

# CIS294 Course Project

## Background

You are a cybersecurity analyst that are tasked to an Apache web server log file and to analyze pcap file.

An Apache log file will consist HTTP requests made to the web server to the /logs/access.log file. An example is:

```
193.19.118.8 - - [30/Sep/2015:14:47:16 -0400] "GET /admin/ HTTP/1.0" 404  
162 "-" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:30.N)  
Gecko/20110302 Firefox/30.0"
```

Cybersecurity professionals often use Wireshark to break down packets of data being transferred across different networks. The user can search and filter for specific packets of data and analyze how they are transferred across their network. These packets can be used for analysis on a real-time or offline basis.

## Required Equipment

- Kali Linux VM or online <https://bellard.org/jslinux/>
- Wireshark installed on Kali Linux, Windows 10 VM, or own PC

## Instructions

- Download the CIS294CP Files.zip from iCampus Course Project to your PC Desktop.
- Unzip the file. There will be two files.
- The CIS294CP.txt is for Part 1 Log Analysis.
- The CIS294CP.pcapng file is for Part 2 PCAP Analysis.

## Part 1 Log Analysis

Analyze the log file using terminal. Each correct answer/screenshot is worth 2.5 points each.

1. How many entries in the log?

10,000

2. Insert a screenshot showing the result.

```
(kali@kali)-[~/Desktop]
└─$ cat -n CIS294CP.txt
9998 66.249.73.135 - - [20/01/2020:12:00:00]
9999 180.76.6.56 - - [20/01/2020:12:00:00]
10000 46.105.14.53 - - [20/01/2020:12:00:00]
```

3. How many different IP addresses reached the server?

1,753

4. Insert a screenshot showing the result.

```
(kali@kali)-[~/Desktop]
└─$ awk '{print $1}' CIS294CP.txt | sort | uniq -c | sort -rn | wc -l
1753
```

5. Which IP address reached the server the most?

66.249.73.135

6. Insert a screenshot showing the result.

```
(kali@kali)-[~/Desktop]
└─$ awk '{print $1}' CIS294CP.txt | sort | uniq -c | sort -rn | head
482 66.249.73.135
364 46.105.14.53
357 130.237.218.86
273 75.97.9.59
113 50.16.19.13
102 209.85.238.199
99 68.180.224.225
84 100.43.83.137
83 208.115.111.72
82 198.46.149.143
```

7. How many times did the IP address with the most entries reached the server?

482 times

8. Insert a screenshot showing the result.

```
(kali@kali)-[~/Desktop]
└─$ grep '66.249.73.135' CIS294CP.txt | wc -l
482
```

9. How many HTTP 200 status code are listed?

9126

10. Insert a screenshot showing the result.

```
(kali@kali)-[~/Desktop]
└─$ grep -w 'HTTP/1.*" 200' CIS294CP.txt | wc -l
9126
```

11. How many HTTP page not found code are in the log?

213

12. Insert a screenshot showing the result.

```
(kali@kali)-[~/Desktop]
└─$ grep -w 'HTTP/1.*" 404' CIS294CP.txt | wc -l
213
```

13. Which IP address was accessing robots.txt files the most times?

208.115.111.72

14. Insert a screenshot showing the result.

```
(kali@kali)-[~/Desktop]
└─$ grep "robots.txt" CIS294CP.txt | awk '{print $1}' | sort | uniq -c | sort -rn
10 208.115.111.72
8 208.115.113.88
7 144.76.95.39
```

15. What was the most common article that was retrieved?

favicon.ico

16. Insert a screenshot showing the result.

```
(kali@kali)-[~/Desktop]
└─$ awk '{print $7}' CIS294CP.txt | sort | uniq -c | sort -rn | head
807 /favicon.ico
546 /style2.css
538 /reset.css
533 /images/jordan-80.png
516 /images/web/2009/banner.png
488 /blog/tags/puppet?flav=rss20
224 /projects/xdotool/
217 /?flav=rss20
197 /
180 /robots.txt
```

### 17.What is the second most common iPhone iOS version used?

**iPhone iOS 7.0.4**

### 18.Insert a screenshot showing the result.

```
-(kali@kali)-[~/Desktop]
└─$ grep "iPhone" CIS294CP.txt | awk '{print $15, $16, $17}' | sort | uniq -c | sort -rn
274 iPhone OS 6 0
59 iPhone OS 7_0_4
6 Mini/7.0.3/34.1244; U; de)
5 iPhone OS 5_1_1
```

### 19.How long did the log file last? In seconds

**298,859 seconds**

### 20.Insert a screenshot showing the result.

```
-(kali@kali)-[~/Desktop]
└─$ awk '{print $4, $5}' CIS294CP.txt | sort | uniq -c | head
2 [17/May/2015:10:05:00 +0000]
3 [17/May/2015:10:05:03 +0000]
1 [17/May/2015:10:05:04 +0000]
1 [17/May/2015:10:05:06 +0000]
1 [17/May/2015:10:05:07 +0000]
1 [17/May/2015:10:05:08 +0000]
1 [17/May/2015:10:05:10 +0000]
2 [17/May/2015:10:05:11 +0000]
1 [17/May/2015:10:05:12 +0000]
1 [17/May/2015:10:05:13 +0000]

-(kali@kali)-[~/Desktop]
└─$ awk '{print $4, $5}' CIS294CP.txt | sort | uniq -c | tail
3 [20/May/2015:21:05:48 +0000]
2 [20/May/2015:21:05:50 +0000]
1 [20/May/2015:21:05:52 +0000]
3 [20/May/2015:21:05:53 +0000]
1 [20/May/2015:21:05:54 +0000]
3 [20/May/2015:21:05:55 +0000]
1 [20/May/2015:21:05:56 +0000]
2 [20/May/2015:21:05:57 +0000]
1 [20/May/2015:21:05:58 +0000]
2 [20/May/2015:21:05:59 +0000]
```

From: Sunday, May 17, 2015 at 10:05:00 am  
To: Wednesday, May 20, 2015 at 9:05:59 pm

#### Result: 3 days, 11 hours, 0 minutes and 59 seconds

The duration is 3 days, 11 hours, 0 minutes and 59 seconds  
Or 3 days, 11 hours, 59 seconds

#### Alternative time units

3 days, 11 hours, 0 minutes and 59 seconds can be converted to one of these units:

- 298,859 seconds
- 4980 minutes (rounded down)
- 83 hours
- 3 days (rounded down)
- 0.95% of 2015

## Part 1 Log Analysis Extra Credit

For extra ten points (5 points for each correct submission), answer and submit a screenshot for the following

### 1. Which IP address and on what date had the most entries?

**75.97.9.59 had the most entries(197) in a single day which occurred on Monday, May 18, 2015 and was the 4th most reoccurring IP in the entire log with 273 total entries.**

**130.237.218.86 had the second most entries(183) in a single day on Wednesday, May 20, 2015 and was the 3rd most reoccurring IP total(357) in the entire log.**

**66.249.73.135 took third place for most entries in a single day with 180 entries on Monday, May 18, 2015 and reached the server 482 times total within the 3 days, 11 hours, and 59 seconds of the(entire) log file.**

### 2. Insert a screenshot showing the result.

```
(kali@kali)-[~/Desktop]
└─$ grep "17/May/2015" CIS294CP.txt | awk '{print $1}' | sort | uniq -c | sort -rn | head
 78 66.249.73.135
 58 65.55.213.73
 58 46.105.14.53
 52 50.139.66.106
 41 144.76.194.187
 38 67.61.65.249
 37 111.199.235.239
 34 122.166.142.108
 27 65.55.213.74
 26 99.252.100.83

(kali@kali)-[~/Desktop]
└─$ grep "18/May/2015" CIS294CP.txt | awk '{print $1}' | sort | uniq -c | sort -rn | head
197 75.97.9.59
180 66.249.73.135
135 46.105.14.53
 50 86.76.247.183
 42 50.16.19.13
 41 199.168.96.66
 40 210.13.83.18
 40 209.85.238.199
 33 80.108.25.232
 33 59.163.27.11

(kali@kali)-[~/Desktop]
└─$ grep "19/May/2015" CIS294CP.txt | awk '{print $1}' | sort | uniq -c | sort -rn | head
174 130.237.218.86
104 66.249.73.135
 87 46.105.14.53
 67 75.97.9.59
 50 14.160.65.22
 43 93.17.51.134
 39 183.179.22.186
 39 115.112.233.75
 38 24.11.96.184
 35 193.244.33.47

(kali@kali)-[~/Desktop]
└─$ grep "20/May/2015" CIS294CP.txt | awk '{print $1}' | sort | uniq -c | sort -rn | head
183 130.237.218.86
120 66.249.73.135
 84 46.105.14.53
 37 89.107.177.18
 37 184.66.149.103
 34 204.62.56.3
 34 200.31.173.106
 33 38.99.236.50
 32 68.180.224.225
```



## Part 2 Pcap Analysis

Use the **CIS294CP.pcapng** file from the **CIS294CP Files** folder on your Windows 10 VM or the host PC that has Wireshark installed. Analyze the pcapng file. Each correct answer/screenshot is worth 2.5 points each.

1. How many ping requests were sent in the capture?

6

2. Insert a screenshot showing the result in Wireshark.

No.	Time	Source	Destination	Protocol	Length	Info
4	12.196170025	10.0.2.22	10.0.2.15	ICMP	98	Echo (ping) request id=0x0841, seq=1/256, ttl=64 (reply in 7)
7	12.196737607	10.0.2.15	10.0.2.22	ICMP	98	Echo (ping) reply id=0x0841, seq=1/256, ttl=128 (request in 4)
8	13.209235817	10.0.2.22	10.0.2.15	ICMP	98	Echo (ping) request id=0x0841, seq=2/512, ttl=64 (reply in 9)
9	13.209557789	10.0.2.15	10.0.2.22	ICMP	98	Echo (ping) reply id=0x0841, seq=2/512, ttl=128 (request in 8)
10	14.233249758	10.0.2.22	10.0.2.15	ICMP	98	Echo (ping) request id=0x0841, seq=3/768, ttl=64 (reply in 11)
11	14.233768129	10.0.2.15	10.0.2.22	ICMP	98	Echo (ping) reply id=0x0841, seq=3/768, ttl=128 (request in 10)
12	15.248605631	10.0.2.22	10.0.2.15	ICMP	98	Echo (ping) request id=0x0841, seq=4/1024, ttl=64 (reply in 13)
13	15.248936891	10.0.2.15	10.0.2.22	ICMP	98	Echo (ping) reply id=0x0841, seq=4/1024, ttl=128 (request in 12)
14	16.273077068	10.0.2.22	10.0.2.15	ICMP	98	Echo (ping) request id=0x0841, seq=5/1280, ttl=64 (reply in 15)
15	16.273407477	10.0.2.15	10.0.2.22	ICMP	98	Echo (ping) reply id=0x0841, seq=5/1280, ttl=128 (request in 14)
17	17.296626187	10.0.2.22	10.0.2.15	ICMP	98	Echo (ping) request id=0x0841, seq=6/1536, ttl=64 (reply in 19)
19	17.296904299	10.0.2.15	10.0.2.22	ICMP	98	Echo (ping) reply id=0x0841, seq=6/1536, ttl=128 (request in 17)

3. From what IP address did the ping request originate from?

10.0.2.22

4. Insert a screenshot showing the result in Wireshark.

No.	Time	Source	Destination	Protocol	Length	Info
4	12.196170025	10.0.2.22	10.0.2.15	ICMP	98	Echo (ping) request id=0x0841, seq=1/256, ttl=64 (reply in 7)
7	12.196737607	10.0.2.15	10.0.2.22	ICMP	98	Echo (ping) reply id=0x0841, seq=1/256, ttl=128 (request in 4)
8	13.209235817	10.0.2.22	10.0.2.15	ICMP	98	Echo (ping) request id=0x0841, seq=2/512, ttl=64 (reply in 9)
9	13.209557789	10.0.2.15	10.0.2.22	ICMP	98	Echo (ping) reply id=0x0841, seq=2/512, ttl=128 (request in 8)
10	14.233249758	10.0.2.22	10.0.2.15	ICMP	98	Echo (ping) request id=0x0841, seq=3/768, ttl=64 (reply in 11)
11	14.233768129	10.0.2.15	10.0.2.22	ICMP	98	Echo (ping) reply id=0x0841, seq=3/768, ttl=128 (request in 10)
12	15.248605631	10.0.2.22	10.0.2.15	ICMP	98	Echo (ping) request id=0x0841, seq=4/1024, ttl=64 (reply in 13)
13	15.248936891	10.0.2.15	10.0.2.22	ICMP	98	Echo (ping) reply id=0x0841, seq=4/1024, ttl=128 (request in 12)
14	16.273077068	10.0.2.22	10.0.2.15	ICMP	98	Echo (ping) request id=0x0841, seq=5/1280, ttl=64 (reply in 15)
15	16.273407477	10.0.2.15	10.0.2.22	ICMP	98	Echo (ping) reply id=0x0841, seq=5/1280, ttl=128 (request in 14)
17	17.296626187	10.0.2.22	10.0.2.15	ICMP	98	Echo (ping) request id=0x0841, seq=6/1536, ttl=64 (reply in 19)
19	17.296904299	10.0.2.15	10.0.2.22	ICMP	98	Echo (ping) reply id=0x0841, seq=6/1536, ttl=128 (request in 17)

5. What is the IP address of the device associated with 08:00:27:4b:e3:60?

10.0.2.15

6. Insert a screenshot showing the result in Wireshark.

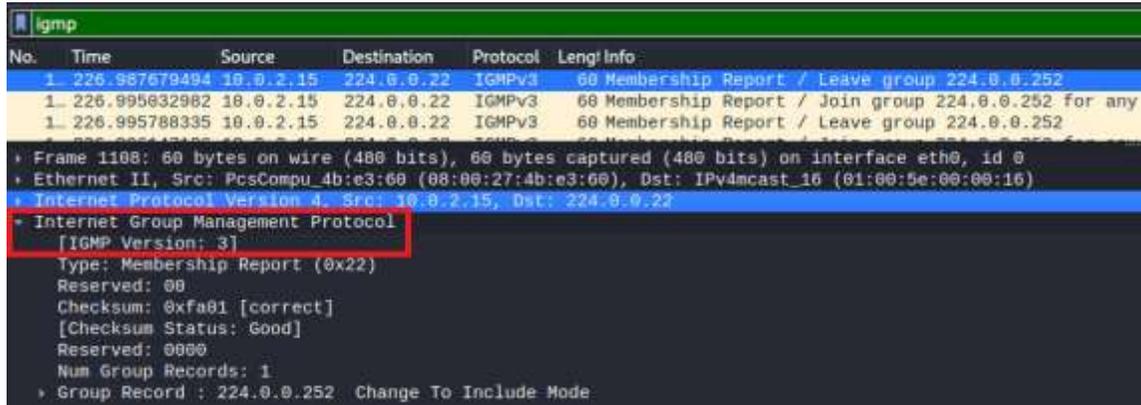
No.	Time	Source	Destination	Protocol	Length	Info
4	12.196170025	10.0.2.22	10.0.2.15	ICMP	98	Echo (ping) request id=0x0841, seq=1/256, ttl=64 (reply in 7)
7	12.196737607	10.0.2.15	10.0.2.22	ICMP	98	Echo (ping) reply id=0x0841, seq=1/256, ttl=128 (request in 4)

Frame 4: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0, id 0  
 Ethernet II, Src: PcsCompu\_7c:8e:8e (08:00:27:7c:8e:8e), Dst: PcsCompu\_4b:e3:60 (08:00:27:4b:e3:60)  
 Destination: PcsCompu\_4b:e3:60 (08:00:27:4b:e3:60)  
 Address: PcsCompu\_4b:e3:60 (08:00:27:4b:e3:60)  
 .. ... = LG bit: Globally unique address (factory default)  
 .. ... = IG bit: Individual address (unicast)  
 Source: PcsCompu\_7c:8e:8e (08:00:27:7c:8e:8e)  
 Type: IPv4 (0x0800)  
 Internet Protocol Version 4, Src: 10.0.2.22, Dst: 10.0.2.15  
 Internet Control Message Protocol

7. What version of Internet Group Management Protocol is in use?

### IGMP Version 3

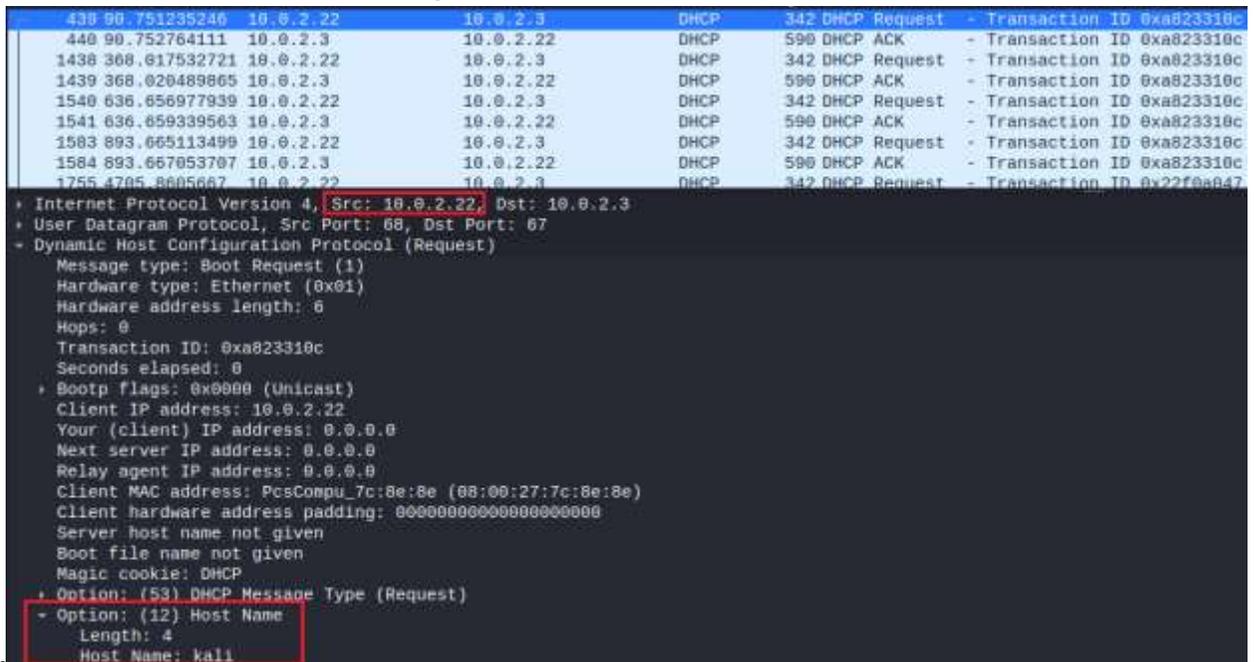
8. Insert a screenshot showing the result in Wireshark.



9. What is the name of the host located at 10.0.2.22?

kali

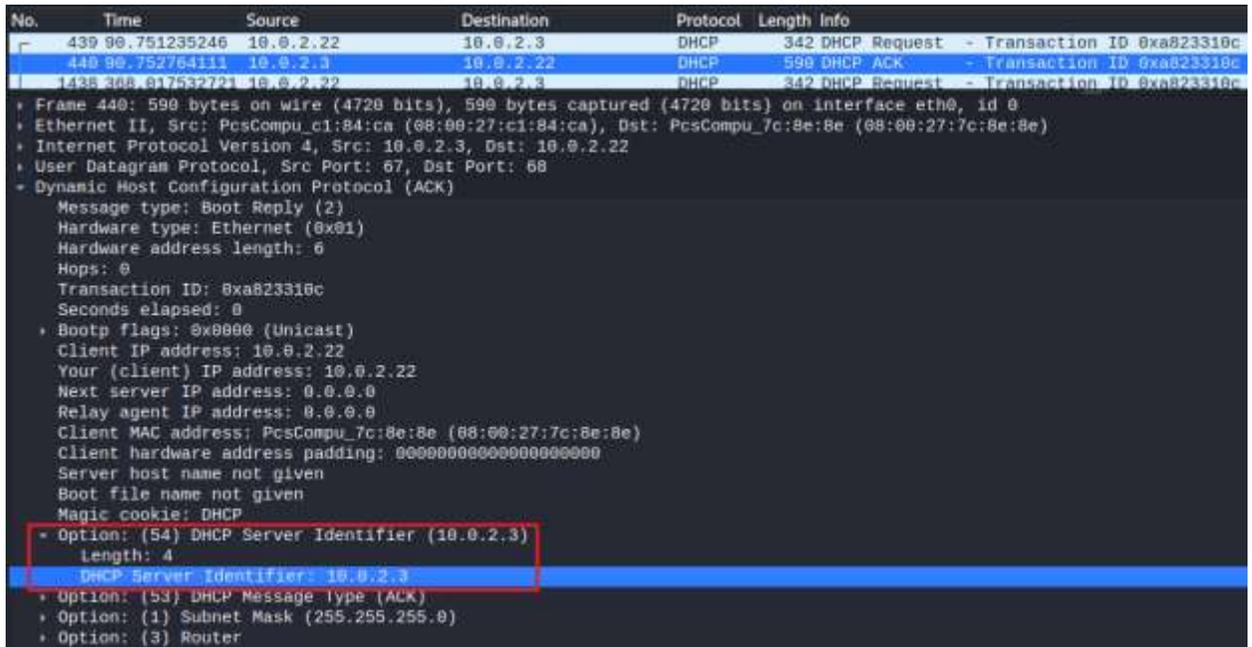
10. Insert a screenshot showing the result in Wireshark.



11. What is the IP address of the DHCP server?

10.0.2.3

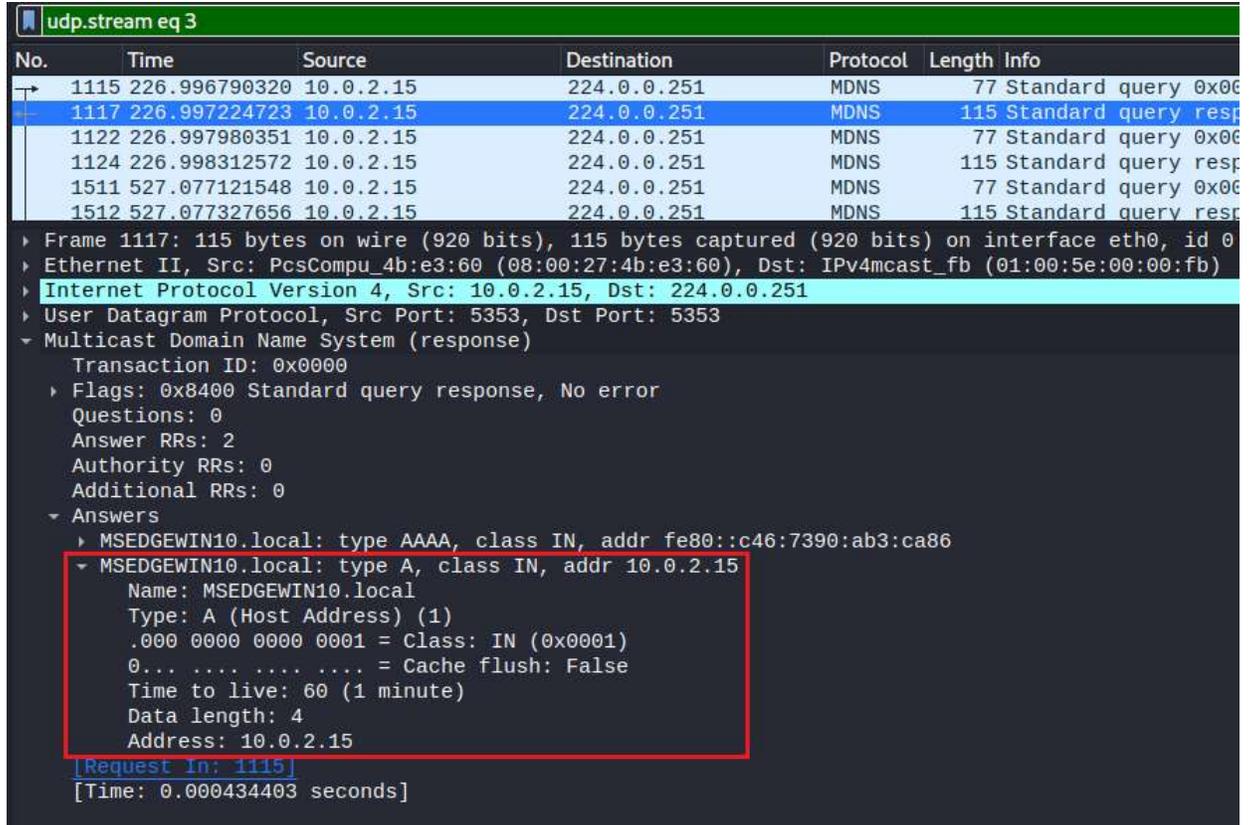
### 12. Insert a screenshot showing the result in Wireshark.



### 13. What is the name of the host located at 10.0.2.15?

MSEEDGEWIN10

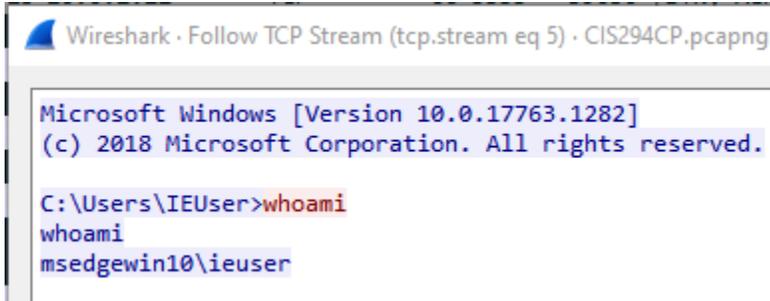
### 14. Insert a screenshot showing the result in Wireshark.



15. What was the first command run by the attacker?

whoami

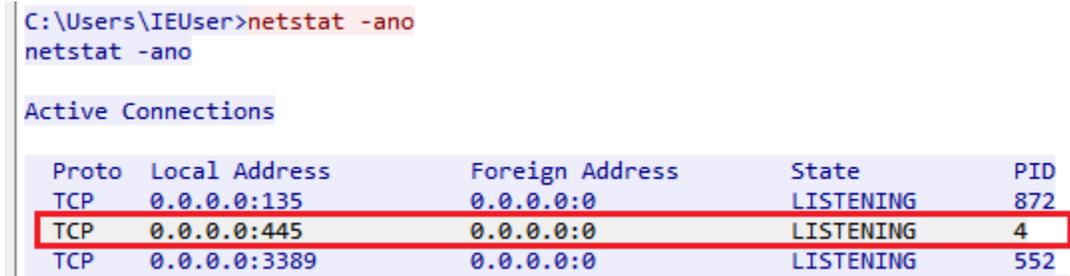
16. Insert a screenshot showing the result in Wireshark.



17. What was the process ID of the SMB session?

4

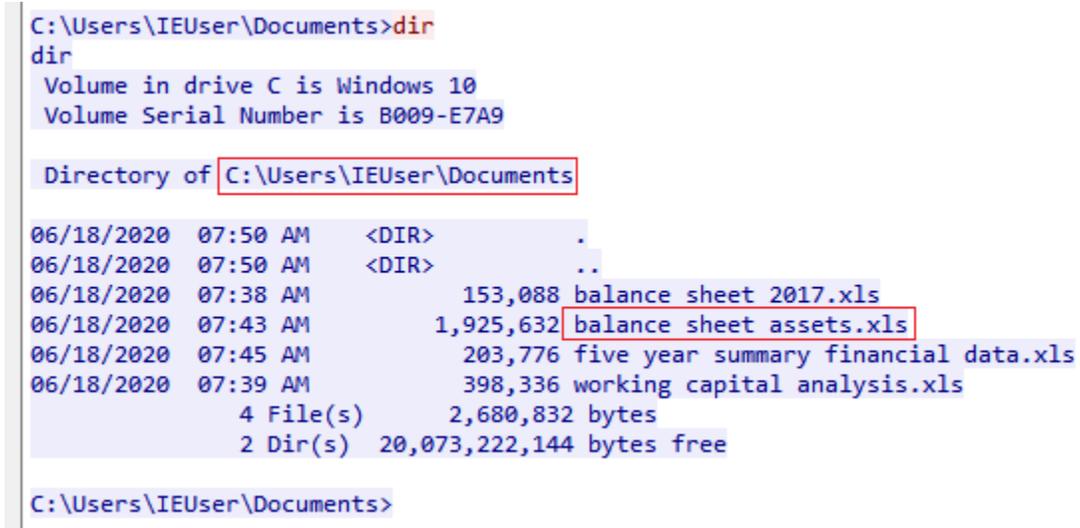
18. Insert a screenshot showing the result in Wireshark.



19. What is the full pathway for balance sheet assets.xls file?

C:\Users\IEUser\Documents\balance sheet assets.xls

20. Insert a screenshot showing the result in Wireshark.



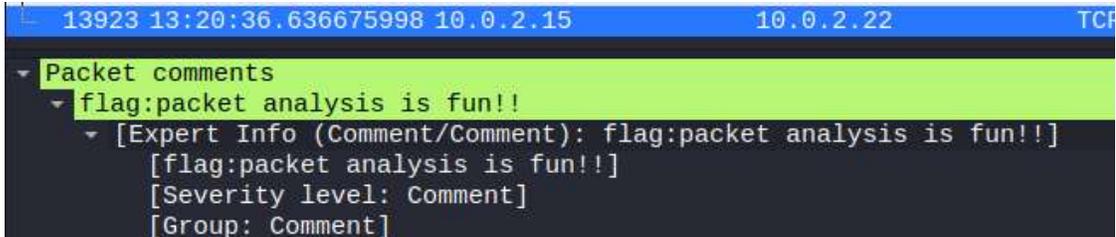
## Part 2 PCAP Analysis Extra Credit

For a potential 10 extra points (each correct answer or screenshot is worth 2.5 point each), look in CIS294CP.pcapng for the following:

### 1. What is the message hidden in the comments?

packet analysis is fun!!

### 2. Insert a screenshot showing the result in Wireshark.



### 3. What type of CPU was used by the attacker? Provide the complete make/model/type

Intel Core i7-9750H CPU @ 2.60GHz (with SSE4.2)

### 4. Insert a screenshot showing the result in Wireshark.

