Wireshark 101 – Network Traffic Analysis Report

TryHackMe Lab

Student Name: Romaissaa Moftah

Course: Cybersecurity / SOC Analysis

Instructor: Eng. Taha Abouelhgag

1. Executive Summary

This report documents the analysis performed during the Wireshark 101 room on TryHackMe. The lab focuses on understanding and analyzing different network protocols using packet capture (PCAP) files.

2. Lab Overview

Wireshark is a powerful packet analysis tool used to capture and inspect network traffic.

3. Tools and Methodology

- Wireshark

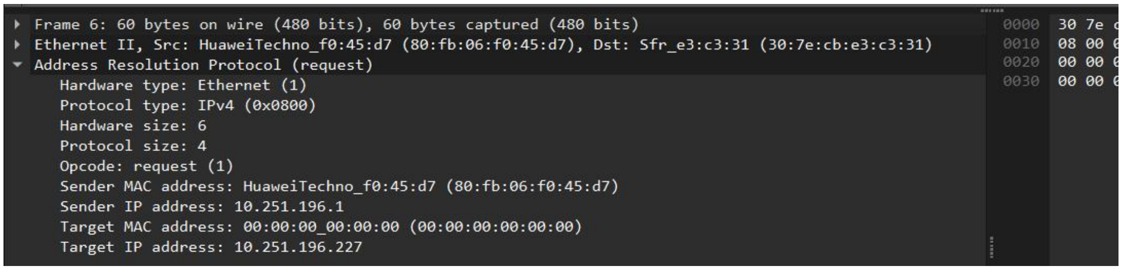
- TryHackMe AttackBox

4. ARP Analysis

What is the Opcode for Packet 6?

address resolution protocol -> opcode ->

Request (1)



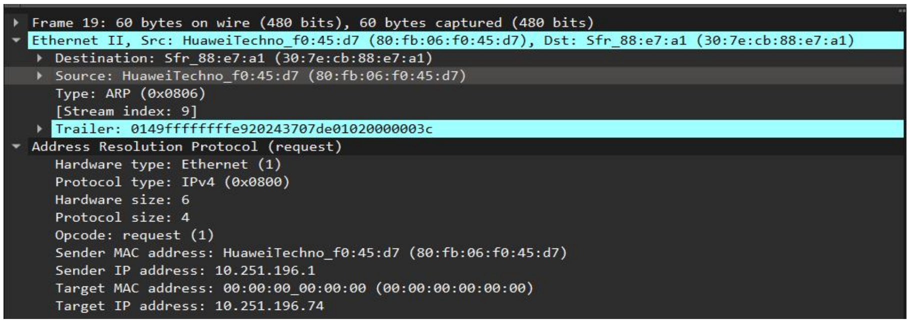
```
▸ Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
▸ Ethernet II, Src: HuaweiTechno_f0:45:d7 (80:fb:06:f0:45:d7), Dst: Sfr_e3:c3:31 (30:7e:cb:e3:c3:31)
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: HuaweiTechno_f0:45:d7 (80:fb:06:f0:45:d7)
    Sender IP address: 10.251.196.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.251.196.227
```

```
0000  30 7e c
0010  08 00 0
0020  00 00 0
0030  00 00 0
```

What is the source MAC Address of Packet 19?

Ethernet ii -> source ->

80:fb:06:f0:45:d7

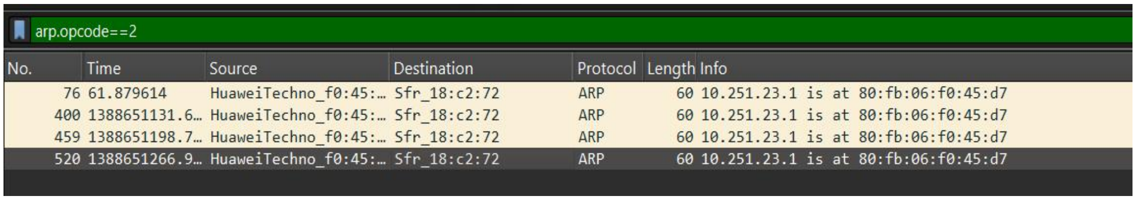


```
▸ Frame 19: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
▾ Ethernet II, Src: HuaweiTechno_f0:45:d7 (80:fb:06:f0:45:d7), Dst: Sfr_88:e7:a1 (30:7e:cb:88:e7:a1)
  ▸ Destination: Sfr_88:e7:a1 (30:7e:cb:88:e7:a1)
  ▸ Source: HuaweiTechno_f0:45:d7 (80:fb:06:f0:45:d7)
    Type: ARP (0x0806)
    [Stream index: 9]
  ▸ Trailer: 0149ffffffffe920243707de01020000003c
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: HuaweiTechno_f0:45:d7 (80:fb:06:f0:45:d7)
    Sender IP address: 10.251.196.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.251.196.74
```

What 4 packets are Reply packets?

using filter -> arp.opcode == 2 -> show the type of ARP (request or reply) ->

76,400,459,520



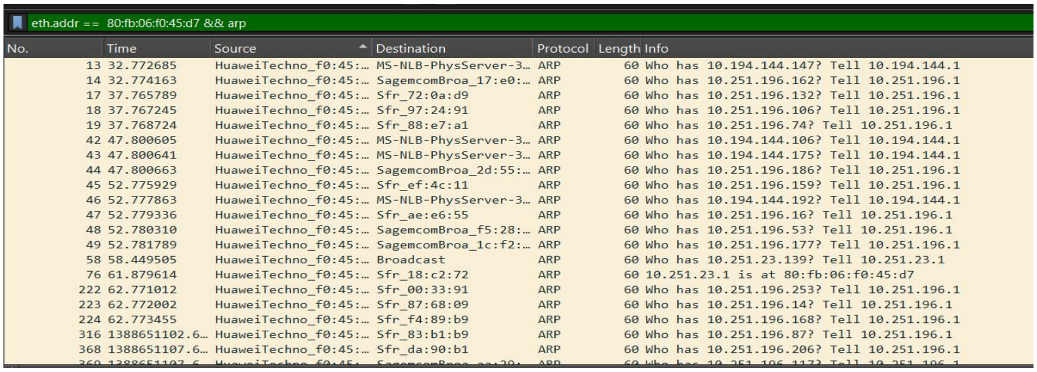
arp.opcode==2

No.	Time	Source	Destination	Protocol	Length	Info
76	61.879614	HuaweiTechno_f0:45:…	Sfr_18:c2:72	ARP	60	10.251.23.1 is at 80:fb:06:f0:45:d7
400	1388651131.6…	HuaweiTechno_f0:45:…	Sfr_18:c2:72	ARP	60	10.251.23.1 is at 80:fb:06:f0:45:d7
459	1388651198.7…	HuaweiTechno_f0:45:…	Sfr_18:c2:72	ARP	60	10.251.23.1 is at 80:fb:06:f0:45:d7
520	1388651266.9…	HuaweiTechno_f0:45:…	Sfr_18:c2:72	ARP	60	10.251.23.1 is at 80:fb:06:f0:45:d7

What IP Address is at 80:fb:06:f0:45:d7?

using filter -> eth.addr == 80:fb:06:f0:45:d7 && arp -> showing all ips used by this MAC address ->

10.251.23.1



eth.addr == 80:fb:06:f0:45:d7 && arp

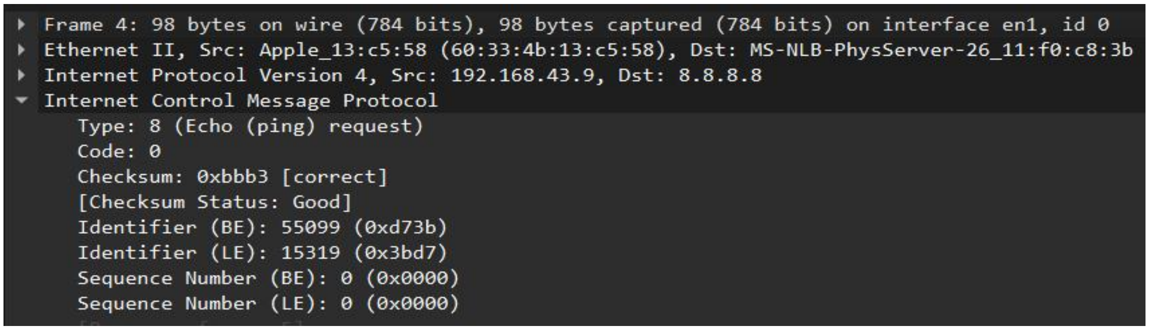
No.	Time	Source	Destination	Protocol	Length	Info
13	32.772685	HuaweiTechno_f0:45:…	MS-NLB-PhysServer-3…	ARP	60	Who has 10.194.144.147? Tell 10.194.144.1
14	32.774163	HuaweiTechno_f0:45:…	SagemcomBroa_17:e0:…	ARP	60	Who has 10.251.196.162? Tell 10.251.196.1
17	37.765789	HuaweiTechno_f0:45:…	Sfr_72:0a:d9	ARP	60	Who has 10.251.196.132? Tell 10.251.196.1
18	37.767245	HuaweiTechno_f0:45:…	Sfr_97:24:91	ARP	60	Who has 10.251.196.106? Tell 10.251.196.1
19	37.768724	HuaweiTechno_f0:45:…	Sfr_88:e7:a1	ARP	60	Who has 10.251.196.74? Tell 10.251.196.1
42	47.800605	HuaweiTechno_f0:45:…	MS-NLB-PhysServer-3…	ARP	60	Who has 10.194.144.106? Tell 10.194.144.1
43	47.800641	HuaweiTechno_f0:45:…	MS-NLB-PhysServer-3…	ARP	60	Who has 10.194.144.175? Tell 10.194.144.1
44	47.800663	HuaweiTechno_f0:45:…	SagemcomBroa_2d:55:…	ARP	60	Who has 10.251.196.186? Tell 10.251.196.1
45	52.775929	HuaweiTechno_f0:45:…	Sfr_ef:4c:11	ARP	60	Who has 10.251.196.159? Tell 10.251.196.1
46	52.777863	HuaweiTechno_f0:45:…	MS-NLB-PhysServer-3…	ARP	60	Who has 10.194.144.192? Tell 10.194.144.1
47	52.779336	HuaweiTechno_f0:45:…	Sfr_ae:e6:55	ARP	60	Who has 10.251.196.16? Tell 10.251.196.1
48	52.780310	HuaweiTechno_f0:45:…	SagemcomBroa_f5:28:…	ARP	60	Who has 10.251.196.53? Tell 10.251.196.1
49	52.781789	HuaweiTechno_f0:45:…	SagemcomBroa_1c:f2:…	ARP	60	Who has 10.251.196.177? Tell 10.251.196.1
58	58.449505	HuaweiTechno_f0:45:…	Broadcast	ARP	60	Who has 10.251.23.139? Tell 10.251.23.1
76	61.879614	HuaweiTechno_f0:45:…	Sfr_18:c2:72	ARP	60	10.251.23.1 is at 80:fb:06:f0:45:d7
222	62.771012	HuaweiTechno_f0:45:…	Sfr_00:33:91	ARP	60	Who has 10.251.196.253? Tell 10.251.196.1
223	62.772002	HuaweiTechno_f0:45:…	Sfr_87:68:09	ARP	60	Who has 10.251.196.14? Tell 10.251.196.1
224	62.773455	HuaweiTechno_f0:45:…	Sfr_f4:89:b9	ARP	60	Who has 10.251.196.168? Tell 10.251.196.1
316	1388651102.6…	HuaweiTechno_f0:45:…	Sfr_83:b1:b9	ARP	60	Who has 10.251.196.87? Tell 10.251.196.1
368	1388651107.6…	HuaweiTechno_f0:45:…	Sfr_da:90:b1	ARP	60	Who has 10.251.196.206? Tell 10.251.196.1

5. ICMP Analysis

What is the type for packet 4?

internet control message -> type ->

8 (request)

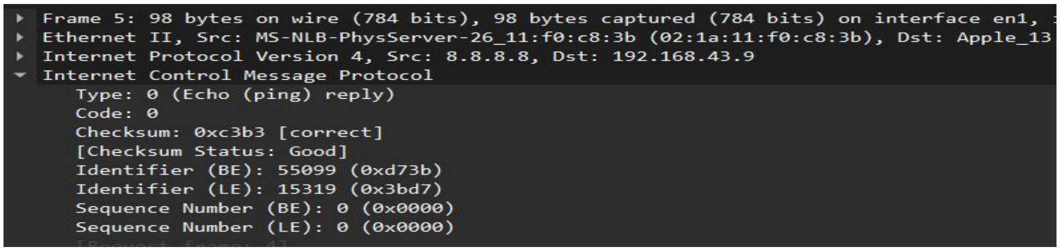


```
▸ Frame 4: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en1, id 0
▸ Ethernet II, Src: Apple_13:c5:58 (60:33:4b:13:c5:58), Dst: MS-NLB-PhysServer-26_11:f0:c8:3b
▸ Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8
▾ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xbbb3 [correct]
    [Checksum Status: Good]
    Identifier (BE): 55099 (0xd73b)
    Identifier (LE): 15319 (0x3bd7)
    Sequence Number (BE): 0 (0x0000)
    Sequence Number (LE): 0 (0x0000)
```

What is the type for packet 5?

internet control message -> type ->

0 (reply)

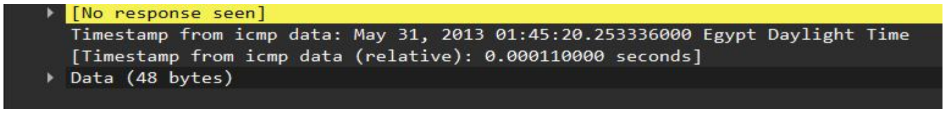


```
▸ Frame 5: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en1,
▸ Ethernet II, Src: MS-NLB-PhysServer-26_11:f0:c8:3b (02:1a:11:f0:c8:3b), Dst: Apple_13
▸ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.43.9
▾ Internet Control Message Protocol
     Type: 0 (Echo (ping) reply)
     Code: 0
     Checksum: 0xc3b3 [correct]
     [Checksum Status: Good]
     Identifier (BE): 55099 (0xd73b)
     Identifier (LE): 15319 (0x3bd7)
     Sequence Number (BE): 0 (0x0000)
     Sequence Number (LE): 0 (0x0000)
```

What is the timestamp for packet 12, only including month day and year?

internet control message -> timestamp ->

May 30, 2013

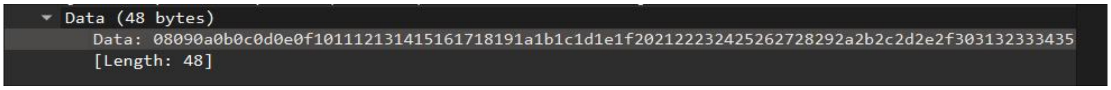


```
  ▸ [No response seen]
    Timestamp from icmp data: May 31, 2013 01:45:20.253336000 Egypt Daylight Time
    [Timestamp from icmp data (relative): 0.000110000 seconds]
  ▸ Data (48 bytes)
```

What is the full data string for packet 18?

internet control message -> data ->

08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637



```
  ▾ Data (48 bytes)
       Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f303132333435
       [Length: 48]
```

6. TCP Overview

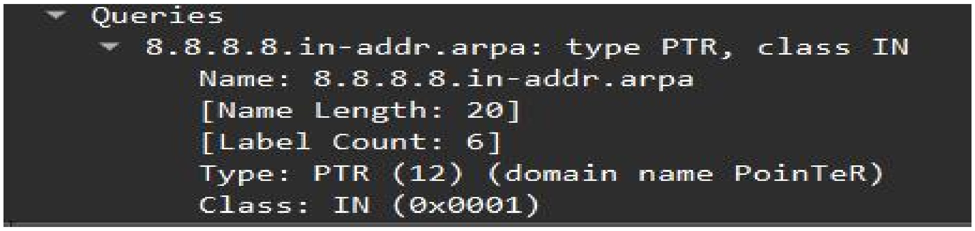
TCP handshake behavior and sequence analysis were reviewed.

7. DNS Analysis

What is being queried in packet 1?

Domain name system -> Queries ->

8.8.8.8.in-addr.arpa

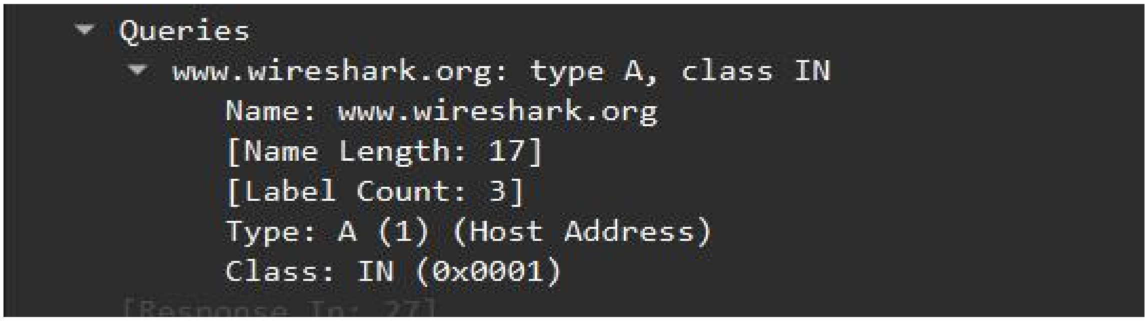


```
▾ Queries
   ▾ 8.8.8.8.in-addr.arpa: type PTR, class IN
        Name: 8.8.8.8.in-addr.arpa
        [Name Length: 20]
        [Label Count: 6]
        Type: PTR (12) (domain name PoinTeR)
        Class: IN (0x0001)
```

What site is being queried in packet 26?

Domain name system -> Queries ->

www.wireshark.org

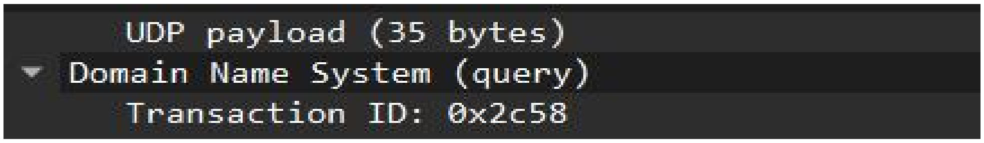


```
▾ Queries
  ▾ www.wireshark.org: type A, class IN
      Name: www.wireshark.org
      [Name Length: 17]
      [Label Count: 3]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
    [Response In: 27]
```

What is the Transaction ID for packet 26?

domain name system (query) -> transaction id ->

0x2c58



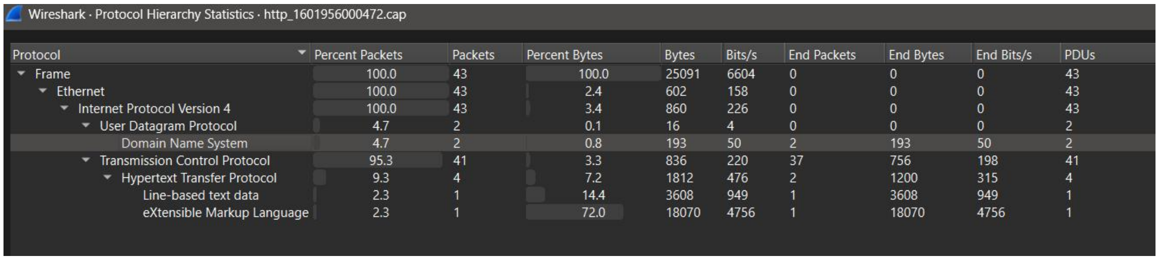
```
    UDP payload (35 bytes)
▾ Domain Name System (query)
    Transaction ID: 0x2c58
```

8. HTTP Analysis

What percent of packets originate from Domain Name System?

statistics -> protocol hierarchy -> domain name system -> percent packet ->

4.7



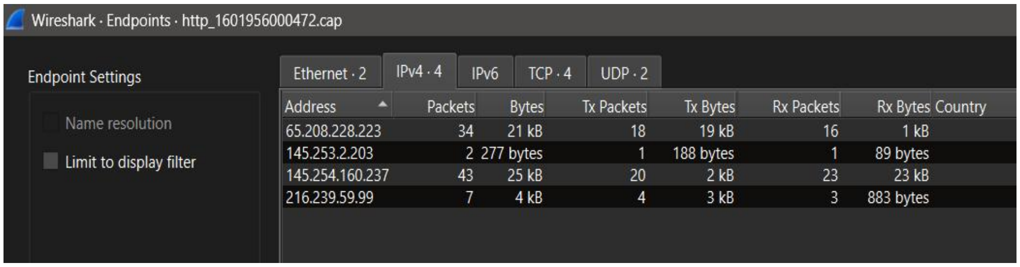
Wireshark · Protocol Hierarchy Statistics · http_1601956000472.cap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
▾ Frame	100.0	43	100.0	25091	6604	0	0	0	43
▾ Ethernet	100.0	43	2.4	602	158	0	0	0	43
▾ Internet Protocol Version 4	100.0	43	3.4	860	226	0	0	0	43
▾ User Datagram Protocol	4.7	2	0.1	16	4	0	0	0	2
Domain Name System	4.7	2	0.8	193	50	2	193	50	2
▾ Transmission Control Protocol	95.3	41	3.3	836	220	37	756	198	41
▾ Hypertext Transfer Protocol	9.3	4	7.2	1812	476	2	1200	315	4
Line-based text data	2.3	1	14.4	3608	949	1	3608	949	1
eXtensible Markup Language	2.3	1	72.0	18070	4756	1	18070	4756	1

What endpoint ends in .237?

statistics -> endpoints -> ipv4 ->

145.254.160.237



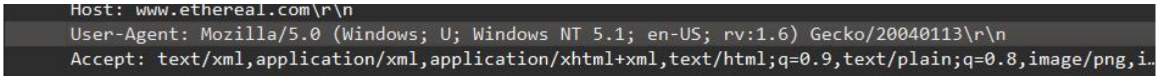
Wireshark · Endpoints · http_1601956000472.cap

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country
65.208.228.223	34	21 kB	18	19 kB	16	1 kB	
145.253.2.203	2	277 bytes	1	188 bytes	1	89 bytes	
145.254.160.237	43	25 kB	20	2 kB	23	23 kB	
216.239.59.99	7	4 kB	4	3 kB	3	883 bytes	

What is the user-agent listed in packet 4?

follow http stream -> user agent ->

Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113\r\n

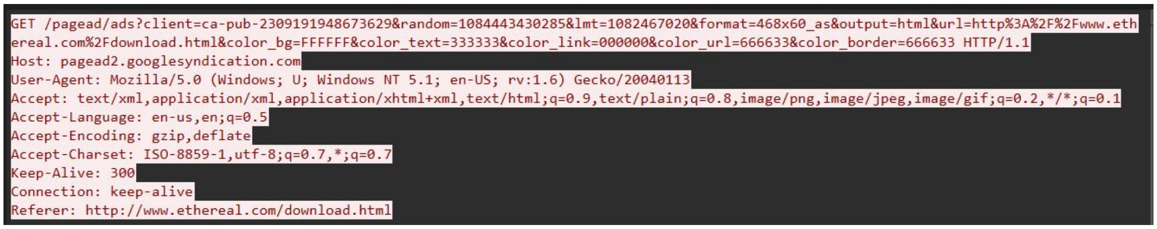


```
        Host: www.ethereal.com\r\n
        User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113\r\n
        Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,i…
```

Looking at the data stream what is the full request URI from packet 18?

rule -> http:// + Host + Request path (GET)

answer -> http://pagead2.googlesyndication.com/pagead/ads?client=ca-pub-2309191948673629&random=1084443430285&lmt=1082467020&format=468x60_as&output=html&url=http://www.ether.eal.com/.download.html&.color_bg=F_FFFFF&color_tex_t=333333&color_li_nk=000000&color_u_rl=666633&color__border=666633

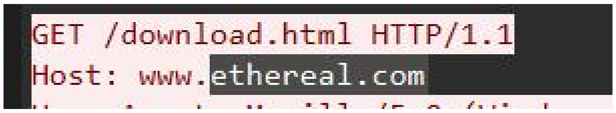


```
GET /pagead/ads?client=ca-pub-2309191948673629&random=1084443430285&lmt=1082467020&format=468x60_as&output=html&url=http%3A%2F%2Fwww.eth
ereal.com%2Fdownload.html&color_bg=FFFFFF&color_text=333333&color_link=000000&color_url=666633&color_border=666633 HTTP/1.1
Host: pagead2.googlesyndication.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=0.2,*/*;q=0.1
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.ethereal.com/download.html
```

What domain name was requested from packet 38?

follow http stream -> domain name ->

www.ethereal.com

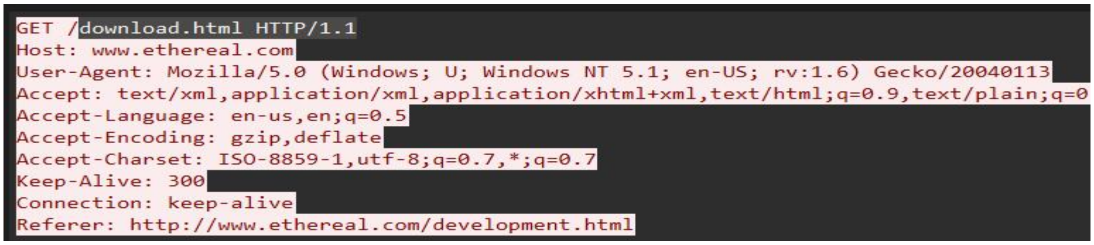


```
GET /download.html HTTP/1.1
Host: www.ethereal.com
```

Looking at the data stream what is the full request URI from packet 38?

rule -> http:// + Host + Request path (GET)

answer -> http://www.ethereal.com/download.html



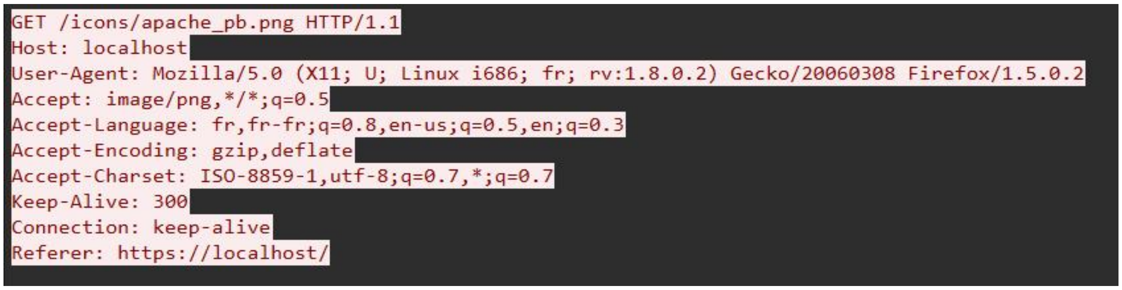
```
GET /download.html HTTP/1.1
Host: www.ethereal.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.ethereal.com/development.html
```

9. HTTPS Analysis

Looking at the data stream what is the full request URI for packet 31?

after decryption by RSA key -> follow tls stream for this packet -> rule -> http:// + Host + Request path (GET) ->

https://localhost/icons/apache_pb.png

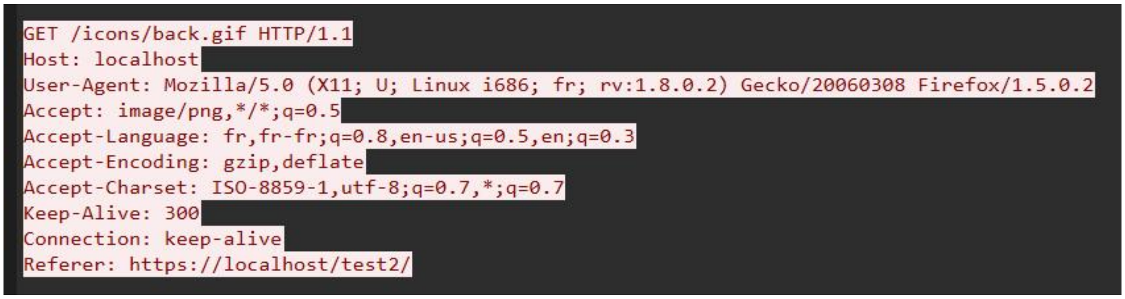


```
GET /icons/apache_pb.png HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; U; Linux i686; fr; rv:1.8.0.2) Gecko/20060308 Firefox/1.5.0.2
Accept: image/png,*/*;q=0.5
Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: https://localhost/
```

Looking at the data stream what is the full request URI for packet 50?

after decryption by RSA key -> follow tls stream for this packet -> rule -> http:// + Host + Request path (GET) ->

https://localhost/icons/back.gif

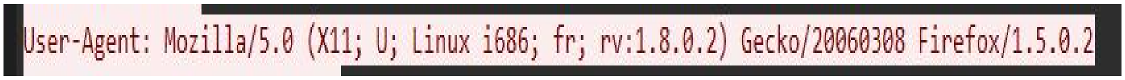


```
GET /icons/back.gif HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; U; Linux i686; fr; rv:1.8.0.2) Gecko/20060308 Firefox/1.5.0.2
Accept: image/png,*/*;q=0.5
Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: https://localhost/test2/
```

What is the User-Agent listed in packet 50?

after decryption by RSA key -> follow tls stream for this packet -> user agent ->

Mozilla/5.0 (X11; U; Linux i686; fr; rv:1.8.0.2) Gecko/20060308 Firefox/1.5.0.2\r\n



```
User-Agent: Mozilla/5.0 (X11; U; Linux i686; fr; rv:1.8.0.2) Gecko/20060308 Firefox/1.5.0.2
```

10. Zerologon PCAP Analysis

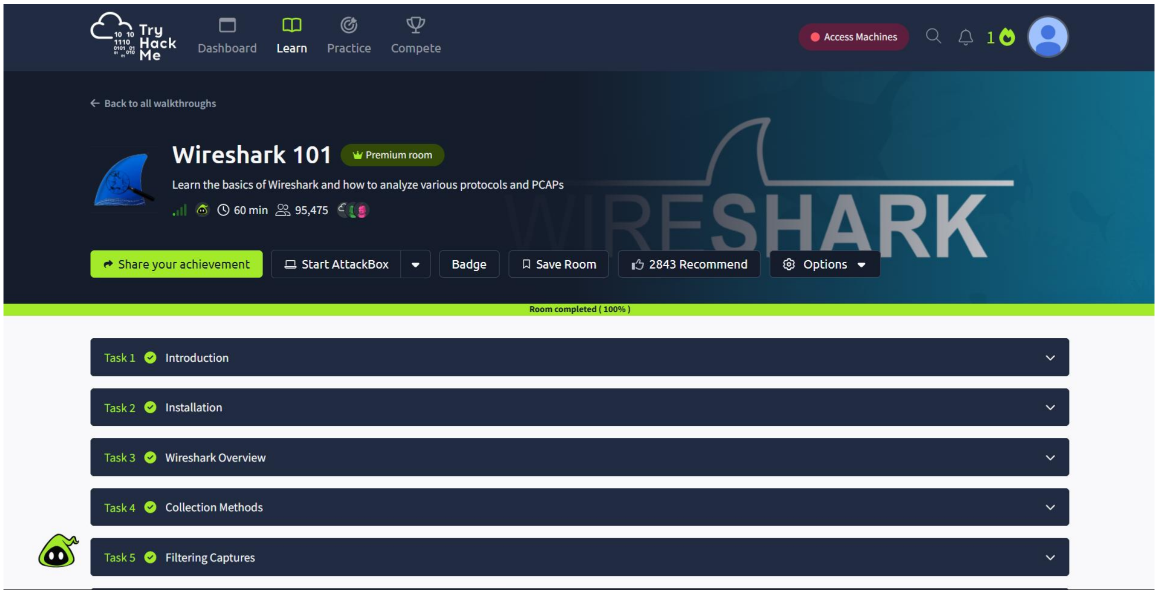
Attacker IP: 192.168.100.128

Victim IP: 192.168.100.6

Exploit evidence via DCERPC and SMB traffic.

11. Conclusion

This lab strengthened packet analysis and network forensics skills.



Wireshark 101

Learn the basics of Wireshark and how to analyze various protocols and PCAPs

Task 1 Introduction

Task 2 Installation

Task 3 Wireshark Overview

Task 4 Collection Methods

Task 5 Filtering Captures