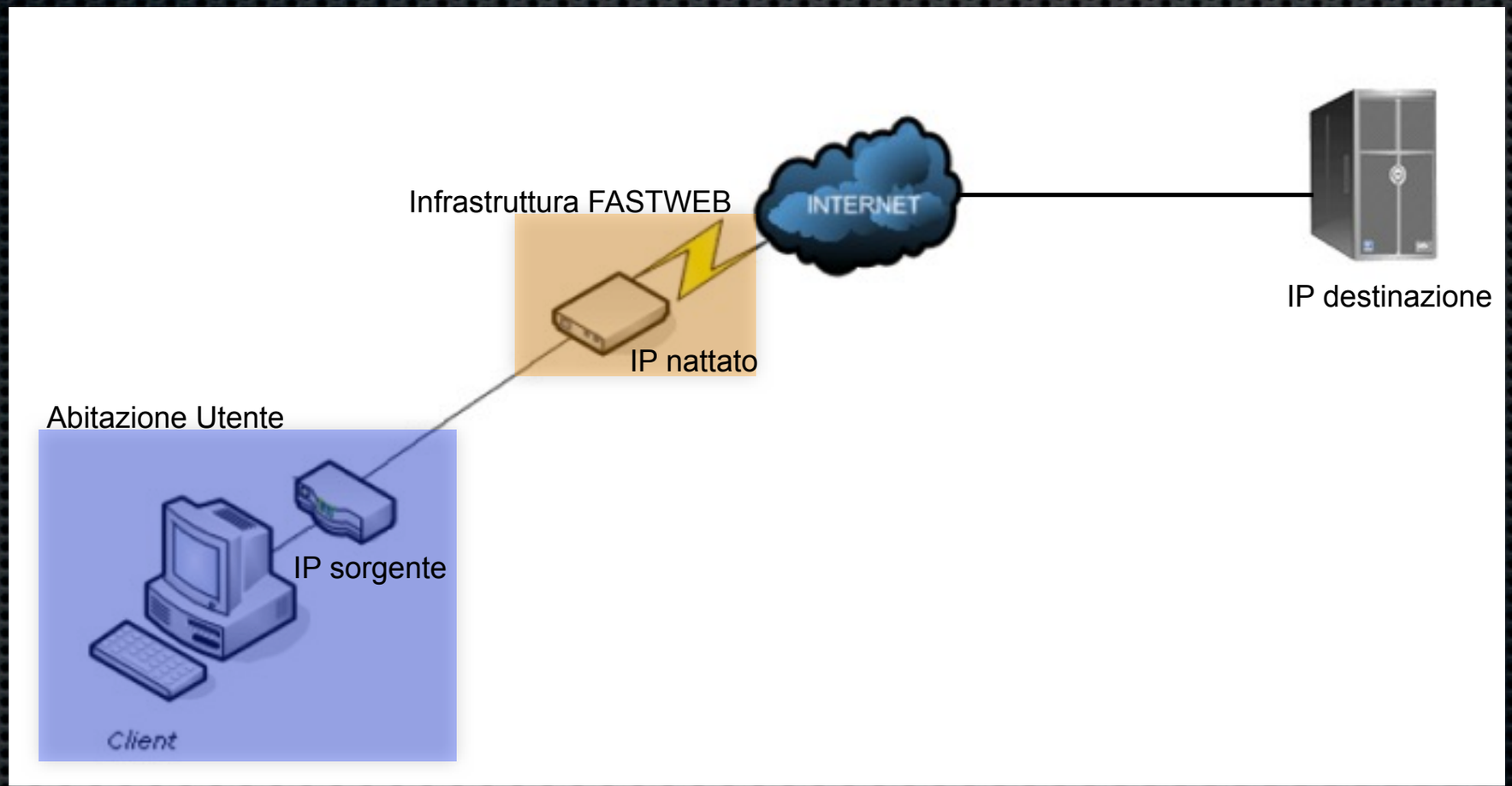
Polizia di Stato

Compartimento Polizia Postale e delle Comunicazioni per l'Umbria

Proc. Pen. 9066/07

Analisi File di Log

Rete Fastweb

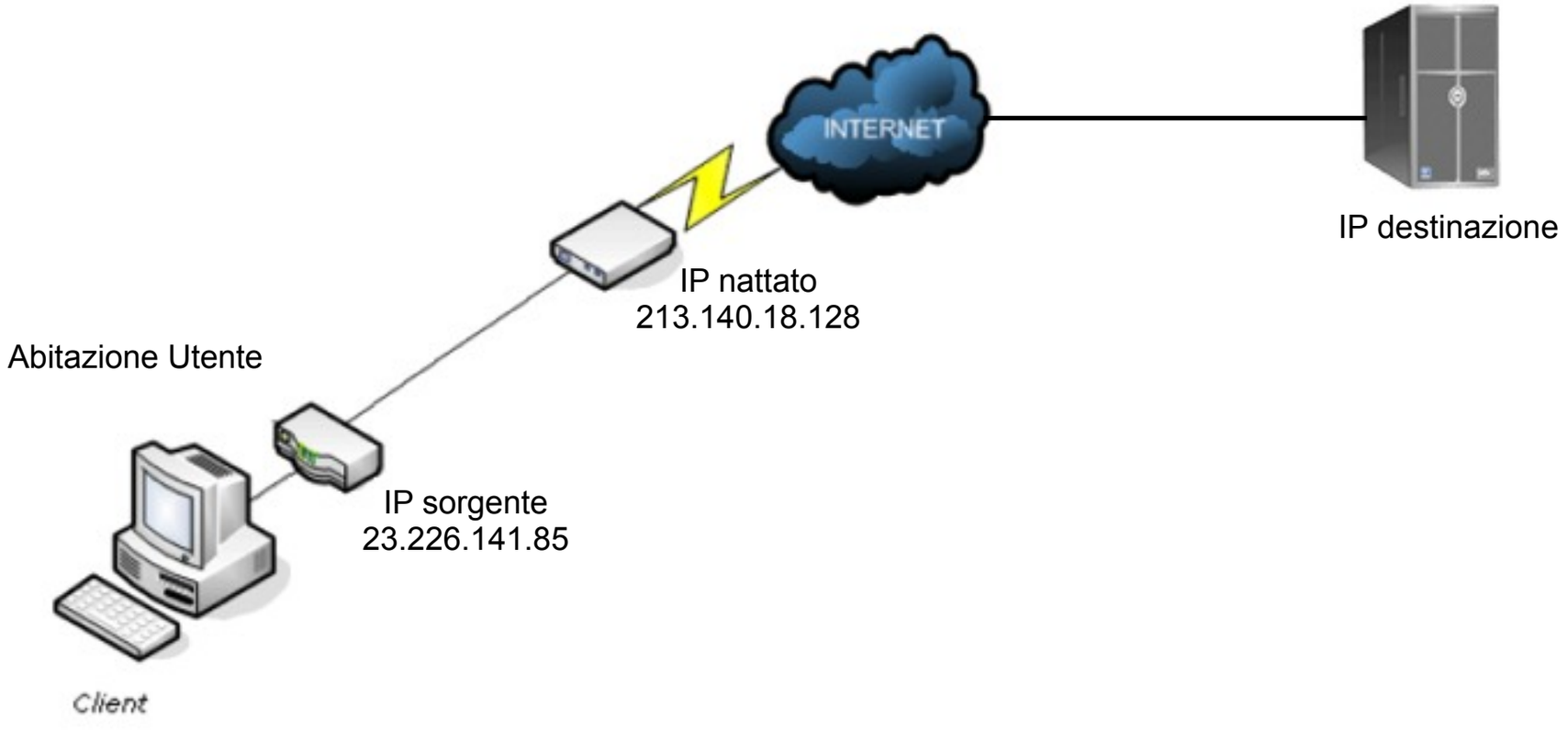


Polizia di Stato

polizia delle comunicazioni

Struttura rete FASTWEB

Rete Fastweb



Log acquisiti in data 16/11/2007

Dati disponibili su file di log

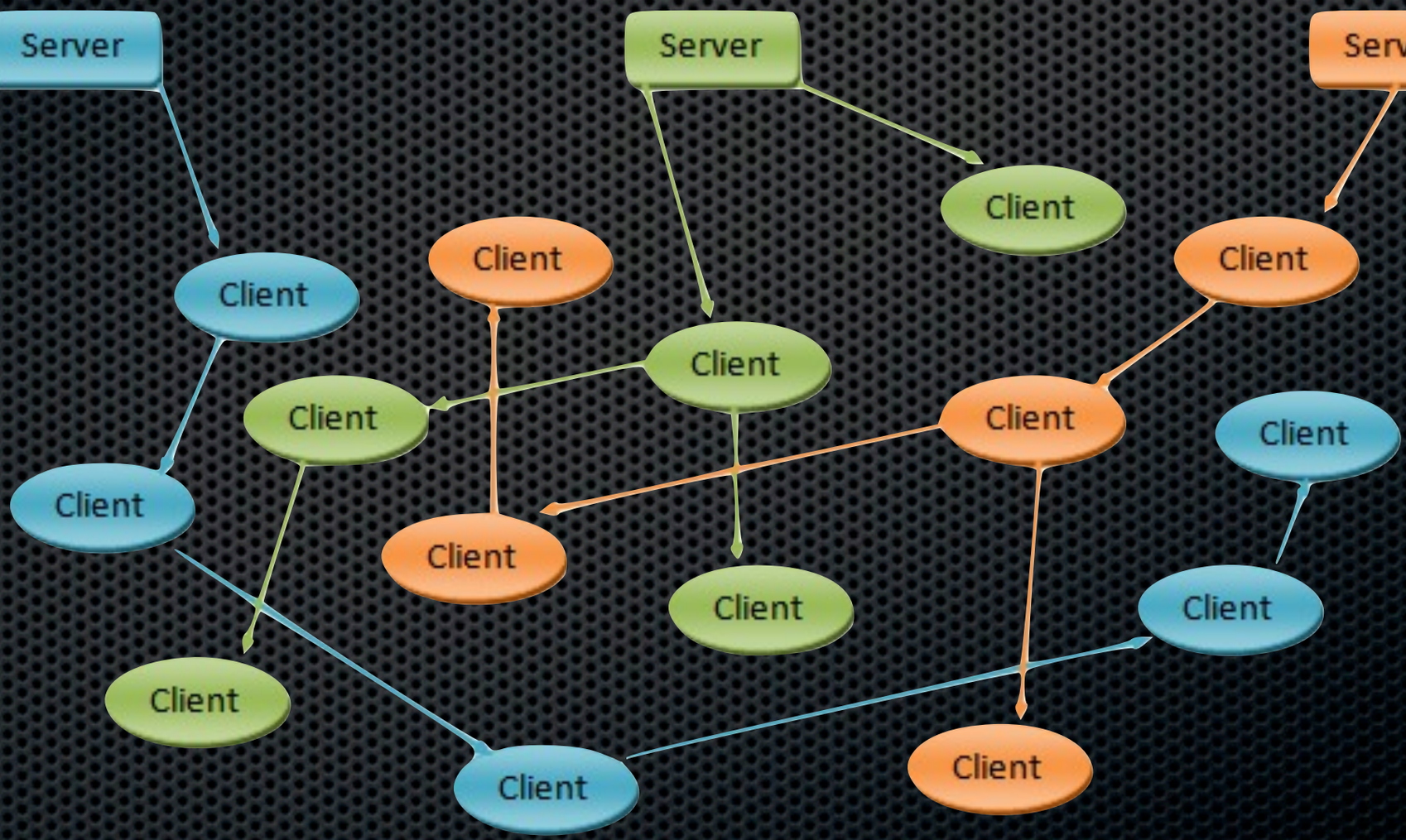
| IP Sorgente | Porta | IP Nattato | Porta | IP Destinazione| Porta | Data Inizio | Data Fine | Durata | Tipo| Bytes | Causa| FW |

Polizia di Stato

@polizia delle comunicazioni

Connettività Peer-to-peer

Connettività Peer-to-peer utilizzata per la condivisione di File tra utenti



Polizia di Stato

polizia delle comunicazioni

Connettività Client/Server

Client

I client non utilizzano porte prestabilite quando si collegano con i server

Server

I server Web offrono i loro servizi tramite apposite porte standard

Polizia di Stato

polizia delle comunicazioni

Esempio Connettività TCP Client/Server pagine web

Richiesta pagina web

Client

L'utente richiede la pagina web al server

porta 80 in ascolto

Server

Google

Polizia di Stato

polizia delle comunicazioni

Esempio Connettività TCP Client/Server pagine web

Richiesta pagina web

Client

L'utente richiede la pagina web al server

porta 80 in ascolto

Server

Google

Polizia di Stato

polizia delle comunicazioni

Esempio Connettività TCP Client/Server pagine web

Richiesta pagina web

Client

L'utente richiede la pagina web al server

il server fornisce la pagina richiesta

porta 80 in ascolto

Server

Google

Polizia di Stato

polizia delle comunicazioni

Esempio Connettività TCP Client/Server pagine web

Richiesta pagina web

Client

L'utente richiede la pagina web al server

il server fornisce la pagina richiesta

porta 80 in ascolto

Server

Google

Polizia di Stato

polizia delle comunicazioni

Esempio Connettività TCP Client/Server pagine web

Richiesta pagina web

Client

L'utente richiede la pagina web al server

il server fornisce la pagina richiesta

porta 80 in ascolto

Server

Google

Il computer riceve i dati li scrive nella cache del browser e li rende disponibili a video per la consultazione

Polizia di Stato

polizia delle comunicazioni

Esempio Connettività TCP Client/Server pagine web

Richiesta pagina web

Client

L'utente richiede la pagina web al server

il server fornisce la pagina richiesta

porta 80 in ascolto

Server

Google

Il computer riceve i dati li scrive nella cache del browser e li rende disponibili a video per la consultazione

Polizia di Stato

polizia delle comunicazioni

Esempio Connettività TCP Client/Server pagine web

Richiesta pagina web

Client

L'utente richiede la pagina web al server

il server fornisce la pagina richiesta

porta 80 in ascolto

Server

Google

Il computer riceve i dati li scrive nella cache del browser e li rende disponibili a video per la consultazione

Polizia di Stato

polizia delle comunicazioni

Esempio Connettività TCP Client/Server pagine web

Richiesta pagina web

Client

porta 80 in ascolto

L'utente richiede la pagina web al server

il server fornisce la pagina richiesta

Server

Google

Il computer riceve i dati li scrive nella cache del browser e li rende disponibili a video per la consultazione

IP Sorgente

dati scambiati
ingresso/uscita

IP Destinazione

Polizia di Stato

polizia delle comunicazioni

cache del browser

Client

Il computer riceve i dati li scrive nella cache del browser e li rende disponibili a video per la consultazione

FILES CREATI

PERIODO\FILES CREATI Page 1

FILES CREATI

1)
Name temp7040842
Full Path HITACHI \HITACHI\1 Merged_Untitled\MacOS HD\NoName\temp7040842
File Created 02/11/07 03:15:07

2)
Name system.log.4.gz
Full Path HITACHI \HITACHI\1 Merged_Untitled\MacOS HD\private\var\log\system.log.4.gz
File Created 02/11/07 03:15:07

3)
Name 54952E7Cd01
Full Path HITACHI \HITACHI\1 Merged_Untitled\MacOS HD\Users\macbookpro\Library\Caches\Firefox\Profiles\7kmlxh3f.default\Cache\54952E7Cd01
File Created 01/11/07 18:33:14

4)
Name 54954E44d01
Full Path HITACHI \HITACHI\1 Merged_Untitled\MacOS HD\Users\macbookpro\Library\Caches\Firefox\Profiles\7kmlxh3f.default\Cache\54954E44d01
File Created 01/11/07 19:33:14

5)
Name 54956E41d01
Full Path HITACHI \HITACHI\1 Merged_Untitled\MacOS HD\Users\macbookpro\Library\Caches\Firefox\Profiles\7kmlxh3f.default\Cache\54956E41d01
File Created 01/11/07 21:03:15

6)
Name 54959E54d01
Full Path HITACHI \HITACHI\1 Merged_Untitled\MacOS HD\Users\macbookpro\Library\Caches\Firefox\Profiles\7kmlxh3f.default\Cache\54959E54d01
File Created 01/11/07 23:03:13

7)
Name 54959E25d01
Full Path HITACHI \HITACHI\1 Merged_Untitled\MacOS HD\Users\macbookpro\Library\Caches\Firefox\Profiles\7kmlxh3f.default\Cache\54959E25d01
File Created 02/11/07 01:33:14

8)
Name 54941E27d01
Full Path HITACHI \HITACHI\1 Merged_Untitled\MacOS HD\Users\macbookpro\Library\Caches\Firefox\Profiles\7kmlxh3f.default\Cache\54941E27d01
File Created 02/11/07 02:33:16

9)
Name 54940E23d01
Full Path HITACHI \HITACHI\1 Merged_Untitled\MacOS HD\Users\macbookpro\Library\Caches\Firefox\Profiles\7kmlxh3f.default\Cache\54940E23d01
File Created 02/11/07 03:33:13

Polizia di Stato

polizia delle comunicazioni

cache del browser

Client

Il computer riceve i dati li scrive nella cache del browser e li rende disponibili a video per la consultazione

3)
Name 54952E7Cd01
Full Path HITACHI \HITACHI\1 Merged_Untitled\MacOS HD\Users\macbookpro\Library\Caches\Firefox\Profiles\7kmlxh3f.default\Cache\54952E7Cd01
File Created 01/11/07 18:33:14

4)
Name 54954E44d01
Full Path HITACHI \HITACHI\1 Merged_Untitled\MacOS HD\Users\macbookpro\Library\Caches\Firefox\Profiles\7kmlxh3f.default\Cache\54954E44d01
File Created 01/11/07 19:33:14

5)
Name 54956E41d01
Full Path HITACHI \HITACHI\1 Merged_Untitled\MacOS HD\Users\macbookpro\Library\Caches\Firefox\Profiles\7kmlxh3f.default\Cache\54956E41d01
File Created 01/11/07 21:03:15

6)
Name 54959E54d01
Full Path HITACHI \HITACHI\1 Merged_Untitled\MacOS HD\Users\macbookpro\Library\Caches\Firefox\Profiles\7kmlxh3f.default\Cache\54959E54d01
File Created 01/11/07 23:03:13

7)
Name 54959E25d01
Full Path HITACHI \HITACHI\1 Merged_Untitled\MacOS HD\Users\macbookpro\Library\Caches\Firefox\Profiles\7kmlxh3f.default\Cache\54959E25d01
File Created 02/11/07 01:33:14

8)
Name 54941E27d01
Full Path HITACHI \HITACHI\1 Merged_Untitled\MacOS HD\Users\macbookpro\Library\Caches\Firefox\Profiles\7kmlxh3f.default\Cache\54941E27d01
File Created 02/11/07 02:33:16

9)
Name 54940E23d01
Full Path HITACHI \HITACHI\1 Merged_Untitled\MacOS HD\Users\macbookpro\Library\Caches\Firefox\Profiles\7kmlxh3f.default\Cache\54940E23d01
File Created 02/11/07 03:33:13

Polizia di Stato

polizia delle comunicazioni

cache del browser

3)
Name 54952E7Cd01
Full Path HITACHI \HITACHI\1 Merged_Untitled\MacOS HD\Users\macbookpro\Library\Caches\Firefox\Profiles\7kmlxh3f.default\Cache\54952E7Cd01
File Created 01/11/07 18:33:14

4)
Name 54954E44d01
Full Path HITACHI \HITACHI\1 Merged_Untitled\MacOS HD\Users\macbookpro\Library\Caches\Firefox\Profiles\7kmlxh3f.default\Cache\54954E44d01
File Created 01/11/07 19:33:14

5)
Name 54956E41d01
Full Path HITACHI \HITACHI\1 Merged_Untitled\MacOS HD\Users\macbookpro\Library\Caches\Firefox\Profiles\7kmlxh3f.default\Cache\54956E41d01
File Created 01/11/07 21:03:15

6)
Name 54959E54d01
Full Path HITACHI \HITACHI\1 Merged_Untitled\MacOS HD\Users\macbookpro\Library\Caches\Firefox\Profiles\7kmlxh3f.default\Cache\54959E54d01
File Created 01/11/07 23:03:13

7)
Name 54959E25d01
Full Path HITACHI \HITACHI\1 Merged_Untitled\MacOS HD\Users\macbookpro\Library\Caches\Firefox\Profiles\7kmlxh3f.default\Cache\54959E25d01
File Created 02/11/07 01:33:14

8)
Name 54941E27d01
Full Path HITACHI \HITACHI\1 Merged_Untitled\MacOS HD\Users\macbookpro\Library\Caches\Firefox\Profiles\7kmlxh3f.default\Cache\54941E27d01
File Created 02/11/07 02:33:16

9)
Name 54940E23d01
Full Path HITACHI \HITACHI\1 Merged_Untitled\MacOS HD\Users\macbookpro\Library\Caches\Firefox\Profiles\7kmlxh3f.default\Cache\54940E23d01
File Created 02/11/07 03:33:13

Tabella riassuntiva cache

Nome File	data ora
54952E7Cd01	01/11/07 18:33:14
54954E44d01	01/11/07 19:33:14
54956E41d01	01/11/07 21:03:15
54959E54d01	01/11/07 23:03:13
54959E25d01	02/11/07 01:33:14
54941E27d01	02/11/07 02:33:16
54940E23d01	02/11/07 03:33:13

Polizia di Stato

polizia delle comunicazioni

Analisi dei dati

Analisi File di Log FASTWEB

data ora	durata	Bytes	IP Destinazione
01/11/2007 18:03:14	0:00:18	3435	209.85.135.91
01/11/2007 18:33:14	0:00:18	117582	209.85.135.91
01/11/2007 19:03:18	0:00:15	1838	209.85.135.91
01/11/2007 19:33:13	0:00:23	77243	209.85.135.91
01/11/2007 20:03:16	0:00:16	1675	209.85.135.91
01/11/2007 20:33:19	0:00:13	1675	209.85.135.91
01/11/2007 21:03:14	0:00:19	203346	209.85.135.91
01/11/2007 21:33:15	0:00:17	2667	209.85.135.91
01/11/2007 22:03:14	0:00:19	4963	209.85.135.91
01/11/2007 22:33:13	0:00:20	1675	209.85.135.91
01/11/2007 23:03:13	0:00:20	114118	209.85.135.91
01/11/2007 23:33:15	0:00:17	3866	209.85.135.91
02/11/2007 00:03:13	0:00:21	7997	209.85.135.91
02/11/2007 00:33:12	0:00:23	5177	209.85.135.91
02/11/2007 01:03:13	0:00:20	2733	209.85.135.91
02/11/2007 01:33:13	0:00:20	98797	209.85.135.91
02/11/2007 02:03:14	0:00:20	1805	209.85.135.91
02/11/2007 02:33:16	0:00:17	133889	209.85.135.91
02/11/2007 03:03:12	0:00:21	5779	209.85.135.91
02/11/2007 03:33:12	0:00:21	97227	209.85.135.91
02/11/2007 04:03:12	0:00:21	6667	209.85.135.91
02/11/2007 04:33:13	0:00:21	3908	209.85.135.91
02/11/2007 05:05:28	0:00:24	2504	209.85.135.91
02/11/2007 05:33:13	0:00:21	6966	209.85.135.91
02/11/2007 06:05:27	0:00:22	10458	209.85.135.91
02/11/2007 06:33:13	0:00:22	3068	209.85.135.91
02/11/2007 07:03:11	0:00:22	8551	209.85.135.91
02/11/2007 07:35:28	0:05:18	6401	209.85.135.91

Tabella riassuntiva cache

Nome File	data ora
54952E7Cd01	01/11/07 18:33:14
54954E44d01	01/11/07 19:33:14
54956E41d01	01/11/07 21:03:15
54959E54d01	01/11/07 23:03:13
54959E25d01	02/11/07 01:33:14
54941E27d01	02/11/07 02:33:16
54940E23d01	02/11/07 03:33:13

L'indirizzo IP 209.85.135.91 appartiene alla società Google Inc.

i collegamenti in oggetto sono fatti in maniera automatica per l'aggiornamento del sistema AntiPhishing di Firefox denominato SafeBrowsing