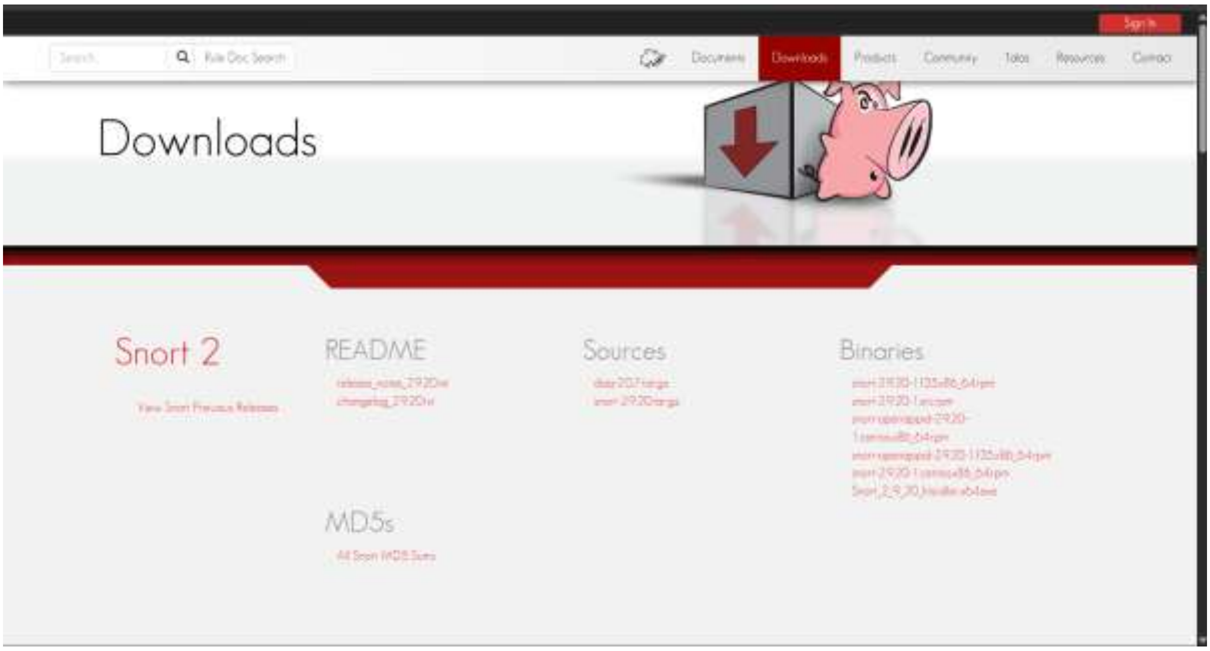
PRACTICAL 6: DEMONSTRATE SNORT



Snort 2

View Snort Previous Releases

README

- release_notes_2.9.20.txt
- changelog_2.9.20.txt

Sources

- daq-2.0.7.tar.gz
- snort-2.9.20.tar.gz

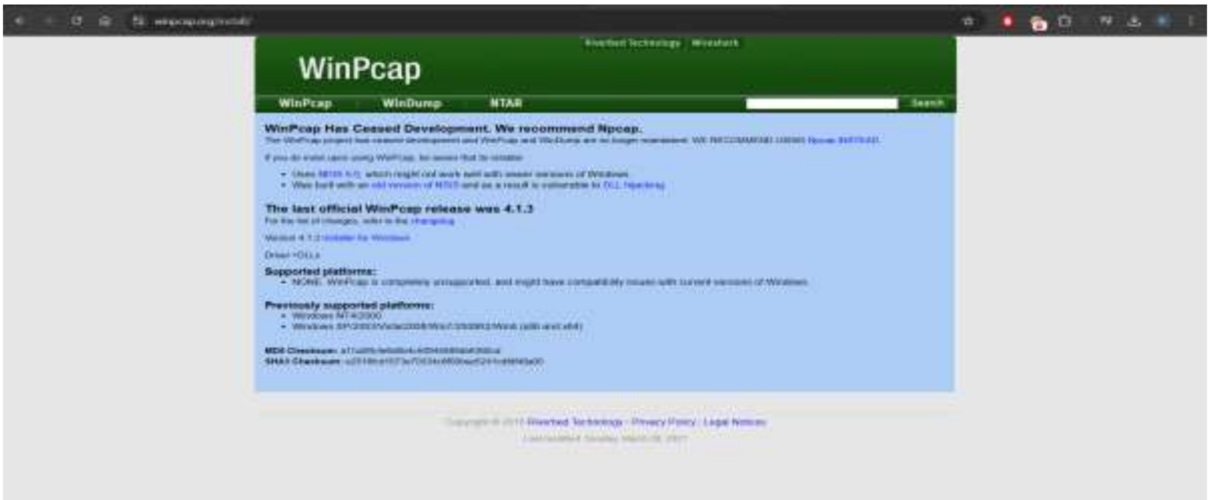
Binaries

- snort-2.9.20-1.f35.x86_64.rpm
- snort-2.9.20-1.src.rpm
- snort-openappid-2.9.20-1.centos.x86_64.rpm
- snort-openappid-2.9.20-1.f35.x86_64.rpm
- snort-2.9.20-1.centos.x86_64.rpm
- Snort_2_9_20_Installer.x64.exe

MD5s

- All Snort MD5 Sums

\



WinPcap Has Ceased Development. We recommend Npcap.

The WinPcap project has ceased development and WinPcap and WinDump are no longer maintained. WE RECOMMEND USING Npcap INSTEAD.

If you do insist upon using WinPcap, be aware that its installer:

- Uses NSIS 2.x, which might not work well with newer versions of Windows
- Was built with an old version of NSIS and as a result is vulnerable to DLL hijacking

The last official WinPcap release was 4.1.3

For the list of changes, refer to the changelog

Version 4.1.3 installer for Windows

Driver +DLLs

Supported platforms:

- NONE. WinPcap is completely unsupported, and might have compatibility issues with current versions of Windows

Previously supported platforms:

- Windows NT4/2000
- Windows XP/2003/Vista/2008/Win7/2008R2/Win8 (x86 and x64)

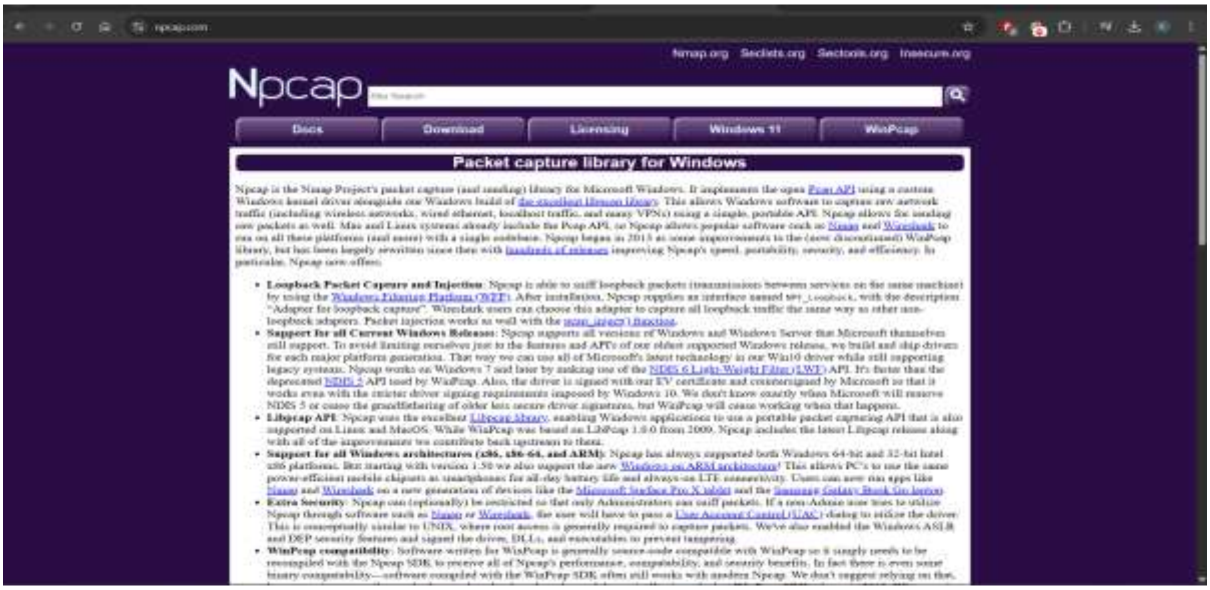
MD5 Checksum: [illegible]

SHA1 Checksum: [illegible]

Copyright © [illegible] Riverbed Technology · Privacy Policy · Legal Notices

Last modified: [illegible]

PRACTICAL 6: DEMONSTRATE SNORT



npcap.com

Nmap.org Seclists.org Sectools.org Insecure.org

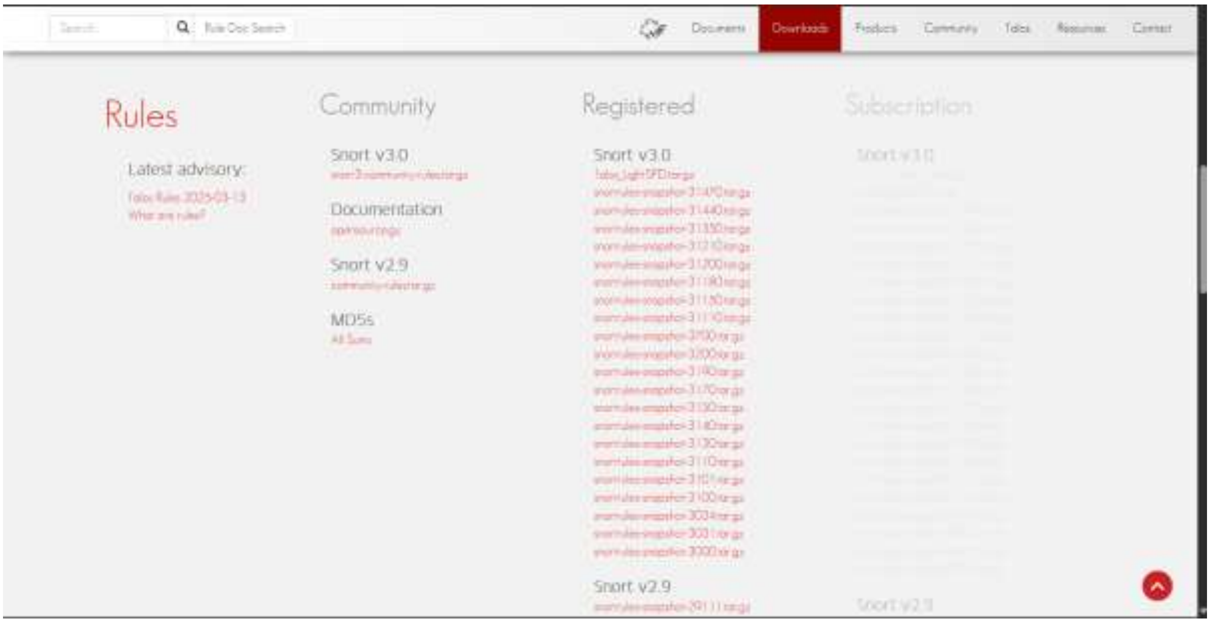
Npcap

Docs | Download | Licensing | Windows 11 | WinPcap

Packet capture library for Windows

Npcap is the Nmap Project's packet capture (and sending) library for Microsoft Windows. It implements the open Pcap API using a custom Windows kernel driver alongside our Windows build of the excellent libpcap library. This allows Windows software to capture raw network traffic (including wireless networks, wired ethernet, localhost traffic, and many VPNs) using a simple, portable API. Npcap allows for sending raw packets as well. Mac and Linux systems already include the Pcap API, so Npcap allows popular software such as Nmap and Wireshark to run on all these platforms (and more) with a single codebase. Npcap began in 2013 as some improvements to the (now discontinued) WinPcap library, but has been largely rewritten since then with hundreds of releases improving Npcap's speed, portability, security, and efficiency. In particular, Npcap now offers:

- **Loopback Packet Capture and Injection**: Npcap is able to sniff loopback packets (transmissions between services on the same machine) by using the Windows Filtering Platform (WFP). After installation, Npcap supplies an interface named NPF_Loopback, with the description "Adapter for loopback capture". Wireshark users can choose this adapter to capture all loopback traffic the same way as other non-loopback adapters. Packet injection works as well with the pcap_inject() function.
- **Support for all Current Windows Releases**: Npcap supports all versions of Windows and Windows Server that Microsoft themselves still support. To avoid limiting ourselves just to the features and API's of our oldest supported Windows release, we build and ship drivers for each major platform generation. That way we can use all of Microsoft's latest technology in our Win10 driver while still supporting legacy systems. Npcap works on Windows 7 and later by making use of the NDIS 6 Light-Weight Filter (LWF) API. It's faster than the deprecated NDIS 5 API used by WinPcap. Also, the driver is signed with our EV certificate and countersigned by Microsoft so that it works even with the stricter driver signing requirements imposed by Windows 10. We don't know exactly when Microsoft will remove NDIS 5 or cease the grandfathering of older less secure driver signatures, but WinPcap will cease working when that happens.
- **Libpcap API**: Npcap uses the excellent Libpcap library, enabling Windows applications to use a portable packet capturing API that is also supported on Linux and MacOS. While WinPcap was based on LibPcap 1.0.0 from 2009, Npcap includes the latest Libpcap release along with all of the improvements we contribute back upstream to them.
- **Support for all Windows architectures (x86, x86-64, and ARM)**: Npcap has always supported both Windows 64-bit and 32-bit Intel x86 platforms. But starting with version 1.50 we also support the new Windows on ARM architecture! This allows PC's to use the same power-efficient mobile chipsets as smartphones for all-day battery life and always-on LTE connectivity. Users can now run apps like Nmap and Wireshark on a new generation of devices like the Microsoft Surface Pro X tablet and the Samsung Galaxy Book Go laptop.
- **Extra Security**: Npcap can (optionally) be restricted so that only Administrators can sniff packets. If a non-Admin user tries to utilize Npcap through software such as Nmap or Wireshark, the user will have to pass a User Account Control (UAC) dialog to utilize the driver. This is conceptually similar to UNIX, where root access is generally required to capture packets. We've also enabled the Windows ASLR and DEP security features and signed the driver, DLLs, and executables to prevent tampering.
- **WinPcap compatibility**: Software written for WinPcap is generally source-code compatible with WinPcap so it simply needs to be recompiled with the Npcap SDK to receive all of Npcap's performance, compatibility, and security benefits. In fact there is even some binary compatibility—software compiled with the WinPcap SDK often still works with modern Npcap. We don't suggest relying on that,



Search... | Rule Doc Search | Documents | Downloads | Products | Community | Talos | Resources | Contact

Rules

Latest advisory:

Talos Rules 2025-03-13

What are rules?

Community

Snort v3.0

snort3-community-rules.tar.gz

Documentation

opensource.tgz

Snort v2.9

community-rules.tar.gz

MD5s

All Sums

Registered

Snort v3.0

Talos_LightSPD.tar.gz

snortrules-snapshot-31470.tar.gz

snortrules-snapshot-31440.tar.gz

snortrules-snapshot-31350.tar.gz

snortrules-snapshot-31210.tar.gz

snortrules-snapshot-31200.tar.gz

snortrules-snapshot-31190.tar.gz

snortrules-snapshot-31150.tar.gz

snortrules-snapshot-31110.tar.gz

snortrules-snapshot-3190.tar.gz

snortrules-snapshot-3200.tar.gz

snortrules-snapshot-3190.tar.gz

snortrules-snapshot-3170.tar.gz

snortrules-snapshot-3150.tar.gz

snortrules-snapshot-3140.tar.gz

snortrules-snapshot-3130.tar.gz

snortrules-snapshot-3110.tar.gz

snortrules-snapshot-3101.tar.gz

snortrules-snapshot-3100.tar.gz

snortrules-snapshot-3004.tar.gz

snortrules-snapshot-3001.tar.gz

snortrules-snapshot-3000.tar.gz

Snort v2.9

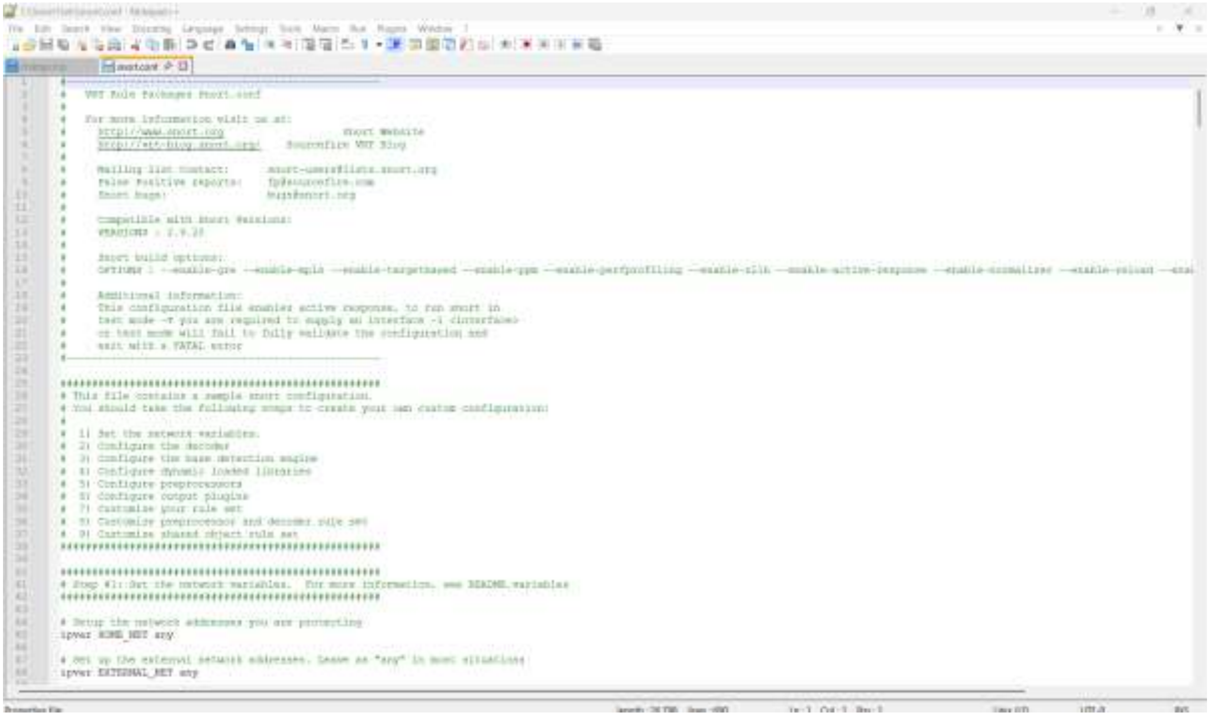
snortrules-snapshot-29111.tar.gz

Subscription

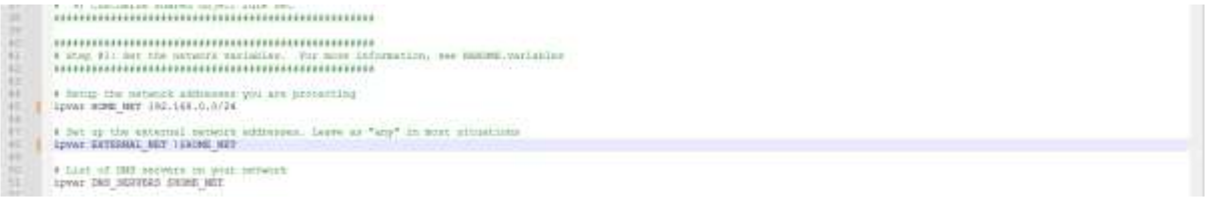
Snort v3.0

Snort v2.9

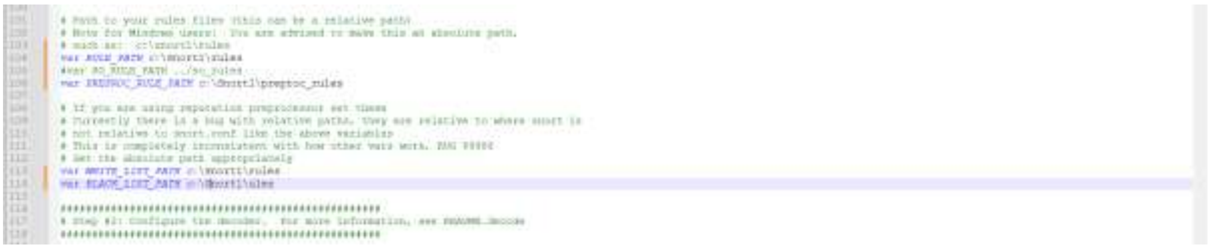
Practical 6: Demonstrate Snort


snort.conf
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

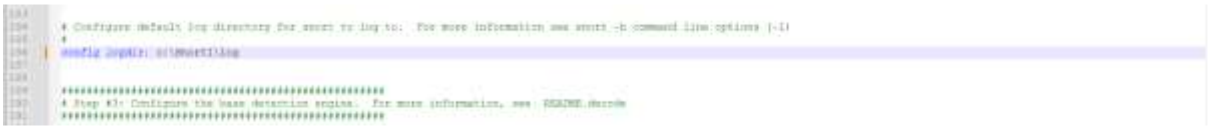
```
#--------------------------------------------------
#   VRT Rule Packages Snort.conf
#
#   For more information visit us at:
#     http://www.snort.org                   Snort Website
#     http://vrt-blog.snort.org/    Sourcefire VRT Blog
#
#     Mailing list Contact:      snort-users@lists.snort.org
#     False Positive reports:    fp@sourcefire.com
#     Snort bugs:                bugs@snort.org
#
#     Compatible with Snort Versions:
#     VERSIONS : 2.9.20
#
#     Snort build options:
#     OPTIONS : --enable-gre --enable-mpls --enable-targetbased --enable-ppm --enable-perfprofiling --enable-zlib --enable-active-response --enable-normalizer --enable-reload --enab
#
#     Additional information:
#     This configuration file enables active response, to run snort in
#     test mode -T you are required to supply an interface -i <interface>
#     or test mode will fail to fully validate the configuration and
#     exit with a FATAL error
#--------------------------------------------------

###################################################
# This file contains a sample snort configuration.
# You should take the following steps to create your own custom configuration:
#
#  1) Set the network variables.
#  2) Configure the decoder
#  3) Configure the base detection engine
#  4) Configure dynamic loaded libraries
#  5) Configure preprocessors
#  6) Configure output plugins
#  7) Customize your rule set
#  8) Customize preprocessor and decoder rule set
#  9) Customize shared object rule set
###################################################

###################################################
# Step #1: Set the network variables.  For more information, see README.variables
###################################################

# Setup the network addresses you are protecting
ipvar HOME_NET any

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
```



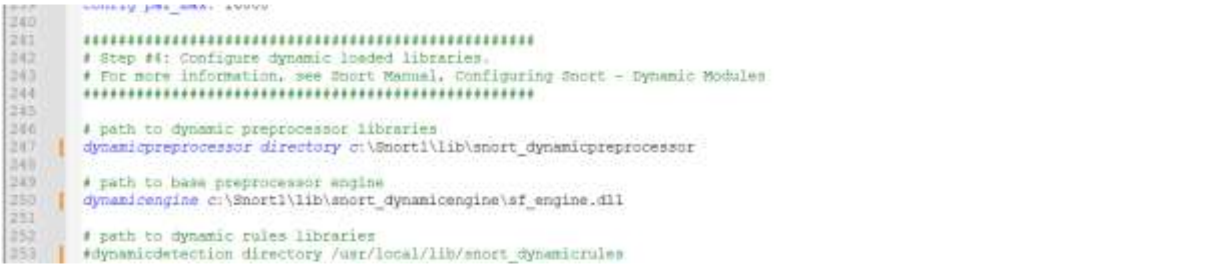
```
###################################################

###################################################
# Step #1: Set the network variables.  For more information, see README.variables
###################################################

# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.0.0/24

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET
```



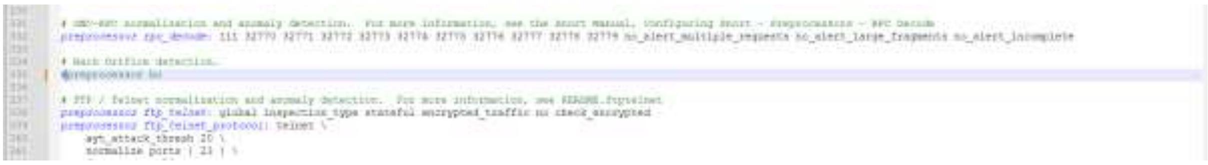
```
# Path to your rules files (this can be a relative path)
# Note for Windows users:  You are advised to make this an absolute path,
# such as:  c:\snort1\rules
var RULE_PATH c:\Snort1\rules
#var SO_RULE_PATH ../so_rules
var PREPROC_RULE_PATH c:\Snort1\preproc_rules

# If you are using reputation preprocessor set these
# Currently there is a bug with relative paths, they are relative to where snort is
# not relative to snort.conf like the above variables
# This is completely inconsistent with how other vars work, BUG 89986
# Set the absolute path appropriately
var WHITE_LIST_PATH c:\Snort1\rules
var BLACK_LIST_PATH c:\Snort1\rules

###################################################
# Step #2: Configure the decoder.  For more information, see README.decode
###################################################
```



```
# Configure default log directory for snort to log to.  For more information see snort -h command line options (-l)
#
config logdir: c:\Snort1\log


###################################################
# Step #3: Configure the base detection engine.  For more information, see  README.decode
###################################################
```

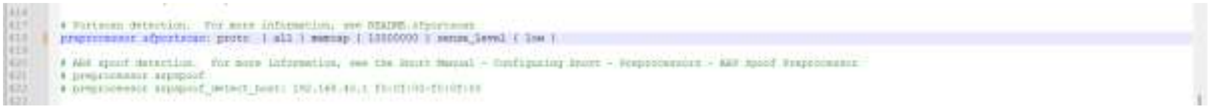


```
###################################################
# Step #4: Configure dynamic loaded libraries.
# For more information, see Snort Manual, Configuring Snort - Dynamic Modules
###################################################

# path to dynamic preprocessor libraries
dynamicpreprocessor directory c:\Snort1\lib\snort_dynamicpreprocessor

# path to base preprocessor engine
dynamicengine c:\Snort1\lib\snort_dynamicengine\sf_engine.dll

# path to dynamic rules libraries
#dynamicdetection directory /usr/local/lib/snort_dynamicrules
```

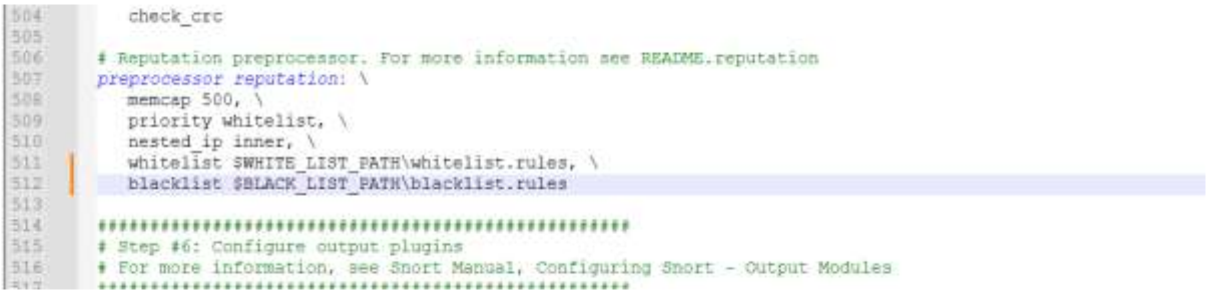


```
# ONC-RPC normalization and anomaly detection.  For more information, see the Snort Manual, Configuring Snort - Preprocessors - RPC Decode
preprocessor rpc_decode: 111 32770 32771 32772 32773 32774 32775 32776 32777 32778 32779 no_alert_multiple_requests no_alert_large_fragments no_alert_incomplete

# Back Orifice detection.
#preprocessor bo

# FTP / Telnet normalization and anomaly detection.  For more information, see README.ftptelnet
preprocessor ftp_telnet: global inspection_type stateful encrypted_traffic no check_encrypted
preprocessor ftp_telnet_protocol: telnet \
    ayt_attack_thresh 20 \
    normalize ports { 23 } \
```

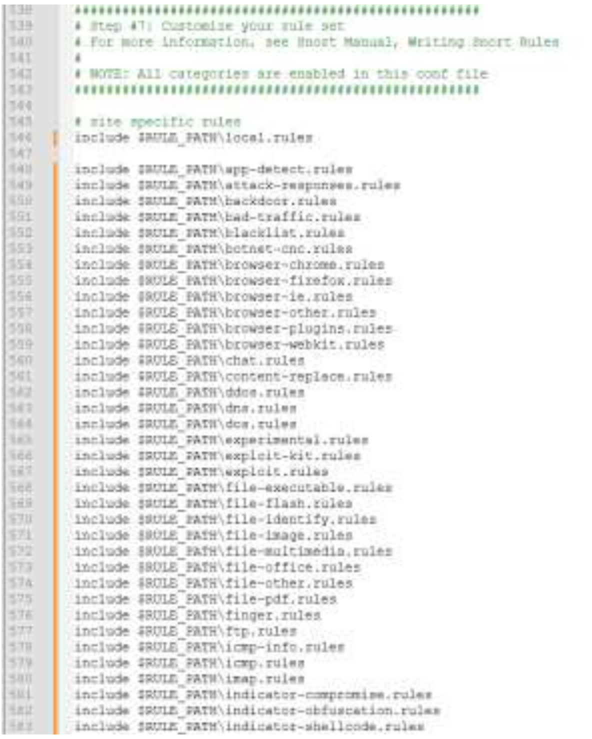
PRACTICAL 6: DEMONSTRATE SNORT



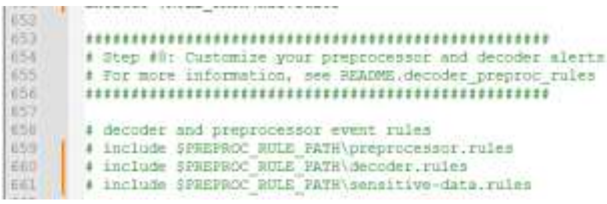
```
# Portscan detection.  For more information, see README.sfportscan
preprocessor sfportscan: proto  { all } memcap { 10000000 } sense_level { low }

# ARP spoof detection.  For more information, see the Snort Manual - Configuring Snort - Preprocessors - ARP Spoof Preprocessor
# preprocessor arpspoof
# preprocessor arpspoof_detect_host: 192.168.40.1 f0:0f:00:f0:0f:00
```



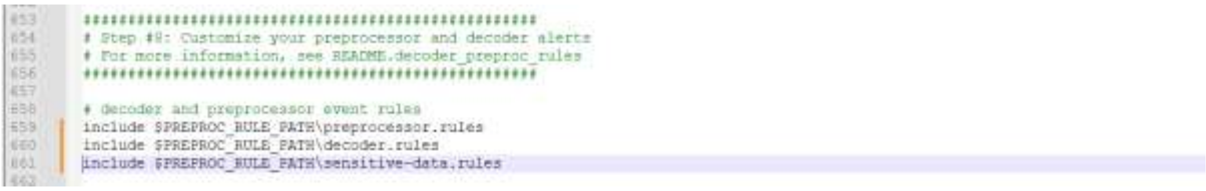
```
   check_crc

# Reputation preprocessor. For more information see README.reputation
preprocessor reputation: \
   memcap 500, \
   priority whitelist, \
   nested_ip inner, \
   whitelist $WHITE_LIST_PATH\whitelist.rules, \
   blacklist $BLACK_LIST_PATH\blacklist.rules

###################################################
# Step #6: Configure output plugins
# For more information, see Snort Manual, Configuring Snort - Output Modules
###################################################
```



```
###################################################
# Step #7: Customize your rule set
# For more information, see Snort Manual, Writing Snort Rules
#
# NOTE: All categories are enabled in this conf file
###################################################

# site specific rules
include $RULE_PATH\local.rules

include $RULE_PATH\app-detect.rules
include $RULE_PATH\attack-responses.rules
include $RULE_PATH\backdoor.rules
include $RULE_PATH\bad-traffic.rules
include $RULE_PATH\blacklist.rules
include $RULE_PATH\botnet-cnc.rules
include $RULE_PATH\browser-chrome.rules
include $RULE_PATH\browser-firefox.rules
include $RULE_PATH\browser-ie.rules
include $RULE_PATH\browser-other.rules
include $RULE_PATH\browser-plugins.rules
include $RULE_PATH\browser-webkit.rules
include $RULE_PATH\chat.rules
include $RULE_PATH\content-replace.rules
include $RULE_PATH\ddos.rules
include $RULE_PATH\dns.rules
include $RULE_PATH\dos.rules
include $RULE_PATH\experimental.rules
include $RULE_PATH\exploit-kit.rules
include $RULE_PATH\exploit.rules
include $RULE_PATH\file-executable.rules
include $RULE_PATH\file-flash.rules
include $RULE_PATH\file-identify.rules
include $RULE_PATH\file-image.rules
include $RULE_PATH\file-multimedia.rules
include $RULE_PATH\file-office.rules
include $RULE_PATH\file-other.rules
include $RULE_PATH\file-pdf.rules
include $RULE_PATH\finger.rules
include $RULE_PATH\ftp.rules
include $RULE_PATH\icmp-info.rules
include $RULE_PATH\icmp.rules
include $RULE_PATH\imap.rules
include $RULE_PATH\indicator-compromise.rules
include $RULE_PATH\indicator-obfuscation.rules
include $RULE_PATH\indicator-shellcode.rules
```

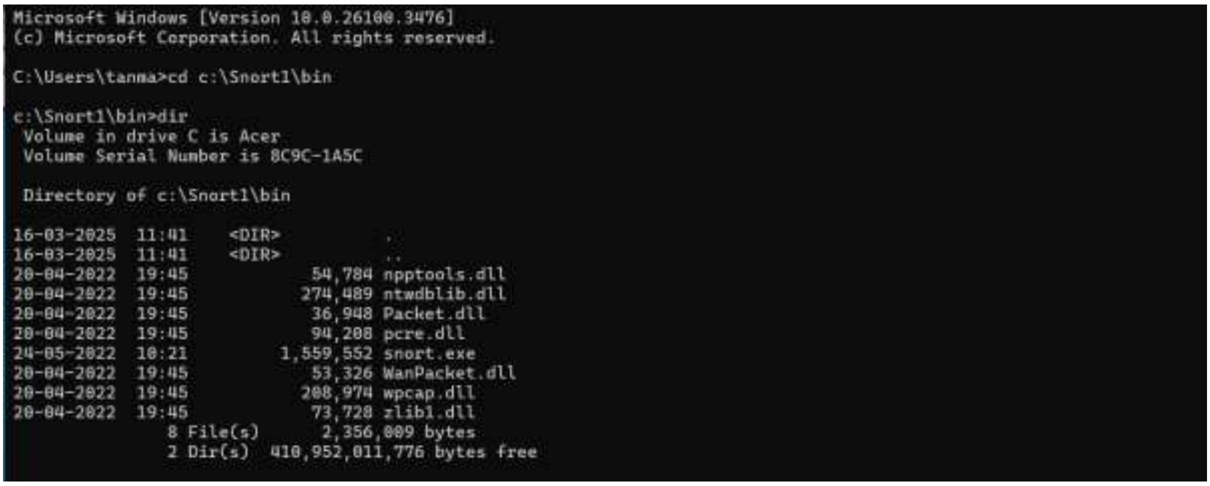


```
###################################################
# Step #8: Customize your preprocessor and decoder alerts
# For more information, see README.decoder_preproc_rules
###################################################

# decoder and preprocessor event rules
# include $PREPROC_RULE_PATH\preprocessor.rules
# include $PREPROC_RULE_PATH\decoder.rules
# include $PREPROC_RULE_PATH\sensitive-data.rules
```

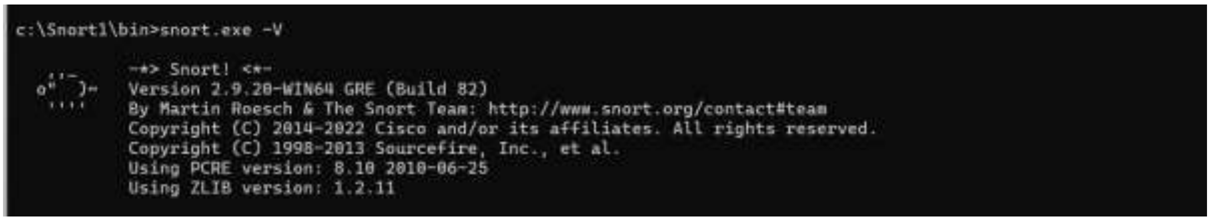


```
###################################################
# Step #8: Customize your preprocessor and decoder alerts
# For more information, see README.decoder_preproc_rules
###################################################

# decoder and preprocessor event rules
include $PREPROC_RULE_PATH\preprocessor.rules
include $PREPROC_RULE_PATH\decoder.rules
include $PREPROC_RULE_PATH\sensitive-data.rules
```

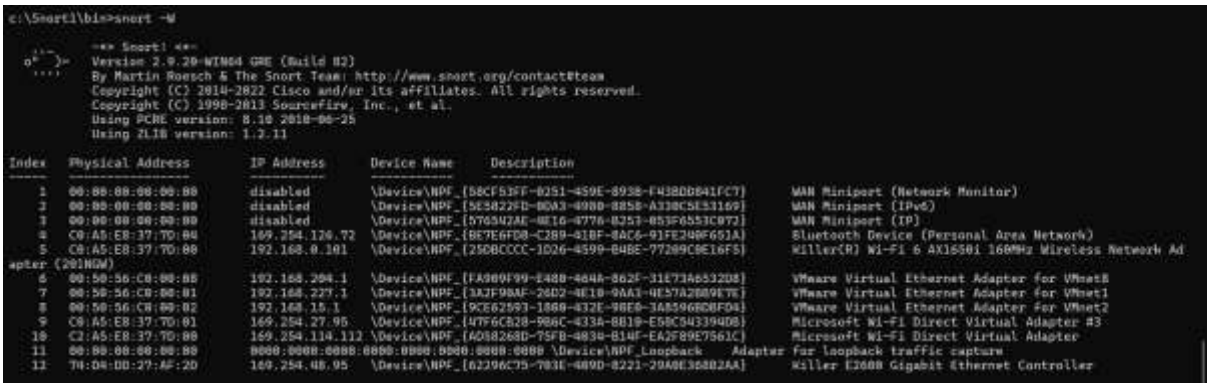
PRACTICAL 6: DEMONSTRATE SNORT



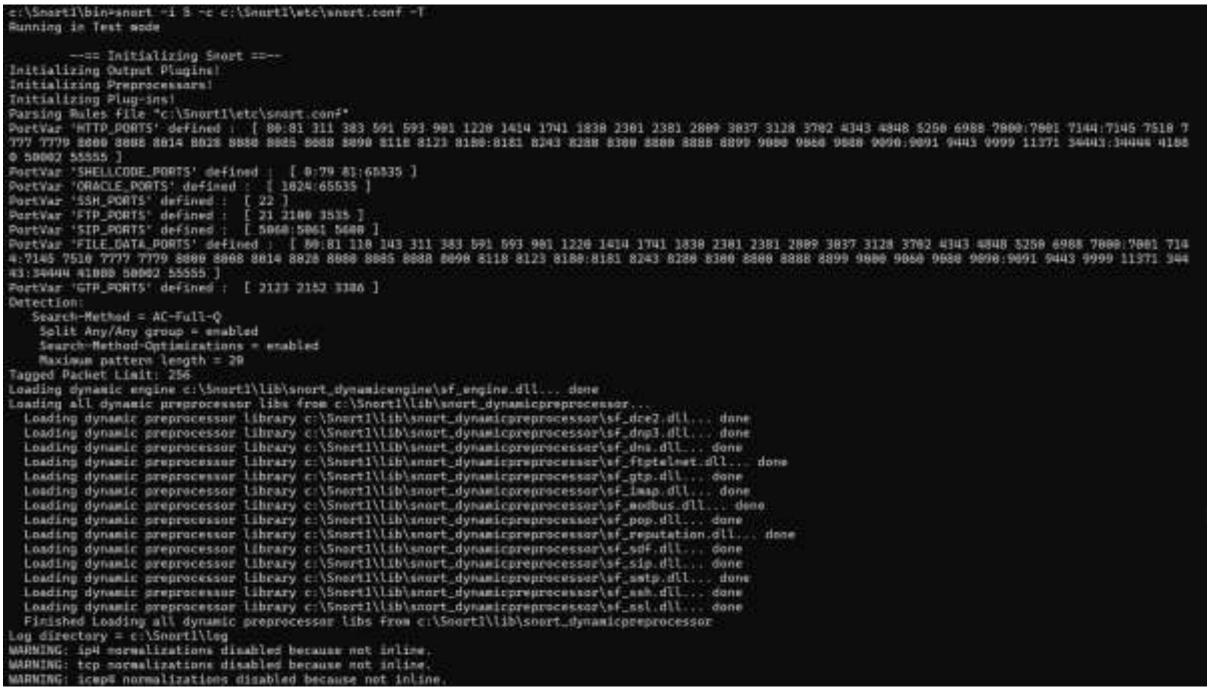
```
Microsoft Windows [Version 10.0.26100.3476]
(c) Microsoft Corporation. All rights reserved.

C:\Users\tanma>cd c:\Snort1\bin

c:\Snort1\bin>dir
 Volume in drive C is Acer
 Volume Serial Number is 8C9C-1A5C

 Directory of c:\Snort1\bin

16-03-2025  11:41    <DIR>          .
16-03-2025  11:41    <DIR>          ..
20-04-2022  19:45            54,784 npptools.dll
20-04-2022  19:45           274,489 ntwdblib.dll
20-04-2022  19:45            36,948 Packet.dll
20-04-2022  19:45            94,208 pcre.dll
24-05-2022  10:21         1,559,552 snort.exe
20-04-2022  19:45            53,326 WanPacket.dll
20-04-2022  19:45           208,974 wpcap.dll
20-04-2022  19:45            73,728 zlib1.dll
               8 File(s)      2,356,009 bytes
               2 Dir(s)  410,952,011,776 bytes free
```



```
c:\Snort1\bin>snort.exe -V

   ,,_     -*> 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
```

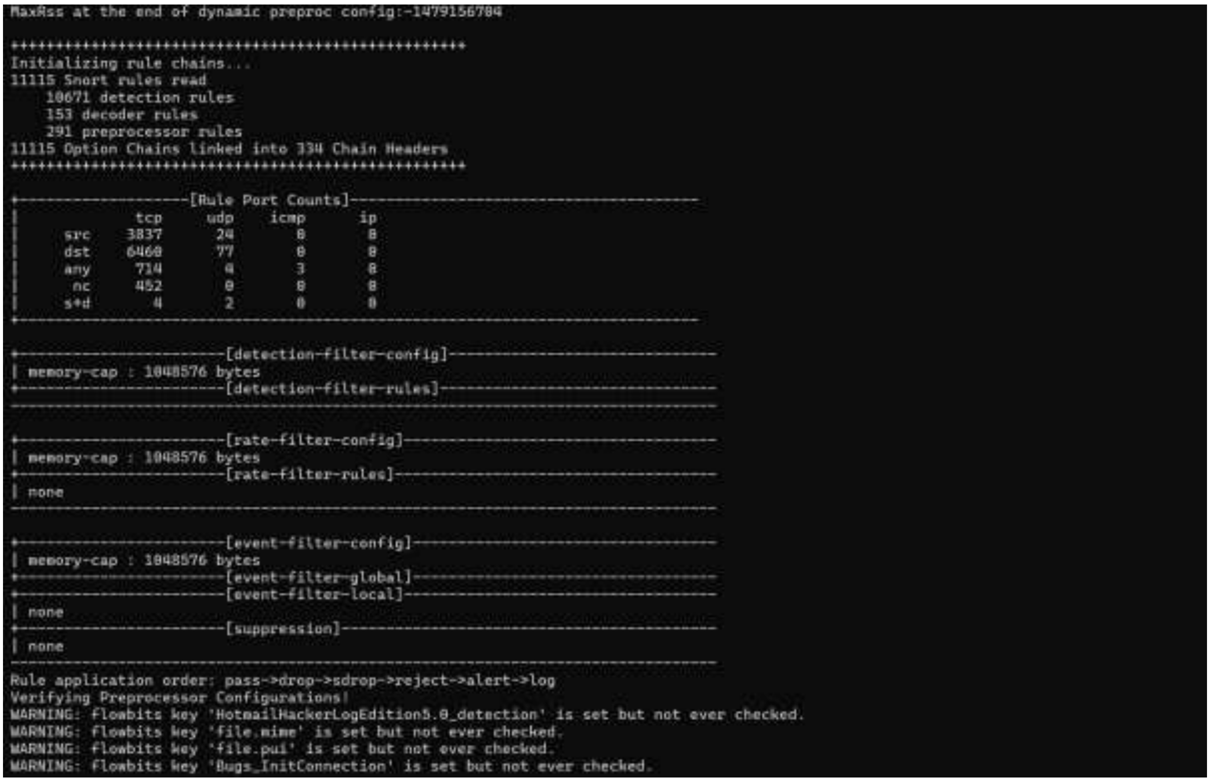


```
c:\Snort1\bin>snort -W

   ,,_     -*> 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_{58CF53FF-0251-459E-8938-F43BDD841FC7}      WAN Miniport (Network Monitor)
    2  00:00:00:00:00:00    disabled         \Device\NPF_{5E5822FD-0DA3-4980-8858-A330C5E53169}      WAN Miniport (IPv6)
    3  00:00:00:00:00:00    disabled         \Device\NPF_{576542AE-0E16-4776-8253-053F6553C072}      WAN Miniport (IP)
    4  C0:A5:E8:37:7D:04    169.254.126.72   \Device\NPF_{BE7E6FD8-C289-41BF-8AC6-91FE240F651A}      Bluetooth Device (Personal Area Network)
    5  C0:A5:E8:37:7D:00    192.168.0.101    \Device\NPF_{25DBCCCC-1D26-4599-B4BE-77209C0E16F5}      Killer(R) Wi-Fi 6 AX1650i 160MHz Wireless Network Ad
apter (201NGW)
    6  00:50:56:C0:00:08    192.168.204.1    \Device\NPF_{FA909F99-E488-464A-862F-31E73A6532D8}      VMware Virtual Ethernet Adapter for VMnet8
    7  00:50:56:C0:00:01    192.168.227.1    \Device\NPF_{3A2F98AF-26D2-4E10-9AA3-4E57A2B09E7E}      VMware Virtual Ethernet Adapter for VMnet1
    8  00:50:56:C0:00:02    192.168.15.1     \Device\NPF_{9CE62593-1860-432E-98E0-3A8596BDBFD4}      VMware Virtual Ethernet Adapter for VMnet2
    9  C0:A5:E8:37:7D:01    169.254.27.95    \Device\NPF_{47F6CB28-986C-433A-8810-E58C543394D8}      Microsoft Wi-Fi Direct Virtual Adapter #3
   10  C2:A5:E8:37:7D:00    169.254.114.112 \Device\NPF_{AD58268D-75FB-4834-814F-EA2F89E7561C}      Microsoft Wi-Fi Direct Virtual Adapter
   11  00:00:00:00:00:00    0000:0000:0000:0000:0000:0000:0000:0000 \Device\NPF_Loopback    Adapter for loopback traffic capture
   12  74:D4:DD:27:AF:2D    169.254.48.95    \Device\NPF_{62296C75-703E-489D-8221-29A0E36802AA}      Killer E2600 Gigabit Ethernet Controller
```



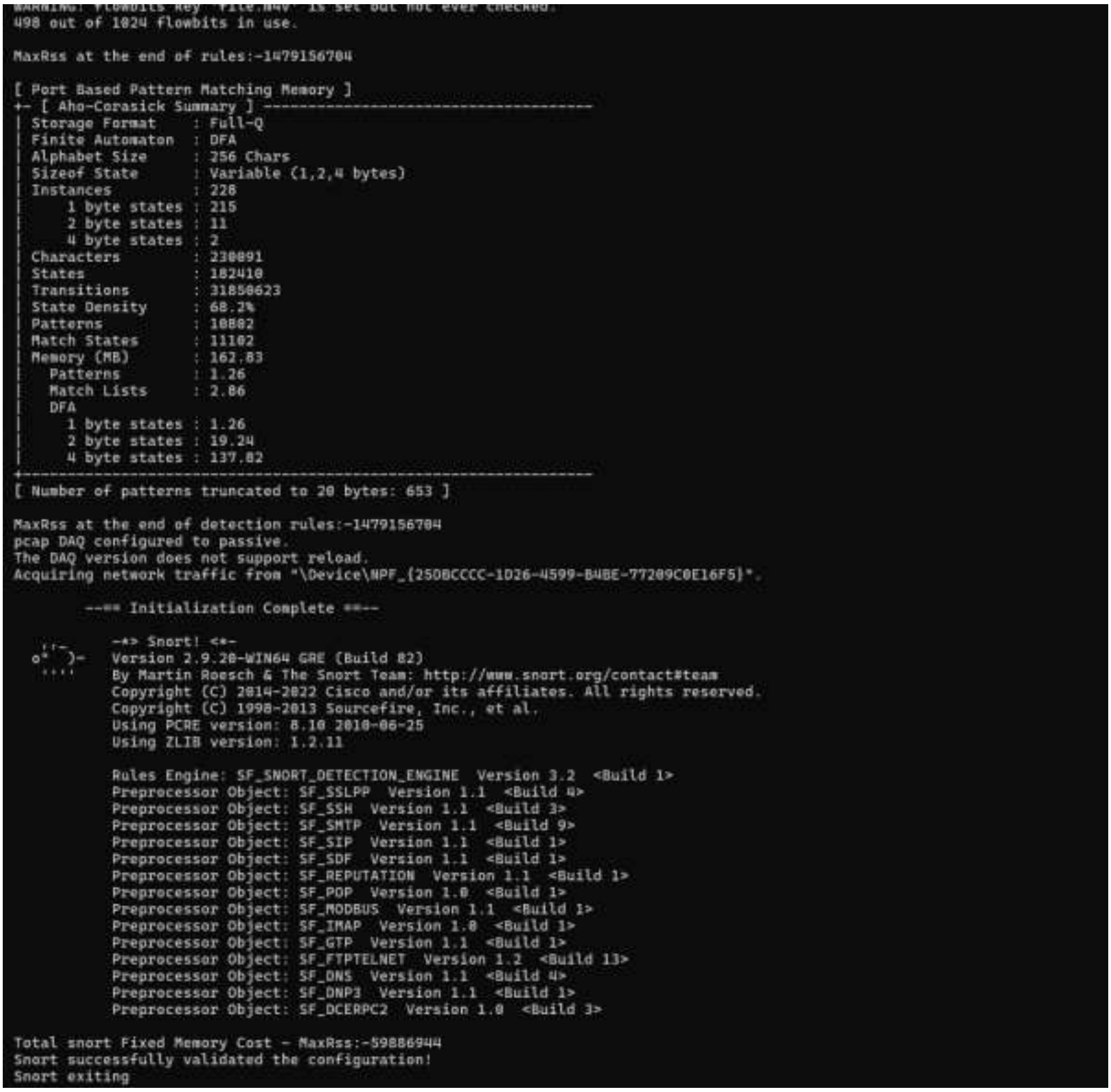
```
c:\Snort1\bin>snort -i 5 -c c:\Snort1\etc\snort.conf -T
Running in Test mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "c:\Snort1\etc\snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7
777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 4100
0 50002 55555 ]
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 3037 3128 3702 4343 4848 5250 6988 7000:7001 714
4:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 344
43:34444 41000 50002 55555 ]
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:\Snort1\lib\snort_dynamicengine\sf_engine.dll... done
Loading all dynamic preprocessor libs from c:\Snort1\lib\snort_dynamicpreprocessor...
  Loading dynamic preprocessor library c:\Snort1\lib\snort_dynamicpreprocessor\sf_dce2.dll... done
  Loading dynamic preprocessor library c:\Snort1\lib\snort_dynamicpreprocessor\sf_dnp3.dll... done
  Loading dynamic preprocessor library c:\Snort1\lib\snort_dynamicpreprocessor\sf_dns.dll... done
  Loading dynamic preprocessor library c:\Snort1\lib\snort_dynamicpreprocessor\sf_ftptelnet.dll... done
  Loading dynamic preprocessor library c:\Snort1\lib\snort_dynamicpreprocessor\sf_gtp.dll... done
  Loading dynamic preprocessor library c:\Snort1\lib\snort_dynamicpreprocessor\sf_imap.dll... done
  Loading dynamic preprocessor library c:\Snort1\lib\snort_dynamicpreprocessor\sf_modbus.dll... done
  Loading dynamic preprocessor library c:\Snort1\lib\snort_dynamicpreprocessor\sf_pop.dll... done
  Loading dynamic preprocessor library c:\Snort1\lib\snort_dynamicpreprocessor\sf_reputation.dll... done
  Loading dynamic preprocessor library c:\Snort1\lib\snort_dynamicpreprocessor\sf_sdf.dll... done
  Loading dynamic preprocessor library c:\Snort1\lib\snort_dynamicpreprocessor\sf_sip.dll... done
  Loading dynamic preprocessor library c:\Snort1\lib\snort_dynamicpreprocessor\sf_smtp.dll... done
  Loading dynamic preprocessor library c:\Snort1\lib\snort_dynamicpreprocessor\sf_ssh.dll... done
  Loading dynamic preprocessor library c:\Snort1\lib\snort_dynamicpreprocessor\sf_ssl.dll... done
  Finished Loading all dynamic preprocessor libs from c:\Snort1\lib\snort_dynamicpreprocessor
Log directory = c:\Snort1\log
WARNING: ip4 normalizations disabled because not inline.
WARNING: tcp normalizations disabled because not inline.
WARNING: icmp4 normalizations disabled because not inline.
```

Practical 6: Demonstrate Snort

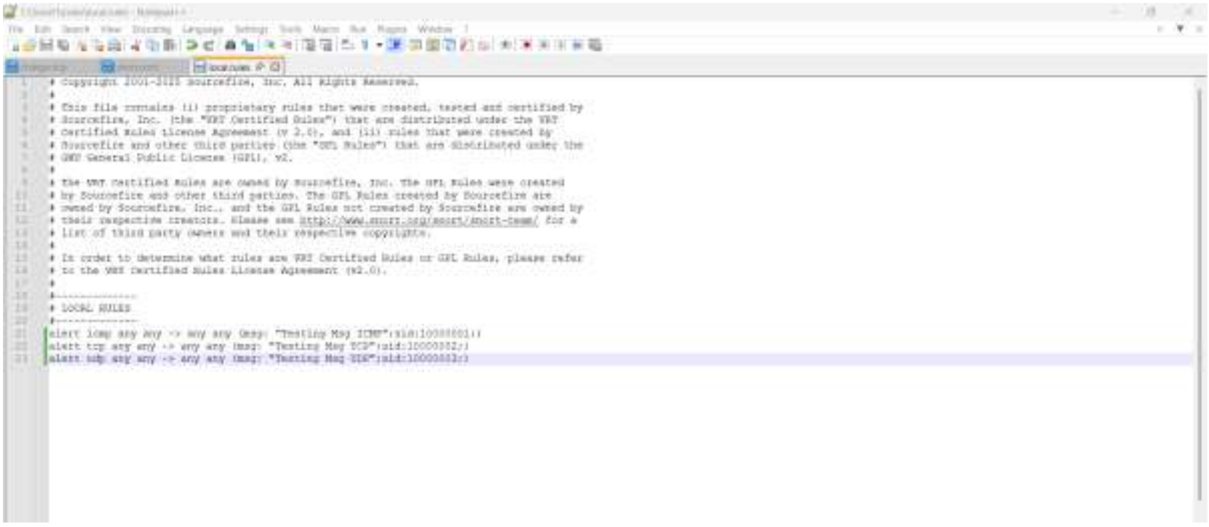


```
MaxRss at the end of dynamic preproc config:-1479156784

+++++++++++++++++++++++++++++++++++++++++++++++++++
Initializing rule chains...
11115 Snort rules read
    10671 detection rules
    153 decoder rules
    291 preprocessor rules
11115 Option Chains linked into 334 Chain Headers
+++++++++++++++++++++++++++++++++++++++++++++++++++

+-------------------[Rule Port Counts]---------------------------------------
|             tcp     udp    icmp      ip
|     src    3837      24       0       0
|     dst    6460      77       0       0
|     any     714       4       3       0
|      nc     452       0       0       0
|     s+d       4       2       0       0
+----------------------------------------------------------------------------

+-----------------------[detection-filter-config]------------------------------
| memory-cap : 1048576 bytes
+-----------------------[detection-filter-rules]-------------------------------
-------------------------------------------------------------------------------

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

+-----------------------[event-filter-config]----------------------------------
| memory-cap : 1048576 bytes
+-----------------------[event-filter-global]----------------------------------
+-----------------------[event-filter-local]-----------------------------------
| none
+-----------------------[suppression]------------------------------------------
| none
-------------------------------------------------------------------------------
Rule application order: pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!
WARNING: flowbits key 'HotmailHackerLogEdition5.0_detection' is set but not ever checked.
WARNING: flowbits key 'file.mime' is set but not ever checked.
WARNING: flowbits key 'file.pui' is set but not ever checked.
WARNING: flowbits key 'Bugs_InitConnection' is set but not ever checked.
```

PRACTICAL 6: DEMONSTRATE SNORT

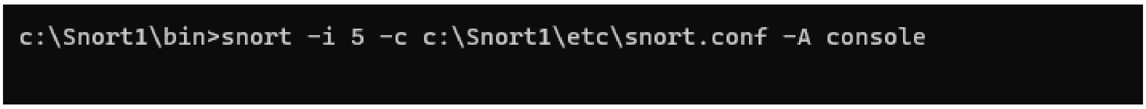


```
WARNING: flowbits key 'file.m4v' is set but not ever checked.
498 out of 1024 flowbits in use.

MaxRss at the end of rules:-1479156704

[ 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         : 228
|     1 byte states : 215
|     2 byte states : 11
|     4 byte states : 2
| Characters        : 230891
| States            : 182410
| Transitions       : 31850623
| State Density     : 68.2%
| Patterns          : 10802
| Match States      : 11102
| Memory (MB)       : 162.83
|   Patterns        : 1.26
|   Match Lists     : 2.86
|   DFA
|     1 byte states : 1.26
|     2 byte states : 19.24
|     4 byte states : 137.82
+----------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 653 ]

MaxRss at the end of detection rules:-1479156704
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{250BCCCC-1D26-4599-B4BE-77209C0E16F5}".

        --== Initialization Complete ==--

   ,,_     -*> 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

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.2  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>

Total snort Fixed Memory Cost - MaxRss:-59886944
Snort successfully validated the configuration!
Snort exiting
```



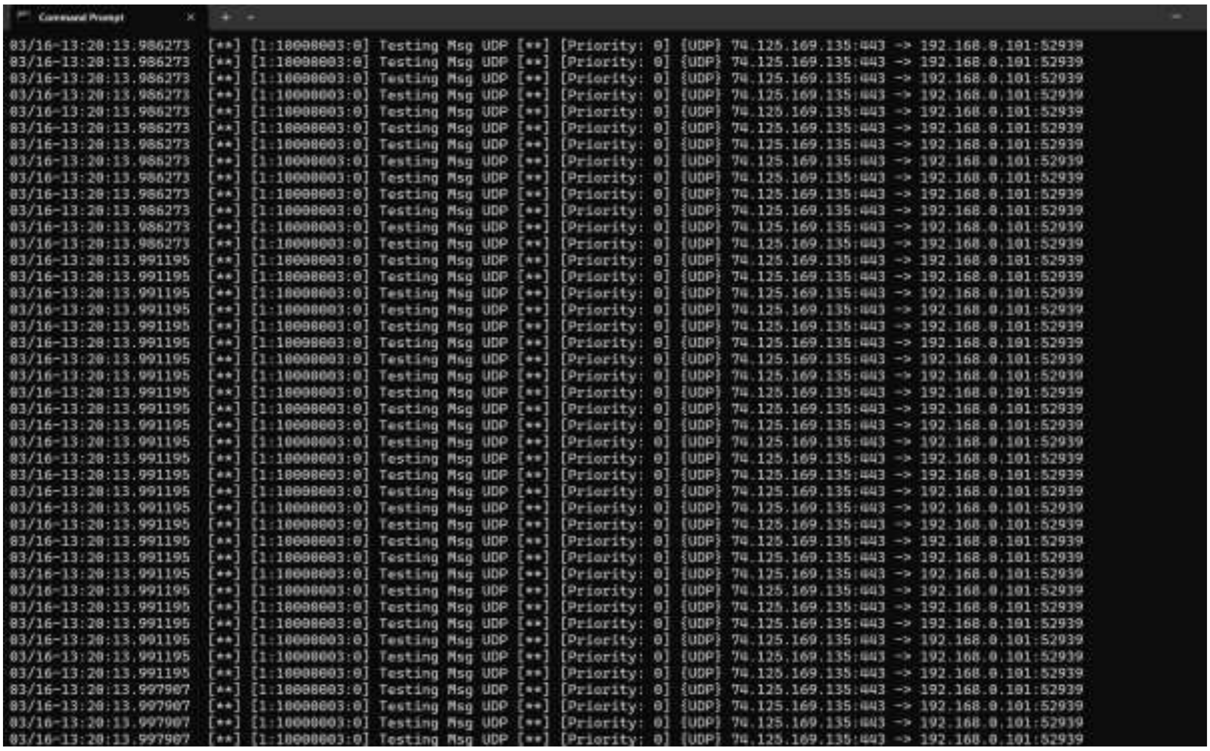
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
local.rules

```
# Copyright 2001-2022 Sourcefire, Inc. All Rights Reserved.
#
# This file contains (i) proprietary rules that were created, tested and certified by
# Sourcefire, Inc. (the "VRT Certified Rules") that are distributed under the VRT
# Certified Rules License Agreement (v 2.0), and (ii) rules that were created by
# Sourcefire and other third parties (the "GPL Rules") that are distributed under the
# GNU General Public License (GPL), v2.
#
# The VRT Certified Rules are owned by Sourcefire, Inc. The GPL Rules were created
# by Sourcefire and other third parties. The GPL Rules created by Sourcefire are
# owned by Sourcefire, Inc., and the GPL Rules not created by Sourcefire are owned by
# their respective creators. Please see http://www.snort.org/snort/snort-team/ for a
# list of third party owners and their respective copyrights.
#
# In order to determine what rules are VRT Certified Rules or GPL Rules, please refer
# to the VRT Certified Rules License Agreement (v2.0).
#
#-------------
# LOCAL RULES
#-------------
alert icmp any any -> any any (msg: "Testing Msg ICMP";sid:10000001;)
alert tcp any any -> any any (msg: "Testing Msg TCP";sid:10000002;)
alert udp any any -> any any (msg: "Testing Msg UDP";sid:10000003;)
```

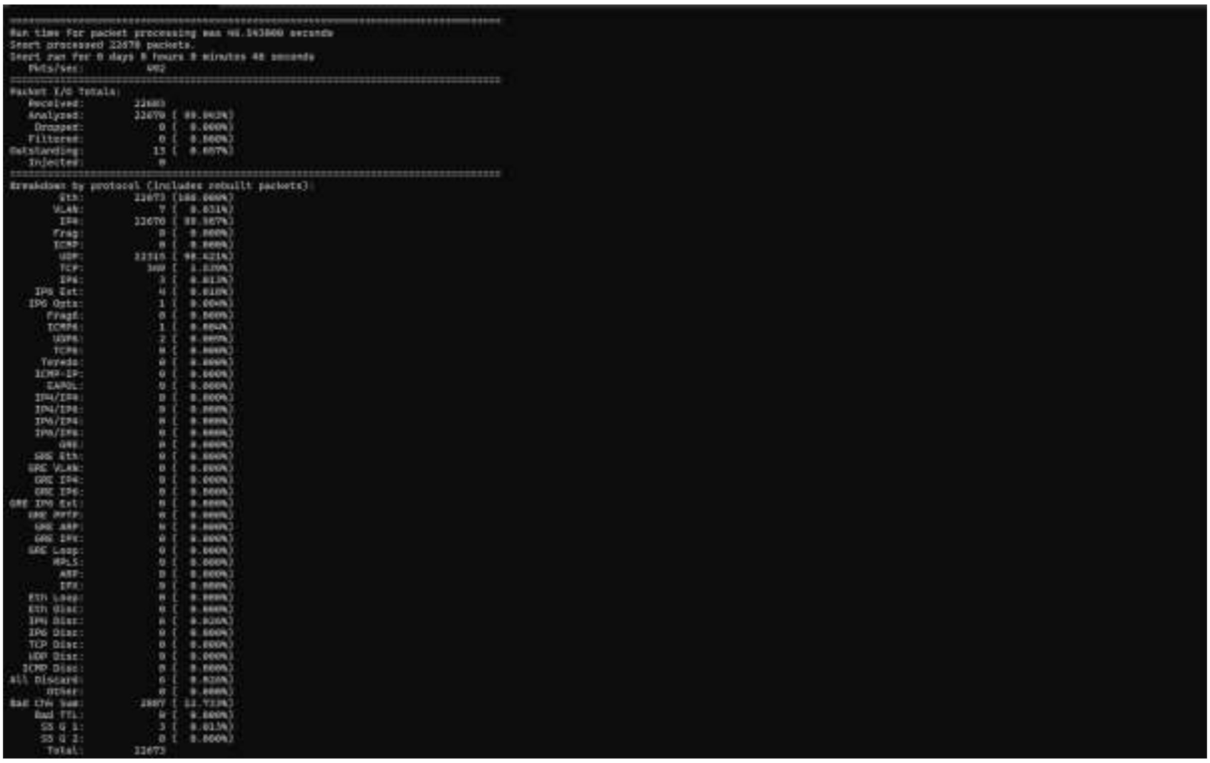


```
c:\Snort1\bin>snort -i 5 -c c:\Snort1\etc\snort.conf -A console
```

PRACTICAL 6: DEMONSTRATE SNORT

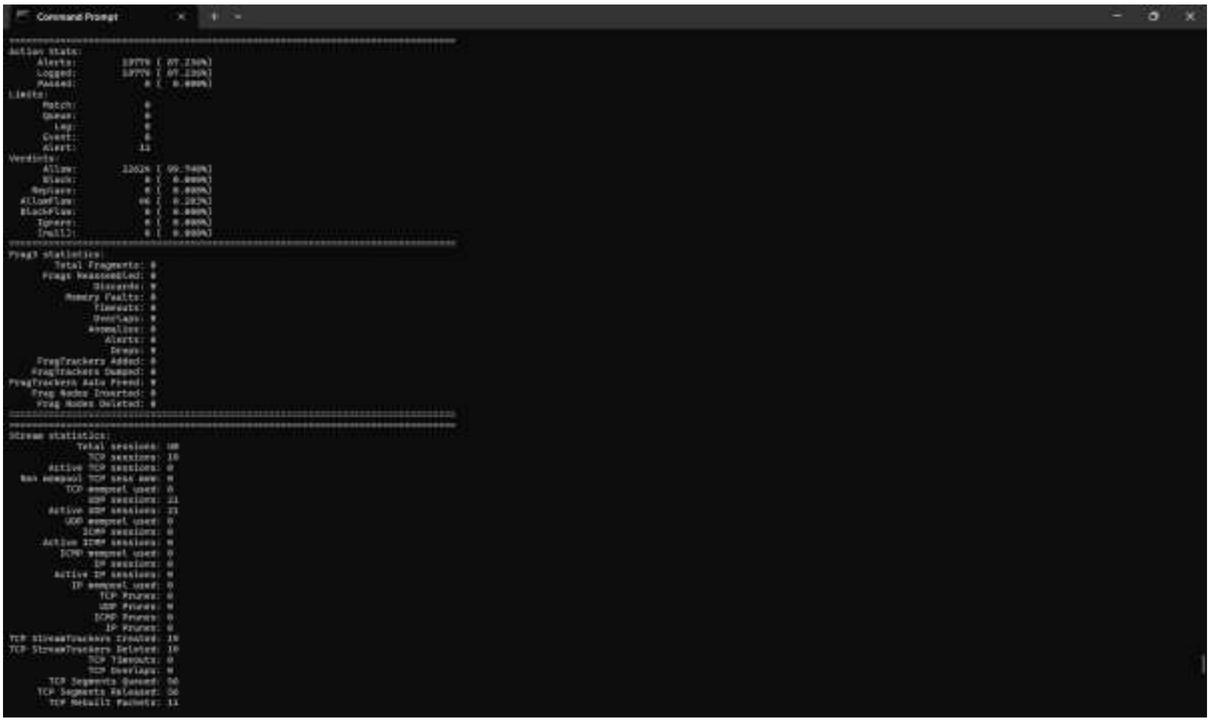


```
03/16-13:20:13.986273  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.986273  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.986273  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.986273  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.986273  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.986273  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.986273  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.986273  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.986273  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.986273  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.986273  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.986273  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.986273  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.991195  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.991195  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.991195  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.991195  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.991195  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.991195  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.991195  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.991195  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.991195  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.991195  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.991195  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.991195  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.991195  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.991195  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.991195  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.991195  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.991195  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.991195  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.991195  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.991195  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.991195  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.991195  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.991195  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.991195  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.991195  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.991195  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.997907  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.997907  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.997907  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
03/16-13:20:13.997907  [**] [1:10000003:0] Testing Msg UDP [**] [Priority: 0] {UDP} 74.125.169.135:443 -> 192.168.0.101:52939
```

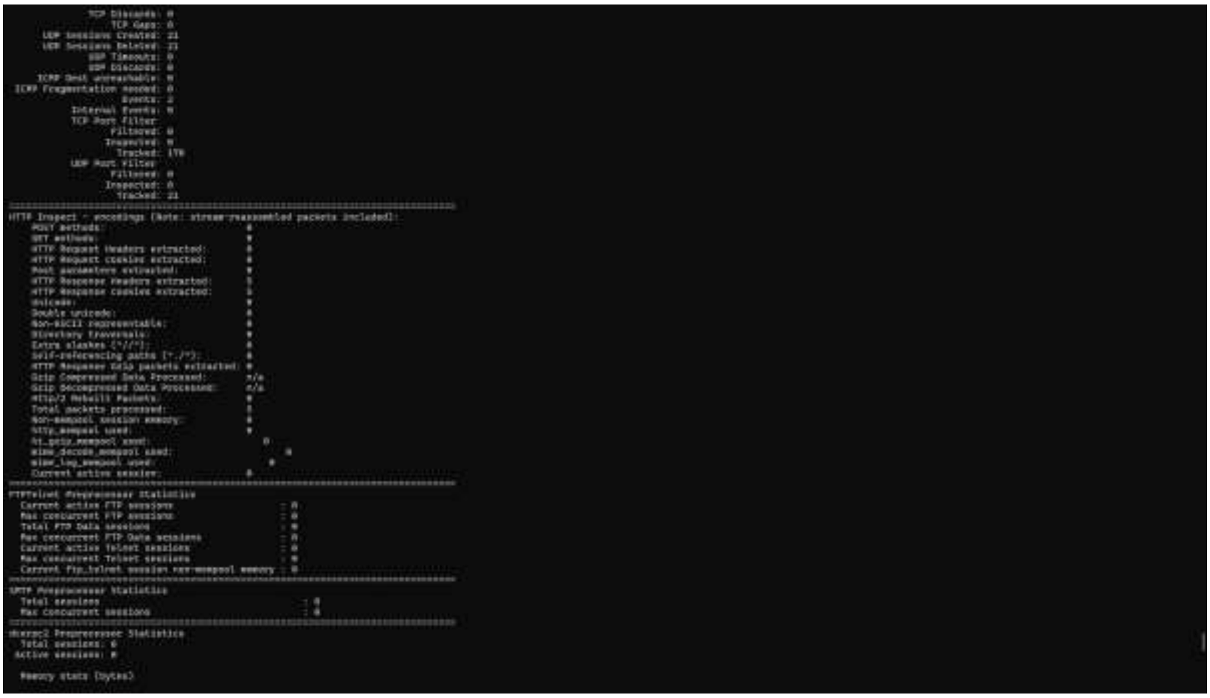


```
===============================================================================
Run time for packet processing was 46.343000 seconds
Snort processed 22670 packets.
Snort ran for 0 days 0 hours 0 minutes 46 seconds
   Pkts/sec:          492
===============================================================================
Packet I/O Totals:
   Received:        22683
   Analyzed:        22670 ( 99.943%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:           13 (  0.057%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:        22673 (100.000%)
       VLAN:            7 (  0.031%)
        IP4:        22670 ( 99.987%)
       Frag:            0 (  0.000%)
       ICMP:            0 (  0.000%)
        UDP:        22315 ( 98.421%)
        TCP:          300 (  1.323%)
        IP6:            3 (  0.013%)
    IP6 Ext:            4 (  0.018%)
   IP6 Opts:            1 (  0.004%)
      Frag6:            0 (  0.000%)
      ICMP6:            1 (  0.004%)
       UDP6:            2 (  0.009%)
       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:            6 (  0.026%)
   IP6 Disc:            0 (  0.000%)
   TCP Disc:            0 (  0.000%)
   UDP Disc:            0 (  0.000%)
  ICMP Disc:            0 (  0.000%)
All Discard:            6 (  0.026%)
      Other:            0 (  0.000%)
Bad Chk Sum:         2887 ( 12.733%)
    Bad TTL:            0 (  0.000%)
     S5 G 1:            3 (  0.013%)
     S5 G 2:            0 (  0.000%)
      Total:        22673
```

Practical 6: Demonstrate Snort

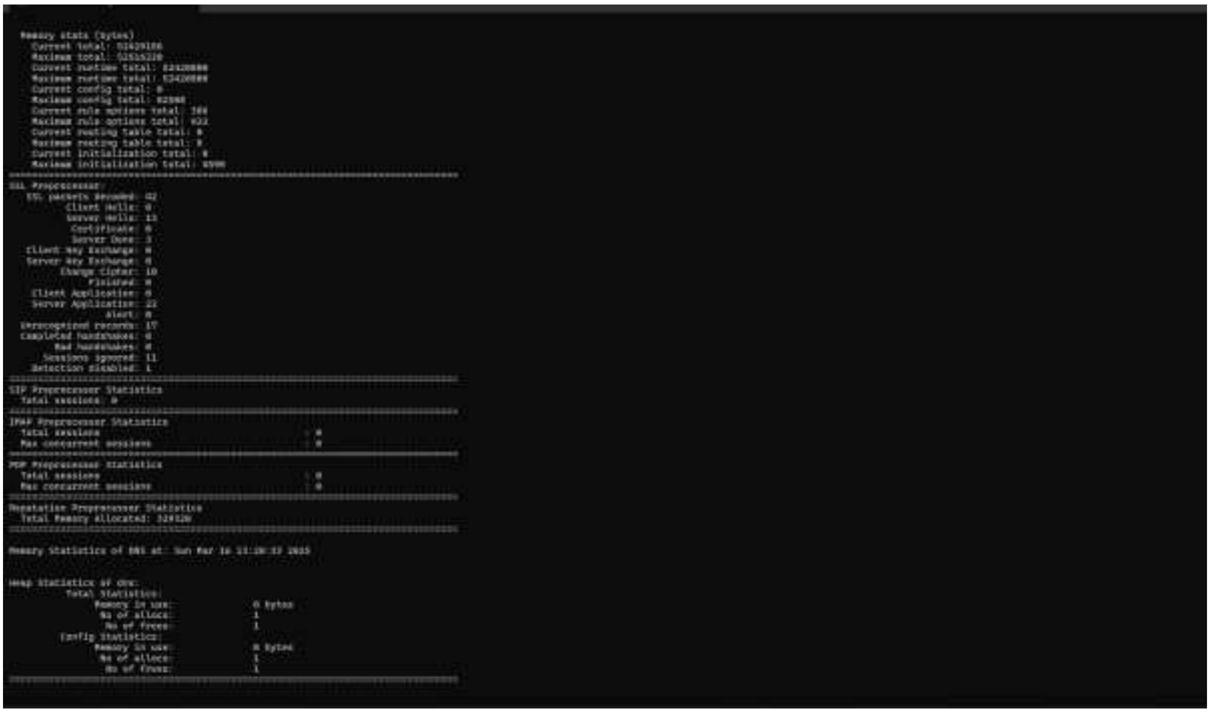


```
===============================================================================
Action Stats:
     Alerts:        19779 ( 87.236%)
     Logged:        19779 ( 87.236%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
      Queue:            0
        Log:            0
      Event:            0
      Alert:           11
Verdicts:
      Allow:        22626 ( 99.740%)
      Block:            0 (  0.000%)
    Replace:            0 (  0.000%)
  AllowFlow:           46 (  0.203%)
  BlockFlow:            0 (  0.000%)
     Ignore:            0 (  0.000%)
      Retry:            0 (  0.000%)
===============================================================================
Frag3 statistics:
        Total Fragments: 0
      Frags Reassembled: 0
               Discards: 0
          Memory Faults: 0
               Timeouts: 0
               Overlaps: 0
              Anomalies: 0
                 Alerts: 0
                  Drops: 0
     FragTrackers Added: 0
    FragTrackers Dumped: 0
FragTrackers Auto Freed: 0
    Frag Nodes Inserted: 0
     Frag Nodes Deleted: 0
===============================================================================
===============================================================================
Stream statistics:
            Total sessions: 40
              TCP sessions: 19
       Active TCP sessions: 0
  Non mempool TCP sess mem: 0
         TCP mempool used: 0
              UDP sessions: 21
       Active UDP sessions: 21
         UDP mempool used: 0
             ICMP sessions: 0
      Active ICMP sessions: 0
        ICMP mempool used: 0
               IP sessions: 0
        Active IP sessions: 0
          IP mempool used: 0
               TCP Prunes: 0
               UDP Prunes: 0
              ICMP Prunes: 0
                IP Prunes: 0
TCP StreamTrackers Created: 19
TCP StreamTrackers Deleted: 19
              TCP Timeouts: 0
              TCP Overlaps: 0
       TCP Segments Queued: 56
     TCP Segments Released: 56
       TCP Rebuilt Packets: 11
```

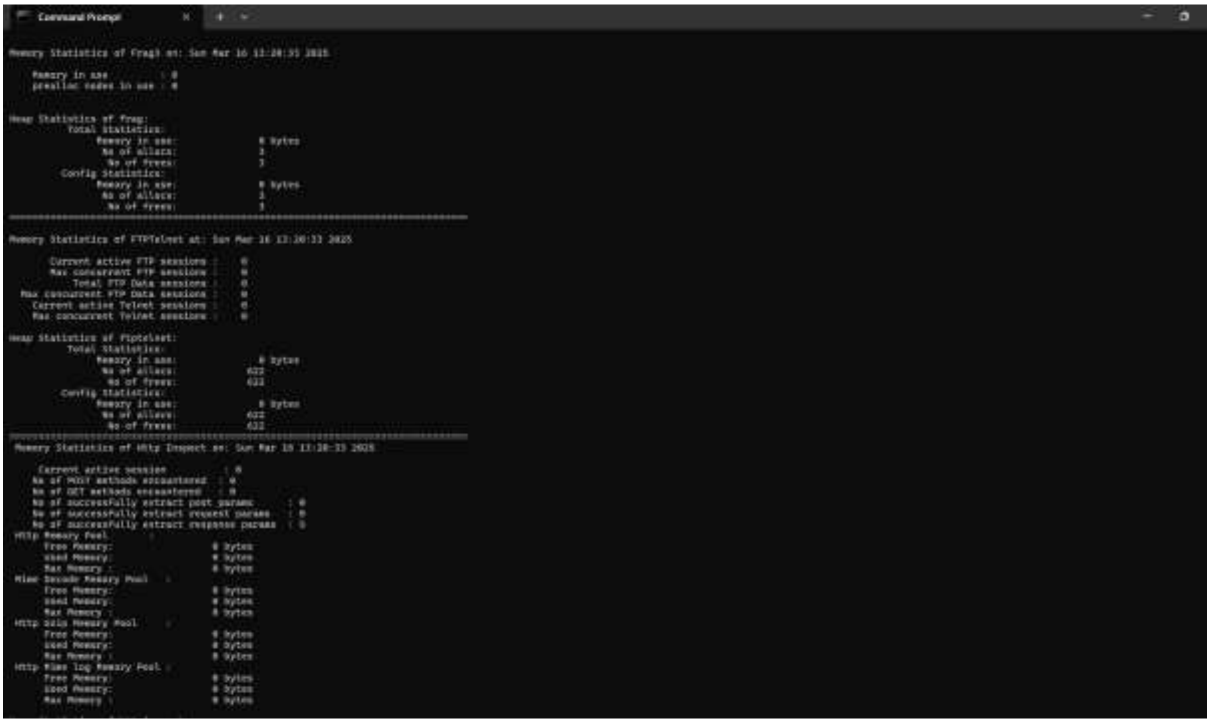


```
              TCP Discards: 0
                  TCP Gaps: 0
      UDP Sessions Created: 21
      UDP Sessions Deleted: 21
              UDP Timeouts: 0
              UDP Discards: 0
     ICMP Dest unreachable: 0
 ICMP Fragmentation needed: 0
                    Events: 2
           Internal Events: 0
           TCP Port Filter
                  Filtered: 0
                 Inspected: 0
                   Tracked: 178
           UDP Port Filter
                  Filtered: 0
                 Inspected: 0
                   Tracked: 21
===============================================================================
HTTP Inspect - encodings (Note: stream-reassembled packets included):
    POST methods:                         0
    GET methods:                          0
    HTTP Request Headers extracted:       0
    HTTP Request cookies extracted:       0
    Post parameters extracted:            0
    HTTP Response Headers extracted:      1
    HTTP Response cookies extracted:      1
    Unicode:                              0
    Double unicode:                       0
    Non-ASCII representable:              0
    Directory traversals:                 0
    Extra slashes ("//"):                 0
    Self-referencing paths ("./"):        0
    HTTP Response Gzip packets extracted: 0
    Gzip Compressed Data Processed:       n/a
    Gzip Decompressed Data Processed:     n/a
    Http/2 Rebuilt Packets:               0
    Total packets processed:              1
    Non-mempool session memory:           0
    http_mempool used:                    0
    hi_gzip_mempool used:                    0
    mime_decode_mempool used:                    0
    mime_log_mempool used:                    0
    Current active session:               0
===============================================================================
FTPTelnet Preprocessor Statistics
  Current active FTP sessions                     : 0
  Max concurrent FTP sessions                     : 0
  Total FTP Data sessions                         : 0
  Max concurrent FTP Data sessions                : 0
  Current active Telnet sessions                  : 0
  Max concurrent Telnet sessions                  : 0
  Current ftp_telnet session non-mempool memory   : 0
===============================================================================
SMTP Preprocessor Statistics
  Total sessions                                    : 0
  Max concurrent sessions                           : 0
===============================================================================
dcerpc2 Preprocessor Statistics
  Total sessions: 0
 Active sessions: 0

  Memory stats (bytes)
```

PRACTICAL 6: DEMONSTRATE SNORT

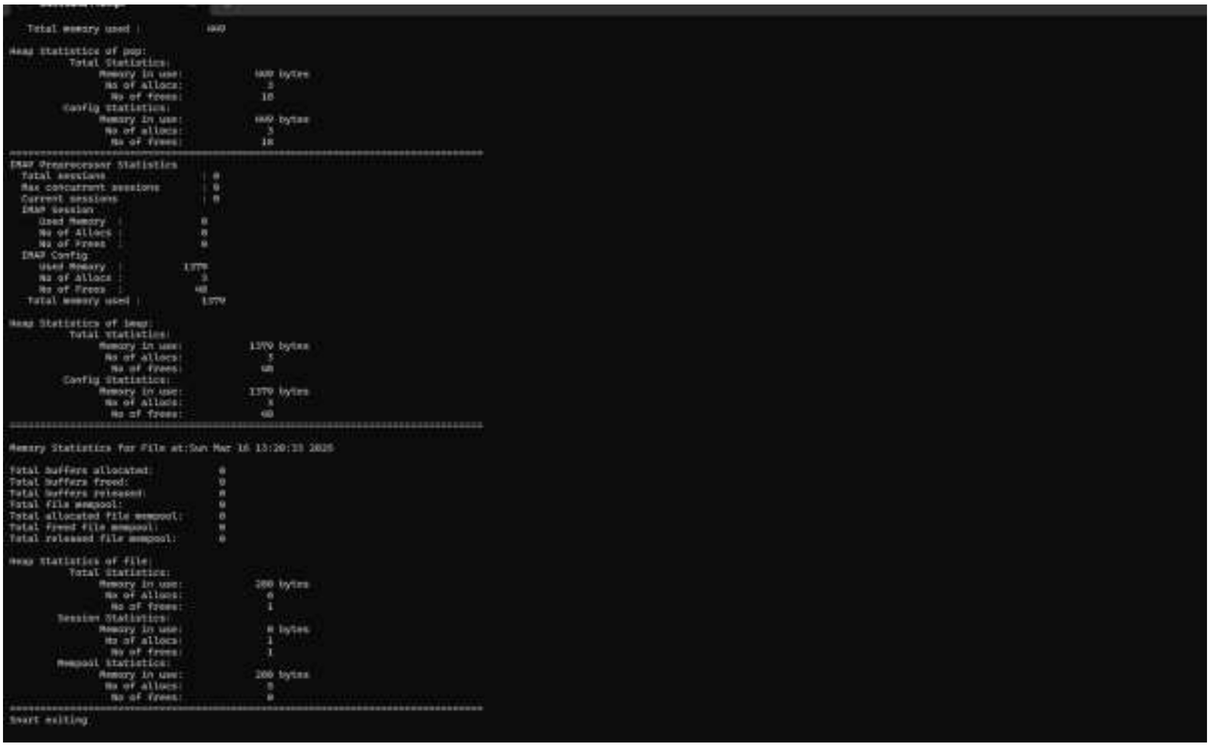


```
  Memory stats (bytes)
    Current total: 52429186
    Maximum total: 52515220
    Current runtime total: 52428800
    Maximum runtime total: 52428800
    Current config total: 0
    Maximum config total: 82988
    Current rule options total: 388
    Maximum rule options total: 422
    Current routing table total: 0
    Maximum routing table total: 0
    Current initialization total: 0
    Maximum initialization total: 6900
===============================================================================
SSL Preprocessor:
   SSL packets decoded: 42
          Client Hello: 0
          Server Hello: 13
           Certificate: 0
           Server Done: 3
   Client Key Exchange: 0
   Server Key Exchange: 0
         Change Cipher: 10
              Finished: 0
    Client Application: 0
    Server Application: 22
                 Alert: 0
  Unrecognized records: 17
  Completed handshakes: 0
        Bad handshakes: 0
      Sessions ignored: 11
    Detection disabled: 1
===============================================================================
SIP Preprocessor Statistics
  Total sessions: 0
===============================================================================
IMAP Preprocessor Statistics
  Total sessions                                    : 0
  Max concurrent sessions                           : 0
===============================================================================
POP Preprocessor Statistics
  Total sessions                                    : 0
  Max concurrent sessions                           : 0
===============================================================================
Reputation Preprocessor Statistics
  Total Memory Allocated: 328320
===============================================================================

Memory Statistics of DNS at: Sun Mar 16 13:20:33 2025


Heap Statistics of dns:
          Total Statistics:
               Memory in use:             0 bytes
                No of allocs:             1
                 No of frees:             1
         Config Statistics:
               Memory in use:             0 bytes
                No of allocs:             1
                 No of frees:             1
===============================================================================
```



```
Memory Statistics of Frag3 on: Sun Mar 16 13:20:33 2025

    Memory in use          : 0
    prealloc nodes in use  : 0


Heap Statistics of frag:
          Total Statistics:
               Memory in use:             0 bytes
                No of allocs:             1
                 No of frees:             1
         Config Statistics:
               Memory in use:             0 bytes
                No of allocs:             1
                 No of frees:             1
===============================================================================

Memory Statistics of FTPTelnet at: Sun Mar 16 13:20:33 2025

       Current active FTP sessions :     0
       Max concurrent FTP sessions :     0
           Total FTP Data sessions :     0
  Max concurrent FTP Data sessions :     0
    Current active Telnet sessions :     0
    Max concurrent Telnet sessions :     0

Heap Statistics of ftptelnet:
          Total Statistics:
               Memory in use:             0 bytes
                No of allocs:           422
                 No of frees:           422
         Config Statistics:
               Memory in use:             0 bytes
                No of allocs:           422
                 No of frees:           422
===============================================================================
 Memory Statistics of Http Inspect on: Sun Mar 16 13:20:33 2025

     Current active session          : 0
    No of POST methods encountered  : 0
    No of GET methods encountered   : 0
    No of successfully extract post params      : 0
    No of successfully extract request params   : 0
    No of successfully extract response params  : 0
 Http Memory Pool       :
      Free Memory:                  0 bytes
      Used Memory:                  0 bytes
      Max Memory :                  0 bytes
 Mime Decode Memory Pool    :
      Free Memory:                  0 bytes
      Used Memory:                  0 bytes
      Max Memory :                  0 bytes
 Http gzip Memory Pool     :
      Free Memory:                  0 bytes
      Used Memory:                  0 bytes
      Max Memory :                  0 bytes
 Http Mime log Memory Pool :
      Free Memory:                  0 bytes
      Used Memory:                  0 bytes
      Max Memory :                  0 bytes
```

Practical 6: Demonstrate Snort



```
  Total memory used :          4449

Heap Statistics of pop:
          Total Statistics:
               Memory in use:          4449 bytes
                No of allocs:             3
                 No of frees:            18
         Config Statistics:
               Memory in use:          4449 bytes
                No of allocs:             3
                 No of frees:            18
================================================================================
IMAP Preprocessor Statistics
  Total sessions                   : 0
  Max concurrent sessions          : 0
  Current sessions                 : 0
  IMAP Session
     Used Memory  :           0
     No of Allocs :           0
     No of Frees  :           0
  IMAP Config
     Used Memory  :        1379
     No of Allocs :           3
     No of Frees  :          48
   Total memory used :          1379

Heap Statistics of imap:
          Total Statistics:
               Memory in use:          1379 bytes
                No of allocs:             3
                 No of frees:            48
         Config Statistics:
               Memory in use:          1379 bytes
                No of allocs:             3
                 No of frees:            48
================================================================================

Memory Statistics for File at:Sun Mar 16 13:20:33 2025

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:           288 bytes
                No of allocs:             6
                 No of frees:             1
        Session Statistics:
               Memory in use:             0 bytes
                No of allocs:             1
                 No of frees:             1
        Mempool Statistics:
               Memory in use:           288 bytes
                No of allocs:             5
                 No of frees:             0
================================================================================
Snort exiting
```