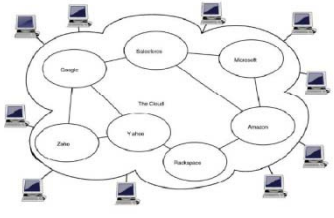
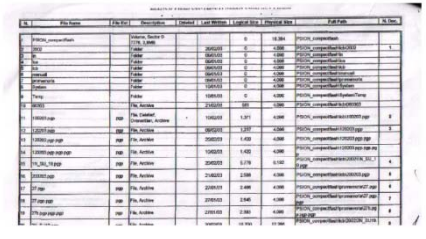
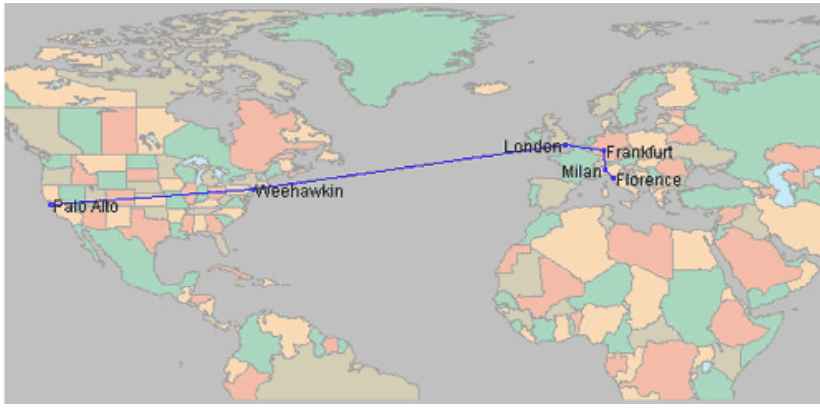
avv. Stefano Aterno
avvocato del Foro di Roma
docente universitario

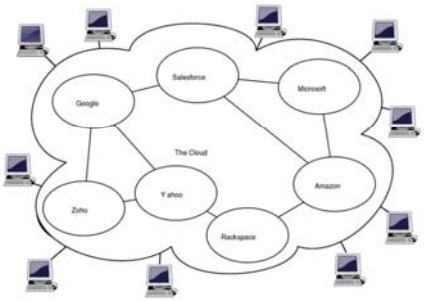
10-08-2007	18:15	0227003***	Milano	0:00:28
13-08-2007	20:53	026100***	Milano	0:02:39
15-06-2007	15:29	039328***	Monza	0:00:26
15-06-2007	15:09	039328***	Monza	0:05:35
15-06-2007	15:18	068578***	Roma	0:00:26
21-06-2007	10:04	068578***	Roma	0:01:47
02-07-2007	10:15	039328***	Monza	0:02:25
02-07-2007	10:20	068578***	Roma	0:00:08
02-07-2007	10:25	068578***	Roma	0:00:09
04-07-2007	17:40	068578***	Roma	0:00:06
04-07-2007	18:03	068578***	Roma	0:00:32
05-07-2007	09:24	068578***	Roma	0:00:43
05-07-2007	09:26	068578***	Roma	0:00:14
05-07-2007	09:27	068578***	Roma	0:01:08
05-07-2007	09:40	039328***	Monza	0:00:20
05-07-2007	10:02	0393282***	Monza	0:01:10
08-07-2007	15:13	0392848***	Monza	0:00:45
10-07-2007	15:00	068578***	Roma	0:00:10
10-07-2007	18:27	0396904***	Monza	0:01:51
11-07-2007	09:42	068578***	Roma	0:00:14
11-07-2007	09:43	068578***	Roma	0:01:39
16-07-2007	15:27	01413D***	Asti	0:00:49
16-07-2007	17:54	0396904***	Monza	0:01:57
20-07-2007	11:08	0332824***	Varese	0:16:20
20-07-2007	12:17	031261***	Como	0:26:19
31-07-2007	22:14	045597***	Verona	0:00:17

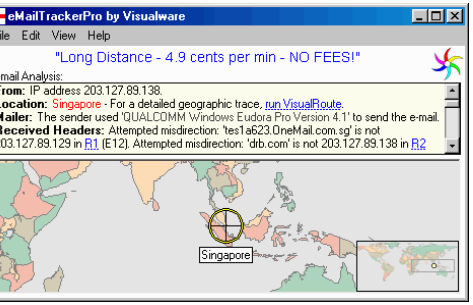




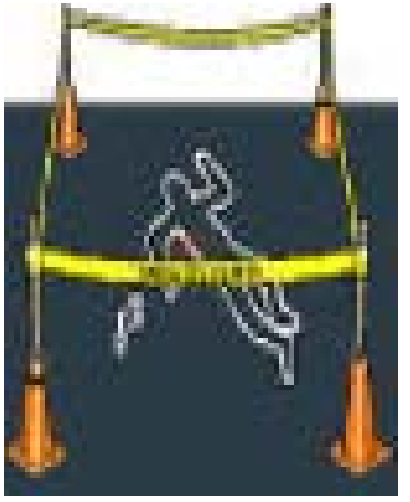


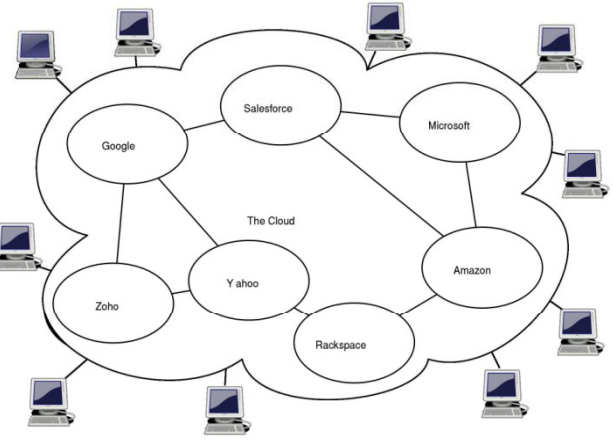
Nuovi scenari sulla Rete e……. sul Cloud……





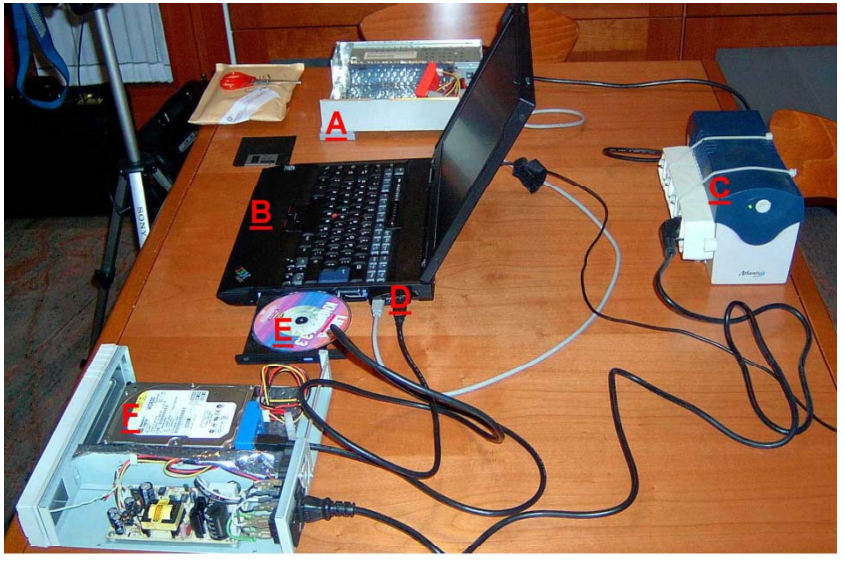
Scena del crimine (non solo) informatico

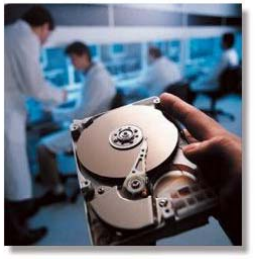




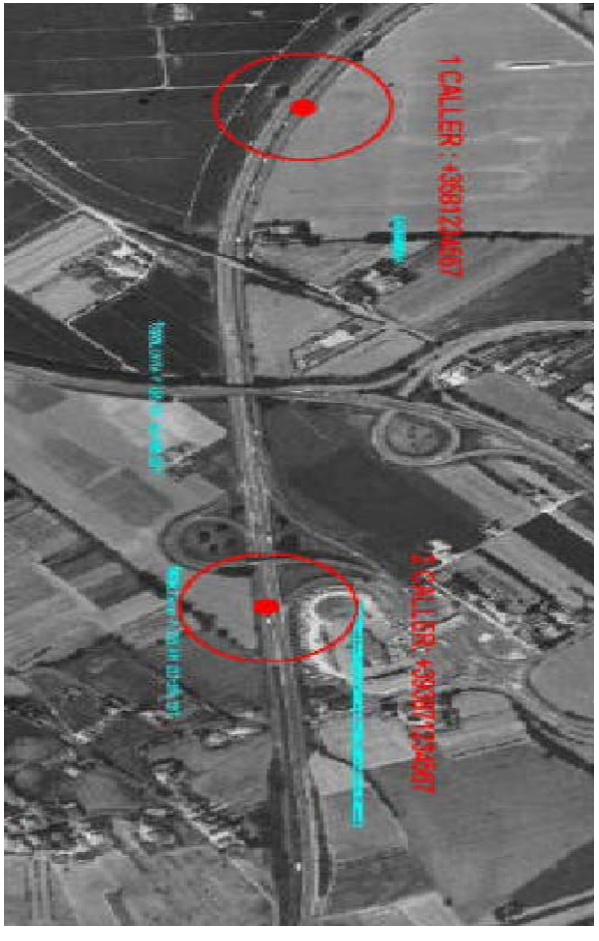
volatilità - modificabilità – alterabilità

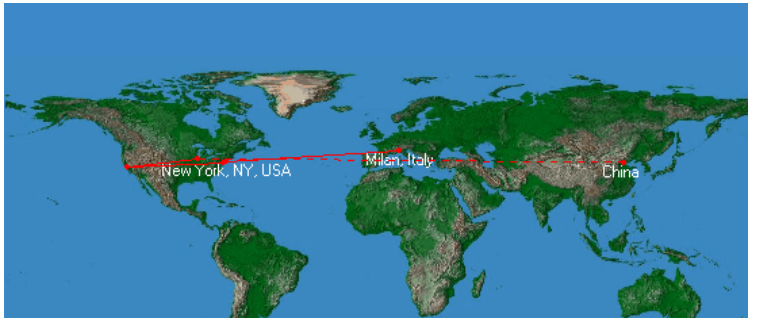
dell'elemento di prova digitale





Nuovi scenari = nuovi strumenti





Legge n. 48 del 2008

Ratifica della convenzione di Budapest 2001

Art. 244 c.p.p. - Casi e forme delle ispezioni

Art. 247 c.p.p. - Casi e forme delle perquisizioni

Art. 254-*bis* c.p.p. *(Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni)*

Art. 352 c.p.p. - Perquisizioni

Art. 354 c.p.p. - accertamenti urgenti

COOPERAZIONE INTERNAZIONALE FUORI ROGATORIA art. 33 art.35

adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione

" …adozione di misure tecniche dirette ad assicurare la conservazione dei dati originali ed ad impedirne l'alterazione…." (art. 244 cpp)

" acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità"

" ….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….." (art. 354 c.p.p)

Impedire l’alterazione

Immodificabilità

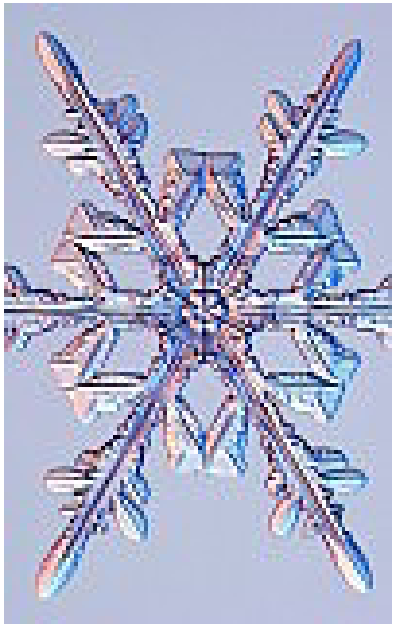
Integrità

Volatilità del dato

L’hash..

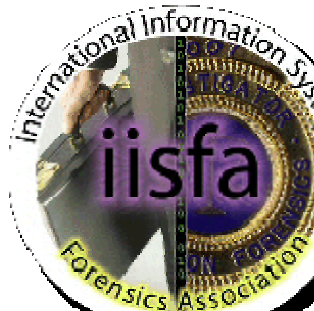
Cos’è l’hashing ? O meglio, l’algoritmo di hash ?

a5031419c40c75831c0521e27e6fa728

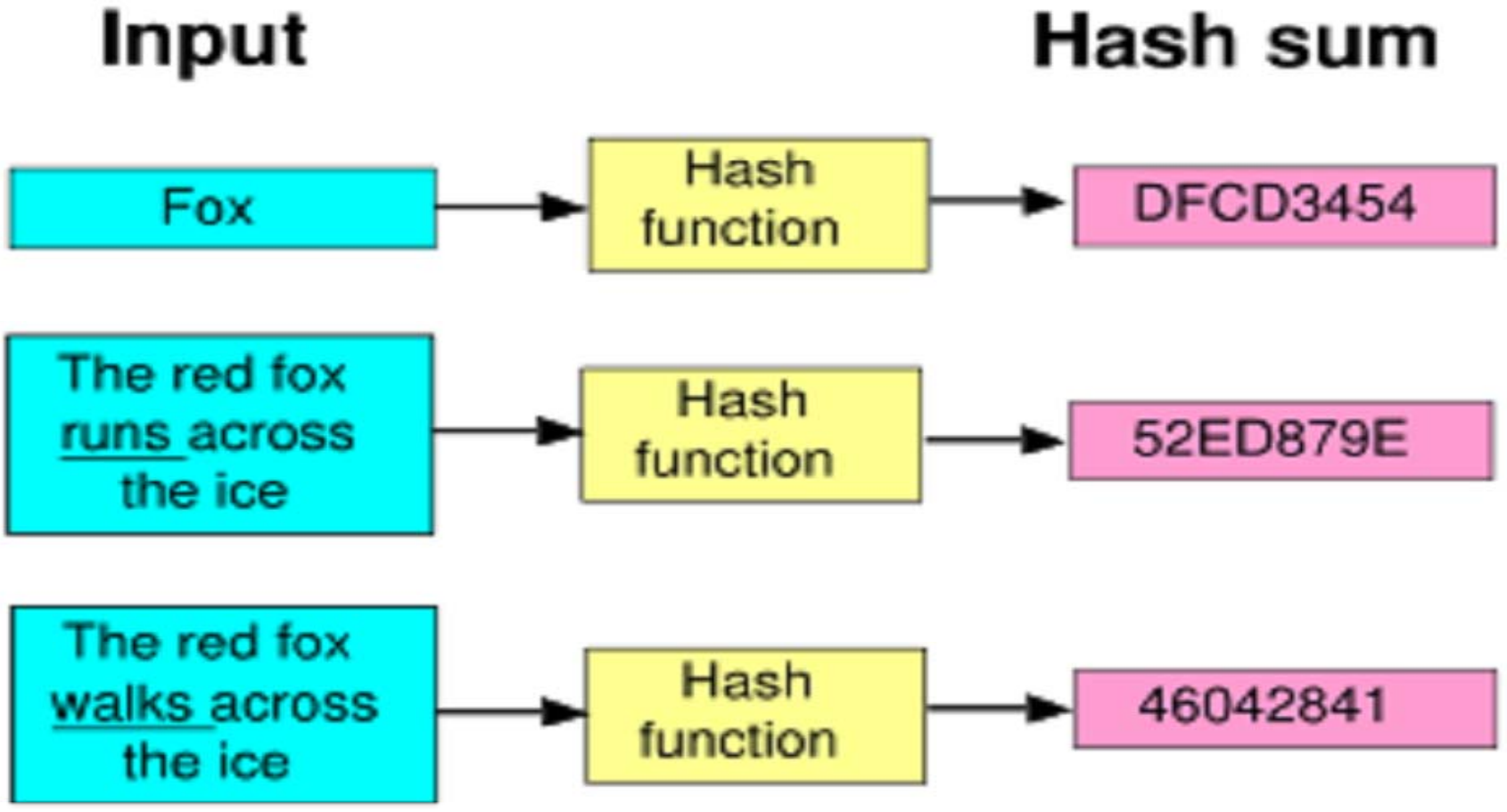


Non esistono 2 uguali

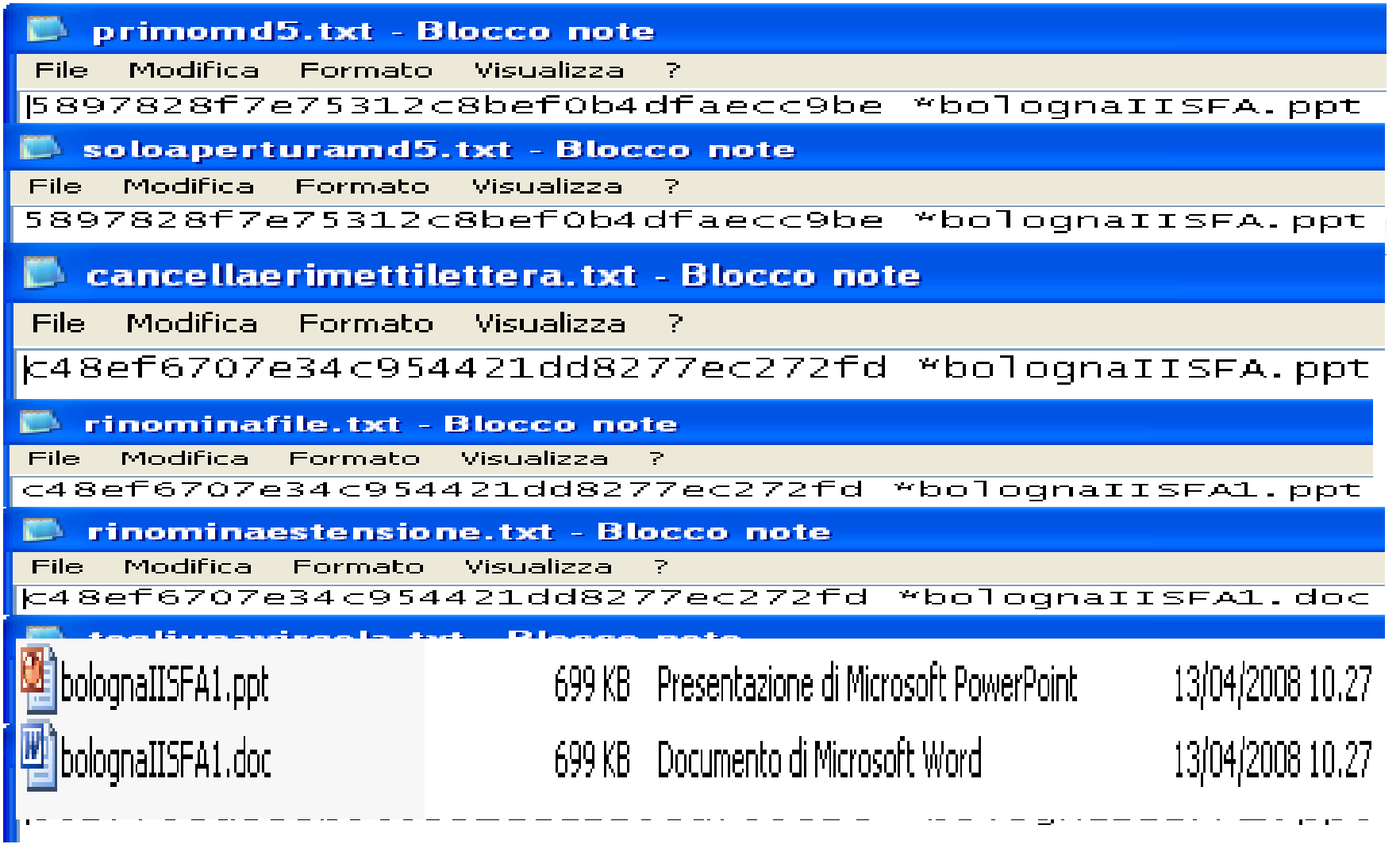
*Nel linguaggio scientifico, l'**hash** è una funzione univoca operante in un solo senso (ossia, che non può essere invertita), atta alla trasformazione di un testo di lunghezza arbitraria in una stringa di lunghezza fissa, relativamente limitata. Tale stringa rappresenta una sorta di "impronta digitale" del testo in chiaro, e viene detta valore di hash, checksum crittografico o message digest.*



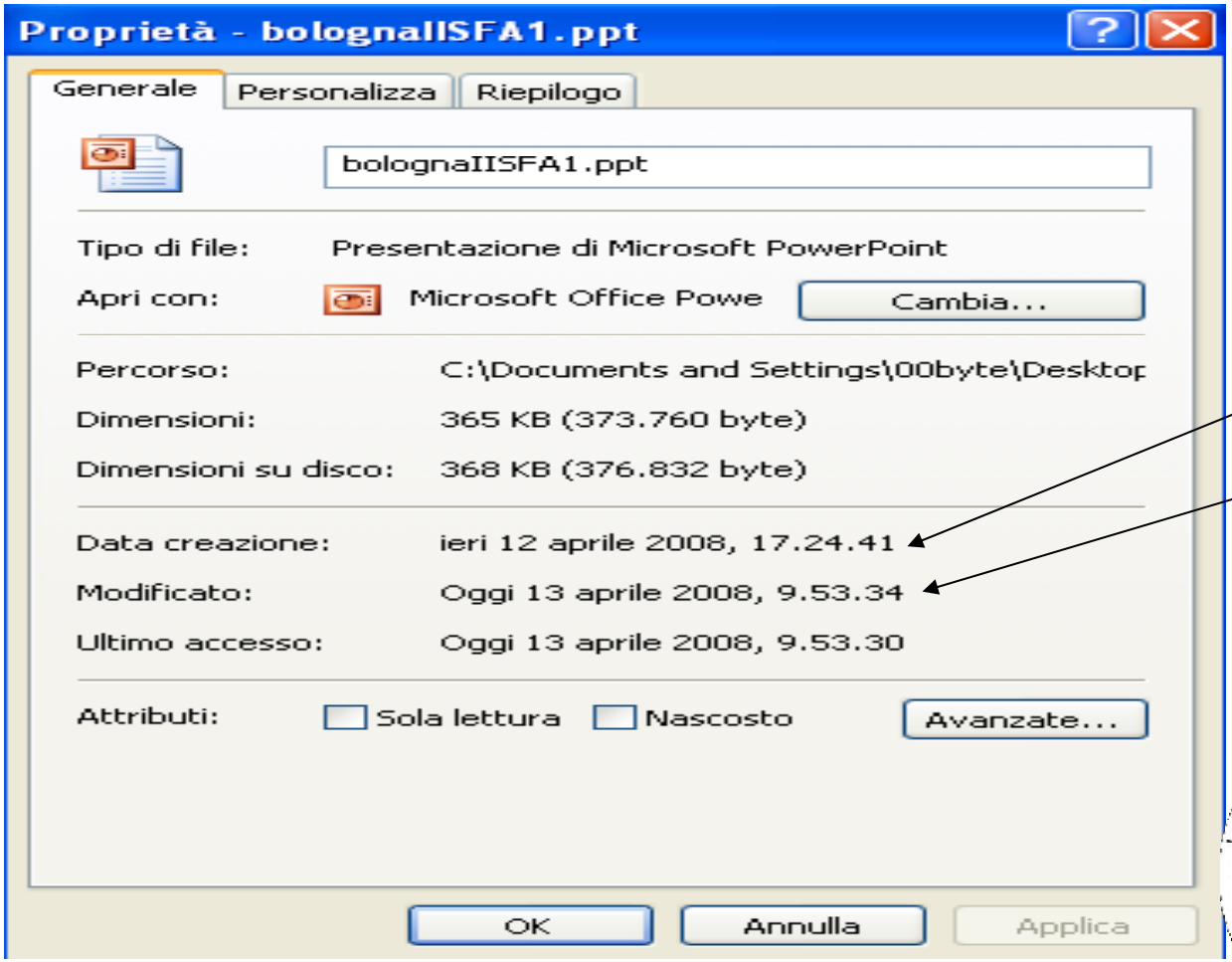
Fonte: Wikipedia



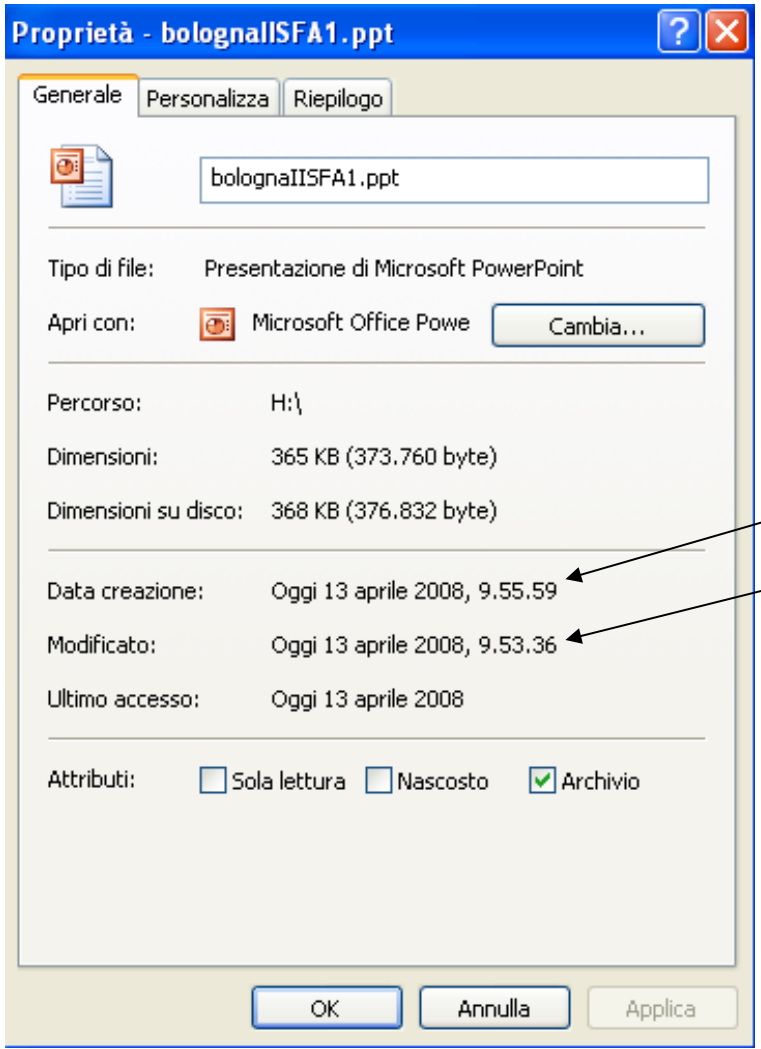
Ecco i risultati



Prima del trascinamento



Dopo il trascinamento sul pen drive



Attenzione quindi

NON sempre

se il file viene

aperto, duplicato, salvato

Esso **è alterato nel contenuto**

Bisogna vedere caso per caso e soprattutto cosa stiamo cercando di dimostrare

Le prime pronunce della Cassazione

- **Cass.** Sez. Lavoro n. 2912/04 del 18.2.2004
- **Cass**. 12 dicembre 2008-13 marzo 2009 n. 11135, **B.**
- ***Cass.*** *n.* 11503 del 16/03/2009, **Dell'Av.**
- ***Cass.*** *n.* 11863 *del* 18/03/2009, **Ammu.**
- ***Cass.*** *n.* 14511 *del*02/04/2009. **Stab.**
- **Cass.** n. 2388, 19.1.2010, **Pirr.**
- ***Cass.*** *n.* 16556 *del* 29/04/2010 sul **cd captatore informatico**

su una pagina web la Cassazione dice:

"le informazioni tratte da una rete telematica sono per natura volatili e suscettibili di continua trasformazione e, a prescindere dalla ritualità della produzione, **va esclusa la qualità di documento in una copia su supporto cartaceo** che non risulti essere stata raccolta con garanzie di rispondenza all'originale e di riferibilità ad un ben individuato momento"

(**Cass. Sez. Lavoro n. 2912/04 del 18.2.2004**)

Acquisizione di un file su server di una Banca

Cass. 12 dicembre 2008-13 marzo 2009 n. 11135, B.

L'esperibilità delle procedure di hashing, ossia delle tecniche volte a verificare l'integrità e la conformità all'originale del dato informatico sequestrato e conservato in copia su un apposito supporto (nella specie Cd-Rom), è una questione di merito, potendosi in sede di legittimità **esclusivamente delibare se gli accorgimenti adottati dalla polizia giudiziaria delegata siano o meno idonei in astratto a tutelare le finalità indicate dal legislatore** negli articoli 247, comma 1-bis, e 354, comma 2, del C.p.p. per come modificati dalla legge 48/2008 di ratifica della Convenzione del Consiglio d'Europa sul cybercrime.

La Cassazione e la lettura “post mortem” del PC. Ripetibiltà.

***Cass. Sez.* 1, *del* 25/02/2009, *n.*11503 (dep.16/03/2009)**Dell'Avers**.**

Ipotesi di analisi/lettura del PC in assenza dei difensori in assenza di una accertata alterazione del disco informatico, tra l’altro appartenente ad un terzo soggetto.

Non dà luogo ad accertamento tecnico irripetibile la lettura dell' "hard disk" di un computer sequestrato, che è attività di polizia giudiziaria volta, anche con urgenza, all'assicurazione delle fonti di prova. E’ quindi **ripetibile**.

STUDIO LEGALE
ATERNO

La Cassazione e l'estrazione dei dati da parte di personale esperto

Cass. Sez. 1, del 26/02/2009 n. 11863, (dep. 18/03/2009) Amm.

L'estrazione dei dati contenuti in un supporto informatico, se eseguita da personale esperto in grado di evitare la perdita dei medesimi dati, costituisce un accertamento tecnico ripetibile.

STUDIO LEGALE
ATERNO

La Cassazione e la ripetibilità degli atti prelevati su PC

*Ca***ss.** *Sez.* 1, *n.* 14511 *del* 05/03/2009 Cc. (dep. 02/04/2009)
S. Av.

- Non rientra nel novero degli atti irripetibili l'attività di estrazione di copia di "file" da un computer oggetto di sequestro, dal momento che essa **non comporta alcuna attività di carattere valutativo su base tecnico-scientifica**, né determina alcuna alterazione dello stato delle cose, tale da recare pregiudizio alla genuinità del contributo conoscitivo nella prospettiva dibattimentale, essendo sempre comunque assicurata la riproducibilità d'informazioni identiche a quelle contenute nell'originale

3. Ciò posto, è da escludere che l'attività di estrazione di copia di "file" da un computer costituisca un atto irripetibile (nel senso in precedenza indicato), atteso che non comporta alcuna attività di carattere valutativo su base tecnico-scientifica né determina alcuna alterazione dello stato delle cose, tale da recare pregiudizio alla genuinità del contributo conoscitivo nella prospettiva dibattimentale, essendo sempre comunque assicurata la riproducibilità di informazioni identiche a quelle contenute nell'originale.

Lo stesso ricorrente, del resto, non ha in concreto allegato alcuna forma di distruzione o alterazione dei dati acquisiti, tale da confortare il suo assunto, ma si è limitato a prospettare ipoteticamente alcune situazioni potenziali che esulano dalla fattispecie sottoposta all'esame della Corte.

STUDIO LEGALE
ATERNO

Le prime pronunce della Cassazione

- **Cass**. 12 dicembre 2008-13 marzo 2009 n. 11135, **B.**
- ***Cass.*** *n.* 11503 del 16/03/2009, **Dell'Av.**
- ***Cass.*** *n.* 11863 *del* 18/03/2009, **Ammu.**
- ***Cass.*** *n.* 14511 *del*02/04/2009. **Stab.**
- **Cass.** n. 2388, 19.1.2010, **Pirr.**
- ***Cass.*** *n.* 16556 *del* 29/04/2010 sul **cd captatore informatico**

Un paio di Tecniche investigative informatiche

1. **L'Appostamento informatico – cass. 7giugno 2013(conferma Tribunale di Milano – 22.2.2010 – n. 1877)**

   caso *www.svanityfair.com*

   (non si riusciva a individuare il soggetto responsabile delle pubblicazioni diffamatorie. Il provider era all'estero)

   DECRETO DEL PUBBLICO MINISTERO

   "*idonea attività di technointelligence e […] indagini oggettivamente atipiche di polizia giudiziaria*":

- *- tracciamento del sito internet www.svanityfair.com e di tutte le caselle di posta elettronica riconducibili allo stesso, anche mediante l'utilizzo di azioni atipiche di invio anonimo di messaggi di posta basate su innovative tecniche di social engineering che si riterranno opportune;*

2. Geolocalizzazione - GPs e non .....

Sez. 6, Sentenza n. 15396 del 11/12/2007 Ud. (dep. 11/04/2008) Rv. 239635
Presidente: Lattanzi G. Estensore: Fidelbo G. Relatore: Fidelbo G. Imputato: Sitzia e altri. P.M. Ciani G. (Conf.)

La localizzazione mediante il sistema di rilevamento satellitare (cosiddetta G.P.S.) degli spostamenti di una persona nei cui confronti siano in corso indagini costituisce una forma di pedinamento non assimilabile all'attività di intercettazione di conversazioni o comunicazioni, per la quale non è necessaria alcuna autorizzazione preventiva da parte del giudice, dovendosi escludere l'applicabilità delle disposizioni di cui agli artt. 266 ss. c.p.p. -

(Fattispecie relativa al pedinamento satellitare dell'autovettura di un indagato).

Sez. 4, Sentenza n. 3017 del 28/11/2007 Cc. (dep. 21/01/2008) Rv. 238679
Presidente: Campanato G. Estensore: Bernardi S. Relatore: Bernardi S. Imputato: Bresin. P.M. Iannelli M. (Conf.)

Il provvedimento con cui il PM dispone l'installazione di un sistema di localizzazione dei veicoli (G.P.S.) non necessita della preventiva autorizzazione del G.I.P., in quanto è diretto a disporre, mediante l'ausilio di impianti tecnici, un pedinamento e non una intercettazione.

Sez. 4, Sentenza n. 8871 del 29/01/2007 Cc. (dep. 01/03/2007) Rv. 236112
Presidente: Marzano F. Estensore: Piccialli P. Relatore: Piccialli P. Imputato: Navarro Mongort. P.M. Baglione T. (Conf.)

L'attività di indagine, volta a seguire gli spostamenti di un soggetto localizzato attraverso il sistema di rilevamento satellitare, costituisce una forma di pedinamento e non di intercettazione, con la conseguenza che ad essa non si applicano le disposizioni di cui agli artt. 266 e ss. c.p.p. -

---

Sez. 5, Sentenza n. 24715 del 07/05/2004 Ud. (dep. 31/05/2004) Rv. 228731
Presidente: Marrone F. Estensore: Ferrua G. Imputato: Massa ed altro. P.M. Viglietta G. (Parz. Diff.)

La localizzazione mediante sistema satellitare (cosiddetto G.P.S.) degli spostamenti di una persona nei cui confronti siano in corso indagini si traduce in una sorta di pedinamento e non è, pertanto, assimilabile all'attività di intercettazione di conversazioni e comunicazioni; conseguentemente, essa non necessita di alcuna autorizzazione preventiva da parte del giudice per le indagini preliminari.

Sez. 5, Sentenza n. 16130 del 27/02/2002 Cc. (dep. 02/05/2002) Rv. 221918
Presidente: Marrone F. Estensore: Fumo M. Imputato: Bresciani ed altri. P.M. Galati G. (Conf.)

La localizzazione tramite sistema satellitare (così detto G.P.S.) degli spostamenti di un soggetto nei confronti del quale sono in corso indagini, **benché comporti un controllo non poco invasivo a carico del soggetto medesimo, non è in alcun modo assimilabile alla attività di intercettazione, prevista dagli artt. 266 e seguenti c.p.p.** e non necessita quindi di alcuna autorizzazione preventiva da parte del giudice per le indagini preliminari.

STUDIO LEGALE
ATERNO

Legge n. 43 del 2015

- Art. 4 bis - deroga all'art. 132 codice privacy

- ***Art. 234-bis. - (Acquisizione di documenti e dati informatici). - 1. E' sempre consentita l'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, previo consenso, in quest'ultimo caso, del legittimo titolare».***

Captatore informatico e remote forensics

La Cassazione sulla **captazione occulta** di dati da remoto (il cd Trojan di Stato)

- *Sez.* 5, ***Sentenza*** *n.* 16556 *del* 14/10/2009 Ud. (dep. 29/04/2010)

- **È legittimo il decreto del pubblico ministero di acquisizione in copia**, attraverso l'installazione di un captatore informatico, della documentazione informatica memorizzata nel "personal computer" in uso all'imputato e installato **presso un ufficio pubblico**, qualora il provvedimento abbia riguardato l'estrapolazione di dati, non aventi ad oggetto un flusso di comunicazioni, già formati e contenuti nella memoria del "personal computer" o che in futuro sarebbero stati memorizzati. (Nel caso di specie, l'attività autorizzata dal P.M., consistente nel prelevare e copiare documenti memorizzati sull'"hard disk" del computer in uso all'imputato, aveva avuto ad oggetto non un "flusso di comunicazioni", richiedente un dialogo con altri soggetti, ma "una relazione operativa tra microprocessore e video del sistema elettronico", ossia "un flusso unidirezionale di dati" confinati all'interno dei circuiti del computer; la S.C. ha ritenuto corretta **la qualificazione** dell'attività di captazione in questione quale **prova atipica**, sottratta alla disciplina prescritta dagli artt. 266 ss. cod. proc. pen.).

Caratteristiche più o meno tipiche del captatore informatico/trojan

- Entra nel sistema “target” e prende il completo controllo…..(anche della webcam) ;
- È in grado di attivare il microfono del sistema e ascolta come un’ambientale;
- È programmato per sfuggire agli antivirus;
- Acquisisce e recapita on line, ad intervalli di tempo, all’investigatore TUTTO il contenuto del PC (ogni tipo di file, log di navigazione web, posta elettronica, foto, screen shot schermo, screen shot dei siti web visitati);
- Si autodistrugge con un comando…..pulendo le sue tracce ed è difficilissimo capire se e quando è stato istallato;
- Ah dimenticavo…….
- ……può “uplodare” qualsiasi tipo di file salvandolo sul pc “vittima”……
- N.B. : I PM e la PG non lo faranno mai, ma loro hanno il controllo della situazione ?

- **Prova atipica ?? …ex art. 189 c.p.p. ?**

- **Siamo sicuri che non ci sia anche una intercettazione di un flusso di comunicazioni ? E quindi sia necessario il GIP ?**

- **Siamo proprio sicuri che non sia necessario il GIP anche <u>per tutto ciò che non è</u> intercettazione ambientale o telefonica ?**

Altre criticità del trojan di stato

- Il trojan (di Stato) altera il computer “target” ergo è attività irripetibile ?
- Capta, monitorizza, registra anche comportamenti non comunicativi (Cass. SSUU 2006);
- Differenziare tra sistemi informatici “privati” da quelli “pubblici” (prob. del domicilio informatico);
- È un mezzo di ricerca atipico ovvero prova atipica effettiva e giustificata ? (se è possibile perquisizione e sequestro per acquisire tutto ciò….. ?);
- Problemi di competenza nel caso di sistemi all’estero ? Nel caso di Cloud computing su server all’estero ? Giurisprudenza sull’instradamento ?

Ma….chi effettua le operazioni di installazione, controllo e conservazione ?

“La legge del Capitano della nave di Panama”

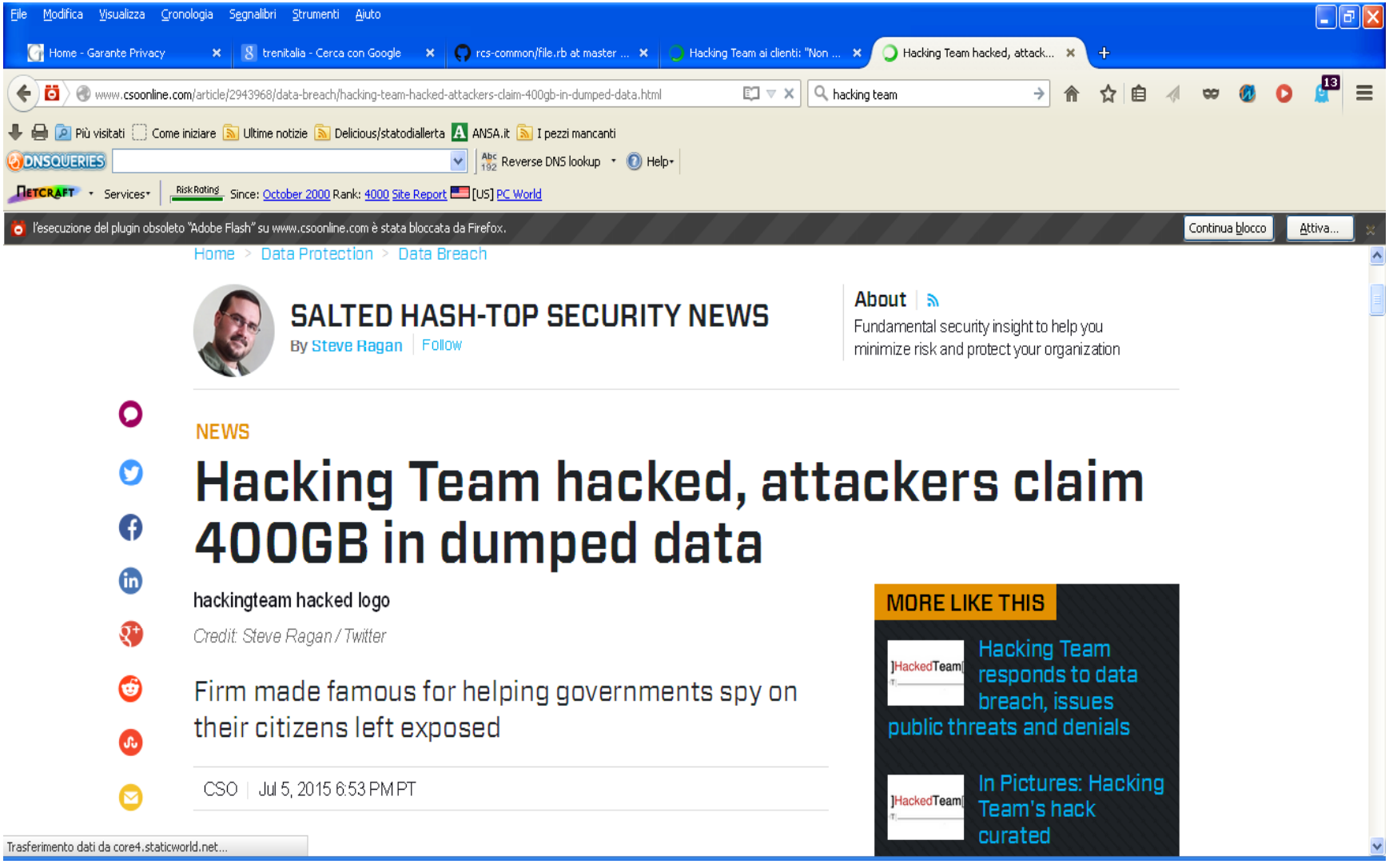
Si …..ma chi è il capitano in questa situazione ?

IL PM /PG o le società di intercettazione ?

Indubbi vantaggi investigativi……..MA…..alcune soluzioni possibili ?

- Decreto del GIP;
- solo casi di notifica ritardata sequestro e/o su indagini su piattaforme cloud;
- Verbale di PG con dettaglio delle operazioni eseguite ed eventuale nomina A.PG di consulenti e indicazione utilizzo);
- Certificazione del sw ;
- (eventuale) contemporanea autointercettazione telematica;
- Logging client “attaccante”, time stamp e firma digitale;
- (eventuale) deposito agli atti delle indagini le specifiche identificative e tecniche del software Trojan utilizzato;
- Successiva analisi del PC/supporto informatico sempre con il 360 c.p.p
- Forse non basta.....forse è il caso che intervenga IMMEDIATAMENTE il Legislatore…..

Il 5 luglio 2015……domenica pomeriggio



File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto

Home - Garante Privacy | trenitalia - Cerca con Google | rcs-common/file.rb at master ... | Hacking Team ai clienti: "Non ... | Hacking Team hacked, attack...

www.repubblica.it/tecnologia/sicurezza/2015/07/07/news/hacking_team_galileo-118552287/

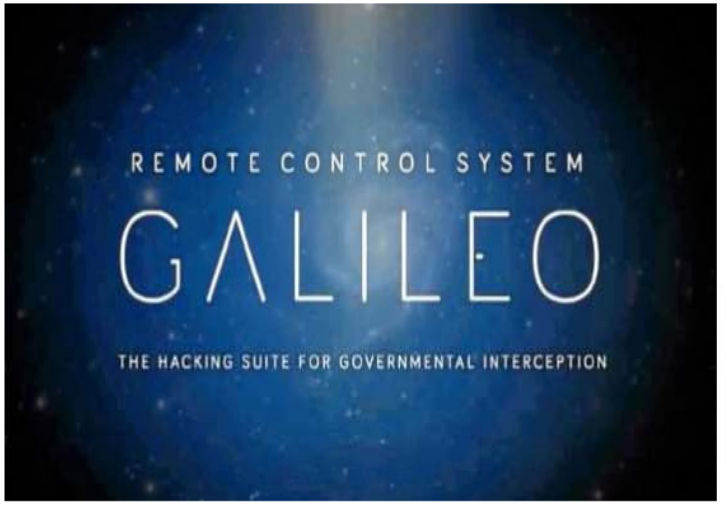
hacking team

Più visitati | Come iniziare | Ultime notizie | Delicious/statodiallerta | ANSA.it | I pezzi mancanti

DNSQUERIES | Reverse DNS lookup | Help

NETCRAFT | Services | Risk Rating | Since: August 1996 Rank: 124 Site Report [IT] Kataweb S.p.A

Hacking Team ai clienti: "Non usate il nostro programma-spia". E quello strano account Twitter...



Day after per la società milanese di sorveglianza informatica colpita da un fatale furto di dati e informazioni da 400GB dai quali si evincono e si confermano rapporti con governi e regimi dittatoriali, Sudan incluso. Un misterioso profilo sul social traccia un collegamento con un fatto analogo dello scorso anno contro la britannica Gamma

di SIMONE COSIMI

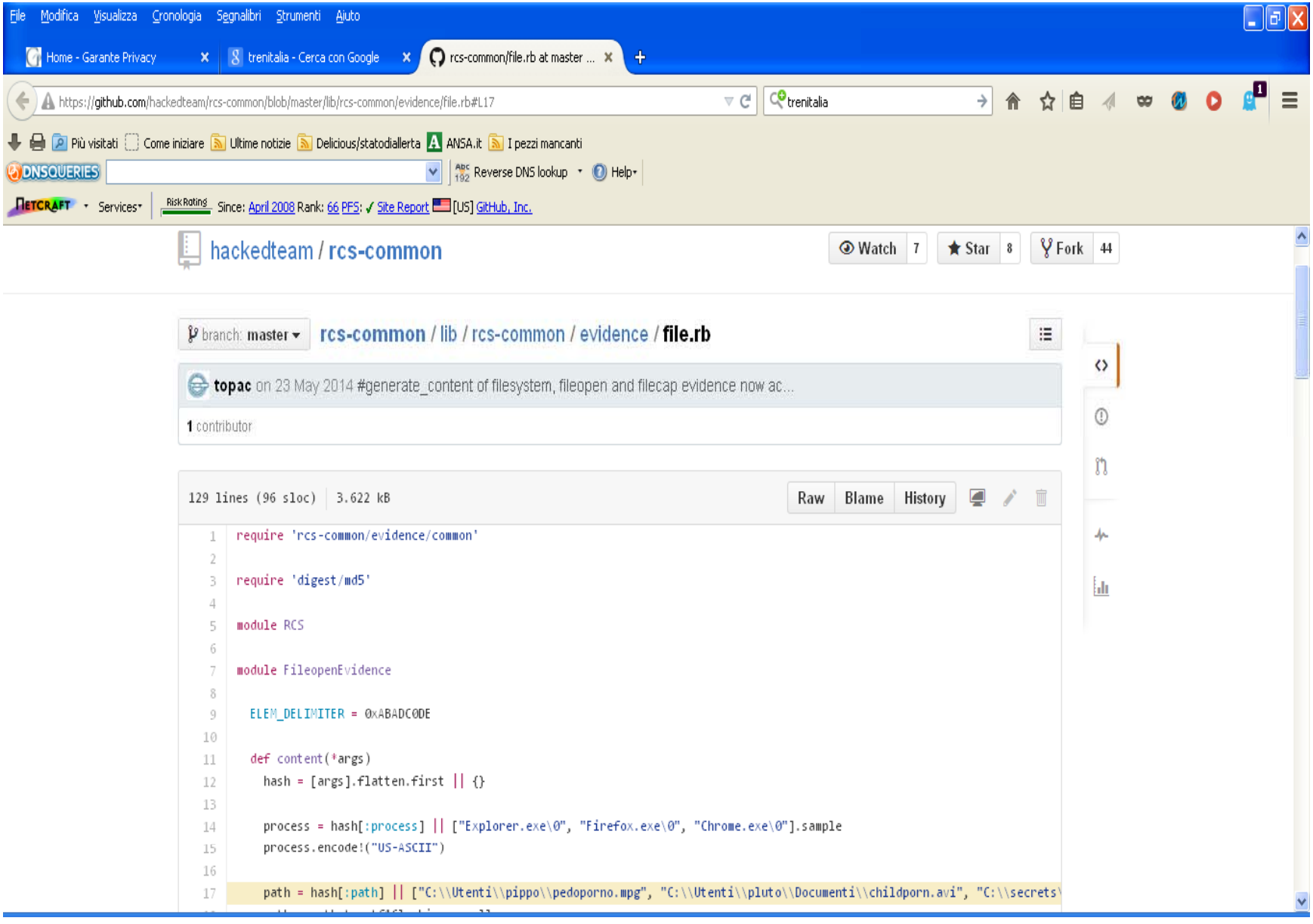
In attesa di scripts.kataweb.it...

https://github.com/hackedteam/rcs-common/blob/master/lib/rcs-common/evidence/file.rb#L17

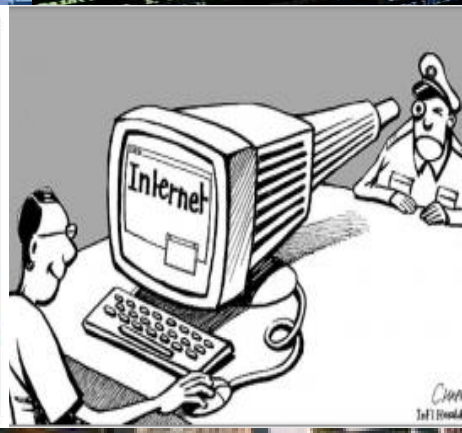
Nei sorgenti leakkati di HackingTeam pare siano presenti righe di codice che sembra servano per creare dei falsi files sui computer degli utenti dai nomi singolari... Tipo pedoporno.mpg, childporn.avi.....

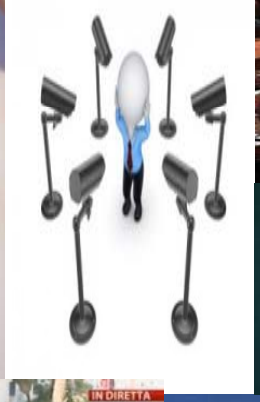
spero sia uno scherzo.....

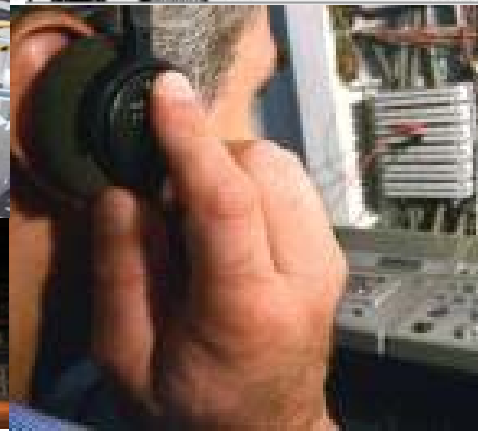
2015\rcs-common · GitHub.pdf



La SICUREZZA come DIRITTO DI LIBERTÀ e diritto alla RISERVATEZZA







Avv. Prof. Stefano Aterno

Camera Deputati – Roma 2 luglio 2015

La sicurezza da percepire come diritto di libertà, uno dei tanti diritti di libertà che possiamo evidenziare come altamente democratica in quanto contiene in sé i valori e i limiti propri di ciascun diritto di libertà, primo tra tutti quello di non poter negare sé stessa.

CARLO MOSCA

Grazie per l’attenzione

resto a vostra disposizione per eventuali domande

Avv. Stefano Aterno

www.studioaterno.it

s.aterno@studioaterno.it

STUDIO LEGALE ATERNO