Cyber Security & Autodifesa Digitale

Ing. Selene Giupponi

Selene Giupponi:

- Ingegnere Informatico, specializzato in Computer Forensics & Digital Investigations.
- Membro della Commissione ICT dell'Ordine degli Ingegneri della Provincia di Latina.
- Segretario Generale e Socio IISFA (INFORMATION SYSTEM FORENSICS ASSOCIATION ITALIAN CHAPTER).
- CT per Procure della Repubblica e Forze dell'Ordine.
- Advisor European Courage Focus Group – Cyber Terrorism & CyberCrime – EOS Member. Board
- ITU ROSTER OF EXPERTS.
- HTCC HIGH TECH CRIME CONSORTIUM Member.
- Official Trainer NATO & U.S. NAVY.
- CIFI - Certified Information Forensics Investigator, SPEKTOR & UFED.
- ECSO (European Cyber Security Organization) – Founder Member.
- Cyber Security Advisor, Senior Digital Forensics Consultant & Cyber Intelligence Investigations
- Founder Security Brokers Scpa

- Le informazioni contenute in questa presentazione sono solo a scopo formativo e informativo, l'autore (Ing. Selene Giupponi) non è responsabile se il contenuto viene utilizzato in modo errato per danneggiare persone o cose.

- L'autore (Ing. Selene Giupponi) detiene la proprietà intellettuale di questa presentazione e dei suoi contenuti, la cui riproduzione è severamente vietata e punita ai sensi di legge.

- Il contenuto di questa presentazione può essere utilizzato o riprodotto, purché l'autore (Ing. Selene Giupponi) ne venga informato, ne dia autorizzazione e venga opportunamente citato e ne acconsenta la riproduzione.

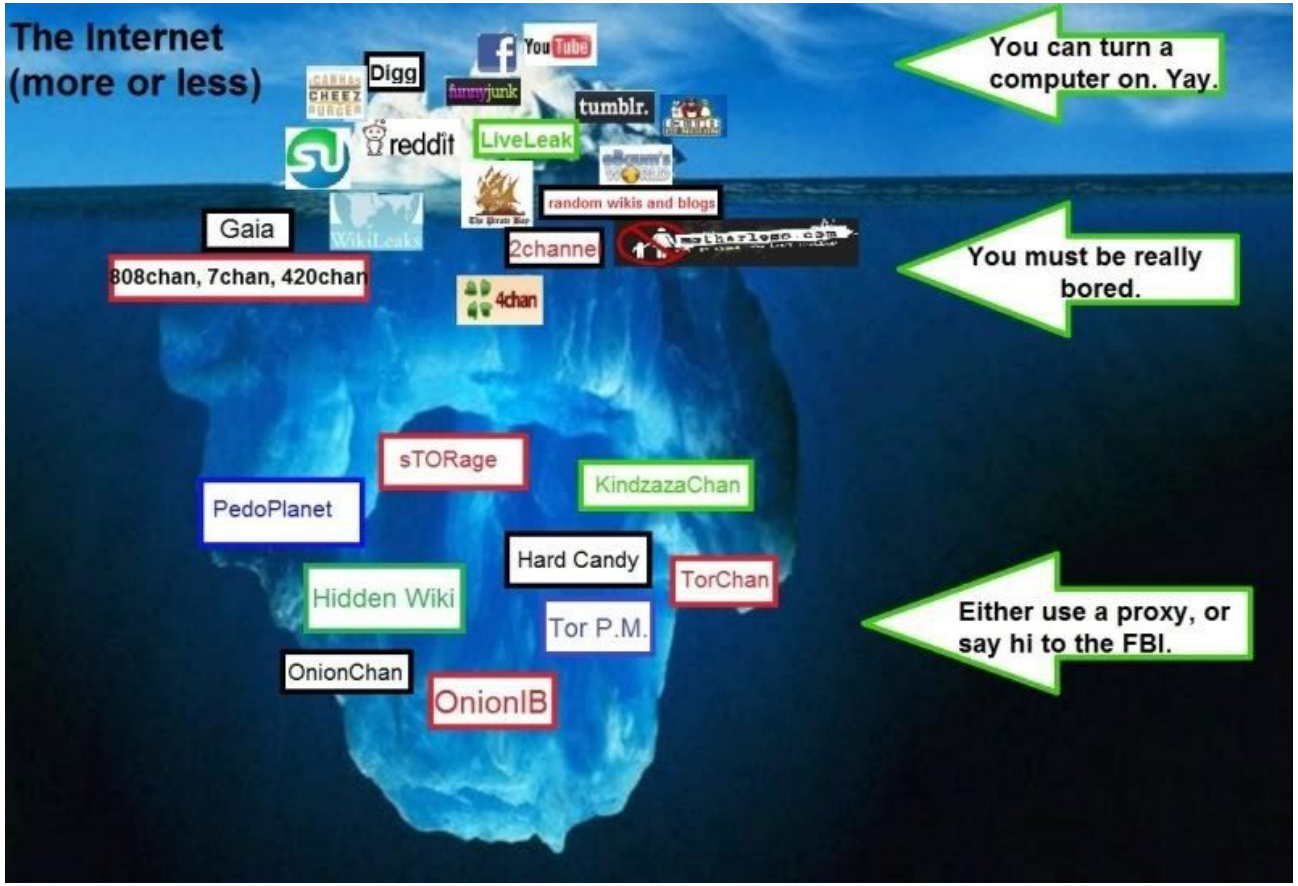
DEEP WEB ≠ DARK WEB

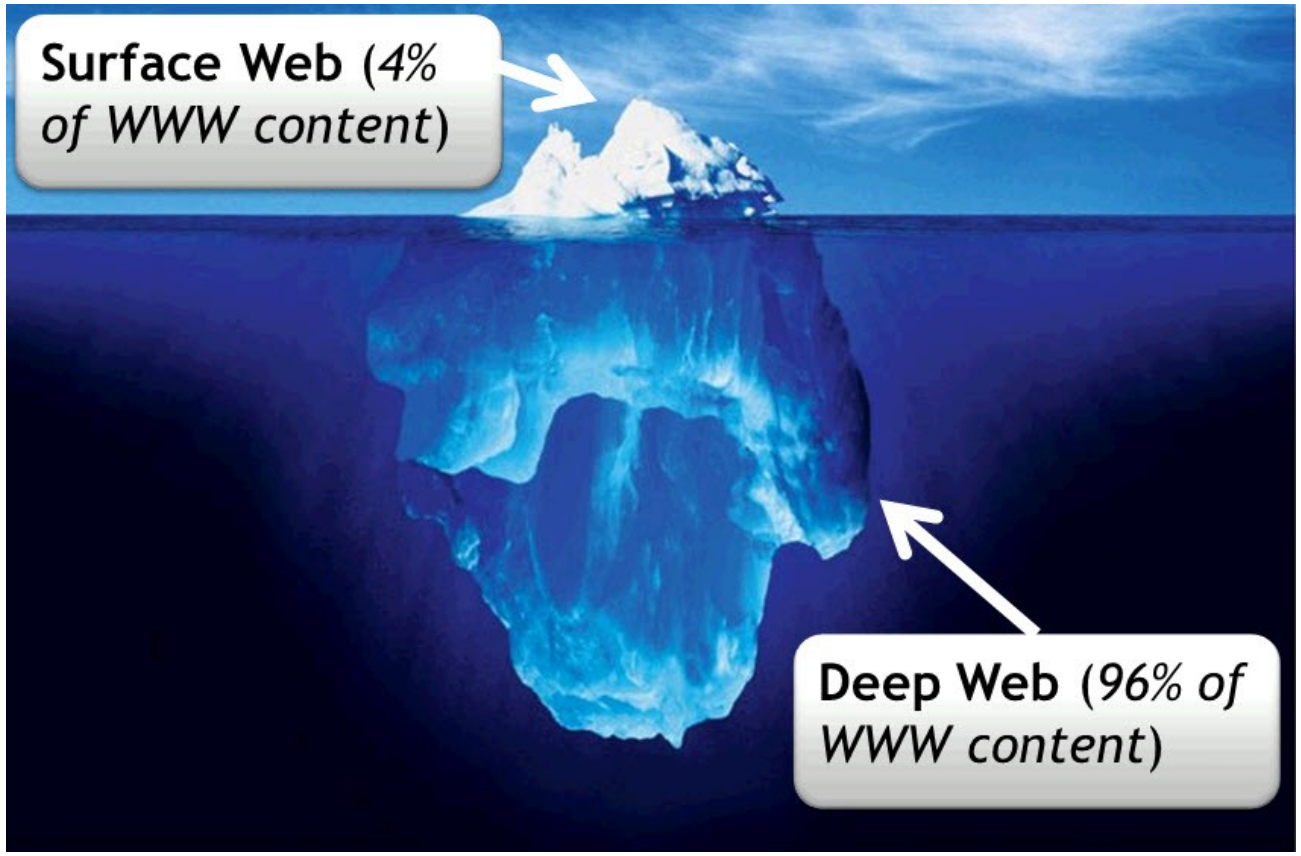
- Il DEEP WEB è costituito da tutte le informazioni che **non** sono indicizzate dai motori di ricerca tradizionali.
- Google, Bing e altri motori utilizzano spider per la scansionare il web ed i contenuti delle pagine.
- Se vi è un blocco di sicurezza, codice corrotto, configurazioni speciali (es. htaccess), password di accesso, per cui lo spider non può scansionare il contenuto, questo non sarà indicizzato.
- Di questa categoria fanno quindi parte nuovi siti non ancora indicizzati, pagine web a contenuto dinamico, web software e siti privati aziendali.

- Il DARK WEB è un sottoinsieme del Deep Web. Per accedervi si devono utilizzare determinati software specifici che fanno da bridge tra la rete Internet e la cosiddetta “DarkNet”.

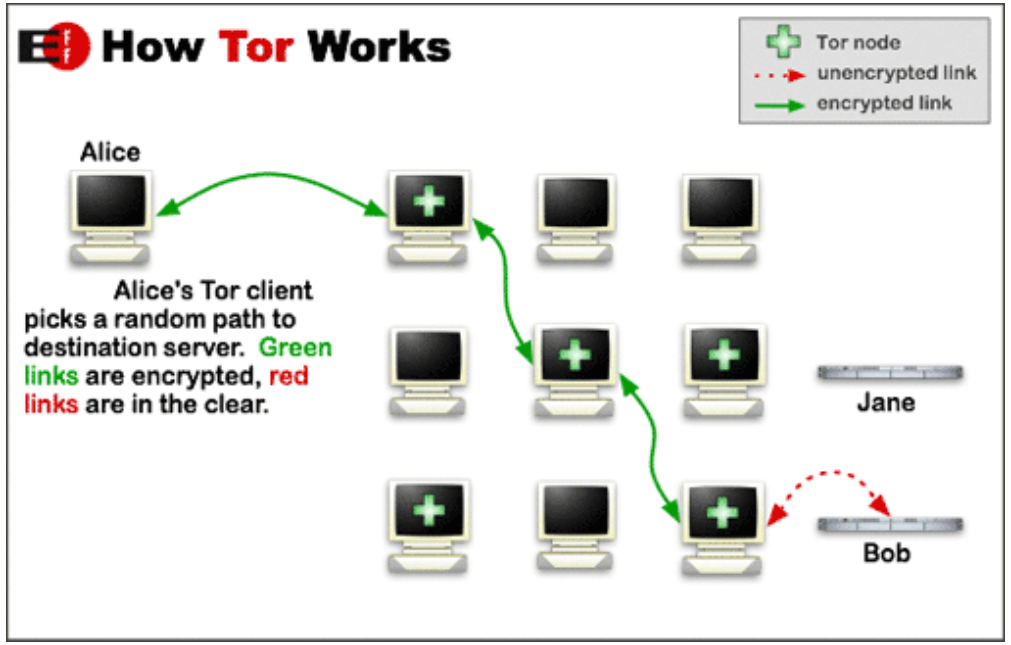
- Le darknet più comuni sono Tor, I2P e Freenet. Uno dei più famosi è Tor che, oltre a fornire accesso all'omonima rete, garantisce l'anonimato all'utente, permettendogli di navigare anonimamente anche sul normale World Wide Web da uno dei nodi della rete Tor.


SURFACE WEB
Google
Bing
Wikipedia
DEEP WEB
Academic Information
Medical Records
Legal Documents
Scientific Reports
Subscription Information
Contains 90% of the information on the Internet, but is not accessible by Surface Web crawlers.
Social Media
Multilingual Databases
Financial Records
Government Resources
Competitor Websites
Organization-specific Repositories
(DARK WEB)
A part of the Deep Web accessible only through certain browsers such as Tor designed to ensure anonymity. Deep Web Technologies has zero involvement with the Dark Web.
Illegal Information
TOR-Encrypted sites
Political Protests
Drug Trafficking sites
Private Communications


The Internet
(more or less)
You can turn a computer on. Yay.
You must be really bored.
Either use a proxy, or say hi to the FBI.
Digg
YouTube
funnyjunk
tumblr.
reddit
LiveLeak
random wikis and blogs
Gaia
808chan, 7chan, 420chan
2channe
4chan
sTORage
KindzazaChan
PedoPlanet
Hard Candy
TorChan
Hidden Wiki
Tor P.M.
OnionChan
OnionIB


Surface Web (4% of WWW content)
Deep Web (96% of WWW content)

TOR: nato come progetto della marina militare americana e ora diffuso in tutto il mondo, è un software sviluppato dal Team del Tor Project che si propone per garantire la navigazione in rete anonima:



Silk Road

anonymous marketplace

Welcome

messages(0) | orders(0) | account(฿0) | settings | log out

(0)

Home & Garden(25)
- **Seeds(3)**
- **Cuttings(3)**
- **Gardening Supplies(6)**

Drugs(746)
Lab Supplies(9)
Digital goods(166)
Services(58)
Money(42)
Jewelry(3)
Weaponry(7)
Food(2)

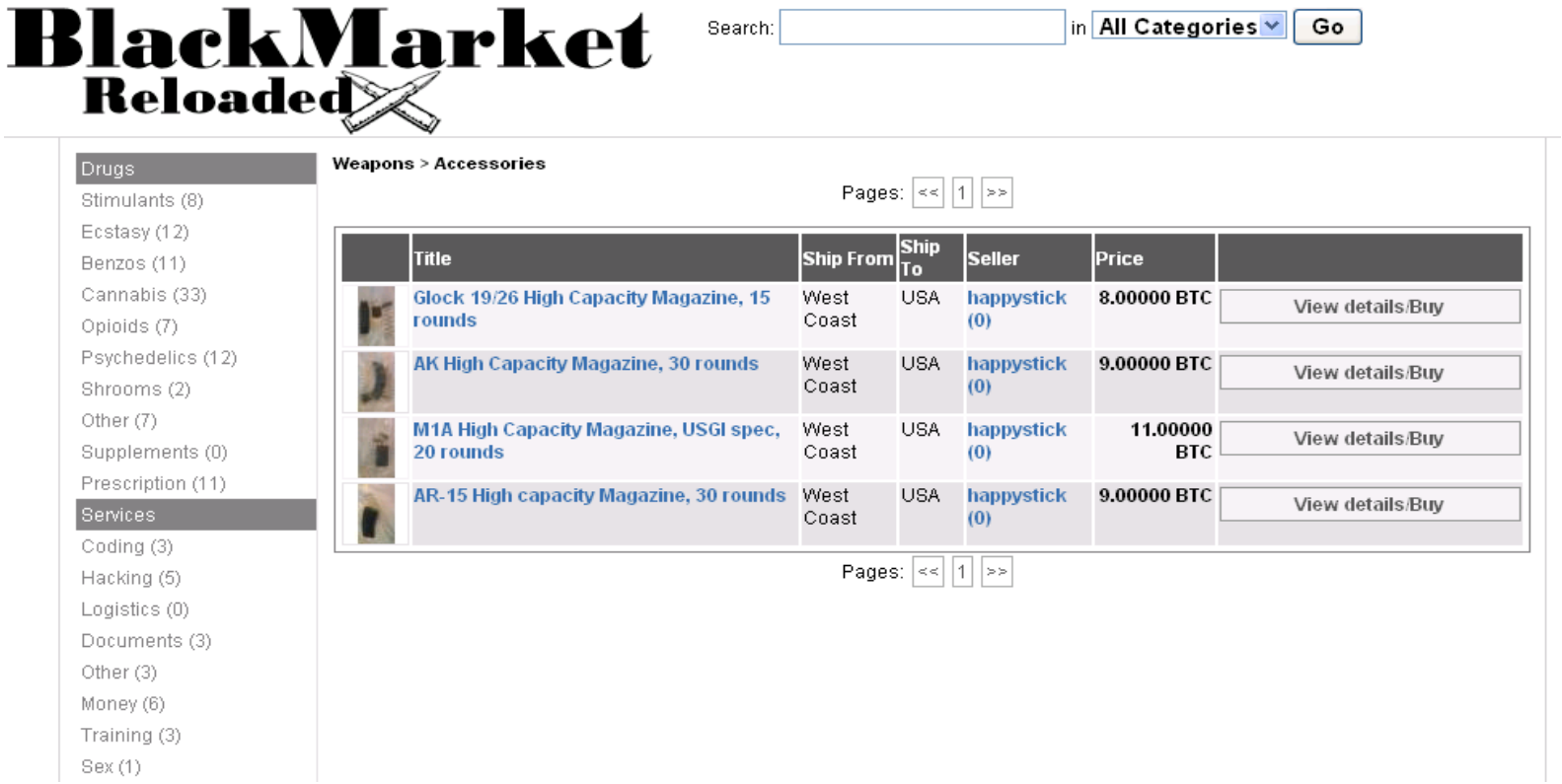
sort by seller feedback go

title	price	seller	ship to	ship from	
Telstra Pillar Key	฿0.44	qawsed	Australia	Me	add to cart
Wii - Super Mario Galaxy 2 (used)	฿1.54	HazednConfused	Germany	Germany	add to cart
Flowerpots, squared, 0,2L (2 pieces)	฿0.01	HazednConfused	Germany	Germany	add to cart
Flowerpots, squared 0,5L	฿0.01	HazednConfused	Germany	Germany	add to cart
Flowerpots squared, 1L	฿0.01	HazednConfused	Germany	Germany	add to cart
Flowerpots, squared, 1,7L	฿0.03	HazednConfused	Germany	Germany	add to cart
Flowerpots, squared, 3,5L	฿0.05	HazednConfused	Germany	Germany	add to cart
Hydrometer / Thermometer	฿0.70	HazednConfused	Germany	Germany	add to cart
Cannabis cutting, freshly rooted, female	฿0.51	HazednConfused	Germany	Germany	add to cart
Salvia divinorum Cutting / Steckling	฿0.90	OJP	EU(World)	Austria	add to cart
White Widow Cannabis Cutting / Clone / Steckling	฿0.45	OJP	worldwide	Germany	add to cart
Peyote - lophophora williamsii - 10 Seeds	฿0.20	OJP	World	Germany	add to cart
Peruvian Torch - peruviana - 10 Seeds	฿0.20	OJP	World	Germany	add to cart
San Pedro - Echinopsis pachanoi - 10 Seeds	฿0.20	OJP	World	Germany	add to cart
Vintage taxidermied hawksbill sea turtle	฿93.41	lbhx	worldwide	EU	add to cart
Organic Worm Castings Soil Amendment 8 lbs.	฿0.66	0ccultu$	US	US	add to cart
INCREDIBOWL M420 (Blue)	฿2.15	headmeds	Worldwide	Canada	add to cart

bitcoin

Università di Roma

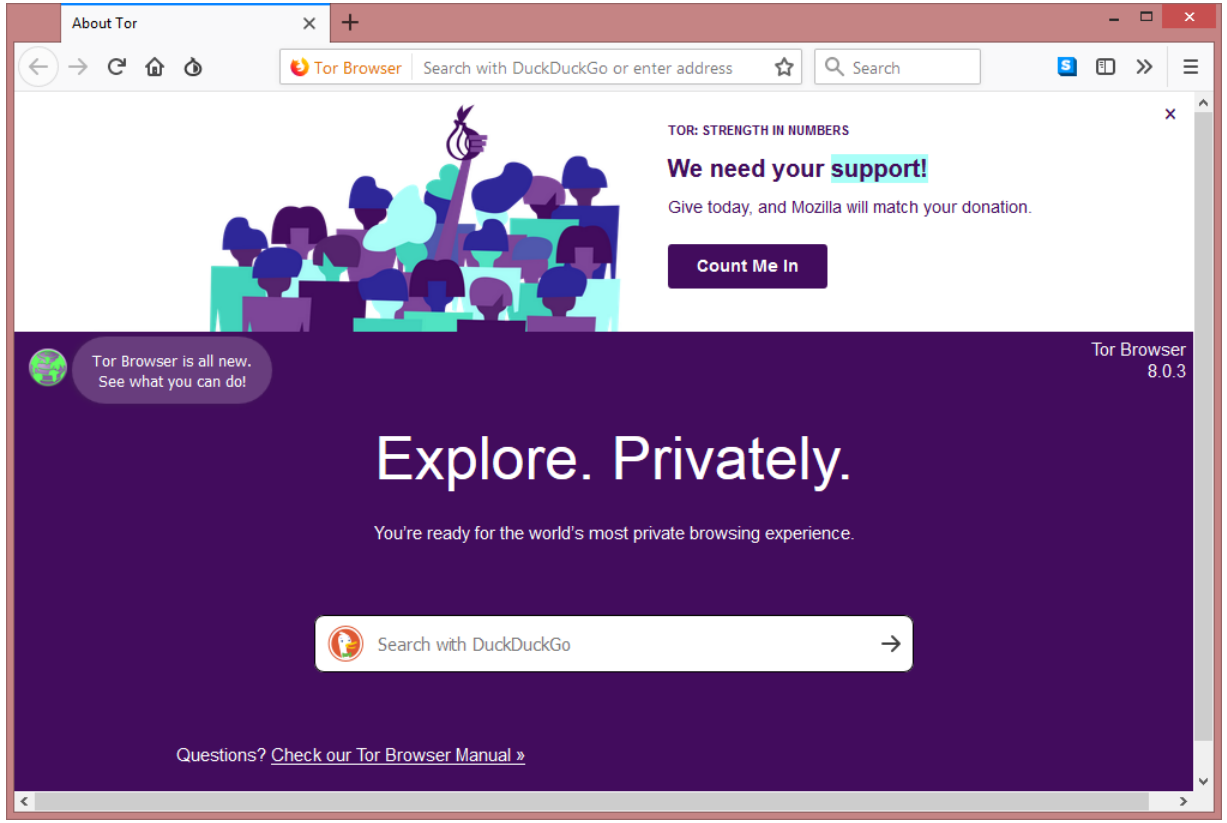
Silk Road, Bitcoin

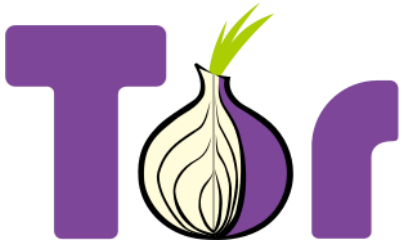


Università di Roma

TOR – Esercitazione

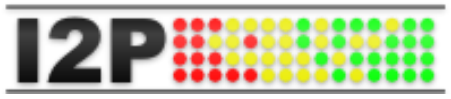
www.torproject.org





I2P – Esercitazione

I2P: è una rete di copertura anonima, una rete dentro la rete. Il suo scopo è di proteggere le comunicazioni dal controllo a tappeto e dal monitoraggio di terze parti come gli ISP.
https://geti2p.net/it/



FREENET

- **Freenet** è una rete decentralizzata, creata per resistere alla censura, che sfrutta le risorse (banda passante, spazio su disco) dei suoi utenti per permettere la pubblicazione e la fruizione di qualsiasi tipo di informazione. Freenet è stata costruita pensando ad anonimato e sicurezza, non alla velocità di trasmissione.

- **Freenet** è un software libero distribuito con GNU General Public License; essendo scritto in Java può funzionare su Microsoft Windows, GNU/Linux, macOS e su tutti i sistemi operativi dotati di Java Virtual Machine.

- **https://freenetproject.org/**

Motori di Ricerca del Deep Web

- Torch
- Duck Duck go
- Onion URL Repository
- Uncensored Hidden Wiki
- The WWW Virtual Library
- notEvil
- ParaZite
- TorLinks
- StartPage
- AHMIA
- Haystak

- elitepvpers.com
- offensivecommunity.net
- Bitcointalk.org
- evolution-forums-20140930201410l6-rasmusanderson

- Bin4023600Source TypeCC CardDetect
- Date15 May, 2018Shop Namehdjd6wv7hjngjhkb.onion
- BankPOSTE ITALIANE S.P.A. (BANCO POSTA)
- Base09.01-MIX_SNIFFp2Expire Year20Expire
- Month06Card OwnerPoste PayCountryitalyStatestateCitycityZipzip codePrice12.00


Cos'è
Perché lo raccolgo
Come lo raccolgo
Come informo la persona
Dove lo conservo
Per quanto lo conservo
Come lo cancello
Come lo tutelo
DATO PERSONALE

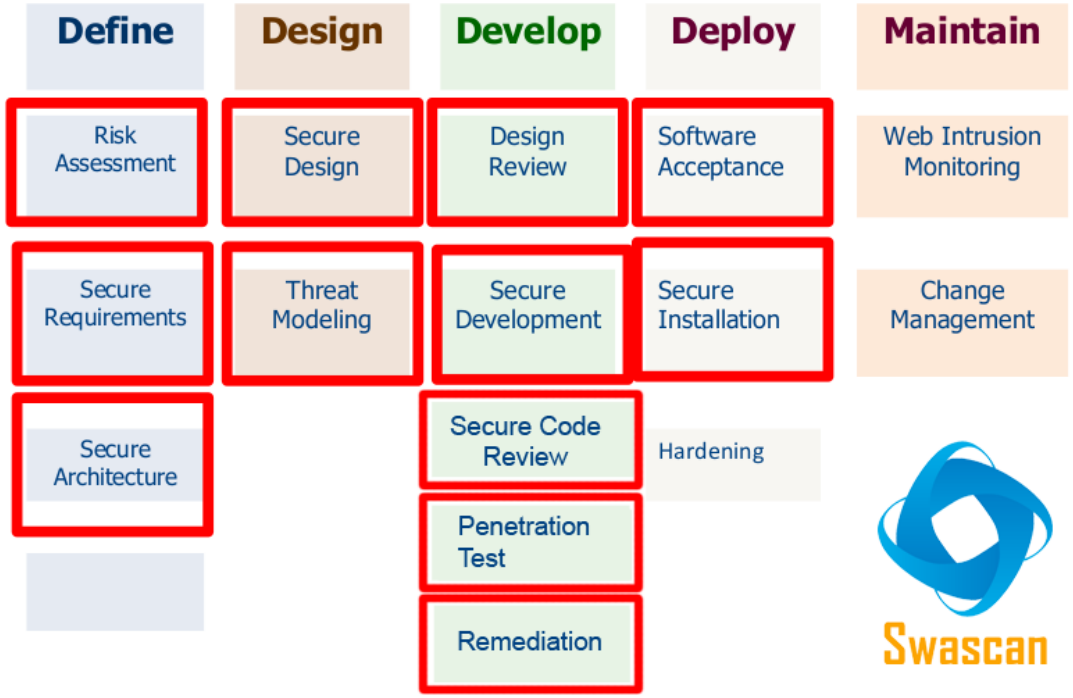
- Il GDPR introduce l'obbligo di trattare i dati secondo due tipo di progettazione:

- **By Design** cioè analizzando il trattamento per tutto il ciclo di vita dei dati. Fa riferimento all'obbligo di tutelare i diritti dell'interessato nell'attività di trattamento fin dalla fase della progettazione e per l'intera gestione del ciclo di vita dei dati, ponendo in essere misure di carattere tecnico ed organizzativo quali la minimizzazione e la pseudonimizzazione

- **By Default** cioè il partire da configurazioni "chiuse" dei sistemi informatici, per poi gradualmente ampliarle solo dopo avere valutato l'impatto di eventuali aperture ovvero le impostazioni predefinite devono essere quella che garantiscono il maggior rispetto della privacy, affinché i dati personali non siano resi accessibili ad un numero indefinito di persone senza l'intervento umano

SLDC & GDPR

Art. 25: Security by Design



- «**FEDERPRIVACY**»: Per **dato personale** Si intende qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale. Si considera tale il dato oggettivo, ma anche il dato valutativo.

- «**GARANTE PRIVACY**»: Sono **dati personali** le informazioni che identificano o rendono identificabile, **direttamente o indirettamente**, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc..

- Particolarmente importanti sono:

  - i **dati che permettono l'identificazione diretta** - come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc. - e i **dati che permettono l'identificazione indiretta**, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa);
  - i **dati rientranti in particolari categorie**: si tratta dei dati c.d. "sensibili", cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute, alla vita o all'orientamento sessuale. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici e i dati biometrici;

- i **dati relativi a condanne penali e reati**: si tratta dei dati c.d. *"giudiziari"*, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il **Regolamento (UE) 2016/679** (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

- Con l'evoluzione delle nuove tecnologie, **altri dati personali** hanno assunto un ruolo significativo, come **quelli relativi alle comunicazioni elettroniche** (via Internet o telefono) e **quelli che consentono la geolocalizzazione**, fornendo informazioni sui luoghi frequentati e sugli spostamenti.

Notizie principali

Effetto Cambridge Analytica-GDPR su Facebook, crollo degli utenti in Europa
Key4biz · 10 ore fa

Facebook paga lo scandalo Cambridge Analytica: ricavi sotto le attese - Economia
Unione Sarda · 10 ore fa

Dopo Cambridge Analytica, Facebook sospende un'altra società di analisi dei dati
La Repubblica · 5 giorni fa

→ Altri risultati per cambridge analytica

Immuni, i dubbi **privacy** e sicurezza dopo la release del codice
Agenda Digitale - 28 mag 2020
Esaminiamo allora la **privacy** e la security dell'app **Immuni**, alla luce delle informazioni che attualmente abbiamo a disposizione. Indice degli ...

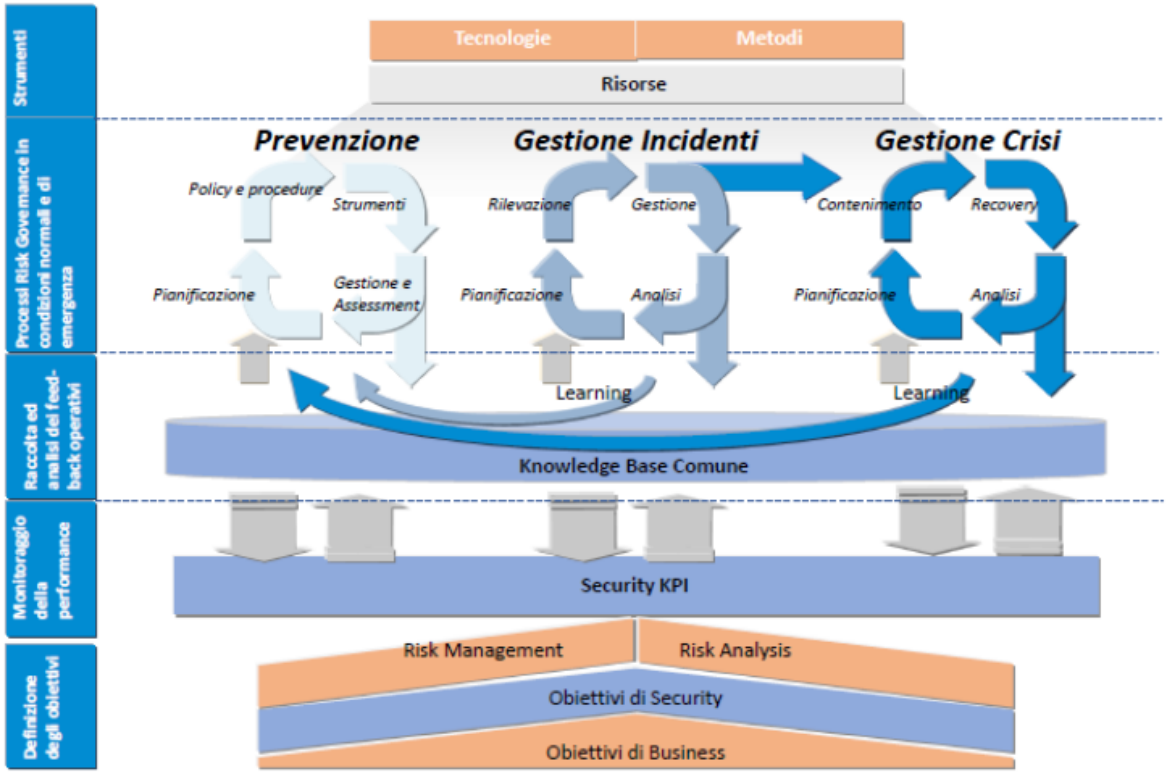
App **Immuni**: mette a rischio la nostra **privacy**?
Metropolitano.it - 29 mag 2020
Saranno sei e non più tre le regioni tester. **Immuni**, l'applicazione scelta dal Governo Italiano per il tracciamento dei soggetti risultati positivi al ...

Immuni, le FAQ del Governo tra **privacy** e funzionamento: non ...
Fanpage - 12 mag 2020
Immuni, le FAQ del Governo tra **privacy** e funzionamento: non chiederà dati personali. Il Ministero per l'innovazione tecnologica e la ...

L'App **Immuni** del Governo non chiederà dati personali: le ...
Notizie.it - 12 mag 2020

Mostra tutti

Security Management: value proposition



Da

- Con il termine **data breach** si intende un incidente di sicurezza in cui dati sensibili, protetti o riservati vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato. Solitamente il data breach si realizza con una divulgazione di dati riservati o confidenziali all'interno di un ambiente privo di misure di sicurezze (da esempio, su web) in maniera involontaria o volontaria. Tale divulgazione può avvenire in seguito a:
- **perdita accidentale**: ad esempio, data breach causato da smarrimento di una chiavetta USB contenente dati riservati
- **furto**: ad esempio, data breach causato da furto di un notebook contenente dati confidenziali
- **infedeltà aziendal**e: ad esempio, data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico
- **accesso abusivo**: ad esempio, data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite


Elex
July 22
Almost 1.6M users accounts
Bon Secours Health System
August 12
655K patients' records
Illinois Board of Elections
August 30
200K personal voter records
ClixSense
September 14
6.6M user records
Washington Department of Fish and Wildlife
October 14
1.7M customers' personal records
FourSquare
October 21
22.5M user accounts
Michigan State University
November 18
400K personal records
Google Android
November 30
Over 1M user accounts
Community Health Plan of Washington
December 21
382K members' personal information
JUL
AUG
SEP
OCT
NOV
DEC
Disney Consumer Products and Interactive Media
July 30
356K Playdom Forum users' records
Epic Games Forums
August 23
808K user accounts
Brazzers.com
September 6
Nearly 800K user information
Yahoo!
September 22
500M user accounts
Weebly
October 20
43M records
FriendFinder
November 16
412M user accounts
United States Navy Career Waypoints
November 23
134K user accounts
Yahoo!
December 14
1B user accounts

- Per data breach, nella versione italiana **violazione dei** dati personali si intende la **violazione di sicurezza** che comporta **accidentalmente o in modo illecito** la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

- Sempre secondo il GDPR, la notifica di eventuali violazioni di dati dovrà avvenire possibilmente senza ingiustificato ritardo e, ove possibile, **entro 72 ore**, dal momento in cui si è venuto a conoscenza della violazione, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

- L'eventuale ritardo dovrà essere motivato.

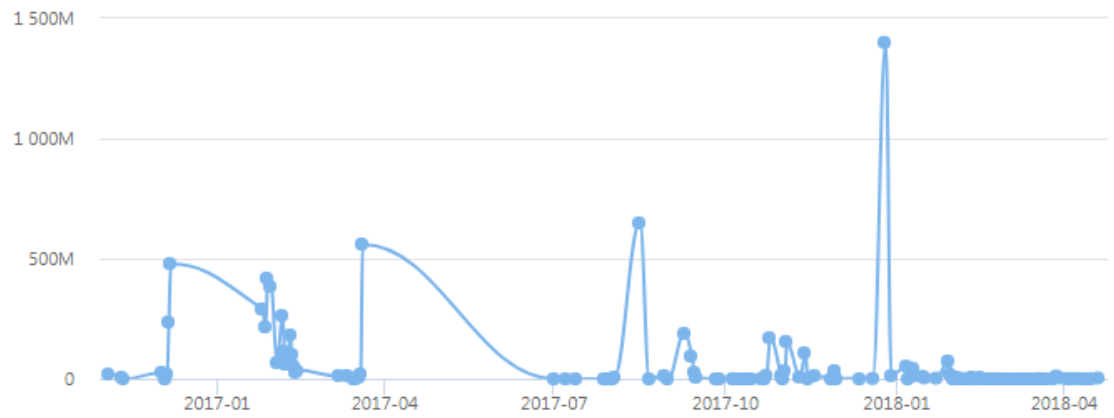
I **dati violati con un data breach** possono riguardare tutti gli ambiti, esempi reali:

- **finanziario**, ad esempio dati di carte di credito, di conti correnti…
- **sanitario**, ad esempio informazioni sulla salute personale, malattie…
- **proprietà industriale**, ad esempio segreti commerciali, brevetti, documentazione riservata, lista clienti, progetti finalizzati ad esempio a pratiche di concorrenza sleale…
- **personali**, ad esempio dati di documenti di identità, codici personali…

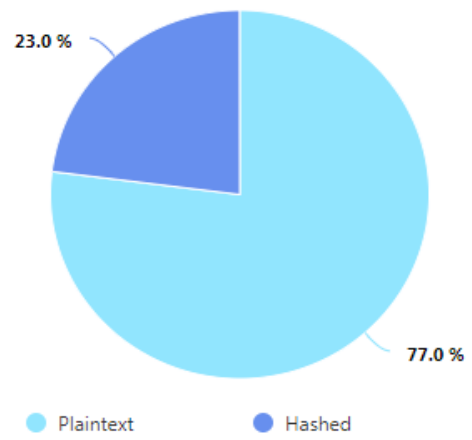
DATA BREACH INTELLIGENCE

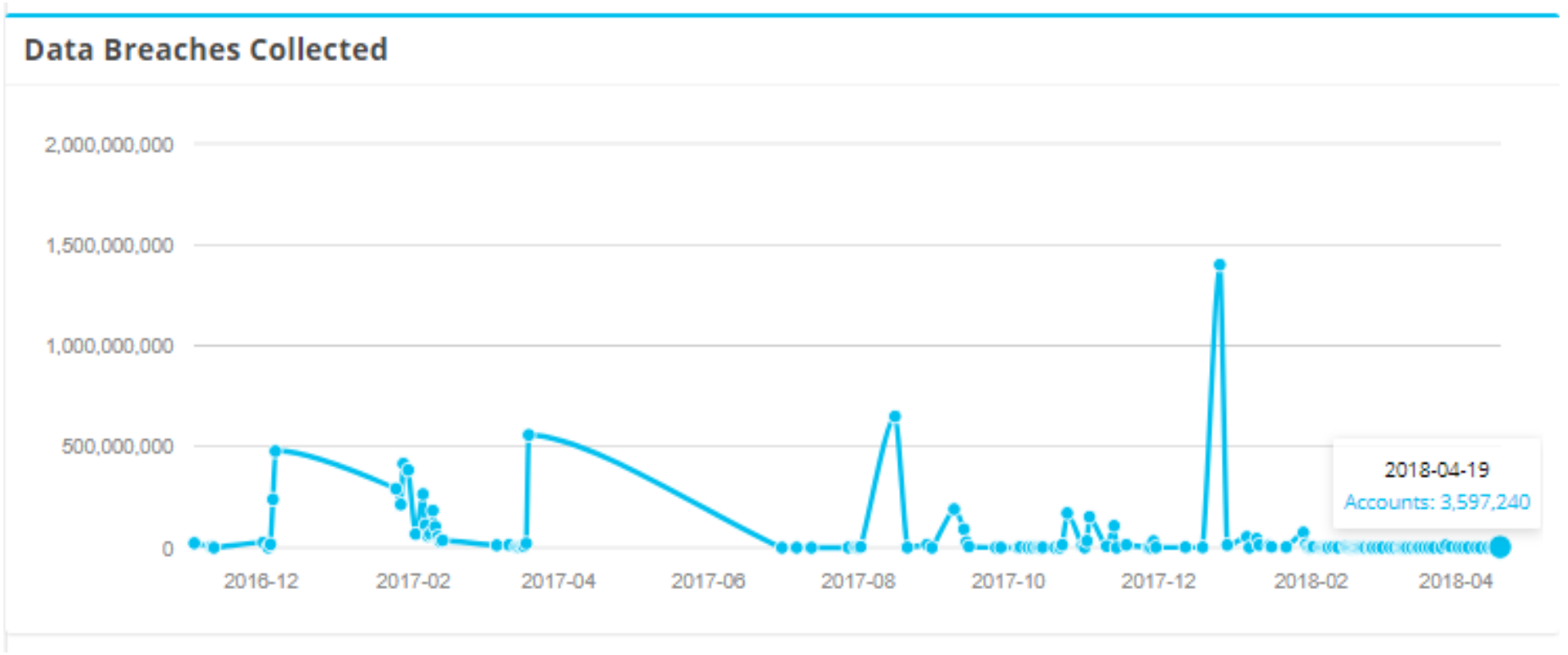
Total records	Passwords (hashed)	Passwords (plaintext)	E-mails	Users names	IPs
6.95B	**1.53B**	**5.17B**	**6.25B**	**1.19B**	**123M**

Data Breaches Collected

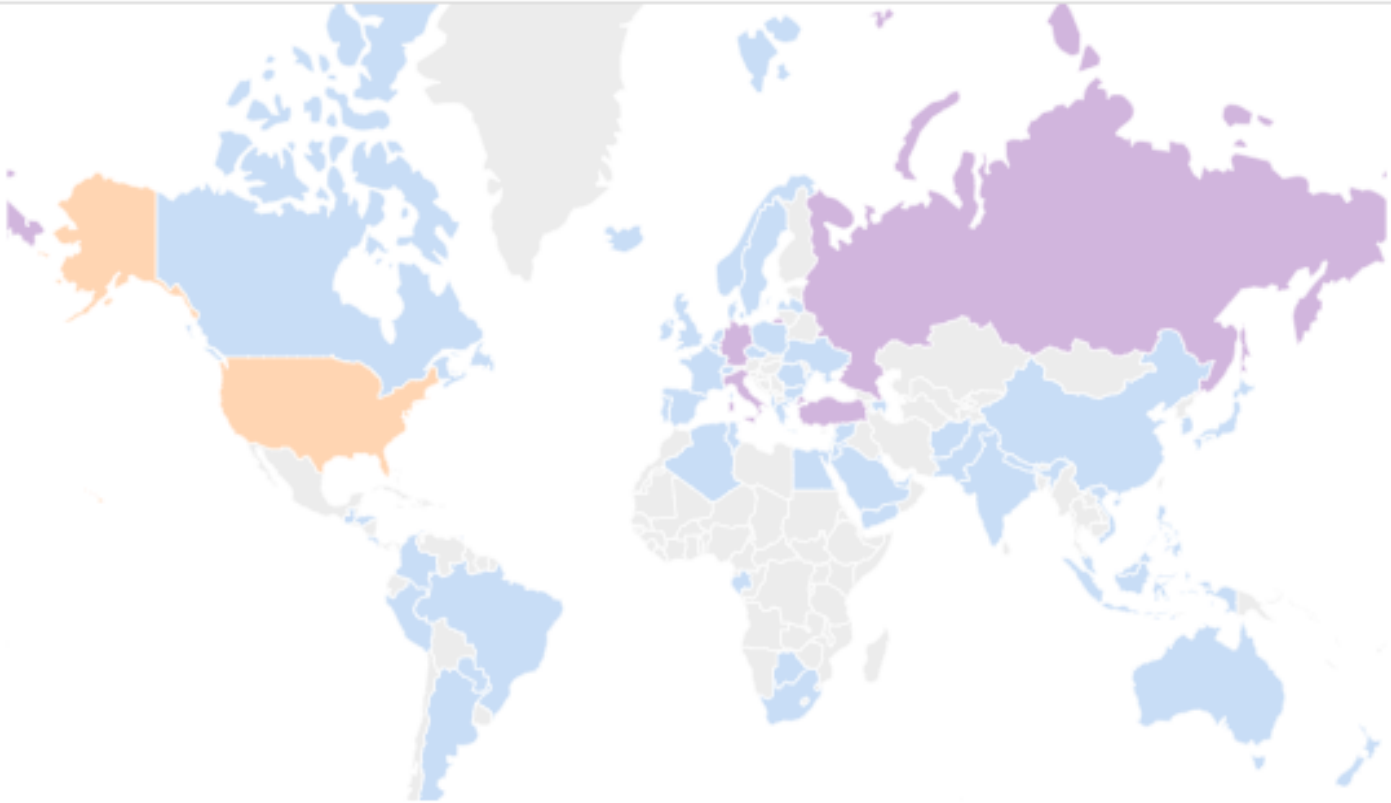


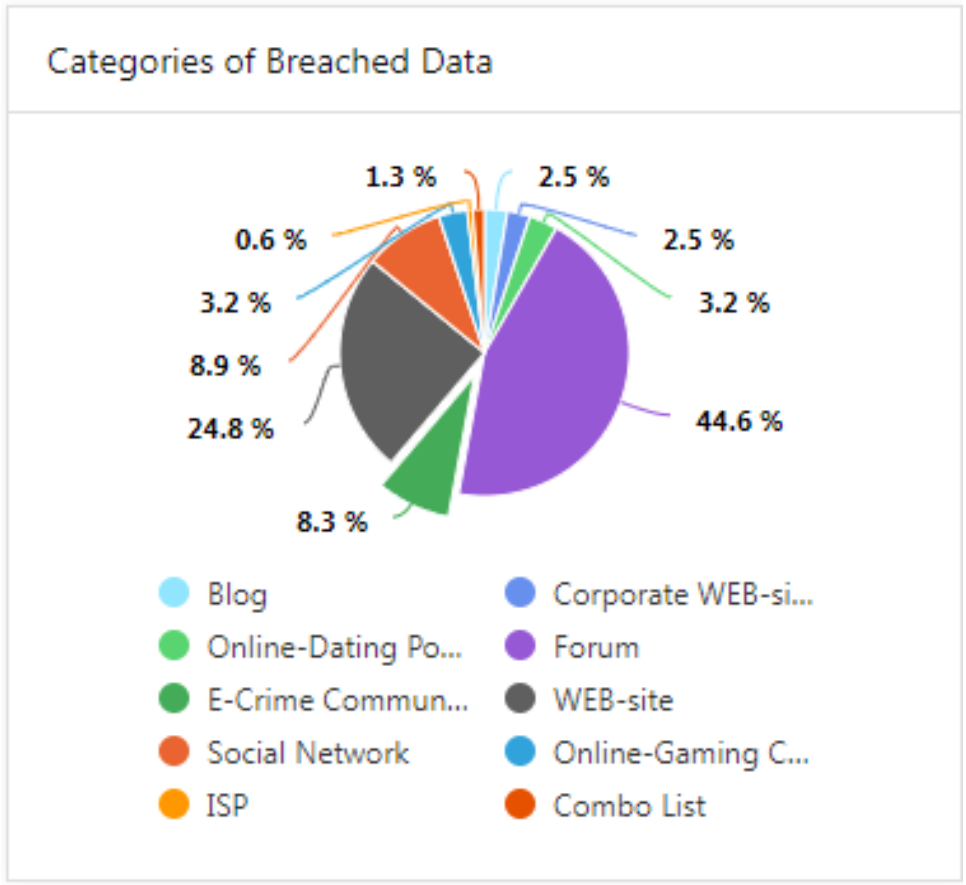
Password Type Distribution

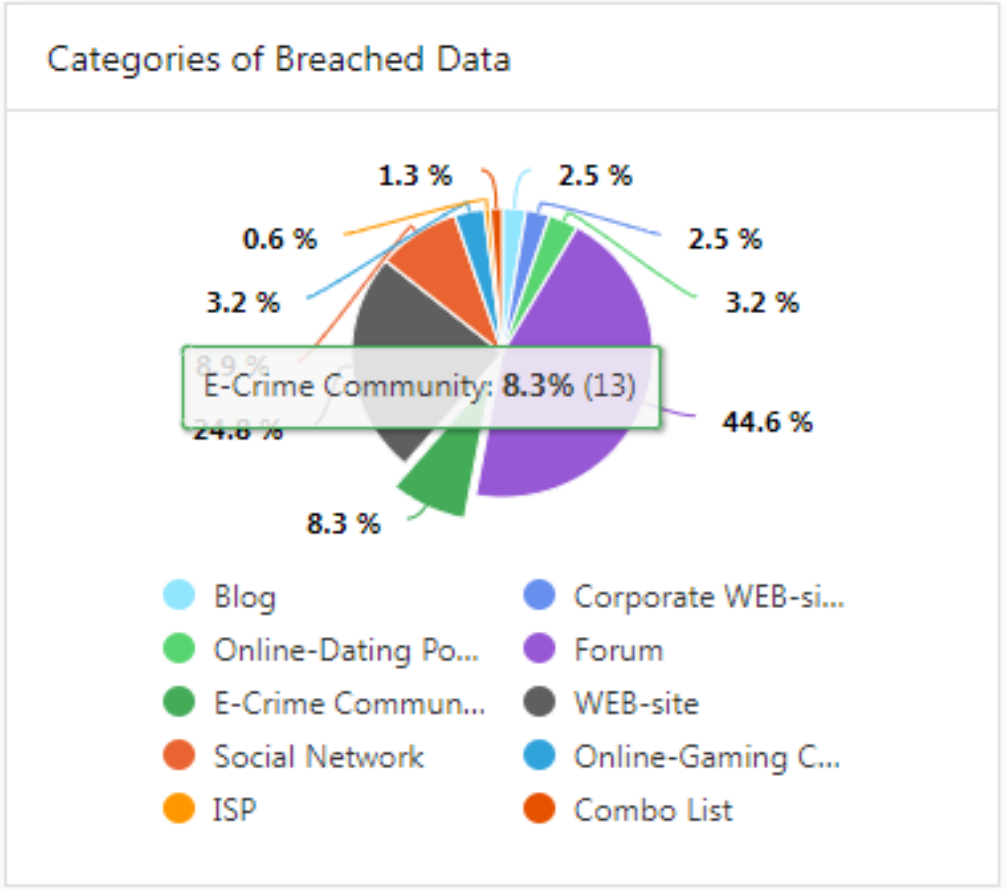



Data Breaches Collected
2,000,000,000
1,500,000,000
1,000,000,000
500,000,000
0
2016-12
2017-02
2017-04
2017-06
2017-08
2017-10
2017-12
2018-02
2018-04
2018-04-19
Accounts: 3,597,240

Geographical Destribution

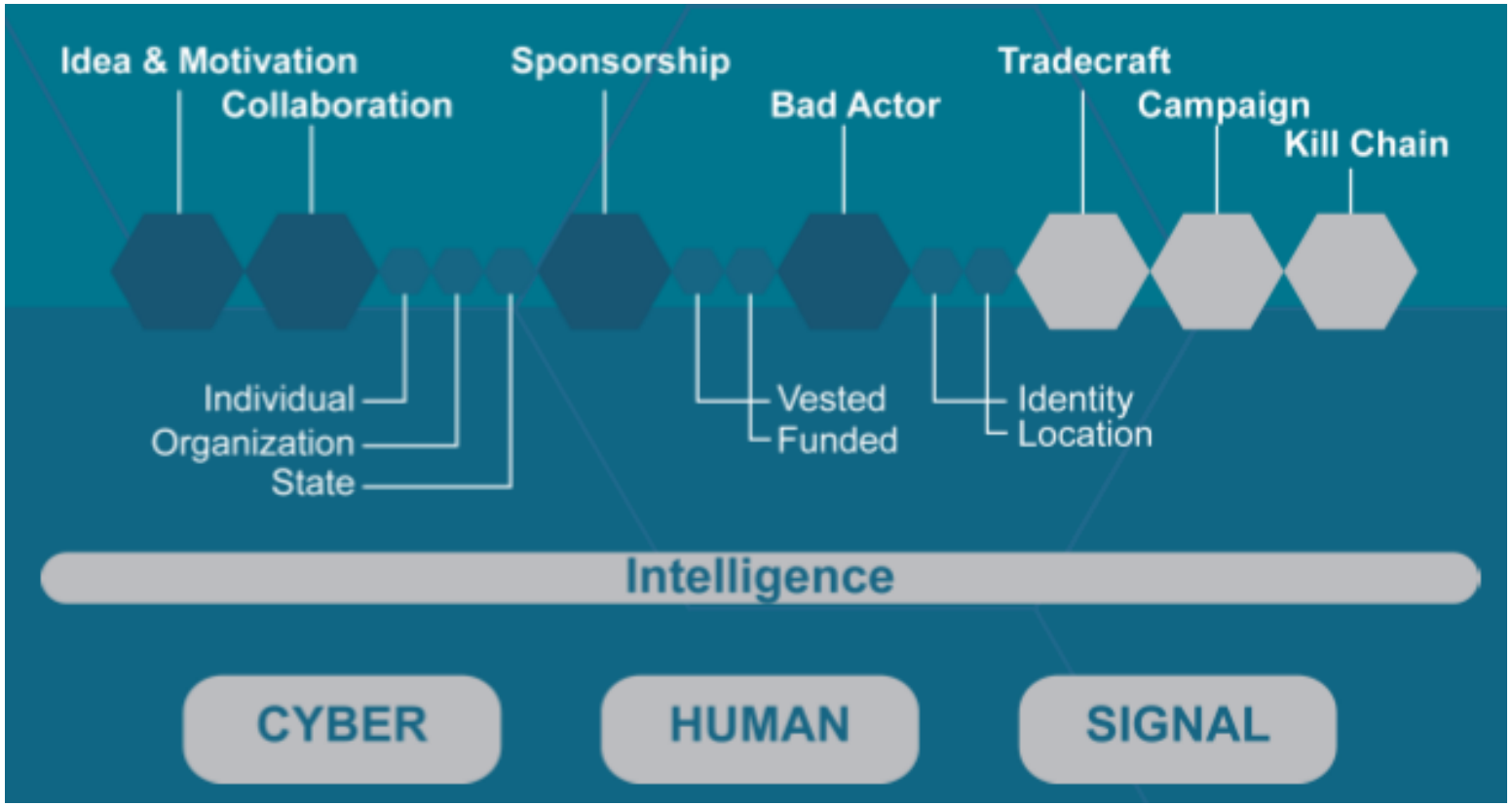



Categories of Breached Data
1.3 %
2.5 %
0.6 %
2.5 %
3.2 %
3.2 %
8.9 %
44.6 %
24.8 %
8.3 %
Blog
Corporate WEB-si...
Online-Dating Po...
Forum
E-Crime Commun...
WEB-site
Social Network
Online-Gaming C...
ISP
Combo List


Categories of Breached Data
1.3 %
2.5 %
0.6 %
2.5 %
3.2 %
3.2 %
E-Crime Community: 8.3% (13)
44.6 %
8.3 %
Blog
Corporate WEB-si...
Online-Dating Po...
Forum
E-Crime Commun...
WEB-site
Social Network
Online-Gaming C...
ISP
Combo List


HACKING DETECTED
RISK ALERT
85%
67%
50%


CYBER THREAT INTELLIGENCE

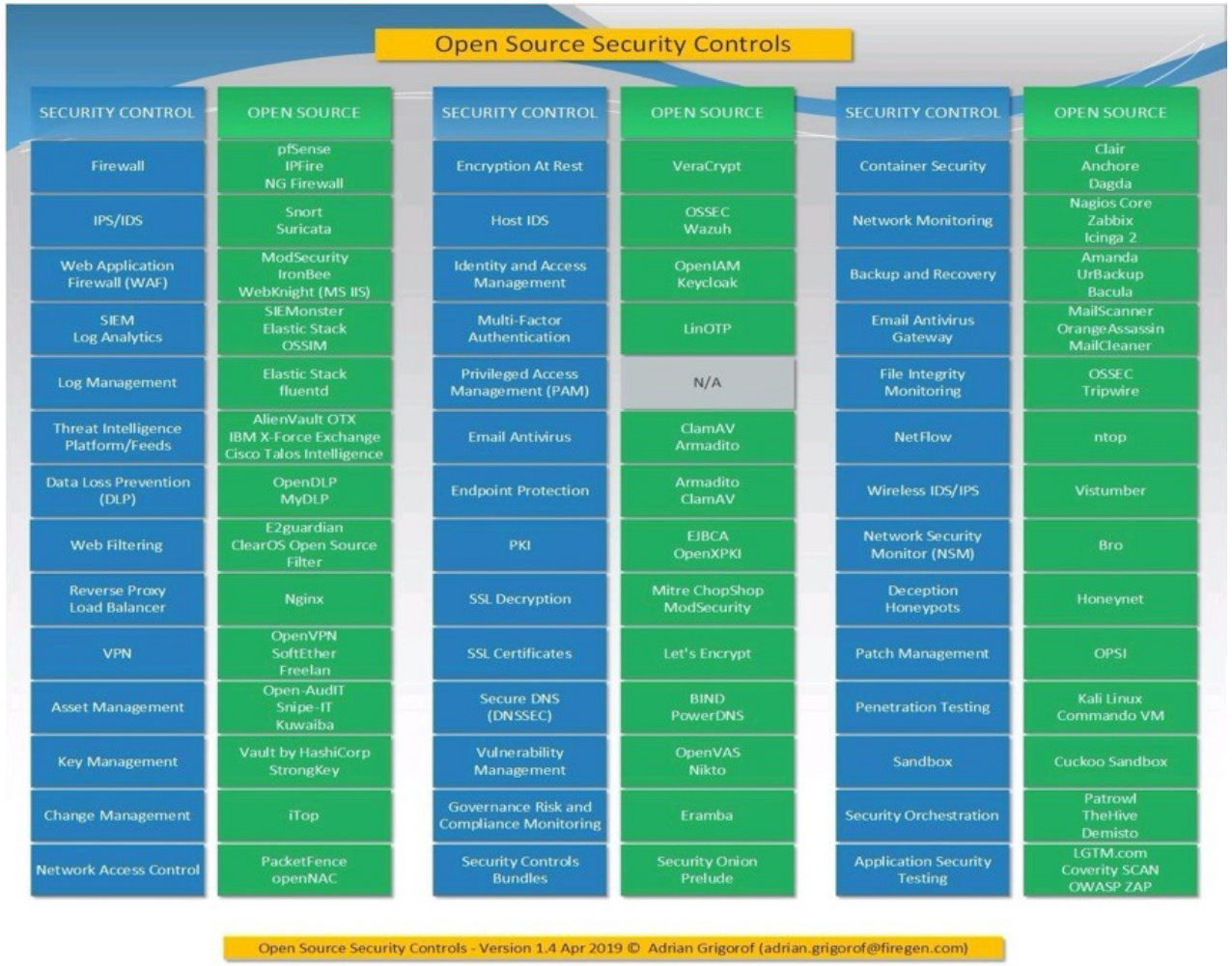

Idea & Motivation
Collaboration
Sponsorship
Bad Actor
Tradecraft
Campaign
Kill Chain
Individual
Organization
State
Vested
Funded
Identity
Location
Intelligence
CYBER
HUMAN
SIGNAL

Milioni di contatti succhiati dalle caselle email o dalle chat sui social network.
Un sistema capillare, invasivo, praticamente impossibile da arginare. Basta un dato a dimostrarlo: in un solo giorno nel 2012 sono stati intercettati 444.743 liste di contatti da account Yahoo!, 82.857 da Facebook, 33.697 da Gmail e 22.881 da altri fornitori di servizi internet.

250 MILIONI DI CONTATTI ALL'ANNO. Equivalenti a circa 250 milioni di gruppi di nomi sotto osservazione all'anno: per lo più cittadini non americani. E dunque europei, sudamericani, asiatici.

Perché la cifratura oggi

- TOR – https://www.torproject.org/
- FOCA – https://www.elevenpaths.com/labstools/foca/index.html
- Maltego – https://www.paterva.com/downloads.php
- VeraCrypt – https://www.veracrypt.fr/en/Downloads.html
- Eraser – https://eraser.heidi.ie/download/
- Recuva – https://www.ccleaner.com/recuva/download
- GPG4Win – https://www.gpg4win.org/


Open Source Security Controls
SECURITY CONTROL
OPEN SOURCE
Firewall
pfSense
IPFire
NG Firewall
IPS/IDS
Snort
Suricata
Web Application Firewall (WAF)
ModSecurity
IronBee
WebKnight (MS IIS)
SIEM Log Analytics
SIEMonster
Elastic Stack
OSSIM
Log Management
Elastic Stack
fluentd
Threat Intelligence Platform/Feeds
AlienVault OTX
IBM X-Force Exchange
Cisco Talos Intelligence
Data Loss Prevention (DLP)
OpenDLP
MyDLP
Web Filtering
E2guardian
ClearOS Open Source Filter
Reverse Proxy Load Balancer
Nginx
VPN
OpenVPN
SoftEther
Freelan
Asset Management
Open-AudIT
Snipe-IT
Kuwaiba
Key Management
Vault by HashiCorp
StrongKey
Change Management
iTop
Network Access Control
PacketFence
openNAC
SECURITY CONTROL
OPEN SOURCE
Encryption At Rest
VeraCrypt
Host IDS
OSSEC
Wazuh
Identity and Access Management
OpenIAM
Keycloak
Multi-Factor Authentication
LinOTP
Privileged Access Management (PAM)
N/A
Email Antivirus
ClamAV
Armadito
Endpoint Protection
Armadito
ClamAV
PKI
EJBCA
OpenXPKI
SSL Decryption
Mitre ChopShop
ModSecurity
SSL Certificates
Let's Encrypt
Secure DNS (DNSSEC)
BIND
PowerDNS
Vulnerability Management
OpenVAS
Nikto
Governance Risk and Compliance Monitoring
Eramba
Security Controls Bundles
Security Onion
Prelude
SECURITY CONTROL
OPEN SOURCE
Container Security
Clair
Anchore
Dagda
Network Monitoring
Nagios Core
Zabbix
Icinga 2
Backup and Recovery
Amanda
UrBackup
Bacula
Email Antivirus Gateway
MailScanner
OrangeAssassin
MailCleaner
File Integrity Monitoring
OSSEC
Tripwire
NetFlow
ntop
Wireless IDS/IPS
Vistumber
Network Security Monitor (NSM)
Bro
Deception Honeypots
Honeynet
Patch Management
OPSI
Penetration Testing
Kali Linux
Commando VM
Sandbox
Cuckoo Sandbox
Security Orchestration
Patrowl
TheHive
Demisto
Application Security Testing
LGTM.com
Coverity SCAN
OWASP ZAP
Open Source Security Controls - Version 1.4 Apr 2019 © Adrian Grigorof (adrian.grigorof@firegen.com)

- Cancellazione Sicura di Documenti
- Recuperare documenti cancellati dal PC
- Contatti, Sms, foto e file da un cellulare
- Ricevere email cifrate, cifrare file
- Documenti, hard disk, chiavette Usb
- Metodi di Antiforensics
- Comunicazioni mobili sicure
- Live Demo

- I file system memorizzano i file in piccole unità di allocazione chiamate “cluster” registrando la posizione del file, il nome ed altre informazioni definite metadati (data creazione, proprietario, permessi, data modifica…) in speciali strutture che cambiano a seconda del tipo di file system

- Un file sarà scritto su più cluster, creando una “catena” di cluster e una “mappa” che identifica quali cluster appartengono al file.

- All'inizio ed alla fine della “catena” di cluster sono posti delle sequenze di caratteri che identificano il tipo di file: header e footer

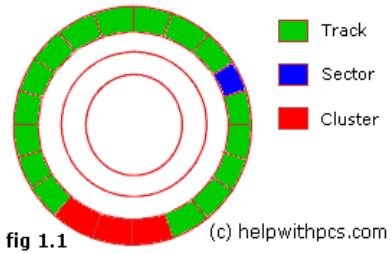
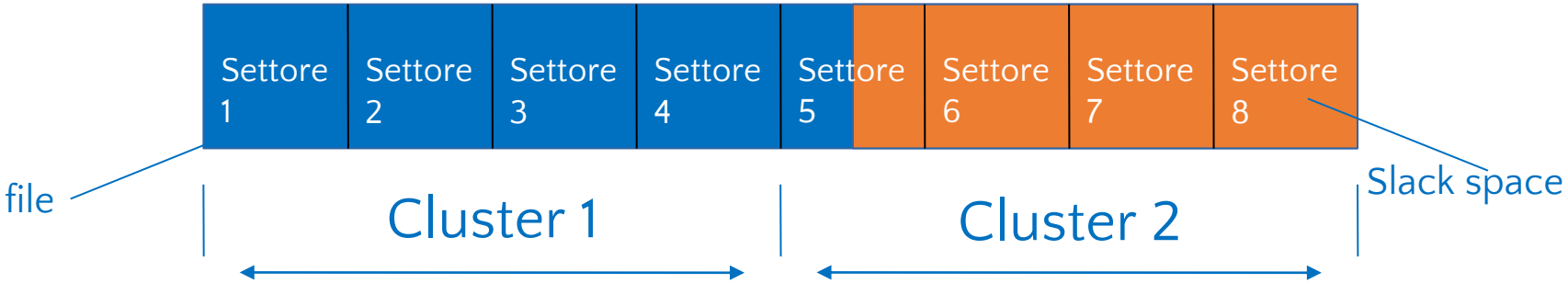


fig 1.1

- Quando viene cancellato un file viene solo messo un flag (l'operazione effettiva è diversa in base ai file system) per indicare che il file è “deleted” ed i cluster utilizzati dal file cancellato vengono resi nuovamente disponibili per altri file.

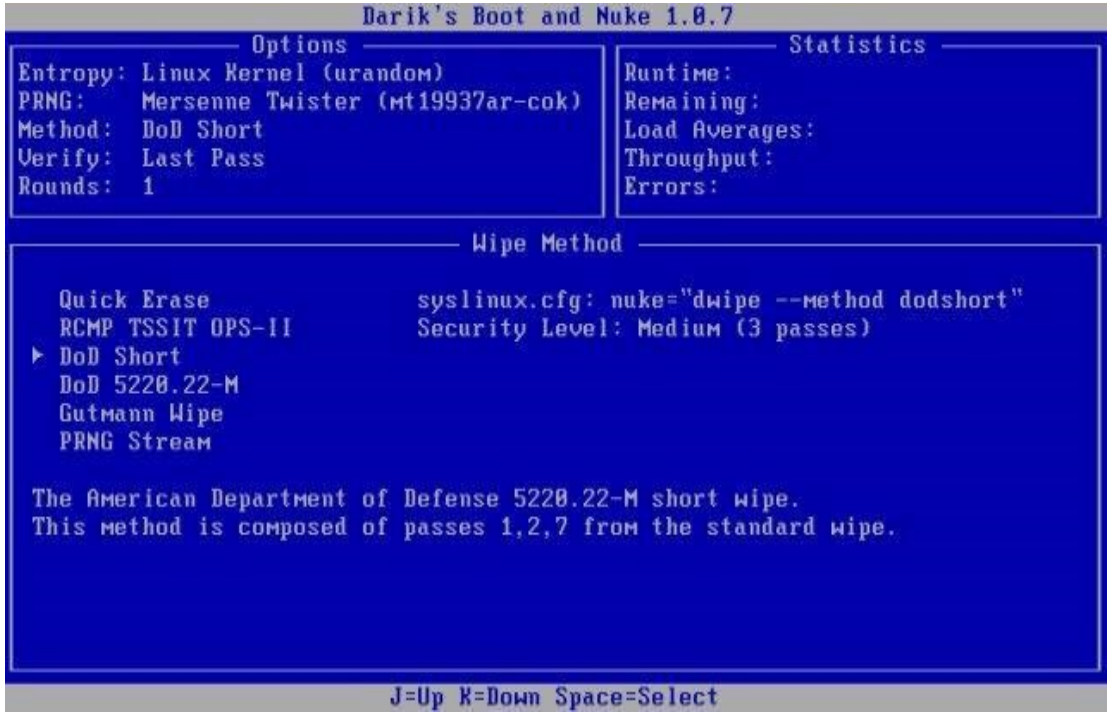
- L'operazione di cancellazione di un file **non ripulisce i cluster** del loro contenuto permettendo così il recupero dei file cancellati se non sono stati sovrascritti.

- Se il contenuto di un file non riempie completamente un cluster, possono rimanere parti del file che occupava precedentemente quel cluster. Si parla di **Slack Space**.



- Le norme sulla privacy impongono la cancellazione sicura dei dati personali memorizzati su supporti dismessi
- Possono essere utilizzati vari metodi, fra cui:
  - Distruzione fisica del supporto (punzonatura)
  - Smagnetizzazione (degauss)
  - Sovrascrittura (wiping)
- Lo standard DoD 5220.22-M (Department of Defence USA) prevede riscritture successive dei file con diversi pattern
- Il metodo Gutman

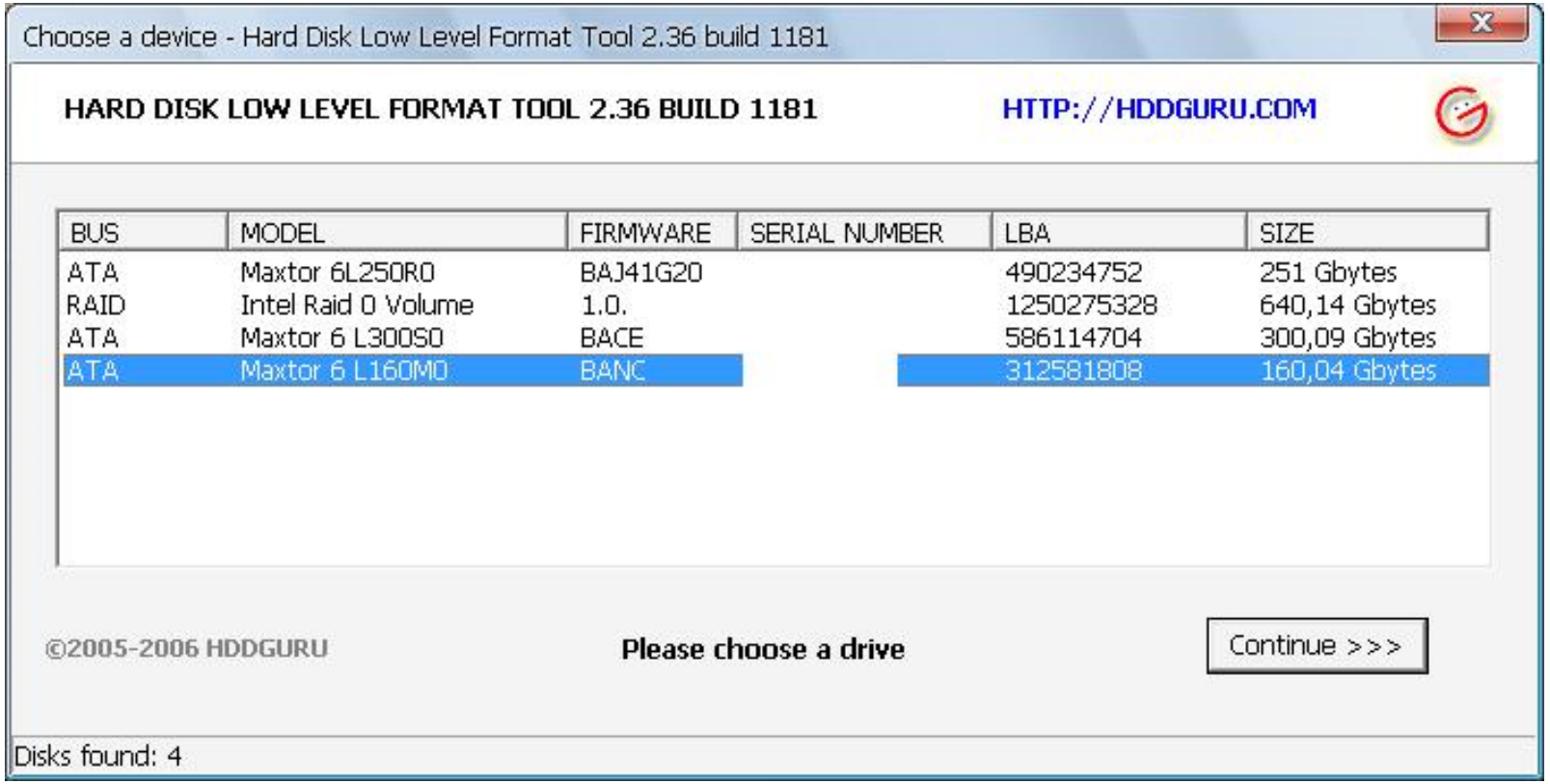
- Software specifico per wiping di file (shred)
- Sovrascrittura device con dd (dd if=/dev/null of=/dev/device)
- Una distribuzione GNU/Linux specifica: (usa anche lo standard DoD)



- Mettere un file nel cestino non cancella davvero, ed i files possono essere recuperati anche dopo anni dalla presunta cancellazione. Esistono molti programmi per la cancellazione sicura, ma siamo sicuri che funzionino ?

- http://eraser.heidi.ie/
- ERASE

- Formattazione a basso livello



Molte volte andando di fretta cancelliamo tutto ciò che in quel momento ci risulta superfluo, ma poi successivamente si ha necessità di recuperare.

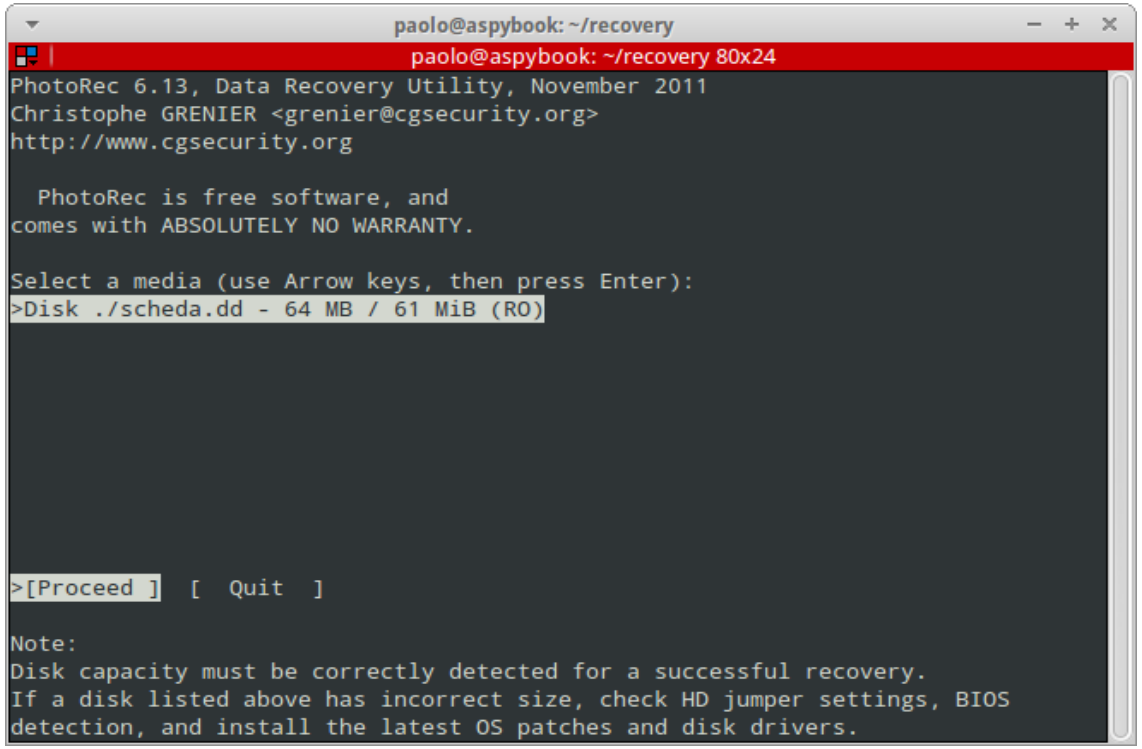
Tantissimi programmi in rete millantano di recuperare dati informatici….ma attenzione possono essere malevoli….

Fare il download solo dal sito del produttore Software….

Cosa si utilizza????

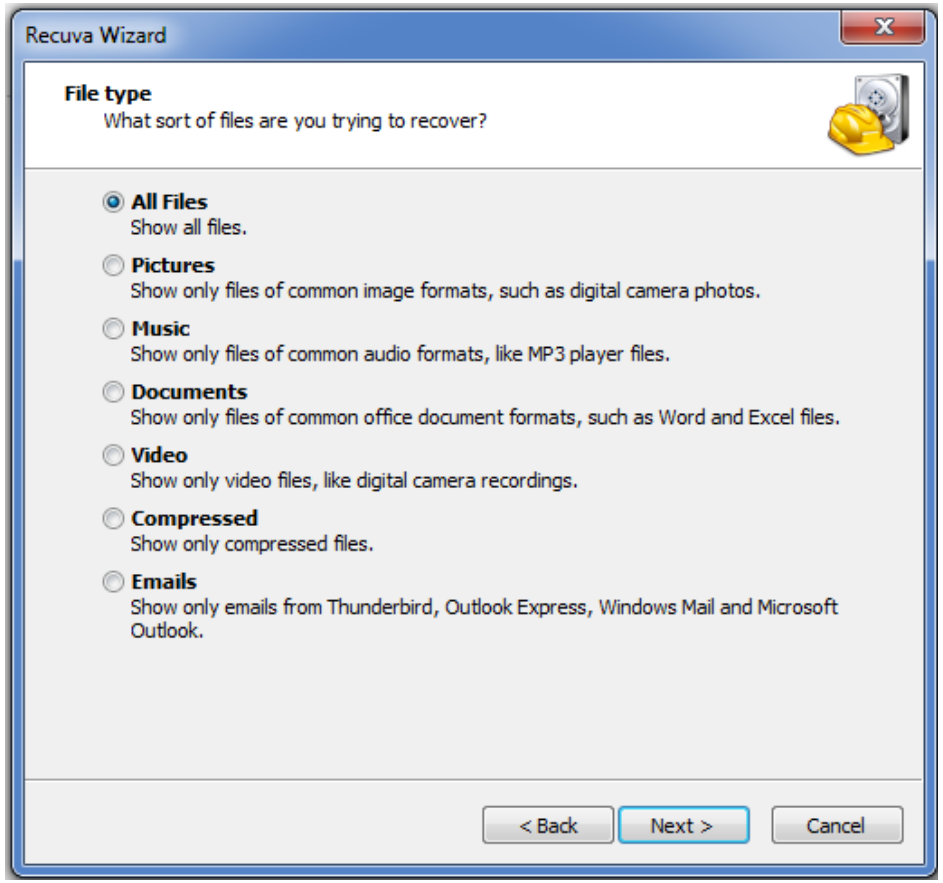
- **Photorec / Testdisk**

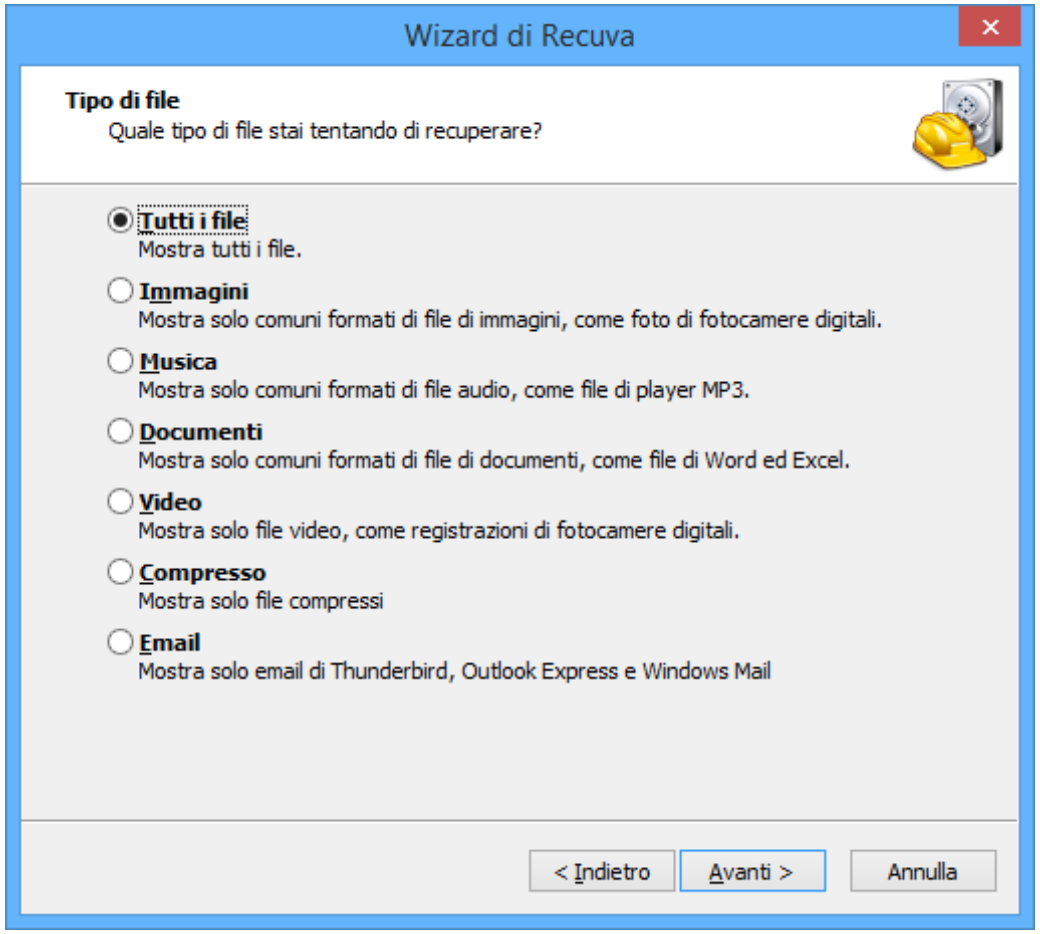
Su sistemi Linux viene aperta una shell mentre nelle ultime versioni per Windows è presente anche una interfaccia grafica. In entrambi i casi viene mostrato un menu dal quale effettuare le scelte del tipo di file system, ecc. I file recuperati vengono memorizzati in cartelle chiamate recup_dir.1, 2, 3…

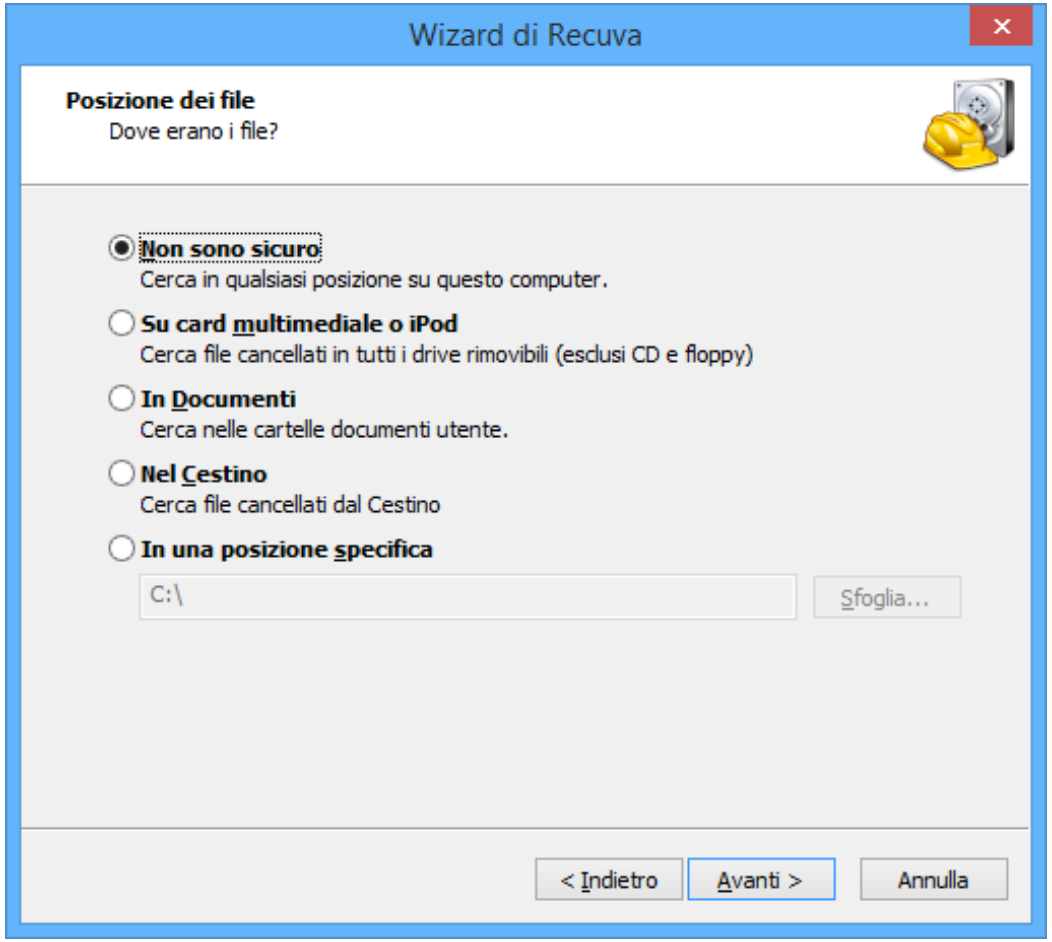


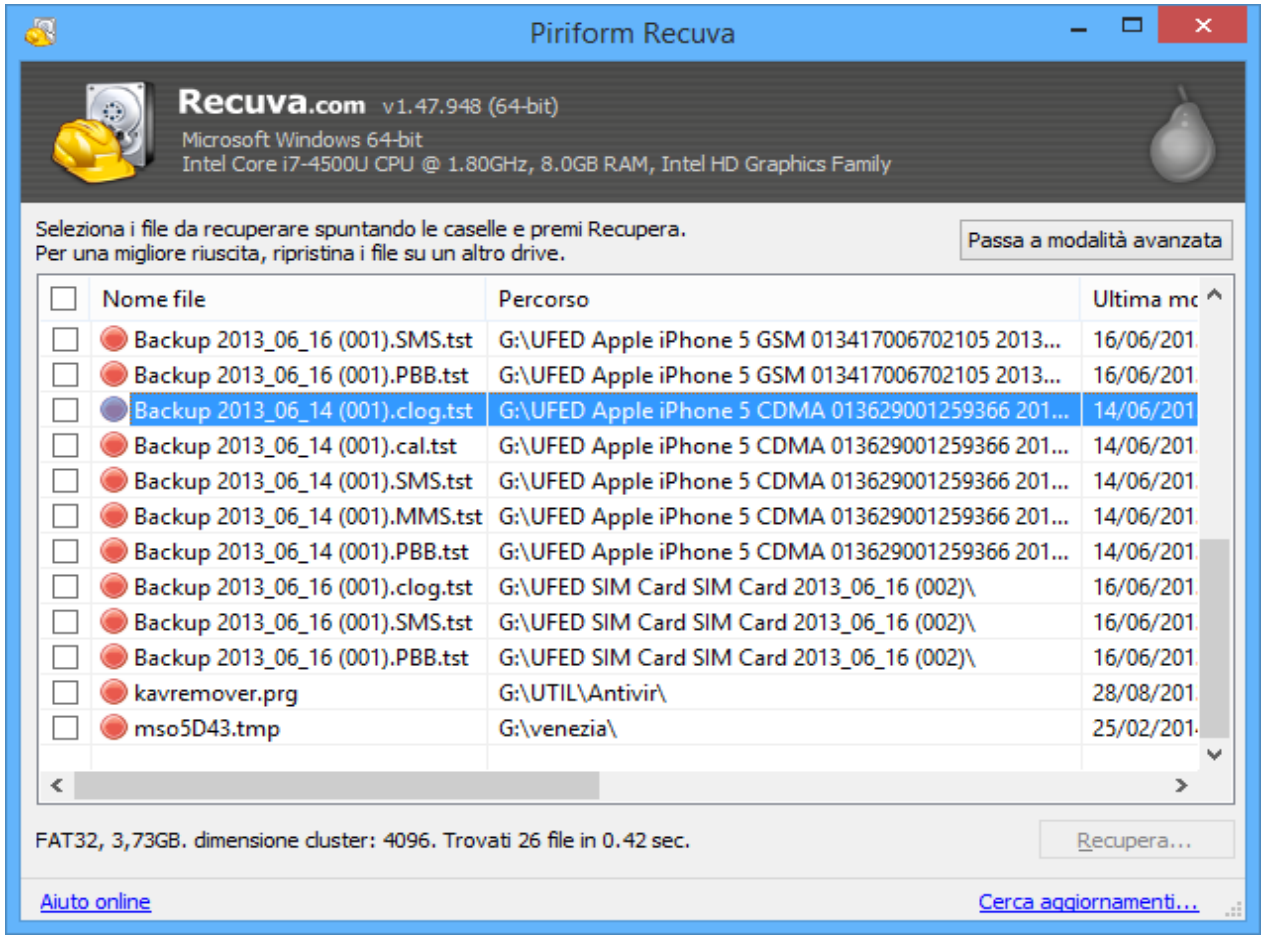
Recuva

- Recuva propone un wizard che guida attraverso varie fasi al recupero di file.



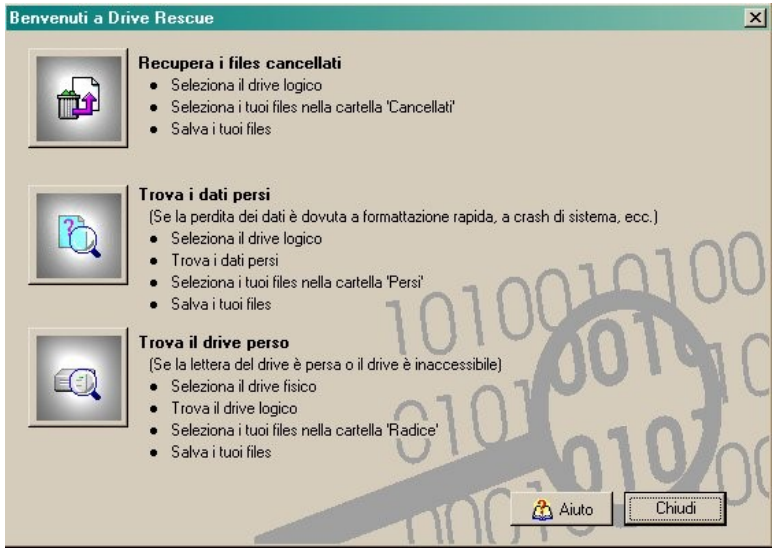

Wizard di Recuva
Tipo di file
Quale tipo di file stai tentando di recuperare?
Tutti i file
Mostra tutti i file.
Immagini
Mostra solo comuni formati di file di immagini, come foto di fotocamere digitali.
Musica
Mostra solo comuni formati di file audio, come file di player MP3.
Documenti
Mostra solo comuni formati di file di documenti, come file di Word ed Excel.
Video
Mostra solo file video, come registrazioni di fotocamere digitali.
Compresso
Mostra solo file compressi
Email
Mostra solo email di Thunderbird, Outlook Express e Windows Mail
< Indietro
Avanti >
Annulla

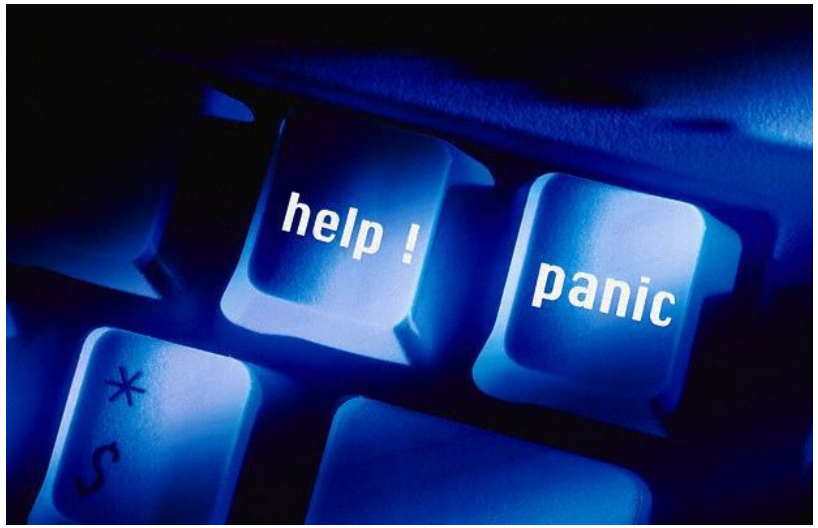

Wizard di Recuva
Posizione dei file
Dove erano i file?
Non sono sicuro
Cerca in qualsiasi posizione su questo computer.
Su card multimediale o iPod
Cerca file cancellati in tutti i drive rimovibili (esclusi CD e floppy)
In Documenti
Cerca nelle cartelle documenti utente.
Nel Cestino
Cerca file cancellati dal Cestino
In una posizione specifica
C:\
Sfoglia...
< Indietro
Avanti >
Annulla


Piriform Recuva
Recuva.com v1.47.948 (64-bit)
Microsoft Windows 64-bit
Intel Core i7-4500U CPU @ 1.80GHz, 8.0GB RAM, Intel HD Graphics Family
Seleziona i file da recuperare spuntando le caselle e premi Recupera.
Per una migliore riuscita, ripristina i file su un altro drive.
Passa a modalità avanzata
Nome file
Percorso
Ultima mc
Backup 2013_06_16 (001).SMS.tst G:\UFED Apple iPhone 5 GSM 013417006702105 2013... 16/06/201
Backup 2013_06_16 (001).PBB.tst G:\UFED Apple iPhone 5 GSM 013417006702105 2013... 16/06/201
Backup 2013_06_14 (001).clog.tst G:\UFED Apple iPhone 5 CDMA 013629001259366 201... 14/06/201
Backup 2013_06_14 (001).cal.tst G:\UFED Apple iPhone 5 CDMA 013629001259366 201... 14/06/201
Backup 2013_06_14 (001).SMS.tst G:\UFED Apple iPhone 5 CDMA 013629001259366 201... 14/06/201
Backup 2013_06_14 (001).MMS.tst G:\UFED Apple iPhone 5 CDMA 013629001259366 201... 14/06/201
Backup 2013_06_14 (001).PBB.tst G:\UFED Apple iPhone 5 CDMA 013629001259366 201... 14/06/201
Backup 2013_06_16 (001).clog.tst G:\UFED SIM Card SIM Card 2013_06_16 (002)\ 16/06/201
Backup 2013_06_16 (001).SMS.tst G:\UFED SIM Card SIM Card 2013_06_16 (002)\ 16/06/201
Backup 2013_06_16 (001).PBB.tst G:\UFED SIM Card SIM Card 2013_06_16 (002)\ 16/06/201
kavremover.prg G:\UTIL\Antivir\ 28/08/201
mso5D43.tmp G:\venezia\ 25/02/201
FAT32, 3,73GB. dimensione cluster: 4096. Trovati 26 file in 0.42 sec.
Recupera...
Aiuto online
Cerca aggiornamenti...

- Ricordiamo che Recuva è uno dei tanti sw ma non è un software di recupero dati professionale e forense….. A volte non riesce a recuperare tutto, ma un utente prima di andare da chi si occupa proprio di Data Recovery, può eseguire una prova da solo.

- Un altro software che riesce ad estrarre molte informazioni è RTT-STUDIO, compatibile sia per piattaforme Windows, MacOS e Linux. Stellar, EASEUS.





La medesima logica vale per:

- Chiavette USB;
- Memory Card;
- Hard Disk;

- Smartphone, Tablet, GPS, etc……

- La **crittografia asimmetrica** è conosciuta anche come crittografia a coppia di chiavi, crittografia a chiave pubblica/privata o anche solo crittografia a chiave pubblica.
  Come si evince dal nome, ogni attore coinvolto possiede una **coppia di chiavi:**

- la **chiave privata**, personale e segreta, viene utilizzata per decodificare un documento criptato;

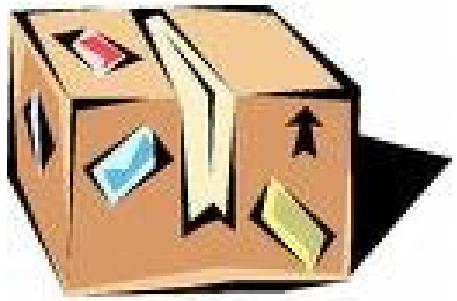
- la **chiave pubblica**, che deve essere distribuita; serve a criptare un documento destinato alla persona che possiede la relativa chiave privata.

- L'idea base della crittografia con coppia di chiavi diviene più chiara se si usa un'analogia postale, in cui il mittente è Alice ed il destinatario Bob.

- I **lucchetti** fanno le veci delle chiavi pubbliche e le chiavi recitano la parte delle chiavi private:

- 1) Alice chiede a Bob di spedirle il suo lucchetto, già aperto. La chiave dello stesso verrà però gelosamente conservata da Bob.

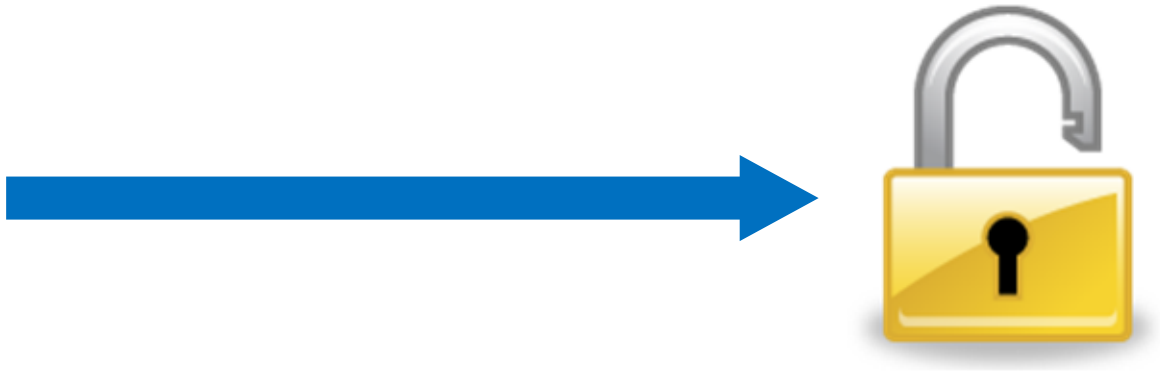
- 2) Alice riceve il **lucchetto** e, con esso, chiude il pacco e lo spedisce a Bob.



+

- 3) Bob riceve il pacco e può aprirlo con la **chiave** di cui è l'unico proprietario.

Se adesso Bob volesse mandare un altro pacco ad Alice, dovrebbe farlo chiudendolo con il ***lucchetto*** di Alice, che lei dovrebbe mandare a Bob e che solo lei potrebbe aprire.
Si può notare come per "***chiudere***" i pacchi ci sia bisogno del ***lucchetto*** **del destinatario** mentre per ricevere viene usata esclusivamente la **propria *chiave* segreta**, rendendo l'intero processo di criptazione/decriptazione asimmetrico.



Ricapitoliamo:

Una **chiave pubblica** è una chiave crittografica utilizzata in un sistema di crittografia asimmetrica; ogni **chiave pubblica** è associata ad una **chiave privata**.

- La caratteristica dei crittosistemi asimmetrici è che ogni coppia di chiavi è formata in modo tale che ciò che viene cifrato con una, può essere decifrato solo con l'altra.
- Le due chiavi sono, a priori, perfettamente interscambiabili, ma generalmente una delle due viene definita "pubblica" e una "privata" perché il poter distribuire una (e una sola!) delle due è il principale vantaggio dei crittosistemi asimmetrici.

Le chiavi pubbliche *possono essere scambiate anche su un canale non sicuro* (via e-mail, tramite un key server, su una pagina web o quant'altro), l'importante è sapere che una chiave pubblica non è di per sé associata a una "persona", ma esclusivamente ad una chiave privata. Per associarla ad una persona si fa generalmente uso di un **certificato digitale**

Le chiavi private ***non devono essere scambiate né conosciute da nessuno*** che non sia il legittimo proprietario.
Per maggiore sicurezza la maggior parte dei programmi memorizza su disco la chiave privata solo cifrata con una password definita dall'utente.
Quando si teme che una chiave privata sia stata letta da terzi, la cosa migliore da fare è revocarla.

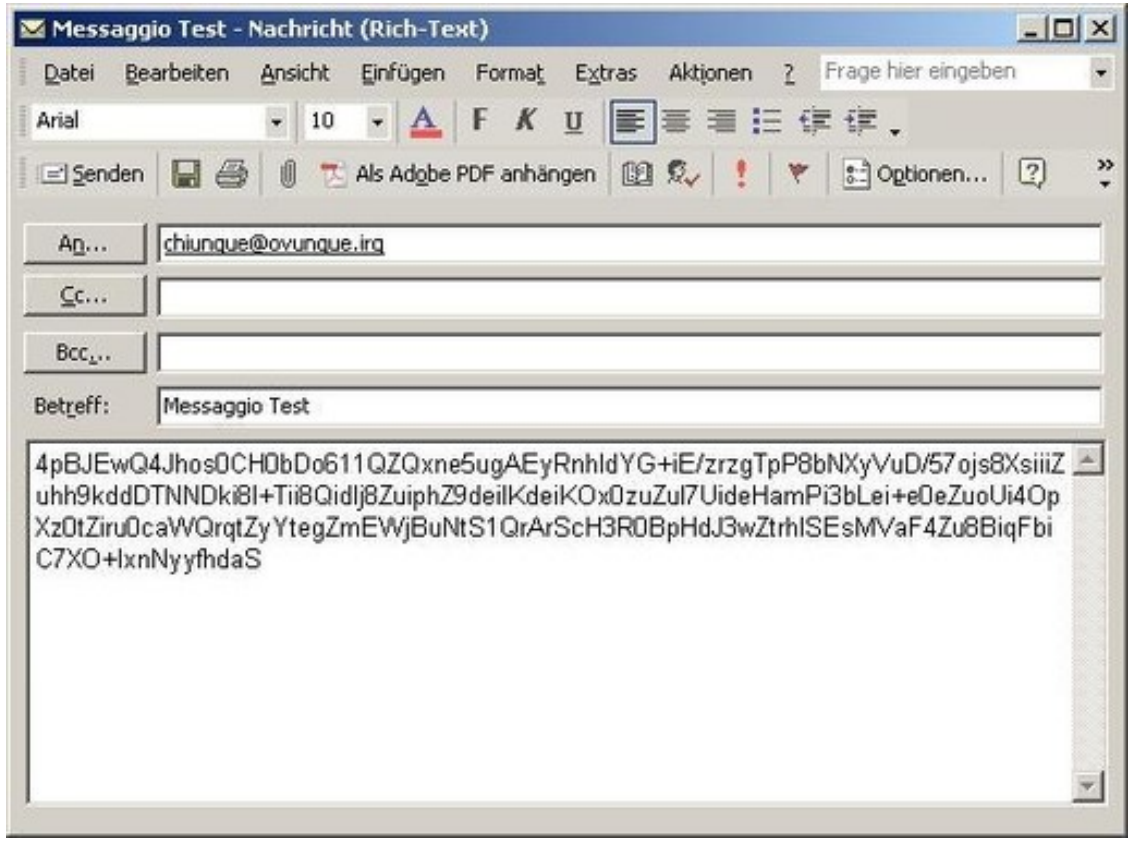
- Pretty Good Privacy (PGP) è un programma che permette di usare autenticazione e privacy crittografica. Nelle sue varie versioni è probabilmente il crittosistema più usato al mondo. In Applied Cryptography, il crittografo Bruce Schneier lo ha descritto come il modo per arrivare "probabilmente il più vicino alla crittografia di livello militare"

- PGP è stato originariamente sviluppato da Phil Zimmermann nel 1991. Attualmente è un programma proprietario venduto su licenza.

- Utilizza le librerie Open Source OpenPGP, il che ha permesso di creare una alternativa libera chiamata GPG, GNU Privacy Guard , totalmente compatibile con lo standard IETF.

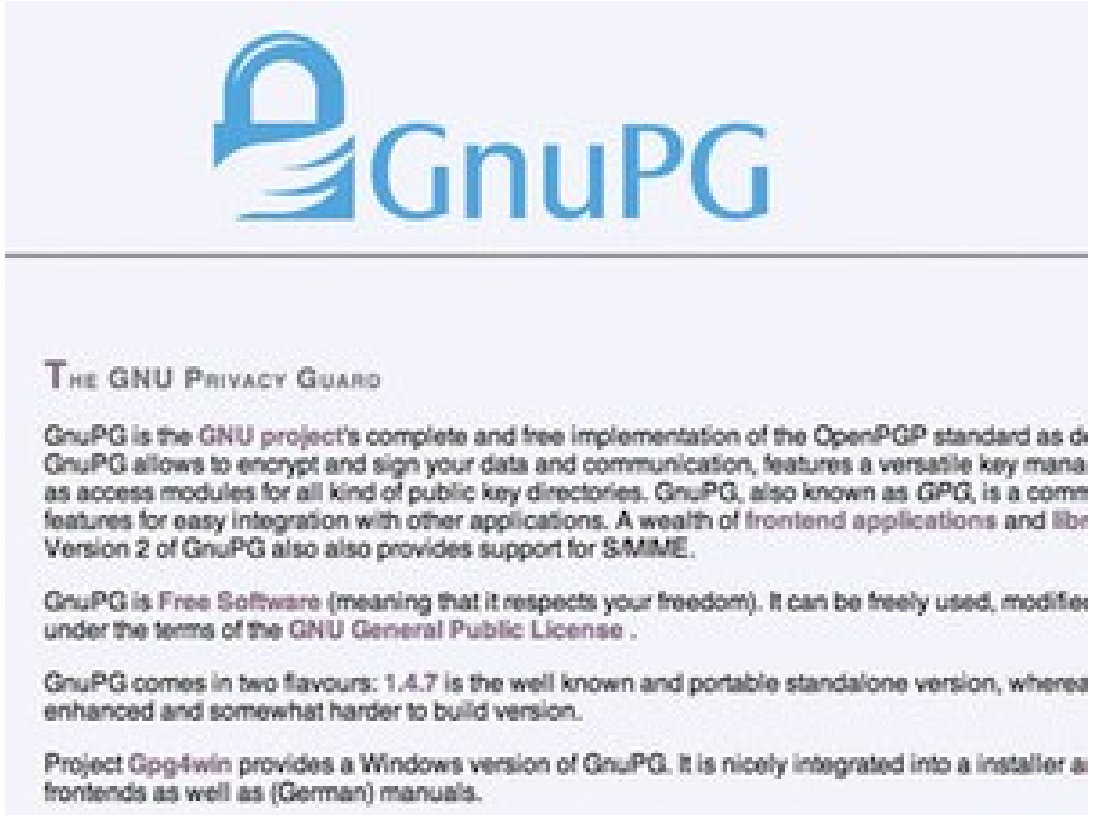
- Thunderbird, Client di posta elettronica Open Source
- Enigmail, addon per Thunderbird
- GPG4Win, pacchetto per gestione della cifratura asimmetrica per mail e file, si integra con Enigmail e comprende il software Kleopatra per la criptazione dei file

Come cifrare email, file usando PGP, GPG



Università di Roma

Creare una chiave pubblica e privata



Università di Roma

Differenza tra chiave pubblica e privata

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.22 (MingW32)

mQENBE+gdaIBCACyiD1GasakMZaiim/EgKxoxSe+Nr7LdjGCAqh/uzf7rtezViRz
q06BFjwPvSEWclrL3aMNFduWEzUm3wqncd71kz+jqA82CRqvB1eaPj90J8ghzEvZ
Nok+1U+a033eDTbbT7QG0/riLaYG78y0MgCsn65rVkkfC+y7/b3fls+nunUHN5Pn
WCPTwJKivE4KUvQyVjQuFZVZydZNaJA23oU2kohKPH6OIH+gHXiWyYCaIhEBWNJQ
ZrNoymSjH9QOCaCBjhWUrjdOPuScebq18CU11RmmalH/dqN79QD/UFQM1iIol/cL

VeraCrypt

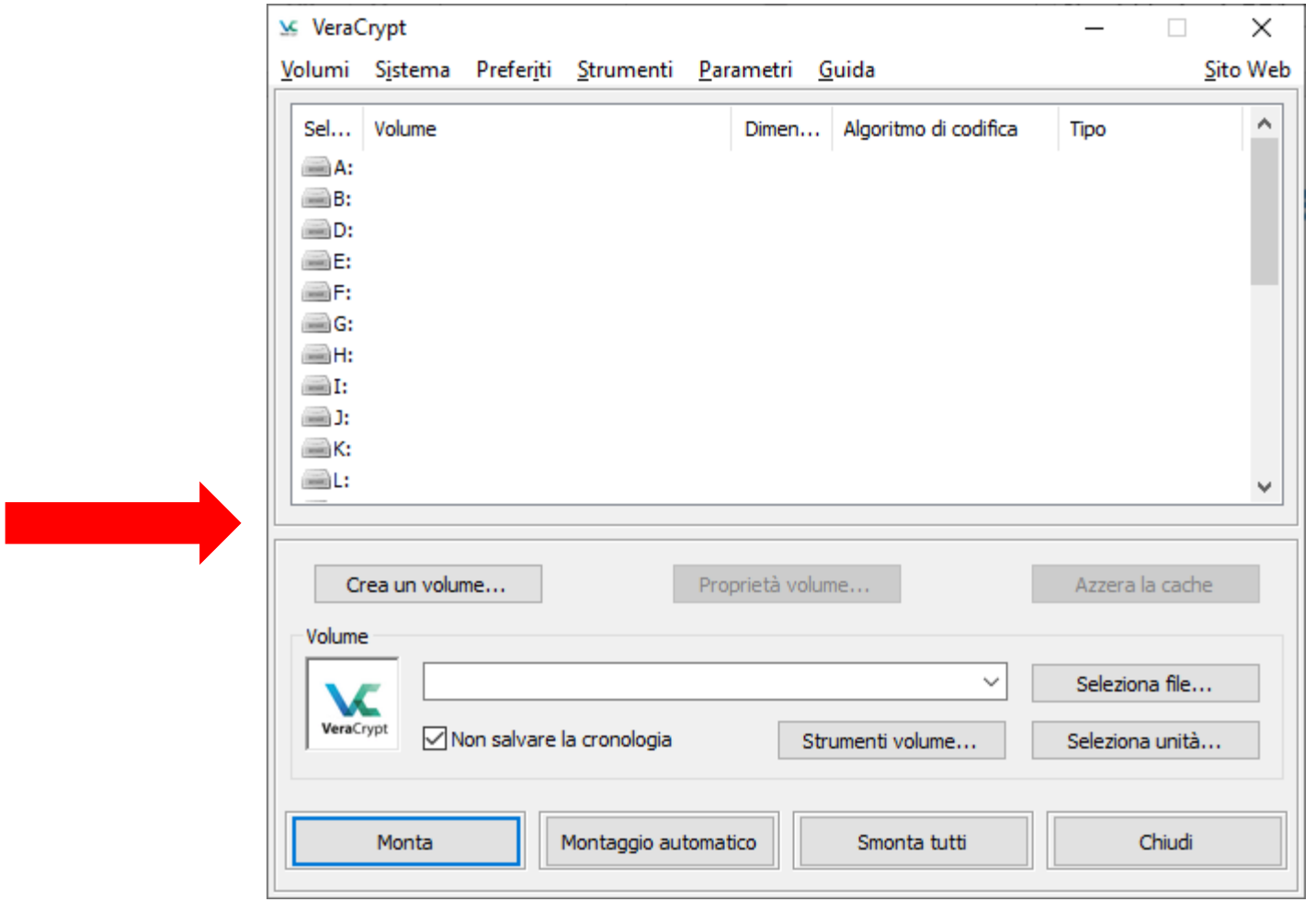
https://www.veracrypt.fr/en/Downloads.html

Security concerns. **TrueCrypt** is vulnerable to various known attacks which are also present in other software-based disk encryption software such as BitLocker. To prevent those, the documentation distributed with **TrueCrypt** requires users to follow various **security** precautions.

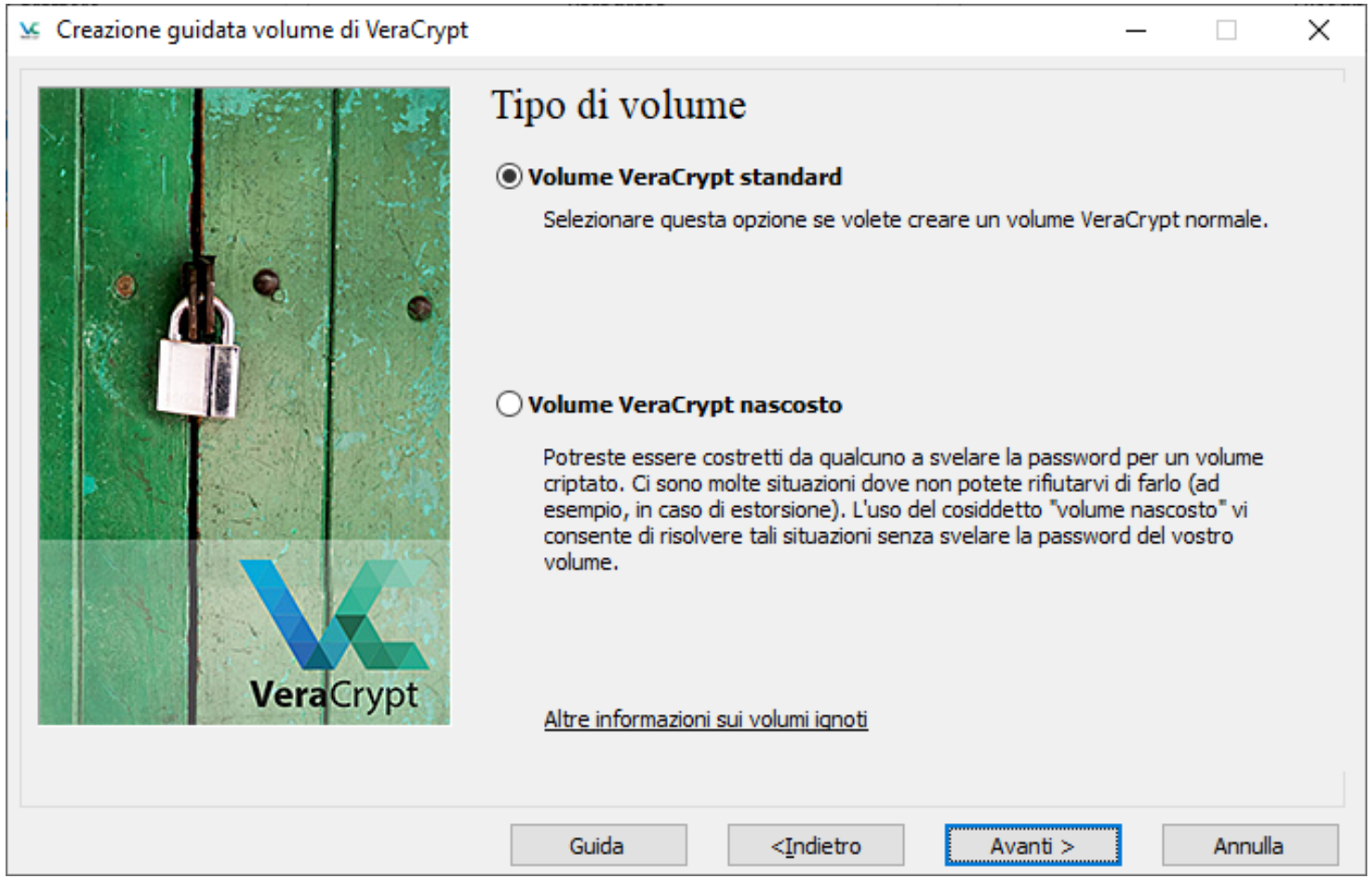
en.wikipedia.org › wiki › TrueCrypt ▾

TrueCrypt - Wikipedia

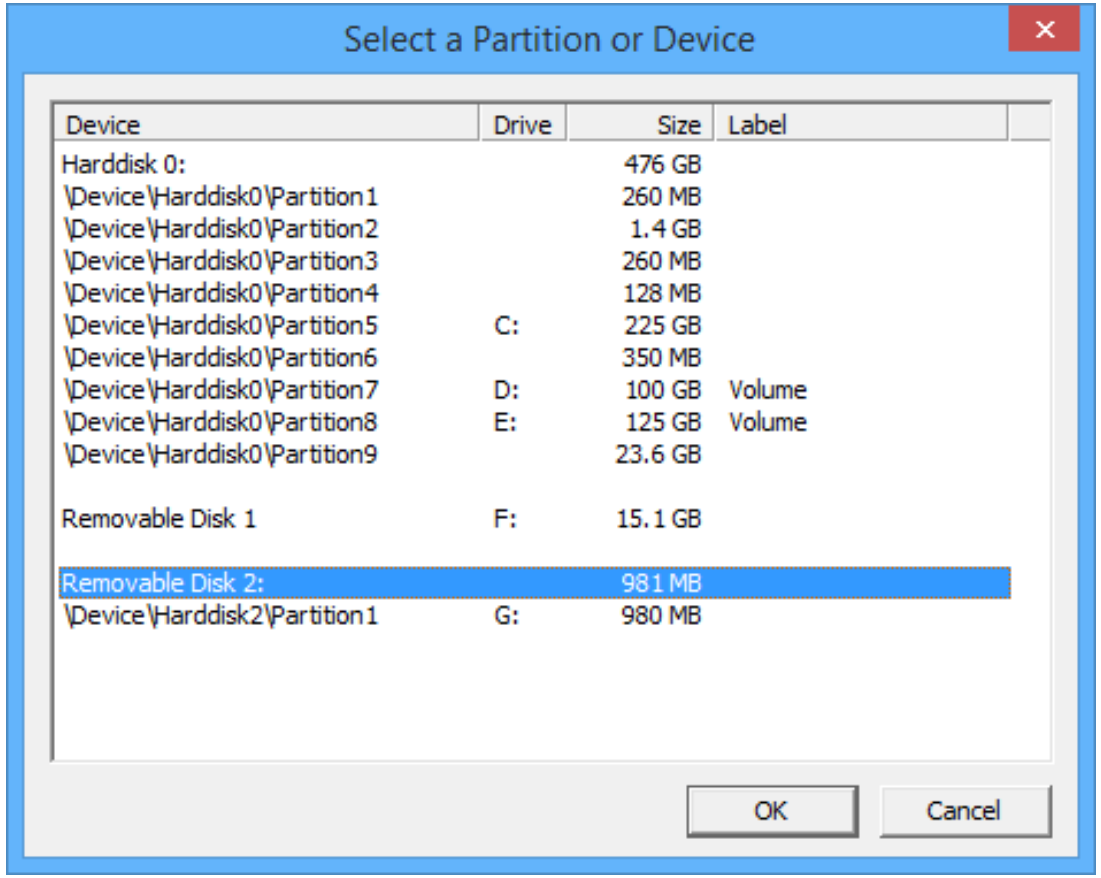
https://www.veracrypt.fr/en/Downloads.html

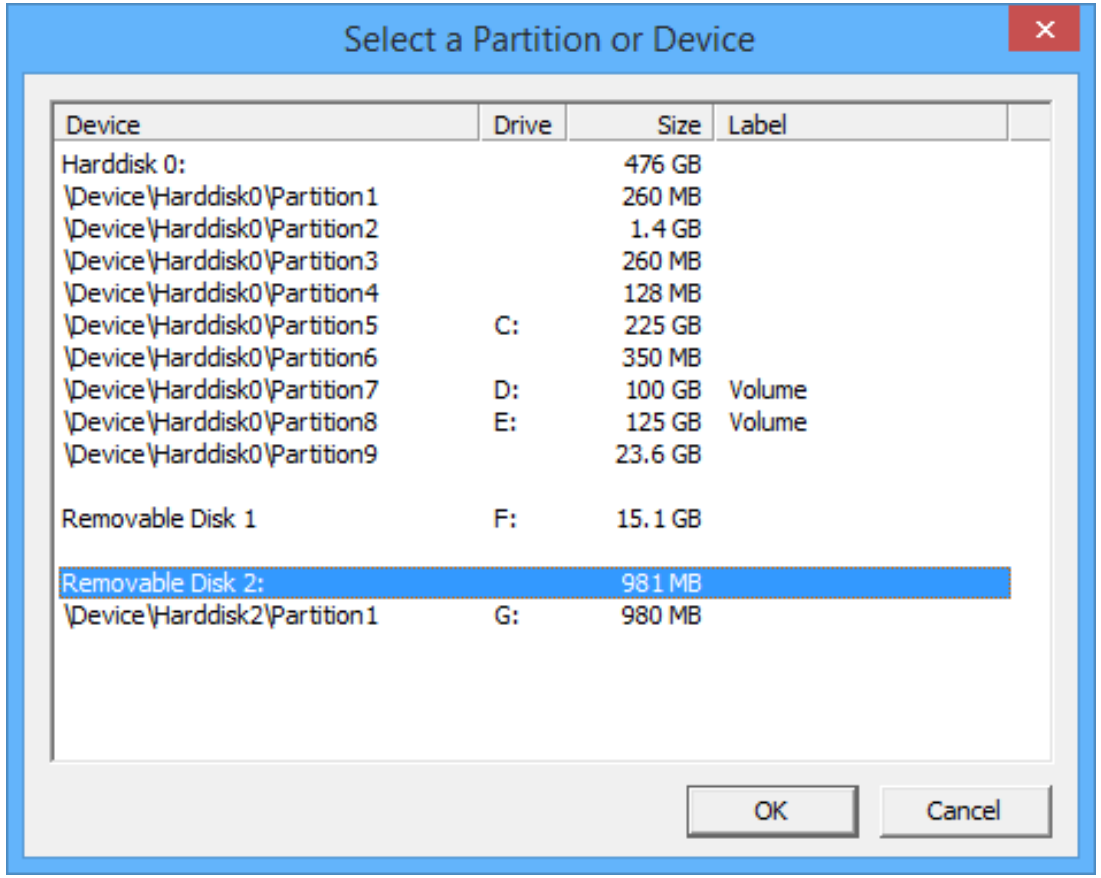

VeraCrypt
Volumi
Sistema
Preferiti
Strumenti
Parametri
Guida
Sito Web
Sel...
Volume
Dimen...
Algoritmo di codifica
Tipo
A:
B:
D:
E:
F:
G:
H:
I:
J:
K:
L:
Crea un volume...
Proprietà volume...
Azzera la cache
Volume
VeraCrypt
Seleziona file...
Non salvare la cronologia
Strumenti volume...
Seleziona unità...
Monta
Montaggio automatico
Smonta tutti
Chiudi

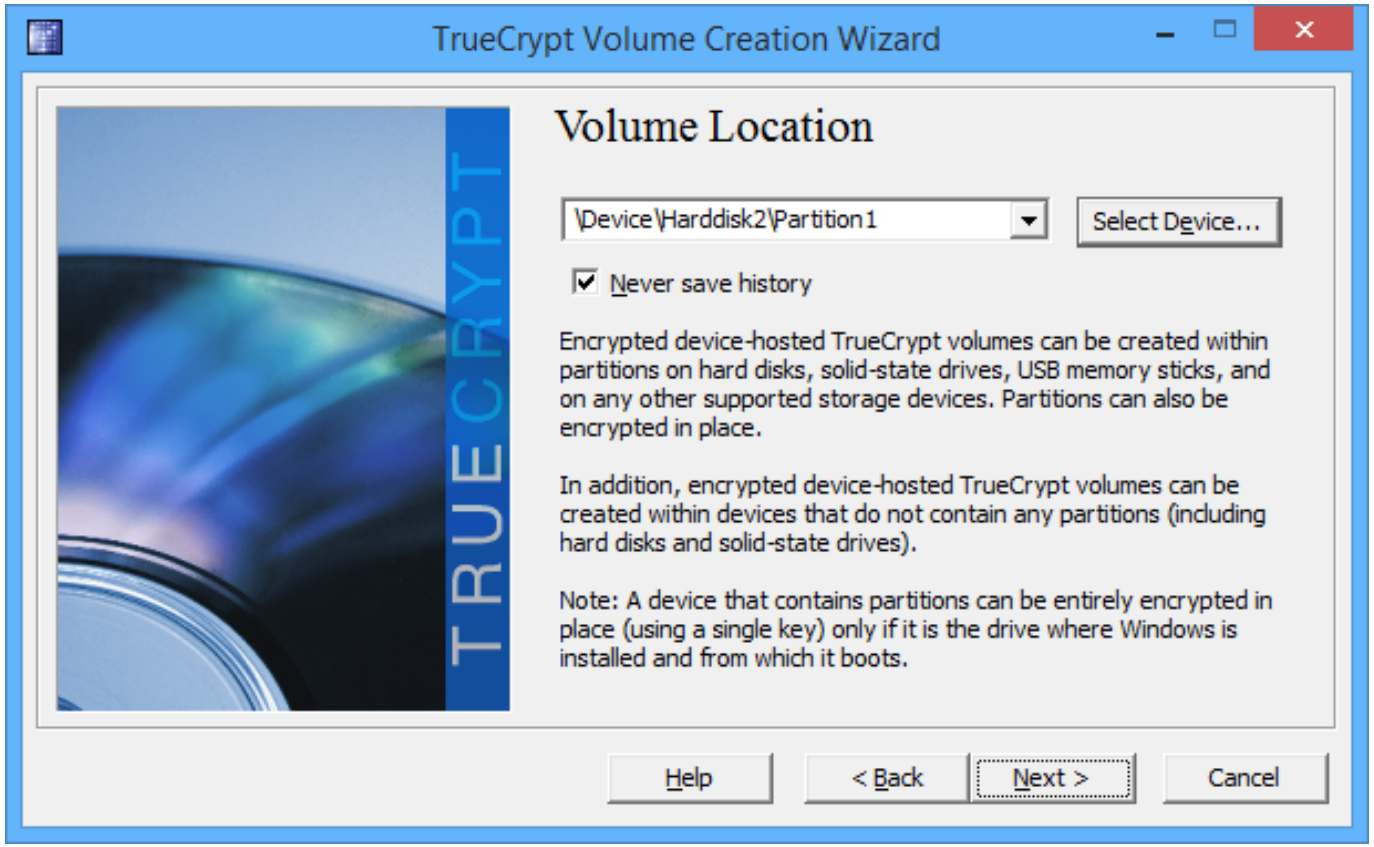

Creazione guidata volume di VeraCrypt
Creazione guidata volume VeraCrypt
VeraCrypt
Crea un file contenitore criptato
Crea un disco virtuale criptato all'interno di un file. Raccomandato per utenti inesperti.
Altre informazioni
Codifica una partizione/disco non di sistema
Codifica una partizione non di sistema o qualsiasi disco interno o esterno (es. un flash drive). Eventualmente crea un volume nascosto.
Codifica la partizione o tutto il disco di sistema
Codifica la partizione/disco dove Windows è installato. Chi vuole avere l'accesso ed usare il sistema, leggere e scrivere file, ecc, deve digitare ogni volta la password corretta prima dell'avvio di Windows. In alternativa, crea un sistema nascosto.
Altre informazioni sulla codifica di sistema
Guida
<Indietro
Avanti >
Annulla

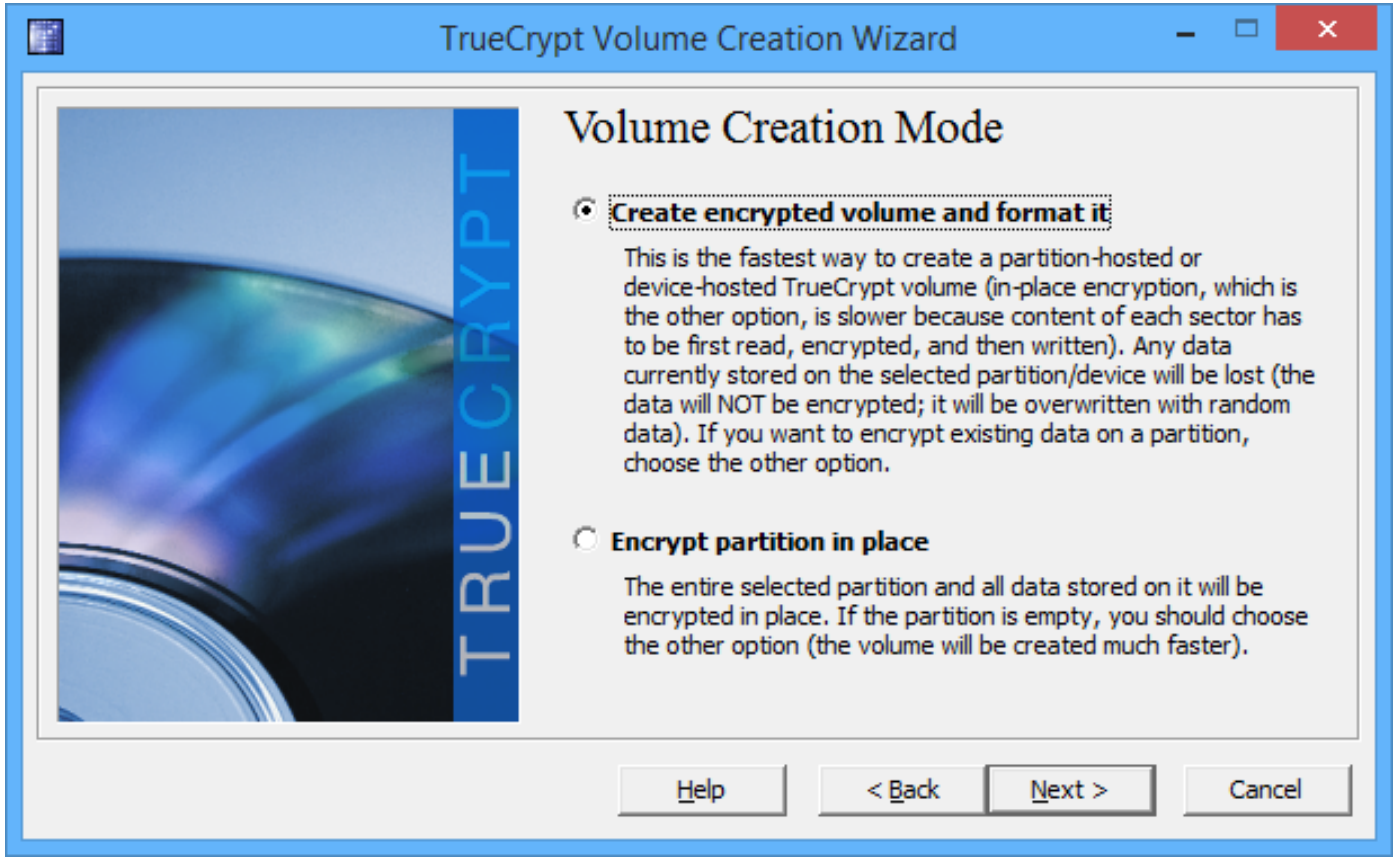

Creazione guidata volume di VeraCrypt
Tipo di volume
Volume VeraCrypt standard
Selezionare questa opzione se volete creare un volume VeraCrypt normale.
Volume VeraCrypt nascosto
Potreste essere costretti da qualcuno a svelare la password per un volume criptato. Ci sono molte situazioni dove non potete rifiutarvi di farlo (ad esempio, in caso di estorsione). L'uso del cosiddetto "volume nascosto" vi consente di risolvere tali situazioni senza svelare la password del vostro volume.
Altre informazioni sui volumi ignoti
VeraCrypt
Guida
<Indietro
Avanti >
Annulla


Creazione guidata volume di VeraCrypt
Percorso del volume
Seleziona file...
Non salvare la cronologia
Un volume VeraCrypt può risiedere in un file (chiamato VeraCrypt contenitore), che può risiedere in un disco rigido, su un'unità flash USB, ecc. Un contenitore VeraCrypt è simile a qualsiasi altro file normale (può essere, ad esempio, spostato o cancellato come un qualsiasi altro file). Fate clic su 'Seleziona file' per scegliere un nome file per il contenitore e selezionare il percorso dove esso deve essere creato.
ATTENZIONE: Selezionando un file esistente, VeraCrypt NON lo cifrerà; il file sarà eliminato e sostituito con il file contenitore VeraCrypt creato nuovamente. Potrete cifrare i file esistenti (in seguito) muovendoli nel contenitore VeraCrypt che state creando adesso.
VeraCrypt
Guida
<Indietro
Avanti >
Annulla


Select a Partition or Device
Device
Drive
Size
Label
Harddisk 0: 476 GB
\Device\Harddisk0\Partition1 260 MB
\Device\Harddisk0\Partition2 1.4 GB
\Device\Harddisk0\Partition3 260 MB
\Device\Harddisk0\Partition4 128 MB
\Device\Harddisk0\Partition5 C: 225 GB
\Device\Harddisk0\Partition6 350 MB
\Device\Harddisk0\Partition7 D: 100 GB Volume
\Device\Harddisk0\Partition8 E: 125 GB Volume
\Device\Harddisk0\Partition9 23.6 GB
Removable Disk 1 F: 15.1 GB
Removable Disk 2: 981 MB
\Device\Harddisk2\Partition1 G: 980 MB
OK
Cancel

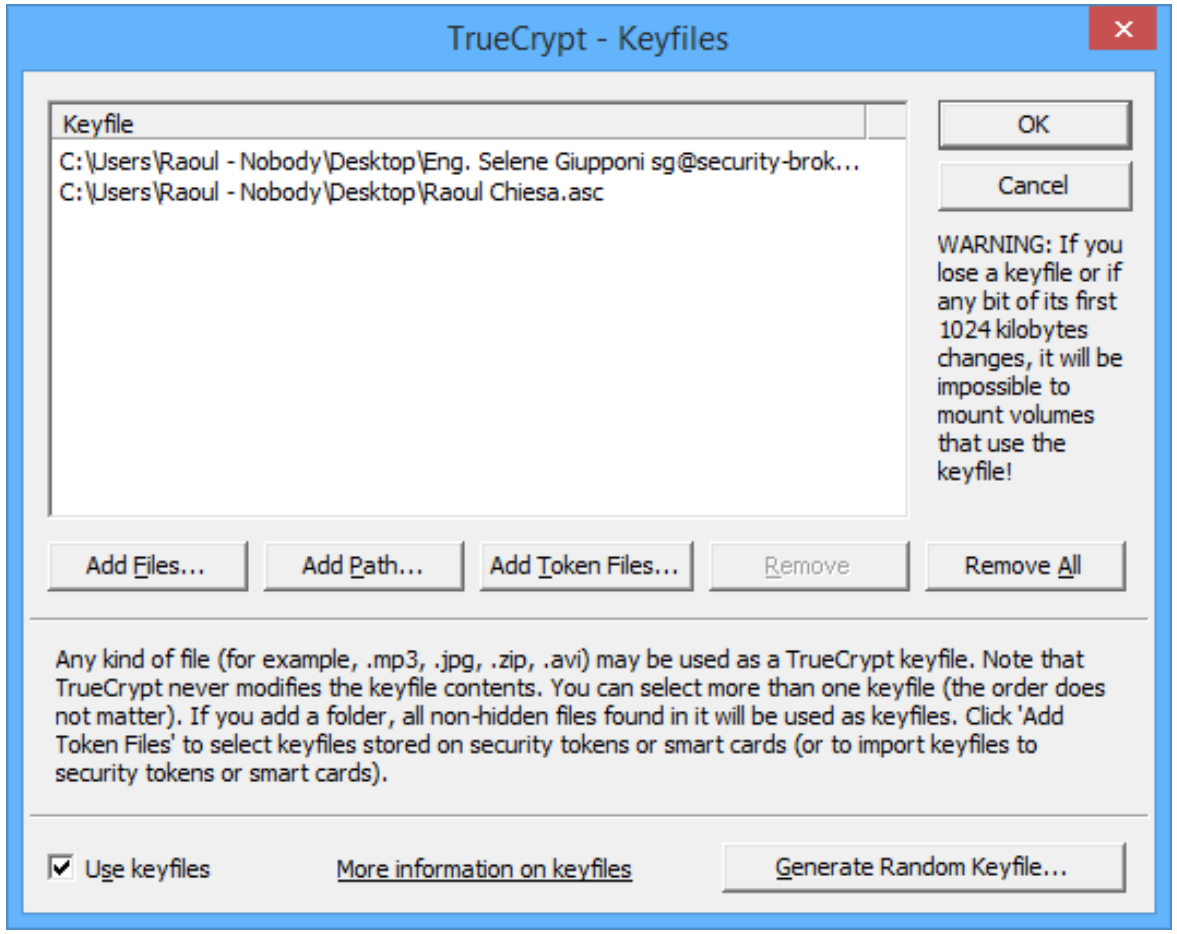

Select a Partition or Device
Device
Drive
Size
Label
Harddisk 0: 476 GB
\Device\Harddisk0\Partition1 260 MB
\Device\Harddisk0\Partition2 1.4 GB
\Device\Harddisk0\Partition3 260 MB
\Device\Harddisk0\Partition4 128 MB
\Device\Harddisk0\Partition5 C: 225 GB
\Device\Harddisk0\Partition6 350 MB
\Device\Harddisk0\Partition7 D: 100 GB Volume
\Device\Harddisk0\Partition8 E: 125 GB Volume
\Device\Harddisk0\Partition9 23.6 GB
Removable Disk 1 F: 15.1 GB
Removable Disk 2: 981 MB
\Device\Harddisk2\Partition1 G: 980 MB
OK
Cancel


TrueCrypt Volume Creation Wizard
TRUECRYPT
Volume Location
\Device\Harddisk2\Partition1
Select Device...
Never save history
Encrypted device-hosted TrueCrypt volumes can be created within partitions on hard disks, solid-state drives, USB memory sticks, and on any other supported storage devices. Partitions can also be encrypted in place.
In addition, encrypted device-hosted TrueCrypt volumes can be created within devices that do not contain any partitions (including hard disks and solid-state drives).
Note: A device that contains partitions can be entirely encrypted in place (using a single key) only if it is the drive where Windows is installed and from which it boots.
Help
< Back
Next >
Cancel

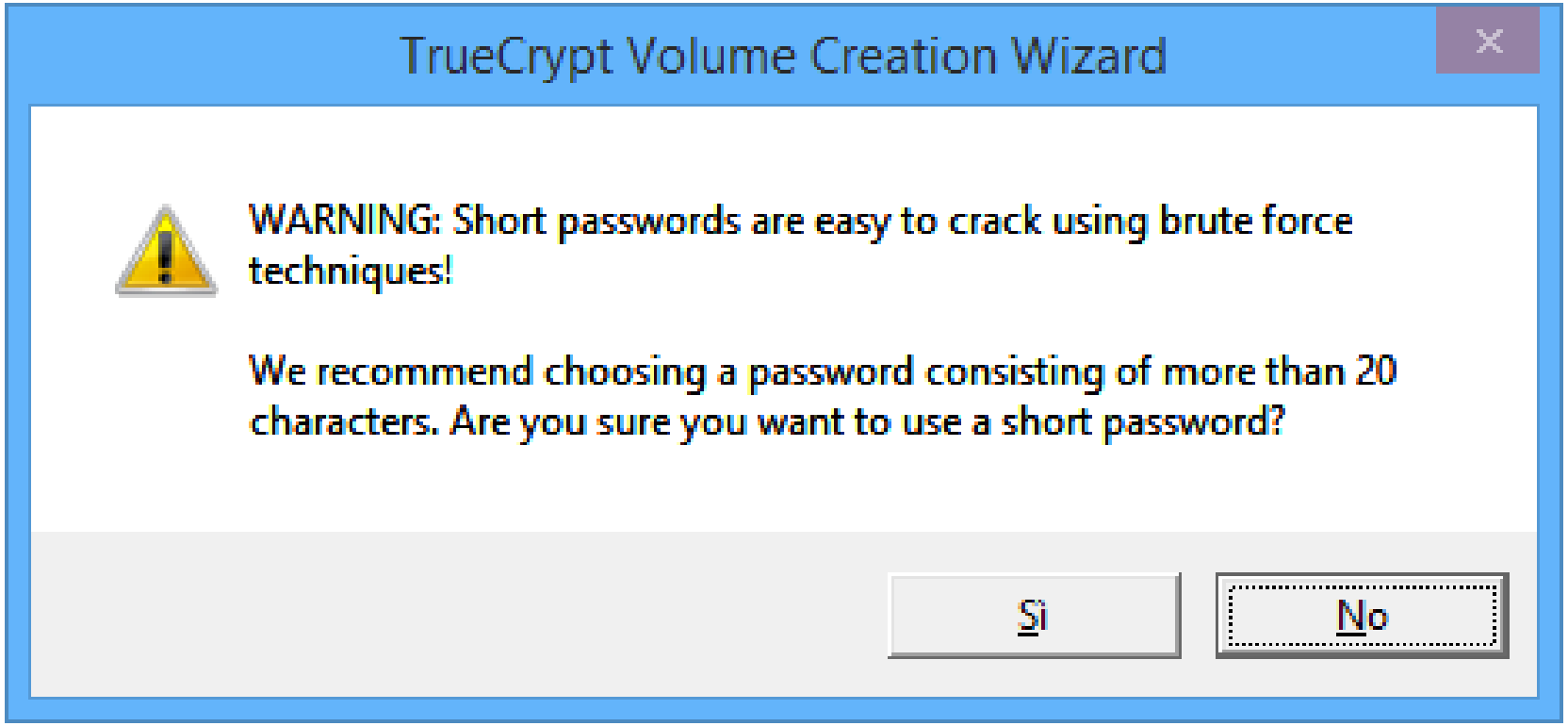

TrueCrypt Volume Creation Wizard
TRUECRYPT
Volume Creation Mode
Create encrypted volume and format it
This is the fastest way to create a partition-hosted or device-hosted TrueCrypt volume (in-place encryption, which is the other option, is slower because content of each sector has to be first read, encrypted, and then written). Any data currently stored on the selected partition/device will be lost (the data will NOT be encrypted; it will be overwritten with random data). If you want to encrypt existing data on a partition, choose the other option.
Encrypt partition in place
The entire selected partition and all data stored on it will be encrypted in place. If the partition is empty, you should choose the other option (the volume will be created much faster).
Help
< Back
Next >
Cancel

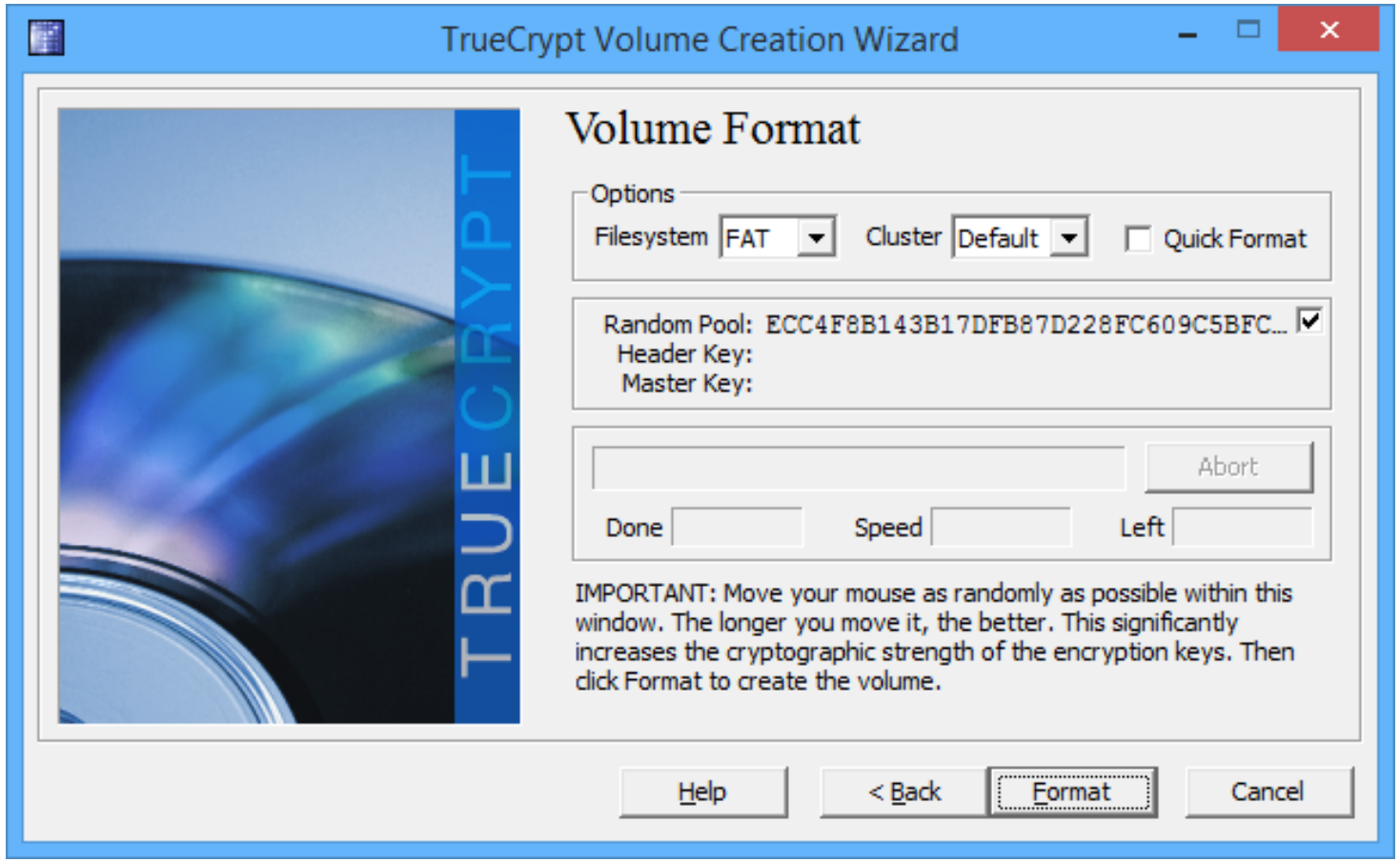

TrueCrypt Volume Creation Wizard
Encryption Options
TRUECRYPT
Encryption Algorithm
AES
Test
AES
Serpent
Twofish
AES-Twofish
AES-Twofish-Serpent
Serpent-AES
Serpent-Twofish-AES
Twofish-Serpent
1998) that may be
agencies to protect
evel. 256-bit key,
of operation is XTS.
Benchmark
Hash Algorithm
RIPEMD-160
Information on hash algorithms
Help
< Back
Next >
Cancel

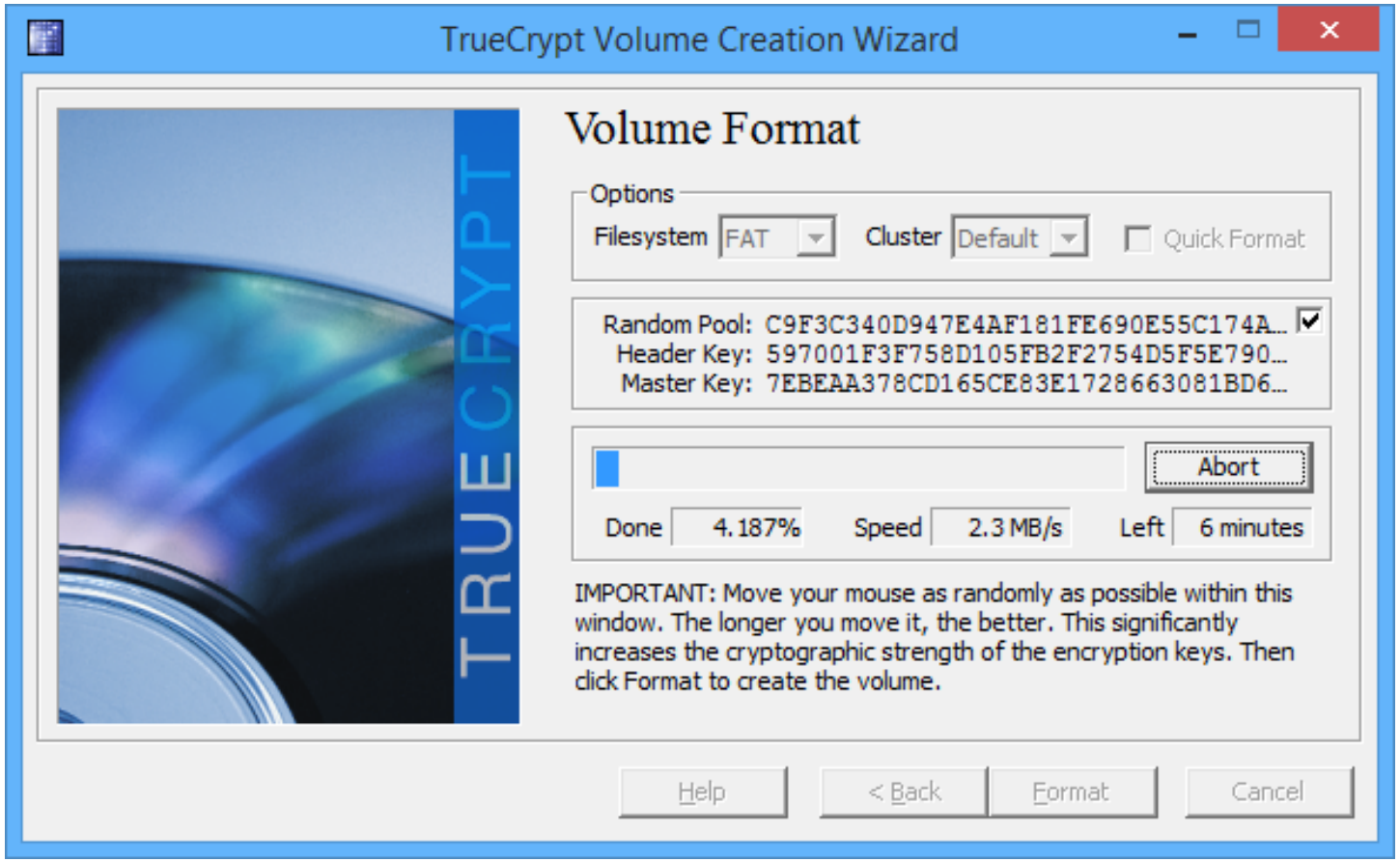

TrueCrypt Volume Creation Wizard
TRUECRYPT
Volume Password
Password:
Confirm:
Use keyfiles
Keyfiles...
Display password
It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of more than 20 characters (the longer, the better). The maximum possible length is 64 characters.
Help
< Back
Next >
Cancel


TrueCrypt - Keyfiles
Keyfile
C:\Users\Raoul - Nobody\Desktop\Eng. Selene Giupponi sg@security-brok...
C:\Users\Raoul - Nobody\Desktop\Raoul Chiesa.asc
OK
Cancel
WARNING: If you lose a keyfile or if any bit of its first 1024 kilobytes changes, it will be impossible to mount volumes that use the keyfile!
Add Files...
Add Path...
Add Token Files...
Remove
Remove All
Any kind of file (for example, .mp3, .jpg, .zip, .avi) may be used as a TrueCrypt keyfile. Note that TrueCrypt never modifies the keyfile contents. You can select more than one keyfile (the order does not matter). If you add a folder, all non-hidden files found in it will be used as keyfiles. Click 'Add Token Files' to select keyfiles stored on security tokens or smart cards (or to import keyfiles to security tokens or smart cards).
Use keyfiles
More information on keyfiles
Generate Random Keyfile...

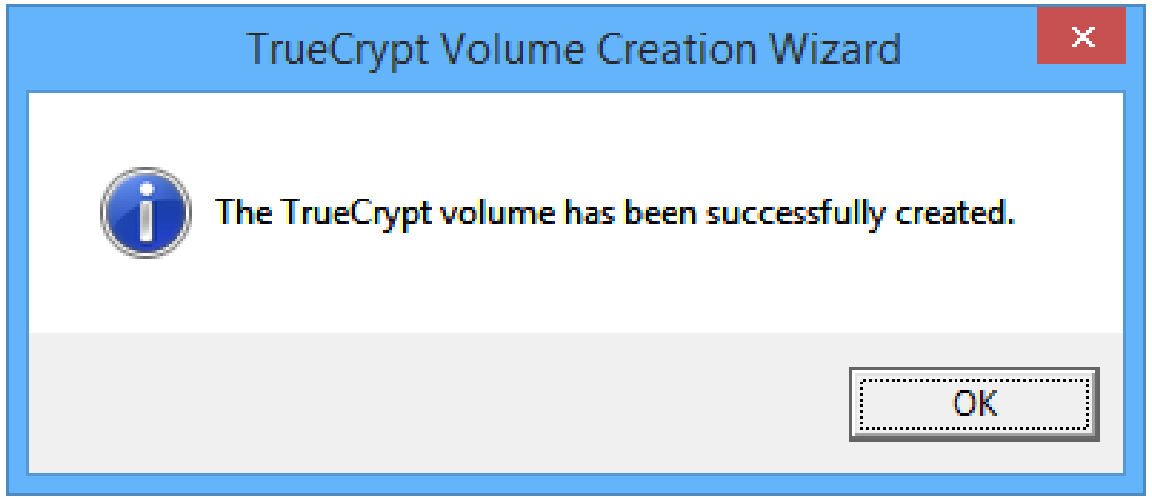

TrueCrypt Volume Creation Wizard
TRUECRYPT
Volume Password
Password:
V3G@20!4
Confirm:
V3G@20!4
Use keyfiles
Display password
Keyfiles...
It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of more than 20 characters (the longer, the better). The maximum possible length is 64 characters.
Help
< Back
Next >
Cancel

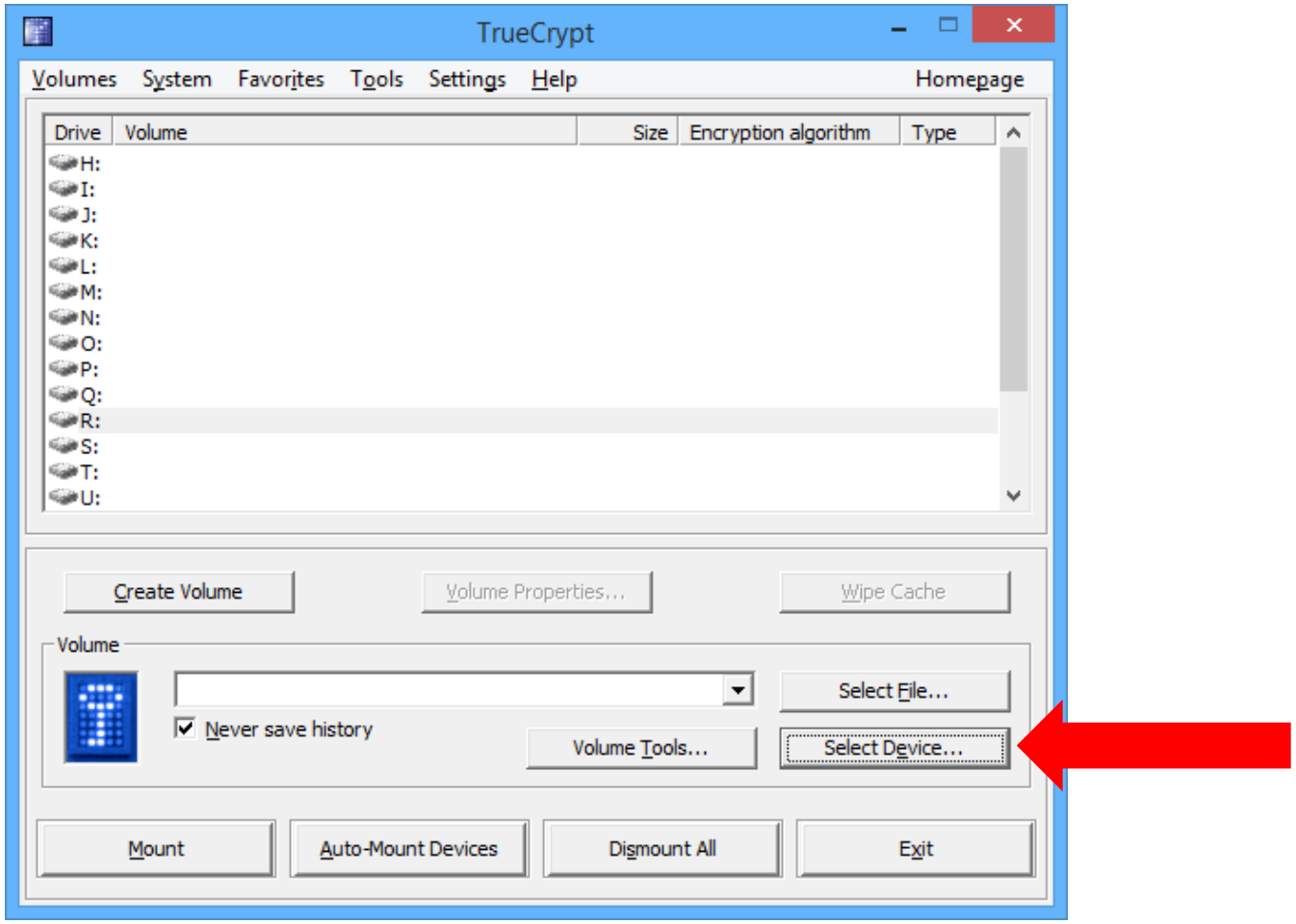

TrueCrypt Volume Creation Wizard
WARNING: Short passwords are easy to crack using brute force techniques!
We recommend choosing a password consisting of more than 20 characters. Are you sure you want to use a short password?
Si
No

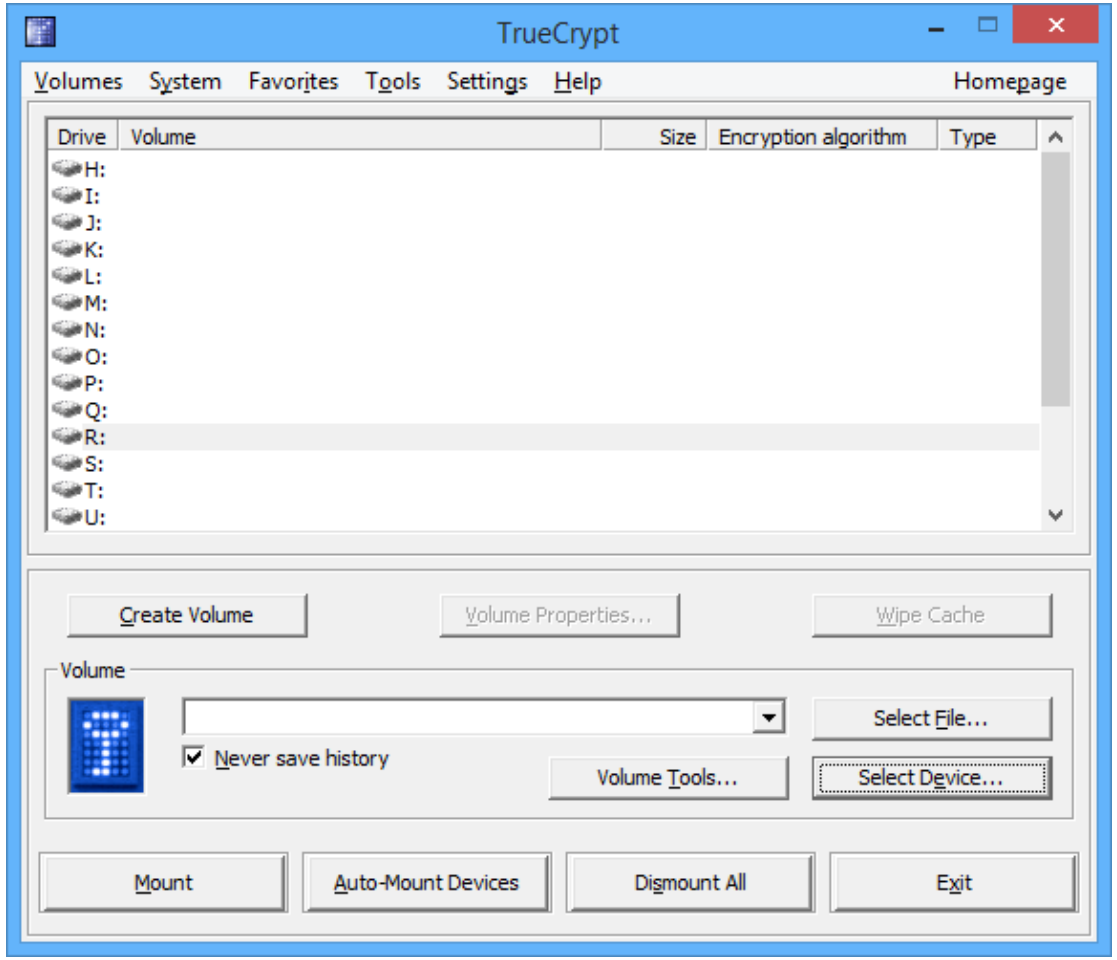

TrueCrypt Volume Creation Wizard
TRUECRYPT
Volume Format
Options
Filesystem FAT
Cluster Default
Quick Format
Random Pool: ECC4F8B143B17DFB87D228FC609C5BFC...
Header Key:
Master Key:
Abort
Done
Speed
Left
IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.
Help
< Back
Format
Cancel

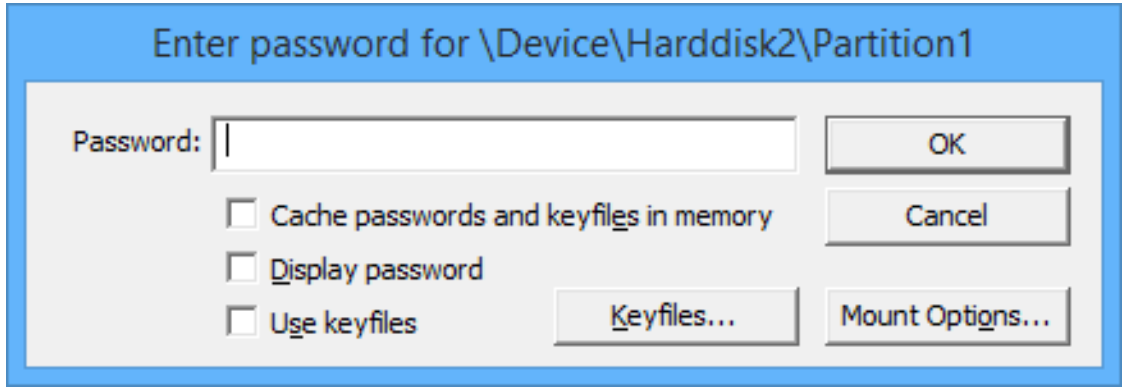

TrueCrypt Volume Creation Wizard
TRUECRYPT
Volume Format
Options
Filesystem FAT
Cluster Default
Quick Format
Random Pool: C9F3C340D947E4AF181FE690E55C174A...
Header Key: 597001F3F758D105FB2F2754D5F5E790...
Master Key: 7EBEAA378CD165CE83E1728663081BD6...
Abort
Done 4.187%
Speed 2.3 MB/s
Left 6 minutes
IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.
Help
< Back
Format
Cancel

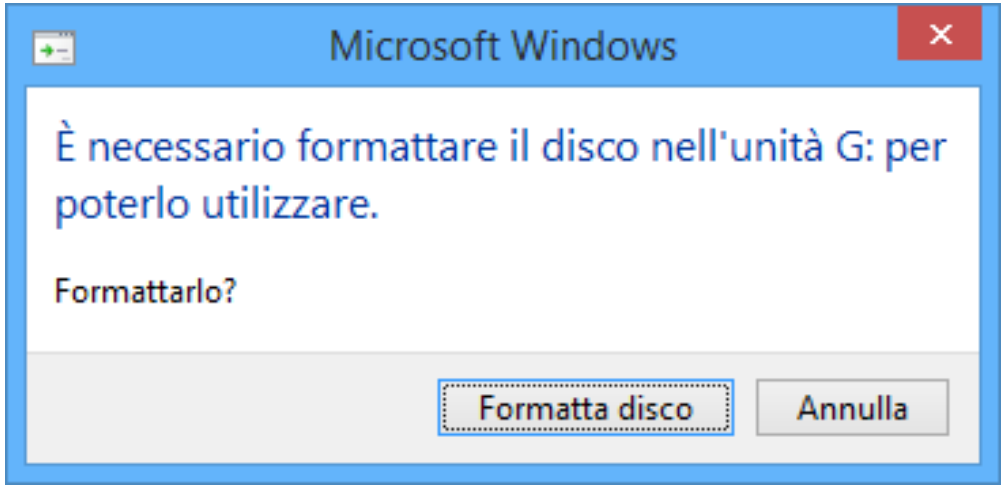

TrueCrypt Volume Creation Wizard
IMPORTANT: Please keep in mind that this volume can NOT be mounted/accessed using the drive letter G:, which is currently assigned to it!
To mount this volume, click 'Auto-Mount Devices' in the main TrueCrypt window (alternatively, in the main TrueCrypt window, click 'Select Device', then select this partition/device, and click 'Mount'). The volume will be mounted to a different drive letter, which you select from the list in the main TrueCrypt window.
The original drive letter G: should be used only in case you need to remove encryption from the partition/device (e.g., if you no longer need encryption). In such a case, right-click the drive letter G: in the 'Computer' (or 'My Computer') list and select 'Format'. Otherwise, the drive letter G: should never be used (unless you remove it, as described e.g. in the TrueCrypt FAQ, and assign it to another partition/device).
OK


TrueCrypt Volume Creation Wizard
The TrueCrypt volume has been successfully created.
OK


TrueCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption algorithm Type
H:
I:
J:
K:
L:
M:
N:
O:
P:
Q:
R:
S:
T:
U:
Create Volume
Volume Properties...
Wipe Cache
Volume
Select File...
Never save history
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit

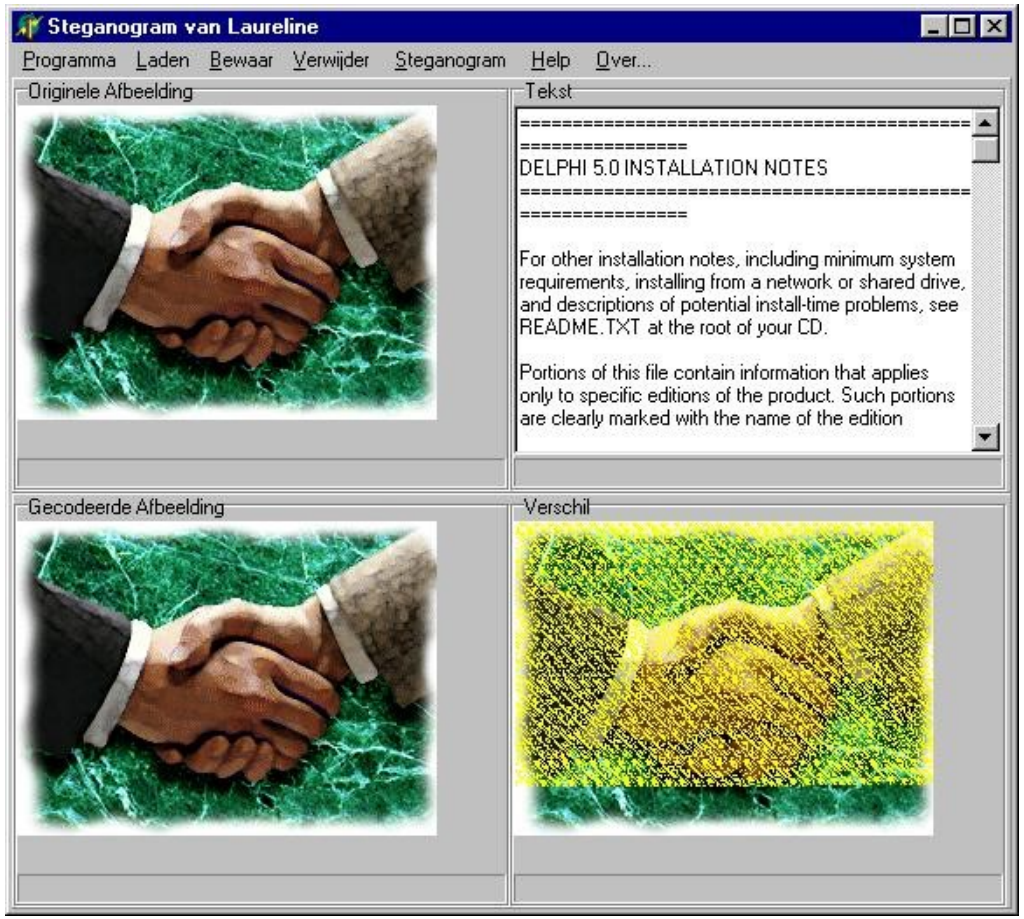

TrueCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption algorithm Type
H:
I:
J:
K:
L:
M:
N:
O:
P:
Q:
R:
S:
T:
U:
Create Volume
Volume Properties...
Wipe Cache
Volume
Never save history
Volume Tools...
Select File...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit


Enter password for \Device\Harddisk2\Partition1
Password:
OK
Cancel
Cache passwords and keyfiles in memory
Display password
Use keyfiles
Keyfiles...
Mount Options...

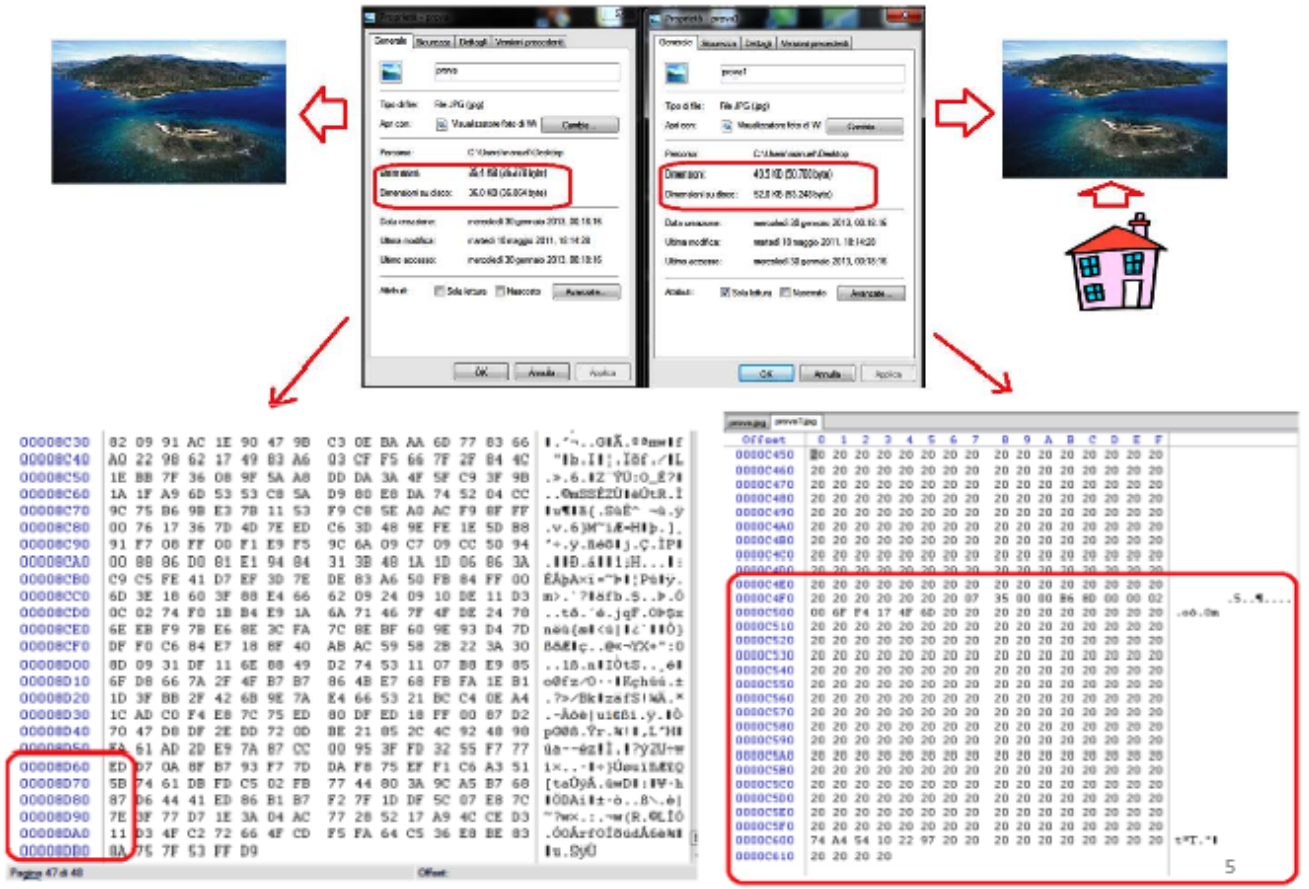

Microsoft Windows
È necessario formattare il disco nell'unità G: per poterlo utilizzare.
Formattarlo?
Formatta disco
Annulla

- La cifratura è un ottimo metodo di Antiforensics. Esistono anche altre tipologie di Antiforensics come la steganografia e la cancellazione sicura dei file.

- Il termine steganografia deriva dal greco, e il suo significato letterale è "scrittura nascosta". E' differente dalla crittografia in quanto, la steganografia nasconde un'informazione (l'esistenza di una informazione), mentre la crittografia la cifra (nasconde il contenuto dell'informazione). **Le due tecniche possono essere abbinate e sono complementari. Utilizzando la crittografia vediamo il messaggio, ma cifrato, mentre l'obiettivo della steganografia è di nascondere un qualcosa (messaggio) all'interno di un contenitore noto.** Per tecnica steganografica quindi si intende quel processo di occultamento di un' informazione. (Camouflage)


Steganogram van Laureline
Programma Laden Bewaar Verwijder Steganogram Help Over...
Originele Afbeelding
Tekst
==========
==========
DELPHI 5.0 INSTALLATION NOTES
==========
==========
For other installation notes, including minimum system requirements, installing from a network or shared drive, and descriptions of potential install-time problems, see README.TXT at the root of your CD.
Portions of this file contain information that applies only to specific editions of the product. Such portions are clearly marked with the name of the edition
Gecodeerde Afbeelding
Verschil

Scenario



ALCUNI VANTAGGI:

- Nascondere l'informazione – (quindi non attiriamo l'attenzione a differenza di un' informazione cifrata);
- Possibilità di nascondere l'informazione in diversi file cover, irriconoscibili dall'occhio umano;
- Difficile monitoring;
- Dimostrarne l'esistenza!

ALCUNI SVANTAGGI:

- Dimensione dei file cover (contenitore informazione nascosta);
- Dimensioni informazione nascosta.


SONY
10:35


500
Fairbanks Ct
N Michigan Ave
E Wacker Dr
N McClurg Ct
30
Menu
5:33
GARMIN nüvi


12:03
You
SAP
box
salesforce

Inizialmente la Digital Forensics è stata usata **solo per i crimini tecnologici (i «più comuni»)**.

- Intrusioni informatiche;
- Web defacement;
- Danneggiamento/Furto di dati;
- Pedofilia online;
- Azioni di Phishing/Whaling e/o Furto di Identità e Frode Bancaria.

Negli altri casi i computer sono stati *semplicemente ignorati* (e non solo quelli ☹)

Alcuni casi “non informatici” risolti negli ultimi anni e di cui si è letto sui media nazionali:

- **Frode telefonica:** analisi di dispositivi “GSM-box”-like al fine di individuare il *Modus Operandi tecnologico* ed il *modello di business* criminale.

- **Spionaggio Industriale:** supporto ad azienda nella risoluzione e conseguenti azioni in Tribunale (furto di disegni e progetti industriali).

- **Antipedofilia digitale:** analisi di evidence elettroniche a supporto dell’AA.GG., verso PC e smartphone sequestrati all’indagato.

- È quindi lampante come l'analisi delle evidenze digitali si rende **necessaria** anche per **crimini che nulla hanno a che fare con la tecnologia**.

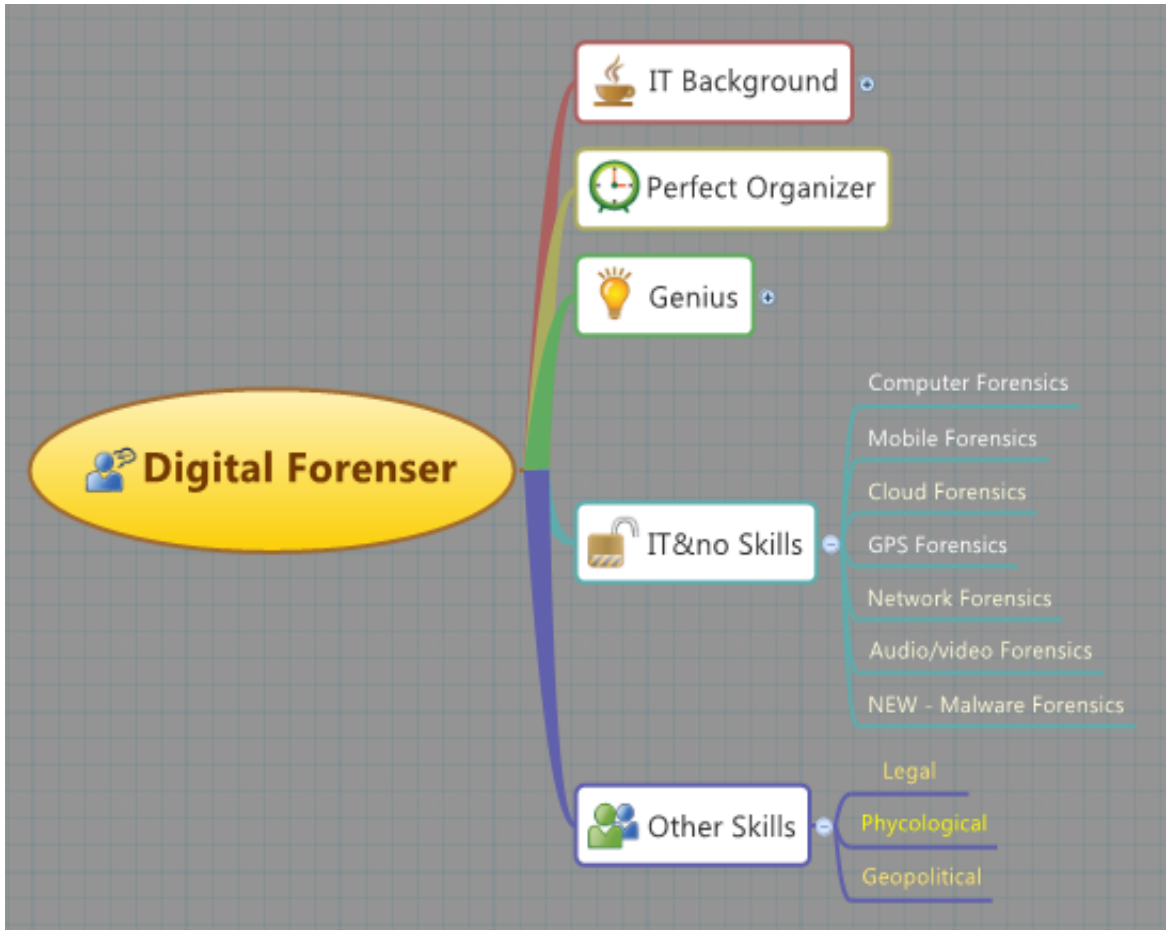
- Dal **palmare della Lioce** al **delitto di Garlasco e di Avetrana**…sino agli **atti di bullismo e cyberstalking a mezzo Facebook,** ed altre cronache recenti

- Non sono stati portati all'attenzione del grande pubblico **molti altri casi**, risolti per merito delle evidenze digitali.

- Adesso la Digital Forensics "**è di moda**"!!!

- Questo è **un bene** in quanto vi è:
  - **Maggiore scambio** di informazioni;
  - **Nuovi** tools e nuove tecnologie;
  - Un **più rapido sviluppo**;
  - Una **maggiore sensibilità** al problema.

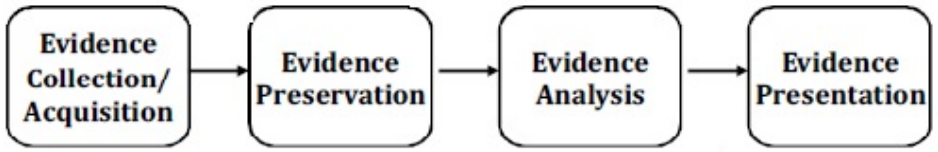
- Questo è **un male** perché:
  - **Tutti vogliono lanciarsi** in questo mercato;
  - Ci sono **molti** "presunti esperti", **improvvisati** e molto **spesso privi dei necessari** skills, strumenti, laboratori ed esperienza sul campo;
  - Tutti **promettono tool** "facili da usare";
  - Il fatto di scrivere "forensics" su un programma di 10 anni fa **non lo rende necessariamente più adatto allo scopo…** ☹


Digital Forenser
IT Background
Perfect Organizer
Genius
IT&no Skills
Computer Forensics
Mobile Forensics
Cloud Forensics
GPS Forensics
Network Forensics
Audio/video Forensics
NEW - Malware Forensics
Other Skills
Legal
Phycological
Geopolitical

La **Digital Forensics** è la scienza che studia come **ottenere**, **preservare**, **analizzare** e **documentare** le evidenze digitali (prove) dai dispositivi elettronici come: Tablet PC, Server, PDA, fax machine, digital camera, iPod, Smartphone (Mobile Forensics) e tutti gli altri dispositivi di memorizzazione.

- Una **digital evidence** può essere definita come **qualsiasi informazione avente valore probatorio che sia memorizzata o trasmessa in forma digitale**

- Una digital evidence può quindi essere estratta da:
  - Un **dispositivo di memorizzazione digitale**
    - Personal computer, notebook, hard disk esterno, floppy, nastro, CD/DVD, memory card, USB drive,…
    - **Telefoni cellulari, SIM, SmartPhone, Tablet, Navigatori satellitari**,…
  - Una **Rete Intranet/Internet**
    - Intercettazione di traffico dati
    - Pagine Web, Blog, Social Network, Chat/IM, P2P, ecc.



- **Identificazione**, **Collezione ed Acquisizione**;
- **Preservazione** (Chain of Custody);
- **Analisi**: estrazione delle informazioni significative per l'investigazione;
- **Evidence Presentation**: è la fase finale ma anche la più importante, nella quale anche i non addetti ai lavori riescono a capire il lavoro eseguito. È la redazione di un documento nel quale vengono analizzati passo passo tutti i risultati ottenuti ed estratti dalle digital evidence.

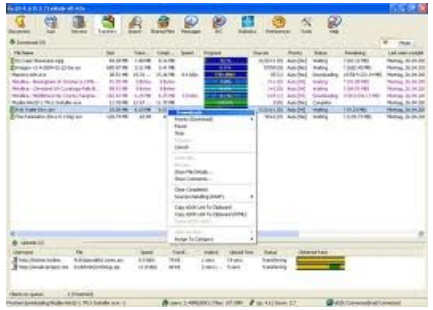
Goal: To explain the current state of Digital Artifact

Università di Roma

Digital Forensics

Dead Analysis

Live Analysis



Università di Roma

Oggigiorno chi ha l'informazione, ha il potere: proteggiamo i nostri dati.
E non fidiamoci troppo!

- **Educare gli utenti**
- **Dotarsi di strumenti all'avanguardia che non solo possono aiutarci a capire se abbiamo ricevuto delle minacce**
- Comprendere e prendere coscienza che ad oggi molte informazioni sono già all'esterno delle nostre organizzazioni
- Con noi potete sapere in tempo reale chi, cosa, perché e a quanto stanno vendendo i Vostri dati!

Siamo entrati in una NUOVA ERA dell'Information Security

Cyber Security & Autodifesa Digitale

Ing. Selene Giupponi

Cyber Security Advisor & Senior
Digital Forensics Consultant