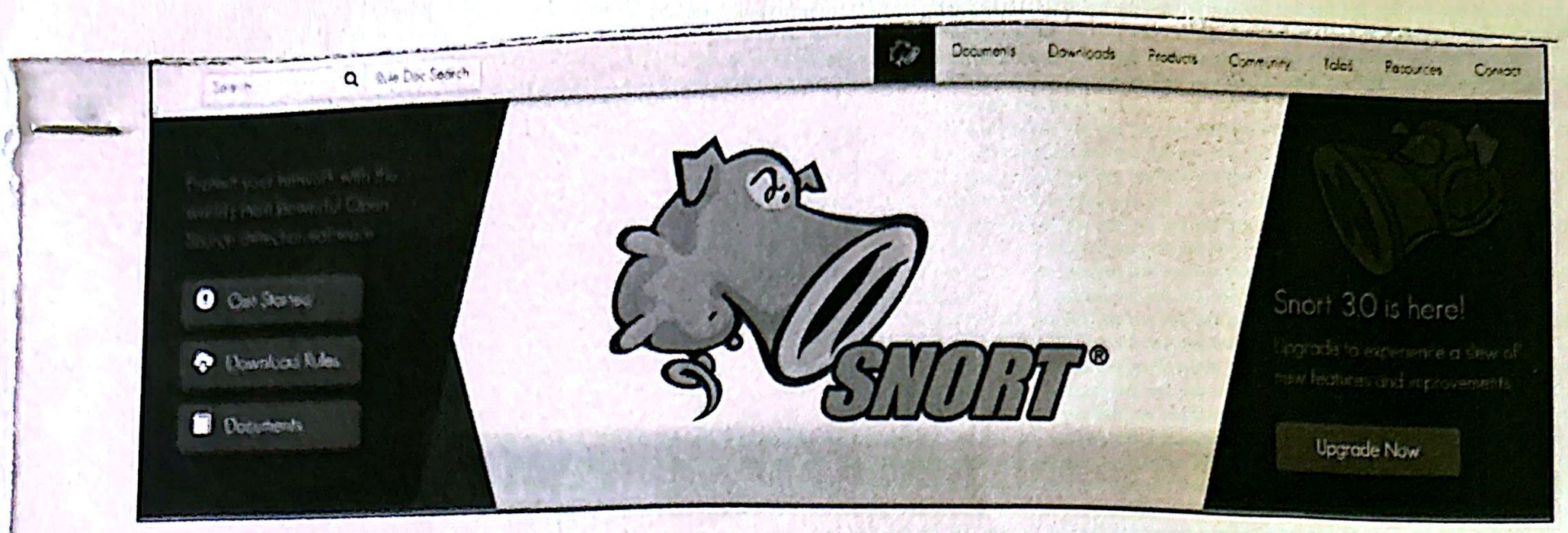
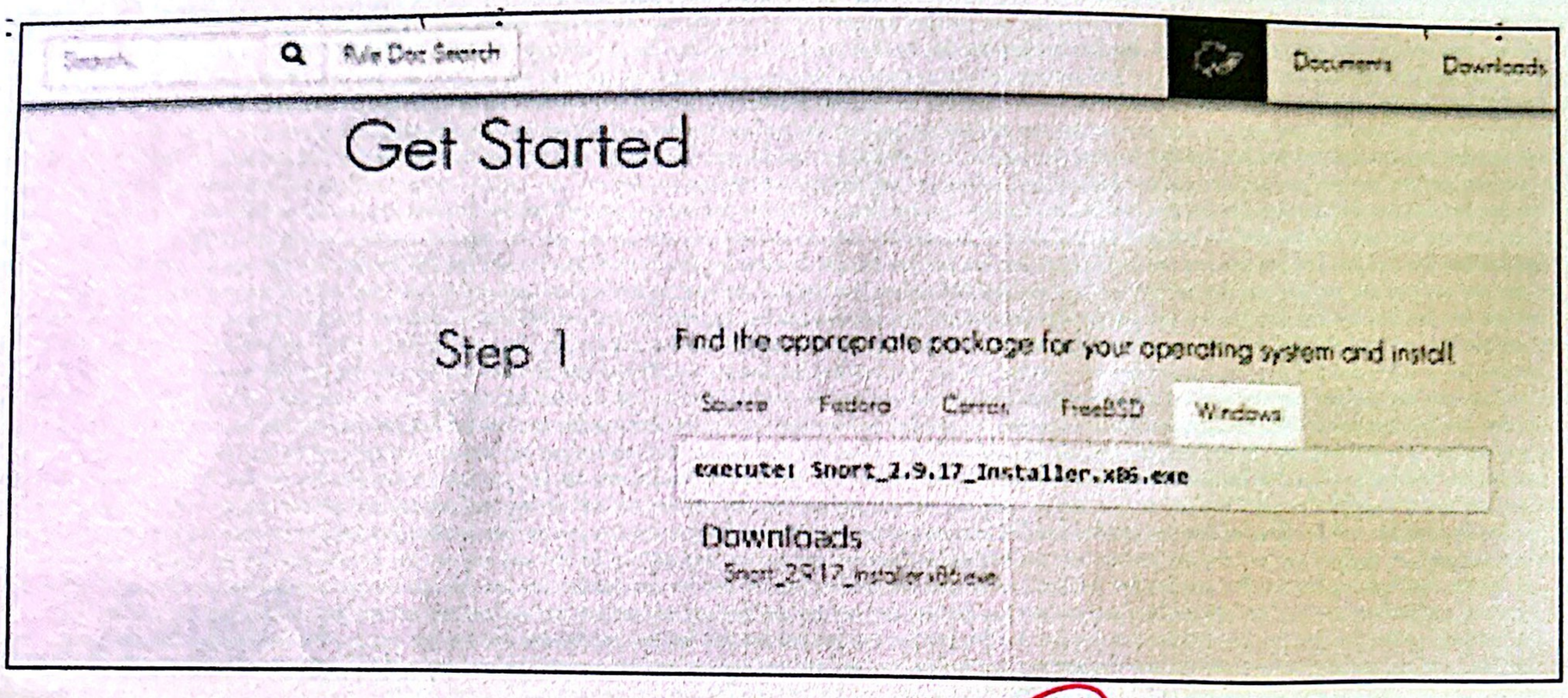
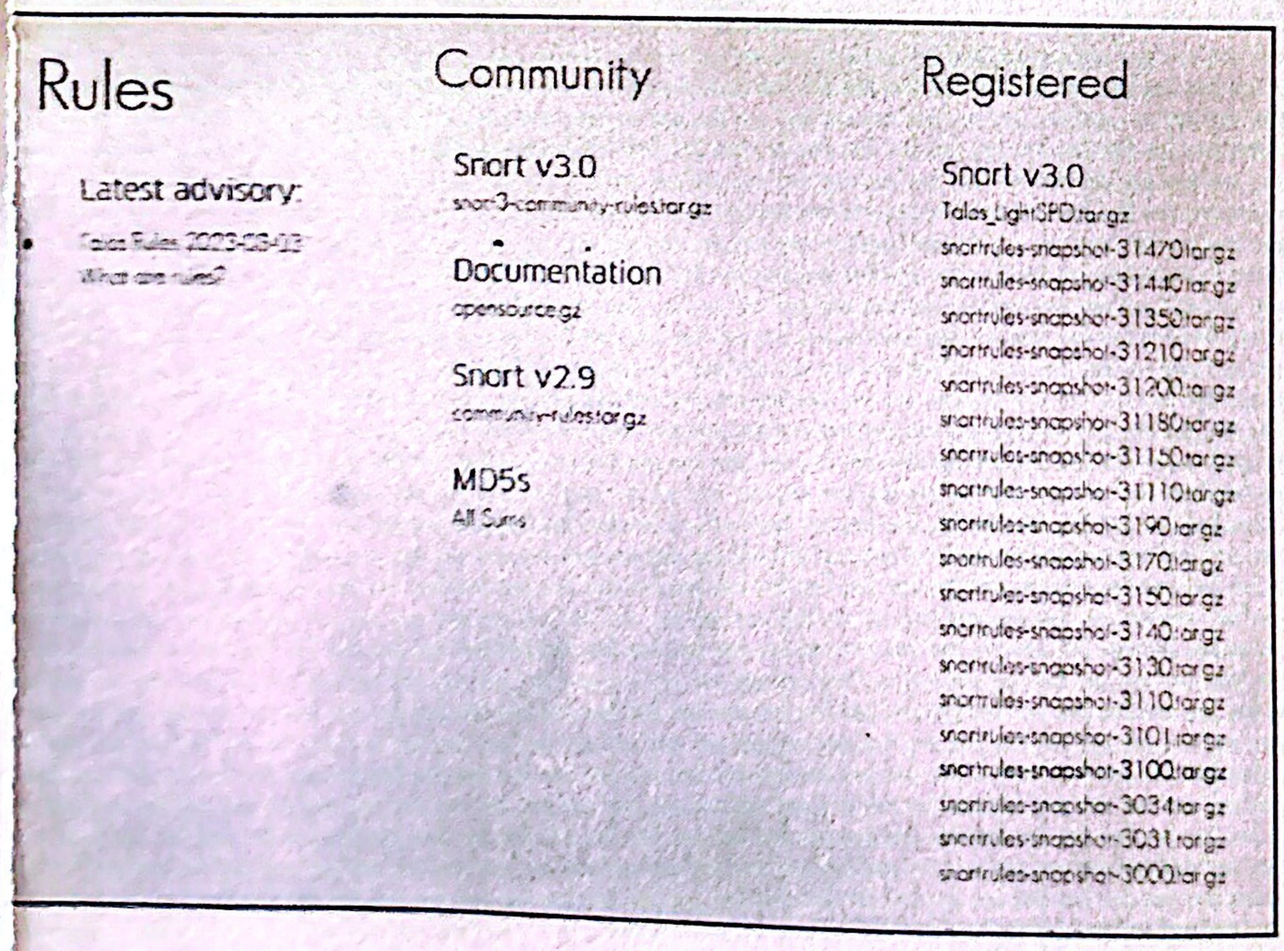


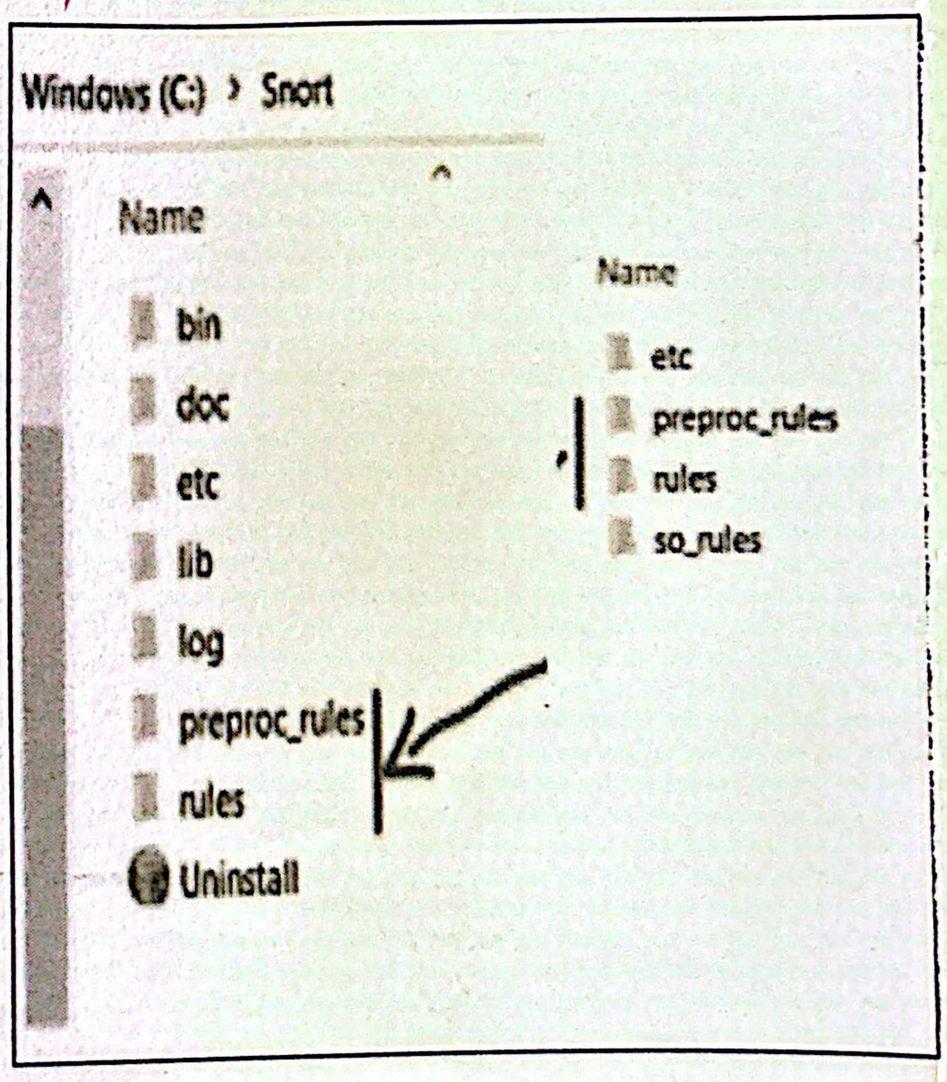
1.1. Snort Home Page



1.2. Installing .exe file for Snort



1.3. Installing Rules Set



1.4. Copying folders to Snort folder

Date : 7/8/23

Installing Snort And Npcap for Windows

Page No. : 1

Expt. No. : 1

Aim

To Install Snort and NPCAP For Windows

Objective

To Moniter the Traffic and Secure the database in windows

Procedure

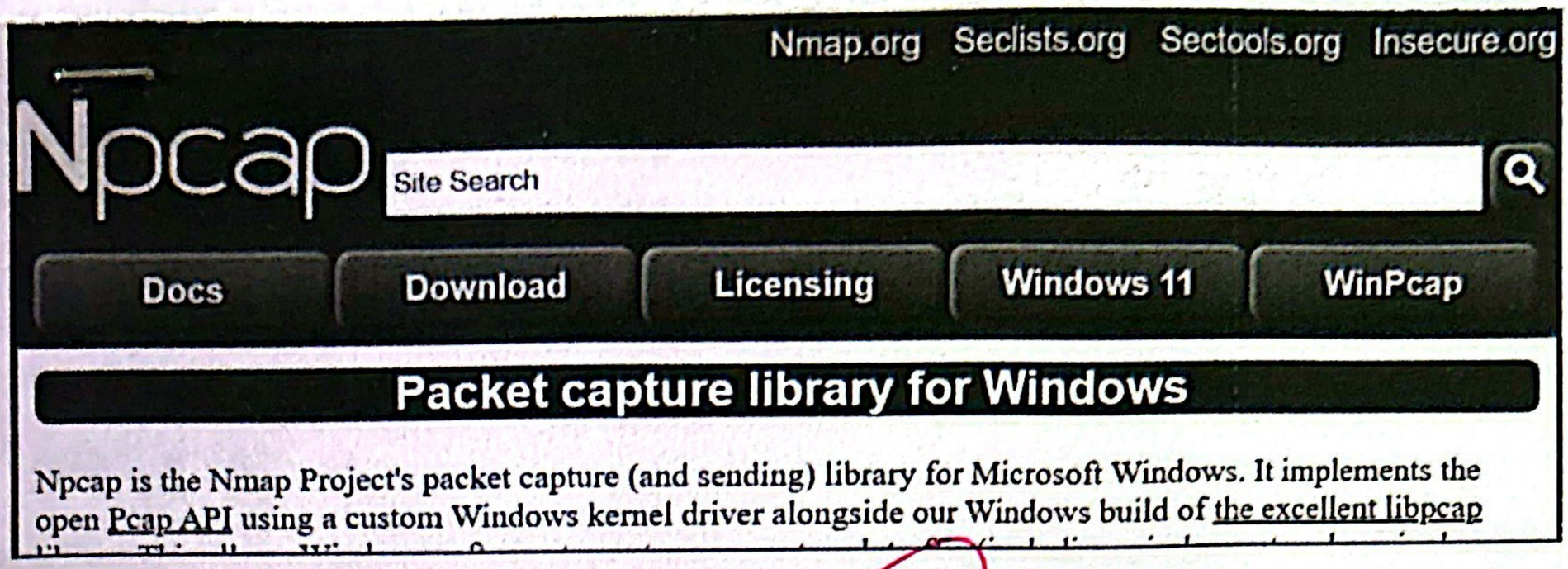
SNORT:-

- Visit Snort website www.snort.org
- Click on get started, redirect to download page
- Select OS as windows, x64
- Click on Snort_2.9.17_installer, download exe file

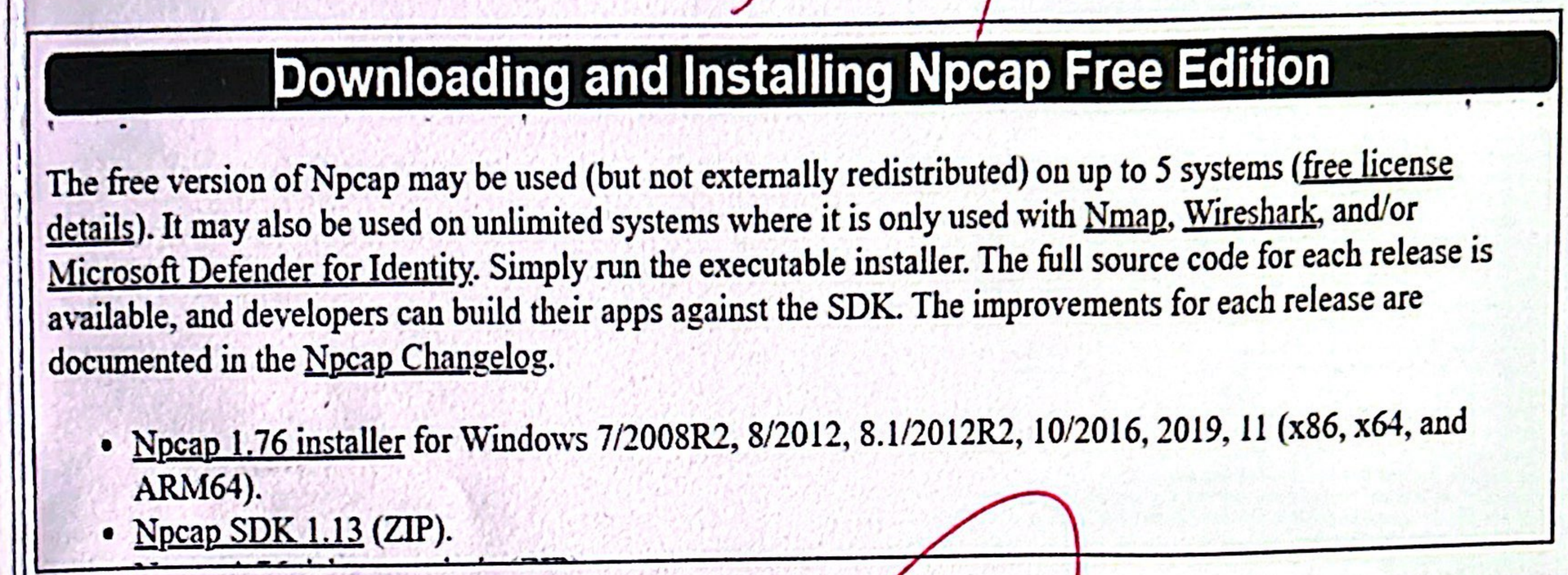
- Go to home page
- Create and login the account for snort rules
- Download the rules "Snortrules-snapshot-29170.tar.gz"
- Install the files, accept all default option
- extract rules zip folder
- Copy the rules & preproc-rules from extracted zip folder & paste in snort folder
- Go to C drive, folder with name snort appears, go to rules and replace the files with copied ones

NPCAP → PTO

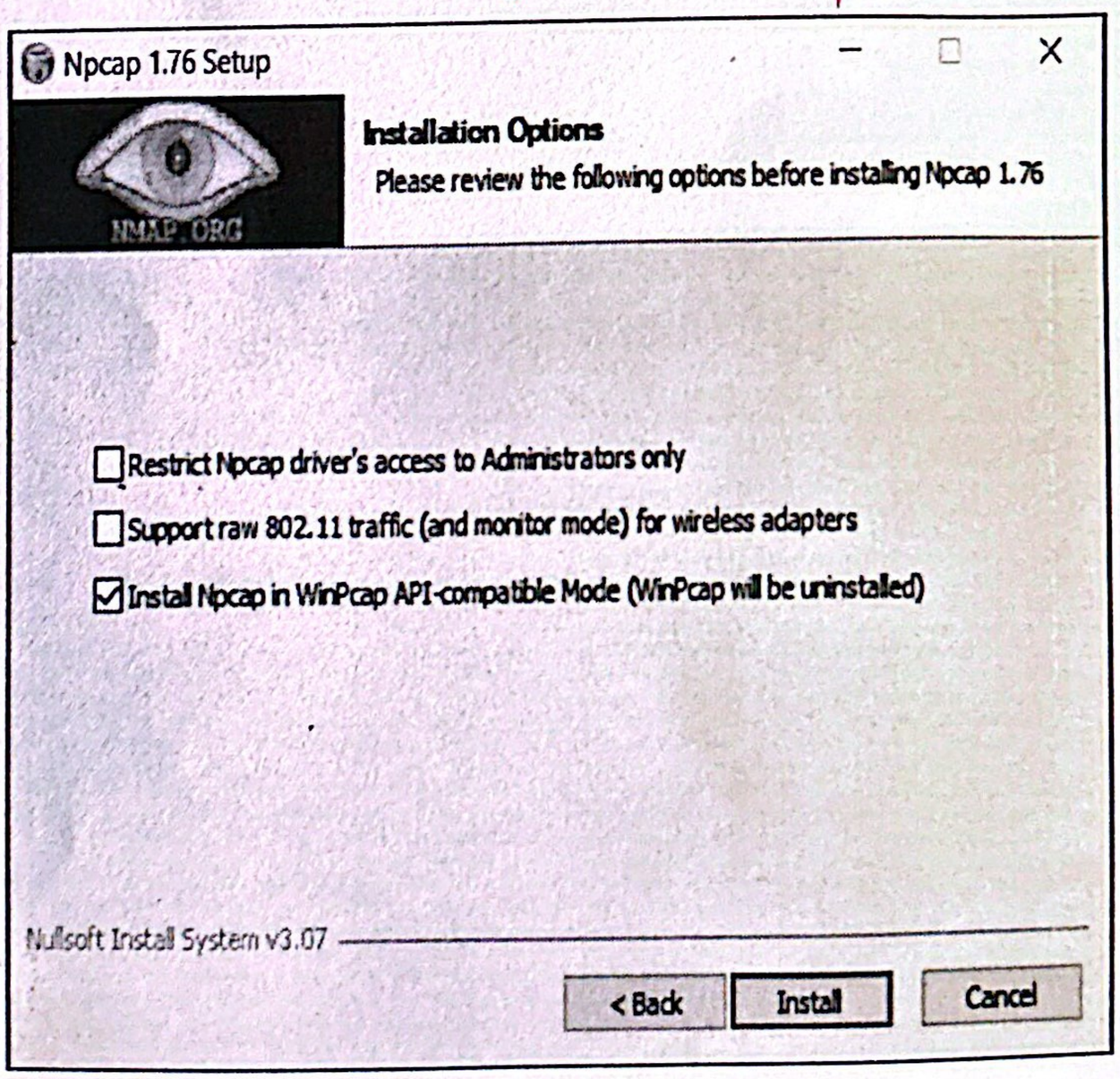
Teacher's Signature:



1.5. Npcap Home Page



1.6. Install Npcap 1.76 installer from Downloads



1.7. Installing Npcap

Date :

Page No. : 2

Expt. No. : 1

NPCAP :-

Goto the below URL

nmap.org/npcap & download npcap

- Downloads section
- Npcap 1.76 for windows, download this exe
- Install the exe & grant all permissions
- Click on install to fix the npcap for windows

Result

Installation of snort & npcap is sorted

Teacher's Signature:

```
40  ##################################################
41  # Step #1: Set the network variables.  For more information,
42  ##################################################
43
44  # Setup the network addresses you are protecting
45  ipvar HOME_NET 192.[redacted]
46
```

2.1. Setting the network address

```
46
47  # Set up the external network addresses. Leave as "any" in most situations
48  ipvar EXTERNAL_NET !$HOME_NET
49
```

2.2. Setting the external network address

```
100
101 # Path to your rules files (this can be a relative path)
102 # Note for Windows users:  You are advised to make this an absolute path,
103 # such as:  c:\snort\rules
104 var RULE_PATH c:\Snort\rules
105 #var SO_RULE_PATH ../so_rules
106 var PREPROC_RULE_PATH c:\Snort\preproc_rules
107
```

2.3. Setting the correct paths

```
108 # If you are using reputation preprocessor set these
109 # Currently there is a bug with relative paths, they are relative to where snort is
110 # not relative to snort.conf like the above variables
111 # This is completely inconsistent with how other vars work, BUG 89986
112 # Set the absolute path appropriately
113 var WHITE_LIST_PATH c:\Snort\rules
114 var BLACK_LIST_PATH c:\Snort\rules
115
```

2.4. Modifying the path for white_list and black_list

```
183
184 # Configure default log directory for snort to log to.
185 #
186 config logdir: c:\Snort\log
187
```

2.5. Configuring the log directory

```
245
246 # path to dynamic preprocessor libraries
247 dynamicpreprocessor directory c:\Snort\lib\snort_dynamicpreprocessor
248
249 # path to base preprocessor engine
250 dynamicengine c:\Snort\lib\snort_dynamicengine\sf_engine.dll
251
252 # path to dynamic rules libraries
253 # dynamicdetection directory /usr/local/lib/snort_dynamicrules
254
```

2.6. Set the paths for dynamic preprocessor, dynamic engine and dynamic detection

Date : 14-8-23

Snorting through logs and Alerts

Page No. : 3

Expt. No. : 2

Aim

To modify the configuration file and snorting through logs and alerts

Objective

To maintain real-time traffic, logging analysis on networks and detecting types of cyber attack based on the rules.

Procedure

- Go to the folder etc in the path C:\snort\etc.
- Open the snort-conf file to edit/modify it.
- line number 45, change last part from any to network default gateway in CIDR notation
- line 48, replace "~~Any~~ ANY" with "! $HOME_NET" to limit everything not in home network
- line 104 edit the path of the rules and insert correct path i.e "C:\Snort\rules".
- Comment line 105
- Edit path in 106 to "C:\Snort\preproc-rules".
- Edit path of whitelist & blacklist (line 113 & 114) add C:\Snort\rules.
- line 186, uncomment the line by adding path as C:\snort\log
- Add the path C:\Snort\lib\Snort_dynamicpreprocessor C:\snort\lib\snort_dynamicengine\sf_engine.dll"

247 & 250 line

Uncomment it by removing the hashtag before

- 253rd line, add hashtag and comment it at beginning of the line
- Comment 265-269 and 335
- Remove comment (#) from line 418
- Open (Blacklist.rules) file

Line 19 change to whitelist.rules

Teacher's Signature:

```
262
263 # Inline packet normalization. For more information,
264 # Does nothing in IDS mode
265 #preprocessor normalize_ip4
266 #preprocessor normalize_tcp: ips ecn stream
267 #preprocessor normalize_icmp4
268 #preprocessor normalize_ip6
269 #preprocessor normalize_icmp6
270
```

2.7. Commenting the unnecessary lines

```
333
334 # Back Orifice detection.
335 #preprocessor bo
336
```

2.8. Commenting the line

```
416
417 # Portscan detection.  For more information, see README.sfportscan
418  preprocessor sfportscan: proto  { all } memcap { 10000000 } sense_level { low
419
```

2.9. Removing the hashtag

```
# Copyright 2001-2021 Sourcefire, Inc. All Rights Rese
#
# This file contains (i) proprietary rules that were c
# Sourcefire, Inc. (the "VRT Certified Rules") that ar
# Certified Rules License Agreement (v 2.0), and (ii)
# Sourcefire and other third parties (the "GPL Rules")
# GNU General Public License (GPL), v2.
#
# The VRT Certified Rules are owned by Sourcefire, Inc
# by Sourcefire and other third parties. The GPL Rules
# owned by Sourcefire, Inc., and the GPL Rules not cre
# their respective creators. Please see http://www.snc
# list of third party owners and their respective copy
#
# In order to determine what rules are VRT Certified R
# to the VRT Certified Rules License Agreement (v2.0).
#
#------------------
# BLACKLIST RULES
#------------------
```

```
# Copyright 2001-2021 Sourcefire, Inc. All Right
#
# This file contains (i) proprietary rules that
# Sourcefire, Inc. (the "VRT Certified Rules") t
# Certified Rules License Agreement (v 2.0), and
# Sourcefire and other third parties (the "GPL R
# GNU General Public License (GPL), v2.
#
# The VRT Certified Rules are owned by Sourcefir
# by Sourcefire and other third parties. The GPL
# owned by Sourcefire, Inc., and the GPL Rules n
# their respective creators. Please see http://w
# list of third party owners and their respectiv
#
# In order to determine what rules are VRT Certi
# to the VRT Certified Rules License Agreement (
#
#------------------
# WHITELIST RULES
#------------------
```

2.10. Change the Black_list to white_list in the files and save it.

Date :

Page No. : 4
Expt. No. : 2

- Save this file as whitelist.rules in the same path which we had blacklist files
- In this config file, goto line 511 512 change path of whitelist & blacklist Saved in C:\snort\rules path
Change forward slash to backand similarly 546-651
- To activate it, uncomment 659-661
Save all changes made in config file

→ Test if all config files are working ←
→ Open CMD in admin mode
→ Check path, set it to C:\snort\bin by changing directory
→ Snort -v is for version
→ Snort -w is to check list of interfaces we have.
To know the interface that connects, type ipconfig & run in seperate cmd

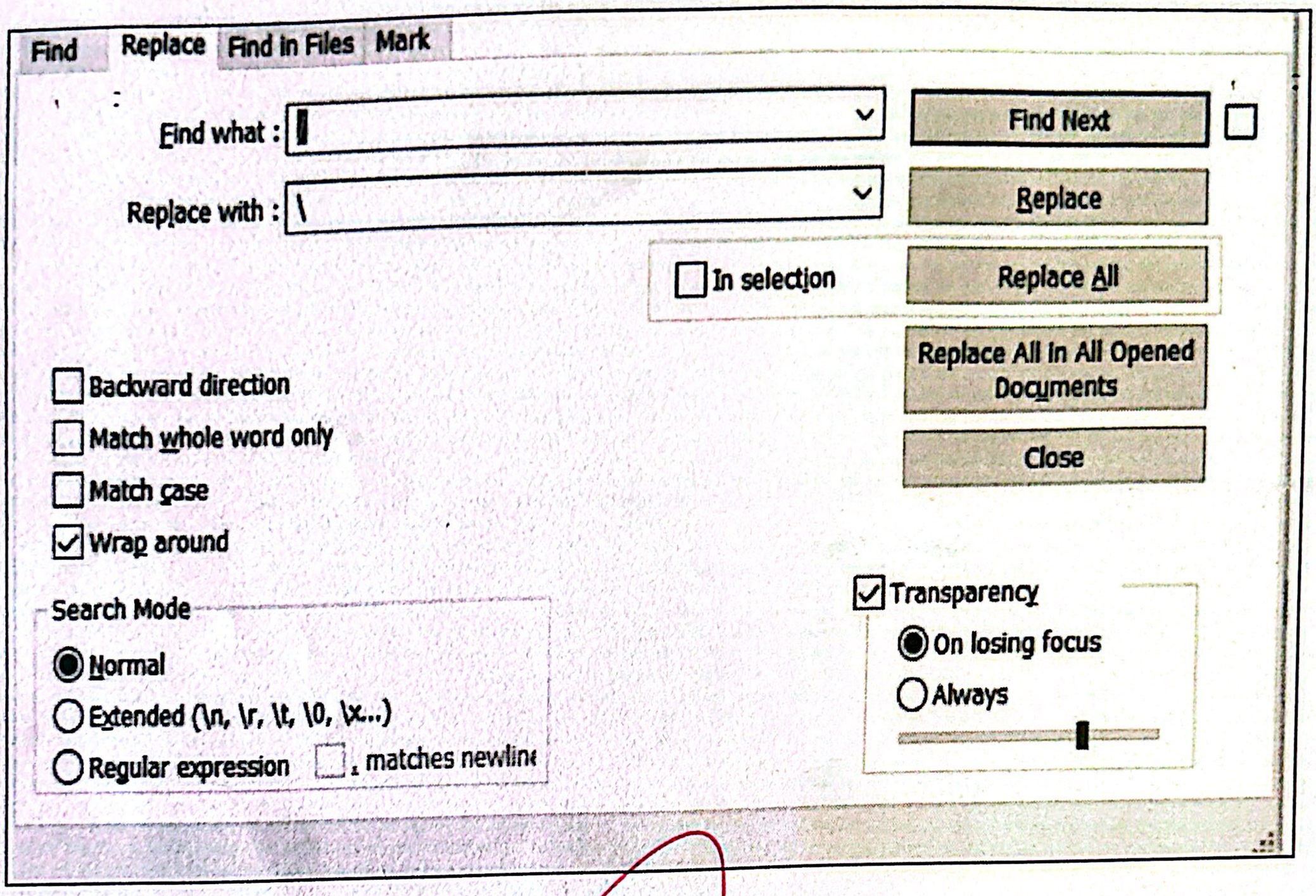
→ Snort -i 3 -c c:\snort\etc\snort.conf -T".
I → interface C → tells where snort to run for file
T → Test

If everything is successful, it will show successfully validated Hence Configuration is OK

Teacher's Signature:

```
# Reputation preprocessor ...                    ... memcap,reputation
preprocessor reputation: \
    memcap 500, \
    priority whitelist, \
    nested_ip inner, \
    whitelist $WHITE_LIST_PATH\whitelist.rules, \
    blacklist $BLACK_LIST_PATH\blacklist.rules
```

2.11. Change the paths in the configuration file.



2.12. Replacing the / with \

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

2.13. Customizing the preprocessor and decoder alerts for more information.

Date :

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

        -*> Snort! <*-
o"  )~  Version 2.9.17-WIN64 GRE (Build 199)
        By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
        Copyright (C) 2014-2020 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
```

2.14. Checking the version of Snort

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

        -*> Snort! <*-
o"  )~  Version 2.9.17-WIN64 GRE (Build 199)
        By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
        Copyright (C) 2014-2020 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_{6A42E39A-03CF-4D19-9ED9-CE8E81898675}
     WAN Miniport (Network Monitor)
    2   00:00:00:00:00:00       disabled        \Device\NPF_{B4048A5E-C869-4D95-BA1E-2C641A452447}
     WAN Miniport (IPv6)
    3   00:00:00:00:00:00       disabled        \Device\NPF_{901D8FD5-E5DC-4E1E-8377-4573491CD8EB}
     WAN Miniport (IP)
    4   00:50:56:C0:00:08       192.168.115.1   \Device\NPF_{F7448E8F-984F-47BA-AFA4-DD86BE0ECE95}
     VMware Virtual Ethernet Adapter for VMnet8
    5   00:50:56:C0:00:01       192.168.234.1   \Device\NPF_{561BB23D-1DFB-4013-9001-5CDC8E5B83C7}
     VMware Virtual Ethernet Adapter for VMnet1
    6   C8:5A:CF:06:68:19       192.168.72.254  \Device\NPF_{520CEC20-3BE8-41A9-9288-541146865F48}
     Intel(R) Ethernet Connection (11) I219-LM
    7   00:00:00:00:00:00       0000:0000:0000:0000:0000:0000:0000:0000 \Device\NPF_Loopback    Ada
pter for loopback traffic capture
```

2.15. Checking the list of interfaces

```
C:\Snort\bin>snort -i 4 -c C:\Snort\etc\snort.conf -T
Running in Test mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "C:\Snort\etc\snort.conf"
```

2.16. Testing the modified configuration file

2.17. Result of testing the configuration file

Result Thus snorting is done through logs & alerts by modifying the configuration file successfully

Teacher's Signature:

Date :

2.14 to 2.16

OPEN ↑

```
      --== Initialization Complete ==--

  ,,_     -*> Snort! <*-
 o"  )~   Version 2.9.17-WIN64 GRE (Build 199)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2020 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 3.1  <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>

Snort successfully validated the configuration!
Snort exiting
```

2.17. Result of testing the configuration file

Result Thus snorting is done through logs & alerts by modifying the configuration file successfully

Teacher's Signature: