

Hacker's Corner - Festival del Giornalismo

Perugia, 24-28 aprile 2013



TAILS - Il tuo nuovo pc: *tascabile, sicuro, non intercettabile e gratuito*

Marco A. Calamari

Centro HERMES per la trasparenza ed i diritti digitali

marco.calamari@logioshermes.org

Progetto Winston Smith

marcoc@winstonsmith.org

Copyright 2013, Marco A. Calamari

È garantito il permesso di copiare,
distribuire e/o modificare questo documento
seguendo i termini della GNU General Public
License, Versione 2 o versioni successive
pubblicata dalla Free Software Foundation.
Una copia della licenza tradotta in italiano
è acclusa come nota a questa slide;
l'originale in lingua inglese è reperibile
all'URL

<http://www.fsf.org/licenses/gpl.html>

- **Perche' "Il tuo nuovo PC"?**
- **TAILS?**
- **Ma quando lo distribuirete?**
- **Ma funziona su ?**
- **Tre pillole di Storia**
 - Pgp**
 - Remailer anonimi**
 - Tor**
- **Linux? GNU? Boum.org HERMES? GlobaLeaks?**
- **Live CD / Live USB**
- **Tracce e prove informatiche**

- **Perche' sara' a tutti gli effetti, se lo vorrete e/o dovrete usare, come avere un nuovo pc**
- **The Amnesic Incognito Live System**
- **Alla fine del workshop**
- **Ma funziona su ?**
- **Linux? GNU? Boum.org HERMES? GlobaLeaks**
- **Live CD / Live USB**

Venticinque anni fa, quando la Rete a stento emergeva dalle universita', chi creava e diffondeva questi strumenti era considerato "strano" anche tra gli internettari di allora.

Oggi la Rete e' quello che e', ed uno dei suoi impieghi assai diffusi e' di strumento economico e potentissimo contro la liberta' ed i diritti civili.

La cosa piu' pericolosa e' che il tutto lavora in maniera invisibile, sotto il pelo dell'acqua, e che alla fin fine quasi tutti sono convinti che nessuno se li fili, che la cosa non li riguardi.

Bene, se avrete pazienza forse uscirete di qui con una soluzione, od almeno un pezzo di soluzione a problemi che non sapevate di avere.

E poiche' la storia del passato e' indispensabile per capire il presente ed immaginare il futuro, cominciamo proprio da tre pillole di storia.



Prima pillola: **Storia**

La storia della crittografia copre oltre due millenni, ma può essere riassunta con una manciata di nomi e di fatti.

circa 450 a.e.v. - **Erodoto** racconta la storia di un nobile persiano che fece rasare i capelli ad uno schiavo fidato, gli fece tatuare un messaggio sul cranio, attese fino a quando i capelli furono ricresciuti e lo inviò a destinazione con l'istruzione di rasarsi nuovamente i capelli una volta arrivato. Metodo con larghezza di banda limitata, forte latenza ed oltretutto steganografia, non crittografia.

58 a.e.v. - **Gaio Giulio Cesare** usa e più tardi descrive nel *“De Bello Gallico”* il *cifrario cesariano*, o di sostituzione monoalfabetica, per corrispondere con Lucio Cornelio Balbo Maggiore mentre era impegnato nelle sue campagne militari. Primo esempio moderno di separazione tra chiave ed algoritmo, usato oggi solo alle elementari per scambiarsi bigliettini che la maestra non dovrebbe riuscire a leggere..

1586 p.e.v. - nel *“Traité des Chiffres”* **Blaise de Vigenère** descrive il primo metodo storico di sostituzione polialfabetica, che è un metodo a chiave singola, privata

1941 p.e.v. - **Konrad Zuse** costruisce lo **Z3** il primo elaboratore automatico non meccanico controllato da un programma

1976 p.e.v.: l'NSA ed il governo americano eleggono un algoritmo crittografico a chiave privata, proposto in maniera non troppo indipendente da IBM, a standard crittografico FIPS federale (**DES**).

circa 1970 p.e.v. - varie persone hanno una idea rivoluzionaria, la crittografia a chiave pubblica. che permette di evitare lo scambio delle chiavi tra i corrispondenti e rappresenta **LA** tecnologia abilitante per le applicazioni crittografiche moderne.

Scoperta da **James Ellis** impiegato dell'MI5 intorno al 1970 e chiusa in un cassetto dai suoi capi fino al 1997, prima perche' non ne avevano capito l'importanza e poi probabilmente per la vergogna o per non essere silurati.

Riscoperta in maniera sostanzialmente indipendente da **Withfield Diffie e Martin Hellmann** nel 1976 (DH), e da **Ron Rivest, Adi Shamir e Leonard Adleman** al MIT nel 1977(RSA). Diffie vi sarebbe stato simpatico, un vero personaggio. Anche per gli standard degli anni '70 era un fricchettone eccezionale, geniale e motivato alla Stallmann o meglio alla Wau Holland.

Nel **1981** David Chaum introdusse, teorizzò e sistematizzò il concetto di **Mix-net [1]**, cioè di rete paritaria di scambio di messaggi cifrati.

Nel **1986** una famosa querelle giuridica, suscitata da una iniziativa della **religione di Scientology** provoca l'inizio della reazione del gruppo Cypherpunks e la nascita dei sistemi crittografici di comunicazione moderni, implementando per la prima volta in maniera crittograficamente robusta il meccanismo delle **Mixnet**.

Nel **1991** **Philip R. Zimmermann**, un programmatore freelance di Boulder, Colorado, pubblica in Rete **Pretty Good Privacy**, il primo programma di crittografia forte disponibile al pubblico. Il nome è preso da una sitcom radiofonica dell'epoca, in cui esisteva un emporio di frutta e verdura "Pretty Good Grocery". Il nome è fuorviante perché la privacy garantita dal programma non è *"piuttosto buona"* ma **eccezionale**.

Pgp poteva cifrare sia mail che file generici

Nel **1993** PGP si diffonde anche all'estero, e questo pone Zimmermann **nel mirino delle indagini dell'FBI**. Gli Stati Uniti durante la guerra hanno ben giocato la partita dei codici cifrati e nel dopoguerra hanno creato la piu' grossa organizzazione del mondo dedicata alla crittografia e la crittoanalisi, la **National Security Agency**, per gli amici degli acronimi **NSA**.

Esiste infatti gia' da anni una legge, **l'ITAR**, che vieta l'esportazione fuori dal territorio federale di armi da guerra, tecnologie nucleari e sistemi crittografici. Attorno a lui, oltre che un provvidenziale collegio di difesa finanziato da persone di ogni estrazione e nazionalita' (me incluso), si crea un movimento libertario di opinione come ormai in Rete non si vedono piu'.

Dopo quasi 4 di indagini anni viene trovata una scappatoia di tipo legale, anzi un vero hacking legale....

Si tratta di ritorcere il sistema legale americano contro se' stesso. Il codice sorgente di PGP venne [pubblicato su un libro](#), monotono ma interessante, della MIT Press, venduto a 60 dollari in tutto il mondo.

La possibilita' di diffondere il libro in ogni modo, anche all'estero, e' garantita dal Primo Emendamento della Costituzione americana sulla liberta' di espressione, che come principio costituzionale prevale su qualsiasi legge contraria.

Col solo fatto di esistere il libro poteva, in linea di principio, essere scannerizzato e sottoposto ad OCR, riproducendo cosi' all'estero una copia dei sorgenti, e quindi rendeva legale la loro esportazione.

L'ITAR si rivela cosi' non applicabile, perche' impone un vincolo che una legge piu' forte permette di ignorare ed intorno al 1997 le indagini su Zimmerman cessano senza che si sia mai arrivati ad una formale incriminazione.

Superpotenza Globale 0 – Popolo della Rete 1 (allora poteva succedere....)

Negli **anni '90** Paul Syverson ed altri estesero l'applicazione delle **Mixnet** all'incapsulamento crittografico per il routing di pacchetti di informazioni, il cosiddetto **Onion Routing** [2] .

E siamo già arrivati ad oggi

Tutto è partito da queste poche pietre miliari risalenti ormai a millenni passati.

Il terzo millennio ancora non ha prodotto nessun nuovo sviluppo di importanza paragonabile)



Seconda pillola: **Posta Elettronica**

Perche' la posta elettronica? Perche' fino all'avvento del web e' stata l'applicazione Internet per eccellenza.

La comunicazione via posta internet, come la controparte cartacea, e' caratterizzata da quattro tipi di informazioni

- **Il contenuto del messaggio**
- **Il mittente del messaggio**
- **Il destinatario del messaggio**
- **L'esistenza stessa di una comunicazione**

Mantenere la riservatezza del contenuto e' un problema risolto, grazie ad esempio a Pgp.

Mantenere le altre informazioni riservate e' un problema piu' complesso ma risolto; programmi come i Remailer Anonimi, i Server di Pseudonimi e la steganografia esistono e sono stati realizzati, ma non sono adatti ad essere serviti in pillole.....

Un interessante fatto storico sui remailer anonimi e' stato la violazione di uno di essi con metodi non tecnologici.

Il remailer anon.penet.fi, realizzato da Johan "Julf" Helsingius nel 1993 ed operativo fino al 1996, fu appunto violato costringendo per vie legali il suo remop (gli operatori dei remailer vengono chiamati tradizionalmente "*remop*") a fornire l'indirizzo reale del mittente.

In due distinti casi un ex adepto di una nota setta religiosa diffuse documenti "segreti" usando il remailer.

Invocando una violazione di copyright ed una rogatoria internazionale tramite l'Interpol, [la religione di Scientology](#), da allora [nemica "storica"](#) della crittografia, costrinse Julf a rivelare il nome dell'adepto, cosa che lo obbligo' per correttezza a chiudere l'ormai "abusato" remailer

A large, stylized version of the HERMES logo, with the 'H' in dark blue and the rest of the letters in a lighter blue.

terza pillola: **Tor**

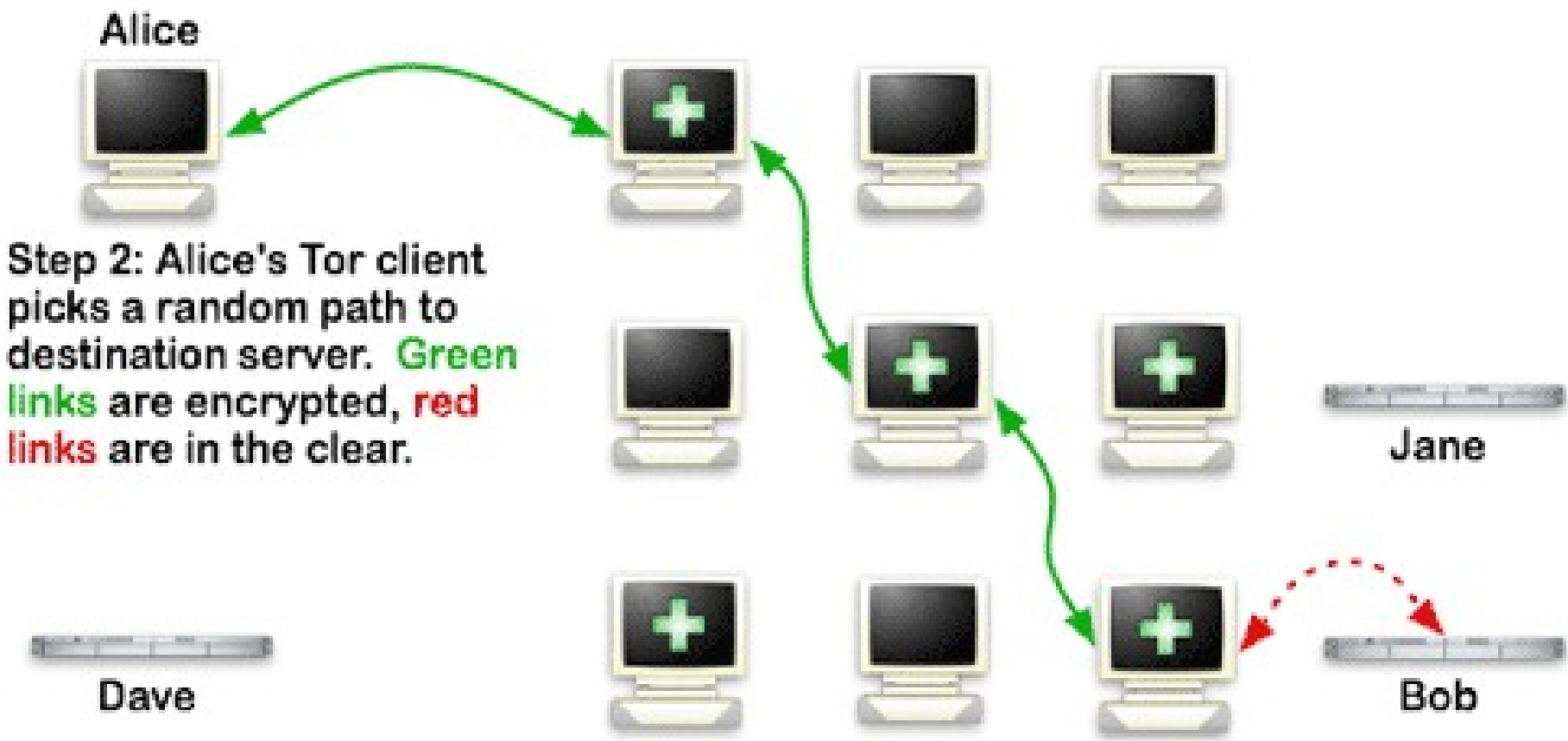
Tor - The second generation Onion Routing [3] e' una rete anonimizzante di proxy criptati che permette di rendere anonima qualunque comunicazione avvenga tramite l'utilizzo di TCP.

Implementata come proxy SOCKS, permette di usare tutti i piu' comuni programmi per l'accesso ad internet quali browser web, chat, posta elettronica, newsgroup e qualunque applicazione utilizzi solo circuiti TCP (niente UDP, quindi niente streaming).

Tor e' una PET di seconda generazione, sviluppata con particolare cura e che pone a livello di progettazione la difesa anche legale (plausible deniability) del degli utenti e dei gestore di router Tor.

EFF How Tor Works: 2

-  Tor node
-  unencrypted link
-  encrypted link



Tor anonimizza la vostra connessione TCP, facendola uscire attraverso un router Tor scelto a caso, **MA da solo**

NON nasconde l'appartenenza alla mixnet TOR

NON protegge l'ultima parte della connessione dal router Tor di uscita fino al server di destinazione

NON protegge le informazioni trasmesse

NON impedisce alle applicazioni di far uscire informazioni rivelatrici attraverso la normale Rete (es. richieste DNS)

NON impedisce a contenuti passivi od attivi di rivelare l'identità del mittente (cookies, javascript) su un canale esterno nascosto.

NON impedisce l'**harvesting** (spigolatura) di informazioni da parte di un router di uscita malizioso



Impronte ed orme: il PC

PATENT PENDING

MAGNET
FORENSICS.

M

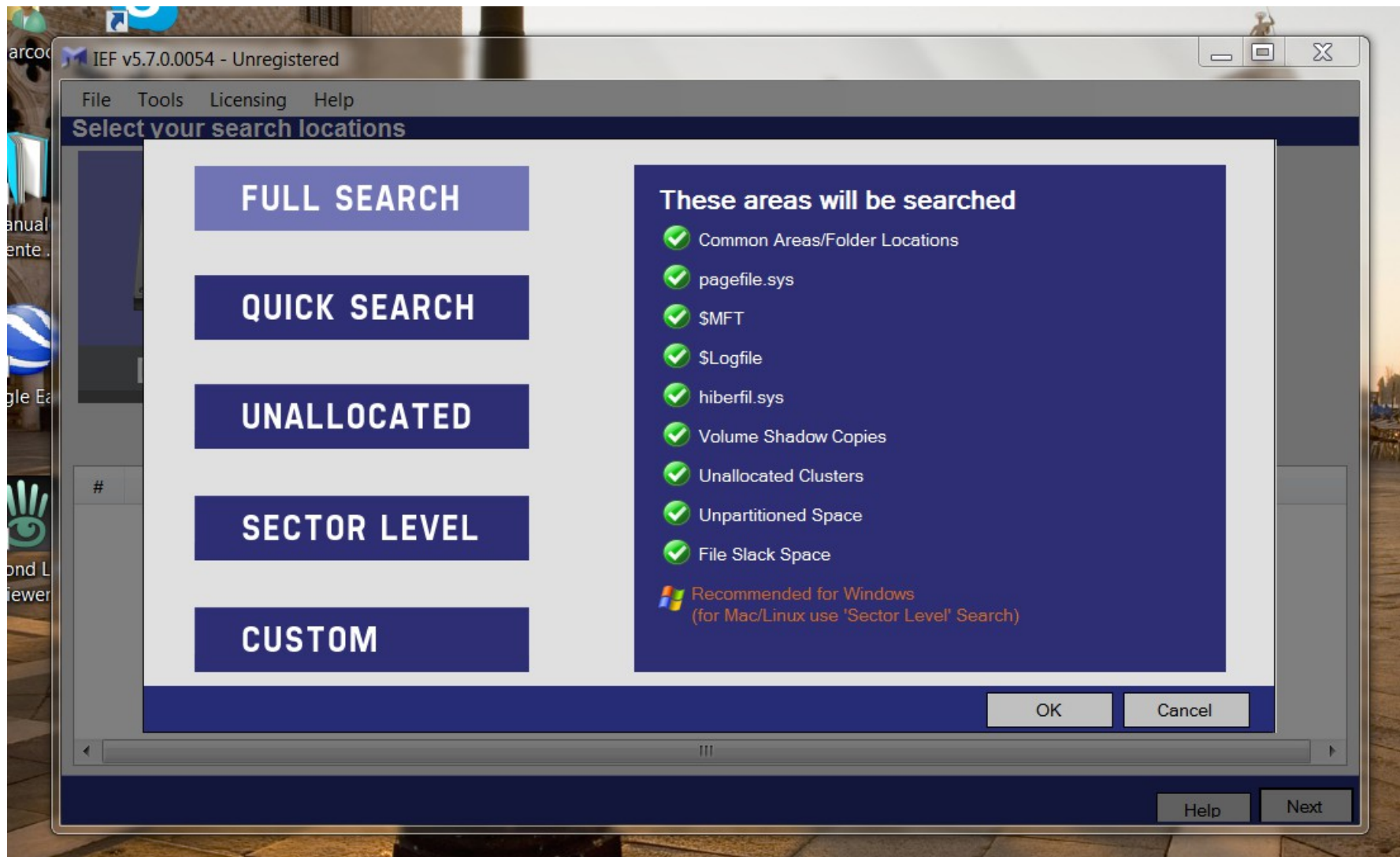
INTERNET EVIDENCE FINDER

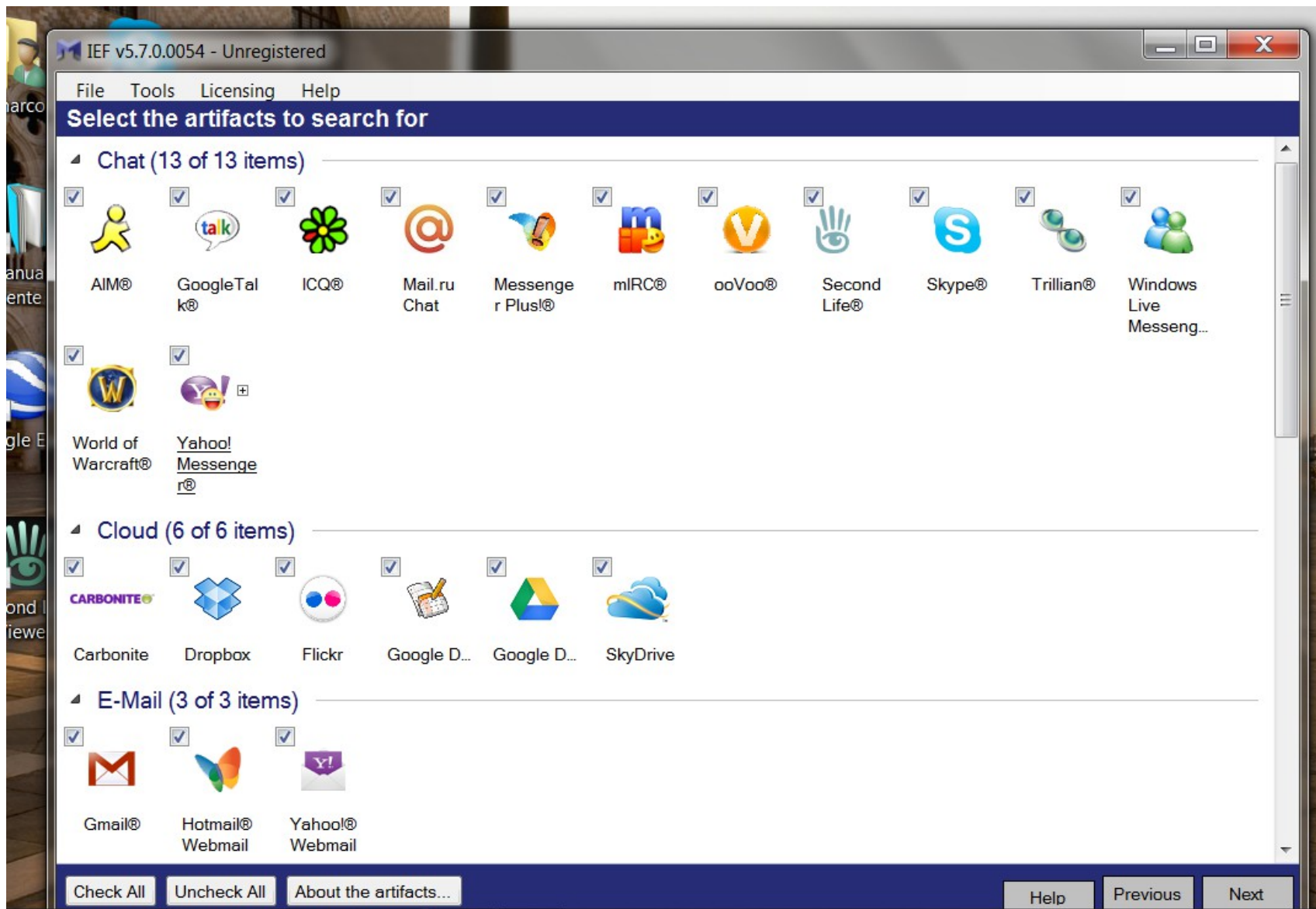
Click anywhere to continue.

By using this software you are agreeing to the End User License Agreement.

Running in demo mode

Cestino





IEF Report Viewer v5.7.0.0054 - Case: 1

File Edit **Tools** Go To Help Default Encoding

Recovered Artifacts	Items
IEF Refined Results	
Facebook URLs	4
Parsed Search Queries	21
Rebuilt Webpages	4
Social Media URLs	5
Chat	
Second Life Chat	20
Skype Accounts - calamarim	2
Skype Calls - calamarim	15
Skype Carved Messages	20
Skype Chat Messages - calamarim	20
Skype chatsync Message...	20
Skype Contacts - calamarim	20
Skype File Transfers - calamarim	9
Skype Group Chat - calamarim	5
Skype SMS - calamarim	1
Skype Sync Chat Message...	20
Skype Voicemails - calamarim	9
Media	
Pictures	39
Videos	1

★ #	Date/Time - (UTC)	Message	Source	Located At
1...	17/04/2013 11:0...	cosi' e' forse piu...	C:\Users\marcoc...	File offset 36860
1...	27/09/2092 17:1...	<files alt="Poste...	C:\Users\marcoc...	File offset 37101
1...	19/04/2013 08:3...	uh. mi sa che c'...	C:\Users\marcoc...	File offset 40956
1...	19/04/2013 10:2...	de nada :)	C:\Users\marcoc...	File offset 42011
1...	19/04/2013 10:2...	io ho messo su ...	C:\Users\marcoc...	File offset 43035
1...	19/04/2013 10:2...	va in release tra ...	C:\Users\marcoc...	File offset 43249
1...	19/04/2013 10:4...	ok, sentiamo un ...	C:\Users\marcoc...	File offset 43921
2...	19/04/2013 10:4...	che e' vagrant?	C:\Users\marcoc...	File offset 44137

Previous Showing results 1 - 20 of 20

Date/Time - (UTC) (dd/MM/yyyy) 19/04/2013 10:46:20
Message ok, sentiamo un po' che ci dice :)
Source C:\Users\marcoc\AppData\roaming\Skype\calamarim\chatsync\41\41bdd88fd21d8096.dat
Located At File offset 43921

Alerts Bookmarks Filter Search

L'attività su un personal computer, uno smartphone, un tablet od un pad lascia non solo tracce in Rete, ma anche sul pc o device stesso.

Esistono modi per evitare di lasciare un singolo tipo di traccia, ma un sistema operativo moderno, unito alla varietà e complessità dei metodi che si usano per comunicare in rete, ne rende praticamente impossibile la completa eliminazione.

L'unica soluzione semplice consisterebbe nel distruggere completamente il pc dopo l'uso, o trovare un modo per riportarlo esattamente nelle condizioni iniziali.

Questo modo esiste grazie a versioni particolari di Linux che funzionano direttamente da CD o chiavetta usb senza scrivere assolutamente niente sul vostro pc.



...e finalmente: il gadget

TAILS e' una di queste versioni “live”, che appunto:

- 1. Non lascia traccia del suo utilizzo sul pc**
- 2. Impedisce, anche per sbaglio, di “uscire” dalla rete Tor e di rendersi quindi intercettabile tramite le usuali tecniche di sorveglianza**
- 3. Permette, se usato da chiavetta USB, di utilizzare quando necessario un'area crittografata ed inaccessibile della chiavetta stessa per memorizzare file, mail e preferenze che fosse necessario conservare.**

Ad esempio, un lifesaver del giornalista che debba comunicare con la redazione mentre si trova in paesi poco liberali, od addirittura in zone di guerra.

- [1] **Untraceable Electronic Mail, Return addresses, and Digital Pseudonyms** - *David L. Chaum, 1981* <http://www.weidai.com/mix-net.txt>
- [2] **Hiding Routing Information** - *David M. Goldschlag, Michael G. Reed, and Paul F. Syverson, 1996* - Workshop on Information Hiding, Cambridge – <http://www.onion-router.net/Publications/IH-1996.pdf>
- [3] **Tor: The Second-Generation Onion Router** – *R. Dingledine et al., 2004* – <http://www.torproject.org/svn/trunk/doc/design-paper/tor-design.pdf>
- [4] **Crowds: Anonymity for Web Transactions** - *Michael K. Reiter, Aviel D. Rubin, 1997* ACM Transactions on Information and System Security
- [5] **The Darknet and the Future of Content Distribution** - *Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, 2002* proceedings of ACM Workshop on Digital Rights Management
- **Tor** <http://www.torproject.org>
- **TAILS** <http://tails.boum.org>
- **Kryptonite: fuga dal controllo globale** - *Joe Lametta* Edizioni Nautilus/Shake, 1998 - <http://isole.ecn.org/kryptonite/kripto.zip>

Grazie a tutti per l'attenzione

ci sono domande ?

Potete contattarmi qui: marco.calamari@logioshermes.org

Centro HERMES per la trasparenza ed I diritti digitali

<http://www.logioshermes.org>

Il Progetto Winston Smith

<http://www.winstonsmith.org>