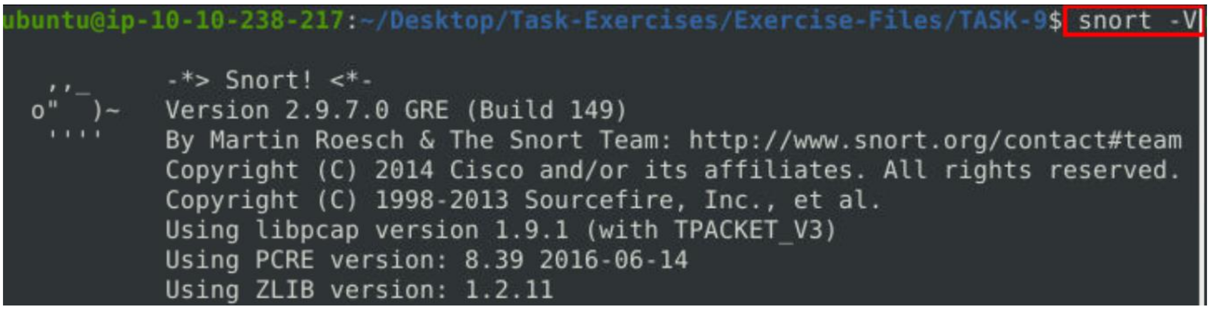
Name:Ramya Ajay

Roll No:CB.EN.P2CYS22004 Snort

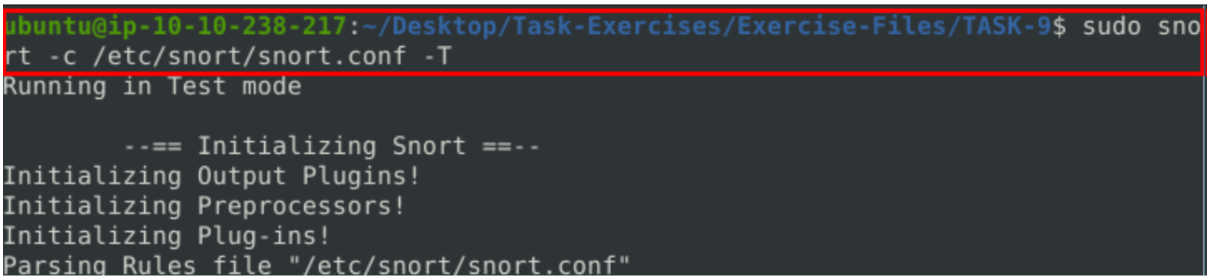
Snort Version check



```
ubuntu@ip-10-10-238-217:~/Desktop/Task-Exercises/Exercise-Files/TASK-9$ snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.7.0 GRE (Build 149)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.9.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11
```

- Checking configuration file is valid or not

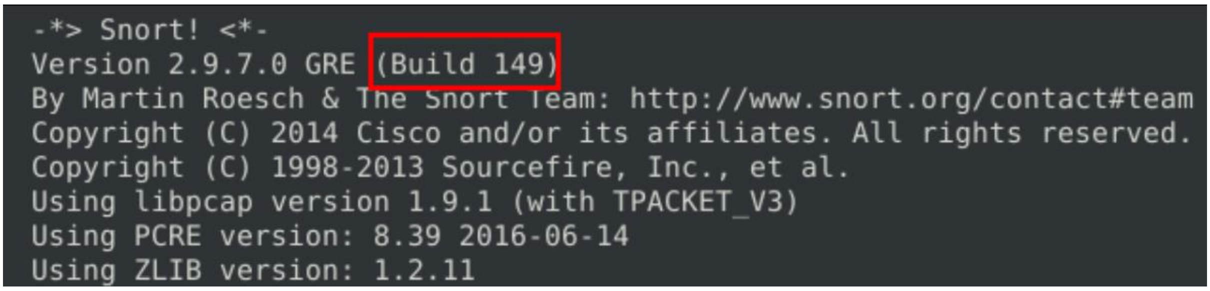


```
ubuntu@ip-10-10-238-217:~/Desktop/Task-Exercises/Exercise-Files/TASK-9$ sudo sno
rt -c /etc/snort/snort.conf -T
Running in Test mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
```

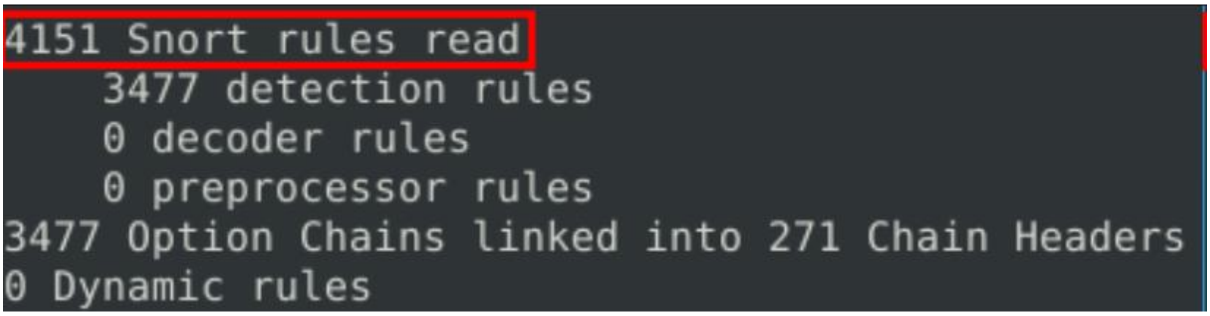
Task 4

- Run the Snort instance and check the build number.



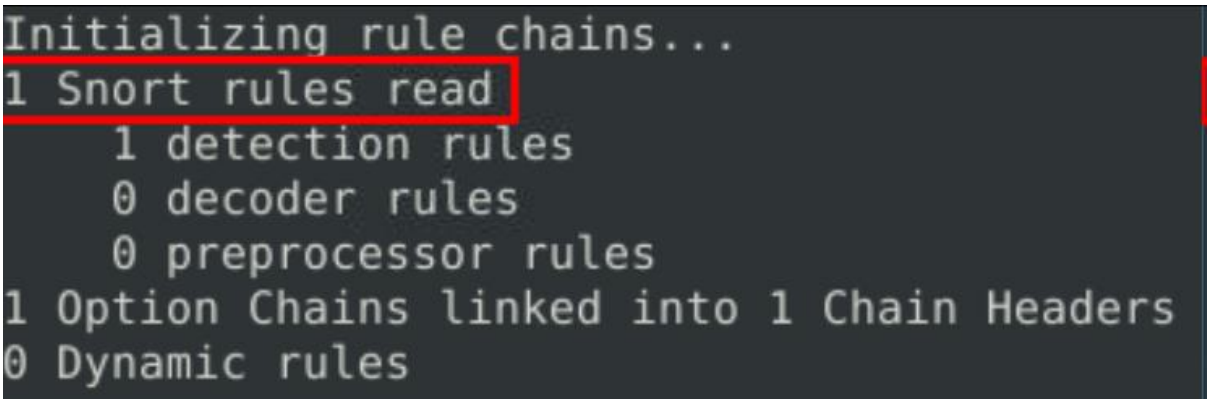
```
  -*> Snort! <*-
  Version 2.9.7.0 GRE (Build 149)
  By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
  Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
  Copyright (C) 1998-2013 Sourcefire, Inc., et al.
  Using libpcap version 1.9.1 (with TPACKET_V3)
  Using PCRE version: 8.39 2016-06-14
  Using ZLIB version: 1.2.11
```

- Test the current instance with "/etc/snort/snort.conf" file and check how many rules are loaded with the current build.



```
4151 Snort rules read
    3477 detection rules
    0 decoder rules
    0 preprocessor rules
3477 Option Chains linked into 271 Chain Headers
0 Dynamic rules
```

- Test the current instance with "/etc/snort/snortv2.conf" file and check how many rules are loaded with the current build.



```
Initializing rule chains...
1 Snort rules read
    1 detection rules
    0 decoder rules
    0 preprocessor rules
1 Option Chains linked into 1 Chain Headers
0 Dynamic rules
```

Task-6:Operation Mode 2: Packet Logger Mode

Investigate the traffic with the default configuration file with ASCII mode.

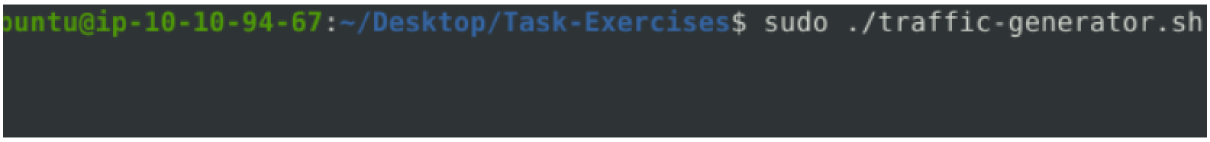
sudo snort -dev -K ASCII -l .

Execute the traffic generator script and choose "TASK-6 Exercise". Wait until the traffic ends, then stop the Snort instance. Now analyse the output summary and answer the question.

sudo ./traffic-generator.sh

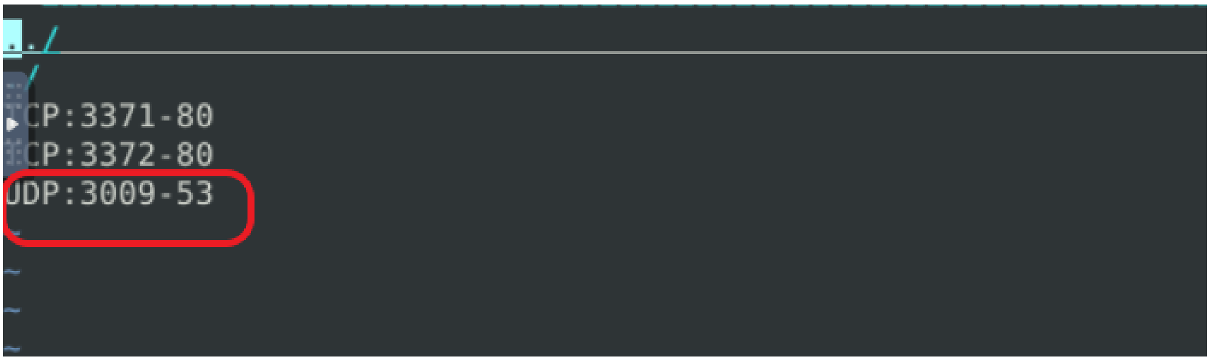
a) Now, you should have the logs in the current directory. Navigate to folder "145.254.160.237". What is the source port used to connect port 53?

- First we perform the traffic-generator and get the folders



```
buntu@ip-10-10-94-67:~/Desktop/Task-Exercises$ sudo ./traffic-generator.sh
```

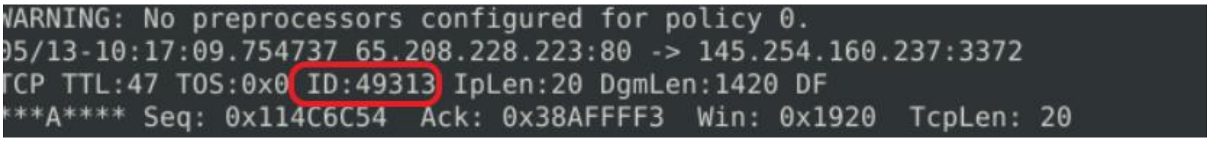
- Now we get into the file and read the port



```
../
/
CP:3371-80
CP:3372-80
JDP:3009-53
~
~
~
```

b) Read the snort.log file with Snort; what is the IP ID of the 10th packet?

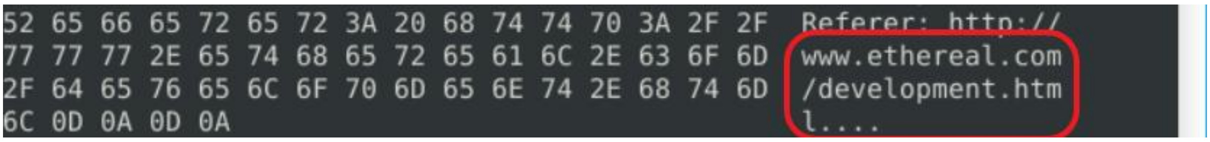
- Now we navigate into the 'Exercise-files' and select the 'TASK-6' file to get the snort.log.1640048004 to get the id of the 10th packet



```
WARNING: No preprocessors configured for policy 0.
05/13-10:17:09.754737 65.208.228.223:80 -> 145.254.160.237:3372
TCP TTL:47 TOS:0x0 ID:49313 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0x114C6C54  Ack: 0x38AFFFF3  Win: 0x1920  TcpLen: 20
```

c) Read the "snort.log.1640048004" file with Snort; what is the referer of the 4th packet?

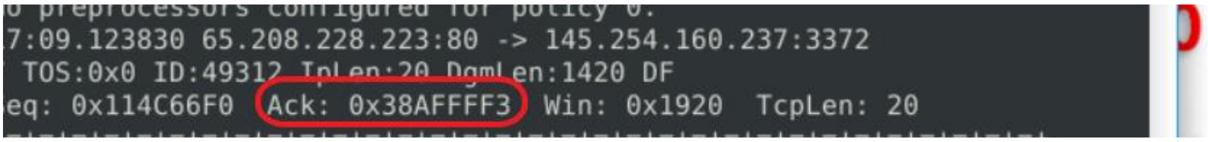
- When we give the command 'snort -r snort.log.1640048004 -n 4 -K'



```
52 65 66 65 72 65 72 3A 20 68 74 74 70 3A 2F 2F  Referer: http://
77 77 77 2E 65 74 68 65 72 65 61 6C 2E 63 6F 6D  www.ethereal.com
2F 64 65 76 65 6C 6F 70 6D 65 6E 74 2E 68 74 6D  /development.htm
6C 0D 0A 0D 0A                                   l....
```

d) Read the "snort.log.1640048004" file with Snort; what is the Ack number of the 8th packet?

- Now we give the command 'snort -r snort.log.1640048004 -n 8 -K'



```
o preprocessors configured for policy 0.
7:09.123830 65.208.228.223:80 -> 145.254.160.237:3372
 TOS:0x0 ID:49312 IpLen:20 DgmLen:1420 DF
eq: 0x114C66F0  Ack: 0x38AFFFF3  Win: 0x1920  TcpLen: 20
```