Università del Piemonte Orientale

Centro Studi Interdipartimentale

sulla Criminalità Informatica

Convegno

"Processo penale e Criminalità Informatica: Una nuova realtà dopo la ratifica della Convenzione di Budapest"

Dott. Sergio Staro

VQA della Polizia Postale e delle Comunicazioni

Alessandria, 16 settembre 2009

Organizzazione sul territorio nazionale della Polizia Postale e delle Comunicazioni

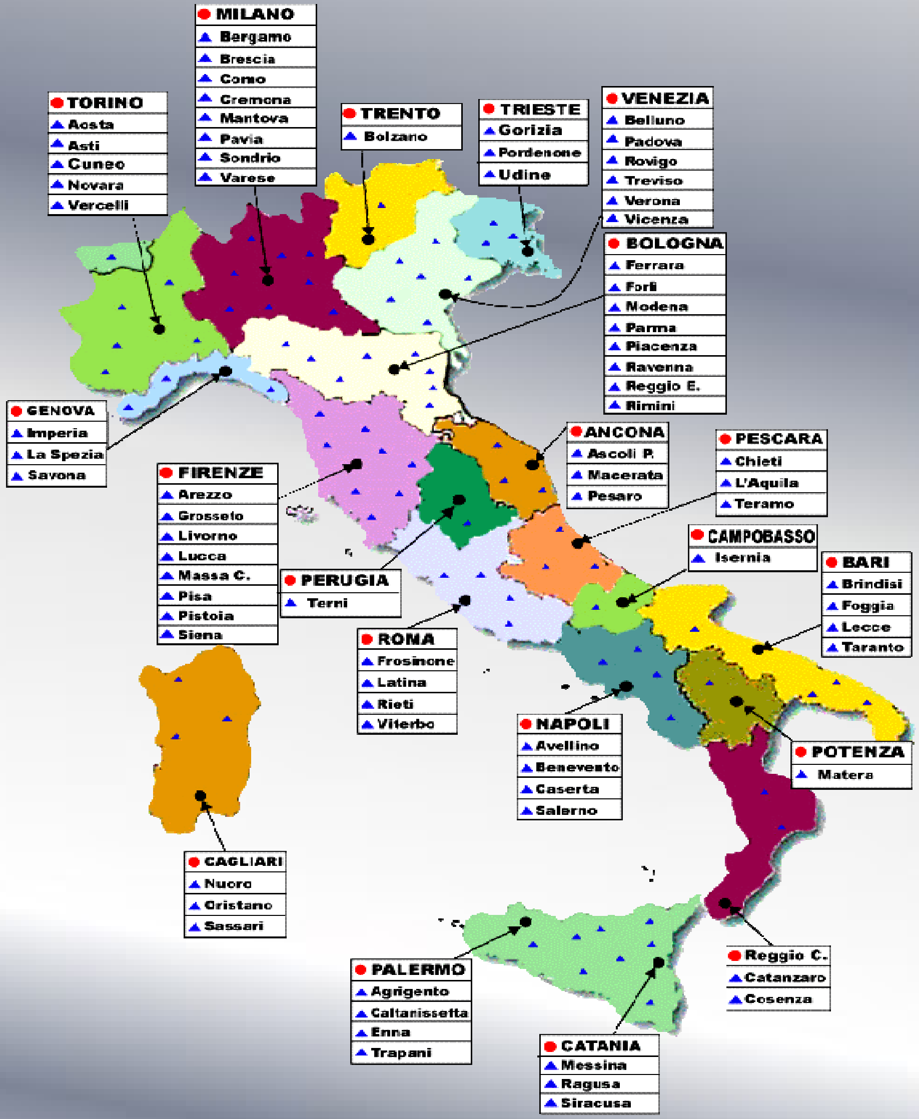
20 Compartimenti regionali

76 Sezioni provinciali

1856 operatori

● Compartimenti Polizia Postale

▲ Sezioni della Polizia Postale

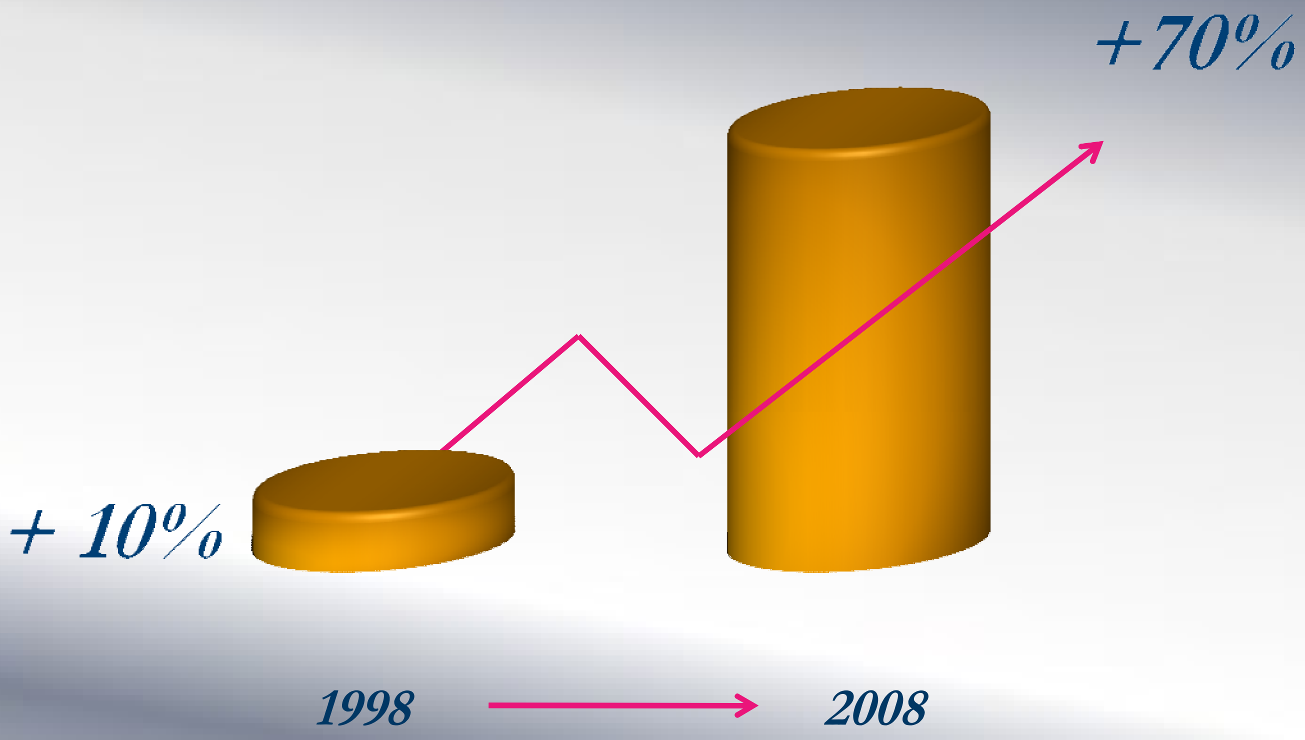


Competenze
della Polizia Postale e delle Comunicazioni

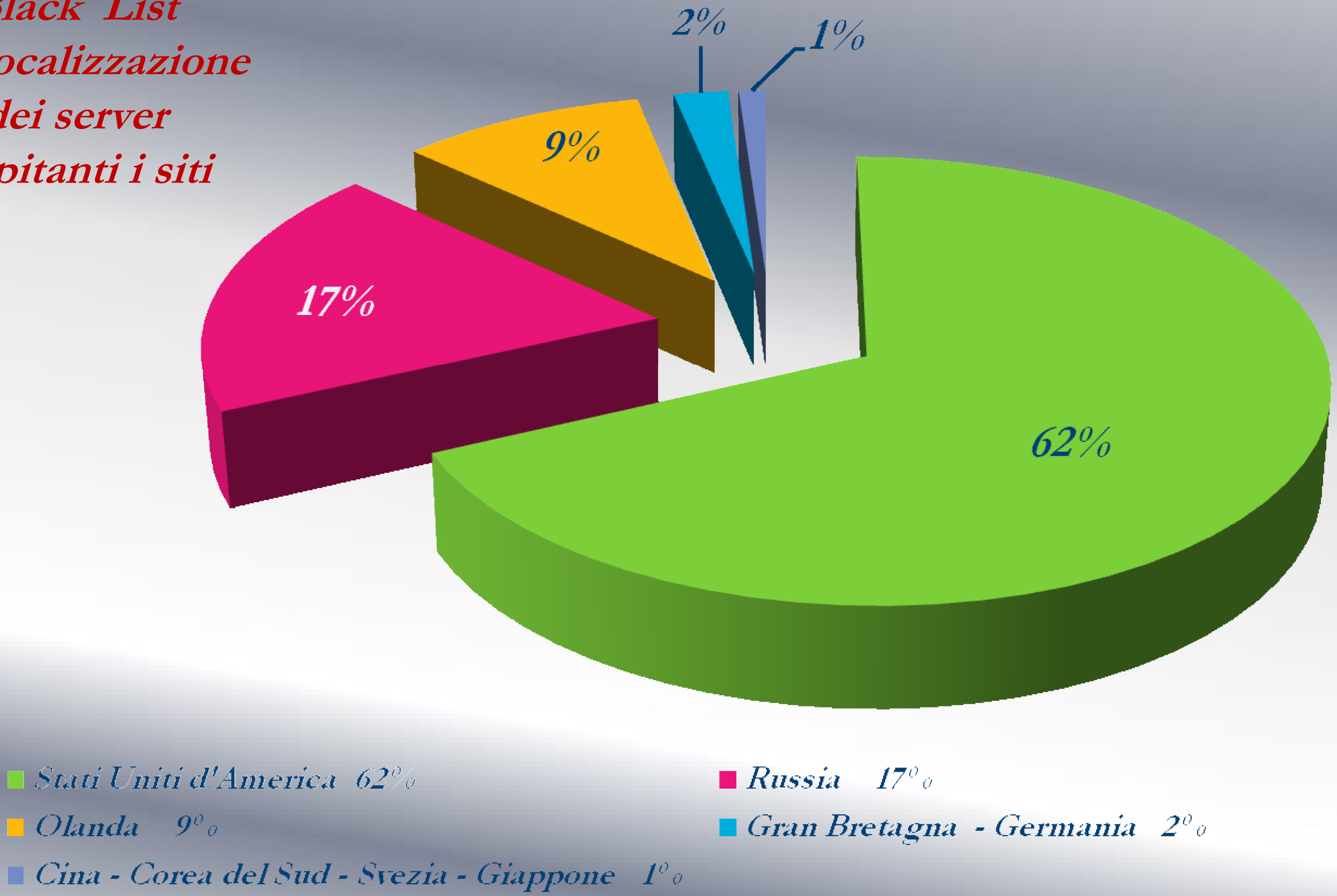
- *Cyberterrorismo*
- *Computer forensic*
- *Controllo radio frequenze*
- *Copyright*
- *E-Commerce*
- *E- Banking*
- *Giochi e scommesse on line (legge 266/'05)*
- *Hacking*
- *Pedofilia On line*
- *Protezione infrastrutture critiche*
- *Pirateria satellitare*
- *Reati postali e falsi filatelici*
- *Sorveglianza del mercato (D.lgs 269/2001)*
- *Collaborazione operativa con Forze di Polizia straniere (h 24 / 7)*

Il crimine informatico transnazionale

Indagini condivise con altri Paesi

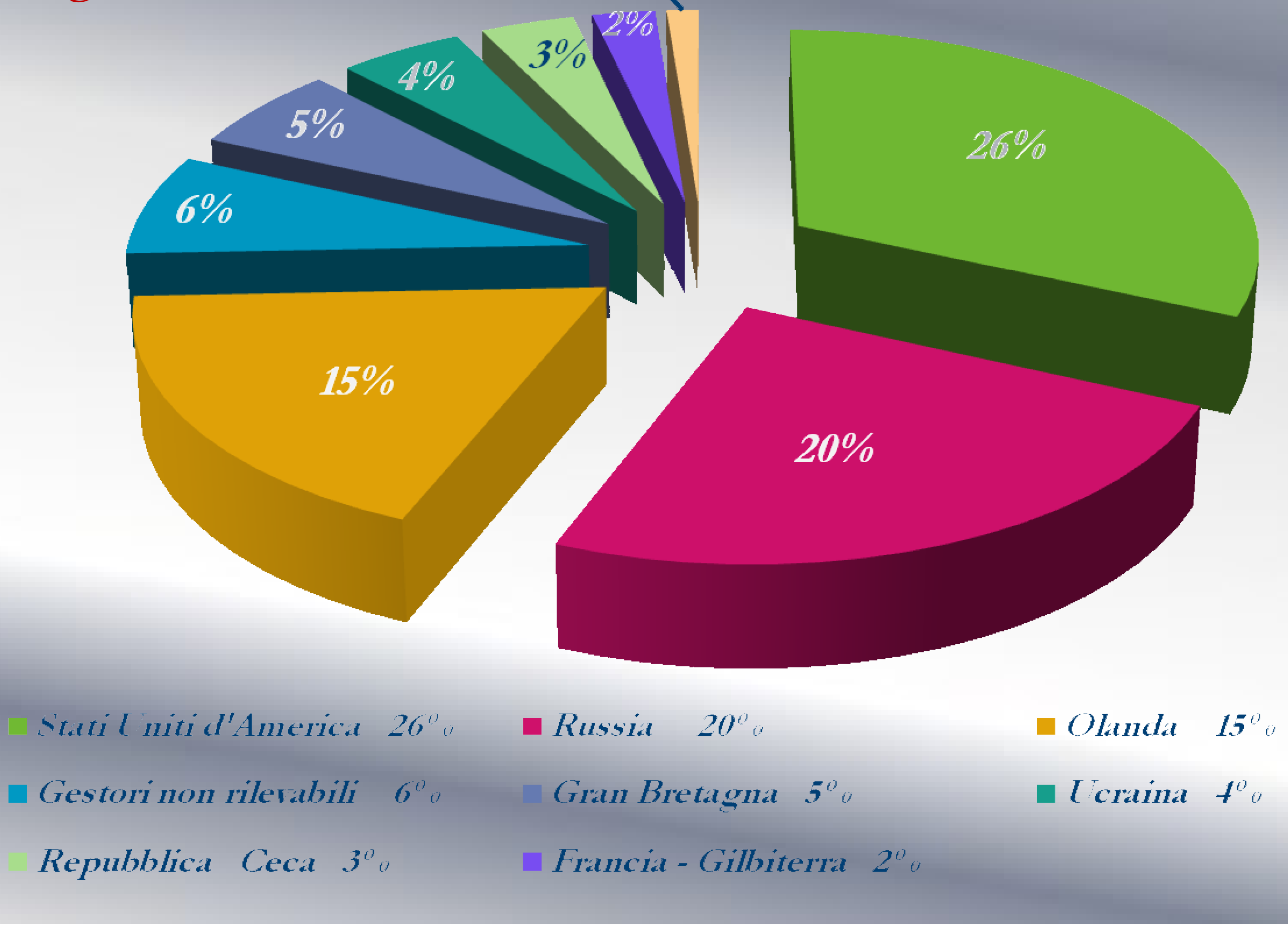


Black List
Geolocalizzazione dei server ospitanti i siti



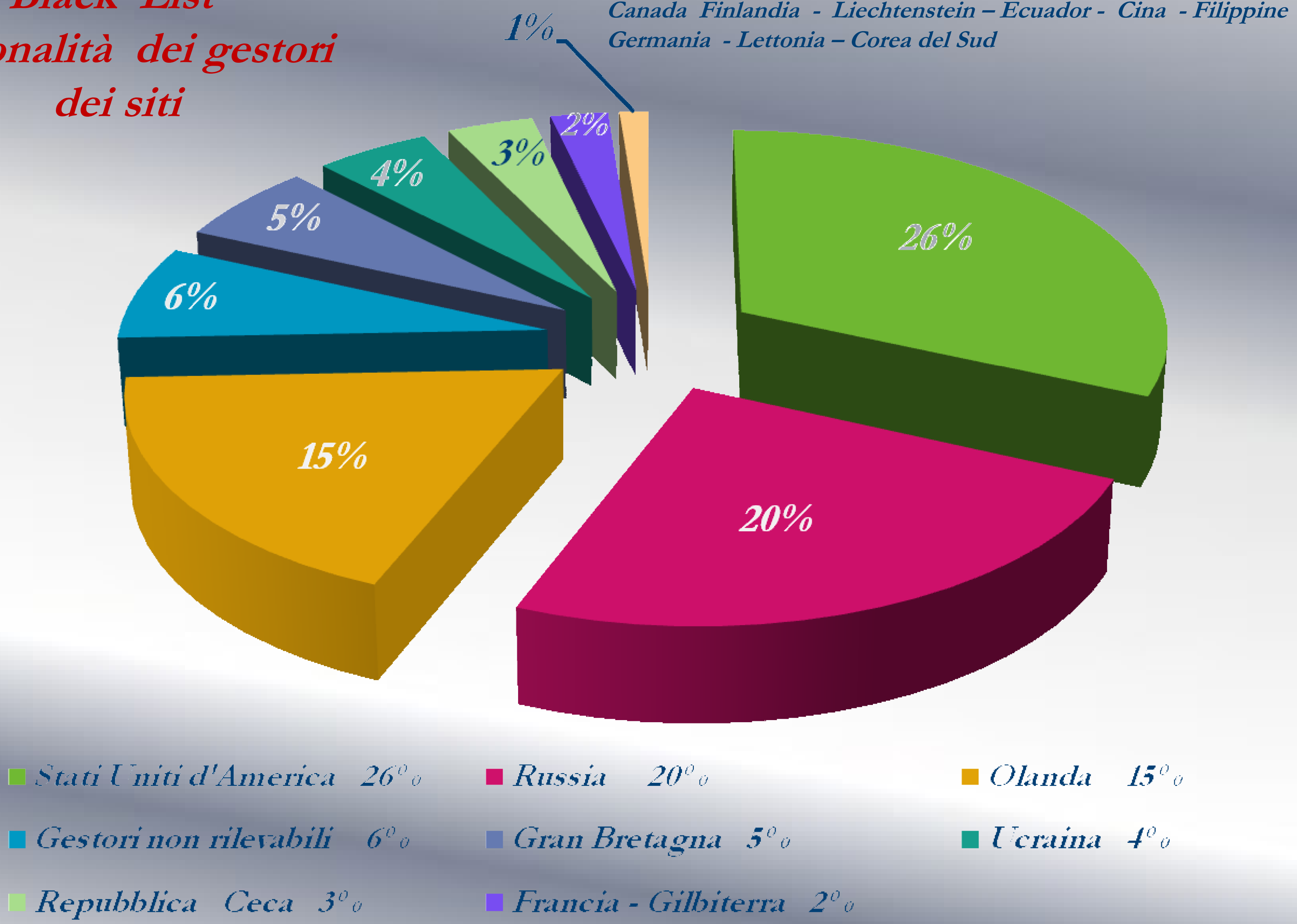
Black List
Nazionalità dei soggetti registranti i siti

Canada Finlandia - Liechtenstein – Ecuador - Cina - Filippine
Germania - Lettonia – Corea del Sud



CNCPO - Centro Nazionale per il Contrasto della Pedopornografia On-line

Black List Nazionalità dei gestori dei siti



Collaborazione investigativa

- *27 Paesi*
- *C.O.*

- *coop. giudiziaria*
- *circa 190 Paesi*
- *I - 24/7*
- *NCB*

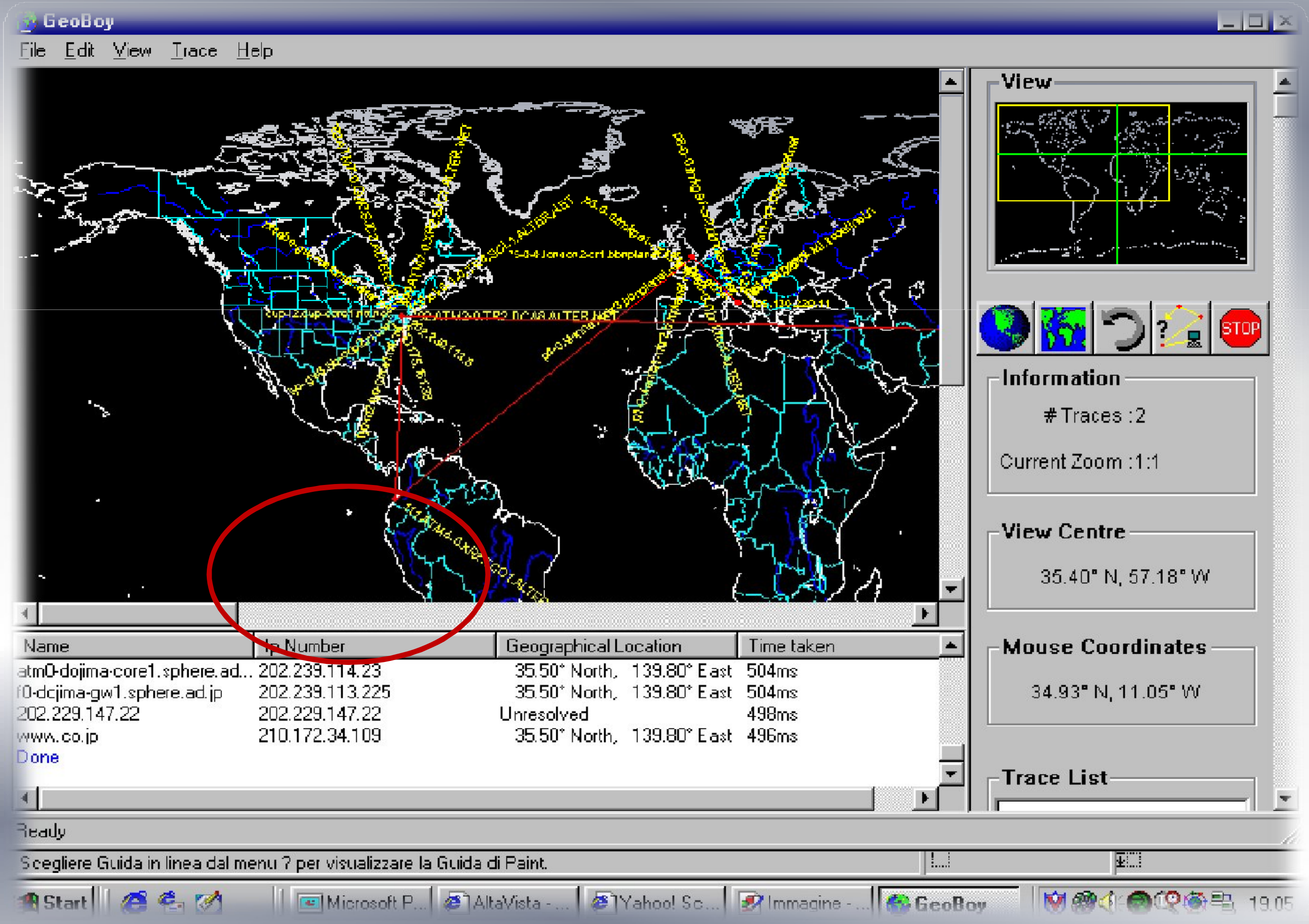
Collaborazione investigativa

•http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=18/09/2005&CL=ENG

- http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc
  - ➢ 10.6.2009: 20 sottoscrizioni; 26 ratifiche (su 46 Stati membri)

Tracciamento telematico

– IP address –



Information

Traces :2

Current Zoom :1:1

View Centre

35.40° N, 57.18° W

Mouse Coordinates

34.93° N, 11.05° W

Trace List

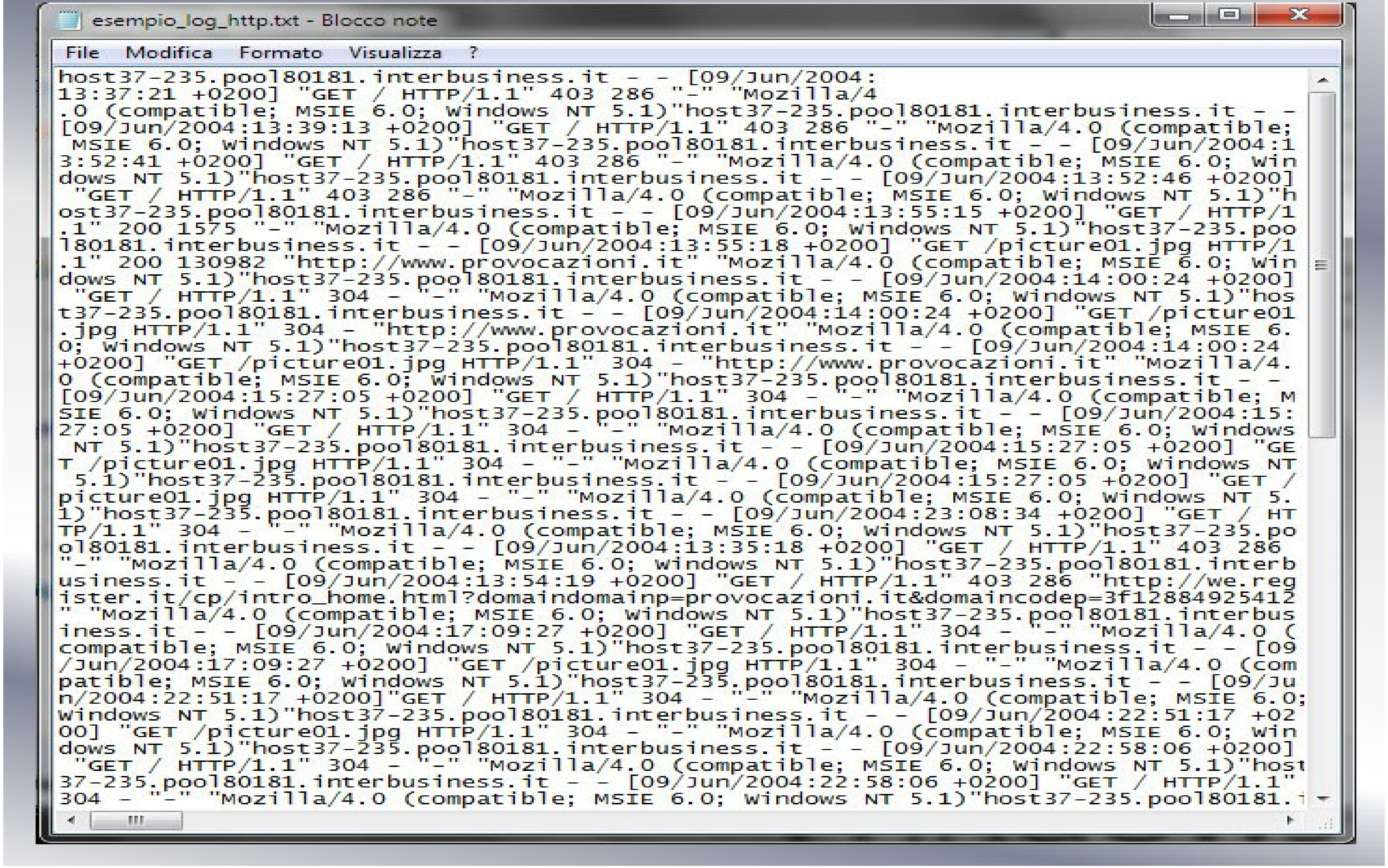
Name	Ip Number	Geographical Location	Time taken
atm0-dojima-core1.sphere.ad...	202.239.114.23	35.50° North, 139.80° East	504ms
f0-dcjima-gw1.sphere.ad.jp	202.239.113.225	35.50° North, 139.80° East	504ms
202.229.147.22	202.229.147.22	Unresolved	498ms
www.co.jp	210.172.34.109	35.50° North, 139.80° East	496ms

Done

Ready

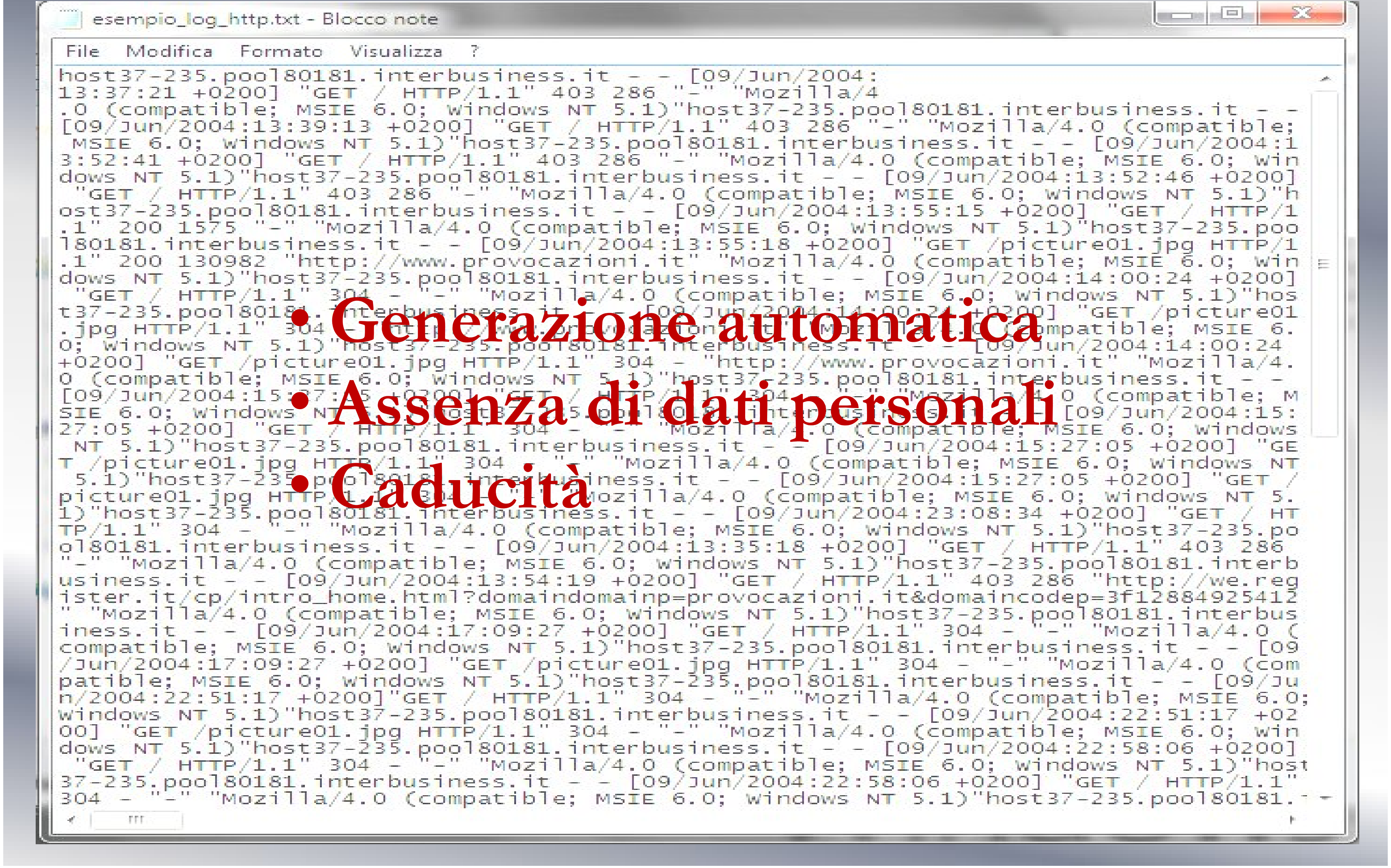
Scegliere Guida in linea dal menu ? per visualizzare la Guida di Paint.

Il file di Log



```
host37-235.pool80181.interbusiness.it - - [09/Jun/2004:
13:37:21 +0200] "GET / HTTP/1.1" 403 286 "-" "Mozilla/4
.0 (compatible; MSIE 6.0; Windows NT 5.1)"host37-235.pool80181.interbusiness.it - -
[09/Jun/2004:13:39:13 +0200] "GET / HTTP/1.1" 403 286 "-" "Mozilla/4.0 (compatible;
 MSIE 6.0; Windows NT 5.1)"host37-235.pool80181.interbusiness.it - - [09/Jun/2004:1
3:52:41 +0200] "GET / HTTP/1.1" 403 286 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Win
dows NT 5.1)"host37-235.pool80181.interbusiness.it - - [09/Jun/2004:13:52:46 +0200]
 "GET / HTTP/1.1" 403 286 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"h
ost37-235.pool80181.interbusiness.it - - [09/Jun/2004:13:55:15 +0200] "GET / HTTP/1
.1" 200 1575 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"host37-235.poo
l80181.interbusiness.it - - [09/Jun/2004:13:55:18 +0200] "GET /picture01.jpg HTTP/1
.1" 200 130982 "http://www.provocazioni.it" "Mozilla/4.0 (compatible; MSIE 6.0; Win
dows NT 5.1)"host37-235.pool80181.interbusiness.it - - [09/Jun/2004:14:00:24 +0200]
 "GET / HTTP/1.1" 304 - "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"hos
t37-235.pool80181.interbusiness.it - - [09/Jun/2004:14:00:24 +0200] "GET /picture01
.jpg HTTP/1.1" 304 - "http://www.provocazioni.it" "Mozilla/4.0 (compatible; MSIE 6.
0; Windows NT 5.1)"host37-235.pool80181.interbusiness.it - - [09/Jun/2004:14:00:24
+0200] "GET /picture01.jpg HTTP/1.1" 304 - "http://www.provocazioni.it" "Mozilla/4.
0 (compatible; MSIE 6.0; Windows NT 5.1)"host37-235.pool80181.interbusiness.it - -
[09/Jun/2004:15:27:05 +0200] "GET / HTTP/1.1" 304 - "-" "Mozilla/4.0 (compatible; M
SIE 6.0; Windows NT 5.1)"host37-235.pool80181.interbusiness.it - - [09/Jun/2004:15:
27:05 +0200] "GET / HTTP/1.1" 304 - "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows
 NT 5.1)"host37-235.pool80181.interbusiness.it - - [09/Jun/2004:15:27:05 +0200] "GE
T /picture01.jpg HTTP/1.1" 304 - "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
 5.1)"host37-235.pool80181.interbusiness.it - - [09/Jun/2004:15:27:05 +0200] "GET /
picture01.jpg HTTP/1.1" 304 - "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.
1)"host37-235.pool80181.interbusiness.it - - [09/Jun/2004:23:08:34 +0200] "GET / HT
TP/1.1" 304 - "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"host37-235.po
ol80181.interbusiness.it - - [09/Jun/2004:13:35:18 +0200] "GET / HTTP/1.1" 403 286
"-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"host37-235.pool80181.interb
usiness.it - - [09/Jun/2004:13:54:19 +0200] "GET / HTTP/1.1" 403 286 "http://we.reg
ister.it/cp/intro_home.html?domaindomainp=provocazioni.it&domaincodep=3f12884925412
" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"host37-235.pool80181.interbus
iness.it - - [09/Jun/2004:17:09:27 +0200] "GET / HTTP/1.1" 304 - "-" "Mozilla/4.0 (
compatible; MSIE 6.0; Windows NT 5.1)"host37-235.pool80181.interbusiness.it - - [09
/Jun/2004:17:09:27 +0200] "GET /picture01.jpg HTTP/1.1" 304 - "-" "Mozilla/4.0 (com
patible; MSIE 6.0; Windows NT 5.1)"host37-235.pool80181.interbusiness.it - - [09/Ju
n/2004:22:51:17 +0200]"GET / HTTP/1.1" 304 - "-" "Mozilla/4.0 (compatible; MSIE 6.0;
Windows NT 5.1)"host37-235.pool80181.interbusiness.it - - [09/Jun/2004:22:51:17 +02
00] "GET /picture01.jpg HTTP/1.1" 304 - "-" "Mozilla/4.0 (compatible; MSIE 6.0; Win
dows NT 5.1)"host37-235.pool80181.interbusiness.it - - [09/Jun/2004:22:58:06 +0200]
 "GET / HTTP/1.1" 304 - "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"host
37-235.pool80181.interbusiness.it - - [09/Jun/2004:22:58:06 +0200] "GET / HTTP/1.1"
304 - "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"host37-235.pool80181.i
```

Il file di Log



esempio_log_http.txt - Blocco note
File Modifica Formato Visualizza ?

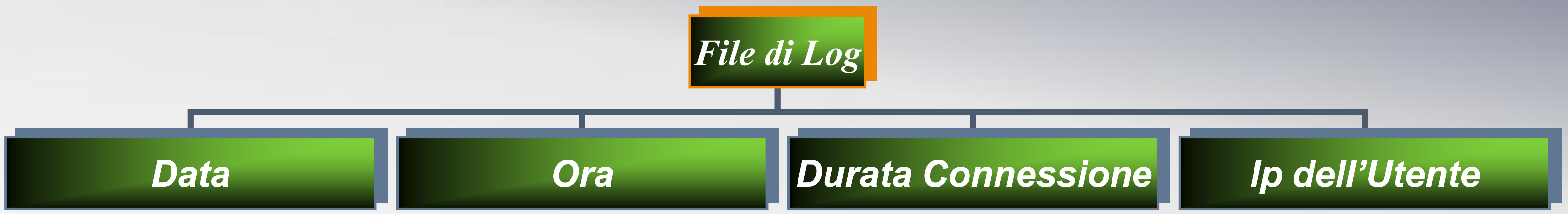
```
host37-235.pool80181.interbusiness.it - - [09/Jun/2004:
13:37:21 +0200] "GET / HTTP/1.1" 403 286 "-" "Mozilla/4
.0 (compatible; MSIE 6.0; Windows NT 5.1)"host37-235.pool80181.interbusiness.it - -
[09/Jun/2004:13:39:13 +0200] "GET / HTTP/1.1" 403 286 "-" "Mozilla/4.0 (compatible;
 MSIE 6.0; Windows NT 5.1)"host37-235.pool80181.interbusiness.it - - [09/Jun/2004:1
3:52:41 +0200] "GET / HTTP/1.1" 403 286 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Win
dows NT 5.1)"host37-235.pool80181.interbusiness.it - - [09/Jun/2004:13:52:46 +0200]
 "GET / HTTP/1.1" 403 286 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"h
ost37-235.pool80181.interbusiness.it - - [09/Jun/2004:13:55:15 +0200] "GET / HTTP/1
.1" 200 1575 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"host37-235.poo
l80181.interbusiness.it - - [09/Jun/2004:13:55:18 +0200] "GET /picture01.jpg HTTP/1
.1" 200 130982 "http://www.provocazioni.it" "Mozilla/4.0 (compatible; MSIE 6.0; Win
dows NT 5.1)"host37-235.pool80181.interbusiness.it - - [09/Jun/2004:14:00:24 +0200]
 "GET / HTTP/1.1" 304 - "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"hos
t37-235.pool80181.interbusiness.it - - [09/Jun/2004:14:00:24 +0200] "GET /picture01
.jpg HTTP/1.1" 304 - "http://www.provocazioni.it" "Mozilla/4.0 (compatible; MSIE 6.
0; Windows NT 5.1)"host37-235.pool80181.interbusiness.it - - [09/Jun/2004:14:00:24
+0200] "GET /picture01.jpg HTTP/1.1" 304 - "http://www.provocazioni.it" "Mozilla/4.
0 (compatible; MSIE 6.0; Windows NT 5.1)"host37-235.pool80181.interbusiness.it - -
[09/Jun/2004:15:27:05 +0200] "GET / HTTP/1.1" 304 - "-" "Mozilla/4.0 (compatible; M
SIE 6.0; Windows NT 5.1)"host37-235.pool80181.interbusiness.it - - [09/Jun/2004:15:
27:05 +0200] "GET / HTTP/1.1" 304 - "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows
 NT 5.1)"host37-235.pool80181.interbusiness.it - - [09/Jun/2004:15:27:05 +0200] "GE
T /picture01.jpg HTTP/1.1" 304 - "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
 5.1)"host37-235.pool80181.interbusiness.it - - [09/Jun/2004:15:27:05 +0200] "GET /
picture01.jpg HTTP/1.1" 304 - "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.
1)"host37-235.pool80181.interbusiness.it - - [09/Jun/2004:23:08:34 +0200] "GET / HT
TP/1.1" 304 - "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"host37-235.po
ol80181.interbusiness.it - - [09/Jun/2004:13:35:18 +0200] "GET / HTTP/1.1" 403 286
"-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"host37-235.pool80181.interb
usiness.it - - [09/Jun/2004:13:54:19 +0200] "GET / HTTP/1.1" 403 286 "http://we.reg
ister.it/cp/intro_home.html?domaindomainp=provocazioni.it&domaincodep=3f12884925412
" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"host37-235.pool80181.interbus
iness.it - - [09/Jun/2004:17:09:27 +0200] "GET / HTTP/1.1" 304 - "-" "Mozilla/4.0 (
compatible; MSIE 6.0; Windows NT 5.1)"host37-235.pool80181.interbusiness.it - - [09
/Jun/2004:17:09:27 +0200] "GET /picture01.jpg HTTP/1.1" 304 - "-" "Mozilla/4.0 (com
patible; MSIE 6.0; Windows NT 5.1)"host37-235.pool80181.interbusiness.it - - [09/Ju
n/2004:22:51:17 +0200]"GET / HTTP/1.1" 304 - "-" "Mozilla/4.0 (compatible; MSIE 6.0;
Windows NT 5.1)"host37-235.pool80181.interbusiness.it - - [09/Jun/2004:22:51:17 +02
00] "GET /picture01.jpg HTTP/1.1" 304 - "-" "Mozilla/4.0 (compatible; MSIE 6.0; Win
dows NT 5.1)"host37-235.pool80181.interbusiness.it - - [09/Jun/2004:22:58:06 +0200]
 "GET / HTTP/1.1" 304 - "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"host
37-235.pool80181.interbusiness.it - - [09/Jun/2004:22:58:06 +0200] "GET / HTTP/1.1"
304 - "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"host37-235.pool80181.
```

- Generazione automatica
- Assenza di dati personali
- Caducità

Collaborazione con il settore privato

- ***1997 : Conferenza sul computer crime (FBI - Chase Manhattan Bank)***
- ***2000-1 : Dialogo con le industrie (Parigi – Berlino - Tokyo)***
- ***2005 : TTE sulle IC***

INDICAZIONI UTILI ALLE INDAGINI: I file di log



File di Log

Data

Ora

Durata Connessione

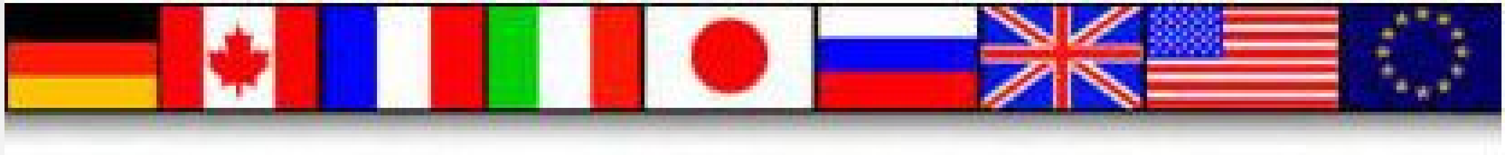
Ip dell'Utente

Finalità

Caller Id Utente

Collaborazione investigativa

G – 8
Sottogruppo *High Tech Crime*



- rete 24 / 7

G 8 - Group of Eight

Il Sottogruppo High-Tech Crime

- Nel 1997, i Ministri della Giustizia e dell’Interno si rivolsero al Gruppo di Lione per rispondere al crescente problema del crimine informatico transnazionale.

- Il Gruppo di Lione convocò il primo meeting del Sottogruppo High-Tech Crime.

G 8 - Group of Eight

Washington Communiqué

10 dicembre 1997

- Riconoscimento della natura internazionale del crimine informatico e della necessità di soluzioni internazionali

- I “Ten Principles”
  - Sviluppo di misure legislative globali sostanziali e processuali che escludano i “paradisi informatici”;
  - Addestrameto ed allocazione di risorse dedicate;
  - Definizione di protocolli per la celere cooperazione internazionale, proceduralale ed operativa
  - Sinergia con l’industria di settore

G 8 - Group of Eight

Principi e Piano d'Azione

- Ten Point Action Plan
  - Designate 24/7 Points of Contact
  - Take steps to increase training and resources
  - Review Legal Systems
  - Develop solutions for data preservation and access to data
  - Develop expedited procedures for obtaining traffic data across international borders and passing data internationally
  - Develop compatible forensics standards
  - Encourage security standards and technology

G 8 - Group of Eight

La rete 24 / 7 - definizione

- Una lista di “International Points of Contact”
- Carattere sperimentale
- In grado di assicurare una celere risposta per il contrasto del crimine High Tech
- Allo scopo di integrare senza sostituire i canali internazionali tradizionali

G 8 - Group of Eight

La rete 24 / 7 - obiettivo

- Ogni Stati membro deve identificare un idoneo Punto di Contatto

- Il Punto di Contatto deve essere disponibile 24h/7gg attraverso telefoni mobili e fissi, fax, email, ecc.

- Il Punto di Contatto è responsabile della ricezione e dell'inoltro delle richieste di cooperazione da/verso i Paesi membri.

G 8 - Group of Eight

G – 8
High Tech Crime Subgroup
Rete Punti di Contatto 24/7

- Reclutamento internazionale
  - 1999 – 8
  - 2000 – 16
  - 2009 – 52 (aprile)

G 8 - Group of Eight

G – 8
High Tech Crime Subgroup
Rete Punti di Contatto 24/7

- Training Conferences
  - Roma, marzo 2003 (23)
  - Roma, ottobre 2006 (42)
  - Roma, in corso di programmazione

G 8 - Group of Eight

Per l'Italia le funzioni sono svolte dal Servizio Polizia Postale e delle Comunicazioni

D. M. INTERNO 19.1.1999

Art. 1

Il Servizio Polizia Postale e delle Comunicazioni è organo centrale del Ministero dell'Interno per la sicurezza e la regolarità dei servizi delle telecomunicazioni

Article 35: 24/7 Network

Each Party shall designate a point of contact available on a 24 hour, 7-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include the following measures:

- the provision of technical advice;
- the preservation of data pursuant to Articles 29 and 30;
- the collection of evidence, the provision of legal information, and locating of suspects.

Article 35: 24/7 Network

-2-

- A Party’s point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.
- If the point of contact designated by a Party is not part of that Party’s authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

Article 35: 24/7 Network

-3-

- Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Explanatory Report

Title 3 – 24/7 Network
24/7 Network (Article 35)
Paragrafi 298 - 302

298. (…) effective combating of crimes committed by use of computer systems and effective collection of evidence in electronic form requires very rapid response. (…) For this reason, existing police co-operation and mutual assistance modalities require supplemental channels to address the challenges of the computer age effectively. The channel established in this Article is based upon the experience gained from an already functioning network created under the auspices of the G8 group of nations. (…) It was agreed that establishment of this network is among the most important means provided by this Convention of ensuring that Parties can respond effectively to the law enforcement challenges posed by computer- or computer-related crime.

Explanatory Report

- 2 -

300. Each Party is at liberty to determine where to locate the point of contact within its law enforcement structure. Some Parties may wish to house the 24/7 contact within its central authority for mutual assistance, some may believe that the best location is with a police unit specialised in fighting computer- or computer-related crime,
(…) due consideration should be given to the need to communicate with points of contacts using other languages.

301. (…) it must have the ability to co-ordinate expeditiously with other relevant components within its government, such as the central authority for international extradition or mutual assistance, in order that appropriate action may be taken at any hour of the day or night. Moreover, paragraph 2 requires each Party's 24/7 contact to have the capacity to carry out communications with other members of the network on an expedited basis.

Explanatory Report

- 3 -

302. Paragraph 3 requires each point of contact in the network to have proper equipment.
(…) also requires that personnel participating as part of a Party's team for the network be properly trained regarding computer- or computer-related crime and how to respond to it effectively

Risultati operativi (pedofilia on line)

276	*Arresti*
5.338	*Denunciati*
4.702	*Perquisizioni*

311.901	*Siti monitorati*
11.034	*Siti pedofili segnalati all'estero*
177	*Siti pedofili chiusi in Italia*

Dal 1998 al 14 luglio 2009

"Let's Make Internet a Safer Place"