Informatica forense

Qualche esempio di attività di analisi:

disk forensics e network forensics

Michele Ferrazzano

Le 5 fasi

- Identificazione
- Acquisizione
- Analisi
- Valutazione
- Presentazione

Identificazione

- Rilevare/scovare cosa è effettivamente utile per l'indagine
  - Sistemi informatici
  - Sistemi di comunicazione
  - Supporti di memorizzazione esterna
  - Supporti non digitali e informazioni
    - Documenti, post-it…
    - Password, modalità di accesso a sistemi complessi…

Acquisizione

- Duplicare le informazioni in maniera fedele all'originale
  - Cloni
  - Immagini bit-a-bit
    - Es: DD
  - Immagini bit-a-bit compresse
    - Es: EWF (Expert Witness Format)
- Obiettivi
  - Acquisire il maggior numero di dati (possibilmente tutti)
  - Rendere l'attività di acquisizione ripetibile
  - Limitare i tempi di inattività di server "importanti"

Analisi

- Mettere in evidenza i dati con contenuto informativo importante per l'indagine
  - A favore
  - A sfavore
- Documentare il processo di analisi

Analisi

- Principali funzioni svolte durante l'analisi
  - Visualizzazione dei dati
  - Ricerca per parola chiave
  - Decompressione di archivi
  - Carving
  - Decifratura
  - Calcolo della timeline

Valutazione

- Interpretare i dati evidenziati in fase di analisi per sostenere le proprie tesi
  - A favore
  - A sfavore

Presentazione

- Documentare
  - Cosa è stato fatto
  - Come è stato fatto
  - Cosa è emerso
  - Che significato hanno i dati emersi
- Adattare il registro all'interlocutore
  - Tecnico
  - Giurista

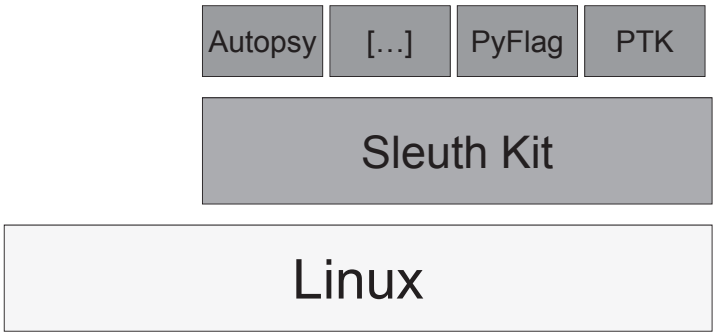
Analisi forense con Autopsy

Autopsy e Sleuth Kit

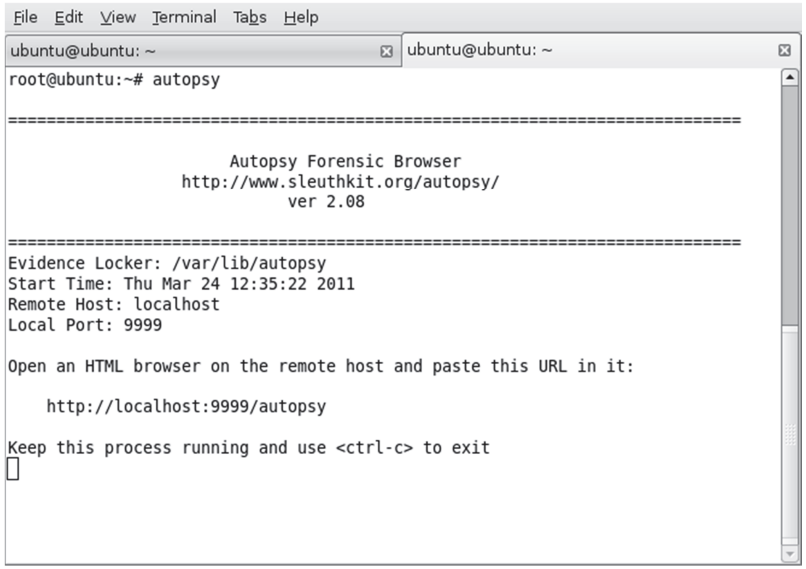
- Lo **Sleuth Kit** è una collezione di programmi a linea di comando che consente di realizzare analisi forense di dischi e file system. Il tool può essere incorporato in un gran numero di sistemi per analisi forense che possono utilizzare tali comandi per accedere direttamente ai dati.
- **Autopsy Forensic Browser** è un'interfaccia grafica verso i comandi dello Sleut Kit. Assieme consentono di condurre un'analisi forense di dischi e di file system di computer.

http://www.sleuthkit.org

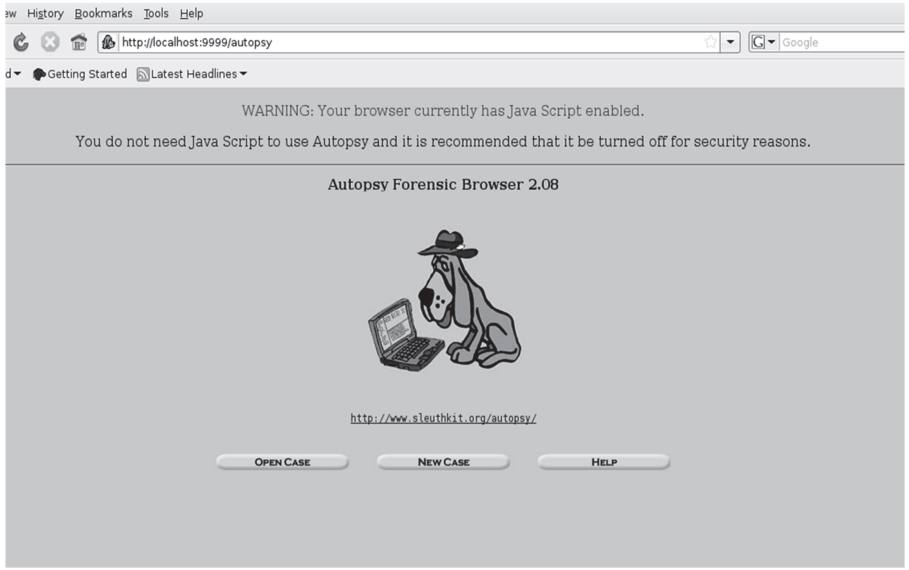
Autopsy e Sleuth Kit (architettura)



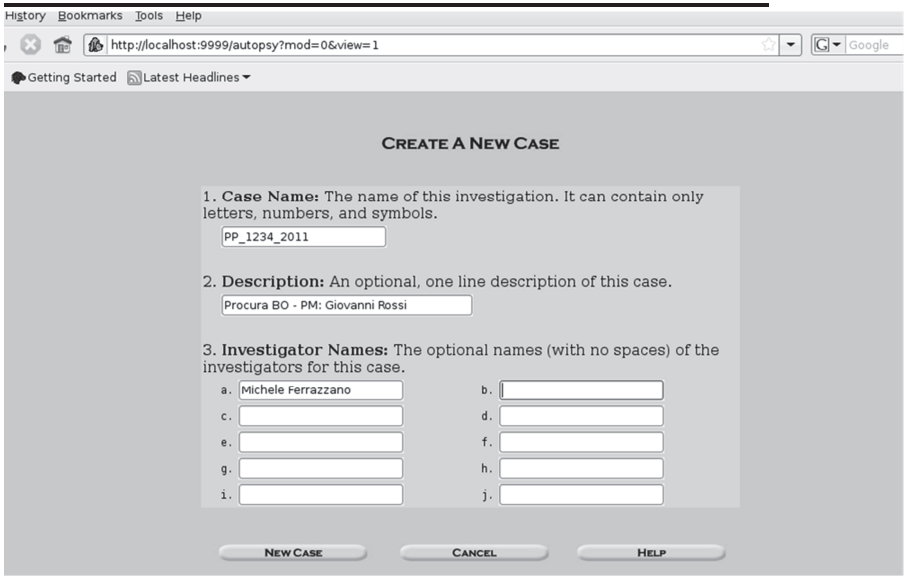
Avvio di Autopsy



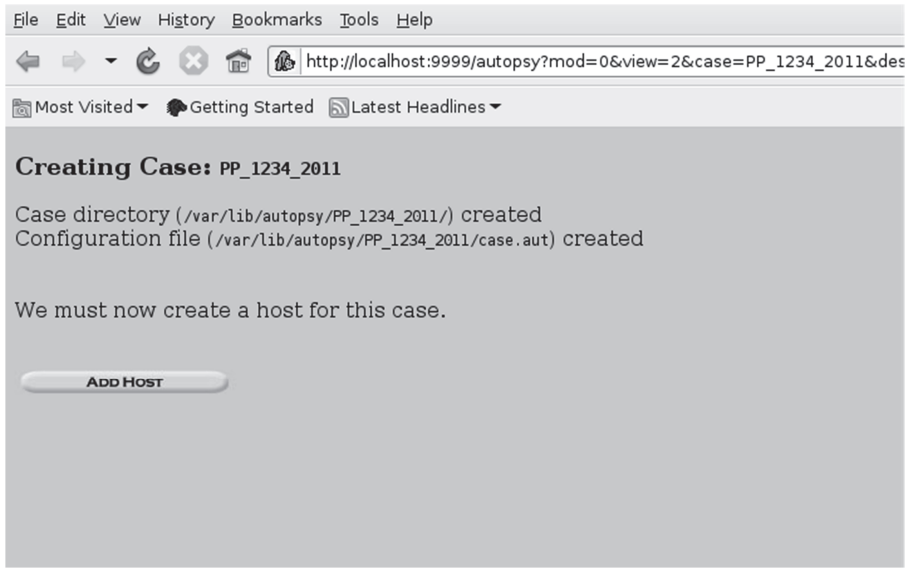
Avvio di Autopsy



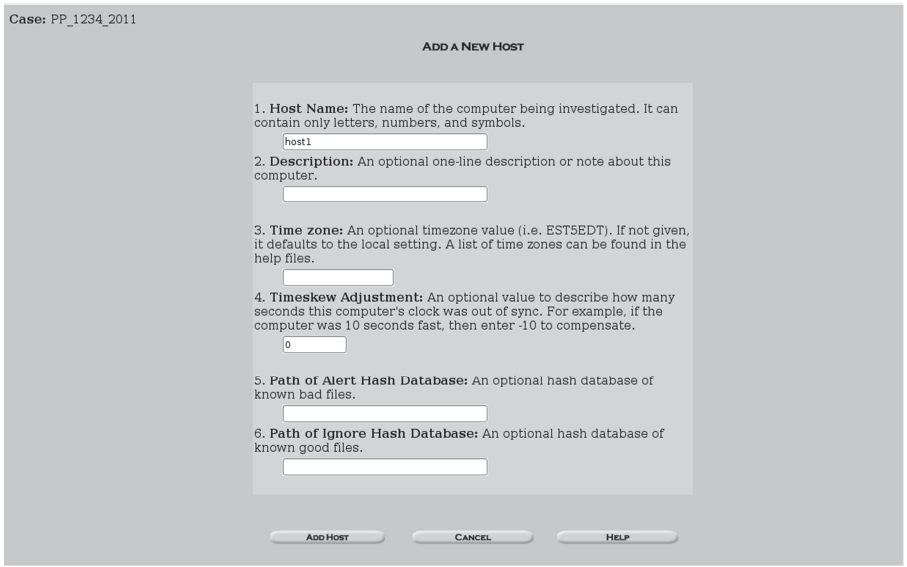
Autopsy – Creazione di un nuovo caso



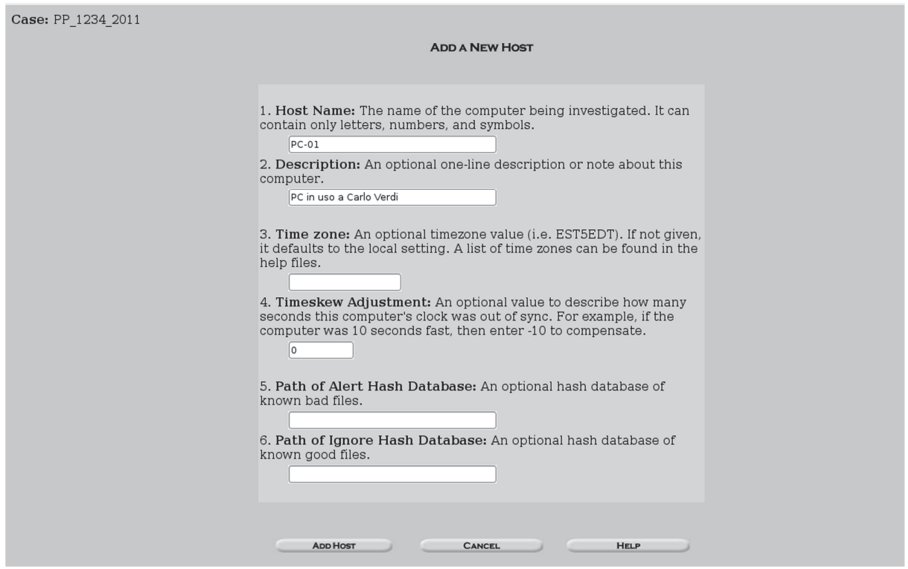
Autopsy – Creazione di un nuovo caso



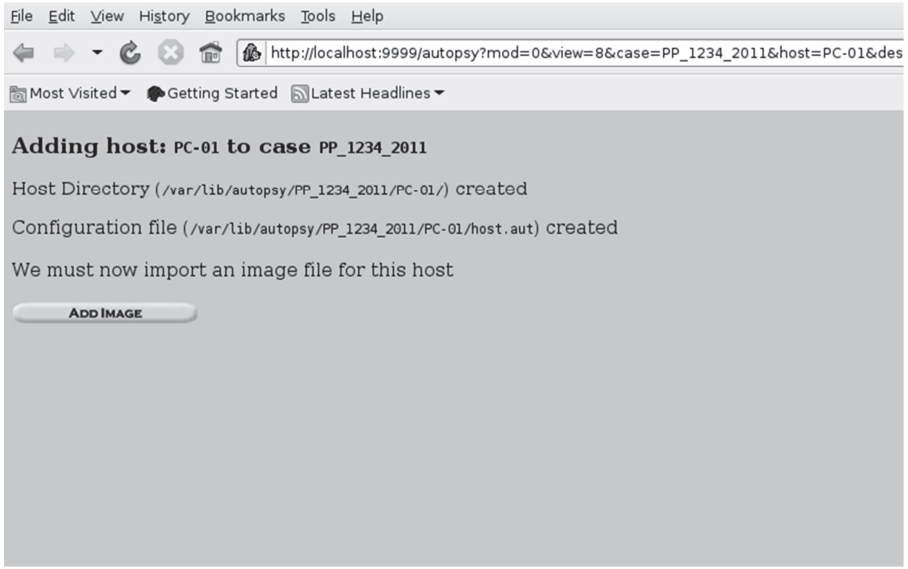
Autopsy – Aggiunta di un host



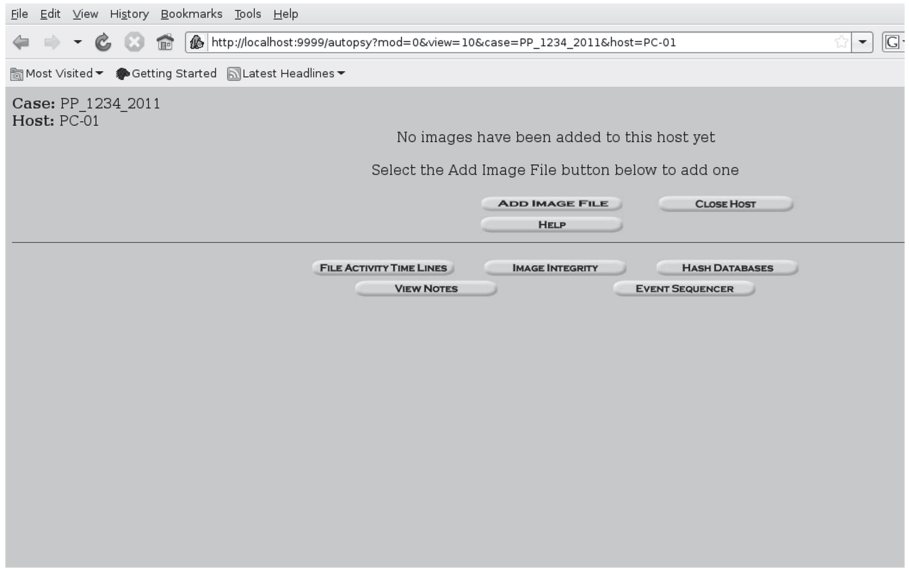
Autopsy – Aggiunta di un host



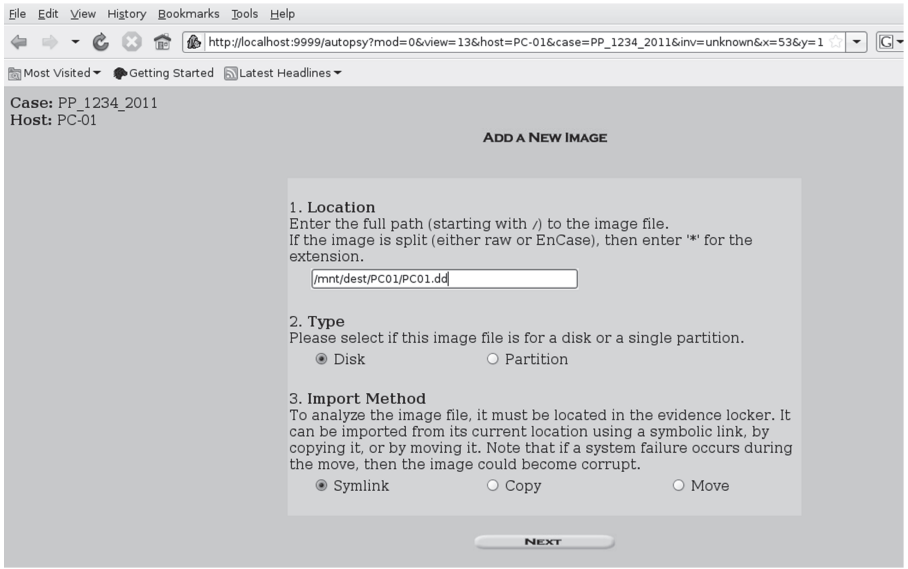
Autopsy – Aggiunta di un host



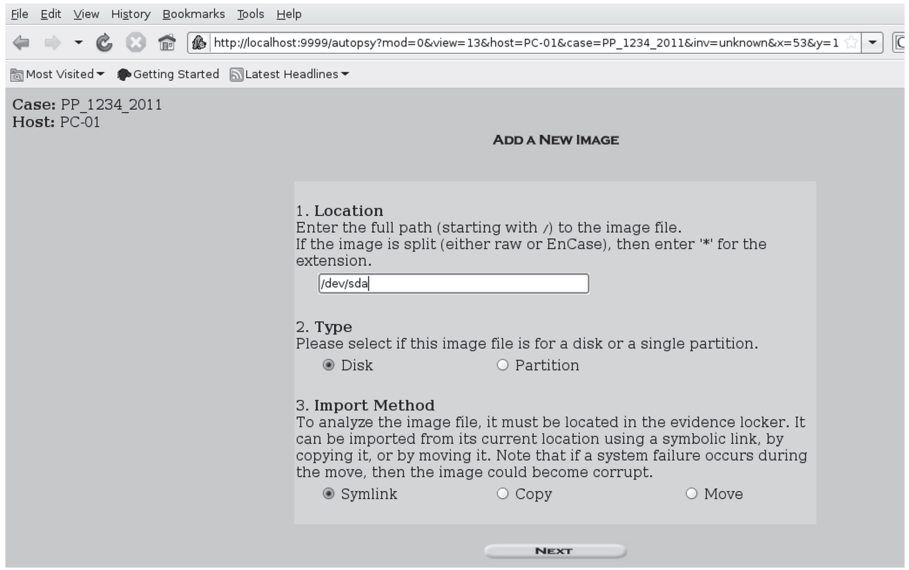
Autopsy – Aggiunta di un host



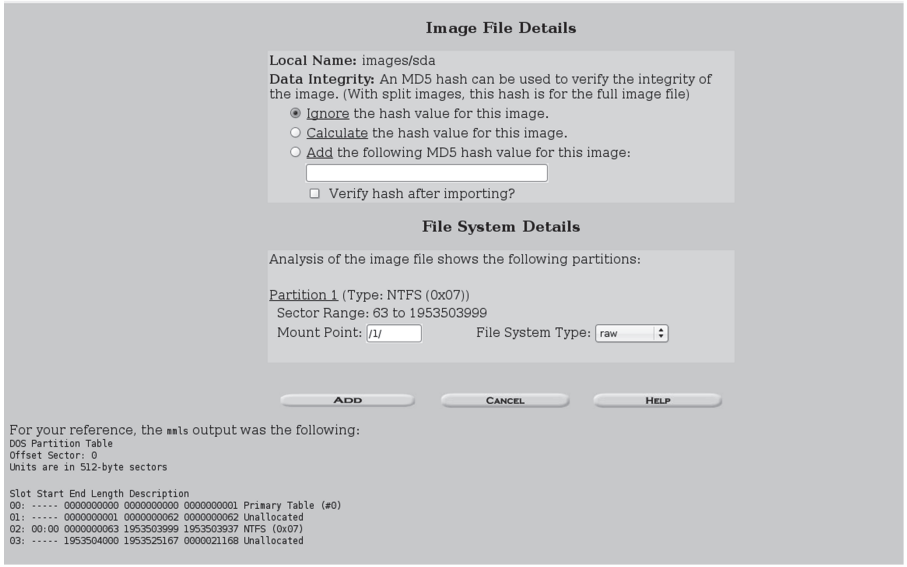
Autopsy – Aggiunta di un'immagine



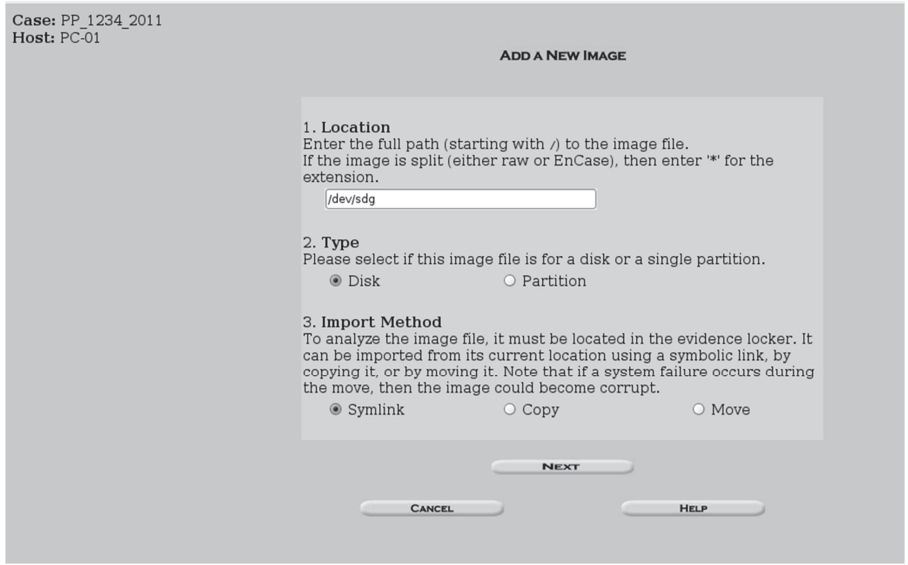
Autopsy – Aggiunta di un disco



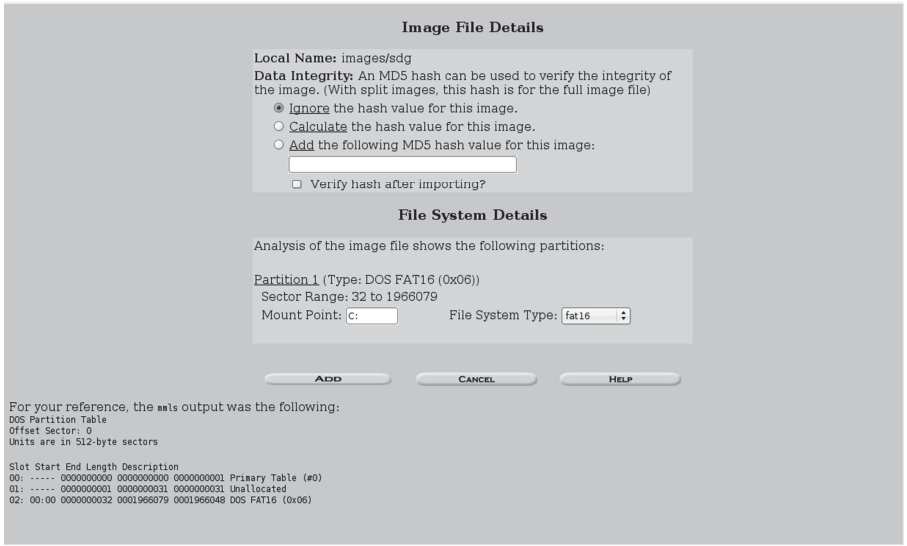
Autopsy – Aggiunta di un disco



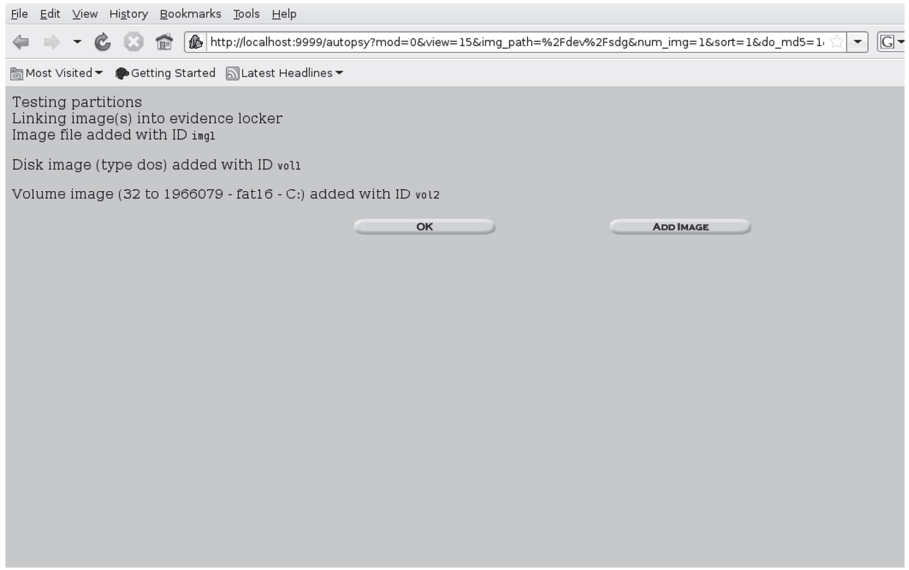
Autopsy – Aggiunta di un disco



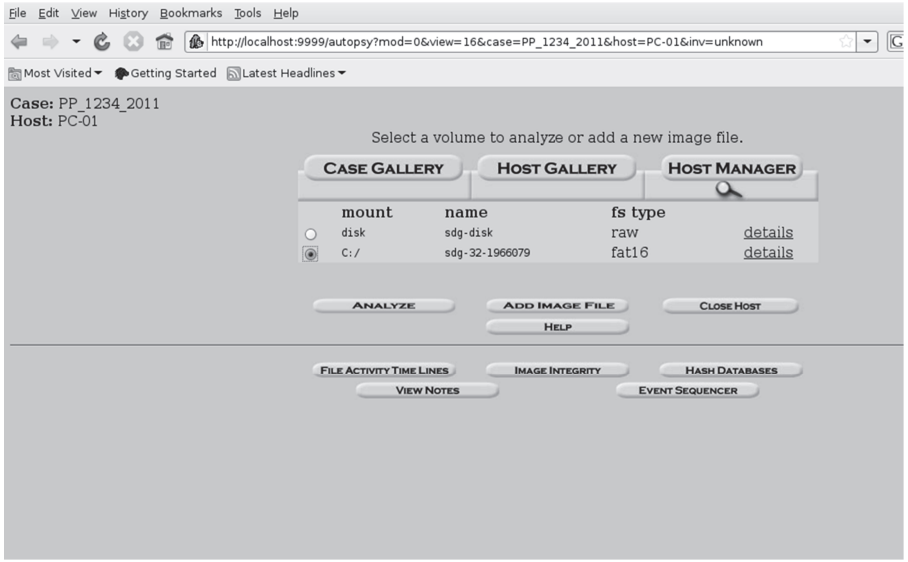
Autopsy – Aggiunta di un disco



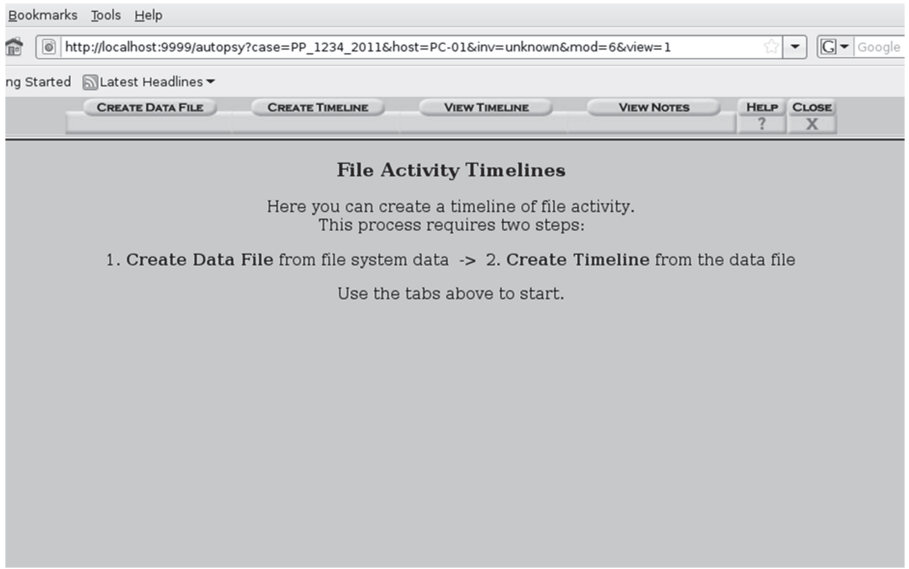
Autopsy – Aggiunta di un disco



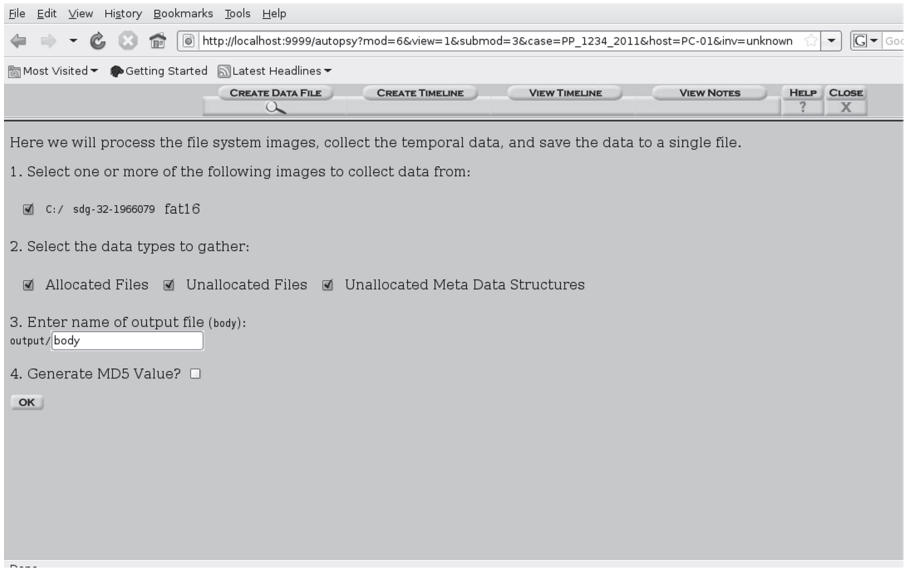
Autopsy – Aggiunta di un disco



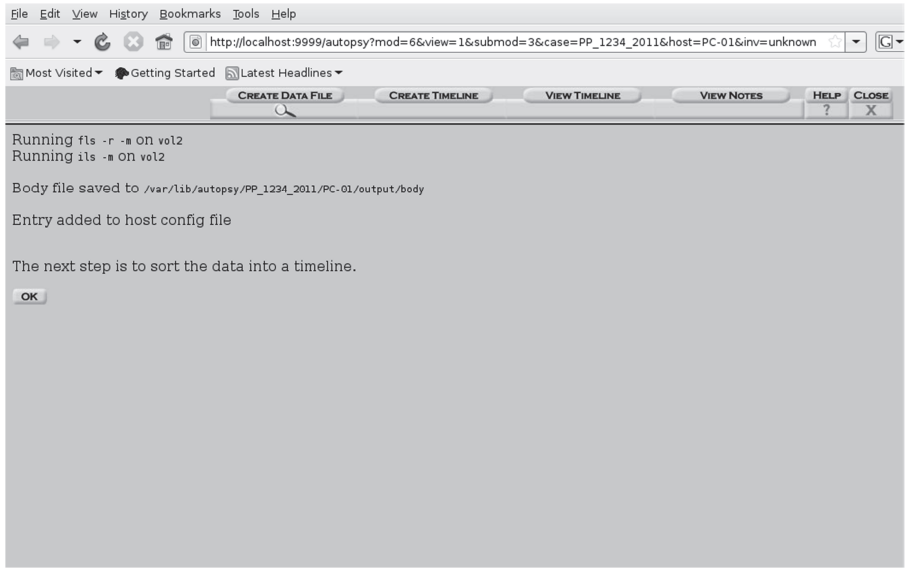
Autopsy – Timeline



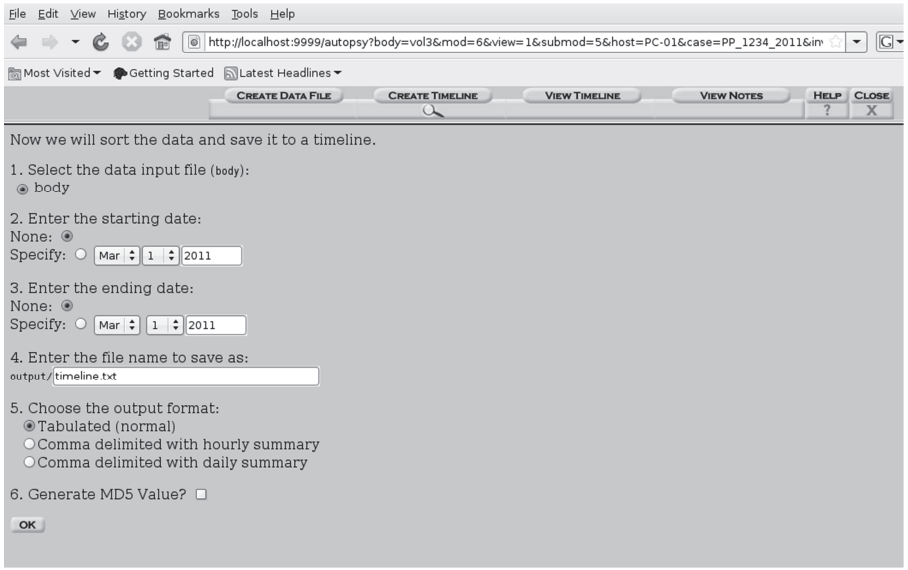
Autopsy – Timeline



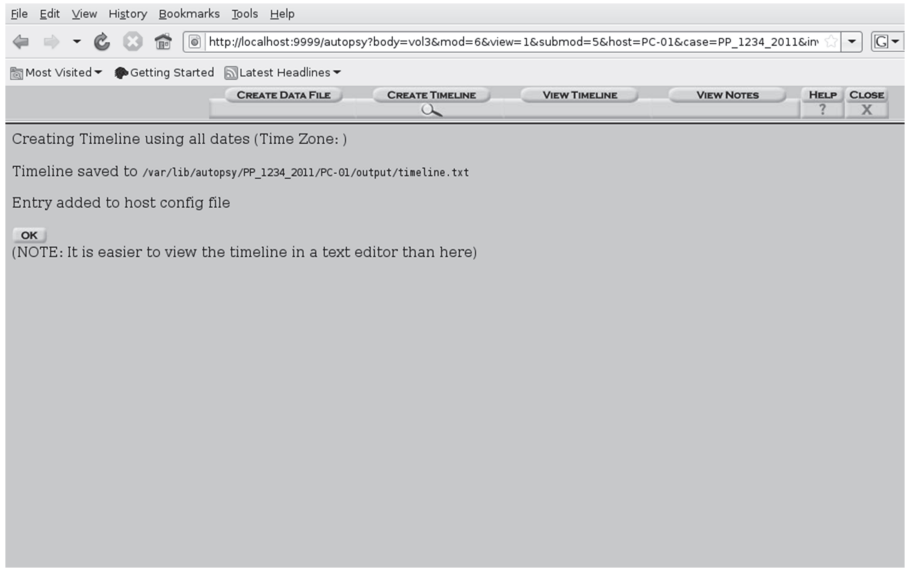
Autopsy – Timeline



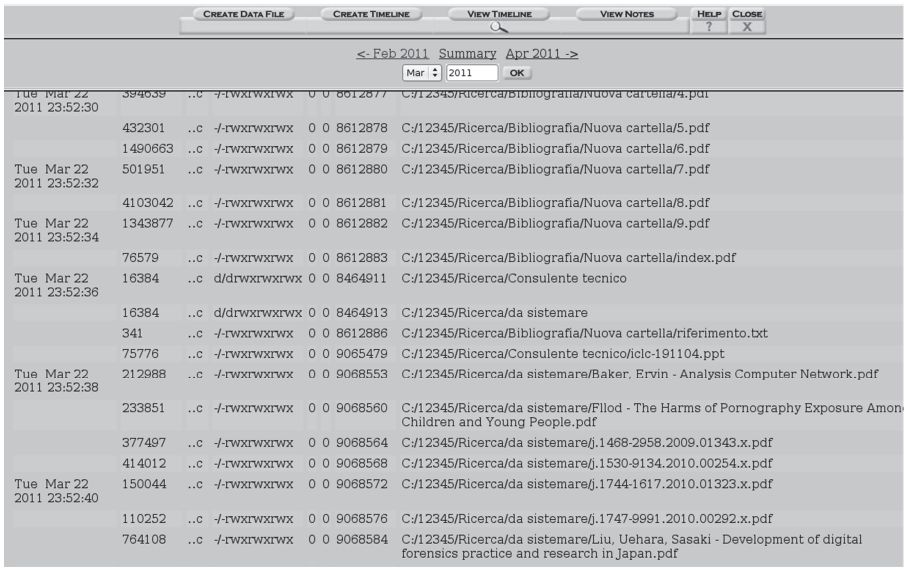
Autopsy – Timeline



Autopsy – Timeline



Autopsy – Timeline

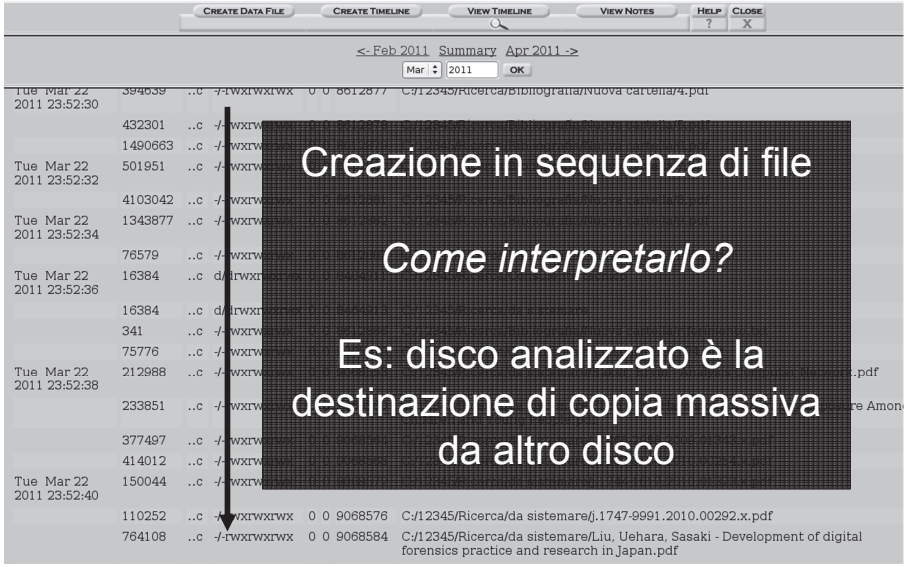


Tue Mar 22 2011 23:52:30	394639	..c	-/-rwxrwxrwx	0	0	8612877	C:/12345/Ricerca/Bibliografia/Nuova cartella/4.pdf
	432301	..c	-/-rwxrwxrwx	0	0	8612878	C:/12345/Ricerca/Bibliografia/Nuova cartella/5.pdf
	1490663	..c	-/-rwxrwxrwx	0	0	8612879	C:/12345/Ricerca/Bibliografia/Nuova cartella/6.pdf
Tue Mar 22 2011 23:52:32	501951	..c	-/-rwxrwxrwx	0	0	8612880	C:/12345/Ricerca/Bibliografia/Nuova cartella/7.pdf
	4103042	..c	-/-rwxrwxrwx	0	0	8612881	C:/12345/Ricerca/Bibliografia/Nuova cartella/8.pdf
Tue Mar 22 2011 23:52:34	1343877	..c	-/-rwxrwxrwx	0	0	8612882	C:/12345/Ricerca/Bibliografia/Nuova cartella/9.pdf
	76579	..c	-/-rwxrwxrwx	0	0	8612883	C:/12345/Ricerca/Bibliografia/Nuova cartella/index.pdf
Tue Mar 22 2011 23:52:36	16384	..c	d/drwxrwxrwx	0	0	8464911	C:/12345/Ricerca/Consulente tecnico
	16384	..c	d/drwxrwxrwx	0	0	8464913	C:/12345/Ricerca/da sistemare
	341	..c	-/-rwxrwxrwx	0	0	8612886	C:/12345/Ricerca/Bibliografia/Nuova cartella/riferimento.txt
	75776	..c	-/-rwxrwxrwx	0	0	9065479	C:/12345/Ricerca/Consulente tecnico/icic-191104.ppt
Tue Mar 22 2011 23:52:38	212988	..c	-/-rwxrwxrwx	0	0	9068553	C:/12345/Ricerca/da sistemare/Baker, Ervin - Analysis Computer Network.pdf
	233851	..c	-/-rwxrwxrwx	0	0	9068560	C:/12345/Ricerca/da sistemare/Fllod - The Harms of Pornography Exposure Amon Children and Young People.pdf
	377497	..c	-/-rwxrwxrwx	0	0	9068564	C:/12345/Ricerca/da sistemare/j.1468-2958.2009.01343.x.pdf
	414012	..c	-/-rwxrwxrwx	0	0	9068568	C:/12345/Ricerca/da sistemare/j.1530-9134.2010.00254.x.pdf
Tue Mar 22 2011 23:52:40	150044	..c	-/-rwxrwxrwx	0	0	9068572	C:/12345/Ricerca/da sistemare/j.1744-1617.2010.01323.x.pdf
	110252	..c	-/-rwxrwxrwx	0	0	9068576	C:/12345/Ricerca/da sistemare/j.1747-9991.2010.00292.x.pdf
	764108	..c	-/-rwxrwxrwx	0	0	9068584	C:/12345/Ricerca/da sistemare/Liu, Uehara, Sasaki - Development of digital forensics practice and research in Japan.pdf

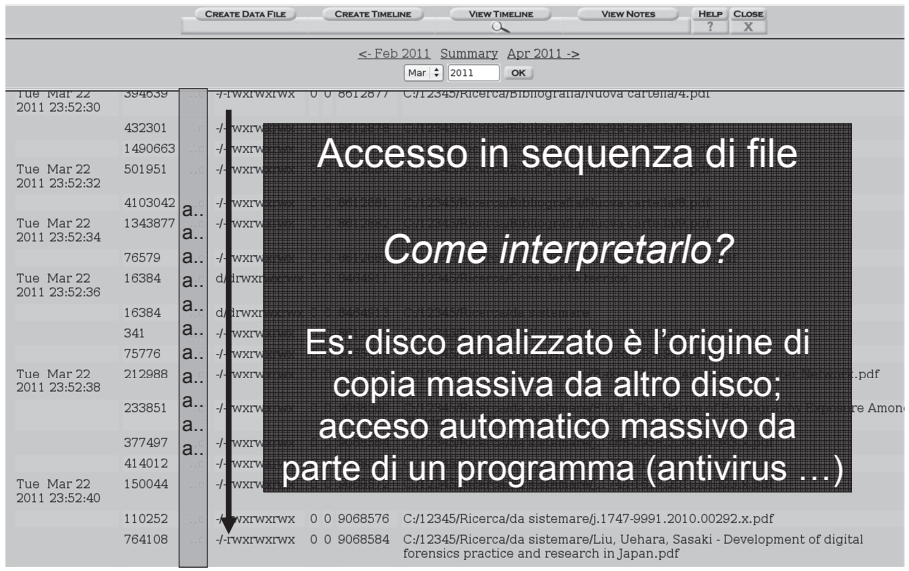
Autopsy – Timeline

Come interpretare questa timeline?

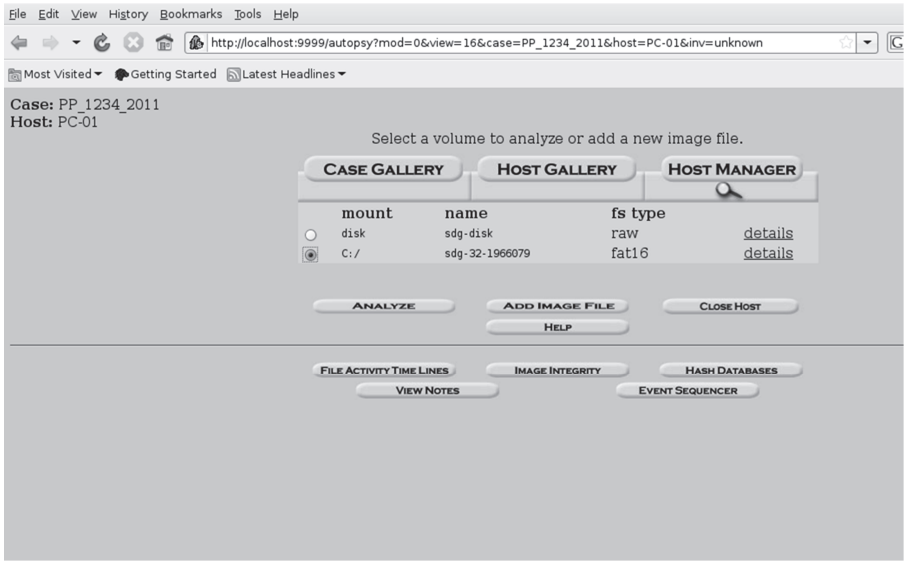
Autopsy – Timeline



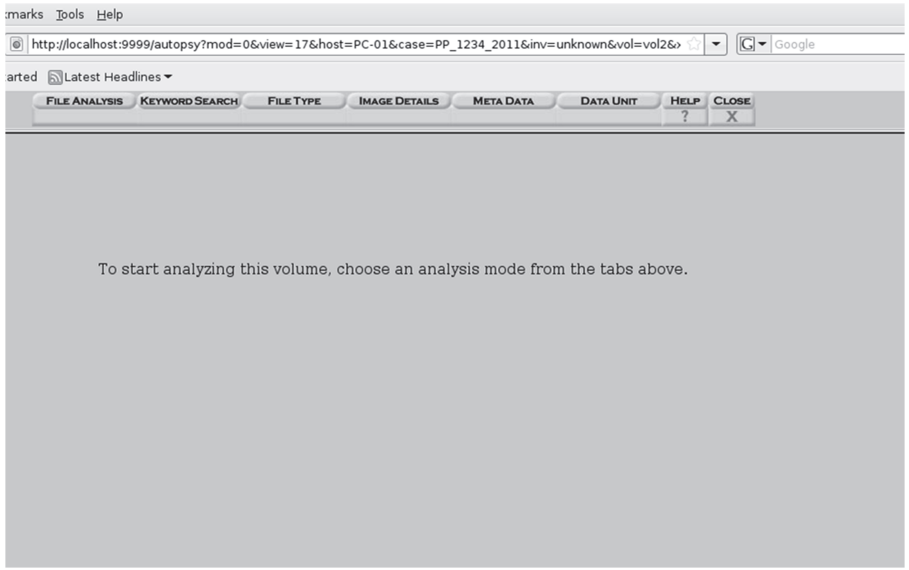
Autopsy – Timeline



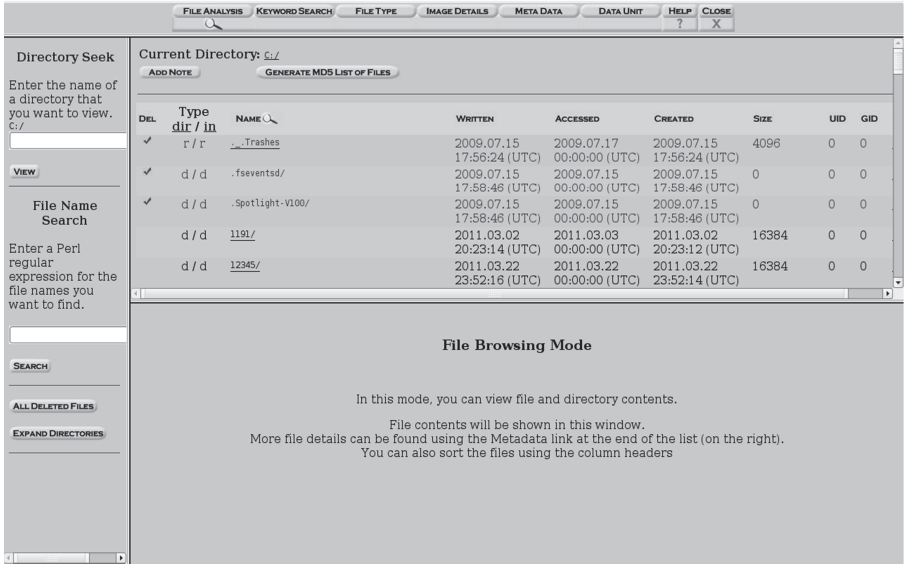
Autopsy – Analisi



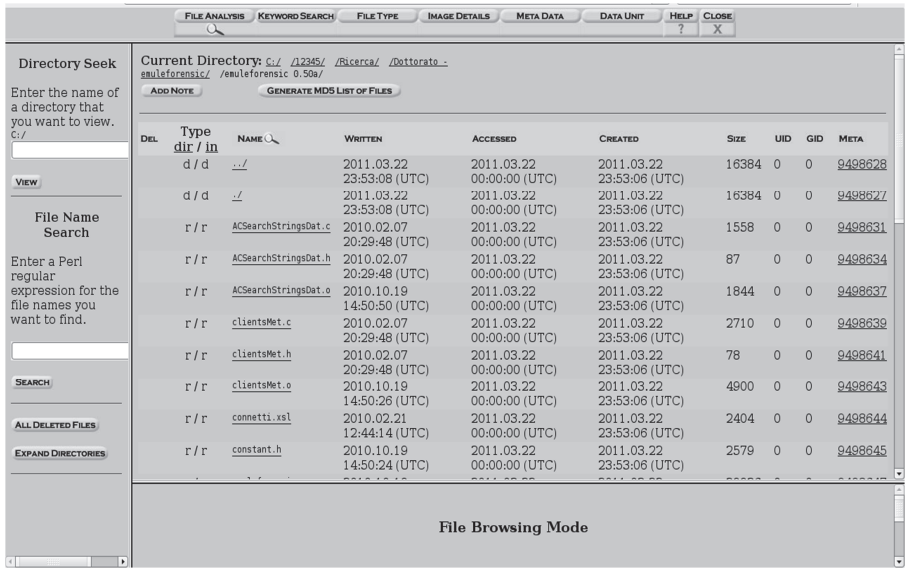
Autopsy – Analisi



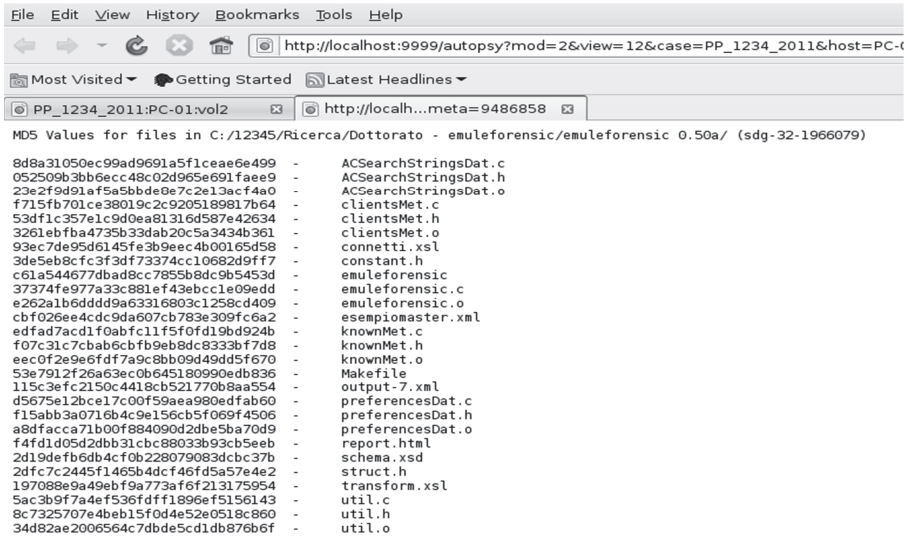
Autopsy – Analisi



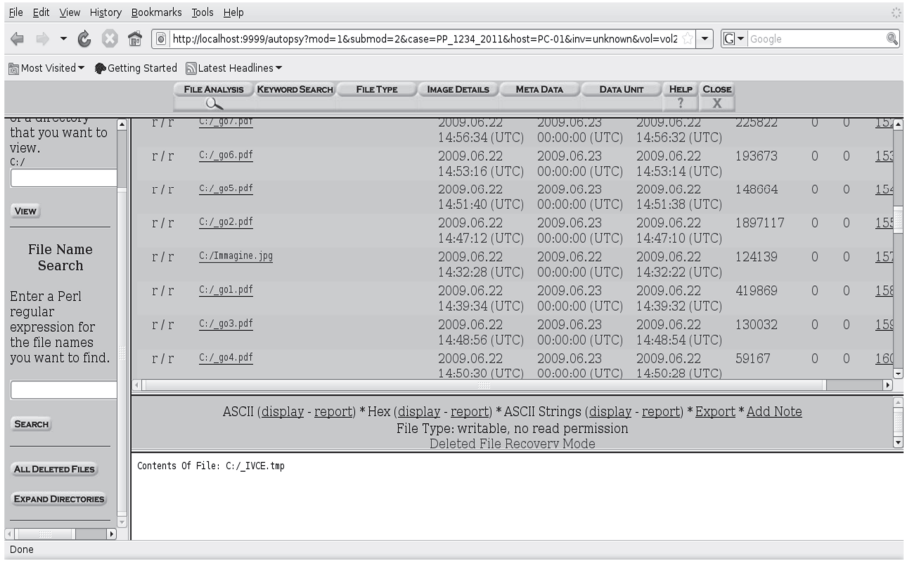
Autopsy – Analisi – File in chiaro



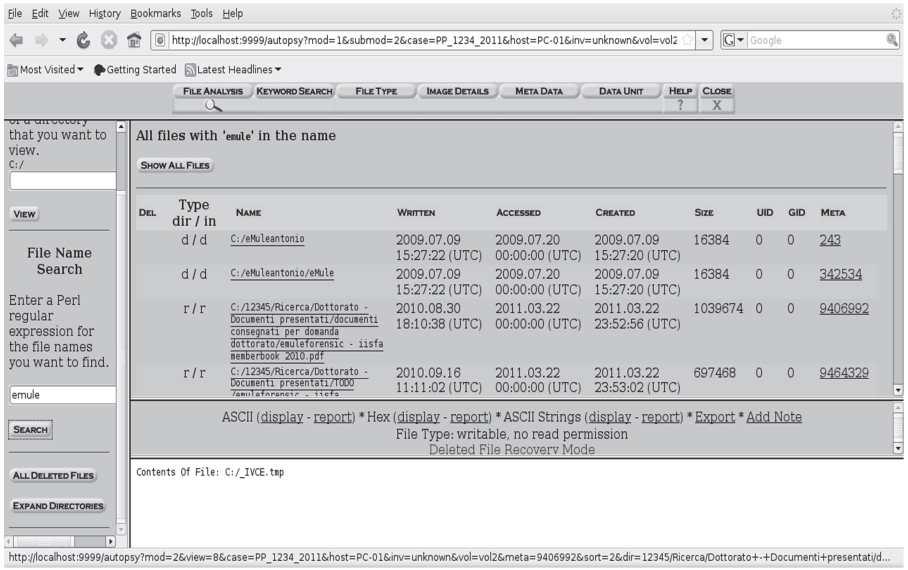
Autopsy – Analisi – Calcolo hash file



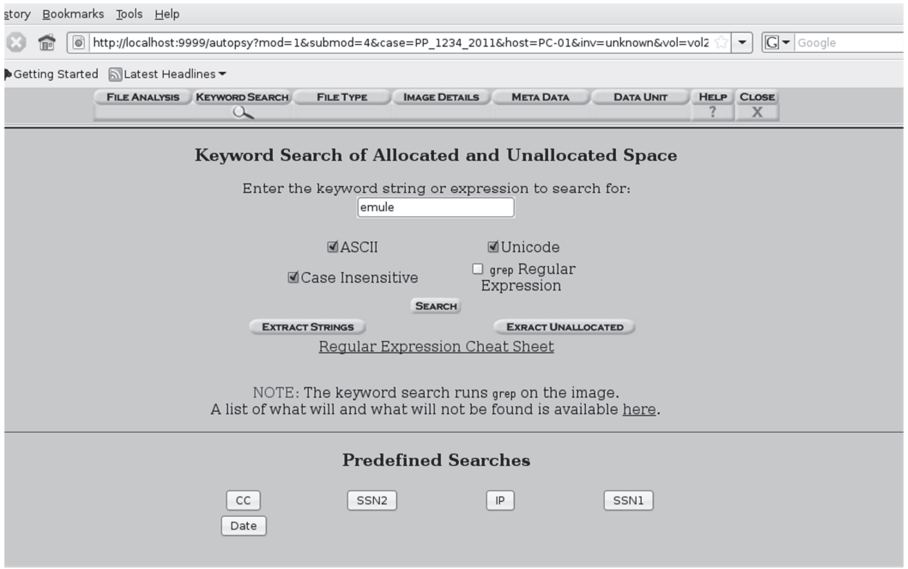
Autopsy – Analisi – File cancellati



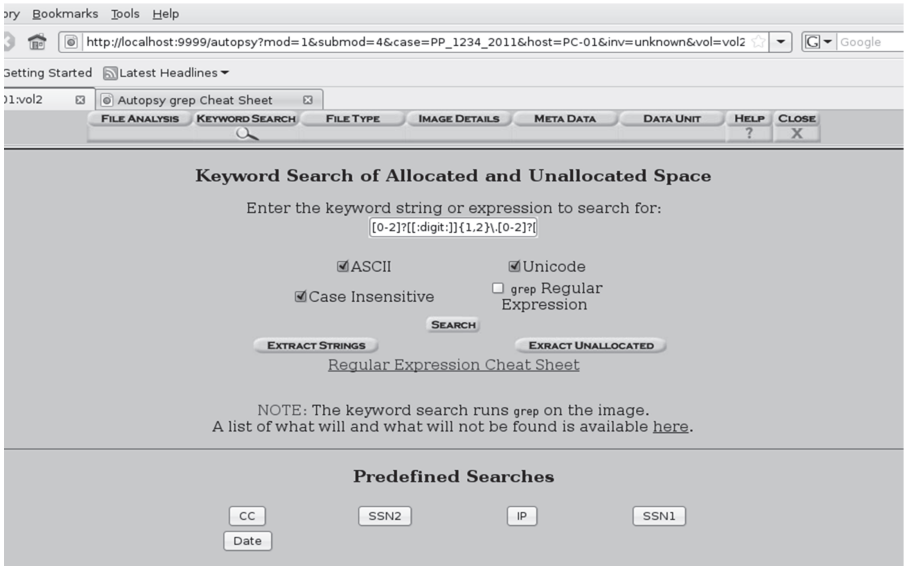
Autopsy – Analisi – Ricerca per keyword nel nome del file



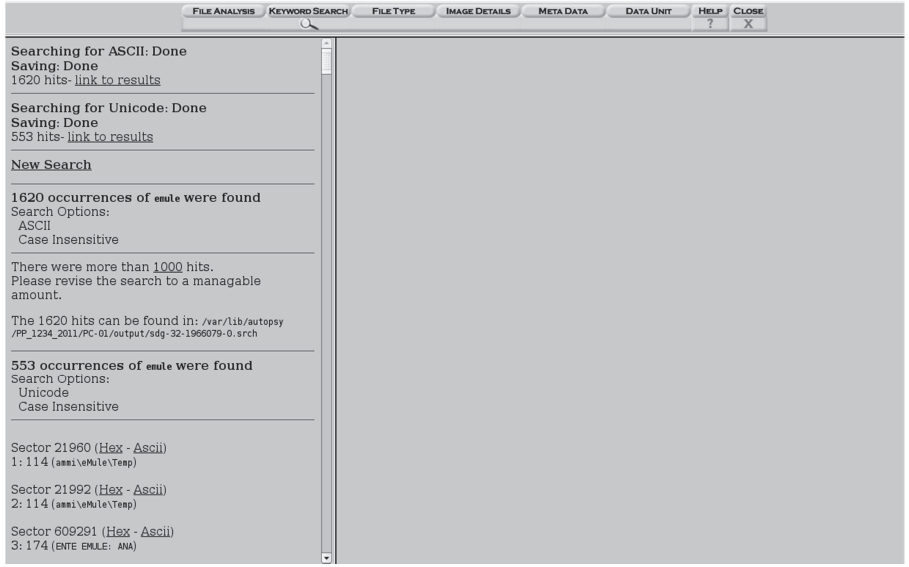
Autopsy – Ricerca per keyword nel contenuto



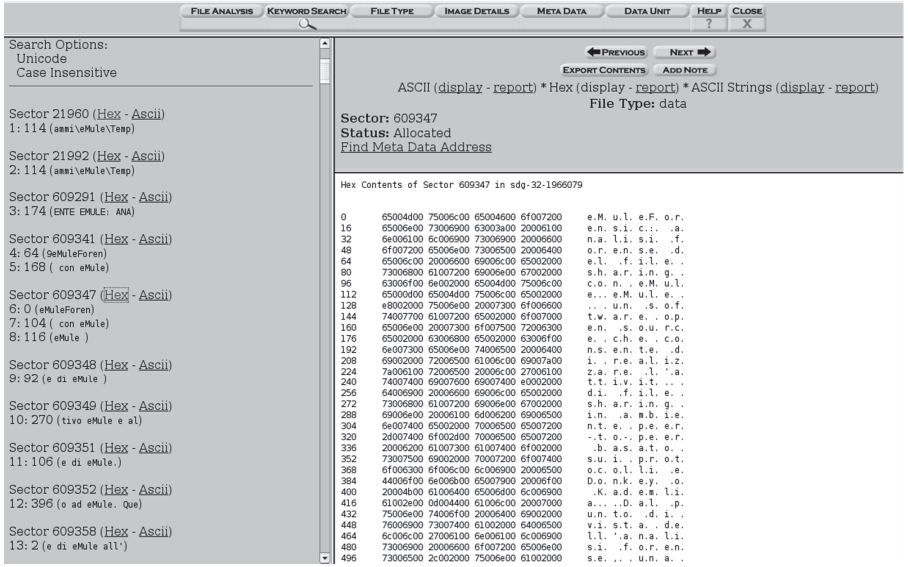
Autopsy – Ricerca per keyword nel contenuto



Autopsy – Ricerca per keyword nel contenuto



Autopsy – Ricerca per keyword nel contenuto



Riga di comando

- Calcolo hash tutti i file

```
find . type -f -exec md5sum '{}'
```

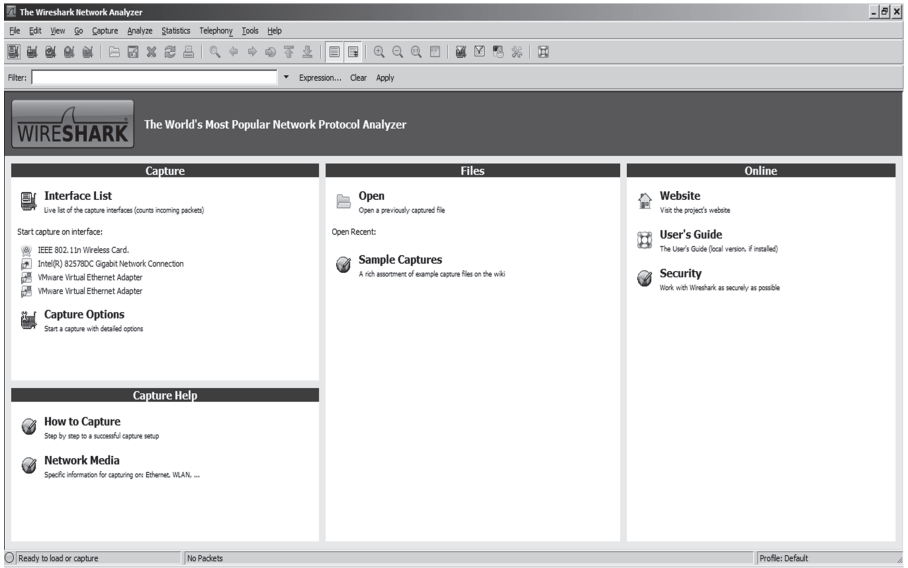
- Cancellare tutti i file *.md5
  - `find ./ -iname \*.md5 -exec rm {} \;`

Analisi di una email

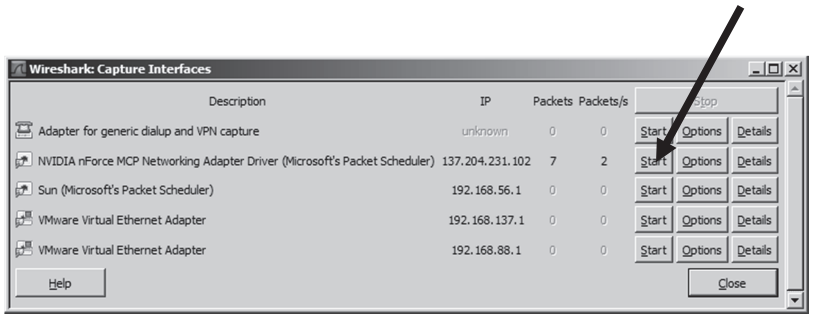
```
Return-Path: mittente@gmail.com
Received: from [192.168.1.83] (dynamic-adsl-84-220-169-6.clienti.tiscali.it
    [84.220.169.6])
    by mx.google.com with ESMTPS id bs4sm597962wbb.35.2011.03.25.12.31.02
    (version=SSLv3 cipher=OTHER);
Fri, 25 Mar 2011 12:31:03 -0700 (PDT)
Message-ID: 4D8CED7B.2050105@gmail.com
Date: Fri, 25 Mar 2011 20:31:07 +0100
From: Mittente Neri mittente@gmail.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; it; rv:1.9.2.15)
    Gecko/20110303 Lightning/1.0b2 Thunderbird/3.1.9
MIME-Version: 1.0
To: Destinatario Rossi destinatario@gmail.com
Subject: Re: Verbale ultimo
References: <4D8A677E.2060002@gmail.com> AANLkTinG17F2-8PuOfL3A_prj952-FT-
    KbAceJKW8mxg@mail.gmail.com
In-Reply-To: AANLkTinG17F2-8PuOfL3A_prj952-FT-KbAceJKW8mxg@mail.gmail.com
Content-Type: multipart/alternative;
boundary="------------060500090204050700070106"
This is a multi-part message in MIME format.
--------------060500090204050700070106
Content-Type: text/plain; charset=ISO-8859-1; format=flowed
Content-Transfer-Encoding: 8bit
Il 25/03/2011 19:37, Destinatario Rossi ha scritto:
 > Ciao ciao ciao.
 > > Ciao2 ciao2 ciao2
```

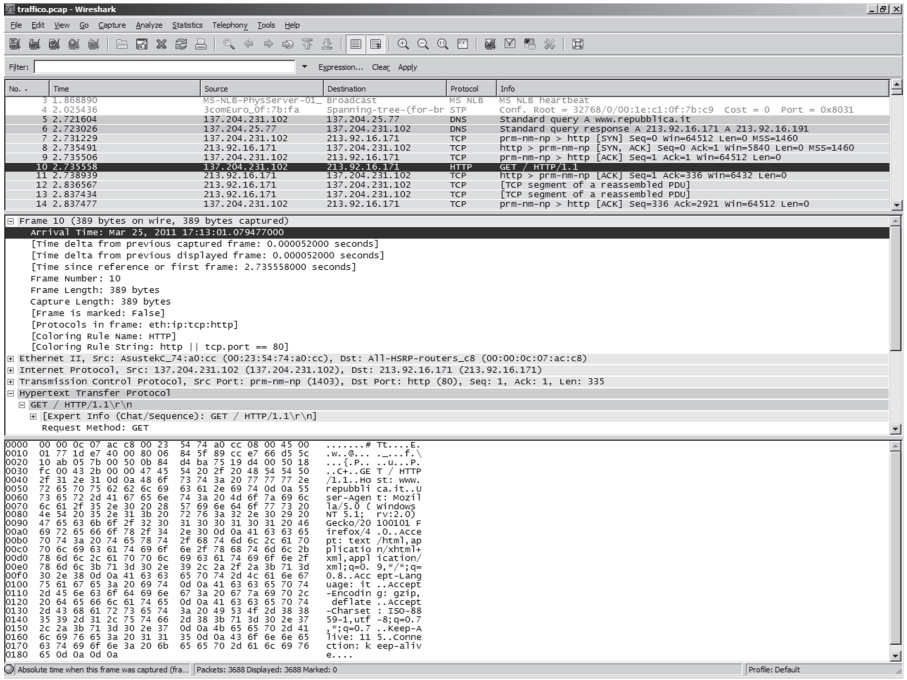
Analisi forense di traffico di rete

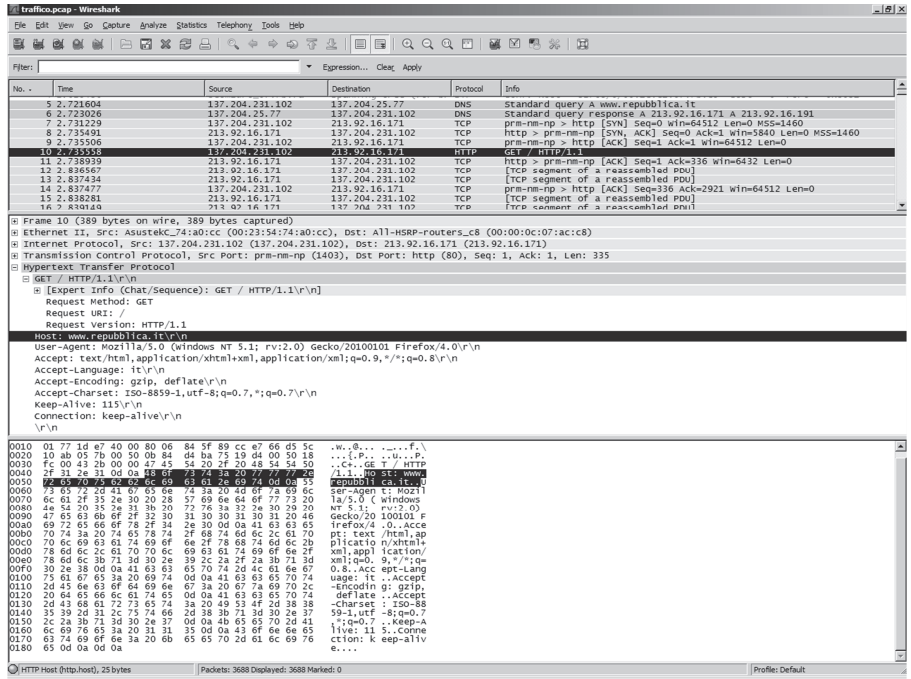
Wireshark

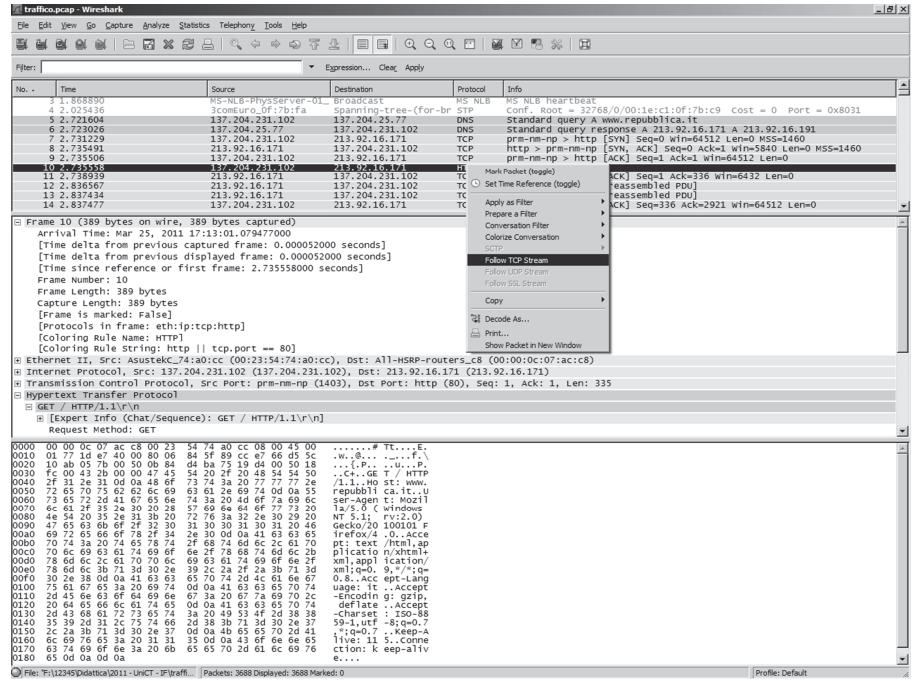


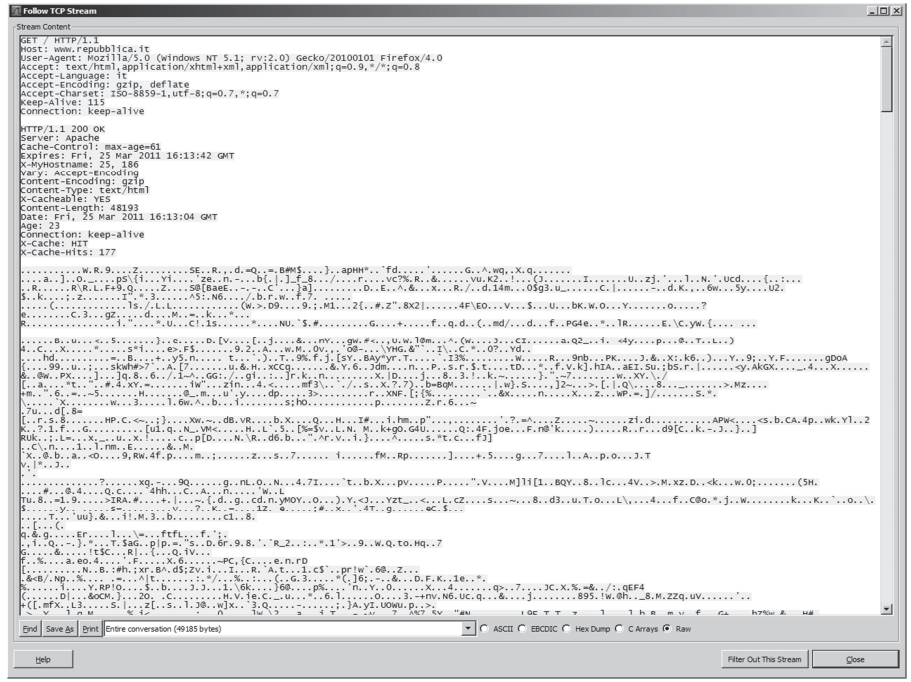
Avvio dell'intercettazione del traffico

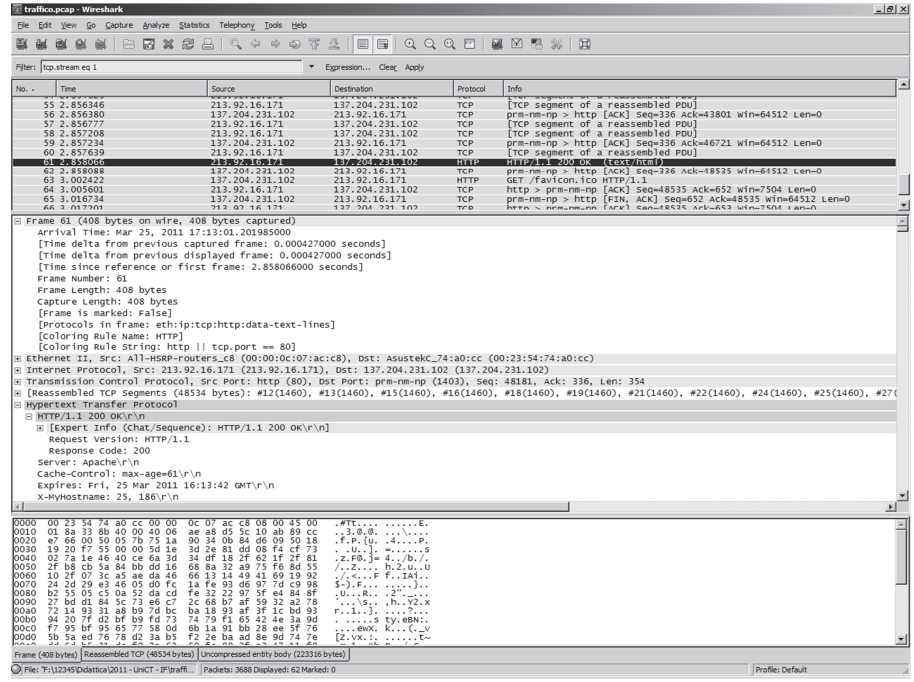


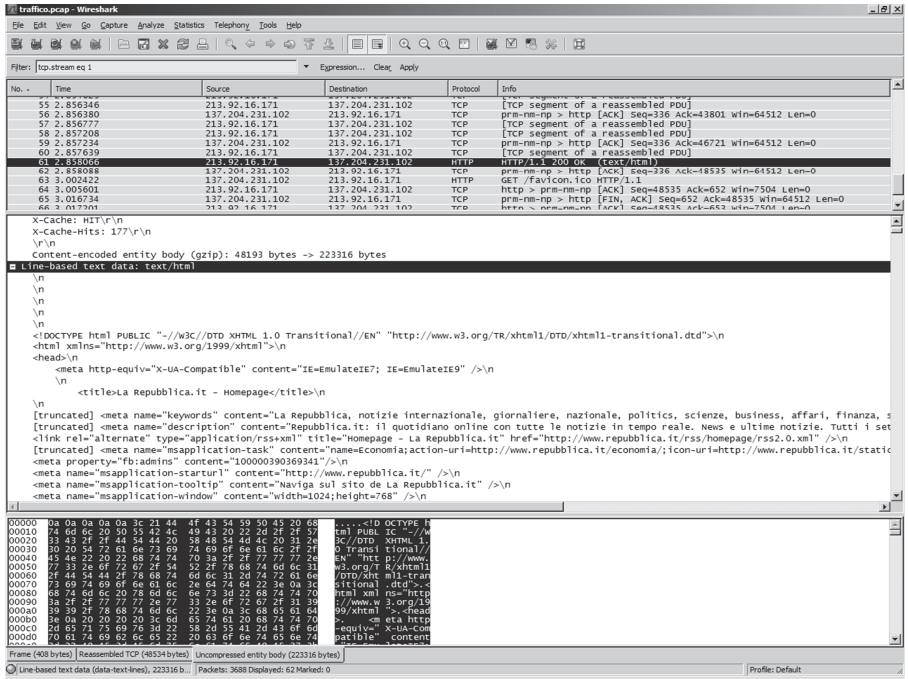


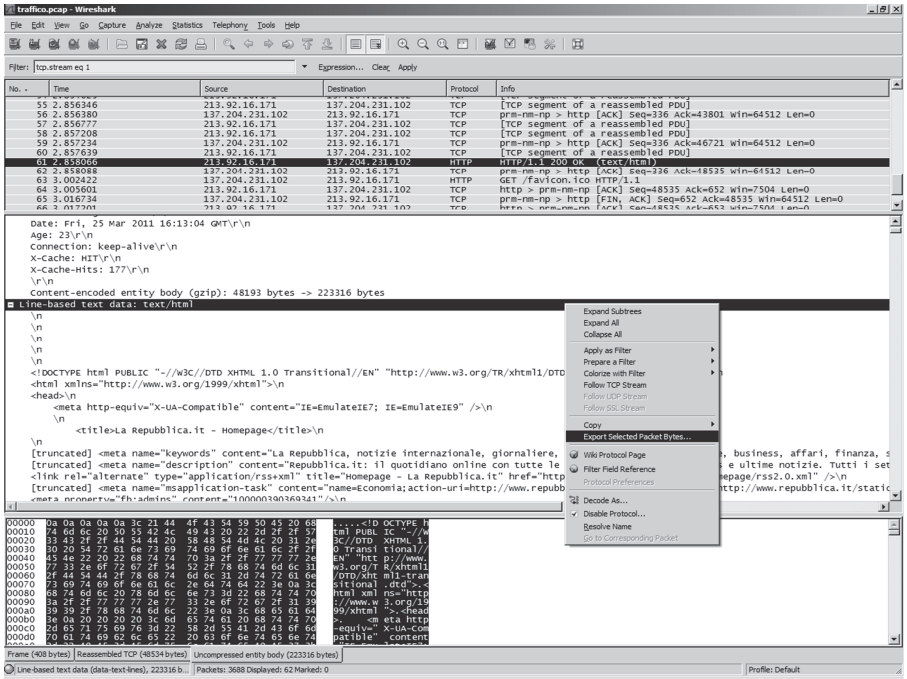

traffico.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply
No. - Time Source Destination Protocol Info
5 2.721604 137.204.231.102 137.204.25.77 DNS Standard query A www.repubblica.it
6 2.723026 137.204.25.77 137.204.231.102 DNS Standard query response A 213.92.16.171 A 213.92.16.191
7 2.731229 137.204.231.102 213.92.16.171 TCP prm-nm-np > http [SYN] Seq=0 Win=64512 Len=0 MSS=1460
8 2.735491 213.92.16.171 137.204.231.102 TCP http > prm-nm-np [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
9 2.735506 137.204.231.102 213.92.16.171 TCP prm-nm-np > http [ACK] Seq=1 Ack=1 Win=64512 Len=0
10 2.735558 137.204.231.102 213.92.16.171 HTTP GET / HTTP/1.1
11 2.738939 213.92.16.171 137.204.231.102 TCP http > prm-nm-np [ACK] Seq=1 Ack=336 Win=6432 Len=0
12 2.836567 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
13 2.837434 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
14 2.837477 137.204.231.102 213.92.16.171 TCP prm-nm-np > http [ACK] Seq=336 Ack=2921 Win=64512 Len=0
15 2.838281 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
16 2.839149 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
Frame 10 (389 bytes on wire, 389 bytes captured)
Ethernet II, Src: AsustekC_74:a0:cc (00:23:54:74:a0:cc), Dst: All-HSRP-routers_c8 (00:00:0c:07:ac:c8)
Internet Protocol, Src: 137.204.231.102 (137.204.231.102), Dst: 213.92.16.171 (213.92.16.171)
Transmission Control Protocol, Src Port: prm-nm-np (1403), Dst Port: http (80), Seq: 1, Ack: 1, Len: 335
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
Request Method: GET
Request URI: /
Request Version: HTTP/1.1
Host: www.repubblica.it\r\n
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:2.0) Gecko/20100101 Firefox/4.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: it\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: 115\r\n
Connection: keep-alive\r\n
\r\n
0010 01 77 1d e7 40 00 80 06 84 5f 89 cc e7 66 d5 5c .w..@... ._...f.\
0020 10 ab 05 7b 00 50 0b 84 d4 ba 75 19 d4 00 50 18 ...{.P.. ..u...P.
0030 fc 00 43 2b 00 00 47 45 54 20 2f 20 48 54 54 50 ..C+..GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e /1.1..Ho st: www.
0050 72 65 70 75 62 62 6c 69 63 61 2e 69 74 0d 0a 55 repubbli ca.it..U
0060 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c ser-Agen t: Mozil
0070 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 la/5.0 (windows
0080 4e 54 20 35 2e 31 3b 20 72 76 3a 32 2e 30 29 20 NT 5.1; rv:2.0)
0090 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 Gecko/20 100101 F
00a0 69 72 65 66 6f 78 2f 34 2e 30 0d 0a 41 63 63 65 irefox/4 .0..Acce
00b0 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 pt: text /html,ap
00c0 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b plicatio n/xhtml+
00d0 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f xml,appl ication/
00e0 78 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f 2a 3b 71 3d xml;q=0. 9,*/*;q=
00f0 30 2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 0.8..Acc ept-Lang
0100 75 61 67 65 3a 20 69 74 0d 0a 41 63 63 65 70 74 uage: it ..Accept
0110 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c -Encodin g: gzip,
0120 20 64 65 66 6c 61 74 65 0d 0a 41 63 63 65 70 74 deflate ..Accept
0130 2d 43 68 61 72 73 65 74 3a 20 49 53 4f 2d 38 38 -Charset : ISO-88
0140 35 39 2d 31 2c 75 74 66 2d 38 3b 71 3d 30 2e 37 59-1,utf -8;q=0.7
0150 2c 2a 3b 71 3d 30 2e 37 0d 0a 4b 65 65 70 2d 41 ,*;q=0.7 ..Keep-A
0160 6c 69 76 65 3a 20 31 31 35 0d 0a 43 6f 6e 6e 65 live: 11 5..Conne
0170 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 ction: k eep-aliv
0180 65 0d 0a 0d 0a e....
HTTP Host (http.host), 25 bytes
Packets: 3688 Displayed: 3688 Marked: 0
Profile: Default

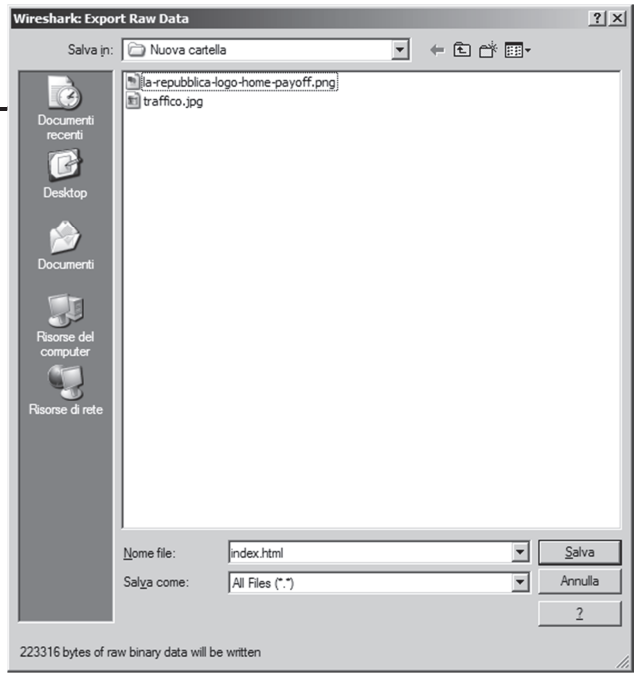

traffico.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply
No. - Time Source Destination Protocol Info
3 1.868890 MS-NLB-PhysServer-01_ Broadcast MS NLB MS NLB heartbeat
4 2.025436 3comEuro_0f:7b:fa Spanning-tree-(for-br STP Conf. Root = 32768/0/00:1e:c1:0f:7b:c9 Cost = 0 Port = 0x8031
5 2.721604 137.204.231.102 137.204.25.77 DNS Standard query A www.repubblica.it
6 2.723026 137.204.25.77 137.204.231.102 DNS Standard query response A 213.92.16.171 A 213.92.16.191
7 2.731229 137.204.231.102 213.92.16.171 TCP prm-nm-np > http [SYN] Seq=0 Win=64512 Len=0 MSS=1460
8 2.735491 213.92.16.171 137.204.231.102 TCP http > prm-nm-np [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
9 2.735506 137.204.231.102 213.92.16.171 TCP prm-nm-np > http [ACK] Seq=1 Ack=1 Win=64512 Len=0
10 2.735558 137.204.231.102 213.92.16.171 HTTP GET / HTTP/1.1
11 2.738939 213.92.16.171 137.204.231.102 TCP http > prm-nm-np [ACK] Seq=1 Ack=336 Win=6432 Len=0
12 2.836567 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
13 2.837434 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
14 2.837477 137.204.231.102 213.92.16.171 TCP prm-nm-np > http [ACK] Seq=336 Ack=2921 Win=64512 Len=0
Mark Packet (toggle)
Set Time Reference (toggle)
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Copy
Decode As...
Print...
Show Packet in New Window
Frame 10 (389 bytes on wire, 389 bytes captured)
Arrival Time: Mar 25, 2011 17:13:01.079477000
[Time delta from previous captured frame: 0.000052000 seconds]
[Time delta from previous displayed frame: 0.000052000 seconds]
[Time since reference or first frame: 2.735558000 seconds]
Frame Number: 10
Frame Length: 389 bytes
Capture Length: 389 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:tcp:http]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80]
Ethernet II, Src: AsustekC_74:a0:cc (00:23:54:74:a0:cc), Dst: All-HSRP-routers_c8 (00:00:0c:07:ac:c8)
Internet Protocol, Src: 137.204.231.102 (137.204.231.102), Dst: 213.92.16.171 (213.92.16.171)
Transmission Control Protocol, Src Port: prm-nm-np (1403), Dst Port: http (80), Seq: 1, Ack: 1, Len: 335
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
Request Method: GET
0000 00 00 0c 07 ac c8 00 23 54 74 a0 cc 08 00 45 00 ....# Tt....E.
0010 01 77 1d e7 40 00 80 06 84 5f 89 cc e7 66 d5 5c .w..@... ._...f.\
0020 10 ab 05 7b 00 50 0b 84 d4 ba 75 19 d4 00 50 18 ...{.P.. ..u...P.
0030 fc 00 43 2b 00 00 47 45 54 20 2f 20 48 54 54 50 ..C+..GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e /1.1..Ho st: www.
0050 72 65 70 75 62 62 6c 69 63 61 2e 69 74 0d 0a 55 repubbli ca.it..U
0060 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c ser-Agen t: Mozil
0070 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 la/5.0 (windows
0080 4e 54 20 35 2e 31 3b 20 72 76 3a 32 2e 30 29 20 NT 5.1; rv:2.0)
0090 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 Gecko/20 100101 F
00a0 69 72 65 66 6f 78 2f 34 2e 30 0d 0a 41 63 63 65 irefox/4 .0..Acce
00b0 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 pt: text /html,ap
00c0 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b plicatio n/xhtml+
00d0 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f xml,appl ication/
00e0 78 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f 2a 3b 71 3d xml;q=0. 9,*/*;q=
00f0 30 2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 0.8..Acc ept-Lang
0100 75 61 67 65 3a 20 69 74 0d 0a 41 63 63 65 70 74 uage: it ..Accept
0110 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c -Encodin g: gzip,
0120 20 64 65 66 6c 61 74 65 0d 0a 41 63 63 65 70 74 deflate ..Accept
0130 2d 43 68 61 72 73 65 74 3a 20 49 53 4f 2d 38 38 -Charset : ISO-88
0140 35 39 2d 31 2c 75 74 66 2d 38 3b 71 3d 30 2e 37 59-1,utf -8;q=0.7
0150 2c 2a 3b 71 3d 30 2e 37 0d 0a 4b 65 65 70 2d 41 ,*;q=0.7 ..Keep-A
0160 6c 69 76 65 3a 20 31 31 35 0d 0a 43 6f 6e 6e 65 live: 11 5..Conne
0170 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 ction: k eep-aliv
0180 65 0d 0a 0d 0a e....
File: 'F:\12345\Didattica\2011 - UniCT - IF\traffi...
Packets: 3688 Displayed: 3688 Marked: 0
Profile: Default

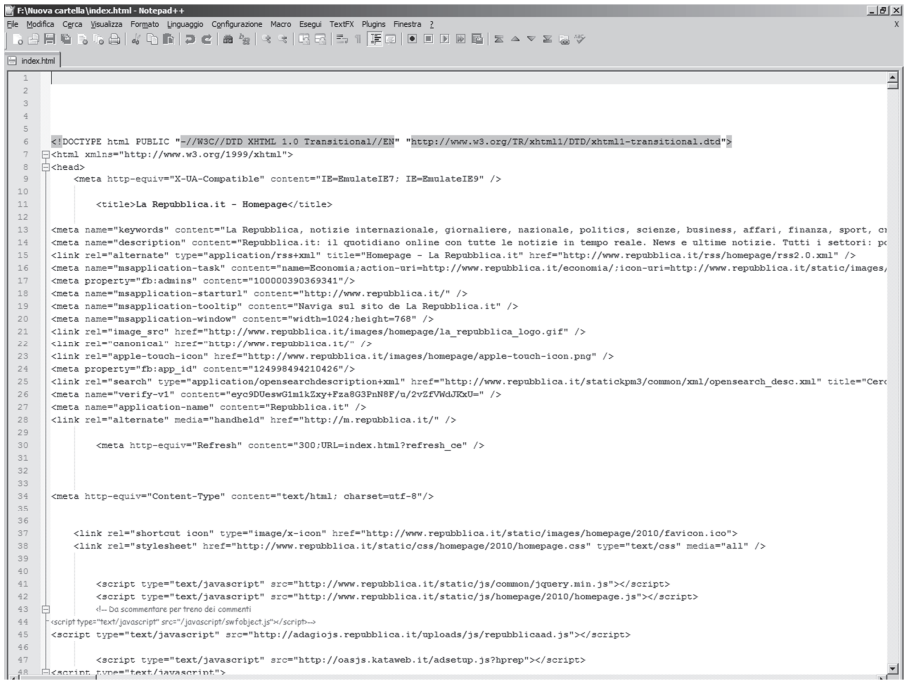

Follow TCP Stream
Stream Content
GET / HTTP/1.1
Host: www.repubblica.it
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:2.0) Gecko/20100101 Firefox/4.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: it
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
HTTP/1.1 200 OK
Server: Apache
Cache-Control: max-age=61
Expires: Fri, 25 Mar 2011 16:13:42 GMT
X-MyHostname: 25, 186
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Type: text/html
X-Cacheable: YES
Content-Length: 48193
Date: Fri, 25 Mar 2011 16:13:04 GMT
Age: 23
Connection: keep-alive
X-Cache: HIT
X-Cache-Hits: 177
Find Save As Print Entire conversation (49185 bytes)
ASCII EBCDIC Hex Dump C Arrays Raw
Help
Filter Out This Stream
Close

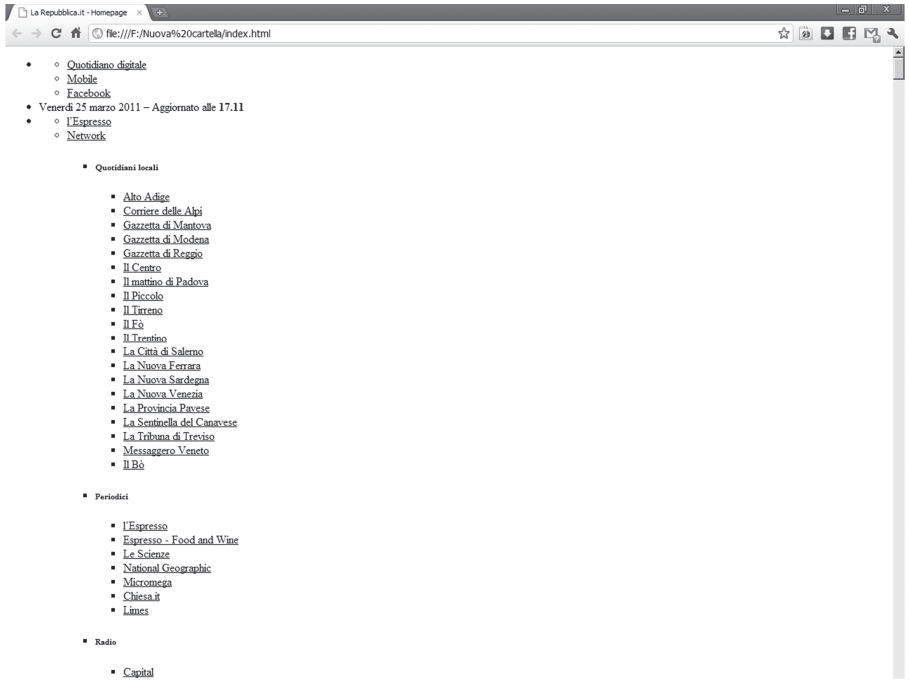

traffico.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: tcp.stream eq 1
Expression... Clear Apply
No. - Time Source Destination Protocol Info
55 2.856346 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
56 2.856380 137.204.231.102 213.92.16.171 TCP prm-nm-np > http [ACK] Seq=336 Ack=43801 Win=64512 Len=0
57 2.856777 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
58 2.857208 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
59 2.857234 137.204.231.102 213.92.16.171 TCP prm-nm-np > http [ACK] Seq=336 Ack=46721 Win=64512 Len=0
60 2.857639 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
61 2.858066 213.92.16.171 137.204.231.102 HTTP HTTP/1.1 200 OK (text/html)
62 2.858088 137.204.231.102 213.92.16.171 TCP prm-nm-np > http [ACK] Seq=336 Ack=48535 Win=64512 Len=0
63 3.002422 137.204.231.102 213.92.16.171 HTTP GET /favicon.ico HTTP/1.1
64 3.005601 213.92.16.171 137.204.231.102 TCP http > prm-nm-np [ACK] Seq=48535 Ack=652 Win=7504 Len=0
65 3.016734 137.204.231.102 213.92.16.171 TCP prm-nm-np > http [FIN, ACK] Seq=652 Ack=48535 Win=64512 Len=0
66 3.017201 213.92.16.171 137.204.231.102 TCP http > prm-nm-np [ACK] Seq=48535 Ack=653 Win=7504 Len=0
Frame 61 (408 bytes on wire, 408 bytes captured)
Arrival Time: Mar 25, 2011 17:13:01.201985000
[Time delta from previous captured frame: 0.000427000 seconds]
[Time delta from previous displayed frame: 0.000427000 seconds]
[Time since reference or first frame: 2.858066000 seconds]
Frame Number: 61
Frame Length: 408 bytes
Capture Length: 408 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:tcp:http:data-text-lines]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80]
Ethernet II, Src: All-HSRP-routers_c8 (00:00:0c:07:ac:c8), Dst: AsustekC_74:a0:cc (00:23:54:74:a0:cc)
Internet Protocol, Src: 213.92.16.171 (213.92.16.171), Dst: 137.204.231.102 (137.204.231.102)
Transmission Control Protocol, Src Port: http (80), Dst Port: prm-nm-np (1403), Seq: 48181, Ack: 336, Len: 354
[Reassembled TCP Segments (48534 bytes): #12(1460), #13(1460), #15(1460), #16(1460), #18(1460), #19(1460), #21(1460), #22(1460), #24(1460), #25(1460), #27(
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
Request Version: HTTP/1.1
Response Code: 200
Server: Apache\r\n
Cache-Control: max-age=61\r\n
Expires: Fri, 25 Mar 2011 16:13:42 GMT\r\n
X-MyHostname: 25, 186\r\n
0000 00 23 54 74 a0 cc 00 00 0c 07 ac c8 08 00 45 00 .#Tt.... ......E.
0010 01 8a 33 8b 40 00 40 06 ae a8 d5 5c 10 ab 89 cc ..3.@.@. ...\....
0020 e7 66 00 50 05 7b 75 1a 90 34 0b 84 d6 09 50 18 .f.P.{u. .4....P.
0030 19 20 f7 55 00 00 5d 1e 3d 2e 81 dd 08 f4 cf 73 . .U..]. =......s
0040 02 7a 1e 46 40 ce 6a 3d 34 df 18 2f 62 1f 2f 81 .z.F@.j= 4../b./.
0050 2f b8 cb 5a 84 bb dd 16 68 8a 32 a9 75 f6 8d 55 /..Z.... h.2.u..U
0060 10 2f 07 3c a5 ae da 46 66 13 14 49 41 69 19 92 ./.<...F f..IAi..
0070 24 2d 29 e3 46 05 d0 fc 1a fe 93 d6 97 7d c9 98 $-).F... .....}..
0080 b2 55 05 c5 0a 52 da cd fe 32 22 97 5f e4 84 8f .U...R.. .2"._...
0090 27 bd d1 84 5c 73 e6 c7 2c 68 b7 af 59 32 a2 78 '...\s.. ,h..Y2.x
00a0 72 14 93 31 a8 b9 7d bc ba 18 93 af 3f 1c bd 93 r..1..}. ....?...
00b0 94 20 7f d2 bf b9 fd 73 74 79 f1 65 42 4e 3a 9d . ..... sty.eBN:.
00c0 f7 95 bf 95 65 77 58 0d 6b 1a 91 bb 28 ee 5f 76 ....ewX. k...(._v
00d0 5b 5a ed 76 78 d2 3a b5 f2 2e ba ad 8e 9d 74 7e [Z.vx.:. ......t~
Frame (408 bytes) Reassembled TCP (48534 bytes) Uncompressed entity body (223316 bytes)
File: 'F:\12345\Didattica\2011 - UniCT - IF\traffi...
Packets: 3688 Displayed: 62 Marked: 0
Profile: Default


traffico.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: tcp.stream eq 1
Expression... Clear Apply
No. Time Source Destination Protocol Info
55 2.856346 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
56 2.856380 137.204.231.102 213.92.16.171 TCP prm-nm-np > http [ACK] Seq=336 Ack=43801 Win=64512 Len=0
57 2.856777 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
58 2.857208 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
59 2.857234 137.204.231.102 213.92.16.171 TCP prm-nm-np > http [ACK] Seq=336 Ack=46721 Win=64512 Len=0
60 2.857639 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
61 2.858066 213.92.16.171 137.204.231.102 HTTP HTTP/1.1 200 OK (text/html)
62 2.858088 137.204.231.102 213.92.16.171 TCP prm-nm-np > http [ACK] Seq=336 Ack=48535 Win=64512 Len=0
63 3.002422 137.204.231.102 213.92.16.171 HTTP GET /favicon.ico HTTP/1.1
64 3.005601 213.92.16.171 137.204.231.102 TCP http > prm-nm-np [ACK] Seq=48535 Ack=652 Win=7504 Len=0
65 3.016734 137.204.231.102 213.92.16.171 TCP prm-nm-np > http [FIN, ACK] Seq=652 Ack=48535 Win=64512 Len=0
X-Cache: HIT\r\n
X-Cache-Hits: 177\r\n
\r\n
Content-encoded entity body (gzip): 48193 bytes -> 223316 bytes
Line-based text data: text/html
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7; IE=EmulateIE9" />
<title>La Repubblica.it - Homepage</title>
Frame (408 bytes) Reassembled TCP (48534 bytes) Uncompressed entity body (223316 bytes)
Line-based text data (data-text-lines), 223316 b... Packets: 3688 Displayed: 62 Marked: 0 Profile: Default

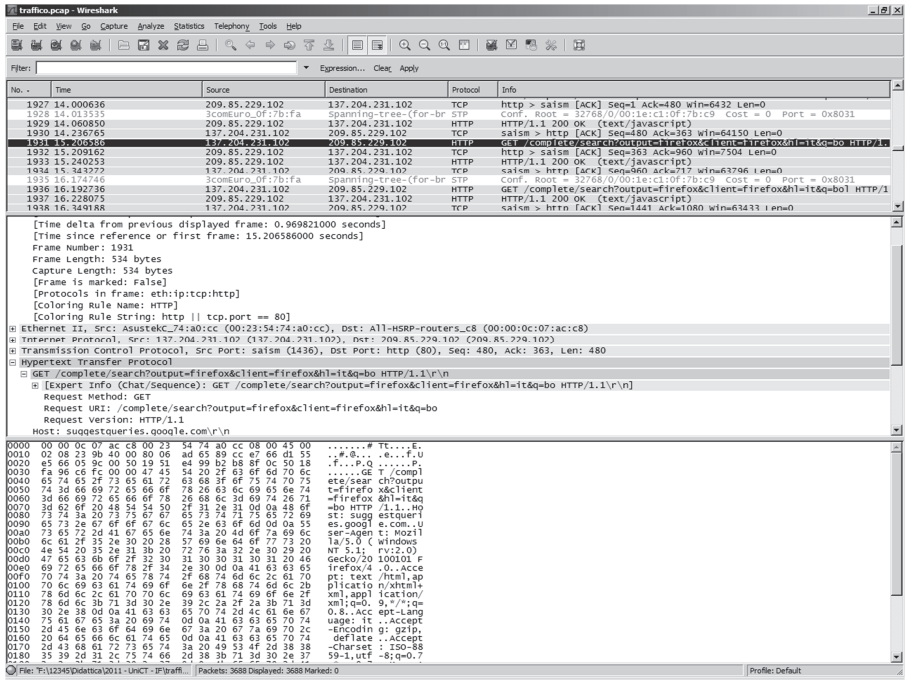

traffico.pcap - Wireshark
Expand Subtrees
Expand All
Collapse All
Apply as Filter
Prepare a Filter
Colorize with Filter
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Copy
Export Selected Packet Bytes...
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As...
Disable Protocol...
Resolve Name
Go to Corresponding Packet

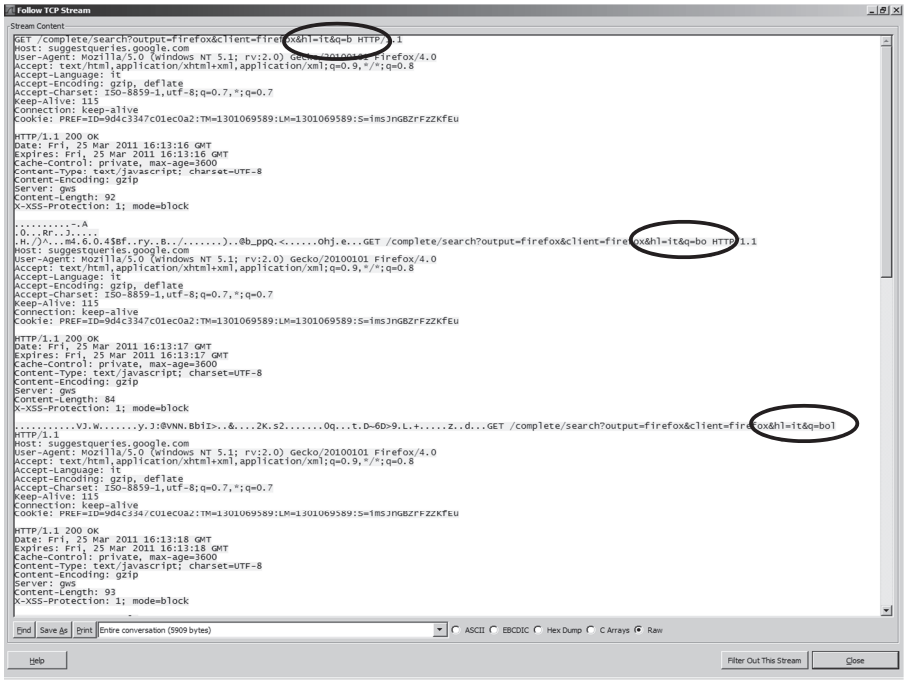

Wireshark: Export Raw Data
Salva in: Nuova cartella
la-repubblica-logo-home-payoff.png
traffico.jpg
Documenti recenti
Desktop
Documenti
Risorse del computer
Risorse di rete
Nome file: index.html
Salva come: All Files (*.*)
Salva
Annulla
223316 bytes of raw binary data will be written

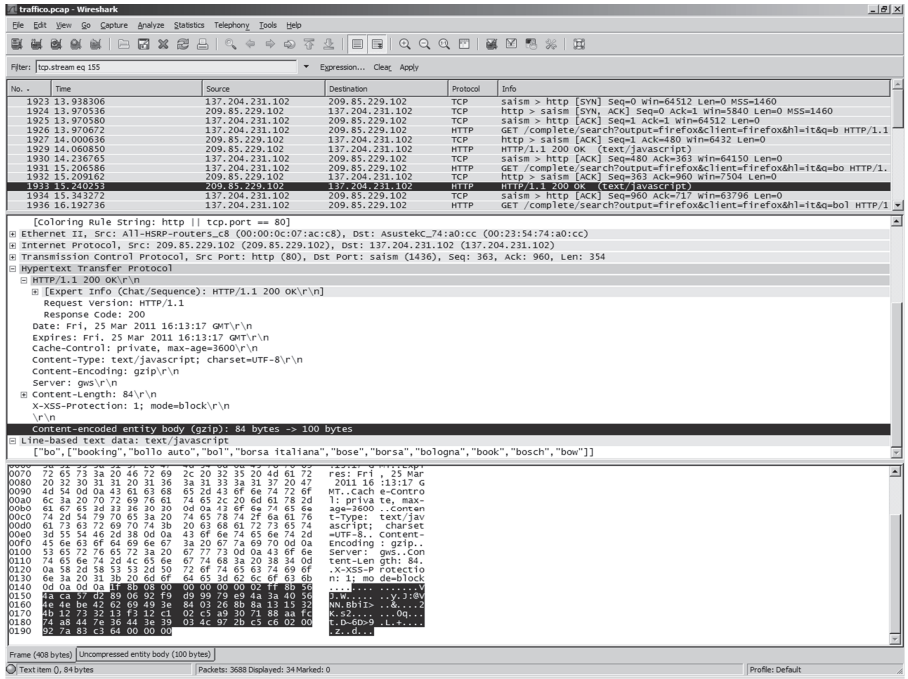

F:\Nuova cartella\index.html - Notepad++
File Modifica Cerca Visualizza Formato Linguaggio Configurazione Macro Esegui TextFX Plugins Finestra ?
index.html
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7; IE=EmulateIE9" />
<title>La Repubblica.it - Homepage</title>
<meta name="keywords" content="La Repubblica, notizie internazionale, giornaliere, nazionale, politics, scienze, business, affari, finanza, sport,
<meta name="description" content="Repubblica.it: il quotidiano online con tutte le notizie in tempo reale. News e ultime notizie. Tutti i settori: p
<link rel="alternate" type="application/rss+xml" title="Homepage - La Repubblica.it" href="http://www.repubblica.it/rss/homepage/rss2.0.xml" />
<meta name="msapplication-task" content="name=Economia;action-uri=http://www.repubblica.it/economia/;icon-uri=http://www.repubblica.it/static/images/
<meta property="fb:admins" content="100000390369341"/>
<meta name="msapplication-starturl" content="http://www.repubblica.it/" />
<meta name="msapplication-tooltip" content="Naviga sul sito de La Repubblica.it" />
<meta name="msapplication-window" content="width=1024;height=768" />
<link rel="image_src" href="http://www.repubblica.it/images/homepage/la_repubblica_logo.gif" />
<link rel="canonical" href="http://www.repubblica.it/" />
<link rel="apple-touch-icon" href="http://www.repubblica.it/images/homepage/apple-touch-icon.png" />
<meta property="fb:app_id" content="124998494210426"/>
<link rel="search" type="application/opensearchdescription+xml" href="http://www.repubblica.it/statickpm3/common/xml/opensearch_desc.xml" title="Cerc
<meta name="verify-v1" content="eyc9DUeswG1mlkZxy+Fza8G3PnN8F/q/2vZfVWdJKxU=" />
<meta name="application-name" content="Repubblica.it" />
<link rel="alternate" media="handheld" href="http://m.repubblica.it/" />
<meta http-equiv="Refresh" content="300;URL=index.html?refresh_ce" />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
<link rel="shortcut icon" type="image/x-icon" href="http://www.repubblica.it/static/images/homepage/2010/favicon.ico">
<link rel="stylesheet" href="http://www.repubblica.it/static/css/homepage/2010/homepage.css" type="text/css" media="all" />
<script type="text/javascript" src="http://www.repubblica.it/static/js/common/jquery.min.js"></script>
<script type="text/javascript" src="http://www.repubblica.it/static/js/homepage/2010/homepage.js"></script>
<!-- Da scommentare per treno dei commenti
<script type="text/javascript" src="/javascript/swfobject.js"></script-->
<script type="text/javascript" src="http://adagiojs.repubblica.it/uploads/js/repubblicaad.js"></script>
<script type="text/javascript" src="http://oasjs.kataweb.it/adsetup.js?hprep"></script>
<script type="text/javascript">
Ln : 1 Col : 1 Sel : 0 | 0 Dos\Windows ANSI INS

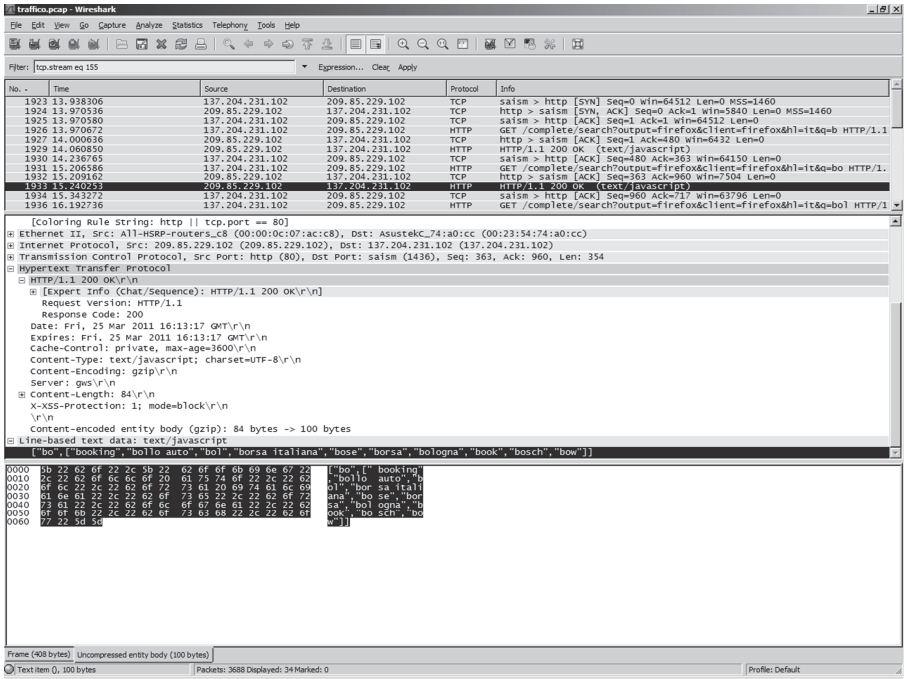

La Repubblica.it - Homepage
file:///F:/Nuova%20cartella/index.html
Quotidiano digitale
Mobile
Facebook
Venerdì 25 marzo 2011 – Aggiornato alle 17.11
l'Espresso
Network
Quotidiani locali
Alto Adige
Corriere delle Alpi
Gazzetta di Mantova
Gazzetta di Modena
Gazzetta di Reggio
Il Centro
Il mattino di Padova
Il Piccolo
Il Tirreno
Il Fò
Il Trentino
La Città di Salerno
La Nuova Ferrara
La Nuova Sardegna
La Nuova Venezia
La Provincia Pavese
La Sentinella del Canavese
La Tribuna di Treviso
Messaggero Veneto
Il Bò
Periodici
l'Espresso
Espresso - Food and Wine
Le Scienze
National Geographic
Micromega
Chiesa.it
Limes
Radio
Capital


La Repubblica.it - Homepage
file:///F:/Nuova%20cartella/index.html
la Repubblica | Mobile | Facebook
Venerdì 25 marzo 2011 – Aggiornato alle 17.11
l'Espresso | Network
EDIZIONI LOCALI: BARI - BOLOGNA - FIRENZE - GENOVA - MILANO - NAPOLI - PALERMO - PARMA - ROMA - TORINO
Cerca
Home | Pubblico | Affari&Finanza | Sport | Spettacoli&Cultura | Motori | Viaggi | Moda | Casa | Salute | Meteo | Lavoro | Annunci
Repubblica TV | Cronaca | Esteri | Scienze | Tecnologia | Ambiente | Scuola&Giovani | Repubblica@Scuola | Mondo Solidale | Ora per Ora | Foto
Libia, nuovo duello tra Italia e Francia
Frattini a Sarkozy: "Anche noi abbiamo idee"
Diario Tripoli: "Messinscena del regime" - Tv
DIRETTA. Accordo a Bruxelles, all'Alleanza guida dell'intera missione. Frattini: "Operativo da lunedì". Berlusconi soddisfatto (video). Parigi: Con Londra lavoriamo a soluzione politica. La secca risposta della Farnesina. Assedio a Misurata (video), i ribelli denunciano: "Massacro di civili" dall'inviato VINCENZO NICRO
Onu, nasce l'asse dei "Bric" di F. RAMPINI
La dietrologia dell'assurdo
Cinema | Società | Il caso
Metti un figlio e un padre asceta sotto un albero
Dall'ultimo libro di Tiziano Terzani, scrittore-mito, un film con Bruno Ganz ed Elio Germano (foto). Il "vero" figlio: "Mio padre era un pellegrino a pagamento" di C. MORGOCLIONE Interviste
Anche la Siria in fiamme, 20 morti
Decine arresti a Damasco - Video
Oltre 50 feriti in scontri in Giordania
Marcia per portare sostegno alla città assediata di Dara. Manifestazioni anti-regime anche nella capitale, a Homs e Qamishli: la polizia spara. Abbattute statue di Assad che ieri aveva annunciato riforme. Yemen, fallite le trattative con i ribelli
Parmalat, su scalata Lactalis la procura apre un'inchiesta
parmalat
I pm di Milano indagano sull'acquisizione da parte del gruppo transalpino delle quote detenute dai fondi esteri. Alla vigilia del decreto del governo frena-Opa, i francesi avevano rastrellato il 29% delle azioni dell'azienda italiana. L'ad Bondi (nella foto) sentito come teste
TABLET MANIA
Video L'iPad2 sbarca in Italia
c'è chi ha fatto 24 ore di fila
FOTO L'attesa a Milano
Ecco la nostra prova
TVZAP
Avanzi, venti anni fa satira che non invecchia
TUTTI I TORMENTONI
TVZAP Avanzi , venti anni fa satira che non invecchia TUTTI I TORMENTONI
"Il premier non ha cantato" smentita sul sito del governo
L'INTERATTIVO
Domani sera l'ora legale lancette avanti di 60 minuti
IL CONCORSO
World Press Photo
OGGI IN PUBBLICO
LA SITUAZIONE
I magistrati vanno al contrattacco nel mirino il premier
Continua
I POTERI
POTERI INVISIBILI
Giustizia, l'allarme dei magistrati
"Leggi piegate a interessi di parte"
Durissima nota dei vertici dell'Anm. "Prescrizione breve incostituzionale, viola principio di uguaglianza". "Norma su responsabilità delle toghe assurda e disorganica, è un atto di aggressione". "Il vero disegno è colpire i giudici"
REPUBBLICA DOMANI
Perché il governo rimpiange Gheddafi

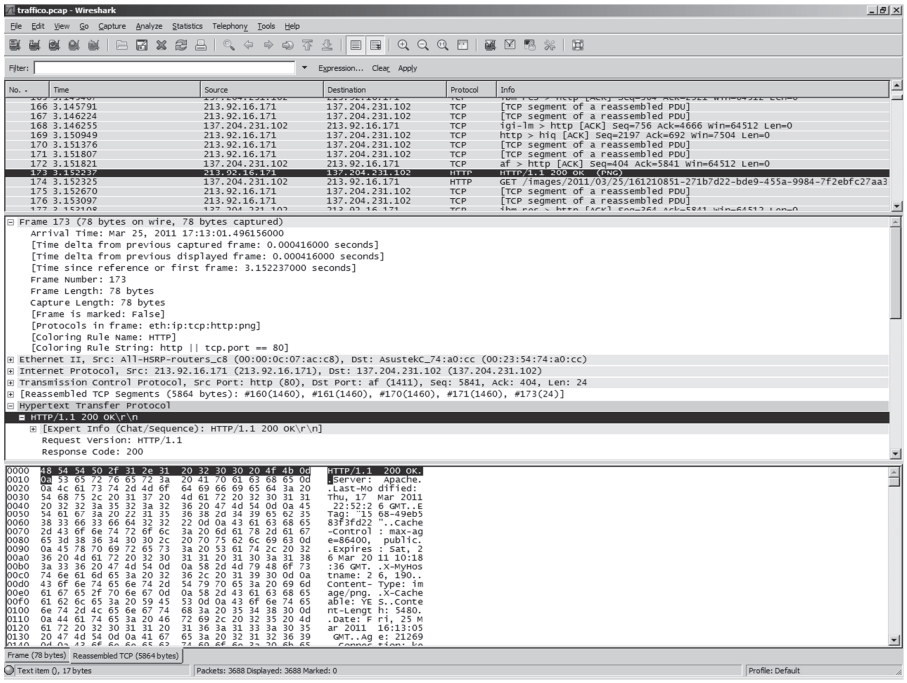

traffico.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
1927 14.000636 209.85.229.102 137.204.231.102 TCP http > saism [ACK] Seq=1 Ack=480 Win=6432 Len=0
1928 14.013535 3comEuro_0f:7b:fa Spanning-tree-(for-br STP Conf. Root = 32768/0/00:1e:c1:0f:7b:c9 Cost = 0 Port = 0x8031
1929 14.060850 209.85.229.102 137.204.231.102 HTTP HTTP/1.1 200 OK (text/javascript)
1930 14.236765 137.204.231.102 209.85.229.102 TCP saism > http [ACK] Seq=480 Ack=363 Win=64150 Len=0
1931 15.206586 137.204.231.102 209.85.229.102 HTTP GET /complete/search?output=firefox&client=firefox&hl=it&q=bo HTTP/1.
1932 15.209162 209.85.229.102 137.204.231.102 TCP http > saism [ACK] Seq=363 Ack=960 Win=7504 Len=0
1933 15.240253 209.85.229.102 137.204.231.102 HTTP HTTP/1.1 200 OK (text/javascript)
1934 15.343272 137.204.231.102 209.85.229.102 TCP saism > http [ACK] Seq=960 Ack=717 Win=63796 Len=0
1935 16.174746 3comEuro_0f:7b:fa Spanning-tree-(for-br STP Conf. Root = 32768/0/00:1e:c1:0f:7b:c9 Cost = 0 Port = 0x8031
1936 16.192726 137.204.231.102 209.85.229.102 HTTP GET /complete/search?output=firefox&client=firefox&hl=it&q=bol HTTP/1
1937 16.228075 209.85.229.102 137.204.231.102 HTTP HTTP/1.1 200 OK (text/javascript)
1938 16.349188 137.204.231.102 209.85.229.102 TCP saism > http [ACK] Seq=1441 Ack=1080 Win=63433 Len=0
[Time delta from previous displayed frame: 0.969821000 seconds]
[Time since reference or first frame: 15.206586000 seconds]
Frame Number: 1931
Frame Length: 534 bytes
Capture Length: 534 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:tcp:http]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80]
Ethernet II, Src: AsustekC_74:a0:cc (00:23:54:74:a0:cc), Dst: All-HSRP-routers_c8 (00:00:0c:07:ac:c8)
Internet Protocol, Src: 137.204.231.102 (137.204.231.102), Dst: 209.85.229.102 (209.85.229.102)
Transmission Control Protocol, Src Port: saism (1436), Dst Port: http (80), Seq: 480, Ack: 363, Len: 480
Hypertext Transfer Protocol
GET /complete/search?output=firefox&client=firefox&hl=it&q=bo HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /complete/search?output=firefox&client=firefox&hl=it&q=bo HTTP/1.1\r\n]
Request Method: GET
Request URI: /complete/search?output=firefox&client=firefox&hl=it&q=bo
Request Version: HTTP/1.1
Host: suggestqueries.google.com\r\n
0000 00 00 0c 07 ac c8 00 23 54 74 a0 cc 08 00 45 00 ....# Tt....E.
0010 02 08 23 9b 40 00 80 06 ad 65 89 cc e7 66 d1 55 ..#.@.... .e...f.U
0020 e5 66 05 9c 00 50 19 51 e4 99 b2 b8 8f 0c 50 18 .f...P.Q ......P.
0030 fa 96 c6 fc 00 00 47 45 54 20 2f 63 6f 6d 70 6c ......GE T /compl
0040 65 74 65 2f 73 65 61 72 63 68 3f 6f 75 74 70 75 ete/sear ch?outpu
0050 74 3d 66 69 72 65 66 6f 78 26 63 6c 69 65 6e 74 t=firefo x&client
0060 3d 66 69 72 65 66 6f 78 26 68 6c 3d 69 74 26 71 =firefox &hl=it&q
0070 3d 62 6f 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f =bo HTTP /1.1..Ho
0080 73 74 3a 20 73 75 67 67 65 73 74 71 75 65 72 69 st: sugg estqueri
0090 65 73 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 0d 0a 55 es.googl e.com..U
00a0 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c ser-Agen t: Mozil
00b0 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 la/5.0 (Windows
00c0 4e 54 20 35 2e 31 3b 20 72 76 3a 32 2e 30 29 20 NT 5.1; rv:2.0)
00d0 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 Gecko/20 100101 F
00e0 69 72 65 66 6f 78 2f 34 2e 30 0d 0a 41 63 63 65 irefox/4 .0..Acce
00f0 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 pt: text /html,ap
0100 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b plicatio n/xhtml+
0110 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f xml,appl ication/
0120 78 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f 2a 3b 71 3d xml;q=0. 9,*/*;q=
0130 30 2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 0.8..Acc ept-Lang
0140 75 61 67 65 3a 20 69 74 0d 0a 41 63 63 65 70 74 uage: it ..Accept
0150 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c -Encodin g: gzip,
0160 20 64 65 66 6c 61 74 65 0d 0a 41 63 63 65 70 74 deflate ..Accept
0170 2d 43 68 61 72 73 65 74 3a 20 49 53 4f 2d 38 38 -Charset : ISO-88
0180 35 39 2d 31 2c 75 74 66 2d 38 3b 71 3d 30 2e 37 59-1,utf -8;q=0.7
File: "F:\12345\Didattica\2011 - UniCT - IF\traffi... Packets: 3688 Displayed: 3688 Marked: 0 Profile: Default

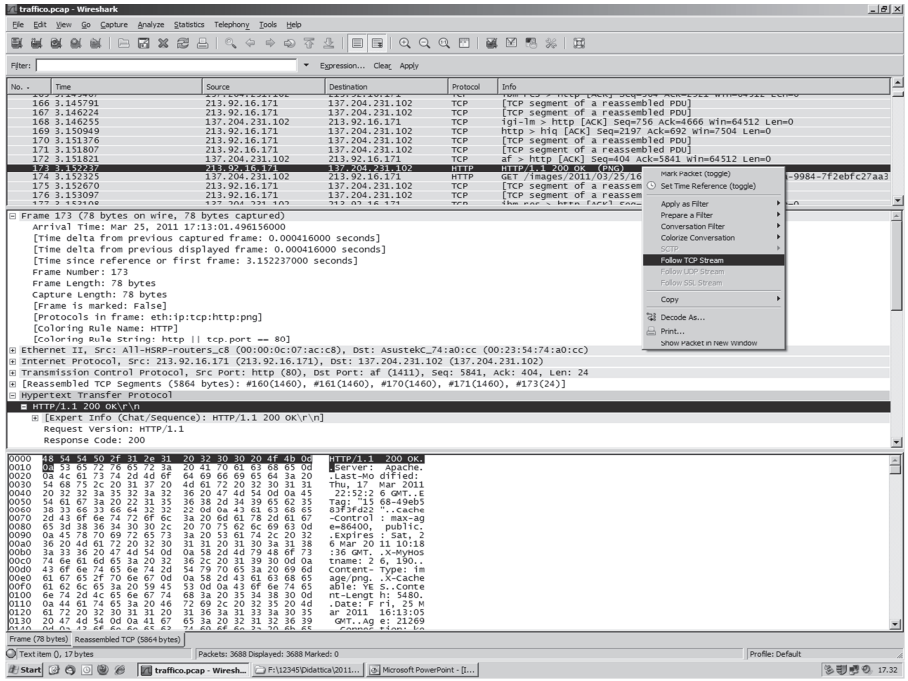

Follow TCP Stream
Stream Content
GET /complete/search?output=firefox&client=firefox&hl=it&q=b HTTP/1.1
Host: suggestqueries.google.com
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:2.0) Gecko/20100101 Firefox/4.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: it
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Cookie: PREF=ID=9d4c3347c01ec0a2:TM=1301069589:LM=1301069589:S=imsJnGBZrFzZKfEu
HTTP/1.1 200 OK
Date: Fri, 25 Mar 2011 16:13:16 GMT
Expires: Fri, 25 Mar 2011 16:13:16 GMT
Cache-Control: private, max-age=3600
Content-Type: text/javascript; charset=UTF-8
Content-Encoding: gzip
Server: gws
Content-Length: 92
X-XSS-Protection: 1; mode=block
.....-.A
.0...Rr..J.....
.H./)^...m4.6.0.4$bf..ry..B../.......)..@b_ppQ.<.....Ohj.e...GET /complete/search?output=firefox&client=firefox&hl=it&q=bo HTTP/1.1
Host: suggestqueries.google.com
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:2.0) Gecko/20100101 Firefox/4.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: it
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Cookie: PREF=ID=9d4c3347c01ec0a2:TM=1301069589:LM=1301069589:S=imsJnGBZrFzZKfEu
HTTP/1.1 200 OK
Date: Fri, 25 Mar 2011 16:13:17 GMT
Expires: Fri, 25 Mar 2011 16:13:17 GMT
Cache-Control: private, max-age=3600
Content-Type: text/javascript; charset=UTF-8
Content-Encoding: gzip
Server: gws
Content-Length: 84
X-XSS-Protection: 1; mode=block
.....VJ.W.....y.J:0VNN.BbiI>..&....2K.s2.....0q...t.D~6D>9.L.+.....z..d...GET /complete/search?output=firefox&client=firefox&hl=it&q=bol
HTTP/1.1
Host: suggestqueries.google.com
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:2.0) Gecko/20100101 Firefox/4.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: it
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Cookie: PREF=ID=9d4c3347c01ec0a2:TM=1301069589:LM=1301069589:S=imsJnGBZrFzZKfEu
HTTP/1.1 200 OK
Date: Fri, 25 Mar 2011 16:13:18 GMT
Expires: Fri, 25 Mar 2011 16:13:18 GMT
Cache-Control: private, max-age=3600
Content-Type: text/javascript; charset=UTF-8
Content-Encoding: gzip
Server: gws
Content-Length: 93
X-XSS-Protection: 1; mode=block
Find Save As Print Entire conversation (5909 bytes) ASCII EBCDIC Hex Dump C Arrays Raw
Help
Filter Out This Stream
Close

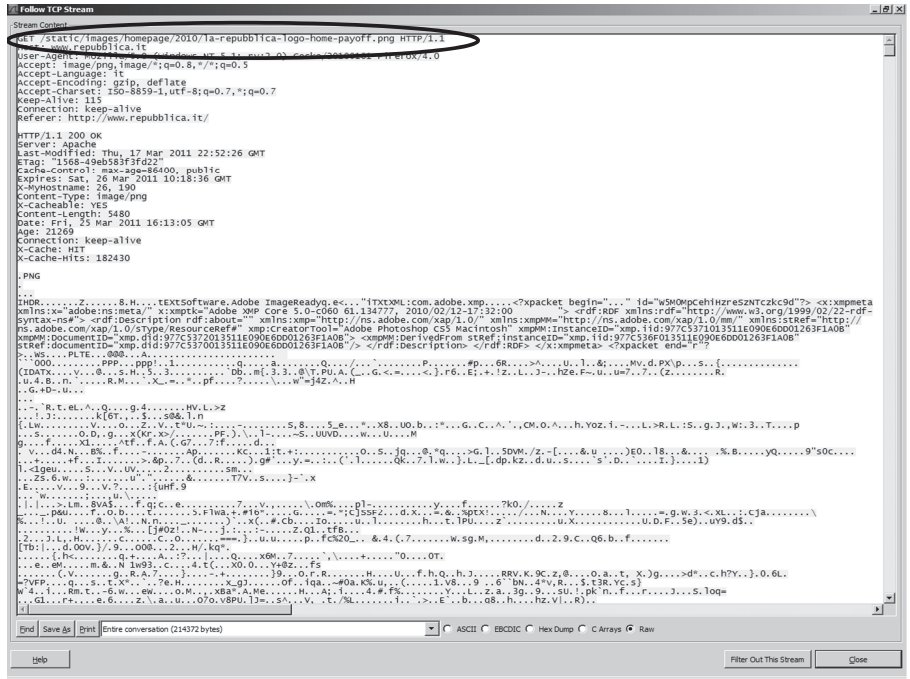


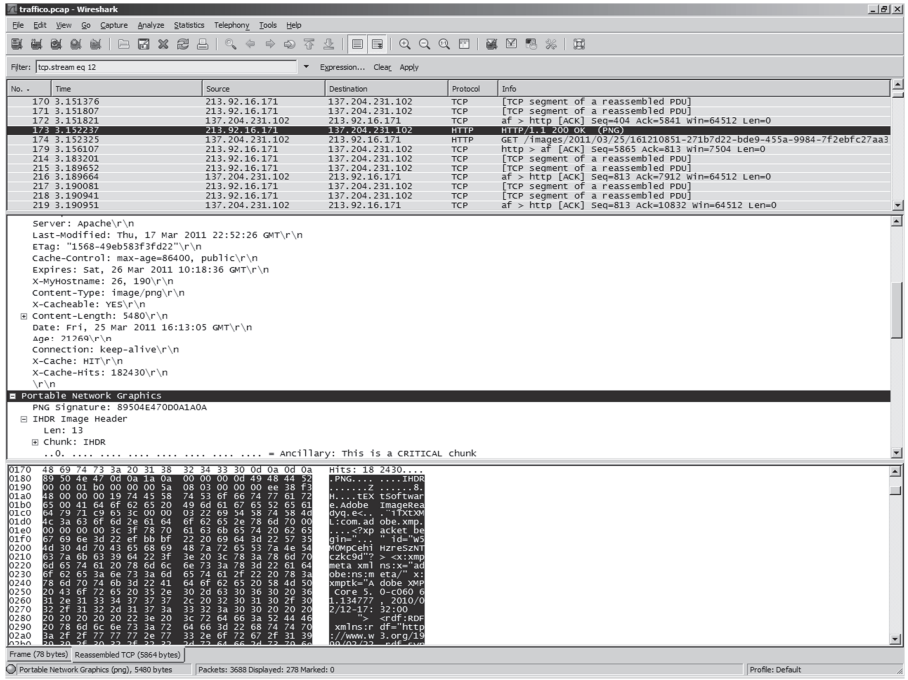


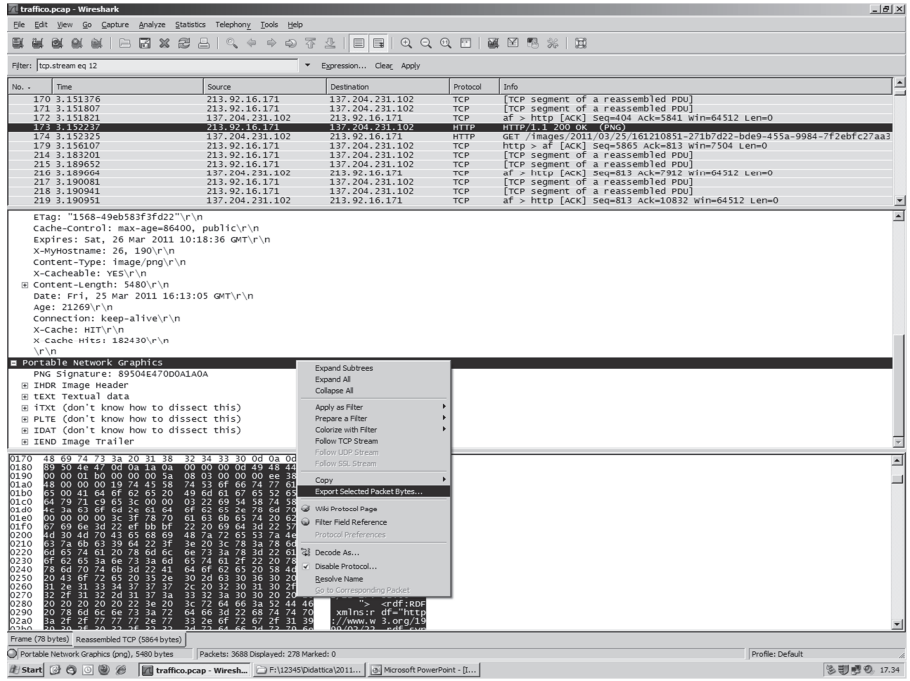
Estrazione di dati dall'intercettazione

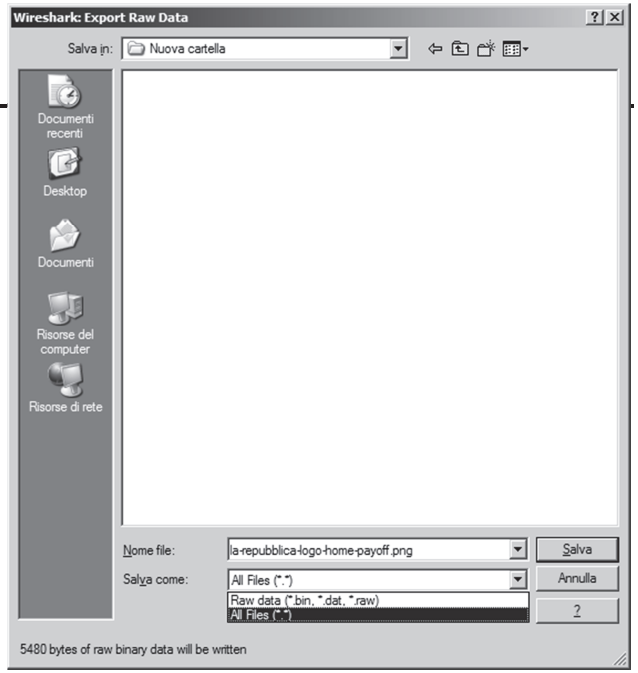



traffico.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply
No. - Time Source Destination Protocol Info
166 3.145791 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
167 3.146224 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
168 3.146255 137.204.231.102 213.92.16.171 TCP igi-lm > http [ACK] Seq=756 Ack=4666 Win=64512 Len=0
169 3.150949 213.92.16.171 137.204.231.102 TCP http > hlq [ACK] Seq=2197 Ack=692 Win=7504 Len=0
170 3.151376 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
171 3.151807 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
172 3.151821 137.204.231.102 213.92.16.171 TCP af > http [ACK] Seq=404 Ack=5841 Win=64512 Len=0
173 3.152237 213.92.16.171 137.204.231.102 HTTP HTTP/1.1 200 OK (PNG)
174 3.152325 137.204.231.102 213.92.16.171 HTTP GET /images/2011/03/25/16 -9984-7f2ebfc27aa3
175 3.156107 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassem
176 3.153097 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassem
Mark Packet (toggle)
Set Time Reference (toggle)
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Copy
Decode As...
Print...
Show Packet in New Window
Frame 173 (78 bytes on wire, 78 bytes captured)
Arrival Time: Mar 25, 2011 17:13:01.496156000
[Time delta from previous captured frame: 0.000416000 seconds]
[Time delta from previous displayed frame: 0.000416000 seconds]
[Time since reference or first frame: 3.152237000 seconds]
Frame Number: 173
Frame Length: 78 bytes
Capture Length: 78 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:tcp:http:png]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80]
Ethernet II, Src: All-HSRP-routers_c8 (00:00:0c:07:ac:c8), Dst: AsustekC_74:a0:cc (00:23:54:74:a0:cc)
Internet Protocol, Src: 213.92.16.171 (213.92.16.171), Dst: 137.204.231.102 (137.204.231.102)
Transmission Control Protocol, Src Port: http (80), Dst Port: af (1411), Seq: 5841, Ack: 404, Len: 24
[Reassembled TCP Segments (5864 bytes): #160(1460), #161(1460), #170(1460), #171(1460), #173(24)]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
Request Version: HTTP/1.1
Response Code: 200
0000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK.
0010 0a 53 65 72 76 65 72 3a 20 41 70 61 63 68 65 0d .Server: Apache.
0020 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64 3a 20 .Last-Mo dified:
0030 54 68 75 2c 20 31 37 20 4d 61 72 20 32 30 31 31 Thu, 17 Mar 2011
0040 20 32 32 3a 35 32 3a 32 36 20 47 4d 54 0d 0a 45 22:52:2 6 GMT..E
0050 54 61 67 3a 20 22 31 35 36 38 2d 34 39 65 62 35 Tag: "15 68-49eb5
0060 38 33 66 33 66 64 32 32 22 0d 0a 43 61 63 68 65 83f3fd22 "..Cache
0070 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 67 -Control : max-ag
0080 65 3d 38 36 34 30 30 2c 20 70 75 62 6c 69 63 0d e=86400, public.
0090 0a 45 78 70 69 72 65 73 3a 20 53 61 74 2c 20 32 .Expires : Sat, 2
00a0 36 20 4d 61 72 20 32 30 31 31 20 31 30 3a 31 38 6 Mar 20 11 10:18
00b0 3a 33 36 20 47 4d 54 0d 0a 58 2d 4d 79 48 6f 73 :36 GMT. .X-MyHos
00c0 74 6e 61 6d 65 3a 20 32 36 2c 20 31 39 30 0d 0a tname: 2 6, 190..
00d0 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 69 6d Content- Type: im
00e0 61 67 65 2f 70 6e 67 0d 0a 58 2d 43 61 63 68 65 age/png. .X-Cache
00f0 61 62 6c 65 3a 20 59 45 53 0d 0a 43 6f 6e 74 65 able: YE S..Conte
0100 6e 74 2d 4c 65 6e 67 74 68 3a 20 35 34 38 30 0d nt-Leng th: 5480.
0110 0a 44 61 74 65 3a 20 46 72 69 2c 20 32 35 20 4d .Date: F ri, 25 M
0120 61 72 20 32 30 31 31 20 31 36 3a 31 33 3a 30 35 ar 2011 16:13:05
0130 20 47 4d 54 0d 0a 41 67 65 3a 20 32 31 32 36 39 GMT..Ag e: 21269
0140 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 ..Connec tion: ke
Frame (78 bytes) Reassembled TCP (5864 bytes)
Text item (), 17 bytes
Packets: 3688 Displayed: 3688 Marked: 0
Profile: Default
Start
traffico.pcap - Wiresh...
F:\12345\Didattica\2011...
Microsoft PowerPoint - [...
17.32

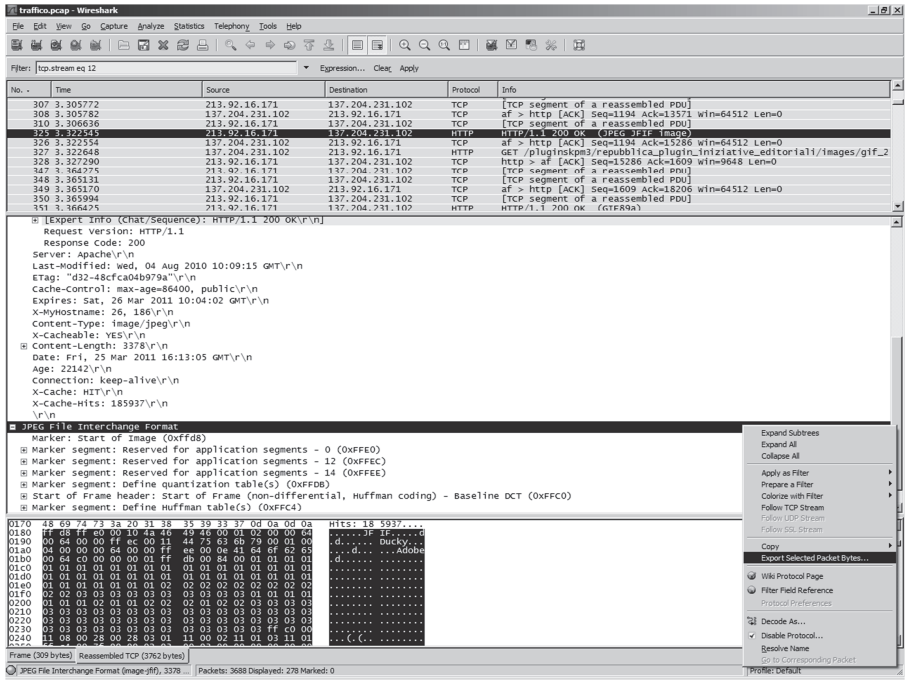

Follow TCP Stream
Stream Content
GET /static/images/homepage/2010/la-repubblica-logo-home-payoff.png HTTP/1.1
Host: www.repubblica.it
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:2.0) Gecko/20100101 Firefox/4.0
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: it
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Referer: http://www.repubblica.it/
HTTP/1.1 200 OK
Server: Apache
Last-Modified: Thu, 17 Mar 2011 22:52:26 GMT
ETag: "1568-49eb583f3fd22"
Cache-Control: max-age=86400, public
Expires: Sat, 26 Mar 2011 10:18:36 GMT
X-MyHostname: 26, 190
Content-Type: image/png
X-Cacheable: YES
Content-Length: 5480
Date: Fri, 25 Mar 2011 16:13:05 GMT
Age: 21269
Connection: keep-alive
X-Cache: HIT
X-Cache-Hits: 182430
.PNG
IHDR
iTXtSoftware
Find
Save As
Print
Entire conversation (214372 bytes)
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close

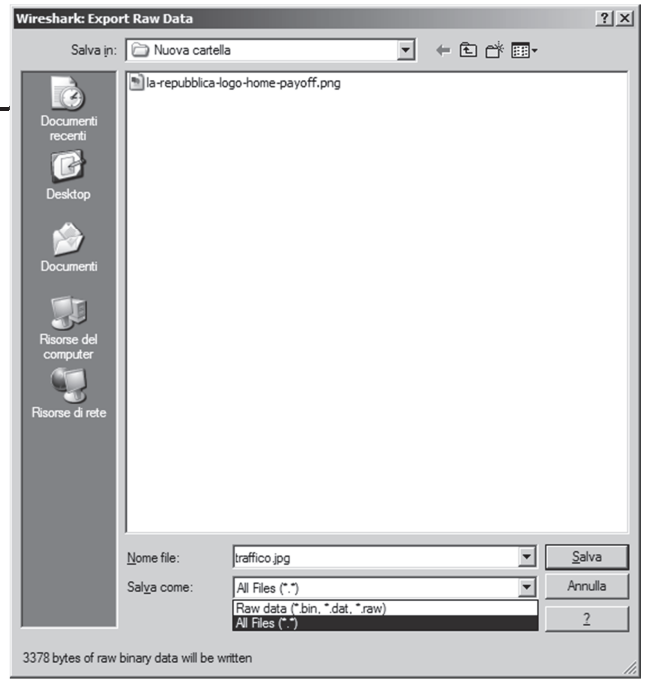

traffico.pcap - Wireshark
Filter: tcp.stream eq 12
No. - Time Source Destination Protocol Info
170 3.151376 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
171 3.151807 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
172 3.151821 137.204.231.102 213.92.16.171 TCP af > http [ACK] Seq=404 Ack=5841 Win=64512 Len=0
173 3.152237 213.92.16.171 137.204.231.102 HTTP HTTP/1.1 200 OK (PNG)
174 3.152325 137.204.231.102 213.92.16.171 HTTP GET /images/2011/03/25/161210851-271b7d22-bde9-455a-9984-7f2ebfc27aa3
179 3.156107 213.92.16.171 137.204.231.102 TCP http > af [ACK] Seq=5865 Ack=813 Win=7504 Len=0
214 3.183201 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
215 3.189652 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
216 3.189664 137.204.231.102 213.92.16.171 TCP af > http [ACK] Seq=813 Ack=7912 Win=64512 Len=0
217 3.190081 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
218 3.190941 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
219 3.190951 137.204.231.102 213.92.16.171 TCP af > http [ACK] Seq=813 Ack=10832 Win=64512 Len=0
Server: Apache\r\n
Last-Modified: Thu, 17 Mar 2011 22:52:26 GMT\r\n
ETag: "1568-49eb583f3fd22"\r\n
Cache-Control: max-age=86400, public\r\n
Expires: Sat, 26 Mar 2011 10:18:36 GMT\r\n
X-MyHostname: 26, 190\r\n
Content-Type: image/png\r\n
X-Cacheable: YES\r\n
Content-Length: 5480\r\n
Date: Fri, 25 Mar 2011 16:13:05 GMT\r\n
Age: 21269\r\n
Connection: keep-alive\r\n
X-Cache: HIT\r\n
X-Cache-Hits: 182430\r\n
\r\n
Portable Network Graphics
PNG Signature: 89504E470D0A1A0A
IHDR Image Header
Len: 13
Chunk: IHDR
..0. .... = Ancillary: This is a CRITICAL chunk
0170 48 69 74 73 3a 20 31 38 32 34 33 30 0d 0a 0d 0a Hits: 18 2430....
0180 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 .PNG.... ....IHDR
0190 00 00 01 b0 00 00 00 5a 08 03 00 00 00 ee 38 f3 ....Z ......8.
01a0 48 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 H....tEX tSoftwar
01b0 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 e.Adobe ImageRea
01c0 64 79 71 c9 65 3c 00 00 03 22 69 54 58 74 58 4d dyq.e<.. ."iTXtXM
01d0 4c 3a 63 6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00 L:com.ad obe.xmp.
01e0 00 00 00 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 ....<?xp acket be
01f0 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 gin="... " id="W5
0200 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 M0MpCehi HzreSzNT
0210 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 czkc9d"? > <x:xmp
0220 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 meta xml ns:x="ad
0230 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a obe:ns:m eta/" x:
0240 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 xmptk="A dobe XMP
0250 20 43 6f 72 65 20 35 2e 30 2d 63 30 36 30 20 36 .Core 5. 0-c060 6
0260 31 2e 31 33 34 37 37 37 2c 20 32 30 31 30 2f 30 1.134777 , 2010/0
0270 32 2f 31 32 2d 31 37 3a 33 32 3a 30 30 20 20 20 2/12-17: 32:00
0280 20 20 20 20 20 20 22 3e 20 3c 72 64 66 3a 52 44 46 "> <rdf:RDF
0290 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 xmlns:r df="http
02a0 3a 2f 2f 77 77 77 2e 72 33 2e 6f 72 67 2f 31 39 ://www.w 3.org/19
Frame (78 bytes) Reassembled TCP (5864 bytes)
Portable Network Graphics (png), 5480 bytes
Packets: 3688 Displayed: 278 Marked: 0
Profile: Default

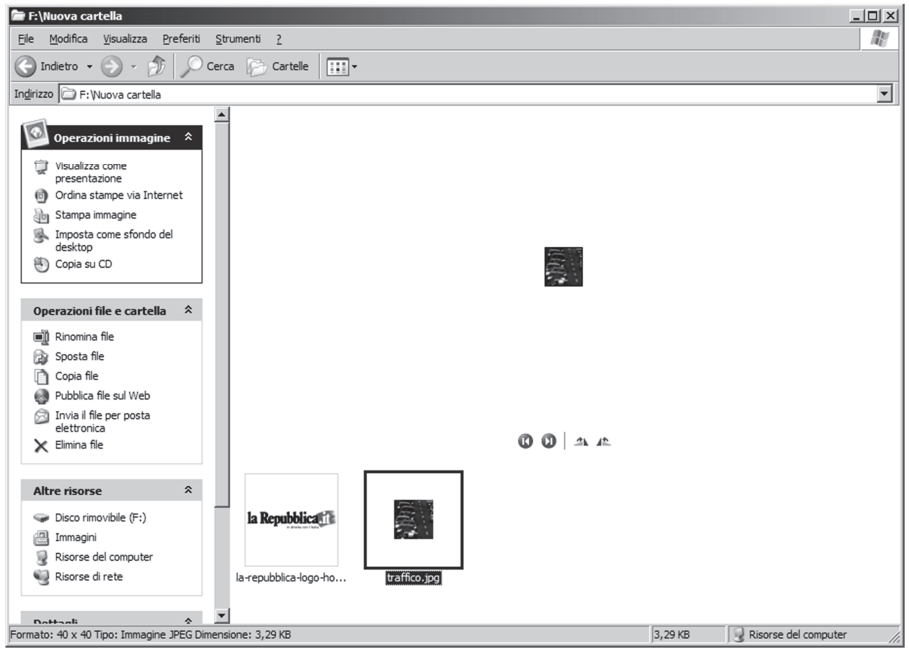

traffico.pcap - Wireshark
Filter: tcp.stream eq 12
No. - Time Source Destination Protocol Info
170 3.151376 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
171 3.151807 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
172 3.151821 137.204.231.102 213.92.16.171 TCP af > http [ACK] Seq=404 Ack=5841 Win=64512 Len=0
173 3.152237 213.92.16.171 137.204.231.102 HTTP HTTP/1.1 200 OK (PNG)
174 3.152325 137.204.231.102 213.92.16.171 HTTP GET /images/2011/03/25/161210851-271b7d22-bde9-455a-9984-7f2ebfc27aa3
179 3.156107 213.92.16.171 137.204.231.102 TCP http > af [ACK] Seq=5865 Ack=813 Win=7504 Len=0
214 3.183201 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
215 3.189652 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
216 3.189664 137.204.231.102 213.92.16.171 TCP af > http [ACK] Seq=813 Ack=7912 Win=64512 Len=0
217 3.190081 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
218 3.190941 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
219 3.190951 137.204.231.102 213.92.16.171 TCP af > http [ACK] Seq=813 Ack=10832 Win=64512 Len=0
ETag: "1568-49eb583f3fd22"\r\n
Cache-Control: max-age=86400, public\r\n
Expires: Sat, 26 Mar 2011 10:18:36 GMT\r\n
X-MyHostname: 26, 190\r\n
Content-Type: image/png\r\n
X-Cacheable: YES\r\n
Content-Length: 5480\r\n
Date: Fri, 25 Mar 2011 16:13:05 GMT\r\n
Age: 21269\r\n
Connection: keep-alive\r\n
X-Cache: HIT\r\n
X-Cache-Hits: 182430\r\n
\r\n
Portable Network Graphics
PNG Signature: 89504E470D0A1A0A
IHDR Image Header
tEXt Textual data
iTXt (don't know how to dissect this)
PLTE (don't know how to dissect this)
IDAT (don't know how to dissect this)
IEND Image Trailer
Expand Subtrees
Expand All
Collapse All
Apply as Filter
Prepare a Filter
Colorize with Filter
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Copy
Export Selected Packet Bytes...
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As...
Disable Protocol...
Resolve Name
Go To Corresponding Packet
0170 48 69 74 73 3a 20 31 38 32 34 33 30 0d 0a 0d 0a Hits: 18 2430....
0180 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 .PNG.... ....IHDR
0190 00 00 01 b0 00 00 00 5a 08 03 00 00 00 ee 38 f3 ....Z ......8.
01a0 48 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 H....tEX tSoftwar
01b0 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 e.Adobe ImageRea
01c0 64 79 71 c9 65 3c 00 00 03 22 69 54 58 74 58 4d dyq.e<.. ."iTXtXM
01d0 4c 3a 63 6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00 L:com.ad obe.xmp.
01e0 00 00 00 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 ....<?xp acket be
01f0 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 gin="... " id="W5
0200 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 M0MpCehi HzreSzNT
0210 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 czkc9d"? > <x:xmp
0220 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 meta xml ns:x="ad
0230 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a obe:ns:m eta/" x:
0240 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 xmptk="A dobe XMP
0250 20 43 6f 72 65 20 35 2e 30 2d 63 30 36 30 20 36 .Core 5. 0-c060 6
0260 31 2e 31 33 34 37 37 37 2c 20 32 30 31 30 2f 30 1.134777 , 2010/0
0270 32 2f 31 32 2d 31 37 3a 33 32 3a 30 30 20 20 20 2/12-17: 32:00
0280 20 20 20 20 20 20 22 3e 20 3c 72 64 66 3a 52 44 46 "> <rdf:RDF
0290 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 xmlns:r df="http
02a0 3a 2f 2f 77 77 77 2e 72 33 2e 6f 72 67 2f 31 39 ://www.w 3.org/19
Frame (78 bytes) Reassembled TCP (5864 bytes)
Portable Network Graphics (png), 5480 bytes
Packets: 3688 Displayed: 278 Marked: 0
Profile: Default


Wireshark: Export Raw Data
Salva in:
Nuova cartella
Documenti recenti
Desktop
Documenti
Risorse del computer
Risorse di rete
Nome file:
la-repubblica-logo-home-payoff.png
Salva
Salva come:
All Files (*.*)
Annulla
Raw data (*.bin, *.dat, *.raw)
All Files (*.*)
?
5480 bytes of raw binary data will be written

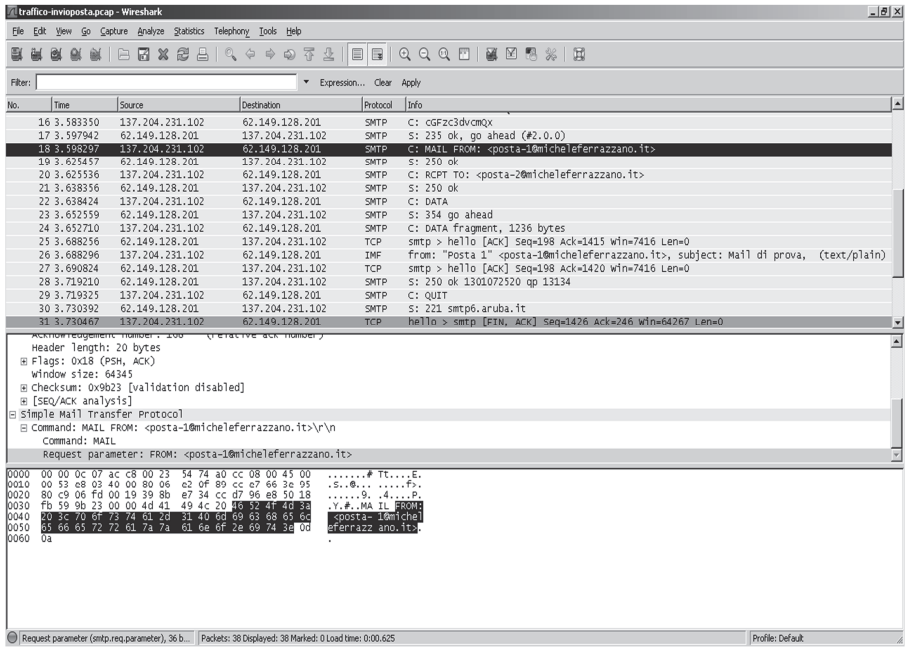

F:\Nuova cartella
File Modifica Visualizza Preferiti Strumenti ?
Indietro
Cerca
Cartelle
Indirizzo
F:\Nuova cartella
Operazioni immagine
Visualizza come presentazione
Ordina stampe via Internet
Stampa immagine
Imposta come sfondo del desktop
Copia su CD
Operazioni file e cartella
Rinomina file
Sposta file
Copia file
Pubblica file sul Web
Invia il file per posta elettronica
Elimina file
Altre risorse
Disco rimovibile (F:)
Immagini
Risorse del computer
Risorse di rete
la Repubblica.it
In diretta con l'Italia
la-repubblica-logo-home-payoff.png
Formato: 432 x 90 Tipo: Immagine PNG Dimensione: 5,35 KB
5,35 KB
Risorse del computer

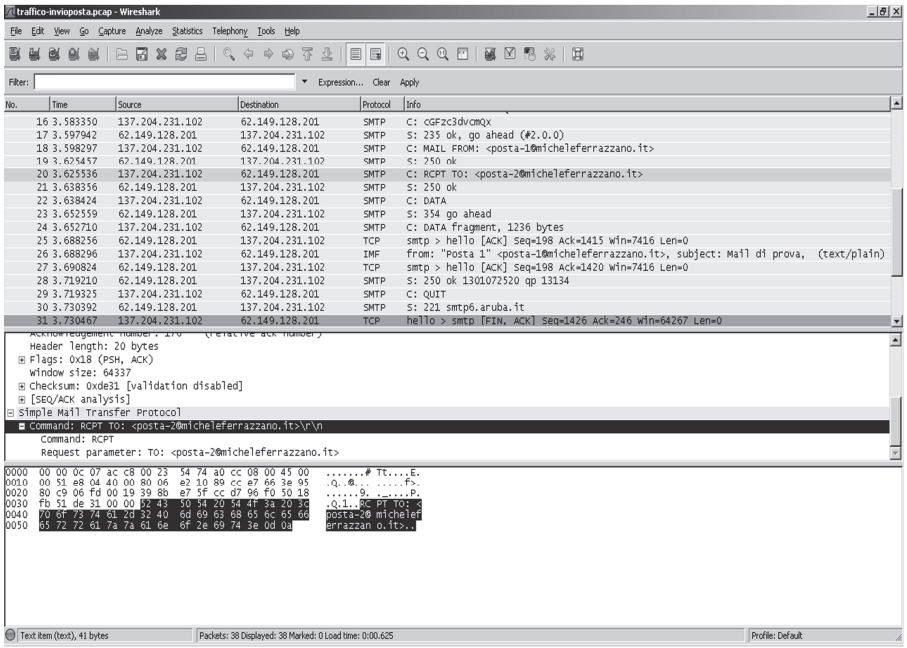

traffico.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: tcp.stream eq 12
Expression... Clear Apply
No. Time Source Destination Protocol Info
307 3.305772 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
308 3.305782 137.204.231.102 213.92.16.171 TCP af > http [ACK] Seq=1194 Ack=13571 Win=64512 Len=0
310 3.306636 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
325 3.322545 213.92.16.171 137.204.231.102 HTTP HTTP/1.1 200 OK (JPEG JFIF image)
326 3.322554 137.204.231.102 213.92.16.171 TCP af > http [ACK] Seq=1194 Ack=15286 Win=64512 Len=0
327 3.322648 137.204.231.102 213.92.16.171 HTTP GET /pluginskpm3/repubblica_plugin_iniziative_editoriali/images/gif_2
328 3.327290 213.92.16.171 137.204.231.102 TCP http > af [ACK] Seq=15286 Ack=1609 Win=9648 Len=0
347 3.364275 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
348 3.365131 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
349 3.365170 137.204.231.102 213.92.16.171 TCP af > http [ACK] Seq=1609 Ack=18206 Win=64512 Len=0
350 3.365994 213.92.16.171 137.204.231.102 TCP [TCP segment of a reassembled PDU]
351 3.366425 213.92.16.171 137.204.231.102 HTTP HTTP/1.1 200 OK (GIF89a)
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
Request Version: HTTP/1.1
Response Code: 200
Server: Apache\r\n
Last-Modified: Wed, 04 Aug 2010 10:09:15 GMT\r\n
ETag: "d32-48cfca04b979a"\r\n
Cache-Control: max-age=86400, public\r\n
Expires: Sat, 26 Mar 2011 10:04:02 GMT\r\n
X-MyHostname: 26, 186\r\n
Content-Type: image/jpeg\r\n
X-Cacheable: YES\r\n
Content-Length: 3378\r\n
Date: Fri, 25 Mar 2011 16:13:05 GMT\r\n
Age: 22142\r\n
Connection: keep-alive\r\n
X-Cache: HIT\r\n
X-Cache-Hits: 185937\r\n
\r\n
JPEG File Interchange Format
Marker: Start of Image (0xffd8)
Marker segment: Reserved for application segments - 0 (0xFFE0)
Marker segment: Reserved for application segments - 12 (0xFFEC)
Marker segment: Reserved for application segments - 14 (0xFFEE)
Marker segment: Define quantization table(s) (0xFFDB)
Start of Frame header: Start of Frame (non-differential, Huffman coding) - Baseline DCT (0xFFC0)
Marker segment: Define Huffman table(s) (0xFFC4)
Hits: 18 5937....
Expand Subtrees
Expand All
Collapse All
Apply as Filter
Prepare a Filter
Colorize with Filter
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Copy
Export Selected Packet Bytes...
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As...
Disable Protocol...
Resolve Name
Go to Corresponding Packet
Frame (309 bytes)
Reassembled TCP (3762 bytes)
JPEG File Interchange Format (image-jfif), 3378 ...
Packets: 3688 Displayed: 278 Marked: 0
Profile: Default

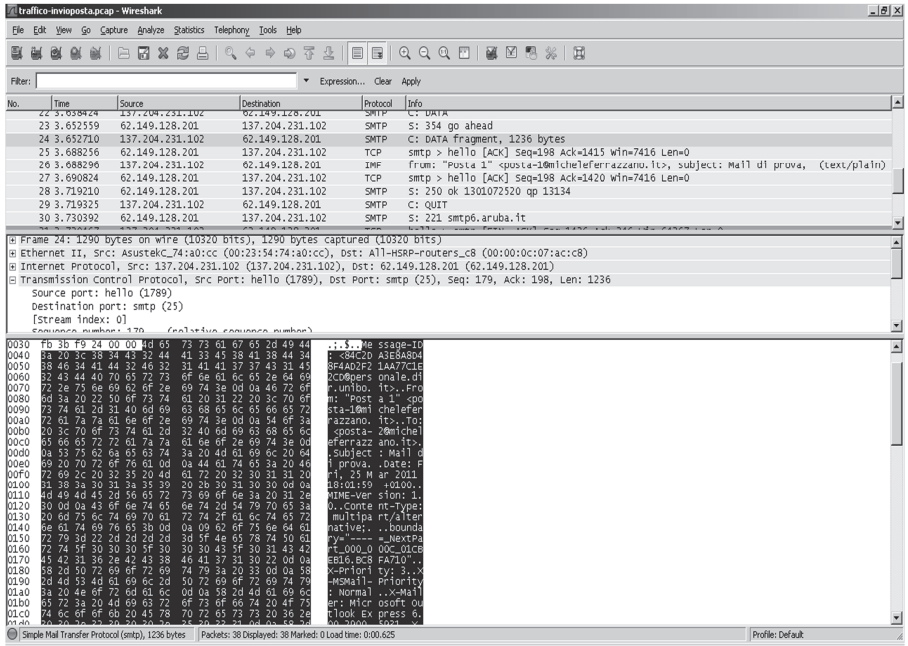

Wireshark: Export Raw Data
Salva in:
Nuova cartella
la-repubblica-logo-home-payoff.png
Documenti recenti
Desktop
Documenti
Risorse del computer
Risorse di rete
Nome file:
traffico.jpg
Salva
Salva come:
All Files (*.*)
Annulla
Raw data (*.bin, *.dat, *.raw)
All Files (*.*)
?
3378 bytes of raw binary data will be written

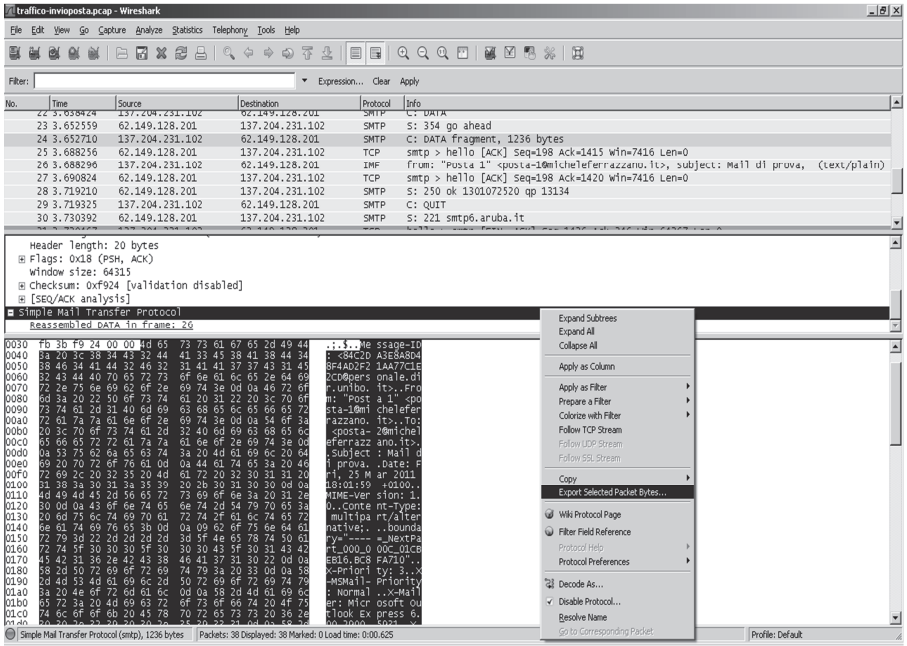


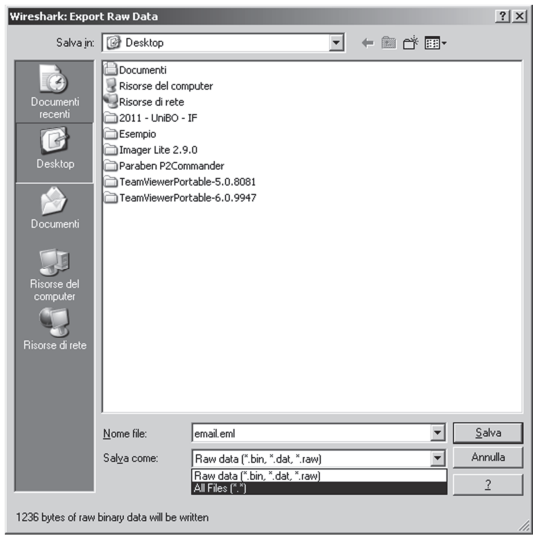
Invio di posta elettronica

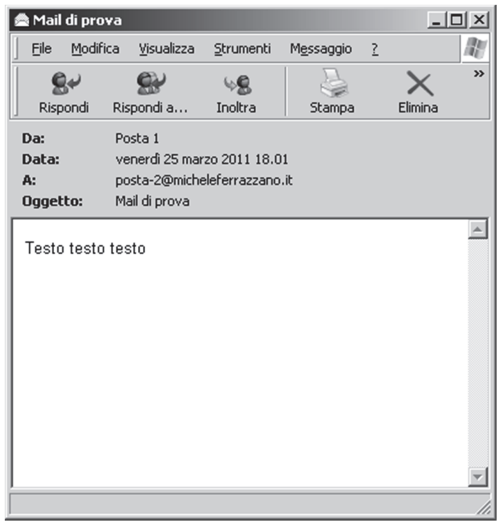




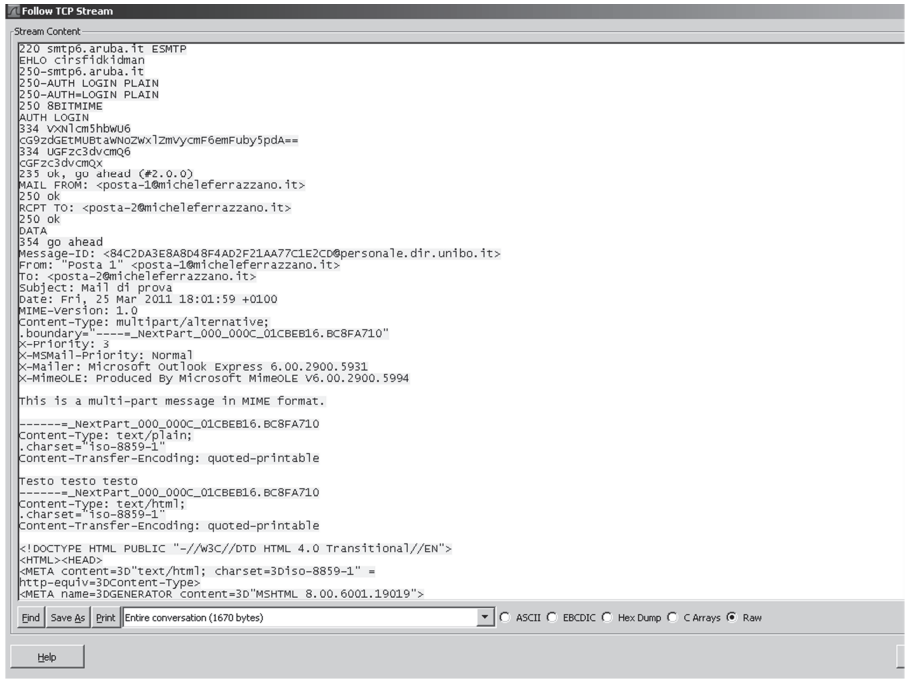

traffico-inviaposta.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
23 3.652559 62.149.128.201 137.204.231.102 SMTP S: 354 go ahead
24 3.652710 137.204.231.102 62.149.128.201 SMTP C: DATA fragment, 1236 bytes
25 3.688256 62.149.128.201 137.204.231.102 TCP smtp > hello [ACK] Seq=198 Ack=1415 Win=7416 Len=0
26 3.688296 137.204.231.102 62.149.128.201 IMF from: "Posta 1" <posta-1@micheleferrazzano.it>, subject: Mail di prova, (text/plain)
27 3.690824 62.149.128.201 137.204.231.102 TCP smtp > hello [ACK] Seq=198 Ack=1420 Win=7416 Len=0
28 3.719210 62.149.128.201 137.204.231.102 SMTP S: 250 ok 1301072520 qp 13134
29 3.719325 137.204.231.102 62.149.128.201 SMTP C: QUIT
30 3.730392 62.149.128.201 137.204.231.102 SMTP S: 221 smtp6.aruba.it
Frame 24: 1290 bytes on wire (10320 bits), 1290 bytes captured (10320 bits)
Ethernet II, Src: AsustekC_74:a0:cc (00:23:54:74:a0:cc), Dst: All-HSRP-routers_c8 (00:00:0c:07:ac:c8)
Internet Protocol, Src: 137.204.231.102 (137.204.231.102), Dst: 62.149.128.201 (62.149.128.201)
Transmission Control Protocol, Src Port: hello (1789), Dst Port: smtp (25), Seq: 179, Ack: 198, Len: 1236
Source port: hello (1789)
Destination port: smtp (25)
[Stream index: 0]
Simple Mail Transfer Protocol (smtp), 1236 bytes
Packets: 38 Displayed: 38 Marked: 0 Load time: 0:00.625
Profile: Default

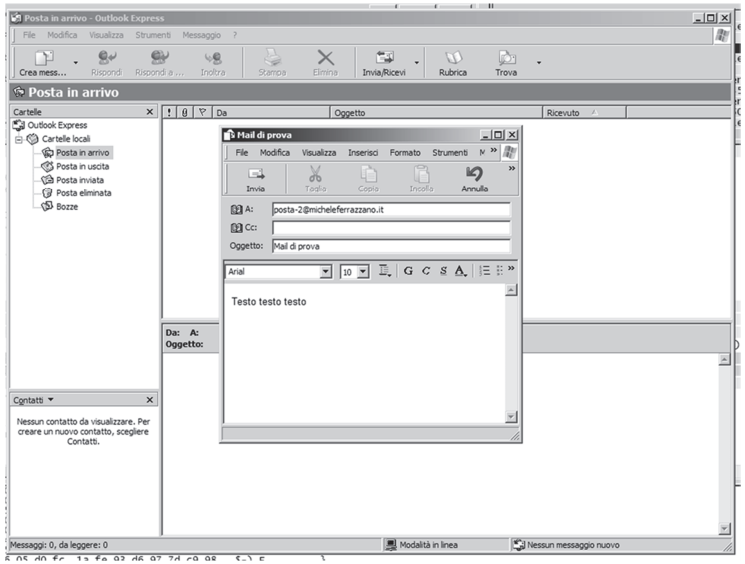

traffico-inviaposta.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
23 3.652559 62.149.128.201 137.204.231.102 SMTP S: 354 go ahead
24 3.652710 137.204.231.102 62.149.128.201 SMTP C: DATA fragment, 1236 bytes
25 3.688256 62.149.128.201 137.204.231.102 TCP smtp > hello [ACK] Seq=198 Ack=1415 Win=7416 Len=0
26 3.688296 137.204.231.102 62.149.128.201 IMF from: "Posta 1" <posta-1@micheleferrazzano.it>, subject: Mail di prova, (text/plain)
27 3.690824 62.149.128.201 137.204.231.102 TCP smtp > hello [ACK] Seq=198 Ack=1420 Win=7416 Len=0
28 3.719210 62.149.128.201 137.204.231.102 SMTP S: 250 ok 1301072520 qp 13134
29 3.719325 137.204.231.102 62.149.128.201 SMTP C: QUIT
30 3.730392 62.149.128.201 137.204.231.102 SMTP S: 221 smtp6.aruba.it
Header length: 20 bytes
Flags: 0x18 (PSH, ACK)
Window size: 64315
Checksum: 0xf924 [validation disabled]
[SEQ/ACK analysis]
Simple Mail Transfer Protocol
Reassembled DATA in frame: 26
Expand Subtrees
Expand All
Collapse All
Apply as Column
Apply as Filter
Prepare a Filter
Colorize with Filter
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Copy
Export Selected Packet Bytes...
Wiki Protocol Page
Filter Field Reference
Protocol Help
Protocol Preferences
Decode As...
Disable Protocol...
Resolve Name
Go to Corresponding Packet
Simple Mail Transfer Protocol (smtp), 1236 bytes
Packets: 38 Displayed: 38 Marked: 0 Load time: 0:00.625
Profile: Default

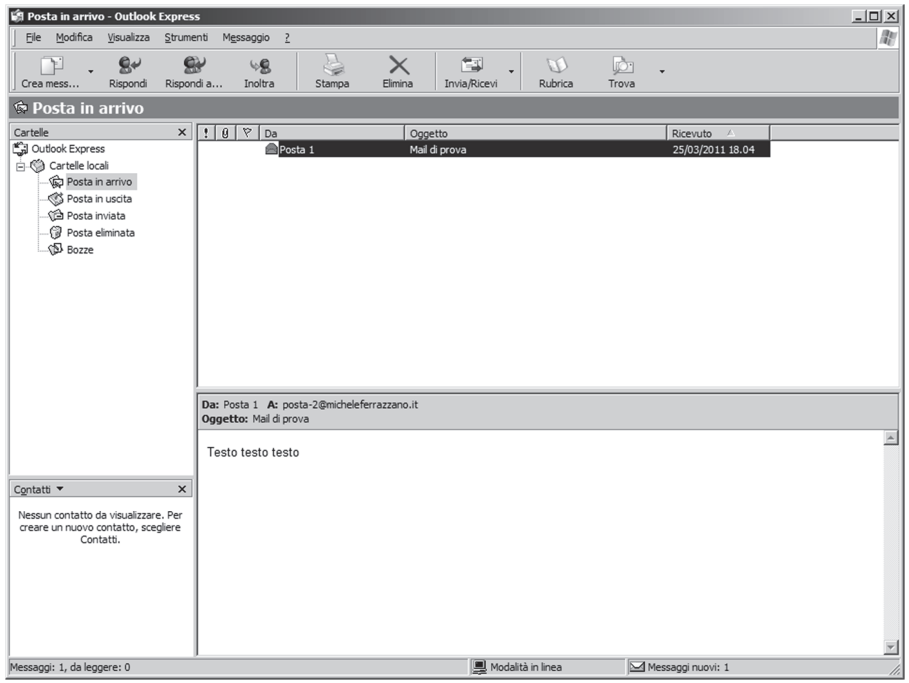

Wireshark: Export Raw Data
Salva in: Desktop
Documenti recenti
Desktop
Documenti
Risorse del computer
Risorse di rete
Documenti
Risorse del computer
Risorse di rete
2011 - UniBO - IF
Esempio
Imager Lite 2.9.0
Paraben P2Commander
TeamViewerPortable-5.0.8081
TeamViewerPortable-6.0.9947
Nome file: email.eml
Salva come: Raw data (*.bin, *.dat, *.raw)
Salva
Annulla
?
Raw data (*.bin, *.dat, *.raw)
All Files (*.*)
1236 bytes of raw binary data will be written

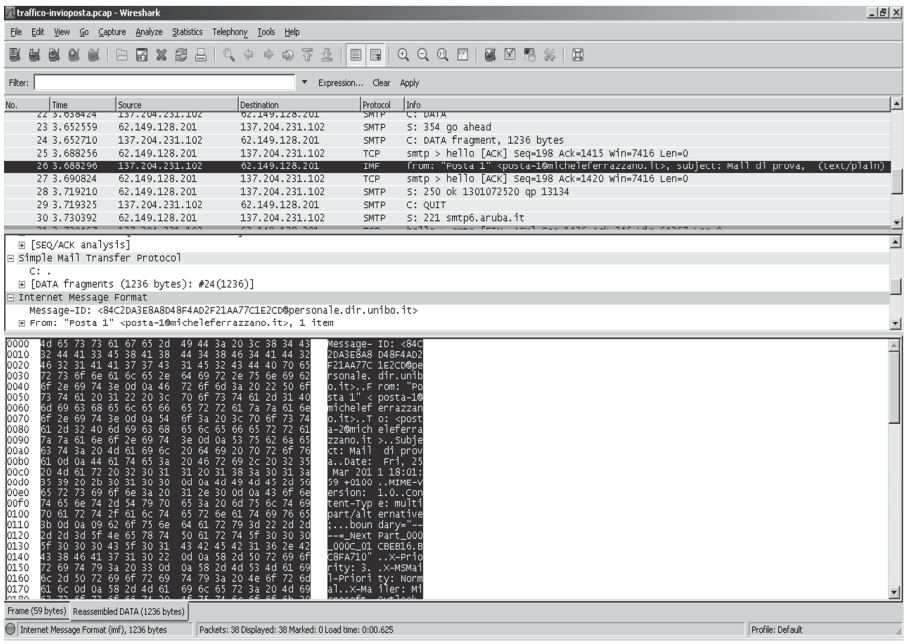

Mail di prova
File Modifica Visualizza Strumenti Messaggio ?
Rispondi
Rispondi a...
Inoltra
Stampa
Elimina
Da: Posta 1
Data: venerdì 25 marzo 2011 18.01
A: posta-2@micheleferrazzano.it
Oggetto: Mail di prova
Testo testo testo

Effettivamente era accaduto questo…

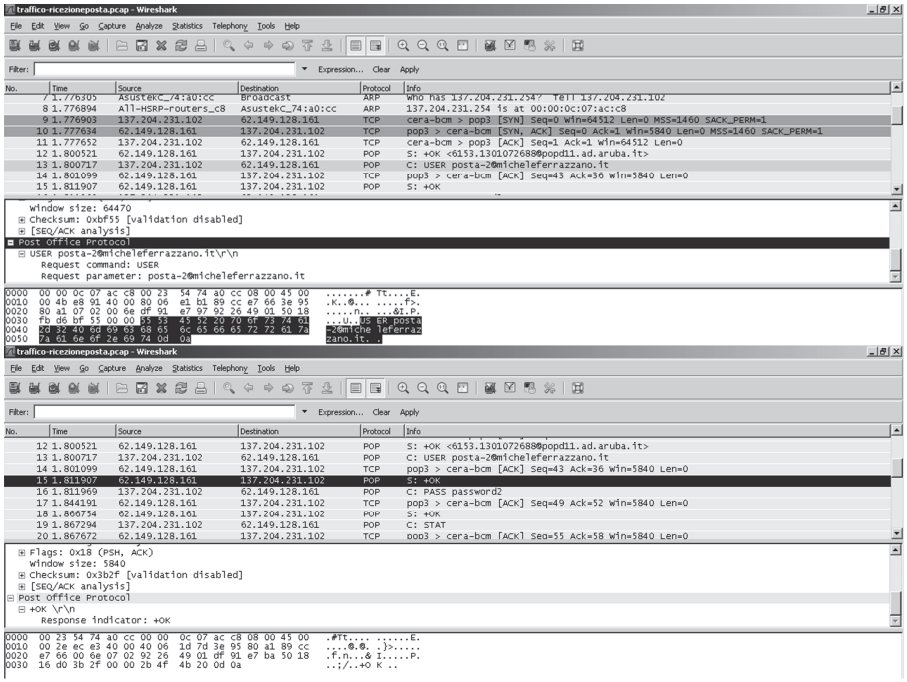


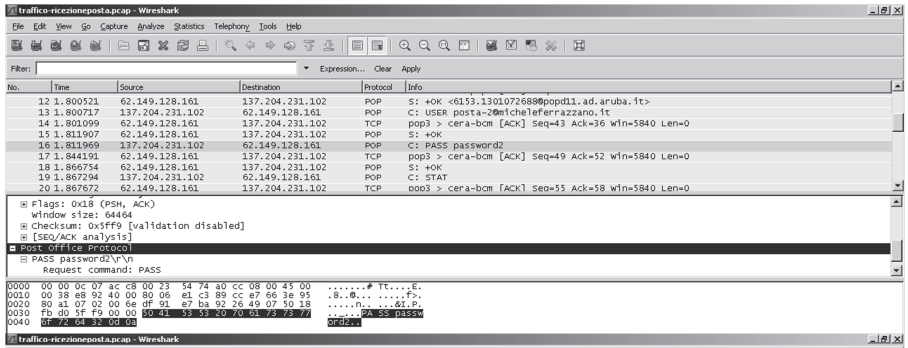


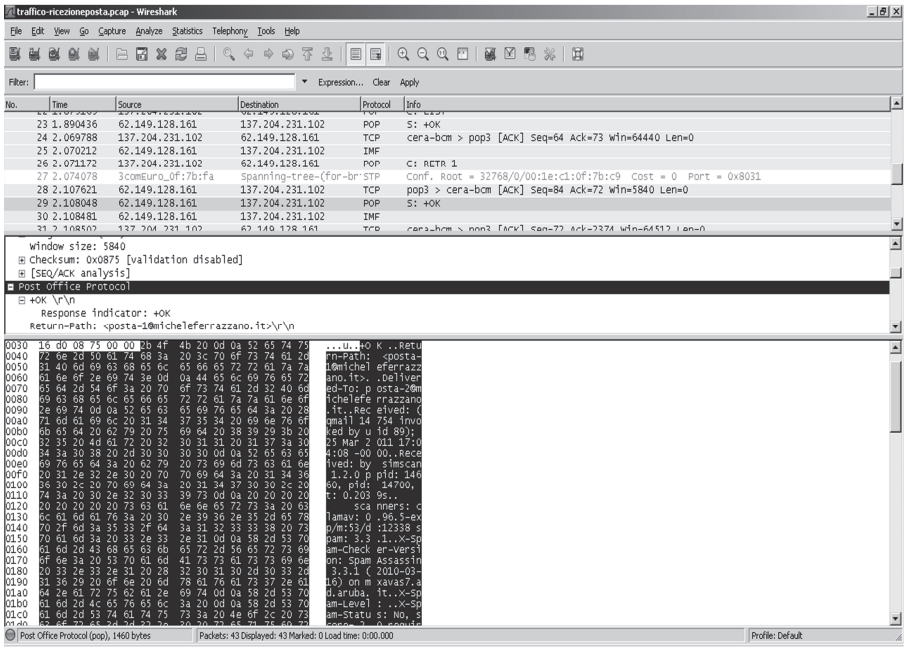


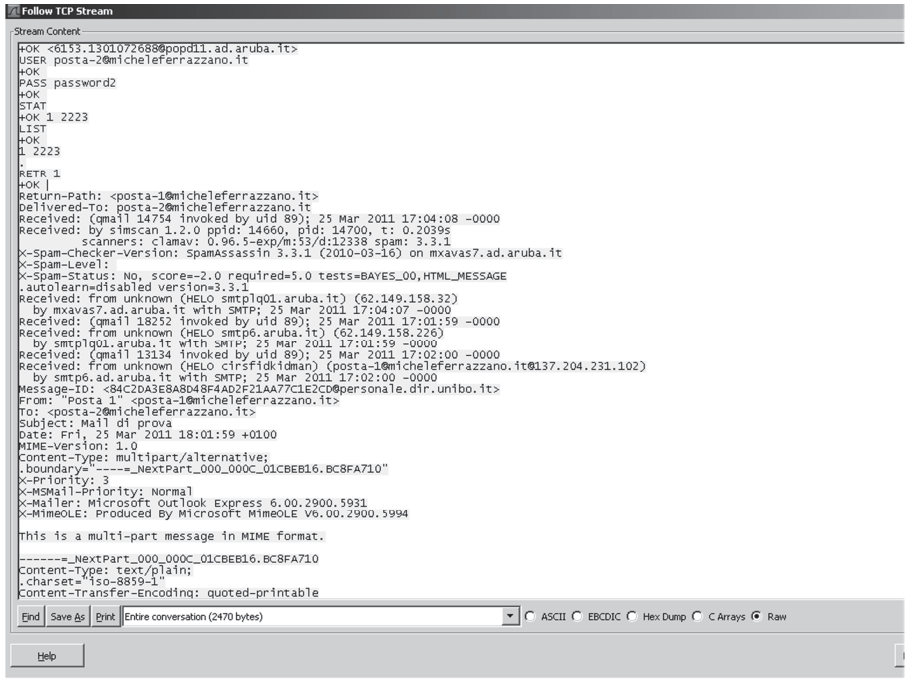


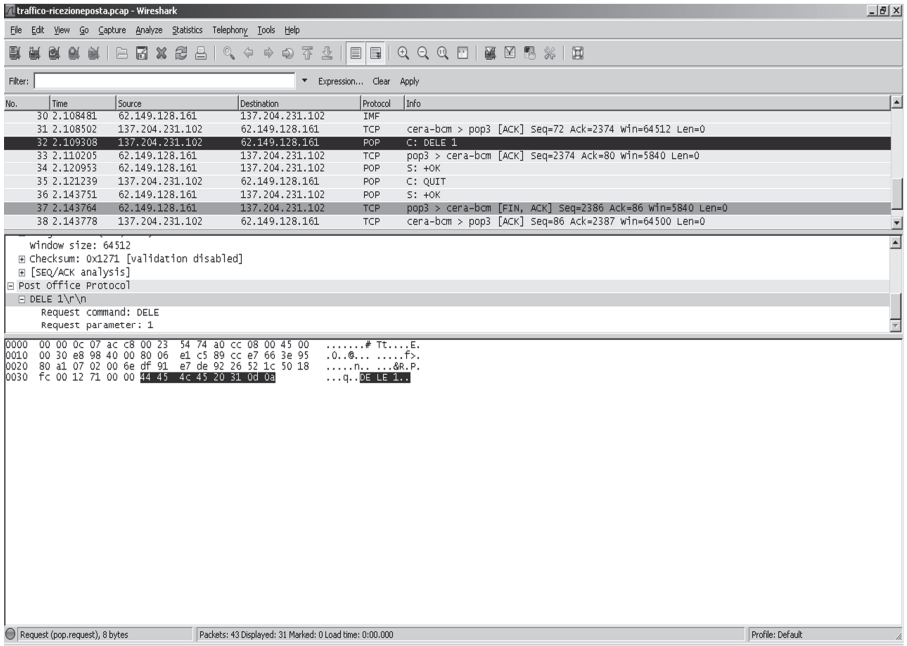
Ricezione di posta elettronica








Follow TCP Stream
Stream Content
+OK <6153.1301072688@popd11.ad.aruba.it>
USER posta-2@micheleferrazzano.it
+OK
PASS password2
+OK
STAT
+OK 1 2223
LIST
+OK
1 2223
.
RETR 1
+OK
Return-Path: <posta-1@micheleferrazzano.it>
Delivered-To: posta-2@micheleferrazzano.it
Received: (qmail 14754 invoked by uid 89); 25 Mar 2011 17:04:08 -0000
Received: by simscan 1.2.0 ppid: 14660, pid: 14700, t: 0.2039s
scanners: clamav: 0.96.5-exp/m:53/d:12338 spam: 3.3.1
X-Spam-Checker-Version: SpamAssassin 3.3.1 (2010-03-16) on mxavas7.ad.aruba.it
X-Spam-Level:
X-Spam-Status: No, score=-2.0 required=5.0 tests=BAYES_00,HTML_MESSAGE
autolearn=disabled version=3.3.1
Received: from unknown (HELO smtplq01.aruba.it) (62.149.158.32)
by mxavas7.ad.aruba.it with SMTP; 25 Mar 2011 17:04:07 -0000
Received: (qmail 18252 invoked by uid 89); 25 Mar 2011 17:01:59 -0000
Received: from unknown (HELO smtp6.aruba.it) (62.149.158.226)
by smtplq01.aruba.it with SMTP; 25 Mar 2011 17:01:59 -0000
Received: (qmail 13134 invoked by uid 89); 25 Mar 2011 17:02:00 -0000
Received: from unknown (HELO cirsfidkidman) (posta-1@micheleferrazzano.it@137.204.231.102)
by smtp6.ad.aruba.it with SMTP; 25 Mar 2011 17:02:00 -0000
Message-ID: <84C2DA3E8A8D48F4AD2F21AA77C1E2CD@personale.dir.unibo.it>
From: "Posta 1" <posta-1@micheleferrazzano.it>
To: <posta-2@micheleferrazzano.it>
Subject: Mail di prova
Date: Fri, 25 Mar 2011 18:01:59 +0100
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="----=_NextPart_000_000C_01CBEB16.BC8FA710"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.5931
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.5994
This is a multi-part message in MIME format.
------=_NextPart_000_000C_01CBEB16.BC8FA710
Content-Type: text/plain;
charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
Find
Save As
Print
Entire conversation (2470 bytes)
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help


traffico-ricezioneposta.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
30 2.108481 62.149.128.161 137.204.231.102 IMF
31 2.108502 137.204.231.102 62.149.128.161 TCP cera-bcm > pop3 [ACK] Seq=72 Ack=2374 Win=64512 Len=0
32 2.109308 137.204.231.102 62.149.128.161 POP C: DELE 1
33 2.110205 62.149.128.161 137.204.231.102 TCP pop3 > cera-bcm [ACK] Seq=2374 Ack=80 Win=5840 Len=0
34 2.120953 62.149.128.161 137.204.231.102 POP S: +OK
35 2.121239 137.204.231.102 62.149.128.161 POP C: QUIT
36 2.143751 62.149.128.161 137.204.231.102 POP S: +OK
37 2.143764 62.149.128.161 137.204.231.102 TCP pop3 > cera-bcm [FIN, ACK] Seq=2386 Ack=86 Win=5840 Len=0
38 2.143778 137.204.231.102 62.149.128.161 TCP cera-bcm > pop3 [ACK] Seq=86 Ack=2387 Win=64500 Len=0
Window size: 64512
Checksum: 0x1271 [validation disabled]
[SEQ/ACK analysis]
Post Office Protocol
DELE 1\r\n
Request command: DELE
Request parameter: 1
0000 00 00 0c 07 ac c8 00 23 54 74 a0 cc 08 00 45 00 ....# Tt....E.
0010 00 30 e8 98 40 00 80 06 e1 c5 89 cc e7 66 3e 95 .0..@... .....f>.
0020 80 a1 07 02 00 6e df 91 e7 de 92 26 52 1c 50 18 .....n.. ...&R.P.
0030 fc 00 12 71 00 00 44 45 4c 45 20 31 0d 0a ...q..DE LE 1..
Request (pop.request), 8 bytes
Packets: 43 Displayed: 31 Marked: 0 Load time: 0:00.000
Profile: Default