SNORT - Using Snort as a sniffer, logging the sniffed packets via logger mode and investigating individual packets

In this scenario I am a Junior SOC analyst with numerous tasks as seen below.

My task is to Investigate the traffic with the default configuration file with ASCII mode.

Then execute the traffic generator script and choose "TASK-6 Exercise". Wait until the traffic ends, then stop the Snort instance. And finally analyse the output summary and answer the questions.

I have broken up the command used in this task below to explain each section

“sudo snort -dev -K ASCII -l .”

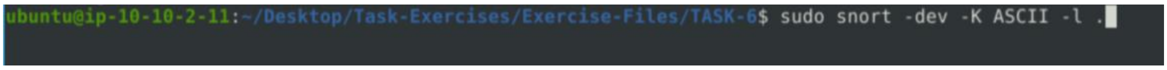
sudo: Execute the command with superuser privileges.

snort: The command itself, for running the Snort intrusion detection system.

-dev: Run in development mode. Development mode is used for testing and debugging.

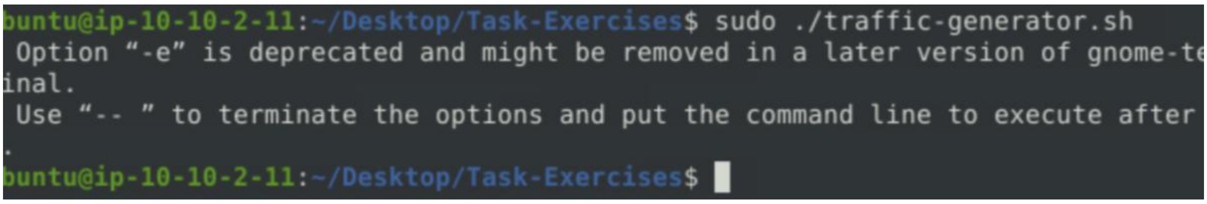
-K ASCII: This option specifies the output format for the generated logs and alerts. I

-l . : Specifies the output directory for generated logs and reports. In this case, the” . “ indicates the current directory where the command is being executed.



```
ubuntu@ip-10-10-2-11:~/Desktop/Task-Exercises/Exercise-Files/TASK-6$ sudo snort -dev -K ASCII -l .
```

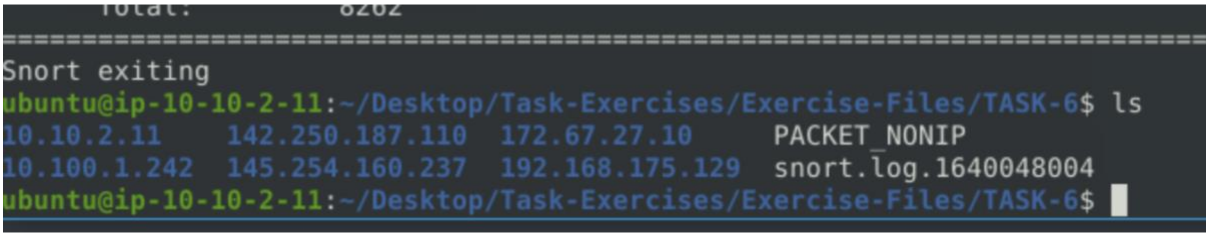
As requested I used the following command above whilst also using the traffic generator below.



```
buntu@ip-10-10-2-11:~/Desktop/Task-Exercises$ sudo ./traffic-generator.sh
 Option “-e” is deprecated and might be removed in a later version of gnome-te
inal.
 Use “-- ” to terminate the options and put the command line to execute after
.
buntu@ip-10-10-2-11:~/Desktop/Task-Exercises$ 
```

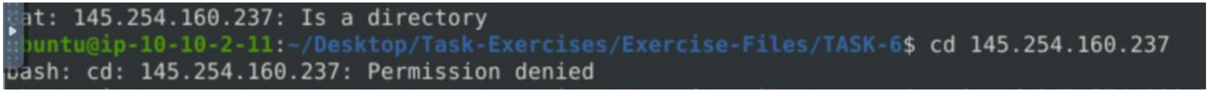
Question 1.Now, you should have the logs in the current directory. Navigate to folder "145.254.160.237". What is the source port used to connect port 53?

Once completed I reviewed the “TASK-6” folder and as you can see new logs were saved with folder “145.254.160.237" listed below.



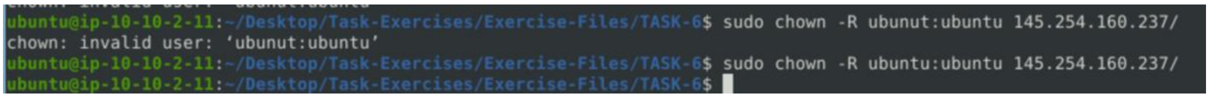
```
===============================================================================
Snort exiting
ubuntu@ip-10-10-2-11:~/Desktop/Task-Exercises/Exercise-Files/TASK-6$ ls
10.10.2.11     142.250.187.110  172.67.27.10     PACKET_NONIP
10.100.1.242   145.254.160.237  192.168.175.129  snort.log.1640048004
ubuntu@ip-10-10-2-11:~/Desktop/Task-Exercises/Exercise-Files/TASK-6$
```

I attempted opening the folder however permission was denied as seen below



```
cat: 145.254.160.237: Is a directory
ubuntu@ip-10-10-2-11:~/Desktop/Task-Exercises/Exercise-Files/TASK-6$ cd 145.254.160.237
bash: cd: 145.254.160.237: Permission denied
```

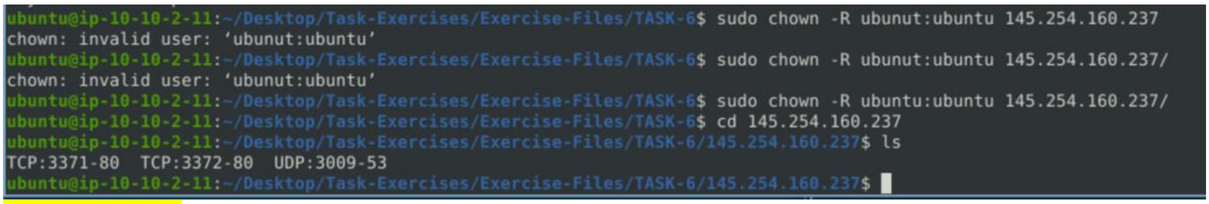
I then used the following command to alter permission rights for the folder in order to allow me access.



```
ubuntu@ip-10-10-2-11:~/Desktop/Task-Exercises/Exercise-Files/TASK-6$ sudo chown -R ubunut:ubuntu 145.254.160.237/
chown: invalid user: ‘ubunut:ubuntu’
ubuntu@ip-10-10-2-11:~/Desktop/Task-Exercises/Exercise-Files/TASK-6$ sudo chown -R ubuntu:ubuntu 145.254.160.237/
ubuntu@ip-10-10-2-11:~/Desktop/Task-Exercises/Exercise-Files/TASK-6$
```

This allowed me to open the folder and as you can see there were a total of 2 TCP packets and 1 DNS packet. The question above was “What is the source port used to connect port 53?

As you can see the answer is 3009



```
ubuntu@ip-10-10-2-11:~/Desktop/Task-Exercises/Exercise-Files/TASK-6$ sudo chown -R ubunut:ubuntu 145.254.160.237
chown: invalid user: ‘ubunut:ubuntu’
ubuntu@ip-10-10-2-11:~/Desktop/Task-Exercises/Exercise-Files/TASK-6$ sudo chown -R ubunut:ubuntu 145.254.160.237/
chown: invalid user: ‘ubunut:ubuntu’
ubuntu@ip-10-10-2-11:~/Desktop/Task-Exercises/Exercise-Files/TASK-6$ sudo chown -R ubuntu:ubuntu 145.254.160.237/
ubuntu@ip-10-10-2-11:~/Desktop/Task-Exercises/Exercise-Files/TASK-6$ cd 145.254.160.237
ubuntu@ip-10-10-2-11:~/Desktop/Task-Exercises/Exercise-Files/TASK-6/145.254.160.237$ ls
TCP:3371-80  TCP:3372-80  UDP:3009-53
ubuntu@ip-10-10-2-11:~/Desktop/Task-Exercises/Exercise-Files/TASK-6/145.254.160.237$
```

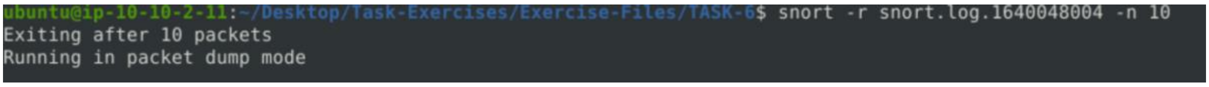
Answer: 3009

Question 2. Use snort.log.1640048004

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

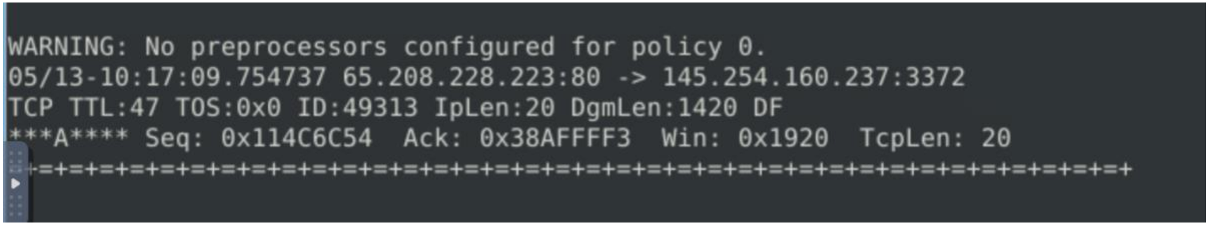
snort -r snort.log.1640048004 -n 10

I used the command as noted.



```
ubuntu@ip-10-10-2-11:~/Desktop/Task-Exercises/Exercise-Files/TASK-6$ snort -r snort.log.1640048004 -n 10
Exiting after 10 packets
Running in packet dump mode
```

As you can clearly see, in the center the IP ID is shown “49313”

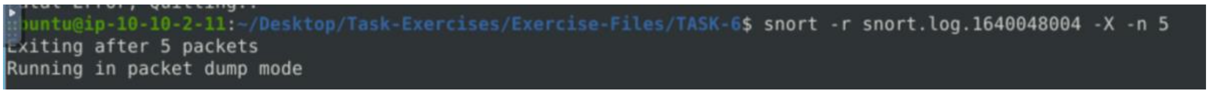


```
WARNING: No preprocessors configured for policy 0.
05/13-10:17:09.754737 65.208.228.223:80 -> 145.254.160.237:3372
TCP TTL:47 TOS:0x0 ID:49313 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0x114C6C54  Ack: 0x38AFFFF3  Win: 0x1920  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+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

Answer: 49313

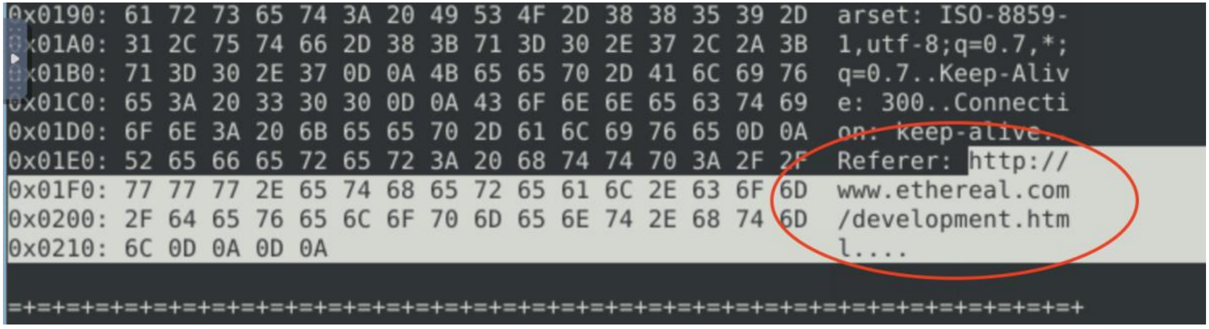
Question 3. Read the "snort.log.1640048004" file with Snort; what is the referer of the 4th packet?

Originally when analysing the packet I was unable to find the “referer” until I decided to change the parameter in the command to “-X” which provides a more in depth analysis of each packet. Furthermore I added “-n 5” to only provide the first 5 packets in order to keep the list short.



```
buntu@ip-10-10-2-11:~/Desktop/Task-Exercises/Exercise-Files/TASK-6$ snort -r snort.log.1640048004 -X -n 5
Exiting after 5 packets
Running in packet dump mode
```

From there I was able to find the referer as highlighted below in the 4th packet



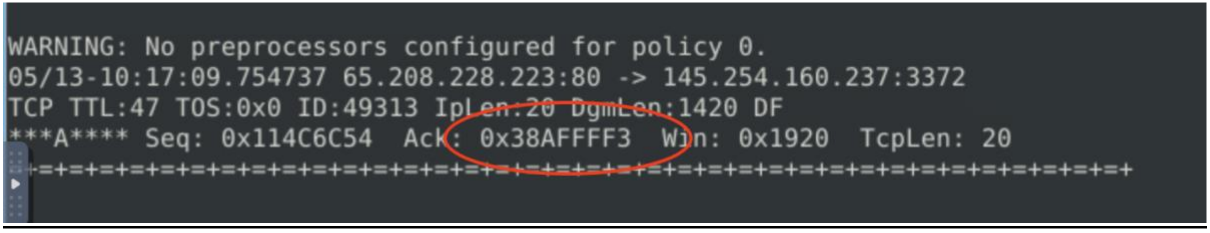
```
0x0190: 61 72 73 65 74 3A 20 49 53 4F 2D 38 38 35 39 2D  arset: ISO-8859-
0x01A0: 31 2C 75 74 66 2D 38 3B 71 3D 30 2E 37 2C 2A 3B  1,utf-8;q=0.7,*;
0x01B0: 71 3D 30 2E 37 0D 0A 4B 65 65 70 2D 41 6C 69 76  q=0.7..Keep-Aliv
0x01C0: 65 3A 20 33 30 30 0D 0A 43 6F 6E 6E 65 63 74 69  e: 300..Connecti
0x01D0: 6F 6E 3A 20 6B 65 65 70 2D 61 6C 69 76 65 0D 0A  on: keep-alive..
0x01E0: 52 65 66 65 72 65 72 3A 20 68 74 74 70 3A 2F 2F  Referer: http://
0x01F0: 77 77 77 2E 65 74 68 65 72 65 61 6C 2E 63 6F 6D  www.ethereal.com
0x0200: 2F 64 65 76 65 6C 6F 70 6D 65 6E 74 2E 68 74 6D  /development.htm
0x0210: 6C 0D 0A 0D 0A                                   l....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Answer: http://www.ethereal.com/development.html

Question 4. Read the "snort.log.1640048004" file with Snort; what is the Ack number of the 8th packet?

Answer is highlighted in the screenshot below

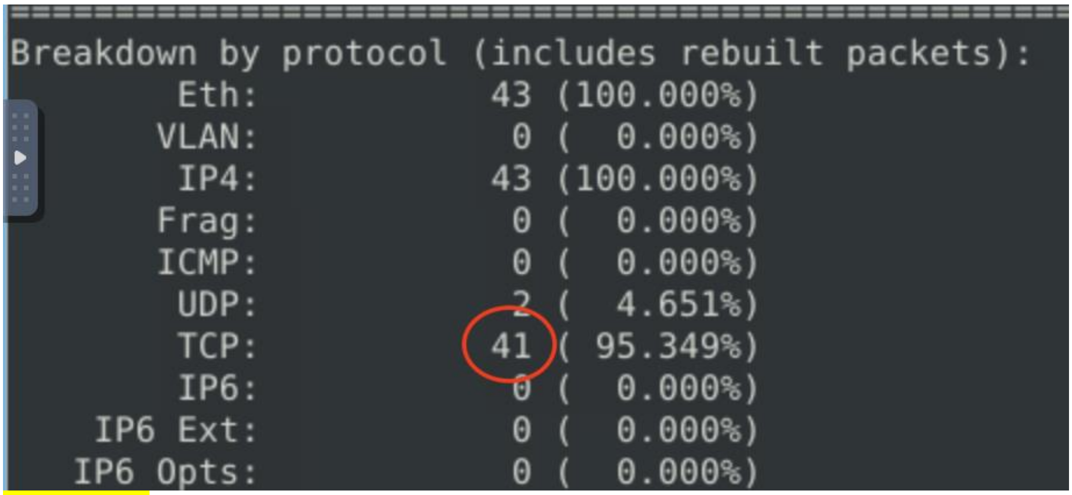


```
WARNING: No preprocessors configured for policy 0.
05/13-10:17:09.754737 65.208.228.223:80 -> 145.254.160.237:3372
TCP TTL:47 TOS:0x0 ID:49313 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0x114C6C54  Ack: 0x38AFFFF3  Win: 0x1920  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+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

Answer: 0x38AFFFF3

Question 5. Read the "snort.log.1640048004" file with Snort; what is the number of the "TCP port 80" packets?

As the original command only provided the first 10 packets I had to remove “-n 10” which provided all the packets from the log. The screen shot below is from the summary.



```
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:           43 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:           43 (100.000%)
       Frag:            0 (  0.000%)
       ICMP:            0 (  0.000%)
        UDP:            2 (  4.651%)
        TCP:           41 ( 95.349%)
        IP6:            0 (  0.000%)
    IP6 Ext:            0 (  0.000%)
   IP6 Opts:            0 (  0.000%)
```

Answer: 41