Linux Day **Firenze** - ***25 ottobre 2014***

TAILS

un computer in tasca a prova di ficcanaso

Marco A. Calamari
Centro HERMES per la trasparenza ed i diritti digitali
marco.calamari@logioshermes.org
Progetto Winston Smith
marcoc@winstonsmith.org

Sommario

- **Tre pillole di Storia**
  - **Pgp**
  - **Remailer anonimi**
  - **Tor**
- **Impronte ed orme; (non) lasciare tracce e prove informatiche sul pc**
- **Workshop, hands-on (avete portato il portatile, vero?)**

Domande

- **Tool del “dopo Datagate””?**
- **TAILS?**
- **Ma quando distribuite la chiavetta?**
- **Ma funziona su ….. ?**
- **Linux? GNU? Boum.org? HERMES? GlobaLeaks**
- **Lasciare tracce e prove informatiche sul pc**

Risposte

- **Se lo usano tutti da anni, non ultimi Edward Snowden e Glenn Greenwald, ci sara' un motivo**
- **The Amnesic Incognito Live System**
- **Alla fine del workshop**
- **.. quasi su tutto ...**
- **Linux! GNU! Boum.org! HERMES! GlobaLeaks!**
- **Live CD / Live USB**

Perche' la crittografia?

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

Cenni storici...

La storia della crittografia copre oltre due millenni, ma puo' 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 invio' 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 piu' 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 biglettini che la maestra non dovrebbe riuscire a leggere..

...Cenni storici...

1586 p.e.v. - nel *"Traité des Chiffres"* **Blaise de Vigenère** descrive il primo metodo storico di sostituzione polialfabetica, che e' 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**).

...Cenni storici

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.

Le origini

Nel **1981** David Chaum introdusse, teorizzo' e sistematizzo' il concetto di **Mix-net [1]** , cioe' 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 e' preso da una sitcom radiofonica dell'epoca, in cui esisteva un emporio di frutta e verdura “Pretty Good Grocery”. Il nome e' fuorviante perche la privacy garantita dal programma non e' *”piuttosto buona”* ma eccezionale.

Pgp poteva cifrare sia mail che file generici

...PGP...

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 terriotorio 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....

...PGP

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....)

...PGP

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 gia'arrivati ad oggi

Tutto e' partito da queste poche pietre miliari risalenti orami a millenni passati.

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

Seconda pillola: Posta Elettronica

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.

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

Anonymous Remailer

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

HERMES

terza pillola: Tor

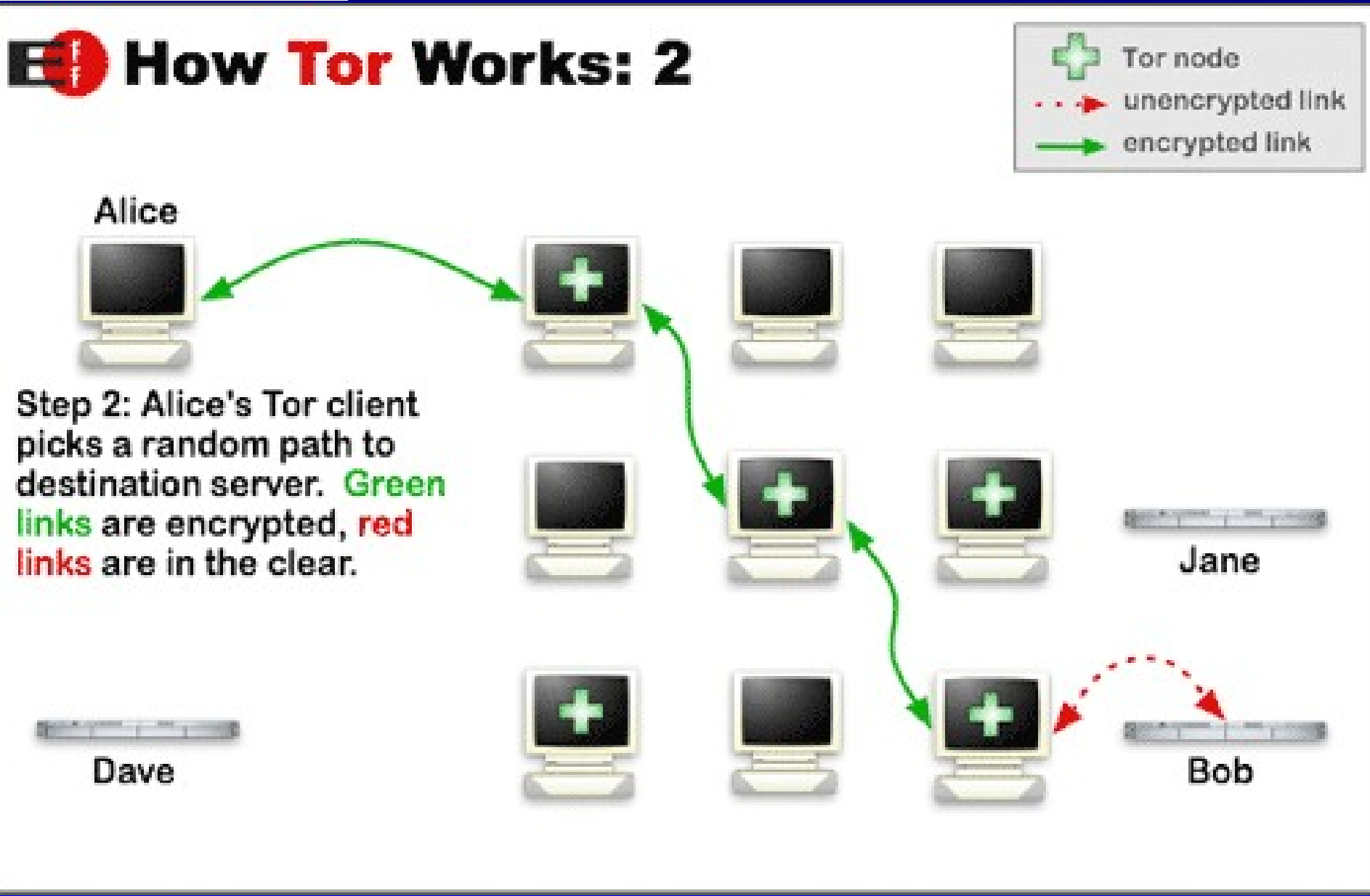
Tor ...

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.

... Tor ...



... Tor

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)

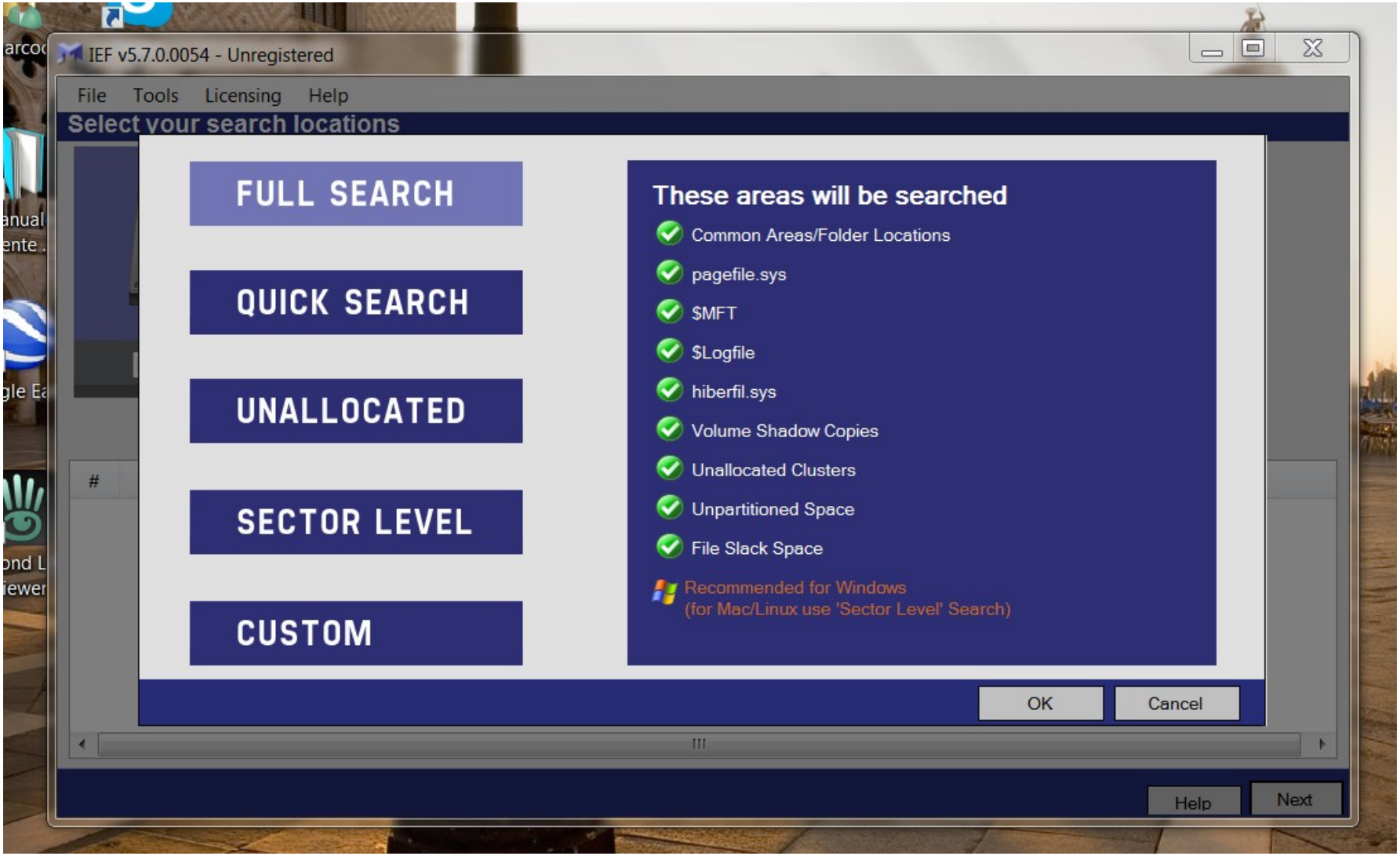
NON impedisce a contenuti passivi od attivi di rivelare l'identita' del mittente (cookies, javascript) su un canale esterno nascosto.

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

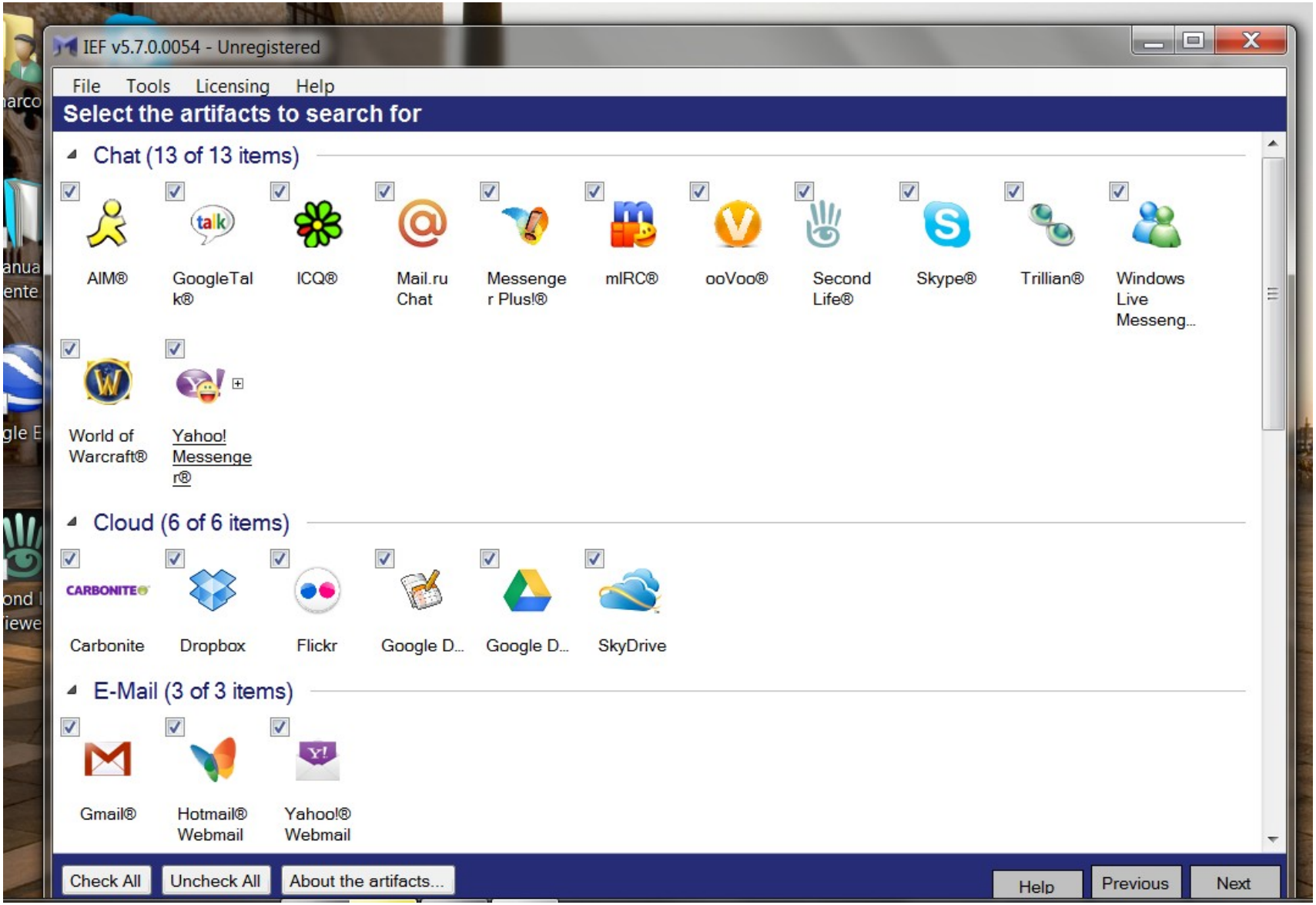
Impronte ed orme: il PC

Perche' Live CD / Live USB

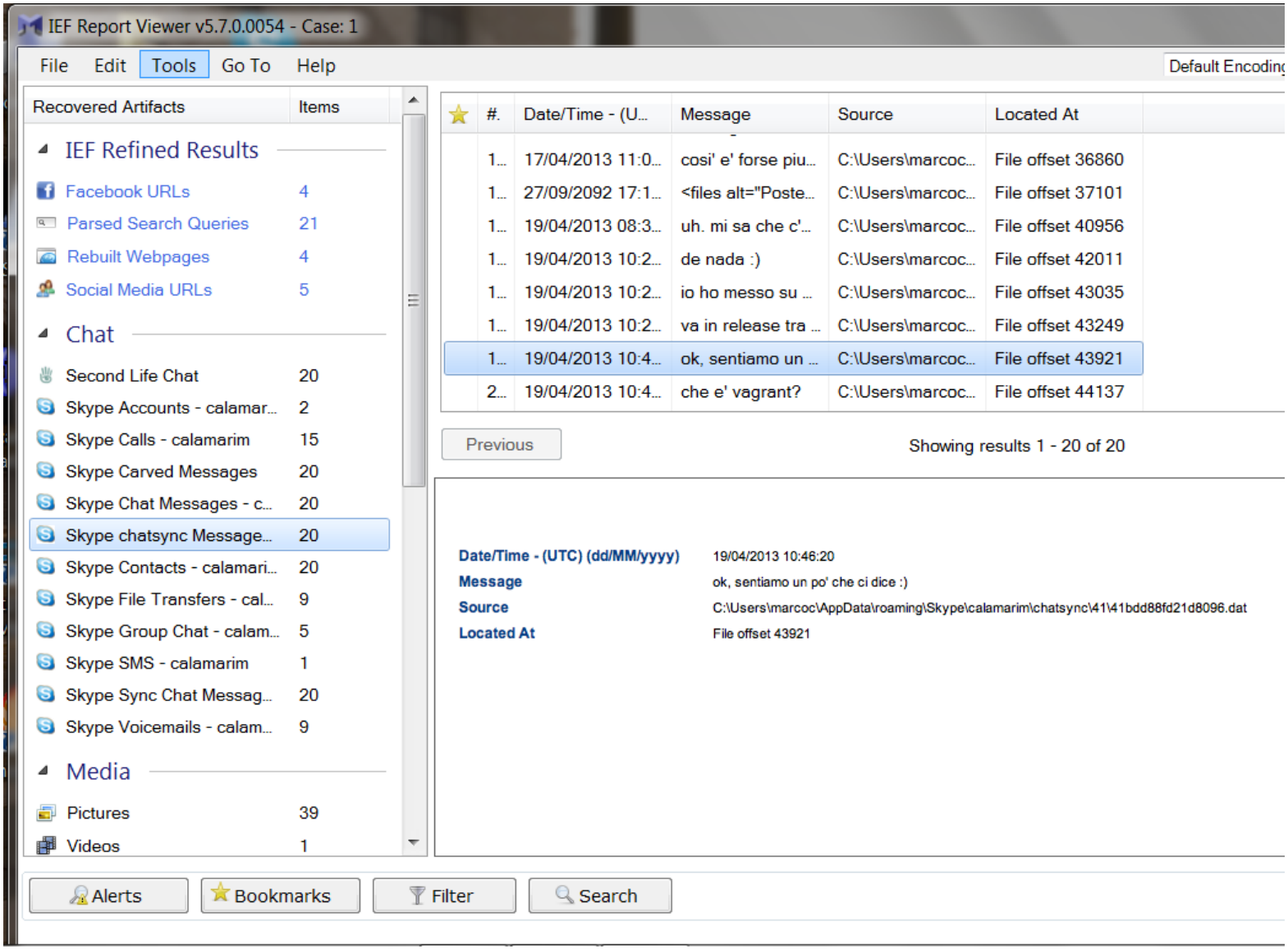
Perche' Live CD / Live USB



Perche' Live CD / Live USB



Perche' Live CD / Live USB



Tracce

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

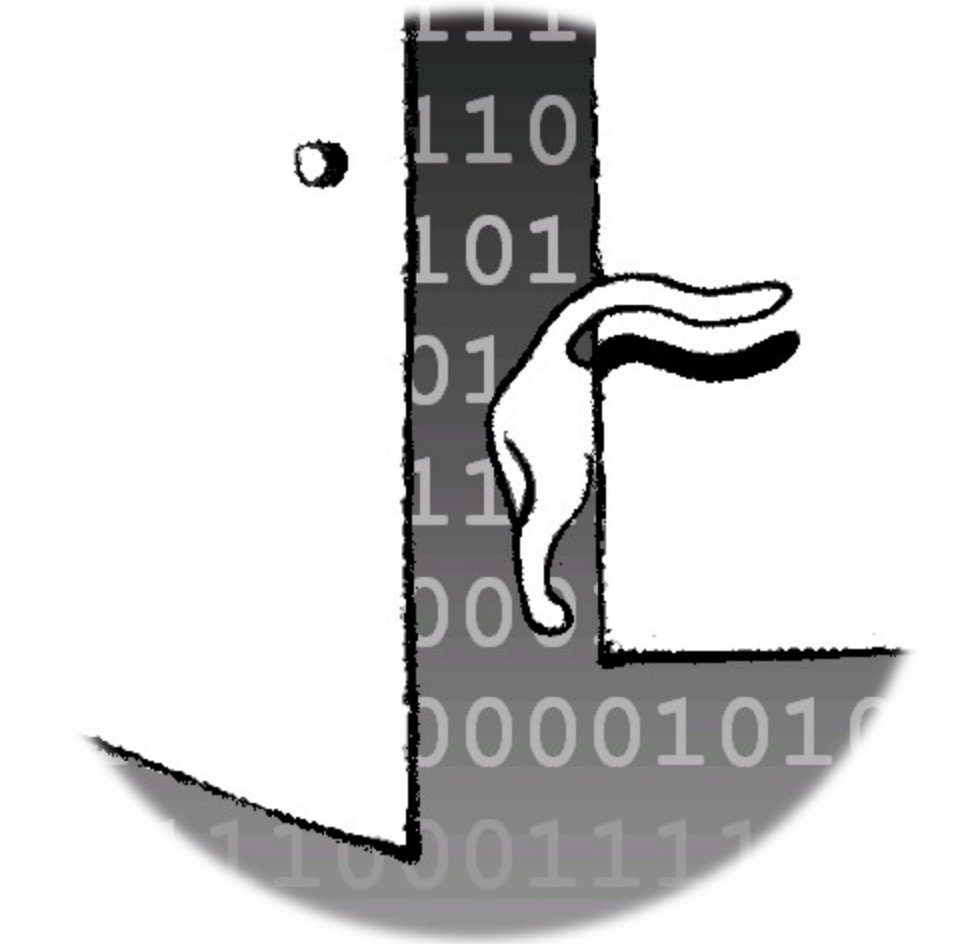
Esistono modi per evitare di lasciare un singolo tipo di traccia, ma un sistema operativo moderno, unito alla varieta' e complessita' dei metodi che si usano per comunicare in rete, ne rende praticamente impossibile la competa eliminazione.

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.

Tails
theamnesicincognitolivesystem

...e finalmente TAILS



GNU/Linux TAILS

TAILS e' una versioni “live” di GNU/Linux 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 memorizzzare file, mail e preferenze che fosse necessario conservare.

Un lifesaver del giornalista che debba comunicare con la redazione mentre si trova in paesi poco liberali, od addirittura in zone di guerra, o debba divulgare porcherie di qualche agenzia triletterata

Itinerario del workshop - 1

Configurare il boot da USB (F12, etc.)

Eventuale TAB per aggiungere “truecrypt” in fondo per abilitarlo. Perche' si e perche' no.

Schermata di boot; in basso selezione linguaggio, paese e tastiera

Schermata di boot; cosa e' “abilita persistenza”?

Schermata di boot; cosa sono “opzioni aggiuntive”?

Opzioni aggiuntive: decidere la password di rroot

Opzioni aggiuntive; mimetizzarzi graficamente

Opzioni aggiuntive: mimetizzare il mio indirizzo MAC di rete

Via!

Collegamento alla rete

Parte Tor

Perche' non possono sapere chi sono quando navigo?

Merito di Tor, ma non dite chi siete!

Ed ora, che posso fare? Lancio il browser a navigo anonimo

Ma e' vecchia! Perche' non date la 1.0? Come faccio ad aggiornarla? Mi serve farlo?

SI puo' aggiornare direttamente online sulla chiavetta che state usando, e funziona ,,,,

Itinerario del workshop – 2

Browser sicuro

Doppio click sulla cipollina verde sulla barra in alto; Vidalia e la mappa della rete. Da dove passa la mia connessione?

Gpg e mail cifrata ……

Pidgin + OffTeRecord; chat sicura

Truecrypt , Palimpsest e LUKS per cifrare tutto

Gestore di password KeePassX

Dove sono I miei file? Ed I miei settaggi?

Ma se devo scrivere (calcolare, ascoltare musica, elaborare file aaudio, elaborare immagini, elaborare filmati, fare un cd, antani …) ? C'e' gia' tutto,

Quello che non fosse disponibile posso memorizzarlo nella partizione cifrata ed installarlo al volo quando mi server.

Browser “pericoloso”: perche' c'e' ed a cosa serve?

Cambiare la password “cambiamisubito”. Meglio riformattare la partizione comunque.

Configurazione ed aggiornamento del disco cifrato e della persistenza dei dati

E per finire, lo strappo della chiavetta!!!

Letture suggerite

- [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
- **Kriptonite: fuga dal controllo globale** - *Joe Lametta* Edizioni Nautilus/Shake, 1998 - http://isole.ecn.org/kriptonite/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