## cattura di pacchetti http

accesso al sito del corso

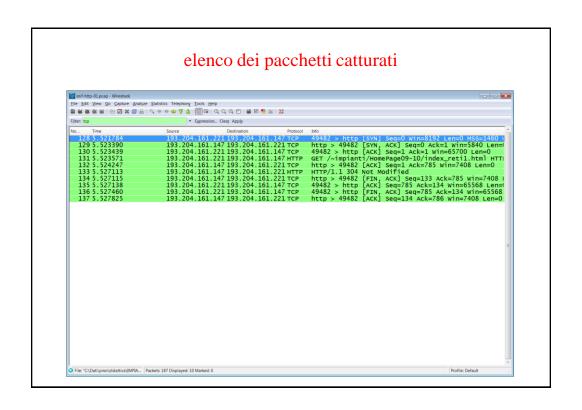
giuseppe di battista

## nota di copyright

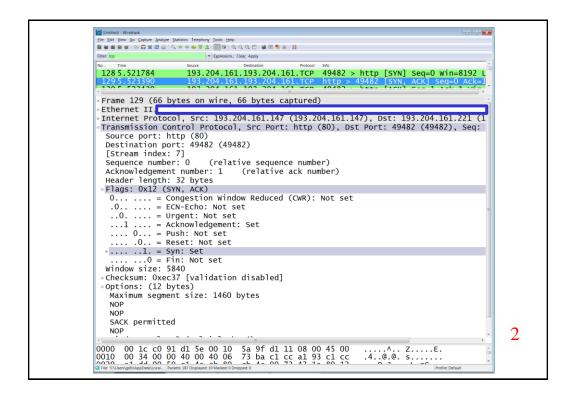
- questo insieme di slides è protetto dalle leggi sul copyright
- il titolo ed il copyright relativi alle slides (inclusi, ma non limitatamente, immagini, foto, animazioni, video, audio, musica e testo) sono di proprietà degli autori indicati sulla prima pagina
- le slides possono essere riprodotte ed utilizzate liberamente, non a fini di lucro, da università e scuole pubbliche e da istituti pubblici di ricerca
- ogni altro uso o riproduzione è vietata, se non esplicitamente autorizzata per iscritto, a priori, da parte degli autori
- l'informazione contenuta in queste slides è fornita per scopi didattici e non può essere usata in progetti di reti, impianti, prodotti, ecc.
- gli autori non si assumono nessuna responsabilità per il contenuto delle slides, che sono comunque soggette a cambiamento
- questa nota di copyright non deve essere mai rimossa e deve essere riportata anche in casi di uso parziale

## cattura dei pacchetti con wireshark

- accesso alla pagina http://www.dia.uniroma3.it/~impianti/HomePage09-10/index\_reti1.html
- browser usato: mozilla firefox



```
Filter: tcp Expression.. Clear Apply
 129 5.523390 193.204.161.193.204.161.TCP http > 49482 [SYN, ACK] Seq=0 Ack=1
 Frame 128 (66 bytes on wire, 66 bytes captured)
 Ethernet II,
Internet Protocol, Src: 193.204.161.221 (193.204.161.221), Dst: 193.204.161.147 (19
 Transmission Control Protocol, Src Port: 49482 (49482), Dst Port: http (80), Seq: 0
  Source port: 49482 (49482)
  Destination port: http (80)
  [Stream index: 7]
  Sequence number: 0
                       (relative sequence number)
  Header length: 32 bytes
  Flags: 0x02 (SYN)
  0... = Congestion Window Reduced (CWR): Not set .0... = ECN-Echo: Not set
   ..0. .... = Urgent: Not set
   ...0 ... = Acknowledgement: Not set
...0 ... = Push: Not set
...0. = Reset: Not set
  .... ...0 = Fin: Not set
Window size: 8192
  Checksum: 0x79e6 [validation disabled]
  Options: (12 bytes)
   Maximum segment size: 1460 bytes
  NOP
  Window scale: 2 (multiply by 4)
  NOP
  NOP
   SACK permitted
                                                                                       1
```

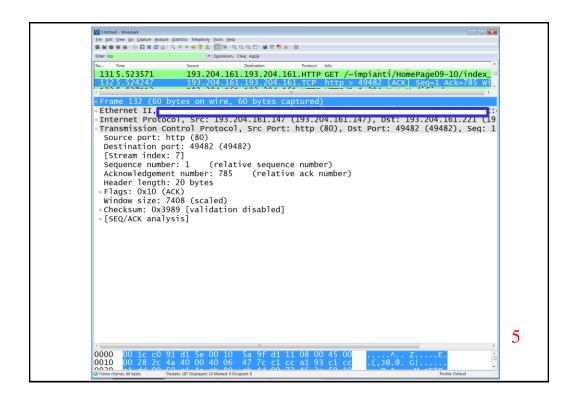


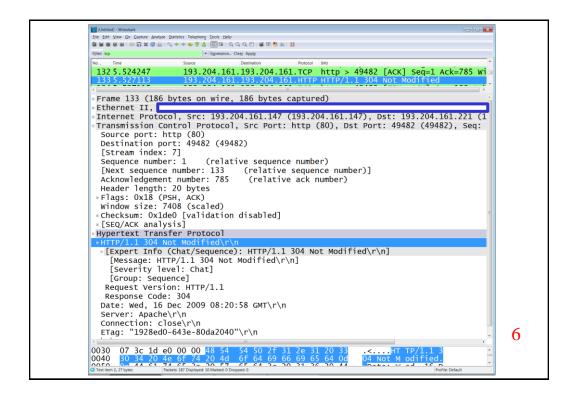
```
Elle Edit View Go Capture Analyze Statistics Tele
193.204.161.193.204.161.TCP http > 49482 [SYN, ACK] Seq=0 Ack=1
 Frame 130 (54 bytes on wire, 54 bytes captured)
 Ethernet II,
Internet Protocol, Src: 193.204.161.221 (193.204.161.221), Dst: 193.204.161.147
 Transmission Control Protocol, Src Port: 49482 (49482), Dst Port: http (80), Seq: 1 Source port: 49482 (49482)
  Destination port: http (80)
  [Stream index: 7]
  Sequence number: 1
                         (relative sequence number)
  Acknowledgement number: 1
                                (relative ack number)
  Header length: 20 bytes
  Flags: 0x10 (ACK)
   0... = Congestion Window Reduced (CWR): Not set
   .0.. .... = ECN-Echo: Not set
   ..0. .... = Urgent: Not set
   ...1 .... = Acknowledgement: Set
  Window size: 65700 (scaled)
 Checksum: 0x03ac [validation disabled][SEQ/ACK analysis]
                                                                                              3
0000 00 10 5a 9f d1 11 00 1c c0 91 d1 5e 08 00 45 00 0010 00 28 13 e6 40 00 80 06 1f e0 c1 cc al dd c1 cc
                                                             ..Z.....^..E.
```

```
File Edit View Go Capture Analyze Statistics Telephony Iools Help
Filter: tcp - Expression... Clear Apply
 130 5.523439 193.204.161.193.204.161.TCP 49482 > http [ACK] Seq=1 Ack=1 Win=
 Frame 131 (838 bytes on wire, 838 bytes captured)
 Transmission Control Protocol, Src Port: 49482 (49482), Dst Port: http (80), Seq: 1
 Hypertext Transfer Protocol
  Expert Info (Chat/Sequence): GET /~impianti/HomePage09-10/index_reti1.html HTTP/

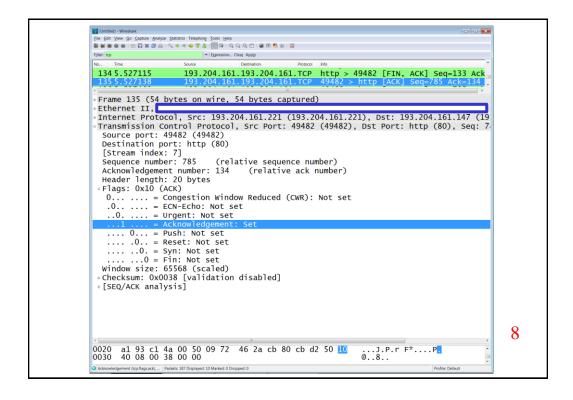
[Message: GET /~impianti/HomePage09-10/index_reti1.html HTTP/1.1\r\n]

[Severity level: Chat]
     [Group: Sequence]
   Request Method: GET
Request URI: /~impianti/HomePage09-10/index_reti1.html
   Request Version: HTTP/1.1
  Host: www.dia.uniroma3.it\r\n
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.0; it; rv:1.9.0.15) Gecko/200910:
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Accept-Language: it-it, it;q=0.8,en-us;q=0.5,en;q=0.3\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
  Cookie: __utma=235113285.403594858.1227188804.1260781913.1260868098.138; __utmz=23
If-Modified-since: Mon, 07 Dec 2009 15:56:41 GMT\r\n
If-None-Match: "1928ed0-643e-80da2040"\r\n
Cache-Control: max-age=0\r\n
  \r\n
                                                                                                                4
       @).}..GE T /~imp
anti/Hom ePage09
0030
```





```
▼ Expression... Clear Apply
 135 5.527138
                          193.204.161.193.204.161.TCP 49482 > http [ACK] Seq=785 Ack=134
 Ethernet II
  Internet Protocol, Src: 193.204.161.147 (193.204.161.147), Dst: 193.204.161.221 (19
  Transmission Control Protocol, Src Port: http (80), Dst Port: 49482 (49482), Seq: 1
  Source port: http (80)
Destination port: 49482 (49482)
[Stream index: 7]
   Sequence number: 133
                                    (relative sequence number)
  Acknowledgement number: 785 (relative ack number)
Header length: 20 bytes
Flags: 0x11 (FIN, ACK)
    0... = Congestion Window Reduced (CWR): Not set
.0. = ECN-Echo: Not set
    .0. ... = Urgent: Not set
...1 ... = Acknowledgement: Set
...0 ... = Push: Not set
...0 ... = Reset: Not set
...0 ... = Reset: Not set
    .... ..0. = Syn: Not set
.... ...1 = Fin: Set
  [Expert Info (Chat/Sequence): Connection finish (FIN)]
window size: 7408 (scaled)
  Checksum: 0x3904 [validation disabled]
0000
0010
                c0 91 d1 5e 00 10 5a 9f d1
2c 4e 40 00 40 06 47 78 c1
```



```
Elle Edit View Go Capture Analyze Statistics Telepl
▼ Expression... Clear Apply
                          193.204.161.193.204.161.TCP 49482 > http [ACK] Seq=785 Ack=134
 Frame 136 (54 bytes on wire, 54 bytes captured) Ethernet II
 Internet Protocol, Src: 193.204.161.221 (193.204.161.221), Dst: 193.204.161.147 (19
 Transmission Control Protocol, Src Port: 49482 (49482), Dst Port: http (80), Seq: 7. Source port: 49482 (49482)
Destination port: http (80)
  [Stream index: 7]
  Sequence number: 785
                                   (relative sequence number)
  Acknowledgement number: 134
Header length: 20 bytes
                                           (relative ack number)
  Flags: 0x11 (FIN, ACK)
   0..... = Congestion Window Reduced (CWR): Not set
.0.... = ECN-Echo: Not set
.0... = Urgent: Not set
.1... = Acknowledgement: Set
    .... 0... = Push: Not set
   .... .0.. = Reset: Not set
.... .0. = Syn: Not set
.... .1 = Fin: Set
   [Expert Info (Chat/Sequence): Connection finish (FIN)]
[Message: Connection finish (FIN)]
[Severity level: Chat]
      [Group: Sequence]
  Window size: 65568 (scaled)
 • Checksum: 0x0037 [validation disabled]
                                                                                                                       9
                                                                             00 10 5a 9f d1 11 00 1c c0 91 d1 5e 08 00 45 00 00 28 13 e9 40 00 80 06 1f dd c1 cc a1 dd c1 cc
0010
```

