Sniffery

- Narzędzia do
  - Przechwytywania danych przesyłanych w sieci
  - Analizowania tych danych

- Wykorzystanie
  - Diagnostyka sieci (administratorzy)
    - Problemy z wydajnością lub niezawodnością
    - Wykrywanie potencjalnych intruzów
  - Monitorowanie aktywności użytkowników trzecich w sieci
    - Niezgodne z prawem!
    - W celu ochrony stosowana kryptografia

Sniffery

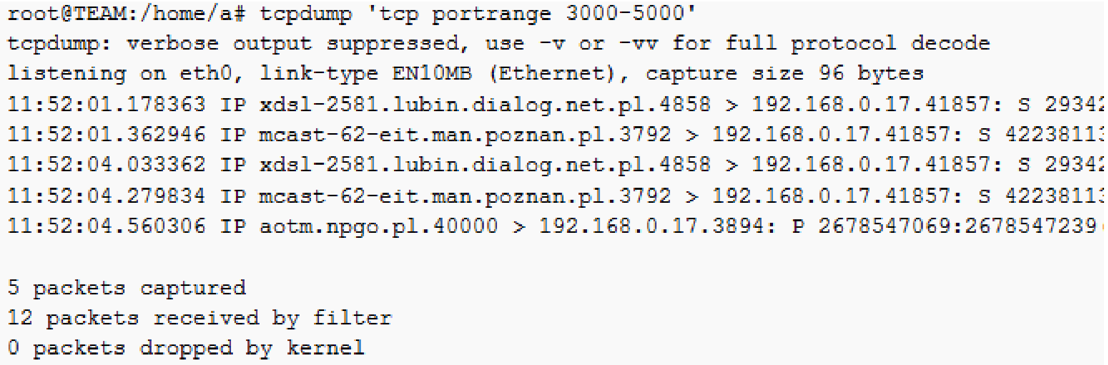
- W sieci Ethernet istnieje możliwość odczytywania także danych, które nie są przeznaczone dla nas!
  – Po ustawieniu karty sieciowej w odpowiedni tryb

Ale o tym porozmawiamy przy okazji omawiania niższych warstw modelu Internetu…

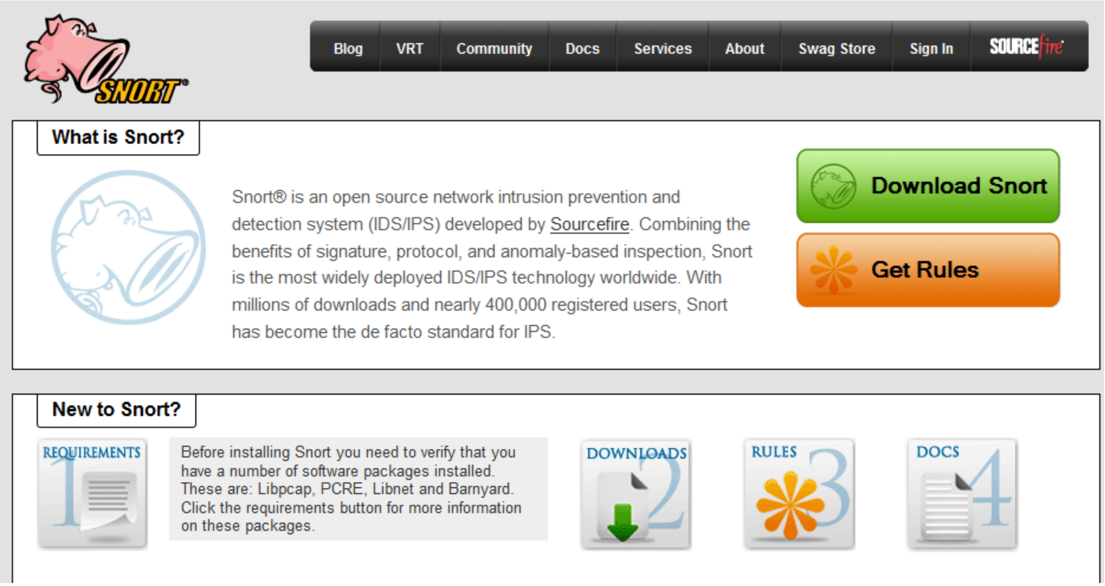
Sniffery

- Programy
  - wireshark
  - tcpdump
  - snort

    http://www.snort.org/



```
root@TEAM:/home/a# tcpdump 'tcp portrange 3000-5000'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
11:52:01.178363 IP xdsl-2581.lubin.dialog.net.pl.4858 > 192.168.0.17.41857: S 29342
11:52:01.362946 IP mcast-62-eit.man.poznan.pl.3792 > 192.168.0.17.41857: S 4223811
11:52:04.033362 IP xdsl-2581.lubin.dialog.net.pl.4858 > 192.168.0.17.41857: S 29342
11:52:04.279834 IP mcast-62-eit.man.poznan.pl.3792 > 192.168.0.17.41857: S 4223811
11:52:04.560306 IP aotm.npgo.pl.40000 > 192.168.0.17.3894: P 2678547069:2678547239

5 packets captured
12 packets received by filter
0 packets dropped by kernel
```



What is Snort?

Snort® is an open source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire. Combining the benefits of signature, protocol, and anomaly-based inspection, Snort is the most widely deployed IDS/IPS technology worldwide. With millions of downloads and nearly 400,000 registered users, Snort has become the de facto standard for IPS.

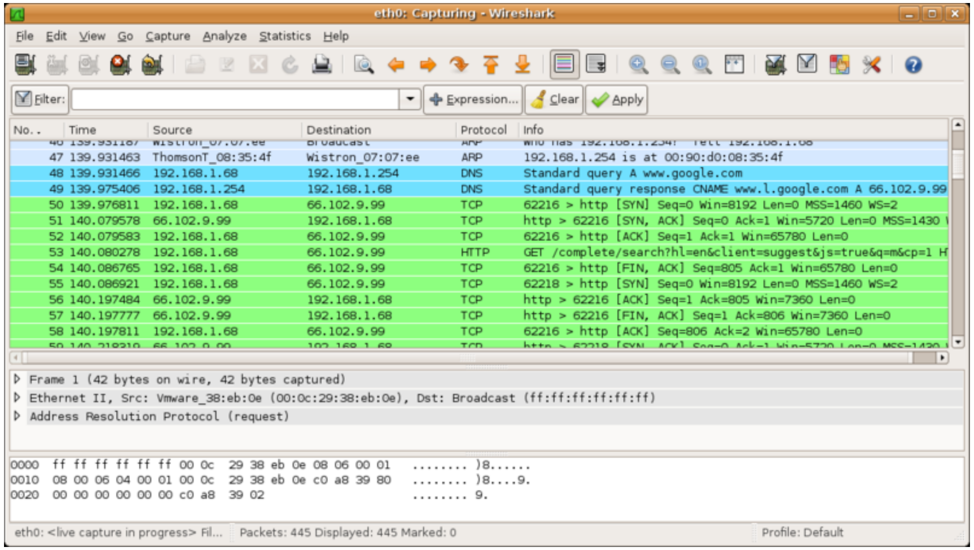
New to Snort?

Before installing Snort you need to verify that you have a number of software packages installed. These are: Libpcap, PCRE, Libnet and Barnyard. Click the requirements button for more information on these packages.

Wireshark

http://www.wireshark.org/

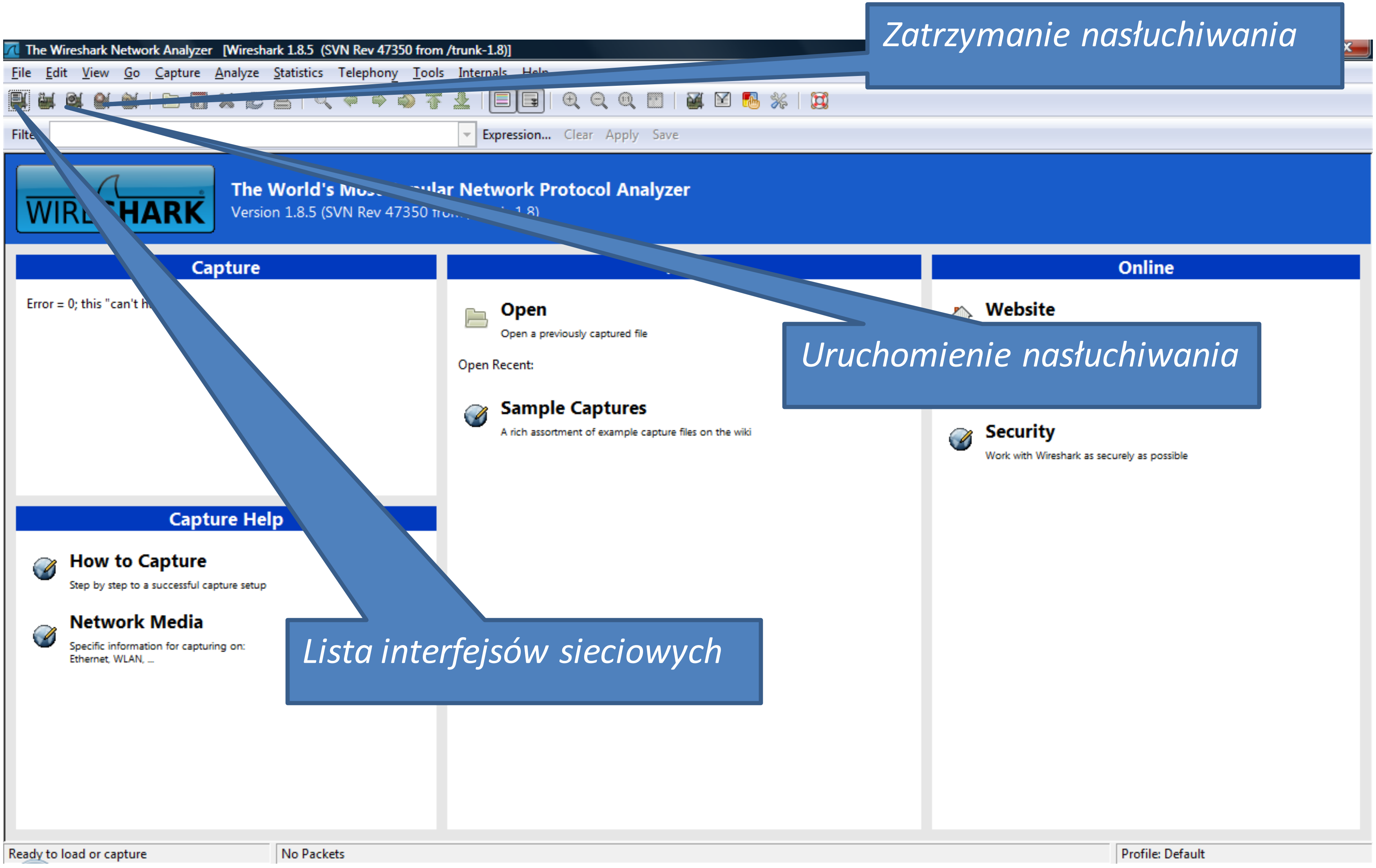
Gerald Combs


eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply

```
No. .  Time        Source             Destination        Protocol  Info
   46 139.931187  Wistron_07:07:ee   Broadcast          ARP       Who has 192.168.1.254?  Tell 192.168.1.68
   47 139.931463  ThomsonT_08:35:4f  Wistron_07:07:ee   ARP       192.168.1.254 is at 00:90:d0:08:35:4f
   48 139.931466  192.168.1.68       192.168.1.254      DNS       Standard query A www.google.com
   49 139.975406  192.168.1.254      192.168.1.68       DNS       Standard query response CNAME www.l.google.com A 66.102.9.99
   50 139.976811  192.168.1.68       66.102.9.99        TCP       62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
   51 140.079578  66.102.9.99        192.168.1.68       TCP       http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 \
   52 140.079583  192.168.1.68       66.102.9.99        TCP       62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
   53 140.080278  192.168.1.68       66.102.9.99        HTTP      GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
   54 140.086765  192.168.1.68       66.102.9.99        TCP       62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
   55 140.086921  192.168.1.68       66.102.9.99        TCP       62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
   56 140.197484  66.102.9.99        192.168.1.68       TCP       http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
   57 140.197777  66.102.9.99        192.168.1.68       TCP       http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
   58 140.197811  192.168.1.68       66.102.9.99        TCP       62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
   59 140.218319  66.102.9.99        192.168.1.68       TCP       http > 62218 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 \

▷ Frame 1 (42 bytes on wire, 42 bytes captured)
▷ Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 0c  29 38 eb 0e 08 06 00 01   ........ )8......
0010  08 00 06 04 00 01 00 0c  29 38 eb 0e c0 a8 39 80   ........ )8....9.
0020  00 00 00 00 00 00 c0 a8  39 02                     ........ 9.

eth0: <live capture in progress> Fil...   Packets: 445 Displayed: 445 Marked: 0      Profile: Default
```

- Dawniej Ethereal
- Sniffer
  - Wieloplatformowy
  - Posiada graficzny interfejs użytkownika

Wireshark



The Wireshark Network Analyzer [Wireshark 1.8.5 (SVN Rev 47350 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filte
Expression... Clear Apply Save
WIRESHARK

The World's Mos ular Network Protocol Analyzer

Version 1.8.5 (SVN Rev 47350 fro 1.8)

Error = 0; this "can't h

Capture Help
How to Capture

Step by step to a successful capture setup

Specific information for capturing on: Ethernet, WLAN, ...

Open a previously captured file

Open Recent:

A rich assortment of example capture files on the wiki

Work with Wireshark as securely as possible

Ready to load or capture

No Packets

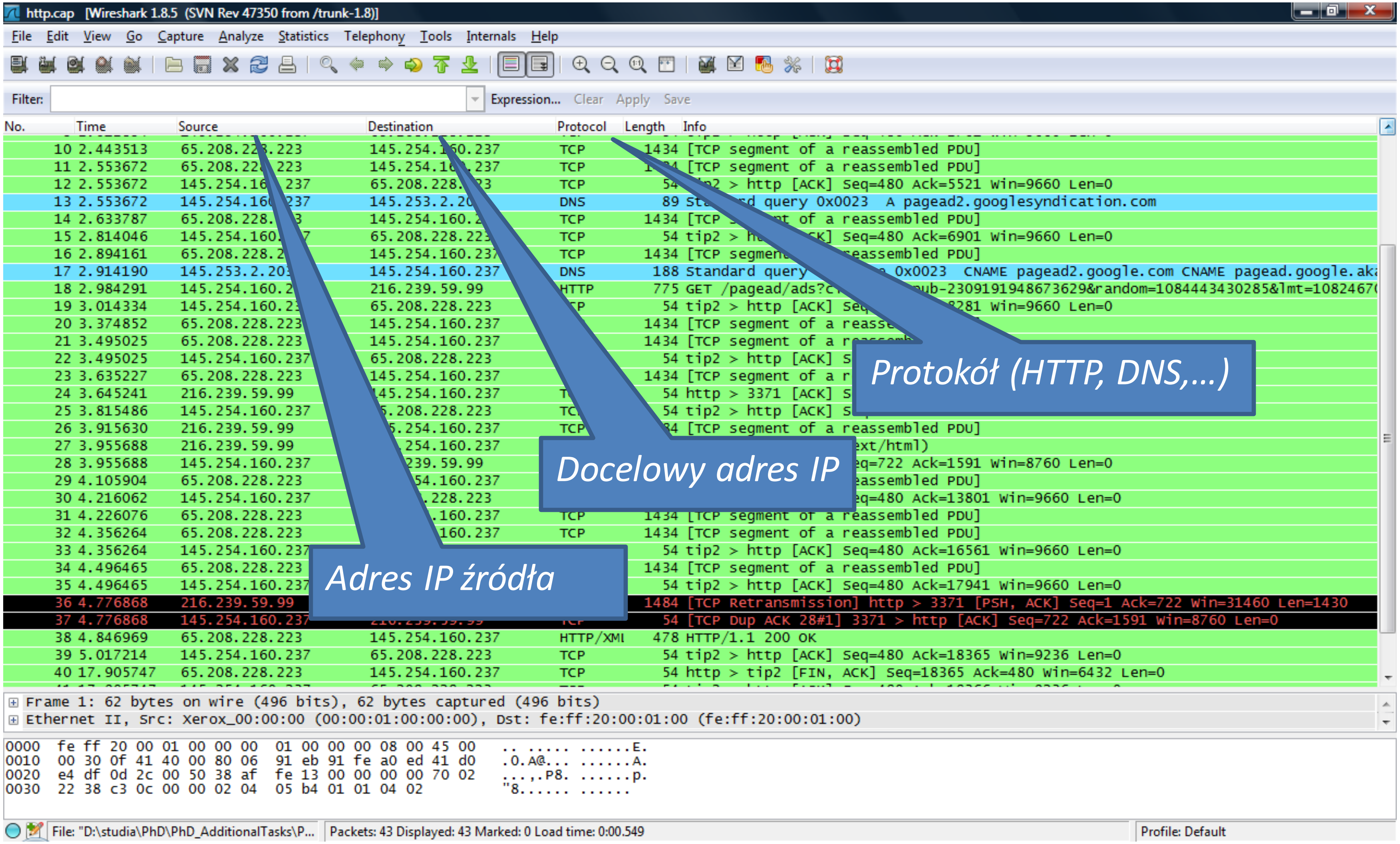
Profile: Default

Zatrzymanie nasłuchiwania

Uruchomienie nasłuchiwania

Lista interfejsów sieciowych

Wireshark



http.cap [Wireshark 1.8.5 (SVN Rev 47350 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.    Time       Source            Destination       Protocol  Length  Info
    10 2.443513   65.208.22 .223    145.254.1 0.237   TCP       1434 [TCP segment of a reassembled PDU]
    11 2.553672   65.208.22  223    145.254.16 .237   TCP       1 34 [TCP segment of a reassembled PDU]
    12 2.553672   145.254.16  237   65.208.228. 3     TCP         54   2 > http [ACK] Seq=480 Ack=5521 Win=9660 Len=0
    13 2.553672   145.254.160 237   145.253.2.20      DNS         89 St   rd query 0x0023  A pagead2.googlesyndication.com
    14 2.633787   65.208.228.   3   145.254.160.2     TCP       1434 [TCP     nt of a reassembled PDU]
    15 2.814046   145.254.160.  7   65.208.228.22     TCP         54 tip2 > h     K] Seq=480 Ack=6901 Win=9660 Len=0
    16 2.894161   65.208.228.2      145.254.160.23    TCP       1434 [TCP segmen      eassembled PDU]
    17 2.914190   145.253.2.20      145.254.160.237   DNS        188 Standard query       0x0023  CNAME pagead2.google.com CNAME pagead.google.aka
    18 2.984291   145.254.160.2     216.239.59.99     HTTP       775 GET /pagead/ads?c        ub-2309191948673629&random=1084443430285&lmt=10824670
    19 3.014334   145.254.160.2     65.208.228.223     P          54 tip2 > http [ACK] Seq        281 Win=9660 Len=0
    20 3.374852   65.208.228.223    145.254.160.237             1434 [TCP segment of a reasse
    21 3.495025   65.208.228.223    145.254.160.237             1434 [TCP segment of a r
    22 3.495025   145.254.160.237   65.208.228.223                54 tip2 > http [ACK] S
    23 3.635227   65.208.228.223    145.254.160.237             1434 [TCP segment of a r
    24 3.645241   216.239.59.99     145.254.160.237   T           54 http > 3371 [ACK] S
    25 3.815486   145.254.160.237   5.208.228.223     TC          54 tip2 > http [ACK] S
    26 3.915630   216.239.59.99     5.254.160.237     TCP         4 [TCP segment of a reassembled PDU]
    27 3.955688   216.239.59.99     .254.160.237                     ext/html)
    28 3.955688   145.254.160.237   239.59.99                        eq=722 Ack=1591 Win=8760 Len=0
    29 4.105904   65.208.228.223    54.160.237                       eassembled PDU]
    30 4.216062   145.254.160.237   .228.223                         eq=480 Ack=13801 Win=9660 Len=0
    31 4.226076   65.208.228.223    .160.237          TCP       1434 [TCP segment of a reassembled PDU]
    32 4.356264   65.208.228.223    .160.237          TCP       1434 [TCP segment of a reassembled PDU]
    33 4.356264   145.254.160.237                                 54 tip2 > http [ACK] Seq=480 Ack=16561 Win=9660 Len=0
    34 4.496465   65.208.228.223                                1434 [TCP segment of a reassembled PDU]
    35 4.496465   145.254.160.237                                 54 tip2 > http [ACK] Seq=480 Ack=17941 Win=9660 Len=0
    36 4.776868   216.239.59.99                                 1484 [TCP Retransmission] http > 3371 [PSH, ACK] Seq=1 Ack=722 Win=31460 Len=1430
    37 4.776868   145.254.160.237                                 54 [TCP Dup ACK 28#1] 3371 > http [ACK] Seq=722 Ack=1591 Win=8760 Len=0
    38 4.846969   65.208.228.223    145.254.160.237   HTTP/XMl   478 HTTP/1.1 200 OK
    39 5.017214   145.254.160.237   65.208.228.223    TCP         54 tip2 > http [ACK] Seq=480 Ack=18365 Win=9236 Len=0
    40 17.905747  65.208.228.223    145.254.160.237   TCP         54 http > tip2 [FIN, ACK] Seq=18365 Ack=480 Win=6432 Len=0
```

```
⊞ Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
⊞ Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
```

```
0000  fe ff 20 00 01 00 00 00  01 00 00 00 08 00 45 00   .. ..... ......E.
0010  00 30 0f 41 40 00 80 06  91 eb 91 fe a0 ed 41 d0   .0.A@... ......A.
0020  e4 df 0d 2c 00 50 38 af  fe 13 00 00 00 00 70 02   ...,.P8. ......p.
0030  22 38 c3 0c 00 00 02 04  05 b4 01 01 04 02         "8...... ......
```

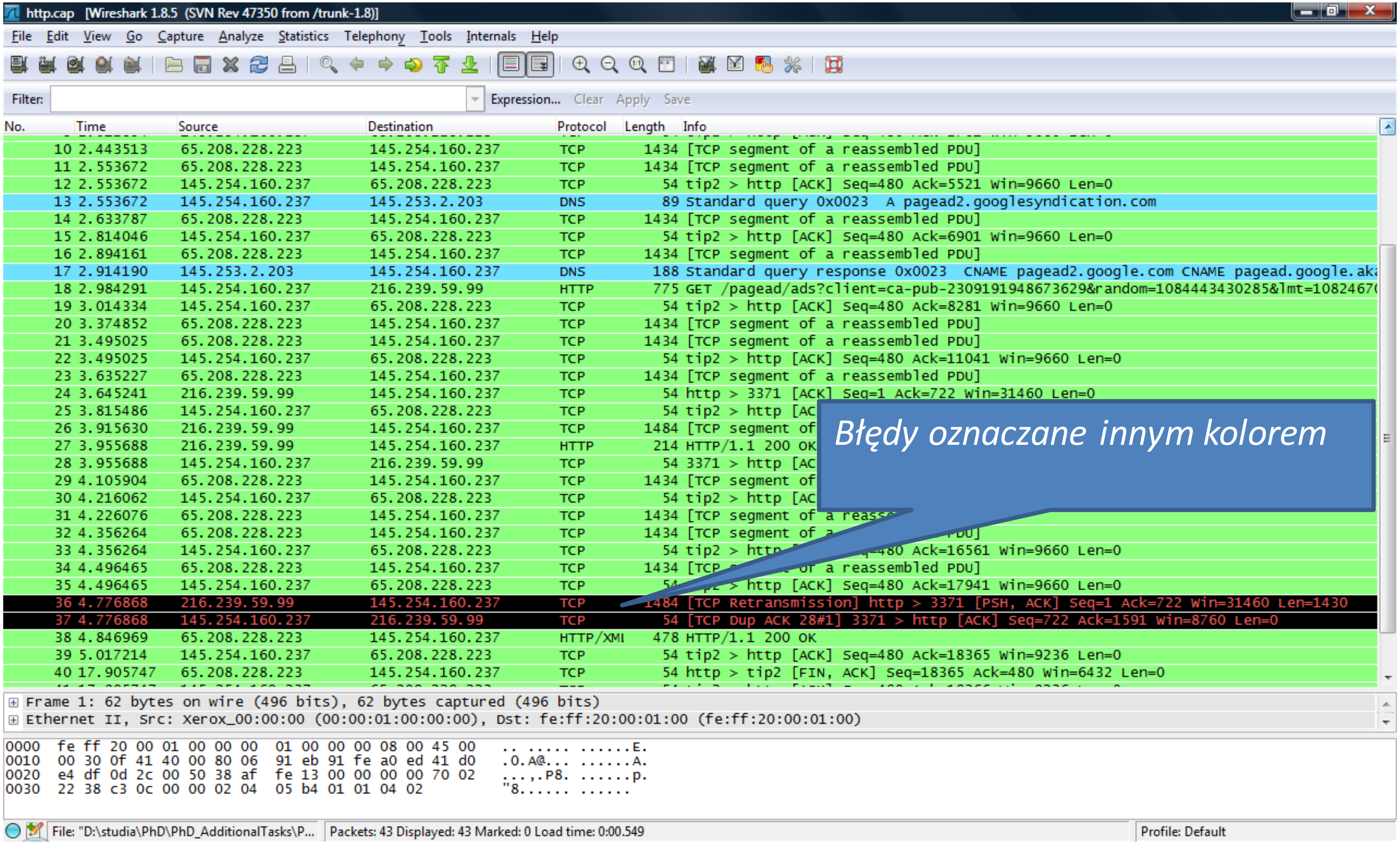
File: "D:\studia\PhD\PhD_AdditionalTasks\P... Packets: 43 Displayed: 43 Marked: 0 Load time: 0:00.549 Profile: Default

Protokół (HTTP, DNS,...)

Docelowy adres IP

Adres IP źródła

Wireshark



http.cap [Wireshark 1.8.5 (SVN Rev 47350 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.   Time      Source           Destination      Protocol Length Info
   10 2.443513  65.208.228.223   145.254.160.237  TCP      1434 [TCP segment of a reassembled PDU]
   11 2.553672  65.208.228.223   145.254.160.237  TCP      1434 [TCP segment of a reassembled PDU]
   12 2.553672  145.254.160.237  65.208.228.223   TCP        54 tip2 > http [ACK] Seq=480 Ack=5521 Win=9660 Len=0
   13 2.553672  145.254.160.237  145.253.2.203    DNS        89 Standard query 0x0023  A pagead2.googlesyndication.com
   14 2.633787  65.208.228.223   145.254.160.237  TCP      1434 [TCP segment of a reassembled PDU]
   15 2.814046  145.254.160.237  65.208.228.223   TCP        54 tip2 > http [ACK] Seq=480 Ack=6901 Win=9660 Len=0
   16 2.894161  65.208.228.223   145.254.160.237  TCP      1434 [TCP segment of a reassembled PDU]
   17 2.914190  145.253.2.203    145.254.160.237  DNS       188 Standard query response 0x0023  CNAME pagead2.google.com CNAME pagead.google.aka
   18 2.984291  145.254.160.237  216.239.59.99    HTTP      775 GET /pagead/ads?client=ca-pub-2309191948673629&random=1084443430285&lmt=1082467
   19 3.014334  145.254.160.237  65.208.228.223   TCP        54 tip2 > http [ACK] Seq=480 Ack=8281 Win=9660 Len=0
   20 3.374852  65.208.228.223   145.254.160.237  TCP      1434 [TCP segment of a reassembled PDU]
   21 3.495025  65.208.228.223   145.254.160.237  TCP      1434 [TCP segment of a reassembled PDU]
   22 3.495025  145.254.160.237  65.208.228.223   TCP        54 tip2 > http [ACK] Seq=480 Ack=11041 Win=9660 Len=0
   23 3.635227  65.208.228.223   145.254.160.237  TCP      1434 [TCP segment of a reassembled PDU]
   24 3.645241  216.239.59.99    145.254.160.237  TCP        54 http > 3371 [ACK] Seq=1 Ack=722 Win=31460 Len=0
   25 3.815486  145.254.160.237  65.208.228.223   TCP        54 tip2 > http [AC
   26 3.915630  216.239.59.99    145.254.160.237  TCP      1484 [TCP segment of
   27 3.955688  216.239.59.99    145.254.160.237  HTTP      214 HTTP/1.1 200 OK
   28 3.955688  145.254.160.237  216.239.59.99    TCP        54 3371 > http [AC
   29 4.105904  65.208.228.223   145.254.160.237  TCP      1434 [TCP segment of
   30 4.216062  145.254.160.237  65.208.228.223   TCP        54 tip2 > http [AC
   31 4.226076  65.208.228.223   145.254.160.237  TCP      1434 [TCP segment of a reass
   32 4.356264  65.208.228.223   145.254.160.237  TCP      1434 [TCP segment of a          PDU]
   33 4.356264  145.254.160.237  65.208.228.223   TCP        54 tip2 > http        480 Ack=16561 Win=9660 Len=0
   34 4.496465  65.208.228.223   145.254.160.237  TCP      1434 [TCP        of a reassembled PDU]
   35 4.496465  145.254.160.237  65.208.228.223   TCP        54        > http [ACK] Seq=480 Ack=17941 Win=9660 Len=0
   36 4.776868  216.239.59.99    145.254.160.237  TCP      1484 [TCP Retransmission] http > 3371 [PSH, ACK] Seq=1 Ack=722 Win=31460 Len=1430
   37 4.776868  145.254.160.237  216.239.59.99    TCP        54 [TCP Dup ACK 28#1] 3371 > http [ACK] Seq=722 Ack=1591 Win=8760 Len=0
   38 4.846969  65.208.228.223   145.254.160.237  HTTP/XMl  478 HTTP/1.1 200 OK
   39 5.017214  145.254.160.237  65.208.228.223   TCP        54 tip2 > http [ACK] Seq=480 Ack=18365 Win=9236 Len=0
   40 17.905747 65.208.228.223   145.254.160.237  TCP        54 http > tip2 [FIN, ACK] Seq=18365 Ack=480 Win=6432 Len=0
```

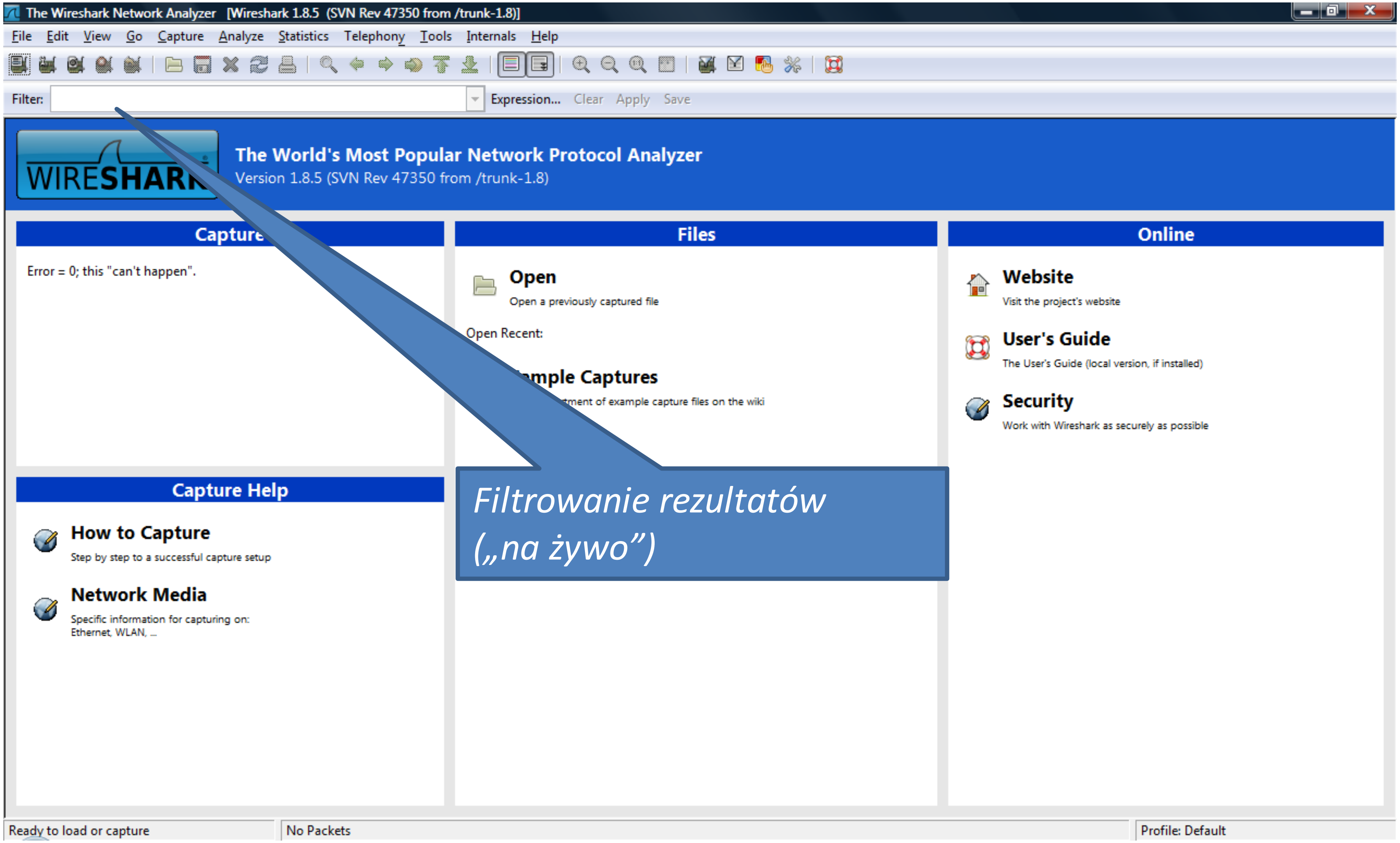
```
⊞ Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
⊞ Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
```

```
0000  fe ff 20 00 01 00 00 00  01 00 00 00 08 00 45 00   .. ..... ......E.
0010  00 30 0f 41 40 00 80 06  91 eb 91 fe a0 ed 41 d0   .0.A@... ......A.
0020  e4 df 0d 2c 00 50 38 af  fe 13 00 00 00 00 70 02   ...,.P8. ......p.
0030  22 38 c3 0c 00 00 02 04  05 b4 01 01 04 02         "8...... ......
```

File: "D:\studia\PhD\PhD_AdditionalTasks\P... | Packets: 43 Displayed: 43 Marked: 0 Load time: 0:00.549 | Profile: Default

Błędy oznaczane innym kolorem

Wireshark



The Wireshark Network Analyzer [Wireshark 1.8.5 (SVN Rev 47350 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
WIRESHARK

The World's Most Popular Network Protocol Analyzer
Version 1.8.5 (SVN Rev 47350 from /trunk-1.8)

Error = 0; this "can't happen".

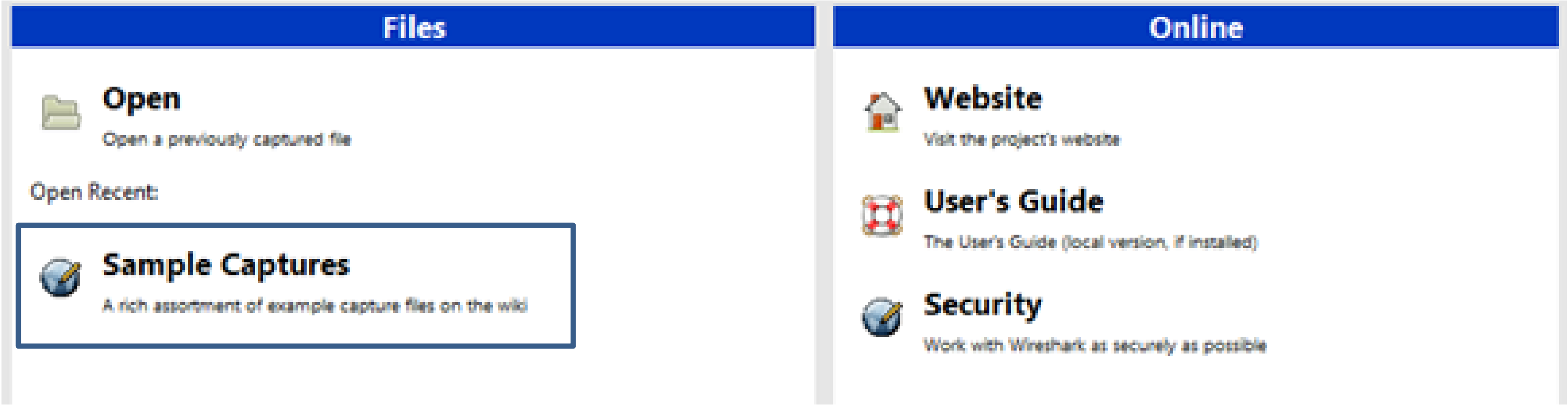
Files
Open
Open a previously captured file
Open Recent:
mple Captures
tment of example capture files on the wiki
Online
Website
Visit the project's website
User's Guide
The User's Guide (local version, if installed)
Security
Work with Wireshark as securely as possible
Capture Help
How to Capture
Step by step to a successful capture setup
Network Media
Specific information for capturing on:
Ethernet, WLAN, ...
Ready to load or capture
No Packets
Profile: Default

Filtrowanie rezultatów („na żywo”)

Wireshark

- Przykładowe pliki z zapisanymi danymi

  http://wiki.wireshark.org/SampleCaptures



Files

Open

Open a previously captured file

Open Recent:

Sample Captures

A rich assortment of example capture files on the wiki

Online

Website

Visit the project's website

User's Guide

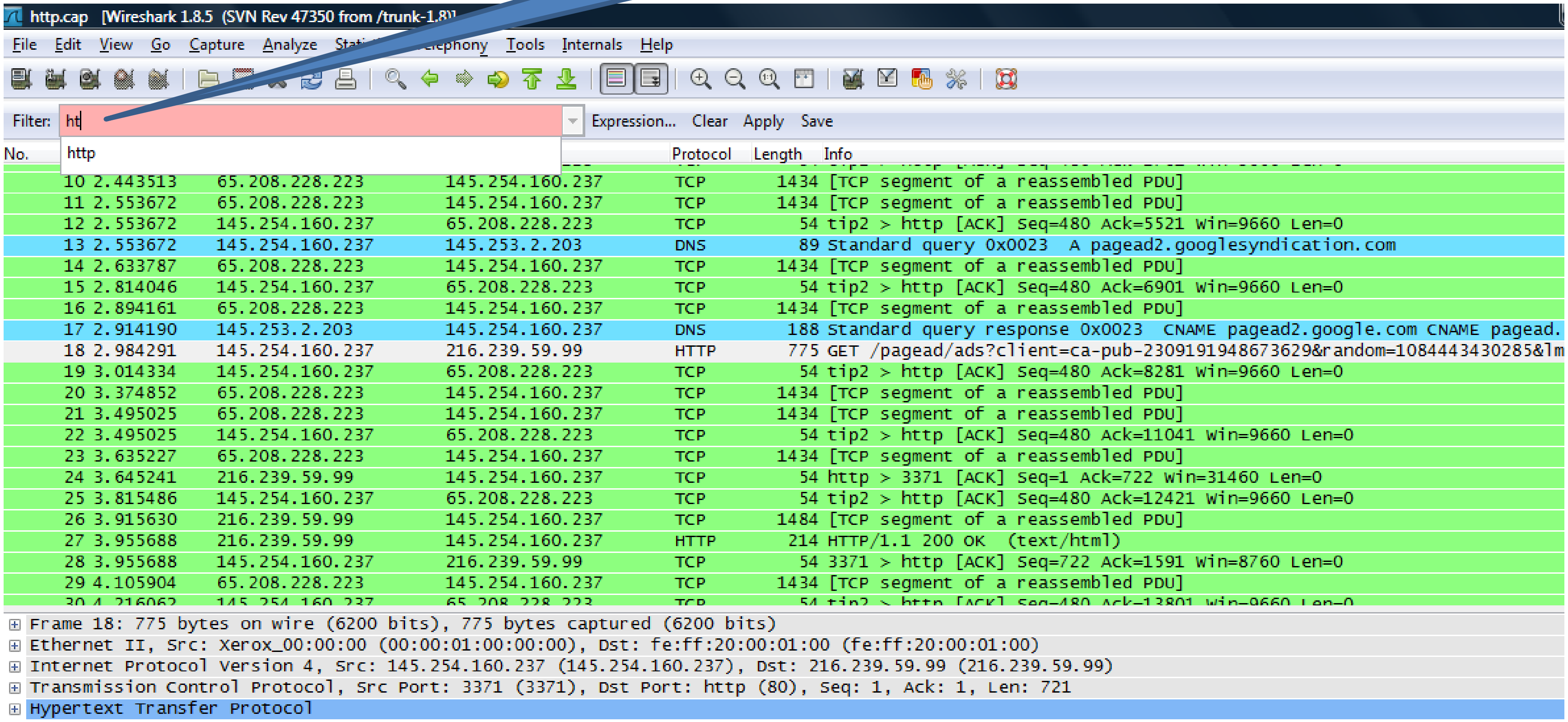
The User's Guide (local version, if installed)

Security

Work with Wireshark as securely as possible

Wireshark

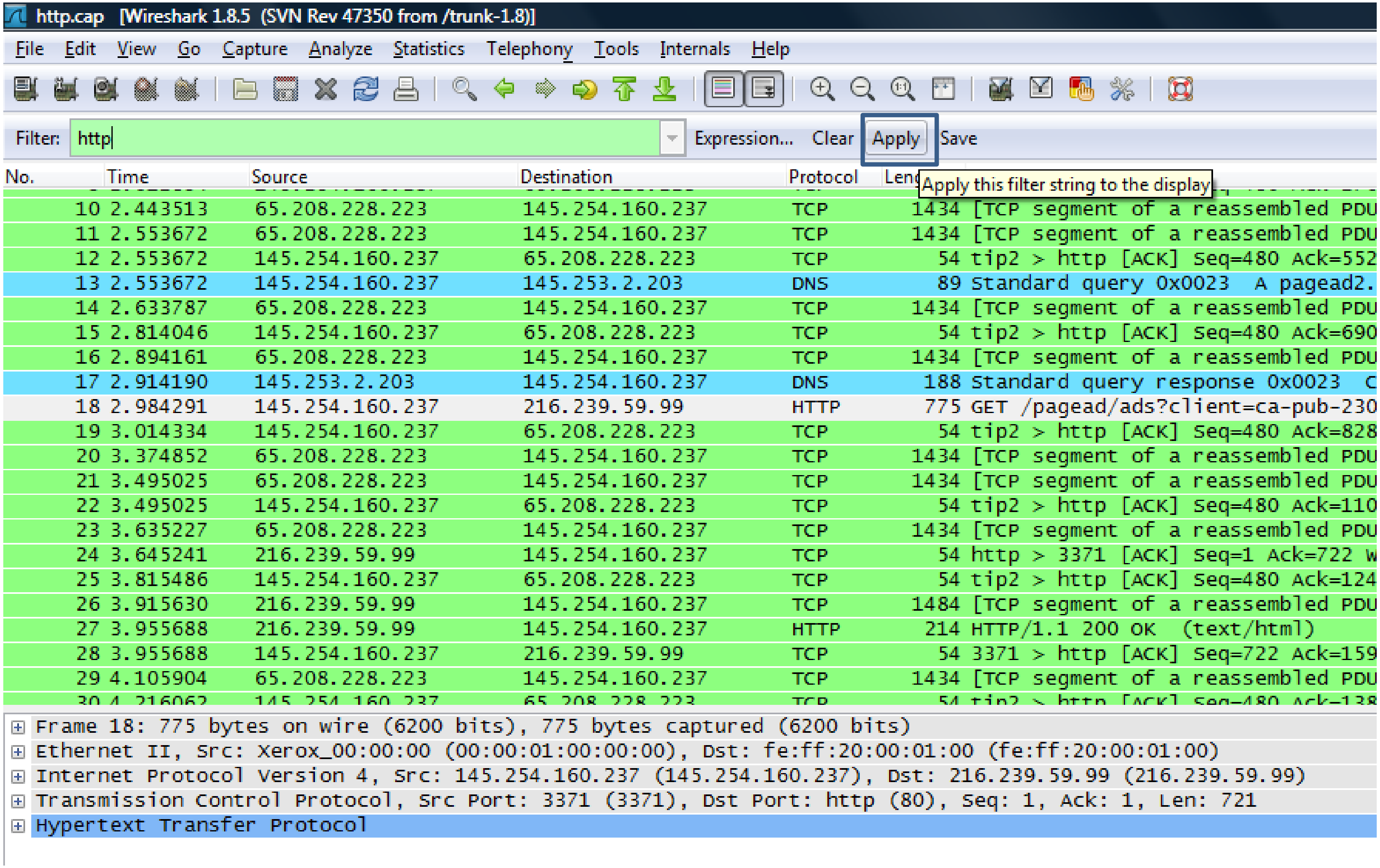
Zakładamy, że chcemy analizować tylko komunikację HTTP



```
10 2.443513   65.208.228.223    145.254.160.237   TCP    1434 [TCP segment of a reassembled PDU]
11 2.553672   65.208.228.223    145.254.160.237   TCP    1434 [TCP segment of a reassembled PDU]
12 2.553672   145.254.160.237   65.208.228.223    TCP      54 tip2 > http [ACK] Seq=480 Ack=5521 Win=9660 Len=0
13 2.553672   145.254.160.237   145.253.2.203     DNS      89 Standard query 0x0023  A pagead2.googlesyndication.com
14 2.633787   65.208.228.223    145.254.160.237   TCP    1434 [TCP segment of a reassembled PDU]
15 2.814046   145.254.160.237   65.208.228.223    TCP      54 tip2 > http [ACK] Seq=480 Ack=6901 Win=9660 Len=0
16 2.894161   65.208.228.223    145.254.160.237   TCP    1434 [TCP segment of a reassembled PDU]
17 2.914190   145.253.2.203     145.254.160.237   DNS     188 Standard query response 0x0023  CNAME pagead2.google.com CNAME pagead.
18 2.984291   145.254.160.237   216.239.59.99     HTTP    775 GET /pagead/ads?client=ca-pub-2309191948673629&random=1084443430285&lm
19 3.014334   145.254.160.237   65.208.228.223    TCP      54 tip2 > http [ACK] Seq=480 Ack=8281 Win=9660 Len=0
20 3.374852   65.208.228.223    145.254.160.237   TCP    1434 [TCP segment of a reassembled PDU]
21 3.495025   65.208.228.223    145.254.160.237   TCP    1434 [TCP segment of a reassembled PDU]
22 3.495025   145.254.160.237   65.208.228.223    TCP      54 tip2 > http [ACK] Seq=480 Ack=11041 Win=9660 Len=0
23 3.635227   65.208.228.223    145.254.160.237   TCP    1434 [TCP segment of a reassembled PDU]
24 3.645241   216.239.59.99     145.254.160.237   TCP      54 http > 3371 [ACK] Seq=1 Ack=722 Win=31460 Len=0
25 3.815486   145.254.160.237   65.208.228.223    TCP      54 tip2 > http [ACK] Seq=480 Ack=12421 Win=9660 Len=0
26 3.915630   216.239.59.99     145.254.160.237   TCP    1484 [TCP segment of a reassembled PDU]
27 3.955688   216.239.59.99     145.254.160.237   HTTP    214 HTTP/1.1 200 OK  (text/html)
28 3.955688   145.254.160.237   216.239.59.99     TCP      54 3371 > http [ACK] Seq=722 Ack=1591 Win=8760 Len=0
29 4.105904   65.208.228.223    145.254.160.237   TCP    1434 [TCP segment of a reassembled PDU]
30 4.216062   145.254.160.237   65.208.228.223    TCP      54 tip2 > http [ACK] Seq=480 Ack=13801 Win=9660 Len=0
```

```
⊞ Frame 18: 775 bytes on wire (6200 bits), 775 bytes captured (6200 bits)
⊞ Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
⊞ Internet Protocol Version 4, Src: 145.254.160.237 (145.254.160.237), Dst: 216.239.59.99 (216.239.59.99)
⊞ Transmission Control Protocol, Src Port: 3371 (3371), Dst Port: http (80), Seq: 1, Ack: 1, Len: 721
⊞ Hypertext Transfer Protocol
```

Wireshark

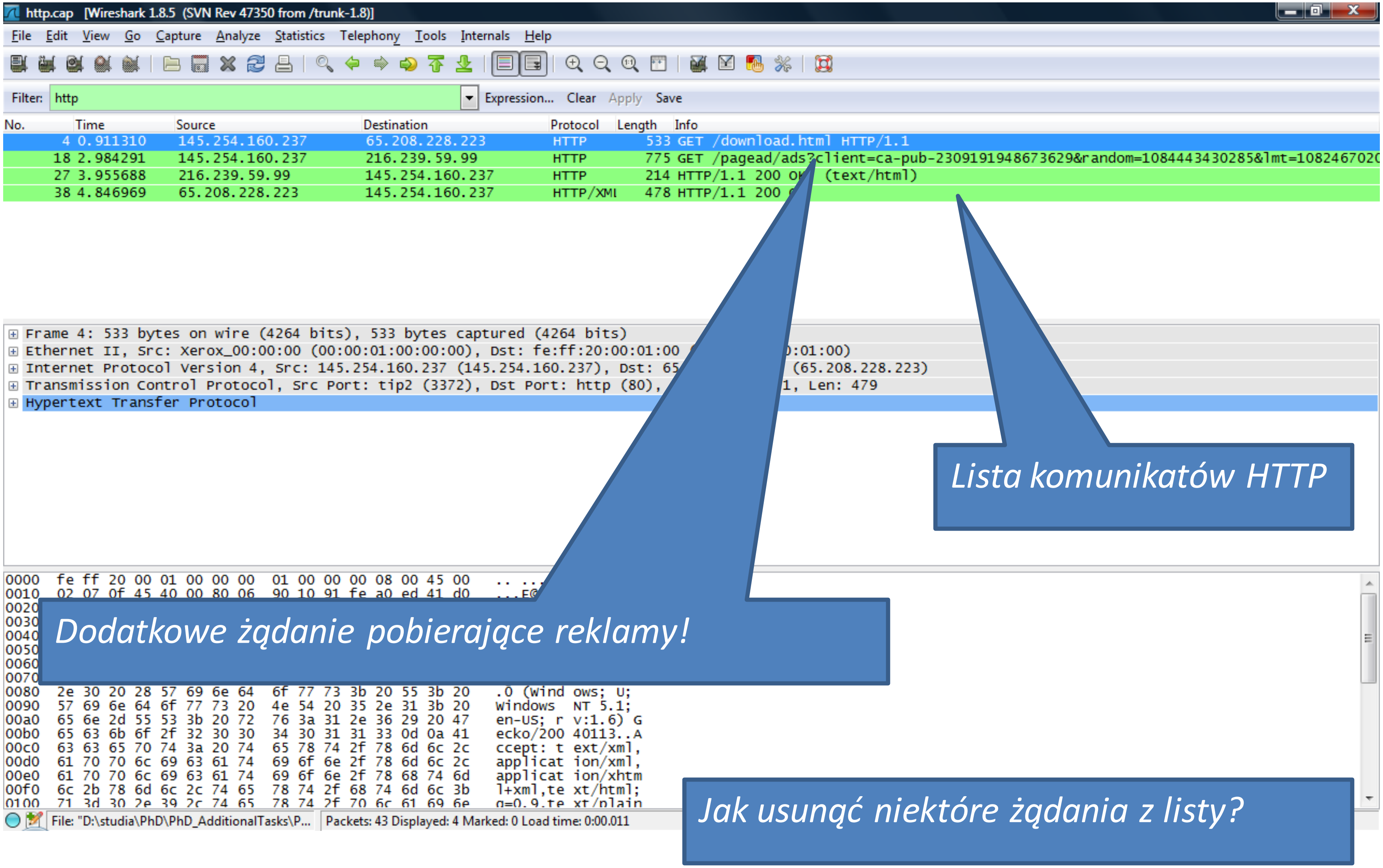

http.cap [Wireshark 1.8.5 (SVN Rev 47350 from /trunk-1.8)]
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Tools
Internals
Help
Expression...
Clear
Apply
Save
Apply this filter string to the display

Filter: http

```
No.     Time        Source            Destination       Protocol  Leng
     10 2.443513    65.208.228.223    145.254.160.237   TCP       1434 [TCP segment of a reassembled PDU
     11 2.553672    65.208.228.223    145.254.160.237   TCP       1434 [TCP segment of a reassembled PDU
     12 2.553672    145.254.160.237   65.208.228.223    TCP         54 tip2 > http [ACK] Seq=480 Ack=552
     13 2.553672    145.254.160.237   145.253.2.203     DNS         89 Standard query 0x0023  A pagead2.
     14 2.633787    65.208.228.223    145.254.160.237   TCP       1434 [TCP segment of a reassembled PDU
     15 2.814046    145.254.160.237   65.208.228.223    TCP         54 tip2 > http [ACK] Seq=480 Ack=690
     16 2.894161    65.208.228.223    145.254.160.237   TCP       1434 [TCP segment of a reassembled PDU
     17 2.914190    145.253.2.203     145.254.160.237   DNS        188 Standard query response 0x0023  C
     18 2.984291    145.254.160.237   216.239.59.99     HTTP       775 GET /pagead/ads?client=ca-pub-230
     19 3.014334    145.254.160.237   65.208.228.223    TCP         54 tip2 > http [ACK] Seq=480 Ack=828
     20 3.374852    65.208.228.223    145.254.160.237   TCP       1434 [TCP segment of a reassembled PDU
     21 3.495025    65.208.228.223    145.254.160.237   TCP       1434 [TCP segment of a reassembled PDU
     22 3.495025    145.254.160.237   65.208.228.223    TCP         54 tip2 > http [ACK] Seq=480 Ack=110
     23 3.635227    65.208.228.223    145.254.160.237   TCP       1434 [TCP segment of a reassembled PDU
     24 3.645241    216.239.59.99     145.254.160.237   TCP         54 http > 3371 [ACK] Seq=1 Ack=722 W
     25 3.815486    145.254.160.237   65.208.228.223    TCP         54 tip2 > http [ACK] Seq=480 Ack=124
     26 3.915630    216.239.59.99     145.254.160.237   TCP       1484 [TCP segment of a reassembled PDU
     27 3.955688    216.239.59.99     145.254.160.237   HTTP       214 HTTP/1.1 200 OK  (text/html)
     28 3.955688    145.254.160.237   216.239.59.99     TCP         54 3371 > http [ACK] Seq=722 Ack=159
     29 4.105904    65.208.228.223    145.254.160.237   TCP       1434 [TCP segment of a reassembled PDU
     30 4.216062    145.254.160.237   65.208.228.223    TCP         54 tip2 > http [ACK] Seq=480 Ack=138
```

```
⊞ Frame 18: 775 bytes on wire (6200 bits), 775 bytes captured (6200 bits)
⊞ Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
⊞ Internet Protocol Version 4, Src: 145.254.160.237 (145.254.160.237), Dst: 216.239.59.99 (216.239.59.99)
⊞ Transmission Control Protocol, Src Port: 3371 (3371), Dst Port: http (80), Seq: 1, Ack: 1, Len: 721
⊞ Hypertext Transfer Protocol
```

Wireshark



http.cap [Wireshark 1.8.5 (SVN Rev 47350 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: http

```
No.    Time       Source            Destination       Protocol  Length Info
     4 0.911310   145.254.160.237   65.208.228.223    HTTP         533 GET /download.html HTTP/1.1
    18 2.984291   145.254.160.237   216.239.59.99     HTTP         775 GET /pagead/ads?client=ca-pub-2309191948673629&random=1084443430285&lmt=108246702C
    27 3.955688   216.239.59.99     145.254.160.237   HTTP         214 HTTP/1.1 200 OK  (text/html)
    38 4.846969   65.208.228.223    145.254.160.237   HTTP/XMl     478 HTTP/1.1 200 C
```

```
⊞ Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)
⊞ Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00              ):01:00)
⊞ Internet Protocol Version 4, Src: 145.254.160.237 (145.254.160.237), Dst: 65               (65.208.228.223)
⊞ Transmission Control Protocol, Src Port: tip2 (3372), Dst Port: http (80),                1, Len: 479
⊞ Hypertext Transfer Protocol
```

```
0000  fe ff 20 00 01 00 00 00  01 00 00 00 08 00 45 00   .. ...
0010  02 07 0f 45 40 00 80 06  90 10 91 fe a0 ed 41 d0   ...E@
0020
0030
0040
0050
0060
0070
0080  2e 30 20 28 57 69 6e 64  6f 77 73 3b 20 55 3b 20   .0 (Wind ows; U;
0090  57 69 6e 64 6f 77 73 20  4e 54 20 35 2e 31 3b 20   Windows  NT 5.1;
00a0  65 6e 2d 55 53 3b 20 72  76 3a 31 2e 36 29 20 47   en-US; r v:1.6) G
00b0  65 63 6b 6f 2f 32 30 30  34 30 31 31 33 0d 0a 41   ecko/200 40113..A
00c0  63 63 65 70 74 3a 20 74  65 78 74 2f 78 6d 6c 2c   ccept: t ext/xml,
00d0  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 6d 6c 2c   applicat ion/xml,
00e0  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 68 74 6d   applicat ion/xhtm
00f0  6c 2b 78 6d 6c 2c 74 65  78 74 2f 68 74 6d 6c 3b   l+xml,te xt/html;
0100  71 3d 30 2e 39 2c 74 65  78 74 2f 70 6c 61 69 6e   q=0.9,te xt/plain
```

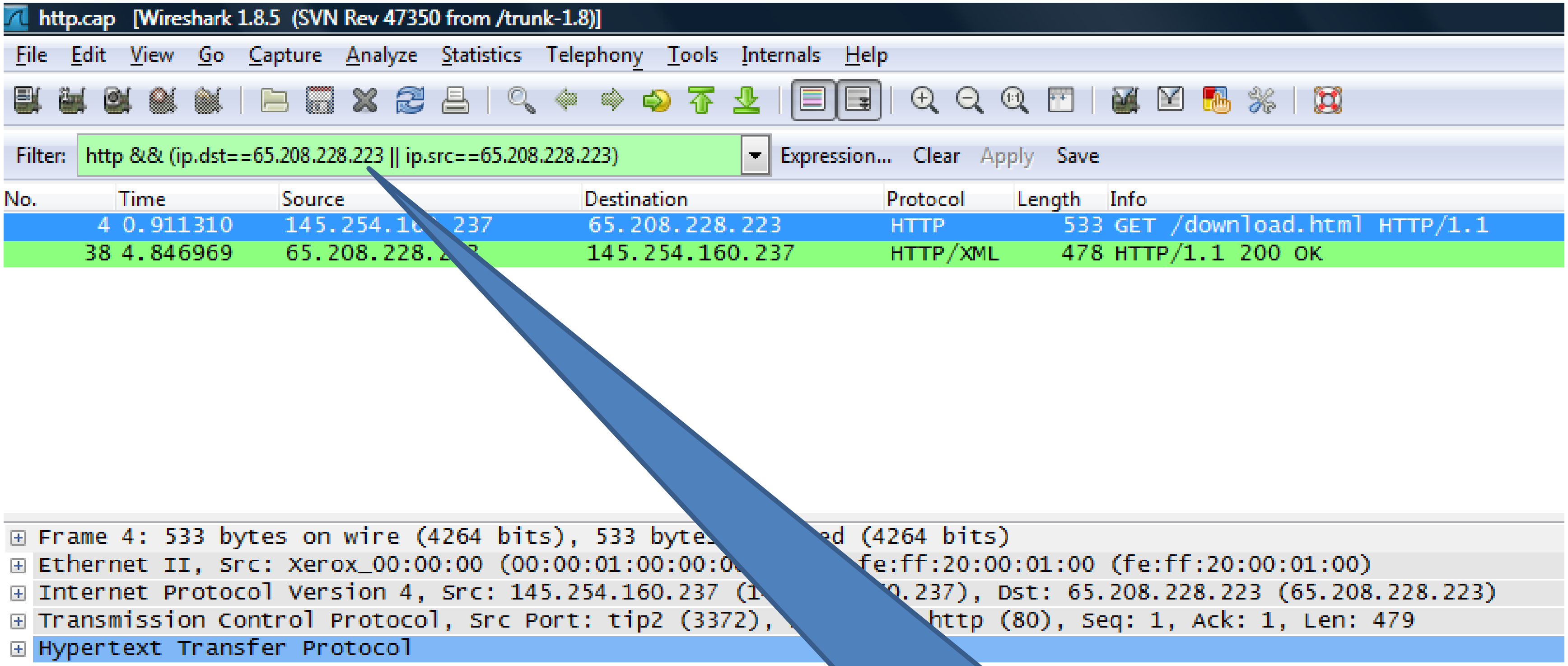
File: "D:\studia\PhD\PhD_AdditionalTasks\P...   Packets: 43 Displayed: 4 Marked: 0 Load time: 0:00.011

Lista komunikatów HTTP

Dodatkowe żądanie pobierające reklamy!

Jak usunąć niektóre żądania z listy?

Wireshark


http.cap [Wireshark 1.8.5 (SVN Rev 47350 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

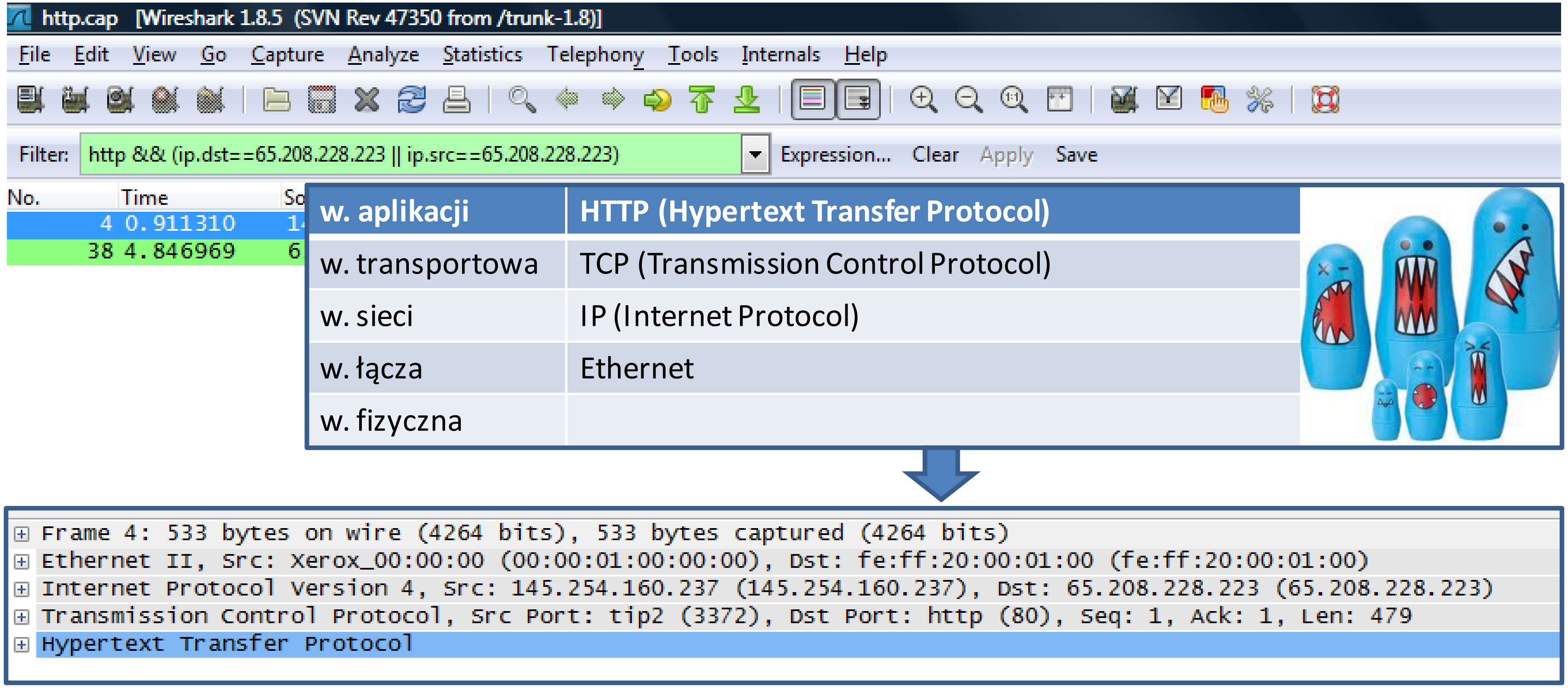
Filter: http && (ip.dst==65.208.228.223 || ip.src==65.208.228.223)

```
No.   Time        Source            Destination        Protocol   Length Info
    4 0.911310    145.254.1   237   65.208.228.223     HTTP          533 GET /download.html HTTP/1.1
   38 4.846969    65.208.228.2      145.254.160.237    HTTP/XML      478 HTTP/1.1 200 OK
```

```
⊞ Frame 4: 533 bytes on wire (4264 bits), 533 byte        ed (4264 bits)
⊞ Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:0       fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
⊞ Internet Protocol Version 4, Src: 145.254.160.237 (1       0.237), Dst: 65.208.228.223 (65.208.228.223)
⊞ Transmission Control Protocol, Src Port: tip2 (3372),        http (80), Seq: 1, Ack: 1, Len: 479
⊞ Hypertext Transfer Protocol
```

Modyfikacja filtra…

Wireshark


http.cap [Wireshark 1.8.5 (SVN Rev 47350 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: http && (ip.dst==65.208.228.223 || ip.src==65.208.228.223)

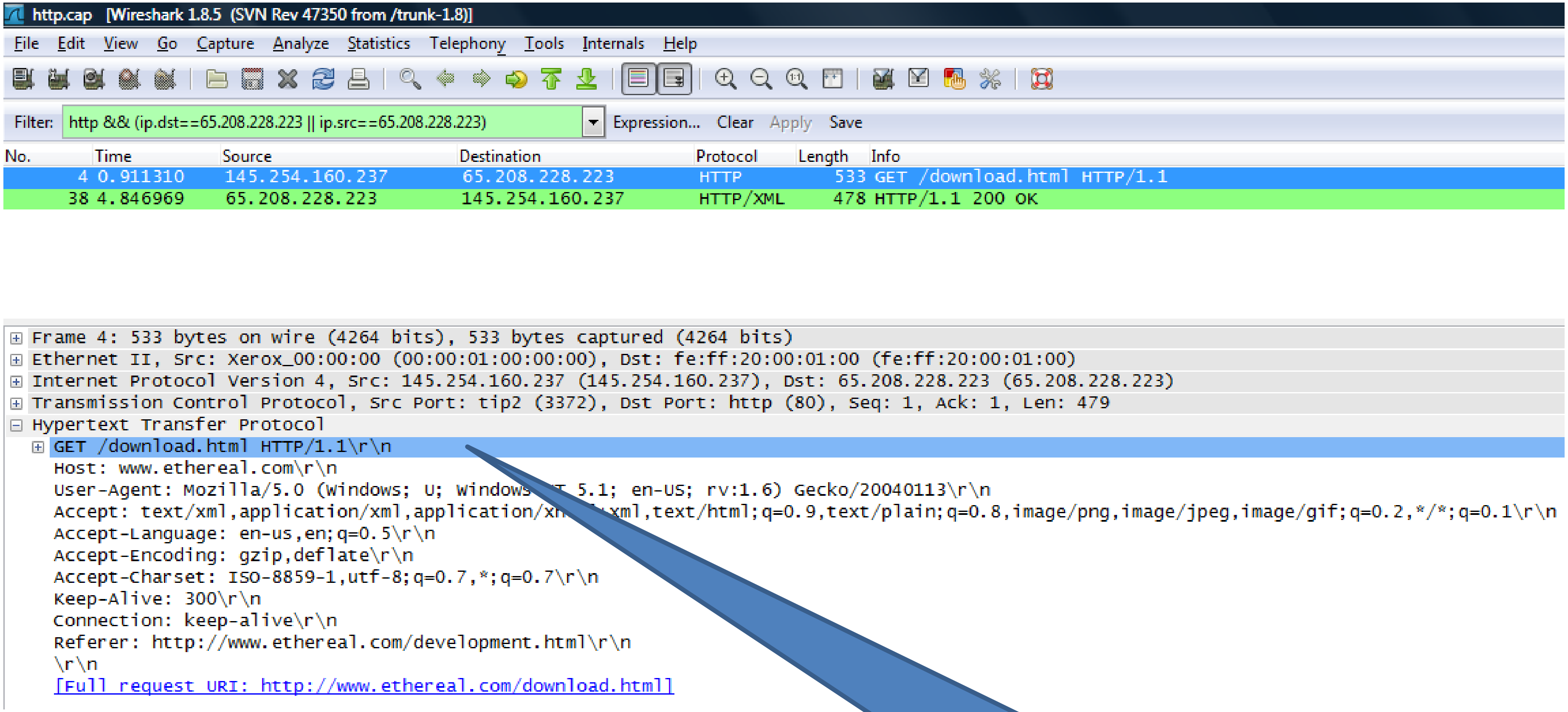
```
No.       Time          So
     4 0.911310         14
    38 4.846969         6
```

w. aplikacji	HTTP (Hypertext Transfer Protocol)
w. transportowa	TCP (Transmission Control Protocol)
w. sieci	IP (Internet Protocol)
w. łącza	Ethernet
w. fizyczna	

```
⊞ Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)
⊞ Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
⊞ Internet Protocol Version 4, Src: 145.254.160.237 (145.254.160.237), Dst: 65.208.228.223 (65.208.228.223)
⊞ Transmission Control Protocol, Src Port: tip2 (3372), Dst Port: http (80), Seq: 1, Ack: 1, Len: 479
⊞ Hypertext Transfer Protocol
```

W tym oknie szczegółowe informacje dotyczące zaznaczonej wyżej wiadomości…

Wireshark


http.cap [Wireshark 1.8.5 (SVN Rev 47350 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

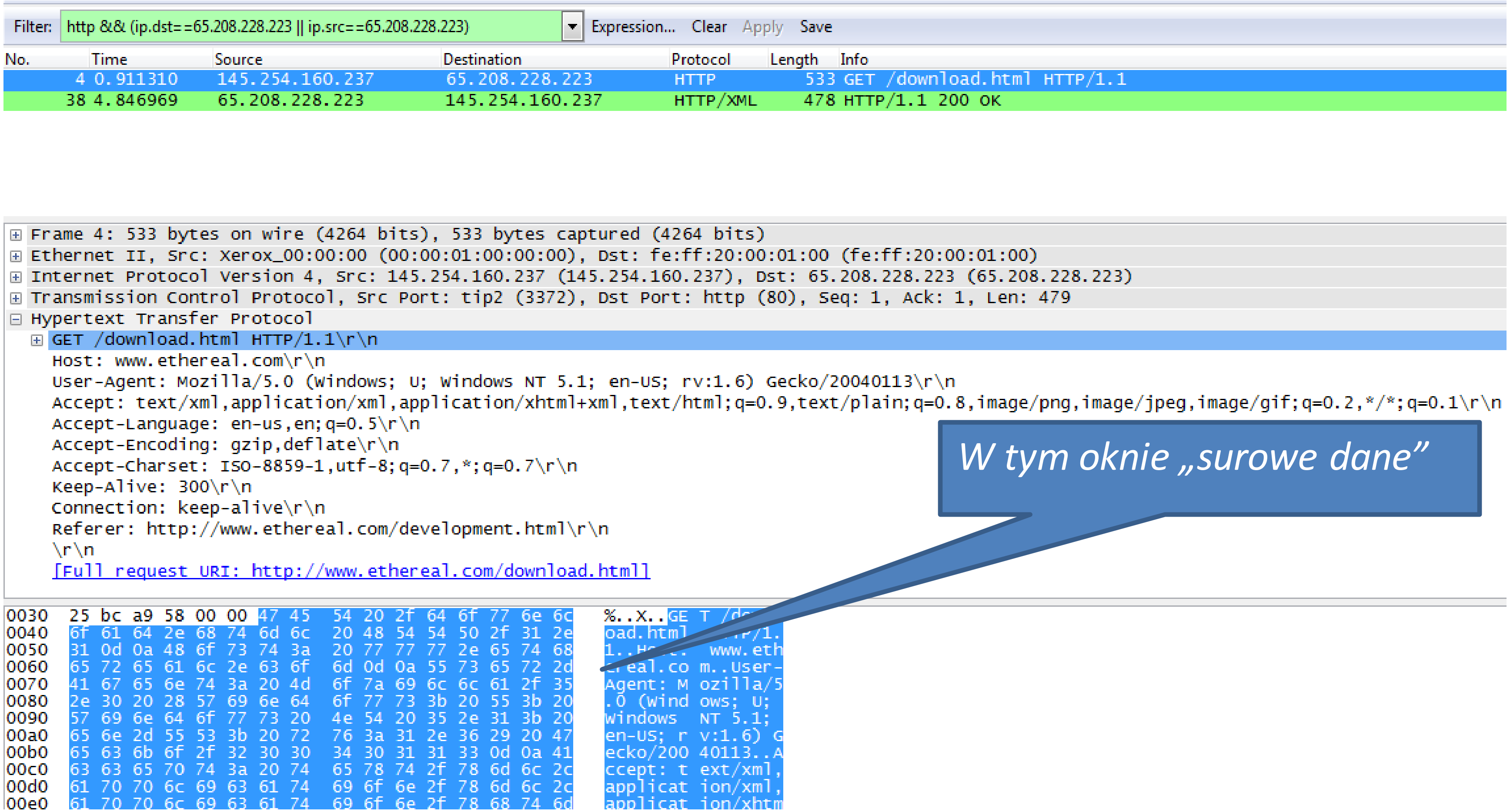
Filter: http && (ip.dst==65.208.228.223 || ip.src==65.208.228.223)

```
No.     Time        Source            Destination       Protocol   Length  Info
      4 0.911310    145.254.160.237   65.208.228.223    HTTP          533  GET /download.html HTTP/1.1
     38 4.846969    65.208.228.223    145.254.160.237   HTTP/XML      478  HTTP/1.1 200 OK
```

```
⊞ Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)
⊞ Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
⊞ Internet Protocol Version 4, Src: 145.254.160.237 (145.254.160.237), Dst: 65.208.228.223 (65.208.228.223)
⊞ Transmission Control Protocol, Src Port: tip2 (3372), Dst Port: http (80), Seq: 1, Ack: 1, Len: 479
⊟ Hypertext Transfer Protocol
  ⊞ GET /download.html HTTP/1.1\r\n
    Host: www.ethereal.com\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113\r\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=0.2,*/*;q=0.1\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    Referer: http://www.ethereal.com/development.html\r\n
    \r\n
    [Full request URI: http://www.ethereal.com/download.html]
```

Polecenie wygląda znajomo?

Wireshark



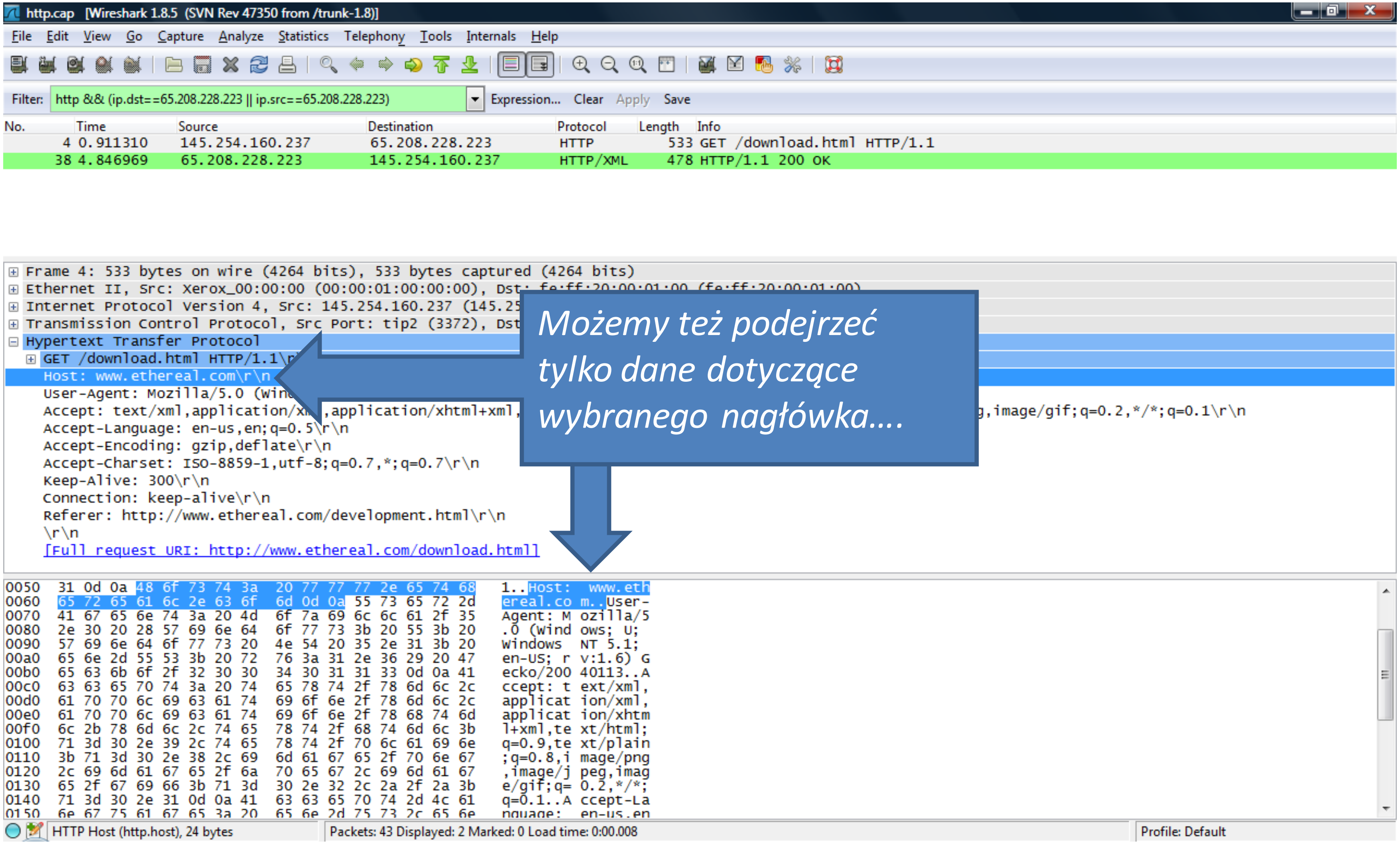
```
Filter: http && (ip.dst==65.208.228.223 || ip.src==65.208.228.223)

No.   Time       Source           Destination      Protocol  Length  Info
    4 0.911310   145.254.160.237  65.208.228.223   HTTP         533  GET /download.html HTTP/1.1
   38 4.846969   65.208.228.223   145.254.160.237  HTTP/XML     478  HTTP/1.1 200 OK
```

```
⊞ Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)
⊞ Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
⊞ Internet Protocol Version 4, Src: 145.254.160.237 (145.254.160.237), Dst: 65.208.228.223 (65.208.228.223)
⊞ Transmission Control Protocol, Src Port: tip2 (3372), Dst Port: http (80), Seq: 1, Ack: 1, Len: 479
⊟ Hypertext Transfer Protocol
  ⊞ GET /download.html HTTP/1.1\r\n
    Host: www.ethereal.com\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113\r\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=0.2,*/*;q=0.1\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    Referer: http://www.ethereal.com/development.html\r\n
    \r\n
    [Full request URI: http://www.ethereal.com/download.html]
```

```
0030  25 bc a9 58 00 00 47 45  54 20 2f 64 6f 77 6e 6c   %..X..GE T /d
0040  6f 61 64 2e 68 74 6d 6c  20 48 54 54 50 2f 31 2e   oad.html   P/1.
0050  31 0d 0a 48 6f 73 74 3a  20 77 77 77 2e 65 74 68   1..H       www.eth
0060  65 72 65 61 6c 2e 63 6f  6d 0d 0a 55 73 65 72 2d    eal.co m..User-
0070  41 67 65 6e 74 3a 20 4d  6f 7a 69 6c 6c 61 2f 35   Agent: M ozilla/5
0080  2e 30 20 28 57 69 6e 64  6f 77 73 3b 20 55 3b 20   .0 (Wind ows; U;
0090  57 69 6e 64 6f 77 73 20  4e 54 20 35 2e 31 3b 20   Windows  NT 5.1;
00a0  65 6e 2d 55 53 3b 20 72  76 3a 31 2e 36 29 20 47   en-US; r v:1.6) G
00b0  65 63 6b 6f 2f 32 30 30  34 30 31 31 33 0d 0a 41   ecko/200 40113..A
00c0  63 63 65 70 74 3a 20 74  65 78 74 2f 78 6d 6c 2c   ccept: t ext/xml,
00d0  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 6d 6c 2c   applicat ion/xml,
00e0  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 68 74 6d   applicat ion/xhtm
```

W tym oknie „surowe dane”

Wireshark



http.cap [Wireshark 1.8.5 (SVN Rev 47350 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

Filter: http && (ip.dst==65.208.228.223 || ip.src==65.208.228.223)

```
No.   Time        Source            Destination       Protocol   Length  Info
    4 0.911310    145.254.160.237   65.208.228.223    HTTP          533  GET /download.html HTTP/1.1
   38 4.846969    65.208.228.223    145.254.160.237   HTTP/XML      478  HTTP/1.1 200 OK
```

```
⊞ Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)
⊞ Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
⊞ Internet Protocol Version 4, Src: 145.254.160.237 (145.25
⊞ Transmission Control Protocol, Src Port: tip2 (3372), Dst
⊟ Hypertext Transfer Protocol
  ⊞ GET /download.html HTTP/1.1\r
    Host: www.ethereal.com\r\n
    User-Agent: Mozilla/5.0 (Win
    Accept: text/xml,application/x ,application/xhtml+xml,          g,image/gif;q=0.2,*/*;q=0.1\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    Referer: http://www.ethereal.com/development.html\r\n
    \r\n
    [Full request URI: http://www.ethereal.com/download.html]
```

```
0050  31 0d 0a 48 6f 73 74 3a  20 77 77 77 2e 65 74 68   1..Host:  www.eth
0060  65 72 65 61 6c 2e 63 6f  6d 0d 0a 55 73 65 72 2d   ereal.co m..User-
0070  41 67 65 6e 74 3a 20 4d  6f 7a 69 6c 6c 61 2f 35   Agent: M ozilla/5
0080  2e 30 20 28 57 69 6e 64  6f 77 73 3b 20 55 3b 20   .0 (Wind ows; U;
0090  57 69 6e 64 6f 77 73 20  4e 54 20 35 2e 31 3b 20   Windows  NT 5.1;
00a0  65 6e 2d 55 53 3b 20 72  76 3a 31 2e 36 29 20 47   en-US; r v:1.6) G
00b0  65 63 6b 6f 2f 32 30 30  34 30 31 31 33 0d 0a 41   ecko/200 40113..A
00c0  63 63 65 70 74 3a 20 74  65 78 74 2f 78 6d 6c 2c   ccept: t ext/xml,
00d0  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 6d 6c 2c   applicat ion/xml,
00e0  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 68 74 6d   applicat ion/xhtm
00f0  6c 2b 78 6d 6c 2c 74 65  78 74 2f 68 74 6d 6c 3b   l+xml,te xt/html;
0100  71 3d 30 2e 39 2c 74 65  78 74 2f 70 6c 61 69 6e   q=0.9,te xt/plain
0110  3b 71 3d 30 2e 38 2c 69  6d 61 67 65 2f 70 6e 67   ;q=0.8,i mage/png
0120  2c 69 6d 61 67 65 2f 6a  70 65 67 2c 69 6d 61 67   ,image/j peg,imag
0130  65 2f 67 69 66 3b 71 3d  30 2e 32 2c 2a 2f 2a 3b   e/gif;q= 0.2,*/*;
0140  71 3d 30 2e 31 0d 0a 41  63 63 65 70 74 2d 4c 61   q=0.1..A ccept-La
0150  6e 67 75 61 67 65 3a 20  65 6e 2d 75 73 2c 65 6e   nguage:  en-us,en
```

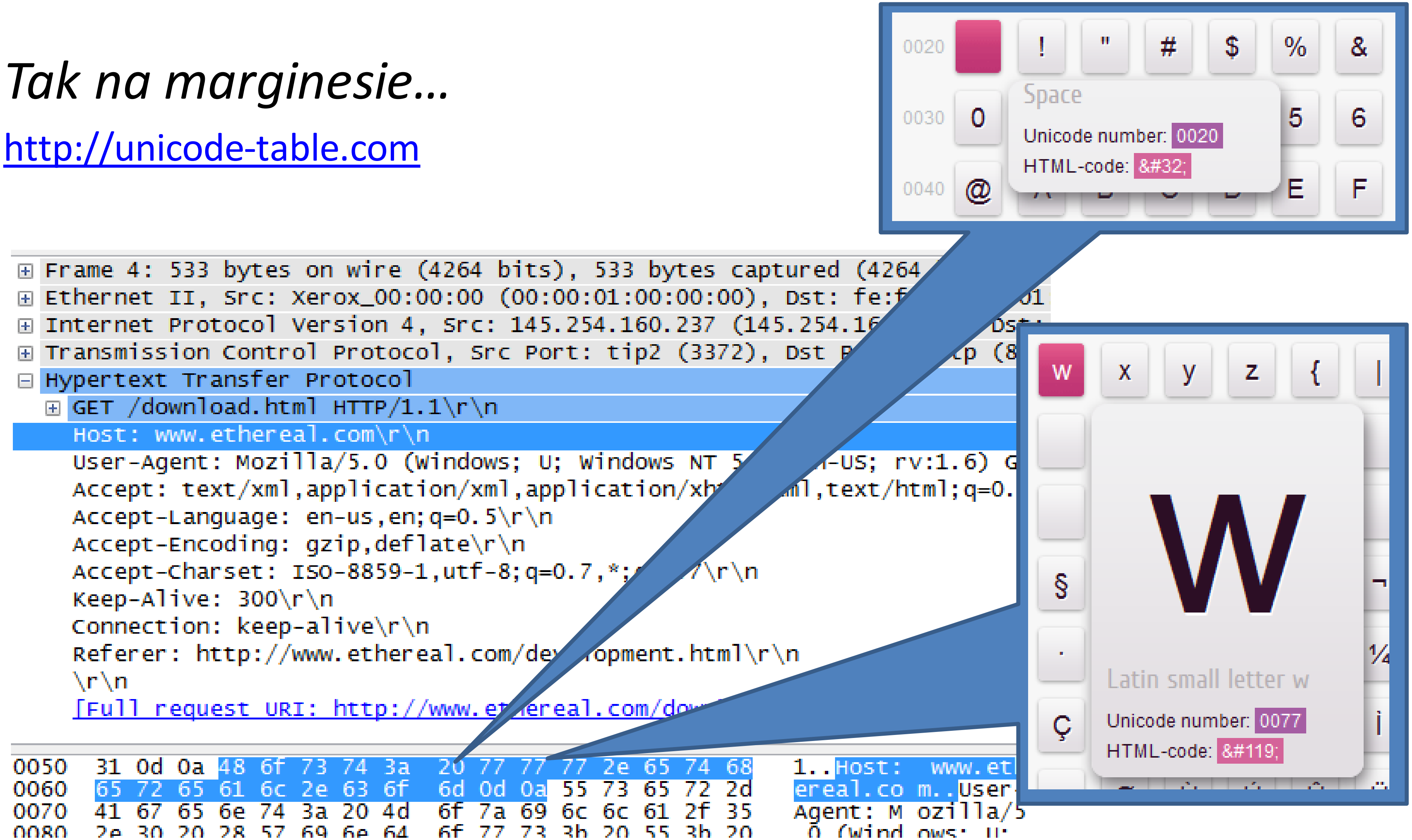
HTTP Host (http.host), 24 bytes | Packets: 43 Displayed: 2 Marked: 0 Load time: 0:00.008 | Profile: Default

Możemy też podejrzeć tylko dane dotyczące wybranego nagłówka….

Wireshark

Tak na marginesie…

http://unicode-table.com



```
⊞ Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264
⊞ Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:f            01
⊞ Internet Protocol Version 4, Src: 145.254.160.237 (145.254.16          Dst:
⊞ Transmission Control Protocol, Src Port: tip2 (3372), Dst P          tp (8
⊟ Hypertext Transfer Protocol
  ⊞ GET /download.html HTTP/1.1\r\n
    Host: www.ethereal.com\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5        n-US; rv:1.6) G
    Accept: text/xml,application/xml,application/xh        ml,text/html;q=0.
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;     7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    Referer: http://www.ethereal.com/de    opment.html\r\n
    \r\n
    [Full request URI: http://www.ethereal.com/dow

0050  31 0d 0a 48 6f 73 74 3a  20 77 77 77 2e 65 74 68   1..Host:  www.et
0060  65 72 65 61 6c 2e 63 6f  6d 0d 0a 55 73 65 72 2d   ereal.co m..User
0070  41 67 65 6e 74 3a 20 4d  6f 7a 69 6c 6c 61 2f 35   Agent: M ozilla/5
0080  2e 30 20 28 57 69 6e 64  6f 77 73 3b 20 55 3b 20    0 (Wind ows; U;
```

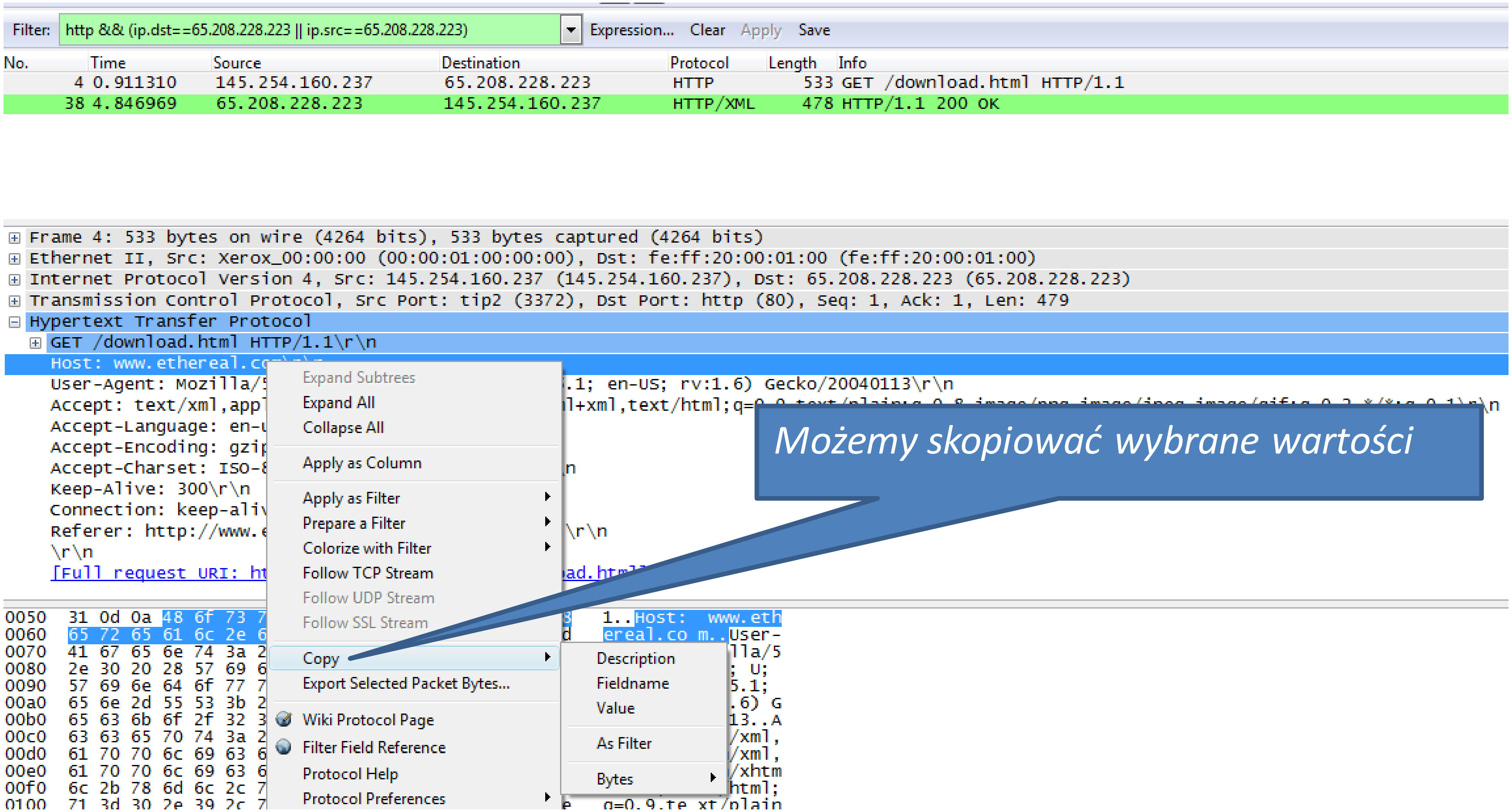
Unicode number: 0020

HTML-code: &#32;

Unicode number: 0077

HTML-code: &#119;

Wireshark



```
Filter: http && (ip.dst==65.208.228.223 || ip.src==65.208.228.223)    Expression...  Clear  Apply  Save

No.   Time        Source            Destination       Protocol   Length  Info
    4 0.911310    145.254.160.237   65.208.228.223    HTTP          533  GET /download.html HTTP/1.1
   38 4.846969    65.208.228.223    145.254.160.237   HTTP/XML      478  HTTP/1.1 200 OK
```

```
⊞ Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)
⊞ Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
⊞ Internet Protocol Version 4, Src: 145.254.160.237 (145.254.160.237), Dst: 65.208.228.223 (65.208.228.223)
⊞ Transmission Control Protocol, Src Port: tip2 (3372), Dst Port: http (80), Seq: 1, Ack: 1, Len: 479
⊟ Hypertext Transfer Protocol
  ⊞ GET /download.html HTTP/1.1\r\n
    Host: www.ethereal.co
    User-Agent: Mozilla/5                           .1; en-US; rv:1.6) Gecko/20040113\r\n
    Accept: text/xml,appl                           l+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=0.2,*/*;q=0.1\r\n
    Accept-Language: en-u
    Accept-Encoding: gzip
    Accept-Charset: ISO-8                           n
    Keep-Alive: 300\r\n
    Connection: keep-aliv
    Referer: http://www.e                           \r\n
    \r\n
    [Full request URI: ht                           oad.html]
```

```
0050  31 0d 0a 48 6f 73 7                    8    1..Host:  www.eth
0060  65 72 65 61 6c 2e 6                    d    ereal.co m..User-
0070  41 67 65 6e 74 3a 2                              lla/5
0080  2e 30 20 28 57 69 6                              ; U;
0090  57 69 6e 64 6f 77 7                              5.1;
00a0  65 6e 2d 55 53 3b 2                              .6) G
00b0  65 63 6b 6f 2f 32 3                              13..A
00c0  63 63 65 70 74 3a 2                              /xml,
00d0  61 70 70 6c 69 63 6                              /xml,
00e0  61 70 70 6c 69 63 6                              /xhtm
00f0  6c 2b 78 6d 6c 2c 7                              html;
0100  71 3d 30 2e 39 2c 7                    e    q=0.9.te xt/plain
```

Możemy skopiować wybrane wartości

Wireshark

Bardzo podstawowe wprowadzenie do Wiresharka dla nieobecnych (lub dociekliwych ;))

http://wiresharkdownloads.riverbed.com/video/wireshark/introduction-to-wireshark/

(wersja angielska)