Generazione ed Analisi di una Timeline Forense

Vincenzo Calabrò

vincenzo.calabro@computer.org

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

Evidenza digitale: una definizione

- “Qualsiasi informazione, con valore probatorio, che sia memorizzata o trasmessa in formato digitale “ [*Scientific Working Group on Digital Evidence, 1998*]

Proprieta' dell'evidenza digitale

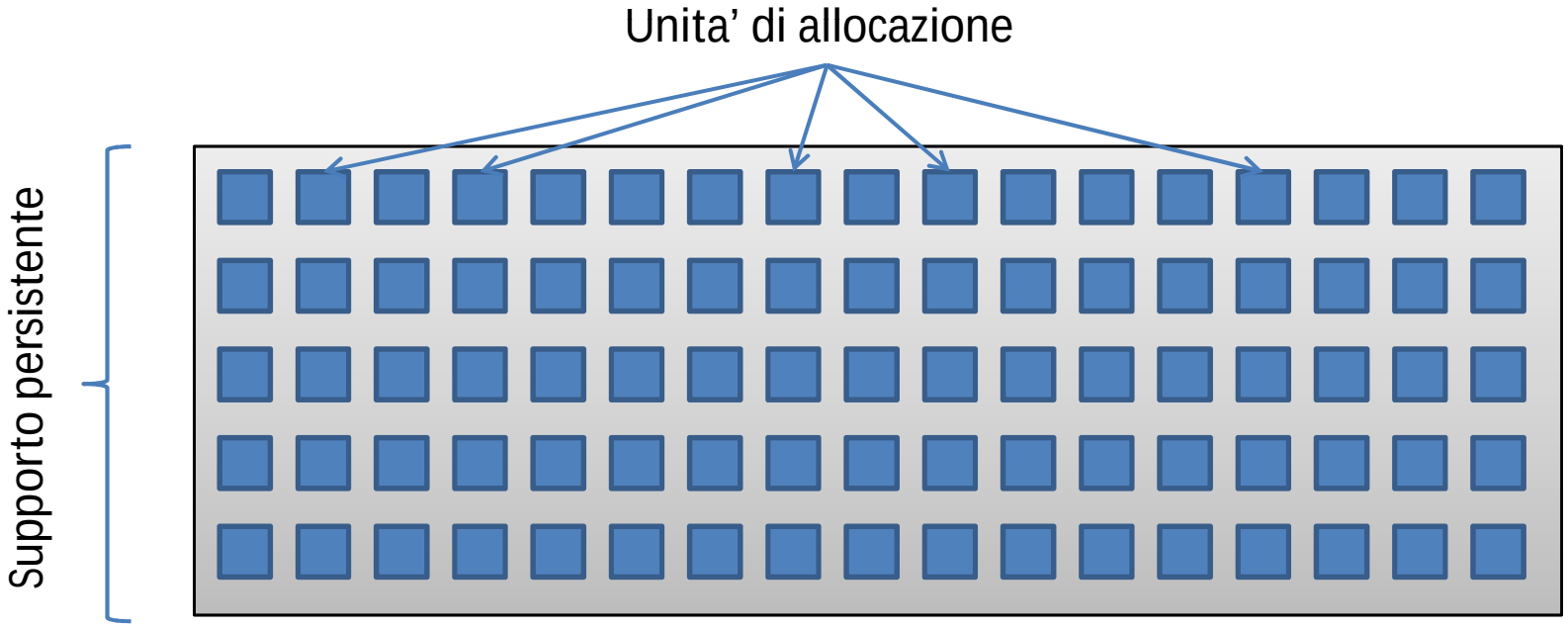
- Per assumere valore probatorio, l'evidenza digitale deve essere:
  - *Integra*: non devono esserci alterazioni negli artefatti
  - *Autentica*: la provenienza degli artefatti deve essere certa
  - *Vera*: l'interpretazione degli artefatti e delle azioni che ne hanno determinato la comparsa deve essere corretta
  - *Completa*: deve essere ottenuta mediante l'analisi di tutti gli artefatti ad essa riferibili

Artefatti digitali: immaterialita’ e fragilita’

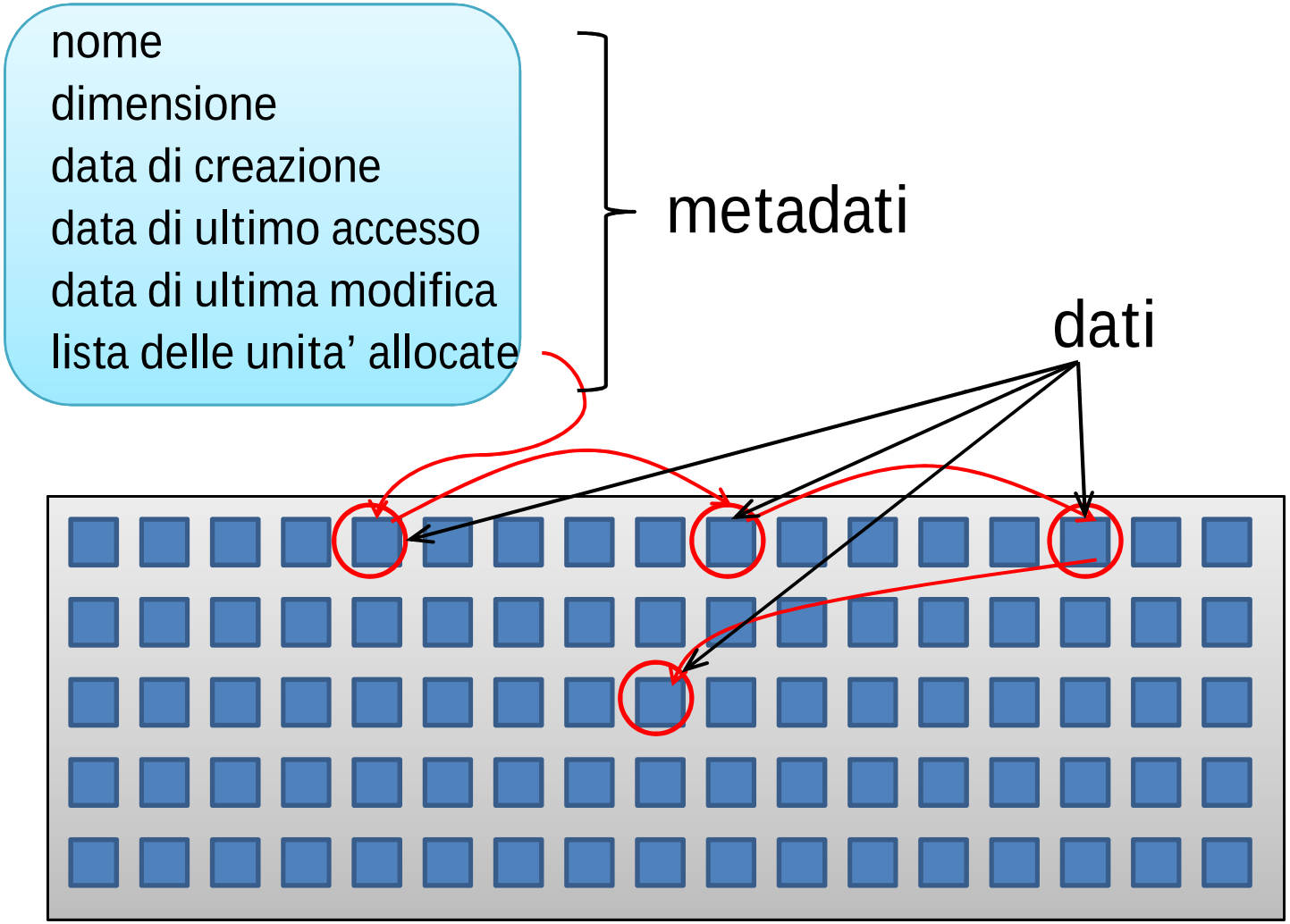
- Gli artefatti digitali sono:
  - *immateriali:*non esistono come oggetto fisico, ma consistono in *sequenze di bit* memorizzate su dei *dispositivi di memorizzazione dati*
  - *fragili* : sono facilmente alterabili nel caso in cui il dispositivo che li contiene sia maneggiato in modo inappropriato
- La fragilitá impone l’uso di particolari precauzioni quando si accede ai dispositivi di memorizzazione

Supporti, file system e file

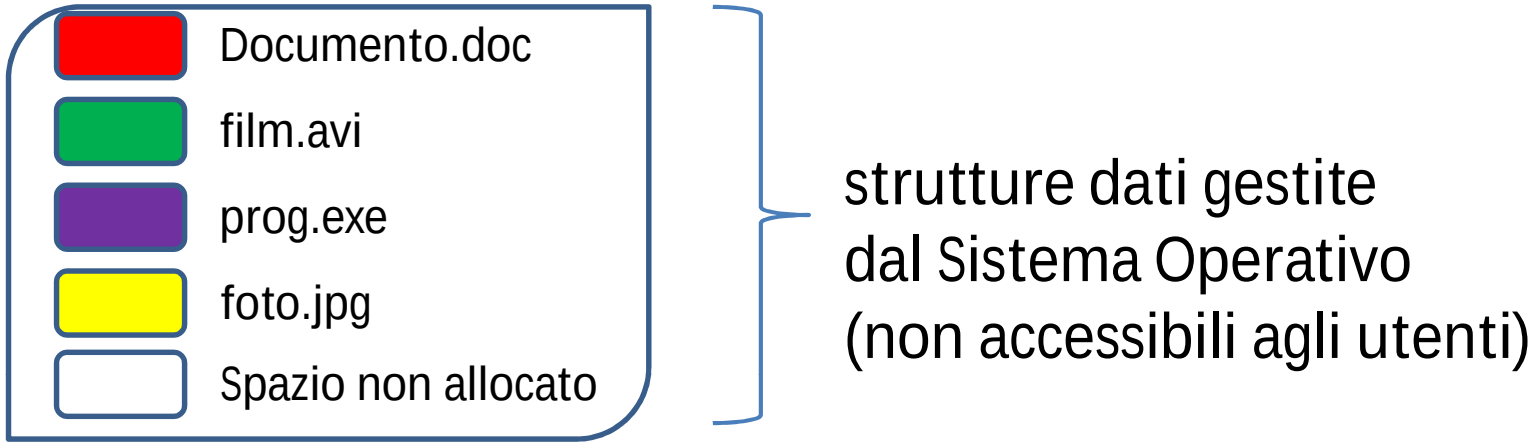
- I supporti persistenti (hard disk, CD/DVD-ROM, pendrive, nastri, ecc.) sono in genere *formattati*, ovvero strutturati logicamente in modo da memorizzare i dati in forma di *file*

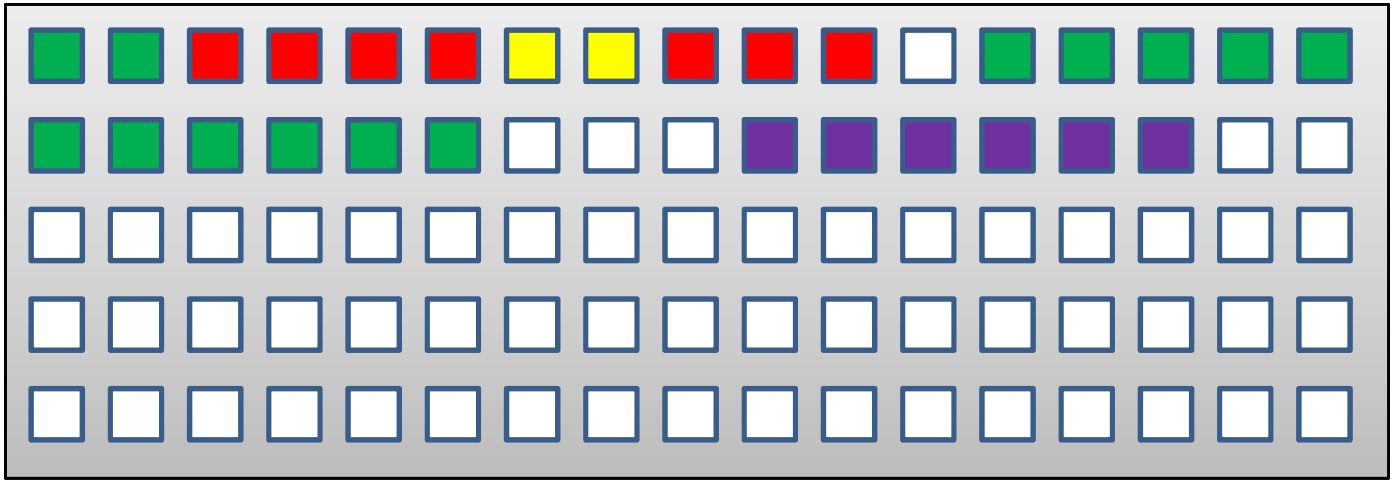


Il concetto di *file*

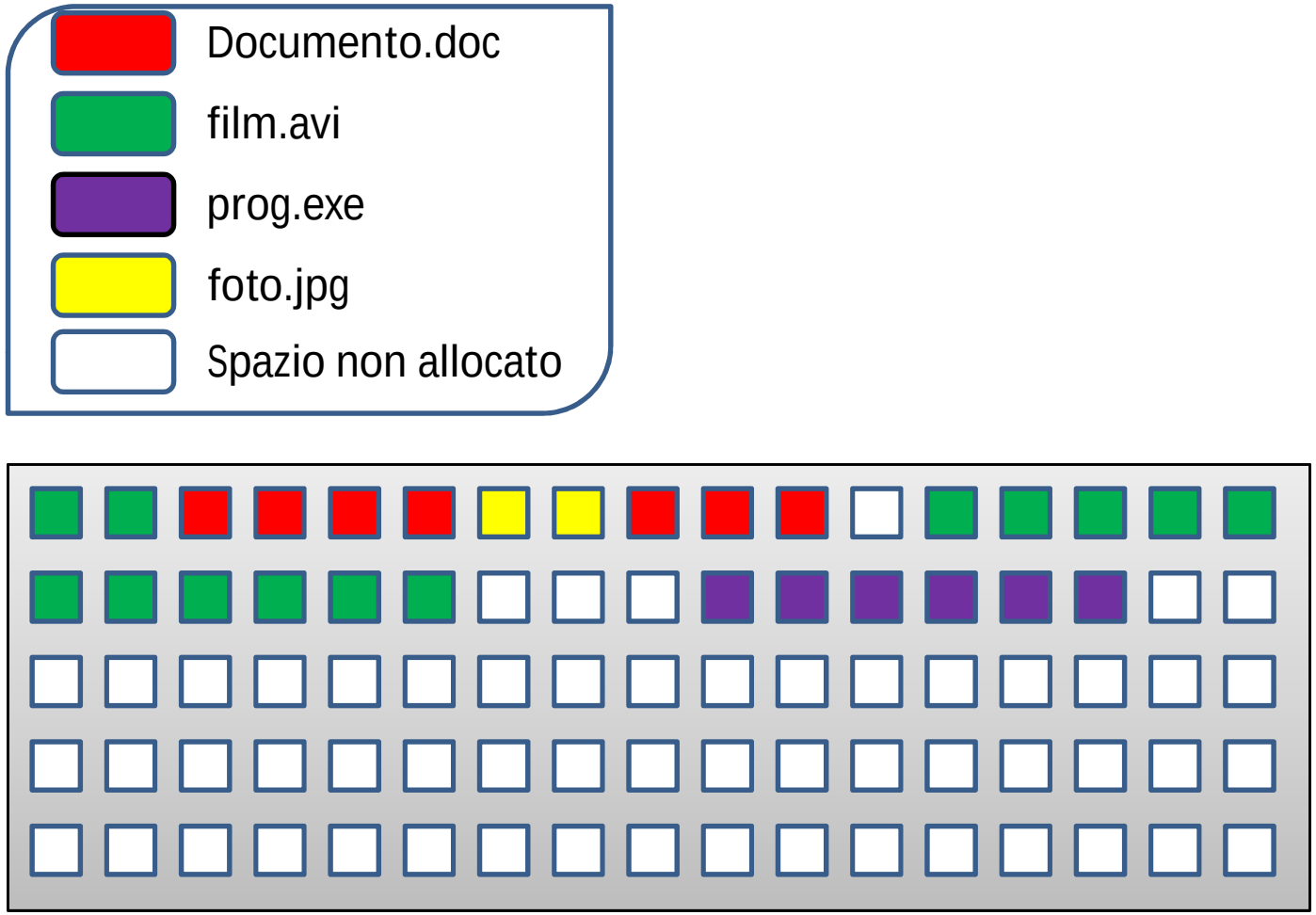


Il concetto di *file system*

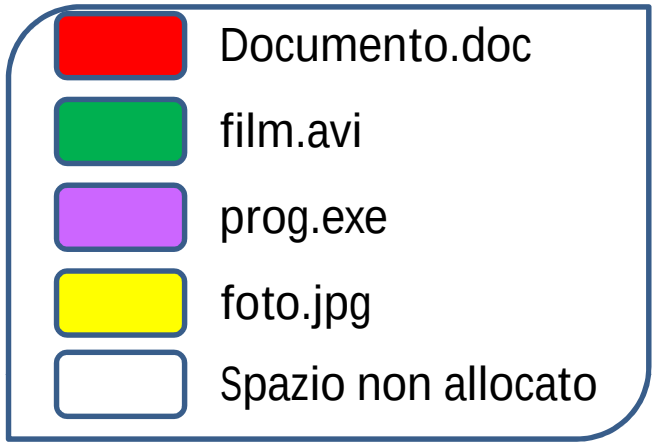




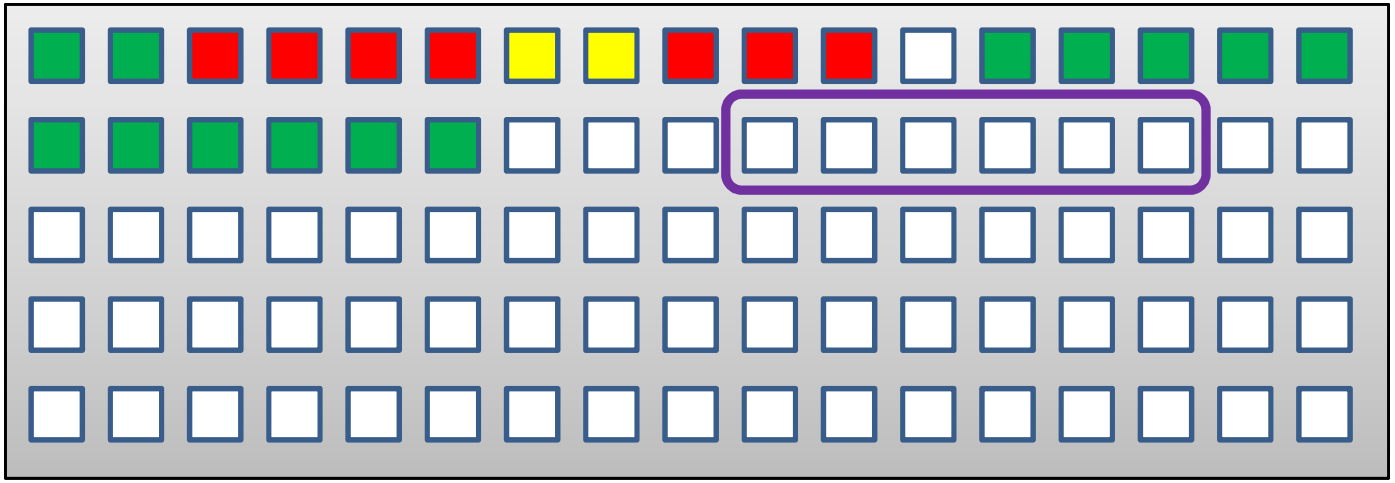
La cancellazione dei file (1)



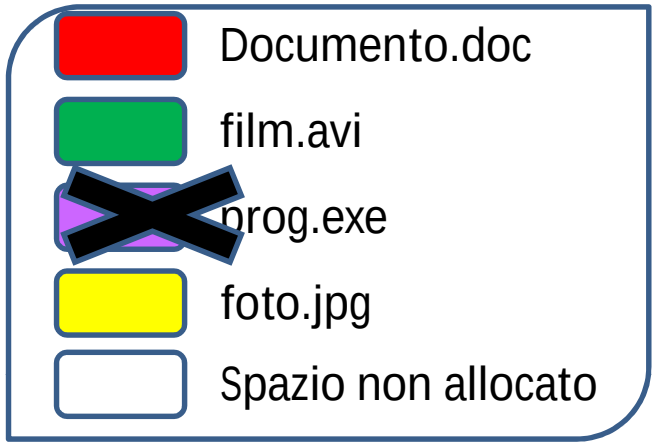
La cancellazione dei file (2)



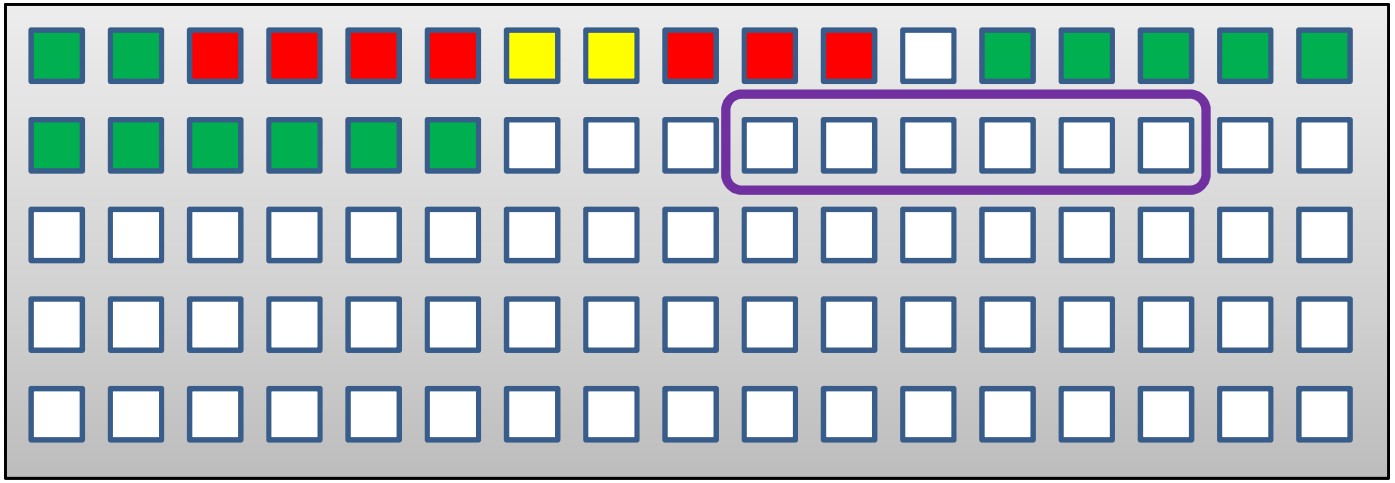
Se i metadati relativi al file non sono stati cancellati, vi e' ancora traccia di quali blocchi erano allocati al file: e' possibile recuperare sia i metadati che i dati di un file cancellato



La cancellazione dei file (3)



Se invece i metadati sono stati cancellati, si possono recuperare i dati (ma non le proprieta' del file) mediante tecniche opportune



Compromissione dell'integrita'

- L'accensione ed utilizzo di un computer (puo') comporta(re)
  - Creazione di nuovi file
    - Sovrascrittura di aree non allocate
    - Sovrascrittura di metadati relativi a file cancellati
  - Modifica del contenuto di file esistenti
    - Alterazione di dati e metadati del file
    - Sovrascrittura di aree non allocate (se si aggiunge contenuto)
  - Accesso in lettura a file
    - Alterazione della data di ultimo accesso

Come garantire l'integrita'?

- E' necessario utilizzare di metodologie e strumenti in grado di garantire *in modo dimostrabile* che l'evidenza non e' stata modificata durante l'analisi
- Regola fondamentale: le operazioni di analisi vanno effettuate su copie identiche dei dispositivi originali
  - E' possibile comunque la cosiddetta "preview" se effettuata in modalita' di "sola lettura"

Acquisizione dei dispositivi

- L'operazione di copia viene denominata *acquisizione* al termine della quale viene prodotto un *file di immagine* (*copia forense*) contenente una copia di tutti i bit memorizzati nel dispositivo
  - Il requisito di completezza impone l'acquisizione di *tutte le aree del dispositivo*, e non solo i file allocati

Come impedire modifiche dei dati?

- Il supporto da acquisire deve essere collegato ad un sistema di acquisizione mediante un “write blocker” (dispositivo che blocca le operazioni di scrittura)

Come certificare i contenuti ?

- Calcolo del *codice hash* relativo all'intero supporto incluse aree non allocate ad alcun file, o non assegnate ad alcuna partizione

Algoritmo di hash crittografico

60d683e2eba7c242e3f46fe5eba979af

Proprieta’ dei codici hash (1)

- Proprieta’ 1: due sequenze di input identiche danno luogo allo stesso codice hash
- Se i codici hash di originale e copia differiscono, si puo’ concludere con certezza che i rispettivi contenuti sono a loro volta differenti

Proprieta' dei codici hash (2)

- *Proprieta' 2: la probabilita' che sequenze di input diverse diano luogo allo stesso codice hash e' praticamente nulla*
- Se i codici hash di originale e copia sono identici, si puo' ritenere che i relativi contenuti siano identici con altissima probabilita'

Proprieta’ dei codici hash (3)

- Alcuni esempi relativi ai due algoritmi di hash piu’ diffusi in informatica forense
  - MD5: Probabilita’ di collisione pari a 1 su piu’ di 18 miliardi di miliardi
  - SHA1: Probabilita’ di collisione pari a 1 su piu’ di 1200 miliardi di miliardi

Proprieta’ dei codici hash (4)

- In ogni caso, tali sequenze sarebbero con altissima probabilita’ molto diverse tra loro
- In altre parole, non e’ ancora noto un metodo computazionalmente fattibile che permetta di produrre una variante leggermente diversa del contenuto di un supporto che abbia pero’ lo stesso codice hash

Codici hash ed utilizzabilita’ (1)

- Se i codici hash di originale e copia differiscono e’ ancora possibile utilizzare le tracce digitali contenute nel supporto, oppure esse diventano inammissibili in quanto la loro integrita’ e’ stata compromessa?
- Si, se e’ possibile individuare quali file e/o aree dati differiscono

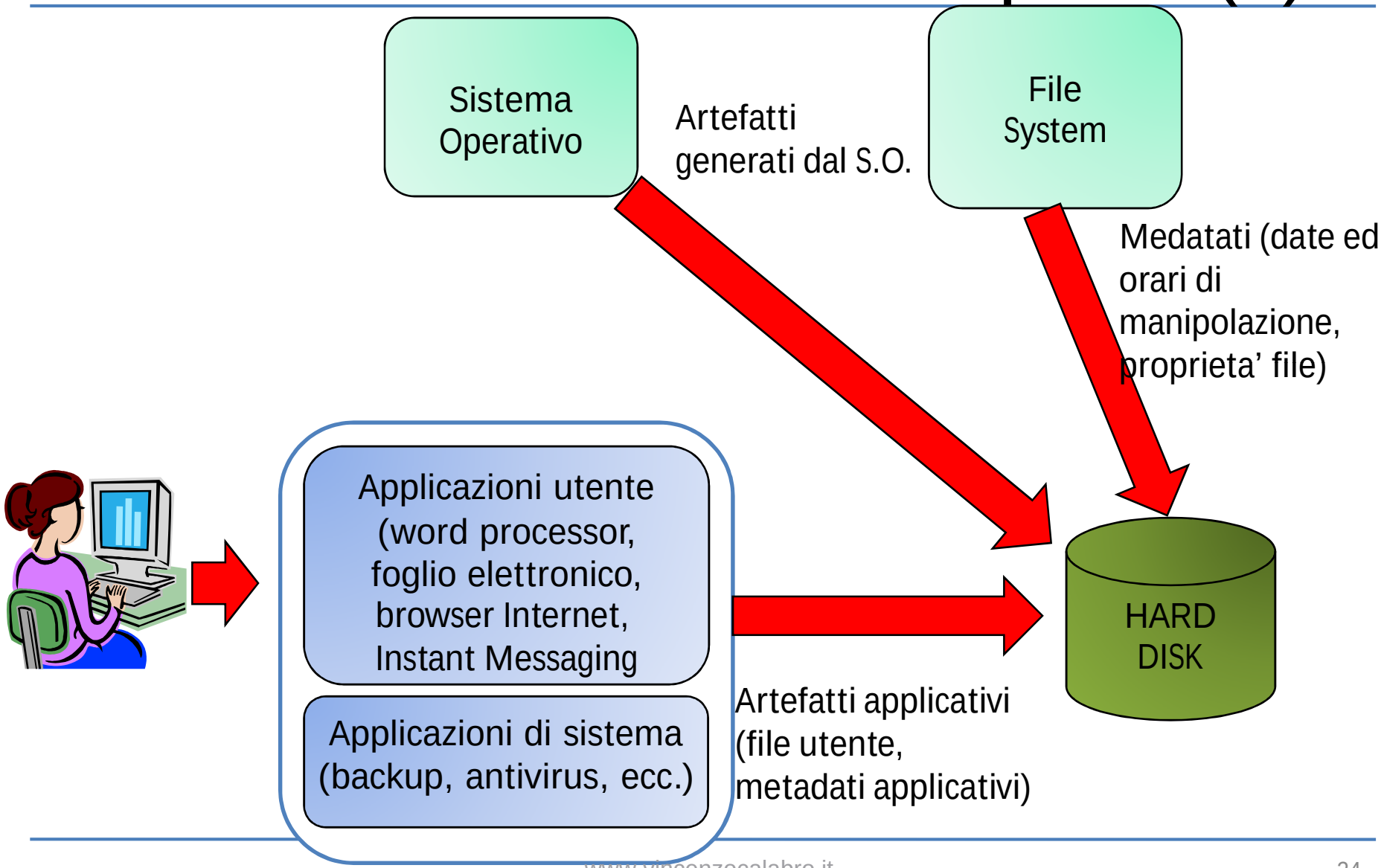
Codici hash ed utilizzabilita’ (2)

- In fase di acquisizione, oltre all’hash dell’intero supporto si calcola l’hash anche di tutti i file memorizzati su di esso
- In caso di discrepanza dei valori di hash riferiti all’intero supporto, si procede a controllare gli hash dei singoli file in modo da identificare i file che hanno subito modifiche

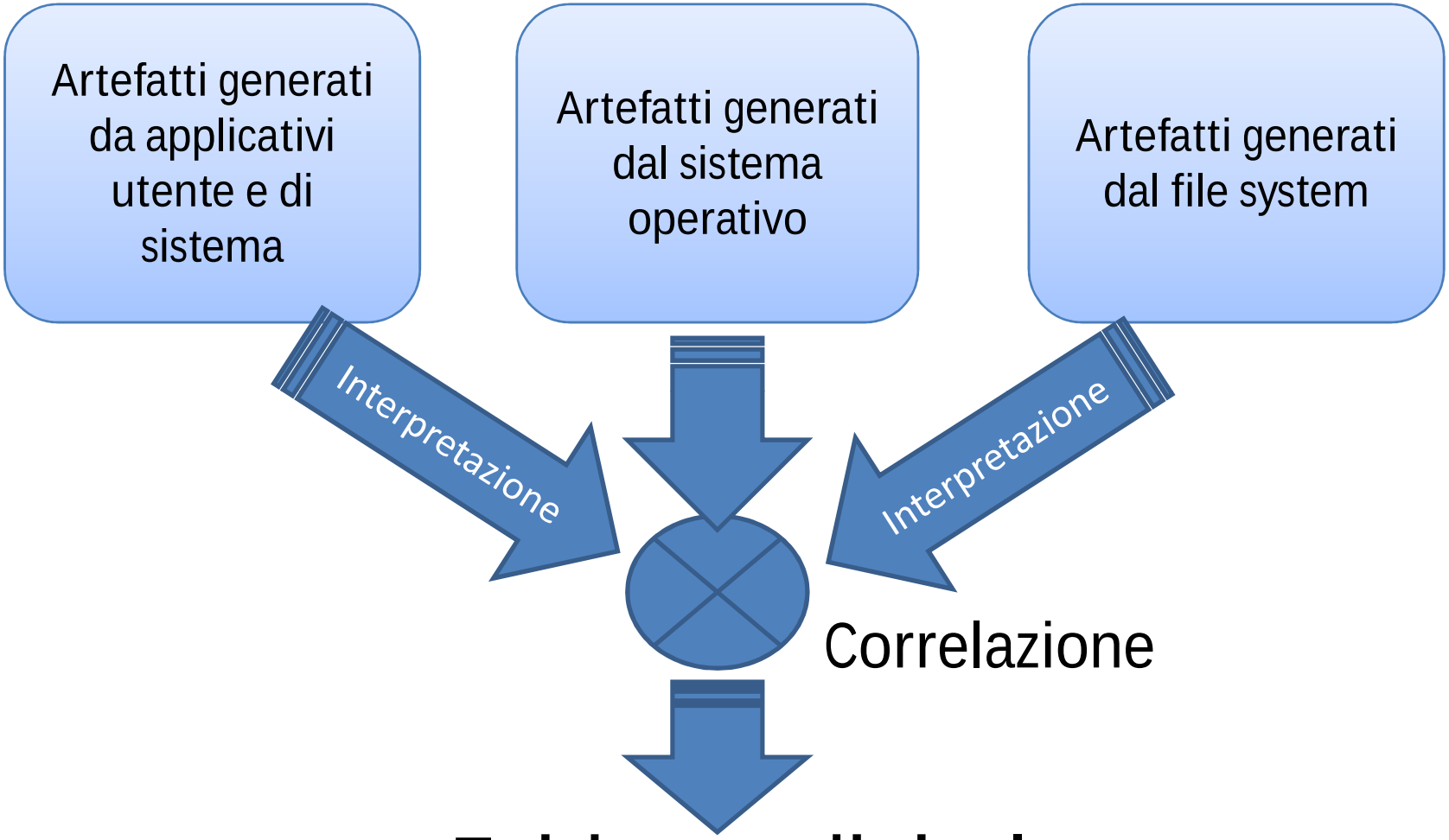
Analisi forense di un computer (1)

- Ricostruzione delle attivitá che hanno determinato lo stato del computer con l’obiettivo di individuare elementi di prova che concorrano a dimostrare o confutare dei fatti

Analisi forense di un computer (2)



Analisi forense di un computer (3)



Operazioni preliminari

- Recupero di file cancellati o loro frammenti
- Filtraggio dei file irrilevanti
- Individuazione di file potenzialmente rilevanti
  - ricerca con parole chiave
  - Individuazione di file che l'utente ha cercato di occultare
  - ...

Ricostruzione delle attivita’

- Necessaria per determinare con certezza la provenienza e le azioni che hanno determinato la comparsa degli artefatti di interesse

Costruzione della *timeline*

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

Metadati dei file (1)

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

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

Metadati dei file (1)

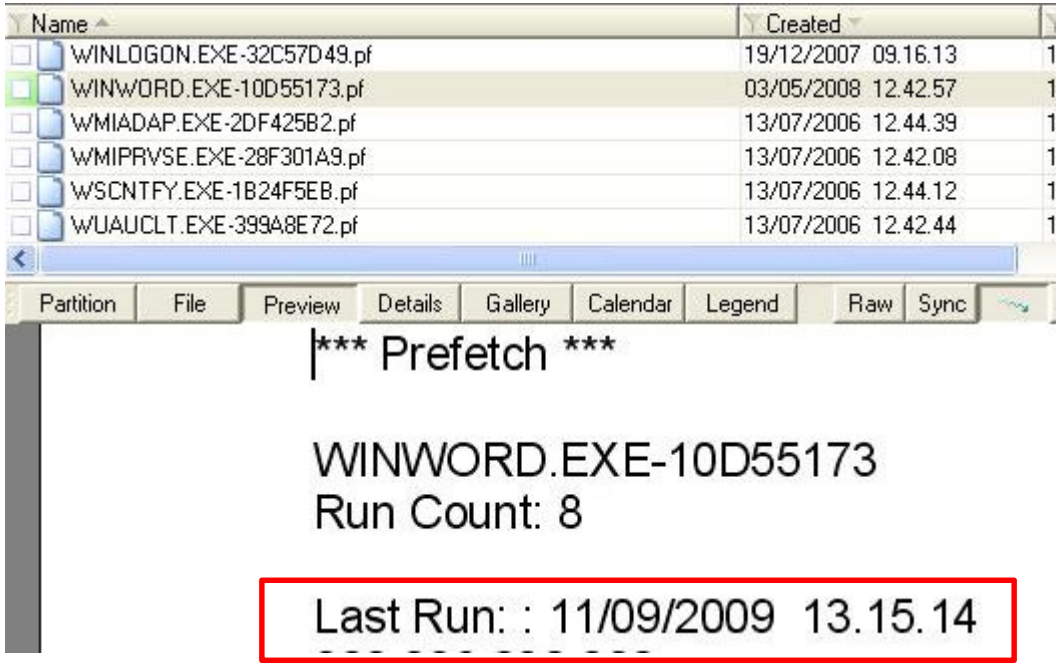
Data / Ora	Evento	Oggetto
02/05/2008 09.31.15	Creazione file	Parte1.doc
02/05/2008 09.31.15	Creazione file	Parte2.doc
04/05/2008 12.32.04	Modifica – Accesso file	Parte1.doc
04/05/2008 12.32.04	Modifica – Accesso file	Parte2.doc
05/05/2008 21.36.33	Creazione – Modifica file	DocumentoImportante.doc
06/05/2008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

Esecuzione di programmi (1)

- Il sistema operativo registra varie informazioni relative all'esecuzione dei programmi, che possono contenere informazioni temporali relative alle varie esecuzioni

Esecuzione di programmi (2)

- File speciali (“prefetch”) creati dal sistema operativo Windows



Esecuzione di programmi (3)

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

Comandi eseguiti dagli utenti (1)

- Il Sistema Operativo tiene spesso traccia della sequenza di comandi eseguiti da ciascun utente, associandovi anche data ed ora delle esecuzioni (o dell'ultima di esse)

Comandi eseguiti dagli utenti (2)

- 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

Comandi eseguiti dagli utenti (3)

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

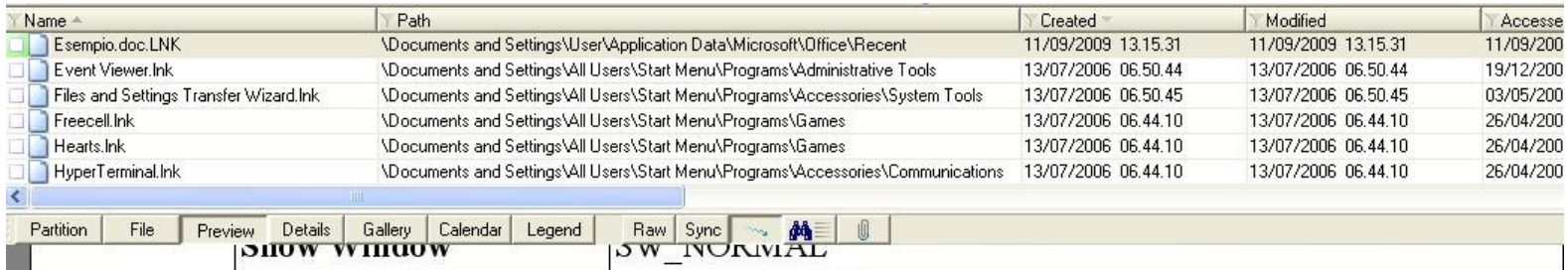
- L’utente “*User*” ha avviato WINWORD.EXE pochi secondi prima che fosse creato il file ‘Esempio.doc’

Artefatti generati da programmi (1)

- Alcuni programmi generano artefatti ad ogni loro esecuzione
  - Elenco file aperti recentemente
  - File di cronologia della “navigazione” su Internet
  - File di log (ad esempio, gli antivirus)

Artefatti generati da programmi (2)

- 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

Artefatti generati da programmi (3)

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

Artefatti generati da programmi (4)

- 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

Cronologia di navigazione Internet (1)

- 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

Cronologia di navigazione Internet (2)

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

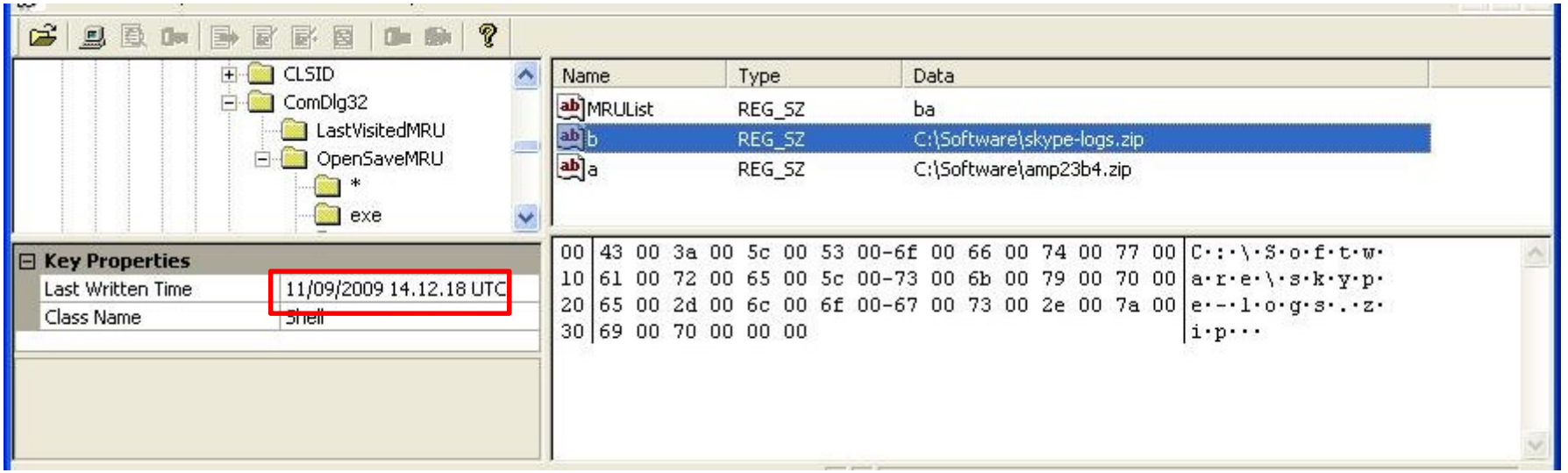
- '*User*' ha scaricato 'skype-logs.zip' da un account WebMail prima che la cartella in questione fosse creata

Operazioni di salvataggio file (1)

- Il sistema operativo Windows registra le ultime 10 operazioni di salvataggio di file
  - Nome del file salvato
  - Cartella in cui il file viene salvato
  - Data ed ora del salvataggio

Operazioni di salvataggio file (2)

- Artefatti nel registro di Windows relativi al salvataggio di file



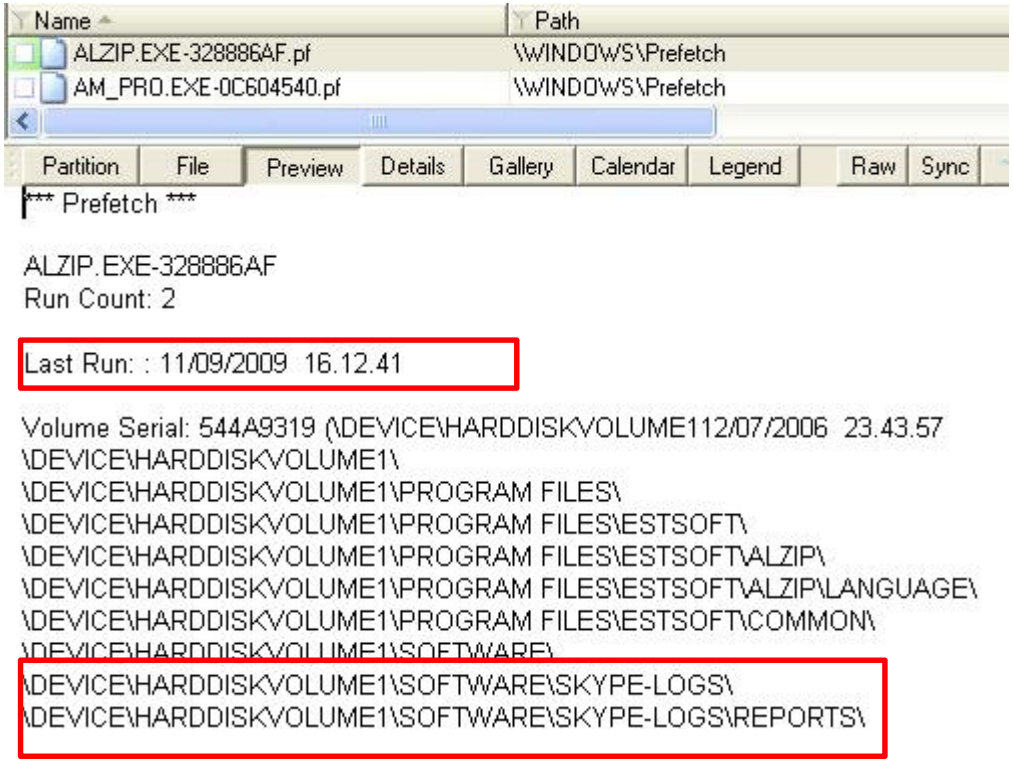
Operazioni di salvataggio file (3)

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

Esecuzione di programmi (1)

- Nome del programma, data ed ora di ultima esecuzione

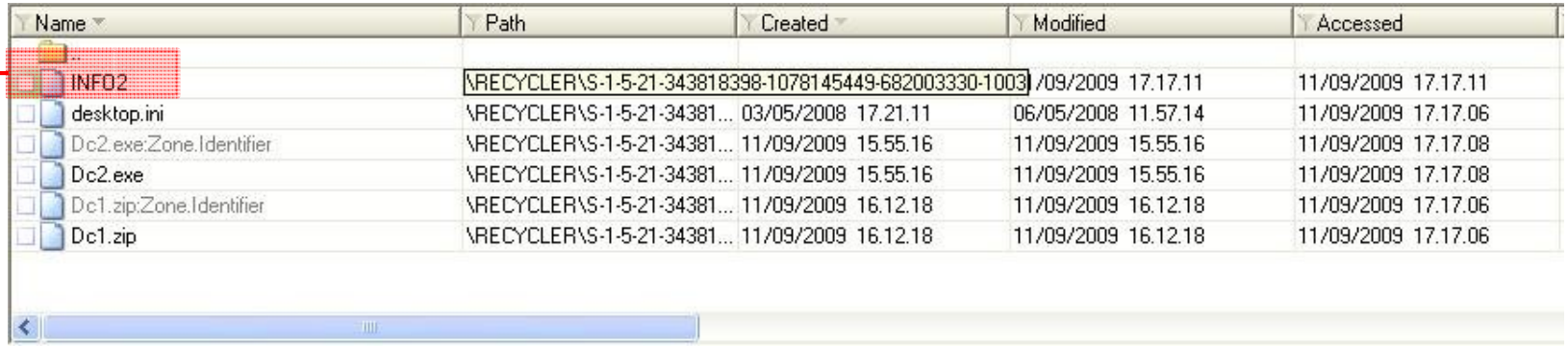


Esecuzione di programmi (2)

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

Cancellazione di file (1)

- 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

Cancellazione di file (2)

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

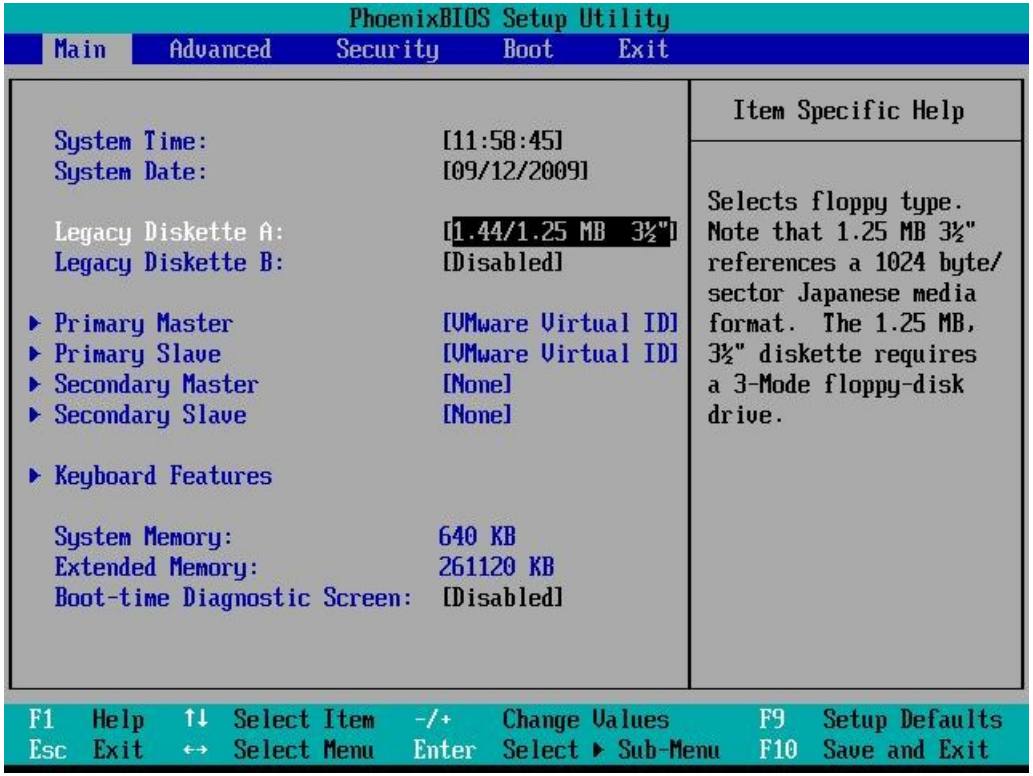
- Dopo aver decompresso skype-logs.zip, ‘*User*’ lo ha cancellato spostandolo nel Cestino

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)

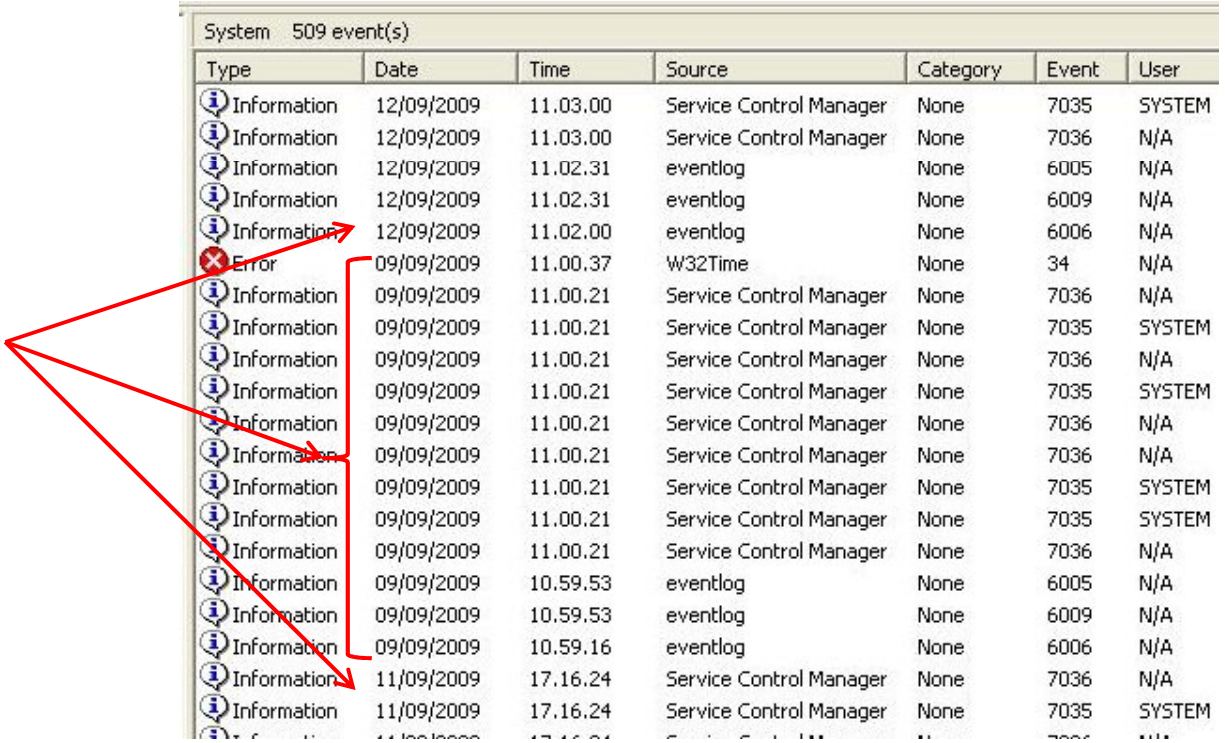
- All’atto dell’acquisizione (o del sequestro) annotare le impostazioni del BIOS relative ad ora e data del computer



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)

- É comunque possibile alterare i timestamp di singoli file senza dover alterare l'orologio di sistema
- Queste manomissioni possono essere rilevate mediante l'analisi di metadati non visibili agli utenti

Correttezza dei timestamp (5)

- *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

Metadati applicativi

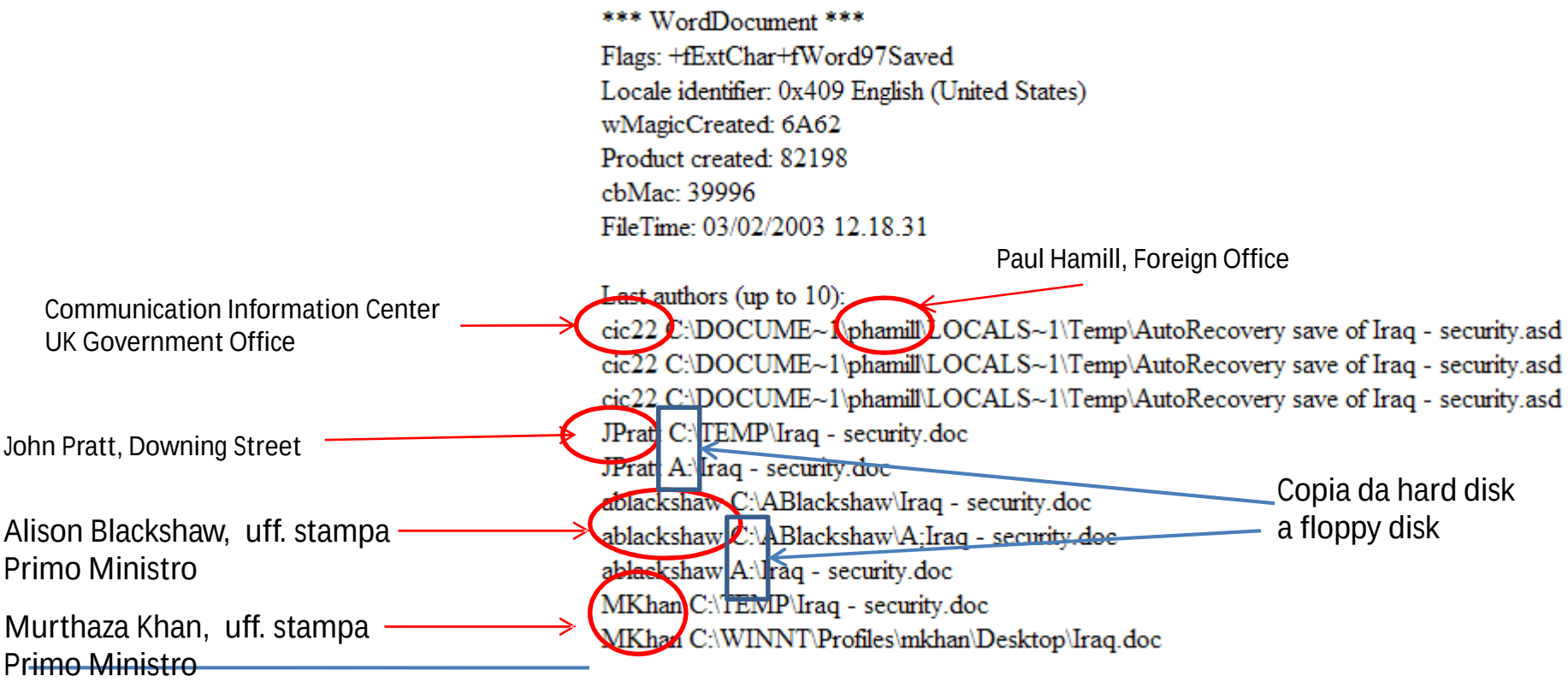
- Molte applicazioni memorizzano, spesso all'insaputa dell'utente, informazioni di varia natura (metadati) nei file prodotti mediante di esse
- Questi medatati non sono normalmente visibili all'utente, ma possono essere estratti dai programmi di analisi forense e possono fornire molte informazioni utili ai fini probatori

Metadati applicativi: MS Office (1)

- Il 30/1/2003, il governo inglese pubblico' su un proprio sito web un dossier sulla struttura delle organizzazioni di intelligence e sicurezza irachene, che fu citato da Colin Powell nella sua relazione all'Assemblea delle Nazioni Unite il 5/2/2003
- Il Dr. G. Rangwala (U. Cambridge) si accorse che il dossier era stato in larghissima parte copiato da un articolo di un ricercatore del Monterey Institute of International Studies in California (e pubblicato su una rivista scientifica) senza citare la fonte

Metadati applicativi: MS Office (2)

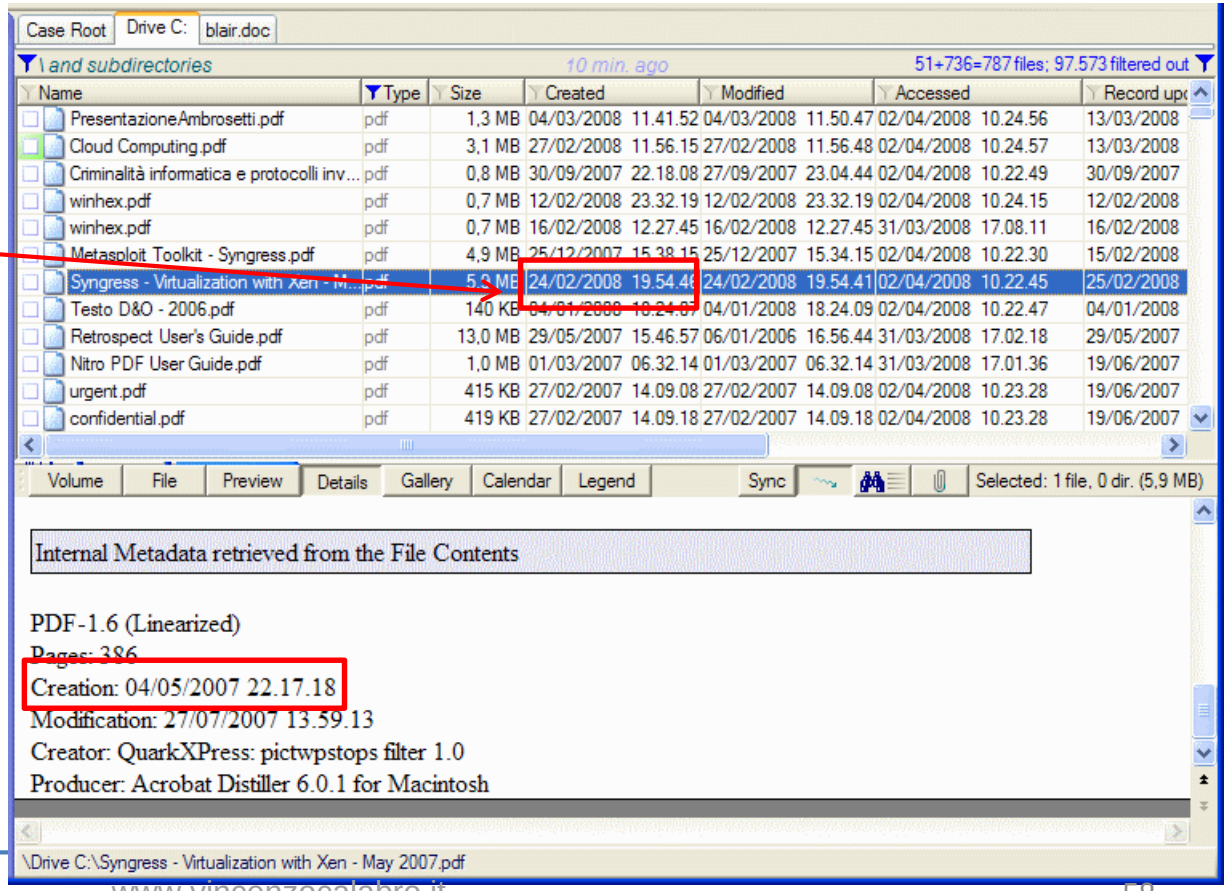
- L'analisi dei metadati del documento Word (pubblicato da Downing Street) ha permesso di identificare gli autori del plagio



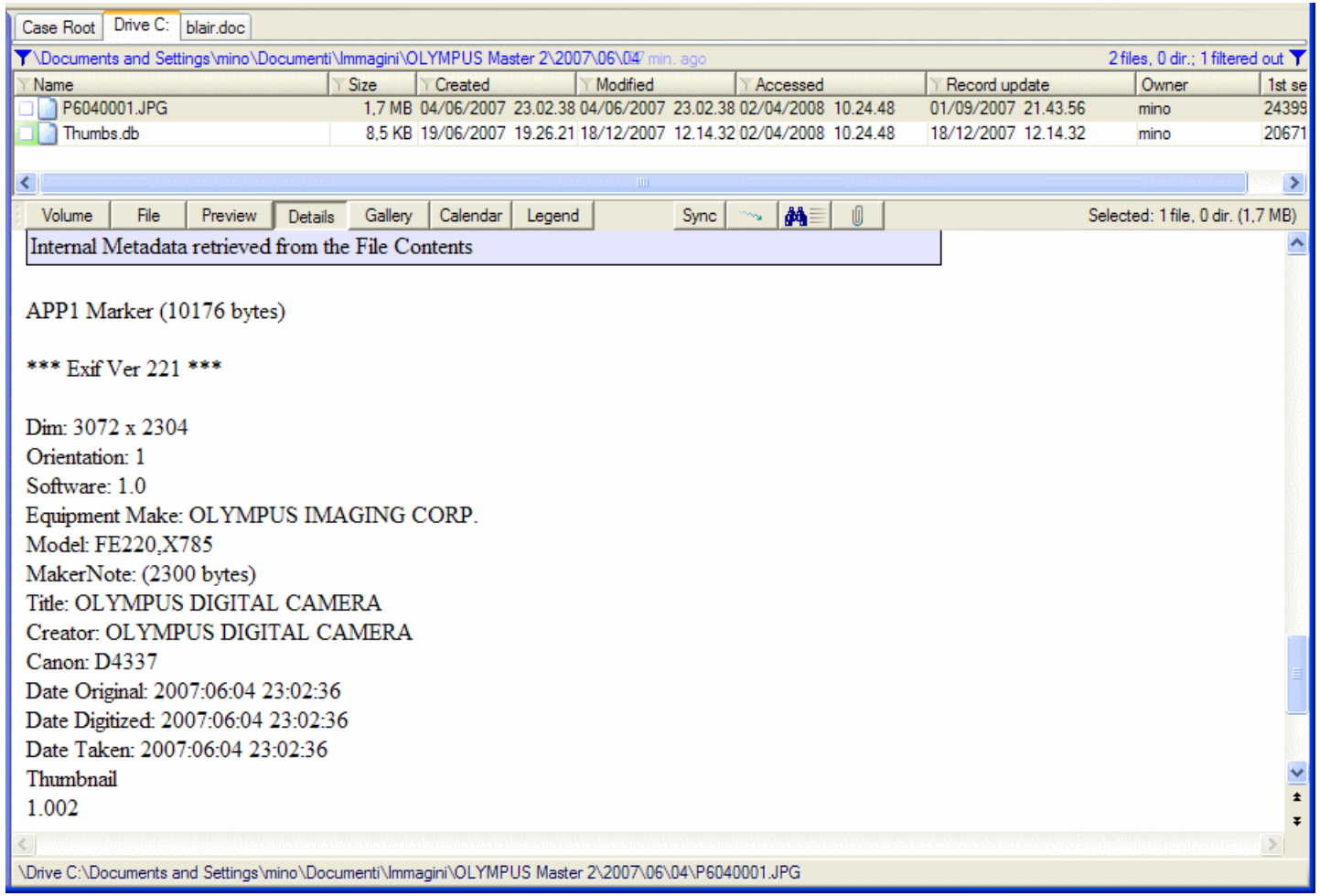
Metadati applicativi: file PDF

- I metadati sono presenti anche nei file PDF

La differenza indica che il documento e' stato creato su un altro computer e poi trasferito



Metadati applicativi: file immagine



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)

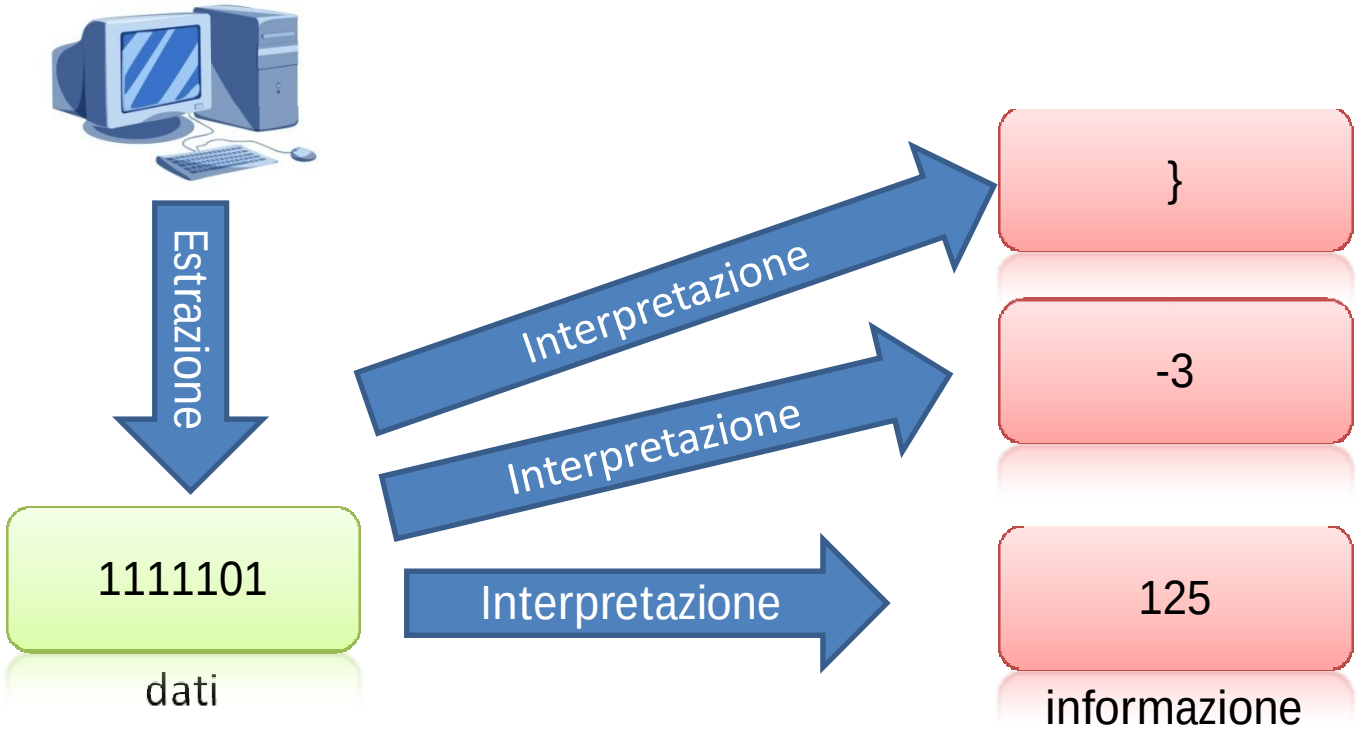
- Analisi del contenuto della memoria
  - tecnica relativamente recente
  - salvataggio del contenuto della memoria del computer su apposito supporto esterno
  - decodifica ed analisi del suo contenuto
- Vantaggi rispetto all'analisi live:
  - congelamento dello stato della memoria volatile
  - ripetibile 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' dell'evidenza digitale (1)

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



Veridicita’ dell’evidenza digitale (2)

- Necessita’ di verificare sperimentalmente l’interpretazione degli artefatti e la sequenza di eventi/azioni che li hanno generati
  - Sperimentazione da effettuarsi in condizioni operative identiche o simili a quelle del sistema analizzato
  - I risultati della sperimentazione devono essere riproducibili

Veridicita’ e validazione degli strumenti

- Strumenti software utilizzati in fase di analisi
  - Semplificano ed automatizzano i processi di decodifica, ricerca e correlazione degli artefatti
  - Come tutti i sistemi software complessi, possono essere affetti da vari problemi e/o errori
- L’analista dovrebbe sempre validare i propri risultati utilizzando il metodo scientifico, al fine da escludere al presenza di errori

Ammissibilitá dell'evidenza

- "*With miracles, any sort of evidence will suffice; facts require proof*"(M. Twain)
- Quali sono i criteri di ammissibilitá dell'evidenza digitale?
- Negli Stati Uniti, viene impiegato il cosiddetto "test di Daubert"

Il test di Daubert

- Valuta l'ammissibilitá sulla base delle seguenti caratteristiche:
  - Verifica sperimentale della teoria scientifica o la tecnica applicata
  - Peer-review e pubblicazione della teoria/tecnica
  - Conoscenza della probabilitá di errore (nota o potenziale)?
  - Qualifica e reputazione dell'esperto nella comunitá scientifica

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

Approfondimenti

V. Calabrò, P. Dal Checcho, B. Fiammella

La Timeline: Aspetti tecnici e rilevanza processuale

IISFA Memberbook 2011