Security ed Anti-Forensic
nell'ambito della rete aziendale

Alessio L.R. Pennasilico
mayhem@alba.st

Daniele Martini
cyrax@alba.st

Security Evangelist @ 

Board of Directors:

AIP, AIPSI/ISSA, CLUSIT, Italian Linux Society, LUGVR, OPSI, Metro Olografix, OpenBeer, Sikurezza.org

CrISTAL, Hacker's Profiling Project, Recursiva.org

$ whois Cyrax

Responsabile team Networking @

OpenSource Enthusiast - Command Line fanatic

Network Addicted

Anti-Forensic

Tecniche utilizzate per nascondere od occultare i dati, se non addirittura a prevenire eventuali indagini su dati elaborati da un calcolatore

Cerca di modificare le informazioni normalmente analizzate dai programmi di forensic

Buona o Cattiva?

Buona o Cattiva?

Anti-Forensic o Pro-Privacy?

Tecniche Anti-Forensic

Alessio L.R. Pennasilico - Daniele Martini

Tecniche

Artifact wiping

Data Hiding

Trail obfuscation

Attacks against CF

http://en.wikipedia.org/wiki/Anti-computer_forensics

Artifact Wiping

Alessio L.R. Pennasilico - Daniele Martini

Cancellazione

Indice	Dato	Dato
Dato	Dato	Dato
Dato		

Secure Deletion

Ripetute sovrascritture

Pulizia dello spazio libero

Quante riscritture?

USA DoD 5220-22.M 3 “pass”

Alcuni standard impongono 7 “pass”

Si ha notizia di recuperi dopo 14 “pass”

Alcuni programmi usano default molto alti (shred 38)

Secure Deletion?

Secure Deletion?

Sovrascrivo singoli file o l'intero media?

Secure Deletion?

Sovrascrivo singoli file o l'intero media?

Scrivo dati ripetitivi o random data?

Secure Deletion?

Sovrascrivo singoli file o l'intero media?

Scrivo dati ripetitivi o random data?

… ed il journaling?

Secure Deletion?

Sovrascrivo singoli file o l'intero media?

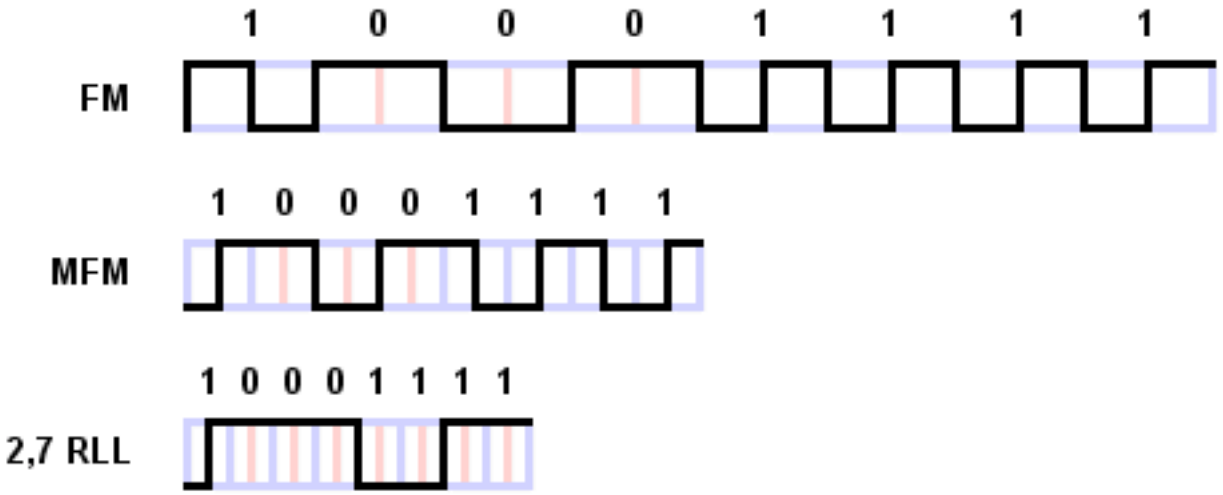
Scrivo dati ripetitivi o random data?

… ed il journaling?

… e lo slack space?

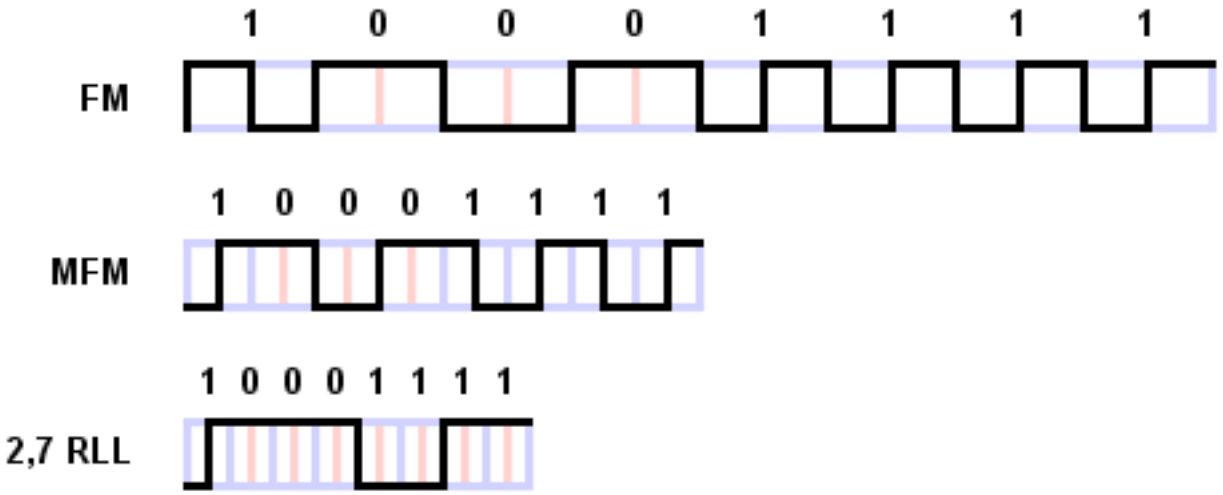
Magnetic Force Microscopy

E’ possibile recuperare il dato analizzando “analogicamente” la variazione del campo magnetico dovuto alle riscritture (cfr. Gutmann).



Magnetic Force Microscopy

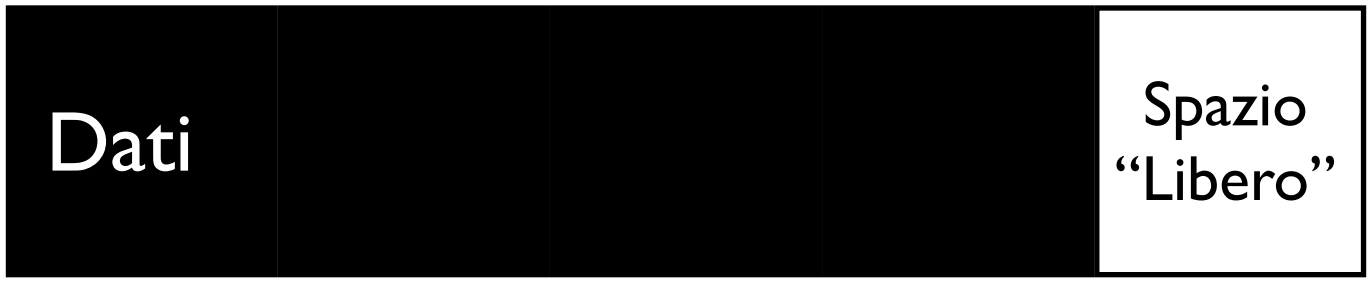
E’ possibile recuperare il dato analizzando “analogicamente” la variazione del campo magnetico dovuto alle riscritture (cfr. Gutmann).



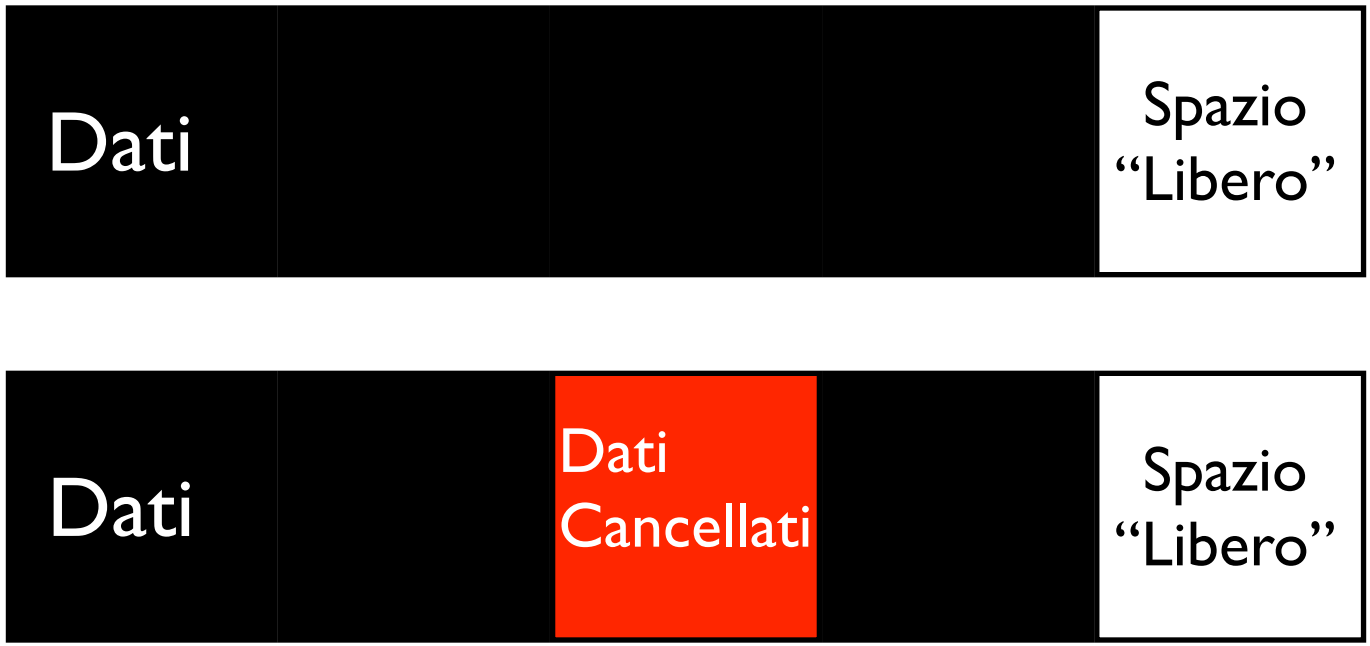
Leggenda urbana?

Slack Space

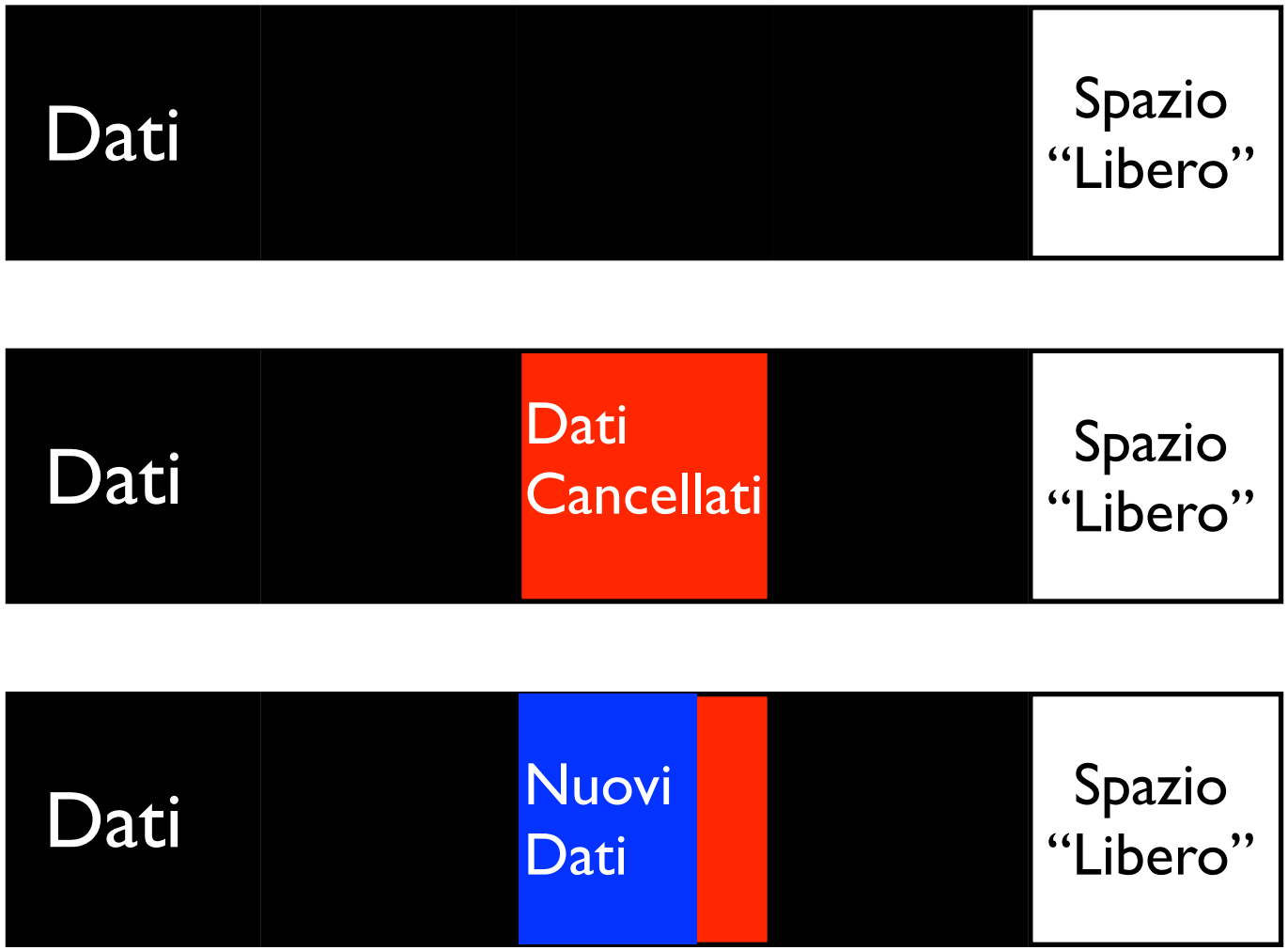
Slack Space



Slack Space



Slack Space


Dati
Spazio
“Libero”
Dati
Dati
Cancellati
Spazio
“Libero”
Dati
Nuovi
Dati
Spazio
“Libero”

Altre considerazioni...

Dischi in RAID

File system “non standard”

Settori danneggiati

Feature dei NAS

Feature delle VM

...

Solo per i cattivi?

Il Garante Italiano per la Privacy norma la distruzione dei dati con cancellazione sicura dei supporti dismessi in azienda

Degaussing

Applicazione di un intenso campo magnetico al fine di rendere il supporto illeggibile.

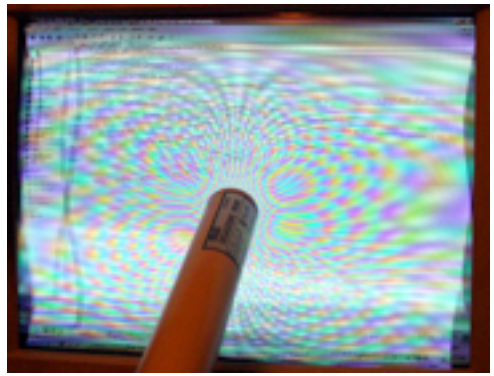
Spesso per sempre...

Degaussing

Applicazione di un intenso campo magnetico al fine di rendere il supporto illeggibile.

Spesso per sempre...

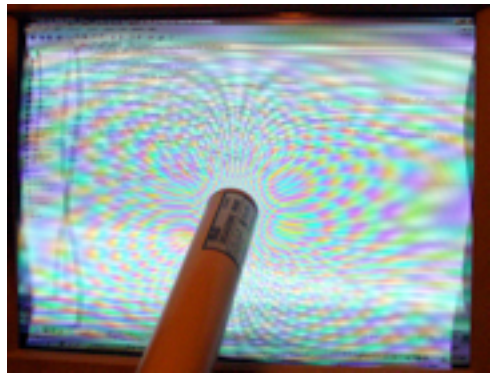
Degaussing



Applicazione di un intenso campo magnetico al fine di rendere il supporto illeggibile.

Spesso per sempre...

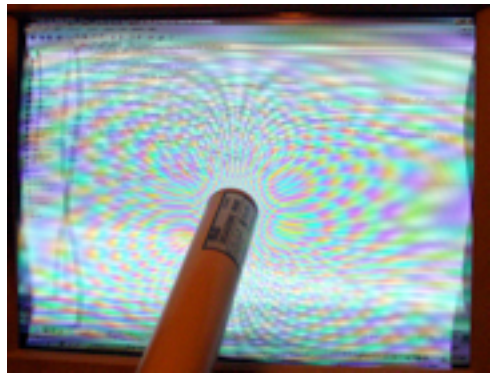
Degaussing



Applicazione di un intenso campo magnetico al fine di rendere il supporto illeggibile.

Spesso per sempre...

Degaussing



Applicazione di un intenso campo magnetico al fine di rendere il supporto illeggibile.

Spesso per sempre...

WORM

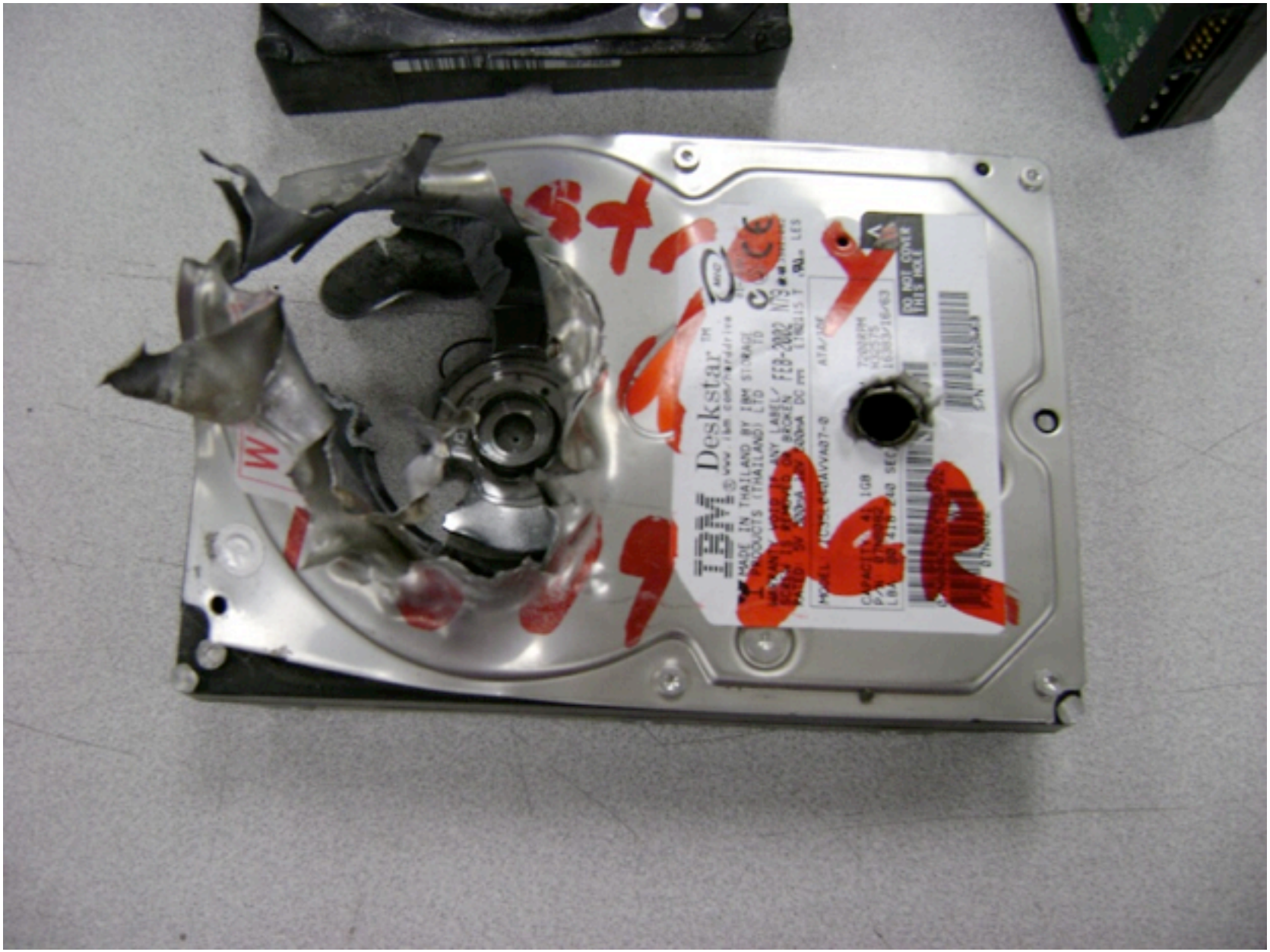
Write Once, Read Many

sono dischi ottici

Decine di degaussing

li lasciano intatti...

Distruzione fisica



Per definizione la RAM è “volatile”

Il suo contenuto viene perso in caso di reboot, spegnimento, etc etc

Cold Boot Attack

http://citp.princeton.edu/pub/coldboot.pdf

Data Hiding

Alessio L.R. Pennasilico - Daniele Martini

Data Hiding

Posso registrare le informazioni in luoghi inusuali

Una normale attività di data recovery potrebbe non accorgersi della presenza di tali informazioni...

Dove nascondere?

Bad Blocks

Slack Space

Journal

Spazi riservati del file system o del device

Encryption

Alessio L.R. Pennasilico - Daniele Martini

Encryption

Buona pratica per proteggere i propri dati da accessi indesiderati da parte di persone non autorizzate

FS Encryption

Criptare l'intero file system

Criptare il contenuto di alcune directory

previene l'analisi del file system

a chiunque sia sprovvisto della password

FS Encryption

Criptare l'intero file system

Criptare il contenuto di alcune directory

previene l'analisi del file system

a chiunque sia sprovvisto della password

Davvero?

Accorgimenti

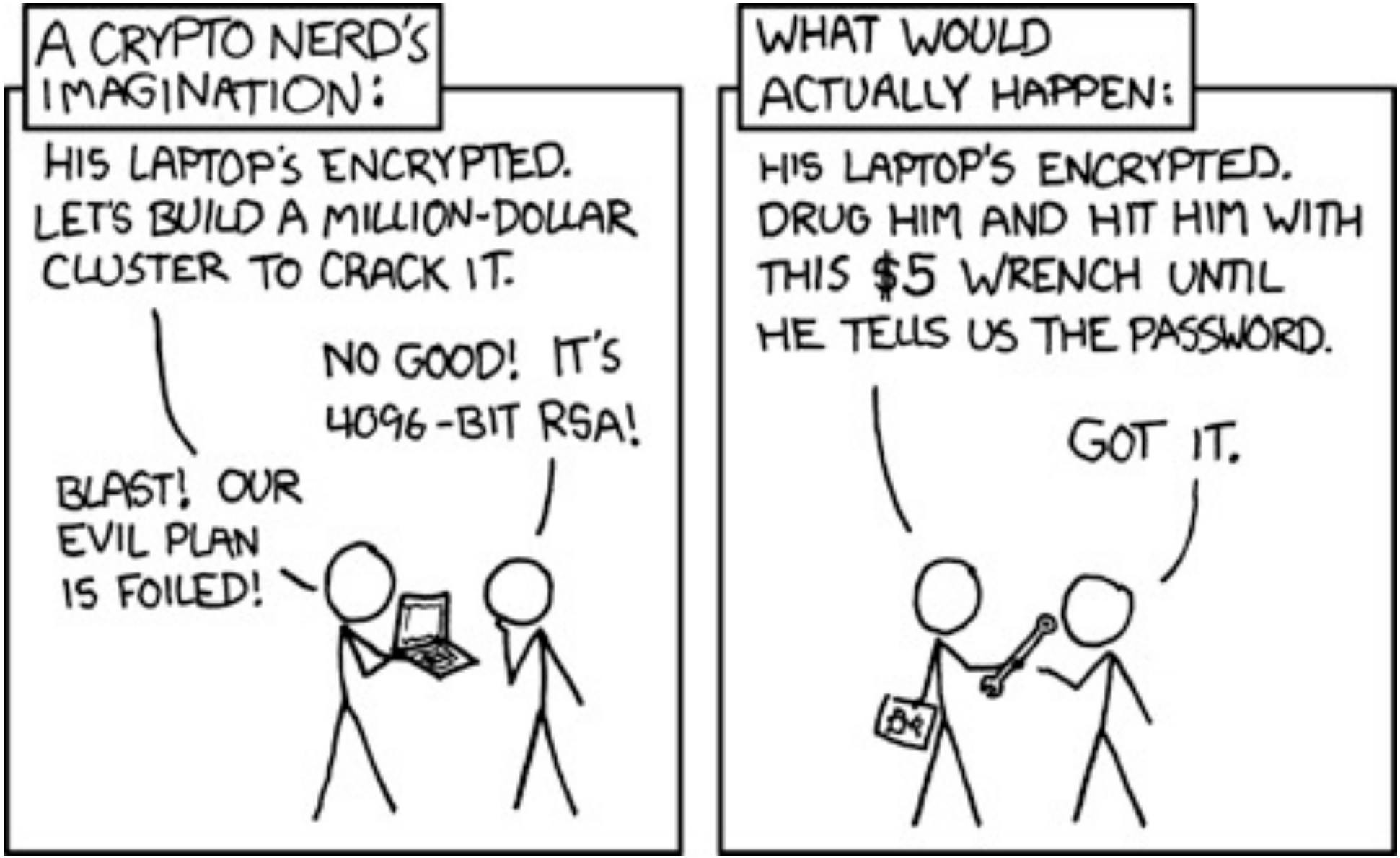
Sto criptando lo swap file?

Sto tenendo cache/log delle attività di accesso ai dati criptati?

cold boot attack

implementazioni buggate


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Esempio multipiattaforma e gratuito di gestione di file system cifrati, con diverse feature avanzate

Plausible Deniability

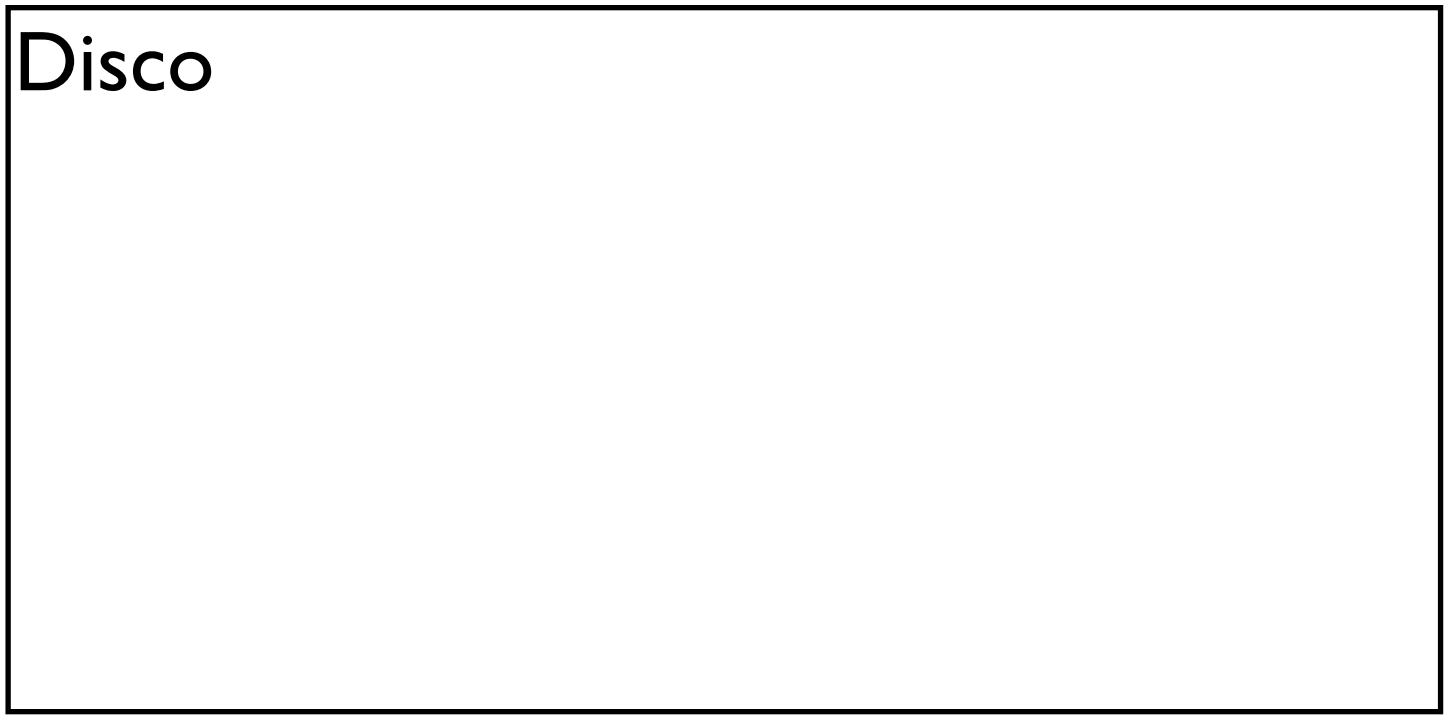
Dato un volume di TC

è impossibile dire

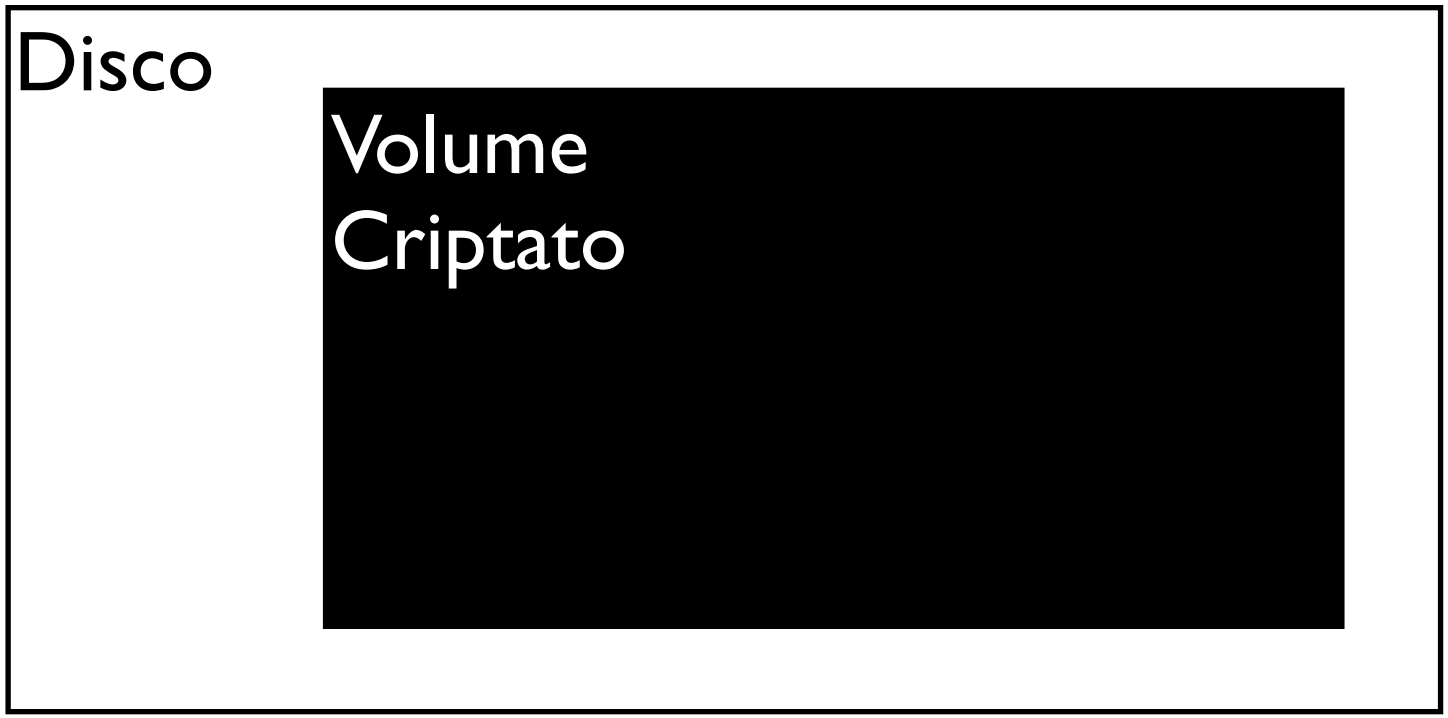
anche a fronte di una attenta analisi

se quel volume sia criptato o meno

Hidden Volumes

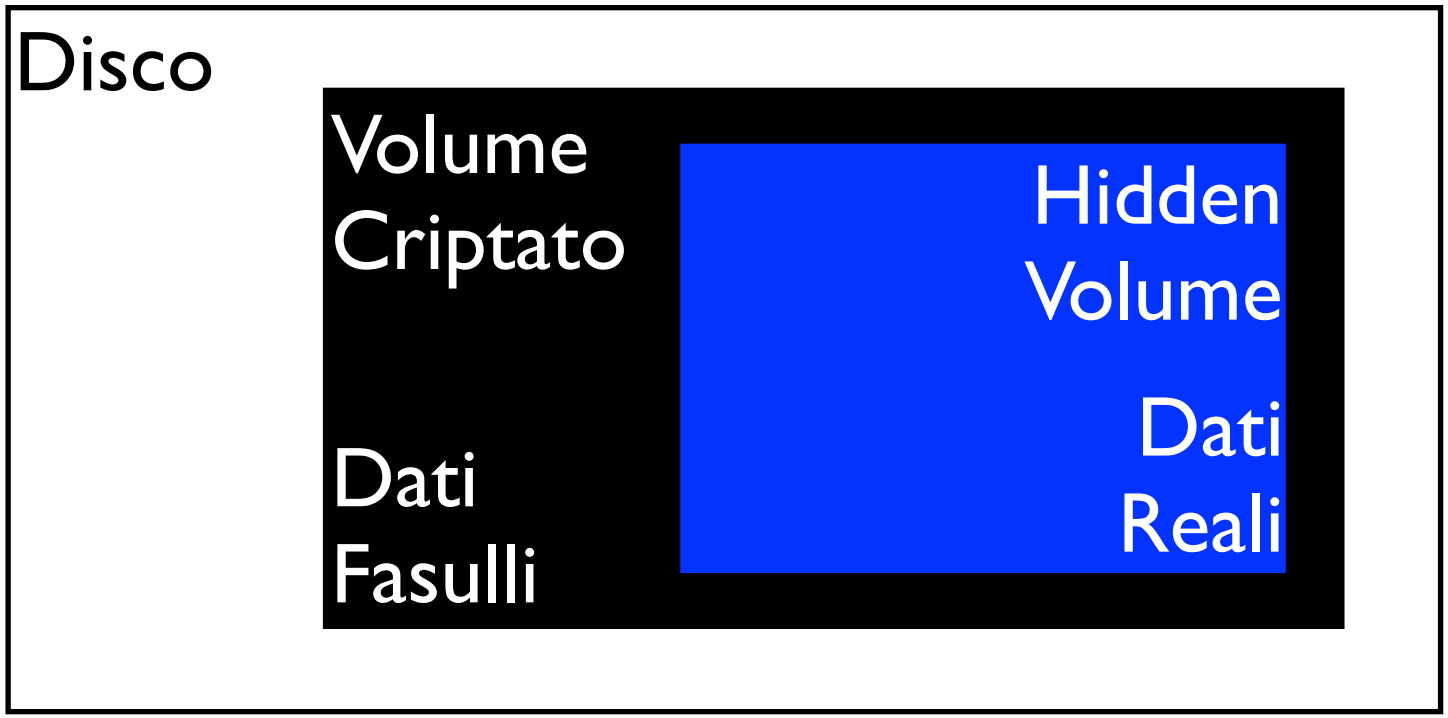


Hidden Volumes



Hidden Volumes

Hidden Volumes



Ho protetto i miei dati

in osservanza del D.Lgs. 196/03

non li volevo nascondere

"Password? che password?"

"Ah si, avevo fatto delle prove, ma non lo uso… non so nemmeno che password abbia"

"(In Italia) non sono obbligato a fornirvi la password di accesso ai miei dati"

"(In Italia) non sono obbligato a fornirvi la password di accesso ai miei dati"

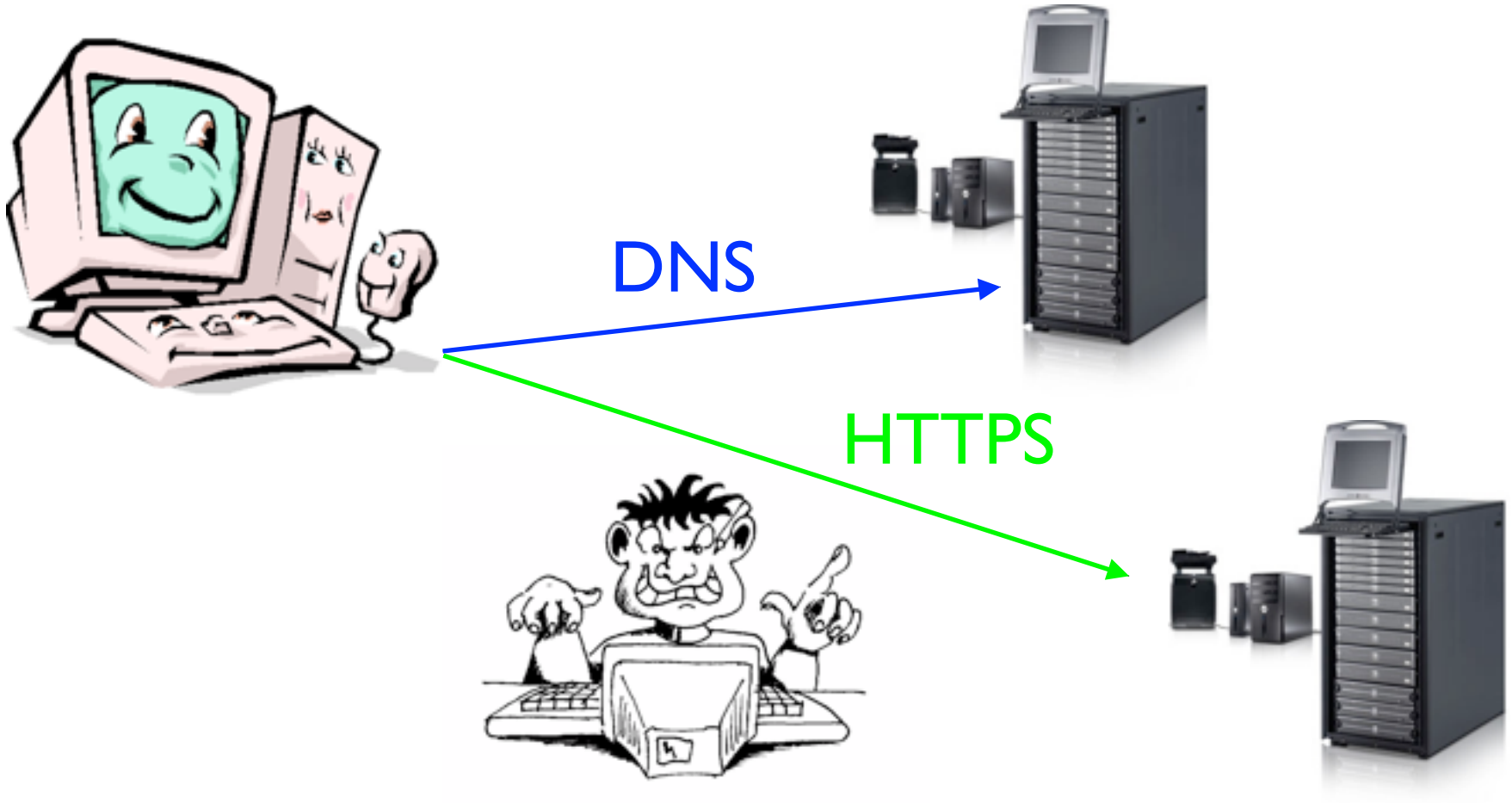
"non fornire la password sono 3 anni di reclusione, ma con quello che troverebbero dentro sono 5 … mi rifiuto di dare la password…"

NET Encryption

Criptare il traffico ne assicura la riservatezza, forse l'integrità e la non ripudiabilità

Criptare il traffico all'interno di un tunnel ne impedisce una analisi qualitativa

SSL



Steganografia

Il termine steganografia è composto dalle parole greche στεγανός (nascosto) e γράφειν (scrittura) e individua una tecnica risalente all'antica Grecia che si prefigge di nascondere la comunicazione tra due interlocutori

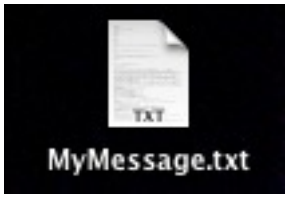
La "Steganographia" di Tritemio si proponeva di poter inviare messaggi tramite l'uso di linguaggi magici, sistemi di apprendimento accelerato e senza l'utilizzo di simboli o messaggeri

http://it.wikipedia.org/wiki/Steganografia

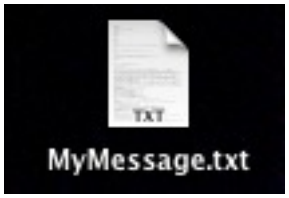
Steganalisi

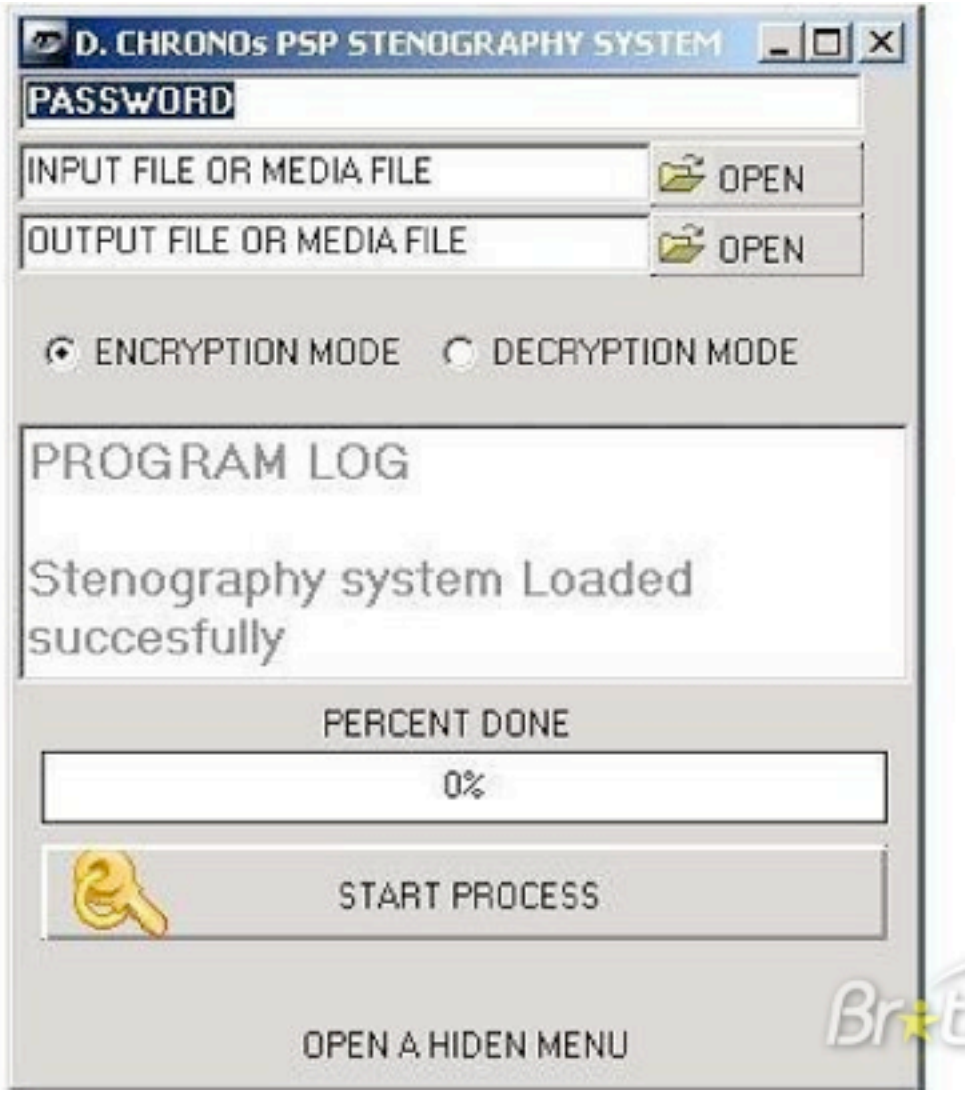
La steganografia si pone come obiettivo di mantenere nascosta l'esistenza di dati a chi non conosce la chiave atta ad estrarli, mentre per la crittografia è non rendere accessibili i dati nascosti a chi non conosce la chiave. La crittanalisi è l'attacco alla crittografia, che mira ad estrarre i dati cifrati senza chiave. L'obiettivo della steganalisi non è quindi quello di estrarre i dati nascosti, ma semplicemente di dimostrarne l'esistenza.

Esempio

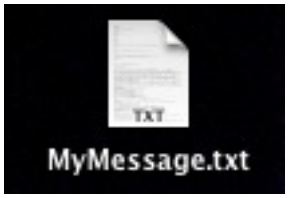


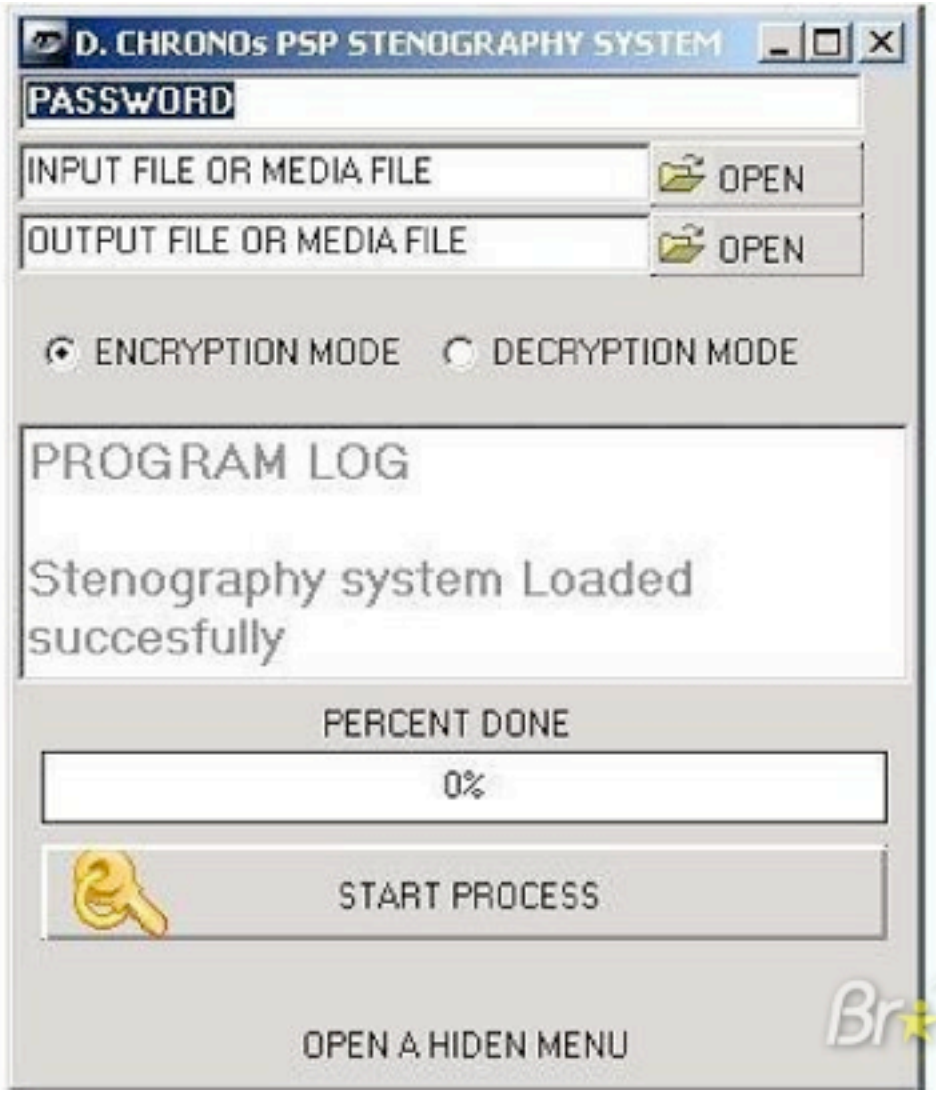
Esempio


TXT
MyMessage.txt


D. CHRONOs PSP STENOGRAPHY SYSTEM
PASSWORD
INPUT FILE OR MEDIA FILE
OPEN
OUTPUT FILE OR MEDIA FILE
OPEN
ENCRYPTION MODE
DECRYPTION MODE
PROGRAM LOG
Stenography system Loaded succesfully
PERCENT DONE
0%
START PROCESS
OPEN A HIDEN MENU
Brothersoft

Esempio


TXT
MyMessage.txt


D. CHRONOs PSP STENOGRAPHY SYSTEM
PASSWORD
INPUT FILE OR MEDIA FILE
OPEN
OUTPUT FILE OR MEDIA FILE
OPEN
ENCRYPTION MODE
DECRYPTION MODE
PROGRAM LOG
Stenography system Loaded succesfully
PERCENT DONE
0%
START PROCESS
OPEN A HIDEN MENU

La stessa tecnica si può utilizzare su "informazioni" diverse dalle immagini

Trail Obfuscation

Alessio L.R. Pennasilico - Daniele Martini

Rootkit

Programma che modifica i binari di sistema al fine di nascondere alcune informazioni

Ne esistono di molti tipi, atti a fornire accessi facilitati (ssh), nascondere file/processi/utenti (binutils), non tenere log (syslog), etc.

Metadati

Data creazione

Modifica

Accesso

Ultimo accesso

Metadati

Posso modificarli

sovrascriverli

evitare che vengano scritti

Dopo avere installato di proposito un po' di porcherie sul proprio PC:

"Non sono stato io! Il PC era infetto, sarà stato qualche hacker ad utilizzare la mia macchina per fare quello di cui mi accusate!"

Hash

Alcuni strumenti cercano sul disco immagini che verificano certi hash (vedi pedoporno)

Se modifico l'immagine (contenuto, exif, appendo dati, etc) l'hash sarà verificato?

Attacks against CF

Alessio L.R. Pennasilico - Daniele Martini

Forensic detection

Possono essere attivate protezioni che distruggono alcuni dati al verificarsi di alcune conseguenze

Forensic detection

Possono essere attivate protezioni che distruggono alcuni dati al verificarsi di alcune conseguenze

(non mi riferisco all'ingoiare chiavette USB…)

Come?

Utilizzo della procedura standard di spegnimento

Particolari procedure di avvio

Login con certi utenti

Accensione fuori rete

Accensione su una rete diversa

Accensione come VM

Esempio

COFEE - Tool Microsoft per gli investigatori

Decaf - Se un supporto USB con il tool presente viene inserito, *puf*, viene vanificata ogni analisi

Ho adottato una misura per proteggere i dati, o volevo evitare un controllo?

(cfr. la storia del grosso bottone rosso)

Limiti

Queste tecniche funzionano solo in caso di analisi "LIVE"

Conclusioni

Alessio L.R. Pennasilico - Daniele Martini

Anti-Forensic

Esistono molti strumenti per applicarla

Può essere utilizzata per proteggere i dati

Una non accurata implementazione la vanifica

Architetture non usuali complicano la vita dell'investigatore come alcune tecniche

Anti-Forensic vs Pro-Privacy

Security ed Anti-Forensic
nell’ambito della rete aziendale

Alessio L.R. Pennasilico
mayhem@alba.st

Daniele Martini
cyrax@alba.st