JHU SU20 IDS Module 4 Assignment

Audrey Long

06/20/2020

1. Introduction and "Testing Data" sections to get a feel for the experiment:
https://www.ll.mit.edu/r-d/datasets/1999-darpaintrusion-detection-eva
This week we’re going to look at research conducted by the Air Force Research Lab that tried to classify attacks against actual Air Force networks. Start by reading the "Overview", "Training Data",luation-dataset . You'll see that 3 weeks of training data and 2 weeks of test data were given to the participants. We'll be working with the Fourth week (Week 4) Monday data for this assignment.

2. Downloading the Data
Once you’ve read the introduction, please download the following ZIP file, which contains an actual ”packet dump” of data from the experiment, to your Ubuntu VM. Note this is the Week 4 Monday testing data. It contains normal background traffic with a smattering of ”cyber events” that you’ll be searching for in this assignment:

The TCPDump file should end up in your ’Downloads’ directory; open a Terminal window, navigate to your directory using the ’cd’ command and unzip the file using the ’gunzip’ command.

3. Ground Truth
You’ll hear the term ”ground truth” a lot when examining cyber-attacks. Ground truth simply refers to a record of the actual malicious events that happened. It does not include false positive, etc., it ONLY contains the actual malicious occurrences. Of course, it’s not possible to know ground truth ahead of time because we never know how/when we might be attacked, but the MIT LL page provides a ground truth file for this exercise.

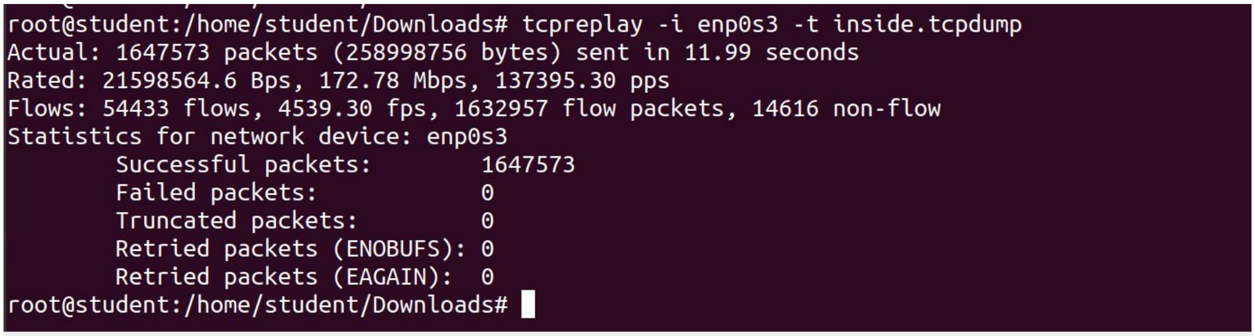
In your write-up, please provide a link to the ground truth file and download it to your VM. Also, how many attacks occurred in Week 4?

4. Examining the PCAP data using Snort. Next, open a Terminal window in your Ubuntu VM.

Use Snort to ingest the file directly. Please provide screenshots of the commands before you run them and after they complete displaying the results of the Snort analysis.

Please also explain each command line option you decide to use in your Snort command.
How many alerts did you receive when scanning the file locally?
Finally, you’ll notice the timestamps of the attacks in the ground truth file differ from the timestamps in the Snort alerts. What causes this?

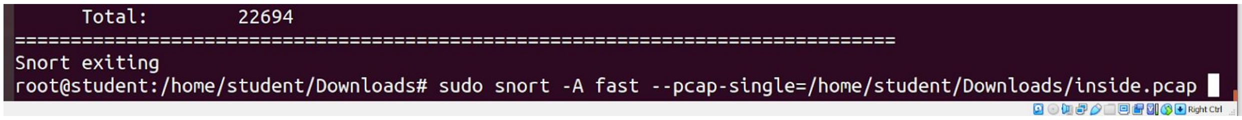
Ingesting the snort data was fairly straight forward, the websites
https://archive.ll.mit.edu/ideval/files/master-listfile-condensed.txt
https://archive.ll.mit.edu/ideval/files/master_identifications.list
provided the actual data presented from week 4 findings from the MIT Lincoln Labs findings. The following analysis will provide more insights from findings we can extract from pcap files using Snort and other command line tools.



```
root@student:/home/student/Downloads# tcpreplay -i enp0s3 -t inside.tcpdump
Actual: 1647573 packets (258998756 bytes) sent in 11.99 seconds
Rated: 21598564.6 Bps, 172.78 Mbps, 137395.30 pps
Flows: 54433 flows, 4539.30 fps, 1632957 flow packets, 14616 non-flow
Statistics for network device: enp0s3
        Successful packets:        1647573
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
root@student:/home/student/Downloads# 
```

Figure 1: tcp replay on the inside.tcpdump file

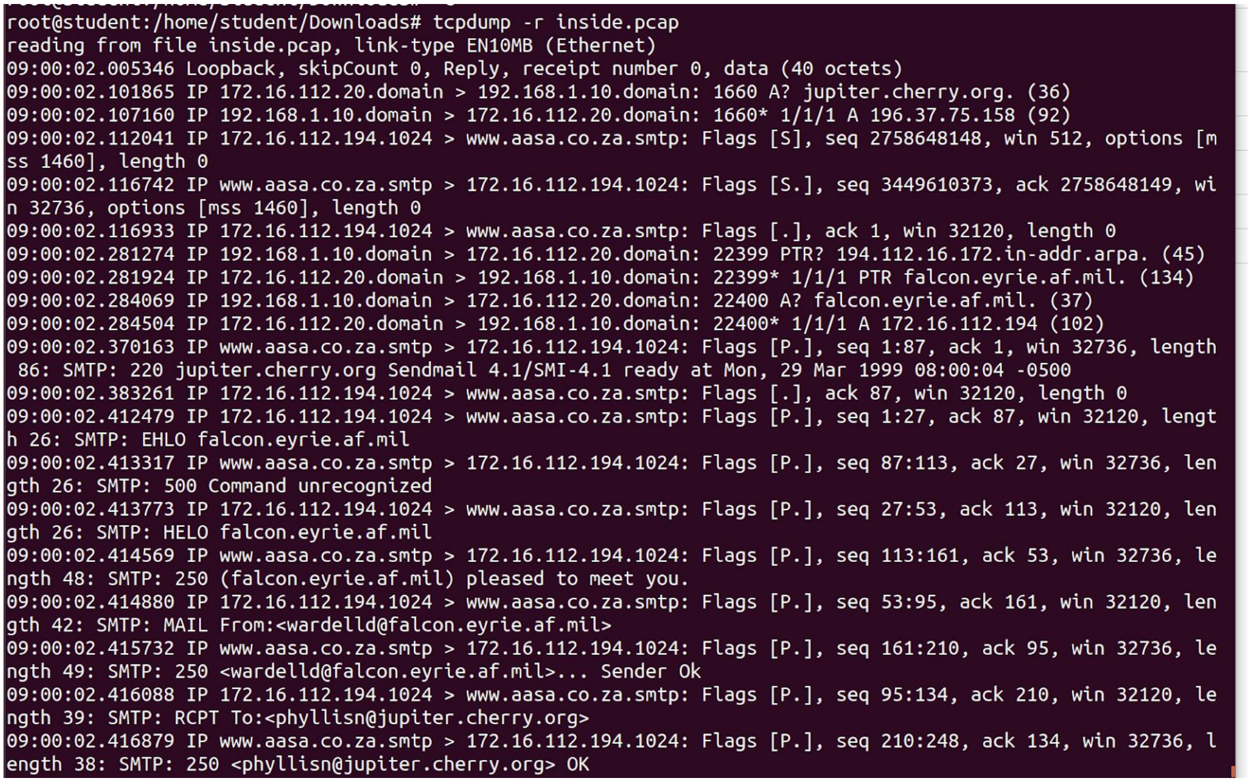
Figure one above shows the tcp replay along with how many successful packets were retrieved from the pcap file. The command "-i" is the client to server interface primary traffic output interface. The command "-t" says to replay packets as fast as possible. This option must not appear in combination with any of the following options: mbps, multiplier, pps, oneatatime.



```
     Total:        22694
===============================================================================
Snort exiting
root@student:/home/student/Downloads# sudo snort -A fast --pcap-single=/home/student/Downloads/inside.pcap 
```

Figure 2: snort reading pcap file.

The command above shows the following options that have been run with snort -A alert-mode Alert using the specified *alert-mode.* Valid alert modes include fast, full, none, and unsock. --pcap-file=*file* File that contains a list of pcaps to read. Can specify path to pcap or directory to recurse to get pcaps.



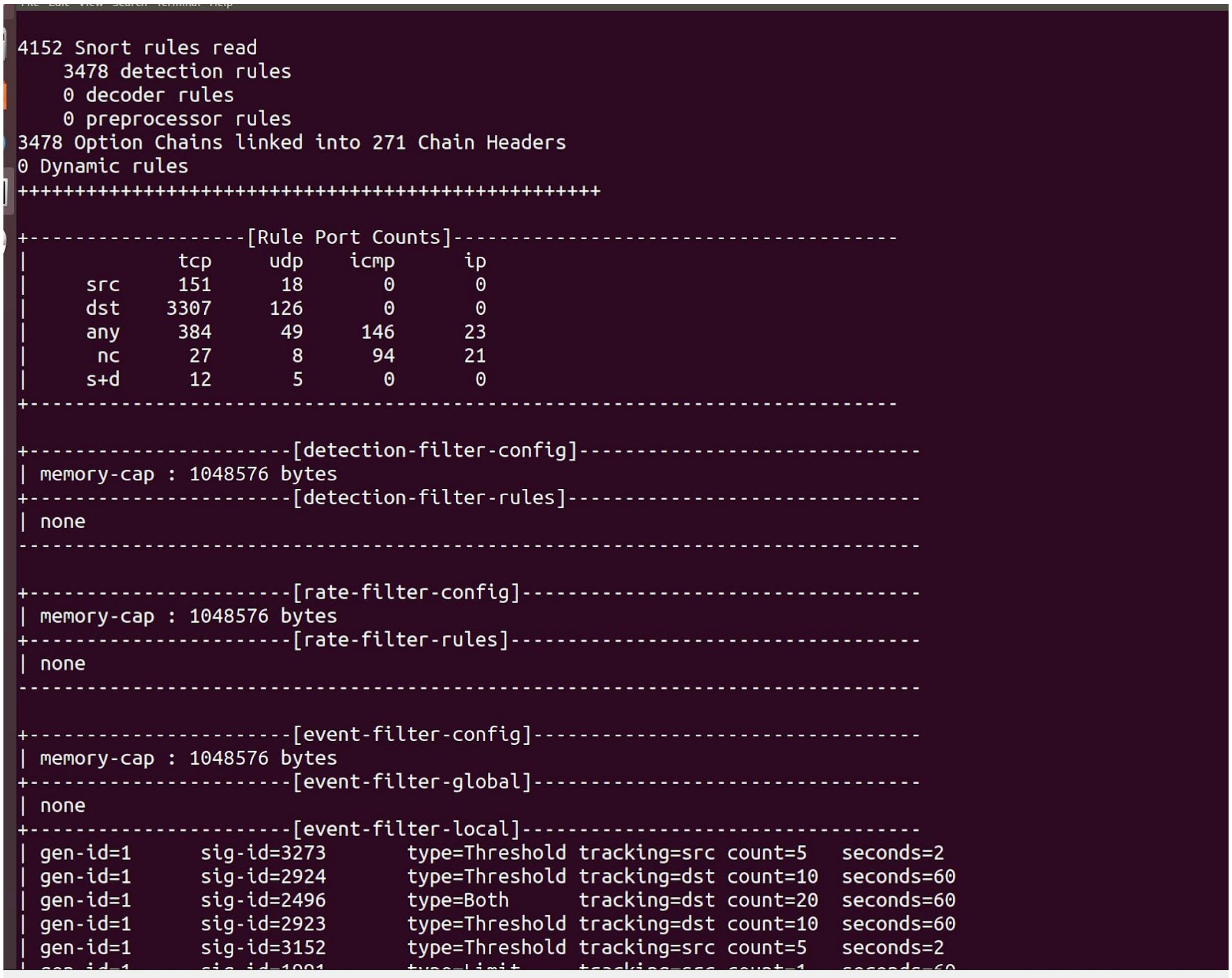
```
root@student:/home/student/Downloads# tcpdump -r inside.pcap
reading from file inside.pcap, link-type EN10MB (Ethernet)
09:00:02.005346 Loopback, skipCount 0, Reply, receipt number 0, data (40 octets)
09:00:02.101865 IP 172.16.112.20.domain > 192.168.1.10.domain: 1660 A? jupiter.cherry.org. (36)
09:00:02.107160 IP 192.168.1.10.domain > 172.16.112.20.domain: 1660* 1/1/1 A 196.37.75.158 (92)
09:00:02.112041 IP 172.16.112.194.1024 > www.aasa.co.za.smtp: Flags [S], seq 2758648148, win 512, options [m
ss 1460], length 0
09:00:02.116742 IP www.aasa.co.za.smtp > 172.16.112.194.1024: Flags [S.], seq 3449610373, ack 2758648149, wi
n 32736, options [mss 1460], length 0
09:00:02.116933 IP 172.16.112.194.1024 > www.aasa.co.za.smtp: Flags [.], ack 1, win 32120, length 0
09:00:02.281274 IP 192.168.1.10.domain > 172.16.112.20.domain: 22399 PTR? 194.112.16.172.in-addr.arpa. (45)
09:00:02.281924 IP 172.16.112.20.domain > 192.168.1.10.domain: 22399* 1/1/1 PTR falcon.eyrie.af.mil. (134)
09:00:02.284069 IP 192.168.1.10.domain > 172.16.112.20.domain: 22400 A? falcon.eyrie.af.mil. (37)
09:00:02.284504 IP 172.16.112.20.domain > 192.168.1.10.domain: 22400* 1/1/1 A 172.16.112.194 (102)
09:00:02.370163 IP www.aasa.co.za.smtp > 172.16.112.194.1024: Flags [P.], seq 1:87, ack 1, win 32736, length
 86: SMTP: 220 jupiter.cherry.org Sendmail 4.1/SMI-4.1 ready at Mon, 29 Mar 1999 08:00:04 -0500
09:00:02.383261 IP 172.16.112.194.1024 > www.aasa.co.za.smtp: Flags [.], ack 87, win 32120, length 0
09:00:02.412479 IP 172.16.112.194.1024 > www.aasa.co.za.smtp: Flags [P.], seq 1:27, ack 87, win 32120, lengt
h 26: SMTP: EHLO falcon.eyrie.af.mil
09:00:02.413317 IP www.aasa.co.za.smtp > 172.16.112.194.1024: Flags [P.], seq 87:113, ack 27, win 32736, len
gth 26: SMTP: 500 Command unrecognized
09:00:02.413773 IP 172.16.112.194.1024 > www.aasa.co.za.smtp: Flags [P.], seq 27:53, ack 113, win 32120, len
gth 26: SMTP: HELO falcon.eyrie.af.mil
09:00:02.414569 IP www.aasa.co.za.smtp > 172.16.112.194.1024: Flags [P.], seq 113:161, ack 53, win 32736, le
ngth 48: SMTP: 250 (falcon.eyrie.af.mil) pleased to meet you.
09:00:02.414880 IP 172.16.112.194.1024 > www.aasa.co.za.smtp: Flags [P.], seq 53:95, ack 161, win 32120, len
gth 42: SMTP: MAIL From:<wardelld@falcon.eyrie.af.mil>
09:00:02.415732 IP www.aasa.co.za.smtp > 172.16.112.194.1024: Flags [P.], seq 161:210, ack 95, win 32736, le
ngth 49: SMTP: 250 <wardelld@falcon.eyrie.af.mil>... Sender Ok
09:00:02.416088 IP 172.16.112.194.1024 > www.aasa.co.za.smtp: Flags [P.], seq 95:134, ack 210, win 32120, le
ngth 39: SMTP: RCPT To:<phyllisn@jupiter.cherry.org>
09:00:02.416879 IP www.aasa.co.za.smtp > 172.16.112.194.1024: Flags [P.], seq 210:248, ack 134, win 32736, l
ength 38: SMTP: 250 <phyllisn@jupiter.cherry.org> OK
```

Figure 3: tcpdump on the inside.pcap file

The command above demonstrates the tcpdump on the inside.pcap file where the **-r** flag causes it to read from a saved packet file. This command literally dumps the contents of the pcap file onto the console,it's a bit difficult to see all the data fly by on the console, it would be wise to pipe out the contents to a file.

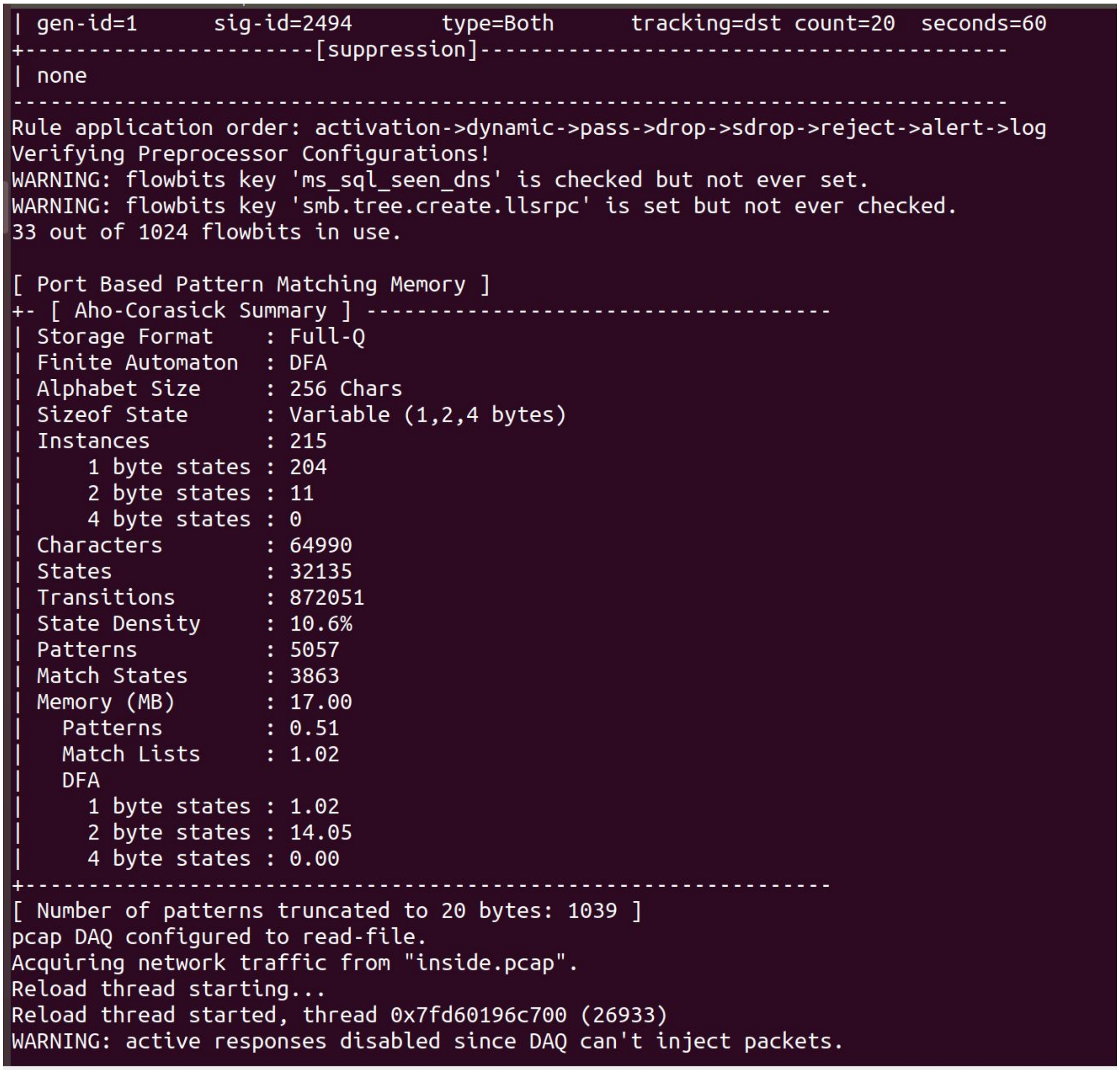
The report below (snort snip 1 - 7) was generated as a snort file using the command "snort -c /etc/snort/snort.conf -r inside.pcap" which will read the file inside.pcap and process it though all of your snort rules according to your snort_pcap.conf file. The Report generated is very detailed and I thought the data looked relevant enough to copy and paste out. Looking at the parameters passed into the command: -c config-file Use the rules located in file *config-file.* -r tcpdump-file

> Read the tcpdump-formatted file tcpdump-file. This will cause
> Snort to read and process the file fed to it. This is useful
> if, for instance, you've got a bunch of SHADOW files that you
> want to process for content, or even if you've got a bunch of
> reassembled packet fragments which have been written into a tcp-
> dump formatted file.



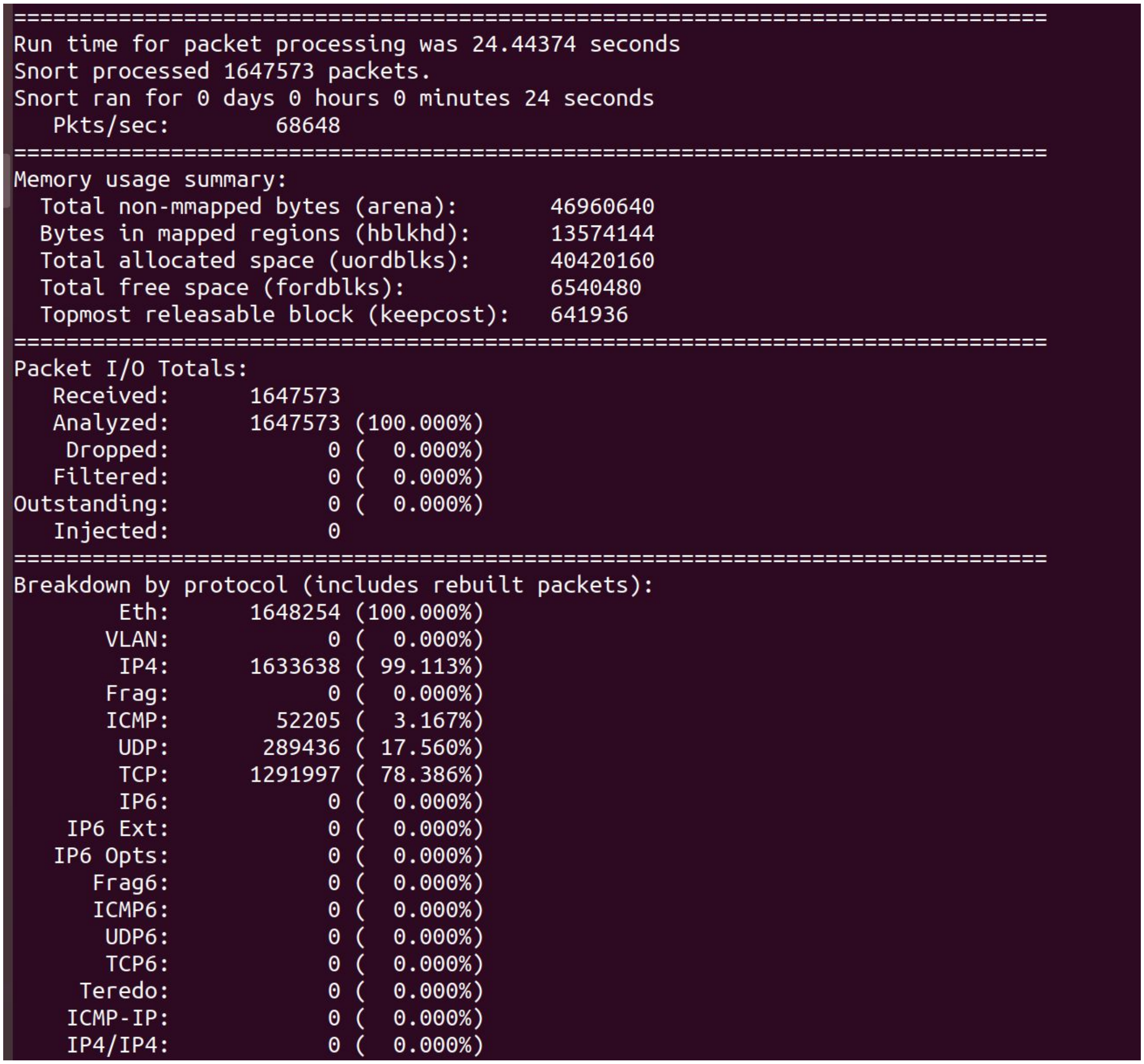
```
4152 Snort rules read
    3478 detection rules
    0 decoder rules
    0 preprocessor rules
3478 Option Chains linked into 271 Chain Headers
0 Dynamic rules
+++++++++++++++++++++++++++++++++++++++++++++++++++

+-------------------[Rule Port Counts]---------------------------------------
|             tcp     udp    icmp      ip
|     src     151      18       0       0
|     dst    3307     126       0       0
|     any     384      49     146      23
|      nc      27       8      94      21
|     s+d      12       5       0       0
+----------------------------------------------------------------------------

+-----------------------[detection-filter-config]------------------------------
| memory-cap : 1048576 bytes
+-----------------------[detection-filter-rules]-------------------------------
| none
-------------------------------------------------------------------------------

+-----------------------[rate-filter-config]-----------------------------------
| memory-cap : 1048576 bytes
+-----------------------[rate-filter-rules]------------------------------------
| none
-------------------------------------------------------------------------------

+-----------------------[event-filter-config]----------------------------------
| memory-cap : 1048576 bytes
+-----------------------[event-filter-global]----------------------------------
| none
+-----------------------[event-filter-local]-----------------------------------
| gen-id=1      sig-id=3273       type=Threshold tracking=src count=5   seconds=2
| gen-id=1      sig-id=2924       type=Threshold tracking=dst count=10  seconds=60
| gen-id=1      sig-id=2496       type=Both      tracking=dst count=20  seconds=60
| gen-id=1      sig-id=2923       type=Threshold tracking=dst count=10  seconds=60
| gen-id=1      sig-id=3152       type=Threshold tracking=src count=5   seconds=2
| gen-id=1      sig-id=1991       type=Limit     tracking=src count=1   seconds=60
```

Snort file snip 1



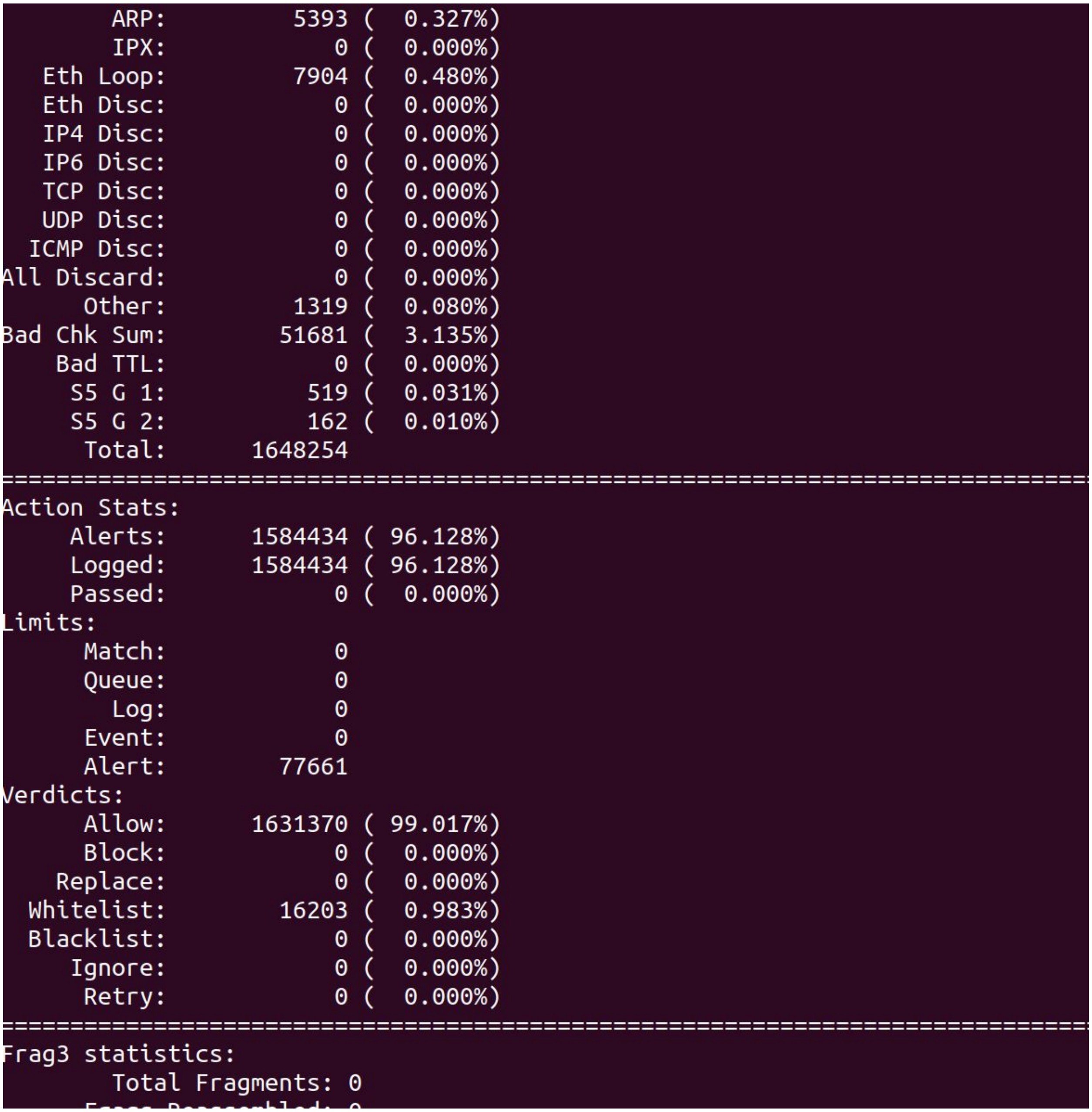
```
| gen-id=1      sig-id=2494       type=Both      tracking=dst count=20  seconds=60
+-----------------------[suppression]------------------------------------------
| none
-------------------------------------------------------------------------------
Rule application order: activation->dynamic->pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!
WARNING: flowbits key 'ms_sql_seen_dns' is checked but not ever set.
WARNING: flowbits key 'smb.tree.create.llsrpc' is set but not ever checked.
33 out of 1024 flowbits in use.

[ Port Based Pattern Matching Memory ]
+- [ Aho-Corasick Summary ] -------------------------------------
| Storage Format    : Full-Q
| Finite Automaton  : DFA
| Alphabet Size     : 256 Chars
| Sizeof State      : Variable (1,2,4 bytes)
| Instances         : 215
|     1 byte states : 204
|     2 byte states : 11
|     4 byte states : 0
| Characters        : 64990
| States            : 32135
| Transitions       : 872051
| State Density     : 10.6%
| Patterns          : 5057
| Match States      : 3863
| Memory (MB)       : 17.00
|   Patterns        : 0.51
|   Match Lists     : 1.02
|   DFA
|     1 byte states : 1.02
|     2 byte states : 14.05
|     4 byte states : 0.00
+----------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 1039 ]
pcap DAQ configured to read-file.
Acquiring network traffic from "inside.pcap".
Reload thread starting...
Reload thread started, thread 0x7fd60196c700 (26933)
WARNING: active responses disabled since DAQ can't inject packets.
```

Snort snip 2



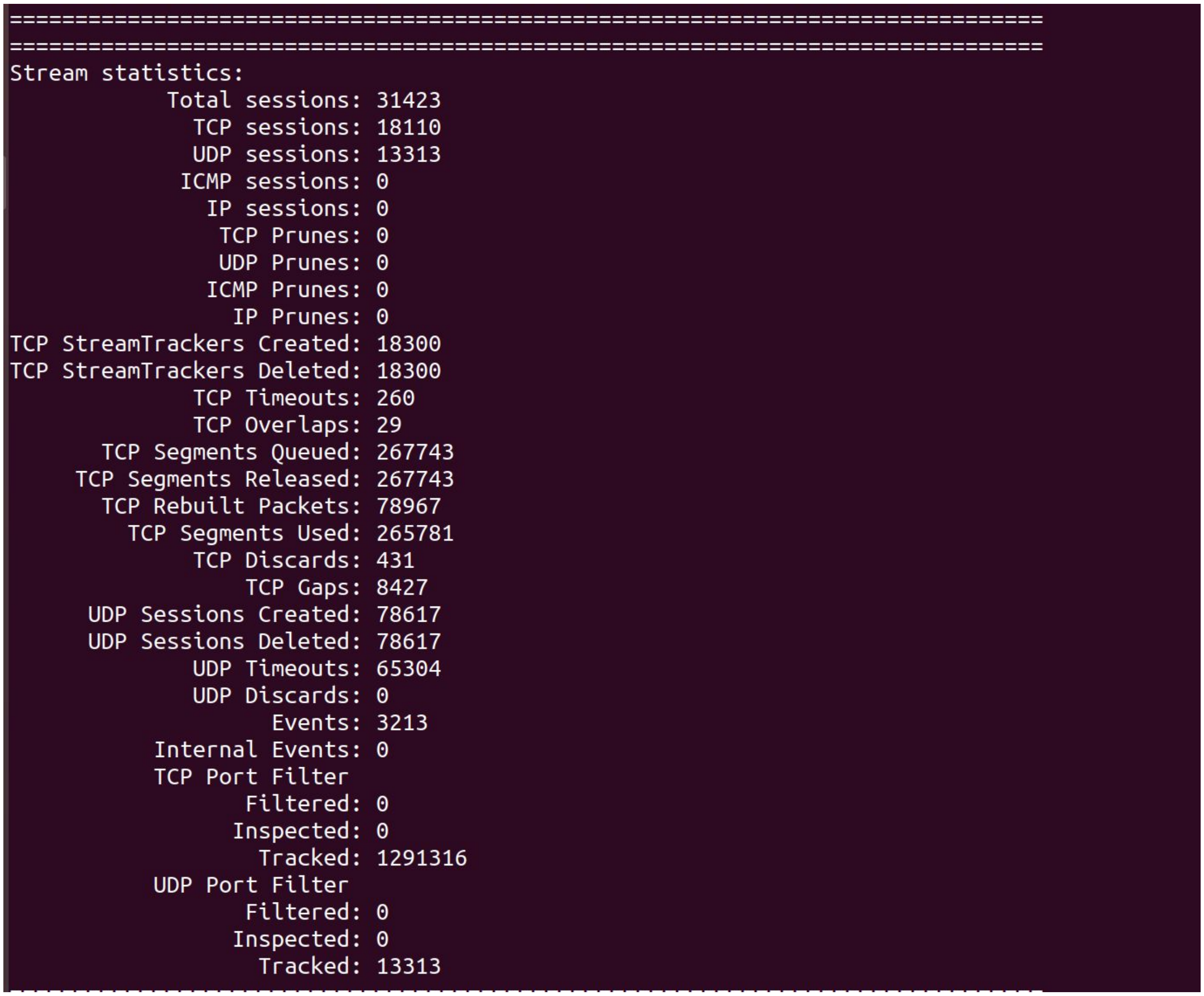
```
===============================================================================
Run time for packet processing was 24.44374 seconds
Snort processed 1647573 packets.
Snort ran for 0 days 0 hours 0 minutes 24 seconds
   Pkts/sec:        68648
===============================================================================
Memory usage summary:
  Total non-mmapped bytes (arena):       46960640
  Bytes in mapped regions (hblkhd):      13574144
  Total allocated space (uordblks):      40420160
  Total free space (fordblks):           6540480
  Topmost releasable block (keepcost):   641936
===============================================================================
Packet I/O Totals:
   Received:      1647573
   Analyzed:      1647573 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:      1648254 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:      1633638 ( 99.113%)
       Frag:            0 (  0.000%)
       ICMP:        52205 (  3.167%)
        UDP:       289436 ( 17.560%)
        TCP:      1291997 ( 78.386%)
        IP6:            0 (  0.000%)
    IP6 Ext:            0 (  0.000%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            0 (  0.000%)
       UDP6:            0 (  0.000%)
       TCP6:            0 (  0.000%)
     Teredo:            0 (  0.000%)
    ICMP-IP:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
```

Snort snip 3



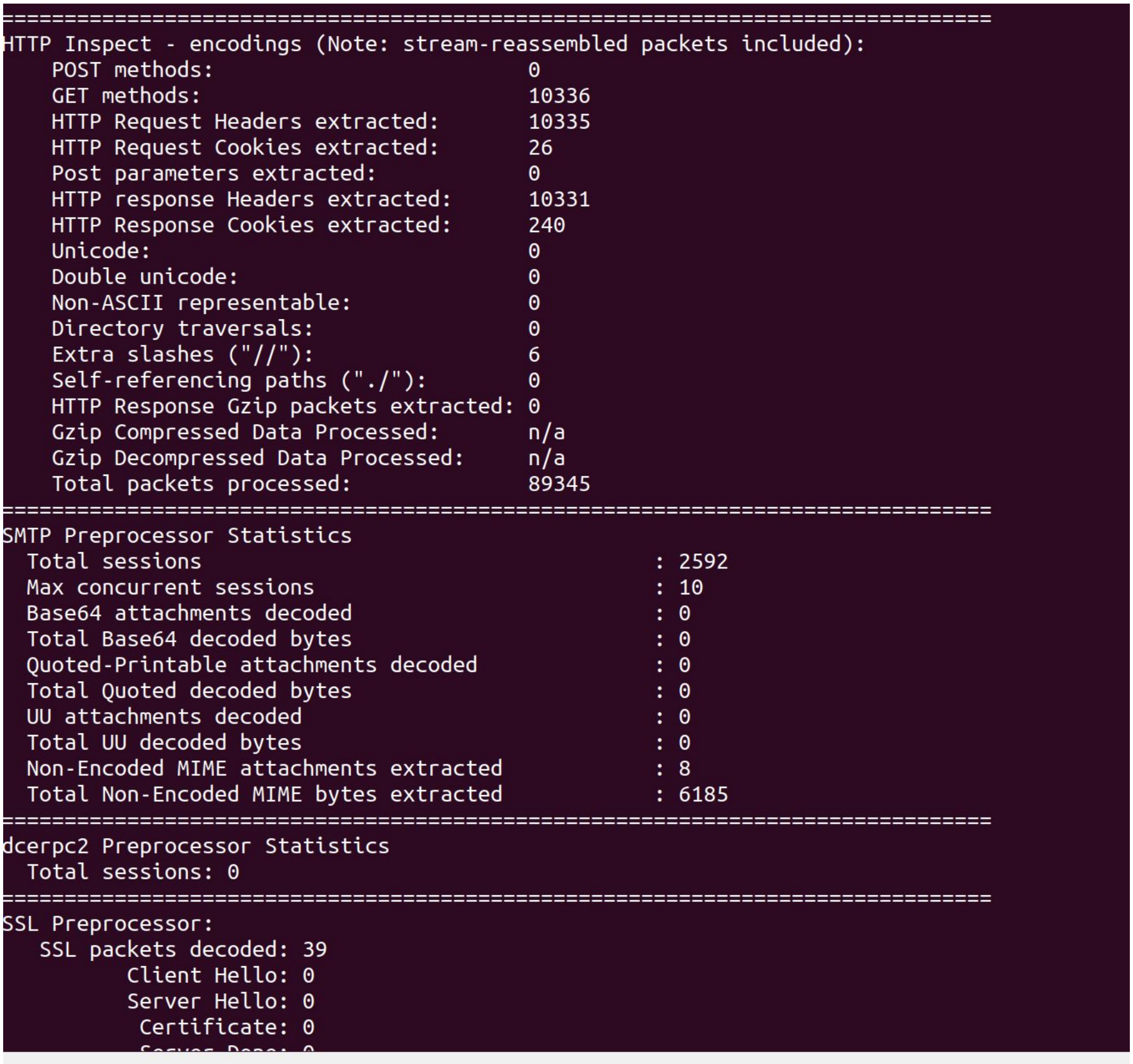
```
        ARP:         5393 (  0.327%)
        IPX:            0 (  0.000%)
   Eth Loop:         7904 (  0.480%)
   Eth Disc:            0 (  0.000%)
   IP4 Disc:            0 (  0.000%)
   IP6 Disc:            0 (  0.000%)
   TCP Disc:            0 (  0.000%)
   UDP Disc:            0 (  0.000%)
  ICMP Disc:            0 (  0.000%)
All Discard:            0 (  0.000%)
      Other:         1319 (  0.080%)
Bad Chk Sum:        51681 (  3.135%)
    Bad TTL:            0 (  0.000%)
     S5 G 1:          519 (  0.031%)
     S5 G 2:          162 (  0.010%)
      Total:      1648254
===============================================================================
Action Stats:
     Alerts:      1584434 ( 96.128%)
     Logged:      1584434 ( 96.128%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
      Queue:            0
        Log:            0
      Event:            0
      Alert:        77661
Verdicts:
      Allow:      1631370 ( 99.017%)
      Block:            0 (  0.000%)
    Replace:            0 (  0.000%)
  Whitelist:        16203 (  0.983%)
  Blacklist:            0 (  0.000%)
     Ignore:            0 (  0.000%)
      Retry:            0 (  0.000%)
===============================================================================
Frag3 statistics:
        Total Fragments: 0
      Frags Reassembled: 0
```

snort snip 4



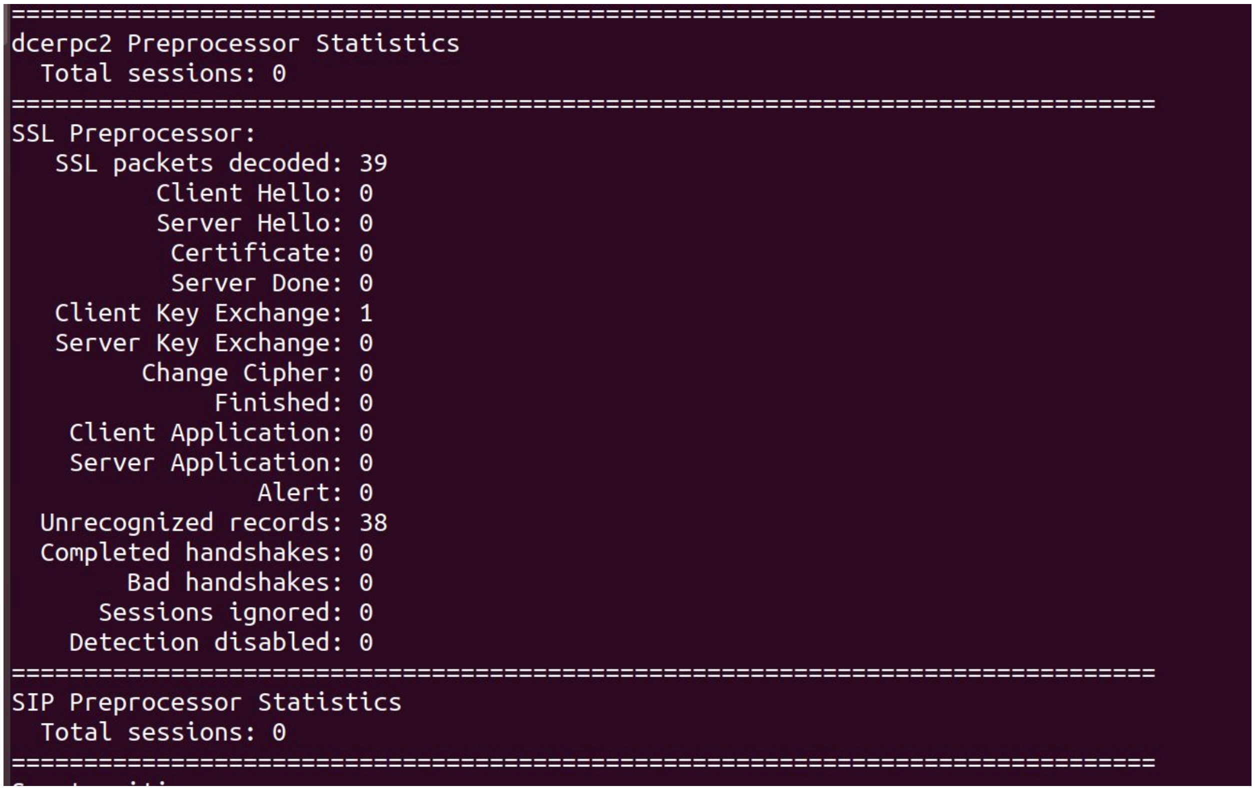
```
================================================================================
================================================================================
Stream statistics:
            Total sessions: 31423
              TCP sessions: 18110
              UDP sessions: 13313
             ICMP sessions: 0
               IP sessions: 0
                TCP Prunes: 0
                UDP Prunes: 0
               ICMP Prunes: 0
                 IP Prunes: 0
TCP StreamTrackers Created: 18300
TCP StreamTrackers Deleted: 18300
              TCP Timeouts: 260
              TCP Overlaps: 29
       TCP Segments Queued: 267743
     TCP Segments Released: 267743
       TCP Rebuilt Packets: 78967
         TCP Segments Used: 265781
              TCP Discards: 431
                  TCP Gaps: 8427
      UDP Sessions Created: 78617
      UDP Sessions Deleted: 78617
              UDP Timeouts: 65304
              UDP Discards: 0
                    Events: 3213
           Internal Events: 0
           TCP Port Filter
                  Filtered: 0
                 Inspected: 0
                   Tracked: 1291316
           UDP Port Filter
                  Filtered: 0
                 Inspected: 0
                   Tracked: 13313
--------------------------------------------------------------------------------
```

Snort snip 5



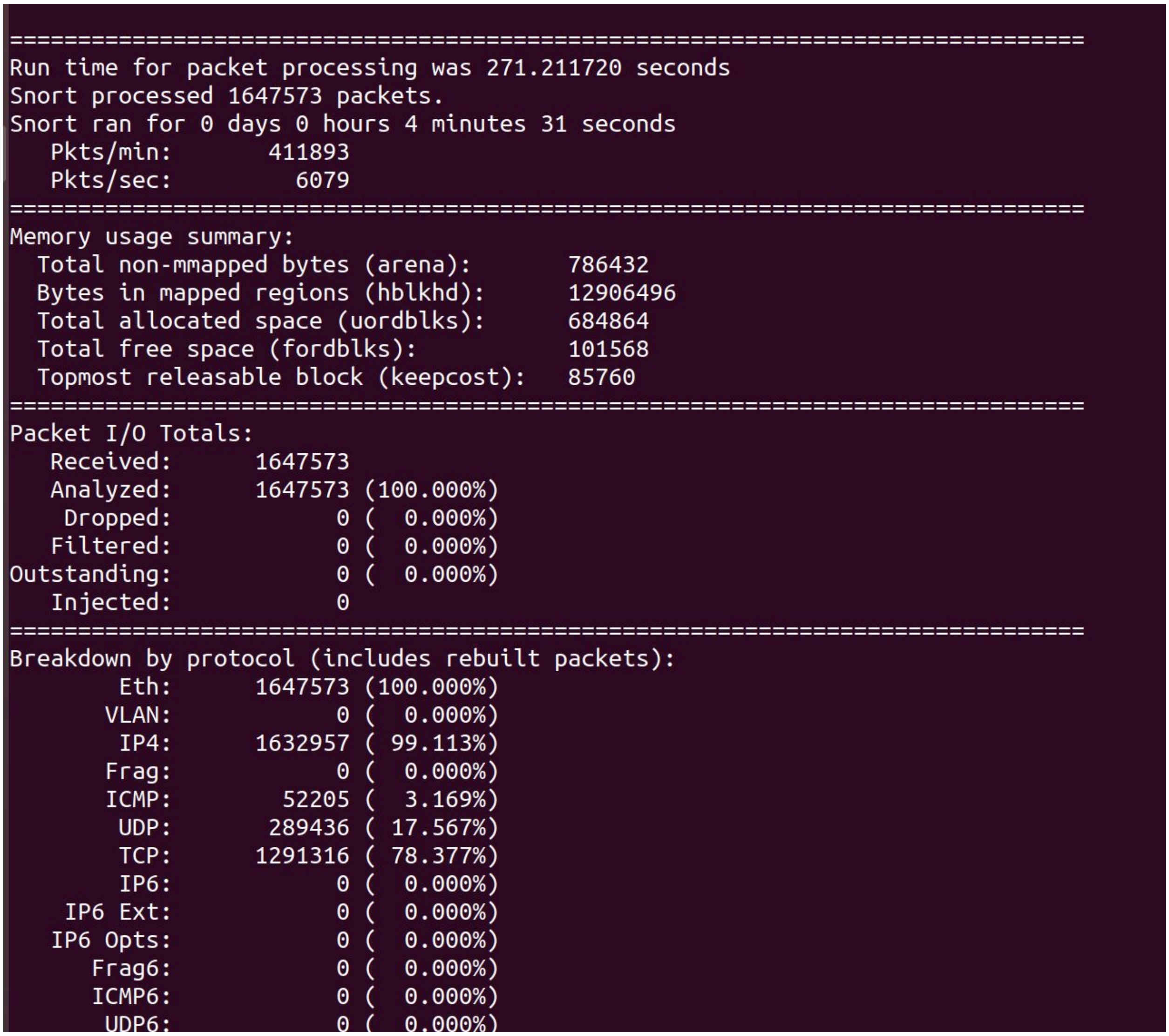
```
===============================================================================
HTTP Inspect - encodings (Note: stream-reassembled packets included):
    POST methods:                         0
    GET methods:                          10336
    HTTP Request Headers extracted:       10335
    HTTP Request Cookies extracted:       26
    Post parameters extracted:            0
    HTTP response Headers extracted:      10331
    HTTP Response Cookies extracted:      240
    Unicode:                              0
    Double unicode:                       0
    Non-ASCII representable:              0
    Directory traversals:                 0
    Extra slashes ("//"):                 6
    Self-referencing paths ("./"):        0
    HTTP Response Gzip packets extracted: 0
    Gzip Compressed Data Processed:       n/a
    Gzip Decompressed Data Processed:     n/a
    Total packets processed:              89345
===============================================================================
SMTP Preprocessor Statistics
  Total sessions                                    : 2592
  Max concurrent sessions                           : 10
  Base64 attachments decoded                        : 0
  Total Base64 decoded bytes                        : 0
  Quoted-Printable attachments decoded              : 0
  Total Quoted decoded bytes                        : 0
  UU attachments decoded                            : 0
  Total UU decoded bytes                            : 0
  Non-Encoded MIME attachments extracted            : 8
  Total Non-Encoded MIME bytes extracted            : 6185
===============================================================================
dcerpc2 Preprocessor Statistics
  Total sessions: 0
===============================================================================
SSL Preprocessor:
   SSL packets decoded: 39
          Client Hello: 0
          Server Hello: 0
           Certificate: 0
           Server Done: 0
```

Snort snip 6



```
===============================================================================
dcerpc2 Preprocessor Statistics
  Total sessions: 0
===============================================================================
SSL Preprocessor:
   SSL packets decoded: 39
          Client Hello: 0
          Server Hello: 0
           Certificate: 0
           Server Done: 0
   Client Key Exchange: 1
   Server Key Exchange: 0
         Change Cipher: 0
              Finished: 0
    Client Application: 0
    Server Application: 0
                 Alert: 0
  Unrecognized records: 38
  Completed handshakes: 0
        Bad handshakes: 0
      Sessions ignored: 0
     Detection disabled: 0
===============================================================================
SIP Preprocessor Statistics
  Total sessions: 0
===============================================================================
```

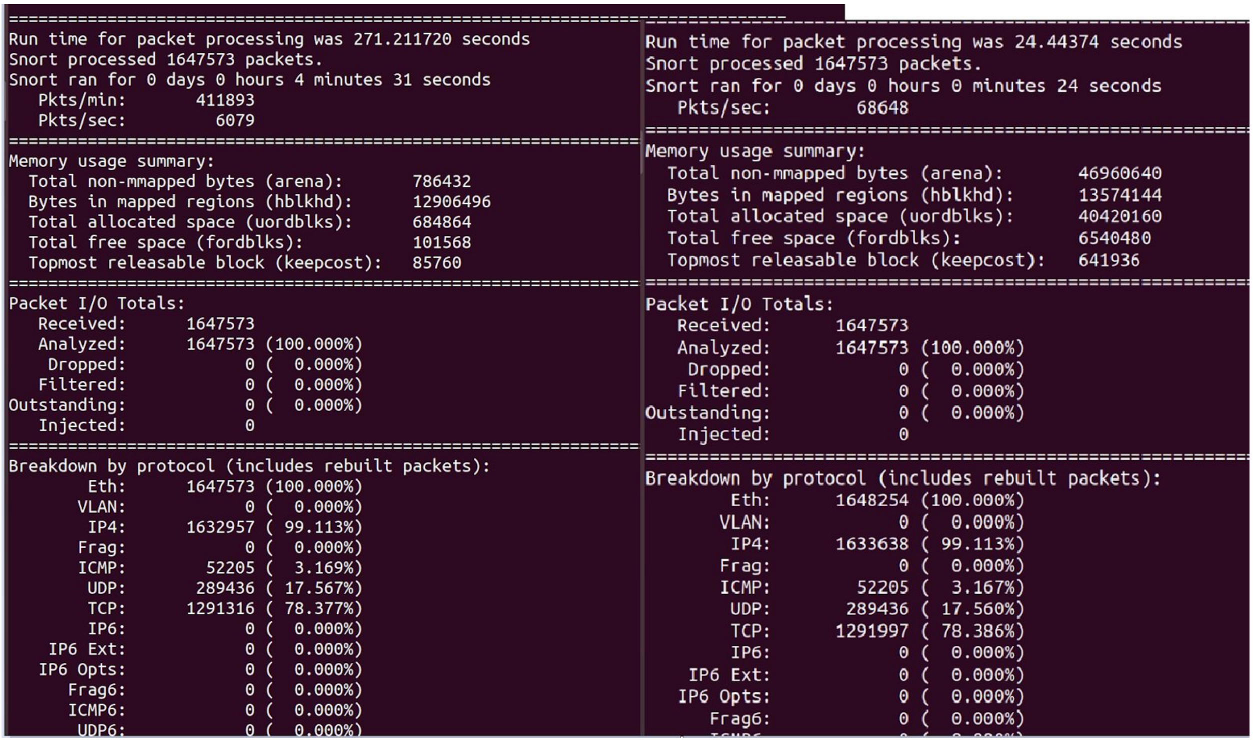
Snort snip 7



```
===============================================================================
Run time for packet processing was 271.211720 seconds
Snort processed 1647573 packets.
Snort ran for 0 days 0 hours 4 minutes 31 seconds
   Pkts/min:       411893
   Pkts/sec:         6079
===============================================================================
Memory usage summary:
  Total non-mmapped bytes (arena):       786432
  Bytes in mapped regions (hblkhd):      12906496
  Total allocated space (uordblks):      684864
  Total free space (fordblks):           101568
  Topmost releasable block (keepcost):   85760
===============================================================================
Packet I/O Totals:
   Received:      1647573
   Analyzed:      1647573 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:      1647573 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:      1632957 ( 99.113%)
       Frag:            0 (  0.000%)
       ICMP:        52205 (  3.169%)
        UDP:       289436 ( 17.567%)
        TCP:      1291316 ( 78.377%)
        IP6:            0 (  0.000%)
    IP6 Ext:            0 (  0.000%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            0 (  0.000%)
       UDP6:            0 (  0.000%)
```

Figure 4:Snort pcap read

The following above was generated using the command “snort -A fast --pcap-single=inside.pcap”



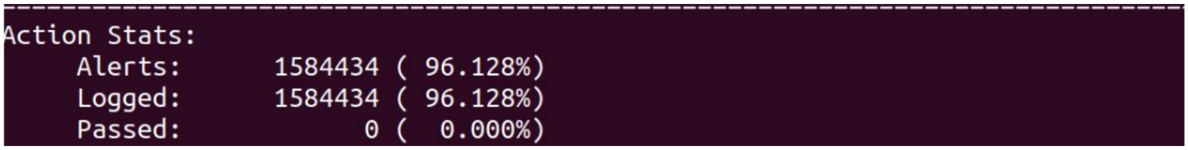
```
===============================================================================
Run time for packet processing was 271.211720 seconds
Snort processed 1647573 packets.
Snort ran for 0 days 0 hours 4 minutes 31 seconds
   Pkts/min:       411893
   Pkts/sec:         6079
===============================================================================
Memory usage summary:
  Total non-mmapped bytes (arena):       786432
  Bytes in mapped regions (hblkhd):      12906496
  Total allocated space (uordblks):      684864
  Total free space (fordblks):           101568
  Topmost releasable block (keepcost):   85760
===============================================================================
Packet I/O Totals:
   Received:      1647573
   Analyzed:      1647573 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:      1647573 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:      1632957 ( 99.113%)
       Frag:            0 (  0.000%)
       ICMP:        52205 (  3.169%)
        UDP:       289436 ( 17.567%)
        TCP:      1291316 ( 78.377%)
        IP6:            0 (  0.000%)
    IP6 Ext:            0 (  0.000%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            0 (  0.000%)
       UDP6:            0 (  0.000%)
```

```
===============================================================================
Run time for packet processing was 24.44374 seconds
Snort processed 1647573 packets.
Snort ran for 0 days 0 hours 0 minutes 24 seconds
   Pkts/sec:        68648
===============================================================================
Memory usage summary:
  Total non-mmapped bytes (arena):       46960640
  Bytes in mapped regions (hblkhd):      13574144
  Total allocated space (uordblks):      40420160
  Total free space (fordblks):           6540480
  Topmost releasable block (keepcost):   641936
===============================================================================
Packet I/O Totals:
   Received:      1647573
   Analyzed:      1647573 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:      1648254 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:      1633638 ( 99.113%)
       Frag:            0 (  0.000%)
       ICMP:        52205 (  3.167%)
        UDP:       289436 ( 17.560%)
        TCP:      1291997 ( 78.386%)
        IP6:            0 (  0.000%)
    IP6 Ext:            0 (  0.000%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
```

Figure 5: snort analysis comparisons

Above are the side by side comparisons between the snort reports generated from the command snort -A fast --pcap-single=inside.pcap” on the left and “snort -c /etc/snort/snort.conf -r inside.pcap” on the right. It's interesting to see which commands give you more information from reading the single pcap file compared to running it against the snort.conf.

How many alerts did you receive when scanning the file locally?



```
===============================================================================
Action Stats:
     Alerts:      1584434 ( 96.128%)
     Logged:      1584434 ( 96.128%)
     Passed:            0 (  0.000%)
```

Figure 6: Total alerts

Finally, you’ll notice the timestamps of the attacks in the ground truth file differ from the timestamps in the Snort alerts. What causes this?

From researching around snort i found out the following information about the timestamps from the Snort tool: Snort is indeed single threaded, meaning it takes more time to process these events, thus leading to a slower timestamp and delaying the alert being sent.

References

https://www.coresentinel.com/processing-pcap-files-snort/

https://tcpreplay.appneta.com/wiki/tcpreplay-man.html

manpagez.com/man/8/snort/