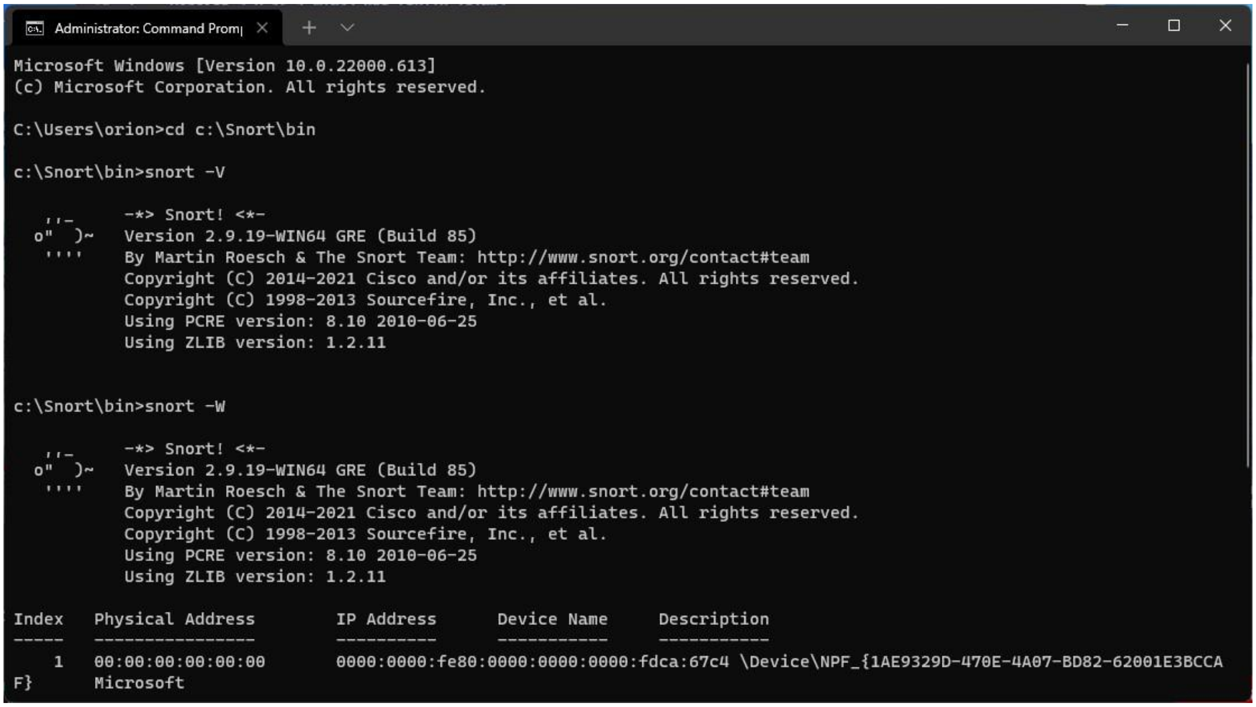
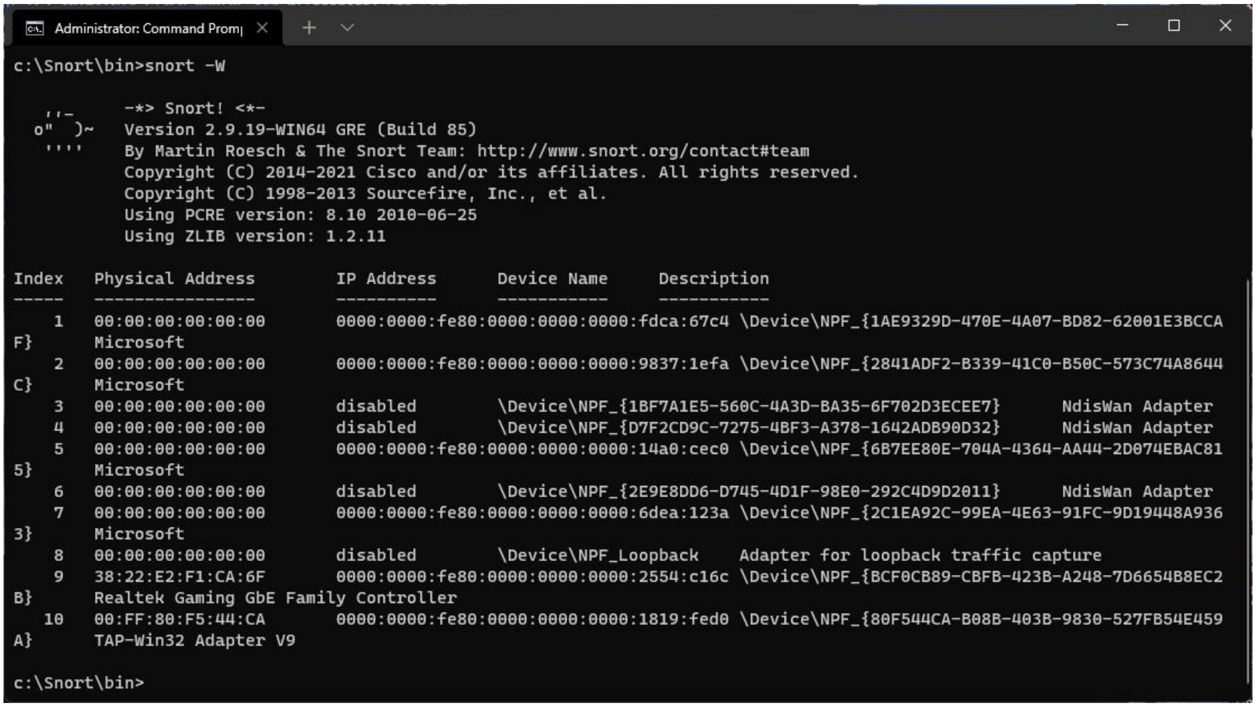
ECPS 207 Assignment Tools:

Using Snort



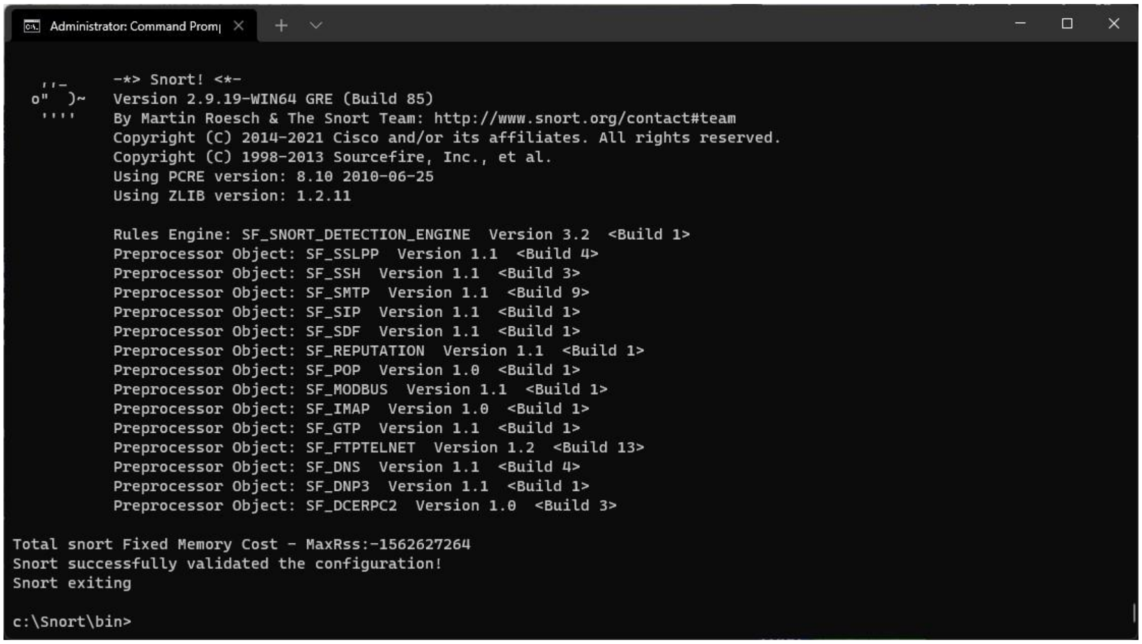
```
Microsoft Windows [Version 10.0.22000.613]
(c) Microsoft Corporation. All rights reserved.

C:\Users\orion>cd c:\Snort\bin

c:\Snort\bin>snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.19-WIN64 GRE (Build 85)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11


c:\Snort\bin>snort -W

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.19-WIN64 GRE (Build 85)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:fdca:67c4 \Device\NPF_{1AE9329D-470E-4A07-BD82-62001E3BCCA
F}      Microsoft
```

Snort Version installed



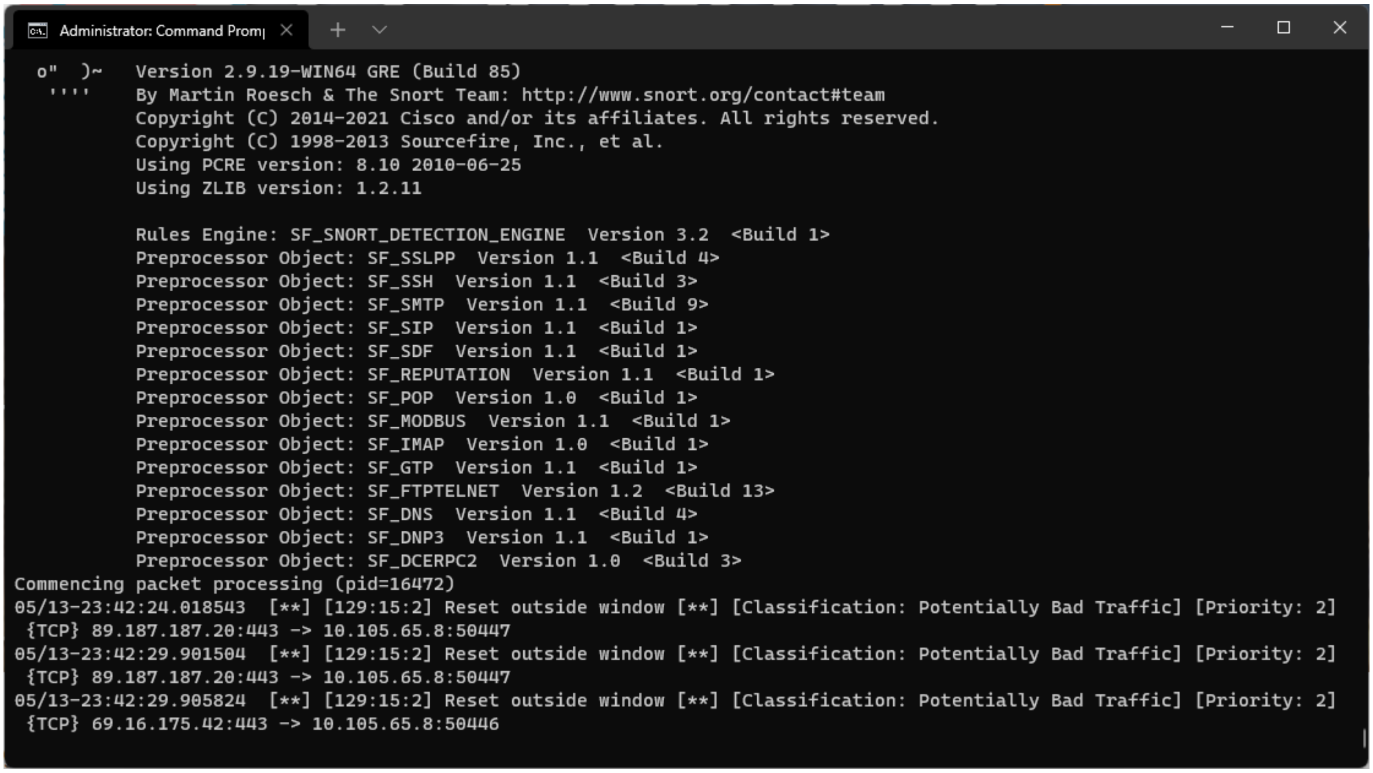
```
c:\Snort\bin>snort -W

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.19-WIN64 GRE (Build 85)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:fdca:67c4 \Device\NPF_{1AE9329D-470E-4A07-BD82-62001E3BCCA
F}      Microsoft
    2   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:9837:1efa \Device\NPF_{2841ADF2-B339-41C0-B50C-573C74A8644
C}      Microsoft
    3   00:00:00:00:00:00       disabled        \Device\NPF_{1BF7A1E5-560C-4A3D-BA35-6F702D3ECEE7}      NdisWan Adapter
    4   00:00:00:00:00:00       disabled        \Device\NPF_{D7F2CD9C-7275-4BF3-A378-1642ADB90D32}      NdisWan Adapter
    5   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:14a0:cec0 \Device\NPF_{6B7EE80E-704A-4364-AA44-2D074EBAC81
5}      Microsoft
    6   00:00:00:00:00:00       disabled        \Device\NPF_{2E9E8DD6-D745-4D1F-98E0-292C4D9D2011}      NdisWan Adapter
    7   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:6dea:123a \Device\NPF_{2C1EA92C-99EA-4E63-91FC-9D19448A936
3}      Microsoft
    8   00:00:00:00:00:00       disabled        \Device\NPF_Loopback    Adapter for loopback traffic capture
    9   38:22:E2:F1:CA:6F       0000:0000:fe80:0000:0000:0000:2554:c16c \Device\NPF_{BCF0CB89-CBFB-423B-A248-7D6654B8EC2
B}      Realtek Gaming GbE Family Controller
   10   00:FF:80:F5:44:CA       0000:0000:fe80:0000:0000:0000:1819:fed0 \Device\NPF_{80F544CA-B08B-403B-9830-527FB54E459
A}      TAP-Win32 Adapter V9

c:\Snort\bin>
```

Snort Interfaces



```
   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.19-WIN64 GRE (Build 85)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

           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:-1562627264
Snort successfully validated the configuration!
Snort exiting

c:\Snort\bin>
```

Successful Snort Configuration



```
   o"  )~   Version 2.9.19-WIN64 GRE (Build 85)
    ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
            Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
            Copyright (C) 1998-2013 Sourcefire, Inc., et al.
            Using PCRE version: 8.10 2010-06-25
            Using ZLIB version: 1.2.11

            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=16472)
05/13-23:42:24.018543  [**] [129:15:2] Reset outside window [**] [Classification: Potentially Bad Traffic] [Priority: 2]
 {TCP} 89.187.187.20:443 -> 10.105.65.8:50447
05/13-23:42:29.901504  [**] [129:15:2] Reset outside window [**] [Classification: Potentially Bad Traffic] [Priority: 2]
 {TCP} 89.187.187.20:443 -> 10.105.65.8:50447
05/13-23:42:29.905824  [**] [129:15:2] Reset outside window [**] [Classification: Potentially Bad Traffic] [Priority: 2]
 {TCP} 69.16.175.42:443 -> 10.105.65.8:50446
```

After visiting https://www.ics.uci.edu/

Command used to log packets: c:\Snort\bin>snort -i 2 -c c:\Snort\etc\snort.conf -A console > c:\Snort\log\pingtest.txt