Computer Forensics
nel nuovo panorama tecnico investigativo italiano

a cura di **Massimiliano Graziani**

CIFI CFE ACE OPSA

Board of Directors IISFA Italian Chapter

Senior Security Consultant Visiant Security

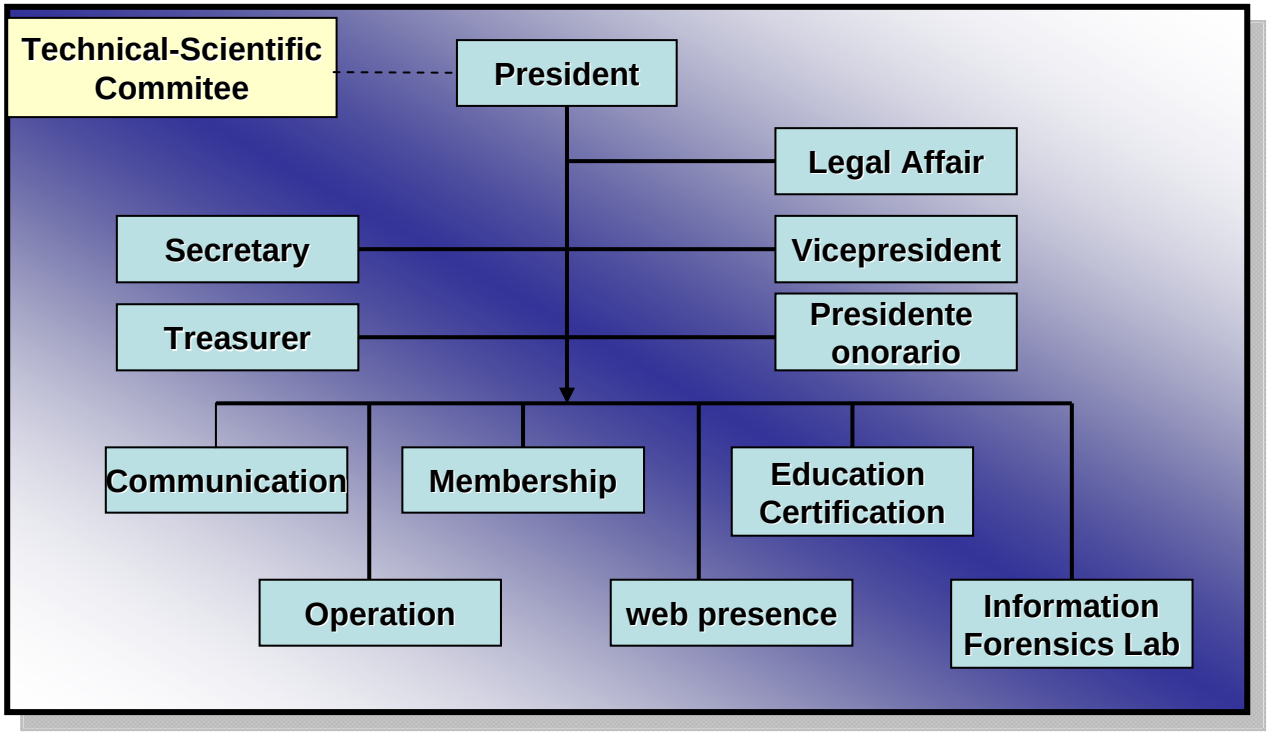
INDICE DELLA PRESENTAZIONE :

Che cosa è IISFA?

- L'International Information Systems Forensics Association (IISFA) è un organizzazione senza scopo di lucro, aperta a tecnici e giuristi, con la missione di promuovere la disciplina dell'information forensics attraverso la divulgazione, l'apprendimento e la certificazione.

- Le attività ruotano intorno ad un codice etico ed alla possibilità di far parte di un network di specialisti, con lo scopo di costituire insieme una squadra che, nel medio periodo, rappresenti un punto di riferimento nello specifico settore, allo stato sottolineato da forti individualità

Breve presentazione di IISFA



SOCI
Istituzionali, Ordinari
(cyber law, forze dell'ordine, professional , aziende)

Breve presentazione di IISFA

Breve presentazione di IISFA

la Certificazione come metodo e non come titolo nell'Information Forensics

Anticipazione 2010 nuove certificazioni CIFI e CIFE

INDICE DELLA PRESENTAZIONE :

Information forensics….

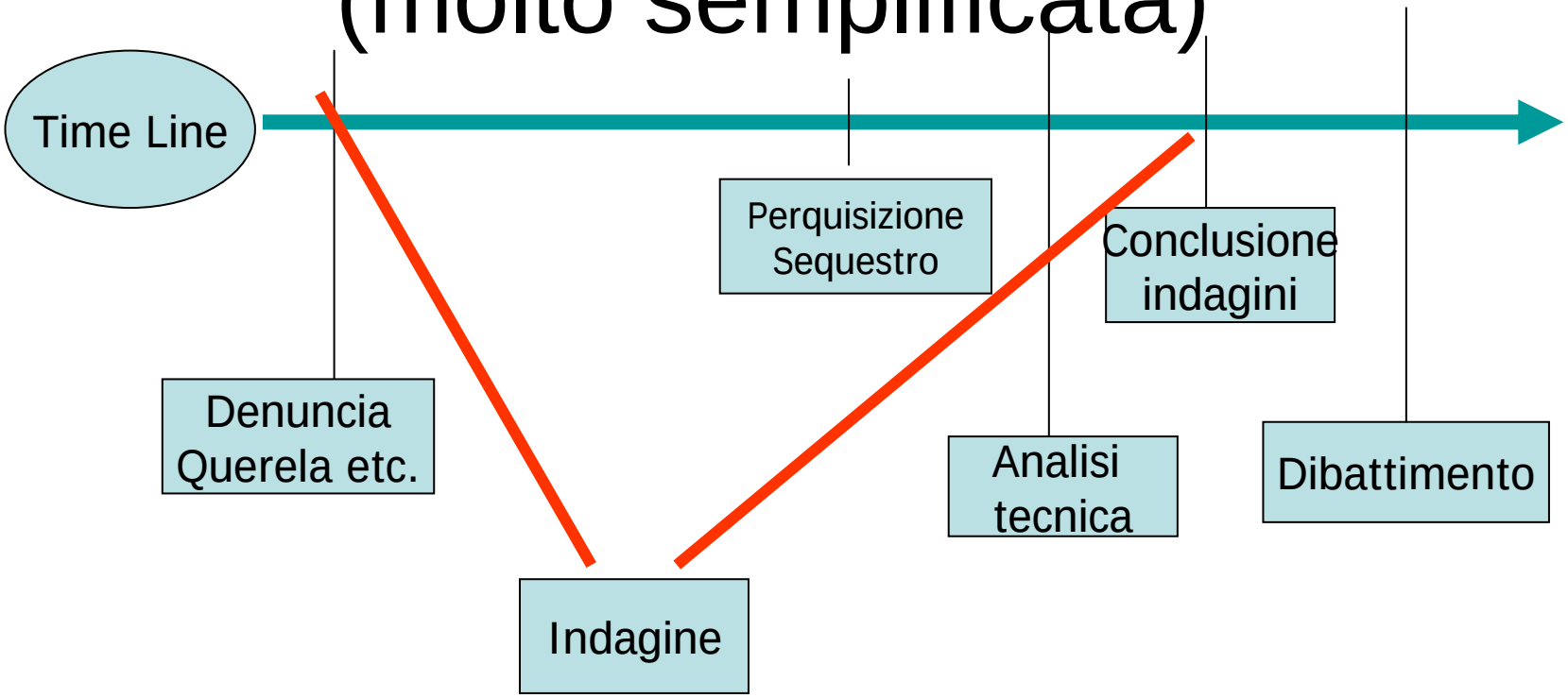
- Disciplina che si occupa della preservazione, dell'identificazione, dello studio, della documentazione dei computer, o dei sistemi informativi in generale, al fine di evidenziare prove per scopi di indagine.

Il ruolo del computer

- Parte "attiva" dell'azione criminale..
- Obiettivo di atti criminali….
- Contenitore delle prove per attività illecita di tipo "comune"…..

Il ruolo del computer

Attività investigativa (molto semplificata)



INDICE DELLA PRESENTAZIONE :

Tipologie di Computer Forensics

Analisi post-mortem:

Ci si riferisce all'analisi di una macchina fatta dopo un'intrusione perpetrata con successo oppure a seguito di un illecito. Nel caso di alcuni reati informatici, l'attività deve essere svolta tenendo conto del fatto che l'intruso potrebbe aver a acquisito privilegi di amministrazione sulla macchina, e che quindi potrebbe avere alterato i log di sistema (questo aspetto riguarda la valutazione dei dati).

Live Forensics Analysis:

Comprende tecniche di analisi su sistemi attivi, sviluppate negli ultimi anni; infatti gli attacchi più recenti spesso non lasciano tracce sugli hard disk ma operano sui dati in memoria, che si perderebbero spegnendo il dispositivo; inoltre spesso i dispositivi di storage connessi sono protetti da meccanismi di cifratura, e le chiavi possono essere contenute in memoria.

Definisce la modalità di analisi

Definisce la locazione del dato

Network Forensics:

Il termine si riferisce all'analisi di sistemi di rete, al fine di determinare elementi probatori inerenti un determinato caso investigativo

Disk Forensics:

Una specifica attività legata all'estrazione di informazioni dagli hard disk dei sistemi, previa generazione di immagini inalterabili su cui effettuare l'analisi o applicazione di altra tecnica a tutela del dato originale.

Memory Forensics:

E' il recupero dell'informazione contenuta nella memoria RAM di un computer, caratterizzata da una forte volatilità (non sopravvive allo spegnimento). Si interseca con la Disk Forensics citata sopra, ove si consideri l'analisi dello SWAP Space

Internet Forensics:

Specializza le tecniche e le metodologie proprie delle altre tipologie di forensics al caso specifico di illeciti che coinvolgono Internet (reati commessi "su" Internet o "mediante" Internet)

INDICE DELLA PRESENTAZIONE :

Le fasi di formazione della “prova informatica”..

Individuazione

(e successivo sequestro/ispezione)

Acquisizione

(durante o post sequestro)

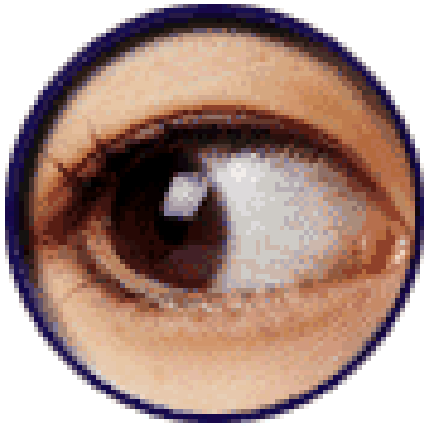
Analisi

(consulente o perito)

Valutazione

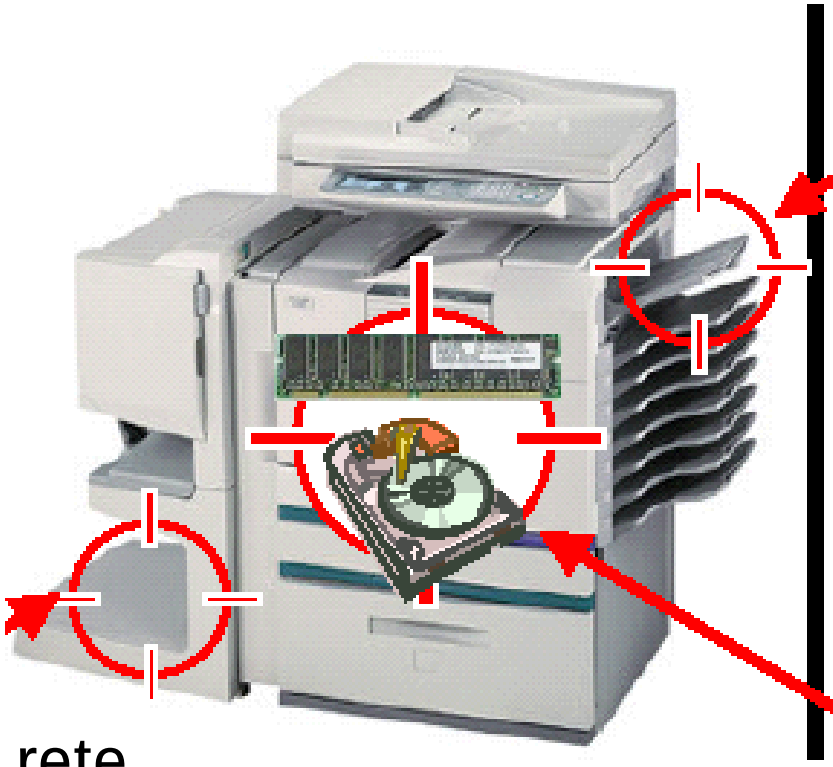
Individuazione

E’ la parte investigativa fondamentale…..
…Capire quali sono gli “oggetti informatici” che “parlano”…



La formazione della "prova informatica“

La formazione della "prova informatica“



Accesso fisico ai risultati

Estrapolazione “storica” dall’hard disk

Accesso in rete

La formazione della "prova informatica“

Il processo di acquisizione del dato deve tenere conto di alcuni vincoli dettati dalle normative

Modalità di acquisizione del dato

	Acquisizione dati in movimento	Acquisizione/Duplicazione	Acquisizione hardware
Modalità	Acquisizione del dato nella sua fase di trasferimento da un sistema all'altro.	Clonazione dispositivo Duplicazione parziale	Principalmente inteso come “sottrazione dell'elemento dalla disponibilità dell'utente” (es. software contraffatto)
Descrizione	L'acquisizione del dato può avvenire in questo caso attraverso l'ausilio di apposite sonde in grado di acquisire log e raccogliere il traffico proveniente da uno o più sistemi	La duplicazione del dato presuppone l'acquisizione del medesimo dal supporto di memoria. La copia del dato (clonazione del dispositivo o duplicazione parziale) deve essere verificata per garantire l'identicità con il dato originale (tecniche di hashing).	Gli asset informatici di proprietà dell'azienda possono essere acquisiti per indagini forensi interne

Che “Tempo” abbiamo?

Rilevare sempre lo scarto orario durante le acquisizioni.

Uno degli errori nella lettura dei LOG, è quella di non dare importanza ai simboli e numeri “intorno” all’orario…

Abbiamo orari GMT, UTC (Zulu)

Acquisizione

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

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

Gli strumenti:

HW: Write Blocker semplici e avanzati

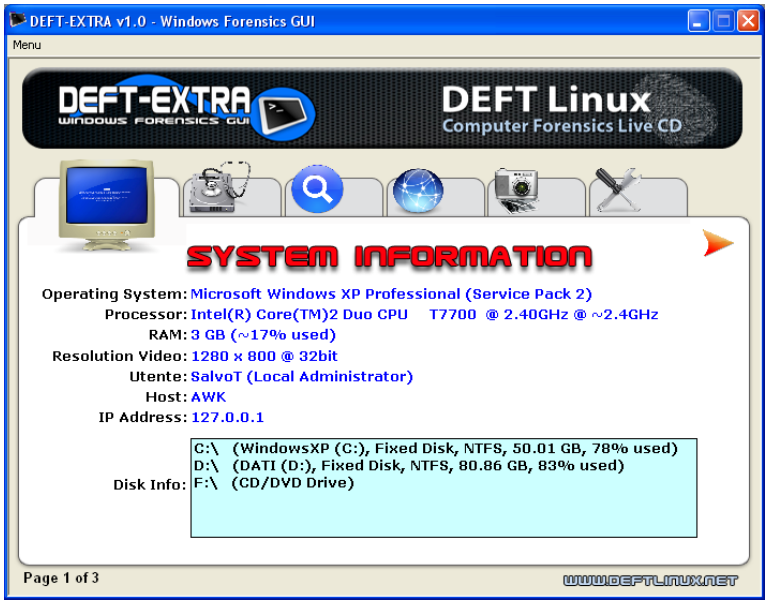
SW Open: DEFT, CAINE, ecc.

SW Closed Freeware: Write Blocker, FTK Imager, ecc.

SW Closed: FTK, Encase, X-Ways Forensics, ecc

La formazione della "prova informatica“

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



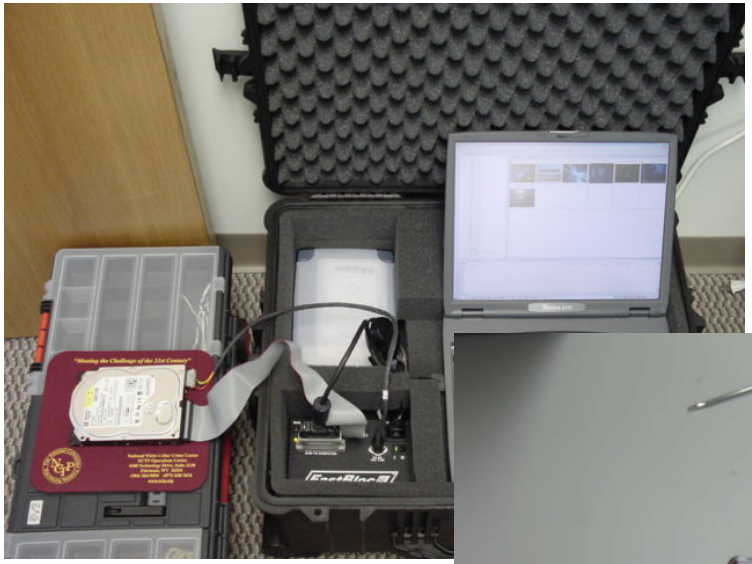
La formazione della "prova informatica“

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

Windows Side Ready

La formazione della "prova informatica“

Un piccolo filmato mostra il funzionamento di un WB HW specifico per CF….



Software per CF

Quando proprio non si può evitare

Ripassiamo…

- La fase più delicata dell’azione di polizia giudiziaria, quando sono “trattate” informazioni digitali, è quella dell’acquisizione.
- E’ necessario, infatti, per evitare sgradite sorprese in fase dibattimentale e consentire eventuali perizie di parte su informazioni “genuine”, che l’attività di analisi delle tracce informatiche sia operata non sull’originale del supporto sequestrato, ma su di una “immagine” dello stesso, consentendo in un secondo momento di effettuare una medesima attività a riscontro delle risultanze investigative ivi compendiate.
- La “bit stream image”, a differenza della mera copia, consentirà di operare su un hard disk praticamente identico all’originale, sia in maniera logica che fisica, quindi anche su eventuali parti presumibilmente vuote dello stesso, che potrebbero contenere file o frammenti di file cancellati non sempre visibili con i normali strumenti di windows.

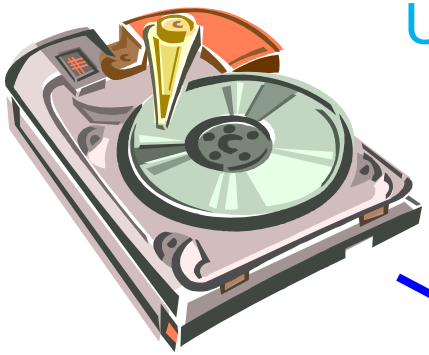
Necessità vs Opportunità

- Utilizzare Software semplice, conosciuto e ritenuto affidabile
- Utilizzare blocchi hardware in scrittura, ove possibile
- Calcolare gli hash dei file/hard disk e fare un report
- Masterizzare più copie ed allegarle al verbale
- Non installare nulla in giro sulle postazioni, specialmente presso aziende
- Documentare il tutto nel migliore dettaglio possibile
- Sterilizzare l’ambiente di analisi

FTK Imager

- Forensics Tool Kit (FTK) è un software di computer forensics.
- Esiste una versione Imager per effettuare le attività di acquisizione forense.
- Tale versione è gratuita ed è utilizzabile in modalità che consente la successiva analisi con altri software di analisi (o con la componente FTK di analisi forense)

…Vediamo….

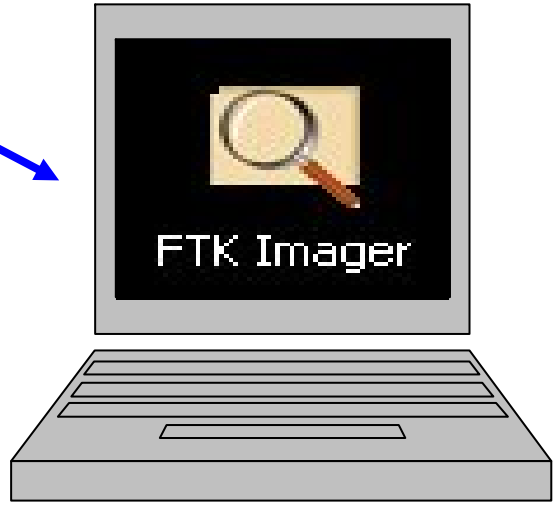


Usando FTK Imager
è possibile:

Esportare hash e
convertire
immagini

Hardware
Write Protect
Device

Preview
Immagine



Alcune proprietà

- Varia in base ai file system
- Mostra le info sulle immagini

Evidence Info

General	
Evidence Source Path	H:\Mantooth\mantooth3.E01
Evidence Type	Forensic Disk Image
Verification Hashes	
MD5 verification hash	c34da7fca44a8a9394e7b2965460dbcd
Drive Geometry	
Bytes per Sector	512
Sector Count	40,718,160
Image	
Image Type	E01
Case number	07-12345
Evidence number	G54321-0000
Examiner	Warren
Notes	
Operating system	Windows XP
Program version	FTKI2.5.2
Acquire date	4/20/2007 7:58:45 PM
System date	4/20/2007 7:58:45 PM
Unique description	Mantooth PC

FAT and NTFS

General	
Name	scan1.jpg
File Class	Regular file
File Size	41,903
Physical Size	45,056
Start Cluster	48,372
Date Accessed	3/6/2007 2:03:11 AM
Date Created	3/6/2007 1:52:35 AM
Date Modified	3/6/2007 1:18:00 AM
Encrypted	☐
Compressed	☐
DOS Attributes	
Hidden	☐
System	☐
Read only	☐
Archive	☑
NTFS Information	
MFT Record Number	41,545
Record date	3/6/2007 2:03:11 AM
Resident	☐
Offline	☐
Custom Content	☐
Temporary	☐
Owner SID	S-1-5-32-544
Owner Name	Administrators
Group SID	S-1-5-21-3166329-3263506726-1320
NTFS Access Control Entry	
ACE Type	Allow Access
SID	S-1-5-21-3166329-3263506726-1320
Access Mask	001f01ff
Execute File	☑

Proprietà

Varia a file system

Linux/EXT

General	
Name	wineusr-guide.pdf
File Class	Regular file
File Size	257,306
Physical Size	258,048
Start Cluster	6,025,217
Date Accessed	5/22/2007 3:56:38 AM
Date Created	5/21/2007 11:11:03 PM
Date Modified	5/21/2007 11:10:58 PM
UNIX Security Attributes	
Unix Permissions	-rw-r--r--
UID	1,000
GID	1,000
Ext2/3 Information	
Inode Number	2,992,459

MAC/HFS

General	
Name	FTK 2.0 BLURB MARCH 2007.doc
File Class	Regular file
File Size	34,816
Physical Size	36,864
Start Cluster	5,693,401
Date Accessed	5/21/2007 6:31:23 PM
Date Created	3/21/2007 12:35:20 AM
Date Modified	3/21/2007 12:35:20 AM
UNIX Security Attributes	
Unix Permissions	-rw-r--r--
UID	501
GID	501
HFS Information	
Catalog Node ID	582,050
File Type	WDBN [5744424e]
File Creator	MSWD [4d535744]
Locked	☐
Name Locked	☐
Invisible	☐

I vari formati

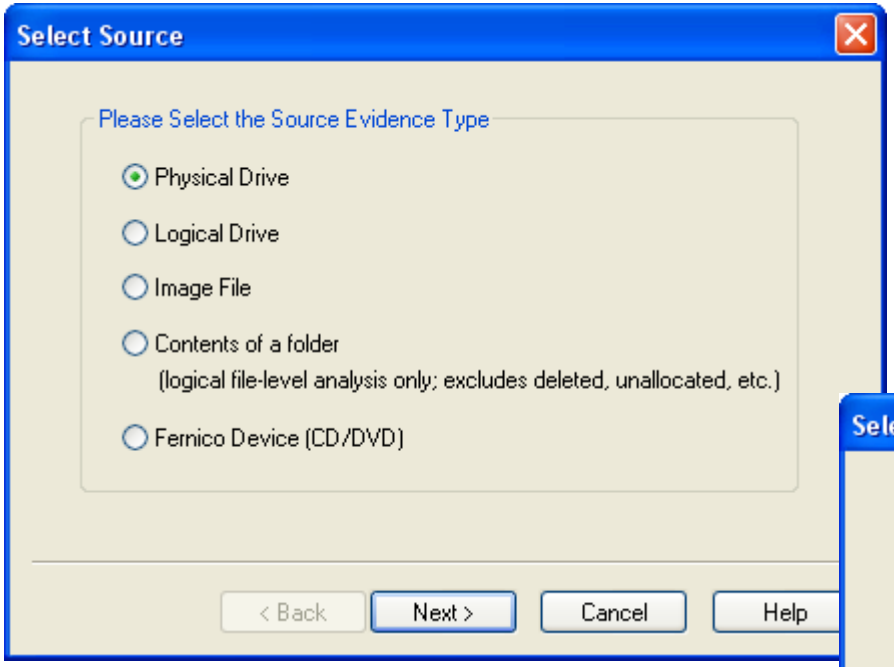
FTK Imager crea questi formati:

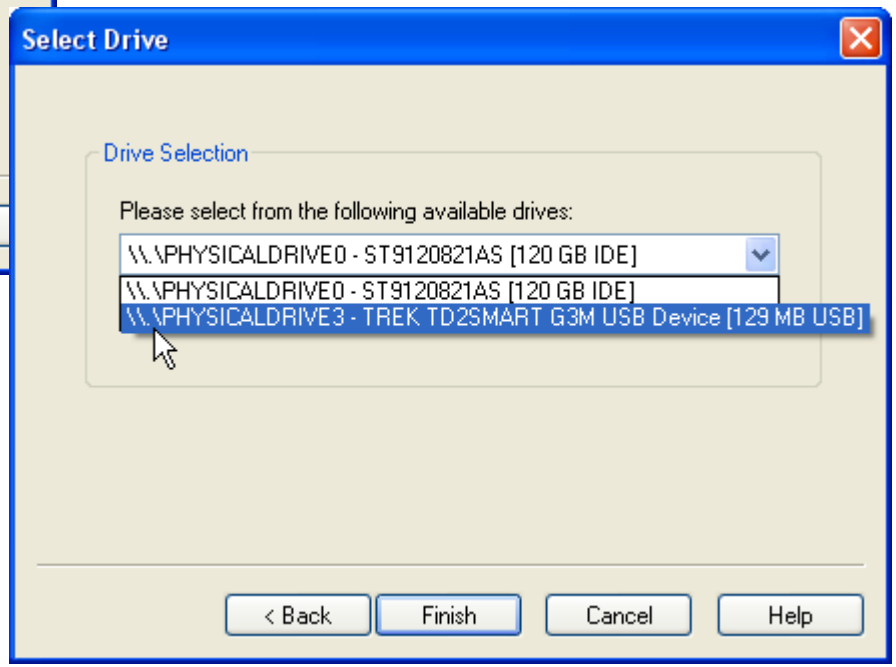
.001/.E01
.ISO/.CUE
.AD1/.S01

Imager legge questi formati:

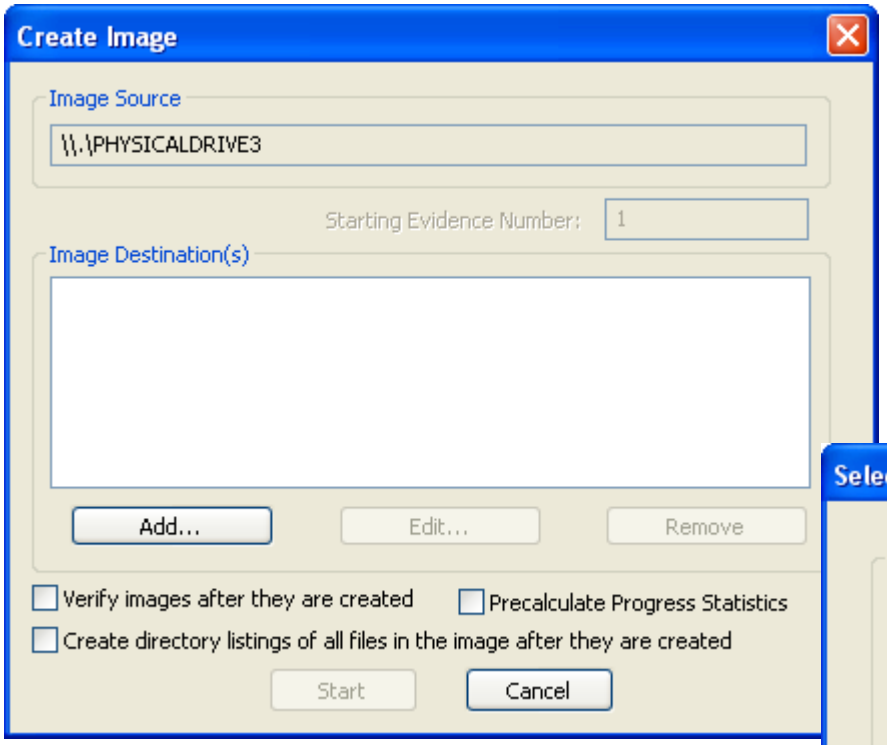
All Files (*.*)
E01 Images (*.e01)
SMART Images (*.s01)
ICS Images (*.I01)
SafeBack / SnapBack Images (*.001)
Tar Archive (*.tar)
Zip Archive (*.zip)
AccessData Logical Image (*.AD1)
VMDK Virtual Drive (*.vmdk)
Ghost Raw Image (*.gho)
Raw CD/DVD image (*.iso; *.img; *.bin; *.tao; *.dao)
Alcohol CD image (*.mds)
DiscJuggler image (*.cdi)
CloneCD image (*.ccd)
Gear CD Image (*.p01)
IsoBuster CD image (*.cue)
Nero CD image (*.nrg)
Philips/OptImage CD image (*.cd)
Pinnacle CD image (*.pdi)
Plextools CD image (*.pxi)
Prassi CD Right Image Plus (*.gcd)
Prassi PrimoDVD Image (*.gi)
Roxio CD Creator Image (*.cif)
Virtual CD image (*.vc4)
WinOnCD image (*.c2d)

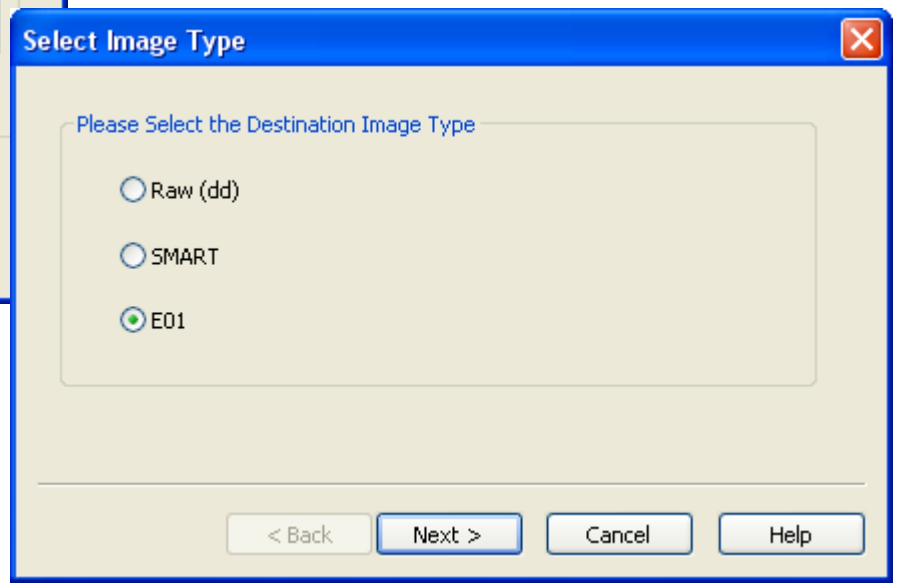
Acquisizione



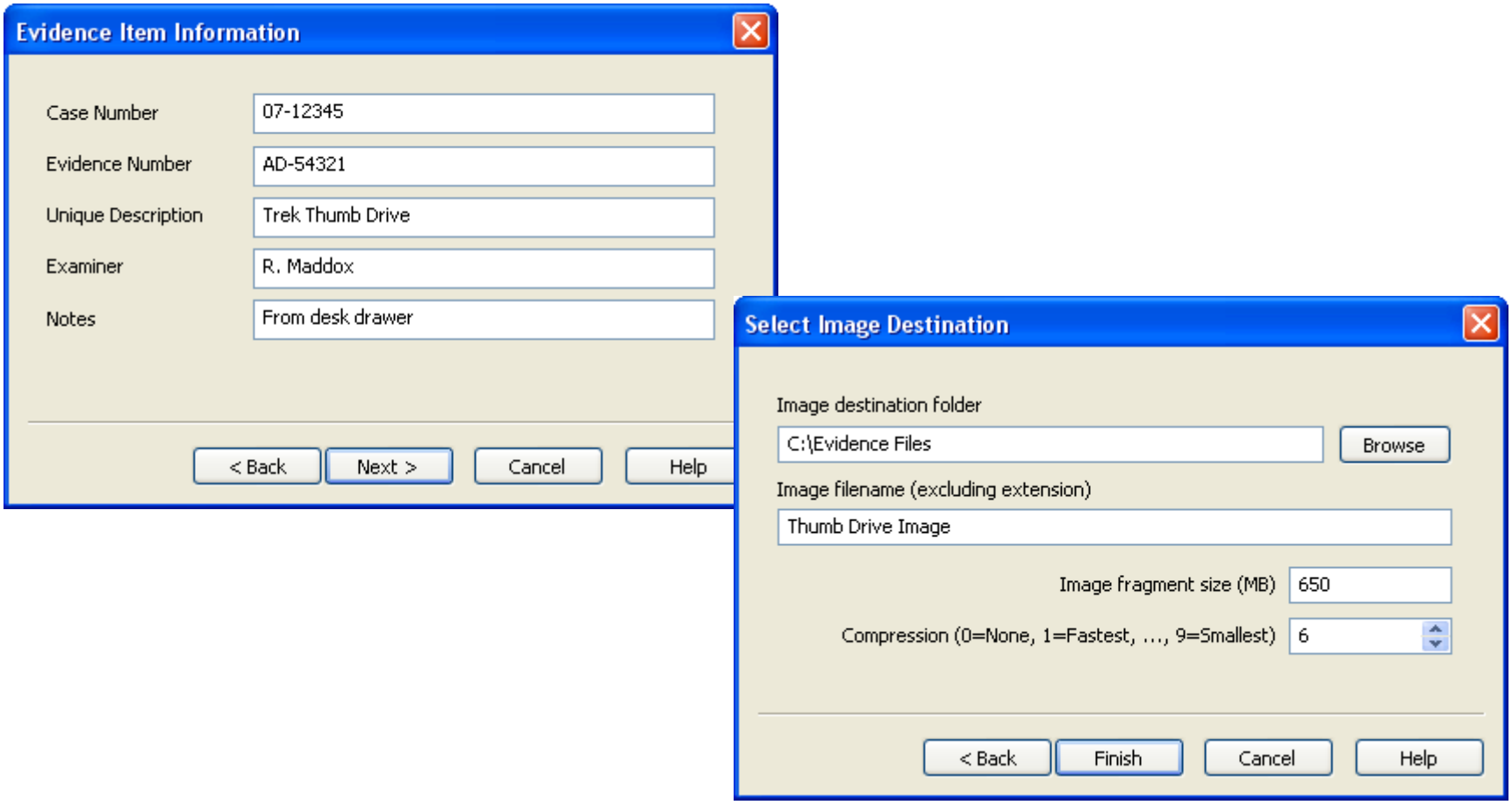


Acquisizione

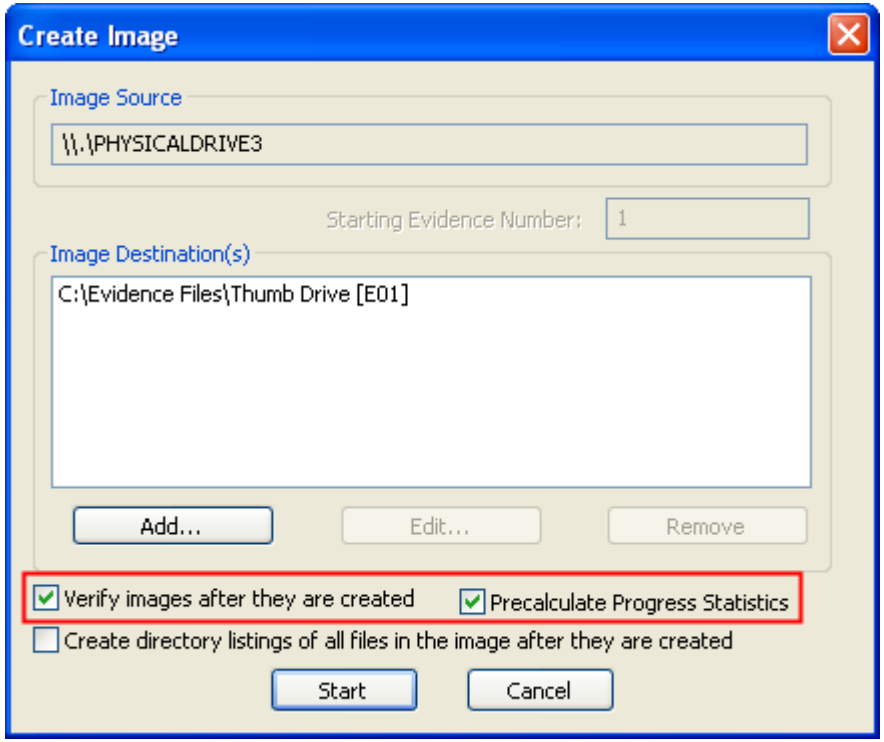


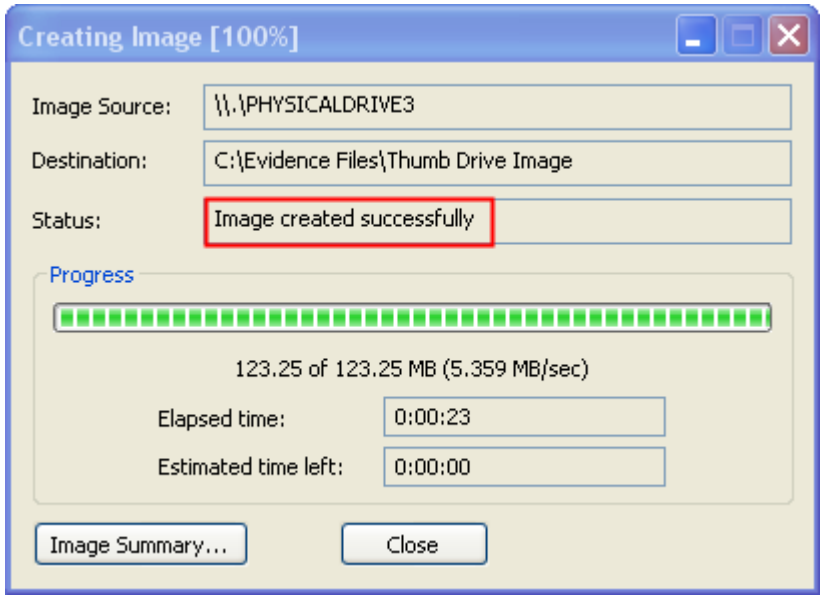


Acquisizione

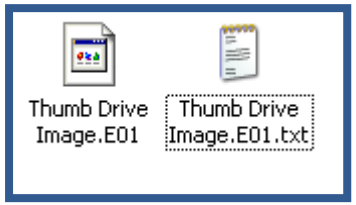


Acquisizione





Acquisizione

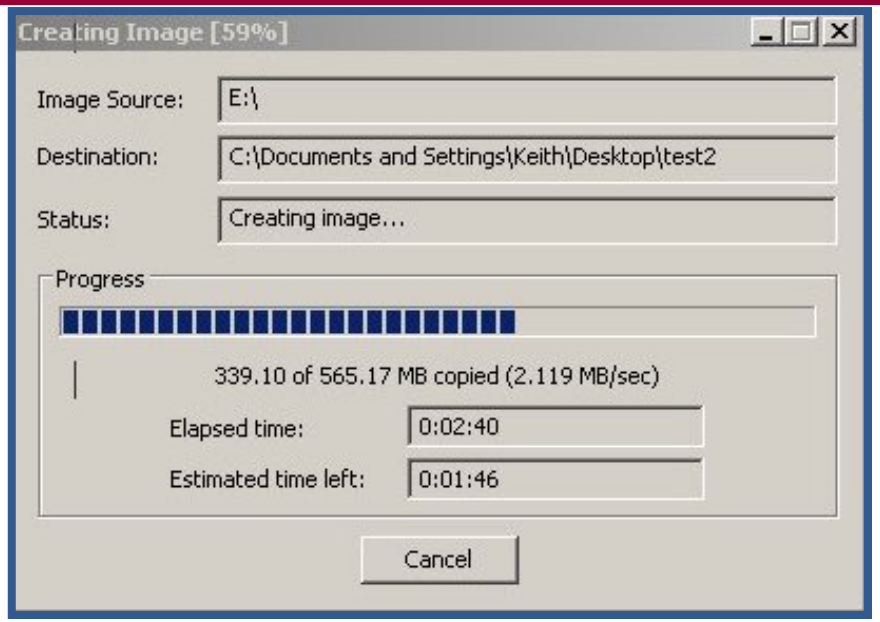


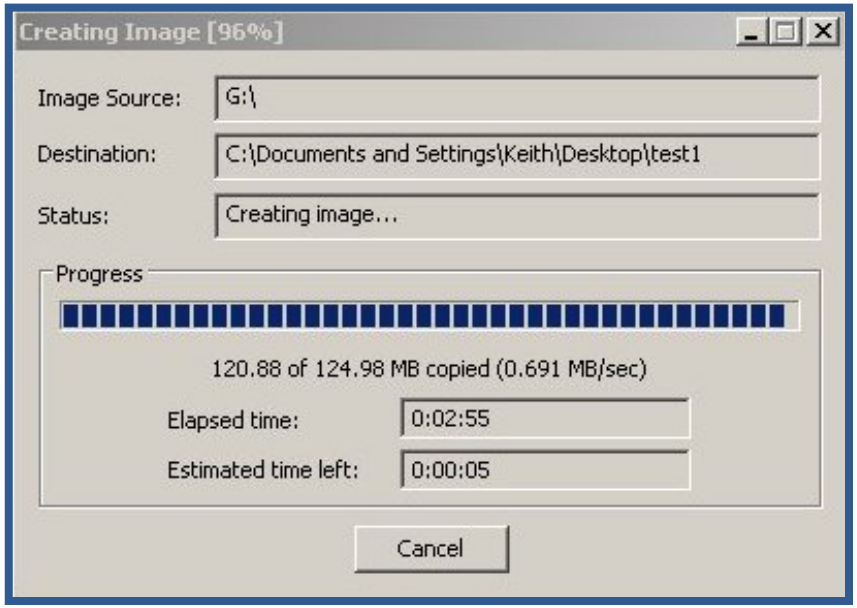
Thumb Drive Image.E01.txt - Notepad

File Edit Format View Help

```
Created By AccessData® FTK® Imager 2.5.3.14 071018

Case Information:
Case Number: 07-12345
Evidence Number: AD-54321
Unique Description: Trek Thumb Drive
Examiner: R. Maddox
Notes: From Desk Drawer

--------------------------------------------------------------

Information for C:\Evidence Files\Thumb Drive Image:

Physical Evidentiary Item (Source) Information:
[Drive Geometry]
 Cylinders: 15
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 252,416
[Physical Drive Information]
 Drive Model: TREK TD2SMART G3M USB Device
 Drive Interface Type: USB
 Source data size: 123 MB
 Sector count:    252416
[Computed Hashes]
 MD5 checksum:    c3f3494f1c9fa5d255e7fd8aa823a708
 SHA1 checksum:   19c11c0f359393c56f9ee26302637799bda796e8

Image Information:
 Acquisition started:   Wed Jan 09 15:31:37 2008
 Acquisition finished:  Wed Jan 09 15:32:01 2008
 Segment list:
  C:\Evidence Files\Thumb Drive Image.E01

Image Verification Results:
 Verification started:  Wed Jan 09 15:32:01 2008
 Verification finished: Wed Jan 09 15:32:03 2008
 MD5 checksum:    c3f3494f1c9fa5d255e7fd8aa823a708 : verified
 SHA1 checksum:   19c11c0f359393c56f9ee26302637799bda796e8 : verified
```

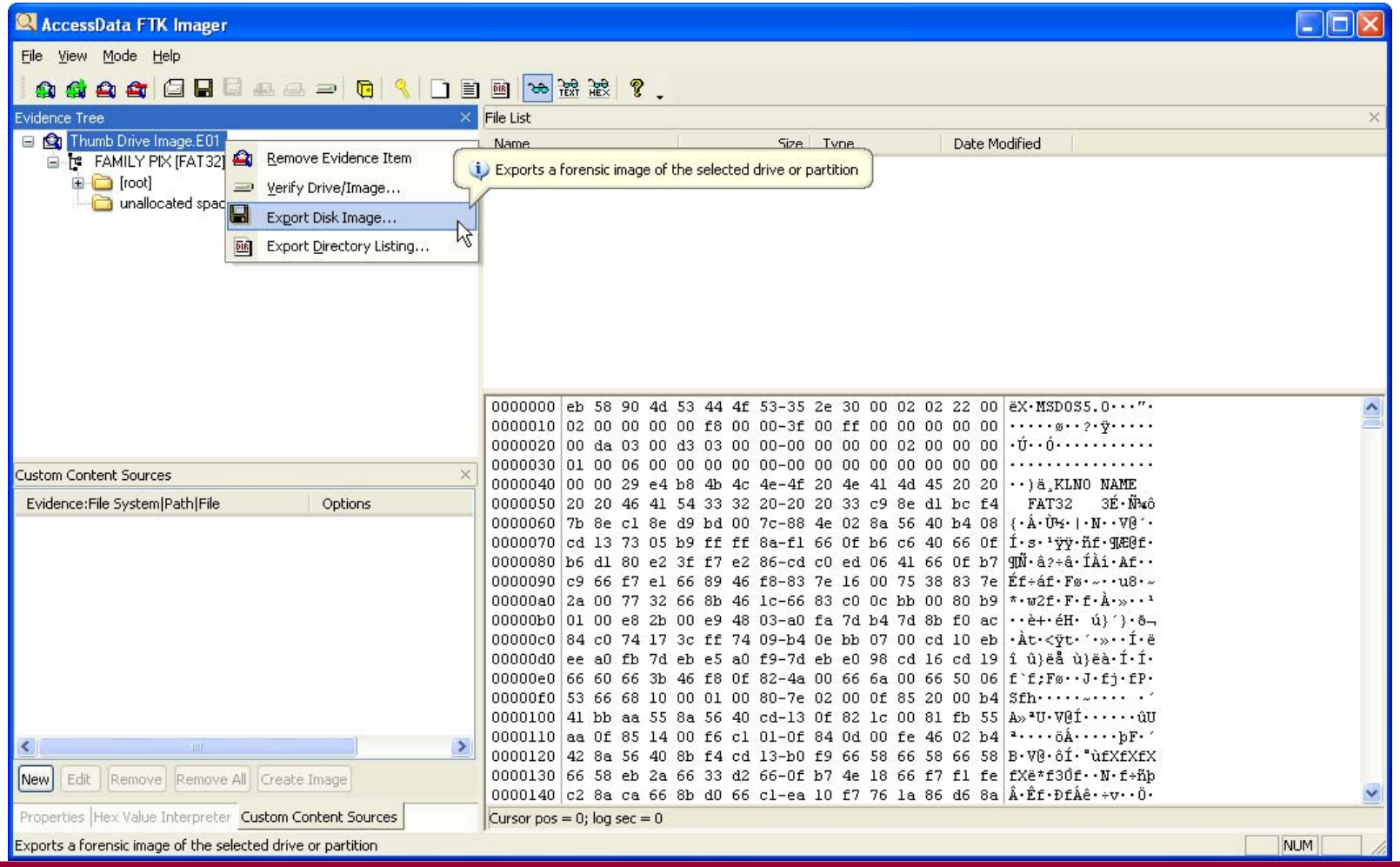
Multi Sorgente – Multi Image





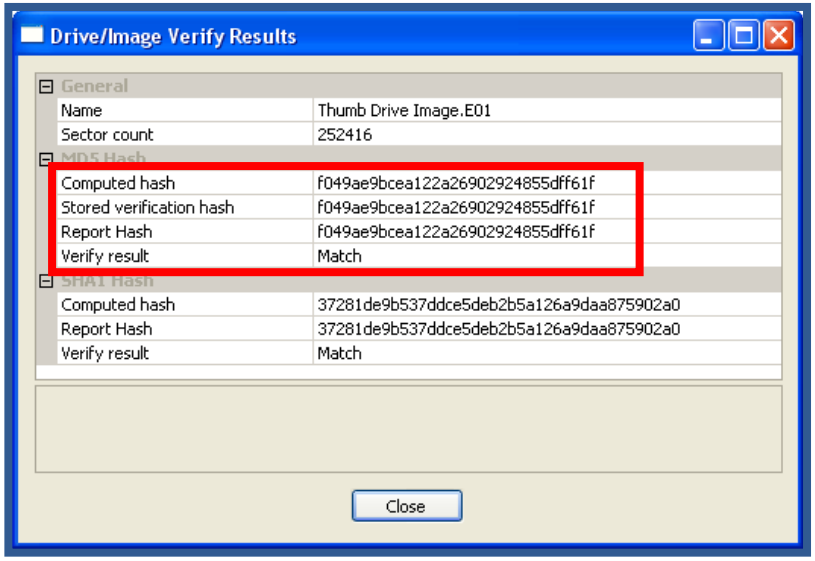
Crea multiple immagini da Multiple sorgenti contemporaneamente !!

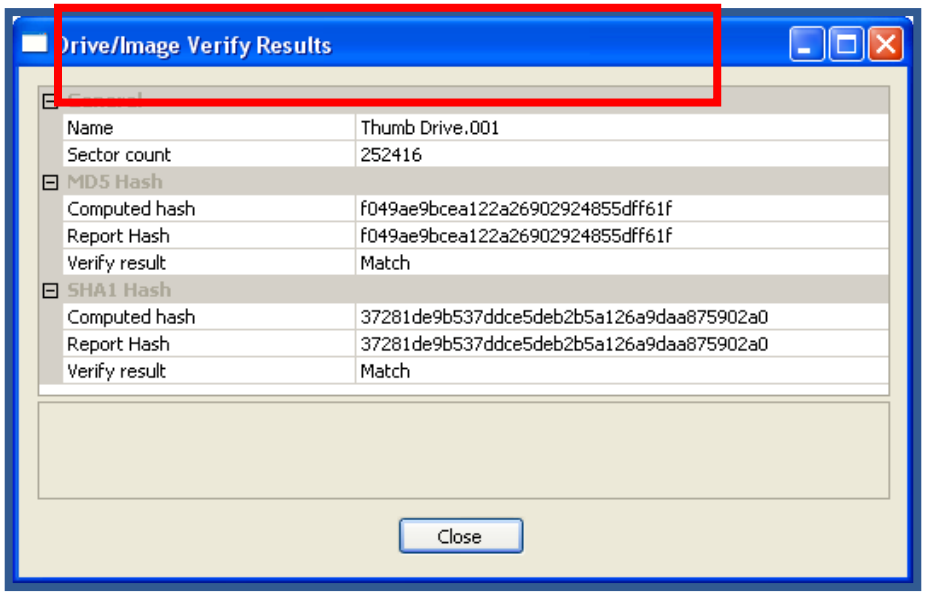
Conversion – Image and Image



Verifica

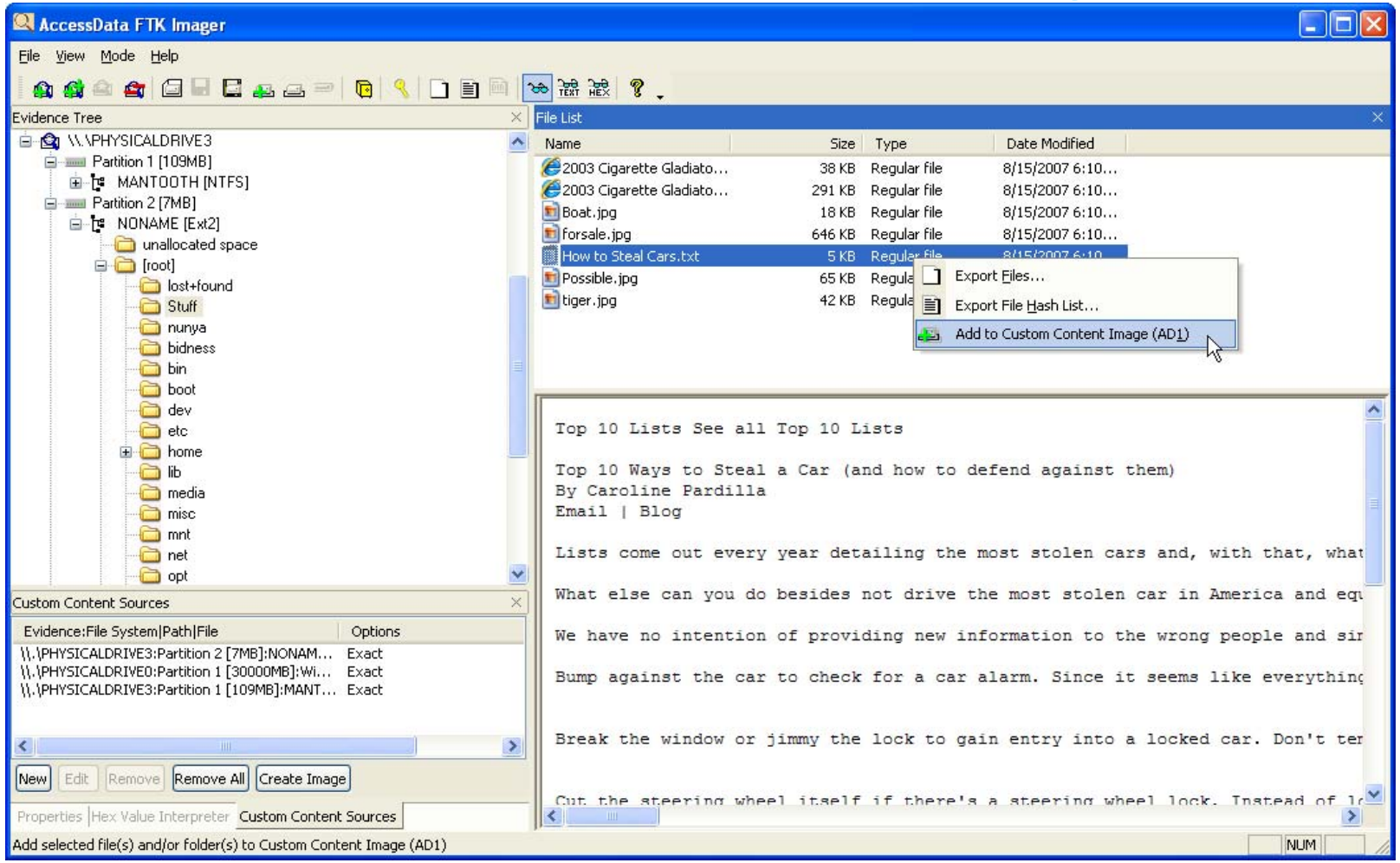
Encase / DD ??



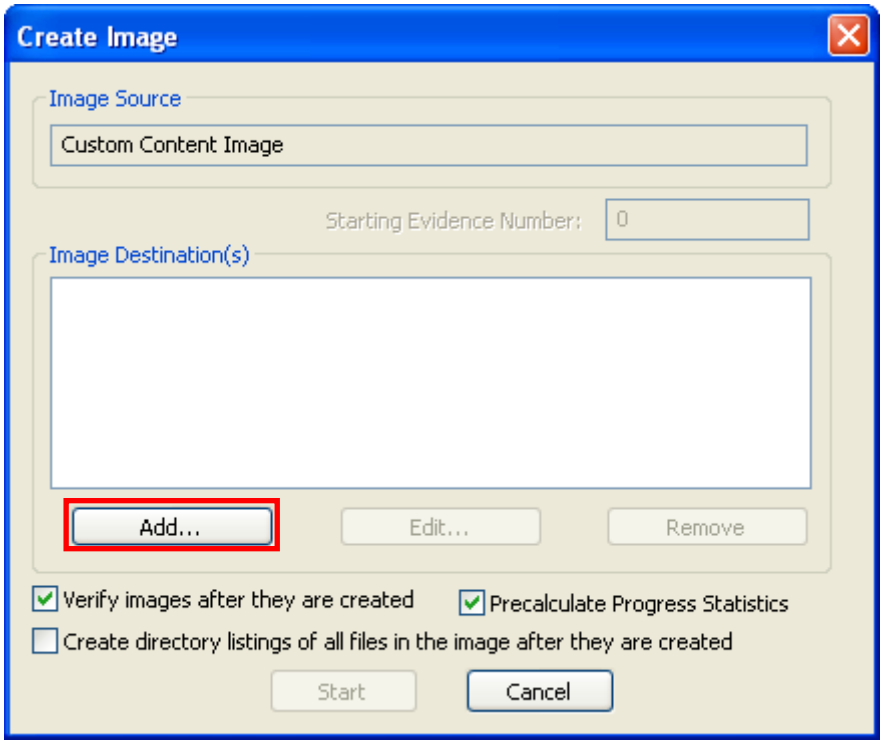


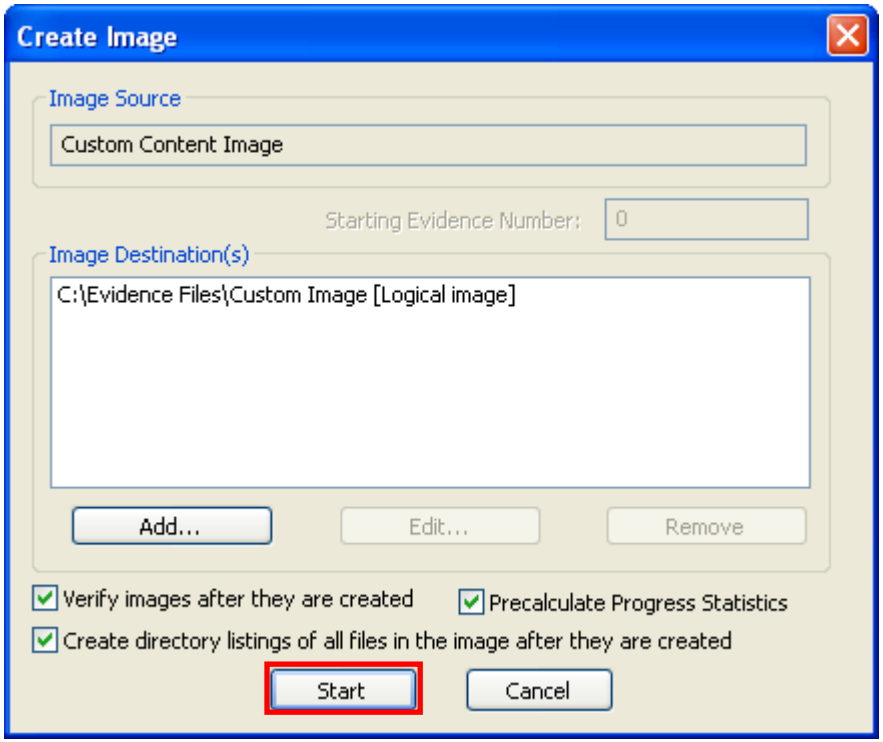
Verified based on image format

Custom Content Images



Custom Content Images





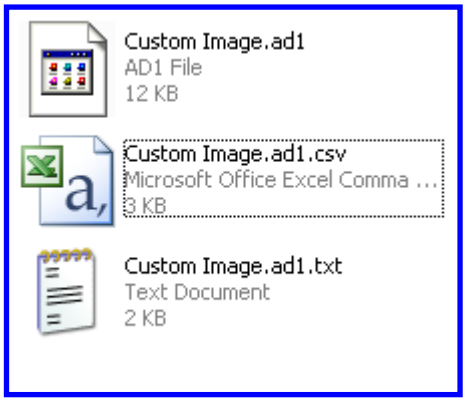
- Puo includere sorgenti multiple
- Puo includere spazio non allocato
- Risultato nel formato .AD1

La formazione della "prova informatica“

Custom Image.ad1.txt - Notepad

File Edit Format View Help

```
Created By AccessData® FTK® Imager 2.5.3.14 071018

Case Information:
Case Number: My Custom Image
Evidence Number: 08-12345
Unique Description: From Bob's Office PC
Examiner: B. Tidwell
Notes:

--------------------------------------------------------------

Information for C:\Evidence Files\Custom Image.ad1:
[Custom Content Sources]
 \\.\PHYSICALDRIVE3:Partition 2 [7MB]:NONAME [Ext2]|[root]|Stuff|How to Steal Cars.txt(Exact)
 \\.\PHYSICALDRIVE0:Partition 1 [30000MB]:WinXP [NTFS]|[root]|kl2log.log(Exact)
 \\.\PHYSICALDRIVE3:Partition 1 [109MB]:MANTOOTH [NTFS]|backup boot sector(Exact)
[Computed Hashes]
 MD5 checksum:    08aff8f22d40965e57d7fd81c0247d98
 SHA1 checksum:   2e843c52a0a0b839d62736045e61d36eada2fab8

Image information:
 Acquisition started:   Wed Jan 09 16:28:19 2008
 Acquisition finished:  Wed Jan 09 16:28:19 2008
 Segment list:
  C:\Evidence Files\Custom Image.ad1

Image Verification Results:
 Verification started:  Wed Jan 09 16:28:19 2008
 Verification finished: Wed Jan 09 16:28:20 2008
 MD5 checksum:    08aff8f22d40965e57d7fd81c0247d98 : verified
 SHA1 checksum:   2e843c52a0a0b839d62736045e61d36eada2fab8 : verified
```

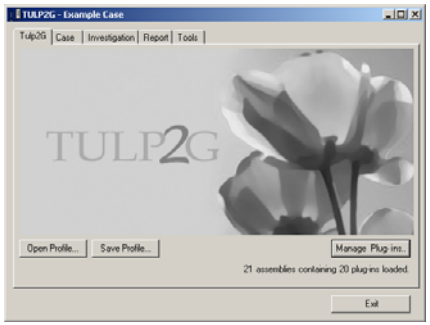


La formazione della "prova informatica“

Microsoft Excel - Custom Image.ad1.csv

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Filename	Full Path	Size	Created	Modified	Accessed	Is Deleted	Stored MD5 Hash	Stored SHA1 Hash				
2	[root]	Custom Con	160	2006-Jul-22 18:28:35.8	2008-Jan-09	2008-Jan-09 2	no						
3	kl2log.log	Custom Con	2	2007-May-23 15:33:08	2007-May-2	2007-Oct-25 2	no	c4103f122d27677c9	1489f923c4dca729178b3e3233458550d8dddf29				
4	backup boo	Custom Con	512				no	2257d8c6e500d9388	fd6c0ae1e855f81d5cd20bd6b5b48f1c3eb7a587				
5	[root]	Custom Con	1024	2007-Aug-15 18:15:10	2007-Aug-15	2007-Aug-15 1	no						
6	Stuff	Custom Con	1024	2007-Aug-15 18:10:46	2007-Aug-15	2007-Aug-15 1	no						
7	How to Stea	Custom Con	4956	2007-Aug-15 18:10:46	2007-Aug-15	2007-Aug-15 1	no	9866e5371005b1e53	6a8c743c61f3997bb0e7503cb68088b5abc04b10				

Mobile Forensics



DIBATTITO

Come garantire la ripetibilità in un apparato che appena acceso è in grado di trasmettere e ricevere dati?

I cellulari più evoluti sono paragonabili ad un computer?

Cosa è la SIM Forensics? E il dump della memoria?

Esistono software Open Source?

RAM Forensics

Nella memoria di un computer acceso si possono trovare dati di fondamentale importanza per una investigazione, che, andrebbero persi per sempre quando il computer verrà spento!

Problematiche:

•I dati in memoria sono organizzati in modo diverso in base al sistema operativo e tipologia di Hardware utilizzato (CPU).

•Un software di acquisizione dei dati in memoria, per funzionare modificherà una parte dei dati in memoria

•Esiste un solo strumento hardware in grado di accedere fisicamente alla memoria sospendendo le attività della CPU per il periodo di acquisizione, funziona tramite bus PCI ma non è mai stato commercializzato

RAM Forensics

Segue Problematiche:

•Esistono 2 tool misti HW e SW che utilizzano uno la porta firewire e l’altro una PenDrive USB

•Il tool su porta firewire sfrutta DMA ma richiede che il sistema sia compatibile con la tecnologia firewire, il software utilizzato è presente su alcune distro live linux e si chiama **Pythonraw1394**, da test effettuati nel lab iisfa questo software funziona bene per limitate porzioni di memoria

•Il secondo tool che fa uso di una Pendrive USB utilizza una distro live minimale di linux e mira a recuperare i dati in memoria appena questa viene disalimentata, garantendone una certa teorica stabilità raffreddando i circuiti elettrici….. ma non è pratico procurarsi idrogeno liquido ed il software **ram2usb** non è stato rilasciato……

RAM Forensics

Soluzioni praticabili:

•Utilizzare tool commerciali che tramite agent eseguono un dump della memoria e lo trasferiscono ad un software di analisi (soluzioni molto costose che incontrano anche problematiche di privacy nel loro uso).

•Provare ad utilizzare la tecnica di **Schatz** che praticava il crash dump, ma anche questa tecnica ha mostrato limiti al di sopra dei 2 Gb

•Usare **Fastdump Pro** oppure **Win32dd**, quest'ultimo nel lab iisfa è stato quello con funzioni più forensics sound (uso di SHA1)

•Ad esempio nell'ultima versione di DEFT EXTRA sono disponibili i tool **mdd, win32dd** e **winen** che possono essere utili al recupero dei dati in memoria sui sistemi Windows.

INDICE DELLA PRESENTAZIONE :

Best practices e consigli utili

Alcune best practices:

- Maneggiare sempre i reperti con guanti elettrostatici
- Fotografare e documentare tutte le fasi di acquisizione
- Eseguire sempre il wipe sicuro dei dischi di destinazione conservandone un log
- Utilizzare sempre il write blocker hardware per proteggere i dischi sorgente
- Calcolare sempre l'impronta hash del disco sorgente e dei file interessanti
- Custodire sempre i dischi in buste elettrostatiche e in contenitori anticaduta

Alcuni consigli:

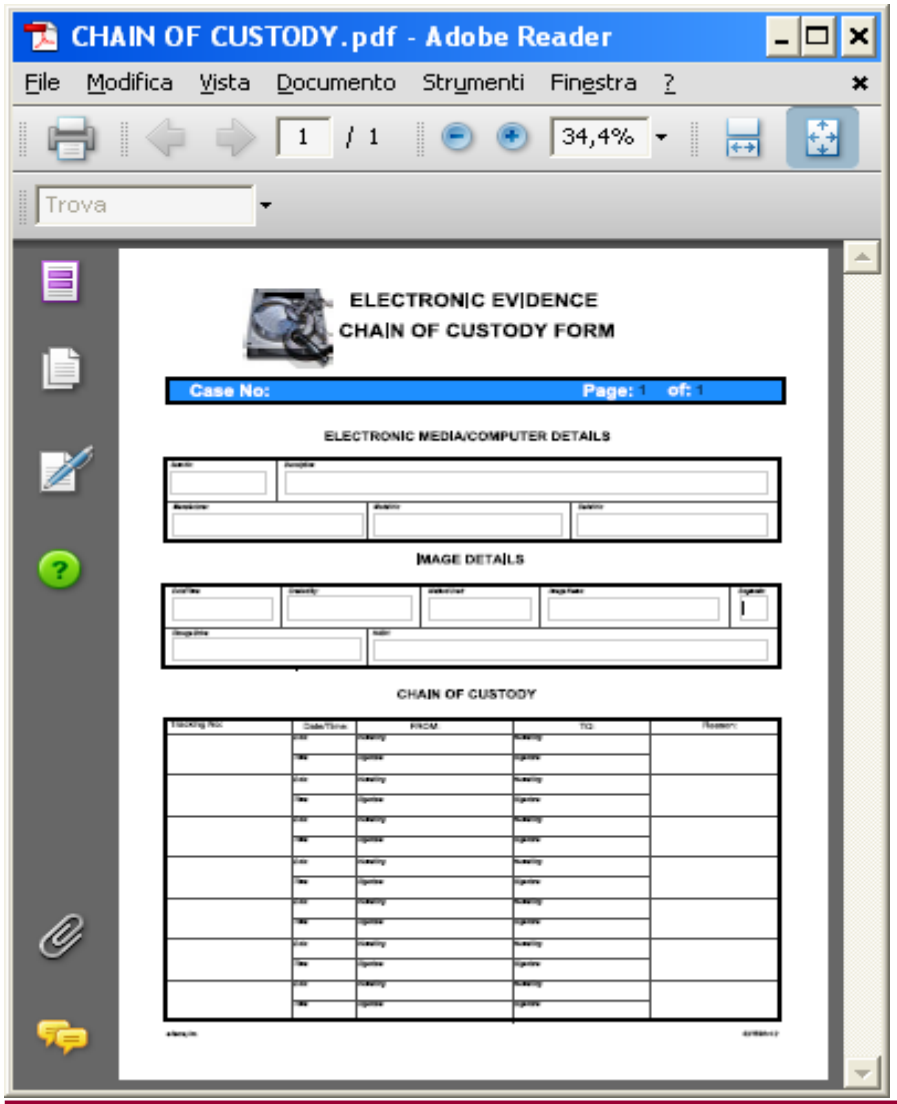
- Effettuare la copia in formato DD in porzioni da 4 Gb (è più pratico)
- Di fronte ad un sistema non conosciuto non improvvisare ma prendere le opportune precauzioni con i giusti tempi (vedi SCSI con controller proprietario o sistemi Legacy)
- Calcolare l'hash con doppio algoritmo es. MD5 + SHA1 oppure usare SHA256

INDICE DELLA PRESENTAZIONE :

La “chain of custody”...

E’ il processo di documentazione del “percorso” delle tracce informatiche dall’individuazione all’aula del tribunale.

La catena di custodia



E' buona prassi utilizzarla anche nei casi di Computer Forensics Aziendale!

Deve riportare i dati identificativi della memoria originale compresa l'impronta di hash (?).

Deve riportare come un LOG tutti gli spostamenti, gli owner e le manipolazioni della memoria originale….

CONSIDERAZIONI

INDICE DELLA PRESENTAZIONE :

Cenni sulla Legge 48

Cenni utili a comprendere la:

Ratifica della Convenzione di Budapest
Nuova legge sul Cybercrime

Legge n. 48 del 2008

Cenni sulla Legge 48

In udienza si ascolta:

- computer come una “provetta” e la Pg con la “siringa”….

- “la prova informatica è per sua natura volatile, come i residui da sparo”...

Testo finale dell'art. 247
Casi e forme delle perquisizioni.

- 1. Quando vi è fondato motivo di ritenere che taluno occulti sulla persona il corpo del reato o cose pertinenti al reato, è disposta perquisizione personale. Quando vi è fondato motivo di ritenere che tali cose si trovino in un determinato luogo ovvero che in esso possa eseguirsi l'arresto dell'imputato o dell'evaso, è disposta perquisizione locale.
- 1-bis. Quando vi e` fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne e` disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.
- 2. La perquisizione è disposta con decreto motivato.
- 3. L'autorità giudiziaria può procedere personalmente ovvero disporre che l'atto sia compiuto da ufficiali di polizia giudiziaria delegati con lo stesso decreto.

SPUNTI DI RIFLESSIONE

- Perquisizione?

Cenni sulla Legge 48

Testo finale - Art. 244 cpp

Casi e forme delle ispezioni.

- 1. L'ispezione delle persone, dei luoghi e delle cose è disposta con decreto motivato quando occorre accertare le tracce e gli altri effetti materiali del reato.
- 2. Se il reato non ha lasciato tracce o effetti materiali, o se questi sono scomparsi o sono stati cancellati o dispersi, alterati o rimossi, l'autorità giudiziaria descrive lo stato attuale e, in quanto possibile, verifica quello preesistente, curando anche di individuare modo, tempo e cause delle eventuali modificazioni. L'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

SPUNTI DI RIFLESSIONE

- Il concetto di alterazione e gli accertamenti irripetibili
- Il rapporto tra ispezione e perquisizione

Ispezione ex art 246 cpp e ss.

Il computer, e non solo quello ovviamente, può assumere la veste di mero contenitore della prova del crimine, ad esempio può immagazzinare il piano di una rapina o le mail intercorse tra i complici. In tal caso non sarà necessaria un'azione di sequestro, ma potrà essere operata in contraddittorio una semplice masterizzazione delle tracce pertinenti al reato, con lo strumento di polizia giudiziaria più appropriato, come ad esempio un'ispezione delegata ex art. 246 cpp.

INDICE DELLA PRESENTAZIONE :

L'alibi… una definizione…

- Il mezzo di prova tendente a dimostrare che l'imputato *"in tali die, in illa hora, non fuisse in tali loco, sed alibi"…*

Una provocazione:

Il computer portatile fino a
che punto può rappresentare
Il contenitore di informazioni
per provare l'alibi?

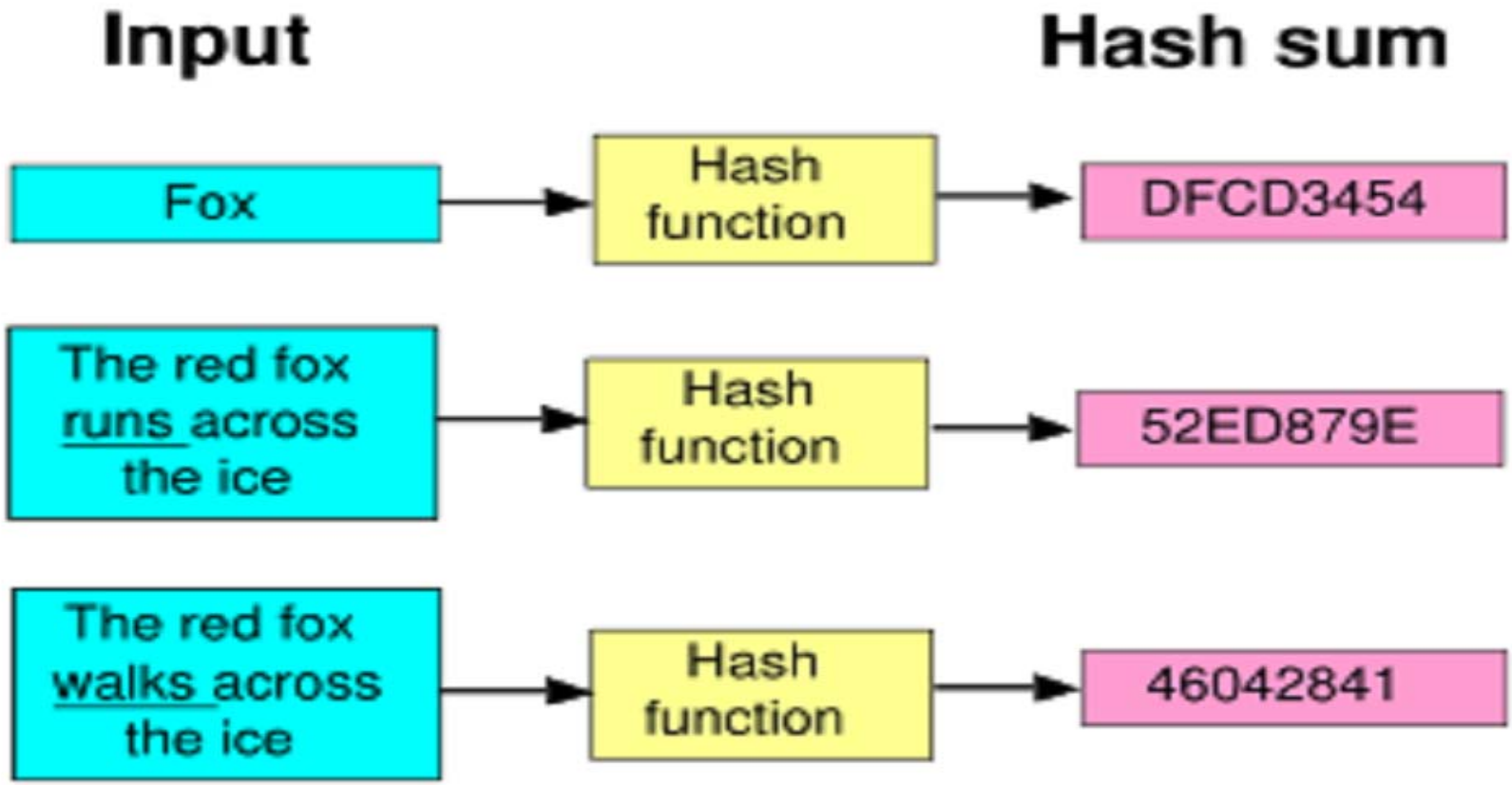
DIBATTITO

INDICE DELLA PRESENTAZIONE :

HASH -> Fonte: Wikipedia

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

Fonte: Wikipedia



FACCIAMO CHIAREZZA SULLA VALIDITA' DELL'HASH IN AMBITO FORENSE

Gli algoritmi di hash possono essere soggetti a 2 tipi di attacco:

- collision attack
- preimage attack

Il primo tipo di attacco si ottiene forgiando file appositamente per creare una collisione e sia MD5 che SHA1 sono risultati deboli a questo tipo di attacco, questo non ha nessun valore nella determinazione dell'univocità di un file generico perché non è praticabile su un caso reale.

Il secondo tipo di attacco è quello che rende possibile alterare un file qualsiasi, modificarlo e salvarlo facendo in modo che abbia lo stesso hash del file precedente, tutti gli algoritmi di hash come MD5, SHA1, ecc. non sono risultati deboli a riguardo, sono quindi entrambi ancora validi, si pensi che l'integrità della firma digitale è ancora garantita da SHA1.

Queste affermazioni sono valide nel momento di realizzazione di questa slide.

QUINDI: Si consiglia sempre il calcolo in doppio hash.

Dati, metadati e l'utilità dell'HASH

Questo test serve a comprendere il legame tra file e metadati giocando con la funzione di HASH, per farlo useremo:

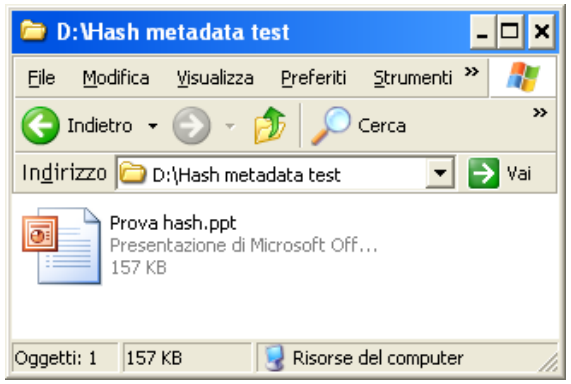
1 File in formato Power Point
1 Software per calcolare l'hash
1 pendrive USB

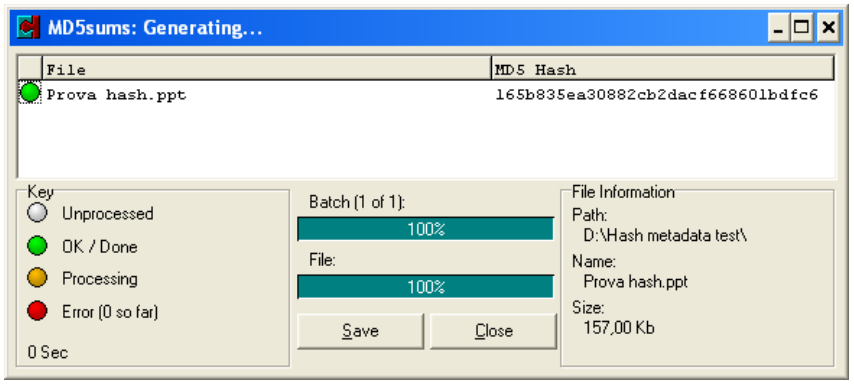
Calcolate l'hash del file e poi rispondete alle seguenti domande:

1)Se apro il file e lo richiudo subito* senza fare nulla l'hash cambia?
2)Se apro il file, cancello una lettera e poi ci riscrivo la stessa lettera e lo salvo, l'hash cambia?
3)Se rinomino il file l'hash cambia?
4)Se cambio l'estensione al file l'hash cambia?
5)Se copio il file dal desktop su una chiavetta USB l'hash cambia?

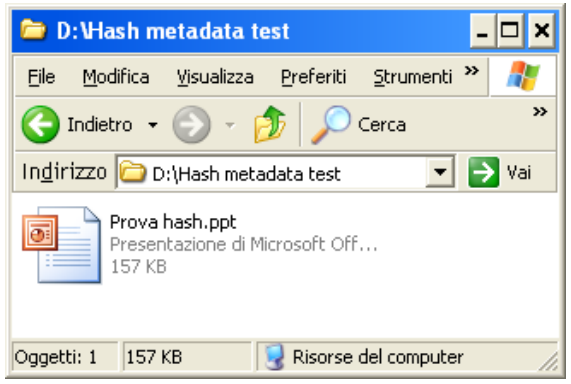
* Attenzione alle funzioni di autosalvataggio che potrebbero alterare il test.

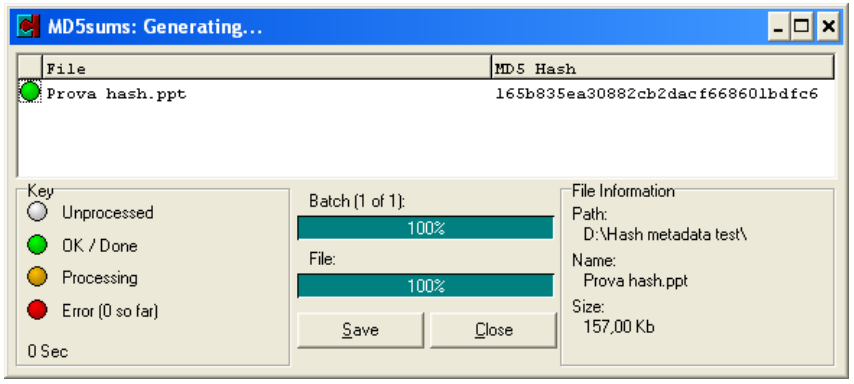
Dati, metadati e l'utilità dell'HASH



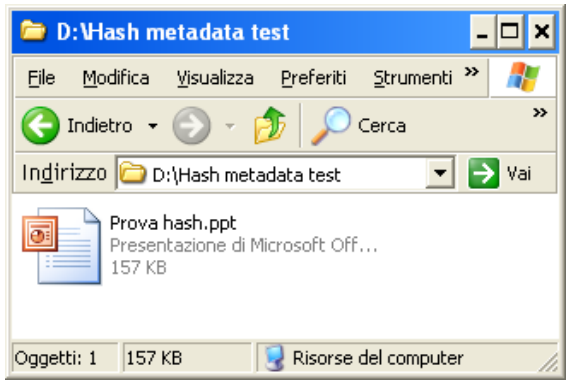


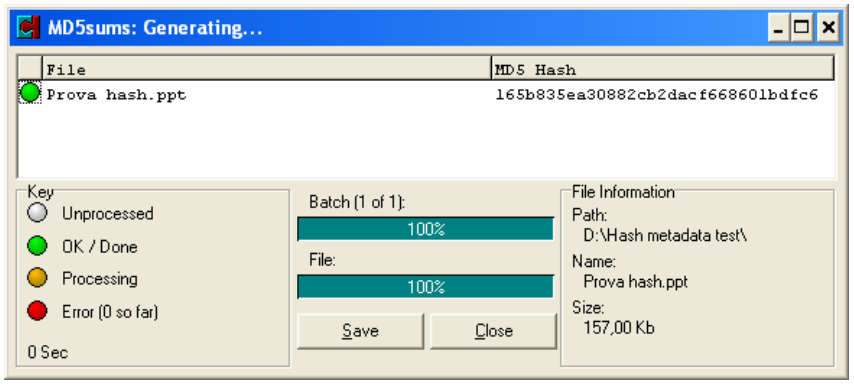
Apro file e richiudo subito.



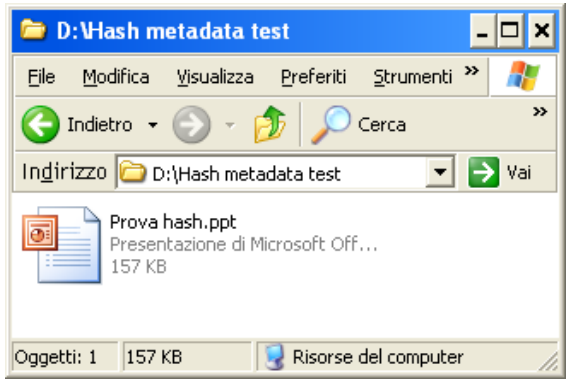


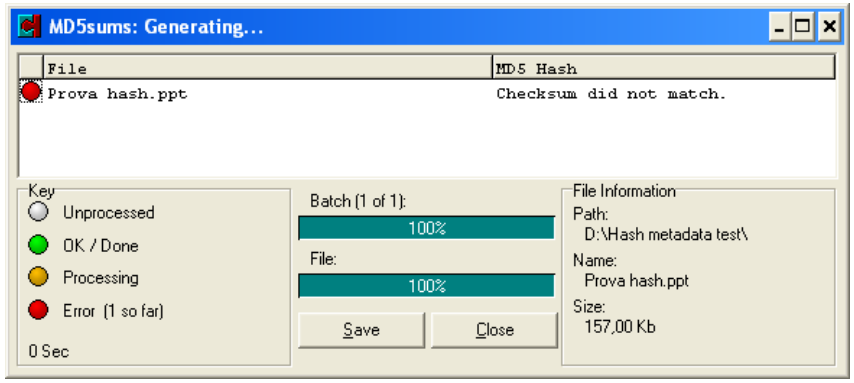
Dati, metadati e l'utilità dell'HASH



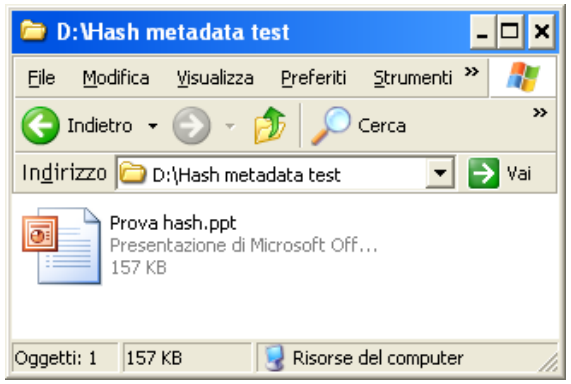


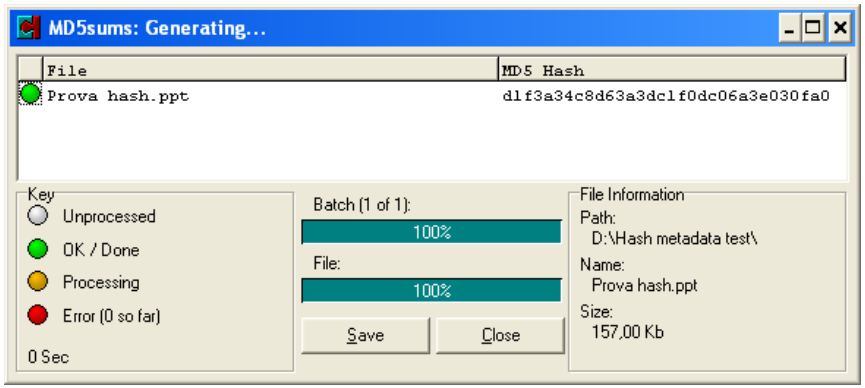
Apro tolgo lettere e rimetto lettera.



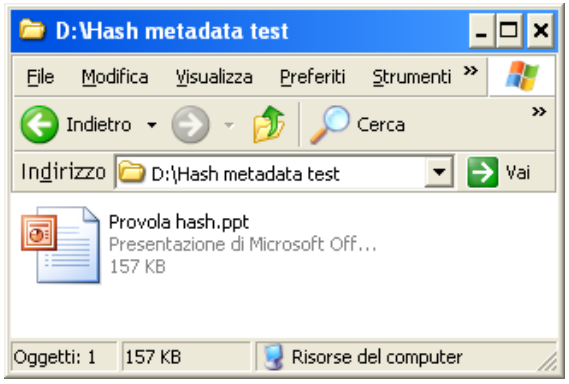


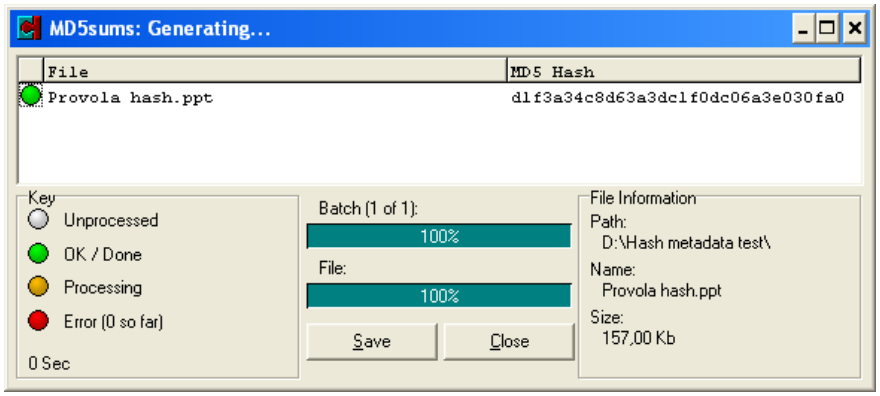
Dati, metadati e l'utilità dell'HASH



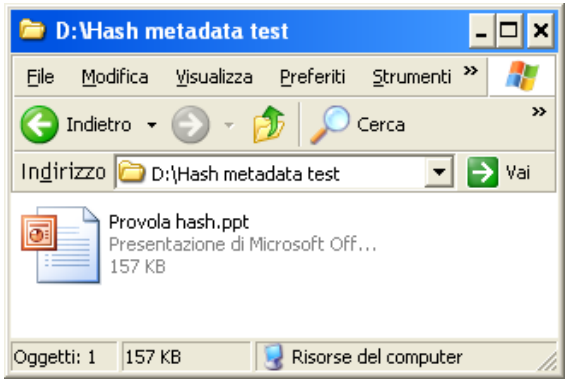


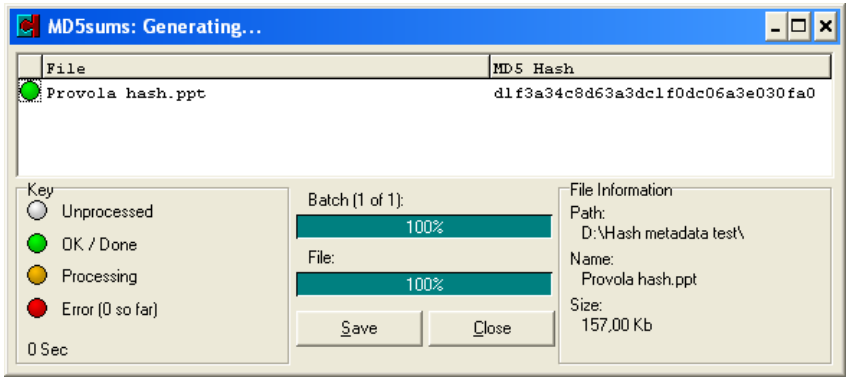
Rinomino file.



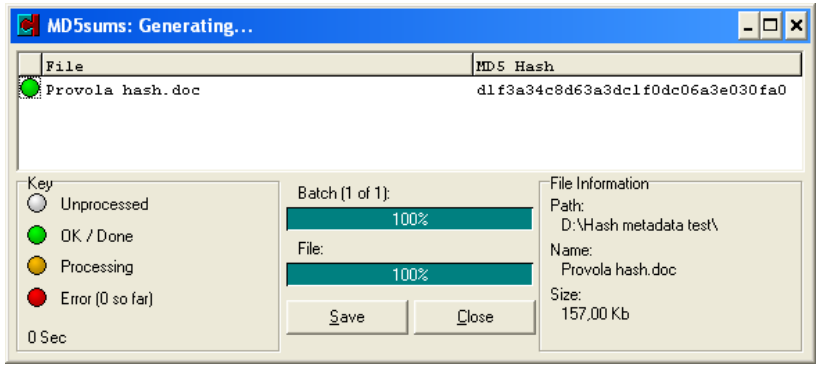


Dati, metadati e l'utilità dell'HASH

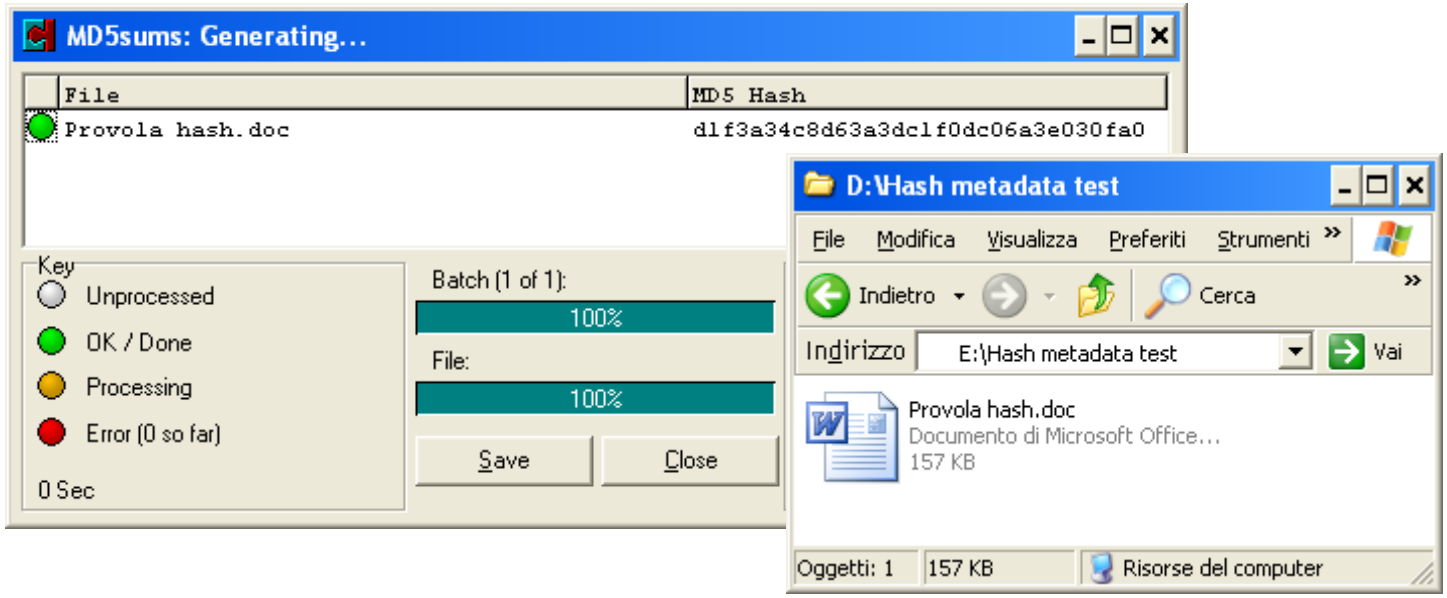




Cambio estensione al file.



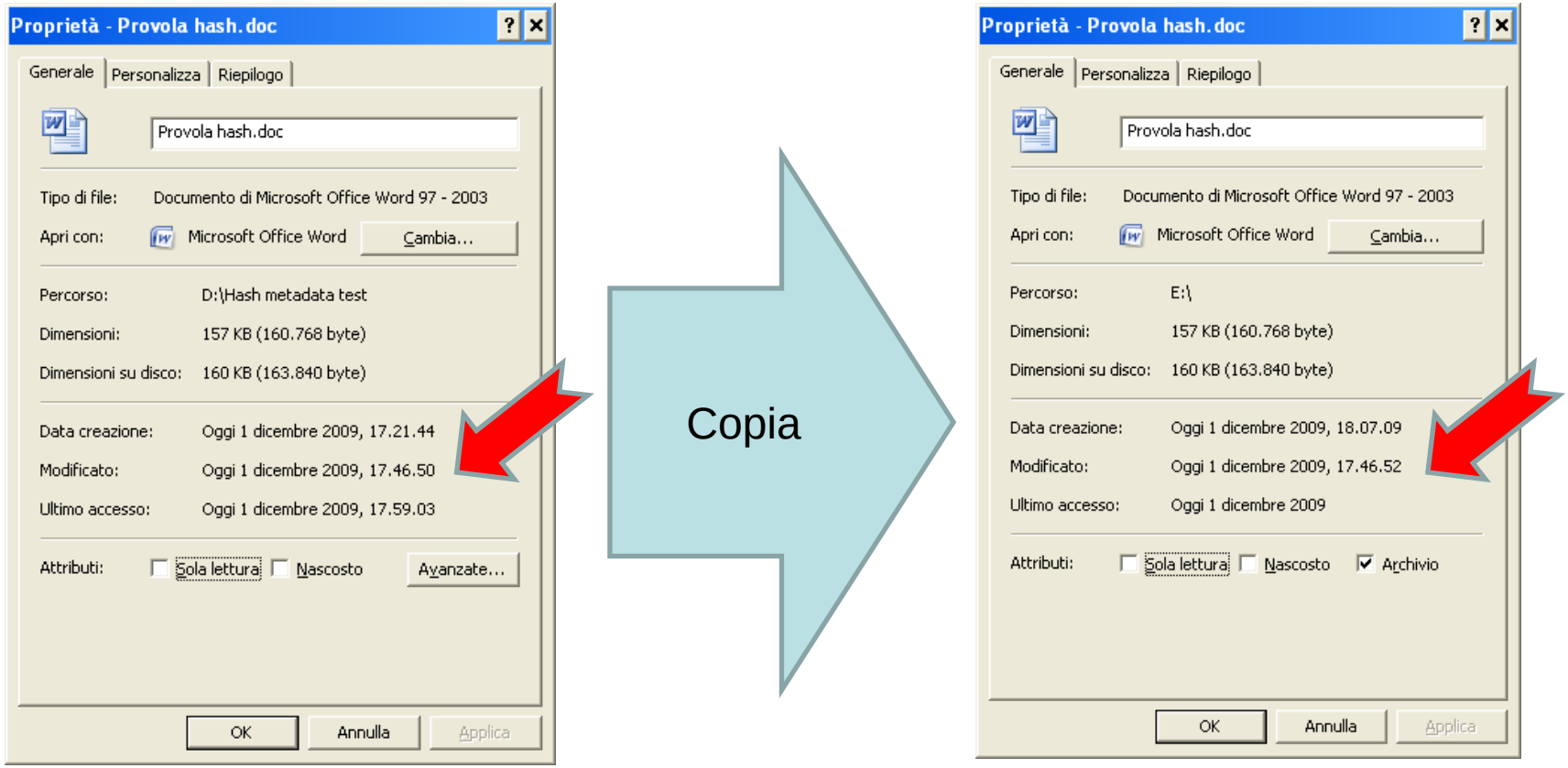
Dati, metadati e l'utilità dell'HASH



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

Dati, metadati e l'utilità dell'HASH

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



Metadati del file originale **Metadati del file copiato**

FATE QUINDI MOLTA ATTENZIONE

ALL'IMPORTANZA

TRA DATI E METADATI

!!

INDICE DELLA PRESENTAZIONE :

2 scuole di pensiero sull'uso di software open o closed, pro e contro

UNA considerazione importante:

Ricordatevi che:

L'uso di un Write Blocker Hardware vi mette al sicuro da errori umani e da eventuali bug che un software in determinate condizioni potrebbe presentare.

Saper usare una distribuzione live forensics è determinante in caso di guasto degli apparati hardware certificati

INDICE DELLA PRESENTAZIONE :

Bibliografia e sitografia :

Link per approfondire:
http://www.iisfa.it/
http://www.marcomattiucci.it/

Software Open Source:
http://www.caine-live.net/
http://www.deftlinux.net/
http://tulp2g.sourceforge.net/

Software Closed Freeware
- http://blog.zoller.lu/2009/03/new-tool-usb-write-blocker.html
- http://redwolfcomputerforensics.com/index.php?option=com_content&task=view&id=42&Itemid=55
- http://www.accessdata.com/downloads.html

INDICE DELLA PRESENTAZIONE :

DIBATTITO

??? DOMANDE

&

RISPOSTE !!!

RINGRAZIAMENTI

Per il contributo alla realizzazione di queste slide RINGRAZIO:

Gerardo Costabile *Presidente IISFA*

Stefano Aterno *Vicepresidente IISFA*

Giuseppe Mazzaraco *Certification IISFA*

Francesco Schifilliti *socio IISFA*

RINGRAZIAMENTI

Grazie per l'attenzione

Per ulteriori informazioni e approfondimenti

scrivetemi all'indirizzo

webmaster@iisfa.it