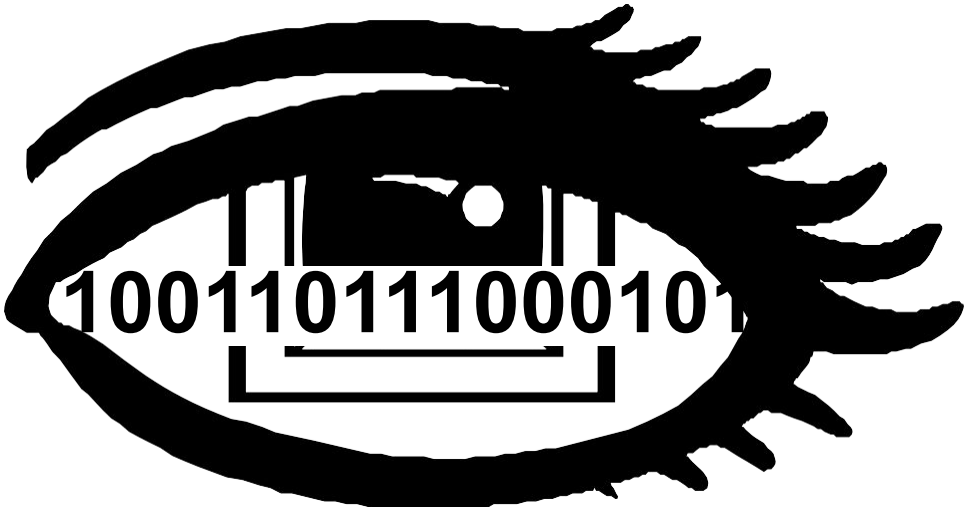
Мережева безпека



Інструменти для аналізу трафіка

Перелік тем

- «Перегляд» мережевого трафіка.
- Області аналізу.
- Огляд інструментів:
  - TCPdump;
  - Tshark;
  - Wireshark.
- Огляд Wireshark.

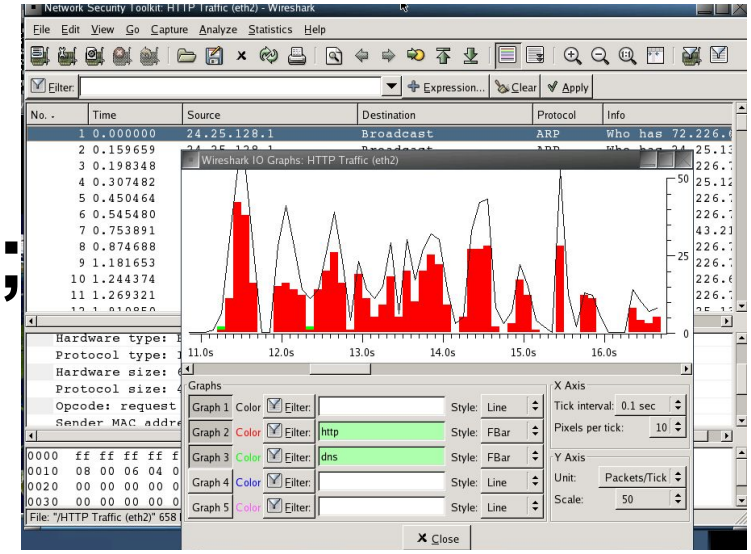
«Перегляд» мережевого трафіка

- Перегляд вихідного потоку бітів є технічно невиправданим, тому ми будемо використовувати спеціальну програму, що називається аналізатор протоколів, для захоплення, трансляції та представлення пакетів у зручній для людини формі.
- Інтерпретація відповідно до форматів заголовків, визначених у документах RFC, справа нескладна.

Області аналізу

- **Мережевий аналіз здійснюють з низкою мет:**

1. **загальний аналіз:**
2. **пошук і усунення несправностей;**
3. **безпековий аналіз;**
4. **продуктивність програм.**



1. Завдання загального аналізу

- Пошук вузлів, що ведуть найбільш активний обмін даними в ме
- огляд мережевих комунікацій як «простого тексту»;
- огляд програм, що використовуються хостами;
- визначення базового рівня нормальних мережевих комунікацій;
- перевірка належності мережевих операцій;
- визначення, хто намагається приєднатися до бездротової мережі;
- ведення захоплення трафіка в кількох мережах одночасно;
- здійснення захоплення трафіка без нагляду адміністратора;
- захоплення й аналіз трафіка в напрямку до/від конкретного хоста чи підмережі;
- перегляд і повторне збирання файлів, що передаються по FTP або HTTP;
- імпорт файлів трасування з інших інструментів захоплення;
- захоплення з використанням мінімуму ресурсів.

2. Завдання пошуку й усунення несправностей

- **Створення спеціалізованого аналітичного середовища для пошуку й усунення несправностей;**
- **визначення шляху, клієнта та затримок сервера;**
- **визначення проблем із TCP;**
- **виявлення проблем із HTTP-проксі;**
- **виявлення відповідей з помилками від програм;**
- **побудова графіків швидкості введення-виведення і зіставлення просадок із проблемами в мережі;**
- **визначення перевантажених буферів;**
- **порівняння повільних комунікацій із базовим рівнем нормальних комунікацій;**
- **пошук дублікатів IP-адрес;**
- **визначення проблем із DHCP-сервером чи ретранслятором у мережі;**
- **визначення проблем із потужністю сигналу бездротової мережі;**
- **виявлення повторних спроб передавання у бездротовій мережі;**
- **захоплення трафіка, який призводить до проблем (і, ймовірно, є їх причиною);**

3. Завдання безпекового (криміналістичного) аналізу

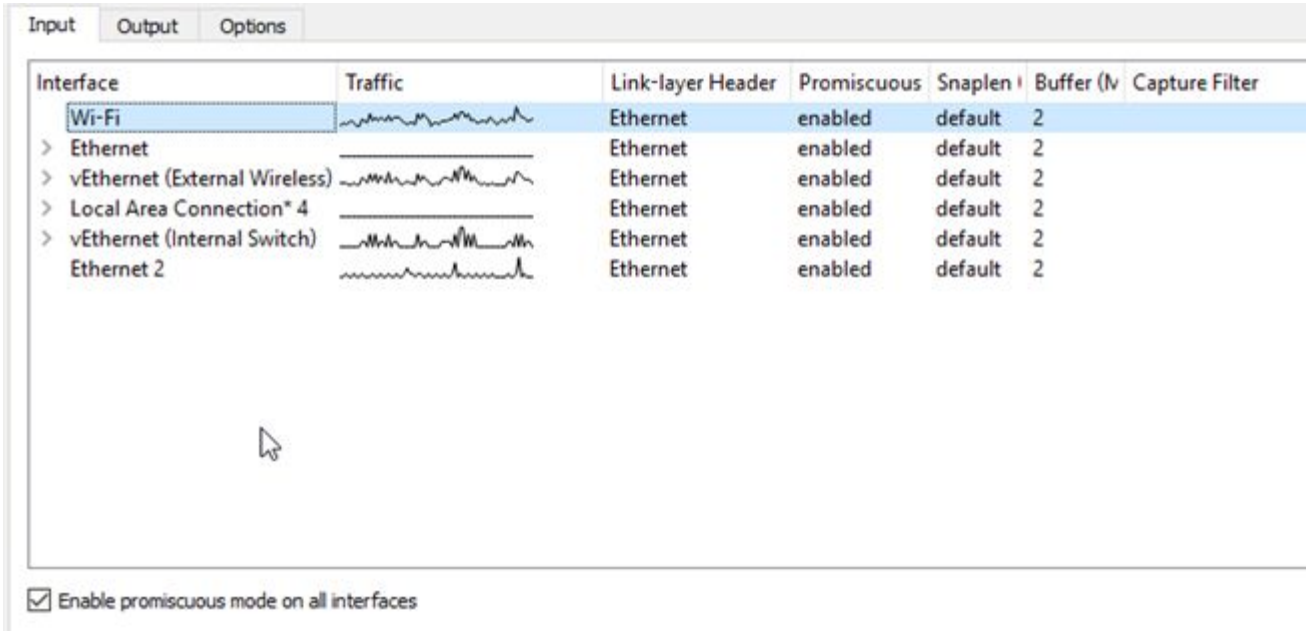
- **Створення спеціалізованого аналітичного середовища для мережевої криміналістики;**
- **виявлення програм, що використовують нестандартні порти;**
- **визначення трафіка до/від підозрілих хостів;**
- **огляд того, які хости намагаються отримати IP-адресу;**
- **визначення трафіка типу «дзвінків додому»;**
- **визначення процесів, що збирають дані про мережу;**
- **визначення розташування та побудова глобальної мапи віддалених цільових адрес;**
- **виявлення сумнівних перенаправлень трафіка;**
- **перевірка конкретного сеансу обміну даними TCP або UDP між клієнтом і сервером;**
- **виявлення пакетів, сформованих із потенційно зловмисною метою;**
- **виявлення сигнатур відомої атаки за ключовими словами в мережевому трафіку.**

4. Завдання аналізу прикладних програм

- Дослідження роботи програм і протоколів;
- побудова графіка використання смуги пропускання програмою;
- визначення достатності каналу для програми;
- перевірка продуктивності програми після оновлення/розширення;
- виявлення відповідей з помилками від нещодавно встановленої програми;
- визначення того, які користувачі запускають конкретну програму;
- перевірка того, як програма використовує транспортні протоколи, як-от TCP чи UDP.

За лаштунками

- Драйвери карт мережевих інтерфейсів.
- Всі інструменти мережевого аналізу залежать від драйверів канального рівня в отриманні безпосереднього доступу до сигналів у мережі.
- Два найбільш поширені мережеві драйвери:
  - libpcap на Unix (у тому числі й MacOS);
  - Winpcap на Windows.



Огляд інструментів

- **Tcpdump:**
  - **інструмент для командного рядка Unix, що слугує для перехоплення пакетів;**
    - **має фільтри для виловлювання тільки потрібних пакетів;**
  - **зчитує трафік у реальному часі на інтерфейсі, заданому параметром -i;**
  - **або з попередньо записаного файлу трасування, заданого параметром -r;**
    - **ці файли можливо створювати під час захоплення трафіку реального часу за допомогою параметра -w.**

- **Tshark:**
  - **аналогічна до tcpdump програма захоплення, що йде в комплекті із Wireshark;**
  - **поведінка та прапорці дуже схожі на такі в tcpdump.**

- **Wireshark:**
  - **удосконалений графічний інтерфейс для відображення трасувань пакетів libpcap/Winpcap.**

Приклад tcpdump

виведення tcpdump на Unix-машині

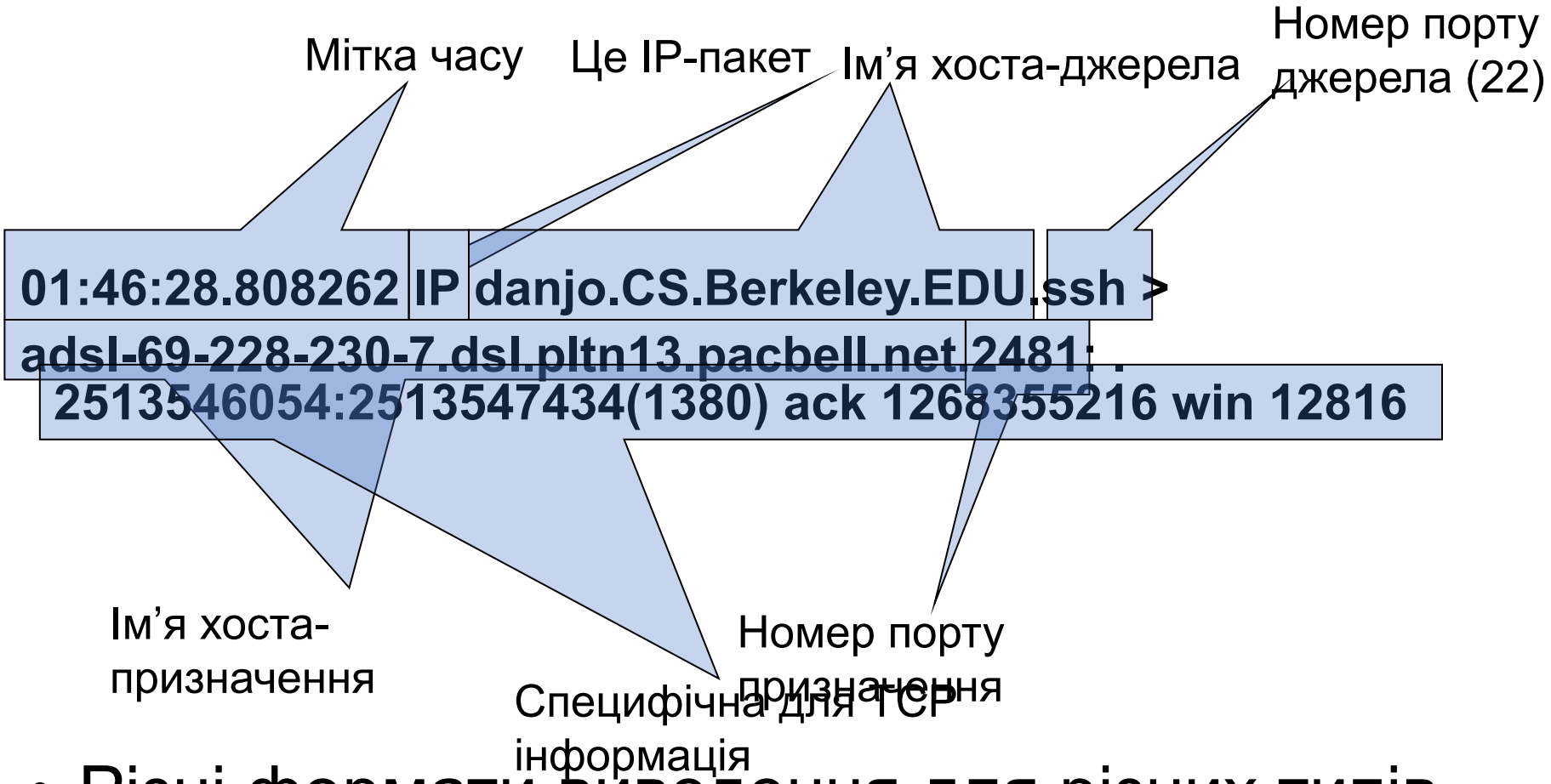
```
01:46:28.808262 IP danjo.CS.Berkeley.EDU.ssh >
adsl-69-228-230-7.dsl.pltn13.pacbell.net.2481:
. 2513546054:2513547434(1380) ack 1268355216
win 12816

01:46:28.808271 IP danjo.CS.Berkeley.EDU.ssh >
adsl-69-228-230-7.dsl.pltn13.pacbell.net.2481:
P 1380:2128(748) ack 1 win 12816

01:46:28.808276 IP danjo.CS.Berkeley.EDU.ssh >
adsl-69-228-230-7.dsl.pltn13.pacbell.net.2481:
. 2128:3508(1380) ack 1 win 12816

01:46:28.890021 IP
adsl-69-228-230-7.dsl.pltn13.pacbell.net.2481
> danjo.CS.Berkeley.EDU.ssh: P 1:49(48) ack
1380 win 16560
```

Про що говорить цей рядок?



- Різні формати виведення для різних типів пакетів

Аналогічне виведення Tshark

```
1190003744.940437 61.184.241.230 -> 128.32.48.169
SSH Encrypted request packet len=48

1190003744.940916 128.32.48.169 -> 61.184.241.230
SSH Encrypted response packet len=48

1190003744.955764 61.184.241.230 -> 128.32.48.169
TCP 6943 > ssh [ACK] Seq=48 Ack=48 Win=65514 Len=0
TSV=445871583 TSER=632535493

1190003745.035678 61.184.241.230 -> 128.32.48.169
SSH Encrypted request packet len=48

1190003745.036004 128.32.48.169 -> 61.184.241.230
SSH Encrypted response packet len=48

1190003745.050970 61.184.241.230 -> 128.32.48.169
TCP 6943 > ssh [ACK] Seq=96 Ack=96 Win=65514 Len=0
TSV=445871583 TSER=632535502
```

tshark

C:\Program Files\Wireshark>tshark -help
TShark 1.0.0
Dump and analyze network traffic.
See http://www.wireshark.org for more information.

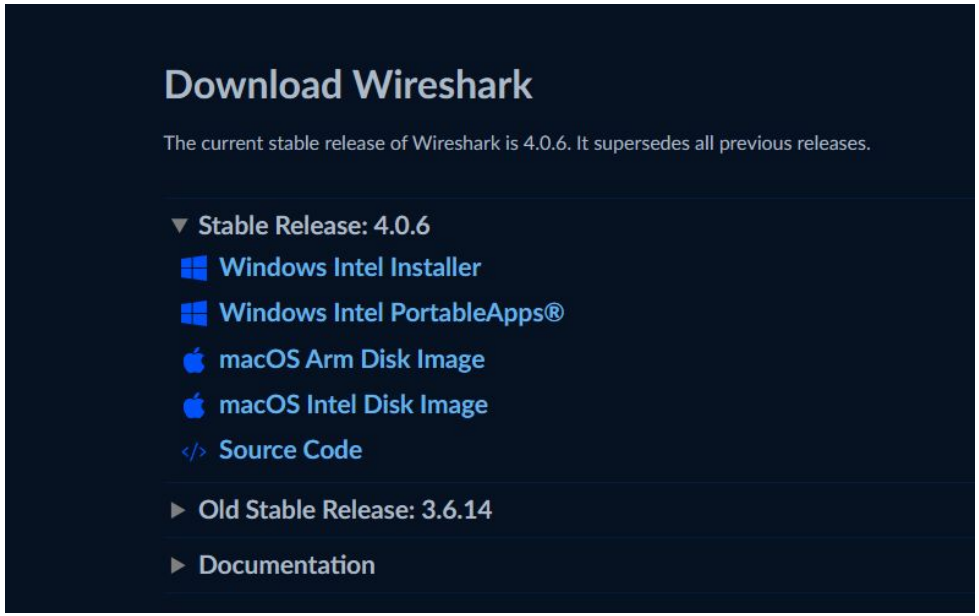
Usage: tshark [options] ...

Capture interface:
  -i <interface> name or idx of interface (def: first non-loopback)
  -f <capture filter> packet filter in libpcap filter syntax
  -s <snaplen>   packet snapshot length (def: 65535)
  -p   don't capture in promiscuous mode
  -B <buffer size>   size of kernel buffer (def: 1MB)
  -y <link type>   link layer type (def: first appropriate)
  -D   print list of interfaces and exit
  -L   print list of link-layer types of iface and exit

Capture stop conditions:

Wireshark

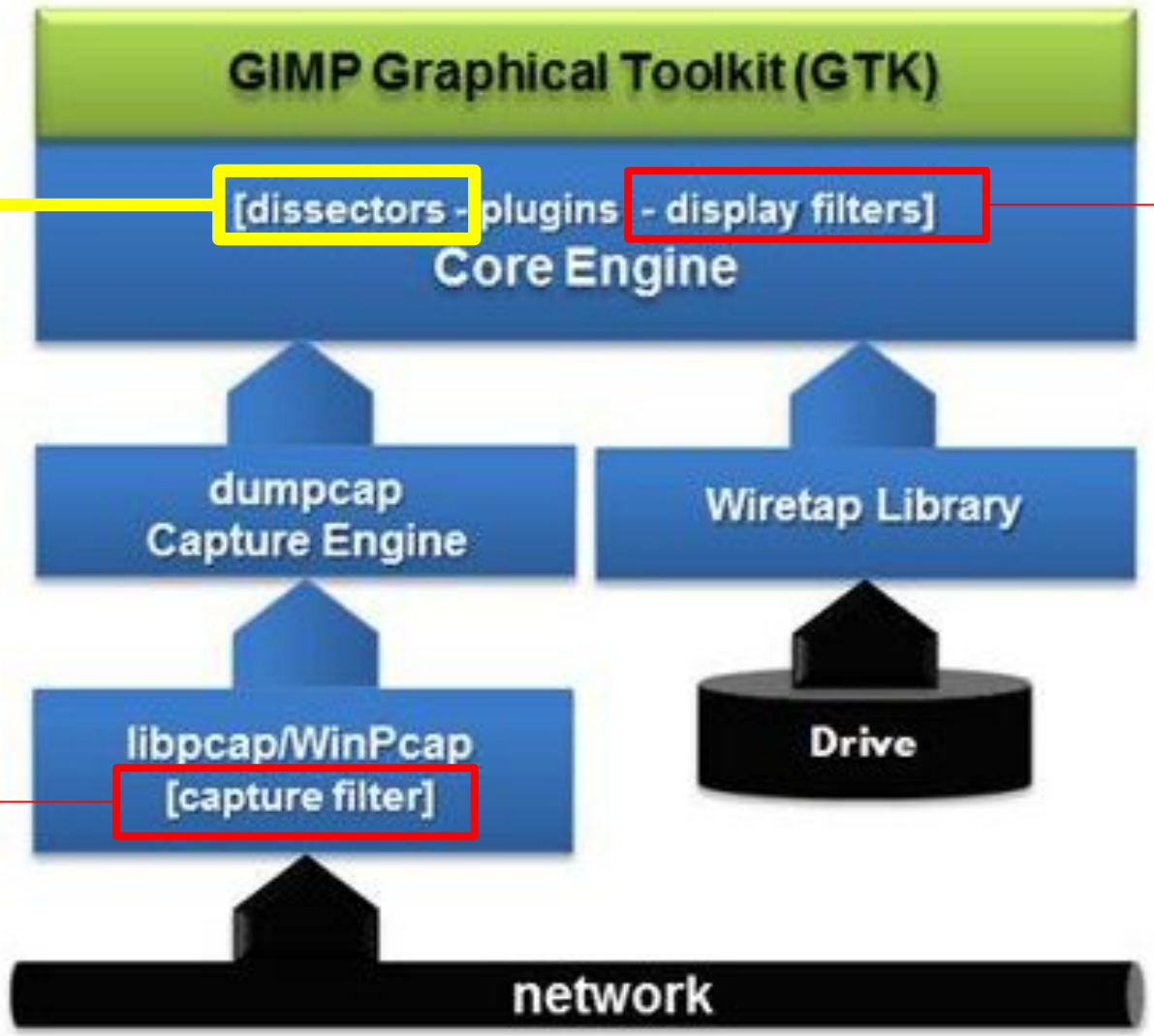
- **Прослуховувач пакетів/аналізатор протоколів.**
- **Мережевий інструмент із відкритим вихідним кодом.**
- **Актуальна версія інструмента Ethereal.**



https://www.wireshark.org/download.html

Як Wireshark захоплює трафік?

Розбирає елементи протоколу (тисячі їх)



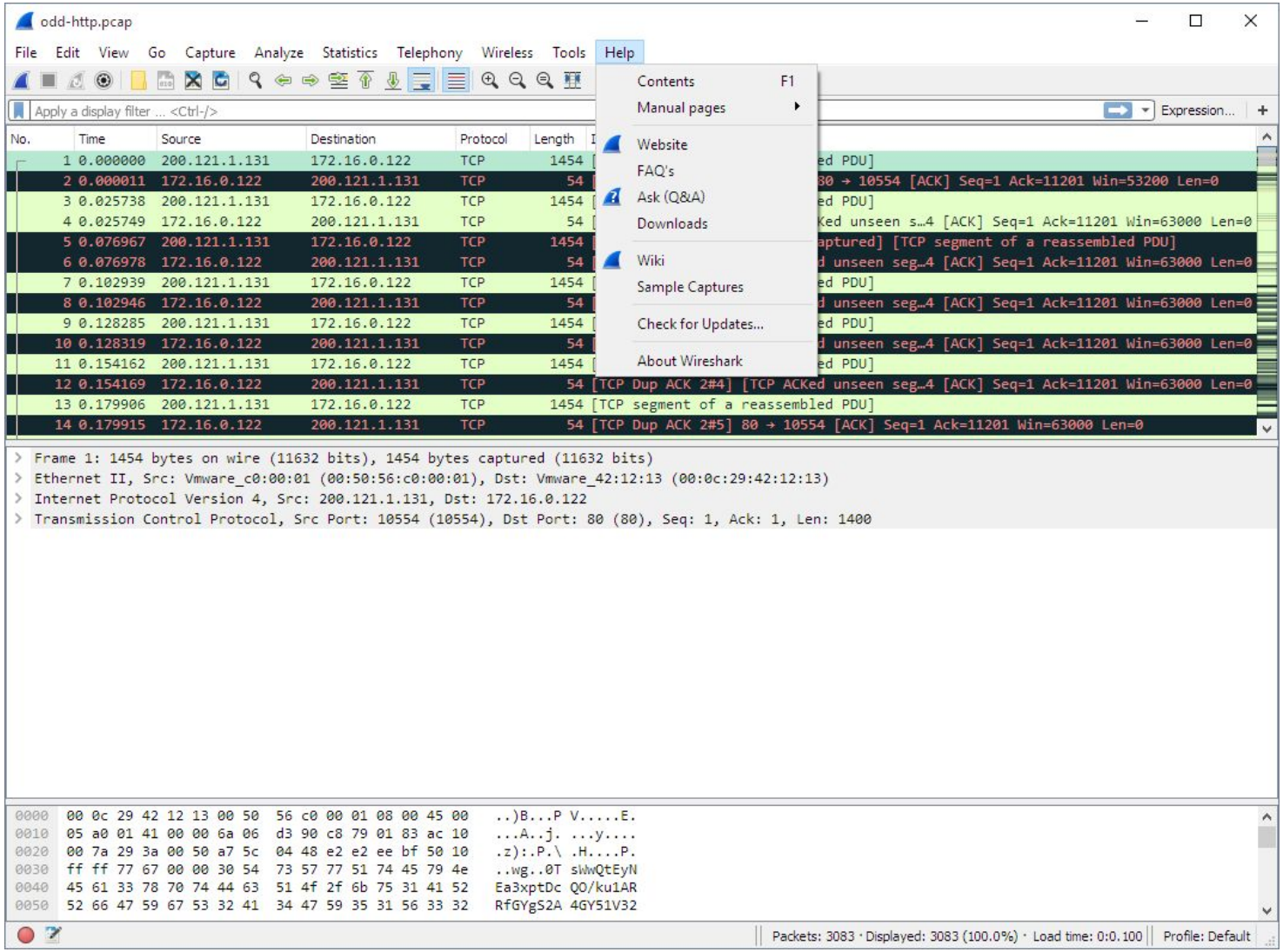
Оптимізує візуалізацію

Оптимізує зберігання

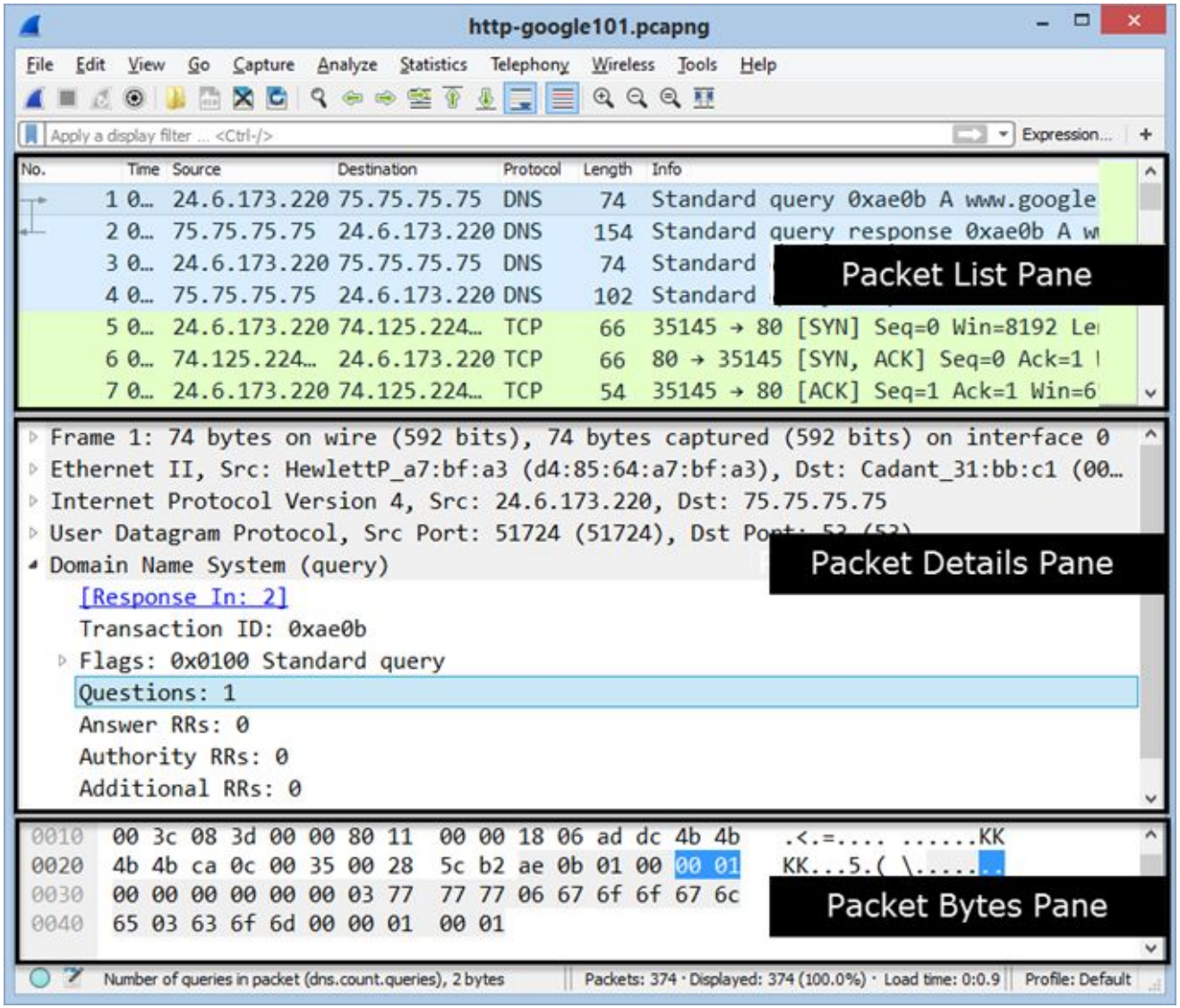
Основи: чому Wireshark?

- Вільний аналізатор протоколів із відкритим кодом.
- Простий у вивченні та використанні.
- Використовується фахівцями в різноманітних цілях:
  - загальний аналіз трафіку;
  - пошук і усунення несправностей;
  - безпековий аналіз;
  - аналіз програм.
- Підтримується багатьма ОС.

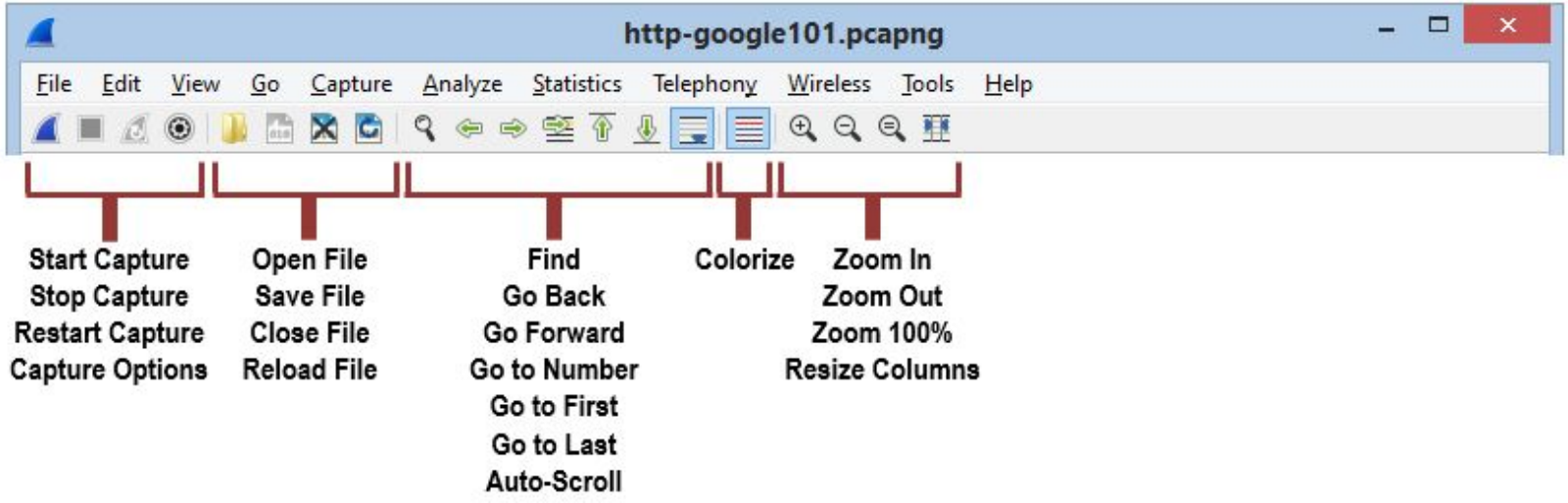
Меню «Help» (Довідка)

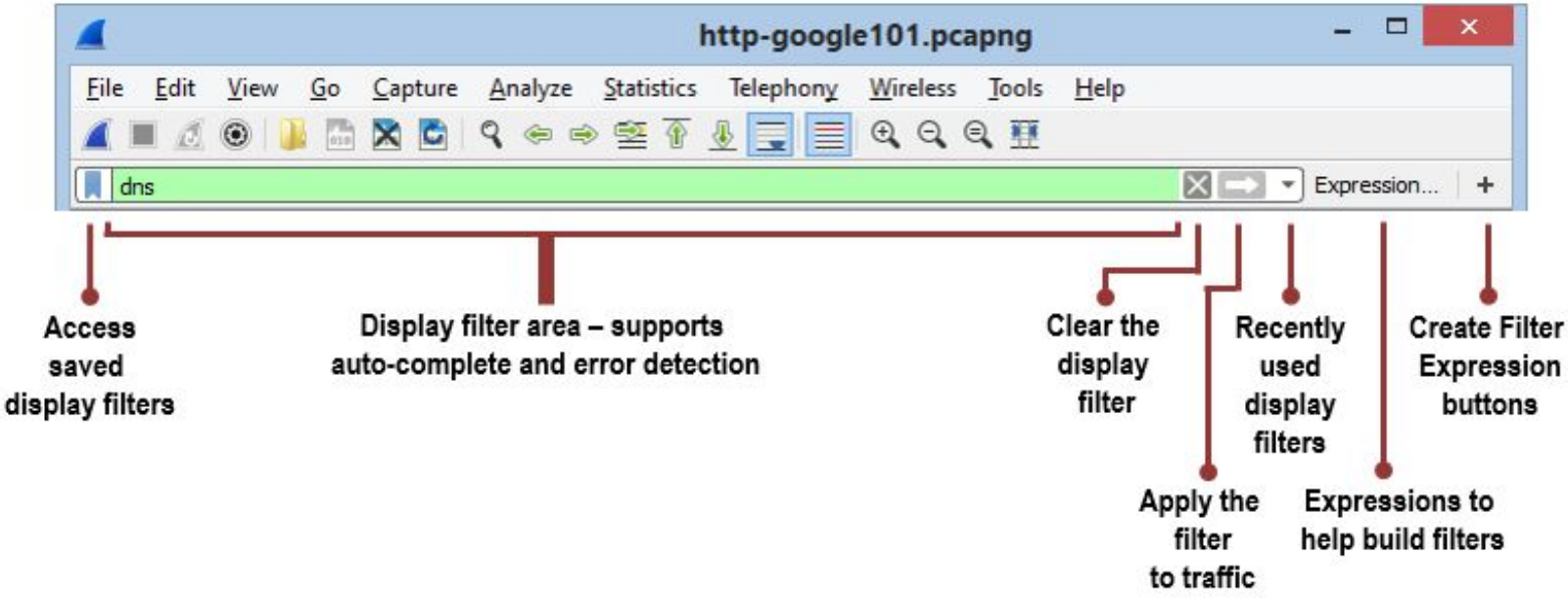


Подання з трьома областями за промовчанням



Використання основного представлення Wireshark



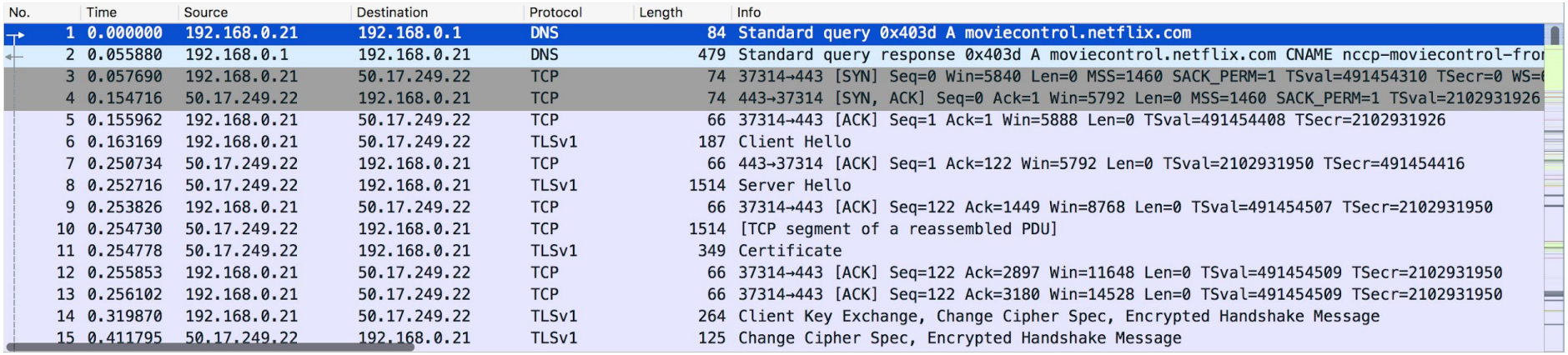


Фільтри відображення (постфільтри)

- Фільтри відображення (також відомі як постфільтри) відфільтровують тільки те, що виводиться на екран.
  - Захоплені пакети нікуди з трасування не подінуться.
- Фільтри відображення мають свій формат і набагато потужніші за фільтри захоплення.

Область «Packet List» (Список пакетів)

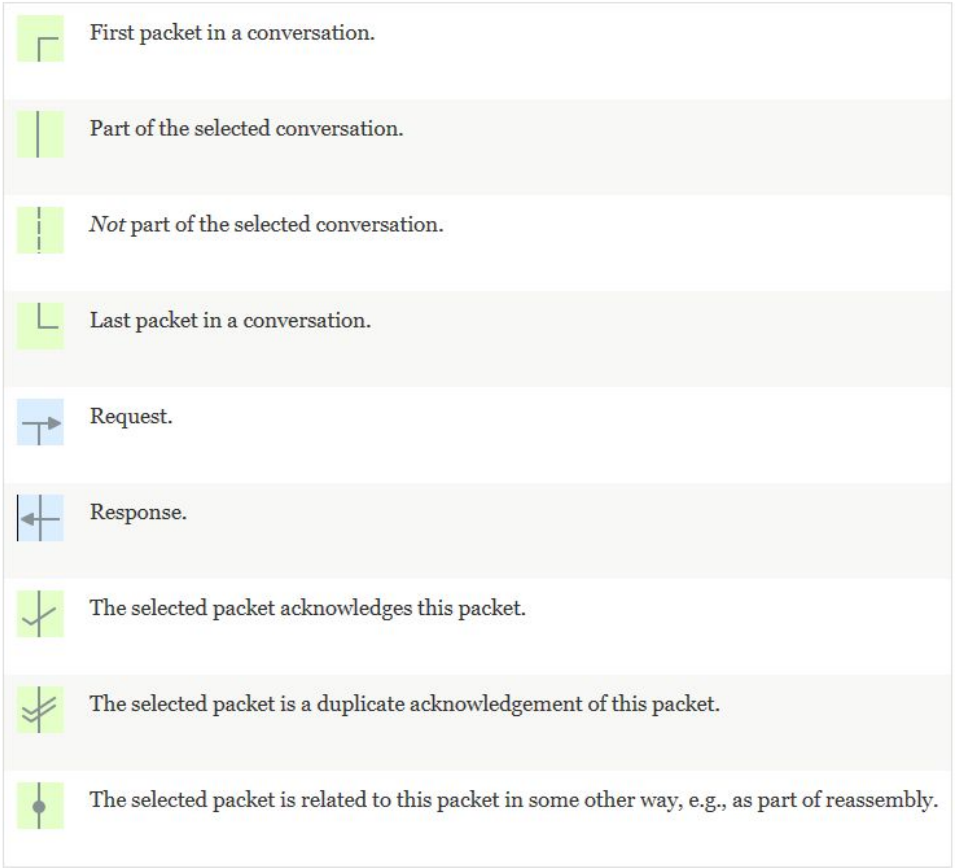
- **В області списку пакетів відображуються всі пакети в поточному файлі захоплення.**



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.21	192.168.0.1	DNS	84	Standard query 0x403d A moviecontrol.netflix.com
2	0.055880	192.168.0.1	192.168.0.21	DNS	479	Standard query response 0x403d A moviecontrol.netflix.com CNAME nccp-moviecontrol-fro
3	0.057690	192.168.0.21	50.17.249.22	TCP	74	37314→443 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491454310 TSecr=0 WS=
4	0.154716	50.17.249.22	192.168.0.21	TCP	74	443→37314 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=2102931926
5	0.155962	192.168.0.21	50.17.249.22	TCP	66	37314→443 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491454408 TSecr=2102931926
6	0.163169	192.168.0.21	50.17.249.22	TLSv1	187	Client Hello
7	0.250734	50.17.249.22	192.168.0.21	TCP	66	443→37314 [ACK] Seq=1 Ack=122 Win=5792 Len=0 TSval=2102931950 TSecr=491454416
8	0.252716	50.17.249.22	192.168.0.21	TLSv1	1514	Server Hello
9	0.253826	192.168.0.21	50.17.249.22	TCP	66	37314→443 [ACK] Seq=122 Ack=1449 Win=8768 Len=0 TSval=491454507 TSecr=2102931950
10	0.254730	50.17.249.22	192.168.0.21	TCP	1514	[TCP segment of a reassembled PDU]
11	0.254778	50.17.249.22	192.168.0.21	TLSv1	349	Certificate
12	0.255853	192.168.0.21	50.17.249.22	TCP	66	37314→443 [ACK] Seq=122 Ack=2897 Win=11648 Len=0 TSval=491454509 TSecr=2102931950
13	0.256102	192.168.0.21	50.17.249.22	TCP	66	37314→443 [ACK] Seq=122 Ack=3180 Win=14528 Len=0 TSval=491454509 TSecr=2102931950
14	0.319870	192.168.0.21	50.17.249.22	TLSv1	264	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
15	0.411795	50.17.249.22	192.168.0.21	TLSv1	125	Change Cipher Spec, Encrypted Handshake Message

Область «Packet List» (Список пакетів)

- Сім стовпців за промовчанням:
  - «No.» (№), «Time» (Час), «Source» (Джерело), «Destination» (Призначення), «Protocol» (Протокол), «Length» (Довжина), «Packet Information» (Інформація пакета).
- В першому стовпці зазначається, який стосунок кожен з пакетів має до вибраного пакета.

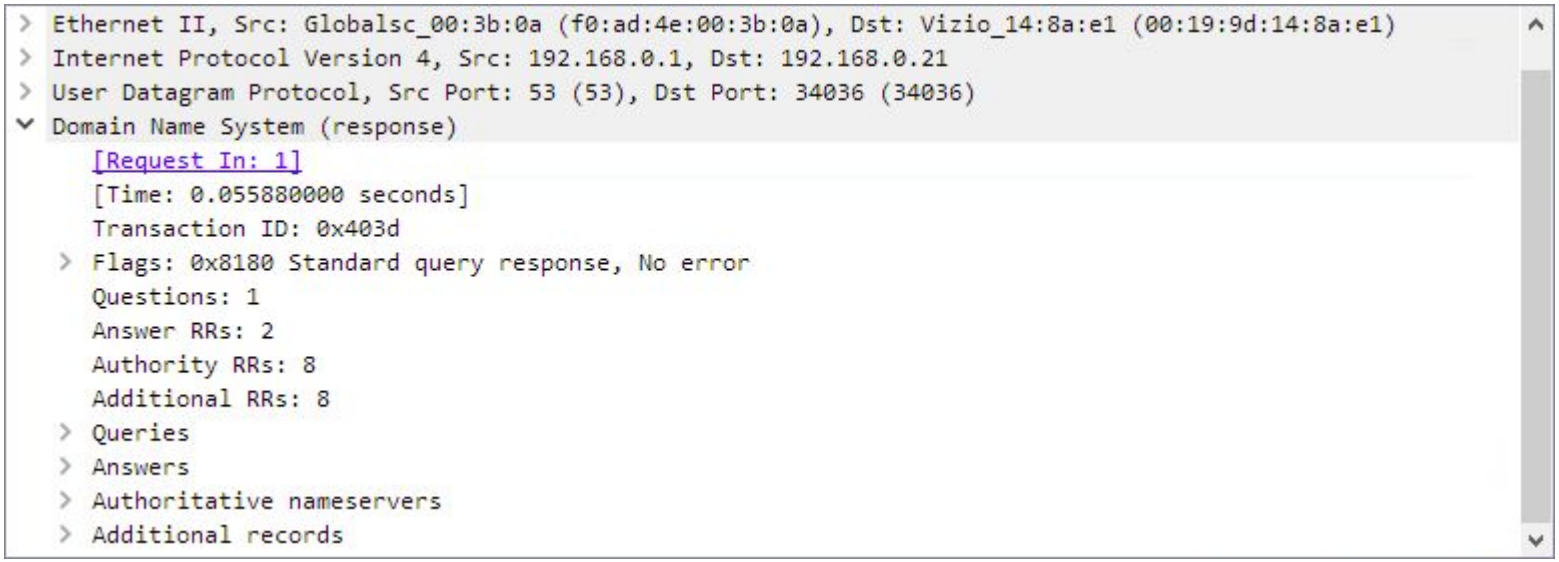


Використання області «Packet List» (Список пакетів)

- **Змінення порядку стовпців.**
- **Сортування інформації у стовпці:**
  - **тільки коли захоплення зупинене.**
- **Приховування, відображення, перейменування та видалення стовпців за натисненням правою кнопкою миші на заголовку стовпця.**
- **Перегляд доступних функцій за натисненням правою кнопкою миші в області «Packet List» (Список пакетів):**
  - **застосування фільтра;**
  - **розфарбовування трафіка;**
  - **повторне збирання трафіка;**
  - **розгортання всіх полів;**
  - **додавання стовпців;**
  - **та багато іншого.**

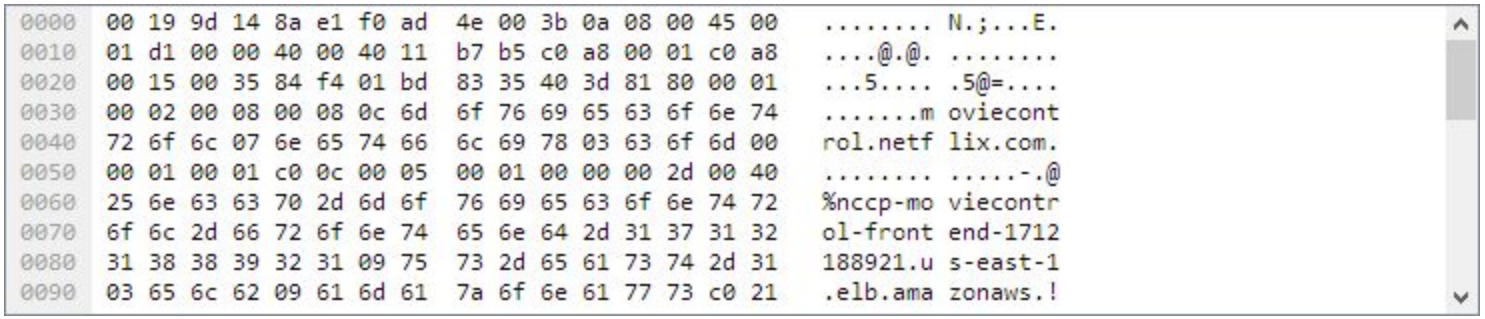
Область «Packet Details» (Деталі пакета)

- **Відображає протоколи та поля протоколів обраного пакета.**
- **Рядки опису протоколу (мітки піддерева) та поля пакета відображаються у формі дерева, яке можна розгортати та згортати.**



Область «Packet Bytes» (Байти пакета)

- **Відображає дані поточного пакета (вибраного в області «Packet List» (Список пакетів)) у шістнадцятковому поданні.**
  - **Кожен рядок містить зсув даних, 16 байтів у шістнадцятковому поданні та 16 байтів у ASCII-поданні. Замість недрукованих байтів підставляється крапка («.»).**

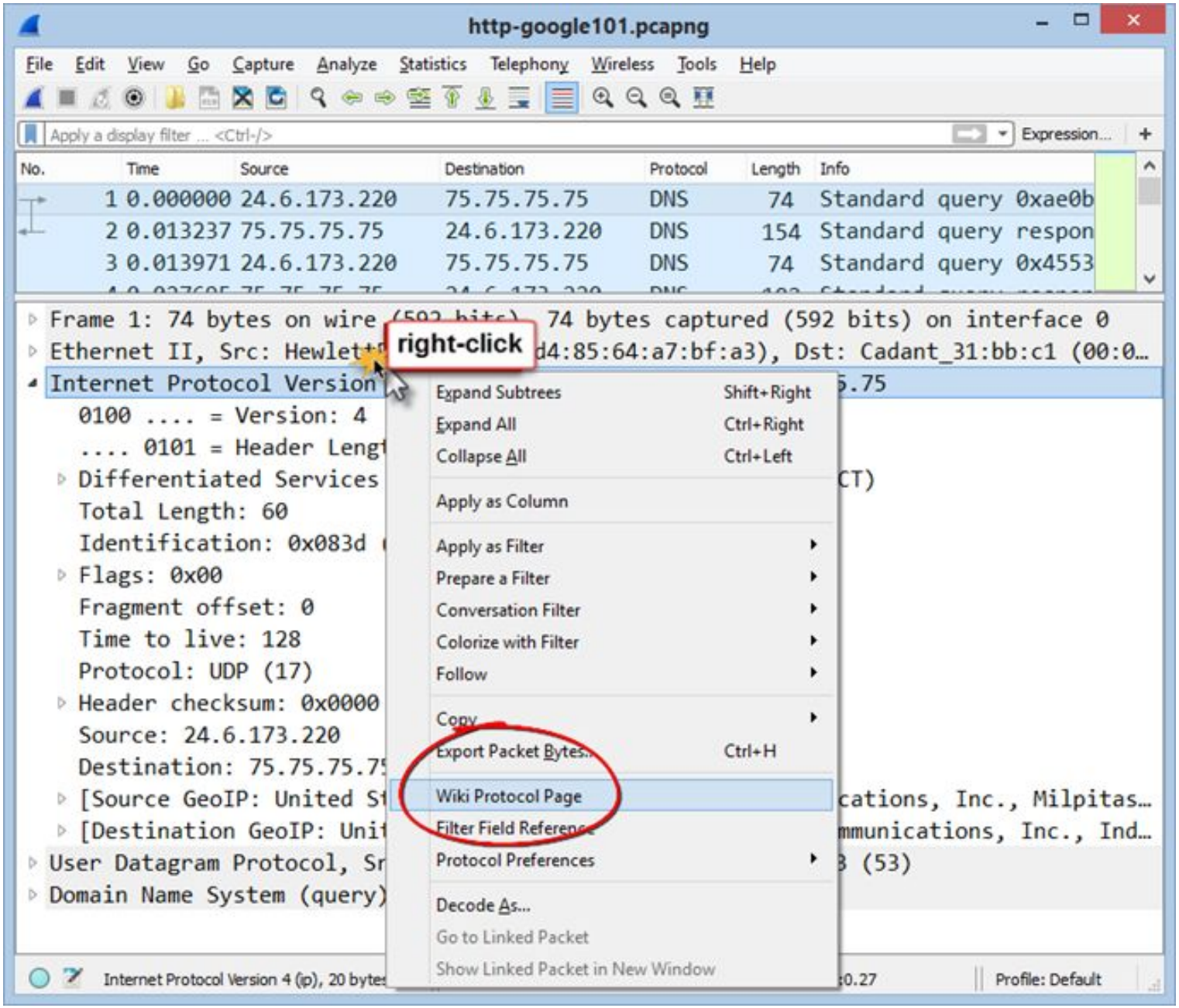


```
0000  00 19 9d 14 8a e1 f0 ad  4e 00 3b 0a 08 00 45 00   ........ N.;...E.
0010  01 d1 00 00 40 00 40 11  b7 b5 c0 a8 00 01 c0 a8   ....@.@. ........
0020  00 15 00 35 84 f4 01 bd  83 35 40 3d 81 80 00 01   ...5.... .5@=....
0030  00 02 00 08 00 08 0c 6d  6f 76 69 65 63 6f 6e 74   .......m oviecont
0040  72 6f 6c 07 6e 65 74 66  6c 69 78 03 63 6f 6d 00   rol.netf lix.com.
0050  00 01 00 01 c0 0c 00 05  00 01 00 00 00 2d 00 40   ........ .....-.@
0060  25 6e 63 63 70 2d 6d 6f  76 69 65 63 6f 6e 74 72   %nccp-mo viecontr
0070  6f 6c 2d 66 72 6f 6e 74  65 6e 64 2d 31 37 31 32   ol-front end-1712
0080  31 38 38 39 32 31 09 75  73 2d 65 61 73 74 2d 31   188921.u s-east-1
0090  03 65 6c 62 09 61 6d 61  7a 6f 6e 61 77 73 c0 21   .elb.ama zonaws.!
```

Куди податися, якщо не вдається розпізнати протокол?

- Google.
- wiki.wireshark.org:
  - якщо протокол визначений користувачем, результати можуть різнитися;
  - в загальному випадку достатньо ввести адресу wiki.wireshark.org/<протокол>,
    - наприклад: wiki.wireshark.org/SSDP;
  - домашня сторінка: wiki.wireshark.org/ProtocolReference;
    - можна переглядати за сімействами протоколів;
  - описи фільтрів відображення (http://www.wireshark.org/docs/dfref/):
    - визначення конкретних полів для кожного протоколу.

Ресурс Wireshark: вікісторінки



Кінець