

Тестування та контроль якості (QA) вбудованих систем
Лабораторна робота 1
Виконав студент групи ІВ-91
Кучеренко Іван

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

```
ivan@ivan-VirtualBox:~$ sudo add-apt-repository ppa:wireshark-dev/stable
[sudo] пароль для ivan:
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
Больше информации: https://launchpad.net/~wireshark-dev/+archive/ubuntu/stable
Нажмите [ENTER] для продолжения или Ctrl-C, чтобы отменить добавление.

Суц:1 http://ua.archive.ubuntu.com/ubuntu focal InRelease
Пол:2 http://ua.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Пол:3 http://ua.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Пол:4 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Пол:5 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu focal InRelease [24,4 kB]
Суц:6 https://repo.skype.com/deb stable InRelease
Пол:7 http://ua.archive.ubuntu.com/ubuntu focal-updates/main i386 Packages [720 kB]
Пол:8 http://ua.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [2.086 kB]
Пол:9 http://ua.archive.ubuntu.com/ubuntu focal-updates/main Translation-en [371 kB]
Пол:10 http://ua.archive.ubuntu.com/ubuntu focal-updates/main amd64 DEP-11 Metadata [520 kB]
Пол:37 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu focal/main amd64 Packages [4.248 B]
Пол:38 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu focal/main Translation-en [1.932 B]
Пол:39 http://security.ubuntu.com/ubuntu focal-security/main Translation-en [288 kB]
Пол:40 http://security.ubuntu.com/ubuntu focal-security/main amd64 DEP-11 Metadata [40,7 kB]
Пол:41 http://security.ubuntu.com/ubuntu focal-security/main amd64 c-n-f Metadata [11,1 kB]
Пол:42 http://security.ubuntu.com/ubuntu focal-security/restricted amd64 Packages [1.175 kB]
Пол:43 http://security.ubuntu.com/ubuntu focal-security/restricted Translation-en [166 kB]
Пол:44 http://security.ubuntu.com/ubuntu focal-security/universe amd64 Packages [721 kB]
Пол:45 http://security.ubuntu.com/ubuntu focal-security/universe i386 Packages [560 kB]
Пол:46 http://security.ubuntu.com/ubuntu focal-security/universe Translation-en [132 kB]
Пол:47 http://security.ubuntu.com/ubuntu focal-security/universe amd64 DEP-11 Metadata [77,3 kB]
Пол:48 http://security.ubuntu.com/ubuntu focal-security/universe amd64 c-n-f Metadata [14,8 kB]
Пол:49 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 DEP-11 Metadata [2.464 B]
Получено 13,2 МВ за 8с (1.570 kB/s)
Чтение списков пакетов... Готово
ivan@ivan-VirtualBox:~$
```

2. Оновлюємо списки пакетів з репозиторіїв для оновлення пакетів:

```
ivan@ivan-VirtualBox:~$ sudo apt-get update
Суц:1 http://ua.archive.ubuntu.com/ubuntu focal InRelease
Суц:2 http://ua.archive.ubuntu.com/ubuntu focal-updates InRelease
Суц:3 http://ua.archive.ubuntu.com/ubuntu focal-backports InRelease
Суц:4 https://repo.skype.com/deb stable InRelease
Пол:5 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Суц:6 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu focal InRelease
Пол:7 http://security.ubuntu.com/ubuntu focal-security/main amd64 DEP-11 Metadata [40,8 kB]
Пол:8 http://security.ubuntu.com/ubuntu focal-security/universe amd64 DEP-11 Metadata [77,5 kB]
Пол:9 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 DEP-11 Metadata [2.464 B]
Получено 235 kB за 2с (106 kB/s)
Чтение списков пакетов... Готово
ivan@ivan-VirtualBox:~$
```

3. Завантажуємо wireshark:

```
ivan@ivan-VirtualBox:~$ sudo apt-get install wireshark
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Будут установлены следующие дополнительные пакеты:
libdouble-conversion3 libminizip1 libpcrc2-16-0 libqt5core5a libqt5dbus5
libqt5gui5 libqt5multimedia5 libqt5multimedia5-plugins
libqt5multimediagsttools5 libqt5multimediawidgets5 libqt5network5
libqt5opengl5 libqt5printsupport5 libqt5svg5 libqt5widgets5 libsmi2ldbl
libsnappy1v5 libspandsp2 libssh-gcrypt-4 libwireshark-data libwireshark15
libwiretap12 libwsutil13 libxcb-xinerama0 libxcb-xinput0
qt5-gtk-platformtheme qttranslations5-l10n wireshark-common wireshark-qt
Предлагаемые пакеты:
qt5-image-formats-plugins qtwayland5 snmp-mibs-downloader geoipupdate
geoip-database geoip-database-extra libjs-leaflet
libjs-leaflet.markercluster wireshark-doc
Следующие НОВЫЕ пакеты будут установлены:
libdouble-conversion3 libminizip1 libpcrc2-16-0 libqt5core5a libqt5dbus5
libqt5gui5 libqt5multimedia5 libqt5multimedia5-plugins
libqt5multimediagsttools5 libqt5multimediawidgets5 libqt5network5
libqt5opengl5 libqt5printsupport5 libqt5svg5 libqt5widgets5 libsmi2ldbl
libsnappy1v5 libspandsp2 libssh-gcrypt-4 libwireshark-data libwireshark15
libwiretap12 libwsutil13 libxcb-xinerama0 libxcb-xinput0
qt5-gtk-platformtheme qttranslations5-l10n wireshark wireshark-common
wireshark-qt
Обновлено 0 пакетов, установлено 30 новых пакетов, для удаления отмечено 0 пакетов, и 483 пакетов не обновлено.
Необходимо скачать 35,3 МВ архивов.
После данной операции объем занятого дискового пространства возрастёт на 177 МВ
```

Настраивается wireshark-common

Dumpcap can be installed in a way that allows members of the "wireshark" system group to capture packets. This is recommended over the alternative of running Wireshark/Tshark directly as root, because less of the code will run with elevated privileges.

For more detailed information please see [/usr/share/doc/wireshark-common/README.Debian.gz](#) once the package is installed.

Enabling this feature may be a security risk, so it is disabled by default. If in doubt, it is suggested to leave it disabled.

Should non-superusers be able to capture packets?

<Да>

<Нет>

Хотите продолжить? [Д/Н] Y

Пол:1 [Пол:2 \[Пол:3 \\[Пол:4 \\\[Пол:5 \\\\[Пол:6 \\\\\[Пол:7 \\\\\\[Пол:8 \\\\\\\[Пол:9 \\\\\\\\[Пол:10 \\\\\\\\\[Пол:11 \\\\\\\\\\[Пол:12 \\\\\\\\\\\[Пол:13 \\\\\\\\\\\\[Пол:14 \\\\\\\\\\\\\[Пол:15\\\\\\\\\\\\\]\\\\\\\\\\\\\(http://ua.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5multimedia5 amd64 5.12.8-0ubuntu1 \\\\\\\\\\\\\[36,8 kB\\\\\\\\\\\\\]</p></div><div data-bbox=\\\\\\\\\\\\\)\\\\\\\\\\\\]\\\\\\\\\\\\(http://ua.archive.ubuntu.com/ubuntu focal-updates/universe amd64 libqt5opengl5 amd64 5.12.8+dfsg-0ubuntu2.1 \\\\\\\\\\\\[136 kB\\\\\\\\\\\\]</p></div><div data-bbox=\\\\\\\\\\\\)\\\\\\\\\\\]\\\\\\\\\\\(http://ua.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5multimedia5 amd64 5.12.8-0ubuntu1 \\\\\\\\\\\[283 kB\\\\\\\\\\\]</p></div><div data-bbox=\\\\\\\\\\\)\\\\\\\\\\]\\\\\\\\\\(http://ua.archive.ubuntu.com/ubuntu focal/universe amd64 libminizip1 amd64 1.1-8build1 \\\\\\\\\\[20,2 kB\\\\\\\\\\]</p></div><div data-bbox=\\\\\\\\\\)\\\\\\\\\]\\\\\\\\\(http://ua.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5svg5 amd64 5.12.8-0ubuntu1 \\\\\\\\\[131 kB\\\\\\\\\]</p></div><div data-bbox=\\\\\\\\\)\\\\\\\\]\\\\\\\\(http://ua.archive.ubuntu.com/ubuntu focal-updates/universe amd64 libqt5widgets5 amd64 5.12.8+dfsg-0ubuntu2.1 \\\\\\\\[2.295 kB\\\\\\\\]</p></div><div data-bbox=\\\\\\\\)\\\\\\\]\\\\\\\(http://ua.archive.ubuntu.com/ubuntu focal-updates/universe amd64 libqt5gui5 amd64 5.12.8+dfsg-0ubuntu2.1 \\\\\\\[2.971 kB\\\\\\\]</p></div><div data-bbox=\\\\\\\)\\\\\\]\\\\\\(http://ua.archive.ubuntu.com/ubuntu focal/main amd64 libxcb-xinput0 amd64 1.14-2 \\\\\\[29,3 kB\\\\\\]</p></div><div data-bbox=\\\\\\)\\\\\]\\\\\(http://ua.archive.ubuntu.com/ubuntu focal/main amd64 libxcb-xinerama0 amd64 1.14-2 \\\\\[5.260 B\\\\\]</p></div><div data-bbox=\\\\\)\\\\]\\\\(http://ua.archive.ubuntu.com/ubuntu focal-updates/universe amd64 libqt5network5 amd64 5.12.8+dfsg-0ubuntu2.1 \\\\[673 kB\\\\]</p></div><div data-bbox=\\\\)\\\]\\\(http://ua.archive.ubuntu.com/ubuntu focal-updates/universe amd64 libqt5dbus5 amd64 5.12.8+dfsg-0ubuntu2.1 \\\[208 kB\\\]</p></div><div data-bbox=\\\)\\]\\(http://ua.archive.ubuntu.com/ubuntu focal-updates/universe amd64 libqt5core5a amd64 5.12.8+dfsg-0ubuntu2.1 \\[2.006 kB\\]</p></div><div data-bbox=\\)\]\(http://ua.archive.ubuntu.com/ubuntu focal/main amd64 libpcre2-16-0 amd64 10.34-7 \[181 kB\]</p></div><div data-bbox=\)](http://ua.archive.ubuntu.com/ubuntu focal/universe amd64 libdouble-conversion3 amd64 3.1.5-4ubuntu1 [37,9 kB]</p></div><div data-bbox=)

```

Настраивается пакет libqt5core5a:amd64 (5.12.8+dfsg-0ubuntu2.1) ...
Настраивается пакет libwireshark-data (3.6.5-1~ubuntu20.04.0+wiresharkdevstable) ...
Настраивается пакет libqt5dbus5:amd64 (5.12.8+dfsg-0ubuntu2.1) ...
Настраивается пакет libqt5network5:amd64 (5.12.8+dfsg-0ubuntu2.1) ...
Настраивается пакет libwireshark15:amd64 (3.6.5-1~ubuntu20.04.0+wiresharkdevstable) ...
Настраивается пакет wireshark-common (3.6.5-1~ubuntu20.04.0+wiresharkdevstable) ...
Настраивается пакет libqt5gui5:amd64 (5.12.8+dfsg-0ubuntu2.1) ...
Настраивается пакет libqt5widgets5:amd64 (5.12.8+dfsg-0ubuntu2.1) ...
Настраивается пакет qt5-gtk-platformtheme:amd64 (5.12.8+dfsg-0ubuntu2.1) ...
Настраивается пакет libqt5multimedia5:amd64 (5.12.8-0ubuntu1) ...
Настраивается пакет libqt5sprintsupport5:amd64 (5.12.8+dfsg-0ubuntu2.1) ...
Настраивается пакет libqt5opengl5:amd64 (5.12.8+dfsg-0ubuntu2.1) ...
Настраивается пакет libqt5svg5:amd64 (5.12.8-0ubuntu1) ...
Настраивается пакет libqt5multimediawidgets5:amd64 (5.12.8-0ubuntu1) ...
Настраивается пакет wireshark-qt (3.6.5-1~ubuntu20.04.0+wiresharkdevstable) ...
Настраивается пакет libqt5multimediagsttools5:amd64 (5.12.8-0ubuntu1) ...
Настраивается пакет libqt5multimedia5-plugins:amd64 (5.12.8-0ubuntu1) ...
Настраивается пакет wireshark (3.6.5-1~ubuntu20.04.0+wiresharkdevstable) ...
Обрабатываются триггеры для libc-bin (2.31-0ubuntu9) ...
Обрабатываются триггеры для man-db (2.9.1-1) ...
Обрабатываются триггеры для shared-mime-info (1.15-1) ...
Обрабатываются триггеры для desktop-file-utils (0.24-1ubuntu3) ...
Обрабатываются триггеры для mime-support (3.64ubuntu1) ...
Обрабатываются триггеры для hicolor-icon-theme (0.17-2) ...
Обрабатываются триггеры для gnome-menus (3.36.0-1ubuntu1) ...
ivan@ivan-VirtualBox:~$

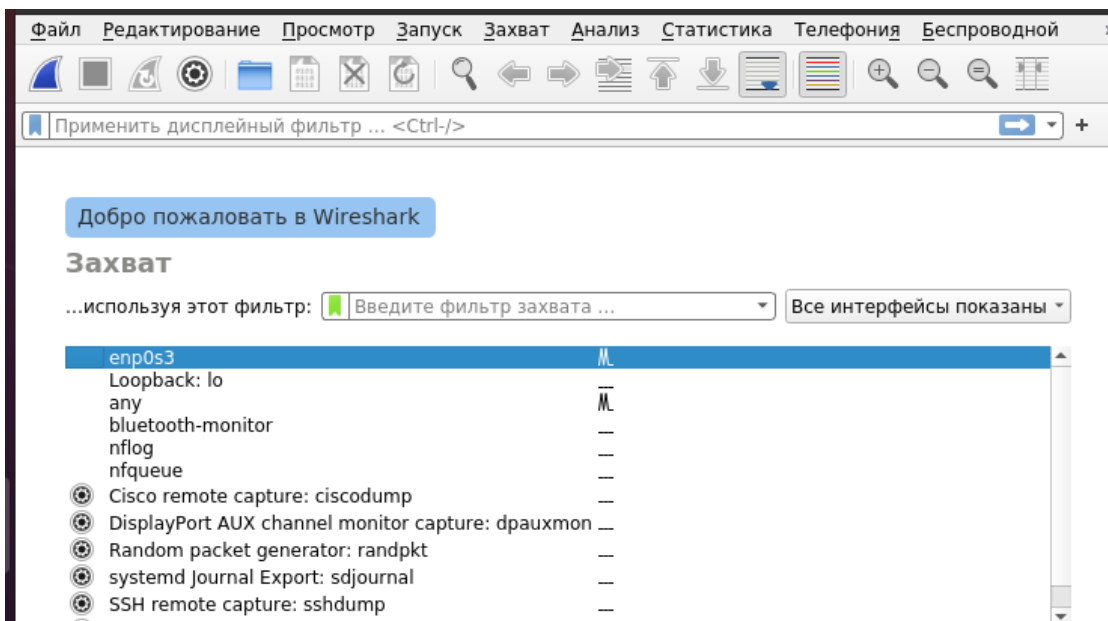
```

4. Запускаємо wireshark:

```

ivan@ivan-VirtualBox:~$ sudo wireshark
** (wireshark:6977) 16:34:04.043641 [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:

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной							
Применить дисплейный фильтр ... <Ctrl-/>							
No.	Time	Source	Destination	Protocol	Length	Info	
39	20.114491319	216.58.215.106	10.0.2.15	UDP	70	443 → 50499	Len=28
40	21.028978338	10.0.2.15	142.250.75.14	ICMP	98	Echo (ping) request	
41	21.047022547	142.250.75.14	10.0.2.15	ICMP	98	Echo (ping) reply	
42	22.030176372	10.0.2.15	142.250.75.14	ICMP	98	Echo (ping) request	
43	22.047501681	142.250.75.14	10.0.2.15	ICMP	98	Echo (ping) reply	
44	23.031251231	10.0.2.15	142.250.75.14	ICMP	98	Echo (ping) request	
45	23.052874061	142.250.75.14	10.0.2.15	ICMP	98	Echo (ping) reply	

▶ Frame 1: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface enp0s3, id 0
 ▶ Ethernet II, Src: PcsCompu_52:25:98 (08:00:27:52:25:98), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
 ▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 216.58.215.106
 ▶ User Datagram Protocol, Src Port: 50499, Dst Port: 443
 ▶ Data (29 bytes)

0000	52 54 00 12 35 02 08 00	27 52 25 98 08 00 45 00	RT..5... 'R%...E.
0010	00 39 00 00 40 00 40 11	7f 00 0a 00 02 0f d8 3a	·9·@·@·:
0020	d7 6a c5 43 01 bb 00 25	bb ea 6d 73 6e 25 e0 6c	·j·C...% ··msn%·l
0030	33 94 95 c5 f0 cd 5e 96	cd c0 65 0d 59 52 d0 b8	3.....^...·e·YR·
0040	33 8b a7 90 9f a8 ce		3.....

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

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной							
Применить дисплейный фильтр ... <Ctrl-/>							
No.	Time	Source	Destination	Protocol	Length	Info	
1320	91.135603743	10.0.2.15	142.250.75.14	ICMP	98	Echo (ping) request	
1321	91.152789550	142.250.75.14	10.0.2.15	ICMP	98	Echo (ping) reply	
1322	92.137504867	10.0.2.15	142.250.75.14	ICMP	98	Echo (ping) request	
1323	92.154654962	142.250.75.14	10.0.2.15	ICMP	98	Echo (ping) reply	
1324	92.720563618	142.250.203.206	10.0.2.15	UDP	81	443 → 33691 Len=39	
1325	92.720563842	142.250.203.206	10.0.2.15	UDP	235	443 → 33691 Len=193	
1326	92.721221778	10.0.2.15	142.250.203.206	UDP	75	33691 → 443 Len=33	

▶ Frame 1322: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s3, id 0
 ▶ Ethernet II, Src: PcsCompu_52:25:98 (08:00:27:52:25:98), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
 ▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 142.250.75.14
 ▶ Internet Control Message Protocol

0000	52 54 00 12 35 02 08 00	27 52 25 98 08 00 45 00	RT..5... 'R%...E.
0010	00 54 7a 36 40 00 40 01	da 5b 0a 00 02 0f 8e fa	·Tz6@·@· [.....
0020	4b 0e 08 00 b8 32 00 01	00 4a df 70 28 63 00 00	K...·2... ·J·p(c·
0030	00 00 77 db 01 00 00 00	00 00 10 11 12 13 14 15	··w.....
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	&'()*+,-./012345
0060	36 37		67

Щоб припинити захоплення пакетів, необхідно натиснути на червону піктограму:

Применить дисплейный фильтр ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
3267	258.641875245	142.250.203.206	10.0.2.15	UDP	71	443 → 33691 Len=
3268	258.642979236	10.0.2.15	142.250.203.206	UDP	74	33691 → 443 Len=
3269	258.660946284	142.250.203.206	10.0.2.15	UDP	71	443 → 33691 Len=
3270	259.391465912	10.0.2.15	142.250.75.14	ICMP	98	Echo (ping) requ
3271	259.410344716	142.250.75.14	10.0.2.15	ICMP	98	Echo (ping) repl
3272	260.392828154	10.0.2.15	142.250.75.14	ICMP	98	Echo (ping) requ
3273	260.410093185	142.250.75.14	10.0.2.15	ICMP	98	Echo (ping) repl

Frame 1322: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s3, id 0
 Ethernet II, Src: PcsCompu_52:25:98 (08:00:27:52:25:98), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
 Internet Protocol Version 4, Src: 10.0.2.15, Dst: 142.250.75.14
 Internet Control Message Protocol

0000 52 54 00 12 35 02 08 00 27 52 25 98 08 00 45 00 RT..5... 'R%...E.
 0010 00 54 7a 36 40 00 40 01 da 5b 0a 00 02 0f 8e fa .Tz6@.@.[.....
 0020 4b 0e 08 00 b8 32 00 01 00 4a df 70 28 63 00 00 K...2... J.p(c..
 0030 00 00 77 db 01 00 00 00 00 00 10 11 12 13 14 15 ..w.....
 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 &'()*+,-./012345
 0060 36 37 67

Приклад фільтрів по протоколу:

icmp

No.	Time	Source	Destination	Protocol	Length	Info
1157	88.149145248	142.250.75.14	10.0.2.15	ICMP	98	Echo (ping) repl
1198	89.133569017	10.0.2.15	142.250.75.14	ICMP	98	Echo (ping) requ
1199	89.152548633	142.250.75.14	10.0.2.15	ICMP	98	Echo (ping) repl
1318	90.135265781	10.0.2.15	142.250.75.14	ICMP	98	Echo (ping) requ
1319	90.152390371	142.250.75.14	10.0.2.15	ICMP	98	Echo (ping) repl
1320	91.135603743	10.0.2.15	142.250.75.14	ICMP	98	Echo (ping) requ
1321	91.152789550	142.250.75.14	10.0.2.15	ICMP	98	Echo (ping) repl

Frame 1322: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s3, id 0
 Ethernet II, Src: PcsCompu_52:25:98 (08:00:27:52:25:98), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
 Internet Protocol Version 4, Src: 10.0.2.15, Dst: 142.250.75.14
 Internet Control Message Protocol

0000 52 54 00 12 35 02 08 00 27 52 25 98 08 00 45 00 RT..5... 'R%...E.
 0010 00 54 7a 36 40 00 40 01 da 5b 0a 00 02 0f 8e fa .Tz6@.@.[.....
 0020 4b 0e 08 00 b8 32 00 01 00 4a df 70 28 63 00 00 K...2... J.p(c..
 0030 00 00 77 db 01 00 00 00 00 00 10 11 12 13 14 15 ..w.....
 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 &'()*+,-./012345
 0060 36 37 67

Виводимо arp таблицю, попередньо очистивши історію:

```
[ 1793.387559] device enp0s3 left promiscuous mode
[ 7679.888396] loop0: detected capacity change from 0 to 94056
[ 7694.755474] audit: type=1400 audit(1663617369.187:55): apparmor="STATUS" operation="profile_replace" info="same as current profile, skipping" profile="unconfined" name="/snap/snapd/16778/usr/lib/snapd/snap-confine" pid=9078 comm="apparmor_parser"
[ 7694.755484] audit: type=1400 audit(1663617369.187:56): apparmor="STATUS" operation="profile_replace" info="same as current profile, skipping" profile="unconfined" name="/snap/snapd/16778/usr/lib/snapd/snap-confine//mount-namespace-capture-helper" pid=9078 comm="apparmor_parser"
[ 7700.370928] audit: type=1400 audit(1663617374.803:57): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap-update-ns.snap-store" pid=9080 comm="apparmor_parser"
[ 7701.722968] audit: type=1400 audit(1663617376.155:58): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.hook.config" pid=9083 comm="apparmor_parser"
[ 7705.951868] audit: type=1400 audit(1663617380.383:59): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.snap-store" pid=9084 comm="apparmor_parser"
[ 7710.174772] audit: type=1400 audit(1663617384.607:60): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.ubuntu-soft" pid=9085 comm="apparmor_parser"
[ 7714.402572] audit: type=1400 audit(1663617388.835:61): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.ubuntu-soft" pid=9086 comm="apparmor_parser"
ivan@ivan-VirtualBox:~$ dmesg
ivan@ivan-VirtualBox:~$ arp -a
_gateway (10.0.2.2) в 52:54:00:12:35:02 [ether] на enp0s3
ivan@ivan-VirtualBox:~$
```

Робимо підключення до мережі з іншим пристроєм (в моєму випадку це WI-FI та мобільний телефон), виводимо інформацію:

```
ivan@ivan-VirtualBox:~$ dmesg
ivan@ivan-VirtualBox:~$ arp -a
_gateway (10.0.2.2) в 52:54:00:12:35:02 [ether] на enp0s3
ivan@ivan-VirtualBox:~$ sudo dmesg
ivan@ivan-VirtualBox:~$ sudo dmesg
ivan@ivan-VirtualBox:~$ sudo dmesg
ivan@ivan-VirtualBox:~$ sudo dmesg
[19214.292607] e1000: enp0s3 NIC Link is Down
[19218.324211] e1000: enp0s3 NIC Link is Up 1000 Mbps Full Duplex, Flow Control
: RX
ivan@ivan-VirtualBox:~$
```

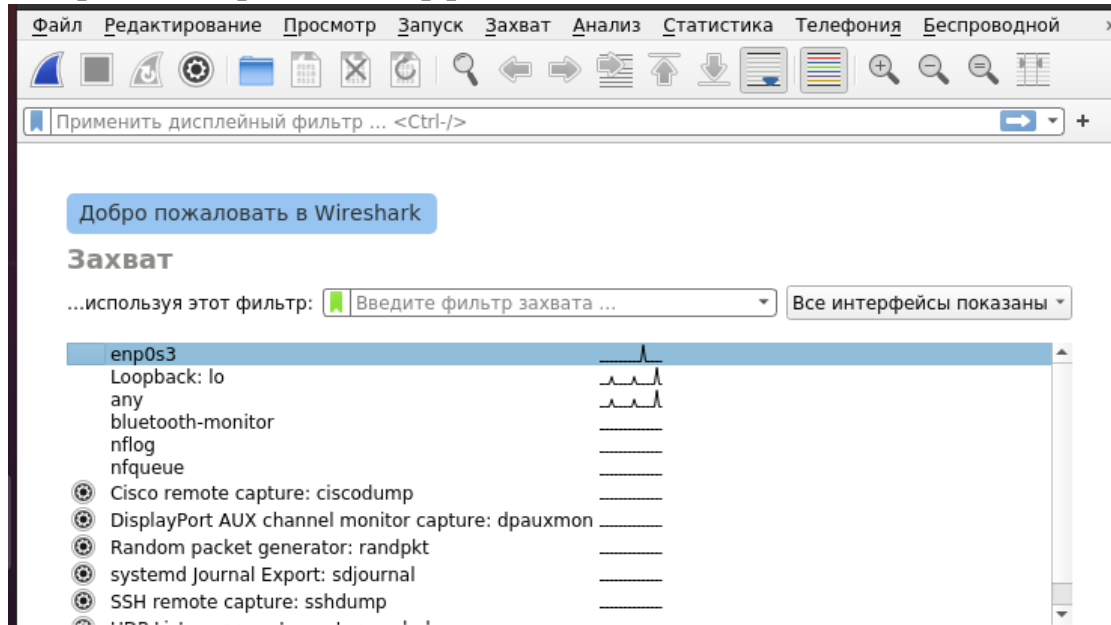
Виводимо список доступних мережевих інтерфейсів (виділено локальну ip-адресу):

```
ivan@ivan-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 fq_codel state UP group default qlen 1000
    link/ether 08:00:27:52:25:98 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 67109sec preferred_lft 67109sec
    inet6 fe80::1123:a455:ad6f:4cfe/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
ivan@ivan-VirtualBox:~$
```

Запуск системи:

```
ivan@ivan-VirtualBox:~$ sudo wireshark
[sudo] пароль для ivan:
** (wireshark:10342) 09:40:54.289552 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```

Обираємо потрібний інтерфейс:



Запускаємо пінг іншого пристрою(телефону):

```
64 bytes from 192.168.0.192: icmp_seq=79 ttl=64 time=546 ms
64 bytes from 192.168.0.192: icmp_seq=80 ttl=64 time=10.5 ms
64 bytes from 192.168.0.192: icmp_seq=81 ttl=64 time=21.2 ms
64 bytes from 192.168.0.192: icmp_seq=82 ttl=64 time=98.6 ms
64 bytes from 192.168.0.192: icmp_seq=83 ttl=64 time=32.9 ms
64 bytes from 192.168.0.192: icmp_seq=84 ttl=64 time=142 ms
64 bytes from 192.168.0.192: icmp_seq=85 ttl=64 time=161 ms
64 bytes from 192.168.0.192: icmp_seq=86 ttl=64 time=182 ms
64 bytes from 192.168.0.192: icmp_seq=87 ttl=64 time=204 ms
64 bytes from 192.168.0.192: icmp_seq=88 ttl=64 time=229 ms
64 bytes from 192.168.0.192: icmp_seq=89 ttl=64 time=247 ms
64 bytes from 192.168.0.192: icmp_seq=90 ttl=64 time=271 ms
64 bytes from 192.168.0.192: icmp_seq=91 ttl=64 time=295 ms
64 bytes from 192.168.0.192: icmp_seq=92 ttl=64 time=419 ms
```


Відповідь:

Файл

Редактирование

Просмотр

Запуск

Захват

Анализ

Статистика

Телефония

Беспроводной

<

Пінг продовжується:

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной									
Применить дисплейный фильтр ... <Ctrl-/>									
	Source	Destination	Protocol	Length	Info				
678	Tp-LinkT_ac:3d:05	Broadcast	ARP	60	Who has 192.168.0.143? Tell 192.168.0.1				
874	192.168.0.177	192.168.0.192	ICMP	98	Echo (ping) request id=0x000a, seq=5/12				
891	Tp-LinkT_ac:3d:05	Broadcast	ARP	60	Who has 192.168.0.143? Tell 192.168.0.1				
909	192.168.0.192	192.168.0.177	ICMP	98	Echo (ping) reply id=0x000a, seq=5/12				
890	192.168.0.177	192.168.0.192	ICMP	98	Echo (ping) request id=0x000a, seq=6/12				
906	Tp-LinkT_ac:3d:05	Broadcast	ARP	60	Who has 192.168.0.143? Tell 192.168.0.1				
827	192.168.0.192	192.168.0.177	ICMP	98	Echo (ping) reply id=0x000a, seq=6/12				
656	2a:bc:b0:df:c1:60	Broadcast	ARP	60	Who has 192.168.0.177? Tell 192.168.0.1				
411	PcsCompu_52:25:98	2a:bc:b0:df:c1:60	ARP	42	192.168.0.177 is at 08:00:27:52:25:98				
416	192.168.0.177	192.168.0.192	ICMP	98	Echo (ping) request id=0x000a, seq=7/12				
243	192.168.0.192	192.168.0.177	ICMP	98	Echo (ping) reply id=0x000a, seq=7/12				
985	Tp-LinkT_ac:3d:05	Broadcast	ARP	60	Who has 192.168.0.143? Tell 192.168.0.1				
645	192.168.0.177	192.168.0.192	ICMP	98	Echo (ping) request id=0x000a, seq=8/12				
449	Tp-LinkT_ac:3d:05	Broadcast	ARP	60	Who has 192.168.0.143? Tell 192.168.0.1				
Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface enp0s3, id 0									
Ethernet II, Src: Tp-LinkT_ac:3d:05 (ac:84:c6:ac:3d:05), Dst: PcsCompu_52:25:98 (08:00:27:52:25:98)									
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.177									
User Datagram Protocol, Src Port: 52674, Dst Port: 137									
NetBIOS Name Service									
0000 08 00 27 52 25 98 ac 84 c6 ac 3d 05 08 00 45 00 ..R%... ..=...E.									
0010 00 4e 00 00 40 00 40 11 b8 9c c0 a8 00 01 c0 a8 ..N..@...									
0020 00 b1 cd c2 00 89 00 3a 11 14 5f de 00 00 00 01:									
0030 00 00 00 00 00 00 20 43 4b 41 41 41 41 41 41C KAAAAAAAA									
0040 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAA AAAAAAAAA									
0050 41 41 41 41 41 41 41 00 00 21 00 01 AAAAAA .!..									

Виводимо таблицю arp:

```
64 bytes from 192.168.0.192: icmp_seq=96 ttl=64 time=506 ms
64 bytes from 192.168.0.192: icmp_seq=97 ttl=64 time=560 ms
64 bytes from 192.168.0.192: icmp_seq=98 ttl=64 time=1065 ms
64 bytes from 192.168.0.192: icmp_seq=99 ttl=64 time=61.1 ms
^C
--- 192.168.0.192 ping statistics ---
99 packets transmitted, 98 received, 1.0101% packet loss, time 98147ms
rtt min/avg/max/mdev = 6.265/224.583/1064.797/200.935 ms, pipe 2
ivan@ivan-VirtualBox:~$ arp -a
? (192.168.0.192) в 2a:bc:b0:df:c1:60 [ether] на enp0s3
_gateway (192.168.0.1) в ac:84:c6:ac:3d:05 [ether] на enp0s3
ivan@ivan-VirtualBox:~$
```

Для зручності застосовуємо фільтри:

Файл	Редактирование	Просмотр	Запуск	Захват	Анализ	Статистика	Телефония	Беспроводной
arp								
	Source	Destination	Protocol	Length	Info			
5569	Tp-LinkT_ac:3d:05	Broadcast	ARP	60	Who has 192.168.0.143? Tell 192.168.0.1			
3458	Tp-LinkT_ac:3d:05	Broadcast	ARP	60	Who has 192.168.0.133? Tell 192.168.0.1			
1792	Tp-LinkT_ac:3d:05	Broadcast	ARP	60	Who has 192.168.0.177? Tell 192.168.0.1			
1182	PcsCompu_52:25:98	Tp-LinkT_ac:3d:05	ARP	42	192.168.0.177 is at 08:00:27:52:25:98			
3700	Tp-LinkT_ac:3d:05	Broadcast	ARP	60	Who has 192.168.0.143? Tell 192.168.0.1			
2789	Tp-LinkT_ac:3d:05	Broadcast	ARP	60	Who has 192.168.0.143? Tell 192.168.0.1			
3017	Tp-LinkT_ac:3d:05	Broadcast	ARP	60	Who has 192.168.0.143? Tell 192.168.0.1			
1212	Tp-LinkT_ac:3d:05	Broadcast	ARP	60	Who has 192.168.0.133? Tell 192.168.0.1			
1352	Tp-LinkT_ac:3d:05	Broadcast	ARP	60	Who has 192.168.0.177? Tell 192.168.0.1			
3935	PcsCompu_52:25:98	Tp-LinkT_ac:3d:05	ARP	42	192.168.0.177 is at 08:00:27:52:25:98			
3828	Tp-LinkT_ac:3d:05	Broadcast	ARP	60	Who has 192.168.0.133? Tell 192.168.0.1			
3647	Tp-LinkT_ac:3d:05	Broadcast	ARP	60	Who has 192.168.0.177? Tell 192.168.0.1			
3272	PcsCompu_52:25:98	Tp-LinkT_ac:3d:05	ARP	42	192.168.0.177 is at 08:00:27:52:25:98			

Frame 90: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface enp0s3, id 0
Ethernet II, Src: Tp-LinkT_ac:3d:05 (ac:84:c6:ac:3d:05), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

```
0000  ff ff ff ff ff ff ac 84 c6 ac 3d 05 08 06 00 01  .....=.....
0010  08 00 06 04 00 01 ac 84 c6 ac 3d 05 c0 a8 00 01  .....=.....
0020  00 00 00 00 00 00 c0 a8 00 85 00 00 00 00 00 00  .....
0030  00 00 00 00 00 00 00 00 00 00 00 00  .....

```

Для достовірності інформації приводимо скріншот даних про телефон:

Сеть с лимитным подключением

Автоматическое определение

Тип MAC-адреса

Рандомизированный MAC-адрес

MAC-адрес

2a:bc:b0:df:c1:60

IP-адрес

192.168.0.192

fe80::28bc:b0ff:fedf:c160

```
ivan@ivan-VirtualBox:~$ arp -a
? (192.168.0.192) в 2a:bc:b0:df:c1:60 [ether] на enp0s3
_gateway (192.168.0.1) в ac:84:c6:ac:3d:05 [ether] на enp0s3
ivan@ivan-VirtualBox:~$
```

Test Case:

Setup Description:

PC ----- WI-FI ----- Mobiletelefon(Mb)

PC: 192.168.0.1

Mb: 192.168.0.192

Steps:

1. Clean arp table:
arp -d <for PC of Mb>
ER: verify that value for Mb is absent
2. Run Wireshark for Wi-Fi
3. Run ping from PC to Mb
ER: ping is running
4. Verify that ARP table with arp -a command
MAC was resolved by ARP protocol for Mb and appeared in ARP table
5. Verify that in Wireshark ARP request and ARP reply are present for IP and MAC of Mb

Висновки: Під час виконання даної лабораторної роботи було напрацьовано навички налаштовувати мережне оточення для тестування вбудованих систем та пристроїв IoT, також використовувати утиліту wireshark для аналізу трафіка в комп'ютерній мережі. Протестувати мережне оточення на канальному рівні моделі OSI.