* Wireshark (раніше звався Ethereal) — програма для аналізу мережевих пакетів [Ethernet](https://uk.wikipedia.org/wiki/Ethernet) і інших мереж ([сніфер](https://uk.wikipedia.org/wiki/%D0%A1%D0%BD%D1%96%D1%84%D0%B5%D1%80)) з [вільним вихідним кодом](https://uk.wikipedia.org/wiki/%D0%92%D1%96%D0%BB%D1%8C%D0%BD%D0%B5_%D1%82%D0%B0_%D0%B2%D1%96%D0%B4%D0%BA%D1%80%D0%B8%D1%82%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%B5_%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F). Має [графічний інтерфейс користувача](https://uk.wikipedia.org/wiki/%D0%93%D1%80%D0%B0%D1%84%D1%96%D1%87%D0%BD%D0%B8%D0%B9_%D1%96%D0%BD%D1%82%D0%B5%D1%80%D1%84%D0%B5%D0%B9%D1%81_%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D1%83%D0%B2%D0%B0%D1%87%D0%B0). У червні [2006](https://uk.wikipedia.org/wiki/2006) року проєкт був перейменований на Wireshark через проблеми з [торговою маркою](https://uk.wikipedia.org/wiki/%D0%A2%D0%BE%D1%80%D0%B3%D0%BE%D0%B2%D0%B0_%D0%BC%D0%B0%D1%80%D0%BA%D0%B0).
* Wireshark — це програма, яка розпізнає структуру найрізноманітніших мережевих протоколів, і тому дозволяє розібрати мережевий пакет, відображаючи значення кожного поля протоколу будь-якого рівня. Оскільки для захоплення пакетів використовується [*pcap*](https://uk.wikipedia.org/w/index.php?title=Pcap&action=edit&redlink=1), існує можливість захоплення даних тільки з тих мереж, які підтримуються цією бібліотекою.   
  PCAP по суті перетворює цифрову інформацію в радіосигнали, які називаються пакетами, за допомогою спеціального алгоритму.  
  Проте, Wireshark вміє працювати з безліччю форматів початкових даних, відповідно, можна відкривати файли даних, захоплених іншими програмами, що розширює можливості захоплення.
* Основні можливості:
  + Дані можуть бути захоплені "у реальному часі" з живого мережевого з'єднання або зчитані з файлу вже захоплених пакетів.
  + Живі дані можна зчитувати з різних типів мереж, включаючи Ethernet, IEEE 802.11, PPP і loopback.
  + Захоплені мережеві дані можна переглядати за допомогою графічного інтерфейсу користувача або через термінальну (командний рядок) версію утиліти TShark.
  + Захоплені файли можна програмно редагувати або конвертувати за допомогою параметрів командного рядка в програму "editcap".
  + Відображення даних можна уточнити за допомогою фільтра відображення.
  + Можна створювати плагіни для аналізу нових протоколів.
  + Виклики VoIP у захопленому трафіку можуть бути виявлені. Якщо закодовано у сумісному кодуванні, медіа-потік можна навіть відтворювати.
  + Необроблений трафік USB може бути захоплений.
  + Бездротові з’єднання також можна фільтрувати, якщо вони проходять через мережу Ethernet, що контролюється.
  + Різноманітні параметри, таймери та фільтри можна встановити, щоб забезпечити можливість фільтрації виходу захопленого трафіку.
* Безпека:
  + Перехоплення необробленого мережевого трафіку з інтерфейсу потребує підвищених привілеїв на деяких платформах. З цієї причини старіші версії Wireshark і TShark часто запускалися з правами суперкористувача. Враховуючи величезну кількість дисекторів протоколів, які викликаються під час захоплення трафіку, і розпізнавання можливості помилки в дисекторі, може виникнути серйозний ризик для безпеки. Через досить велику кількість вразливостей у минулому (багато з яких дозволяли дистанційне виконання коду) і сумніви розробників щодо кращого майбутнього розвитку, OpenBSD видалив Ethereal зі свого дерева портів до OpenBSD.
  + Підвищені привілеї не потрібні для всіх операцій. Наприклад, альтернативою є запуск tcpdump або утиліти dumpcap, яка постачається разом із Wireshark, із правами суперкористувача, щоб перехоплювати пакети у файл, а потім аналізувати пакети, запускаючи Wireshark із обмеженими правами. Щоб імітувати аналіз майже в реальному часі, кожен захоплений файл може бути об’єднаний mergecap у зростаючий файл, оброблений Wireshark. У бездротових мережах можна використовувати інструменти бездротової безпеки Aircrack для захоплення кадрів IEEE 802.11 і читання отриманих файлів дампа за допомогою Wireshark.
  + Починаючи з Wireshark 0.99.7, Wireshark і TShark запускають dumpcap для захоплення трафіку. Платформи, які потребують спеціальних привілеїв для захоплення трафіку, потребують лише запуску dumpcap із цими привілеями. Ні Wireshark, ні TShark не потребують і не повинні запускатися зі спеціальними привілеями.
* Wireshark має відкритий ісходний код, тому можна щось доробляти, також розробники надають можливість для створення плагінів для ПЗ