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.

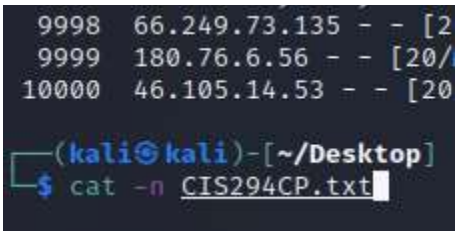
Part 1 Log Analysis

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**.



3. **How many different IP addresses reached the server?**

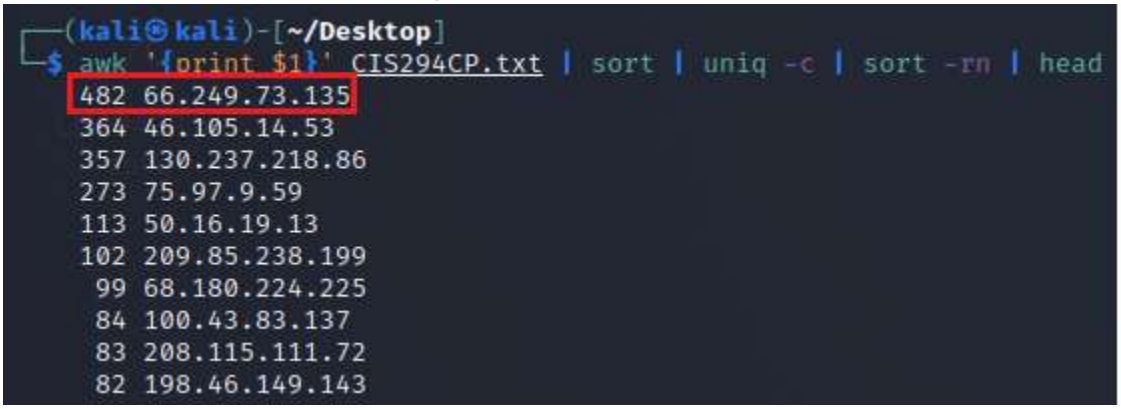
1,753

4. **Insert a screenshot showing the result.**

5. **Which IP address reached the server the most?**

66.249.73.135

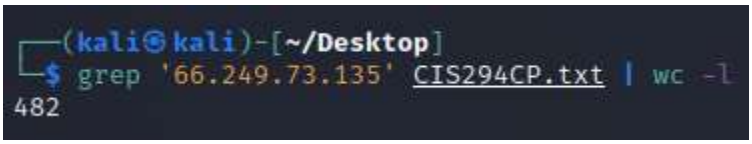
6. **Insert a screenshot showing the result.**



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

482 times

8. **Insert a screenshot showing the result.**



9. **How many HTTP 200 status code are listed?**

9126

10. **Insert a screenshot showing the result.**

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

213

12. **Insert a screenshot showing the result.**

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

208.115.111.72

14. **Insert a screenshot showing the result.**

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

favicon.ico

16. **Insert a screenshot showing the result.**

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

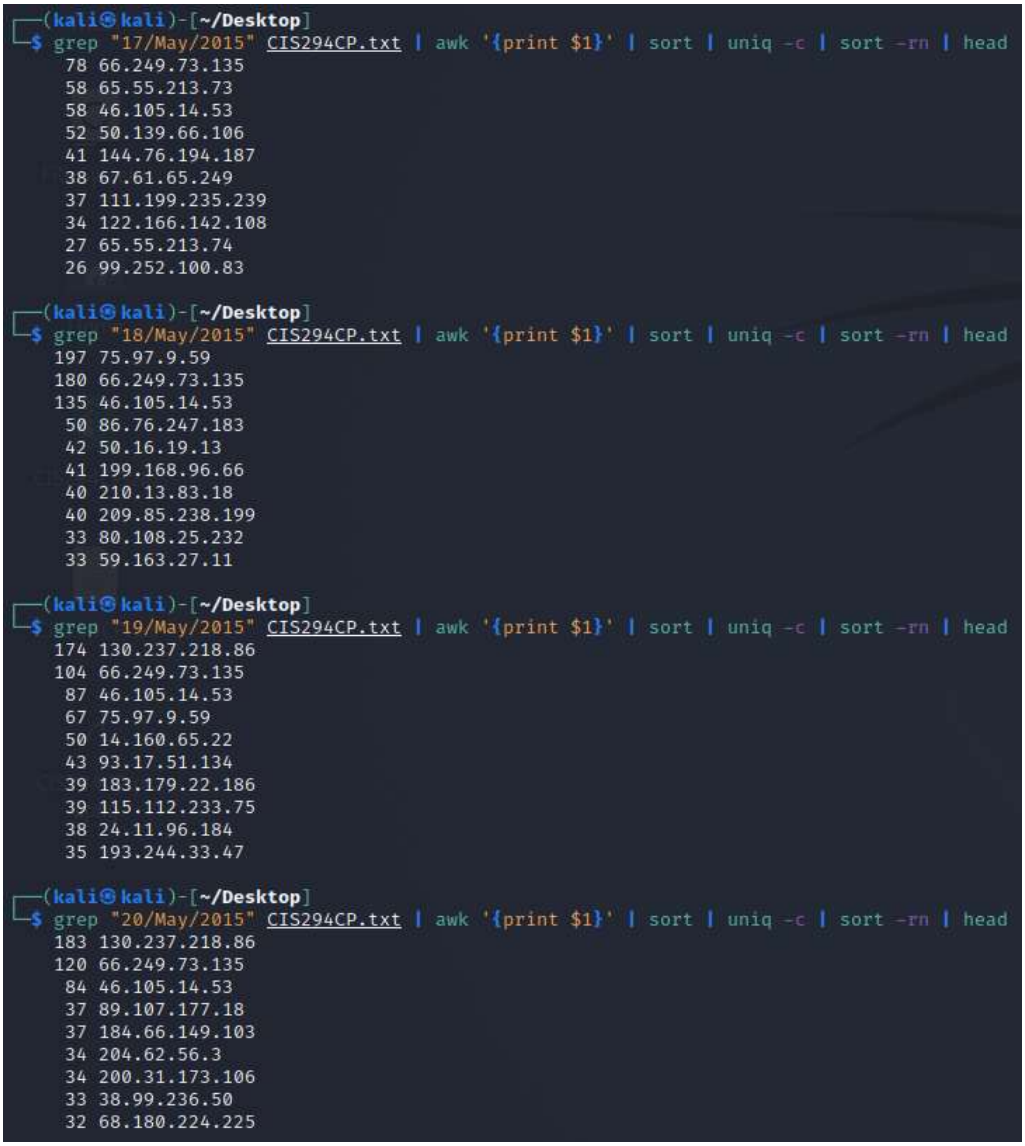
Part 1 Log Analysis Extra Credit

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.**



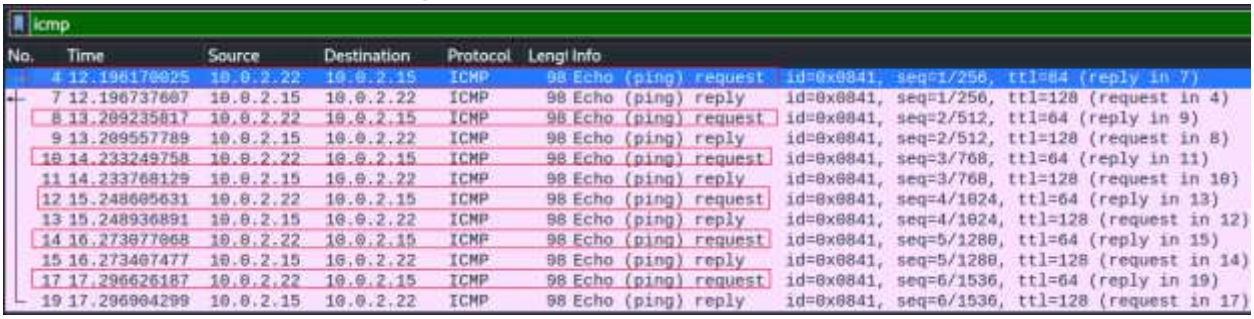
Part 2 Pcap Analysis

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

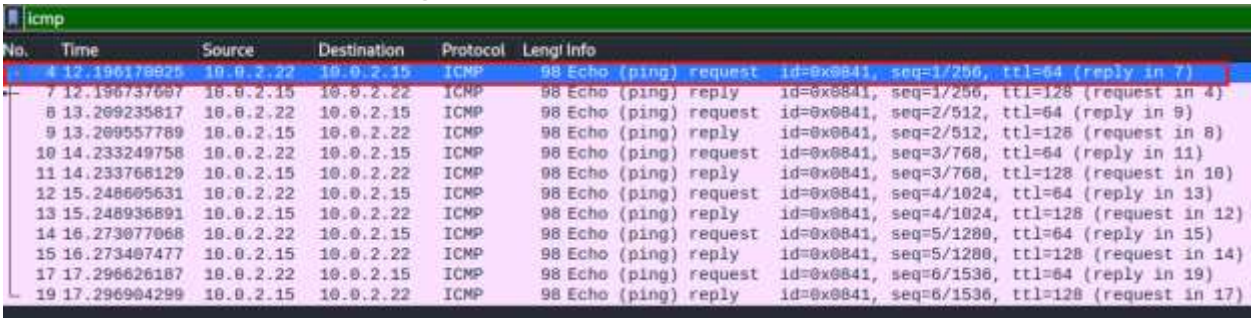
2. **Insert a screenshot showing the result in Wireshark.**



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

   10.0.2.22

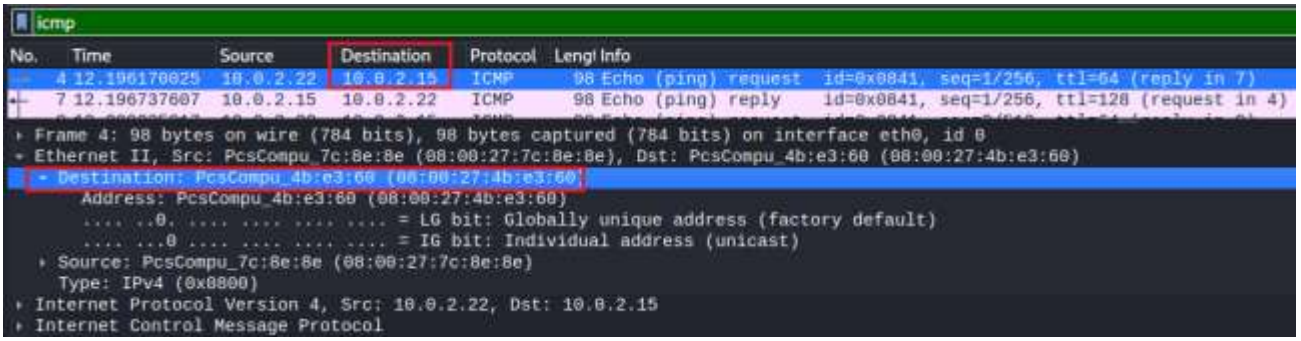
4. **Insert a screenshot showing the result in Wireshark.**



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

   10.0.2.15

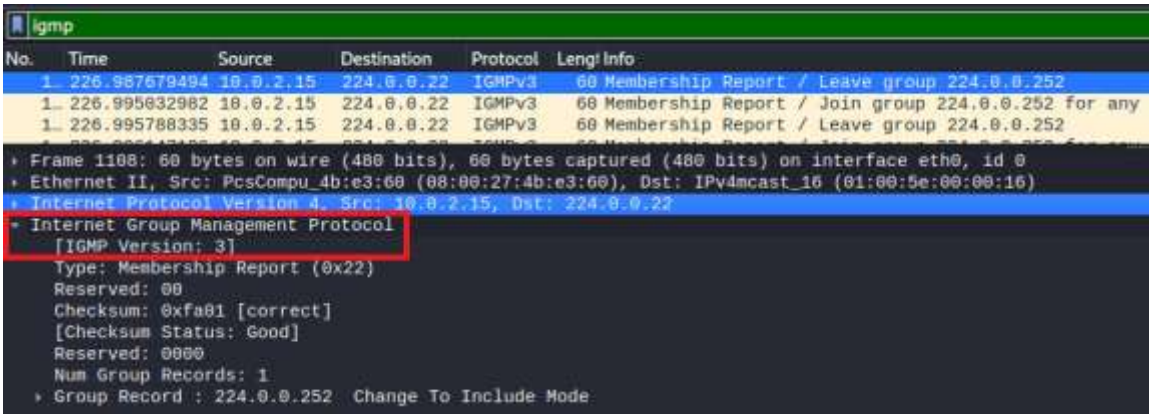
6. **Insert a screenshot showing the result in Wireshark.**



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

IGMP Version 3

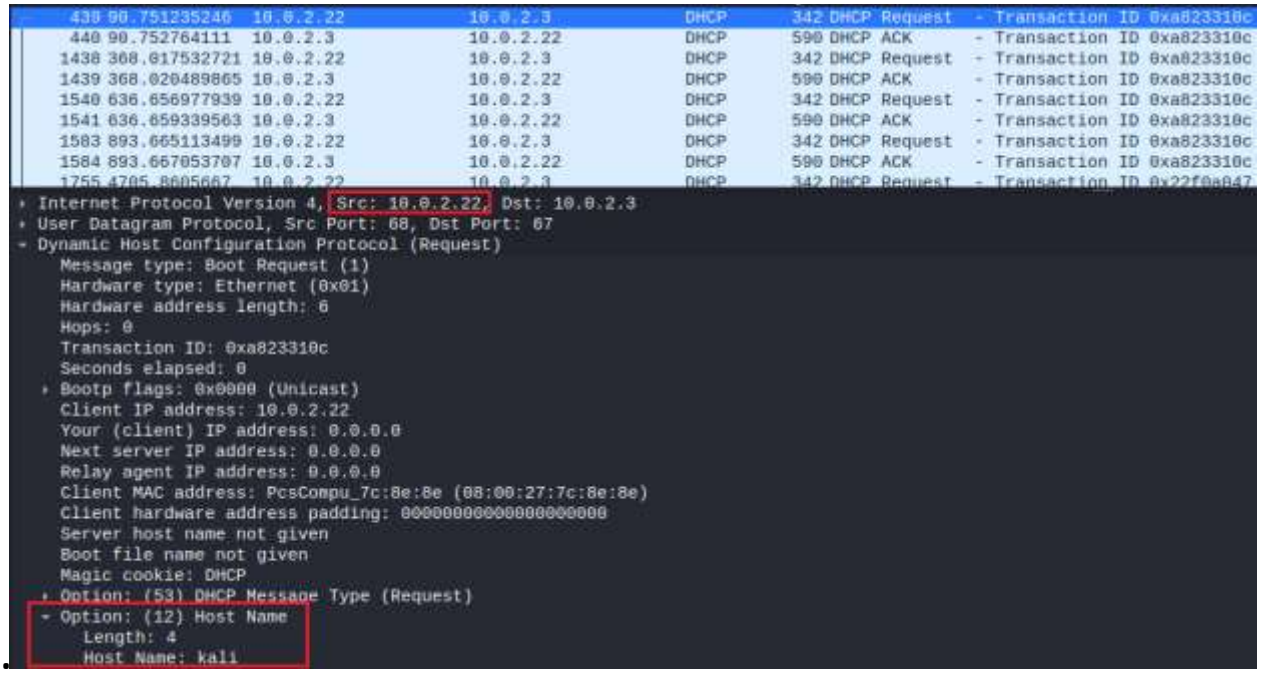
8. **Insert a screenshot showing the result in Wireshark.**



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

kali

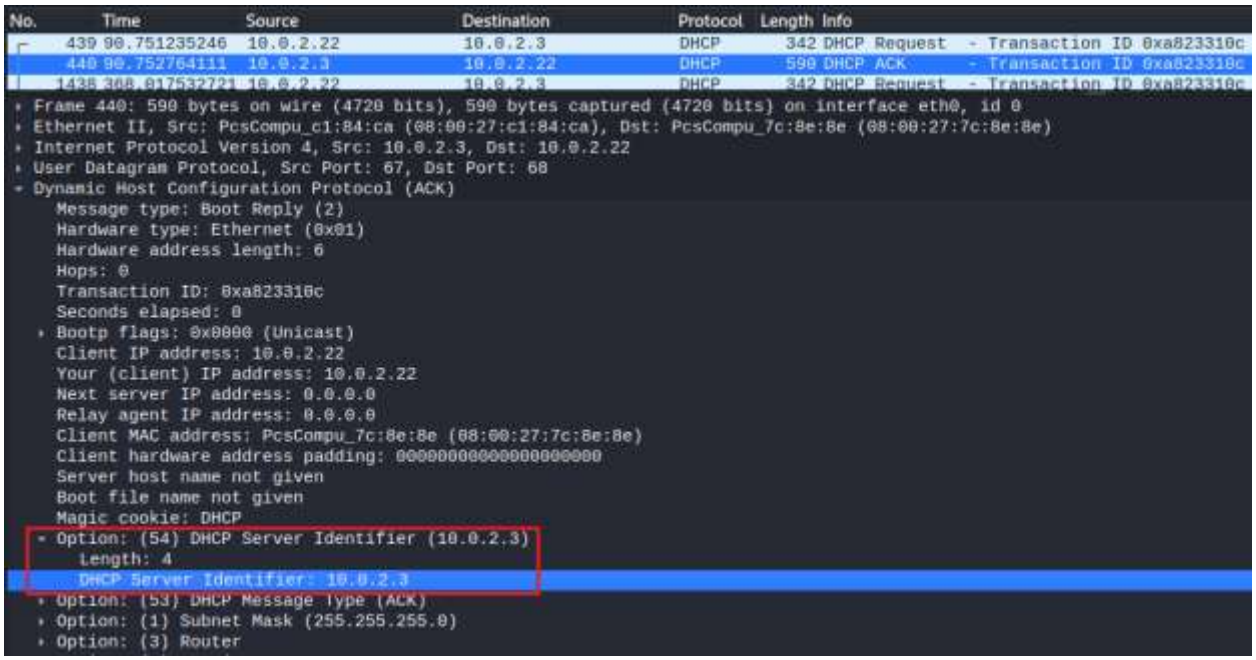
10. **Insert a screenshot showing the result in Wireshark.**



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

10.0.2.3

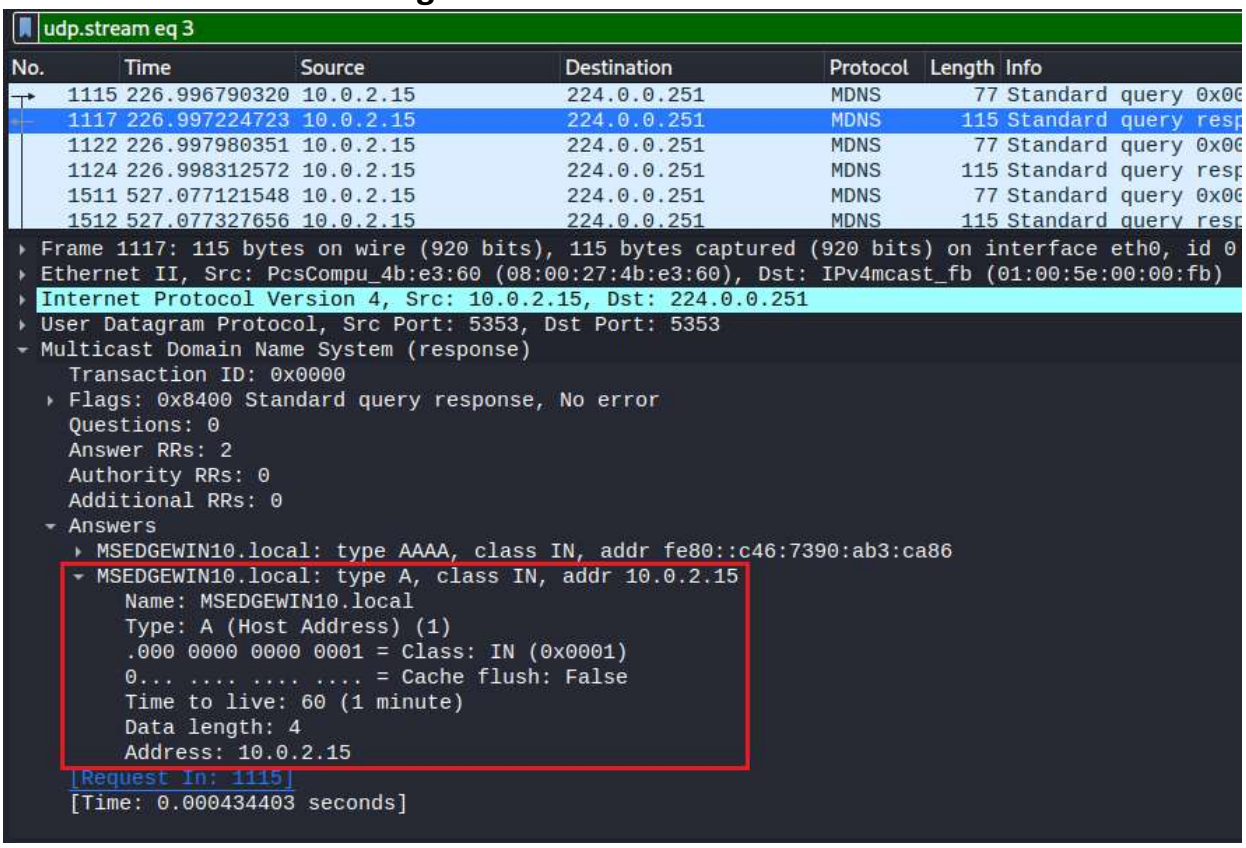
12.Insert a screenshot showing the result in Wireshark.



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

MSEDGEWIN10

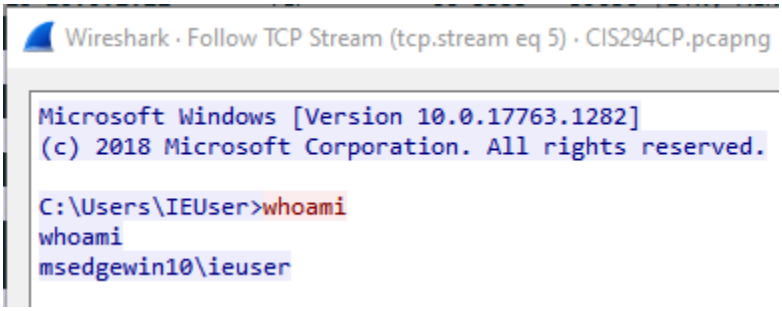
14.Insert a screenshot showing the result in Wireshark.



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

whoami

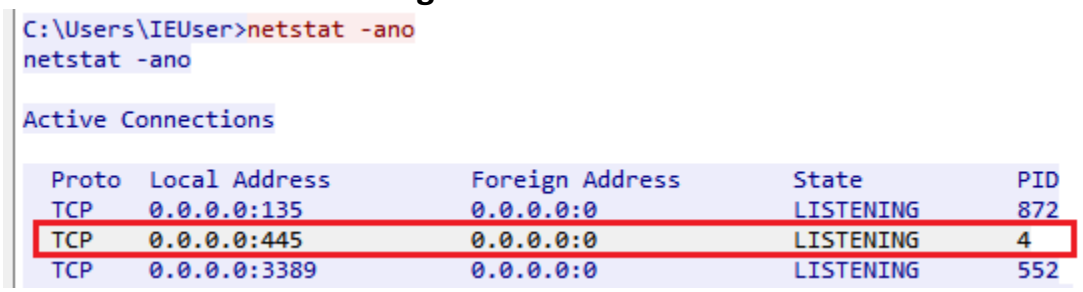
16.Insert a screenshot showing the result in Wireshark.



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

4

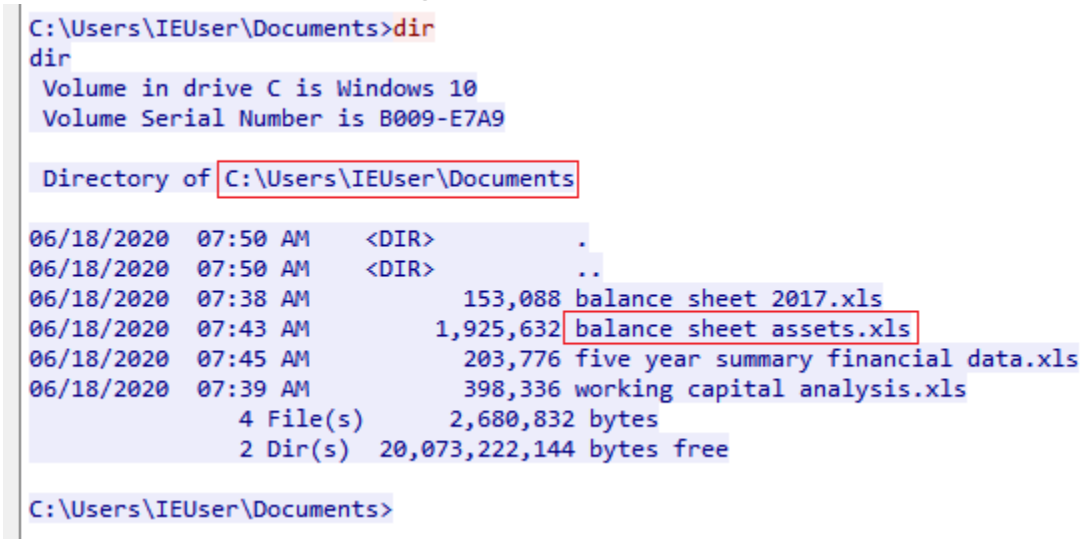
18.Insert a screenshot showing the result in Wireshark.



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.



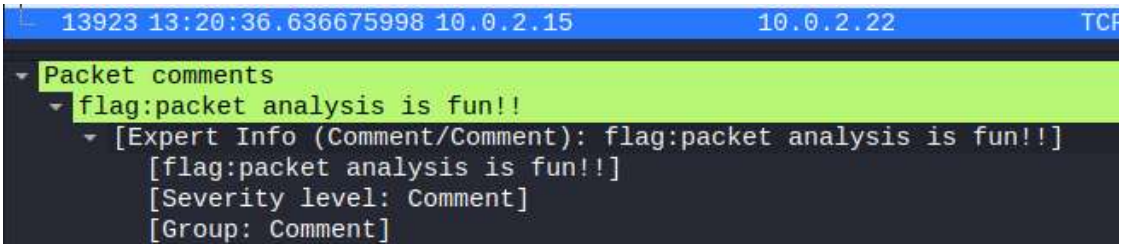
Part 2 PCAP Analysis Extra Credit

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.**