COMPUTER FORENSICS FAI DA TE

Scritto da Matteo Giardino

L' informatica forense (in inglese, **computer forensics**) è una nuova branca dell' informatica che si occupa dell' analisi di qualsiasi dispositivo elettronico, possa essere utilizzato per memorizzare dati, allo scopo di estrarre informazioni utilizzabili in un processo giuridico. L' informatica forense non è quindi incentrata solo sull' analisi di computer ma su tutto ciò che costituisce una memoria di massa: Hard disk, pendrive USB, supporti ottici e magnetici, ecc…
Si inizia a parlare di informatica forense nel 1984, quando la direzione dell' FBI costituisce una nuova sezione denominata **CART** (**Computer Analysis and Response Team**) che si occupa di aiutare gli agenti FBI procedendo all' analisi dei dispositivi elettronici.
L' informatica forense introduce la figura professionale del **computer forensics expert** (abbreviato per comodità a **computer forenser**) che è l' investigatore digitale che si occupa dello svolgimento delle indagini di informatica forense.
Le tecniche di computer forensics possono essere usate non solamente per verificare se sono stati commessi determinati reati ma anche per identificare problemi che possono essere alla base del malfunzionamento di un sistema informatico, per questo la computer forensics e la sicurezza informatica hanno molti aspetti in comune.
In informatica forense la conservazione dei dati presenti sui supporti di memoriazzazione è importantissima infatti tutte le analisi condotte devono essere eseguite nella cosiddetta **modalità ripetibile;** ovvero tutte le informazioni raccolte devono poter essere verificabili da chiunque e in qualsiasi momento. Proprio per questo motivo generalmente si preferisce lavorare su delle copie speculari di supporti di memoria (dette **immagini**) piuttosto che sui supporti fisici stessi.
Queste indagini, che hanno come obiettivo la raccolta di informazioni utilizzabili in tribunale richiedono particolare attenzione e cautela da parte del forenser poiché la mancata applicazione delle procedure idonee potrebbe portare le autorità giudiziare ad attribuire un reato ad un soggetto piuttosto che a un altro.
La **IACIS** (**International Association of Computer Investigative Specialist**) ha emanato un **codice di etica professionale** nel quale sono riportare una serie di regole di base che il forenser è tenuto a seguire per poter svolgere in maniera

corretta un' indagine di informatica forense. Questo codice di etica (ovviamente in inglese) è pubblicato sul sito ufficiale ACIS.

– STRUMENTI UTILI AL FORENSER

Il forenser per svolgere al meglio e in totale sicurezza le sue indagini ha bisogno di una serie di strumenti che possono essere sia **hardware** (come i write locker) sia **software** (ad esempio i software di recupero dati). I software disponibili per le analisi forensi sono sia a pagamento (come **Forensics Toolkit**) sia open-source (come **Caine** e **WinTaylor**).
Generalmente al forenser servono moltissimi software che svolgono ognuno la propria funzione, per ovviare a questo è stato progettato **Caine**, una distro di linux che contiene moltissime utility usate in campo forense.

– CAINE: COMPUTER AIDED INVESTIGATION ENVIRONMENT

Caine è interamente sviluppato in Italia ed è attualmente gestito dall' esperto di computer forensics **Giovanni Bassetti**. Il sito ufficiale del progetto Caine è *http://www.caine-live.net*. Da questo sito è possibile effettuare il download di Caine e di WinTaylor un' utility per Windows, sviluppata in **Visual Basic 6**, che svolge funzioni molto simili alle utility incluse in Caine.
Le utility più importanti incluse in Caine sono:

- **AIR** (Automated Image Restore): utiliy avanzata per la creazione di immagini di supporti di memoria.
- **Autopsy**: software per eseguire analisi su file e eventualmente recuperare quelli cancellati.
- **Exif**: un software che permette di estrarre i metadati EXIF dalle fotografie digitali.
- **Guymager**: creazione di immagini dei supporti di memoria; meno complesso rispetto ad AIR.
- **DvdDisaster**: recupero di dati da supporti ottici danneggiati.
- **Wipe**: software per cancellare file in modo che non siano più recuperabili.
- **Fundl**: software per il recupero rapido dei dati cancellati.
- **Ophcrack**: cracking delle password di Windows utilizzando le rainbow tables.
- **Stegbreak**: estrazione dei dati nascosti in file JPG mediante steganografia.
- **GtkHash**: calcolo dell' hash di un file mediante diversi algoritmi.
- **Pasco**: analisi avanzata della cache di Internet Explorer.
- **Photorec**: software per il recupero dei files cancellati mediante tecniche di data carving.

Caine può essere installato su qualsiasi computer, ma l' installazione può facilmente essere evitata utilizzando le modalità **liveCD** e **liveUSB** che permettono di avviare il sistema rispettivamente da CD (o DVD) o da chiavetta USB. Per l' avvio liveCD è necessario inserire un supporto ottico che contenga i file di Caine e selezionare come dispositivo di avvio dal Bios del proprio PC, il lettore CD/DVD.

– *ANALISI FORENSE SU UN DRIVE USB*

L' immagine di un disco viene utilizzata dal forenser per evitare di eliminare o alterare file e informazioni contenuti sul dispositivo di memoria da analizzare. Per eseguire le analisi si possono usare i singoli software integrati oppure utilizzare l' interfaccia centrale di Caine che permette di accedere più velocemente alle varie utility.

E' preferibile utilizzare l' interfaccia centrale poiché questa integra anche un sistema di reporting, che alla fine delle indagini permettera di stampare un report contenente tutte le informazioni riguardanti le operazioni eseguite mediante l' interfaccia stessa, o mediante le utility incluse in Caine.

Per avviare la registrazione delle operazioni e quindi per poter stampare un report alla fine dell indagini bisogna aprire un nuovo caso utilizzando l' interfaccia di Caine.
Verra richiesto di inserire il nome dell' indagine e quello dell' investigatore. Terminata questa procedura si potrà iniziare a investigare sul dispositivo "sequestrato". Si segnala che solamente le operazioni compiute mediante l' interfaccia centrale vengono registrate dal sistema di reporting.

STEP 1: ***CREAZIONE DI UN NUOVO CASO***

Sul desktop, fare click su **Caine Interface** per avviare l' interfacca dentrale di Caine.

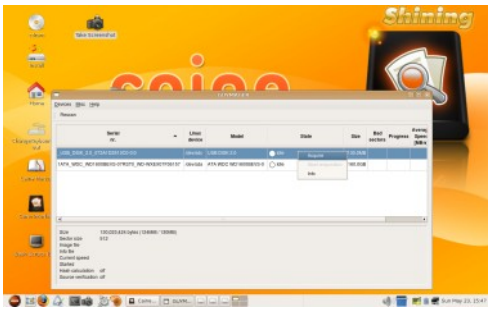
Per avviare la registrazione delle operazioni effettuate cliccare su **Create Report**.

Sarà necessario inserire il nome dell' indagine e quello dell' investigatore. Una volta terminato l' inserimento fare click su **OK**

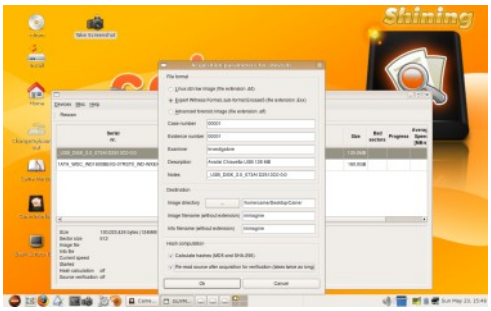
Terminata la creazione del nuovo caso, è possibile creare un' immagine del supporto USB. Per fare questo useremo Guymager. Caine integra anche un altro strumento per la creazione di immagini, AIR, che svolge la medesima funzione di Guymager ma è più avanzato è più complicato da utilizzare. Le immagini di Guymager possono essere salvati in tre formati. Il primo formato (.exx – Expert Witness Format) è quello di default ed è un formato compresso progettato per le indagini forensi. Expert Witness supporta anche lo split dell' immagine in immagini più piccole. Durante questa "indagine" useremo il formato Expert Witness Format.

STEP 2: ***ACQUISIZIONE DELL' IMMAGINE***

Selezionare la scheda **Collection** e selezionare **Guymager** per avviare il programma di acquisizione immagini.



Fare click con il tasto destro sul dispositivo da acquisire e fare click su **Acquire** nel menu a tendina che appare.

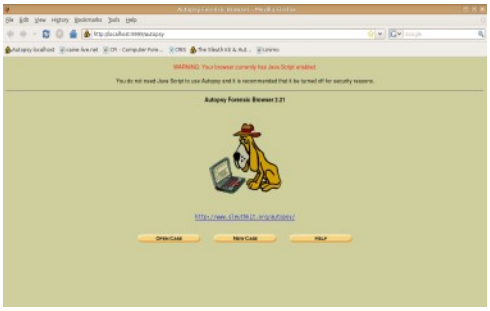


Inserire i vari dati, lasciare il formato immagine predefinito (.exx) e cliccare su **OK**. Attendere poi che l' acquisizione venga completata.

Il prossimo passo riguarda il recupero dei dati cancellati con **Autopsy**. Questo è possibile perchè eliminare un file utilizzando il cestino di Windows non vuol dire farlo sparire definitivamente dall' hard disk. Ovviamente i file diventano invsibili e per recuperarli bisogna ricorrere a programmi specifici come Autopsy.

Putroppo non in tutte le situazioni è possibile recuperare l' intero files: talvolta è possibile che il recupero non sia possibile. Questo caso si verifica solitamente quando il file è stato sovrascritto da un' altro files o sono stati usati dei software appositi detti **software di wiping** per cancellare totalmente il file. Questi software si basano in generale su cicli casuali di sovrascrittura mirati a sovrascrivere i settori dove si trova il file da cancellare. I software di wiping più avanzati utilizzano particolari algoritmi come il **DOD (Department Of Defense)** o il m**etodo Guttman** (che prevede 35 passaggi di sovrascrittura).

STEP 3: ***RECUPERO DEI FILES CANCELLATI***

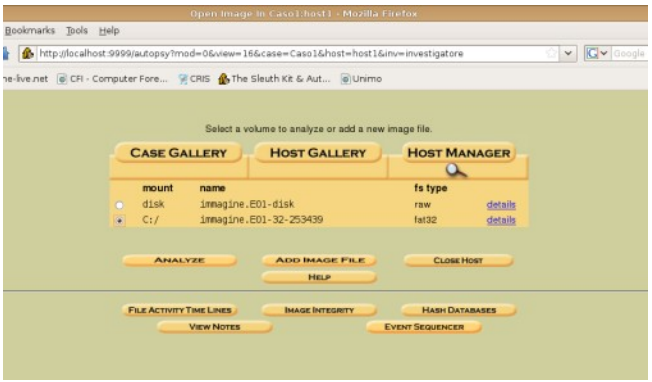


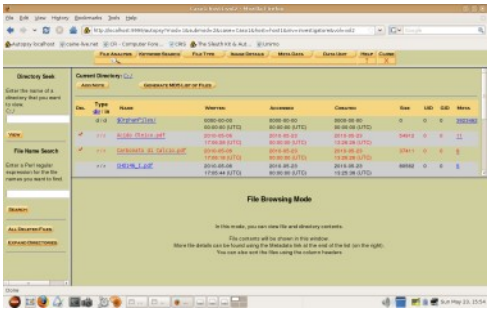
Nell' interfaccia principale di Caine, nella scheda **Analysis** cliccare su **Autopsy**
Nella finestra principale di Autopsy cliccare su **New Case** per aprire una nuovo caso.

Nella finestra che appare inserire i dati del caso e cliccare su **New Case**. Poi su **Add Host** e su **Add Image**.
Nella finestra che appare selezionare **Add Image File.**

Inserire la posizione dell' immagine (**Location**), selezionare le opzioni **Disk** e **Symlink**. Poi clicare su **Next** e su **Add.**

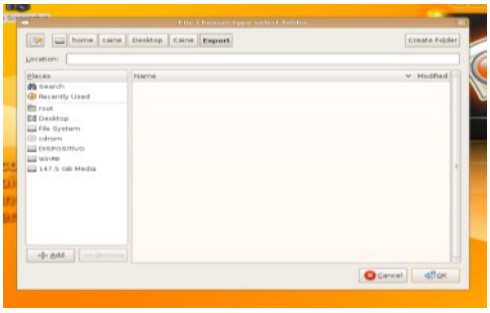
Per iniziare l' analisi selezionare il dispositivo che ha un file system qualsiasi (Fat, Fat32, NTFS, ExFat, ecc..) ma comunque diverso da **RAW**. Cliccare poi su **Analyze** per avviare l' analisi. Nella finestra che appare fare click su **File Analysis** nella barra in alto per visualizzare i file presenti nel supporto.





Nella finestra che appare vengono visualizzati tutti i file (sia cancellati che non). Quelli cancellati sono evidenziati in rosso. Cliccare sulla riga del file da recuperare.

Adesso è possibile vedere una semplice anteprima del file (che in questo caso è un PDF).
Nella barra che appare cliccare su **Export** per recuperare e salvare il file che è stato selezionato.



Cliccare su **Save file** e selezionare il percorso in cui salvare il file. Cliccare poi su **OK**

STEP 4: ***RECUPERO DI TUTTI I FILES CON FOREMOST***

Avviare **Foremost**, facendo click sull' apposito pulsante nella scheda **Analysis** dell' interfaccia centrale.

Cliccare su **Open input File** e selezionare l' immagine da cui recuperare i file. Cliccare **su Select Directory** e selezionare la cartella dove salvare i file estratti. Cliccare poi su **Run Foremost**.

Attendere che Foremost estragga i files. Cliccare su **Quit** nel messagio che indica la fine del processo e cliccare su **Open Output Directory** per visualizzare i file estratti.

CANCELLARE UN FILE DEFINITIVAMENTE

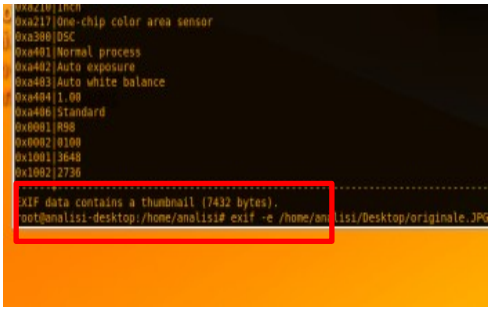
Per impedire il recupero di un file con programmi tipo Autopsy è possibile utilizzare **Wiper**, un software di **wiping** (cancellazione sicura dei dati) che si utilizza mediante il terminale di Caine. Una volta avviato il terminale, utilizzando in pulsante **Run terminal** presente nella scheda **Collection** dell' interfaccia centralizzata, digitare **wipe –f nomefile** e premere **INVIO**. Ovviamente **nomefile** va sostituito con il percorso completo del file da cancellare. Verrà poi mostrato un messaggio di conferma che attesterà l' avvenuta cancellazione del file.

– *ESTRAZIONE DEI DATI EXIF DA UNA FOTO*

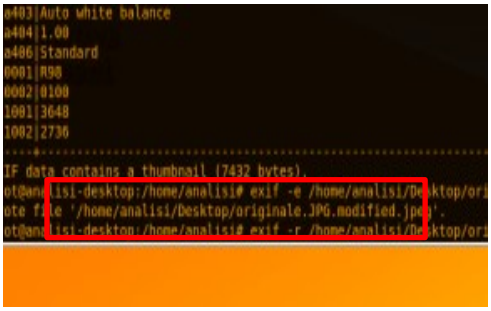
Exif (**Exchangeable image file format**) è una specifica per il formato dei file immagine utilizzato dalla fotocamere digitali. L' Exif supporta alcuni formati tra cui il **JPG** ai quali aggiunge delle etichette (dette **metadati**) che contengono le informazioni relative alla marca, al modello della fotocamera, alla data, all' ora in cui è stata scattata e alle impostazioni della fotocamera al momento dello scatto (sensibilità ISO, bilanciamento del bianco, lunghezza focale, zoom, flash, ecc...).
I dati Exif includono anche una piccola anteprima (detta **thumbnail**) della foto in modo da rendere più veloce il caricamento per l' anteprima sui display a bassa risoluzione (come quelli delle fotocamere digitali).

Le informazioni Exif vengono scritte dal software della fotocamera e durante le operazioni di fotoritocco non sempre vengono aggiornate. In alcuni casi la modifica di una foto non comporta l' aggiornamento dell' anteprima Exif, e così il recupero di quest' ultima permette di ottenere un copia (seppur a bassa risoluzione) della foto originaria. L' unico problema dei metadati Exif è che possono essere facilmente eliminati o modificati e non esiste il modo di capire quando questi siano stati alterati con un apposito software. I metadati Exif non costituiscono quindi una vera e propria prova perchè chiunque e con poco sforzo può riuscire a modificarli o cancellarli.

Avviare il terminale di Caine facendo click sul pulsante **Run Terminal** nella scheda **Collection** dell' interfaccia centrale.

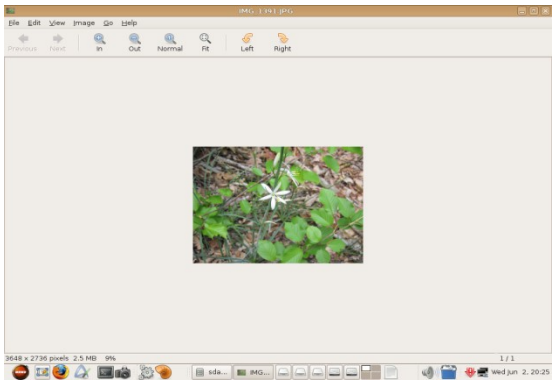


Digitare **sudo su** e premere invio per otteneri privilegi di amministratore (utente root). Digitare poi **exif –i nomefile** e premere **INVIO**, dove **nomefile** va rimpiazzato con il percorso del file da analizzare.



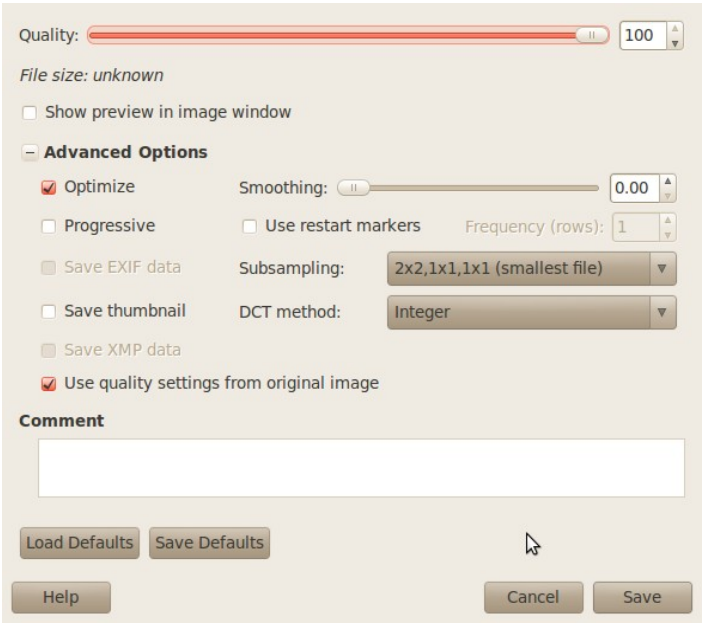
Alla fine del report è indicato se è presente un' anteprima Exif. Se presente digitare **exif –e nomefile** e premere **Invio.** Anche in questo caso bisogna sostituire **nomefile**.

ll programma crerà nella stessa posizione nella quale si trova il file un' altro file in formato Jpeg (che pesa solitamente meno di 10 KB) che contiene l' anteprima Exif. Per eliminare l' anteprima Exif da un' immagine ed impedire quindi questa analisi si può utilizzare il comando **exif –r nomefile**.



AGGIORNARE IL THUMBNAIL EXIF

Quando si effettuano operazioni di fotoritocco su una foto, raramente ci si ricorda di aggiornare l' anteprima Exif per evitare la possibilità di ricostruzione dell' immagine originaria mediante l' estrazione della thumbnail Exif. Alcuni programmi come **GIMP** possono aggiornare l' anteprima Exif. Per salvare il file, alla fine delle operazioni di fotoritocco, fare click su **Save as..** che si trova nel menu **File**, selezionare l' estensione **JPG** e premere **Save**. Nella finestra che si apre selezionare **Save thumbnail** e premere di nuovo **Save**.

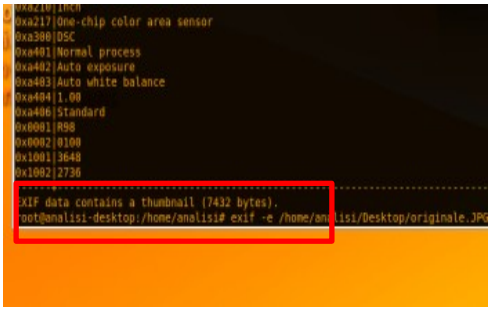


– *STEGANOGRAFIA: ESTRARRE DATI NASCOSTI*

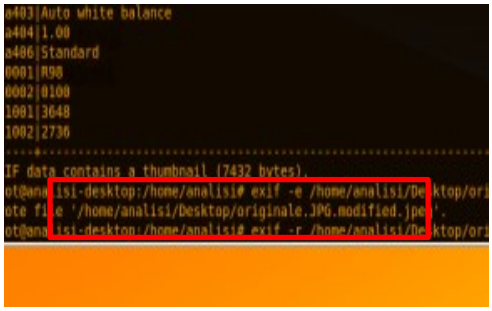
Steganografia è una parola che deriva dal greco e significa “scrittura nascosta”. La steganografia è una tecnica che permette di nascondere dei messaggi testuali all’ interno di un file immagine (generalmente in formato JPG). Il metodo più utilizzato per la steganografia è l’ **algoritmo LSB** (Least Significant Bit), che si basa sul fatto che ogni pixel di un’ immagine è composto da un differente colore e cambiando il bit meno significativo di un pixel il contenuto dell’ immagine rimarrà lo stesso (almeno per l' occhio umano). L’ algoritmo LSB richiede un contenitore (l’ immagine JPG), un dato da nascondere (ad esempio un file txt) e una password per cifrare il messaggio.

Inseriti il dato da nascondere, l' immagine contenitore e la password, l’ algoritmo LSB procede cercando nel contenitore tutti i bit meno significativi, sovrascivendone ognugno con un bit del file da nascondere e generando così il dato steganografico. Ovviamente esiste un limite ai bit che si possono sovrascrivere in un immagine (oltre il quale ci sarebbero cambiamenti troppo vistosi nell' immagine) e quindi un limite alla dimensione del file che ci si può “nascondere” dentro con una tecnica di steganografia. Il tool preposto, in Caine, a nascondere file dentro immagini JPG mediante steganografia è **Steghide**. Per estrarre il file nascosto in un’ immagine senza conoscere la chiave si usa invece **Stegbreak.** Per individuare un contenuto nascosto in un' immagine si utilizza **Stegdetect**.

Cliccare su **Stedetect** nella scheda **Analysis**. Selezionare **Input Directory** per selezionare la cartella che contiene le immagini da analizzare.



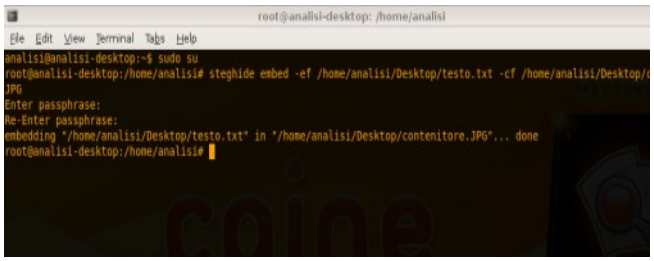
Cliccare su **Run Stegdetect** per avviare l’ analisi. Si aprirà una finestra del terminale dove sarà indicato il risultato dell’ analisi.



Se un’ immagine risultasse positiva al test, avviare il terminale, digitare **sudo su** e preme invio. Poi digitare **stegbreak –tp nomefile** e premere Invio.

STEGANOGRAFIA CON STEGHIDE

Acquisiti i privilegi di utente root (comando sudo su) digitare **steghide embed –ef testo.xt –cf immagine.jpg –p password** e premere Invio. Ovviamente **testo.txt** va sostituito con il percorso completo del file da nascondere, **immagine.jpg** con quello dell' immagine-contenitore e **password** con la password per cifrare il testo. Per estrarre il testo nascosto nell' immagine in comando **è steghide extract –sf immagine.jpg –p password**.



– *CALCOLO DELL' HASH DI UN FILE*

La funzione hash è una funzione non iniettiva che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita. Esistono vari algoritmi che permettono di calcolare gli hash di un file, ma sicuramente i più diffusi sono lo **SHA1** e l' **MD5**. Ogni algoritmo restituisce una stringa alfanumerica a partire da un qualsiasi flusso di bit di qualsiasi dimensione (può essere un file ma anche una stringa). L'output (ovvero la stringa di hash) è detto **digest**. L' hash di un file è tipico di esso è costituisce quindi un identificatore univoco di quel file.

La lunghezza dell' hash varia a seconda dell' algoritmo (128 bit per l' MD5, 160 bit per lo SHA1 o 256 bit per lo SHA256).

Gli hash si usano in analisi forense, sia per effettuare confronti tra file, sia per essere sicuri che un file non sia stato modificato durante l' indagine. Infatti anche una minima modifica del file comporterebbe una variazione dell' hash. Gli hash vengono anche utilizzati per identificare gli errori nella trasmissione di file: il confronto tra l' hash del file spedito e di quello ricevuto permette di capire se una o più parti del file sono state alterate durante la trasmissione (molti siti indicano accanto a downloads la checksum MD5 o SHA1) Il software di Caine che si occupa del calcolo degli hash è **GtkHash**. GtkHash calcola di default l' hash di ogni file che gli viene indicato utilizzando l' algoritmo SHA1 e MD5 ma è possibile abilitare il calcolo dell' hash utilizzando fino a 27 algoritmi differenti.

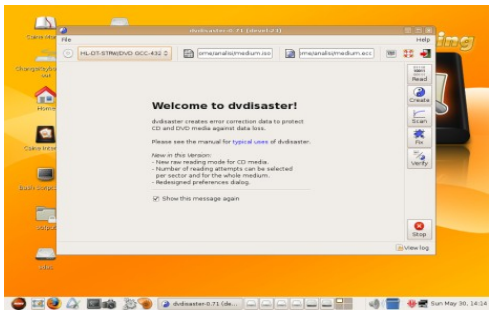
Avviare **GtkHash**, cliccando su **Menu** e poi su **Forensics Tools**.

Cliccare sull' icona a forma di cartella, in alto a destra, per selezionare il file.Cliccare su **Hash** per calcolare l' hash.

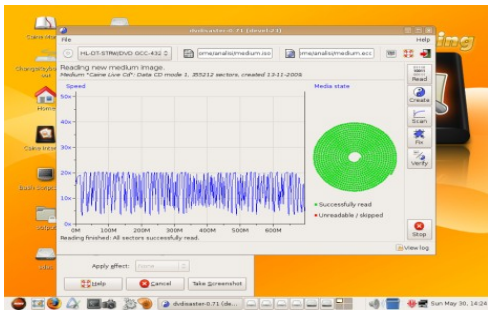
Cliccare su **View** e poi su **Preferences** per poter scegliere altri algoritmi per calcolare l' hash.

– *RECUPERO DATI DA UN CD/DVD DANNEGGIATO*

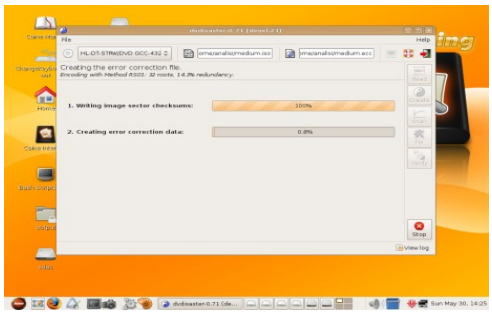
Molte volte un CD o un DVD è talmente rigato che inserendolo nel lettore CD/DVD non si riesce nemmeno a visualizzare i file che sono contenuti in esso. Per recuperare i dati in esso contenuti bisogna allora utilizzare un software specifico come DvdDisaster che permette di creare immagini .iso dei supporti danneggiati. Anche Dvdisaster ha dei limiti: tutti i settori danneggiati (quindi che Dvdisaster non riesce a leggere) vengono riempiti con degli zero binari, se il CD/DVD è troppo danneggiato, Dvdisaster riempirà molti settori con il valore e quindi molti settori saranno illeggibili anche nell' immagine iso generata.



Avviare **DvdDisaster** dal menu **Forensics Tools**. Selezionare il lettore **CD/DVD** contenente il supporto utilizzando il menu a tendina nell' angolo in alto a sinistra.



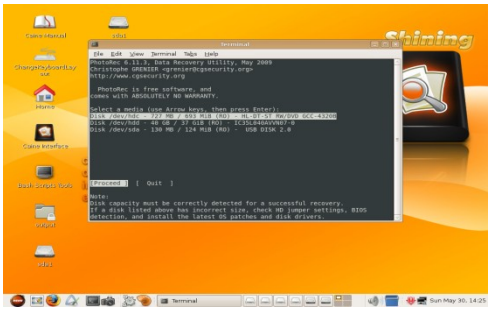
Aggiungere la posizione dell' **immagine .iso** da creare e cliccare su **Read** nella colonna di destra. Attendere la fine dell' operazione.



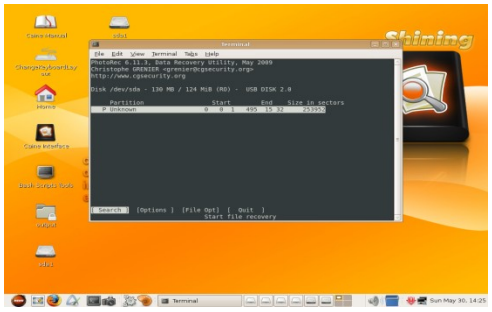
Cliccare su **Create**, che si trova sotto il pulsante Read e attendere. A questo punto l' immagine del **CD/DVD** danneggiato è pronta per essere masterizza con un software come **Brasero Disc Burner**.

– *DATACARVING CON PHOTOREC*

Il Data Carving è il processo di ricomposizione di frammenti di file di computer, in assenza di metadati del filesystem. Il data carving viene reso possibile dall' analisi degli **header** e dei **footer**. Gli header e i footer sono sequenze alfanumeriche che sono sempre presenti in una determinata posizione di un tipo di file (gli header all'inizio del file e i footer alla fine).
Per esempio l' header di un file **JPEG** è sempre **0xFFD8FFI1**. L' analisi di queste sequenze permette di ricostuire un file. Il programma di Caine che si occupa di data carving è **Photorec** che permette di recuperare da qualsiasi dispositivo file JPG, MP3, PDF, HTML e TXT e altri.



Avviare **PhotoRec**, cliccando su **Menu** e poi su **Forensics Tools**. Scegliere il dispostivo da analizzare e premere **Invio**.



Selezionare la partizione del dispositivo e premere **Invio**.

Attendere che l' analisi sia comletata e premere **Invio** per uscire dall' applicazione.

Come in Autopsy, anche il recupero dati con Photorec ha dei limiti. Anche in questo caso se un file è stato sovrascritto con un software di wiping le possibilità di recupero sono molto ridotte (se non nulle).

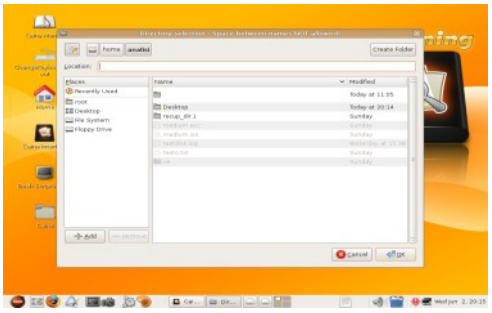
– *ESPORTAZIONE DEL REPORT*

Alla fine dell' indagine è possibile esportare il report automatico che contiene tutte le indicazioni sulle analisi effettuate e sui supporti coinvolti (CD,DVD, chiavette USB, Memory Cards, ecc…).

Il report può essere esportato in formato HTML e in formato RTF. Esportandolo in RTF si potrà poi integrare con eventuali note e aggiunte dell' investigatore utilizzando un qualsiasi word processor, come Abiword (incluso in Caine).

Spostarsi nella scheda **Report** dell' interfaccia centrale e fare click su **HTML Format** (per esportare il report in HTML) o su **RTF Format** (per esportarlo in HTML).

Nella finestra che appare selezionare la lingua nella quale si desira sia scritto il report e premere **Ok**.



Selezionare il percorso di destinazione e cliccare su **Ok**. Attendere che il processo venga completato.

– *BIBLIOGRAFIA DELLE FONTI*

AA.VV., *"Computer Forensics"*, Apogeo editore, Milano 2007, p. 366, € 35,00

Michele Petrecca, *"Steganografia: l' arte di nascondere i messaggi"*, da Linux Magazine (agosto 2009 - anno XI - n° 8), Edizioni Master

Alessandro Di Nicola, *"L' investigatore digitale"*, da Linux Magazine (giugno 2010 - anno XII - n° 6), Edizioni Master

AA.VV., *"Sulla scena del crimine"*, da Win Magazine (luglio 2010 - anno XIII - n° 7), Edizioni Master

Contributori di Wikipedia, "Exchangeable image file format", *Wikipedia, L'enciclopedia libera*, http://it.wikipedia.org/w/index.php?title=Exchangeable_image_file_format&oldid=31766119 (in data 31 maggio 2010).

Contributori di Wikipedia, "Steganografia", *Wikipedia, L'enciclopedia libera*, http://it.wikipedia.org/w/index.php?title=Steganografia&oldid=32070023 (in data 31 maggio 2010).

Contributori di Wikipedia, "Informatica forense", *Wikipedia, L'enciclopedia libera*, http://it.wikipedia.org/w/index.php?title=Informatica_forense&oldid=31241898 (in data 31 maggio 2010).

http://www.caine-live.net/page11/page11.html

http://dvdisaster.net/en/

http://dvdisaster.net/en/index10.html

http://www.denisfrati.it/?p=525