ISACA®

Sistemi informativi: averne fiducia e trarne valore

Rome Chapter

“Evoluzione della Digital Forensics Professionale, dall’analisi post mortem alla live forensics: evoluzione pratica”

Massimiliano Graziani CFE CIFI CFIP CDFP OPSA ACE TCNU

Roma 24/07/2020

Agenda

- Presentazione relatore
- Riepilogo delle regole fondamentali
- Accenni alla ISO27037
- Evoluzione degli strumenti hardware professionali
- Evoluzione degli strumenti software professionali
- Live Forensics e Sniper Forensics
- Qualche esempio pratico
- Q&A

Agenda

- Presentazione relatore
- Riepilogo delle regole fondamentali
- Accenni alla ISO27037
- Evoluzione degli strumenti hardware professionali
- Evoluzione degli strumenti software professionali
- Live Forensics e Sniper Forensics
- Qualche esempio pratico
- Q&A

Presentazione relatore

Massimiliano Graziani *attualmente CEO Cybera Srl e CISO Adora ICT srl*

Fondatore, insieme ad altri nel 2005 del capitolo italiano dell'OWASP.

Socio fondatore del capitolo italiano dell' International Information Systems Forensics Association (IISFA), e dell'Osservatorio Nazionale Informatica Forense (ONIF), è in possesso delle seguenti certificazioni internazionali:

- CIFI (Certified Information Forensics Investigator rilasciata da IISFA)
- CFE (Certified Fraud Examiner rilasciata da ACFE)
- ACE (AccessData Certified Examiner rilasciata da AccessData)
- OPSA (OSSTMM Professional Security Analyst rilasciata da ISECOM)
- CIFIP (Certified Forensic Investigation Professional rilasciata da IICFIP)
- CDFP (Certified Digital Forensics Professional rilasciata da IICFIP).

Docente in materia di Digital Forensics Pratica presso Scuola di Polizia Tributaria della Guardia di Finanza (Corso Operativo di Computer Forensics con Logicube Dossier e Falcon), Università La Sapienza Roma (Corso Informatica Giuridica con Aterno), Università LUMSA Roma (Corso Diritto Penale dell'Informatica con Zanotti), Università di Salerno (Convegno La Tecnologia al servizio dell'Indagine Scientifica con De Santis, Cattaneo, Palmieri), Università del Molise (Master Information Security Management – Modulo Computer Forensics con Perrone), Università degli studi Link Campus University di Roma (modulo forensics di vari master). Docente volontario presso IISFA, OLAF, FF.OO., Consiglio Superiore Magistratura Milano, Ministero Economia e Finanze UCAMP, ISACA Roma e ACFE Italia e Centro Interforze di Formazione Intelligence/GE, Board of Directors ACFE Central.

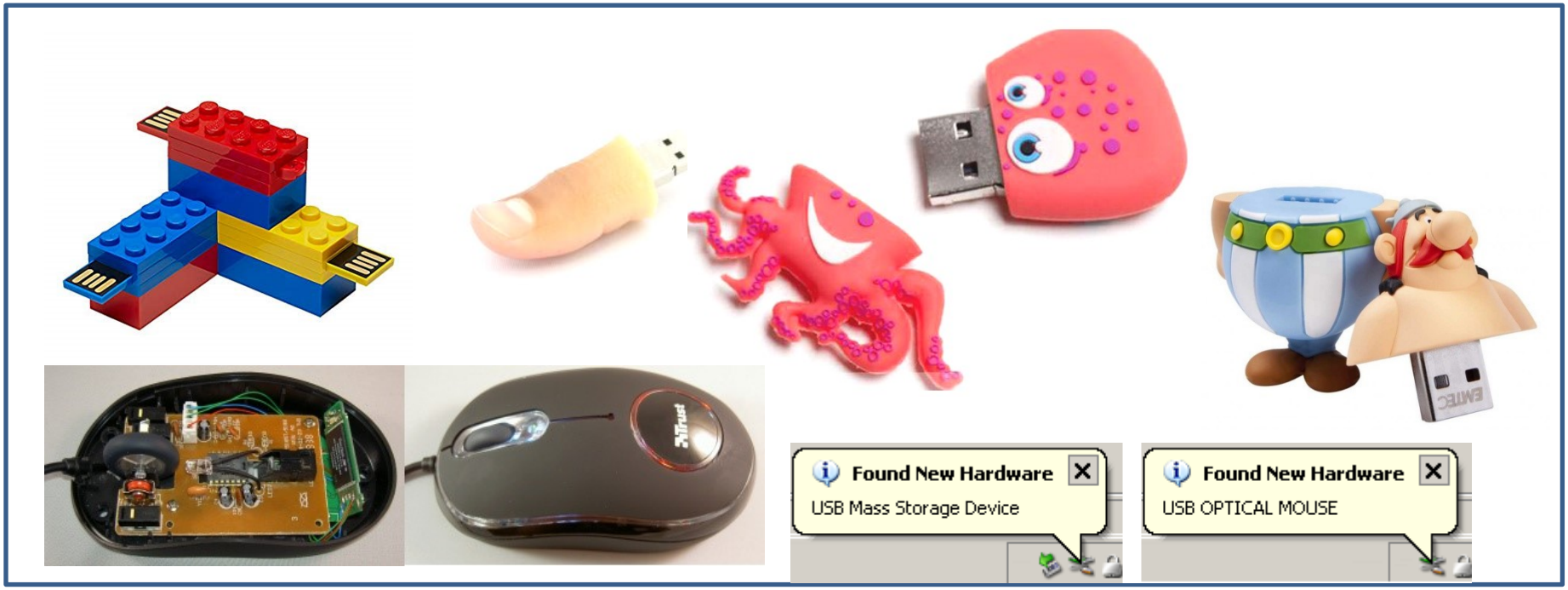
Agenda

- Presentazione relatore
- Riepilogo delle regole fondamentali
- Accenni alla ISO27037
- Evoluzione degli strumenti hardware professionali
- Evoluzione degli strumenti software professionali
- Live Forensics e Sniper Forensics
- Qualche esempio pratico
- Q&A

Riepilogo delle regole fondamentali

"L'informatica forense" è la scienza relativa alle attività di identificazione, acquisizione, preservazione, studio, analisi e documentazione delle memorie rilevate nei computer o sistemi informativi in generale, al fine di evidenziare prove per scopi di indagine.

Riepilogo delle regole fondamentali



"L'informatica forense" è la scienza relativa alle attività di identificazione, acquisizione, preservazione, studio, analisi e documentazione delle memorie rilevate nei computer o sistemi informativi in generale, al fine di evidenziare prove per scopi di indagine.

Riepilogo delle regole fondamentali

La vita quotidiana è pervasa da moltissimi dispositivi digitali e la maggior parte delle nostre azioni lasciano, anche a nostra insaputa, tracce informatiche su numerosi sistemi.

Queste tracce, se trattate in modo corretto, hanno un enorme valore per le aziende al fine di proteggere il proprio patrimonio informativo, contrastare le frodi e, all'occorrenza, essere usate per fini legali.

Riepilogo delle regole fondamentali

Ricordiamo che nelle attività investigative il computer può avere diversi ruoli:

- parte "attiva" dell'azione criminale
- obiettivo di atti criminali
- contenitore delle prove per attività illecita

All'aumento del trattamento dei dati con sistemi informatici, consegue l'incremento della domanda di analisi dei dati digitali ai fini investigativi per:

- reati informatici e telematici
- reati non informatici ma commessi con sistemi informatici
- reati in cui si rinvengono tracce o indizi nei sistemi
- investigazione contrasto frodi
- investigazioni preventive a tutela del patrimonio aziendale

Tipologie di Computer Forensics

ANALISI POST MORTEM (ex359 cpp ripetibile)

Le attività di repertamento e analisi sono ripetibili, avviene quasi sempre su un dato cristallizzato.

ANALISI LIVE (ex360 cpp non ripetibile)

quasi sempre irripetibile, avviene quasi sempre su un dato “in movimento”

Regole di base

A) COMPUTER SPENTO: vengono acquisite tutte le memorie rilevate al suo interno.
I dischi devono essere maneggiati con guanti con protezione elettrostatica, tutte le fasi di repertamento devono essere fotografate.

B) COMPUTER ACCESO: verificare la presenza di sistemi di cifratura, effettuare una live forensics, acquisire eventuali dischi cifrati montati in chiaro, acquisire il dump della RAM, scollegare il cavo di alimentazione e procedere al repertamento come al punto A

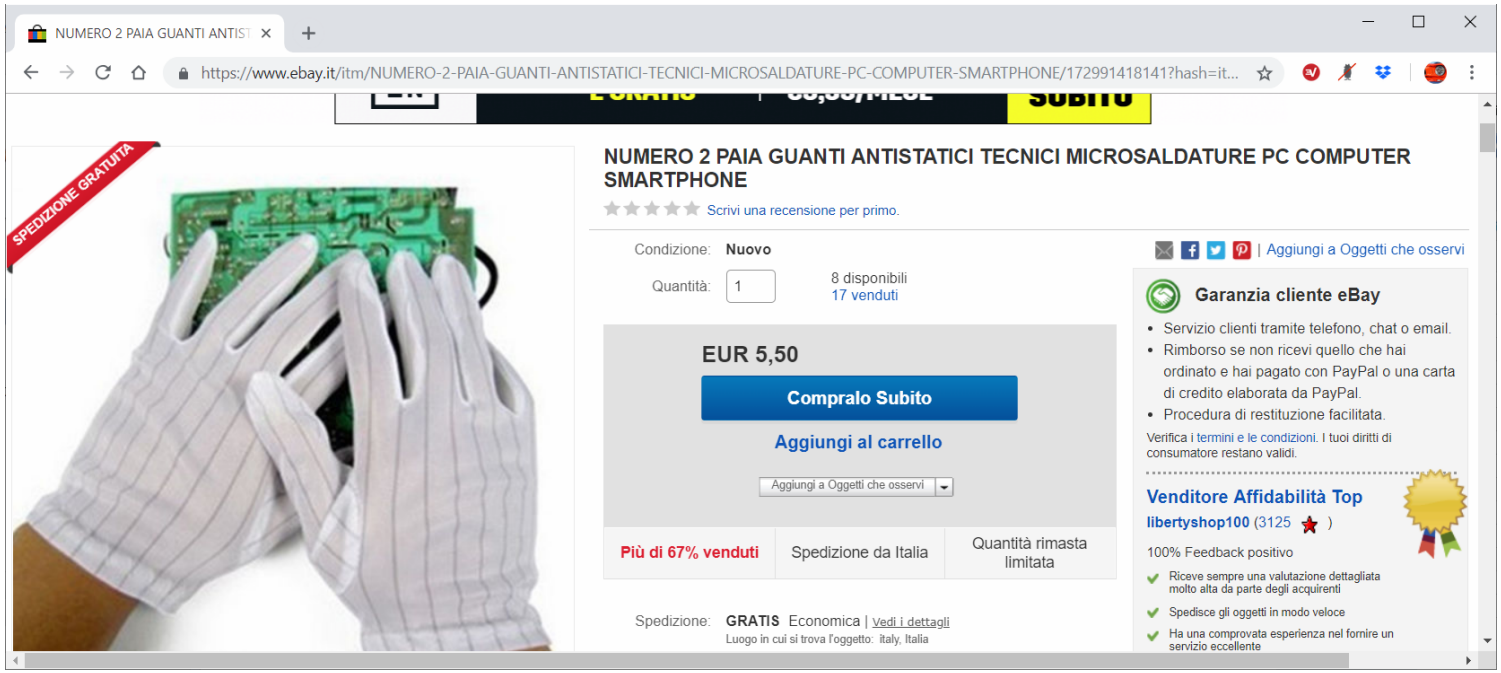
C) COMPUTER PORTATILE: se acceso eseguire i passi come al punto B, se non si è sicuri del suo stato (suspend o freeze) procedere alla rimozione della batteria prima di togliere l'alimentazione (se alimentato). Attenzione alcuni portatili in suspend si accendono aprendo lo schermo o premendo un qualsiasi tasto…

Riepilogo delle regole fondamentali

Usare sempre i guanti antistatici per maneggiare le prove informatiche:

1) Per evitare di contaminare impronte
2) Per evitare danni da energia elettrostatica

Costano pochi euro, perché ancora oggi nessuno li utilizza?



Riepilogo delle regole fondamentali

Rilevare sempre lo scarto orario durante le acquisizioni.

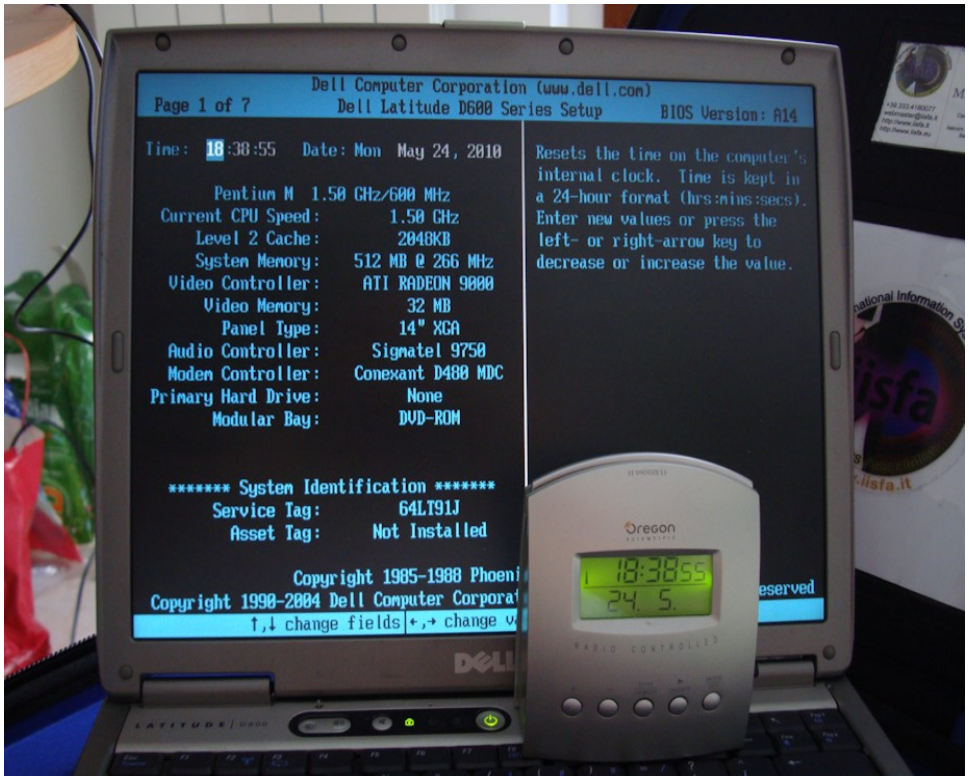
La stessa regola vale sui LOG.

Uno degli errori classici che avviene nell'interpretazione dei LOG, è quella di non dare importanza ai simboli e numeri rappresentati vicino l'ora…

Abbiamo orari GMT, +0000, +1, ecc.

```
80.220.249.244 - - [09/Mar/2015:05:21:27 +0000] "GET /puzzle/random HTTP/1.1" 200 1318 0.0028
dsl-jklbrasgw2-50dcf9-244.dhcp.inet.fi - - [09/Mar/2015:05:21:27 GMT] "GET /puzzle/random HTTP/1.1" 200 1318
- -> /puzzle/random
80.220.249.244 - - [09/Mar/2015:05:21:32 +0000] "GET /puzzle/random HTTP/1.1" 200 1820 0.0032
dsl-jklbrasgw2-50dcf9-244.dhcp.inet.fi - - [09/Mar/2015:05:21:32 GMT] "GET /puzzle/random HTTP/1.1" 200 1820
- -> /puzzle/random
80.220.249.244 - - [09/Mar/2015:05:22:40 +0000] "POST /user/login HTTP/1.1" 202 2 0.0012
dsl-jklbrasgw2-50dcf9-244.dhcp.inet.fi - - [09/Mar/2015:05:22:40 GMT] "POST /user/login HTTP/1.1" 202 2
- -> /user/login
80.220.249.244 - - [09/Mar/2015:05:22:44 +0000] "GET /user/puzzles?unique=G:661665932 HTTP/1.1" 200 24885 0.(
dsl-jklbrasgw2-50dcf9-244.dhcp.inet.fi - - [09/Mar/2015:05:22:44 GMT] "GET /user/puzzles?unique=G:661665932 H
24885
- -> /user/puzzles?unique=G:661665932
80.220.249.244 - - [09/Mar/2015:05:22:56 +0000] "GET /puzzle/random HTTP/1.1" 200 724 0.0027
dsl-jklbrasgw2-50dcf9-244.dhcp.inet.fi - - [09/Mar/2015:05:22:56 GMT] "GET /puzzle/random HTTP/1.1" 200 724
- -> /puzzle/random
80.220.249.244 - - [09/Mar/2015:05:23:02 +0000] "GET /puzzle/random HTTP/1.1" 200 1637 0.0047
dsl-jklbrasgw2-50dcf9-244.dhcp.inet.fi - - [09/Mar/2015:05:23:02 GMT] "GET /puzzle/random HTTP/1.1" 200 1637
- -> /puzzle/random
80.220.249.244 - - [09/Mar/2015:05:23:09 +0000] "GET /puzzle/random HTTP/1.1" 200 2186 0.0035
dsl-jklbrasgw2-50dcf9-244.dhcp.inet.fi - - [09/Mar/2015:05:23:09 GMT] "GET /puzzle/random HTTP/1.1" 200 2186
```

Riepilogo delle regole fondamentali



Una fase del repertamento:
Rilevazione dello scarto orario dal bios del computer analizzato:

- Avere sempre un orologio preciso e sincronizzato
- Accedete al bios solo dopo aver scollegato le memorie di massa

Riepilogo delle regole fondamentali

Una fase del repertamento:

Scattare foto e se necessario video, per documentare il più possibile le fasi iniziali di repertamento.

Usare uno buono smartphone che imprima data e ora e posizione GPS nei dati EXIF è un MUST ed è alla portata di tutti!

Tutti avete uno smartphone di gamma alta vero?

Acquisizione RIPETIBILE

Bisogna “congelare” il dato informatico ed esaminare successivamente una copia dell’originale…

Se viene commesso un errore non si può cliccare sul tasto “annulla”…

Riepilogo delle regole fondamentali

EVITARE ASSOLUTAMENTE:

- FRETTA: perdita di concentrazione che favorisce l'errore umano
- STRUMENTI IMPROVVISATI e non collaudati
- STRESS da troppo lavoro
- Collaboratori agitati che non vedono l'ora di accendere quel maledetto PC
- Di improvvisare, ovvero fare cose di cui non si ha padronanza assoluta
- Operare senza aver deciso ruoli e responsabilità

Riepilogo delle regole fondamentali

Legge 48 del 2008 detta “Ratifica di Budapest”

Introduce :

1. obblighi e modalità di custodia art. 259 2° comma c.p.p.

2. sigilli e vincolo delle cose sequestrate art.260 1° e 2° comma c.p.p.

Sorge la necessità di assicurare pieno controllo sull’operato degli organi inquirenti, in particolare la verifica sulle procedure acquisitive della prova.
Il legislatore sottolinea l’importanza della salvaguardia dei dati e la necessità di adottare “misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l’alterazione”

Riepilogo delle regole fondamentali

Normative e best practice parlano di:

Sigillo digitale = HASH meglio se calcolato con 2 algoritmi distinti

Catena di Custodia = Chain of Custody

Sono elementi “fondamentali” per la formazione della “prova informatica”

NON SONO PIU’ OPTIONAL !!!

Riepilogo delle regole fondamentali

Funzioni hash: a cosa servono e perché dovresti conoscerle

Per prima cosa, partiamo con la definizione generica: le **funzioni di hash** sono, appunto, delle funzioni che a partire da un qualsiasi stringa o insieme di dati in input A, producono una stringa B (impronta) che ha una lunghezza costante, a prescindere dalle dimensioni di A.

Allora a che mi servono le funzioni di hash? Posso vivere senza?

No, sono funzioni che servono a garantire l'integrità di un insieme di dati, e sono caratterizzate da:

Irreversibilità - Determinismo

Lunghezza fissa - Effetto valanga

Riepilogo delle regole fondamentali

Irreversibilità

Le funzioni di hash sono irreversibili. Questa caratteristica è molto importante, ed è anche quella che maggiormente distingue l'hashing dall'encrypting:
Hashing (ottenere un hash) è una operazione **IRREVERSIBILE**
Encrypting (criptare un testo) è una operazione **REVERSIBILE** (tramite chiave)

L'hashing è irreversibile dato che conoscendo l'hash, è matematicamente IMPOSSIBILE ricostruire il dato originale.

Determinismo

L'input A produce e produrrà sempre lo stesso hash B. Le funzioni di hash sono deterministiche proprio perché l'output di un input fisso è sempre uguale.

Lunghezza fissa

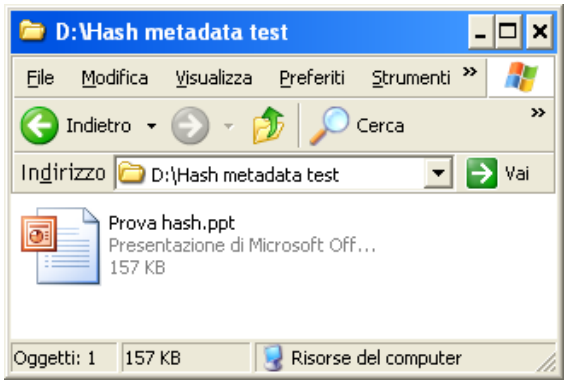
L'output prodotto dalle funzioni di hash ha una lunghezza fissa. Nell'esempio dell'MD5, gli hash in output sono sempre di 32 caratteri.

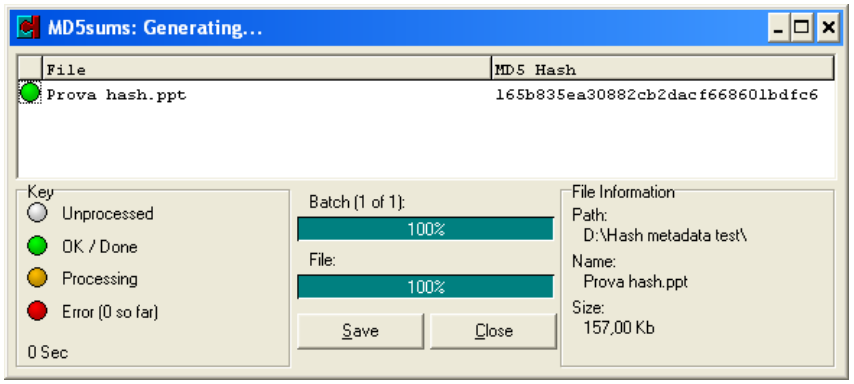
Effetto valanga

E' una proprietà per cui una piccola variazione nell'input A, produce una notevole variazione nella firma finale di hash.

Riepilogo delle regole fondamentali

Riepilogo delle regole fondamentali

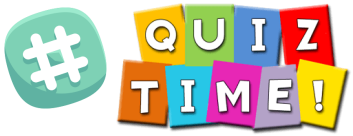


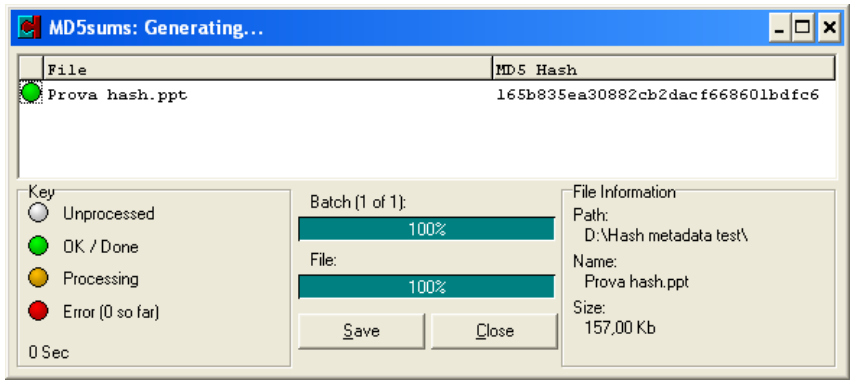


Apro file e richiudo subito.

?

Riepilogo delle regole fondamentali

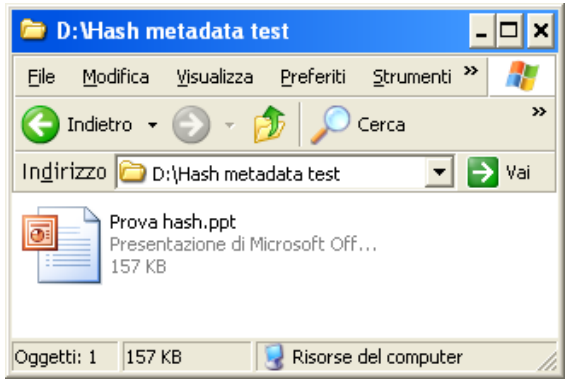


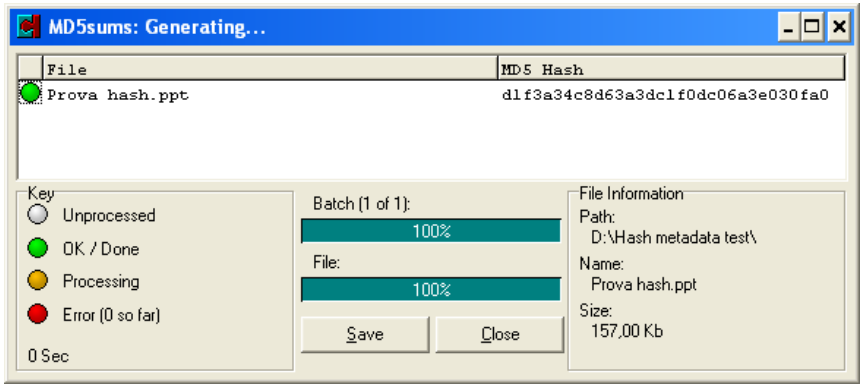


Apro tolgo lettere e rimetto lettera.

?

Riepilogo delle regole fondamentali

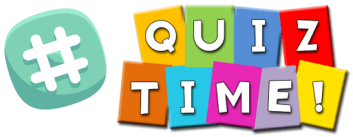


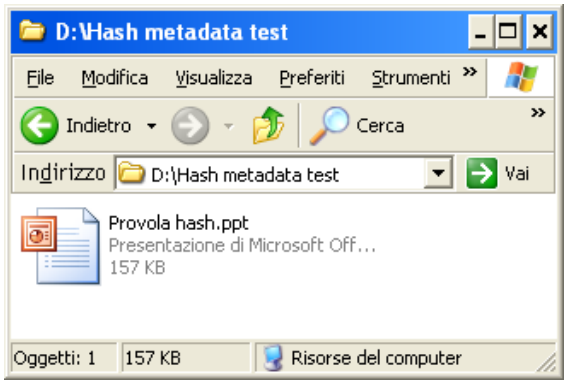


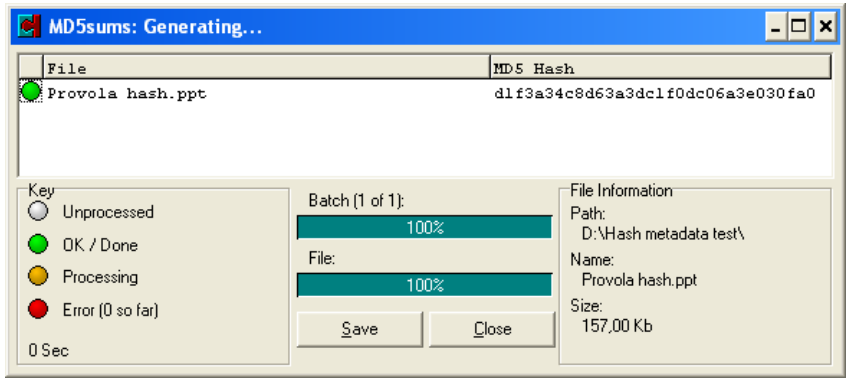
Rinomino file.

?

Riepilogo delle regole fondamentali



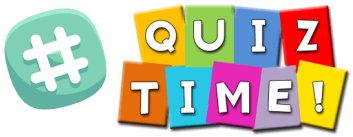


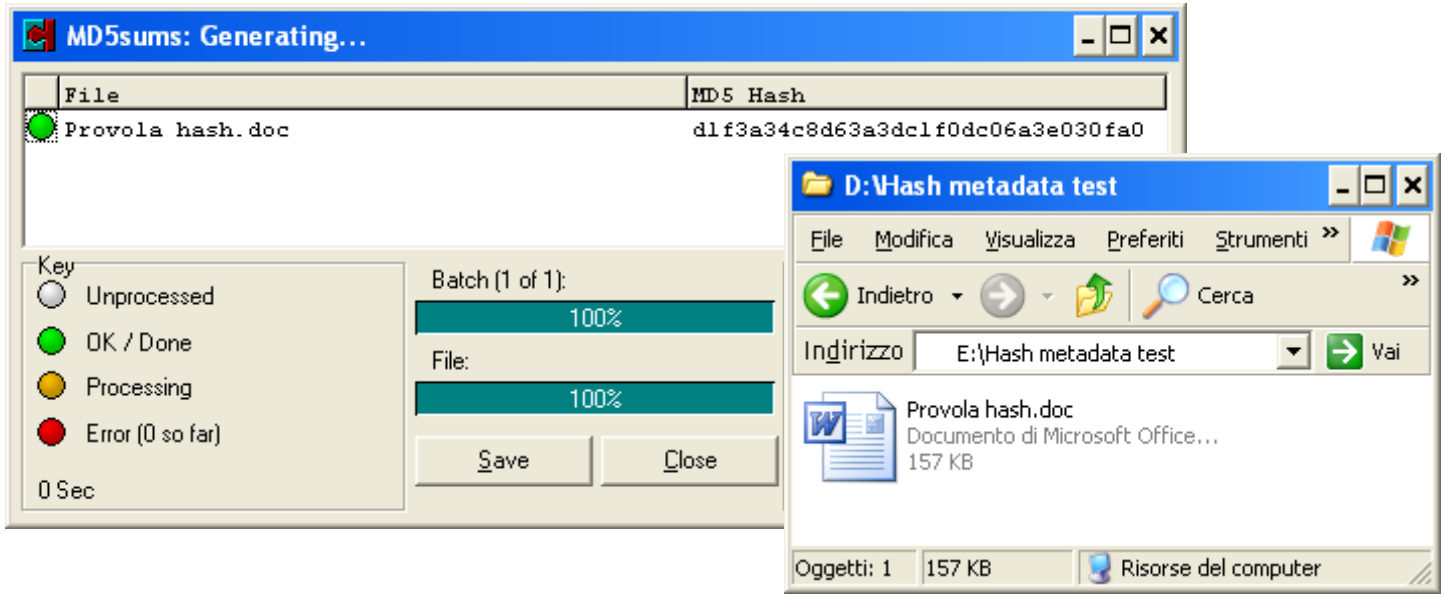


Cambio estensione al file.

?

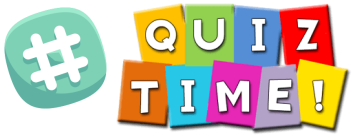
Riepilogo delle regole fondamentali

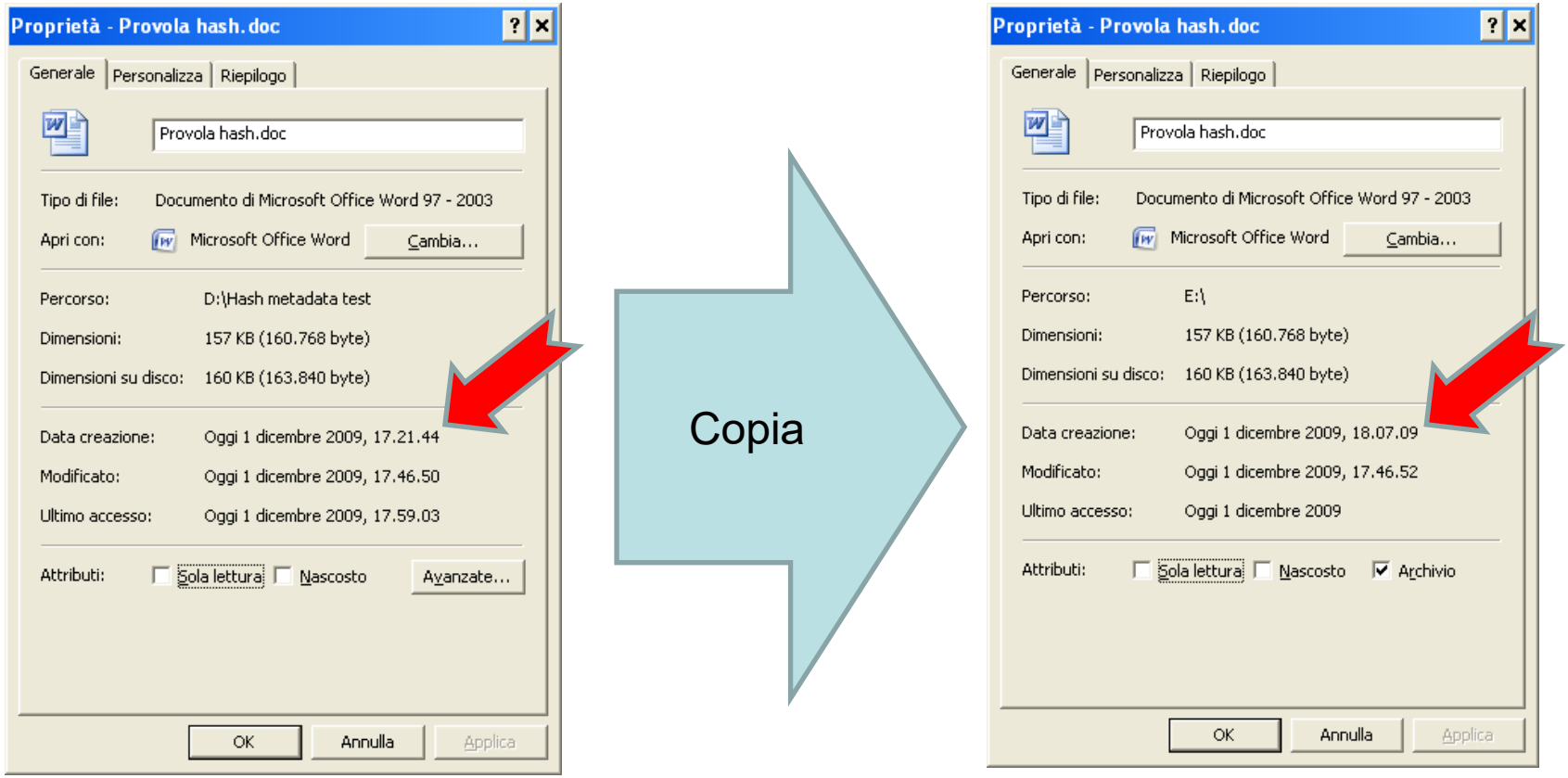




Nella fase di copia l'hash non cambia ma cosa è cambiato?

Riepilogo delle regole fondamentali

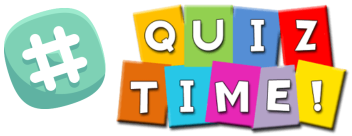




Metadati del file originale

Metadati del file copiato

Riepilogo delle regole fondamentali



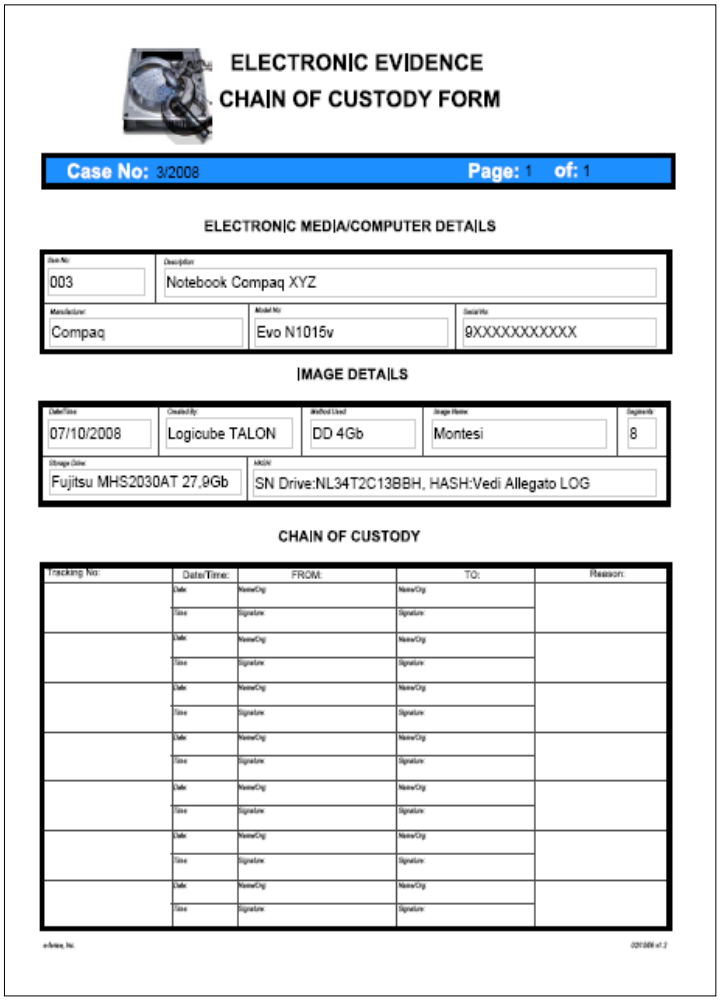
FATE QUINDI MOLTA ATTENZIONE

ALL’IMPORTANZA

DEI DATI E METADATI

!!

Riepilogo delle regole fondamentali



ELECTRONIC EVIDENCE
CHAIN OF CUSTODY FORM

Case No: 3/2008 **Page:** 1 **of:** 1

ELECTRONIC MEDIA/COMPUTER DETAILS

003	Notebook Compaq XYZ	
Compaq	Evo N1015v	9XXXXXXXXXX

IMAGE DETAILS

07/10/2008	Logicube TALON	DD 4Gb	Montesi	8
Fujitsu MHS2030AT 27,9Gb	SN Drive:NL34T2C13BBH, HASH:Vedi Allegato LOG			

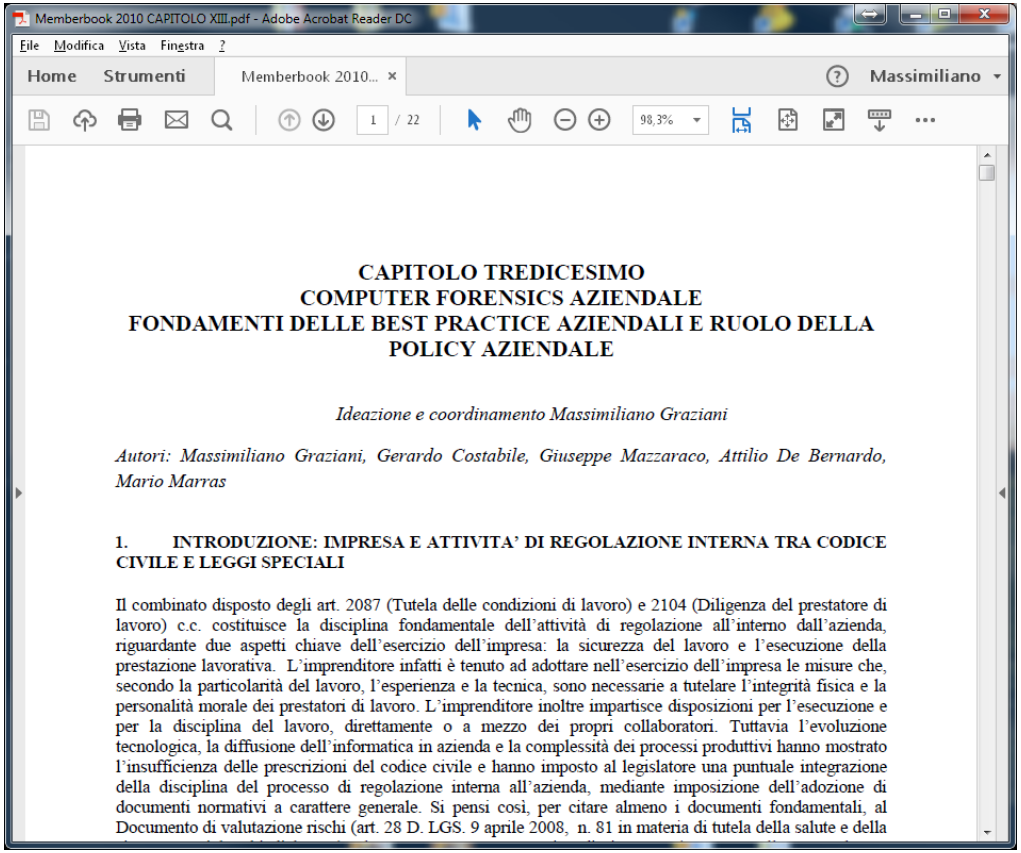
CHAIN OF CUSTODY

Tracking No:	Date/Time:	FROM:	TO:	Reason:

Allegare al reperto sempre il documento di Catena di Custodia

Questo documento riporta tutti dati utili a tracciare le attività svolte sulla digital evidence custodita.
Dati fondamentali sono ad esempio i codici di hash, i dati fisici del disco, chi, come, quando, dove e perché ha avuto accesso alla digital evidence.....

Riepilogo delle regole fondamentali



Unico testo italiano per la digital forensics aziendale è stato pubblicato da IISFA nel 2010 ed è basato su esperienza pratica presso grandi aziende italiane

Riepilogo delle regole fondamentali

La Digital Forensics in azienda deve essere svolta:

1) Sempre con l'affiancamento di un legale esterno
2) Può coinvolgere HR, Legal, Vertici, CdA Organi di Vigilanza, Rappresentanti Sindacali
3) Necessita di una impalcatura di policy aziendali che ne agevolino l'intervento
4) Meglio se è già definita in Azienda una procedura scritta
5) Internal Audit e Antifrode devono avvalersi di consulenti tecnici esterni meglio se certificati
6) Deve esistere un modello di collaborazione tra le strutture aziendali
7) Le attività si devono eseguire a norma di legge, tutelando anche il dipendente

Riepilogo delle regole fondamentali

Indagini preliminari e processo penale: cosa sono le indagini difensive.

La nuova legge sulle indagini difensive con l'inserimento nel libro V del codice, del titolo VIbis intitolato «***Investigazioni difensive***», prosegue il percorso del legislatore mirante a garantire un'effettiva *parità tra accusa e difesa* (art. 111 Cost.)
Dispone l'art. 327bis che «fin dal momento dell'incarico professionale, risultante da atto scritto, il difensore ha facoltà di svolgere investigazioni per ricercare ed individuare elementi di prova a favore del proprio assistito, nelle forme e finalità stabilite nel titolo VIbis».

Una novità di rilievo è costituita dal fatto che le investigazioni difensive possono essere compiute non solo quando è già in corso il procedimento penale, ma anche quando è solo eventuale la sua instaurazione (art. 391novies: cd. attività investigativa preventiva); ad esempio: una persona temendo di poter essere coinvolta nelle indagini per una rapina, pur senza essere indagata, potrebbe dare incarico al suo difensore di svolgere investigazioni preventive per documentare il suo alibi.
Inoltre, cosi come già era previsto per il P.M., anche il difensore può compiere attività integrativa di indagine successivamente al rinvio a giudizio (v. nuova formulazione dell'art. 430). Tale facoltà è estesa ai sostituti del difensore, agli investigatori privati autorizzati ed ai consulenti tecnici.

Riepilogo delle regole fondamentali

Alcuni consigli utili

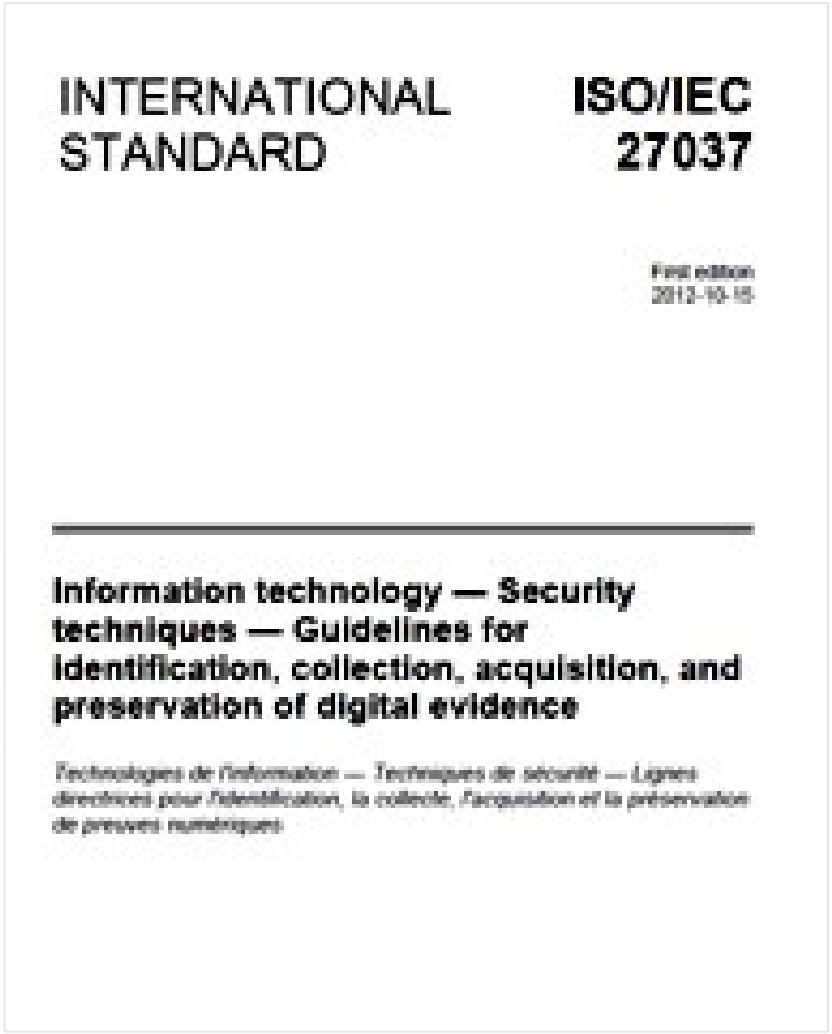
Notate sempre se il consulente quando opera:

- Maneggia sempre i reperti con guanti elettrostatici
- Fotografa e documenta tutte le fasi di acquisizione
- In caso di clone, esegue sempre il wipe sicuro dei dischi di destinazione conservandone un log
- In caso di imaging, salva i dati (DD e LOG) dentro una cartella (chiamandola con il nome del caso)
- Utilizza sempre il **write blocker hardware** per proteggere i dischi sorgente (suspect)
- Calcola sempre il digest in doppio hash del disco sorgente e dei file interessanti e ne effettua la verifica
- Compila correttamente la catena di custodia
- Custodisce sempre i dischi in buste elettrostatiche e in contenitori anticaduta
- Garantisce la riservatezza, integrità e disponibilità dei dati trattati
- Di fronte ad un sistema non conosciuto non improvvisa ma prendere le opportune precauzioni con i giusti tempi (vedi RAID con controller proprietario o sistemi Legacy)
- E' compatibile con il trattamento dei dati del caso… e ha ricevuto regolare incarico e ha firmato un NDA…

Agenda

- Presentazione relatore
- Riepilogo delle regole fondamentali
- Accenni alla ISO27037
- Evoluzione degli strumenti hardware professionali
- Evoluzione degli strumenti software professionali
- Live Forensics e Sniper Forensics
- Qualche esempio pratico
- Q&A

Accenni alla ISO 27037



INTERNATIONAL STANDARD

ISO/IEC 27037

First edition
2012-10-15

Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques

Accenni alla ISO 27037

Il 15 Ottobre 2012 è stata pubblicata la prima versione approvata della ISO/IEC 27037

"Guidelines for identification, collection, acquisition and preservation of digital evidence"


INTERNATIONAL STANDARD

ISO/IEC 27037

First edition
2012-10-15

Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques

Accenni alla ISO 27037


INTERNATIONAL STANDARD
ISO/IEC 27037
First edition 2012-10-15
Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence
Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques

ISO/IEC 27037:2012 (48 pagine)

- 7 Capitoli
    1. Scopo
    2. Riferimenti Normativi
    3. Terminologia e Definizioni
    4. Abbreviazioni Convenzionali
    5. Panoramica Generale
    6. Componenti chiave
    7. Istanze di Digital Forensics
- 2 Allegati
    - Allegato A: DEFR abilità e competenze
    - Allegato B: requisiti minimi per la movimentazione degli elementi di prova

Accenni alla ISO 27037

Introduce le figure:

DEFR
Digital Evidence First Responders

DES
Digital Evidence Specialists


INTERNATIONAL STANDARD
ISO/IEC 27037
First edition 2012-10-15
Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence
Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques

La norma internazionale è stata creata allo scopo di fornire una linea guida per i responsabili dell'identificazione, la raccolta, l'acquisizione e la conservazione delle prove digitali. Questi individui fanno parte del Gruppo di primo intervento di Computer Forensics e Specialisti di Computer Forensics, specialisti di risposta agli incidenti e manager dei laboratori di Computer Forensics. Rappresenta una metodologia pratica accettabile per le persone incaricate di gestire le potenziali prove digitali di tutto il mondo, con l'obiettivo di agevolare le indagini che coinvolgono i dispositivi digitali e le prove digitali in modo sistematico e imparziale, preservando l'integrità e l'autenticità della prova digitale.

Accenni alla ISO 27037


INTERNATIONAL STANDARD
ISO/IEC 27037
First edition 2012-10-15
Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence
Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques

ISO 27037 è uno standard internazionale contenente le linee guida per identificazione, raccolta, acquisizione e conservazione di evidenze digitali

Di cosa si occupa

- Trattamento del reperto informatico
- Definizione linee guida nelle fasi di
    - Identificazione (ispezione)
    - Raccolta (sequestro)
    - Acquisizione (sequestro virtuale)
    - Conservazione (sigillo e catena di custodia)
- Integrità della prova informatica e metodologia al fine di rendere ammissibile la prova in giudizio
- Per prova informatica si fa riferimento a dati in formato nativo digitale

Inoltre per ogni fase:

- Documentazione (logging)
- Tracciabilità (aggiornamento chain of custody)
- Priorità di intervento (plan)
- Imballaggio dei reperti (protection)
- Trasporto dei reperti (real/virtual)
- Ruoli nel passaggio dei reperti (who & why)

Accenni alla ISO 27037

Di cosa non si occupa

- Aspetti legali : è internazionale quindi non legata ad un singolo ordinamento
- Analisi
- Strumenti tecnici
- Redazione di report e presentazione

Introduce gli operatori che trattano le digital evidence

Digital evidence first responders (***DEFRs)***

- Operatore che si approccia per primo ai sistemi (supporti di memorizzazione e dati) di potenziale interesse
- Deve avere adeguata esperienza e competenze
- Può avvalersi di collaboratori

Accenni alla ISO 27037


INTERNATIONAL STANDARD

ISO/IEC 27037

First edition 2012-10-15

Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence

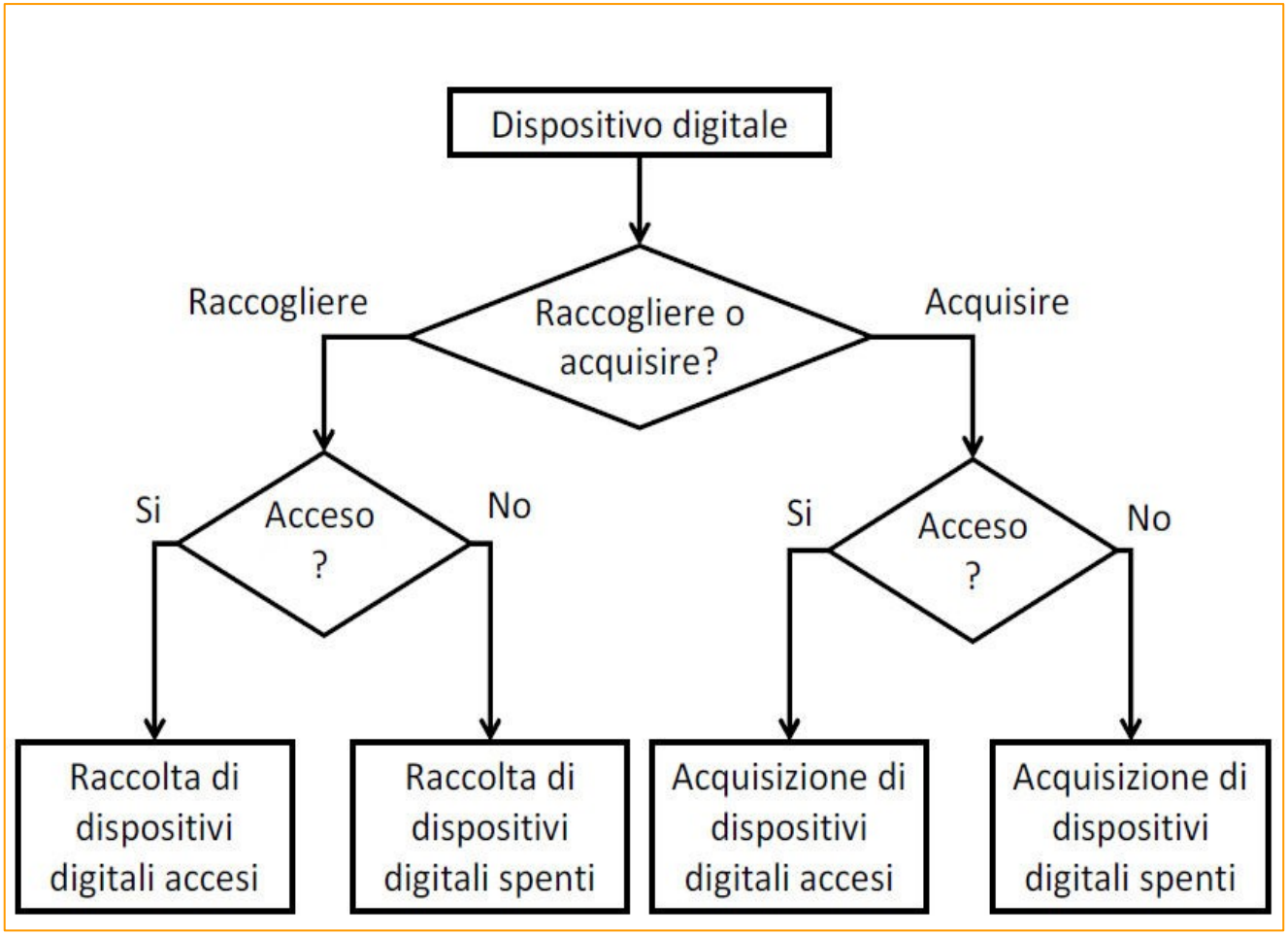
Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques

Compiti del DEFR

Il DEFR deve mettere in sicurezza e proteggere il luogo appena possibile

- Mettere in sicurezza e controllare l'area che contiene i dispositivi di memorizzazione digitale
- Individuare il responsabile dell'area
- Allontanare le persone dai dispositivi digitali e dall'alimentazione elettrica
- Documentare tutti quelli che sono autorizzati ad accedere all'area e chi potrebbe avere interesse a modificare i dati
- Non mutare lo stato delle apparecchiature (se acceso non spegnere, se spento non accendere)
- Documentare la scena, componenti, cavi (fotografie, video, disegni, schemi)
- Individuare note, appunti, diari, fogli, manuali
- Ricerca password e PIN

Accenni alla ISO 27037



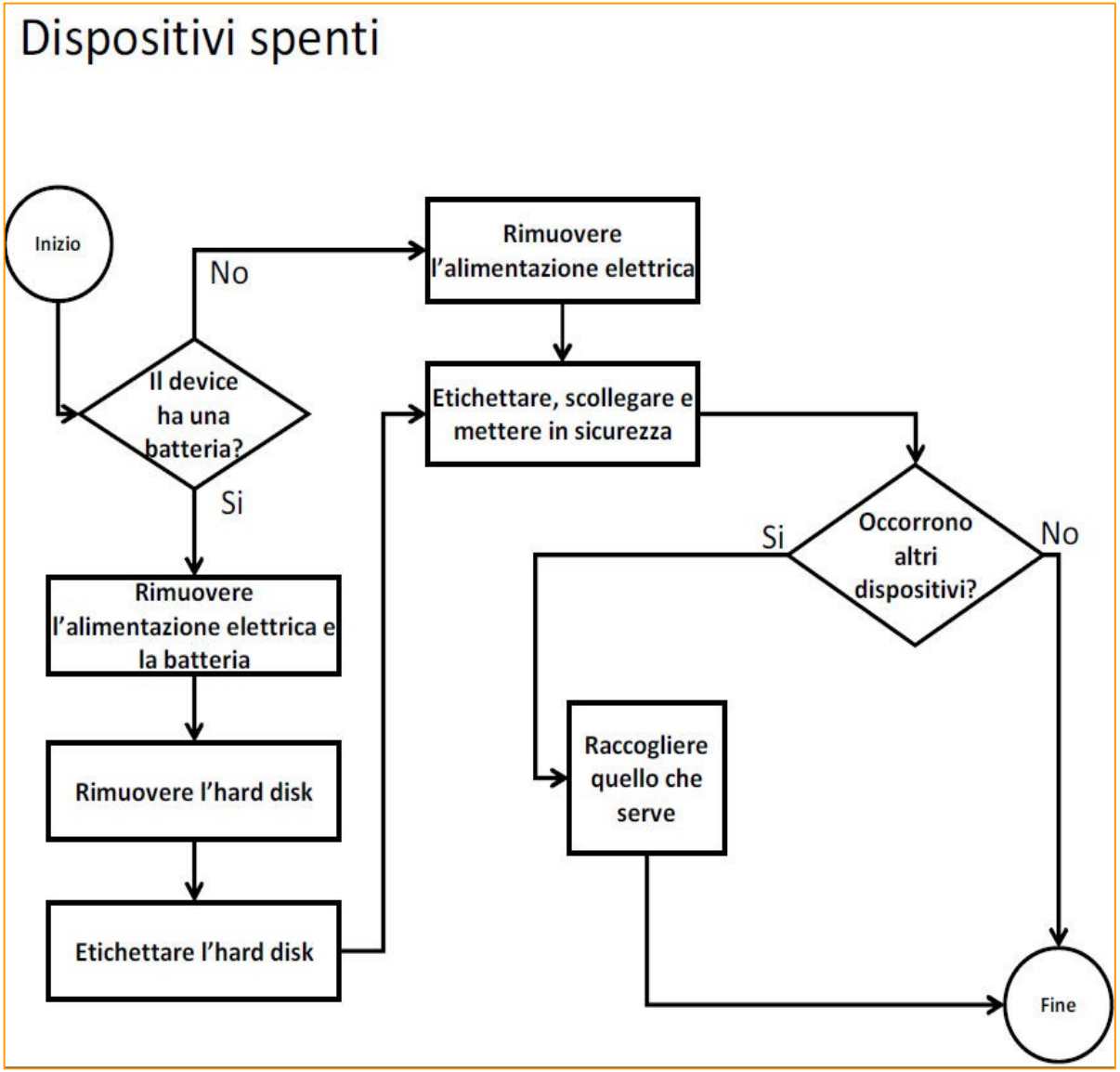

INTERNATIONAL STANDARD **ISO/IEC 27037**

First edition 2012-10-15

Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques

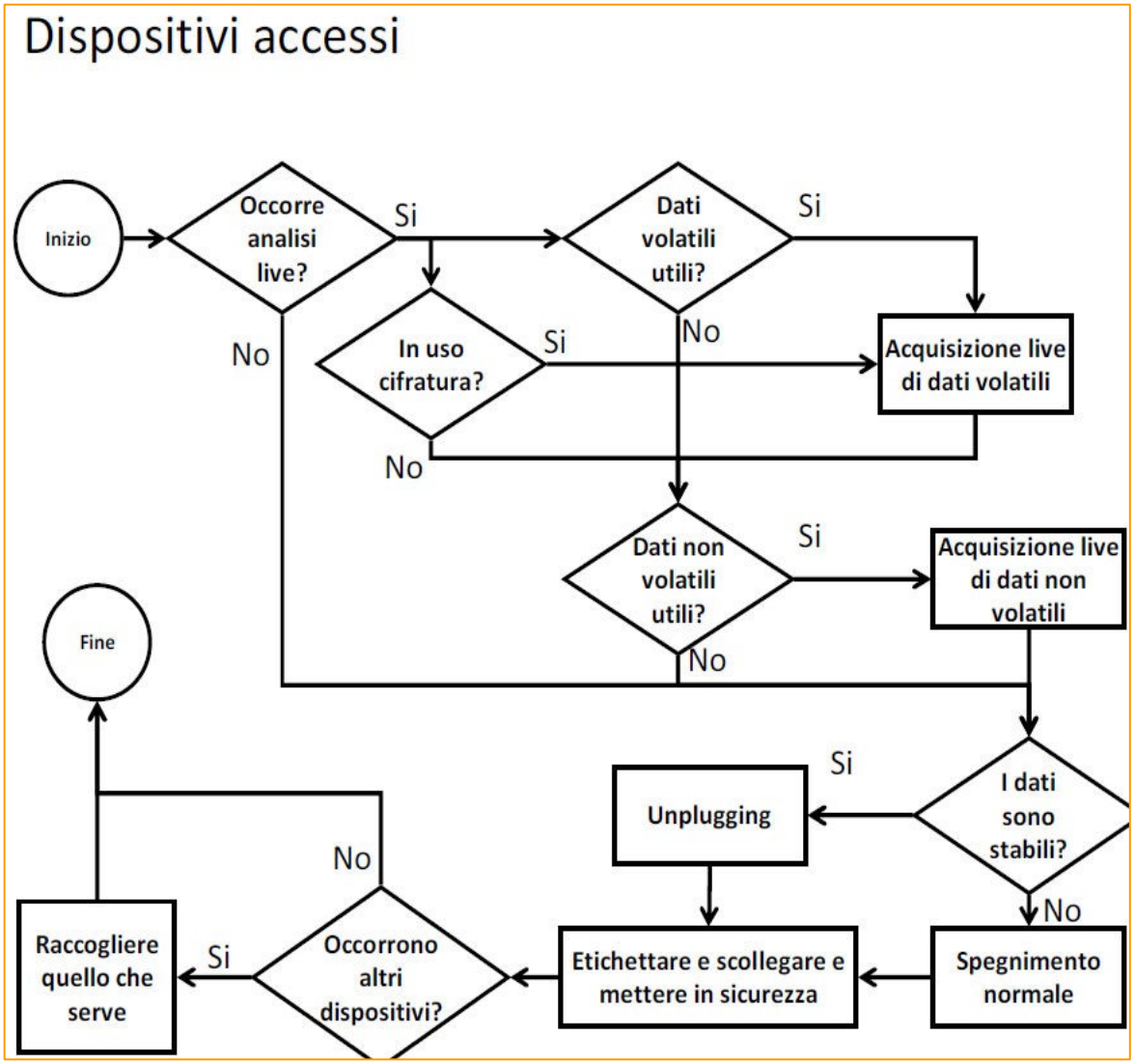
Accenni alla ISO 27037




INTERNATIONAL STANDARD ISO/IEC 27037

Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence

Accenni alla ISO 27037




INTERNATIONAL STANDARD ISO/IEC 27037

First edition 2012-10-15

Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques

Accenni alla ISO 27037

Prevede la gestione delle Situazioni Critiche


INTERNATIONAL STANDARD

ISO/IEC 27037

First edition
2012-10-15

Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques

In alcuni casi, i dispositivi non possono essere spenti a causa della natura del sistema, come ad esempio: data center che offrono servizi a terzi, sistemi di sorveglianza, sistemi medici, altri sistemi critici…

Occorre prevedere particolari attenzioni ed è possibile procedere con

- Acquisizione live
- Acquisizione parziale

Accenni alla ISO 27037

Descrive le Competenze minime degli operatori che si occupano delle fasi di

- Identificazione
- Raccolta
- Acquisizione
- Conservazione

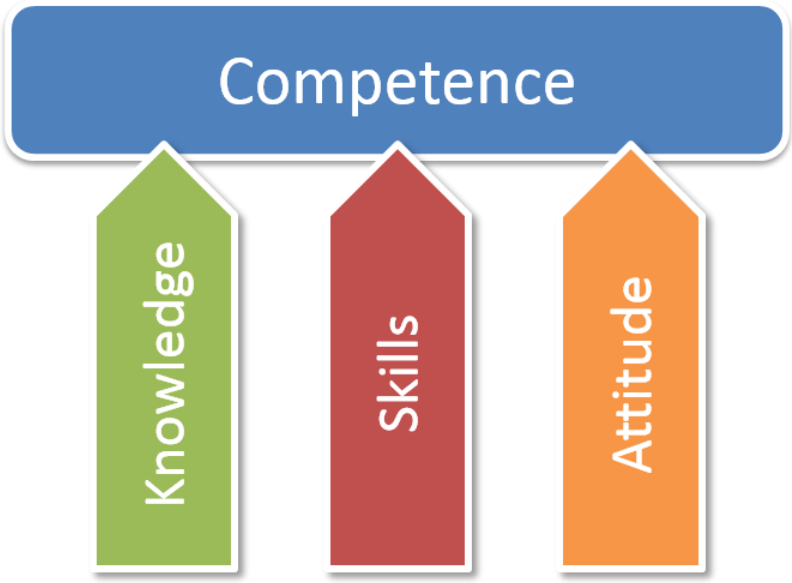

INTERNATIONAL STANDARD

ISO/IEC 27037

First edition
2012-10-15

Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques

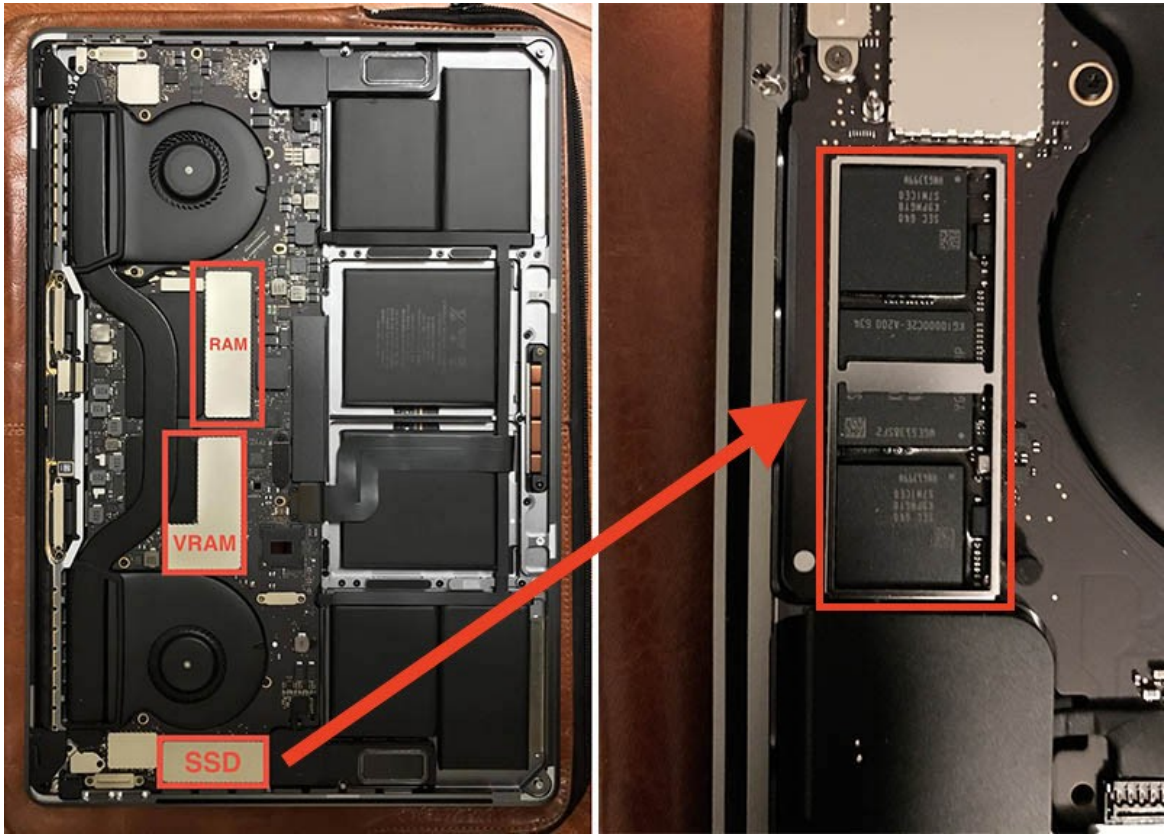


Agenda

- Presentazione relatore
- Riepilogo delle regole fondamentali
- Accenni alla ISO27037
- Evoluzione degli strumenti hardware professionali
- Evoluzione degli strumenti software professionali
- Live Forensics e Sniper Forensics
- Qualche esempio pratico
- Q&A

Evoluzione degli strumenti hardware professionali

Le operazioni di cristallizzazione diventano sempre più complesse.
Memorie a stato solido e crittografia, rendono sempre più complesso il lavoro…
…non bisogna comunque scoraggiarsi…



Hard Disk SSD Macbook Pro con Touch Bar non rimovibile…

Evoluzione degli strumenti hardware professionali

Prima di passare agli strumenti
bisogna comprendere la
differenza tra
Open Source - Free
e Strumenti Professionali

Evoluzione degli strumenti hardware professionali

Perché usare uno strumento professionale piuttosto che Open Source?

Lo scenario tipico di attività aziendali potrebbe essere: Cristallizzare 30 computer in 24 ore…

- ✓ Sistemi come Logicube Falcon, Mediaclone Field, Tableau Tx1 e WiebeTECH Ditto DX supportano acquisizioni multiple fisiche, via rete (anche a 10Gb con il Tx1 e Falcon NEO), su Hard Disk, NAS e repository di rete, anche con il protocollo iSCSI.
- ✓ Apparati come il Mediaclone Field sono equipaggiati anche con software di analisi come Oxygen, FTK, X-ways Forensics, Cellebrite UFED 4PC, ecc.
- ✓ Tutti questi strumenti sono costruiti per avere le massime prestazioni di copia, calcolo e verifica di HASH, anche multipli.
- ✓ Il Ditto DX si può inserire in rete in modalità stealth, e può essere agganciato per fare acquisizioni in rete via vpn e interfaccia web.
- ✓ Tutti i sistemi sono dotati di write blocker certificato. Impediscono l'errore umano.
- ✓ Sono upgradabili e supportati nel tempo.

…ma ricordate sempre che se uno strumento si rompe, dovete saper usare bene anche sistemi Open Source e write blocker software!

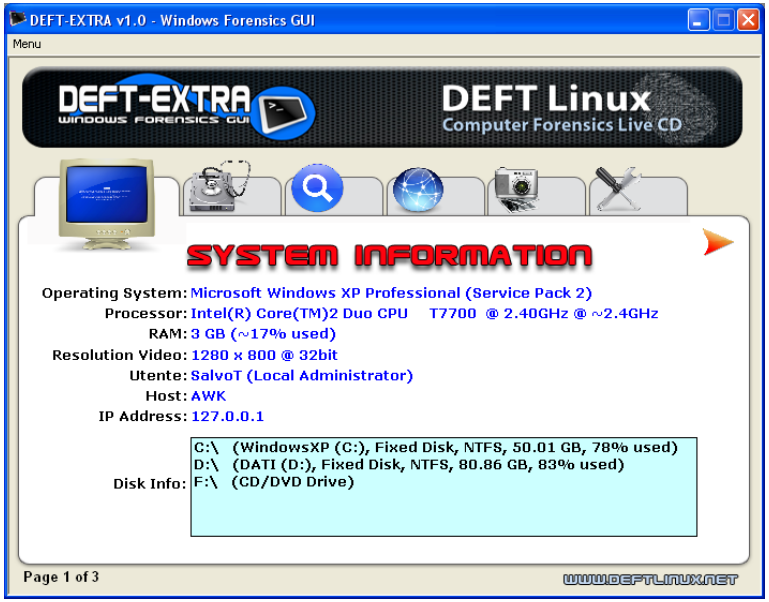
Evoluzione degli strumenti hardware professionali

CAINE is an Italian GNU/Linux live distribution created as a project of Digital Forensics .

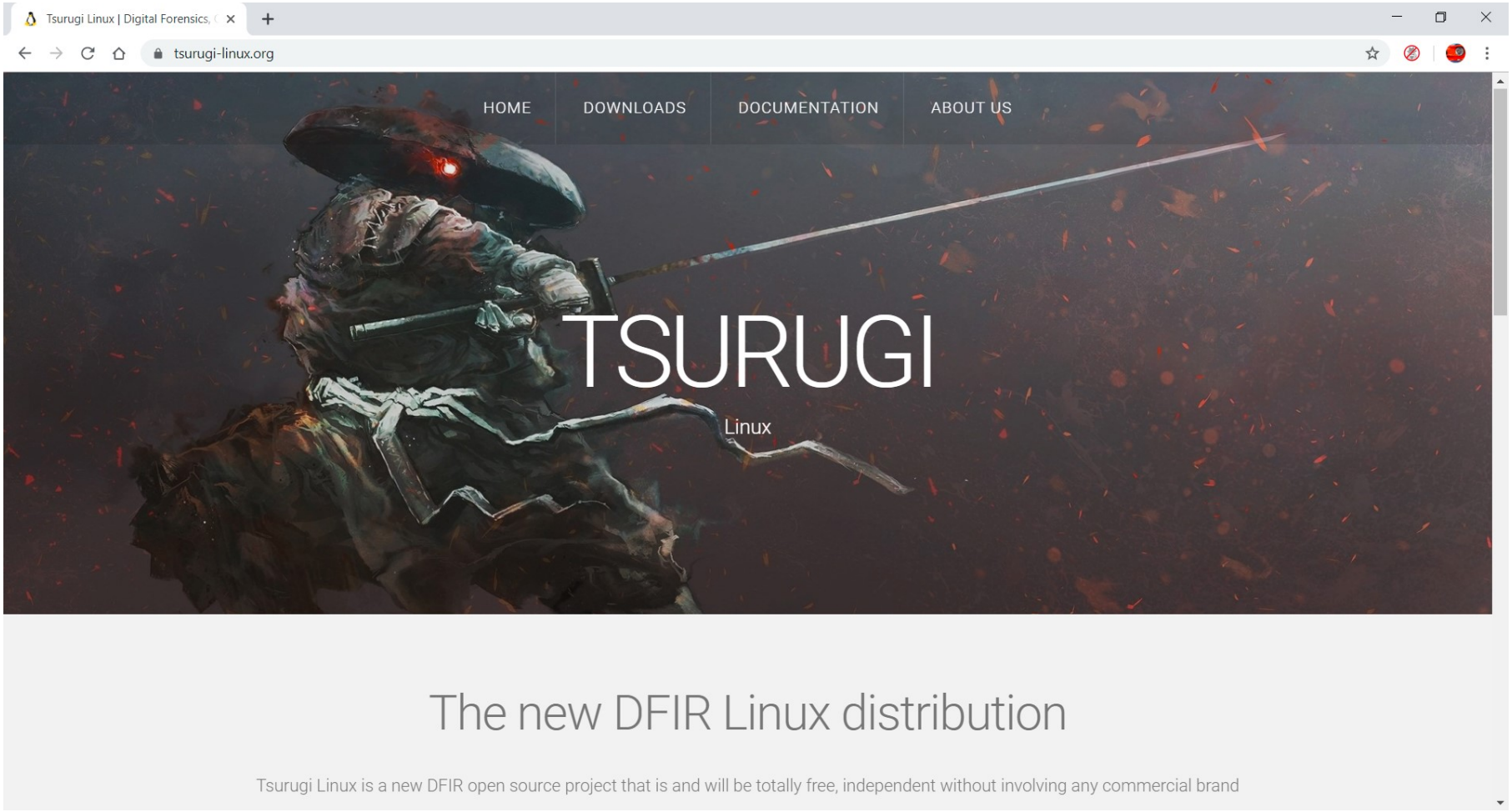
Windows Side Ready

Evoluzione degli strumenti hardware professionali

Xubuntu Kernel 2.6.31 (Linux side)
DEFT Extra 2.0 (Computer Forensic GUI) with the best freeware Windows Computer Forensic s tools



Evoluzione degli strumenti hardware professionali



Evoluzione degli strumenti hardware professionali

LOGICUBE FALCON

- ✓ Falcon Verified By NIST
- ✓ Extreme speed, imaging at over 30GB/min*
- ✓ Image & verify from 4 source to 5 destination drives
- ✓ Write-blocked preview & triage directly on the Falcon
- ✓ Image to/from a network location
- ✓ Multi-task.Perform image, wipe, hash tasks concurrently
- ✓ Logical Imaging. Targeted Imaging feature creates a logical image using pre-set, custom filters, file signature files and keyword search to capture only specific files needed
- ✓ Partition Imaging. Select and image specific partitions on the source drive
- ✓ BitLocker support. Image source drives that have been encrypted using BitLocker
- ✓ Supports PCIe SSDs (M.2 SATA/AHCI/NVME), PCIe and mini-PCIe cards with optional adapters

Evoluzione degli strumenti hardware professionali

LOGICUBE FALCON NEO

- **Extreme speed, imaging at surpassing 50GB/min*. Clone PCIe to PCIe at speeds over 90GB/min.**
- **Image directly to/from Thunderbolt™ 3/USB-C external storage enclosures with an optional I/O card.**
- **Image & verify from up to 5 source to up to 9 destination drives for ultra-efficient imaging.**
- **Concurrent Image+Verify feature. Verification starts shortly after imaging process begins, significantly reducing the image plus verification process time.**
- **Image to/from Fibre Channel drives and enclosures with the optional Fibre Channel Module.**
- **Recognize source drives and partitions that are possibly encrypted.**
- **Cloud storage acquisition software renewable option provides convenient capture of OneDrive, Google Drive, and Dropbox files.**
- **Capture from mobile devices including Apple® iPhones, iPads, Android phones and tablets with an optional renewable software package.**
- **Secure Erase NVMe SSDs.**
- **File Browser/write-blocked drive preview feature provides logical access to drives and network repositories connected to Falcon-NEO. View contents of dd, e01, ex01, and dmg image files created by Falcon-NEO.**
- **Secure sensitive evidence data with whole disk, open standard, drive encryption using the NIST recommended XTS-AES-256 cipher mode, decrypt using Falcon-NEO or Veracrypt.**
- **Logical Imaging feature creates a logical image using pre-set, custom filters, file signature files and keyword search to capture only specific files needed.**
- **Image to/from a network location using two 10GbE connections for fast network imaging performance and to minimize bottlenecks.**
- **Image from a laptop using our iSCSI boot client or from a Mac®computer using Target Disk Mode without removing the hard drive.**
- **Multi-task. Perform image, wipe, hash tasks simultaneously. Little or no speed degradation when imaging from three sources to three destinations.**
- **Network Traffic Capture. Capture network traffic, VOIP, internet activity.**

Evoluzione degli strumenti hardware professionali

GUIDANCE TABLEAU Tx1

- ✓ CUSTOM-BUILT FOR DIGITAL INVESTIGATIONS
- ✓ In the lab, or in the field, the **NEW Tableau Forensic Imager (TX1)** acquires more data, faster, from more media types, without ever sacrificing ease-of-use or portability.
- ✓ Successor to the Tableau TD3 and redesigned from the circuit board up, the TX1 is built on a custom Linux kernel, making it lean and powerful. Every component is hand-selected and tested to guarantee reliability and performance when conducting forensic imaging operations.
- ✓ BROAD MEDIA SUPPORT
- ✓ The TX1 can forensically image a broad range of media, including PCIe and 10Gb Ethernet devices, and supports up to two active forensic jobs at a time (simultaneous imaging). When imaging, TX1 outputs to raw .DD and .dmg formats, .e01 (compressed), or .ex01 (compressed), and features extensive file system support (ExFAT, NTFS, EXT4, FAT32, HFS+).
- ✓ **TX1-S1 DRIVE BAY**
- ✓ Adds two additional cable-less SATA/SAS destination drive connections to the TX1
- ✓ Compatible with 2.5” and 3.5” SATA/SAS drives
- ✓ Internal fan provides drive cooling
- ✓ Easy modular connection – Just slide to connect/disconnect from the TX1

Evoluzione degli strumenti hardware professionali

CRU WiebeTECH Ditto DX

- ✓ Native Suspect Inputs: USB 3.0, SATA /eSATA, PATA, Ethernet (iS
- ✓ Native Outputs: Dual USB 3.0, Dual SATA/eSATA, SD card, and Ethernet (iSCSI, NFS, SMB)
- ✓ A new status bar that is colour coded so you can instantly see the status of the process.
- ✓ Massively improved imaging speeds: The Ditto DX now images logically at twice the speed of Ditto, saving you precious time on imaging large data storage areas. SSD to SSD imaging is also doubled.
- ✓ The Ditto DX retains the same hardwearing fanless casing, allowing the covert application of the DX. The multiple data acquisition formats:.E01; clone; dd all of which is backed up by MD5,SHA-1 and SHA-256 hashing makes it a formidable forensic tool.
- ✓ The powerful web interface has been improved and still allows the full preview of remote attached devices; discover files by file type; multiple accounts to fully control the users' interaction with the DX.

Evoluzione degli strumenti hardware professionali

MEDIACLONE FIELD

- ✓ The SuperImager Plus 8” Field Unit (i7) - is a mobile, compact an extremely fast Forensic Imaging unit that can serve as a complete Field Computer Forensic
- ✓ Investigation platform. The unit is running under Linux Ubuntu OS and it can perform:
  - ✓ Forensic Imaging with full compression
  - ✓ Erase Data
  - ✓ View Data
  - ✓ Encrypt Data
  - ✓ Cellphone/Tablets Extract and Analysis Data, and Forensic Full Analysis.
- ✓ Some example of the unit’s performances:
  - ✓ Complete HASH verification operation with SHA-1 enabled on SSD @ 31GB/min, on WD 1TB Blue @10GB/min
  - ✓ Complete Forensic Imaging 1:2 with SHA-1 enabled on 3 SanDisk Extreme II 120GB SSD @ 29GB/Min
  - ✓ Forensic Imaging of 1:2 with E01 format with compression level 1 @ 8GB/min
- ✓ The SuperImager® Plus 8” Field unit is very compact and easy to carry, has built-in 8” Touchscreen color LCD display, 4 native SAS/SATA ports, 6 native USB3.0 ports, e-SATA port, 1Gigabit Ethernet ports, HDMI port, and audio ports.

Evoluzione degli strumenti hardware professionali

Cellebrite UFED

Evoluzione degli strumenti hardware professionali

Attenzione: i cellulari, gli smartphone e tablet devono essere sempre acquisiti in modalità irripetibile (ex 360 cpp).

Garantendo comunque la minima alterazione possibile.

Come è possibile?

Esistono scuole di pensiero diverse?

SI

ma si offre il fianco ad una invalidazione tramite contropeizia

Evoluzione degli strumenti hardware professionali

Faraday Bag

Clone della SIM

Faraday Box

Jammer

Agenda

- Presentazione relatore
- Riepilogo delle regole fondamentali
- Accenni alla ISO27037
- Evoluzione degli strumenti hardware professionali
- Evoluzione degli strumenti software professionali
- Live Forensics e Sniper Forensics
- Qualche esempio pratico
- Q&A

Evoluzione degli strumenti software professionali

Prima di parlare di software professionali, va ricordato che ci si deve dotare di workstation professionali come Talino e FRED

Evoluzione degli strumenti software professionali

Attualmente i software professionali specifici per analisi di digital forensics presenti sul mercato sono:

- Nuix Investigate
- AccessData FTK
- OpenText Guidance EnCase
- Magnet AXIOM
- Xways-Forensics
- The Sleuthkit Autopsy

I più diffusi anche nelle forze di polizia internazionale sono

Molti offrono suite di e-discovery complete per investigazione con più operatori e su ambienti enterprise…

Evoluzione degli strumenti software professionali

Nuix Investigate

Visualize large volumes of information and communications to find hidden connections among people, objects, locations, and events

Collaborate within and across teams to share insights and find critical facts faster, putting the right data into the hands of the right people, no matter where they are.

Ingest data from all evidence sources into a single platform with a unified view.

Merge Challenging Data into Meaningful Intelligence

Evoluzione degli strumenti software professionali

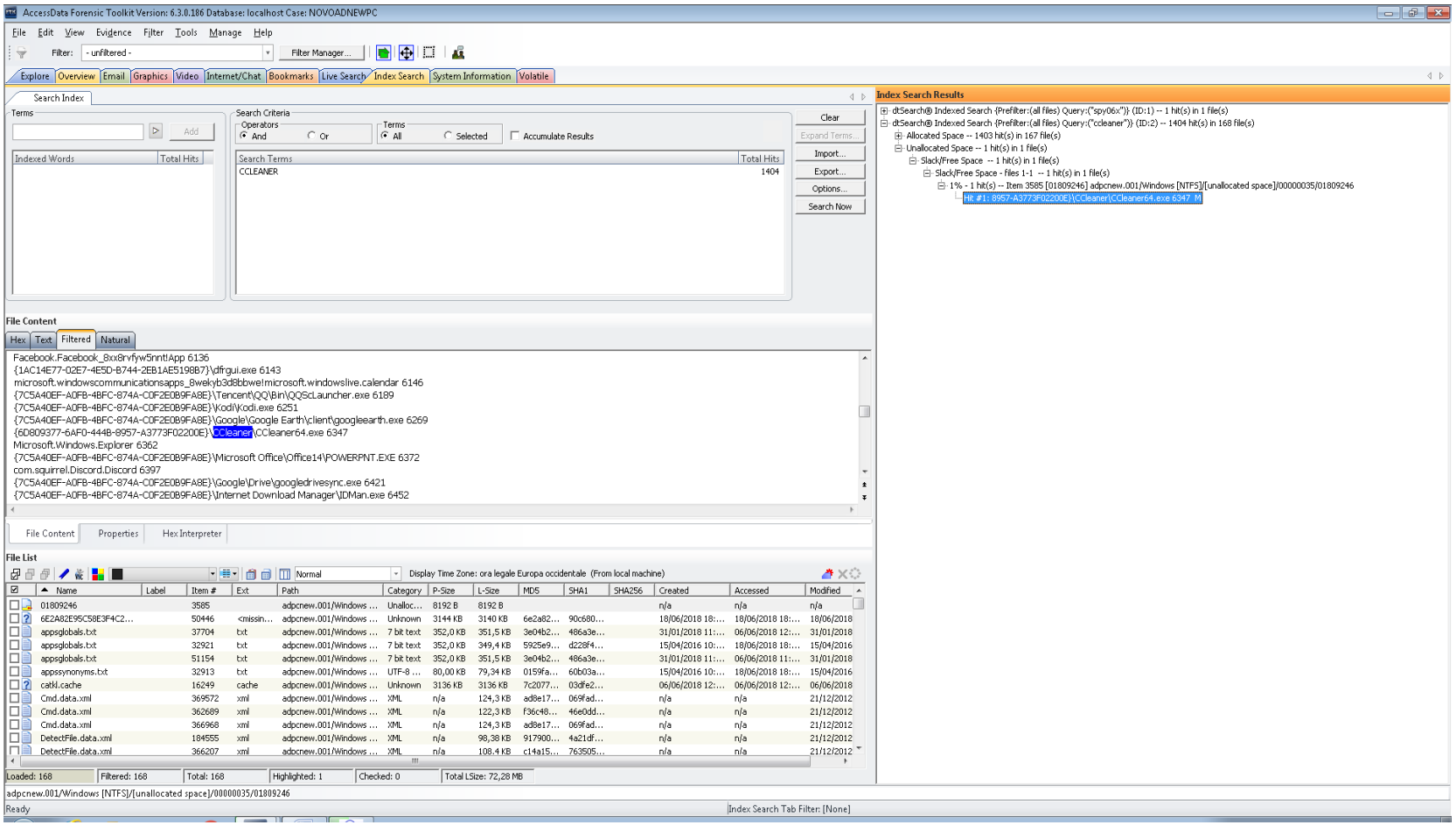
ACCESSDATA

UNMATCHED SPEED AND STABILITY

FASTER SEARCHING

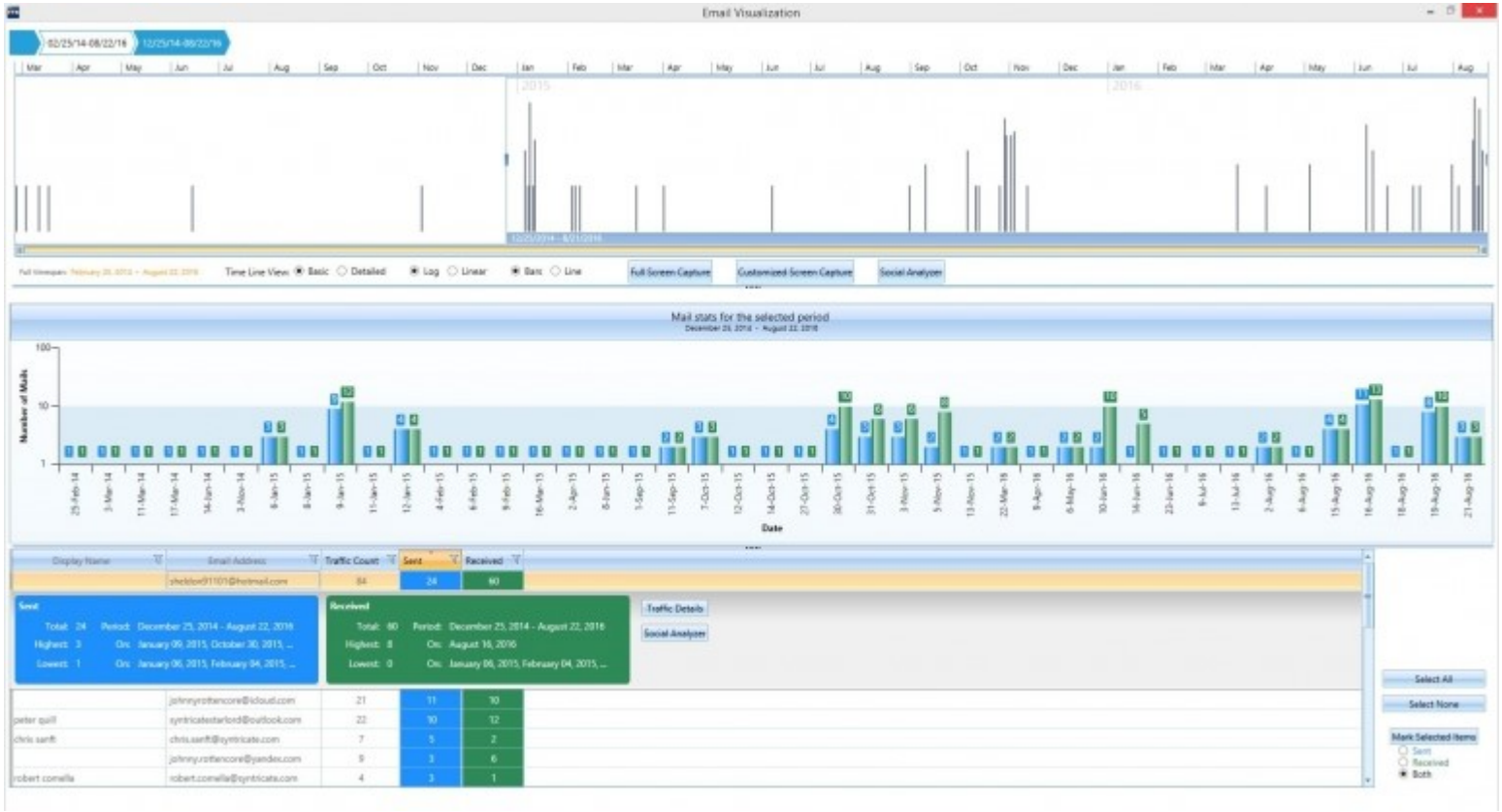
DATABASE DRIVEN

Evoluzione degli strumenti software professionali



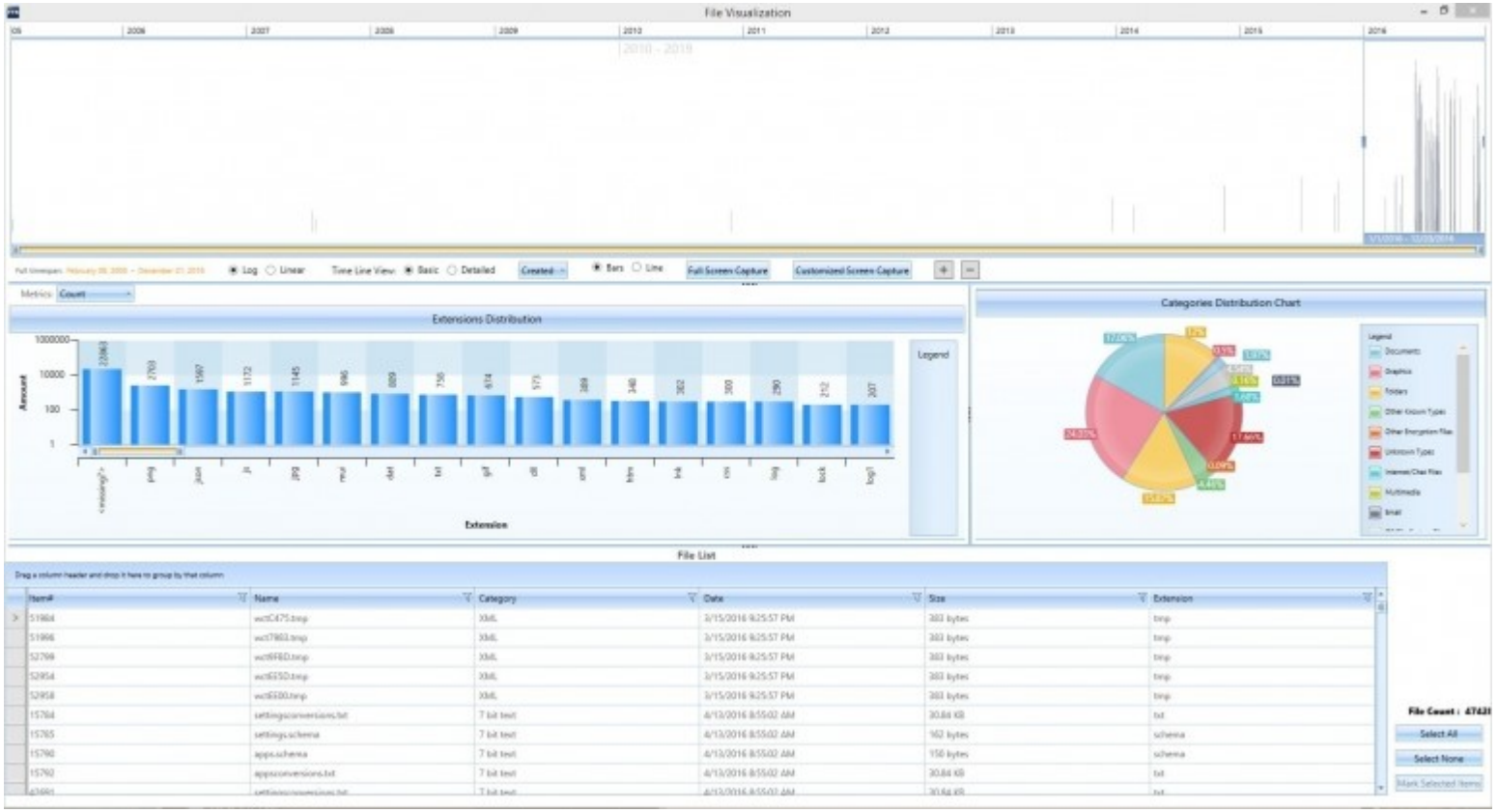
Evoluzione degli strumenti software professionali

ACCESSDATA



Evoluzione degli strumenti software professionali

ACCESSDATA

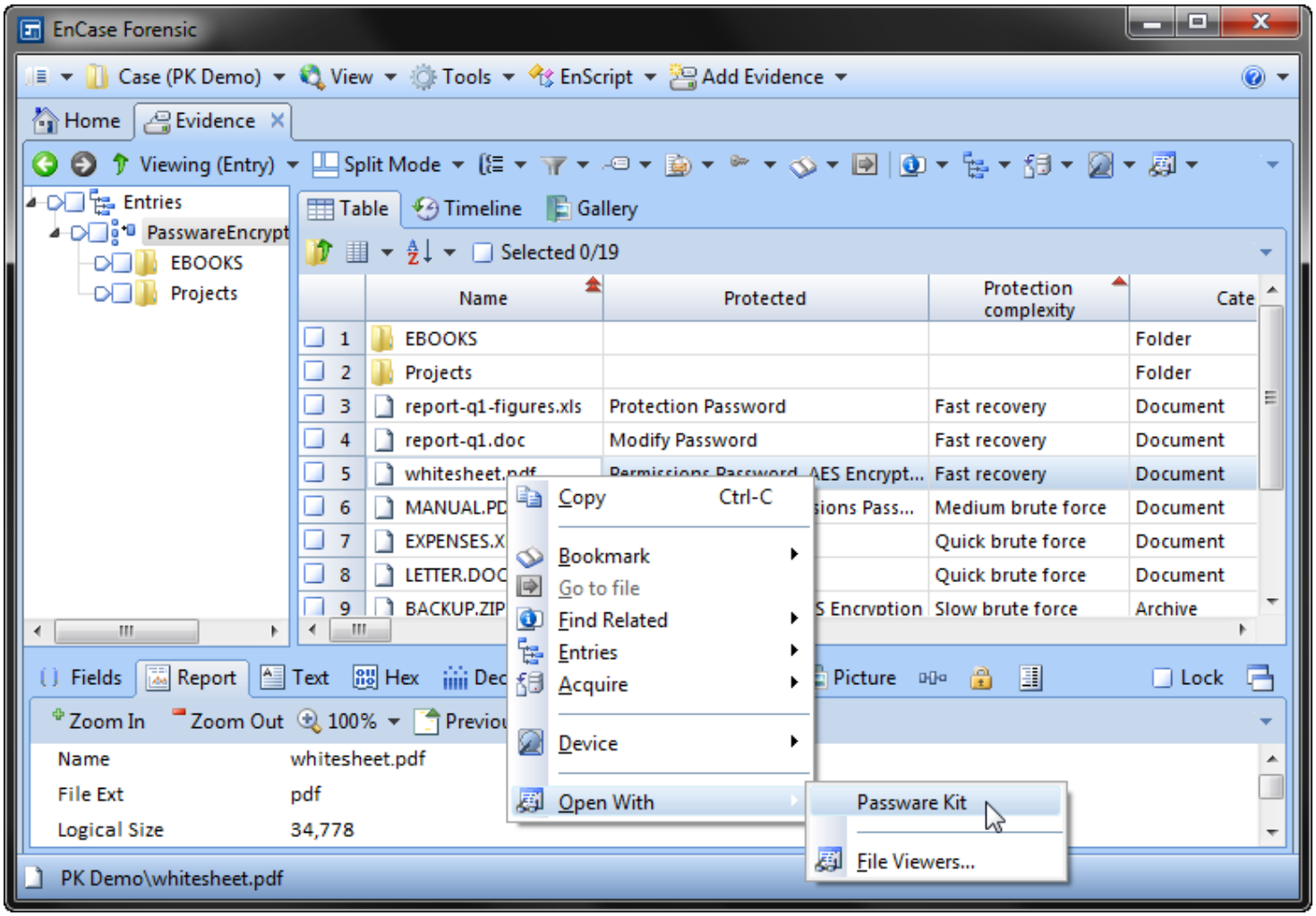


Evoluzione degli strumenti software professionali

COMPLEMENTARY PRODUCTS

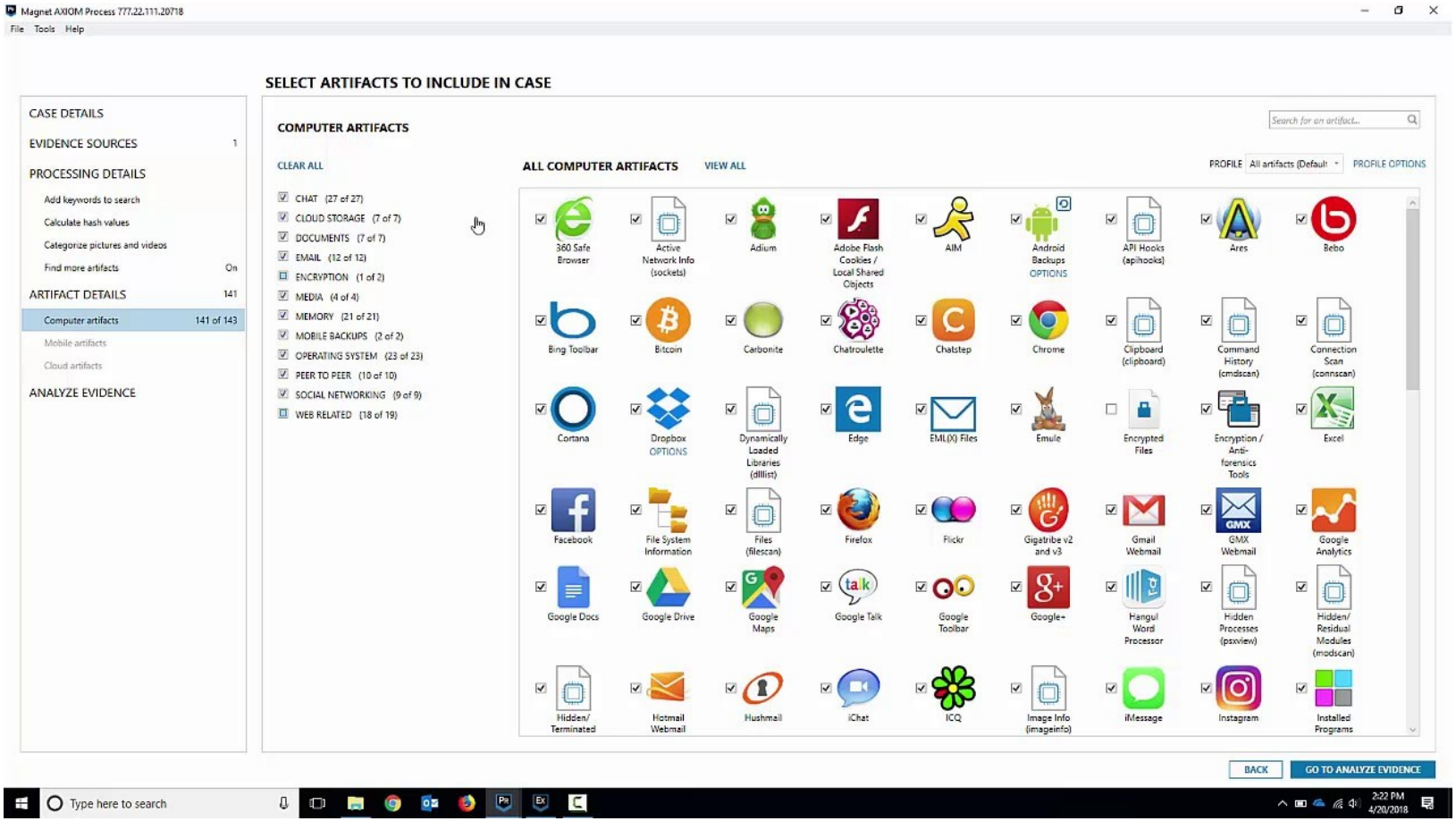
- **QUIN-C™**
  Deeper Insights from Dynamic Investigations
- **AD Lab**
  Large-Scale Investigation and Processing
- **Cerberus**
  Proactively identify compromised systems
- **AD Triage**
  On-scene Computer Collection
- **Mobile Solutions**
  MPE+® and nFIELD™

Evoluzione degli strumenti software professionali



Evoluzione degli strumenti software professionali

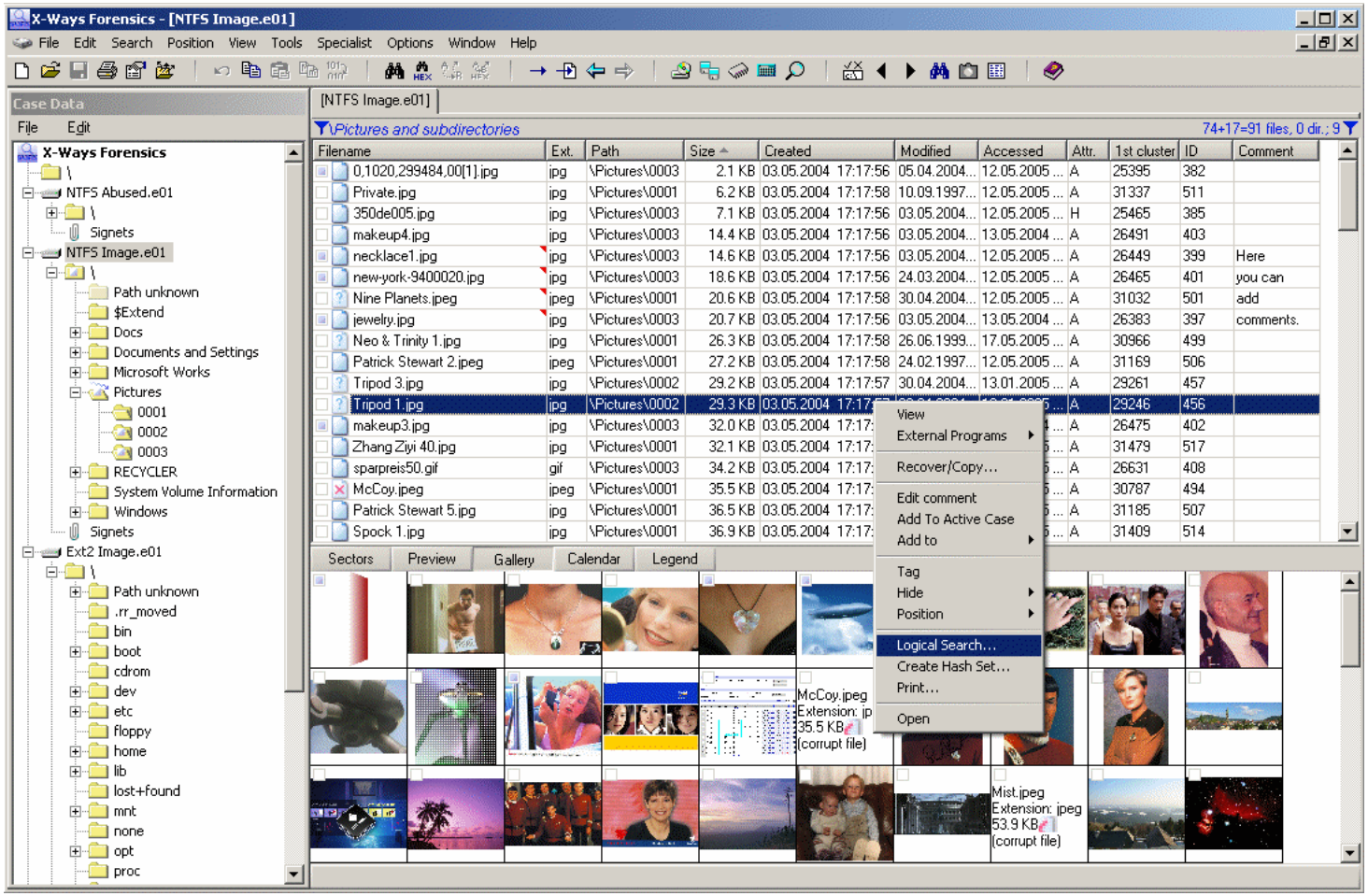
MAGNET FORENSICS



ISACA Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Evoluzione degli strumenti software professionali

X-Ways Forensics

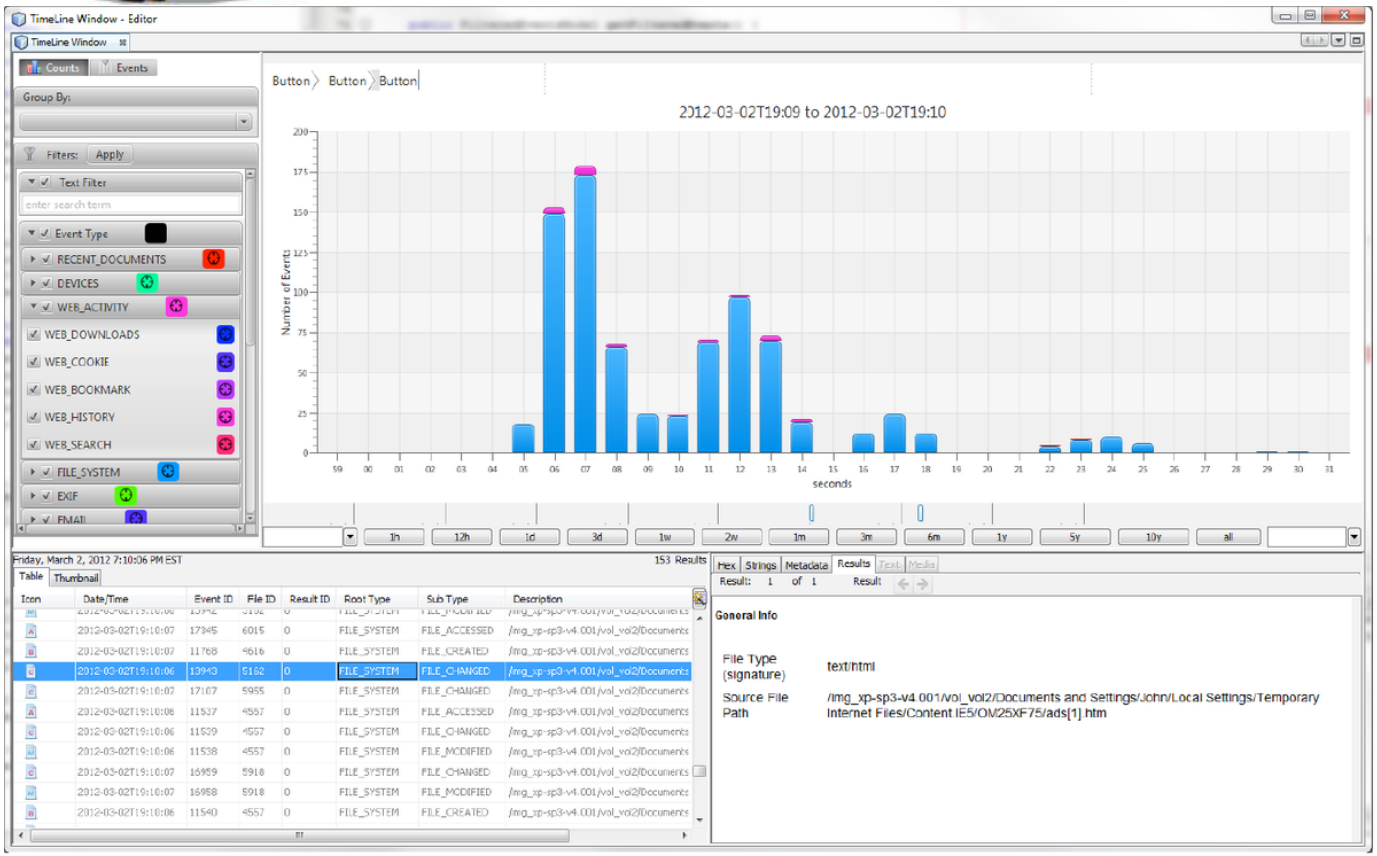


Evoluzione degli strumenti software professionali

Autopsy®

BASIS TECHNOLOGY

Attualmente Ancora GRATUITO



Evoluzione degli strumenti software professionali

Esistono poi una serie di software a corredo per attività specialistiche, come:

Live forensics tool
Cyber Triage
Malware Forensics
Intelligence
OSINT
Crittoanalisi
ecc.

Agenda

- Presentazione relatore
- Riepilogo delle regole fondamentali
- Accenni alla ISO27037
- Evoluzione degli strumenti hardware professionali
- Evoluzione degli strumenti software professionali
- Live Forensics e Sniper Forensics
- Qualche esempio pratico
- Q&A

Live Forensics

1. *Attività non ripetibile (alterazione parziale ram e dati in movimento)*
2. *Minimizzare l'impatto sul sistema (tool live)*
3. *Evitare il blocco del sistema (mouse jiggler)*

Tipicamente si svolge nei seguenti passaggi:

- *Definire attività sulla rete: dump o disconnessione*
- *Acquisire RAM*
- *Conoscere processi in esecuzione*
- *Conoscere attività di rete e IP della macchina*
- *Verificare presenza volumi cifrati ed acquisire*
- *Rilevazione ultime attività di sistema*
- *Rilevazione password*
- *ecc.*

Live Forensics

Necessità di assegnare una priorità a causa della volatilità dei dati, generalmente:

1. *Memoria RAM*
2. *File di Swap*
3. *Processi di rete*
4. *Processi di sistema*
5. *Informazioni del file system*
6. *Password utenti*
6. *Volumi logici cifrati e presenti in chiaro*
7. *Volumi fisici*

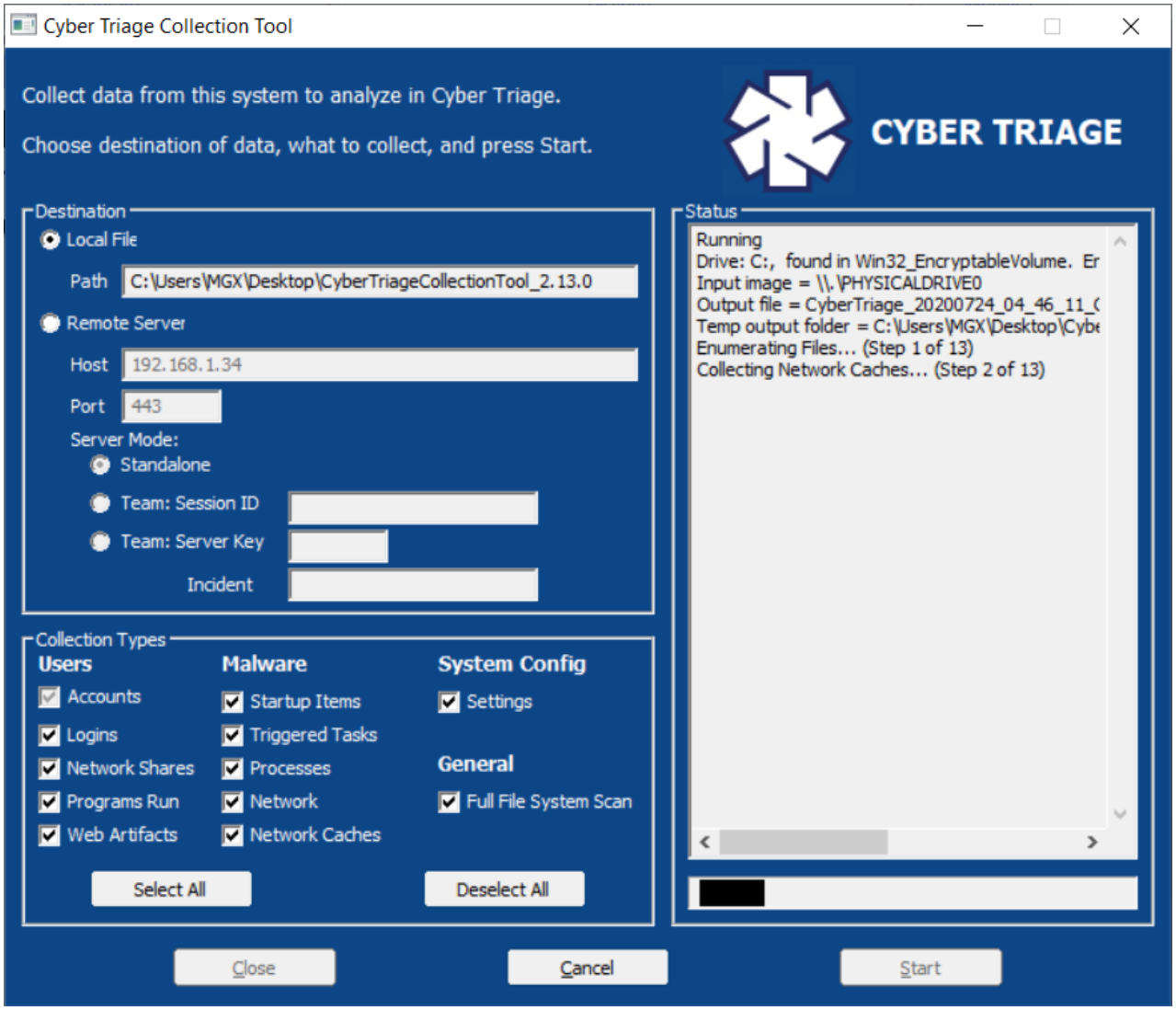
Live Forensics e Sniper Forensics

La scelta dei tool avviene testando molti prodotti in laboratorio, scegliendo la suite più completa possibile. Trovate diversi link nella slide SITOGRAFIA.

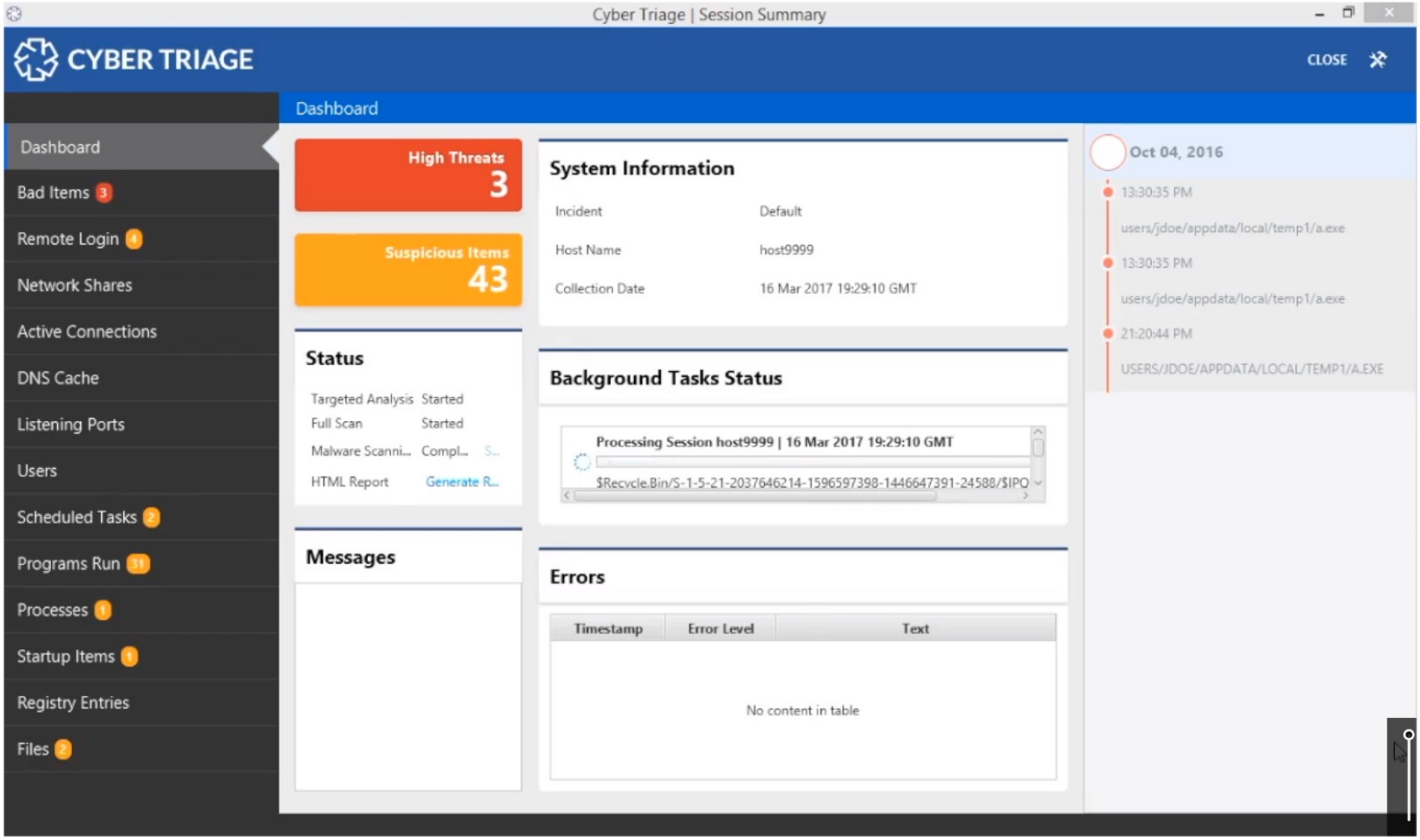
Durante la live forensics ricordare che:

1. *Prima di operare assicurarsi di avere i diritti di amministratore*
2. *Ogni azione intrapresa deve essere verbalizzata con i riferimenti temporali*
3. *Gli strumenti usati dovranno essere fidati e collaudati, e devono essere eseguiti su una chiavetta USB creata ad hoc*
4. *I dati estratti devono essere sottoposti ad hash, prima di essere analizzati*
5. *I dati che non sono volatili, devono essere acquisiti secondo metodologia post mortem*

Live Forensics e Sniper Forensics



Live Forensics e Sniper Forensics



Sniper Forensics

Il servizio di Sniper Forensics è mirato a dare risposte rapide e circoscritte.
Una normale analisi di Digital Forensics esaustiva e ripetibile può richiedere mesi di lavoro.
Se per risolvere un caso, il cliente ha una domanda precisa e gli serve un dato specifico e solo quello…
Il servizio di analisi mirata a dare una sola risposta richiede meno tempo e reportistica di tipo smart.
E' una soluzione più economica di una generica analisi di digital forensics tradizionale.

Agenda

- Presentazione relatore
- Riepilogo delle regole fondamentali
- Accenni alla ISO27037
- Evoluzione degli strumenti hardware professionali
- Evoluzione degli strumenti software professionali
- Live Forensics e Sniper Forensics
- Qualche esempio pratico
- Q&A

Qualche esempio pratico

Catena di Custodia

DIGITAL EVIDENCE CHAIN OF CUSTODY FORM						
CASO N.	1		Pag.	1	di	1
Tipologia media/pc sequestrato						
Oggetto N.	1	Descrizione	Hard Disk ISACAROMA			
Marca	Seagate		Modello	ATA ST960813AS		
Note	interfaccia dati SATA					
Foto reperto:						

Dettagli acquisizione						
Data	24/07/2020	Ora	13:10	Creato da	LOGICUBE FALCON NEO	
Metodo usato	DD 2Gb + V Disco	Nome immagine	ESERCIZIO1		Numero segmenti	28
Storage Drive	5LY7EYA2	Alg. HASH	Md5 + Sha1	Hash	MD5: 0x086E478BF4C15146B05966035EB51344 SHA1: 0x600DEE45BA8A96F1B90B931F00340ECA2ADC8FF2	

Catena di Custodia				
Operazione N.	Data e Ora	Da	A	Motivazioni
1	Data:24/07/2020	Nominativo:Massimiliano Graziani	Nominativo:Glauco Benigno	Acquisizione e analisi contenuto del dispositivo
	Ora:14:00 PM	Firma:	Firma:	
2	Data:	Nominativo:	Nominativo:	
	Ora:	Firma:	Firma:	
3	Data:	Nominativo:	Nominativo:	
	Ora:	Firma:	Firma:	
4	Data:	Nominativo:	Nominativo:	
	Ora:	Firma:	Firma:	

Vediamo alcuni modelli di incarico

Qualche esempio pratico

Qualche esempio pratico

Progetto NEXT:

valigetta da campo

con

dotazioni di base

per digital forensics.

Qualche esempio pratico

Vediamo uno smart report sniper forensics

Qualche esempio pratico

Vediamo una consulenza tecnica reale

Agenda

- Presentazione relatore
- Riepilogo delle regole fondamentali
- Accenni alla ISO27037
- Evoluzione degli strumenti hardware professionali
- Evoluzione degli strumenti software professionali
- Live Forensics e Sniper Forensics
- Qualche esempio pratico
- Q&A

Sitografia pagina 1

Titolo	URL
IISFA	https://www.iisfa.it/
ONIF	https://www.onif.it/
CAINE	https://www.caine-live.net/page11/page11.html
DEFT	http://www.linuxandubuntu.com/home/deft-linux-a-linux-distribution-for-computer-forensics
TSURUGI	https://tsurugi-linux.org/downloads.php
NIRSOFT tools	https://www.nirsoft.net/utils/
LIVE 4N6 tools	https://techtalk.gfi.com/top-20-free-digital-forensic-investigation-tools-for-sysadmins/
Magnet Forensics Tools	https://www.magnetforensics.com/blog/new-magnet-custom-artifact-generator-and-other-updated-free-tools/
Marco Mattiucci resources	http://www.marcomattiucci.it/informatica_digitalforensics_liveforensics.php
FTK Imager	https://accessdata.com/products-services/forensic-toolkit-ftk/ftkimager
Manuale FTK Imager su Reality.net	http://www.realitynet.it/services/digital-forensics/tutorial/acquisizione-di-un-hard-disk-con-ftk-imager/
FTK Imager video tutorial	https://www.youtube.com/watch?v=TkG4JqUcx_U
FTK Imager Lite	https://support.accessdata.com/hc/en-us/articles/203681809-Run-FTK-Imager-from-a-flash-drive-Imager-Lite-

Sitografia pagina 2

Titolo	URL
Computer Forensics Tools	https://resources.infosecinstitute.com/7-best-computer-forensics-tools/#gref
LOGICUBE	https://www.logicube.com/shop/category/forensics-solutions/?v=cd32106bcb6d
MEDIACLONE	http://www.media-clone.net/
Guidance Tableau TX1	https://www.forensiccomputers.com/tableau-tx1-forensic-imager.html
CRU Wiebetech	https://www.cru-inc.com/products/wiebetech/
AccessData FTK	https://accessdata.com/products-services/forensic-toolkit-ftk
Guidance EnCase	https://resources.infosecinstitute.com/category/computerforensics/introduction/commercial-computer-forensics-tools/encase-product-suite-overview/#gref
Magnet AXIOM	https://www.magnetforensics.com/
Xways Forensics	http://www.x-ways.net/forensics/
Memberbook IISFA Versione digitale anche gratuita per kindle	https://www.amazon.it/s?k=iisfa+memberbook&i=stripbooks&__mk_it_IT=%C3%85M%C3%85%C5%BD%C3%95%C3%91&ref=nb_sb_noss_1

Contatti

massimiliano.graziani@cybera.it

Dubbi, altre domande? Desiderate approfondimenti riguardo gli argomenti trattati? Scrivetemi, rispondo sempre a tutti!

Grazie…

Era il 6 giugno 2018 mentre ero relatore al Security Summit di Roma, non rispondevo al cellulare e non potevo soccorrere mio padre, colto da un infarto, mentre tutti mi chiamavano…

Tra sensi di colpa e rimorso per non essere arrivato in tempo per vederlo ancora vivo, per l'ultima volta…
…alla fine ho superato questo blocco dedicando a Giuseppe, mio padre, ogni attività di divulgazione e condivisione accademica, sempre con la stessa umiltà e passione che mi ha contraddistinto negli anni.

Grazie di tutto papà.

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter