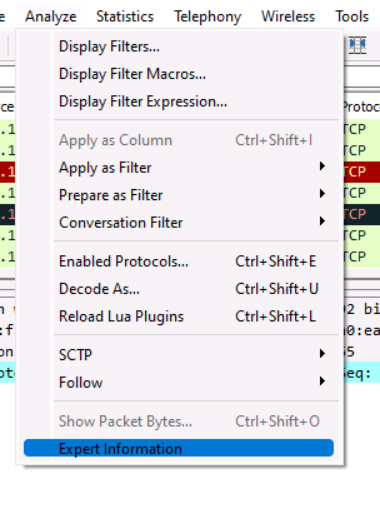
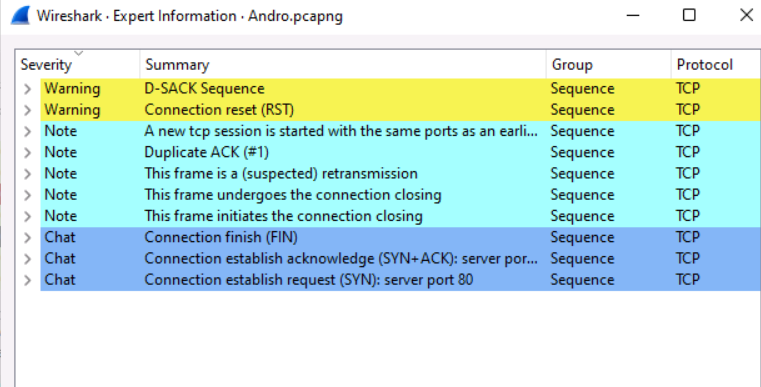
CEH Engage part 4

1. The mobile device of an employee in CEHORG has been hacked by the hacker to perform DoS attack on one of the server in company network. You are assigned to analyse "Andro.pcapng" located in Documents directory of EH workstation-2 and identify the severity level of the attack. (Note: perform deep down Expert Info analysis). (Format: Aaaaaaa )

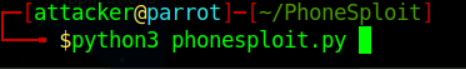
Answer: Warning

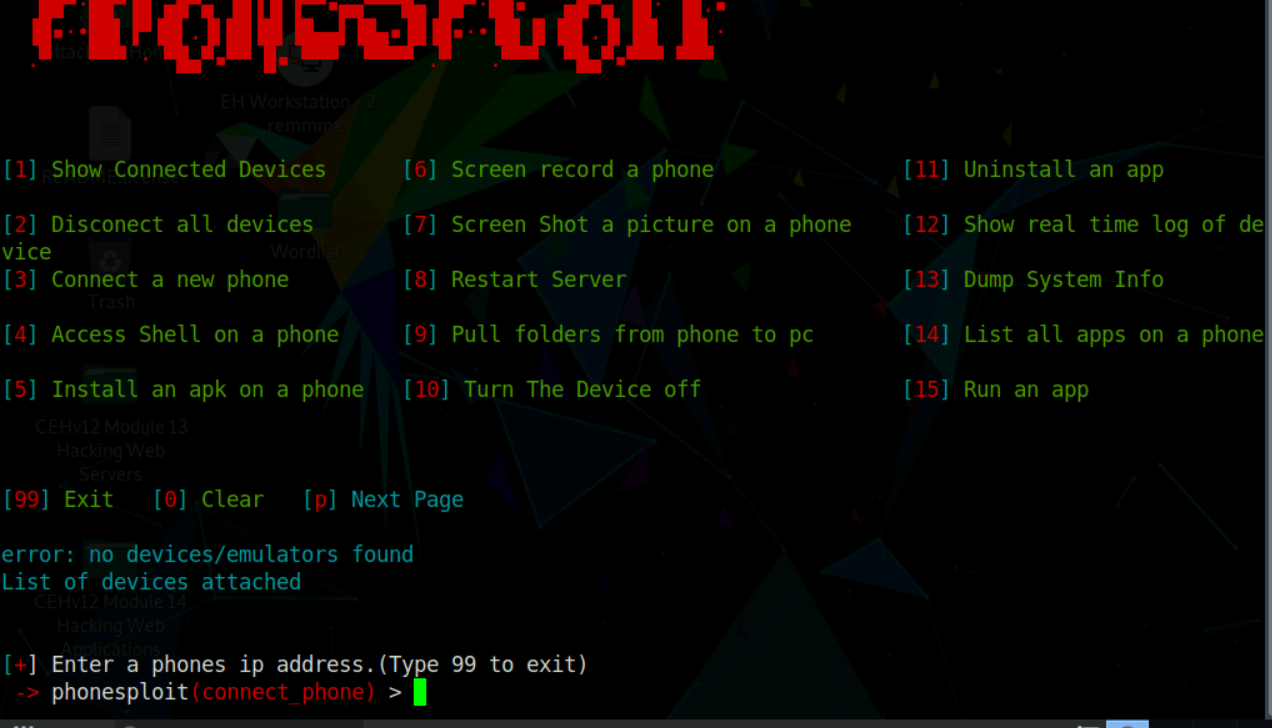




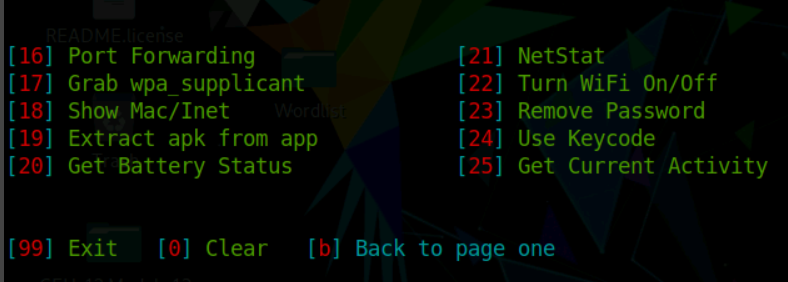
1. An ex-employee of CEHORG is suspected to be performing insider attack. You are assigned a task to attain KEYCODE-75 used in the employees' mobile phone. Note: use option p in PhoneSploit for next page. (Format: AAAAAAAAAA )

Answer: APOSTROPHE

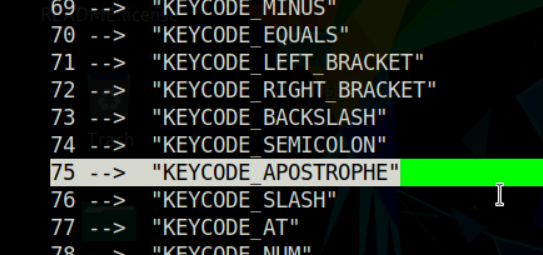




Press p for check other options.



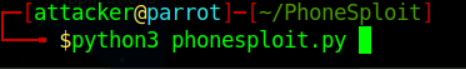
Press 24 for keycode.

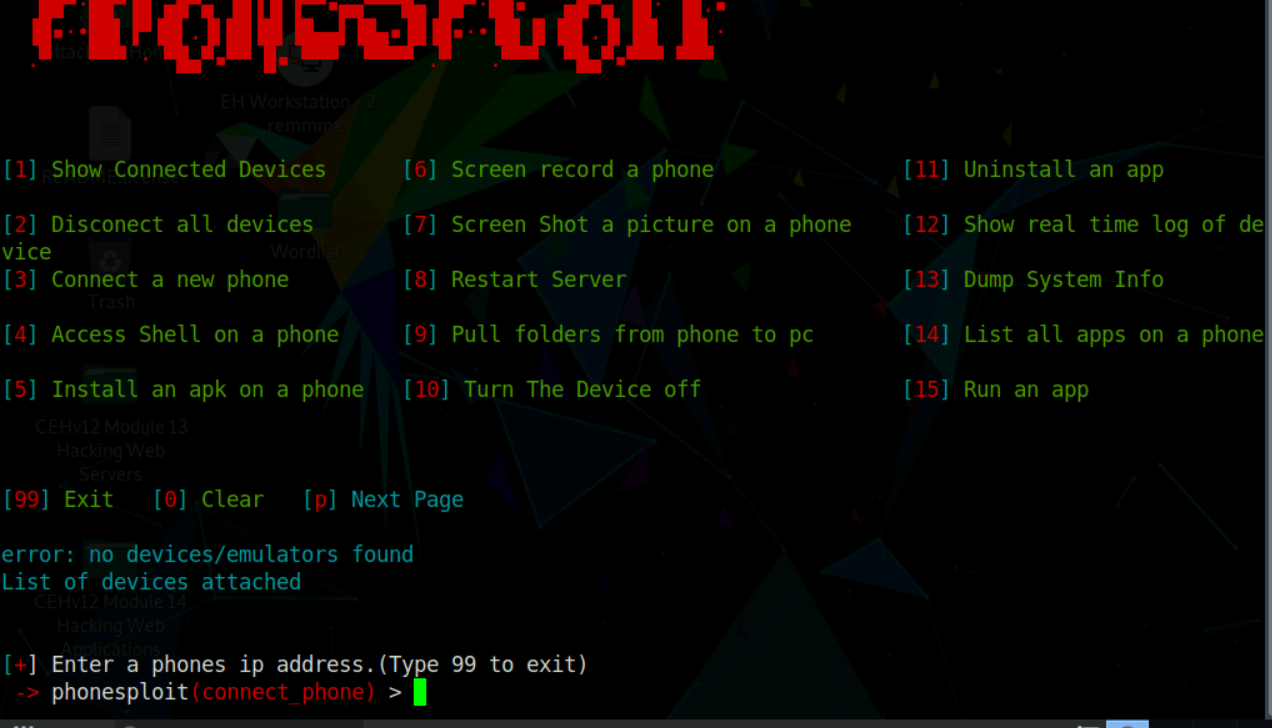


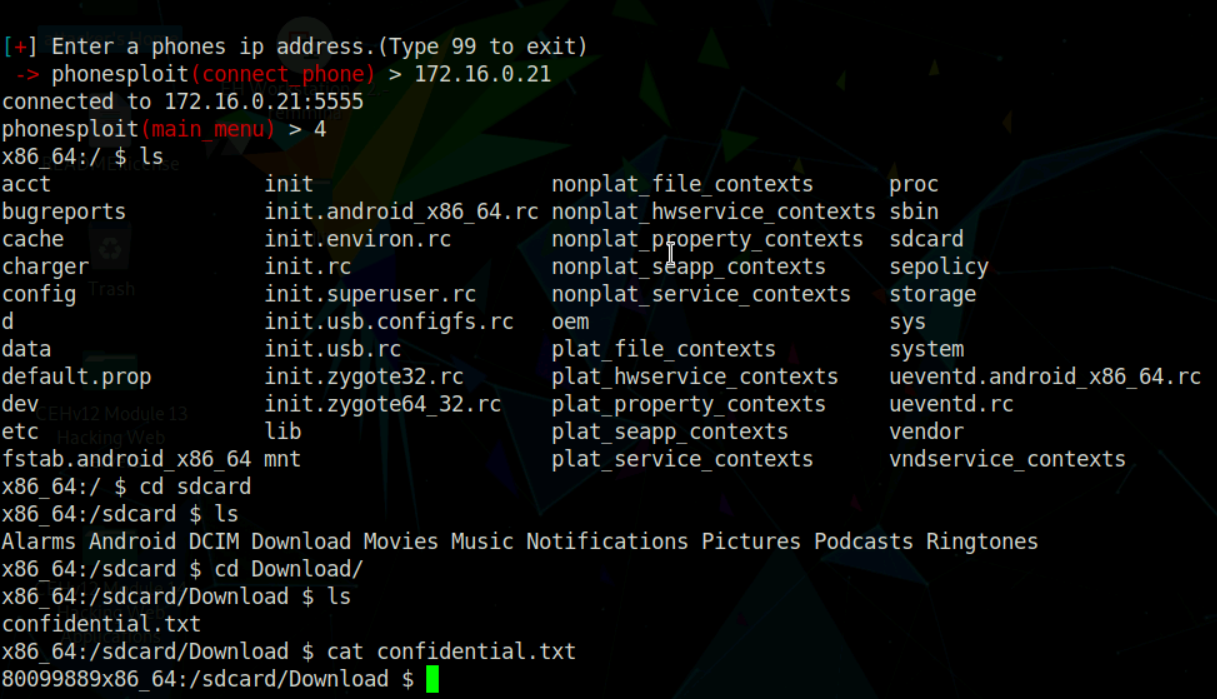
1. An employee in CEHORG has secretly acquired Confidential access ID through an application from the company. He has saved this information on the Downloads folder of his Android mobile phone. You have been assigned a task as an ethical hacker to access the file and delete it covertly. Enter the account information present in the file. Note: Only provide the numeric values in the answer field. (Format: NNNNNNNN)

Answer: 80099889





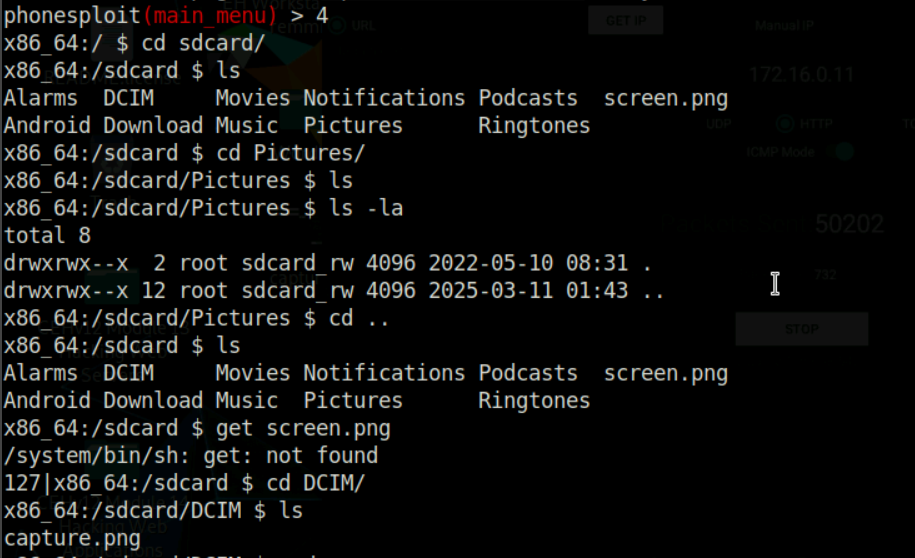




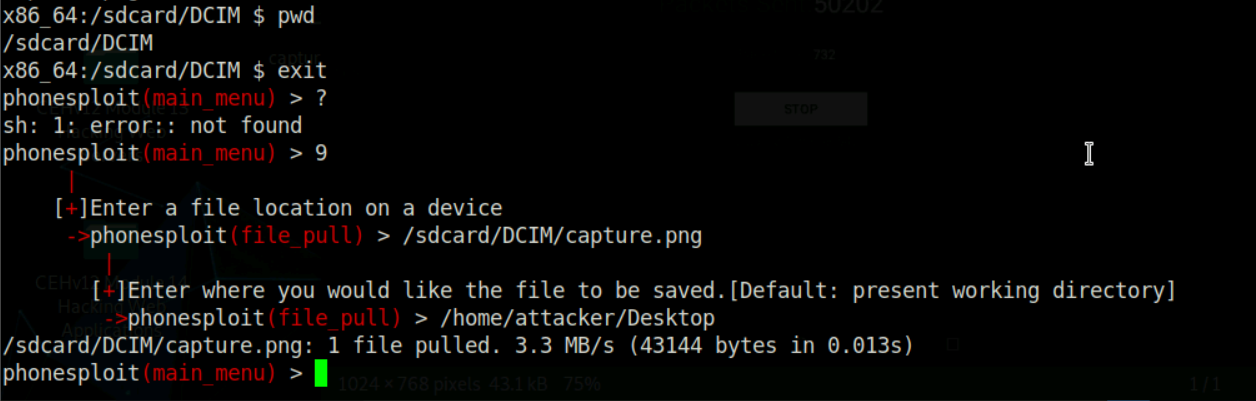
1. An attacker has hacked one of the employees android device in CEHORG and initiated LOIC attack from the device. You are an ethical hacker who had obtained a screenshot of the attack using a background application. Obtain the screenshot of the attack using PhoneSploit from the attacked mobile device and determine the targeted machine IP along with send method. (Format: NNN.NN.N.NN/AAAA)

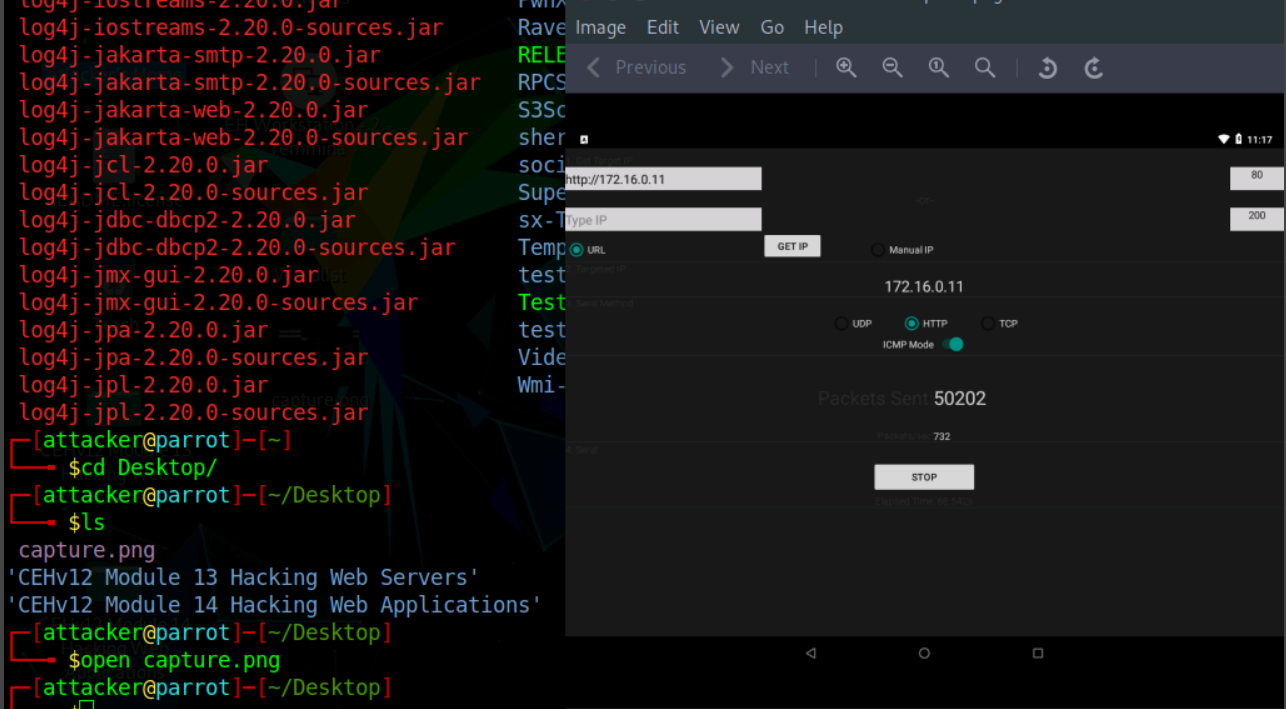
Answer: 172.16.0.11/HTTP

Connect the phone by give the IP in start.



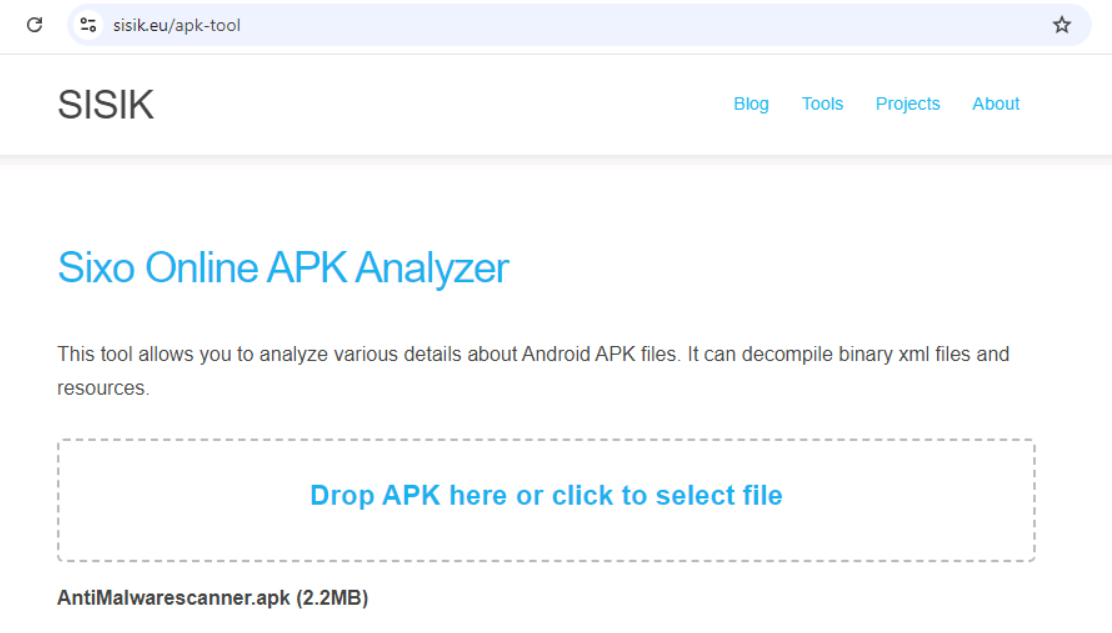
We have capture.png file and to get it we have to get back and pull that file



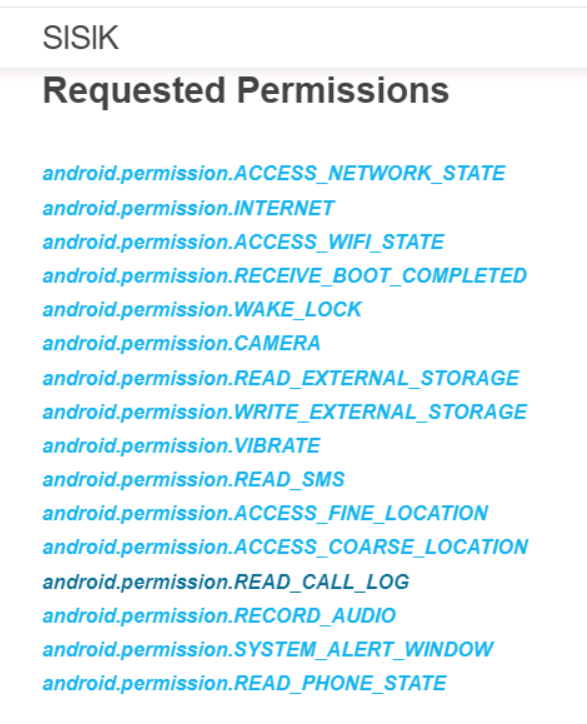


1. An attacker installed a malicious mobile application 'AntiMalwarescanner.apk' on the victims android device which is located in EH workstation-2 documents folder. You are assigned a task to perform security audit on the mobile application and find out whether the application using permission to Read-call-logs. (Format: Aaa )

Answer: Yes

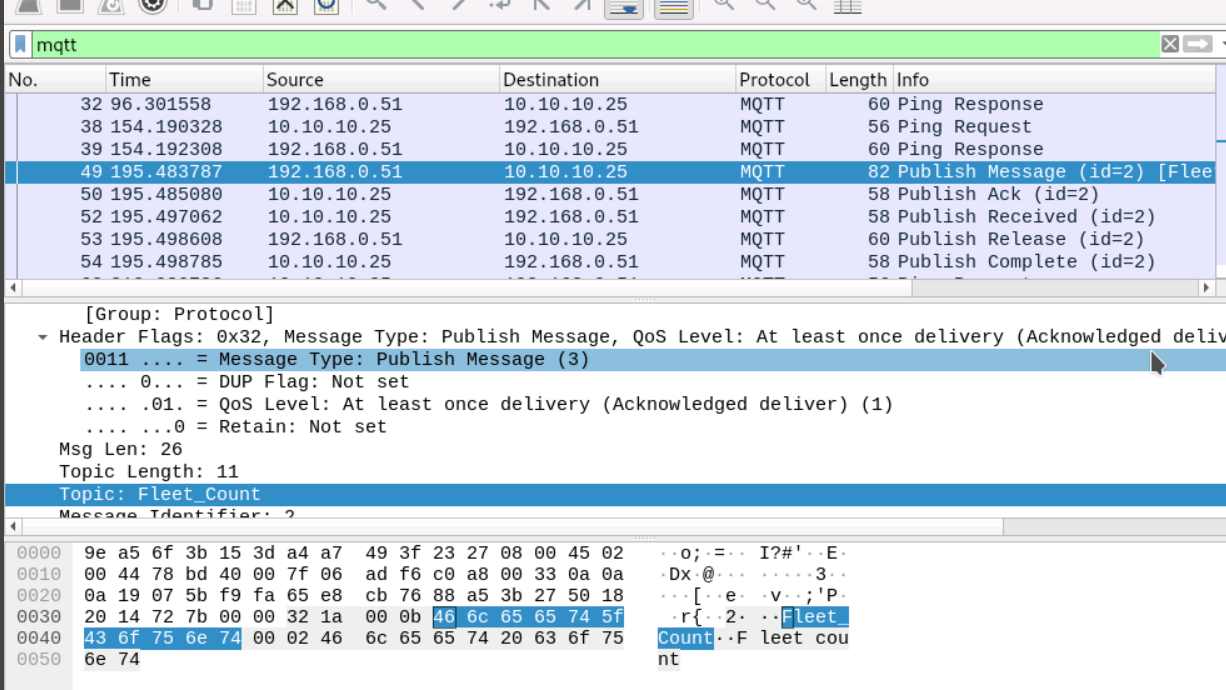


Scroll down and check permission and the permission is there.



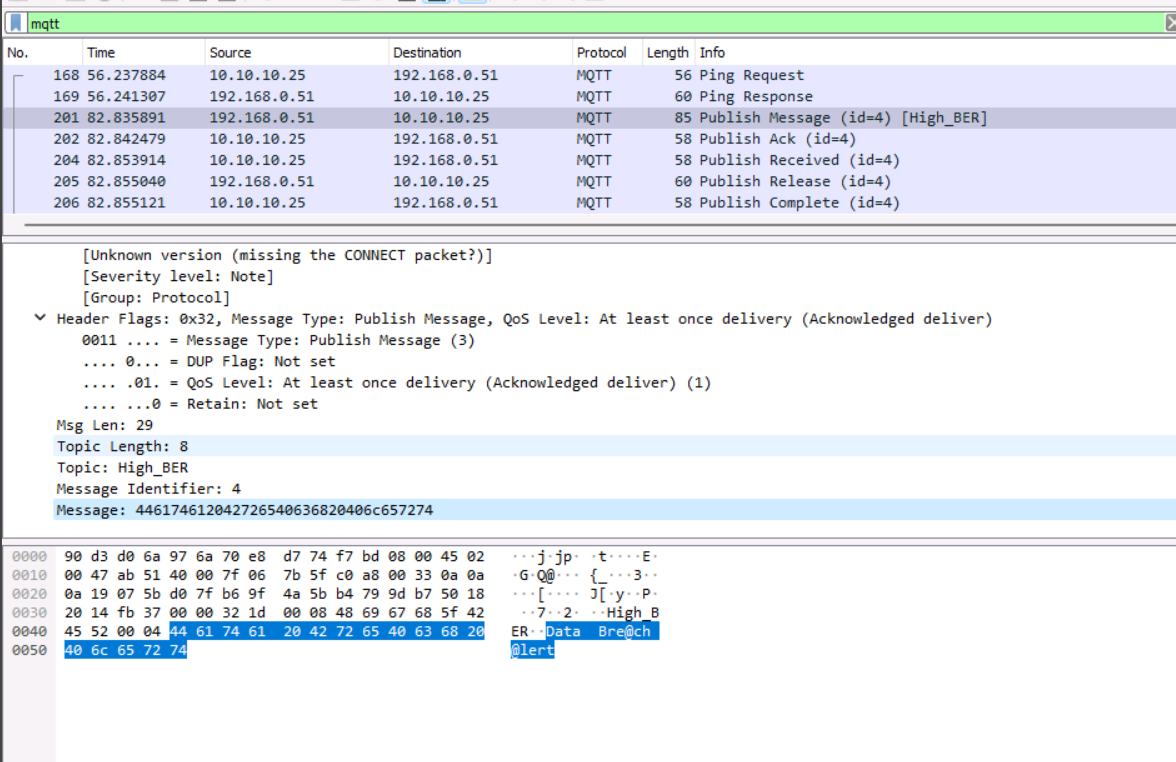
1. CEHORG hosts multiple IOT devices and sensors to manage its supply chain fleet. You are assinged a task to examine the file "IOT Traffic.pcapng" located in the Home directory of the root user in the "EH Workstation - 1" machine. Analyze the packet and find the topic of the message sent to the sensor. (Format: Aaaaa\*Aaaaa)

Answer: Fleet\_Count



1. CEHORG hosts multiple IOT devices and network sensors to manage its IT-department. You are assigned a task to examine the file "NetworkNS\_Traffic.pcapng" located in the Documents folder of the user in the "EH Workstation - 2" machine. Analyze the packet and find the alert message sent to the sensor. (Format: Aaaa Aaa\*aa \*aaaa)

Answer: Data Bre@ch @lert

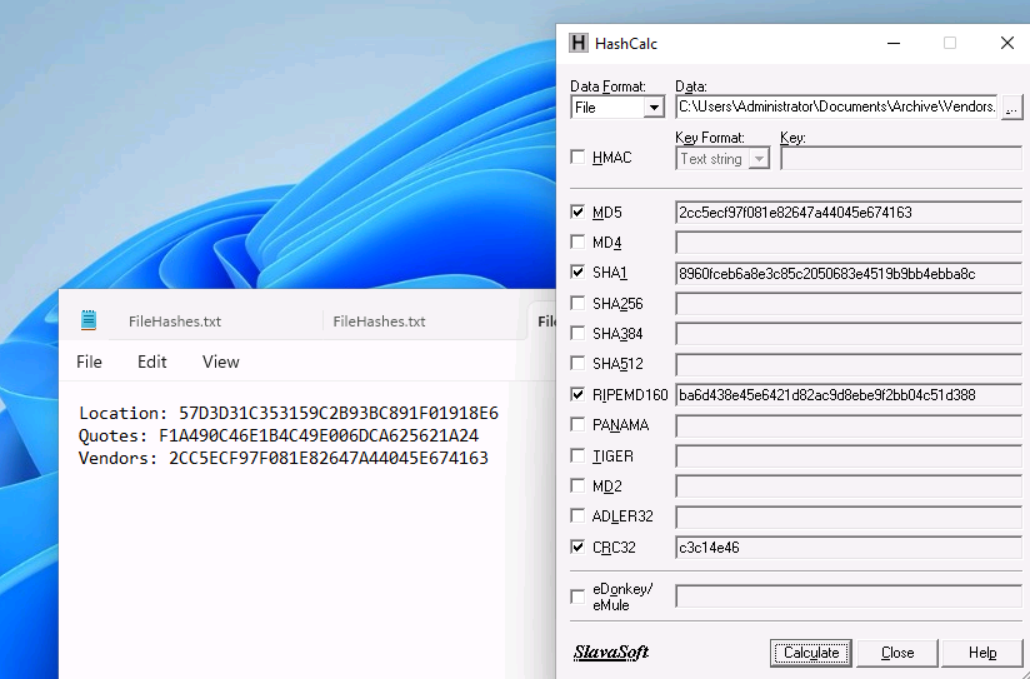


1. You have received a folder named "Archive" from a vendor. You suspect that someone might have tampered with the files during transmission. The Original hashes of the files have been sent by the sender separately and are stored in a file named FileHashes.txt stored in the Document folder in the "EH Workstation – 2" machine. Your task is to check the integrity of the files by comparing the MD5 hashes. Compare the hash values and determine the file name that has been tampered with. Note: Exclude the file extension in the answer field. The answer is case-sensitive. (Format: Aaaaaa)TOO

Answer: Quotes

Open Filehashes and check all 3 hashes are same as in hashcalc.

One by one select files(vendors, Location, Quotes) in hashcalc and match/check the MD5 string.

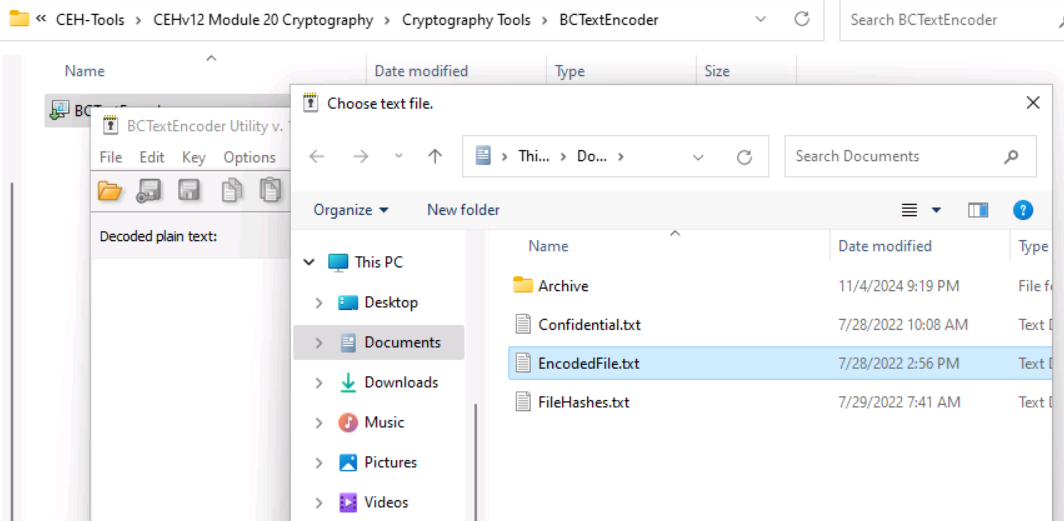


Quotes string is seem different.

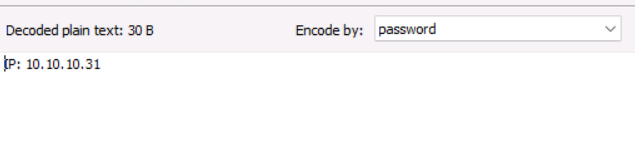


1. An attacker has intruded into the CEHORG network with malicious intent. He has identified a vulnerability in a machine. He has encoded the machine's IP address and left it in the database. While auditing the database, the encoded file was identified by the database admin. Decode the EncodedFile.txt file in the Document folder in the "EH Workstation – 2" machine and enter the IP address as the answer. (Hint: Password to decode the file is Pa$$w0rd). (Format: NN.NN.NN.NN)

Answer: 10.10.10.31

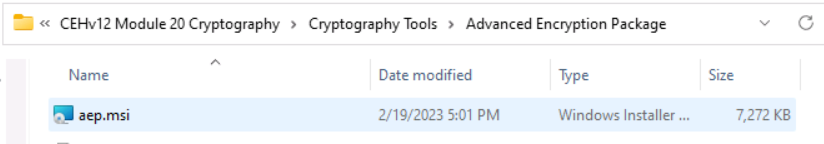


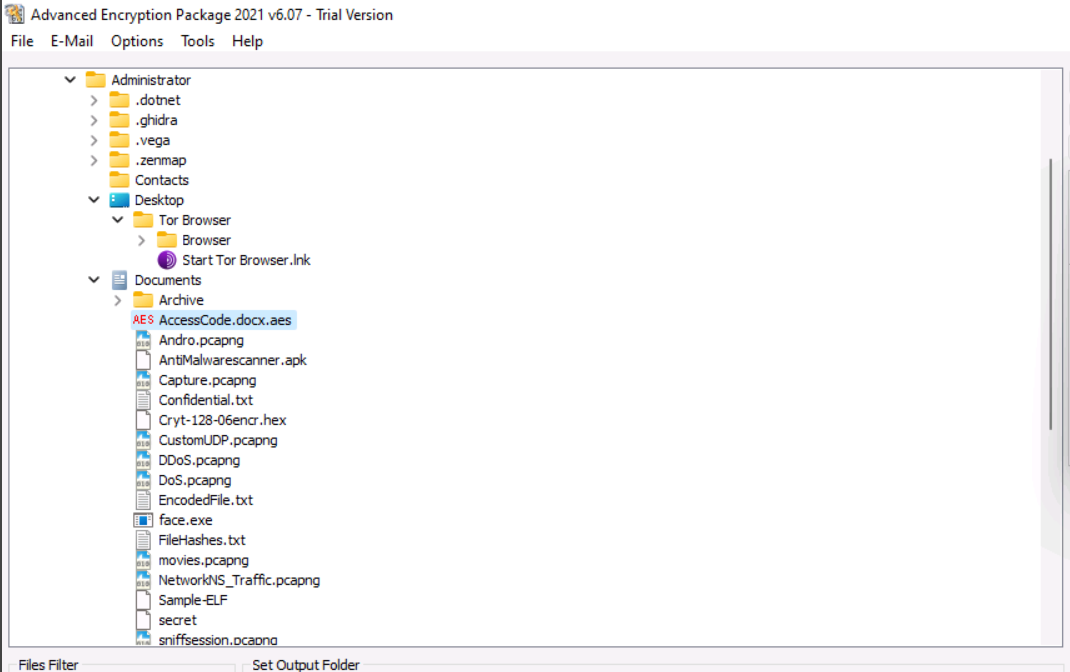
Give password: Pa$$w0rd and we decode and get the result which is an ip



1. The Access code of an employee was stolen from the CEHORG database. The attacker has encrypted the file using the Advance Encryption Package. You have been assigned a task to decrypt the file; the organization has retained the cipher file ""AccessCode.docx.aes"" in the Document folder in the ""EH Workstation – 2"" machine. Determine the access code by decrypting the file. Hint: Use ""qwerty"" as the decryption password. Note: Advanced Encryption Package is available at E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptography Tools. (Format: AAA\*AAA\*NNNN)

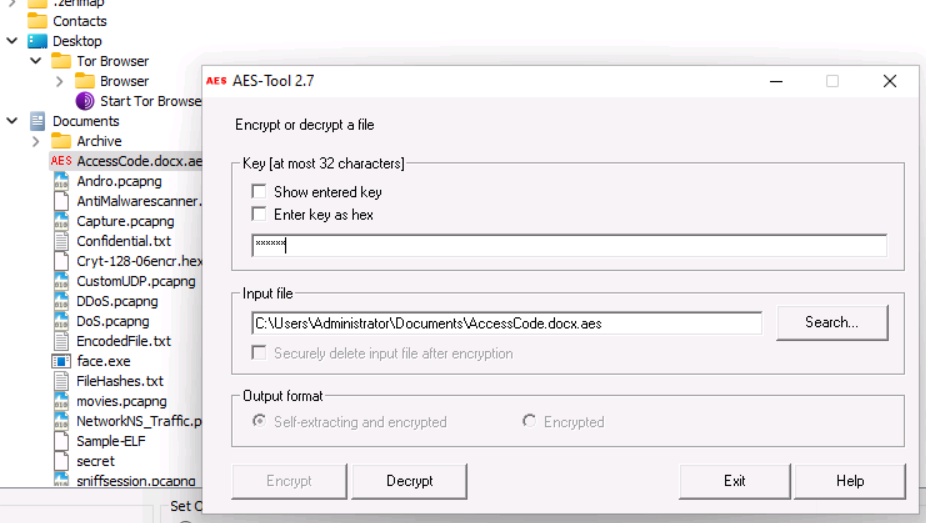
Answer: ECC-CSC-2006

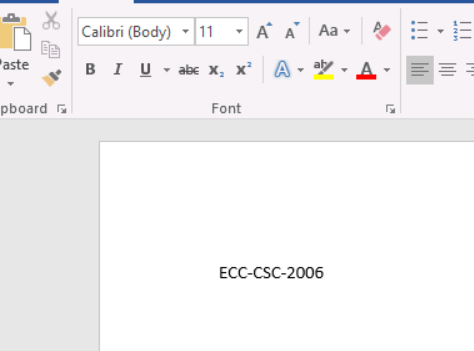




Doublle click on AccessCode.aes file and give password “qwerty” and click on decrypt

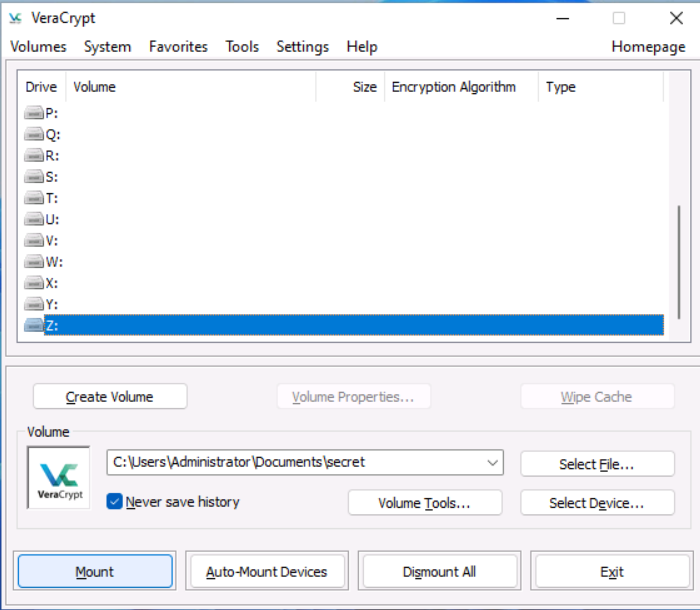
Make sure that both checkbox is unchecked. Then you will able to write the password.



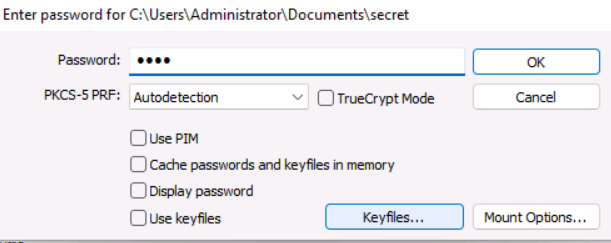


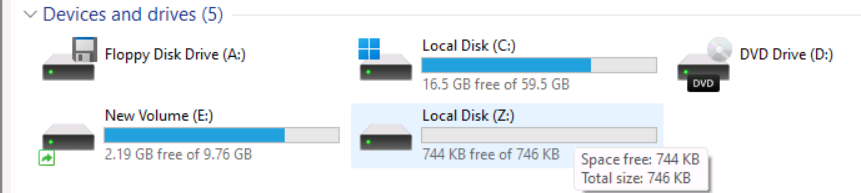
1. A VeraCrypt volume file "secret" is stored on the Document folder in the "EH Workstation – 2" machine. You are an ethical hacker working with CEHORG; you have been tasked to decrypt the encrypted volume and determine the number of files stored in the volume. (Hint: Password: test). (Format: N)

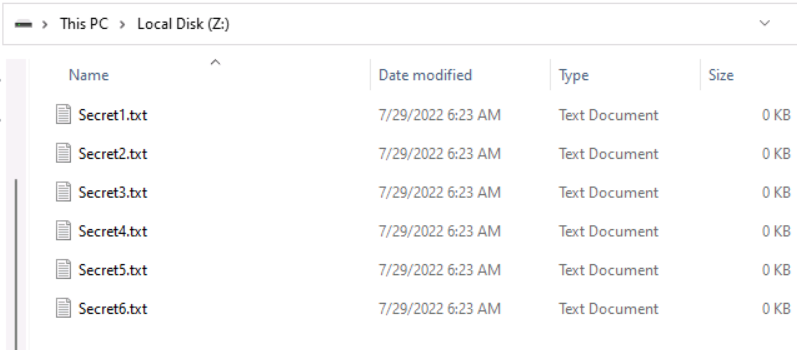
Answer: 6



Select the secret file and select any drive (Z:) and Click on mount. Give password test and OK

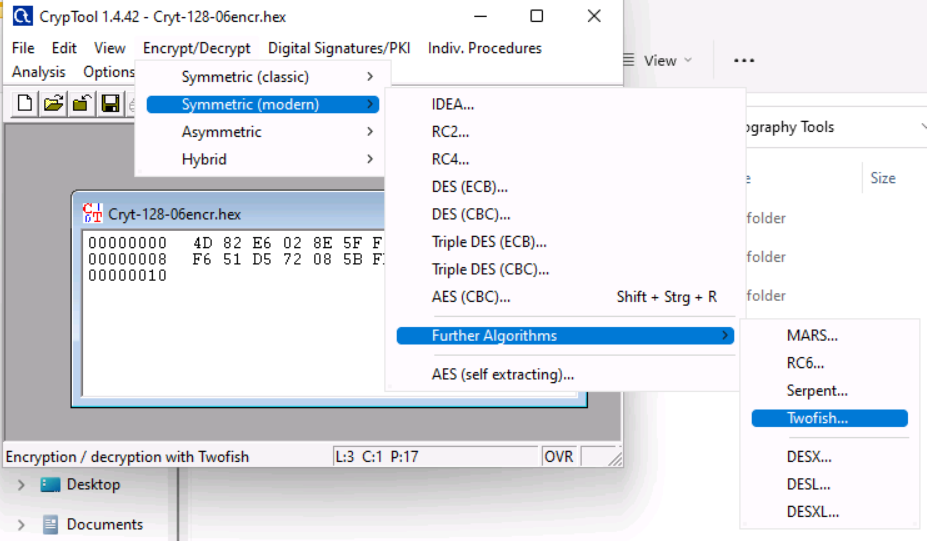






1. An attacker had sent a file cryt-128-06encr.hex containing ransom file password, which is located in documents folder of EH-workstation-2. You are assigned a task to decrypt the file using cryp tool. Perform cryptanalysis, Identify the algorithm used for file encryption and hidden text. Note: check filename for key length and hex characters. (Format: Aaaaaaa/\*\*aa\*\*aA\*a)

Answer: Twofish/@!ph@|tE\*t



After select Twofish write 06 06 in given box because filename has 128-06. And Decrypt

