VIT®

Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

Information Security Management
CSE3502

Lab Assignment 2
SNORT and Malware Analysis

Slot : L25+L26

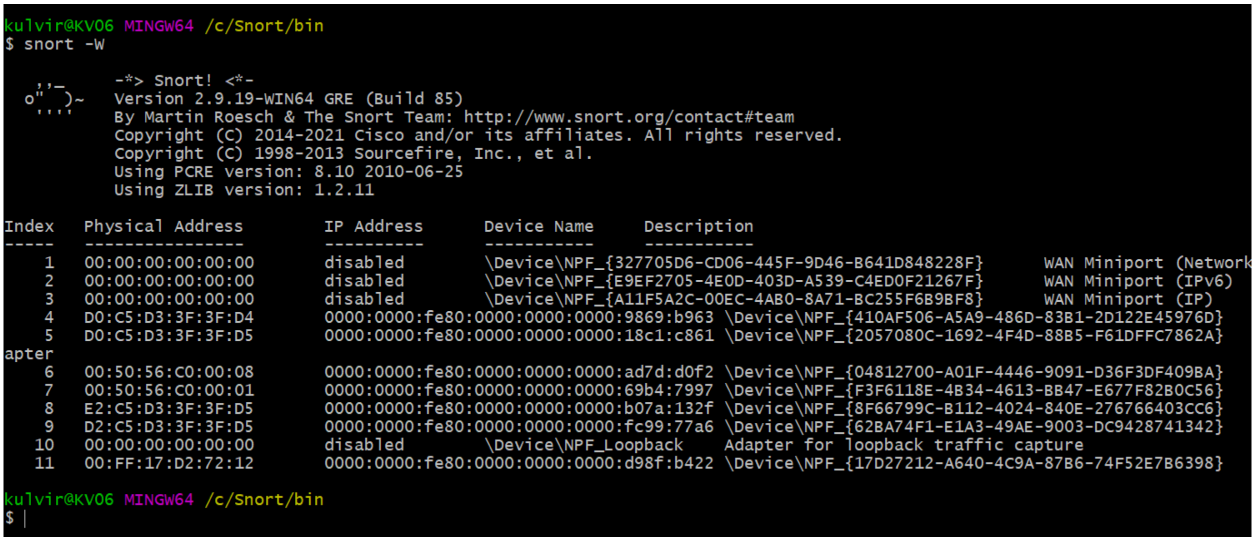
Name : Kulvir Singh

Register Number : 19BCE2074

Experiment 1 : Snort

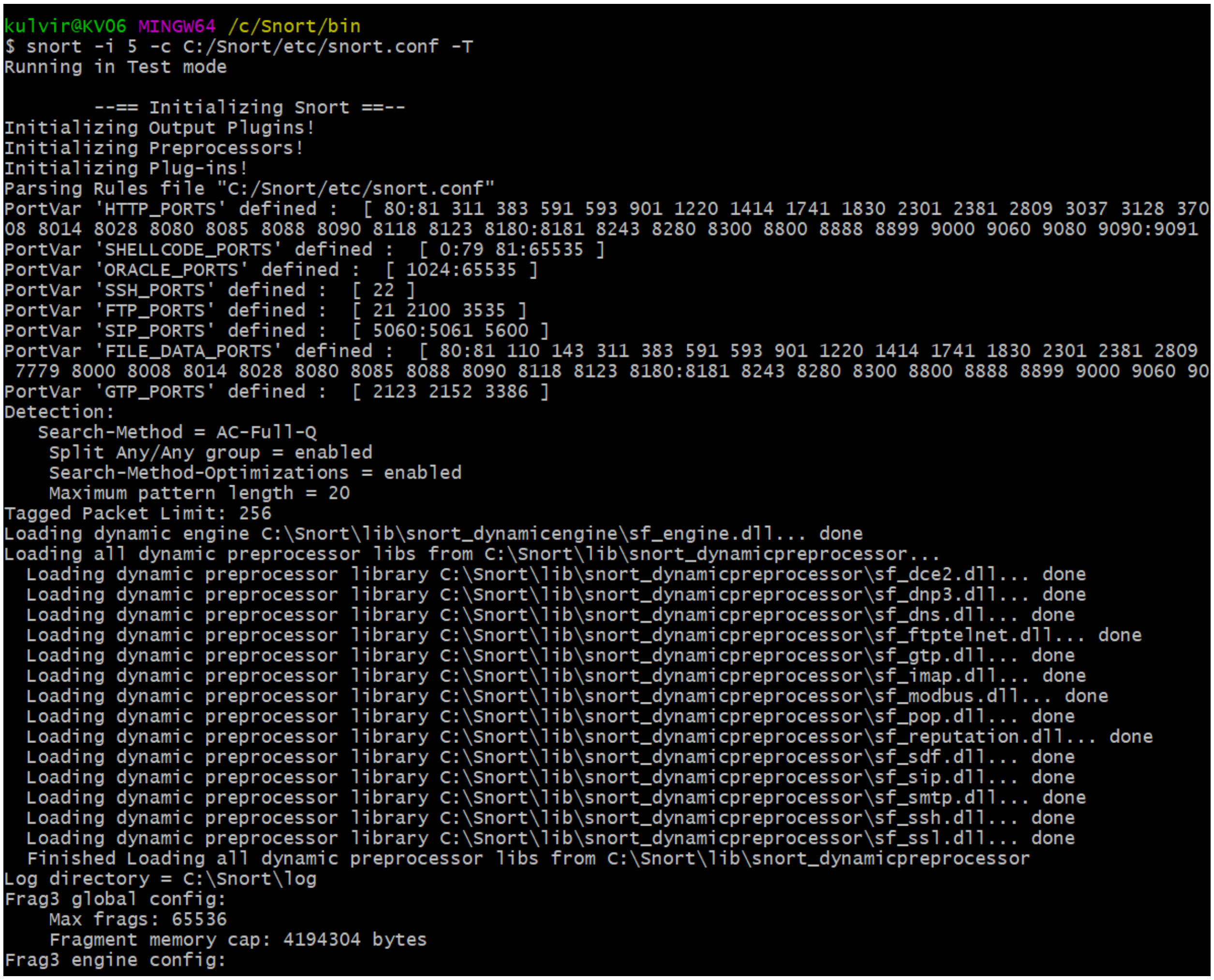
After completing the download and making the said changes this is the output that we get on running the following commands :

Command 1-> snort -W



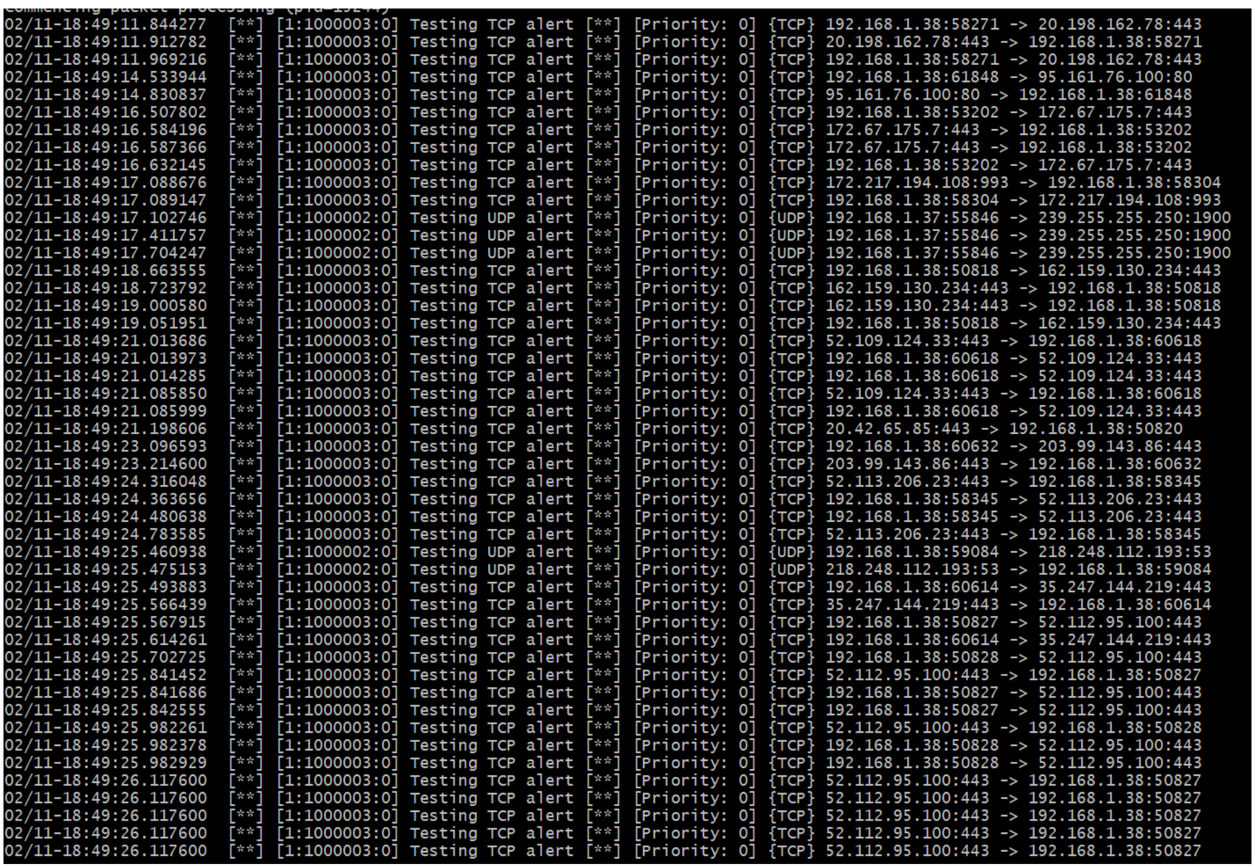
```
kulvir@KV06 MINGW64 /c/Snort/bin
$ snort -W

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.19-WIN64 GRE (Build 85)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 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_{327705D6-CD06-445F-9D46-B641D848228F}      WAN Miniport (Network
    2   00:00:00:00:00:00       disabled        \Device\NPF_{E9EF2705-4E0D-403D-A539-C4ED0F21267F}      WAN Miniport (IPv6)
    3   00:00:00:00:00:00       disabled        \Device\NPF_{A11F5A2C-00EC-4AB0-8A71-BC255F6B9BF8}      WAN Miniport (IP)
    4   D0:C5:D3:3F:3F:D4       0000:0000:fe80:0000:0000:0000:9869:b963 \Device\NPF_{410AF506-A5A9-486D-83B1-2D122E45976D}
    5   D0:C5:D3:3F:3F:D5       0000:0000:fe80:0000:0000:0000:18c1:c861 \Device\NPF_{2057080C-1692-4F4D-88B5-F61DFFC7862A}
apter
    6   00:50:56:C0:00:08       0000:0000:fe80:0000:0000:0000:ad7d:d0f2 \Device\NPF_{04812700-A01F-4446-9091-D36F3DF409BA}
    7   00:50:56:C0:00:01       0000:0000:fe80:0000:0000:0000:69b4:7997 \Device\NPF_{F3F6118E-4B34-4613-BB47-E677F82B0C56}
    8   E2:C5:D3:3F:3F:D5       0000:0000:fe80:0000:0000:0000:b07a:132f \Device\NPF_{8F66799C-B112-4024-840E-276766403CC6}
    9   D2:C5:D3:3F:3F:D5       0000:0000:fe80:0000:0000:0000:fc99:77a6 \Device\NPF_{62BA74F1-E1A3-49AE-9003-DC9428741342}
   10   00:00:00:00:00:00       disabled        \Device\NPF_Loopback    Adapter for loopback traffic capture
   11   00:FF:17:D2:72:12       0000:0000:fe80:0000:0000:0000:d98f:b422 \Device\NPF_{17D27212-A640-4C9A-87B6-74F52E7B6398}

kulvir@KV06 MINGW64 /c/Snort/bin
$ |
```

Command 2-> snort -i 5 -c C:/Snort/etc/snort.conf -T



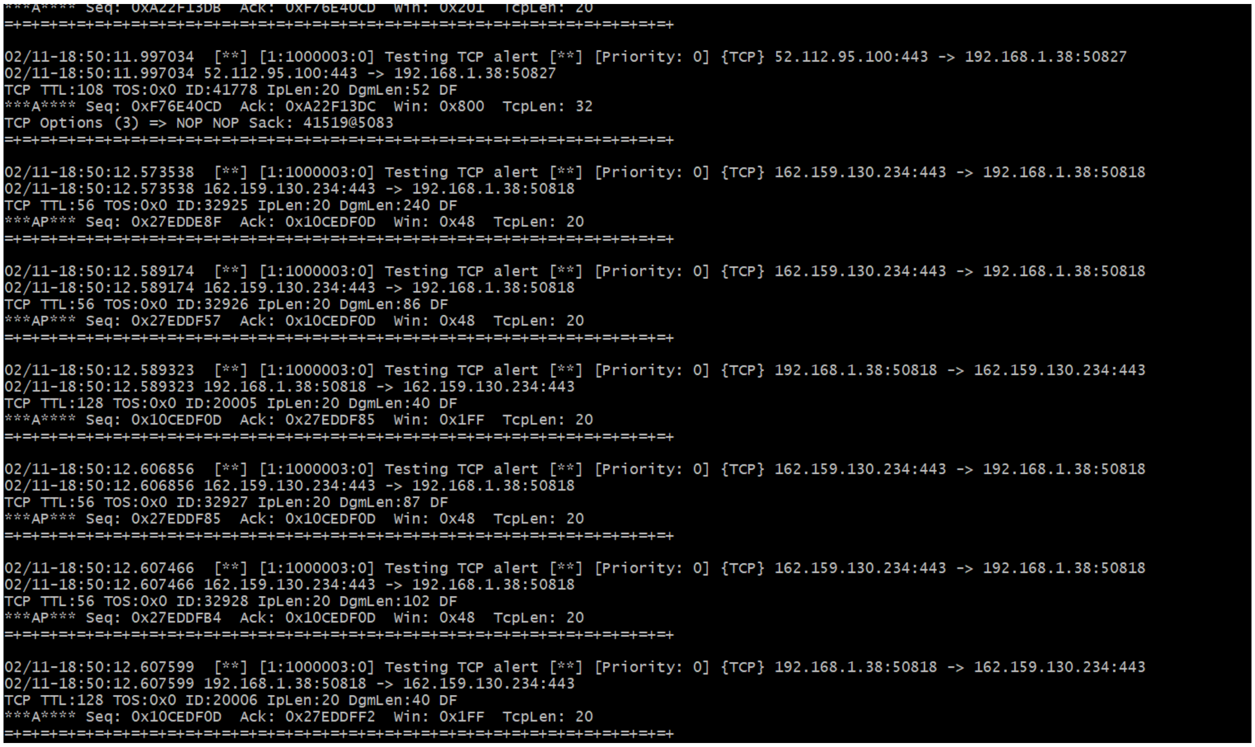
```
kulvir@KV06 MINGW64 /c/Snort/bin
$ snort -i 5 -c C:/Snort/etc/snort.conf -T
Running in Test mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "C:/Snort/etc/snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 370
08 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809
 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 90
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine C:\Snort\lib\snort_dynamicengine\sf_engine.dll... done
Loading all dynamic preprocessor libs from C:\Snort\lib\snort_dynamicpreprocessor...
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dce2.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dnp3.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dns.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ftptelnet.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_gtp.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_imap.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_modbus.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_pop.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_reputation.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_sdf.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_sip.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_smtp.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ssh.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ssl.dll... done
  Finished Loading all dynamic preprocessor libs from C:\Snort\lib\snort_dynamicpreprocessor
Log directory = C:\Snort\log
Frag3 global config:
    Max frags: 65536
    Fragment memory cap: 4194304 bytes
Frag3 engine config:
```

Command 3-> snort -i 5 -c C:/Snort/etc/snort.conf -A console



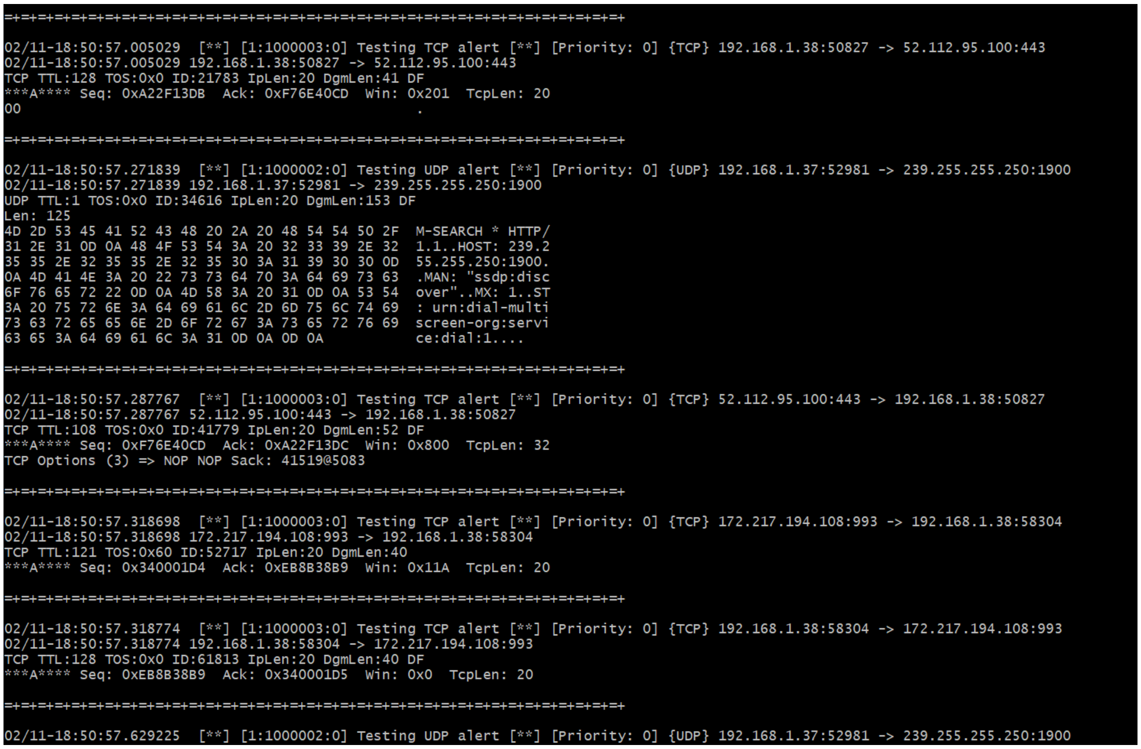
```
Commencing packet processing (pid=19244)
02/11-18:49:11.844277  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.1.38:58271 -> 20.198.162.78:443
02/11-18:49:11.912782  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 20.198.162.78:443 -> 192.168.1.38:58271
02/11-18:49:11.969216  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.1.38:58271 -> 20.198.162.78:443
02/11-18:49:14.533944  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.1.38:61848 -> 95.161.76.100:80
02/11-18:49:14.830837  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 95.161.76.100:80 -> 192.168.1.38:61848
02/11-18:49:16.507802  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.1.38:53202 -> 172.67.175.7:443
02/11-18:49:16.584196  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 172.67.175.7:443 -> 192.168.1.38:53202
02/11-18:49:16.587366  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 172.67.175.7:443 -> 192.168.1.38:53202
02/11-18:49:16.632145  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.1.38:53202 -> 172.67.175.7:443
02/11-18:49:17.088676  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 172.217.194.108:993 -> 192.168.1.38:58304
02/11-18:49:17.089147  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.1.38:58304 -> 172.217.194.108:993
02/11-18:49:17.102746  [**] [1:1000002:0] Testing UDP alert [**] [Priority: 0] {UDP} 192.168.1.37:55846 -> 239.255.255.250:1900
02/11-18:49:17.411757  [**] [1:1000002:0] Testing UDP alert [**] [Priority: 0] {UDP} 192.168.1.37:55846 -> 239.255.255.250:1900
02/11-18:49:17.704247  [**] [1:1000002:0] Testing UDP alert [**] [Priority: 0] {UDP} 192.168.1.37:55846 -> 239.255.255.250:1900
02/11-18:49:18.663555  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.1.38:50818 -> 162.159.130.234:443
02/11-18:49:18.723792  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 162.159.130.234:443 -> 192.168.1.38:50818
02/11-18:49:19.000580  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 162.159.130.234:443 -> 192.168.1.38:50818
02/11-18:49:19.051951  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.1.38:50818 -> 162.159.130.234:443
02/11-18:49:21.013686  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 52.109.124.33:443 -> 192.168.1.38:60618
02/11-18:49:21.013973  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.1.38:60618 -> 52.109.124.33:443
02/11-18:49:21.014285  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.1.38:60618 -> 52.109.124.33:443
02/11-18:49:21.085850  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 52.109.124.33:443 -> 192.168.1.38:60618
02/11-18:49:21.085999  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.1.38:60618 -> 52.109.124.33:443
02/11-18:49:21.198606  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 20.42.65.85:443 -> 192.168.1.38:50820
02/11-18:49:23.096593  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.1.38:60632 -> 203.99.143.86:443
02/11-18:49:23.214600  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 203.99.143.86:443 -> 192.168.1.38:60632
02/11-18:49:24.316048  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 52.113.206.23:443 -> 192.168.1.38:58345
02/11-18:49:24.363656  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.1.38:58345 -> 52.113.206.23:443
02/11-18:49:24.480638  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.1.38:58345 -> 52.113.206.23:443
02/11-18:49:24.783585  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 52.113.206.23:443 -> 192.168.1.38:58345
02/11-18:49:25.460938  [**] [1:1000002:0] Testing UDP alert [**] [Priority: 0] {UDP} 192.168.1.38:59084 -> 218.248.112.193:53
02/11-18:49:25.475153  [**] [1:1000002:0] Testing UDP alert [**] [Priority: 0] {UDP} 218.248.112.193:53 -> 192.168.1.38:59084
02/11-18:49:25.493883  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.1.38:60614 -> 35.247.144.219:443
02/11-18:49:25.566439  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 35.247.144.219:443 -> 192.168.1.38:60614
02/11-18:49:25.567915  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.1.38:50827 -> 52.112.95.100:443
02/11-18:49:25.614261  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.1.38:60614 -> 35.247.144.219:443
02/11-18:49:25.702725  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.1.38:50828 -> 52.112.95.100:443
02/11-18:49:25.841452  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 52.112.95.100:443 -> 192.168.1.38:50827
02/11-18:49:25.841686  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.1.38:50827 -> 52.112.95.100:443
02/11-18:49:25.842555  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.1.38:50827 -> 52.112.95.100:443
02/11-18:49:25.982261  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 52.112.95.100:443 -> 192.168.1.38:50828
02/11-18:49:25.982378  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.1.38:50828 -> 52.112.95.100:443
02/11-18:49:25.982929  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.1.38:50828 -> 52.112.95.100:443
02/11-18:49:26.117600  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 52.112.95.100:443 -> 192.168.1.38:50827
02/11-18:49:26.117600  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 52.112.95.100:443 -> 192.168.1.38:50827
02/11-18:49:26.117600  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 52.112.95.100:443 -> 192.168.1.38:50827
02/11-18:49:26.117600  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 52.112.95.100:443 -> 192.168.1.38:50827
02/11-18:49:26.117600  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 52.112.95.100:443 -> 192.168.1.38:50827
```

Command 4-> snort -i 5 -c C:/Snort/etc/snort.conf -A console -v



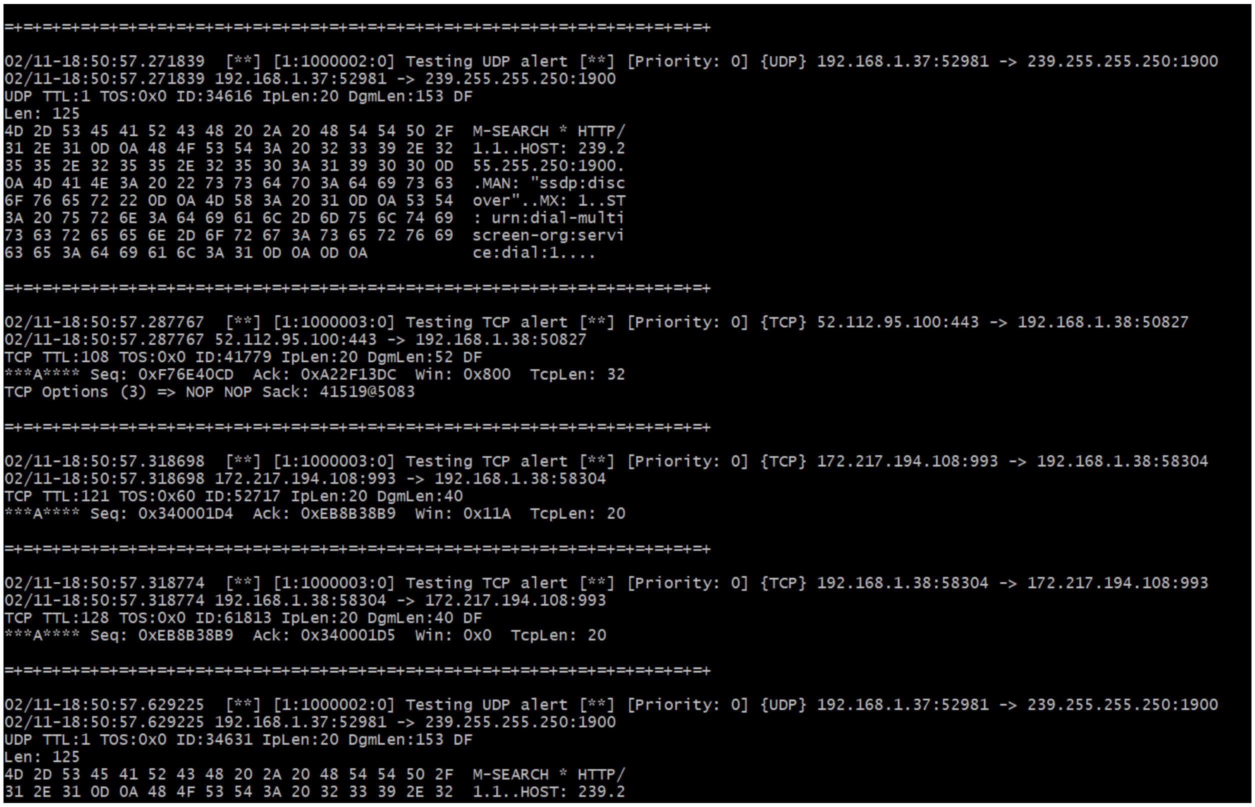
```
***A**** Seq: 0xA22F13DB  Ack: 0xF76E40CD  Win: 0x201  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/11-18:50:11.997034  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 52.112.95.100:443 -> 192.168.1.38:50827
02/11-18:50:11.997034 52.112.95.100:443 -> 192.168.1.38:50827
TCP TTL:108 TOS:0x0 ID:41778 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xF76E40CD  Ack: 0xA22F13DC  Win: 0x800  TcpLen: 32
TCP Options (3) => NOP NOP Sack: 41519@5083
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/11-18:50:12.573538  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 162.159.130.234:443 -> 192.168.1.38:50818
02/11-18:50:12.573538 162.159.130.234:443 -> 192.168.1.38:50818
TCP TTL:56 TOS:0x0 ID:32925 IpLen:20 DgmLen:240 DF
***AP*** Seq: 0x27EDDE8F  Ack: 0x10CEDF0D  Win: 0x48  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/11-18:50:12.589174  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 162.159.130.234:443 -> 192.168.1.38:50818
02/11-18:50:12.589174 162.159.130.234:443 -> 192.168.1.38:50818
TCP TTL:56 TOS:0x0 ID:32926 IpLen:20 DgmLen:86 DF
***AP*** Seq: 0x27EDDF57  Ack: 0x10CEDF0D  Win: 0x48  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/11-18:50:12.589323  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.1.38:50818 -> 162.159.130.234:443
02/11-18:50:12.589323 192.168.1.38:50818 -> 162.159.130.234:443
TCP TTL:128 TOS:0x0 ID:20005 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x10CEDF0D  Ack: 0x27EDDF85  Win: 0x1FF  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/11-18:50:12.606856  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 162.159.130.234:443 -> 192.168.1.38:50818
02/11-18:50:12.606856 162.159.130.234:443 -> 192.168.1.38:50818
TCP TTL:56 TOS:0x0 ID:32927 IpLen:20 DgmLen:87 DF
***AP*** Seq: 0x27EDDF85  Ack: 0x10CEDF0D  Win: 0x48  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/11-18:50:12.607466  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 162.159.130.234:443 -> 192.168.1.38:50818
02/11-18:50:12.607466 162.159.130.234:443 -> 192.168.1.38:50818
TCP TTL:56 TOS:0x0 ID:32928 IpLen:20 DgmLen:102 DF
***AP*** Seq: 0x27EDDFB4  Ack: 0x10CEDF0D  Win: 0x48  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/11-18:50:12.607599  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.1.38:50818 -> 162.159.130.234:443
02/11-18:50:12.607599 192.168.1.38:50818 -> 162.159.130.234:443
TCP TTL:128 TOS:0x0 ID:20006 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x10CEDF0D  Ack: 0x27EDDFF2  Win: 0x1FF  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Command 5-> snort -i 5 -c C:/Snort/etc/snort.conf -A console -vd



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

02/11-18:50:57.005029  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.1.38:50827 -> 52.112.95.100:443
02/11-18:50:57.005029 192.168.1.38:50827 -> 52.112.95.100:443
TCP TTL:128 TOS:0x0 ID:21783 IpLen:20 DgmLen:41 DF
***A**** Seq: 0xA22F13DB  Ack: 0xF76E40CD  Win: 0x201  TcpLen: 20
00                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/11-18:50:57.271839  [**] [1:1000002:0] Testing UDP alert [**] [Priority: 0] {UDP} 192.168.1.37:52981 -> 239.255.255.250:1900
02/11-18:50:57.271839 192.168.1.37:52981 -> 239.255.255.250:1900
UDP TTL:1 TOS:0x0 ID:34616 IpLen:20 DgmLen:153 DF
Len: 125
4D 2D 53 45 41 52 43 48 20 2A 20 48 54 54 50 2F  M-SEARCH * HTTP/
31 2E 31 0D 0A 48 4F 53 54 3A 20 32 33 39 2E 32  1.1..HOST: 239.2
35 35 2E 32 35 35 2E 32 35 30 3A 31 39 30 30 0D  55.255.250:1900.
0A 4D 41 4E 3A 20 22 73 73 64 70 3A 64 69 73 63  .MAN: "ssdp:disc
6F 76 65 72 22 0D 0A 4D 58 3A 20 31 0D 0A 53 54  over"..MX: 1..ST
3A 20 75 72 6E 3A 64 69 61 6C 2D 6D 75 6C 74 69  : urn:dial-multi
73 63 72 65 65 6E 2D 6F 72 67 3A 73 65 72 76 69  screen-org:servi
63 65 3A 64 69 61 6C 3A 31 0D 0A 0D 0A           ce:dial:1....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/11-18:50:57.287767  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 52.112.95.100:443 -> 192.168.1.38:50827
02/11-18:50:57.287767 52.112.95.100:443 -> 192.168.1.38:50827
TCP TTL:108 TOS:0x0 ID:41779 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xF76E40CD  Ack: 0xA22F13DC  Win: 0x800  TcpLen: 32
TCP Options (3) => NOP NOP Sack: 41519@5083

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/11-18:50:57.318698  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 172.217.194.108:993 -> 192.168.1.38:58304
02/11-18:50:57.318698 172.217.194.108:993 -> 192.168.1.38:58304
TCP TTL:121 TOS:0x60 ID:52717 IpLen:20 DgmLen:40
***A**** Seq: 0x340001D4  Ack: 0xEB8B38B9  Win: 0x11A  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/11-18:50:57.318774  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.1.38:58304 -> 172.217.194.108:993
02/11-18:50:57.318774 192.168.1.38:58304 -> 172.217.194.108:993
TCP TTL:128 TOS:0x0 ID:61813 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xEB8B38B9  Ack: 0x340001D5  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/11-18:50:57.629225  [**] [1:1000002:0] Testing UDP alert [**] [Priority: 0] {UDP} 192.168.1.37:52981 -> 239.255.255.250:1900
```

Command 6-> snort -i 5 -c C:/Snort/etc/snort.conf -A console -d -v -e



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

02/11-18:50:57.271839  [**] [1:1000002:0] Testing UDP alert [**] [Priority: 0] {UDP} 192.168.1.37:52981 -> 239.255.255.250:1900
02/11-18:50:57.271839 192.168.1.37:52981 -> 239.255.255.250:1900
UDP TTL:1 TOS:0x0 ID:34616 IpLen:20 DgmLen:153 DF
Len: 125
4D 2D 53 45 41 52 43 48 20 2A 20 48 54 54 50 2F  M-SEARCH * HTTP/
31 2E 31 0D 0A 48 4F 53 54 3A 20 32 33 39 2E 32  1.1..HOST: 239.2
35 35 2E 32 35 35 2E 32 35 30 3A 31 39 30 30 0D  55.255.250:1900.
0A 4D 41 4E 3A 20 22 73 73 64 70 3A 64 69 73 63  .MAN: "ssdp:disc
6F 76 65 72 22 0D 0A 4D 58 3A 20 31 0D 0A 53 54  over"..MX: 1..ST
3A 20 75 72 6E 3A 64 69 61 6C 2D 6D 75 6C 74 69  : urn:dial-multi
73 63 72 65 65 6E 2D 6F 72 67 3A 73 65 72 76 69  screen-org:servi
63 65 3A 64 69 61 6C 3A 31 0D 0A 0D 0A           ce:dial:1....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/11-18:50:57.287767  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 52.112.95.100:443 -> 192.168.1.38:50827
02/11-18:50:57.287767 52.112.95.100:443 -> 192.168.1.38:50827
TCP TTL:108 TOS:0x0 ID:41779 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xF76E40CD  Ack: 0xA22F13DC  Win: 0x800  TcpLen: 32
TCP Options (3) => NOP NOP Sack: 41519@5083

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/11-18:50:57.318698  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 172.217.194.108:993 -> 192.168.1.38:58304
02/11-18:50:57.318698 172.217.194.108:993 -> 192.168.1.38:58304
TCP TTL:121 TOS:0x60 ID:52717 IpLen:20 DgmLen:40
***A**** Seq: 0x340001D4  Ack: 0xEB8B38B9  Win: 0x11A  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/11-18:50:57.318774  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.1.38:58304 -> 172.217.194.108:993
02/11-18:50:57.318774 192.168.1.38:58304 -> 172.217.194.108:993
TCP TTL:128 TOS:0x0 ID:61813 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xEB8B38B9  Ack: 0x340001D5  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/11-18:50:57.629225  [**] [1:1000002:0] Testing UDP alert [**] [Priority: 0] {UDP} 192.168.1.37:52981 -> 239.255.255.250:1900
02/11-18:50:57.629225 192.168.1.37:52981 -> 239.255.255.250:1900
UDP TTL:1 TOS:0x0 ID:34631 IpLen:20 DgmLen:153 DF
Len: 125
4D 2D 53 45 41 52 43 48 20 2A 20 48 54 54 50 2F  M-SEARCH * HTTP/
31 2E 31 0D 0A 48 4F 53 54 3A 20 32 33 39 2E 32  1.1..HOST: 239.2
```

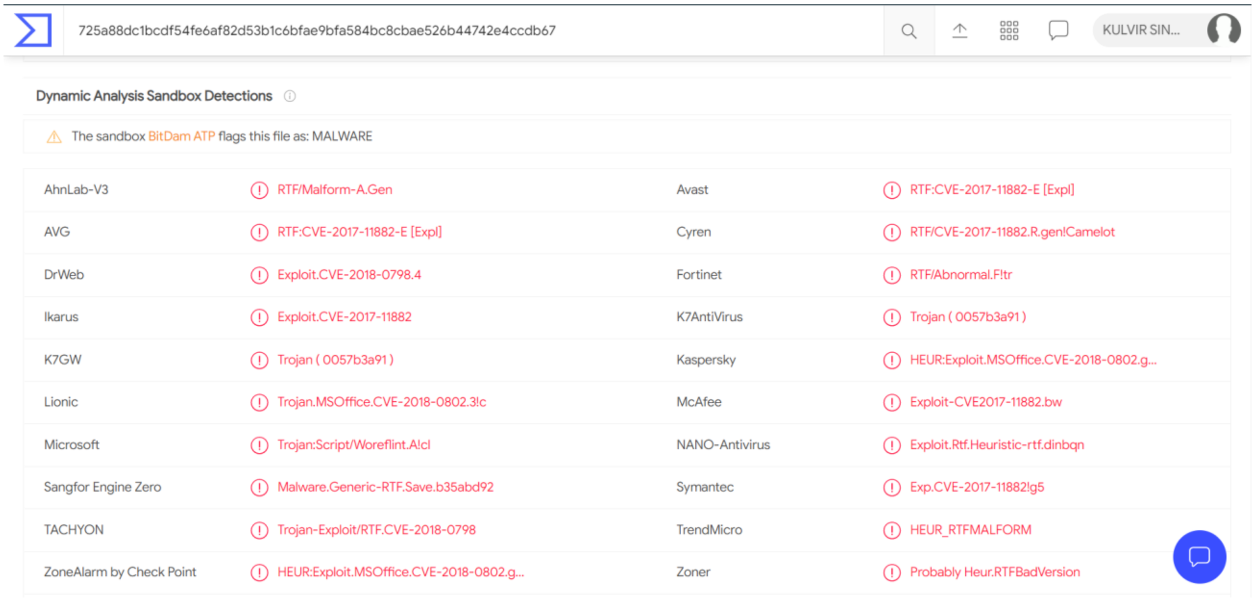
Experiment 2 : Malware Analysis Report on Virus Total

3 hash values of deadly malware is taken from malwarebazar.com and is analyzed on virus total platform

Hash 1 :

725a88dc1bcdf54fe6af82d53b1c6bfae9bfa584bc8cbae526b44742e4ccdb67

Results on Virus Total

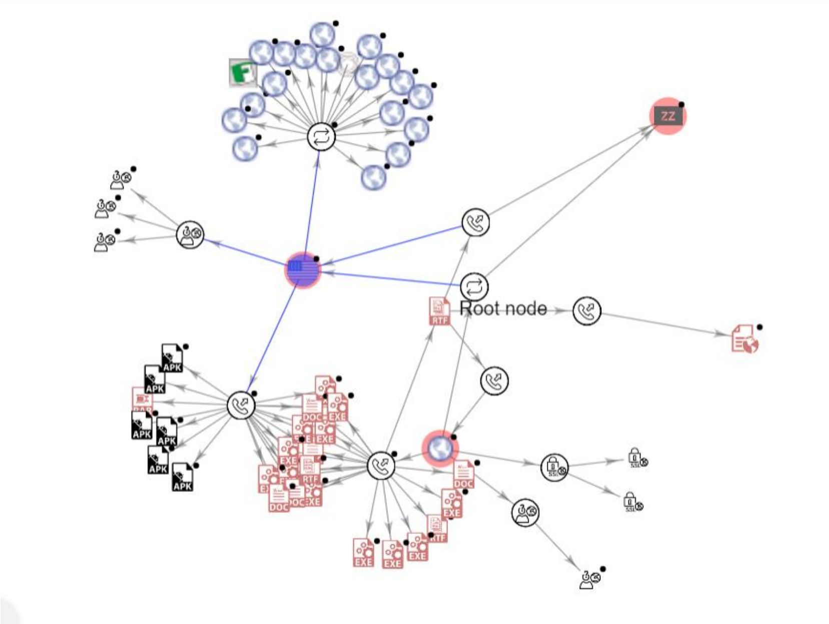


725a88dc1bcdf54fe6af82d53b1c6bfae9bfa584bc8cbae526b44742e4ccdb67

Dynamic Analysis Sandbox Detections

The sandbox BitDam ATP flags this file as: MALWARE

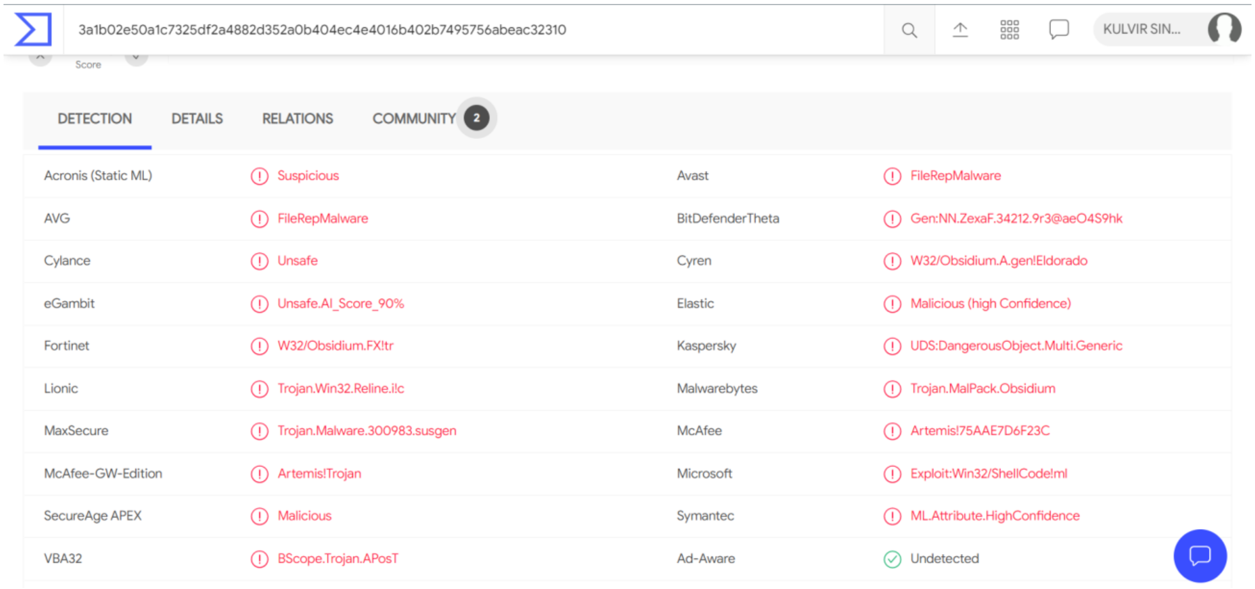
AhnLab-V3	RTF/Malform-A.Gen	Avast	RTF:CVE-2017-11882-E [Expl]
AVG	RTF:CVE-2017-11882-E [Expl]	Cyren	RTF/CVE-2017-11882.R.gen!Camelot
DrWeb	Exploit.CVE-2018-0798.4	Fortinet	RTF/Abnormal.F!tr
Ikarus	Exploit.CVE-2017-11882	K7AntiVirus	Trojan (0057b3a91)
K7GW	Trojan (0057b3a91)	Kaspersky	HEUR:Exploit.MSOffice.CVE-2018-0802.g...
Lionic	Trojan.MSOffice.CVE-2018-0802.3!c	McAfee	Exploit-CVE2017-11882.bw
Microsoft	Trojan:Script/Woreflint.A!cl	NANO-Antivirus	Exploit.Rtf.Heuristic-rtf.dinbqn
Sangfor Engine Zero	Malware.Generic-RTF.Save.b35abd92	Symantec	Exp.CVE-2017-11882!g5
TACHYON	Trojan-Exploit/RTF.CVE-2018-0798	TrendMicro	HEUR_RTFMALFORM
ZoneAlarm by Check Point	HEUR:Exploit.MSOffice.CVE-2018-0802.g...	Zoner	Probably Heur.RTFBadVersion


F
ZZ
Root node
RTF
APK
DOC
EXE

Hash 2

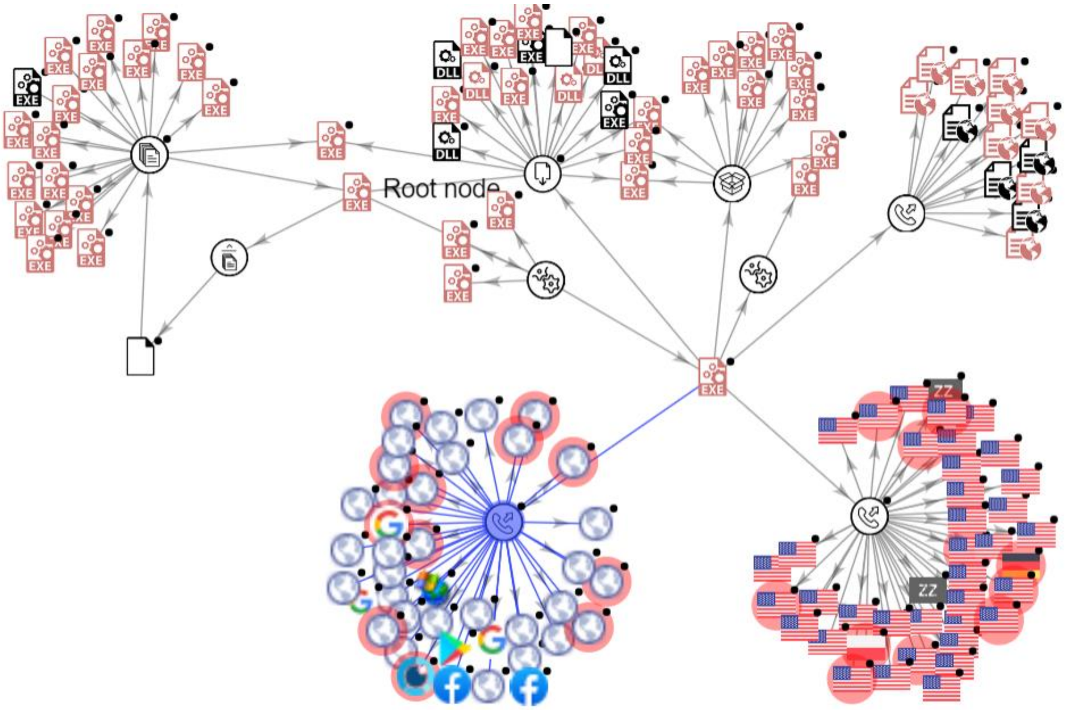
3a1b02e50a1c7325df2a4882d352a0b404ec4e4016b402b7495756abeac32310

Results on Virus Total



3a1b02e50a1c7325df2a4882d352a0b404ec4e4016b402b7495756abeac32310
KULVIR SIN...
Score
DETECTION
DETAILS
RELATIONS
COMMUNITY 2

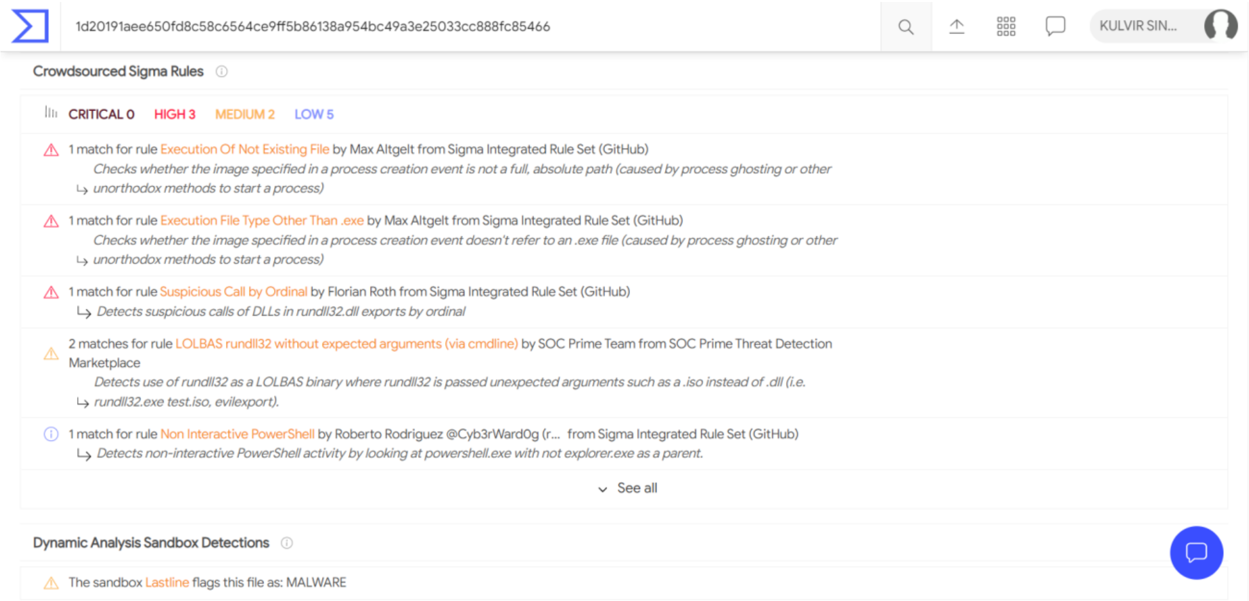
Acronis (Static ML)	ⓘ Suspicious	Avast	ⓘ FileRepMalware
AVG	ⓘ FileRepMalware	BitDefenderTheta	ⓘ Gen:NN.ZexaF.34212.9r3@aeO4S9hk
Cylance	ⓘ Unsafe	Cyren	ⓘ W32/Obsidium.A.gen!Eldorado
eGambit	ⓘ Unsafe.AI_Score_90%	Elastic	ⓘ Malicious (high Confidence)
Fortinet	ⓘ W32/Obsidium.FX!tr	Kaspersky	ⓘ UDS:DangerousObject.Multi.Generic
Lionic	ⓘ Trojan.Win32.Reline.i!c	Malwarebytes	ⓘ Trojan.MalPack.Obsidium
MaxSecure	ⓘ Trojan.Malware.300983.susgen	McAfee	ⓘ Artemis!75AAE7D6F23C
McAfee-GW-Edition	ⓘ Artemis!Trojan	Microsoft	ⓘ Exploit:Win32/ShellCode!ml
SecureAge APEX	ⓘ Malicious	Symantec	ⓘ ML.Attribute.HighConfidence
VBA32	ⓘ BScope.Trojan.APosT	Ad-Aware	✓ Undetected



Hash 3:

1d20191aee650fd8c58c6564ce9ff5b86138a954bc49a3e25033cc888fc85466

Results on virus total



1d20191aee650fd8c58c6564ce9ff5b86138a954bc49a3e25033cc888fc85466

KULVIR SIN...

Crowdsourced Sigma Rules ⓘ

CRITICAL 0 HIGH 3 MEDIUM 2 LOW 5

⚠ 1 match for rule Execution Of Not Existing File by Max Altgelt from Sigma Integrated Rule Set (GitHub)
↳ *Checks whether the image specified in a process creation event is not a full, absolute path (caused by process ghosting or other unorthodox methods to start a process)*

⚠ 1 match for rule Execution File Type Other Than .exe by Max Altgelt from Sigma Integrated Rule Set (GitHub)
↳ *Checks whether the image specified in a process creation event doesn't refer to an .exe file (caused by process ghosting or other unorthodox methods to start a process)*

⚠ 1 match for rule Suspicious Call by Ordinal by Florian Roth from Sigma Integrated Rule Set (GitHub)
↳ *Detects suspicious calls of DLLs in rundll32.dll exports by ordinal*

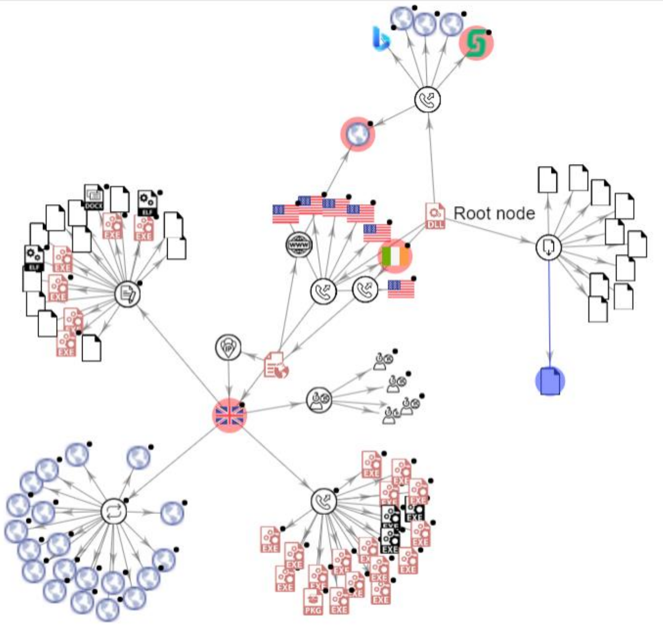
⚠ 2 matches for rule LOLBAS rundll32 without expected arguments (via cmdline) by SOC Prime Team from SOC Prime Threat Detection Marketplace
↳ *Detects use of rundll32 as a LOLBAS binary where rundll32 is passed unexpected arguments such as a .iso instead of .dll (i.e. rundll32.exe test.iso, evilexport).*

ⓘ 1 match for rule Non Interactive PowerShell by Roberto Rodriguez @Cyb3rWard0g (r... from Sigma Integrated Rule Set (GitHub)
↳ *Detects non-interactive PowerShell activity by looking at powershell.exe with not explorer.exe as a parent.*

See all

Dynamic Analysis Sandbox Detections ⓘ

⚠ The sandbox Lastline flags this file as: MALWARE


Root node
DLL
DOCX
ELF
EXE
PKG