20BDS0146

VENNELA G

School of Computer Science and Engineering
CSE3502-ISM LAB EXERCISES

Slot L37 + L38

Ex No: 5A Malware Analysis

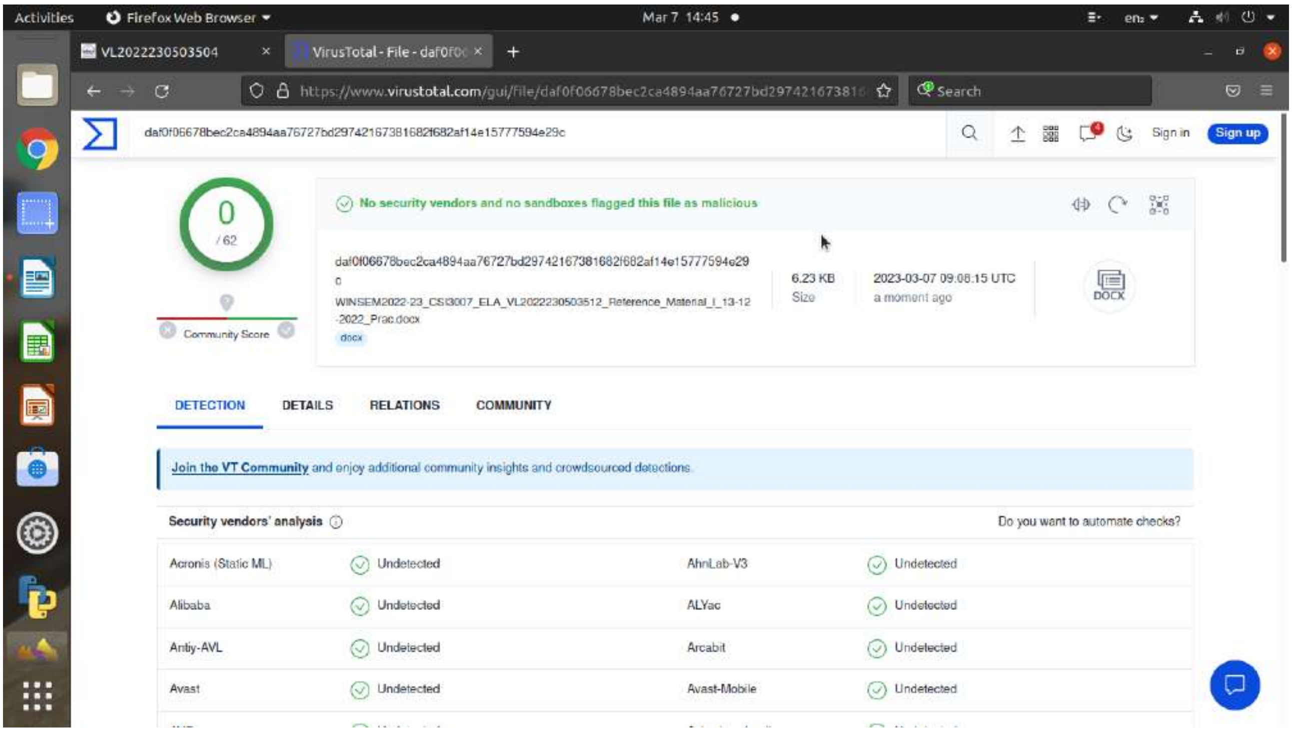
Utilize the below given web links and perform the malware analysis

Malware Analysis tools

- https://www.virustotal.com/gui/home/upload
- https://www.hybrid-analysis.com

Malware Database

https://bazaar.abuse.ch/browse/


Activities
Firefox Web Browser
Mar 7 14:45
VL2022230503504
VirusTotal - File - daf0f0
https://www.virustotal.com/gui/file/daf0f06678bec2ca4894aa76727bd29742167381
Search
Sign in
Sign up

daf0f06678bec2ca4894aa76727bd29742167381682f682af14e15777594e29c

0 / 62

Community Score

No security vendors and no sandboxes flagged this file as malicious

daf0f06678bec2ca4894aa76727bd29742167381682f682af14e15777594e29c

WINSEM2022-23_CSI3007_ELA_VL2022230503512_Reference_Material_I_13-12-2022_Prac.docx

docx

6.23 KB
Size

2023-03-07 09:08:15 UTC
a moment ago

DOCX

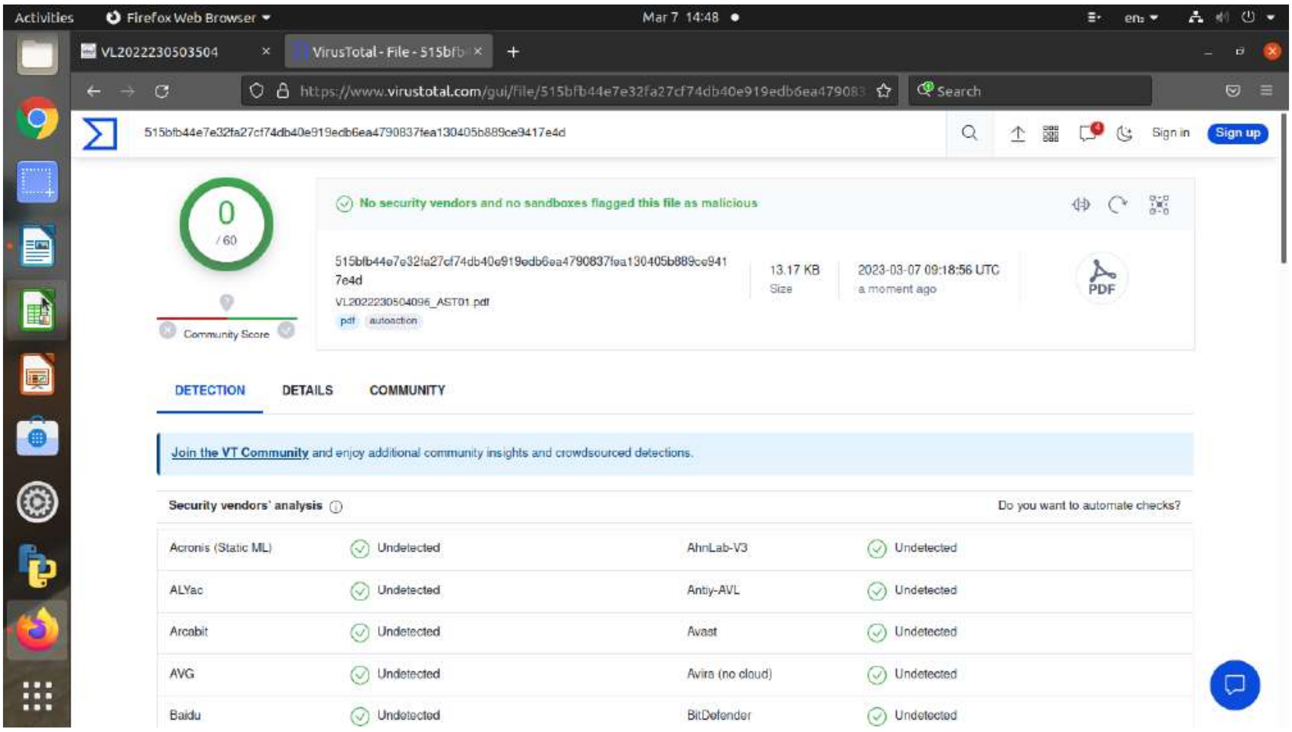
DETECTION DETAILS RELATIONS COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections.

Security vendors' analysis ⓘ

Do you want to automate checks?

Acronis (Static ML)	✓ Undetected	AhnLab-V3	✓ Undetected
Alibaba	✓ Undetected	ALYac	✓ Undetected
Antiy-AVL	✓ Undetected	Arcabit	✓ Undetected
Avast	✓ Undetected	Avast-Mobile	✓ Undetected


Activities
Firefox Web Browser
Mar 7 14:48
VL2022230503504
VirusTotal - File - 515bfb
https://www.virustotal.com/gui/file/515bfb44e7e32fa27cf74db40e919edb6ea47908
Search
Sign in
Sign up

515bfb44e7e32fa27cf74db40e919edb6ea4790837fea130405b889ce9417e4d

0 / 60

Community Score

No security vendors and no sandboxes flagged this file as malicious

515bfb44e7e32fa27cf74db40e919edb6ea4790837fea130405b889ce9417e4d

VL2022230504096_AST01.pdf

pdf autoaction

13.17 KB
Size

2023-03-07 09:18:56 UTC
a moment ago

PDF

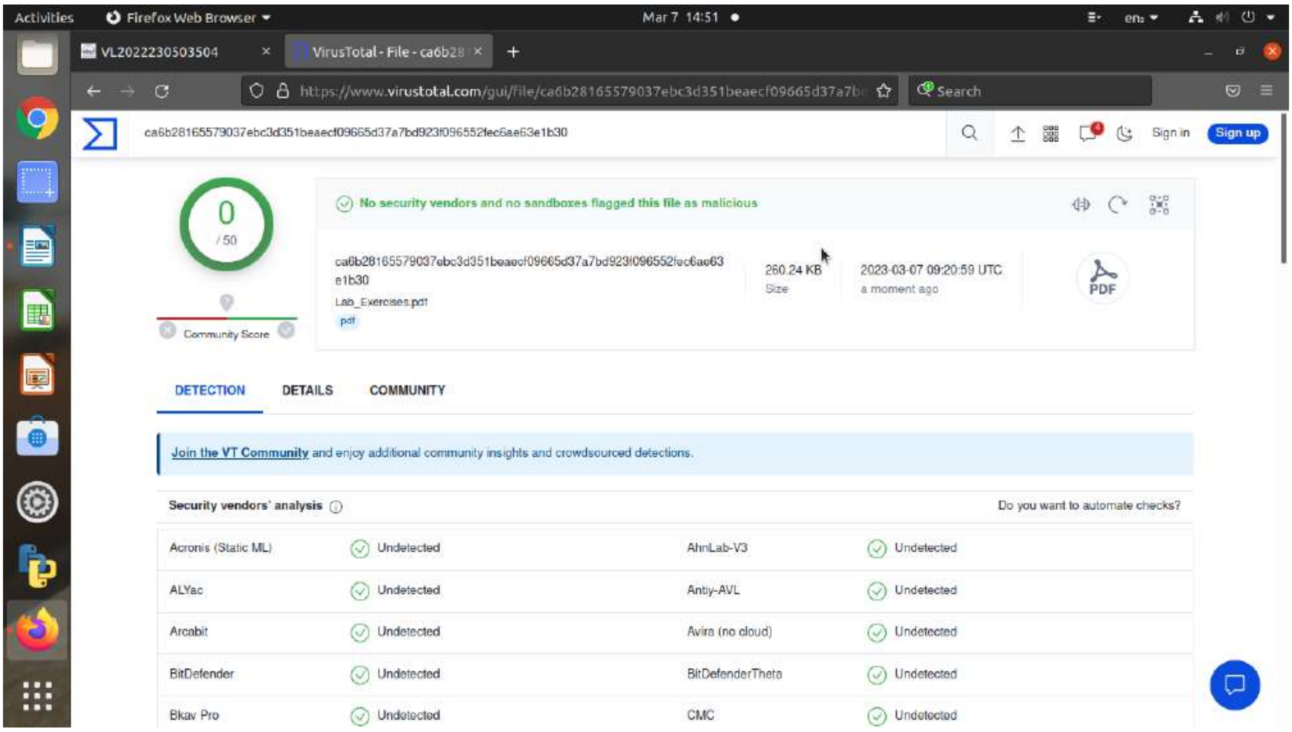
DETECTION DETAILS COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections.

Security vendors' analysis ⓘ

Do you want to automate checks?

Acronis (Static ML)	✓ Undetected	AhnLab-V3	✓ Undetected
ALYac	✓ Undetected	Antiy-AVL	✓ Undetected
Arcabit	✓ Undetected	Avast	✓ Undetected
AVG	✓ Undetected	Avira (no cloud)	✓ Undetected
Baidu	✓ Undetected	BitDefender	✓ Undetected


Activities
Firefox Web Browser
Mar 7 14:51
VL2022230503504
VirusTotal - File - ca6b28
https://www.virustotal.com/gui/file/ca6b28165579037ebc3d351beaecf09665d37a7b
Search
Sign in
Sign up

ca6b28165579037ebc3d351beaecf09665d37a7bd923f096552fec6ae63e1b30

0 / 50

Community Score

No security vendors and no sandboxes flagged this file as malicious

ca6b28165579037ebc3d351beaecf09665d37a7bd923f096552fec6ae63e1b30

Lab_Exercises.pdf

pdf

260.24 KB
Size

2023-03-07 09:20:59 UTC
a moment ago

PDF

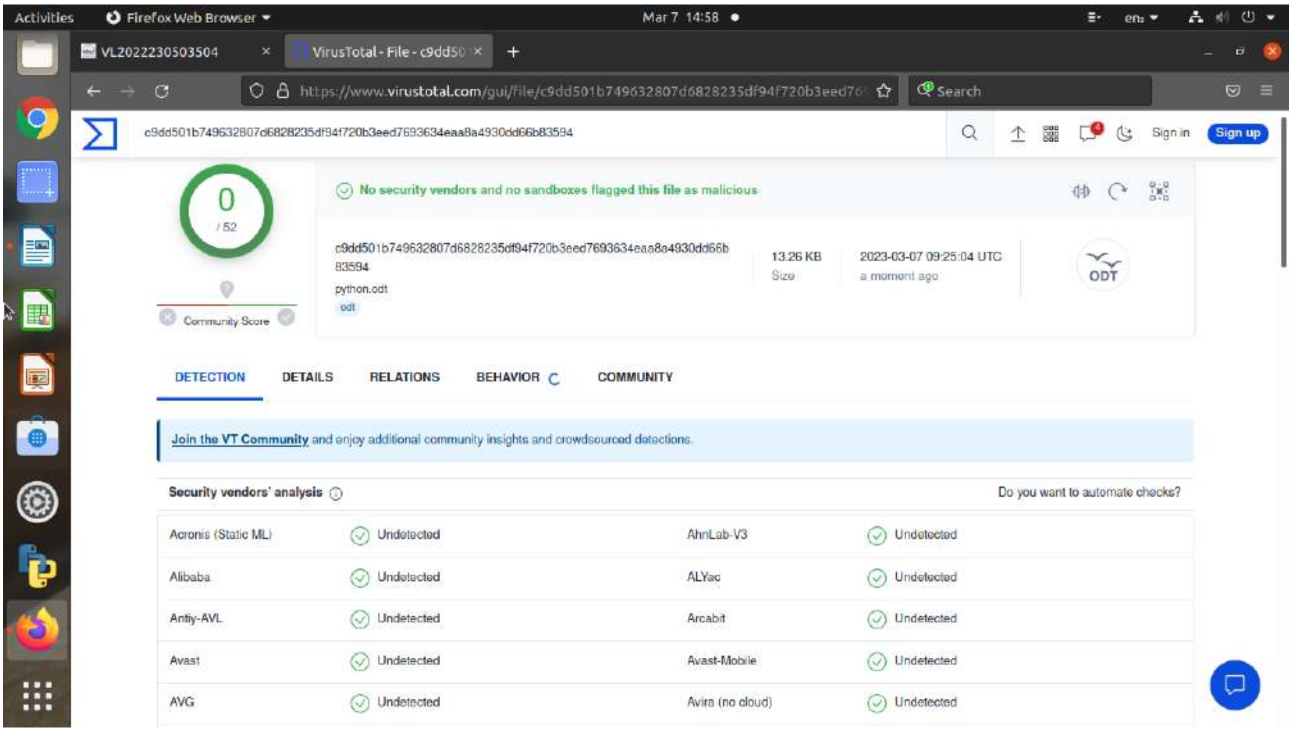
DETECTION DETAILS COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections.

Security vendors' analysis ⓘ

Do you want to automate checks?

Acronis (Static ML)	✓ Undetected	AhnLab-V3	✓ Undetected
ALYac	✓ Undetected	Antiy-AVL	✓ Undetected
Arcabit	✓ Undetected	Avira (no cloud)	✓ Undetected
BitDefender	✓ Undetected	BitDefenderTheta	✓ Undetected
Bkav Pro	✓ Undetected	CMC	✓ Undetected


Activities
Firefox Web Browser
Mar 7 14:58
VL2022230503504
VirusTotal - File - c9dd50
https://www.virustotal.com/gui/file/c9dd501b749632807d6828235df94f720b3eed76
Search
Sign in
Sign up

c9dd501b749632807d6828235df94f720b3eed7693634eaa8a4930dd66b83594

0 / 52

Community Score

No security vendors and no sandboxes flagged this file as malicious

c9dd501b749632807d6828235df94f720b3eed7693634eaa8a4930dd66b83594

python.odt

odt

13.26 KB
Size

2023-03-07 09:25:04 UTC
a moment ago

ODT

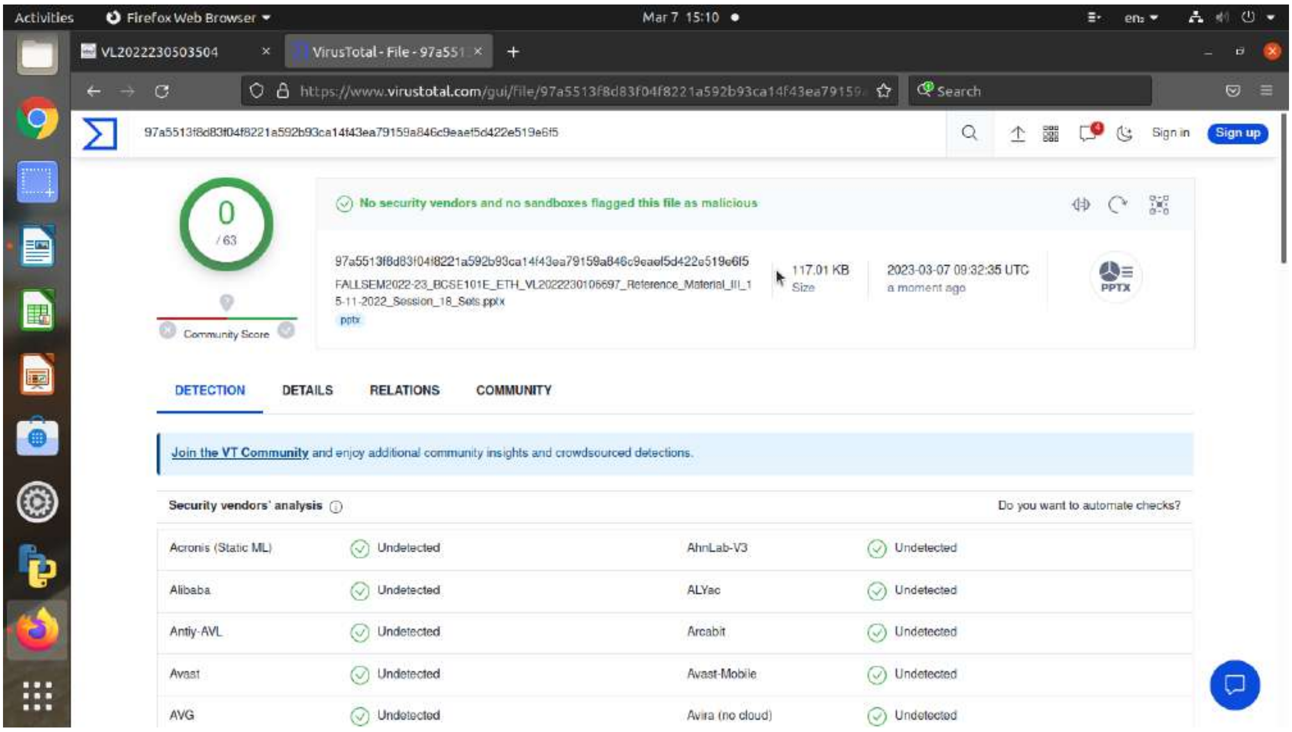
DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections.

Security vendors' analysis ⓘ

Do you want to automate checks?

Acronis (Static ML)	✓ Undetected	AhnLab-V3	✓ Undetected
Alibaba	✓ Undetected	ALYac	✓ Undetected
Antiy-AVL	✓ Undetected	Arcabit	✓ Undetected
Avast	✓ Undetected	Avast-Mobile	✓ Undetected
AVG	✓ Undetected	Avira (no cloud)	✓ Undetected



Activities
Firefox Web Browser
Mar 7 15:10
VL2022230503504
VirusTotal - File - 97a551
https://www.virustotal.com/gui/file/97a5513f8d83f04f8221a592b93ca14f43ea79159
Search
Sign in
Sign up

97a5513f8d83f04f8221a592b93ca14f43ea79159a846c9eaef5d422e519e6f5

0 / 63

Community Score

No security vendors and no sandboxes flagged this file as malicious

97a5513f8d83f04f8221a592b93ca14f43ea79159a846c9eaef5d422e519e6f5
FALLSEM2022-23_BCSE101E_ETH_VL2022230106697_Reference_Material_III_15-11-2022_Session_18_Sets.pptx
pptx

117.01 KB
Size

2023-03-07 09:32:35 UTC
a moment ago

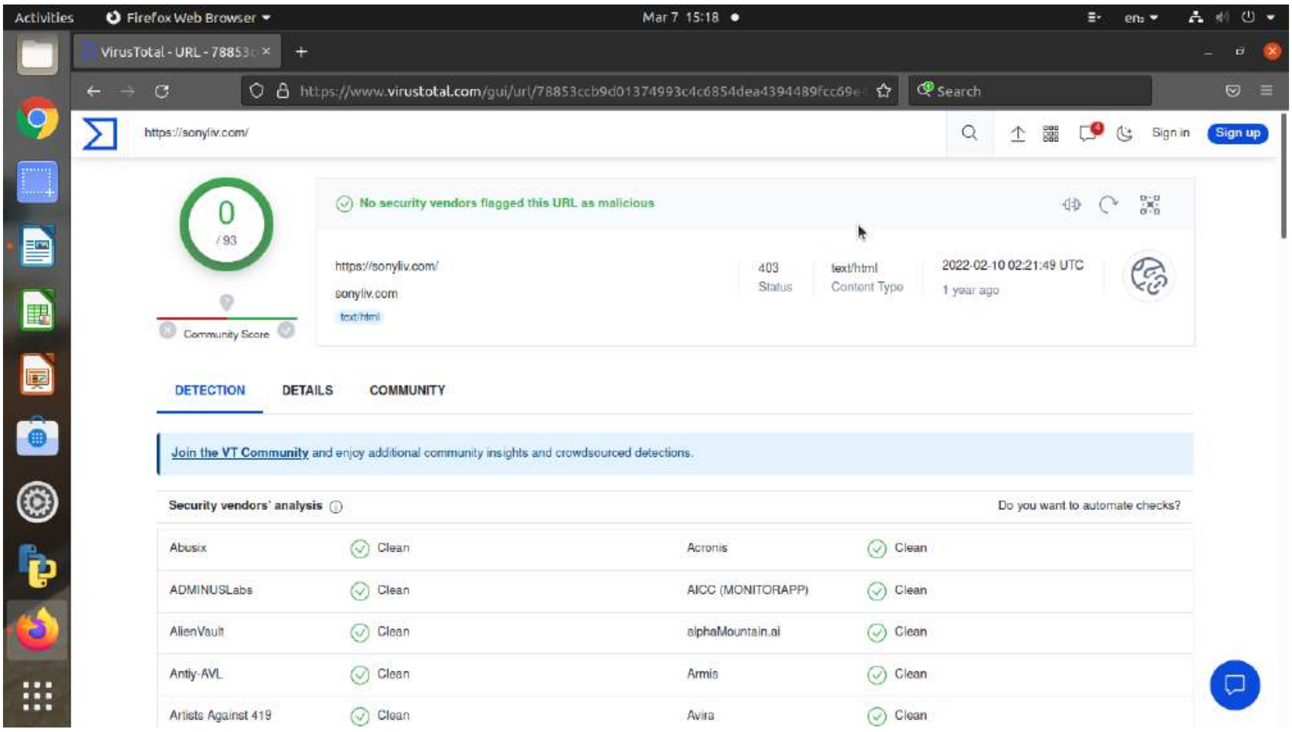
PPTX

DETECTION DETAILS RELATIONS COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections.

Security vendors' analysis ⓘ — Do you want to automate checks?

Acronis (Static ML)	✓ Undetected	AhnLab-V3	✓ Undetected
Alibaba	✓ Undetected	ALYac	✓ Undetected
Antiy-AVL	✓ Undetected	Arcabit	✓ Undetected
Avast	✓ Undetected	Avast-Mobile	✓ Undetected
AVG	✓ Undetected	Avira (no cloud)	✓ Undetected



https://sonyliv.com/

0 / 93

Community Score

No security vendors flagged this URL as malicious

https://sonyliv.com/
sonyliv.com
text/html

403
Status

text/html
Content Type

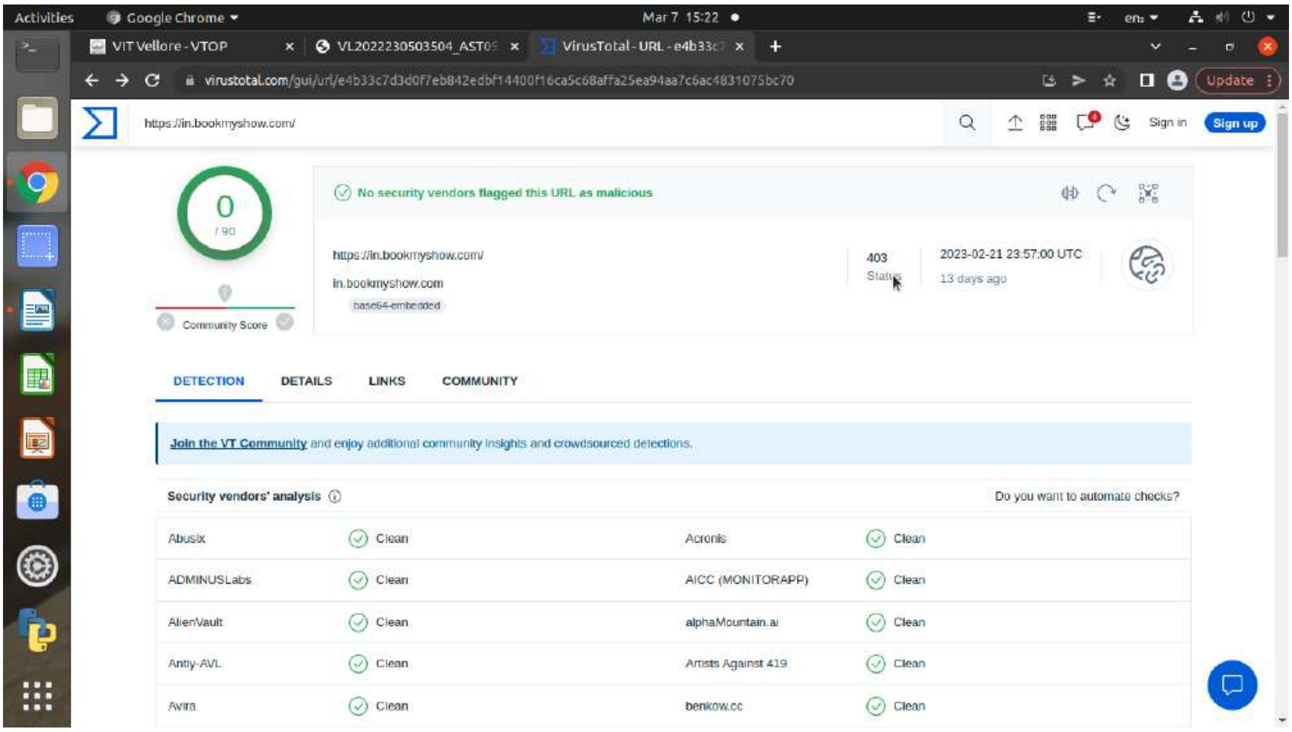
2022-02-10 02:21:49 UTC
1 year ago

DETECTION DETAILS COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections.

Security vendors' analysis ⓘ — Do you want to automate checks?

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AICC (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	alphaMountain.ai	✓ Clean
Antiy-AVL	✓ Clean	Armis	✓ Clean
Artists Against 419	✓ Clean	Avira	✓ Clean



virustotal.com/gui/url/e4b33c7d3d0f7eb842edbf14400f16ca5c68affa25ea94aa7c6ac4831075bc70

https://in.bookmyshow.com/

0
/ 90

Community Score

No security vendors flagged this URL as malicious

https://in.bookmyshow.com/
in.bookmyshow.com
base64-embedded

403
Status

2023-02-21 23:57:00 UTC
13 days ago

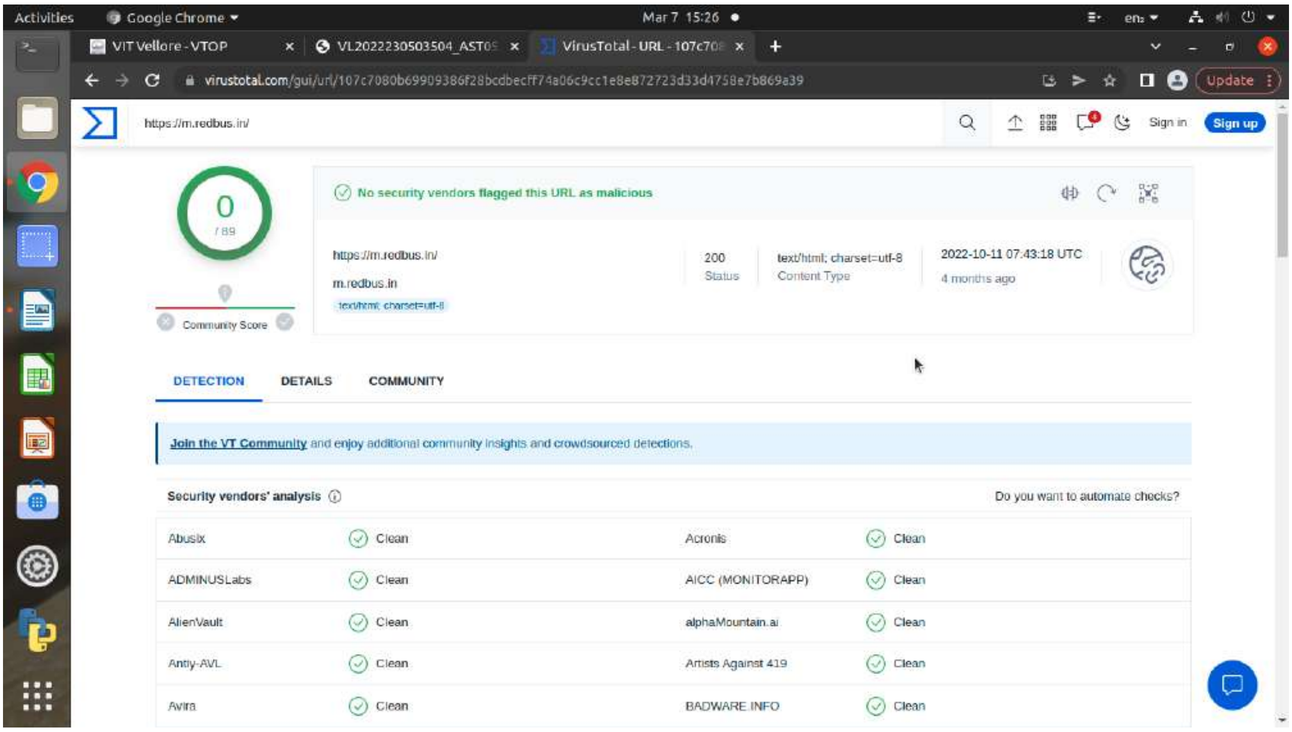
DETECTION DETAILS LINKS COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections.

Security vendors' analysis

Do you want to automate checks?

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AICC (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	alphaMountain.ai	✓ Clean
Antiy-AVL	✓ Clean	Artists Against 419	✓ Clean
Avira	✓ Clean	benkow.cc	✓ Clean



virustotal.com/gui/url/107c7080b69909386f28bcdbecff74a06c9cc1e8e872723d33d4758e7b869a39

https://m.redbus.in/

0
/ 89

Community Score

No security vendors flagged this URL as malicious

https://m.redbus.in/
m.redbus.in
text/html; charset=utf-8

200
Status

text/html; charset=utf-8
Content Type

2022-10-11 07:43:18 UTC
4 months ago

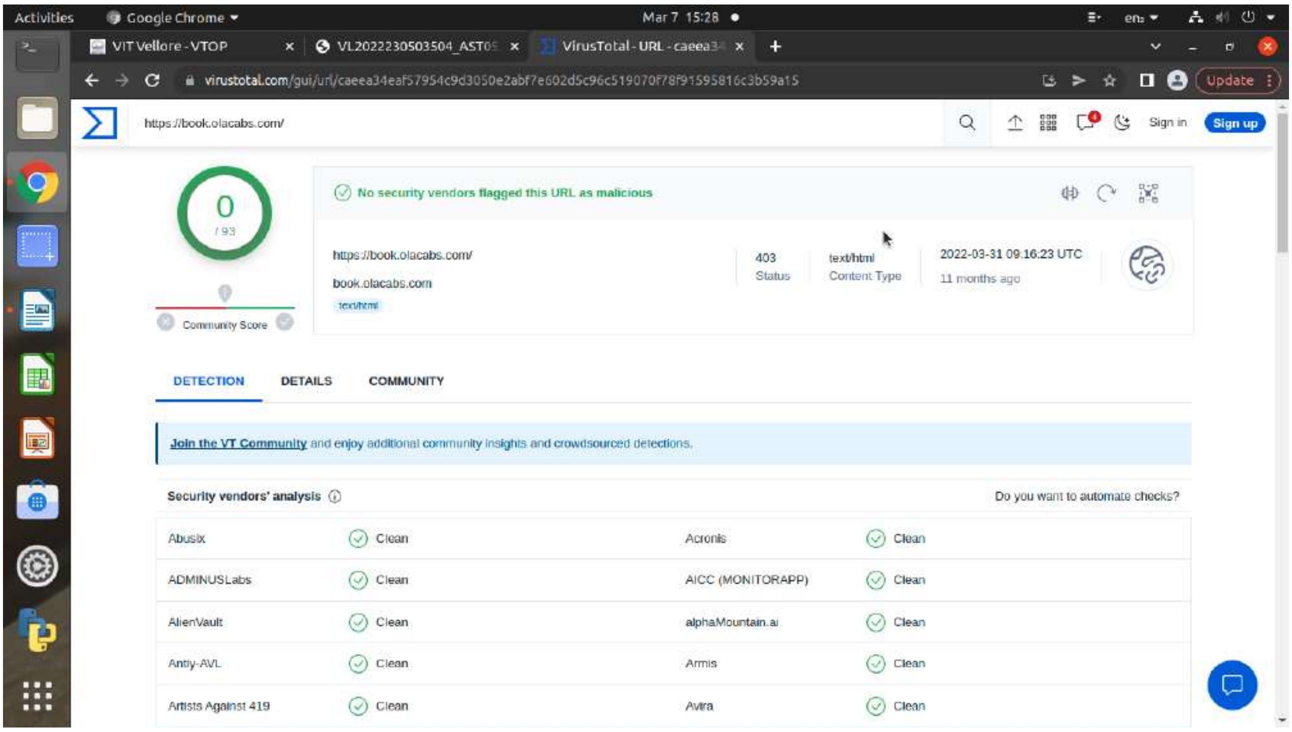
DETECTION DETAILS COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections.

Security vendors' analysis

Do you want to automate checks?

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AICC (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	alphaMountain.ai	✓ Clean
Antiy-AVL	✓ Clean	Artists Against 419	✓ Clean
Avira	✓ Clean	BADWARE.INFO	✓ Clean



virustotal.com/gui/url/caeea34eaf57954c9d3050e2abf7e602d5c96c519070f78f91595816c3b59a15

https://book.olacabs.com/

0 / 93

Community Score

No security vendors flagged this URL as malicious

https://book.olacabs.com/
book.olacabs.com
text/html

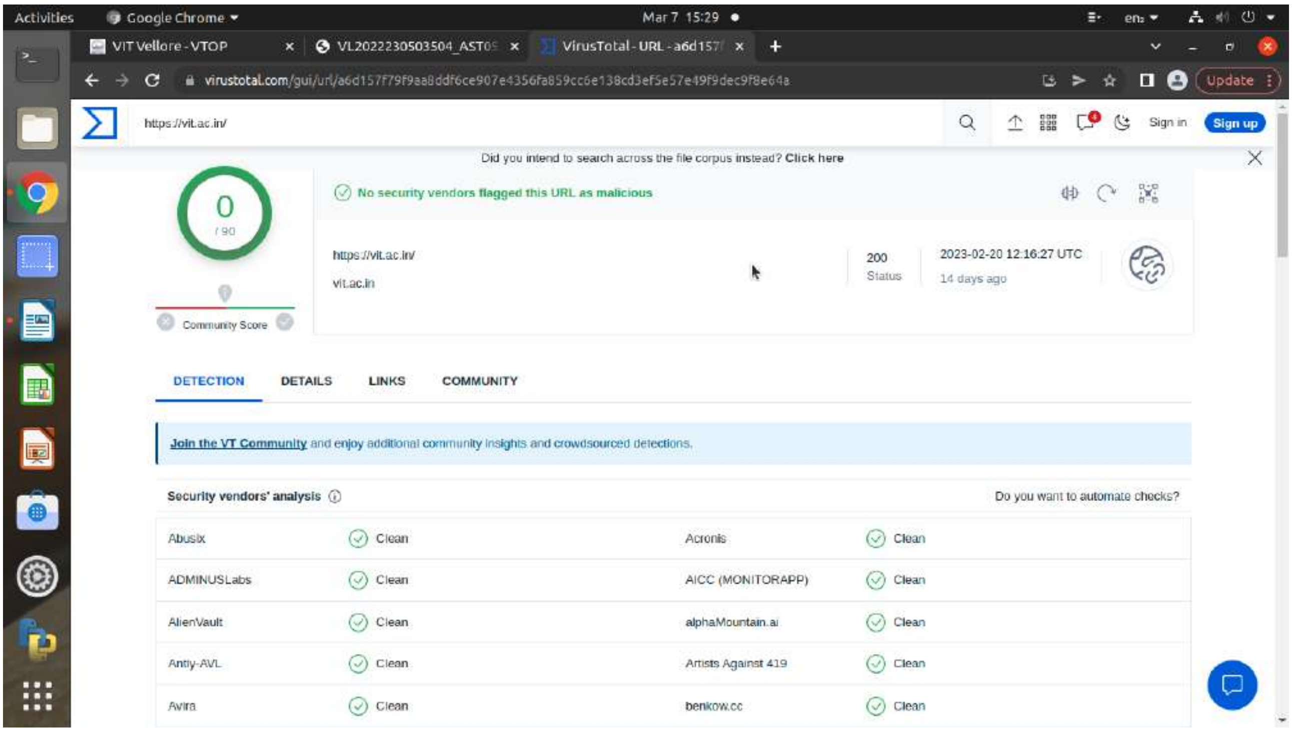
403 Status | text/html Content Type | 2022-03-31 09:16:23 UTC 11 months ago

DETECTION DETAILS COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections.

Security vendors' analysis | Do you want to automate checks?

Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AICC (MONITORAPP)	Clean
AlienVault	Clean	alphaMountain.ai	Clean
Antiy-AVL	Clean	Armis	Clean
Artists Against 419	Clean	Avira	Clean



virustotal.com/gui/url/a6d157f79f9aa8ddf6ce907e4356fa859cc6e138cd3ef5e57e49f9dec9f8e64a

https://vit.ac.in/

Did you intend to search across the file corpus instead? **Click here**

0 / 90

Community Score

No security vendors flagged this URL as malicious

https://vit.ac.in/
vit.ac.in

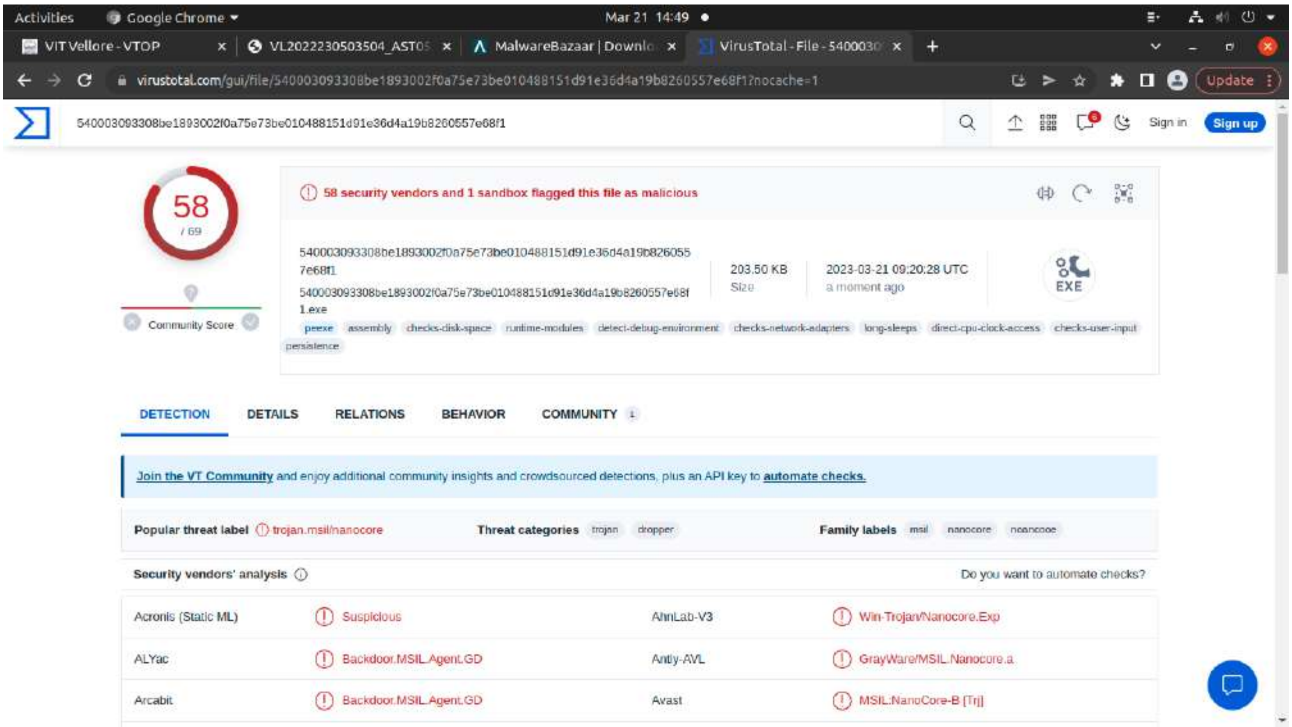
200 Status | 2023-02-20 12:16:27 UTC 14 days ago

DETECTION DETAILS LINKS COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections.

Security vendors' analysis | Do you want to automate checks?

Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AICC (MONITORAPP)	Clean
AlienVault	Clean	alphaMountain.ai	Clean
Antiy-AVL	Clean	Artists Against 419	Clean
Avira	Clean	benkow.cc	Clean



540003093308be1893002f0a75e73be010488151d91e36d4a19b8260557e68f1

58 security vendors and 1 sandbox flagged this file as malicious

540003093308be1893002f0a75e73be010488151d91e36d4a19b8260557e68f1

540003093308be1893002f0a75e73be010488151d91e36d4a19b8260557e68f1.exe

peexe assembly checks-disk-space runtime-modules detect-debug-environment checks-network-adapters long-sleeps direct-cpu-clock-access checks-user-input persistence

203.50 KB
Size

2023-03-21 09:20:28 UTC
a moment ago

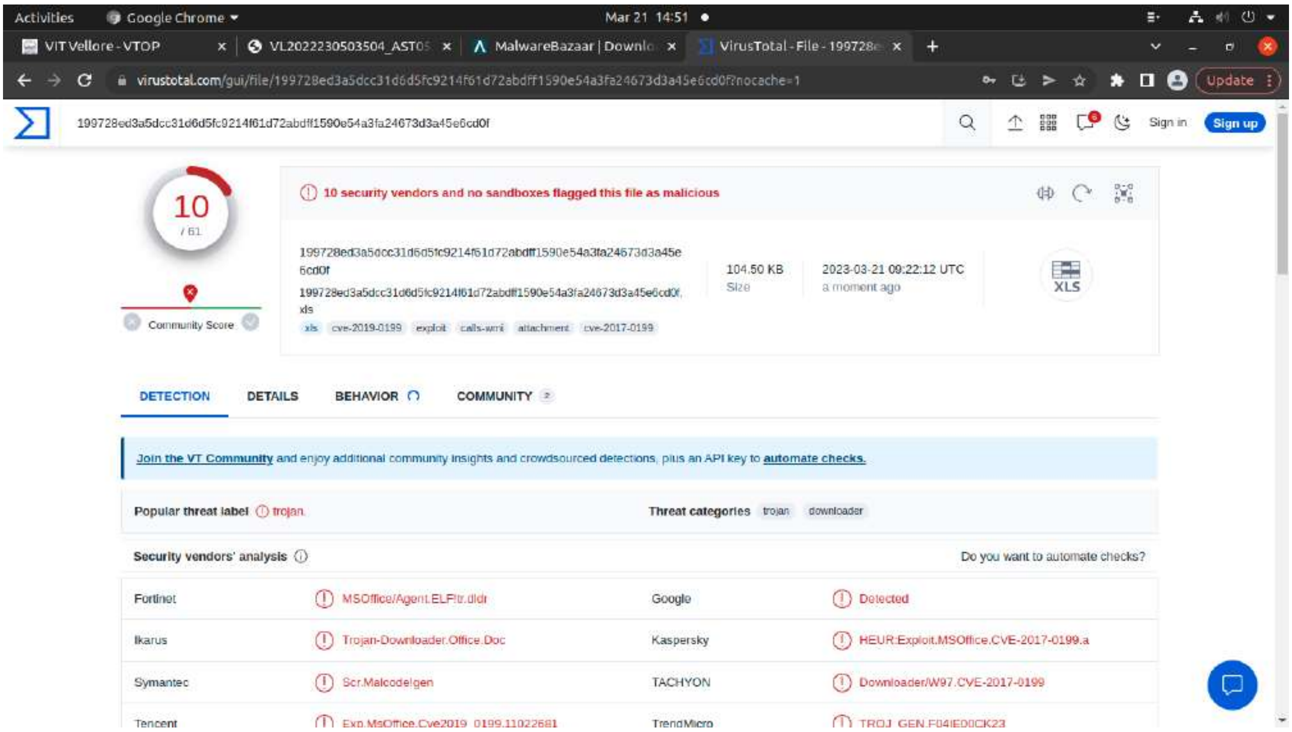
DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 1

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.msil/nanocore **Threat categories** trojan dropper **Family labels** msil nanocore noancooe

Security vendors' analysis Do you want to automate checks?

Acronis (Static ML)	Suspicious	AhnLab-V3	Win-Trojan/Nanocore.Exp
ALYac	Backdoor.MSIL.Agent.GD	Antiy-AVL	GrayWare/MSIL.Nanocore.a
Arcabit	Backdoor.MSIL.Agent.GD	Avast	MSIL:NanoCore-B [Trj]



199728ed3a5dcc31d6d5fc9214f61d72abdff1590e54a3fa24673d3a45e6cd0f

10 security vendors and no sandboxes flagged this file as malicious

199728ed3a5dcc31d6d5fc9214f61d72abdff1590e54a3fa24673d3a45e6cd0f

199728ed3a5dcc31d6d5fc9214f61d72abdff1590e54a3fa24673d3a45e6cd0f.xls

xls cve-2019-0199 exploit calls-wmi attachment cve-2017-0199

104.50 KB
Size

2023-03-21 09:22:12 UTC
a moment ago

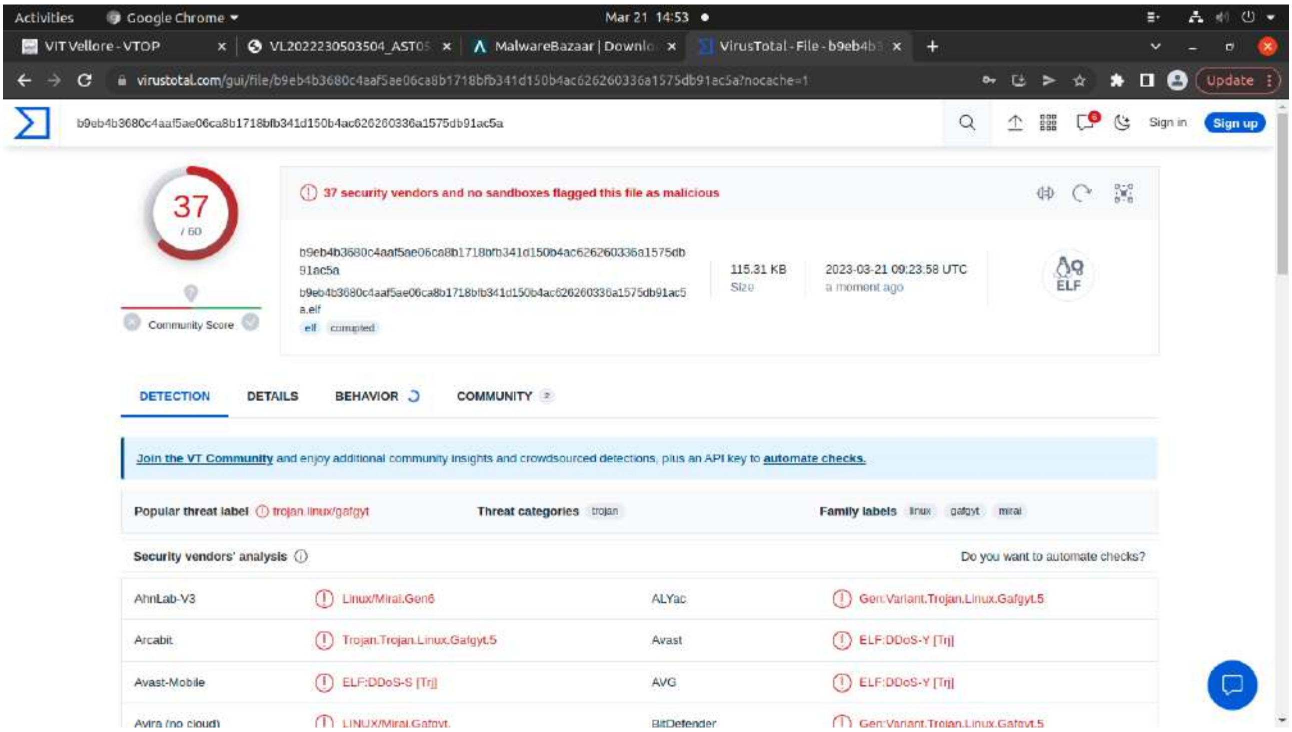
DETECTION DETAILS BEHAVIOR COMMUNITY 2

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan. **Threat categories** trojan downloader

Security vendors' analysis Do you want to automate checks?

Fortinet	MSOffice/Agent.ELFltr.dldr	Google	Detected
Ikarus	Trojan-Downloader.Office.Doc	Kaspersky	HEUR:Exploit.MSOffice.CVE-2017-0199.a
Symantec	Scr.Malcodelgen	TACHYON	Downloader/W97.CVE-2017-0199
Tencent	Exp.MsOffice.Cve2019_0199.11022681	TrendMicro	TROJ_GEN.F04IE00CK23



b9eb4b3680c4aaf5ae06ca8b1718bfb341d150b4ac626260336a1575db91ac5a

37 security vendors and no sandboxes flagged this file as malicious

b9eb4b3680c4aaf5ae06ca8b1718bfb341d150b4ac626260336a1575db91ac5a

b9eb4b3680c4aaf5ae06ca8b1718bfb341d150b4ac626260336a1575db91ac5a.elf

elf corrupted

115.31 KB
Size

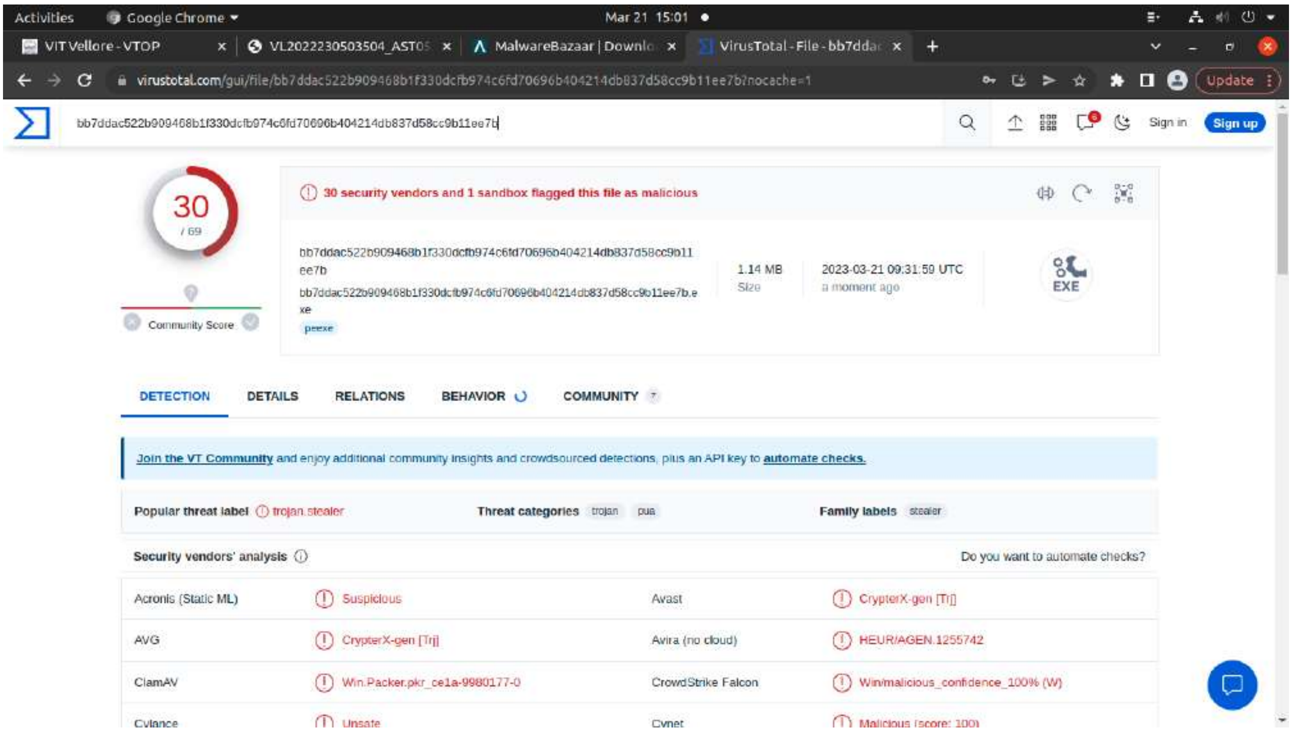
2023-03-21 09:23:58 UTC
a moment ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.linux/gafgyt Threat categories trojan Family labels linux gafgyt mirai

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Linux/Mirai.Gen6	ALYac	Gen:Variant.Trojan.Linux.Gafgyt.5
Arcabit	Trojan.Trojan.Linux.Gafgyt.5	Avast	ELF:DDoS-Y [Trj]
Avast-Mobile	ELF:DDoS-S [Trj]	AVG	ELF:DDoS-Y [Trj]
Avira (no cloud)	LINUX/Mirai.Gafgyt.	BitDefender	Gen:Variant.Trojan.Linux.Gafgyt.5



bb7ddac522b909468b1f330dcfb974c6fd70696b404214db837d58cc9b11ee7b

30 security vendors and 1 sandbox flagged this file as malicious

bb7ddac522b909468b1f330dcfb974c6fd70696b404214db837d58cc9b11ee7b

bb7ddac522b909468b1f330dcfb974c6fd70696b404214db837d58cc9b11ee7b.exe

peexe

1.14 MB
Size

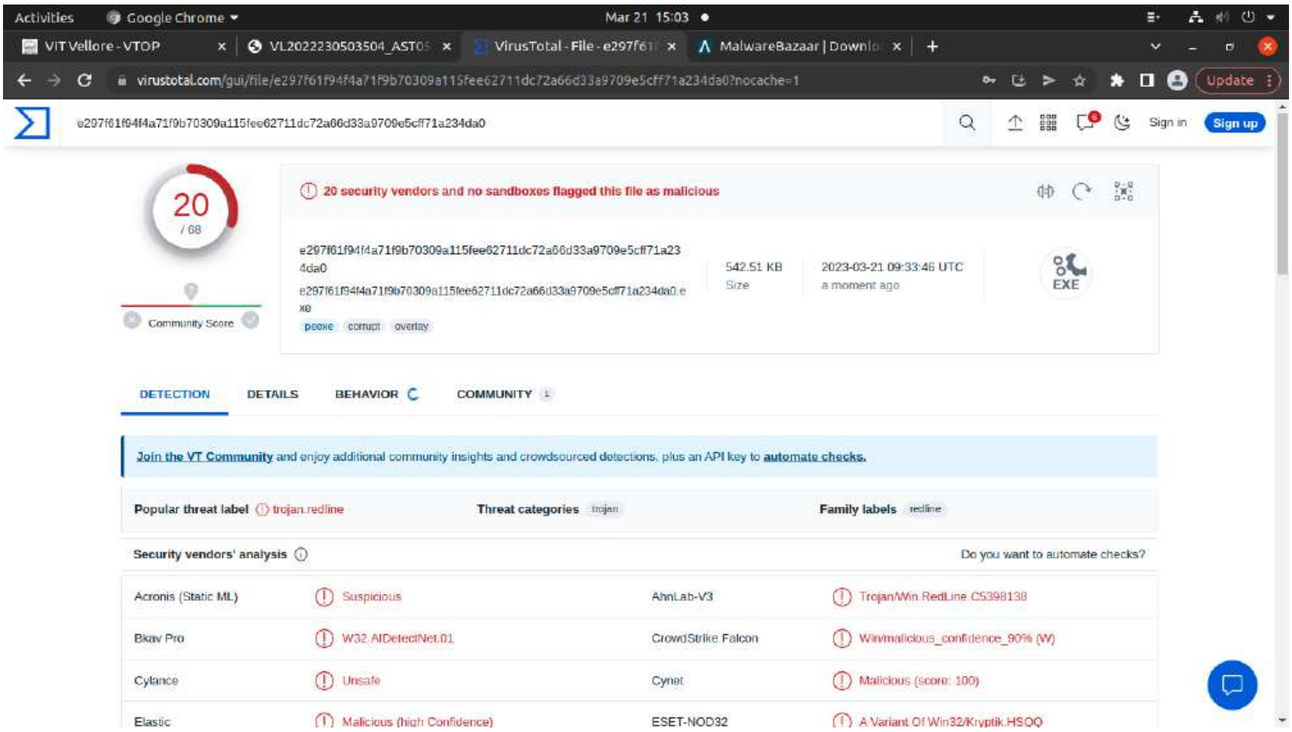
2023-03-21 09:31:59 UTC
a moment ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.stealer Threat categories trojan pua Family labels stealer

Security vendors' analysis Do you want to automate checks?

Acronis (Static ML)	Suspicious	Avast	CrypterX-gen [Trj]
AVG	CrypterX-gen [Trj]	Avira (no cloud)	HEUR/AGEN.1255742
ClamAV	Win.Packer.pkr_ce1a-9980177-0	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cynet	Malicious (score: 100)


Activities
Google Chrome
Mar 21 15:03
VIT Vellore - VTOP
VL2022230503504_AST05
VirusTotal - File - e297f61
MalwareBazaar | Downlo
virustotal.com/gui/file/e297f61f94f4a71f9b70309a115fee62711dc72a66d33a9709e5cff71a234da0?nocache=1
Update
Sign in
Sign up
EXE

e297f61f94f4a71f9b70309a115fee62711dc72a66d33a9709e5cff71a234da0

20 / 68

Community Score

20 security vendors and no sandboxes flagged this file as malicious

e297f61f94f4a71f9b70309a115fee62711dc72a66d33a9709e5cff71a234da0

e297f61f94f4a71f9b70309a115fee62711dc72a66d33a9709e5cff71a234da0.exe

peexe corrupt overlay

542.51 KB
Size

2023-03-21 09:33:46 UTC
a moment ago

DETECTION DETAILS BEHAVIOR COMMUNITY 1

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.redline Threat categories trojan Family labels redline

Security vendors' analysis Do you want to automate checks?

Acronis (Static ML)	Suspicious	AhnLab-V3	Trojan/Win.RedLine.C5398138
Bkav Pro	W32.AIDetectNet.01	CrowdStrike Falcon	Win/malicious_confidence_90% (W)
Cylance	Unsafe	Cynet	Malicious (score: 100)
Elastic	Malicious (high Confidence)	ESET-NOD32	A Variant Of Win32/Kryptik.HSQQ

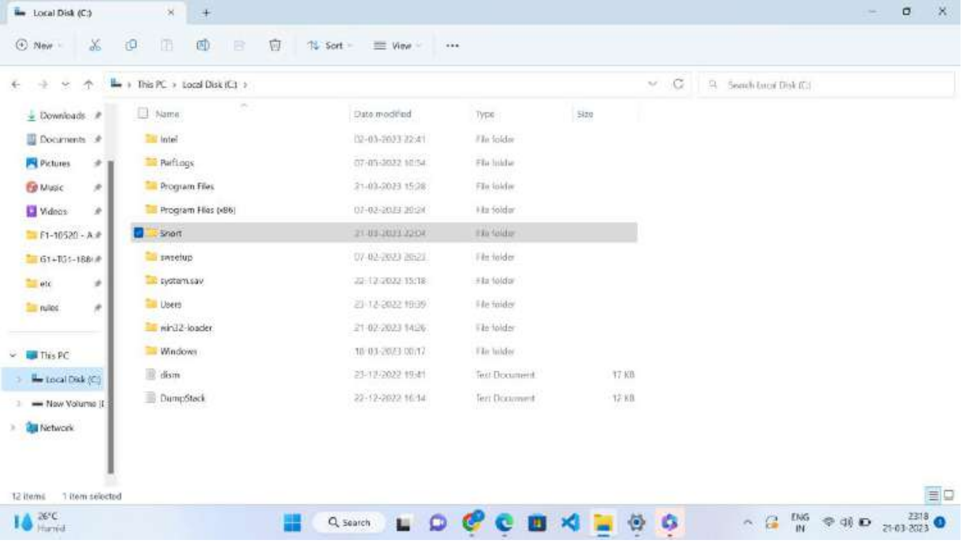
Ex. 5B: Installing and Configuring SNORT Intrusion Detection System

Download the latest version of snort and configure it as per the steps given below:

1. Download SNORT from https://www.snort.org/downloads

2. Install npcap in your system from (https://npcap.com/#:~:text=Downloading%20and%20Installing%20Npcap%20Free%20Edition&text=Simply%20run%20the%20executable%20installer,documented%20in%20the%20Npcap%20Changelog).

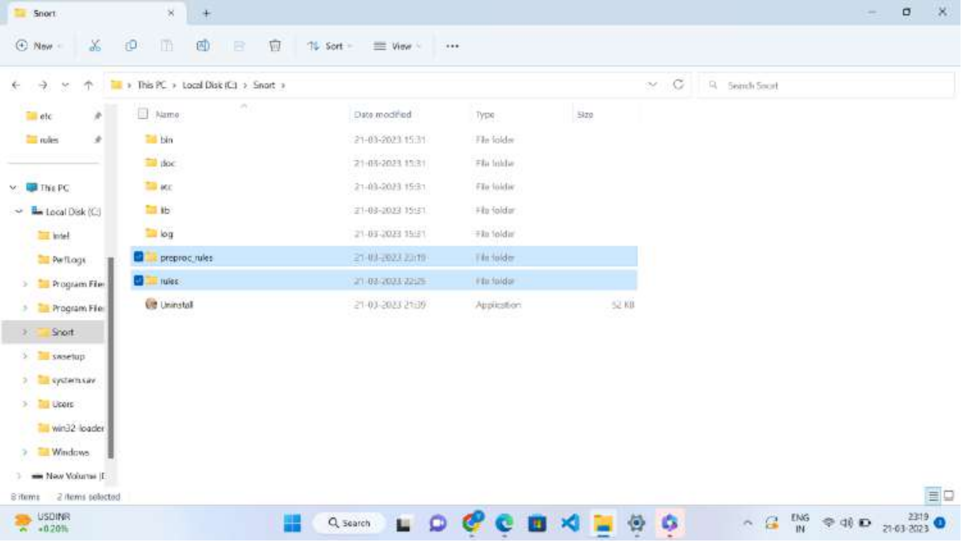
4. Download the SNORT rules w.r.to SNORT version downloaded from the above website



Name	Date modified	Type	Size
Intel	02-03-2023 22:41	File folder	
PerfLogs	07-05-2022 10:54	File folder	
Program Files	21-03-2023 15:28	File folder	
Program Files (x86)	07-02-2023 20:24	File folder	
Snort	21-03-2023 22:04	File folder	
swsetup	07-02-2023 20:23	File folder	
system.sav	22-12-2022 15:18	File folder	
Users	23-12-2022 19:39	File folder	
win32-loader	21-02-2023 14:26	File folder	
Windows	18-03-2023 00:17	File folder	
dism	23-12-2022 19:41	Text Document	17 KB
DumpStack	22-12-2022 16:14	Text Document	12 KB

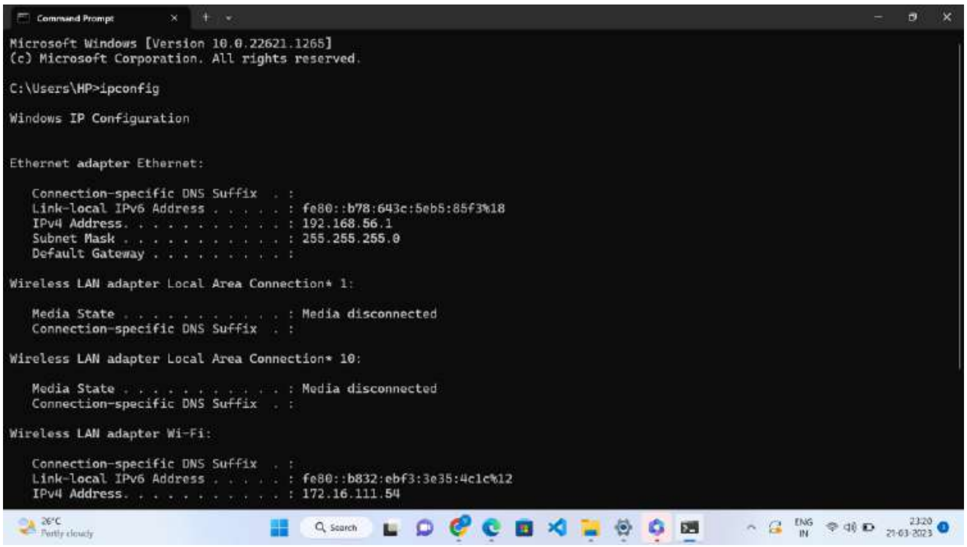
5. Unzip and Replace the rule folder to C:\Snort\rules

6. Replace the rule folder to C:\Snort\preproc_rules



Name	Date modified	Type	Size
bin	21-03-2023 15:31	File folder	
doc	21-03-2023 15:31	File folder	
etc	21-03-2023 15:31	File folder	
lib	21-03-2023 15:31	File folder	
log	21-03-2023 15:31	File folder	
preproc_rules	21-03-2023 23:19	File folder	
rules	21-03-2023 22:25	File folder	
Uninstall	21-03-2023 21:39	Application	52 KB

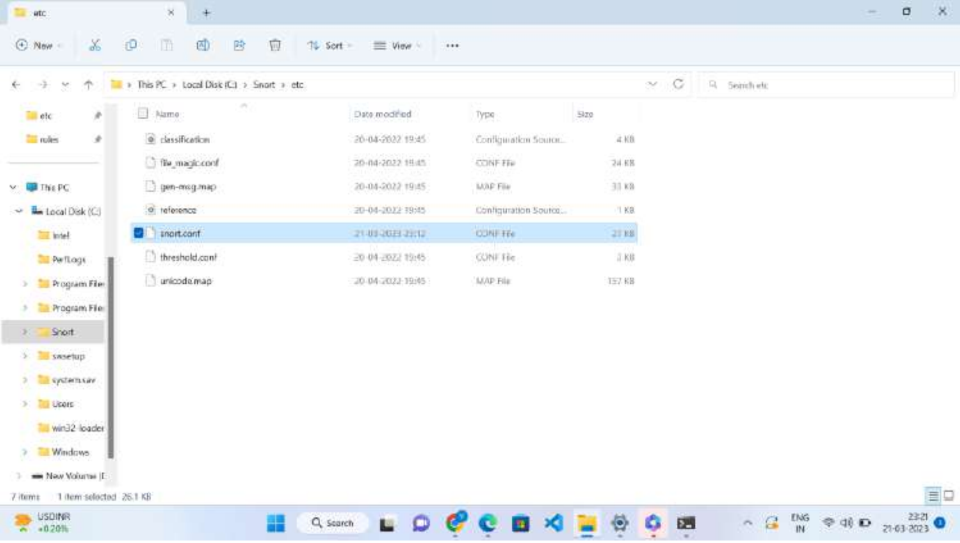
7. Open cmd and ipconfig to find the IP address of the system: 192.168.56.1/24, subnetmask: 255.255.255.0



```
Microsoft Windows [Version 10.0.22621.1265]
(c) Microsoft Corporation. All rights reserved.

C:\Users\HP>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b78:643c:5eb5:85f3%18
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b832:ebf3:3e35:4c1c%12
   IPv4 Address. . . . . . . . . . . : 172.16.111.54
```

8. Go to the SNORT installed folder C:\Snort\etc, open Snort.config using notepad++ or notepad

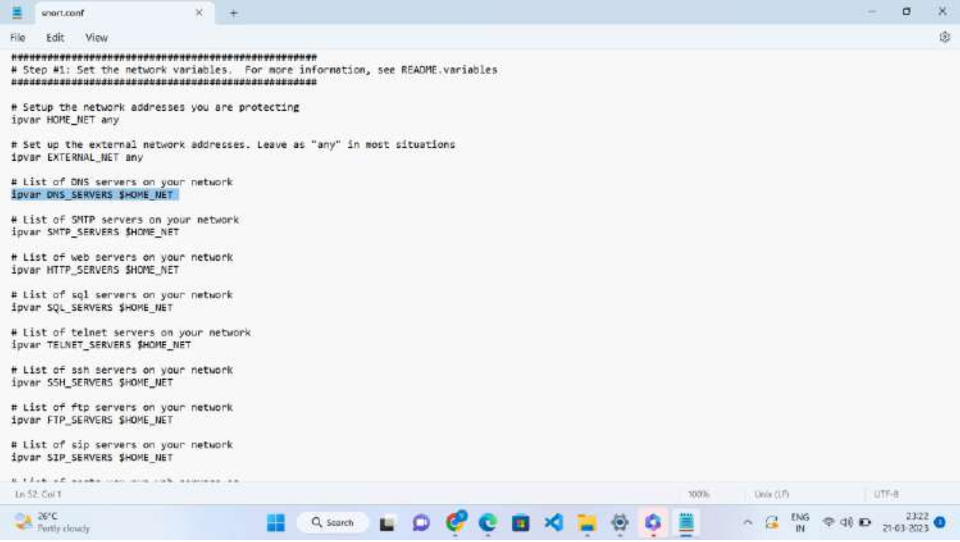
9. After all this do the required changes to configure snort in snort.config folder.



Name	Date modified	Type	Size
classification	20-04-2022 19:45	Configuration Source...	4 KB
file_magic.conf	20-04-2022 19:45	CONF File	24 KB
gen-msg.map	20-04-2022 19:45	MAP File	33 KB
reference	20-04-2022 19:45	Configuration Source...	1 KB
☑ snort.conf	21-03-2023 23:12	CONF File	27 KB
threshold.conf	20-04-2022 19:45	CONF File	3 KB
unicode.map	20-04-2022 19:45	MAP File	157 KB

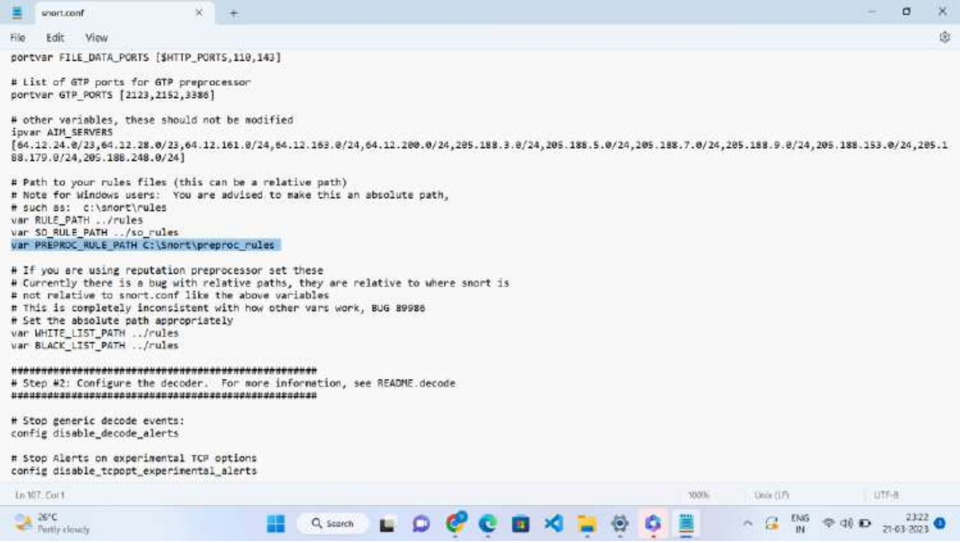
10. Perform the following commands.

Change 1



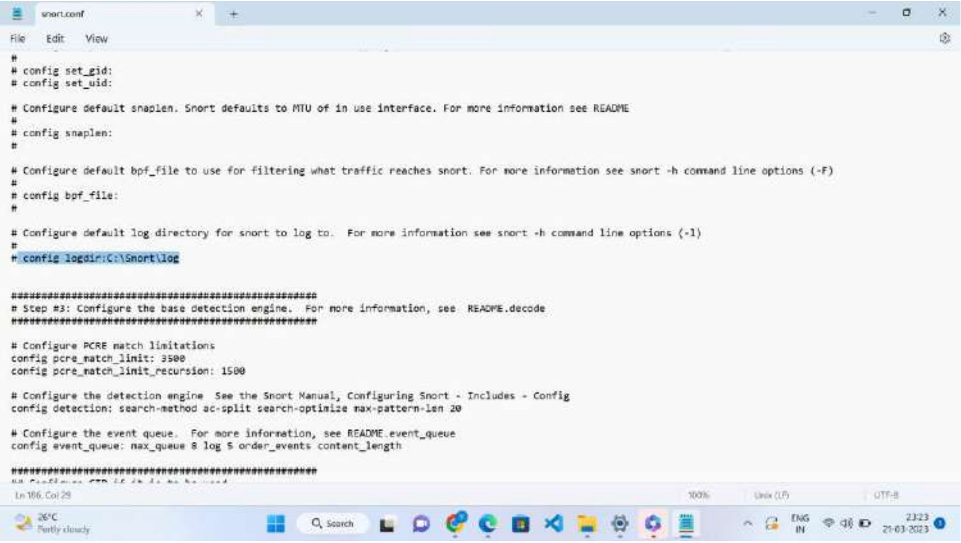
```
###################################################
# Step #1: Set the network variables.  For more information, see README.variables
###################################################

# 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

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

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET

# List of sql servers on your network
ipvar SQL_SERVERS $HOME_NET

# List of telnet servers on your network
ipvar TELNET_SERVERS $HOME_NET

# List of ssh servers on your network
ipvar SSH_SERVERS $HOME_NET

# List of ftp servers on your network
ipvar FTP_SERVERS $HOME_NET

# List of sip servers on your network
ipvar SIP_SERVERS $HOME_NET
```

Change 2



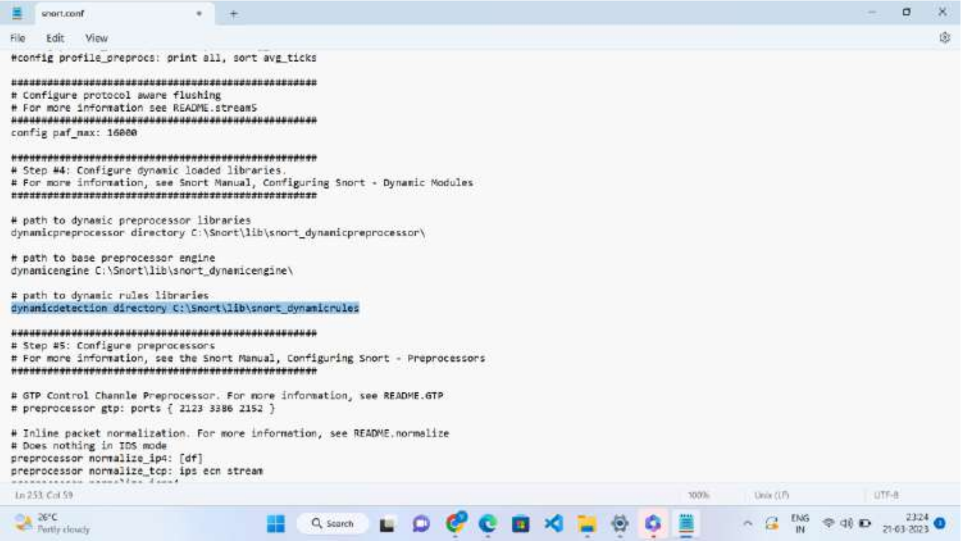
```
portvar FILE_DATA_PORTS [$HTTP_PORTS,110,143]

# List of GTP ports for GTP preprocessor
portvar GTP_PORTS [2123,2152,3386]

# other variables, these should not be modified
ipvar AIM_SERVERS
[64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188.3.0/24,205.188.5.0/24,205.188.7.0/24,205.188.9.0/24,205.188.153.0/24,205.1
88.179.0/24,205.188.248.0/24]

# 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:\snort\rules
var RULE_PATH ../rules
var SO_RULE_PATH ../so_rules
var PREPROC_RULE_PATH C:\Snort\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 ../rules
var BLACK_LIST_PATH ../rules

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

# Stop generic decode events:
config disable_decode_alerts

# Stop Alerts on experimental TCP options
config disable_tcpopt_experimental_alerts
```

Change 3



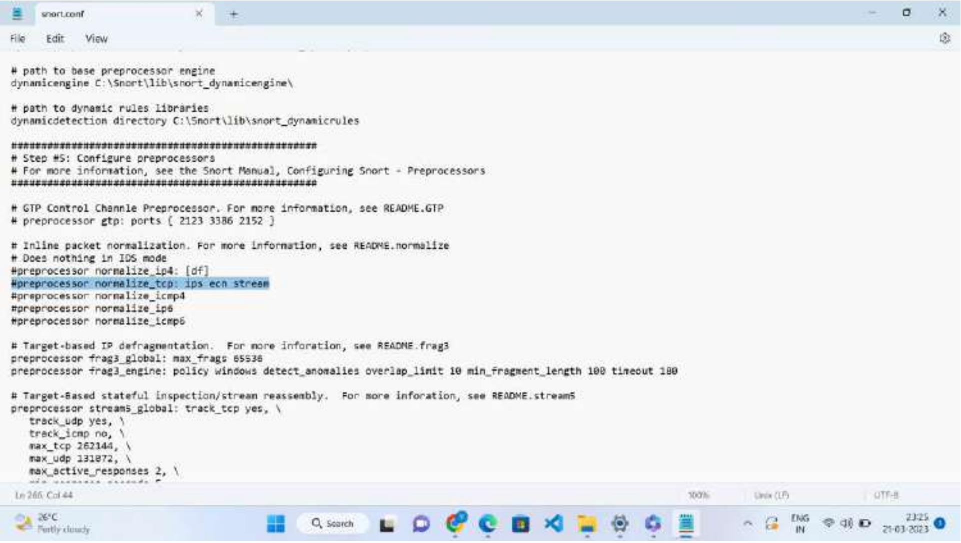
```
#
# config set_gid:
# config set_uid:

# Configure default snaplen. Snort defaults to MTU of in use interface. For more information see README
#
# config snaplen:
#

# Configure default bpf_file to use for filtering what traffic reaches snort. For more information see snort -h command line options (-F)
#
# config bpf_file:
#

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


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

# Configure PCRE match limitations
config pcre_match_limit: 3500
config pcre_match_limit_recursion: 1500

# Configure the detection engine  See the Snort Manual, Configuring Snort - Includes - Config
config detection: search-method ac-split search-optimize max-pattern-len 20

# Configure the event queue.  For more information, see README.event_queue
config event_queue: max_queue 8 log 5 order_events content_length

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

Change 4



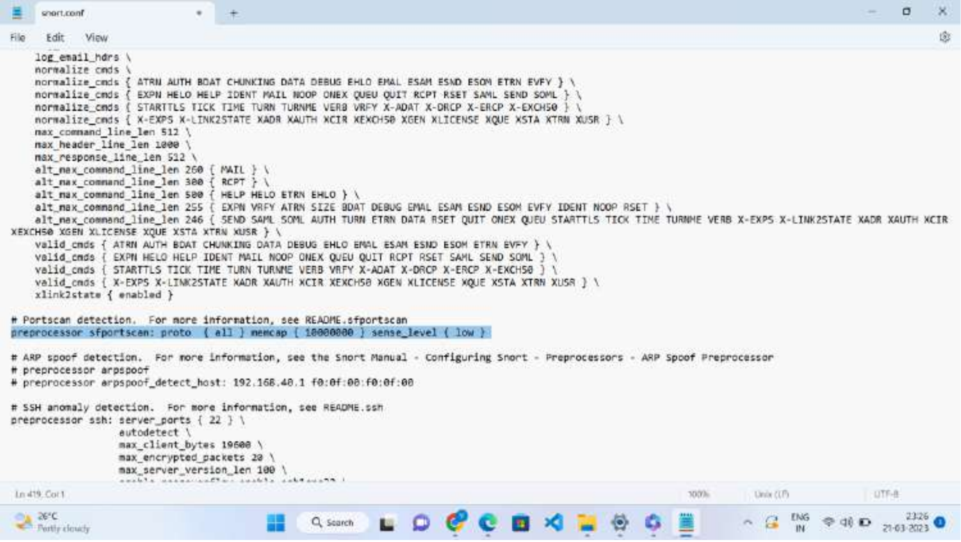
```
#config profile_preprocs: print all, sort avg_ticks

###################################################
# Configure protocol aware flushing
# For more information see README.stream5
###################################################
config paf_max: 16000

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

# path to dynamic preprocessor libraries
dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor\

# path to base preprocessor engine
dynamicengine C:\Snort\lib\snort_dynamicengine\

# path to dynamic rules libraries
dynamicdetection directory C:\Snort\lib\snort_dynamicrules

###################################################
# Step #5: Configure preprocessors
# For more information, see the Snort Manual, Configuring Snort - Preprocessors
###################################################

# GTP Control Channle Preprocessor. For more information, see README.GTP
# preprocessor gtp: ports { 2123 3386 2152 }

# Inline packet normalization. For more information, see README.normalize
# Does nothing in IDS mode
preprocessor normalize_ip4: [df]
preprocessor normalize_tcp: ips ecn stream
```

Change 5



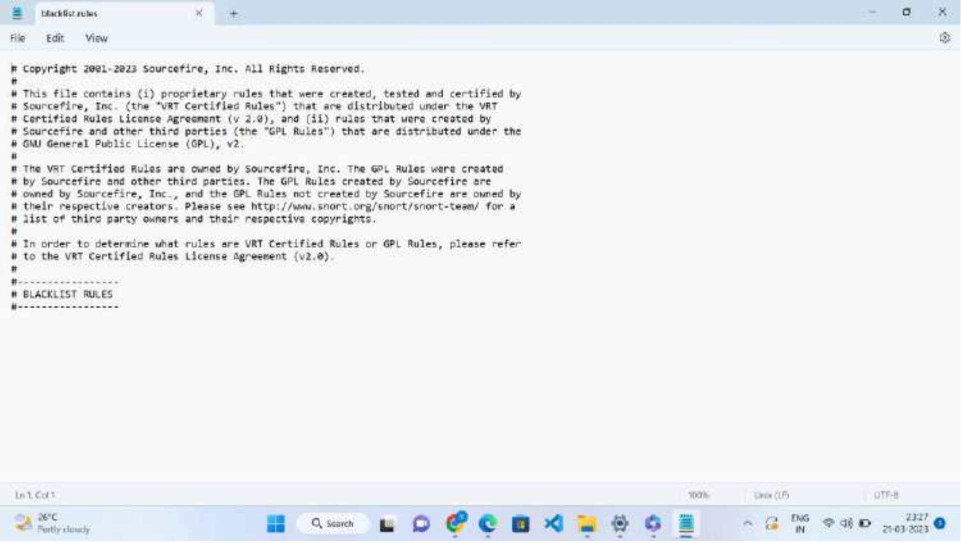
```
# path to base preprocessor engine
dynamicengine C:\Snort\lib\snort_dynamicengine\

# path to dynamic rules libraries
dynamicdetection directory C:\Snort\lib\snort_dynamicrules

###################################################
# Step #5: Configure preprocessors
# For more information, see the Snort Manual, Configuring Snort - Preprocessors
###################################################

# GTP Control Channle Preprocessor. For more information, see README.GTP
# preprocessor gtp: ports { 2123 3386 2152 }

# Inline packet normalization. For more information, see README.normalize
# Does nothing in IDS mode
#preprocessor normalize_ip4: [df]
#preprocessor normalize_tcp: ips ecn stream
#preprocessor normalize_icmp4
#preprocessor normalize_ip6
#preprocessor normalize_icmp6

# Target-based IP defragmentation.  For more inforation, see README.frag3
preprocessor frag3_global: max_frags 65536
preprocessor frag3_engine: policy windows detect_anomalies overlap_limit 10 min_fragment_length 100 timeout 180

# Target-Based stateful inspection/stream reassembly.  For more inforation, see README.stream5
preprocessor stream5_global: track_tcp yes, \
   track_udp yes, \
   track_icmp no, \
   max_tcp 262144, \
   max_udp 131072, \
   max_active_responses 2, \
```

Change 6



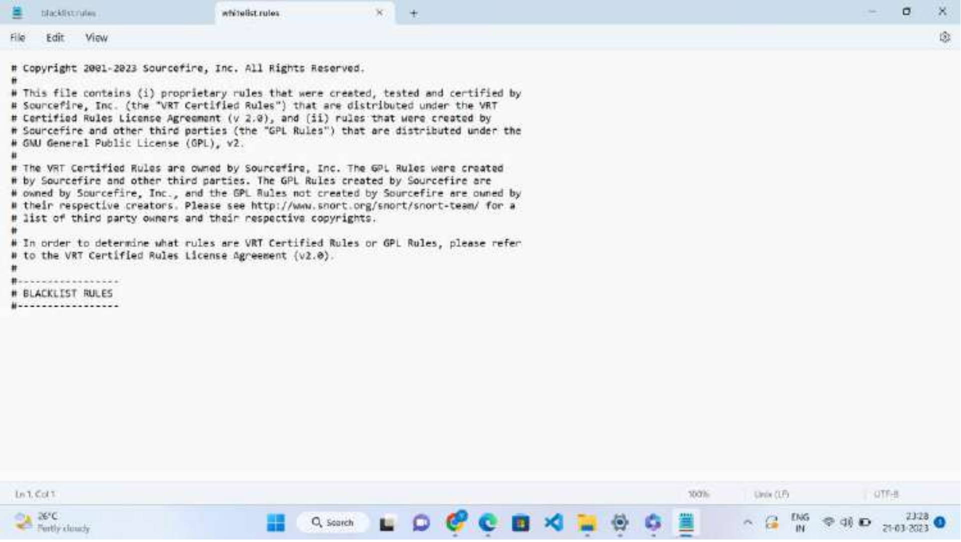
```
    log_email_hdrs \
    normalize cmds \
    normalize_cmds { ATRN AUTH BDAT CHUNKING DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY } \
    normalize_cmds { EXPN HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SOML } \
    normalize_cmds { STARTTLS TICK TIME TURN TURNME VERB VRFY X-ADAT X-DRCP X-ERCP X-EXCH50 } \
    normalize_cmds { X-EXPS X-LINK2STATE XADR XAUTH XCIR XEXCH50 XGEN XLICENSE XQUE XSTA XTRN XUSR } \
    max_command_line_len 512 \
    max_header_line_len 1000 \
    max_response_line_len 512 \
    alt_max_command_line_len 260 { MAIL } \
    alt_max_command_line_len 300 { RCPT } \
    alt_max_command_line_len 500 { HELP HELO ETRN EHLO } \
    alt_max_command_line_len 255 { EXPN VRFY ATRN SIZE BDAT DEBUG EMAL ESAM ESND ESOM EVFY IDENT NOOP RSET } \
    alt_max_command_line_len 246 { SEND SAML SOML AUTH TURN ETRN DATA RSET QUIT ONEX QUEU STARTTLS TICK TIME TURNME VERB X-EXPS X-LINK2STATE XADR XAUTH XCIR
XEXCH50 XGEN XLICENSE XQUE XSTA XTRN XUSR } \
    valid_cmds { ATRN AUTH BDAT CHUNKING DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY } \
    valid_cmds { EXPN HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SOML } \
    valid_cmds { STARTTLS TICK TIME TURN TURNME VERB VRFY X-ADAT X-DRCP X-ERCP X-EXCH50 } \
    valid_cmds { X-EXPS X-LINK2STATE XADR XAUTH XCIR XEXCH50 XGEN XLICENSE XQUE XSTA XTRN XUSR } \
    xlink2state { enabled }

# 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

# SSH anomaly detection.  For more information, see README.ssh
preprocessor ssh: server_ports { 22 } \
                  autodetect \
                  max_client_bytes 19600 \
                  max_encrypted_packets 20 \
                  max_server_version_len 100 \
```

blacklist.rules



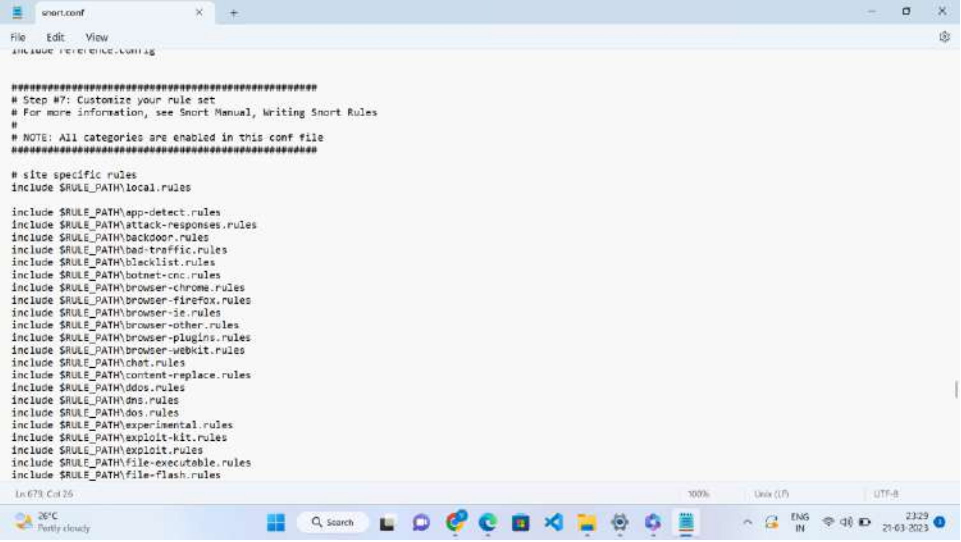
```
# Copyright 2001-2023 Sourcefire, Inc. All Rights Reserved.
#
# This file contains (i) proprietary rules that were created, tested and certified by
# Sourcefire, Inc. (the "VRT Certified Rules") that are distributed under the VRT
# Certified Rules License Agreement (v 2.0), and (ii) rules that were 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).
#
#-----------------
# BLACKLIST RULES
#-----------------
```

whitelist.rules

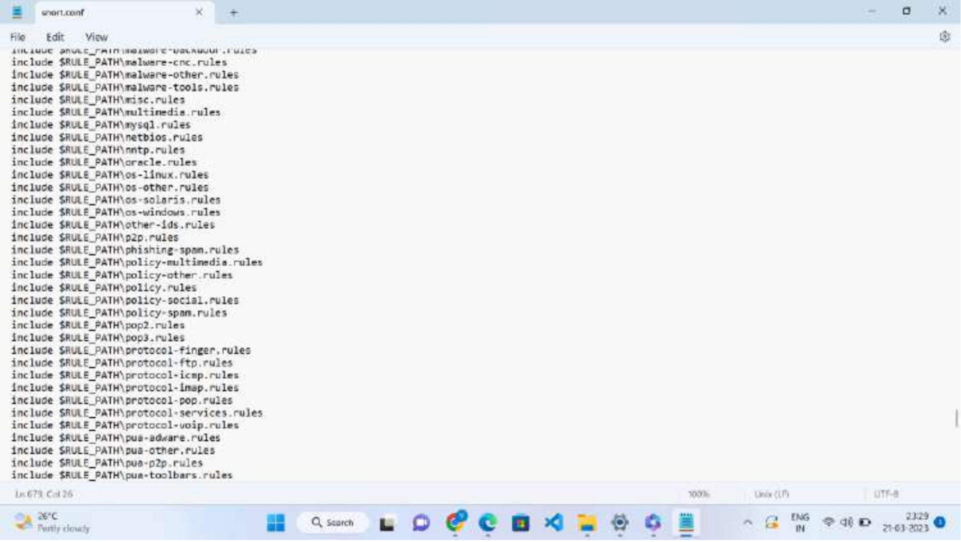


```
# Copyright 2001-2023 Sourcefire, Inc. All Rights Reserved.
#
# This file contains (i) proprietary rules that were created, tested and certified by
# Sourcefire, Inc. (the "VRT Certified Rules") that are distributed under the VRT
# Certified Rules License Agreement (v 2.0), and (ii) rules that were 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).
#
#-----------------
# BLACKLIST RULES
#-----------------
```

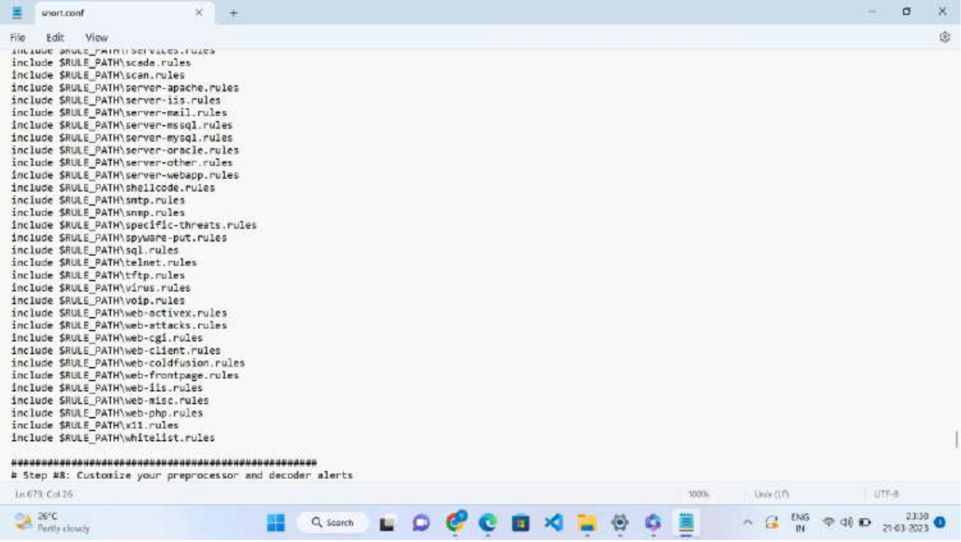
Change 7



```
include reference.config


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

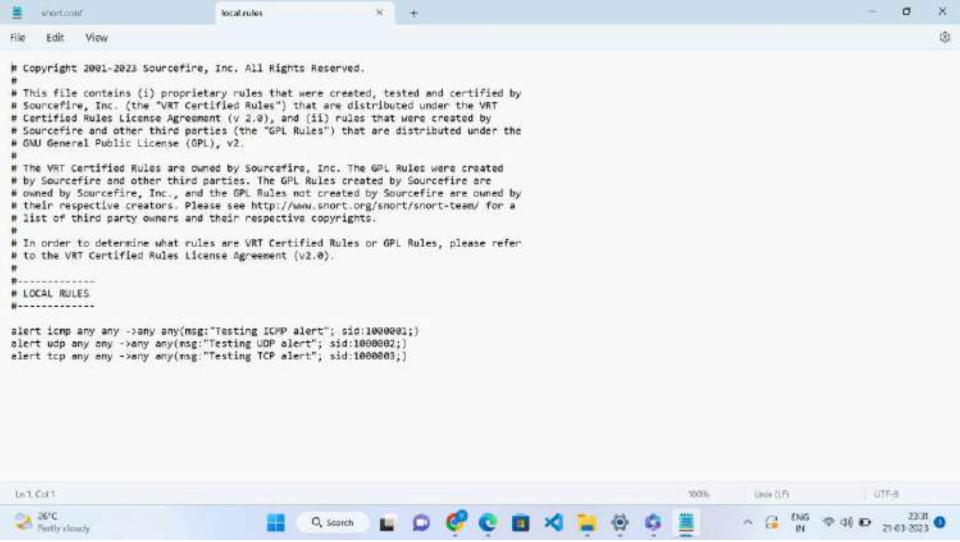


```
include $RULE_PATH\malware-backdoor.rules
include $RULE_PATH\malware-cnc.rules
include $RULE_PATH\malware-other.rules
include $RULE_PATH\malware-tools.rules
include $RULE_PATH\misc.rules
include $RULE_PATH\multimedia.rules
include $RULE_PATH\mysql.rules
include $RULE_PATH\netbios.rules
include $RULE_PATH\nntp.rules
include $RULE_PATH\oracle.rules
include $RULE_PATH\os-linux.rules
include $RULE_PATH\os-other.rules
include $RULE_PATH\os-solaris.rules
include $RULE_PATH\os-windows.rules
include $RULE_PATH\other-ids.rules
include $RULE_PATH\p2p.rules
include $RULE_PATH\phishing-spam.rules
include $RULE_PATH\policy-multimedia.rules
include $RULE_PATH\policy-other.rules
include $RULE_PATH\policy.rules
include $RULE_PATH\policy-social.rules
include $RULE_PATH\policy-spam.rules
include $RULE_PATH\pop2.rules
include $RULE_PATH\pop3.rules
include $RULE_PATH\protocol-finger.rules
include $RULE_PATH\protocol-ftp.rules
include $RULE_PATH\protocol-icmp.rules
include $RULE_PATH\protocol-imap.rules
include $RULE_PATH\protocol-pop.rules
include $RULE_PATH\protocol-services.rules
include $RULE_PATH\protocol-voip.rules
include $RULE_PATH\pua-adware.rules
include $RULE_PATH\pua-other.rules
include $RULE_PATH\pua-p2p.rules
include $RULE_PATH\pua-toolbars.rules
```



```
include $RULE_PATH\services.rules
include $RULE_PATH\scada.rules
include $RULE_PATH\scan.rules
include $RULE_PATH\server-apache.rules
include $RULE_PATH\server-iis.rules
include $RULE_PATH\server-mail.rules
include $RULE_PATH\server-mssql.rules
include $RULE_PATH\server-mysql.rules
include $RULE_PATH\server-oracle.rules
include $RULE_PATH\server-other.rules
include $RULE_PATH\server-webapp.rules
include $RULE_PATH\shellcode.rules
include $RULE_PATH\smtp.rules
include $RULE_PATH\snmp.rules
include $RULE_PATH\specific-threats.rules
include $RULE_PATH\spyware-put.rules
include $RULE_PATH\sql.rules
include $RULE_PATH\telnet.rules
include $RULE_PATH\tftp.rules
include $RULE_PATH\virus.rules
include $RULE_PATH\voip.rules
include $RULE_PATH\web-activex.rules
include $RULE_PATH\web-attacks.rules
include $RULE_PATH\web-cgi.rules
include $RULE_PATH\web-client.rules
include $RULE_PATH\web-coldfusion.rules
include $RULE_PATH\web-frontpage.rules
include $RULE_PATH\web-iis.rules
include $RULE_PATH\web-misc.rules
include $RULE_PATH\web-php.rules
include $RULE_PATH\x11.rules
include $RULE_PATH\whitelist.rules

###################################################
# Step #8: Customize your preprocessor and decoder alerts
```

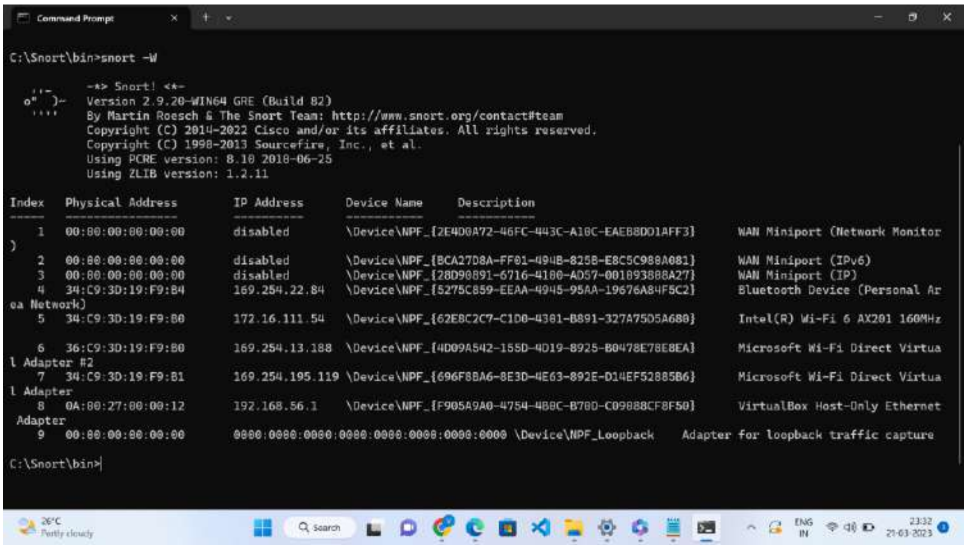
Local rules



```
# Copyright 2001-2023 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 ICMP alert"; sid:1000001;)
alert udp any any ->any any(msg:"Testing UDP alert"; sid:1000002;)
alert tcp any any ->any any(msg:"Testing TCP alert"; sid:1000003;)
```

Test for 1st (For Testing Snort):

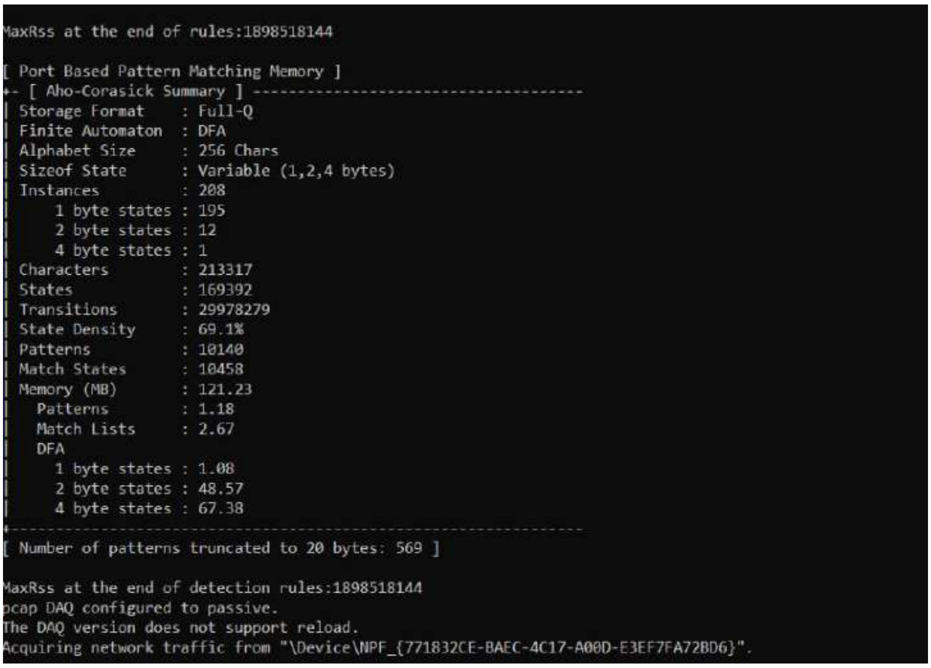
Snort -W



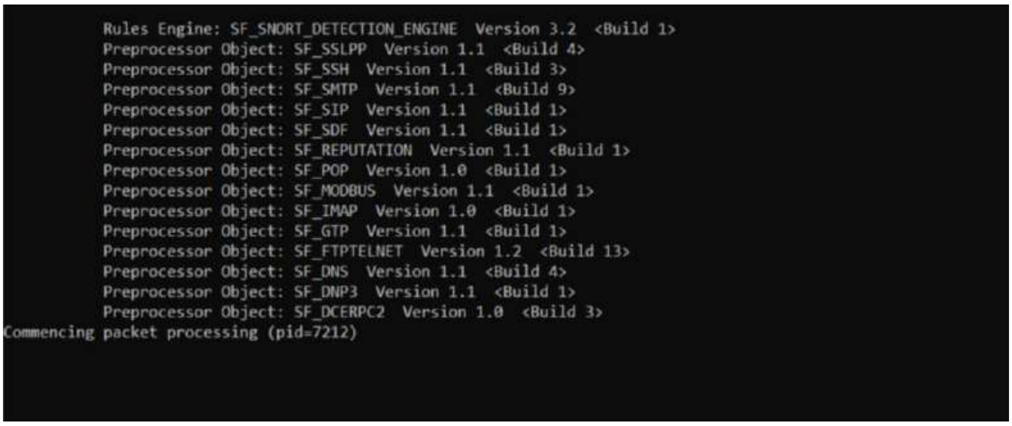
```
C:\Snort\bin>snort -W

   ,,_     -*> 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_{2E4D0A72-46FC-443C-A10C-EAEB8DD1AFF3}     WAN Miniport (Network Monitor
)
    2   00:00:00:00:00:00        disabled        \Device\NPF_{BCA27D8A-FF01-494B-825B-E8C5C988A081}     WAN Miniport (IPv6)
    3   00:00:00:00:00:00        disabled        \Device\NPF_{28D90891-6716-4100-AD57-001093888A27}     WAN Miniport (IP)
    4   34:C9:3D:19:F9:B4        169.254.22.84   \Device\NPF_{5275C859-EEAA-4945-95AA-19676A84F5C2}     Bluetooth Device (Personal Ar
ea Network)
    5   34:C9:3D:19:F9:B0        172.16.111.54   \Device\NPF_{62E8C2C7-C1D0-4381-B891-327A75D5A680}     Intel(R) Wi-Fi 6 AX201 160MHz

    6   36:C9:3D:19:F9:B0        169.254.13.188  \Device\NPF_{4D09A542-155D-4D19-8925-B0478E78E8EA}     Microsoft Wi-Fi Direct Virtua
l Adapter #2
    7   34:C9:3D:19:F9:B1        169.254.195.119 \Device\NPF_{696F8BA6-8E3D-4E63-892E-D14EF52885B6}     Microsoft Wi-Fi Direct Virtua
l Adapter
    8   0A:00:27:00:00:12        192.168.56.1    \Device\NPF_{F905A9A0-4754-4B8C-B78D-C09888CF8F50}     VirtualBox Host-Only Ethernet
 Adapter
    9   00:00:00:00:00:00        0000:0000:0000:0000:0000:0000:0000:0000 \Device\NPF_Loopback    Adapter for loopback traffic capture

C:\Snort\bin>
```

Test for 2nd Cmd:

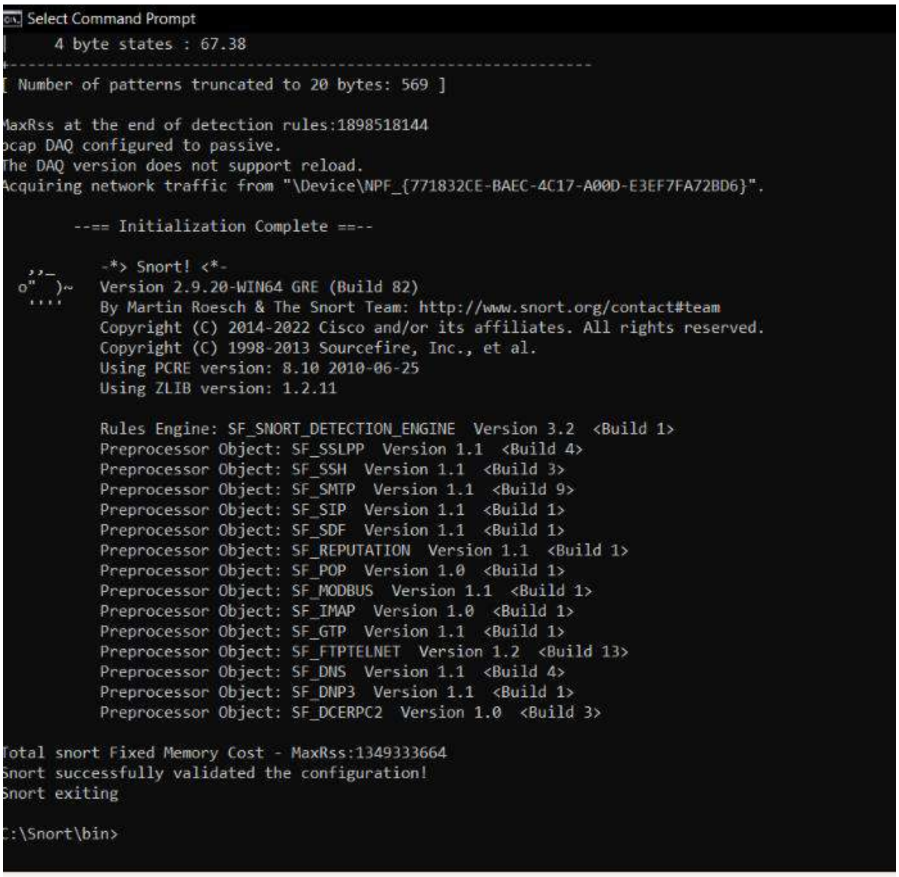
Snort -i 1 -c C:\Snort\etc\snort.conf -T



```
MaxRss at the end of rules:1898518144

[ 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         : 208
|     1 byte states : 195
|     2 byte states : 12
|     4 byte states : 1
| Characters        : 213317
| States            : 169392
| Transitions       : 29978279
| State Density     : 69.1%
| Patterns          : 10140
| Match States      : 10458
| Memory (MB)       : 121.23
|   Patterns        : 1.18
|   Match Lists     : 2.67
|   DFA
|     1 byte states : 1.08
|     2 byte states : 48.57
|     4 byte states : 67.38
+----------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 569 ]

MaxRss at the end of detection rules:1898518144
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{771832CE-BAEC-4C17-A00D-E3EF7FA72BD6}".
```



```
           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>
Commencing packet processing (pid=7212)
```

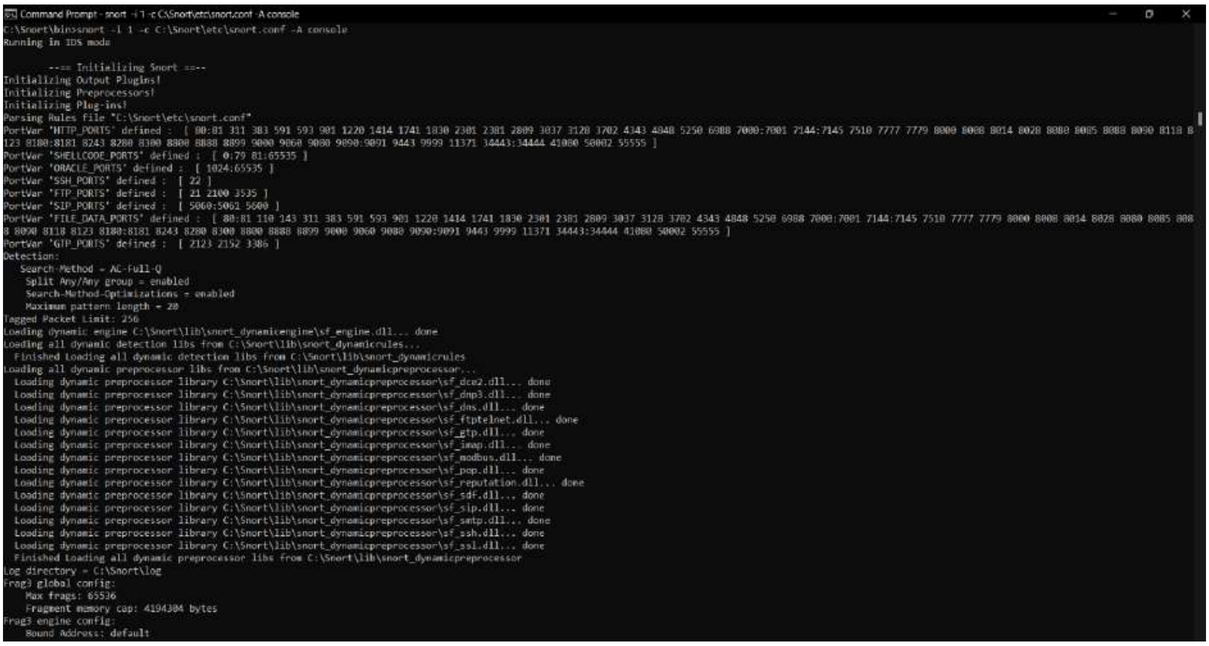


Select Command Prompt

```
|     4 byte states : 67.38
+-----------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 569 ]

MaxRss at the end of detection rules:1898518144
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{771832CE-BAEC-4C17-A00D-E3EF7FA72BD6}".

        --== 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:1349333664
Snort successfully validated the configuration!
Snort exiting

C:\Snort\bin>
```

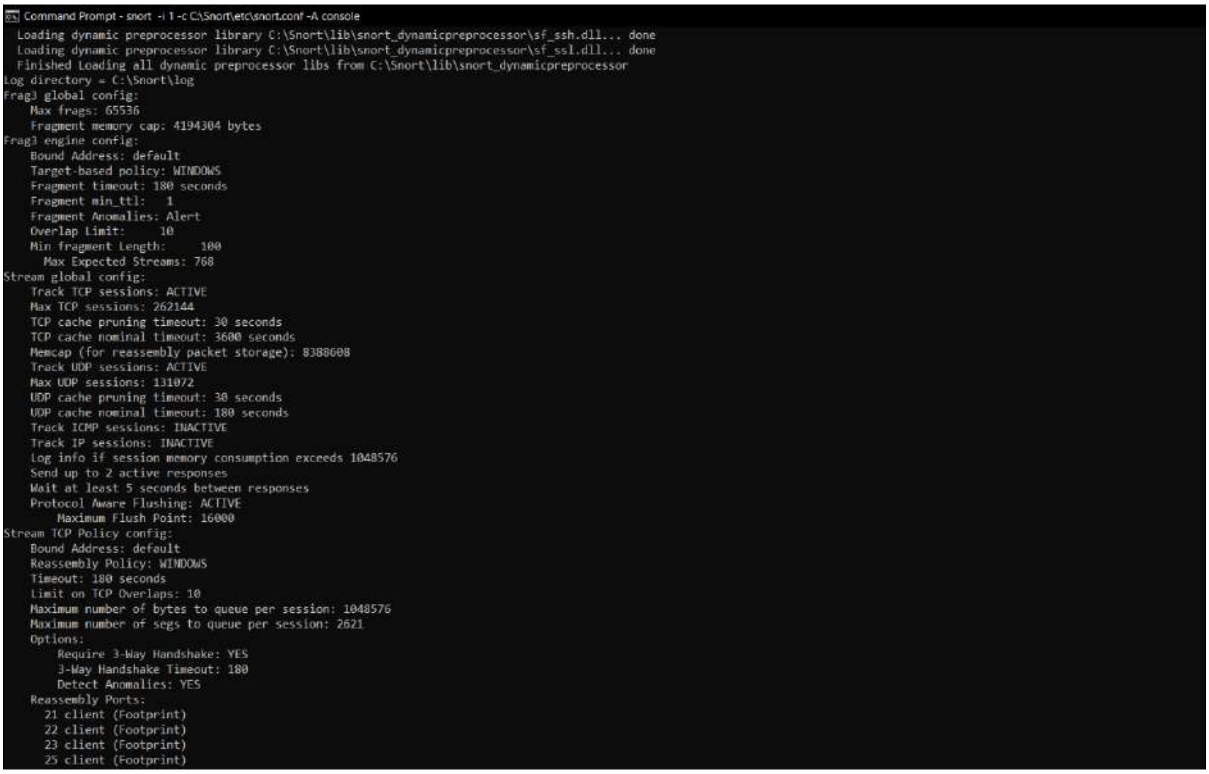
Test for 3rd Cmd:

Snort -I 1 -c C:\Snort\etc\snort.conf -A console



Command Prompt - snort -i 1 -c C:\Snort\etc\snort.conf -A console

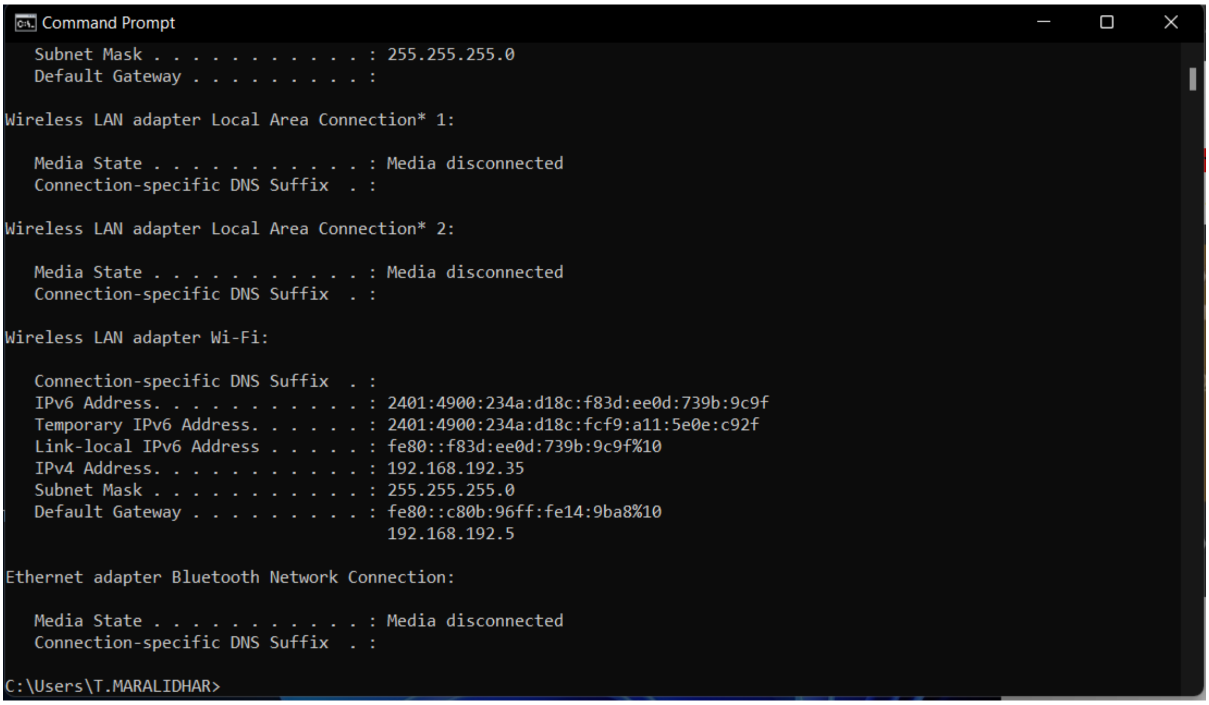
```
C:\Snort\bin>snort -i 1 -c C:\Snort\etc\snort.conf -A console
Running in IDS mode

        --== 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 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8
123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 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 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 808
8 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 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:\Snort\lib\snort_dynamicengine\sf_engine.dll... done
Loading all dynamic detection libs from C:\Snort\lib\snort_dynamicrules...
  Finished Loading all dynamic detection libs from C:\Snort\lib\snort_dynamicrules
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:
    Bound Address: default
```


Command Prompt - snort -i 1 -c C:\Snort\etc\snort.conf -A console

```
  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:
    Bound Address: default
    Target-based policy: WINDOWS
    Fragment timeout: 180 seconds
    Fragment min_ttl:   1
    Fragment Anomalies: Alert
    Overlap Limit:     10
    Min fragment Length:     100
      Max Expected Streams: 768
Stream global config:
    Track TCP sessions: ACTIVE
    Max TCP sessions: 262144
    TCP cache pruning timeout: 30 seconds
    TCP cache nominal timeout: 3600 seconds
    Memcap (for reassembly packet storage): 8388608
    Track UDP sessions: ACTIVE
    Max UDP sessions: 131072
    UDP cache pruning timeout: 30 seconds
    UDP cache nominal timeout: 180 seconds
    Track ICMP sessions: INACTIVE
    Track IP sessions: INACTIVE
    Log info if session memory consumption exceeds 1048576
    Send up to 2 active responses
    Wait at least 5 seconds between responses
    Protocol Aware Flushing: ACTIVE
        Maximum Flush Point: 16000
Stream TCP Policy config:
    Bound Address: default
    Reassembly Policy: WINDOWS
    Timeout: 180 seconds
    Limit on TCP Overlaps: 10
    Maximum number of bytes to queue per session: 1048576
    Maximum number of segs to queue per session: 2621
    Options:
        Require 3-Way Handshake: YES
        3-Way Handshake Timeout: 180
        Detect Anomalies: YES
    Reassembly Ports:
      21 client (Footprint)
      22 client (Footprint)
      23 client (Footprint)
      25 client (Footprint)
```

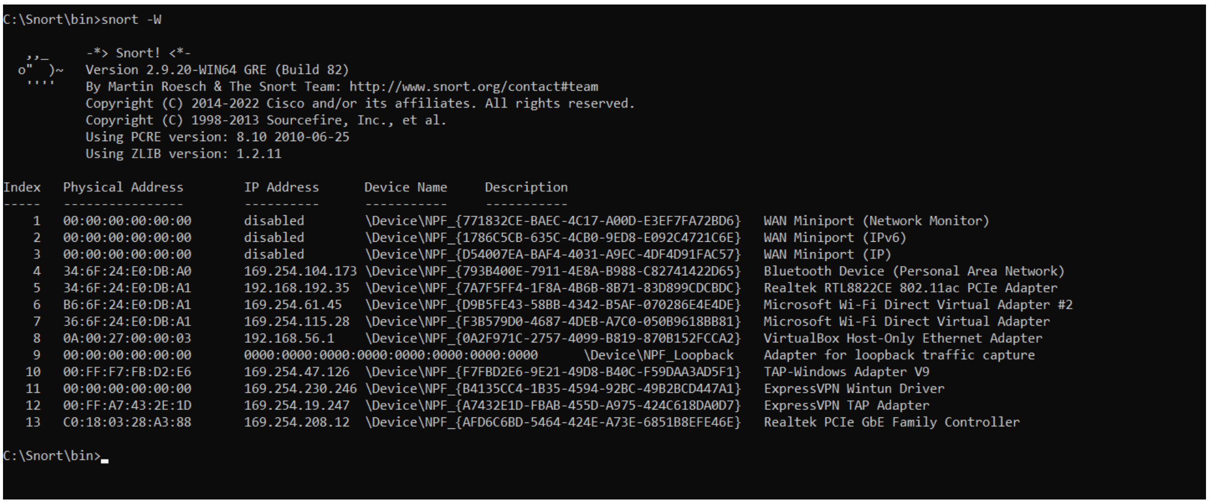
After connecting to Wi-fi:

IP Address:



```
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2401:4900:234a:d18c:f83d:ee0d:739b:9c9f
   Temporary IPv6 Address. . . . . . : 2401:4900:234a:d18c:fcf9:a11:5e0e:c92f
   Link-local IPv6 Address . . . . . : fe80::f83d:ee0d:739b:9c9f%10
   IPv4 Address. . . . . . . . . . . : 192.168.192.35
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::c80b:96ff:fe14:9ba8%10
                                       192.168.192.5

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\T.MARALIDHAR>
```

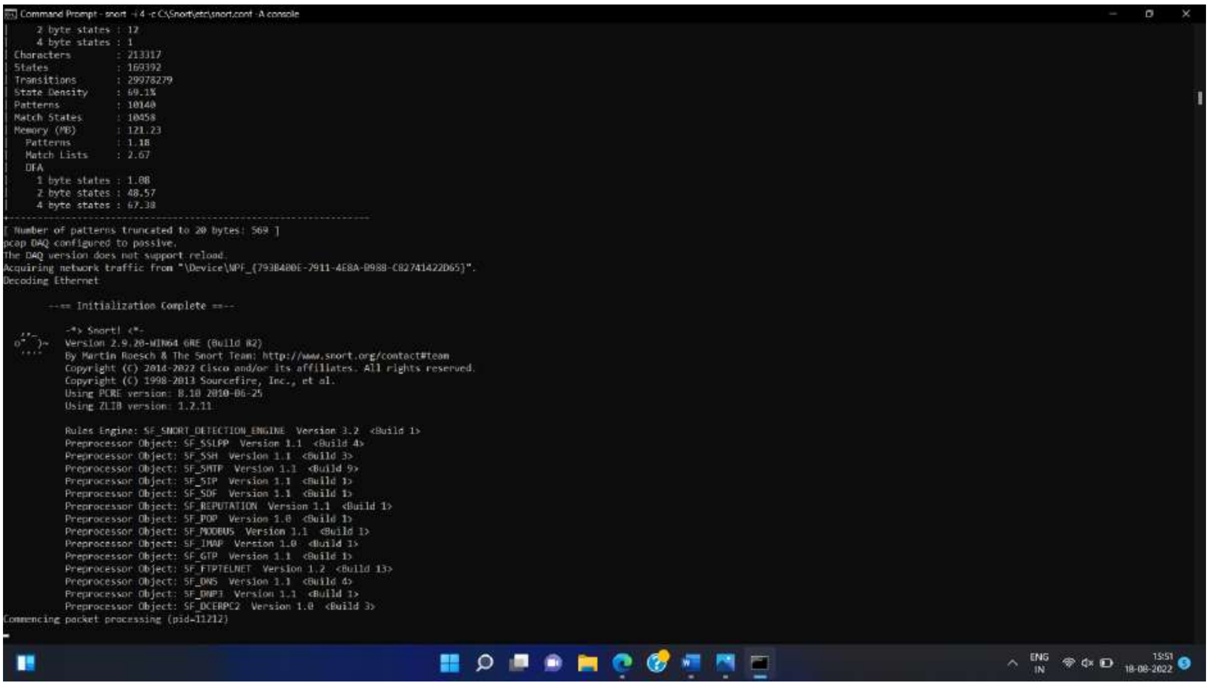
Test using snort –W:



```
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_{771832CE-BAEC-4C17-A00D-E3EF7FA72BD6}  WAN Miniport (Network Monitor)
    2  00:00:00:00:00:00     disabled        \Device\NPF_{1786C5CB-635C-4CB0-9ED8-E092C4721C6E}  WAN Miniport (IPv6)
    3  00:00:00:00:00:00     disabled        \Device\NPF_{D54007EA-BAF4-4031-A9EC-4DF4D91FAC57}  WAN Miniport (IP)
    4  34:6F:24:E0:DB:A0     169.254.104.173 \Device\NPF_{793B400E-7911-4E8A-B988-C82741422D65}  Bluetooth Device (Personal Area Network)
    5  34:6F:24:E0:DB:A1     192.168.192.35  \Device\NPF_{7A7F5FF4-1F8A-4B6B-8B71-83D899CDCBDC}  Realtek RTL8822CE 802.11ac PCIe Adapter
    6  B6:6F:24:E0:DB:A1     169.254.61.45   \Device\NPF_{D9B5FE43-58BB-4342-B5AF-070286E4E4DE}  Microsoft Wi-Fi Direct Virtual Adapter #2
    7  36:6F:24:E0:DB:A1     169.254.115.28  \Device\NPF_{F3B579D0-4687-4DEB-A7C0-050B9618BB81}  Microsoft Wi-Fi Direct Virtual Adapter
    8  0A:00:27:00:00:03     192.168.56.1    \Device\NPF_{0A2F971C-2757-4099-B819-870B152FCCA2}  VirtualBox Host-Only Ethernet Adapter
    9  00:00:00:00:00:00     0000:0000:0000:0000:0000:0000:0000:0000      \Device\NPF_Loopback  Adapter for loopback traffic capture
   10  00:FF:F7:FB:D2:E6     169.254.47.126  \Device\NPF_{F7FBD2E6-9E21-49D8-B40C-F59DAA3AD5F1}  TAP-Windows Adapter V9
   11  00:00:00:00:00:00     169.254.230.246 \Device\NPF_{B4135CC4-1B35-4594-92BC-49B2BCD447A1}  ExpressVPN Wintun Driver
   12  00:FF:A7:43:2E:1D     169.254.19.247  \Device\NPF_{A7432E1D-FBAB-455D-A975-424C618DA0D7}  ExpressVPN TAP Adapter
   13  C0:18:03:28:A3:88     169.254.208.12  \Device\NPF_{AFD6C6BD-5464-424E-A73E-6851B8EFE46E}  Realtek PCIe GbE Family Controller

C:\Snort\bin>_
```

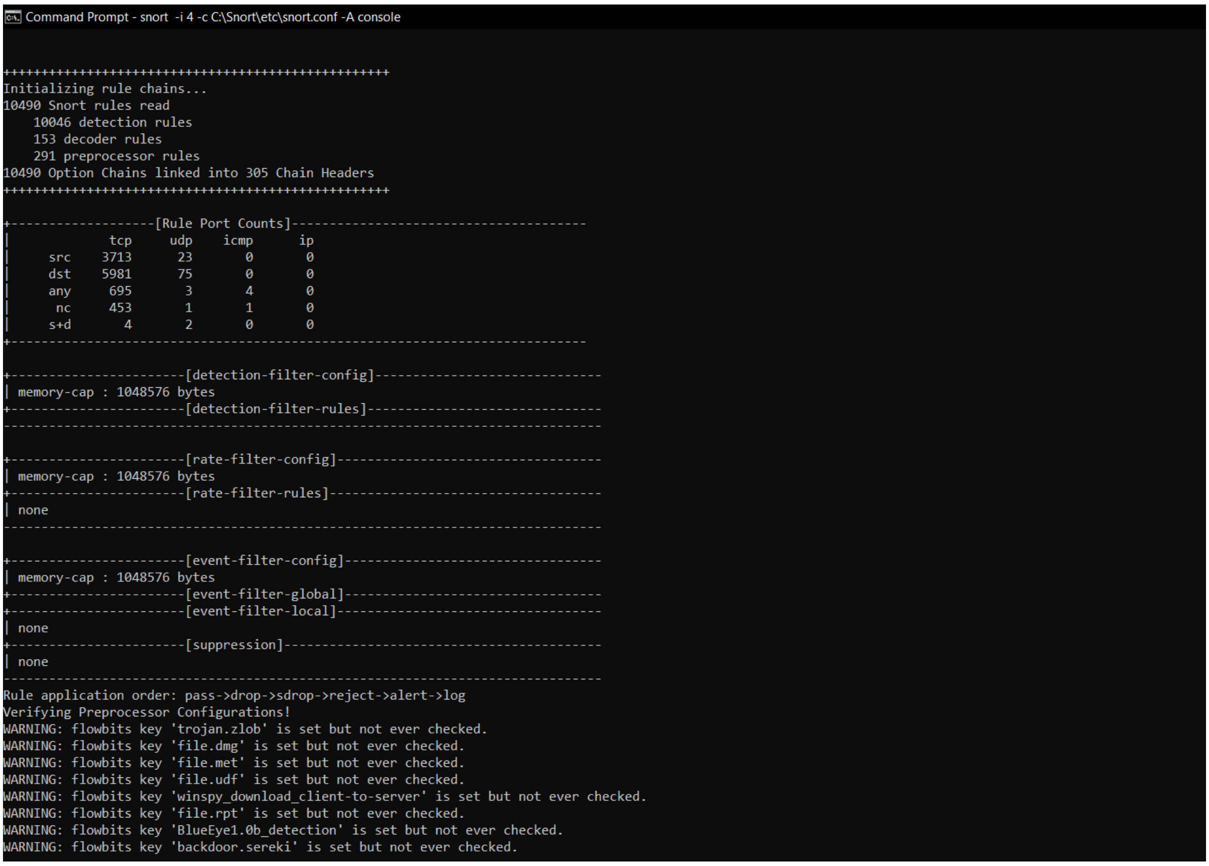
Test for 5th Cmd:

Snort -i 4 -c C:\Snort\etc\snort.conf -A console



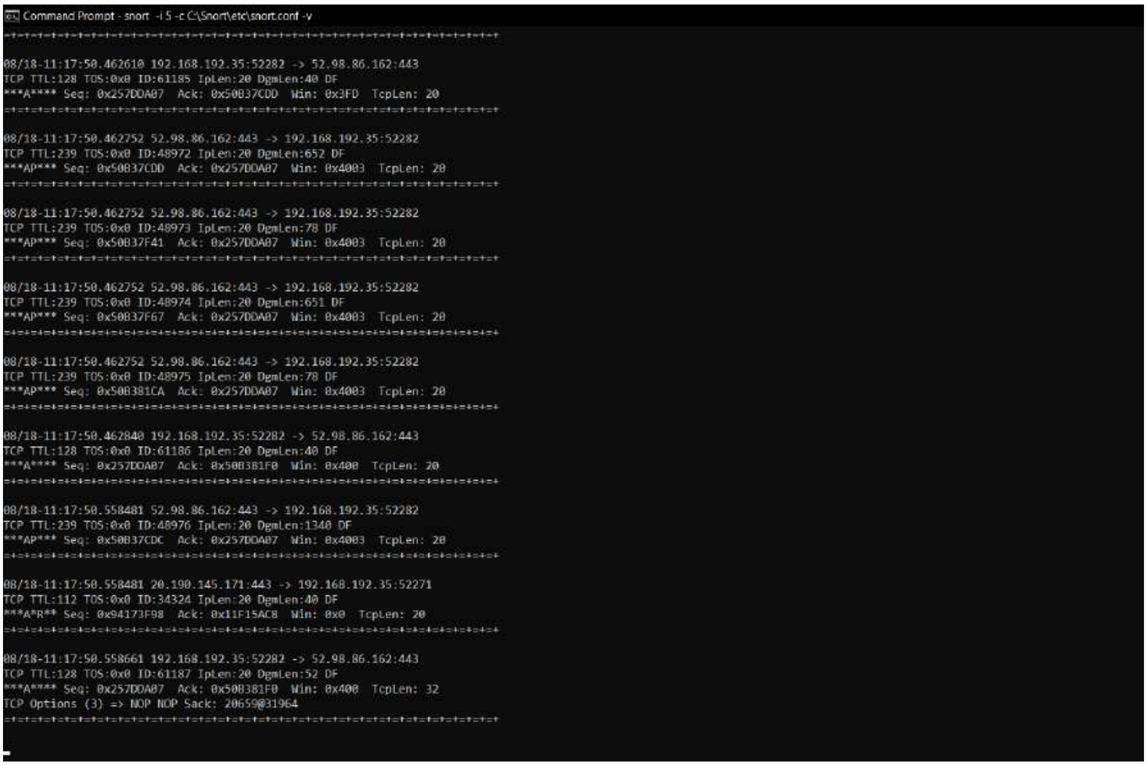
Command Prompt - snort -i 4 -c C:\Snort\etc\snort.conf -A console
ENG
IN
15:51
18-08-2022

```
|      2 byte states : 12
|      4 byte states : 1
| Characters         : 213317
| States             : 169392
| Transitions        : 29978279
| State Density      : 69.1%
| Patterns           : 10140
| Match States       : 10458
| Memory (MB)        : 121.23
|   Patterns         : 1.18
|   Match Lists      : 2.67
|   DFA
|     1 byte states : 1.08
|     2 byte states : 48.57
|     4 byte states : 67.38
+----------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 569 ]
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{793B400E-7911-4E8A-B988-C82741422D65}".
Decoding Ethernet

        --== 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>
Commencing packet processing (pid=11212)
_
```



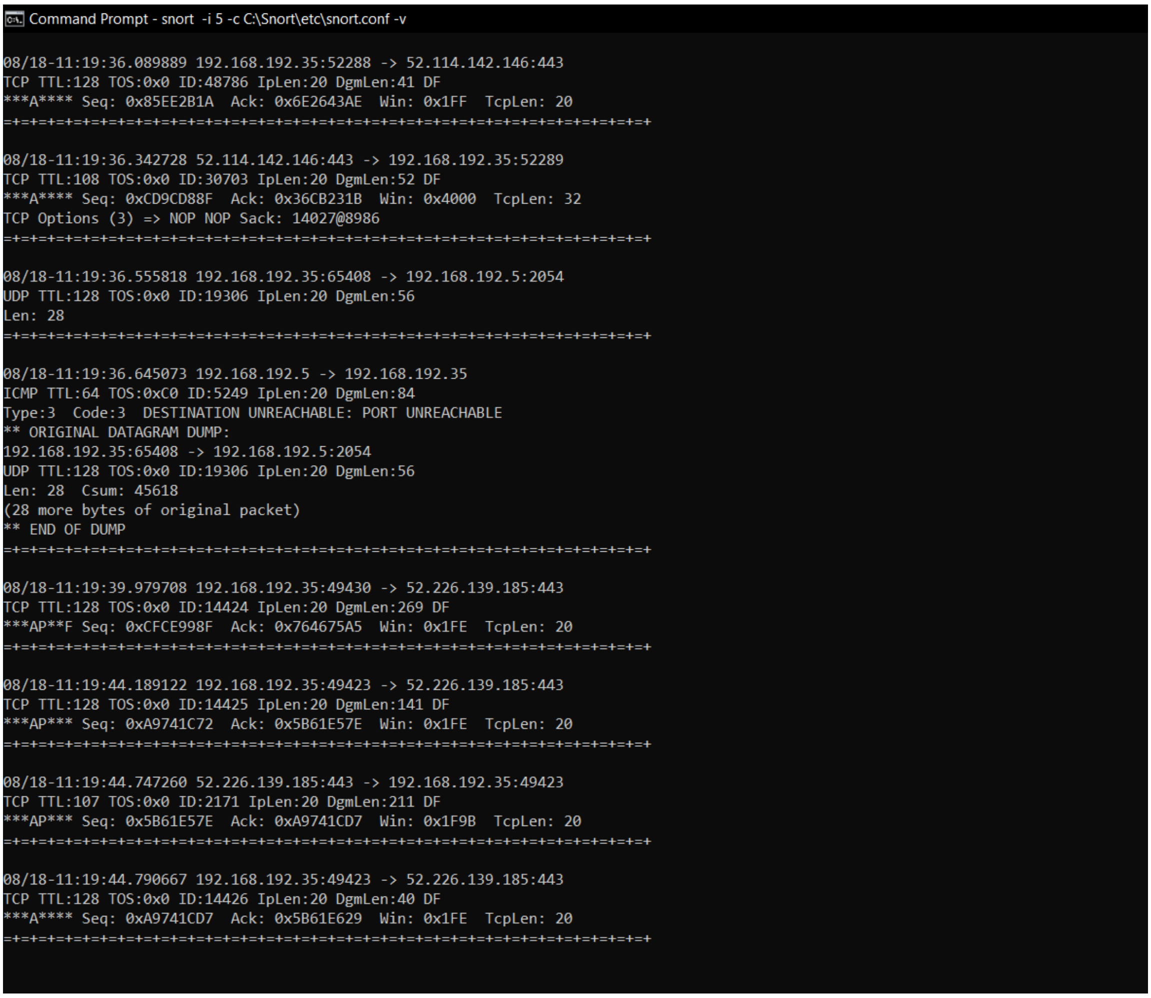
Command Prompt - snort -i 4 -c C:\Snort\etc\snort.conf -A console

```
+++++++++++++++++++++++++++++++++++++++++++++++++++
Initializing rule chains...
10490 Snort rules read
    10046 detection rules
    153 decoder rules
    291 preprocessor rules
10490 Option Chains linked into 305 Chain Headers
+++++++++++++++++++++++++++++++++++++++++++++++++++

+-------------------[Rule Port Counts]---------------------------------------
|             tcp     udp    icmp      ip
|     src     3713     23       0       0
|     dst     5981     75       0       0
|     any      695      3       4       0
|      nc      453      1       1       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 'trojan.zlob' is set but not ever checked.
WARNING: flowbits key 'file.dmg' is set but not ever checked.
WARNING: flowbits key 'file.met' is set but not ever checked.
WARNING: flowbits key 'file.udf' is set but not ever checked.
WARNING: flowbits key 'winspy_download_client-to-server' is set but not ever checked.
WARNING: flowbits key 'file.rpt' is set but not ever checked.
WARNING: flowbits key 'BlueEye1.0b_detection' is set but not ever checked.
WARNING: flowbits key 'backdoor.sereki' is set but not ever checked.
```



Command Prompt - snort -i 5 -c C:\Snort\etc\snort.conf -v

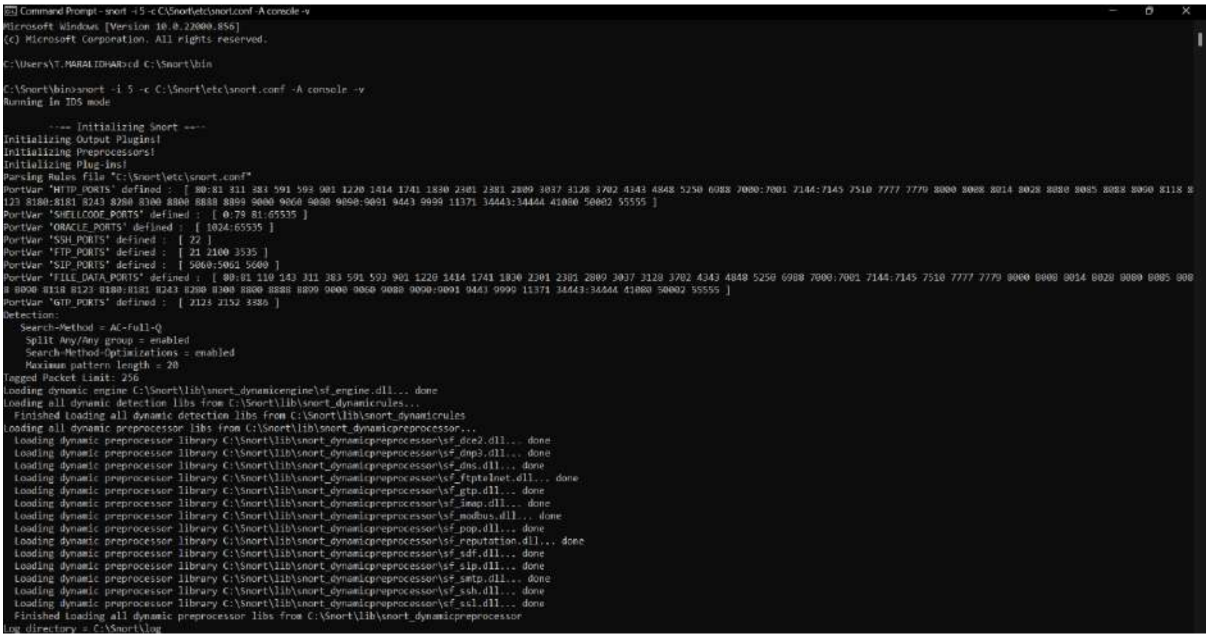
```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

08/18-11:17:50.462610 192.168.192.35:52282 -> 52.98.86.162:443
TCP TTL:128 TOS:0x0 ID:61185 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x257DDA07  Ack: 0x50B37CDD  Win: 0x3FD  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

08/18-11:17:50.462752 52.98.86.162:443 -> 192.168.192.35:52282
TCP TTL:239 TOS:0x0 ID:48972 IpLen:20 DgmLen:652 DF
***AP*** Seq: 0x50B37CDD  Ack: 0x257DDA07  Win: 0x4003  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

08/18-11:17:50.462752 52.98.86.162:443 -> 192.168.192.35:52282
TCP TTL:239 TOS:0x0 ID:48973 IpLen:20 DgmLen:78 DF
***AP*** Seq: 0x50B37F41  Ack: 0x257DDA07  Win: 0x4003  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

08/18-11:17:50.462752 52.98.86.162:443 -> 192.168.192.35:52282
TCP TTL:239 TOS:0x0 ID:48974 IpLen:20 DgmLen:651 DF
***AP*** Seq: 0x50B37F67  Ack: 0x257DDA07  Win: 0x4003  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

08/18-11:17:50.462752 52.98.86.162:443 -> 192.168.192.35:52282
TCP TTL:239 TOS:0x0 ID:48975 IpLen:20 DgmLen:78 DF
***AP*** Seq: 0x50B381CA  Ack: 0x257DDA07  Win: 0x4003  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

08/18-11:17:50.462840 192.168.192.35:52282 -> 52.98.86.162:443
TCP TTL:128 TOS:0x0 ID:61186 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x257DDA07  Ack: 0x50B381F0  Win: 0x400  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

08/18-11:17:50.558481 52.98.86.162:443 -> 192.168.192.35:52282
TCP TTL:239 TOS:0x0 ID:48976 IpLen:20 DgmLen:1340 DF
***AP*** Seq: 0x50B37CDC  Ack: 0x257DDA07  Win: 0x4003  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

08/18-11:17:50.558481 20.190.145.171:443 -> 192.168.192.35:52271
TCP TTL:112 TOS:0x0 ID:34324 IpLen:20 DgmLen:40 DF
***A*R** Seq: 0x94173F98  Ack: 0x11F15AC8  Win: 0x0  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

08/18-11:17:50.558661 192.168.192.35:52282 -> 52.98.86.162:443
TCP TTL:128 TOS:0x0 ID:61187 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x257DDA07  Ack: 0x50B381F0  Win: 0x400  TcpLen: 32
TCP Options (3) => NOP NOP Sack: 20659@31964
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```



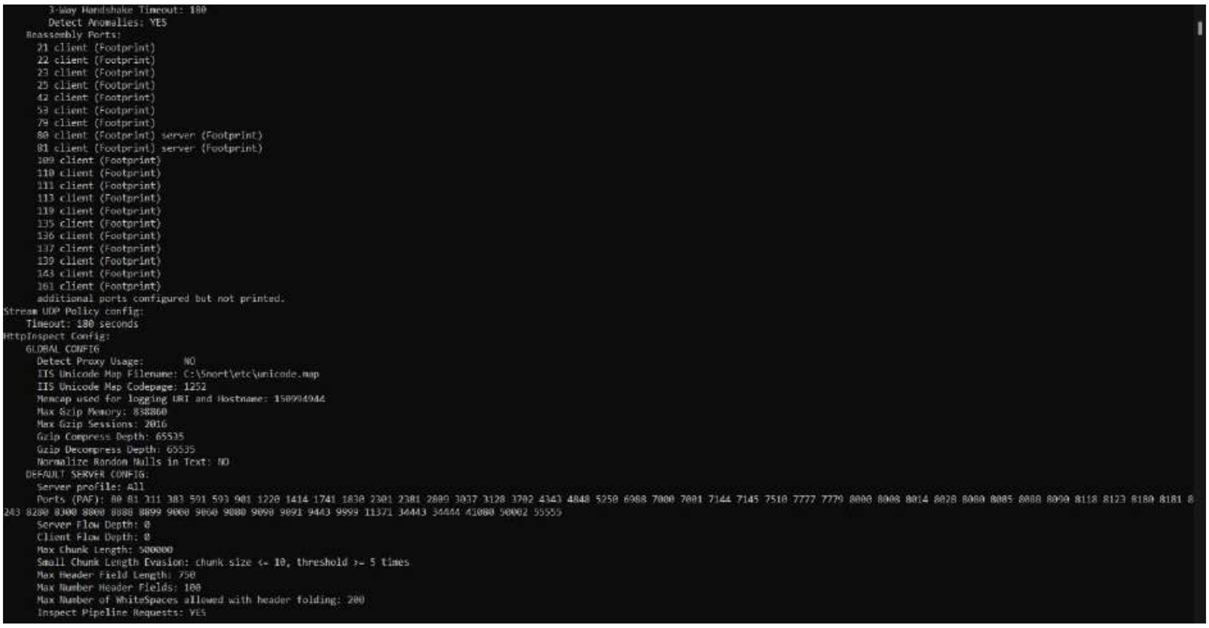
```
08/18-11:19:36.089889 192.168.192.35:52288 -> 52.114.142.146:443
TCP TTL:128 TOS:0x0 ID:48786 IpLen:20 DgmLen:41 DF
***A**** Seq: 0x85EE2B1A  Ack: 0x6E2643AE  Win: 0x1FF  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

08/18-11:19:36.342728 52.114.142.146:443 -> 192.168.192.35:52289
TCP TTL:108 TOS:0x0 ID:30703 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCD9CD88F  Ack: 0x36CB231B  Win: 0x4000  TcpLen: 32
TCP Options (3) => NOP NOP Sack: 14027@8986
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

08/18-11:19:36.555818 192.168.192.35:65408 -> 192.168.192.5:2054
UDP TTL:128 TOS:0x0 ID:19306 IpLen:20 DgmLen:56
Len: 28
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

08/18-11:19:36.645073 192.168.192.5 -> 192.168.192.35
ICMP TTL:64 TOS:0xC0 ID:5249 IpLen:20 DgmLen:84
Type:3  Code:3  DESTINATION UNREACHABLE: PORT UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
192.168.192.35:65408 -> 192.168.192.5:2054
UDP TTL:128 TOS:0x0 ID:19306 IpLen:20 DgmLen:56
Len: 28  Csum: 45618
(28 more bytes of original packet)
** END OF DUMP
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

08/18-11:19:39.979708 192.168.192.35:49430 -> 52.226.139.185:443
TCP TTL:128 TOS:0x0 ID:14424 IpLen:20 DgmLen:269 DF
***AP**F Seq: 0xCFCE998F  Ack: 0x764675A5  Win: 0x1FE  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

08/18-11:19:44.189122 192.168.192.35:49423 -> 52.226.139.185:443
TCP TTL:128 TOS:0x0 ID:14425 IpLen:20 DgmLen:141 DF
***AP*** Seq: 0xA9741C72  Ack: 0x5B61E57E  Win: 0x1FE  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

08/18-11:19:44.747260 52.226.139.185:443 -> 192.168.192.35:49423
TCP TTL:107 TOS:0x0 ID:2171 IpLen:20 DgmLen:211 DF
***AP*** Seq: 0x5B61E57E  Ack: 0xA9741CD7  Win: 0x1F9B  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

08/18-11:19:44.790667 192.168.192.35:49423 -> 52.226.139.185:443
TCP TTL:128 TOS:0x0 ID:14426 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xA9741CD7  Ack: 0x5B61E629  Win: 0x1FE  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Test for 6th Cmd:

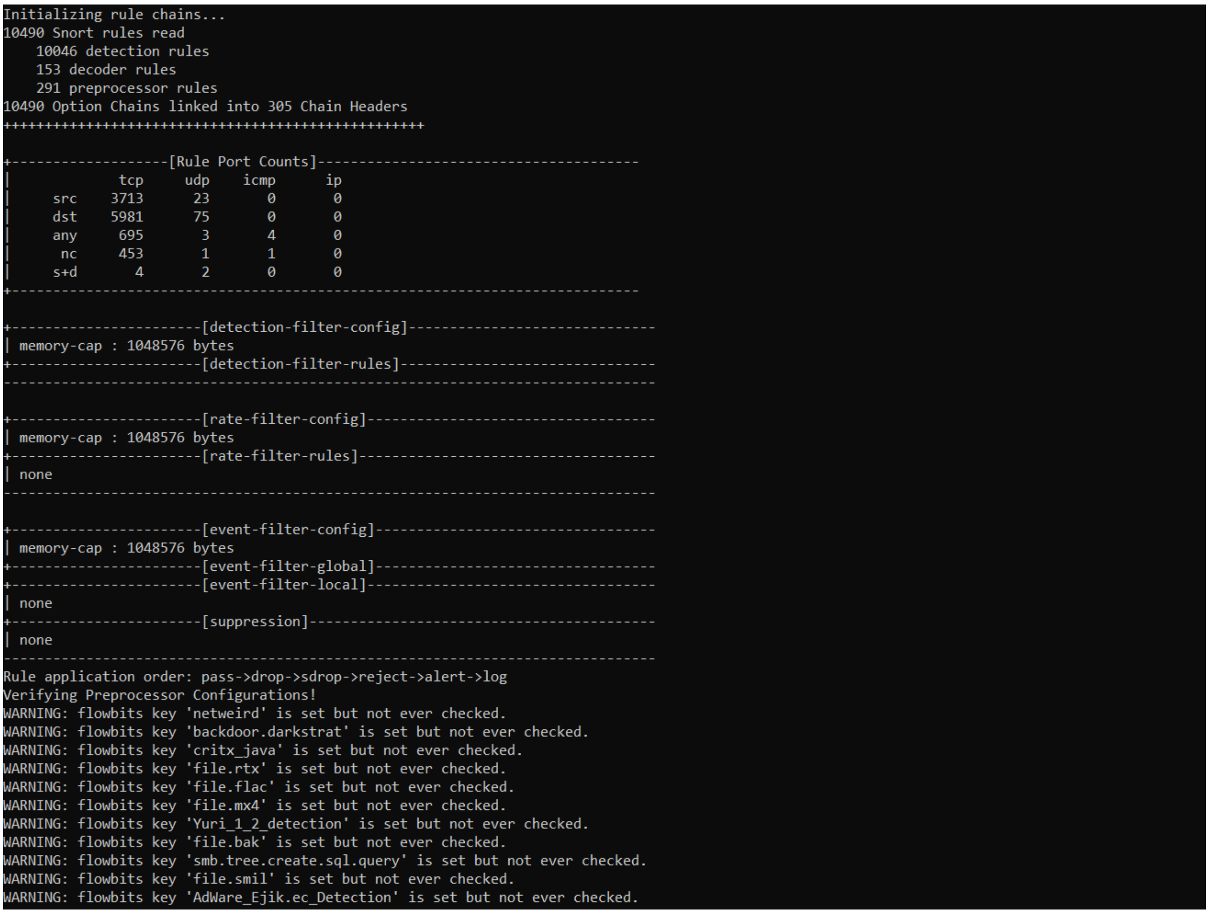
Snort -i 5 -c C:\Snort\etc\snort.conf -A console -vd


Command Prompt - snort -i 5 -c C:\Snort\etc\snort.conf -A console -v

```
Microsoft Windows [Version 10.0.22000.856]
(c) Microsoft Corporation. All rights reserved.

C:\Users\T.MARALIDHAR>cd C:\Snort\bin

C:\Snort\bin>snort -i 5 -c C:\Snort\etc\snort.conf -A console -v
Running in IDS 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 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8
123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 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 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 808
8 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 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:\Snort\lib\snort_dynamicengine\sf_engine.dll... done
Loading all dynamic detection libs from C:\Snort\lib\snort_dynamicrules...
  Finished Loading all dynamic detection libs from C:\Snort\lib\snort_dynamicrules
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
```



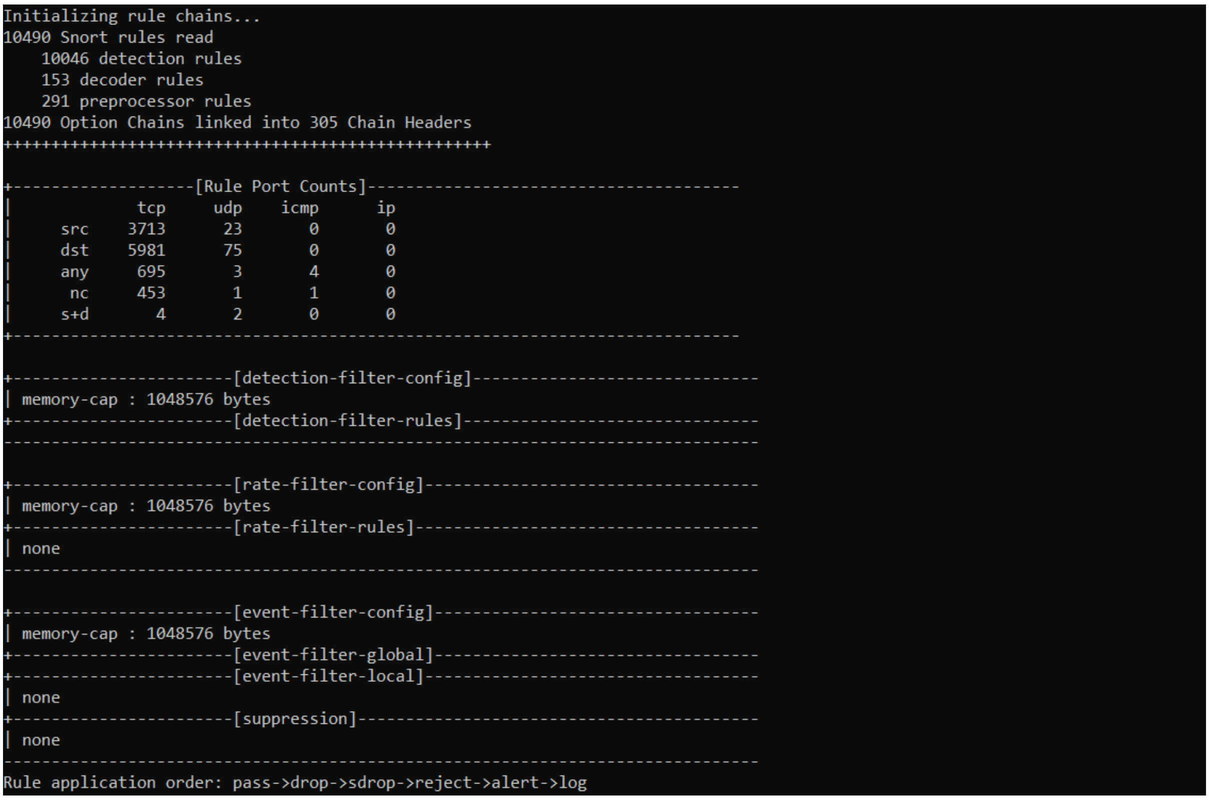
```
        3-Way Handshake Timeout: 180
        Detect Anomalies: YES
    Reassembly Ports:
      21 client (Footprint)
      22 client (Footprint)
      23 client (Footprint)
      25 client (Footprint)
      42 client (Footprint)
      53 client (Footprint)
      79 client (Footprint)
      80 client (Footprint) server (Footprint)
      81 client (Footprint) server (Footprint)
      109 client (Footprint)
      110 client (Footprint)
      111 client (Footprint)
      113 client (Footprint)
      119 client (Footprint)
      135 client (Footprint)
      136 client (Footprint)
      137 client (Footprint)
      139 client (Footprint)
      143 client (Footprint)
      161 client (Footprint)
      additional ports configured but not printed.
Stream UDP Policy config:
    Timeout: 180 seconds
HttpInspect Config:
    GLOBAL CONFIG
      Detect Proxy Usage:       NO
      IIS Unicode Map Filename: C:\Snort\etc\unicode.map
      IIS Unicode Map Codepage: 1252
      Memcap used for logging URI and Hostname: 150994944
      Max Gzip Memory: 838860
      Max Gzip Sessions: 2016
      Gzip Compress Depth: 65535
      Gzip Decompress Depth: 65535
      Normalize Random Nulls in Text: NO
    DEFAULT SERVER CONFIG:
      Server profile: All
      Ports (PAF): 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 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180 8181 8
243 8280 8300 8800 8888 8899 9000 9060 9080 9090 9091 9443 9999 11371 34443 34444 41080 50002 55555
      Server Flow Depth: 0
      Client Flow Depth: 0
      Max Chunk Length: 500000
      Small Chunk Length Evasion: chunk size <= 10, threshold >= 5 times
      Max Header Field Length: 750
      Max Number Header Fields: 100
      Max Number of WhiteSpaces allowed with header folding: 200
      Inspect Pipeline Requests: YES
```



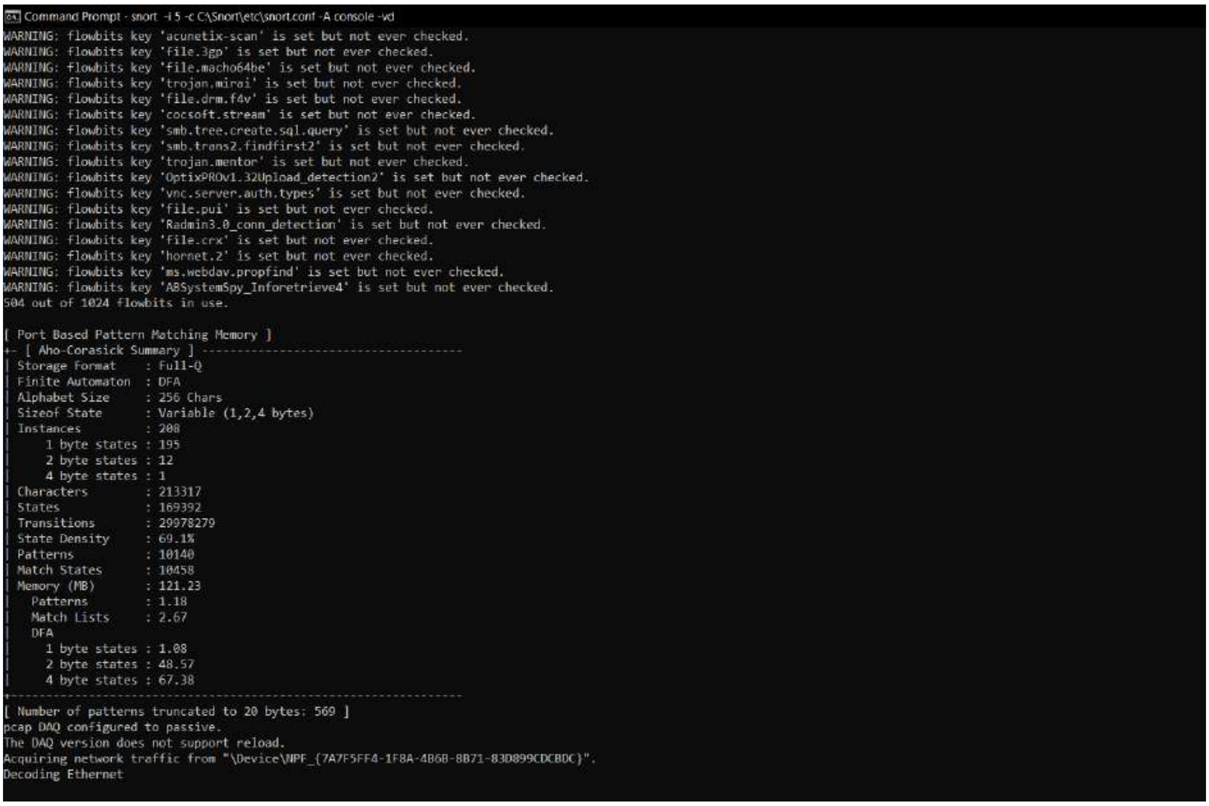
```
Initializing rule chains...
10490 Snort rules read
    10046 detection rules
    153 decoder rules
    291 preprocessor rules
10490 Option Chains linked into 305 Chain Headers
+++++++++++++++++++++++++++++++++++++++++++++++++++

+-------------------[Rule Port Counts]---------------------------------------
|             tcp     udp    icmp      ip
|     src     3713      23       0       0
|     dst     5981      75       0       0
|     any      695       3       4       0
|      nc      453       1       1       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 'netweird' is set but not ever checked.
WARNING: flowbits key 'backdoor.darkstrat' is set but not ever checked.
WARNING: flowbits key 'critx_java' is set but not ever checked.
WARNING: flowbits key 'file.rtx' is set but not ever checked.
WARNING: flowbits key 'file.flac' is set but not ever checked.
WARNING: flowbits key 'file.mx4' is set but not ever checked.
WARNING: flowbits key 'Yuri_1_2_detection' is set but not ever checked.
WARNING: flowbits key 'file.bak' is set but not ever checked.
WARNING: flowbits key 'smb.tree.create.sql.query' is set but not ever checked.
WARNING: flowbits key 'file.smil' is set but not ever checked.
WARNING: flowbits key 'AdWare_Ejik.ec_Detection' is set but not ever checked.
```

Test for 7th Cmd:

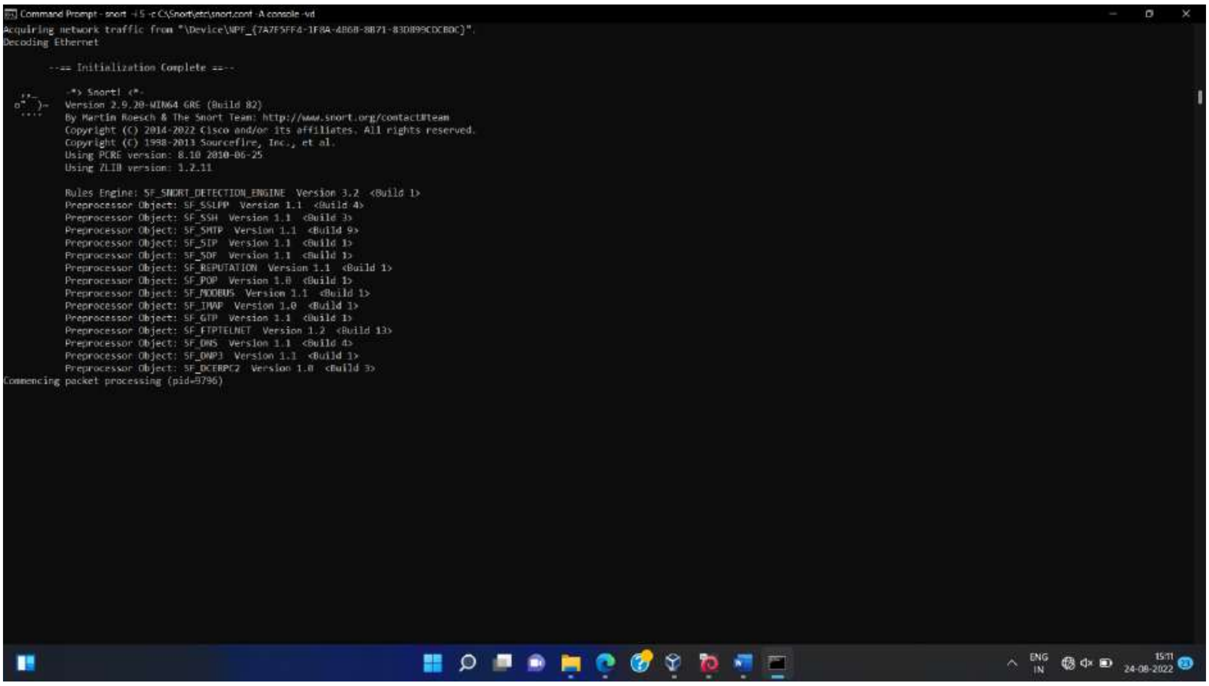
Snort -i 5 -c C:\Snort\etc\snort.conf -A console -v



```
Initializing rule chains...
10490 Snort rules read
    10046 detection rules
    153 decoder rules
    291 preprocessor rules
10490 Option Chains linked into 305 Chain Headers
+++++++++++++++++++++++++++++++++++++++++++++++++++

+-------------------[Rule Port Counts]---------------------------------------
|             tcp     udp    icmp      ip
|     src     3713      23       0       0
|     dst     5981      75       0       0
|     any      695       3       4       0
|      nc      453       1       1       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
```


Command Prompt - snort -i 5 -c C:\Snort\etc\snort.conf -A console -vd

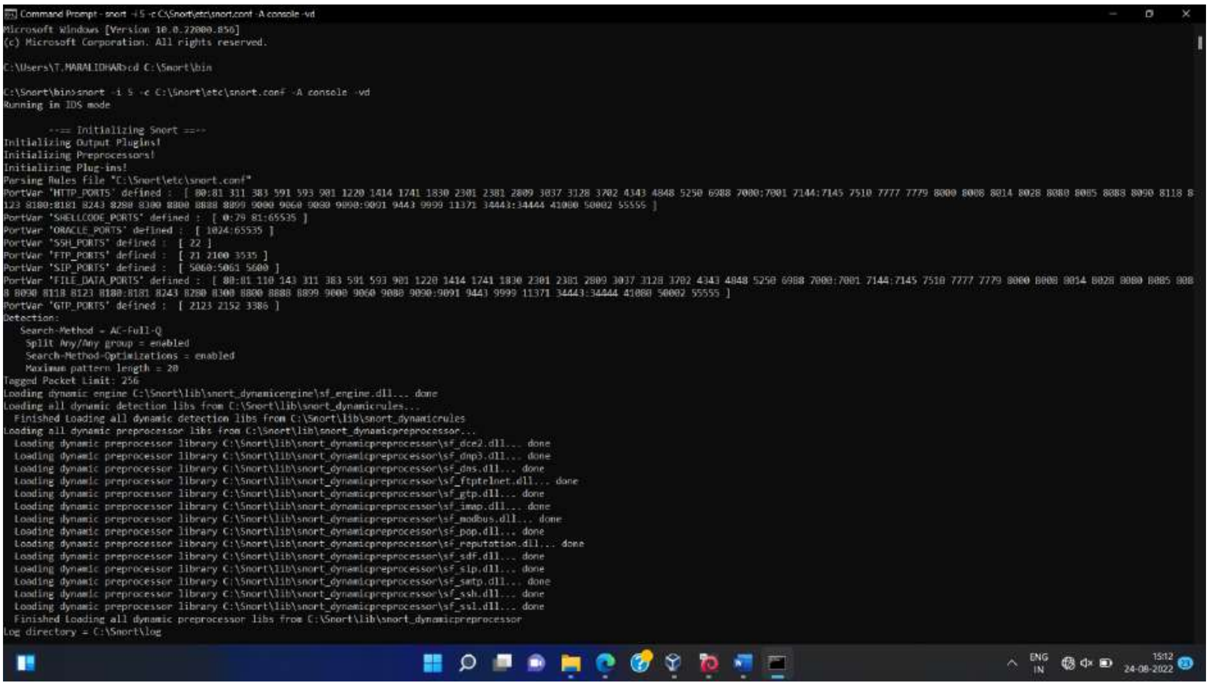
```
WARNING: flowbits key 'acunetix-scan' is set but not ever checked.
WARNING: flowbits key 'file.3gp' is set but not ever checked.
WARNING: flowbits key 'file.macho64be' is set but not ever checked.
WARNING: flowbits key 'trojan.mirai' is set but not ever checked.
WARNING: flowbits key 'file.drm.f4v' is set but not ever checked.
WARNING: flowbits key 'cocsoft.stream' is set but not ever checked.
WARNING: flowbits key 'smb.tree.create.sql.query' is set but not ever checked.
WARNING: flowbits key 'smb.trans2.findfirst2' is set but not ever checked.
WARNING: flowbits key 'trojan.mentor' is set but not ever checked.
WARNING: flowbits key 'OptixPROv1.32Upload_detection2' is set but not ever checked.
WARNING: flowbits key 'vnc.server.auth.types' is set but not ever checked.
WARNING: flowbits key 'file.pui' is set but not ever checked.
WARNING: flowbits key 'Radmin3.0_conn_detection' is set but not ever checked.
WARNING: flowbits key 'file.crx' is set but not ever checked.
WARNING: flowbits key 'hornet.2' is set but not ever checked.
WARNING: flowbits key 'ms.webdav.propfind' is set but not ever checked.
WARNING: flowbits key 'ABSystemSpy_Inforetrieve4' is set but not ever checked.
504 out of 1024 flowbits in use.

[ Port Based Pattern Matching Memory ]
+- [ Aho-Corasick Summary ] -------------------------------------
| Storage Format    : Full-Q
| Finite Automaton  : DFA
| Alphabet Size     : 256 Chars
| Sizeof State      : Variable (1,2,4 bytes)
| Instances         : 208
|     1 byte states : 195
|     2 byte states : 12
|     4 byte states : 1
| Characters        : 213317
| States            : 169392
| Transitions       : 29978279
| State Density     : 69.1%
| Patterns          : 10140
| Match States      : 10458
| Memory (MB)       : 121.23
|   Patterns        : 1.18
|   Match Lists     : 2.67
|   DFA
|     1 byte states : 1.08
|     2 byte states : 48.57
|     4 byte states : 67.38
+----------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 569 ]
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{7A7F5FF4-1F8A-4B6B-8B71-83D899CDCBDC}".
Decoding Ethernet
```


Command Prompt - snort -i 5 -c C:\Snort\etc\snort.conf -A console -vd
ENG
IN
15:11
24-08-2022

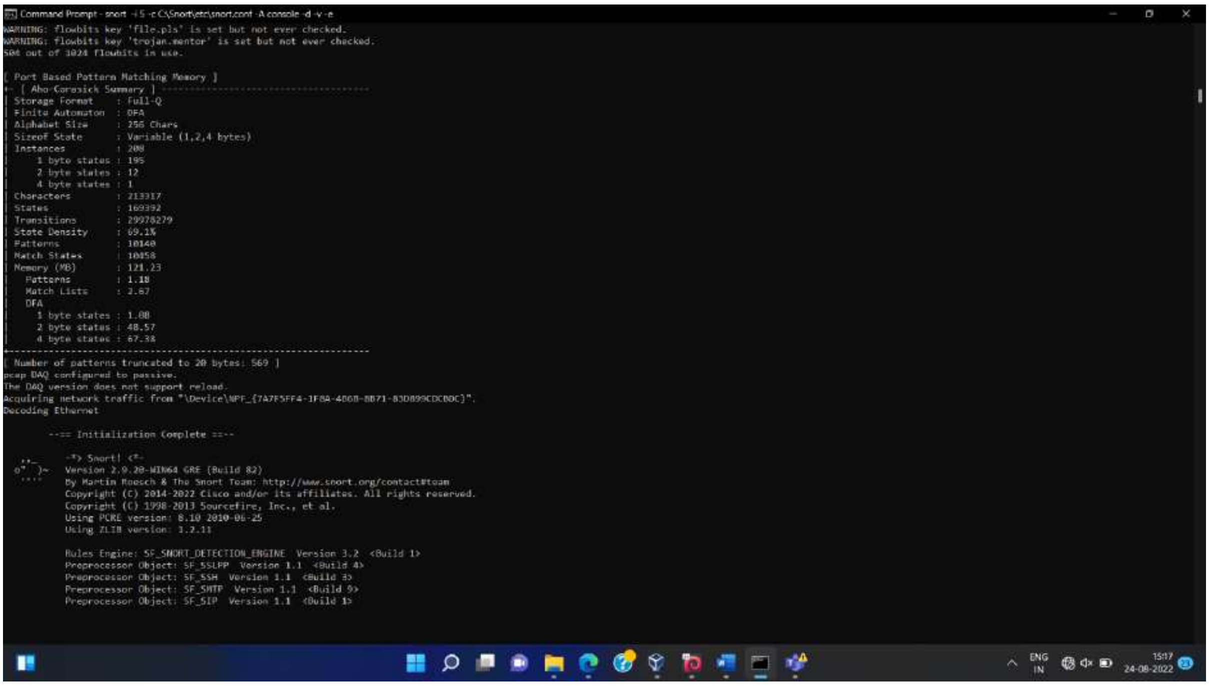
```
Acquiring network traffic from "\Device\NPF_{7A7F5FF4-1F8A-4868-8B71-83D899CDCBDC}".
Decoding Ethernet

        --== 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>
Commencing packet processing (pid=9796)
```

Test for 8th Cmd:

Snort -i 5 -c C:\Snort\etc\snort.conf -A console -vd

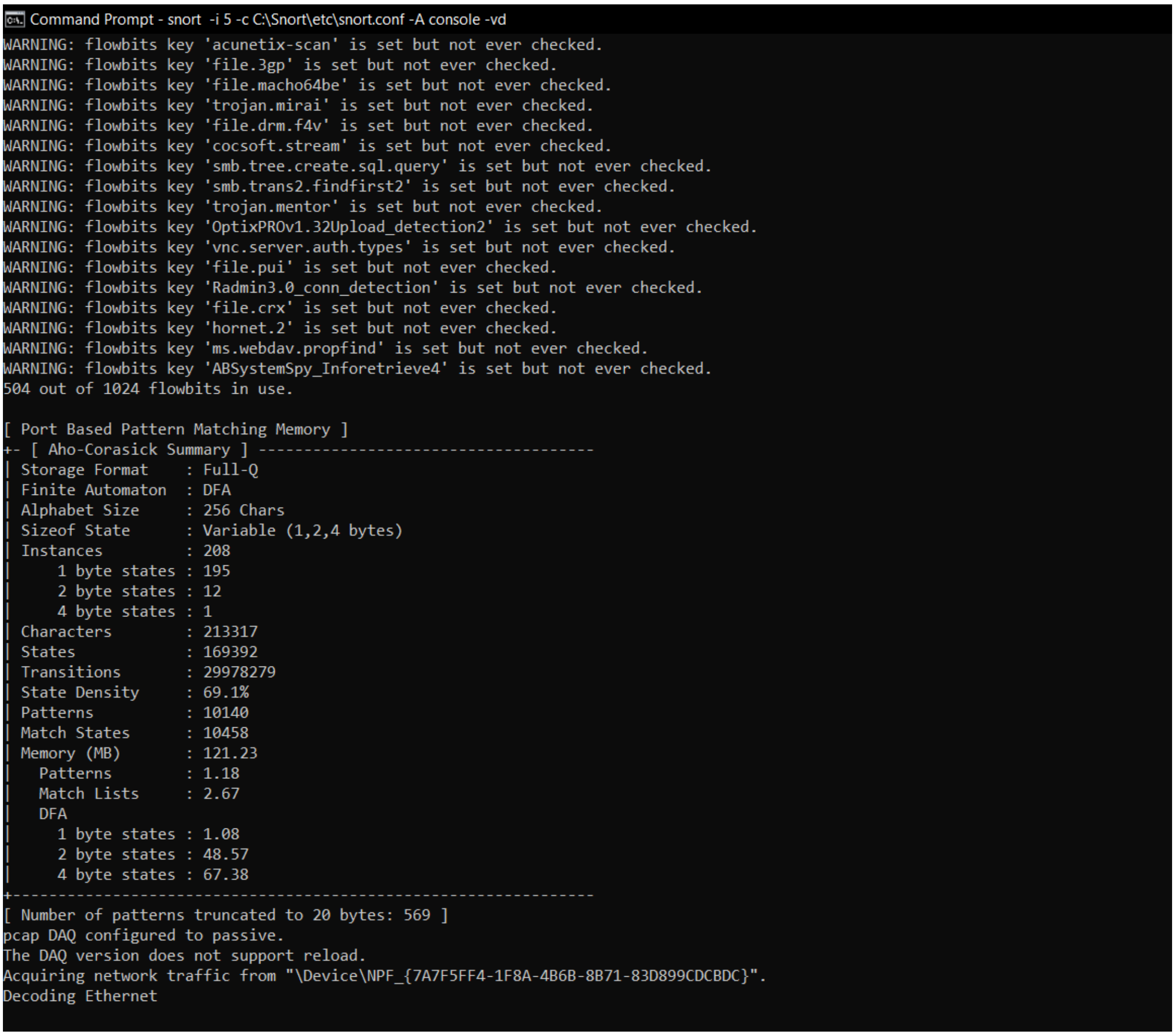

Command Prompt - snort -i 5 -c C:\Snort\etc\snort.conf -A console -vd
ENG
IN
15:12
24-08-2022

```
Microsoft Windows [Version 10.0.22000.856]
(c) Microsoft Corporation. All rights reserved.

C:\Users\T.MARALIDHAR>cd C:\Snort\bin

C:\Snort\bin>snort -i 5 -c C:\Snort\etc\snort.conf -A console -vd
Running in IDS 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 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8
123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 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 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 808
8 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 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:\Snort\lib\snort_dynamicengine\sf_engine.dll... done
Loading all dynamic detection libs from C:\Snort\lib\snort_dynamicrules...
  Finished Loading all dynamic detection libs from C:\Snort\lib\snort_dynamicrules
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
```



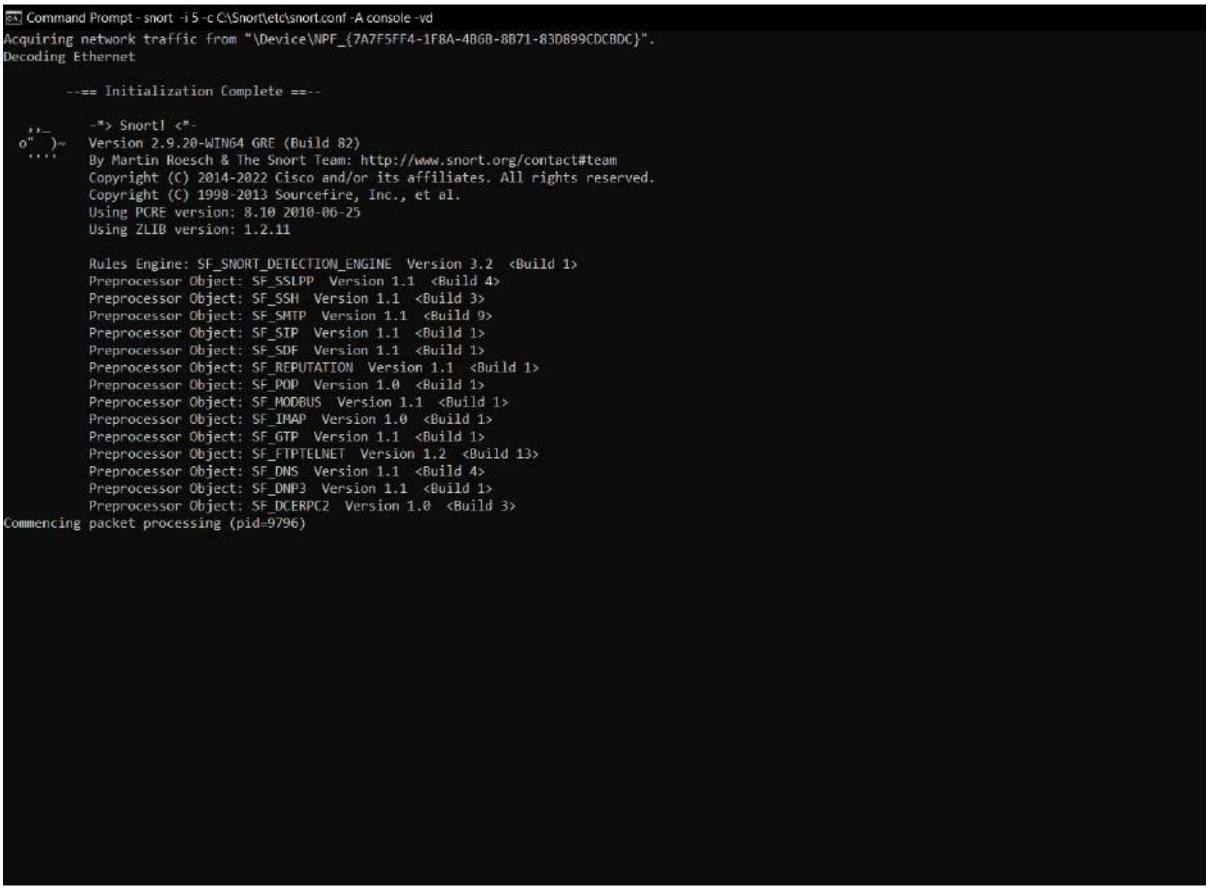
Command Prompt - snort -i 5 -c C:\Snort\etc\snort.conf -A console -d -v -e

```
WARNING: flowbits key 'file.pls' is set but not ever checked.
WARNING: flowbits key 'trojan.mentor' is set but not ever checked.
504 out of 1024 flowbits in use.

[ Port Based Pattern Matching Memory ]
+- [ Aho-Corasick Summary ] -------------------------------------
| Storage Format    : Full-Q
| Finite Automaton  : DFA
| Alphabet Size     : 256 Chars
| Sizeof State      : Variable (1,2,4 bytes)
| Instances         : 208
|     1 byte states : 195
|     2 byte states : 12
|     4 byte states : 1
| Characters        : 213317
| States            : 169392
| Transitions       : 29978279
| State Density     : 69.1%
| Patterns          : 10140
| Match States      : 10458
| Memory (MB)       : 121.23
|   Patterns        : 1.18
|   Match Lists     : 2.67
|   DFA
|     1 byte states : 1.08
|     2 byte states : 48.57
|     4 byte states : 67.38
+----------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 569 ]
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{7A7F5FF4-1F8A-4B6B-8B71-83D899CDCBDC}".
Decoding Ethernet

        --== 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>
```



Command Prompt - snort -i 5 -c C:\Snort\etc\snort.conf -A console -vd

```
WARNING: flowbits key 'acunetix-scan' is set but not ever checked.
WARNING: flowbits key 'file.3gp' is set but not ever checked.
WARNING: flowbits key 'file.macho64be' is set but not ever checked.
WARNING: flowbits key 'trojan.mirai' is set but not ever checked.
WARNING: flowbits key 'file.drm.f4v' is set but not ever checked.
WARNING: flowbits key 'cocsoft.stream' is set but not ever checked.
WARNING: flowbits key 'smb.tree.create.sql.query' is set but not ever checked.
WARNING: flowbits key 'smb.trans2.findfirst2' is set but not ever checked.
WARNING: flowbits key 'trojan.mentor' is set but not ever checked.
WARNING: flowbits key 'OptixPROv1.32Upload_detection2' is set but not ever checked.
WARNING: flowbits key 'vnc.server.auth.types' is set but not ever checked.
WARNING: flowbits key 'file.pui' is set but not ever checked.
WARNING: flowbits key 'Radmin3.0_conn_detection' is set but not ever checked.
WARNING: flowbits key 'file.crx' is set but not ever checked.
WARNING: flowbits key 'hornet.2' is set but not ever checked.
WARNING: flowbits key 'ms.webdav.propfind' is set but not ever checked.
WARNING: flowbits key 'ABSystemSpy_Inforetrieve4' is set but not ever checked.
504 out of 1024 flowbits in use.

[ Port Based Pattern Matching Memory ]
+- [ Aho-Corasick Summary ] -------------------------------------
| Storage Format    : Full-Q
| Finite Automaton  : DFA
| Alphabet Size     : 256 Chars
| Sizeof State      : Variable (1,2,4 bytes)
| Instances         : 208
|     1 byte states : 195
|     2 byte states : 12
|     4 byte states : 1
| Characters        : 213317
| States            : 169392
| Transitions       : 29978279
| State Density     : 69.1%
| Patterns          : 10140
| Match States      : 10458
| Memory (MB)       : 121.23
|   Patterns        : 1.18
|   Match Lists     : 2.67
|   DFA
|     1 byte states : 1.08
|     2 byte states : 48.57
|     4 byte states : 67.38
+----------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 569 ]
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{7A7F5FF4-1F8A-4B6B-8B71-83D899CDCBDC}".
Decoding Ethernet
```



Command Prompt - snort -i 5 -c C:\Snort\etc\snort.conf -A console -vd

```
Acquiring network traffic from "\Device\NPF_{7A7F5FF4-1F8A-4B6B-8B71-83D899CDCBDC}".
Decoding Ethernet

        --== 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>
Commencing packet processing (pid=9796)
```