Network Analysis using Wireshark

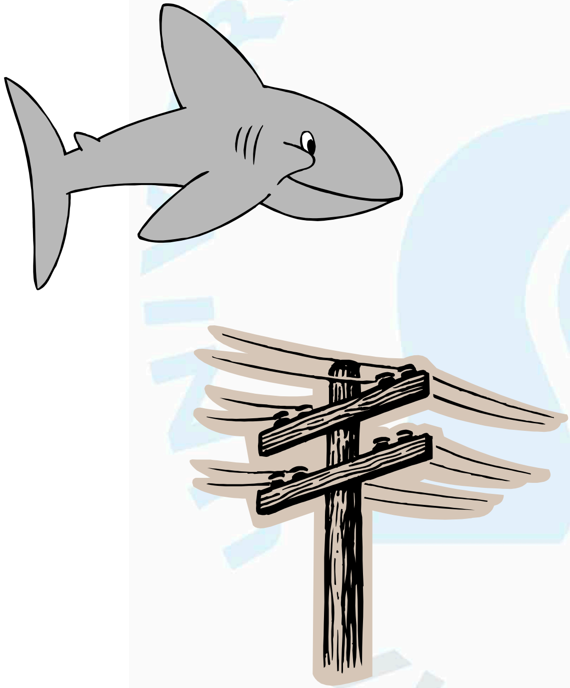
Jens Myrup Pedersen
jens@es.aau.dk

This document contains

- An introduction to Wireshark. Please go through it.
- Questions for the mini project (part 1 and part 2).
- Please upload the mini project before the deadline.
- The course homepage also contains the pcap files referred to in the presentation/questions.

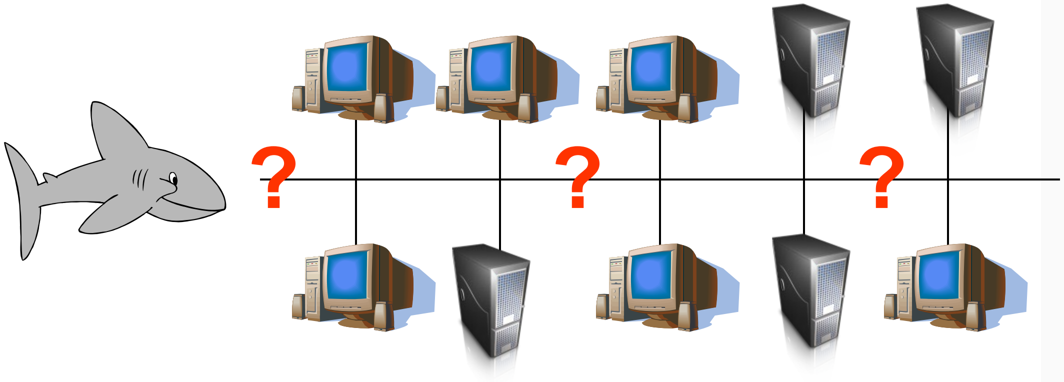
Wireshark (practical)

- Basic funtions
  - Setting up network interface card
  - Start/stop logging
  - Save/open logs
  - What you see...
- Application of analysis functions
  - Filtering data
  - Statistics
  - Measured data
- Learning goals
  - Wireshark as a tool
  - Basic functionalities
  - Basic setup



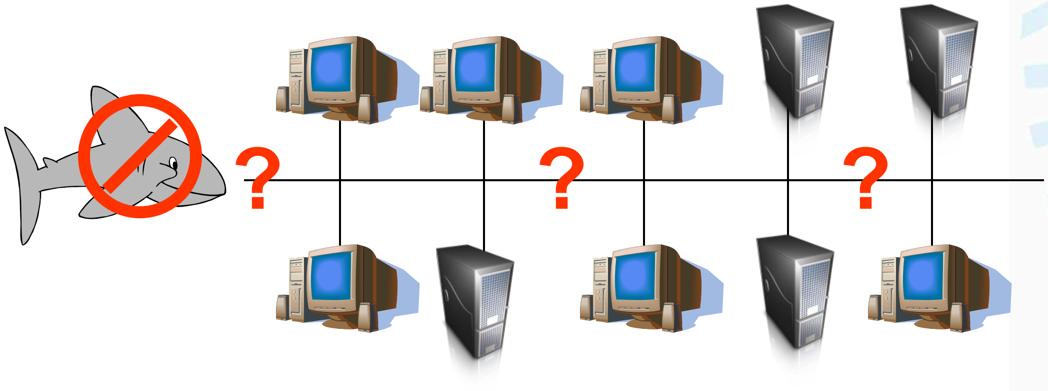
Wireshark - intro

- What is wireshark, and what can it be used for?
  - Finding problems in the network
  - Study security problems
  - Debugging protocol implementations
  - Learning about network protocols ☺
  - And much more…



Wireshark - intro

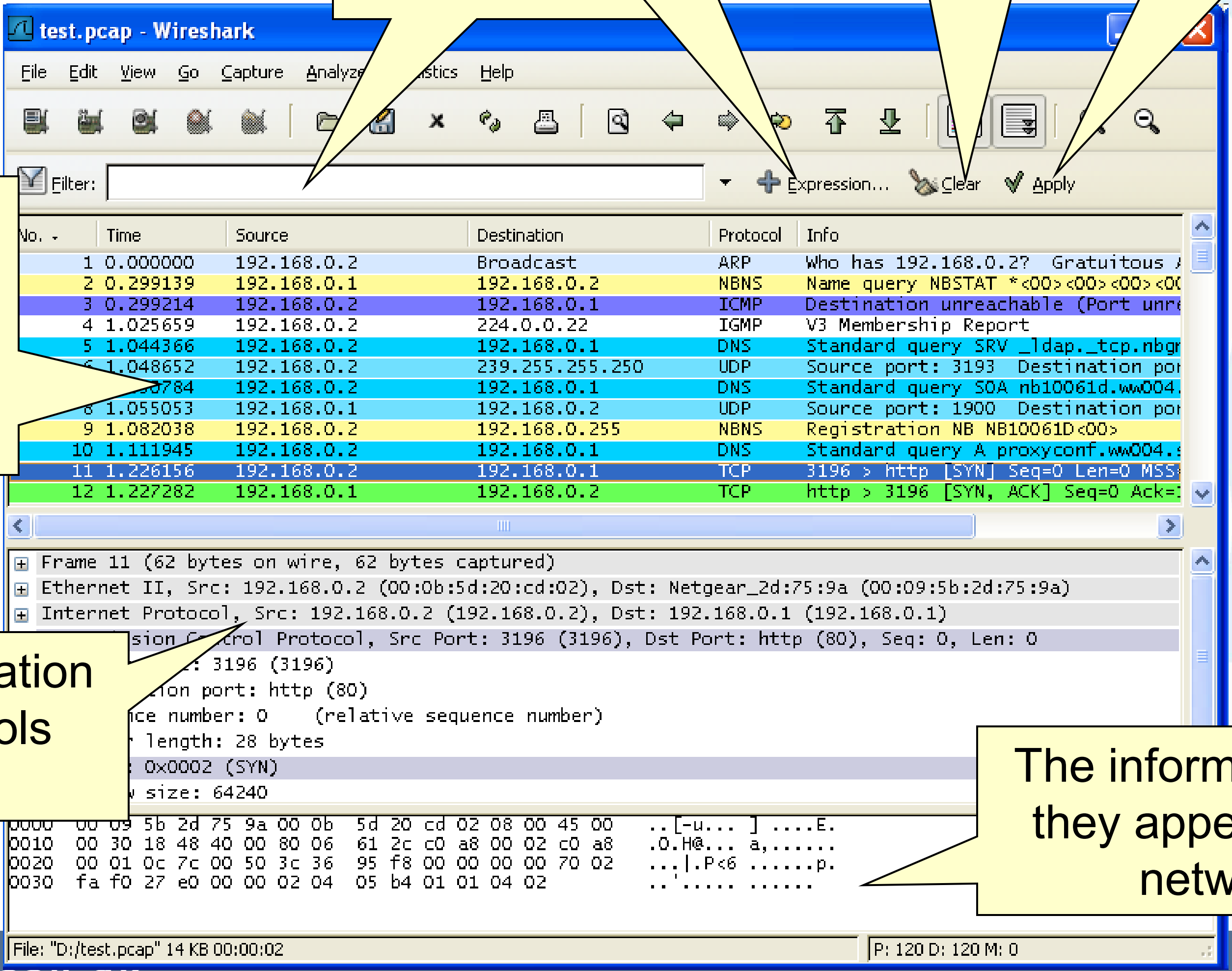
- Wireshark can NOT
  - Detect anormalities ”by itself”
  - Manipulate traffic – Wireshark is for monitoring and listening



Wireshark – useful information

- Wireshark can be obtained for Windows, Unix, Linux..
  - http://www.wireshark.org/download.html
- Wireshark is an open source program under GNU General Public License (GPL)
- You can find lots of ressources at
  - http://wiki.wireshark.org/

Overview



```
No. -   Time       Source          Destination       Protocol  Info
  1 0.000000   192.168.0.2     Broadcast         ARP       Who has 192.168.0.2?  Gratuitous A
  2 0.299139   192.168.0.1     192.168.0.2       NBNS      Name query NBSTAT *<00><00><00><00
  3 0.299214   192.168.0.2     192.168.0.1       ICMP      Destination unreachable (Port unre
  4 1.025659   192.168.0.2     224.0.0.22        IGMP      V3 Membership Report
  5 1.044366   192.168.0.2     192.168.0.1       DNS       Standard query SRV _ldap._tcp.nbgr
  6 1.048652   192.168.0.2     239.255.255.250   UDP       Source port: 3193  Destination por
     0784      192.168.0.2     192.168.0.1       DNS       Standard query SOA nb10061d.ww004.
  8 1.055053   192.168.0.1     192.168.0.2       UDP       Source port: 1900  Destination por
  9 1.082038   192.168.0.2     192.168.0.255     NBNS      Registration NB NB10061D<00>
 10 1.111945   192.168.0.2     192.168.0.1       DNS       Standard query A proxyconf.ww004.s
 11 1.226156   192.168.0.2     192.168.0.1       TCP       3196 > http [SYN] Seq=0 Len=0 MSS
 12 1.227282   192.168.0.1     192.168.0.2       TCP       http > 3196 [SYN, ACK] Seq=0 Ack=1
```

```
⊞ Frame 11 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)
⊞ Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
      sion Control Protocol, Src Port: 3196 (3196), Dst Port: http (80), Seq: 0, Len: 0
     : 3196 (3196)
     ion port: http (80)
     nce number: 0    (relative sequence number)
     r length: 28 bytes
     : 0x0002 (SYN)
     w size: 64240
```

```
0000  00 09 5b 2d 75 9a 00 0b  5d 20 cd 02 08 00 45 00   ..[-u... ] ....E.
0010  00 30 18 48 40 00 80 06  61 2c c0 a8 00 02 c0 a8   .0.H@... a,......
0020  00 01 0c 7c 00 50 3c 36  95 f8 00 00 00 00 70 02   ...|.P<6 ......p.
0030  fa f0 27 e0 00 00 02 04  05 b4 01 01 04 02         ..'..... ......
```

File: "D:/test.pcap" 14 KB 00:00:02 | P: 120 D: 120 M: 0

Make new filter

Filter field!

Clear filter

Apply filter

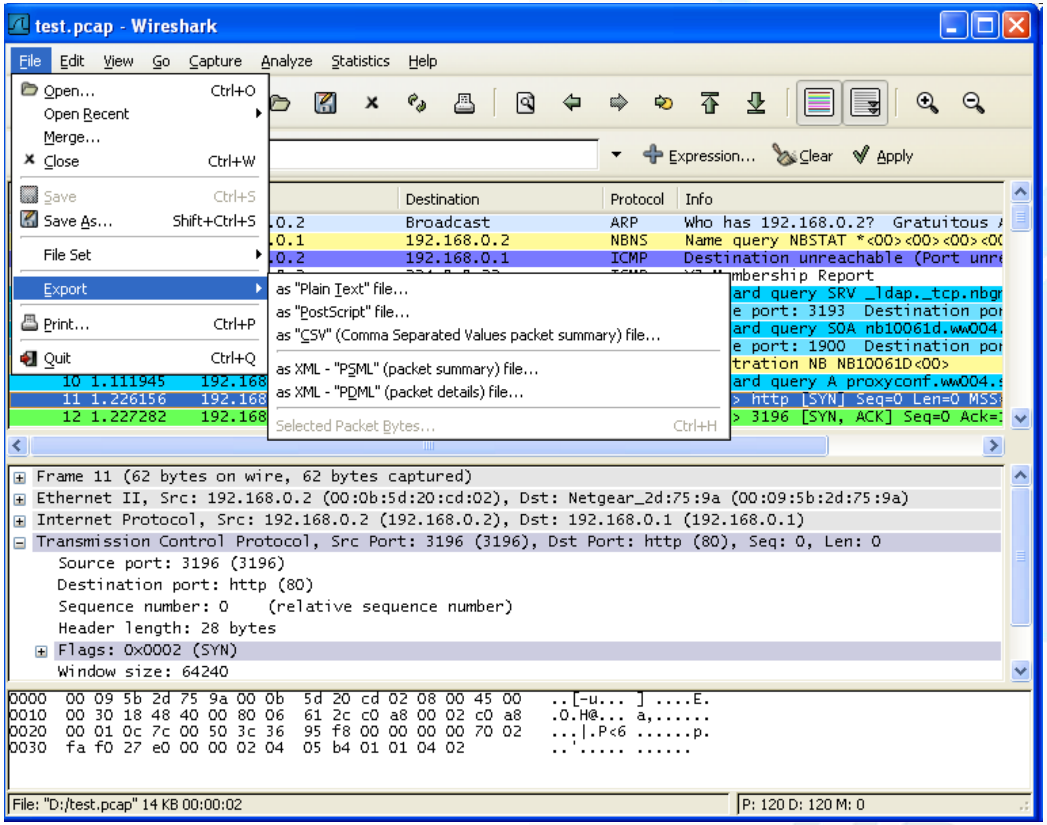
Network traffic (colors makes it easier to get an overview)

Detailed information on the protocols

The informations as they appear in the network

Import/Export options

- Open..
  - Import files
  - Supports multiple formats
- Export
  - Different formats
    - .txt
    - .ps
    - .cvs
  - All or selected



```
                Destination      Protocol  Info
.0.2            Broadcast        ARP       Who has 192.168.0.2?  Gratuitous A
.0.1            192.168.0.2      NBNS      Name query NBSTAT *<00><00><00><0C
.0.2            192.168.0.1      ICMP      Destination unreachable (Port unre
                                           mbership Report
                                           ard query SRV _ldap._tcp.nbgr
                                           e port: 3193  Destination por
                                           ard query SOA nb10061d.ww004.
                                           e port: 1900  Destination por
                                           tration NB NB10061D<00>
   10 1.111945  192.168                    ard query A proxyconf.ww004.s
   11 1.226156  192.168                    > http [SYN] Seq=0 Len=0 MSS=
   12 1.227282  192.168                    > 3196 [SYN, ACK] Seq=0 Ack=1
```

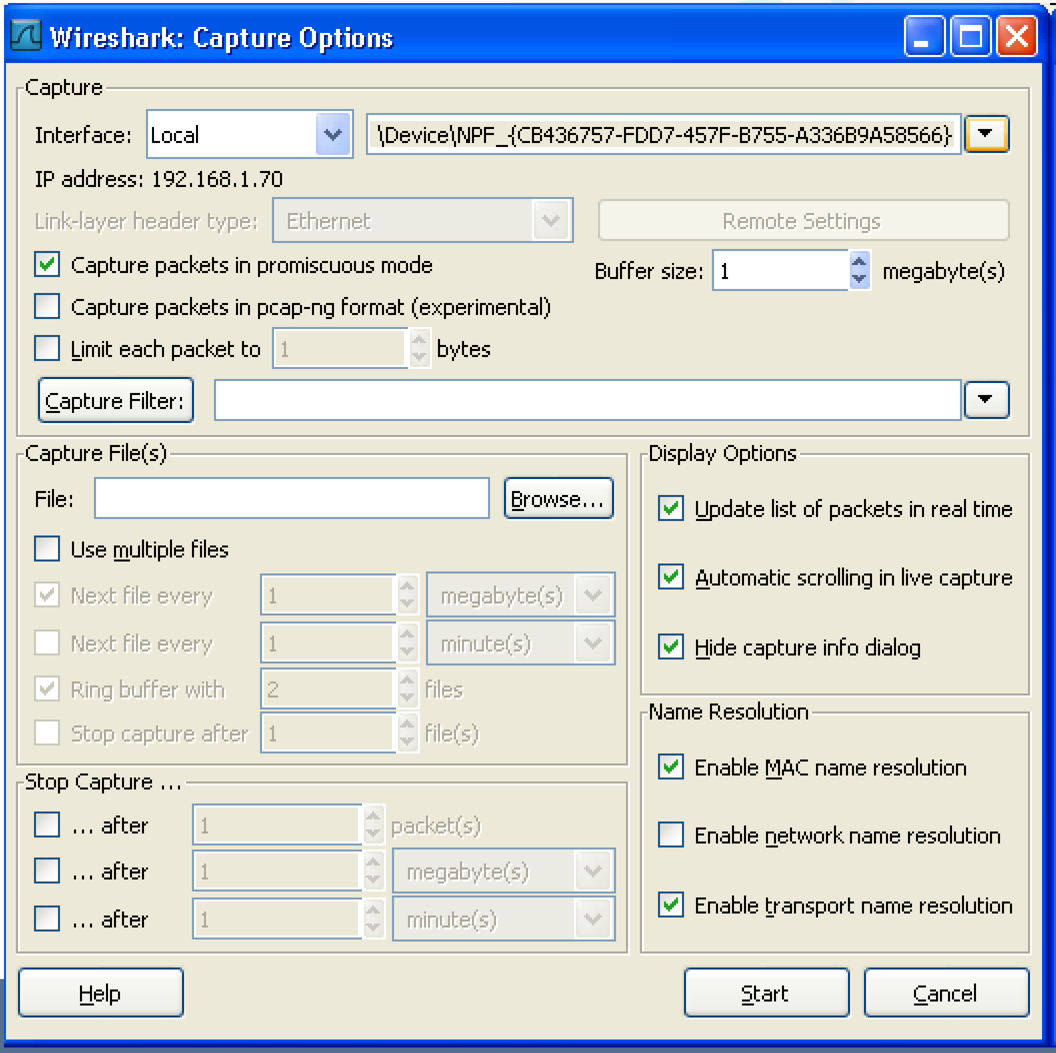
```
⊞ Frame 11 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)
⊞ Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
⊟ Transmission Control Protocol, Src Port: 3196 (3196), Dst Port: http (80), Seq: 0, Len: 0
    Source port: 3196 (3196)
    Destination port: http (80)
    Sequence number: 0    (relative sequence number)
    Header length: 28 bytes
  ⊞ Flags: 0x0002 (SYN)
    Window size: 64240
```

```
0000  00 09 5b 2d 75 9a 00 0b  5d 20 cd 02 08 00 45 00   ..[-u... ] ....E.
0010  00 30 18 48 40 00 80 06  61 2c c0 a8 00 02 c0 a8   .0.H@... a,......
0020  00 01 0c 7c 00 50 3c 36  95 f8 00 00 00 00 70 02   ...|.P<6 ......p.
0030  fa f0 27 e0 00 00 02 04  05 b4 01 01 04 02         ..'..... ......
```

File: "D:/test.pcap" 14 KB 00:00:02   P: 120 D: 120 M: 0

Capture menu

- First select which network cards to listen at
- Next select a number of options
- Start a session when you for example visit a particular website



Wireshark: Capture Options

Capture

Interface: Local \Device\NPF_{CB436757-FDD7-457F-B755-A336B9A58566}

IP address: 192.168.1.70

Link-layer header type: Ethernet

☑ Capture packets in promiscuous mode

Buffer size: 1 megabyte(s)

□ Capture packets in pcap-ng format (experimental)

□ Limit each packet to 1 bytes

Capture Filter:

Capture File(s)

File:

□ Use multiple files

☑ Next file every 1 megabyte(s)

□ Next file every 1 minute(s)

☑ Ring buffer with 2 files

□ Stop capture after 1 file(s)

Stop Capture ...

□ ... after 1 packet(s)

□ ... after 1 megabyte(s)

□ ... after 1 minute(s)

Display Options

☑ Update list of packets in real time

☑ Automatic scrolling in live capture

☑ Hide capture info dialog

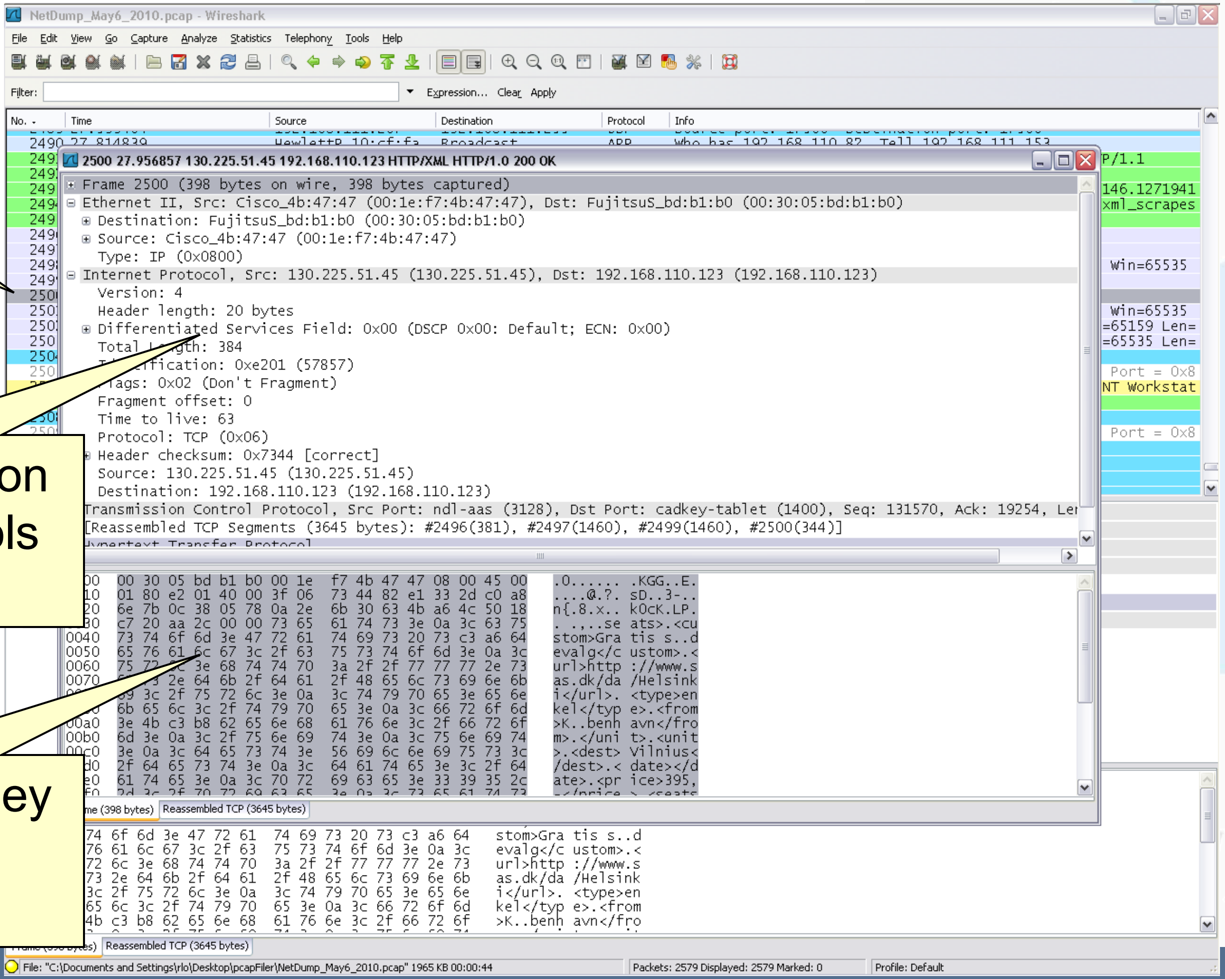
Name Resolution

☑ Enable MAC name resolution

□ Enable network name resolution

☑ Enable transport name resolution

Investigating single data packets


NetDump_May6_2010.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
2490 27.814839 HewlettP_10:cf:fa Broadcast ARP Who has 192.168.110.82 Tell 192.168.111.153
Frame (398 bytes)
Reassembled TCP (3645 bytes)

2500 27.956857 130.225.51.45 192.168.110.123 HTTP/XML HTTP/1.0 200 OK

```
⊞ Frame 2500 (398 bytes on wire, 398 bytes captured)
⊟ Ethernet II, Src: Cisco_4b:47:47 (00:1e:f7:4b:47:47), Dst: FujitsuS_bd:b1:b0 (00:30:05:bd:b1:b0)
  ⊞ Destination: FujitsuS_bd:b1:b0 (00:30:05:bd:b1:b0)
  ⊞ Source: Cisco_4b:47:47 (00:1e:f7:4b:47:47)
    Type: IP (0x0800)
⊟ Internet Protocol, Src: 130.225.51.45 (130.225.51.45), Dst: 192.168.110.123 (192.168.110.123)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 384
    Identification: 0xe201 (57857)
    Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 63
    Protocol: TCP (0x06)
  ⊞ Header checksum: 0x7344 [correct]
    Source: 130.225.51.45 (130.225.51.45)
    Destination: 192.168.110.123 (192.168.110.123)
Transmission Control Protocol, Src Port: ndl-aas (3128), Dst Port: cadkey-tablet (1400), Seq: 131570, Ack: 19254, Len
[Reassembled TCP Segments (3645 bytes): #2496(381), #2497(1460), #2499(1460), #2500(344)]
Hypertext Transfer Protocol
```

```
0000  00 30 05 bd b1 b0 00 1e  f7 4b 47 47 08 00 45 00   .0...... .KGG..E.
0010  01 80 e2 01 40 00 3f 06  73 44 82 e1 33 2d c0 a8   ....@.?. sD..3-..
0020  6e 7b 0c 38 05 78 0a 2e  6b 30 63 4b a6 4c 50 18   n{.8.x.. k0cK.LP.
0030  c7 20 aa 2c 00 00 73 65  61 74 73 3e 0a 3c 63 75   . .,..se ats>.<cu
0040  73 74 6f 6d 3e 47 72 61  74 69 73 20 73 c3 a6 64   stom>Gra tis s..d
0050  65 76 61 6c 67 3c 2f 63  75 73 74 6f 6d 3e 0a 3c   evalg</c ustom>.<
0060  75 72 6c 3e 68 74 74 70  3a 2f 2f 77 77 77 2e 73   url>http ://www.s
0070  61 73 2e 64 6b 2f 64 61  2f 48 65 6c 73 69 6e 6b   as.dk/da /Helsink
0080  69 3c 2f 75 72 6c 3e 0a  3c 74 79 70 65 3e 65 6e   i</url>. <type>en
0090  6b 65 6c 3c 2f 74 79 70  65 3e 0a 3c 66 72 6f 6d   kel</typ e>.<from
00a0  3e 4b c3 b8 62 65 6e 68  61 76 6e 3c 2f 66 72 6f   >K..benh avn</fro
00b0  6d 3e 0a 3c 2f 75 6e 69  74 3e 0a 3c 75 6e 69 74   m>.</uni t>.<unit
00c0  3e 0a 3c 64 65 73 74 3e  56 69 6c 6e 69 75 73 3c   >.<dest> Vilnius<
00d0  2f 64 65 73 74 3e 0a 3c  64 61 74 65 3e 3c 2f 64   /dest>.< date></d
00e0  61 74 65 3e 0a 3c 70 72  69 63 65 3e 33 39 35 2c   ate>.<pr ice>395,
```

```
74 6f 6d 3e 47 72 61  74 69 73 20 73 c3 a6 64   stom>Gra tis s..d
76 61 6c 67 3c 2f 63  75 73 74 6f 6d 3e 0a 3c   evalg</c ustom>.<
72 6c 3e 68 74 74 70  3a 2f 2f 77 77 77 2e 73   url>http ://www.s
73 2e 64 6b 2f 64 61  2f 48 65 6c 73 69 6e 6b   as.dk/da /Helsink
3c 2f 75 72 6c 3e 0a  3c 74 79 70 65 3e 65 6e   i</url>. <type>en
65 6c 3c 2f 74 79 70  65 3e 0a 3c 66 72 6f 6d   kel</typ e>.<from
4b c3 b8 62 65 6e 68  61 76 6e 3c 2f 66 72 6f   >K..benh avn</fro
```

File: "C:\Documents and Settings\rlo\Desktop\pcapFiler\NetDump_May6_2010.pcap" 1965 KB 00:00:44 | Packets: 2579 Displayed: 2579 Marked: 0 | Profile: Default

Double click a packet

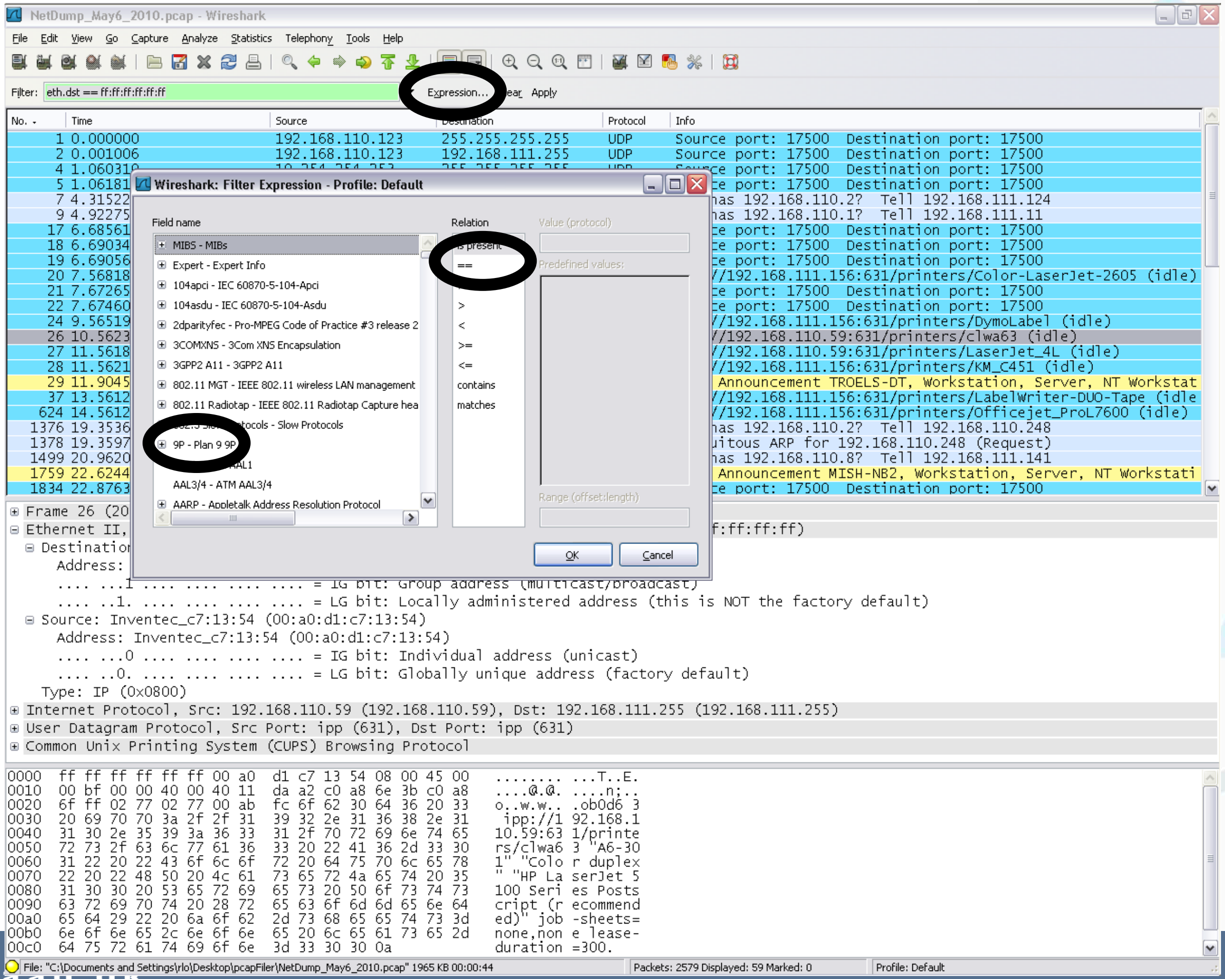
Detailed information about the protocols

Informations as they ”appear” in the network.

Filtering data packets

- To see all TCP traffic, write in the filter field
  - tcp
- To see traffic where130.255.51.45 is included write
  - ip.addr == 130.225.51.45
- To see traffic where130.255.51.45 is NOT included write
  - !(ip.addr == 130.225.51.45)
  - NB! ip.addr!=130.225.51.45 will NOT work (as you want it to)
- In the rules field note the colors
  - Green if the rule is valid
  - Red if the rule is invalid

Filtering via Graphical User Interface (GUI)


NetDump_May6_2010.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression...
Clear
Apply
Wireshark: Filter Expression - Profile: Default
Field name
Relation
Value (protocol)
Predefined values:
Range (offset:length)
OK
Cancel

Filter: eth.dst == ff:ff:ff:ff:ff:ff

Field name:
- ⊞ MIBS - MIBs
- ⊞ Expert - Expert Info
- ⊞ 104apci - IEC 60870-5-104-Apci
- ⊞ 104asdu - IEC 60870-5-104-Asdu
- ⊞ 2dparityfec - Pro-MPEG Code of Practice #3 release 2
- ⊞ 3COMXNS - 3Com XNS Encapsulation
- ⊞ 3GPP2 A11 - 3GPP2 A11
- ⊞ 802.11 MGT - IEEE 802.11 wireless LAN management
- ⊞ 802.11 Radiotap - IEEE 802.11 Radiotap Capture hea
- ...otocols - Slow Protocols
- ⊞ 9P - Plan 9 9P
- ...AAL1
- AAL3/4 - ATM AAL3/4
- ⊞ AARP - Appletalk Address Resolution Protocol

Relation:
- is present
- ==
- >
- <
- >=
- <=
- contains
- matches

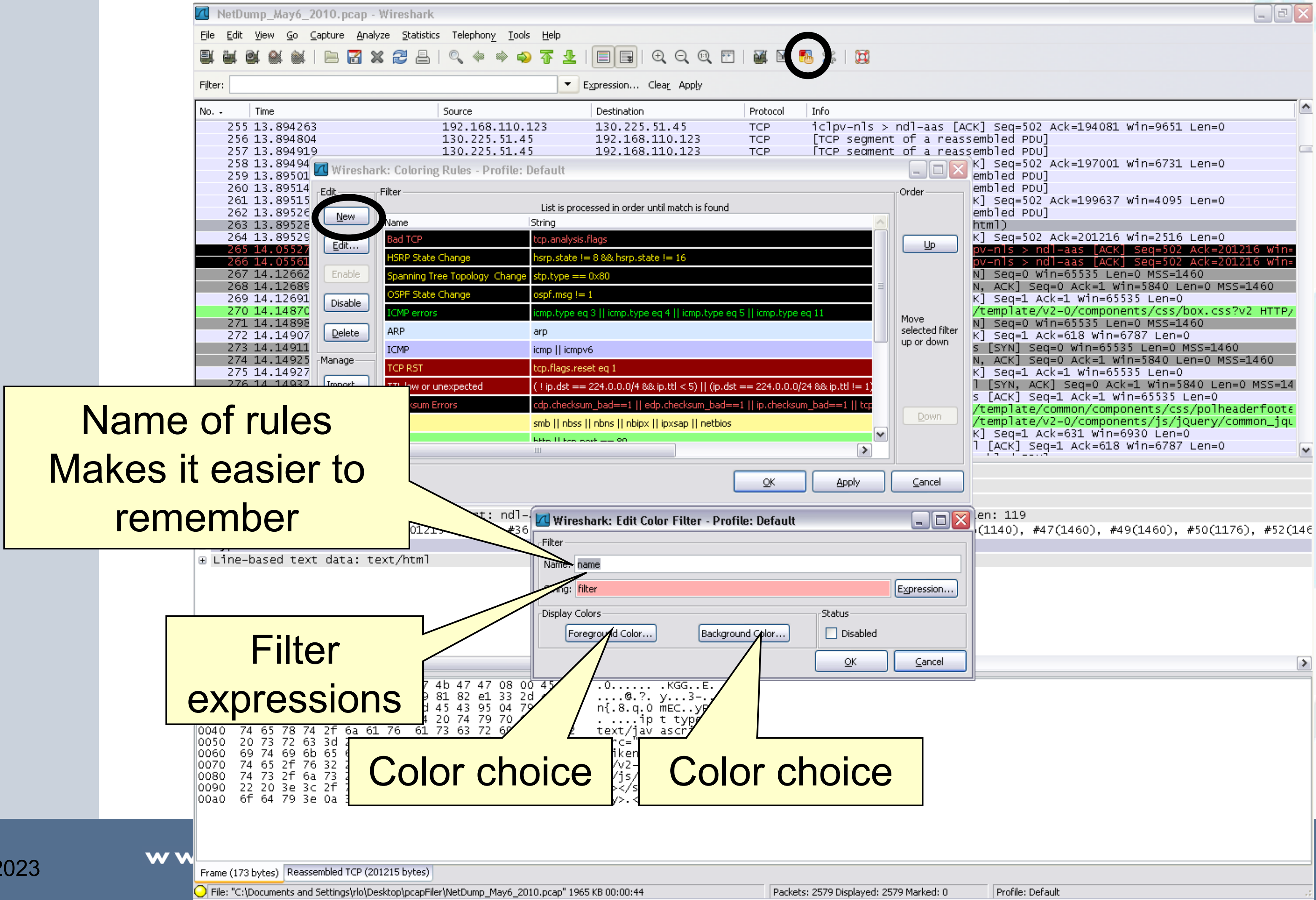
```
No. .  Time          Source            Destination       Protocol  Info
    1 0.000000     192.168.110.123   255.255.255.255   UDP       Source port: 17500  Destination port: 17500
    2 0.001006     192.168.110.123   192.168.111.255   UDP       Source port: 17500  Destination port: 17500
    4 1.060310                                                   Source port: 17500  Destination port: 17500
    5 1.06181                                                    ce port: 17500  Destination port: 17500
    7 4.31522                                                    has 192.168.110.2?  Tell 192.168.111.124
    9 4.92275                                                    has 192.168.110.1?  Tell 192.168.111.11
   17 6.68561                                                    ce port: 17500  Destination port: 17500
   18 6.69034                                                    ce port: 17500  Destination port: 17500
   19 6.69056                                                    ce port: 17500  Destination port: 17500
   20 7.56818                                                    //192.168.111.156:631/printers/Color-LaserJet-2605 (idle)
   21 7.67265                                                    ce port: 17500  Destination port: 17500
   22 7.67460                                                    ce port: 17500  Destination port: 17500
   24 9.56519                                                    //192.168.111.156:631/printers/DymoLabel (idle)
   26 10.5623                                                    //192.168.110.59:631/printers/clwa63 (idle)
   27 11.5618                                                    //192.168.110.59:631/printers/LaserJet_4L (idle)
   28 11.5621                                                    //192.168.111.156:631/printers/KM_C451 (idle)
   29 11.9045                                                     Announcement TROELS-DT, Workstation, Server, NT Workstat
   37 13.5612                                                    //192.168.111.156:631/printers/LabelWriter-DUO-Tape (idle
  624 14.5612                                                    //192.168.111.156:631/printers/Officejet_ProL7600 (idle)
 1376 19.3536                                                    has 192.168.110.2?  Tell 192.168.110.248
 1378 19.3597                                                    uitous ARP for 192.168.110.248 (Request)
 1499 20.9620                                                    has 192.168.110.8?  Tell 192.168.111.141
 1759 22.6244                                                     Announcement MISH-NB2, Workstation, Server, NT Workstati
 1834 22.8763                                                    ce port: 17500  Destination port: 17500
```

```
⊞ Frame 26 (20
⊟ Ethernet II,                                                   f:ff:ff:ff)
  ⊟ Destinatio
      Address:
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
  ⊟ Source: Inventec_c7:13:54 (00:a0:d1:c7:13:54)
      Address: Inventec_c7:13:54 (00:a0:d1:c7:13:54)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 192.168.110.59 (192.168.110.59), Dst: 192.168.111.255 (192.168.111.255)
⊞ User Datagram Protocol, Src Port: ipp (631), Dst Port: ipp (631)
⊞ Common Unix Printing System (CUPS) Browsing Protocol
```

```
0000  ff ff ff ff ff ff 00 a0  d1 c7 13 54 08 00 45 00   ........ ...T..E.
0010  00 bf 00 00 40 00 40 11  da a2 c0 a8 6e 3b c0 a8   ....@.@. ....n;..
0020  6f ff 02 77 02 77 00 ab  fc 6f 62 30 64 36 20 33   o..w.w.. .ob0d6 3
0030  20 69 70 70 3a 2f 2f 31  39 32 2e 31 36 38 2e 31    ipp://1 92.168.1
0040  31 30 2e 35 39 3a 36 33  31 2f 70 72 69 6e 74 65   10.59:63 1/printe
0050  72 73 2f 63 6c 77 61 36  33 20 22 41 36 2d 33 30   rs/clwa6 3 "A6-30
0060  31 22 20 22 43 6f 6c 6f  72 20 64 75 70 6c 65 78   1" "Colo r duplex
0070  22 20 22 48 50 20 4c 61  73 65 72 4a 65 74 20 35   " "HP La serJet 5
0080  31 30 30 20 53 65 72 69  65 73 20 50 6f 73 74 73   100 Seri es Posts
0090  63 72 69 70 74 20 28 72  65 63 6f 6d 6d 65 6e 64   cript (r ecommend
00a0  65 64 29 22 20 6a 6f 62  2d 73 68 65 65 74 73 3d   ed)" job -sheets=
00b0  6e 6f 6e 65 2c 6e 6f 6e  65 20 6c 65 61 73 65 2d   none,non e lease-
00c0  64 75 72 61 74 69 6f 6e  3d 33 30 30 0a            duration =300.
```

File: "C:\Documents and Settings\rlo\Desktop\pcapFiler\NetDump_May6_2010.pcap" 1965 KB 00:00:44 | Packets: 2579 Displayed: 59 Marked: 0 | Profile: Default

Rules can become colors



NetDump_May6_2010.pcap - Wireshark

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

```
No. -  Time         Source            Destination       Protocol  Info
  255 13.894263     192.168.110.123   130.225.51.45     TCP       iclpv-nls > ndl-aas [ACK] Seq=502 Ack=194081 Win=9651 Len=0
  256 13.894804     130.225.51.45     192.168.110.123   TCP       [TCP segment of a reassembled PDU]
  257 13.894919     130.225.51.45     192.168.110.123   TCP       [TCP segment of a reassembled PDU]
  258 13.89494                                                    K] Seq=502 Ack=197001 Win=6731 Len=0
  259 13.89501                                                    embled PDU]
  260 13.89514                                                    embled PDU]
  261 13.89515                                                    K] Seq=502 Ack=199637 Win=4095 Len=0
  262 13.89526                                                    embled PDU]
  263 13.89528                                                    html)
  264 13.89529                                                    K] Seq=502 Ack=201216 Win=2516 Len=0
  265 14.05527                                                    pv-nls > ndl-aas [ACK] Seq=502 Ack=201216 Win=
  266 14.05561                                                    pv-nls > ndl-aas [ACK] Seq=502 Ack=201216 Win=
  267 14.12662                                                    N] Seq=0 Win=65535 Len=0 MSS=1460
  268 14.12689                                                    N, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
  269 14.12691                                                    K] Seq=1 Ack=1 Win=65535 Len=0
  270 14.14870                                                    /template/v2-0/components/css/box.css?v2 HTTP/
  271 14.14898                                                    N] Seq=0 Win=65535 Len=0 MSS=1460
  272 14.14907                                                    K] Seq=1 Ack=618 Win=6787 Len=0
  273 14.14911                                                    s [SYN] Seq=0 Win=65535 Len=0 MSS=1460
  274 14.14925                                                    N, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
  275 14.14927                                                    K] Seq=1 Ack=1 Win=65535 Len=0
                                                                  l [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=14
                                                                  s [ACK] Seq=1 Ack=1 Win=65535 Len=0
                                                                  /template/common/components/css/polheaderfoote
                                                                  /template/v2-0/components/js/jQuery/common_jqu
                                                                  K] Seq=1 Ack=631 Win=6930 Len=0
                                                                  l [ACK] Seq=1 Ack=618 Win=6787 Len=0
```

Wireshark: Coloring Rules - Profile: Default

List is processed in order until match is found

Name	String
Bad TCP	tcp.analysis.flags
HSRP State Change	hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change	stp.type == 0x80
OSPF State Change	ospf.msg != 1
ICMP errors	icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11
ARP	arp
ICMP	icmp || icmpv6
TCP RST	tcp.flags.reset eq 1
TTL low or unexpected	(! ip.dst == 224.0.0.0/4 && ip.ttl < 5) || (ip.dst == 224.0.0.0/24 && ip.ttl != 1)
Checksum Errors	cdp.checksum_bad==1 || edp.checksum_bad==1 || ip.checksum_bad==1 || tcp
	smb || nbss || nbns || nbipx || ipxsap || netbios
	http || tcp.port == 80

```
t: ndl-                          en: 119
0121           #36               (1140), #47(1460), #49(1460), #50(1176), #52(146
⊞ Line-based text data: text/html
```

Wireshark: Edit Color Filter - Profile: Default

Filter
Name: name
String: filter

☐ Disabled

```
7 4b 47 47 08 00 45      .O...... .KGG..E.
9 81 82 e1 33 2d         ....@.?. y...3-..
d 45 43 95 04 79         n{.8.q.O mEC..yF
4 20 74 79 70            . ....ip t typ
0040  74 65 78 74 2f 6a 61 76  61 73 63 72 69      text/jav ascr
0050  20 73 72 63 3d                              rc="
0060  69 74 69 6b 65                              iken
0070  74 65 2f 76 32                              /v2-
0080  74 73 2f 6a 73                              /js/
0090  22 20 3e 3c 2f                              ></s
00a0  6f 64 79 3e 0a                              y>.<
```

Frame (173 bytes) | Reassembled TCP (201215 bytes)

File: "C:\Documents and Settings\rlo\Desktop\pcapFiler\NetDump_May6_2010.pcap" 1965 KB 00:00:44 | Packets: 2579 Displayed: 2579 Marked: 0 | Profile: Default

Name of rules
Makes it easier to
remember

Filter
expressions

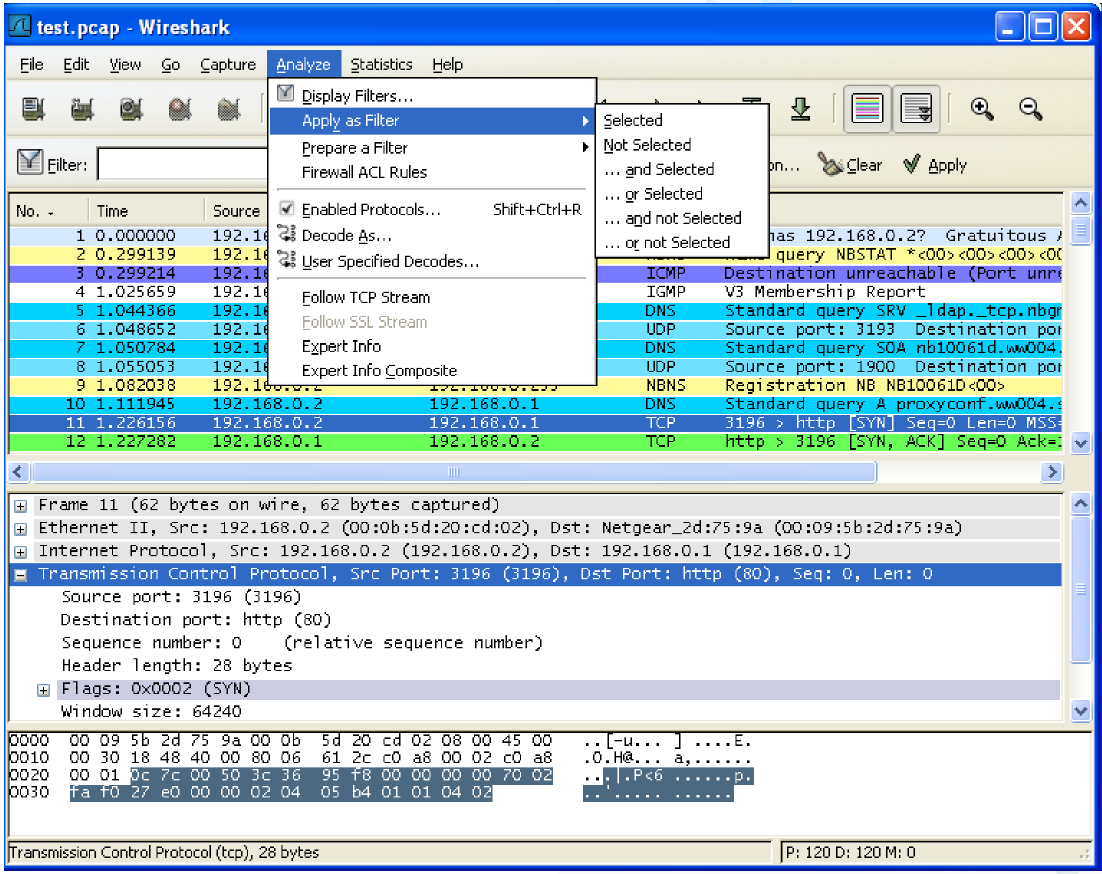
Color choice

Color choice

Wireshark for analyzing data

The analyze menu has several pratical entries

- Make a filter from marked packets
- Protocols on/off
- Decoding of e.g. Ports as specific protocols.
- Follow
  - TCP flows
  - UDP dialog
- Expert information
  - Dialog
  - Errors
  - Warnings



```
No. -   Time        Source
    1 0.000000    192.16                                                  has 192.168.0.2?  Gratuitous A
    2 0.299139    192.16                                                  query NBSTAT *<00><00><00><0
    3 0.299214    192.16                                          ICMP    Destination unreachable (Port unre
    4 1.025659    192.16                                          IGMP    V3 Membership Report
    5 1.044366    192.16                                          DNS     Standard query SRV _ldap._tcp.nbgr
    6 1.048652    192.16                                          UDP     Source port: 3193  Destination por
    7 1.050784    192.16                                          DNS     Standard query SOA nb10061d.ww004.
    8 1.055053    192.16                                          UDP     Source port: 1900  Destination por
    9 1.082038    192.168.0.2           192.168.0.255             NBNS    Registration NB NB10061D<00>
   10 1.111945    192.168.0.2           192.168.0.1               DNS     Standard query A proxyconf.ww004.s
   11 1.226156    192.168.0.2           192.168.0.1               TCP     3196 > http [SYN] Seq=0 Len=0 MSS=
   12 1.227282    192.168.0.1           192.168.0.2               TCP     http > 3196 [SYN, ACK] Seq=0 Ack=1
```

```
⊞ Frame 11 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)
⊞ Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
⊟ Transmission Control Protocol, Src Port: 3196 (3196), Dst Port: http (80), Seq: 0, Len: 0
    Source port: 3196 (3196)
    Destination port: http (80)
    Sequence number: 0    (relative sequence number)
    Header length: 28 bytes
  ⊞ Flags: 0x0002 (SYN)
    Window size: 64240
```

```
0000  00 09 5b 2d 75 9a 00 0b  5d 20 cd 02 08 00 45 00   ..[-u... ] ....E.
0010  00 30 18 48 40 00 80 06  61 2c c0 a8 00 02 c0 a8   .0.H@... a,......
0020  00 01 0c 7c 00 50 3c 36  95 f8 00 00 00 00 70 02   ...|.P<6 ......p.
0030  fa f0 27 e0 00 00 02 04  05 b4 01 01 04 02         ..'..... ......
```

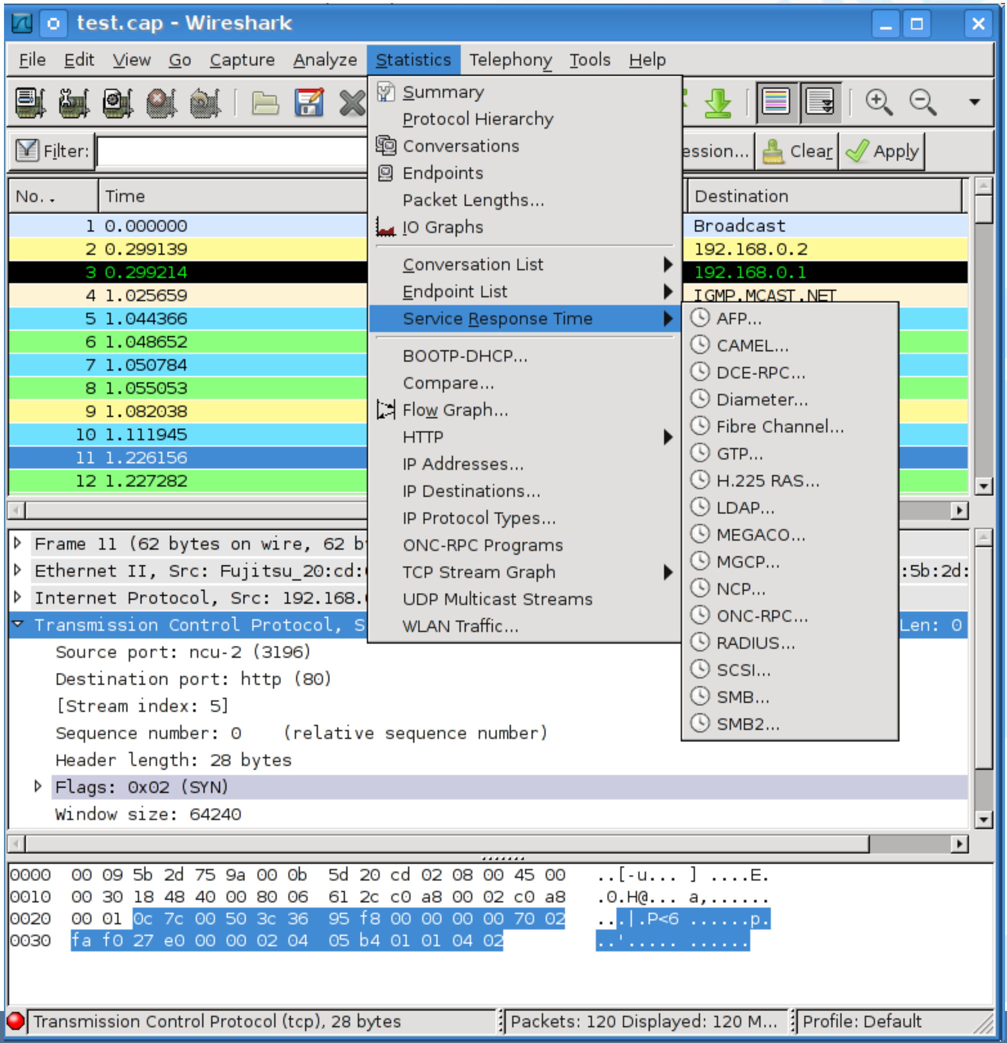
Transmission Control Protocol (tcp), 28 bytes

P: 120 D: 120 M: 0

Wireshark - Statistics

- General statistics
- Protocol hierarchy
- Conversations
- End points
- Input/Output
- Data flows
  - HTTP traffic
  - TCP and UDP

- And much more …



```
No. .   Time                Destination
    1 0.000000              Broadcast
    2 0.299139              192.168.0.2
    3 0.299214              192.168.0.1
    4 1.025659              IGMP.MCAST.NET
    5 1.044366
    6 1.048652
    7 1.050784
    8 1.055053
    9 1.082038
   10 1.111945
   11 1.226156
   12 1.227282
```

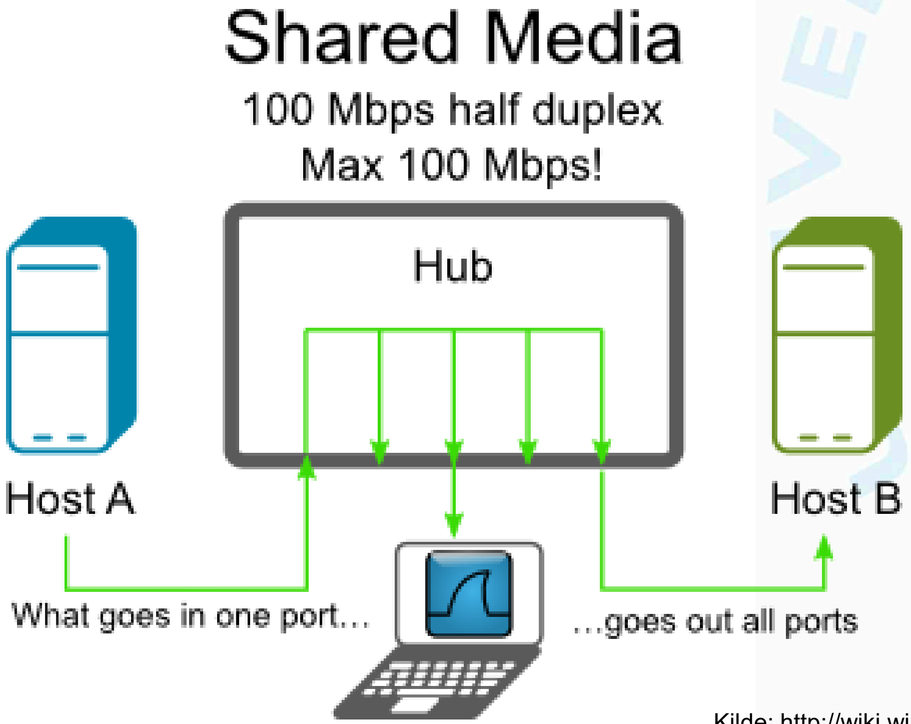
```
▷ Frame 11 (62 bytes on wire, 62 b
▷ Ethernet II, Src: Fujitsu_20:cd:                 :5b:2d:
▷ Internet Protocol, Src: 192.168.
▽ Transmission Control Protocol, S                 Len: 0
    Source port: ncu-2 (3196)
    Destination port: http (80)
    [Stream index: 5]
    Sequence number: 0    (relative sequence number)
    Header length: 28 bytes
  ▷ Flags: 0x02 (SYN)
    Window size: 64240
```

```
0000  00 09 5b 2d 75 9a 00 0b  5d 20 cd 02 08 00 45 00   ..[-u... ] ....E.
0010  00 30 18 48 40 00 80 06  61 2c c0 a8 00 02 c0 a8   .0.H@... a,......
0020  00 01 0c 7c 00 50 3c 36  95 f8 00 00 00 00 70 02   ...|.P<6 ......p.
0030  fa f0 27 e0 00 00 02 04  05 b4 01 01 04 02         ..'..... ......
```

Transmission Control Protocol (tcp), 28 bytes | Packets: 120 Displayed: 120 M... | Profile: Default

Place your wireshark monitor in the right place#1

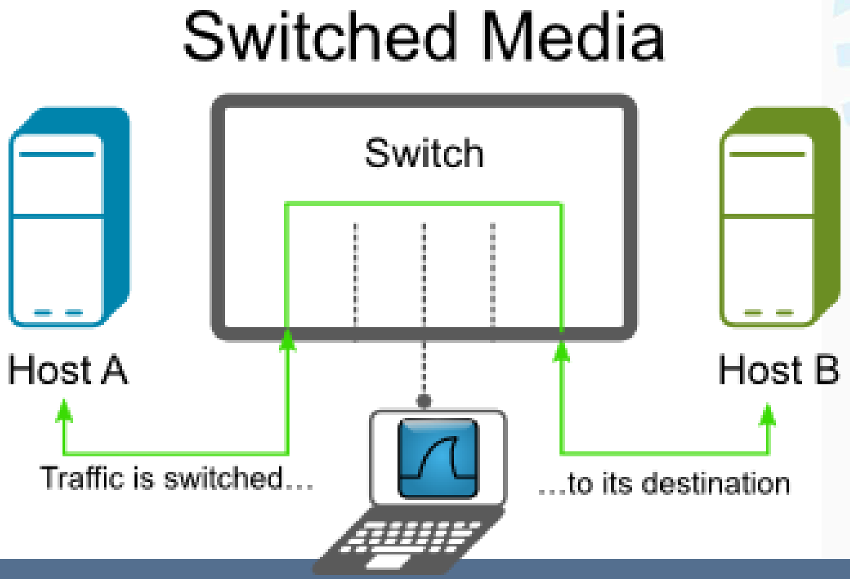
- Simple LAN with a hub
  - Wireshark will see everything that is electrical ☺



Kilde: http://wiki.wireshark.org/CaptureSetup/Ethernet

Place your wireshark monitor in the right place#2

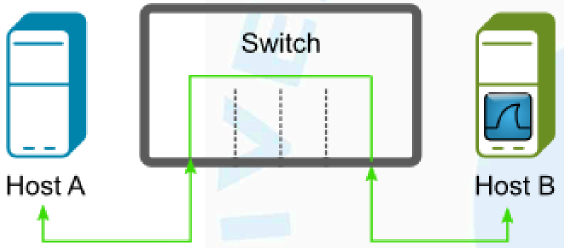
- A switched Ethernet is a bit more tricky
  - Only unicast to/from the machine and broadcast/multicast messages are captures, even in promiscous mode.
  - Routers/switches may have a monitor port though…
  - VLAN does the same



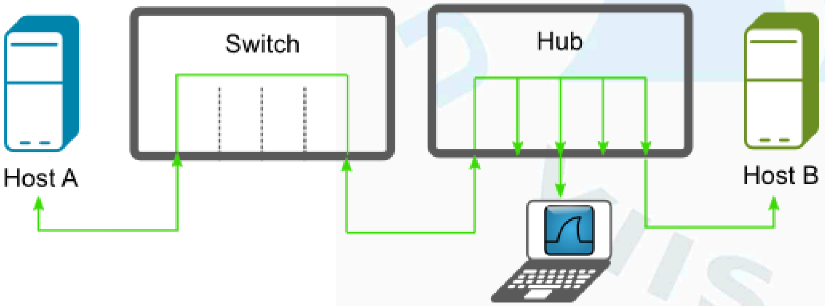
Place your wireshark monitor in the right place#3

- Solutions
  - Same computer
    - Easy solution
    - Cannot see other kinds of traffic than broad/multicast and to/from Host B
  - Insert a hub
    - Quite easy
    - Temporary network abruption for setting it up
    - Little performance loss
    - NB!
      Some hubs are actually switches!

Switched Media — Same Computer

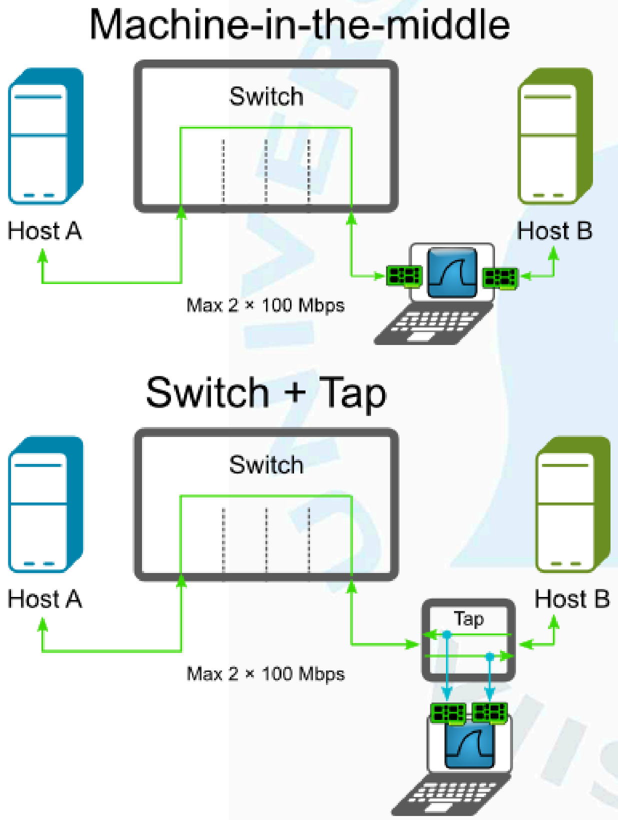


Switched Media — "Hubbing Out



Place your wireshark monitor in the right place#4

- Machine-in-the-middle
  - No changes in the hosts
  - Dedicated configuration required – as well as access to the network on the HOST B side.
- Special cable TAPs are also available



Place your wireshark monitor in the right place#5

- Wireless networks
  - Select the right frequency and channel
  - Select the right SSID/ESSID
- Promiscous mode only works on networks with the same SSID, and often gives problems in Windows...
- To observe all packets at a given frequency, despite SSID, Wireshark must be put into monitor mode (not supported by Windows).

Assignment Part 1

Jens Myrup Pedersen
jens@es.aau.dk

Problem 1.1

- Install and set up wireshark for monitoring traffic
  - Setup the interface to monitor
- Try to catch traffic, when e.g. opening a website
- How much traffic do you see on the network
  - How many packets?
  - What is the average
    - Packet size?
    - Number of packets per second?
    - Total number of bytes – and bytes per second?
- How many types of protocols did you find in your measurements?

Problem 1.2 – Layer 2

- Find the MAC address of your machine
  - In Ethernet and/or wireless network interface -> Start a command prompt and write ”ipconfig /all”
  - What is the name of your interface?
- Make a dump of what happens in the network
  - What is your machine sending and receiving?

Problem 1.3 – IP addressing

- First try this
  - Find your IP address using ”ipconfig /all”
    - Which services are registrered, and what are their IP addresses?
  - Reset Wireshark, capture for a few minutes (or reuse)
    - Is the communication to your registrered devices?

- Open netdump_may6_2010.pcap
  - What traffic goes to and from
    - 192.168.110.123
    - 192.168.111.255
    - 10.254.254.253
  - What network type and class are we on?
  - Who is asking for who in the network?

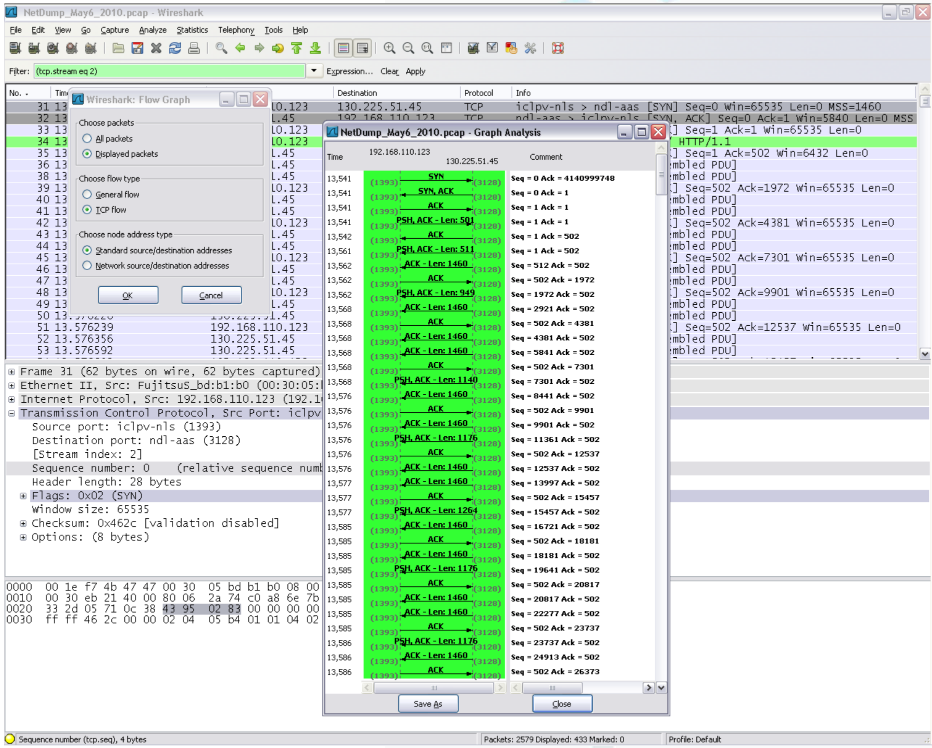
Problem 1.4 - UDP

- Open netdump_may6_2010.pcap
  - Who is speaking to who, and why?
    - NB! Husk broadcast har en IP adresse!
  - Who is the most often (UDP) communicating IP device on the network? To what port? How many packets/data?
  - How large share of the total traffic is UDP?

- The application dropbox sends out UDP packets at a frequency on part 17500 – what is the frequency?

Problem 1.5 - TCP

- Open http.pcap
- Follow the TCP flow in the diagram
- Question
  - What happens?
  - How big are the TCP packets?



NetDump_May6_2010.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression... Clear Apply
Wireshark: Flow Graph
OK
Cancel
NetDump_May6_2010.pcap - Graph Analysis
Save As
Close

Filter: (tcp.stream eq 2)

Choose packets: ○ All packets ● Displayed packets

Choose flow type: ○ General flow ● TCP flow

Choose node address type: ● Standard source/destination addresses ○ Network source/destination addresses

```
No. .  Time        Destination     Protocol  Info
31 13              130.225.51.45   TCP       iclpv-nls > ndl-aas [SYN] Seq=0 Win=65535 Len=0 MSS=1460
32 13              192.168.110.123 TCP       ndl-aas > iclpv-nls [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS
33 13  10.123                                ] Seq=1 Ack=1 Win=65535 Len=0
34 13  10.123                                HTTP/1.1
35 13  L.45                                  ] Seq=1 Ack=502 Win=6432 Len=0
36 13  L.45                                  mbled PDU]
38 13  L.45                                  mbled PDU]
39 13  10.123                                ] Seq=502 Ack=1972 Win=65535 Len=0
40 13  L.45                                  mbled PDU]
41 13  L.45                                  mbled PDU]
42 13  10.123                                ] Seq=502 Ack=4381 Win=65535 Len=0
43 13  L.45                                  mbled PDU]
44 13  L.45                                  mbled PDU]
45 13  10.123                                ] Seq=502 Ack=7301 Win=65535 Len=0
46 13  L.45                                  mbled PDU]
47 13  L.45                                  mbled PDU]
48 13  10.123                                ] Seq=502 Ack=9901 Win=65535 Len=0
49 13  L.45                                  mbled PDU]
50 13.                 1.45                  mbled PDU]
51 13.576239     192.168.110.123             ] Seq=502 Ack=12537 Win=65535 Len=0
52 13.576356     130.225.51.45               mbled PDU]
53 13.576592     130.225.51.45               mbled PDU]
```

```
⊞ Frame 31 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: FujitsuS_bd:b1:b0 (00:30:05:
⊞ Internet Protocol, Src: 192.168.110.123 (192.1
⊟ Transmission Control Protocol, Src Port: iclpv
    Source port: iclpv-nls (1393)
    Destination port: ndl-aas (3128)
    [Stream index: 2]
    Sequence number: 0    (relative sequence numb
    Header length: 28 bytes
  ⊞ Flags: 0x02 (SYN)
    Window size: 65535
  ⊞ Checksum: 0x462c [validation disabled]
  ⊞ Options: (8 bytes)
```

```
0000  00 1e f7 4b 47 47 00 30  05 bd b1 b0 08 00
0010  00 30 eb 21 40 00 80 06  2a 74 c0 a8 6e 7b
0020  33 2d 05 71 0c 38 43 95  02 83 00 00 00 00
0030  ff ff 46 2c 00 00 02 04  05 b4 01 01 04 02
```

Time	192.168.110.123		130.225.51.45	Comment
13,541	(1393)	SYN →	(3128)	Seq = 0 Ack = 4140999748
13,541	(1393)	← SYN, ACK	(3128)	Seq = 0 Ack = 1
13,541	(1393)	ACK →	(3128)	Seq = 1 Ack = 1
13,541	(1393)	PSH, ACK - Len: 501 →	(3128)	Seq = 1 Ack = 1
13,542	(1393)	← ACK	(3128)	Seq = 1 Ack = 502
13,561	(1393)	← PSH, ACK - Len: 511	(3128)	Seq = 1 Ack = 502
13,562	(1393)	← ACK - Len: 1460	(3128)	Seq = 512 Ack = 502
13,562	(1393)	ACK →	(3128)	Seq = 502 Ack = 1972
13,562	(1393)	← PSH, ACK - Len: 949	(3128)	Seq = 1972 Ack = 502
13,568	(1393)	← ACK - Len: 1460	(3128)	Seq = 2921 Ack = 502
13,568	(1393)	ACK →	(3128)	Seq = 502 Ack = 4381
13,568	(1393)	← ACK - Len: 1460	(3128)	Seq = 4381 Ack = 502
13,568	(1393)	← ACK - Len: 1460	(3128)	Seq = 5841 Ack = 502
13,568	(1393)	ACK →	(3128)	Seq = 502 Ack = 7301
13,568	(1393)	← PSH, ACK - Len: 1140	(3128)	Seq = 7301 Ack = 502
13,576	(1393)	← ACK - Len: 1460	(3128)	Seq = 8441 Ack = 502
13,576	(1393)	ACK →	(3128)	Seq = 502 Ack = 9901
13,576	(1393)	← ACK - Len: 1460	(3128)	Seq = 9901 Ack = 502
13,576	(1393)	← PSH, ACK - Len: 1176	(3128)	Seq = 11361 Ack = 502
13,576	(1393)	ACK →	(3128)	Seq = 502 Ack = 12537
13,576	(1393)	← ACK - Len: 1460	(3128)	Seq = 12537 Ack = 502
13,577	(1393)	← ACK - Len: 1460	(3128)	Seq = 13997 Ack = 502
13,577	(1393)	ACK →	(3128)	Seq = 502 Ack = 15457
13,577	(1393)	← PSH, ACK - Len: 1264	(3128)	Seq = 15457 Ack = 502
13,585	(1393)	← ACK - Len: 1460	(3128)	Seq = 16721 Ack = 502
13,585	(1393)	ACK →	(3128)	Seq = 502 Ack = 18181
13,585	(1393)	← ACK - Len: 1460	(3128)	Seq = 18181 Ack = 502
13,585	(1393)	← PSH, ACK - Len: 1176	(3128)	Seq = 19641 Ack = 502
13,585	(1393)	ACK →	(3128)	Seq = 502 Ack = 20817
13,585	(1393)	← ACK - Len: 1460	(3128)	Seq = 20817 Ack = 502
13,585	(1393)	← ACK - Len: 1460	(3128)	Seq = 22277 Ack = 502
13,585	(1393)	ACK →	(3128)	Seq = 502 Ack = 23737
13,586	(1393)	← PSH, ACK - Len: 1176	(3128)	Seq = 23737 Ack = 502
13,586	(1393)	← ACK - Len: 1460	(3128)	Seq = 24913 Ack = 502
13,586	(1393)	ACK →	(3128)	Seq = 502 Ack = 26373

Sequence number (tcp.seq), 4 bytes | Packets: 2579 Displayed: 433 Marked: 0 | Profile: Default

Problem 1.6 - statistics

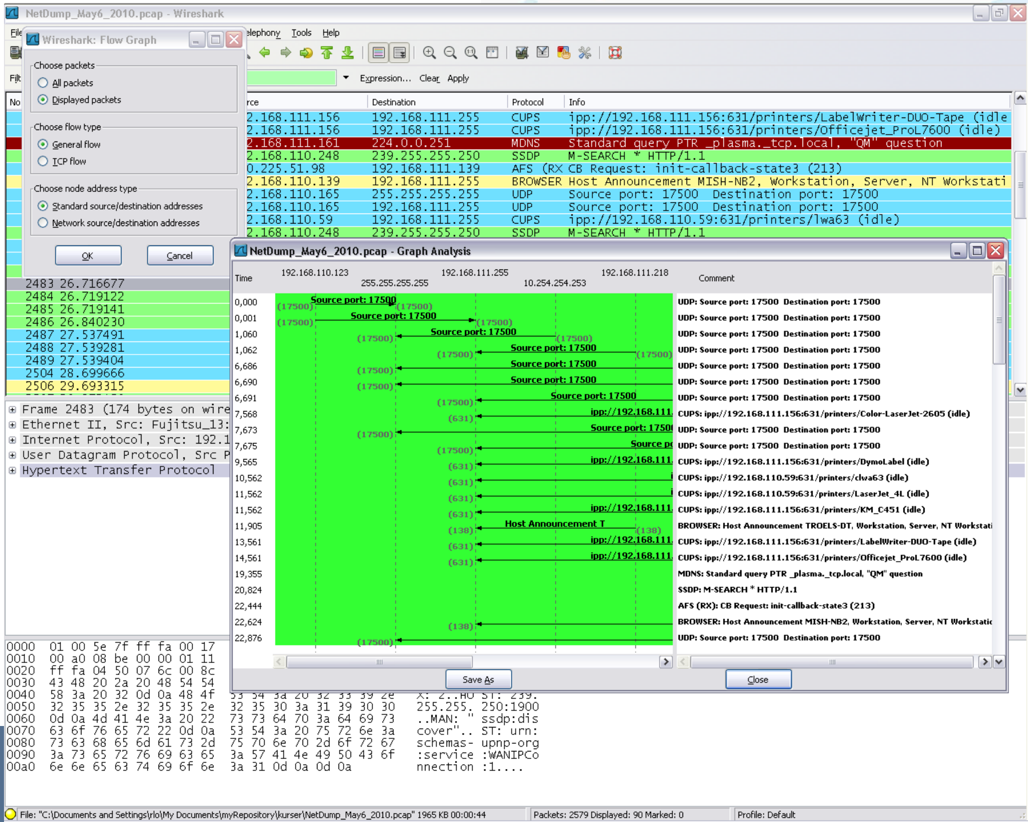
- Choose Statistics -> Packet Length..
  - Click ”create stat” with a given filter
  - What is the typical packet size? Why?
- TCP endpoints – who are we really communicating with?
  - Choose Statistics-> EndPoint list -> TCP(IPv4&IPv6)
  - Who has the machine been in touch with?
- Choose Analyze -> Expert Info
  - What do we see here?

Problem 1.7 – more TCP

- Record a sequence where you visit a website (that do not require password or contain sensitive data).
- Investigate the TCP conversations
  - Filter TCP packets between different machines
    - Write e.g. *(ip.addr==192.168.110.123||ip.addr==130.225.51.45)&&tcp*
  - Choose a TCP packet, og go to Analyze->Follow TCP flow
    - You might filter the TCP stream with ”tcp.stream eq x”, where x is a number that indicated a stream number.
  - Filter the stream by clicking ”Filter out this stream” and remove ”!” from the filter field.

Problem 1.8 - filtering

- See what UDP traffic there is...
  - Write *udp* in the filter field and click 'apply'
- Go to Statistics-> Flowchart
- Follow the conversations
  - Who's talking to who, and why?



NetDump_May6_2010.pcap - Wireshark

Wireshark: Flow Graph

Choose packets
○ All packets
● Displayed packets

Choose flow type
● General flow
○ TCP flow

Choose node address type
● Standard source/destination addresses
○ Network source/destination addresses

```
rce              Destination      Protocol Info
2.168.111.156    192.168.111.255  CUPS     ipp://192.168.111.156:631/printers/LabelWriter-DUO-Tape (idle
2.168.111.156    192.168.111.255  CUPS     ipp://192.168.111.156:631/printers/Officejet_ProL7600 (idle)
2.168.111.161    224.0.0.251      MDNS     Standard query PTR _plasma._tcp.local, "QM" question
2.168.110.248    239.255.255.250  SSDP     M-SEARCH * HTTP/1.1
0.225.51.98      192.168.111.139  AFS (RX CB Request: init-callback-state3 (213)
2.168.110.139    192.168.111.255  BROWSER Host Announcement MISH-NB2, Workstation, Server, NT Workstati
2.168.110.165    255.255.255.255  UDP      Source port: 17500  Destination port: 17500
2.168.110.165    192.168.111.255  UDP      Source port: 17500  Destination port: 17500
2.168.110.59     192.168.111.255  CUPS     ipp://192.168.110.59:631/printers/lwa63 (idle)
2.168.110.248    239.255.255.250  SSDP     M-SEARCH * HTTP/1.1
```

```
No
2483 26.716677
2484 26.719122
2485 26.719141
2486 26.840230
2487 27.537491
2488 27.539281
2489 27.539404
2504 28.699666
2506 29.693315
```

```
⊞ Frame 2483 (174 bytes on wire
⊞ Ethernet II, Src: Fujitsu_13:
⊞ Internet Protocol, Src: 192.1
⊞ User Datagram Protocol, Src P
⊞ Hypertext Transfer Protocol
```

```
0000  01 00 5e 7f ff fa 00 17
0010  00 a0 08 be 00 00 01 11
0020  ff fa 04 50 07 6c 00 8c
0030  43 48 20 2a 20 48 54 54
0040  58 3a 20 32 0d 0a 48 4f  53 54 3a 20 32 33 39 2e   X: 2..HO ST: 239.
0050  32 35 35 2e 32 35 35 2e  32 35 30 3a 31 39 30 30   255.255. 250:1900
0060  0d 0a 4d 41 4e 3a 20 22  73 73 64 70 3a 64 69 73   ..MAN: " ssdp:dis
0070  63 6f 76 65 72 22 0d 0a  53 54 3a 20 75 72 6e 3a   cover".. ST: urn:
0080  73 63 68 65 6d 61 73 2d  75 70 6e 70 2d 6f 72 67   schemas- upnp-org
0090  3a 73 65 72 76 69 63 65  3a 57 41 4e 49 50 43 6f   :service :WANIPCo
00a0  6e 6e 65 63 74 69 6f 6e  3a 31 0d 0a 0d 0a         nnection :1....
```

NetDump_May6_2010.pcap - Graph Analysis

```
Time    Comment
0,000   UDP: Source port: 17500  Destination port: 17500
0,001   UDP: Source port: 17500  Destination port: 17500
1,060   UDP: Source port: 17500  Destination port: 17500
1,062   UDP: Source port: 17500  Destination port: 17500
6,686   UDP: Source port: 17500  Destination port: 17500
6,690   UDP: Source port: 17500  Destination port: 17500
6,691   UDP: Source port: 17500  Destination port: 17500
7,568   CUPS: ipp://192.168.111.156:631/printers/Color-LaserJet-2605 (idle)
7,673   UDP: Source port: 17500  Destination port: 17500
7,675   UDP: Source port: 17500  Destination port: 17500
9,565   CUPS: ipp://192.168.111.156:631/printers/DymoLabel (idle)
10,562  CUPS: ipp://192.168.110.59:631/printers/clwa63 (idle)
11,562  CUPS: ipp://192.168.110.59:631/printers/LaserJet_4L (idle)
11,562  CUPS: ipp://192.168.111.156:631/printers/KM_C451 (idle)
11,905  BROWSER: Host Announcement TROELS-DT, Workstation, Server, NT Workstati
13,561  CUPS: ipp://192.168.111.156:631/printers/LabelWriter-DUO-Tape (idle)
14,561  CUPS: ipp://192.168.111.156:631/printers/Officejet_ProL7600 (idle)
19,355  MDNS: Standard query PTR _plasma._tcp.local, "QM" question
20,824  SSDP: M-SEARCH * HTTP/1.1
22,444  AFS (RX): CB Request: init-callback-state3 (213)
22,624  BROWSER: Host Announcement MISH-NB2, Workstation, Server, NT Workstatic
22,876  UDP: Source port: 17500  Destination port: 17500
```

File: "C:\Documents and Settings\rlo\My Documents\myRepository\kurser\NetDump_May6_2010.pcap" 1965 KB 00:00:44 | Packets: 2579 Displayed: 90 Marked: 0 | Profile: Default

Problem 1.9 - TCP/UDP

- Open telnet.pcap
  - Example of a telnet session, but who is involved?
  - Based on the IP addresses, what can we say about the involved?
  - Go to Analyze -> Follow TCP stream: what is the password for this user?
- Open tcp-scan.pcap
  - Explain – what happens here?
  - How much traffic is generated?
  - How long time does it take?
- Open udp-scan.pcap
  - What happens here?
  - What is the difference from tcp-scan.pcap?

Problem 1.10 – DHCP and DNS

- DHCP
  - From DHCP.pcap,
  - How long time does it take to get an IP address
  - Which address did the client get, and for how long?
  - How long into the header is the IP address found?
- DNS
  - Open HTTP.pcap
  - How much is the DNS traffic taking up? Of the total traffic?
  - Where is the DNS server?
  - What is the question – and the answer?

Problem 1.11 – Encrypted traffic

- Try to set up network with different encryption schemes, e.g. WEP and WPA-2. Can you monitor the traffic from others and listening in on the encrypted traffic?
- You are welcome to solve this problem in bigger groups.
- You are welcome to use hardware, e.g. Pineapple and WiFi de-author.

Assignment Part 2

Problem 2.1 - MyBot

Purpose
•This bot scans the LAN network, probably to spread to nearby computers as a worm. This can for example be used in order to spread in companies in order to harvest informations.

Exercise
1.Open ”bot_trace1.pcap”
2.Can you tell what happens here?

Problem 2.2 - Grum

Purpose

•This bot tries to distribute spam in the form of emails. Maybe to spread itself through emails, for phishing , or simply just spam…

Exercise

1.Open ”bot_trace7.pcap”
2.Can you tell what happens here?
3.Is the bot allowed to send emails?

Problem 2.3 – Agobot.aeq

Purpose

•This bot reveals an unknown attack functionality, since the bot never receives commands (the C&C server does not exist anymore), so it goes into a sleep mode.

Exercise

•Open ”agobot-aeq-test1.pcap”

•Can you tell what happens here?

Problem 2.4 – Agobot.02.d

Purpose

- This bot tries to connect to an IRC server and channel. This succeeds, but the IRC has defeated the bot and writes as a response that the computer is infected. When no commands are received it goes into sleep mode.

Exercise

- Open ”agobot-02-d-test1.pcap”
- Can you tell what happens here (hint) Filter ”dns” find us.undernet.org and remove filter
- What happens after the IP address lookup?

Problem 2.5 – Agobot.eo

Exercise

- What do you think happens here?

Problem 2.6 – Botnet Mix

Exercise

- How many different things can you find?