

**Luigi SCIOLLA**

Università di Genova

# Network Security

## Analisi del traffico di rete con Wireshark



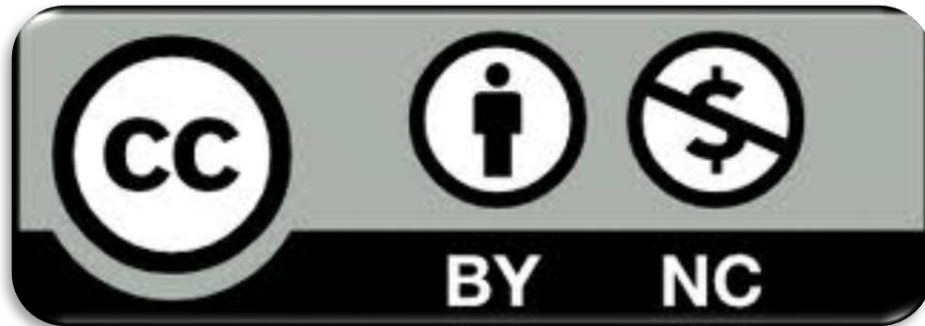
<https://cybersecnatlab.it>

# License & Disclaimer

2

## License Information

This presentation is licensed under the Creative Commons BY-NC License



To view a copy of the license, visit:

<http://creativecommons.org/licenses/by-nc/3.0/legalcode>

## Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

# Obiettivi

3

- Imparare a salvare il traffico di rete
- Essere in grado di analizzare il traffico di rete attraverso Wireshark

# Prerequisiti

4

- Network 1.1 - Fondamenti di reti di calcolatori

# Indice

5

- Salvare il traffico di rete
- Introduzione a Wireshark
- Wireshark: elementi nella GUI
- Wireshark: lavorare con i pacchetti
- Wireshark: seguire gli stream ed estrarre artefatti

# Indice

6

- **Salvare il traffico di rete**
- Introduzione a Wireshark
- Wireshark: elementi nella GUI
- Wireshark: lavorare con i pacchetti
- Wireshark: seguire gli stream ed estrarre artefatti

# Salvare il traffico di rete

7

- Per poter analizzare il traffico di rete passato è necessario prima salvarlo (dump del traffico)
- Tcpcmdump (<https://github.com/the-tcpdump-group/tcpdump>) è un esempio di tool che permette di visualizzare e salvare il traffico di rete
- Generalmente il traffico viene salvato all'interno di file con formato Packet Capture dall'estensione **.pcap**
- Esistono tool e stack più avanzati per il monitoring del traffico (anche in tempo reale) come Packetbeat

# Indice

8

- Salvare il traffico di rete
- **Introduzione a Wireshark**
- Wireshark: elementi nella GUI
- Wireshark: lavorare con i pacchetti
- Wireshark: seguire gli stream ed estrarre artefatti



# Wireshark

9

- Wireshark è un tool che permette di catturare traffico da una rete (sniffer) e analizzarlo
  - L'analisi può essere effettuata real-time oppure usando un file precedentemente salvato
  - I pacchetti sono composti da dati *generic*, essi andranno poi valutati livello per livello per estrapolarne informazioni
- Disponibile sia su Linux che Windows:
  - <https://www.wireshark.org/>

# Challenges di network

10

- Nella maggior parte delle sfide di network security vengono forniti ai giocatori dei file PCAP
- Per risolvere queste challenge i giocatori devono saper analizzare questi file per
  - Trovare la flag direttamente tra i byte
  - Rispondere a delle domande relative al traffico analizzato
- Wireshark è uno strumento utile per risolvere questo tipo di sfide

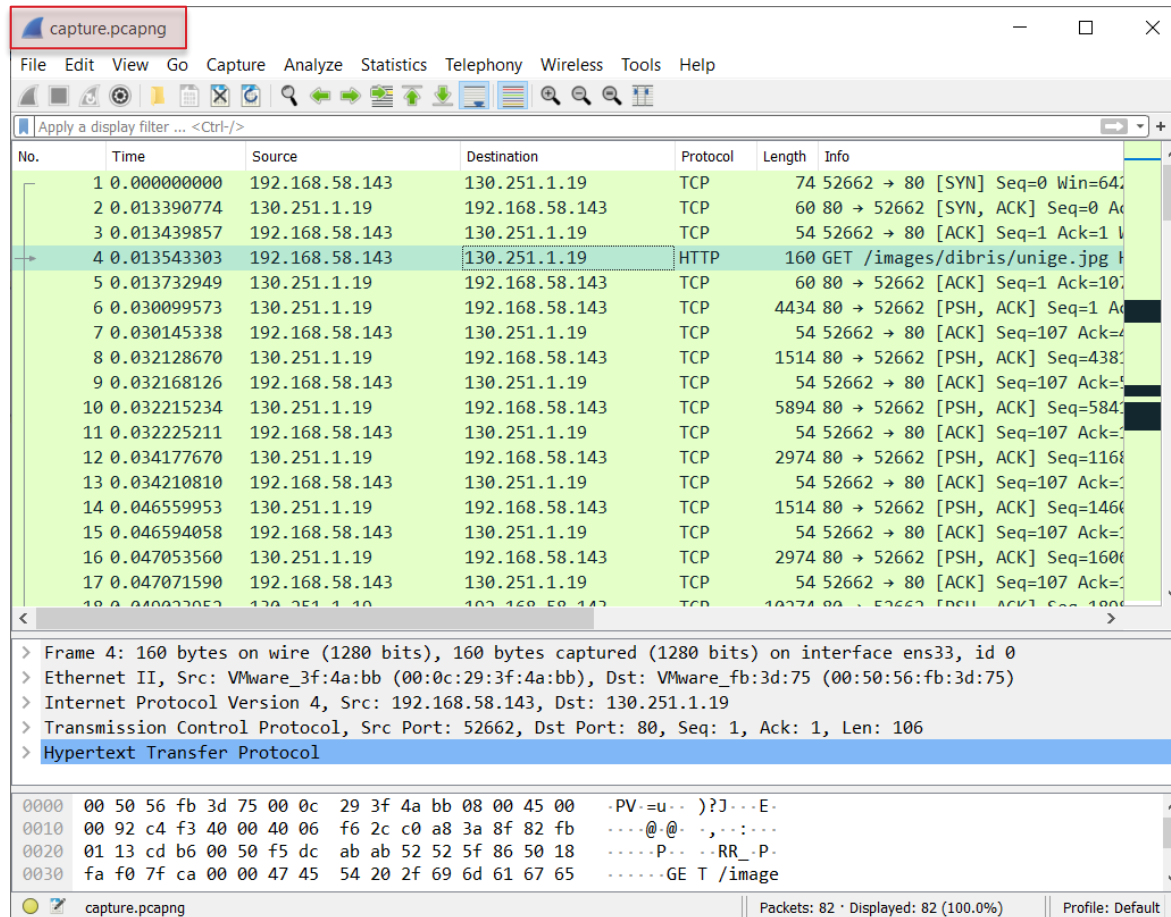
# Indice

11

- Salvare il traffico di rete
- Introduzione a Wireshark
- **Wireshark: elementi nella GUI**
- Wireshark: lavorare con i pacchetti
- Wireshark: seguire gli stream ed estrarre artefatti

# Wireshark GUI

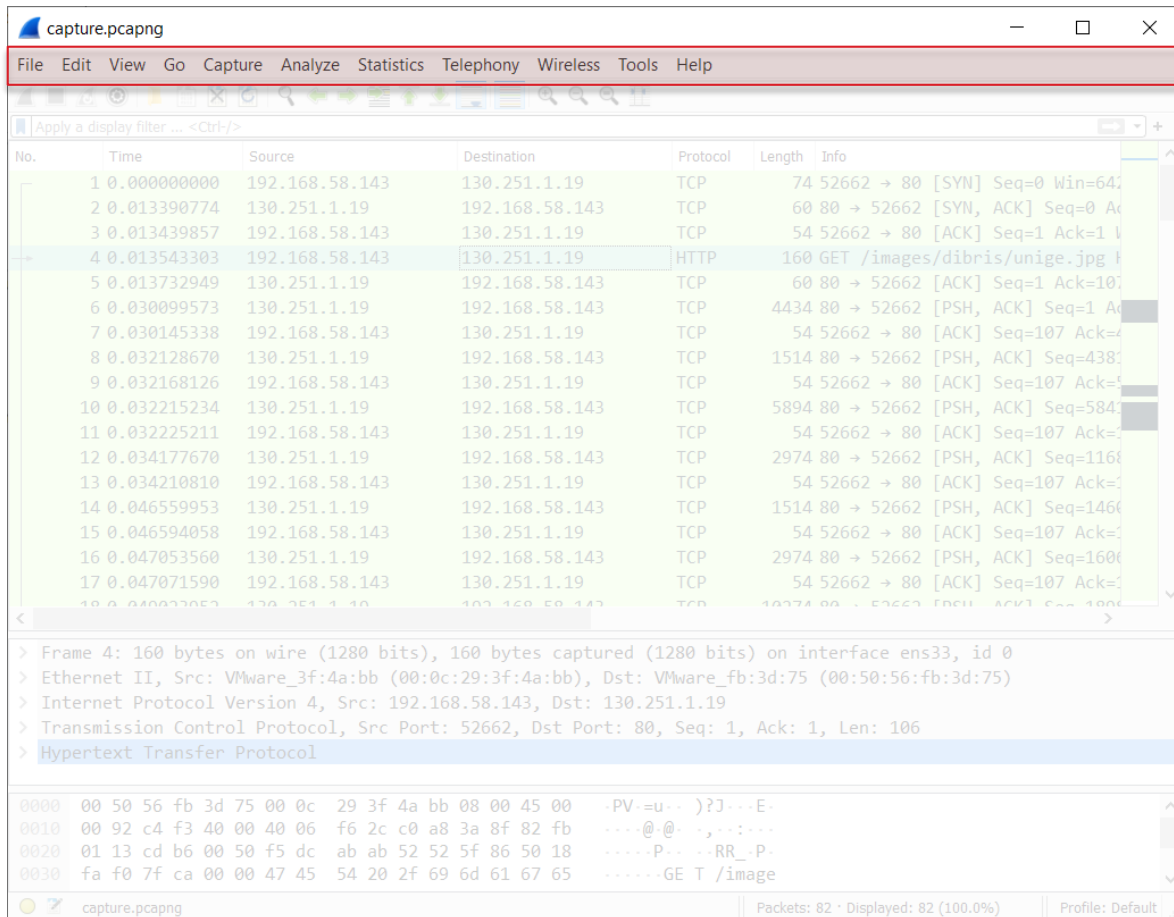
12



- Wireshark ha una interfaccia grafica (Graphical User Interface GUI)
- È possibile aprire un file .pcap da analizzare dal menu *File* oppure utilizzando il comando open (CTRL+o)  
Esso apparirà nella schermata principale
- Utilizzando una versione di Wireshark in inglese è più facile cercare aiuto e informazioni su Internet

# Wireshark GUI: menu

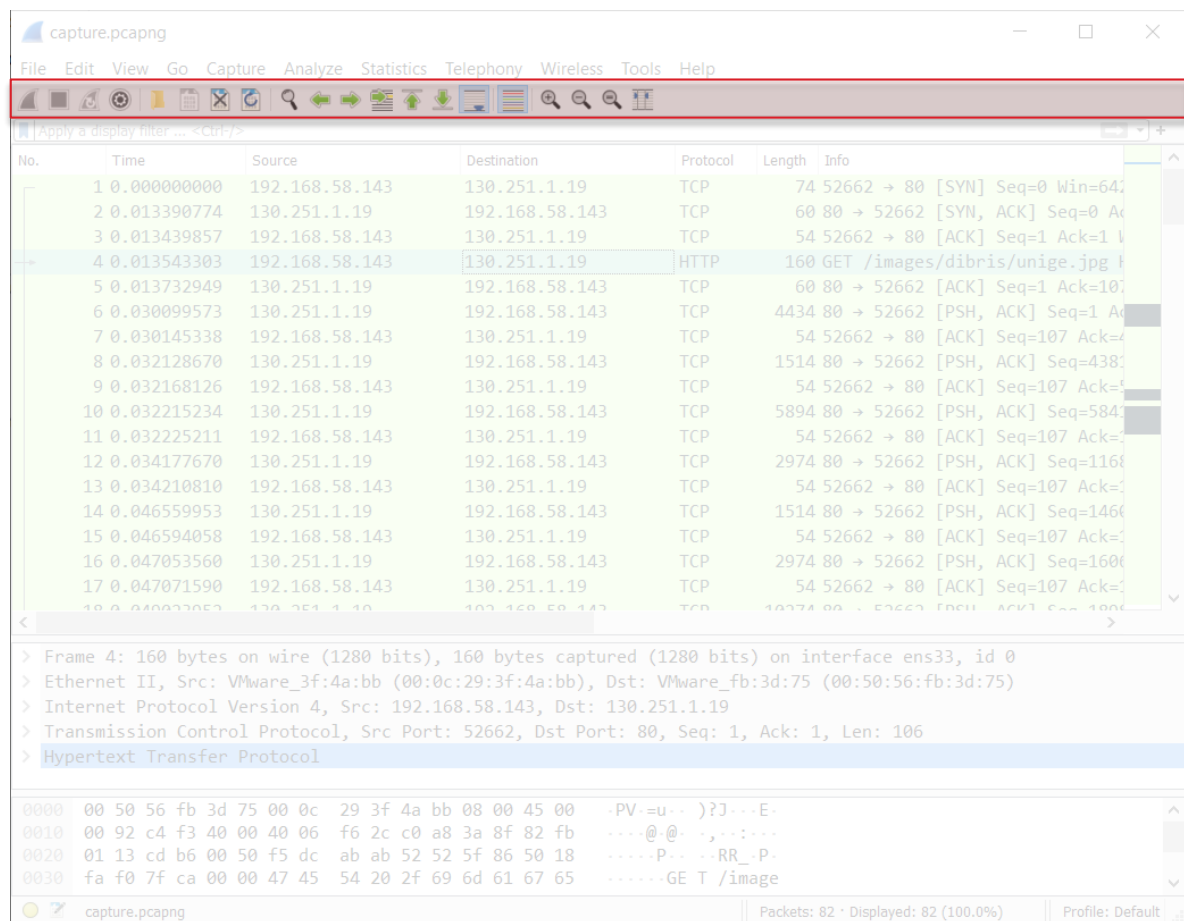
13



- Il **menu** è utilizzato per effettuare azioni
- Le azioni di maggiore interesse sono:
  - **File**: aprire o raggruppare file, salvare, stampare o esportare dati
  - **Edit**: trovare un pacchetto, evidenziare flussi, gestire le configurazioni
  - **View**: controllare come vengono visualizzati i pacchetti (colore, font ...)
  - **Go**: andare ad un determinato pacchetto
  - **Analyze**: manipolare, filtrare, attivare o disattivare il focus su determinati protocolli, seguire i flussi (stream)
  - **Statistics**: visualizzare diverse statistiche quali gli indirizzi IP coinvolti nella comunicazione, numero di pacchetti scambiati etc. Utili per farsi un'idea iniziale sul tipo di traffico contenuto in quel file aperto

# Wireshark GUI: toolbar principale

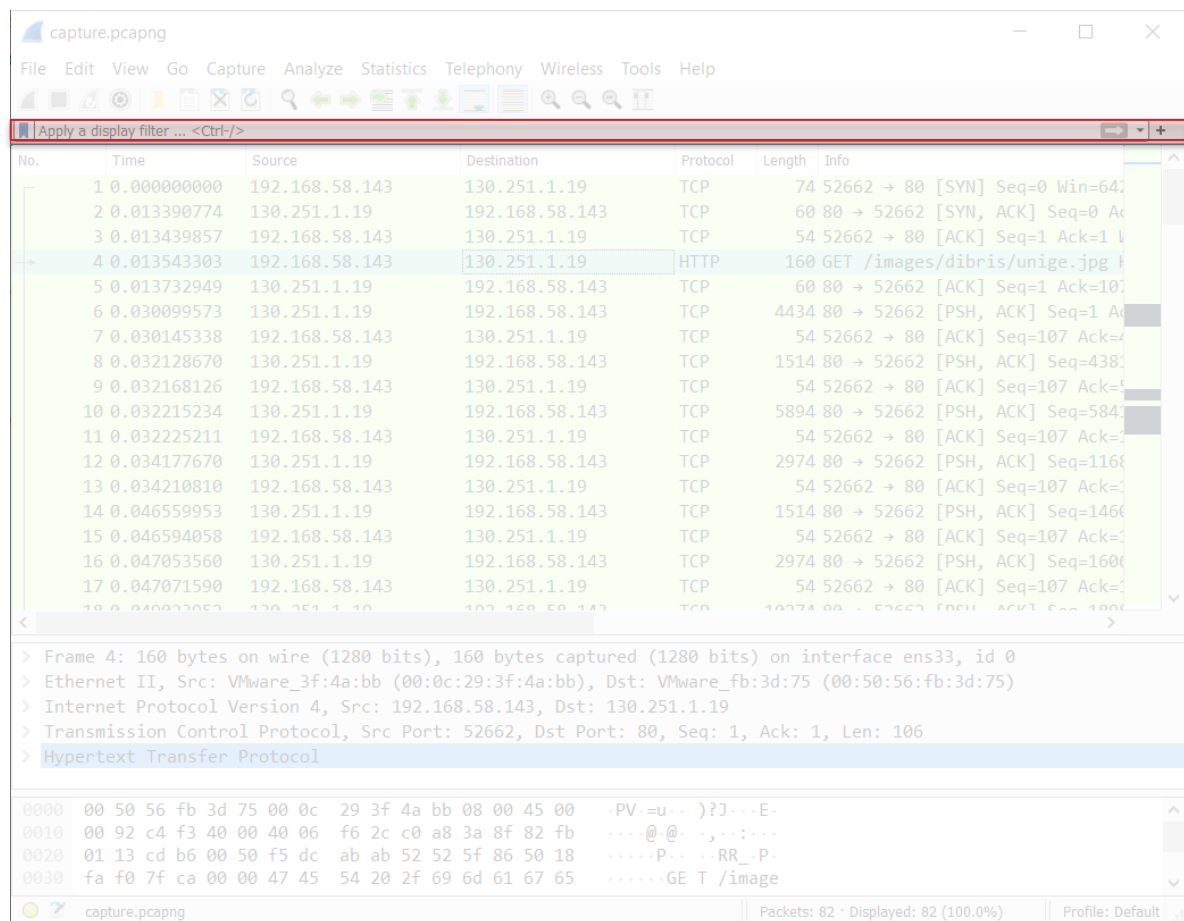
14








- La toolbar principale (main toolbar) permette l'accesso rapido agli elementi del menu più utilizzati
- Gli elementi nella toolbar si possono attivare o disattivare come i corrispondenti elementi del menu

# Wireshark GUI: filter toolbar

15



- Il menu dei filtri permette di modificare e applicare rapidamente dei filtri sui pacchetti
- Gestire o salvare filtri salvati 
- Reset dei filtri 
- Applicare il filtro corrente 
- Selezionare un filtro da una lista di filtri usati di recente 
- Aggiungere un nuovo filter button (shortcut per applicare un determinato filtro) 

# Wireshark GUI: lista dei pacchetti

16

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.58.143	130.251.1.19	TCP	74	52662 → 80 [SYN] Seq=0 Win=64
2	0.013390774	130.251.1.19	192.168.58.143	TCP	60	80 → 52662 [SYN, ACK] Seq=0 Ac
3	0.013439857	192.168.58.143	130.251.1.19	TCP	54	52662 → 80 [ACK] Seq=1 Ack=1
4	0.013543303	192.168.58.143	130.251.1.19	HTTP	160	GET /images/dibris/unige.jpg
5	0.013732949	130.251.1.19	192.168.58.143	TCP	60	80 → 52662 [ACK] Seq=1 Ack=10
6	0.030099573	130.251.1.19	192.168.58.143	TCP	4434	80 → 52662 [PSH, ACK] Seq=1 Ac
7	0.030145338	192.168.58.143	130.251.1.19	TCP	54	52662 → 80 [ACK] Seq=107 Ack=
8	0.032128670	130.251.1.19	192.168.58.143	TCP	1514	80 → 52662 [PSH, ACK] Seq=438
9	0.032168126	192.168.58.143	130.251.1.19	TCP	54	52662 → 80 [ACK] Seq=107 Ack=
10	0.032215234	130.251.1.19	192.168.58.143	TCP	5894	80 → 52662 [PSH, ACK] Seq=584
11	0.032225211	192.168.58.143	130.251.1.19	TCP	54	52662 → 80 [ACK] Seq=107 Ack=
12	0.034177670	130.251.1.19	192.168.58.143	TCP	2974	80 → 52662 [PSH, ACK] Seq=116
13	0.034210810	192.168.58.143	130.251.1.19	TCP	54	52662 → 80 [ACK] Seq=107 Ack=
14	0.046559953	130.251.1.19	192.168.58.143	TCP	1514	80 → 52662 [PSH, ACK] Seq=146
15	0.046594058	192.168.58.143	130.251.1.19	TCP	54	52662 → 80 [ACK] Seq=107 Ack=
16	0.047053560	130.251.1.19	192.168.58.143	TCP	2974	80 → 52662 [PSH, ACK] Seq=160
17	0.047071590	192.168.58.143	130.251.1.19	TCP	54	52662 → 80 [ACK] Seq=107 Ack=

- Il pannello centrale mostra la lista di tutti i pacchetti catturati
- Ogni linea corrisponde a un pacchetto catturato
- Selezionando un pacchetto (singolo click) vengono visualizzati i dettagli del pacchetto all'interno della sottostante sezione *packet details* e *packet bytes*
- Si può cliccare sulle colonne per ordinare i pacchetti



# Wireshark GUI: packet details

17

The screenshot shows the Wireshark interface with a packet list table and a detailed view of a selected packet. The packet list table has the following columns: No., Time, Source, Destination, Protocol, Length, and Info. The selected packet (No. 4) is an HTTP GET request for /images/dibris/unige.jpg. The details pane below shows the following structure:

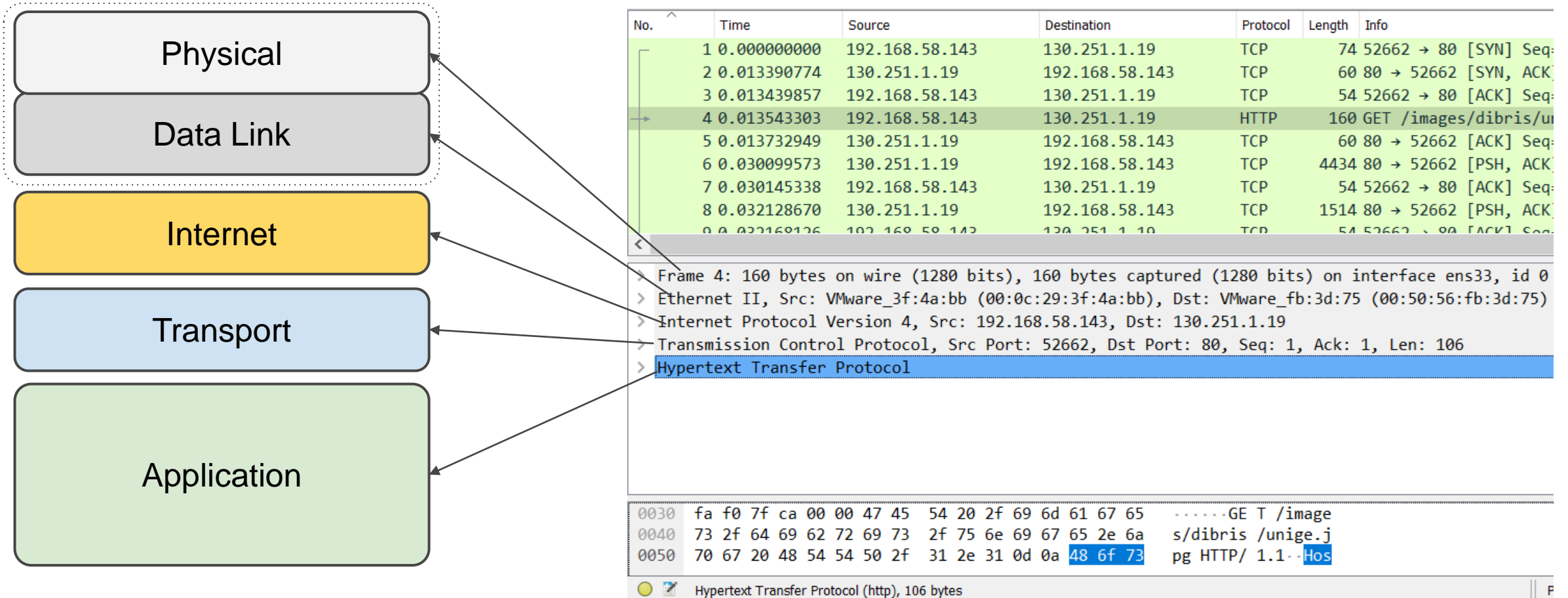
- > Frame 4: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface ens33, id 0
- > Ethernet II, Src: VMware\_3f:4a:bb (00:0c:29:3f:4a:bb), Dst: VMware\_fb:3d:75 (00:50:56:fb:3d:75)
- > Internet Protocol Version 4, Src: 192.168.58.143, Dst: 130.251.1.19
- > Transmission Control Protocol, Src Port: 52662, Dst Port: 80, Seq: 1, Ack: 1, Len: 106
- > Hypertext Transfer Protocol

The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII format, starting with 0000 00 50 56 fb 3d 75 00 0c 29 3f 4a bb 08 00 45 00 -PV=u...)?J...E-.

- Il pannello sottostante alla lista dei pacchetti mostra i dettagli del pacchetto selezionato
- In particolare mostra i protocolli e i campi del pacchetto con una struttura ad albero. Ciascun ramo corrisponde ad un protocollo e può essere espanso per visualizzare i corrispondenti dati contenuti all'interno

# Wireshark GUI: packet details

18



# Wireshark GUI: packet bytes

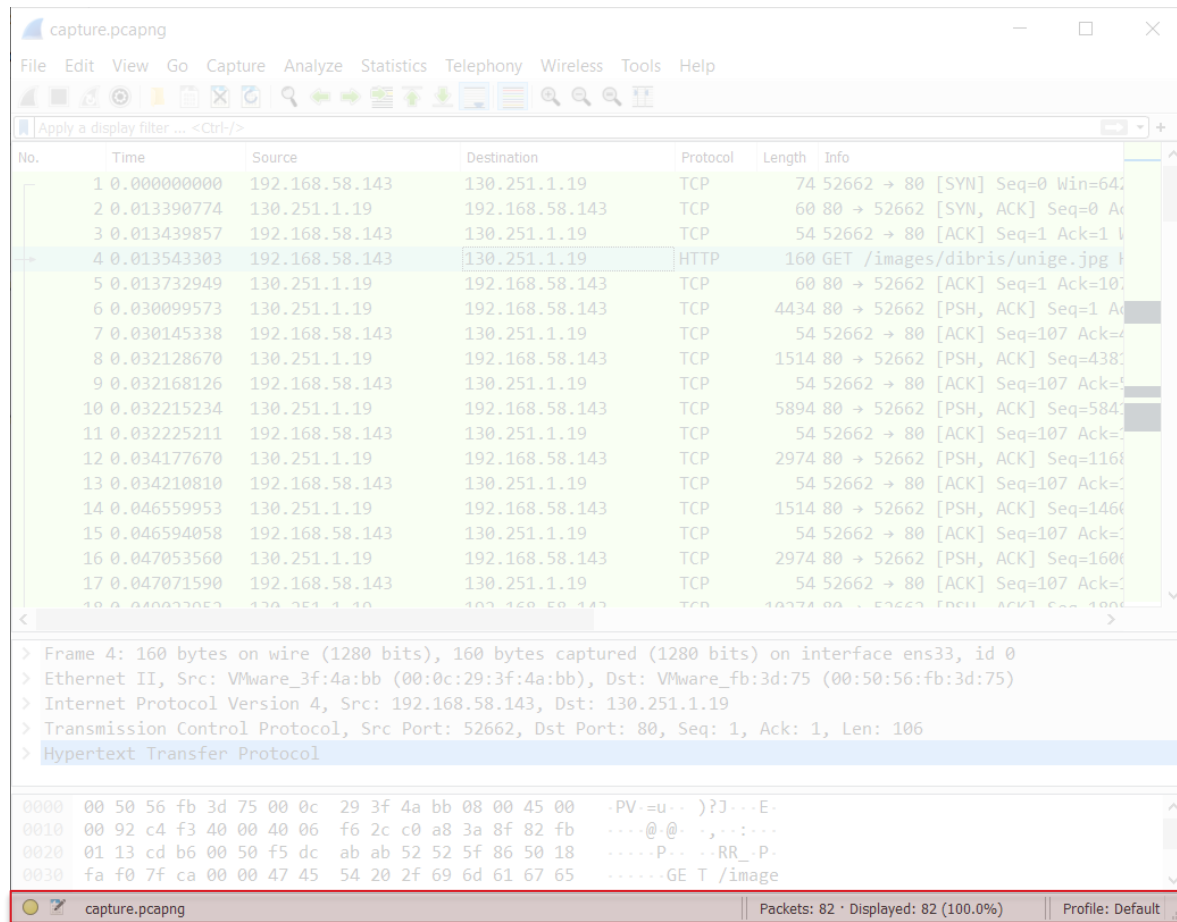
19

The screenshot shows the Wireshark interface with a packet capture named 'capture.pcapng'. The packet list pane shows several packets, with packet 4 selected. The packet details pane shows the structure of the selected packet: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet bytes pane shows the hex dump of the selected packet, with the first 16 bytes highlighted in red. The hex dump shows the following bytes: 0000 00 50 56 fb 3d 75 00 0c 29 3f 4a bb 08 00 45 00 .PV.=u.. )?J...E-  
0010 00 92 c4 f3 40 00 40 06 f6 2c c0 a8 3a 8f 82 fb ....@.@. ,...:..  
0020 01 13 cd b6 00 50 f5 dc ab ab 52 52 5f 86 50 18 .....P... ..RR\_ P  
0030 fa f0 7f ca 00 00 47 45 54 20 2f 69 6d 61 67 65 .....GE T /image



- Il pannello contenente i *packet bytes* mostra i dati del pacchetto selezionato in stile *hexdump*
- Ciascuna linea contiene:
  - L'offset dei dati
  - 16 byte rappresentati in base esadecimale
  - 16 caratteri ASCII (i caratteri non stampabili vengono rappresentati con un punto ".")

# Wireshark GUI: statusbar

20



➤ La *statusbar* mostra messaggi informativi:

- Il cerchio colorato apre le informazioni per esperti, esse contengono una lista di anomalie e altri elementi interessanti trovati nel file. 
- L'icona di modifica ti permette di aggiungere commenti al file 
- A sinistra viene visualizzato il nome del file
- Al centro viene visualizzato il numero del pacchetto selezionato
- Sulla destra viene visualizzato il profilo attivo

# Indice

21

- Salvare il traffico di rete
- Introduzione a Wireshark
- Wireshark: elementi nella GUI
- **Wireshark: lavorare con i pacchetti**
- Wireshark: seguire gli stream ed estrarre artefatti

# La lista dei pacchetti

22

Pacchetti collegati

No.	Time	Source	Destination	Protocol	Length	Info	colonne
1	0.000000000	192.168.58.143	130.251.1.19	TCP	74	52662 → 80 [SYN] Seq=0 Win=64240 Len=0	
2	0.013390774	130.251.1.19	192.168.58.143	TCP	60	80 → 52662 [SYN, ACK] Seq=0 Ack=1 Win=6	
3	0.013439857	192.168.58.143	130.251.1.19	TCP	54	52662 → 80 [ACK] Seq=1 Ack=1 Win=64240	
4	0.013543303	192.168.58.143	130.251.1.19	HTTP	160	GET /images/dibris/unige.jpg HTTP/1.1	
5	0.013732949	130.251.1.19	192.168.58.143	TCP	60	80 → 52662 [ACK] Seq=1 Ack=107 Win=6424	Pacchetto selezionato
6	0.030099573	130.251.1.19	192.168.58.143	TCP	4434	80 → 52662 [PSH, ACK] Seq=1 Ack=107 Win	

1. **No.** Numero del pacchetto all'interno del file. Anche se vengono applicati dei filtri questo numero non cambia.
2. **Time** Timestamp del pacchetto (per cambiare formato andare su View → Time display format)
3. **Source** Indirizzo IP del mittente
4. **Destination** Indirizzo IP del destinatario
5. **Protocol** Nome del protocollo
6. **Length** Lunghezza del pacchetto
7. **Info** Informazioni riguardo il contenuto del pacchetto

# Aggiungere colonne (esempio)

23

Window: 64240  
[Calculated window size: 64240]  
[Window size scaling factor: -2 (no window scaling used)]  
Checksum: 0x7fca [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
> [SEQ/ACK analysis]  
> [Timestamps]  
TCP payload (106 bytes)

▼ Hypertext Transfer Protocol  
▼ GET /images/dibris/unige.jpg HTTP/1.1\r\n  
> [Expert Info (Chat/Sequence): GET /images/dibris/unige.jpg HTTP/1.1\r\n  
Request Method: GET  
Request URI: /images/dibris/unige.jpg

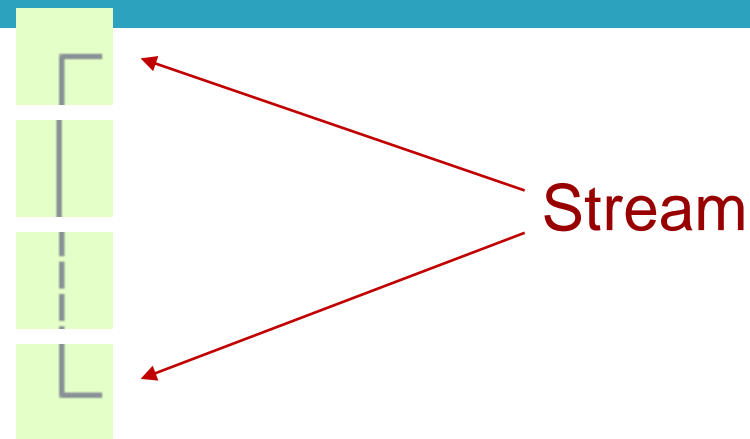
Click tasto destro →  
Apply as Column.  
(CTRL-Shift-I)

- Aggiungere una nuova Colonna che mostra l'URI del pacchetto HTTP
  - Selezionare un pacchetto HTTP
  - Espandere il protocollo HTTP nella sezione packet details
  - Click con il tasto destro sul campo Request URI e cliccare su Apply as Column

# Simboli per pacchetti collegati (stesso flusso/stream)

24

- Primo pacchetto del flusso
- Parte del flusso selezionato
- **Non** parte del flusso selezionato
- Ultimo pacchetto del flusso
- Richiesta
- Risposta
- Il pacchetto selezionato è una conferma di ricezione di questo pacchetto
- Il pacchetto selezionato è un duplicato di conferma di ricezione di questo pacchetto
- Il pacchetto selezionato ha a che fare con questo pacchetto (as esempio parte del contenuto)

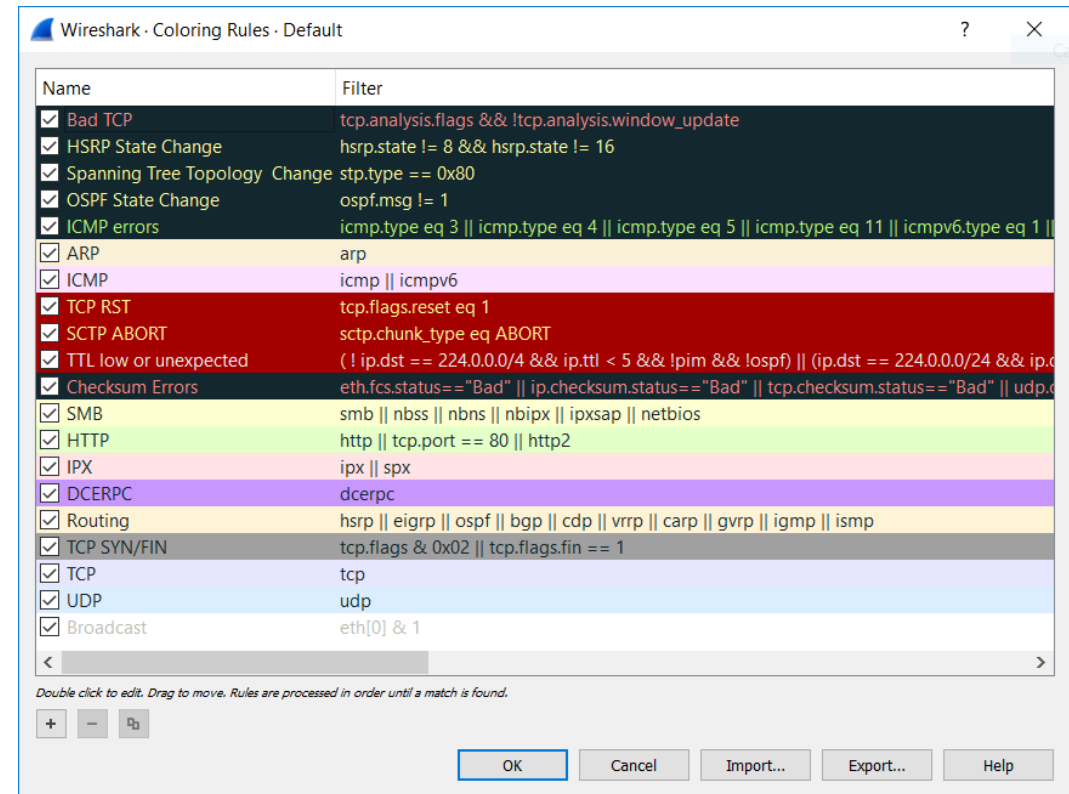




# Evidenziare pacchetti con colori

25

- Wireshark permette di evidenziare i pacchetti con colori diversi basandosi su regole (ad esempio protocolli diversi colori diversi)
- Per visualizzare la configurazione o modificarla
  - View → Coloring Rules...



# Filtri

26

- Wireshark fornisce un linguaggio per gestire i filtri
- Con i filtri è possibile controllare quali pacchetti andare a visualizzare
- I filtri possono essere utilizzati per:
  - Visualizzare solo pacchetti di un determinato protocollo
  - Cercare pacchetti con un campo con un determinato valore
  - [...]
- I filtri possono essere combinati formando espressioni complesse, utilizzando operatori logici e parentesi

# Creare un filtro

27

1. Help → Manual Pages → Wireshark Filters
2. Expression builder: click con il tasto destroy sulla toolbar → Display Filter Expression...
3. Selezionare il campo sul pannello *packet details*:
  1. Apply as filter: filtra la lista dei pacchetti con solo quelli che soddisfano l'espressione
  2. Prepare as filter: scrive l'espressione ma essa non viene ancora applicata alla lista dei pacchetti

The screenshot shows the Wireshark interface. On the left, the 'packet details' pane is open, showing the 'Transmission Control Protocol' section. The 'Source Address' field is highlighted with a red box and labeled 'Campo protocollo'. A red arrow points from this field to the 'Display Filter Expression' field on the right, which is labeled 'Prepare a Filter'. The filter expression 'ip.src == 145.254.160.237' is entered in the filter field. Below the filter field, a table with columns 'No.', 'Time', and 'Source' is visible. The 'Source Address' field in the packet details pane is also highlighted with a red box and labeled 'Filter field'.

# Indice

28

- Salvare il traffico di rete
- Introduzione a Wireshark
- Wireshark: elementi nella GUI
- Wireshark: lavorare con i pacchetti
- **Wireshark: seguire gli stream ed estrarre artefatti**

# Seguire stream

29

- **Seguire uno stream** mostra una diversa visualizzazione del traffico di rete: anziché visualizzare un pacchetto singolo, vengono visualizzati i dati trasmessi tra mittente e destinatario
- Quando viene visualizzato uno stream, un filtro relativo allo stream corrente viene applicato. Solo i pacchetti di quello stream verranno visualizzati

7	9.025432	72.163.7.54	192.168.1.135	ETD	07	Response	220-\tCisco System
8	9.025433	72.163.7.54	192.168.1.135				220-
9	9.025434	72.163.7.54	192.168.1.135				220- \t\t\t\t\t\t
10	9.025434	72.163.7.54	192.168.1.135				220-\tPhone: +1.8
11	9.025435	72.163.7.54	192.168.1.135				220-
12	9.025435	72.163.7.54	192.168.1.135				220- Local time
13	9.025435	72.163.7.54	192.168.1.135				220-
14	9.025532	192.168.1.135	72.163.7.54				[ACK] Seq=1 Ack=
15	9.025860	72.163.7.54	192.168.1.135				220-\tThis system
16	9.037860	72.163.7.54	192.168.1.135				220-\t- FILES.CI
17	9.037862	72.163.7.54	192.168.1.135				220-
18	9.037863	72.163.7.54	192.168.1.135				220-\tPlease read
19	9.037864	72.163.7.54	192.168.1.135				220-\tWARNING! -
20	9.037864	72.163.7.54	192.168.1.135				220-\t+PASSWORD AR
21	9.037865	72.163.7.54	192.168.1.135				
22	9.037866	72.163.7.54	192.168.1.135				

Frame 7: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface 0  
Ethernet II, Src: Amtec 32:a1:59:00:60:3b, 32:a1:59:00:60:3b, Dst: 08:00:27:00:00:00

- Mark/Unmark Packet Ctrl+M
- Ignore/Unignore Packet Ctrl+D
- Set/Unset Time Reference Ctrl+T
- Time Shift... Ctrl+Shift+T
- Packet Comment... Ctrl+Alt+C
- Edit Resolved Name
- Apply as Filter
- Prepare a Filter
- Conversation Filter
- Colorize Conversation
- SCTP
- Follow**
  - TCP Stream
  - UDP Stream
  - SSL Stream
  - HTTP Stream
- Copy
- Protocol Preferences
- Decode As...

# Seguire uno stream (esempio)

30

- Telnet è un protocollo di tipo client-server che può essere utilizzato per aprire la linea di comando su un host remoto
- In **blu** vengono visualizzati i dati dal server al client (ad esempio il prompt di login)
- In **rosso** vengono visualizzati i dati dal client al server (ad esempio il client che invia la password al server)
- I caratteri non stampabili vengono rappresentati con il punto “.”

```
.....!..".'.#...%.....!..".'.....P.....".....b.....b..... B.
.....".'.#...&..$..&..$.....#.....'.9600,9600....#.bam.zing.org:
0.0....'.DISPLAY.bam.zing.org:0.0.....xterm-color.....".....
OpenBSD/i386 (oof) (tty1)

login: .."....."ffaakkee
.
Password:user
.
Last login: Thu Dec  2 21:32:59 on tty1 from bam.zing.org
Warning: no Kerberos tickets issued.
OpenBSD 2.6-beta (OOF) #4: Tue Oct 12 20:42:32 CDT 1999

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code.  With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.

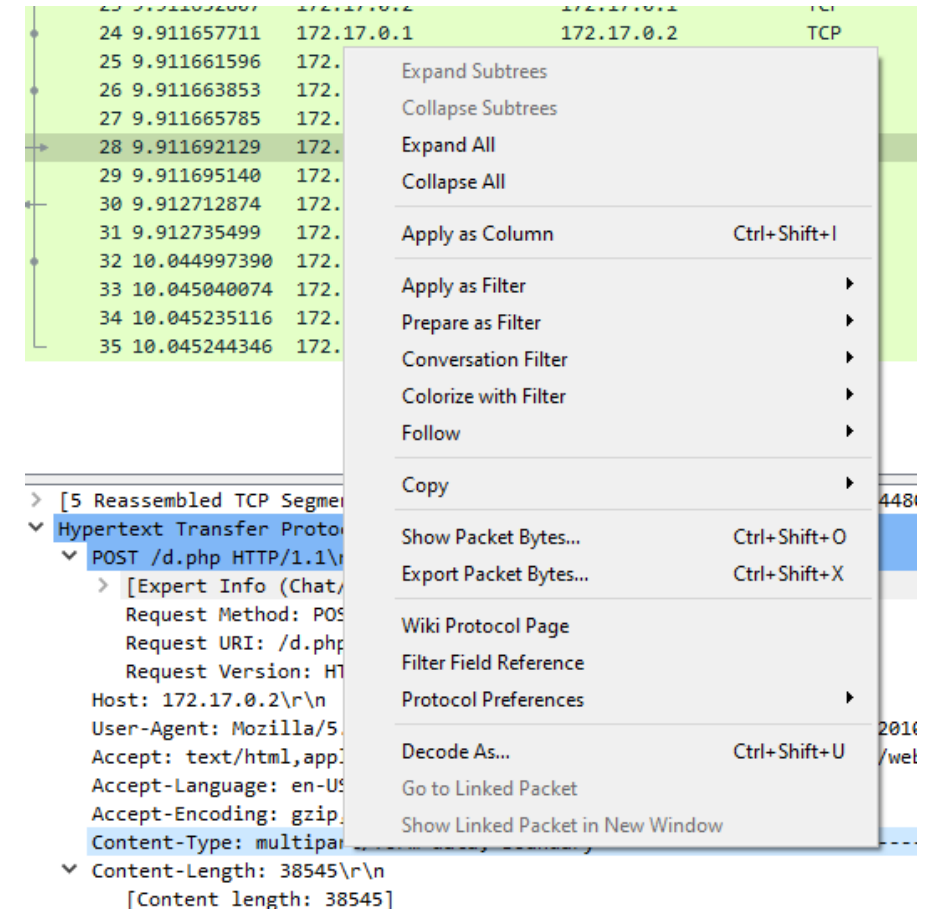
$ llss
.
$ llss --aa
.
.  ..  .cshrc  .login  .mailrc  .profile  .rhosts
$ //ssbbiinn//ppiinnngg  wwwwww..yyaahhooool..ccoomm
.
PING www.yahoo.com (204.71.200.74): 56 data bytes
64 bytes from 204.71.200.74: icmp_seq=0 ttl=239 time=73.569 ms
64 bytes from 204.71.200.74: icmp_seq=1 ttl=239 time=71.099 ms
64 bytes from 204.71.200.74: icmp_seq=2 ttl=239 time=68.728 ms
64 bytes from 204.71.200.74: icmp_seq=3 ttl=239 time=73.122 ms
64 bytes from 204.71.200.74: icmp_seq=4 ttl=239 time=71.276 ms
64 bytes from 204.71.200.74: icmp_seq=5 ttl=239 time=75.831 ms
64 bytes from 204.71.200.74: icmp_seq=6 ttl=239 time=70.101 ms
64 bytes from 204.71.200.74: icmp_seq=7 ttl=239 time=74.528 ms
64 bytes from 204.71.200.74: icmp_seq=8 ttl=239 time=74.514 ms
64 bytes from 204.71.200.74: icmp_seq=9 ttl=239 time=75.188 ms
64 bytes from 204.71.200.74: icmp_seq=10 ttl=239 time=72.925 ms
64 bytes from 204.71.200.74: icmp_seq=11 ttl=239 time=72.925 ms
...^C
---- www.yahoo.com ping statistics ----
13 packets transmitted, 11 packets received, 15% packet loss
round-trip min/avg/max = 68.728/72.807/75.831 ms
$ eexxiitt
.
```

# Estrarre artefatti dagli stream: esempio

31

## ➤ Estrarre e salvare un file JPEG scaricato usando HTTP

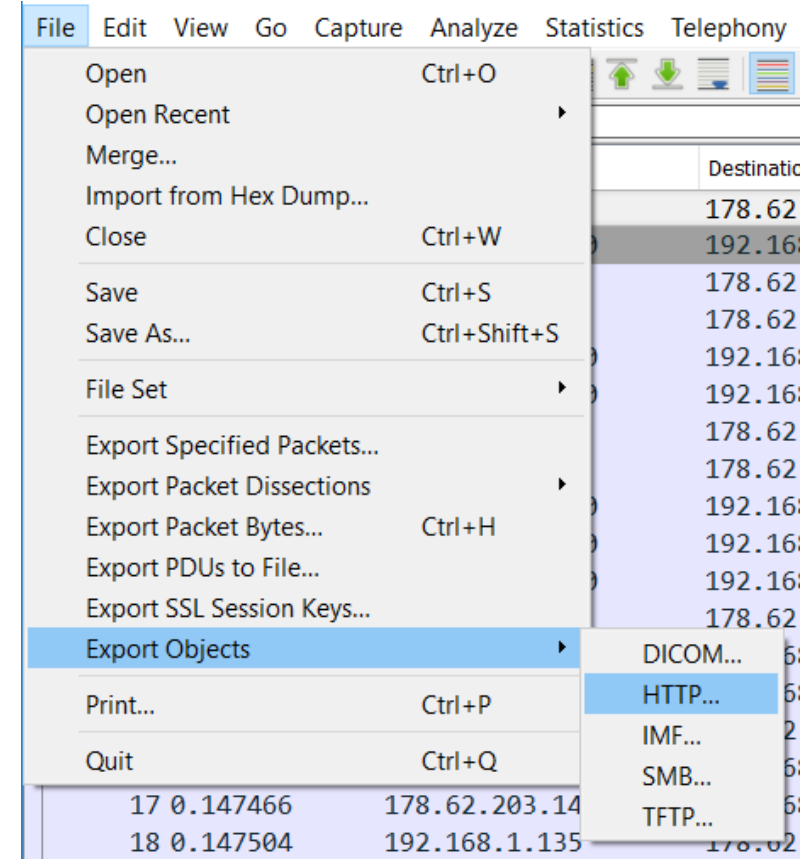
1. Selezionare il pacchetto
2. Andare sul packet bytes del pacchetto
3. Cliccare con il tasto destro sul campo contenente l'artefatto
4. Cliccare su *Export packet Bytes*
5. Salvare il file



# Estrarre artefatti: esempio 2

32

- File → Export Objects
- Questa feature analizza gli stream di alcuni protocolli e ricostruisce alcuni oggetti come le pagine HTML, immagini etc...
- Questi file possono essere esportati e salvati su disco





# Network Security

## Analisi del traffico di rete con Wireshark

**Luigi SCIOLLA**

Università di Genova



<https://cybersecnatlab.it>