



Course: CYB301 Security Defense and  
Response (Canadian Context)

Lab 11: NIDS (Snort with Three Modes)

Coordinator and Instructor:  
Muhammad Siddiqui

Student: Saiprasad Raman (23074624)

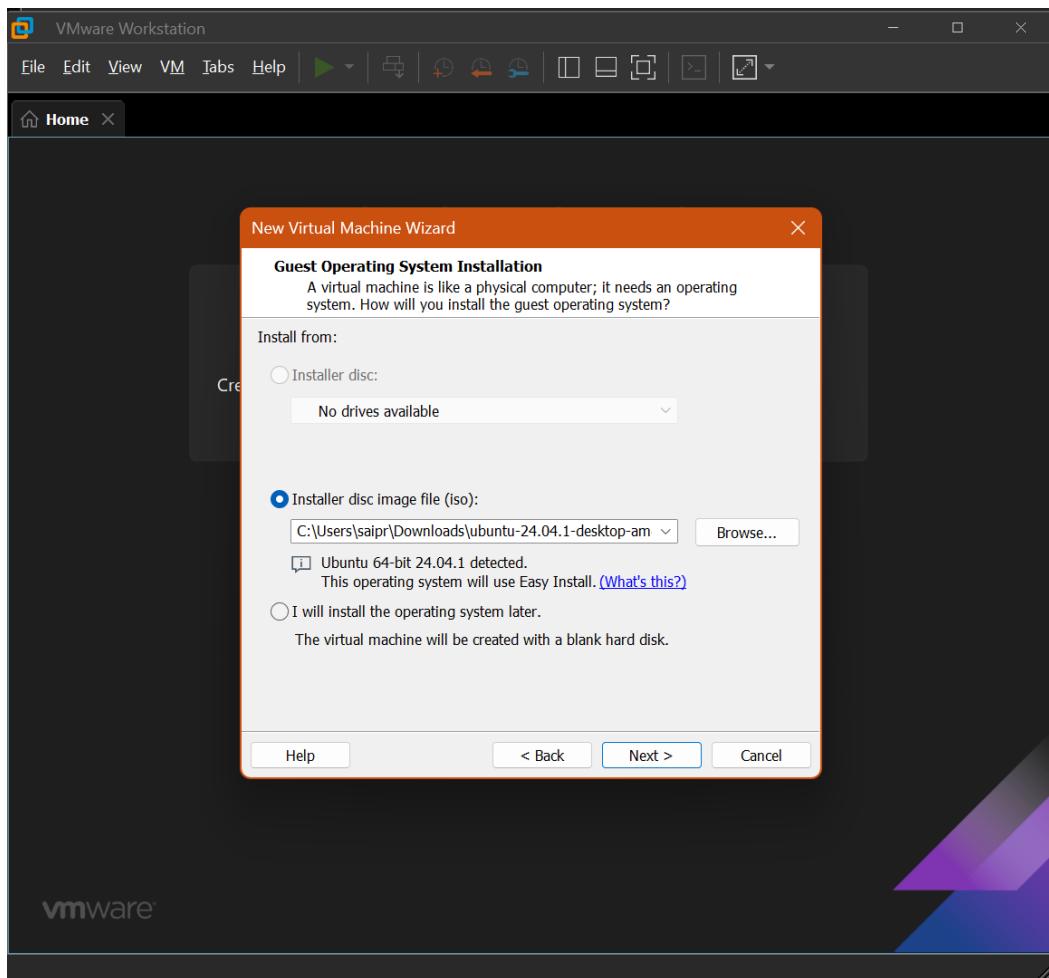
## Installing Ubuntu (VMWare)

Installing Ubuntu is similar to how you installed Kali Linux previously.

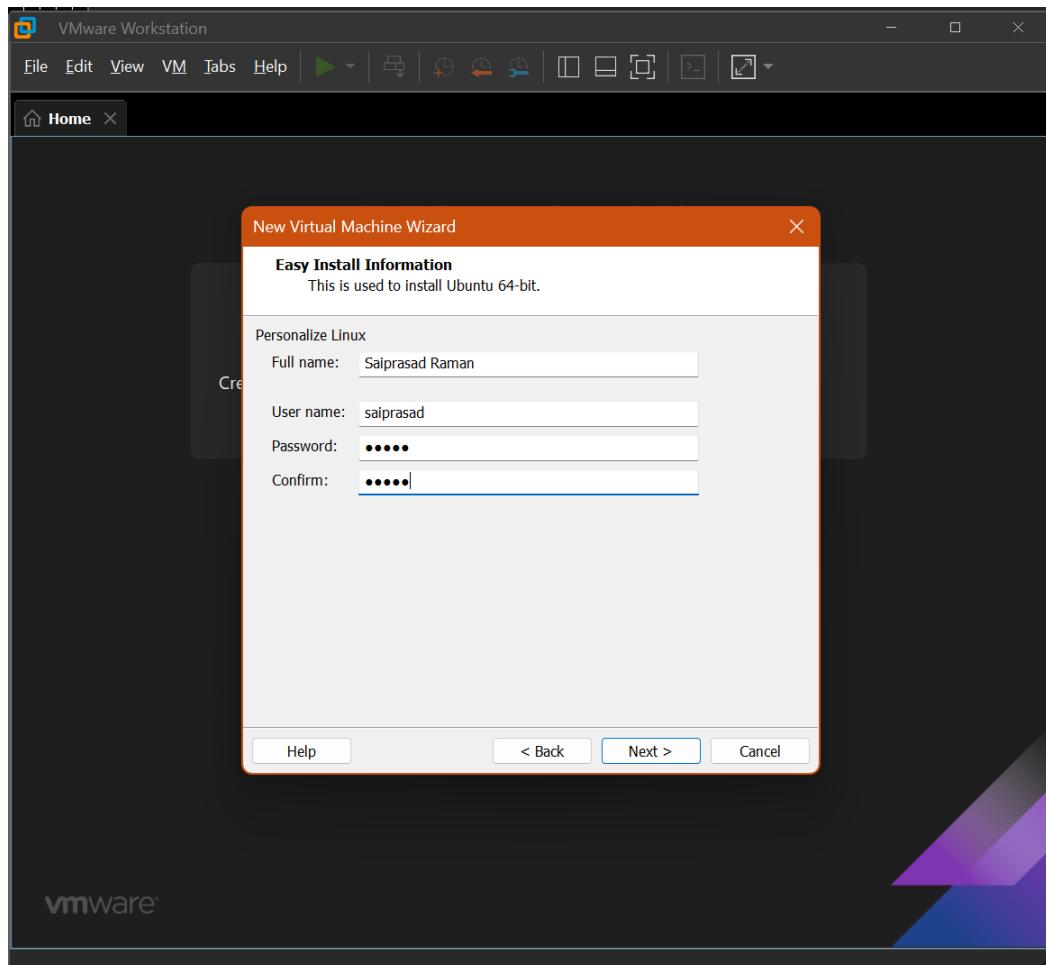
**Step 1:** Download an Ubuntu ISO and install the OS through VMWare Workstation Player. a)

Go to: <https://ubuntu.com/>

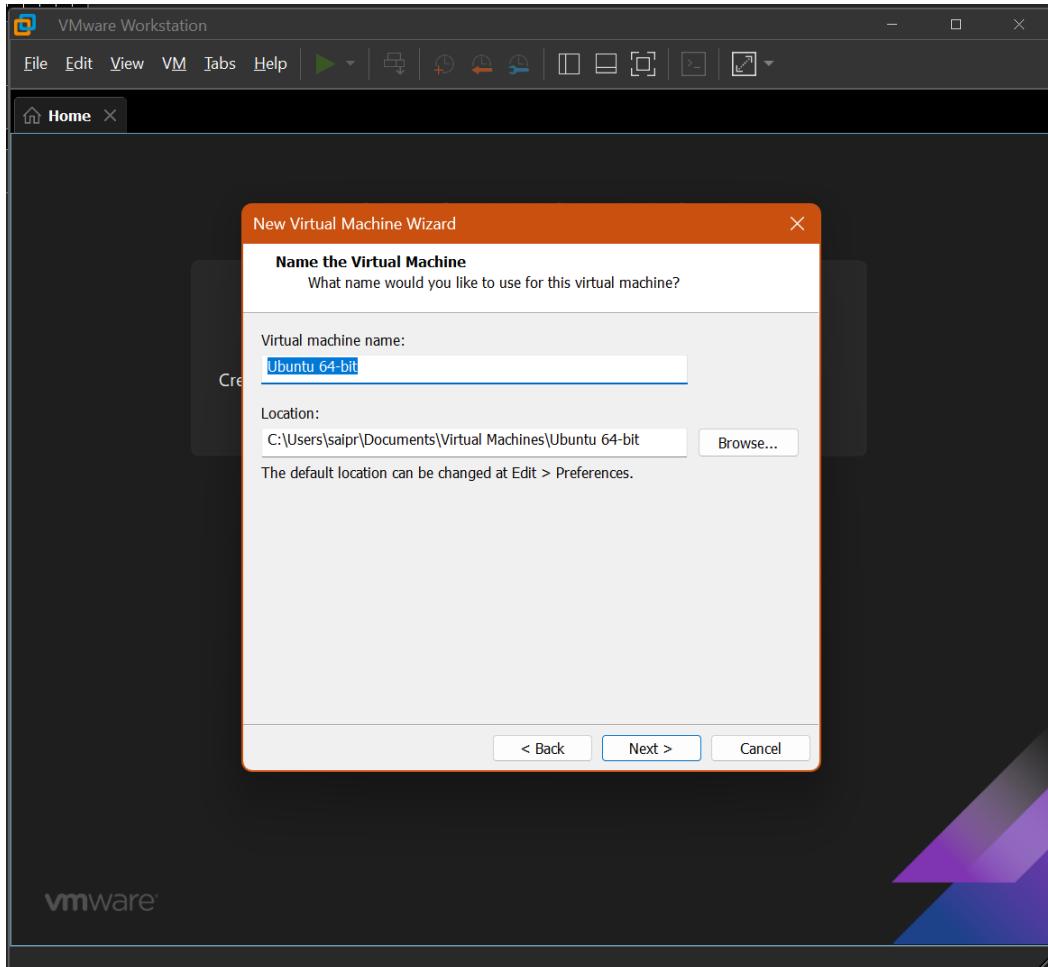
- b) Click the Download link in the menu at the top of the page.
- c) Under Ubuntu Desktop, click the current version. At the time of publication, it is 20.04 LTS.
- d) The download should start automatically, but if not, click the **Download Now** hyperlink at the top.
- e) Run **VMware Workstation Player**.
- f) Click **Create a New Virtual Machine**.
- g) With the **Installer Disc Image File (ISO)**: radio button selected, browse to the Ubuntu ISO, which will be in your Downloads folder. Click **Next**.



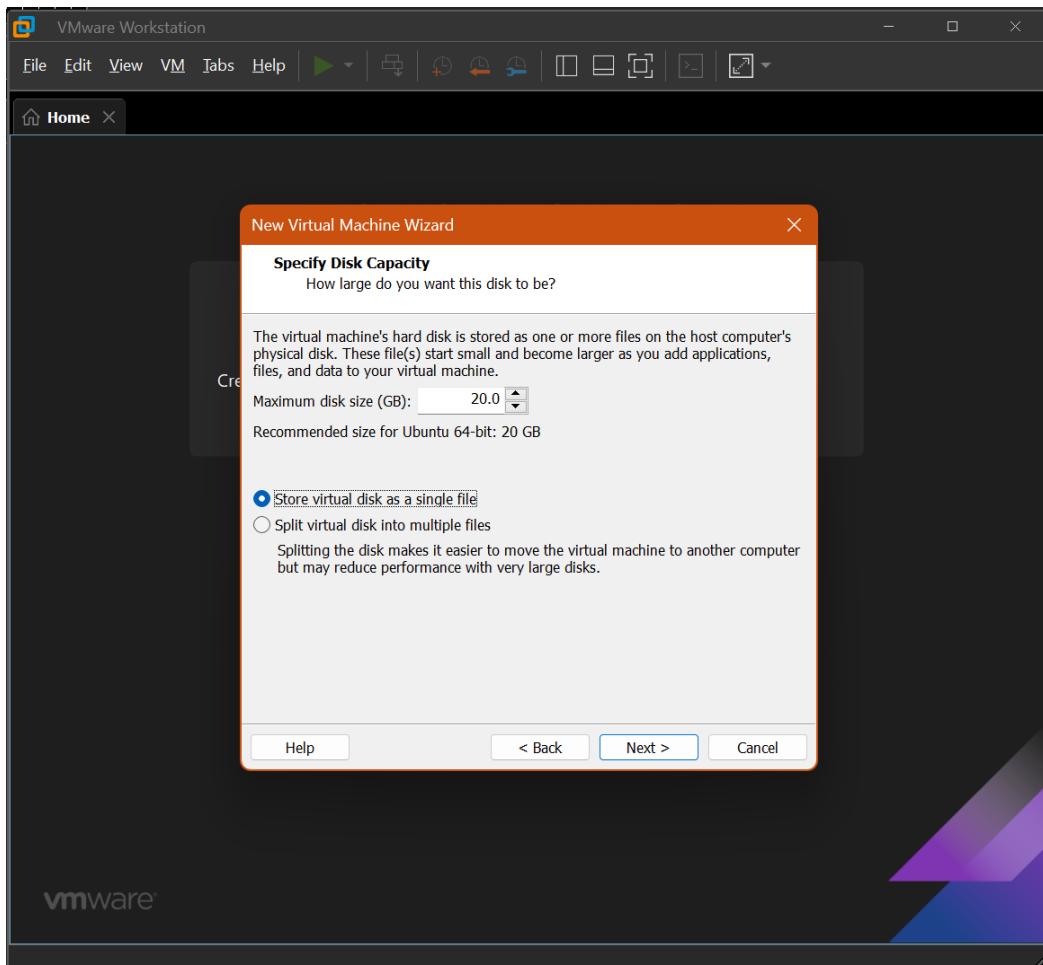
- h) Provide the easy install information, including full name, username, password, and password confirmation. Click **Next**.



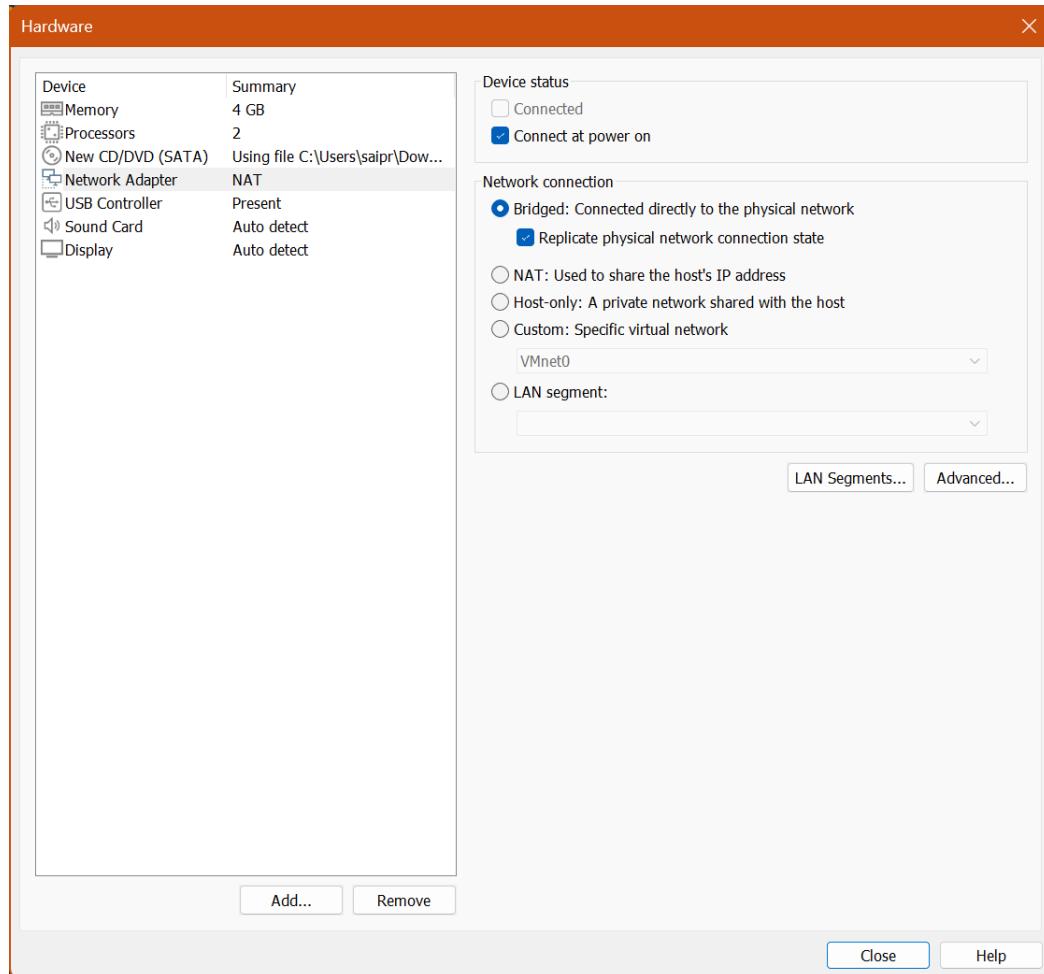
- i) In the textbox, change or keep the name of Ubuntu 64-bit and then click **Next**.



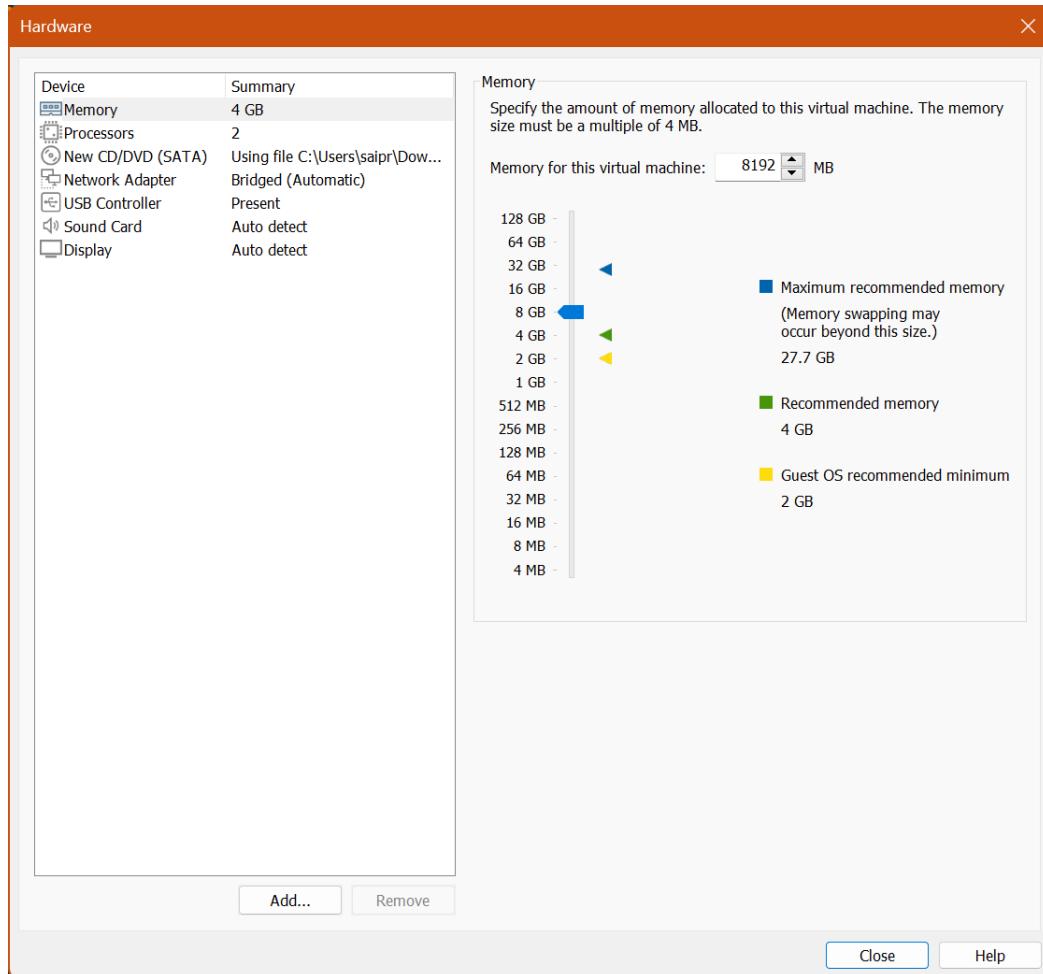
- j) Keep the default maximum disk size but select the Store Virtual Disk As a Single File radio button instead of using the default selection. Click **Next**.



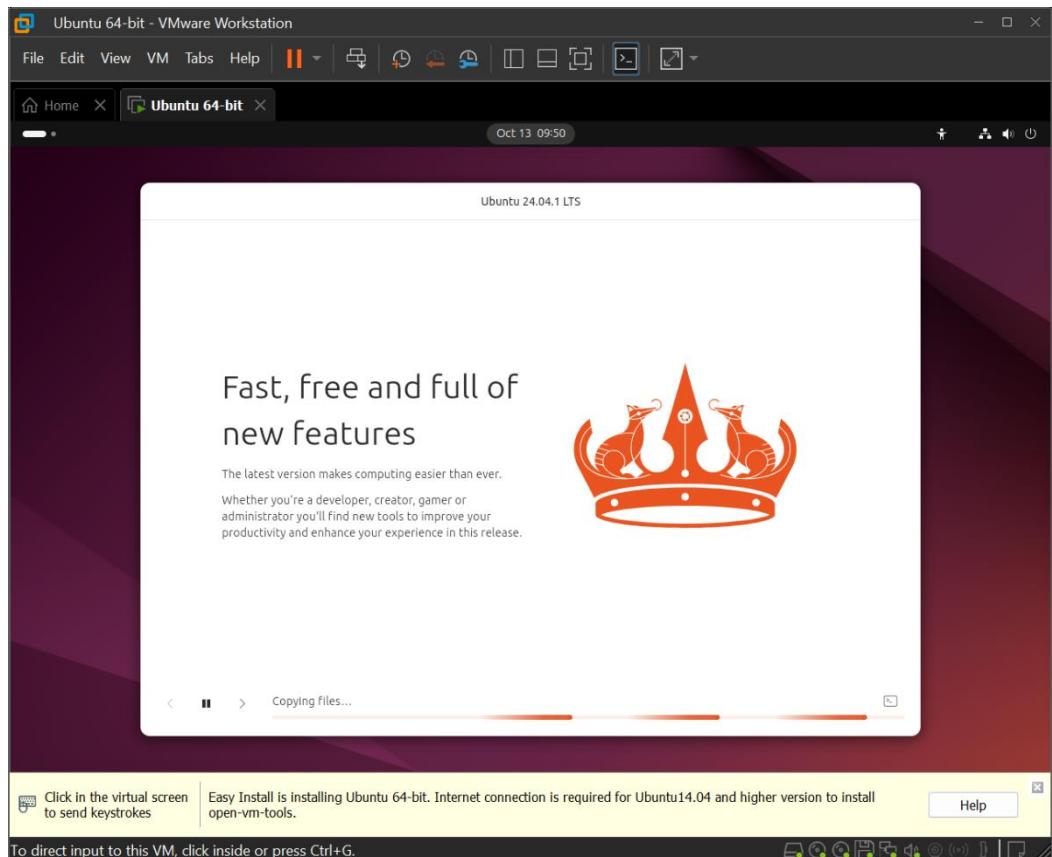
- k) Click **Customize Hardware....**
- l) On the left, select **Network Adapter** and select the radio button **Bridged: Connected Directly To The Physical Network** and the checkbox **Replicate Physical Network Connection State**.



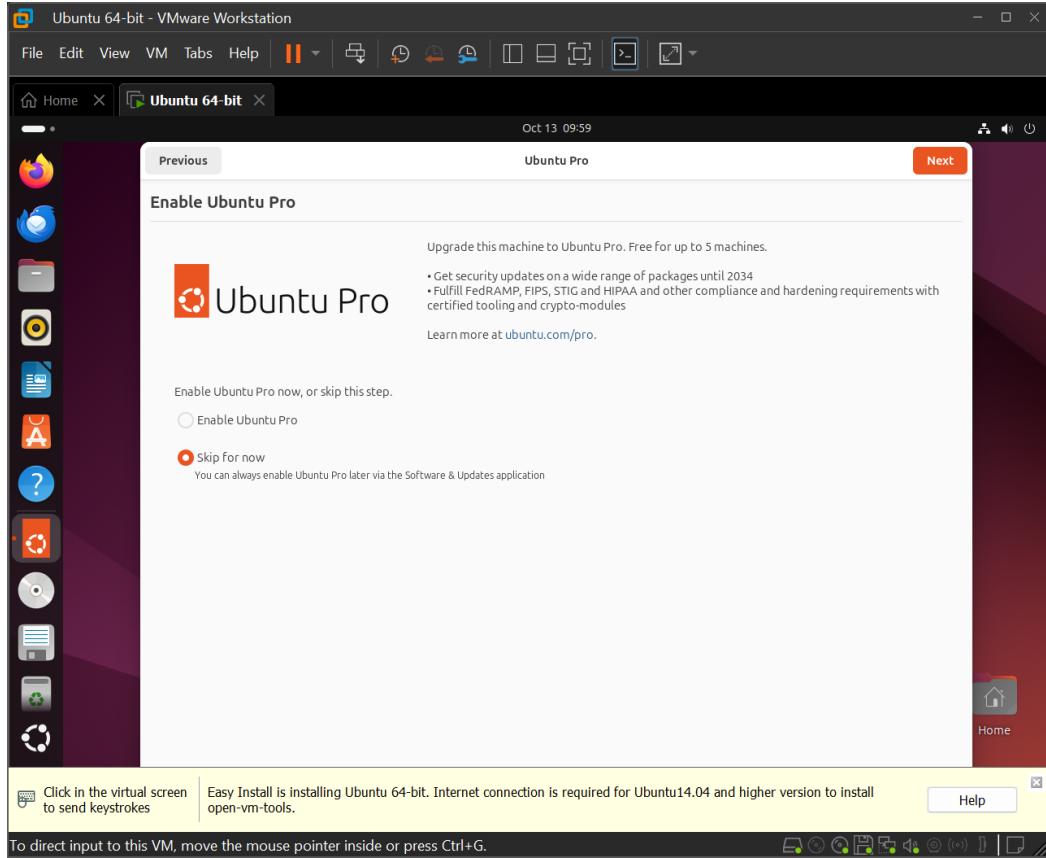
- m) Feel free to increase the VM's RAM, if desired, by clicking Memory and increasing the allocated memory.
- n) Click **Close** and then click **Finish**.



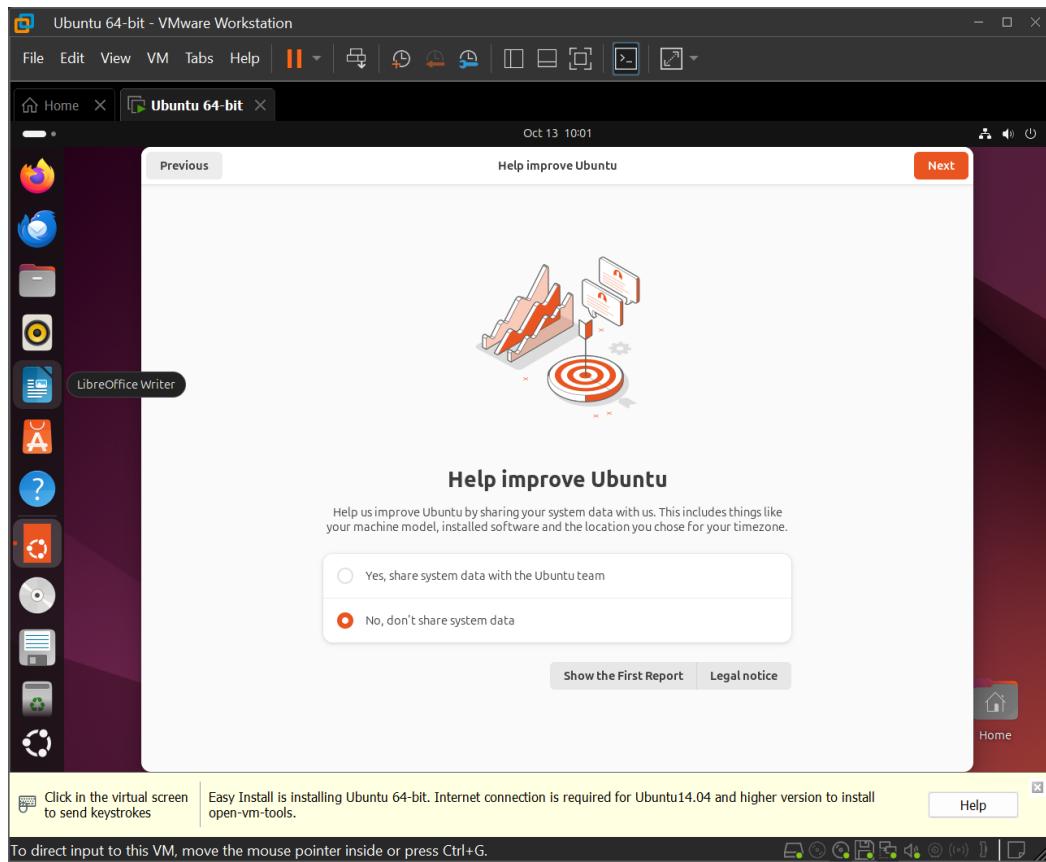
- o) After some verification checks and the copying of files, the installation will start.



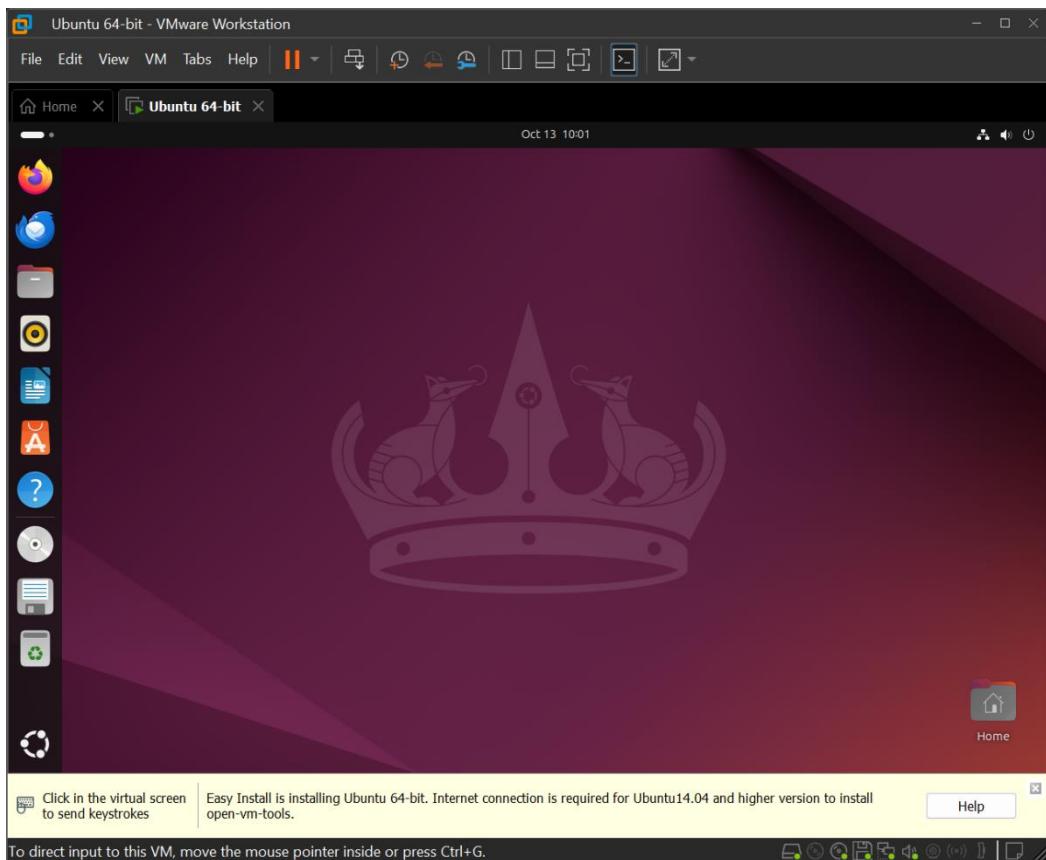
- p) When the installation completes, click your username, provide your password, and press **ENTER** to log in.
- q) Click **Skip** at the top right of the Online Accounts screen.



- r) Click **Next** at the top right on the Livepatch screen.
- s) Click the radio button next to **No, Don't Send System Info** and then click **Next** at the top right of the screen.



- t) Click **Next** at the top right of the Privacy screen.
- u) Click **Done** in the top right of the Ready to Go screen.
- v) If the Software Updater pops up, click the Install Now button. When prompted, provide your password. Then, when you see The Computer Needs to Restart to Finish Installing Updates, click Restart Now. After the VM reboots, log in once again.

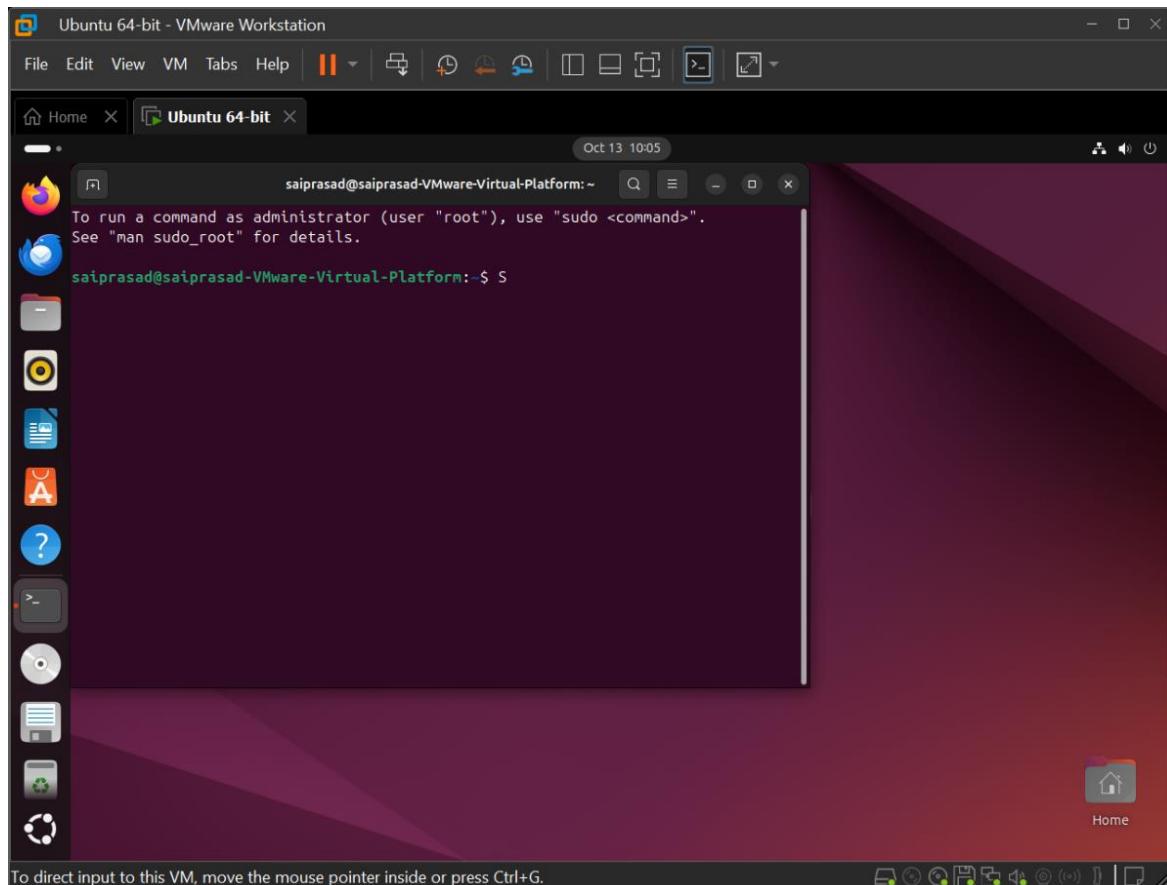


## Installing Wireshark and Snort

**Step 2:** Download and install Wireshark and Snort.

- a) Press **CTRL-G** or click in the VM to work in the VM. Press **CTRL-ALT** to return focus to the host machine.

- b) In the Ubuntu VM, click the **Show Applications** button at the bottom of the Ubuntu Launcher Bar on the left of the screen. Click in the search bar, type **Terminal**, and click the **Terminal** icon. Alternatively, pressing **CTRL-ALT-T** will open up a terminal.



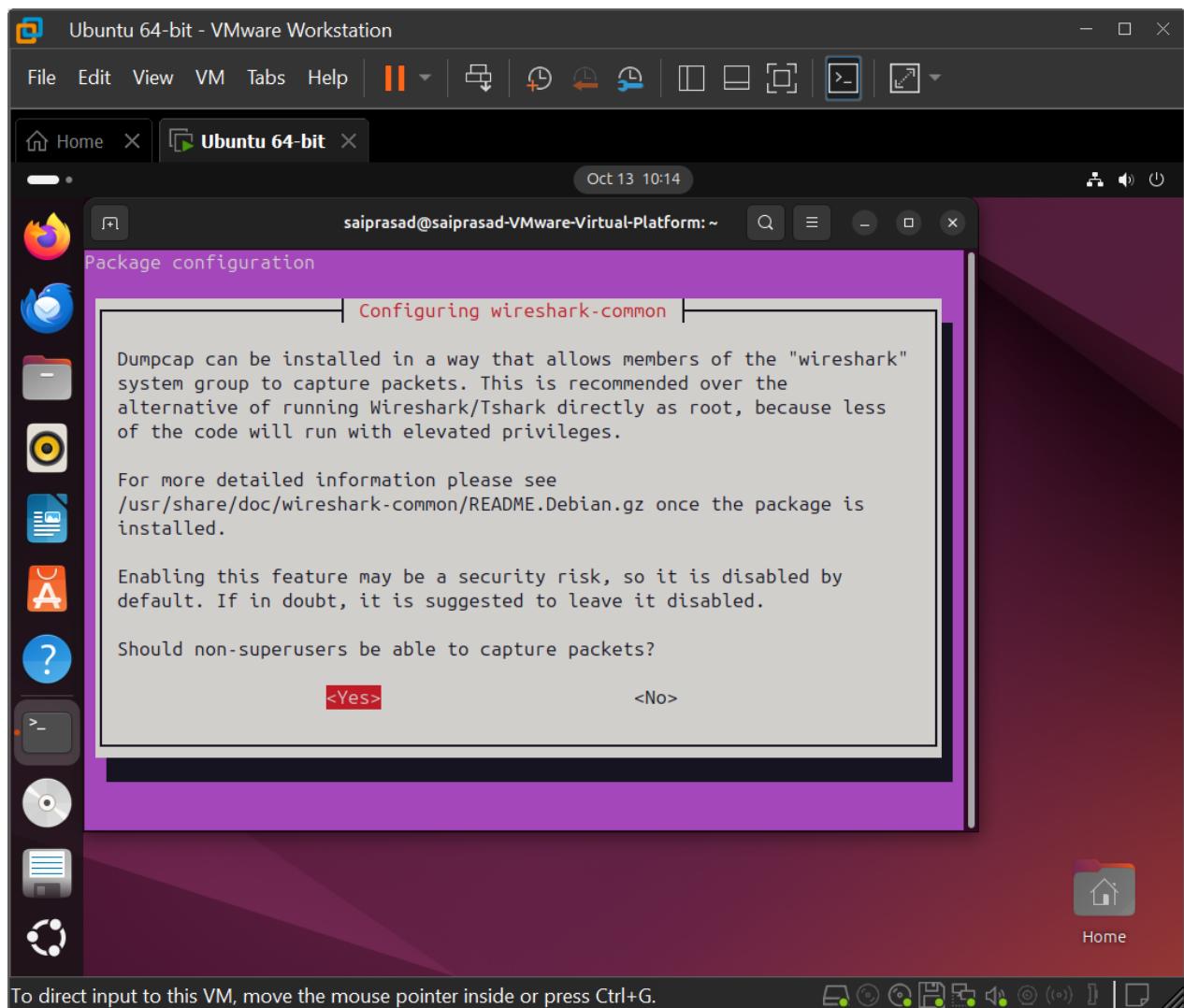
- c) Execute the following two commands. The first downloads package information from every configured source. The second upgrades all installed packages to their latest versions.

**sudo apt update**

**sudo apt upgrade**

```
saiprasad@saiprasad-VMware-Virtual-Platform:~$ sudo apt update
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 http://ca.archive.ubuntu.com/ubuntu noble InRelease
Hit:3 http://ca.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:4 http://ca.archive.ubuntu.com/ubuntu noble-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
71 packages can be upgraded. Run 'apt list --upgradable' to see them.
saiprasad@saiprasad-VMware-Virtual-Platform:~$ sudo apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
Get more security updates through Ubuntu Pro with 'esm-apps' enabled:
  lib cJSON1 libpostproc57 libavcodec60 libavutil58 libswscale7 libswresample4
  libavformat60 libavfilter9
Learn more about Ubuntu Pro at https://ubuntu.com/pro
The following upgrades have been deferred due to phasing:
  python3-distupgrade shotwell shotwell-common ubuntu-release-upgrader-core
  ubuntu-release-upgrader-gtk
The following packages will be upgraded:
  apparmor cloud-init dmsetup fonts-opensymbol fwupd gir1.2-mutter-14
  gnome-shell gnome-shell-common gnome-shell-extension-appindicator
  gnome-shell-extension-ubuntu-dock initramfs-tools initramfs-tools-bin
  initramfs-tools-core libapparmor1 libcryptsetup12 libdevmapper1.02.1
  libfwupd2 libmutter-14-0 libproc2-0 libreoffice-base-core libreoffice-calc
  libreoffice-common libreoffice-core libreoffice-draw libreoffice-gnome
```

- d) Unlike Kali Linux, Ubuntu does not come with Wireshark, the world-renowned packet sniffer. Execute the following command to download and install it: **sudo apt install wireshark**  
Put in your password and press **ENTER** when prompted now and throughout this lab. Type **Y** and press **ENTER** when prompted to continue. At the “Should Non-superusers Be Able to Capture Packets?” question, press the left arrow to select **Yes** and then press **ENTER**.



- e) Enter the following command to download and install Snort: **sudo apt install snort**

Type **Y** and press **ENTER** when prompted to continue. At the Configuring Snort screen, press **ENTER** to select **OK**. In the Interface(s) Which Snort Should Listen On: textbox, using **BACKSPACE**, change the **eth0** entry to **ens33**, which is the interface name used by Ubuntu. Press **ENTER** to select **OK**. If you see an Invalid Interface message, press **ENTER** to select **OK**. You will be brought back to the first screen again. Once again, press **ENTER** to select **OK**, and then press **ENTER** again to select **OK** with **ens33** still in the textbox from before. You will get that Invalid Interface message again. Press **ENTER** to select **OK**. This time, the installation completes. This is a known bug for this version of Snort at the time of writing, and it may be resolved by the time you are doing this lab exercise. Even with that pushback from the Snort installer, Snort has been successfully installed.

```
Processing triggers for desktop-file-utils (0.27-2build1) ...
saiprasad@saiprasad-VMware-Virtual-Platform: $ sudo apt install snort
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libdaq2t64 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common
  libnetfilter-queue1 libpcre3 net-tools oinkmaster snort-common
  snort-common-libraries snort-rules-default
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  libdaq2t64 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common
  libnetfilter-queue1 libpcre3 net-tools oinkmaster snort-common
  snort-common-libraries snort-rules-default
0 upgraded, 12 newly installed, 0 to remove and 5 not upgraded.
Need to get 2,869 kB of archives.
After this operation, 12.2 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ca.archive.ubuntu.com/ubuntu noble/universe amd64 libluajit-5.1-common all 2.1.0+git20231223.c525bcb+dfsg-1 [49.2 kB]
Get:2 http://ca.archive.ubuntu.com/ubuntu noble/universe amd64 libluajit-5.1-2 amd64 2.1.0+git20231223.c525bcb+dfsg-1 [275 kB]
Get:3 http://ca.archive.ubuntu.com/ubuntu noble/universe amd64 libpcre3 amd64 2:
```

## Activity 1: Snort Sniffer Mode

In this lab exercise, you will use Snort as a packet sniffer. Just like Wireshark, Snort can sniff packets.

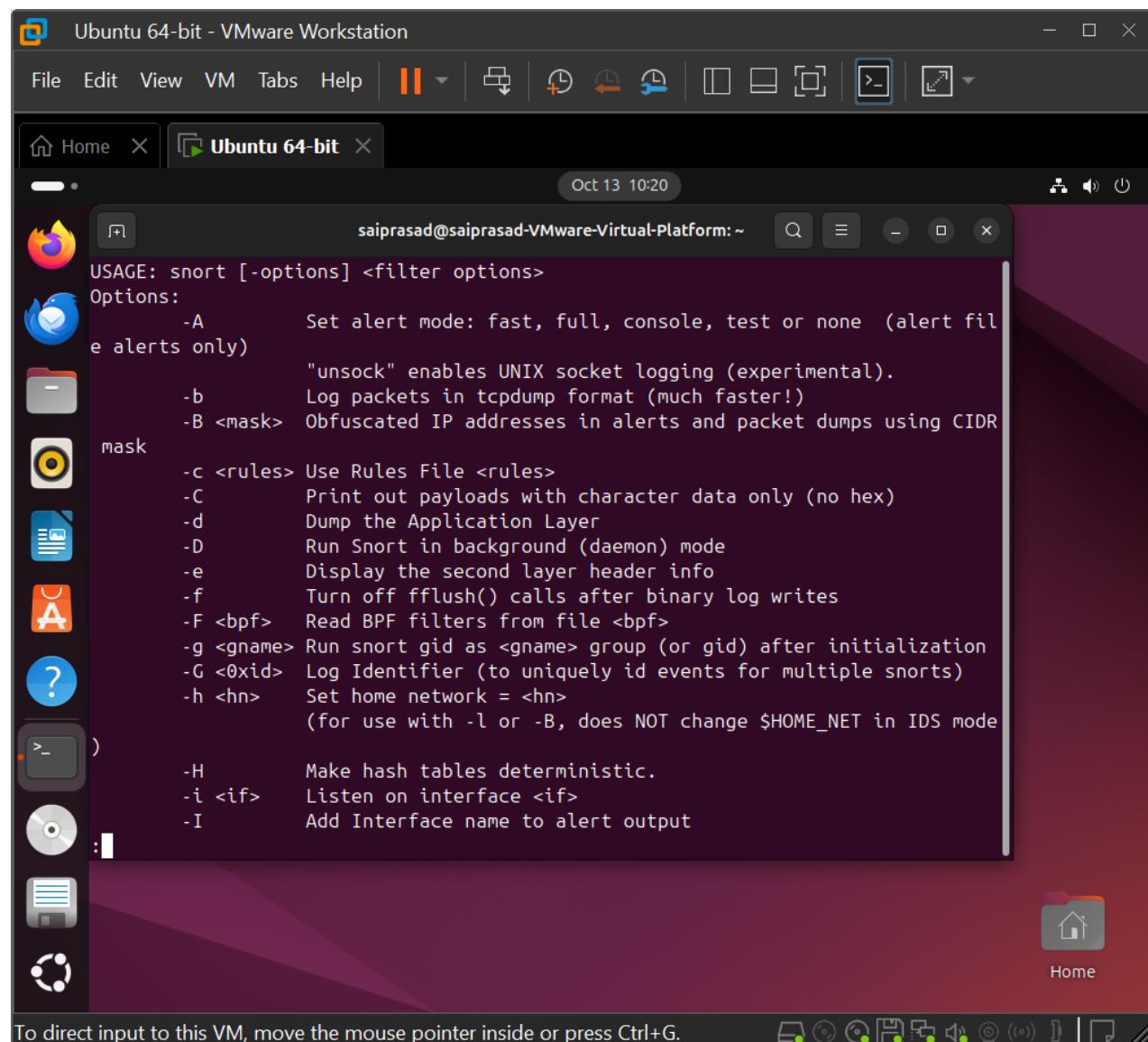
The fields and values that Snort sniffs are displayed to the console in Sniffer mode.

- In the Ubuntu VM, press **CTRL-ALT-T** to open up a new console. Press **ENTER** after every command.

**Step 1:** Examine the Snort help output and man page entry, as well as the version of Snort.

a) Look at the Snort help output: **snort -h | less**

Advance line by line by pressing **ENTER**. Advance page by page with the spacebar. You can use the up and down arrows to move back and forth. Type **q** to quit.



b) Check out the man page entry for Snort: **man snort**

The screenshot shows a VMware Workstation interface with a single running VM titled "Ubuntu 64-bit". Inside the VM, a terminal window is open with the command "man snort" run. The terminal output is as follows:

```
saiprasad@saiprasad-Virtual-Platform: ~
SNORT(8)           System Manager's Manual           SNORI(8)

NAME
    Snort - open source network intrusion detection system

SYNOPSIS
    snort [-bCdDeEfHIMNOpqQsTUVVwWxXy?] [-A alert-mode] [-B address-con-
    version-mask] [-c rules-file] [-F bpf-file] [-g group-name] [-G id]
    [-h home-net] [-i interface] [-k checksum-mode] [-K logging-mode]
    [-l log-dir] [-L bin-log-file] [-m umask] [-n packet-count] [-P
    snap-length] [-r tcpdump-file] [-R name] [-S variable=value]
    [-t chroot_directory] [-u user-name] [-Z pathname] [--logid id]
    [--perfmon-file pathname] [--pid-path pathname] [--snaplen snap-
    length] [--help] [--version] [--dynamic-engine-lib file]
    [--dy-
    namic-engine-lib-dir directory] [--dynamic-detection-lib file]
    [--dy-
    namic-detection-lib-dir directory] [--dump-dynamic-rules directory]
    [--dynamic-preprocessor-lib file] [--dynamic-preprocessor-lib-dir di-
    rectory] [--dynamic-output-lib file] [--dynamic-output-lib-dir direc-
    tory] [--alert-before-pass] [--treat-drop-as-alert] [--treat-drop-
    as-ignore] [--process-all-events] [--enable-inline-test] [--create-
    pidfile] [--nolock-pidfile] [--no-interface-pidfile] [--disable-at-
    tribute-reload-thread] [--pcap-single= tcpdump-file] [--pcap-filter=
    filter] [--pcap-list= list] [--pcap-dir= directory] [--pcap-file=
    file]
Manual page snort(8) line 1 (press h for help or q to quit)
```

The terminal window has a dark background with light-colored text. The title bar shows the session is on "Ubuntu 64-bit". The status bar at the bottom of the terminal window indicates "Manual page snort(8) line 1 (press h for help or q to quit)".

c) See the version number of Snort: **snort -V**

```
saiprasad@saiprasad-Virtual-Platform:~$ snort -h | less
saiprasad@saiprasad-Virtual-Platform:~$ man snort
saiprasad@saiprasad-Virtual-Platform:~$ 
saiprasad@saiprasad-Virtual-Platform:~$ snort -V

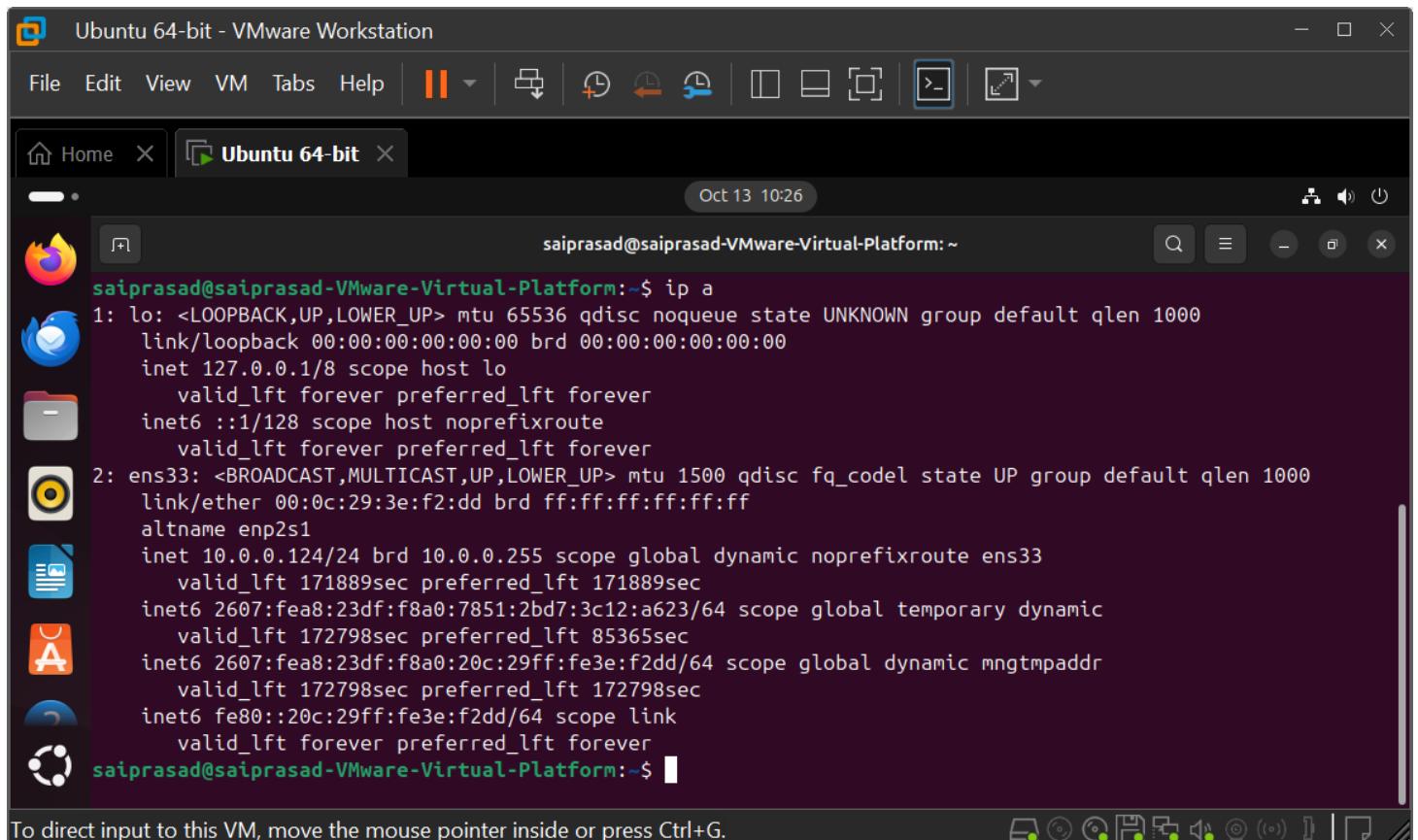
      _.-> Snort! <*-.
o" )~ Version 2.9.20 GRE (Build 82)
    '' By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
    Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
    Copyright (C) 1998-2013 Sourcefire, Inc., et al.
    Using libpcap version 1.10.4 (with TPACKET_V3)
    Using PCRE version: 8.39 2016-06-14
    Using ZLIB version: 1.3

saiprasad@saiprasad-Virtual-Platform:~$
```

**Step 2:** Get your VM's IP address and start using Snort, generating output of certain Layer 3 and (if applicable) Layer 4 header information.

- Find the Ubuntu VM's IP address by entering the following command: `ip a`

It is listed after inet in the ens33 interface section.



```
saiprasad@saiprasad-Virtual-Platform:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:3e:f2:dd brd ff:ff:ff:ff:ff:ff
        altname enp2s1
        inet 10.0.0.124/24 brd 10.0.0.255 scope global dynamic noprefixroute ens33
            valid_lft 171889sec preferred_lft 171889sec
        inet6 2607:fea8:23df:f8a0:7851:2bd7:3c12:a623/64 scope global temporary dynamic
            valid_lft 172798sec preferred_lft 85365sec
        inet6 2607:fea8:23df:f8a0:20c:29ff:fe3e:f2dd/64 scope global dynamic mngtmpaddr
            valid_lft 172798sec preferred_lft 172798sec
        inet6 fe80::20c:29ff:fe3e:f2dd/64 scope link
            valid_lft forever preferred_lft forever
saiprasad@saiprasad-Virtual-Platform:~$
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

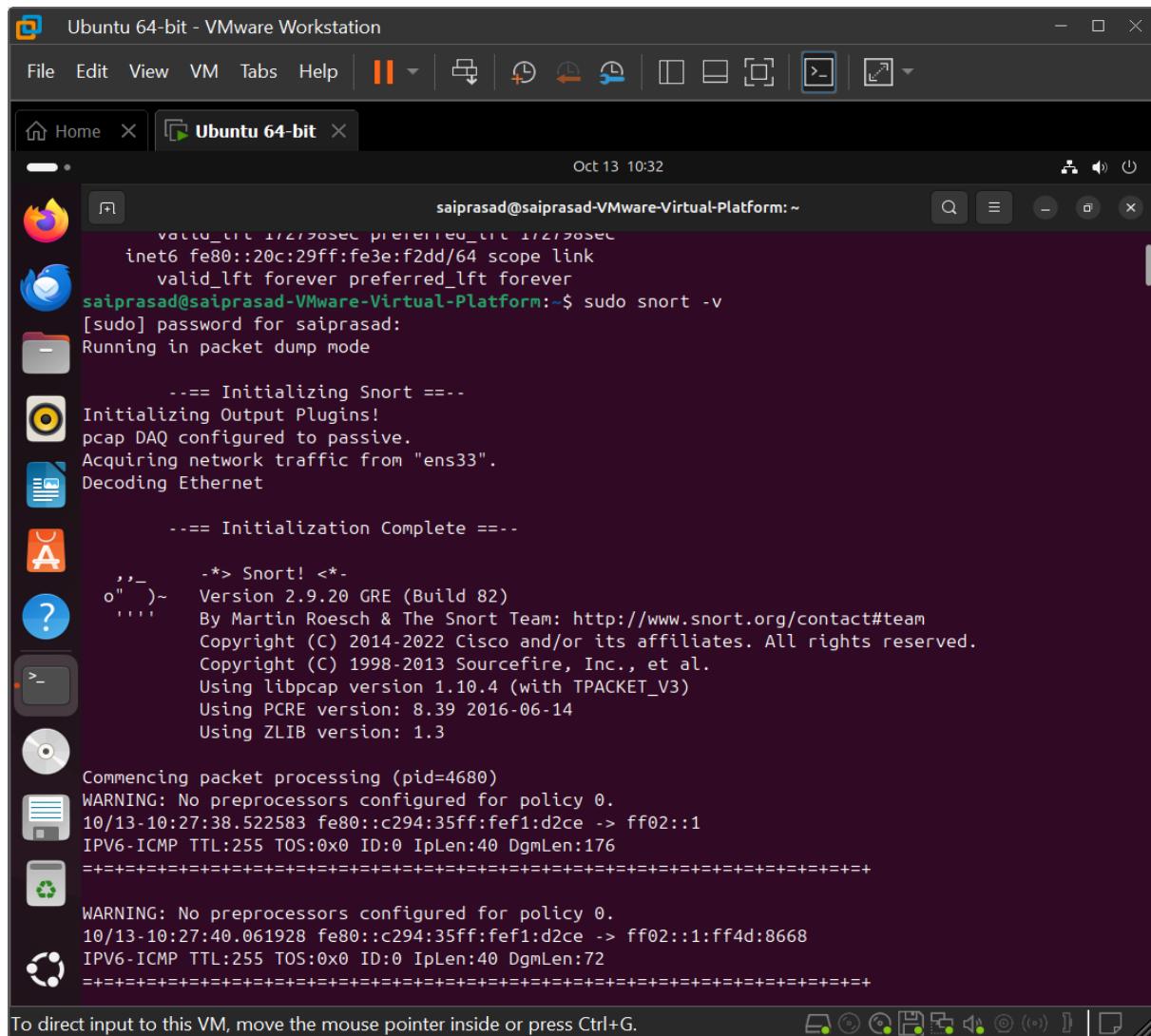
- b) Enter the following command: **sudo snort -v**

The following is from the Snort man page:

-v Be verbose. Prints packets out to the console. There is one big problem with verbose mode:

it is slow. If you are doing IDS work with Snort, do not use the '-v' switch, you WILL drop packets Snort runs and only displays information from the Layer 3 header, although not all fields and values are included. Snort will also display port numbers from Layer 4 headers when TCP or UDP is used. Ignore the "WARNING: No preprocessors configured for policy 0." message that is repeatedly shown. We will fix that shortly. Any packet going in and out of the Ubuntu VM will be displayed in the console.

You can stop Snort with **CTRL-C**. It might take a few seconds for Snort to stop and for information such as the following to be displayed: how long Snort ran for, how many packets it processed, the number of packets per minute and packets per second, memory usage summary, packet I/O totals, and a breakdown by protocol.



The screenshot shows a terminal window in an Ubuntu 64-bit VMware Workstation environment. The terminal output is as follows:

```
saiprasad@saiprasad-Virtual-Platform:~$ sudo snort -v
[sudo] password for saiprasad:
Running in packet dump mode

     == Initializing Snort ==
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "ens33".
Decoding Ethernet

     == Initialization Complete ==

      ,,-      -*> Snort! <*- 
o"   )~  Version 2.9.20 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 libpcap version 1.10.4 (with TPACKET_V3)
     Using PCRE version: 8.39 2016-06-14
     Using ZLIB version: 1.3

Commencing packet processing (pid=4680)
WARNING: No preprocessors configured for policy 0.
10/13-10:27:38.522583 fe80::c294:35ff:fef1:d2ce -> ff02::1
IPV6-ICMP TTL:255 TOS:0x0 ID:0 IpLen:40 DgmLen:176
=====+
WARNING: No preprocessors configured for policy 0.
10/13-10:27:40.061928 fe80::c294:35ff:fef1:d2ce -> ff02::1:ff4d:8668
IPV6-ICMP TTL:255 TOS:0x0 ID:0 IpLen:40 DgmLen:72
=====+
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

- c) Enter the following command: **sudo snort -v -i ens33**

If you had multiple interfaces, the `-i` option would be the way to specify a certain interface that Snort should sniff on. Try it now, although with the current setup featuring one nonloopback interface, the same thing will happen with or without the `-i` option.

From the Windows 10 VM or host machine, ping the IP address of the Ubuntu VM. You should be able to see the pings in the output of Snort. **Take the screenshot**. Break out with **CTRL-C**.

d) Enter the following command: **sudo snort -v -i lo**

e) To see the difference, open up a new terminal, ping the loopback address (127.0.0.1), and observe the output in the terminal in which Snort is sniffing. **Take the screenshot**. You can break out with **CTRL-C**.

**Step 3:** Run Snort, generating upper layer data, in addition to Layer 3 and Layer 4 header information.

a) Enter the following command: **sudo snort -vd**

The following is from the Snort man page:

**-d** Dump the application layer data when displaying packets in verbose or packet logging mode. After running Snort with the **-v** and **-d** options together (**-vd**), stop Snort with CTRL-C.

Snort runs and shows the upper layer data, in addition to information from Layer 3 and Layer 4 (when TCP or UDP is used). **Take the screenshot.**

- b) Enter the following command:

```
sudo snort -ve
```

The following is from the Snort man page:

-e Display/log the link layer packet headers. After running Snort with the -v and -e options together (-ve), stop Snort with CTRL-C. Snort runs and shows information from Layer 2, in addition to information from Layer 3. **Take the screenshot.**

```
saiprasad@saiprasad-VMware-Virtual-Platform:~$ sudo snort -ve
Running in packet dump mode
--= Initializing Snort =--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "ens33".
Decoding Ethernet
--= Initialization Complete =--
--> Snort! <-
o" )~ Version 2.9.20 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 libpcap version 1.10.4 (with TPACKET_V3)
     Using PCRE version: 8.39 2016-06-14
     Using ZLIB version: 1.3
Commencing packet processing (pid=5136)
WARNING: No preprocessors configured for policy 0.
10/13-11:11:52.994015 58:1C:F8:B0:49:42 -> 01:00:5E:4D:4D:4D type:0x800 len:0x94
10.0.0.140:12177 -> 224.77.77.77:12177 UDP TTL:1 TOS:0x0 ID:31961 IpLen:20 DgmLen:134
Len: 106
=====
WARNING: No preprocessors configured for policy 0.
10/13-11:11:53.007006 58:1C:F8:B0:49:42 -> 01:00:5E:4D:4D:4D type:0x800 len:0x94
10.0.0.140:12177 -> 224.77.77.77:12177 UDP TTL:1 TOS:0x0 ID:31962 IpLen:20 DgmLen:134
Len: 106
=====
WARNING: No preprocessors configured for policy 0.
10/13-11:11:53.007457 58:1C:F8:B0:49:42 -> 01:00:5E:4D:4D:4D type:0x800 len:0x94
10.0.0.140:12177 -> 224.77.77.77:12177 UDP TTL:1 TOS:0x0 ID:31963 IpLen:20 DgmLen:134
Len: 106
=====
WARNING: No preprocessors configured for policy 0.
10/13-11:11:53.007887 58:1C:F8:B0:49:42 -> 01:00:5E:4D:4D:4D type:0x800 len:0x94
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

- c) Enter the following command:

**sudo snort -vde**

After running Snort with the -v, -d, and -e options together (-vde), stop Snort with CTRL-C.

Snort runs and shows header information from Layer 2, Layer 3, and upper-layer data.

The switches could have been typed separately, and in a different order, for the same results, like this: **sudo snort -d -v -e**

Furthermore, the `-v` option becomes redundant with either the `-d` or `-e` option. In other words, if you were to leave off the `-v` option, sudo snort `-de` would have done the same thing.



## Activity 2: Snort Packet Logger Mode

In this lab exercise, you will sniff with Snort, but instead of viewing the output in the console, you will log the packets to a file.

You can instruct Snort to record packets to a file by using the **-l** option and specifying a directory that the log should be sent to. Then the log file can be opened up in a packet sniffer, like Wireshark.

- In the Ubuntu VM, press **CTRL-ALT-T** to open up a new terminal. Press **ENTER** after every command.

Step 1: Log packets that Snort sniffs to a file.

- a) Enter the following command: **sudo snort -l .**

The dot at the end of the command represents the current directory. The following is from the Snort man page:

**-l log-dir**

Set the output logging directory to log-dir. All plain text alerts and packet logs go into this directory. If this option is not specified, the default logging directory is set to /var/log/snort.

You do not need **-v**, **-d**, or **-e**, contrary to documentation out there, including Snort's own documentation.

- b) Send a ping from the Windows 10 VM or host machine to the Ubuntu VM running Snort. Stop Snort with **CTRL-C**. **Take the screenshot.**

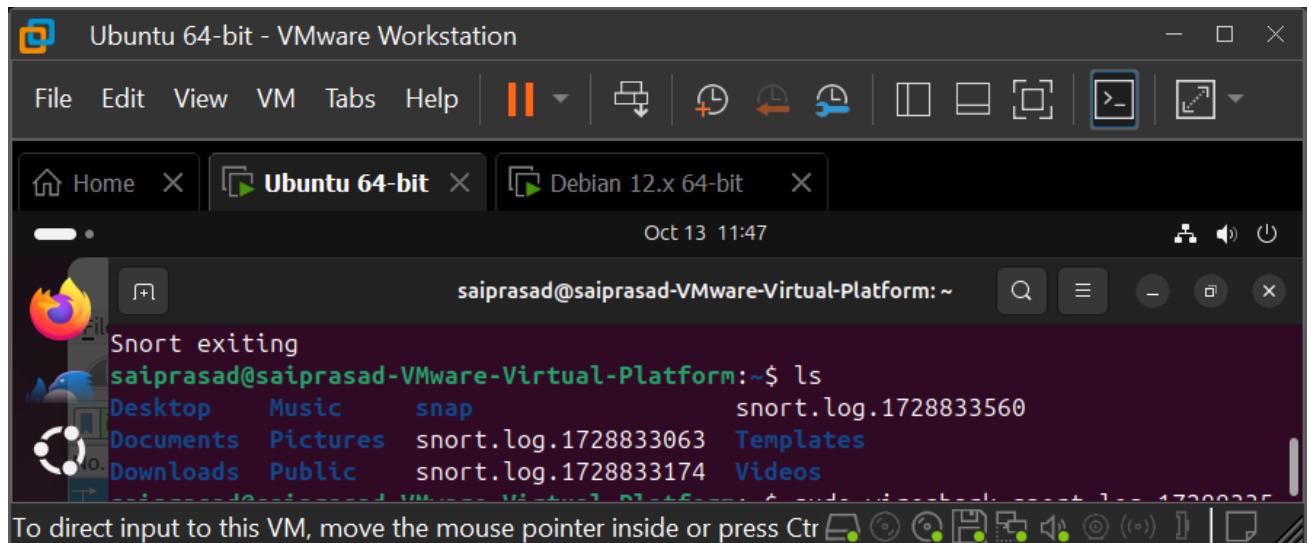


Step 2: Examine the logged packets.

a) Enter the following command:

**ls**

See the name of the log file generated.



Ubuntu 64-bit - VMware Workstation

File Edit View VM Tabs Help | **Ubuntu 64-bit** | **Debian 12.x 64-bit** | Oct 13 11:47

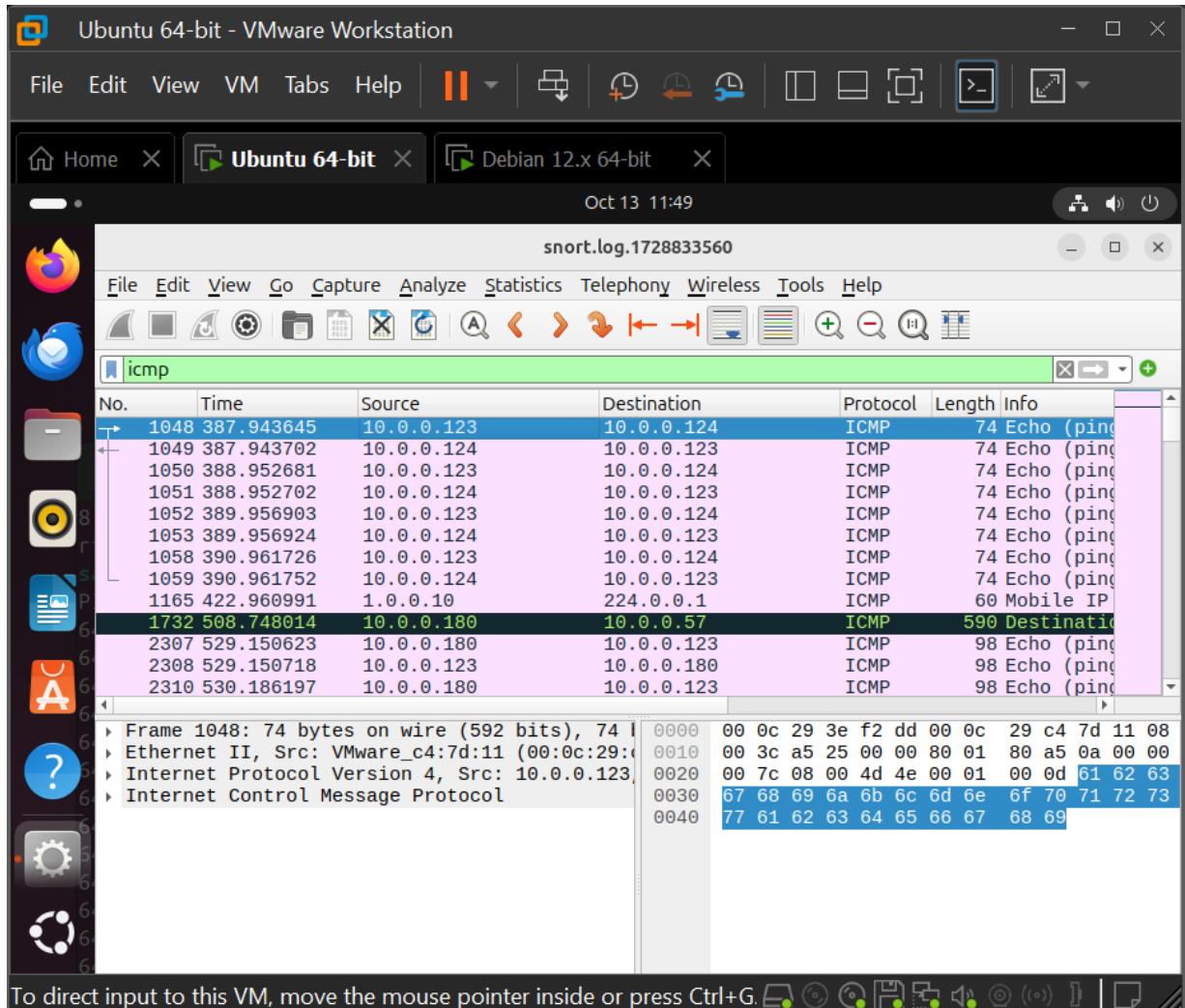
Snort exiting  
saiprasad@saiprasad-Virtual-Platform:~\$ ls  
Desktop Music snap snort.log.1728833560  
Documents Pictures snort.log.1728833063 Templates  
Downloads Public snort.log.1728833174 Videos

To direct input to this VM, move the mouse pointer inside or press Ctrl

b) Enter the following command: **sudo wireshark**

**snort.log.159604382**

Wireshark and packet sniffing in general were introduced previously and will be explored further in this lab. For now, simply open up the logged packets in Wireshark. In the display filter bar (where it says “Apply a display filter...”), type icmp and press ENTER to see just the pings from Step 1b. **Take the screenshot.**

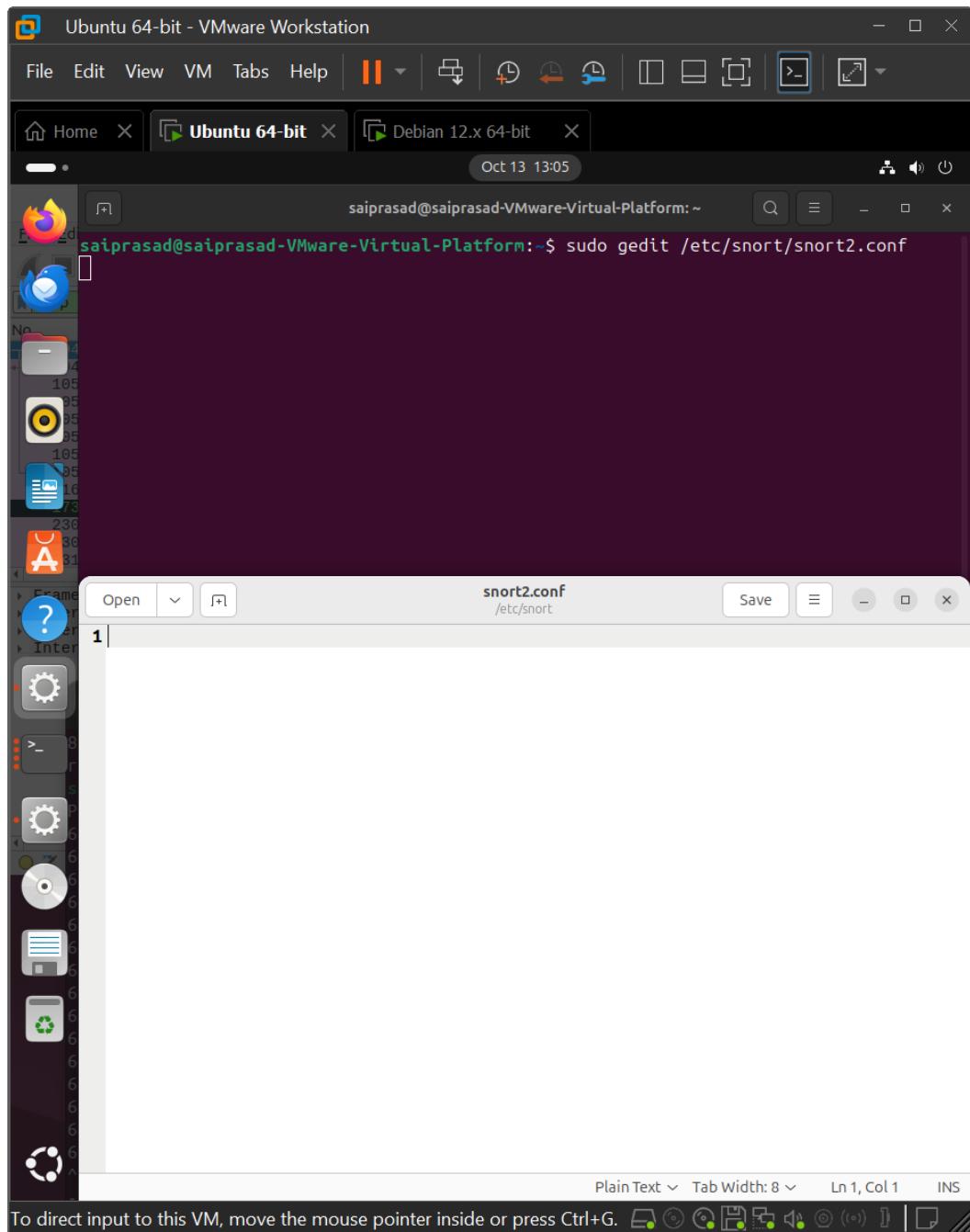


---

### Activity 3: Snort NIDS Mode (Network Intrusion Detection System)

**Step 1** Use custom and default Snort configuration files.

- Before we use Snort's default configuration file and rules, let's write a simple one, to get started: **sudo gedit /etc/snort/snort2.conf**



Use the gedit text editor to create and edit the snort2.conf file, stored in /etc/snort, which is where the default snort.conf file is. For the variable HOME\_NET (of type ipvar), use 192.168.2.0/24 if that is your network ID. Otherwise, modify it for your IP addressing scheme. The route command will show you your network ID. Add the following lines (using your network ID on line 3) to your configuration file:

```
preprocessor frag3_global: max_frags 65536
include classification.config
ipvar HOME_NET 192.168.1.0/24
var RULE_PATH /etc/snort/rules
include $RULE_PATH/local.rules
```

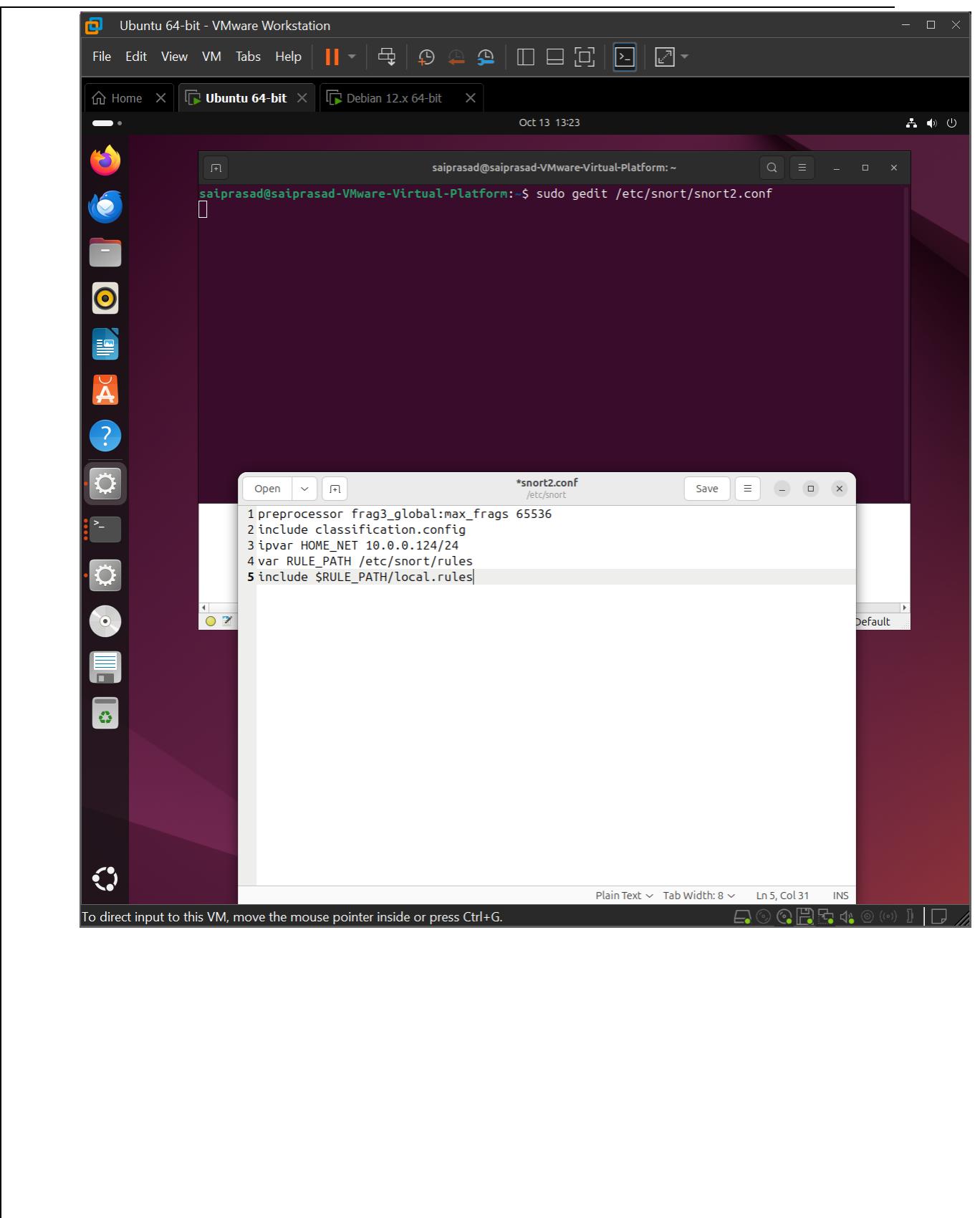
Click the red X at the top right of the screen and then click the **Save** button. This adds a minimal set of lines to the configuration file that will be used when started.

A default preprocessor is included to get rid of the message “WARNING: No preprocessors configured for policy 0.” You can read more about preprocessors, including this specific one, at:

<http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node17.html> The file, classification.config, is included.

The following is from <http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node16.html> :

The include keyword allows other snort config files to be included within the snort.conf indicated on the Snort command line. The #include from the C programming language, reading the contents of the named file, and adding the contents in the file. The include statement appears in the file.



To see the classification.config file on your system, type:

```
gedit /etc/snort/classification.config
```

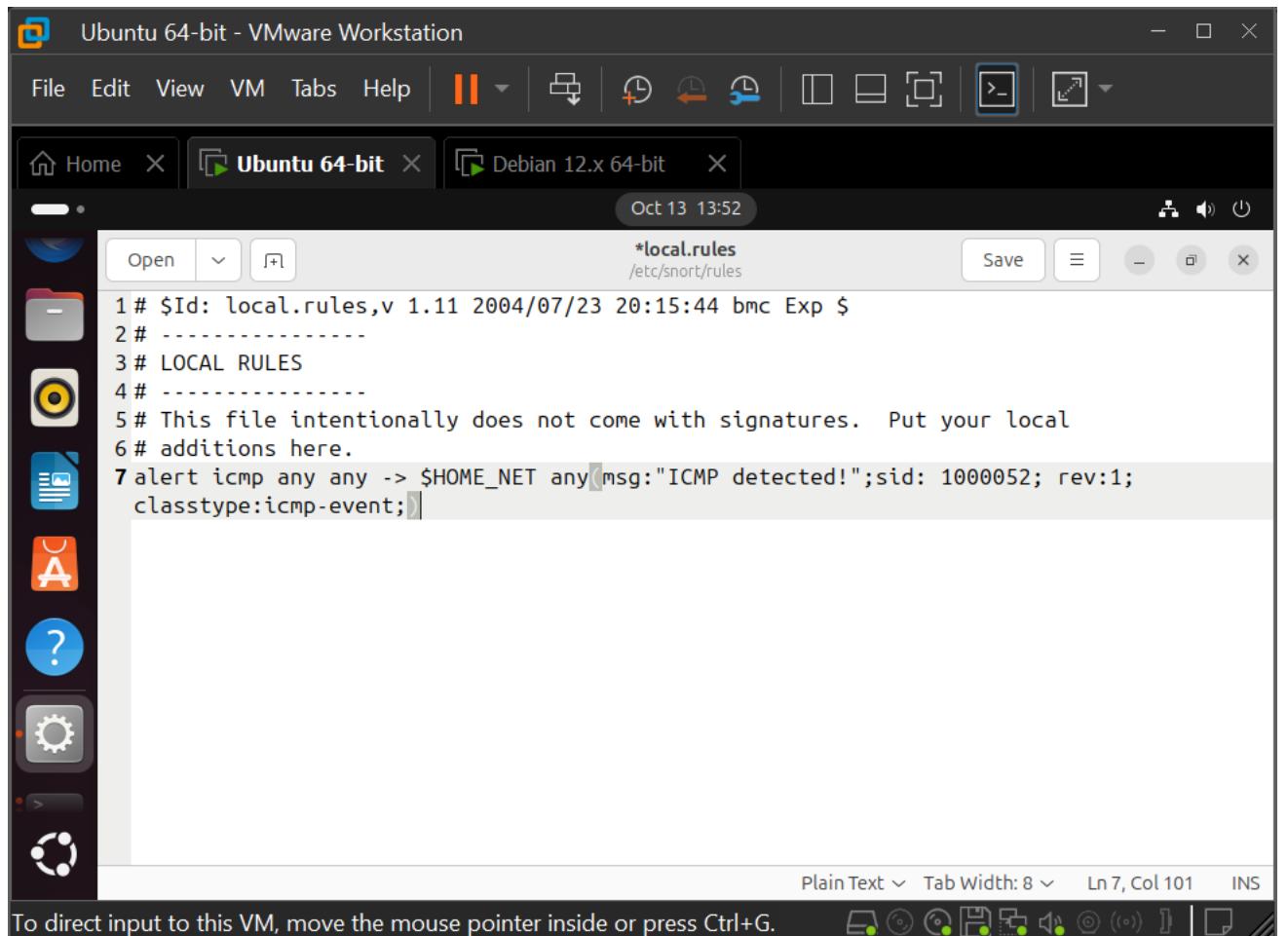
and then press **ENTER**. Take the screenshot.

For the variable RULE\_PATH (of type var), assign the value /etc/snort/rules. The include statement will expand that path (/etc/snort/rules) before /local.rules to produce an absolute reference for the rules file. Using a variable for the rule path allows you to use the variable for multiple references and also allows you to change just the RULE\_PATH variable, if necessary, as opposed to each include statement. Close **gedit** after looking through **classification.config**.

b) Enter the following command: ***sudo gedit /etc/snort/rules/local.rules***

The following is from the comments section in the file:

This file intentionally does not come with signatures. Put your local additions here. Add the following rule on one single line. Do not press ENTER to break up the line. The text will wrap, if necessary, to the next line. ***alert icmp any any -> \$HOME\_NET any (msg:"ICMP detected!";sid: 1000052; rev:1; classtype:icmp-event;)***



The screenshot shows a VMware Workstation window with two tabs: "Ubuntu 64-bit" and "Debian 12.x 64-bit". The "Ubuntu 64-bit" tab is active, displaying a terminal window. The terminal window title is "Ubuntu 64-bit" and the file path is "/etc/snort/rules". The file content is as follows:

```
1 # $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $  
2 # -----  
3 # LOCAL RULES  
4 # -----  
5 # This file intentionally does not come with signatures. Put your local  
6 # additions here.  
7 alert icmp any any -> $HOME_NET any (msg:"ICMP detected!";sid: 1000052; rev:1;  
classtype:icmp-event;)
```

The terminal window also shows status information at the bottom: "Plain Text" dropdown, "Tab Width: 8" dropdown, "Ln 7, Col 101" text, and "INS" indicator. A message at the bottom of the terminal window says "To direct input to this VM, move the mouse pointer inside or press Ctrl+G.".

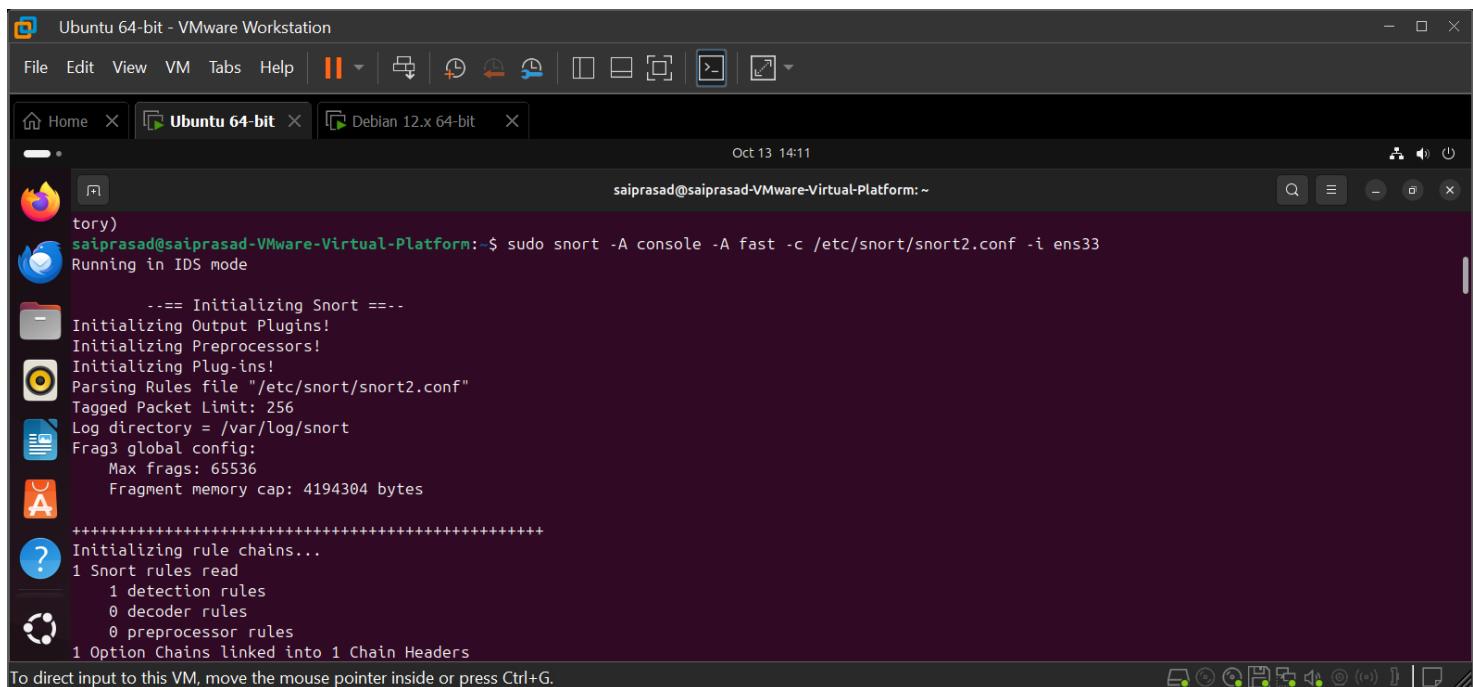
- c) Now start Snort in IDS mode and instruct it to display alerts to the console: **sudo snort -A console -A fast -c /etc/snort/snort2.conf -i ens33** Here, -c specifies the configuration file and -i specifies the interface. The following is from the Snort man page:

-A alert-mode

Alert using the specified alert-mode. Valid alert modes include fast, full, none, and unsock. Fast writes alerts to the default “alert” file in a single-line, syslog style alert message. Full writes the alert to the “alert” file with the full decoded header as well as the alert message. None turns off alerting. Unsock is an experimental mode that sends the alert information out over a UNIX socket to another process that attaches to that socket. -c config-file

Use the rules located in file config-file.

More on alert modes can be found here at <http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node6.html>



```
tory)
saiprasad@saiprasad-Virtual-Platform:~$ sudo snort -A console -A fast -c /etc/snort/snort2.conf -i ens33
Running in IDS mode

==== Initializing Snort ====
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort2.conf"
Tagged Packet Limit: 256
Log directory = /var/log/snort
Frag3 global config:
    Max frags: 65536
    Fragment memory cap: 4194304 bytes

+++++
? Initializing rule chains...
1 Snort rules read
    1 detection rules
    0 decoder rules
    0 preprocessor rules
1 Option Chains linked into 1 Chain Headers
```

- d) From the Windows 10 VM or host machine, ping the Ubuntu VM. You will notice eight ICMP alerts (four Echo Requests and four Echo Replies). **Take the screenshot.**

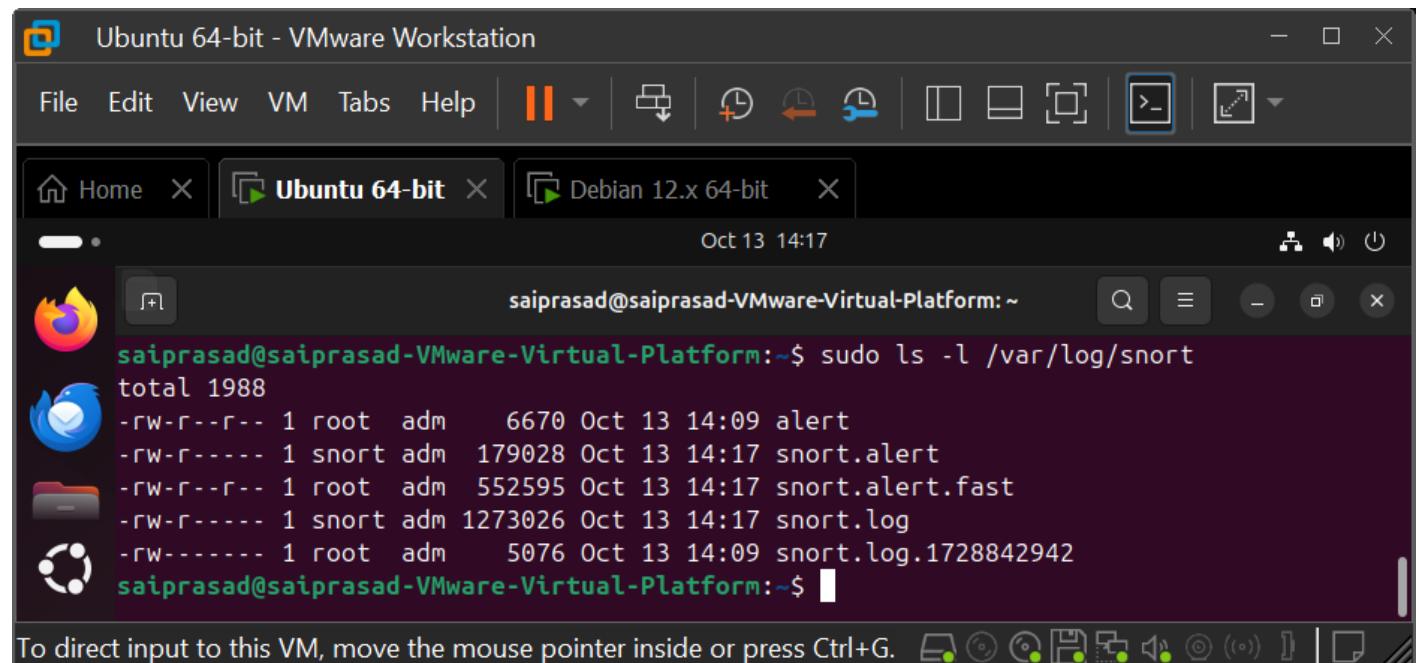
Press **CTRL-C** to break out. Notice all the information at the end of the output, including the following sections:

- Run time for packet processing      • Number of packets processed
- Memory usage summary              • Packet I/O Total
- Breakdown by protocol (includes rebuilt packets)
- Action stats                      • Frag3 statistics
- Stream statistics                • SMTP Preprocessor Statistics
- Dcerpc2 Preprocessor Statistics      • SIP Preprocessor Statistics

42



- e) Enter the following command to see the name of the log file: **sudo ls -l /var/log/snort** (Take the screenshot.)



The screenshot shows a VMware Workstation interface with a single virtual machine named "Ubuntu 64-bit". The terminal window displays the following command execution:

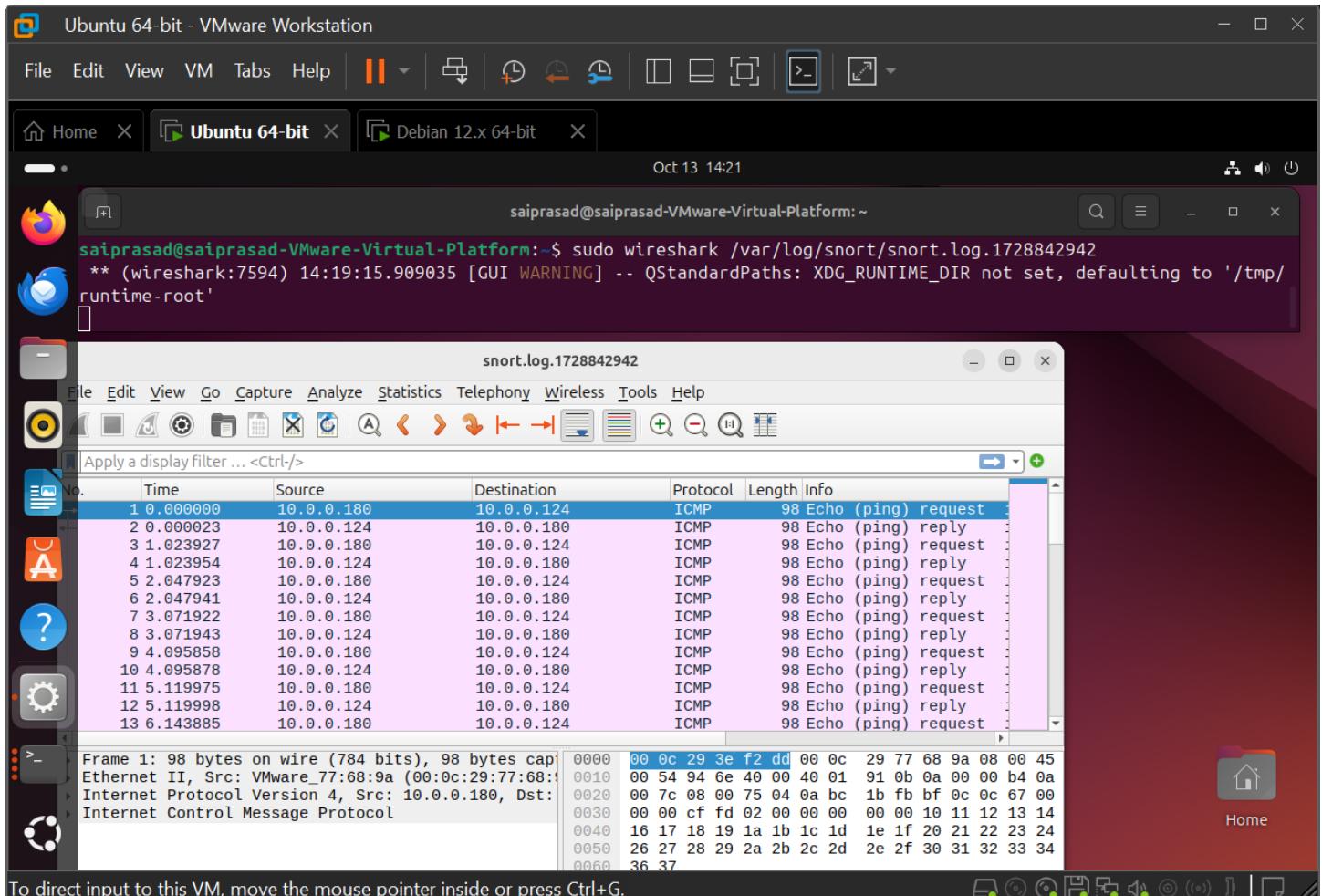
```
saiprasad@saiprasad-VMware-Virtual-Platform:~$ sudo ls -l /var/log/snort
total 1988
-rw-r--r-- 1 root adm    6670 Oct 13 14:09 alert
-rw-r----- 1 snort adm 179028 Oct 13 14:17 snort.alert
-rw-r--r-- 1 root adm 552595 Oct 13 14:17 snort.alert.fast
-rw-r----- 1 snort adm 1273026 Oct 13 14:17 snort.log
-rw----- 1 root adm    5076 Oct 13 14:09 snort.log.1728842942
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

f) Open the log file in Wireshark:

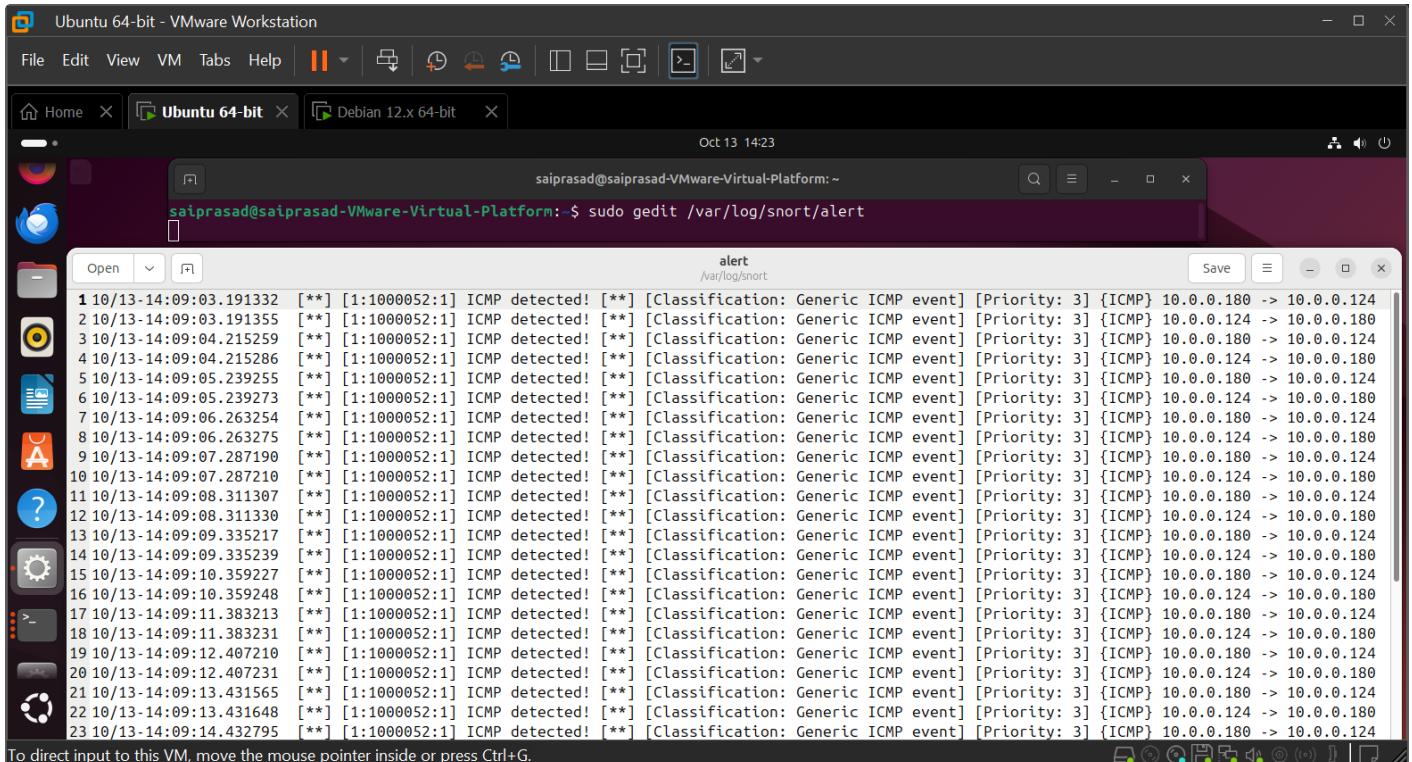
```
sudo wireshark /var/log/snort/snort.log.[numbers seen here]
```

When you get to the end of the filename in the command after snort.log., press **TAB**, and the rest of the filename, consisting of numbers, will autocomplete.



g) Open the alert file: **sudo gedit /var/log/snort/alert**

**Take the screenshot.** The file contains contents similar to what was outputted in the Terminal earlier.



The screenshot shows a Gnome desktop environment with several windows open. In the foreground, a terminal window titled 'alert' is displayed, showing the contents of the file '/var/log/snort/alert'. The terminal output lists numerous ICMP detection events from October 13, 2013, at various times between 03:19 and 14:43. Each event is timestamped and includes details such as classification, priority, and source/destination IP addresses. The terminal window has a dark theme and is located in the bottom right corner of the screen. Other windows visible in the background include a file manager, a browser, and system settings.

```
saiprasad@saiprasad-Virtual-Platform: ~$ sudo gedit /var/log/snort/alert
alert
/var/log/snort
1 10/13-14:09:03.191332 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.180 -> 10.0.0.124
2 10/13-14:09:03.191355 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.124 -> 10.0.0.180
3 10/13-14:09:04.215259 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.180 -> 10.0.0.124
4 10/13-14:09:04.215286 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.124 -> 10.0.0.180
5 10/13-14:09:05.239255 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.180 -> 10.0.0.124
6 10/13-14:09:05.239273 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.124 -> 10.0.0.180
7 10/13-14:09:06.263254 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.180 -> 10.0.0.124
8 10/13-14:09:06.263275 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.124 -> 10.0.0.180
9 10/13-14:09:07.287190 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.180 -> 10.0.0.124
10 10/13-14:09:07.287210 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.124 -> 10.0.0.180
11 10/13-14:09:08.311307 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.180 -> 10.0.0.124
12 10/13-14:09:08.311330 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.124 -> 10.0.0.180
13 10/13-14:09:09.335217 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.180 -> 10.0.0.124
14 10/13-14:09:09.335239 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.124 -> 10.0.0.180
15 10/13-14:09:10.359227 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.180 -> 10.0.0.124
16 10/13-14:09:10.359248 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.124 -> 10.0.0.180
17 10/13-14:09:11.383213 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.180 -> 10.0.0.124
18 10/13-14:09:11.383231 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.124 -> 10.0.0.180
19 10/13-14:09:12.407210 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.180 -> 10.0.0.124
20 10/13-14:09:12.407231 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.124 -> 10.0.0.180
21 10/13-14:09:13.431565 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.180 -> 10.0.0.124
22 10/13-14:09:13.431648 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.124 -> 10.0.0.180
23 10/13-14:09:14.432795 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.180 -> 10.0.0.124
```

- h) Remove the alert file and restart Snort, changing the **-A** value from **fast** to **full**: **sudo rm /var/log/snort/alert**
- sudo snort -A console -A full -c /etc/snort/snort2.conf -i ens33** From the Windows 10 VM or host machine, ping the Ubuntu VM.

You will notice eight ICMP alerts (four Echo Requests and four Echo Replies). Press **CTRL-C** to break out. The fast option has been replaced by full.

```
saiprasad@saiprasad-VMware-Virtual-Platform:~$ sudo rm /var/log/snort/alert
saiprasad@saiprasad-VMware-Virtual-Platform:~$ sudo snort -A console -A full -c /etc/snort/snort2.conf -i ens33
Running in IDS mode

     === Initializing Snort ===
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort2.conf"
Tagged Packet Limit: 256
Log directory = /var/log/snort
Frag3 global config:
    Max frags: 65536
    Fragment memory cap: 4194304 bytes

+++++
Initializing rule chains...
1 Snort rules read
    1 detection rules
    0 decoder rules
    0 preprocessor rules
1 Option Chains linked into 1 Chain Headers
+++++
+[Rule Port Counts]-
|      tcp   udp   icmp   ip
|      0     0     0     0
|      src   dst
|      0     0     0     0
|      any
|      nc
|      s+d
+-----[detection-filter-config]-
| memory-cap : 1048576 bytes
+-----[detection-filter-rules]-
| none
+-----[rate-filter-config]-
| memory-cap : 1048576 bytes
+-----[rate-filter-rules]-
| none
```

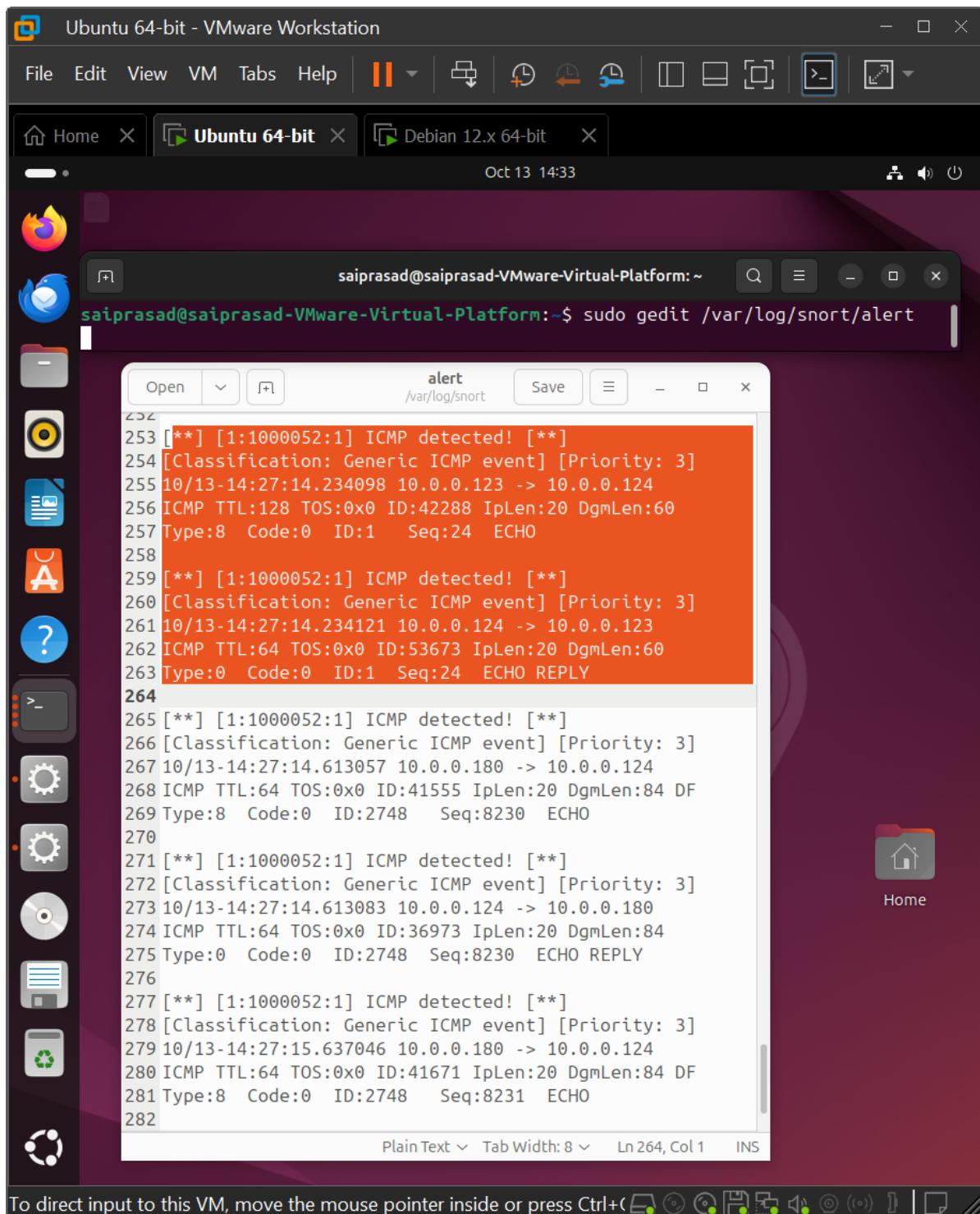
```

Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help ||| Home X Ubuntu 64-bit X Debian 12.x 64-bit X
Oct 13 14:28
saiprasad@saiprasad-VMware-Virtual-Platform:~ 
10/13-14:27:13.588991 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] [ICMP] 10.0.0.124 -> 10.0.0.180
10/13-14:27:14.234098 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] [ICMP] 10.0.0.123 -> 10.0.0.124
10/13-14:27:14.234121 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] [ICMP] 10.0.0.124 -> 10.0.0.123
10/13-14:27:14.613057 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] [ICMP] 10.0.0.180 -> 10.0.0.124
10/13-14:27:14.613083 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] [ICMP] 10.0.0.124 -> 10.0.0.180
10/13-14:27:15.637046 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] [ICMP] 10.0.0.180 -> 10.0.0.124
10/13-14:27:15.637069 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] [ICMP] 10.0.0.124 -> 10.0.0.180
^C*** Caught Int-Signal
=====
Run time for packet processing was 22.4006 seconds
Snort processed 574 packets.
Snort ran for 0 days 0 hours 0 minutes 22 seconds
Pkts/sec: 26
=====
A Memory usage summary:
Total non-mapped bytes (arena): 5025792
Bytes in mapped regions (hb1khd): 30130176
Total allocated space (uordblks): 4669600
Total free space (fordblk): 356192
Topmost releasable block (keepcost): 68016
=====
Packet I/O Totals:
Received: 583
Analyzed: 574 ( 98.456%)
Dropped: 0 ( 0.000%)
Filtered: 0 ( 0.000%)
Outstanding: 9 ( 1.544%)
Injected: 0
=====
Breakdown by protocol (includes rebuilt packets):
Eth: 574 (100.000%)
VLAN: 0 ( 0.000%)
IP4: 249 ( 43.380%)
Frag: 0 ( 0.000%)
ICMP: 48 ( 8.362%)
UDP: 92 ( 16.028%)
TCP: 90 ( 15.679%)
IP6: 318 ( 55.401%)
IP6 Ext: 321 ( 55.923%)
IP6 Opts: 6 ( 1.045%)
Frag6: 0 ( 0.000%)
ICMP6: 11 ( 1.916%)
UDP6: 264 ( 45.993%)
TCP6: 40 ( 6.969%)
Teredo: 0 ( 0.000%)
TCPS-TP: 0 ( 0.000%)
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```

- i) Enter the following command: **sudo gedit /var/log/snort/alert**

**Take the screenshot.** Notice the full IP headers (although, excluding some fields) for each alert in the alert file.

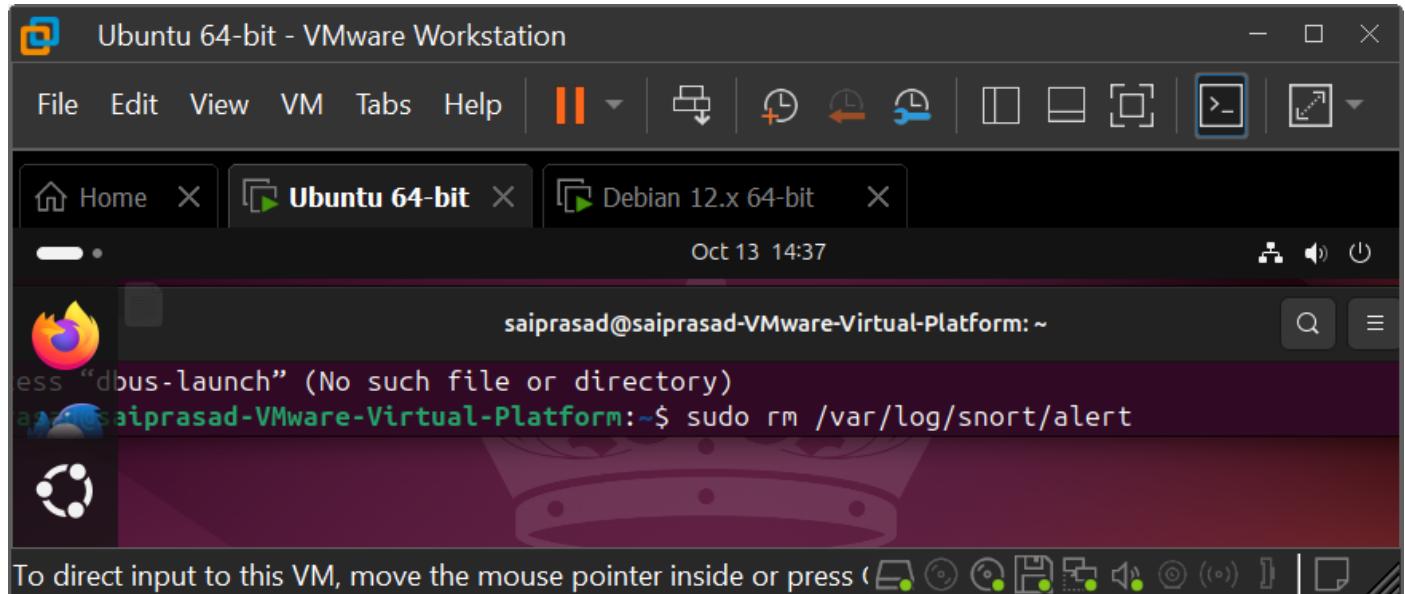


The screenshot shows a VMware Workstation interface with an Ubuntu 64-bit VM running. The terminal window displays the following log entries from /var/log/snort/alert:

```
253 [**] [1:1000052:1] ICMP detected! [**]
254 [Classification: Generic ICMP event] [Priority: 3]
255 10/13-14:27:14.234098 10.0.0.123 -> 10.0.0.124
256 ICMP TTL:128 TOS:0x0 ID:42288 IpLen:20 DgmLen:60
257 Type:8 Code:0 ID:1 Seq:24 ECHO
258
259 [**] [1:1000052:1] ICMP detected! [**]
260 [Classification: Generic ICMP event] [Priority: 3]
261 10/13-14:27:14.234121 10.0.0.124 -> 10.0.0.123
262 ICMP TTL:64 TOS:0x0 ID:53673 IpLen:20 DgmLen:60
263 Type:0 Code:0 ID:1 Seq:24 ECHO REPLY
264
265 [**] [1:1000052:1] ICMP detected! [**]
266 [Classification: Generic ICMP event] [Priority: 3]
267 10/13-14:27:14.613057 10.0.0.180 -> 10.0.0.124
268 ICMP TTL:64 TOS:0x0 ID:41555 IpLen:20 DgmLen:84 DF
269 Type:8 Code:0 ID:2748 Seq:8230 ECHO
270
271 [**] [1:1000052:1] ICMP detected! [**]
272 [Classification: Generic ICMP event] [Priority: 3]
273 10/13-14:27:14.613083 10.0.0.124 -> 10.0.0.180
274 ICMP TTL:64 TOS:0x0 ID:36973 IpLen:20 DgmLen:84
275 Type:0 Code:0 ID:2748 Seq:8230 ECHO REPLY
276
277 [**] [1:1000052:1] ICMP detected! [**]
278 [Classification: Generic ICMP event] [Priority: 3]
279 10/13-14:27:15.637046 10.0.0.180 -> 10.0.0.124
280 ICMP TTL:64 TOS:0x0 ID:41671 IpLen:20 DgmLen:84 DF
281 Type:8 Code:0 ID:2748 Seq:8231 ECHO
282
```

- j) Remove the alert file and restart Snort, using both fast and full with two -A options:

```
sudo rm /var/log/snort/alert
```



The screenshot shows a VMware Workstation interface with a single virtual machine named "Ubuntu 64-bit". The VM is currently running, as indicated by the green arrow icon in the title bar. The title bar also includes other tabs for "Home" and "Debian 12.x 64-bit". The main window contains a terminal session with the following text:  
saiprasad@saiprasad-VMware-Virtual-Platform:~\$  
ess “dbus-launch” (No such file or directory)  
saiprasad@saiprasad-VMware-Virtual-Platform:~\$ sudo rm /var/log/snort/alert  
The terminal prompt shows the user is in their home directory on the Ubuntu system. The command entered is "sudo rm /var/log/snort/alert". The output indicates that the file does not exist, which is expected since Snort has not been configured to generate alerts yet.

```
sudo snort -A console -A fast -A full -c  
/etc/snort/snort2.conf -i ens33
```

From the Windows 10 VM or host machine, ping the Ubuntu VM. You will notice eight ICMP alerts (four Echo Requests and four Echo Replies). Press **CTRL-C** to break out. Both the **full** and **fast** options are being used now.

```
Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help || Home X Ubuntu 64-bit X Debian 12.x 64-bit X
Oct 13 14:43
saiprasad@saiprasad-VMware-Virtual-Platform: ~
10/13-14:39:19.093889 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.124 -> 10.0.0.180
10/13-14:39:20.117998 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.180 -> 10.0.0.124
10/13-14:39:20.118018 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.124 -> 10.0.0.180
10/13-14:39:21.070128 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.123 -> 10.0.0.124
10/13-14:39:21.070154 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.124 -> 10.0.0.123
10/13-14:39:21.2412004 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.180 -> 10.0.0.124
10/13-14:39:21.242024 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.124 -> 10.0.0.180
10/13-14:39:22.078234 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.123 -> 10.0.0.124
10/13-14:39:22.078254 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.124 -> 10.0.0.123
10/13-14:39:22.165985 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.180 -> 10.0.0.124
10/13-14:39:22.166007 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.124 -> 10.0.0.180
10/13-14:39:23.081533 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.123 -> 10.0.0.124
10/13-14:39:23.081550 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.124 -> 10.0.0.123
10/13-14:39:23.190007 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.180 -> 10.0.0.124
10/13-14:39:23.190026 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.124 -> 10.0.0.180
10/13-14:39:24.097257 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.123 -> 10.0.0.124
10/13-14:39:24.097276 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.124 -> 10.0.0.123
10/13-14:39:24.214166 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.180 -> 10.0.0.124
10/13-14:39:24.214186 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.124 -> 10.0.0.180
10/13-14:39:25.238028 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.180 -> 10.0.0.124
10/13-14:39:25.238049 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.124 -> 10.0.0.180
10/13-14:39:26.262123 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.180 -> 10.0.0.124
10/13-14:39:26.262143 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.124 -> 10.0.0.180
10/13-14:39:27.286276 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.180 -> 10.0.0.124
10/13-14:39:27.286298 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.124 -> 10.0.0.180
^C*** Caught Int-Signal
10/13-14:39:28.310122 [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.180 -> 10.0.0.124
=====
Run time for packet processing was 16.3075 seconds
Snort processed 77 packets.
Snort ran for 0 days 0 hours 0 minutes 16 seconds
Pkts/sec: 4
=====
Memory usage summary:
Total non-mmapped bytes (arena): 5025792

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

- k) Enter the following command: **`sudo gedit /var/log/snort/alert`**

With both the fast and full options specified at the same time, you will now see output from both (one after the other) in each individual alert. **Take the screenshot.**

```
saiprasad@saiprasad-VMware-Virtual-Platform:~$ sudo gedit /var/log/snort/alert
alert
/var/log/snort
188
189 10/13-14:39:24.097257  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.123 -> 10.0.0.124
190 [**] [1:1000052:1] ICMP detected! [**]
191 [Classification: Generic ICMP event] [Priority: 3]
192 10/13-14:39:24.097276 10.0.0.124 -> 10.0.0.123
193 ICMP TTL:64 TOS:0x0 ID:3518 IpLen:20 DgmLen:60
194 Type:0 Code:0 ID:1 Seq:28 ECHO REPLY
195
196 10/13-14:39:24.097276  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.124 -> 10.0.0.123
197 [**] [1:1000052:1] ICMP detected! [**]
198 [Classification: Generic ICMP event] [Priority: 3]
199 10/13-14:39:24.214166 10.0.0.180 -> 10.0.0.124
200 ICMP TTL:64 TOS:0x0 ID:4616 IpLen:20 DgmLen:84 DF
201 Type:8 Code:0 ID:2748 Seq:8943 ECHO
202
203 10/13-14:39:24.214166  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.180 -> 10.0.0.124
204 [**] [1:1000052:1] ICMP detected! [**]
205 [Classification: Generic ICMP event] [Priority: 3]
206 10/13-14:39:24.214186 10.0.0.124 -> 10.0.0.180
207 ICMP TTL:64 TOS:0x0 ID:19627 IpLen:20 DgmLen:84
208 Type:0 Code:0 ID:2748 Seq:8943 ECHO REPLY
209
210 10/13-14:39:24.214186  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.124 -> 10.0.0.180
211 [**] [1:1000052:1] ICMP detected! [**]
212 [Classification: Generic ICMP event] [Priority: 3]
213 10/13-14:39:25.238028 10.0.0.180 -> 10.0.0.124
214 ICMP TTL:64 TOS:0x0 ID:4840 IpLen:20 DgmLen:84 DF
215 Type:8 Code:0 ID:2748 Seq:8944 ECHO
216
217 10/13-14:39:25.238028  [**] [1:1000052:1] ICMP detected! [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.180 -> 10.0.0.124
218 [**] [1:1000052:1] ICMP detected! [**]
219 [Classification: Generic ICMP event] [Priority: 3]
220 10/13-14:39:25.238049 10.0.0.124 -> 10.0.0.180
221 ICMP TTL:64 TOS:0x0 ID:20328 IpLen:20 DgmLen:84
222 Type:0 Code:0 ID:2748 Seq:8944 ECHO REPLY
```

To direct input to this VM, move the mouse pointer inside or press **Ctrl+G**.