

# Informatica forense

---

## Esempi pratici disk forensics e network forensics

*Michele Ferrazzano*

24/04/2012

## 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 Sleuth 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

```

File Edit View Terminal Tabs Help
ubuntu@ubuntu: ~
root@ubuntu:~# autopsy

=====

Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.08

=====

Evidence Locker: /var/lib/autopsy
Start Time: Thu Mar 24 12:35:22 2011
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

    http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit

```



14

## Autopsy – Creazione di un nuovo caso

History Bookmarks Tools Help

http://localhost:9999/autopsy?mod=0&view=1

Getting Started Latest Headlines

CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

2. **Description:** An optional, one line description of this case.

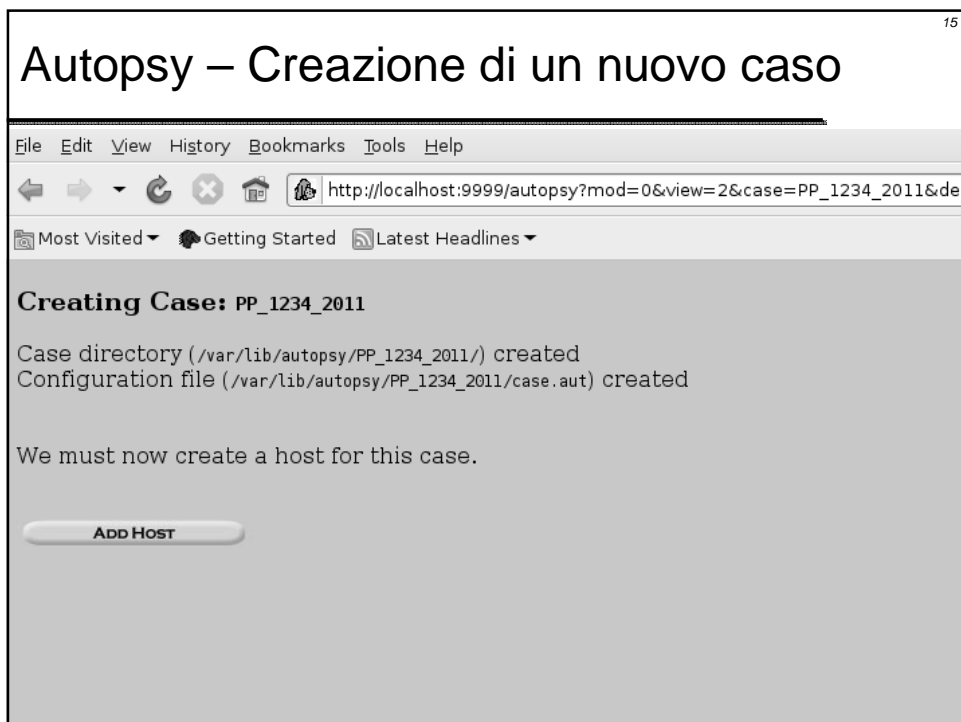
3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a. <input type="text" value="Michele Ferrazzano"/>	b. <input type="text"/>
c. <input type="text"/>	d. <input type="text"/>
e. <input type="text"/>	f. <input type="text"/>
g. <input type="text"/>	h. <input type="text"/>
i. <input type="text"/>	j. <input type="text"/>

NEW CASE CANCEL HELP

15

## Autopsy – Creazione di un nuovo caso



File Edit View History Bookmarks Tools Help

http://localhost:9999/autopsy?mod=0&view=2&case=PP\_1234\_2011&des

Most Visited Getting Started Latest Headlines

### Creating Case: PP\_1234\_2011

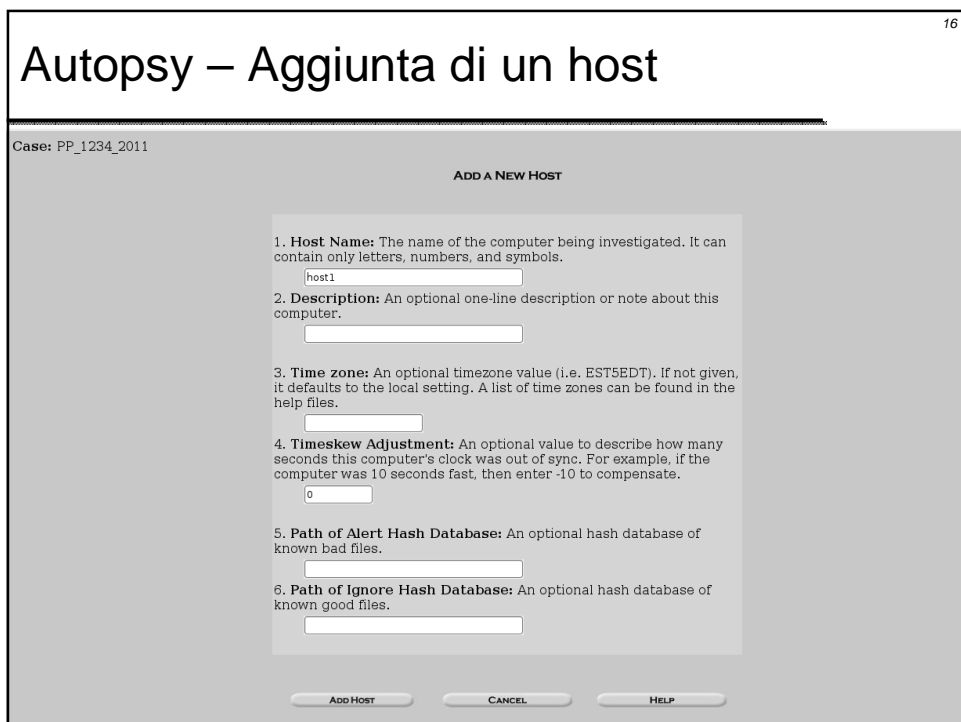
Case directory (/var/lib/autopsy/PP\_1234\_2011/) created  
Configuration file (/var/lib/autopsy/PP\_1234\_2011/case.aut) created

We must now create a host for this case.

ADD HOST

16

## Autopsy – Aggiunta di un host



Case: PP\_1234\_2011

### ADD A NEW HOST

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.

2. **Description:** An optional one-line description or note about this computer.

3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

6. **Path of Ignore Hash Database:** An optional hash database of known good files.

ADD HOST CANCEL HELP



17

## Autopsy – Aggiunta di un host

Case: PP\_1234\_2011

ADD A NEW HOST

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.

2. **Description:** An optional one-line description or note about this computer.

3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

6. **Path of Ignore Hash Database:** An optional hash database of known good files.

18

## Autopsy – Aggiunta di un host

File Edit View History Bookmarks Tools Help

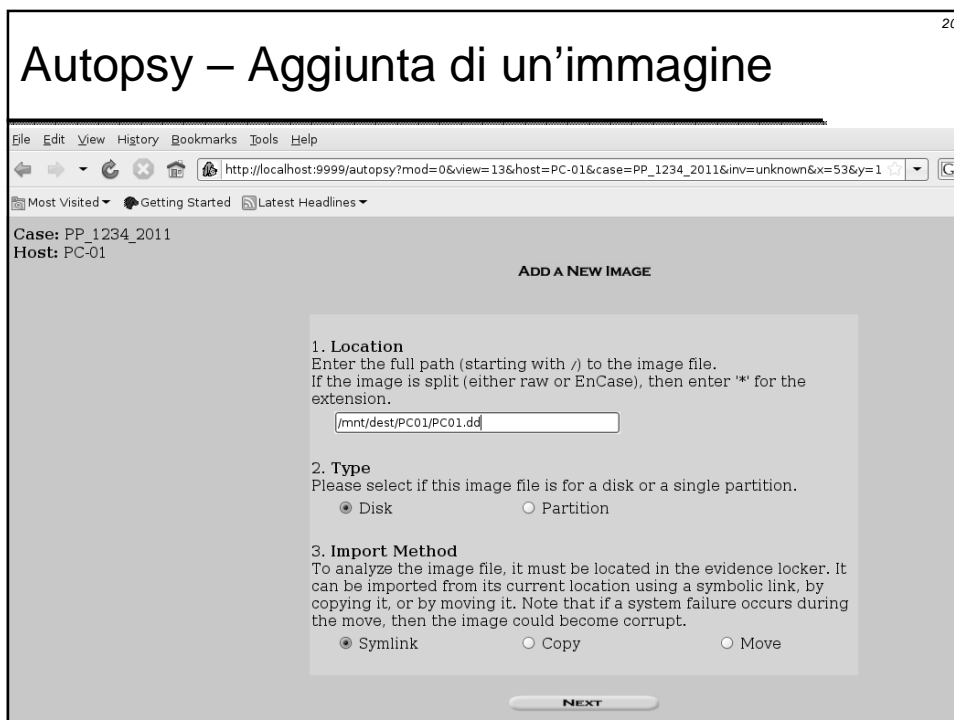
http://localhost:9999/autopsy?mod=0&view=8&case=PP\_1234\_2011&host=PC-01&des

**Adding host: PC-01 to case PP\_1234\_2011**

Host Directory (/var/lib/autopsy/PP\_1234\_2011/PC-01/) created

Configuration file (/var/lib/autopsy/PP\_1234\_2011/PC-01/host.aut) created

We must now import an image file for this host



## Autopsy – Aggiunta di un disco

File Edit View History Bookmarks Tools Help

http://localhost:9999/autopsy?mod=0&view=13&host=PC-01&case=PP\_1234\_2011&inv=unknown&x=53&y=1

Most Visited Getting Started Latest Headlines

Case: PP\_1234\_2011  
Host: PC-01

### ADD A NEW IMAGE

- 1. Location**  
Enter the full path (starting with /) to the image file.  
If the image is split (either raw or EnCase), then enter '\*' for the extension.
- 2. Type**  
Please select if this image file is for a disk or a single partition.  
☒ Disk ☐ Partition
- 3. Import Method**  
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.  
☒ Symlink ☐ Copy ☐ Move

NEXT

## Autopsy – Aggiunta di un disco

### Image File Details

Local Name: images/sda

**Data Integrity:** An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

☒ Ignore the hash value for this image.  
☐ Calculate the hash value for this image.  
☐ Add the following MD5 hash value for this image:  
  
☐ Verify hash after importing?

### File System Details

Analysis of the image file shows the following partitions:

Partition 1 (Type: NTFS (0x07))  
 Sector Range: 63 to 1953503999  
 Mount Point:  File System Type:

ADD CANCEL HELP

For your reference, the mmls output was the following:  
 DOS Partition Table  
 Offset Sector: 0  
 Units are in 512-byte sectors

Slot	Start	End	Length	Description
00:	-----	0000000000	0000000000	0000000001 Primary Table (#0)
01:	-----	0000000001	0000000062	0000000062 Unallocated
02:	00:00	0000000063	1953503999	1953503937 NTFS (0x07)
03:	-----	1953504000	1953525167	0000021168 Unallocated

## Autopsy – Aggiunta di un disco

Case: PP\_1234\_2011  
Host: PC-01

### ADD A NEW IMAGE

#### 1. Location

Enter the full path (starting with /) to the image file.  
If the image is split (either raw or EnCase), then enter '\*' for the extension.

#### 2. Type

Please select if this image file is for a disk or a single partition.

☒ Disk

☐ Partition

#### 3. Import Method

To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

☒ Symlink

☐ Copy

☐ Move




## Autopsy – Aggiunta di un disco

### Image File Details

Local Name: images/sdg

**Data Integrity:** An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

☒ Ignore the hash value for this image.

☐ Calculate the hash value for this image.

☐ Add the following MD5 hash value for this image:

☐ Verify hash after importing?

### File System Details

Analysis of the image file shows the following partitions:

**Partition 1** (Type: DOS FAT16 (0x06))

Sector Range: 32 to 1966079

Mount Point: C:

File System Type: fat16

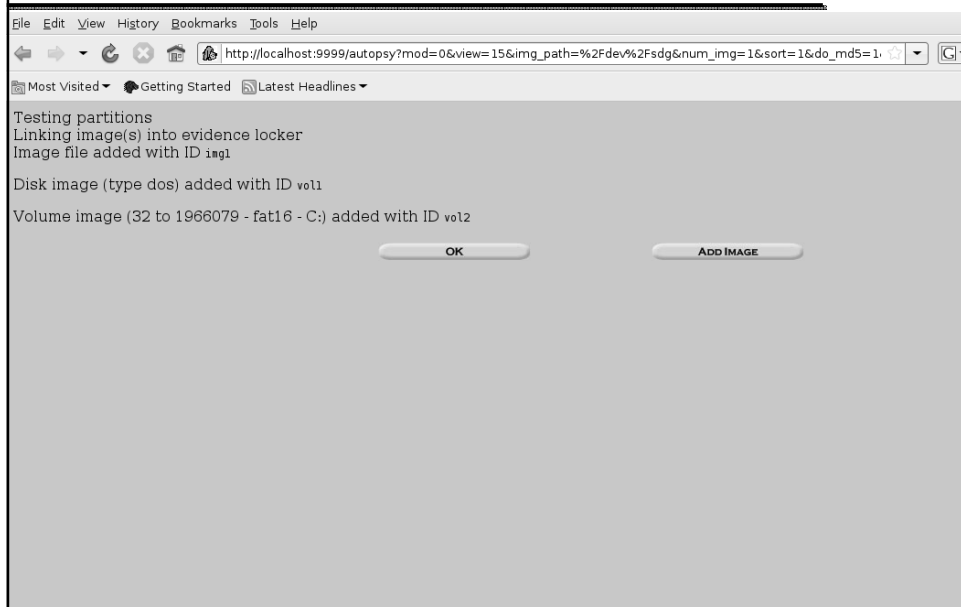



For your reference, the mmls output was the following:

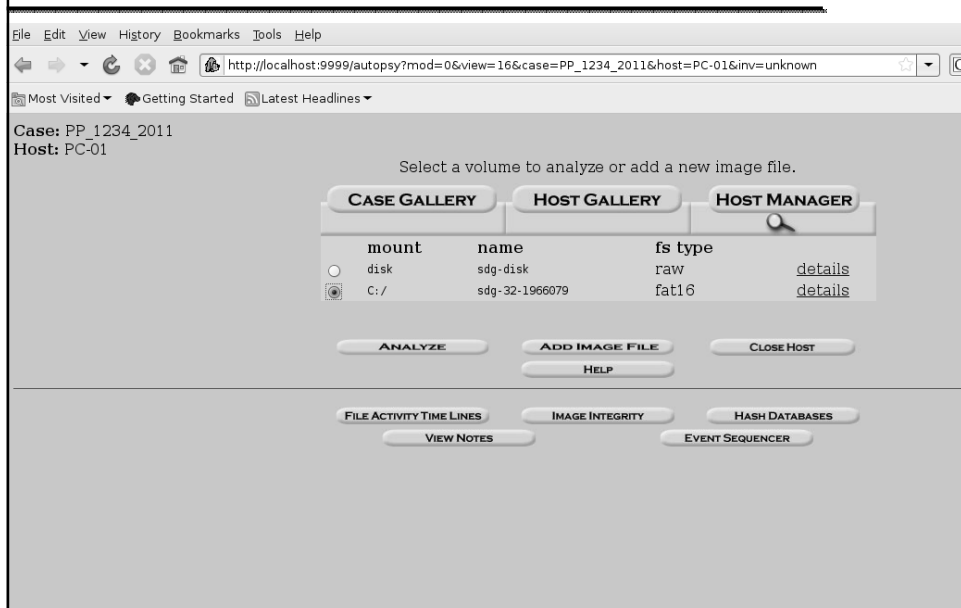
```
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

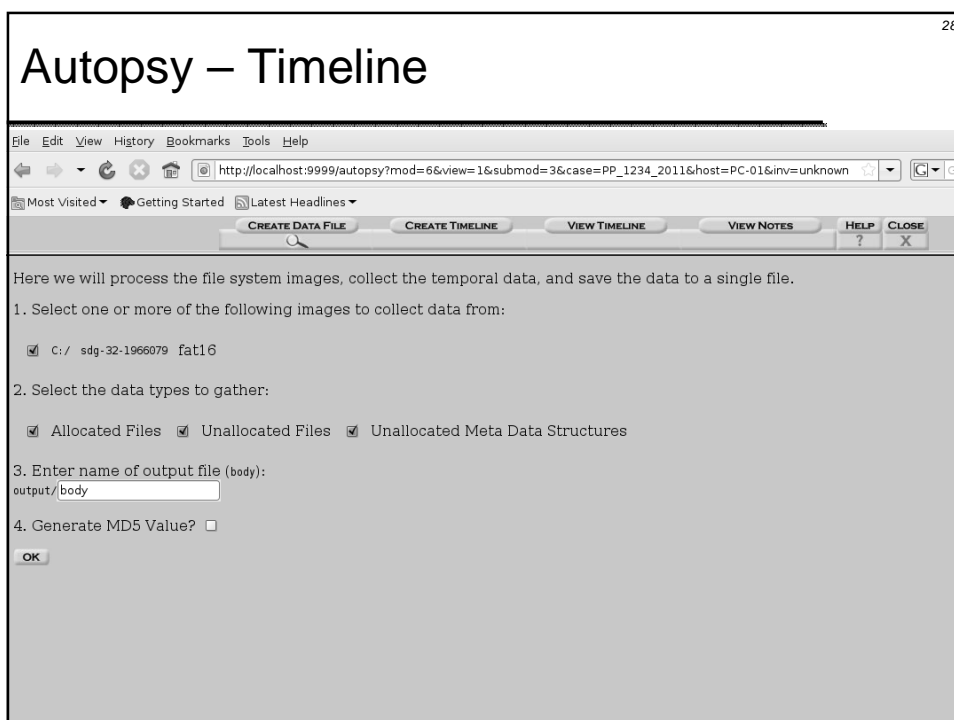
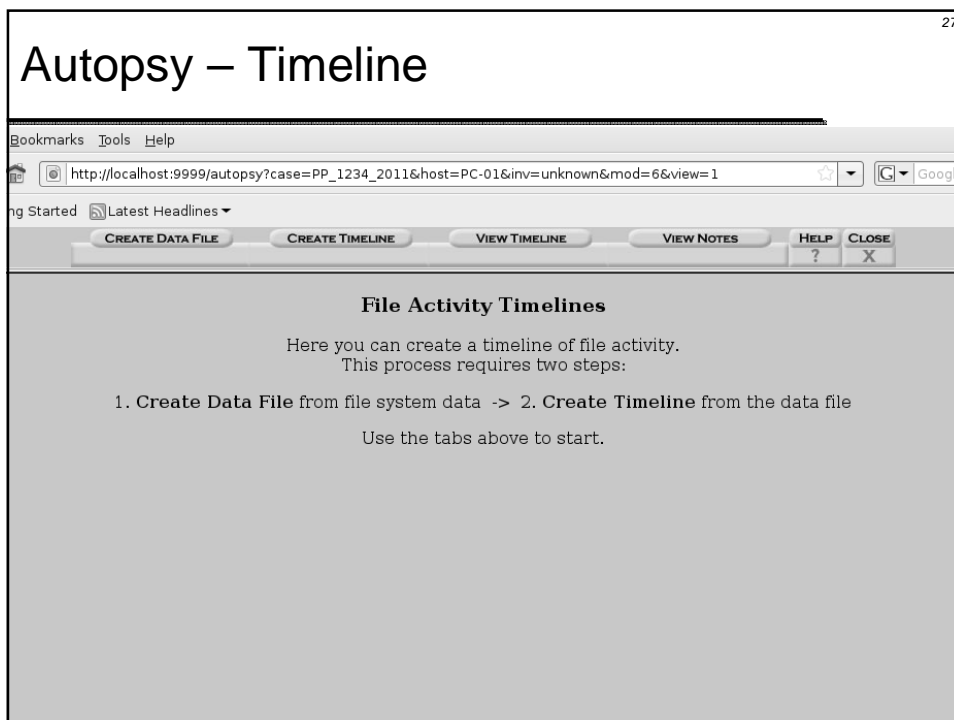
Slot Start End Length Description
00: ---- 0000000000 0000000000 0000000001 Primary Table (#0)
01: ---- 0000000001 0000000021 0000000001 Unallocated
02: 00:00 0000000032 0001966079 0001966048 DOS FAT16 (0x06)
```

## Autopsy – Aggiunta di un disco

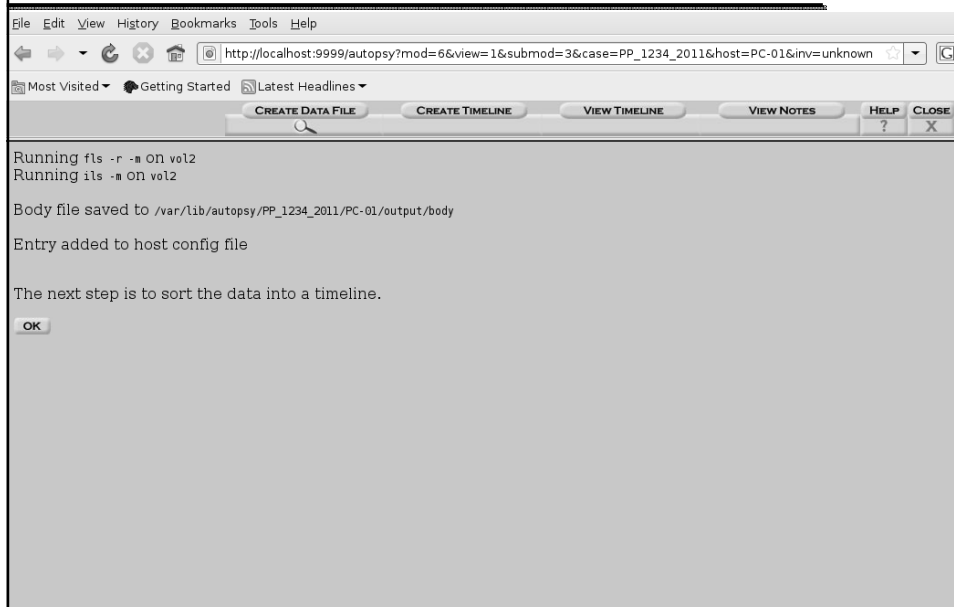


## Autopsy – Aggiunta di un disco

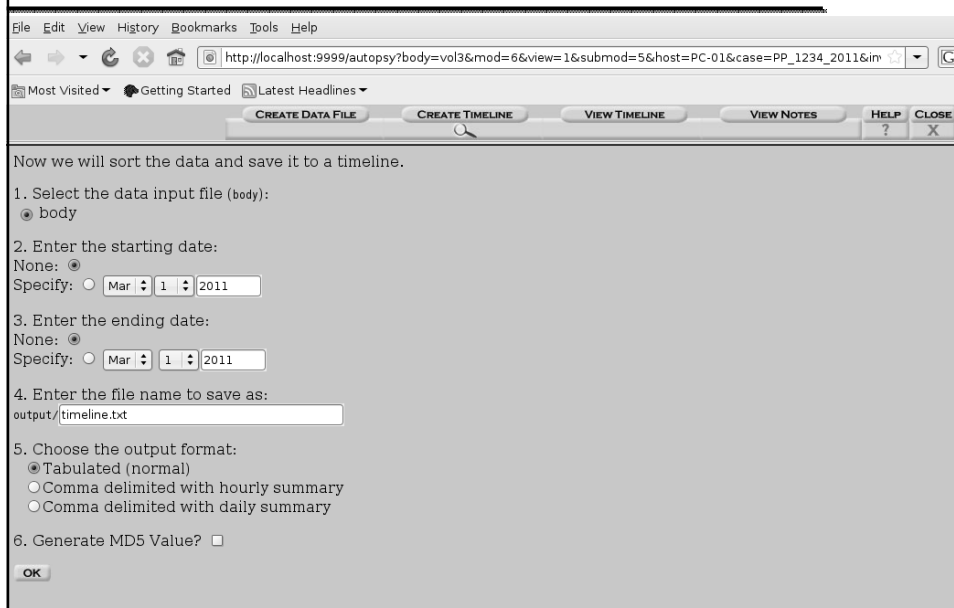




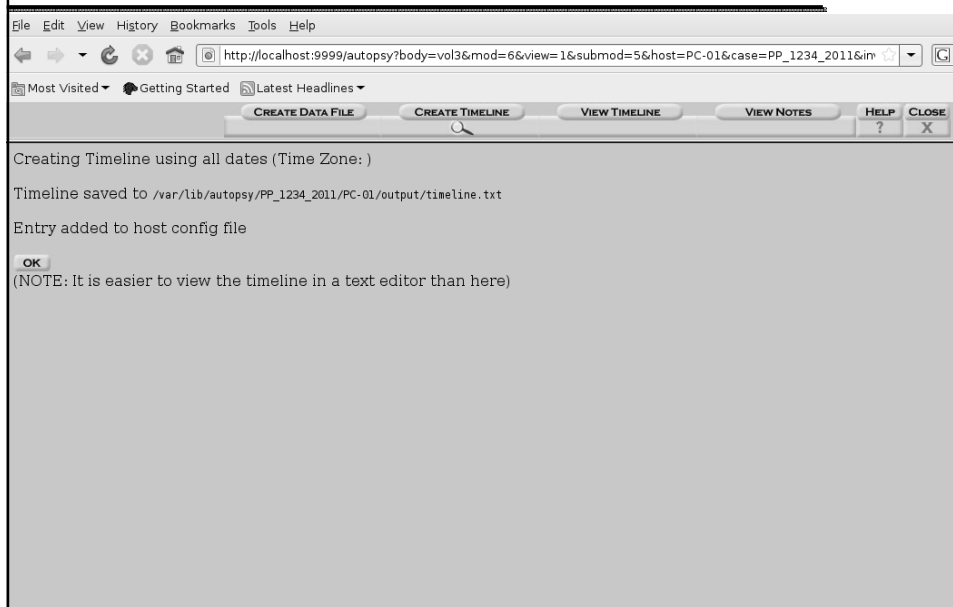
# Autopsy – Timeline



# Autopsy – Timeline



# Autopsy – Timeline

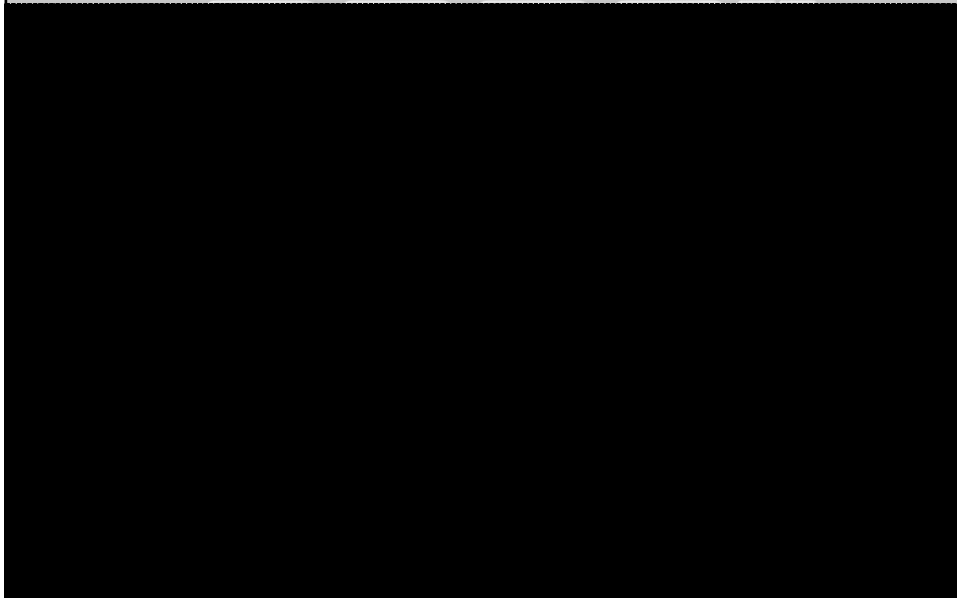


# Autopsy – Timeline

<div> <div>CREATE DATA FILE</div> <div>CREATE TIMELINE</div> <div>VIEW TIMELINE</div> <div>VIEW NOTES</div> <div>HELP</div> <div>CLOSE</div> </div>						
<div> <div>&lt;- Feb 2011</div> <div>Summary</div> <div>Apr 2011 &gt;</div> <div>Mar 2011</div> <div>OK</div> </div>						
Tue Mar 22 2011 23:52:30	394039	..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/rwxrwxrwx	0 0	8464911	C:/12345/Ricerca/Consulente tecnico
	16384	..c	d/rwxrwxrwx	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/iclc-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/Filod - The Harms of Pornography Exposure Among 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



## Autopsy – Timeline

CREATE DATA FILE CREATE TIMELINE VIEW TIMELINE VIEW NOTES HELP ? CLOSE X

<- Feb 2011 Summary Apr 2011 ->

Mar 2011 OK

Tue Mar 22 2011 23:52:30	394039	..c	-rw-rw-rw-rw	0 0 8012677	C:/12345/Ricerca/bibliografia/nuova cartella/4.pdf
	432301	..c	-rw-rw-rw-rw		
	1490663	..c	-rw-rw-rw-rw		
Tue Mar 22 2011 23:52:32	501951	..c	-rw-rw-rw-rw		
	4103042	..c	-rw-rw-rw-rw		
Tue Mar 22 2011 23:52:34	1343877	..c	-rw-rw-rw-rw		
	76579	..c	-rw-rw-rw-rw		
Tue Mar 22 2011 23:52:36	16384	..c	-rw-rw-rw-rw		
	16384	..c	-rw-rw-rw-rw		
	341	..c	-rw-rw-rw-rw		
	75776	..c	-rw-rw-rw-rw		
Tue Mar 22 2011 23:52:38	212988	..c	-rw-rw-rw-rw		...pdf
	233851	..c	-rw-rw-rw-rw		...re Amor
	377497	..c	-rw-rw-rw-rw		
	414012	..c	-rw-rw-rw-rw		
Tue Mar 22 2011 23:52:40	150044	..c	-rw-rw-rw-rw		
	110252	..c	-rw-rw-rw-rw	0 0 9068576	C:/12345/Ricerca/da sistemare/j.1747-9991.2010.00292.x.pdf
	764108	..c	-rw-rw-rw-rw	0 0 9068584	C:/12345/Ricerca/da sistemare/Liu, Uehara, Sasaki - Development of digital forensics practice and research in Japan.pdf

## Autopsy – Timeline

The screenshot shows the Autopsy Timeline interface. At the top, there are buttons: CREATE DATA FILE, CREATE TIMELINE, VIEW TIMELINE, VIEW NOTES, HELP, and CLOSE. Below these is a navigation bar with '<- Feb 2011 Summary Apr 2011 ->' and a date selector set to 'Mar 2011'. The main area displays a list of events with columns for time, offset, and file path. A large black rectangular area obscures the middle portion of the timeline.

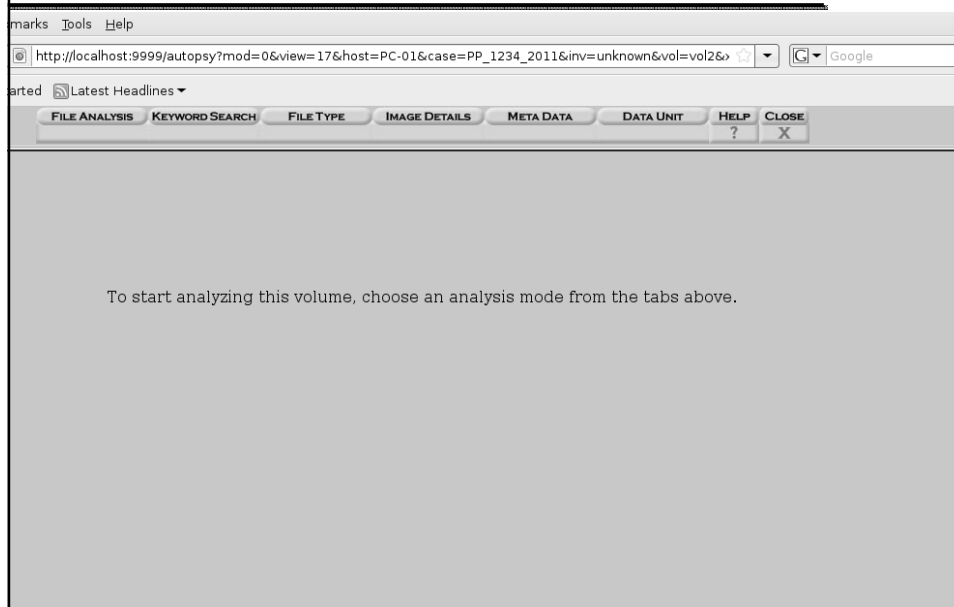
Time	Offset	File Path
Tue Mar 22 2011 23:52:30	394539	C:/12345/Ricerca/da sistemare/fj.1747-9991.2010.00292.x.pdf
	432301	
	1490663	
Tue Mar 22 2011 23:52:32	501951	
	4103042	
Tue Mar 22 2011 23:52:34	1343877	
	76579	
Tue Mar 22 2011 23:52:36	16384	
	16384	
	341	
	75776	
Tue Mar 22 2011 23:52:38	212988	
	233851	
	377497	
	414012	
Tue Mar 22 2011 23:52:40	150044	
	110252	
	764108	

## Autopsy – Analisi

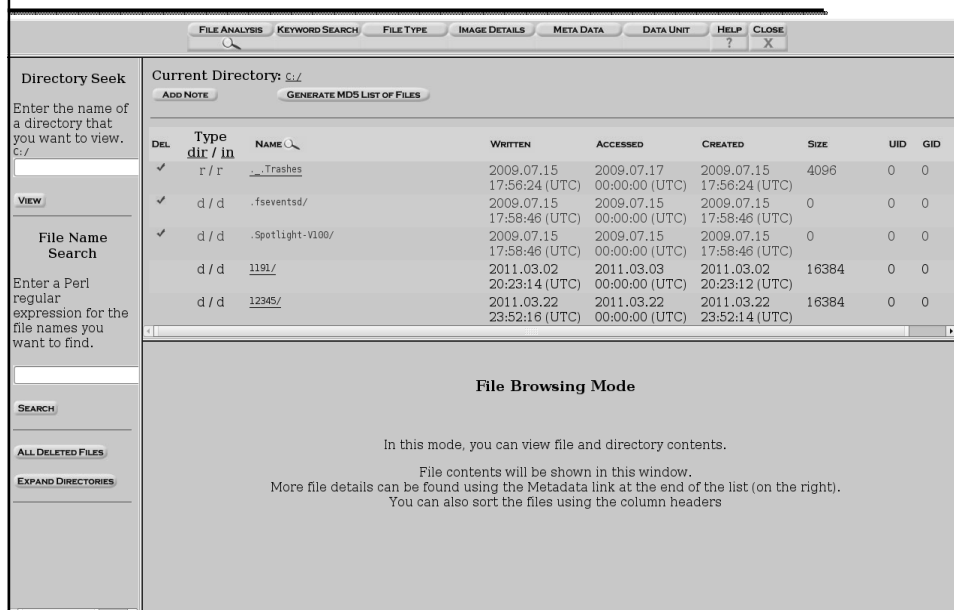
The screenshot shows the Autopsy web interface. At the top, there is a menu bar with 'File', 'Edit', 'View', 'History', 'Bookmarks', 'Tools', and 'Help'. Below the menu bar is a browser address bar showing 'http://localhost:9999/autopsy?mod=0&view=16&case=PP\_1234\_2011&host=PC-01&inv=unknown'. The main content area displays 'Case: PP\_1234\_2011' and 'Host: PC-01'. Below this is a section titled 'Select a volume to analyze or add a new image file.' with three tabs: 'CASE GALLERY', 'HOST GALLERY', and 'HOST MANAGER'. The 'CASE GALLERY' tab is active, showing a table with columns 'mount', 'name', 'fs type', and 'details'. Below the table are buttons for 'ANALYZE', 'ADD IMAGE FILE', 'CLOSE HOST', and 'HELP'. At the bottom, there are buttons for 'FILE ACTIVITY TIME LINES', 'IMAGE INTEGRITY', 'HASH DATABASES', 'VIEW NOTES', and 'EVENT SEQUENCER'.

mount	name	fs type	details
<input type="radio"/> disk	sdg-disk	raw	<a href="#">details</a>
<input checked="" type="radio"/> C: /	sdg-32-1966079	fat16	<a href="#">details</a>

# Autopsy – Analisi



# Autopsy – Analisi



## Autopsy – Analisi

File ANALYSIS Keyword SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP ? CLOSE X

Directory Seek  
Enter the name of a directory that you want to view.  
C:/

VIEW

File Name Search  
Enter a Perl regular expression for the file names you want to find.

SEARCH

ALL DELETED FILES

EXPAND DIRECTORIES

Current Directory: C:/12345/Ricerca/Dottorato - emuleforensic/ /emuleforensic 0.50a/

ADD NOTE GENERATE MD5 LIST OF FILES

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
	d / d	..	2011.03.22 23:53:08 (UTC)	2011.03.22 00:00:00 (UTC)	2011.03.22 23:53:06 (UTC)	16384	0	0	9498628
	d / d	.	2011.03.22 23:53:08 (UTC)	2011.03.22 00:00:00 (UTC)	2011.03.22 23:53:06 (UTC)	16384	0	0	9498627
	r / r	ACSearchStringsDat.c	2010.02.07 20:29:48 (UTC)	2011.03.22 00:00:00 (UTC)	2011.03.22 23:53:06 (UTC)	1558	0	0	9498631
	r / r	ACSearchStringsDat.h	2010.02.07 20:29:48 (UTC)	2011.03.22 00:00:00 (UTC)	2011.03.22 23:53:06 (UTC)	87	0	0	9498634
	r / r	ACSearchStringsDat.o	2010.10.19 14:50:50 (UTC)	2011.03.22 00:00:00 (UTC)	2011.03.22 23:53:06 (UTC)	1844	0	0	9498637
	r / r	clientsMet.c	2010.02.07 20:29:48 (UTC)	2011.03.22 00:00:00 (UTC)	2011.03.22 23:53:06 (UTC)	2710	0	0	9498639
	r / r	clientsMet.h	2010.02.07 20:29:48 (UTC)	2011.03.22 00:00:00 (UTC)	2011.03.22 23:53:06 (UTC)	78	0	0	9498641
	r / r	clientsMet.o	2010.10.19 14:50:26 (UTC)	2011.03.22 00:00:00 (UTC)	2011.03.22 23:53:06 (UTC)	4900	0	0	9498643
	r / r	connetti.xml	2010.02.21 12:44:14 (UTC)	2011.03.22 00:00:00 (UTC)	2011.03.22 23:53:06 (UTC)	2404	0	0	9498644
	r / r	constant.h	2010.10.19 14:50:24 (UTC)	2011.03.22 00:00:00 (UTC)	2011.03.22 23:53:06 (UTC)	2579	0	0	9498645

File Browsing Mode

## Autopsy – Analisi

File Edit View History Bookmarks Tools Help

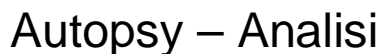
http://localhost:9999/autopsy?mod=2&view=12&case=PP\_1234\_2011&host=PC-

Most Visited Getting Started Latest Headlines

PP\_1234\_2011:PC-01:vol2 http://localhost...meta=9486858

MD5 Values for files in C:/12345/Ricerca/Dottorato - emuleforensic/emuleforensic 0.50a/ (sdg-32-1966079)

8d8a31050ec99ad9691a5f1ceae6e499	-	ACSearchStringsDat.c
052509b3bb6ecc48c02d965e691faee9	-	ACSearchStringsDat.h
23e2f9d91af5a5bbde8e7c2e13acf4a0	-	ACSearchStringsDat.o
f715fb701ce38019c2c9205189817b64	-	clientsMet.c
53df1c357e1c9d0ea81316d587e42634	-	clientsMet.h
3261ebfba4735b33dab20c5a3434b361	-	clientsMet.o
93ec7de95d6145fe3b9eec4b00165d58	-	connetti.xml
3de5eb8cf3f3df73374cc10682d9ff7	-	constant.h
c61a544677dbad8cc7855b8dc9b5453d	-	emuleforensic
37374fe977a33c881ef43ebcc1e09edd	-	emuleforensic.c
e262alb6ddd9a63316803c1258cd409	-	emuleforensic.o
cbf026ee4cdc9da607cb783e309fc6a2	-	esempiomaster.xml
edfad7acd1f0abfc11f5f0fd19bd924b	-	knownMet.c
f07c31c7cbab6cbfb9eb8dc833bf7d8	-	knownMet.h
ee0f2e9e6fd7a9c8bb09d49dd5f670	-	knownMet.o
53e7912f26a63ec0b645180990edb836	-	Makefile
115c3efc2150c4418cb521770b8aa554	-	output-7.xml
d5675e12bce17c00f59aea980edfab60	-	preferencesDat.c
f15abb3a0716b4c9e156cb5f069f4506	-	preferencesDat.h
a8dfacca71b00f884090d2dbe5ba70d9	-	preferencesDat.o
f4fd1d05d2dbb31cbc88033b93cb5eeb	-	report.html
2d19defb6db4cf0b228079083dcbc37b	-	schema.xsd
2dfc7c2445f1465b4dcf46fd5a57e4e2	-	struct.h
197088e9a49ebf9a773af6f213175954	-	transform.xml
5ac3b9f7a4ef536fdff1896ef5156143	-	util.c
8c7325707e4beb15f0d4e52e0518c860	-	util.h
34d82ae2006564c7dbde5cd1db876b6f	-	util.o



## Autopsy – Analisi

The screenshot shows the Autopsy web interface with the 'FILE ANALYSIS' tab selected. The left sidebar contains a 'File Name Search' section with a search box containing 'emule' and buttons for 'SEARCH', 'ALL DELETED FILES', and 'EXPAND DIRECTORIES'. The main content area displays a table of files with 'emule' in the name.

**All files with 'emule' in the name**

[SHOW ALL FILES](#)

DEL	Type	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
d / d		C:/eMuleantonio	2009.07.09 15:27:22 (UTC)	2009.07.20 00:00:00 (UTC)	2009.07.09 15:27:20 (UTC)	16384	0	0	243
d / d		C:/eMuleantonio/eMule	2009.07.09 15:27:22 (UTC)	2009.07.20 00:00:00 (UTC)	2009.07.09 15:27:20 (UTC)	16384	0	0	342534
r / r		C:/12345/Ricerca/Dottorato - Documenti presentati/documenti consegnati per domanda dottorato/emuleforensic - iisfa memberbook 2010.pdf	2010.08.30 18:10:38 (UTC)	2011.03.22 00:00:00 (UTC)	2011.03.22 23:52:56 (UTC)	1039674	0	0	9406992
r / r		C:/12345/Ricerca/Dottorato - Documenti presentati/7000/emuleforensic - iisfa	2010.09.16 11:11:02 (UTC)	2011.03.22 00:00:00 (UTC)	2011.03.22 23:53:02 (UTC)	697468	0	0	9464329

ASCII (display - report) \* Hex (display - report) \* ASCII Strings (display - report) \* Export \* Add Note

File Type: writable, no read permission  
Deleted File Recovery Mode

Contents Of File: C:/\_IUCE.tmp

http://localhost:9999/autopsy?mod=2&view=8&case=PP\_1234\_2011&host=PC-01&inv=unknown&vol=vol2&meta=9406992&sort=2&dir=12345/Ricerca/Dottorato+-+Documenti+presentati/d...

## Autopsy – Ricerca

The screenshot shows the Autopsy web interface with the 'KEYWORD SEARCH' tab selected. The left sidebar contains a 'File Name Search' section with a search box containing 'emule' and buttons for 'SEARCH', 'ALL DELETED FILES', and 'EXPAND DIRECTORIES'. The main content area displays the 'Keyword Search of Allocated and Unallocated Space' interface.

**Keyword Search of Allocated and Unallocated Space**

Enter the keyword string or expression to search for:

emule

☒ ASCII ☒ Unicode

☒ Case Insensitive ☐ grep Regular Expression

[SEARCH](#)

[EXTRACT STRINGS](#) [EXTRACT UNALLOCATED](#)

[Regular Expression Cheat Sheet](#)

NOTE: The keyword search runs `grep` on the image.  
A list of what will and what will not be found is available [here](#).

**Predefined Searches**

[CC](#) [SSN2](#) [IP](#) [SSN1](#)

[Date](#)

# Autopsy – Ricerca

Autopsy Bookmarks Tools Help

http://localhost:9999/autopsy?mod=1&submod=4&case=PP\_1234\_2011&host=PC-01&inv=unknown&vol=vol2

Getting Started Latest Headlines

1.vol2 Autopsy grep Cheat Sheet

FILE ANALYSIS **KEYWORD SEARCH** FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE

## Keyword Search of Allocated and Unallocated Space

Enter the keyword string or expression to search for:

☒ ASCII ☒ Unicode

☒ Case Insensitive ☐ grep Regular Expression

[Regular Expression Cheat Sheet](#)

NOTE: The keyword search runs `grep` on the image.  
A list of what will and what will not be found is available [here](#).

## Predefined Searches

# Autopsy – Ricerca

FILE ANALYSIS **KEYWORD SEARCH** FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE

Searching for ASCII: Done  
Saving: Done  
1620 hits- [link to results](#)

Searching for Unicode: Done  
Saving: Done  
553 hits- [link to results](#)

**New Search**

**1620 occurrences of emule were found**  
Search Options:  
ASCII  
Case Insensitive

There were more than 1000 hits.  
Please revise the search to a manageable amount.

The 1620 hits can be found in: /var/lib/autopsy/PP\_1234\_2011/PC-01/output/sdg-32-1966079-0.srch

**553 occurrences of emule were found**  
Search Options:  
Unicode  
Case Insensitive

Sector 21960 (Hex - Ascii)  
1: 114 (anni\emule\Temp)

Sector 21992 (Hex - Ascii)  
2: 114 (anni\emule\Temp)

Sector 609291 (Hex - Ascii)  
3: 174 (ENTE EMULE: ANA)

# Autopsy – Ricerca

FILE ANALYSIS   KEYWORD SEARCH   FILE TYPE   IMAGE DETAILS   META DATA   DATA UNIT   HELP   CLOSE

Search Options:  
Unicode  
Case insensitive

Export Contents   Add Note

ASCII (display - report) \* Hex (display - report) \* ASCII Strings (display - report)  
File Type: data

Sector: 609347  
Status: Allocated  
Find Meta Data Address

Hex Contents of Sector 609347 in sdg-32-1966079

0	65004d00	75006c00	65004600	6f007200	e.M.u.l.e.F.o.r.
16	65006e00	73006900	63003a00	20006100	e.n.s.i.c.r..a
32	6e006100	6c006900	73006900	20006600	n.a.l.l.s.i..f.
48	6f007200	65006e00	73006500	20006400	o.r.e.n.s.e..d.
64	65006c00	20006600	69006c00	65002000	e.l..f.i.l.e..
80	73006900	61007200	65006e00	67002000	s.h.a.r.l.n.g..
96	63006f00	6e002000	65004d00	75006c00	c.o.n..e.M.u.l.
112	65000d00	65004d00	75006c00	65002000	e...e.M.u.l.e..
128	e9002000	75006e00	20007300	6f006600	...u.n..s.e.f.
144	74007700	61007200	65002000	6f007000	t.v.a.r.e..o.p.
160	65006e00	20007300	6f007500	72006300	e.n..s.o.u.r.c.
176	65002000	63006800	65002000	63006f00	e..c.h.e..c.o.
192	6e007300	65006e00	74006500	20006400	n.s.e.n.t.e..d.
208	69002000	72006500	61006c00	69007a00	i..r.e.a.l.i.z.
224	7a006100	72006500	20006c00	27006100	z.a.r.e..l..a.
240	74007400	69007600	69007400	e0002000	t.t.i.v.i.t..
256	64006900	20006600	69006c00	65002000	d.i..f.i.l.e..
272	73006800	61007200	69006e00	67002000	s.h.a.r.l.n.g..
288	69006e00	20006100	6d006200	69006500	i.n..a.m.b.i.e.
304	6e007400	65002000	70006500	65007200	n.t.e..p.e.e.r.
320	2d007400	6f002d00	70006500	65007200	-t.o..p.e.e.r.
336	20006200	61007300	61007400	6f002000	.b.a.s.a.t.o..
352	73007500	69002000	70007200	6f007400	s.u.i..p.r.o.t.
368	6f006300	6f006c00	6c006900	20006500	o.c.o.l.l.i..e.
384	44006f00	6e006b00	65007900	20006f00	O.o.n.k.e.y..o.
400	20004b00	61006400	65006d00	6c006900	.K.a.d.e.m.l.i.
416	61002e00	9d004400	61006c00	20007000	a...d.a.l..p.
432	75006e00	74006f00	20006400	69002000	u.n.t.o..d.i..
448	76006900	73007400	61002000	64006500	v.i.s.t.a..d.e.
464	6c006c00	27006100	6e006100	6c006900	l.l.'a.n.a.l.i.
480	73006900	20006600	6f007200	65006e00	s.i.l..f.o.r.e.n.
496	73006500	2c002000	75006e00	61002000	e.e..u.n.a

# Analisi di una email

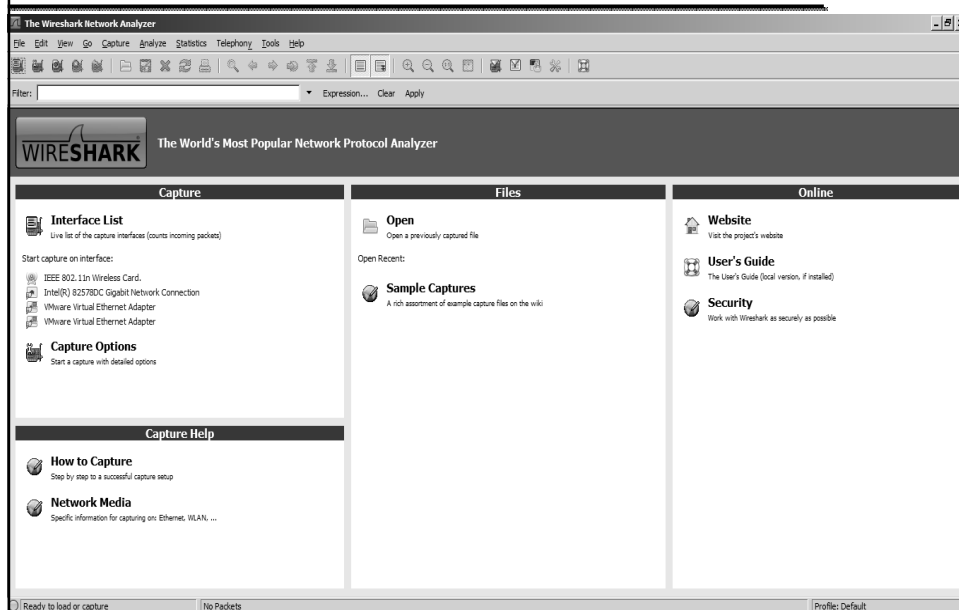
```
Return-Path: mittente@gmail.com
Received: from [192.168.1.83] (dynamic-adsl-84-220-169-6.clienti.tiscali.it
[84.220.169.6])
    by mx.google.com with ESMTPS id bs4sm597962wbb.35.2011.03.25.12.31.02
    (version=SSLv3 cipher=OTHER);
Fri, 25 Mar 2011 12:31:03 -0700 (PDT)
Message-ID: 4D8CED7B.2050105@gmail.com
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
```



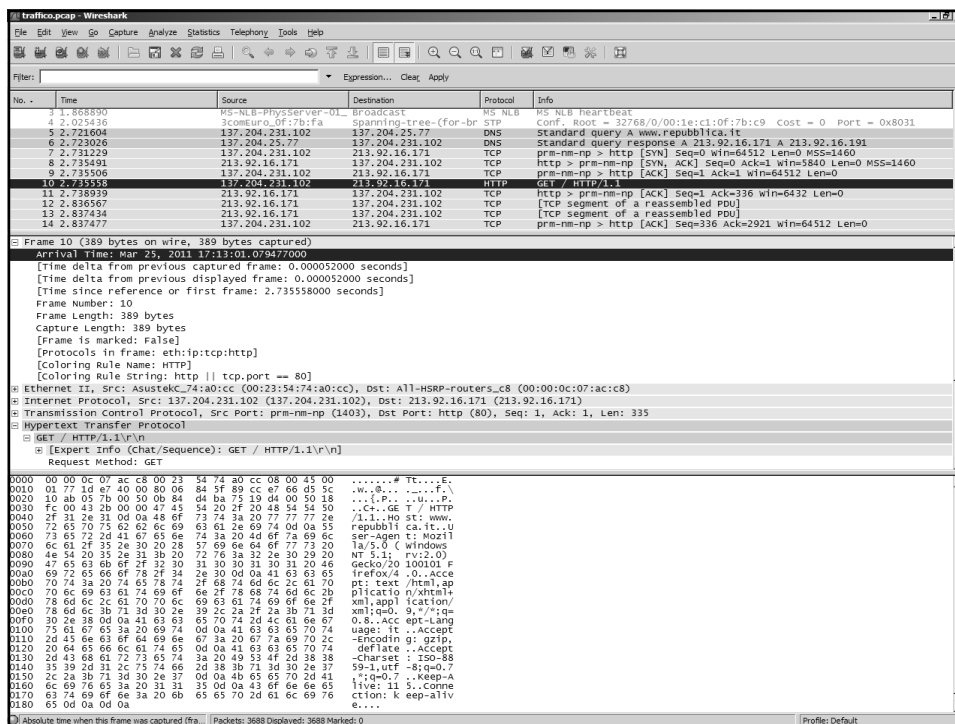
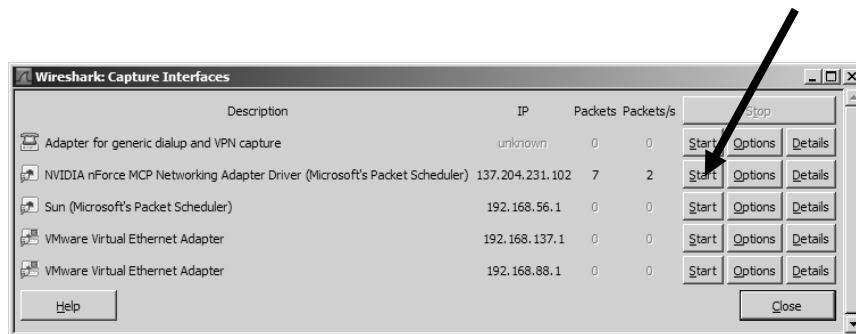
# Analisi forense con Wireshark



# Wireshark

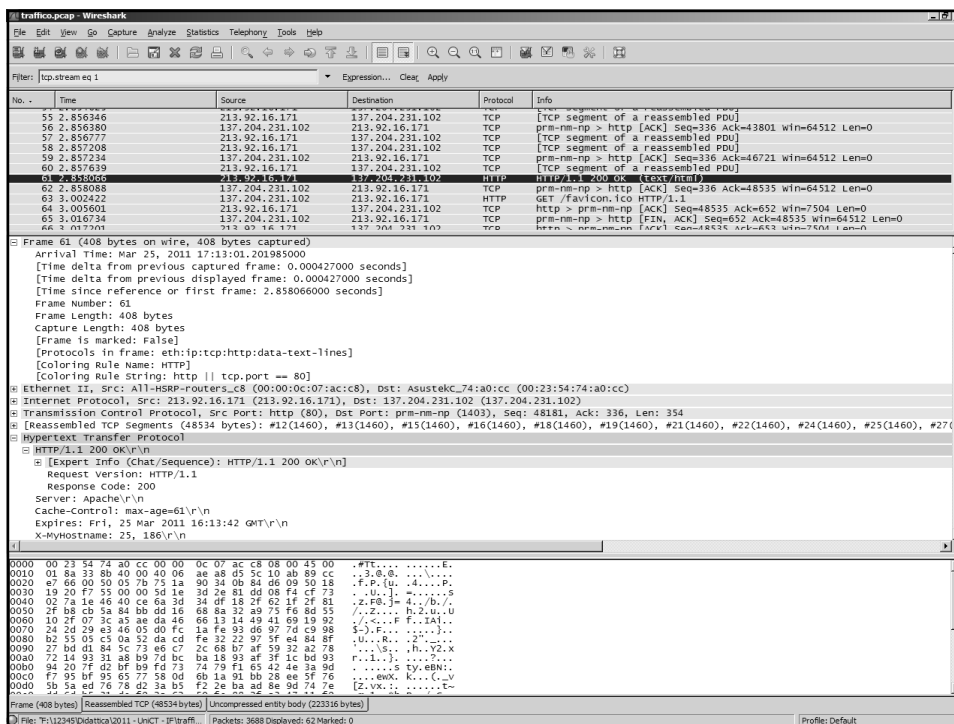


# Avvio dell'intercettazione del traffico



Wireshark packet capture analysis showing a GET request to www.repubblica.it. The packet list shows a standard query and a successful HTTP response (200 OK). The packet details pane shows the request method, URI, and various headers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Wireshark packet capture analysis showing a GET request to www.repubblica.it. The packet list shows a standard query and a successful HTTP response (200 OK). The packet details pane shows the request method, URI, and various headers. The packet bytes pane shows the raw data in hexadecimal and ASCII.



Wireshark interface showing a packet capture of an HTTP GET request to the La Repubblica website. The packet list shows a TCP segment (No. 62) and an HTTP GET request (No. 63). The packet details pane shows the HTTP request structure, including the status bar (200 OK), content type (text/html), and the request body (48193 bytes). The packet bytes pane shows the raw data of the request body, which is a gzipped HTML document.

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	prn-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	prn-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	2.858005	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	prn-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 > prn-nm-np [ACK] Seq=48535 Ack=652 win=7504 Len=0
65	3.016734	137.204.231.102	213.92.16.171	TCP	prn-nm-np > http [FIN, ACK] Seq=652 Ack=48535 win=64512 Len=0
66	3.017701	213.92.16.171	137.204.231.102	TCP	http > prn-nm-np [ACK] Seq=48535 Ack=652 win=7504 Len=0

Packet 62 details:

```

X-Cache: HIT\r\n
X-Cache-Hits: 177\r\n
Content-encoding: gzip\r\n
Content-length: 48193 bytes
Content-type: text/html

```

Packet 63 details:

```

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">\n
<html xmlns="http://www.w3.org/1999/xhtml">\n
<head>\n
<meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7; IE=EmulateIE9" /\n
<title>La Repubblica.it - Homepage</title>\n
<meta name="keywords" content="La Repubblica, notizie internazionale, giornaliere, nazionale, politics, scienze, business, affari, finanza, s
[truncated]
<meta name="description" content="Repubblica.it: il quotidiano online con tutte le notizie in tempo reale. News e ultime notizie. Tutti i set
[truncated]
<link rel="alternate" type="application/rss+xml" title="Homepage - La Repubblica.it" href="http://www.repubblica.it/rss/homepage/rss2.0.xml" /\n
[truncated]
<meta name="fb:admins" content="100000390369341" /\n
<meta name="msapplication-starturl" content="http://www.repubblica.it/" /\n
<meta name="msapplication-tooltip" content="Naviga sul sito de La Repubblica.it" /\n
<meta name="msapplication-window" content="width=1024;height=68" /\n

```

Wireshark interface showing the same packet capture, but with a context menu open over the packet details pane. The menu options include: Expand Subtree, Expand All, Collapse All, Apply as Filter, Prepare a Filter, Colorize with Filter, Follow TCP Stream, Follow UDP Stream, Follow HTTP Stream, Copy, Export Selected Packet Bytes..., Wiki Protocol Page, Filter Field Reference, Protocol Preferences, Decode As..., Disable Protocol..., Resolve Name, and Go to Corresponding Packet.

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	prn-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	prn-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	2.858005	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	prn-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 > prn-nm-np [ACK] Seq=48535 Ack=652 win=7504 Len=0
65	3.016734	137.204.231.102	213.92.16.171	TCP	prn-nm-np > http [FIN, ACK] Seq=652 Ack=48535 win=64512 Len=0
66	3.017701	213.92.16.171	137.204.231.102	TCP	http > prn-nm-np [ACK] Seq=48535 Ack=652 win=7504 Len=0

Packet 62 details:

```

Date: Fri, 25 Mar 2011 16:13:04 GMT\r\n
Age: 23\r\n
Connection: keep-alive\r\n
X-Cache: HIT\r\n
X-Cache-Hits: 177\r\n
Content-encoding: gzip\r\n
Content-length: 48193 bytes
Content-type: text/html

```

Packet 63 details:

```

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">\n
<html xmlns="http://www.w3.org/1999/xhtml">\n
<head>\n
<meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7; IE=EmulateIE9" /\n
<title>La Repubblica.it - Homepage</title>\n
<meta name="keywords" content="La Repubblica, notizie internazionale, giornaliere, nazionale, politics, scienze, business, affari, finanza, s
[truncated]
<meta name="description" content="Repubblica.it: il quotidiano online con tutte le notizie in tempo reale. News e ultime notizie. Tutti i set
[truncated]
<link rel="alternate" type="application/rss+xml" title="Homepage - La Repubblica.it" href="http://www.repubblica.it/rss/homepage/rss2.0.xml" /\n
[truncated]
<meta name="fb:admins" content="100000390369341" /\n
<meta name="msapplication-starturl" content="http://www.repubblica.it/" /\n
<meta name="msapplication-tooltip" content="Naviga sul sito de La Repubblica.it" /\n
<meta name="msapplication-window" content="width=1024;height=68" /\n

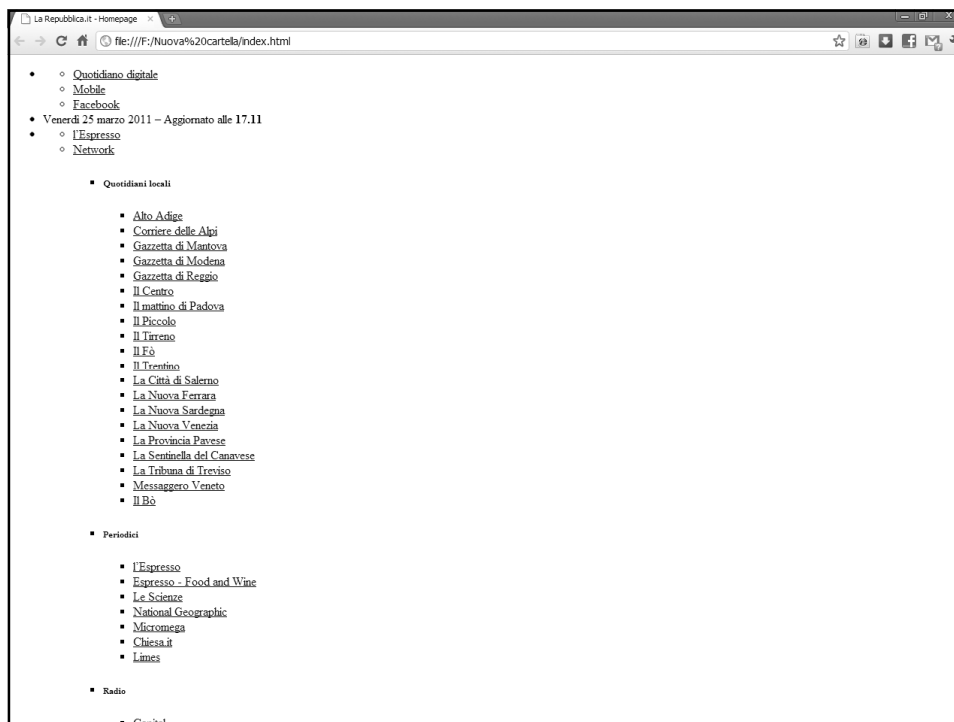
```

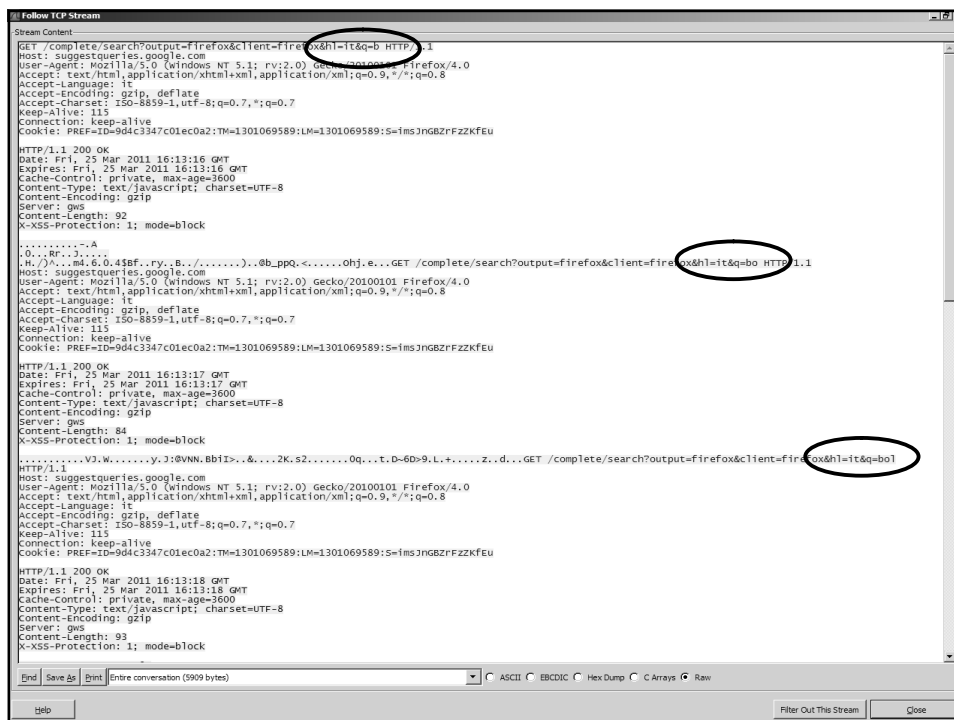


```

1
2
3
4
5
6 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
7 <html xmlns="http://www.w3.org/1999/xhtml">
8 <head>
9   <meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7; IE=EmulateIE9" />
10   <title>La Repubblica.it - Homepage</title>
11
12   <meta name="keywords" content="La Repubblica, notizie internazionale, giornaliere, nazionale, politica, scienze, business, affari, finanza, sport, c">
13   <meta name="description" content="Repubblica.it: il quotidiano online con tutte le notizie in tempo reale. News e ultime notizie. Tutti i settori: po">
14   <link rel="alternate" type="application/rss+xml" title="Homepage - La Repubblica.it" href="http://www.repubblica.it/rss/homepage/rss2.0.xml" />
15   <meta name="msapplication-task" content="name=Economia;action-uri=http://www.repubblica.it/economia;icon-uri=http://www.repubblica.it/static/images">
16   <meta property="fb:admins" content="100000390369341"/>
17   <meta name="msapplication-startup" content="http://www.repubblica.it/" />
18   <meta name="msapplication-tooltip" content="Naviga sul sito de la Repubblica.it" />
19   <meta name="msapplication-window" content="width=1024;height=768" />
20   <link rel="image_src" href="http://www.repubblica.it/images/homepage/la_repubblica_logo.gif" />
21   <link rel="canonical" href="http://www.repubblica.it/" />
22   <link rel="apple-touch-icon" href="http://www.repubblica.it/images/homepage/apple-touch-icon.png" />
23   <meta property="fb:app_id" content="124998494210426"/>
24   <link rel="search" type="application/opensearchdescription+xml" href="http://www.repubblica.it/static/p3/common/xml/opensearch_desc.xml" title="Cerc">
25   <meta name="verify-v1" content="eyc9D0eavGmlkEzy+Fza8G3Pn8F/a/2vZfVdJXkU=" />
26   <meta name="application-name" content="Repubblica.it" />
27   <link rel="alternate" media="handheld" href="http://m.repubblica.it/" />
28
29   <meta http-equiv="Refresh" content="300;URL=index.html?refresh_oc" />
30
31
32
33   <meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
34
35
36
37   <link rel="shortcut icon" type="image/x-icon" href="http://www.repubblica.it/static/images/homepage/2010/favicon.ico">
38   <link rel="stylesheet" href="http://www.repubblica.it/static/css/homepage/2010/homepage.css" type="text/css" media="all" />
39
40   <script type="text/javascript" src="http://www.repubblica.it/static/js/common/jquery.min.js"></script>
41   <script type="text/javascript" src="http://www.repubblica.it/static/js/homepage/2010/homepage.js"></script>
42   <!-- Do consentire per tutto del commenti
43   <script type="text/javascript" src="/javascript/swfobject.js"></script>
44   <script type="text/javascript" src="http://adagio.js.repubblica.it/uploads/js/repubblicoad.js"></script>
45   <script type="text/javascript" src="http://oas.js.kataweb.it/adsetup.js?hpre"></script>
46
47   <script type="text/javascript">
48     <script type="text/javascript">

```







Wireshark interface showing packet capture data. The packet list shows a series of HTTP requests and responses. The selected packet (1936) is an HTTP 1.1 200 OK response. The packet details pane shows the response structure, including the status line, headers, and the body content (HTML). The packet bytes pane shows the raw data in hexadecimal and ASCII.

Filter: tcp.stream eq 155

Packet List:

No.	Time	Source	Destination	Protocol	Info
1923	13.938306	137.204.231.102	209.85.229.102	TCP	saism > http [SYN] Seq=0 Win=64512 Len=0 MSS=1460
1924	13.970536	209.85.229.102	137.204.231.102	TCP	http > saism [ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
1925	13.970580	137.204.231.102	209.85.229.102	TCP	saism > http [ACK] Seq=1 Ack=1 Win=64512 Len=0
1926	13.970672	137.204.231.102	209.85.229.102	HTTP	GET /complete/search?output=firefox&client=firefox&hl=it&q=b HTTP/1.1
1927	14.000636	209.85.229.102	137.204.231.102	TCP	http > saism [ACK] Seq=1 Ack=480 Win=6432 Len=0
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=b HTTP/1.1
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
1936	16.192736	137.204.231.102	209.85.229.102	HTTP	GET /complete/search?output=firefox&client=firefox&hl=it&q=b HTTP/1.1

Packet Details:

[Coloring Rule String: http || tcp.port == 80]

Ethernet II, Src: All-HSRP-routers\_c8 (00:00:0c:07:ac:c8), Dst: Asustek\_74:a0:cc (00:23:54:74:a0:cc)

Internet Protocol, Src: 209.85.229.102 (209.85.229.102), Dst: 137.204.231.102 (137.204.231.102)

Transmission Control Protocol, Src Port: http (80), Dst Port: saism (1436), Seq: 363, Ack: 960, Len: 354

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

Date: Fri, 25 Mar 2011 16:13:17 GMT\r\n

Expires: Fri, 25 Mar 2011 16:13:17 GMT\r\n

Cache-Control: private, max-age=3600\r\n

Content-Type: text/javascript; charset=UTF-8\r\n

Content-Encoding: gzip\r\n

Server: gws\r\n

Content-Length: 84\r\n

X-XSS-Protection: 1; mode=block\r\n

\r\n

Content-encoded entity body (gzip): 84 bytes -> 100 bytes

Line-based text data: text/javascript

[\"bo\",[\"booking\", \"bollo auto\", \"bol\", \"borsa italiana\", \"bose\", \"borsa\", \"bologna\", \"book\", \"bosch\", \"bow\"]]

Wireshark interface showing packet capture data. The packet list shows a series of HTTP requests and responses. The selected packet (1936) is an HTTP 1.1 200 OK response. The packet details pane shows the response structure, including the status line, headers, and the body content (HTML). The packet bytes pane shows the raw data in hexadecimal and ASCII.

Filter: tcp.stream eq 155

Packet List:

No.	Time	Source	Destination	Protocol	Info
1923	13.938306	137.204.231.102	209.85.229.102	TCP	saism > http [SYN] Seq=0 Win=64512 Len=0 MSS=1460
1924	13.970536	209.85.229.102	137.204.231.102	TCP	http > saism [ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
1925	13.970580	137.204.231.102	209.85.229.102	TCP	saism > http [ACK] Seq=1 Ack=1 Win=64512 Len=0
1926	13.970672	137.204.231.102	209.85.229.102	HTTP	GET /complete/search?output=firefox&client=firefox&hl=it&q=b HTTP/1.1
1927	14.000636	209.85.229.102	137.204.231.102	TCP	http > saism [ACK] Seq=1 Ack=480 Win=6432 Len=0
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=b HTTP/1.1
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
1936	16.192736	137.204.231.102	209.85.229.102	HTTP	GET /complete/search?output=firefox&client=firefox&hl=it&q=b HTTP/1.1

Packet Details:

[Coloring Rule String: http || tcp.port == 80]

Ethernet II, Src: All-HSRP-routers\_c8 (00:00:0c:07:ac:c8), Dst: Asustek\_74:a0:cc (00:23:54:74:a0:cc)

Internet Protocol, Src: 209.85.229.102 (209.85.229.102), Dst: 137.204.231.102 (137.204.231.102)

Transmission Control Protocol, Src Port: http (80), Dst Port: saism (1436), Seq: 363, Ack: 960, Len: 354

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

Date: Fri, 25 Mar 2011 16:13:17 GMT\r\n

Expires: Fri, 25 Mar 2011 16:13:17 GMT\r\n

Cache-Control: private, max-age=3600\r\n

Content-Type: text/javascript; charset=UTF-8\r\n

Content-Encoding: gzip\r\n

Server: gws\r\n

Content-Length: 84\r\n

X-XSS-Protection: 1; mode=block\r\n

\r\n

Content-encoded entity body (gzip): 84 bytes -> 100 bytes

Line-based text data: text/javascript

[\"bo\",[\"booking\", \"bollo auto\", \"bol\", \"borsa italiana\", \"bose\", \"borsa\", \"bologna\", \"book\", \"bosch\", \"bow\"]]

# Estrazione di dati dall'intercettazione

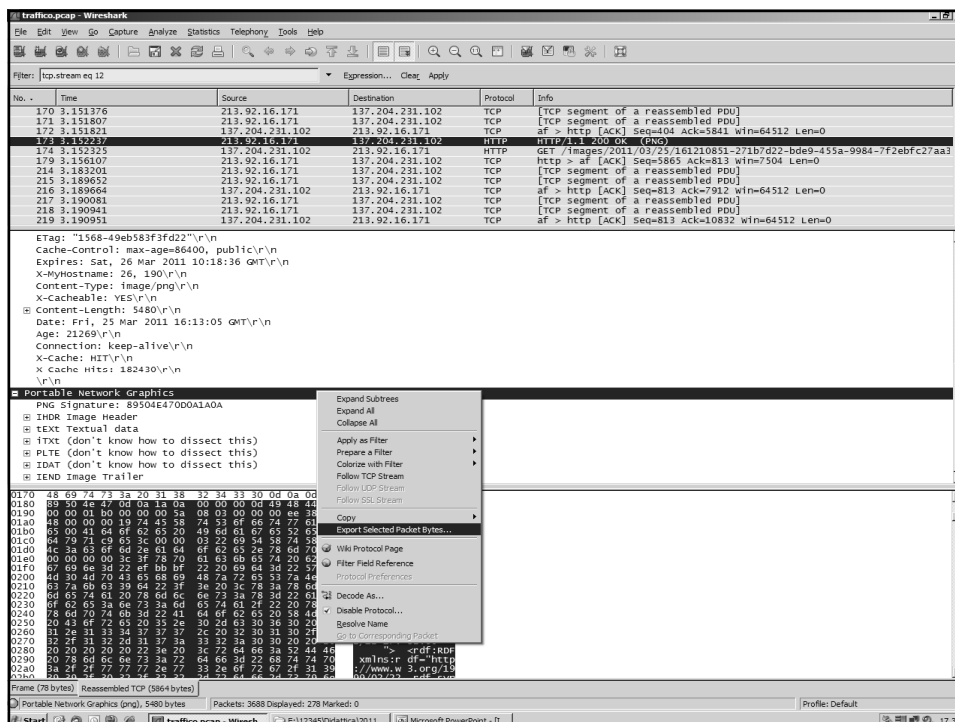
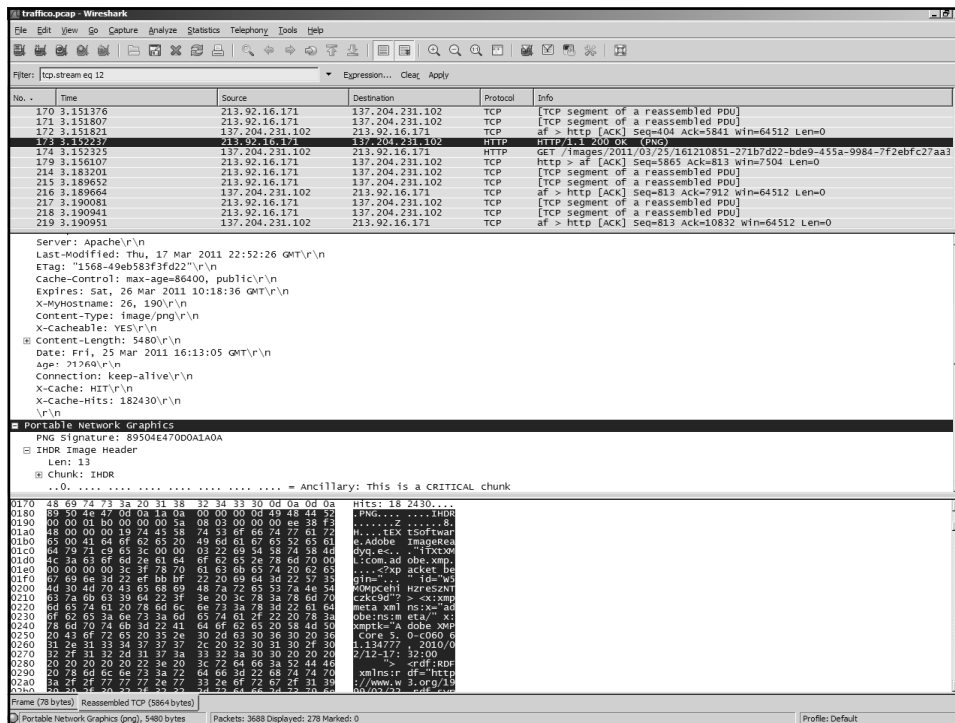
Wireshark interface showing packet capture data. The main pane displays a list of captured packets, including TCP segments and an HTTP GET request. The packet list shows details for packets 166 through 173, all originating from 137.204.231.102 and destined to 213.92.16.171. Packet 173 is highlighted, showing it is an HTTP GET request for the file /images/2011/03/25/161210851-271b7d22-bde9-455a-9984-7f2ebfc27aa3.

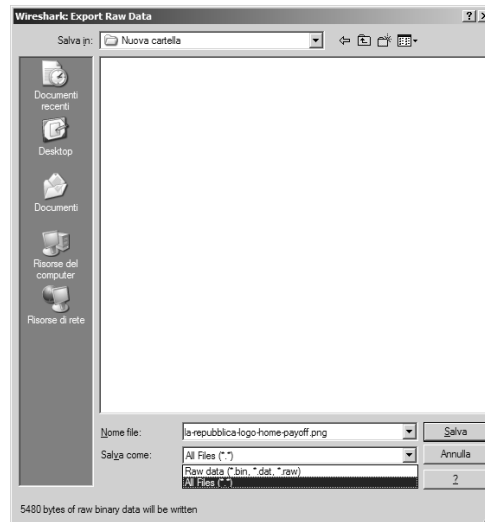
The packet details pane for packet 173 shows the following structure:

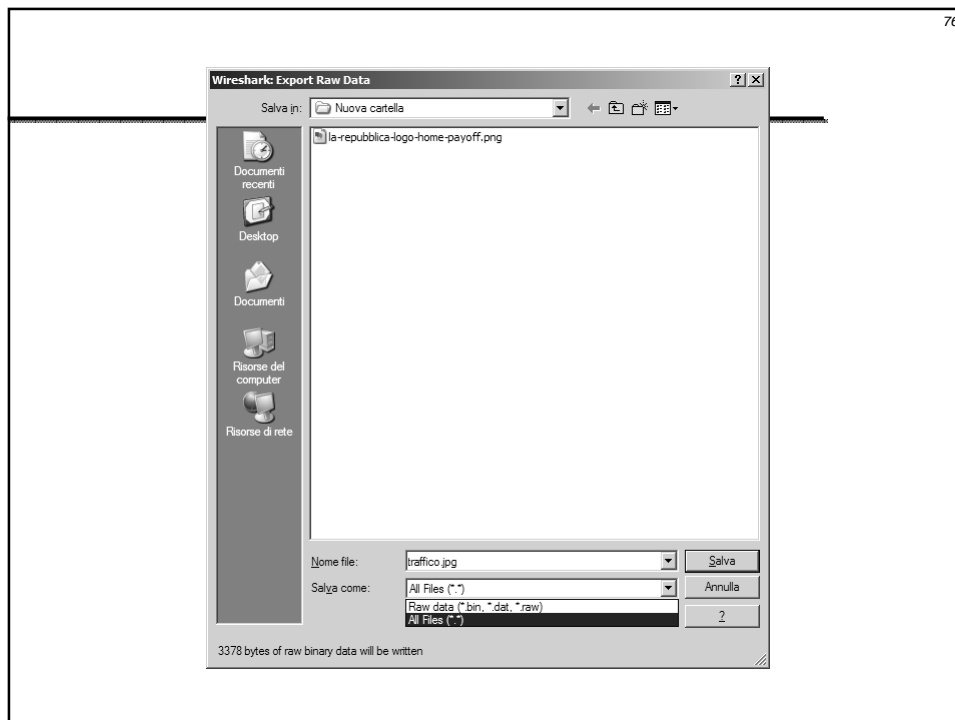
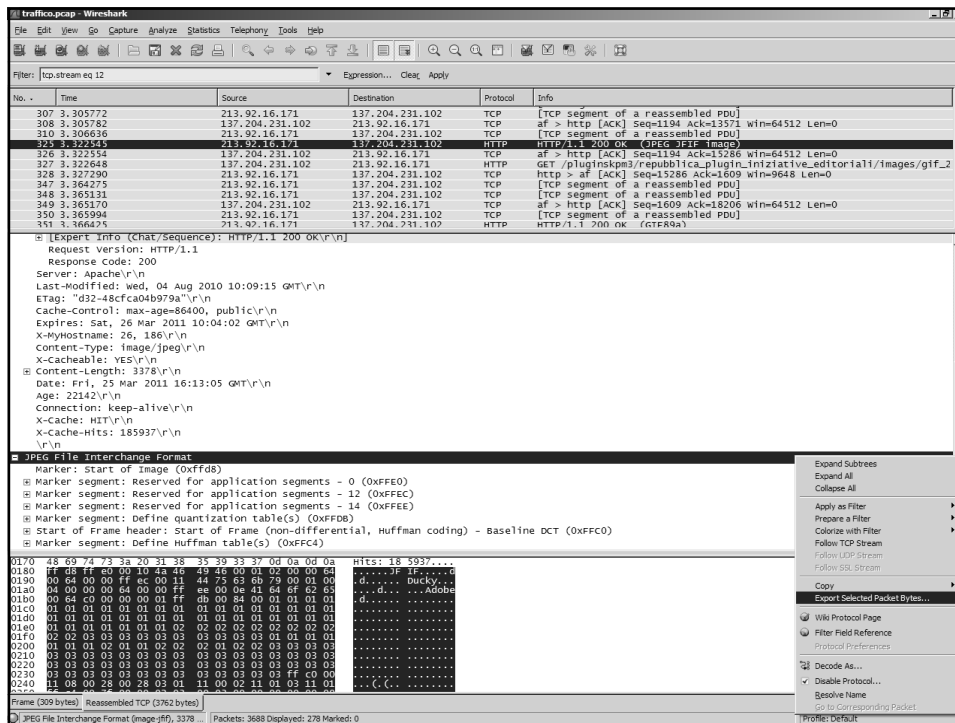
- Ethernet II, Src: All-MSRP-routers\_c8 (00:00:0c:07:ac:c8), Dst: Asustek\_74:a0:cc (00:23:54:74:a0:cc)
- Internet Protocol, Src: 137.204.231.102 (213.92.16.171), Dst: 137.204.231.102 (137.204.231.102)
- Transmission Control Protocol, Src Port: http (80), Dst Port: af (1413), Seq: 5841, Ack: 404, Len: 24
- (Reassembled TCP segments (5864 bytes): #160(1460), #161(1460), #170(1460), #171(1460), #173(24))
- Hypertext Transfer Protocol
  - [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
  - Request Version: HTTP/1.1
  - Response Code: 200

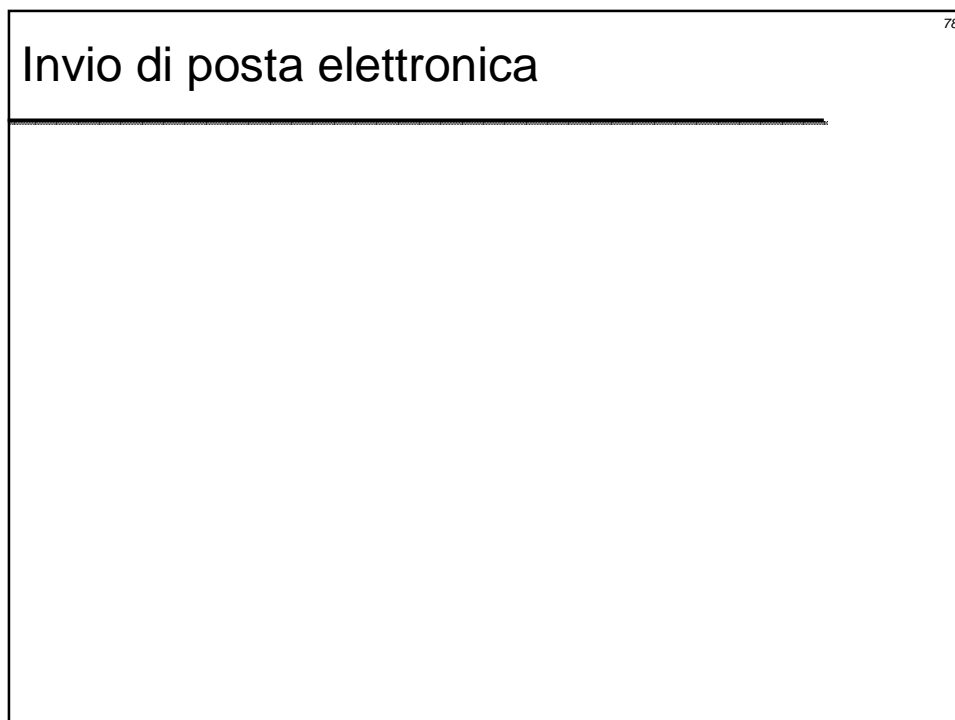
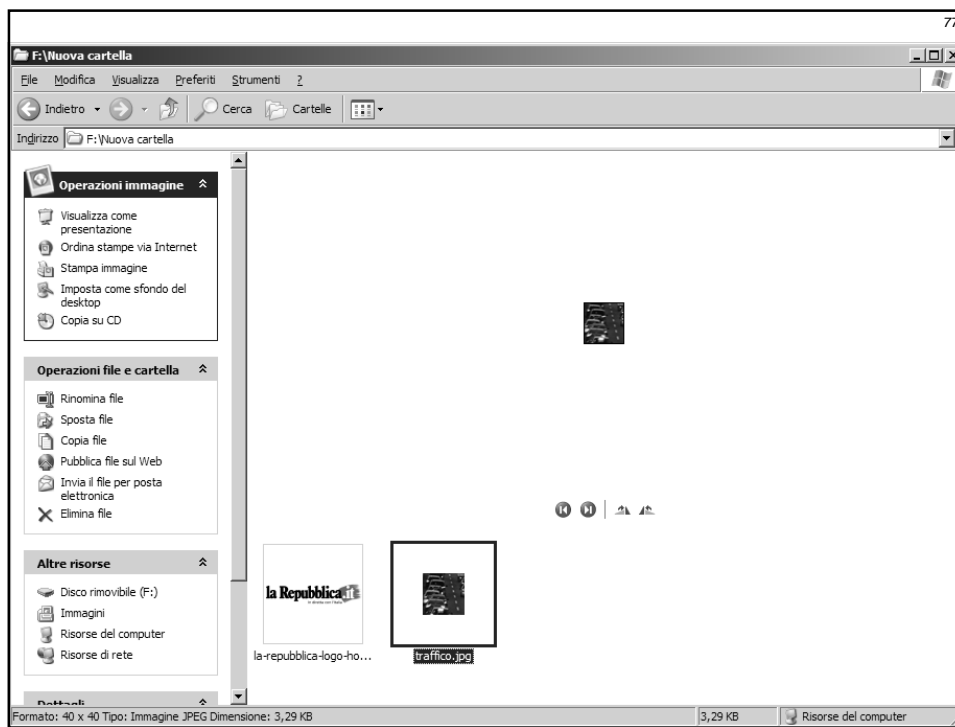
The packet bytes pane shows the raw data of the packet, including the HTTP response status line: HTTP/1.1 200 OK.











79

tráfico-inviopostapcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
16	3.583350	137.204.231.102	62.149.128.201	SMTP	C: GPFzc3dvcmQx
17	3.597942	62.149.128.201	137.204.231.102	SMTP	S: 235 ok, go ahead (#2.0.0)
18	3.598297	137.204.231.102	62.149.128.201	SMTP	C: MAIL FROM: <posta-1@micheleferrazzano.it>
19	3.625457	62.149.128.201	137.204.231.102	SMTP	S: 250 ok
20	3.625536	137.204.231.102	62.149.128.201	SMTP	C: RCPT TO: <posta-2@micheleferrazzano.it>
21	3.638356	62.149.128.201	137.204.231.102	SMTP	S: 250 ok
22	3.638424	137.204.231.102	62.149.128.201	SMTP	C: DATA
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
31	3.730467	137.204.231.102	62.149.128.201	TCP	hello > smtp [FIN, ACK] Seq=1426 Ack=246 Win=64267 Len=0

Acknowledgment Number: 1426 (Effective ACK Number)  
Header Length: 20 bytes  
Flags: 0x18 (PSH, ACK)  
Window Size: 64345  
Checksum: 0x9023 (validation disabled)  
[Seq/ACK analysis]  
Simple Mail Transfer Protocol  
Command: MAIL FROM: <posta-1@micheleferrazzano.it>\r\n  
Command: MAIL  
Request parameter: FROM: <posta-1@micheleferrazzano.it>

```

0000 00 00 0c 07 ac c8 00 23 54 74 a0 cc 08 00 45 00 .....# Tt...E.
0010 00 53 e8 03 40 00 80 06 e2 0f 89 cc e7 66 3e 95 .S.0...P>
0020 80 c9 06 fd 00 19 39 8b e7 34 cc d7 96 e8 50 18 .....9...P>
0030 fb 59 9b 23 00 00 4d 43 49 4c 20 00 00 00 00 .V.#.MAIL FROM:
0040 20 3c 70 67 23 74 61 2d 31 40 6d 69 63 68 65 64 <posta-1@miche
0050 65 66 65 72 72 61 7a 7a 61 6e 6f 2e 69 74 3e 0d eFerrazzano.it>
0060 0a

```

Request parameter (smtp.req.parameter), 36 b... Packets: 38 Displayed; 38 Marked; 0 Load time: 0:00.625 Profile: Default

80

tráfico-inviopostapcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
16	3.583350	137.204.231.102	62.149.128.201	SMTP	C: GPFzc3dvcmQx
17	3.597942	62.149.128.201	137.204.231.102	SMTP	S: 235 ok, go ahead (#2.0.0)
18	3.598297	137.204.231.102	62.149.128.201	SMTP	C: MAIL FROM: <posta-1@micheleferrazzano.it>
19	3.625457	62.149.128.201	137.204.231.102	SMTP	S: 250 ok
20	3.625536	137.204.231.102	62.149.128.201	SMTP	C: RCPT TO: <posta-2@micheleferrazzano.it>
21	3.638356	62.149.128.201	137.204.231.102	SMTP	S: 250 ok
22	3.638424	137.204.231.102	62.149.128.201	SMTP	C: DATA
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
31	3.730467	137.204.231.102	62.149.128.201	TCP	hello > smtp [FIN, ACK] Seq=1426 Ack=246 Win=64267 Len=0

Acknowledgment Number: 1426 (Effective ACK Number)  
Header Length: 20 bytes  
Flags: 0x18 (PSH, ACK)  
Window Size: 64337  
Checksum: 0x0e31 (validation disabled)  
[Seq/ACK analysis]  
Simple Mail Transfer Protocol  
Command: RCPT TO: <posta-2@micheleferrazzano.it>\r\n  
Request parameter: TO: <posta-2@micheleferrazzano.it>

```

0000 00 00 0c 07 ac c8 00 23 54 74 a0 cc 08 00 45 00 .....# Tt...E.
0010 00 51 e8 04 40 00 80 06 e2 10 89 cc e7 66 3e 95 .Q.0...P>
0020 80 c9 06 fd 00 19 39 8b e7 3f cc d7 96 f0 50 18 .....9...P>
0030 fb 51 0e 31 00 00 52 43 30 34 20 54 4f 3a 20 34 .Q.1...RCPT TO:
0040 20 3c 70 67 23 74 61 2d 31 40 6d 69 63 68 65 64 <posta-2@michelef
0050 65 72 72 61 7a 7a 61 6e 6f 2e 69 74 3e 0d 0a eFerrazzano.it>

```

Text item (text), 41 bytes Packets: 38 Displayed; 38 Marked; 0 Load time: 0:00.625 Profile: Default



81

Wifalico-inviopostapcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
22	3.652559	137.204.231.102	62.149.128.201	SMTP	C: DATA
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@micheleferazzano.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: AsustekC74iA0: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]

Sequence numbers: 179 (relative sequence number)

0030 fb 3b f9 24 00 00 4d 65 73 73 61 67 65 2d 49 44 ...:..Message-ID:  
0040 88 20 3c 38 34 43 32 44 41 33 45 38 41 38 44 34 ...:88203c38344332444133453841384434  
0050 38 46 34 41 44 32 46 32 31 41 41 37 37 43 31 41 ...:88463441443246323141413737433141  
0060 32 43 44 40 70 65 72 73 6f 6e 61 6c 65 2e 64 69 ...:32434440706572736f6e616c652e6469  
0070 72 2e 75 6e 69 62 6f 2e 69 74 3e 0d 0a 46 72 6f ...:722e756e69626f2e69743e0d0a46726f  
0080 6d 3a 20 22 50 6f 73 74 61 20 31 22 20 3c 70 6f ...:6d3a2022506f737461203122203c706f  
0090 73 74 61 20 31 40 6d 69 63 68 65 6c 65 66 63 72 ...:7374612031406d696368656c65666372  
00a0 72 61 7a 7a 61 6e 6f 2e 69 74 3e 0d 0a 54 6f 3a ...:72617a7a616e6f2e69743e0d0a546f3a  
00b0 20 3c 70 6f 73 74 61 2d 32 40 6d 69 63 68 65 6c ...:203c706f7374612d32406d696368656c  
00c0 65 66 63 72 72 61 7a 61 6e 6f 2e 69 74 3e 0d ...:6566637272617a616e6f2e69743e0d  
00d0 0a 53 75 62 6a 65 63 74 3a 20 4d 61 69 6c 20 64 ...:0a5375626a6563743a204d61696c2064  
00e0 69 20 70 72 6f 76 61 0d 0a 44 61 74 65 3a 20 46 ...:692070726f76610d0a446174653a2046  
00f0 72 69 2c 20 32 35 20 4d 61 72 20 32 30 31 31 20 ...:72692c203235204d6172203230313120  
0100 31 38 3a 30 31 3a 35 39 20 2b 30 31 30 30 0d 0a ...:31383a30313a3539202b303130300d0a  
0110 4d 49 4d 43 2d 36 65 72 73 69 6f 6e 3a 20 31 2e ...:4d494d432d36657273696f6e3a20312e  
0120 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 63 3a ...:0d0a436f6e74656e742d547970633a  
0130 20 6d 74 6e 74 69 70 61 72 74 2f 61 6c 74 65 72 ...:206d746e7469706172742f616c746572  
0140 6e 61 74 69 76 65 3b 0d 0a 09 62 6f 75 6e 64 61 ...:6e61746976653b0d0a09626f756e6461  
0150 72 79 3d 22 2d 2d 2d 2d 3d 3f 4e 65 78 74 50 61 ...:72793d222d2d2d2d3d3f4e6578745061  
0160 72 74 5f 30 30 3f 30 30 43 3f 30 31 43 43 ...:72745f30303f3030433f30314343  
0170 45 42 31 36 2e 42 43 38 46 41 37 31 30 22 0d 0a ...:454231362e4243384641373130220d0a  
0180 58 2d 50 72 69 6f 72 69 74 79 3a 20 33 0d 0a 58 ...:582d5072696f726974793a20330d0a58  
0190 2d 4d 53 4d 69 6c 0d 50 72 69 6f 72 69 74 79 ...:2d4d534d696c0d5072696f72697479  
01a0 3a 20 46 6f 72 6d 61 6c 0d 0a 58 2d 4d 61 69 6c ...:3a20466f726d616c0d0a582d4d61696c  
01b0 65 72 3a 20 4d 69 63 72 6f 73 6f 66 74 20 4f 73 ...:65723a204d6963726f736f6674204f73  
01c0 74 6c 6f 6b 20 45 78 70 72 65 73 73 20 36 2e ...:746c6f6b204578707265737320362e  
01d0 24 26 23 43 43 43 43 43 43 43 43 43 43 43 43 ...:242623434343434343434343434343

Simple Mail Transfer Protocol (smtp), 1236 bytes Packets: 38 Displayed: 38 Marked: 0 Load time: 0:00:625 Profile: Default

82

Wifalico-inviopostapcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
22	3.652559	137.204.231.102	62.149.128.201	SMTP	C: DATA
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@micheleferazzano.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]

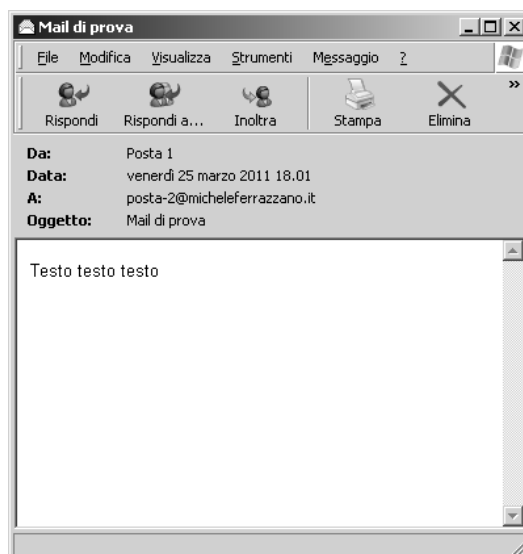
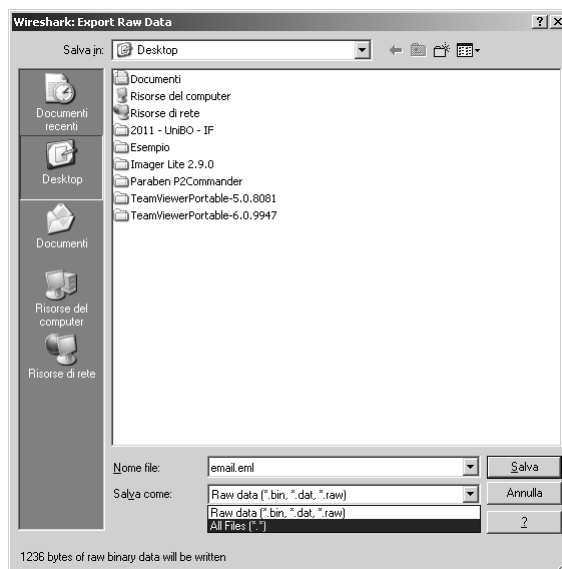
Simple Mail Transfer Protocol

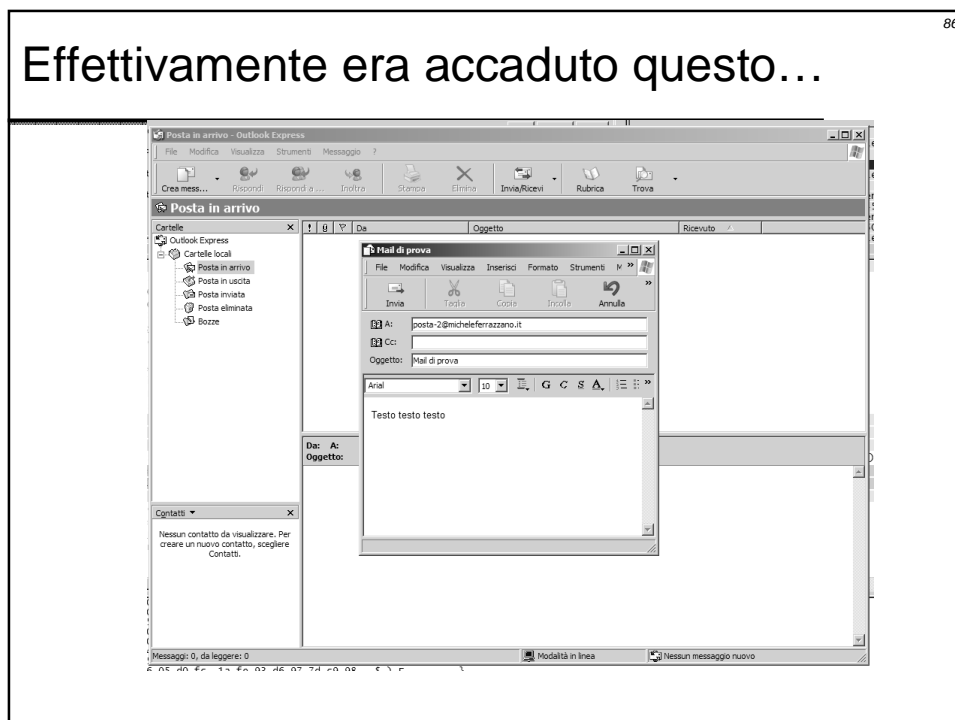
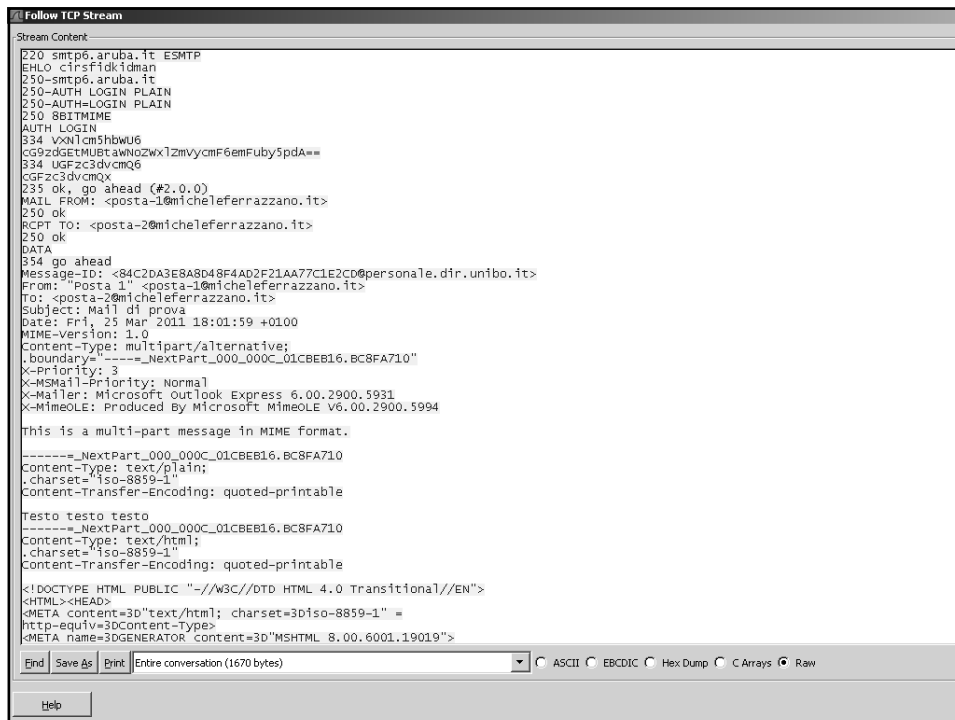
Reassembled DATA in frame: 26

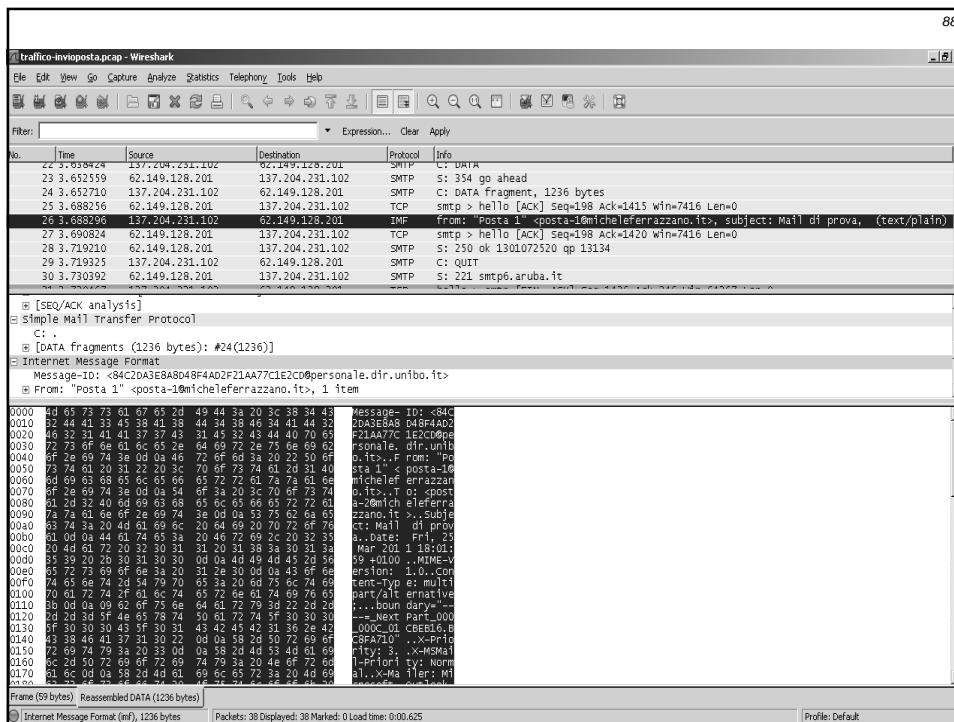
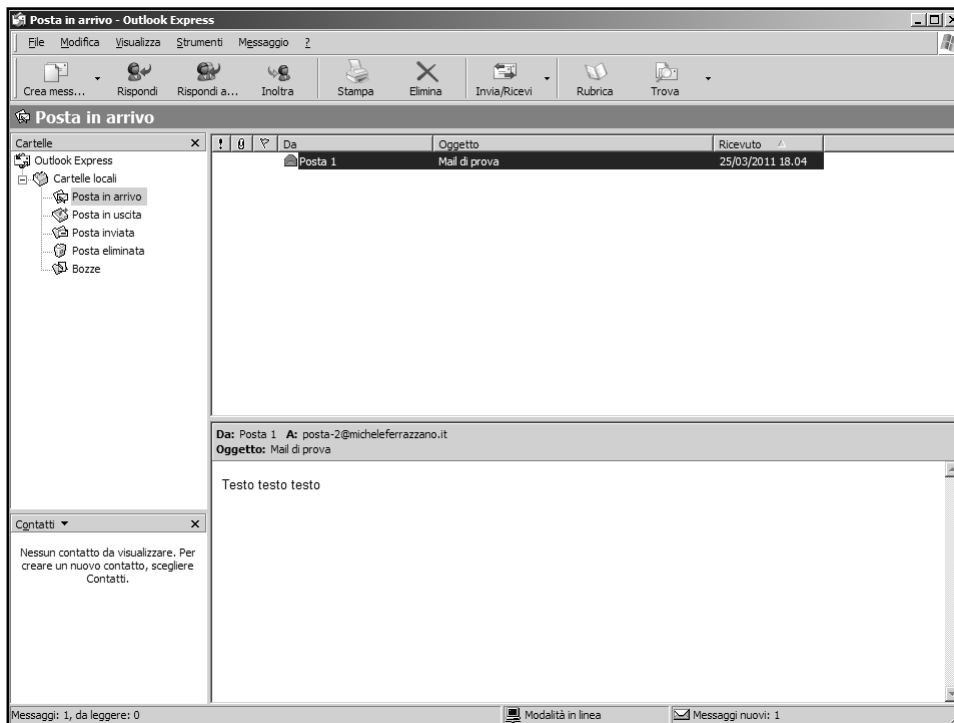
0030 fb 3b f9 24 00 00 4d 65 73 73 61 67 65 2d 49 44 ...:..Message-ID:  
0040 88 20 3c 38 34 43 32 44 41 33 45 38 41 38 44 34 ...:88203c38344332444133453841384434  
0050 38 46 34 41 44 32 46 32 31 41 41 37 37 43 31 41 ...:38463441443246323141413737433141  
0060 32 43 44 40 70 65 72 73 6f 6e 61 6c 65 2e 64 69 ...:32434440706572736f6e616c652e6469  
0070 72 2e 75 6e 69 62 6f 2e 69 74 3e 0d 0a 46 72 6f ...:722e756e69626f2e69743e0d0a46726f  
0080 6d 3a 20 22 50 6f 73 74 61 20 31 22 20 3c 70 6f ...:6d3a2022506f737461203122203c706f  
0090 73 74 61 20 31 40 6d 69 63 68 65 6c 65 66 63 72 ...:7374612031406d696368656c65666372  
00a0 72 61 7a 7a 61 6e 6f 2e 69 74 3e 0d 0a 54 6f 3a ...:72617a7a616e6f2e69743e0d0a546f3a  
00b0 20 3c 70 6f 73 74 61 2d 32 40 6d 69 63 68 65 6c ...:203c706f7374612d32406d696368656c  
00c0 65 66 63 72 72 61 7a 61 6e 6f 2e 69 74 3e 0d ...:6566637272617a616e6f2e69743e0d  
00d0 0a 53 75 62 6a 65 63 74 3a 20 4d 61 69 6c 20 64 ...:0a5375626a6563743a204d61696c2064  
00e0 69 20 70 72 6f 76 61 0d 0a 44 61 74 65 3a 20 46 ...:692070726f76610d0a446174653a2046  
00f0 72 69 2c 20 32 35 20 4d 61 72 20 32 30 31 31 20 ...:72692c203235204d6172203230313120  
0100 31 38 3a 30 31 3a 35 39 20 2b 30 31 30 30 0d 0a ...:31383a30313a3539202b303130300d0a  
0110 4d 49 4d 43 2d 36 65 72 73 69 6f 6e 3a 20 31 2e ...:4d494d432d36657273696f6e3a20312e  
0120 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 63 3a ...:0d0a436f6e74656e742d547970633a  
0130 20 6d 74 6e 74 69 70 61 72 74 2f 61 6c 74 65 72 ...:206d746e7469706172742f616c746572  
0140 6e 61 74 69 76 65 3b 0d 0a 09 62 6f 75 6e 64 61 ...:6e61746976653b0d0a09626f756e6461  
0150 72 79 3d 22 2d 2d 2d 2d 3d 3f 4e 65 78 74 50 61 ...:72793d222d2d2d2d3d3f4e6578745061  
0160 72 74 5f 30 30 3f 30 30 43 3f 30 31 43 43 ...:72745f30303f3030433f30314343  
0170 45 42 31 36 2e 42 43 38 46 41 37 31 30 22 0d 0a ...:454231362e4243384641373130220d0a  
0180 58 2d 50 72 69 6f 72 69 74 79 3a 20 33 0d 0a 58 ...:582d5072696f726974793a20330d0a58  
0190 2d 4d 53 4d 69 6c 0d 50 72 69 6f 72 69 74 79 ...:2d4d534d696c0d5072696f72697479  
01a0 3a 20 46 6f 72 6d 61 6c 0d 0a 58 2d 4d 61 69 6c ...:3a20466f726d616c0d0a582d4d61696c  
01b0 65 72 3a 20 4d 69 63 72 6f 73 6f 66 74 20 4f 73 ...:65723a204d6963726f736f6674204f73  
01c0 74 6c 6f 6b 20 45 78 70 72 65 73 73 20 36 2e ...:746c6f6b204578707265737320362e  
01d0 24 26 23 43 43 43 43 43 43 43 43 43 43 43 43 ...:242623434343434343434343434343

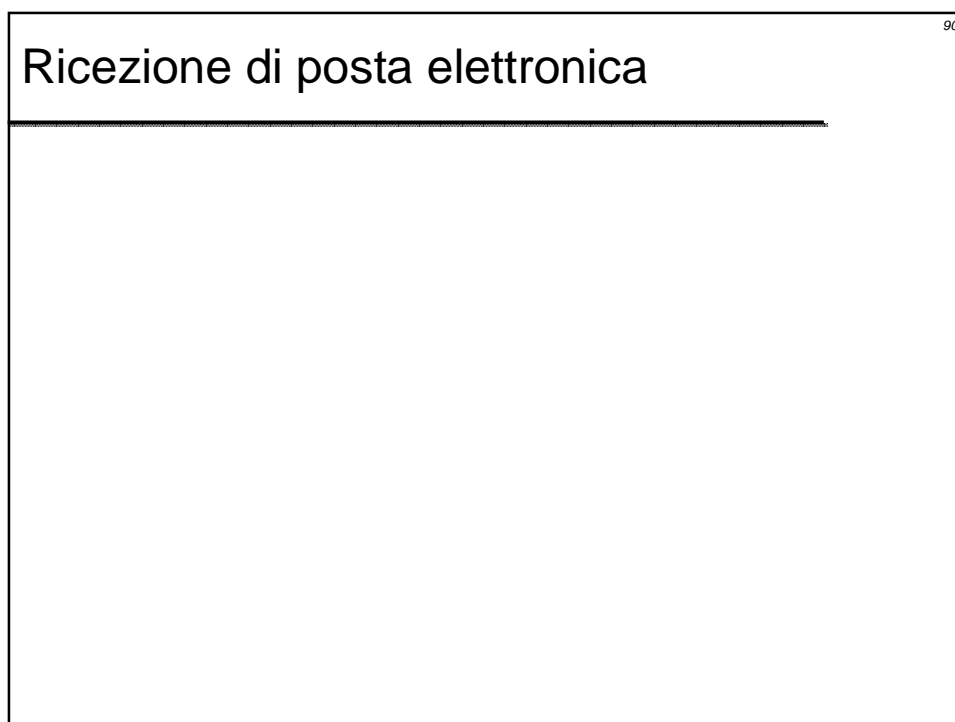
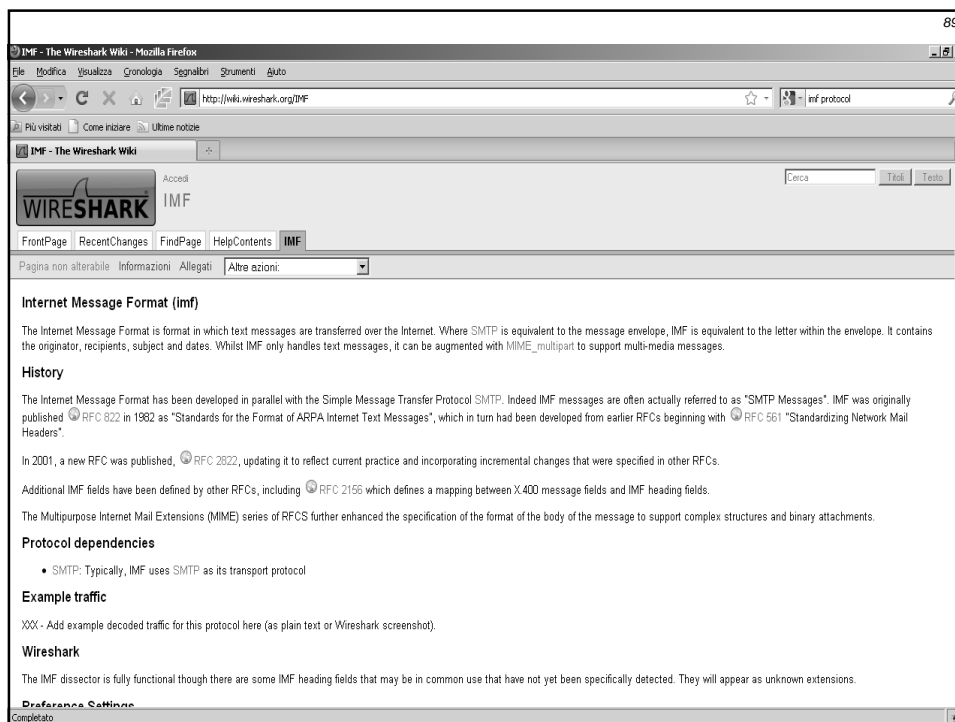
Simple Mail Transfer Protocol (smtp), 1236 bytes Packets: 38 Displayed: 38 Marked: 0 Load time: 0:00:625 Profile: Default

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 SCTP 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









[[ traffico-ricerzonepostapcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
7	1.776305	AsustekC_74:80:c	BFO10C33	ARP	Who has 137.204.231.254? Tell 137.204.231.102
8	1.776894	All-HSRP-routers_c8	AsustekC_74:80:c	ARP	137.204.231.254 is at 00:00:0c:07:ac:c8
9	1.776903	137.204.231.102	62.149.128.161	TCP	cera-bcm > pop3 [SYN] Seq=0 Win=64512 Len=0 MSS=1460 SACK_PERM=1
10	1.777534	62.149.128.161	137.204.231.102	TCP	pop3 > cera-bcm [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
11	1.777652	137.204.231.102	62.149.128.161	TCP	cera-bcm > pop3 [ACK] Seq=1 Ack=1 Win=64512 Len=0
12	1.800521	62.149.128.161	137.204.231.102	POP	S: +OK <6153.130107268@popd11.ad.aruba.it>
13	1.800717	137.204.231.102	62.149.128.161	POP	C: USER posta-2@micheleferrazzano.it
14	1.801099	62.149.128.161	137.204.231.102	TCP	pop3 > cera-bcm [ACK] Seq=43 Ack=36 Win=5840 Len=0
15	1.811907	62.149.128.161	137.204.231.102	POP	S: +OK
16	1.811969	137.204.231.102	62.149.128.161	POP	C: PASS password2
17	1.844191	62.149.128.161	137.204.231.102	TCP	pop3 > cera-bcm [ACK] Seq=49 Ack=52 Win=5840 Len=0
18	1.866754	62.149.128.161	137.204.231.102	POP	S: +OK
19	1.867294	137.204.231.102	62.149.128.161	POP	C: STAT
20	1.867672	62.149.128.161	137.204.231.102	TCP	pop3 > cera-bcm [ACK] Seq=55 Ack=58 Win=5840 Len=0

Window size: 64470  
Checksum: 0xbf55 (validation disabled)  
[SEQ/ACK analysis]  
Post Office Protocol  
USER posta-2@micheleferrazzano.it\r\n  
Request command: USER  
Request parameter: posta-2@micheleferrazzano.it

```

0000 00 00 0c 07 ac c8 00 23 54 74 a0 cc 08 00 45 00 .....#Tt...E.
0010 00 4b e8 9d 40 00 80 06 e1 b1 89 cc e7 66 3e 95 ...K.0... ..P.
0020 80 a1 07 02 00 6e df 91 e7 b3 92 26 49 01 50 18 ....n... ..P.
0030 fb d6 bf 55 00 00 55 53 45 92 20 70 6f 73 74 61 ...U..S ER posta
0040 20 32 40 ed 69 63 68 65 6c 65 66 65 72 72 61 7d ...michele ferraz
0050 7a 61 66 6f 3e 69 74 0d 0a .....ano.it...

```

[[ traffico-ricerzonepostapcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
12	1.800521	62.149.128.161	137.204.231.102	POP	S: +OK <6153.130107268@popd11.ad.aruba.it>
13	1.800717	137.204.231.102	62.149.128.161	POP	C: USER posta-2@micheleferrazzano.it
14	1.801099	62.149.128.161	137.204.231.102	TCP	pop3 > cera-bcm [ACK] Seq=43 Ack=36 Win=5840 Len=0
15	1.811907	62.149.128.161	137.204.231.102	POP	S: +OK
16	1.811969	137.204.231.102	62.149.128.161	POP	C: PASS password2
17	1.844191	62.149.128.161	137.204.231.102	TCP	pop3 > cera-bcm [ACK] Seq=49 Ack=52 Win=5840 Len=0
18	1.866754	62.149.128.161	137.204.231.102	POP	S: +OK
19	1.867294	137.204.231.102	62.149.128.161	POP	C: STAT
20	1.867672	62.149.128.161	137.204.231.102	TCP	pop3 > cera-bcm [ACK] Seq=55 Ack=58 Win=5840 Len=0

Flags: 0x18 (PSH, ACK)  
Window size: 5840  
Checksum: 0x3b2f (validation disabled)  
[SEQ/ACK analysis]  
Post Office Protocol  
+OK \r\n  
Response indicator: +OK

```

0000 00 23 54 74 a0 cc 00 00 0c 07 ac c8 08 00 45 00 ..#Tt... ..E.
0010 00 2e ec e3 40 00 40 06 1d 7d 3e 95 80 a1 89 cc ...0.0. .>.....
0020 e7 6e 00 6e 07 02 92 26 49 01 df 91 e7 ba 50 18 ....n... ..P.
0030 16 d0 3b 2f 00 00 2b 4f 4b 20 0d 0a .....K...

```

[[ traffico-ricerzonepostapcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
12	1.800521	62.149.128.161	137.204.231.102	POP	S: +OK <6153.130107268@popd11.ad.aruba.it>
13	1.800717	137.204.231.102	62.149.128.161	POP	C: USER posta-2@micheleferrazzano.it
14	1.801099	62.149.128.161	137.204.231.102	TCP	pop3 > cera-bcm [ACK] Seq=43 Ack=36 Win=5840 Len=0
15	1.811907	62.149.128.161	137.204.231.102	POP	S: +OK
16	1.811969	137.204.231.102	62.149.128.161	POP	C: PASS password2
17	1.844191	62.149.128.161	137.204.231.102	TCP	pop3 > cera-bcm [ACK] Seq=49 Ack=52 Win=5840 Len=0
18	1.866754	62.149.128.161	137.204.231.102	POP	S: +OK
19	1.867294	137.204.231.102	62.149.128.161	POP	C: STAT
20	1.867672	62.149.128.161	137.204.231.102	TCP	pop3 > cera-bcm [ACK] Seq=55 Ack=58 Win=5840 Len=0

Flags: 0x18 (PSH, ACK)  
Window size: 64464  
Checksum: 0x5ff9 (validation disabled)  
[SEQ/ACK analysis]  
Post Office Protocol  
PASS password2\r\n  
Request command: PASS

```

0000 00 00 0c 07 ac c8 00 23 54 74 a0 cc 08 00 45 00 .....#Tt...E.
0010 00 38 e8 92 40 00 80 06 e1 c3 89 cc e7 66 3e 95 ...8.0... ..P.
0020 80 a1 07 02 00 6e df 91 e7 ba 92 26 49 07 50 18 ....n... ..P.
0030 fb d0 5f f9 00 00 50 41 93 93 20 70 61 73 72 77 ...BA SS passw
0040 8a 72 53 3a 00 00 .....

```

[[ traffico-ricerzonepostapcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
12	1.800521	62.149.128.161	137.204.231.102	POP	S: +OK <6153.130107268@popd11.ad.aruba.it>
13	1.800717	137.204.231.102	62.149.128.161	POP	C: USER posta-2@micheleferrazzano.it
14	1.801099	62.149.128.161	137.204.231.102	TCP	pop3 > cera-bcm [ACK] Seq=43 Ack=36 Win=5840 Len=0
15	1.811907	62.149.128.161	137.204.231.102	POP	S: +OK
16	1.811969	137.204.231.102	62.149.128.161	POP	C: PASS password2
17	1.844191	62.149.128.161	137.204.231.102	TCP	pop3 > cera-bcm [ACK] Seq=49 Ack=52 Win=5840 Len=0
18	1.866754	62.149.128.161	137.204.231.102	POP	S: +OK
19	1.867294	137.204.231.102	62.149.128.161	POP	C: STAT
20	1.867672	62.149.128.161	137.204.231.102	TCP	pop3 > cera-bcm [ACK] Seq=55 Ack=58 Win=5840 Len=0

Flags: 0x18 (PSH, ACK)  
Window size: 5840  
Checksum: 0x3b19 (validation disabled)  
[SEQ/ACK analysis]  
Post Office Protocol  
+OK \r\n  
Response indicator: +OK

```

0000 00 23 54 74 a0 cc 00 00 0c 07 ac c8 08 00 45 00 ..#Tt... ..E.
0010 00 2e ec e3 40 00 40 06 1d 7b 3e 95 80 a1 89 cc ...0.0. .>.....
0020 e7 6e 00 6e 07 02 92 26 49 07 df 91 e7 ca 50 18 ....n... ..P.
0030 16 d0 3b 19 00 00 2b 4f 4b 20 0d 0a .....K...

```

93

traliccio-nicezonepostapcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
23	1.890436	62.149.128.161	137.204.231.102	POP	S: +OK
24	2.069788	137.204.231.102	62.149.128.161	TCP	cera-bcm > pop3 [ACK] Seq=64 Win=64440 Len=0
25	2.070212	62.149.128.161	137.204.231.102	IMF	
26	2.071172	137.204.231.102	62.149.128.161	POP	C: RETR 1
27	2.074078	3compuo017bifa	Spanning-tree (for-br>STP	Conf.	Root = 32768/0/00:1a:c1:0f:7b:c9 Cost = 0 Port = 0x8031
28	2.107621	62.149.128.161	137.204.231.102	TCP	pop3 > cera-bcm [ACK] Seq=84 Ack=72 Win=5840 Len=0
29	2.108048	62.149.128.161	137.204.231.102	POP	S: +OK
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=7374 Win=64512 Len=0

Window size: 5840  
Checksum: 0x0875 [validation disabled]  
[SEQ/ACK analysis]

Post Office Protocol

+OK \r\n  
Response indicator: +OK  
Return-Path: <posta-1@micheleferrazzano.it>\r\n

0030 16 00 08 75 00 00 2b 4f 4b 20 0d 0a 52 65 74 73 ...u...Po K...Retu  
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...  
0050 31 40 6d 69 63 68 65 6c 65 06 65 72 72 61 7a 7a ...michel eferrazz  
0060 61 6e 6f 2e 69 74 3e 0d 0a 44 65 6c 69 76 65 72 ...ano, it>...delive  
0070 65 64 2d 34 6f 3a 20 70 6f 73 74 61 2d 32 40 6d ...ed-To: p osta-2@m  
0080 69 63 68 65 6c 65 66 65 70 72 61 7a 61 6e 6f ...michele ferrazzano  
0090 2e 69 74 0d 0a 32 65 63 65 69 76 65 64 3a 20 28 ...it, received: (C  
00a0 71 6d 61 69 6c 20 31 34 37 35 34 20 69 6e 76 6f ...mail 14 754 invo  
00b0 65 64 2d 32 40 6d 79 20 71 69 64 20 38 39 29 39 73 ...ed by uid 89):  
00c0 32 33 20 4d 61 72 20 32 30 31 31 20 31 37 3a 30 ...25 Mar 2 01:17:0  
00d0 34 3a 38 20 2d 30 30 30 30 0d 0a 52 65 63 63 ...4:08 -00 00...Rece  
00e0 69 76 65 64 3a 20 62 79 20 73 69 6d 73 63 61 6e ...lived: by simscan  
00f0 20 31 2e 32 4e 20 70 70 69 64 3a 20 31 34 36 ...1.2.0 p pid: 146  
0100 36 30 2c 20 70 69 64 3a 20 31 34 37 30 30 2c 20 ...60, pid: 14700,  
0110 74 3a 20 30 2e 32 30 33 39 73 0d 0a 20 20 20 20 ...t: 0.203 9s.,  
0120 20 20 20 20 73 61 6e 6e 65 72 73 3a 20 63 ...scanners: c  
0130 6c 61 6d 61 76 3a 20 30 2e 39 36 2e 33 0d 65 78 ...lamav: 0.96,5-exp  
0140 70 2f 6d 3a 35 33 2f 64 3a 31 32 33 33 38 20 73 ...o/m:53/d:12338 5  
0150 70 61 6d 3a 20 33 2e 33 2e 31 0d 0a 58 2d 53 70 ...spam: 3.3 1..X-Sp  
0160 61 6d 2d 43 68 65 63 68 65 72 2d 16 65 72 73 69 ...am-check er-versi  
0170 6f 6e 3a 20 53 70 61 6d 41 73 73 61 73 73 69 6e ...on: Spam Assassin  
0180 20 33 2e 33 2e 31 20 28 32 30 31 30 2d 30 33 2d ...3.3.1 ( 2010-03-  
0190 61 38 29 20 6d 78 61 76 61 73 2e 61 ...10) on mxavas7.a  
01a0 64 2e 61 73 75 62 61 2e 69 74 0d 0a 58 2d 53 70 ...d.aruba, it..X-Sp  
01b0 61 6d 2d 4c 65 76 65 6c 3a 20 0d 0a 58 2d 53 70 ...am-Level: ..X-Sp  
01c0 61 6d 2d 53 74 61 74 73 73 3a 20 4e 6f 2c 20 73 ...am-Statu si: No, 5  
01d0 62 2e 73 64 61 74 20 30 31 34 37 30 30 2c 20 ...t: 0.203 9s.,

Post Office Protocol (pop), 1460 bytes Packets: 43 Displayed: 43 Marked: 0 Load time: 0:00.000 Profile: Default

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: (mail 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 smtp1q01.aruba.it) (62.149.158.32)
by mxavas7.ad.aruba.it with SMTP; 25 Mar 2011 17:04:07 -0000
Received: (mail 18252 invoked by uid 89); 25 Mar 2011 17:01:59 -0000
Received: from unknown (HELO smtp6.aruba.it) (62.149.158.226)
by smtp1q01.aruba.it with SMTP; 25 Mar 2011 17:01:59 -0000
Received: (mail 13134 invoked by uid 89); 25 Mar 2011 17:02:00 -0000
Received: from unknown (HELO clrsfjgk1dman) (posta-1@micheleferrazzano.it@137.204.231.102)
by smtp6.ad.aruba.it with SMTP; 25 Mar 2011 17:02:00 -0000
Message-ID: <84c20a3e8a8d48f4ad2f21aa77c1e2cd@personale.dfr.unibo.it>
From: <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_01CBE816_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_01CBE816_BC8FA710
Content-Type: text/plain;
charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
```

End Save As Print Entire conversation (2470 bytes) ASCII EBCDIC Hex Dump C Arrays Raw

Help

The screenshot displays the Wireshark network protocol analyzer interface. The title bar indicates the file being analyzed is "traffico-riczioneposta.pcap - Wireshark".

**Menu Bar:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Help.

**Toolbar:** Contains icons for common actions like opening files, saving, zooming, and filtering.

**Filter Bar:** Shows the current filter expression as "Expression... Clear Apply".

**Packet List Panel:** Displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, and Info.

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	2.110953	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

**Packet Details Panel:** Provides a hierarchical view of the selected packet's structure.

- windows size: 64512
- # Checksum: 0x1271 [validation disabled]
- # [seq/ack analysis]
- # Post office Protocol
- ☐ DELE 1\r\n
  - Request command: DELE
  - Request parameter: 1

**Packet Bytes Panel:** Shows the raw hexadecimal and ASCII representation of the packet data.

```

0000 00 00 0c 07 ac c8 00 23 54 74 a0 cc 08 00 45 00 .....# TE....E.
0010 00 30 e8 98 40 00 80 06 e1 c5 89 cc e7 66 3e 95 ...0..0.....F..
0020 80 a1 07 02 00 06 df 91 e7 de 92 26 52 1c 50 18 .....n....GR.P.
0030 fc 00 12 71 00 00 ..N 45 4c 45 20 31 0d 06 ....q..DE LE 1..
  
```

**Status Bar:** Located at the bottom, it shows summary information: "Request (pop.request), 8 bytes", "Packets: 43 Displayed: 31 Marked: 0 Load time: 0:00.000", and "Profile: Default".