IL FUTURO DELLA DIGITAL FORENSICS

Limiti e miti forensi.

L'Open Source ci può salvare?

BY

NANNI BASSETTI

INTRODUZIONE

ABOUT ME

CHI SONO

Mi occupo di digital forensics dal **2005/2006**, sono project manager di **CAINE** (distro usata in tutto il mondo)

Fondatore di **CFI** (Computer Forensics Italy)

Scrittore di parecchi articoli scientifici e software free/open source per la D.F.

Membro fondatore di **ONIF** (Osservatorio Informatica Forense).

Scrittore di parecchi articoli scientifici e software free/open source per la D.F.

Coinvolto in casi di rilevanza nazionale come:

* Consulente tecnico informatico di parte civile nel caso del transessuale **"Brenda" (caso Brenda-Marrazzo)**.

* CTP (Consulente tecnico di parte) per gli Avv. Vito Russo ed Emilia Velletri nel caso **Sarah Scazzi** (Avetrana (Ta))

* Consulente tecnico informatico di parte civile nel caso della scomparsa di **Roberto Straccia**

* Consulente tecnico informatico di parte civile nel caso della scomparsa della piccola **Angela Celentano**

Definizione

La Digital Forensics è la disciplina scientifica che serve per identificare, acquisire ed analizzare una fonte di prova digitale, preservandola da eventuali alterazioni.

Scientifica: ripetibile (Galileo Galilei)

è la modalità tipica con cui la scienza procede per raggiungere una conoscenza della realtà oggettiva, affidabile, verificabile e condivisibile. Esso consiste, da una parte, nella raccolta di evidenza empirica e misurabile attraverso l'osservazione e l'esperimento; dall'altra, nella formulazione di ipotesi e teorie da sottoporre nuovamente al vaglio dell'esperimento.

POPPER: ciò che conta di una teoria scientifica non è la sua genesi soggettiva, ma il fatto che essa sia espressa in forma criticabile e falsificabile sul piano oggettivo.

Fonte di prova: deve garantire il suo uso in tribunale

Chi NON è il digital forensics expert

- Il ragazzo che installa i programmi
- Il negozio di computer
- L'amico “bravo” suggerito da uno non del settore
- Quello che si qualifica coi “tesserini”
- Gli informatici che fanno altro...
- I non informatici che hanno la passione nel tempo libero
- Il cuggggino :-D

Chi è il digital forensics expert

- NESSUNO
- Chi ha delle pubblicazioni online/offline
- Chi ha un C.V. qualificante
- Chi sviluppa sw. Digital forensics
- Chi conosce i sw e hw della digital forensics
- Chi conosce leggi e metodologie della digital forensics

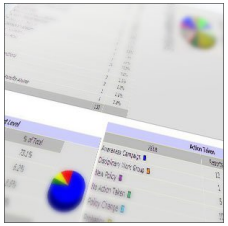
Definizione

Le fasi principali sono 4:

1)Identificazione

2)Acquisizione

3)Analisi e valutazione



4)Presentazione

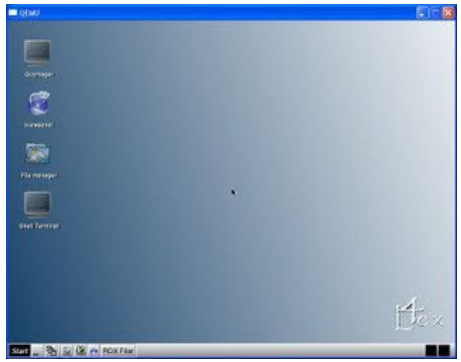
L’identificazione ed acquisizione

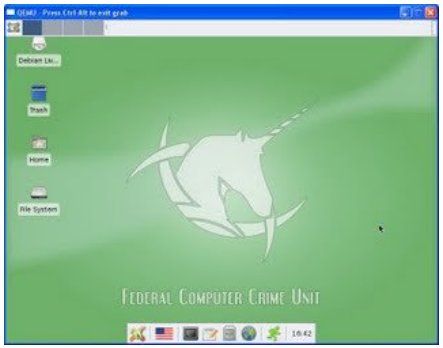
Arrivano le Live DISTRO!

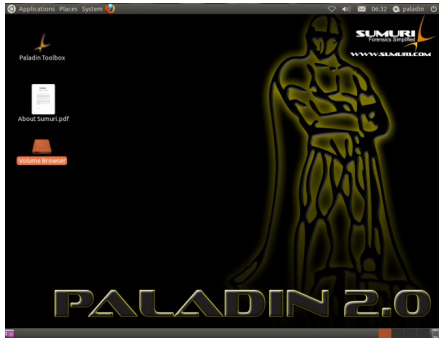
OPEN SOURCE:

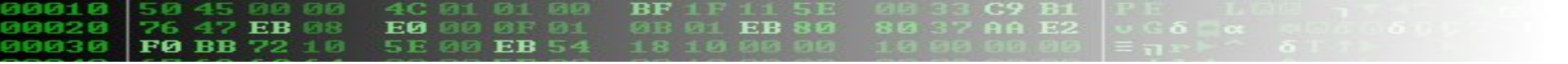
Live distro Linux:

1. CAINE
2. DEFT
3. FORLEX
4. FCCU
5. HELIX
6. PALADIN










Computer
Keyboard Changer
caine's Home
Mixed scripts
Trash
Systemback (installer)
CAINE Info
Caja (root)
Firefox Web Browser
Guymager
CAINE
Computer Aided INvestigative Environment
DARK MATTER
0 B/s
78 B/s
lun ott 6
07:36


OPEN SOURCE DAY
2014

Write Blocker & Co.

Foto:
Wikipedia

HDD Imaing
source : joncrel@flickr

L’Attrezzatura “portatile”

Sulla scena del crimine

Sulla scena del crimine

Mobile Forensics

Gabbia di Faraday

UFED

CellDek

XRY

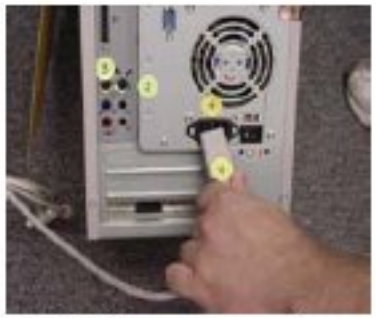
Sulla scena del crimine

STAND ALONE DESKTOP(S)
One or more computers not connected to

• Photograph the scene

• Photograph Screen

• Label Connections



• Pull the power plug

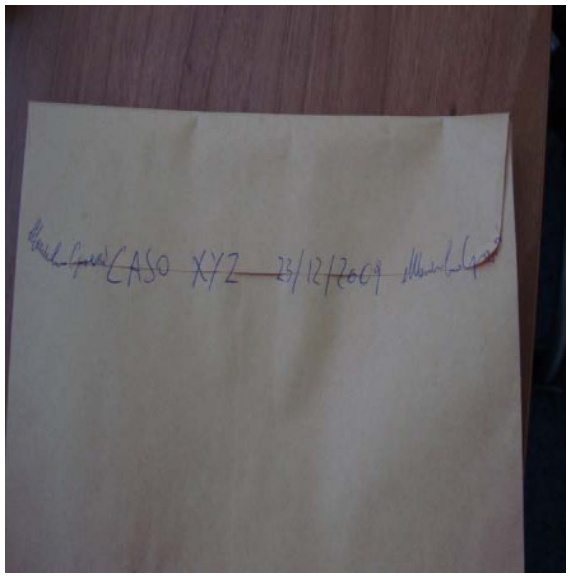
LAPTOP COMPUTERS

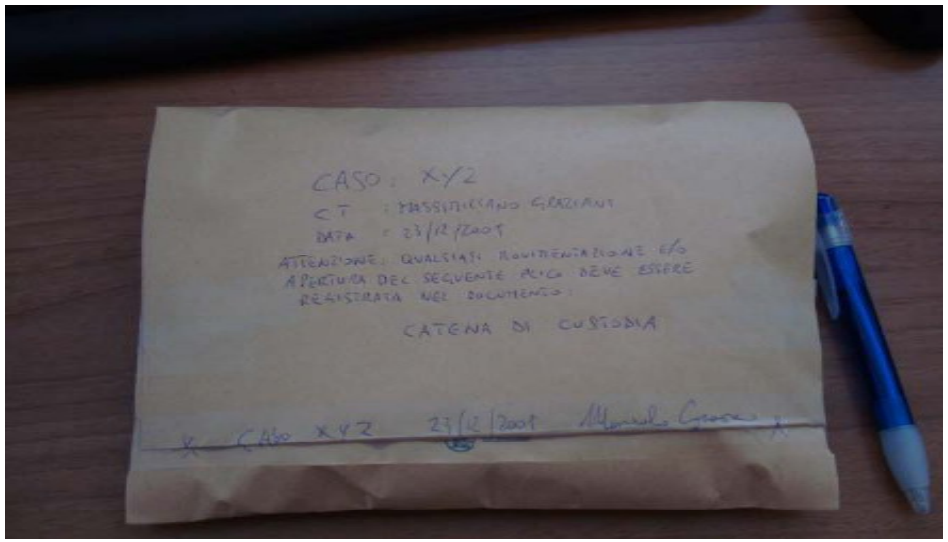
- Photograph laptop computer screen if needed.
- Remove battery from the laptop.
- Unplug from the laptop and the wall.
- If unable to locate or disconnect battery, press power button for approximately 30 seconds for hard shutdown
- Seize the computer case and all the laptop parts you find. The laptop power supply is very important.
- Place in paper sack and seal with evidence tape

EQUIPMENT LIST FOR SEARCH KIT

- Camera
- Needle Nosed Pliers
- Indelible Ink Pen (Sharpie)
- Tamper Resistant Tape
- Screw Drivers (Phillips and flat head)
- Flashlight
- Regular Pliers
- Masking Tape
- Labels/ Post it Notes

Impacchettamento





Conservazione del disco originale e creazione della catena di custodia, ossia seriale, hash, passaggi di mano, ecc.

Foto by Massimiliano Graziani

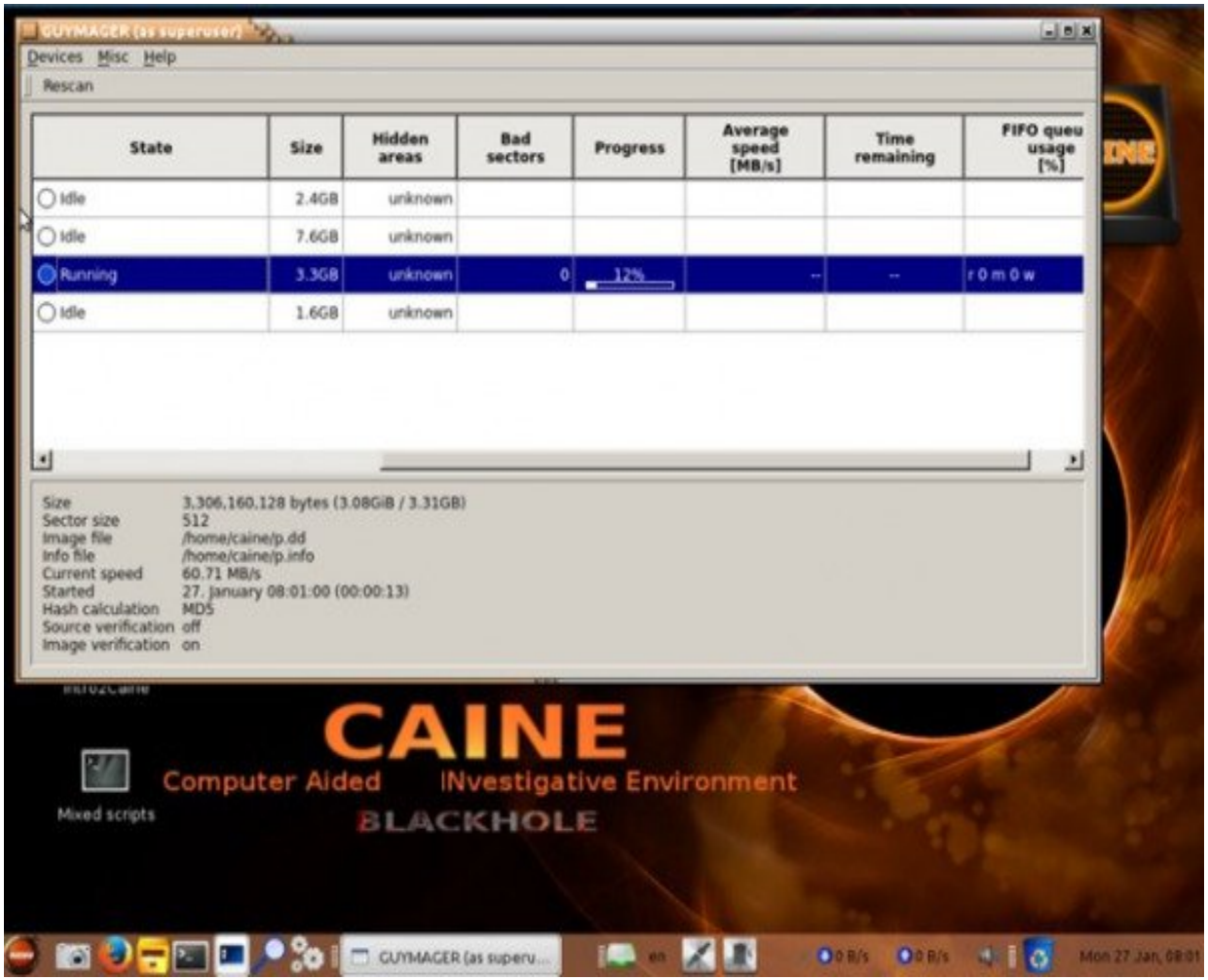
I MITI

www.nannibassetti.com

LE BUFALE INFORMATICHE

- cracking di password complesse con la semplice pressione compulsiva di tasti;
- recuperare file cancellati con velocità inimmaginabile
- riconoscimenti facciali
- accessi a tutte le reti e database del mondo
- analisi di qualsiasi telefonino, contenuti decriptati al volo
- Zoom esagerati!

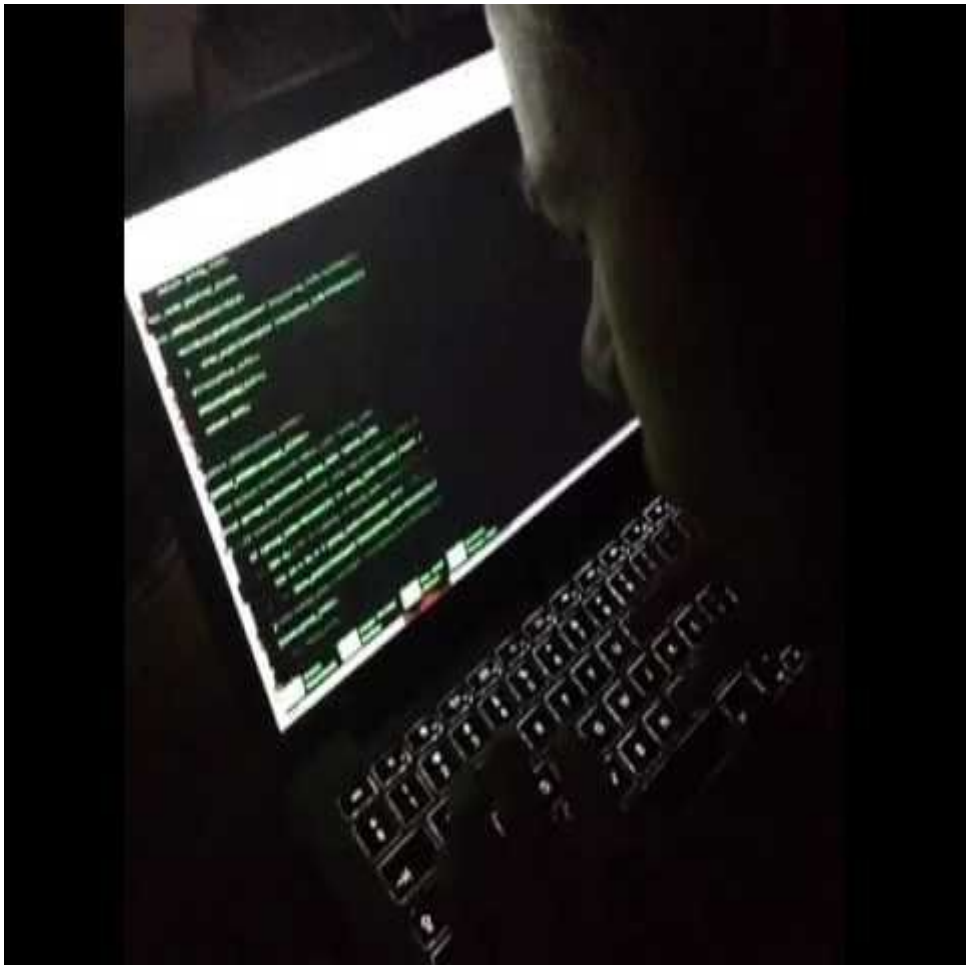
LE BUFALE INFORMATICHE



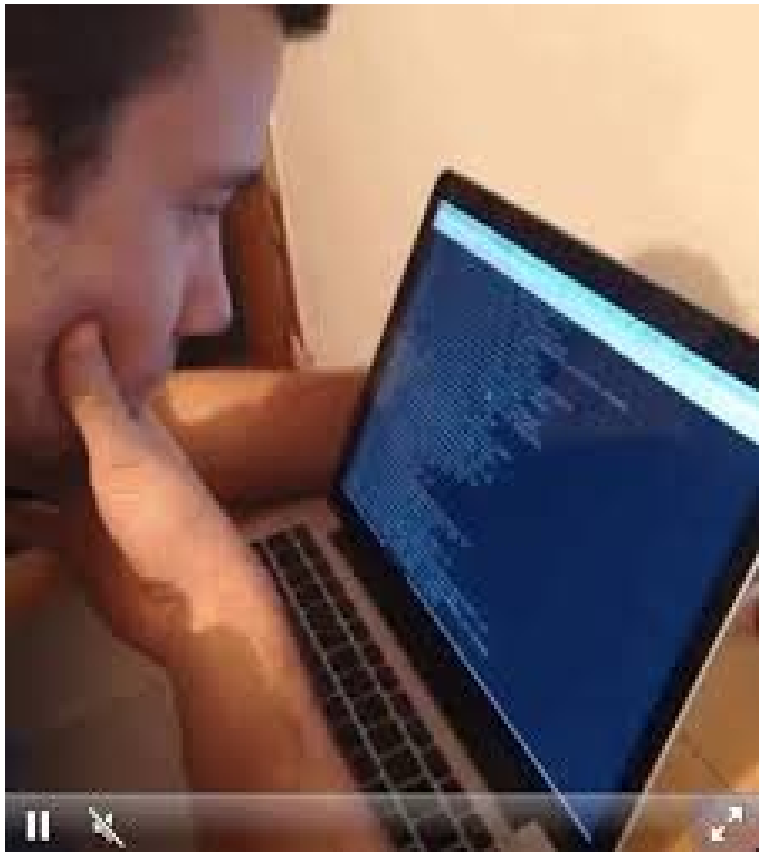
La duplicazione dei dischi è lenta e noiosa.

nel recupero di file cancellati il tempo è il nemico, infatti per operazioni simili la famosa barra d'avanzamento ricompare e rimane con noi per svariate ore o giorni

NEI FILM È COSÌ:



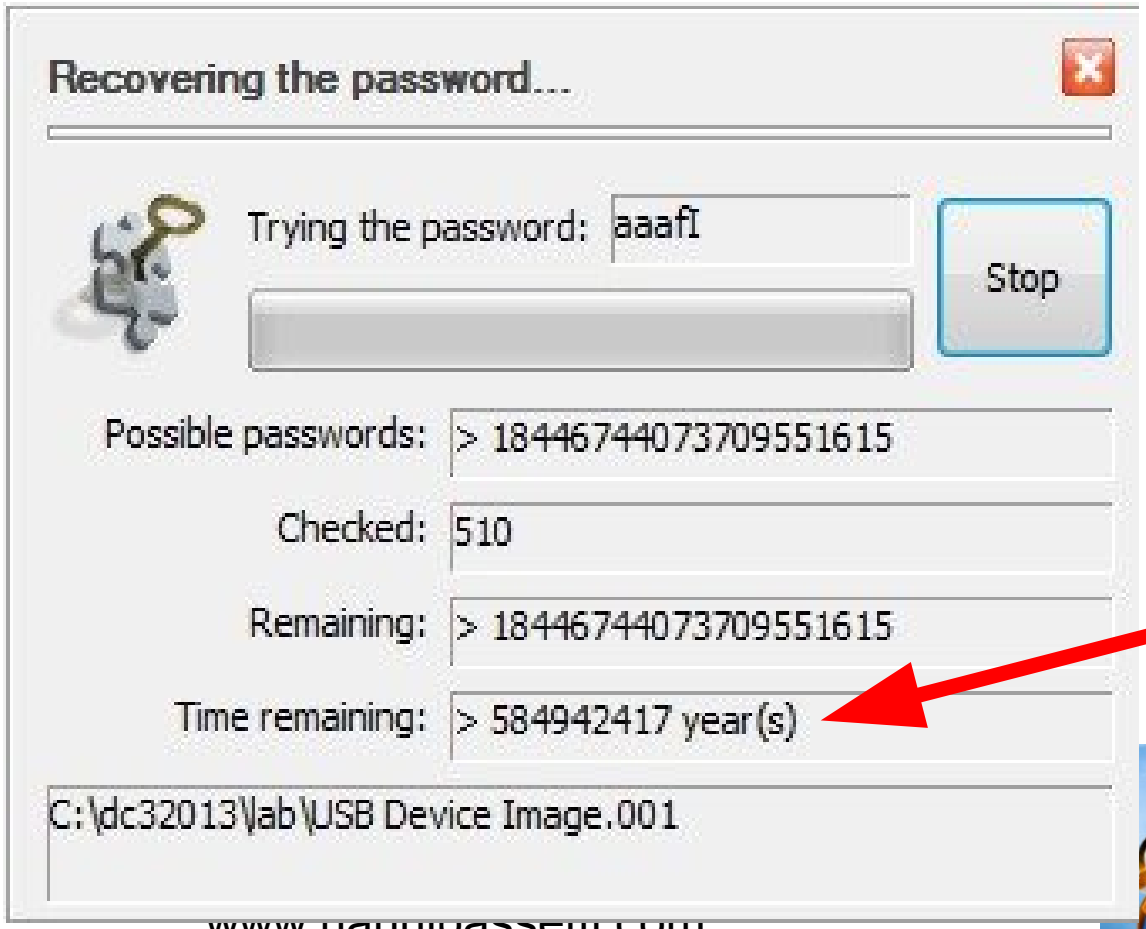
NELLA REALTÀ È COSÌ:



www.nannibassetti.com

PASSWORD CRACKING

Che bello sarebbe lanciare un programmino che in pochi minuti trova la password di un file criptato o l'accesso ad un sito web, a un firewall, a un PC o altro.
"*... ah... codice criptato a 128 bit... difficile... ma non per me!*" ed in meno di 30 secondi lo ha gia' scardinato...



Ehmmm....

RETI

In molti film fanno vedere come alcuni hacker o forze dell'ordine riescano ad accedere ovunque, si collegano alle reti di ogni Ente, azienda, ecc., in tempo reale. Ma è possibile?

In alcuni casi proprio no, perché non tutti i sistemi sono raggiungibili da Internet: alcune reti infatti sono delle LAN senza affaccio sulla Rete né tanto meno raggiungibili via Web. Alcune di queste reti a volte possono essere collegate a computer che a loro volta hanno un accesso a Internet, ma anche in questi casi l'accesso è quasi impossibile, e di certo non si ottiene in quattro e quattr'otto come si vede al cinema.

Non esistono database in rete di tutto, dalle moquette dei tappetini delle auto, alle marche di bulloni...in Italia non c'è ancora nemmeno la banca dati del DNA!!!!

RETI

Fatte le dovute (e poche) eccezioni non esistono cose simili: non ci si collega e controlla un satellite militare così con due click, non ci si collega alla rete Wi-Fi di un privato che sta a centinaia di miglia di distanza, non è possibile usare la webcam di qualcuno senza prima averlo infettato con qualcosa, non è possibile ascoltare le conversazioni telefoniche di qualcuno se non si ha infettato il telefono (non sempre possibile e/o illegale) o messo sotto intercettazione (solo forze dell'ordine), non si entra nelle reti o ricevono informazioni sensibili (tabulati e altro di gestori telefonici, Enti, aziende, social network, Google, etc.) al volo e senza passare dalle richieste dell'Autorità Giudiziaria.

TELEFONI

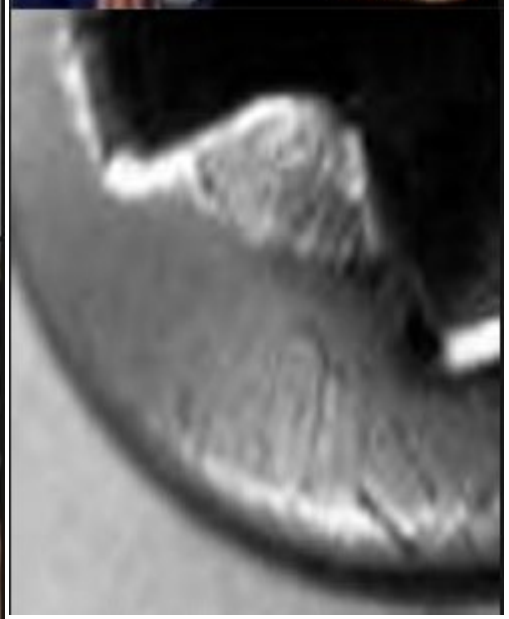
E ancora, i telefonini spenti non comunicano con le celle, e non si possono usare per intercettazioni ambientali a meno che non siano opportunamente modificati via software o hardware. I cellulari accesi invece si possono usare come microspie, se sotto intercettazione o infettati, altrimenti non c'è modo, specialmente da parte di privati, di agganciarsi al telefonino di Tizio e sentire i fatti suoi senza averlo mai infettato con qualcosa.

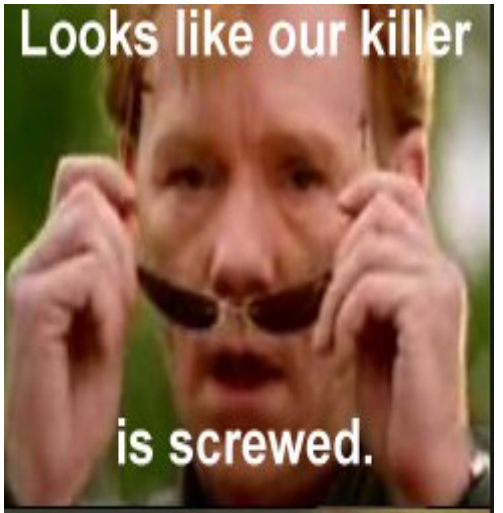
Gli SMS non vengono conservati dai gestori telefonici, infatti quest'ultimi forniscono solo i tabulati di mittente, destinatario, data ed ora, ma non il testo del messaggio, anche se ci sarà sempre un ***"cugggino"*** che ha un "amico" nella Telecom che dirà il contrario.

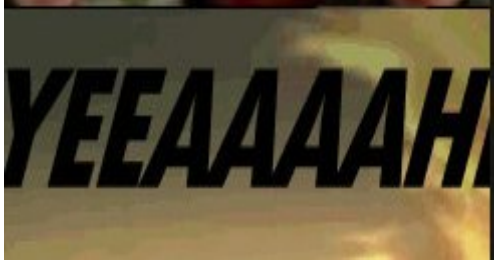
SuperZOOOM!!!!

com

SuperZOOOM!!!!







Fonte:
http://imgur.com/dnfe6JO

CONCLUSIONI

Insomma la digital forensics è spesso lenta e noiosa, e si scontra sovente contro le limitazioni tecnologiche degli strumenti e delle conoscenze: i sistemi proprietari sono in aumento, i sistemi crittografici sempre più diffusi, i dati viaggiano sulle "nuvole" e sono in mano a Big Company dislocate su tutto il globo, ma **l'effetto CSI e l'ignoranza informatica** permettono di accettare qualunque cosa, creando richieste assurde da parte di chi si rivolge al digital forensics expert. Si pensa che tutto è possibile, tutto è veloce e non ci sono differenze tra sistemi operativi, hardware, reti e quant'altro, è tutto "informatica".

Chiudo ricordando la super-chicca di "Indipendence Day" (R. Emmerich 1996) film nel quale si sviluppa un virus su un Mac, lo si carica sull'astronave madre degli alieni invasori e funziona. Strano che nel mondo reale un virus per Windows non funzioni su Mac o Linux e viceversa, ma poi si riesca a scrivere un virus per un computer alieno.

I LIMITI

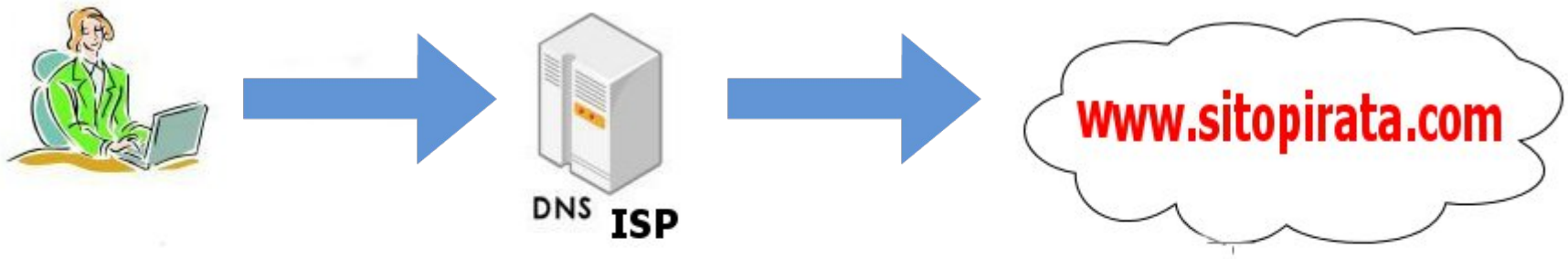
www.nannibassetti.com

NASCONDERSI ONLINE

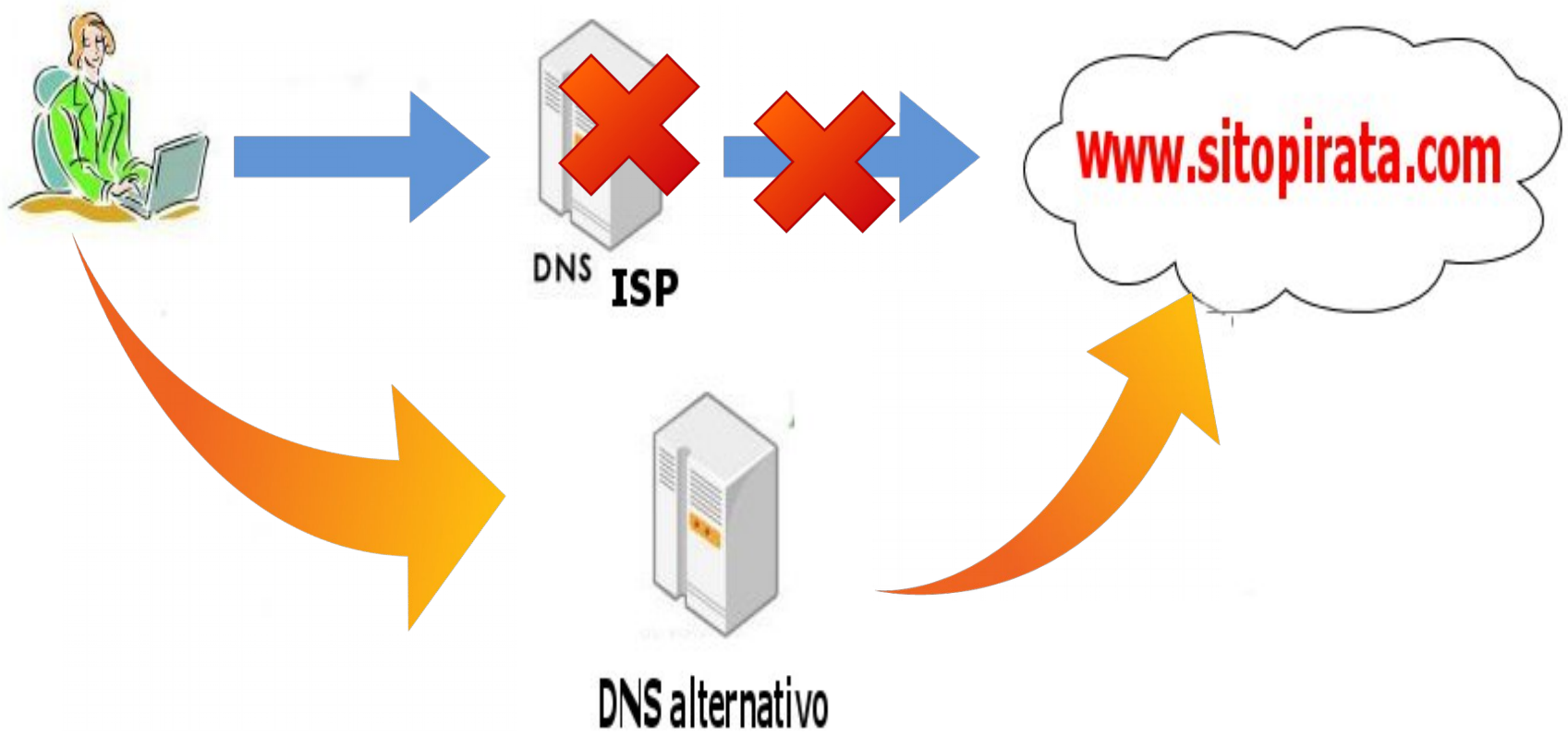
NASCONDERSI ONLINE

222.200.20.20	www.sitopirata.com

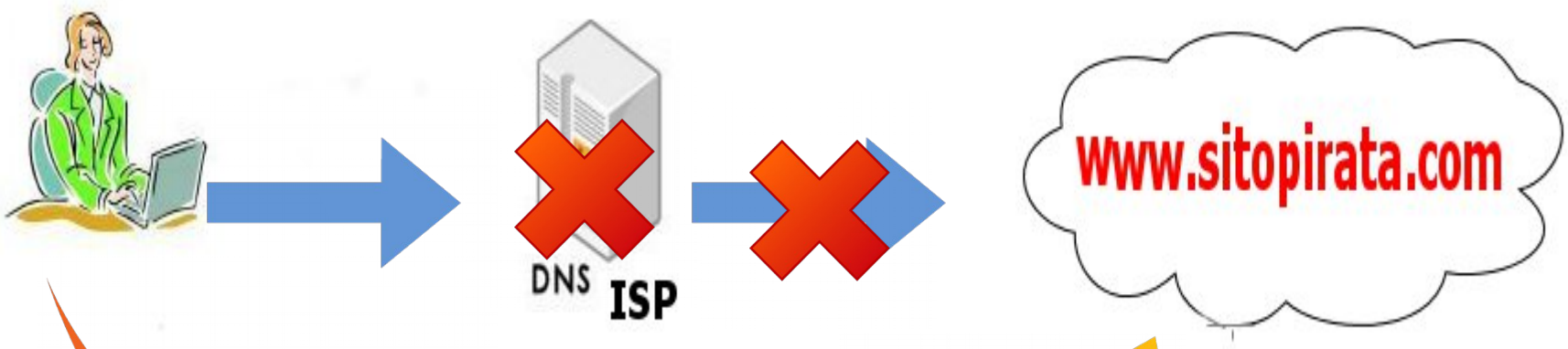
NASCONDERSI ONLINE

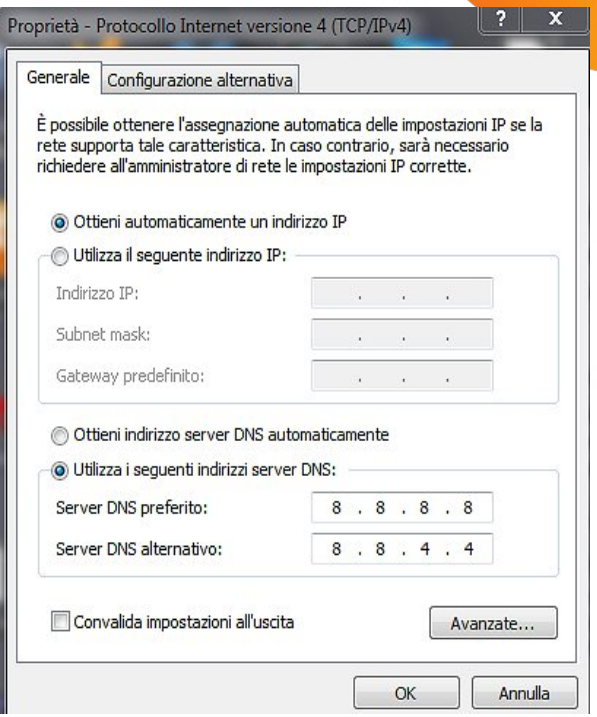


NASCONDERSI ONLINE



NASCONDERSI ONLINE





DNS alternativo

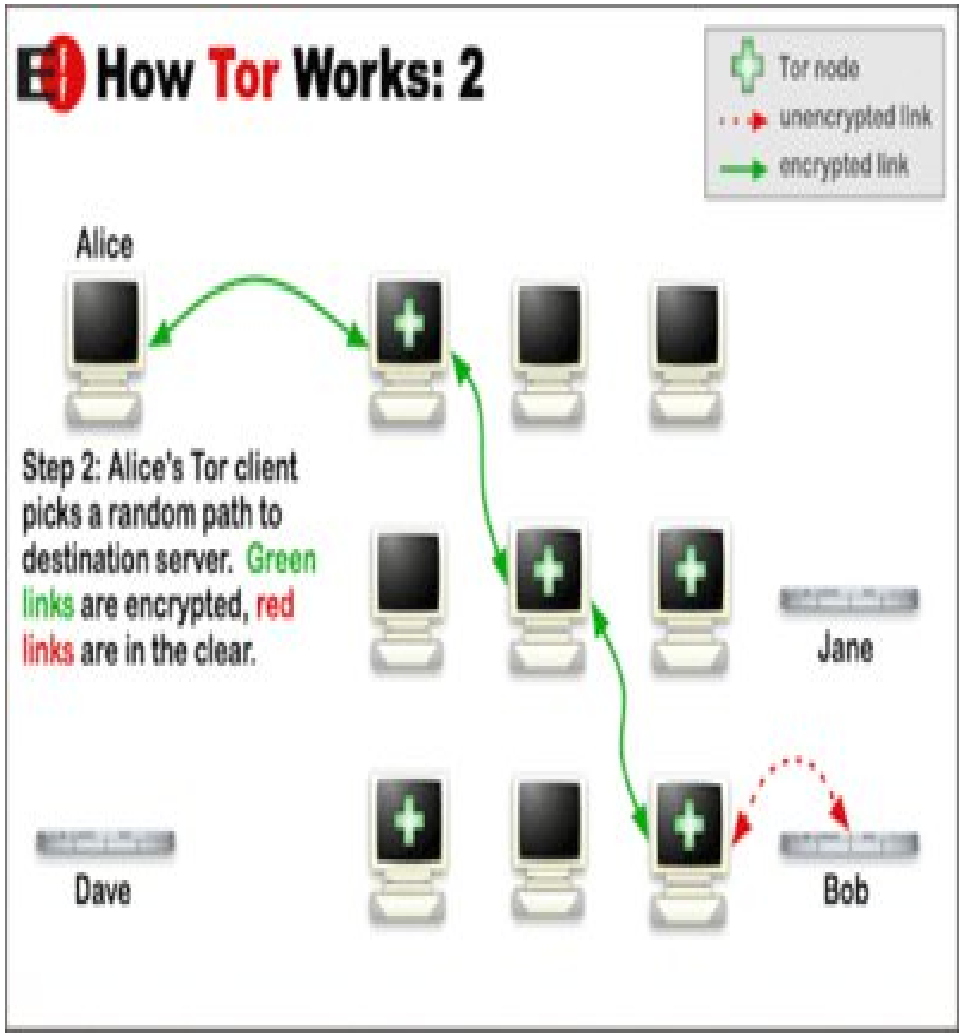
OpenNIC: 85.126.4.170,151.236.10.135
192.71.245.208, 5.9.28.125
Google: 8.8.8.8, 8.8.4.4
OpenDns:208.67.222.222,208.67.220.220

www.nannibassetti.com

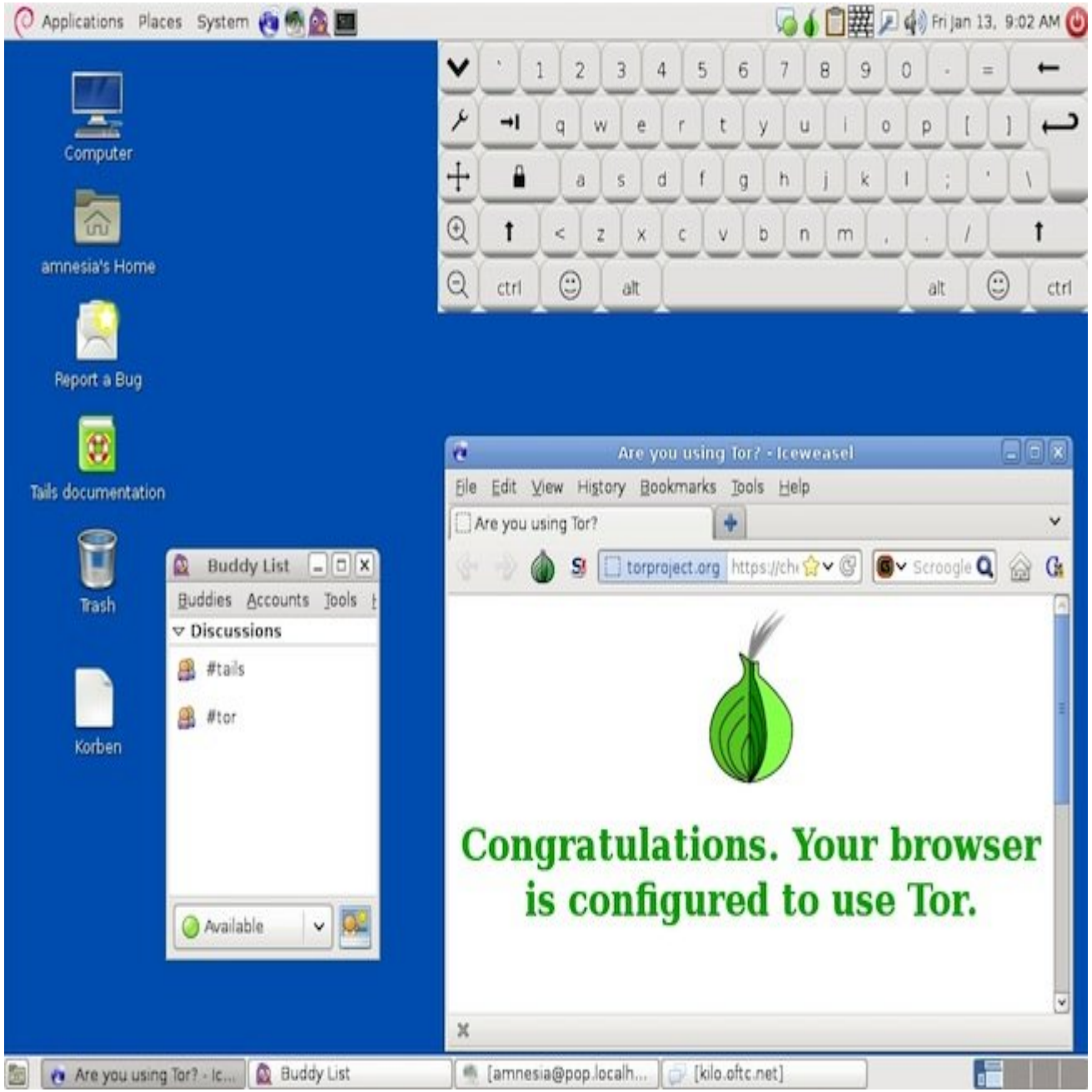
NASCONDERSI ONLINE

NASCONDERSI ONLINE

TOR

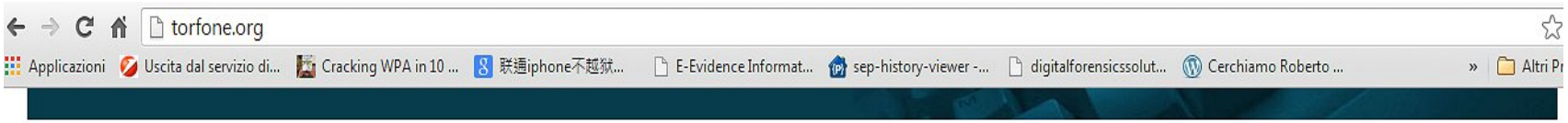


TOR – TAIL



TAIL – distro Linux per rimanere anonimi

TOR



TORFone - voice add-on for TorChat

This product is produced independently from the Tor® anonymity software and carries no guarantee from The Tor Project.

The fundamental right to privacy, guaranteed by the Fifth and Fourteenth Amendments to the U. S. Constitution, protects against unwarranted invasions of privacy by federal or state entities, or arms thereof.

Internet telephony is now an important part of people communications and should be protected from intruders, collecting information

TORFone V1.1b (01.06.13) features:

- useable with TorChat as a voice add-on;
- full duplex, PTT and VOX modes;
- fully portable (can be run from removable disk or TrueCrypt volume);
- can be run under virtual Win32 OS or Wine under any linux;
- own protected chat;
- protected files transfer;
- fully open source (compiled by VC6 under WinXP without any external libs)

Cryptography:

- Diffie-Hellman 4096 under Tor;
- AES 256 OCB mode (with 128 bit MAC);
- PKDF2/HMAC

About Tor

Tor (short for The Onion Router) is a system intended to enable online anonymity. Tor client software directs internet traffic through a worldwide volunteer network of servers to conceal a user's location or usage from anyone conducting network surveillance or traffic analysis. More...

About TorChat

TorChat is a decentralized anonymous instant messenger that uses Tor hidden services as its underlying Network. It can be used for text messaging and to transfer files to other users. More...

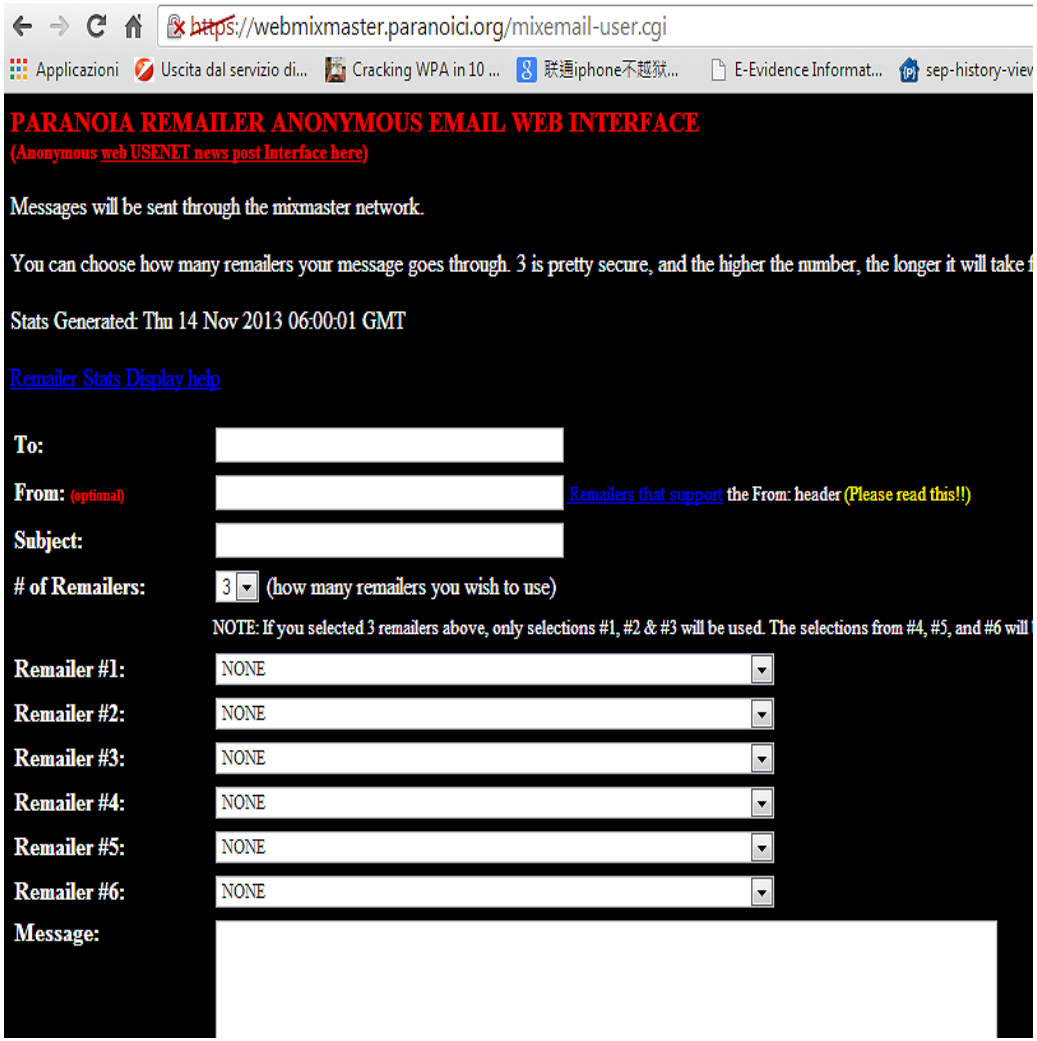
www.nannibassetti.com

E-Mail Sicure

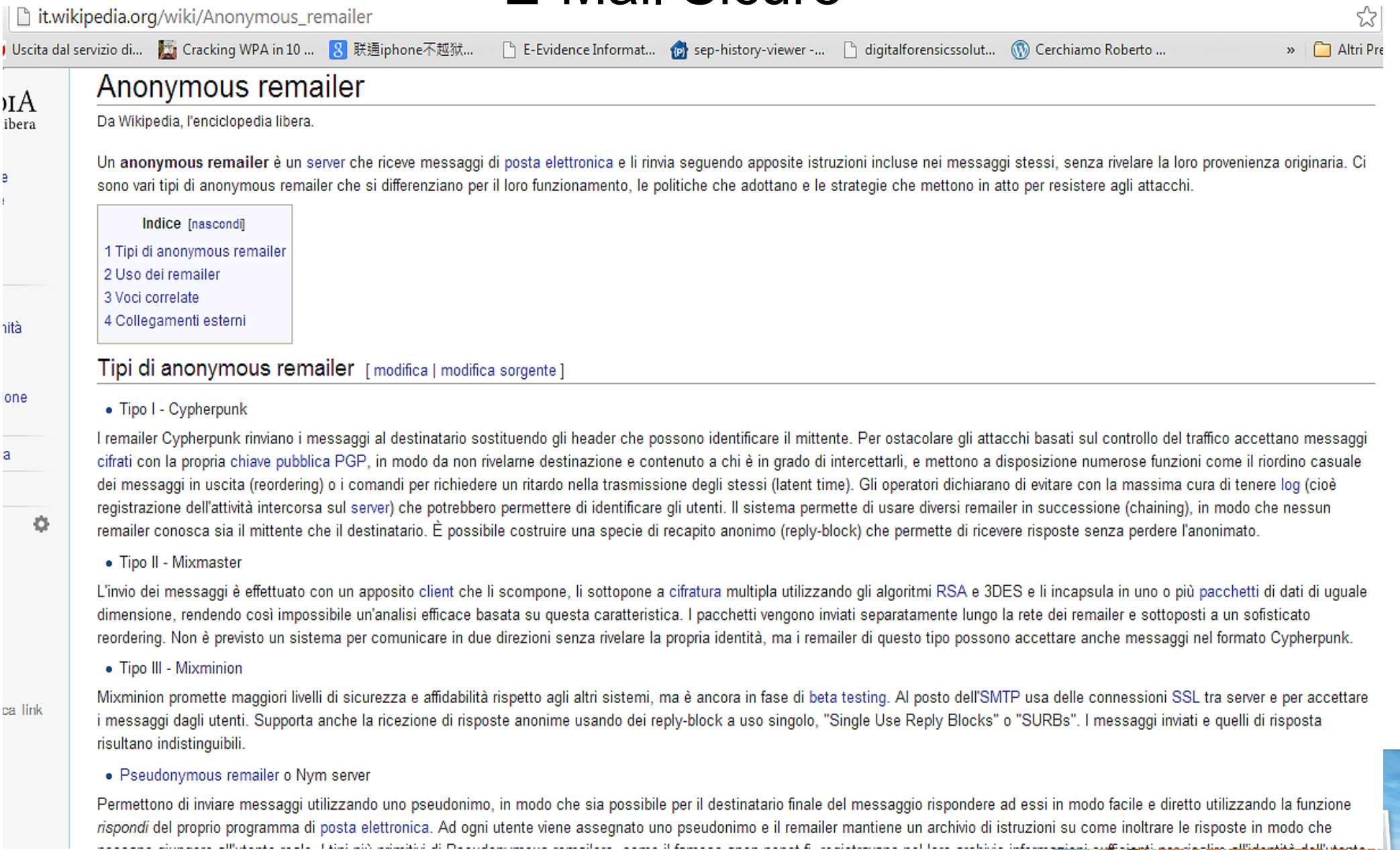
E-Mail criptate online

E-Mail client che criptano

E-Mail anonime e remailer



E-Mail Sicure



E-Mail Sicure

www.hongkiat.com/blog/anonymous-email-providers/

Uscita dal servizio di... | Cracking WPA in 10 ... | 联通iphone不越狱... | E-Evidence Informat... | sep-history-viewer -... | digitalforensicssolut...

HONGKIAT.COM | Share this post - Mi piace 52 | Tweet 122 | g+1 12 | E.g. Free

Encrypted / Anonymous Email Service

Here are some of the anonymous email services that lets you send and receive emails anonymously online. Some of them have encryption features, others are disposable or will self-destruct after a specified period of time. Here are 5.

Anonymous Email – TorGuard – This service provides you an anonymous inbox with lots of privacy and cryptographic features. You get **10MB storage, and end-to-end security** using SSL encryption for connection and **G/PGP encryption** for securing the messages.

POPULAR NOW

1 How To Custom DevTools Them

2 Logo Parodies W You Think

3 Cross-Platform V Blue Jeans Netw

4 10 Premium Mu Best Of

5 The Pursuit Of H Truly Happy)

6 Send Anonymou Your Identity Hid

7 100 OS X Maver

8 iPhone 6 Conce

Tor Mail – Tor Mail is a Tor Hidden service that provides **truly anonymous email service**. It runs

E-Mail Sicure

https://www.enigmail.net/home/index.php

Uscita dal servizio di... | Cracking WPA in 10 ... | 联通iphone不越狱... | E-Evidence Informat... | sep-history-viewer -... | digitalf

THE ENIGMAIL PROJECT

OPENPGP EMAIL SECURITY FOR MOZILLA APPLICATIONS

Home | Download | Documentation | Support | News | Links

A simple interface for OpenPGP email security

Download

v1.6 for Windows (32-bit)
on Thunderbird 24.0

Announcements

Enigmail has a new home

About Enigmail

Features
Screenshots
FAQ
Quick start guide
Handbook
Configuration

Community

Subscribe to the mailing list
Browse the list archives
Join the forums
Contact the dev team

What is this all about?

Enigmail is a security extension to Mozilla Thunderbird and Seamonkey. It enables you to write and receive email messages signed and/or encrypted with the OpenPGP standard.

Sending and receiving encrypted and digitally signed email is simple using Enigmail.

When starting it for the first time, you are guided through the basic setup. We also prepared a new users' guide that explains how to use OpenPGP.

Enigmail automatically

How should I start?

New users should look at our Quick start guide.

Then install GnuPG and the right Enigmail package for your system.

Where can I get help?

The best place to get help is our mailing list. User support forums are also available.

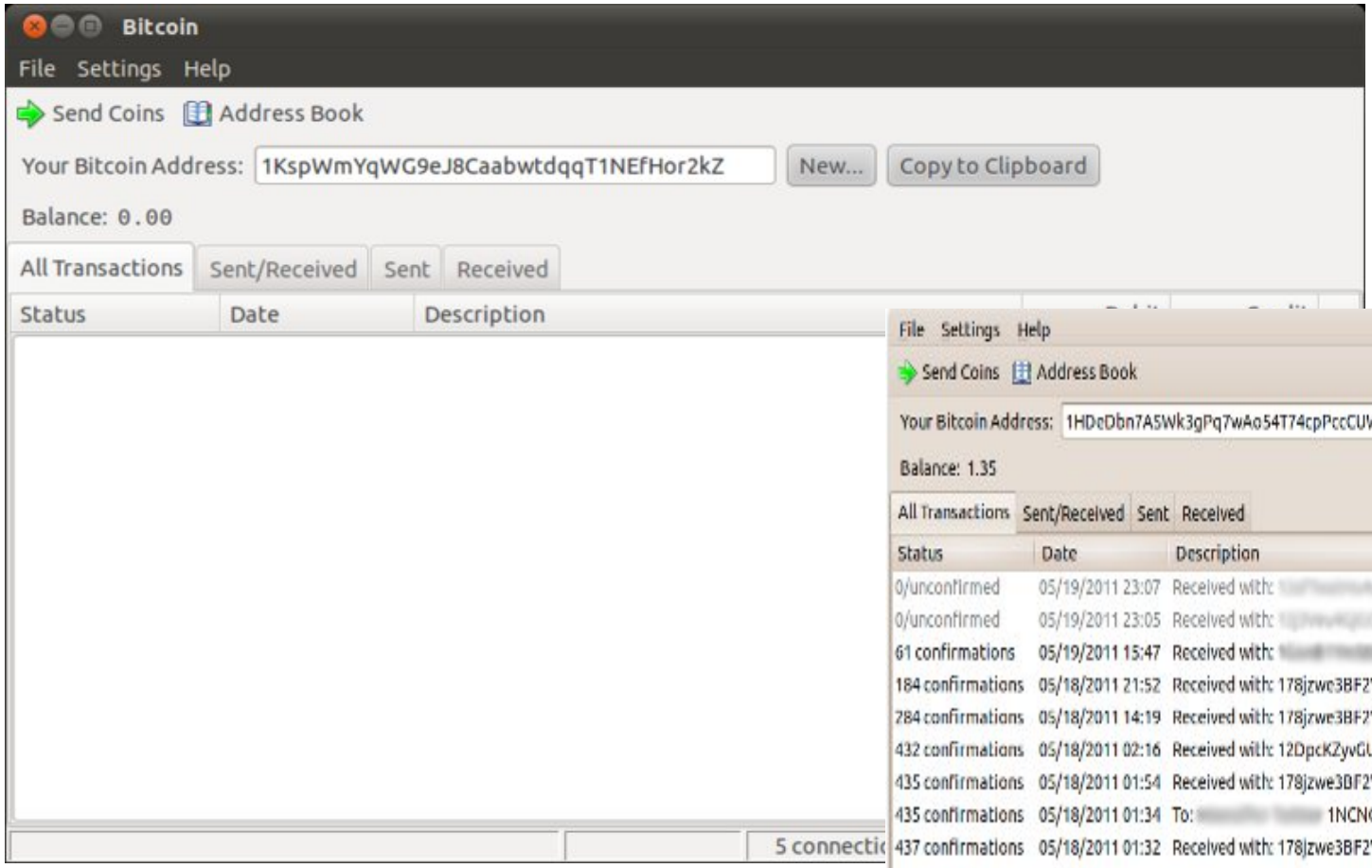
How can I contribute?

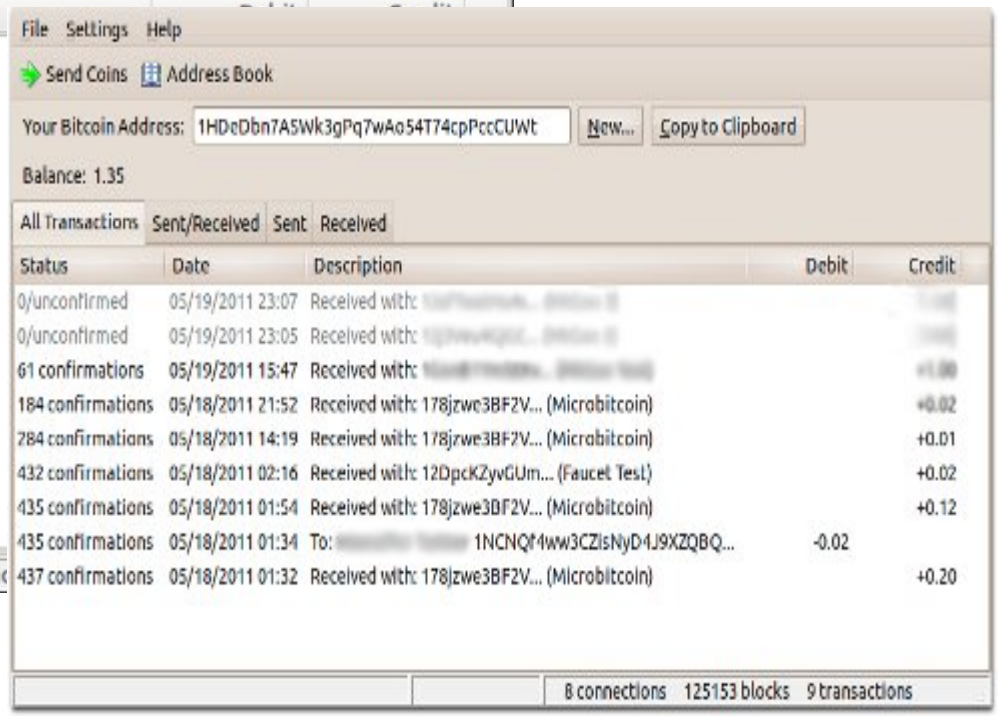
We'd love it if you did! Telling other people about Enigmail

Is there a manual?

BitCoin

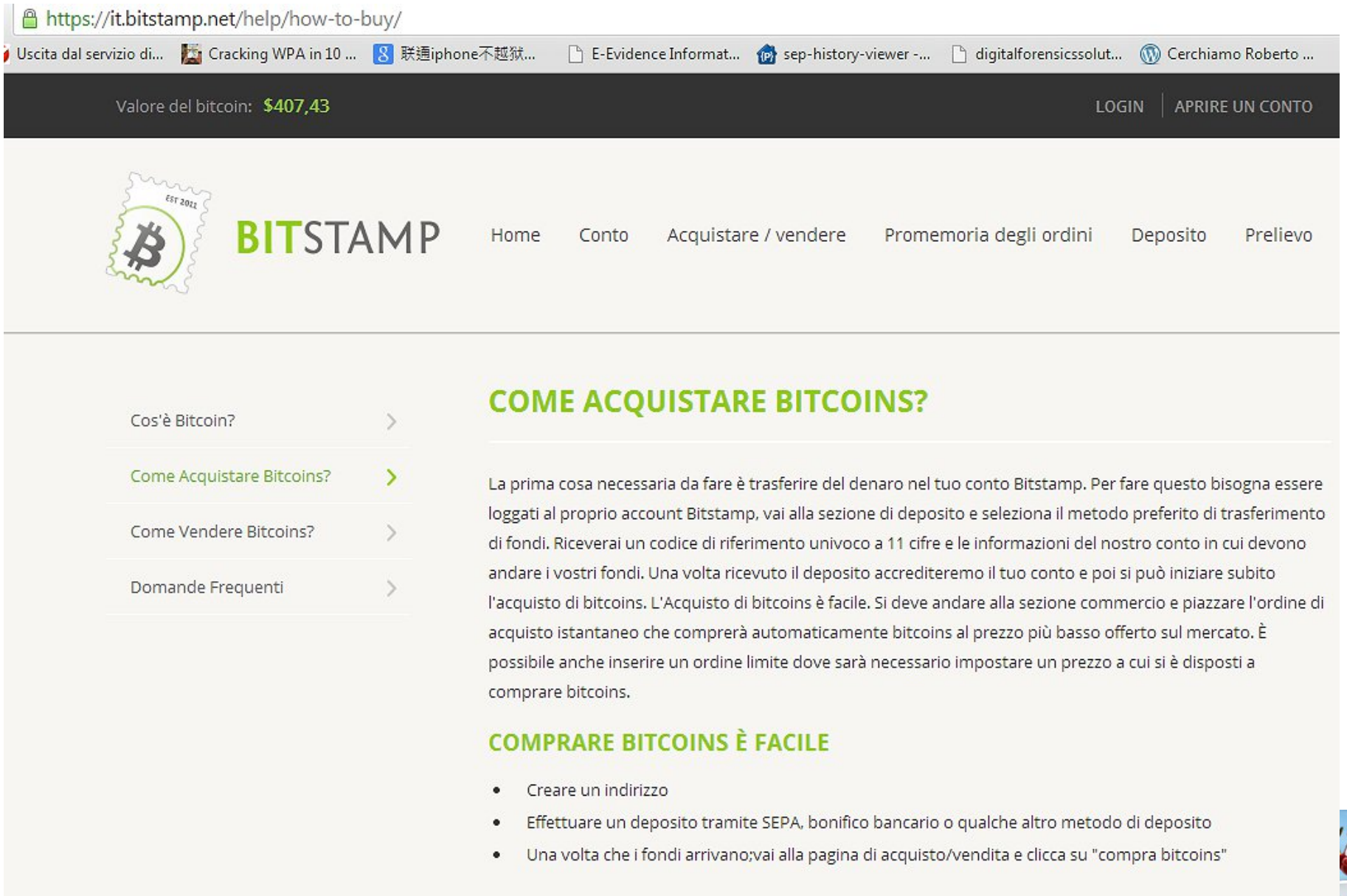
Pagare con i BitCoin – cripto-valuta peer to peer





Fonte- Wikipedia

BitCoin



Altri sistemi

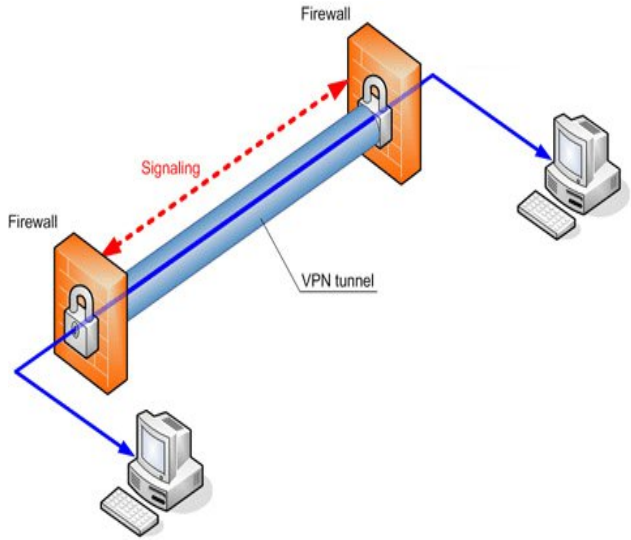
VPN

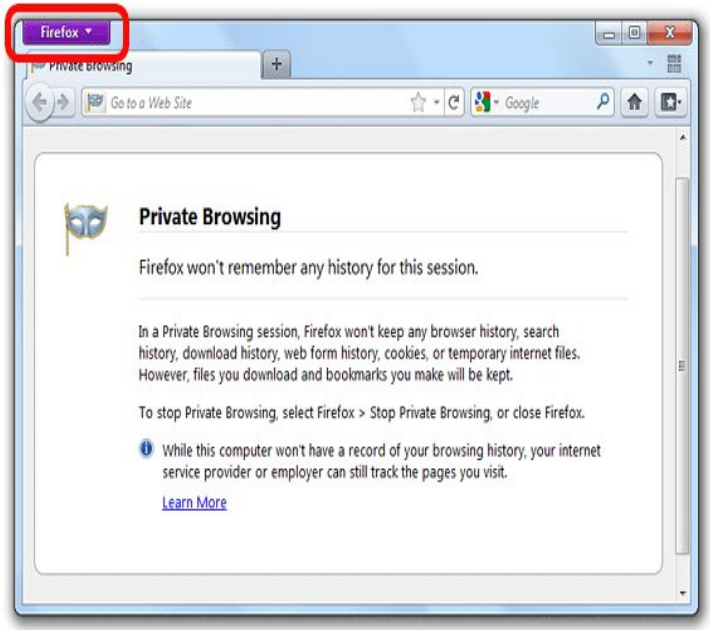
Eliminare documenti recenti

Private browsing

App IM e Chat poco diffuse

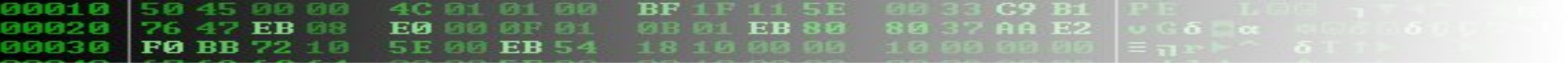
Uso macchine virtuali su supporti esterni





Altri sistemi

Awareness – Aumentano le competenze e la consapevolezza tecnica delle persone, oggi criptano, cancellano in maniera sicura, usano pw, data storare online, macchine virtuali, TOR, TrueCrypt, PGP, AxCrypt, Bitlocker, Live distro, Secure Eraser, Wipe, Ccleaner, Disk Eraser, UPX, ecc.?



www.vpnbook.com

Uscita dal servizio di... | Cracking WPA in 10 ... | 联通iphone不越狱... | E-Evidence Informat... | sep-history-viewer -... | digitalforensicssolut... | Cerchiamo Roberto ...

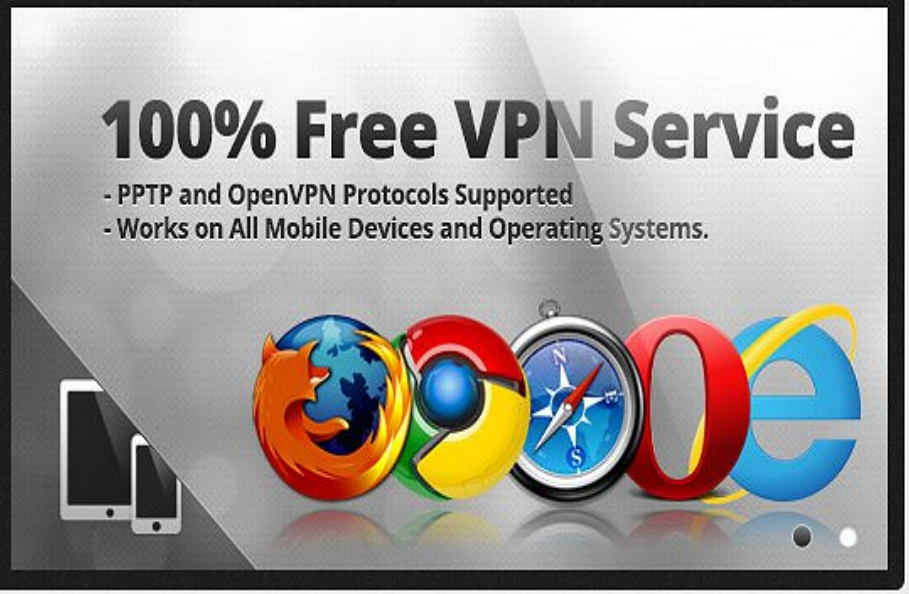
VPNBOOK

VPNBook news | Free VPN accounts | Free Web proxy | How-To setup | Features service | Privacy contact

Free VPN

Our **Free VPN** (Virtual Private Network) server is designed with the latest technologies and most advanced cryptographic techniques to keep you safe on the internet from prying eyes and hackers. Our VPN securely routing all your internet traffic through an encrypted tunnel to bypass government censorship, defeat corporate surveillance and monitoring by your ISP. VPNBook strives to keep the internet a safe and free place by providing free and secure PPTP and OpenVPN service access for everyone.

Free OpenVPN Account

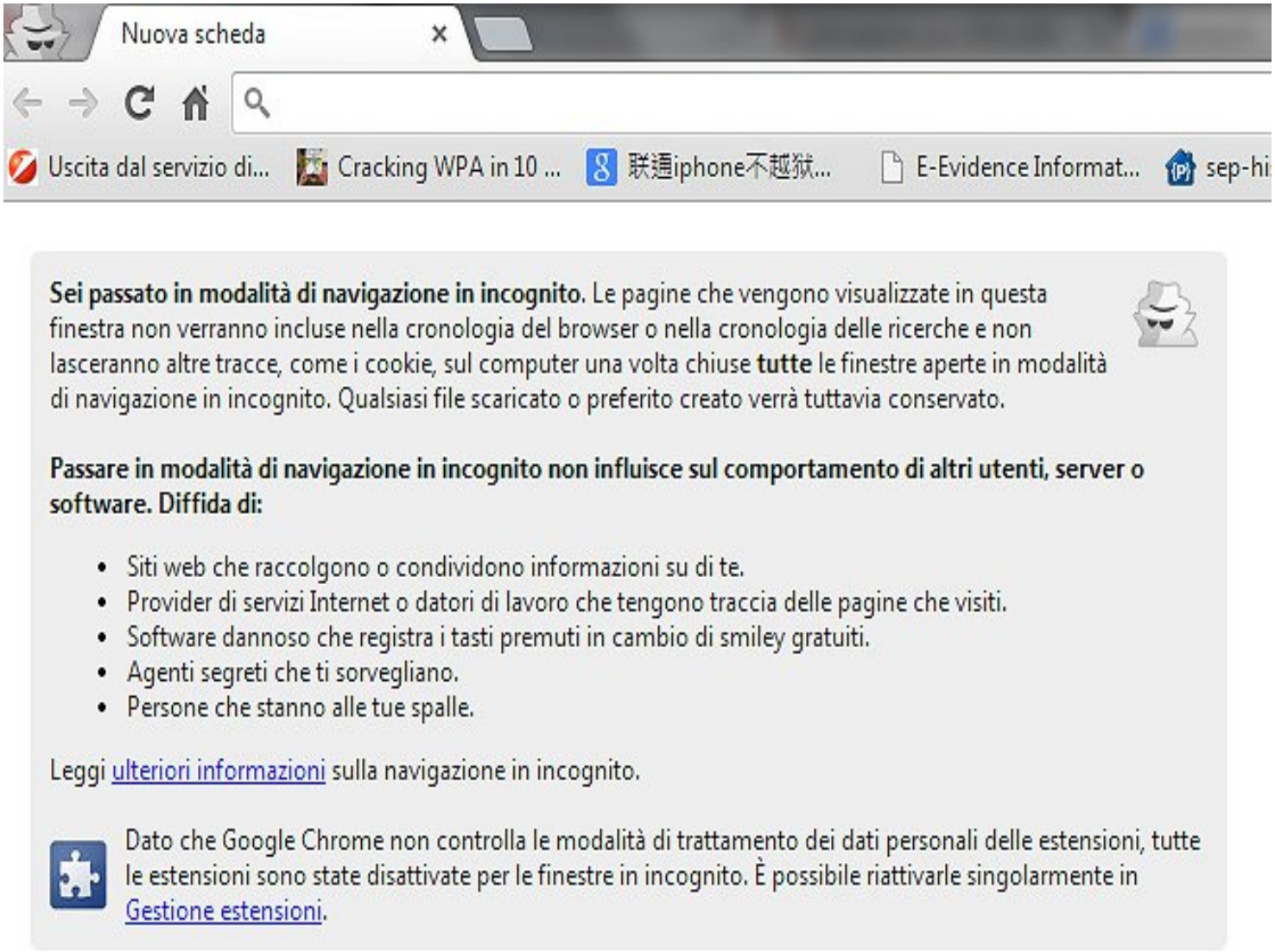


PPTP and OpenVPN
No Registration Required!

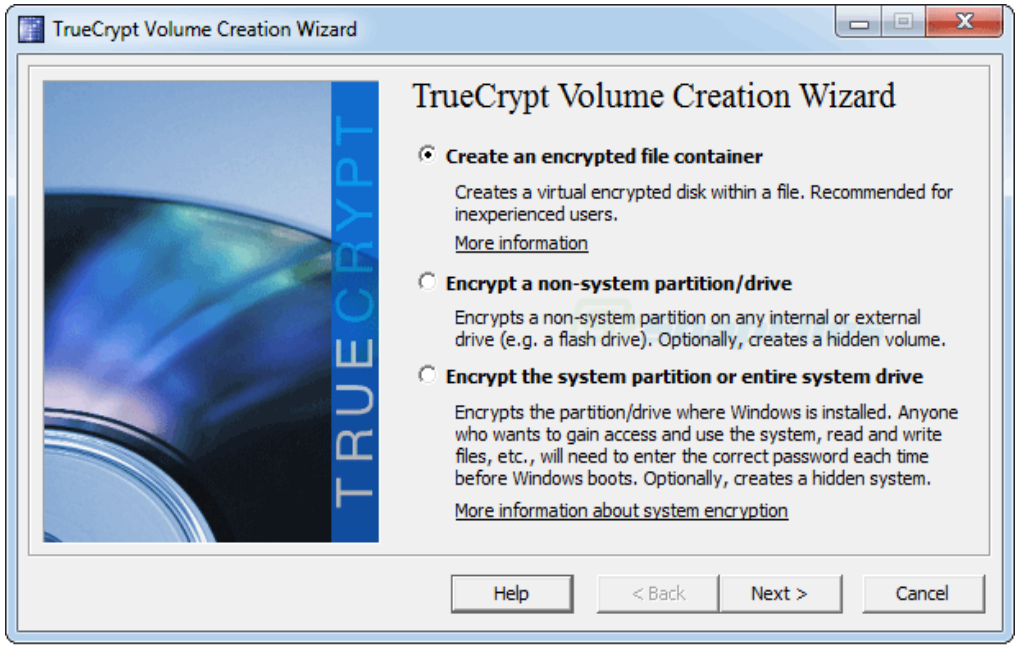
Unblock Websites
Surf the Web anonymously

100% Free
Why Pay For VPN Service Again?

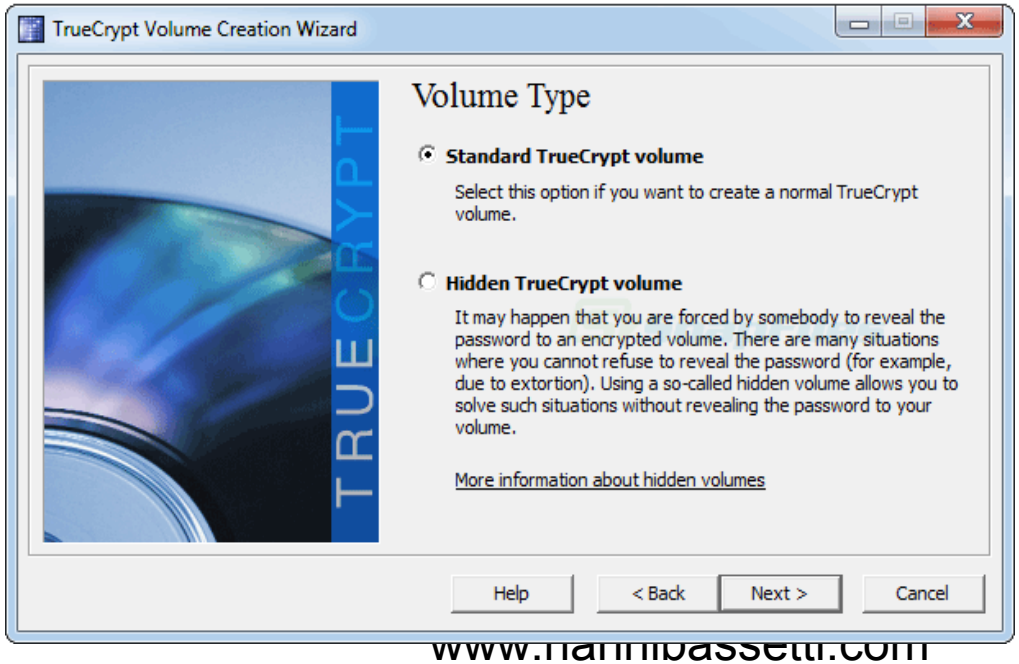
Private Browsing – Navigazione anonima



TrueCrypt creazione di un volume criptato



Possiamo creare un volume, criptato, che sul nostro PC apparirà come un file,(es. **ppp.sec**), questo file però può esser montato come Volume ed apparire come, per esempio, DISCO M, nel quale si possono inserire vari file.



Digital Forensics – The Future

Home > News and Topics >

Search in News and Topics

Toshiba Launches Wipe Technology in Self-Encrypting 2.5-Type Hard Disk Drives

New technology improves data security and reduces the risk of leaks of sensitive information stored on copiers and printer systems and IT devices

13 Apr, 2011

TOKYO— Toshiba Corporation (TOKYO: 6502) today announced the launch of the world's first [1] series of Self-Encrypting Drives (SED) equipped with Wipe Technology, Toshiba's proprietary suite of security functions that bring an unsurpassed level of data protection to IT equipment. Wipe Technology allows users to determine a range of security settings, including invalidation of encryption keys and data invalidation when a drive is removed from its housing or connected to an unauthorized host system.

The five models in the 2.5-type MK6461GSYG family range from 160 gigabytes (GB) to 640GB and are designed for use in copiers, printers, POS systems, PCs and other IT devices. Sampling will start from the end of April with mass production following at the end of June.

Digital Forensics – The Future

I dischi Toshiba da 2,5” tipo MK6461GSYG.
Nel caso in cui un modello di col self-encryptig viene rubato e tenta di connettersi a un sistema non-familiare , il disco rigido e l'host iniziano un processo di autenticazione .

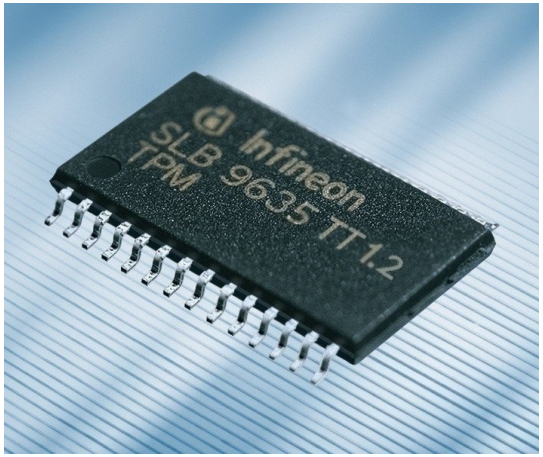
Se il tentativo di autenticazione ha esito negativo, il disco può essere configurato per negare l'accesso o cripto/cancellare i dati sensibili.

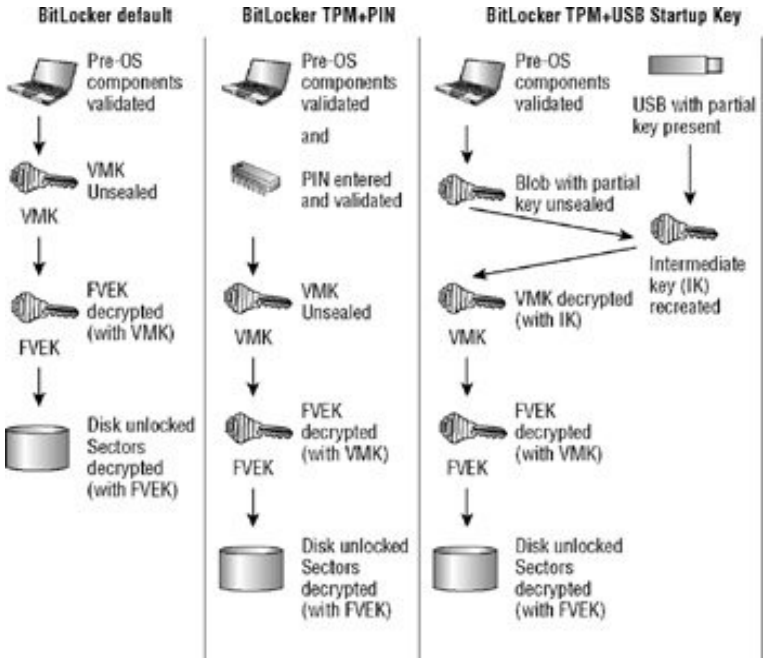
Digital Forensics – The Future

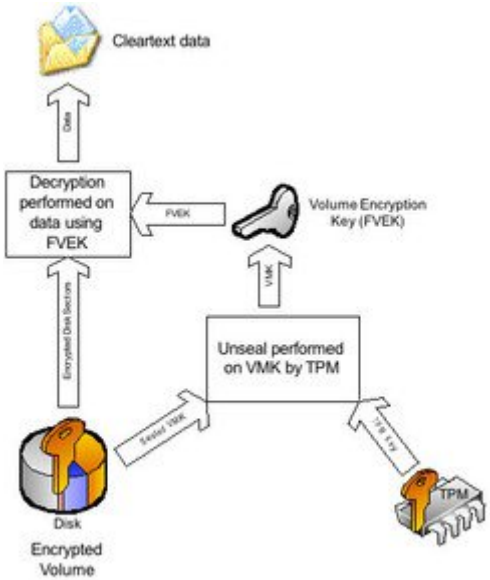
Che cosa è un TPM ?

Il TPM è un microchip progettato per fornire funzioni relative alla sicurezza di base , che coinvolgono principalmente le chiavi di crittografia . Il TPM è di solito installato sulla scheda madre di un computer desktop o portatili , e comunica con il resto del sistema usando un bus hardware .

Computer che incorporano un TPM hanno la capacità di creare chiavi crittografiche e crittografare loro in modo che possano essere decifrati solo dal TPM .





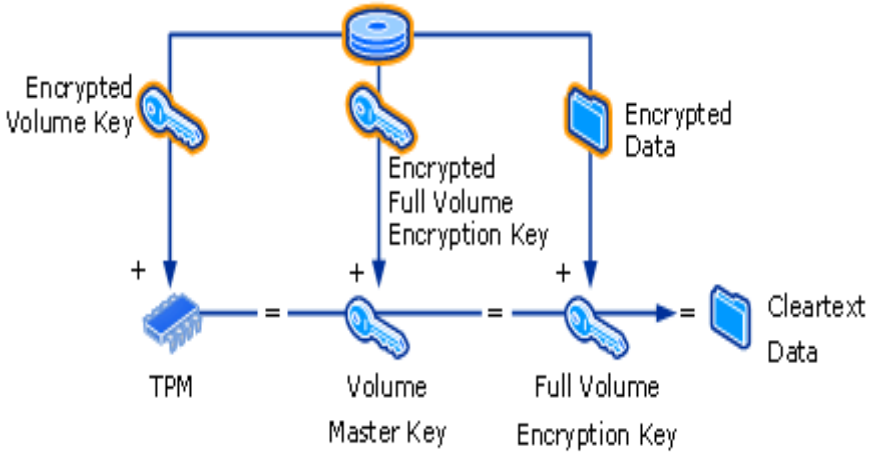


Digital Forensics – The Future

Come funziona il lavoro di BitLocker Drive Encryption?
I vostri dati sono protetti con crittografia dell'intero volume del sistema operativo Windows.
Se il computer è dotato di un TPM compatibile, BitLocker utilizza il TPM per bloccare le chiavi di crittografia che proteggono i dati. Di conseguenza, le chiavi non sono accessibili finché il TPM ha verificato lo stato del computer.

La crittografia dell'intero volume protegge tutti i dati, compreso il sistema operativo, il registro di Windows, i file temporanei, e il file di ibernazione. Poiché le chiavi necessarie per decriptare i dati rimangono bloccati dal TPM, un attaccante non può leggere i dati semplicemente rimuovendo il disco rigido e installandolo in un altro computer.

When the computer is started, the TPM chip provides the decryption key for the partition only after comparing a hash of several operating system configuration values. If the drive is removed from the computer it was encrypted on and placed in another computer system, ***the drive will not decrypt without the password recovery key****. Additionally, if changes are detected in the basic input output system (BIOS), or any of the startup files, the TPM will not release the decryption key and the drive will not unlock without the password recovery key, all of which may cause challenges to the forensic examiner if the password recovery key is not available.*



http://www.justice.gov/usao/eousa/foia_reading_room/usab5601.pdf

www.nannibassetti.com

Digital Forensics – The Future

Se anche si riuscisse a ricavare una key per il decrypting poi servirebbe anche l'eventuale password per l'unlock del disco.
"*Se durante l'avvio del computer viene rilevata una condizione che potrebbe rappresentare un rischio per la protezione, ad esempio errori del disco, una modifica al BIOS o a un qualsiasi file di avvio, BitLocker blocca l'unità e richiede una password di ripristino speciale per sbloccarla. Assicurarsi di creare la password di ripristino quando si attiva BitLocker per la prima volta, altrimenti potrebbe non essere più possibile accedere ai file.*

BitLocker utilizza in genere il chip Trusted Platform Module (TPM) nel computer per archiviare le chiavi utilizzate per sbloccare il disco rigido crittografato. Quando si accede al computer, BitLocker richiede a TPM le chiavi per il disco rigido e lo sblocca. Poiché TPM invia le chiavi a BitLocker immediatamente dopo che è stato eseguito l'accesso al computer, la protezione del computer dipende dalla complessità della password di accesso. Se è stata creata una password complessa che impedisce l'accesso agli utenti non autorizzati, il disco rigido protetto tramite BitLocker resterà bloccato." - http://windows.microsoft.com/it-it/windows-vista/help-protect-your-files-using-bitlocker-drive-encryption

Digital Forensics – The Future

Con Windows 8.1 la crittografia del disco è sempre attiva. Microsoft ha infatti deciso di applicare la protezione crittografica ai tablet o ai PC usando la funzione "device encryption" in modo automatico - in passato invece era l'utente a dover attivare la crittografia manualmente.

http://www.tomshw.it/cont/news/windows-8-1-crittografia-e-sicurezza-facile-per-tutti/50108/1.html

Digital Forensics – The Future

SSD e l'auto corrosione.

- I dischi allo stato solido subiscono il fenomeno dell'"auto-corrosione", ossia quando si cancella un file, il comando TRIM del sistema operativo dice al controller del disco di cancellarlo, quindi il file va nella garbage collection. Poichè gli SSD seguono la regola del wear leveling e per cancellare un file devono prima scrivere, le operazioni di cancellazione non sono in tempo reale, ma in background e gestite dal controller, poi una volta cancellati i blocchi, non si recupera più il file, poiché sovrascritto.
  Quindi, quando si stacca un SSD e lo si attacca ad un altro computer, il write blocker non blocca l'auto-corrosione, dato che il fenomeno si attiva dall'interno, appena il controller riceve corrente elettrica.

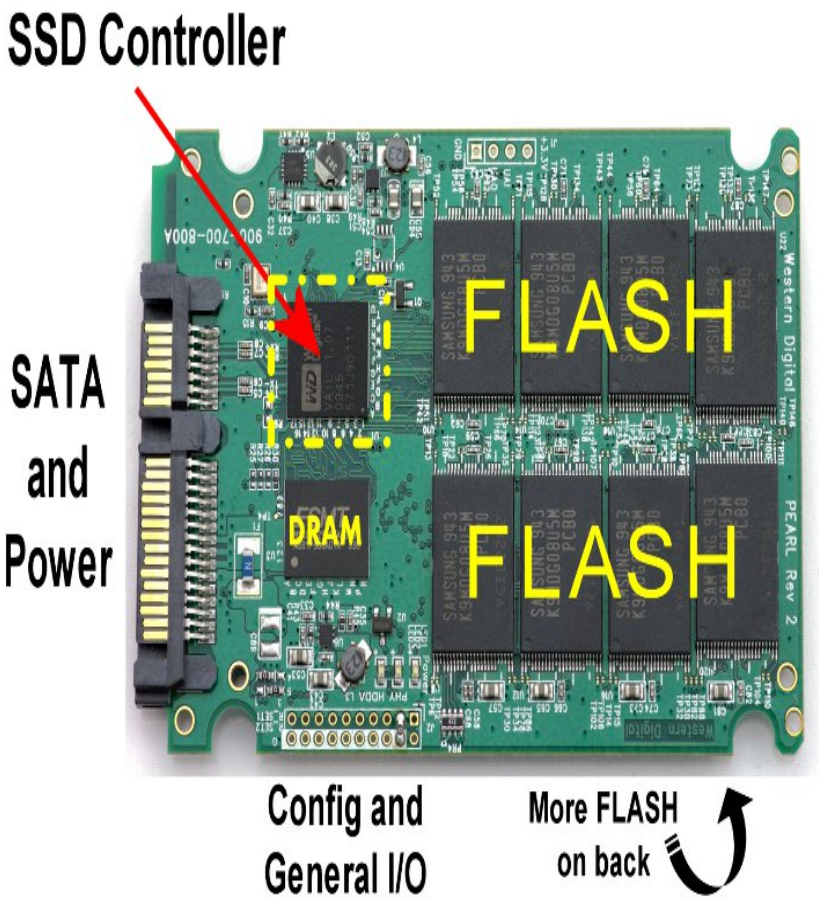
SSD

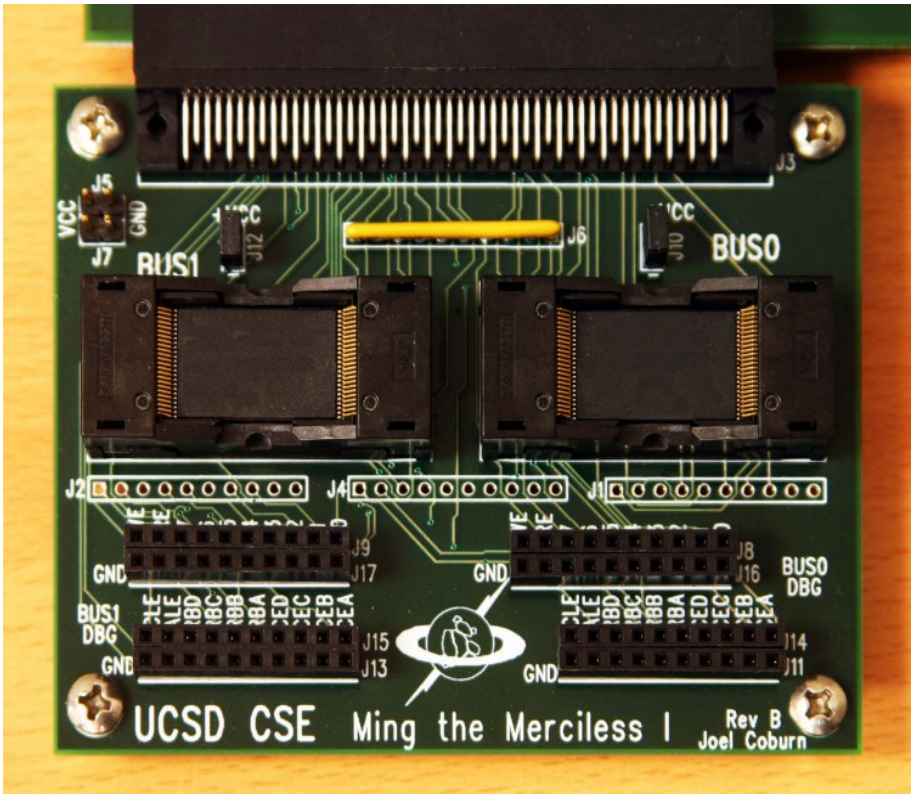
Wear Leveling: Per aumentare la vita delle celle di memoria. Statico: lo si applica a tutta la ssd, Dinamico: lo si applica solo allo spazio libero di memoria.

Ciclicamente il drive SSD deve eseguire una operazione chiamata Garbage Collection: il contenuto del blocco è copiato in un altro blocco ignorando le Page marcate “da cancellare”, in modo da liberare spazio. I controller di alcuni SSD eseguono questa operazione nelle fasi di inattività (Idle Garbage Collection o Background Garbage Collection) per esser più performanti nelle fasi di attività.

Digital Forensics – The Future

http://forensic.belkasoft.com/en/why-ssd-destroy-court-evidence





A group of scientists from University of California [4] designed an FPGA-based device providing direct access to flash chips of the SSD drive while bypassing the controller. The researchers estimated the cost of their prototype as $1000, while their estimate for building production units using microcontrollers instead of FPGA's was as little as $200.

Digital Forensics – The Future

iPhone 6 è criptato, l'Fbi insorge contro la privacy di Apple

Postato il 29 settembre 2014 da Isotta Esposito

Risolvere alcune azioni criminali attraverso foto, e-mail e contatti sarà difficile anche per l'Fbi; perché? iPhone 6 è criptato e l'Fbi insorge contro la privacy di Apple

James Comey, l'attuale numero uno dell'Fbi, ha confermato l'affermazione della **Apple: iPhone 6 è criptato ed inviolabile; la privacy di iPhone 6** è garantita al massimo anche per l'Fbi. Che cosa garantisce la massima privacy e fa insorgere **l'Fbi contro Apple**?

Un algoritmo complicato e personale protegge **sia iOS 8 che la prossima versione di Android;** nemmeno l'azienda produttrice è in grado di bypassarlo. Da una parte, quindi, gli utenti ne sono molto contenti, dall'altra, invece, i servizi segreti lo sono un po' meno. Perché? Anche sotto mandato di un giudice, **per l'Fbi ci potrebbero volere più di 5 anni per riuscire a decriptare un iPhone 6.**

James Comey ha commentato la vicenda, dicendo: "Verrà un giorno che tutto ciò sarà di enorme importanza per i cittadini, si tratta della possibilità di avere accesso agli smartphone o altri dispositivi", riferendosi all'**importanza di risolvere alcune azioni criminali attraverso i dati personali come foto, email e contatti**.

FONTE: http://urbanpost.it/iphone-6-e-criptato-lfbi-insorge-contro-la-privacy-di-apple

Digital Forensics – The Future

IL CLOUD

Molti esperti riconoscono che non vi è alcun metodo universale per l'estrazione di prove in modo ammissibile da applicazioni cloud-based, e in alcuni casi, solo poche prove sono estraibili. Come tale, il cloud computing rappresenta uno degli sviluppi tecnologici, che presenta una sfida continua per i legislatori, funzionari di polizia, e gli analisti di computer forensic. O detto in altro modo, la sfida per gli ispettori legali e forze dell'ordine è quello di determinare il "chi, cosa, quando, dove, come, e perché" delle attività criminali basate su cloud.

Digital Forensics – The Future

IL CLOUD

- **SaaS** (Software as a Service) - Pensiamo a Gmail, Facebook, ecc. In genere il client è il browser, tutto è online, gli elementi cancellati dove sono? Come si recuperano? Ci sono gli snapshot e le tracce di eventuali client (Dropbox, GoogleDrive, ecc.), ci sono i log? Chi li possiede? Per quanto tempo? Si dipende quasi in toto dal gestore della SaaS.
  PaaS (Platform as a Service) – Pensiamo a Windows Azure, Google App Engine, ecc. Sono piattaforme per lo sviluppo di applicazioni, si ha controllo solo sui layer dati ed application.
  IaaS (Infrastructure as a Service) – qui si può avere più libertà di manovra, dato che può essere un computer virtualizzato, quindi il cliente ha completa autonomia sulla macchina.

In tutti i casi comunque si è dipendenti dal fornitore del cloud, che è formato da macchine virtuali, che per il load balancing spesso si spostano nella rete e distribuiscono i carichi tra i vari computer che formano la nuvola.

Digital Forensics – The Future

ALTRO

- **Dispositivi mobili (cellulari, tablet, ecc.) sempre più modelli, ci sono i cinesi, i sw/hw per il dump ed analisi sono pochi, limitati e costosi e con aggiornamenti lenti rispetto all'uscita impetuosa di nuovi modelli e sistemi operativi.**

Investigator weakness – sempre più Gb/Tb da gestire, costi, complessità, si parla di dischi di parecchi gigabyte o terabyte, Raid, usare tecniche di data hiding e a quel punto le analisi da condurre porterebbero via moltissime risorse in termini di tempo e denaro, costringendo l'investigatore a lavorare alla grossa.

Awareness – Aumentano le competenze e la consapevolezza tecnica delle persone, oggi criptano, cancellano in maniera sicura, usano pw, data storare online, macchine virtuali, TOR, TrueCrypt, PGP, AxCrypt, Bitlocker, Live distro, Secure Eraser, Wipe, Ccleaner, Disk Eraser, UPX, ecc.?

Digital Forensics – The Future

ALTRO

- **ATA HDD PW – una banalità pure vecchia, ma ancora un bell'ostacolo. Ci sono due modalità di ATA Password security, HIGH e MAXIMUM, se la security è HIGH si può sbloccare il disco con la password USER o quella MASTER (di fabbrica), se è MAXIMUM solo con la password USER.**

L'OPEN SOURCE

www.nannibassetti.com

E L'OPEN SOURCE?

In scenari simili l'Open Source ed il Free/libre Software “potrebbero” giocare un ruolo importante....

I PRO:
1) Sviluppo costante da parte della community.
2) Controllo del software e possibilità di migliorarlo ed aggiornarlo
3) Attenzione verso “cose minori”
4) Sviluppo dei propri tools
5) Per il cybercrime Linux is better! Molti tool analisi di rete e molti sistemi di rete sono basati su Linux.

I CONTRO:
1) Frammentazione dei team di sviluppo.
2) Difficoltà negli aggiornamenti/testing.
3) Documentazione spesso scarsa.
4) Spesso solo per utenti esperti.

E L'OPEN SOURCE?

Attenzione verso “cose minori”

ESEMPI:
Parser per BBThumbs.db presente nei BlackBerry (pre OS 5)

```
python bbt.py -b bbthumbs.dat
*** Processing bbthumbs.dat on 2011-08-25 17:49:20.656000
+ Nota vocale00001-20110201-1700.amr // Tue Feb 01 17:03:18 2011 (Device Time) /
/ 231a5c4096cfd7334d0a4ee9e7c72c5a3e1fac2c
+ Nota vocale00002-20110201-1730.amr // Tue Feb 01 17:35:09 2011 (Device Time) /
/ dc75f42aab6c9f3d84ba66920ffd98b1fcb8c02c
+ Nota vocale00003-20110201-1800.amr // Tue Feb 01 18:01:11 2011 (Device Time) /
/ 54eb7b4347e21b977d4a981375f2c5e7e44be874
+ Nota vocale00004-20110201-1900.amr // Tue Feb 01 19:01:06 2011 (Device Time) /
/ 439c360c7dd849b0e1681652fc2d8716a4368921
*** bbthumbs.dat has 4 records
```


E L'OPEN SOURCE?

- **Zenrecovery - script in python che permete di estrarre i dati dal lettore multimediale (ZEN) e verificare i file in esso contenuti!**

zenrecover.py # embed

```
#!/usr/bin/python

# Copyright 2007 by Tobia Conforto <tobia.conforto@gmail.com>
#
# This program is free software; you can redistribute it and/or modify it under the terms of the GNU General
# Public License as published by the Free Software Foundation; either version 2 of the License, or (at your
# option) any later version.
#
# This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the
# implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License
# for more details.
#
# You should have received a copy of the GNU General Public License along with this program.
# If not, see http://www.gnu.org/licenses/


# Use this program to extract files from a disk image from a Creative Zen Xtra or Zen Vision M player.
# Unlike the zenrecover.py this is based on (https://gist.github.com/483969), this also finds deleted files
# and can extract most files after the player has been formatted. However, it doesn't distinguish between
# "songs" and "archives" areas on the player, and also extracts a few player system files.
#
```


E L'OPEN SOURCE?

Crearsi piccoli frameworks ma efficienti!

articles.forensicfocus.com/2013/04/23/ks-an-open-source-bash-script-for-indexing-data/

ita dal servizio di... | Cracking WPA in 10 ... | 联通iphone不越狱... | E-Evidence Informat... | sep-history-viewer -... | digitalforensicss

FORENSIC FOCUS

FOR DIGITAL FORENSICS AND EDISCOVERY PROFESSIONALS

SEARCH

Home | Subscribe

NEWS | FORUMS | ARTICLES | INTERVIEWS | JOB VACANCIES | EDUCATION | WEBINARS | NEWSLET

DATA RECOVERY, E-DISCOVERY, FORENSIC ACCOUNTING, FORENSICS 101, METHODOLOGY, RESEARCH, SOFTWARE, UNCATEGORIZED

KS – an open source bash script for indexing data

POSTED BY NANNIB - APRIL 23, 2013 - 2 COMMENTS

FILED UNDER COMPUTER FORENSICS, DATABASE STORAGE, OPEN SOURCE, SOFTWARE

KS – an open source bash script for indexing data

ABSTRACT: This is a keywords searching tool working on the allocated, unallocated data and the slackspace, using an indexer software and a database storage .

Often during a computer forensics analysis we need to have all the keywords indexed into a database for making many searches on it in a fast way.

We could use strings and grep, for searching the keywords, but we cannot have a database and an engine, then we can't search them inside many formats, like compressed files, including the ODT, DOCX, XLSX, etc..

So, I tried to solve this problem, first of all we need to extract, what I call "*spaces*":

E L'OPEN SOURCE?

Esempi:

Facebook forensics → Open Source → Tools aggiornati?
Facebook forensics → Commercial → Tools aggiornati!

Open Source su sistemi complessi/proprietari → Reverse Engineering → Tempo/risorse umane.

Commercial su sistemi complessi/proprietari → Reverse Engineering o Accordi → Tempo/risorse umane → $$$ €€€

E L'OPEN SOURCE?

QUINDI?

- Creare dei team
- Creare documentazione
- Creare dei repository per gli update
- Esser sempre più “user friendly” e meno “geekkosi” :-)

http://events.linuxfoundation.org/sites/events/files/slides/Linux%20and%20Law%20Enforcement.pdf

KOREA LINUX FORUM

#lfklf

Ritz-Carlton Seoul
Seoul, South Korea
November 11, 2014

Linux and Law Enforcement
Challenges and Opportunities

Dr. Joshua I. James
Digital Forensic Investigation Research Laboratory
SoonChunHyang University
Joshua@cybercrimetech.com

Open Source Tools

- A number of the most popular Linux-based open source tools include:
  - The Sleuth Kit http://www.sleuthkit.org/
  - Guymager http://guymager.sourceforge.net/
  - Digital Forensics Framework http://www.digital-forensic.org/
- Live CD distributions:
  - DEFT http://www.deftlinux.net/
  - CAINE http://www.caine-live.net/
  - KALI http://www.kali.org/
- Many "investigation automation programs" are built on top these systems
- Linux can already handle a lot of investigation tasks 'out-of-the-box'
- Again, many popular tools are cross-platform
  - Investigators need to support data collection and analysis on every kind of device

http://events.linuxfoundation.org/sites/events/files/slides/Linux%20and%20Law%20Enforcement.pdf

Perception of Linux by LE / Gov.

- Legal (cont):
  - Some (few) countries actually ***prefer*** Open Source tools for investigations
  - **Italy**: gives priority to free and open source tools for investigations
  - Why? We can check the source to see exactly what the code is doing
  - Third-parties can verify the code is working as expected

For an interesting discussion, please see: http://www.digital-evidence.org/papers/opensrc_legal.pdf

FIREBrick http://digitalFIRE.ucd.ie - O.S. Hardware/Software

www.nannibassetti.com

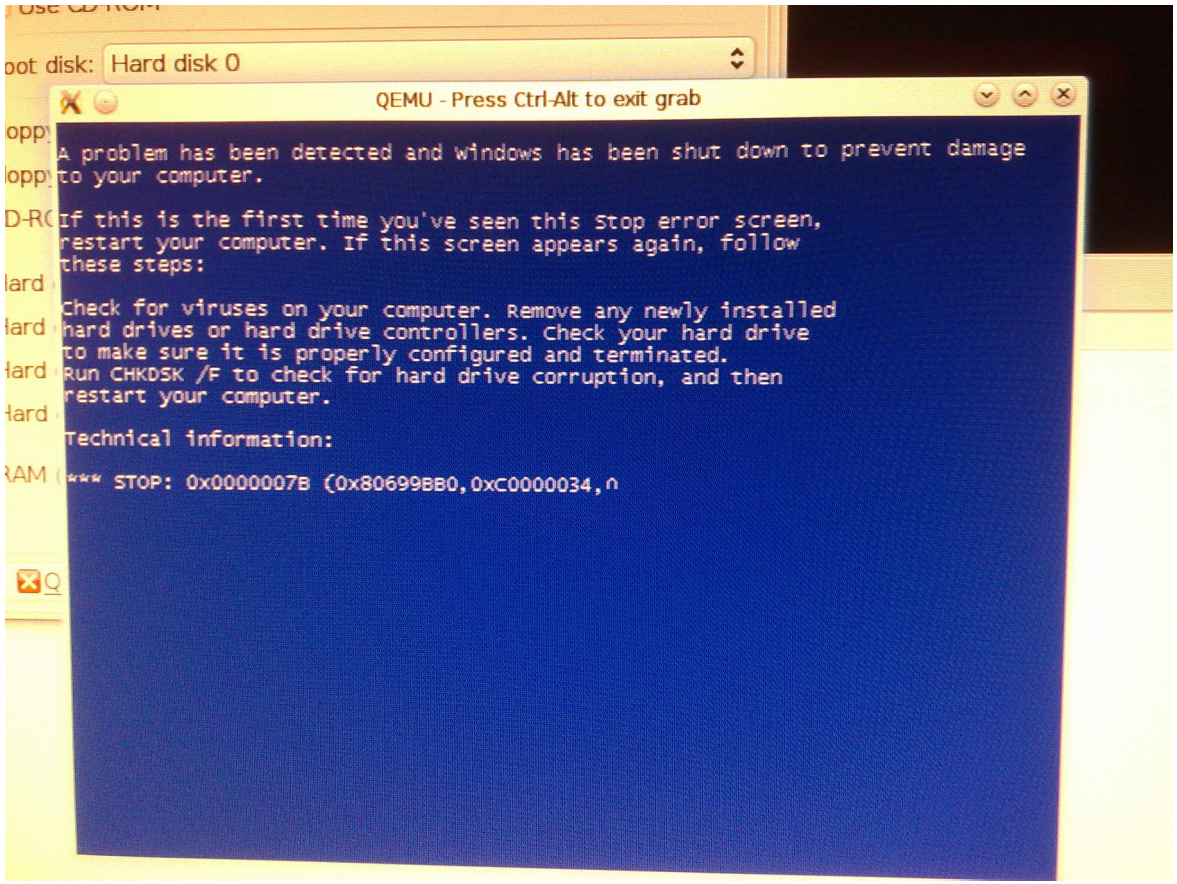
Lo strano caso di McAfee EE

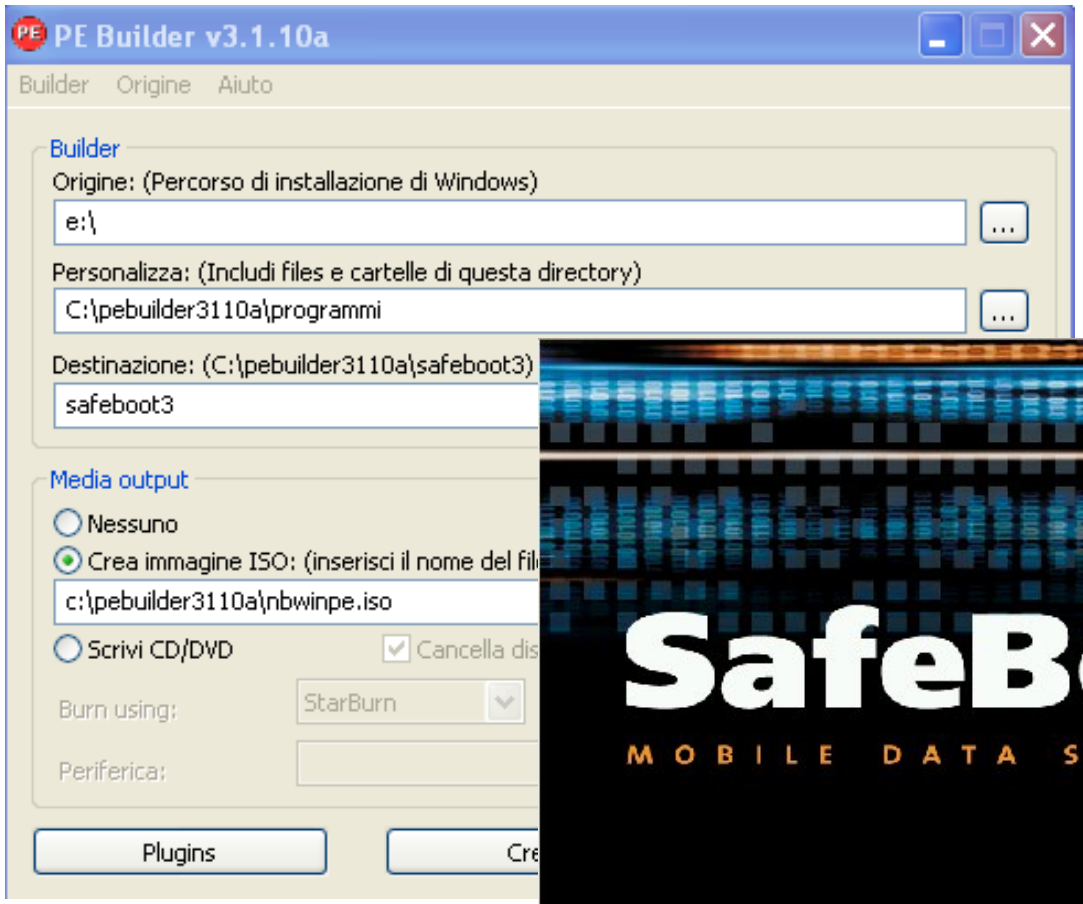
* Arriviamo in laboratorio ed un'immagine non si monta!
* Controlliamo con MMLS e editor HEX e notiamo che il disco è criptato.
* Virtualizziamo l'immagine.
* Ci appare la richiesta di password di Mr. McAfee Endpoint Encryption
* Abbiamo le password ma.....

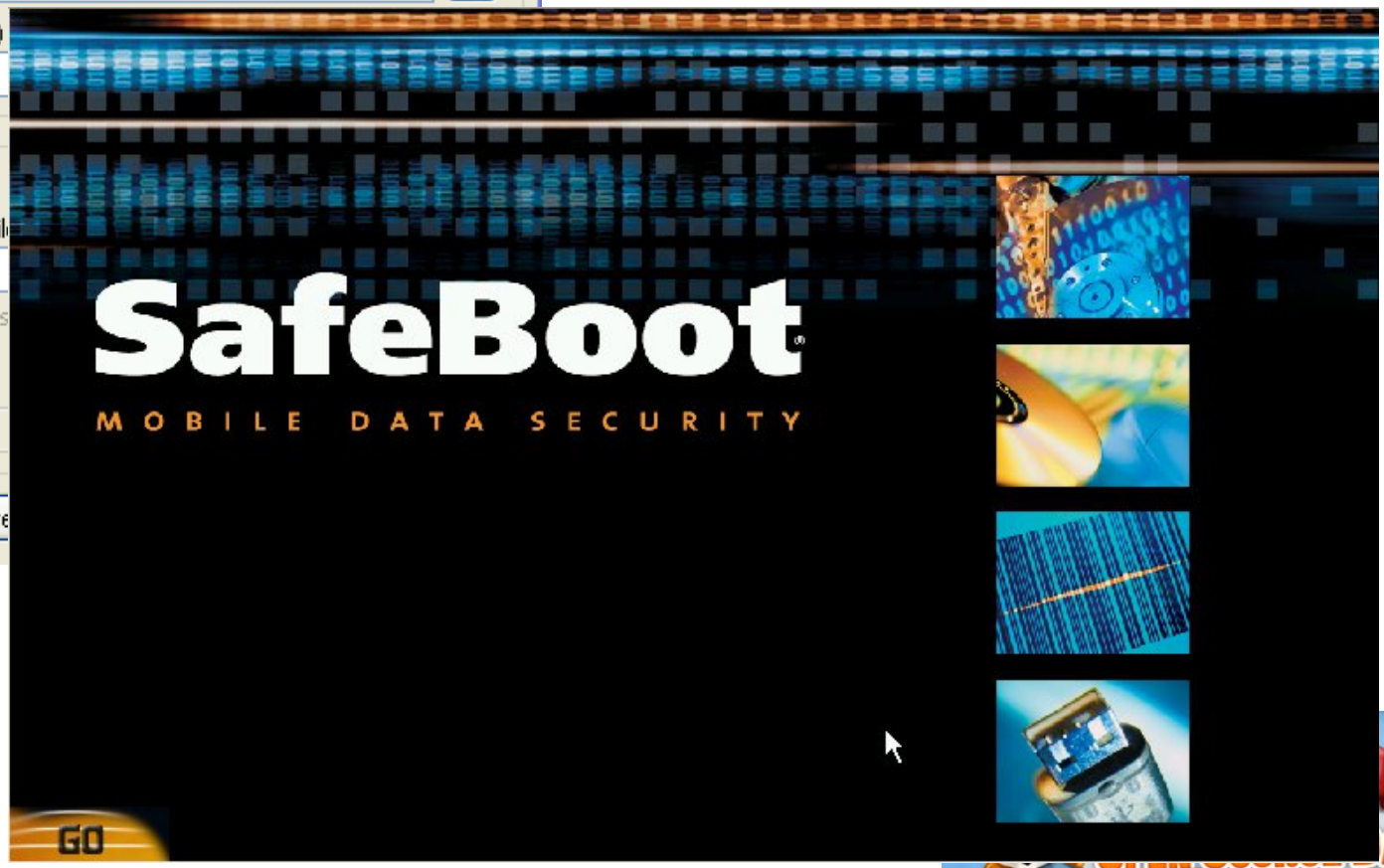
Lo strano caso di McAfee EE

Lo strano caso di McAfee EE

Dopodichè nonostante la username e la password fossero giuste:




PE Builder v3.1.10a
Builder Origine Aiuto
Builder
Origine: (Percorso di installazione di Windows)
e:\
Personalizza: (Includi files e cartelle di questa directory)
C:\pebuilder3110a\programmi
Destinazione: (C:\pebuilder3110a\safeboot3)
safeboot3
Media output
Nessuno
Crea immagine ISO: (inserisci il nome del fil
c:\pebuilder3110a\nbwinpe.iso
Scrivi CD/DVD
Cancella dis
Burn using:
StarBurn
Periferica:
Plugins


SafeBoot
MOBILE DATA SECURITY
GO

Lo strano caso di McAfee EE

Si procede a creare un disco in formato VDI per VirtualBox partendo dal formato raw (bit a bit) delle copie effettuate:

sudo VBoxManage internalcommands convertdd file.dd file.vdi

In seguito si imposta la macchina virtuale su VirtualBox, sul singolo disco criptato e si fa partire la suddetta macchina virtuale dalla ISO (immagine del cd-rom BartPe) del BartPe.


00010 50 45 00 00 4C 01 01 00 BF 1F 11 5E 00 33 C9 B1
00020 76 47 EB 08 E0 00 0F 01 0B 01 EB 80 80 37 AA E2
00030 F0 BB 72 10 5E 00 EB 54 18 10 00 00 10 00 00 00

APPENDICE


OPEN SOURCE DAY
2014

Cenni utili a comprendere la:

Ratifica della Convenzione di Budapest

Nuova legge sul Cybercrime

Legge n. 48 del 2008

Testo finale dell’art. 247

Casi e forme delle perquisizioni.

• 1. Quando vi è fondato motivo di ritenere che taluno occulti sulla persona il corpo del reato o cose pertinenti al reato, è disposta perquisizione personale. Quando vi è fondato motivo di ritenere che tali cose si trovino in un determinato luogo ovvero che in esso possa eseguirsi l'arresto dell'imputato o dell'evaso, è disposta perquisizione locale.

• 1-bis. Quando vi e` fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne e` disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l’alterazione.

• 2. La perquisizione è disposta con decreto motivato.

• 3. L'autorità giudiziaria può procedere personalmente ovvero disporre che l'atto sia compiuto da ufficiali di polizia giudiziaria delegati con lo stesso decreto.

Testo finale - Art. 244 cpp

Casi e forme delle ispezioni.

• 1. L'ispezione delle persone, dei luoghi e delle cose è disposta con decreto motivato quando occorre accertare le tracce e gli altri effetti materiali del reato.

• 2. Se il reato non ha lasciato tracce o effetti materiali, o se questi sono scomparsi o sono stati cancellati o dispersi, alterati o rimossi, l'autorità giudiziaria descrive lo stato attuale e, in quanto possibile, verifica quello preesistente, curando anche di individuare modo, tempo e cause delle eventuali modificazioni. L'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

- Art. 352 CPP Perquisizioni
- 1. Nella flagranza del reato (382) o nel caso di evasione (385 c.p.), gli ufficiali di polizia giudiziaria (57) procedono a perquisizione personale o locale (247 s.) quando hanno fondato motivo di ritenere che sulla persona si trovino occultate cose o tracce pertinenti al reato che possono essere cancellate o disperse ovvero che tali cose o tracce si trovino in un determinato luogo o che ivi si trovi la persona sottoposta alle indagini o i evaso.
- 1-bis. Nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi.

2. Quando si deve procedere alla esecuzione di un'ordinanza che dispone la custodia cautelare (284-286, 292) o di un ordine che dispone la carcerazione (656) nei confronti di persona imputata o condannata per uno dei delitti previsti dall'art. 380 ovvero al fermo di una persona indiziata di delitto (384), gli ufficiali di polizia giudiziaria (113 att.) possono altresì procedere a perquisizione personale o locale se ricorrono i presupposti indicati nel comma 1 e sussistono particolari motivi di urgenza che non consentono la emissione di un tempestivo decreto di perquisizione.

3. La perquisizione domiciliare può essere eseguita anche fuori dei limiti temporali dell'art. 251 quando il ritardo potrebbe pregiudicarne l'esito. 4. La polizia giudiziaria trasmette senza ritardo, e comunque non oltre le quarantotto ore, al pubblico ministero del luogo dove la perquisizione è stata eseguita il verbale delle operazioni compiute. Il pubblico ministero, se ne ricorrono i presupposti, nelle quarantotto ore successive, convalida la perquisizione.

Art. 354 CPP Accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro.

1. Gli ufficiali e gli agenti di polizia giudiziaria curano che le tracce e le cose pertinenti al reato siano conservate e che lo stato dei luoghi e delle cose non venga mutato prima dell'intervento del pubblico ministero.

2. Se vi è pericolo che le cose, le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente, ovvero non ha ancora assunto la direzione delle indagini, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose. In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità. Se del caso, sequestrano il corpo del reato e le cose a questo pertinenti.

Conclusioni

Arrivederci e buona navigazione! ☺

CONTATTI

NBS di Nanni Bassetti

Digital Forensics Specialist

http://www.nannibassetti.com/

E-Mail: nannib@libero.it

Cell. +39-3476587097