Live Forensics

Fabio Fulgido, Gaetano Rocco, Mario Fiore Vitale

Tesina di Sicurezza

Università degli Studi di Salerno

Prof. Alfredo De Santis

Dott. Aniello Castiglione

Dott. Bonaventura D'Alessio

Anno Accademico 2010/2011

Novembre 2011

Introduzione

1. Introduzione

La Computer Forensics è la scienza che studia l'individuazione, la conservazione, la protezione, l'estrazione, la documentazione e ogni altra forma di trattamento del dato informatico al fine di essere valutato in un processo giuridico e studia, ai fini probatori, le tecniche e gli strumenti per l'esame metodologico dei sistemi informatici [1] [2].

Essendo una materia di recente nascita e quindi in via di sviluppo (la sua nascita si colloca intorno al 1980 ad opera dei laboratori tecnici della FBI), è al costante inseguimento della tecnologia. Ciò è causato dal fatto che i computer crescono di numero e di capacità, gli hard disk sono sempre più grandi e le memorie si sprecano in vari dispositivi, dai DVD, alle USB Flash Memory, alle memory card, ai cellulari etc.

L'autorità giudiziaria è messa in difficoltà dalla continua evoluzione degli apparati elettronici contenenti dati alterabili e talvolta deperibili. A partire da queste problematiche è necessario da parte degli investigatori del futuro adottare un protocollo comune di repertaggio, di custodia e di analisi dei dati. La scelta comune degli strumenti di repertaggio è caduta sull'Open Source Software (tutti quei programmi il cui codice è disponibile) in modo tale da essere immuni da eventuali contestazioni a riguardo. In Italia, la legge di riferimento per l'informatica forense è la Legge n.48/2008, nota come "Legge di ratifica della Convenzione di Budapest".

In questo documento tratteremo della live forensics che è una disciplina collocata all'interno della computer forensics. Nel capitolo 2 verranno espletati i concetti di computer forensics facendo riferimento all'ambito di applicazione, nello specifico illustreremo l'analisi post mortem e l'analisi live. Nel capitolo 3 verranno analizzati alcuni dei tool utilizzati nella computer forensics introducendo anche le distribuzioni contenenti i suddetti tool. Nel capitolo 4 verranno mostrati tool specifici per: il dump della RAM, l'analisi del dump della RAM, le informazioni sui processi in esecuzione ed il contenuto della clipboard. Infine nel capitolo 5 verrà mostrato il caso di studio trattato con obiettivi e risultati ottenuti.

Computer Forensics

2. Computer Forensics

La Computer Forensics è la disciplina atta a risolvere tutto ciò che riguarda i crimini informatici o crimini generici dove il computer gioca un ruolo nella sua attuazione. Cosa intendiamo per Crimine Informatico? Un crimine informatico è un fenomeno criminale che si caratterizza come un abuso della tecnologia informatica. Tutti i reati informatici sono caratterizzati da:

- Utilizzo delle tecnologia informatica per compiere l'abuso;
- Utilizzo dell'elaboratore per compiere l'abuso.

Il crimine informatico è una truffa tipicamente perpetrata tramite mail da phisher (phishing: "spillaggio" di dati sensibili) che hanno lo scopo di sottrarre informazioni riservate. Gli strumenti sul mercato nero utilizzati per gli attacchi sono i programmi cosiddetti "crimeware": bot (abbreviazione di robot, programma creato per simulare l'attività umana in rete), trojan (cavallo di troia, software nascosto dentro un programma) e spyware (software che raccoglie informazioni riguardanti l'attività online di un utente senza il suo consenso come siti visitati, acquisti online etc., trasmettendole tramite internet ad un'organizzazione che le utilizzerà per trarne profitto).

Per potere effettuare computer forensics c'è bisogno di elevate conoscenze informatiche congiunte a buone capacità di analisi, osservazione e pazienza. Mentre le metodologie di base rimangono sempre costanti, le tecnologie che permettono l'acquisizione e l'analisi sono in continuo aggiornamento.

Nelle attività di indagine troviamo essenzialmente due casistiche:

- Il computer è il mezzo usato per compiere un'azione criminosa;
- Il computer è a sua volta vittima di un crimine.

Bisogna tener presente che a tutt'oggi non esiste ancora una legislazione chiara che individui un modus operandi, ma si hanno comunque delle linee guida definite "best practices" che garantiscono il corretto svolgimento di tutte le fasi lavorative.

Le metodologie in questione si svolgono nel modo seguente:

- Acquisire le evidenze senza alterare o danneggiare i dati originali;
- Autenticare che l'evidenza recuperata corrisponda col dato analizzato in originale;
- Analizzare i dati senza modificarli.

Il primo punto è fondamentale nell'informatica forense perché in esso assume un ruolo centrale l'integrità dei dati. Per la salvaguardia di questi ultimi gli operatori predisposti utilizzano determinate metodologie volte a garantire e provare l'esatta corrispondenza dei contenuti in un momento qualsiasi dell'analisi. Risulta necessario "congelare" il dato utilizzando tutti i possibili accorgimenti tecnologici atti ad impedire scritture anche accidentali di bit e a verificare che in un momento successivo i dati siano gli stessi. Per adempiere a tali obblighi è necessario l'impiego di hardware e software specifici che inibiscano ogni scrittura sui sistemi di archiviazione. C'è bisogno anche degli algoritmi hash come l'MD5 e SHA1 i quali applicano una funzione non invertibile ed atta alla trasformazione di un testo di lunghezza arbitraria in una stringa di lunghezza fissata. Il risultato dell'hash viene visto come una sorta di impronta digitale dell'evidenza, esso si definisce anche "valore di hash".

I dispositivi hardware che permettono di accedere a periferiche di memorizzazione in sola lettura sono i write blocker. Essi si presentano come dispositivi che possono solo leggere i dati contenuti nella periferica impedendo quindi un inquinamento dei dati.

La figura professionale che presta la sua opera in ambito di reati informatici o del computer crime si definisce "computer forensics expert" e la sua attività riguarda non solo i computer, ma qualsiasi attrezzatura elettronica che abbia la capacità di memorizzare dati. Il suo lavoro è reso particolarmente arduo dal fatto che spesso quando giunge sul luogo del crimine, esso è già stato manomesso dall'utente-vittima minando dunque l'indagine in partenza.

Dall'esperienza dei computer forensics experts è emerso che, nonostante possibili analogie, ogni caso criminale è diverso da un altro e presenta proprie peculiarità e caratteristiche; tale considerazione ha portato all'idea di offrire un servizio più orientato ad un'attività di analisi/consulenza frutto dell'esperienza piuttosto che ad una serie di prodotti e soluzioni. Uno dei metodi proposti si basa su una metodologia detta "full spectrum approach", idea nata dall'USAF (United States Air Force) e basata sul fatto che la

computer forensics non va affrontata nei soli aspetti tecnici ed informatici perché sarebbe troppo limitativo, bensì vanno tenuti in considerazione quattro aspetti ben distinti correlati tra loro:

- **Tecnologico** che implica un aggiornamento costante sulle nuove tecnologie e sull'utilizzo dei sistemi. Gli esperti utilizzano le più avanzate tecnologie a supporto delle attività di analisi ed investigazione, assicurando il rispetto delle normative e l'uniformità con la "best practices" di riferimento.

- **Procedurale** che raccoglie tutte le informazioni possibili, vaglia, analizza, protocolla e sviluppa le linee guida. Lo scopo è quello di operare in modo da rendere le evidenze e gli eventi identificati resistenti, non imputabili, non ripudiabili ed integri in caso di contestazioni.

- **Sociale** che salvaguardia la privacy dell'individuo tenendo conto delle esigenze degli investigatori: ecco perché le attività degli esperti vengono svolte nella massima riservatezza e confidenzialità, garantendo sempre ampia disponibilità, discrezione ed affidabilità.

- **Legale** che consiste nel gestire il tutto in conformità con i riferimenti legislativi in essere. Questo è uno degli aspetti peculiari del lavoro forense che prevede anche un'attività di consulenza nella produzione della documentazione necessaria prima, durante e dopo l'investigazione e necessaria a garantire la correttezza legale delle operazioni svolte.

La computer forensics si divide in due branche:

- Analisi post mortem
- Analisi live

2.1. Metodologie

2.1.1. Analisi post mortem

E' la metodologia che viene usata quando il supporto (in genere hard disk) da analizzare non è in funzione. Per questo motivo si effettua l'acquisizione dei dati in maniera RAW o bit a bit in modo da poter lavorare sui dati presenti sull'hard disk, consentendo di acquisirne tutte le informazioni, inclusi slack space e file cancellati, così da poterne avere una copia perfetta che andrà memorizzata su un supporto esterno sterilizzato tramite la procedura di wiping (di cui è bene conservare il log) o su un file immagine. Fondamentale è effettuare l'analisi su una copia del file per consentire la ripetibilità e non perdere i dati iniziali. In questo modo anche se si verificherà un errore durante le varie procedure si può tornare al dato iniziale e non compromettere le indagini in corso. Gli strumenti usati per l'analisi devono essere anzitutto collaudati e accettati dalla comunità degli esperti e, chi li usa, deve avere una conoscenza approfondita per poterli utilizzare nel modo giusto. Per una maggior sicurezza dei dati trattati i dischi si custodiscono sempre in buste elettrostatiche e anti caduta e l'analisi viene eseguita in ambienti sterili.

2.1.1.1 Strumenti

Sono di tipo hardware e software. Si possono scegliere sia tool commerciali/proprietari o tool Open Source. La scelta deve essere fatta in base alla qualità che viene offerta dal tool oppure dalle operazioni che esso supporta per una determinata analisi. Alcuni tipi di tool open source sono:

- CAINE
- DEFT
- HELIX

Fra i tool proprietari ci sono:

- EnCase
- Forensic Toolkit
- X-Ways Forensics
- P2 Commander.

Come descritto precedentemente uno degli strumenti fondamentali per proteggere i dischi da acquisire è il write blocker, dispositivo che previene eventuali scritture sull'hard

disk oggetto di investigazione. Esso viene generalmente posto tra il disco e il computer utilizzato per esaminarlo. Ci sono tre tipologie di write blocker:

- **Firmware based**: tramite il BIOS che inibisce ogni tipo di scrittura sul disco d'origine
- **Software based**: software di basso livello che impedisce qualsiasi scrittura sulla memoria di massa considerata. In questo caso non è più il BIOS a impedire l'alterazione, ma il sistema operativo.
- **Hardware based**: dispositivo elettronico che taglia il bus di comunicazione tra l'unità su cui si stanno copiando i dati e la scheda madre del computer analizzato. E' come un intermediario che inibisce qualsiasi modifica ai dati del dispositivo incriminato, mettendo al sicuro l'analisi dagli errori umani e da eventuali bug.

Oltre a tutto ciò è necessario anche che l'operatore abbia una certa esperienza e una sorta di "sesto senso", infatti come su una vera e propria scena del crimine, le evidenze possono essere nascoste in posti introvabili (protette da password, nascoste dentro immagini [steganografia], server internet). A volte, per risparmiare tempo e andare a colpo sicuro nella ricerca dei reperti, può essere utile un profiling del sospettato dedicando un po' di tempo al suo profilo psicologico per facilitare la ricerca delle evidenze. Due approcci possono essere quello deduttivo, adattando l'idea generale che si ha del colpevole al caso specifico del crimine commesso, o induttivo, avvalendosi di un'analisi statistica del caso particolare per poi risalire a una descrizione più generale.

2.1.2 Analisi live

Quando non si può fare a meno di agire sulla scena del crimine, cosa succede? Talvolta l'analisi deve iniziare prima della copia o del sequestro fisico.

La procedura che per anni è stata considerata la migliore possibile è quella della catalogazione dei reperti fisici dei personal computer. Questa prassi operativa è stata sempre applicata con l'apparente certezza che il computer sulla scena del crimine fosse stato spento ma, in realtà, senza assicurarsi che il sistema operativo ne fosse avveduto.

- Esempio: Spegnimento forzato mediante l'interruzione dell'alimentazione elettrica.

Nonostante si sappia che lo spegnimento porti alla perdita delle informazioni ed in particolare quelle contenute nella RAM, si è ritenuto che il costo di queste perdite fosse minimo rispetto all'interazione di un non specialista con la macchina.

La complessità anche dei piccoli sistemi, nonché quella scontata dei grandi sistemi, rende sempre più grande la perdita di dati inerente lo spegnimento forzato che, sempre più spesso, elimina fonti di evidenza determinanti. Molte delle possibili evidenze presenti a runtime in RAM non vengono repertate e possono essere:

- Comunicazioni con dati non persistenti (es. chat) che risiedono per la massima parte in RAM e quindi la loro degradazione nello spegnimento forzato è pressoché totale.
- Protezioni criptate per intere partizioni che al momento dell'impiego della macchina sono abbassate per evidenti necessità di efficienza della memoria di massa; allo spegnimento del sistema l'accesso alla partizione può risultare complicato se non impossibile.
- Dati recenti non ancora salvati sull'hard disk.

E' necessario quindi, in queste condizioni, accedere alla macchina con competenza e prontezza.

Se si ipotizza la possibilità di interagire sulla scena del crimine con la macchina, risulterà che:

- Alcuni dati da copiare possono emergere durante l'interazione con la macchina per cui il repertamento dati avviene a fasi incrementali.
- Preparazione ed analisi sono ridotti al minimo durante l'interazione con il sistema proprio per diminuire la possibilità di causare cambiamenti rilevanti nelle memorie digitali in analisi e lasciare la parte approfondita all'approccio statico.
- Il reporting non è quello del forensics statico, che si propone di spiegare le operazioni in dettaglio e presentarle in dibattimento. In termini di polizia giudiziaria, l'obiettivo dell'analisi live non è una sorta di verbale tecnico.

E' importante sottolineare che le attività principale dal punto di vista tecnico nel computer forensics statico, ossia preparazione ed analisi, divengono minime nell'attività live.

Mentre l'approccio statico tende a generare attività ripetibili dal punto di vista sia tecnico che legale, le attività live sono intrinsecamente irripetibili, da cui l'assoluta necessità di un affidabile reporting.

L'irripetibilità della live forensics è:

- **Di natura tecnica**: non esiste infatti possibilità di realizzare analisi e repertamento dati live senza modificare almeno una parte della memoria del sistema
- **Di natura temporale**: la situazione della macchina all'atto dell'attività è frutto del momento e la sua complessità ed è tale da non poter essere riprodotta.
- **Di natura strutturale**: lo stato di un computer non è completamente osservabile perché la sonda che si dovrebbe inserire per compiere tale osservazione andrebbe a modificare proprio lo stato (paradosso del gatto di Schroedinger)

2.1.2.1 Acquisire le evidenze

Alcune regole di massima riguardano il fare attenzione allo stato evidente della macchina e quindi screen saver attivi, la lista dei processi, l'alimentazione elettrica, la presenza di dati cifrati, le periferiche e le connessioni wired/wireless presenti. Le pratiche più importanti di cui tener conto per massimizzare la qualità delle evidenze sono:

- **Running known good binaries**: un investigatore non dovrebbe affidarsi agli eseguibili del sistema su cui va a operare ma dovrebbe fornire lui stesso gli eseguibili per raccogliere evidenze. Questi eseguibili possono essere copiati sul sistema, anche se questa azione potrebbe sovrascrivere alcune evidenze. Tuttavia, se la scelta deve essere tra perdere alcune evidenze e non ottenerne affatto, è meglio rischiare.
- **Hashing all evidence**: una volta acquisita, l'evidenza deve essere preservata in modo tale che l'investigatore possa, in un secondo momento, dimostrare che nulla è stato contaminato. Il metodo più accettato è quello di calcolare un hash dei dati (solitamente tramite funzioni quali MD5 o SHA-1). L'hash, così, viene ricalcolato e comparato con l'hash del primo repertamento.
- **Gathering data in order of volatility**: alcuni dati sono più effimeri di altri. Le evidenze dovrebbero essere raccolte in base all'ordine di volatilità (vd. 2.1.2.2) e

l'investigatore deve tener conto del contesto dell'investigazione nella sua totalità in modo da prendere decisioni sull'ordine di acquisizione delle evidenze.

L'acquisizione dei dati può venire in diversi modi:

- **Computer forense collegato al reperto tramite connessione ethernet**: vi è la necessità di configurare il reperto per la connessione, il vantaggio è che si può operare dall'esterno e il trasferimento dati può essere piuttosto semplice.
- **Drive esterni**: si sfruttano le connessioni USB del reperto per connettere una memoria di massa o un disco esterno. Il vantaggio è che procurarsi memorie di massa esterne è in generale semplice e poco costoso, purtroppo però in questa operazione si deve impiegare il reperto direttamente per tutta l'attività.
- **Ripresa video o printscreen**: in genere vengono usati come elemento aggiuntivo ad uno dei due o sostitutivo dei precedenti.

Una volta che le evidenze sono state acquisite, devono essere analizzate. E' spesso impensabile analizzare tutte le possibili informazioni ottenute in un' analisi live, un investigatore deve quindi effettuare una scrematura per poi esaminarli.

2.1.2.2 Ordini di volatilità

I dati su un sistema hanno un ordine di volatilità [3]. In generale, i dati tenuti in memoria, nell'area di swap, all'interno dei processi di rete ed all'interno dei processi di sistema sono più volatili rispetto ad i dati contenuti nell'hard disk e possono essere perduti in seguito ad un riavvio. Per cercare delle evidenze e quindi estrarre dati è necessario procedere dalle componenti con volatilità più alta per terminare a quelle di scarsa volatilità. Stiliamo quindi un ordine di volatilità (indice piccolo corrisponde ad alta volatilità):

1. Memoria RAM
2. Memoria di swap
3. Processi di rete
4. Processi di sistema
5. Informazioni del file system
6. Dati sul disco

La RAM risulta essere più volatile in quanto vengono effettuati continuamente accessi, la memoria di swap ha una priorità inferiore ma comunque alta dato che è usata per lo swap delle pagine della memoria. Alcuni processi possono scambiare dati usando la rete e lo scambio avviene in tempi molto veloci utilizzando talvolta buffer, per questo i processi di rete hanno un'alta volatilità. Per i processi di sistema la volatilità è inferiore in quanto un processo, a meno che non venga terminato volontariamente, ha il suo tempo di vita che dipende dal tipo di operazioni che il processo deve effettuare. Infine i dati sul disco ed i metadati relativi (data di creazione, autore, dimensione etc.) hanno una volatilità molto bassa in quanto persistono anche ad un riavvio del computer.

Distribuzioni

3. Distribuzioni

3.1. Introduzione

Per effettuare tutte le attività forensi c'è bisogno di utilizzare alcune distribuzioni che sono state progettate per rendere possibili tali analisi. Le distribuzioni più usate per effettuare computer forensics sono Helix, CAINE, DEFT tutte basate sul kernel Linux, che offrono strumenti ed applicazioni software (vd. Allegato), che siano esse freeware, open source o commerciali. In queste distribuzioni solitamente è presente anche una modalità live che permette di effettuare l'analisi live.

3.2. Helix

Helix è una distribuzione Linux per l'analisi forense (www.e-fense.com/helix/). Attualmente è alla versione 3Pro 2009 R3 rilasciata il 23 Dicembre del 2009 che comprende anche un'interfaccia applicativa per l'analisi Live di un ambiente Windows.

L'applicativo per l'analisi live è **Helix.exe** che viene avviato automaticamente all'inserimento del CD. Il suo funzionamento è stato testato in Windows 98SE, Windows NT4, Windows 2000, Windows XP, Windows 2003 e Windows Vista. È importante notare che l'esecuzione dell'applicativo in un sistema acceso ne modifica lo stato, poiché richiede l'utilizzo di alcune DLL di sistema e di un certo quantitativo di spazio all'interno della RAM.

La scelta di non includere le DLL all'interno del CD dipende dalla diversità della versione del sistema operativo.

Di seguito verranno illustrate le principali funzionalità e i principali software presenti in Helix.

3.2.1 Avvio di Helix

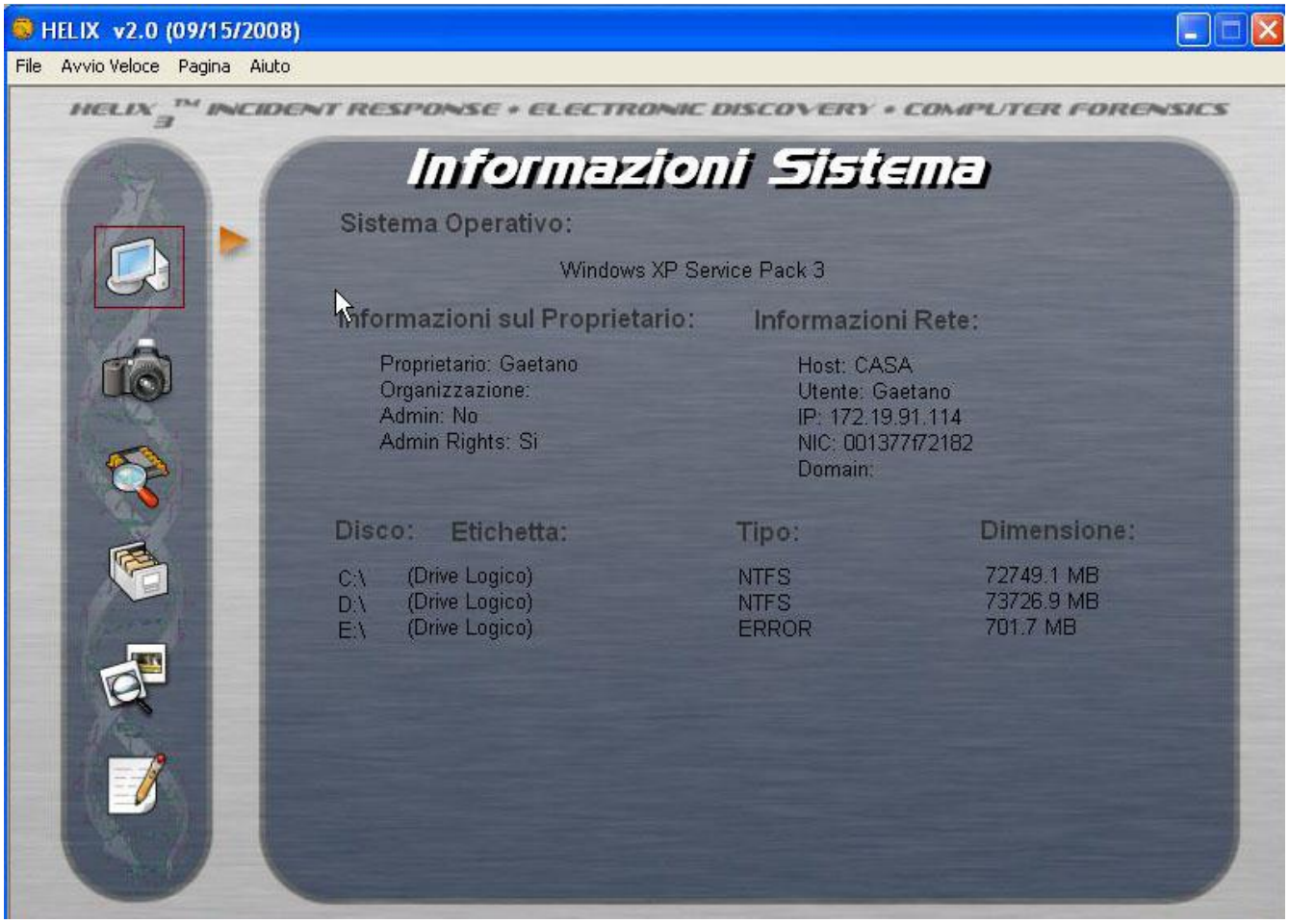
Appena inserito il CD (se nel sistema è attivo l'autorun) compare una schermata che avvisa l'investigatore che l'esecuzione del programma comporta una modifica al sistema attivo. Selezionare la lingua desiderata (nell'esempio Italiano) e fare clic sul tasto "**Accettare**"

Viene caricata la schermata principale del programma.

Helix fornisce un'icona nella tray bar per ridimensionare e chiudere il programma.

3.2.2 Anteprima informazioni di sistema

Dalla schermata principale è possibile effettuare una "**Anteprima informazioni di sistema**" dove sono visualizzate le informazioni principali del sistema (versione del sistema operativo, informazioni di rete, informazioni sul proprietario e dispositivi collegati al sistema)



Facendo clic sulla freccia arancione si accede alla seconda pagina di informazioni, che contiene la lista dei processi attivi.

L'esecuzione dal CD garantisce l'integrità delle informazioni visualizzate. L'utilizzo del **Task Manager** del sistema operativo per ottenere queste informazioni non è opportuna, poiché potrebbe essere stato modificato da rootkit o virus.

3.2.3 Acquisizione

Dalla schermata principale facendo clic su "**Acquisisci un'immagine Live**" si accede agli strumenti per l'acquisizione di dispositivi collegati alla macchina.

Helix mette a disposizione principalmente due programmi per l'acquisizione:

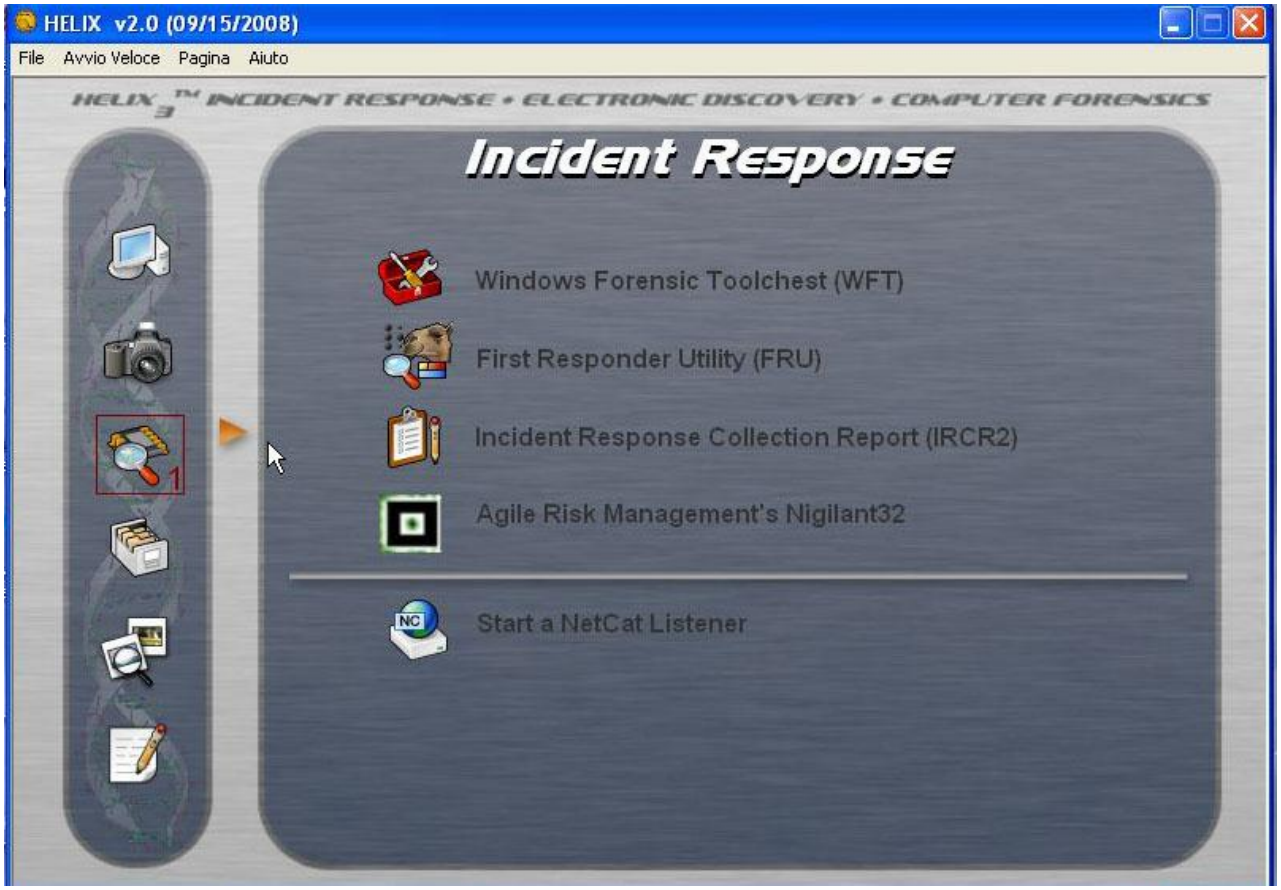
- **dd per Windows**
- **Access Data FTKImager**

Questi tool permettono l'acquisizione di diversi tipi di drive (ad esempio: hard disk o RAM) presenti nel sistema generando un report.

Facendo clic sulla freccia arancione si accede alla pagina per l'esecuzione di FTKImager.

3.2.4 Incident Response

Helix mette a disposizione anche alcuni "**strumenti di incident Response**" che consistono in un set di tool che permettono diversi tipi di analisi come: diagnosi dei processi in real-time, analisi delle cache dei diversi browser, analisi del registro di Windows, tool per la visualizzazione di password, analisi dei client di posta elettronica, monitoraggio della rete e tool per il file recovery.


HELIX v2.0 (09/15/2008)
File Avvio Veloce Pagina Aiuto
HELIX 3 INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
Incident Response
Windows Forensic Toolchest (WFT)
First Responder Utility (FRU)
Incident Response Collection Report (IRCR2)
Agile Risk Management's Nigilant32
Start a NetCat Listener


HELIX v2.0 (09/15/2008)
File Avvio Veloce Pagina Aiuto
HELIX 3 INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
Incident Response
FILE:
MD5:
...
Hash
Command Shell
File Recovery
VNC Server
Rootkit Revealer
PuTTY SSH
Screen Capture
WinAudit
PC On/Off Time
Questo pulsante aprirÉ una shell di terminale sicura (cmd.exe) dal CD HELIX.
VerrÉ cio avviato un file binario non compromesso da un media non volatile
in un percorso chiuso.


HELIX v2.0 (09/15/2008)
File Avvio Veloce Pagina Aiuto
HELIX 3 INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
Incident Response
PST Password Viewer
Mail Password Viewer
Messenger Password
Network Password Viewer
Protected Storage Viewer
Asterisk Logger
IE History Viewer
Mozilla Cookie Viewer
IE Cookie Viewer
Registry Viewer
IE Password Viewer
USB Deview
MozillaCookiesView mostra in una tabella i dettagli di tutti i cookies contenuti
all'interno del file dei cookie (cookies.txt), permettendo di salvare la lista in un file
di testo, HTML o XML, cancellando i cookies non desiderati, ed eseguendo un
backup/restore del file dei cookies.

3.3. CAINE

CAINE (Computer Aided Investigative Environment) è una distribuzione italiana GNU/Linux live creata come progetto di Digital Forensics(http://www.caine-live.net/). Attualmente è alla versione 2.5.1 denominata "*Supernova*" ed il project manager è Nanni Bassetti. CAINE offre un ambiente completo di digital forensics organizzato per integrare strumenti esistenti tramite una interfaccia grafica. Gli obiettivi principali di progettazione di CAINE sono i seguenti:

- un ambiente interoperabile che supporta l'investigatore digitale durante le quattro fasi dell'indagine digitale
- un' interfaccia grafica user friendly
- una semi-automatica compilazione della relazione finale

CAINE rappresenta pienamente lo spirito della filosofia Open Source perché il progetto è completamente aperto, chiunque potrebbe prendere l'eredità del precedente sviluppatore e project manager. Per quanto riguarda l'analisi live di sistemi Windows CAINE fornisce un modulo chiamato **WinTaylor**.

L'applicativo WinTaylor sempre sviluppato dallo stesso team ed anch'esso alla versione 2.5.1 si avvia tramite WinTaylor.exe presente sul sito della distribuzione. Il suo

funzionamento è stato testato in Windows 98SE, Windows NT4, Windows 2000, Windows XP, Windows 2003 e Windows Vista.

Avviato WinTaylor compare una schermata generale che permette di avviare diversi tool

per l'analisi live, in particolare si hanno a disposizione tool per:

- l'analisi del sistema
- l'acquisizione della memoria RAM, HDD o di altri dispositivi
- l'analisi dei processi in esecuzione
- l'analisi dei diversi browser

Inoltre WinTaylor permette di generare un report che traccia tutte le operazioni che sono state effettuate dall'avvio alla chiusura dell'applicativo WinTaylor.

3.4. DEFT

DEFT [4] (http://www.deftlinux.net/), acronimo di Digital Evidence e Forensics Toolkit, è un'altra distribuzione linux per la computer forensics che è nata nel 2005, sviluppata dall'Università degli studi di Bologna, e successivamente migliorata grazie alla collaborazione con l'IISFA. Attualmente è alla versione 6.1.1 rilasciata il 28 Ottobre 2011. DEFT è una distribuzione Live e al suo interno sono presenti numerosi strumenti applicativi Open Suorce per la computer forensics. A partire della versione 3 è stato avviato un processo di sviluppo di software "ex novo" che ha l'obiettivo di venire incontro ad alcune delle esigenze specifiche di chi lavora nel settore dell'informatica forense. Per quanto riguarda l'analisi live la distribuzione DEFT offre DEFT Extra (rilasciata il 26 Maggio 2009) una interfaccia grafica, utilizzabile solo sui sistemi operativi della famiglia Microsoft Windows che permette l'esecuzione di una selezione di programmi per 'analisi live.

All'avvio della GUI viene chiesto all'utente dove salvare il file di log che conterrà il report delle attività svolte; nel caso in cui viene annullata l'operazione, DEFT Extra non terrà traccia delle operazione compiute.

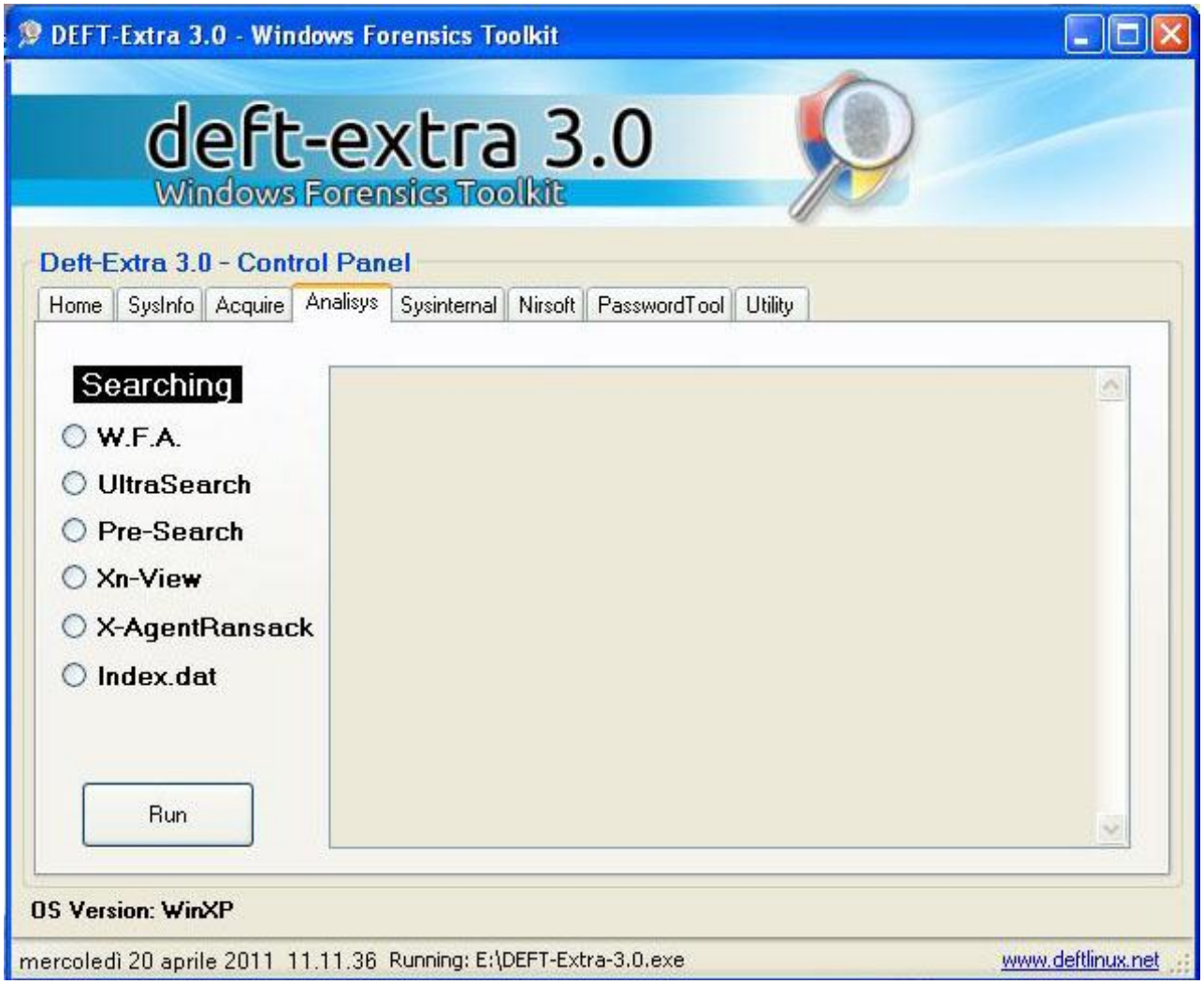
L'utilizzo di DEFT Extra e dei tool che la compongono potrebbe alterare alcuni dati del sistema sottoposto ad analisi, come:

- Chiavi del registro di Windows che memorizzeranno l'avvio di DEFT Extra mediante l'autorun (se abilitato).
- Data ultimo accesso del file posto ad analisi.
- Processo DEFT-Extra.exe in esecuzione.
- Scrittura del report in formato .txt nel caso in cui l'utilizzatore decidesse di salvare il report all'interno della memoria di massa del sistema (e non su un supporto esterno).

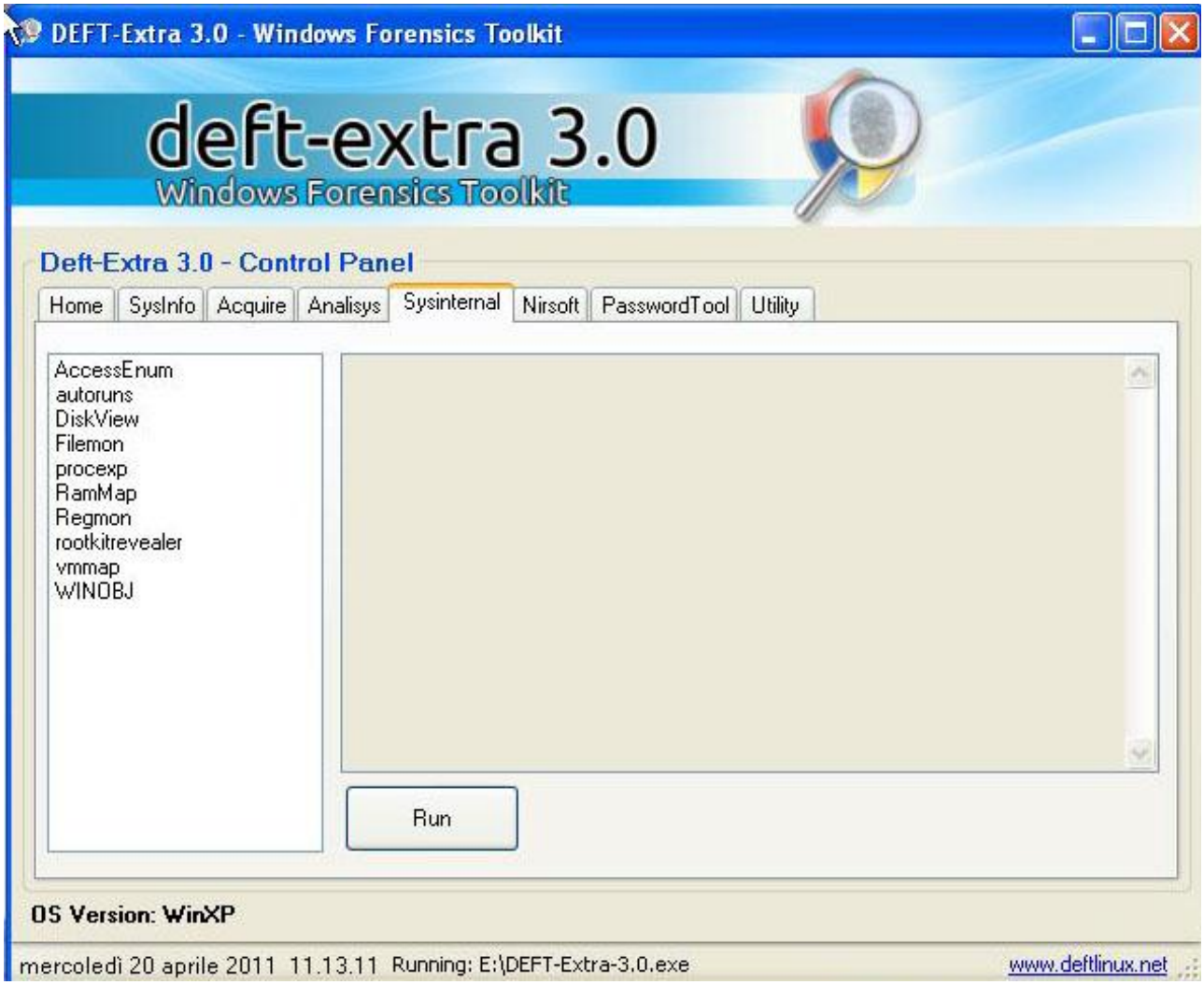
DEFT Extra è organizzato in sotto-menu in modo tale da dividere per categoria i tipi di tool.

Nella sezione SysInfo sono riportati i tool che effettuano una scansione della macchina fornendo le informazioni di base su come è composto il sistema.

La sezione Acquire contiene i tool per l'acquisizione dei dispositivi quali hard disk, RAM ed altri tipi di memorie di massa.



Il sotto-menu Analisys raccoglie tool per l'analisi delle acquisizioni effettuate con i tool presenti nella schermata precedente.



La sezione SysInternal offre dei tool per il monitoraggio del sistema a runtime al fine di rilevare possibili programmi ombra o comportamenti sospetti del sistema.

Il sotto-menu NirSoft comprende dei tool sviluppati dalla società NirSoft per il monitoraggio dei diversi browser delle loro cronologie e cache oltre a tool per l'analisi dei client di posta elettronica.

La sezione PasswordTool mette a disposizione diversi tool per il recupero di password di diverse applicazioni.

L'ultima sezione chiamata Utility raccoglie un gruppo di tool di supporto ad esempio per la cattura delle immagini del desktop.

Analisi Forense Dati Volatili

4. Analisi forense dati volatili

4.1. Tool utilizzati

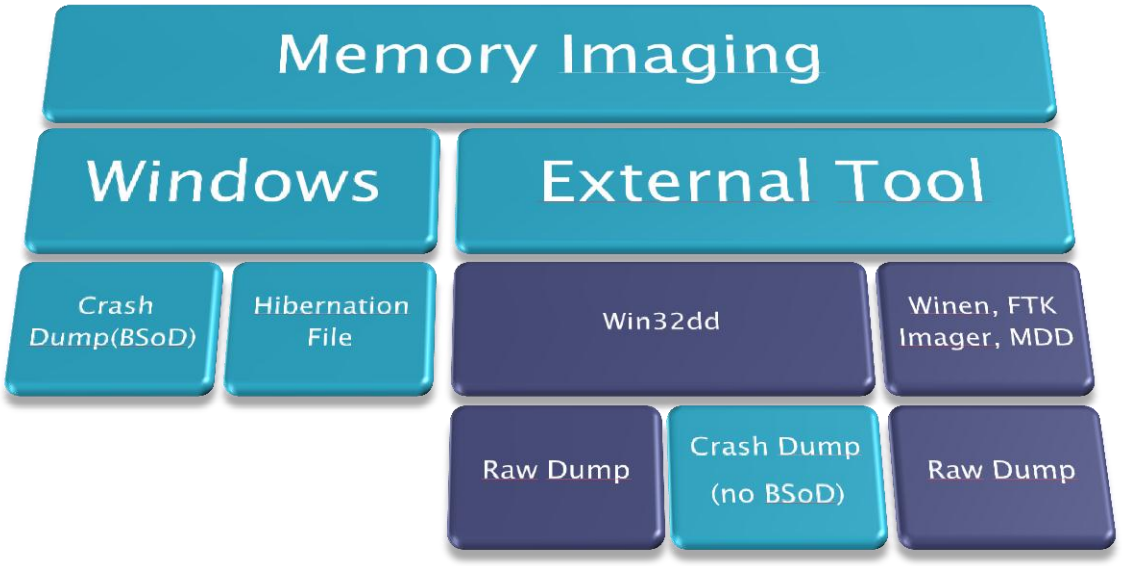
I tool utilizzati nel caso di studio riguardano: il dump e l'analisi del contenuto della RAM, il monitoraggio dei processi e delle loro ripercussioni sui file del filesystem, ed infine il contenuto della clipboard che sia esso un file o una porzione di testo. Per il dump mostreremo il funzionamento di Win32dd, Winen, MDD ed FTKImager [5] (relativo al dump). Per l'analisi del dump mostriamo come può essere fatta tramite FTKImager (relativo all'analisi). Per il monitoraggio dei processi e le loro ripercussioni sui file del filesystem mostreremo VMMap e FileMonitor. Infine per il contenuto della clipboard mostreremo InsideClipboard.

4.2. Dump RAM

Prima di iniziare a descrivere i tool definiamo prima le diverse tipologie di dump della RAM esistenti per i sistemi Windows [6]. Le tipologie di dump sono:

- Raw
- Crash
- Hibernation file

Il dump di tipo Raw è un dump che contiene l'intero contenuto della memoria RAM e può essere equiparato al dd per le memorie di massa, unico problema di questo tipo di dump è che non è possibile tener traccia del contenuto dei registri e lo stato del processore. L'altra tipologia ovvero il dump di tipo Crash riguarda la memorizzazione delle pagine del Windows Memory Manager (la parte di Windows che si occupa dello swap) e delle pagine relative al sistema operativo ed ai processi utente; il problema è che non vengono acquisite le pagine iniziali della RAM dov'è contenuta la password di accesso per l'account di Windows. Ultima tipologia, ma non per importanza, è l'hibernation file che si presenta come un file nascosto *hiberfil.sys* all'interno di C:\. L'hibernation file è creato quando viene richiesta l'ibernazione dal menù Start di Windows ed oltre al contenuto della memoria salva anche il contenuto dei registri e lo stato del processore, inoltre la suddetta procedura è possibile avviarla da Windows 98 fino a Windows 7.

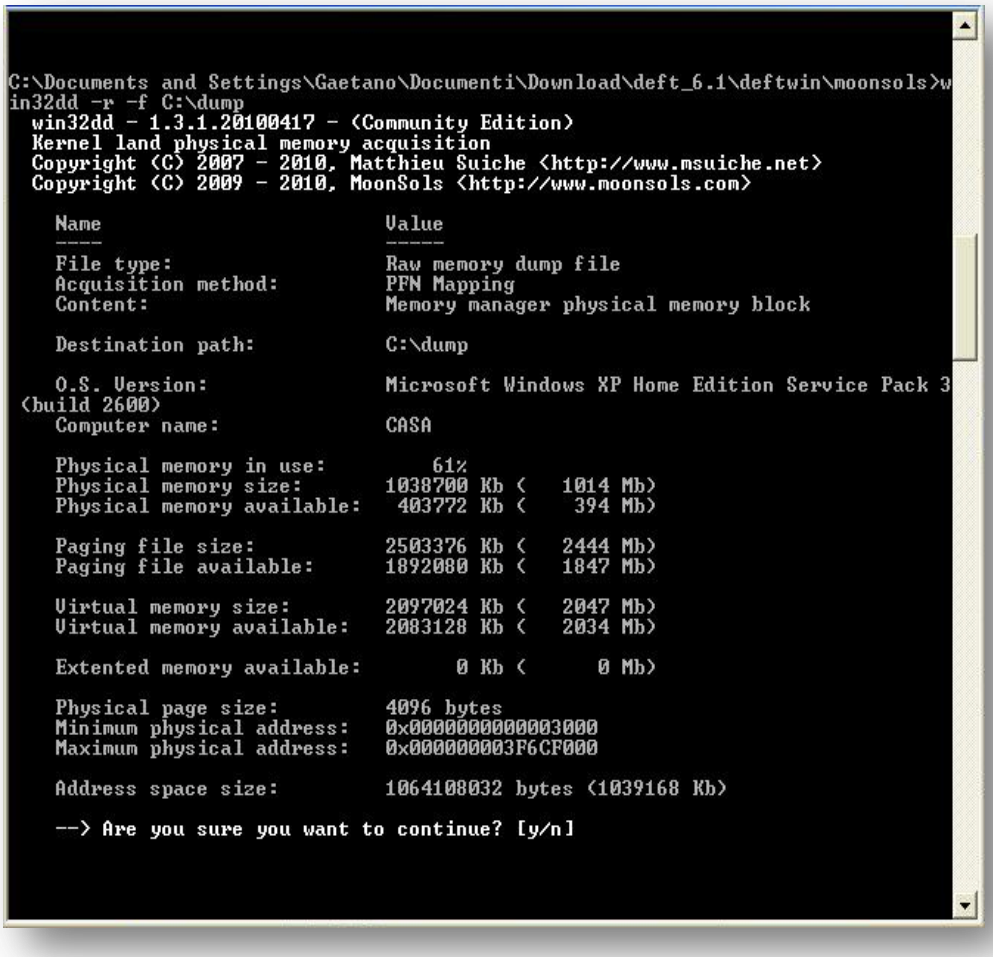


La figura precedente mostra quali tipi di dump possono essere effettuati da quali tool. Windows consente il Crash dump solo alla comparsa della famosa schermata blu e crea l'hibernation file quando si sceglie di ibernare il pc. Win32dd consente invece il dump di tipo Raw e il dump di tipo Crash, mentre gli altri tool consentono solo il dump di tipo Raw.

Il primo tool che mostriamo è Win32dd. E' un tool da linea di comando che come già detto permette dump di tipo Raw e di tipo Crash. Il tool ha le seguenti opzioni:

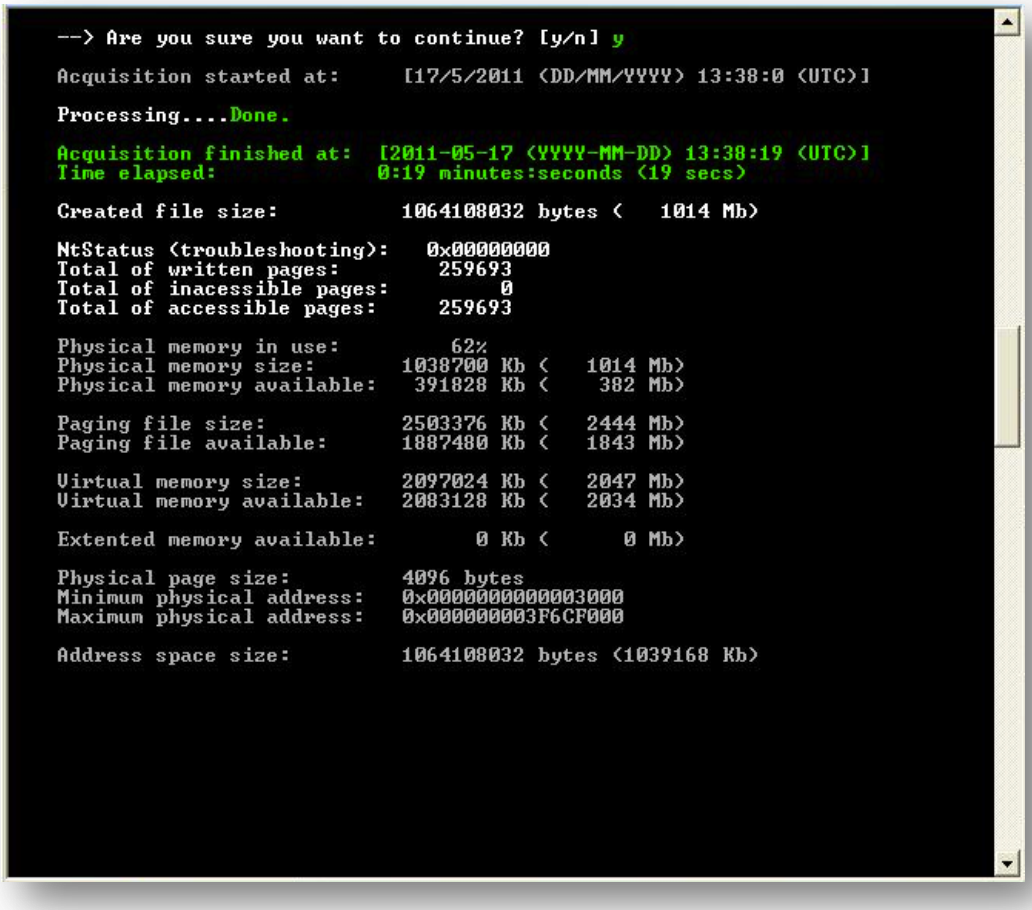
- -f <filename> *File di output*
- -r *Raw dump (default)*
- -d *Crash dump*
- -s <value> *Funzione Hash*
  - 0 Nessun algoritmo
  - 1 SHA1
  - 2 MD5
  - 3 SHA-256

Nella figura sottostante viene richiesto un dump di tipo raw che viene memorizzato all'interno del file di nome *dump* nella cartella C:\. Prima di chiedere la conferma ci vengono mostrati alcuni dati: il tipo di dump, il percorso del file di destinazione, la



percentuale di utilizzo della memoria etc..

Quando si vuole avviare il dump basta digitare "*y*" e premere <invio> e comparirà una schermata simile alla seguente.



Viene quindi mostrata la data d'inizio della procedura ed in verde la data di fine e quanto tempo è intercorso tra l'avvio e la terminazione. Vengono poi anche mostrate informazioni per avere un'idea sull'impatto che il tool ha avuto sulla memoria.

Il secondo tool che mostriamo è Winen, può essere eseguito o in maniera standalone oppure lo si può utilizzare all'interno di EnCase. Anch'esso è un tool da linea di comando e si può utilizzare nel seguente modo:

- winen <-f nome_file_conf>

Senza l'opzione -f il programma chiederà le credenziali del caso (esaminatore, path dell'evidenza, numero del caso, livello di compressione, nome dell'evidenza, numero del caso, etc.), in caso contrario si può utilizzare un file formattato in maniera simile alla

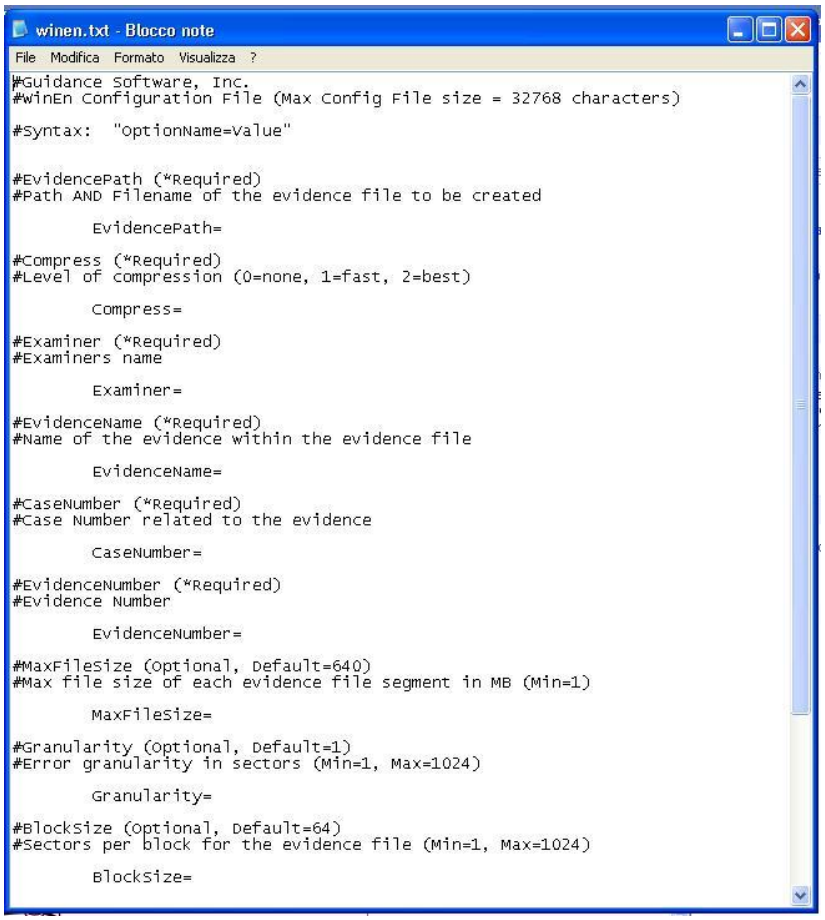
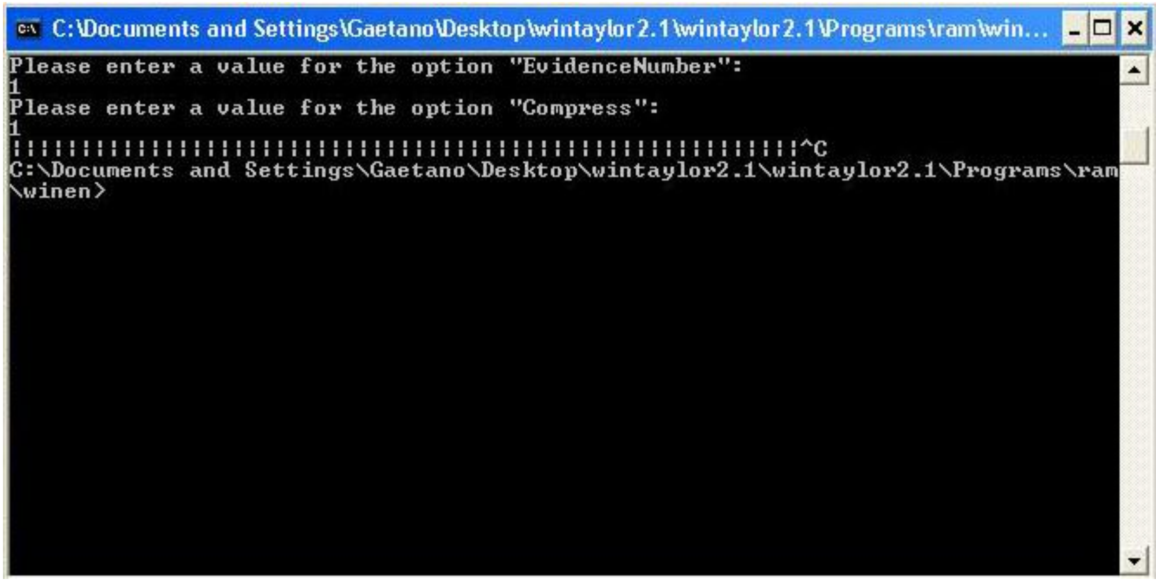


figura sottostante.

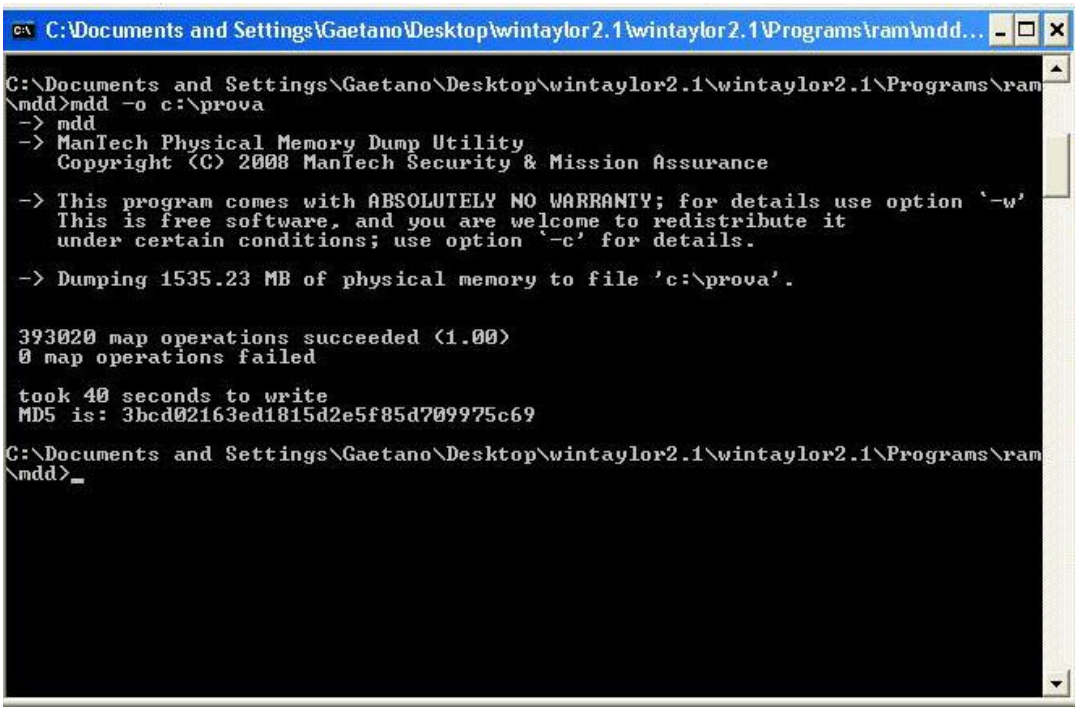
Un esempio di esecuzione del programma è mostrato di seguito.



Il programma stesso chiede all'utente di immettere almeno i parametri richesti. Verrà salvato un file con estensione .e01 leggibile tramite EnCase.

Altro tool è MemoryDD, è sempre un tool da linea di comando, ma non è più in sviluppo. MDD ricalca un po' le caratteristiche dei precedenti tool visti e il suo utilizzo è:

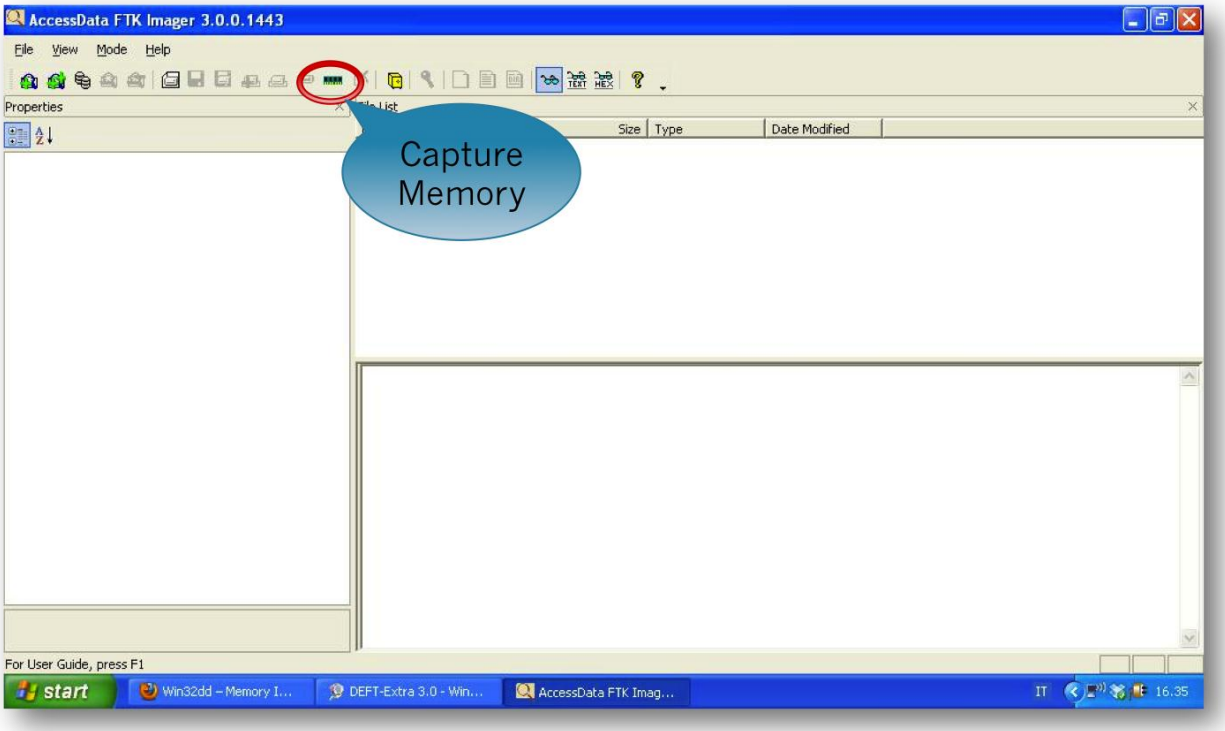
- mdd <opzioni>
    - -o *filename* – richiesto
    - -w – informazioni di licenza
    - -v – verbose



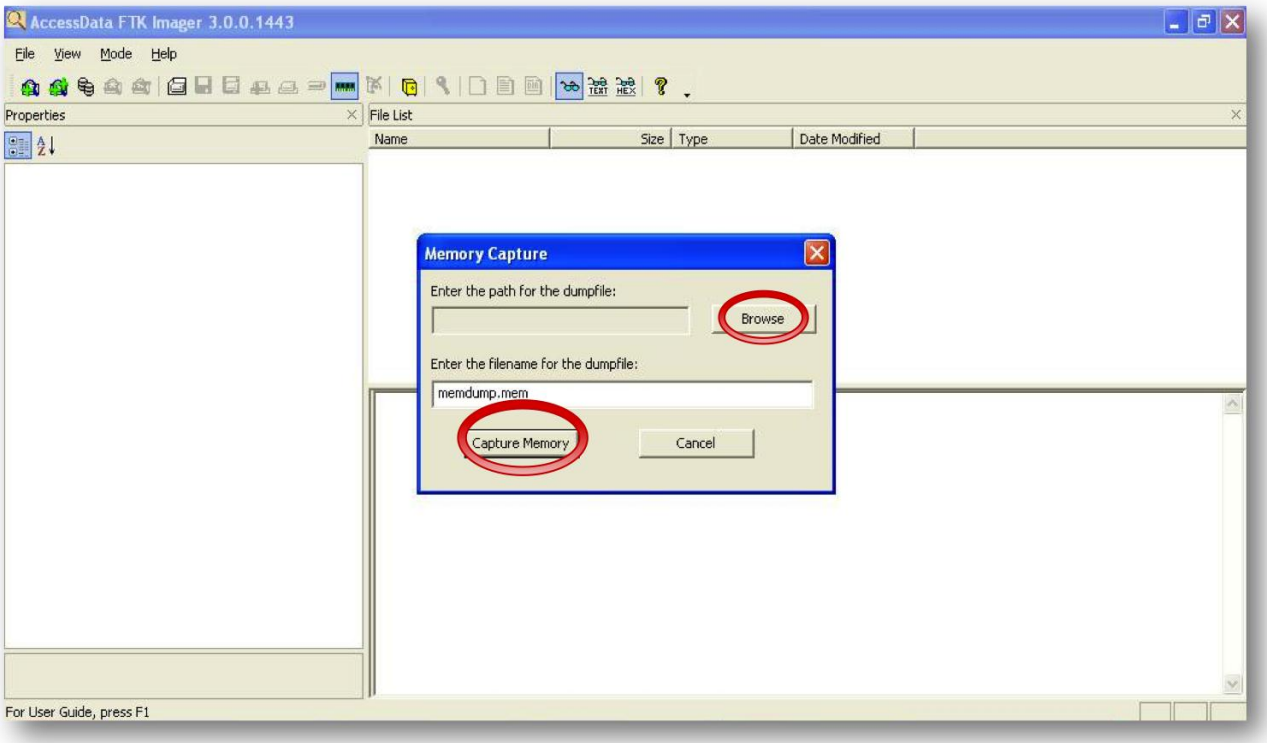
Nell'esempio mostrato nella figura precedente il tool è stato istruito definendo solo il path del file di output cioè *C:|prova*. Al termine della sua esecuzione il programma mostra la dimensione del dump, il numero di operazioni fallite, quanti secondi ha impiegato e l'MD5 del dump.

FTKImager (http://accessdata.com/support/adownloads#FTKImager) è un tool che verrà mostrato in questo paragrafo per quanto riguarda la creazione del dump, e nel prossimo paragrafo per l'analisi del dump. FTKImager è stato sviluppato dalla AccessData ed è alla versione 3.4.1 rilasciata il 24 Agosto 2011. Esso è un tool che permette di effettuare anche dump di memorie di massa quindi hard disk, floppy, CD e DVD. Inoltre consente di mostrare i contenuti di dischi locali e di periferiche locali con storage.

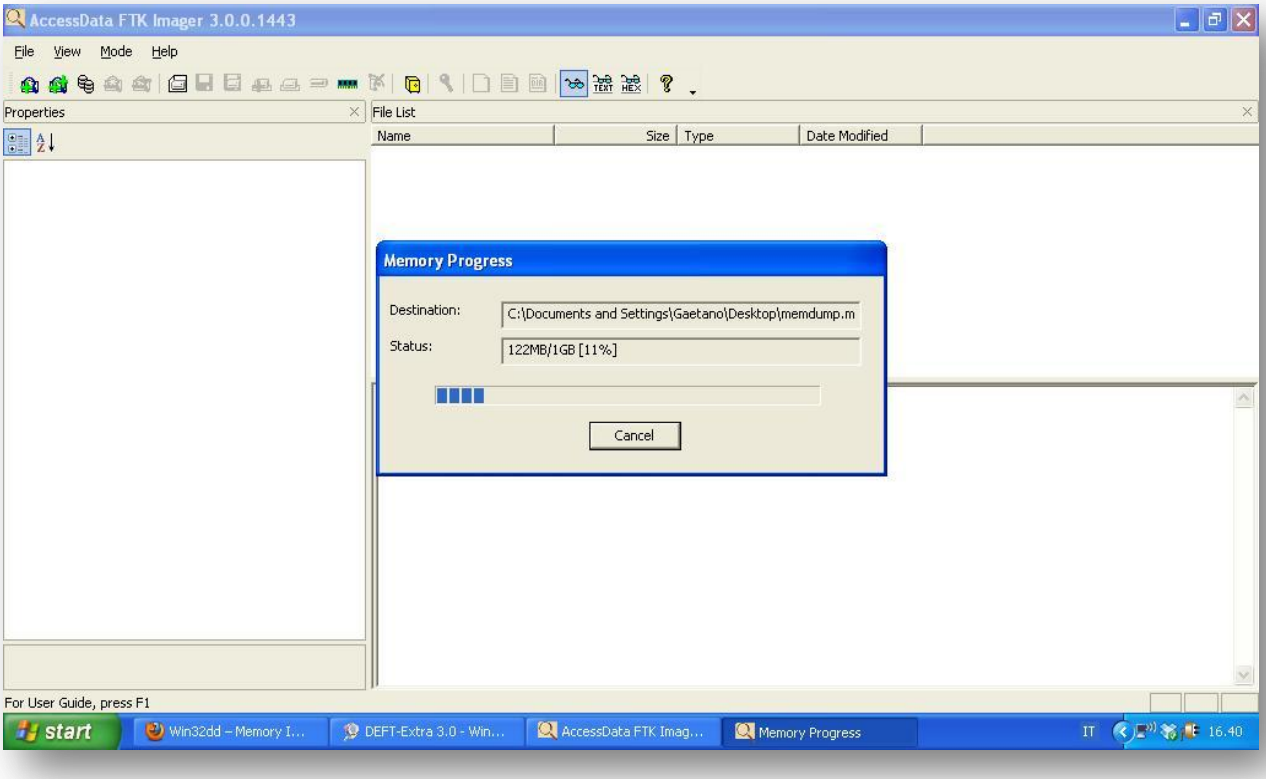
Una volta avviato il tool comparirà una schermata simile alla seguente.



Per effettuare il dump della RAM bisogna cliccare su Capture Memory come mostrato nella figura precedente. Compare quindi una schermata simile alla figura sottostante.



Bisogna settare il path del file e ciò viene fatto cliccando su *Browse,* poi è possibile nominare il file a nostro piacimento nella casella sotto al pulsante *Browse*, ed infine è



possibile avviare la creazione del dump cliccando su *Capture Memory*. E durante la procedura verrà mostrata una schermata di progresso.

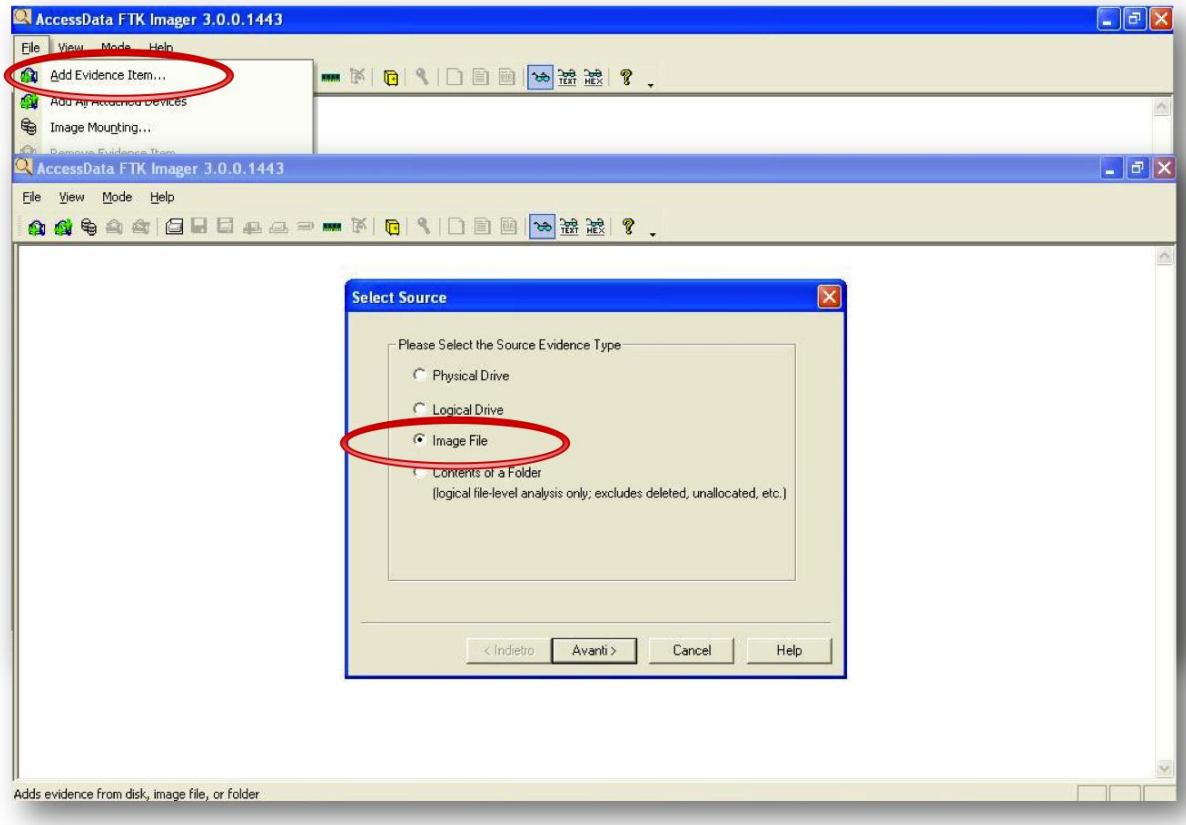
Di seguito è mostrata una tabella riassuntiva delle caratteristiche dei diversi tool messe a confronto.

	Win32dd	Winen	MDD	FTKImager
Acquisizione/Analisi	Solo Acquisizione	Solo Acquisizione	Solo Acquisizione	Entrambe
Tipo dump	Crash e RAW	RAW	RAW	RAW
GUI/Shell	Shell	Shell	Shell	GUI
Dettagli sul caso	NO	SI	NO	NO

Dettagli sul caso (vd. Winen in 4.2): esaminatore, Id dell'evidenza, tipo di compressione, etc.

4.3. Analisi RAM

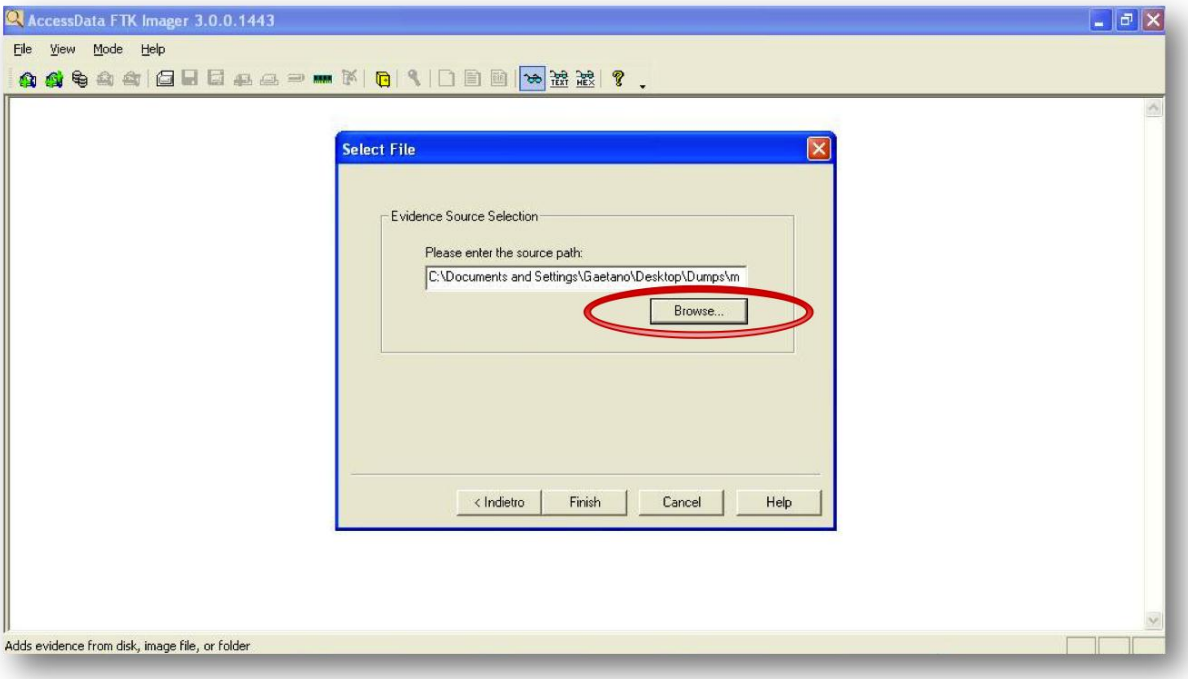
L'analisi del dump viene effettuata con FTKImager. Il fattore positivo di questo tool sta nel fatto che è possibile fare l'analisi anche di dump creati da Win32dd e MemoryDD; Winen ha un formato proprietario e quindi è possibile analizzare il dump solo utilizzando EnCase. Abbiamo mostrato nel paragrafo precedente quali azioni bisognava compiere per effettuare un dump della RAM con FTKImager, ora mostriamo come aprire il dump creato in precedenza.



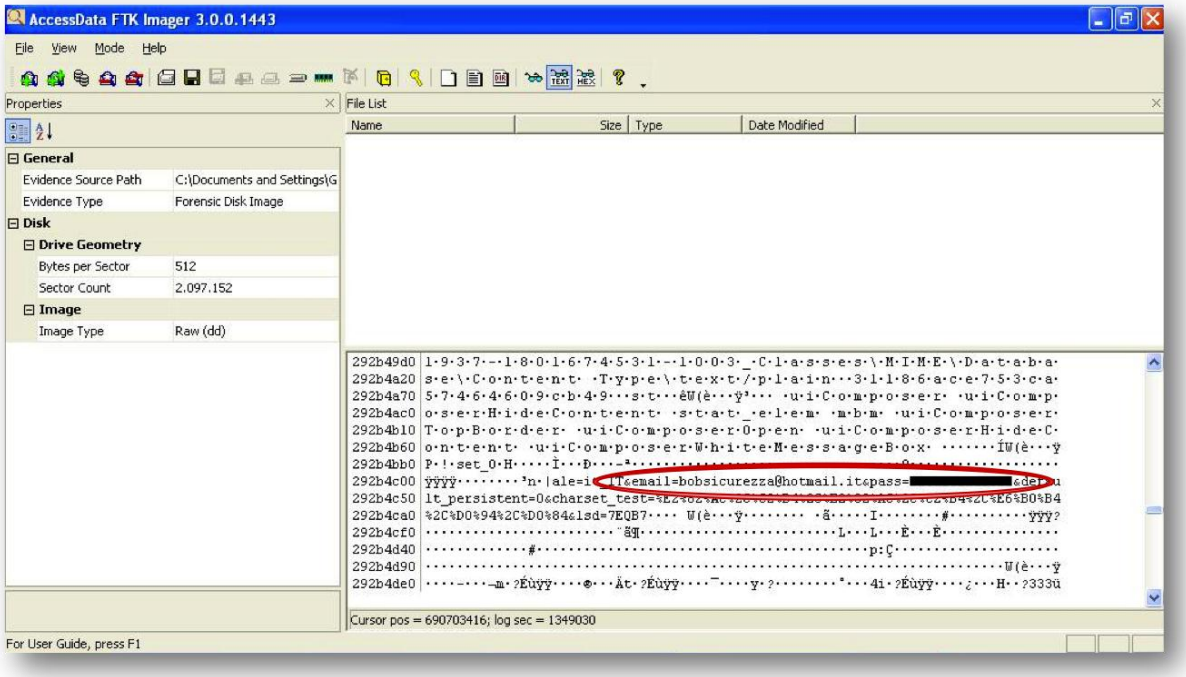
Cliccando su *File* si aprirà il menù a tendina mostrato nell'immagine precedente. Bisogna cliccare poi su *Add Evidence Item* che è la voce che permette di caricare un qualsiasi tipo di dump. Una volta cliccatoci su ci apparirà una schermata simile all'immagine successiva.

Selezionare poi *Image File* per istruire FTKImager ad aprire un file di tipo immagine. Le altre opzioni servono se non è stato effettuato un dump, in particolare: *Physical Drive* viene selezionato per analizzare un drive senza considerare con quale partizione è formattato, *Logical Drive* viene selezionato per analizzare un drive attraverso la partizione, *Contents of a Folder* viene selezionato per avere un'analisi di una cartella

presente su qualche memoria di massa connessa al pc.



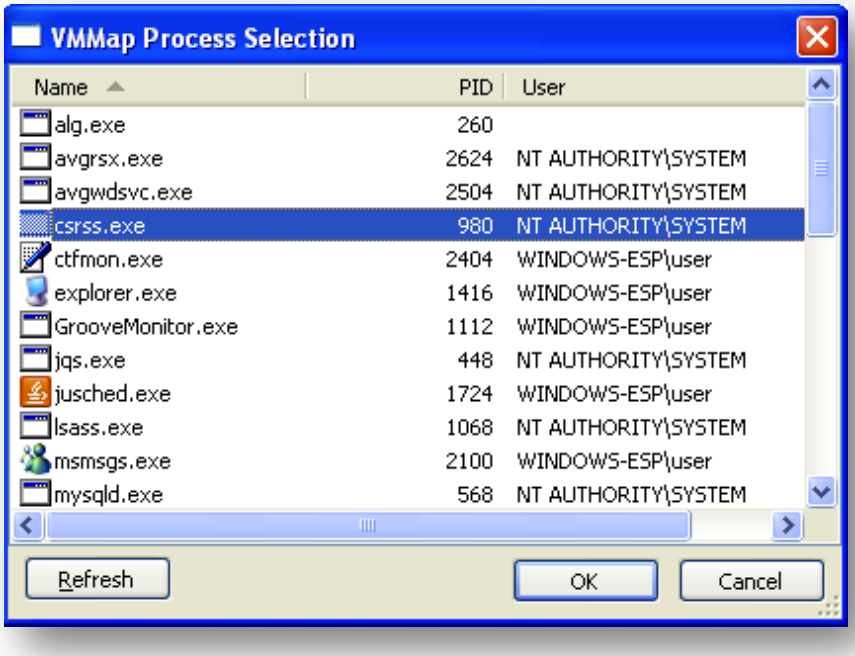
L'immagine precedente mostra che FTKImager richiede il path dove salvare il dump della memoria, il pulsante *Browse* ci semplifica la vita e permette all'utente di selezionare il file muovendosi tra le cartelle. Infine cliccando su Finish si termina la procedura e comparirà una schermata simile alla seguente.



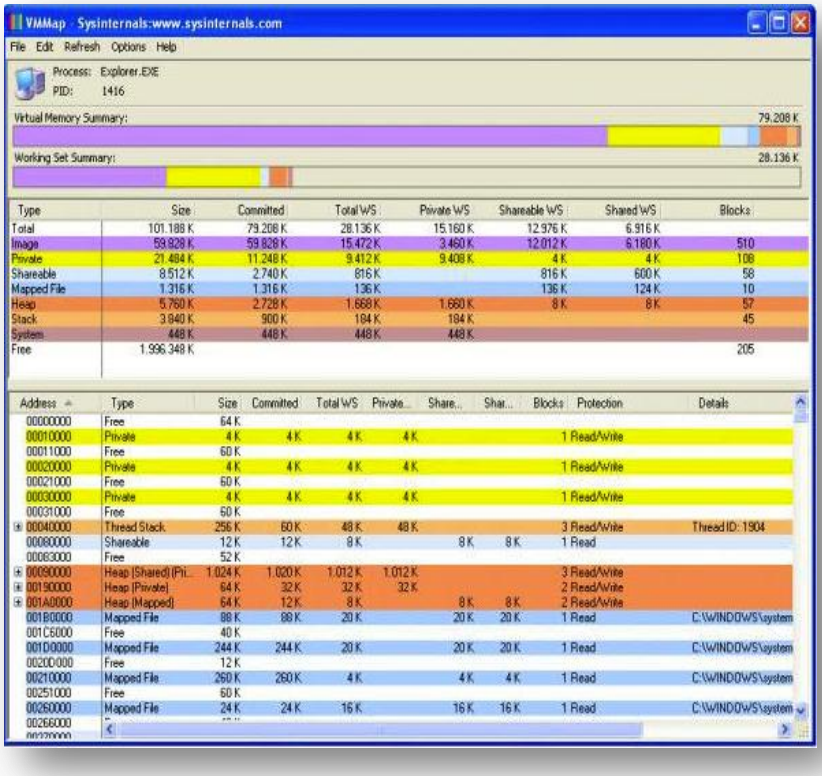
Ci viene mostrato il contenuto del file e la locazione di memoria corrispondente. E' possibile cercare una parola utilizzando *Ctrl+f* tramite il quale ci comparirà una finestra che richiede la parola da cercare.

4.4. Processi in esecuzione

Per quanto riguarda il monitoraggio dei processi in esecuzione abbiamo esaminato due tool. Il primo è VmMap che è un programma che mostra quale processo utilizza quale porzione di memoria. Oltre a rappresentazioni grafiche di utilizzo della memoria, VMMap mostra anche le informazioni di riepilogo e una mappa dettagliata della memoria gestita da un determinato processo. All'apertura del programma ci viene chiesto di selezionare il processo da analizzare (vedi figura successiva).



Una volta selezionato il processo e premuto *OK*, ci comparirà una schermata come quella mostrata nell'immagine seguente.



La prima parte mostra per ogni tipo di zona quanta memoria occupa il processo, mentre nella seconda parte viene mostrato qual è il tipo di memoria associato ad un determinato indirizzo e quanto è grande la suddetta zona.

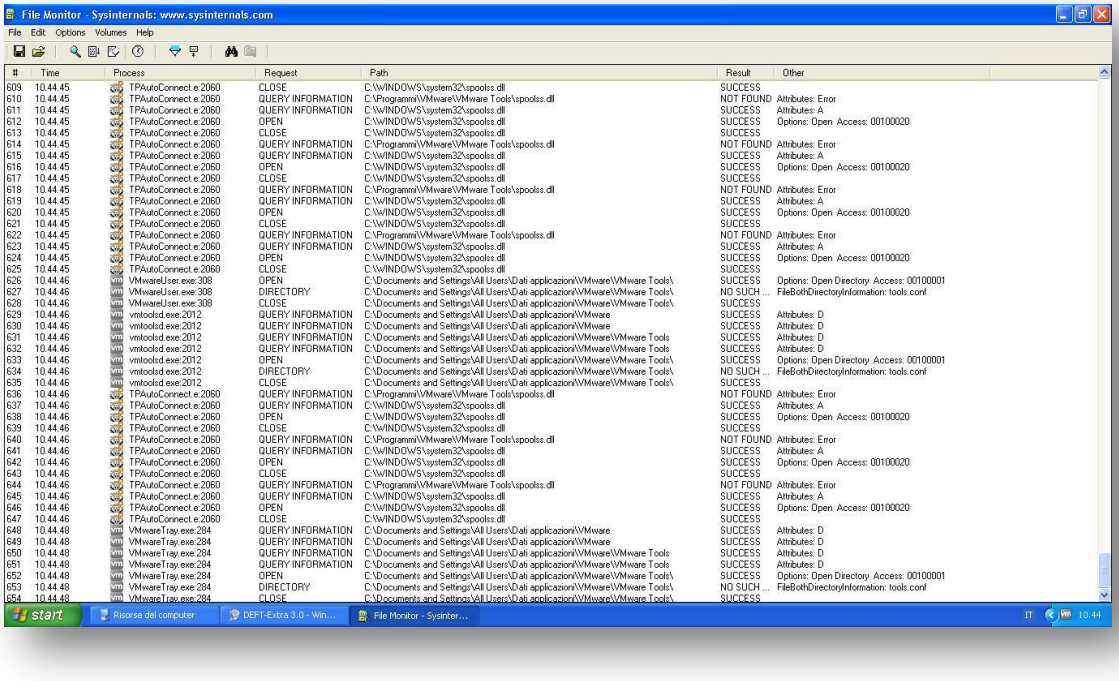
I tipi di zona sono:

- Image
  - Indica il codice da eseguire
- Private
  - Indica la porzione di memoria che non può essere condivisa con altri processi
- Shareable
  - Indica la porzione di memoria condivisa con altri processi
- Mapped File
  - Indica la porzione di memoria contenente i path dei file in esecuzione
- Heap
  - Indica la porzione di memoria gestita dal processo

- Stack
    - Indica la porzione di memoria che contiene i parametri delle funzioni invocate
- System
    - Indica la porzione di memoria relativa al processo che viene gestita dal sistema operativo

L'altro tool che mostriamo è FileMonitor che si occupa di visualizzare attività di sistema in tempo reale e di vedere come i processi utilizzano i file e le DLL. FileMonitor mostra infatti esattamente quando ogni processo apre, legge, scrive o elimina un determinato file.

L'interfaccia è mostrata nella figura sequente.

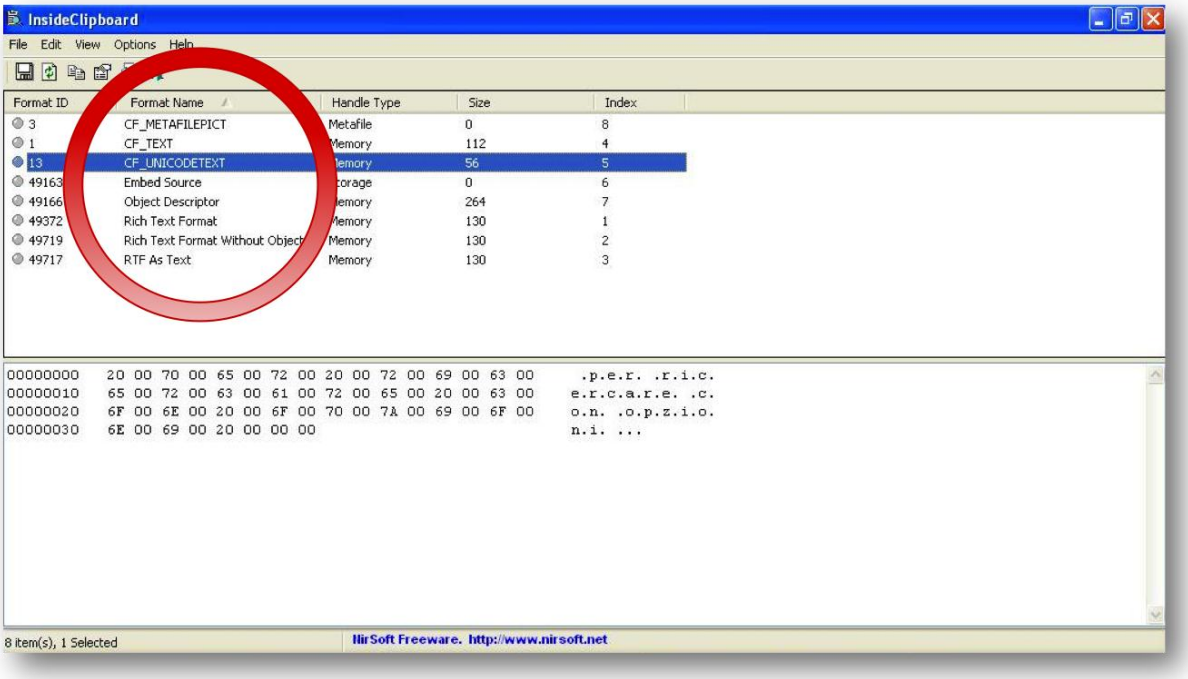


Nella prima colonna è mostrato un ID, nella seconda è mostrato il timestamp, nella terza il nome del processo, nella quarta il tipo di azione, nella quinta il path del file che riceve l'azione, nella sesta se l'azione ha successo o meno e nella settima altre informazioni aggiuntive.

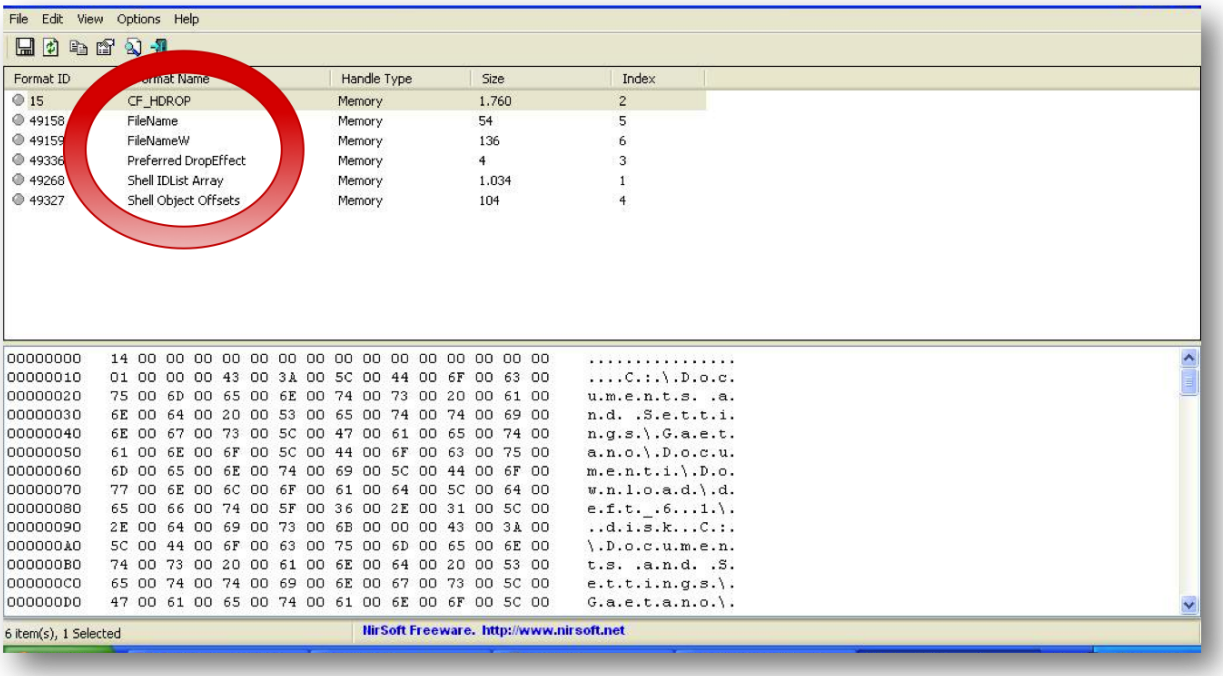
4.5. Clipboard

Per l'analisi della clipboard (ciò che rimane memorizzato quando si effettua un'azione di tipo *taglia* o *copia*) abbiamo utilizzato un tool della Nirsoft chiamato InsideClipboard. Questo tool permette di visualizzare ciò che è contenuto nella clipboard sotto formato binario e consente anche di salvare il suddetto contenuto in un file.

Per quanto riguarda la copia di un testo l'immagine sottostante mostra un esempio di tale visualizzazione.



Per quanto riguarda la copia di un file all'interno della clipboard viene inserito solo il percorso del file copiato. Possiamo vedere un esempio nell'immagine sottostante.



Caso di studio

5. Caso di studio

5.1. Obiettivi

L'obiettivo che ci siamo preposti è quello di utilizzare i tool mostrati nel capitolo precedente per individuare eventuali evidenze digitali presenti nella RAM. In particolare abbiamo focalizzato la nostra attenzione sulla ricerca di evidenze relative ai seguenti servizi:

- Facebook
- Windows Live Messenger
- Windows Hotmail (Webmail)
- Skype
- Gmail

La scelta è ricaduta su questi servizi perché sono alcuni dei servizi che presentano un largo utilizzo. In particolare la webmail è stata scelta perché ad oggi è un modo sicuro di scambiare informazioni salvandole come bozza, in questo modo non vi è nessuno invio di dati sulla rete e nessun dato presente sulla macchina dalla quale viene effettuato l'accesso alla webmail.

5.2. Ambiente di lavoro

Per la realizzazione del progetto abbiamo analizzato le diverse distribuzioni in particolare abbiamo fatto uso dei tool per l'analisi live (visti nei capitoli precedenti). Come sistema di test abbiamo creato due macchine virtuali utilizzando il software Vmware Player, con le seguenti caratteristiche:

Macchina 1

- Sistema Operativo: Windows Xp Professional Service Pack 3
- Ram: 1GB

Macchina 2

- Sistema Operativo: Windows 7 Professional
- Ram: 1GB

Su entrambi i sistemi sono stati installati i seguenti software:

- Skype 5.3.0.111
- Windows Live Messenger – versione 2009 (Build 14.0.8117.416)
- Internet Explorer 8.0.6001.18702IC
- Chrome 11.0.696.60

Inoltre abbiamo creato gli account per i vari servizi, in particolare:

- 2 Account Hotmail
  - alicesicurezza@hotmail.it
  - bobsicurezza@hotmail.it
- 2 Account Facebook
  - Alice Sicurezza
  - Bob Sicurezza
- 2 Account Skype
  - alice.sicurezza
  - bob.sicurezza
- 1 Account Gmail
  - alicesicurezza@gmail.com

per quanto riguarda Windows Live Messenger sono stati usati gli account di Hotmail.

Per l'acquisizione e l'analisi dei dump abbiamo utilizzato il software FTKImager contenuto in DEFT Extra, la scelta è ricaduta su quest'ultimo in quanto permette di effettuare sia l'acquisizione che la successiva analisi del dump.

5.3. Risultati

Il lavoro svolto è stato suddiviso nelle seguenti fasi:

1. Avvio della macchina virtuale
2. Utilizzo del servizio da analizzare
3. Acquisizione del dump
4. Analisi del dump

Abbiamo eseguito le fasi precedentemente descritte sia per la Macchina 1 che per la Macchina 2 ed i risultati descritti dal paragrafo 5.3.1 al 5.3.5 sono identici per entrambe le macchine. Il test descritto nel paragrafo 5.3.6 è stato invece effettuato solo sulla Macchina 1 in quanto l'obiettivo era quello di testare la permanenza in RAM delle evidenze. Nel paragrafo 5.3.7 abbiamo eseguito il test descritto nel paragrafo 5.3.1 usando però il browser Chrome. Nel paragrafo 5.3.8 descriviamo il risultato della ricerca che abbiamo effettuato riguardo l'acquisizione della RAM video. Nel paragrafo 5.3.9 abbiamo effettuato il test descritto nel paragrafo 5.3.1 utilizzando Chrome in modalità incognito.

5.3.1. Facebook

Abbiamo avviato il browser Internet Explorer 8, ci siamo collegati al sito www.facebook.it e abbiamo effettuato l'accesso con l'account bobsicurezza@hotmail.it e successivamente abbiamo postato un messaggio in bacheca e usato la chat effettuando la seguente conversazione:

Bob: Ciao alice

Alice: ciao bob ☺

Bob: come stai ?

Alice: bene te?

Bob: benvenuto su Facebook

Alice: grazie mille :D

Abbiamo poi effettuato il logout e chiuso il browser e a questo punto abbiamo eseguito FTKImager avviando la procedura di acquisizione del dump.

Successivamente abbiamo analizzato il dump alla ricerca delle evidenze digitali e abbiamo trovato i dati di accesso (nome utente e password) e anche evidenze relative alla conversazione effettuata usando la chat di Facebook.

5.3.2. Windows Live Messenger

Abbiamo avviato Windows Live Messenger ed effettuato il login con l'account bobsicurezza@hotmail.it e successivamente abbiamo aggiunto all'elenco degli amici l'account alicesicurezza@hotmail.it collegato contemporaneamente ma su di un altro computer. Quindi abbiamo effettuato la seguente conversazione:

Bob: Ciao Alice

Alice: Ciao bob

Come stai?

da quanto tempo

Bob: Tutto bene stato preparando l'esame di Sicurezza!

Bob: invia il file Tramonto.jpg

Terminata la conversazione abbiamo effettuato il logout e iniziato l'acquisizione del dump.

Dall'analisi del dump possiamo dire che le credenziali di accesso non sono presenti questo è dovuto al fatto che dopo il rilascio di MSN 6, è stato introdotto il nuovo protocollo **MSNP9** [7], che utilizza l'HTTP Secure Socket Layer per negoziare un'autenticazione sicura, al contrario di quanto avveniva prima, quando, cioè,

l'autenticazione veniva effettuata semplicemente in *plain text.* Per quanto riguarda la conversazione essa appare nel dump nella sua interezza.

5.3.3. Skype

Abbiamo avviato Skype, effettuato il login con l'account bob.sicurezza e abbiamo aggiungo all'elenco dei contatti alice.sicurezza. Quindi abbiamo effettuato una conversazione fittizia tra i due account utilizzando la chat di Skype e successivamente dall'account bob.sicurezza abbiamo inviato una richiesta di chiamata, la durata della chiamata è stata di 12 secondi.

Dall'analisi del dump non è possibile risalire alle credenziali dell'account e non vi è traccia della conversazione. Questo perché Skype usa algoritmi di crittografia, sono emerse però tracce relative alla chiamata effettuata in particolare è possibile risalire al chiamante e alla durata della conversazione.

5.3.4. Hotmail

Abbiamo avviato il browser Internet Explorer 8, ci siamo collegati al sito www.hotmail.it e siamo stati riportati sul sito:

> https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=11&ct=1308921997&rver=6.1.6206.0&wp=MBI&wreply=http:%2F%2Fmail.live.com%2Fdefault.aspx&lc=1040&id=64855&mkt=it-it&cbcxt=mai&snsc=1

abbiamo effettuato l'accesso con l'account bobsicurezza@hotmail.it e abbiamo scritto un messaggio di posta salvandolo poi nelle bozze. Effettuato il logout dalla webmail e una volta chiuso il browser abbiamo avviato l'acquisizione del dump.

Dall'analisi del dump sono emerse evidenze relative alle credenziali di accesso alla webmail e relative al messaggio salvato nelle bozze.

5.3.5. Gmail

Abbiamo avviato il browser Internet Explorer 8, ci siamo collegati al sito

https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=http%3A%2F%2Fmail.google.com%2Fmail%2F%3Fhl%3Dit%26tab%3Dwm%26ui%3Dhtml%26zy%3Dl&bsv=llya694le36z&scc=1&ltmpl=default&ltmplcache=2&hl=it&from=login

Abbiamo effettuato l'accesso con l'account alicesicurezza@gmail.com e abbiamo scritto un messaggio di posta salvandolo poi nelle bozze. Effettuato il logout dalla webmail e una volta chiuso il browser abbiamo avviato l'acquisizione del dump. Dall'analisi del dump non sono emerse le evidenze relative alle credenziali di accesso ma sono emerse le evidenze relative al messaggio salvato nelle bozze.

5.3.6 Test durabilità dei dati

Abbiamo riprodotto quanto descritto nel paragrafo 5.3.1 e constatato la presenza delle evidenze, successivamente abbiamo avviato il gioco Neverwinter Nights 2 ed effettuato una sessione di 30 minuti di gioco. Dopo la sessione di gioco abbiamo rieseguito l'acquisizione del dump riscontrando la non presenza delle evidenze precedentemente acquisite. Neverwinter Nights 2 è stato scelto per i requisiti hardware consigliati nello specifico per la dimensione della RAM richiesta. Infatti la capacità della RAM della Macchina 1 e della Macchina 2 corrisponde alla quantità richiesta dai requisiti.

Requisiti hardware consigliati per Neverwinter Nights 2:

- Sistema operativo: Windows XP
- Processore: Intel Pentium 4 3.0 GHz / AMD Athlon 64 o superiori
- RAM: 1 GB
- Scheda video: compatibile Pixel Shader Model 2.0 con 128 MB di memoria dedicata
- Spazio su disco fisso: 5.5 GB liberi
- Versione DirectX: 9.0c o superiori

5.3.7 Chrome su Windows 7

Una differenza che abbiamo notato è che usando Windows 7 e il browser Chrome non siamo riusciti a individuare le credenziali di accesso a Facebook (vd. 5.3.1).

5.3.8 Acquisizione RAM Video

Abbiamo effettuato delle ricerche che non hanno avuto esito positivo in quanto non siamo riusciti a trovare alcuna informazione e alcun software che permettesse l'acquisizione della memoria video.

5.3.9 Chrome in modalità Incognito

Abbiamo eseguito il test su Facebook (vd. 5.3.1) utilizzando Chrome in modalità incognito (modalità nella quale il browser non registra la cronologia di navigazione o di ricerca, e non lascia traccia sul computer, ad esempio sotto forma di cookie, una volta chiusa la finestra) e sono comunque emerse le evidenze riscontrate su Internet Explorer. Il test è stato effettuato solo sulla Macchina 1 in quanto come mostrato nel paragrafo 5.3.7 utilizzando Chrome sulla Macchina 2 (Windows 7) le evidenze non sono emerse.

5.4. Metodologie di Ricerca

I risultati mostrati nel paragrafo precedente sono stati individuati perché ovviamente conoscevamo le informazioni da cercare. In questo paragrafo descriveremo delle metodologie di ricerca per i vari servizi, laddove possibile, per estrapolare le evidenze digitali se presenti.

5.4.1. Facebook

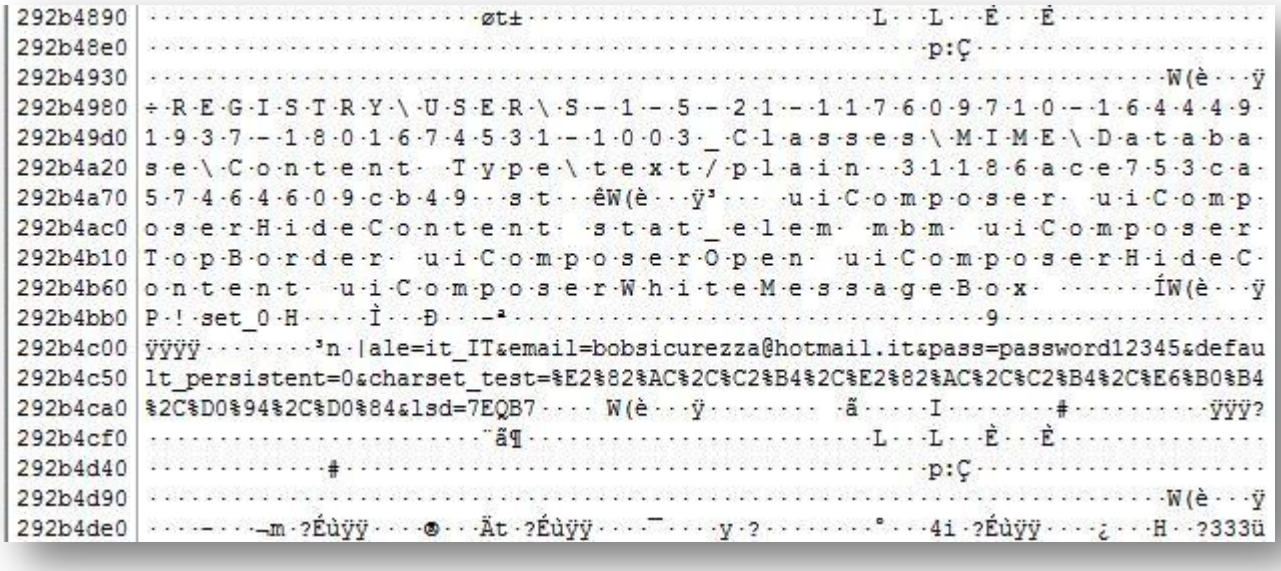


Figura 1

Dalla Figura 1 è possibile notare che le credenziali appaiono in una forma ben definita:

email=nomeutente&pass=password

è possibile quindi cercare la stringa testuale “email=” oppure “&pass=” e nel caso le evidenze sono presenti esse verranno individuate.

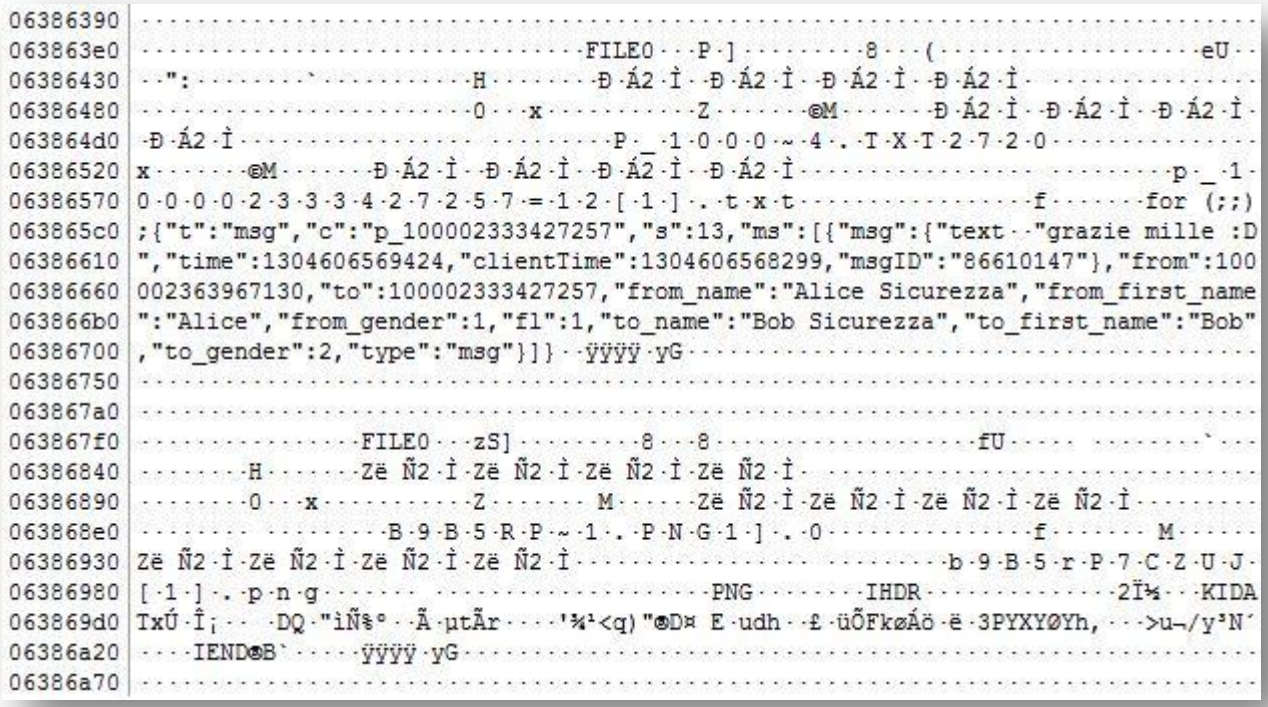


Figura 2

In figura 2 invece è possibile notale la presenza di parti del messaggio che anche in questo caso hanno una forma ben definita, per questo è possibile ricercare la stringa

[{"msg":{"text"

5.4.2. Windows Live Messenger

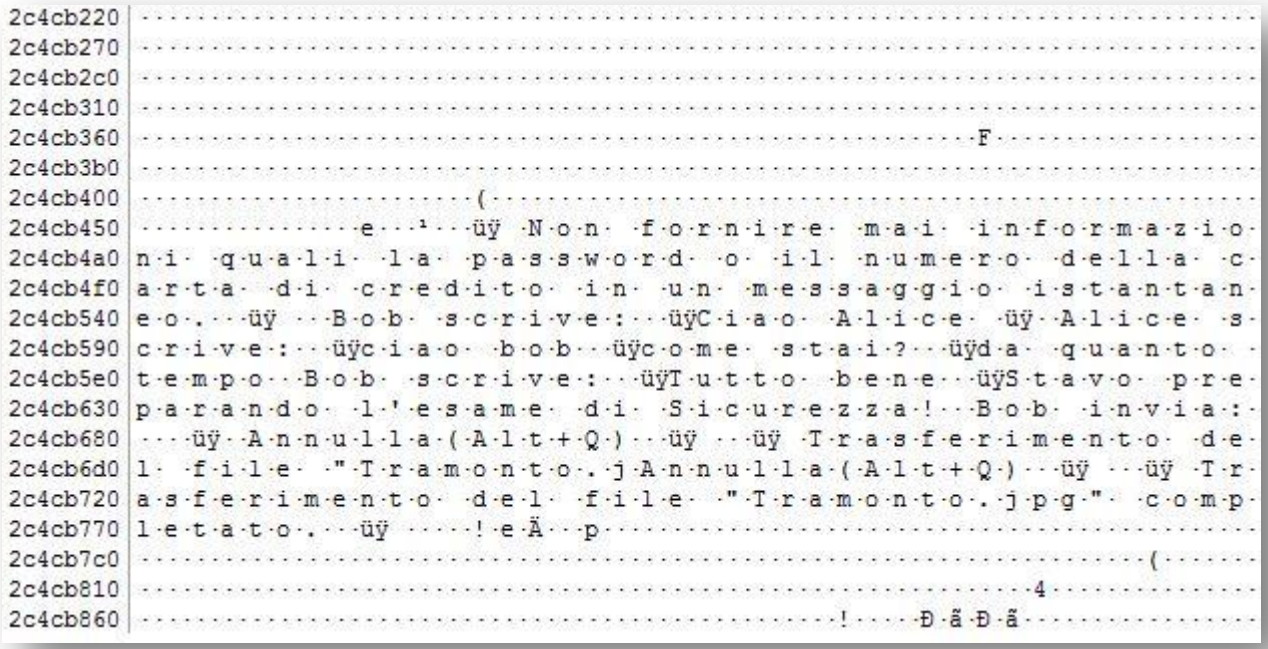


Figura 3

La figura 3 mostra il contenuto della conversazione effettuata utilizzando il client Windows Live Messenger. La conversazione è presente in modo chiaro ma non è strutturata in modo preciso. E' possibile ricercare la stringa

scrive:

per poter risalire alle evidenze della conversazione nel caso esistano.

5.4.3. Skype

Figura 4

Come si può vedere nella figura 4 le informazioni relative alla chiamata effettuata su Skype son ben visibili e strutturate. Per ricercare eventuali evidenze basterà cercare la stringa

<part identity= oppure <duration>.

Inoltre alla stringa "<part Identity=" è seguito l'account del chiamante.

5.4.4. Hotmail

Figura 5

Nella figura 5 si può notare che sono presenti le credenziali di accesso dell'account e sono ben strutturate, per ricercarle è infatti possibile ricercare la stringa

"login=" oppure "&passwd=".

Per quanto riguarda le bozze è possibile ricercare la stringa "bozze" in questo modo possiamo trovare la porzione della pagina web della webmail in cui è mostrato il numero di bozze (Figura 6), da qui possiamo quindi capire se ci sono delle bozze e in tal caso il numero di quest'ultime. Un altro modo è quello di ricercare la stringa "bozza salvata" che appunto indica che è stata salvata una bozza.

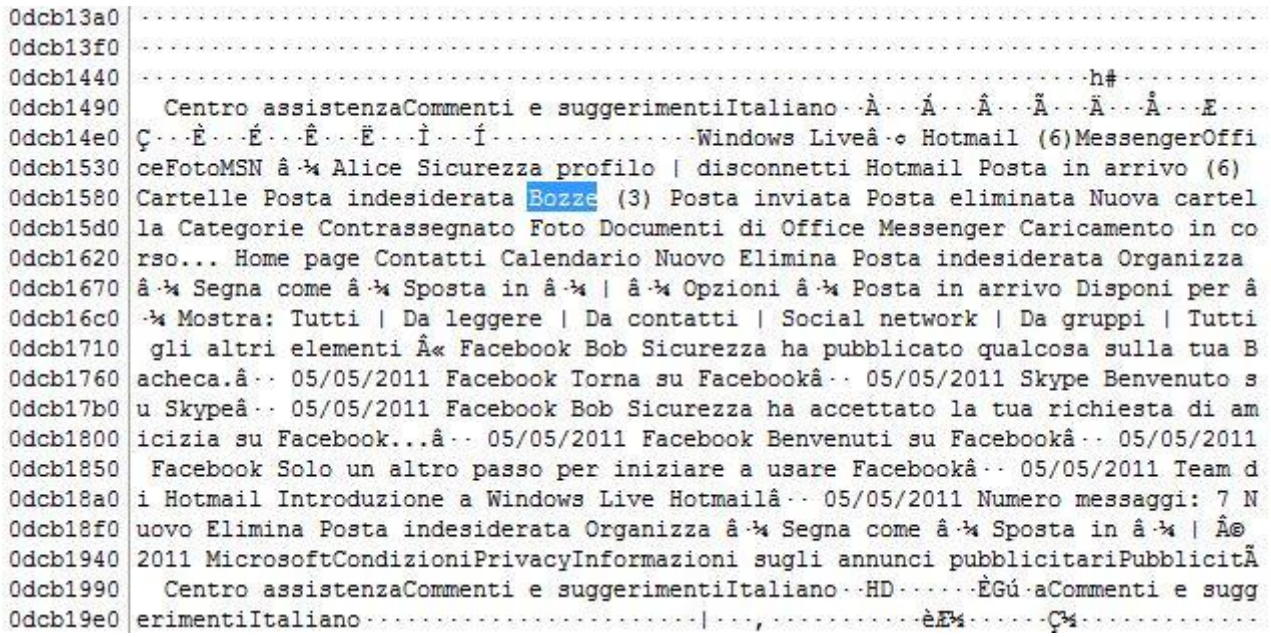


Figura 6

Quello che abbiamo notato è che quando salviamo una bozza senza inserire l'indirizzo del destinatario, cercando la stringa "(sconosciuto)" è possibile individuare la parte di pagina in cui sono presenti gli oggetti delle bozze (Figura 7)

Figura 7

Ricercando la stringa “class=ReadMsgSubject>” è possibile individuare il testo contenuto nel campo oggetto dell’email (Figura8). Cercando invece la stringa “class=ReadMsgBody” è possibile individuare il testo del messaggio (Figura 9).

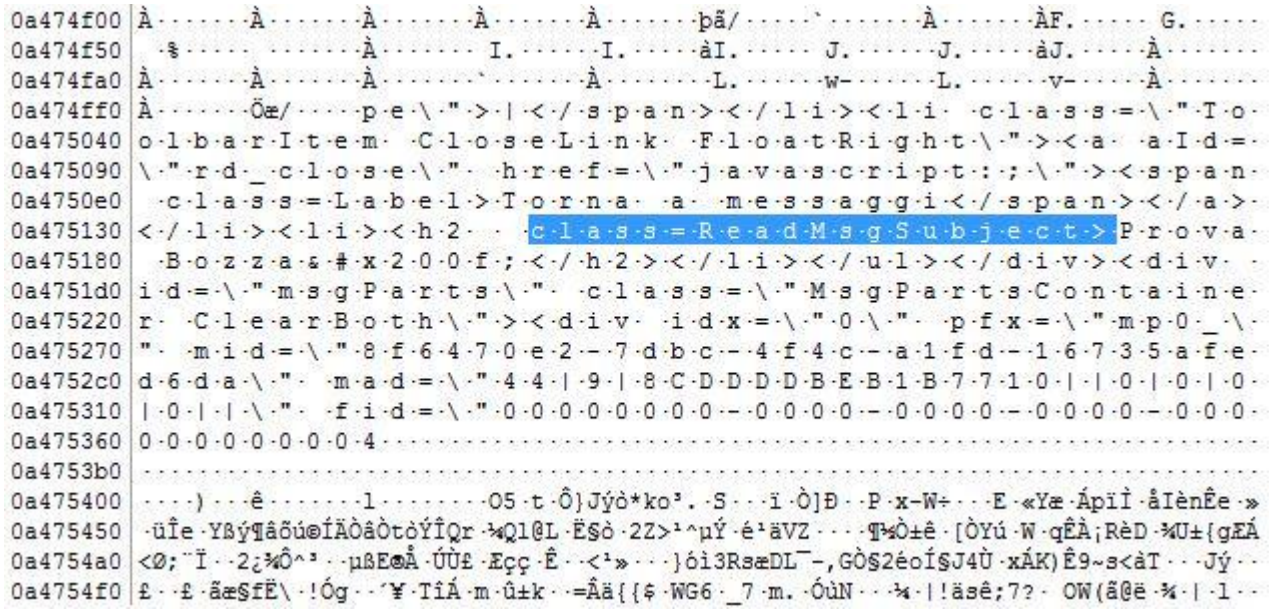


Figura 8

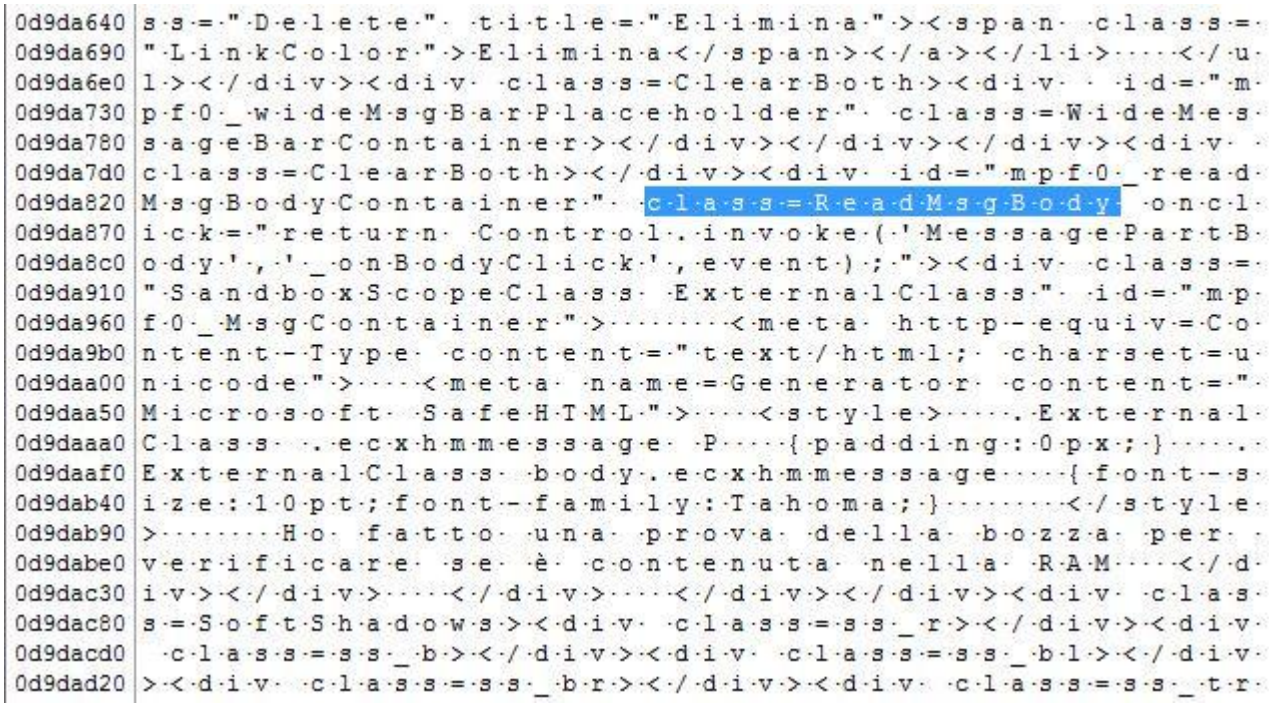


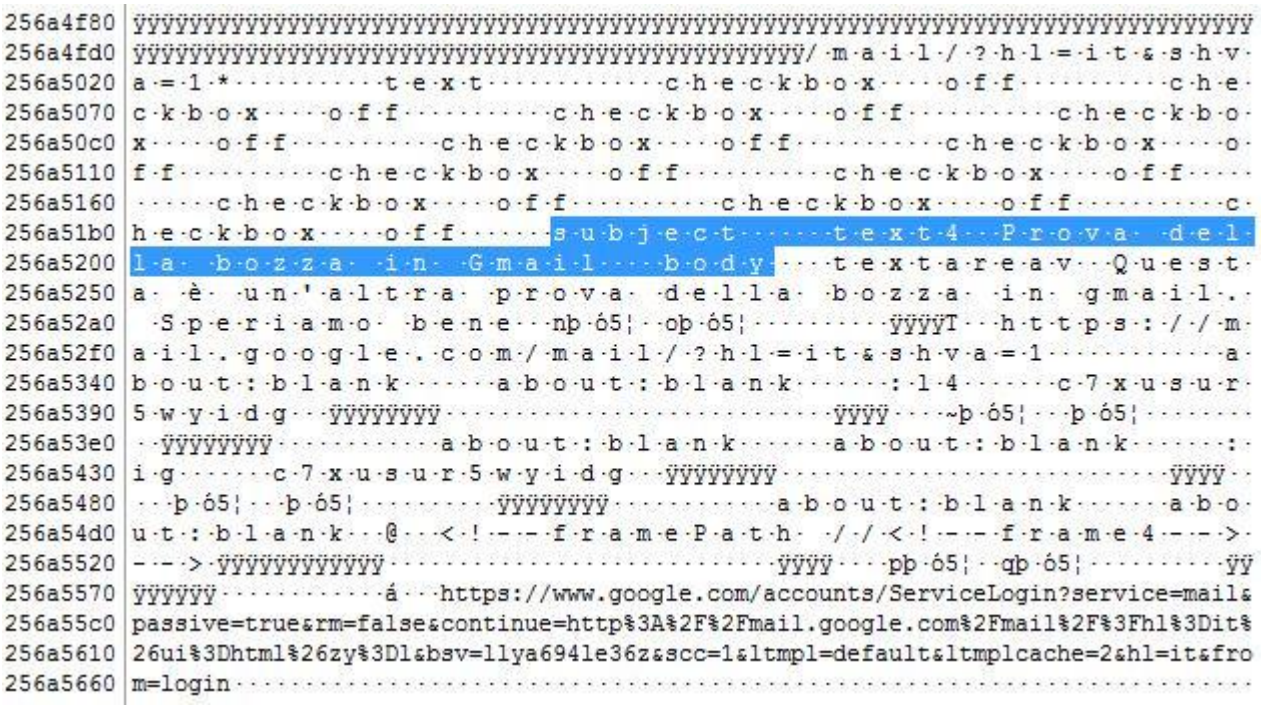
Figura 9

5.4.5. Gmail

In Gmail è possibile individuare il solo account di accesso e non la password, infatti cercando la stringa "@gmail.com" è possibile individuare l'account di accesso (Figura 10).

Figura 10

Per quanto riguarda il contenuto è possibile individuare sia l'oggetto che il corpo di una eventuale email salvata nelle bozze usando per la ricerca l'espressione regolare "subject.*body" (Figura 11).



5.5. Script Automatico

Abbiamo realizzato uno script bash per l'estrazione automatica delle evidenze, se presenti. Lo script ha due parametri:

1. Nome del file dump
2. Tipo di analisi:
    a. fb: evidenze relative a Facebook
    b. msn: evidenze relative a Windows Live Messanger, in questo caso viene richiesto un terzo parametro di tipo numerico che indica il numero di linee da considerare dopo la stringa "scrive:"
    c. wb: evidenze relative alla Webmail Hotmail
    d. sk: evidenze relative a Skype
    e. all: evidenze per tutti i servizi

Nel caso di Facebook lo script viene eseguito in questo modo

./analizzadump.sh <path dump> fb

l'output sarà presentato a video e nel caso lo si voglia su un file è possibile usare il comando di redirezione in questo modo

./analizzadump.sh <path dump> fb > fileout

In questo modo l'output sarà salvato nel file "fileout"

```
#!/bin/bash
#Utilizzo ./analizzadump.sh <path_dump>
if [ -z "$1" ]; then
        echo "usage: $0 <path_dump>"
        exit
fi

if [ "$2" = "fb" ]; then
     echo "Facebook:"
     echo "Chat:"
     strings -a --encoding=S "$1" | grep 'for (;;);{"t":"msg",.*time"'
     echo "Username & Password:"
     strings -a --encoding=S "$1" | grep 'email=.*pass=.*&'
     exit
fi
if [ "$2" = "msn" ]; then
     if [ -z "$3" ]; then
         echo "usage: $0 <path_dump> <# line after match>"
         exit
     fi
     echo "Msn:"
     strings -a --encoding=l "$1" | grep -E -A "$3" 'scrive:'
     exit
fi
if [ "$2" = "wb" ]; then
     echo "Webmail login & password:"
     grep -E --text -o 'login=.*&passwd=.*' "$1"
     exit
fi
if [ "$2" = "sk" ]; then
     echo "Skype:"
     strings -a --encoding=l memdumpSkype.mem | grep -E '<part
identity=.*</part>'
     exit
fi
if [ "$2" = "all" ]; then
     if [ -z "$3" ]; then
         echo "usage: $0 <path_dump> <# line after match>"
         exit
     fi
     echo "Facebook:"
     echo "Chat:"
     strings -a --encoding=S "$1" | grep 'for (;;);{"t":"msg",.*time"'
     echo "Username & Password:"
     strings -a --encoding=S "$1" | grep 'email=.*pass=.*&'
     echo
"*************************************************************************"
     echo "Msn:"
     strings -a --encoding=l "$1" | grep -E -A "$3" 'scrive:'
     echo
"*************************************************************************"
     echo "Webmail login & password:"
     grep -E --text -o 'login=.*&passwd=.*' "$1"
     echo
"*************************************************************************"
     echo "Skype:"
     strings -a --encoding=l "$1"  | grep -E '<part identity=.*</part>'
     exit
fi
```

Allegato

Tipo Tool	HELIX	CAINE	DEFT	Nome Tool	Descrizione
PasswordTool	x			Access PassView (accesspv)	Programma che visualizza in chiaro le password di Access
Sysinternal	x		x	AccessEnum	Programma che controlla le protezioni dei file, autorizzazioni e conferisce pieno controllo delle autorizzazioni sulle protezioni
Nirsoft	x			Adapter Watch(awatch)	Programma che visualizza informazioni sulle schede di rete
Utility		X		Advanced LAN Scanner	Programma che monitora i terminali connessi su una LAN
SysInfo	x			Agile Risk Management	Programma per il recupero di informazioni digitali
Nirsoft	x		x	AlternateStreamView	Utility che permette di effettuare scansioni su dischi NTFS
Nirsoft	x			Asterisk Logger (astlog)	Programma che svela password celate dietro asterischi
Sysinternal	x		x	autoruns	Programma che rileva tutti i programmi in esecuzione automatica nel sistema
Utility			x	AviScreen	Programma che registra cio che succede al desktop
Utility	x			BinText 3.00	Programma che ricerca stringhe all'interno di qualsiasi tipo di file
PasswordTool			x	BulletsPassView	Programma di recupero password
Nirsoft			x	ChromeCacheView	Utility che permette di visualizzare la cache del browser chrome
PasswordTool			x	ChromePass	Utility che permette di recuperare le password contenute nel browser chorome
Nirsoft	x		x	Cports	Programma che permette di avere un elenco di tutte le porte utilizzate da TCP/IP e UDP
Nirsoft			x	Cports64	Programma che permette di avere un elenco di tutte le porte utilizzate da TCP/IP e UDP
Nirsoft			x	Cprocess	Utility che visualizza tutti i processi attivi con un elenco di tutte le dll e della memoria utilizzata
PasswordTool			x	Dialupass	Utility che permette il recupero di password utilizzate per la connessione remota ad altri pc
Utility			x	DiskDigger	Programma che permette il recupero di file eliminati dal proprio disco o schede di memorie
Sysinternal	x		x	DiskView	Programma che permette una visualizzazione grafica del Disco

					cosi da individuare la posizione effettiva del file
SysInfo	x	x		DriveManager	Programma per la gestione dei dischi
SysInfo	x			dumpReg	Programma per il dump dei valori dei registri
SysInfo	x			dumpSEC	Programma per il dump dei permessi
Sysinternal			x	Filemon	Programma che permette la visualizzazione delle attività del sistema e di come esse interagiscono tra di loro
SysInfo	x			FileWatch 1.00	Programma che controlla e monitora i file di registro del sistema
Nirsoft			x	Folrep	Utility che effettua un reporto su tutti le cartelle file contenuti nel file system
Acquire	x	x	x	FTKImager	Pachetto che di programmi che permette di rilevare varie informazioni sul sistema Esempio: dump della memoria, scansione dei Dischi ecc.
SysInfo		x		Hash My File	Programma che formisce l'hash dei file
Utility			x	Hoverdesk	Programma che permette di accedere a tutti i vostri programmi, file, comandi di sistema e siti web, utilizzando un'interfaccia personalizzata che è possibile creare
SysInfo	x			HoverSnap ! 0.8	Programma che fa screenshot dello schermo
Nirsoft	x		x	IECacheView	Utility che permette di visualizzare la cache del browser Internet Explorer
Nirsoft	x		x	IEcv	Utility che visualizza tutti i cookie memorizzati nel browser Explorer
Nirsoft	x		x	IEhv	Utility che permette di visualizzare lo storico delle Url del browser Explorer
PasswordTool	x		x	iepv	Utility che permette il recupero di password utilizzate nel browser Explorer
Analisys			x	Index.dat	Programma che permette di effettuare un tracciamento completo di tutta la navigazione e attivita Internet effettuata
Nirsoft			x	InsideClipboard	Utility che permette di visualizzare il contenuto della clipboard

Nirsoft	x			IPNetInfo	Fornisce informazioni su un IP Address
Nirsoft			x	LiveContactsView	Utility che permette di visualizzare tutte le informazioni riguardo ai contatti di windows live messenger
PasswordTool			x	LSASecretsdump	Utility che permette di estrarre e decriptare i segreti LSA dal registro di sistema
PasswordTool			x	LSASecretsdump64	Utility che permette di estrarre e decriptare i segreti LSA dal registro di sistema
PasswordTool	x		x	LSASecretsView	Utility che permette di visualizzare i segreti LSA del registro di sistema
PasswordTool			x	LSASecretsView64	Utility che permette di visualizzare i segreti LSA del registro di sistema
Utility			x	LTFViewer	Programma per la gestione e la visualizzazione dei file testuali
PasswordTool	x		x	mailpv	Utility che permette il recupero di password relative a client di posta elettronica
SysInfo	x	x		MDD	Programma per il dump della RAM
SysInfo		x		Mitec Exadedimal Editor	Editor esadecimale
SysInfo		x		Mitec System Information	Programma per il sysinfo
Nirsoft	x		x	MozillaCacheView	Utility che permette di visualizzare la cache del browser firefox
Nirsoft	x		x	MozillaHistoryView	Utility che permette di visualizzare la history del browser firefox
PasswordTool	x		x	mspass	Utility che permette di recuperare la password di applicazioni instant messenger
Nirsoft			x	MUICacheView	Utility che visualizza il contenuto della MUICache di windows
Nirsoft			x	MyEventViewer	Utility che visualizza gli eventi pianificati da windows
Nirsoft			x	MyLastSearch	Utility che permette di visualizzare tutte le più recenti ricerche effettuate con i motori di ricerca o ricerche effettuate attraverso social network
Nirsoft	x		x	MZcv	Utility che permette di visualizzare il contenuto della cache del browser firefox
PasswordTool	x		x	netpass	Utility che permette il recupero della password utilizzata in reti LAN per la connessione ad un server remoto attraverso NET Passaport account
PasswordTool			x	netpass64	Utility che permette il recupero della password utilizzata in reti LAN per la connessione ad un

					server remoto attraverso NET Passaport account
SysInfo	x			NetResView	Programma che visualizza tutte le risorse condivise
PasswordTool			x	Netscapass (FORSE)	Utility che permette il recupero della password di Netscape Communicator
Acquire			x	Nigilant32	Programma che permette di estrarre da un sistema quante più informazioni è possibile con il minor impatto possibile
Nirsoft			x	OpenedFilesView	Utility che visualizza tutti i file aperti nel sistema
Nirsoft			x	OperaCacheView	Utility che permette di visualizzare la cache del browser Opera
PasswordTool			x	OperaPassView	Utility che permette di recuperare e decriptare le password contenute nel browser Opera
Nirsoft			x	OutlookAttachView	Programma che permette di visualizzare tutti i messaggi archiviati e dei relativi allegati
Nirsoft			x	OutlookAttachView64	Programma che permette di visualizzare tutti i messaggi archiviati e dei relativi allegati
PasswordTool			x	PasswordFox	Utility che permette il recupero delle password contenute nel browser fireforx
SysInfo	x			PC Inspector File Recovery	Programma per il recovery dei file
PasswordTool			x	PCAnyPass	Utility in grado di recuperare immediatamente le password da Symantec pcAnywhere.
SysInfo	x	x		PCOnOffTime	Programma che visualizza le fasce orarie di utilizzo del sistema
Utility			x	PCTime	Programma per la schedulazione dei task
Utility		x	x	Photorec	Programma di recupero dati da dichi
Analisys	x		x	Pre-Search	Programma che permette l'acquisizione di tutte le immagini presenti nel sistema
Nirsoft			x	Process-Activity-view	Programma che fornisce una sintesi di tutti i file e cartelle che un dato processo accede
Nirsoft			x	Process-Activity-view64	Programma che fornisce una sintesi di tutti i file e cartelle che un dato processo accede
Sysinternal			x	procexp	Programma che permette di rilevare quali file sono attualmente in uso da un'applicazione

PasswordTool	x		x	pspv	Utility che rivela le password memorizzate dal browser explore,msn Explore outlook
PasswordTool			x	PstPassword	Utility che recupera le password di Outlook.pst
SysInfo	x			Putty	Programma client SSH
Sysinternal			x	RamMap	Programma che permette di visualizzare come la RAM assegna gli indirizzi ai processi utenti e ai processi kernel
PasswordTool	x		x	rdpv	Utility che rivela le password memorizzate da Microsoft Remote Desktop all'interno del file. rdp
Nirsoft			x	RecentFilesView	Utility che permette di visualizzare tutti i file utilizzati recentemente
Sysinternal	x		x	Regmon	Programma che permette di monitorare il registro di sistema visualizzandone le chiavi e gli accessi da parte delle applicazioni
Nirsoft	x		x	RegScanner	Utility che permette ricerche di informazioni all'interno del registro di sistema
Nirsoft			x	RegScanner64	Utility che permette ricerche di informazioni all'interno del registro di sistema
Nirsoft			x	RegScanner98	Utility che permette ricerche di informazioni all'interno del registro di sistema
SysInfo	x			ReSysInfo	Programma per il sysinfo
Sysinternal	x		x	rootkitrevealer	Programma che permette il rilevamento di rootkit
Nirsoft			x	Serviwin	Utility che fornisce l'elenco dei drive e dei servizi presenti nel sistema
Nirsoft			x	SkypeLogView	Utility che permette la visualizzazione dei file di log di Skype
Nirsoft			x	Smsniff	Utility che permette la cattura di pacchetti spediti sulla rete
Nirsoft			x	Smsniff64	Utility che permette la cattura di pacchetti spediti sulla rete
Utility			x	SophosAR	Antivirus
Utility			x	Spartacus	Shell utilizzata come superuser
Nirsoft			x	Strun	Utility che visualizza tutte le applicazioni caricate automaticamente da windwos in fase di avvio del sistema
Utility			x	Ternimal	Terminale
Utility		x	x	Testdisk	Programma che effettua il test dei dischi

Utility			x	TreeSizeFree	Programma per la gestione dello spazio sul disco
Analisys			x	UltraSearch	Programma che permette la ricerca di file sul file system
SysInfo		x		USB Write Protector	Programma che funge da write blocker
Nirsoft			x	USBAssistView	Utility che permette di visualizzare tutte le chiavi si assistenza utilizzate
Nirsoft	x	x	x	USBDeview	Utility che visualizza tutte le periferiche connesse via USB
Nirsoft			x	USBDeview64	Utility che visualizza tutte le periferiche connesse via USB
Nirsoft			x	UserProfilesView	Utility che visualizza tutte le informazioni sui profili utente presenti nel sistemi
PasswordTool			x	VCNPassView	Utility che recupera la password dal tool VCN
Nirsoft			x	VideoCacheView	Utility che permette di estrarre dalla cache del browser il video scaricato per poterlo rivedere
Sysinternal			x	vmmap	Programma che permette di monitorare la memoria virtuale usata dai processi
Analisys		x	x	W.F.A.	Applicazione che permette la decodifica di alcuni file speciali del sistema operativo windows
Acquire	x		x	W.F.T.	Programma che permette di estrarre informazioni sullo stato del sistema e sulla sua sicurezza
SysInfo			x	W.R.R.	Programma che permette di leggere i file di Windows 9x,NT,2k,XP relativi al registro ed estrae informazioni relative alla configurazione della macchina
Nirsoft			x	WhatInStartup	Utility visualizza tutte le informazioni sui programmi caricati in fase di startup del sistema
SysInfo		x		Whois	Programma per le informazioni dell'indirizzo ip
Acquire	x	x	x	win32dd	Programma che permette l'acquisizione della memoria fisica
Acquire		x	x	win64dd	Programma che permette l'acquisizione della memoria fisica
PasswordTool			x	win9xpv	Utility che rivela le password memorizzate nel sistema operativo windows 95/98
SysInfo	x	x	x	WinAudit	Programma che effettua un inventario del software, licence,

					configurazioni di rete e Hardware
SysInfo	x	x		winen	Programma per il dump della RAM
SysInfo	x			WinInfo	Programma che visualizza le informazioni sui programmi in esecuzione
Sysinternal	x		x	WINOBJ	Programma che permette di monitorare la sicurezza di un sistema
Nirsoft			x	WinPrefetchView	Utility che visualizza informazioni riguardo la fase di prefatch dei processi
Utility			x	WinVNC	Programma per il controllo remoto del pc
PasswordTool	x		x	WirelessKeyView	Utility che recupera la chieave per la connessione wireless per windows xp/vista
PasswordTool			x	WirelessKeyView64	Utility che recupera la chieave per la connessione wireless per windows xp/vista
Analisys			x	X-AgentRansack	Programma che effettua ricerche di file su HDD
Analisys			x	Xn-View	Programma di photo viewer
SysInfo	x		x	ZeroView	Programma che rileva se il Disco è stato crittografato

Bibliografia

[1] «Wikipedia,» [Online]. Available: http://it.wikipedia.org/wiki/Informatica_forense.

[2] M. Epifani, 2011. [Online]. Available: www.associazionearchimede.it/Unisa/phocadownload/ssi2011.pdf.

[3] M. MCDougal, «Live Forensics on Windows System using Windows Forensic Toolchest,» 2003-2006. [Online]. Available: http://www.foolmoon.net/downloads/Live_Forensics_Using_WFT.pdf.

[4] S. R. Stefano Fratepietro, «DEFT Manuale d'uso,» 2011. [Online]. Available: http://www.deftlinux.net/doc/[it]deft_manuale_full.pdf.

[5] AccessData, «Forensic ToolKit User Guide,» 22 Maggio 2008. [Online]. Available: http://accessdata.com/downloads/media/FTK_1.80_Manual.pdf.

[6] M. Suiche, «Challenges of Windows physical memory acquisition and exploitation,» Giugno 2009. [Online]. Available: http://shakacon.org/talks/NFI-Shakacon-win32dd0.3.pdf.

[7] R. Galati, «MSNP9,il protocollo di MSN,» 3 Gennaio 2008. [Online]. Available: http://www.programmazione.it/index.php?entity=eitem&idItem=38198.