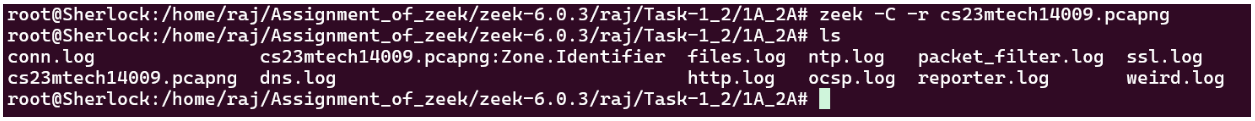
Assignment 8: Hands-on with Zeek

CS23MTECH14009

Task 1A: Collect network traffic (only packet headers up to MAC layer to reduce the size of pcap file) using tcpdump for wireshark on your personal laptop for 10 mins and show the source IP addresses that generated the most network traffic, organized in descending order using zeek-cut. Deliverables: pcap file generated and relevant zeek log files; A screenshot of zeek-cut and its options used for answering this query and the output generated.

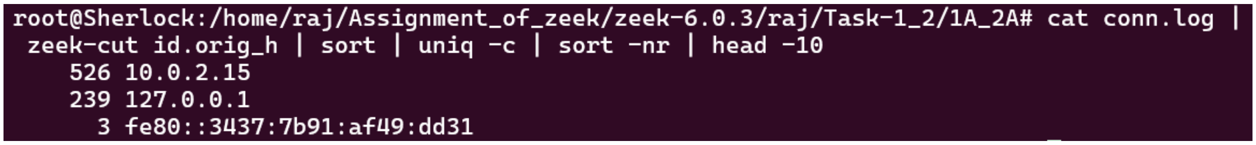
Solution : I have cs23mtech14009.pcapng in Task-1_2/1A_2A
I am going to apply zeek -C -r cs23mtech14009.pcapng
Were -r for the reading the input and -C is for configuration (without it showing checksum error)

By this command i am getting this log files



```
root@Sherlock:/home/raj/Assignment_of_zeek/zeek-6.0.3/raj/Task-1_2/1A_2A# zeek -C -r cs23mtech14009.pcapng
root@Sherlock:/home/raj/Assignment_of_zeek/zeek-6.0.3/raj/Task-1_2/1A_2A# ls
conn.log               cs23mtech14009.pcapng:Zone.Identifier  files.log  ntp.log   packet_filter.log  ssl.log
cs23mtech14009.pcapng  dns.log                                http.log   ocsp.log  reporter.log       weird.log
root@Sherlock:/home/raj/Assignment_of_zeek/zeek-6.0.3/raj/Task-1_2/1A_2A# 
```

After this i am applying the cat conn.log | zeek-cut id.orig_h | sort | uniq -c | sort -nr | head -10
Which takes a unique id.orig_h to sort it reverse order of frequency.
This gives me top source ip addresses here we can see 10.0.2.15 is top source ip address.



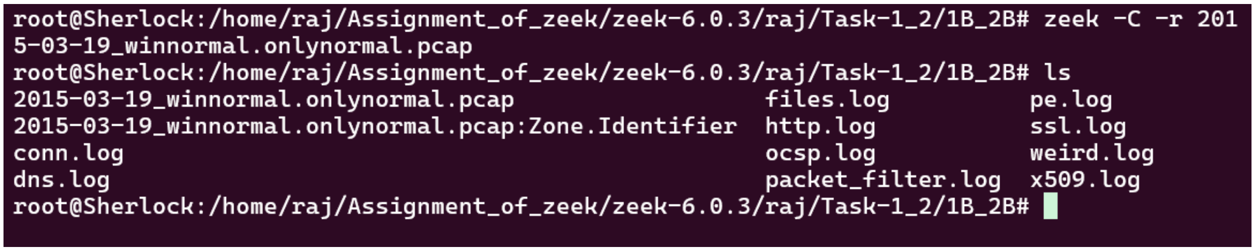
```
root@Sherlock:/home/raj/Assignment_of_zeek/zeek-6.0.3/raj/Task-1_2/1A_2A# cat conn.log |
 zeek-cut id.orig_h | sort | uniq -c | sort -nr | head -10
    526 10.0.2.15
    239 127.0.0.1
      3 fe80::3437:7b91:af49:dd31
```

Task 1B: Repeat Task 1A by using one of the pcap files from
https://www.stratosphereips.org/datasets-mixed or
https://www.honeynetproject.com/dataset.html
Deliverables: link of the pcap file used; A screenshot of zeek-cut and its options used for answering this query and the output generated.

Link of the winnormal.onlynormal.pcap is :
https://mcfp.felk.cvut.cz/publicDatasets/CTU-Mixed-Capture-5/2015-03-19_winnormal.onlynormal.pcap
Which is in the Task-1_2/1B_2B

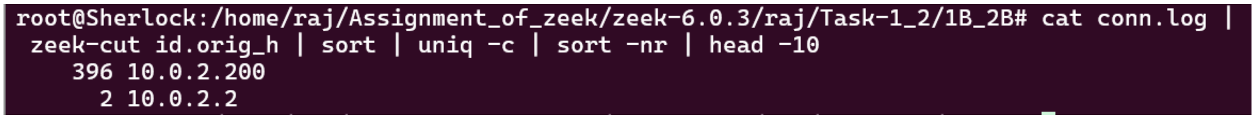
Solution :

By using zeek-C -r command i am getting following log files



```
root@Sherlock:/home/raj/Assignment_of_zeek/zeek-6.0.3/raj/Task-1_2/1B_2B# zeek -C -r 201
5-03-19_winnormal.onlynormal.pcap
root@Sherlock:/home/raj/Assignment_of_zeek/zeek-6.0.3/raj/Task-1_2/1B_2B# ls
2015-03-19_winnormal.onlynormal.pcap                  files.log          pe.log
2015-03-19_winnormal.onlynormal.pcap:Zone.Identifier  http.log           ssl.log
conn.log                                              ocsp.log           weird.log
dns.log                                               packet_filter.log  x509.log
root@Sherlock:/home/raj/Assignment_of_zeek/zeek-6.0.3/raj/Task-1_2/1B_2B# 
```

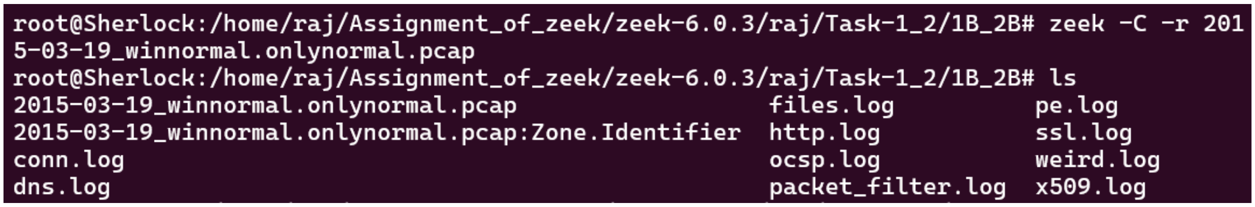
Here we can see 10.0.2.200 as top ip address



```
root@Sherlock:/home/raj/Assignment_of_zeek/zeek-6.0.3/raj/Task-1_2/1B_2B# cat conn.log |
 zeek-cut id.orig_h | sort | uniq -c | sort -nr | head -10
    396 10.0.2.200
      2 10.0.2.2
```

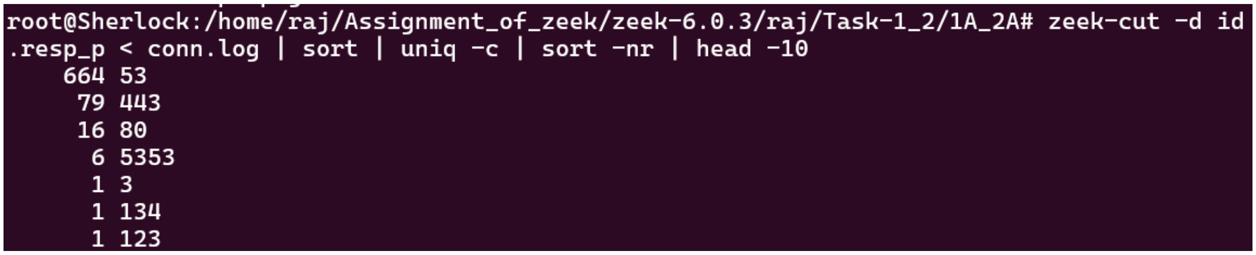
Task 2A: Show the 10 destination ports that received the most network traffic,organized in descending order using zeek-cut. Deliverables: Relevant zeek log files and a screenshot of zeek-cut and its options used for answering this query and the output generated.

Solution :
We have same log files same as Task 1A



```
root@Sherlock:/home/raj/Assignment_of_zeek/zeek-6.0.3/raj/Task-1_2/1B_2B# zeek -C -r 201
5-03-19_winnormal.onlynormal.pcap
root@Sherlock:/home/raj/Assignment_of_zeek/zeek-6.0.3/raj/Task-1_2/1B_2B# ls
2015-03-19_winnormal.onlynormal.pcap                  files.log          pe.log
2015-03-19_winnormal.onlynormal.pcap:Zone.Identifier  http.log           ssl.log
conn.log                                              ocsp.log           weird.log
dns.log                                               packet_filter.log  x509.log
```

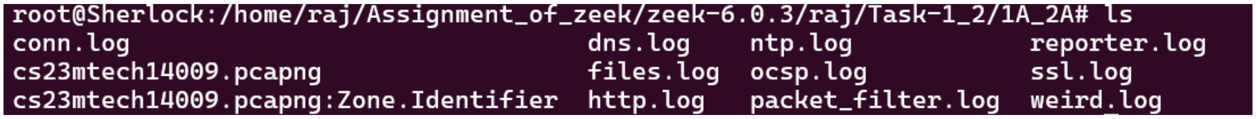
Here I have used the command given in the image which will give me top 10 destination ports that received the most network traffic, here we can see port 53 is having the highest frequency count.



```
root@Sherlock:/home/raj/Assignment_of_zeek/zeek-6.0.3/raj/Task-1_2/1A_2A# zeek-cut -d id
.resp_p < conn.log | sort | uniq -c | sort -nr | head -10
    664 53
     79 443
     16 80
      6 5353
      1 3
      1 134
      1 123
```

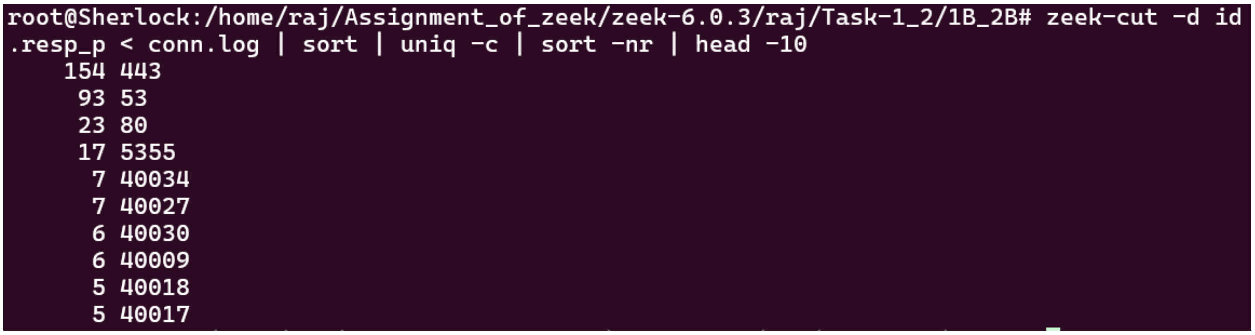
Task 2B: Repeat Task 2A by using one of the pcap files from https://www.stratosphereips.org/datasets-mixed or https://www.honeynetproject.com/dataset.html
Deliverables: link of the pcap file used for completing this task; Relevant zeek log files; A screenshot of zeek-cut and its options used for answering this query and the output generated.

Solution :



```
root@Sherlock:/home/raj/Assignment_of_zeek/zeek-6.0.3/raj/Task-1_2/1A_2A# ls
conn.log                                 dns.log    ntp.log            reporter.log
cs23mtech14009.pcapng                    files.log  ocsp.log           ssl.log
cs23mtech14009.pcapng:Zone.Identifier    http.log   packet_filter.log  weird.log
```

Here we can see port 443 as top result

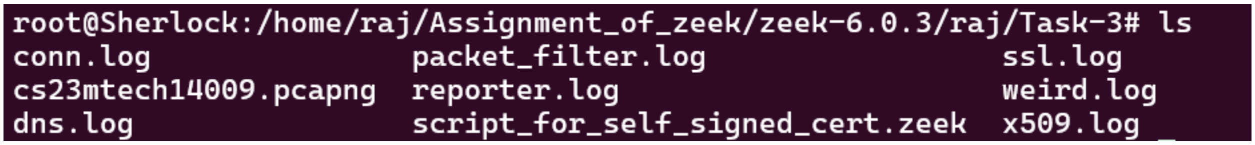


```
root@Sherlock:/home/raj/Assignment_of_zeek/zeek-6.0.3/raj/Task-1_2/1B_2B# zeek-cut -d id
.resp_p < conn.log | sort | uniq -c | sort -nr | head -10
    154 443
     93 53
     23 80
     17 5355
      7 40034
      7 40027
      6 40030
      6 40009
      5 40018
      5 40017
```

Task 3: Write a Zeek script to identify the Self Signed Certificate of the website: https://self-signed.badssl.com/

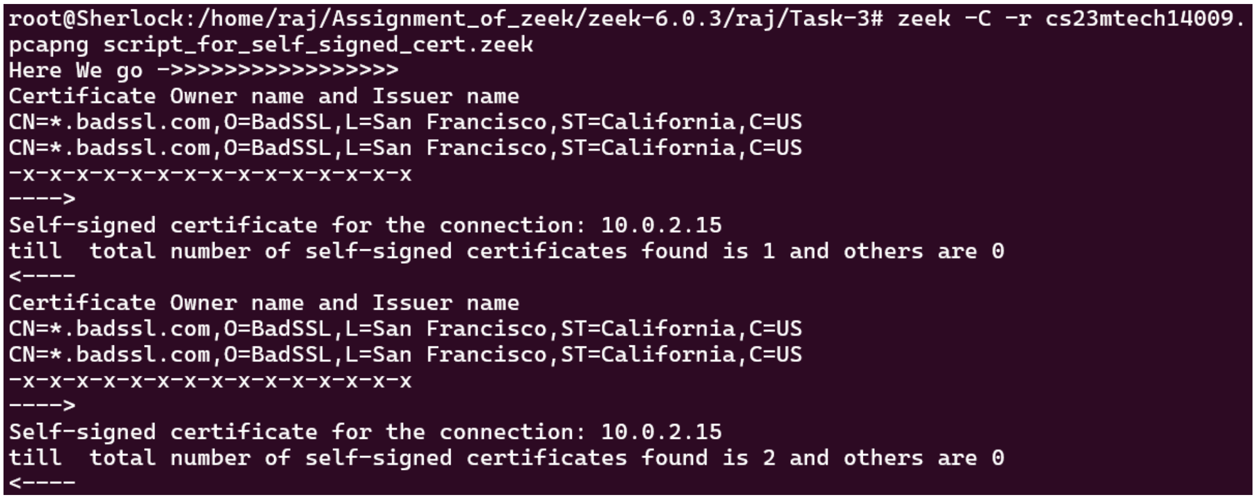
Solution :

Pcp file use cs23mtech14009.pcapng

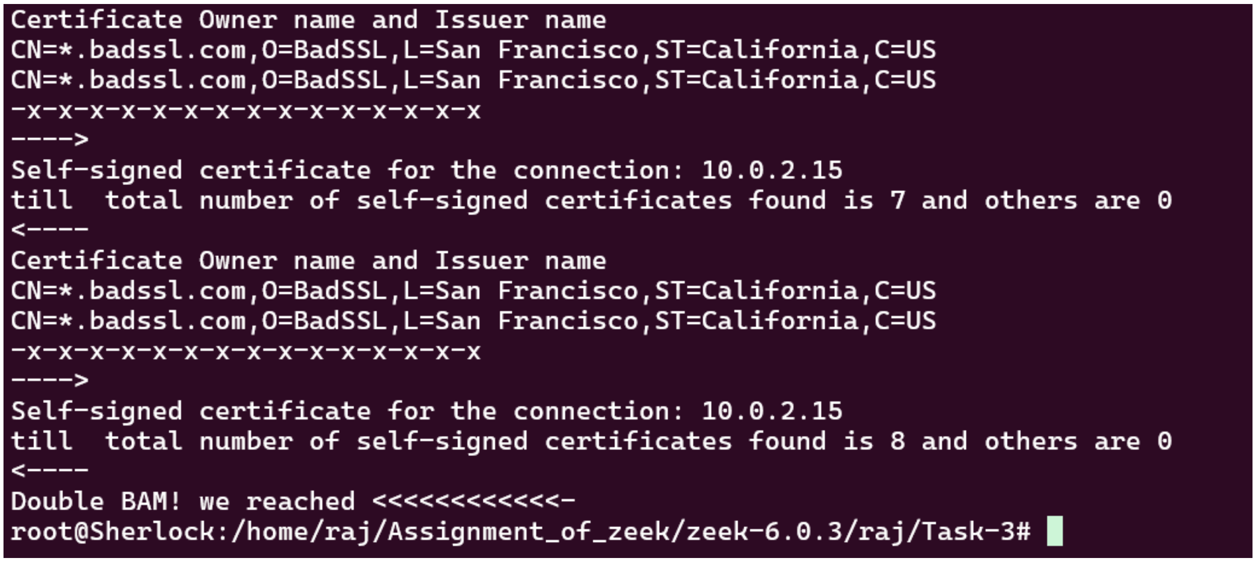


```
root@Sherlock:/home/raj/Assignment_of_zeek/zeek-6.0.3/raj/Task-3# ls
conn.log               packet_filter.log                ssl.log
cs23mtech14009.pcapng  reporter.log                     weird.log
dns.log                script_for_self_signed_cert.zeek x509.log
```

Here I am using an event ssl established which has the connection as argument and from the certificate chain get the first certificate and compare the subject name and the issuer name, if both are same then it is a self signed certificate. I am also printing num. Of certificates.



```
root@Sherlock:/home/raj/Assignment_of_zeek/zeek-6.0.3/raj/Task-3# zeek -C -r cs23mtech14009.
pcapng script_for_self_signed_cert.zeek
Here We go ->>>>>>>>>>>>>>>>>>
Certificate Owner name and Issuer name
CN=*.badssl.com,O=BadSSL,L=San Francisco,ST=California,C=US
CN=*.badssl.com,O=BadSSL,L=San Francisco,ST=California,C=US
-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x
---->
Self-signed certificate for the connection: 10.0.2.15
till  total number of self-signed certificates found is 1 and others are 0
<----
Certificate Owner name and Issuer name
CN=*.badssl.com,O=BadSSL,L=San Francisco,ST=California,C=US
CN=*.badssl.com,O=BadSSL,L=San Francisco,ST=California,C=US
-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x
---->
Self-signed certificate for the connection: 10.0.2.15
till  total number of self-signed certificates found is 2 and others are 0
<----
```



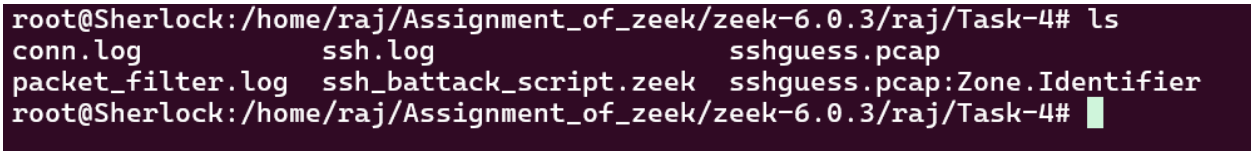
```
Certificate Owner name and Issuer name
CN=*.badssl.com,O=BadSSL,L=San Francisco,ST=California,C=US
CN=*.badssl.com,O=BadSSL,L=San Francisco,ST=California,C=US
-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x
---->
Self-signed certificate for the connection: 10.0.2.15
till  total number of self-signed certificates found is 7 and others are 0
<----
Certificate Owner name and Issuer name
CN=*.badssl.com,O=BadSSL,L=San Francisco,ST=California,C=US
CN=*.badssl.com,O=BadSSL,L=San Francisco,ST=California,C=US
-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x
---->
Self-signed certificate for the connection: 10.0.2.15
till  total number of self-signed certificates found is 8 and others are 0
<----
Double BAM! we reached <<<<<<<<<<<<-
root@Sherlock:/home/raj/Assignment_of_zeek/zeek-6.0.3/raj/Task-3#
```

Task 4: Write a Zeek script to identify the ssh brute force password attacks in the following pcap file. Print the hosts that are guessing ssh passwords along with your name and RollNo in the generated log.
https://github.com/bro/bro/raw/master/testing/btest/Traces/ssh/sshguess.pcap

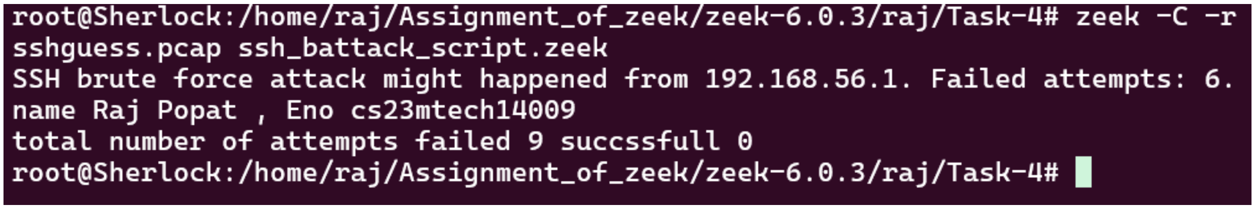
Solution :

Pcap file using is sshguess.pcap

Script name is ssh_battack_script.zeek



```
root@Sherlock:/home/raj/Assignment_of_zeek/zeek-6.0.3/raj/Task-4# ls
conn.log           ssh.log                    sshguess.pcap
packet_filter.log  ssh_battack_script.zeek    sshguess.pcap:Zone.Identifier
root@Sherlock:/home/raj/Assignment_of_zeek/zeek-6.0.3/raj/Task-4#
```



```
root@Sherlock:/home/raj/Assignment_of_zeek/zeek-6.0.3/raj/Task-4# zeek -C -r
sshguess.pcap ssh_battack_script.zeek
SSH brute force attack might happened from 192.168.56.1. Failed attempts: 6.
name Raj Popat , Eno cs23mtech14009
total number of attempts failed 9 succssfull 0
root@Sherlock:/home/raj/Assignment_of_zeek/zeek-6.0.3/raj/Task-4#
```

In this script first i am creating a map(in python like dictionary) which stores the ip address as key and number of unsuccessful attempts as value and using the ssh auth result which have the connection and authentication result and authentication attempts as argument were first i check the result if it is true remove the ip entry from the table then or increase the value of the attempts in table of respective ip. If it exceeds the threshold then printing the alert message.

PLAGIARISM STATEMENT <Include it in your report>

I certify that this assignment/report is my own work, based on my personal study and/or research and that I have acknowledged all material and sources used in its preparation, whether they be books, articles, reports, lecture notes, and any other kind of document, electronic or personal communication. I also certify that this assignment/report has not previously been submitted for assessment in any other course, except where specific permission has been granted from all course instructors involved, or at any other time in this course, and that I have not copied in part or whole or otherwise plagiarized the work of other students and/or persons. I pledge to uphold the principles of honesty and responsibility at CSE@IITH. In addition, I understand my responsibility to report honor violations by other students if I become aware of it.

Name: Popat Raj Ramehkumar
Date: 31/03/2024
Signature: CS23MTECH14009