

## Lab 7: Deep Freeze

**Course Name:** Malware Analysis and Reverse Engineering (IAM302)

**Student Name:** Nguyễn Trần Vinh – SE160258

**Instructor Name:** Mai Hoàng Đỉnh

**Lab Due Date:** 1/2/2023

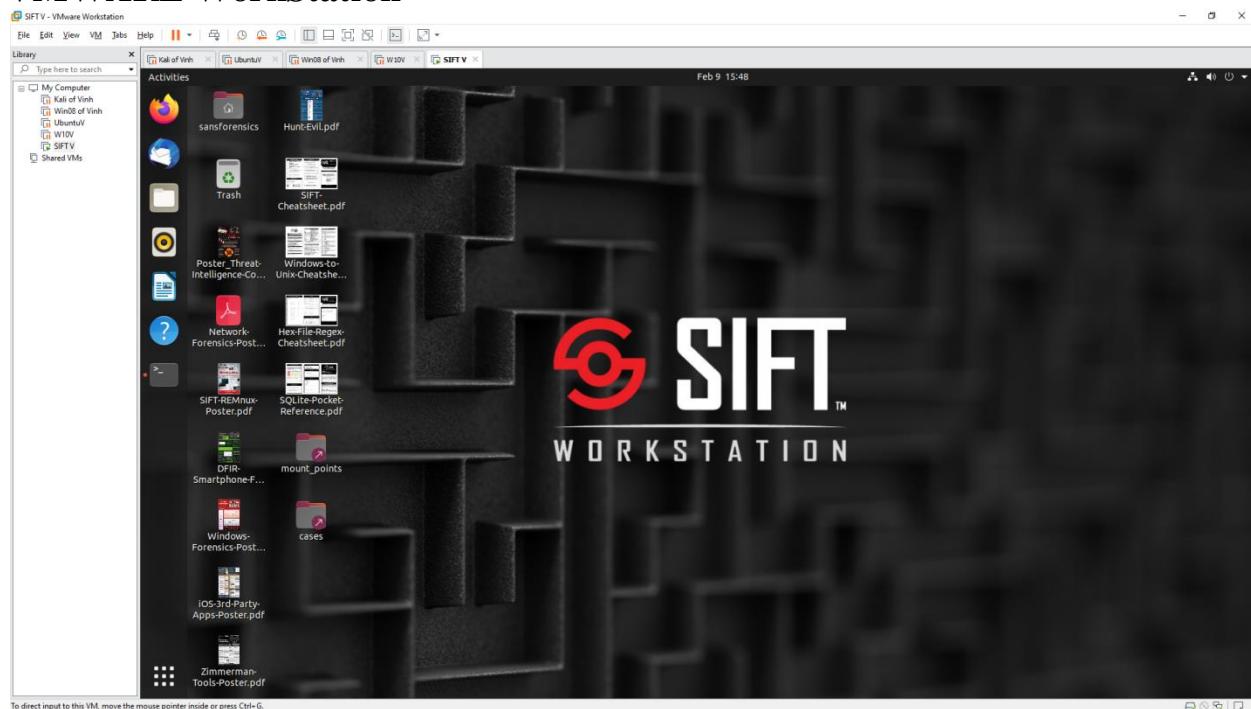
### Purpose:

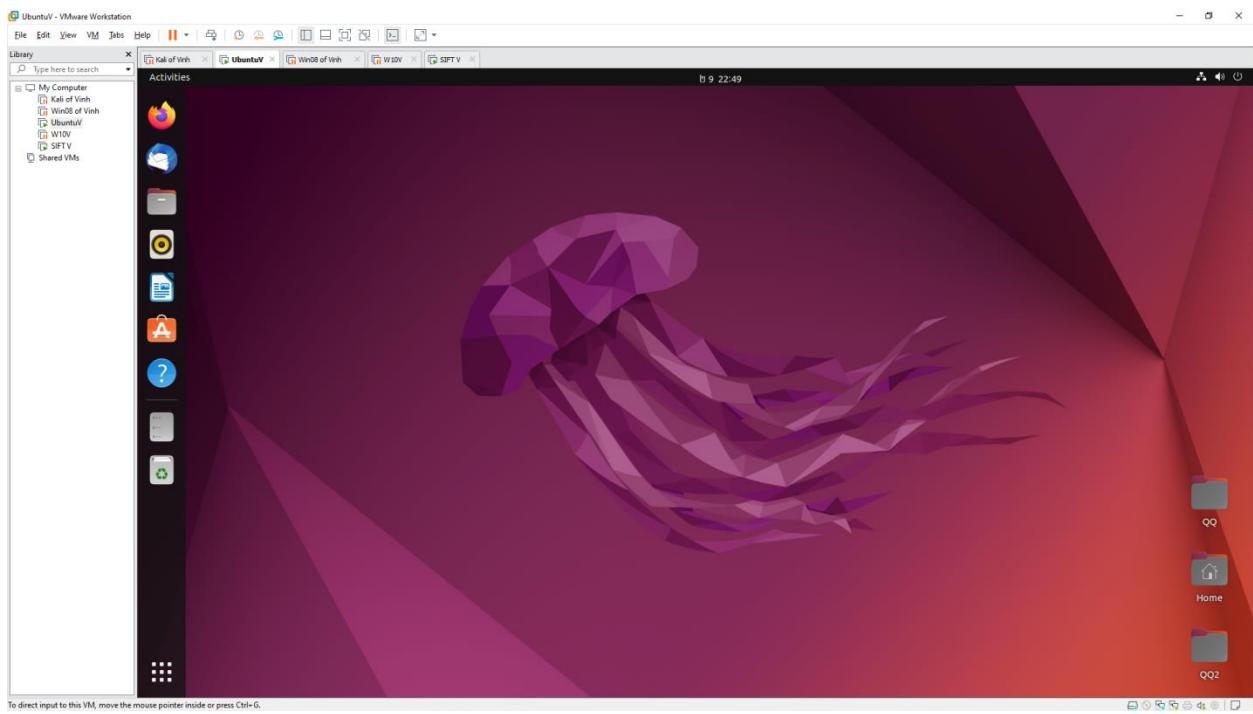
Configuring a Malware Lab Manipulating HTTP/HTTPS with Burp Suite Using Deep Freeze to Preserve Physical Systems

### What we need:

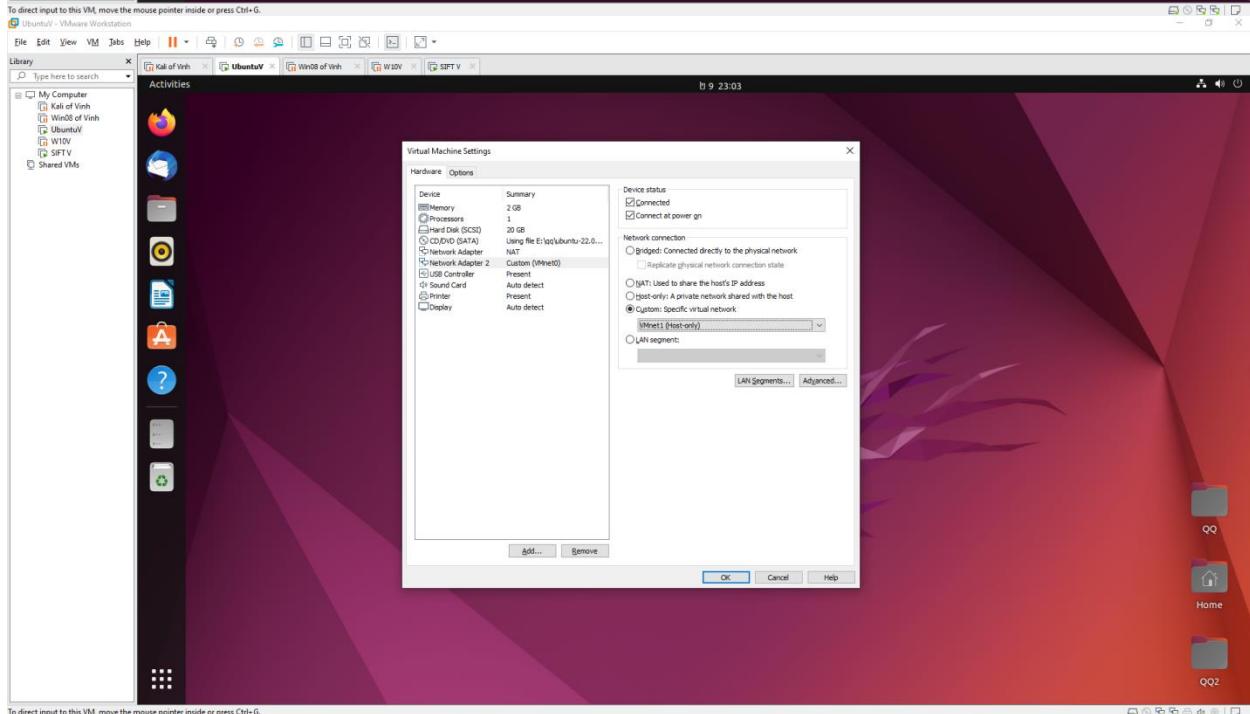
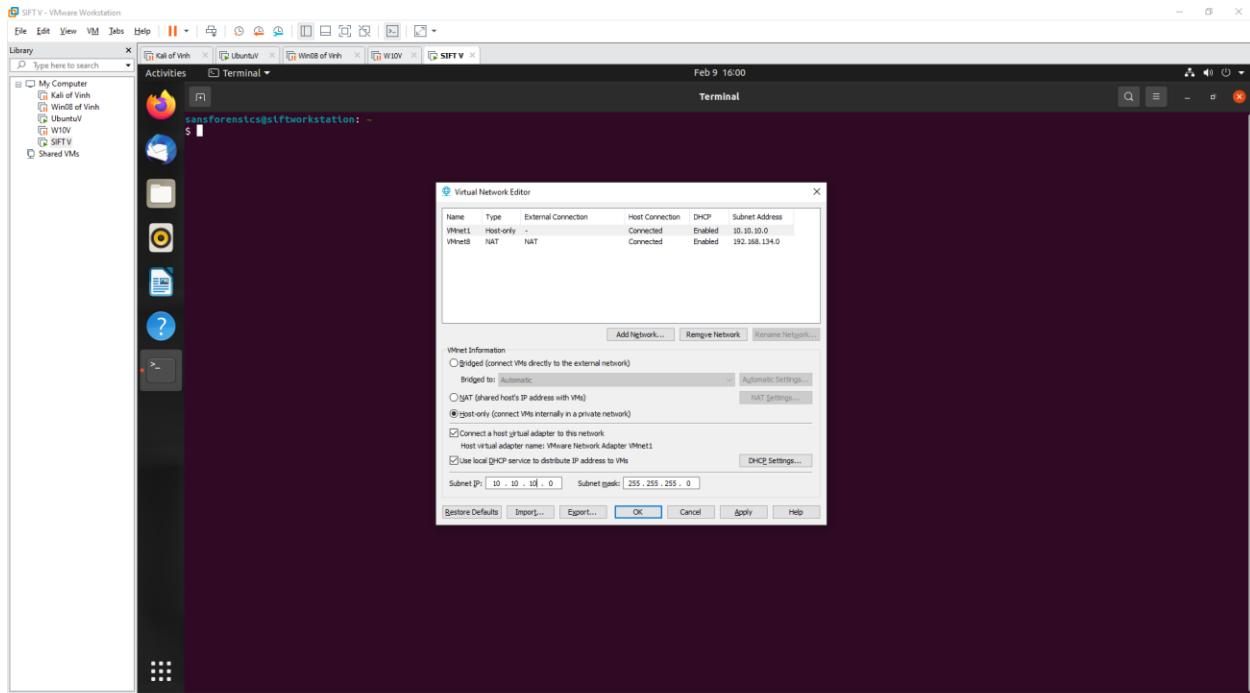
- VMWARE is not freely available open source software
- 6 network modes are available
  - Not attached, NAT, Bridged Adapter, Internal Network, Host only Adapter, Generic Driver

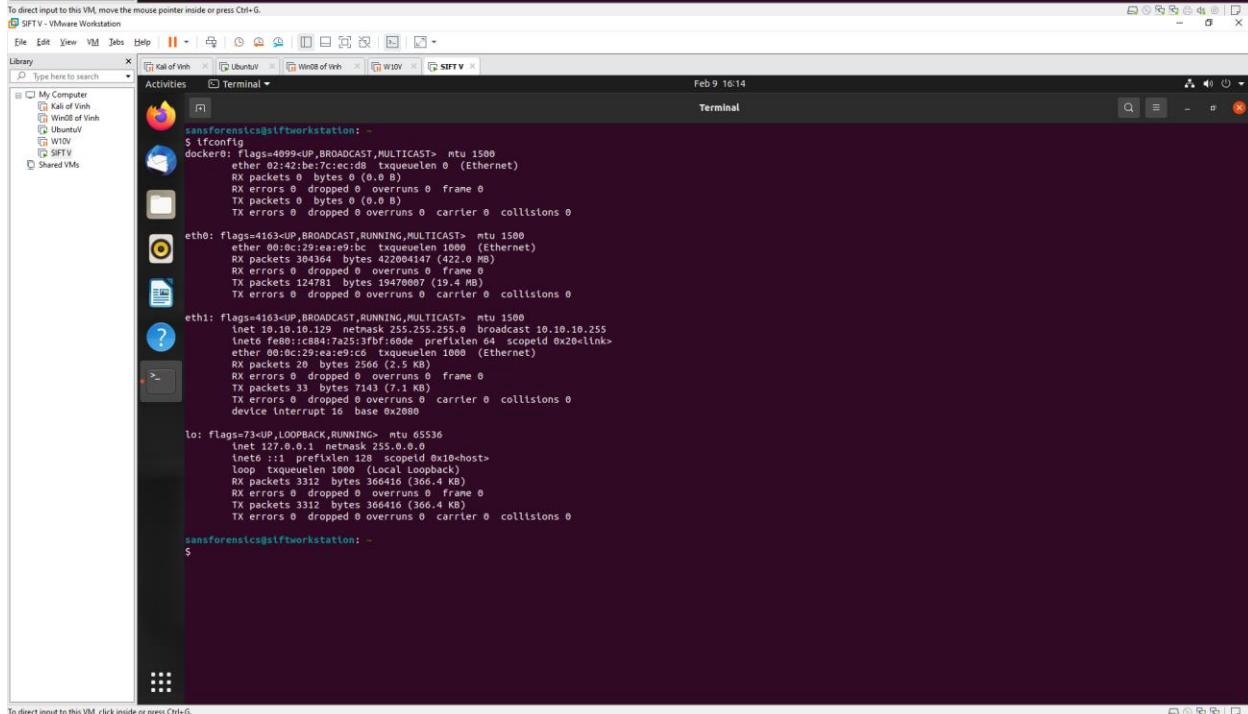
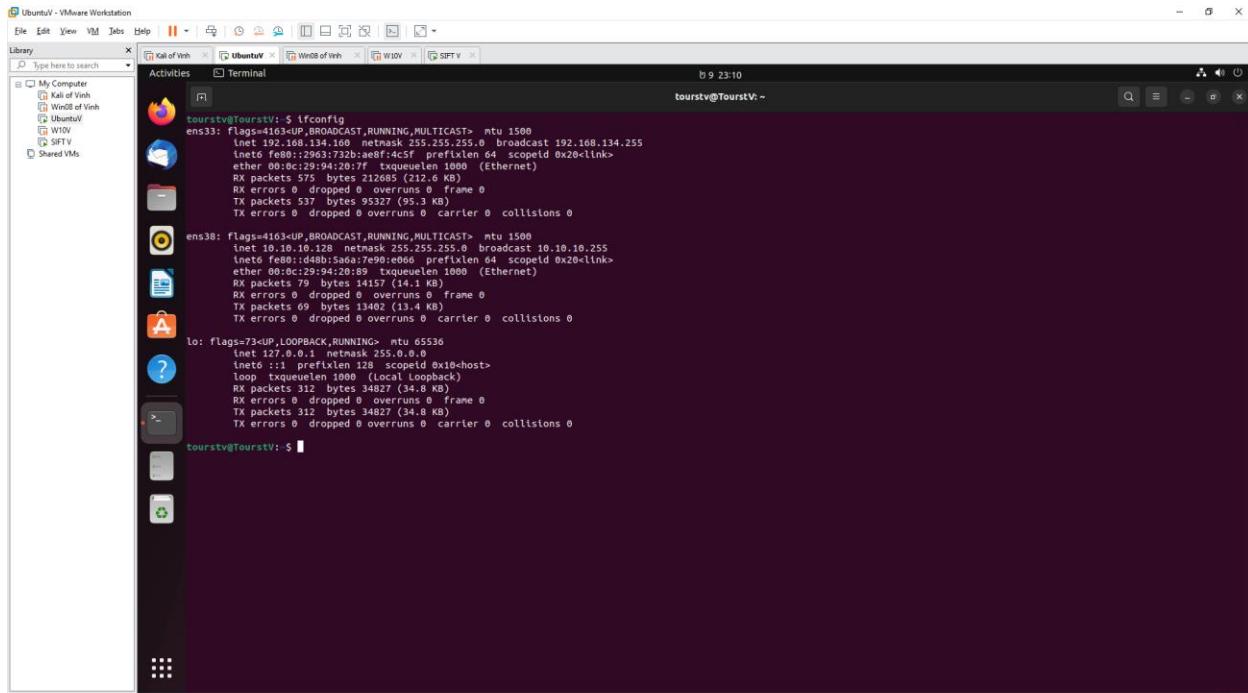
### VMWARE WorkStation





## Configurations of NETWORK on vmware workstation





The screenshot shows a Kali Linux desktop environment within a VMware Workstation window. The terminal window displays the following command and its output:

```
tourstv@TourstV: ~$ ping 10.10.10.129
PING 10.10.10.129 (10.10.10.129) 56(84) bytes of data.
64 bytes from 10.10.10.129: icmp_seq=1 ttl=64 time=1.15 ms
64 bytes from 10.10.10.129: icmp_seq=2 ttl=64 time=1.15 ms
64 bytes from 10.10.10.129: icmp_seq=3 ttl=64 time=1.15 ms
64 bytes from 10.10.10.129: icmp_seq=4 ttl=64 time=0.431 ms
64 bytes from 10.10.10.129: icmp_seq=5 ttl=64 time=0.327 ms
64 bytes from 10.10.10.129: icmp_seq=6 ttl=64 time=0.526 ms
64 bytes from 10.10.10.129: icmp_seq=7 ttl=64 time=0.271 ms
64 bytes from 10.10.10.129: icmp_seq=8 ttl=64 time=16.4 ms
...
--- 10.10.10.129 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7081ms
rtt min/avg/max/mdev = 0.271/4.761/16.376/5.844 ms
```

## Install Wireshark

- WireShark

A screenshot of a Linux desktop environment, likely Ubuntu, within a VMware Workstation window. The desktop has a dark theme with a dock at the bottom containing icons for Home, Applications, Dash, and others. A terminal window is open in the center, showing the command line interface for installing Wireshark. The terminal output includes package dependencies and upgrade information, such as 'libbz2-1.0-6' being upgraded to '1.0.6-1'. The desktop also shows a file manager window with a folder named 'Kali of Win8' and a library window listing various virtual machines.

- tshark

Ubuntu - VMware Workstation

File Edit View VM Help

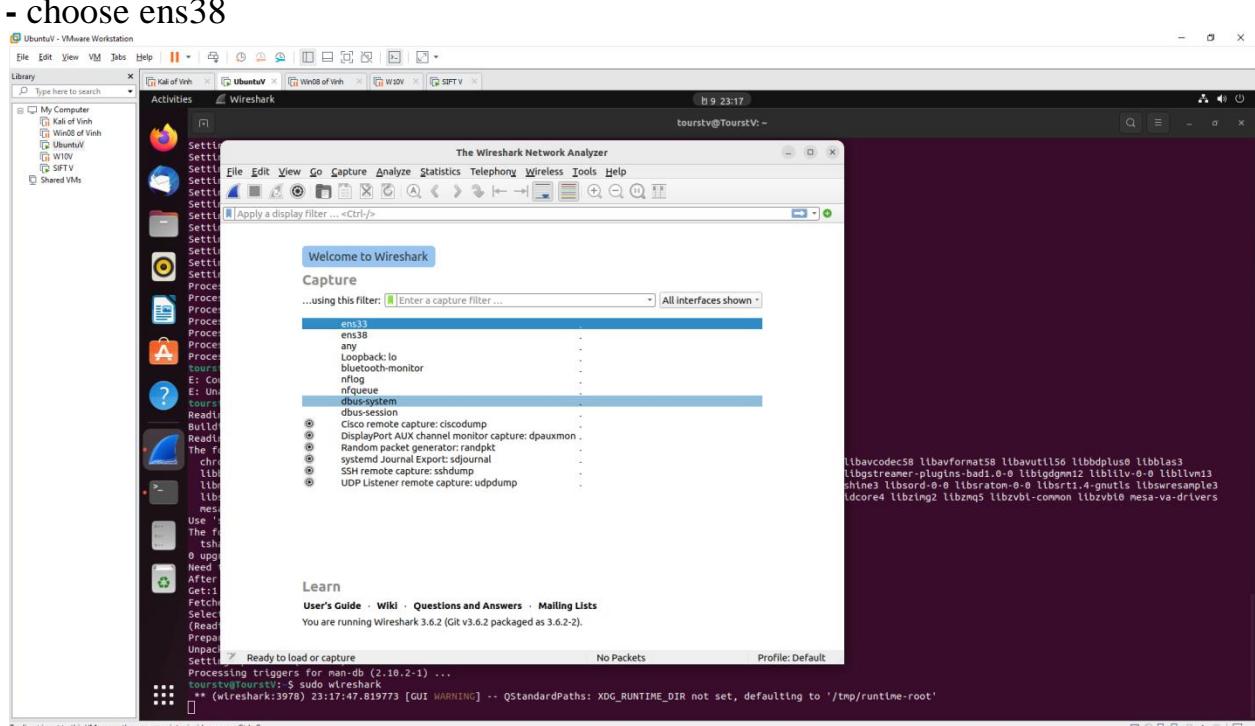
Library Type here to search

Kali of Vnsh Ubuntu WindOf Vnsh W10V SIFT V

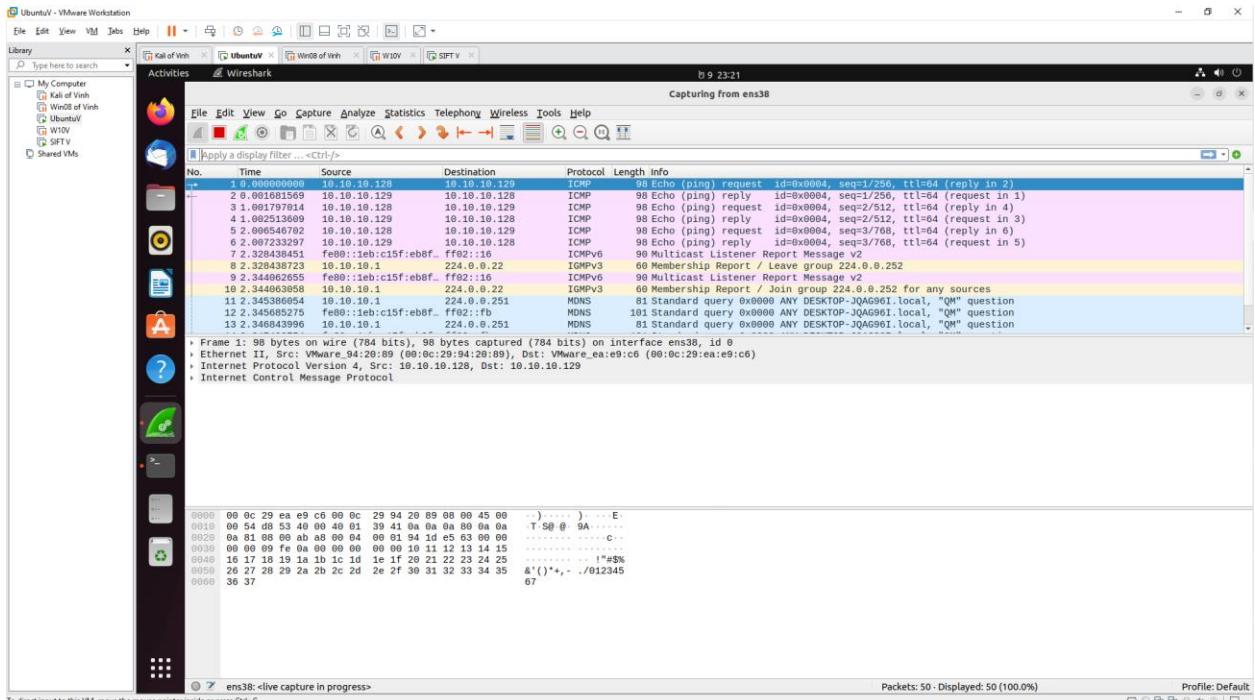
Activities Terminal b 9 23:17 tourstv@TourstV: ~

```
Setting up libqt5core5a:amd64 (5.15.3-3dfsg-2ubuntu0.2) ...
Setting up libqt5鲜hresh-dtata (3.6.2-2) ...
Setting up libqt5鲜hresh-鲜d (3.6.2-2) ...
Setting up libqt5SqlDbus:amd64 (5.15.3-3dfsg-2ubuntu0.2) ...
Setting up liblmb4c0:amd64 (0.4.8-1) ...
Setting up libqt5Networks:amd64 (5.15.3-3dfsg-2ubuntu0.2) ...
Setting up liblwfreshark15:amd64 (3.6.2-2) ...
Setting up wireshark-common (3.6.2-2) ...
Setting up libqt5SqlSrp:amd64 (5.15.3-3dfsg-2ubuntu0.2) ...
Setting up libqt5Sqlcipher:amd64 (5.15.3-3dfsg-2ubuntu0.2) ...
Setting up qt5-gtk-platformtheme:amd64 (5.15.3-3dfsg-2ubuntu0.2) ...
Setting up libqt5Multimedia5:amd64 (5.15.3-1) ...
Setting up libqt5PrintSupports:amd64 (5.15.3-3dfsg-2ubuntu0.2) ...
Setting up libqt5MultimediaWidgets5:amd64 (5.15.3-1) ...
Setting up libqt5Multimedia5-plugins:amd64 (5.15.3-1) ...
Setting up libqt5Svg5:amd64 (5.15.3-1) ...
Setting up wireshark-qt (3.6.2-2) ...
Setting up wireshark (3.6.2-2) ...
Processing triggers for man-db (2.10.2-1)
Processing triggers for shared-mime-info (2.1-2) ...
Processing triggers for mlocate (3.70+nut-mutubunt1) ...
Processing triggers for desktop-file-utils (0.26-1ubuntu3) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for gnome-menus (3.13.1-0.1ubuntu3) ...
Processing triggers for ufw (0.35-1) ...
Reading package lists... Done
Building dependency tree... Done
Reading status information... Done
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi intel-media-va-driver libaaacs0 libbam3 libbass9 libavcodec58 libavformat58 libavutil56 libbdplus libblbas3 libbluray libbts2b0 libchromaprint libcodecc1-1.0 libdavids liblflashrom liblflite1 liblfrtd1-2 libgme0 libbsm1 libgstreamer-plugins-bad1.0 liblbgdm11 liblbt1-0-0 liblbb1m13 libmfx1 libmysqfa1 libnorm1 libvapenpmto libbpm-5.3-0 libpostprocess librabitmq4 librubberband2 libserd-0-0 libshine3 liblsord-0-0 librato1.4-0 libsrat1.4-grnult libswresample3 libswscale4 libufreadriver libvba-drn2 libvba-wxayland2 libvba-x11-2 libvdpau libvldstab1.1 libx26-199 libxvidcore4 libzing2 libzmq5 libzbv1l-common libzbv1l-mesa-va-drivers libzv1l-vdpau libzv1l-vdpau-all libzv1l-vdpau-driver-all
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  tshark
0 upgraded, 1 newly installed, 0 to remove and 6 not upgraded.
Need to get 139 kB of archives.
After this operation, 433 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu jammy/universe amd64 tshark amd64 [3.6.2-2 [157 kB]
Fetched 157 kB in 1s (134 kB/s)
Selecting previously unselected package tshark.
(Reading database ... 70%
```

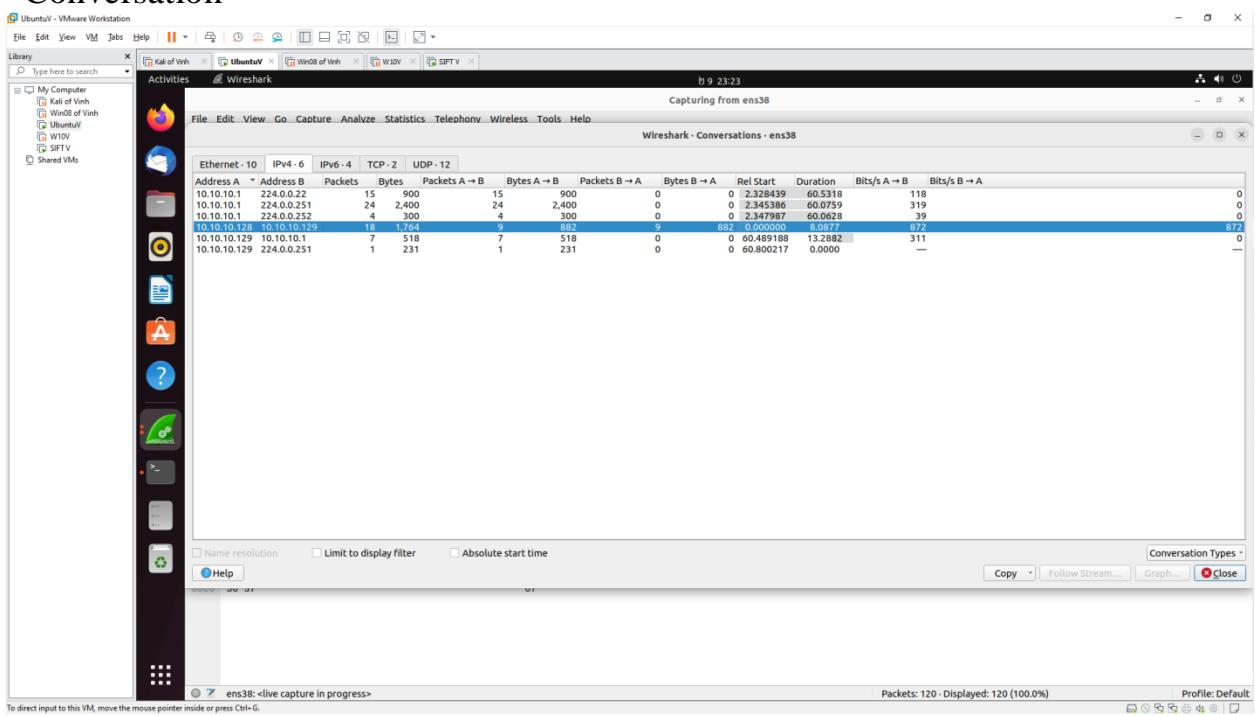
To direct input to this VM, move the mouse pointer inside or press Ctrl+G



# CAPTURE PACKET BY WIRESHARK



## - Conversation



## Install InetSim

Install:

```

apt-get install libnet-server-perl
apt-get install libnet-dns-perl
apt-get install libipc-shareable-perl
    
```

```
apt-get install libdigest-sha-perl  
apt-get install libio-socket-ssl-perl  
apt-get install iptables-dev
```

```
Ubuntu1 - VMware Workstation
File Edit View VM Jobs Help ||| Kill of Vmh Ubuntu1* Win10 of Vmh Win10 SFTY
Library Type here to search
Activities Terminal tourstv@TourstV: ~
tourstv@TourstV: ~
64 bytes from 10.10.10.129: icmp_seq=1 ttl=64 time=1.09 ms
64 bytes from 10.10.10.129: icmp_seq=2 ttl=64 time=0.737 ms
64 bytes from 10.10.10.129: icmp_seq=3 ttl=64 time=0.735 ms
64 bytes from 10.10.10.129: icmp_seq=4 ttl=64 time=0.572 ms
64 bytes from 10.10.10.129: icmp_seq=5 ttl=64 time=0.533 ms
64 bytes from 10.10.10.129: icmp_seq=6 ttl=64 time=0.533 ms
64 bytes from 10.10.10.129: icmp_seq=7 ttl=64 time=0.14 ms
64 bytes from 10.10.10.129: icmp_seq=8 ttl=64 time=0.342 ms
64 bytes from 10.10.10.129: icmp_seq=9 ttl=64 time=0.706 ms
...
-- 10.10.10.129 ping statistics --
9 packets transmitted, 9 received, 0% packet loss, time 8087ms
rtt min/avg/max/mdev = 0.342/1.565/5.834/1.726 ms
tourstv@TourstV: ~ $ sudo apt-get install libnet-server-perl
[sudo] password for tourstv:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
chromium-codesc-ffmpeg-extra gstreamer1.0-vaapi_1.965+va-driver_1.1.0-1~deb10u1 media-player libbaacs0 libbaa3 libbass9 libavcodec58 libavformat58 libavutil56 libbdplus0 libblbas3
liblburay2 libbbs2b0 libchromaprint libcodecs2_1.0 libdavids libflashrom libflite1 libftdi1-2 libgme0 libgsml libgstreamer-plugins-bad1.0-0 libigdgmm12 liblily-0-0 libllm13
liblircclient liblircmd liblircmd2 liblircrc liblircrc2 liblircrc3 liblircrc4 liblircrc5 liblircrc6 liblircrc7 liblircrc8 liblircrc9 liblircrc10 liblircrc11 liblircrc12 liblircrc13
liblircrc14 liblircrc15 liblircrc16 liblircrc17 liblircrc18 liblircrc19 liblircrc20 liblircrc21 liblircrc22 liblircrc23 liblircrc24 liblircrc25 liblircrc26 liblircrc27 liblircrc28
liblircrc29 liblircrc30 liblircrc31 liblircrc32 liblircrc33 liblircrc34 liblircrc35 liblircrc36 liblircrc37 liblircrc38 liblircrc39 liblircrc40 liblircrc41 liblircrc42 liblircrc43
mesa-vdpau-drivers pocketphinx-en-us va-driver-all vdpau-driver-all
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
libfcgi-fast-perl libfcgi-pm-perl libfcgi-bin libfcgi-perl libfcgi-ldbl libio-multiplex-perl liblio-socket-inet6-perl libnet-cidr-perl libsockets-perl
Suggested packages:
liblircrc20-perl
The following NEW packages will be installed:
libfcgi-fast-perl libfcgi-pm-perl libfcgi-bin libfcgi-perl libfcgi-ldbl libio-multiplex-perl liblio-socket-inet6-perl libnet-cidr-perl libnet-server-perl libsockets-perl
0 upgraded, 10 newly installed, 0 to remove and 6 not upgraded.
Need to get 493 kB of archives.
After this operation, 1,395 kB of additional disk space will be used.
Do you want to continue? [Y/n]
Get:1 http://archive.ubuntu.com/ubuntu jammy/main amd64 libfcgi-pm-perl all 2.4.5-1 [188 kB]
Get:2 http://archive.ubuntu.com/ubuntu jammy/main amd64 libfcgi-ldbl amd64 2.4.2-2build2 [28.0 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy/main amd64 libfcgi-perl amd64 2.4.2-2build2 [22.8 kB]
Get:4 http://archive.ubuntu.com/ubuntu jammy/main amd64 libfcgi-fast-perl all 1.2.15-1 [10.5 kB]
Get:5 http://archive.ubuntu.com/ubuntu jammy/main amd64 libfcgi-bin amd64 2.4.2-2build2 [11.2 kB]
Get:6 http://archive.ubuntu.com/ubuntu jammy/main amd64 libfcgi-socket-inet6-perl amd64 2.4.2-2build2 [20.7 kB]
Get:7 http://archive.ubuntu.com/ubuntu jammy/main amd64 libsockets-perl amd64 0.29-1build1 [19.7 kB]
Get:8 http://archive.ubuntu.com/ubuntu jammy/main amd64 liblio-socket-inet6-perl all 2.23.1-1 [14.7 kB]
Get:9 http://archive.ubuntu.com/ubuntu jammy/main amd64 libnet-cidr-perl all 0.21-1 [14.4 kB]
Get:10 http://archive.ubuntu.com/ubuntu jammy/main amd64 libnet-server-perl all 2.009-2 [166 kB]
Fetched 493 kB in 3s (189 kB/s)
```

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

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

```
Ubuntu 6 - VMware Workstation
File Edit View VM Help
Activities Terminal 9:23:25
tourstv@TourstV: ~
tourstv@TourstV: ~
tourstv@TourstV: ~

Type here to search
Kali of Vnsh Ubuntu 6 Wind of Vnsh W10V SFTV
Activities Terminal tourstv@TourstV: ~
tourstv@TourstV: ~

Selecting previously unselected package libdigest-hmac-perl.
Preparing to unpack .../libdigest-hmac-perl_1.04-0dfsg_1_all.deb ...
Unpacking libdigest-hmac-perl (1.04-0dfsg) ...
Selecting previously unselected package libnet-ip-perl.
Preparing to unpack .../libnet-ip-perl_1.26-2_all.deb ...
Unpacking libnet-ip-perl (1.26-2) ...
Selecting previously unselected package libnet-dns-perl.
Preparing to unpack .../libnet-dns-perl_1.33-1_all.deb ...
Unpacking libnet-dns-perl (1.33-1) ...
Selecting previously unselected package libnet-dns-sec-perl.
Preparing to unpack .../libnet-dns-sec-perl_1.19-1build2_amd64.deb ...
Unpacking libnet-dns-sec-perl (1.19-1build2) ...
Selecting previously unselected package libnet-libidn-perl.
Preparing to unpack .../libnet-libidn-perl_0.12.ds-3build6_amd64.deb ...
Unpacking libnet-libidn-perl (0.12.ds-3build6) ...
Selecting previously unselected package libperlio-corelibs-perl.
Preparing to unpack .../libperlio-corelibs-perl_0.004-2_all.deb ...
Unpacking libperlio-corelibs-perl (0.004-2) ...
Setting up libperlio-corelibs-perl (0.004-2) ...
Selecting previously unselected package libdigest-bubblebabble-perl.
Setting up libdigest-bubblebabble-perl (0.13.ds-3build6) ...
Setting up libnet-ip-perl (1.26-2) ...
Setting up libdigest-bubblebabble-perl (0.02-2.1) ...
Setting up libnet-dns-perl (1.33-1) ...
Setting up libnet-dns-sec-perl (1.19-1build2) ...
Processing triggers for man-db (2.10.2-1)
tourstv@TourstV: ~ sudo apt-get install libipc-shareable-perl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libcomerr1 libcomerr1-firmware extra git-repo1er1.8-vapiti_1.965-via-driver intel-mediuva-driver libbaacs0 libbaon3 libbass9 libbavcdec58 libbayformat58 libbayutil56 libbbddplus0 libblases3 libbluray2 libbsbs2bo libchromaprint libcodecs2-1.0 libdavids libflashrom libfbtl1 libftdi2-1 libgme0 libgsnl libgstcameraplugins-bad1.0-0 liblqdpmi12 liblvi-0-0 liblvim13 liblxflib myllysofa1 libmorn1 libmp3lrb0 libmp3lrb0 libpostproc55 librabitmq4 librubberband2 libserd-0-0 libsrat0n-0-0 libsrat0n-1-4 gnutls libswresamples3 libwscale5 libxdrread libxva2 libxwayland2 libxvba-2.1 libxvba libxvdpau libxvidstab1.1 libxv265-199 libxvldcore4 libzimg2 libzmq5 libzbvbi-common libzbvb0 mesa-va-drivers mesa-vdpau-drivers pocketphinx-en-us va-driver-all vdpau-driver-all
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libcomon-sense-perl libjison-perl libjison-xs-perl liblstring-crc32-perl libtypes-serialiser-perl
The following NEW packages will be installed:
  libcomon-sense-perl libipc-shareable-perl libjison-perl libjison-xs-perl liblstring-crc32-perl libtypes-serialiser-perl
  0 upgraded, 0 newly installed, 0 to remove and 6 not upgraded.
  Need to get 258 kB of archives.
  After this operation, 760 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu jammy/main amd64 libcommon-sense-perl amd64 3.75-2build1 [21.1 kB]
  0% [1 libcommon-sense-perl 0 B/21.1 kB 0%]
```

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

Ubuntu VM - VMware Workstation

File Edit View VM Tools Help

Library Type here to search

Kali of Vinh Ubuntu VM Win8B of Vinh SIFTY

Activities Terminal tourstv@TourstV: ~

tourstv@TourstV: ~

tourstv@TourstV: ~

Unpacking libjson-perl (0.40000-1) ...  
Selecting previously unselected package libattrng-crc32-perl:amd64.  
Preparing to unpack .../libstring-crc32-perl\_2.100-1build1\_amd64.deb ...  
Unpacking libstring-crc32-perl:amd64 (2.100-1build1) ...  
Selecting previously unselected package liblpc-shareable-perl.  
Preparing to unpack .../liblpc-shareable-perl\_1.06-2\_all.deb ...  
Unpacking liblpc-shareable-perl (1.06-2) ...  
Selecting previously unselected package libtypes-serialiser-perl.  
Preparing to unpack .../libtypes-serialiser-perl\_1.01-1\_all.deb ...  
Unpacking libtypes-serialiser-perl (1.01-1) ...  
Selecting previously unselected package libjson-xs-perl.  
Preparing to unpack .../libjson-xs-perl\_4.030-1build3\_amd64.deb ...  
Unpacking libjson-xs-perl (4.030-1build3) ...  
Setting up libcommon-sense-perl:amd64 (3.75-2build1) ...  
Setting up libstring-crc32-perl:amd64 (2.100-1build1) ...  
Setting up liblpc-shareable-perl (1.06-2) ...  
Setting up libjson-perl (4.04000-1) ...  
Setting up libjson-xs-perl (4.030-1build3) ...  
Setting up liblpc-shareable-perl (1.06-2) ...  
Processing triggers for man-db (2.10.2-1) ...  
tourstv@TourstV: ~\$ sudo apt-get install libdigest-sha-perl  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi\_1.965-va-driver intel-media-va-driver libbaacs0 libbaa3 libbasecodecs8 libbaformat58 libbautil56 libbdplus0 libbbals3 libbluray2 libbbs2b0 libchromaprint libcodec2\_1.0 libdavids libflashrom libffite1 libftdi1-2 libgme0 libgsml libgstreamer-plugins-bad1.0 liblqdpm12 libllyb0-0 liblvdgm12 libllyb1m13 liblxf1 liblxf2 liblxf3 libopenpmp0 libpbgm-5.3-0 libpostproc55 librabbitmq4 librubberband2 libserd-0-0 libshines1 libsrord-0-0 libsratom-0-0 libsrtr1.4-grnnts libswresample3 libtiff4 libtiff5 libvdpau-driver libvdpau-driver-all libvdpau-driver-all libvdpau-driver-all mesa-vdpau-drivers pocketphinx-en-us va-driver-all vdpau-driver-all  
Use "sudo apt autoremove" to remove them.  
The following NEW packages will be installed:  
libdigest-sha-perl  
0 upgraded, 1 newly installed, 0 to remove and 6 not upgraded.  
After this operation, 128 kB of additional disk space will be used.  
Get: http://archive.ubuntu.com/ubuntu jammy/universe amd64 libdigest-sha-perl amd64 6.02-1build4 [45.2 kB]  
Fetched 45.2 kB in 2s (18.3 kB/s)  
Selecting previously unselected package libdigest-sha-perl.  
(Reading database ... 206581 files and directories currently installed.)  
Preparing to unpack .../libdigest-sha-perl\_6.02-1build4\_amd64.deb ...  
Adding file 'libdigest-sha-perl' to /bin/shasum.bundled by libdigest-sha-perl'  
Adding 'diversion of /usr/share/man/man1/shasum1.gz to /usr/share/man/man1/shasum.bundled.1.gz by libdigest-sha-perl'  
Unpacking libdigest-sha-perl (6.02-1build4) ...  
Setting up libdigest-sha-perl (6.02-1build4) ...  
Processing triggers for man-db (2.10.2-1) ...

```
Ubuntu - VMware Workstation
File Edit View VM Jobs Help ||| Kali of Vnsh Ubuntu Win7 of Vnsh W10V SIFTY
Library Type here to search
Activities Terminal 9 23:26
tourstv@TourstV: ~
tourstv@TourstV: ~
chromium-codecs-ffmpeg-extra gstreamer-1.0-vaapi_1.065-va-driver intel-media-va-driver libbaacs0 libbam3 libbass9 libavcodec58 libavformat58 libavutil56 libbdblplus0 libblas3 libblray2 libchromaprint libcodecs1.0 libdavids libflashrom libftdi1-2 libgmed libgsm1 libgsreamer-plugins-bad1.0-0 liblbidgsm12 liblbtv-0-0 liblbtvml13 liblfrx1 libosifof libmnl1 libomp5.1-5.3-0 libpostproc55 librabbitmq librubberband2 libserd-0-0 libshine1 libsrard-0-0 libsratom-0-0 libsrts1.4-grutls libswresamples3 libswscale5 libvdrread1 libva-drm2 libva-wayland2 libva-x11-2 libvba libvdpau libvidstab1.1 libx265-199 libxvldcore4 libzimg2 libzmq5 libzvbl-common libzbvbl mesa-va-drivers mesa-vdpau-drivers pocketphinx-en-us va-driver-all vdpau-driver-all
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
chromium-codecs-ffmpeg-extra gstreamer-1.0-vaapi_1.065-va-driver intel-media-va-driver libbaacs0 libbam3 libbass9 libavcodec58 libavformat58 libavutil56 libbdblplus0 libblas3 libblray2 libchromaprint libcodecs1.0 libdavids libflashrom libftdi1-2 libgmed libgsm1 libgsreamer-plugins-bad1.0-0 liblbidgsm12 liblbtv-0-0 liblbtvml13 liblfrx1 libosifof libmnl1 libomp5.1-5.3-0 libpostproc55 librabbitmq librubberband2 libserd-0-0 libshine1 libsrard-0-0 libsratom-0-0 libsrts1.4-grutls libswresamples3 libswscale5 libvdrread1 libva-drm2 libva-wayland2 libva-x11-2 libvba libvdpau libvidstab1.1 libx265-199 libxvldcore4 libzimg2 libzmq5 libzvbl-common libzbvbl mesa-va-drivers mesa-vdpau-drivers pocketphinx-en-us va-driver-all vdpau-driver-all
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
chromium-codecs-ffmpeg-extra gstreamer-1.0-vaapi_1.065-va-driver intel-media-va-driver libbaacs0 libbam3 libbass9 libavcodec58 libavformat58 libavutil56 libbdblplus0 libblas3 libblray2 libchromaprint libcodecs1.0 libdavids libflashrom libftdi1-2 libgmed libgsm1 libgsreamer-plugins-bad1.0-0 liblbidgsm12 liblbtv-0-0 liblbtvml13 liblfrx1 libosifof libmnl1 libomp5.1-5.3-0 libpostproc55 librabbitmq librubberband2 libserd-0-0 libshine1 libsrard-0-0 libsratom-0-0 libsrts1.4-grutls libswresamples3 libswscale5 libvdrread1 libva-drm2 libva-wayland2 libva-x11-2 libvba libvdpau libvidstab1.1 libx265-199 libxvldcore4 libzimg2 libzmq5 libzvbl-common libzbvbl mesa-va-drivers mesa-vdpau-drivers pocketphinx-en-us va-driver-all vdpau-driver-all
Need to get 45.2 kB of archives.
After this operation, 128 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu jammy/universe amd64 liblbidgest-sha-perl amd64 6.02~ub1d4 [45.2 kB]
Fetched:45.2 kB in 2s (18.3 kB/s)
Selecting previously unselected package liblbidgest-sha-perl.
(Reading database ... 26051 files and directories currently installed.)
Preparing to unpack .../liblbidgest-sha-perl_6.02~ub1d4_amd64.deb ...
Adding 'diversion of /usr/bin/shasum to /usr/bin/shasum.bundled by liblbidgest-sha-perl'
Adding 'diversion of /usr/share/man/man1/shasum.1.gz to /usr/share/man/man1/shasum.bundled.1.gz by liblbidgest-sha-perl'
Unpacking liblbidgest-sha-perl (6.02~ub1d4) ...
Selecting previously unselected package libio-socket-ssl-perl.
Processing triggers for man-db (2.10.2-1)
tourstv@TourstV: ~$ sudo apt-get install libio-socket-ssl-perl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
libio-socket-ssl-perl is already the newest version (2.074-2).
libio-socket-ssl-perl set to manually installed.
The following packages were automatically installed and are no longer required:
chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi_1.065-va-driver intel-media-va-driver libbaacs0 libbam3 libbass9 libavcodec58 libavformat58 libavutil56 libbdblplus0 libblas3 libblray2 libchromaprint libcodecs1.0 libdavids libflashrom libftdi1-2 libgmed libgsm1 libgsreamer-plugins-bad1.0-0 liblbidgsm12 liblbtv-0-0 liblbtvml13 liblfrx1 libosifof libmnl1 libomp5.1-5.3-0 libpostproc55 librabbitmq librubberband2 libserd-0-0 libshine1 libsrard-0-0 libsratom-0-0 libsrts1.4-grutls libswresamples3 libswscale5 libvdrread1 libva-drm2 libva-wayland2 libva-x11-2 libvba libvdpau libvidstab1.1 libx265-199 libxvldcore4 libzimg2 libzmq5 libzvbl-common libzbvbl mesa-va-drivers mesa-vdpau-drivers pocketphinx-en-us va-driver-all vdpau-driver-all
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
tourstv@TourstV: ~$ sudo apt-get install iptables-dev
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Package iptables-dev is not available, but is referred to by another package.
This may mean that the package is missing, has been obsoleted, or
is only available from another source
However the following packages replace it:
libxtables-dev:1.8.6 libipq4tc-dev:1.8.6 libxttables-dev libipq4tc-dev libip4tc-dev
E: Package 'iptables-dev' has no installation candidate
tourstv@TourstV: ~
```

## Dowload the INetSim

```
dpkg -i inetsim_1.2.4-1_all.deb
```

```

tourstv@TourstV:~$ sudo apt-get update -y
Get:1 http://archive.ubuntu.com/ubuntu jammy InRelease [119 kB]
Get:2 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [107 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy-backports InRelease [107 kB]
Get:4 http://archive.ubuntu.com/ubuntu jammy-security InRelease [109 kB]
Get:5 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 DEP-11 Metadata [102 kB]
Get:6 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 DEP-11 Metadata [265 kB]
Get:7 http://archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 DEP-11 Metadata [540 kB]
Get:8 http://archive.ubuntu.com/ubuntu jammy-backports/main amd64 DEP-11 Metadata [8,000 B]
Get:9 http://archive.ubuntu.com/ubuntu jammy-backports/universe amd64 DEP-11 Metadata [13.3 kB]
Get:10 http://archive.ubuntu.com/ubuntu jammy-security/main amd64 DEP-11 Metadata [41.6 kB]
Get:11 http://archive.ubuntu.com/ubuntu jammy-security/universe amd64 DEP-11 Metadata [13.3 kB]
Fetched 779 kB in 3s (285 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Package iptables-dev is not available, but is referred to by another package.
This may mean that the package is missing, has been obsoleted, or
is only available from another source.
However the following packages replace it:
  libxtables-dev:i386 libipqtc-dev:i386 libiptables-dev libip6tc-dev libipt4tc-dev

E: Package 'iptables-dev' has no installation candidate
tourstv@TourstV:~$ wget http://www.inetsim.org/debian/binary/inetnsim_1.2.4-1_all.deb
--2023-02-09 23:29:00 5 85.214.152.164 Connecting to www.inetsim.org (www.inetsim.org)|85.214.152.164|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 298772 (292K) [application/x-debian-package]
Saving to: 'inetnsim_1.2.4-1_all.deb'

inetnsim_1.2.4-1_all.deb          100%[=====] 291.77K   343KB/s   in 0.9s
2023-02-09 23:29:00 (343 kB/s) - 'inetnsim_1.2.4-1_all.deb' saved [298772/298772]

tourstv@TourstV:~$ ls
Desktop  Documents  Downloads  inetnsim_1.2.4-1_all.deb  Music  Pictures  Public  snap  Templates  Videos
tourstv@TourstV:~$ 

```

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

```

tourstv@TourstV:~$ sudo apt-get update -y
Get:4 http://archive.ubuntu.com/ubuntu jammy-backports InRelease [107 kB]
Get:5 http://archive.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:6 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 DEP-11 Metadata [102 kB]
Get:7 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 DEP-11 Metadata [265 kB]
Get:8 http://archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 DEP-11 Metadata [540 kB]
Get:9 http://archive.ubuntu.com/ubuntu jammy-backports/main amd64 DEP-11 Metadata [8,000 B]
Get:10 http://archive.ubuntu.com/ubuntu jammy-backports/universe amd64 DEP-11 Metadata [12.4 kB]
Get:11 http://archive.ubuntu.com/ubuntu jammy-security/main amd64 DEP-11 Metadata [41.6 kB]
Get:12 http://archive.ubuntu.com/ubuntu jammy-security/universe amd64 DEP-11 Metadata [13.3 kB]
Fetched 779 kB in 3s (285 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Package iptables-dev is not available, but is referred to by another package.
This may mean that the package is missing, has been obsoleted, or
is only available from another source.
However the following packages replace it:
  libxtables-dev:i386 libipqtc-dev:i386 libiptables-dev libip6tc-dev libipt4tc-dev

E: Package 'iptables-dev' has no installation candidate
tourstv@TourstV:~$ wget http://www.inetsim.org/debian/binary/inetnsim_1.2.4-1_all.deb
--2023-02-09 23:28:58- 85.214.152.164 Connecting to www.inetsim.org (www.inetsim.org)|85.214.152.164|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 298772 (292K) [application/x-debian-package]
Saving to: 'inetnsim_1.2.4-1_all.deb'

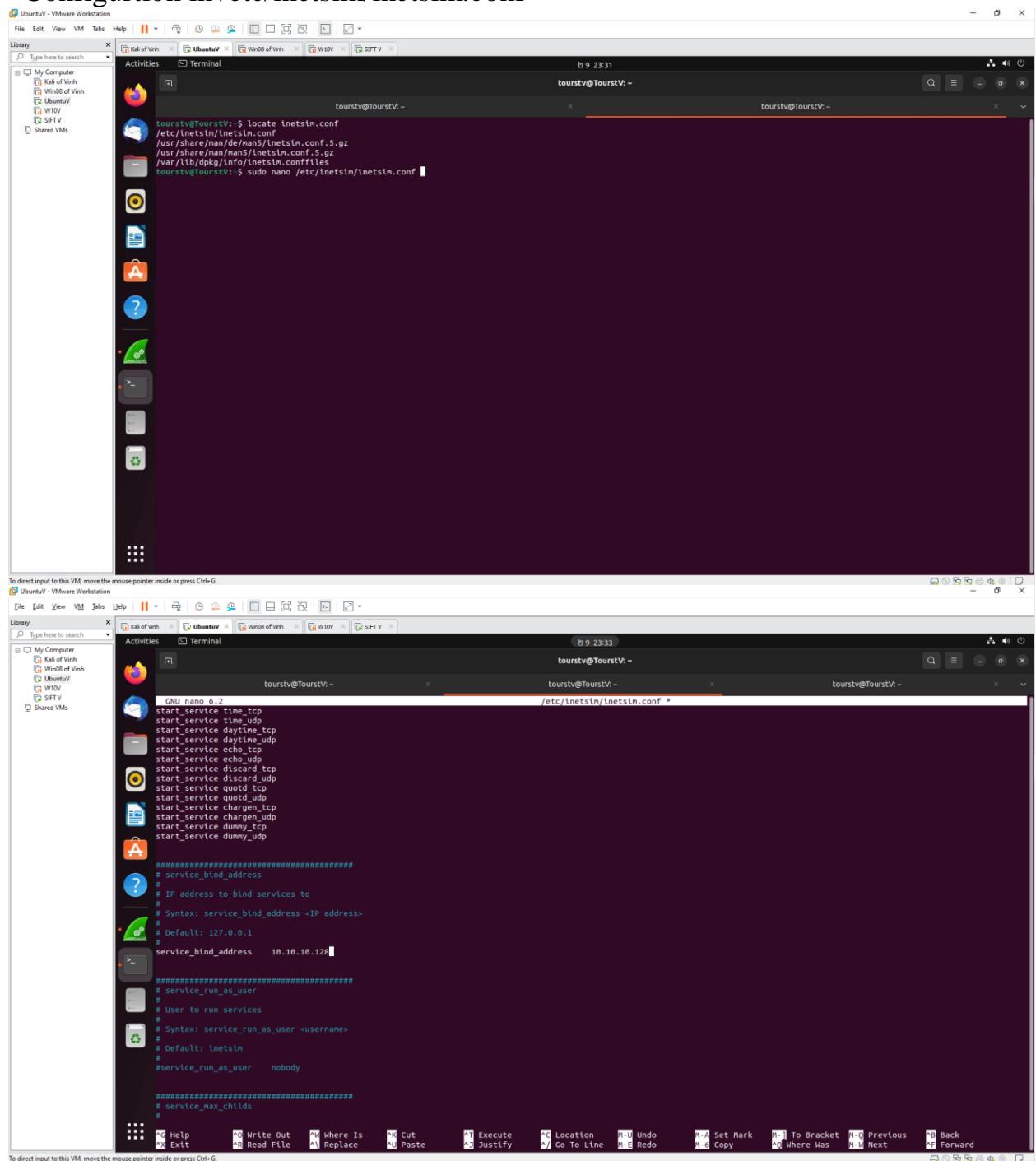
inetnsim_1.2.4-1_all.deb          100%[=====] 291.77K   343KB/s   in 0.9s
2023-02-09 23:29:00 (343 kB/s) - 'inetnsim_1.2.4-1_all.deb' saved [298772/298772]

tourstv@TourstV:~$ ls
Desktop  Documents  Downloads  inetnsim_1.2.4-1_all.deb  Music  Pictures  Public  snap  Templates  Videos
tourstv@TourstV:~$ sudo dpkg -i inetnsim_1.2.4-1_all.deb
Selecting previously unselected package inetnsim.
(Reading database ... 20066 files and directories currently installed.)
Preparing to unpack .../inetnsim_1.2.4-1_all.deb ...
Unpacking inetnsim (1.2.4-1) ...
Setting up inetnsim (1.2.4-1) ...
Creating default SSL key and certificate... done.
Processing triggers for man-db (2.10.2-1) ...
tourstv@TourstV:~$ ls
Desktop  Documents  Downloads  inetnsim_1.2.4-1_all.deb  Music  Pictures  Public  snap  Templates  Videos
tourstv@TourstV:~$ 

```

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

## - Configuration in /etc/inetsim/inetsim.conf



```
tourstv@TourstV: ~$ locate inetsim.conf
/etc/inetsim/inetsim.conf
/usr/share/man/de/man5/inetsim.conf.5.gz
/usr/share/man/man5/inetsim.conf.5.gz
/var/lib/dpkg/info/inetsim.conffiles
tourstv@TourstV: ~$ sudo nano /etc/inetsim/inetsim.conf
```

```
GNU nano 6.2
start_service time_tcp
start_service time_udp
start_service daytime_tcp
start_service daytime_udp
start_service echo_tcp
start_service echo_udp
start_service discard_tcp
start_service discard_udp
start_service quod_tcp
start_service quod_udp
start_service chargen_tcp
start_service chargen_udp
start_service dummy_tcp
start_service dummy_udp

#####
# service_bind_address
# IP address to bind services to
# Syntax: service_bind_address <IP address>
# Default: 127.0.0.1
# service_bind_address 10.10.10.128

#####
# service_run_as_user
# User to run services
# Syntax: service_run_as_user <username>
# Default: inetsim
# service_run_as_user nobody

#####
# service_max_childs
#
```

```
tourstv@TourstV:~
```

```
tourstv@TourstV:~
```

```
/etc/lnetsim/lnetsim.conf *
```

```
GNU nano 6.2
```

```
#dunnnny_banner_walt      3
```

```
#####
```

```
# Redirect
```

```
#####
```

```
# redirect_enabled
```

```
# Turn connection redirection on or off.
```

```
# Syntax: redirect_enabled [yes|no]
```

```
# Default: no
```

```
redirect_enabled      yes
```

```
#####
```

```
# redirect_unknown_services
```

```
# Redirect connection attempts to unbound ports
```

```
to dummy service
```

```
# Syntax: redirect_unknown_services [yes|no]
```

```
# Default: yes
```

```
redirect_unknown_services      no
```

```
#####
```

```
# redirect_external_address
```

```
# IP address used as source address if INetSim
```

```
acts as a router for redirecting packets to
```

```
external networks.
```

```
# This option only takes effect if static rules
```

```
for redirecting packets to external networks
```

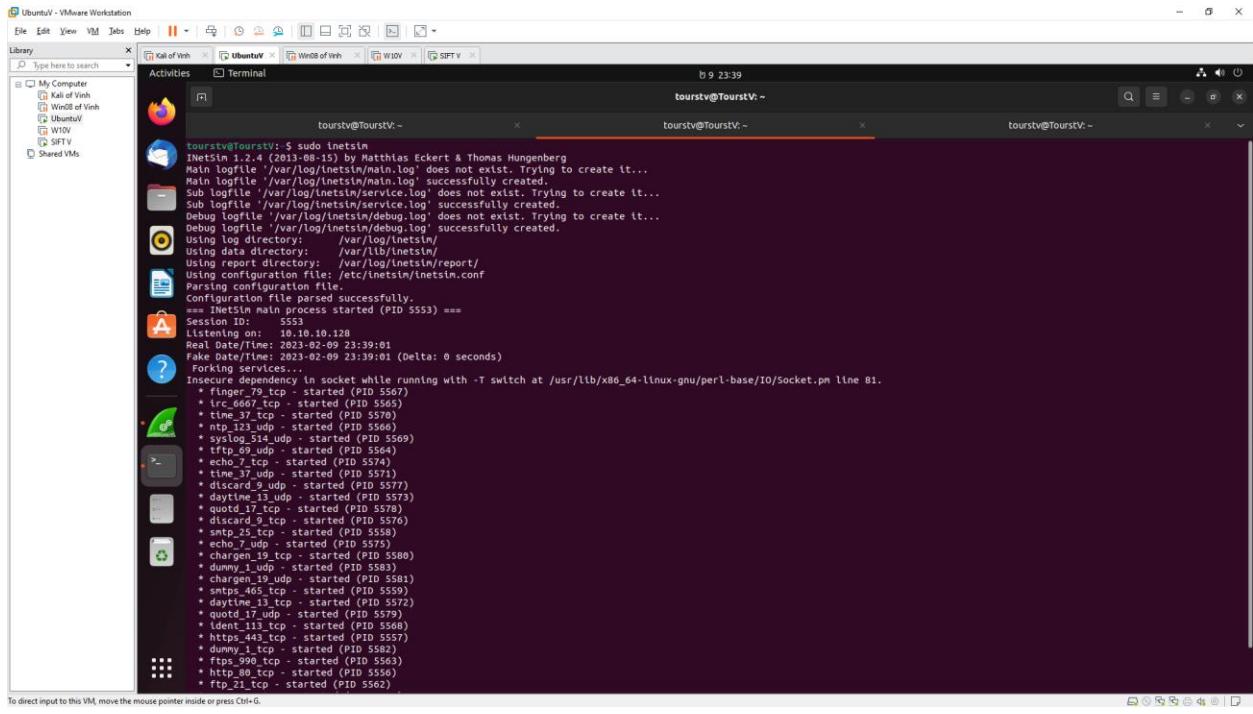
```
are defined (see 'redirect_static_rule' below).
```

```
GNU nano 6.2
#redirect_static_rule    icmp 10.10.10.20:echo-request 10.1.0.25
#
# Redirection based on IP address and/or port:
#redirect_static_rule    tcp 10.10.10.55:88 10.10.1.1:80
#redirect_static_rule    tcp 10.10.10.20:99 192.168.1.1:25
#redirect_static_rule    tcp 10.10.10.20: 172.16.1.2:
#####
# redirect_change_ttl
# Change the time-to-live header field to a random value
# in outgoing IP packets.
#
# Syntax: redirect_change_ttl [yes|no]
# Default: no
#
#redirect_change_ttl yes

#####
# redirect_exclude_port
# Connections to <service_bind_address> on this port
# are not redirected
#
# Syntax: redirect_exclude_port <protocol:port>
# Default: none
#
#redirect_exclude_port      tcp:22
#redirect_exclude_port      udp:111

#####
# redirect_ignore_bootp
#
# If set to 'yes', BOOTP (DHCP) broadcasts will not be redirected
# (UDP packets with source address 0.0.0.0, port 68 and
# destination address 255.255.255.255, port 67 or vice versa)
#
# Syntax: redirect_ignore_bootp [yes|no]
```

## **sudo inetsim**

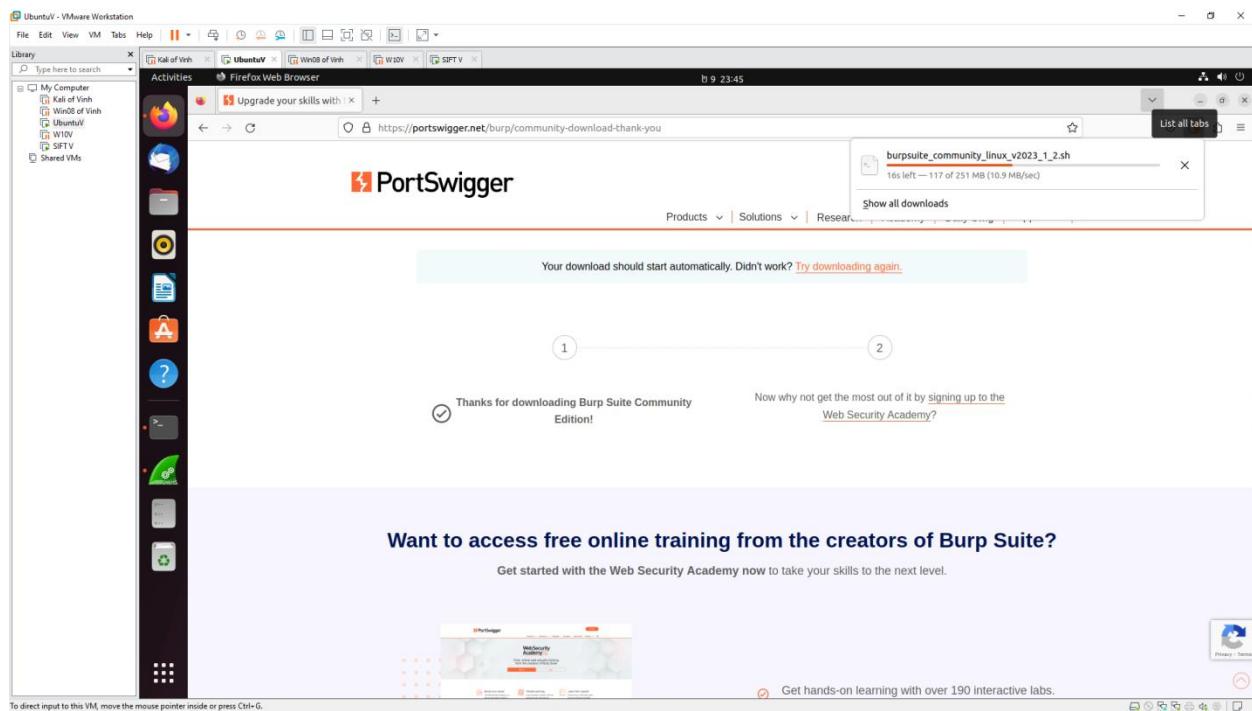


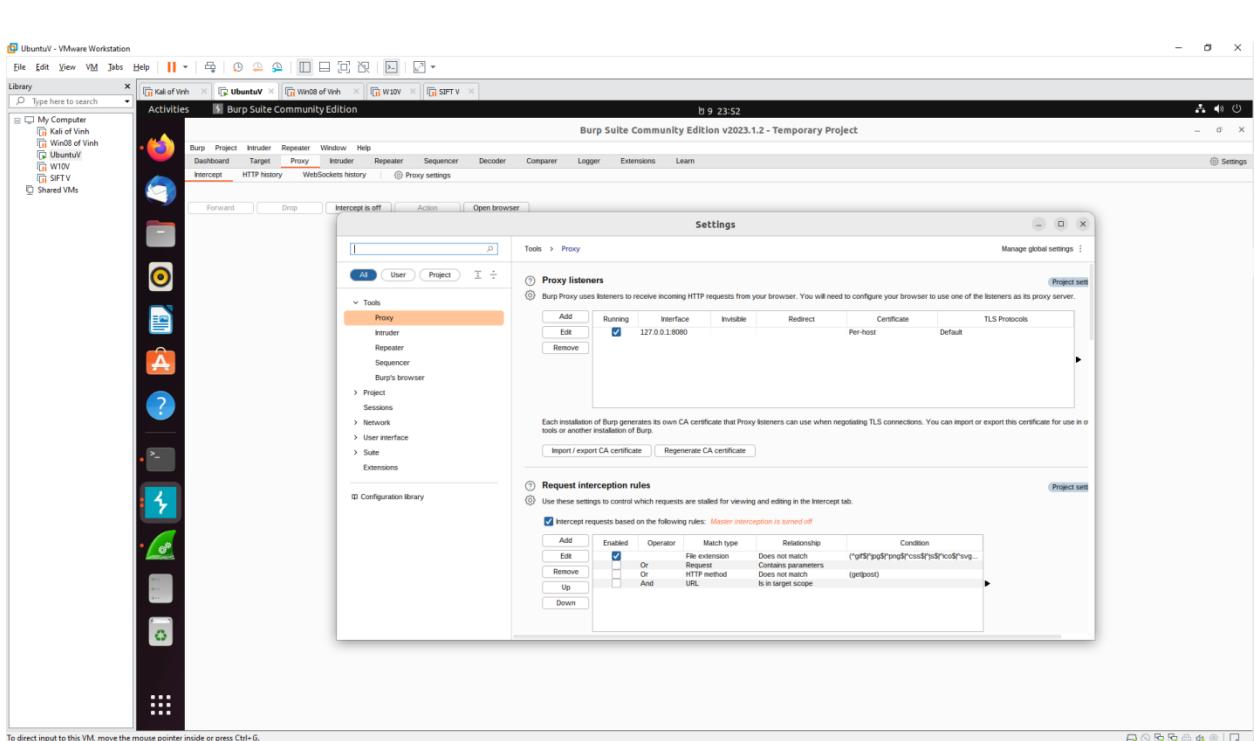
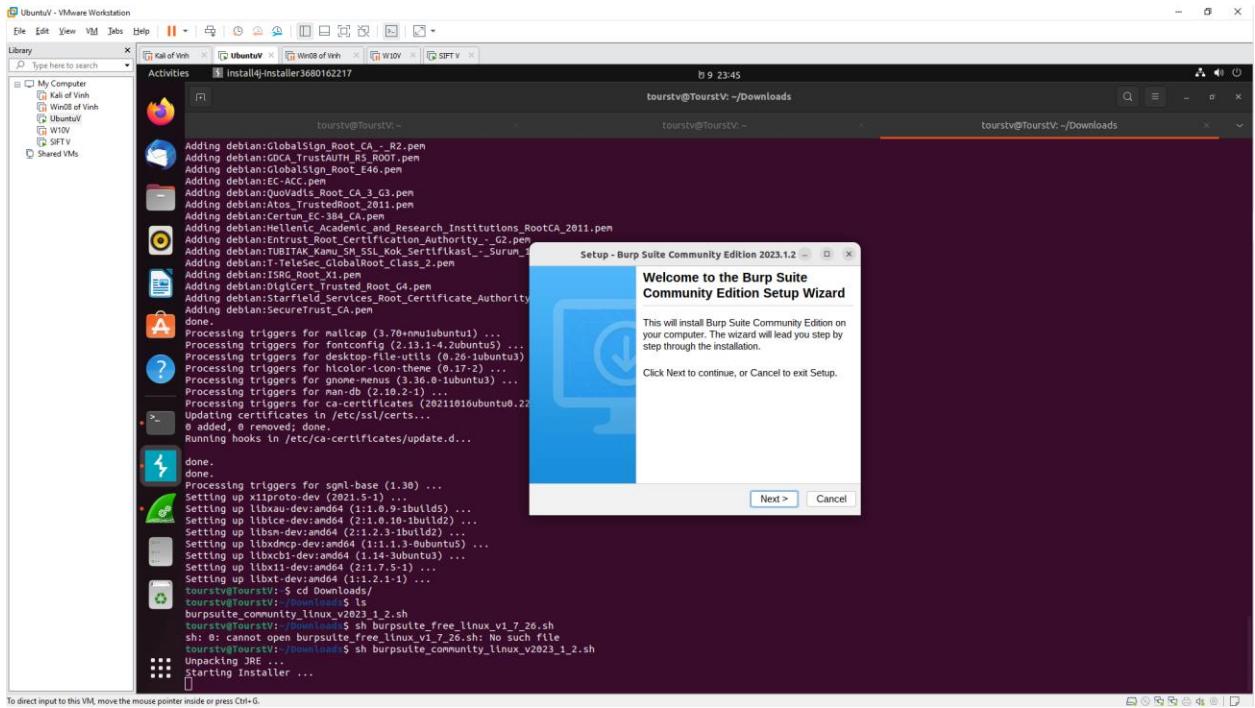
The screenshot shows a Linux desktop environment within a VMware Workstation window. The desktop interface includes a top bar with 'File', 'Edit', 'View', 'VM', 'Jobs', 'Help' menus, and several icons. A 'Library' sidebar on the left lists 'My Computer' with entries like 'Kali of Vinh', 'Win8 of Vinh', 'UbuntuV', 'W10V', and 'SIFTV'. Below these are sections for 'Shared VMs' and 'Recent VMs'. The main workspace contains two terminal windows. The left terminal window, titled 'tourstv@TourstV: ~', displays the output of the command 'sudo iNetSim'. The output shows the initialization of iNetSim version 1.2.4, configuration parsing, and the start of various network services. Services listed include 'finger\_11\_tcp', 'irc\_667\_tcp', 'time\_37\_tcp', 'ntp\_123\_udp', 'syslog\_514\_udp', 'tfm\_69\_udp', 'echo\_7\_udp', 'chargen\_19\_tcp', 'chargen\_19\_udp', 'dummy\_1\_udp', 'dummy\_1\_tcp', 'smtps\_465\_tcp', 'discard\_9\_udp', 'quotd\_17\_udp', 'ldent\_113\_tcp', 'https\_443\_tcp', 'dummy\_1\_tcp', 'ftps\_993\_tcp', 'http\_80\_tcp', and 'ftp\_21\_tcp'. The right terminal window, also titled 'tourstv@TourstV: ~', is currently empty. The status bar at the bottom indicates 'b 9 23:39'.

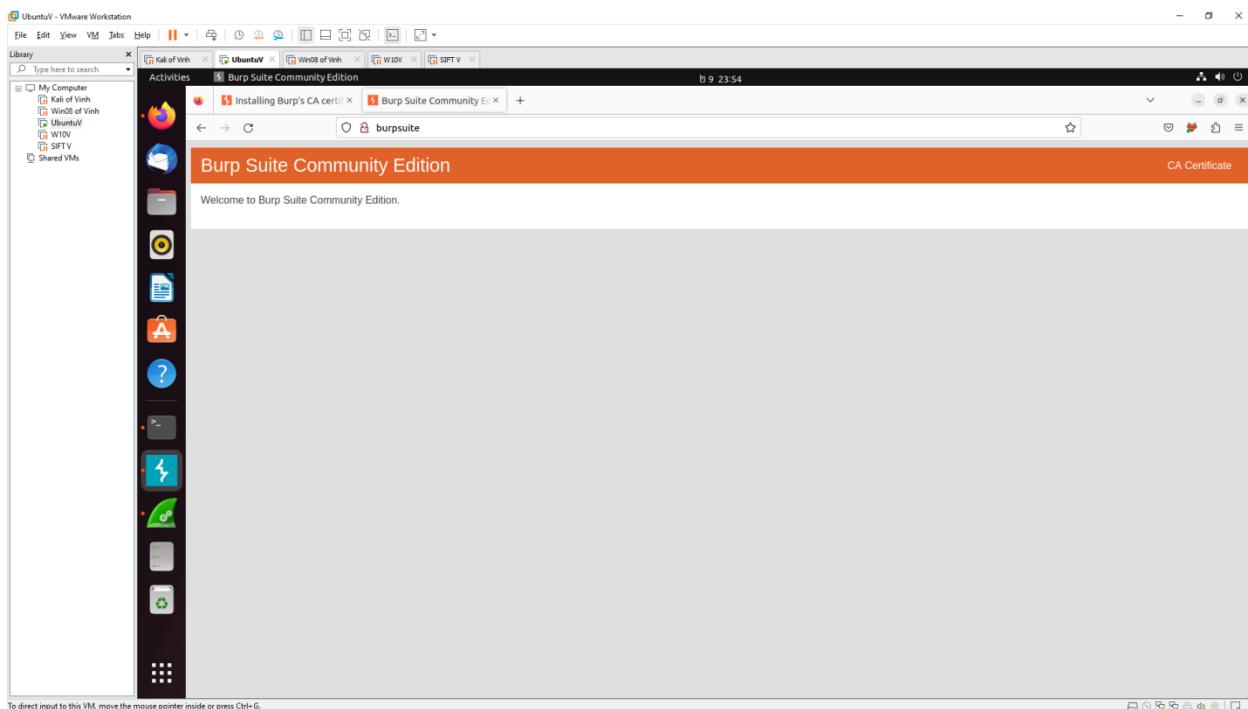
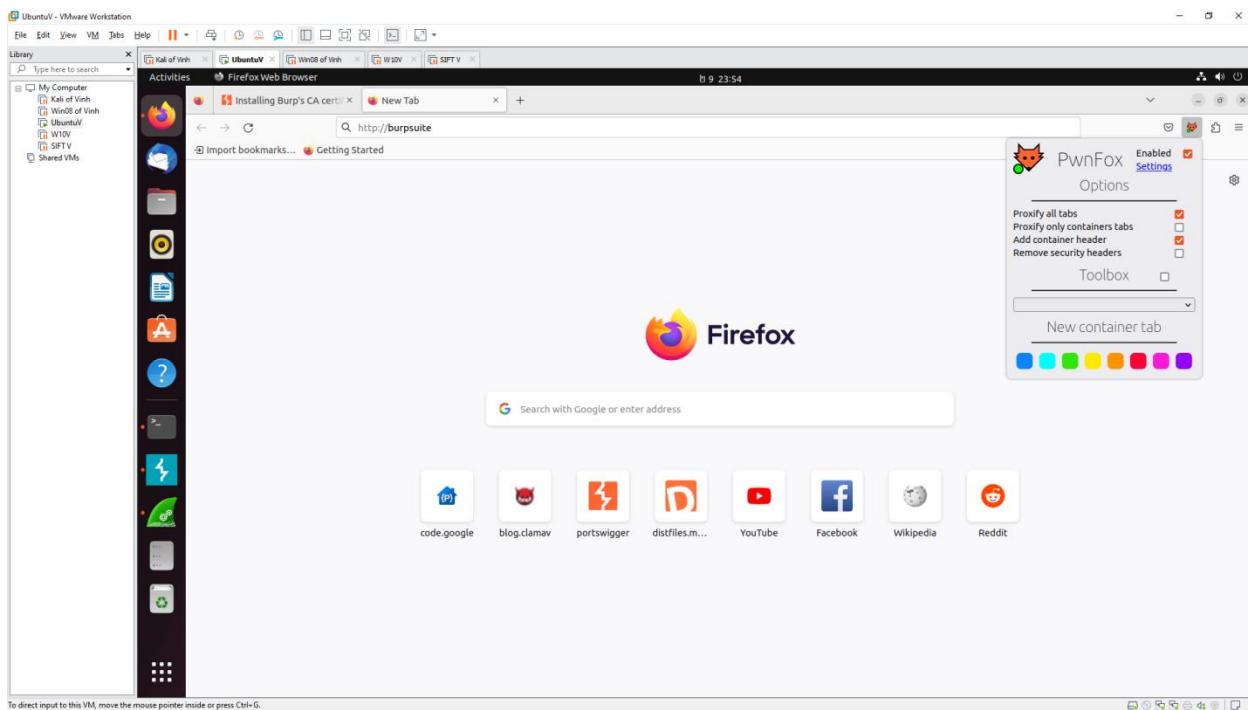
```
iNetSim 1.2.4 (2013-08-15) by Matthias Eckert & Thomas Hungenberg
Main logfile '/var/log/iNetSim/main.log' does not exist. Trying to create it...
Main logfile '/var/log/iNetSim/main.log' successfully created.
Main logfile '/var/log/iNetSim/service.log' does not exist. Trying to create it...
Sub logfile '/var/log/iNetSim/service.log' successfully created.
Debug logfile '/var/log/iNetSim/debug.log' does not exist. Trying to create it...
Debug logfile '/var/log/iNetSim/debug.log' successfully created.
Using log directory: '/var/log/iNetSim'
Using data directory: '/var/lib/iNetSim'
Using report directory: '/var/log/iNetSim/report'
Using configuration file: /etc/iNetSim/iNetSim.conf
Parsing configuration file...
Configuration file parsed successfully.
*** iNetSim main process started (PID 5553) ***
Services started:
Listening on: 192.168.1.10:128
Real Date/Time: 2023-02-09 23:39:01
Fake Date/Time: 2023-02-09 23:39:01 (Delta: 0 seconds)
Forking services...
Insecure dependency in socket while running with -i switch at /usr/lib/x86_64-linux-gnu/perl-base/Io/Socket.pm line 81.
* finger_11_tcp - started (PID 5547)
* irc_667_tcp - started (PID 5545)
* time_37_tcp - started (PID 5546)
* ntp_123_udp - started (PID 5568)
* syslog_514_udp - started (PID 5569)
* tfm_69_udp - started (PID 5564)
* echo_7_udp - started (PID 5574)
* chargen_19_tcp - started (PID 5571)
* time_37_udp - started (PID 5571)
* discard_9_udp - started (PID 5577)
* daytime_13_udp - started (PID 5573)
* quotd_17_tcp - started (PID 5578)
* discard_9_tcp - started (PID 5576)
* smtps_465_tcp - started (PID 5579)
* https_443_tcp - started (PID 5557)
* dummy_1_tcp - started (PID 5582)
* ftplib_993_tcp - started (PID 5563)
* http_80_tcp - started (PID 5568)
* ftp_21_tcp - started (PID 5562)
```

## Install Burp Suite

A screenshot of a Linux desktop environment, likely Kali Linux, running in a VMware Workstation window. The desktop has a dark theme with a top bar showing the title 'UbuntuV - VMware Workstation' and various system icons. On the left, there's a 'Library' sidebar with items like 'My Computer', 'Kali 1.0.6', 'Win10 of Vinh', 'UbuntuV', 'W10V', 'SIFTY', and 'Shared VMs'. The main workspace contains several windows: a file manager ('Nautilus') showing a directory tree; a terminal window titled 'tourstv@TourstV: ~' with a command history including apt-get installations for openjdk-9-jdk, openjdk-11-jdk, and openjdk-11-jre; and another terminal window showing a long list of Java packages and their dependencies. A bottom status bar at the bottom of the screen displays the message 'To direct input to this VM, move the mouse pointer inside or press Ctrl+G.'







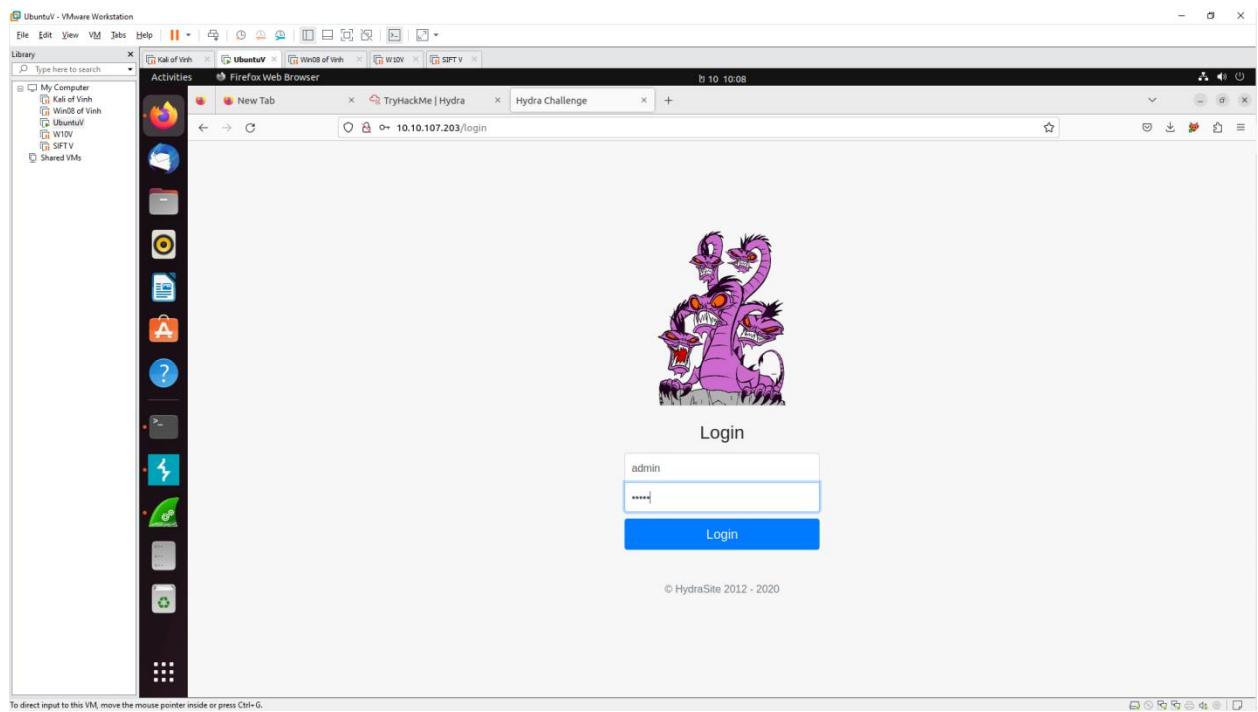
## WORKSHOP1

The screenshot shows a Linux desktop environment with a window titled "UbuntuU - VMware Workstation". Inside the window, a Firefox browser is open to a SANS Institute page titled "How to identify malicious HTTP Requests". The page content includes a brief introduction, author information, a download button, and a copyright notice. A sidebar on the left lists various VMs in the library.

## Using hydra to Bruteforce

The screenshot shows a Linux desktop environment with a window titled "UbuntuU - VMware Workstation". Inside the window, a Firefox browser is open to a Hydra login page for a TryHackMe challenge. The page features a cartoon dragon illustration and a login form with fields for Username and Password. A PwnFox extension toolbar is visible on the right side of the browser window.

- login with 'admin@admin'



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

UbuntuV - VMware Workstation

Activities

Burp Suite Community Edition

File Edit View VM Jobs Help | 10:10:08

Request to http://detectportal.firefox.com:80 [34.107.221.80]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1. GET /canonical.html HTTP/1.1
   Host: detectportal.firefox.com
   User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/109.0
2. Accept: */*
3. Accept-Language: en-US,en;q=0.5
4. Accept-Encoding: gzip, deflate
5. Cache-Control: no-cache
6. Pragma: no-cache
7. Connection: close
```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 0

Request cookies 0

Request headers 8

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

UbuntuV - VMware Workstation

Activities

Burp Suite Community Edition

File Edit View VM Jobs Help | 10:10:10

Request to http://10.10.107.203:80

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1. POST /login HTTP/1.1
   Host: 10.10.107.203
   Content-Type: application/x-www-form-urlencoded
2. Cache-Control: max-age=0
3. Upgrade-Insecure-Requests: 1
4. User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.96 (KHTML, like Gecko) Chrome/110.0.5481.79 Safari/537.96
5. Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6. Referer: http://10.10.107.203/login
7. Content-Type: application/x-www-form-urlencoded
8. Accept-Language: en-US,en;q=0.5
9. Accept-Encoding: gzip, deflate
10. Connection: close
11. Cookie: connect.sid=s%3AzUgzbPB-OKMjQcDl6r7RLxcbzV2lIp.xMc%2B1Dn72LeyHng8IXGLq4t7tcVge%2bdP%2F2EUOU
12. [username=admin&password=admin]
```

Comment this item

Inspector

Selection 29 (0x1d)

Selected text username=admin&password=admin

Decoded from: URL encoding

username=admin&password=admin

Cancel Apply changes

Request attributes 2

Request query parameters 0

Request body parameters 2

Request cookies 1

Request headers 13

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

```

tourstv@TourstV:~$ hydra -L molly -P Downloads/kali-wordlists/rockyou.txt 10.10.107.203 http-post-form "/login:username^USER^&password^PASS^:Your username or password is incorrect."
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (1:1:p:14344399), -896525 tries per task
[DATA] attacking http-post-form://10.10.107.203:80/login:username^USER^&password^PASS^:Your username or password is incorrect.
[!] [http-post-form] host: 10.10.107.203 login: molly password: sunshine
[+] 1 of 1 targets successfully completed
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-10 10:22:15
tourstv@TourstV:~$ 

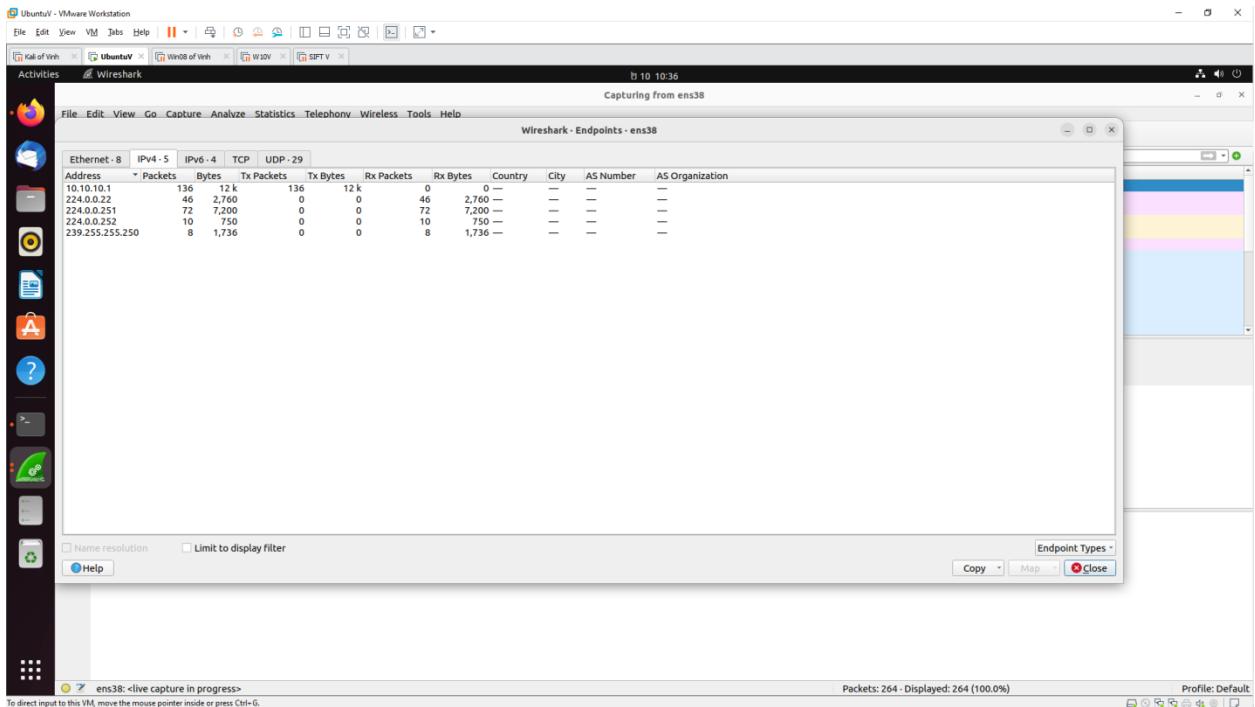
```

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

## WORKSHOP2

Which systems (i.e. IP addresses) are involved?



- What can you find out about the attacking host (e.g., where is it located)?

The Honeynet Project - IP and website location: https://www.honey.net/ip-info/host=https%3A%2F%2Fwww.honeynet.org%2Fnode%2F504&csrf\_token=0d01a2c967c77b16248c053e0f3704fe75af3746

IP: 172.67.9.102 Country: Viet Nam (Ho Chi Minh, Quan Saу) Change IP

Info | Ping | HTTP | TCP port | UDP port | DNS

IP and website location: www.honeynet.org

DB-IP (02.02.2023)

IP address	172.67.9.102
Host name	172.67.9.102
IP range	172.67.7.0-172.67.12.255 CIDR
ISP	Cloudflare, Inc.
Organization	Cloudflare, Inc.
Country	United States of America (US)
Region	New Jersey
City	Newark
Time zone	America/New_York, GMT-0500
Local time	22:41:44 (EST) / 2023.02.09
Postal Code	07175

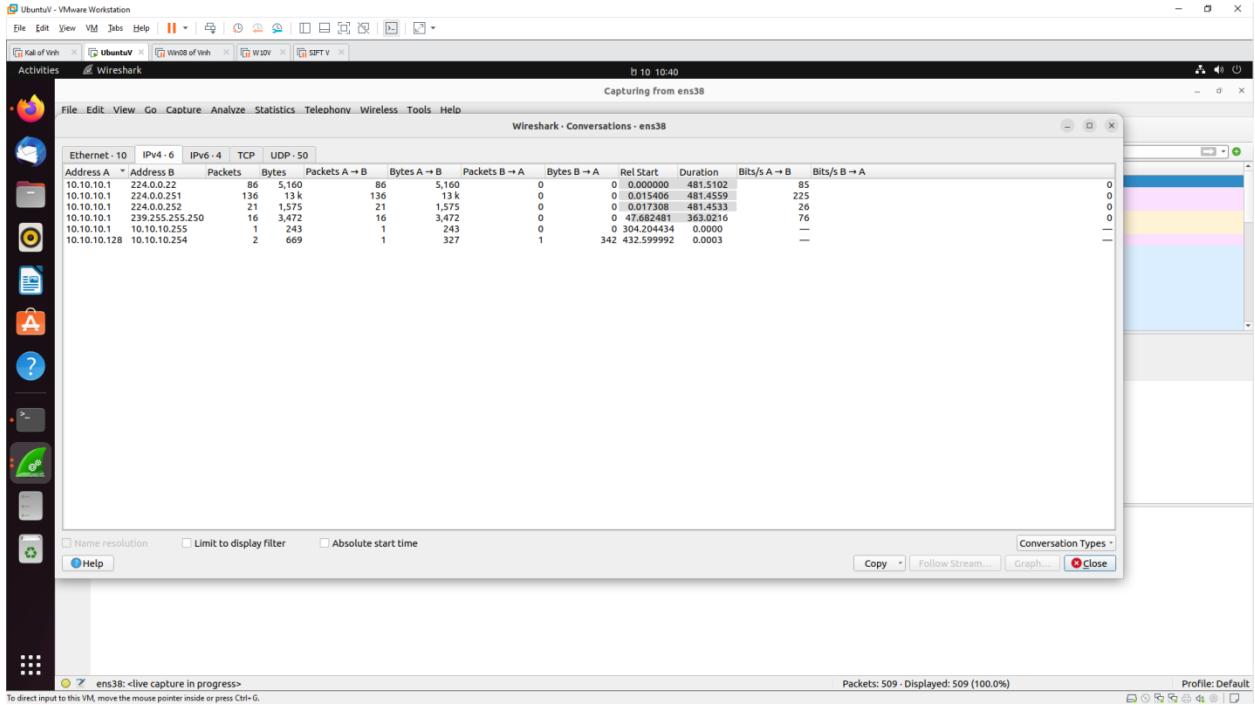
Powered by DB-IP

IPGeolocation.io (01.02.2023)

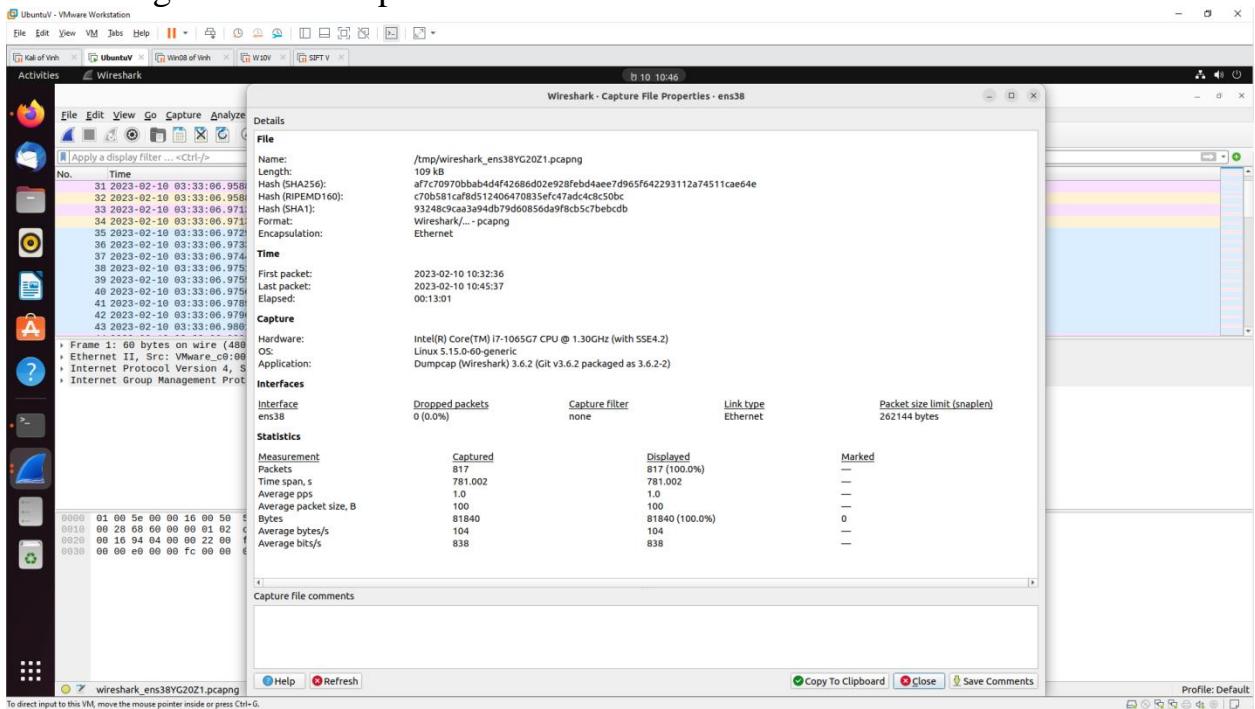
IP address	172.67.9.102
Host name	172.67.9.102
IP range	172.67.9.0-172.67.9.255 CIDR
ISP	Cloudflare, Inc.
Organization	Cloudflare, Inc.
Country	United States (US)
Region	California
City	San Francisco
Time zone	America/Los_Angeles, GMT-0800
Local time	19:41:44 (PST) / 2023.02.09
Postal Code	94107-1907

Powered by IPGeolocation.io

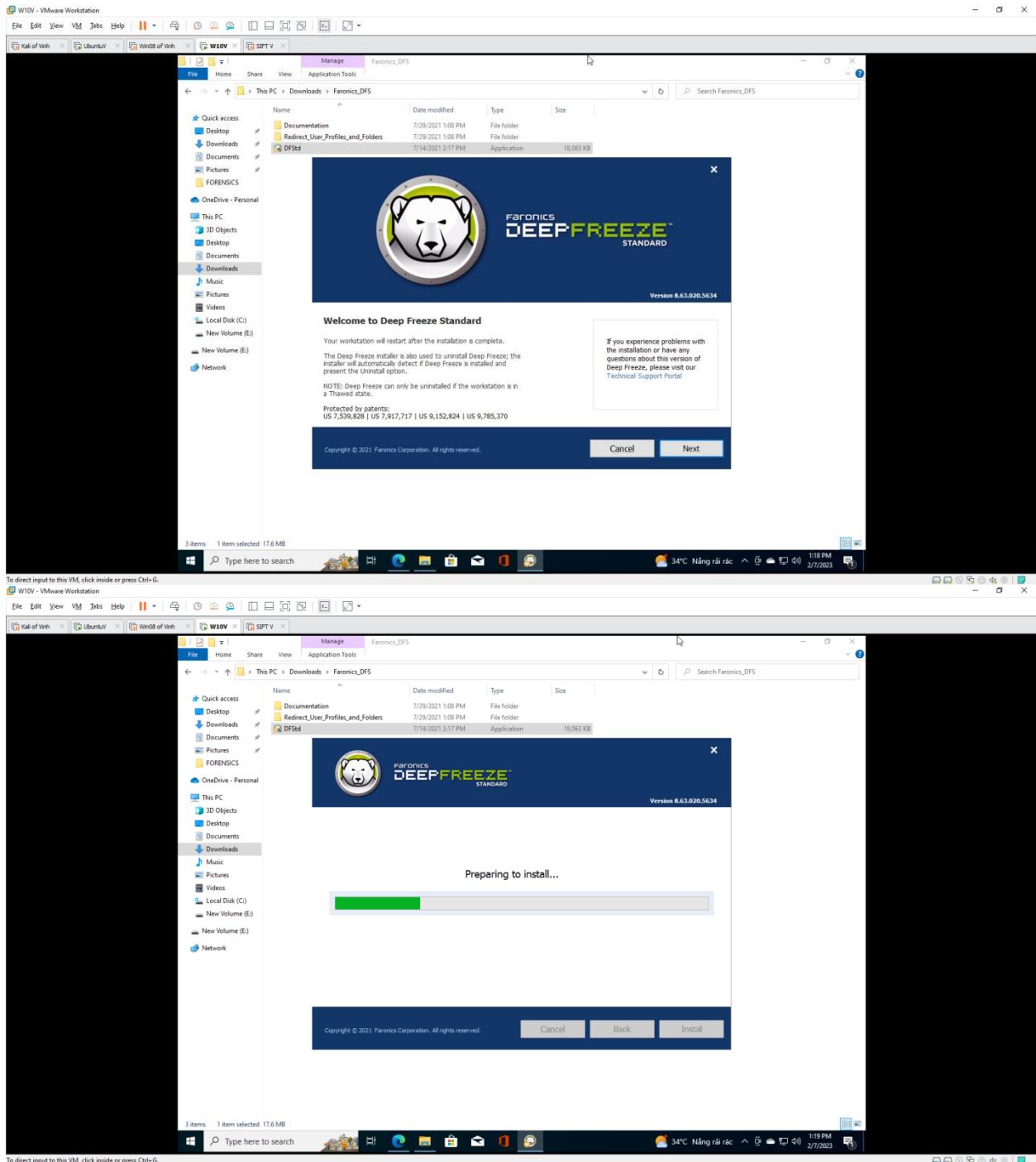
- How many TCP sessions are contained in the dump file?



- How long did it take to perform the attack?



## Install Deep Freeze



## LAB 7.2: Registry Forensics with RegRipper Plug-ins

### Purpose:

- Introduction to the window registry.
- Introduction to RegRipper.
- Analysis of Registry files with RegRipper.

## Download RegRipper

The screenshot shows a Windows 10 desktop environment with a VMware Workstation window titled "W10V - VMware Workstation". Inside the window, a Google Chrome browser is open to the URL <https://code.google.com/archive/p/regripper/downloads>. The page title is "Google Code Archive". The "regripper" project is selected. The "Downloads" section displays a table of files:

File	Summary + Labels	Uploaded	Size
autorip_08-26-13.zip	autorip_08-26-13.zip	Aug 26, 2013	1.79MB
ripexp.zip	RipXP	Jun 29, 2013	1.55MB
auto_rip-5-16-2013.zip	auto_rip, 16 May 2013 [Deprecation]	May 22, 2013	1.79MB
rnv2.8.zip	RegRipper v2.8	Apr 30, 2013	4.06MB
plugins20130429.zip	Plugin updates, 29 April 2013	Apr 30, 2013	365.67KB
plugins20130418.zip	Plugin updates, 18 April 2013	Apr 19, 2013	356.36KB
plugins20130404.zip	RegRipper plugin archive	Apr 4, 2013	358.63KB
rnv2.5.zip	RegRipper download	Apr 4, 2013	4.06MB
samples.zip	Sample hives	Oct 2, 2012	31.23MB

The desktop taskbar at the bottom shows icons for File Explorer, Task View, Start, Taskbar settings, and system notifications. The system tray indicates the date as 2/10/2023 and the time as 10:29 AM.

