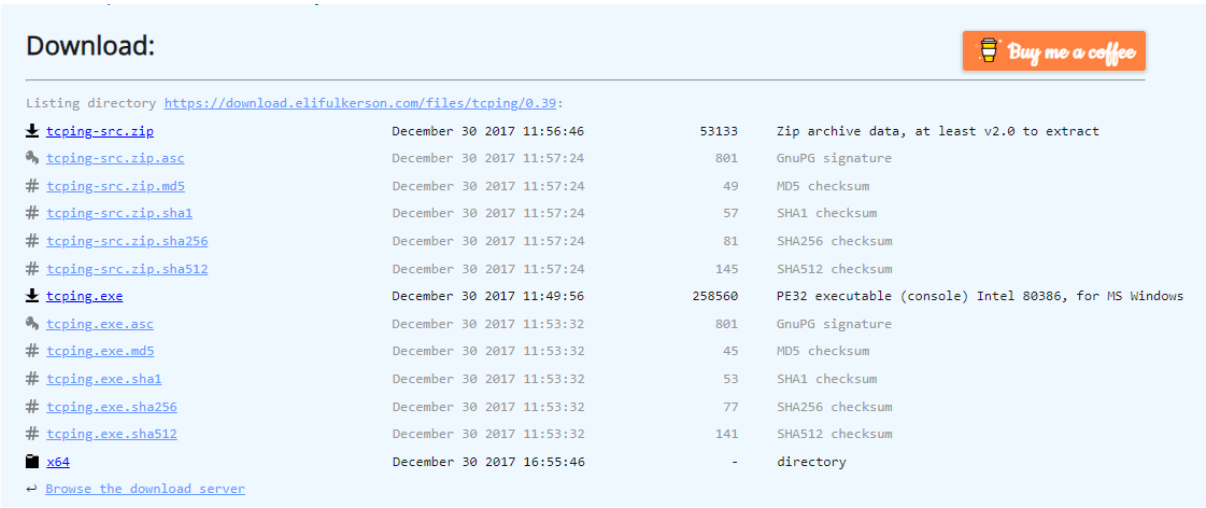
LAB18 TCPing

Name	Tran Dang Khoa
Email address	Khoab2014926@student.ctu.edu.vn
Class	M02
Browser	Safari, Chrome, IE, Firefox

	attacker	target
OS	Windows	Ubuntu
IP		
Attacking tool	**TCPing**	
Monitoring tool		Gnome Wireshark
Blocking tool		Linux iptables
Process	TCPing to target Install wireshark on target Install gnome on target Analyze packet on target using wireshark Monitor network traffic on target using gnome Block attacking IP on target using iptables Confirm blocking result using wireshark on target	

① Install TCPing on windows



Download:

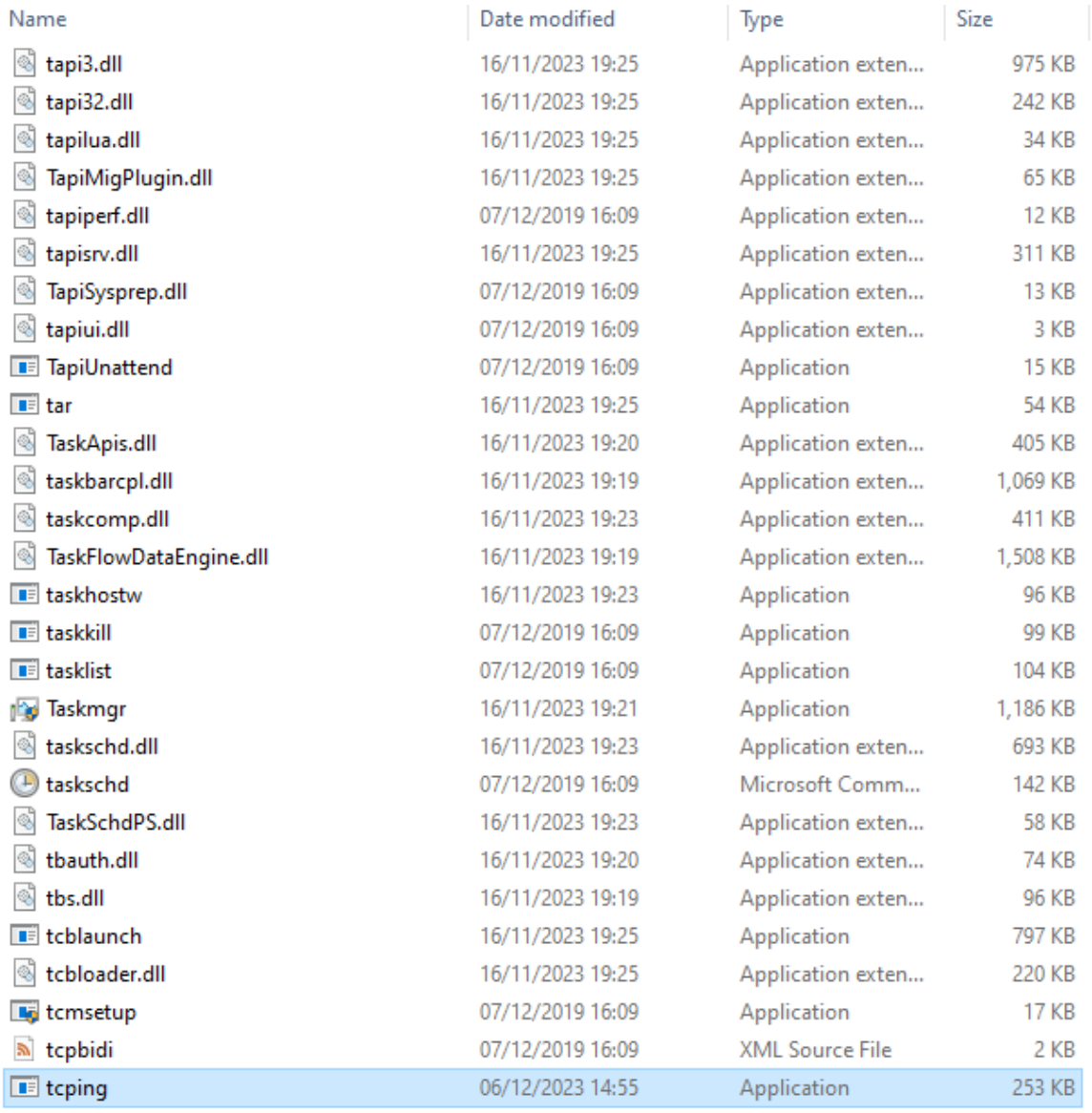
Buy me a coffee

Listing directory https://download.elifulkerson.com/files/tcping/0.39:

tcping-src.zip	December 30 2017 11:56:46	53133	Zip archive data, at least v2.0 to extract
tcping-src.zip.asc	December 30 2017 11:57:24	801	GnuPG signature
tcping-src.zip.md5	December 30 2017 11:57:24	49	MD5 checksum
tcping-src.zip.sha1	December 30 2017 11:57:24	57	SHA1 checksum
tcping-src.zip.sha256	December 30 2017 11:57:24	81	SHA256 checksum
tcping-src.zip.sha512	December 30 2017 11:57:24	145	SHA512 checksum
tcping.exe	December 30 2017 11:49:56	258560	PE32 executable (console) Intel 80386, for MS Windows
tcping.exe.asc	December 30 2017 11:53:32	801	GnuPG signature
tcping.exe.md5	December 30 2017 11:53:32	45	MD5 checksum
tcping.exe.sha1	December 30 2017 11:53:32	53	SHA1 checksum
tcping.exe.sha256	December 30 2017 11:53:32	77	SHA256 checksum
tcping.exe.sha512	December 30 2017 11:53:32	141	SHA512 checksum
x64	December 30 2017 16:55:46	-	directory

Browse the download server

② Move TCPing file to windows => system32



Name	Date modified	Type	Size
tapi3.dll	16/11/2023 19:25	Application exten...	975 KB
tapi32.dll	16/11/2023 19:25	Application exten...	242 KB
tapilua.dll	16/11/2023 19:25	Application exten...	34 KB
TapiMigPlugin.dll	16/11/2023 19:25	Application exten...	65 KB
tapiperf.dll	07/12/2019 16:09	Application exten...	12 KB
tapisrv.dll	16/11/2023 19:25	Application exten...	311 KB
TapiSysprep.dll	07/12/2019 16:09	Application exten...	13 KB
tapiui.dll	07/12/2019 16:09	Application exten...	3 KB
TapiUnattend	07/12/2019 16:09	Application	15 KB
tar	16/11/2023 19:25	Application	54 KB
TaskApis.dll	16/11/2023 19:20	Application exten...	405 KB
taskbarcpl.dll	16/11/2023 19:19	Application exten...	1,069 KB
taskcomp.dll	16/11/2023 19:23	Application exten...	411 KB
TaskFlowDataEngine.dll	16/11/2023 19:19	Application exten...	1,508 KB
taskhostw	16/11/2023 19:23	Application	96 KB
taskkill	07/12/2019 16:09	Application	99 KB
tasklist	07/12/2019 16:09	Application	104 KB
Taskmgr	16/11/2023 19:21	Application	1,186 KB
taskschd.dll	16/11/2023 19:23	Application exten...	693 KB
taskschd	07/12/2019 16:09	Microsoft Comm...	142 KB
TaskSchdPS.dll	16/11/2023 19:23	Application exten...	58 KB
tbauth.dll	16/11/2023 19:20	Application exten...	74 KB
tbs.dll	16/11/2023 19:19	Application exten...	96 KB
tcblaunch	16/11/2023 19:25	Application	797 KB
tcbloader.dll	16/11/2023 19:25	Application exten...	220 KB
tcmsetup	07/12/2019 16:09	Application	17 KB
tcpbidi	07/12/2019 16:09	XML Source File	2 KB
tcping	06/12/2023 14:55	Application	253 KB

③ CMD => TCPing to target

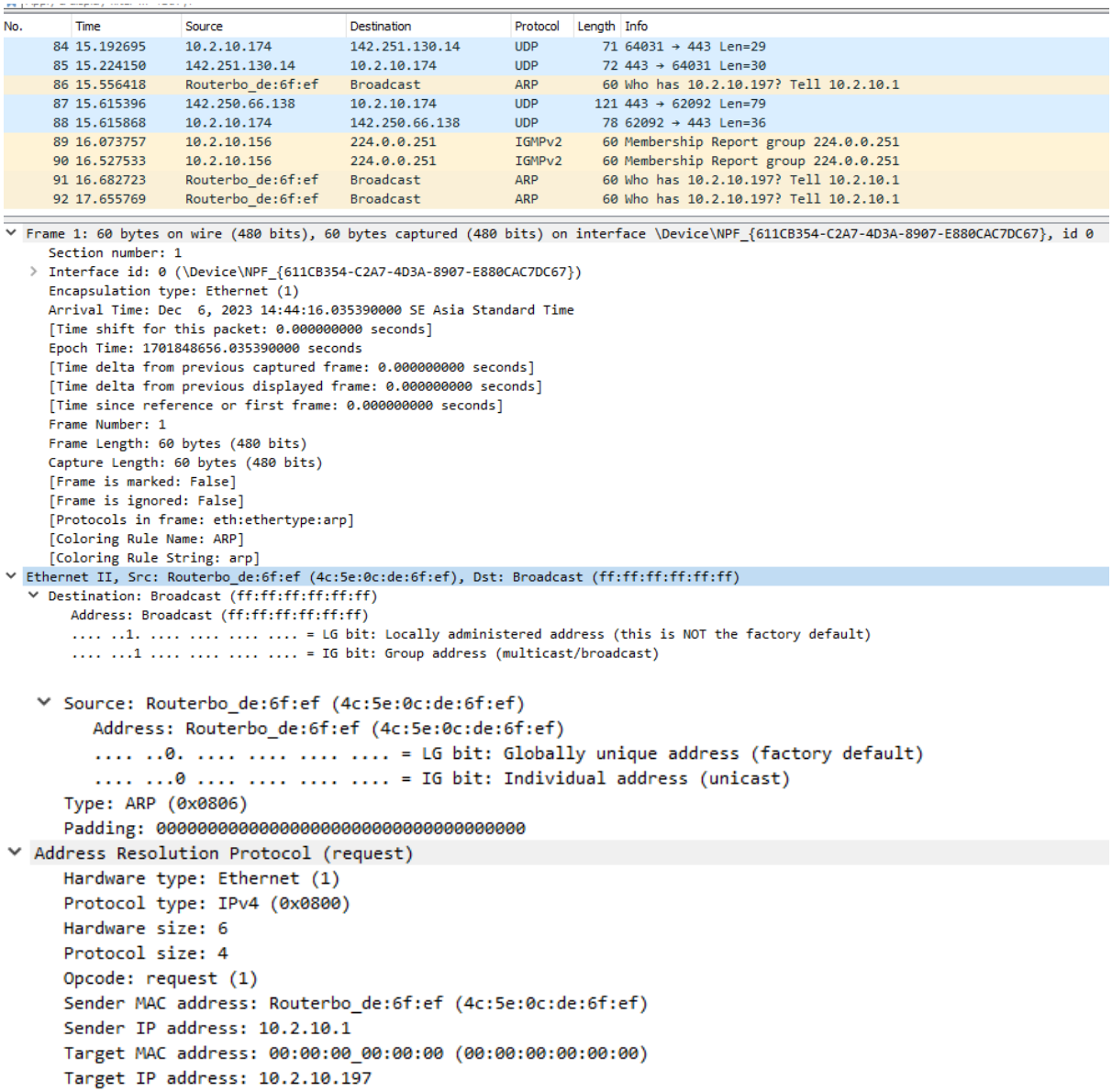
```
C:\Users\PC>tcping 10.2.10.174

Probing 10.2.10.174:80/tcp - No response - time=2003.750ms
Probing 10.2.10.174:80/tcp - No response - time=2001.220ms
Probing 10.2.10.174:80/tcp - No response - time=2001.304ms
Probing 10.2.10.174:80/tcp - No response - time=2001.277ms

Ping statistics for 10.2.10.174:80
     4 probes sent.
     0 successful, 4 failed.  (100.00% fail)
Was unable to connect, cannot provide trip statistics.

C:\Users\PC>
```

④ Install wireshark on ubuntu/ target

apt-get install wireshark

```
khoab2014926@khoab2014926-VirtualBox:~$ sudo apt-get install wireshark
[sudo] password for khoab2014926:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libbcg729-0 libc-ares2 libdouble-conversion3 liblua5.2-0 libmd4c0
  libminizip1 libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5gui5
  libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediagsttools5
  libqt5multimediawidgets5 libqt5network5 libqt5printsupport5 libqt5svg5
  libqt5widgets5 libsmi2ldbl libsnappy1v5 libspandsp2 libssh-gcrypt-4
  libwireshark-data libwireshark15 libwiretap12 libwsutil13 libxcb-xinerama0
  libxcb-xinput0 qt5-gtk-platformtheme qttranslations5-l10n wireshark-common
  wireshark-qt
Suggested packages:
  qt5-image-formats-plugins qtwayland5 snmp-mibs-downloader geoipupdate
  geoip-database geoip-database-extra libjs-leaflet
  libjs-leaflet.markercluster wireshark-doc
The following NEW packages will be installed:
  libbcg729-0 libc-ares2 libdouble-conversion3 liblua5.2-0 libmd4c0
  libminizip1 libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5gui5
  libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediagsttools5
  libqt5multimediawidgets5 libqt5network5 libqt5printsupport5 libqt5svg5
  libqt5widgets5 libsmi2ldbl libsnappy1v5 libspandsp2 libssh-gcrypt-4
```

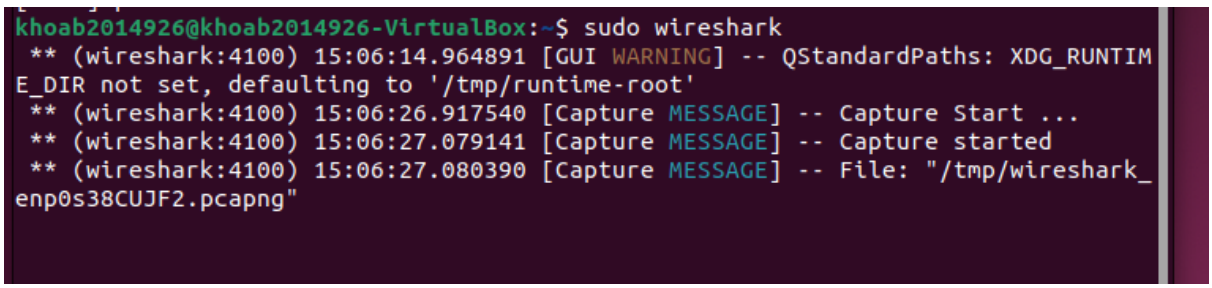
⑤ Analze packet situation on target using wireshark



No.	Time	Source	Destination	Protocol	Length	Info
84	15.192695	10.2.10.174	142.251.130.14	UDP	71	64031 → 443 Len=29
85	15.224150	142.251.130.14	10.2.10.174	UDP	72	443 → 64031 Len=30
86	15.556418	Routerbo_de:6f:ef	Broadcast	ARP	60	Who has 10.2.10.197? Tell 10.2.10.1
87	15.615396	142.250.66.138	10.2.10.174	UDP	121	443 → 62092 Len=79
88	15.615868	10.2.10.174	142.250.66.138	UDP	78	62092 → 443 Len=36
89	16.073757	10.2.10.156	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251
90	16.527533	10.2.10.156	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251
91	16.682723	Routerbo_de:6f:ef	Broadcast	ARP	60	Who has 10.2.10.197? Tell 10.2.10.1
92	17.655769	Routerbo_de:6f:ef	Broadcast	ARP	60	Who has 10.2.10.197? Tell 10.2.10.1

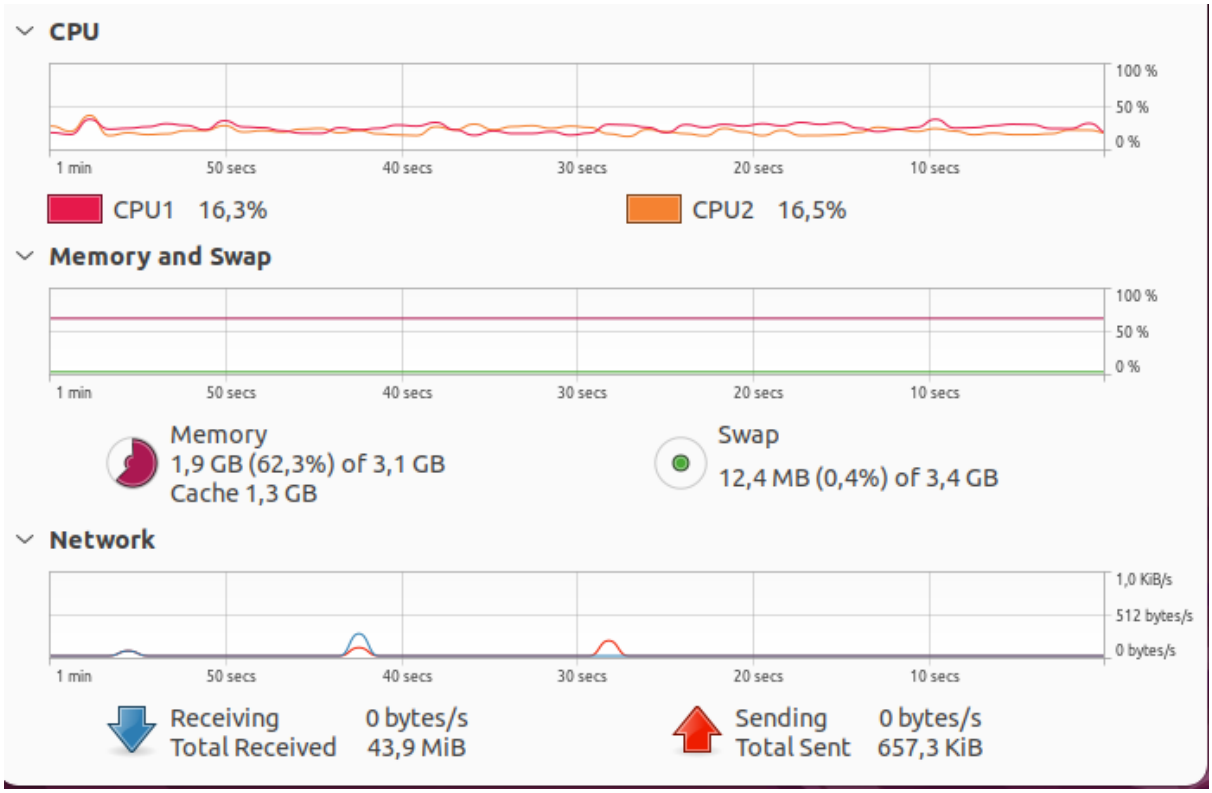
```
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{611CB354-C2A7-4D3A-8907-E880CAC7DC67}, id 0
    Section number: 1
    Interface id: 0 (\Device\NPF_{611CB354-C2A7-4D3A-8907-E880CAC7DC67})
    Encapsulation type: Ethernet (1)
    Arrival Time: Dec  6, 2023 14:44:16.035390000 SE Asia Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1701848656.035390000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 60 bytes (480 bits)
    Capture Length: 60 bytes (480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
Ethernet II, Src: Routerbo_de:6f:ef (4c:5e:0c:de:6f:ef), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
        Address: Broadcast (ff:ff:ff:ff:ff:ff)
        .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
        .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)

    Source: Routerbo_de:6f:ef (4c:5e:0c:de:6f:ef)
        Address: Routerbo_de:6f:ef (4c:5e:0c:de:6f:ef)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Routerbo_de:6f:ef (4c:5e:0c:de:6f:ef)
    Sender IP address: 10.2.10.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.2.10.197
```

⑥ Install gnome on target



```
khoab2014926@khoab2014926-VirtualBox:~$ sudo wireshark
 ** (wireshark:4100) 15:06:14.964891 [GUI WARNING] -- QStandardPaths: XDG_RUNTIM
E_DIR not set, defaulting to '/tmp/runtime-root'
 ** (wireshark:4100) 15:06:26.917540 [Capture MESSAGE] -- Capture Start ...
 ** (wireshark:4100) 15:06:27.079141 [Capture MESSAGE] -- Capture started
 ** (wireshark:4100) 15:06:27.080390 [Capture MESSAGE] -- File: "/tmp/wireshark_
enp0s38CUJF2.pcapng"
```

⑦ Check the traffic volume of target system using relevant tool



⑧ Protect/block the attack from target system

```
khoab2014926@khoab2014926-VirtualBox:~$ sudo iptables -I INPUT -s 10.2.10.174 -j
 DROP
[sudo] password for khoab2014926:
khoab2014926@khoab2014926-VirtualBox:~$
```

⑨ Confirm the Protect/blocking methods on laptop side using relevant tool

```
C:\Users\PC>tcping -t 10.2.10.174

** Pinging continuously.  Press control-c to stop **

Probing 10.2.10.174:80/tcp - No response - time=2002.084ms
Probing 10.2.10.174:80/tcp - No response - time=2000.807ms
Probing 10.2.10.174:80/tcp - No response - time=2001.785ms
Control-C
Probing 10.2.10.174:80/tcp - No response - time=796.277ms

Ping statistics for 10.2.10.174:80
     4 probes sent.
     0 successful, 4 failed.  (100.00% fail)
Was unable to connect, cannot provide trip statistics.
```