Aryaman Mishra
19BCE1027

SCAPY

TASK 1: Identifying the http site and provide URL

http://www.testingmcafeesites.com/

The following steps describe how to install (or update) Scapy itself. Dependent on your platform, some additional libraries might have to be installed to make it actually work.

```
aryaman@aryaman-VirtualBox:~$ sudo apt-get update
[sudo] password for aryaman:
Hit:1 http://in.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://in.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu focal-backports InRelease [101 kB]
Get:4 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [1,258 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu focal-updates/main i386 Packages [545 kB]
Get:7 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [909 kB]
Get:8 http://in.archive.ubuntu.com/ubuntu focal-updates/main Translation-en [265 kB]
Get:9 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 DEP-11 Metadata [283 kB]
Get:10 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 c-n-f Metadata [14.4 kB]
Get:11 http://in.archive.ubuntu.com/ubuntu focal-updates/restricted amd64 Packages [486 kB]
Get:12 http://in.archive.ubuntu.com/ubuntu focal-updates/restricted Translation-en [69.6 kB]
Get:13 http://in.archive.ubuntu.com/ubuntu focal-updates/universe amd64 Packages [864 kB]
Get:14 http://in.archive.ubuntu.com/ubuntu focal-updates/universe i386 Packages [640 kB]
Get:15 http://in.archive.ubuntu.com/ubuntu focal-updates/universe Translation-en [184 kB]
Get:16 http://in.archive.ubuntu.com/ubuntu focal-updates/universe amd64 DEP-11 Metadata [361 kB]
Get:17 http://in.archive.ubuntu.com/ubuntu focal-updates/universe amd64 c-n-f Metadata [19.1 kB]
Get:18 http://in.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 DEP-11 Metadata [944 B]
Get:19 http://in.archive.ubuntu.com/ubuntu focal-backports/universe amd64 DEP-11 Metadata [10.4 kB]
Hit:20 https://linux.teamviewer.com/deb stable InRelease
Get:21 http://security.ubuntu.com/ubuntu focal-security/main i386 Packages [291 kB]
Get:22 http://security.ubuntu.com/ubuntu focal-security/main Translation-en [173 kB]
Get:23 http://security.ubuntu.com/ubuntu focal-security/main amd64 DEP-11 Metadata [29.0 kB]
Get:24 http://security.ubuntu.com/ubuntu focal-security/restricted amd64 Packages [447 kB]
Get:25 http://security.ubuntu.com/ubuntu focal-security/restricted Translation-en [64.1 kB]
Get:26 http://security.ubuntu.com/ubuntu focal-security/universe amd64 Packages [641 kB]
Get:27 http://security.ubuntu.com/ubuntu focal-security/universe i386 Packages [510 kB]
Get:28 http://security.ubuntu.com/ubuntu focal-security/universe Translation-en [102 kB]
Get:29 http://security.ubuntu.com/ubuntu focal-security/universe amd64 DEP-11 Metadata [62.6 kB]
Get:30 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 DEP-11 Metadata [2,464 B]
Fetched 8,559 kB in 18s (477 kB/s)
Reading package lists... Done
```

Make sure you have Python installed before you go on.

```
aryaman@aryaman-VirtualBox:~$ sudo apt-get install python3
Reading package lists... Done
Building dependency tree
Reading state information... Done
python3 is already the newest version (3.8.2-0ubuntu2).
python3 set to manually installed.
The following packages were automatically installed and are no longer required:
  libdouble-conversion3 libllvm11 libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5gui5 libqt5network5 libqt5positioning5 libqt5printsupport5 libqt5qml5 libqt5quick5 libqt5sensors5 libqt5svg5
  libqt5webchannel5 libqt5webkit5 libqt5widgets5 libqt5x11extras5 libxcb-xinput0 linux-headers-5.8.0-43-generic linux-hwe-5.8-headers-5.8.0-43 linux-image-5.8.0-43-generic
  linux-modules-5.8.0-43-generic linux-modules-extra-5.8.0-43-generic qml-module-qtgraphicaleffects qml-module-qtquick-controls qml-module-qtquick-dialogs qml-module-qtquick-layouts
  qml-module-qtquick-privatewidgets qml-module-qtquick-window2 qml-module-qtquick2 qt5-gtk-platformtheme qttranslations5-l10n
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 14 not upgraded.
aryaman@aryaman-VirtualBox:~$ sudo apt-get install python3-pip
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libdouble-conversion3 libllvm11 libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5gui5 libqt5network5 libqt5positioning5 libqt5printsupport5 libqt5qml5 libqt5quick5 libqt5sensors5 libqt5svg5
  libqt5webchannel5 libqt5webkit5 libqt5widgets5 libqt5x11extras5 libxcb-xinput0 linux-headers-5.8.0-43-generic linux-hwe-5.8-headers-5.8.0-43 linux-image-5.8.0-43-generic
  linux-modules-5.8.0-43-generic linux-modules-extra-5.8.0-43-generic qml-module-qtgraphicaleffects qml-module-qtquick-controls qml-module-qtquick-dialogs qml-module-qtquick-layouts
  qml-module-qtquick-privatewidgets qml-module-qtquick-window2 qml-module-qtquick2 qt5-gtk-platformtheme qttranslations5-l10n
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libexpat1-dev libpython3-dev libpython3.8 libpython3.8-dev libpython3.8-minimal libpython3.8-stdlib python-pip-whl python3-dev python3-distutils python3-lib2to3 python3-setuptools python3-wheel
  python3.8 python3.8-dev python3.8-minimal zlib1g-dev
Suggested packages:
  python-setuptools-doc python3.8-venv python3.8-doc binfmt-support
The following NEW packages will be installed:
  libexpat1-dev libpython3-dev libpython3.8-dev python-pip-whl python3-dev python3-distutils python3-lib2to3 python3-pip python3-setuptools python3-wheel python3.8-dev zlib1g-dev
The following packages will be upgraded:
  libpython3.8 libpython3.8-minimal libpython3.8-stdlib python3.8 python3.8-minimal
5 upgraded, 12 newly installed, 0 to remove and 9 not upgraded.
Need to get 13.6 MB of archives.
After this operation, 29.1 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 libpython3.8 amd64 3.8.10-0ubuntu1~20.04.1 [1,625 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 python3.8 amd64 3.8.10-0ubuntu1~20.04.1 [387 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 libpython3.8-stdlib amd64 3.8.10-0ubuntu1~20.04.1 [1,674 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 python3.8-minimal amd64 3.8.10-0ubuntu1~20.04.1 [1,900 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 libpython3.8-minimal amd64 3.8.10-0ubuntu1~20.04.1 [717 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu focal/main amd64 libexpat1-dev amd64 2.2.9-1build1 [116 kB]
Get:7 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 libpython3.8-dev amd64 3.8.10-0ubuntu1~20.04.1 [3,948 kB]
Get:8 http://in.archive.ubuntu.com/ubuntu focal/main amd64 libpython3-dev amd64 3.8.2-0ubuntu2 [7,236 B]
Get:9 http://in.archive.ubuntu.com/ubuntu focal-updates/universe amd64 python-pip-whl all 20.0.2-5ubuntu1.6 [1,805 kB]
Get:10 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 zlib1g-dev amd64 1:1.2.11.dfsg-2ubuntu1.2 [155 kB]
Get:11 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 python3.8-dev amd64 3.8.10-0ubuntu1~20.04.1 [510 kB]
Get:12 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 python3-lib2to3 all 3.8.10-0ubuntu1~20.04 [76.3 kB]
Get:13 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 python3-distutils all 3.8.10-0ubuntu1~20.04 [141 kB]
Get:14 http://in.archive.ubuntu.com/ubuntu focal/main amd64 python3-dev amd64 3.8.2-0ubuntu2 [1,212 B]
Get:15 http://in.archive.ubuntu.com/ubuntu focal/main amd64 python3-setuptools all 45.2.0-1 [330 kB]
Get:16 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 python3-wheel all 0.34.2-1 [23.8 kB]
Get:17 http://in.archive.ubuntu.com/ubuntu focal-updates/universe amd64 python3-pip all 20.0.2-5ubuntu1.6 [231 kB]
Fetched 13.6 MB in 6s (2,210 kB/s)
(Reading database ... 216561 files and directories currently installed.)
Preparing to unpack .../00-libpython3.8_3.8.10-0ubuntu1~20.04.1_amd64.deb ...
Unpacking libpython3.8:amd64 (3.8.10-0ubuntu1~20.04.1) over (3.8.10-0ubuntu1~20.04) ...
Preparing to unpack .../01-python3.8_3.8.10-0ubuntu1~20.04.1_amd64.deb ...
Unpacking python3.8 (3.8.10-0ubuntu1~20.04.1) over (3.8.10-0ubuntu1~20.04) ...
Preparing to unpack .../02-libpython3.8-stdlib_3.8.10-0ubuntu1~20.04.1_amd64.deb ...
Unpacking libpython3.8-stdlib:amd64 (3.8.10-0ubuntu1~20.04.1) over (3.8.10-0ubuntu1~20.04) ...
```

```
Preparing to unpack .../09-zlib1g-dev_1%3a1.2.11.dfsg-2ubuntu1.2_amd64.deb ...
Unpacking zlib1g-dev:amd64 (1:1.2.11.dfsg-2ubuntu1.2) ...
Selecting previously unselected package python3.8-dev.
Preparing to unpack .../10-python3.8-dev_3.8.10-0ubuntu1~20.04.1_amd64.deb ...
Unpacking python3.8-dev (3.8.10-0ubuntu1~20.04.1) ...
Selecting previously unselected package python3-lib2to3.
Preparing to unpack .../11-python3-lib2to3_3.8.10-0ubuntu1~20.04_all.deb ...
Unpacking python3-lib2to3 (3.8.10-0ubuntu1~20.04) ...
Selecting previously unselected package python3-distutils.
Preparing to unpack .../12-python3-distutils_3.8.10-0ubuntu1~20.04_all.deb ...
Unpacking python3-distutils (3.8.10-0ubuntu1~20.04) ...
Selecting previously unselected package python3-dev.
Preparing to unpack .../13-python3-dev_3.8.2-0ubuntu2_amd64.deb ...
Unpacking python3-dev (3.8.2-0ubuntu2) ...
Selecting previously unselected package python3-setuptools.
Preparing to unpack .../14-python3-setuptools_45.2.0-1_all.deb ...
Unpacking python3-setuptools (45.2.0-1) ...
Selecting previously unselected package python3-wheel.
Preparing to unpack .../15-python3-wheel_0.34.2-1_all.deb ...
Unpacking python3-wheel (0.34.2-1) ...
Selecting previously unselected package python3-pip.
Preparing to unpack .../16-python3-pip_20.0.2-5ubuntu1.6_all.deb ...
Unpacking python3-pip (20.0.2-5ubuntu1.6) ...
Setting up libpython3.8-minimal:amd64 (3.8.10-0ubuntu1~20.04.1) ...
Setting up python3-wheel (0.34.2-1) ...
Setting up libexpat1-dev:amd64 (2.2.9-1build1) ...
Setting up zlib1g-dev:amd64 (1:1.2.11.dfsg-2ubuntu1.2) ...
Setting up python3.8-minimal (3.8.10-0ubuntu1~20.04.1) ...
Setting up python-pip-whl (20.0.2-5ubuntu1.6) ...
Setting up libpython3.8-stdlib:amd64 (3.8.10-0ubuntu1~20.04.1) ...
Setting up python3.8 (3.8.10-0ubuntu1~20.04.1) ...
Setting up python3-lib2to3 (3.8.10-0ubuntu1~20.04) ...
Setting up python3-distutils (3.8.10-0ubuntu1~20.04) ...
Setting up python3-setuptools (45.2.0-1) ...
Setting up libpython3.8:amd64 (3.8.10-0ubuntu1~20.04.1) ...
Setting up python3-pip (20.0.2-5ubuntu1.6) ...
Setting up libpython3.8-dev:amd64 (3.8.10-0ubuntu1~20.04.1) ...
Setting up python3.8-dev (3.8.10-0ubuntu1~20.04.1) ...
Setting up libpython3-dev:amd64 (3.8.2-0ubuntu2) ...
Setting up python3-dev (3.8.2-0ubuntu2) ...
Processing triggers for mime-support (3.64ubuntu1) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for desktop-file-utils (0.24-1ubuntu3) ...
```

In fact, since 2.4.3, Scapy comes in 3 bundles:

Bundle	Contains	Pip command
Default	Only Scapy	`pip install scapy`
Basic	Scapy & IPython. **Highly recommended**	`pip install --pre scapy[basic]`
Complete	Scapy & all its main dependencies	`pip install --pre scapy[complete]`

```
Requirement already satisfied: setuptools>=18.5 in /usr/lib/python3/dist-packages (from ipython->scapy[complete]) (45.2.0)
Collecting pickleshare
  Downloading pickleshare-0.7.5-py2.py3-none-any.whl (6.9 kB)
Collecting matplotlib-inline
  Downloading matplotlib_inline-0.1.3-py3-none-any.whl (8.2 kB)
Collecting numpy>=1.17
  Downloading numpy-1.21.2-cp38-cp38-manylinux_2_12_x86_64.manylinux2010_x86_64.whl (15.8 MB)
     |████████████████████████████████| 15.8 MB 140 kB/s
Collecting packaging>=20.0
  Downloading packaging-21.0-py3-none-any.whl (40 kB)
     |████████████████████████████████| 40 kB 1.4 MB/s
Requirement already satisfied: pillow>=6.2.0 in /usr/lib/python3/dist-packages (from matplotlib->scapy[complete]) (7.0.0)
Collecting kiwisolver>=1.0.1
  Downloading kiwisolver-1.3.2-cp38-cp38-manylinux_2_5_x86_64.manylinux1_x86_64.whl (1.2 MB)
     |████████████████████████████████| 1.2 MB 2.3 MB/s
Collecting setuptools-scm>=4
  Downloading setuptools_scm-6.3.2-py3-none-any.whl (33 kB)
Collecting cycler>=0.10
  Downloading cycler-0.10.0-py2.py3-none-any.whl (6.5 kB)
Collecting pyparsing>=2.2.1
  Downloading pyparsing-3.0.0rc2-py3-none-any.whl (94 kB)
     |████████████████████████████████| 94 kB 1.2 MB/s
Collecting fonttools>=4.22.0
  Downloading fonttools-4.27.1-py3-none-any.whl (869 kB)
     |████████████████████████████████| 869 kB 2.1 MB/s
Requirement already satisfied: python-dateutil>=2.7 in /usr/lib/python3/dist-packages (from matplotlib->scapy[complete]) (2.7.3)
Collecting wcwidth
  Downloading wcwidth-0.2.5-py2.py3-none-any.whl (30 kB)
Collecting parso<0.9.0,>=0.8.0
  Downloading parso-0.8.2-py2.py3-none-any.whl (94 kB)
     |████████████████████████████████| 94 kB 1.3 MB/s
Collecting tomli>=1.0.0
  Downloading tomli-1.2.1-py3-none-any.whl (11 kB)
Requirement already satisfied: six in /usr/lib/python3/dist-packages (from cycler>=0.10->matplotlib->scapy[complete]) (1.14.0)
Building wheels for collected packages: scapy, pyx
  Building wheel for scapy (setup.py) ... done
  Created wheel for scapy: filename=scapy-2.4.5-py2.py3-none-any.whl size=1261545 sha256=e9d17f271357b3189ca37e3285552c534baf8536e09692e6f380c2444393b7fb
  Stored in directory: /root/.cache/pip/wheels/51/c7/3d/6c23d4a039ee412a093156be4dbc0725946a2ec64f9b9ab61e
  Building wheel for pyx (setup.py) ... done
  Created wheel for pyx: filename=PyX-0.15-py3-none-any.whl size=434888 sha256=78d8a7fa937194c431fb98076bb02f6a45da5307809f748749dcfefd3bab2dd4
  Stored in directory: /root/.cache/pip/wheels/45/0d/de/0540cebc50a09d82cca3caa03ea55030c752e8de50446783f2
Successfully built scapy pyx
Installing collected packages: pygments, wcwidth, prompt-toolkit, traitlets, decorator, backcall, parso, jedi, pickleshare, matplotlib-inline, ipython, numpy, pyparsing, packaging, kiwisolver, tomli, set
uptools-scm, cycler, fonttools, matplotlib, pyx, scapy
Successfully installed backcall-0.2.0 cycler-0.10.0 decorator-5.1.0 fonttools-4.27.1 ipython-7.28.0 jedi-0.18.0 kiwisolver-1.3.2 matplotlib-3.5.0rc1 matplotlib-inline-0.1.3 numpy-1.21.2 packaging-21.0 pa
rso-0.8.2 pickleshare-0.7.5 prompt-toolkit-3.0.20 pygments-2.10.0 pyparsing-3.0.0rc2 pyx-0.15 scapy-2.4.5 setuptools-scm-6.3.2 tomli-1.2.1 traitlets-5.1.0 wcwidth-0.2.5
```

```
aryaman@aryaman-VirtualBox:~$ sudo python3 -m pip install --pre scapy[complete]
Collecting scapy[complete]
  Downloading scapy-2.4.5.tar.gz (1.1 MB)
     |████████████████████████████████| 1.1 MB 679 kB/s
Requirement already satisfied: cryptography>=2.0 in /usr/lib/python3/dist-packages (from scapy[complete]) (2.8)
Collecting ipython
  Downloading ipython-7.28.0-py3-none-any.whl (788 kB)
     |████████████████████████████████| 788 kB 1.4 MB/s
Collecting matplotlib
  Downloading matplotlib-3.5.0rc1-cp38-cp38-manylinux_2_5_x86_64.manylinux1_x86_64.whl (10.3 MB)
     |████████████████████████████████| 10.3 MB 141 kB/s
Collecting pyx
  Downloading PyX-0.15.tar.gz (2.6 MB)
     |████████████████████████████████| 2.6 MB 159 kB/s
Collecting pygments
  Downloading Pygments-2.10.0-py3-none-any.whl (1.0 MB)
     |████████████████████████████████| 1.0 MB 1.7 MB/s
Requirement already satisfied: pexpect>4.3; sys_platform != "win32" in /usr/lib/python3/dist-packages (from ipython->scapy[complete]) (4.6.0)
Collecting prompt-toolkit!=3.0.0,!=3.0.1,<3.1.0,>=2.0.0
  Downloading prompt_toolkit-3.0.20-py3-none-any.whl (370 kB)
     |████████████████████████████████| 370 kB 2.1 MB/s
Collecting traitlets>=4.2
  Downloading traitlets-5.1.0-py3-none-any.whl (101 kB)
     |████████████████████████████████| 101 kB 2.0 MB/s
Collecting decorator
  Downloading decorator-5.1.0-py3-none-any.whl (9.1 kB)
Collecting backcall
  Downloading backcall-0.2.0-py2.py3-none-any.whl (11 kB)
Collecting jedi>=0.16
  Downloading jedi-0.18.0-py2.py3-none-any.whl (1.4 MB)
     |████████████████████████████████| 1.4 MB 20 kB/s
Requirement already satisfied: setuptools>=18.5 in /usr/lib/python3/dist-packages (from ipython->scapy[complete]) (45.2.0)
Collecting pickleshare
  Downloading pickleshare-0.7.5-py2.py3-none-any.whl (6.9 kB)
Collecting matplotlib-inline
  Downloading matplotlib_inline-0.1.3-py3-none-any.whl (8.2 kB)
Collecting numpy>=1.17
  Downloading numpy-1.21.2-cp38-cp38-manylinux_2_12_x86_64.manylinux2010_x86_64.whl (15.8 MB)
     |████████████████████████████████| 15.8 MB 140 kB/s
Collecting packaging>=20.0
  Downloading packaging-21.0-py3-none-any.whl (40 kB)
     |████████████████████████████████| 40 kB 1.4 MB/s
Requirement already satisfied: pillow>=6.2.0 in /usr/lib/python3/dist-packages (from matplotlib->scapy[complete]) (7.0.0)
Collecting kiwisolver>=1.0.1
  Downloading kiwisolver-1.3.2-cp38-cp38-manylinux_2_5_x86_64.manylinux1_x86_64.whl (1.2 MB)
     |████████████████████████████████| 1.2 MB 2.3 MB/s
Collecting setuptools-scm>=4
```

We can also install TexLive as optional dependancies to avoid errors.

```
aryaman@aryaman-VirtualBox:~$ sudo apt install texlive
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libdouble-conversion3 libllvm11 libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5gui5 libqt5network5 libqt5positioning5 libqt5printsupport5 libqt5qml5 libqt5quick5 libqt5sensors5 libqt5svg5
  libqt5webchannel5 libqt5webkit5 libqt5widgets5 libqt5x11extras5 libxcb-xinput0 linux-headers-5.8.0-43-generic linux-hwe-5.8-headers-5.8.0-43 linux-image-5.8.0-43-generic
  linux-modules-5.8.0-43-generic linux-modules-extra-5.8.0-43-generic qml-module-qtgraphicaleffects qml-module-qtquick-controls qml-module-qtquick-dialogs qml-module-qtquick-layouts
  qml-module-qtquick-privatewidgets qml-module-qtquick-window2 qml-module-qtquick2 qt5-gtk-platformtheme qttranslations5-l10n
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  dvisvgm fonts-lmodern fonts-texgyre libptexenc1 libteckit0 libtexlua53 libtexluajit2 libzzip-0-13 lmodern tex-common tex-gyre texlive-base texlive-binaries texlive-fonts-recommended
  texlive-latex-base texlive-latex-recommended tipa
Suggested packages:
  debhelper perl-tk xzdec texlive-fonts-recommended-doc texlive-latex-base-doc texlive-latex-recommended-doc texlive-luatex texlive-pstricks
The following NEW packages will be installed:
  dvisvgm fonts-lmodern fonts-texgyre libptexenc1 libteckit0 libtexlua53 libtexluajit2 libzzip-0-13 lmodern tex-common tex-gyre texlive texlive-base texlive-binaries texlive-fonts-recommended
  texlive-latex-base texlive-latex-recommended tipa
0 upgraded, 18 newly installed, 0 to remove and 9 not upgraded.
Need to get 19.2 MB/85.7 MB of archives.
After this operation, 269 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 dvisvgm amd64 2.8.1-1build1 [1,048 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 fonts-texgyre all 20180621-3 [10.2 MB]
Get:3 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 texlive-fonts-recommended all 2019.20200218-1 [4,972 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 texlive all 2019.20200218-1 [14.4 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 tipa all 2:1.3-20 [2,978 kB]
Fetched 19.2 MB in 9s (2,218 kB/s)
Preconfiguring packages ...
Selecting previously unselected package tex-common.
(Reading database ... 217425 files and directories currently installed.)
Preparing to unpack .../00-tex-common_6.13_all.deb ...
Unpacking tex-common (6.13) ...
Selecting previously unselected package dvisvgm.
Preparing to unpack .../01-dvisvgm_2.8.1-1build1_amd64.deb ...
Unpacking dvisvgm (2.8.1-1build1) ...
Selecting previously unselected package fonts-lmodern.
Preparing to unpack .../02-fonts-lmodern_2.004.5-6_all.deb ...
Unpacking fonts-lmodern (2.004.5-6) ...
Selecting previously unselected package fonts-texgyre.
```

```
Setting up libzzip-0-13:amd64 (0.13.62-3.2ubuntu1) ...
Setting up tex-common (6.13) ...
update-language: texlive-base not installed and configured, doing nothing!
Setting up libptexenc1:amd64 (2019.20190605.51237-3build2) ...
Setting up libteckit0:amd64 (2.5.8+ds2-5ubuntu2) ...
Setting up fonts-texgyre (20180621-3) ...
Setting up texlive-binaries (2019.20190605.51237-3build2) ...
update-alternatives: using /usr/bin/xdvi-xaw to provide /usr/bin/xdvi.bin (xdvi.bin) in auto mode
update-alternatives: using /usr/bin/bibtex.original to provide /usr/bin/bibtex (bibtex) in auto mode
Setting up fonts-lmodern (2.004.5-6) ...
Setting up texlive-base (2019.20200218-1) ...
mktexlsr: Updating /var/lib/texmf/ls-R-TEXLIVEDIST...
mktexlsr: Updating /var/lib/texmf/ls-R-TEXMFMAIN...
mktexlsr: Updating /var/lib/texmf/ls-R...
mktexlsr: Done.
tl-paper: setting paper size for dvips to a4: /var/lib/texmf/dvips/config/config-paper.ps
tl-paper: setting paper size for dvipdfmx to a4: /var/lib/texmf/dvipdfmx/dvipdfmx-paper.cfg
tl-paper: setting paper size for xdvi to a4: /var/lib/texmf/xdvi/XDvi-paper
tl-paper: setting paper size for pdftex to a4: /var/lib/texmf/tex/generic/config/pdftexconfig.tex
Setting up tex-gyre (20180621-3) ...
Setting up texlive-latex-base (2019.20200218-1) ...
Setting up texlive-latex-recommended (2019.20200218-1) ...
Setting up lmodern (2.004.5-6) ...
Setting up texlive-fonts-recommended (2019.20200218-1) ...
Setting up tipa (2:1.3-20) ...
Regenerating '/var/lib/texmf/fmtutil.cnf-DEBIAN'... done.
Regenerating '/var/lib/texmf/fmtutil.cnf-TEXLIVEDIST'... done.
update-fmtutil has updated the following file(s):
        /var/lib/texmf/fmtutil.cnf-DEBIAN
        /var/lib/texmf/fmtutil.cnf-TEXLIVEDIST
If you want to activate the changes in the above file(s),
you should run fmtutil-sys or fmtutil.
Setting up texlive (2019.20200218-1) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for install-info (6.7.0.dfsg.2-5) ...
Processing triggers for fontconfig (2.13.1-2ubuntu3) ...
Processing triggers for desktop-file-utils (0.24-1ubuntu3) ...
Processing triggers for mime-support (3.64ubuntu1) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
Processing triggers for tex-common (6.13) ...
Running updmap-sys. This may take some time... done.
Running mktexlsr /var/lib/texmf ... done.
Building format(s) --all.
        This may take some time... done.
```

Starting Scapy

Scapy's interactive shell is run in a terminal session. Root privileges are needed to send the packets, so we're using `sudo` here:

INSTALLING SCAPY (METHOD 1)

```
└─$ sudo apt install python3-scapy
[sudo] password for eshandas:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
python3-scapy is already the newest version (2.4.4-4).
python3-scapy set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 867 not upgraded.

┌──(eshandas㉿kali)-[~]
└─$ scapy -h
Usage: scapy.py [-s sessionfile] [-c new_startup_file] [-p new_prestart_file] [-C] [-P] [-H]
Args:
        -H: header-less start
        -C: do not read startup file
        -P: do not read pre-startup file
```

INSTALLING SCAPY (METHOD 2)

```
└─# git clone https://github.com/secdev/scapy
Cloning into 'scapy' ...
remote: Enumerating objects: 35040, done.
remote: Counting objects: 100% (1520/1520), done.
remote: Compressing objects: 100% (718/718), done.
remote: Total 35040 (delta 979), reused 1183 (delta 797), pack-reused 33520
Receiving objects: 100% (35040/35040), 83.60 MiB | 9.78 MiB/s, done.
Resolving deltas: 100% (23318/23318), done.
```

RUN THE SCAPY TOOL

```
aryaman@aryaman-VirtualBox:~$ sudo scapy

                      aSPY//YASa
             apyyyyCY//////////YCa       |
            sY//////YSpcs  scpCY//Pp     | Welcome to Scapy
 ayp ayyyyyyySCP//Pp           syY//C    | Version 2.4.5
 AYAsAYYYYYYYY///Ps              cY//S   |
         pCCCCY//p          cSSps y//Y   | https://github.com/secdev/scapy
         SPPPP///a          pP///AC//Y   |
              A//A            cyP////C   | Have fun!
              p///Ac            sC///a   |
              P////YCpc           A//A   | Craft me if you can.
       scccccp///pSP///p          p//Y   |                    -- IPv6 layer
      sY/////////y  caa           S//P   |
       cayCyayP//Ya               pY/Ya
        sY/PsY////YCc           aC//Yp
         sc  sccaCY//PCypaapyCP//YSs
                  spCPY//////YPSps
                       ccaacs
                                          using IPython 7.28.0
>>>
```

We will start with sniffing 4 packets and using summary() function to view their information.Basically it shows the layer of the packets.We can see Ethernet frame on the network access layer,it's an IP protocol on the Internet layer,at the transport layer,it's UDP and we can view the Domain name(or DNS Query) on the Application layer.

```
>>> sniff(count=4)
<Sniffed: TCP:0 UDP:3 ICMP:0 Other:1>
>>> a= _
>>> a.summary()
Ether / IP / UDP / NTP v??, ??
Ether / IP / UDP / NTP v??, ??
Ether / IPv6 / UDP / DNS Qry "b'_ipps._tcp.local.'"
Ether / ARP who has 10.0.2.2 says 10.0.2.15
```

Scapy has sniffed 4 UDP packets in a single line.

```
>>> sniff(count=4)
<Sniffed: TCP:0 UDP:4 ICMP:0 Other:0>
```

Scapy has sniffed 4 TCP packets in a single line.

```
>>> sniff(count=10)
<Sniffed: TCP:10 UDP:0 ICMP:0 Other:0>
```

We can view the summary of those 10 TCP packets by storing them in a variable a and using the summary() function.

```
>>> a= _
>>> a.summary()
Ether / IP / TCP 10.0.2.15:44710 > 34.107.221.82:http A
Ether / IP / TCP 34.107.221.82:http > 10.0.2.15:44710 A / Padding
Ether / IP / TCP 10.0.2.15:44712 > 34.107.221.82:http A
Ether / IP / TCP 34.107.221.82:http > 10.0.2.15:44712 A / Padding
Ether / IP / TCP 10.0.2.15:50058 > 142.250.67.195:http A
Ether / IP / TCP 142.250.67.195:http > 10.0.2.15:50058 A / Padding
Ether / IP / TCP 10.0.2.15:37218 > 13.35.191.120:https A
Ether / IP / TCP 10.0.2.15:52574 > 54.192.171.73:https A
Ether / IP / TCP 13.35.191.120:https > 10.0.2.15:37218 A / Padding
Ether / IP / TCP 54.192.171.73:https > 10.0.2.15:52574 A / Padding
```

We can view the summary of those 10 UDP packets by storing them in a variable a and using the summary() function.

```
>>> sniff(count=10)
<Sniffed: TCP:0 UDP:10 ICMP:0 Other:0>
>>> a= _
>>> a.summary()
Ether / IP / UDP 74.125.169.230:443 > 10.0.2.15:57671 / Raw
Ether / IP / UDP 10.0.2.15:57671 > 74.125.169.230:443 / Raw
Ether / IP / UDP 74.125.169.230:443 > 10.0.2.15:57671 / Raw
Ether / IP / UDP 74.125.169.230:443 > 10.0.2.15:57671 / Raw
Ether / IP / UDP 74.125.169.230:443 > 10.0.2.15:57671 / Raw
Ether / IP / UDP 74.125.169.230:443 > 10.0.2.15:57671 / Raw
Ether / IP / UDP 10.0.2.15:57671 > 74.125.169.230:443 / Raw
Ether / IP / UDP 74.125.169.230:443 > 10.0.2.15:57671 / Raw
Ether / IP / UDP 74.125.169.230:443 > 10.0.2.15:57671 / Raw
Ether / IP / UDP 74.125.169.230:443 > 10.0.2.15:57671 / Raw
```

We can view the summary of those 10 TCP packets by storing them in a variable a and using the summary() function.

```
>>> sniff(count=10)
<Sniffed: TCP:10 UDP:0 ICMP:0 Other:0>
>>> a= _
>>> a.summary()
Ether / IP / TCP 103.102.166.224:https > 10.0.2.15:37180 PA / Raw
Ether / IP / TCP 10.0.2.15:37180 > 103.102.166.224:https A
Ether / IP / TCP 10.0.2.15:55384 > 49.44.225.237:https A
Ether / IP / TCP 49.44.225.237:https > 10.0.2.15:55384 A / Padding
Ether / IP / TCP 10.0.2.15:50058 > 142.250.67.195:http A
Ether / IP / TCP 142.250.67.195:http > 10.0.2.15:50058 A / Padding
Ether / IP / TCP 10.0.2.15:51344 > 49.44.225.236:https A
Ether / IP / TCP 10.0.2.15:51346 > 49.44.225.236:https A
Ether / IP / TCP 10.0.2.15:37218 > 13.35.191.120:https A
Ether / IP / TCP 10.0.2.15:52574 > 54.192.171.73:https A
```

We can view the summary of those 4 UDP packets by storing them in a variable a and using the summary() function.

```
>>> sniff(count=4)
<Sniffed: TCP:0 UDP:4 ICMP:0 Other:0>
>>> a= _
>>> a.summary()
Ether / IP / UDP 10.0.2.15:52594 > 142.250.77.238:443 / Raw
Ether / IP / UDP 10.0.2.15:52594 > 142.250.77.238:443 / Raw
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:52594 / Raw
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:52594 / Raw
```

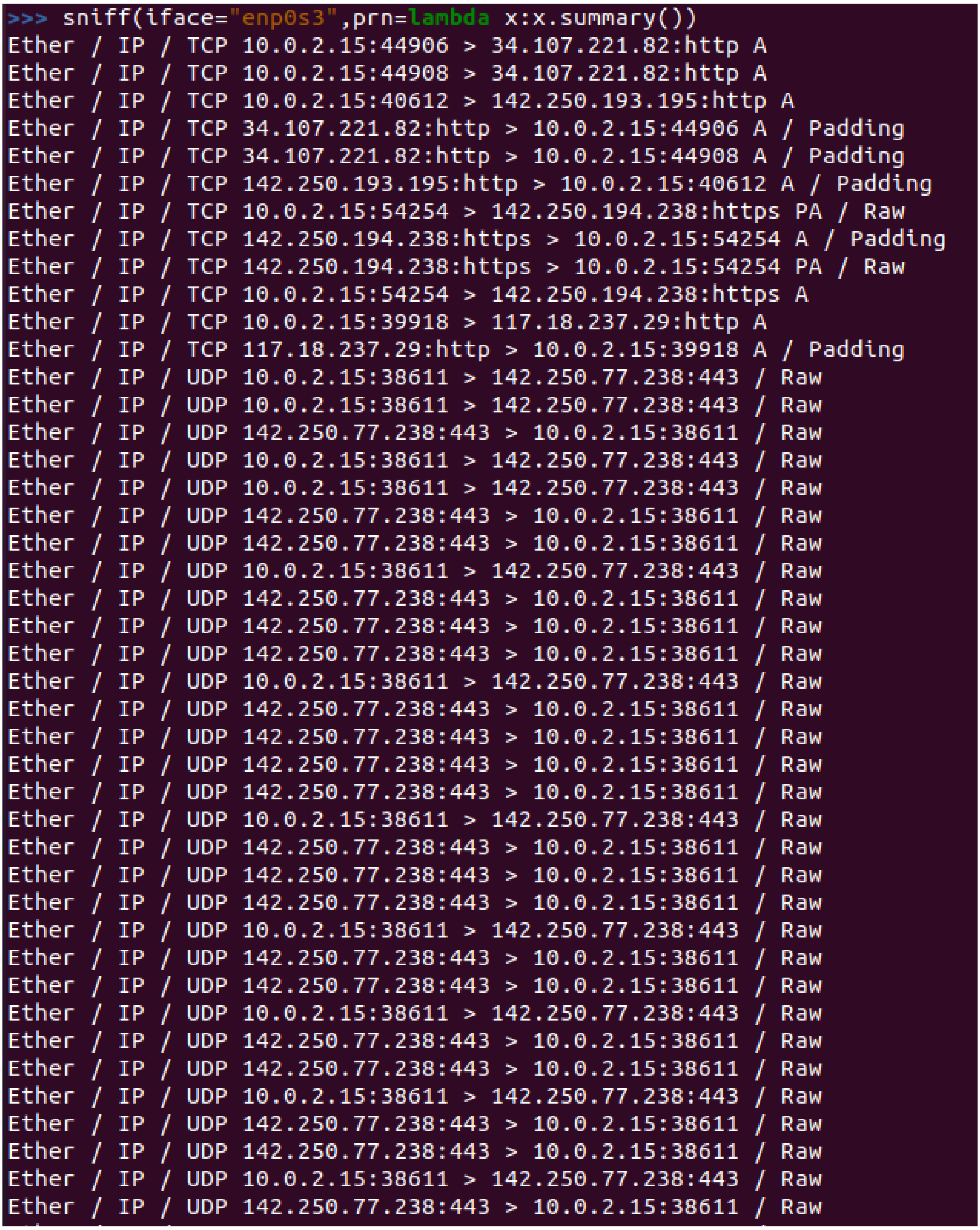
If we want the summary in a single command,we can use the lambda function to find the summary of n number of packets.

```
>>> sniff(count=4,prn=lambda x:x.summary())
Ether / IP / UDP / DNS Qry "b'detectportal.firefox.com.'"
Ether / IP / UDP / DNS Qry "b'detectportal.firefox.com.'"
Ether / IP / UDP / DNS Ans "b'detectportal.prod.mozaws.net.'"
Ether / IP / UDP / DNS Ans "b'detectportal.prod.mozaws.net.'"
<Sniffed: TCP:0 UDP:4 ICMP:0 Other:0>
```

```
>>> sniff(count=4,prn=lambda x:x.summary())
Ether / IP / UDP / DNS Qry "b'prod.ingestion-edge.prod.dataops.mozgcp.net.'"
Ether / IP / UDP / DNS Ans
Ether / IP / TCP 10.0.2.15:49144 > 35.227.207.240:https PA / Raw
Ether / IP / TCP 35.227.207.240:https > 10.0.2.15:49144 A / Padding
<Sniffed: TCP:2 UDP:2 ICMP:0 Other:0>
```

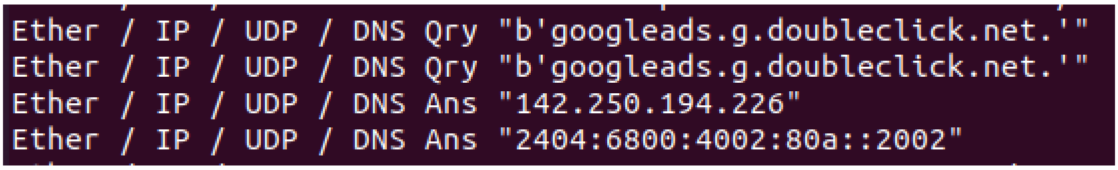
```
>>> sniff(count=4,prn=lambda x:x.summary())
Ether / IP / UDP / DNS Qry "b'youtube-ui.l.google.com.'"
Ether / IP / UDP 10.0.2.15:38611 > 142.250.77.238:443 / Raw
Ether / IP / UDP 10.0.2.15:38611 > 142.250.77.238:443 / Raw
Ether / IP / UDP 10.0.2.15:38611 > 142.250.77.238:443 / Raw
<Sniffed: TCP:0 UDP:4 ICMP:0 Other:0>
```

If we want continuous sniffing of traffic,we can replace the count with iface(interface) and we can monitor the network interface “enp0s3” used by Linux Ubuntu Machine and we can start seeing traffic and related information and we can refresh websites or access them and generate traffic and they can show us the continuously captured packets.They can show us the basics of the layered information which is very helpful.We canuse Ctrl+C to end the capturing and we can see the number of TCP,UDP,ICMP packets captured.If we want to use a more detailed view,we can use the count function to capture information on a single packet and instead of summary(),we can use the show() function to monitor that package.

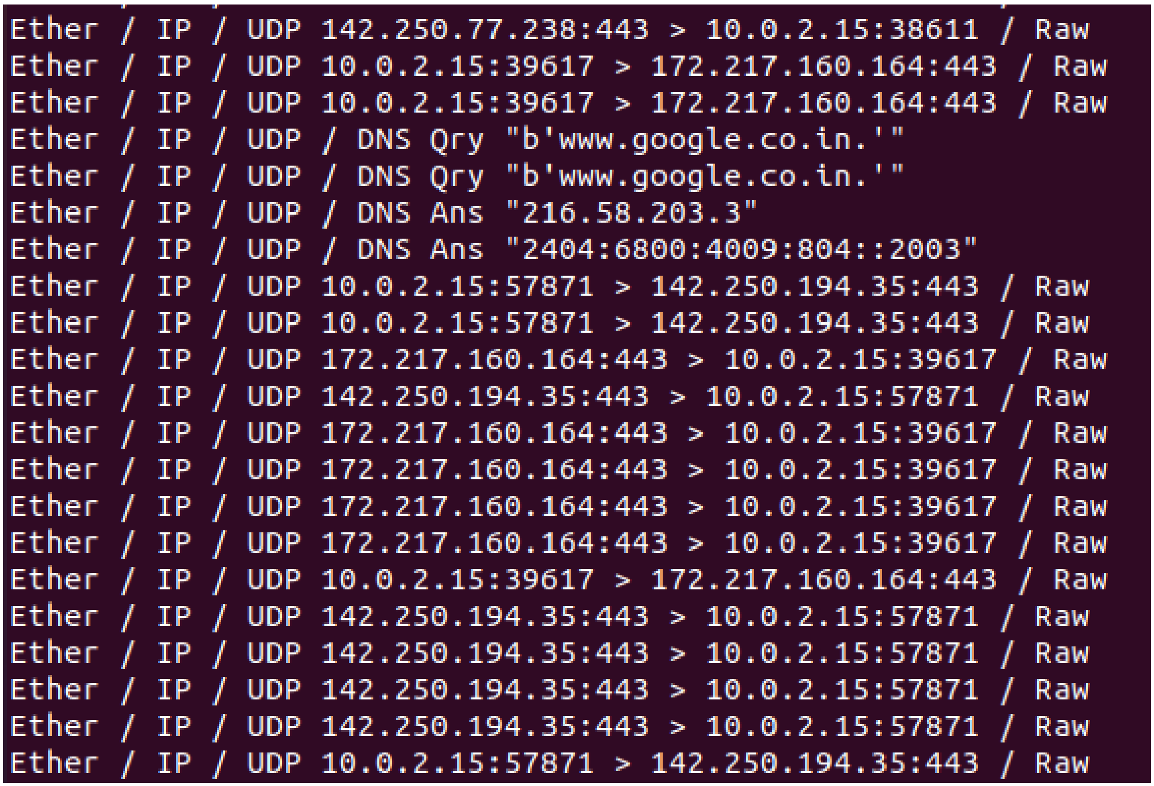


```
>>> sniff(iface="enp0s3",prn=lambda x:x.summary())
Ether / IP / TCP 10.0.2.15:44906 > 34.107.221.82:http A
Ether / IP / TCP 10.0.2.15:44908 > 34.107.221.82:http A
Ether / IP / TCP 10.0.2.15:40612 > 142.250.193.195:http A
Ether / IP / TCP 34.107.221.82:http > 10.0.2.15:44906 A / Padding
Ether / IP / TCP 34.107.221.82:http > 10.0.2.15:44908 A / Padding
Ether / IP / TCP 142.250.193.195:http > 10.0.2.15:40612 A / Padding
Ether / IP / TCP 10.0.2.15:54254 > 142.250.194.238:https PA / Raw
Ether / IP / TCP 142.250.194.238:https > 10.0.2.15:54254 A / Padding
Ether / IP / TCP 142.250.194.238:https > 10.0.2.15:54254 PA / Raw
Ether / IP / TCP 10.0.2.15:54254 > 142.250.194.238:https A
Ether / IP / TCP 10.0.2.15:39918 > 117.18.237.29:http A
Ether / IP / TCP 117.18.237.29:http > 10.0.2.15:39918 A / Padding
Ether / IP / UDP 10.0.2.15:38611 > 142.250.77.238:443 / Raw
Ether / IP / UDP 10.0.2.15:38611 > 142.250.77.238:443 / Raw
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:38611 / Raw
Ether / IP / UDP 10.0.2.15:38611 > 142.250.77.238:443 / Raw
Ether / IP / UDP 10.0.2.15:38611 > 142.250.77.238:443 / Raw
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:38611 / Raw
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:38611 / Raw
Ether / IP / UDP 10.0.2.15:38611 > 142.250.77.238:443 / Raw
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:38611 / Raw
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:38611 / Raw
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:38611 / Raw
Ether / IP / UDP 10.0.2.15:38611 > 142.250.77.238:443 / Raw
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:38611 / Raw
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:38611 / Raw
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:38611 / Raw
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:38611 / Raw
Ether / IP / UDP 10.0.2.15:38611 > 142.250.77.238:443 / Raw
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:38611 / Raw
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:38611 / Raw
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:38611 / Raw
Ether / IP / UDP 10.0.2.15:38611 > 142.250.77.238:443 / Raw
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:38611 / Raw
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:38611 / Raw
Ether / IP / UDP 10.0.2.15:38611 > 142.250.77.238:443 / Raw
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:38611 / Raw
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:38611 / Raw
Ether / IP / UDP 10.0.2.15:38611 > 142.250.77.238:443 / Raw
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:38611 / Raw
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:38611 / Raw
Ether / IP / UDP 10.0.2.15:38611 > 142.250.77.238:443 / Raw
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:38611 / Raw
```

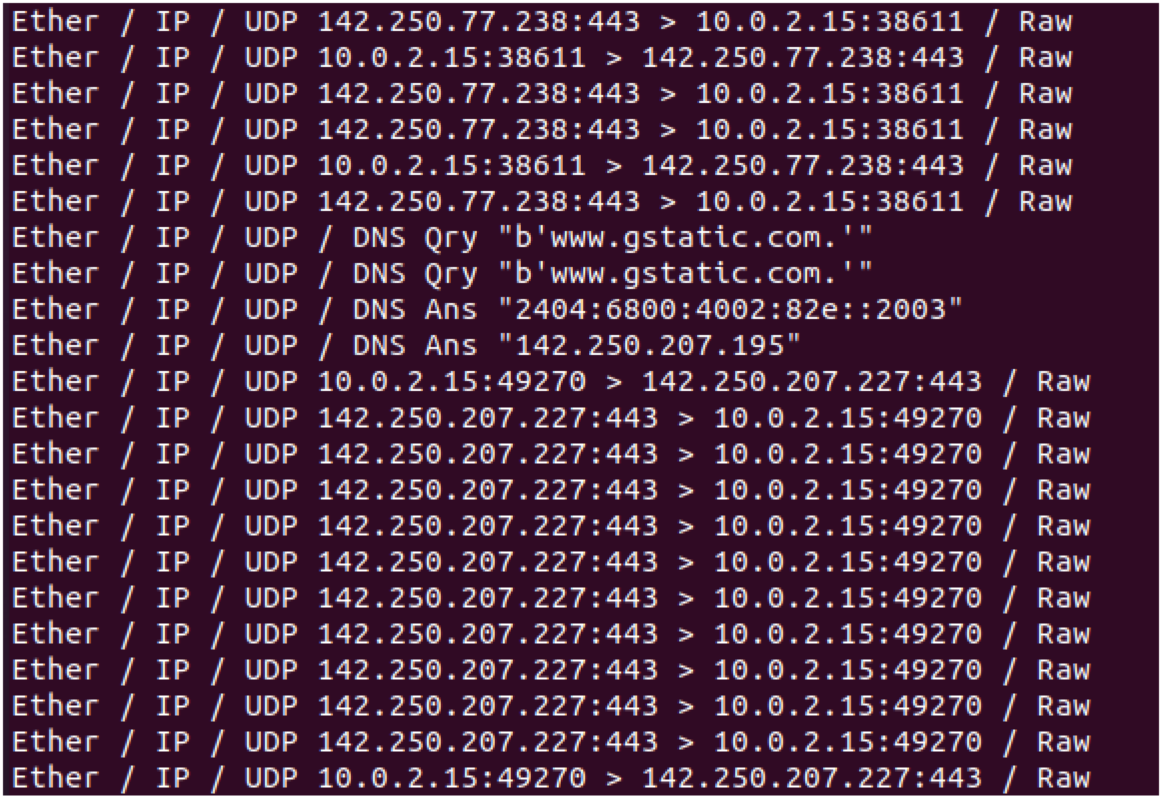
Accessing Google Search Engine:



```
Ether / IP / UDP / DNS Qry "b'googleads.g.doubleclick.net.'"
Ether / IP / UDP / DNS Qry "b'googleads.g.doubleclick.net.'"
Ether / IP / UDP / DNS Ans "142.250.194.226"
Ether / IP / UDP / DNS Ans "2404:6800:4002:80a::2002"
```

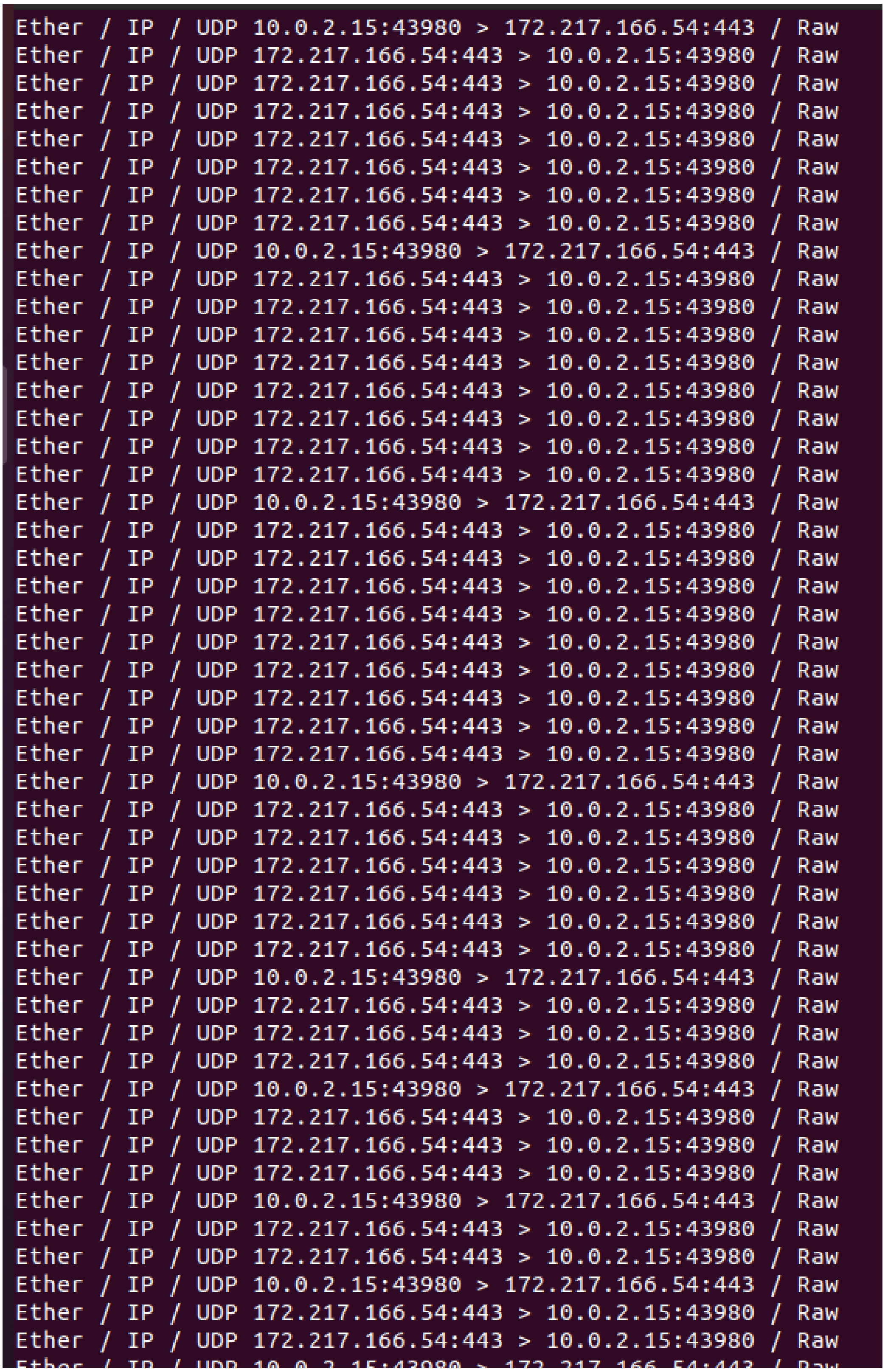


```
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:38611 / Raw
Ether / IP / UDP 10.0.2.15:39617 > 172.217.160.164:443 / Raw
Ether / IP / UDP 10.0.2.15:39617 > 172.217.160.164:443 / Raw
Ether / IP / UDP / DNS Qry "b'www.google.co.in.'"
Ether / IP / UDP / DNS Qry "b'www.google.co.in.'"
Ether / IP / UDP / DNS Ans "216.58.203.3"
Ether / IP / UDP / DNS Ans "2404:6800:4009:804::2003"
Ether / IP / UDP 10.0.2.15:57871 > 142.250.194.35:443 / Raw
Ether / IP / UDP 10.0.2.15:57871 > 142.250.194.35:443 / Raw
Ether / IP / UDP 172.217.160.164:443 > 10.0.2.15:39617 / Raw
Ether / IP / UDP 142.250.194.35:443 > 10.0.2.15:57871 / Raw
Ether / IP / UDP 172.217.160.164:443 > 10.0.2.15:39617 / Raw
Ether / IP / UDP 172.217.160.164:443 > 10.0.2.15:39617 / Raw
Ether / IP / UDP 172.217.160.164:443 > 10.0.2.15:39617 / Raw
Ether / IP / UDP 172.217.160.164:443 > 10.0.2.15:39617 / Raw
Ether / IP / UDP 10.0.2.15:39617 > 172.217.160.164:443 / Raw
Ether / IP / UDP 142.250.194.35:443 > 10.0.2.15:57871 / Raw
Ether / IP / UDP 142.250.194.35:443 > 10.0.2.15:57871 / Raw
Ether / IP / UDP 142.250.194.35:443 > 10.0.2.15:57871 / Raw
Ether / IP / UDP 142.250.194.35:443 > 10.0.2.15:57871 / Raw
Ether / IP / UDP 10.0.2.15:57871 > 142.250.194.35:443 / Raw
```



```
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:38611 / Raw
Ether / IP / UDP 10.0.2.15:38611 > 142.250.77.238:443 / Raw
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:38611 / Raw
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:38611 / Raw
Ether / IP / UDP 10.0.2.15:38611 > 142.250.77.238:443 / Raw
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:38611 / Raw
Ether / IP / UDP / DNS Qry "b'www.gstatic.com.'"
Ether / IP / UDP / DNS Qry "b'www.gstatic.com.'"
Ether / IP / UDP / DNS Ans "2404:6800:4002:82e::2003"
Ether / IP / UDP / DNS Ans "142.250.207.195"
Ether / IP / UDP 10.0.2.15:49270 > 142.250.207.227:443 / Raw
Ether / IP / UDP 142.250.207.227:443 > 10.0.2.15:49270 / Raw
Ether / IP / UDP 142.250.207.227:443 > 10.0.2.15:49270 / Raw
Ether / IP / UDP 142.250.207.227:443 > 10.0.2.15:49270 / Raw
Ether / IP / UDP 142.250.207.227:443 > 10.0.2.15:49270 / Raw
Ether / IP / UDP 142.250.207.227:443 > 10.0.2.15:49270 / Raw
Ether / IP / UDP 142.250.207.227:443 > 10.0.2.15:49270 / Raw
Ether / IP / UDP 142.250.207.227:443 > 10.0.2.15:49270 / Raw
Ether / IP / UDP 142.250.207.227:443 > 10.0.2.15:49270 / Raw
Ether / IP / UDP 142.250.207.227:443 > 10.0.2.15:49270 / Raw
Ether / IP / UDP 142.250.207.227:443 > 10.0.2.15:49270 / Raw
Ether / IP / UDP 10.0.2.15:49270 > 142.250.207.227:443 / Raw
```

This is what shows in idle state during capturing:



```
Ether / IP / UDP 10.0.2.15:43980 > 172.217.166.54:443 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 10.0.2.15:43980 > 172.217.166.54:443 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 10.0.2.15:43980 > 172.217.166.54:443 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 10.0.2.15:43980 > 172.217.166.54:443 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 10.0.2.15:43980 > 172.217.166.54:443 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 10.0.2.15:43980 > 172.217.166.54:443 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 10.0.2.15:43980 > 172.217.166.54:443 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 10.0.2.15:43980 > 172.217.166.54:443 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 172.217.166.54:443 > 10.0.2.15:43980 / Raw
Ether / IP / UDP 10.0.2.15:43980 > 172.217.166.54:443 / Raw
```

```
Ether / IP / TCP 10.0.2.15:37366 > 103.102.166.224:https A
Ether / IP / TCP 103.102.166.224:https > 10.0.2.15:37366 PA / Raw
Ether / IP / TCP 10.0.2.15:37366 > 103.102.166.224:https A
Ether / IP / UDP / DNS Qry "b'tp.c95e7e602-frontier.amazon.in.'"
Ether / IP / UDP / DNS Qry "b'tp.c95e7e602-frontier.amazon.in.'"
Ether / IP / UDP / DNS Ans "b'd1elgm1ww0d6wo.cloudfront.net.'"
Ether / IP / UDP / DNS Qry "b'drive.google.com.'"
Ether / IP / UDP / DNS Qry "b'd1elgm1ww0d6wo.cloudfront.net.'"
Ether / IP / UDP / DNS Ans "b'd1elgm1ww0d6wo.cloudfront.net.'"
Ether / IP / UDP / DNS Ans
Ether / IP / UDP / DNS Ans "2404:6800:4009:822::200e"
Ether / IP / UDP / DNS Qry "b'accounts.google.com.'"
Ether / IP / UDP / DNS Qry "b'accounts.google.com.'"
Ether / IP / UDP / DNS Qry "b'star-mini.c10r.facebook.com.'"
Ether / IP / UDP / DNS Qry "b'star-mini.c10r.facebook.com.'"
Ether / IP / UDP / DNS Ans "2404:6800:4009:80b::200d"
Ether / IP / UDP / DNS Ans "172.217.160.205"
Ether / IP / UDP / DNS Ans "2a03:2880:f144:82:face:b00c:0:25de"
Ether / IP / UDP / DNS Ans "157.240.198.35"
Ether / IP / UDP / DNS Qry "b'reddit.map.fastly.net.'"
Ether / IP / UDP / DNS Qry "b'reddit.map.fastly.net.'"
Ether / IP / UDP / DNS Qry "b'twitter.com.'"
Ether / IP / UDP / DNS Qry "b'getpocket.com.'"
Ether / IP / UDP / DNS Qry "b'getpocket.com.'"
Ether / IP / UDP / DNS Ans
Ether / IP / UDP / DNS Ans
Ether / IP / UDP / DNS Ans "199.232.21.140"
Ether / IP / UDP / DNS Ans "13.224.21.10"
Ether / IP / UDP / DNS Ans
Ether / IP / UDP / DNS Qry "b'www.mozilla.org.'"
Ether / IP / UDP / DNS Qry "b'www.mozilla.org.'"
Ether / IP / UDP / DNS Qry "b'dualstack.guardian.map.fastly.net.'"
Ether / IP / UDP / DNS Qry "b'dualstack.guardian.map.fastly.net.'"
Ether / IP / UDP / DNS Ans "b'www.mozilla.org.cdn.cloudflare.net.'"
Ether / IP / UDP / DNS Ans "b'www.mozilla.org.cdn.cloudflare.net.'"
Ether / IP / UDP / DNS Ans "2a04:4e42:42::367"
Ether / IP / UDP / DNS Ans "199.232.21.111"
Ether / IP / UDP / DNS Qry "b'prod.ingestion-edge.prod.dataops.mozgcp.net.'"
Ether / IP / TCP 10.0.2.15:49144 > 35.227.207.240:https PA / Raw
Ether / IP / TCP 35.227.207.240:https > 10.0.2.15:49144 A / Padding
Ether / IP / UDP / DNS Ans
Ether / IP / TCP 10.0.2.15:49144 > 35.227.207.240:https PA / Raw
```

When we head back to Mozilla Firefox's home page:

```
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:38611 / Raw
Ether / IP / UDP 10.0.2.15:38611 > 142.250.77.238:443 / Raw
Ether / IP / UDP 142.250.77.238:443 > 10.0.2.15:38611 / Raw
Ether / IP / UDP / DNS Qry "b'incoming.telemetry.mozilla.org.'"
Ether / IP / UDP / DNS Qry "b'incoming.telemetry.mozilla.org.'"
Ether / IP / TCP 10.0.2.15:49144 > 35.227.207.240:https PA / Raw
Ether / IP / TCP 35.227.207.240:https > 10.0.2.15:49144 A / Padding
Ether / IP / TCP 10.0.2.15:49144 > 35.227.207.240:https PA / Raw
Ether / IP / TCP 35.227.207.240:https > 10.0.2.15:49144 A / Padding
Ether / IP / UDP / DNS Ans "b'telemetry-incoming.r53-2.services.mozilla.com.'"
Ether / IP / UDP / DNS Ans "b'telemetry-incoming.r53-2.services.mozilla.com.'"
Ether / IP / UDP / DNS Qry "b'prod.ingestion-edge.prod.dataops.mozgcp.net.'"
Ether / IP / UDP / DNS Ans
Ether / IP / TCP 35.227.207.240:https > 10.0.2.15:49144 PA / Raw
Ether / IP / TCP 10.0.2.15:49144 > 35.227.207.240:https PA / Raw
Ether / IP / TCP 35.227.207.240:https > 10.0.2.15:49144 A / Padding
Ether / IP / UDP / DNS Qry "b'img-getpocket.cdn.mozilla.net.'"
Ether / IP / TCP 10.0.2.15:50508 > 34.120.237.76:https PA / Raw
Ether / IP / TCP 34.120.237.76:https > 10.0.2.15:50508 A / Padding
Ether / IP / UDP / DNS Qry "b'img-getpocket.cdn.mozilla.net.'"
Ether / IP / UDP / DNS Ans "b'img-getpocket-cdn.prod.mozaws.net.'"
Ether / IP / UDP / DNS Ans "b'img-getpocket-cdn.prod.mozaws.net.'"
Ether / IP / TCP 34.120.237.76:https > 10.0.2.15:50508 PA / Raw
Ether / IP / TCP 10.0.2.15:50508 > 34.120.237.76:https A
Ether / IP / TCP 34.120.237.76:https > 10.0.2.15:50508 PA / Raw
Ether / IP / TCP 10.0.2.15:50508 > 34.120.237.76:https A
Ether / IP / TCP 34.120.237.76:https > 10.0.2.15:50508 PA / Raw
Ether / IP / TCP 10.0.2.15:50508 > 34.120.237.76:https A
Ether / IP / TCP 10.0.2.15:50508 > 34.120.237.76:https PA / Raw
```

When the images and media of a site are loading up:

```
Ether / IP / UDP 172.217.160.198:443 > 10.0.2.15:60190 / Raw
Ether / IP / UDP / DNS Qry "b'www.gqindia.com.'"
Ether / IP / UDP / DNS Qry "b'scroll.in.'"
Ether / IP / UDP / DNS Qry "b'www.gqindia.com.'"
Ether / IP / UDP / DNS Ans
Ether / IP / UDP / DNS Ans "b'cni-digital.map.fastly.net.'"
Ether / IP / UDP / DNS Ans "b'cni-digital.map.fastly.net.'"
Ether / IP / UDP / DNS Qry "b'cni-digital.map.fastly.net.'"
Ether / IP / UDP / DNS Ans
Ether / IP / TCP 10.0.2.15:52606 > 49.44.178.171:http A
Ether / IP / TCP 49.44.178.171:http > 10.0.2.15:52606 A / Padding
Ether / IP / TCP 10.0.2.15:40644 > 142.250.193.195:http A
Ether / IP / TCP 142.250.193.195:http > 10.0.2.15:40644 A / Padding
Ether / IP / UDP / DNS Qry "b'hearst-hdm.map.fastly.net.'"
Ether / IP / UDP / DNS Qry "b'www.thequint.com.'"
Ether / IP / UDP / DNS Qry "b'www.thequint.com.'"
Ether / IP / UDP / DNS Qry "b'hearst-hdm.map.fastly.net.'"
Ether / IP / UDP / DNS Ans "199.232.20.155"
Ether / IP / UDP / DNS Ans "b'thequint.publisher.quintype.io.'"
Ether / IP / UDP / DNS Ans
Ether / IP / UDP / DNS Ans "b'thequint.publisher.quintype.io.'"
Ether / IP / TCP 10.0.2.15:40640 > 142.250.193.195:http A
Ether / IP / TCP 142.250.193.195:http > 10.0.2.15:40640 A / Padding
Ether / IP / TCP 10.0.2.15:44906 > 34.107.221.82:http A
Ether / IP / TCP 10.0.2.15:44908 > 34.107.221.82:http A
Ether / IP / TCP 10.0.2.15:40612 > 142.250.193.195:http A
Ether / IP / TCP 34.107.221.82:http > 10.0.2.15:44906 A / Padding
Ether / IP / TCP 34.107.221.82:http > 10.0.2.15:44908 A / Padding
Ether / IP / TCP 142.250.193.195:http > 10.0.2.15:40612 A / Padding
Ether / IP / UDP / DNS Qry "b'www.prd.map.nytimes.com.'"
Ether / IP / UDP / DNS Qry "b'www.prd.map.nytimes.com.'"
Ether / IP / UDP / DNS Qry "b'www.politico.com.cdn.cloudflare.net.'"
Ether / IP / UDP / DNS Qry "b'www.politico.com.cdn.cloudflare.net.'"
Ether / IP / UDP / DNS Ans "b'nytimes.map.fastly.net.'"
Ether / IP / UDP / DNS Ans "b'nytimes.map.fastly.net.'"
Ether / IP / UDP / DNS Qry "b'nytimes.map.fastly.net.'"
Ether / IP / UDP / DNS Ans "104.18.16.202"
Ether / IP / UDP / DNS Ans
Ether / IP / UDP / DNS Ans "2606:4700::6812:10ca"
Ether / IP / UDP / DNS Qry "b'getpocket.com.'"
Ether / IP / UDP / DNS Qry "b'i-d.vice.com.'"
Ether / IP / UDP / DNS Ans
Ether / IP / UDP / DNS Qry "b'i-d.vice.com.'"
Ether / IP / UDP / DNS Ans "b'http2.vice.map.fastly.net.'"
Ether / IP / UDP / DNS Ans "b'http2.vice.map.fastly.net.'"
Ether / IP / UDP / DNS Qry "b'http2.vice.map.fastly.net.'"
Ether / IP / UDP / DNS Ans
^C<Sniffed: TCP:190 UDP:802 ICMP:0 Other:0>
```

Viewing details of a single captured packet using show() command:

```
>>> sniff(count=1,iface="enp0s3",prn=lambda x:x.show())
###[ Ethernet ]###
  dst       = 52:54:00:12:35:02
  src       = 08:00:27:ae:d5:14
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 79
     id        = 51578
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = tcp
     chksum    = 0x1210
     src       = 10.0.2.15
     dst       = 172.217.166.54
     \options   \
###[ TCP ]###
        sport     = 53318
        dport     = https
        seq       = 794007849
        ack       = 30149470
        dataofs   = 5
        reserved  = 0
        flags     = PA
        window    = 62780
        chksum    = 0x5f60
        urgptr    = 0
        options   = []
###[ Raw ]###
           load      = '\x17\x03\x03\x00"\\xdf@\\xaa\x0e\\xe0\\xa1=s\\xd0t-z\\x8en\\xf1\\xf0\\xee\\xaf\x1cP\\xec/\\x85\\xfe\\x8eo.4\x0f\\x84+p\\x99x'

<Sniffed: TCP:1 UDP:0 ICMP:0 Other:0>
>>>
```

```
└─# ./run_scapy
INFO: Can't import PyX. Won't be able to use psdump() or pdfdump().

                     aSPY//YASa
             apyyyyCY//////////YCa       |
            sY//////YSpcs  scpCY//Pp     | Welcome to Scapy
 ayp ayyyyyyySCP//Pp           syY//C    | Version 2.4.5rc1.dev159
 AYAsAYYYYYYYY///Ps              cY//S   |
         pCCCCY//p          cSSps y//Y   | https://github.com/secdev/scapy
         SPPPP///a          pP///AC//Y   |
              A//A            cyP////C   | Have fun!
              p///Ac            sC///a   |
              P////YCpc           A//A   | Craft packets like it is your last
       scccccp///pSP///p          p//Y   | day on earth.
      sY/////////y  caa           S//P   |                     -- Lao-Tze
       cayCyayP//Ya               pY/Ya  |
        sY/PsY////YCc           aC//Yp
         sc  sccaCY//PCypaapyCP//YSs
                  spCPY//////YPSps
                       ccaacs
                                   using IPython 7.22.0
```

Show the routing table of networks.

```
>>> conf.route
Network         Netmask         Gateway         Iface   Output IP       Metric
0.0.0.0         0.0.0.0         192.168.152.2   eth0    192.168.152.128 100
127.0.0.0       255.0.0.0       0.0.0.0         lo      127.0.0.1       1
192.168.152.0   255.255.255.0   0.0.0.0         eth0    192.168.152.128 100
```

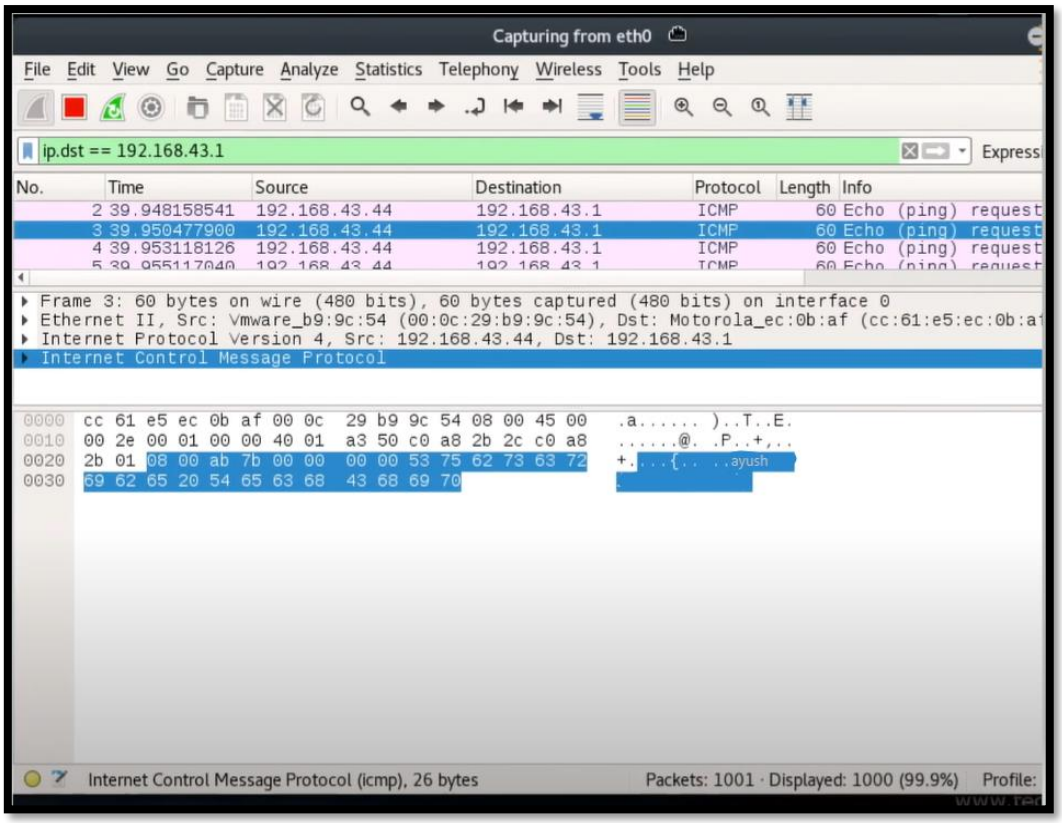
TASK 2 Identify the subdomains

```
>>> x.src='192.168.43.44'
>>> ans, unans = arping('192.168.43.44')
Begin emission:
Finished sending 1 packets.

Received 0 packets, got 0 answers, remaining 1 packets
>>> unans.summary()
Ether / ARP who has 192.168.43.44 says 192.168.43.144
>>> ans.summary()
>>> x.dst='192.168.43.1
```

```
└─# tcpdump -nn -i eth0 -v -w pkt.cap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
Got 612
```

```
File  Edit  View  Search  Terminal  Help
>>> send(x,count=1000)
.......................................................
.......................................................
.......................................................
.......................................................
.......................................................
.......................................................
.......................................................
.......................................................
.......................................................
.......................................................
.......................................................
.......................
Sent 1000 packets.
>>>
```

TASK Analyze the file, i.e., find the no. of TCP, UDP packets etc, provide summary of it. Capturing packets sent using wireshark



Live packet sniffing using scapy

We will launch Scapy from our terminal:

```
aryaman@aryaman-VirtualBox:~$ sudo scapy
[sudo] password for aryaman:

                     aSPY//YASa
             apyyyyCY//////////YCa       |
            sY//////YSpcs  scpCY//Pp     | Welcome to Scapy
 ayp ayyyyyyySCP//Pp           syY//C    | Version 2.4.5
 AYAsAYYYYYYYY///Ps              cY//S   |
        pCCCCY//p          cSSps y//Y    | https://github.com/secdev/scapy
        SPPPP///a          pP///AC//Y    |
             A//A            cyP////C    | Have fun!
             p///Ac            sC///a    |
             P////YCpc           A//A    | We are in France, we say Skappee.
      scccccp///pSP///p          p//Y    | OK? Merci.
     sY/////////y  caa           S//P    |             -- Sebastien Chabal
      cayCyayP//Ya              pY/Ya    |
       sY/PsY////YCc           aC//Yp
        sc  sccaCY//PCypaapyCP//YSs
                 spCPY//////YPSps
                      ccaacs
                                       using IPython 7.28.0
```

We will send and receive a single packet from Slashdot.org and will send an ICMP with a raw string in it.

```
>>> p=sr1(IP(dst="www.slashdot.org")/ICMP()/"XXXXXXXX")
Begin emission:
Finished sending 1 packets.
.*
Received 2 packets, got 1 answers, remaining 0 packets
```

We can then monitor the details of the packets using show function.

```
>>> p
<IP  version=4 ihl=5 tos=0x0 len=36 id=52787 flags= frag=0 ttl=40 proto=icmp chksum=0x7ce8 src=204.68.111.106 dst=10.0.2.15 |<ICMP  type=echo-reply code=0 chksum=0x9e9e id=0x0 seq=0x0 unused='' |<Raw  lo
ad='XXXXXXXX' |<Padding  load='\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00' |>>>>
>>> p.show()
###[ IP ]###
  version   = 4
  ihl       = 5
  tos       = 0x0
  len       = 36
  id        = 52787
  flags     =
  frag      = 0
  ttl       = 40
  proto     = icmp
  chksum    = 0x7ce8
  src       = 204.68.111.106
  dst       = 10.0.2.15
  \options   \
###[ ICMP ]###
     type      = echo-reply
     code      = 0
     chksum    = 0x9e9e
     id        = 0x0
     seq       = 0x0
     unused    = ''
###[ Raw ]###
        load      = 'XXXXXXXX'
###[ Padding ]###
           load      = '\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'
```

Packet has come back to us.We can use show command to view source address to the Linux Virutal Machine.We can see the echo replay and can view more details on the echo.

```
>>> p=sr1(IP(dst="8.8.8.8")/UDP()/DNS(rd=1,qd=DNSQR(qname="www.wikipedia.org")))
Begin emission:
Finished sending 1 packets.
.*
Received 2 packets, got 1 answers, remaining 0 packets
```

We will now perform a DNS Query and we will use Google's DNS server.We will use UDP Protocol and we will put a DNS Query.RD=1 means recursive is desired and will get results recursively.We will then put our query name and will put in Wikipedia to resolve it.We will get DNS Query name and then the answer we will look for in our data is resource record name-Type A and we will get our IP address in rdata variable.The data was resolved between Google's DNS server and my computer.

```
>>> p
<IP  version=4 ihl=5 tos=0x0 len=108 id=52790 flags= frag=0 ttl=64 proto=udp chksum=0x902c src=8.8.8.8 dst=10.0.2.15 |<UDP  sport=domain dport=domain len=88 chksum=0x848b |<DNS  id=0 qr=1 opcode=QUERY aa
=0 tc=0 rd=1 ra=1 z=0 ad=0 cd=0 rcode=ok qdcount=1 ancount=2 nscount=0 arcount=0 qd=<DNSQR  qname='www.wikipedia.org.' qtype=A qclass=IN |> an=<DNSRR  rrname='www.wikipedia.org.' type=CNAME rclass=IN ttl
=20494 rdlen=None rdata='dyna.wikimedia.org.' |<DNSRR  rrname='dyna.wikimedia.org.' type=A rclass=IN ttl=45 rdlen=None rdata=103.102.166.224 |>> ns=None ar=None |>>>
```

```
>>> sr1(IP(dst="8.8.8.8")/UDP()/DNS(rd=1,qd=DNSQR(qname="www.wikipedia.org")))
Begin emission:
Finished sending 1 packets.
.*
Received 1 packets, got 1 answers, remaining 0 packets
<IP  version=4 ihl=5 tos=0x0 len=108 id=52791 flags= frag=0 ttl=64 proto=udp chksum=0x902b src=8.8.8.8 dst=10.0.2.15 |<UDP  sport=domain dport=domain len=88 chksum=0x36a |<DNS  id=0 qr=1 opcode=QUERY aa=
0 tc=0 rd=1 ra=1 z=0 ad=0 cd=0 rcode=ok qdcount=1 ancount=2 nscount=0 arcount=0 qd=<DNSQR  qname='www.wikipedia.org.' qtype=A qclass=IN |> an=<DNSRR  rrname='www.wikipedia.org.' type=CNAME rclass=IN ttl=
20623 rdlen=None rdata='dyna.wikimedia.org.' |<DNSRR  rrname='dyna.wikimedia.org.' type=A rclass=IN ttl=78 rdlen=None rdata=103.102.166.224 |>> ns=None ar=None |>>>
```

If we don't want to put it into a variable,we can delete the assignment part and we can get the details from the send and receive command directly in the command line.

Now we will send and receive continuous packets.This time we will use only sr command to send and receive IP packets to destination(our gateway,my router) and we will send Destination port In which we will include 21,22,23,80.We will send and receive IP packets to my gateway we will use TCP for transfport and destination ports as mentioned above.We will send and receive 4 packets.

```
>>> sr(IP(dst="192.168.8.1")/TCP(dport=[21,22,23,80]))
Begin emission:
Finished sending 4 packets.
.*.
....^C
Received 7 packets, got 1 answers, remaining 3 packets
```

We got only 1 response from the routers of the web management interface.We will get the numbers of unanswered and answered packets.

```
(<Results: TCP:1 UDP:0 ICMP:0 Other:0>,
 <Unanswered: TCP:3 UDP:0 ICMP:0 Other:0>)
```

We will store the data received in ans,uans variables.

>>>ans,uans=_

```
>>> ans.summary()
IP / TCP 192.168.8.205:ftp_data > 192.168.8.1:http S ==> IP / TCP 192.168.8.1:http > 192.168.8.205:ftp_data SA / Paddi
ng
```

After we get the summary,we will notice that an answer has been sent from the gateway to us(with a SYN ACK).

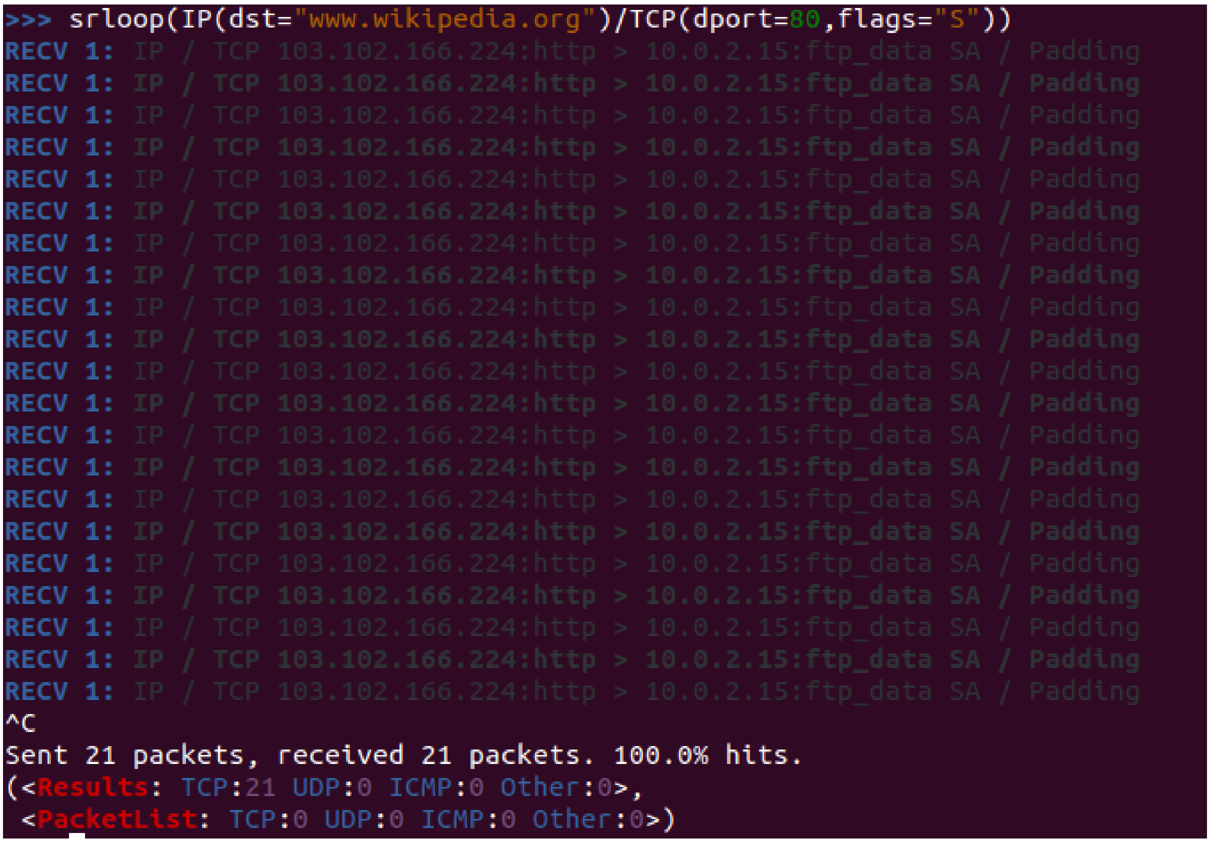
We will print hexdump of packets that we have received and the replies and we will loop through the answers.We want to print the fields of packets that we have received.Since it is SYN and an ACK,we will know that the machine was trying to finish the connection.

```
>>> for snd,rcv in ans:
...:     print(hexdump(rcv), rcv.show())
...:
0000  45 00 00 2C 00 00 40 00 40 06 A8 AD C0 A8 08 01  E..,..@.@.......
0010  C0 A8 08 CD 00 50 00 14 08 B6 F5 9E 00 00 00 01  .....P..........
0020  60 12 72 10 95 2D 00 00 02 04 05 B4 00 00        `.r..-........
###[ IP ]###
```

```
  version= 4
  ihl= 5
  tos= 0x0
  len= 44
  id= 0
  flags= DF
  frag= 0
  ttl= 64
  proto= tcp
  chksum= 0xa8ad
  src= 192.168.8.1
  dst= 192.168.8.205
  \options\
###[ TCP ]###
     sport= http
     dport= ftp_data
     seq= 146208158
     ack= 1
```

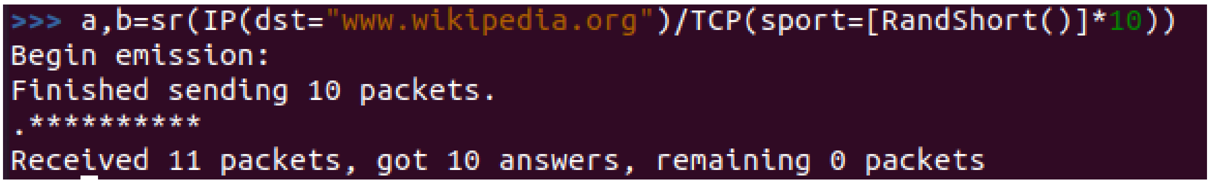
```
     ack= 1
     dataofs= 6
     reserved= 0
     flags= SA
     window= 29200
     chksum= 0x952d
     urgptr= 0
     options= [('MSS', 1460)]
###[ Padding ]###
        load= '\x00\x00'

None None
```

We can send and receive on a loop.Our destination would be Wikipedia and we will send a TCP-a destination port and we will also specify flags.In the TCP transmission to Wikipedia on a loop,we will contact Wikipedia on a loop and we will set the flag to SYN and we will perform a SYN flooding attack and we can specify the timing and how quickly it can happen.The SYN and the ACK will come back to us,which is basically a flooding attack against Wikipedia by sending repeated SYN requests-sending multiple times to establish a 3 way handshake.



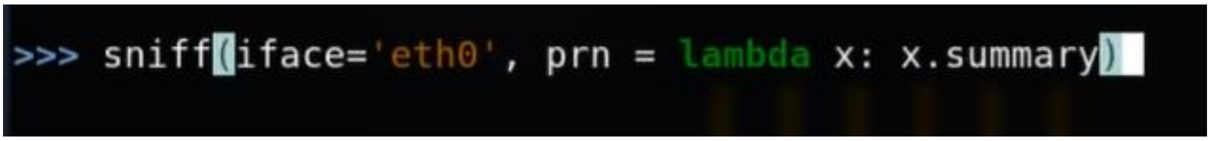
```
>>> srloop(IP(dst="www.wikipedia.org")/TCP(dport=80,flags="S"))
RECV 1: IP / TCP 103.102.166.224:http > 10.0.2.15:ftp_data SA / Padding
RECV 1: IP / TCP 103.102.166.224:http > 10.0.2.15:ftp_data SA / Padding
RECV 1: IP / TCP 103.102.166.224:http > 10.0.2.15:ftp_data SA / Padding
RECV 1: IP / TCP 103.102.166.224:http > 10.0.2.15:ftp_data SA / Padding
RECV 1: IP / TCP 103.102.166.224:http > 10.0.2.15:ftp_data SA / Padding
RECV 1: IP / TCP 103.102.166.224:http > 10.0.2.15:ftp_data SA / Padding
RECV 1: IP / TCP 103.102.166.224:http > 10.0.2.15:ftp_data SA / Padding
RECV 1: IP / TCP 103.102.166.224:http > 10.0.2.15:ftp_data SA / Padding
RECV 1: IP / TCP 103.102.166.224:http > 10.0.2.15:ftp_data SA / Padding
RECV 1: IP / TCP 103.102.166.224:http > 10.0.2.15:ftp_data SA / Padding
RECV 1: IP / TCP 103.102.166.224:http > 10.0.2.15:ftp_data SA / Padding
RECV 1: IP / TCP 103.102.166.224:http > 10.0.2.15:ftp_data SA / Padding
RECV 1: IP / TCP 103.102.166.224:http > 10.0.2.15:ftp_data SA / Padding
RECV 1: IP / TCP 103.102.166.224:http > 10.0.2.15:ftp_data SA / Padding
RECV 1: IP / TCP 103.102.166.224:http > 10.0.2.15:ftp_data SA / Padding
RECV 1: IP / TCP 103.102.166.224:http > 10.0.2.15:ftp_data SA / Padding
RECV 1: IP / TCP 103.102.166.224:http > 10.0.2.15:ftp_data SA / Padding
RECV 1: IP / TCP 103.102.166.224:http > 10.0.2.15:ftp_data SA / Padding
RECV 1: IP / TCP 103.102.166.224:http > 10.0.2.15:ftp_data SA / Padding
RECV 1: IP / TCP 103.102.166.224:http > 10.0.2.15:ftp_data SA / Padding
RECV 1: IP / TCP 103.102.166.224:http > 10.0.2.15:ftp_data SA / Padding
^C
Sent 21 packets, received 21 packets. 100.0% hits.
(<Results: TCP:21 UDP:0 ICMP:0 Other:0>,
 <PacketList: TCP:0 UDP:0 ICMP:0 Other:0>)
```

We can change what we are sending and in the transport layer,we can specify the source port which will be random-it will look like 10 random sources are trying to establish a connection.



```
>>> a,b=sr(IP(dst="www.wikipedia.org")/TCP(sport=[RandShort()]*10))
Begin emission:
Finished sending 10 packets.
.**********
Received 11 packets, got 10 answers, remaining 0 packets
```

We can plot out our answers using a and b variable.We will plot it automatically using a lambda function and we can plot out our sent packets.We can plot our information from Scapy which is a powerful features and we can chart that information on our console as well.



```
>>> sniff(iface='eth0', prn = lambda x: x.summary)
```

```
File  Edit  View  Search  Terminal  Help
>>>>
<bound method Ether.summary of <Ether  dst=01:00:5e:00:00:fc src=b0:10:41:2e:c0:05 type
=0x800 |<IP  version=4 ihl=5 tos=0x0 len=61 id=26359 flags= frag=0 ttl=1 proto=udp chks
um=0x8563 src=192.168.43.177 dst=224.0.0.252 options=[] |<UDP  sport=62235 dport=hostmo
n len=41 chksum=0xc56a |<LLMNRQuery  id=22937 qr=0 opcode=QUERY c=0 tc=0 z=0 rcode=ok q
dcount=1 ancount=0 nscount=0 arcount=0 qd=<DNSQR  qname='DESKTOP-1OPMJR1.' qtype=ALL qc
lass=IN |> an=None ns=None ar=None |>>>>>
<bound method Ether.summary of <Ether  dst=ff:ff:ff:ff:ff:ff src=b0:10:41:2e:c0:05 type
=0x806 |<ARP  hwtype=0x1 ptype=0x800 hwlen=6 plen=4 op=who-has hwsrc=b0:10:41:2e:c0:05
psrc=192.168.43.177 hwdst=00:00:00:00:00:00 pdst=192.168.43.1 |<Padding  load='\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00' |>>>>
<bound method Ether.summary of <Ether  dst=33:33:00:01:00:03 src=b0:10:41:2e:c0:05 type
=0x86dd |<IPv6  version=6 tc=0 fl=385475 plen=41 nh=UDP hlim=1 src=fe80::941:de26:9ddc:
bac8 dst=ff02::1:3 |<UDP  sport=62235 dport=hostmon len=41 chksum=0x552c |<LLMNRQuery
id=22937 qr=0 opcode=QUERY c=0 tc=0 z=0 rcode=ok qdcount=1 ancount=0 nscount=0 arcount=
0 qd=<DNSQR  qname='DESKTOP-1OPMJR1.' qtype=ALL qclass=IN |> an=None ns=None ar=None |>
>>>>
<bound method Ether.summary of <Ether  dst=01:00:5e:00:00:fc src=b0:10:41:2e:c0:05 type
=0x800 |<IP  version=4 ihl=5 tos=0x0 len=61 id=26360 flags= frag=0 ttl=1 proto=udp chks
um=0x8562 src=192.168.43.177 dst=224.0.0.252 options=[] |<UDP  sport=62235 dport=hostmo
n len=41 chksum=0xc56a |<LLMNRQuery  id=22937 qr=0 opcode=QUERY c=0 tc=0 z=0 rcode=ok q
dcount=1 ancount=0 nscount=0 arcount=0 qd=<DNSQR  qname='DESKTOP-1OPMJR1.' qtype=ALL qc
lass=IN |> an=None ns=None ar=None |>>>>>
```

The sniff() function listens for an infinite period of time until the user interrupts.

To restrict the number of packets to be captured sniff() allows a count parameter. By specifying a value for the count, the packet capturing will be restricted to the specified number.

```
Scapy v2.4.4
File  Actions  Edit  View  Help
>>> capture=sniff(count=5)
>>> capture.summary()
Ether / IP / TCP 192.168.147.130:43450 > 103.102.166.224:https PA / Raw
Ether / IP / TCP 103.102.166.224:https > 192.168.147.130:43450 A / Padding
Ether / IP / TCP 192.168.147.130:43450 > 103.102.166.224:https PA / Raw
Ether / IP / TCP 103.102.166.224:https > 192.168.147.130:43450 A / Padding
Ether / IP / TCP 103.102.166.224:https > 192.168.147.130:43450 PA / Raw
>>>
```

TASK 4 Check the route of the provide URL using scapy.

```
File  Edit  View  Search  Terminal  Help
>>> traceroute('http://www.testingexcellence.com')
Begin emission:
*Finished sending 30 packets.
**********************
```

```
File  Edit  View  Search  Terminal  Help
11 49.45.4.85       11
12 49.45.4.103      11
13 38.104.85.57     11
14 38.104.84.254    11
15 104.24.101.192   SA
16 104.24.101.192   SA
17 104.24.101.192   SA
18 104.24.101.192   SA
19 104.24.101.192   SA
20 104.24.101.192   SA
21 104.24.101.192   SA
22 104.24.101.192   SA
23 104.24.101.192   SA
24 104.24.101.192   SA
25 104.24.101.192   SA
26 104.24.101.192   SA
27 104.24.101.192   SA
28 104.24.101.192   SA
29 104.24.101.192   SA
30 104.24.101.192   SA

(<Traceroute: TCP:16 UDP:0 ICMP:8 Other:0>,
 <Unanswered: TCP:6 UDP:0 ICMP:0 Other:0>)
>>>
```

You can also filter packets while sniffing using the filter parameter. It uses a Berkeley Packet Filter (BPF) syntax.

The following command will capture only TCP packets:

sniff(filter="tcp", count=5)

Similarly, you can filter any packet on the basis of source/destination IP address, port number, protocol and lot more by using the BPF syntax.

```
Scapy v2.4.4
File  Actions  Edit  View  Help
>>> sniff(filter="tcp", count=5)
<Sniffed: TCP:5 UDP:0 ICMP:0 Other:0>
>>>
```

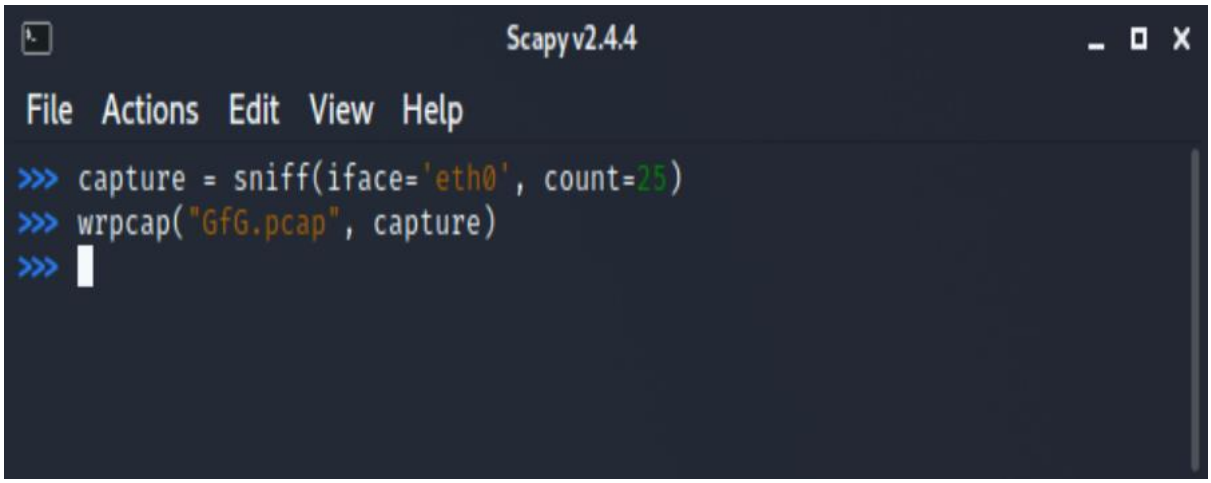
When scapy sniffs packets, it generally sniffs from all of your network interfaces. However, we can explicitly mention the interfaces that we would like to sniff on using the iface parameter. The iface can either be an element or a list of elements.

TASK 5 Provide the packets sent and received summary using SCAPY, store the contents using PCAP file

Scapy also allows us to store the sniffed packets in a pcap file. Running the following command will write the sniffed packets in a pcap:

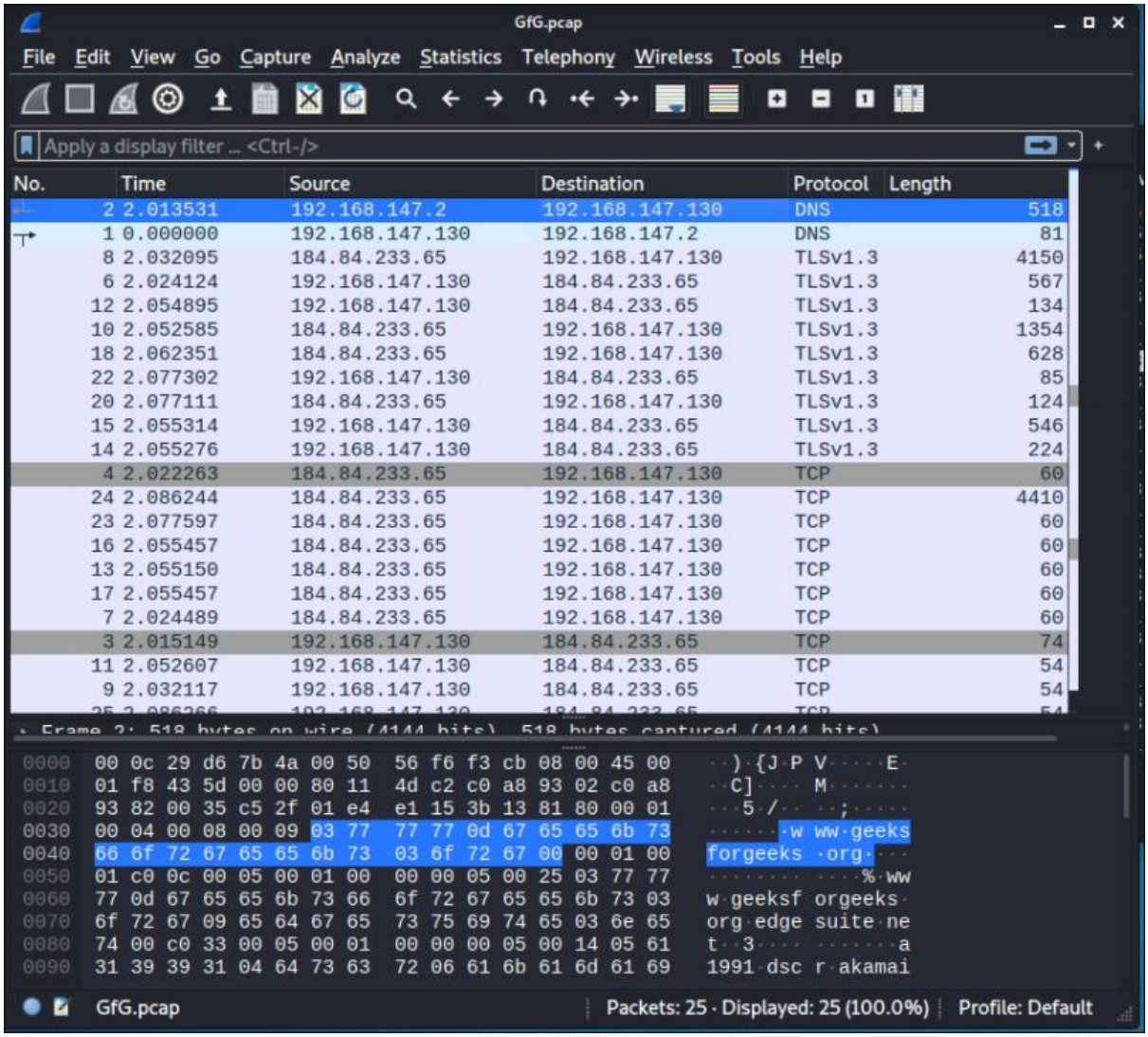
wrpcap("<file name>", capture)

where capture is the list of sniffed packets.



The stored pcap files can be analyzed using Wireshark, tcpdump, WinDump, Packet Square, etc.

Opening GfG.pcap using Wireshark:



We can also sniff packets offline from pcap files by running the following command:

sniff(offline="<file name>")

Scapy v2.4.4

File Actions Edit View Help

```
>>> sniff(offline="GfG.pcap", prn=lambda x:x.summary())
Ether / IP / UDP / DNS Qry "b'www.geeksforgeeks.org.'"
Ether / IP / UDP / DNS Ans "b'www.geeksforgeeks.org.edgesuite.net.'"
Ether / IP / TCP 192.168.147.130:40904 > 184.84.233.65:https S
Ether / IP / TCP 184.84.233.65:https > 192.168.147.130:40904 SA / Padding
Ether / IP / TCP 192.168.147.130:40904 > 184.84.233.65:https A
Ether / IP / TCP 192.168.147.130:40904 > 184.84.233.65:https PA / Raw
Ether / IP / TCP 184.84.233.65:https > 192.168.147.130:40904 A / Padding
Ether / IP / TCP 184.84.233.65:https > 192.168.147.130:40904 PA / Raw
Ether / IP / TCP 192.168.147.130:40904 > 184.84.233.65:https A
Ether / IP / TCP 184.84.233.65:https > 192.168.147.130:40904 PA / Raw
Ether / IP / TCP 192.168.147.130:40904 > 184.84.233.65:https A
Ether / IP / TCP 192.168.147.130:40904 > 184.84.233.65:https PA / Raw
Ether / IP / TCP 184.84.233.65:https > 192.168.147.130:40904 A / Padding
Ether / IP / TCP 192.168.147.130:40904 > 184.84.233.65:https PA / Raw
Ether / IP / TCP 192.168.147.130:40904 > 184.84.233.65:https PA / Raw
Ether / IP / TCP 184.84.233.65:https > 192.168.147.130:40904 A / Padding
Ether / IP / TCP 184.84.233.65:https > 192.168.147.130:40904 A / Padding
Ether / IP / TCP 184.84.233.65:https > 192.168.147.130:40904 PA / Raw
Ether / IP / TCP 192.168.147.130:40904 > 184.84.233.65:https A
Ether / IP / TCP 184.84.233.65:https > 192.168.147.130:40904 PA / Raw
Ether / IP / TCP 192.168.147.130:40904 > 184.84.233.65:https A
Ether / IP / TCP 192.168.147.130:40904 > 184.84.233.65:https PA / Raw
Ether / IP / TCP 184.84.233.65:https > 192.168.147.130:40904 A / Padding
Ether / IP / TCP 184.84.233.65:https > 192.168.147.130:40904 PA / Raw
Ether / IP / TCP 192.168.147.130:40904 > 184.84.233.65:https A
<Sniffed: TCP:23 UDP:2 ICMP:0 Other:0>
>>>
```