Module 08: Network Forensics

Lab Scenario

James, an incident response manager at a software company, received a complaint from Jessica (one of the company's employees), that she is receiving sensitive emails from an unknown person or email ID and that she suspects another employee to be sending these emails. James wanted to capture and analyze all incoming and outgoing packets in the company's network in order to trace the person sending these sensitive emails to Jessica.'

Lab Objectives

The objective of the labs is to help you understand how to analyze network packets of a target network and investigate further. Accomplishing this task will entail the following:

- Investigate network attacks from evidence logs
- Analyze network traffic for artifacts that establish the occurrence of various attacks over a network

Overview of Network Forensics

Network forensics is the process of identifying malicious activities taking place over a network and tracing their origins. Network forensics encompasses the recording, acquisition, and analysis of network traffic and event log data to investigate a network security incident. It enables a forensic investigator to inspect the network traffic and logs to identify and track various types of network attacks.

Lab Tasks

Recommended labs to assist you in performing network forensics:

- Identifying and investigating various network attacks using Wireshark

Lab 1: Identifying and Investigating Various Network Attacks using Wireshark

Lab Scenario

A financial services company discovered that its trade secrets and intellectual property was being stolen. The company suspected that its network might have become susceptible to intrusions or various attacks and this might have led to the loss of sensitive information. It sought the services of cyber-forensic investigators to determine if its network was being subjected to various attacks.

Investigators now have to analyze the packets captured from the traffic flowing across the company's network. Through this, the investigators will be able to retrieve the artifacts related to various types of attacks the company's network is being subjected to.

Forensic investigators must have a sound knowledge on the process of analyzing the packets captured from the network traffic to be able to retrieve the artifacts related to various network attack(s)

Lab Objectives

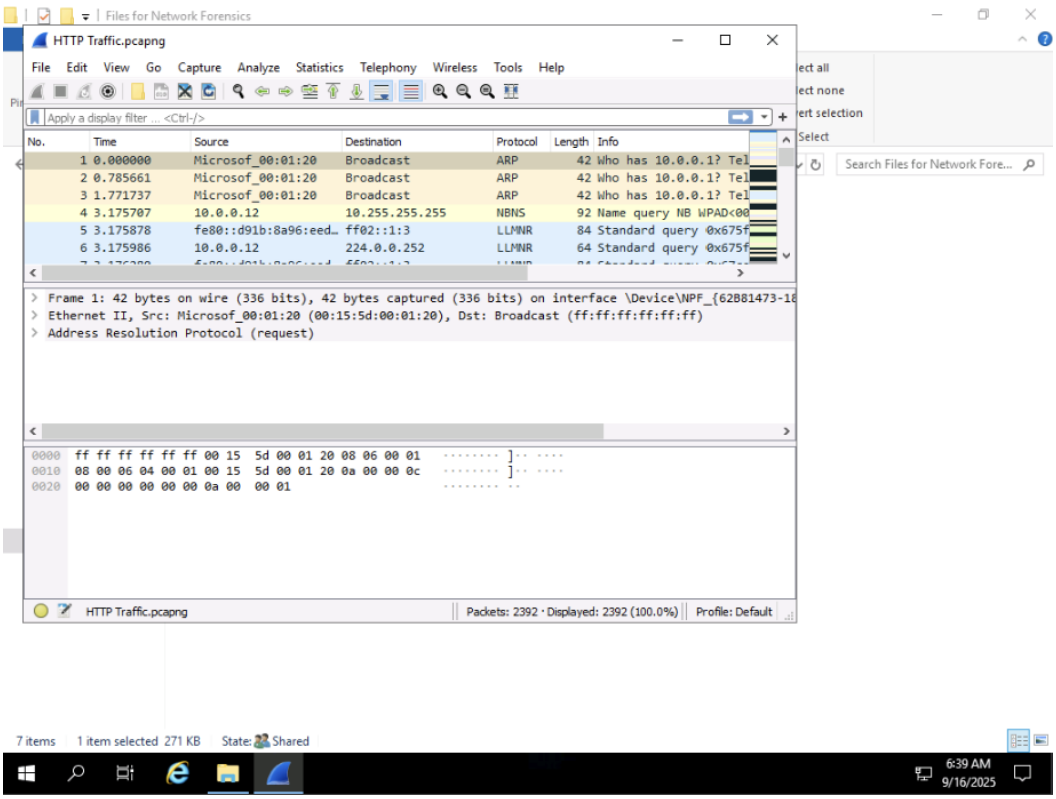
Investigation of network attacks involves an analysis of packets traveling across a network at a given point of time to retrieve the artifacts that reveal or confirm the occurrence of various network attacks.

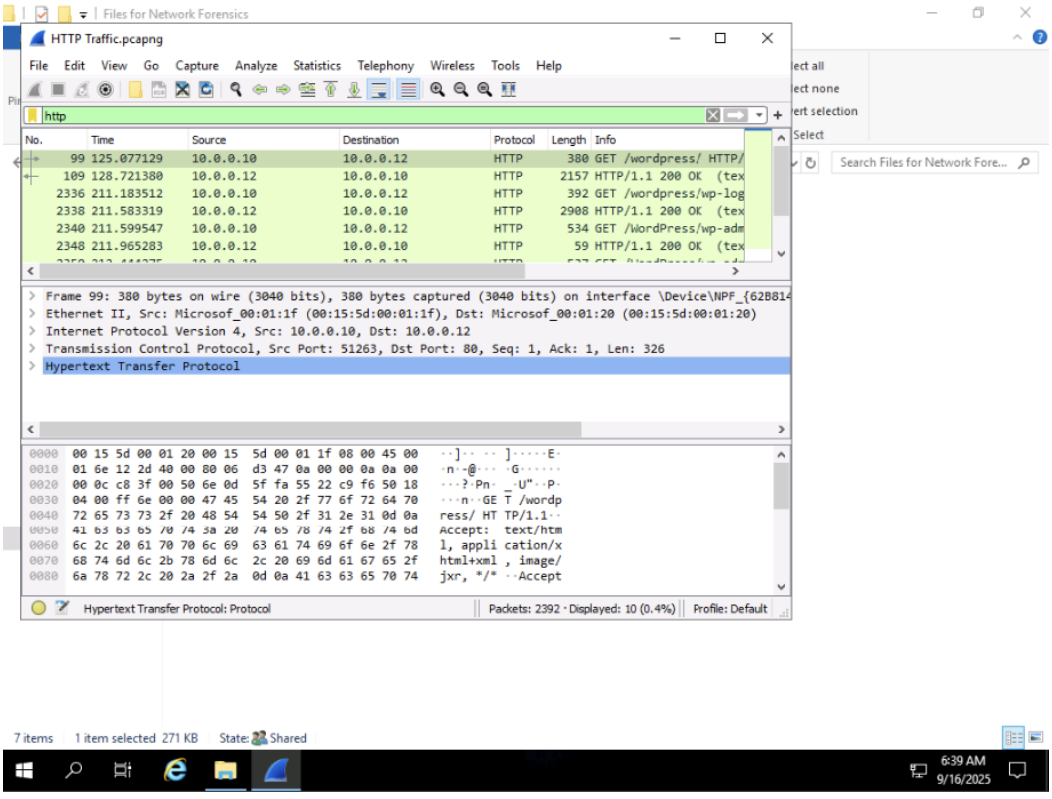
The objective of this lab is to:

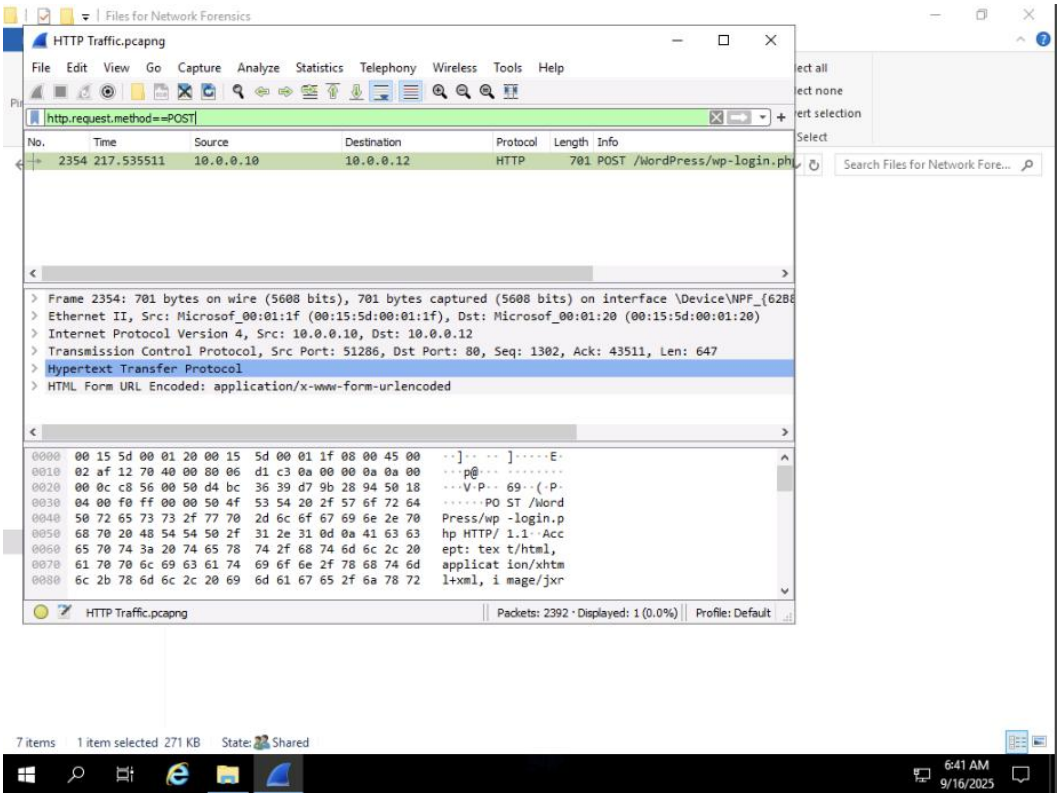
- Analyze incoming and outgoing packets
- Examine various network packet capture files for artifacts of various network attacks

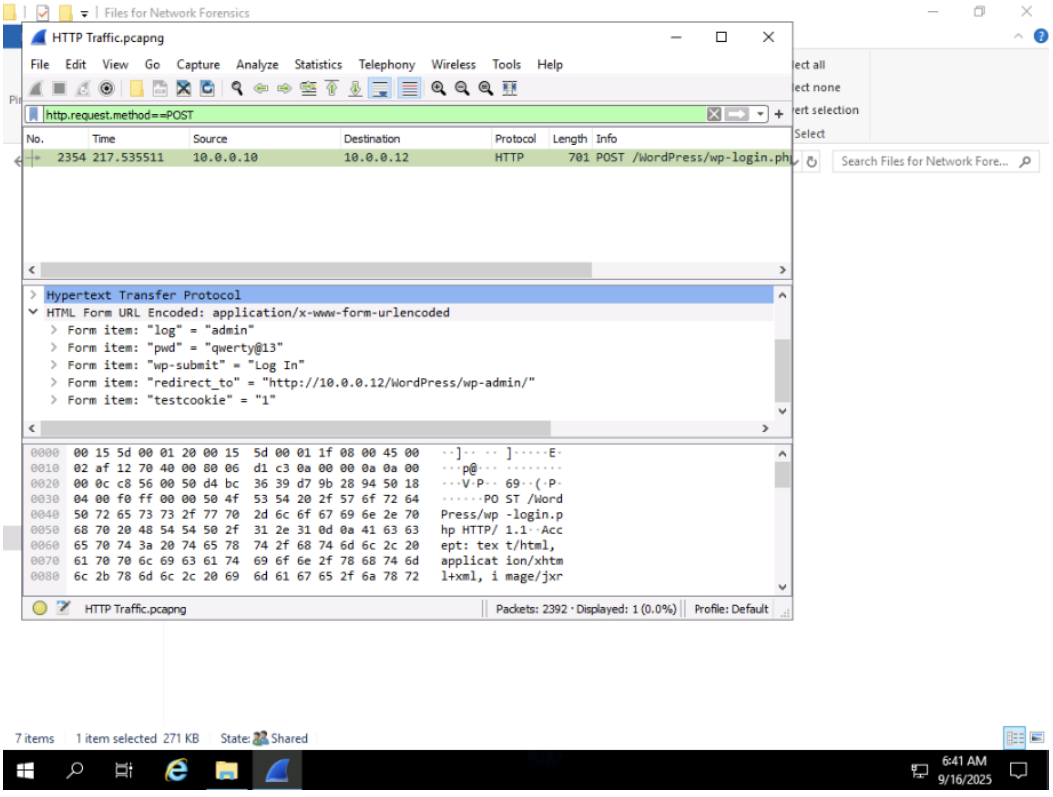
Overview of the Lab

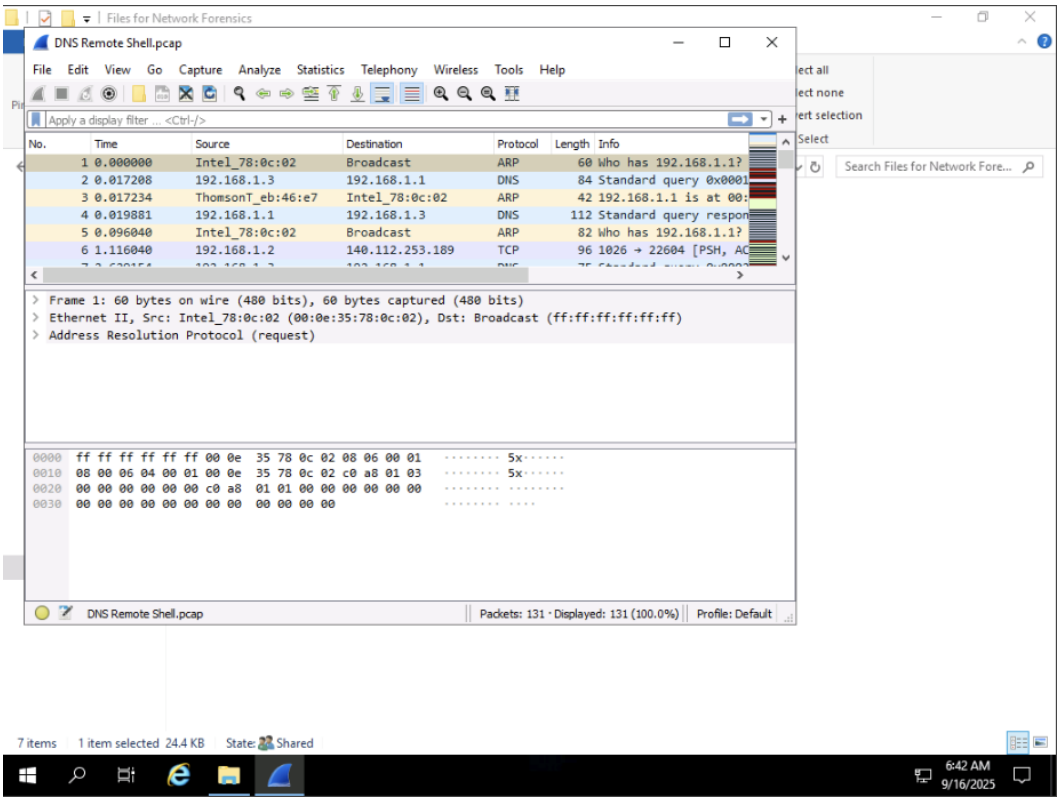
This lab familiarizes you with the process of examining network packet capture files for various network attack indicators and investigating them using Wireshark.

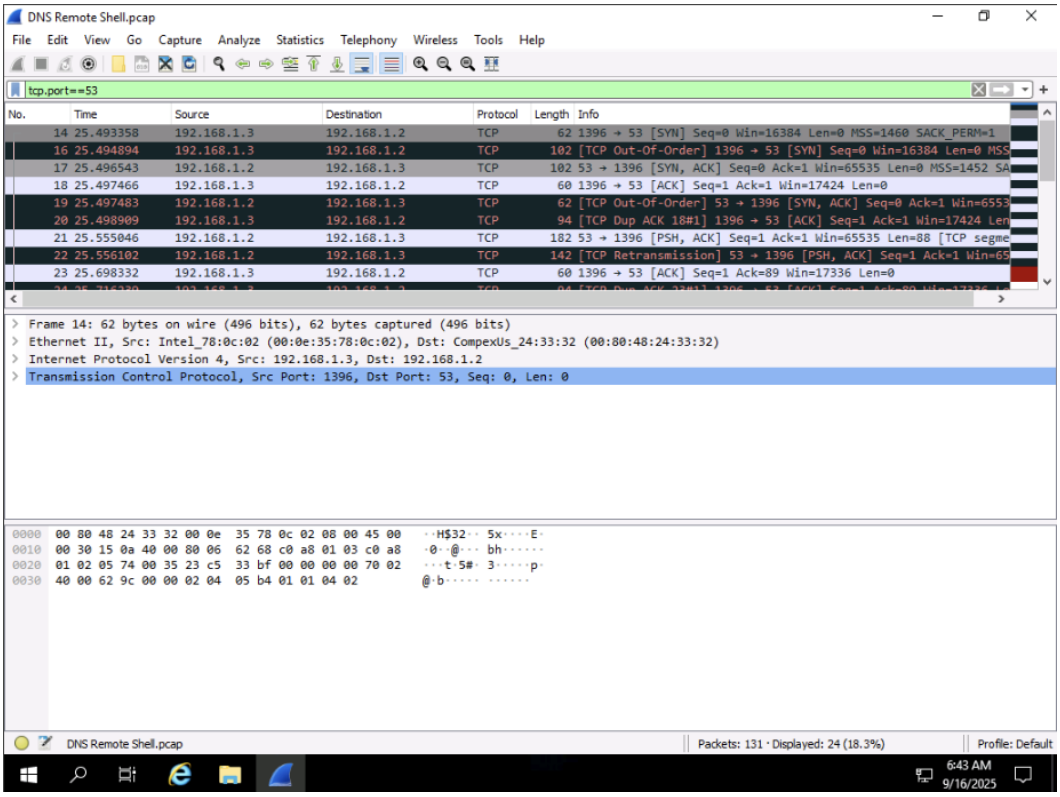

Files for Network Forensics
HTTP Traffic.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 Microsof_00:01:20 Broadcast ARP 42 Who has 10.0.0.1? Tel
2 0.785661 Microsof_00:01:20 Broadcast ARP 42 Who has 10.0.0.1? Tel
3 1.771737 Microsof_00:01:20 Broadcast ARP 42 Who has 10.0.0.1? Tel
4 3.175707 10.0.0.12 10.255.255.255 NBNS 92 Name query NB WPAD<00
5 3.175878 fe80::d91b:8a96:eed… ff02::1:3 LLMNR 84 Standard query 0x675f
6 3.175986 10.0.0.12 224.0.0.252 LLMNR 64 Standard query 0x675f
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{62B81473-18
Ethernet II, Src: Microsof_00:01:20 (00:15:5d:00:01:20), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 00 15 5d 00 01 20 08 06 00 01
0010 08 00 06 04 00 01 00 15 5d 00 01 20 0a 00 00 0c
0020 00 00 00 00 00 00 0a 00 00 01
HTTP Traffic.pcapng
Packets: 2392 · Displayed: 2392 (100.0%)
Profile: Default
7 items
1 item selected 271 KB
State: Shared
6:39 AM
9/16/2025

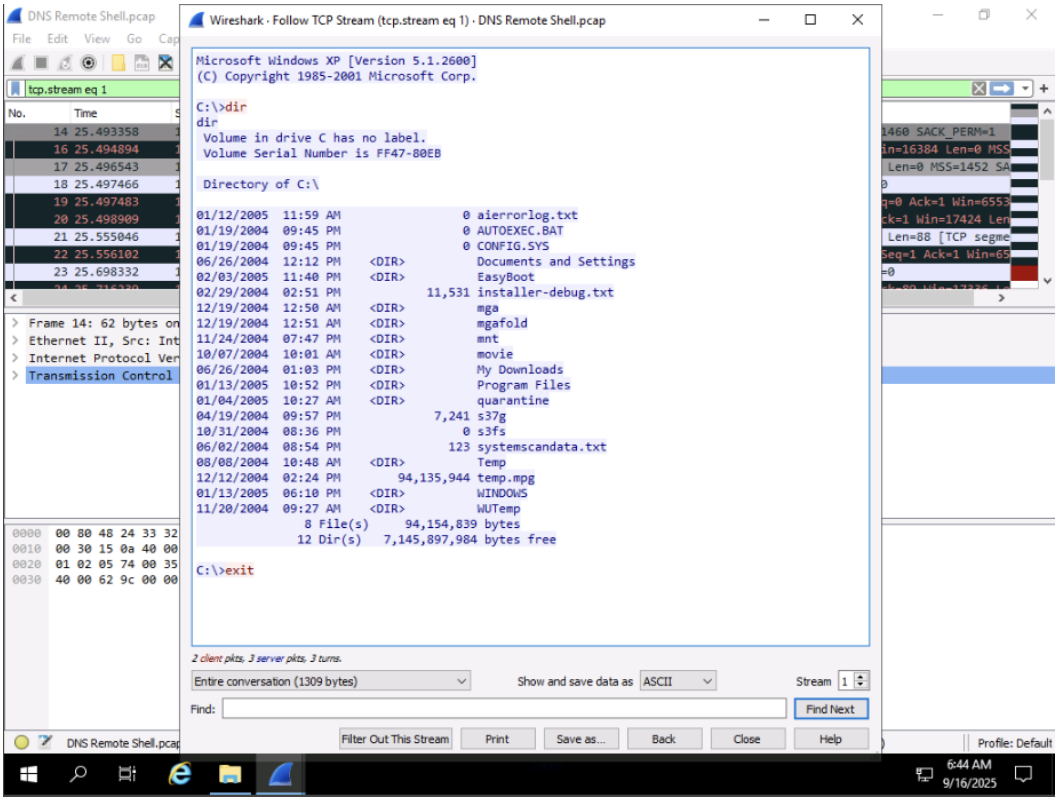

Files for Network Forensics
HTTP Traffic.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
99 125.077129 10.0.0.10 10.0.0.12 HTTP 380 GET /wordpress/ HTTP/
109 128.721380 10.0.0.12 10.0.0.10 HTTP 2157 HTTP/1.1 200 OK (tex
2336 211.183512 10.0.0.10 10.0.0.12 HTTP 392 GET /wordpress/wp-log
2338 211.583319 10.0.0.12 10.0.0.10 HTTP 2908 HTTP/1.1 200 OK (tex
2340 211.599547 10.0.0.10 10.0.0.12 HTTP 534 GET /WordPress/wp-adm
2348 211.965283 10.0.0.12 10.0.0.10 HTTP 59 HTTP/1.1 200 OK (tex
Frame 99: 380 bytes on wire (3040 bits), 380 bytes captured (3040 bits) on interface \Device\NPF_{62B814
Ethernet II, Src: Microsof_00:01:1f (00:15:5d:00:01:1f), Dst: Microsof_00:01:20 (00:15:5d:00:01:20)
Internet Protocol Version 4, Src: 10.0.0.10, Dst: 10.0.0.12
Transmission Control Protocol, Src Port: 51263, Dst Port: 80, Seq: 1, Ack: 1, Len: 326
Hypertext Transfer Protocol
0000 00 15 5d 00 01 20 00 15 5d 00 01 1f 08 00 45 00
0010 01 6e 12 2d 40 00 80 06 d3 47 0a 00 00 0a 0a 00
0020 00 0c c8 3f 00 50 6e 0d 5f fa 55 22 c9 f6 50 18
0030 04 00 ff 6e 00 00 47 45 54 20 2f 77 6f 72 64 70
0040 72 65 73 73 2f 20 48 54 54 50 2f 31 2e 31 0d 0a
0050 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d
0060 6c 2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78
0070 68 74 6d 6c 2b 78 6d 6c 2c 20 69 6d 61 67 65 2f
0080 6a 78 72 2c 20 2a 2f 2a 0d 0a 41 63 63 65 70 74
Hypertext Transfer Protocol: Protocol
Packets: 2392 · Displayed: 10 (0.4%)
Profile: Default
7 items
1 item selected 271 KB
State: Shared
6:39 AM
9/16/2025

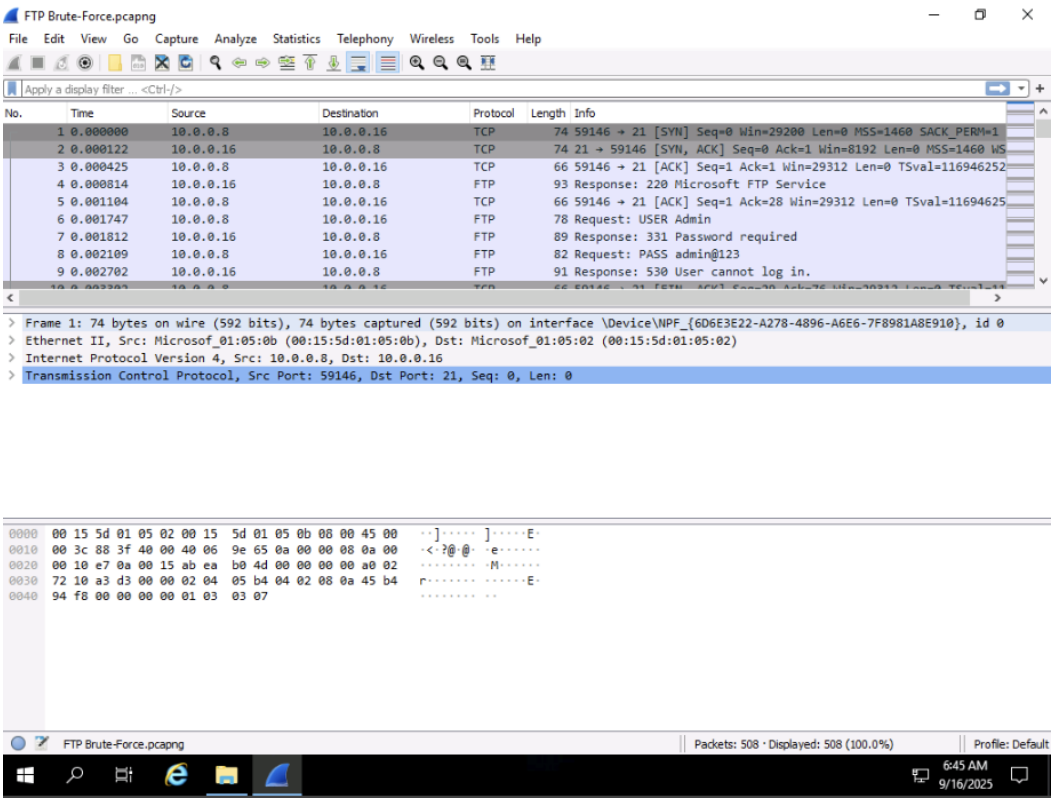

Files for Network Forensics
HTTP Traffic.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request.method==POST
No. Time Source Destination Protocol Length Info
2354 217.535511 10.0.0.10 10.0.0.12 HTTP 701 POST /WordPress/wp-login.ph
Frame 2354: 701 bytes on wire (5608 bits), 701 bytes captured (5608 bits) on interface \Device\NPF_{62B6
Ethernet II, Src: Microsof_00:01:1f (00:15:5d:00:01:1f), Dst: Microsof_00:01:20 (00:15:5d:00:01:20)
Internet Protocol Version 4, Src: 10.0.0.10, Dst: 10.0.0.12
Transmission Control Protocol, Src Port: 51286, Dst Port: 80, Seq: 1302, Ack: 43511, Len: 647
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
0000 00 15 5d 00 01 20 00 15 5d 00 01 1f 08 00 45 00
0010 02 af 12 70 40 00 80 06 d1 c3 0a 00 00 0a 0a 00
0020 00 0c c8 56 00 50 d4 bc 36 39 d7 9b 28 94 50 18
0030 04 00 f0 ff 00 00 50 4f 53 54 20 2f 57 6f 72 64
0040 50 72 65 73 73 2f 77 70 2d 6c 6f 67 69 6e 2e 70
0050 68 70 20 48 54 54 50 2f 31 2e 31 0d 0a 41 63 63
0060 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 20
0070 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d
0080 6c 2b 78 6d 6c 2c 20 69 6d 61 67 65 2f 6a 78 72
HTTP Traffic.pcapng
Packets: 2392 · Displayed: 1 (0.0%)
Profile: Default
7 items 1 item selected 271 KB State: Shared
6:41 AM
9/16/2025

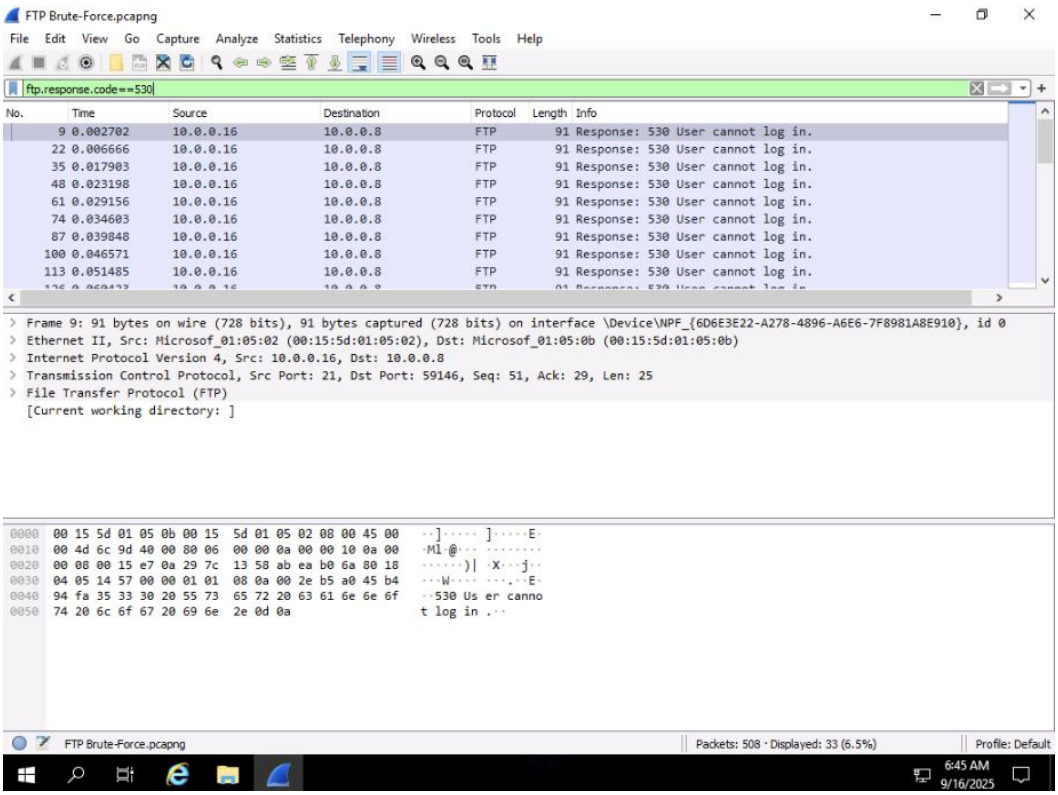

Files for Network Forensics
HTTP Traffic.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request.method==POST
No. Time Source Destination Protocol Length Info
2354 217.535511 10.0.0.10 10.0.0.12 HTTP 701 POST /WordPress/wp-login.ph
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "log" = "admin"
Form item: "pwd" = "qwerty@13"
Form item: "wp-submit" = "Log In"
Form item: "redirect_to" = "http://10.0.0.12/WordPress/wp-admin/"
Form item: "testcookie" = "1"
0000 00 15 5d 00 01 20 00 15 5d 00 01 1f 08 00 45 00
0010 02 af 12 70 40 00 80 06 d1 c3 0a 00 00 0a 0a 00
0020 00 0c c8 56 00 50 d4 bc 36 39 d7 9b 28 94 50 18
0030 04 00 f0 ff 00 00 50 4f 53 54 20 2f 57 6f 72 64
0040 50 72 65 73 73 2f 77 70 2d 6c 6f 67 69 6e 2e 70
0050 68 70 20 48 54 54 50 2f 31 2e 31 0d 0a 41 63 63
0060 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 20
0070 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d
0080 6c 2b 78 6d 6c 2c 20 69 6d 61 67 65 2f 6a 78 72
HTTP Traffic.pcapng
Packets: 2392 · Displayed: 1 (0.0%)
Profile: Default
7 items 1 item selected 271 KB State: Shared
6:41 AM
9/16/2025

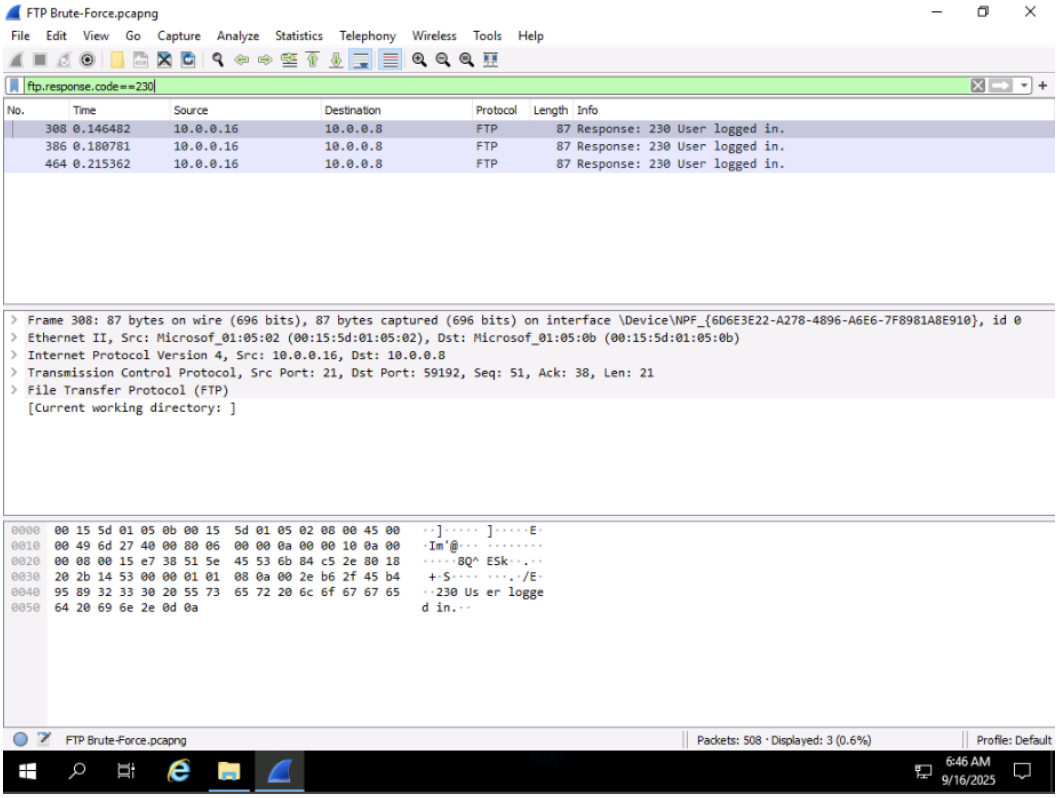

Files for Network Forensics
DNS Remote Shell.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 Intel_78:0c:02 Broadcast ARP 60 Who has 192.168.1.1?
2 0.017208 192.168.1.3 192.168.1.1 DNS 84 Standard query 0x0001
3 0.017234 ThomsonT_eb:46:e7 Intel_78:0c:02 ARP 42 192.168.1.1 is at 00:
4 0.019881 192.168.1.1 192.168.1.3 DNS 112 Standard query respon
5 0.096040 Intel_78:0c:02 Broadcast ARP 82 Who has 192.168.1.1?
6 1.116040 192.168.1.2 140.112.253.189 TCP 96 1026 → 22604 [PSH, AC
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Intel_78:0c:02 (00:0e:35:78:0c:02), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 00 0e 35 78 0c 02 08 06 00 01
0010 08 00 06 04 00 01 00 0e 35 78 0c 02 c0 a8 01 03
0020 00 00 00 00 00 00 c0 a8 01 01 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00
DNS Remote Shell.pcap
Packets: 131 · Displayed: 131 (100.0%)
Profile: Default
7 items
1 item selected 24.4 KB
State: Shared
6:42 AM
9/16/2025

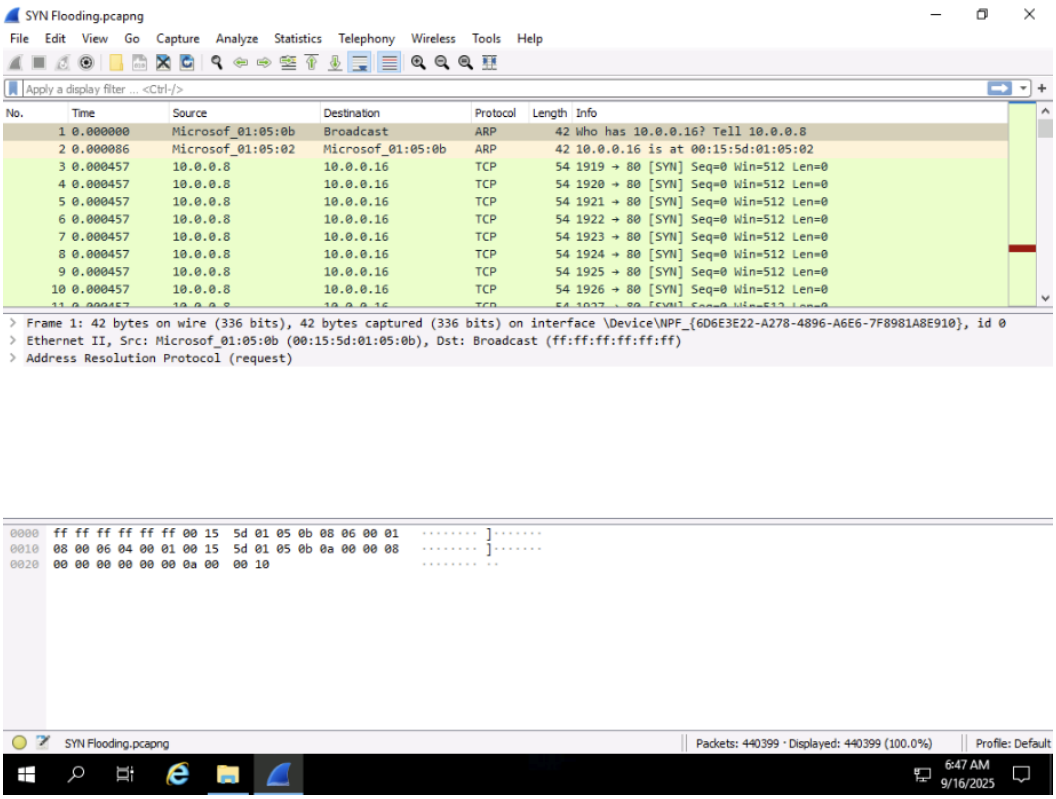

DNS Remote Shell.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port==53
No. Time Source Destination Protocol Length Info
14 25.493358 192.168.1.3 192.168.1.2 TCP 62 1396 → 53 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
16 25.494894 192.168.1.3 192.168.1.2 TCP 102 [TCP Out-Of-Order] 1396 → 53 [SYN] Seq=0 Win=16384 Len=0 MSS
17 25.496543 192.168.1.2 192.168.1.3 TCP 102 53 → 1396 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452 SA
18 25.497466 192.168.1.3 192.168.1.2 TCP 60 1396 → 53 [ACK] Seq=1 Ack=1 Win=17424 Len=0
19 25.497483 192.168.1.2 192.168.1.3 TCP 62 [TCP Out-Of-Order] 53 → 1396 [SYN, ACK] Seq=0 Ack=1 Win=6553
20 25.498909 192.168.1.3 192.168.1.2 TCP 94 [TCP Dup ACK 18#1] 1396 → 53 [ACK] Seq=1 Ack=1 Win=17424 Len
21 25.555046 192.168.1.2 192.168.1.3 TCP 182 53 → 1396 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=88 [TCP segme
22 25.556102 192.168.1.2 192.168.1.3 TCP 142 [TCP Retransmission] 53 → 1396 [PSH, ACK] Seq=1 Ack=1 Win=65
23 25.698332 192.168.1.3 192.168.1.2 TCP 60 1396 → 53 [ACK] Seq=1 Ack=89 Win=17336 Len=0
Frame 14: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
Ethernet II, Src: Intel_78:0c:02 (00:0e:35:78:0c:02), Dst: CompexUs_24:33:32 (00:80:48:24:33:32)
Internet Protocol Version 4, Src: 192.168.1.3, Dst: 192.168.1.2
Transmission Control Protocol, Src Port: 1396, Dst Port: 53, Seq: 0, Len: 0
0000 00 80 48 24 33 32 00 0e 35 78 0c 02 08 00 45 00
0010 00 30 15 0a 40 00 80 06 62 68 c0 a8 01 03 c0 a8
0020 01 02 05 74 00 35 23 c5 33 bf 00 00 00 00 70 02
0030 40 00 62 9c 00 00 02 04 05 b4 01 01 04 02
DNS Remote Shell.pcap
Packets: 131 · Displayed: 24 (18.3%)
Profile: Default
6:43 AM
9/16/2025

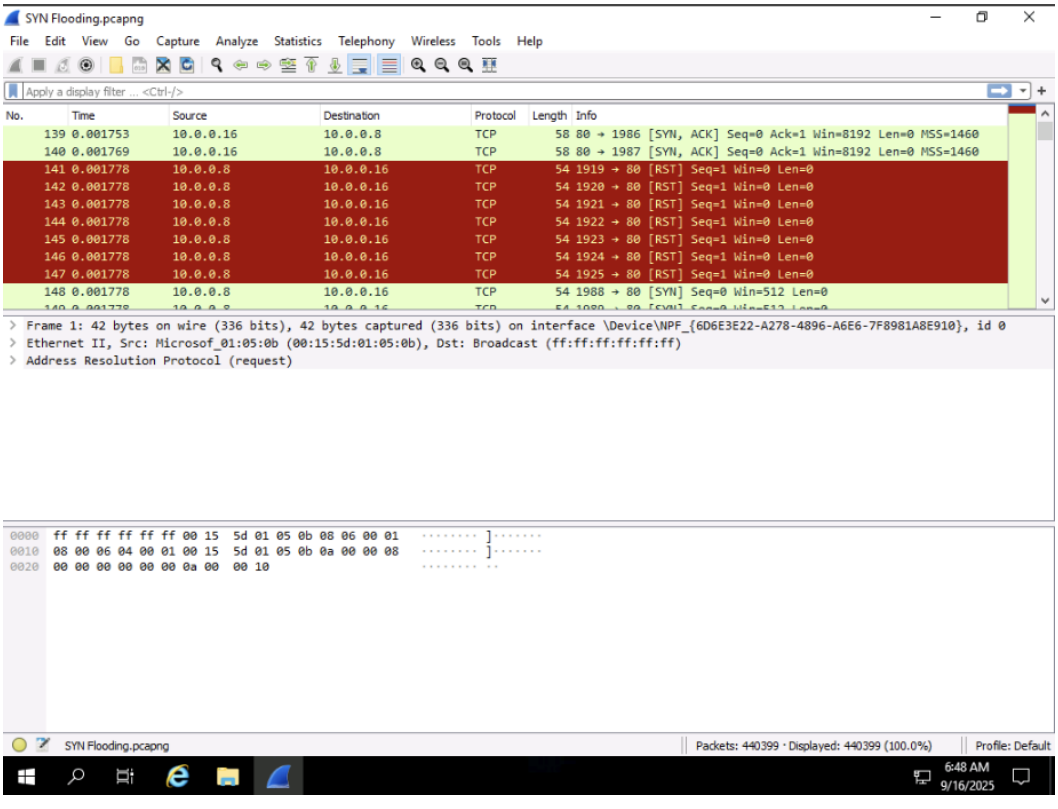

DNS Remote Shell.pcap
Wireshark · Follow TCP Stream (tcp.stream eq 1) · DNS Remote Shell.pcap
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is FF47-80EB
Directory of C:\
01/12/2005 11:59 AM 0 aierrorlog.txt
01/19/2004 09:45 PM 0 AUTOEXEC.BAT
01/19/2004 09:45 PM 0 CONFIG.SYS
06/26/2004 12:12 PM <DIR> Documents and Settings
02/03/2005 11:40 PM <DIR> EasyBoot
02/29/2004 02:51 PM 11,531 installer-debug.txt
12/19/2004 12:50 AM <DIR> mga
12/19/2004 12:51 AM <DIR> mgafold
11/24/2004 07:47 PM <DIR> mnt
10/07/2004 10:01 AM <DIR> movie
06/26/2004 01:03 PM <DIR> My Downloads
01/13/2005 10:52 PM <DIR> Program Files
01/04/2005 10:27 AM <DIR> quarantine
04/19/2004 09:57 PM 7,241 s37g
10/31/2004 08:36 PM 0 s3fs
06/02/2004 08:54 PM 123 systemscandata.txt
08/08/2004 10:48 AM <DIR> Temp
12/12/2004 02:24 PM 94,135,944 temp.mpg
01/13/2005 06:10 PM <DIR> WINDOWS
11/20/2004 09:27 AM <DIR> WUTemp
8 File(s) 94,154,839 bytes
12 Dir(s) 7,145,897,984 bytes free
C:\>exit
2 client pkts, 3 server pkts, 3 turns.
Entire conversation (1309 bytes)
Show and save data as ASCII
Stream 1
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
Profile: Default
6:44 AM
9/16/2025

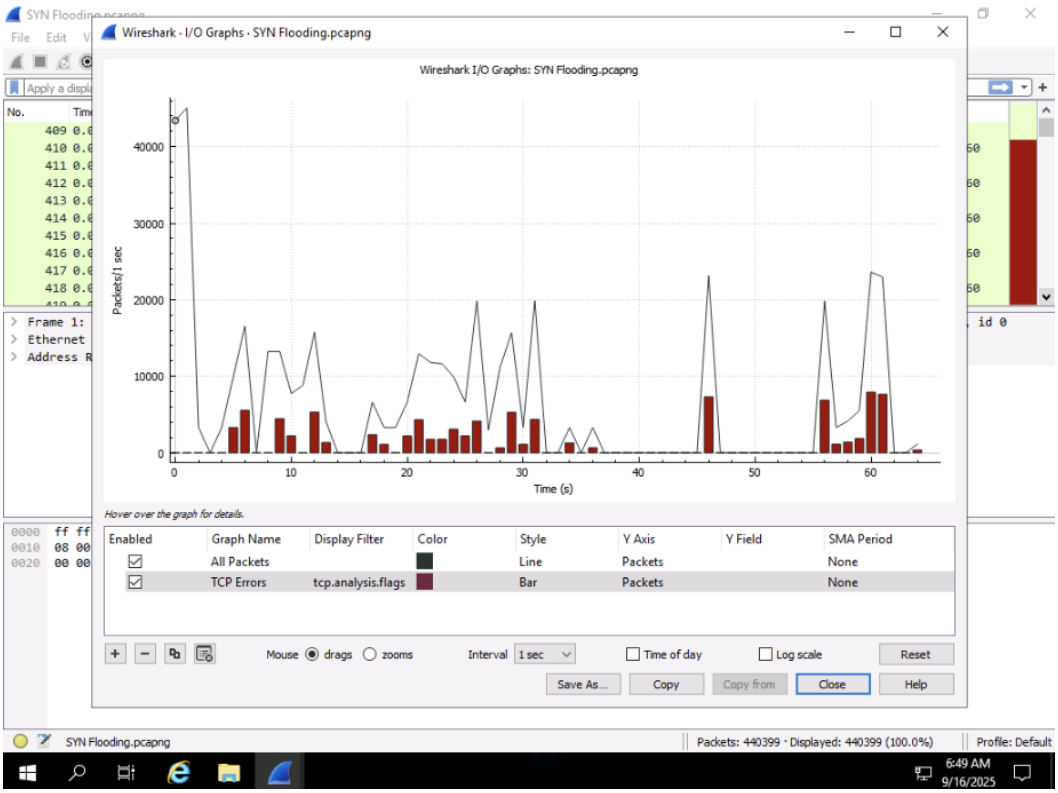

FTP Brute-Force.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 10.0.0.8 10.0.0.16 TCP 74 59146 → 21 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1
2 0.000122 10.0.0.16 10.0.0.8 TCP 74 21 → 59146 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS
3 0.000425 10.0.0.8 10.0.0.16 TCP 66 59146 → 21 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=116946252
4 0.000814 10.0.0.16 10.0.0.8 FTP 93 Response: 220 Microsoft FTP Service
5 0.001104 10.0.0.8 10.0.0.16 TCP 66 59146 → 21 [ACK] Seq=1 Ack=28 Win=29312 Len=0 TSval=11694625
6 0.001747 10.0.0.8 10.0.0.16 FTP 78 Request: USER Admin
7 0.001812 10.0.0.16 10.0.0.8 FTP 89 Response: 331 Password required
8 0.002109 10.0.0.8 10.0.0.16 FTP 82 Request: PASS admin@123
9 0.002702 10.0.0.16 10.0.0.8 FTP 91 Response: 530 User cannot log in.
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{6D6E3E22-A278-4896-A6E6-7F8981A8E910}, id 0
Ethernet II, Src: Microsof_01:05:0b (00:15:5d:01:05:0b), Dst: Microsof_01:05:02 (00:15:5d:01:05:02)
Internet Protocol Version 4, Src: 10.0.0.8, Dst: 10.0.0.16
Transmission Control Protocol, Src Port: 59146, Dst Port: 21, Seq: 0, Len: 0
0000 00 15 5d 01 05 02 00 15 5d 01 05 0b 08 00 45 00
0010 00 3c 88 3f 40 00 40 06 9e 65 0a 00 00 08 0a 00
0020 00 10 e7 0a 00 15 ab ea b0 4d 00 00 00 00 a0 02
0030 72 10 a3 d3 00 00 02 04 05 b4 04 02 08 0a 45 b4
0040 94 f8 00 00 00 00 01 03 03 07
FTP Brute-Force.pcapng
Packets: 508 · Displayed: 508 (100.0%)
Profile: Default
6:45 AM
9/16/2025

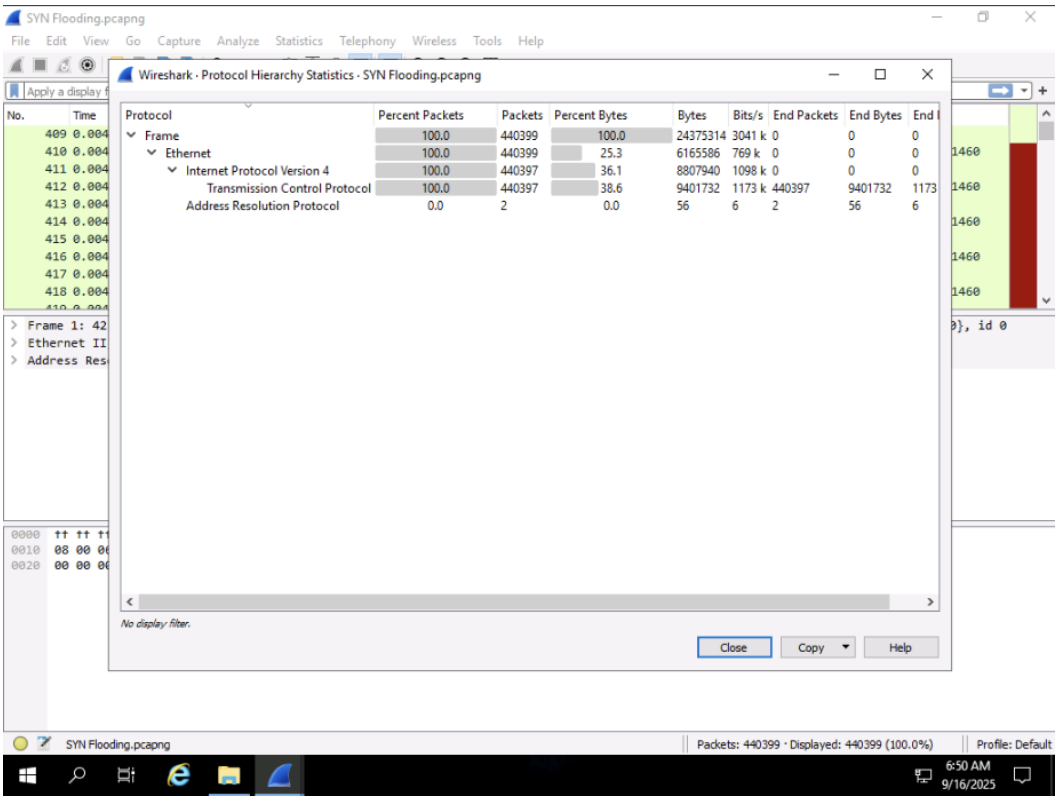

FTP Brute-Force.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ftp.response.code==530
No. Time Source Destination Protocol Length Info
9 0.002702 10.0.0.16 10.0.0.8 FTP 91 Response: 530 User cannot log in.
22 0.006666 10.0.0.16 10.0.0.8 FTP 91 Response: 530 User cannot log in.
35 0.017903 10.0.0.16 10.0.0.8 FTP 91 Response: 530 User cannot log in.
48 0.023198 10.0.0.16 10.0.0.8 FTP 91 Response: 530 User cannot log in.
61 0.029156 10.0.0.16 10.0.0.8 FTP 91 Response: 530 User cannot log in.
74 0.034603 10.0.0.16 10.0.0.8 FTP 91 Response: 530 User cannot log in.
87 0.039848 10.0.0.16 10.0.0.8 FTP 91 Response: 530 User cannot log in.
100 0.046571 10.0.0.16 10.0.0.8 FTP 91 Response: 530 User cannot log in.
113 0.051485 10.0.0.16 10.0.0.8 FTP 91 Response: 530 User cannot log in.
Frame 9: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{6D6E3E22-A278-4896-A6E6-7F8981A8E910}, id 0
Ethernet II, Src: Microsof_01:05:02 (00:15:5d:01:05:02), Dst: Microsof_01:05:0b (00:15:5d:01:05:0b)
Internet Protocol Version 4, Src: 10.0.0.16, Dst: 10.0.0.8
Transmission Control Protocol, Src Port: 21, Dst Port: 59146, Seq: 51, Ack: 29, Len: 25
File Transfer Protocol (FTP)
[Current working directory:]
0000 00 15 5d 01 05 0b 00 15 5d 01 05 02 08 00 45 00
0010 00 4d 6c 9d 40 00 80 06 00 00 0a 00 00 10 0a 00
0020 00 08 00 15 e7 0a 29 7c 13 58 ab ea b0 6a 80 18
0030 04 05 14 57 00 00 01 01 08 0a 00 2e b5 a0 45 b4
0040 94 fa 35 33 30 20 55 73 65 72 20 63 61 6e 6e 6f
0050 74 20 6c 6f 67 20 69 6e 2e 0d 0a
530 User canno
t log in ..
FTP Brute-Force.pcapng
Packets: 508 · Displayed: 33 (6.5%)
Profile: Default
6:45 AM
9/16/2025

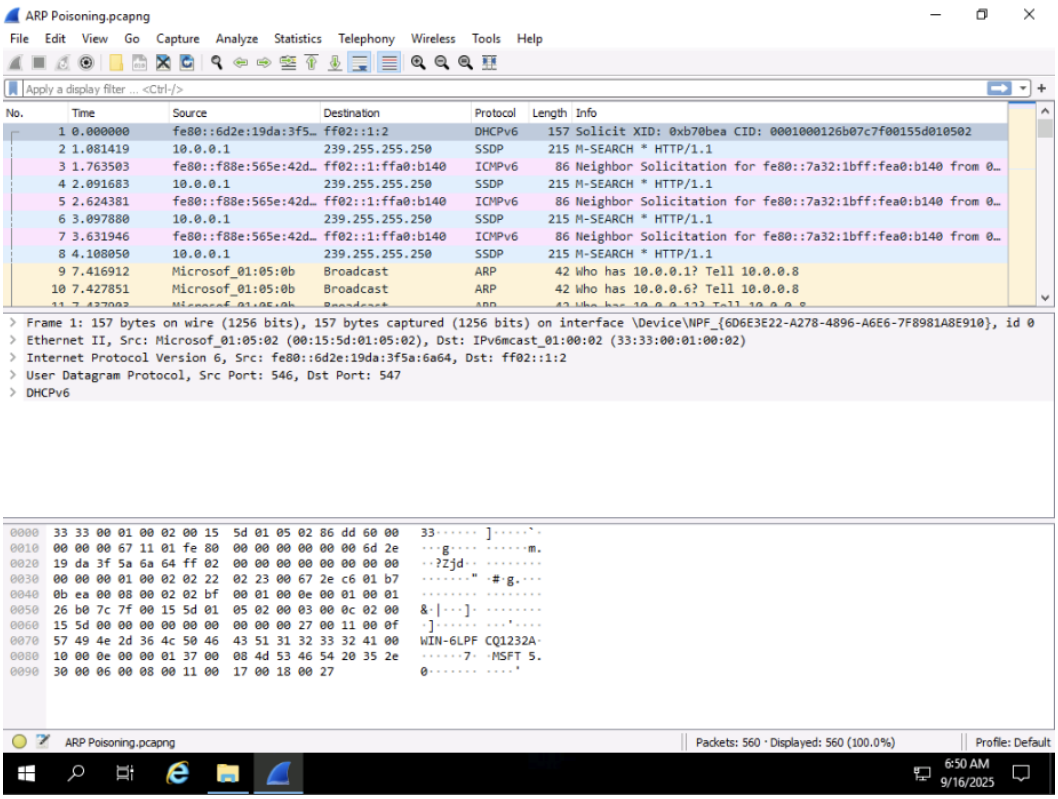

FTP Brute-Force.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ftp.response.code==230
No. Time Source Destination Protocol Length Info
308 0.146482 10.0.0.16 10.0.0.8 FTP 87 Response: 230 User logged in.
386 0.180781 10.0.0.16 10.0.0.8 FTP 87 Response: 230 User logged in.
464 0.215362 10.0.0.16 10.0.0.8 FTP 87 Response: 230 User logged in.
Frame 308: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF_{6D6E3E22-A278-4896-A6E6-7F8981A8E910}, id 0
Ethernet II, Src: Microsof_01:05:02 (00:15:5d:01:05:02), Dst: Microsof_01:05:0b (00:15:5d:01:05:0b)
Internet Protocol Version 4, Src: 10.0.0.16, Dst: 10.0.0.8
Transmission Control Protocol, Src Port: 21, Dst Port: 59192, Seq: 51, Ack: 38, Len: 21
File Transfer Protocol (FTP)
[Current working directory:]
0000 00 15 5d 01 05 0b 00 15 5d 01 05 02 08 00 45 00
0010 00 49 6d 27 40 00 80 06 00 00 0a 00 00 10 0a 00
0020 00 08 00 15 e7 38 51 5e 45 53 6b 84 c5 2e 80 18
0030 20 2b 14 53 00 00 01 01 08 0a 00 2e b6 2f 45 b4
0040 95 89 32 33 30 20 55 73 65 72 20 6c 6f 67 67 65
0050 64 20 69 6e 2e 0d 0a
230 Us er logge
d in..
FTP Brute-Force.pcapng
Packets: 508 · Displayed: 3 (0.6%)
Profile: Default
6:46 AM
9/16/2025

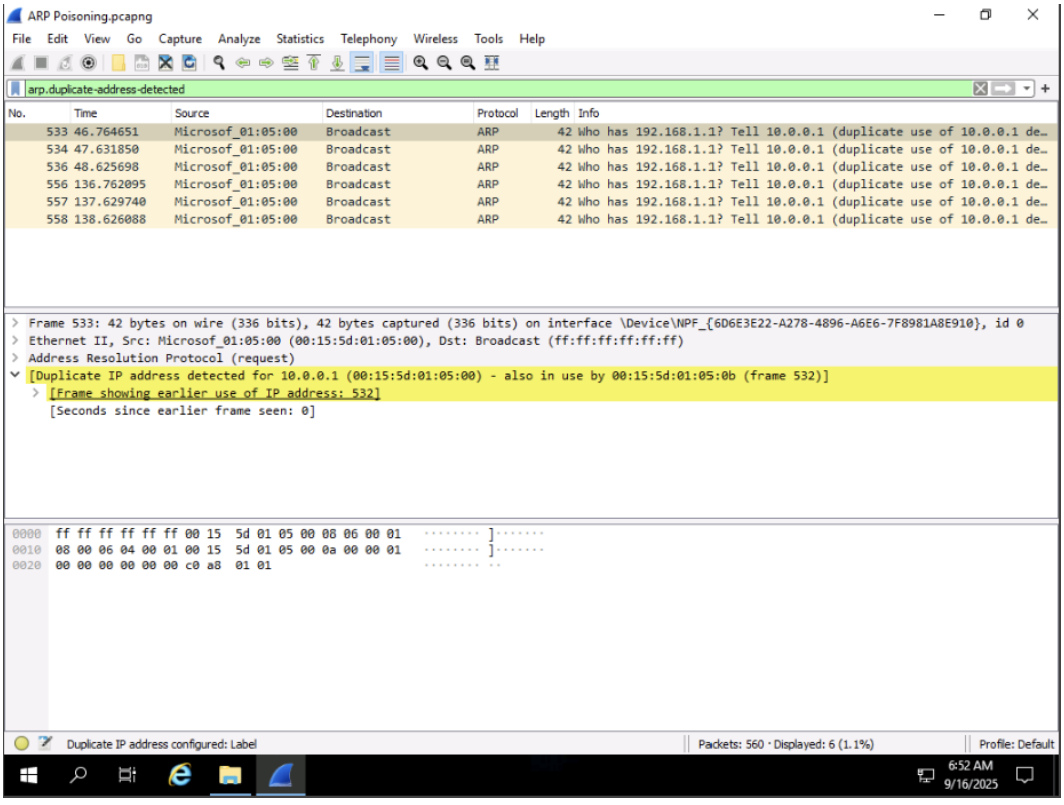

SYN Flooding.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 Microsof_01:05:0b Broadcast ARP 42 Who has 10.0.0.16? Tell 10.0.0.8
2 0.000086 Microsof_01:05:02 Microsof_01:05:0b ARP 42 10.0.0.16 is at 00:15:5d:01:05:02
3 0.000457 10.0.0.8 10.0.0.16 TCP 54 1919 → 80 [SYN] Seq=0 Win=512 Len=0
4 0.000457 10.0.0.8 10.0.0.16 TCP 54 1920 → 80 [SYN] Seq=0 Win=512 Len=0
5 0.000457 10.0.0.8 10.0.0.16 TCP 54 1921 → 80 [SYN] Seq=0 Win=512 Len=0
6 0.000457 10.0.0.8 10.0.0.16 TCP 54 1922 → 80 [SYN] Seq=0 Win=512 Len=0
7 0.000457 10.0.0.8 10.0.0.16 TCP 54 1923 → 80 [SYN] Seq=0 Win=512 Len=0
8 0.000457 10.0.0.8 10.0.0.16 TCP 54 1924 → 80 [SYN] Seq=0 Win=512 Len=0
9 0.000457 10.0.0.8 10.0.0.16 TCP 54 1925 → 80 [SYN] Seq=0 Win=512 Len=0
10 0.000457 10.0.0.8 10.0.0.16 TCP 54 1926 → 80 [SYN] Seq=0 Win=512 Len=0
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{6D6E3E22-A278-4896-A6E6-7F8981A8E910}, id 0
Ethernet II, Src: Microsof_01:05:0b (00:15:5d:01:05:0b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 00 15 5d 01 05 0b 08 06 00 01
0010 08 00 06 04 00 01 00 15 5d 01 05 0b 0a 00 00 08
0020 00 00 00 00 00 00 0a 00 00 10
SYN Flooding.pcapng
Packets: 440399 · Displayed: 440399 (100.0%)
Profile: Default
6:47 AM
9/16/2025


SYN Flooding.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
139 0.001753 10.0.0.16 10.0.0.8 TCP 58 80 → 1986 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
140 0.001769 10.0.0.16 10.0.0.8 TCP 58 80 → 1987 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
141 0.001778 10.0.0.8 10.0.0.16 TCP 54 1919 → 80 [RST] Seq=1 Win=0 Len=0
142 0.001778 10.0.0.8 10.0.0.16 TCP 54 1920 → 80 [RST] Seq=1 Win=0 Len=0
143 0.001778 10.0.0.8 10.0.0.16 TCP 54 1921 → 80 [RST] Seq=1 Win=0 Len=0
144 0.001778 10.0.0.8 10.0.0.16 TCP 54 1922 → 80 [RST] Seq=1 Win=0 Len=0
145 0.001778 10.0.0.8 10.0.0.16 TCP 54 1923 → 80 [RST] Seq=1 Win=0 Len=0
146 0.001778 10.0.0.8 10.0.0.16 TCP 54 1924 → 80 [RST] Seq=1 Win=0 Len=0
147 0.001778 10.0.0.8 10.0.0.16 TCP 54 1925 → 80 [RST] Seq=1 Win=0 Len=0
148 0.001778 10.0.0.8 10.0.0.16 TCP 54 1988 → 80 [SYN] Seq=0 Win=512 Len=0
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{6D6E3E22-A278-4896-A6E6-7F8981A8E910}, id 0
Ethernet II, Src: Microsof_01:05:0b (00:15:5d:01:05:0b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 00 15 5d 01 05 0b 08 06 00 01
0010 08 00 06 04 00 01 00 15 5d 01 05 0b 0a 00 00 08
0020 00 00 00 00 00 00 0a 00 00 10
SYN Flooding.pcapng
Packets: 440399 · Displayed: 440399 (100.0%)
Profile: Default
6:48 AM
9/16/2025


Wireshark · I/O Graphs · SYN Flooding.pcapng
Wireshark I/O Graphs: SYN Flooding.pcapng
Packets/1 sec
Time (s)
Hover over the graph for details.
Enabled
Graph Name
Display Filter
Color
Style
Y Axis
Y Field
SMA Period
All Packets
Line
Packets
None
TCP Errors
tcp.analysis.flags
Bar
Packets
None
Mouse drags zooms
Interval 1 sec
Time of day
Log scale
Reset
Save As...
Copy
Copy from
Close
Help
SYN Flooding.pcapng
Packets: 440399 · Displayed: 440399 (100.0%)
Profile: Default
6:49 AM
9/16/2025


Wireshark · Protocol Hierarchy Statistics · SYN Flooding.pcapng
Protocol
Percent Packets
Packets
Percent Bytes
Bytes
Bits/s
End Packets
End Bytes
Frame 100.0 440399 100.0 24375314 3041 k 0 0
Ethernet 100.0 440399 25.3 6165586 769 k 0 0
Internet Protocol Version 4 100.0 440397 36.1 8807940 1098 k 0 0
Transmission Control Protocol 100.0 440397 38.6 9401732 1173 k 440397 9401732
Address Resolution Protocol 0.0 2 0.0 56 6 2 56
No display filter.
Close
Copy
Help
SYN Flooding.pcapng
Packets: 440399 · Displayed: 440399 (100.0%)
Profile: Default
6:50 AM
9/16/2025


ARP Poisoning.pcapng
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 fe80::6d2e:19da:3f5… ff02::1:2 DHCPv6 157 Solicit XID: 0xb70bea CID: 0001000126b07c7f00155d010502
2 1.081419 10.0.0.1 239.255.255.250 SSDP 215 M-SEARCH * HTTP/1.1
3 1.763503 fe80::f88e:565e:42d… ff02::1:ffa0:b140 ICMPv6 86 Neighbor Solicitation for fe80::7a32:1bff:fea0:b140 from 0…
4 2.091683 10.0.0.1 239.255.255.250 SSDP 215 M-SEARCH * HTTP/1.1
5 2.624381 fe80::f88e:565e:42d… ff02::1:ffa0:b140 ICMPv6 86 Neighbor Solicitation for fe80::7a32:1bff:fea0:b140 from 0…
6 3.097880 10.0.0.1 239.255.255.250 SSDP 215 M-SEARCH * HTTP/1.1
7 3.631946 fe80::f88e:565e:42d… ff02::1:ffa0:b140 ICMPv6 86 Neighbor Solicitation for fe80::7a32:1bff:fea0:b140 from 0…
8 4.108050 10.0.0.1 239.255.255.250 SSDP 215 M-SEARCH * HTTP/1.1
9 7.416912 Microsof_01:05:0b Broadcast ARP 42 Who has 10.0.0.1? Tell 10.0.0.8
10 7.427851 Microsof_01:05:0b Broadcast ARP 42 Who has 10.0.0.6? Tell 10.0.0.8
Frame 1: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits) on interface \Device\NPF_{6D6E3E22-A278-4896-A6E6-7F8981A8E910}, id 0
Ethernet II, Src: Microsof_01:05:02 (00:15:5d:01:05:02), Dst: IPv6mcast_01:00:02 (33:33:00:01:00:02)
Internet Protocol Version 6, Src: fe80::6d2e:19da:3f5a:6a64, Dst: ff02::1:2
User Datagram Protocol, Src Port: 546, Dst Port: 547
DHCPv6
0000 33 33 00 01 00 02 00 15 5d 01 05 02 86 dd 60 00
0010 00 00 00 67 11 01 fe 80 00 00 00 00 00 00 6d 2e
0020 19 da 3f 5a 6a 64 ff 02 00 00 00 00 00 00 00 00
0030 00 00 00 01 00 02 02 22 02 23 00 67 2e c6 01 b7
0040 0b ea 00 08 00 02 02 bf 00 01 00 0e 00 01 00 01
0050 26 b0 7c 7f 00 15 5d 01 05 02 00 03 00 0c 02 00
0060 15 5d 00 00 00 00 00 00 00 00 27 00 11 00 0f
0070 57 49 4e 2d 36 4c 50 46 43 51 31 32 33 32 41 00
0080 10 00 0e 00 00 01 37 00 08 4d 53 46 54 20 35 2e
0090 30 00 06 00 08 00 11 00 17 00 18 00 27
ARP Poisoning.pcapng
Packets: 560 · Displayed: 560 (100.0%)
Profile: Default
6:50 AM
9/16/2025


ARP Poisoning.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp.duplicate-address-detected
No. Time Source Destination Protocol Length Info
533 46.764651 Microsof_01:05:00 Broadcast ARP 42 Who has 192.168.1.1? Tell 10.0.0.1 (duplicate use of 10.0.0.1 de…
534 47.631850 Microsof_01:05:00 Broadcast ARP 42 Who has 192.168.1.1? Tell 10.0.0.1 (duplicate use of 10.0.0.1 de…
536 48.625698 Microsof_01:05:00 Broadcast ARP 42 Who has 192.168.1.1? Tell 10.0.0.1 (duplicate use of 10.0.0.1 de…
556 136.762095 Microsof_01:05:00 Broadcast ARP 42 Who has 192.168.1.1? Tell 10.0.0.1 (duplicate use of 10.0.0.1 de…
557 137.629740 Microsof_01:05:00 Broadcast ARP 42 Who has 192.168.1.1? Tell 10.0.0.1 (duplicate use of 10.0.0.1 de…
558 138.626088 Microsof_01:05:00 Broadcast ARP 42 Who has 192.168.1.1? Tell 10.0.0.1 (duplicate use of 10.0.0.1 de…
Frame 533: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{6D6E3E22-A278-4896-A6E6-7F8981A8E910}, id 0
Ethernet II, Src: Microsof_01:05:00 (00:15:5d:01:05:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
[Duplicate IP address detected for 10.0.0.1 (00:15:5d:01:05:00) - also in use by 00:15:5d:01:05:0b (frame 532)]
[Frame showing earlier use of IP address: 532]
[Seconds since earlier frame seen: 0]
0000 ff ff ff ff ff ff 00 15 5d 01 05 00 08 06 00 01
0010 08 00 06 04 00 01 00 15 5d 01 05 00 0a 00 00 01
0020 00 00 00 00 00 00 c0 a8 01 01
Duplicate IP address configured: Label
Packets: 560 · Displayed: 6 (1.1%)
Profile: Default
6:52 AM
9/16/2025

Module 08: Network Forensics – Lab 1 Summary

In this lab, investigators analyzed network packet captures to identify and investigate potential attacks on a company's network. Using Wireshark, the lab focused on examining incoming and outgoing packets to detect artifacts that indicate malicious activity. The objective was to understand how to inspect network traffic, trace the origins of attacks, and retrieve evidence related to security incidents. This hands-on exercise reinforced skills in recognizing network-based threats and performing forensic analysis on packet-level data.