Tracciabilità delle operazioni in rete e network forensics

Diritto e Nuove Tecnologie

Campus

4 giugno 2011

www.vincenzocalabro.it

Premessa

Siamo ormai arrivati a quello che Mark Weiser nel lontanissimo 1988 definiva "computer ubiquo" *(ubiquitous computing),* intendendo quel sistema di periferiche talmente **pervasivo** e **capillare** da spostare l'utilizzo della rete sullo sfondo costante delle nostre vite reali.

Se il Web 2.0 è stata la piena realizzazione della promessa di un **internet collaborativo** – nel quale gli utenti potevano creare anziché consumare: pensate a Flickr, Facebook, Wikipedia - il Web 3.0 farà loro **dimenticare che stanno creando in rete**.

Quando il sistema GPS del tuo telefono informa un negozio d'interesse della tua presenza, quando Facebook usa il riconoscimento facciale per taggare le foto che posti, quando i tuoi movimenti finanziari vengono tracciati mediante carta di credito in real-time, **qualcosa sta cambiando!**

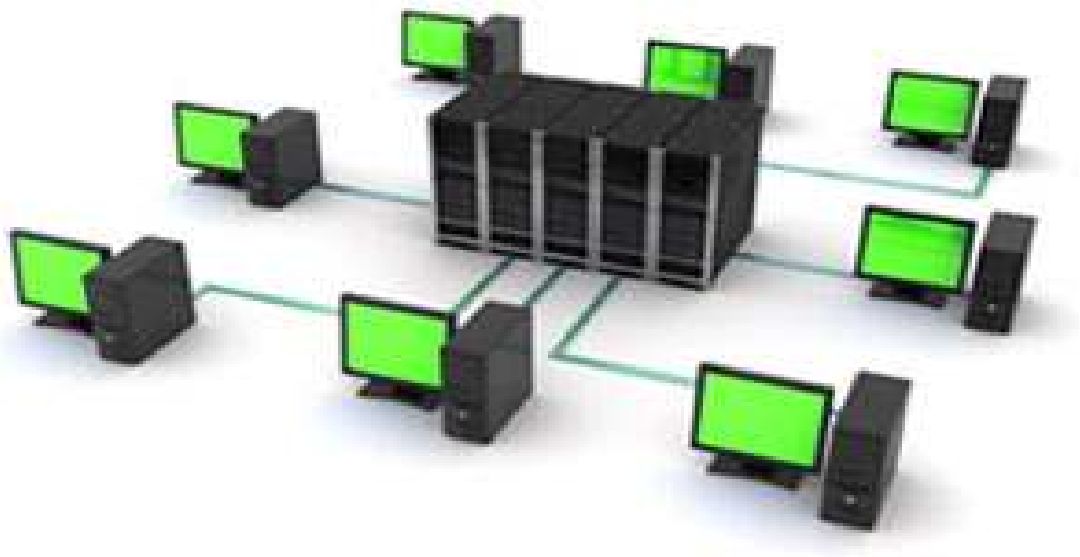
Le tracce

Distinguiamo due tipologie:

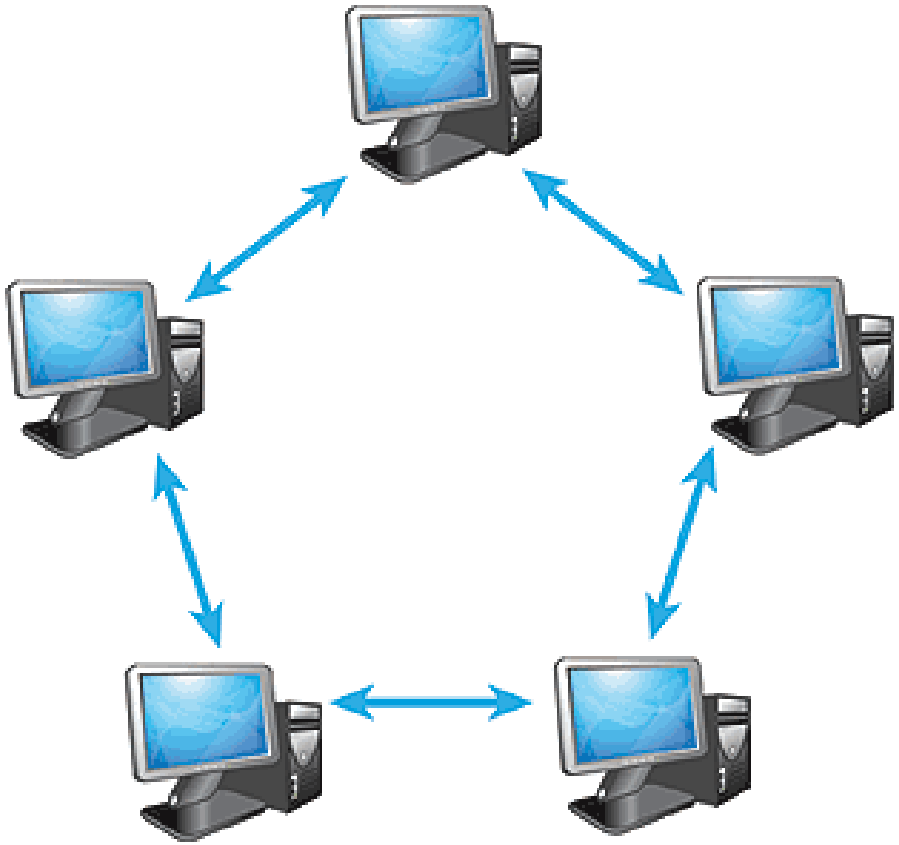
1. Quelle che dimostrano l'avvenuta connessione:
   - **i Log file**, si trovano sugli apparati di comunicazione (switch, router, firewall, ids,...)
   - **i Tabulati del traffico telefonico o dati**, si trovano sui server dei provider telefonici o degli ISP (Internet Service Provider)
2. Quelle che rappresentano il contenuto della comunicazione, o parte di essa:
   - **i Log file di sistema,** presenti nei terminali di comunicazione (sia client che server)
   - **le Memorie di Massa o Cache**, presente nei client di connessione, nei dispositivi proxy, ed i server di rete

Paradigma: Client-Server

- WWW
- Web services
- Email, Newsletter
- Newsgroup
- FTP
- Video-on-demand
- Voip
- Social network
- Cloud computing

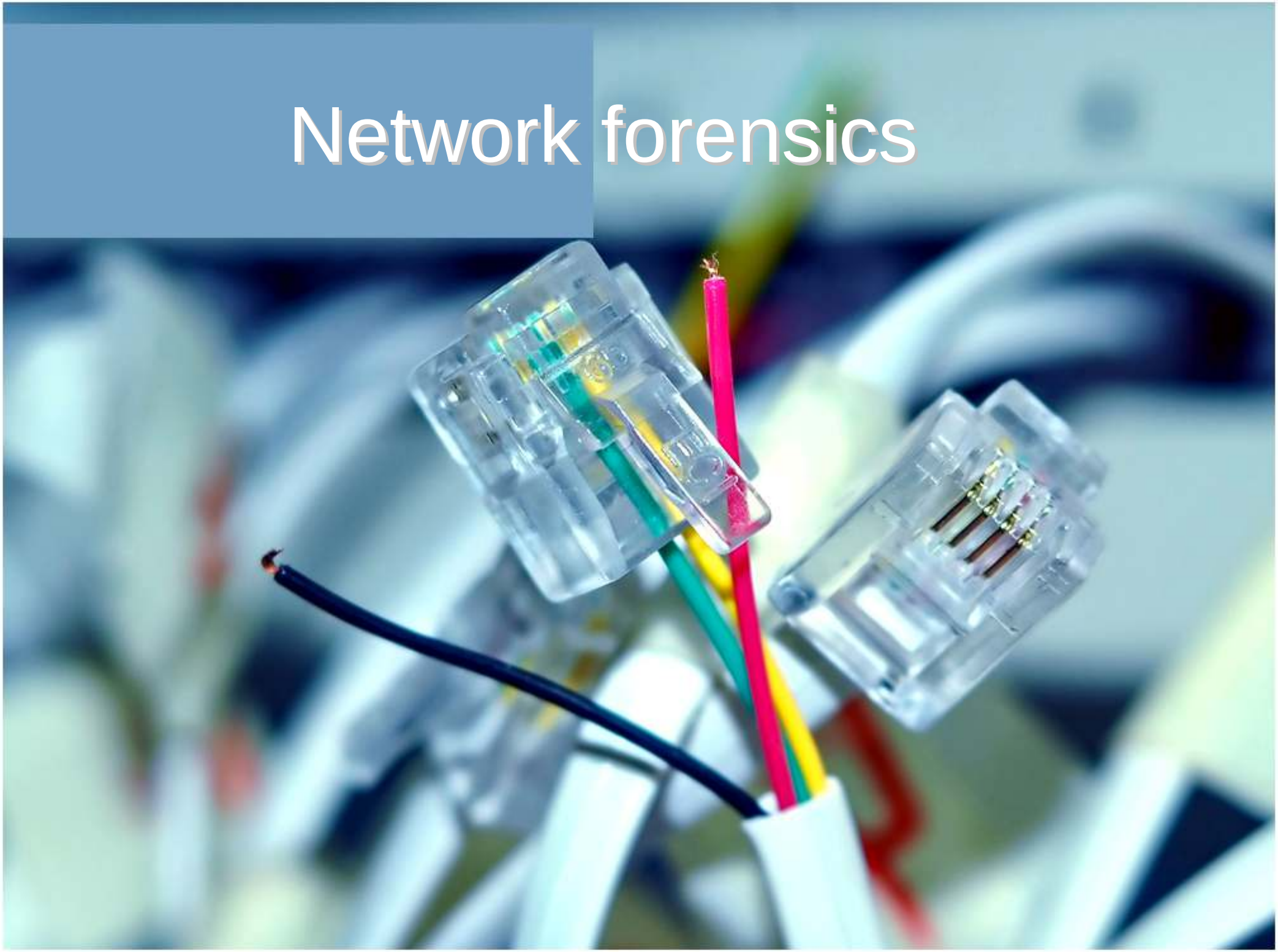


Paradigma: Peer-to-Peer



- Chat (IRC)
- Instant messaging
- Web P2P (Osiris)
- Voip P2P (Skype)
- File sharing (Emule, Kazaa, ecc.)
- Streaming media
- Distributed search engine
- Grid computing

Network forensics



Cos’è la Network forensics?

Si riferisce all’analisi dei sistemi di rete, ivi inclusa la Rete delle reti ossia Internet, al fine di determinare elementi probatori inerenti un determinato caso investigativo.

Si distingue dalla **Network Security**, con cui condivide gli strumenti, perché opera in ambito legale e si occupa delle violazioni delle leggi.

Ambiti di applicazione

"… è il prelievo, la memorizzazione e l'analisi degli eventi di rete al fine di identificare la sorgente degli attacchi alla sicurezza o l'origine di altri problemi del sistema di rete…"

M. Ranum, *Network Forensics and Traffic Monitoring*, Computer Security Journal, Vol. XII, 1997

Distinguiamo:

1. **Ambiti locali (LAN)**
2. **Ambiti geografici (WAN e Internet)**

Metodologie d’analisi

ANALISI REAL TIME o LIVE

Nel contesto delle investigazioni tramite intercettazione telematica, vi è la necessità di conoscere una pluralità di componenti hardware e software per poter eseguire qualsiasi tipo di attività

Componenti hardware di una rete più comuni:

- Hub
- Switch
- Router
- Firewall
- Sonda di rete
- Bilanciatore

Approccio

1. Si individua il target da intercettare
2. Si studiano i software ed i protocolli da analizzare

3. Si sceglie il punto di ascolto, ovvero dove conviene agganciarsi
4. Si inserisce l’apparato d’intercettazione appropriato

5. Si registra il flusso telematico catturato su un dispositivo sicuro
6. Si analizza il traffico acquisito

Analisi

Problematiche da affrontare:

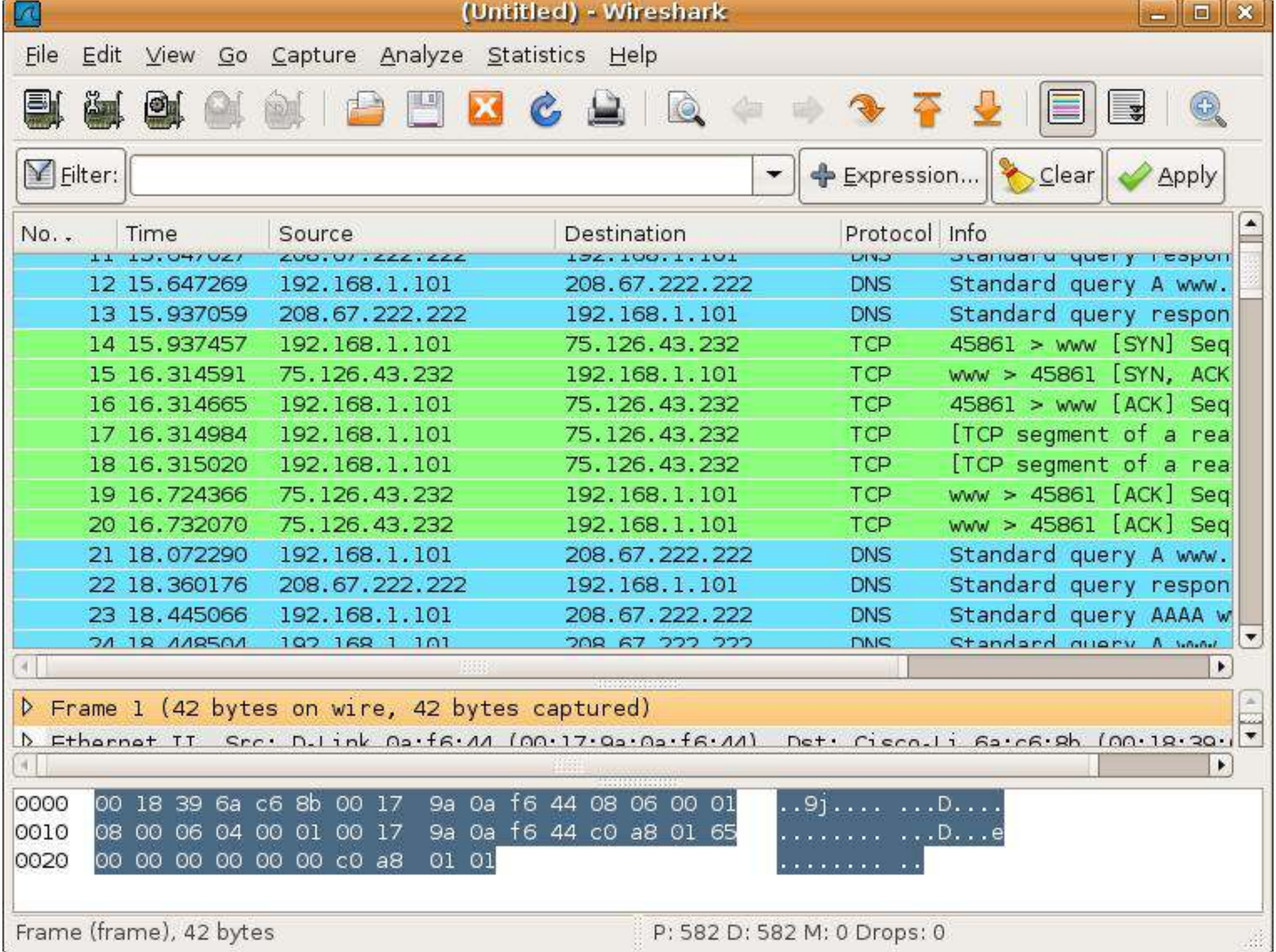
- mole di dati spesso molto elevate
- ricostruzione del dato acquisito
- ricostruzione delle sessioni e dei collegamenti

Utilizzo di software per una giusta interpretazione dei dati:

- Editor testuale (???)
- Wireshark
- Xplico

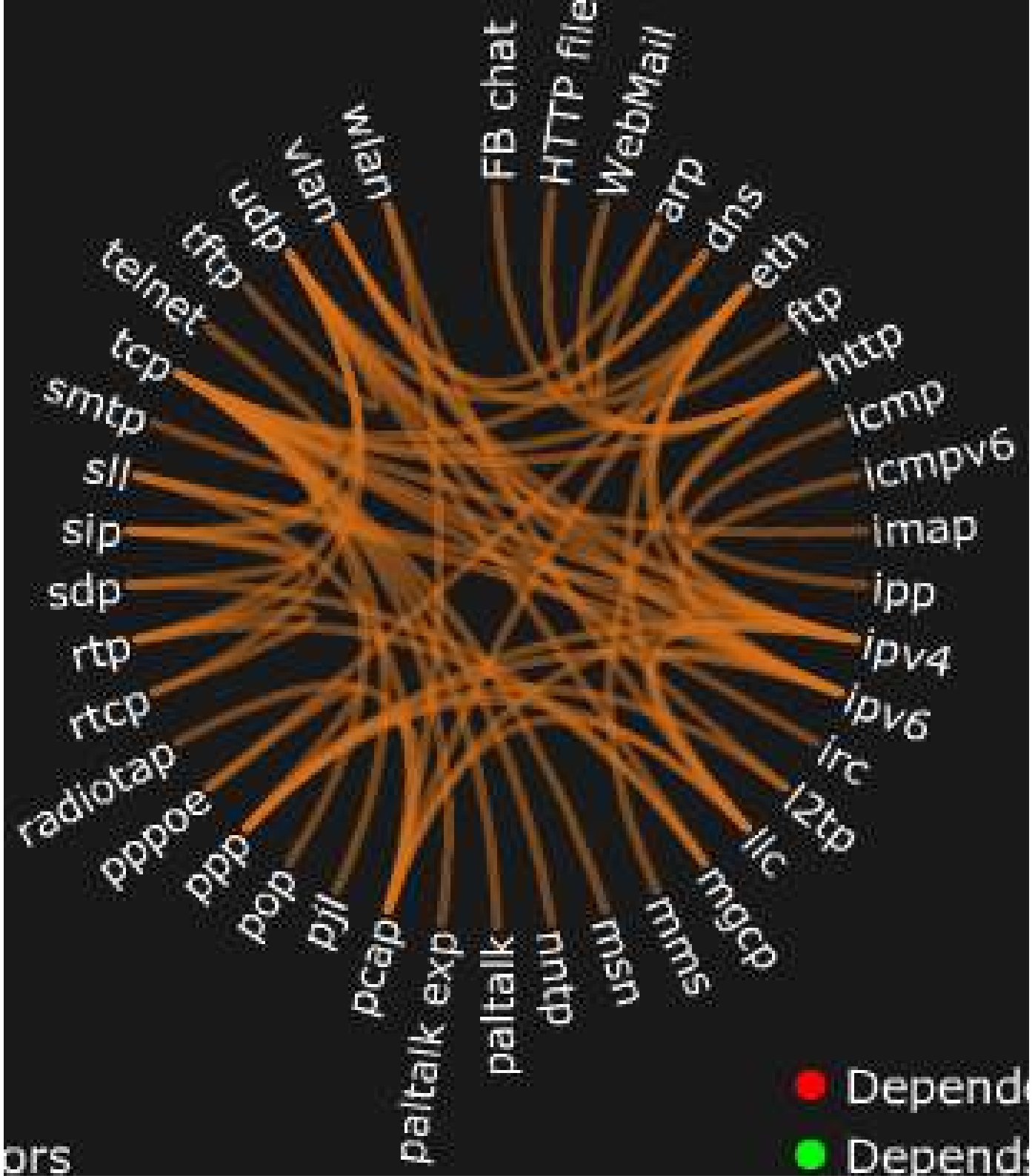
www.wireshark.org

- Possibilità di analizzare dati acquisiti in tempo reale su una rete attiva
- I dati possono essere acquisiti dal vivo su reti Ethernet, FDDI, PPP, Token Ring, IEEE 802.11, IP classico su ATM, e interfacce di loopback (non tutti i tipi sono supportati su tutte le piattaforme)
- Possibilità di filtrare i dati da visualizzare utilizzando filtri di visualizzazione per colorare o evidenziare selettivamente le informazioni sommarie sui pacchetti
- È possibile scomporre e analizzare centinaia di protocolli di comunicazione


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply
No. Time Source Destination Protocol Info
12 15.647269 192.168.1.101 208.67.222.222 DNS Standard query A www.
13 15.937059 208.67.222.222 192.168.1.101 DNS Standard query respon
14 15.937457 192.168.1.101 75.126.43.232 TCP 45861 > www [SYN] Seq
15 16.314591 75.126.43.232 192.168.1.101 TCP www > 45861 [SYN, ACK
16 16.314665 192.168.1.101 75.126.43.232 TCP 45861 > www [ACK] Seq
17 16.314984 192.168.1.101 75.126.43.232 TCP [TCP segment of a rea
18 16.315020 192.168.1.101 75.126.43.232 TCP [TCP segment of a rea
19 16.724366 75.126.43.232 192.168.1.101 TCP www > 45861 [ACK] Seq
20 16.732070 75.126.43.232 192.168.1.101 TCP www > 45861 [ACK] Seq
21 18.072290 192.168.1.101 208.67.222.222 DNS Standard query A www.
22 18.360176 208.67.222.222 192.168.1.101 DNS Standard query respon
23 18.445066 192.168.1.101 208.67.222.222 DNS Standard query AAAA w
Frame 1 (42 bytes on wire, 42 bytes captured)
0000 00 18 39 6a c6 8b 00 17 9a 0a f6 44 08 06 00 01 ..9j.... ...D....
0010 08 00 06 04 00 01 00 17 9a 0a f6 44 c0 a8 01 65 ....D...e
0020 00 00 00 00 00 00 c0 a8 01 01 ....
Frame (frame), 42 bytes
P: 582 D: 582 M: 0 Drops: 0

Xplico.org

Consente una ricostruzione completa dei seguenti contenuti intercettati usando come unica risorsa la capture eseguita



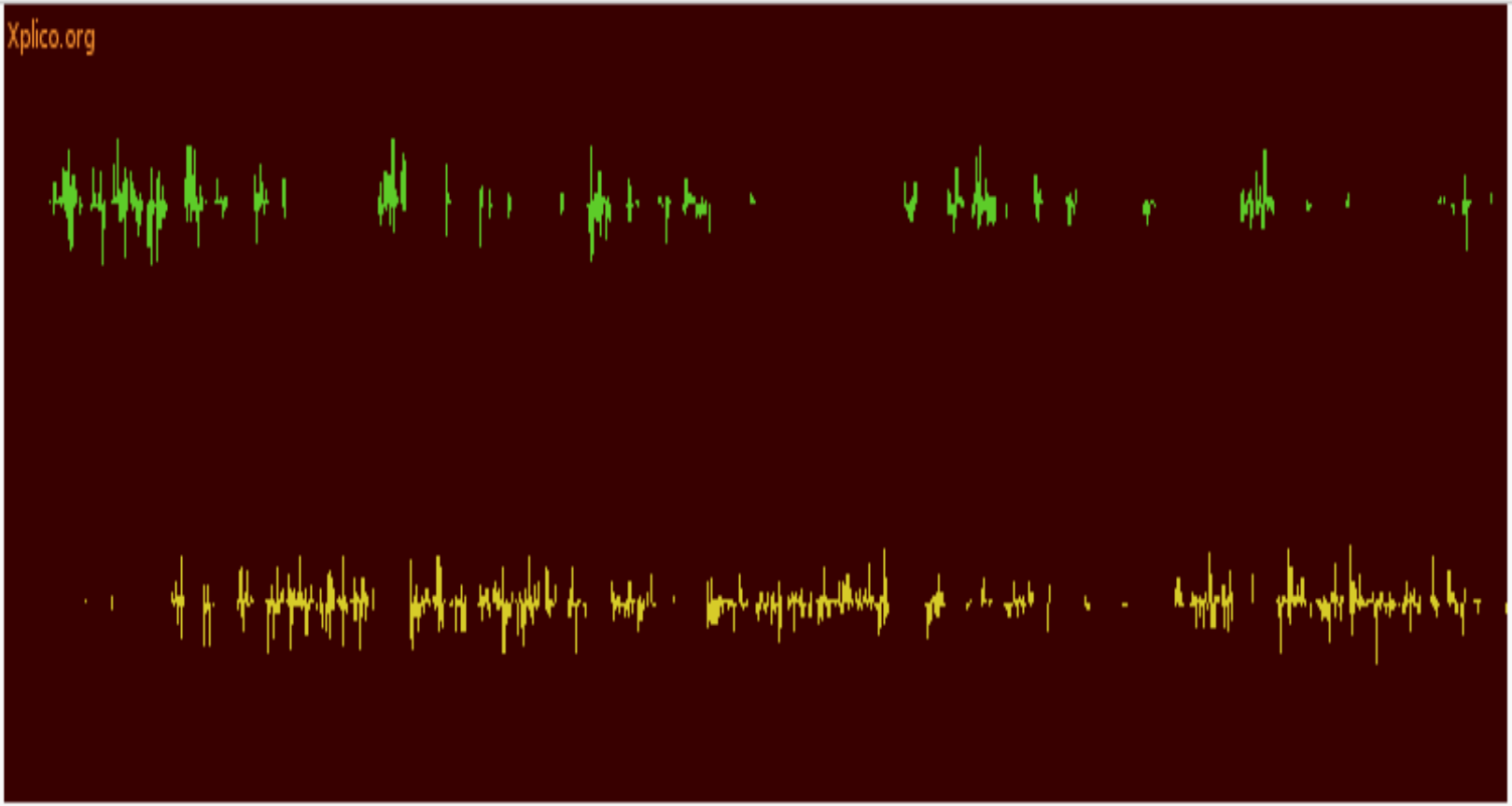
Xplico Interface

User: xplico

Help Forum Wiki Logout

- Case
- Graphs
- Web
- Mail
- Voip
  - Sip
  - Rtp
- Share
- Chat
- Shell
- Undecod

Date:	2010-03-07 11:58:31	
From:	192.168.0.121	play
To:	62.94.199.34	play
Duration:	0:3:48	
Info	info.xml	



Cases
Sols
Email
Sip
Web
Images
Printer
Ftp
Mms
GeoMap

Email to <info@iserm.com>

Subject:	*****SPAM***** Magic is real
Sender:	Shannon Palacios <shraga.davenport@armhule.dk>
Recipient:	
Date:	Tue, 14 Aug 2007 09:05:56 -0900
Username:	
Password:	
EML file:	email.eml
Info:	info.xml

Spam detection software, running on the system "mxavas14.fe.aruba.it", has identified this incoming email as possible spam. The original message has been attached to this so you can view it (if it isn't spam) or label similar future email. If you have any questions, see http://vademecum.aruba.it/start/mail/antispam/ for details.

Content preview: [...]

Content analysis details: (5.1 points, 5.0 required)

pts rule name description

Attached message E-mail message

http://espn.go.com - ESPN: The Worldwide Leader In Sports - Mozilla Firefox

Search | en Español | Sign In | Click here to sign in to ESPN.com | TV Listings | ESPN

ESPN NFL MLB NBA NASCAR IRL NHL College Golf Soccer Page 2 SportsNation Inside

Spilling The Beans

Koichi Kamoshida/Getty Images

Matsuzaka, 26, may command another $45 million to pitch in Boston.

That first $51.1 million? Just the down payment on Daisuke Matsuzaka. So, will Boston be willing to spend another five billion yen? It better be. Blowing this international merger isn't an option. **Jerry Crasnick**

- Red Sox outbid Mets, Yankees | Gammons: A wise investment
- Vote: Is he worth it? | Top 40 free agents | Free agent tracker

Spotlight ▸ 1 vs. 2 | NCAA | Knight | NBA | NFL | Voices

LT and the Chargers only trail two teams in our latest Power Rankings after that miraculous rally against Cincy.

The NFC path to Super Bowl XLI most likely will wind its way through Chicago. So who will face the Bears? **Scouts Inc.**

Redskins fans may wish that Jason Campbell got the starting QB job earlier, but they won't dislike the move. **Pasquarelli**

ESPN360 COMPLETE COVERA THE HISTORICAL RI

CLICK TO

NFL

Kansas City Miami

Scoreboards: NF

ESPNEWS Headline

- Knight: I did nothing
- Skin problem: Porti
- Webb gem: D-Bac
- Chiefs QB Green c
- Fall guy? Bowden's
- Capital gain: Acta t
- Spurs rally, stun R
- Horford sparks Ga
- Rangers net 3 goa
- O.J. to discuss kill
- Hollinger: The NBA
- Karabell: Finding s

More Head

ESPN.com's H NFL power ran

BILL SIMMON

What the heck is go world? Nothing mak

- Upside down work
- Sports Guy's Wor

Completato

Xplico : Webs - Mozilla Firefox

File Modifica Visualizza Cronologia Segnalibri Strumenti Guida

http://localhost:71/webs/index

Tmp iS Creatività AI OS Linux Embed Java HW Web Market Doc Anime

Xplico demo

Welcome deft

Help Logout

Cases
Sols
Email
Sip
Web
Image

This version can be inaccurate in displaying Web pages.

Web URLs: Html Image Flash Video Audio All Go

2006-11-27 06:23:36	c5.zedo.com/jsc/c5/ff2.html?n=636;c=2;s=1;d=7;w=160;h=600
2006-11-27 06:23:32	www.bittorrent.com/search_result.html?client=M5-0-1--a7ae16bc8183&search=madon
2006-11-15 07:26:06	espn-ak.starwave.com/media/motion/2006/1114/hu_061114vitale.jpg
2006-11-15 07:26:04	ad.trafficmp.com/tmpad/banner/ad/tmp.asp?polD=elKk
2006-11-15 07:26:03	ads.espn.adsonar.com/adserving/getAds.jsp?placementId=1266745&&&pid=605757&p
2006-11-15 07:26:03	ads.espn.adsonar.com/adserving/getAds.jsp?&placementId=1265726&pid=605757&ps
2006-11-15 07:26:03	ads.espn.adsonar.com/adserving/getAds.jsp?placementId=1265725&&&pid=605757&p
2006-11-15 07:25:59	sports.espn.go.com/espn/fp/pollDataGenState?pollId=40691
2006-11-15 07:25:58	espn.go.com/undefined
2006-11-15 07:25:57	espn.go.com/motion/fsp/index.html?fp=true
2006-11-15 07:25:56	amch.questionmarket.com/adscgen/log_ut_err.php?adserver=DART&survey_num=26
2006-11-15 07:25:56	amch.questionmarket.com/adscgen/st.php?survey_num=266261&site=14836883&cod
2006-11-15 07:25:52	ad.doubleclick.net/adi/N1942.espn.com/B2000495;sz=728x90;click=http://log.go.com/
2006-11-15 07:25:42	espn.go.com/
2006-11-15 07:25:42	www.espn.com/
2006-03-10 03:33:44	b.rad.msn.com/ADSAdClient31.dll?GetSAd=&PG=NBCPLB&AP=1402
2006-03-10 03:33:42	view.atdmt.com/MSN/iview/msnnkhac001300x250Xnbcfc100151msn/direct/01

FIREFOX 2 | Xplico org | iSerm com | CAKEPHP POWER

Completato

ANALISI POST MORTEM

A volte, nelle investigazioni digitali, vi è la necessità di ottenere ulteriori informazioni a sostegno di una determinata tesi.

Dalla Network Forensics si possono ottenere altri pezzi di un “puzzle”, ulteriori informazioni su “cosa è successo”, cercando tra le tracce lasciate sugli apparati di rete.

Queste informazioni possono essere utilizzate per:

- Ricostruire le sessioni (ad esempio: web, ftp, telnet, IM)
- Trovare i file (scaricati o consultati sulle unità di rete)
- Trovare le password
- Identificare le macchine remote

Approccio

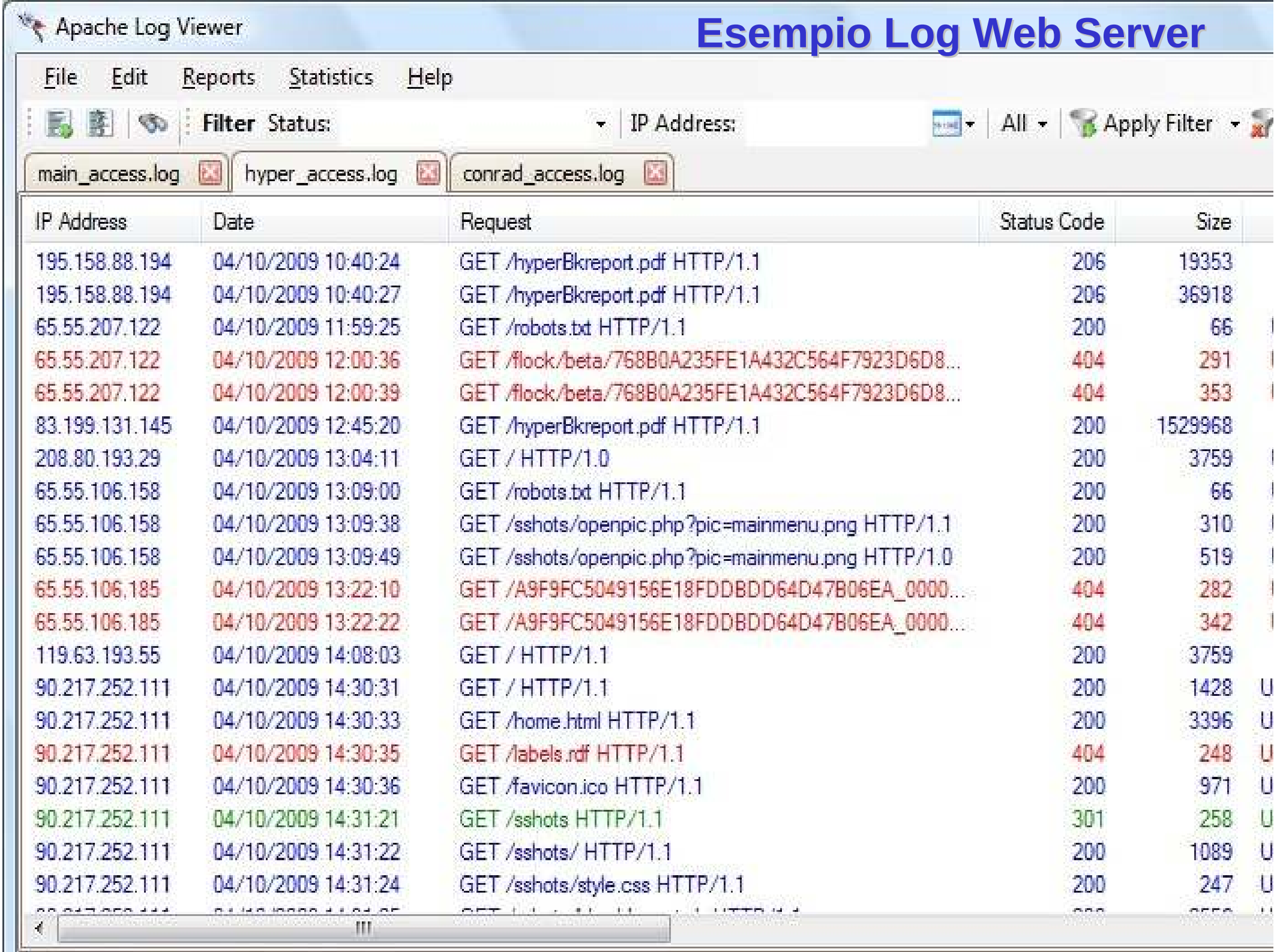
1. Si individua la sorgente e la destinazione della sessione
2. Si verifica quali sistemi e supporti sono stati coinvolti (switch, router, ISP,)
3. Si cercano gli elementi che testimoniano una determinata attività in rete (log, report IDS, journal, …)
4. Si normalizzano i tracciati per ricostruire la comunicazione avvenuta
5. Si individuano le eventuali macchine o supporti di memoria da “girare” alla Computer Forensics

Analisi

Problematiche da affrontare:

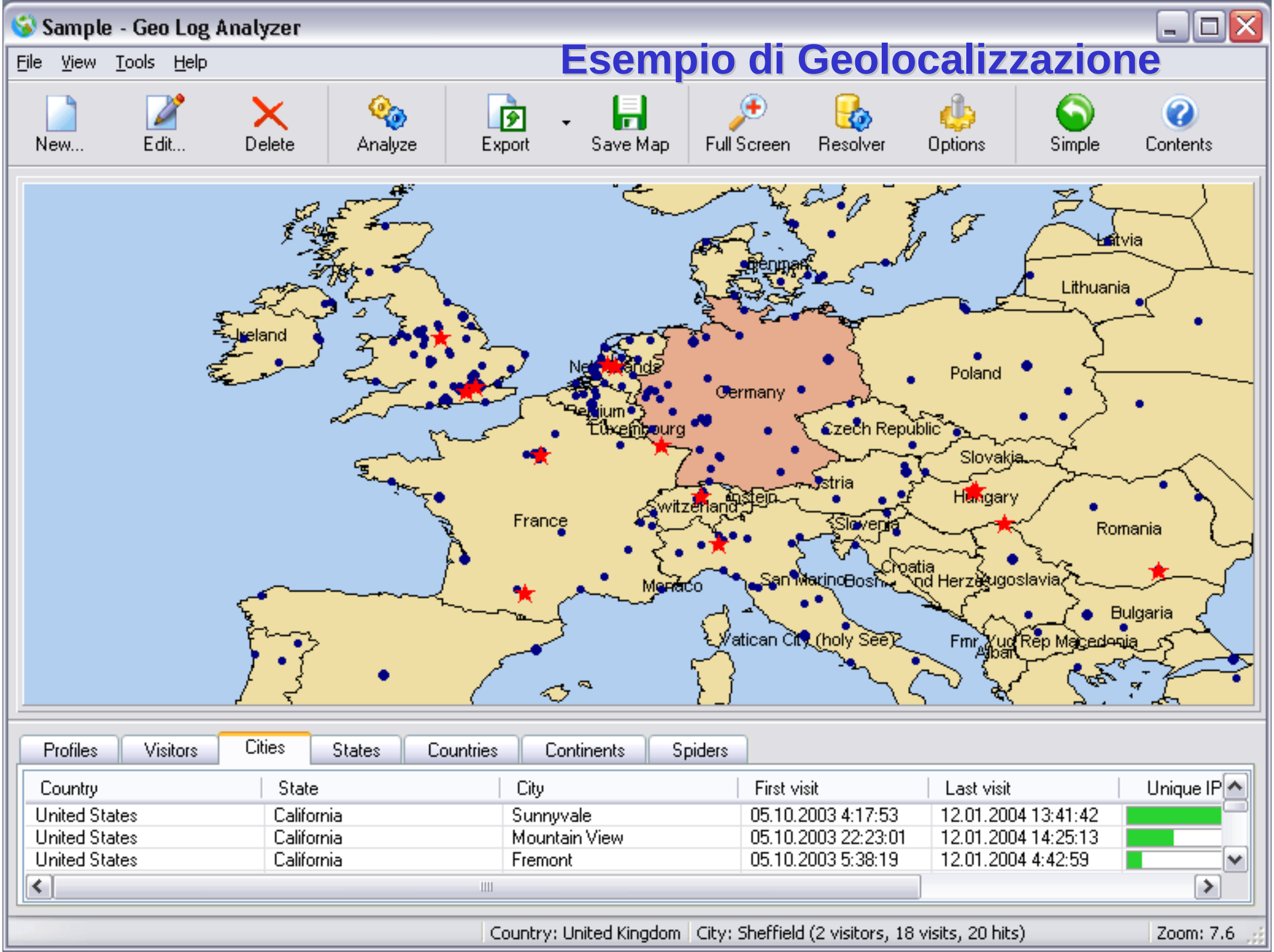
- Sistemi distribuiti
- Raccolta di ipertesti dinamici
- Spesso le macchine non possono essere spente
- Troppi dati da memorizzare
- Difficoltà nel documentare e certificare la copia
- Difficoltà in dibattimento della presentazione dei risultati

Esempio Log Web Server



IP Address	Date	Request	Status Code	Size	
195.158.88.194	04/10/2009 10:40:24	GET /hyperBkreport.pdf HTTP/1.1	206	19353	
195.158.88.194	04/10/2009 10:40:27	GET /hyperBkreport.pdf HTTP/1.1	206	36918	
65.55.207.122	04/10/2009 11:59:25	GET /robots.txt HTTP/1.1	200	66	
65.55.207.122	04/10/2009 12:00:36	GET /flock/beta/768B0A235FE1A432C564F7923D6D8...	404	291	
65.55.207.122	04/10/2009 12:00:39	GET /flock/beta/768B0A235FE1A432C564F7923D6D8...	404	353	
83.199.131.145	04/10/2009 12:45:20	GET /hyperBkreport.pdf HTTP/1.1	200	1529968	
208.80.193.29	04/10/2009 13:04:11	GET / HTTP/1.0	200	3759	
65.55.106.158	04/10/2009 13:09:00	GET /robots.txt HTTP/1.1	200	66	
65.55.106.158	04/10/2009 13:09:38	GET /sshots/openpic.php?pic=mainmenu.png HTTP/1.1	200	310	
65.55.106.158	04/10/2009 13:09:49	GET /sshots/openpic.php?pic=mainmenu.png HTTP/1.0	200	519	
65.55.106.185	04/10/2009 13:22:10	GET /A9F9FC5049156E18FDDBDD64D47B06EA_0000...	404	282	
65.55.106.185	04/10/2009 13:22:22	GET /A9F9FC5049156E18FDDBDD64D47B06EA_0000...	404	342	
119.63.193.55	04/10/2009 14:08:03	GET / HTTP/1.1	200	3759	
90.217.252.111	04/10/2009 14:30:31	GET / HTTP/1.1	200	1428	U
90.217.252.111	04/10/2009 14:30:33	GET /home.html HTTP/1.1	200	3396	U
90.217.252.111	04/10/2009 14:30:35	GET /labels.rdf HTTP/1.1	404	248	U
90.217.252.111	04/10/2009 14:30:36	GET /favicon.ico HTTP/1.1	200	971	U
90.217.252.111	04/10/2009 14:31:21	GET /sshots HTTP/1.1	301	258	U
90.217.252.111	04/10/2009 14:31:22	GET /sshots/ HTTP/1.1	200	1089	U
90.217.252.111	04/10/2009 14:31:24	GET /sshots/style.css HTTP/1.1	200	247	U

Esempio di Geolocalizzazione



Sorgente di: mailbox:///C|/Documents%20and%20Settings/vincenzo/Dati%20applicazioni/Thunderbird/Profiles/1u2xahg6.default

File Modifica Visualizza Aiuto

Esempio Email Header

```
From - Wed May 18 10:02:09 2011
X-Account-Key: account3
X-UIDL: 56877
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
X-Mozilla-Keys:
Return-Path: <register@datahjaelp.com>
Received: from imp-1.mail.tiscali.it (10.39.115.248) by mx-1-it.mail.tiscali.it (8.5.137)
        id 4DCBA92902329843 for vcalabro@tiscali.it; Wed, 18 May 2011 10:02:09 +0200
Received: from mail2.datahjaelp.net ([82.103.132.158])
        by imp-1.mail.tiscali.it with
        id kw281g00J3RCPiA01w28q4; Wed, 18 May 2011 10:02:09 +0200
X-Tiscali-SPF-Pass: TRUE
Received: from localhost (localhost [127.0.0.1])
        by mail2.datahjaelp.net (Postfix) with ESMTP id BC782AA120
        for <vcalabro@tiscali.it>; Wed, 18 May 2011 10:02:07 +0200 (CEST)
X-Virus-Scanned: amavisd-new at mail2.datahjaelp.net
Received: from mail2.datahjaelp.net ([127.0.0.1])
        by localhost (mail2.datahjaelp.net [127.0.0.1]) (amavisd-new, port 10024)
        with ESMTP id nEKiGRbEb7HS for <vcalabro@tiscali.it>;
        Wed, 18 May 2011 10:02:02 +0200 (CEST)
Received: from mail.datahjaelp.net (unknown [92.246.24.225])
        (using TLSv1 with cipher ADH-AES256-SHA (256/256 bits))
        (No client certificate requested)
        by mail2.datahjaelp.net (Postfix) with ESMTPS id 6844AAA101
        for <vcalabro@tiscali.it>; Wed, 18 May 2011 10:02:02 +0200 (CEST)
Received: by mail.datahjaelp.net (Postfix, from userid 33)
        id 18746AA0CF; Wed, 18 May 2011 10:02:02 +0200 (CEST)
To: vcalabro@tiscali.it
Subject: =?ISO-8859-1?Q?Zip_Password_Recovery_serial_key.?=
X-PHP-Originating-Script: 33:libmail.php
Organization: Datahjaelp
From: register@datahjaelp.com
```

6

5

4

3

2

1

0

Notifica della limitazione dell'accesso al conto

Poste Italiane [notifica@poste.it]

Messaggio con priorità Alta.

A:

Posteitaliane

Gentile Cliente,

Nell'ambito delle misure di sicurezza da noi adottate, controlliamo costantemente le attività del sistema. Durante una recente verifica, abbiamo rilevato un problema riguardante il tuo conto.
Abbiamo deciso di limitare l'accesso al tuo conto fino a quando non verrà completata l'implementazione di misure di sicurezza aggiuntive.

Per controllare il tuo conto e le informazioni che Poste Italiane ha utilizzato per decretare di limitare l'accesso al conto, visita il seguente sito:

https://www.poste.it/online/personale/login-home.fcc

http://74.95.34.43/%20/www.poste.it/index.php?MfcISAPICommand=SignInFPP&UsingSSL=1&email=&userid

Se, dopo aver controllato le informazioni sul conto, desideri ulteriori chiarimenti riguardo all'accesso al conto, contatta il modulo Contattaci nell'Aiuto.

Ci scusiamo per gli eventuali disagi.

Cordiali saluti,
© Poste Italiane 2008

Esempio Phishing

16-00000000043BF719EC0EAB4590668F9C327E880C04FC3500[1] - Blocco note

File Modifica Formato Visualizza ?

Esempio Phishing

```
<html>
<div align="center">
<table width="459" border="0" align="left" cellpadding="5">
<tr>
<td  width=445 align="left"><img src="http://www.poste.it/img/homepage/logoposte_home.gif" alt="Poste Italiane"></td>
</tr>
<tr>
  <td align="left"><p><font face=Times New Roman, Times, serif size=3><strong>Gentile Cliente,</strong></font><font face
    </font>
    <p><font face="Times New Roman, Times, serif">Nell'ambito delle misure di sicurezza da noi adottate, controlliamo
      costantemente le attivit&agrave; del sistema. Durante una recente verifica,
      abbiamo rilevato un problema riguardante il tuo conto.<br>
      Abbiamo deciso di limitare l'accesso al tuo conto fino a quando non verr&agrave;
      completata l'implementazione di misure di sicurezza aggiuntive.<br>
    </font>
    <p><font face="Times New Roman, Times, serif">Per controllare il tuo conto e le informazioni che Poste Italiane ha u
      decretare di limitare l'accesso al conto, visita il seguente sito:<br>
      <br>
      <a
href="http://74.95.34.43/%20/www.poste.it/index.php?MfcISAPICommand=SignInFPP&UsingSSL=1&email=&userid">https://www.post
/a><br>
    </font>
    <p><font face="Times New Roman, Times, serif">Se, dopo aver controllato le informazioni sul conto, desideri ulterior
conto, contatta
      il modulo Contattaci nell'Aiuto.<br>
    <br>
    </font>
    <font face="Times New Roman, Times, serif">Ci scusiamo per gli eventuali disagi.<br>
    </font>
    <p><font face="Times New Roman, Times, serif">Cordiali saluti,<br>
    &copy; Poste Italiane 2008</font></p></td>
</tr>
</table>
<p> </p>
<br>
</html>
</div>
<P><FONT SIZE=2 FACE="Arial">No virus found in this incoming message.<BR>
Checked by AVG.<BR>
Version: 8.0.100 / Virus Database: 270.2.0/1494 - Release Date: 10/06/2008 7.22<BR>
</FONT></P>
```


Poste Italiane - Carta postepay - Mozilla Firefox
File Modifica Visualizza Cronologia Segnalibri Strumenti ?
http://74.95.34.43/%20%www.poste.it/
Google
Poste Italiane - Carta postepay
Posteitaliane
Home | Chi siamo | Sala stampa | English
. Registrazione . Accedi
DI COSA HAI BISOGNO?
PRODOTTI
BUSINESS
SERVIZI ONLINE
Carte postepay
Carta postepay
Postepay Gift
Servizi online
Sicurezza
...BancoPostaonline
Servizi online per i titolari di carta postepay
Accedendo ai servizi online puoi visualizzare le informazioni (saldo, lista movimenti, ricarica online) relative alla tua carta, pagare i bollettini ed effettuare le ricariche
Inserisci i tuoi dati identificativi:
Nome utente: mario.rossi
Password: **********
Esegui
Come utilizzare i servizi della carta postepay
Per utilizzare su www.poste.it i servizi online della carta postepay (informazioni, pagamento di bollettini, ricariche, ecc.) occorre essere registrati al sito. Dopo esserti registrato riceverai, nella casella postale Postemail, tutte le comunicazioni relative alla tua carta. Dopo un giorno lavorativo, inserendo i dati identificativi, potrai usufruire dei servizi informativi e dispositivi della carta.
Pagamento bollettini
Con la carta postepay puoi pagare online, in modo semplice e sicuro, i bollettini relativi a utenze, tributi e contravvenzioni.
» Visualizza quali bollettini puoi pagare con carta postepay
» Orari e costi del servizio
» Registrazione al sito
Esempio Phishing
Contattaci | Privacy | Mappa | Trasparenza bancaria | Forniture e gare | Scadenzario fiscale | © Poste Italiane 2007

Esempio Phishing

Localizzazione indirizzo IP

www.lgnet.it/index.php?ip=74.95.34.43

LGNET
LOCALIZZAZIONE PROFESSIONALE DI INDIRIZZI IP

LOCALIZZAZIONE INDIRIZZI IP | PERCHÉ LOCALLIZZARE L'IP? | ISCRIZIONE | IMPLEMENTAZIONE | FAQ | CONTATTACI | SUPPORT

Localizzazione indirizzo IP (gratis)

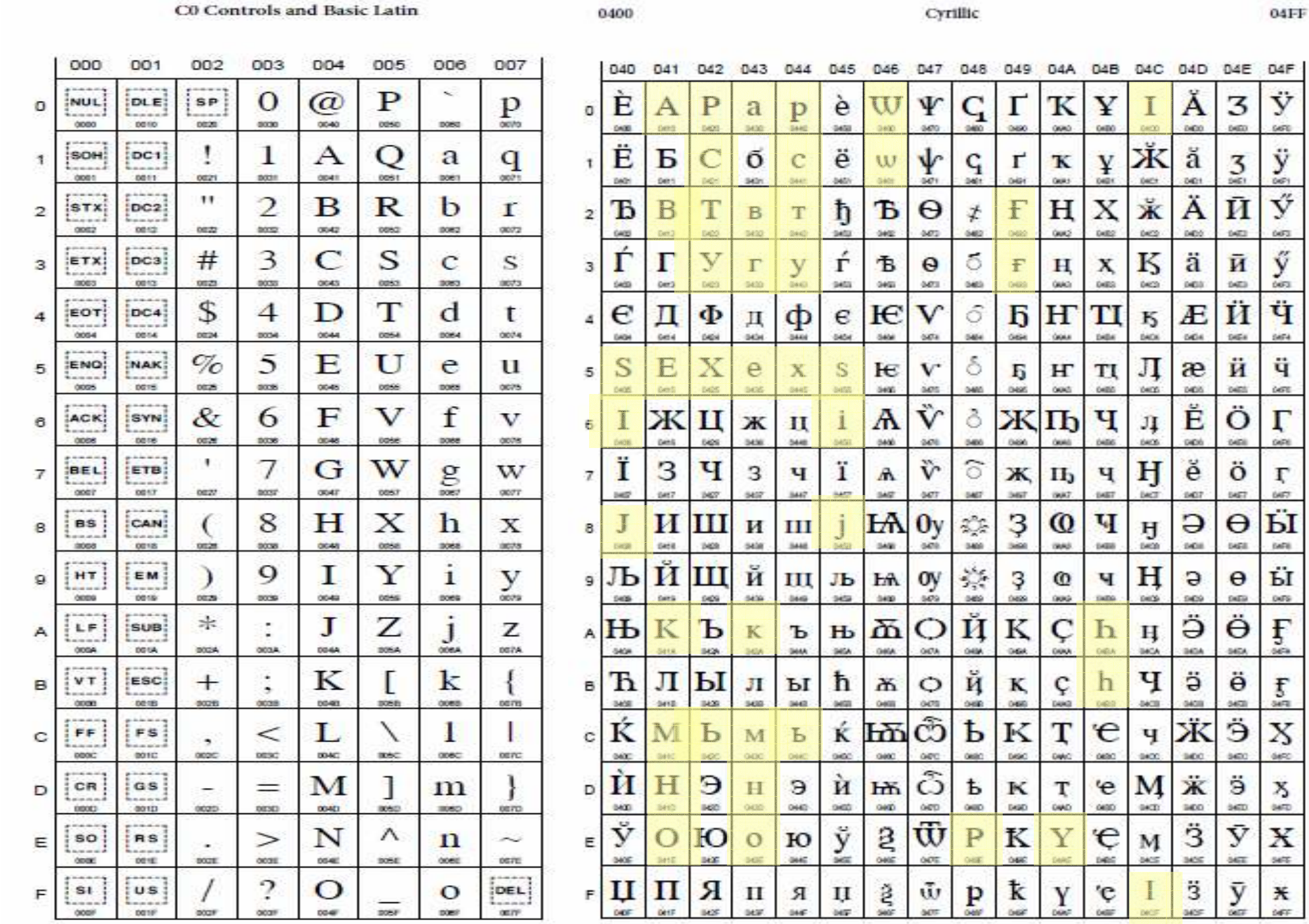
LGNET offre la più accurata e più moderna localizzazione geografica dell'indirizzo IP del visitatore. Risponde ai webmaster in millisecondi con **nazione, regione, città, coordinate terrestre** ed altre informazioni. Nelle database di LGNET sono presenti tra l'altro **9.700 città italiane** e quasi **un millione di indirizzi IP italiani**.

74.95.34.43 [localizza]

Localizzazione del indirizzo IP 74.95.34.43:

Nazione: Stati Uniti
Regione: Oregon
Città: Portland
Provider: Comcast Business Communications
Nome a dominio: 74-95-34-43-Oregon.hfc.comcastbusiness.net
Latitudine: 45.5184
Longhitudine: -122.6554

homograph spoofing attacks



Considerazioni finali

Genuinità dei dati

Nella CF si sono consolidate prassi a garanzia che il supporto analizzato non sia stato alterato prima e dopo l'analisi

Nella NF entrano in gioco tantissime variabili

- Bisogna certificare il processo di ottenimento assieme allo stato della rete in quel momento
- La copia a runtime di dati su una memoria di massa operativa è un'operazione sicuramente irripetibile
- E' molto difficile e complesso chiedersi quali dati recuperare
- Entra in gioco un grado di aleatorietà notevole che rende i dati più un mezzo investigativo (indizi) che elementi probatori

Rischi

Una rete di computer, pur essendo impiegata come mezzo per lo svolgimento di un determinato reato, non è necessariamente tutta coinvolta nel reato stesso: si ha spesso la necessità di allargare l'ambito dell'analisi, ma si rischia di commettere violazioni durante le operazioni che possono implicare danni agli utenti e ricadute economiche

Il personale del sistema informativo non sono minimamente interessati dal reato, ma potrebbero conoscere o mantenere, per ragioni di sicurezza, informazioni determinanti per la dimostrazione dei fatti: l'unico problema è che la metodologia di raccolta e conservazione non sempre corrisponde a canoni forensi e talvolta neanche alle disposizioni sulla privacy

Le autorizzazioni legali

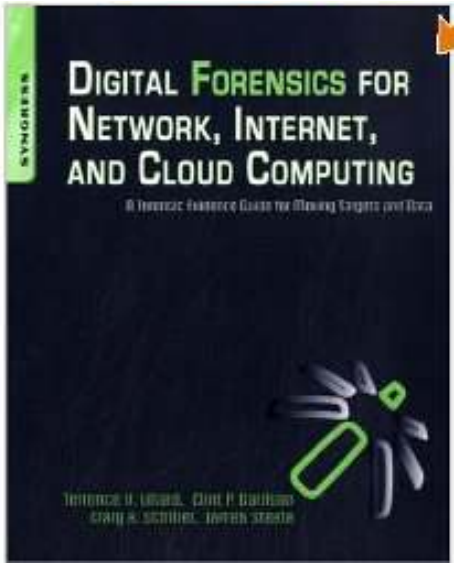
Pertanto vi è la necessità di autorizzazioni specifiche e non generiche di più di quanto accada per la Computer Forensics.

L'aspetto legale si evidenzia perché spesso il NF può essere realizzato attraverso strumenti come il cracking, lo sniffing, il denial of service, ecc. non specificatamente autorizzati dalla magistratura. Queste scorciatoie, problematicamente alla portata di un gran numero di specialisti, conseguono risultati il più delle volte non impiegabili in dibattimento.

I limiti

Infine ci sono dei limiti con cui la Network Forensics deve continuamente fare i conti:

- La sincronizzazione degli orologi
- La mole dei dati
- L’Internazionalità o extraterritorialità
- La Crittografia
- L’Anonimato
- Il Cloud computing
- Le Botnet



Terrence V. Lillard

Digital Forensics for Network, Internet, and Cloud Computing:
A Forensic Evidence Guide for Moving Targets and Data

Syngress; 1 edition (June 16, 2010)

Grazie per l'attenzione

www.vincenzocalabro.it