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

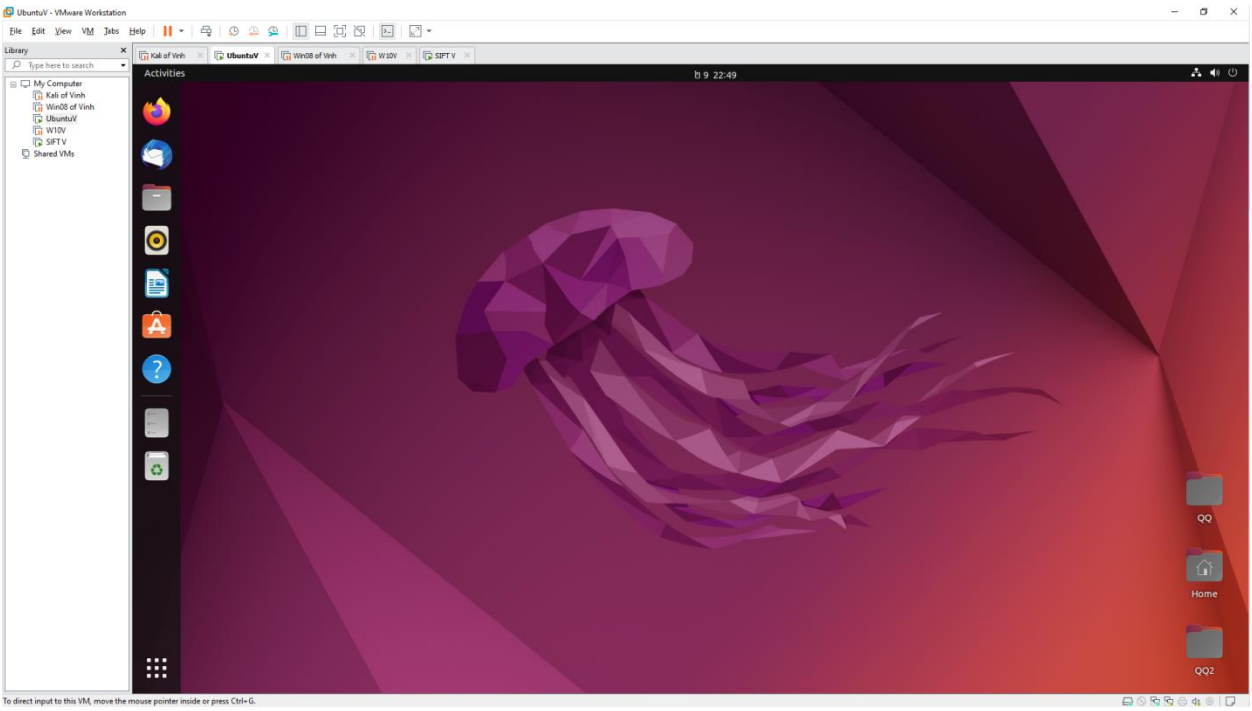
Purpose:

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

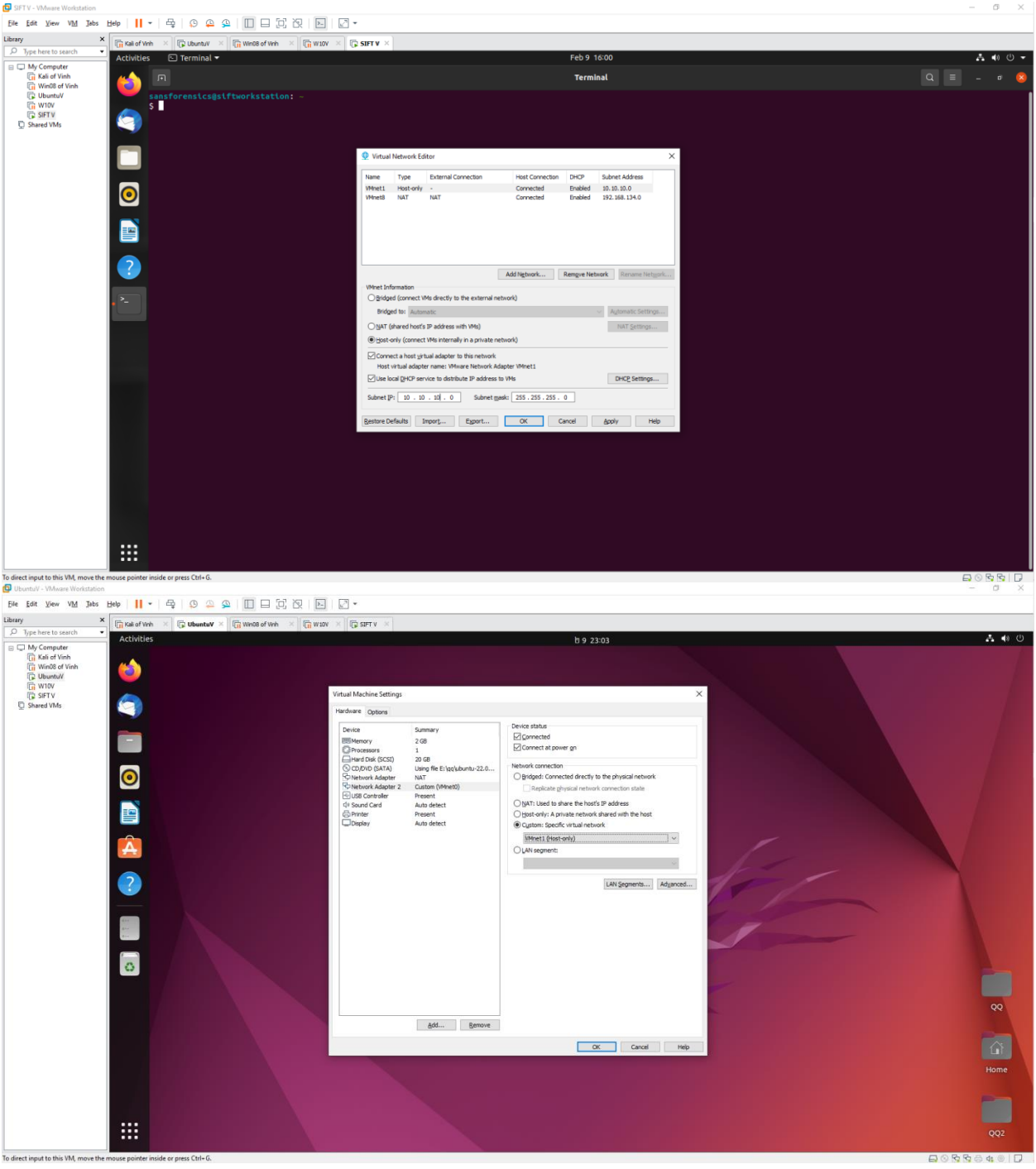
What we need:

- 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

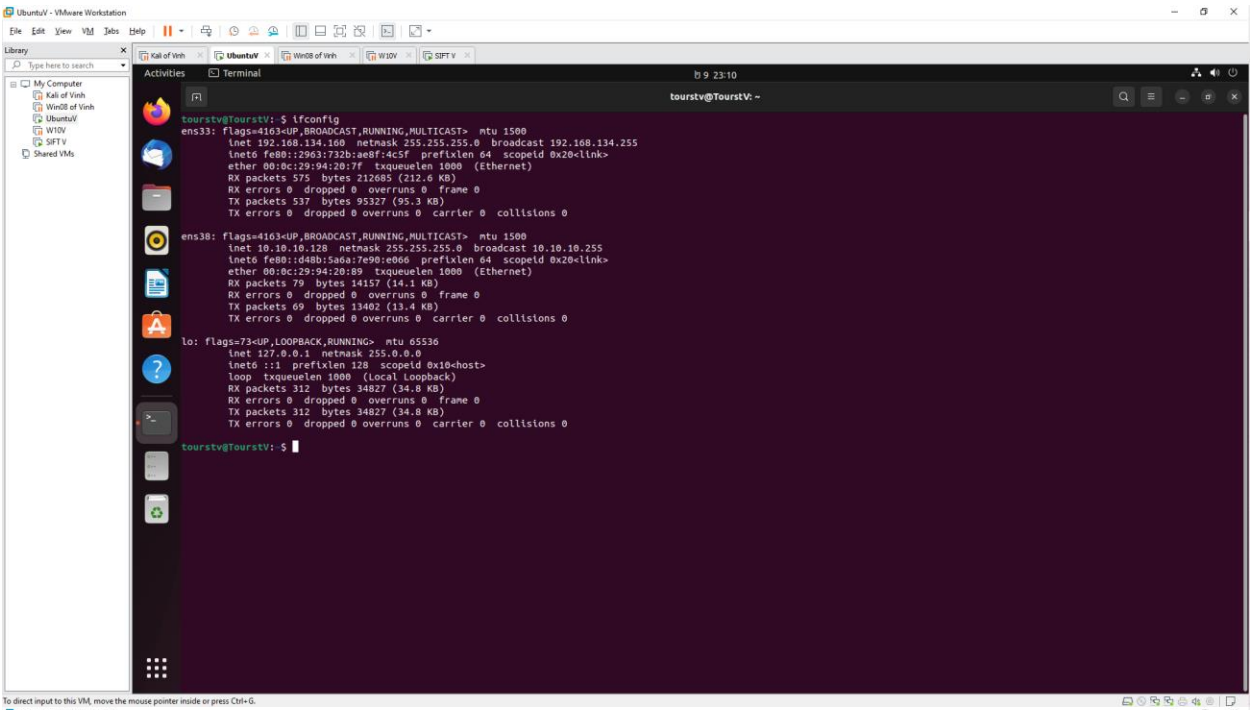
VMWARE WorkStation

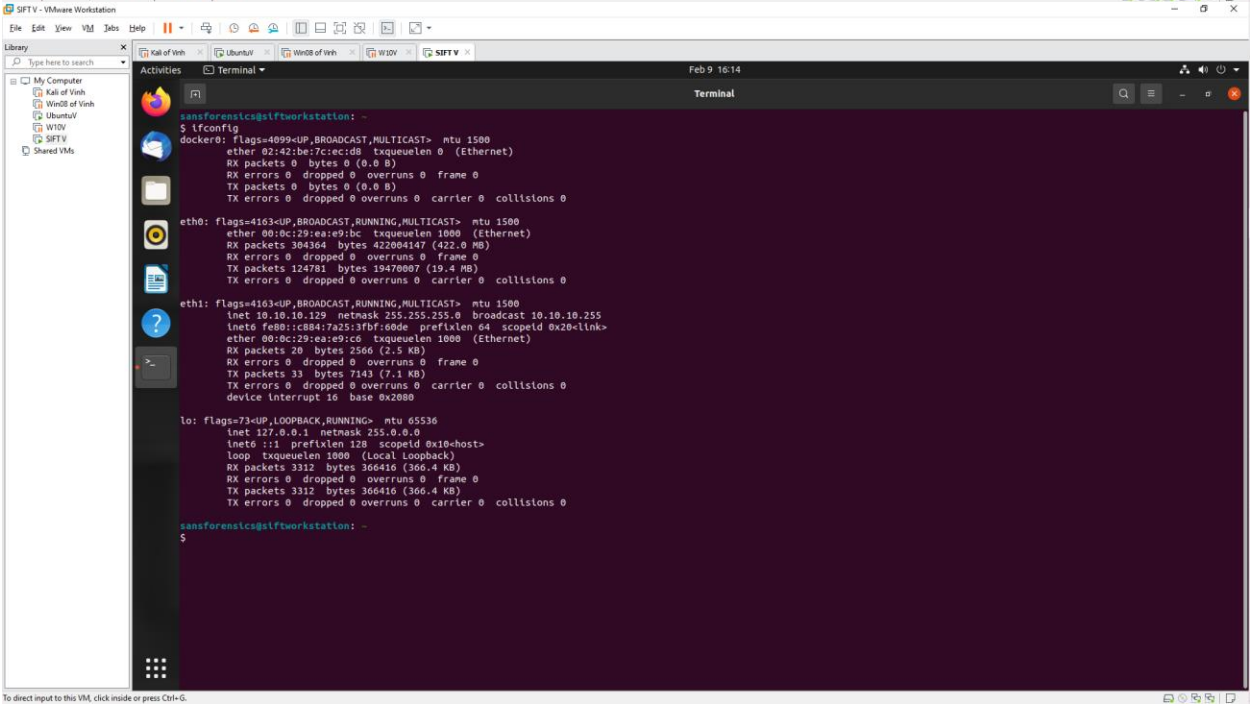


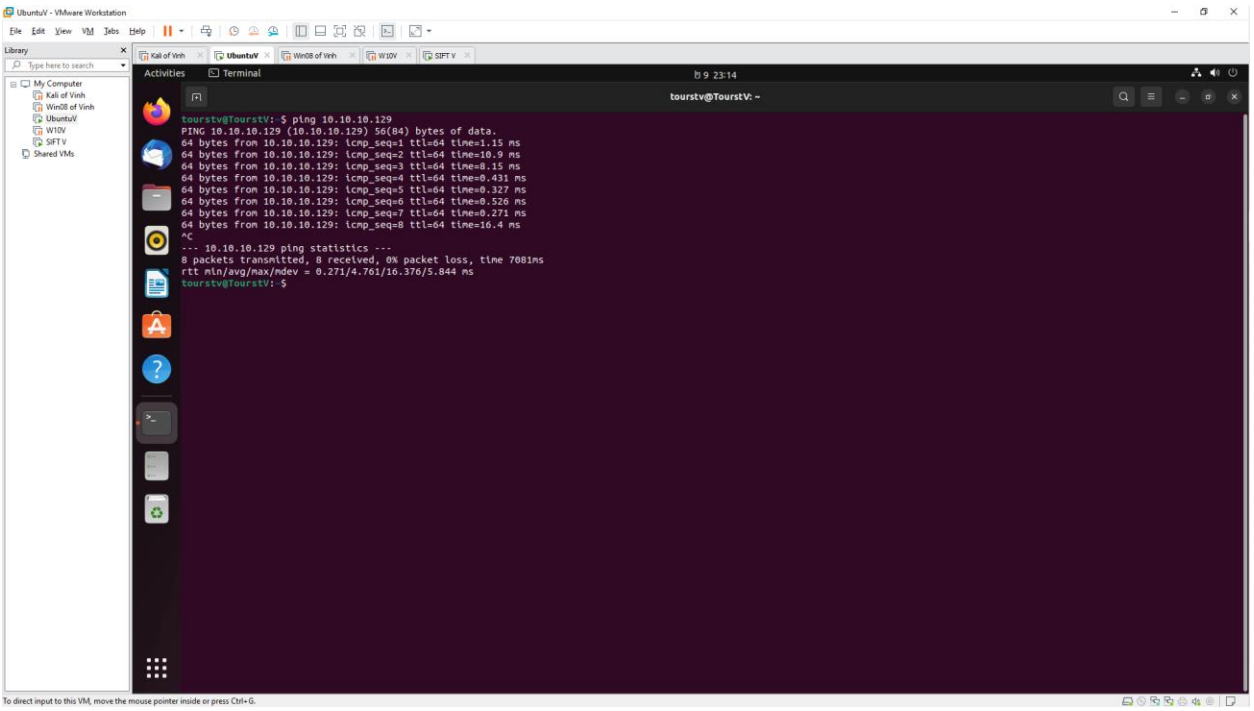
Configurations of NETWORK on vmware workstation


SIFT V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali of Vinh
Win08 of Vinh
UbuntuV
W10V
SIFT V
Shared VMs
Kali of Vinh
UbuntuV
Win08 of Vinh
W10V
SIFT V
Activities
Terminal
Feb 9 16:00
Terminal
sansforensics@siftworkstation: ~
$
Virtual Network Editor
Name Type External Connection Host Connection DHCP Subnet Address
VMnet1 Host-only - Connected Enabled 10.10.10.0
VMnet8 NAT NAT Connected Enabled 192.168.134.0
Add Network... Remove Network Rename Network...
VMnet Information
Bridged (connect VMs directly to the external network)
Bridged to: Automatic Automatic Settings...
NAT (shared host's IP address with VMs) NAT Settings...
Host-only (connect VMs internally in a private network)
Connect a host virtual adapter to this network
Host virtual adapter name: VMware Network Adapter VMnet1
Use local DHCP service to distribute IP address to VMs DHCP Settings...
Subnet IP: 10 . 10 . 10 . 0 Subnet mask: 255 . 255 . 255 . 0
Restore Defaults Import... Export... OK Cancel Apply Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

UbuntuV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali of Vinh
Win08 of Vinh
UbuntuV
W10V
SIFT V
Shared VMs
Kali of Vinh
UbuntuV
Win08 of Vinh
W10V
SIFT V
Activities
9 23:03
Virtual Machine Settings
Hardware Options
Device Summary
Memory 2 GB
Processors 1
Hard Disk (SCSI) 20 GB
CD/DVD (SATA) Using file E:\qq\ubuntu-22.0...
Network Adapter NAT
Network Adapter 2 Custom (VMnet0)
USB Controller Present
Sound Card Auto detect
Printer Present
Display Auto detect
Add... Remove
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet1 (Host-only)
LAN segment:
LAN Segments... Advanced...
OK Cancel Help
QQ
Home
QQZ
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

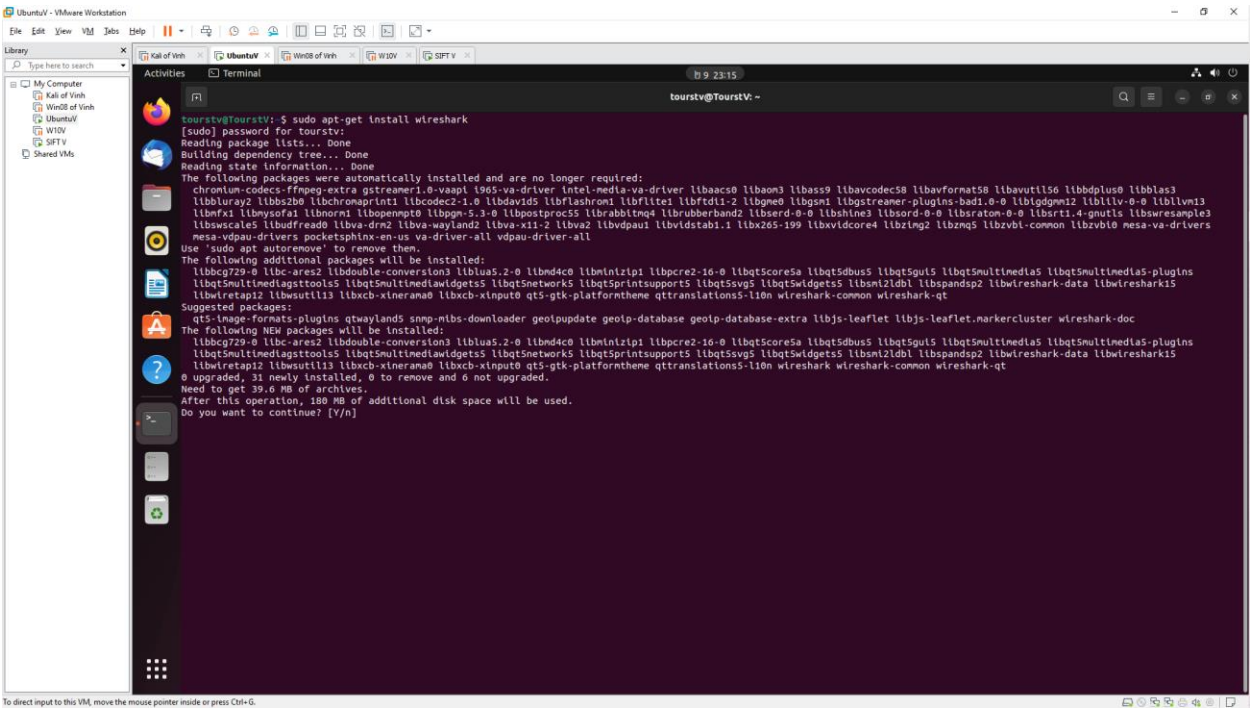

UbuntuV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali of Vinh
Win08 of Vinh
UbuntuV
W10V
SIFT V
Shared VMs
Kali of Vinh
UbuntuV
Win08 of Vinh
W10V
SIFT V
Activities
Terminal
Fri 9 23:10
tourstv@TourstV: ~
tourstv@TourstV: $ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.134.160 netmask 255.255.255.0 broadcast 192.168.134.255
inet6 fe80::2963:732b:ae8f:4c5f prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:94:20:7f txqueuelen 1000 (Ethernet)
RX packets 575 bytes 212685 (212.6 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 537 bytes 95327 (95.3 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
ens38: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.10.10.128 netmask 255.255.255.0 broadcast 10.10.10.255
inet6 fe80::d48b:5a6a:7e98:e066 prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:94:20:89 txqueuelen 1000 (Ethernet)
RX packets 79 bytes 14157 (14.1 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 69 bytes 13402 (13.4 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 312 bytes 34827 (34.8 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 312 bytes 34827 (34.8 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
tourstv@TourstV: $
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


SIFT V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali of Vinh
Win08 of Vinh
UbuntuV
W10V
SIFT V
Shared VMs
Kali of Vinh
UbuntuV
Win08 of Vinh
W10V
SIFT V
Activities
Terminal
Feb 9 16:14
Terminal
sansforensics@siftworkstation: ~
$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
ether 02:42:be:7c:ec:d8 txqueuelen 0 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
ether 00:0c:29:ea:e9:bc txqueuelen 1000 (Ethernet)
RX packets 304364 bytes 422004147 (422.0 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 124781 bytes 19470807 (19.4 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.10.10.129 netmask 255.255.255.0 broadcast 10.10.10.255
inet6 fe80::c884:7a25:3fbf:60de prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:ea:e9:c6 txqueuelen 1000 (Ethernet)
RX packets 20 bytes 2566 (2.5 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 33 bytes 7143 (7.1 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device interrupt 16 base 0x2080
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 3312 bytes 366416 (366.4 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 3312 bytes 366416 (366.4 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
sansforensics@siftworkstation: ~
$
To direct input to this VM, click inside or press Ctrl+G.

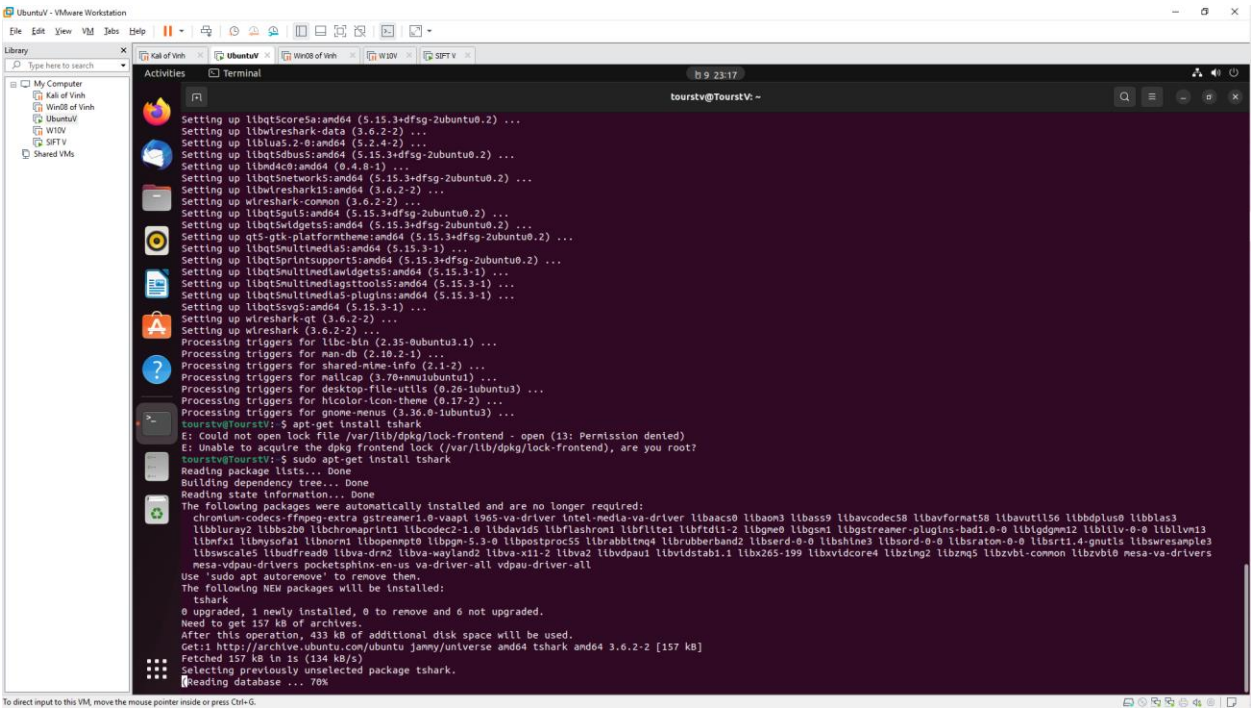


Install WireShark

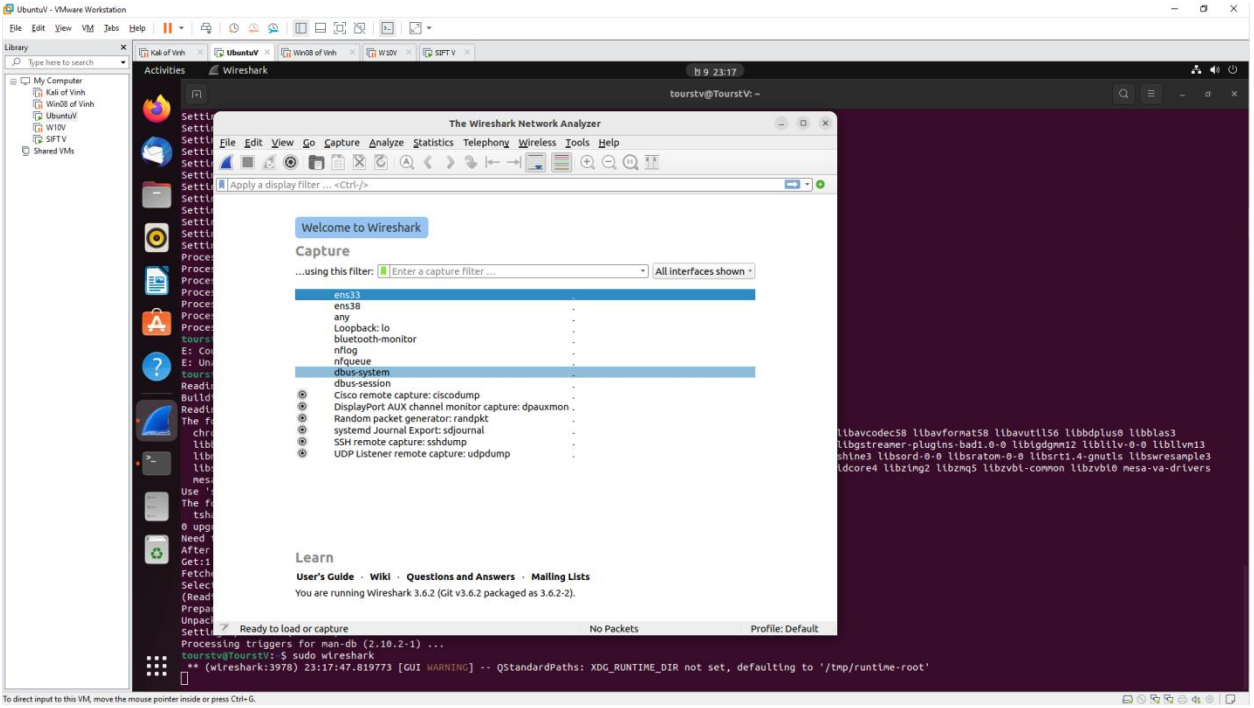
- WireShark



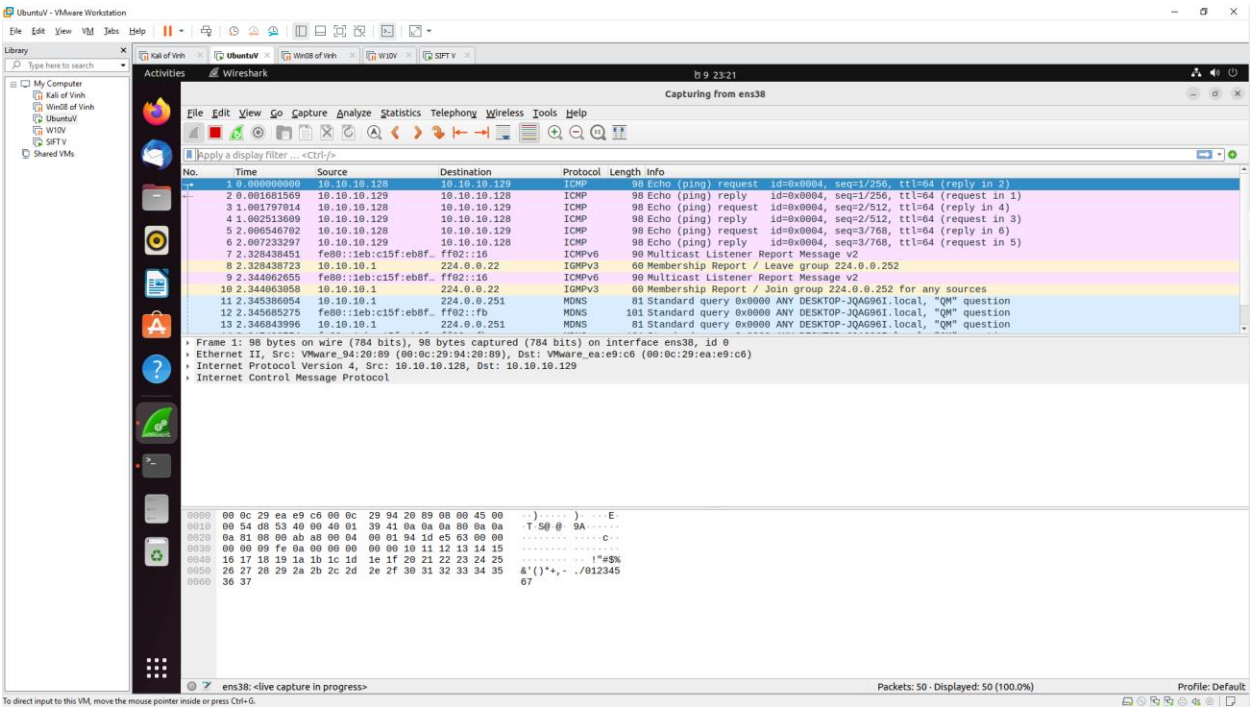
- tshark



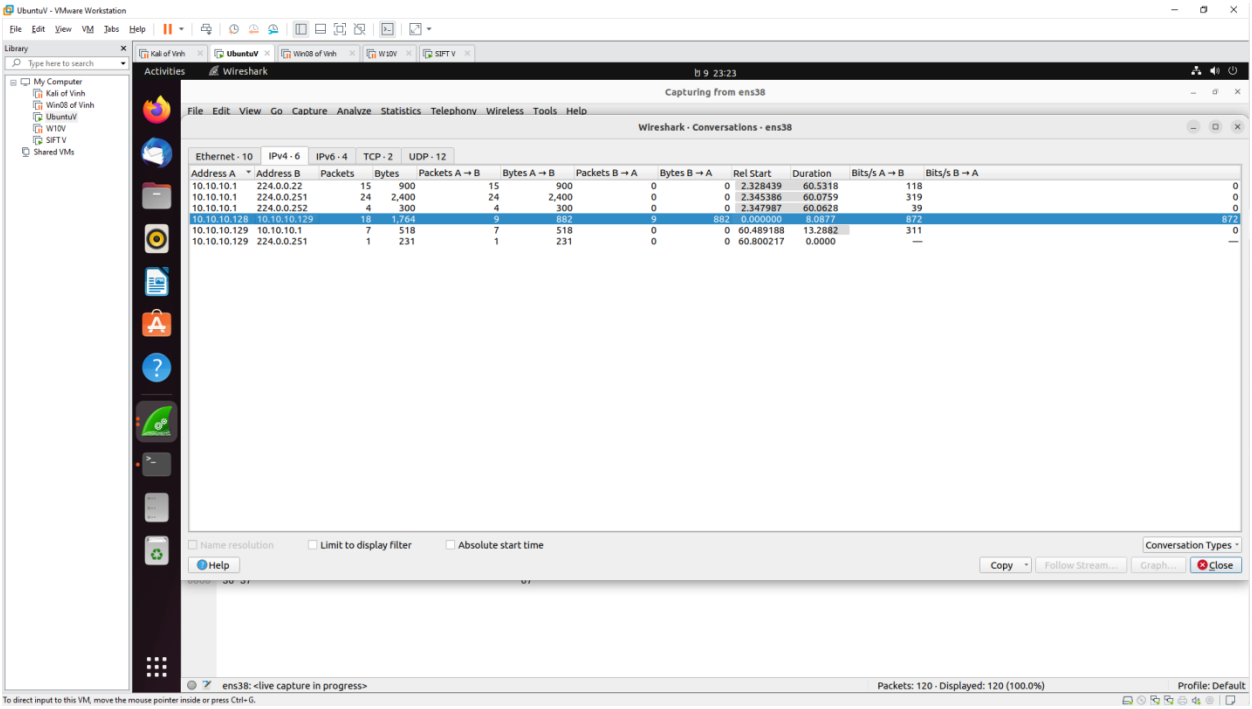
- choose ens38



CAPTURE PACKET BY WIRESHARK



- Conversation

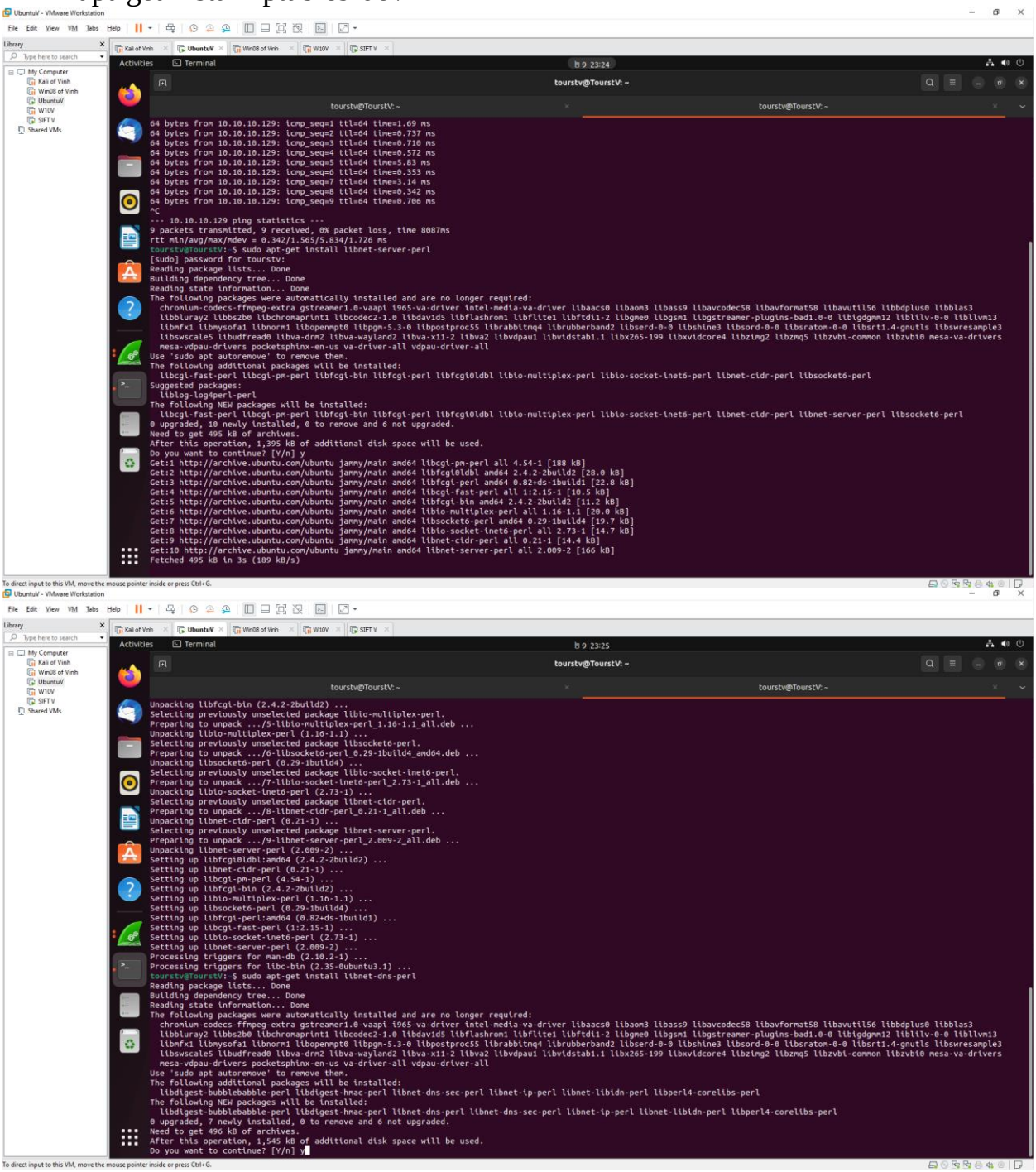


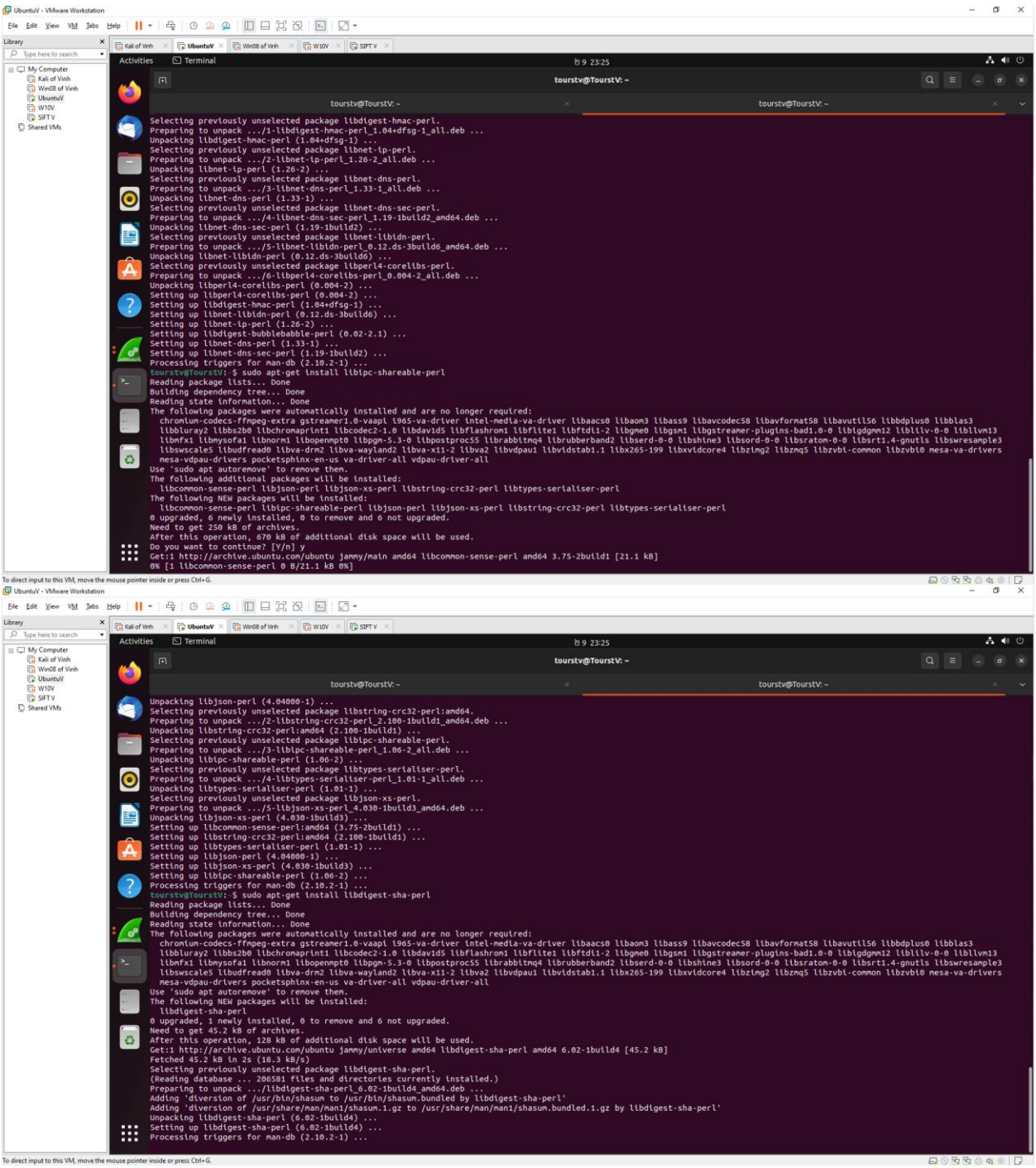
Install InetSim

Install:

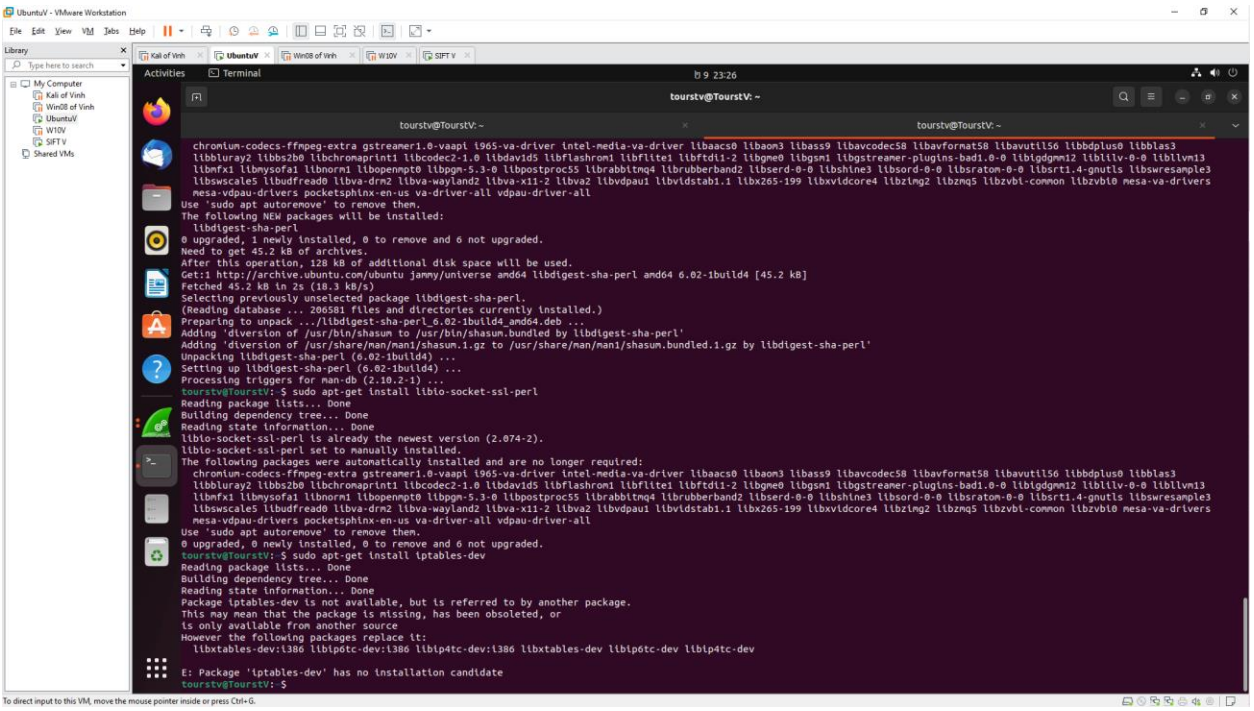
apt-get install libnet-server-perl
apt-get install libnet-dns-perl
apt-get install libipc-shareable-perl

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



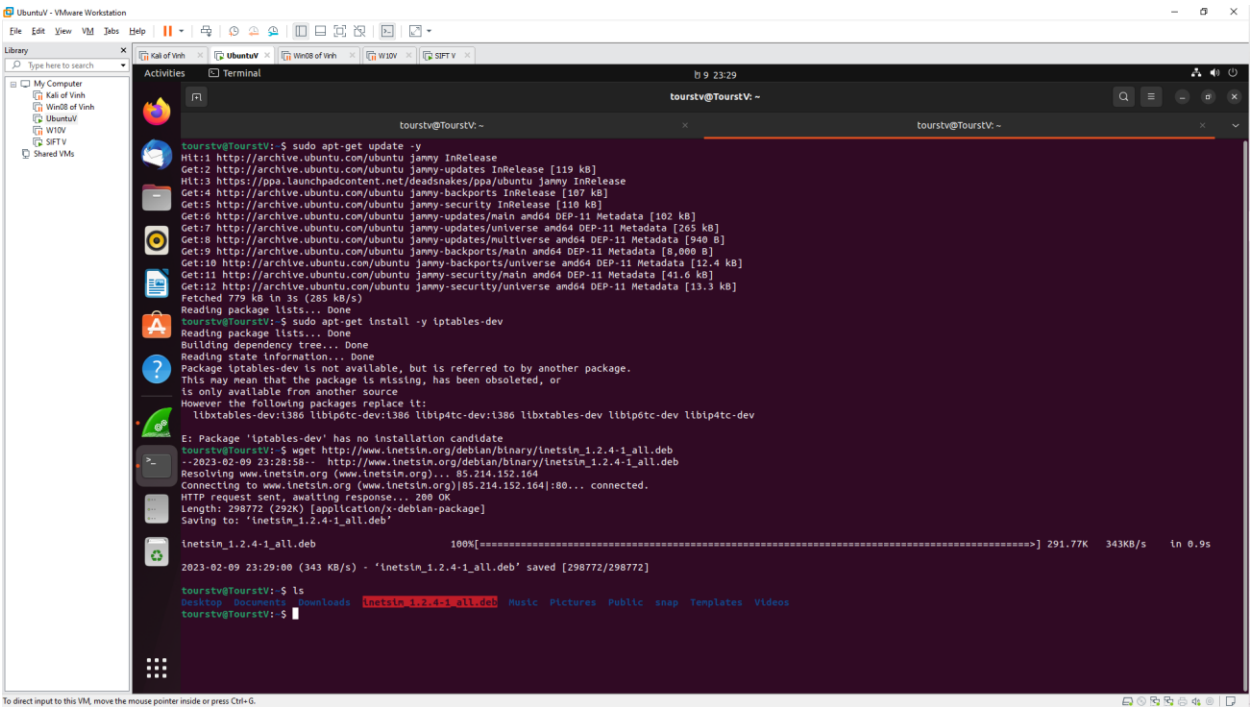

UbuntuV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali of Vinh
Win08 of Vinh
UbuntuV
W10V
SIFT V
Shared VMs
Kali of Vinh
UbuntuV
Win08 of Vinh
W10V
SIFT V
Activities
Terminal
9 23:25
tourstv@TourstV: ~
tourstv@TourstV: ~
tourstv@TourstV: ~
Selecting previously unselected package libdigest-hmac-perl.
Preparing to unpack .../1-libdigest-hmac-perl_1.04+dfsg-1_all.deb ...
Unpacking libdigest-hmac-perl (1.04+dfsg-1) ...
Selecting previously unselected package libnet-ip-perl.
Preparing to unpack .../2-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 .../3-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 .../4-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 .../5-libnet-libidn-perl_0.12.ds-3build6_amd64.deb ...
Unpacking libnet-libidn-perl (0.12.ds-3build6) ...
Selecting previously unselected package libperl4-corelibs-perl.
Preparing to unpack .../6-libperl4-corelibs-perl_0.004-2_all.deb ...
Unpacking libperl4-corelibs-perl (0.004-2) ...
Setting up libperl4-corelibs-perl (0.004-2) ...
Setting up libdigest-hmac-perl (1.04+dfsg-1) ...
Setting up libnet-libidn-perl (0.12.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:
chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi i965-va-driver intel-media-va-driver libaacs0 libaom3 libass9 libavcodec58 libavformat58 libavutil56 libbdplus0 libblas3
libbluray2 libbs2b0 libchromaprint1 libcodec2-1.0 libdav1d5 libflashrom1 libflite1 libftdi1-2 libgme0 libgsm1 libgstreamer-plugins-bad1.0-0 libigdgmm12 liblilv-0-0 libllvm13
libmfx1 libmysofa1 libnorm1 libopenmpt0 libpgm-5.3-0 libpostproc55 librabbitmq4 librubberband2 libserd-0-0 libshine3 libsord-0-0 libsratom-0-0 libsrt1.4-gnutls libswresample3
libswscale5 libudfread0 libva-drm2 libva-wayland2 libva-x11-2 libva2 libvdpau1 libvidstab1.1 libx265-199 libxvidcore4 libzimg2 libzmq5 libzvbi-common libzvbi0 mesa-va-drivers
mesa-vdpau-drivers pocketsphinx-en-us va-driver-all vdpau-driver-all
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
libcommon-sense-perl libjson-perl libjson-xs-perl libstring-crc32-perl libtypes-serialiser-perl
The following NEW packages will be installed:
libcommon-sense-perl libipc-shareable-perl libjson-perl libjson-xs-perl libstring-crc32-perl libtypes-serialiser-perl
0 upgraded, 6 newly installed, 0 to remove and 6 not upgraded.
Need to get 250 kB of archives.
After this operation, 670 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.

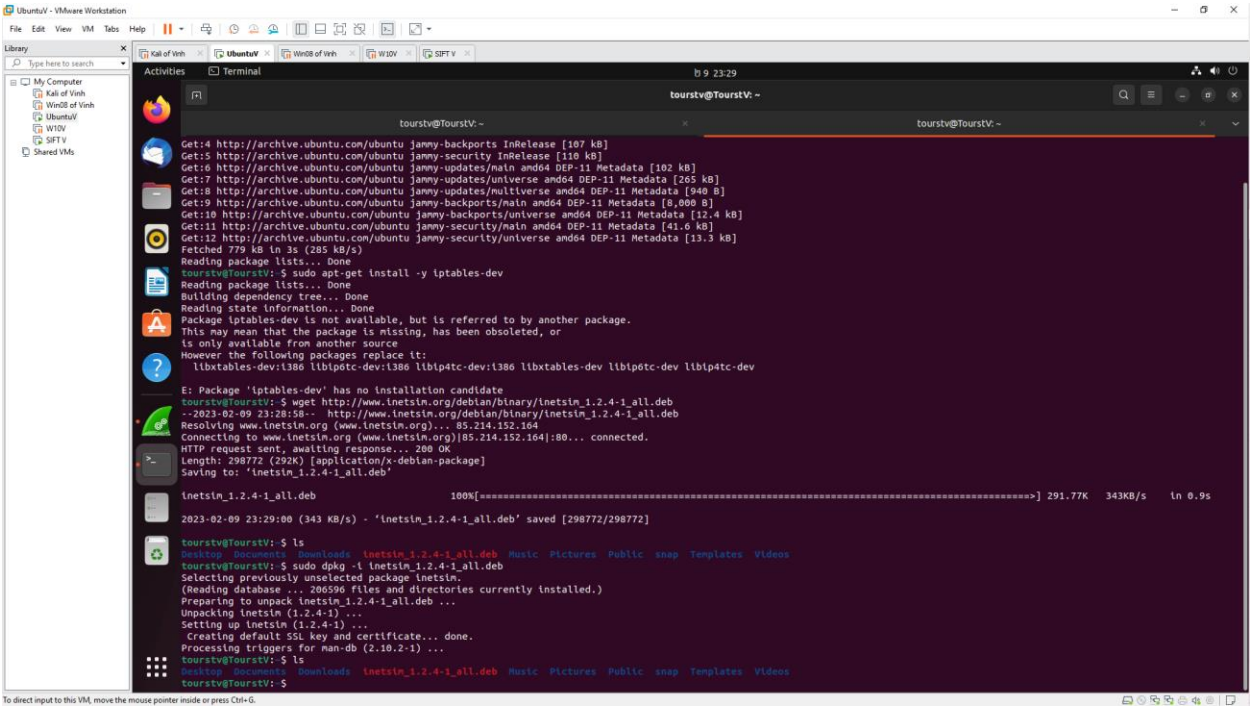
UbuntuV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali of Vinh
Win08 of Vinh
UbuntuV
W10V
SIFT V
Shared VMs
Kali of Vinh
UbuntuV
Win08 of Vinh
W10V
SIFT V
Activities
Terminal
9 23:25
tourstv@TourstV: ~
tourstv@TourstV: ~
tourstv@TourstV: ~
Unpacking libjson-perl (4.04000-1) ...
Selecting previously unselected package libstring-crc32-perl:amd64.
Preparing to unpack .../2-libstring-crc32-perl_2.100-1build1_amd64.deb ...
Unpacking libstring-crc32-perl:amd64 (2.100-1build1) ...
Selecting previously unselected package libipc-shareable-perl.
Preparing to unpack .../3-libipc-shareable-perl_1.06-2_all.deb ...
Unpacking libipc-shareable-perl (1.06-2) ...
Selecting previously unselected package libtypes-serialiser-perl.
Preparing to unpack .../4-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 .../5-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 libtypes-serialiser-perl (1.01-1) ...
Setting up libjson-perl (4.04000-1) ...
Setting up libjson-xs-perl (4.030-1build3) ...
Setting up libipc-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 i965-va-driver intel-media-va-driver libaacs0 libaom3 libass9 libavcodec58 libavformat58 libavutil56 libbdplus0 libblas3
libbluray2 libbs2b0 libchromaprint1 libcodec2-1.0 libdav1d5 libflashrom1 libflite1 libftdi1-2 libgme0 libgsm1 libgstreamer-plugins-bad1.0-0 libigdgmm12 liblilv-0-0 libllvm13
libmfx1 libmysofa1 libnorm1 libopenmpt0 libpgm-5.3-0 libpostproc55 librabbitmq4 librubberband2 libserd-0-0 libshine3 libsord-0-0 libsratom-0-0 libsrt1.4-gnutls libswresample3
libswscale5 libudfread0 libva-drm2 libva-wayland2 libva-x11-2 libva2 libvdpau1 libvidstab1.1 libx265-199 libxvidcore4 libzimg2 libzmq5 libzvbi-common libzvbi0 mesa-va-drivers
mesa-vdpau-drivers pocketsphinx-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.
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 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 'diversion of /usr/bin/shasum to /usr/bin/shasum.bundled by libdigest-sha-perl'
Adding 'diversion of /usr/share/man/man1/shasum.1.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) ...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



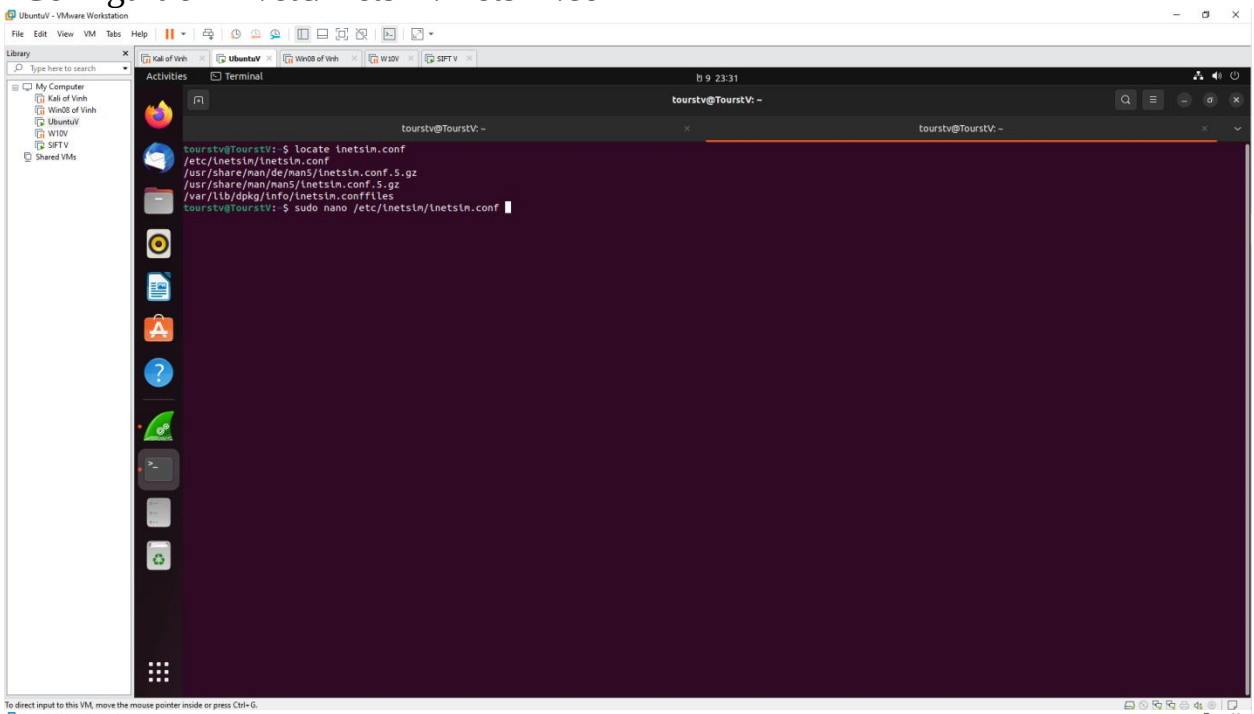
Dowload the INetSim

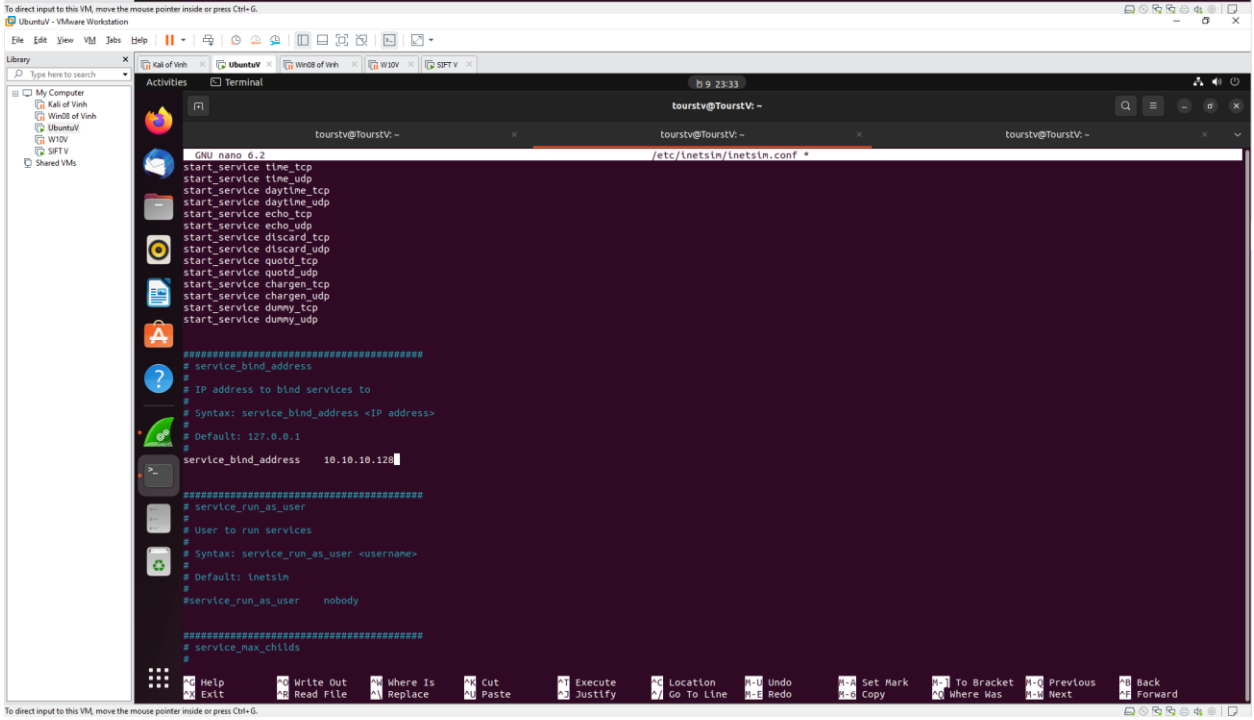
dpkg -i inetsim_1.2.4-1_all.deb

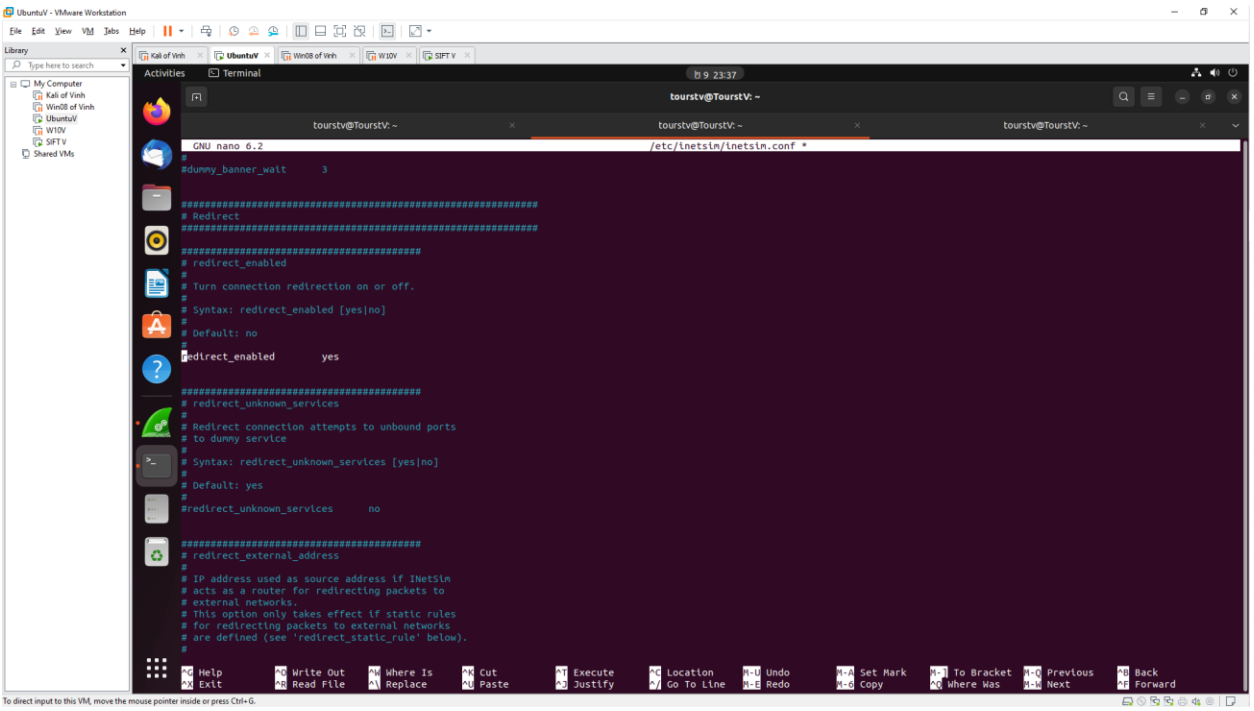

UbuntuV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali of Vinh
Win08 of Vinh
UbuntuV
W10V
SIFT V
Shared VMs
Kali of Vinh
UbuntuV
Win08 of Vinh
W10V
SIFT V
Activities
Terminal
9 23:29
toursv@TourstV: ~
toursv@TourstV: ~
toursv@TourstV: ~
toursv@TourstV:~$ sudo apt-get update -y
Hit:1 http://archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Hit:3 https://ppa.launchpadcontent.net/deadsnakes/ppa/ubuntu jammy InRelease
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 [940 B]
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
toursv@TourstV:~$ sudo apt-get install -y 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:i386 libip6tc-dev:i386 libip4tc-dev:i386 libxtables-dev libip6tc-dev libip4tc-dev
E: Package 'iptables-dev' has no installation candidate
toursv@TourstV:~$ wget http://www.inetsim.org/debian/binary/inetsim_1.2.4-1_all.deb
--2023-02-09 23:28:58-- http://www.inetsim.org/debian/binary/inetsim_1.2.4-1_all.deb
Resolving www.inetsim.org (www.inetsim.org)... 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: 'inetsim_1.2.4-1_all.deb'
inetsim_1.2.4-1_all.deb 100%[=>] 291.77K 343KB/s in 0.9s
2023-02-09 23:29:00 (343 KB/s) - 'inetsim_1.2.4-1_all.deb' saved [298772/298772]
toursv@TourstV:~$ ls
Desktop Documents Downloads inetsim_1.2.4-1_all.deb Music Pictures Public snap Templates Videos
toursv@TourstV:~$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

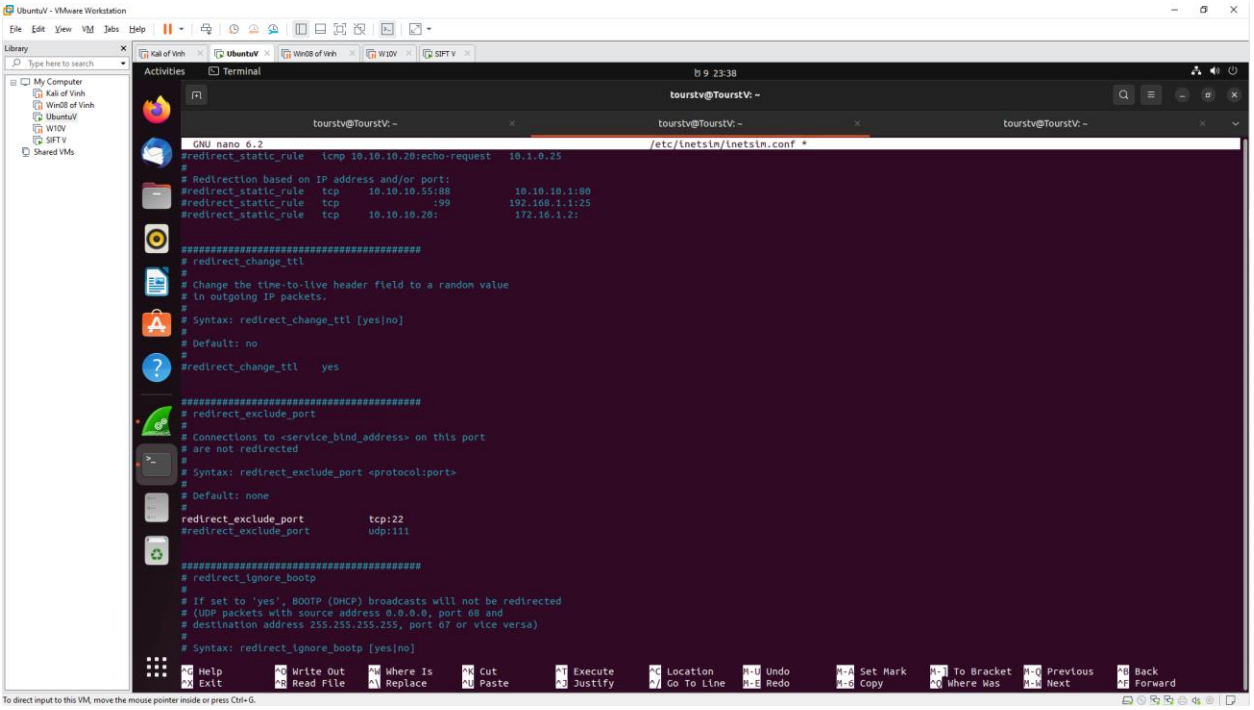

UbuntuV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali of Vinh
Win08 of Vinh
UbuntuV
W10V
SIFT V
Shared VMs
Kali of Vinh
UbuntuV
Win08 of Vinh
W10V
SIFT V
Activities
Terminal
9 23:29
toursv@TourstV: ~
toursv@TourstV: ~
toursv@TourstV: ~
Get:4 http://archive.ubuntu.com/ubuntu 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 [940 B]
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
toursv@TourstV:~$ sudo apt-get install -y 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:i386 libip6tc-dev:i386 libip4tc-dev:i386 libxtables-dev libip6tc-dev libip4tc-dev
E: Package 'iptables-dev' has no installation candidate
toursv@TourstV:~$ wget http://www.inetsim.org/debian/binary/inetsim_1.2.4-1_all.deb
--2023-02-09 23:28:58-- http://www.inetsim.org/debian/binary/inetsim_1.2.4-1_all.deb
Resolving www.inetsim.org (www.inetsim.org)... 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: 'inetsim_1.2.4-1_all.deb'
inetsim_1.2.4-1_all.deb 100%[=>] 291.77K 343KB/s in 0.9s
2023-02-09 23:29:00 (343 KB/s) - 'inetsim_1.2.4-1_all.deb' saved [298772/298772]
toursv@TourstV:~$ ls
Desktop Documents Downloads inetsim_1.2.4-1_all.deb Music Pictures Public snap Templates Videos
toursv@TourstV:~$ sudo dpkg -i inetsim_1.2.4-1_all.deb
Selecting previously unselected package inetsim.
(Reading database ... 206596 files and directories currently installed.)
Preparing to unpack inetsim_1.2.4-1_all.deb ...
Unpacking inetsim (1.2.4-1) ...
Setting up inetsim (1.2.4-1) ...
Creating default SSL key and certificate... done.
Processing triggers for man-db (2.10.2-1) ...
toursv@TourstV:~$ ls
Desktop Documents Downloads inetsim_1.2.4-1_all.deb Music Pictures Public snap Templates Videos
toursv@TourstV:~$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

- Configurtion in /etc/inetsim/inetsim.conf

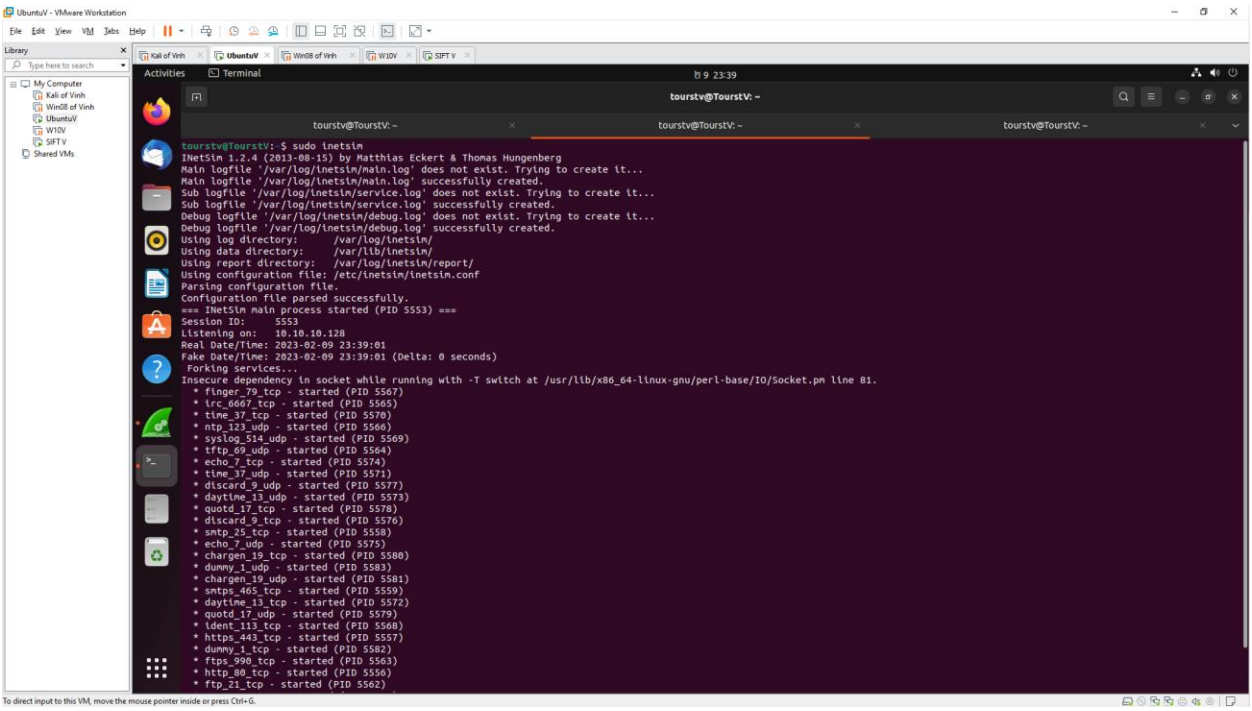




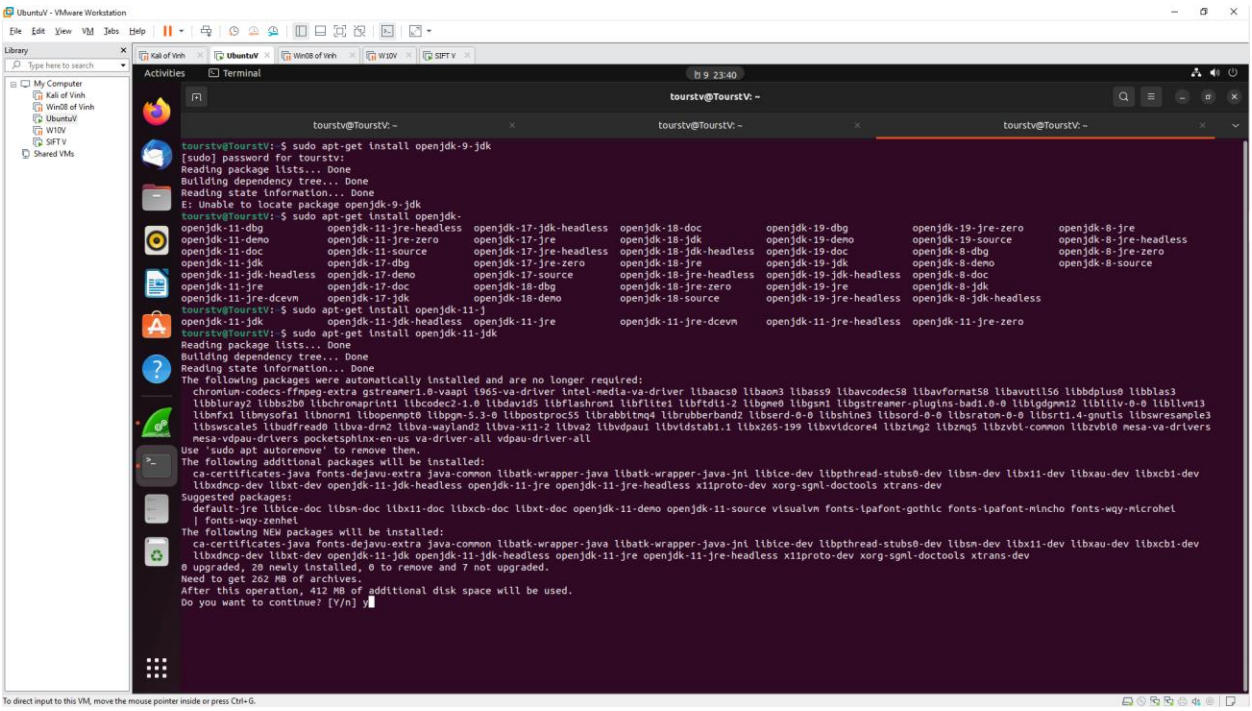


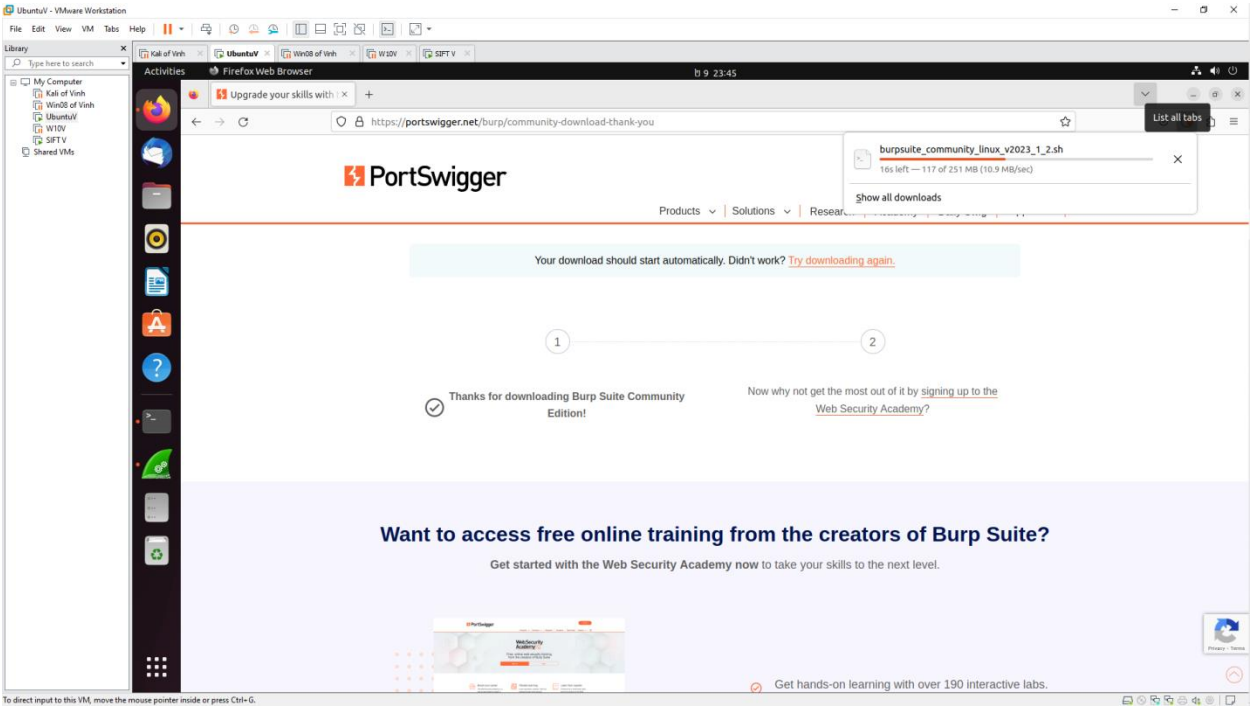


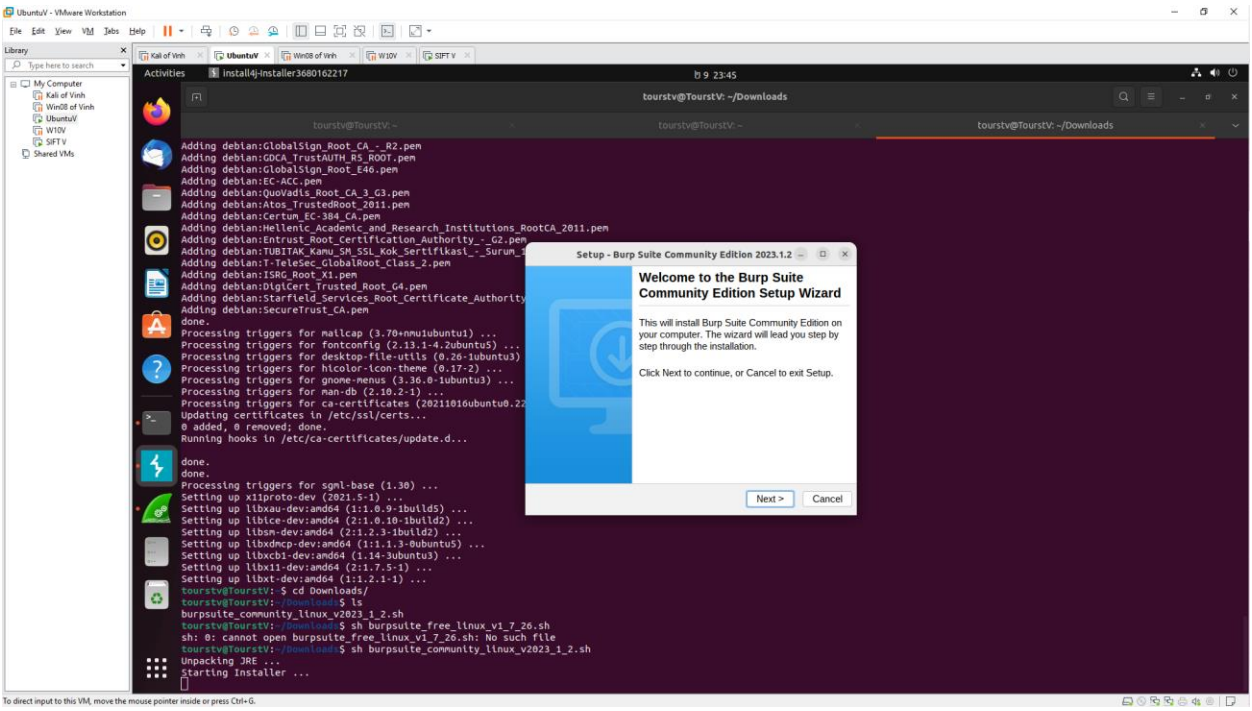
sudo inetsim

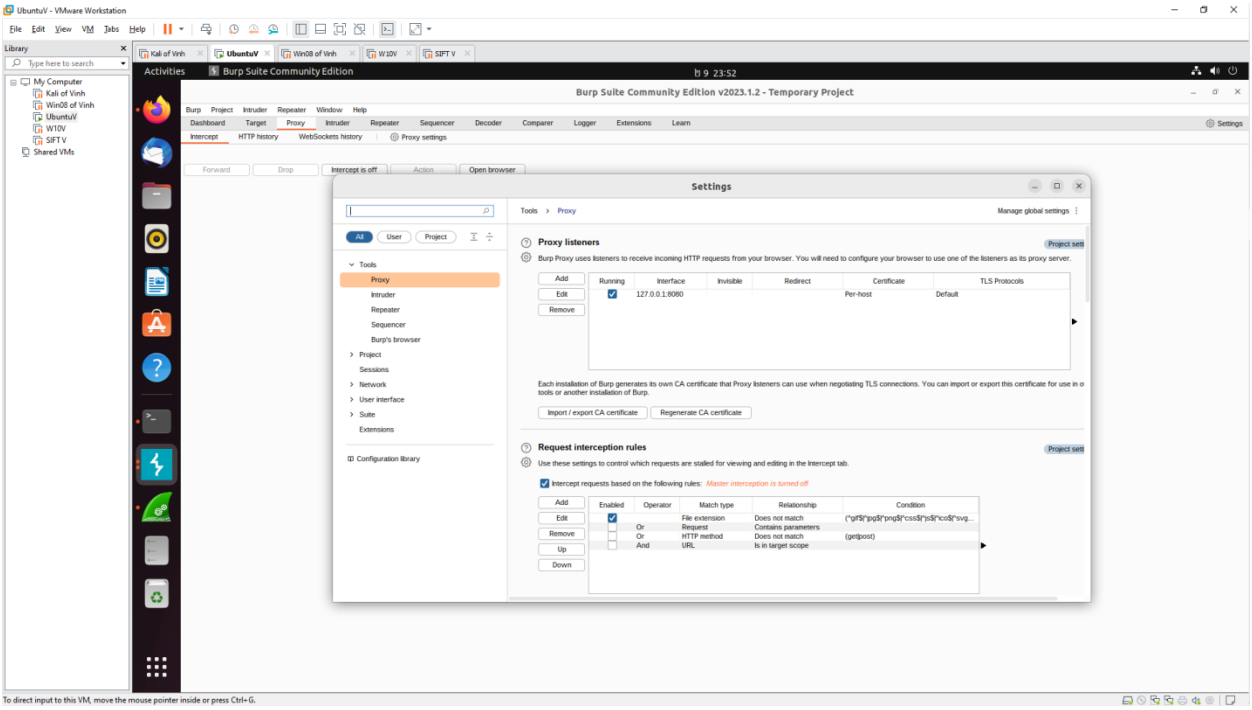


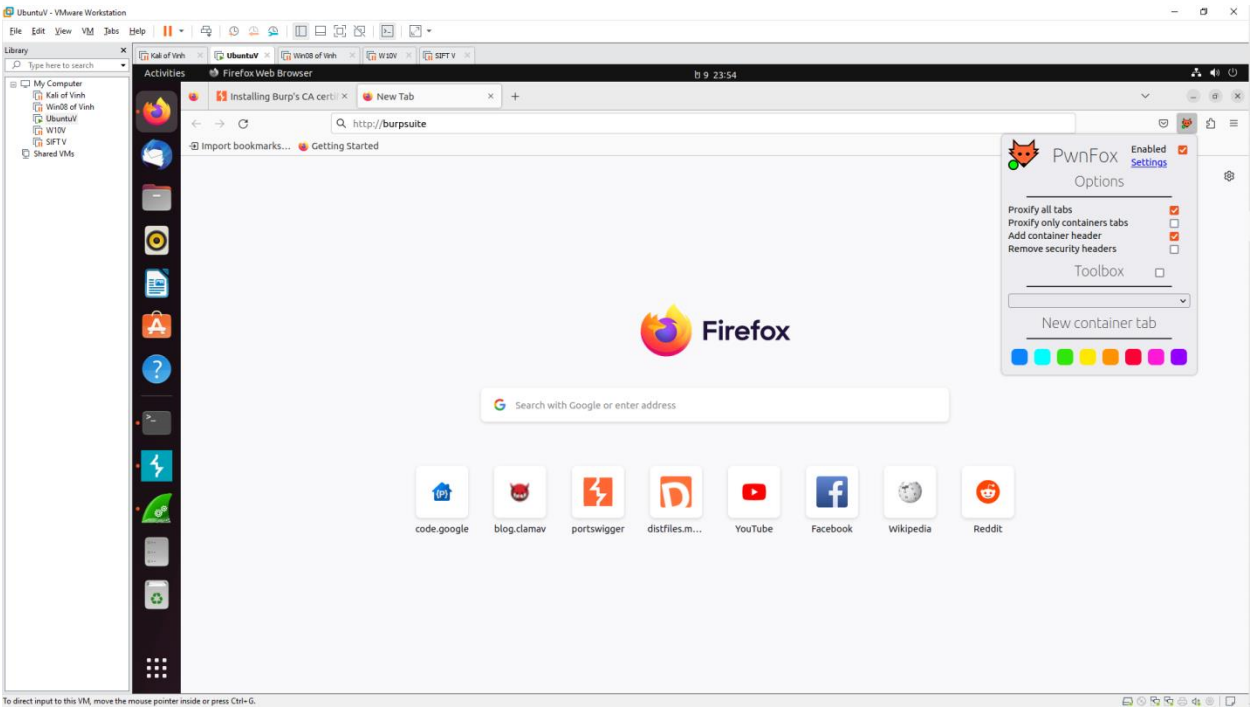
Install Burp Suite

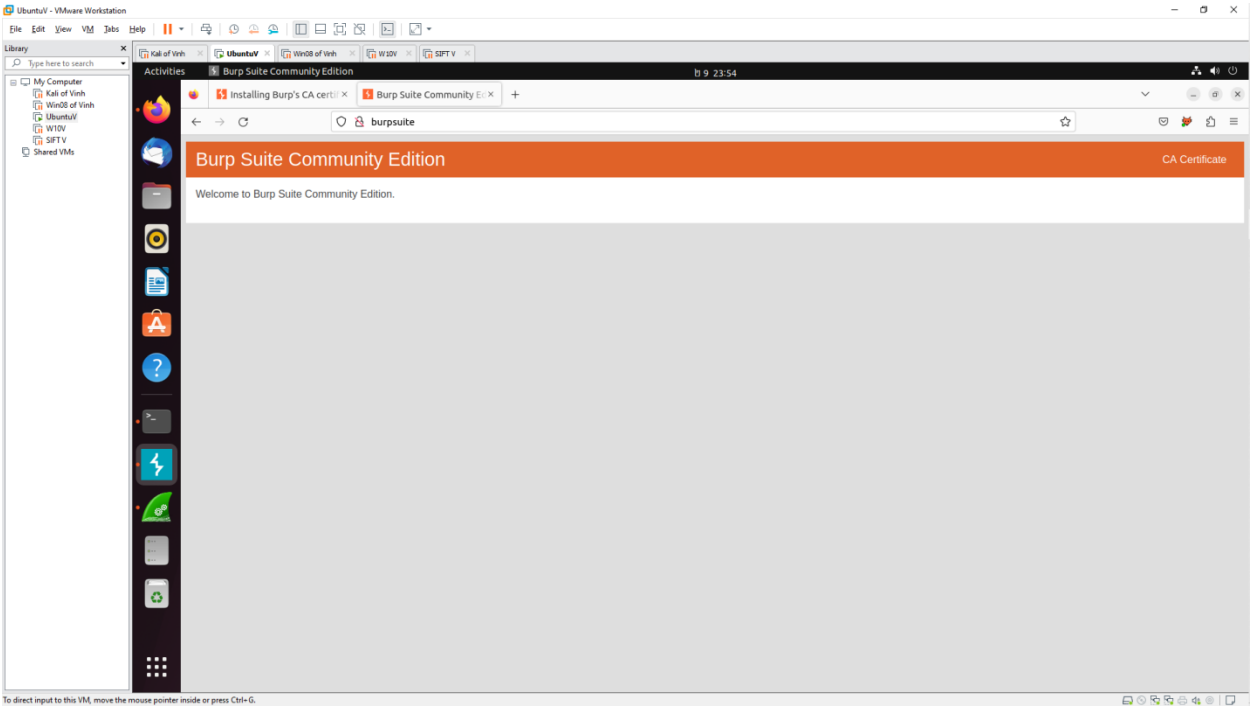

UbuntuV - VMware Workstation
File Edit View VM Tabs Help
Activities
Terminal
toorstv@TourstV: ~
toorstv@TourstV: $ sudo apt-get install openjdk-9-jdk
[sudo] password for toorstv:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package openjdk-9-jdk
toorstv@TourstV: $ sudo apt-get install openjdk-
openjdk-11-dbg openjdk-11-jre-headless openjdk-17-jdk-headless openjdk-18-doc openjdk-19-dbg openjdk-19-jre-zero openjdk-8-jre
openjdk-11-demo openjdk-11-jre-zero openjdk-17-jre openjdk-18-jdk openjdk-19-demo openjdk-19-source openjdk-8-jre-headless
openjdk-11-doc openjdk-11-source openjdk-17-jre-headless openjdk-18-jdk-headless openjdk-19-doc openjdk-8-dbg openjdk-8-jre-zero
openjdk-11-jdk openjdk-17-dbg openjdk-17-jre-zero openjdk-18-jre openjdk-19-jdk openjdk-8-demo openjdk-8-source
openjdk-11-jdk-headless openjdk-17-demo openjdk-17-source openjdk-18-jre-headless openjdk-19-jdk-headless openjdk-8-doc
openjdk-11-jre openjdk-17-doc openjdk-18-dbg openjdk-18-jre-zero openjdk-19-jre openjdk-8-jdk
openjdk-11-jre-dcevm openjdk-17-jdk openjdk-18-demo openjdk-18-source openjdk-19-jre-headless openjdk-8-jdk-headless
toorstv@TourstV: $ sudo apt-get install openjdk-11-j
openjdk-11-jdk openjdk-11-jdk-headless openjdk-11-jre openjdk-11-jre-dcevm openjdk-11-jre-headless openjdk-11-jre-zero
toorstv@TourstV: $ sudo apt-get install openjdk-11-jdk
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 i965-va-driver intel-media-va-driver libaacs0 libaom3 libass9 libavcodec58 libavformat58 libavutil56 libbdplus0 libblas3
libbluray2 libbs2b0 libchromaprint1 libcodec2-1.0 libdav1d5 libflashrom1 libflite1 libftdi1-2 libgme0 libgsm1 libgstreamer-plugins-bad1.0-0 libigdgmm12 liblilv-0-0 libllvm13
libmfx1 libmysofa1 libnorm1 libopenmpt0 libpgm-5.3-0 libpostproc55 librabbitmq4 librubberband2 libserd-0-0 libshine3 libsord-0-0 libsratom-0-0 libsrt1.4-gnutls libswresample3
libswscale5 libudfread0 libva-drm2 libva-wayland2 libva-x11-2 libva2 libvdpau1 libvidstab1.1 libx265-199 libxvidcore4 libzimg2 libzmq5 libzvbi-common libzvbi0 mesa-va-drivers
mesa-vdpau-drivers pocketsphinx-en-us va-driver-all vdpau-driver-all
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
ca-certificates-java fonts-dejavu-extra java-common libatk-wrapper-java libatk-wrapper-java-jni libice-dev libpthread-stubs0-dev libsm-dev libx11-dev libxau-dev libxcb1-dev
libxdmcp-dev libxt-dev openjdk-11-jdk-headless openjdk-11-jre openjdk-11-jre-headless x11proto-dev xorg-sgml-doctools xtrans-dev
Suggested packages:
default-jre libice-doc libsm-doc libx11-doc libxcb-doc libxt-doc openjdk-11-demo openjdk-11-source visualvm fonts-ipafont-gothic fonts-ipafont-mincho fonts-wqy-microhei
| fonts-wqy-zenhei
The following NEW packages will be installed:
ca-certificates-java fonts-dejavu-extra java-common libatk-wrapper-java libatk-wrapper-java-jni libice-dev libpthread-stubs0-dev libsm-dev libx11-dev libxau-dev libxcb1-dev
libxdmcp-dev libxt-dev openjdk-11-jdk openjdk-11-jdk-headless openjdk-11-jre openjdk-11-jre-headless x11proto-dev xorg-sgml-doctools xtrans-dev
0 upgraded, 20 newly installed, 0 to remove and 7 not upgraded.
Need to get 262 MB of archives.
After this operation, 412 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


UbuntuV - VMware Workstation
Activities
Firefox Web Browser
Upgrade your skills with
https://portswigger.net/burp/community-download-thank-you
List all tabs
burpsuite_community_linux_v2023_1_2.sh
16s left — 117 of 251 MB (10.9 MB/sec)
Show all downloads
PortSwigger
Products
Solutions
Your download should start automatically. Didn't work? Try downloading again.
1
2
Thanks for downloading Burp Suite Community Edition!
Now why not get the most out of it by signing up to the Web Security Academy?
Want to access free online training from the creators of Burp Suite?
Get started with the Web Security Academy now to take your skills to the next level.
Get hands-on learning with over 190 interactive labs.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

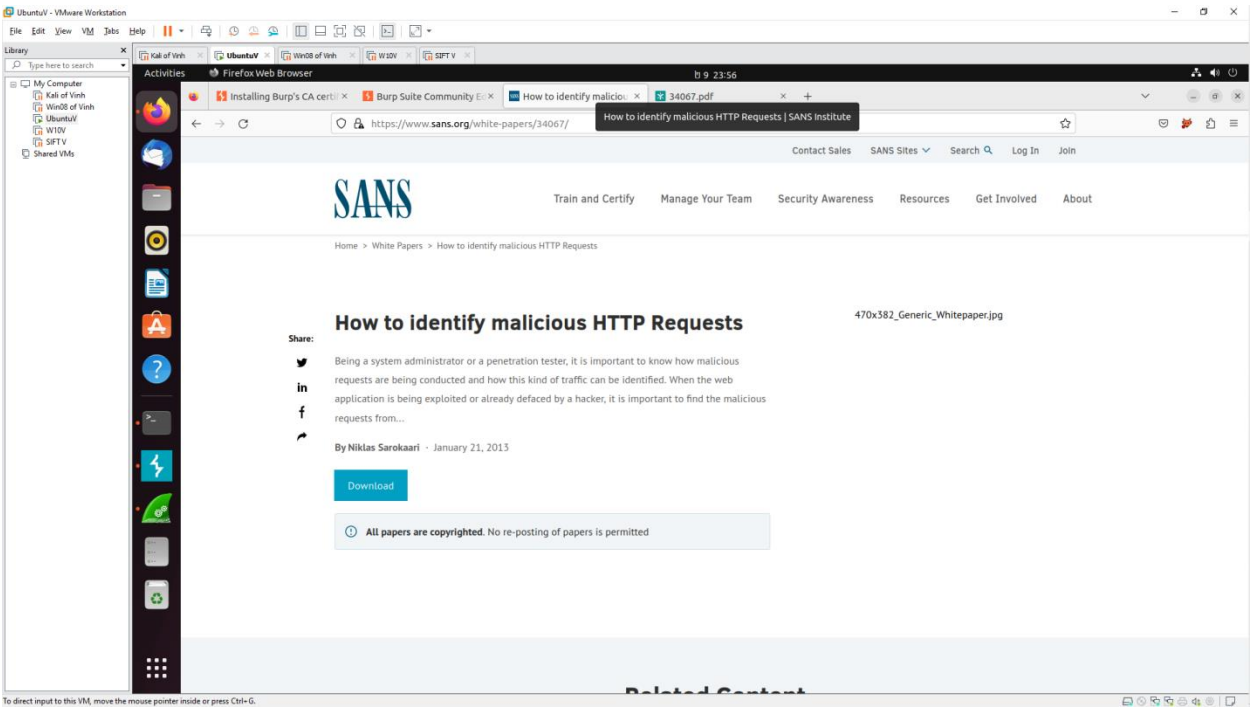

UbuntuV - VMware Workstation
Activities
install4j-installer3680162217
tourstv@TourstV: ~/Downloads
Setup - Burp Suite Community Edition 2023.1.2
Welcome to the Burp Suite Community Edition Setup Wizard
This will install Burp Suite Community Edition on your computer. The wizard will lead you step by step through the installation.
Click Next to continue, or Cancel to exit Setup.
Next >
Cancel
tourstv@TourstV: ~/Downloads$ ls
burpsuite_community_linux_v2023_1_2.sh
tourstv@TourstV: ~/Downloads$ sh burpsuite_free_linux_v1_7_26.sh
sh: 0: cannot open burpsuite_free_linux_v1_7_26.sh: No such file
tourstv@TourstV: ~/Downloads$ sh burpsuite_community_linux_v2023_1_2.sh
Unpacking JRE ...
Starting Installer ...


UbuntuV - VMware Workstation
Activities
Burp Suite Community Edition
Burp Suite Community Edition v2023.1.2 - Temporary Project
Settings
Proxy listeners
Request interception rules

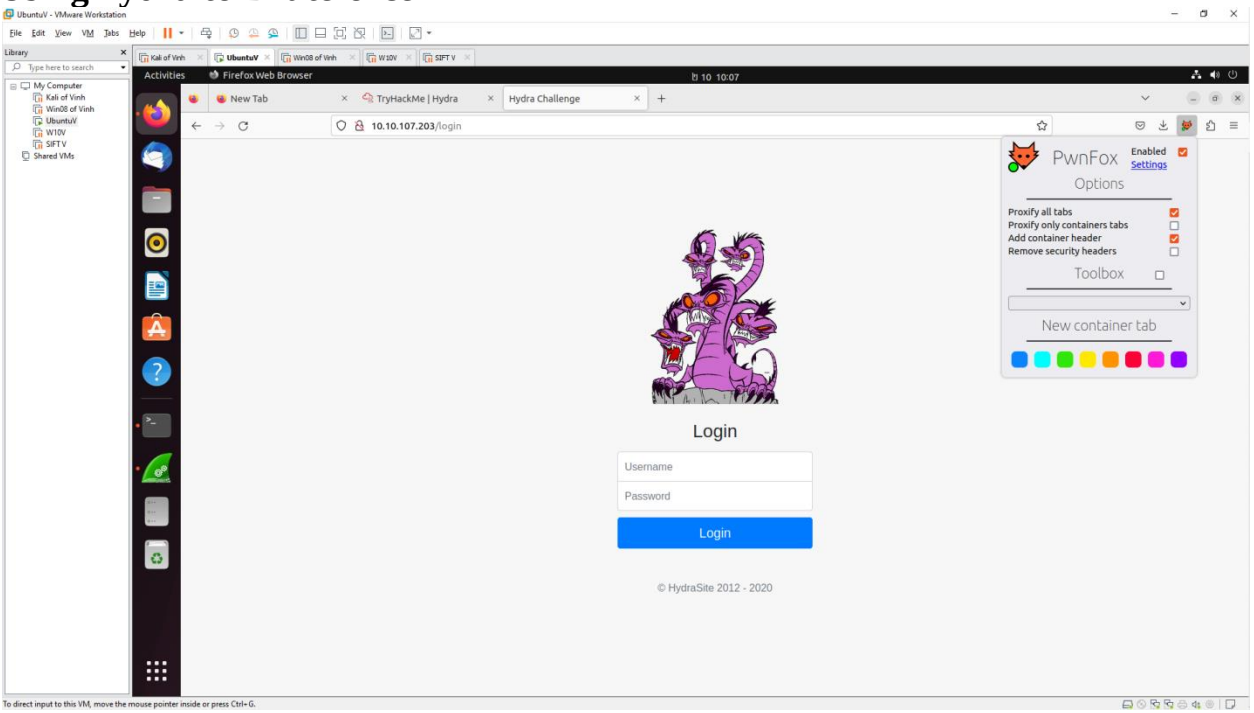

UbuntuV - VMware Workstation
Activities
Firefox Web Browser
Installing Burp's CA certi
New Tab
http://burpsuite
Import bookmarks...
Getting Started
PwnFox
Enabled
Settings
Options
Proxify all tabs
Proxify only containers tabs
Add container header
Remove security headers
Toolbox
New container tab
Firefox
Search with Google or enter address
code.google
blog.clamav
portswigger
distfiles.m...
YouTube
Facebook
Wikipedia
Reddit
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


UbuntuV - VMware Workstation
Activities
Burp Suite Community Edition
Installing Burp's CA certi
Burp Suite Community E
burpsuite
Burp Suite Community Edition
CA Certificate
Welcome to Burp Suite Community Edition.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

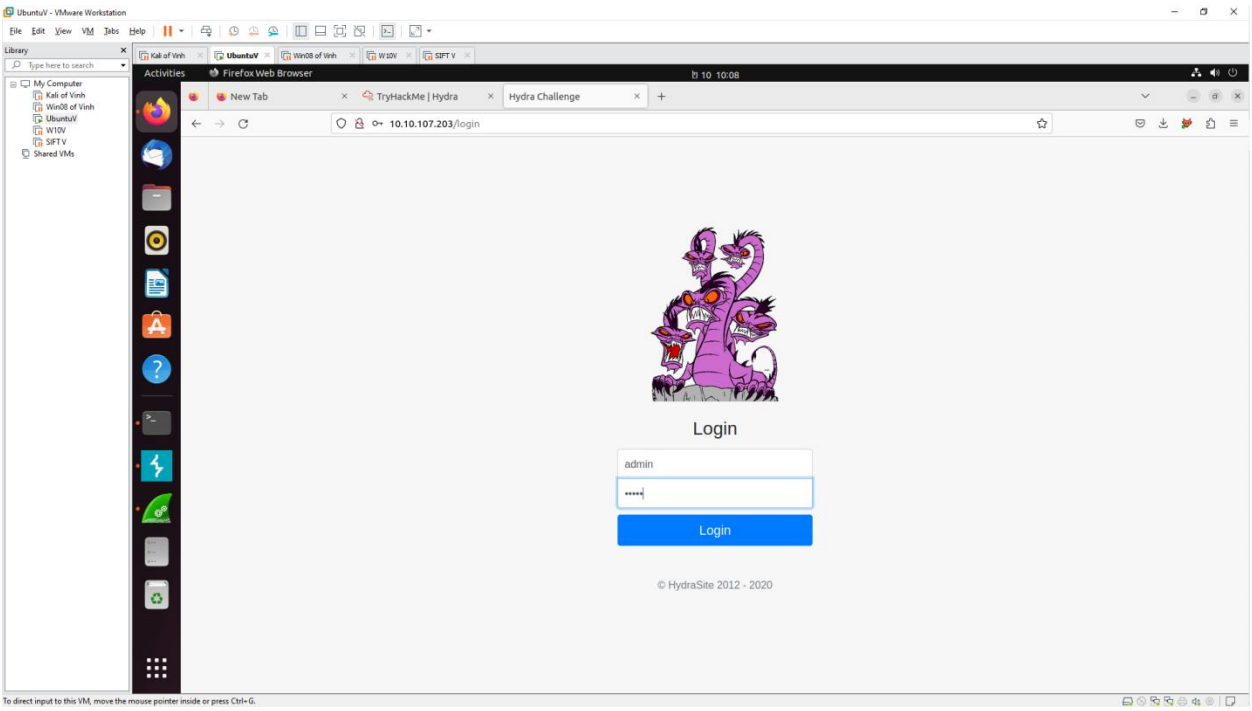
WORKSHOP1

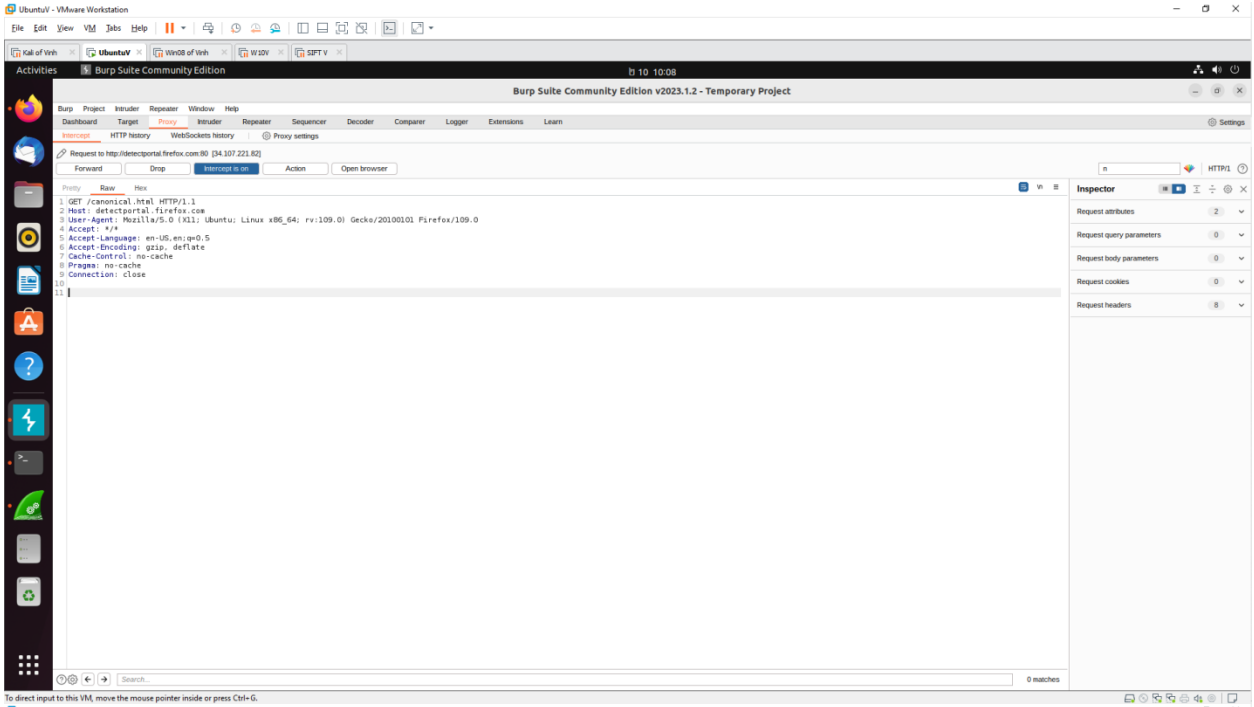


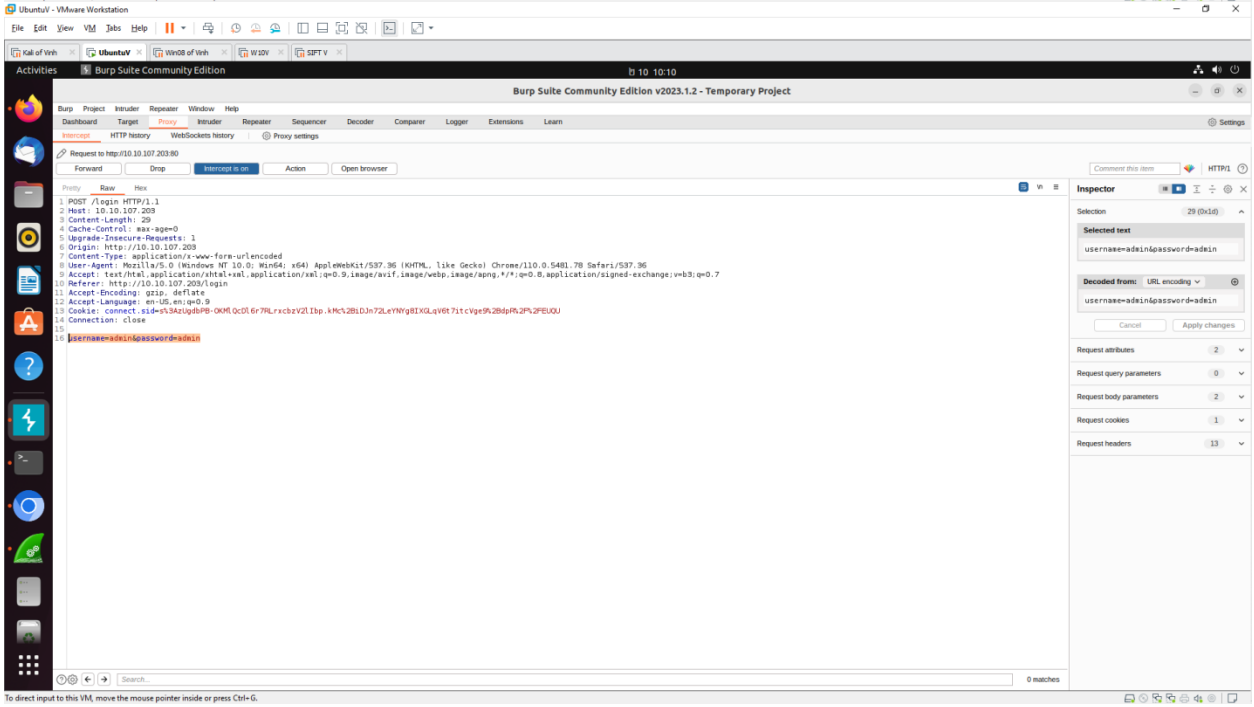
Using hydra to Bruteforce

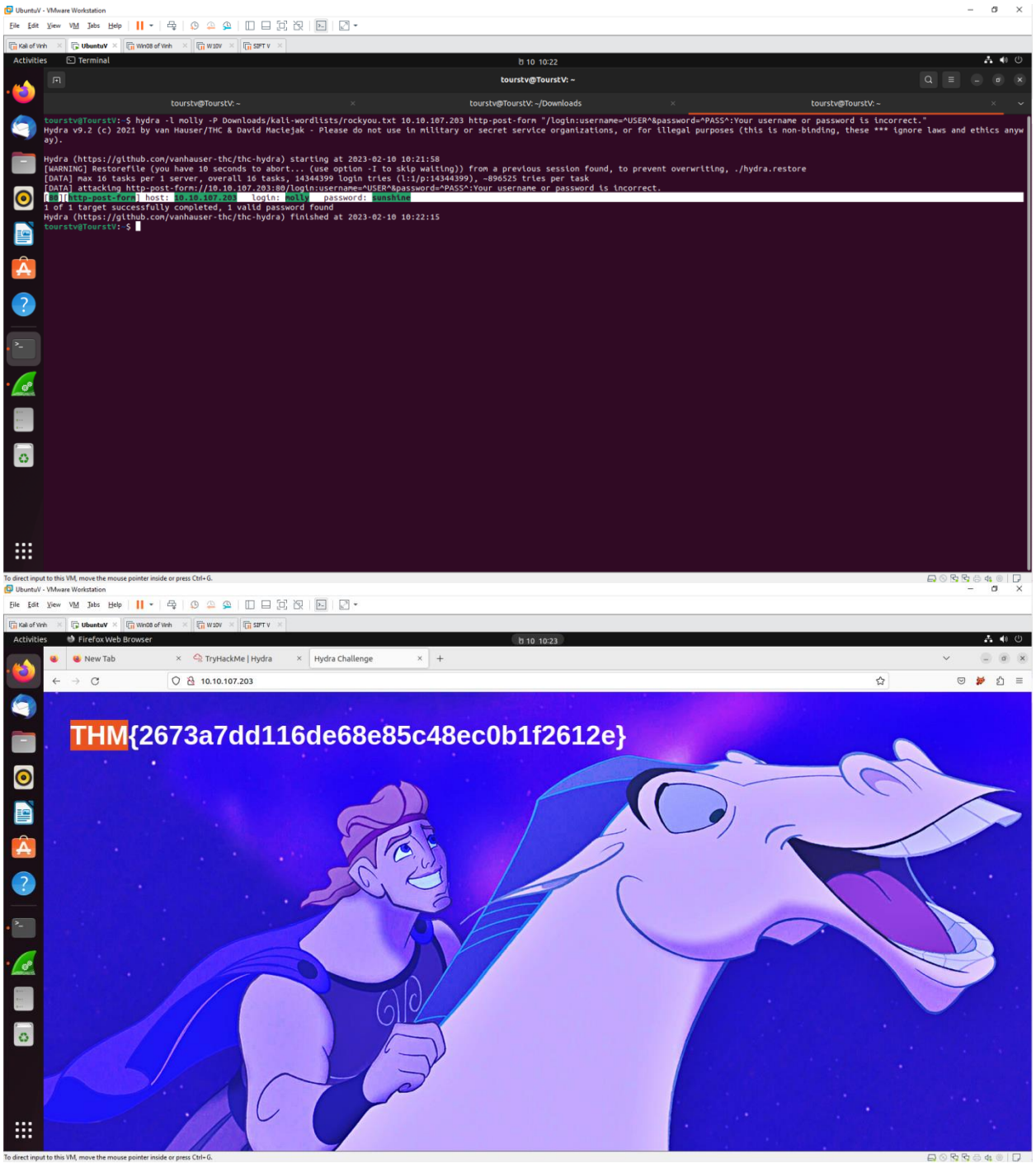


- login with ‘admin@admin’


UbuntuV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali of Vinh
Win08 of Vinh
UbuntuV
W10V
SIFT V
Shared VMs
Activities
Firefox Web Browser
10 10:08
New Tab
TryHackMe | Hydra
Hydra Challenge
10.10.107.203/login
Login
admin
Login
© HydraSite 2012 - 2020
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


UbuntuV - VMware Workstation
Activities
Burp Suite Community Edition
Burp Suite Community Edition v2023.1.2 - Temporary Project
Request to http://detectportal.firefox.com:80 [34.107.221.82]
Forward
Drop
Intercept is on
Action
Open browser
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
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
Pragma: no-cache
Connection: close
Inspector
0 matches
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

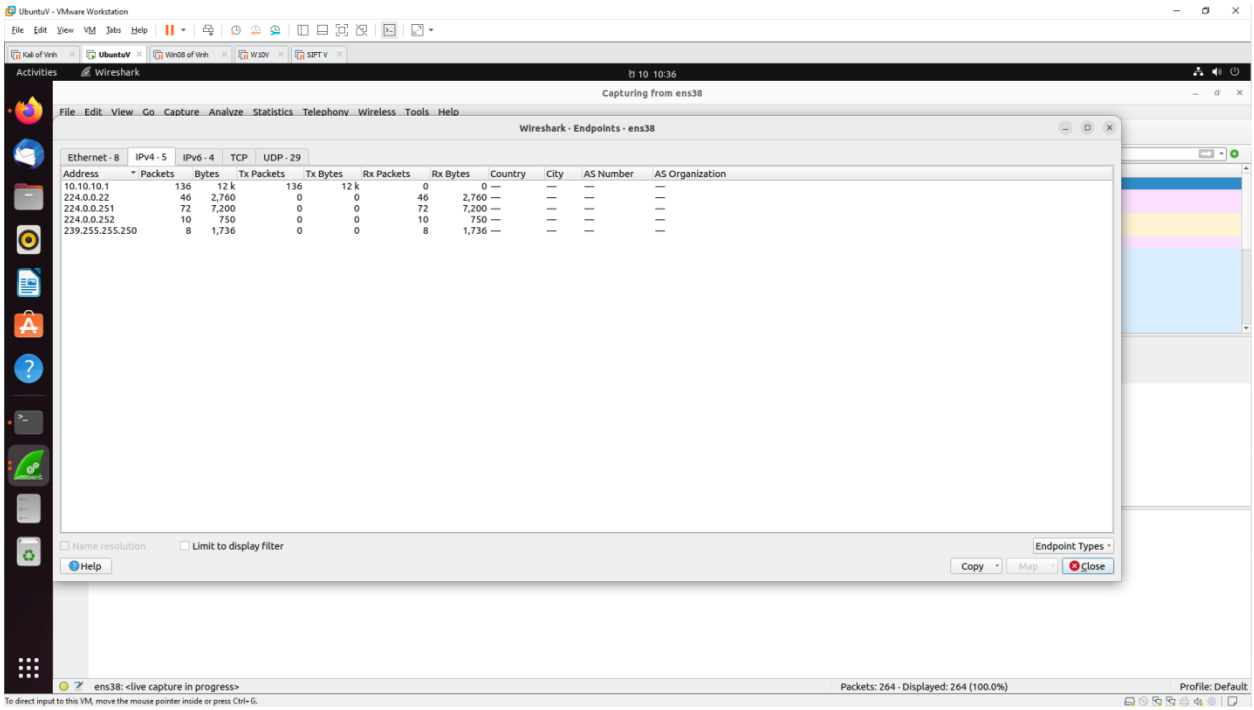

UbuntuV - VMware Workstation
Activities
Burp Suite Community Edition
Burp Suite Community Edition v2023.1.2 - Temporary Project
Request to http://10.10.107.203:80
Forward
Drop
Intercept is on
Action
Open browser
POST /login HTTP/1.1
Host: 10.10.107.203
Content-Length: 29
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.107.203
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.107.203/login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: connect.sid=s%3AzUgdbPB-OKMlQcDl6r7RLrxcbzV2lIbp.kMc%2BiDJn72LeYNYg8IXGLqV6t7itcVge9%2BdpPk2P%2FEUOU
Connection: close
username=admin&password=admin
Inspector
Selection
Selected text
username=admin&password=admin
Decoded from: URL encoding
username=admin&password=admin
Cancel
Apply changes
0 matches
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



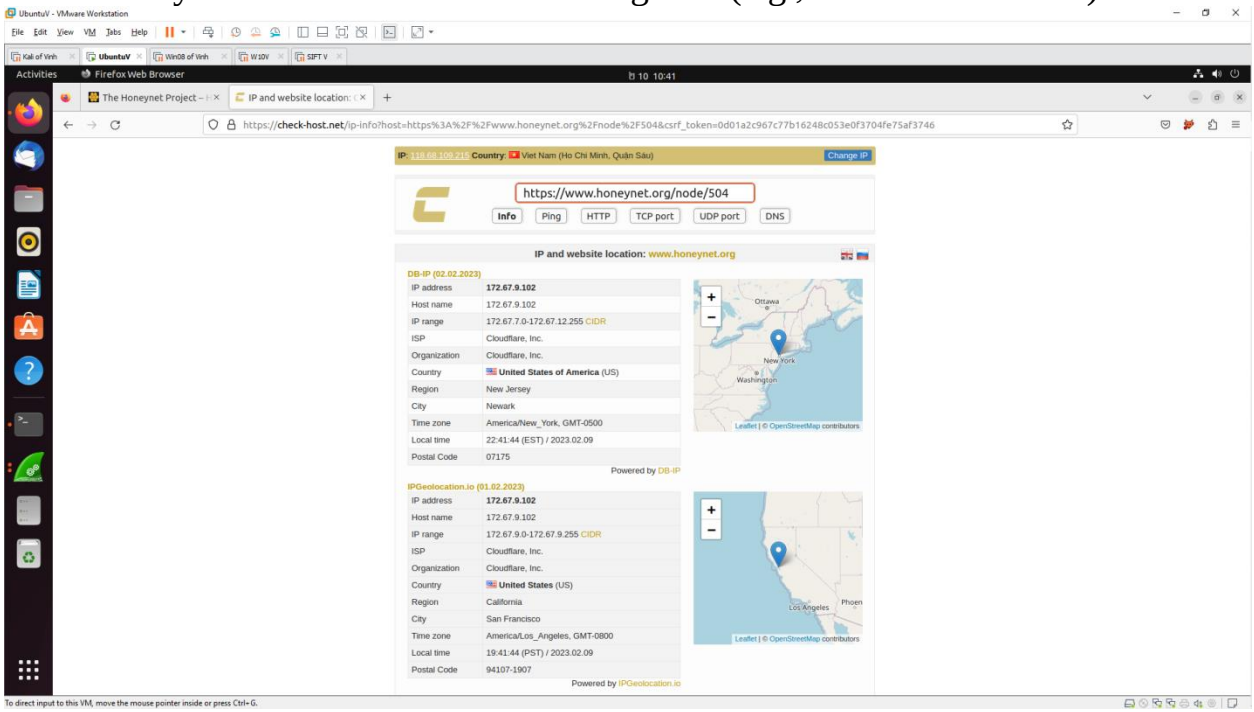
WORKSHOP2

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

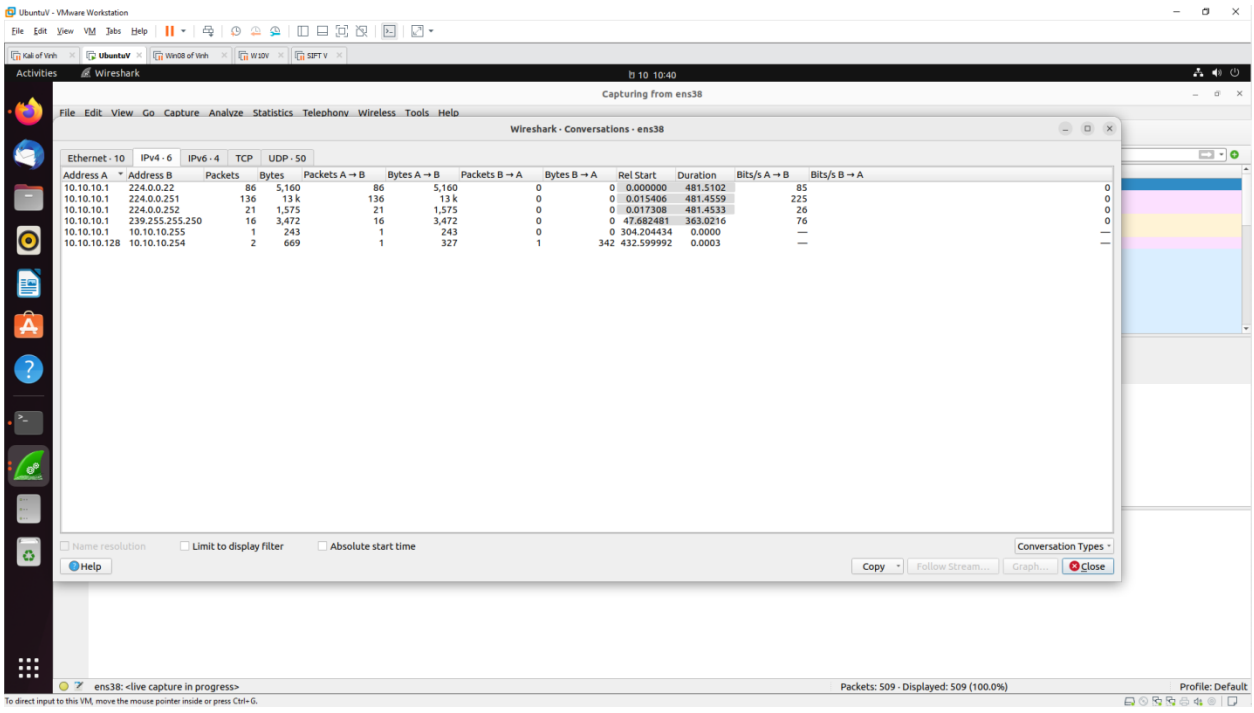
-



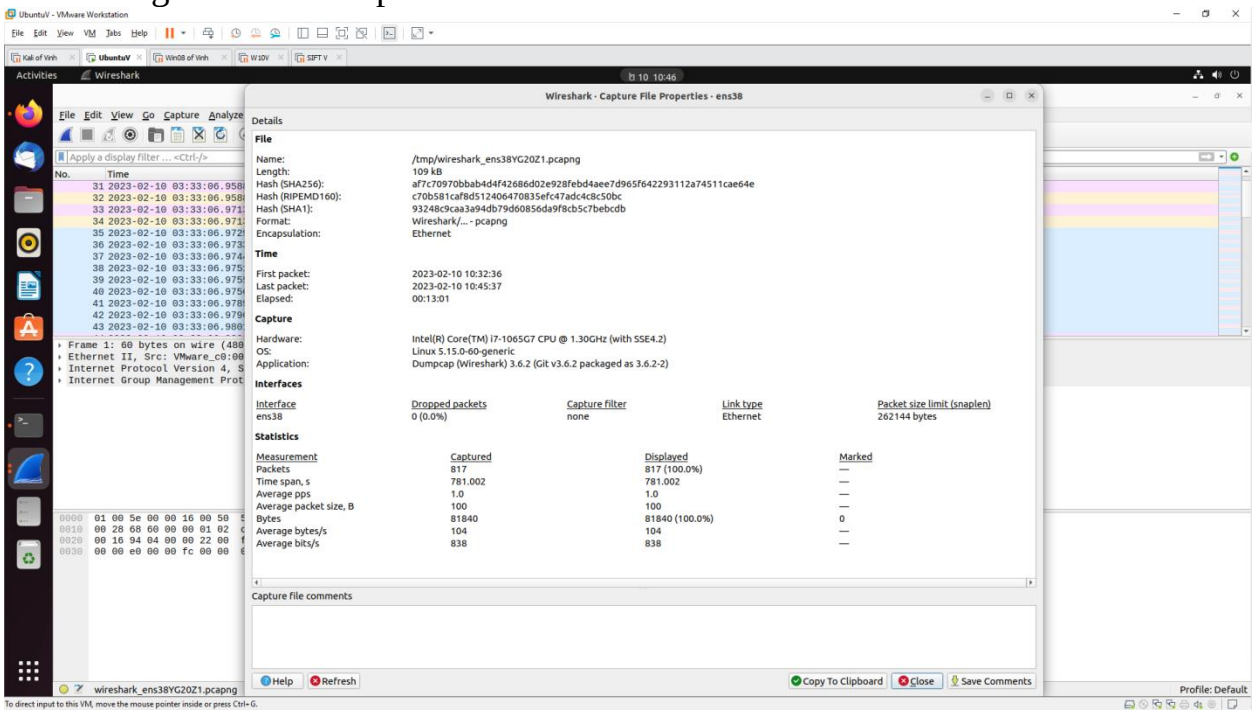
- What can you find out about the attacking host (e.g., where is it located)?



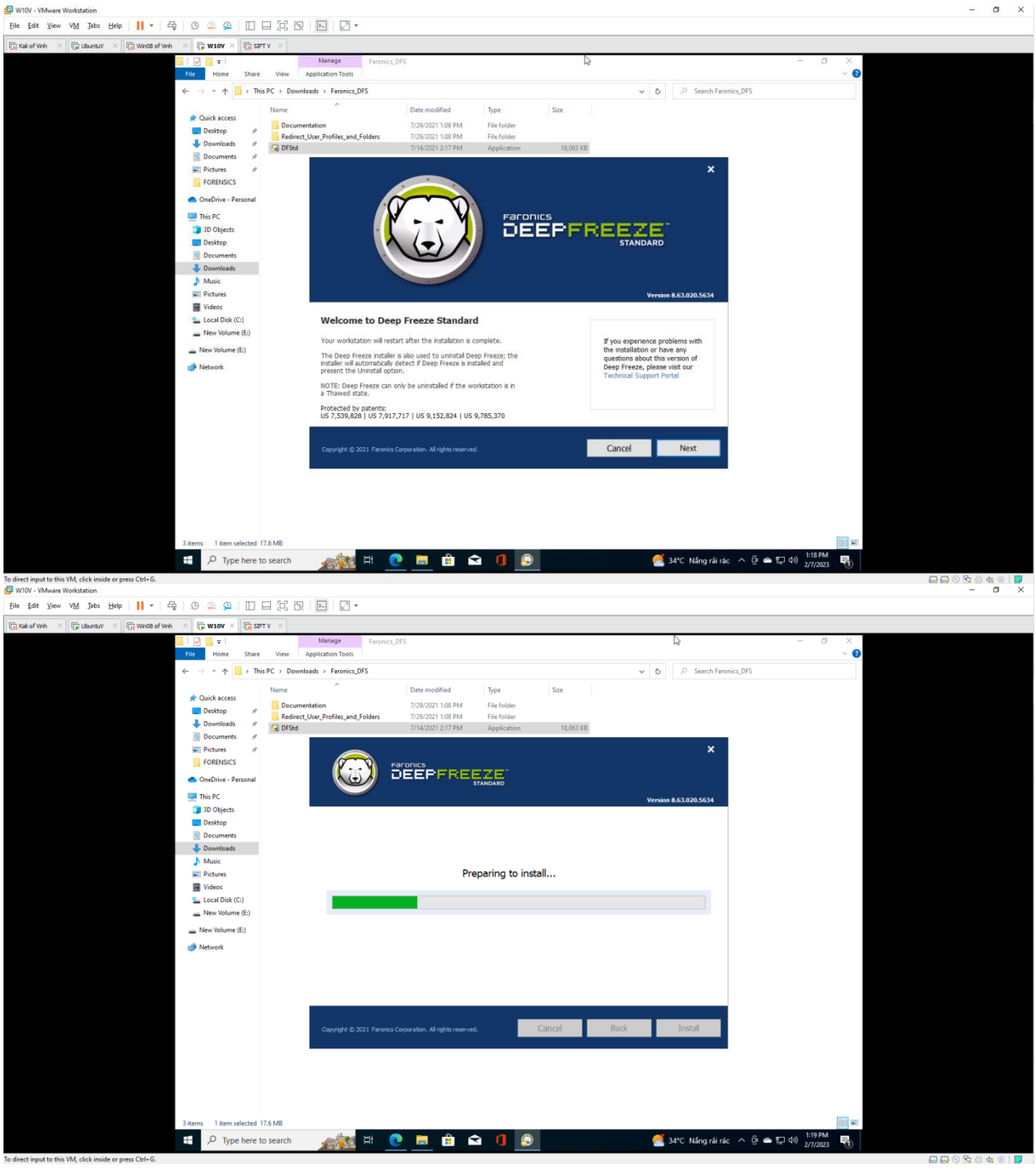
- How many TCP sessions are contained in the dump file?



- How long did it take to perform the attack?



Install Deep Freeze

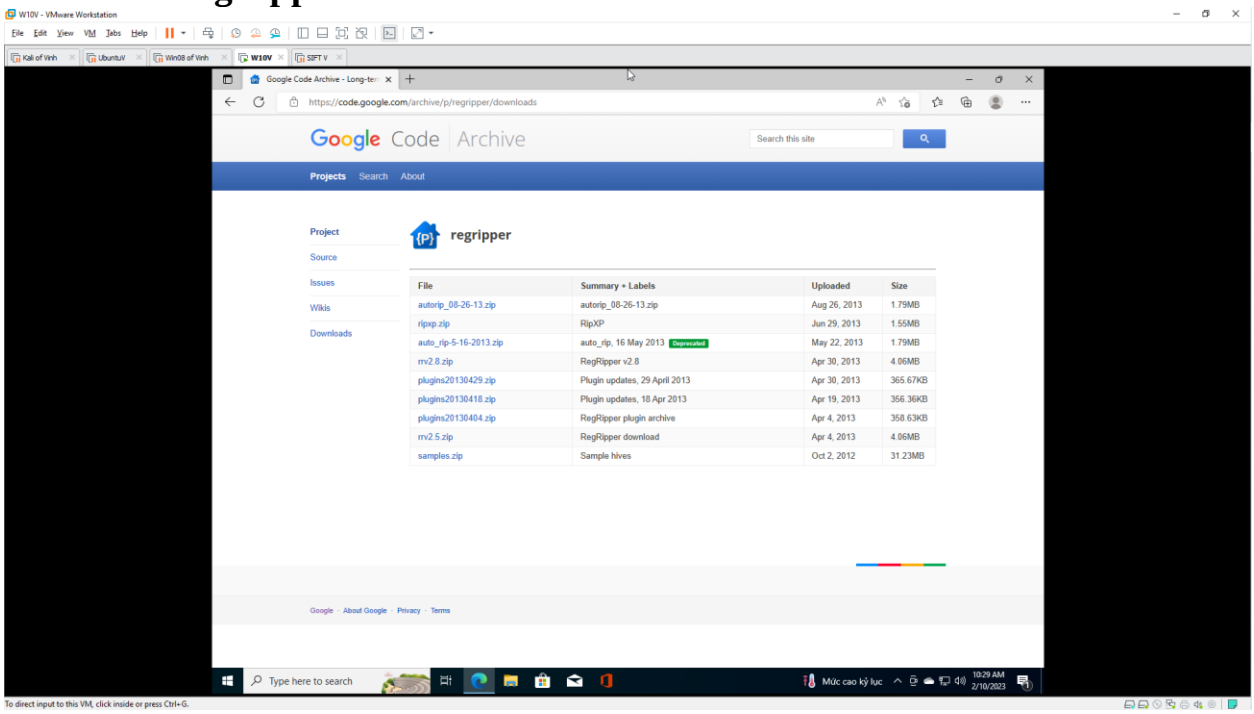


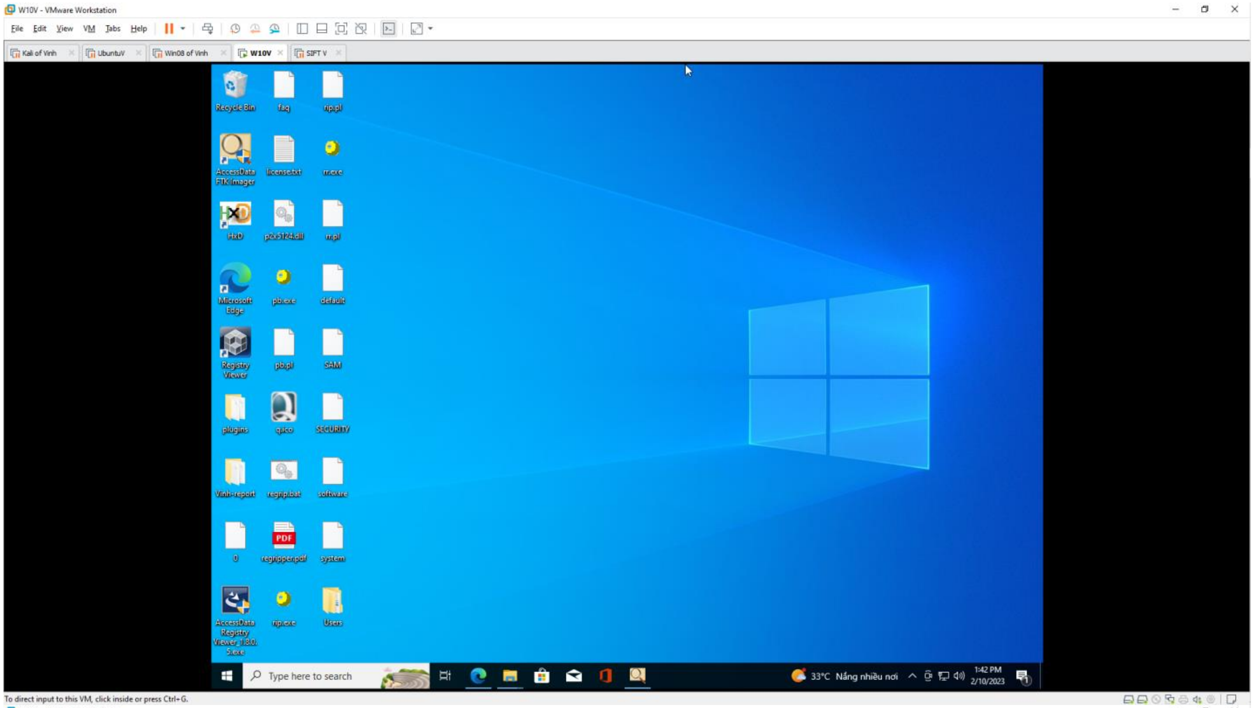
LAB 7.2: Registry Forensics with RegRipper Plug-ins

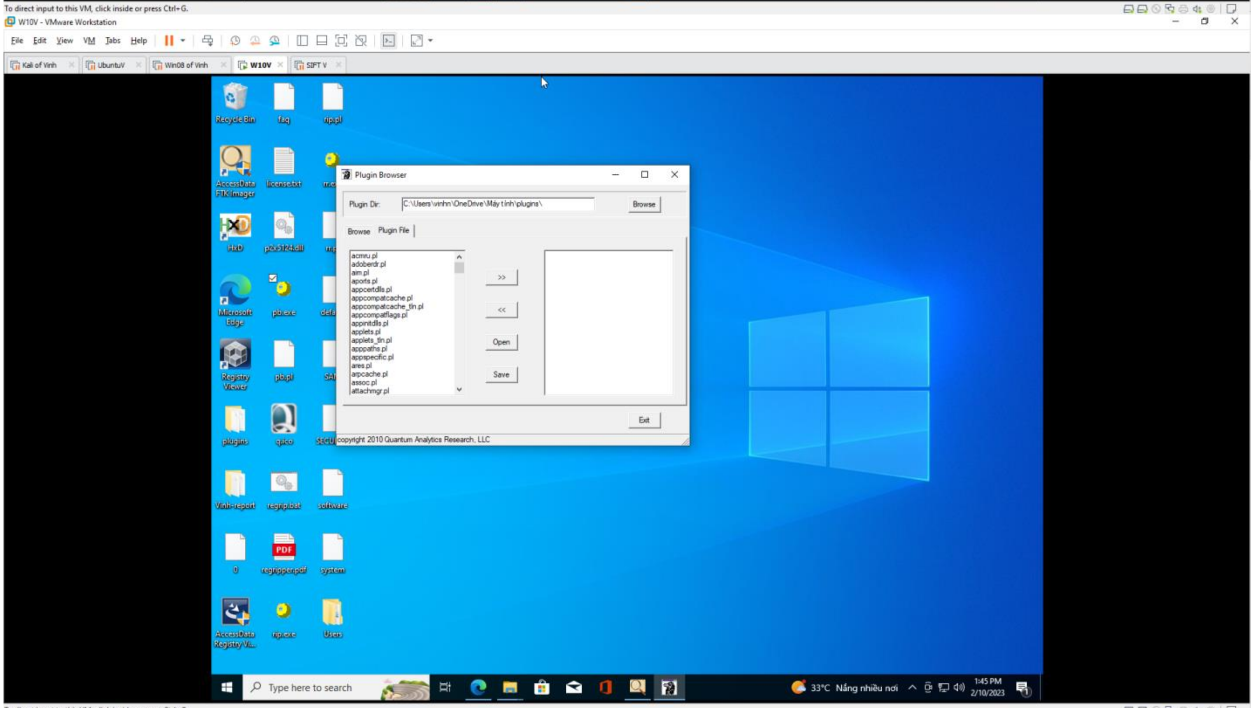
Purpose:

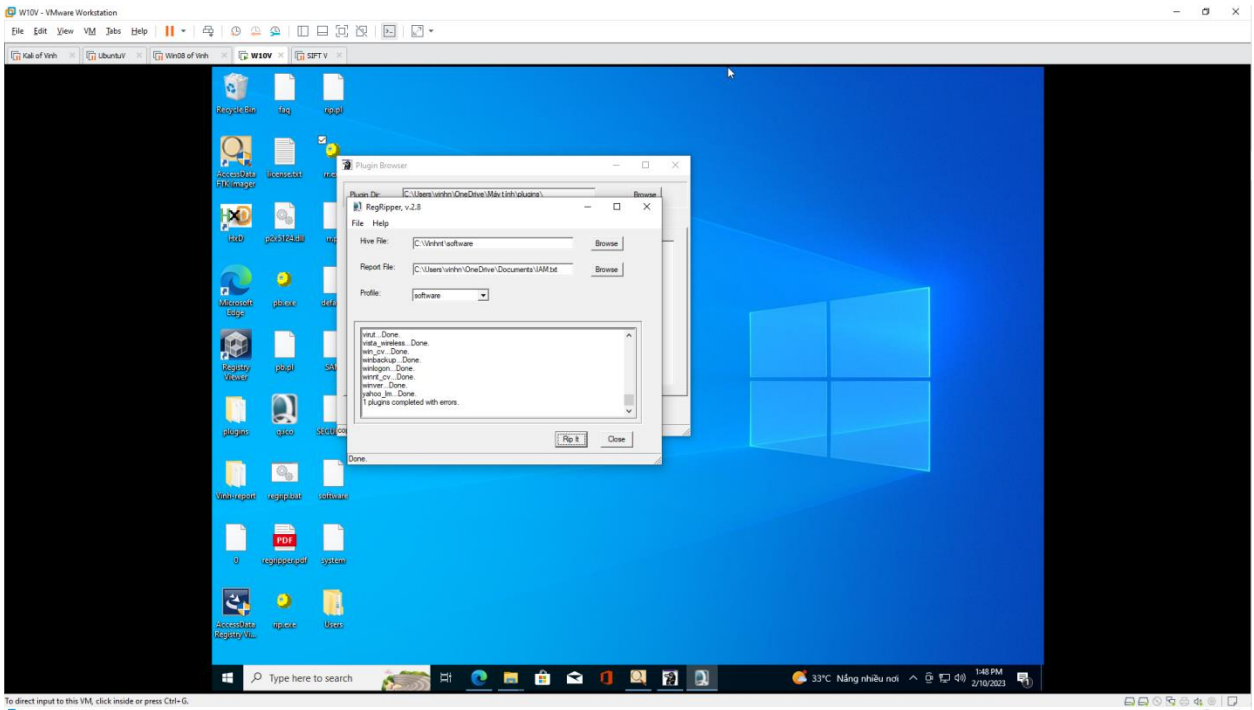
- Introduction to the window registry.
- Introduction to RegRipper.
- Analysis of Registry files with RegRipper.

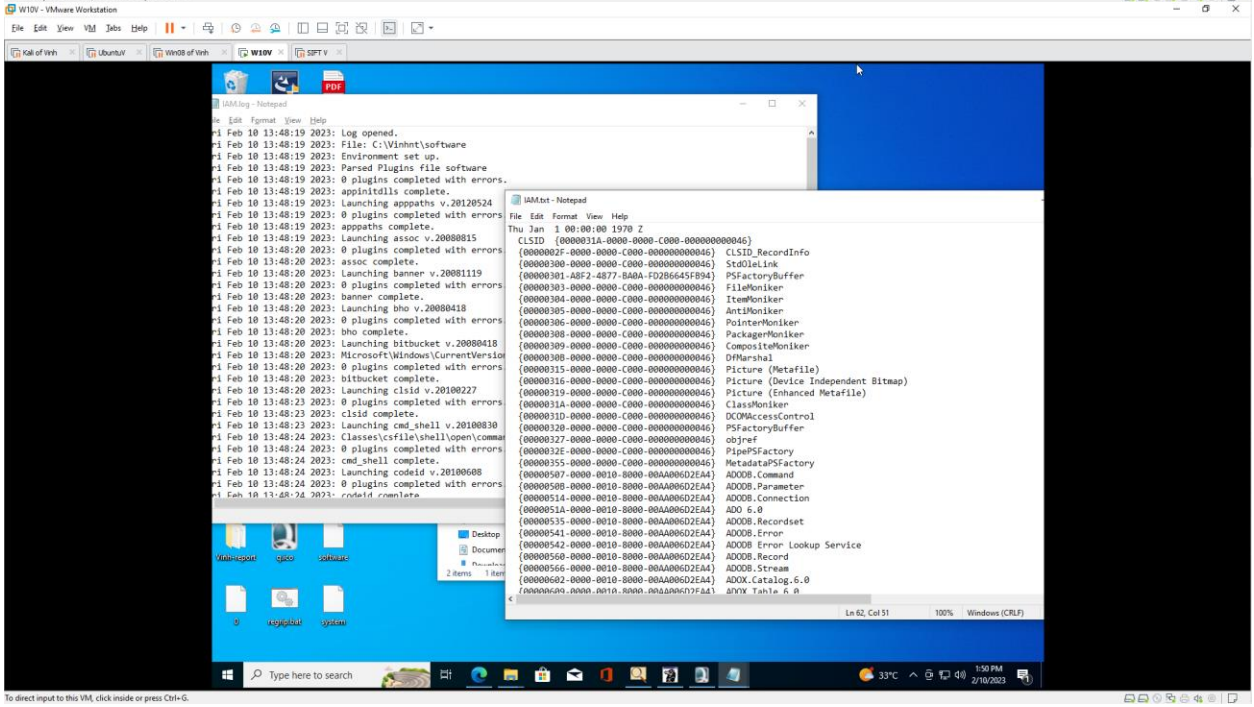
Download RegRipper




W10V - VMware Workstation
File Edit View VM Tabs Help
Kali of Vinh
UbuntuV
Win08 of Vinh
W10V
SIFT V
Type here to search
33°C Nắng nhiều nơi
1:42 PM
2/10/2023
To direct input to this VM, click inside or press Ctrl+G.


W10V - VMware Workstation
File Edit View VM Tabs Help
Kali of Vinh
UbuntuV
Win08 of Vinh
W10V
SIFT V
Plugin Browser
Plugin Dir:
Browse
Plugin File
acmru.pl
adoberdr.pl
aim.pl
aports.pl
appcertdlls.pl
appcompatcache.pl
appcompatcache_tln.pl
appcompatflags.pl
appinitdlls.pl
applets.pl
applets_tln.pl
apppaths.pl
appspecific.pl
arpcache.pl
assoc.pl
attachmgr.pl
>>
<<
Open
Save
Exit
copyright 2010 Quantum Analytics Research, LLC
Type here to search
33°C Nắng nhiều nơi
1:45 PM
2/10/2023
To direct input to this VM, click inside or press Ctrl+G.


W10V - VMware Workstation
RegRipper, v.2.8
Plugin Browser
Hive File: C:\Vinhnt\software
Report File: C:\Users\vinhn\OneDrive\Documents\IAM.txt
Profile: software
1 plugins completed with errors.
Close
Type here to search
33°C Nắng nhiều nơi
1:48 PM
2/10/2023


W10V - VMware Workstation
IAM.txt - Notepad
Thu Jan 1 00:00:00 1970 Z
Type here to search
33°C
1:50 PM
2/10/2023