МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки комп’ютерної та програмної інженерії

Кафедра безпеки інформаційних технологій

**Технології забезпечення конфіденційності і цілісності інформаційних ресурсів**

**Лабораторна робота №2**

Тема: Знайомство з Wireshark

Тривалість заняття: 180 хв.

Київ 2023

**Тема**: Знайомство з Wireshark

**Мета**: Знайомство з інструментом Wireshark для аналізу мережевого трафіку.

**Теоретичні відомості**

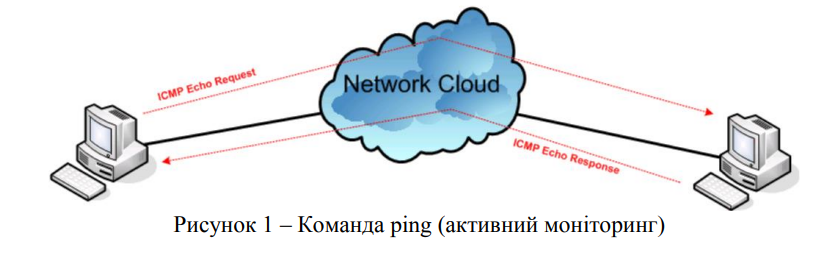
Облік мережевого трафіку є актуальним, і для його реалізації існує ряд програмних і технічних засобів. Зокрема, він реалізується в комерційних цілях при наданні послуг доступу до мережі. Однак зібрані при цьому дані не завжди можна вважати досить об'єктивними, так як обидві сторони - постачальники послуг і абоненти мережі - прагнуть змістити показники трафіку в свою користь або ж іноді невірно ідентифікувати об'єкт свого інтересу до мережі. На підставі даних про трафік в багатьох випадках можуть бути зроблені висновки про фактори, що визначають активність користувачів, а також про об'єкти їх найбільшого інтересу. Таким чином, облік мережевого трафіку фактично є частиною політики щодо забезпечення інформаційної та економічної безпеки фірм і організацій.

Дослідження мережевого трафіку показали, що він являє собою складний динамічний процес і є суперпозицією багатьох потоків з множинними взаємопов'язаними характеристиками, які генеруються різними протоколами. Поперше, це трафіки, пов'язані з управлінням комп’ютерної мережі (КМ), наприклад, трафік ініціалізації клієнтів, серверний трафік і т.д., які генеруються періодично. По-друге, це трафіки мережевих сервісів, додатків (наприклад, DNS, FTP, сеанс NetBIOS, HTTP, P2P, SMTP і т.д.) і протоколів, які становлять основну частину мережевого трафіку КМ.

Основним етапом визначення класифікаційних характеристик мережевого трафіку є процес вимірювання мережевого трафіку [1]. На підставі вимірювання дослідник може отримати важливу інформацію про властивості мережевого трафіку. При цьому вимірювання можуть бути проведені різними способами, в різних місцях мережі і в різні періоди часу і тривалості. Місце вимірювання вказує на те, яка частина або елемент КМ, а також яка величина вимірюється. При цьому дуже важливо розрізняти вимірювання мережевого трафіку від ідентифікації додатків, так як в першому випадку здійснюються збір і обробка даних, а в другому випадку - розпізнавання і класифікація деяких характеристик мережевого трафіку. В свою чергу ідентифікація мережевого трафіку є невід'ємною частиною класифікації, так як класифікація неможлива без його ідентифікації.

Аналіз мережевого трафіку може бути здійснений на декількох абстрактних рівнях: на рівні номера портів, вмісту пакета, потоку, заголовка пакета і на рівні біта (тобто обсягу трафіку). При цьому характеристики мережевого трафіку на кожному рівні відрізняються, наприклад, на рівні пакета, мережевий трафік характеризується розміром пакета і часовим інтервалом між пакетами [2]. Аналіз на рівні біта стосується кількісних характеристик мережевої мережі, таких як інтенсивність передачі і пропускна здатність обміну в каналах мережі. На рівні пакета розглядається процедура прибуття IP-пакетів, тобто інтенсивність їх затримки і втрати пакетів. Активний моніторинг повідомляє проблеми в мережі, збираючи вимірювання між двома кінцевими точками [3]. Система активного виміру має справу з такими метриками, як: корисність, маршрутизатори/маршрути, затримка пакетів, повтор пакетів, втрати пакетів, нестійка синхронізація між прибуттям, вимір пропускної здатності.

Головним чином використання інструментів, таких як команда ping, яка вимірює затримку і втрати пакетів, і traceroute, яка допомагає визначити топологію мережі, є прикладом основних активних інструментів вимірювання. Обидва ці інструменту посилають пробні ICMP-пакети до точки призначення і чекають, коли ця точка відповість відправнику. На рисунку 1 показано приклад команди ping, яка використовує активний спосіб вимірювання, посилаючи Echoзапит від джерела через мережу в встановлену точку. Потім одержувач посилає Echo-запит назад джерелу від якого прийшов запит.



Пасивні вимірювання мають справу з такою інформацією, як: трафік і суміш протоколів, кількість бітів, синхронізація пакетів і час між прибуттям. Пасивний моніторинг може бути здійснений, за допомогою будь-якої програми, що витягує пакети. Пасивний моніторинг кращий активного тому, що дані службових сигналів не додаються в мережу, але пост-обробка може забирати велику кількість часових витрат. Ось чому існує комбінація цих методів моніторингу.

Перехоплення мережевих пакетів — це інструмент діагностики мережі, який дозволяє захоплювати та зберігати пакети, що проходять через мережеві інтерфейси маршрутизатора.

Ви можете увімкнути захоплення мережевого трафіку через певний інтерфейс маршрутизатора. В результаті буде створений спеціальний файл, який можна відкрити для перегляду та аналізу на своєму комп’ютері в програмі Wireshark або надіслати команді підтримки для аналізу.

Дамп мережевих пакетів допоможе вам діагностувати проблеми мережевого трафіку та проаналізувати, що відбувається з конкретними пакетами. На основі цієї інформації можна буде зробити висновок про правильність або неправильність маршрутизації, хоста або шлюзу провайдера, щоб визначити причини проблеми та варіанти їх усунення.

Аналіз та моніторинг мереж – важлива складова сфери інформаційної безпеки та ефективної роботи комп’ютерних мереж. Wireshark і tcpdump – це два потужних інструменти, що дозволяють проводити детальний аналіз пакетів даних у локальних мережах. Вони надають можливість виявлення проблем, відстеження мережевого трафіку та забезпечення безпеки мережевих ресурсів.

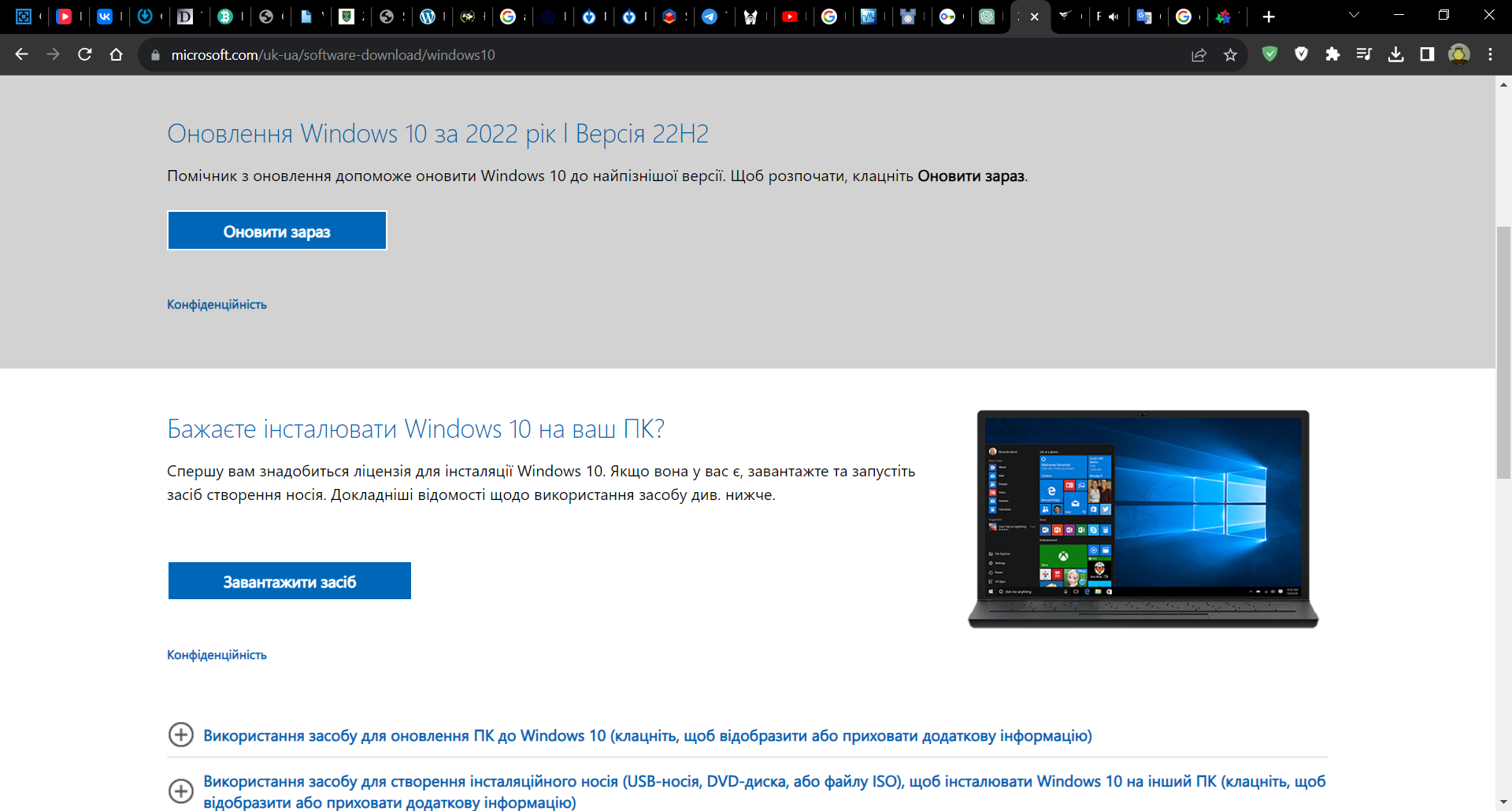
Wireshark – це графічний інструмент аналізу мережі, який дозволяє візуалізувати та фільтрувати пакети даних. Він забезпечує зручний інтерфейс для перегляду мережевого трафіку у реальному часі та в режимі аналізу пакетів. Його можливості дозволяють виявити проблеми, такі як перевантаження мережі, аномалії у спілкуванні між пристроями, атаки та інші аномалії.

Також, Wireshark є потужним інструментом для відлагодження мережевих додатків та служб. Інженери мереж можуть використовувати його для визначення причин низької продуктивності мережі та забезпечення її оптимізації. tcpdump, з іншого боку, є консольним інструментом для перехоплення та аналізу пакетів даних. Він забезпечує можливість моніторити мережевий трафік у реальному часі, а також записувати його для подальшого аналізу. tcpdump особливо корисний для адміністраторів мереж, які працюють у середовищах командного рядка і вимагають точного контролю над процесом аналізу мережі.

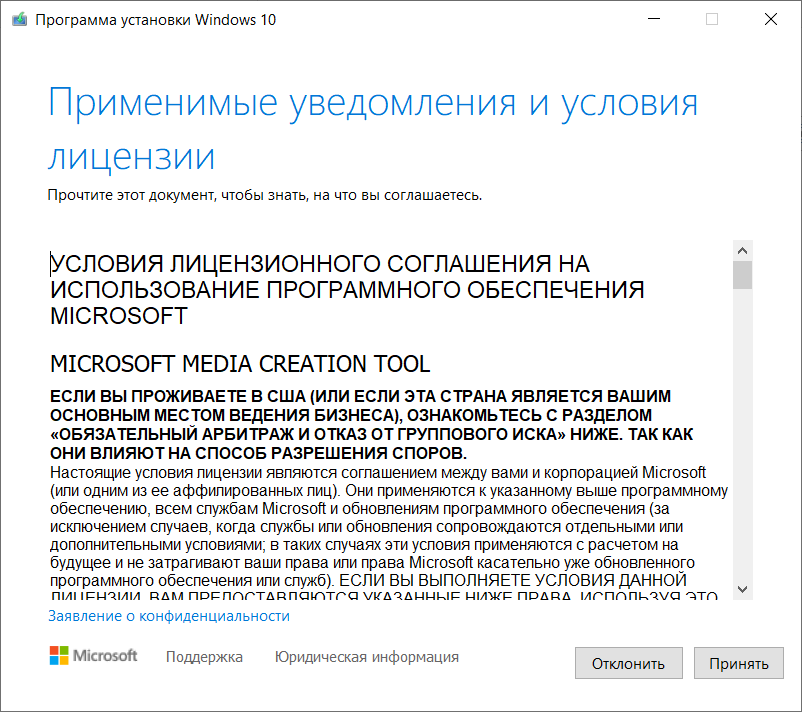
Загалом, Wireshark і tcpdump є незамінними інструментами для професіоналів, які займаються адмініструванням, моніторингом та забезпеченням безпеки комп’ютерних мереж. Вони допомагають виявити та вирішити проблеми у локальних мережах та забезпечують безпеку та ефективність їх функціонування.

**Завдання**

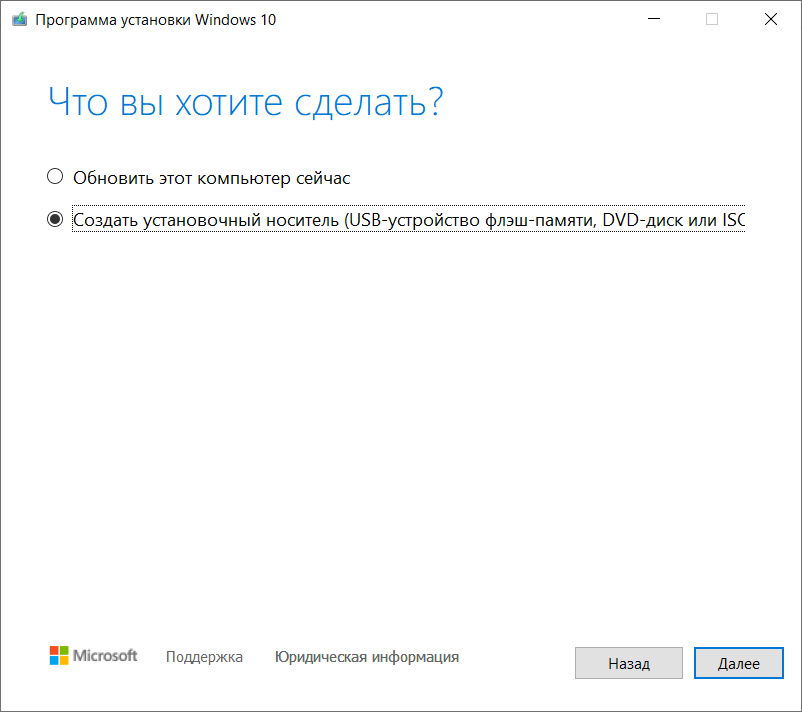
1. Завантажте віртуальну машину з цього сайту <https://www.virtualbox.org/wiki/Downloads>
2. Далі перейдіть до завантаженого вами файлу, та двічі клацнувши по ньому лівою кнопкою миші почніть встановлення віртуальної машини.
3. Для встановлення машини на своєму комп’ютері слідуйте інструкціям в інсталяторі.
4. Відкрийте браузер встановлений на вашому комп’ютері, та скачайте образ Windows 10 <https://www.microsoft.com/uk-ua/software-download/windows10>



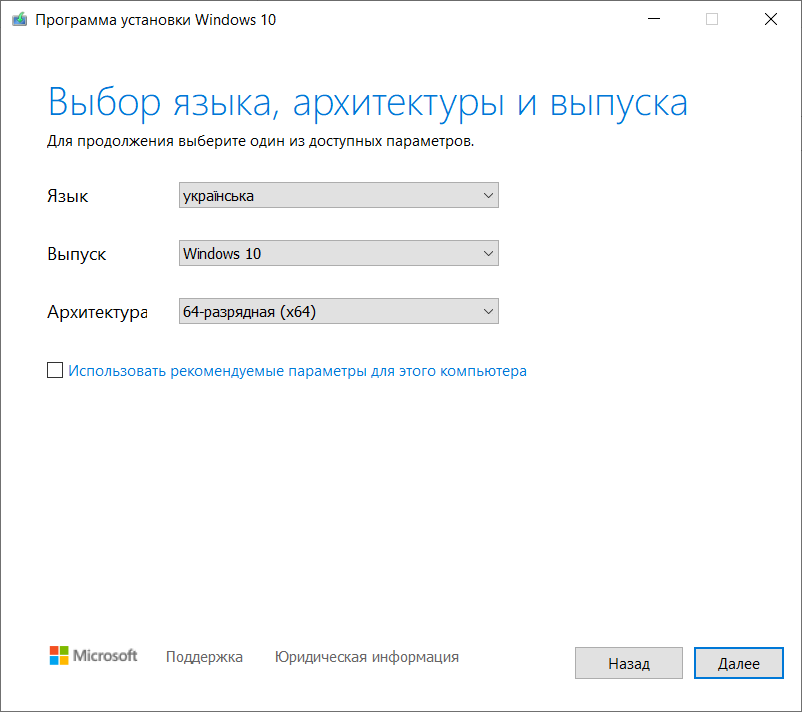
1. Відкрийте завантажену вами програму. У відкритому вікні натисніть кнопку прийняти.



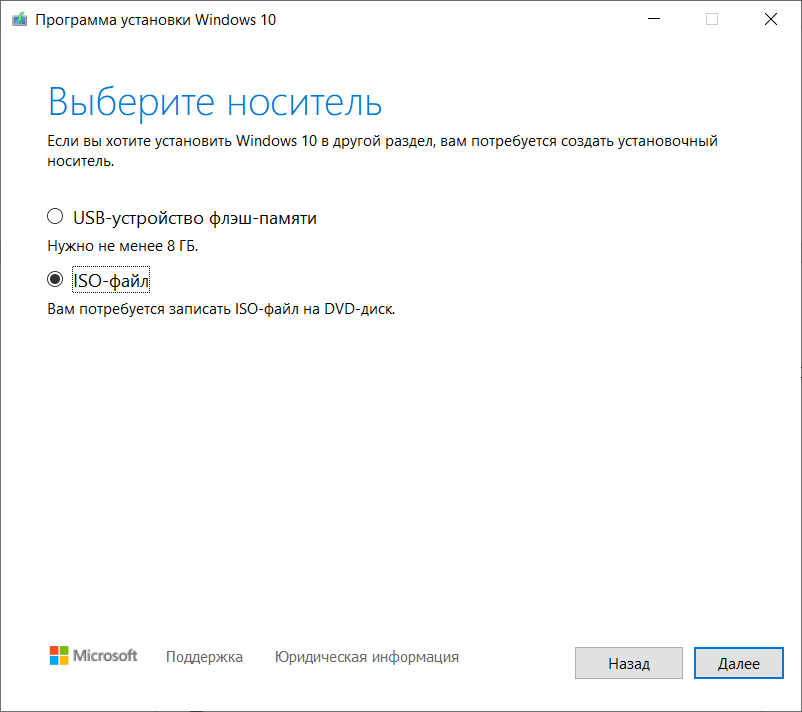
1. Виберіть той самий пункт який вибраний на малюнку, та натисніть кнопку Далі.



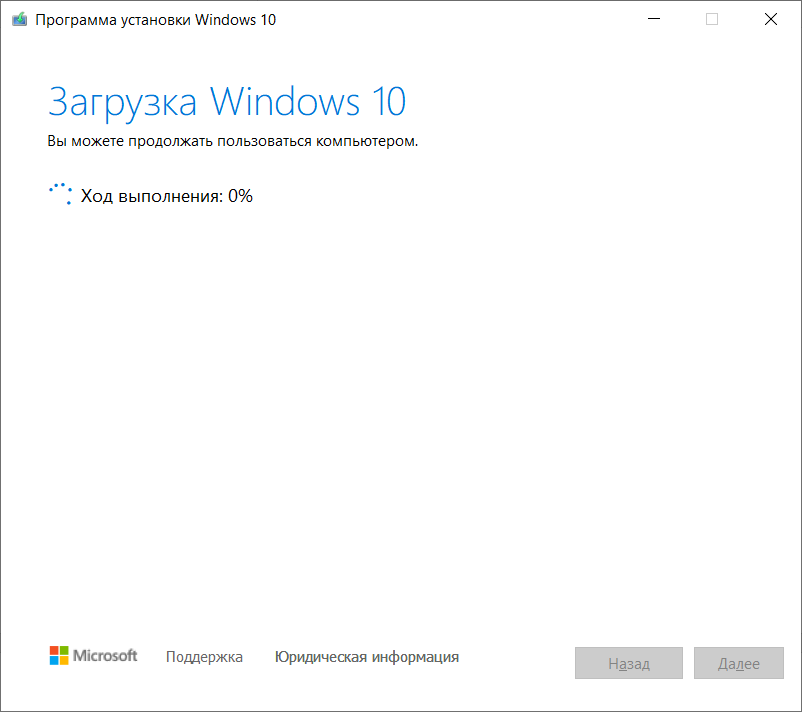
1. Виберіть ті самі пункти які вибрані на малюнку, та натисніть кнопку Далі.

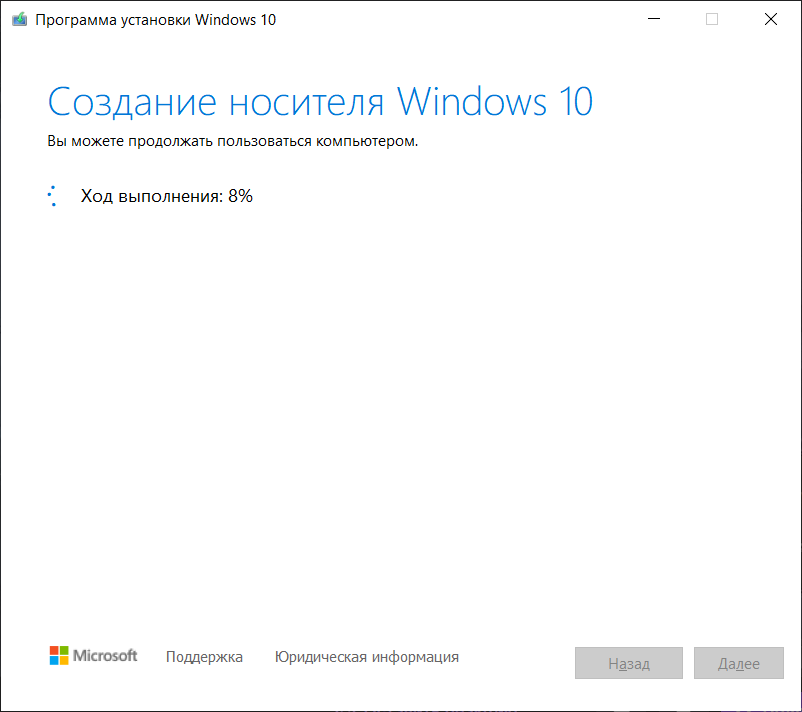


1. На наступному кроці виберіть ISO-файл, та натисніть кнопку Далі.

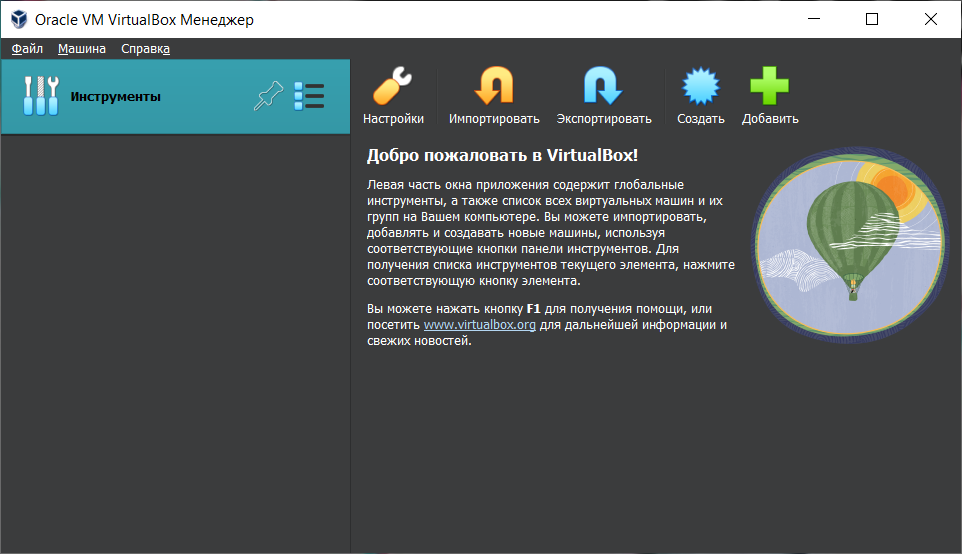


1. У вікні яке відрилось виберіть куди зберегти образ windows 10, та запам’ятайте куди ви зберегли образ.
2. Зачекайте поки буде створено віртуальний образ. Потім натисніть кнопку Готово.

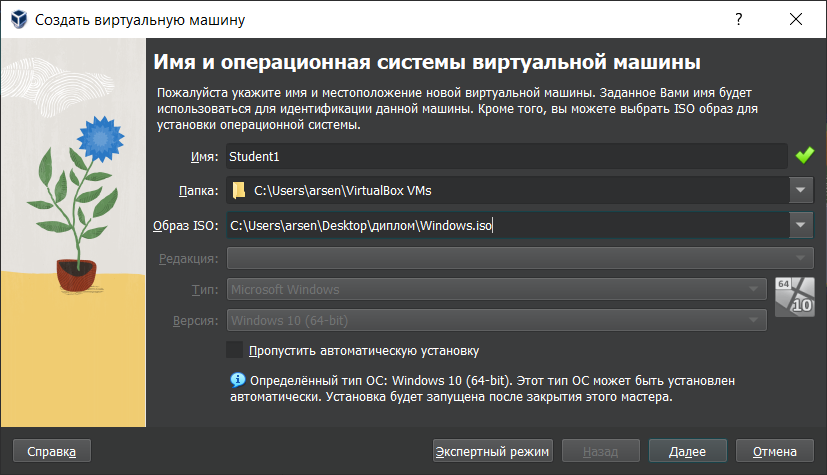




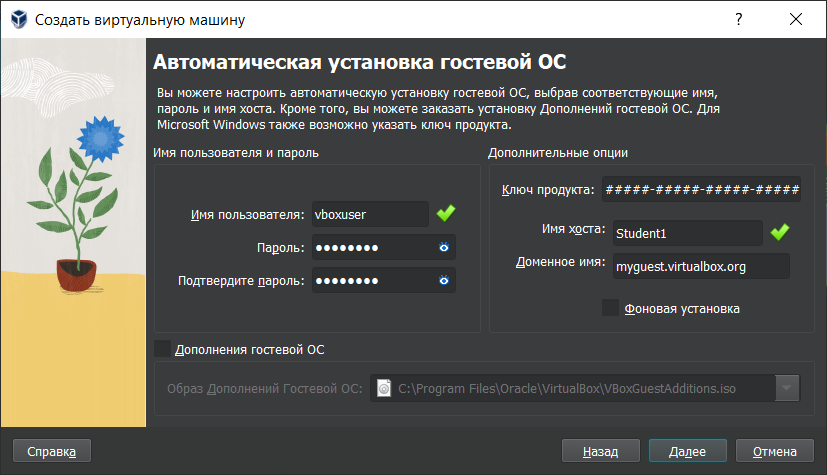
1. Запустіть встановлену вами віртуальну машину. Натисніть кнопку створити



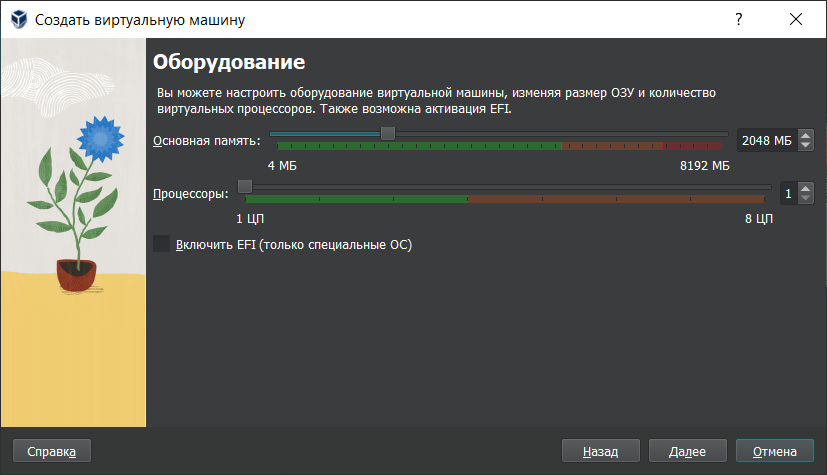
1. Назвіть машину своїм прізвищем, виберіть образ ISO windows 10, та натисніть кнопку Далі.



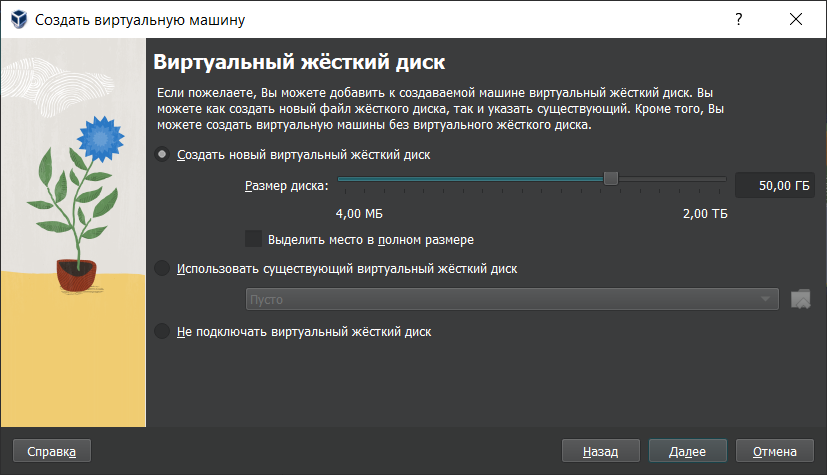
1. У відкритому вікні введіть свій пароль, в полі ім’я користувача впишіть свою фамілію та натисніть кнопку Далі.



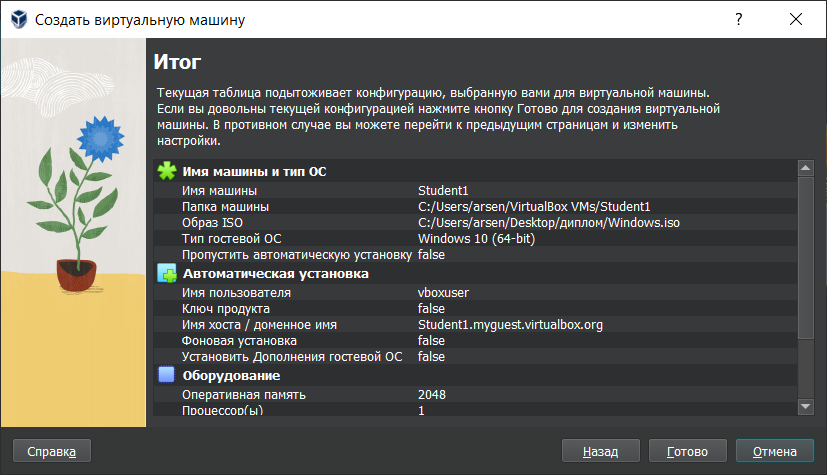
1. Натисніть кнопку Далі.



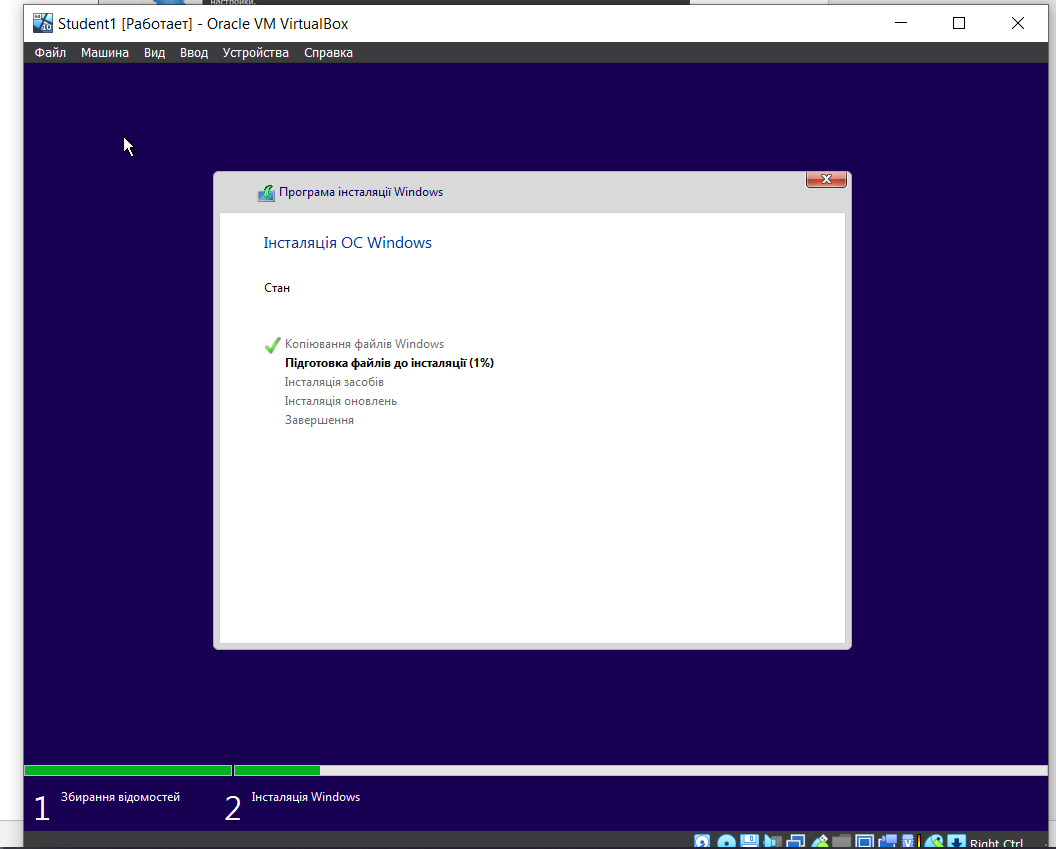
1. Знову натисніть кнопку Далі



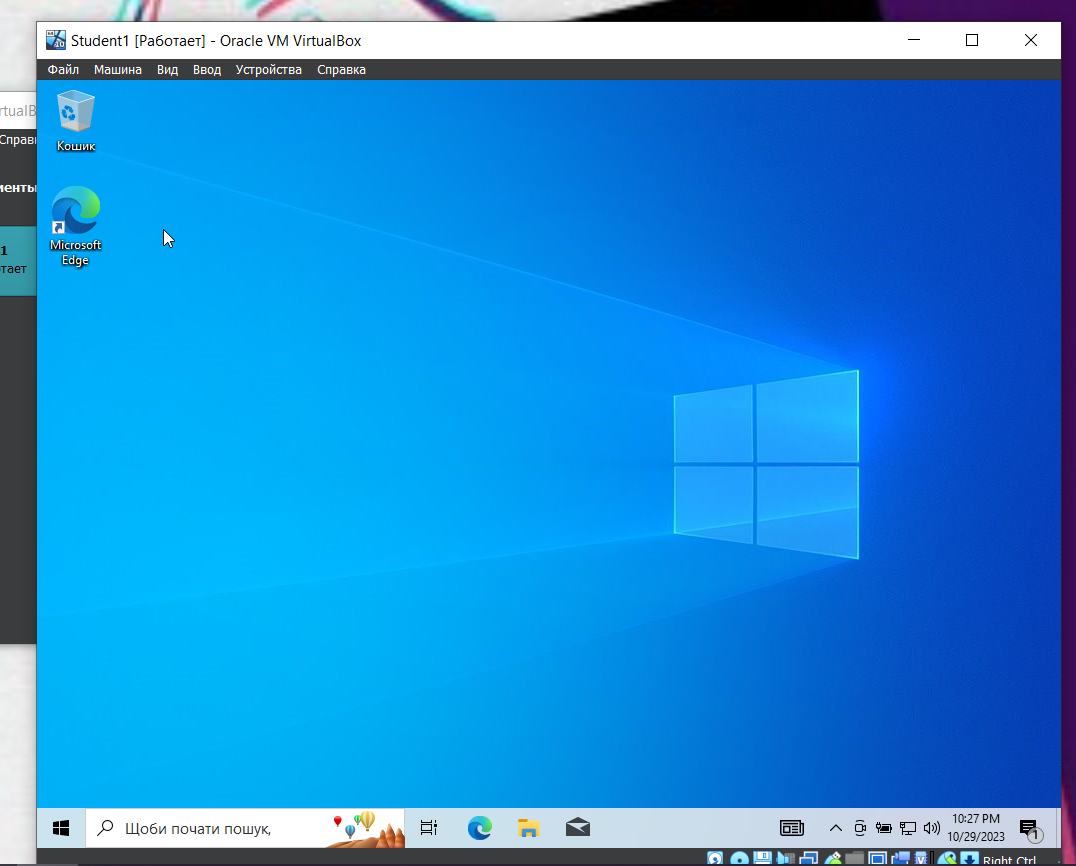
1. Натисніть кнопку Готово



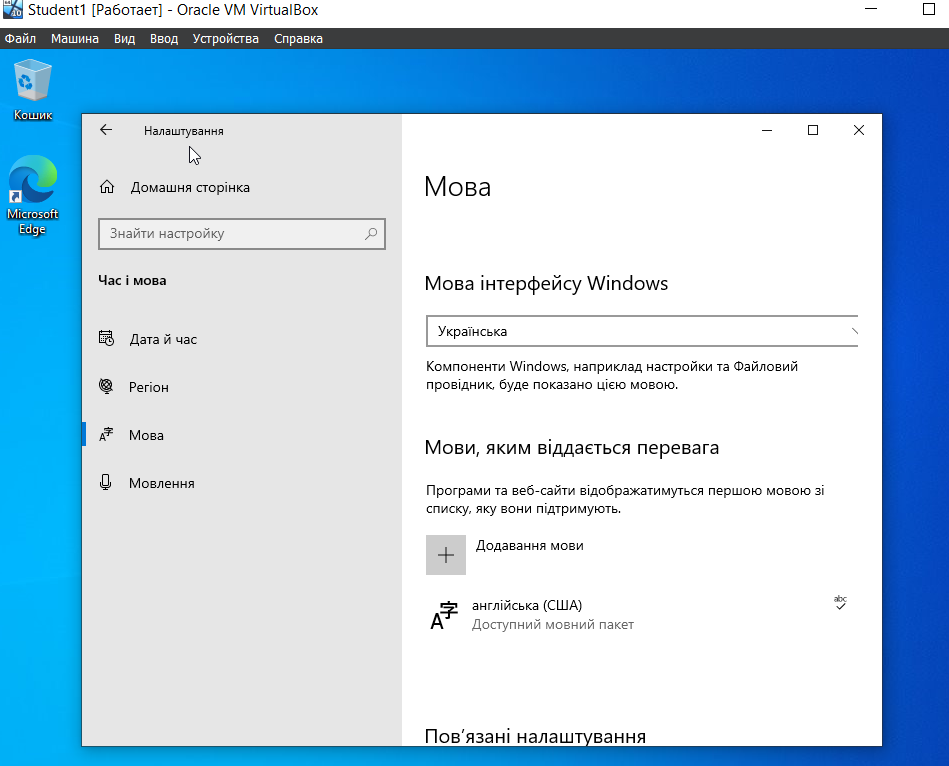
1. Віртуальна машина тепер створена, якщо вона сама не запуститься натисніть по ній два рази мишкою. Тепер на машину нам потрібно поставити windows 10.

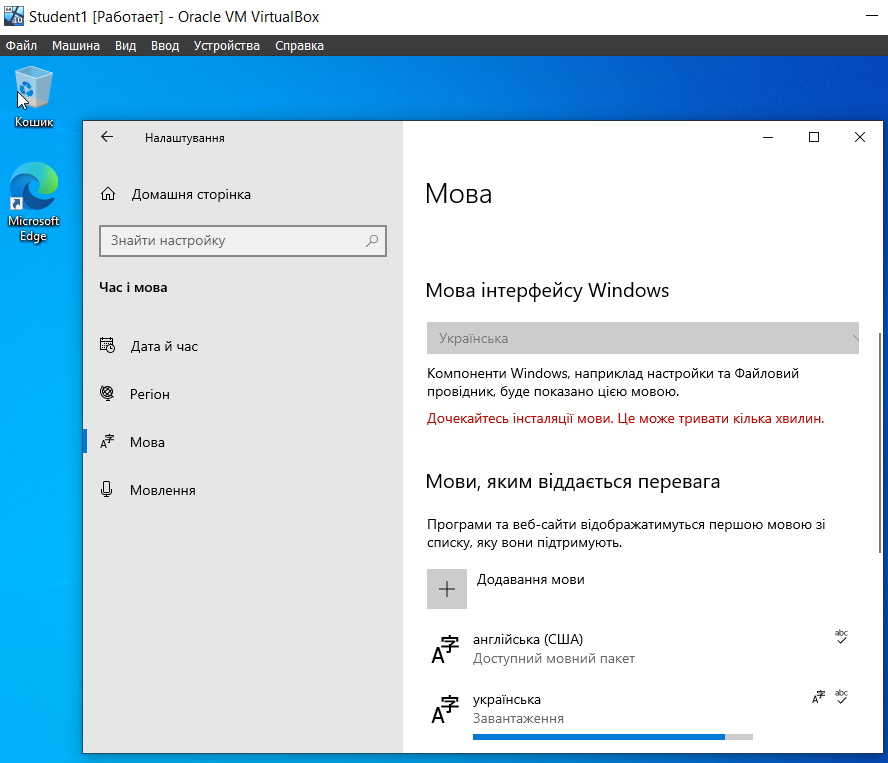


1. Якщо ви виконали все правильно, то у вас має завантажитись windows 10, та буде відкритий робочий стіл.

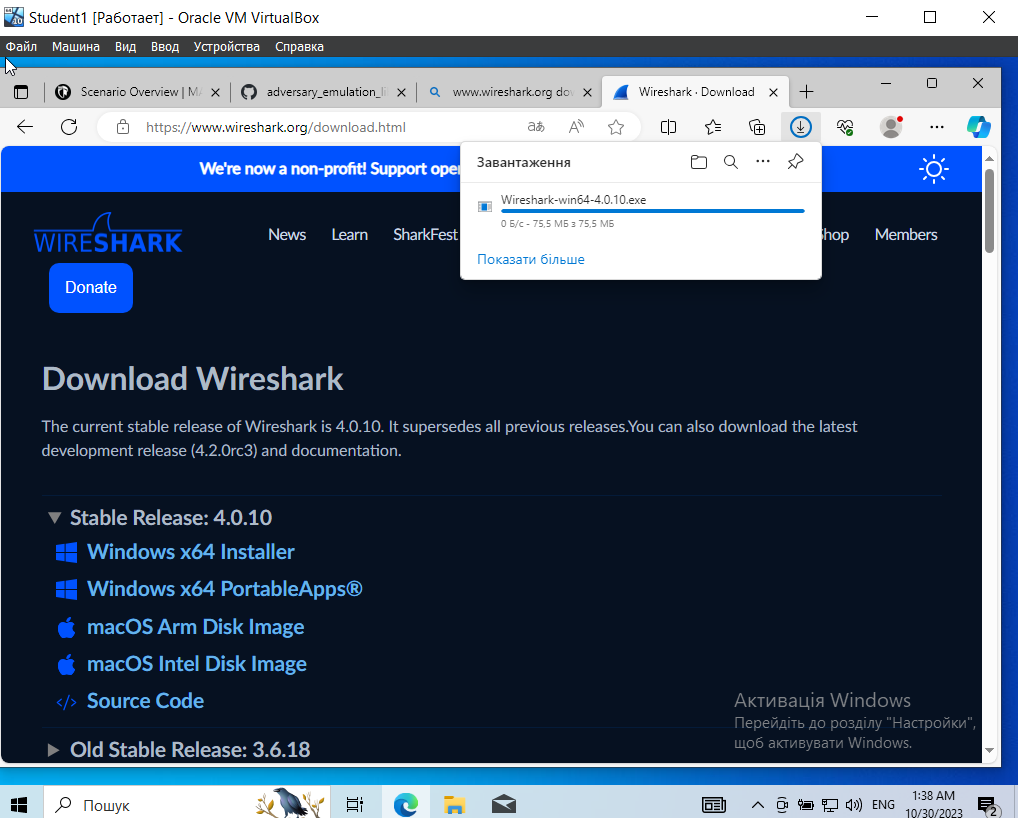


1. Через кнопку windows – параметри – час і мова – мова, додайте українську мову.

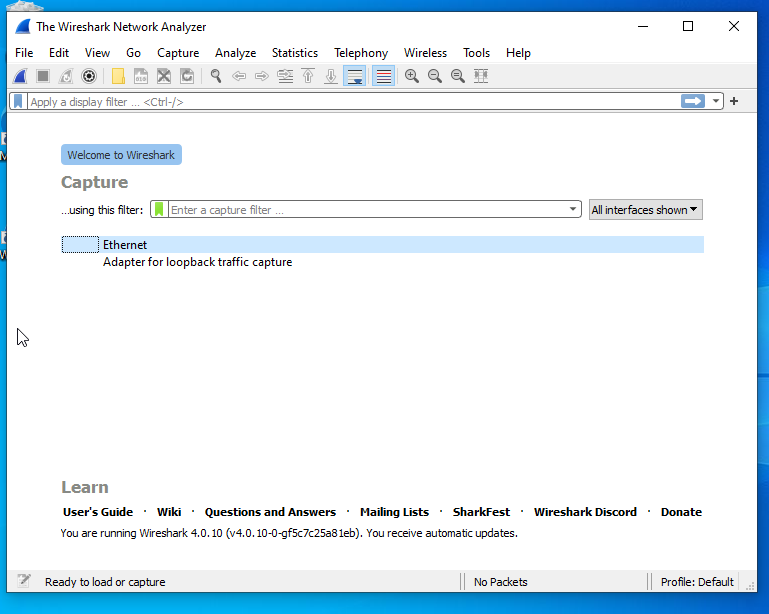




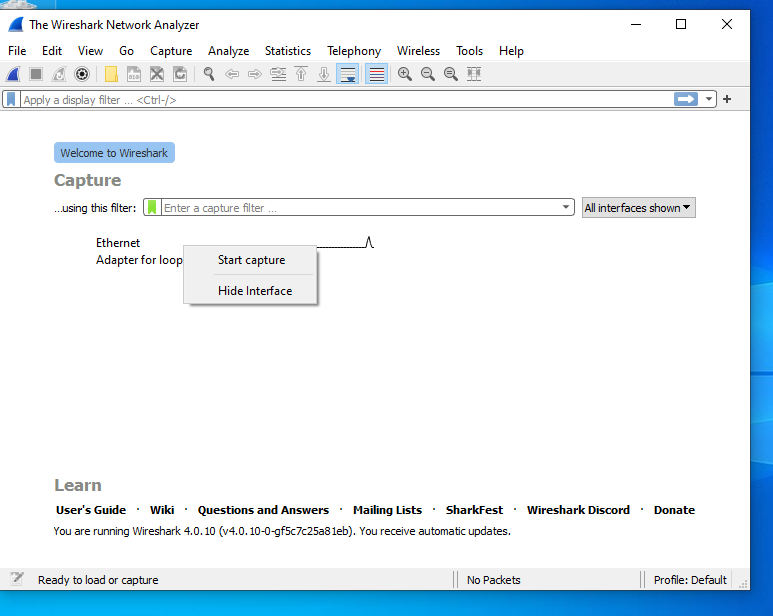
1. Запустіть браузер який встановлений на віртуальній машині (Microsoft Edge), та введіть в пошукову строку таке посилання <https://www.wireshark.org/download.html> (копіювання з лабораторної роботи в віртуальну машину не спрацює, потрібно вводити вручну).



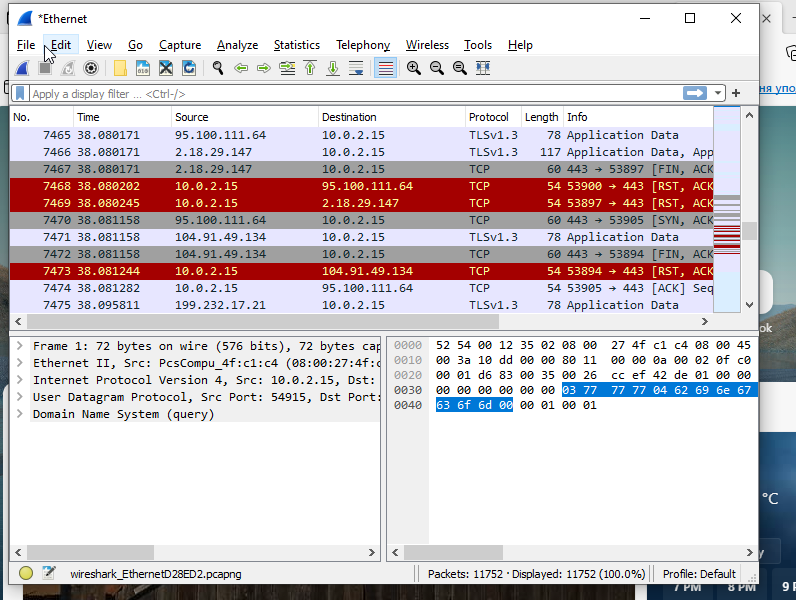
1. Відкрийте щойно встановлений вами файл на віртуальній машині, та слідуйте інструкціям майстра встановлення.
2. Після встановлення, відкрийте встановлену вами програму



1. Далі клацніть правою клавішою мишки по надпису Ethernet, та натисніть кнопку Start capture



1. Після натискання на цю кнопку, вам потрібно зайти в браузер та почати переходити по різноманітним вкладкам та сторінкам. Тоді вам потрібно повернутись в програму, та натиснути на червоний квадратик в лівому верхньому кутку, для того щоб призупинити захват мережевого трафіку.



1. Продивіться захват свого мережевого трафіку. Занесіть до таблиці 25 пакетів.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Time | Source | Destination | Protocol | Length | Info |
|  |  |  |  |  |  |

1. Проаналізуйте додані вами до таблиці пакети, за такими параметрам як в таблиці, аналіз запишіть в звіт лабораторної роботи. Проаналізуйте які пакети можуть бути підозрілими на вашу думку, чим вони відрізняються від всіх інших пакетів.
2. Дайте відповідь на контрольні питання.
3. Звіт має бути з описом вашої виконаної роботи, та зі скріншотами етапів виконання роботи.
4. Зробити висновки та занести їх до звіту.

**Контрольні питання**

1. Що таке мережевий трафік?
2. Що таке мережевий пакет?
3. Яким чином можна проводити аналіз мережевих трафіку та пакетів?
4. Які програми можна використовувати для проведення аналізу мережевого трафіку та пакеті?
5. На яких абстрактних рівнях може бути здійснений аналіз мережевого трафіку?