

**Міністерство освіти і науки України
Національний технічний університет України «КПІ» імені Ігоря Сікорського
Кафедра обчислювальної техніки ФІОТ**

**ЗВІТ
з лабораторної роботи №1
з навчальної дисципліни «Тестування та контроль якості (QA) вбудованих систем »**

Тема:

Дослідження засобів канального рівня моделі OSI. Протокол ARP

Виконав:

Студент 4 курсу кафедри ОТ ФІОТ,
Навчальної групи ІВ-91 Желепа
В.В.

Київ 2022

Хід роботи:

1. Додаємо офіційний РРА, щоб завантажити останню стабільну версію:

```
valentyn@valentyn-VirtualBox:~$ sudo add-apt-repository ppa:wireshark-dev/stable
[sudo] пароль до valentyn:
Latest stable Wireshark releases back-ported from Debian package versions.

Back-porting script is available at https://github.com/rbalint/pkg-wireshark-ubuntu-ppa

From Ubuntu 16.04 you also need to enable "universe" repository, see:
http://askubuntu.com/questions/148638/how-do-i-enable-the-universe-repository

The packaging repository for Debian and Ubuntu is at: https://salsa.debian.org/debian/wireshark
Детальніше: https://launchpad.net/~wireshark-dev/+archive/ubuntu/stable
Натисніть [ENTER] для продовження, або Ctrl-C, щоб скасувати додавання.

В кеші:1 http://ua.archive.ubuntu.com/ubuntu bionic InRelease
В кеші:2 http://ua.archive.ubuntu.com/ubuntu bionic-updates InRelease
В кеші:3 http://ua.archive.ubuntu.com/ubuntu bionic-backports InRelease
Отр:4 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu bionic InRelease [21,3 kB]
Отр:5 http://security.ubuntu.com/ubuntu bionic-security InRelease [88,7 kB]
Отр:6 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu bionic/main amd64 Packages [4 216 B]
Отр:7 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu bionic/main i386 Packages [4 208 B]
Отр:8 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu bionic/main Translation-en [1 932 B]
Отримано 120 kB за 1сВ (109 kB/s)

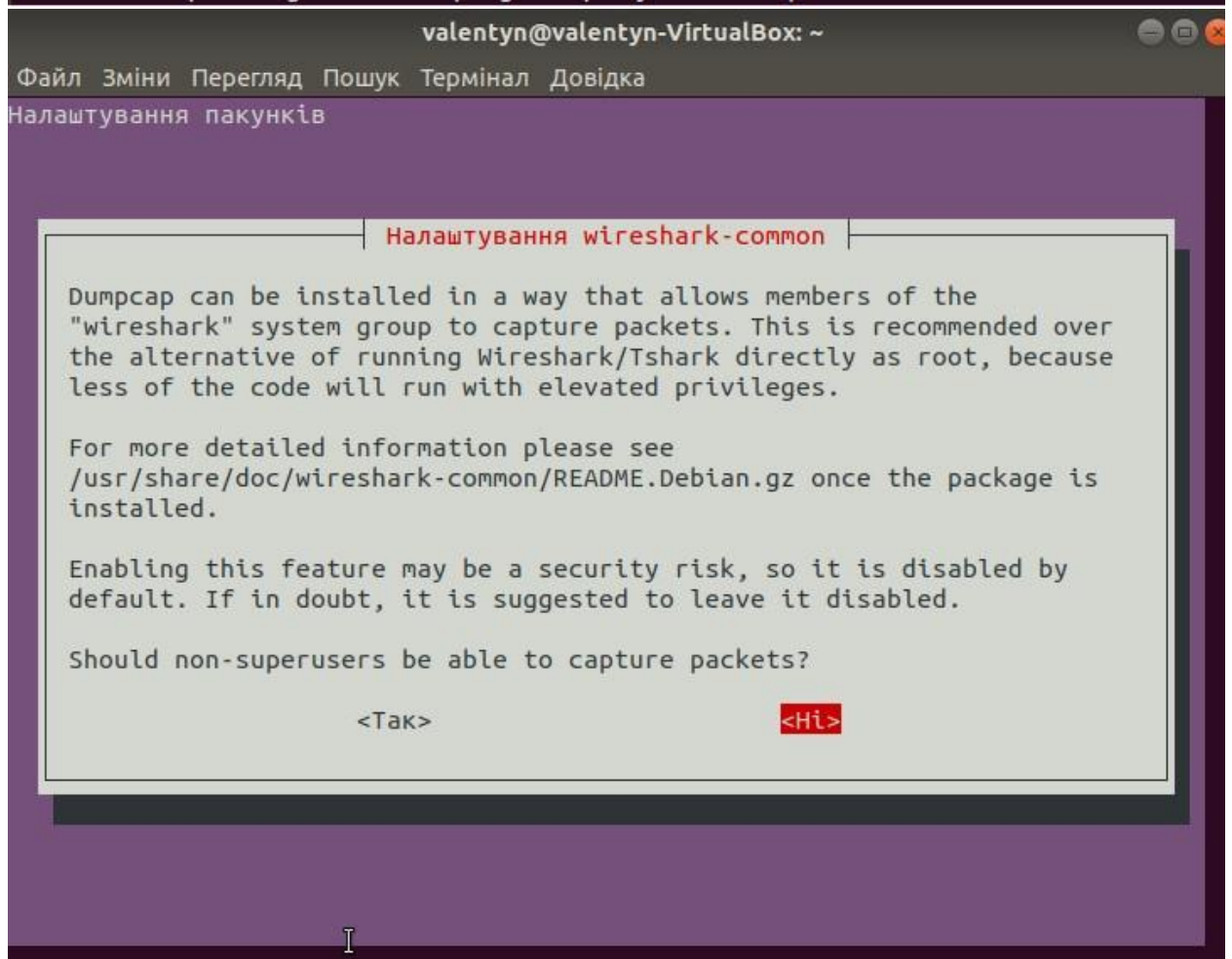
Отр:8 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu bionic/main Translation-en [1 932 B]
Отримано 120 kB за 1сВ (109 kB/s)
Вчитування переліків пакунків... Виконано
valentyn@valentyn-VirtualBox:~$
```

2. Оновлюємо списки пакетів з репозиторіїв для оновлення пакетів:

```
valentyn@valentyn-VirtualBox:~$ sudo apt-get update
В кеші:1 http://ua.archive.ubuntu.com/ubuntu bionic InRelease
В кеші:2 http://ua.archive.ubuntu.com/ubuntu bionic-updates InRelease
В кеші:3 http://ua.archive.ubuntu.com/ubuntu bionic-backports InRelease
Отр:4 http://security.ubuntu.com/ubuntu bionic-security InRelease [88,7 kB]
В кеші:5 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu bionic InRelease
Отримано 88,7 kB за 1сВ (175 kB/s)
Зчитування переліків пакунків... Виконано
valentyn@valentyn-VirtualBox:~$
```

3. Завантажуємо wireshark:

```
valentyn@valentyn-VirtualBox:~$ sudo apt-get install wireshark
Зчитування переліків пакунків... Виконано
Побудова дерева залежностей
Зчитування інформації про стан... Виконано
Наступні пакунки були встановлені автоматично і більше не потрібні:
gir1.2-geocodeglib-1.0 gir1.2-gst-plugins-base-1.0 gir1.2-gstreamer-1.0
gir1.2-gudev-1.0 gir1.2-udisks-2.0 grilo-plugins-0.3-base gstreamer1.0-gtk3
libcdr-0.1-1 libcolamd2 libdazzle-1.0-0 libe-book-0.1-1
libdataserverui-1.2-2 libepubgen-0.1-1 libetonyek-0.1-1 libevent-2.1-6
libexiv2-14 libfreerdp-client2-2 libfreerdp2-2 libgc1c2 libgee-0.8-2
libgexiv2-2 libgom-1.0-0 libgpod-common libgpod4 liblirc-client0
liblua5.3-0 libmediaart-2.0-0 libmtp-0.1-1 libodfgen-0.1-1 libqqwing2v5
libraw16 libsgutils2-2 libssh-4 libsuitesparseconfig5 libvncclient1
libwinpr2-2 libxapian30 lp-solve media-player-info python3-mako
python3-markupsafe syslinux syslinux-common syslinux-legacy
usb-creator-common
Використовуйте 'sudo apt autoremove' щоб видалити їх.
Буде встановлено такі додаткові пакунки:
libc-ares2 libdouble-conversion1 libmaxminddb0 libminizip1 libqgsttools-p1
libqt5core5a libqt5dbus5 libqt5gui5 libqt5multimedia5
libqt5multimedia5-plugins libqt5multimediawidgets5 libqt5network5
libqt5opengl5 libqt5printsupport5 libqt5svg5 libqt5widgets5 libsmi2ldbl
libsnappy1v5 libspandsp2 libssh-gcrypt-4 libwireshark-data libwireshark15
libwiretap12 libwsutil13 libxcb-xinerama0 qt5-gtk-platformtheme
qttranslations5-l10n wireshark-common wireshark-qt
Пропоновані пакунки:
mmdb-bin qt5-image-formats-plugins qtwayland5 snmp-mibs-downloader
```



Пропоновані пакунки:

mmdb-bin qt5-image-formats-plugins qtwayland5 snmp-mibs-downloader
geoipupdate geoip-database-extra libjs-leaflet libjs-leaflet.markercluster
wireshark-doc

НОВІ пакунки, які будуть встановлені:

libc-ares2 libdouble-conversion1 libmaxminddb0 libminizip1 libqgsttools-p1
libqt5core5a libqt5dbus5 libqt5gui5 libqt5multimedia5
libqt5multimedia5-plugins libqt5multimediawidgets5 libqt5network5
libqt5opengl5 libqt5printsupport5 libqt5svg5 libqt5widgets5 libsmi2ldbl
libsnappy1v5 libspandsp2 libssh-gcrypt-4 libwireshark-data libwireshark15
libwiretap12 libwsutil13 libxcb-xinerama0 qt5-gtk-platformtheme
qttranslations5-l10n wireshark wireshark-common wireshark-qt

оновлено 0, встановлено 30 нових, 0 відмічено для видалення і 495 не оновлено.

Необхідно завантажити 34,4 MB архівів.

Після цієї операції об'єм зайнятого дискового простору зросте на 172 MB.

Бажаєте продовжити? [Y=TAK/n=ні] Y

Отр:1 http://ua.archive.ubuntu.com/ubuntu/bionic/main/amd64/libdouble-conversion1-amd64_2.0.1-4ubuntu1 [33,0 kB]

Отр:2 http://ua.archive.ubuntu.com/ubuntu/bionic-updates/main/amd64/libqt5core5a-amd64_5.9.5+dfsg-0ubuntu2.6 [2 035 kB]

Отр:3 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu/bionic/main/amd64/libwireshark-data-all_3.6.5-1-ubuntu18.04.0+wiresharkdevstable [1 581 kB]

Отр:4 http://ua.archive.ubuntu.com/ubuntu/bionic-updates/main/amd64/libqt5dbus5-amd64_5.9.5+dfsg-0ubuntu2.6 [195 kB]

Отр:5 http://ua.archive.ubuntu.com/ubuntu/bionic-updates/main/amd64/libqt5network5-amd64_5.9.5+dfsg-0ubuntu2.6 [634 kB]

Отр:6 http://ua.archive.ubuntu.com/ubuntu/bionic-updates/main/amd64/libxcb-xinerama0-amd64_1.13-2~ubuntu18.04 [5 264 B]

Отр:7 <http://ua.archive.ubuntu.com/ubuntu/bionic-updates/main/amd64/libqt5gui5>

Файл Зміни Перегляд Пошук Термінал Довідка

```

amd64 1.3.1-1 [25,0 kB]
тр:11 http://ua.archive.ubuntu.com/ubuntu bionic/universe amd64 libminizip1 am
64 1.1-8build1 [20,2 kB]
тр:12 http://ua.archive.ubuntu.com/ubuntu bionic/universe amd64 libqt5multimed
a5 amd64 5.9.5-0ubuntu1 [293 kB]
тр:13 http://ua.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libqt5open
l5 amd64 5.9.5+dfsg-0ubuntu2.6 [132 kB]
тр:14 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu bionic/main amd64 l
bwsutil13 amd64 3.6.5-1~ubuntu18.04.0+wiresharkdevstable [126 kB]
тр:15 http://ua.archive.ubuntu.com/ubuntu bionic/universe amd64 libqt5multimed
awidgets5 amd64 5.9.5-0ubuntu1 [36,6 kB]
тр:16 http://ua.archive.ubuntu.com/ubuntu bionic/universe amd64 libqgsttools-p
amd64 5.9.5-0ubuntu1 [72,4 kB]
тр:17 http://ua.archive.ubuntu.com/ubuntu bionic/universe amd64 libqt5multimed
a5-plugins amd64 5.9.5-0ubuntu1 [194 kB]
тр:18 http://ua.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libqt5prin
support5 amd64 5.9.5+dfsg-0ubuntu2.6 [178 kB]
тр:19 http://ua.archive.ubuntu.com/ubuntu bionic/main amd64 libsmi2ldbl amd64
.4.8+dfsg2-15 [100 kB]
тр:20 http://ua.archive.ubuntu.com/ubuntu bionic/universe amd64 libspandsp2 am
64 0.0.6+dfsg-0.1 [273 kB]
тр:21 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu bionic/main amd64 l
bwiretap12 amd64 3.6.5-1~ubuntu18.04.0+wiresharkdevstable [272 kB]
тр:22 http://ua.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libssh-gcr
pt-4 amd64 0.8.0~20170825.94fa1e38-1ubuntu0.7 [172 kB]
тр:23 http://ua.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libc-ares2
amd64 1.14.0-1ubuntu0.1 [37,5 kB]
тр:24 http://ua.archive.ubuntu.com/ubuntu bionic/main amd64 libsnappy1v5 amd64
1.1.7-1 [16,0 kB]

```

```

Отр:24 http://ua.archive.ubuntu.com/ubuntu bionic/main amd64 libsnappy1v5 amd64
1.1.7-1 [16,0 kB]
Отр:25 http://ua.archive.ubuntu.com/ubuntu bionic-updates/main amd64 qt5-gtk-pl
atformtheme amd64 5.9.5+dfsg-0ubuntu2.6 [117 kB]
Отр:26 http://ua.archive.ubuntu.com/ubuntu bionic/main amd64 qttranslations5-l1
0n all 5.9.5-0ubuntu1 [1 485 kB]
Отр:27 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu bionic/main amd64 l
ibwireshark15 amd64 3.6.5-1~ubuntu18.04.0+wiresharkdevstable [16,8 MB]
Отр:28 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu bionic/main amd64 w
ireshark-common amd64 3.6.5-1~ubuntu18.04.0+wiresharkdevstable [481 kB]
Отр:29 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu bionic/main amd64 w
ireshark-qt amd64 3.6.5-1~ubuntu18.04.0+wiresharkdevstable [4 059 kB]
Отр:30 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu bionic/main amd64 w
ireshark amd64 3.6.5-1~ubuntu18.04.0+wiresharkdevstable [46,3 kB]
Отримано 34,4 МВ за 22сВ (1 535 kB/s)
Передналаштування пакунків...
Вибір раніше не обраного пакунку libdouble-conversion1:amd64.
(Читання бази даних ... на дану мить встановлено 163732 файли та каталоги.)
Приготування до розпакування .../00-libdouble-conversion1_2.0.1-4ubuntu1_amd64.
deb ...
Розпакування libdouble-conversion1:amd64 (2.0.1-4ubuntu1)...
Вибір раніше не обраного пакунку libqt5core5a:amd64.
Приготування до розпакування .../01-libqt5core5a_5.9.5+dfsg-0ubuntu2.6_amd64.de
b ...
Розпакування libqt5core5a:amd64 (5.9.5+dfsg-0ubuntu2.6)...
Вибір раніше не обраного пакунку libqt5dbus5:amd64.
Приготування до розпакування .../02-libqt5dbus5_5.9.5+dfsg-0ubuntu2.6_amd64.deb
...
Розпакування libqt5dbus5:amd64 (5.9.5+dfsg-0ubuntu2.6)...

```



```
Розпакування libqt5widgets5:amd64 (5.9.5+dfsg-0ubuntu2.6)...
Вибір раніше не обраного пакунку libqt5svg5:amd64.
Приготування до розпакування .../07-libqt5svg5_5.9.5-0ubuntu1.1_amd64.deb ...
Розпакування libqt5svg5:amd64 (5.9.5-0ubuntu1.1)...
Вибір раніше не обраного пакунку libmaxminddb0:amd64.
Приготування до розпакування .../08-libmaxminddb0_1.3.1-1_amd64.deb ...
Розпакування libmaxminddb0:amd64 (1.3.1-1)...
Вибір раніше не обраного пакунку libminizip1:amd64.
Приготування до розпакування .../09-libminizip1_1.1-8build1_amd64.deb ...
Розпакування libminizip1:amd64 (1.1-8build1)...
Вибір раніше не обраного пакунку libqt5multimedia5:amd64.
Приготування до розпакування .../10-libqt5multimedia5_5.9.5-0ubuntu1_amd64.deb
...
Розпакування libqt5multimedia5:amd64 (5.9.5-0ubuntu1)...
Вибір раніше не обраного пакунку libqt5opengl5:amd64.
Приготування до розпакування .../11-libqt5opengl5_5.9.5+dfsg-0ubuntu2.6_amd64.d
eb ...
Розпакування libqt5opengl5:amd64 (5.9.5+dfsg-0ubuntu2.6)...
Вибір раніше не обраного пакунку libqt5multimediawidgets5:amd64.
Приготування до розпакування .../12-libqt5multimediawidgets5_5.9.5-0ubuntu1_amd
64.deb ...
Розпакування libqt5multimediawidgets5:amd64 (5.9.5-0ubuntu1)...
Вибір раніше не обраного пакунку libqgsttools-p1:amd64.
Приготування до розпакування .../13-libqgsttools-p1_5.9.5-0ubuntu1_amd64.deb ..
.
Розпакування libqgsttools-p1:amd64 (5.9.5-0ubuntu1)...
Вибір раніше не обраного пакунку libqt5multimedia5-plugins:amd64.
Приготування до розпакування .../14-libqt5multimedia5-plugins_5.9.5-0ubuntu1_am
64.deb ...
Вибір раніше не обраного пакунку libwiretap12:amd64.
Приготування до розпакування .../23-libwiretap12_3.6.5-1~ubuntu18.04.0+wireshar
kdevstable_amd64.deb ...
Розпакування libwiretap12:amd64 (3.6.5-1~ubuntu18.04.0+wiresharkdevstable)...
Вибір раніше не обраного пакунку libwireshark15:amd64.
Приготування до розпакування .../24-libwireshark15_3.6.5-1~ubuntu18.04.0+wiresh
arkdevstable_amd64.deb ...
Розпакування libwireshark15:amd64 (3.6.5-1~ubuntu18.04.0+wiresharkdevstable)...
Вибір раніше не обраного пакунку qt5-gtk-platformtheme:amd64.
Приготування до розпакування .../25-qt5-gtk-platformtheme_5.9.5+dfsg-0ubuntu2.6
_amd64.deb ...
Розпакування qt5-gtk-platformtheme:amd64 (5.9.5+dfsg-0ubuntu2.6)...
Вибір раніше не обраного пакунку qttranslations5-l10n.
Приготування до розпакування .../26-qttranslations5-l10n_5.9.5-0ubuntu1_all.deb
...
Розпакування qttranslations5-l10n (5.9.5-0ubuntu1)...
Вибір раніше не обраного пакунку wireshark-common.
Приготування до розпакування .../27-wireshark-common_3.6.5-1~ubuntu18.04.0+wire
sharkdevstable_amd64.deb ...
Розпакування wireshark-common (3.6.5-1~ubuntu18.04.0+wiresharkdevstable)...
Вибір раніше не обраного пакунку wireshark-qt.
Приготування до розпакування .../28-wireshark-qt_3.6.5-1~ubuntu18.04.0+wireshar
kdevstable_amd64.deb ...
Розпакування wireshark-qt (3.6.5-1~ubuntu18.04.0+wiresharkdevstable)...
Вибір раніше не обраного пакунку wireshark.
Приготування до розпакування .../29-wireshark_3.6.5-1~ubuntu18.04.0+wiresharkde
vstable_amd64.deb ...
Розпакування wireshark (3.6.5-1~ubuntu18.04.0+wiresharkdevstable)...
Напаштовування libminizip1:amd64 (1.1-8build1)
```



```

Налаштовування libqt5core5a:amd64 (5.9.5+dfsg-0ubuntu2.6) ...
Налаштовування libqt5dbus5:amd64 (5.9.5+dfsg-0ubuntu2.6) ...
Налаштовування libqt5network5:amd64 (5.9.5+dfsg-0ubuntu2.6) ...
Налаштовування libwireshark12:amd64 (3.6.5-1~ubuntu18.04.0+wiresharkdevstable) ..
.
Налаштовування libqt5gui5:amd64 (5.9.5+dfsg-0ubuntu2.6) ...
Налаштовування qt5-gtk-platformtheme:amd64 (5.9.5+dfsg-0ubuntu2.6) ...
Налаштовування libqt5widgets5:amd64 (5.9.5+dfsg-0ubuntu2.6) ...
Налаштовування libwireshark15:amd64 (3.6.5-1~ubuntu18.04.0+wiresharkdevstable)
...
Налаштовування wireshark-common (3.6.5-1~ubuntu18.04.0+wiresharkdevstable) ...
Налаштовування libqt5printsupport5:amd64 (5.9.5+dfsg-0ubuntu2.6) ...
Налаштовування libqt5opengl5:amd64 (5.9.5+dfsg-0ubuntu2.6) ...
Налаштовування libqt5multimedia5:amd64 (5.9.5-0ubuntu1) ...
Налаштовування libqt5svg5:amd64 (5.9.5-0ubuntu1.1) ...
Налаштовування libqt5multimediawidgets5:amd64 (5.9.5-0ubuntu1) ...
Налаштовування libqgsttools-p1:amd64 (5.9.5-0ubuntu1) ...
Налаштовування wireshark-qt (3.6.5-1~ubuntu18.04.0+wiresharkdevstable) ...
Налаштовування libqt5multimedia5-plugins:amd64 (5.9.5-0ubuntu1) ...
Налаштовування wireshark (3.6.5-1~ubuntu18.04.0+wiresharkdevstable) ...
Обробка тригерів desktop-file-utils (0.23-1ubuntu3.18.04.2)...
Обробка тригерів libc-bin (2.27-3ubuntu1)...
Обробка тригерів man-db (2.8.3-2ubuntu0.1)...
Обробка тригерів shared-mime-info (1.9-2)...
Обробка тригерів gnome-menus (3.13.3-11ubuntu1.1)...
Обробка тригерів hicolor-icon-theme (0.17-2)...
Обробка тригерів mime-support (3.60ubuntu1)...
valentyn@valentyn-VirtualBox:~$ █

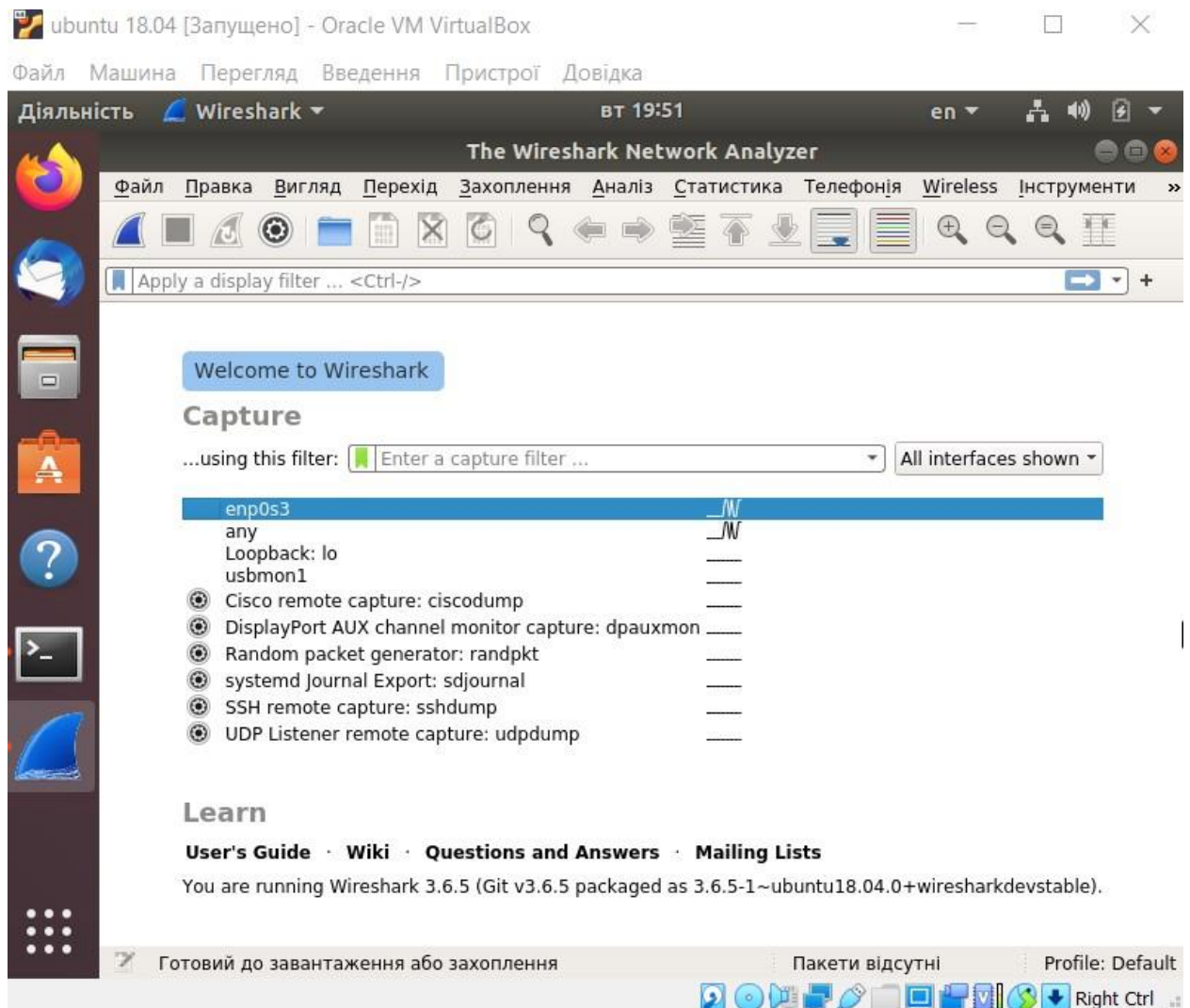
```

4. Запускаємо wireshark:

```

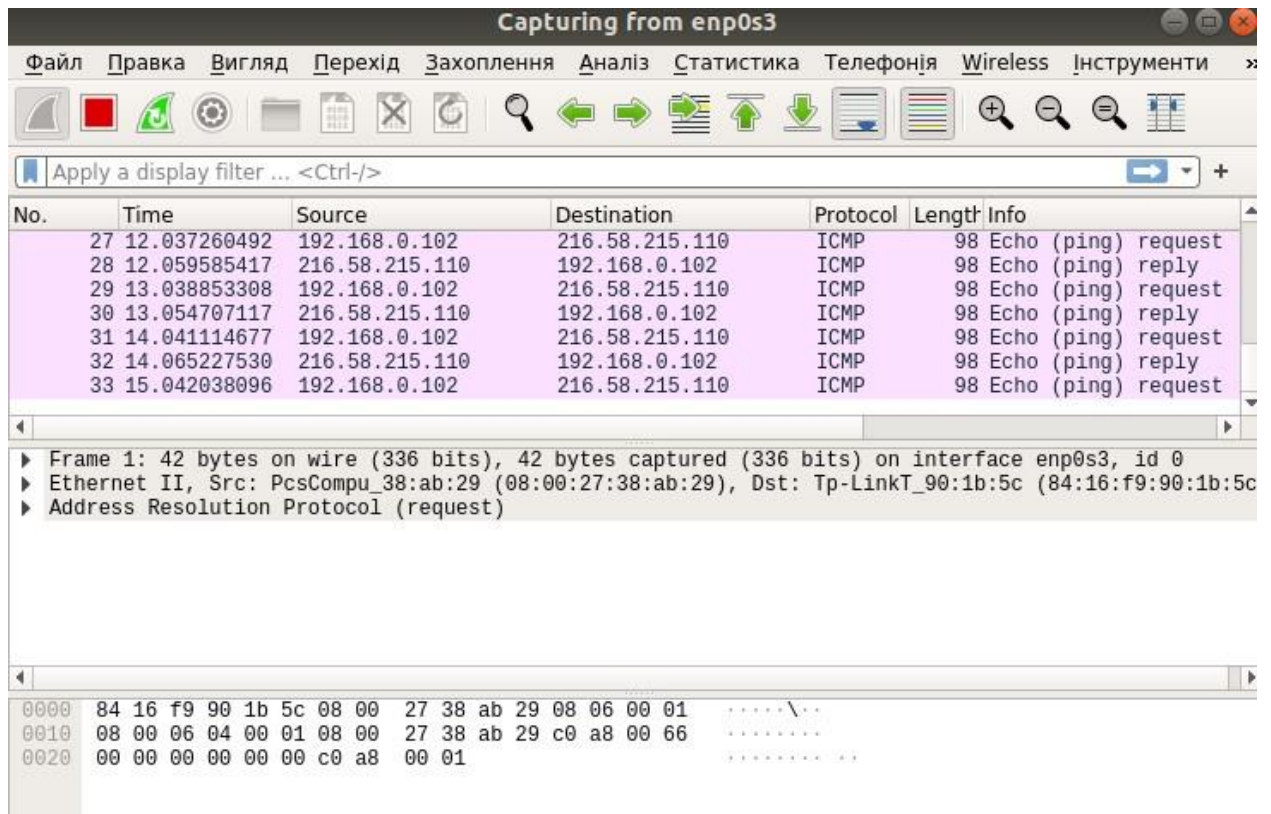
valentyn@valentyn-VirtualBox:~$ sudo wireshark
[sudo] пароль до valentyn:
** (wireshark:3214) 16:56:21.197986 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'

```

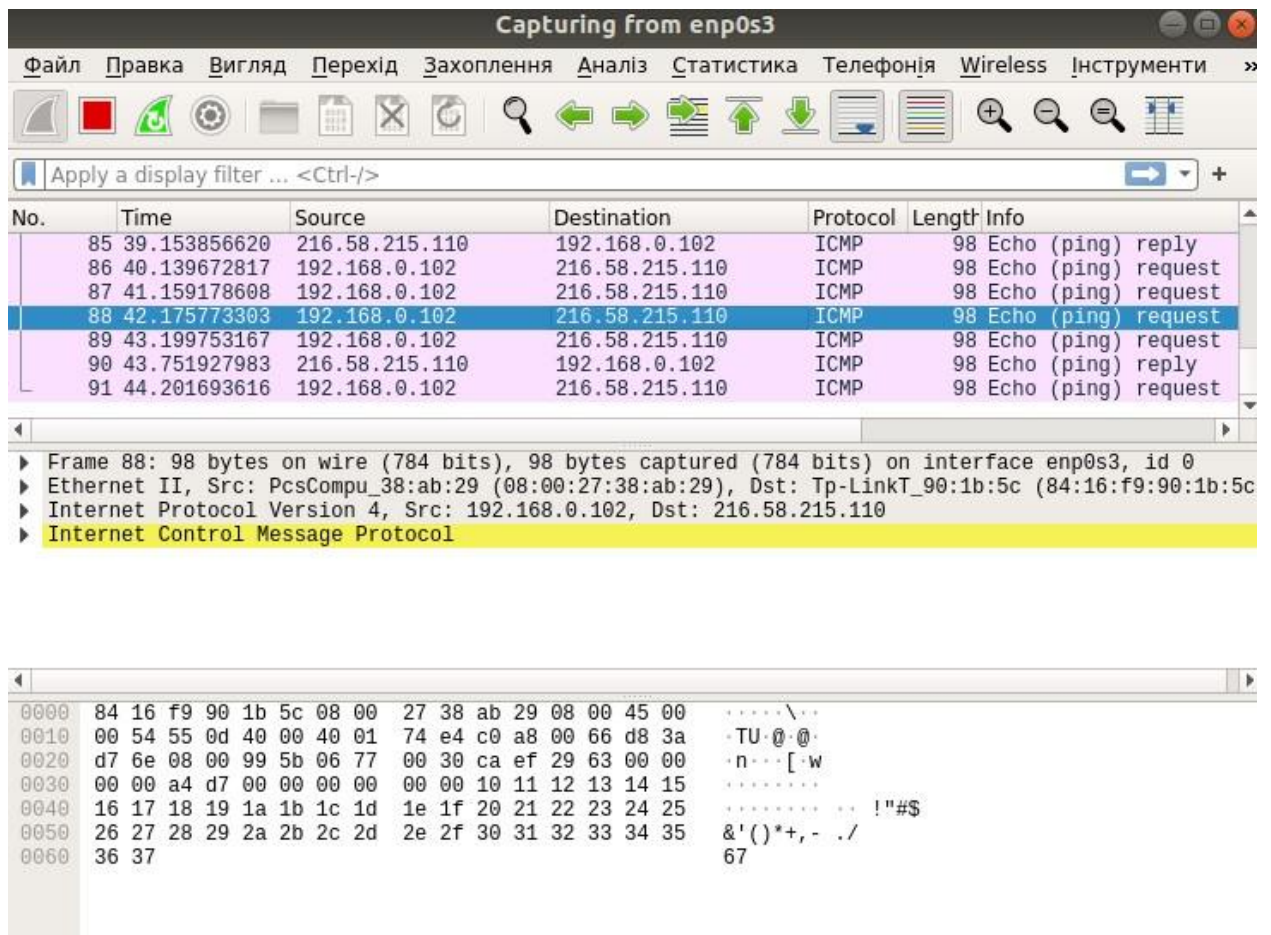



Для захоплення пакетів, оберемо бажаний інтерфейс та натискаємо на піктограму Почати захоплення пакетів.

В іншому терміналі вводимо `$ ping google.com` та відстежуємо трафік, який передається через обраний інтерфейс – захоплення пакетів програмою Wireshark:



Тепер можна виділити будь-який пакет та переглянути детальну інформацію:



Щоб припинити роботу сніфера, необхідно натиснути на червону піктограму:

***enp0s3**

Файл Правка Вигляд Перехід Захоплення Аналіз Статистика Телефонія Wireless Інструменти

Apply a display filter ... <Ctrl-/>

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|----------------|-----------------|----------|--------|------------------|
| 131 | 59.324351925 | 192.168.0.102 | 216.58.215.110 | ICMP | 98 | Echo (ping) requ |
| 132 | 59.396443824 | 216.58.215.110 | 192.168.0.102 | ICMP | 98 | Echo (ping) repl |
| 133 | 59.455782696 | 192.168.0.108 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/ |
| 134 | 59.678103820 | 216.58.215.110 | 192.168.0.102 | ICMP | 98 | Echo (ping) repl |
| 135 | 59.824445639 | 216.58.215.110 | 192.168.0.102 | ICMP | 98 | Echo (ping) repl |
| 136 | 60.325453734 | 192.168.0.102 | 216.58.215.110 | ICMP | 98 | Echo (ping) requ |
| 137 | 60.341827217 | 216.58.215.110 | 192.168.0.102 | ICMP | 98 | Echo (ping) repl |
| 138 | 61.327374015 | 192.168.0.102 | 216.58.215.110 | ICMP | 98 | Echo (ping) requ |

Frame 88: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s3, id 0

Ethernet II, Src: PcsCompu_38:ab:29 (08:00:27:38:ab:29), Dst: Tp-LinkT_90:1b:5c (84:16:f9:90:1b:5c)

Internet Protocol Version 4, Src: 192.168.0.102, Dst: 216.58.215.110

Internet Control Message Protocol

```

0000  84 16 f9 90 1b 5c 08 00 27 38 ab 29 08 00 45 00  ....\..
0010  00 54 55 0d 40 00 40 01 74 e4 c0 a8 00 66 d8 3a  .TU.@.@.
0020  d7 6e 08 00 99 5b 06 77 00 30 ca ef 29 63 00 00  .n...[.w
0030  00 00 a4 d7 00 00 00 00 00 00 10 11 12 13 14 15  ....
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  .....! "$
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,-./
0060  36 37                                     67

```

Приклад роботи фільтра по протоколу (SSDP):

enp0s3

Файл Правка Вигляд Перехід Захоплення Аналіз Статистика Телефонія Wireless Інструменти

ssdp

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|---------------|-----------------|----------|--------|---------------------|
| 121 | 56.452423825 | 192.168.0.108 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 124 | 57.453647844 | 192.168.0.108 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 128 | 58.455425497 | 192.168.0.108 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 133 | 59.455782696 | 192.168.0.108 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |

Frame 121: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface enp0s3, id 0

Ethernet II, Src: IntelCor_84:8f:00 (98:3b:8f:84:8f:00), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)

Internet Protocol Version 4, Src: 192.168.0.108, Dst: 239.255.255.250

User Datagram Protocol, Src Port: 63358, Dst Port: 1900

Simple Service Discovery Protocol

```

0000  01 00 5e 7f ff fa 98 3b 8f 84 8f 00 08 00 45 00  ..^....;
0010  00 cb c7 43 00 00 01 11 40 d0 c0 a8 00 6c ef ff  ...C....
0020  ff fa f7 7e 07 6c 00 b7 e4 0c 4d 2d 53 45 41 52  ...~.l...M-
0030  43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48  CH * HTTP/
0040  4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35  OST: 239 .
0050  2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20  .250:1900MAN:
0060  22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d  "ssdp:di
0070  0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75 72 6e 3a  -MX: 1..ST:
0080  64 69 61 6c 2d 6d 75 6c 74 69 73 63 72 65 65 6e  dial-mult
0090  2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 64 69 61  -org:ser

```

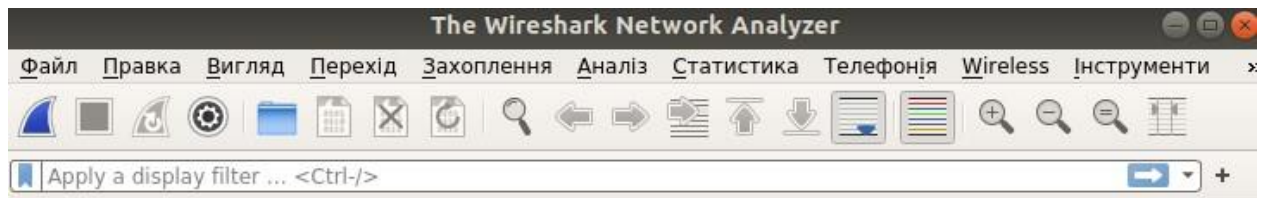
Виводимо арп таблицю, попередньо очистивши історію:


```
valentyn@valentyn-VirtualBox: ~
Файл Зміни Перегляд Пошук Термінал Довідка
ation="profile_load" profile="unconfined" name="man_groff" pid=477 comm="apparmor_parser"
[ 19.667608] audit: type=1400 audit(1663692340.376:9): apparmor="STATUS" operation="profile_load" profile="unconfined" name="libreoffice-oopslash" pid=478 comm="apparmor_parser"
[ 19.674707] audit: type=1400 audit(1663692340.384:10): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/bin/evince" pid=475 comm="apparmor_parser"
[ 19.674710] audit: type=1400 audit(1663692340.384:11): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/bin/evince//sanitized_helper" pid=475 comm="apparmor_parser"
[ 28.010800] e1000: enp0s3 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: RX
[ 28.011134] IPv6: ADDRCONF(NETDEV_CHANGE): enp0s3: link becomes ready
[ 31.142073] systemd-journald[283]: File /var/log/journal/8a6df9cf23c344e5abef18726c29d635/user-1000.journal corrupted or uncleanly shut down, renaming and replacing.
[ 54.277703] rfkill: input handler disabled
[ 116.950446] device enp0s3 entered promiscuous mode
[ 137.925892] device enp0s3 left promiscuous mode
[ 383.497969] device enp0s3 entered promiscuous mode
[ 449.572509] device enp0s3 left promiscuous mode
valentyn@valentyn-VirtualBox:~$ sudo dmesg
valentyn@valentyn-VirtualBox:~$ sudo dmesg
valentyn@valentyn-VirtualBox:~$ arp -a
gateway (192.168.0.1) у 84:16:f9:90:1b:5c [ether] на enp0s3
```

Виводимо список доступних мережевих інтерфейсів (Локальна ір-адреса – 127.0.0.1):

```
valentyn@valentyn-VirtualBox: ~
Файл Зміни Перегляд Пошук Термінал Довідка
valentyn@valentyn-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:38:ab:29 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.102/24 brd 192.168.0.255 scope global dynamic noprefixroute enp0s3
        valid_lft 6638sec preferred_lft 6638sec
    inet6 fe80::70cd:b797:217e:5e31/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Запускаємо сніфер та обираємо інтерфейс:



Welcome to Wireshark

Capture

...using this filter: All interfaces shown ▾

| | |
|---|---|
| enp0s3 | ⌵ |
| any | ⌵ |
| Loopback: lo | — |
| usbmon1 | — |
| ⊗ Cisco remote capture: ciscodump | — |
| ⊗ DisplayPort AUX channel monitor capture: dpauxmon | — |
| ⊗ Random packet generator: randpkt | — |
| ⊗ systemd Journal Export: sdjournal | — |
| ⊗ SSH remote capture: sshdump | — |
| ⊗ UDP Listener remote capture: udpdump | — |

Learn

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

You are running Wireshark 3.6.5 (Git v3.6.5 packaged as 3.6.5-1~ubuntu18.04.0+wiresharkdevstable).



Пінгуємо іншу машину (в моєму випадку планшет)

```

valentyn@valentyn-VirtualBox: ~
Файл Зміни Перегляд Пошук Термінал Довідка
valentyn@valentyn-VirtualBox:~$ ping 192.168.0.103
PING 192.168.0.103 (192.168.0.103) 56(84) bytes of data.
64 bytes from 192.168.0.103: icmp_seq=1 ttl=64 time=72.6 ms
64 bytes from 192.168.0.103: icmp_seq=2 ttl=64 time=258 ms
64 bytes from 192.168.0.103: icmp_seq=3 ttl=64 time=175 ms
64 bytes from 192.168.0.103: icmp_seq=4 ttl=64 time=42.9 ms
64 bytes from 192.168.0.103: icmp_seq=5 ttl=64 time=148 ms
64 bytes from 192.168.0.103: icmp_seq=6 ttl=64 time=75.2 ms
64 bytes from 192.168.0.103: icmp_seq=7 ttl=64 time=330 ms
64 bytes from 192.168.0.103: icmp_seq=8 ttl=64 time=116 ms

```

Перехоплюємо пакети:

Світловий перехід

Файл Правка Вигляд Перехід Захоплення Аналіз Статистика Телефонія Wireless Інструменти »

Apply a display filter ... <Ctrl-/>

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|---------------|---------------|----------|--------|---------------------|
| 28 | 13.211032640 | 192.168.0.103 | 192.168.0.102 | ICMP | 98 | Echo (ping) reply |
| 29 | 14.034279004 | 192.168.0.102 | 192.168.0.103 | ICMP | 98 | Echo (ping) request |
| 30 | 14.656967315 | 192.168.0.103 | 192.168.0.102 | ICMP | 98 | Echo (ping) reply |
| 31 | 15.035552641 | 192.168.0.102 | 192.168.0.103 | ICMP | 98 | Echo (ping) request |
| 32 | 15.662970256 | 192.168.0.103 | 192.168.0.102 | ICMP | 98 | Echo (ping) reply |
| 33 | 16.036897454 | 192.168.0.102 | 192.168.0.103 | ICMP | 98 | Echo (ping) request |
| 34 | 16.051371194 | 192.168.0.103 | 192.168.0.102 | ICMP | 98 | Echo (ping) reply |

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s3, id 0
 Ethernet II, Src: PcsCompu_38:ab:29 (08:00:27:38:ab:29), Dst: Apple_26:7f:ec (34:ab:37:26:7f:ec)
 Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.103
 Internet Control Message Protocol

| | | | | | | | | | | | | | | | | | |
|------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|------------|
| 0000 | 34 | ab | 37 | 26 | 7f | ec | 08 | 00 | 27 | 38 | ab | 29 | 08 | 00 | 45 | 00 | 4.7&... |
| 0010 | 00 | 54 | 34 | ab | 40 | 00 | 40 | 01 | 83 | e0 | c0 | a8 | 00 | 66 | c0 | a8 | ·T4·@·@· |
| 0020 | 00 | 67 | 08 | 00 | 4e | 18 | 06 | c7 | 00 | 1d | f5 | f0 | 29 | 63 | 00 | 00 | ·g·N· |
| 0030 | 00 | 00 | c3 | dc | 01 | 00 | 00 | 00 | 00 | 00 | 10 | 11 | 12 | 13 | 14 | 15 | |
| 0040 | 16 | 17 | 18 | 19 | 1a | 1b | 1c | 1d | 1e | 1f | 20 | 21 | 22 | 23 | 24 | 25 | !"# |
| 0050 | 26 | 27 | 28 | 29 | 2a | 2b | 2c | 2d | 2e | 2f | 30 | 31 | 32 | 33 | 34 | 35 | &'()*+,-./ |
| 0060 | 36 | 37 | | | | | | | | | | | | | | | 67 |

enp0s3: <live capture in progress> Packets: 34 · Displayed: 34 (100.0%) Profile: Default

Capturing from enp0s3

Файл Правка Вигляд Перехід Захоплення Аналіз Статистика Телефонія Wireless Інструменти

Apply a display filter ... <Ctrl-/>

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|-------------------|---------------|----------|--------|-----------------------|
| 115 | 52.131946899 | 192.168.0.102 | 192.168.0.103 | ICMP | 98 | Echo (ping) request |
| 116 | 52.327129685 | 192.168.0.103 | 192.168.0.102 | ICMP | 98 | Echo (ping) reply |
| 117 | 53.025970962 | Tp-LinkT_90:1b:5c | Broadcast | ARP | 60 | Who has 192.168.0.103 |
| 118 | 53.134150119 | 192.168.0.102 | 192.168.0.103 | ICMP | 98 | Echo (ping) request |
| 119 | 53.439853854 | 192.168.0.103 | 192.168.0.102 | ICMP | 98 | Echo (ping) reply |
| 120 | 54.049868687 | Tp-LinkT_90:1b:5c | Broadcast | ARP | 60 | Who has 192.168.0.103 |
| 121 | 54.135084301 | 192.168.0.102 | 192.168.0.103 | ICMP | 98 | Echo (ping) request |

Frame 83: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s3, id 0

Ethernet II, Src: PcsCompu_38:ab:29 (08:00:27:38:ab:29), Dst: Apple_26:7f:ec (34:ab:37:26:7f:ec)

Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.103

Internet Control Message Protocol

```

0000  34 ab 37 26 7f ec 08 00 27 38 ab 29 08 00 45 00  4·7&····
0010  00 54 47 99 40 00 40 01 70 f2 c0 a8 00 66 c0 a8  ·TG·@·@·
0020  00 67 08 00 50 c6 06 c7 00 41 19 f1 29 63 00 00  ·g·P····
0030  00 00 9b 0a 03 00 00 00 00 00 10 11 12 13 14 15  ······
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  ······ !"#
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,-./
0060  36 37 67

```

enp0s3: <live capture in progress> Packets: 121 · Displayed: 121 (100.0%) Profile: Default

Right Ctrl

Зупиняємо перехоплення та додаємо фільтр по протоколам ARP:

*enp0s3

Файл Правка Вигляд Перехід Захоплення Аналіз Статистика Телефонія Wireless Інструменти

arp

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|-------------------|-------------------|----------|--------|------------------|
| 54 | 25.093918834 | PcsCompu_38:ab:29 | Apple_26:7f:ec | ARP | 42 | Who has 192.168. |
| 55 | 25.486088438 | Apple_26:7f:ec | PcsCompu_38:ab:29 | ARP | 60 | 192.168.0.103 1s |
| 59 | 26.709202930 | Tp-LinkT_90:1b:5c | Broadcast | ARP | 60 | Who has 192.168. |
| 62 | 27.734477317 | Tp-LinkT_90:1b:5c | Broadcast | ARP | 60 | Who has 192.168. |
| 65 | 28.654722314 | Tp-LinkT_90:1b:5c | Broadcast | ARP | 60 | Who has 192.168. |
| 76 | 33.979438102 | Tp-LinkT_90:1b:5c | Broadcast | ARP | 60 | Who has 192.168. |
| 79 | 35.006633960 | Tp-LinkT_90:1b:5c | Broadcast | ARP | 60 | Who has 192.168. |
| 82 | 36.027301332 | Tp-LinkT_90:1b:5c | Broadcast | ARP | 60 | Who has 192.168. |

▶ Frame 55: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface enp0s3, id 0
 ▶ Ethernet II, Src: Apple_26:7f:ec (34:ab:37:26:7f:ec), Dst: PcsCompu_38:ab:29 (08:00:27:38:ab:29)
 ▶ Address Resolution Protocol (reply)

```

0000  08 00 27 38 ab 29 34 ab 37 26 7f ec 08 06 00 01  ..'8.)4.
0010  08 00 06 04 00 02 34 ab 37 26 7f ec c0 a8 00 67  ....4.
0020  08 00 27 38 ab 29 c0 a8 00 66 00 00 00 00 00 00  ..'8.)...
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....
  
```

QA завдання:

Переконайтеся в отриманні MAC-адреси по відомій IP-адресі.

Отримуємо пристрій:

```

valentyn@valentyn-VirtualBox:~$ arp -a
_gateway (192.168.0.1) y 84:16:f9:90:1b:5c [ether] на enp0s3
? (192.168.0.103) y 34:ab:37:26:7f:ec [ether] на enp0s3
valentyn@valentyn-VirtualBox:~$
  
```

Перевіряємо мак адрес пристрою:

| | |
|--------------|-------------------|
| Адреса Wi-Fi | 34:AB:37:26:7F:EC |
|--------------|-------------------|

Мак адреси співпали.

Переконайтеся в тому, що arp-таблиця оновлюється при отриманні arp-reply:

До пінгування смартфона в таблицю була відсутня будь-яка інформація, а записи з MAC-адресою з'явилися тільки після процесу пінгування, що і дозволяє нам в цьому переконатися.

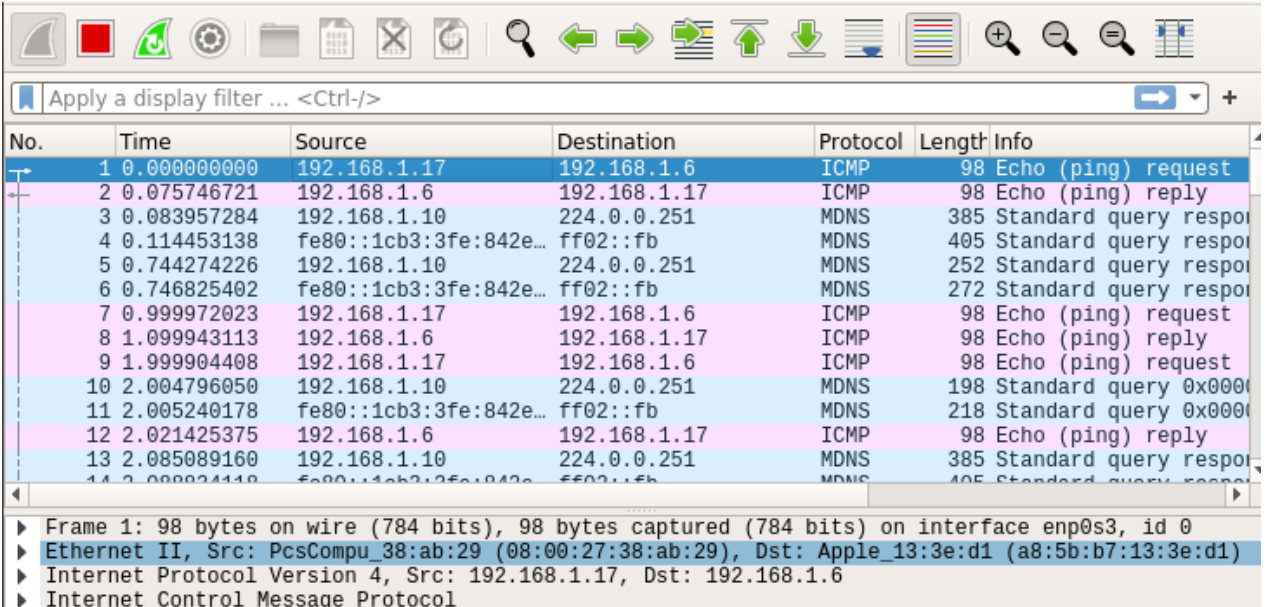
Додати статичний запис у arp-таблицю та після цього пропінгувати інший пристрій, при цьому відстежувати трафік у wireshark.

(виконання цього пункту проводиться з іншим телефоном і вже в іншій мережі)

```
valentyn@valentyn-VirtualBox:~$ arp -a
_gateway (192.168.1.1) у 64:ee:b7:ee:d1:49 [ether] на enp0s3
valentyn@valentyn-VirtualBox:~$ sudo arp -s 192.168.1.6 a8:5b:b7:13:3e:d1
[sudo] пароль до valentyn:
valentyn@valentyn-VirtualBox:~$ arp -a
_gateway (192.168.1.1) у 64:ee:b7:ee:d1:49 [ether] на enp0s3
? (192.168.1.6) у a8:5b:b7:13:3e:d1 [ether] PERM на enp0s3
valentyn@valentyn-VirtualBox:~$
```

Пінгуємо телефон:

```
valentyn@valentyn-VirtualBox:~$ ping 192.168.1.6
PING 192.168.1.6 (192.168.1.6) 56(84) bytes of data.
64 bytes from 192.168.1.6: icmp_seq=1 ttl=64 time=282 ms
64 bytes from 192.168.1.6: icmp_seq=2 ttl=64 time=102 ms
64 bytes from 192.168.1.6: icmp_seq=3 ttl=64 time=23.8 ms
64 bytes from 192.168.1.6: icmp_seq=4 ttl=64 time=45.8 ms
64 bytes from 192.168.1.6: icmp_seq=5 ttl=64 time=67.3 ms
64 bytes from 192.168.1.6: icmp_seq=6 ttl=64 time=88.4 ms
64 bytes from 192.168.1.6: icmp_seq=7 ttl=64 time=111 ms
64 bytes from 192.168.1.6: icmp_seq=8 ttl=64 time=35.0 ms
64 bytes from 192.168.1.6: icmp_seq=9 ttl=64 time=59.4 ms
64 bytes from 192.168.1.6: icmp_seq=10 ttl=64 time=5.73 ms
64 bytes from 192.168.1.6: icmp_seq=11 ttl=64 time=103 ms
```



Wireshark interface showing a packet capture. The top toolbar includes icons for file operations, network analysis, and zooming. Below the toolbar is a filter bar with the text "Apply a display filter ... <Ctrl-/>". The main packet list table displays the following data:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|------------------------|--------------|----------|--------|-------------------------|
| 1 | 0.000000000 | 192.168.1.17 | 192.168.1.6 | ICMP | 98 | Echo (ping) request |
| 2 | 0.075746721 | 192.168.1.6 | 192.168.1.17 | ICMP | 98 | Echo (ping) reply |
| 3 | 0.083957284 | 192.168.1.10 | 224.0.0.251 | MDNS | 385 | Standard query response |
| 4 | 0.114453138 | fe80::1cb3:3fe:842e... | ff02::fb | MDNS | 405 | Standard query response |
| 5 | 0.744274226 | 192.168.1.10 | 224.0.0.251 | MDNS | 252 | Standard query response |
| 6 | 0.746825402 | fe80::1cb3:3fe:842e... | ff02::fb | MDNS | 272 | Standard query response |
| 7 | 0.999972023 | 192.168.1.17 | 192.168.1.6 | ICMP | 98 | Echo (ping) request |
| 8 | 1.099943113 | 192.168.1.6 | 192.168.1.17 | ICMP | 98 | Echo (ping) reply |
| 9 | 1.999904408 | 192.168.1.17 | 192.168.1.6 | ICMP | 98 | Echo (ping) request |
| 10 | 2.004796050 | 192.168.1.10 | 224.0.0.251 | MDNS | 198 | Standard query 0x0000 |
| 11 | 2.005240178 | fe80::1cb3:3fe:842e... | ff02::fb | MDNS | 218 | Standard query 0x0000 |
| 12 | 2.021425375 | 192.168.1.6 | 192.168.1.17 | ICMP | 98 | Echo (ping) reply |
| 13 | 2.085089160 | 192.168.1.10 | 224.0.0.251 | MDNS | 385 | Standard query response |
| 14 | 2.088024410 | fe80::1cb3:3fe:842e... | ff02::fb | MDNS | 405 | Standard query response |

Below the packet list, the packet details pane shows the following information for the selected packet (Frame 1):

- Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s3, id 0
- Ethernet II, Src: PcsCompu_38:ab:29 (08:00:27:38:ab:29), Dst: Apple_13:3e:d1 (a8:5b:b7:13:3e:d1)
- Internet Protocol Version 4, Src: 192.168.1.17, Dst: 192.168.1.6
- Internet Control Message Protocol

Test Case за варіантом:

Варіант: $10 \bmod 3 = 1$ (Переконатися в тому, що arp-таблиця оновлюється при отриманні arp-reply.)

Setup Description:

PC ----- WI-FI ----- Mb

PC: 192.168.1.1

Mb: 192.168.1.6

Steps:

1. Clean arp table: `arp -d ER`: verify that value for Mb is absent
2. Run Wireshark for Wi-Fi
3. Verify that ARP table is clear.
4. Run ping from PC to Mb ER: ping is running
5. Verify that ARP table with `arp -a` command MAC was resolve by ARP protocol for Mb and appeared in ARP table
6. Stop pinging process
7. Verify that ARP table with `arp -a` command
8. Check new result of arp table with mobile value

Expected Results

ARP table is successfully updating while getting arp-replies. A static entry with the smartphone IP address and its MAC address was added to the ARP table.

Actual Result

ARP table is successfully updating while getting arp-replies. A static entry with the smartphone IP address and its MAC address was added to the ARP table.

Status

The test was successful.

Висновок:

Під час виконання даної лабораторної роботи мною було вивчено технологію отримання MAC адреси на канальному рівні мережі за відомою IP адресою, розібрано засоби підтримки протоколу ARP на рівні операційної системи, отримано навички переглядати ARP КЕШ, видаляти із нього записи та очищувати. Також мною закріплено навички аналізу мережного трафіка за допомогою програми WireShark.