Τέταρτη Εργαστηριακή Άσκηση: Φύλλο Απαντήσεων

Ανίχνευση Εισβολής

Ονοματεπώνυμο: Ειρήνη Δόντη
Αριθμός Μητρώου: 03119839
Εξάμηνο: 8ο

Ερώτηση 3.1

Απάντηση στο φυλλάδιο.

Ερώτηση 3.2

Παραθέτουμε τις εντολές και τα στιγμιότυπα οθόνης για τα παρακάτω:
Εντοπισμός πόσων Interfaces: **snort – W**

```
C:\Snort\bin>snort -W

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20-WIN64 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   00:00:00:00:00:00       disabled        \Device\NPF_{859D4491-1CFA-4693-972B-F4DEA74AE28C}      WAN Miniport (Network Monitor)
    2   00:00:00:00:00:00       disabled        \Device\NPF_{8D8C4C84-7549-49E0-ABAC-C188B441D375}      WAN Miniport (IPv6)
    3   00:00:00:00:00:00       disabled        \Device\NPF_{00C5B1FE-5E78-49B2-90EA-03EA14ABC30A}      WAN Miniport (IP)
    4   E8:D0:FC:D5:BA:C5       192.168.169.8   \Device\NPF_{C36EB732-EC11-4051-8A13-E2797DB408AF}      Qualcomm Atheros QCA9377 Wireless Network Adapter
    5   FA:D0:FC:D5:BA:C5       169.254.235.237 \Device\NPF_{5E9E92EA-D686-47F6-BB46-9CBA41D5C0CF}      Microsoft Wi-Fi Direct Virtual Adapter #4
    6   EA:D0:FC:D5:BA:C5       169.254.187.166 \Device\NPF_{26B73D5A-92FB-450F-93E9-3EA92C7356E9}      Microsoft Wi-Fi Direct Virtual Adapter #3
    7   00:00:00:00:00:00       192.168.56.1    \Device\NPF_{4BCAABFB-4AB9-42E0-9D76-43BC1FB5D2DC}      VirtualBox Host-Only Ethernet Adapter
    8   00:00:00:00:00:00       0000:0000:0000:0000:0000:0000:0000:0000 \Device\NPF_Loopback    Adapter for loopback traffic capture
    9   00:FF:B7:65:92:D7       169.254.200.131 \Device\NPF_{B76592D7-1F13-4C00-97E0-DC7A7155CD29}      TAP-Windows Adapter V9
   10   98:FA:9B:3A:2C:9C       169.254.92.193  \Device\NPF_{803B9847-114E-45B0-AFCB-0C1E4CFDC4AF}      Realtek PCIe GbE Family Controller
```

Η παραπάνω εντολή εμφανίζει μία λίστα από 10 interfaces εκ των οποίων τα 7 είναι ενεργά (όσα δε γράφουν disabled στη στήλη IP Address).

Ερώτηση 3.3

(1) Εκτελούμε την εντολή **snort -v -i4** και το Snort εκτελείται στον Network Adapter 4 και «ακούει» τη δικτυακή κίνηση στο ενεργό σας interface.

(2) Ανοίγουμε ένα δεύτερο CMD

(3) Εκτελούμε την εντολή ping 192.168.56.1 από το μηχάνημα του διπλανού μας:

```
PS C:\Users\Ειρήνη>
                    ping 192.168.56.1

Pinging 192.168.56.1 with 32 bytes of data:
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.56.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

(4) Παρατηρούμε τα πακέτα που ανιχνεύει το snort, αφού πιέσουμε Ctrl+C. Παρατηρούμε ότι ανιχνεύτηκαν IP4, UDP και TCP πακέτα, τα οποία είναι πιθανό να οφείλονται στην επικοινωνία μεταξύ των hosts ή δίκτυα βασισμένα στο IP Address.

```
===============================================================================
Packet I/O Totals:
   Received:          134
   Analyzed:          129 ( 96.269%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            5 (  3.731%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:          129 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:          129 (100.000%)
       Frag:            0 (  0.000%)
       ICMP:            0 (  0.000%)
        UDP:           30 ( 23.256%)
        TCP:           99 ( 76.744%)
        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%)
      EAPOL:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
        GRE:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
   GRE VLAN:            0 (  0.000%)
    GRE IP4:            0 (  0.000%)
    GRE IP6:            0 (  0.000%)
GRE IP6 Ext:            0 (  0.000%)
   GRE PPTP:            0 (  0.000%)
    GRE ARP:            0 (  0.000%)
```

```
    GRE IPX:            0 (  0.000%)
   GRE Loop:            0 (  0.000%)
       MPLS:            0 (  0.000%)
        ARP:            0 (  0.000%)
        IPX:            0 (  0.000%)
   Eth Loop:            0 (  0.000%)
   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:            0 (  0.000%)
Bad Chk Sum:            0 (  0.000%)
    Bad TTL:            0 (  0.000%)
     S5 G 1:            0 (  0.000%)
     S5 G 2:            0 (  0.000%)
      Total:          129
===============================================================================

Memory Statistics for File at:Mon May 29 09:31:43 2023

Total buffers allocated:          0
Total buffers freed:              0
Total buffers released:           0
Total file mempool:               0
Total allocated file mempool:     0
Total freed file mempool:         0
Total released file mempool:      0

Heap Statistics of file:
         Total Statistics:
              Memory in use:              0 bytes
               No of allocs:              0
                No of frees:              0
===============================================================================
Snort exiting
```

Το ping προκάλεσε την ανταλλαγή 4 πακέτων τύπου TCP, IP4, UDP.

Ερώτηση 3.4

(1) Εκτελούμε την εντολή **snort -v -i4 -e** και το Snort εκτελείται στον Network Adapter 4 και «ακούει» τη δικτυακή κίνηση στο ενεργό σας interface.

(2) Ανοίγουμε ένα δεύτερο CMD

(3) Εκτελούμε την εντολή ping 192.168.56.1 από το μηχάνημα του διπλανού μας:

```
PS C:\Users\Ειρήνη> ping 192.168.56.1

Pinging 192.168.56.1 with 32 bytes of data:
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.56.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

(4) Παρατηρούμε τα πακέτα που ανιχνεύει το snort, αφού πιέσουμε Ctrl+C. Παρατηρούμε ότι ανιχνεύτηκαν IP4, UDP και TCP πακέτα, τα οποία είναι πιθανό να οφείλονται στην επικοινωνία μεταξύ των hosts ή δίκτυα βασισμένα στο IP Address.

```
===============================================================================
Run time for packet processing was 22.284000 seconds
Snort processed 112 packets.
Snort ran for 0 days 0 hours 0 minutes 22 seconds
   Pkts/sec:           5
===============================================================================
Packet I/O Totals:
   Received:          112
   Analyzed:          112 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:          112 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:          110 ( 98.214%)
       Frag:            0 (  0.000%)
       ICMP:            0 (  0.000%)
        UDP:           45 ( 40.179%)
        TCP:           65 ( 58.036%)
        IP6:            2 (  1.786%)
    IP6 Ext:            2 (  1.786%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            0 (  0.000%)
       UDP6:            2 (  1.786%)
       TCP6:            0 (  0.000%)
     Teredo:            0 (  0.000%)
    ICMP-IP:            0 (  0.000%)
      EAPOL:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
        GRE:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
   GRE VLAN:            0 (  0.000%)
    GRE IP4:            0 (  0.000%)
    GRE IP6:            0 (  0.000%)
GRE IP6 Ext:            0 (  0.000%)
   GRE PPTP:            0 (  0.000%)
    GRE ARP:            0 (  0.000%)
    GRE IPX:            0 (  0.000%)
   GRE Loop:            0 (  0.000%)
       MPLS:            0 (  0.000%)
        ARP:            0 (  0.000%)
        IPX:            0 (  0.000%)
   Eth Loop:            0 (  0.000%)
   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:            0 (  0.000%)
Bad Chk Sum:            0 (  0.000%)
    Bad TTL:            0 (  0.000%)
     S5 G 1:            0 (  0.000%)
     S5 G 2:            0 (  0.000%)
      Total:          112
===============================================================================
```

```
===============================================================================

Memory Statistics for File at:Mon May 29 10:00:26 2023

Total buffers allocated:          0
Total buffers freed:              0
Total buffers released:           0
Total file mempool:               0
Total allocated file mempool:     0
Total freed file mempool:         0
Total released file mempool:      0

Heap Statistics of file:
          Total Statistics:
               Memory in use:              0 bytes
                No of allocs:              0
                 No of frees:              0
===============================================================================
```

Παρατηρούμε ότι εμφανίζονται τα πλήρη περιεχόμενα των πακέτων από το CMD του Snort, όπως εμφανίζεται παρακάτω.

```
WARNING: No preprocessors configured for policy 0.
05/29-10:00:13.596903 86:6D:8C:CC:B6:24 -> E8:D0:FC:D5:BA:C5 type:0x800 len:0x5E
35.186.224.47:443 -> 192.168.169.8:59354 TCP TTL:253 TOS:0x0 ID:59589 IpLen:20 DgmLen:80 DF
***AP*** Seq: 0xA447C52  Ack: 0x8BB29E87  Win: 0x5FF  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
05/29-10:00:13.652167 E8:D0:FC:D5:BA:C5 -> 86:6D:8C:CC:B6:24 type:0x800 len:0x36
192.168.169.8:59354 -> 35.186.224.47:443 TCP TTL:128 TOS:0x0 ID:52943 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x8BB29E87  Ack: 0xA447C7A  Win: 0x202  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
05/29-10:00:13.934400 E8:D0:FC:D5:BA:C5 -> 01:00:5E:00:00:FB type:0x800 len:0x55
192.168.169.8:5353 -> 224.0.0.251:5353 UDP TTL:1 TOS:0x0 ID:55238 IpLen:20 DgmLen:71
Len: 43
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
05/29-10:00:13.935606 E8:D0:FC:D5:BA:C5 -> 33:33:00:00:00:FB type:0x86DD len:0x69
fe80:0000:0000:0000:82ee:2ae4:795e:09f3:5353 -> ff02:0000:0000:0000:0000:0000:00fb:5353 UDP TTL:1 TOS:0x0 ID:0 IpLen:40 DgmLen:91
Len: 43
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
05/29-10:00:14.933169 E8:D0:FC:D5:BA:C5 -> 01:00:5E:00:00:FB type:0x800 len:0x55
192.168.169.8:5353 -> 224.0.0.251:5353 UDP TTL:1 TOS:0x0 ID:55239 IpLen:20 DgmLen:71
Len: 43
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

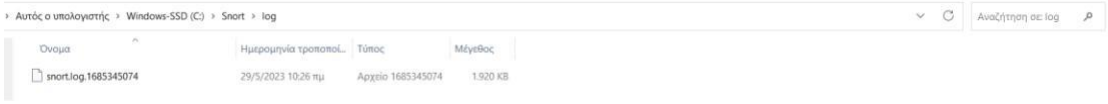
Το ping προκάλεσε την ανταλλαγή 4 πακέτων τύπου TCP, IP4, UDP.

Τα μήκη των header εκάστοτε πακέτων είναι ίσα με την τιμή Len που αναγράφεται στις καταγραφές Snort.

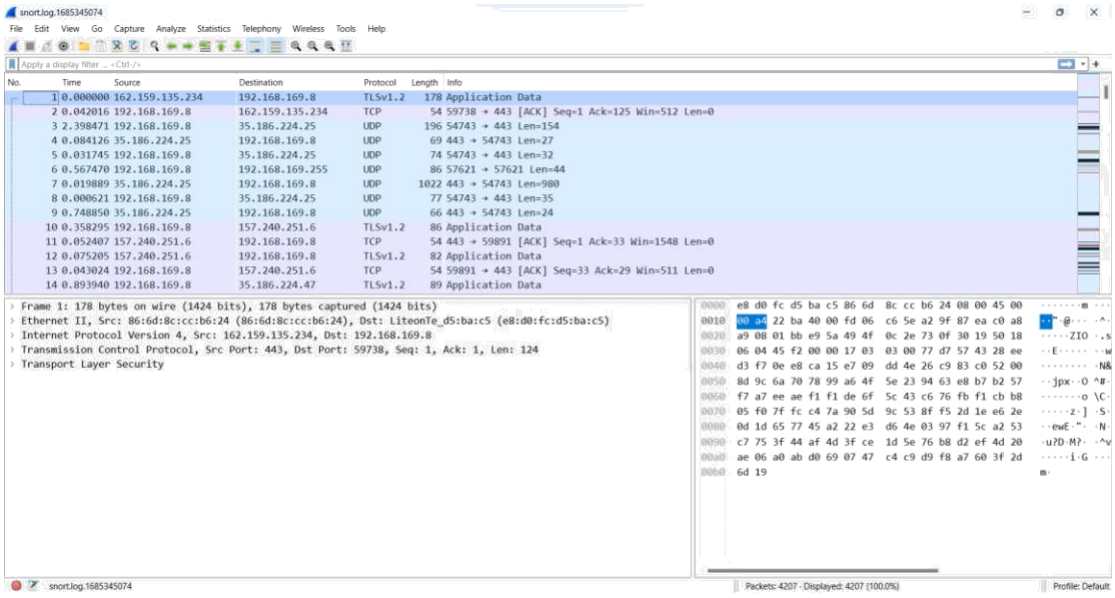
Ερώτηση 3.5

Εκτελούμε την εντολή **snort -v -i4 -l C:\Snort\log** και το Snort εκτελείται στον Network Adapter 4 και «ακούει» τη δικτυακή κίνηση στο ενεργό σας interface.

Επισκεπτόμαστε τις ζητούμενες σελίδες και έπειτα πατάμε Ctrl + C. Εντοπίζουμε το φάκελο C:\Snort\log και έχει αποθηκευτεί το εξής file, όπως φαίνεται παρακάτω:



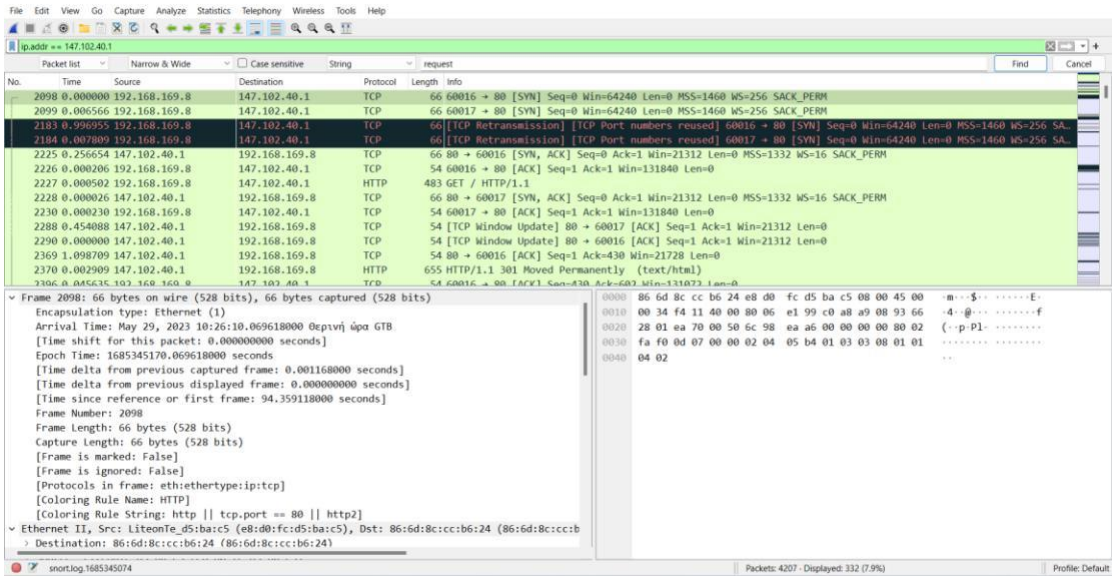
Ανοίγουμε αυτό το file με την εφαρμογή wireshark:



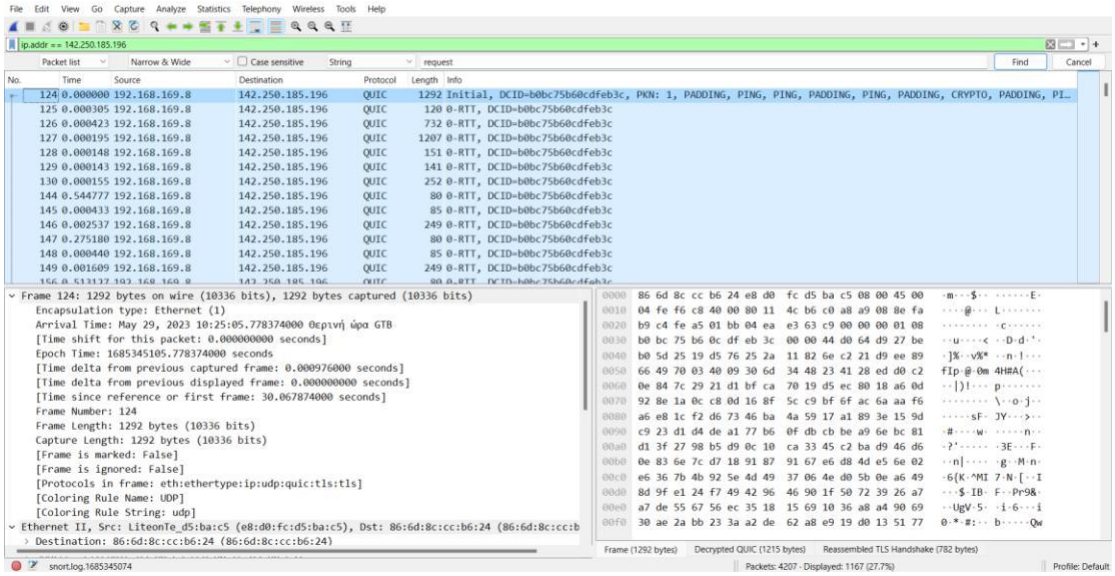
Ανιχνεύτηκαν 4207 πακέτα και έχουν καταγραφεί με τη μορφή Binary.

Παραθέτουμε στιγμιότυπο οθόνης που δείχνουν τα αρχικά requests προς τις δύο ιστοσελίδες:

www.cn.ntua.gr



www.google.com

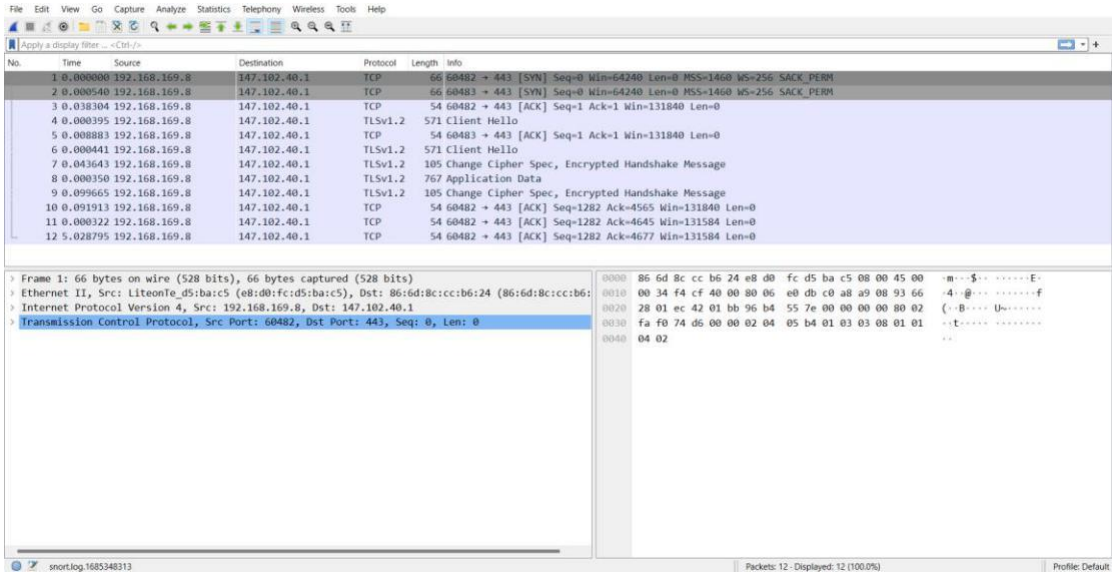


Ερώτηση 3.6

Πληκτρολογούμε τον κανόνα στο αρχείο .txt: log tcp any any -> 147.102.40.1 any (msg: "HTTP to cn.ntua.gr machine!"; isid = 1;).

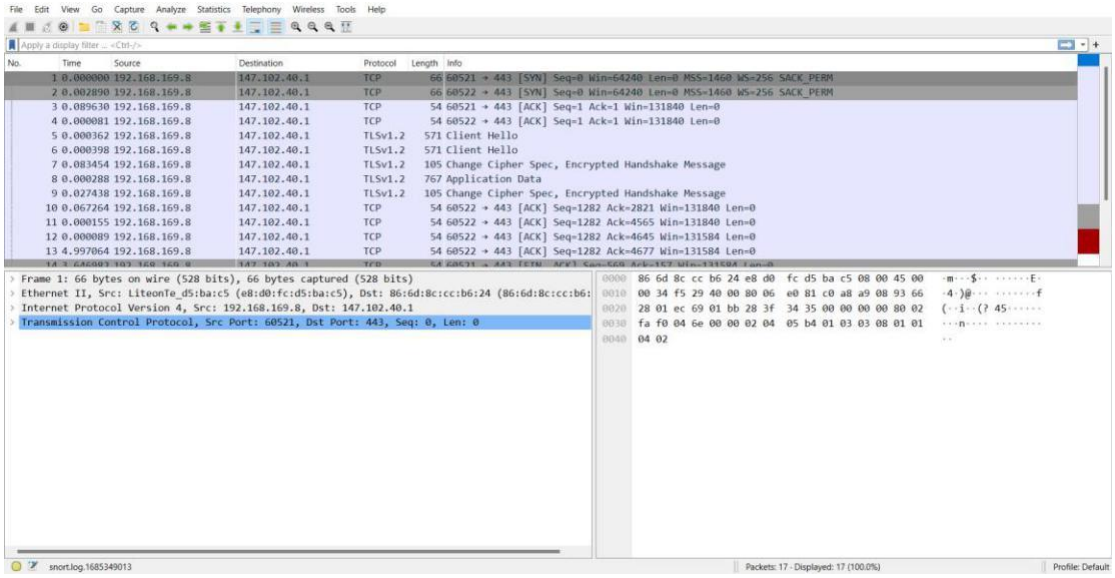
Ο κανόνας αυτός, είναι μία εντολή που εντοπίζει TCP πακέτα από οποιαδήποτε διεύθυνση προς τη διεύθυνση 147.102.40.1 σε οποιοδήποτε θύρα με μήνυμα HTTP to cn.ntua.gr machine! Με αναγνωριστικό (sid) ίσο με 1.

Η εντολή snort -dev -i4 -c “C:\Snort\Rules\DontiEirini_Rules.txt” -l “C:\Snort\log”
Διαβάζει τον κανόνα rules από το .txt file, τον εκτελεί και δημιουργεί log αρχεία στον C:\Snort\log μονοπάτι. Επίσης, δημιουργεί ένα alert αρχείο τύπου IDS.
Ανοίγουμε το log file μέσω Wireshark.

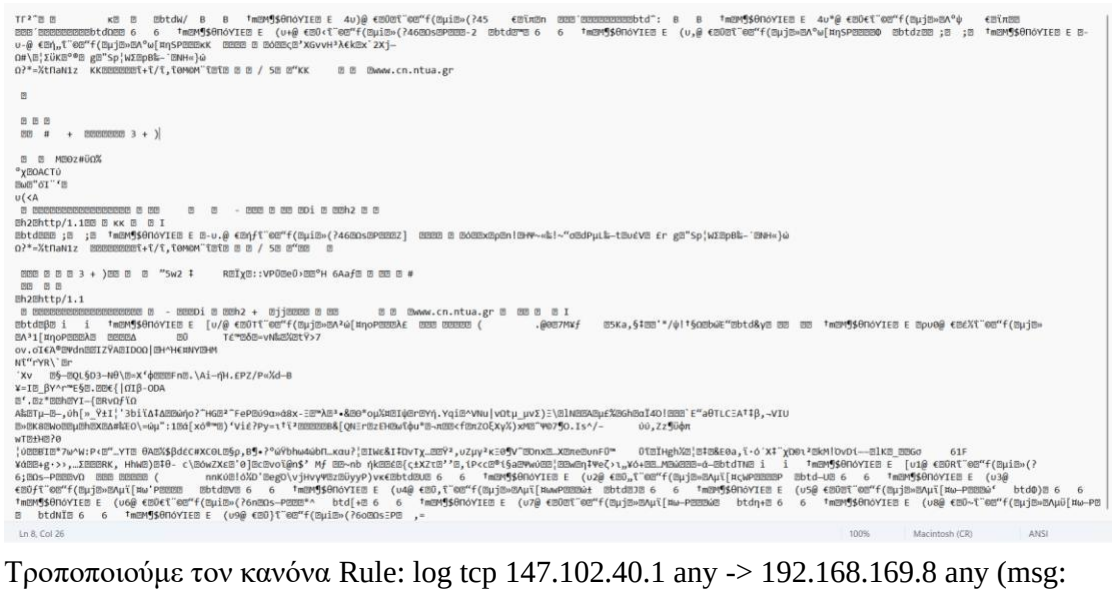


Τροποποιούμε την εντολή: snort -dev -i4 -k none -c “C:\Snort\Rules\DontiEirini_Rules.txt” -l “C:\Snort\log”.

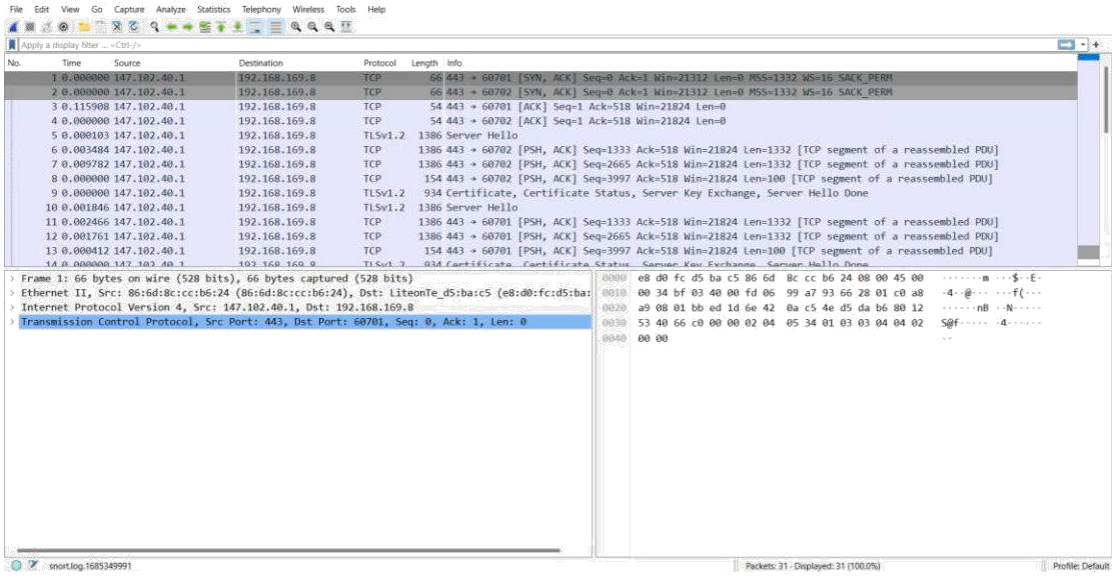
Ανοίγουμε το log file μέσω Wireshark.



Ανοίγουμε το log file μέσω σημειωματάριου και λαμβάνουμε το εξής μήνυμα:



Τροποποιούμε τον κανόνα Rule: log tcp 147.102.40.1 any -> 192.168.169.8 any (msg: "HTTP to cn.ntua.gr machine!"; sid:1;)



Ανοίγουμε το log file μέσω σημειωματάριου και λαμβάνουμε το εξής μήνυμα:

Ερώτηση 3.7

888-65535

Κανόνας:

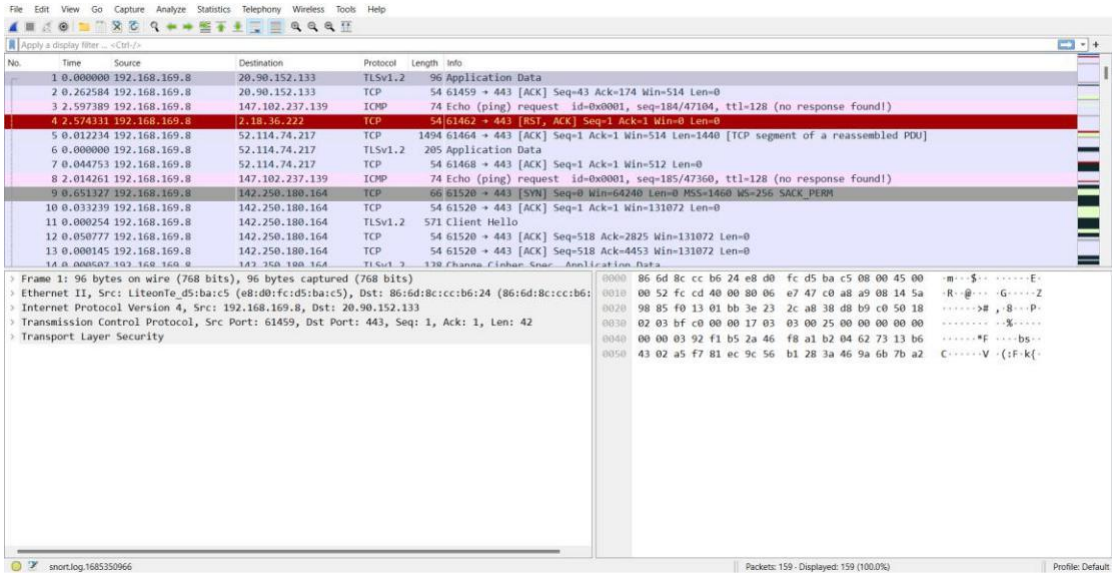
log tcp 192.168.169.8 any -> any !888:65535 (msg: "HTTP to cn.ntua.gr machine!"; sid:1;)

log icmp 192.168.169.8 any -> any !888:65535 (msg: "HTTP to cn.ntua.gr machine!"; sid:2;)

Εντολή στο Snort:

snort -dev -i4 -k none -c “C:\Snort\Rules\DontiEirini_Rules.txt” -l “C:\Snort\log”.

Παραθέτουμε μέσω του wireshark τα πακέτα:



Ερώτηση 3.8

1. log icmp any any -> any any (msg: "HTTP to cn.ntua.gr machine!"; sid:1;)
2. log icmp any any -> any any (msg: "HTTP to cn.ntua.gr machine!"; sid:2; itype:8)
3. log icmp any any -> any any (msg: "HTTP to cn.ntua.gr machine!"; sid:3; itype:0)
4. log icmp any any -> any any (msg: "HTTP to cn.ntua.gr machine!"; sid:4; itype:8; ttl:64;)
   log icmp any any -> any any (msg: "HTTP to cn.ntua.gr machine!"; sid:5; itype:8; ttl:128;)

5. log icmp any any -> any any (msg: "HTTP to cn.ntua.gr machine!"; sid:6; itype:8; dsize:>839;)