Dall'acquisizione del materiale alla formazione della prova informatica

Cosimo Anglano
Centro Studi sulla Criminalita' Informatica
&
Dipartimento di Informatica
Universita' del Piemonte Orientale, Alessandria
Email: cosimo.anglano@unipmn.it
www.cisci.unipmn.it

L’analisi forense dei sistemi digitali

- Ha come obiettivo l’individuazione di informazioni aventi valore probatorio (*evidenze digitali*)
- Si basa sull’interpretazione e correlazione dei dati memorizzati su un sistema digitale (*artefatti*) al fine di ricostruire le azioni effettuate mediante quel sistema

Proprieta' dell'evidenza digitale

- Per assumere valore probatorio, l'evidenza digitale deve soddisfare alcune proprieta':
  - *Integrita'*: assenza di alterazioni negli artefatti
  - *Completezza*: analisi di tutti gli artefatti ad essa riferibili
  - *Autenticita'*: certezza della provenienza degli artefatti
  - *Veridicita'*: correttezza dell'interpretazione degli artefatti e delle azioni che ne hanno determinato la comparsa

Integrita' dell'evidenza digitale

- L'evidenza digitale e' *fragile*, cioe' facilmente alterabile nel caso in cui il dispositivo che la contiene sia maneggiato in modo inappropriato
- E' necessario utilizzare di metodologie e strumenti in grado di garantire *in modo dimostrabile* che l'evidenza non e' stata modificata durante l'analisi

Acquisizione del materiale

- Per preservare l'integrita' delle evidenze digitali, le operazioni di analisi vanno effettuate su copie identiche dei dispositivi originali
- L'operazione di copia viene denominata *acquisizione* al termine della quale viene prodotto un *file di immagine* contente una copia di tutti i bit memorizzati nel dispositivo

Write blocker e codici hash (1)

- L'uso di un *write blocker* permette di escludere modifiche al dispositivo durante l'operazione di acquisizione
- Il confronto tra il codice hash di sorgente e copia dimostra l'identicita' tra originale e copia
- Il ricalcolo del codice hash della copia ed il confronto con il valore ottenuto durante la sua acquisizione permette di escludere che vi siano state modifiche all'evidenza durante l'analisi

Write blocker e codici hash (2)

- Se il dispositivo presenta settori illeggibili (perche' danneggiati), il confronto degli hash non avra' successo
  - annotare i settori illeggibili
- Opportuno calcolare i codici hash dei singoli file
  - Possibile dimostrare l'identicita' delle copie dei file non contenenti settori danneggiati
  - Individuazione di file modificati accidentalmente (es. a causa di mancato uso di write blocker)

Le copie forensi (1)

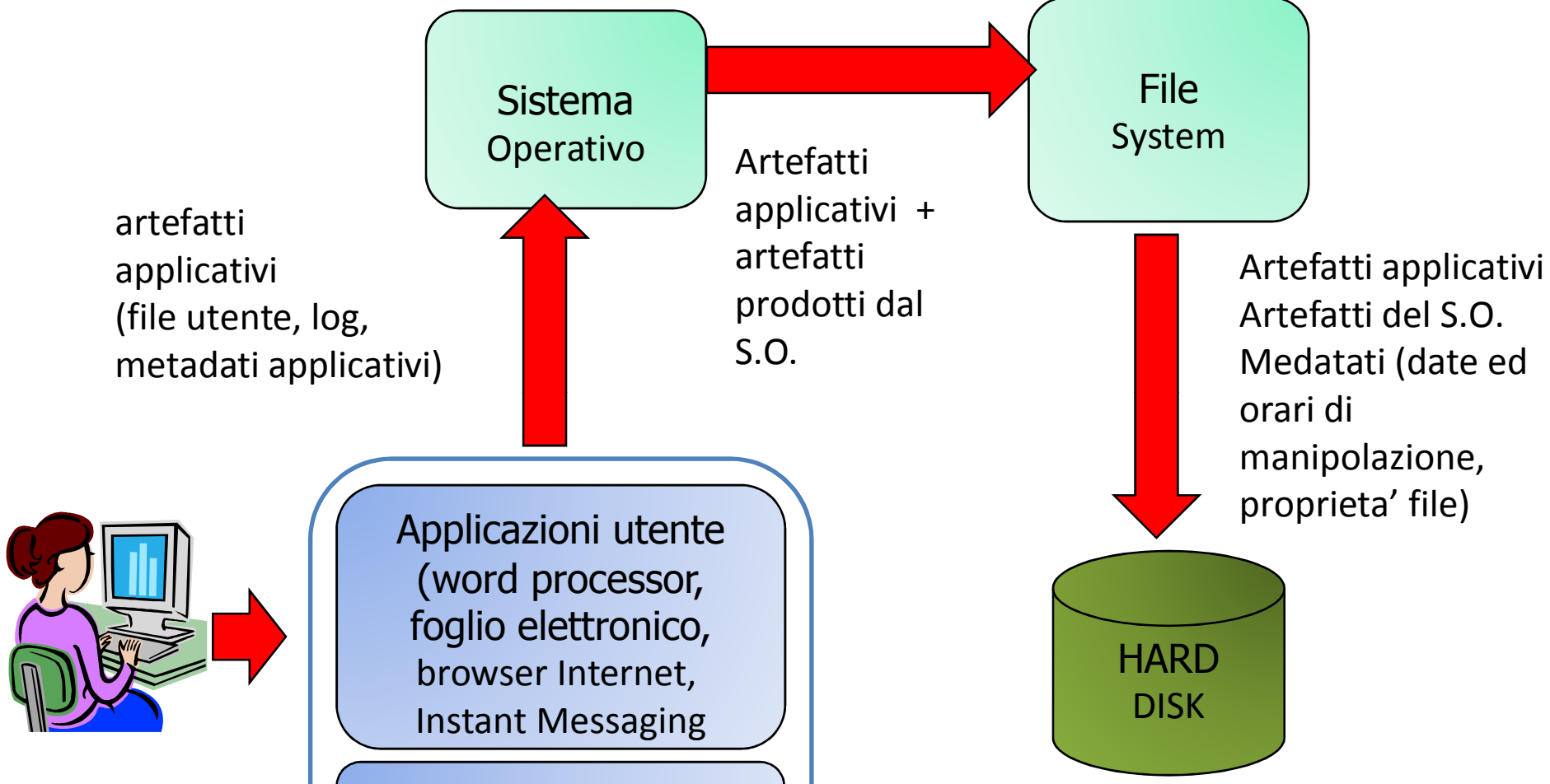
- Lo spazio in un dispositivo di memorizzazione dati e' suddivisibile in
  - Spazio allocato: contiene dati dei file presenti sul dispositivo
  - Spazio non allocato: a disposizione del sistema operativo (puo' contenere dati di file cancellati)
  - Spazio '*slack*': spazio compreso tra la fine logica e fisica di ciascun file (puo' contenere dati di file cancellati)

- Al fine di garantire la completezza, e' necessario acquisire *tutte le aree del dispositivo*, e non solo i file visibili agli utenti
- Tali copie sono dette *copie forensi* o anche *copie bit-a-bit*

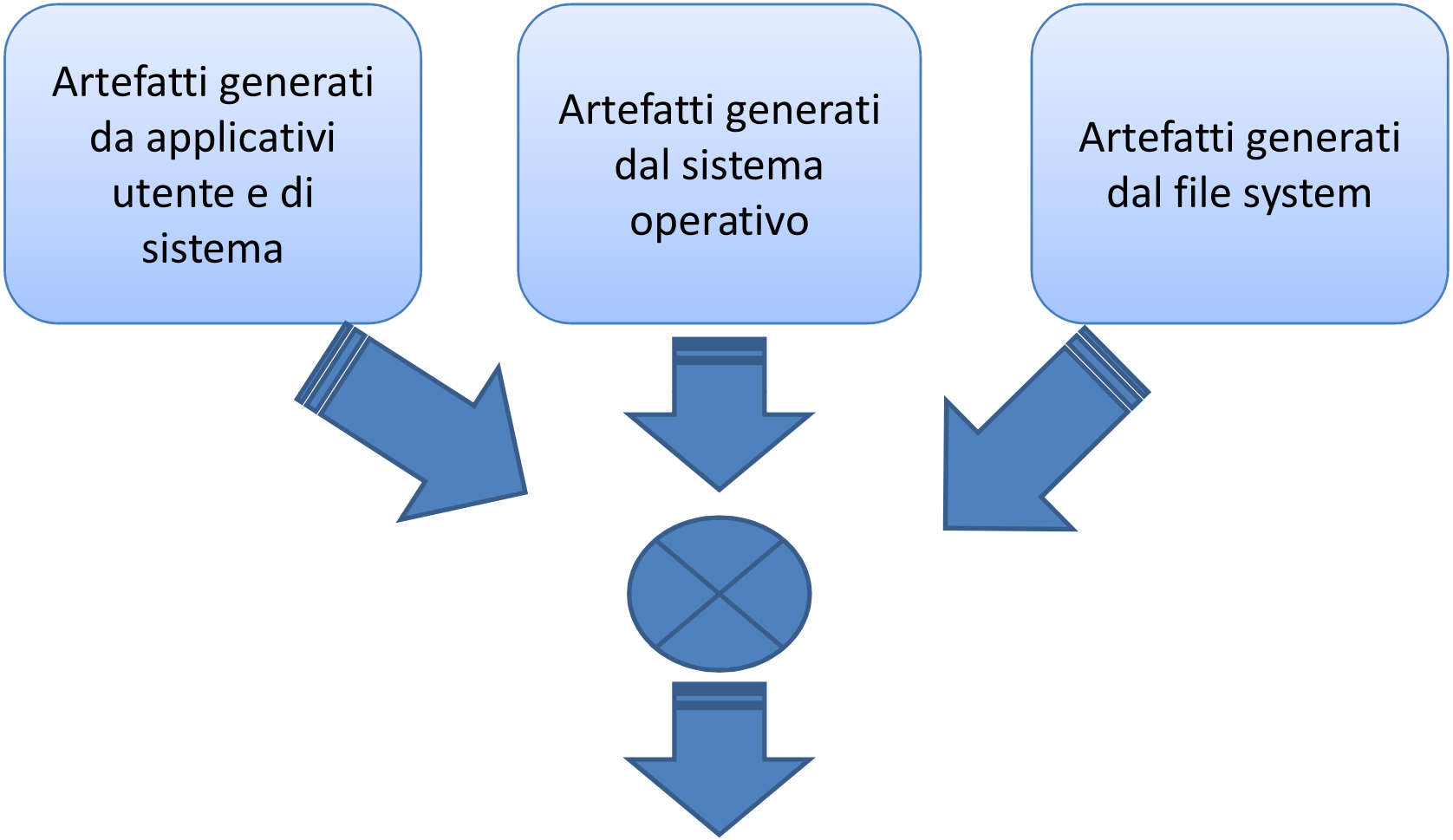
Le copie forensi (2)

- Alcune tipologie di hard disk (quelle piu' diffuse) permettono di impostare aree nascoste non visibili in fase di acquisizione (*Host Protected Area* e *Direct Configuration Overlay*)
- E' quindi necessario verificare l'eventuale presenza di tali aree e rimuoverle prima di effettuare l'acquisizione

Analisi forense di un computer



Analisi forense di un computer



Operazioni preliminari

- Recupero di file cancellati o loro frammenti
- Filtraggio dei file irrilevanti
- Individuazione di file potenzialmente rilevanti
  - ricerca con parole chiave
  - individuazione del corretto tipo dei file (analisi delle firme)
  - classificazione dei file per tipo
  - individuazione di file crittografati e loro decifratura (se e quando possibile)
  - Individuazione di file nascosti
  - estrazione di contenuti da file compositi

Ricostruzione delle attivita’

- L’evidenza digitale e’ autentica se e’ possibile determinare con certezza la sua provenienza e le azioni che hanno determinato la sua creazione
- Occorre quindi effettuare la *ricostruzione* delle attivita’ che hanno portato alla comparsa degli artefatti su cui essa e’ basata

Costruzione della *timeline* (1)

- Creazione di una linea temporale relativa alle attivita' effettuate dal computer analizzato
- Richiede l'integrazione delle varie informazioni temporali (*timestamp*) create dal sistema operativo, dal file system e dalle applicazioni utente

Costruzione della *timeline* (2)

- Timestamp relativi a creazione, ultimo accesso ed ultima modifica dei file

Name	Created	Modified	Accessed
Esempio.doc	11/09/2009 13.15.31	11/09/2009 13.15.31	11/09/2009 13.15.31
DocumentoImportante.doc	05/05/2008 21.36.33	05/05/2008 21.36.15	06/05/2008 11.57.51
Parte1.doc	02/05/2008 09.31.15	04/05/2008 12.32.04	04/05/2008 12.32.04
Parte2.doc	02/05/2008 09.31.15	04/05/2008 12.32.04	04/05/2008 12.32.04

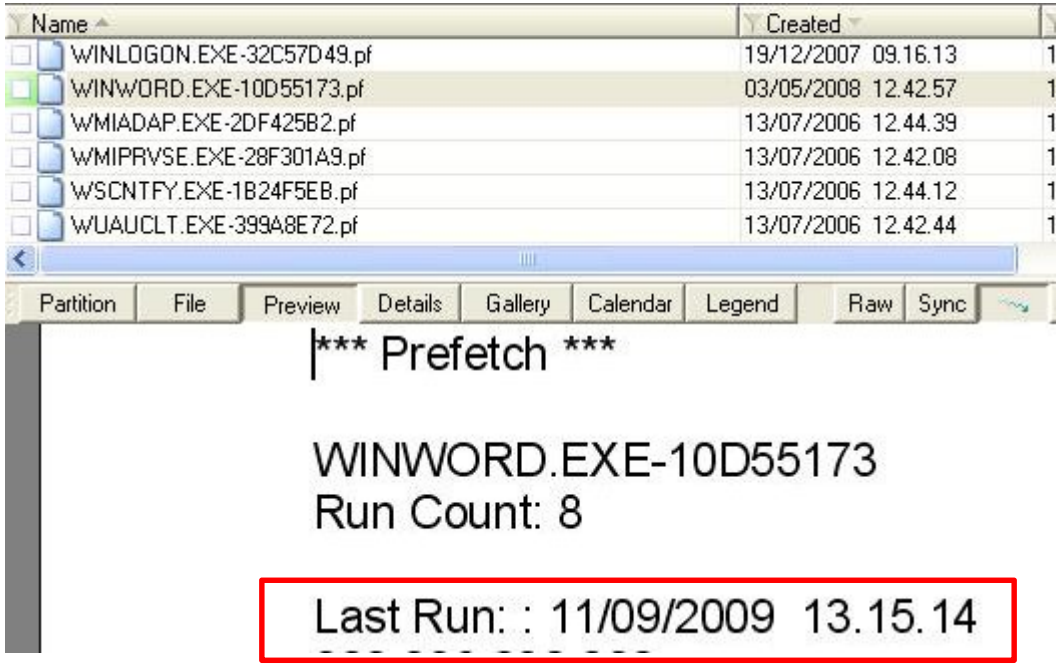
Costruzione della *timeline* (3)

- La prima versione della timeline e' basata sui timestamp dei file

Data / Ora	Evento	Oggetto
02/05/2008 09.31.15	Creazione file	Parte1.doc
02/05/2008 09.31.15	Creazione file	Parte2.doc
04/05/2008 12.32.04	Modifica – Accesso file	Parte1.doc
04/05/2008 12.32.04	Modifica – Accesso file	Parte2.doc
05/05/2008 21.36.33	Creazione – Modifica file	DocumentoImportante.doc
06/05/2008 11.57.51	Accesso file	DocumentoImportante.doc
11/09/2009 13.15.31	Creazione-Modifica-Accesso file	Esempio.doc

Costruzione della *timeline* (4)

- Timestamp relativi all'esecuzione di programmi
  - file di "prefetch" sul sistema operativo Windows



Costruzione della *timeline* (5)

Data / Ora	Evento	Oggetto
02/05/2008 09.31.15	Creazione file	Parte1.doc
02/05/2008 09.31.15	Creazione file	Parte2.doc
04/05/2008 12.32.04	Modifica – Accesso file	Parte1.doc
04/05/2008 12.32.04	Modifica – Accesso file	Parte2.doc
05/05/2008 21.36.33	Creazione – Modifica file	DocumentoImportante.doc
06/05/2008 11.57.51	Accesso file	DocumentoImportante.doc
11/09/2009 13.15.14	Esecuzione programma	WINWORD.EXE
11/09/2009 13.15.31	Creazione-Modifica-Accesso file	Esempio.doc

- Si puo' ipotizzare che il file 'Esempio.doc' sia stato creato durante l'esecuzione di WINWORD.EXE

Costruzione della *timeline* (6)

- Timestamp relativi all'esecuzione di programmi da parte degli utenti
  - analisi del registro di Windows relativo ad uno dei profili utente ("*User*") definiti sul computer analizzato

Key Properties	
Last Written Time	11/09/2009 11.15.13 UTC
Value Properties	
Value Name ROT13	UEME_RUNPIDL:%csidl2%\Microsoft Word.lnk
Time	11/09/2009 11.15.13 UTC

Key Properties	
Last Written Time	11/09/2009 11.15.13 UTC
Value Properties	
Value Name ROT13	UEME_RUNPATH:C:\Program Files\Microsoft Office\Office\WINWORD.EXE
Time	11/09/2009 11.15.13 UTC

Costruzione della *timeline* (7)

Data / Ora	Evento	Oggetto
05/05/2008 21.36.33	Creazione – Modifica file	DocumentoImportante.doc
06/05/2008 11.57.51	Accesso file	DocumentoImportante.doc
11/09/2009 13.14.13	"User" avvia programma mediante menu'	WINWORD.EXE
11/09/2009 13.15.14	Esecuzione programma	WINWORD.EXE
11/09/2009 13.15.31	Creazione-Modifica-Accesso file	Esempio.doc

- L'utente "*User*" ha avviato WINWORD.EXE pochi secondi prima che fosse creato il file 'Esempio.doc'

Costruzione della *timeline* (8)

- Timestamp relativi agli ultimi file aperti con Word da "*User*"

Name	Path	Created	Modified	Accesse
Esempio.doc.LNK	\Documents and Settings\User\Application Data\Microsoft\Office\Recent	11/09/2009 13.15.31	11/09/2009 13.15.31	11/09/200
Event Viewer.lnk	\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools	13/07/2006 06.50.44	13/07/2006 06.50.44	19/12/200
Files and Settings Transfer Wizard.lnk	\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools	13/07/2006 06.50.45	13/07/2006 06.50.45	03/05/200
Freecell.lnk	\Documents and Settings\All Users\Start Menu\Programs\Games	13/07/2006 06.44.10	13/07/2006 06.44.10	26/04/200
Hearts.lnk	\Documents and Settings\All Users\Start Menu\Programs\Games	13/07/2006 06.44.10	13/07/2006 06.44.10	26/04/200
HyperTerminal.lnk	\Documents and Settings\All Users\Start Menu\Programs\Accessories\Communications	13/07/2006 06.44.10	13/07/2006 06.44.10	26/04/200

Partition | File | Preview | Details | Gallery | Calendar | Legend | Raw | Sync

Show Window	SW_NORMAL
Target Created	11/09/2009 13.15.31
Last Written	11/09/2009 13.15.31
Last Accessed	11/09/2009 13.15.31
Workplace	C:\
Volume Type	Fixed
Volume Serial	0x544A9319
Volume Name	
Local Path	C:\Documents and Settings\User\My Documents\Esempio.doc
Relative Path	..\..\..\..\My Documents\Esempio.doc
Host Name	xppro
Volume ID	{E15D49BE-1DBC-4E66-847E-4A0242135E06}
Object ID	{6AC3A980-9EC4-11DE-8A4B-000C29751654}
MAC Address	00 0C 29 75 16 54

Costruzione della *timeline* (9)

Data / Ora	Evento	Oggetto
05/05/2008 21.36.33	Creazione – Modifica file	DocumentoImportante.doc
06/05/2008 11.57.51	Accesso file	DocumentoImportante.doc
11/09/2009 13.14.13	"User" avvia programma mediante menu' "Start"	WINWORD.EXE
11/09/2009 13.15.14	Esecuzione programma	WINWORD.EXE
11/09/2009 13.15.31	"User" salva file	Esempio.doc
11/09/2009 13.15.31	Creazione-Modifica-Accesso file	Esempio.doc

- L'utente "*User*" ha salvato il file 'Esempio.doc' alla stessa ora e data in cui esso e' comparso sull'hard disk
- Conclusione: il file 'Esempio.doc' e' stato creato dall'utente 'User' mediante il programma Microsoft Word

Costruzione della *timeline* (10)

- L'integrazione con artefatti applicativi permette di effettuare altre tipologie di ricostruzioni
- Esempio: determinare le modalita' con le quali e' stata creata la cartella 'C:\Software\skype-logs' ed i file che essa contiene

Data / Ora	Evento	Oggetto
11/09/2009 16.12.48	Creazione – Modifica cartella e file ivi contenuti	C:\Software\skype-logs

Costruzione della *timeline* (11)

- L'analisi dell'attivita' di navigazione su Internet permette di individuare il seguente URL visitato mediante Internet Explorer

Data ed ora	Utente	URL
11/09/2009 16.12.18	User	https://www.di.unito.it/wm/horde/services/download/?module=imp&thismailbox=INBOX&index=43685&mailbox=INBOX&actionID=download_attach&id=2&mimecache=12e632e4d6806fb5d482e1ec8ad57200&fn=%2Fskype-logs.zip

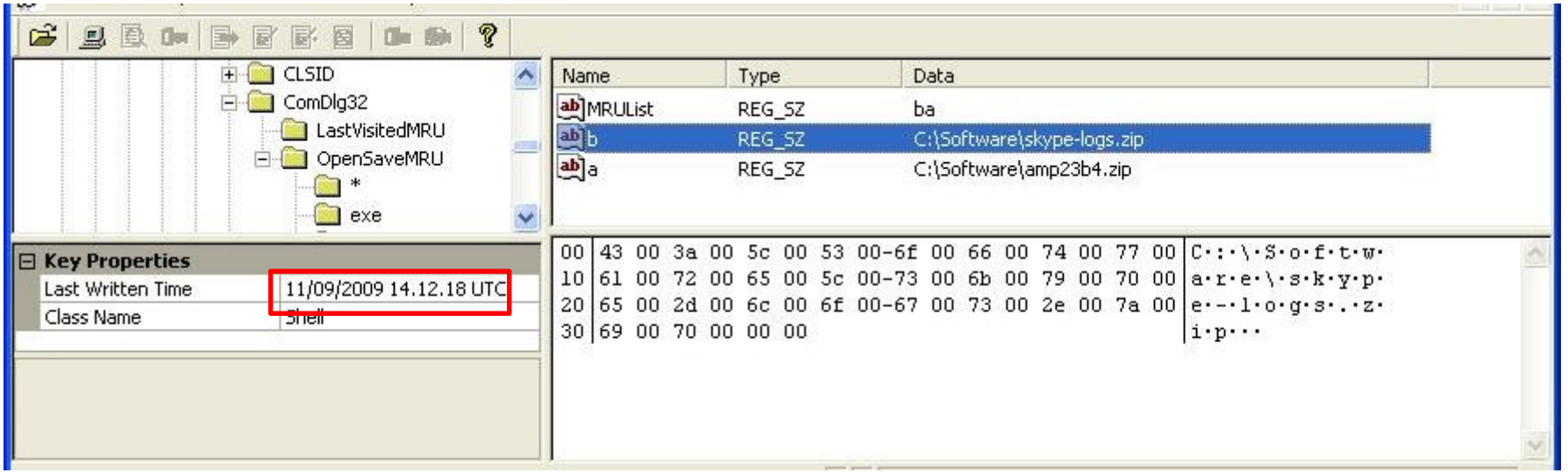
Costruzione della *timeline* (12)

Data / Ora	Evento	Oggetto
11/09/2009 16.12.18	L'utente "User" scarica un allegato da WebMail	skype-logs.zip
11/09/2009 16.12.48	Creazione – Modifica cartella e file ivi contenuti	C:\Software\skype-logs

- '*User*' ha scaricato 'skype-logs.zip' da un account WebMail prima che la cartella in questione fosse creata

Costruzione della *timeline* (13)

- Artefatti nel registro di Windows relativi al salvataggio di file



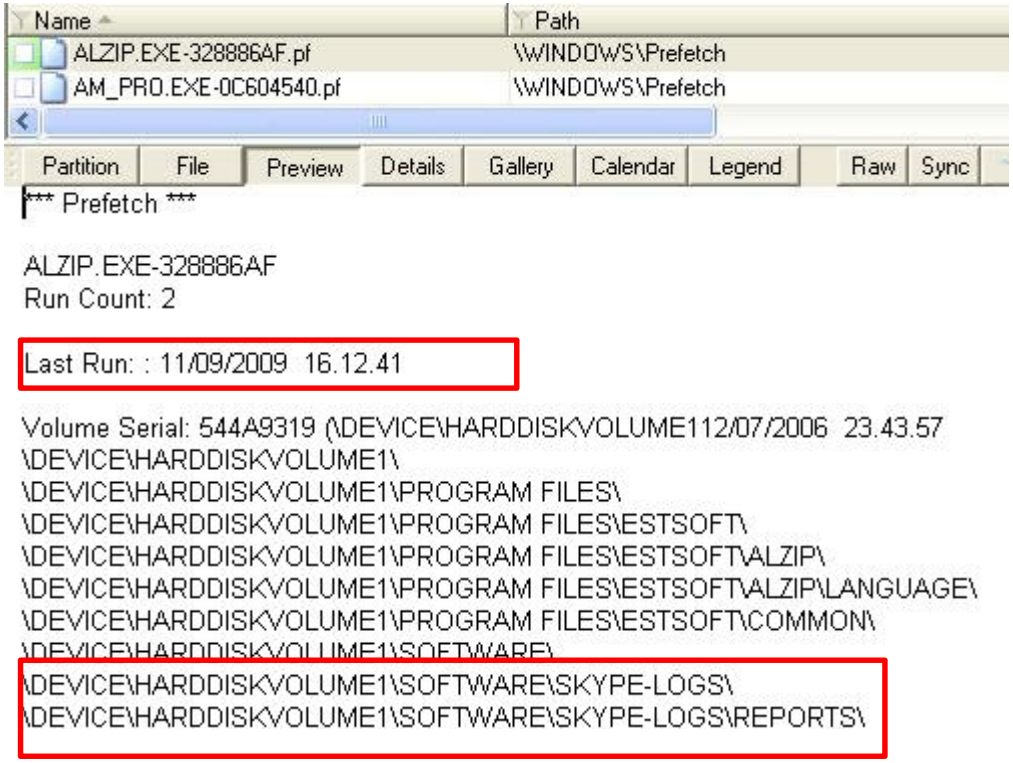
Costruzione della *timeline* (14)

Data / Ora	Evento	Oggetto
11/09/2009 16.12.18	“User” scarica un allegato da WebMail	skype-logs.zip
11/09/2009 16.12.18	“User” salva file	C:\Software\skype-logs.zip
11/09/2009 16.12.48	Creazione – Modifica cartella e file ivi contenuti	C:\Software\skype-logs

- Abbiamo la conferma che ‘*User*’ ha scaricato ‘skype-logs.zip’ da un account WebMail e lo ha salvato nella cartella ‘C:\Software’
- Non conosciamo pero’ le modalita’ con le quali e’ stata creata la cartella C:\Software\skype-logs

Costruzione della *timeline* (15)

- Timestamp relativi all'esecuzione di programmi



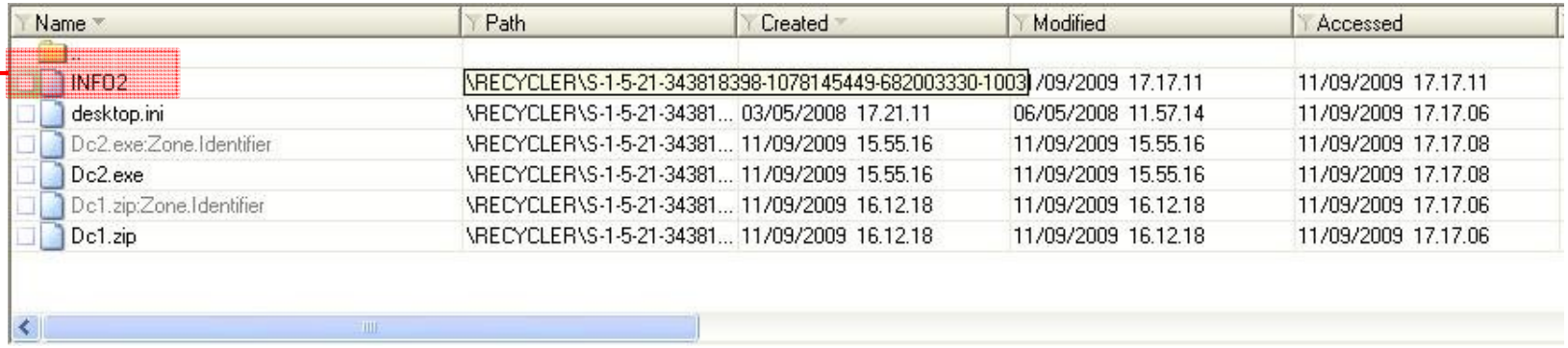
Costruzione della *timeline* (16)

Data / Ora	Evento	Oggetto
11/09/2009 16.12.18	"User" scarica un allegato da WebMail	skype-logs.zip
11/09/2009 16.12.18	"User" salva file	C:\Software\skype-logs.zip
11/09/2009 16.12.41	"User" esegue il programma ALZIP.EXE	C:\Software\skype-logs C:\Software\skype-logs\REPORTS
11/09/2009 16.12.48	Creazione – Modifica cartella e file ivi contenuti	C:\Software\skype-logs

- Dopo aver scaricato skype-logs.zip nella cartella C:\Software, '*User*' lo ha poi decompresso mediante il programma ALZIP.EXE

Costruzione della *timeline* (17)

- Per scoprire cosa ne e' stato di skype-logs.zip, analizziamo il contenuto del "Cestino" di Windows di '*User*'
  - non e' stato svuotato



Name	Path	Created	Modified	Accessed
INFO2	\RECYCLER\S-1-5-21-343818398-1078145449-682003330-1003	/09/2009 17.17.11		11/09/2009 17.17.11
desktop.ini	\RECYCLER\S-1-5-21-34381...	03/05/2008 17.21.11	06/05/2008 11.57.14	11/09/2009 17.17.06
Dc2.exe:Zone.Identifier	\RECYCLER\S-1-5-21-34381...	11/09/2009 15.55.16	11/09/2009 15.55.16	11/09/2009 17.17.08
Dc2.exe	\RECYCLER\S-1-5-21-34381...	11/09/2009 15.55.16	11/09/2009 15.55.16	11/09/2009 17.17.08
Dc1.zip:Zone.Identifier	\RECYCLER\S-1-5-21-34381...	11/09/2009 16.12.18	11/09/2009 16.12.18	11/09/2009 17.17.06
Dc1.zip	\RECYCLER\S-1-5-21-34381...	11/09/2009 16.12.18	11/09/2009 16.12.18	11/09/2009 17.17.06

ID	Moved to Recycle Bin	File Size	Original Filename
1	11/09/2009 17.17.08	1.880.064	C:\Software\skype-logs.zip
2	11/09/2009 17.17.11	6.856.704	C:\Software\ALZip.exe

Costruzione della *timeline* (18)

Data / Ora	Evento	Oggetto
11/09/2009 16.12.18	"User" scarica un allegato da WebMail	skype-logs.zip
11/09/2009 16.12.18	"User" salva file	C:\Software\skype-logs.zip
11/09/2009 16.12.41	"User" esegue il programma ALZIP.EXE	C:\Software\skype-logs C:\Software\skype-logs\REPORTS
11/09/2009 16.12.48	Creazione – Modifica cartella e file ivi contenuti	C:\Software\skype-logs
11/09/2009 17.17.08	"User" ha cancellato file	C:\Software\skype-logs.zip

- Dopo aver decompresso skype-logs.zip, '*User*' lo ha cancellato spostandolo nel Cestino

Limitazioni e problematiche

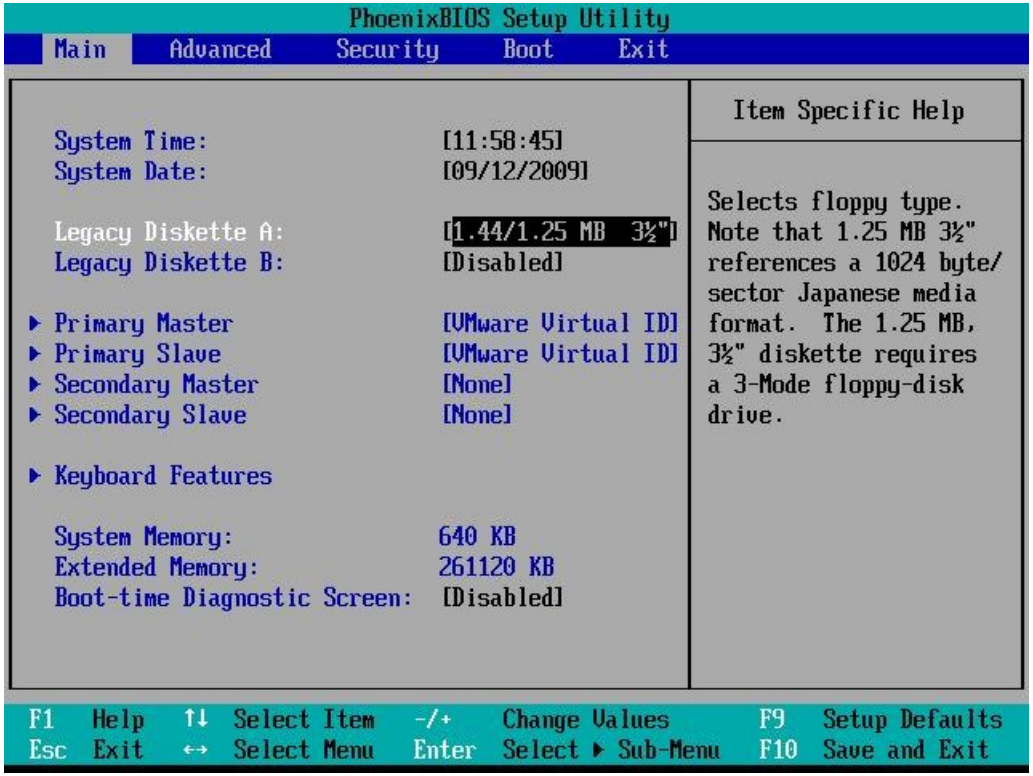
- Non sempre e' possibile ottenere ricostruzioni cosi' complete
  - alcuni artefatti possono essere stati eliminati dal Sistema Operativo nel corso del suo funzionamento
  - Il cestino puo' essere stato svuotato ed il file INFO2 cancellato in modo irrecuperabile
  - La storia di navigazione su Internet puo' essere stata cancellata in modo irrecuperabile dall'utente
- La quantita' ed il tipo di artefatti varia tra i diversi Sistemi Operativi

Correttezza dei timestamp (1)

- Un'ovvia obiezione ad una data ricostruzione e' che le informazioni temporali non siano attendibili
  - Impostazioni errate dell'orologio del computer
  - Alterazione dell'orologio del computer e suo successivo ripristino all'ora corretta
  - Manomissione dei timestamp dei vari file

Correttezza dei timestamp (2)

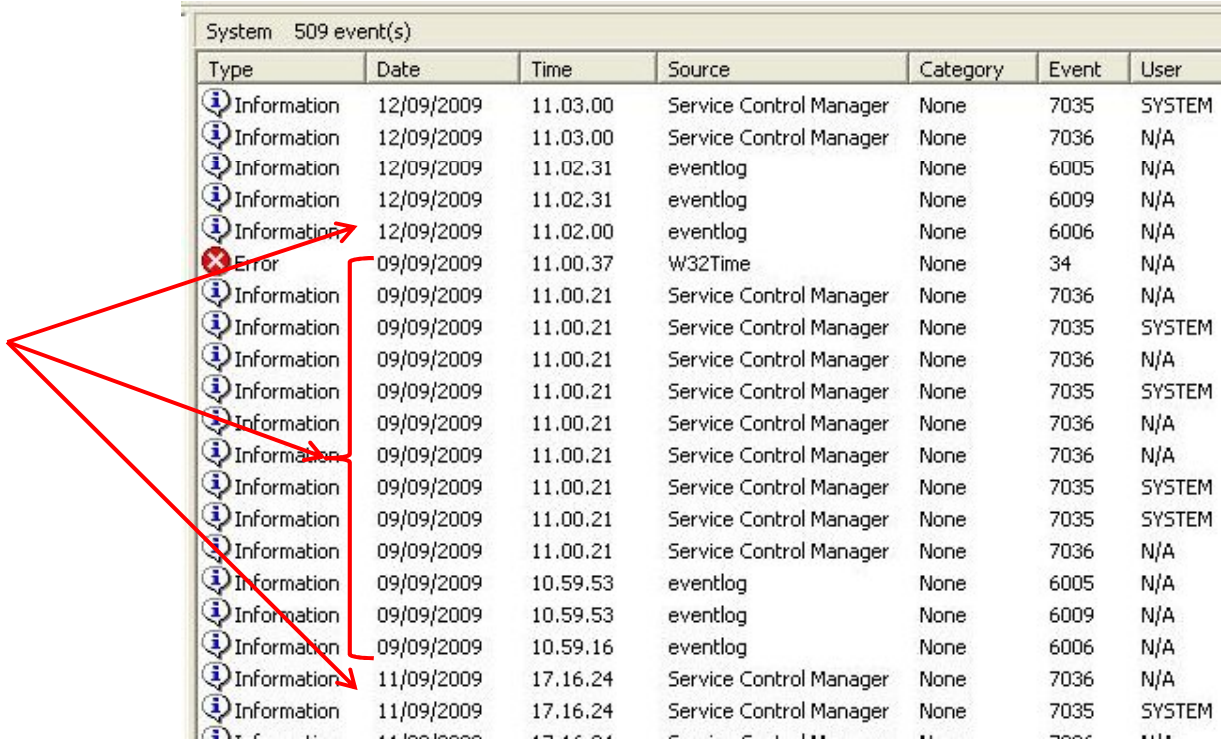
- All'atto dell'acquisizione (o del sequestro) annotare le impostazioni del BIOS relative ad ora e data del computer



Correttezza dei timestamp (3)

- Durante l'analisi, controllare che non vi siano artefatti prodotti da alterazioni e ripristini dell'orologio del computer (file di log di varia natura)

inversione temporale



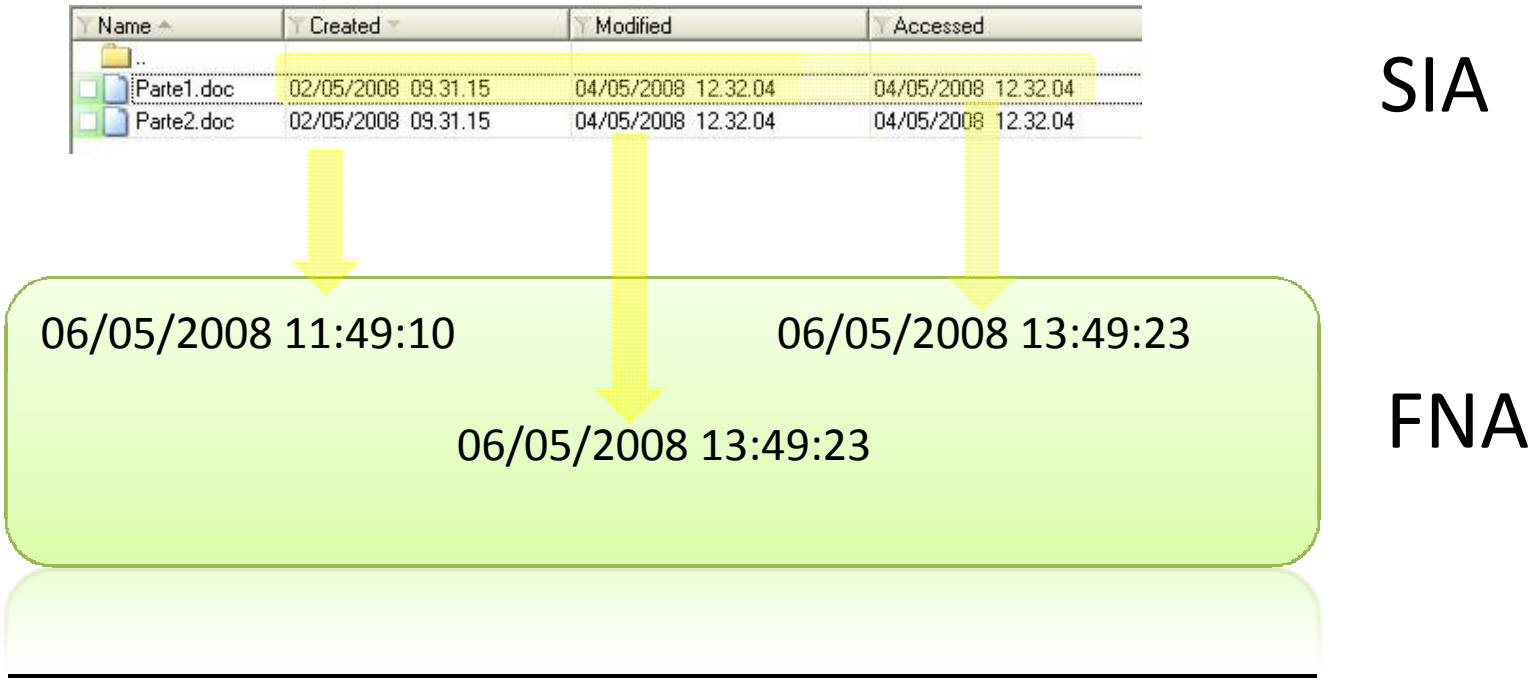
System 509 event(s)

Type	Date	Time	Source	Category	Event	User
Information	12/09/2009	11.03.00	Service Control Manager	None	7035	SYSTEM
Information	12/09/2009	11.03.00	Service Control Manager	None	7036	N/A
Information	12/09/2009	11.02.31	eventlog	None	6005	N/A
Information	12/09/2009	11.02.31	eventlog	None	6009	N/A
Information	12/09/2009	11.02.00	eventlog	None	6006	N/A
Error	09/09/2009	11.00.37	W32Time	None	34	N/A
Information	09/09/2009	11.00.21	Service Control Manager	None	7036	N/A
Information	09/09/2009	11.00.21	Service Control Manager	None	7035	SYSTEM
Information	09/09/2009	11.00.21	Service Control Manager	None	7036	N/A
Information	09/09/2009	11.00.21	Service Control Manager	None	7035	SYSTEM
Information	09/09/2009	11.00.21	Service Control Manager	None	7036	N/A
Information	09/09/2009	11.00.21	Service Control Manager	None	7036	N/A
Information	09/09/2009	11.00.21	Service Control Manager	None	7035	SYSTEM
Information	09/09/2009	11.00.21	Service Control Manager	None	7035	SYSTEM
Information	09/09/2009	11.00.21	Service Control Manager	None	7036	N/A
Information	09/09/2009	10.59.53	eventlog	None	6005	N/A
Information	09/09/2009	10.59.53	eventlog	None	6009	N/A
Information	09/09/2009	10.59.16	eventlog	None	6006	N/A
Information	11/09/2009	17.16.24	Service Control Manager	None	7036	N/A
Information	11/09/2009	17.16.24	Service Control Manager	None	7035	SYSTEM

Correttezza dei timestamp (4)

- La manomissione dei timestamp dei singoli file puo' essere, in alcuni casi, rilevata mediante l'analisi di metadati non visibili agli utenti
  - per ogni file, il file system NTFS mantiene due insiemi di timestamp
    - *Standard Information Attribute (SIA)*: visibili agli utenti e modificati quando si alterano a mano i timestamp
    - *File Name Attribute (FNA)*: non visibili e non modificabili dagli utenti

Correttezza dei timestamp (5)



- In questo caso si puo' dedurre la retrodatazione dei timestamp del file 'Parte1.doc'

Correttezza dei timestamp (6)

- ... o anche dei *metadati applicativi* (come quelli salvati dai programmi del pacchetto Office di Microsoft)

Last authors (up to 10):

Utente Sospetto	C:\Tesi\Parte1.doc

Summary Information

OS	Win32 5.1
Title	
Author	Utente Sospetto
Template	Normal.dot
Last Saved By	Utente Sospetto
Version	2
Creating Application	Microsoft Word 9.0
Total Edit Time	120 min
Created	06/05/2008 11.49.00
Last Saved	06/05/2008 13.49.00
Page count	1

Individuazione del responsabile

- Un’altra obiezione alla ricostruzione e’ relativa all’attribuzione della paternita’ delle azioni individuate
- L’analisi forense di un computer permette di individuare un profilo utente che ha effettuato alcune azioni
- Associare un’identita’ reale al profilo utente puo’ essere talvota piuttosto complesso

La "*malware defense*"

- Affermazione secondo cui le azioni illegittime sono state compiute da un terzo ignoto che ha acquisito il controllo del computer in maniera occulta mediante un cosiddetto "*malware*"
  - Virus
  - Trojan horse che crea una backdoor
  - Worm
  - …

Malware: individuazione ed analisi (1)

- E’ buona norma far analizzare da software specifico (antivirus, anti rootkit, ecc.) le immagini dei dispositivi acquisiti
- Nel caso in cui sia presente del malware, occorre analizzarlo per determinarne le azioni
  - analisi statica mediante reperimento di informazioni sul malware da siti e pubblicazioni
  - analisi dinamica del suo funzionamento in ambienti controllati (macchine virtuali)

Malware: individuazione ed analisi (2)

- La mancata rilevazione di malware su un dispositivo non sempre permette di escludere la sua effettiva presenza
  - un antivirus puo' individuare solo un virus gia' noto
  - nelle comunita' dedite all'hacking ogni tanto qualcuno afferma l'esistenza di malware che risiede unicamente nella memoria RAM (volatile)

Malware: individuazione ed analisi (3)

- Se il computer e' acceso, sarebbe opportuno analizzare il contenuto della memoria volatile
  - Operazioni che fanno ormai parte delle "best practices" internazionali
- Analisi "live": esecuzione di comandi sul computer
  - alterazioni dello stato del sistema
  - non piu' effettuabile dopo aver spento il computer

Malware: individuazione ed analisi (4)

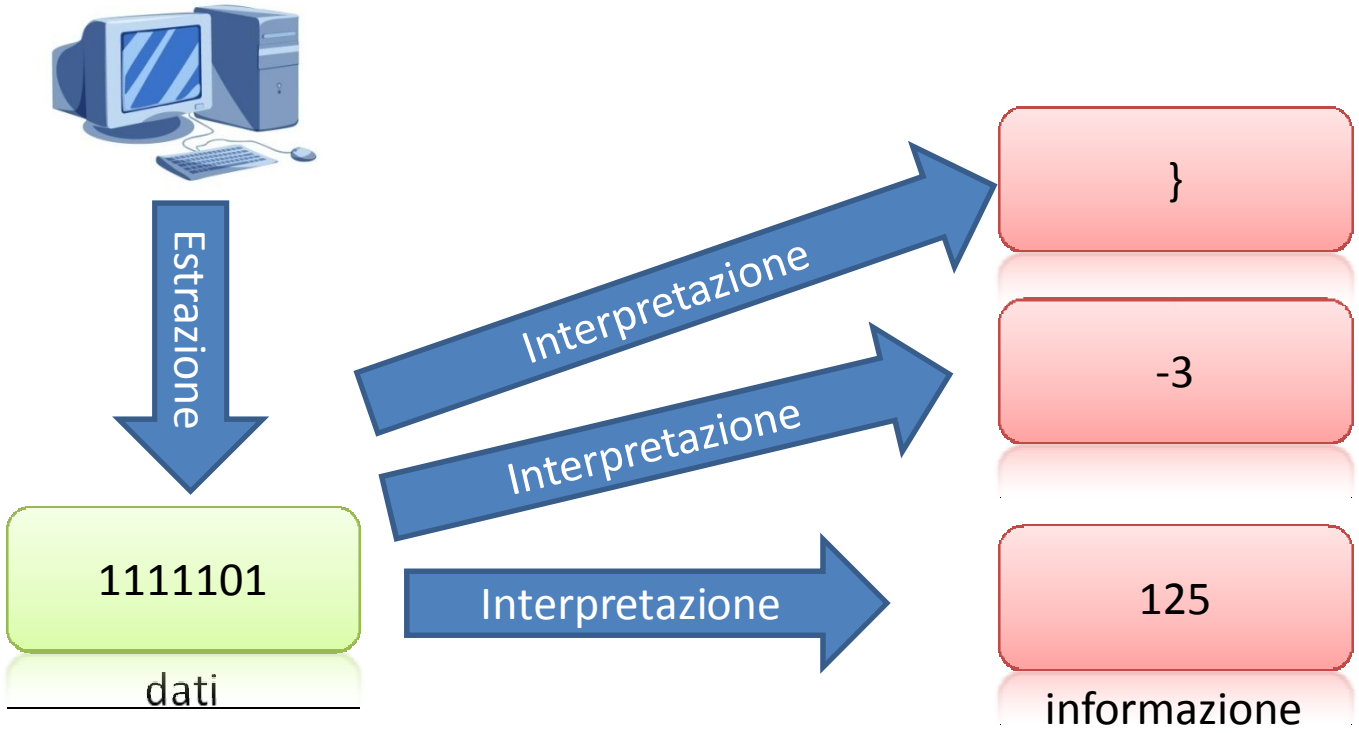
- Analisi del contenuto della memoria
  - tecnica relativamente recente
  - salvataggio del contenuto della memoria del computer su apposito supporto esterno
  - decodifica ed analisi del suo contenuto
- Vantaggi rispetto all'analisi live:
  - congelamento dello stato della memoria volatile
  - ripetibile in qualsiasi momento (non occorre che sia acceso il computer da analizzare)
  - minore invasivita'

Malware: individuazione ed analisi (5)

- Individuazione di malware mediante analisi del contenuto della memoria
  - Elenco di programmi in esecuzione (anche programmi nascosti)
  - Estrazione dell'eseguibile, scansione con antivirus ed analisi in ambiente controllato
  - Elenco di connessioni di rete attive
  - Elenco di utenti collegati

Veridicita' e correttezza

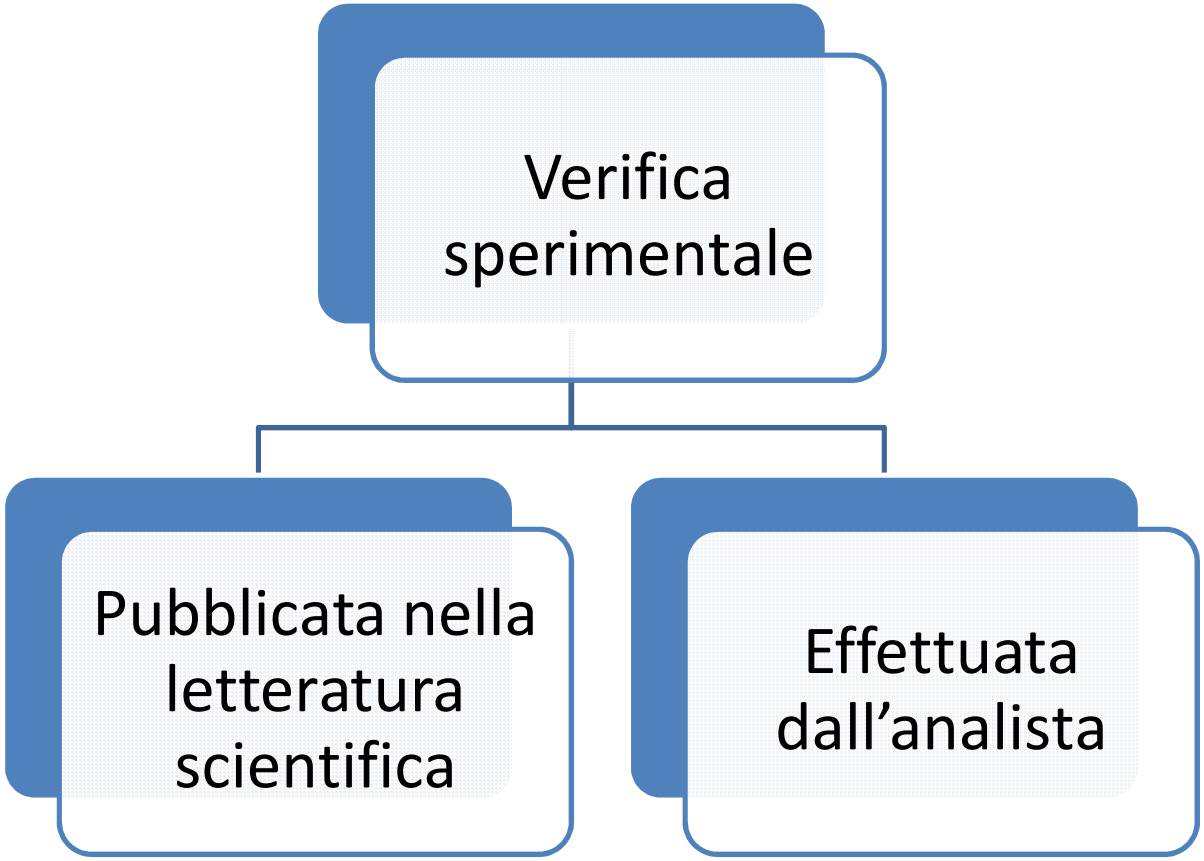
- L'evidenza digitale e' veritiera se sono corrette:
  - la decodifica e l'interpretazione degli artefatti
  - l'individuazione della catena causale che li ha determinati



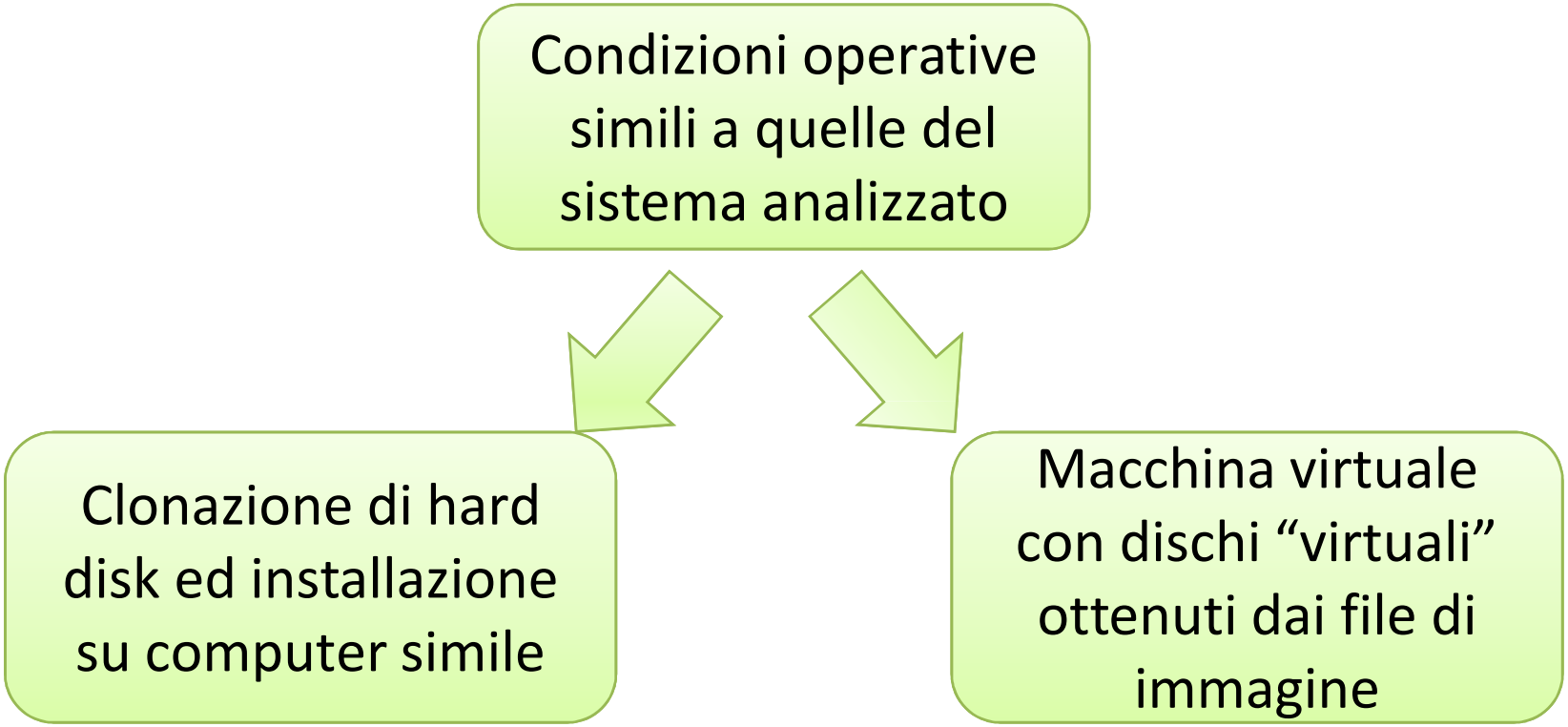
Il metodo scientifico

- La corretta interpretazione di artefatti ed identificazione delle cause che li determinano deve essere verificabile sperimentalmente
- Sperimentazione da effettuarsi in condizioni operative identiche o simili a quelle del sistema analizzato
- I risultati della sperimentazione devono essere riproducibili

La verifica sperimentale (1)



La verifica sperimentale (2)



Maggior controllabilita’ e riproducibilita’ degli esperimenti

La validazione dei programmi di analisi

- Per le analisi forensi, in genere ci si avvale di strumenti software specializzati in grado di semplificare i processi di decodifica, ricerca e correlazione degli artefatti
- Come tutti i sistemi software complessi, possono essere affetti da vari problemi
  - errori di programmazione (“ *bug*”)
  - mancanza di aggiornamento

La validazione dei programmi di analisi

- La maggioranza dei software di analisi forense sono di tipo commerciale e closed-source, e non permettono l'ispezione del codice per accertare eventuali errori
- L'analista dovrebbe sempre validare i propri risultati utilizzando il metodo scientifico, al fine da escludere al presenza di errori

Conclusioni

- L’analisi forense di un computer e’ un processo al cui centro e’ posto l’analista, mentre il ruolo del software di analisi e’ solo strumentale
- La complessita’ e la rapidita’ di evoluzione dei sistemi di elaborazione impongono all’analista:
  - Adesione a standard operativi accettati dalla comunita’ scientifica a livello internazionale
  - Formazione specifica ed aggiornamento
  - Verifiche incrociate ed indipendenti
  - Scrupolosa reportistica