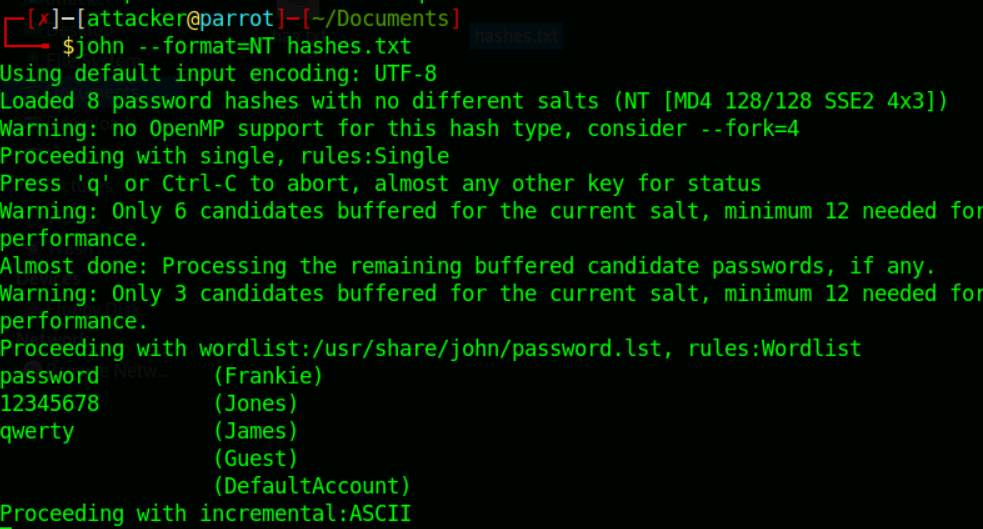
**CEH ENGAGE part 2**

1. You are assigned a task to crack the NTLM password hashes captured by the internal security team. The password hash has been stored in the Documents folder of the Parrot Security console machine. What is the password of user James? (Format: aaaaaa)

Answer: qwerty



1. You are assigned a task to crack the NTLM password hashes captured by the internal security team. The password hash has been stored in the Documents folder of the Parrot Security console machine. What is the password of user Jones? (Format: NNNNNNNN)

Answer: 12345678

Check above image

1. You have been given a task to audit the passwords of a server present in CEHORG network. Find out the password of the user Adam and submit it. (Note: Use Administrator/ CSCPa$$ when asked for credentials). (Format: aaaaaaaaN)

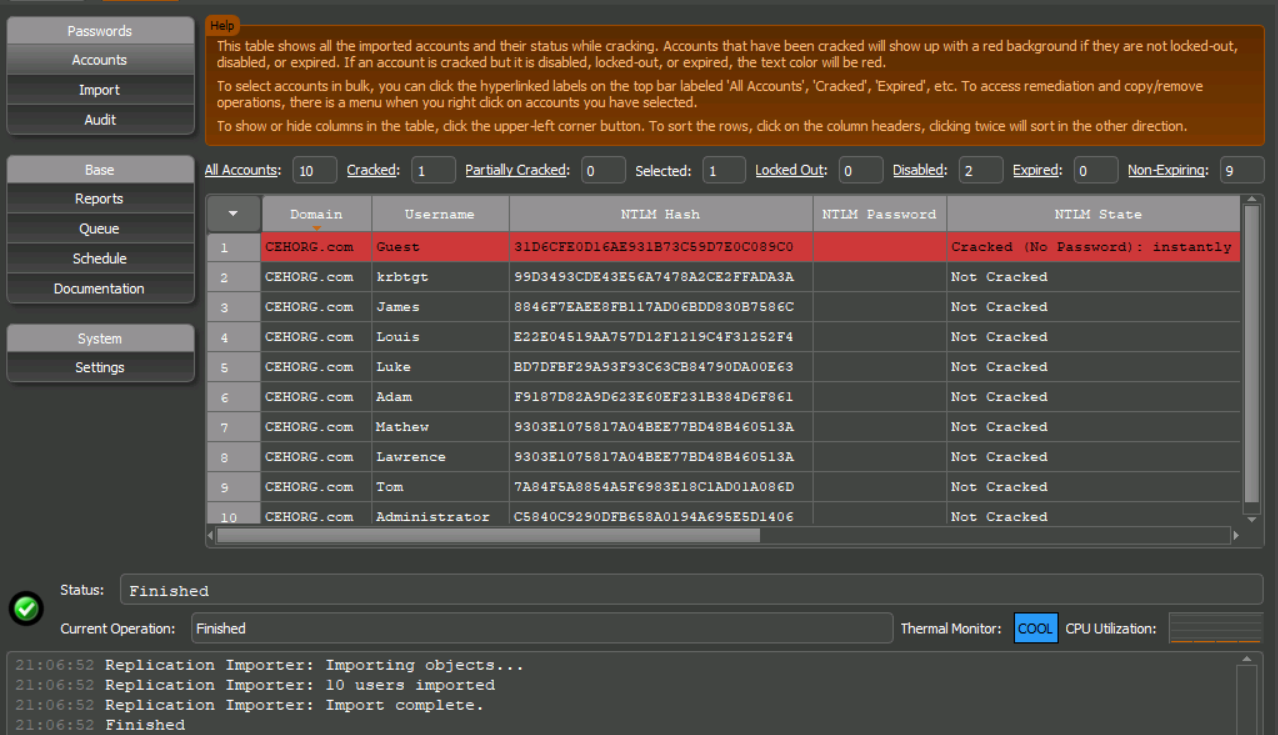
Answer: password4

Start new session

Go to Import - > import from remote windows

Give our IP of perrot os and give username and password which is given in question.

Click on run

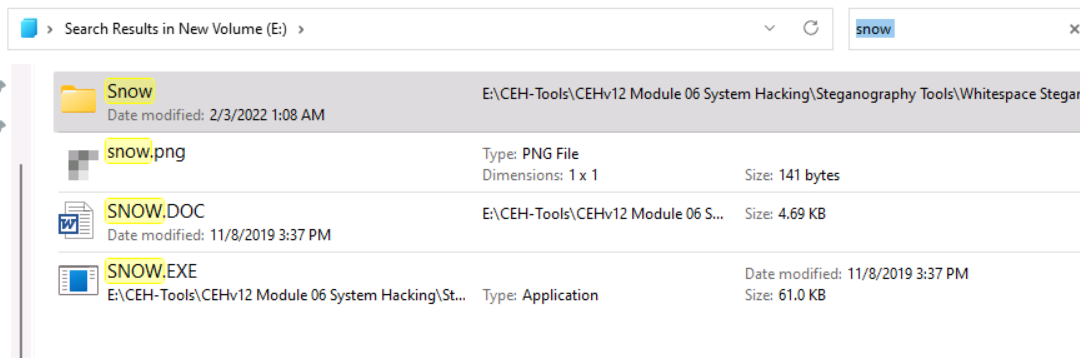


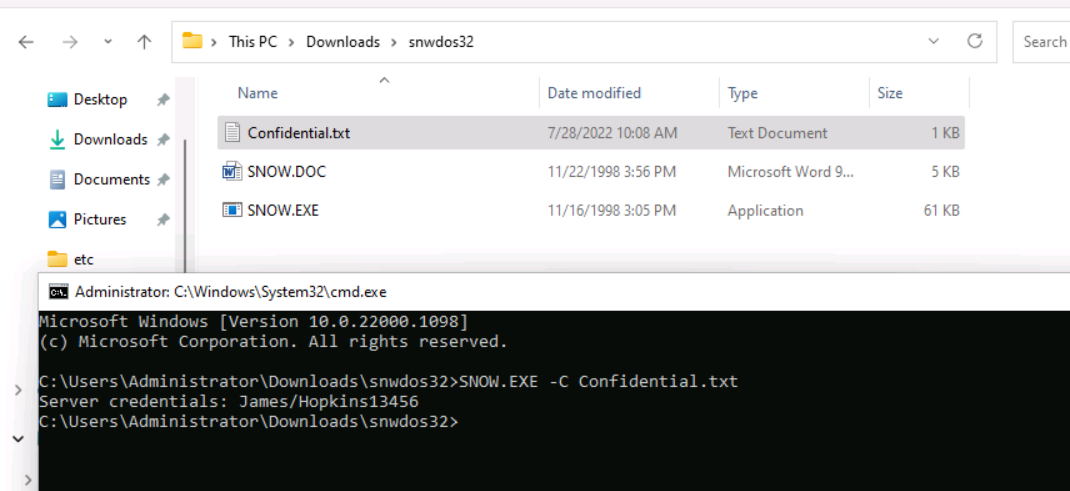


1. An employee in your organization is suspected of sending important information to an accomplice outside the organization. The incident response team has intercepted some files from the employee's system that they believe have hidden information. You are asked to investigate a file named Confidential.txt and extract hidden information. Find out the information hidden in the file. Note: The Confidential.txt file is located at C:\Users\Admin\Documents in EH Workstation – 2 machine. (Format: Aaaaa/AaaaaaaNNNNN)

Answer: James/Hopkins13456

Make sure that confidentials.txt file paste in a folder where snow.exe present

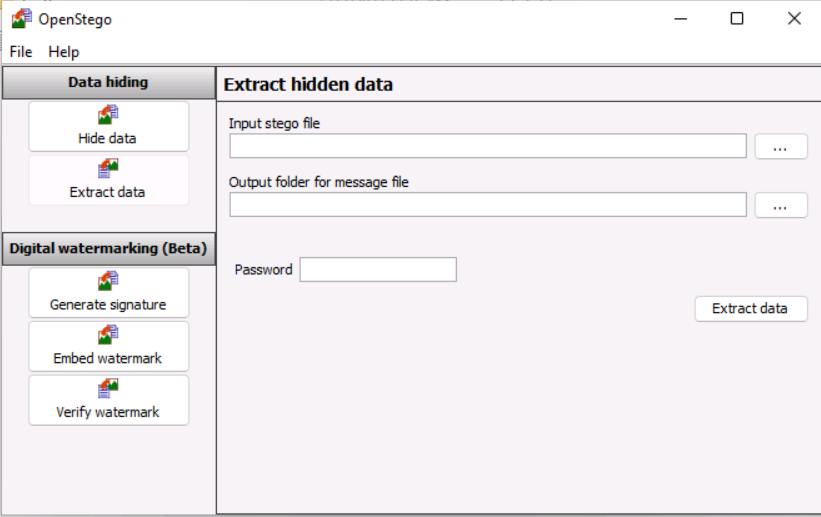




1. The incident response team has intercepted an image file from a communication that is supposed to have just text. You are asked to investigate the file and check if it contains any hidden information. Find out the information hidden in the file. Note: The vacation.bmp file is located at C:\Users\Admin\Documents in EH Workstation – 2 machine. (Format: AAANNNNNNN)

Answer: USD1234567

Select the image file and select where to extract and click Extract data. We got one txt file and it has answer.

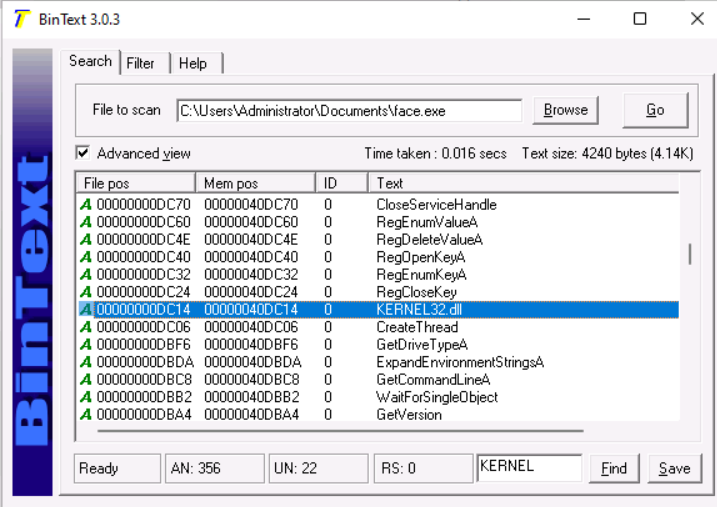


1. A disgruntled employee in CEHORG has used the Covert\_TCP utility to share a secret message with another user in the CEHORG network. Covert\_TCP manipulates the TCP/IP header of the data packets to send a file one byte at a time from any host to a destination. It can be used to hide the data inside IP header fields. The employee used the IP ID field to hide the message. The network capture file “Capture.pcapng” has been retained in the “C:\Users\Administrator\Documents” directory of the “EH Workstation – 2” machine. Analyze the session to get the message that was transmitted. (Format: AN\*A\*AN)

Answer:

1. You are a malware analyst working for CEHORG. During your assessment within your organisation's network, you found a malware face.exe. The malware is extracted and placed at C:\Users\Admin\Documents in the EH Workstation – 2 machine. Analyze the malware and find out the File pos for KERNEL32.dll text. (Hint: exclude zeros.) (Format: AANN)

Answer: DC14

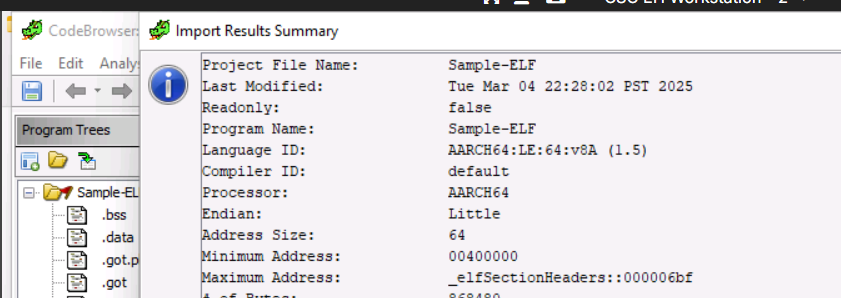


1. Analyze an ELF executable (Sample-ELF) file placed at C:\Users\Admin\Documents in the EH Workstation – 2 machines to determine the CPU Architecture it was built for. (Format: AAAAANN)

Answer: AARCH64

Open GidhraRun.bat to open it.

Then create a project and then click on Dragon Icon and then import sample-ELF file and analyze it.



1. CEHORG has assigned you with analysing the snapshot of the operating system registry and perform the further steps as part of dynamic analysis and find out the whether the driver packages registry is changed. Give your response as Yes/No. (Format: Aaa)

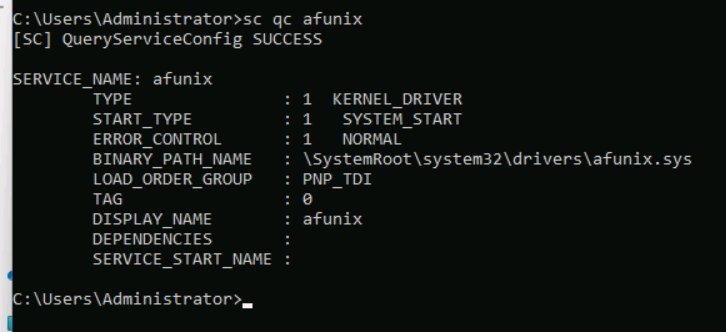
Answer: Yes

It want to check then check in dynamic malware tools

1. Perform windows service monitoring and find out the service type associated with display name "afunix". (Format: aaaaaa)

Answer: driver

Check type it can be kernal or driver

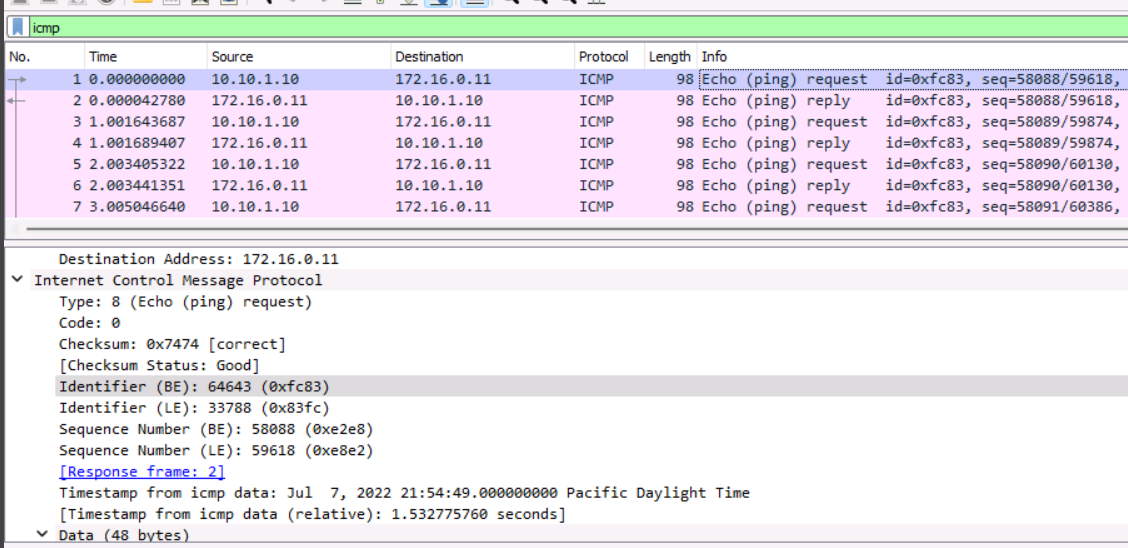


1. Use Yersinia on the “EH Workstation – 1” (Parrot Security) machine to perform the DHCP starvation attack. Analyze the network traffic generated during the attack and find the Transaction ID of the DHCP Discover packets. (Format: NaNNNaNNNN)

Answer:

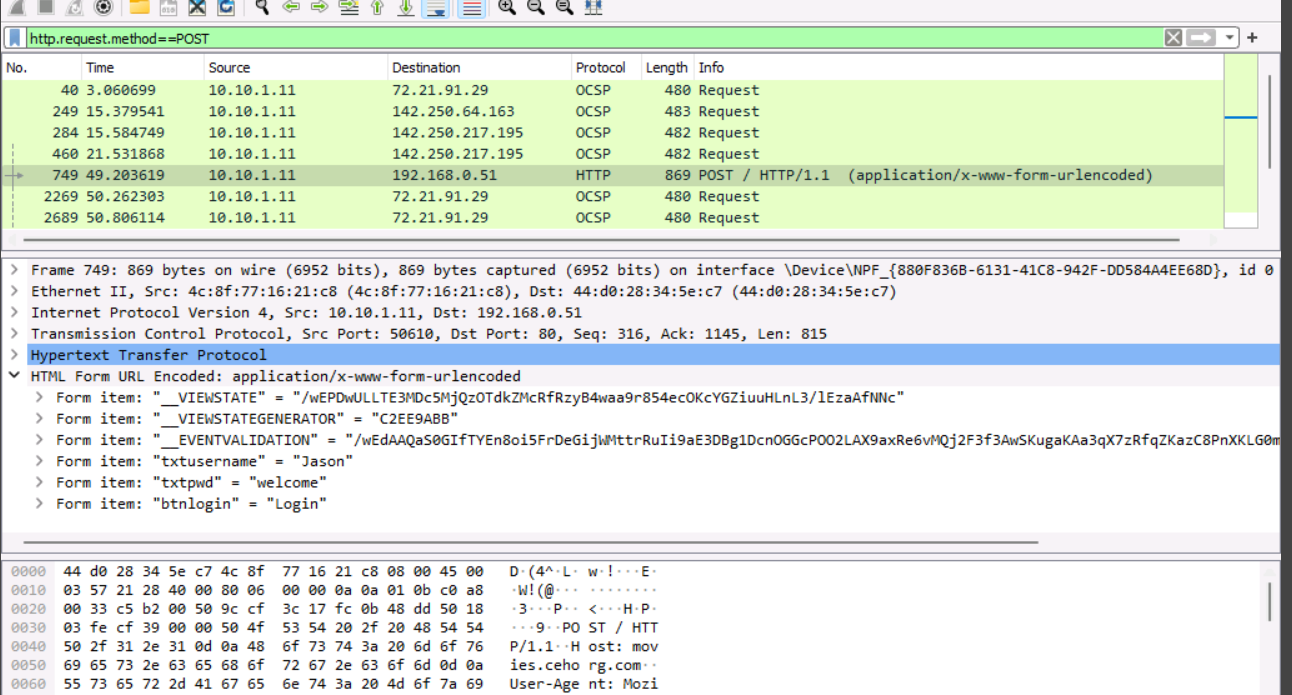
1. CEHORG suspects a possible sniffing attack on a machine in its network. The organization has retained the network traffic data for the session and stored it in the Documents folder in EH Workstation – 2 (Windows 11) machine as sniffsession.pcap. You have been assigned a task to analyze and find out the protocol used for sniffing on its network. (Format: AAA)
2. As an ethical hacker, you are tasked to analyze the traffic capture file webtraffic.pcapng. Find out the packet's id that uses ICMP protocol to communicate. Note: The webtraffic.pcapng file is located at C:\Users\Administrator\Documents\ in the Documents folder on EH Workstation – 2 (Windows 11) machine. (Format: NaaaNN)

Answer: 0xfc83



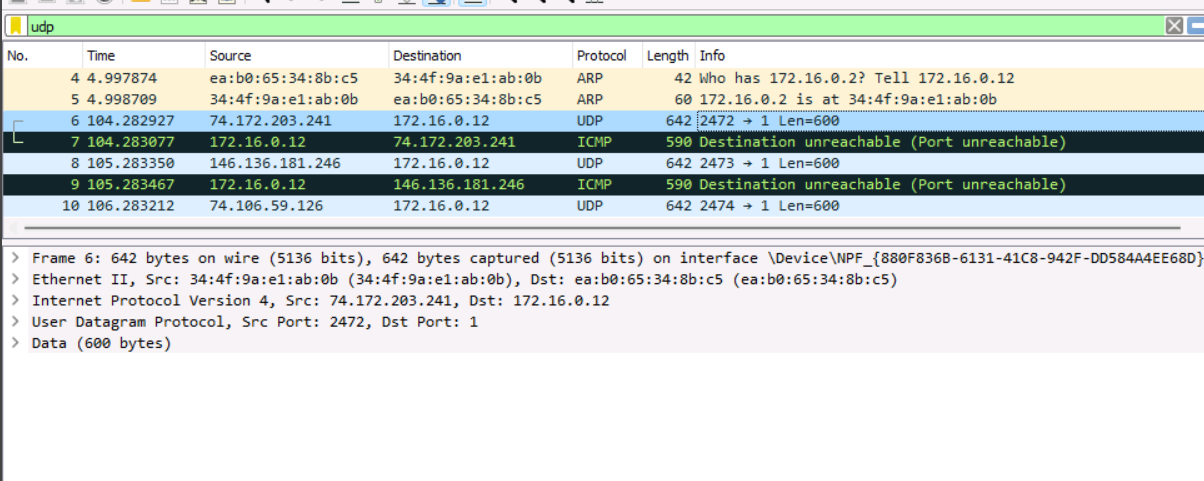
1. CEHORG has found that one of its web application movies.cehorg.com running on its network is leaking credentials in plain text. You have been assigned a task of analysing the movies.pcap file and find out the leaked credentials. Note: The movies.pcapng file is located at C:\Users\Administrator\Documents\ in the Documents folder on EH Workstation – 2 (Windows 11) machine. Make a note of the credentials obtained in this flag, it will be used in the Part 3 of CEH Skill Check. (Format: Aaaaa/aaaaaaa)

Answer: Json/welcome



1. An attacker has created a custom UDP packet and sent it to one of the machines in the CEHORG. You have been given a task to study the ""CustomUDP.pcapng"" file and find the data size of the UDP packet (in bytes). Note: The CustomUDP.pcapng file is located at C:\Users\Administrator\Documents\ in the Documents folder on EH Workstation – 2 (Windows 11) machine. (Format: NNN)

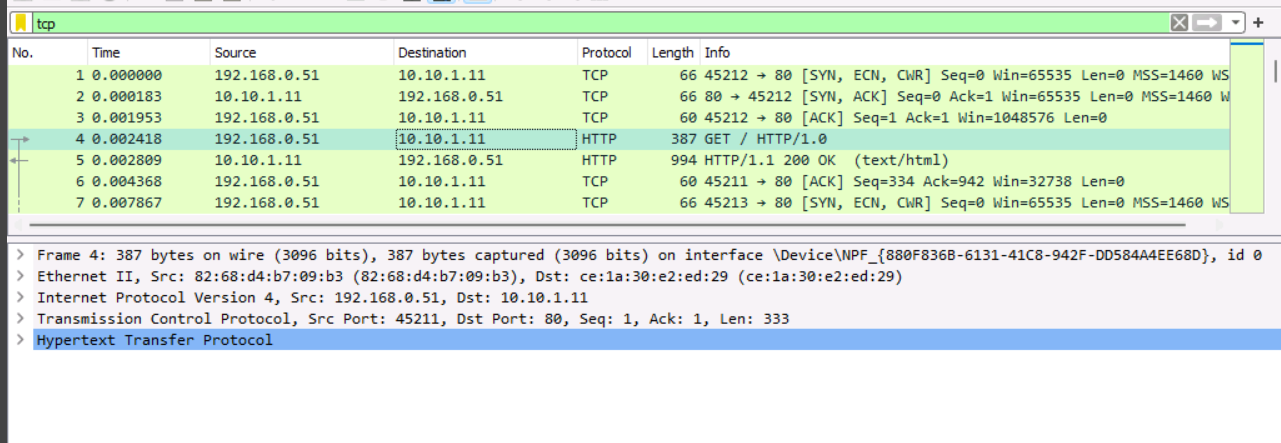
Answer: 600



1. A denial-of-service attack has been launched on a target machine in the CEHORG network. A network session file "DoS.pcapng" has been captured and stored in the Documents folder of the EH Workstation - 2 machine. Find the IP address of the attacker's machine. (Format: NNN.NNN.N.NN)

Answer: 192.168.0.51

Because 2 ip mostly found in source first is 192.168.0.51 and 10.10.1.11(It is mostly our internal ip of org.)



1. CEHORG hosts a datacenter for its bussiness clients. While analyzing the network traffic it was observed that there was a huge surge of incoming traffic from multiple sources. You are given a task to analyze and study the DDoS.pcap file. The captured network session (DDoS.pcapng) is stored in the Documents folder of the EH Workstation -2 machine. Determine the number of machines that were used to initiate the attack. (Format: N)

Answer: 3

In file we saw 192.168.0.51, 172.16.0.12 and 10.10.10.25 they all are retransmit the data in black highlight.

