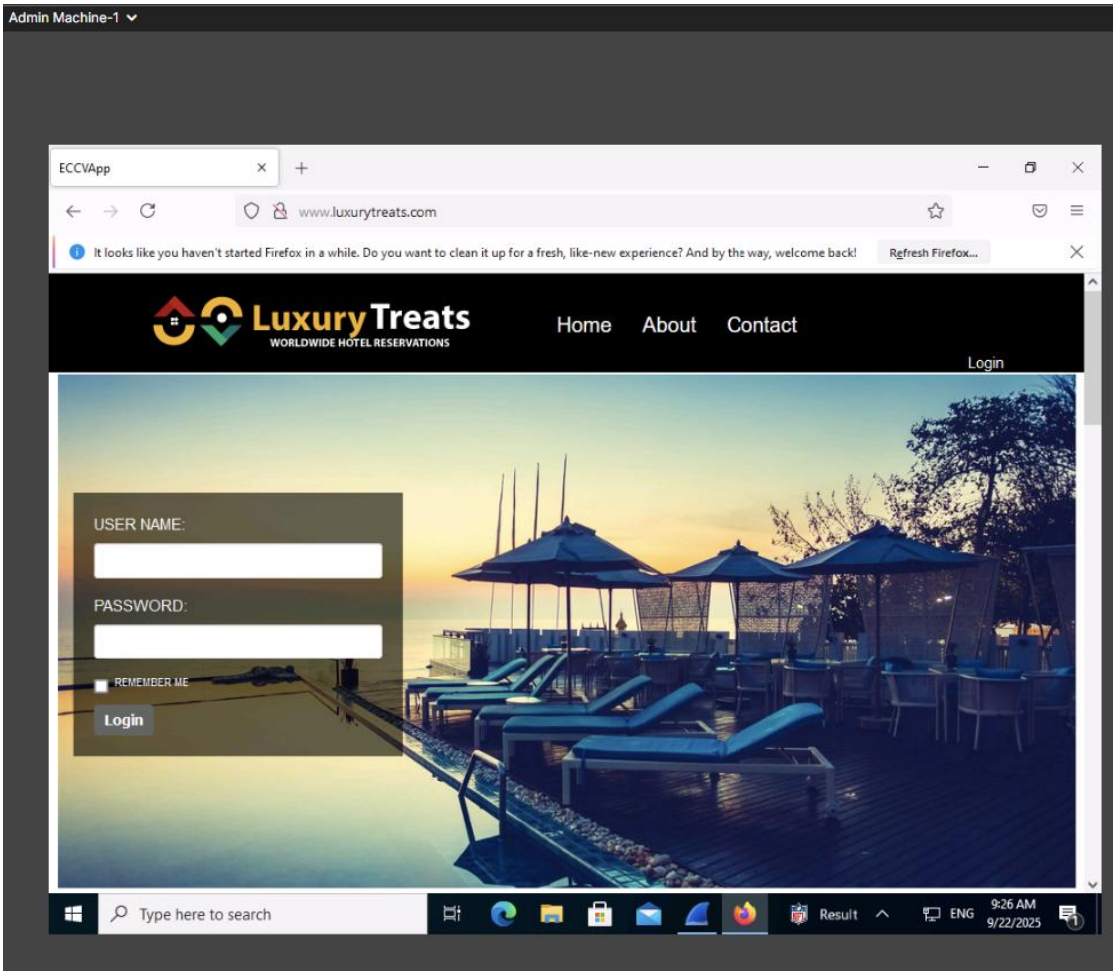
This lab will help you become familiar with various Wireshark filters

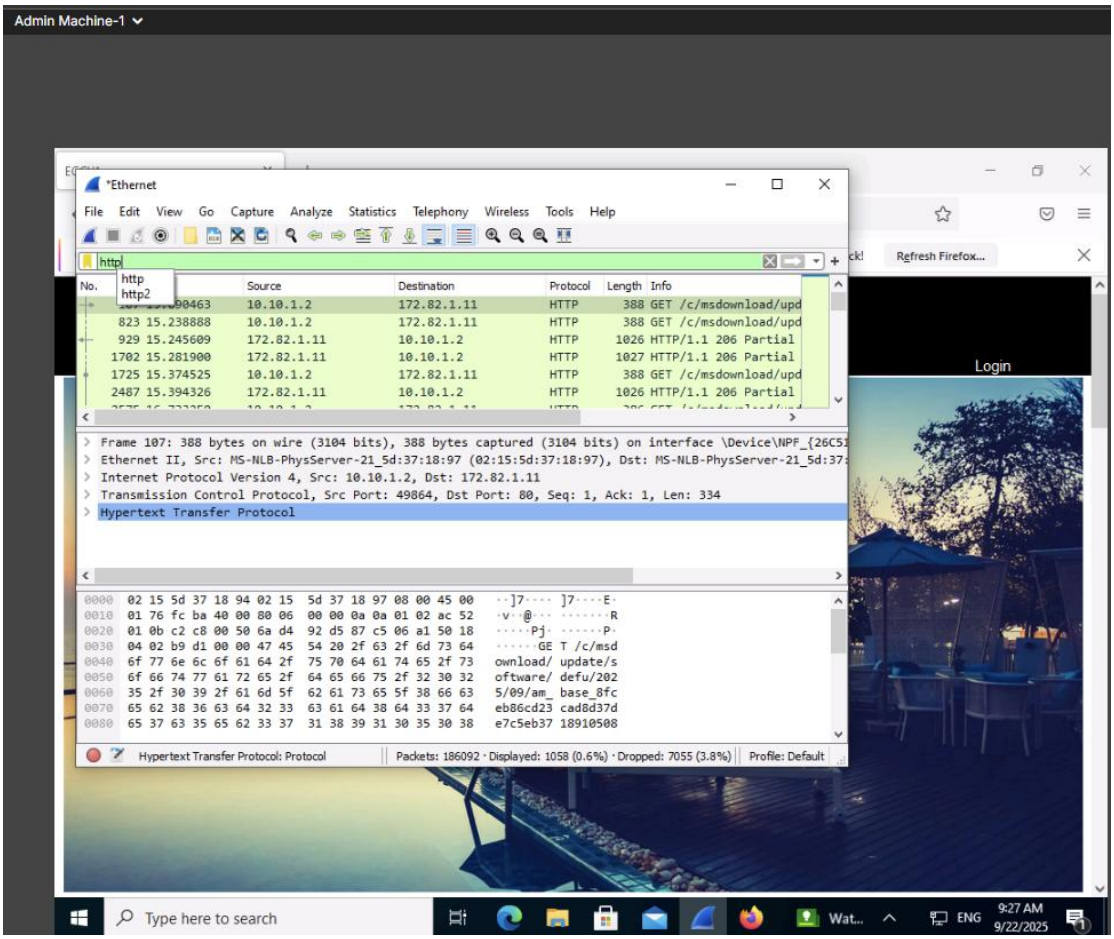
Overview of Wireshark

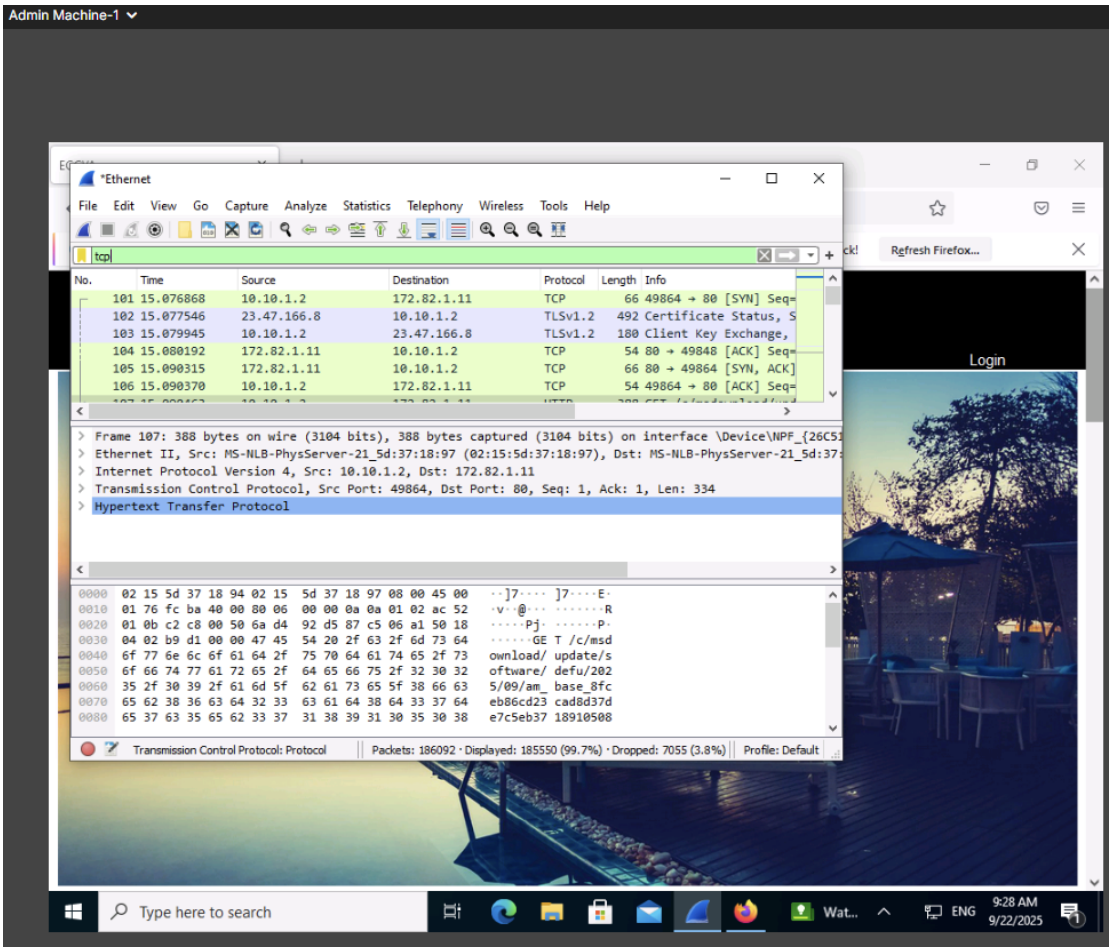
Wireshark has various filters that help you filter packets containing the following:

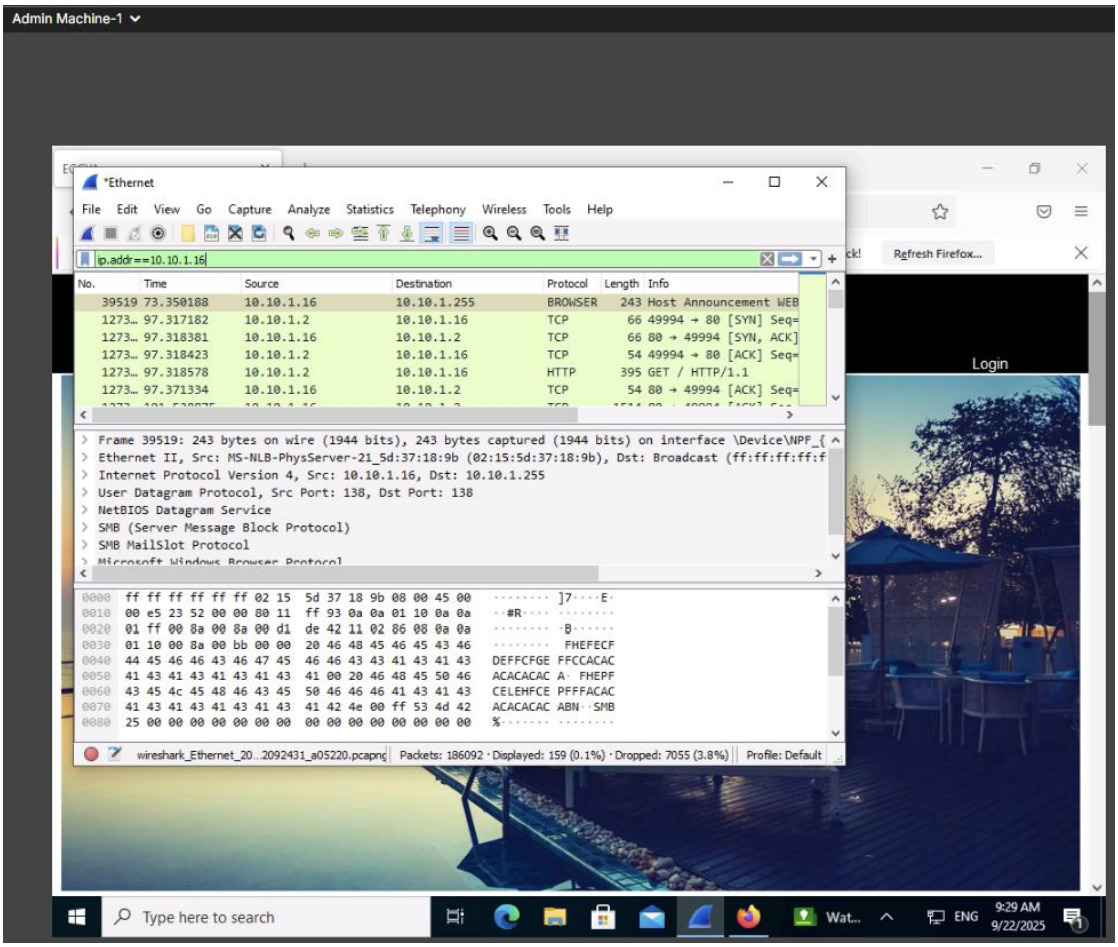
- Source IP address
- Destination IP address
- Internet Control Message Protocol (ICMP) traffic etc.

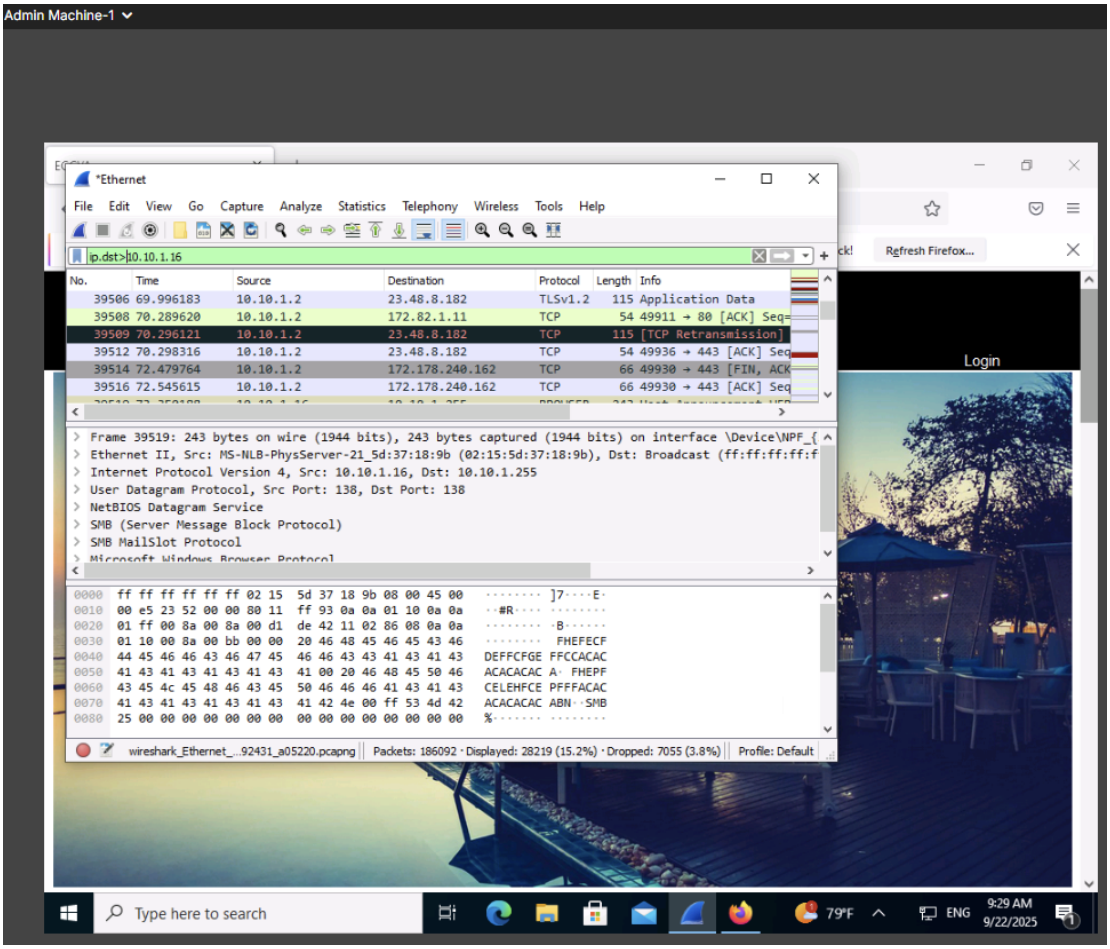


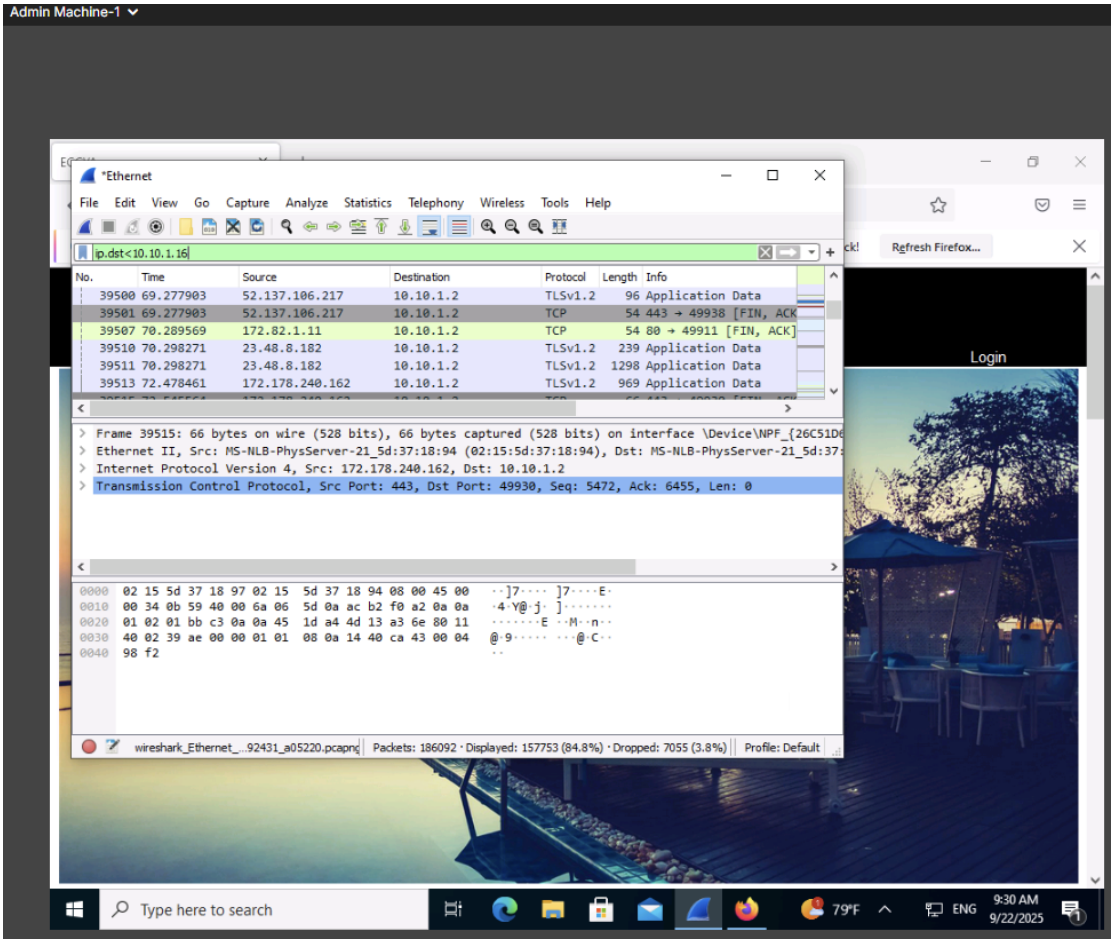

Admin Machine-1
ECCVApp
www.luxurytreats.com
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
Luxury Treats
WORLDWIDE HOTEL RESERVATIONS
Home
About
Contact
Login
USER NAME:
PASSWORD:
REMEMBER ME
Login
Type here to search
Result
ENG
9:26 AM
9/22/2025

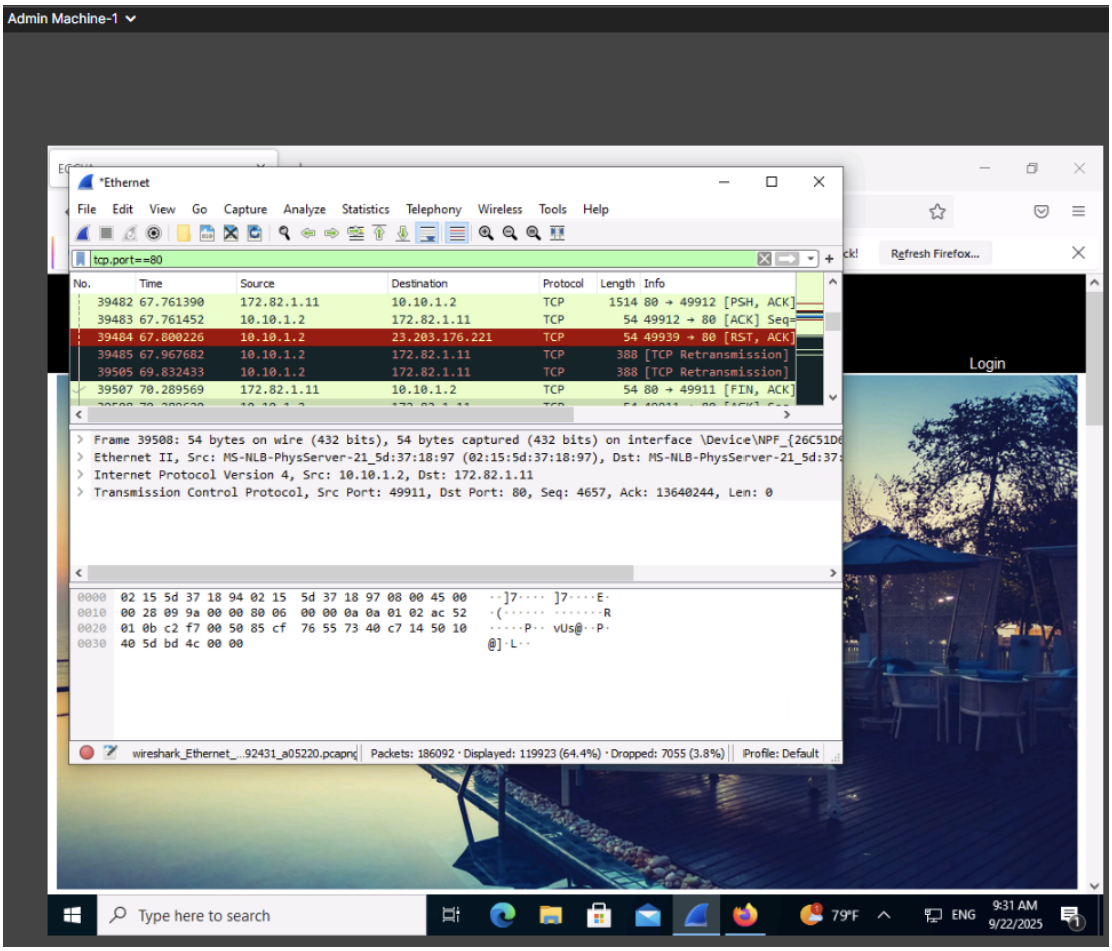

Admin Machine-1
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
http2
No. Source Destination Protocol Length Info
823 15.238888 10.10.1.2 172.82.1.11 HTTP 388 GET /c/msdownload/upd
929 15.245609 172.82.1.11 10.10.1.2 HTTP 1026 HTTP/1.1 206 Partial
1702 15.281900 172.82.1.11 10.10.1.2 HTTP 1027 HTTP/1.1 206 Partial
1725 15.374525 10.10.1.2 172.82.1.11 HTTP 388 GET /c/msdownload/upd
2487 15.394326 172.82.1.11 10.10.1.2 HTTP 1026 HTTP/1.1 206 Partial
Frame 107: 388 bytes on wire (3104 bits), 388 bytes captured (3104 bits) on interface \Device\NPF_{26C51
Ethernet II, Src: MS-NLB-PhysServer-21_5d:37:18:97 (02:15:5d:37:18:97), Dst: MS-NLB-PhysServer-21_5d:37:
Internet Protocol Version 4, Src: 10.10.1.2, Dst: 172.82.1.11
Transmission Control Protocol, Src Port: 49864, Dst Port: 80, Seq: 1, Ack: 1, Len: 334
Hypertext Transfer Protocol
0000 02 15 5d 37 18 94 02 15 5d 37 18 97 08 00 45 00 ··]7····]7····E·
0010 01 76 fc ba 40 00 80 06 00 00 0a 0a 01 02 ac 52 ·v··@··· ·······R
0020 01 0b c2 c8 00 50 6a d4 92 d5 87 c5 06 a1 50 18 ·····Pj· ·····P·
0030 04 02 b9 d1 00 00 47 45 54 20 2f 63 2f 6d 73 64 ·····GE T /c/msd
0040 6f 77 6e 6c 6f 61 64 2f 75 70 64 61 74 65 2f 73 ownload/ update/s
0050 6f 66 74 77 61 72 65 2f 64 65 66 75 2f 32 30 32 oftware/ defu/202
0060 35 2f 30 39 2f 61 6d 5f 62 61 73 65 5f 38 66 63 5/09/am_ base_8fc
0070 65 62 38 36 63 64 32 33 63 61 64 38 64 33 37 64 eb86cd23 cad8d37d
0080 65 37 63 35 65 62 33 37 31 38 39 31 30 35 30 38 e7c5eb37 18910508
Hypertext Transfer Protocol: Protocol
Packets: 186092 · Displayed: 1058 (0.6%) · Dropped: 7055 (3.8%)
Profile: Default
Refresh Firefox...
Login
Type here to search
ENG
9:27 AM
9/22/2025

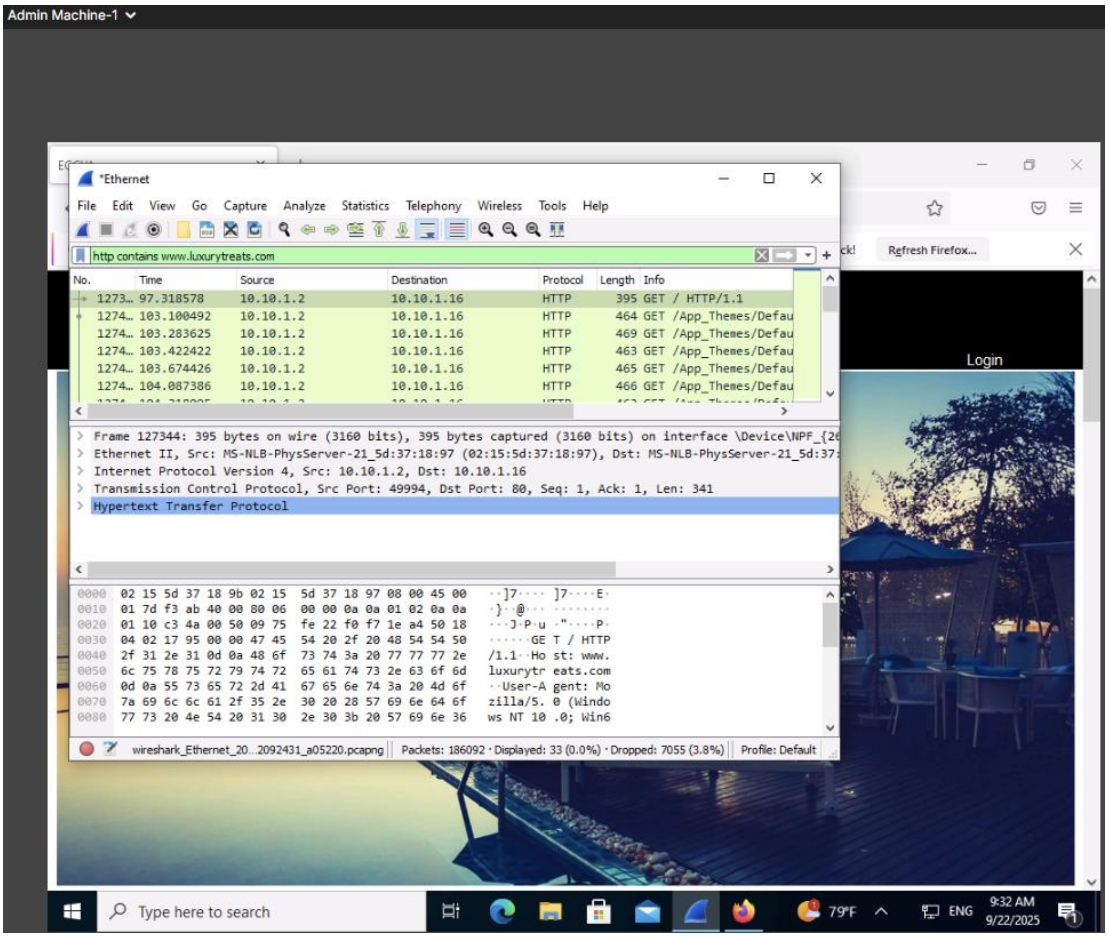

Admin Machine-1
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
101 15.076868 10.10.1.2 172.82.1.11 TCP 66 49864 → 80 [SYN] Seq=
102 15.077546 23.47.166.8 10.10.1.2 TLSv1.2 492 Certificate Status, S
103 15.079945 10.10.1.2 23.47.166.8 TLSv1.2 180 Client Key Exchange,
104 15.080192 172.82.1.11 10.10.1.2 TCP 54 80 → 49848 [ACK] Seq=
105 15.090315 172.82.1.11 10.10.1.2 TCP 66 80 → 49864 [SYN, ACK]
106 15.090370 10.10.1.2 172.82.1.11 TCP 54 49864 → 80 [ACK] Seq=
Frame 107: 388 bytes on wire (3104 bits), 388 bytes captured (3104 bits) on interface \Device\NPF_{26C51
Ethernet II, Src: MS-NLB-PhysServer-21_5d:37:18:97 (02:15:5d:37:18:97), Dst: MS-NLB-PhysServer-21_5d:37:
Internet Protocol Version 4, Src: 10.10.1.2, Dst: 172.82.1.11
Transmission Control Protocol, Src Port: 49864, Dst Port: 80, Seq: 1, Ack: 1, Len: 334
Hypertext Transfer Protocol
0000 02 15 5d 37 18 94 02 15 5d 37 18 97 08 00 45 00 ··]7····]7····E·
0010 01 76 fc ba 40 00 80 06 00 00 0a 01 02 ac 52 ·v··@··· ·····R
0020 01 0b c2 c8 00 50 6a d4 92 d5 87 c5 06 a1 50 18 ·····Pj· ·····P·
0030 04 02 b9 d1 00 00 47 45 54 20 2f 63 2f 6d 73 64 ·····GE T /c/msd
0040 6f 77 6e 6c 6f 61 64 2f 75 70 64 61 74 65 2f 73 ownload/ update/s
0050 6f 66 74 77 61 72 65 2f 64 65 66 75 2f 32 30 32 oftware/ defu/202
0060 35 2f 30 39 2f 61 6d 5f 62 61 73 65 5f 38 66 63 5/09/am_ base_8fc
0070 65 62 38 36 63 64 32 33 63 61 64 38 64 33 37 64 eb86cd23 cad8d37d
0080 65 37 63 35 65 62 33 37 31 38 39 31 30 35 30 38 e7c5eb37 18910508
Transmission Control Protocol: Protocol
Packets: 186092 · Displayed: 185550 (99.7%) · Dropped: 7055 (3.8%)
Profile: Default
Refresh Firefox...
Login
Type here to search
Wat...
ENG
9:28 AM
9/22/2025

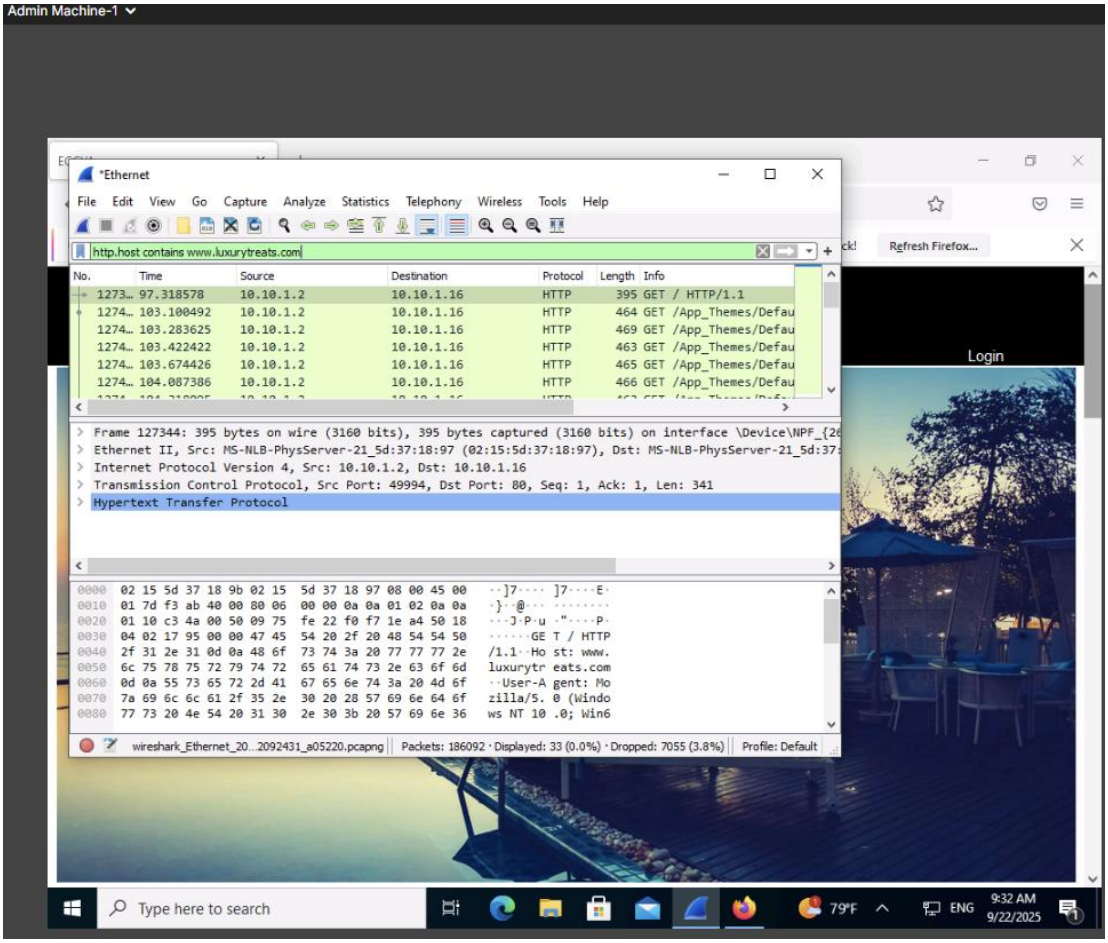

Admin Machine-1
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr==10.10.1.16
No. Time Source Destination Protocol Length Info
39519 73.350188 10.10.1.16 10.10.1.255 BROWSER 243 Host Announcement WEB
1273… 97.317182 10.10.1.2 10.10.1.16 TCP 66 49994 → 80 [SYN] Seq=
1273… 97.318381 10.10.1.16 10.10.1.2 TCP 66 80 → 49994 [SYN, ACK]
1273… 97.318423 10.10.1.2 10.10.1.16 TCP 54 49994 → 80 [ACK] Seq=
1273… 97.318578 10.10.1.2 10.10.1.16 HTTP 395 GET / HTTP/1.1
1273… 97.371334 10.10.1.16 10.10.1.2 TCP 54 80 → 49994 [ACK] Seq=
Frame 39519: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits) on interface \Device\NPF_{
Ethernet II, Src: MS-NLB-PhysServer-21_5d:37:18:9b (02:15:5d:37:18:9b), Dst: Broadcast (ff:ff:ff:ff:f
Internet Protocol Version 4, Src: 10.10.1.16, Dst: 10.10.1.255
User Datagram Protocol, Src Port: 138, Dst Port: 138
NetBIOS Datagram Service
SMB (Server Message Block Protocol)
SMB MailSlot Protocol
Microsoft Windows Browser Protocol
0000 ff ff ff ff ff ff 02 15 5d 37 18 9b 08 00 45 00
0010 00 e5 23 52 00 00 80 11 ff 93 0a 0a 01 10 0a 0a
0020 01 ff 00 8a 00 8a 00 d1 de 42 11 02 86 08 0a 0a
0030 01 10 00 8a 00 bb 00 00 20 46 48 45 46 45 43 46
0040 44 45 46 46 43 46 47 45 46 46 43 43 41 43 41 43
0050 41 43 41 43 41 43 41 43 41 00 20 46 48 45 50 46
0060 43 45 4c 45 48 46 43 45 50 46 46 46 41 43 41 43
0070 41 43 41 43 41 43 41 43 41 42 4e 00 ff 53 4d 42
0080 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
wireshark_Ethernet_20…2092431_a05220.pcapng
Packets: 186092 · Displayed: 159 (0.1%) · Dropped: 7055 (3.8%)
Profile: Default
Refresh Firefox...
Login
Type here to search
ENG
9:29 AM
9/22/2025


Admin Machine-1
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.dst>10.10.1.16
No. Time Source Destination Protocol Length Info
39506 69.996183 10.10.1.2 23.48.8.182 TLSv1.2 115 Application Data
39508 70.289620 10.10.1.2 172.82.1.11 TCP 54 49911 → 80 [ACK] Seq=
39509 70.296121 10.10.1.2 23.48.8.182 TCP 115 [TCP Retransmission]
39512 70.298316 10.10.1.2 23.48.8.182 TCP 54 49936 → 443 [ACK] Seq
39514 72.479764 10.10.1.2 172.178.240.162 TCP 66 49930 → 443 [FIN, ACK
39516 72.545615 10.10.1.2 172.178.240.162 TCP 66 49930 → 443 [ACK] Seq
Frame 39519: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits) on interface \Device\NPF_{
Ethernet II, Src: MS-NLB-PhysServer-21_5d:37:18:9b (02:15:5d:37:18:9b), Dst: Broadcast (ff:ff:ff:ff:f
Internet Protocol Version 4, Src: 10.10.1.16, Dst: 10.10.1.255
User Datagram Protocol, Src Port: 138, Dst Port: 138
NetBIOS Datagram Service
SMB (Server Message Block Protocol)
SMB MailSlot Protocol
Microsoft Windows Browser Protocol
0000 ff ff ff ff ff ff 02 15 5d 37 18 9b 08 00 45 00]7 E
0010 00 e5 23 52 00 00 80 11 ff 93 0a 0a 01 10 0a 0a #R
0020 01 ff 00 8a 00 8a 00 d1 de 42 11 02 86 08 0a 0a B
0030 01 10 00 8a 00 bb 00 00 20 46 48 45 46 45 43 46 FHEFECF
0040 44 45 46 46 43 46 47 45 46 46 43 43 41 43 41 43 DEFFCFGE FFCCACAC
0050 41 43 41 43 41 43 41 43 41 00 20 46 48 45 50 46 ACACACAC A FHEPF
0060 43 45 4c 45 48 46 43 45 50 46 46 46 41 43 41 43 CELEHFCE PFFFACAC
0070 41 43 41 43 41 43 41 43 41 42 4e 00 ff 53 4d 42 ACACACAC ABN SMB
0080 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 %
wireshark_Ethernet_..92431_a05220.pcapng
Packets: 186092 · Displayed: 28219 (15.2%) · Dropped: 7055 (3.8%)
Profile: Default
Refresh Firefox...
Login
Type here to search
79°F
ENG
9:29 AM
9/22/2025


Admin Machine-1
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.dst<10.10.1.16
No. Time Source Destination Protocol Length Info
39500 69.277903 52.137.106.217 10.10.1.2 TLSv1.2 96 Application Data
39501 69.277903 52.137.106.217 10.10.1.2 TCP 54 443 → 49938 [FIN, ACK]
39507 70.289569 172.82.1.11 10.10.1.2 TCP 54 80 → 49911 [FIN, ACK]
39510 70.298271 23.48.8.182 10.10.1.2 TLSv1.2 239 Application Data
39511 70.298271 23.48.8.182 10.10.1.2 TLSv1.2 1298 Application Data
39513 72.478461 172.178.240.162 10.10.1.2 TLSv1.2 969 Application Data
Frame 39515: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{26C51D6
Ethernet II, Src: MS-NLB-PhysServer-21_5d:37:18:94 (02:15:5d:37:18:94), Dst: MS-NLB-PhysServer-21_5d:37:
Internet Protocol Version 4, Src: 172.178.240.162, Dst: 10.10.1.2
Transmission Control Protocol, Src Port: 443, Dst Port: 49930, Seq: 5472, Ack: 6455, Len: 0
0000 02 15 5d 37 18 97 02 15 5d 37 18 94 08 00 45 00
0010 00 34 0b 59 40 00 6a 06 5d 0a ac b2 f0 a2 0a 0a
0020 01 02 01 bb c3 0a 0a 45 1d a4 4d 13 a3 6e 80 11
0030 40 02 39 ae 00 00 01 01 08 0a 14 40 ca 43 00 04
0040 98 f2
wireshark_Ethernet_...92431_a05220.pcapng
Packets: 186092 · Displayed: 157753 (84.8%) · Dropped: 7055 (3.8%)
Profile: Default
Refresh Firefox...
Login
Type here to search
79°F
ENG
9:30 AM
9/22/2025


Admin Machine-1
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port==80
No. Time Source Destination Protocol Length Info
39482 67.761390 172.82.1.11 10.10.1.2 TCP 1514 80 → 49912 [PSH, ACK]
39483 67.761452 10.10.1.2 172.82.1.11 TCP 54 49912 → 80 [ACK] Seq=
39484 67.800226 10.10.1.2 23.203.176.221 TCP 54 49939 → 80 [RST, ACK]
39485 67.967682 10.10.1.2 172.82.1.11 TCP 388 [TCP Retransmission]
39505 69.832433 10.10.1.2 172.82.1.11 TCP 388 [TCP Retransmission]
39507 70.289569 172.82.1.11 10.10.1.2 TCP 54 80 → 49911 [FIN, ACK]
Frame 39508: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{26C51D6
Ethernet II, Src: MS-NLB-PhysServer-21_5d:37:18:97 (02:15:5d:37:18:97), Dst: MS-NLB-PhysServer-21_5d:37:
Internet Protocol Version 4, Src: 10.10.1.2, Dst: 172.82.1.11
Transmission Control Protocol, Src Port: 49911, Dst Port: 80, Seq: 4657, Ack: 13640244, Len: 0
0000 02 15 5d 37 18 94 02 15 5d 37 18 97 08 00 45 00
0010 00 28 09 9a 00 00 80 06 00 00 0a 0a 01 02 ac 52
0020 01 0b c2 f7 00 50 85 cf 76 55 73 40 c7 14 50 10
0030 40 5d bd 4c 00 00
wireshark_Ethernet_..92431_a05220.pcapng
Packets: 186092 · Displayed: 119923 (64.4%) · Dropped: 7055 (3.8%)
Profile: Default
Refresh Firefox...
Login
Type here to search
79°F
ENG
9:31 AM
9/22/2025


Admin Machine-1
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http contains www.luxurytreats.com
No. Time Source Destination Protocol Length Info
1273… 97.318578 10.10.1.2 10.10.1.16 HTTP 395 GET / HTTP/1.1
1274… 103.100492 10.10.1.2 10.10.1.16 HTTP 464 GET /App_Themes/Defau
1274… 103.283625 10.10.1.2 10.10.1.16 HTTP 469 GET /App_Themes/Defau
1274… 103.422422 10.10.1.2 10.10.1.16 HTTP 463 GET /App_Themes/Defau
1274… 103.674426 10.10.1.2 10.10.1.16 HTTP 465 GET /App_Themes/Defau
1274… 104.087386 10.10.1.2 10.10.1.16 HTTP 466 GET /App_Themes/Defau
Frame 127344: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface \Device\NPF_{2
Ethernet II, Src: MS-NLB-PhysServer-21_5d:37:18:97 (02:15:5d:37:18:97), Dst: MS-NLB-PhysServer-21_5d:37:
Internet Protocol Version 4, Src: 10.10.1.2, Dst: 10.10.1.16
Transmission Control Protocol, Src Port: 49994, Dst Port: 80, Seq: 1, Ack: 1, Len: 341
Hypertext Transfer Protocol
0000 02 15 5d 37 18 9b 02 15 5d 37 18 97 08 00 45 00 ··]7····]7····E·
0010 01 7d f3 ab 40 00 80 06 00 00 0a 0a 01 02 0a 0a ·}··@··· ········
0020 01 10 c3 4a 00 50 09 75 fe 22 f0 f7 1e a4 50 18 ···J·P·u ·"····P·
0030 04 02 17 95 00 00 47 45 54 20 2f 20 48 54 54 50 ·····GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e /1.1··Ho st: www.
0050 6c 75 78 75 72 79 74 72 65 61 74 73 2e 63 6f 6d luxurytr eats.com
0060 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f ··User-A gent: Mo
0070 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f zilla/5. 0 (Windo
0080 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e 36 ws NT 10 .0; Win6
wireshark_Ethernet_20…2092431_a05220.pcapng
Packets: 186092 · Displayed: 33 (0.0%) · Dropped: 7055 (3.8%)
Profile: Default
Refresh Firefox...
Login
Type here to search
79°F
ENG
9:32 AM
9/22/2025



Exercise 3: Analyzing and Examining Various Network Packet Headers in Linux using tcpdump

We shall analyze TCP/IP and other packets on Linux host machine using tcpdump.

Lab Scenario

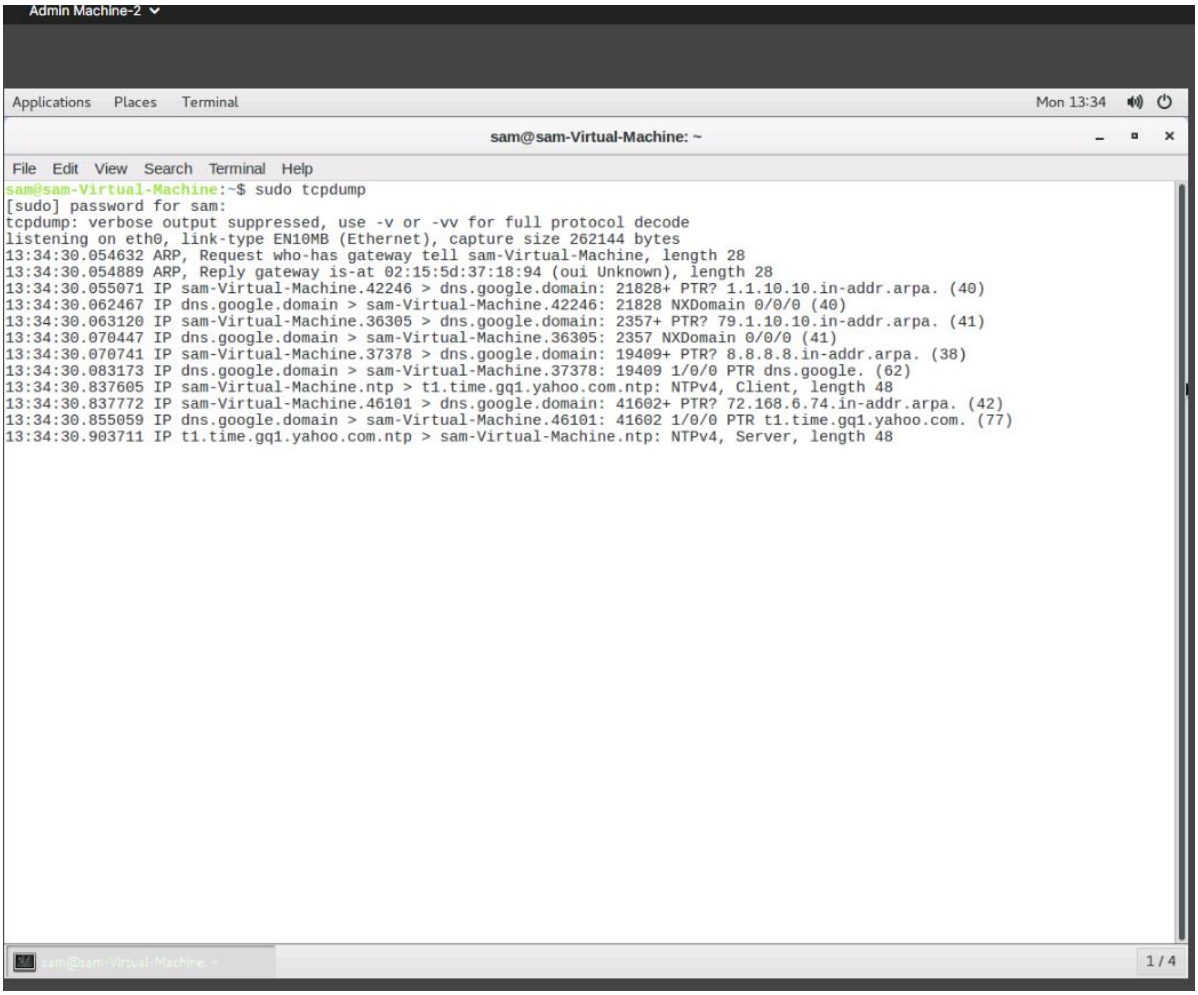
Each packet in a network contains control information and user data, known as the payload. The control information contains data for delivering the payload, which includes, for example, source and destination IP and MAC addresses and sequencing information. The header part of the packet stores this control information. Hence, the network administrator needs to know how to examine the packet headers while examining the data packets.

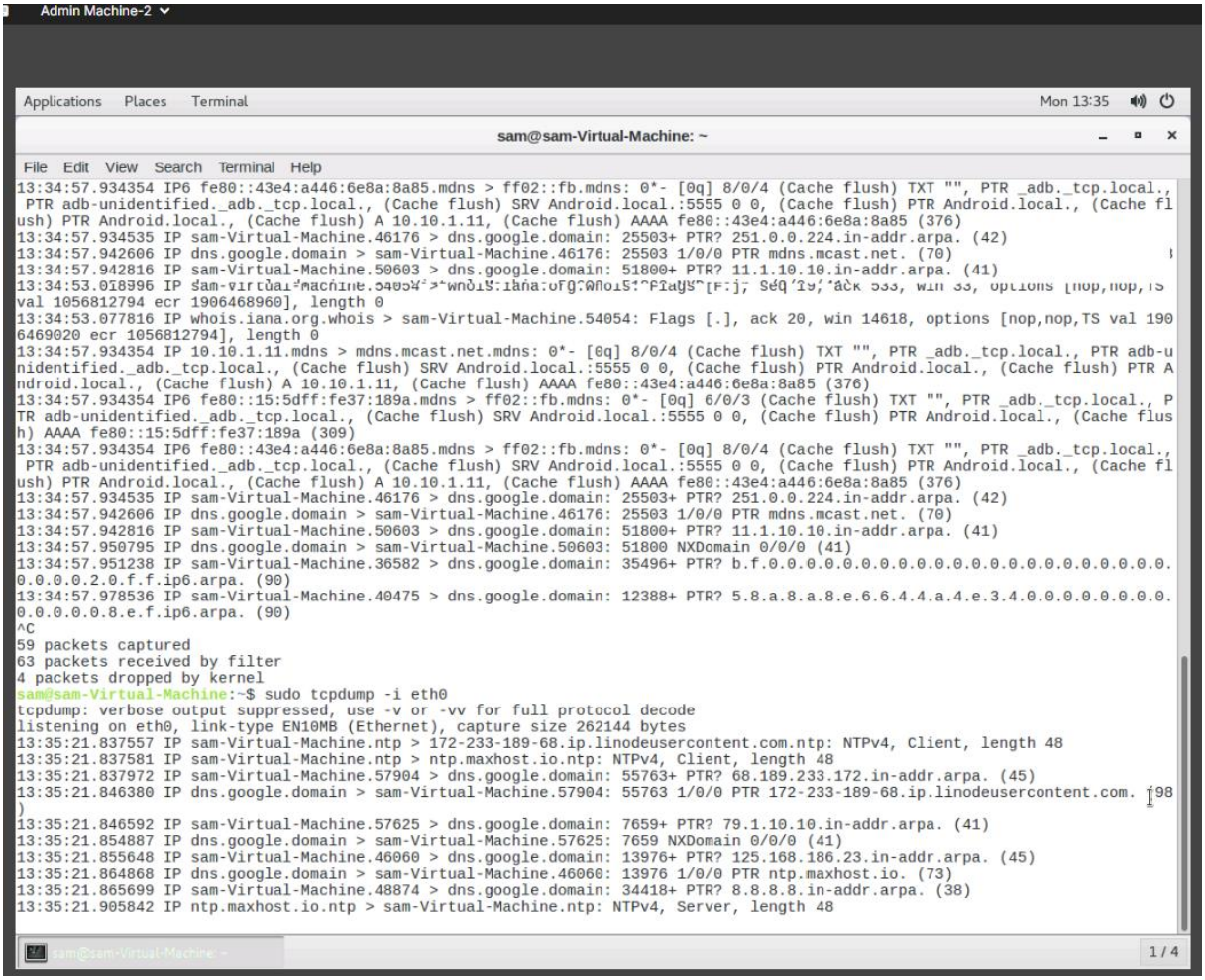
Lab Objectives

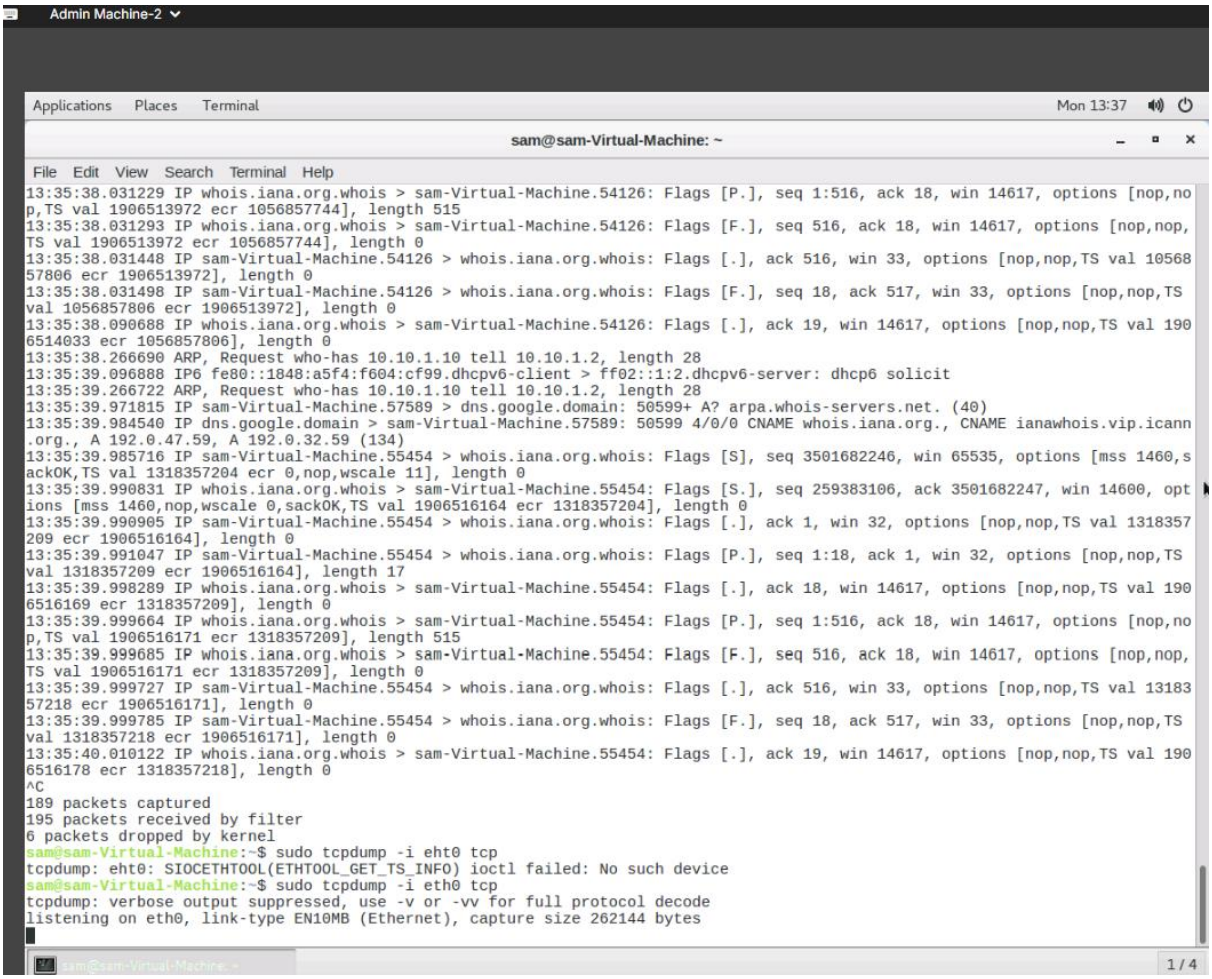
The objective of this lab is to help students learn how to inspect TCP/IP and other packet header fields of different network packets.

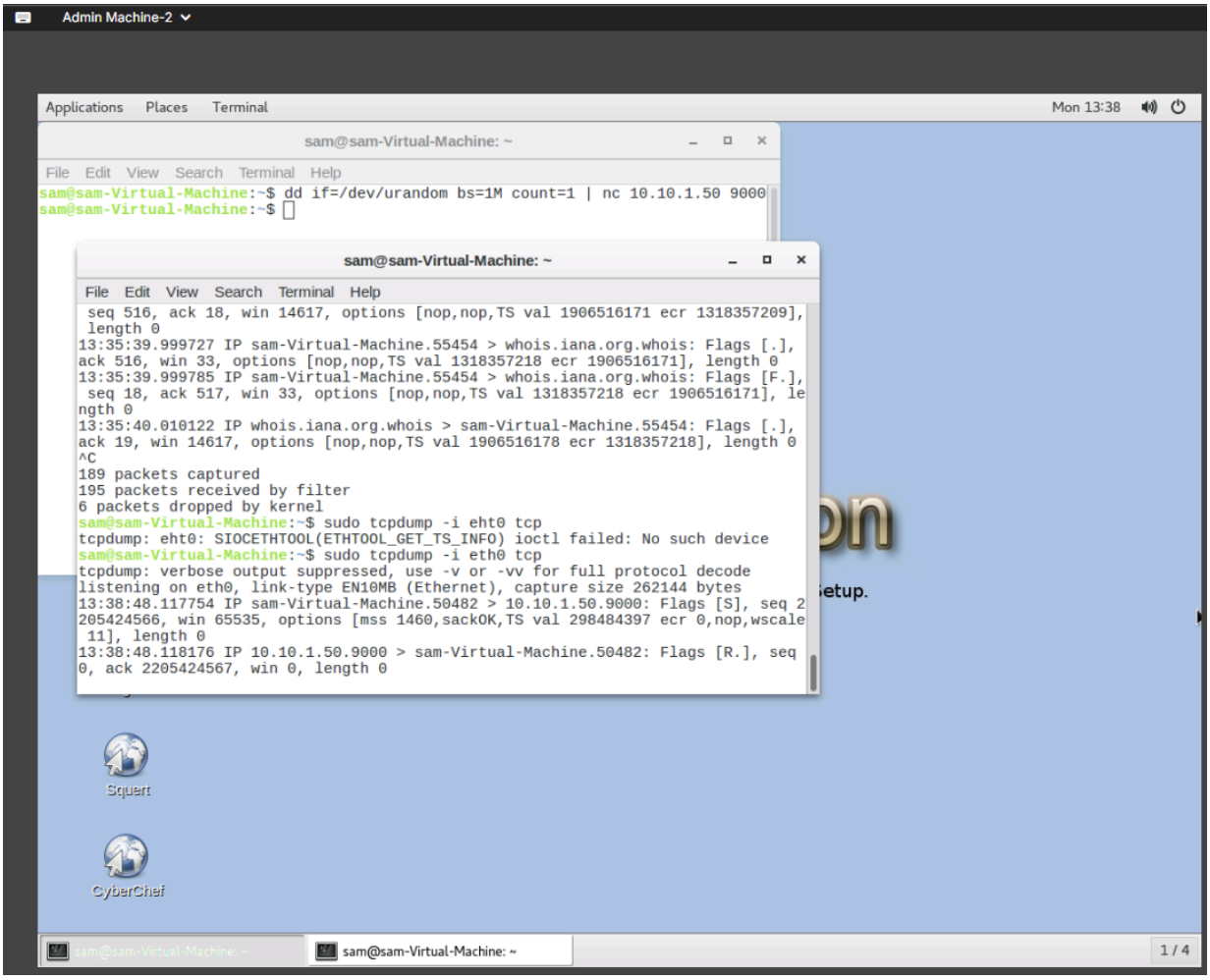
Overview of tcpdump Packet Analyzer

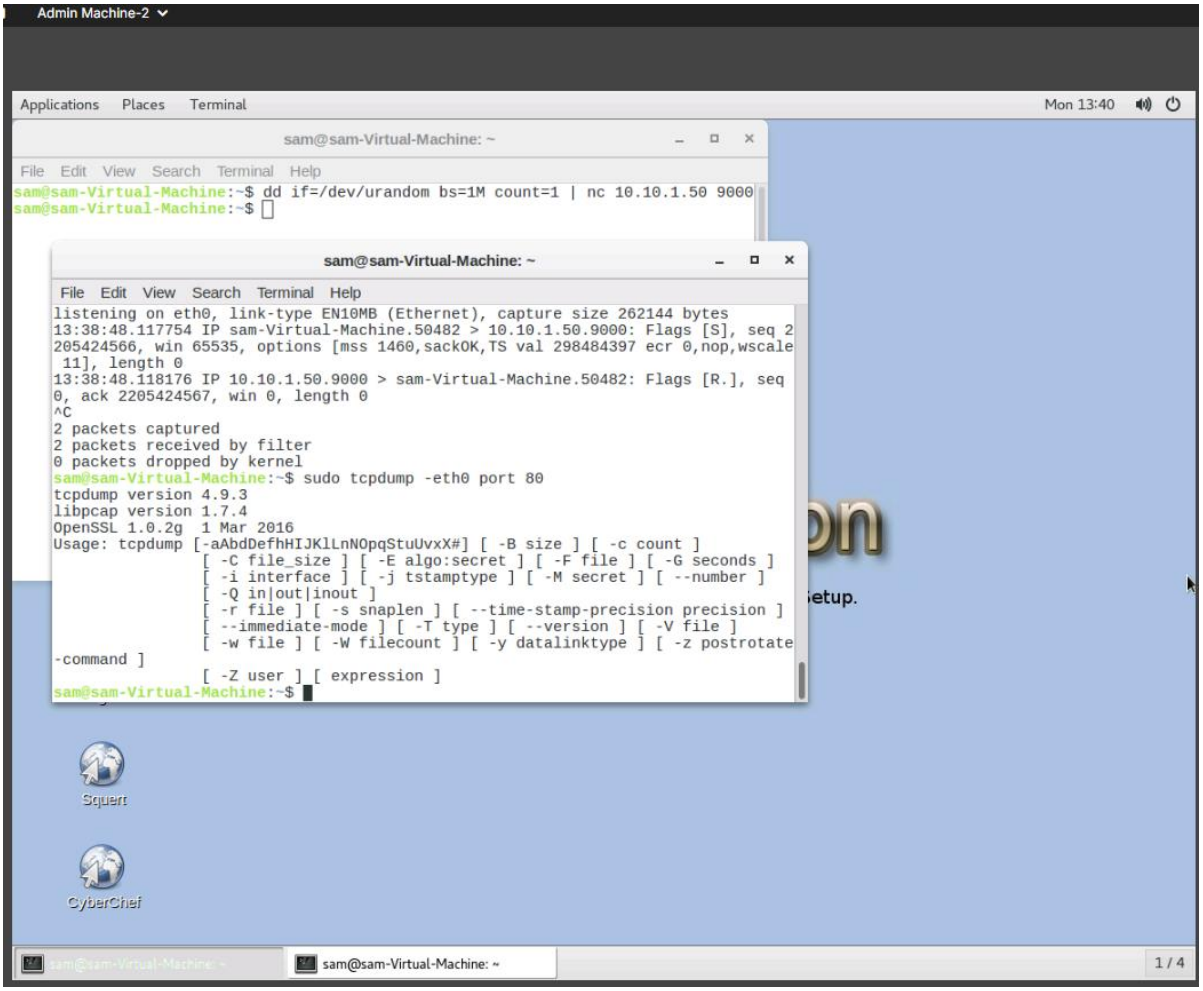
In packet capture, data packets traversing over a network are intercepted using packet capture tools such as tcpdump. These captured packets are analyzed to determine whether proper network security policies are being followed.

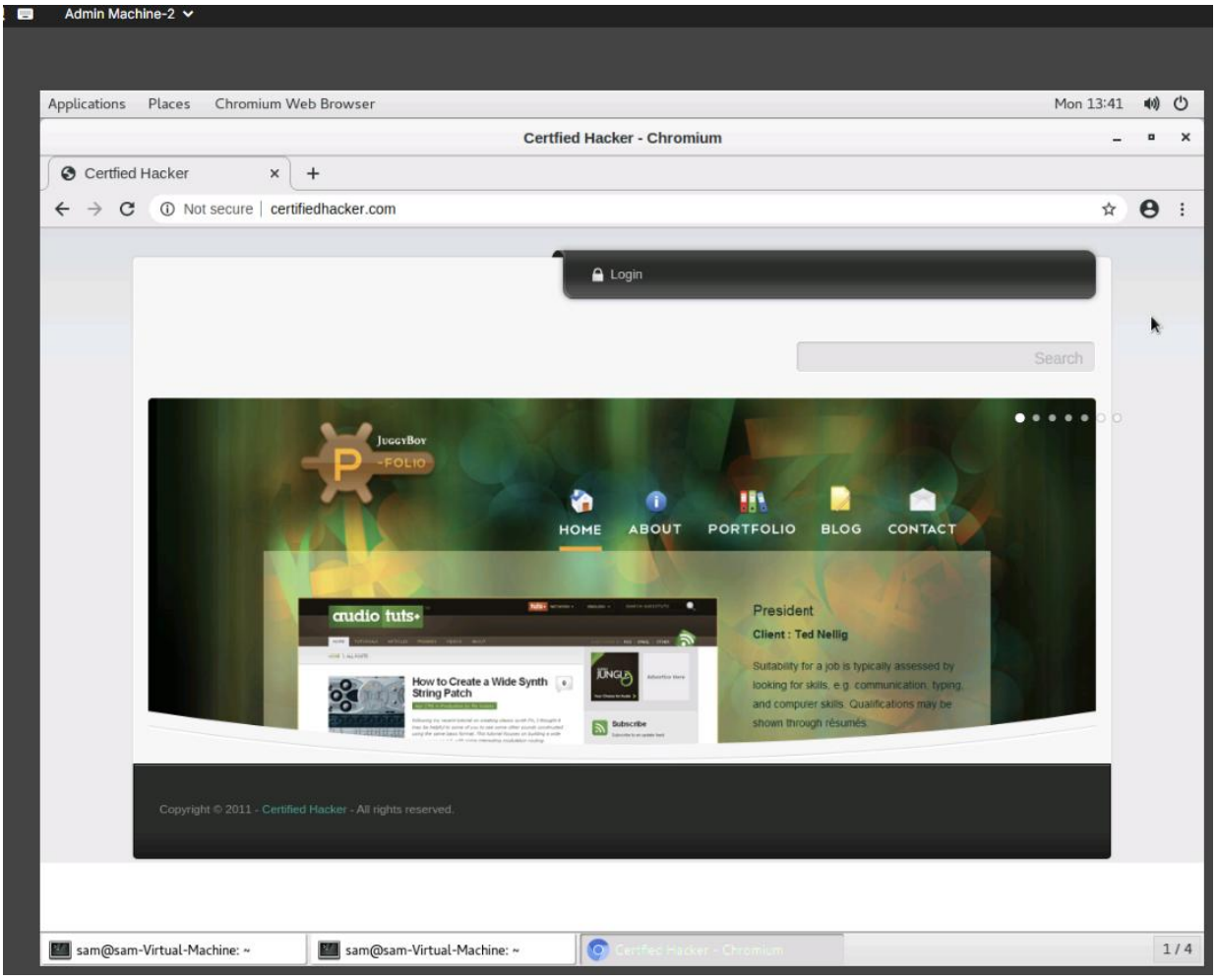


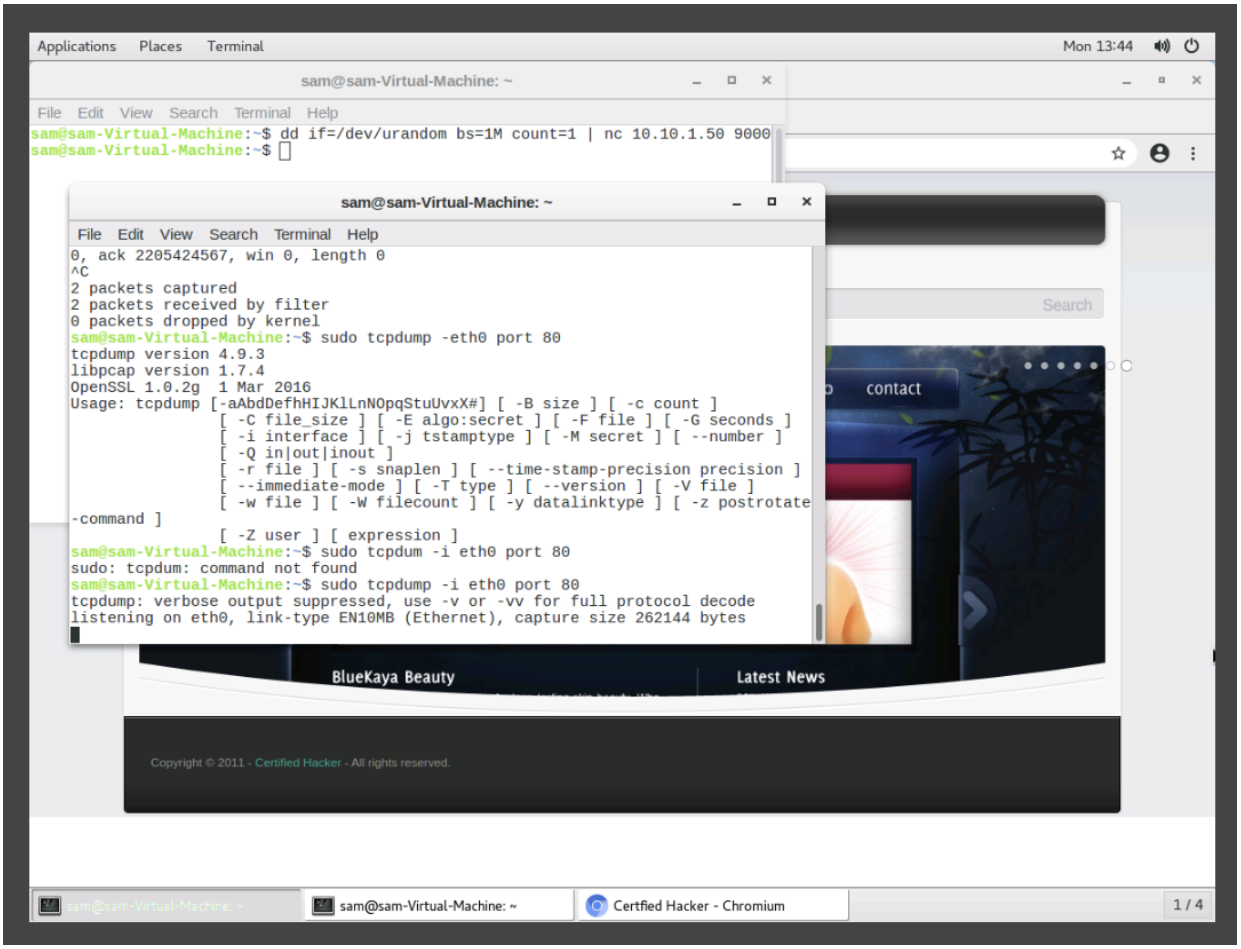

Admin Machine-2
Applications Places Terminal
Mon 13:35
sam@sam-Virtual-Machine: ~
File Edit View Search Terminal Help
13:34:57.934354 IP6 fe80::43e4:a446:6e8a:8a85.mdns > ff02::fb.mdns: 0*- [0q] 8/0/4 (Cache flush) TXT "", PTR _adb._tcp.local., PTR adb-unidentified._adb._tcp.local., (Cache flush) SRV Android.local.:5555 0 0, (Cache flush) PTR Android.local., (Cache flush) PTR Android.local., (Cache flush) A 10.10.1.11, (Cache flush) AAAA fe80::43e4:a446:6e8a:8a85 (376)
13:34:57.934535 IP sam-Virtual-Machine.46176 > dns.google.domain: 25503+ PTR? 251.0.0.224.in-addr.arpa. (42)
13:34:57.942606 IP dns.google.domain > sam-Virtual-Machine.46176: 25503 1/0/0 PTR mdns.mcast.net. (70)
13:34:57.942816 IP sam-Virtual-Machine.50603 > dns.google.domain: 51800+ PTR? 11.1.10.10.in-addr.arpa. (41)
13:34:53.018396 IP sam-virtual-machine.54054 > whois.iana.org.whois: Flags [.], ack 20, win 14618, options [nop,nop,TS val 1056812794 ecr 1906468960], length 0
13:34:53.077816 IP whois.iana.org.whois > sam-Virtual-Machine.54054: Flags [.], ack 20, win 14618, options [nop,nop,TS val 1906469020 ecr 1056812794], length 0
13:34:57.934354 IP 10.10.1.11.mdns > mdns.mcast.net.mdns: 0*- [0q] 8/0/4 (Cache flush) TXT "", PTR _adb._tcp.local., PTR adb-unidentified._adb._tcp.local., (Cache flush) SRV Android.local.:5555 0 0, (Cache flush) PTR Android.local., (Cache flush) PTR Android.local., (Cache flush) A 10.10.1.11, (Cache flush) AAAA fe80::43e4:a446:6e8a:8a85 (376)
13:34:57.934354 IP6 fe80::15:5dff:fe37:189a.mdns > ff02::fb.mdns: 0*- [0q] 6/0/3 (Cache flush) TXT "", PTR _adb._tcp.local., PTR adb-unidentified._adb._tcp.local., (Cache flush) SRV Android.local.:5555 0 0, (Cache flush) PTR Android.local., (Cache flush) AAAA fe80::15:5dff:fe37:189a (309)
13:34:57.934354 IP6 fe80::43e4:a446:6e8a:8a85.mdns > ff02::fb.mdns: 0*- [0q] 8/0/4 (Cache flush) TXT "", PTR _adb._tcp.local., PTR adb-unidentified._adb._tcp.local., (Cache flush) SRV Android.local.:5555 0 0, (Cache flush) PTR Android.local., (Cache flush) PTR Android.local., (Cache flush) A 10.10.1.11, (Cache flush) AAAA fe80::43e4:a446:6e8a:8a85 (376)
13:34:57.934535 IP sam-Virtual-Machine.46176 > dns.google.domain: 25503+ PTR? 251.0.0.224.in-addr.arpa. (42)
13:34:57.942606 IP dns.google.domain > sam-Virtual-Machine.46176: 25503 1/0/0 PTR mdns.mcast.net. (70)
13:34:57.942816 IP sam-Virtual-Machine.50603 > dns.google.domain: 51800+ PTR? 11.1.10.10.in-addr.arpa. (41)
13:34:57.950795 IP dns.google.domain > sam-Virtual-Machine.50603: 51800 NXDomain 0/0/0 (41)
13:34:57.951238 IP sam-Virtual-Machine.36582 > dns.google.domain: 35496+ PTR? b.f.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa. (90)
13:34:57.978536 IP sam-Virtual-Machine.40475 > dns.google.domain: 12388+ PTR? 5.8.a.8.a.8.e.6.6.4.4.a.4.e.3.4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
^C
59 packets captured
63 packets received by filter
4 packets dropped by kernel
sam@sam-Virtual-Machine:~$ sudo tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
13:35:21.837557 IP sam-Virtual-Machine.ntp > 172-233-189-68.ip.linodeusercontent.com.ntp: NTPv4, Client, length 48
13:35:21.837581 IP sam-Virtual-Machine.ntp > ntp.maxhost.io.ntp: NTPv4, Client, length 48
13:35:21.837972 IP sam-Virtual-Machine.57904 > dns.google.domain: 55763+ PTR? 68.189.233.172.in-addr.arpa. (45)
13:35:21.846380 IP dns.google.domain > sam-Virtual-Machine.57904: 55763 1/0/0 PTR 172-233-189-68.ip.linodeusercontent.com. 198
)
13:35:21.846592 IP sam-Virtual-Machine.57625 > dns.google.domain: 7659+ PTR? 79.1.10.10.in-addr.arpa. (41)
13:35:21.854887 IP dns.google.domain > sam-Virtual-Machine.57625: 7659 NXDomain 0/0/0 (41)
13:35:21.855648 IP sam-Virtual-Machine.46060 > dns.google.domain: 13976+ PTR? 125.168.186.23.in-addr.arpa. (45)
13:35:21.864868 IP dns.google.domain > sam-Virtual-Machine.46060: 13976 1/0/0 PTR ntp.maxhost.io. (73)
13:35:21.865699 IP sam-Virtual-Machine.48874 > dns.google.domain: 34418+ PTR? 8.8.8.8.in-addr.arpa. (38)
13:35:21.905842 IP ntp.maxhost.io.ntp > sam-Virtual-Machine.ntp: NTPv4, Server, length 48
sam@sam-Virtual-Machine: ~
1 / 4

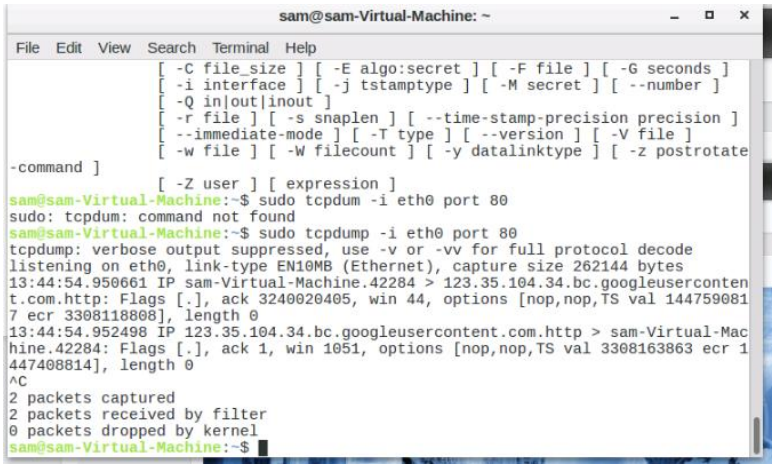

Admin Machine-2
Applications Places Terminal
Mon 13:37
sam@sam-Virtual-Machine: ~
File Edit View Search Terminal Help
13:35:38.031229 IP whois.iana.org.whois > sam-Virtual-Machine.54126: Flags [P.], seq 1:516, ack 18, win 14617, options [nop,nop,TS val 1906513972 ecr 1056857744], length 515
13:35:38.031293 IP whois.iana.org.whois > sam-Virtual-Machine.54126: Flags [F.], seq 516, ack 18, win 14617, options [nop,nop,TS val 1906513972 ecr 1056857744], length 0
13:35:38.031448 IP sam-Virtual-Machine.54126 > whois.iana.org.whois: Flags [.], ack 516, win 33, options [nop,nop,TS val 1056857806 ecr 1906513972], length 0
13:35:38.031498 IP sam-Virtual-Machine.54126 > whois.iana.org.whois: Flags [F.], seq 18, ack 517, win 33, options [nop,nop,TS val 1056857806 ecr 1906513972], length 0
13:35:38.090688 IP whois.iana.org.whois > sam-Virtual-Machine.54126: Flags [.], ack 19, win 14617, options [nop,nop,TS val 1906514033 ecr 1056857806], length 0
13:35:38.266690 ARP, Request who-has 10.10.1.10 tell 10.10.1.2, length 28
13:35:39.096888 IP6 fe80::1848:a5f4:f604:cf99.dhcpv6-client > ff02::1:2.dhcpv6-server: dhcp6 solicit
13:35:39.266722 ARP, Request who-has 10.10.1.10 tell 10.10.1.2, length 28
13:35:39.971815 IP sam-Virtual-Machine.57589 > dns.google.domain: 50599+ A? arpa.whois-servers.net. (40)
13:35:39.984540 IP dns.google.domain > sam-Virtual-Machine.57589: 50599 4/0/0 CNAME whois.iana.org., CNAME ianawhois.vip.icann.org., A 192.0.47.59, A 192.0.32.59 (134)
13:35:39.985716 IP sam-Virtual-Machine.55454 > whois.iana.org.whois: Flags [S], seq 3501682246, win 65535, options [mss 1460,sackOK,TS val 1318357204 ecr 0,nop,wscale 11], length 0
13:35:39.990831 IP whois.iana.org.whois > sam-Virtual-Machine.55454: Flags [S.], seq 259383106, ack 3501682247, win 14600, options [mss 1460,nop,wscale 0,sackOK,TS val 1906516164 ecr 1318357204], length 0
13:35:39.990905 IP sam-Virtual-Machine.55454 > whois.iana.org.whois: Flags [.], ack 1, win 32, options [nop,nop,TS val 1318357209 ecr 1906516164], length 0
13:35:39.991047 IP sam-Virtual-Machine.55454 > whois.iana.org.whois: Flags [P.], seq 1:18, ack 1, win 32, options [nop,nop,TS val 1318357209 ecr 1906516164], length 17
13:35:39.998289 IP whois.iana.org.whois > sam-Virtual-Machine.55454: Flags [.], ack 18, win 14617, options [nop,nop,TS val 1906516169 ecr 1318357209], length 0
13:35:39.999664 IP whois.iana.org.whois > sam-Virtual-Machine.55454: Flags [P.], seq 1:516, ack 18, win 14617, options [nop,nop,TS val 1906516171 ecr 1318357209], length 515
13:35:39.999685 IP whois.iana.org.whois > sam-Virtual-Machine.55454: Flags [F.], seq 516, ack 18, win 14617, options [nop,nop,TS val 1906516171 ecr 1318357209], length 0
13:35:39.999727 IP sam-Virtual-Machine.55454 > whois.iana.org.whois: Flags [.], ack 516, win 33, options [nop,nop,TS val 1318357218 ecr 1906516171], length 0
13:35:39.999785 IP sam-Virtual-Machine.55454 > whois.iana.org.whois: Flags [F.], seq 18, ack 517, win 33, options [nop,nop,TS val 1318357218 ecr 1906516171], length 0
13:35:40.010122 IP whois.iana.org.whois > sam-Virtual-Machine.55454: Flags [.], ack 19, win 14617, options [nop,nop,TS val 1906516178 ecr 1318357218], length 0
^C
189 packets captured
195 packets received by filter
6 packets dropped by kernel
sam@sam-Virtual-Machine:~$ sudo tcpdump -i eht0 tcp
tcpdump: eht0: SIOCETHTOOL(ETHTOOL_GET_TS_INFO) ioctl failed: No such device
sam@sam-Virtual-Machine:~$ sudo tcpdump -i eth0 tcp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
1 / 4

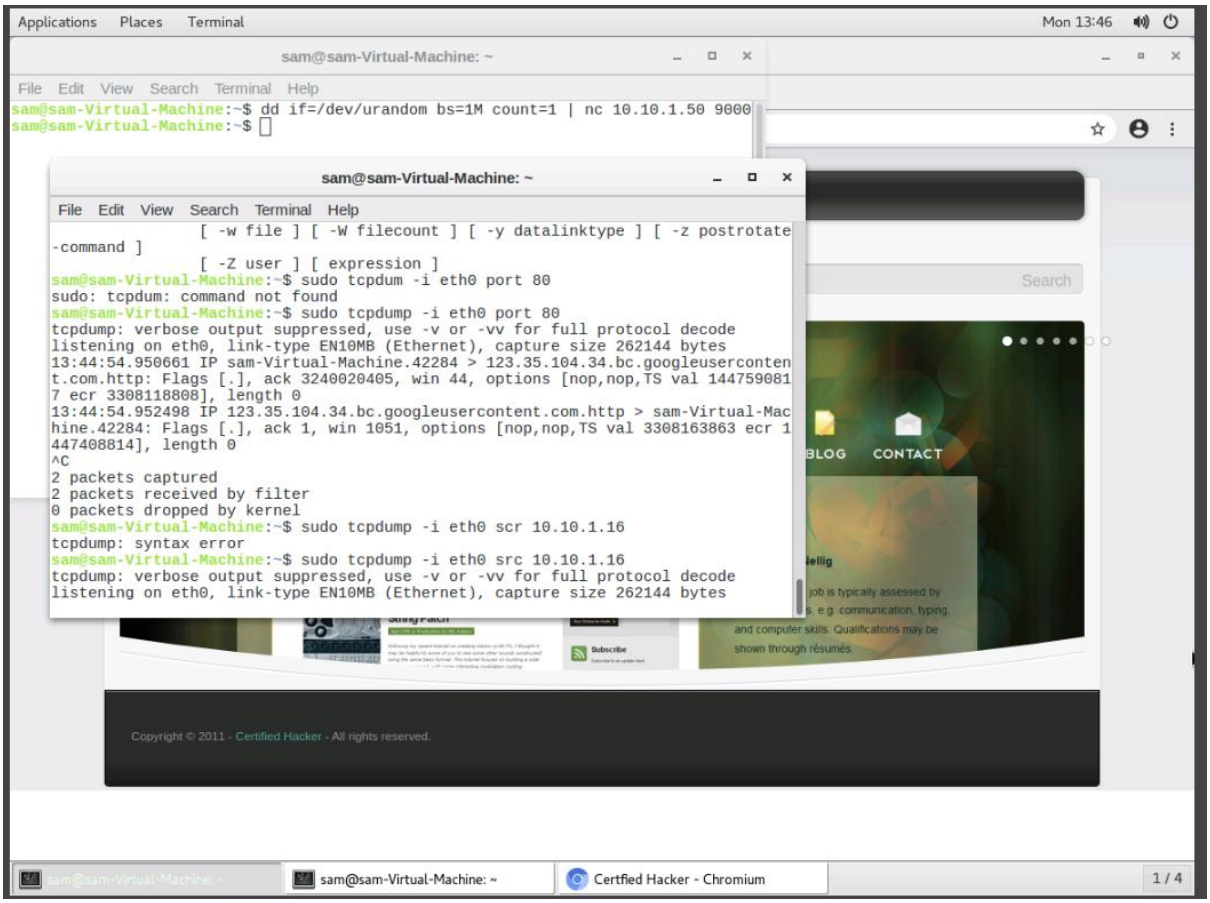

Admin Machine-2
Applications
Places
Terminal
Mon 13:38
sam@sam-Virtual-Machine: ~
File Edit View Search Terminal Help
sam@sam-Virtual-Machine:~$ dd if=/dev/urandom bs=1M count=1 | nc 10.10.1.50 9000
sam@sam-Virtual-Machine:~$
sam@sam-Virtual-Machine: ~
File Edit View Search Terminal Help
seq 516, ack 18, win 14617, options [nop,nop,TS val 1906516171 ecr 1318357209], length 0
13:35:39.999727 IP sam-Virtual-Machine.55454 > whois.iana.org.whois: Flags [.], ack 516, win 33, options [nop,nop,TS val 1318357218 ecr 1906516171], length 0
13:35:39.999785 IP sam-Virtual-Machine.55454 > whois.iana.org.whois: Flags [F.], seq 18, ack 517, win 33, options [nop,nop,TS val 1318357218 ecr 1906516171], length 0
13:35:40.010122 IP whois.iana.org.whois > sam-Virtual-Machine.55454: Flags [.], ack 19, win 14617, options [nop,nop,TS val 1906516178 ecr 1318357218], length 0
^C
189 packets captured
195 packets received by filter
6 packets dropped by kernel
sam@sam-Virtual-Machine:~$ sudo tcpdump -i eht0 tcp
tcpdump: eht0: SIOCETHTOOL(ETHTOOL_GET_TS_INFO) ioctl failed: No such device
sam@sam-Virtual-Machine:~$ sudo tcpdump -i eth0 tcp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
13:38:48.117754 IP sam-Virtual-Machine.50482 > 10.10.1.50.9000: Flags [S], seq 2205424566, win 65535, options [mss 1460,sackOK,TS val 298484397 ecr 0,nop,wscale 11], length 0
13:38:48.118176 IP 10.10.1.50.9000 > sam-Virtual-Machine.50482: Flags [R.], seq 0, ack 2205424567, win 0, length 0
Squert
CyberChef
sam@sam-Virtual-Machine: ~
sam@sam-Virtual-Machine: ~
1 / 4

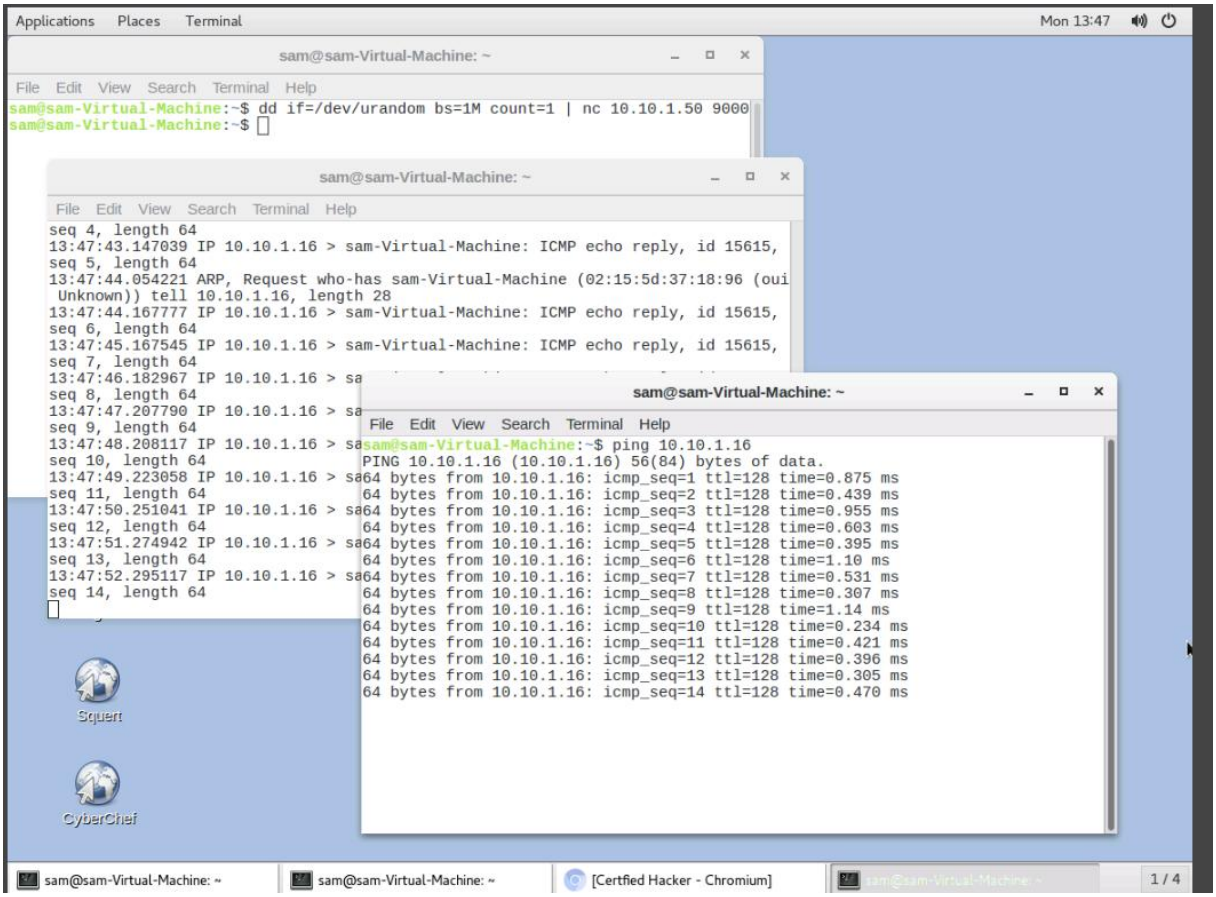

Admin Machine-2
Applications Places Terminal
Mon 13:40
sam@sam-Virtual-Machine: ~
File Edit View Search Terminal Help
sam@sam-Virtual-Machine:~$ dd if=/dev/urandom bs=1M count=1 | nc 10.10.1.50 9000
sam@sam-Virtual-Machine:~$
sam@sam-Virtual-Machine: ~
File Edit View Search Terminal Help
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
13:38:48.117754 IP sam-Virtual-Machine.50482 > 10.10.1.50.9000: Flags [S], seq 2
205424566, win 65535, options [mss 1460,sackOK,TS val 298484397 ecr 0,nop,wscale
11], length 0
13:38:48.118176 IP 10.10.1.50.9000 > sam-Virtual-Machine.50482: Flags [R.], seq
0, ack 2205424567, win 0, length 0
^C
2 packets captured
2 packets received by filter
0 packets dropped by kernel
sam@sam-Virtual-Machine:~$ sudo tcpdump -eth0 port 80
tcpdump version 4.9.3
libpcap version 1.7.4
OpenSSL 1.0.2g 1 Mar 2016
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqStuUvxX#] [-B size] [-c count]
[-C file_size] [-E algo:secret] [-F file] [-G seconds]
[-i interface] [-j tstamptype] [-M secret] [--number]
[-Q in|out|inout]
[-r file] [-s snaplen] [--time-stamp-precision precision]
[--immediate-mode] [-T type] [--version] [-V file]
[-w file] [-W filecount] [-y datalinktype] [-z postrotate
-command]
[-Z user] [expression]
sam@sam-Virtual-Machine:~$
Squert
CyberChef
sam@sam-Virtual-Machine: ~
1 / 4


Admin Machine-2
Applications
Places
Chromium Web Browser
Mon 13:41
Certfied Hacker - Chromium
Certfied Hacker
Not secure | certifiedhacker.com
Login
Search
JUGGYBOY
-FOLIO
HOME
ABOUT
PORTFOLIO
BLOG
CONTACT
audio tuts+
How to Create a Wide Synth String Patch
Subscribe
President
Client : Ted Nellig
Suitability for a job is typically assessed by looking for skills, e.g. communication, typing, and computer skills. Qualifications may be shown through résumés.
Copyright © 2011 - Certified Hacker - All rights reserved.
sam@sam-Virtual-Machine: ~
sam@sam-Virtual-Machine: ~
Certfied Hacker - Chromium
1 / 4


Applications Places Terminal
Mon 13:44
sam@sam-Virtual-Machine: ~
File Edit View Search Terminal Help
sam@sam-Virtual-Machine:~$ dd if=/dev/urandom bs=1M count=1 | nc 10.10.1.50 9000
sam@sam-Virtual-Machine:~$
sam@sam-Virtual-Machine: ~
File Edit View Search Terminal Help
0, ack 2205424567, win 0, length 0
^C
2 packets captured
2 packets received by filter
0 packets dropped by kernel
sam@sam-Virtual-Machine:~$ sudo tcpdump -eth0 port 80
tcpdump version 4.9.3
libpcap version 1.7.4
OpenSSL 1.0.2g 1 Mar 2016
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqStuUvxX#] [-B size] [-c count]
[-C file_size] [-E algo:secret] [-F file] [-G seconds]
[-i interface] [-j tstamptype] [-M secret] [--number]
[-Q in|out|inout]
[-r file] [-s snaplen] [--time-stamp-precision precision]
[--immediate-mode] [-T type] [--version] [-V file]
[-w file] [-W filecount] [-y datalinktype] [-z postrotate
-command]
[-Z user] [expression]
sam@sam-Virtual-Machine:~$ sudo tcpdum -i eth0 port 80
sudo: tcpdum: command not found
sam@sam-Virtual-Machine:~$ sudo tcpdump -i eth0 port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
Search
contact
BlueKaya Beauty
Latest News
Copyright © 2011 - Certified Hacker - All rights reserved.
sam@sam-Virtual-Machine: ~
sam@sam-Virtual-Machine: ~
Certfied Hacker - Chromium
1 / 4


sam@sam-Virtual-Machine: ~
File Edit View Search Terminal Help
[-C file_size] [-E algo:secret] [-F file] [-G seconds]
[-i interface] [-j tstamptype] [-M secret] [--number]
[-Q in|out|inout]
[-r file] [-s snaplen] [--time-stamp-precision precision]
[--immediate-mode] [-T type] [--version] [-V file]
[-w file] [-W filecount] [-y datalinktype] [-z postrotate
-command]
[-Z user] [expression]
sam@sam-Virtual-Machine:~$ sudo tcpdum -i eth0 port 80
sudo: tcpdum: command not found
sam@sam-Virtual-Machine:~$ sudo tcpdump -i eth0 port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
13:44:54.950661 IP sam-Virtual-Machine.42284 > 123.35.104.34.bc.googleuserconten
t.com.http: Flags [.], ack 3240020405, win 44, options [nop,nop,TS val 144759081
7 ecr 3308118808], length 0
13:44:54.952498 IP 123.35.104.34.bc.googleusercontent.com.http > sam-Virtual-Mac
hine.42284: Flags [.], ack 1, win 1051, options [nop,nop,TS val 3308163863 ecr 1
447408814], length 0
^C
2 packets captured
2 packets received by filter
0 packets dropped by kernel
sam@sam-Virtual-Machine:~$


Applications Places Terminal
Mon 13:46
sam@sam-Virtual-Machine: ~
File Edit View Search Terminal Help
sam@sam-Virtual-Machine:~$ dd if=/dev/urandom bs=1M count=1 | nc 10.10.1.50 9000
sam@sam-Virtual-Machine:~$
sam@sam-Virtual-Machine: ~
File Edit View Search Terminal Help
[-w file] [-W filecount] [-y datalinktype] [-z postrotate
-command]
[-Z user] [expression]
sam@sam-Virtual-Machine:~$ sudo tcpdum -i eth0 port 80
sudo: tcpdum: command not found
sam@sam-Virtual-Machine:~$ sudo tcpdump -i eth0 port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
13:44:54.950661 IP sam-Virtual-Machine.42284 > 123.35.104.34.bc.googleusercontent
t.com.http: Flags [.], ack 3240020405, win 44, options [nop,nop,TS val 144759081
7 ecr 3308118808], length 0
13:44:54.952498 IP 123.35.104.34.bc.googleusercontent.com.http > sam-Virtual-Mac
hine.42284: Flags [.], ack 1, win 1051, options [nop,nop,TS val 3308163863 ecr 1
447408814], length 0
^C
2 packets captured
2 packets received by filter
0 packets dropped by kernel
sam@sam-Virtual-Machine:~$ sudo tcpdump -i eth0 scr 10.10.1.16
tcpdump: syntax error
sam@sam-Virtual-Machine:~$ sudo tcpdump -i eth0 src 10.10.1.16
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
Search
BLOG
CONTACT
Subscribe
Copyright © 2011 - Certified Hacker - All rights reserved.
sam@sam-Virtual-Machine: ~
sam@sam-Virtual-Machine: ~
Certfied Hacker - Chromium
1 / 4



Lab Summary: Network Traffic Monitoring

Exercise 1: Capturing Network Traffic using Wireshark

This exercise demonstrated how to use Wireshark to capture and analyze network traffic. The graphical interface of Wireshark made it easier to view live traffic flows compared to command-line tools. By capturing packets, a network defender can observe data flows across protocols and gain visibility into activities on the network. This emphasized the role of packet capture in monitoring compliance with security policies.

Exercise 2: Applying Various Filters in Wireshark

The second exercise focused on applying filters in Wireshark to isolate relevant traffic. Filters such as source IP, destination IP, and ICMP were used to narrow down specific packet types. This step illustrated the efficiency gained by using filters rather than manually scanning through large amounts of captured data. Learning to apply filters is essential for quickly identifying suspicious or malicious traffic patterns.

Exercise 3: Analyzing and Examining Various Network Packet Headers in Linux using tcpdump

The final exercise introduced tcpdump as a command-line packet analyzer. By capturing and examining TCP/IP packet headers directly in Linux, the lab highlighted the importance of reviewing control information such as source/destination IP addresses, MAC addresses, and sequencing details. Tcpdump reinforced the ability to analyze traffic at a low level without a graphical interface, making it useful in environments where GUI tools like Wireshark are unavailable.

Reflection

This module demonstrated both GUI-based (Wireshark) and CLI-based (tcpdump) approaches to network monitoring. Wireshark offered accessibility and filtering for visual analysis, while tcpdump provided granular, low-level inspection of packet headers. Together, these tools gave a comprehensive understanding of packet capture and analysis techniques, equipping a network defender with versatile skills for monitoring traffic and identifying threats.