

# **Appunti del corso di Digital Forensics**

A.A. 2021/2022

# Indice

<b>1</b>	<b>Introduzione</b>	<b>6</b>
1.1	Digital forensics . . . . .	6
1.1.1	Ramificazione della Digital forensics . . . . .	6
1.1.2	I Passi Fondamentali di un Esame Forense . . . . .	7
1.2	Cyber crimine . . . . .	7
1.2.1	Evoluzione dei cyber crimini . . . . .	7
1.3	Investigazione forense . . . . .	8
1.3.1	Fase di indentificazione . . . . .	8
1.3.2	Fase di raccolta . . . . .	11
1.3.3	Ispezione . . . . .	13
1.3.4	Analisi . . . . .	13
1.3.5	Presentazione . . . . .	14
1.4	Distribuzioni Linux per la Digital Forensics . . . . .	14
1.4.1	DEFT Linu . . . . .	14
1.4.2	CAINE . . . . .	14
1.4.3	Parrot Security Linux . . . . .	14
1.4.4	Kali Linux . . . . .	14
<b>2</b>	<b>Acquisizione dei Dati</b>	<b>15</b>
2.1	Concetti di Base . . . . .	15
2.2	Bloccare le Scritture . . . . .	15
2.2.1	Write Blocker Software . . . . .	16
2.2.2	Write Blocker Hardware . . . . .	16
2.3	Immagini Forensi . . . . .	16
2.3.1	Duplication . . . . .	16
2.3.2	Imaging . . . . .	17
2.3.3	Correttezza Duplication e Imaging . . . . .	17
2.3.4	Categorie formati immagini fornisi . . . . .	17
2.4	Il tool DC3DD . . . . .	18
2.4.1	Supporti di Memorizzazione e Partizioni su Linux . . . . .	19
2.4.2	Mantenere la Prova Integra . . . . .	19
2.4.3	Comandi utilizzio DC3DD . . . . .	19
2.4.4	Processo di Clonazione . . . . .	19
2.4.5	Pulizia Forense . . . . .	20
2.5	Il tool Guymager . . . . .	20
2.5.1	Immagini Forensi e Live System . . . . .	20
2.6	Utilizzo di DC3DD su dispositivi Android-based . . . . .	21
2.6.1	Permessi di Root e Accesso a tutte le Partizioni . . . . .	21
2.6.2	Recovery mode e ADB . . . . .	21
2.6.3	Modalità di Acquisizione dei Dati . . . . .	22

2.6.4	Passi Principali per l'acquisizione dei Dati . . . . .	22
<b>3</b>	<b>File Recovery e Data Carving</b>	<b>24</b>
3.1	Recupero tramite Metadati . . . . .	24
3.2	Carving . . . . .	25
3.2.1	Header e footer di un file . . . . .	25
3.3	Slack Space . . . . .	27
3.4	Il tool Foremost . . . . .	27
3.5	Il tool Scalpel . . . . .	29
3.6	Il tool PhotoRec . . . . .	30
3.6.1	Esempio di utilizzo . . . . .	30
3.7	Il tool Bulk Extractor . . . . .	31
3.7.1	Esempio di utilizzo . . . . .	31
<b>4</b>	<b>Alcuni richiami su argomenti dementi</b>	<b>33</b>
4.1	Memoria RAM . . . . .	33
4.2	Memoria Virtuale . . . . .	35
<b>5</b>	<b>Memory Acquisition</b>	<b>36</b>
5.1	Memory Dump e Processo di Memory Acquisition . . . . .	36
5.1.1	Tipologie di memory dump . . . . .	36
5.2	Tool Esterni per la creazione di Memory Dump . . . . .	37
5.2.1	Il tool FTK® Imager® . . . . .	37
5.2.2	Il tool DumpIt . . . . .	37
5.3	Memory Analysis con il Volatility Framework . . . . .	38
5.3.1	Volatility ed i Plugin . . . . .	38
5.3.2	Formati di Memory Dump analizzabili da Volatility . . . . .	38
5.3.3	Profilo del Volatility framework . . . . .	38
5.3.4	Plugin imageinfo . . . . .	39
5.3.5	Categorie di Plugin . . . . .	39
5.3.6	Identificazione di Attività di Rete . . . . .	42
5.3.7	Analisi di librerie DLL (Dynamic Link Library) di Windows . . . . .	43
5.3.8	Informazioni sul Registro di Sistema del S.O. Windows . . . . .	43
5.3.9	Altri plugin . . . . .	44
5.4	Ulteriori Tool Utili . . . . .	45
5.4.1	VMMAP . . . . .	45
5.4.2	Il tool InsideClipboard . . . . .	45
<b>6</b>	<b>Analisi</b>	<b>46</b>
6.1	Il tool Autopsy . . . . .	46
6.1.1	Creazione di un nuovo caso . . . . .	46
6.1.2	Analisi mediante Autopsy . . . . .	48
6.1.3	Riapertura di un Caso . . . . .	49
6.2	Le Super Timeline . . . . .	49
6.2.1	Problemi delle timeline tradizionali . . . . .	50
6.2.2	Tecniche Anti-Forensi per l'alterazione dei Timestamp . . . . .	51
6.2.3	Possibili soluzioni . . . . .	51
6.2.4	Framework Plaso . . . . .	51
6.2.5	Tool di Plaso . . . . .	53
6.2.6	Esempio di utilizzo Super Timeline . . . . .	53
6.2.7	Esempio di Utilizzo 2: Timestamp file Office Open XML . . . . .	54
6.2.8	Esempio di Utilizzo 3 File System + Cronologia Brower Chrome . . . . .	56

---

6.3	Mounting di Immagini Forensi . . . . .	58
6.3.1	Linux . . . . .	58
6.3.2	Windows . . . . .	59
<b>7</b>	<b>Importanza degli Artefatti di Windows</b>	<b>60</b>
7.1	Alcune fonti di artefatti . . . . .	60
7.1.1	Fase di Boot di Windows . . . . .	60
7.1.2	Analisi del Registro di Sistema . . . . .	61
7.2	Analisi del Registro di Sistema . . . . .	65
7.2.1	Tool RegRipper . . . . .	65
7.3	Analisi dei Registri degli Eventi . . . . .	67
7.3.1	Principali categorie di log . . . . .	68
7.3.2	Registro eventi sicurezza . . . . .	69
7.3.3	Il tool Visualizzatore Event . . . . .	69
7.3.4	Esportazione dei Registri . . . . .	69
7.3.5	Il tool FullEventLogView . . . . .	70
7.4	La Cartella Prefetch . . . . .	70
7.4.1	Il tool WinPrefetchView . . . . .	71
7.5	Attività Pianificate di Windows . . . . .	71
7.6	La Cache delle Miniature . . . . .	72
7.6.1	Idee di Base del Funzionamento . . . . .	72
7.7	Il tool Thumbcache Viewer . . . . .	73
7.7.1	Esempio di utilizzo . . . . .	73
7.8	Analisi dei collegamenti . . . . .	75
7.8.1	ExifTool . . . . .	77
7.9	Il cestino virtuale . . . . .	78
7.9.1	RECYCLER . . . . .	78
7.9.2	\$Recycle.Bin . . . . .	78
7.9.3	Tool Rifiuti2 . . . . .	79
7.10	Analisi delle Copie Shadow . . . . .	81
7.10.1	Svantaggi/Limiti . . . . .	81
7.10.2	Il tool ShadowCopyView . . . . .	81
<b>8</b>	<b>Network Forensics</b>	<b>83</b>
8.1	Il tool Xplico . . . . .	83
8.1.1	Esempio di utilizzo . . . . .	84
8.1.2	VoIP . . . . .	85
8.1.3	Protocolli E-mail . . . . .	86
8.2	Acquisizione Traffico di Rete - Wireshark . . . . .	88
8.2.1	Esempio di Utilizzo . . . . .	88
<b>9</b>	<b>Anti-Forensics</b>	<b>89</b>
9.1	Principali categorie per le tecniche anti-forensics . . . . .	89
9.1.1	Nascondere/Eliminare le Evidenze . . . . .	89
9.1.2	Minimizzare le evidenze lasciate dai tools per l'AF . . . . .	91
9.1.3	Sfruttare bug dei tool per l'investigazione forense . . . . .	92
9.1.4	Rilevare l'utilizzo di tool per l'investigazione forense . . . . .	93
9.2	Alcune Contromisure . . . . .	94
9.3	Information Hiding   Cenni e Richiami . . . . .	94
9.3.1	Esempio Didattico 1   Information Hiding in File RTF . . . . .	94
9.3.2	Esempio Didattico 2   Information Hiding in File EXE . . . . .	95

*INDICE*

---

<b>10 Digital Image Forensics</b>	<b>96</b>
10.1 Source Camera Identification (SCI) . . . . .	96
10.1.1 Impronta digitale della camera . . . . .	96
10.1.2 Incastriamo il colpevole . . . . .	97

# Capitolo 1

## Introduzione

### 1.1 Digital forensics

La digital forensics consiste nell'uso di metodi scientificamente provati, per le attività di: conservazione, raccolta, convalida, identificazione, analisi, interpretazione, documentazione e presentazione di dati digitali, derivati da dispositivi informatici, con lo scopo di:

- Semplificare la ricostruzione di eventi criminali o azioni illegali;
- Contribuire ad anticipare le azioni non autorizzate;
- Obiettivo: possibilità di definire operazioni pianificate per evitare tali azioni non autorizzate.

Al centro di ogni investigazione digitale forense, vi sono sicuramente le digital evidence (prove digitali o evidenze digitali).

Una prova digitale è qualsiasi dato digitale, contenente informazioni utilizzabili per supportare o confutare ipotesi di un crimine.

#### 1.1.1 Ramificazione della Digital forensics

La digital forensics si divide in diverse categorie:

- Computer Forensics: è essenzialmente il recupero dei dati rispettando dei vincoli dati dalla legge per rendere le informazioni ammissibili nei procedimenti. I termini digital forensics e cyber forensics sono spesso usati come sinonimi di computer forensics.
- Memory Forensics: si riferisce all'analisi dei dati volatili contenuti all'interno del dump della memoria del computer. I professionisti della sicurezza delle informazioni conducono analisi forensi sulla memoria per indagare e identificare attacchi o comportamenti dannosi che non lasciano tracce facilmente rilevabili sui dati del disco rigido.
- Network Forensics: è un sottoramo della digital forensics relativo al monitoraggio e all'analisi del traffico della rete di un computer ai fini della raccolta di informazioni, prove legali o rilevamento di intrusioni. A differenza di altre aree della scientifica digitale, le indagini di rete si occupano di informazioni volatili e dinamiche.
- Multimedia Forensics: preso un dato digitale multimediale (cioè un'immagine), le tecniche forensi cercano di rispondere a un certo numero di domande forensi relative a:
  - identificazione della fonte (Qual è l'origine dei dati?);
  - verifica integrità/rilevamento manomissioni (I dati hanno subito una modifica? )

## **1. Introduzione**

---

- Mobile Forensics: si occupa di recuperare prove o dati digitali da un dispositivo mobile.
- IoT Forensics: si occupa dei crimini informatici legati all'IoT e comprende l'indagine sui dispositivi connessi, sui sensori e sui dati archiviati su tutte le possibili piattaforme.

### **1.1.2 I Passi Fondamentali di un Esame Forense**

#### **Preservare la Scena del Crimine**

Preservare la scena del crimine è fondamentale ed è importantissimo. Se l'evidenza è contaminata, persa o semplicemente non identificata e/o trascurata, tutto ciò che segue può avere un valore limitato per gli investigatori, i quali mettono insieme le prove del caso.

#### **Riconoscere le Prove**

Riconoscere le prove ed identificarle risulta estremamente rilevante. Individuare i punti in cui cercare può solo migliorare l'esito di un esame forense. Una volta individuate, le prove devono essere raccolte e classificate.

#### **Visione d'Insieme**

Le prove non possono essere viste in maniera isolata. Dovrebbero essere confrontate con altre prove e dovrebbero essere identificate prove «effettive». A tal punto, dovrebbe essere descritte in termini scientifici.

## **1.2 Cyber crimine**

Un cybercrimine è un atto criminale compiuto utilizzando un dispositivo informatico e/o tramite internet. Questo atto trascende i confini nazionali e internazionali e solleva diversi problemi giurisdizionali, che una nazione, da sola, non può mitigare.

### **1.2.1 Evoluzione dei cyber crimini**

#### **I fase '70 - 2000**

Caratterizzata da attacchi diretti contro sistemi e reti.

Obiettivo: Sconfiggere le istituzioni causando il crash di sistemi o causando danni fisici.

Vittime Tipiche: Hardware e istituzioni, NON individuali.

#### **II fase 2000 - ~2019**

Sfrutta punti deboli (ad es., vulnerabilità) della sicurezza del sistema e delle reti.

Obiettivi: Sfruttamento di individui specifici → Vittime Specifiche Il cybercrime diventa PROFITTE-VOLE.

Esempi: Furti di identità, frodi con carte di credito, crimini finanziari, vendette verso persone specifiche, ecc...

#### **III fase ~2019 - futuro**

Questa fase è caratterizzata dalla manipolazione dei social media e dal furto o dall'acquisto di dati personali. Accurata selezione delle vittime in base al loro orientamento politico, istruzione, opinioni e altri fattori che li rendono persuadibili e vulnerabili. Diffusioni fake news, deep fake, fake media, ecc. → aumento dei disordini sociali, cambiamenti nella struttura del potere delle nazioni, ... Transnational cybercime: cybercrime finanziario, cyberwarfare, frodi online, ecc...

## 1.3 Investigazione forense

Il processo di investigazione è articolato in cinque fasi principali consecutive:



- Identificazione del crimine e di fonti contenenti potenzialmente prove digitali;
- Raccolta (o acquisizione) di dati raw («grezzi»), copiandoli, in maniera opportuna, dai dispositivi digitali;
- Ispezione (examination) dei dati raccolti con l'obiettivo di realizzarne una struttura migliore ai fini dell'analisi e della comprensione;
- Nella fase di analisi si cerca di ottenere una migliore comprensione e si cerca di determinare i fatti di un evento o un'azione illegale;
- Le prove digitali, individuate nelle fasi precedenti, vengono adeguatamente presentate nei tribunali e/o negli enti preposti.

### 1.3.1 Fase di identificazione

L'identificazione è una fase estremamente importante, poiché vengono identificate informazioni o fonti di informazioni. Si identificano quindi anche i dispositivi informatici che potrebbero contenere prove digitali, ad esempio: Computer desktop, Laptop/Notebook/PC 2-in-1, Tablet, Supporti di memorizzazione rimovibili, Penne USB, CD/DVD, ecc.

Una corretta pianificazione e preparazione delle attività è una precondizione per una investigazione efficace ed efficiente. La scelta degli strumenti e delle tecnologie da impiegare è strettamente dipendente dalla disponibilità di risorse, ecc. La solidità legale dei suddetti strumenti deve essere preventivamente valutata, in quanto essi devono supportare i principi di integrità. Nelle scene in cui sono presenti dispositivi informatici, è necessario effettuare una fase di preparazione, in cui si configurano adeguatamente hardware e software specifici per l'analisi forense.

#### First responder

Nel momento in cui viene scoperto o sospettato un crimine, dovrebbe esserci un first responder (letteralmente, primo soccorritore), il quale deve allertare gli investigatori forensi e convocarli sulla scena del crimine. In generale, il primo soccorritore ha competenze/conoscenze in relazione alle infrastrutture informatiche (reti, sistemi operativi, ecc.). Fra i primi soccorritori possiamo individuare:

- Amministratori di Sistema;
- Amministratori di Rete;
- Amministratori/Responsabili della Sicurezza Informatica;
- Manager IT.

## *1. Introduzione*

---

Se il primo soccorritore non dovesse avere competenze sufficienti, dovrà comunque mettere in sicurezza i dati, le periferiche, i supporti di memorizzazioni, ecc. In questo modo non verranno utilizzati, alterati o rimossi da soggetti non autorizzati. Fra i doveri del primo soccorritore troviamo:

- Effettuare le prime valutazioni;
- Documentare la scena e la stanza integralmente: il centro della stanza diviene il punto focale della descrizione;
- Assicurare la scena da soggetti non autorizzati;
- Preservare e/o impacchettare i dispositivi per il trasporto.

### **Documentazione e Preservazione delle Prove**

La documentazione della scena dovrebbe essere effettuata dal primo soccorritore, al fine di fornire maggiore supporto agli investigatori. La documentazione dovrebbe includere fotografie, video, registrazioni audio dei seguenti oggetti:

- Stanza dove è allocato il dispositivo
- Scrivania, entrata/uscita, finestre, prese elettriche, ecc.
- Stato del dispositivo
- Acceso/spento/luce di accensione lampeggiante
- Contenuto dello schermo (se il device è avviato)
- Libri, annotazioni, pezzi di carta
- Cavi connessi e cavi non connessi

Il primo soccorritore dovrebbe avere con sé diversi strumenti al fine di svolgere adeguatamente la documentazione e la preservazione delle stesse: Vestiti e occhiali protettivi, Braccialetti anti-statici, Etichette, adesivi, ecc.

### Chain of Custody (Catena di Custodia)

È necessario tracciare lo stato di una prova (una volta identificata) e la relativa responsabilità in qualsiasi momento della sua esistenza. Per ciascuna prova devono essere documentati: dove, quando e da chi è stata scoperta e acquisita, dove, quando e da chi è stata custodita o analizzata, chi l'ha avuta in custodia e in quale periodo, come è stata conservata. Ad ogni passaggio di consegna, deve essere specificato dove, come e tra chi è stata trasferita (da qui, chain of custody o catena di custodia o, abbreviato, CoC).

Gli accessi alla prova devono essere estremamente ristretti e chiaramente documentati.

Ogni volta che la prova è affidata ad un nuovo investigatore, nel documento bisogna aggiungere: nome dell'incaricato all'analisi, data e ora di presa in carico del supporto, data e ora di restituzione del supporto.

<b>EVIDENCE</b>		
<b>Sottoposta dall'Ente/Autorità</b>		
<b>Data e Ora dell'Acquisizione</b>		
<b>Numero del Referto</b>		<b>Numero del Caso</b>
<b>Acquisita Da</b>		
<b>Descrizione</b>		
<b>Luogo Acquisizione</b>		
<b>Tipo di Reato</b>		
<b>CHAIN OF CUSTODY</b>		
<b>Ceduta Da</b>		<b>Presa in Custodia Da</b>
<b>Data e Ora</b>		
<b>Ceduta Da</b>		<b>Presa in Custodia Da</b>
<b>Data e Ora</b>		
<b>Ceduta Da</b>		<b>Presa in Custodia Da</b>
<b>Data e Ora</b>		

### Live system

Denotiamo con live system un sistema in fase di attività che potenzialmente detiene prove, le quali sarebbero difficili da acquisire o potrebbero essere perse nel caso in cui il sistema venga spento. È necessario prestare particolare attenzione a causa della volatilità dei dati. In generale, è necessario ricordare che fasi reboot o spegnimento di un sistema, possono portare alla sovrascrittura di dati su un supporto di memorizzazione (ad esempio, un hard disk), perdita dei dati contenuti nella memoria RAM e perdita del file di paging. Il file di paging è un file molto importante dal punto di vista della digital forensics.

Alcune precauzioni da prendere quando si lavora con i live system:

- Muovere il mouse o spostare leggermente le dita sul touchpad (nel caso di un notebook), per verificare se il device è in stato di stand-by o in sospensione;
- Fotografare e registrare lo schermo del dispositivo, considerando tutti i programmi visibili, data, ora e gli oggetti sul desktop;

- Staccare la spina su PC desktop o rimuovere (in caso di notebook e se possibile) la batteria.

### Dead system

Denotiamo con dead system un sistema NON in fase di attività; In tali sistemi, tutti i dati temporanei (memoria RAM, cache, ecc.) sono tipicamente persi. I dead system non dovrebbero mai essere riaccessi, se non da parte di un investigatore forense. È necessario adottare attenzioni particolari al fine di garantire che i dati esistenti non vengano cancellati e che non vi sia sovrascrittura dei dati. È inoltre importante accertarsi che il sistema sia effettivamente spento e non sia in stato di stand-by/sospensione/ibernazione.

È comunque consigliato fotografare lo schermo e le porte del PC.

### Post Mortem Analysis e Live Analysis

L'analisi dei dead systems è denotata come analisi post mortem (post mortem analysis), mentre l'analisi dei live systems è denotata come live analysis.

### Importanza del File di Paging

I sistemi operativi hanno la possibilità di utilizzare una porzione del disco fisso come una estensione della memoria RAM: la memoria virtuale (o virtual memory). Tale file non è volatile quanto la memoria RAM, proprio perché esso è memorizzato sul disco fisso. Nei sistemi operativi Microsoft Windows, si utilizza un file nascosto denominato pagefile.sys. Il file di paging dovrebbe essere sempre ispezionato, utilizzando appositi strumenti, poiché, poiché potrebbe rivelare utilissime informazioni: password, informazioni sui siti visitati, documenti aperti, ecc.

### 1.3.2 Fase di raccolta

La fase di raccolta è riferita all'acquisizione e/o copia di dati digitali. L'investigatore accede al dispositivo informatico, identificato come rilevante (nella fase di identificazione), contenente appunto i dati digitali utili per l'indagine. Al fine di evitare eventuali compromissioni dei dati originali e, conseguentemente, compromettere le prove, è necessario lavorare su delle copie «esatte» dei dati (maggiori dettagli in seguito).

### Hard Disk e Solid State Disk (SSD)

I dispositivi principali dove vengono memorizzate le informazioni sono i dischi rigidi (detti anche Hard Disk Drive – HDD – o hard disk). Questo tipo di supporto è utile per individuare le prove, poiché i dati non sono convenienti da eliminare definitivamente. Negli ultimi anni, tuttavia, si sono diffusi sempre più i dischi a stato solido (detti anche Solid State Disk – SSD).

Gli SSD sono più veloci, rispetto agli HDD, ed hanno una logica di funzionamento generalmente complessa. Gli SSD memorizzano tipicamente i dati in blocchi, suddivisi in «pagine» composte da grandi array di transistor, detti Negative AND (NAND). A causa della loro natura, gli SSD svolgono delle operazioni di pulizia «automatica», al fine di mantenere veloci gli SSD stessi e allungarne la vita.

- Ciò comporta, però, possibili difficoltà nel reperimento di tracce digitali.

### Memoria RAM

All'interno della memoria centrale (o Random Access Memory – RAM) vengono memorizzati, in binario, dati ed istruzioni. Le istruzioni sono elaborate dalla Central Processing Unit (CPU). La RAM è una memoria volatile, fare una «istantanea» (dump) della RAM può essere molto importante, in quanto la RAM fornisce dettagli sull'uso più recente dell'elaboratore: processi, alcune attività della tastiera, ecc... Tuttavia, in alcuni casi, realizzare un dump della RAM può essere controproducente, in quanto può contaminate il sistema.

## Infrastrutture di Rete

Qualora i dati dovessero essere memorizzati su server di rete (o altri apparati interconnessi in rete), l'accesso può essere fornito collegando un dispositivo alla medesima rete, specificando eventuali dettagli sull'autenticazione. Tuttavia, in diversi casi, è preferibile creare «copie esatte» del server di rete invece di recuperare i dati tramite l'accesso (logico) al sistema operativo del server.

## Problemi relativi alle Fonti di Prove Digitali

I dati e/o i dispositivi hardware potrebbero essere alterati o danneggiati, in maniera:

- Intenzionale: al fine di rendere difficile l'acquisizione agli investigatori;
- Non intenzionale: guasti meccanici (dovuti ad acqua, polvere, piccoli incendi, ecc.).

Talvolta, quindi, vi è quindi necessità di ricostruire dati appunto da hardware/dati danneggiati.

È importante sottolineare che vi sono più minacce per i dati digitali, rispetto ai cosiddetti dati «cartacei»:

<b>Alcune Minacce per i dati digitali</b>	
<ul style="list-style-type: none"> <li>• Errori Umani/Negligenze</li> <li>• Campi elettromagnetici e/o magnetici</li> <li>• Acqua e Condensa</li> <li>• Polvere</li> <li>• Calore</li> </ul>	<ul style="list-style-type: none"> <li>• Impatti fisici</li> <li>• Voltaggio</li> <li>• Elettricità statica</li> <li>• Disastri naturali</li> </ul>

## Integrità delle Prove Digitali

L'integrità di una prova è un aspetto centrale per quanto riguarda l'investigazione forense. È importante che la prova non venga alterata durante la fase di raccolta (ad esempio, durante la copia di file, ecc.). Ci sono dispositivi hardware e strumenti software che proteggono i dati originali da modalità diverse dalla lettura. Per verificare se l'integrità delle prove è preservata, si utilizza il concetto di digital fingerprint. Si realizza mediante le funzioni crittografiche di hash (dette anche funzioni one-way):Eempi: MD5, SHA-1, SHA-256, ecc.

## Ordine di Volatilità delle Prove Digitali

L'ordine di volatilità definisce la priorità con la quale devono essere acquisiti i dati da dispositivi, in base alla volatilità dei dati stessi. I dati «più volatili» devono essere acquisiti prima dei dati «meno volatili».

### 1.3.3 Ispezione

Nella fase di ispezione vi è la preparazione e l'estrazione di potenziali prove digitali dai dati raccolti, nella fase precedente.

#### Ripristino (Recovery) dei Dati

Quando un file viene eliminato dall'utente, di fatto, il relativo puntatore viene contrassegnato come unallocated (non allocato) o available (disponibile) [Operazione efficiente]. Questo significa che lo spazio, allocato per tale file, è disponibile, pertanto, può essere fisicamente sovrascritto da un nuovo file.

#### Riduzione e Filtraggio dei Dati Acquisiti

I dispositivi informatici analizzati dagli investigatori possono contenere svariati terabytes di dati e miliardi di file. È pertanto impossibile o estremamente oneroso fare una analisi completa su una siffatta mole di dati. Quinsi una possibile soluzione è quella di effettuare una fase di filtraggio dei dati (tramite strumenti forensi appositi), individuando quelli potenzialmente significativi. Per esempio i file del sistema operativi possono essere parzialmente ignorati.

#### Carving di File e Dati

I dati raccolti sono solitamente «non strutturati» e/o difficili da interpretare, da parte degli investigatori forensi. Capita molto spesso di avere la necessità di individuare file corrotti, cancellati, frammentati, ecc. Tramite appositi strumenti forensi di data carving (letteralmente, intaglio), è possibile ripristinare i suddetti file anche se contenuti in dati «non strutturati».

### 1.3.4 Analisi

Nella fase di analisi, vengono processate le informazioni con gli obiettivi di determinare i fatti, in relazione ad un evento, e di determinare l'importanza e/o la significatività di una prova e il/i soggetto/i responsabile/i.

#### Ricerca tramite Stringhe e Keyword

Ricerche mediante stringhe e keyword risultano utili nella fase di analisi, in quanto semplificano o comunque possono semplificare il lavoro dell'investigatore. Le ricerche possono avvenire tramite pattern matching di stringhe, includendo espressioni regolari, ecc.

#### Tecniche Anti-Analisi Forense (Cenni)

Sono state sviluppate alcune tecniche note che sono deliberatamente attuate al fine di provare a rendere più difficile l'analisi forense, alcuni esempi:

- Computer Media Wiping strumenti che fanno wiping (letteralmente: pulizia) con l'obiettivo di eliminare definitivamente i file. Remote Wiping: Utilizzato per la cancellazione remota di file su un dispositivo (ad esempio, un dispositivo rubato).
- Cifratura e/o Offuscamento dei Dati: alcuni malware tendono a offuscare/cifrare file di configurazione, ecc. (ad esempio, i ransomware). È necessario individuare la motivazione relativa alla cifratura di un file (se per questioni di protezione di un file o cifratura effettuata da un malware).

#### Analisi delle Timeline degli Eventi

È estremamente utile realizzare delle timeline di eventi basandosi sulle informazioni raccolte (ad esempio, le timestamp inerenti file, processi, ecc.).

### **Analisi dei Collegamenti**

L’analisi dei collegamenti (link analysis) è una potente ed emergente disciplina, nell’ambito della Digital Forensics. L’obiettivo principale è la costruzione di una presentazione strutturata degli oggetti collegati ed interconnessi, al fine di comprendere al meglio le associazioni e i collegamenti fra gli oggetti.

#### **1.3.5 Presentazione**

Nella fase di presentazione, l’investigatore condivide, alle parti interessate, i risultati dell’analisi, in forma di report. Viene prodotta la documentazione finale relativa al risultato dell’investigazione. Tale documentazione deve essere presentata in tribunale o negli uffici preposti.

## **1.4 Distribuzioni Linux per la Digital Forensics**

Sono state sviluppate diverse distribuzioni Linux appositamente pensate per l’uso nell’ambito della Digital Forensics, ciascuna distribuzione ha caratteristiche diverse.

### **1.4.1 DEFT Linu**

Digital Evidence and Forensics Toolkit (DEFT) Linux è un progetto italiano, nato nel 2005, la sua esecuzione esclusivamente in RAM. Nessun meccanismo di swap, in modo da accedere a tutte le memorie secondarie in sola lettura, e non accedendovi mai in scrittura. Si basa su Xubuntu.

### **1.4.2 CAINE**

Computer Aided INvestigative Environment (CAINE) ha un insieme completo di tool per l’analisi forense. È un’ambiente di investigazione affidabile. Interfaccia grafica e user-friendly. Report finale dell’investigazione forense completo e generato in maniera semi-automatizzata. Basato su ubuntu.

### **1.4.3 Parrot Security Linux**

Parrot Security Linux è una distribuzione all-in-one, che contiene diversi tool, per varie attività, fra cui: penetration testing, privacy, digital forensics, reverse engineering e sviluppo applicazioni. Basato su Debian.

### **1.4.4 Kali Linux**

Kali Linux è una distribuzione creata, inizialmente, per le attività relative al Penetration Testing. Il nome iniziale era BackTrack, divenuto poi Kali Linux. Basata su Debian.

Analogamente alle altre tre distribuzioni Linux, viste precedentemente, Kali Linux può essere utilizzata in tre modalità:

1. Modalità live: senza installazione;
2. Modalità forense: utilizzo per gli investigatori forensi;
3. installato sul PC come un classico Sistema Operativo.

#### **Modalità forense**

La modalità forense di Kali Linux permette di lasciare intatti i supporti di memorizzazione del computer, su cui è stata avviata. Disabilita il mounting automatico di penne USB e altri dispositivi. Lascia inalterate le prove (supporti di memorizzazione del computer), durante la fase di indagine.

# Capitolo 2

## Acquisizione dei Dati

### 2.1 Concetti di Base

La fase di raccolta (o acquisizione) del processo di investigazione, dovrebbe garantire quattro proprietà:

- **Affidabilità:** non devono esservi dubbi e/o perplessità in merito all'autenticità e sui risultati ottenuti;
- **Completezza:** devono essere acquisite tutte le informazioni rilevanti, non solo quelle di una parte del caso;
- **Accuratezza:** non devono essere presenti errori nella raccolta dei dati;
- **Verificabilità:** la metodologia deve essere chiara e riproducibile Un altro investigatore dovrebbe essere in grado di arrivare allo stesso risultato, partendo dai medesimi dati.

L'acquisizione dei dati (data acquisition) è l'attività principale della fase di raccolta (o acquisizione) del processo di investigazione. I dati rilevanti vengono acquisiti, da parte di un investigatore, principalmente da due fonti:

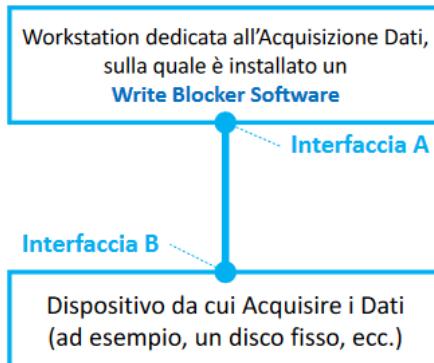
- **Live Systems:** nel caso ci si trovi in presenza di un live system, si considerano anche i live data, ad esempio, il contenuto della memoria RAM;
- **Dead Systems:** nell'acquisizione di dati da un dead system, deve essere effettuata una «copia esatta», attenendosi scrupolosamente a passi ben stabiliti, in modo che l'acquisizione avvenga in maniera valida dal punto di vista forense.

### 2.2 Bloccare le Scritture

Le prove originali devono essere utilizzate esclusivamente per effettuare delle «copie esatte», sulle quali condurre l'analisi forense. Per evitare che vi siano alterazioni dei dati, durante la creazione di una «copia esatta», è necessario utilizzare un write blocker (letteralmente: «bloccatore» di scritture). Un write blocker ha il compito di evitare che vi siano scritture sui dati (è possibile esclusivamente effettuare operazioni di lettura). I write blocker possono essere: implementati via software [Write Blocker Software] oppure dispositivi hardware dedicati [Write Blocker Hardware].

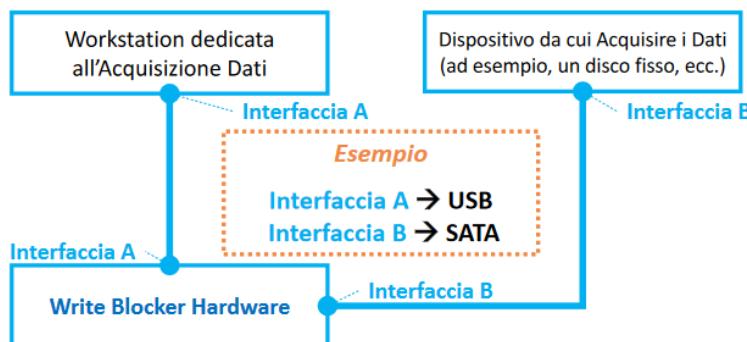
### 2.2.1 Write Blocker Software

La scelta di un write blocker software è principalmente economica. Non richiede l'acquisto di particolari dispositivi. Tuttavia, l'investigatore deve testare costantemente la validità di questa metodologia con la nascita e lo sviluppo dei nuovi standard. Ha lo svantaggio di non essere utilizzabile in alcuni scenari.



### 2.2.2 Write Blocker Hardware

Collega la Workstation per l'Acquisizione Dati (Interfaccia A) al Dispositivo da cui Acquisire i Dati (Interfaccia B) e può bloccarne le scritture. In alcuni modelli, è possibile specificare, mediante un interruttore, se bloccare o meno le scritture.



## 2.3 Immagini Forensi

Per la creazione di una «copia esatta» di un disco fisso (o un altro tipo di supporto di memorizzazione), sono possibili due opzioni: Duplication o Imaging.

### 2.3.1 Duplication

Con il processo di duplication, la destinazione è un altro disco fisso. Il disco fisso destinazione deve essere della stessa marca, dello stesso modello e della stessa taglia del disco fisso sorgente. Tutto il disco sorgente (ovvero, tutto il contenuto di tutti i settori) viene replicato (duplicato) esattamente nella destinazione. L'obiettivo è appunto quello di ottenere una copia esatta, identica in ogni aspetto. Esistono dei dispositivi hardware che si occupano del processo di duplication e sono chiamati forensic hardware duplicator. Caratteristiche:

- Tali dispositivi integrano anche la funzionalità di write blocking del disco fisso originale;
- Inoltre, effettuano anche la verifica dell'esattezza della copia, ottenuta come risultato del processo (maggiori dettagli nelle prossime slide).

Il vantaggio di tali dispositivi è l'estrema rapidità nell'esecuzione del processo di duplication.

### 2.3.2 Imaging

La destinazione del processo di imaging, è un insieme costituito da uno o più file, i quali conterranno, al termine del processo, la copia esatta dell'intero disco fisso sorgente. Quando si effettua una copia logica (ovvero, la copia «tradizionale») di file e/o cartelle, non tutti i file potrebbero essere copiati (a causa di mancanza di permessi, file nascosti, ecc.).

Per evitare che vengano persi dei file/directory, durante la copia logica, è necessario effettuare una copia bit-per-bit dei dati grezzi («raw») dalla sorgente alla destinazione, senza che vi sia alcuna aggiunta o modifica.

Il risultato del processo di duplication o di imaging, è quindi una copia esatta, denominata immagine fisica (physical image) o immagine forense (forensic image).

### 2.3.3 Correttezza Duplication e Imaging

Al fine di verificare che, il processo di duplication o di imaging, abbia effettivamente restituito una copia esatta, si effettuano dei controlli, mediante l'utilizzo di una o più funzioni crittografiche di hash:

- Calcolo dell'hash della sorgente:  $H_S$ ;
- Calcolo dell'hash della destinazione (immagine forense):  $H_D$ ;
- Se  $H_S$  e  $H_D$  sono uguali:  
Sorgente e destinazione risultano effettivamente «identiche»  
altrimenti la destinazione differisce dalla sorgente (anche di un solo bit)

Uno degli algoritmi utilizzati è l'algoritmo crittografico Message Digest (MD5), nonostante non sia recente e contenga delle vulnerabilità, dal punto di vista crittografico. MD5 restituisce un valore di hash di 128 bit (generalmente tale valore è riportato in formato esadecimale).

Un altro algoritmo utilizzato è Secure Hashing Algorithm-1 (SHA-1). Più sicuro di MD5 e produce un valore di hash di 160 bit. Invece dei 128 bit prodotti da MD5. Ad oggi, comunque, una delle funzioni più valide e sicure è la funzione denominata SHA-2. Ci sono poi funzioni di hash denominate SHA-224, SHA- 384 e SHA-512, le quali producono rispettivamente output di dimensione 224, 384 e 512 bit. Da notare che più la funzione crittografica è robusta, più è difficile che vi siano manomissioni/alterazioni, pertanto, è possibile accettare che un'immagine forense rimanga inalterata.

### 2.3.4 Categorie formati immagini fornsi

#### RAW

Restituito da tools che operano a basso livello. Copia bit-per-bit da un drive a un file. I vantaggi sono la velocità di trasferimento, tolleranza a errori di natura minore, diversi tool, per la digital forensics, sono in grado di leggerli. Gli svantaggi sono i seguenti: richiede lo stesso spazio della sorgente. I controlli di validazione vanno conservati a parte (ad esempio, valore hash di MD5, ecc.). Estensioni: ".dd", ".raw", ".img".

### Formati Proprietari

In genere, il formato proprietario ingloba l'immagine RAW, ma ne può effettuare la compressione lossless (maggiori dettagli in seguito). Suddivisione immagini in più file, detti anche segmenti (per memorizzazione su uno o più supporti rimovibili). I vatanggi sono: possono integrare metadati, come, ad esempio: hash dei dati, data e ora di acquisizione, anagrafica investigatore, nome/numero del caso, commenti, etc. Gli svatnaggi sono: non necessariamente supportati da tutti i tool, limitazioni nella taglia dei file, in cui si suddivide l'immagine.

Il formato Expert Witness Format (EWF) è ormai uno standard de facto. Permette la produzione di file compressi o non compressi, in base alle preferenze. Estensione dei file Expert Witness Format: ".E01", ".E02", ".E03", ecc.

### Advanced Forensics Format (AFF)

Immagazzina immagini RAW compresse e non compresse. Nessuna restrizione alla taglia delle immagini. Aggiunta di metadati. Design semplice ed estensibile. Formato Open-Source e per multiple piattaforme. Check interni di consistenza e integrità. Estensioni: ".AFD" per i segmenti e ".AFM" per i metadati.

Un algoritmo di compressione per dati forensi deve necessariamente utilizzare una strategia lossless. Con gli algoritmi di compressione che usano strategie lossless, è possibile riottenere i dati originali, partendo dal file compresso.● Un buon algoritmo potrebbe ridurre la dimensione di una immagine di oltre il 50%. In alcuni casi, un algoritmo di compressione può essere inefficace. Introduce ulteriori rischi di «perdite» di evidenze, in caso di problemi durante il processo di compressione.

## 2.4 Il tool DC3DD

DC3DD è una variante del tool Data Dump (DD), utilizzato per l'acquisizione forense. Caratteristiche di uno strumento di Data Dump

- Acquisizione e clonazione di un supporto di memorizzazione, mediante Bitstream (bit-per-bit)
- Copia delle partizioni di un disco
- Copia delle cartelle e dei file
- Check degli errori di un disco fisso
- Pulizia forense di tutti i dati presenti su un supporto
- Maggiori dettagli in seguito
- Comando per l'installazione

`sudo apt-get install dc3dd`

Il tool DC3DD è stato sviluppato dal “Department of Defense Cyber Crime Center” è un Data Dump con diverse caratteristiche rilevanti:

- Hashing «on-the-fly» usando più algoritmi di hash MD5, SHA-1, SHA-256 e SHA-512
- Indicazione del progresso ed indicazione del tempo di esecuzione
- Scrittura degli errori individuati su un file di log
- Suddivisione dei file di output, in più parti
- Verifica dei file
- Pulizia forense

### 2.4.1 Supporti di Memorizzazione e Partizioni su Linux

Tipicamente un dispositivo di memorizzazione (storage device), in Linux, è indicato nel modo seguente: /dev/sda, dove:

- /dev: fa riferimento al percorso di tutti i device ed i drivers, riconosciuti da Linux.
- /sda: fa riferimento ad un dispositivo di memorizzazione, sd è relativo a storage device (o driver) ed è seguito da una lettera, la quale rappresenta il numero del device di memorizzazione.

Le partizioni sono suddivisione logica di una unità di memorizzazione (ad esempio, un disco fisso, penna USB, ecc.). Le partizioni vengono definite per varie motivazioni, come, ad esempio, installazione di più sistemi operativi, ecc.

Le partizioni in Linux sono riconosciute nel seguente modo:

- sda1 fa riferimento alla partizione 1 sul primo disco (sda)
- sda2 fa riferimento alla partizione 2 sul primo disco (sda)
- sdb1 fa riferimento alla partizione 1 sul secondo disco (sdb)
- sdb2 fa riferimento alla partizione 2 sul secondo disco (sdb)

### 2.4.2 Mantenere la Prova Integra

Per verificare che non vi siano manomissioni, dovrebbe essere calcolato un hash prima, durante e dopo un'acquisizione. In Kali Linux, è possibile utilizzare il comando md5sum seguito dal path del dispositivo (ad esempio, un dispositivo che costituisce una prova), per ottenere il valore hash MD5 associato a tale dispositivo (è possibile utilizzare md5sum anche per i file).

### 2.4.3 Comandi utilizzio DC3DD

```
dc3dd if=/dev/sdb hash=md5 log=dc3ddusb of=test_usb.dd
```

- if: specifica il file di input (ovvero, il dispositivo di cui si intende effettuare la copia esatta)
- hash: specifica l'algoritmo di hash che verrà utilizzato per verificare
- log: specifica il nome del file di log, all'interno del quale verranno riportati tutti i dettagli del dispositivo, del processo di acquisizione ed eventuali errori riscontrati
- of: specifica il file di output relativo all'immagine forense creata dal tool (l'estensione può essere .dd, come nell'esempio, oppure, .img)

### 2.4.4 Processo di Clonazione

DC3DD permette anche di clonare una immagine forense, acquisita precedentemente, su un nuovo dispositivo. Questo processo è denominato processo di clonazione.

Esempio: dc3dd if=test\_usb.dd of=/dev/sdc log=drivecopy.log

### 2.4.5 Pulizia Forense

Si supponga che un investigatore abbia utilizzato, nell'ambito di una indagine forense, attualmente conclusa, un certo disco fisso. Tale investigatore NON può riutilizzare il medesimo disco fisso, così com'è, per una nuova indagine. Il suddetto disco fisso deve essere preliminarmente preparato, al fine di essere riutilizzato, mediante una fase di preparazione. A fase di preparazione del disco fisso è necessaria, onde evitare qualsiasi rischio legato al fatto che tracce, relative alla nuova indagine, possano «interfogliersi» con tracce della precedente indagine (conclusa). Questo comporterebbe l'individuazione di potenziali tracce «non corrette» e potrebbe invalidare la nuova indagine. È consigliabile svolgere la fase di preparazione di un disco fisso, direttamente alla conclusione di una indagine, poiché tale fase potrebbe essere onerosa in termini di tempo.

La pulizia forense, di un disco fisso, prevede la sovrascrittura del contenuto di ciascun settore (di traccia), con valori nulli (zero) o con specifici pattern o con dati random.

Il tool DC3DD fornisce anche la possibilità di effettuare la pulizia forense (opzione wipe). Sono previste tre principali modalità, per la pulizia forense:

- Modalità 1: la pulizia forense viene eseguita sovrascrivendo, con valori zero, il contenuto di ciascun settore del dispositivo specificato. Esempio: dc3dd wipe=/dev/sdb, La pulizia forense viene eseguita sul dispositivo, identificato dal path /dev/sdb (specificato nell'opzione wipe).
- Modalità 2: la pulizia forense viene eseguita sovrascrivendo, con un pattern esadecimale (ripetuto), il contenuto di ciascun settore del dispositivo specificato. Il pattern viene specificato dall'utente, mediante l'opzione pat. Esempio: dc3dd wipe=/dev/sdb pat=101010, pat = pattern esadecimale da utilizzare.
- Modalità 3: la pulizia forense viene eseguita sovrascrivendo, con una stringa (ripetuta), il contenuto di ciascun settore del dispositivo specificato. La stringa viene specificata dall'utente, mediante l'opzione tpat. Esempio: dc3dd wipe=/dev/sdb tpat=digf.

## 2.5 Il tool Guymager

Guymager è Open-Source ed è sviluppato da Guy Voncken. Presenta molteplici caratteristiche di DC3DD ed è disponibile esclusivamente per sistemi operativi Linux-based (preinstallato su Kali Linux). Fornisce una interfaccia grafica (GUI).

### 2.5.1 Immagini Forensi e Live System

Nell'ambito di un live system, è comunque possibile creare una immagine forense del disco fisso, sul quale è in attività il S.O. ed eventuali altri software. Questo processo è denominato live disk acquisition. Passi Principali:

1. Esecuzione di un tool per l'acquisizione forense. NOTA: Il tool viene eseguito sul S.O. in attività, del live system.
2. Acquisizione di una immagine forense del disco fisso su cui è in attività il S.O. ed eventuali altri software. NOTA: Tale disco fisso sarà considerato il disco fisso sorgente, nel processo di imaging.

L'immagine forense acquisita sarà relativa ad un certo istante temporale. Verosimilmente verranno apportate modifiche al contenuto del disco fisso sorgente, anche dopo la creazione dell'immagine forense. Le modifiche verranno apportate dai vari software in esecuzione sul live system (ad esempio, modifiche da parte del S.O./eventuali applicazioni/driver, ecc.). In virtù delle suddette considerazioni, non è quindi possibile preservare l'integrità del disco fisso sorgente. Tuttavia, è possibile preservare l'integrità della prova, considerando la prima immagine forense acquisita.

## 2.6 Utilizzo di DC3DD su dispositivi Android-based

Android consente principalmente due posizioni di memorizzazione:

- interna: una memoria flash, interna al dispositivo, dove viene memorizzato il sistema operativo e le sue componenti: Kernel, librerie compilate, App.
- esterna: non sempre disponibile (dipende dal produttore del dispositivo), tipicamente viene utilizzata una micro-SD, memorizza generalmente dati utente.

Un dispositivo Android presenta un layout specifico di partizionamento, in riferimento alla memoria interna, il quale include le seguenti partizioni:

- Boot [Percorso /boot]: contiene il codice per l'avvio del S.O.
- recovery [Percorso /recovery]
- Data [Percorso /data]: contiene dati dell'utente e app installate
- System [Percorso /system]: contiene i file relativi al S.O.
- Cache [Percorso /cache]: memorizza alcune informazioni su app utilizzate frequentemente, ecc.

La partizione Data è sicuramente la più rilevante, dal punto di vista forense, poiché contiene dati dell'utente e app (le quali possono a loro volta memorizzare dati rilevanti per l'investigazione)

### 2.6.1 Permessi di Root e Accesso a tutte le Partizioni

Affinché risulti possibile l'accesso a tutte le partizioni ed a tutti i relativi dati, è necessario avere i permessi di root. Per ottenere i permessi di root (procedura denominata rooting) è generalmente richiesto lo «sblocco» del bootloader. I produttori prevedono dei blocchi software nel bootloader dei dispositivi prodotti, per evitare modifiche non autorizzate al software dei dispositivi stessi.

### 2.6.2 Recovery mode e ADB

Per poter acquisire i dati (senza alterazione degli stessi) di un dispositivo Android, è necessario avviarlo in modalità di recupero (recovery mode). È un software speciale (integrato nel firmware del dispositivo, memorizzato nella partizione Recovery) che permette di avere alcune funzionalità, utili soprattutto in caso di problemi con il dispositivo, fra cui:

- Ripristino del dispositivo, alle impostazioni di fabbrica
- Pulizia della cache di sistema, ecc.
- Installazione di aggiornamenti

È possibile utilizzare il tool Android Debug Bridge (ADB), per acquisire i dati.

#### ADB

ADB è un tool utilizzato dagli sviluppatori, per il debugging di app, ecc. (fa parte dell'Android SDK). Permette di controllare dispositivi Android, connessi mediante USB (sul dispositivo, se acceso, deve essere attiva la modalità USB Debugging dalle Opzioni Sviluppatore di Android). Permette di mostrare i dispositivi connessi, iniettare file sul dispositivo (push) ed estrarre file dal dispositivo (pull) e di seguire una shell che permette l'esecuzione di comandi sul dispositivo e l'installazione di app sul dispositivo Il comando di ADB è adb.

**NOTA:** ADB lavorerà adeguatamente solo se, sul dispositivo, è stata precedentemente installata la porzione di firmware, relativa alla modalità di recupero ( contenuta nella partizione Recovery), adeguatamente modificata. L'obiettivo è avere una custom recovery mode, in grado di «estendere» le funzionalità della versione preinstallata di tale modalità. Nella custom recovery mode, inoltre, devono essere montate tutte le partizioni alla quale si vuole accedere.

### 2.6.3 Modalità di Acquisizione dei Dati

Vi sono due possibili modalità relative all'acquisizione dei dati:

- fisica: viene effettuata una copia bit-per-bit, il risultato è una copia «raw» della partizione.
- logica: è possibile copiare tutti (o alcuni) file e/o directory. La copia avviene a livello di file system.

### 2.6.4 Passi Principali per l'acquisizione dei Dati

Avviare il dispositivo Android, in custom recovery mode. Collegare il dispositivo Android al PC. Verificare che ADB (precedentemente installato sul PC) riconosca adeguatamente il device connesso, con il seguente comando: adb devices. Viene mostrato un identificativo del device e la modalità tramite la quale sono connessi al PC.

Il passo successivo sarà avviare la shell (la quale verrà avviata sul PC), per eseguire comandi direttamente sul dispositivo. La shell si può avviare mediante il seguente comando: adb shell. Dalla shell avviata possiamo, ad esempio, listare tutte le directory e i file della partizione Data (grazie ai permessi di root)<sup>1</sup>: ls /data.

Possiamo ora uscire dalla shell, avviata da adb shell, mediante il comando: exit. Per estrarre dati e copiarli sul PC (copia logica), possiamo utilizzare l'opzione pull del comando adb:  
adb pull<sup>2</sup> path\_sorgente\_dispositivo path\_destinazione\_PC

La copia logica presenta dei limiti importanti, infatti, ad esempio, non viene copiato lo spazio non allocato (unallocated). In questo modo, non è possibile risalire ad eventuali file cancellati (ma il cui spazio fisico, non è stato ancora sovrascritto). In genere, si tende a minimizzare il numero di scritture su supporti flash, presenti nei dispositivi portabili, per questo i file vengono spesso cancellati solo logicamente (lo spazio viene contrassegnato come non allocato), ma non fisicamente.

Per acquisire una immagine forense, potremmo utilizzare il tool DC3DD. Dal momento che il tool dovrà essere eseguito sul dispositivo, è necessario che il tool venga precedentemente compilato/adattato, in accordo all'architettura della CPU del dispositivo (tipicamente ARM).

Affinché il tool DC3DD possa essere utilizzato sul dispositivo, l'eseguibile deve essere iniettato nel dispositivo<sup>3</sup>. È possibile utilizzare l'opzione push del comando adb, nel modo seguente:  
adb push dc3dd /storage/sdcard1

---

<sup>1</sup>Non possiamo utilizzare il comando cp (per la copia) nella shell, poiché funzionerebbe solo internamente al dispositivo (non sarebbe quindi estrarre dati dal dispositivo e copiarli sul PC, per analizzarli, dal punto di vista forense)

<sup>2</sup>pull -p mostra i progressi durante la fase di copia

<sup>3</sup>Quando possibile, è fortemente consigliato copiare l'eseguibile di DC3DD sulla memoria esterna del dispositivo. Questo è molto utile per evitare di alterare dati contenuti nella memoria interna al dispositivo stesso

La versione Android del tool DC3DD non accetta directory. Vengono accettati esclusivamente block file. Tali file sono associati alle partizioni di Android mediante la shell di comandi di ADB è possibile individuare quali sono i suddetti file:

```
# adb shell  
# ls -l /dev/block
```

Esempio di output:

```
... mmcblk0 ...  
... mmcblk0p1 ...  
... mmcblk0p2 ...  
...  
... mmcblk0p10 ...
```

- Il file mmcblk0 è tipicamente riferito alla memoria interna del dispositivo Le prime tre lettere: mmc, fanno riferimento alla embedded MultiMedia Card (questa è la tipologia di memoria tipicamente utilizzata dai dispositivi portabili). Le ultime tre lettere, seguite dallo 0: blk0, fanno riferimento al primo blocco (identificato dallo 0) della memoria interna (verosimilmente quello principale).
- : Gli altri block file, indicati come mmcblk0pX (dove X è un valore numerico), sono riferiti a partizioni (indicato dalla lettera p) della memoria interna (indicata con mmcblk0)

L'obiettivo deve essere quello di effettuare una immagine forense di tutta la memoria interna principale.

C'è però un problema: di default, Android non prevede l'esecuzione di file eseguibili presenti nella memoria esterna. Quindi, non è possibile eseguire DC3DD. Per poter eseguire il tool DC3DD, è necessario che vengano prima abilitati i permessi di esecuzione (exec), nella memoria esterna, dalla shell di ADB. È possibile utilizzare il comando mount per abilitare tali permessi:

```
# mount -o remount, rw, exec /storage/sdcard1
```

Da ora è possibile utilizzare il tool DC3DD normalmente dalla shell.

# Capitolo 3

## File Recovery e Data Carving

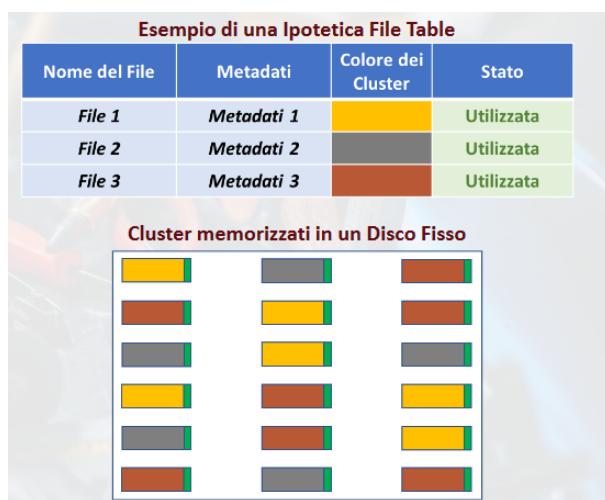
I file eliminati sono importantissimi poiché potrebbero costituire evidenze digitali (ad esempio, documenti finanziari manipolati, immagini pedopornografiche, ecc.)

### 3.1 Recupero tramite Metadati

Nell' esempio che segue, ogni riga della file tabella è riferita ad uno specifico file:

- La prima colonna fa riferimento al nome del file
- La seconda colonna fa riferimento ai metadati del file. Esempio: timestamp di creazione, dimensione del file, ecc.
- La terza colonna indica il colore dei cluster all'interno del disco.
- La quarta colonna specifica se l'entry è utilizzata o non utilizzata

Il cluster (tipicamente di 4 KB) è l'unità più piccola che è possibile indirizzare da un file system. Per la memorizzazione di un file possono servire più cluster.



Nei cluster evidenziati (color ocra) è memorizzato il contenuto del File 3, se verde il cluster è allocato, se rosso il cluster non è allocato (quindi è considerato libero dal S.O.).

### Esempio di cancellazione di file

Supponiamo di voler eliminare il File 2:

- Passo 1: la entry relativa al File 2 viene contrassegnata come non utilizzata (potrà essere riutilizzata, in futuro, dal SO).
- Passo 2: i cluster grigi relativi al File 2, verranno contrassegnati come liberi (non allocati), senza alterarne il contenuto (potranno essere riutilizzati, in futuro, dal SO). Se la entry non è stata sovrascritta sarà possibile recuperare il nome del file, i metadati ed i cluster in cui è/era memorizzato il suo contenuto. Se i cluster non sono stati sovrascritti, sarà possibile recuperare integralmente il contenuto del File 2. Saranno possibili anche eventuali recuperi parziali, nel caso in cui solo alcuni cluster siano stati sovrascritti.

**Nota 1:** cluster non allocati (liberi) costituiscono il cosiddetto unallocated space.

**Nota 2:** Perché tipicamente non viene «pulito» anche il contenuto dei cluster e delle entry della File Table, quando si elimina un file? Per mantenere le performance ottimali: una pulizia forense è più onerosa (soprattutto con file di grandi dimensioni); inoltre, si può incappare in errori non previsti.

### In sintesi

Quando un file viene eliminato la entry della MFT ad esso associata viene contrassegnata come non utilizzata. I cluster, contenenti i dati del file, vengono contrassegnati come liberi (non allocati). L'insieme dei cluster non allocati costituiscono l'unallocated space. Sia i cluster che la relativa entry della MFT potranno essere riutilizzati in futuro dal SO, pertanto, qualora le suddette strutture non siano state sovrascritte dal SO, sarà possibile recuperare il file eliminato. L'unallocated space diviene quindi potenzialmente importante, per la Digital Forensics.

## 3.2 Carving

I metadati dei file, però, potrebbero NON essere presenti o potrebbero essere corrotti. In questi scenari, è comunque possibile sfruttare alcune caratteristiche strutturali del contenuto dei file (nello specifico, gli header e/o i footer), al fine di provare a ricostruire i file eliminati. Queste considerazioni, sono sfruttate nei processi di file carving.

### 3.2.1 Header e footer di un file

Ogni file appartiene generalmente ad una certa tipologia (ad esempio, documenti di Microsoft Word, fogli di calcolo di Microsoft Excel, filmati AVI, ecc.). La tipologia di un file NON è identificata dall'estensione del file stesso (ad esempio, .docx, .xlsx, .avi, ecc.). Nel contenuto di un file, sono generalmente presenti:

- Un header: una sequenza di particolari byte, all'inizio del file (alcuni esempi di header, verranno riportati nelle prossime slide)
- Un footer: una sequenza di particolari byte, alla fine del file

L'header ed il footer caratterizzano la tipologia del file. **Nota:** il footer può essere generalmente omesso (talvolta, è sufficiente quindi esclusivamente l'header per caratterizzare la tipologia di un dato file)

Per cui, anche in caso di modifica dell'estensione del file (ad esempio, da .jpg a .ppp), tramite l'analisi dell'header e/o del footer è possibile provare ad effettuare il recupero. Si deve osservare però che il processo di carving è un processo particolarmente oneroso, in termini di tempo di esecuzione. È consigliato quindi utilizzare strumenti automatizzati, al fine di risparmiare tempo. Può essere particolarmente significativo, per migliorare l'efficacia del carving e, conseguentemente, migliorare l'investigazione, l'utilizzo di più di un tool.

### Esempio header immagine jpg

Rappresentazione esadecimale byte per byte, del contenuto di un file: In questo caso, i primi 4 byte

Offset	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	
000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	48	00	48	00	00	FF	DB	00	43	
000024	00	06	04	05	06	05	04	06	06	05	06	07	07	06	08	0A	10	0A	0A	09	09	0A	14	0E	
000048	0F	0C	10	17	14	18	17	14	16	16	1A	1D	25	1F	1A	1B	23	1C	16	16	20	2C	20		
000072	23	26	27	29	2A	29	19	1F	2D	30	2D	28	30	25	28	29	28	FF	DB	00	43	01	07	07	
000096	07	0A	08	0A	13	0A	13	28	1A	16	1A	28	28	28	28	28	28	28	28	28	28	28	28	28	
000120	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	
000144	28	28	28	28	28	28	28	28	28	28	28	28	28	28	FF	C0	00	11	08	02	8F	01	D0	03	
000168	01	22	00	02	11	01	03	11	01	FF	C4	00	1D	00	00	00	07	01	01	01	00	00	00	00	
000192	00	00	00	00	00	00	00	00	01	02	03	04	05	06	08	07	09	FF	C4	00	5C	10	00	01	03
000216	02	03	04	05	04	0B	0B	09	06	06	02	01	05	01	00	02	03	04	11	05	06	21	07	12	
000240	31	41	13	22	51	61	71	14	32	91	B1	08	15	17	23	33	52	72	73	81	A1	B2	16	24	
000264	25	34	35	36	42	56	62	93	C1	26	37	53	55	63	74	92	C2	D1	18	43	45	82	94	F0	
000288	44	46	54	95	A2	D2	27	F1	83	57	75	85	A4	E1	FF	C4	00	1B	01	00	02	03	01	01	
000312	01	00	00	00	00	00	00	00	00	00	01	02	03	04	05	06	07	FF	C4	00	2F	11			
000336	00	02	02	01	04	01	03	03	05	00	03	01	00	00	00	00	01	02	03	11	04	12	21		
000360	31	05	13	32	41	06	22	51	14	15	61	16	42	71	91	A1	23	52	C1	F1	FF	DA	00	OC	
000384	03	01	00	02	11	03	11	00	3F	00	EA	7E	C1	C6	FD	A8	9A	6E	2F	AE	A9	32	FC	1B	
000408	88	36	21	A6	C7	B1	73	95	46	67	C7	5B	51	30	66	2D	54	00	7B	80	01	C3	4D	4A	
000432	12	25	18	EE	3A	42	E8	BD	16	5C	D7	F7	53	98	07	FC	5E	AC	1F	94	14	0A	9C	DD	

del contenuto identificano la tipologia del file (ovvero, una immagine JPEG). I byte FF D8 FF E0 rappresentano l'Header di una immagine JPEG.

### Esempio header immagine png

Offset	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17
000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	OD	49	48	44	52	00	00	07	80	00	00	04	38
000024	08	02	00	00	00	67	B1	56	14	00	00	00	09	70	48	59	73	00	00	OE	C4	00	00	OE
000048	C4	01	95	2B	0E	1B	00	00	20	00	49	44	41	54	78	9C	EC	9D	79	5C	55	D5	FA	FF
000072	9F	03	2A	88	32	A7	28	02	07	D1	2B	6A	A1	A0	0C	A6	D7	06	53	B0	E1	FE	B4	AE
000096	48	5E	87	34	F4	7A	4D	FD	7A	2F	A9	E5	18	39	34	A8	59	DD	AC	AE	5F	87	2C	B5
000120	52	A8	B4	6F	65	92	7A	2B	AE	26	83	82	C3	55	31	51	08	44	51	19	55	10	E5	70
000144	7E	7F	3C	B2	5A	EC	E9	EC	B3	CF	3E	4C	3E	EF	3F	78	6D	D6	5E	C3	B3	D6	5E	7B
000168	9F	BD	3F	FB	D9	CF	32	F4	EA	D5	0B	08	82	20	09	82	20	9A	1A	93	C9	D4	26	
000192	B4	6C	1C	1D	1D	9B	DA	04	82	20	08	82	20	AC	83	BF	FF	71	70	70	30	18	0C	E2
000216	3C	75	75	75	66	B3	59	97	1F	7A	73	3D	72	6D	A9	01	ED	31	18	0C	0E	0E	66	
000240	B3	B9	AE	AE	8E	ED	C2	44	85	A6	0D	06	03	B6	CB	17	44	7B	E4	0A	2A	F4	85	59
000264	82	29	CA	03	A8	90	41	0D	75	75	75	75	8E	8E	8E	82	1A	58	E5	88	C2	08		
000288	08	32	B3	A3	60	AD	49	E2	8E	AB	6C	5D	A1	36	F6	AF	F2	10	E1	20	28	0F	38	56
000312	68	CB	50	B3	93	42	6E	CE	0B	6C	B6	68	B6	C5	4A	F0	FC	E2	67	A6	42	85	E2	11
000336	C3	44	00	D0	70	34	19	FC	69	A5	AD	06	C9	0A	15	C6	D0	64	32	A1	B5	DA	0E	16
000360	EB	B2	CA	FC	6D	AC	6D	B0	20	08	82	20	08	82	20	08	E2	1E	07	15	55			
000384	A8	17	62	A0	5E	8B	51	AF	1F	31	19	CB	50	8F	5C	4E	CD	AA	96	B8	1E	83	C1	C0
000408	14	34	6D	C2	13	D3	9D	05	DA	AB	72	6D	B8	OB	A5	3D	36	74	AC	A0	55	A2	1B	AF

In questo caso, i primi 8 byte del contenuto identificano la tipologia del file (ovvero, una immagine PNG). Header dell'immagine PNG: 89 50 4A 0D 0A 1A 0A.

### Esempio header file pdf

Offset-00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	
000000	25	50	44	46	2D	31	2E	37	0D	0A	25	B5	B5	B5	0D	0A	31	20	30	20	6F	62	6A	
000024	0D	0A	3C	3C	2F	54	79	70	65	2F	43	61	74	61	6C	6F	67	2F	50	61	67	65	73	20
000048	32	20	30	20	52	2F	4C	61	6E	67	28	69	74	2D	49	54	29	20	2F	53	74	72	75	63
000072	74	54	72	65	65	52	6F	6F	74	20	33	35	37	20	30	20	52	2F	4D	61	72	6B	49	6E
000096	66	6F	3C	3C	2F	4D	61	72	6B	65	64	20	74	72	75	65	3E	3E	2F	4D	65	74	61	64
000120	61	74	61	20	35	35	39	34	20	30	20	52	2F	56	69	65	77	65	72	50	72	65	66	65
000144	72	65	6E	63	65	73	20	35	35	39	35	20	30	20	52	3E	3E	0D	0A	65	6E	64	6F	62
000168	6A	0D	0A	32	20	30	20	6F	62	6A	0D	0A	3C	3C	2F	54	79	70	65	2F	50	61	67	65
000192	73	2F	43	6F	75	6E	74	20	39	39	2F	4B	69	64	73	5B	20	33	20	30	20	52	20	31
000216	36	20	30	20	52	20	32	33	20	30	20	52	20	32	35	20	30	20	52	20	32	39	20	30
000240	20	52	20	33	31	20	30	20	52	20	35	30	20	30	20	52	20	35	33	20	30	20	52	20
000264	36	30	20	30	20	52	20	36	34	20	30	20	52	20	36	37	20	30	20	52	20	37	30	20
000288	30	20	52	20	37	34	20	30	20	52	20	37	39	20	30	20	52	20	38	33	20	30	20	52
000312	20	39	35	20	30	20	52	20	39	37	20	30	20	52	20	31	30	30	20	30	20	52	20	31
000336	30	34	20	30	20	52	20	31	30	39	20	30	20	52	20	31	31	31	20	30	20	52	20	31
000360	31	35	20	30	20	52	20	31	31	39	20	30	20	52	20	31	32	31	20	30	20	52	20	31
000384	32	33	20	30	20	52	20	31	32	37	20	30	20	52	20	31	33	31	20	30	20	52	20	31
000408	33	35	20	30	20	52	20	31	33	37	20	30	20	52	20	31	33	39	20	30	20	52	20	31
000432	34	35	20	30	20	52	20	31	34	39	20	30	20	52	20	31	35	33	20	30	20	52	20	31

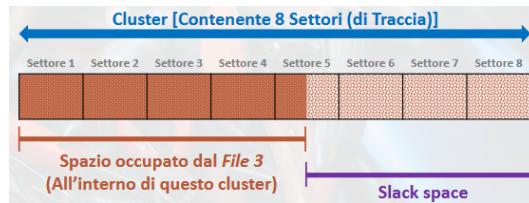
In questo caso, i primi 4 byte del contenuto identificano la tipologia del file (ovvero, un documento PDF). Header del file PDF: 25 50 44 46.

### Esempio header file online

Si può utilizzare un tool online presente al seguente link: <https://www.filesignatures.net/>. In cui si riicerca la tipologia di un file, mediante la sua estensione o mediante il suo header/footer. CI verrà restituita una stringa di ricerca: 89504E470D0A1A0A composta 8 bytes rappresentati in esadecimale (senza spazi) chiamata "Signature".

## 3.3 Slack Space

Il cluster che memorizza l'ultima parte di un file, potrebbe essere non completamente utilizzato. Lo spazio che intercorre dalla fine del file alla fine dell'ultimo cluster è chiamato slack space (letteralmente, spazio allentato). Lo slack space è importante nelle indagini forensi, poiché, al suo interno, possono



esservi dati, appartenenti a file eliminati.

I processi di file recovery e data carving consistono proprio nell'individuare ed estrarre dati e file eliminati.

## 3.4 Il tool Foremost

Il tool Foremost è un tool Open-Source per sistemi Linux-based, installabile mediante il comando:  
sudo apt-get install foremost

Utilizzabile tramite linea di comando (CLI – Command Line Interface). Utilizzabile per il recupero dei file è in grado di leggere l'header e/o il footer dei file, al fine di individuarne la relativa tipologia e recuperarli, è semplice ed efficace.

Esempio comando foremost:

**foremost -i <file> -o <dir> [options]**

- -i: permette di specificare il percorso del file di input. OSSERVAZIONE: il file di input deve essere una immagine forense, precedentemente acquisita, con gli appositi tool (ad esempio, con il tool DC3DD).
  - -o: Permette di specificare la directory di output, dove verranno memorizzati i file, recuperati mediante il processo di file recovering. Esempio nelle prossime slide.

options : Eventuali opzioni (facoltative), da specificare solo se necessarie.

## Esempio

Per l'esempio è utilizzata l'immagine 11-carve-fat.dd scaricabile gratuitamente dal link <http://dfft.sourceforge.net/test11/>.

Per avviare il processo di recovery sull'immagine 11-carve-fat.dd, effettuiamo i seguenti step:

1. Posizioniamoci nella cartella che contiene il file dell'immagine (ad esempio, la Scrivania).
  2. Digitiamo il seguente comando: `foremost -i 11-carve-fat.dd -o Ripristinati`.
  3. L'output del processo verrà riportato nella cartella specificata, ovvero, Ripristinati (La cartella deve essere vuota).

```
root@kali:~/Scrivania# foremost -i 11-carve-fat.dd -o Ripristinati/
Processing: 11-carve-fat.dd
|Foundstart=wword60.txt=0x0(0
0w00kN10aE0I)0x0.056nEK0o0%0I00000%-~0000Ve00D@=0%8#00000000K0E^00+0)/F08/000l070-0
0 000..I`It0000-0|{0000000w000<0$00x"/00WI000Mp0000000:000-z{zq00000000ov00g00JF
QY0a5/02008-0Q0K00:0X00o>y00M_000080(X00^T5003|S$002T00q0000S000uE0|:Z0hxgWI00v/0
000mt0sk)000d0000000/0E0
          Cestino
          q|<.000n0 J010V00ma|000` }00000000
          0-J0y9:0G0E0.0Y0`00000
0//)&Z007t0p+-~0000000Ky0V00
0-0a
*|
root@kali:~/Scrivania#
```

Nonostante i caratteri «strani» mostrati a video, il processo è terminato correttamente.

Al termine del processo, sarà possibile accedere alla cartella Ripristinati. Gli elementi ripristinati sono stati inseriti in apposite sottocartelle, in base alla loro tipologia (ad esempio, le immagini JPEG sono state inserite nella sottocartella jpg).

È possibile inoltre notare anche la presenza di un file testuale, denominato "audit.txt". All'interno di questo file viene riportata una lista dei file ripristinati. Per ciascuno di tali file, viene riportato il nome associato (colonna Name), la dimensione (colonna Size) ed altre informazioni (fra cui eventuali commenti, nella colonna Comment). Viene anche poi riportata una sintesi dei file ripristinati, mostrando il numero totale dei file ripristinati ed il numero di file ripristinati, per ciascuna categoria (ad esempio, sono state ripristinate 3 immagine JPEG, denotate dalla voce jpg).

## osservazioni

Foremost è uno strumento abbastanza potente ed efficace. L'intero processo, nell'esempio, è durato pochi secondi (anche testandolo su configurazioni più lente). Il tempo di elaborazione tuttavia può coprire un arco temporale anche molto lungo, in base alla dimensione del file di input ed altri fattori. Se si conosce la tipologia di file che si intende ripristinare, è possibile utilizzare l'opzione `-t` in modo da ridurre le tempistiche elaborative. Esempio con l'opzione `-t jpeg`, verranno ripristinati esclusivamente le immagini JPEG.

### 3.5 Il tool Scalpel

Il tool Scalpel (letteralmente, scalpello) è presente in Kali Linux. Open-Source per sistemi Linux-based ed utilizzabile tramite linea di comando. Originariamente basato su Foremost, tuttavia, significativamente più efficiente di quest'ultimo. Scalpel risolve i problemi di Foremost, relativi all'utilizzo elevato di CPU e RAM, durante la fase di recovering. A differenza di Foremost, con Scalpel è necessario specificare le tipologie di file che si intende cercare di ripristinare. Scalpel deve essere configurato mediante il relativo file di configurazione, denominato scalpel.conf, individuabile nella directory /etc/scalpel.

Contenuto (parziale) del file di configurazione scalpel.conf: Per ciascuna tipologia di file, scalpel.conf

```
# GIF and JPG files (very common)
#     gif      y      5000000      \x47\x49\x46\x38\x37\x61      \x00\x3b
#     gif      y      5000000      \x47\x49\x46\x38\x39\x61      \x00\x3b
#     jpg      y      5242880      \xff\xd8\xff??Exif      \xff\xd9
```

contiene le seguenti informazioni:

- Estensione, associata alla tipologia
- Header rappresentato in esadecimale
- Footer rappresentato in esadecimale

**Nota:** Tutte le tipologie di file sono commentate (lo si denota dal carattere #), pertanto, è strettamente necessario rimuovere i commenti (rimuovendo il carattere #) per almeno una tipologia.

Esempio comando scalpel: scalpel -o <dir> <file>

- -o: Permette di specificare la directory di output, dove verranno memorizzati i file, recuperati mediante il processo di file recovering.
- <file>: Permette di specificare il percorso del file di input. OSSERVAZIONE: il file di input deve essere una immagine forense, precedentemente acquisita, con gli appositi tool (ad esempio, con il tool DC3DD)

#### Esempio

Per avviare il processo di recovery sull'immagine forense 11-carve-fat.dd (la medesima utilizzata anche con Foremost), effettuiamo i seguenti step:

1. Posizioniamoci nella cartella che contiene il file dell'immagine (ad esempio, la Scrivania)
2. Digitiamo il seguente comando: scalpel -o RipristinatiScalpel/ 11-carve-fat.dd
3. L'output del processo verrà riportato nella cartella specificata, ovvero, RipristinatiScalpel (la cartella deve essere vuota).

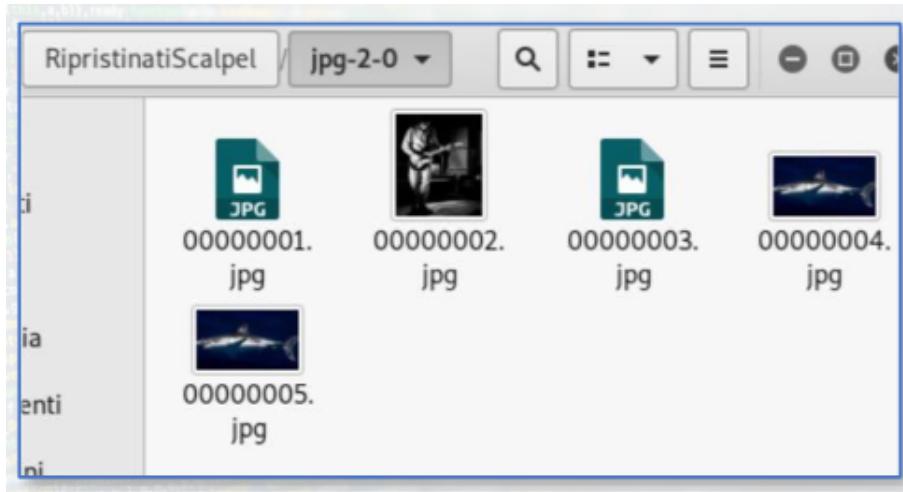
Al termine del processo, sarà possibile accedere alla cartella RipristinatiScalpel. Anche qui all'interno della cartella sarà presente un file audit.txt<sup>4</sup>.

**Nota:** se si utilizza scalpel e foremost sulla stessa immagine non è detto che venga ripristinato lo stesso numero di file.

---

<sup>4</sup>A differenza del file audit.txt, prodotto da Foremost, nel file audit.txt, prodotto da Scalpel, non viene riportata alcuna sintesi in relazione al numero di file estratti per ciascuna tipologia

Il contenuto della cartella RipristinatiScalpel/jpg- 2-0 (contenente cinque file JPEG ripristinate)



Scalpel ha individuato 5 file JPEG (in base al relativo header e/o footer), tuttavia, come si può notare visivamente, dalla figura, solo tre mostrano un'anteprima (00000002.jpg, 00000004.jpg e 00000005.jpg), mentre gli altri due (00000001.jpg e 00000003.jpg) non mostrano alcuna anteprima. I file, per i quali non è mostrata anteprima, sono corrotti: Scalpel ha verosimilmente ripristinato dei «FALSI POSITIVI». Inoltre è possibile osservare che i file 00000004.jpg e 00000005.jpg sono identici (stesso valore di hash, per entrambi i file). In questo caso, in pratica, Scalpel ha ripristinato un numero minore di immagini JPEG (ovvero, 2), rispetto a Foremost (il quale ne aveva ripristinate 3). In virtù di queste osservazioni, risulta ancor più evidente l'importanza di considerare più tool, i quali potrebbero NON restituire il medesimo risultato [operando sulla medesima immagine forense].

## 3.6 Il tool PhotoRec

Il tool PhotoRec è un software di file recovery (supporta circa 100 tipologie di file) da immagini forensi e da vari tipi di supporti (dischi fissi, memory card, ecc.). Funziona anche nel caso di supporti particolarmente danneggiati o formattati. Il comando per utilizzare PhotRec è "photorec [input]".

input : Parametro opzionale che permette di specificare il percorso del file di input. OSSERVAZIONE 1: il file di input può essere una immagine forense (formato .DD oppure .E01) oppure un device. OSSERVAZIONE 2: Se non viene specificato il parametro [input], il tool richiede all'utente di selezionare un device (fra quelli disponibili), da cui effettuare il recupero.

### 3.6.1 Esempio di utilizzo

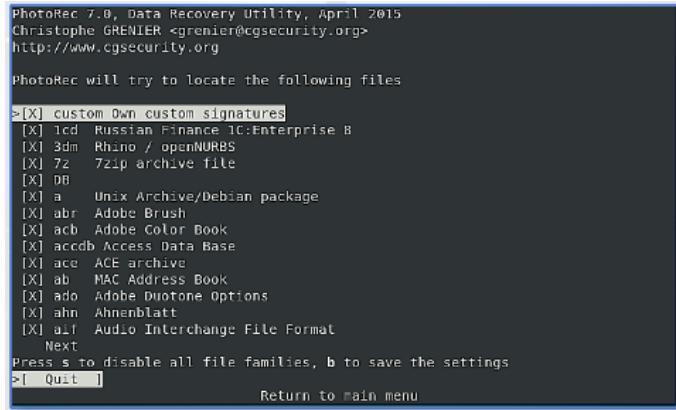
Per avviare il processo di recovery sull'immagine 11-carve-fat.dd, effettuiamo i seguenti step:

1. Posizioniamoci nella cartella che contiene il file dell'immagine (ad esempio, la Scrivania),
2. Digitiamo il seguente comando: "photorec 11-carve-fat.dd",
3. L'output del processo verrà riportato nella cartella `recup_dir`<sup>5</sup>.

All'avvio del comando viene chiesto di selezionare il supporto di origine (nel nostro esempio disk 11-carve), selezioniamo poi l'opzione [Proceed] e confermiamo con il tasto "invio". Successivamente,

<sup>5</sup>Nota: il nome della cartella di output (`recup_dir`), non può essere modificato

PhotoRec richiede di selezionare la partizione dalla quale effettuare il recupero (per esempio "P Unkn0wn"). Selezioniamo poi la tipologia di file da recuperare, nel nostro esempio selezionando [File Opt], sarà possibile selezionare (da una lista fornita da PhotoRec) quali tipologie di file si intende recuperare: Dopo aver eventualmente indicato le tipologie di file di interesse, selezionando [Search] proseguiremo



PhotoRec 7.0, Data Recovery Utility, April 2015  
Christophe GRENIER <grenier@cgsecurity.org>  
<http://www.cgsecurity.org>

PhotoRec will try to locate the following files

```
>[X] custom Own custom signatures
[X] icd Russian Finance IC:Enterprise 8
[X] 3dm Rhino / openNURBS
[X] 7z 7zip archive file
[X] DB
[X] a Unix Archive/Debian package
[X] abr Adobe Brush
[X] acb Adobe Color Book
[X] accdb Access Data Base
[X] ace ACE archive
[X] ab MAC Address Book
[X] ado Adobe Duotone Options
[X] ahn Ahnenblatt
[X] aif Audio Interchange File Format
Next
Press s to disable all file families, b to save the settings
>[ Quit ]
```

Return to main menu

con le opzioni di recupero.

Nel passo successivo, PhotoRec chiede di indicare il file system dell'immagine, fra le due seguenti opzioni:

- ext2, ext3 o ext4
- FAT, NTFS, HFS+, ecc.

Verrà poi chiesta conferma in merito al percorso della cartella di output. Al termine del processo, dopo aver chiuso PhotoRec (selezionando [Quit], nelle varie schermate), sarà possibile accedere alla cartella `recup_dir.1`.

PhotoRec memorizza un report, in formato XML, nel file `report.xml`, contenente dettagli sui file e sulla fase di recupero. Nella prima parte del report, vengono indicate informazioni sulla versione di PhotoRec, sull'immagine sorgente, sulla versione del S= sui cui si è svolta la fase di recupero, ecc. Nella seconda parte del report, per ciascun file recuperato, vengono diverse informazioni, fra cui: nome assegnato da PhotoRec, dimensione del file (espressa in byte).

## 3.7 Il tool Bulk Extractor

Foremost, Scalpel e PhotoRec sono tool per recuperare file eliminati, in accordo alle tipologie specificate o supportate. In alcuni scenari, potrebbe essere estremamente utile recuperare direttamente dati significativi (ad esempio, indirizzi email, numeri di telefono, ecc.) invece di recuperare interi file. Per far ciò, è possibile utilizzare il tool Bulk Extractor. Bulk Extractor è utilizzabile mediante il comando `bulk_extractor` e può essere eseguito dal terminale di Kali Linux: `bulk_extractor -o <dir> <file>`

- `-o`: Permette di specificare la directory di output, dove verranno memorizzati i file, contenenti i dati estratti, tramite il processo di data carving, operato da Bulk Extractor.
- `<file>`: Permette di specificare il percorso del file di input. OSSERVAZIONE: il file di input deve essere una immagine forense, precedentemente acquisita.

### 3.7.1 Esempio di utilizzo

L'esempio si baserà sull'immagine "terry-work-usb-2009-12-11.E01". Per avviare il procedimento di estrazione utilizziamo il seguente comando: "`bulk_extractor -o bulk_output terry-work-usb-2009-12-11.E01`". L'output del processo verrà riportato nella cartella specificata, ovvero, `bulk_output`.

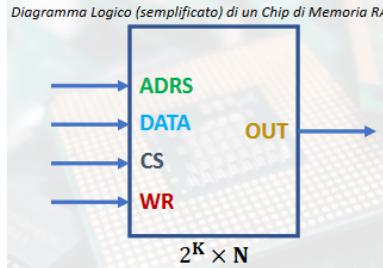
Al termine del processo, Bulk Extractor mostra alcune informazioni utili, fra cui: numero di MB elaborati, valore di Hash (MD5) dell'immagine elaborata e numero di indirizzi email individuate. Al termine del processo, sarà possibile visionare i file, generati da Bulk Extractor, i quali sono contenuti nella cartella bulk\_ouput. Viene generato anche un report, in formato XML, relativo al processo di estrazione, denominato report.xml. I file che contengono per sempio la sottostringa ccn (ad esempio, ccn.txt, ccn\_histogram.txt, ecc.) sono riferiti a numeri di carte di credito, stessa cosa per numero di telefono, email, ecc... Non tutti i file contengono dati, i file contenenti dati hanno dimensione > 0 byte.

# Capitolo 4

## Alcuni richiami su argomenti dementi

### 4.1 Memoria RAM

La memoria Random Access Memory (RAM) è una memoria volatile. Tutte le informazioni sono perse, quando non vi è alimentazione elettrica. Nella memoria RAM, i dati sono organizzati in celle (dette anche word). Ogni cella è accessibile mediante un indirizzo, in un tempo costante. Affinché un programma possa essere eseguito, deve essere «caricato» dal disco fisso, alla memoria RAM. La memoria RAM è decisamente più veloce del disco fisso. Dal punto di vista hardware, la memoria RAM è costituita da diversi chip di memoria.



- k indica che ciascun indirizzo è composto da kbit ( $2^k$  indirizzi/celle)
- N indica che ciascuna cella (word) è composta da N bit
- ADRS → Address (Indirizzo) di kbit
- DATA → Dato da scrivere di N bit
- CS → Chip Select → Abilita (valore 1) o disabilita (valore 0) il chip.
- WR → Specifica l'operazione da eseguire: scrittura (valore 1) o lettura (valore 0)
- OUT → OUTput → Valore di N bit
- Se CS ha valore 1, WR setta il suo bit a 1, si abilita l'operazione di scrittura quindi scrive il valore di DATA (N bit) all'indirizzo specificato dal valore di ADRS (K bit).
- Se CS ha valore 1, WR setta il suo bit a 0, si abilita l'operazione di lettura quindi accede all'indirizzo specificato da ADRS (K bit) e ne restituisce il contenuto in OUT (N bit)

### Principali categorie

In base alla tipologia dei chip, è possibile suddividere la memoria RAM in due categorie:

- RAM Statica (Static RAM – SRAM): I chip che costituiscono le memorie SRAM possono mantenere dati per un tempo potenzialmente infinito. Per questo motivo, tale tipologia di RAM, viene detta statica. Consumi ridotti e poca produzione di calore. Sensibilmente più veloci (e più costose) delle DRAM. Utilizzate tipicamente nelle cache (ad esempio, la cache di primo livello, detta anche L1, delle CPU). Hanno una capienza limitata.
- RAM Dinamica (Dynamic RAM – DRAM): I chip che costituiscono la memoria DRAM possono mantenere i dati, in maniera affidabile, solo per un certo lasso di tempo. È quindi necessario che i dati vengano ricaricati (operazione di refresh), con una certa frequenza, affinché possano essere mantenuti, in maniera affidabile, per periodi temporali, più estesi del suddetto lasso di tempo. Le operazioni di refresh influiscono anche sui tempi di accesso ai dati. Le DRAM sono sensibilmente più economiche delle SRAM e sono comunemente utilizzate (come memoria centrale) in diversi dispositivi (computer, smartphone, ecc.)

### Principali Tipologie di Memoria DRAM

- Extended Data Output RAM (EDO RAM): una delle prime tipologie di DRAM.
- Synchronous Dynamic RAM (SDRAM): la SDRAM è una DRAM sincrona poiché prevede un segnale di clock che sincronizza le operazioni di scambio di dati con la CPU. Velocità oltre le 3 volte superiore rispetto alle EDO RAM. Maximum Transfer Rate pari a 133 MT/s (dove MT indica Milioni di Trasferimenti).
- Double Data Rate SDRAM (DDR-DRAM o DDR o DDR1): raddoppiano la capacità di trasferimento delle memorie SDRAM. Maximum Transfer Rate pari a 400 MT/s.
- DDR2: raddoppiano la capacità di trasferimento delle memorie DDR1. Maximum Transfer Rate pari a 800 MT/s
- DDR3: consumi energetici sensibilmente ridotti rispetto alle memorie DDR2. Maximum Transfer Rate pari a 1600 MT/s
- DDR4: Maximum Transfer Rate pari a 3200 MT/s.

### Aspetto Fisico di un Modulo di Memoria DRAM



La memoria DRAM è generalmente organizzata in moduli, i quali sono costituiti da un certo numero di chip di memoria. È composta da connettori: la tacchetta, all'interno dei connettori, serve per il far sì che il modulo di RAM venga inserito in maniera corretta nell'alloggiamento (slot). I fori necessari per mantenere ben «ancorato» il modulo di memoria RAM, all'interno dell'apposito alloggiamento.

## 4.2 Memoria Virtuale

La memoria virtuale costituisce un'astrazione, gestita dai sistemi operativi. Permette di simulare uno spazio di memoria centrale maggiore di quello fisicamente presente o disponibile. Viene utilizzato un apposito spazio (detto, talvolta, area di swap o di paging) di una memoria secondaria (ad esempio, un disco fisso). Il suo scopo è di elaborare dati/eseguire processi, la cui necessità di spazio eccederebbe lo spazio disponibile nella memoria RAM. L'Elaborazione di grandi quantitativi di dati ed esecuzione di processi di grandi dimensioni.

I meccanismi di gestione della memoria virtuale, permettono di associare un indirizzo di memoria virtuale ad un indirizzo fisico. La memoria virtuale è suddivisa in blocchi, chiamati pagine (page). La tabella delle pagine si occupa dell'associazione tra pagine relative (riferite alla memoria virtuale) a pagine fisiche ( dette anche frame).

# Capitolo 5

## Memory Acquisition

Analisi di un live system (sistema acceso) analizzando la memoria RAM (memory analysis), insieme ai processi in esecuzione, di alcune attività di rete, ecc.

Possibile irripetibilità di alcuni passi, si deve minimizzare l'impatto sul sistema.

Alcuni passi della live analysis, potrebbero quindi risultare irripetibili, per via principalmente delle seguenti problematiche:

- Problematiche di Carattere Tecnico: Non è possibile effettuare l'eventuale analisi di alcuni dati, senza alterare (quantomeno in parte) lo stato del sistema (contenuto della memoria RAM, ecc.).  
**NOTA:**Anche la fase di acquisizione di alcuni dati, può provocare l'alterazione dello stato della macchina (ad esempio, l'acquisizione del contenuto della memoria RAM)
- Problematiche di Carattere Temporale: È necessario considerare inoltre che lo stato della macchina, all'atto dell'attività, è frutto del «momento». È estremamente complesso (se non impossibile) riprodurre lo stato

Poiché, come precedentemente osservato, non tutti i dati hanno la stessa volatilità, è assolutamente definire un ordine di volatilità (Order Of Volatility – OOV). In virtù della natura volatile, della memoria RAM, i dati in essa contenuti, hanno generalmente elevata priorità nell'OOV. Risulta quindi importante il processo di acquisizione del contenuto della memoria (memory acquisition).

### 5.1 Memory Dump e Processo di Memory Acquisition

Ricordiamo che un memory dump (detto talvolta memory image) è una «istantanea» del contenuto della memoria RAM. Il processo di acquisizione di un memory dump è detto memory acquisition (o memory imaging). Un memory dump può essere acquisito da tool esterni.Talvolta, è il S.O. stesso che produce automaticamente un memory dump. Ad esempio, al verificarsi di un problema grave ed irreversibile, all'interno del sistema, il quale deve necessariamente essere riavviato poiché non può più assicurare un comportamento corretto.

#### 5.1.1 Tipologie di memory dump

Esistono diverse tipologie di memory dump, fra cui:

- Memory dump in formato RAW:
  - Pro: copia «esatta» del contenuto della memoria RAM, analogia con le immagini forensi, generate dal tool come, ad esempio, DC3DD, ecc.

- Contro: non contiene lo stato del processore (contenuto dei registri)
- Memory dump prodotti automaticamente dal S.O. [sistemi Windows-based]:
  - Memory dump prodotto in seguito ad un grave crash di sistema
  - Memory dump prodotto dal processo di ibernazione (dove il processo di ibernazione è avviato dall'utente)

### Memory Dump | Prodotto a causa di Gravi Crash

Nei sistemi Windows-based, al verificarsi di un grave crash del S.O. (a seguito del quale è necessario effettuare il riavvio del sistema), viene generata una BSoD (Blue Screen of Death). Nei recenti sistemi Windows-based, dopo aver mostrato all'utente la BSoD, il S.O. produce automaticamente un memory dump. È possibile utilizzare tale memory dump, al fine di individuare la possibile causa, che ha condotto al crash del sistema (ad esempio, problema con un applicativo, problema con un driver, ecc.).

- Pro: include tutte le pagine gestite dal Windows Memory Manager (sistema di gestione della memoria di Windows). Include aspetti relativi all'utente ed al kernel
- Contro: non è disponibile su sistemi a 32 bit e non acquisisce alcuni dati iniziali (ad esempio, password –cifrate– dell'autenticazione, ecc.)

### Memory Dump | Prodotto dal Processo di Ibernazione

Grazie al processo di ibernazione (o sospensione), è possibile spegnere il sistema, mantenendo esattamente il suo «stato» (contenuto della memoria RAM/altre memorie volatili, contenuto del disco fisso, ecc.). Alla riattivazione del sistema, verrà ripristinato lo stato del sistema, al momento, immediatamente precedente, dell'avvio dell'ibernazione. Durante il processo di ibernazione, viene acquisito anche un memory dump (utilizzato per ripristinare il contenuto della memoria RAM, alla riattivazione del sistema).

- Pro: memorizza, all'interno del file hiberfil.sys, diverse informazioni: Contenuto dei registri, Memory dump
- Contro: disponibile solo per alcune versioni di Windows (da Windows 98 a Windows Vista). Viene eseguita esclusivamente se l'utente richiede l'ibernazione del sistema

## 5.2 Tool Esterni per la creazione di Memory Dump

Vi sono molti tool esterni Open-Source e commerciali che permettono la memory acquisition. Un tool esterno deve essere eseguito direttamente sul live system Memory Acquisition. **NOTA:** L'esecuzione stessa di tale tool, impatta sul contenuto della memoria RAM, del live system.

### 5.2.1 Il tool FTK® Imager®

FTK® (Forensic Toolkit®) Imager è un software sviluppato da AccessData. Permette di creare immagini forensi di differenti supporti (dischi fissi, CD/DVD, ecc.) e memory dump. Benché il tool risulti particolarmente completo ed efficace, verranno brevemente trattati solo degli aspetti relativi alla memory acquisition.

### 5.2.2 Il tool DumpIt

DumpIt è utilizzabile su sistemi Windows a 32 bit (x86) ed a 64 bit (x64) è un tool con interfaccia a linea di comando. Capace di acquisire memory dump, in formato RAW, e di effettuare la comparazione tramite una funzione di hash.

## 5.3 Memory Analysis con il Volatility Framework

All'interno della RAM (e del file di paging), è possibile individuare diversi dati, potenzialmente rilevanti (password, informazioni dell'utente, ecc...). Considerati i suddetti aspetti, è estremamente significativo effettuare una investigazione forense sulla memoria (memory forensics).

Il Volatility Framework permette l'analisi della memoria. È Open-Source, installabile mediante il comando: `sudo apt-get install volatility`

### 5.3.1 Volatility ed i Plugin

Volatility permette di estrarre specifiche informazioni dal memory dump, su cui si sta conducendo l'analisi, tramite l'utilizzo dei plugin. Ad esempio, è possibile estrarre informazioni specifiche sui processi, informazioni specifiche sulle attività di rete, ecc. Sono supportati molteplici plugin dal Volatility Framework. La lista completa dei plugin (con una descrizione sintetica per ciascun plugin) è specificata dall'help di Volatility (opzione `-h`, vista nella slide precedente).

### 5.3.2 Formati di Memory Dump analizzabili da Volatility

Volatility è in grado di analizzare diversi formati di memory dump, fra i quali: formato RAW (estensione `.dd`, `.img`, `.dmp`, `.mem`, ...), memory dump automaticamente prodotti da sistemi Windows-based (relativi a crash/ibernazioni), memory dump acquisiti da Virtual Machine e anche i memory dump, acquisiti dai tool, discussi precedentemente, possono essere analizzati da Volatility.

#### Sintassi

```
volatility -f <file> [plugin] [options]
```

- `-f`: Permette di specificare il percorso del file di input. NOTA: il file di input deve essere un memory dump, in uno dei formati supportati.
- `plugin`: Permette di specificare il nome del plugin, da utilizzare (parametro opzionale)
- `options`: Permette di specificare eventuali opzioni (se necessarie)

### 5.3.3 Profili del Volatility framework

Al fine di analizzare, in maniera più accurata possibile, un memory dump, è quindi necessario conoscere il profilo del S.O. (ovvero, la tipologia, la versione, ecc.), da cui è stata effettuata l'acquisizione. Tramite il profilo, è possibile risalire all'organizzazione logica della memoria RAM (e conseguentemente del memory dump).

Volatility ha precaricati diversi profili, relativi a molteplici S.O. Se non si conosce il profilo del S.O., Volatility è in grado di suggerirci, analizzando il memory dump, il/i profilo/i più adeguato/i, mediante il plugin `imageinfo`.

#### Memory dump usato per i prossimi test

Nei prossimi esempi, verrà utilizzato un memory dump di esempio, denominato `cridex.vmem`. Memory dump acquisito su un sistema con Windows XP, in esecuzione su una macchina virtuale (VMWare)

### 5.3.4 Plugin imageinfo

Utilizziamo il plugin imageinfo, per avere indicazioni sui profili suggeriti da Volatility (simulando di non disporre di alcuna informazione, in merito al memory dump, denominato cridex.vmem), es: `volatility -f cridex.vmem imageinfo`.

In output avremo diverse informazioni come il numero di processori (o numero di core), presenti nel sistema, da cui è stato acquisito il memory dump (nome del campo number of processor). Vengono riportate anche informazioni riguardanti la data e l'ora in cui è stato acquisito il memory dump. Infine i profili suggeriti (Suggested Profile(s)), da Volatility, mediante il plugin imageinfo, sono i seguenti due:

- WinXPSP2x86
- WinXPSP3x86

Dove WinXP, fa riferimento al Sistema Operativo Microsoft Windows XP; SP2 e SP3, sono riferite rispettivamente alla Service Pack 2 (SP2) ed alla Service Pack 3 (SP3)<sup>6</sup> e infine x86, fa riferimento alla versione del S.O., progettato/ottimizzato per CPU con architettura a 32 bit.

### 5.3.5 Categorie di Plugin

Possiamo suddividere i plugin del Volatility Framework, in diverse categorie.

#### Analisi dei Processi

Il Volatility Framework permette di elencare i processi ed ottenere diverse informazioni su di essi (ad esempio, la data e l'ora in cui il processo è stato avviato, ecc.). Per ottenere tali informazioni è possibile utilizzare i seguenti plugin:

- pslist: `volatility -profile=WinXPSP3x86 -f cridex.vmem pslis`. viene mostrata la lista dei processi (sia avviati direttamente dal sistema sia avviati dall'utente). Per ciascuno dei processi (riportati sulla righe), vengono mostrate anche le due seguenti informazioni: PID (Process ID) riferito al processo e PPID (Parent Process ID) riferito al processo padre. Per ciascuno dei processi (riportati sulle righe), viene inoltre riportata anche la data e l'ora in cui esso è stato avviato (colonna: Start)

Nome Processo	Descrizione (Cenni)
<code>smss.exe</code>	Acronimo di <b>SessiOn Manager SubSystem</b>  Responsabile dell'avvio della sessione utente; è inizializzato da Windows (termina generalmente quando il sistema viene spento). Inoltre, avvia il processo Winlogon ( <code>winlogon.exe</code> ) ed il processo <code>csrss.exe</code>
<code>csrss.exe</code>	Acronimo di <b>ClienT/Server Run-time SubSystem</b>  Responsabile della gestione delle applicazioni del prompt dei comandi (terminale), ecc.

---

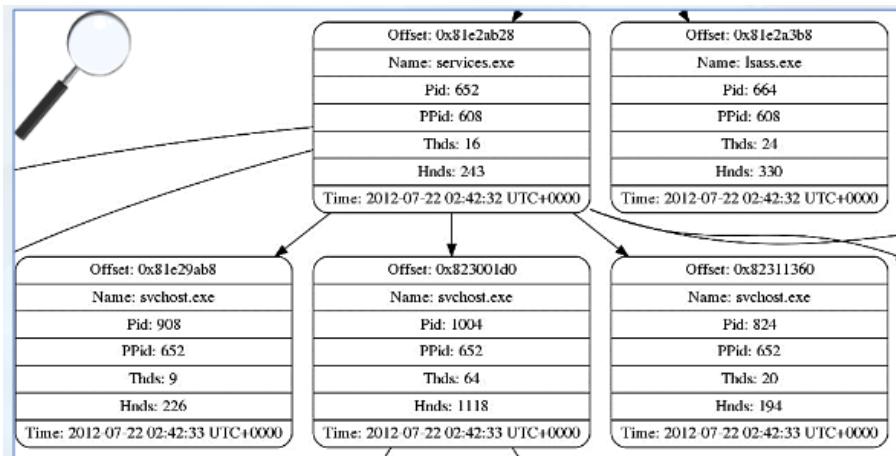
<sup>6</sup>Una Service Pack (SP) è un insieme di correzioni e patch, scaricabile ed installabile, per un software o per un sistema operativo

Nome Processo	Descrizione (Cenni)
winlogon.exe	Si occupa della fase di autenticazione (logon)/disconnessione in Windows (contrazione di <b>Windows Logon</b> )
scvhost.exe	Processo host generico che permette l'esecuzione (e download) dei servizi di Windows, memorizzati nelle librerie DLL ( <i>maggiori dettagli sulle librerie DLL, in seguito</i> )
explorer.exe	Esegue il Windows Program Manager (o Windows Explorer), ovvero, il gestore dell'interfaccia grafica di Windows
spoolsv.exe	Esegue il servizio di spooling della stampante, ovvero un servizio che si occupa del caching dei lavori in fase di stampa, ecc. (contrazione di <b>Spooler Service</b> )

Nome Processo	Descrizione (Cenni)
winlogon.exe	Si occupa della fase di autenticazione (logon)/disconnessione in Windows (contrazione di <b>Windows Logon</b> )
scvhost.exe	Processo host generico che permette l'esecuzione (e download) dei servizi di Windows, memorizzati nelle librerie DLL ( <i>maggiori dettagli sulle librerie DLL, in seguito</i> )
explorer.exe	Esegue il Windows Program Manager (o Windows Explorer), ovvero, il gestore dell'interfaccia grafica di Windows
spoolsv.exe	Esegue il servizio di spooling della stampante, ovvero un servizio che si occupa del caching dei lavori in fase di stampa, ecc. (contrazione di <b>Spooler Service</b> )

- pstree: volatility -profile=WinXPSP3x86 -f cridex.vmem pstree. Analogamente al plugin pslist, il plugin pstree mostra la lista dei processi. In questo caso, la lista è ad «albero», infatti, vengono indentati i processi figli, in modo che risulti più immediato distinguere i processi padri ed i processi figli. Mediante i seguenti due comandi è possibile ottenere una rappresentazione grafica, relativa all'albero dei processi. La rappresentazione grafica viene memorizzata in una immagine (nell'esempio, nell'immagine processi.jpg):

```
volatility -profile=WinXPSP3x86 -f cridex.vmem pstree --output=dot --output-file=processi.dot
dot -Tjpg processi.dot > processi.jpg
```



- psscan: volatility –profile=WinXPSP3x86 -f cridex.vmem psscan. Mediante il plugin psscan, il Volatility Framework mostra la lista dei processi, includendo eventuali processi nascosti. **NOTA:** I processi nascosti potrebbero essere indice della presenza di malware, questi ultimi, cercano di nascondersi sia all'utente sia ai software anti-malware, al fine di effettuare azioni malevoli. Al fine di individuare eventuali processi nascosti (da malware, ecc.), è consigliato comparare l'output ottenuto con il plugin pslist e l'output ottenuto con il plugin psscan. Anche qui tramite il comando dot si può rappresentare l'albero:

```
volatility –profile=WinXPSP3x86 -f cridex.vmem psscan –output=dot –output-file=processi.dot
dot –Tjpg processi.dot > processi.jpg
```

- psxview: volatility –profile=WinXPSP3x86 -f cridex.vmem psxview. Utilizzato per individuare eventuali processi nascosti (riconducibili a malware). Permette di effettuare una comparazione incrociata, considerando l'output di diversi plugin, atti ad elencare i processi in memoria. Considera anche l'output dei plugin pslist e psscan. Vengono stampati elenco (parziale) dei plugin considerati, elenco dei processi, individuati da tutti i plugin considerati. Per ciascuno dei processi (riportati sulle righe), viene indicato se esso è stato individuato (valore True) o meno (valore False), dal plugin, specificato dalla colonna. Per ciascuno dei processi (riportati sulle righe), viene indicato se esso è stato individuato (valore True) o meno (valore False), dal plugin pslist. Per ciascuno dei processi (riportati sulle righe), viene indicato se esso è stato individuato (valore True) o meno (valore False), dal plugin psscan (visto nelle slide precedenti). È possibile osservare che tutti i processi sono elencati sia dal plugin pslist sia dal plugin psscan, infatti, tutte le relative entry, hanno valore True. Pertanto, in questo caso, non sono stati individuati possibili processi nascosti.

Name	pslist	psscan	thrdproc	pspcid	csrss	session	deskthrd
winlogon.exe	True	True	True	True	True	True	True
svchost.exe	True	True	True	True	True	True	True
alg.exe	True	True	True	True	True	True	True
spoolsv.exe	True	True	True	True	True	True	True
services.exe	True	True	True	True	True	True	True
svchost.exe	True	True	True	True	True	True	True
reader_sl.exe	True	True	True	True	True	True	True
svchost.exe	True	True	True	True	True	True	True
svchost.exe	True	True	True	True	True	True	True
svchost.exe	True	True	True	True	True	True	True
wuauctl.exe	True	True	True	True	True	True	True
wuauctl.exe	True	True	True	True	True	True	True
lsass.exe	True	True	True	True	True	True	True
explorer.exe	True	True	True	True	True	True	True
svchost.exe	True	True	True	True	True	True	True
smss.exe	True	True	True	True	False	False	False
System	True	True	True	True	False	False	False
csrss.exe	True	True	True	True	False	True	True

### 5.3.6 Identificazione di Attività di Rete

I servizi e le connessioni di rete, utilizzati dai processi, possono fornire molte informazioni rilevanti, quali ad esempio, indirizzi IP locali e remoti, le porte utilizzate, ecc. I seguenti plugin sono quelli principalmente utilizzati per carpire informazioni circa servizi e/o connessioni di rete:

- connections: volatility –profile=WinXPSP3x86 -f cridex.vmem connections. Mostra le connessioni attive, riportando, per ciascuna di esse, le seguenti informazioni:
  - PID (Process ID) del processo, a cui è riferita la connessione
  - IP locale (con la relativa porta della connessione)
  - IP remoto (con la relativa porta della connessione)

**NOTA:** questo plugin può essere utilizzato esclusivamente da memory dump, acquisiti da PC con Windows XP o Windows 2003 Server (32/64 bit).

- connscan: volatility –profile=WinXPSP3x86 -f cridex.vmem connscan. Mostra le connessioni attive e terminate, riportando, per ciascuna di esse, le seguenti informazioni:
  - PID (Process ID) del processo, a cui è riferita la connessione
  - IP locale (con la relativa porta della connessione)
  - IP remoto (con la relativa porta della connessione)

**NOTA:** questo plugin può essere utilizzato esclusivamente da memory dump, acquisiti da PC con Windows XP o Windows 2003 Server (32/64 bit).

- sockets: volatility –profile=WinXPSP3x86 -f cridex.vmem sockets. Mostra informazioni aggiuntive sulle connessioni, in cui sono presenti socket in «ascolto» (stato di listening). Sono supportati i protocolli:
  - TCP
  - UDP

**NOTA:** questo plugin può essere utilizzato esclusivamente da memory dump, acquisiti da PC con Windows XP o Windows 2003 Server (32/64 bit).

- netscan: volatility –profile=<Profilo> -f <MemoryDump> netscan. Per memory dump, acquisiti da sistemi Windows-based, con una versione di Windows Vista o superiore (32 o 64 bit), è possibile utilizzare il plugin netscan. Tale plugin permette di individuare tracce di attività di rete, relative a connessioni basate su protocolli TCP e UDP. Per ciascuna attività di rete, individuata, vengono riportate diverse informazioni, fra cui:
  - Indirizzo IP locale (e la relativa porta) ed indirizzo IP remoto (e la relativa porta)
  - Data/ora relativa al momento in cui la connessione è stata avviata
  - Ecc.

### 5.3.7 Analisi di librerie DLL (Dynamic Link Library) di Windows

Una libreria DLL (Dynamic Link Library) è costituita da porzioni di codice (simili a funzioni) e da dati più processi possono utilizzare simultaneamente la medesima libreria DLL. Grazie alle librerie DLL è possibile progettare un programma e suddividerlo in moduli (dove ogni modulo è una libreria DLL). Un processo può caricare dinamicamente (dynamic) la libreria DLL (se installata). Il loro vantaggio è una riduzione dei tempi di caricamento, poiché i moduli vengono caricati solo in caso vi sia effettiva necessità.

L'identificazione dei processi, che caricano delle librerie DLL, e la versione delle librerie stesse, può essere di aiuto nella correlazione di diversi processi, inoltre, mediante i processi e le librerie DLL, è possibile eventualmente mettere in relazione eventuali account multipli, di un utente. Fra i vari plugin, preposti per l'analisi delle DLL, possiamo individuare i seguenti:

- verinfo: volatility --profile=WinXPSP3x86 -f cridex.vmem verinfo. Mostra informazioni estremamente dettagliate, in riferimento alle librerie DLL, utilizzate da processi generati da Portable Executable (PE) di Windows. Un eseguibile PE è strutturato in modo tale che possa contenere tutto il necessario per l'esecuzione in Windows, senza utilizzo di ulteriori file o librerie esterne.
- dlllist: volatility --profile=WinXPSP3x86 -f cridex.vmem dlllist. Per ciascun processo, vengono mostrate tutte le librerie DLL, utilizzate da tale processo.

### 5.3.8 Informazioni sul Registro di Sistema del S.O. Windows

Il registro è una componente dei sistemi Windows-based e memorizza informazioni in merito a diversi aspetti, impostazioni e preferenze, fra cui:

- Impostazioni/Preferenze del S.O. stesso
- Impostazioni/Preferenze di alcuni programmi
- Impostazioni/Preferenze di driver
- Ecc.

Vengono inoltre memorizzate anche alcune preferenze dell'utente. Dal punto di vista forense, il registro è una risorsa notevole, poiché è una sorta di database, contenente tantissimi valori, dai quali estrarre informazioni. Il registro ha una struttura gerarchica ad albero, è suddiviso in cinque chiavi radice, all'interno delle quali sono presenti sotto-chiavi e valori:

- HKEY\_CLASSES\_ROOT: descrive il comportamento di Windows, in relazione ad alcune azioni dell'utente. Esempi: cosa deve fare il sistema quando viene collegato un nuovo drive al PC (ad esempio, una Penna USB, ecc.). Quale programma deve essere avviato, dal sistema, all'apertura di un file con una specifica estensione.
- HKEY\_CURRENT\_USER: contiene le configurazioni di Windows e le configurazioni del software installato, in relazione all'utente autenticato (ad esempio, sfondo selezionato, variabili d'ambiente, configurazione del layout della tastiera, ecc.).
- HKEY\_LOCAL\_MACHINE: contiene configurazioni in merito alla maggior parte del software installato, configurazioni in merito a Windows stesso ed informazioni, relative ad hardware e driver.
- HKEY\_USERS: Sono presenti dati ed informazioni, in merito a tutti gli utenti connessi al sistema.
- HKEY\_CURRENT\_CONFIG: contiene sotto-chiavi che puntano a configurazioni riferite all'hardware in uso.

Ogni chiave radice corrisponde ad uno o più file, presenti nel file system. I suddetti file vengono spesso chiamati hive (letteralmente, alveari). Poiché il registro è potenzialmente acceduto, in maniera frequente, dal S.O., alcune informazioni sugli hive ed alcune informazioni del registro, sono generalmente mantenute in memoria. Il Volatility Framework prevede diversi plugin, per individuare informazioni sugli hive e sul registro. Un plugin particolarmente utile è il seguente:

- hivelist: volatility –profile=WinXPSP3x86 -f cridex.vmem hivelist. Mediante il plugin hivelist, è possibile ottenere informazioni sugli hive, individuati all'interno del memory dump. Viene indicato il percorso degli hive, all'interno del file system. In questo modo, sarà possibile localizzare gli hive.

### 5.3.9 Altri plugin

- filescan: volatility –profile=WinXPSP3x86 -f cridex.vmem filescan. Un processo che intende creare, scrivere o leggere un certo file, deve effettuarne preliminarmente l'apertura. Windows mantiene, in memoria, i «riferimenti» di tutti i file aperti. Tramite il plugin filescan, vengono cercati, all'interno del memory dump, tutti i suddetti riferimenti. Il plugin filescan elencherà quindi tutti i file aperti ed eventuali file non visibili, da alcuni tool standard (i file non visibili potrebbero potenzialmente essere nascosti da un malware). Per ciascun file, verrà riportato il percorso completo ed i permessi effettivamente garantiti al file. Nell'elenco dei file, riportato dal plugin filescan, è possibile individuare anche tracce di file eseguibili (.exe). È importante considerare anche gli eseguibili (ed eventualmente anche le librerie DLL), poiché potrebbero essere stati aperti da malware, al fine di modificarli, iniettandovi del codice malevole.

#### Permessi file

I permessi sono esplicitati nel formato, specificato dalla seguente espressione regolare: (R|-)(W|-)(D|-)(r|-)(w|-)(d|-)

- R|–) è riferito al permesso di lettura (il carattere R indica che tale permesso è garantito, invece, il carattere - indica che tale permesso non è garantito)
- (W|–) è riferito al permesso di scrittura (il carattere W indica che tale permesso è garantito, invece, il carattere - indica che tale permesso non è garantito)
- (D|–) è riferito al permesso di cancellazione (il carattere D indica che tale permesso è garantito, invece, il carattere - indica che tale permesso non è garantito)

Il blocco (r|–)(w|–)(d|–) è riferito ai diritti di accesso, concessi contemporaneamente a due o più client, che condividono il file (ad esempio, file contenuti in cartelle condivise, ecc.)

- timeliner: volatility –profile=WinXPSP3x86 -f cridex.vmem timeliner. Il plugin timeliner risulta particolarmente utile agli investigatori, poiché permette di ottenere una timeline degli eventi individuati nel memory dump. Gli eventi vengono raggruppati in base alla data e all'orario (avvio di un processo, utilizzo di una libreria DLL, utilizzo del registro di Windows, ecc.).
- malfind: volatility –profile=WinXPSP3x86 -f cridex.vmem malfind. Il plugin malfind aiuta gli investigatori nell'individuazione di eventuali malware, riportando codice potenzialmente malevolo iniettato nella memoria. Si basa su alcune caratteristiche proprie dei malware, per individuare codice potenzialmente malevolo. È importante identificare eventuali malware, poiché potrebbero aver svolto operazioni malevole, all'insaputa dell'utente. Pertanto, l'investigatore dovrebbe essere in grado di individuare quali sono tali operazioni, onde evitare di attribuirle all'utente.

### Opzione -p

volatility –profile=WinXPSP3x86 -f cridex.vmem malfind –p 608. Mediante l’opzione –p è possibile specificare il PID di uno dei processi Nell’esempio, il PID specificato è pari a 608 (ovvero, il processo winlogon.exe).

## 5.4 Ulteriori Tool Utili

### 5.4.1 VMMap

Il tool VMMap è in grado di fornire dettagli accurati sulla memoria (fisica e virtuale), utilizzata da un processo in Windows. Mostra la suddivisione della memoria, allocata per un processo. Mostra utili rappresentazioni grafiche della memoria ed ulteriori informazioni dettagliate. Da utilizzare direttamente sul live system.

### 5.4.2 Il tool InsideClipboard

Negli Appunti di Windows (Clipboard) potrebbero essere presenti delle informazioni di interesse all’investigazione forense. Componente del S.O. che permette lo scambio di dati (testo, immagini, ecc.), da una applicazione all’altra. Alcune Operazioni, in cui tale componente è coinvolto:

- Copia e Incolla
- Taglia e Incolla
- Drag & Drop (trascinamento)
- I dati «copiati» e/o «tagliati», vengono temporaneamente mantenuti in memoria RAM

Il tool freeware InsideClipboard, sviluppato dalla NirSoft, permette di visualizzare i dati contenuti negli appunti di Windows. Visualizzazione dei dati, presenti negli appunti, in diversi formati (es., ASCII, esadecimale, ...). Da utilizzare direttamente sul live system, non necessita di installazione e file aggiuntivi.

# Capitolo 6

## Analisi

### 6.1 Il tool Autopsy

Il tool Autopsy permette di effettuare efficientemente l'analisi di dischi fissi, immagini forensi, ecc. Supporta diversi formati di immagini forensi, incluso il formato RAW, il formato EWF ed il formato AFF. Presenta una architettura modulare, con possibilità di realizzare plugin e/o moduli personalizzati. Fornisce una semplice ed efficace GUI (Graphical User Interface). La maggior parte delle operazioni eseguibili con Autopsy, sono eseguibili anche mediante la suite The Sleuth Kit (TSK), tramite l'interazione con il terminale. I tool di tale suite sono utilizzabili esclusivamente tramite terminale (Command Line Interface – CLI). Il tool Autopsy permette di svolgere diverse attività, fra le quali:

- Analisi di immagini forensi: permette l'analisi di una immagine forense, mostrandone informazioni su file e/o directory
- Timeline in merito alle attività sui file: permette la realizzazione di una timeline, in base ai timestamp dei file (data/ora di creazione/accesso/modifica)
- Verifica dell'integrità di immagini forensi: calcola l'hash MD5 di immagini forensi e/o di file/directory specifici
- Ricerca mediante keyword: permette di ricercare dati/informazioni mediante delle keyword e/o espressioni regolari
- Analisi dei file e analisi di metadati: permette di visualizzare i dettagli relativi ai metadati e permette l'analisi di specifici file/directory

#### 6.1.1 Creazione di un nuovo caso

1. Cliccare sul bottone «New Case»
2. Inserire le informazioni riguardanti il nome del caso (Case Name), la descrizione (Description), il nome degli investigatori (Investigator Names), ecc.
3. Dopo aver compilato i vari campi (come nell'esempio), è necessario fare click su «New Case». Ci viene indicato che il caso Primo è stato creato e le relative informazioni sono memorizzate nella cartella /var/lib/autopsy/Primo.

**NOTA:**la cartella /var/lib/autopsy è la cartella denominata Evidence Locker, specificata all'avvio del tool, ed è la cartella in cui vengono memorizzate tutte le informazioni dei vari casi, registrati da Autopsy. Cliccare su «Add Host» per proseguire.

## 6. Analisi

---

4. Inserire i dettagli relativi al nome del computer su cui si sta investigando (Host Name) e la relativa descrizione (Description)
5. È inoltre possibile aggiungere opzionalmente ulteriori dettagli dell'host, fra cui: fuso orario (Time zone), è possibile opzionalmente specificare il fuso orario (se non viene specificato niente, si utilizza il fuso orario del Sistema Operativo)
6. Cliccare sul tasto «Add Host» per proseguire
7. Verrà mostrata la conferma che l'host (nell'esempio, host1) è stato aggiunto correttamente e verranno indicate le informazioni relative alle directory, in cui è avvenuta la memorizzazione delle informazioni. Cliccare quindi su «Add Image» per proseguire
8. Cliccare sul tasto «Add Image File» per aggiungere una immagine forense
9. Specificare, in primo luogo, la posizione (location) dove è memorizzata l'immagine forense (nel-l'esempio, /host/Scrivania/8-jpeg-search.dd). Viene poi richiesto se l'immagine è relativa ad un intero disco fisico (Disk), oppure, è relativa ad una singola partizione (Partition). Infine, viene richiesto di specificare il metodo di importazione (Import Method), in virtù del fatto che l'immagine deve essere necessariamente acceduta dalla cartella Evidence Locker. Le possibilità sono le seguenti:
  - La creazione di un collegamento (link) simbolico (opzione Simlink) all'immagine specificata, all'interno della cartella Evidence Locker. Con un collegamento simbolico si evitano i rischi legati alla copia e spostamento.
  - La creazione di una copia (opzione Copy), dell'immagine specificata, all'interno cartella Evidence Locker.
  - Lo spostamento dell'immagine all'interno della cartella Evidence Locker (opzione Move).
10. Cliccare sul tasto «Next» per proseguire
11. Verranno mostrati diversi dettagli dell'immagine importata. Selezioniamo la checkbox «Calculate» e spuntiamo la checkbox «Verify hash after importing?», per verificare l'integrità dell'immagine importata
12. Come ulteriori informazioni, è possibile osservare come venga indicato che il file system dell'immagine è di tipo NTFS
13. Cliccare su «Add» per proseguire
14. Dopo aver cliccato «Add», al passo precedente, viene riportato il valore dell'hash MD5 ed il link simbolico creato, nella cartella Evidence Locker. Possiamo quindi cliccare il tasto «OK», per proseguire; eventualmente, è anche possibile inserire una ulteriore immagine (cliccando il tasto «Add Image»)
15. A questo punto, è possibile avviare il processo di analisi dell'immagine importata.
16. È preferibile però effettuare prima una verifica dell'integrità dell'immagine importata, cliccando sul tasto «Image Integrity». Viene poi mostrato il nome dell'immagine (8-jpeg-search.dd) e l'hash MD5
17. Cliccando su «Validate», è possibile visualizzare il risultato della validazione. Clicchiamo su «Close», per ritornare al menu precedente
18. È ora possibile cliccare sul tasto «Analyze» per iniziare il processo di analisi.

### 6.1.2 Analisi mediante Autopsy



- Per avere informazioni dettagliate in relazione all'immagine importata, è possibile cliccare su «Image Details». Vengono riportate informazioni sulla versione del Sistema Operativo (Versione Name), nell'esempio, Windows XP, sul file system (nell'esempio, NTFS), il nome del volume (Volume Name) ed il relativo numero seriale (Volume Serial Number).
- Cliccando su «File Analysis», si accederà ad una nuova schermata che permetterà di effettuare diverse opzioni in merito ai file. Vengono mostrati tutti i file e le directory, contenuti nella Current Directory(C:\). Per ciascuno dei file/directory nella lista, vengono mostrate diverse caratteristiche:

Type	Name	Written	Accessed	Changed	Created	Size	UID	GID	META
<b>dir / in</b>									
Parsing File (Invalid Characters?):									
?: \$OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 0 0 0									
r / r	\$AttrDef	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2560	48	0	4-128-4
r / r	\$BadClus	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	0	0	0	8-128-2
r / r	\$BadClus:\$Bad	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	10289152	0	0	8-128-1
r / r	\$Bitmap	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2512	0	0	6-128-1
r / r	\$Boot	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	2004-06-10 05:22:22 (CEST)	8192	48	0	7-128-1
d / d	\$Extend/	2004-06-10	2004-06-10	2004-06-10	2004-06-10	344	0	0	11-144-4

- Con il tasto «Generate MD5 List of Files» è possibile generare i valori di hash MD5, per ciascun file/directory (utile per controlli sull'integrità). L'investigatore potrà aggiungere anche delle annotazioni sui file (ad esempio, anomalie, ecc.), con il tasto «Add Note».

Si aprirà anche un pannello a sinistra permette di svolgere quattro utili operazioni:

- Directory Seek: permette la ricerca di directory
- File Name Search: permette di effettuare ricerche di file (è anche possibile utilizzare espressioni regolari)
- Expand Directories: espande la visualizzazione di tutte le directory, per avere una vista più completa
- All Deleted Files Cerca, a l'interno dell'immagine, eventuali file eliminati. Cliccando su di essa verranno mostrati tutti i file eliminati (riportati in rosso), che Autopsy ha recuperato. Per ciascuno di tali file, sono riportate le informazioni relative alla data e ora dell'ultima scrittura/modifica/accesso e della creazione del file, la dimensione ed i relativi metadati. Cliccando sul nome di un file (riportato nella colonna Name), nel pannello File Browsing Mode, verrà mostrata un'anteprima del file selezionato. Cliccando su meta,c i verranno mostrati i metadati del file; sono riportate tutte le parti (ciascuna memorizzata all'interno di un cluster), che compongono il file C:/del2/file7.hmm. Cliccando su ciascuna parte del file verrà riportato il contenuto byte-per-byte (in ASCII).
- File type: L'utilizzo dei metadati è poco pratico quando, nell'immagine forense, sono presenti diverse tipologie di file da analizzare. È possibile utilizzare l'opzione «File Type» per ordinare, in base alla tipologia, le seguenti categorie di file: file presenti nell'immagine

(allocated), file cancellati (unallocated), file nascosti. Cliccando su file type avremo due opzioni.

- \* «Sort Files by Type», si aprirà una nuova schermata che chiederà come deve essere effettuato l'ordinamento dei file. Cliccando «Ok», verrà creata una lista dei file, ordinata per tipologia dei file stessi e ci verrà mostrata una sintesi del risultato. Nella sintesi del risultato viene riportato il numero di file, appartenenti a ciascuna tipologia. L'ordinamento per tipologia è stato eseguito, poiché, nella schermata precedente, è stata selezionata la voce, riportata nella figura in basso
- \* Cliccando su «View Sorted Files», appare il seguente messaggio informativo, in cui ci viene indicato il percorso per visionare la lista ordinata

### 6.1.3 Riapertura di un Caso

1. Per riaprire un caso, precedentemente creato, cliccare sul tasto «Open Case»
2. Selezionare il caso desiderato, fra quelli elencati nella colonna «Case Gallery»
3. Cliccare su «Ok» per riaprire il caso selezionato

## 6.2 Le Super Timeline

Un timestamp (letteralmente, marca temporale) registra il momento temporale, in cui un evento avviene. Le evidenze tipicamente dispongono di un timestamp. Alcuni Esempi:

- • Timestamp di un File: è possibile reperire, dal file system, la data e l'ora di creazione, la data e l'ora dell'ultima modifica, ecc.
- Timestamp di un Processo: nei live system, dal memory dump è possibile ottenere la data e l'ora di avvio/terminazione
- Ecc.

Esistono diversi formati di timestamp, provenienti dal file system, relativi ai file:

- Nei sistemi Windows-based, un timestamp è rappresentato con 64 bit, nel formato FILETIME. Le informazioni sul fuso orario (timezone) sono specificate nel registro di Windows, al percorso: HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation
- Nei sistemi Linux-based, un timestamp è memorizzato in formato Posix o Epoch (32 bit). Le informazioni sul fuso orario sono specificate in /etc/localtime

Nei sistemi Windows-based, per ciascun file, vengono memorizzati diversi timestamp, che riportano le cosiddette informazioni MACB:

Lettera	Descrizione
M	Data e ora dell'ultima modifica
A	Data e ora dell'ultimo accesso al file
C	Data e ora dell'ultima modifica ai metadati
B	Data e ora di creazione del file

In alcuni casi, vengono riportate esclusivamente le cosiddette informazioni MAC.

I timestamp sono generalmente memorizzati nei metadati di ciascun file. Nel file system NTFS, ad esempio, i timestamp sono memorizzati, per ciascun file, all'interno della Master File Table (MFT). Tutti i file e gli oggetti memorizzati dal file system, sono descritti all'interno della MFT. Ciascuna entry (detta anche record) della MFT, contiene la descrizione di un file ed il puntatore ai dati (ovvero, il contenuto del file). In caso di un file di piccole dimensioni, la entry conterrà direttamente il contenuto di tale file.

LA struttura di un record della MFT è la seguente:

Standard Information	Nome del File	Security Descriptor	Data
----------------------	---------------	---------------------	------

Utilizzando i timestamp è possibile realizzare una timeline. Grazie alla timeline, gli investigatori forensi possono analizzare l'andamento temporale degli eventi. Inoltre, è anche possibile individuare eventi temporali vicini ed effettuare, di conseguenza, delle ipotesi sulla loro eventuale correlazione. Esempio:

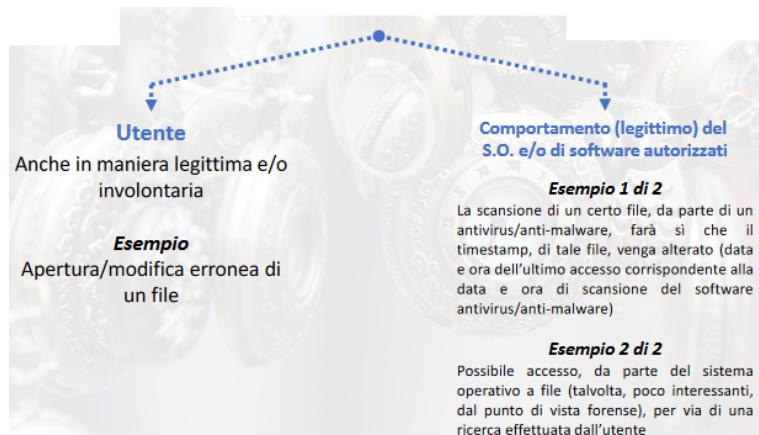
- Creazione di un file → Modifica di una presentazione
- Apertura di un programma → Creazione di un documento
- Modifica di una immagine → Modifica di un file di testo

Le timeline tradizionali sono essenzialmente basate sui timestamp, specificati dal file system:

Esempio di una semplice timeline, basata su timestamp del file system				
Timestamp	Operazione	Nome del File	Note	
03/03/2019 10:00	Ultimo Accesso	C:\DigFor.txt	Apertura di un file di testo	
03/03/2019 10:30	Creazione	C:\DF_TEST.doc	Creazione di un documento	
03/03/2019 10:45	Modifica del Contenuto	C:\DF_TEST.doc	Salvataggio del documento	

### 6.2.1 Problemi delle timeline tradizionali

Uno dei principali problemi della timeline, basata su timestamp del file system, è che, i timestamp, possono essere modificati moltissime volte da parte di:



Alcuni sistemi operativi, per ragioni legate principalmente alle performance, potrebbero NON effettuare sempre l'aggiornamento della data e dell'ora, relativa all'ultimo accesso di un file. In Windows,

mediante una modifica al registro di sistema, è possibile disabilitare completamente l'aggiornamento della data ed ora dell'ultimo accesso di un file. Anche in Linux è possibile specificare l'opzione noatime, del comando mount, che disabilita l'aggiornamento delle suddette informazioni (tale opzione è può anche essere resa permanente).

Inoltre, il fatto di basarsi esclusivamente sui timestamp del file system, non indica il contesto (o lo indica parzialmente), esempio: un file potrebbe essere ripetutamente acceduto dal sistema operativo (ad esempio, file di log d sistema/servizi/programmi), per svariate ragioni.

**NOTA:** è possibile notare come i timestamp, del file system, abbiano una natura potenzialmente poco attendibile. Ciò potrebbe portare gli investigatori a realizzare una timeline non corretta o parzialmente alterata.

### 6.2.2 Tecniche Anti-Forensi per l'alterazione dei Timestamp

Come qualsiasi dato digitale, il valore del timestamp (del file system) può essere alterato maliziosamente, tramite appositi tool. Ad esempio, tramite dei tool specifici, è possibile modificare il campo Standard Information di un record della MFT (File System NTFS). Esistono poi altre tecniche anti-forensi in grado di alterare i timestamp.

**NOTA:** A causa delle tecniche anti-forensi, è estremamente importante che gli investigatori abbiano accesso a informazioni da più punti, per validare/confutare il risultato ottenuto.

### 6.2.3 Possibili soluzioni

Una possibile soluzione, ai problemi identificati precedentemente, è quella di estendere la timeline, arricchendola con informazioni provenienti da più fonti, in tal modo, è possibile avere un quadro più chiaro e minimizzare anche l'eventuale impatto ottenuto dall'utilizzo di tecniche anti-forensi. Infatti, è estremamente più difficile, tramite tecniche anti-forensi, alterare tutte le informazioni, ottenute da diverse fonti.

La super timeline è una estensione della timeline, che prevede l'inclusione di diverse informazioni, provenienti da diverse fonti, fra cui: file di log (del sistema operativo, ecc.), metadati del file system, registro di sistema (sistemi Windows-based) e ecc.

### 6.2.4 Framework Plaso

Plaso (Plaso Langar Að Safna Öllu, dall'islandese, letteralmente, Plaso vuole raccogliere tutto) è un tool per la realizzazione di super timeline. È scritto in Python ed è Open-Source. Plaso supporta diversi formati in input:

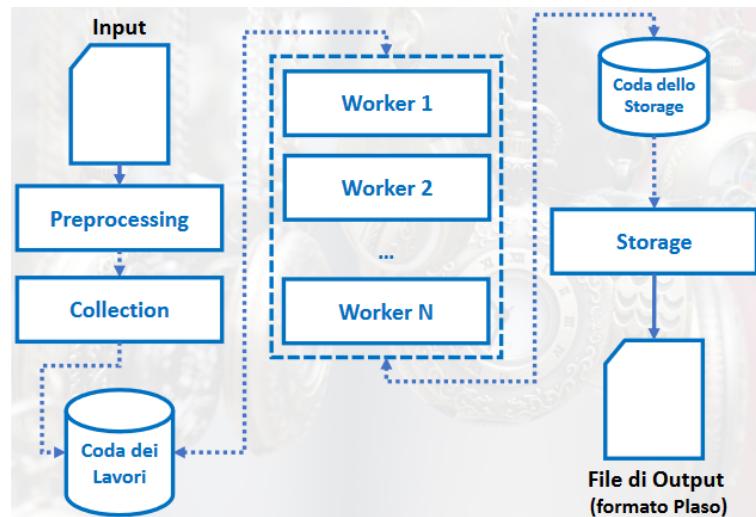
- Storage Media Image File Formats
- Volume System Format
- File System Format
- File Format : Apple System Log (ASL), Android usage-history (app usage), Basic Security Module (BSM), Bencode files, Chrome cache files, Chrome preferences file, CUPS IPP, ecc
- ecc.

Plaso presenta un'architettura, suddivisa in quattro componenti principali, indipendenti:

- Preprocessing: l'attività di preprocessing è svolta preliminarmente da Plaso e si occupa di reperire alcune informazioni, in relazione a quelle che saranno le fasi successive. Alcune delle informazioni reperite: versione del Sistema Operativo, informazioni sul fuso orario (timezone), eventuale nome della macchina (hostname), determinare le applicazioni di default (ad esempio, browser di default, ecc.) e determinare gli utenti e l'eventuale path associato ad essi.
- Collection: nell'attività di collection, invece, vengono individuati tutti i file, che dovranno essere elaborati, nelle fasi successive.
- Worker
- Storage

### Worker e Storage

I worker costituiscono l'elemento chiave di Plaso, infatti, elaborano ciascun file della lista degli input, individuata precedentemente (attività di collection). Nello specifico, un worker si occuperà di determinare, in primo luogo, la tipologia del file e, successivamente, svolgerà diverse attività. Alcune attività svolte dal Worker: determinare quale parser dovrà essere applicato al file, il parser è in grado di elaborare un determinato file, in base alla sua struttura. Elaborare il file, con il parser adeguato. Applicare alcuni filtri predefiniti al file. Inviare le informazioni estratte alla componente di storage. La componente di storage, si occupa della costruzione/memorizzazione del file di output, in accordo alle specifiche fornite. Determinare eventualmente se si sta elaborando un archivio, il quale potrebbe contenere, al suo interno, dei file che devono essere elaborati.



### 6.2.5 Tool di Plaso

Plaso mette a disposizione diversi tool, utilizzabili da linea di comando:

- log2timeline: è il front-end di Plaso e permette di interagire con il framework, estraendo i vari eventi e memorizzandoli in formato Plaso. I file nel formato Plaso, possono poi essere riutilizzati, ulteriormente elaborati ed analizzati. Sintassi semplificata: log2timeline [STORAGE\_FILE] [SOURCE]:
  - [STORAGE\_FILE]: Permette di specificare il percorso del file di output. **NOTA:** il file di output, verrà memorizzato in formato Plaso
  - [SOURCE]: Permette di specificare l'input da elaborare (l'input deve essere in uno dei formati supportati)

La sintassi completa è mostrata quando viene avviato il comando log2timeline, senza alcun argomento.

- pinfo: semplice tool che permette di estrarre e visualizzare informazioni contenute all'interno di un file, in formato Plaso
- pprof: serve soprattutto per gli sviluppatori, al fine di ottimizzare determinati parser
- preg: fornisce un front-end diverso dedicato alla gestione dei parser del registro di sistema dei sistemi Windows-based. Permette anche di ottenere informazioni sul registro, partendo da una sua sotto-chiave
- pshell: terminale (basato su Python) per l'interazione con il back-end di Plaso, permette l'analisi avanzata tramite l'accesso a tutte le librerie di Plaso
- psort: importante tool che effettua la conversione dal formato Plaso (non human-readable) a diversi formati, che possono essere visualizzati e post elaborati (eventualmente con tool esterni, come, ad esempio, Microsoft Excel, ecc.). Sintassi semplificata: psort [STORAGE\_FILE] -o FORMATO -w OUTPUT:
  - [STORAGE\_FILE]: Permette di specificare il percorso del file di input. **NOTA:** il file di input (N.B. Non di output, come per il comando log2timeline), deve necessariamente essere memorizzato in formato Plaso
  - -o: Con l'opzione -o, è possibile specificare il formato (FORMATO) di output. **NOTA:** psort supporta tantissimi formati di output, i quali sono visibili con il seguente comando: psort -o list.
  - -w: Con l'opzione -w, è possibile specificare il percorso del file di output (OUTPUT)

### 6.2.6 Esempio di utilizzo Super Timeline

#### Esempio di Utilizzo 1: Cronologia Browser Chrome

L'analisi della timeline della cronologia del browser, è molto importante dal punto di vista forense, per avere un quadro più chiaro sulle attività effettuate tramite il Web.

1. Il primo passo consiste nel fornire in input, il file, relativo alla cronologia di Google Chrome, di cui si intende analizzare la timeline, al fine di ottenere, in output, un file, in formato Plaso. Nei sistemi Windows-based, il file, relativo alla cronologia di Google Chrome, è denominato History ed il percorso tipico, ove esso risiede, è il seguente: *C : \Users\ < NomeUtente > \AppData \ Local \ Google \ Chrome \ UserData \ Default*.

log2timeline CronologiaChrome.plaso "E : \[...] \ History"

Plaso è in grado, automaticamente, mediante il preprocessing, di riconoscere il formato del file ed analizzarlo correttamente. Il comando log2timeline produce il file CronologiaChrome.plaso. Il comando pinfo, il quale mostra informazioni in merito ad un file, in formato Plaso: pinfo CronologiaChrome.plaso.

2. Tramite psort è possibile convertire il file in formato Plaso (non human-readable), in un formato human-readable, ad esempio, il formato XLSX, leggibile da Microsoft Excel (o altri software, come OpenOffice, ecc.):

```
psort CronologiaChrome.plaso -o XLSX -w CronologiaChrome.xlsx
```

Produce il file CronologiaChrome.xlsx.

3. Analisi del File Prodotto (CronologiaChrome.xlsx): Per ciascun evento, specificato sulle righe abbiamo:

- Datetime: la colonna datetime ne riporta il timestamp, esplicitando la data e l'ora, nel seguente formato: YYYY-MM-DD HH:mm:ss,lli (lli indicano i millisecondi)
- Message: la colonna message ne riporta una descrizione, esplicitando alcune informazioni utili
- Timestamp\_desc: indica la tipologia del timestamp
- Source: identificativo della rete
- Source\_long: descrizione, in formato human-readable, della fonte
- Parser: la colonna parser ne riporta il parser, utilizzato da Plaso
- Display\_name: la colonna display\_name è specificato, in questo caso, il percorso completo del file della cronologia: *E : \[...] \ History*

Avendo a disposizione gli URL dei vari siti visitati, estratti dalla cronologia, sarebbe possibile accedere direttamente a tali siti, per visionarne l'eventuale contenuto, senza effettuarne una analisi preventiva (o effettuandone una superficiale). È bene però considerare che gli URL potrebbero essere diretti a siti malevoli/illegali/ecc. Una richiesta, proveniente da una fonte sconosciuta (ovvero, la richiesta effettuata con il link diretto, effettuata dall'investigatore), potrebbe mettere «in allerta» gli «amministratori» dei suddetti siti (ed eventualmente alterare il corso di eventuali altre indagini, in atto, o ulteriori indagini su questi siti). Pertanto, un'accurata analisi è sicuramente preferibile ed è consigliabile accedere all'URL solo in caso vi sia sufficiente sicurezza e/o per valide motivazioni, ai fini dell'indagine che si sta svolgendo. Oppure, gli URL potrebbero innescare azioni (ad esempio, cancellazione di dati, attivare/disattivare oggetti, ecc.).

### 6.2.7 Esempio di Utilizzo 2: Timestamp file Office Open XML

L'analisi dei timestamp dei file Office (memorizzati generalmente nel formato Office Open XML) è particolarmente importante (a volte, tali file sono utilizzati come alibi, ecc.). Il formato Office Open XML (OOXML) è un formato di memorizzazione per documenti, fra cui:

- Presentazioni (estensione tipica dei file.pptx)
- File di testo formattati (estensione tipica dei file .docx)
- Fogli di calcolo (estensione tipica dei file .xlsx)

Due differenti set di specifiche:

1. Transitional: supporto della retrocompatibilità
2. Strict: definiscono concretamente lo standard

## 6. Analisi

---

Un file OOXML è essenzialmente un archivio compresso, in formato ZIP. Contiene diversi elementi e file XML. I file XML contengono principalmente metadati e specificano: la struttura del documento e altre caratteristiche/informazioni.

Dal momento che un file in formato OOXML è un archivio compresso, si può visionare la struttura interna:

- Il file *[Content\_Types].xml*, contiene informazioni sul contenuto del documento
- Il file *core.xml* (nella directory *docProps*), contiene alcuni metadati, i quali indicano informazioni di carattere generale, in merito al documento (titolo, creatore, data e ora di creazione, data e ora dell'ultima modifica, ecc.)
- Il file *.rels* (file XML), nella directory *\_rels*, contiene eventuali informazioni sulle relazioni di alcuni elementi strutturali del documento

Passi di utilizzo:

1. Analogamente all'esempio precedente, effettuiamo la memorizzazione del file di output, in formato Plaso, fornendo in input il percorso relativo al file *presentazione.pptx*

```
log2timeline EsempioOOXML.plaso E:\DigitalForensics.pptx
```

2. Mediante il tool *psort*, il file in formato Plaso (output del tool *log2timeline*) verrà convertito in formato XLSX

```
psort EsempioOOXML.plaso -o xlsx -w EsempioOOXML.xlsx
```

3. Analisi del File Prodotto (EsempioOOXML.xlsx):

- Datetime
- Message
- Timestamp\_desc
- Source
- Source\_long
- Parser
- Display\_name

In generale, una incoerenza tra i timestamp di due o più fonti diverse, dovrebbe far sorgere diversi interrogativi/ipotesi all'investigatore. È possibile che si tratti di un tentativo di alterare l'indagine forense (strategia anti-forense)? In caso affermativo:

- Il soggetto era in possesso di adeguate competenze?
- È stato aiutato da un'altra persona?
- Per quale motivazione è stata tenuta questa condotta?
- Quale/i informazioni sono state alterate?
- Il file potrebbe contenere dati nascosti, ad esempio, mediante tecniche di steganografia?

Il file potrebbe essere la copia di un altro file?

- In caso affermativo: l'originale è più aggiornato? L'originale è stato eliminato? Eventualmente, per quale motivo? Potrebbe essersi trattato di un errore? L'originale potrebbe contenere dati che volevano essere tenuti nascosti? È possibile che esistano altre copie, con contenuti (rilevanti) leggermente diversi?
- In caso negativo: l'autore del file è il soggetto su cui si indaga? Può averlo creato su un altro dispositivo e poi copiato su quello in analisi?

### 6.2.8 Esempio di Utilizzo 3 File System + Cronologia Browser Chrome

In questo esempio, verrà realizzata una super timeline, in cui saranno considerate due fonti:

1. Metadati dell'intero file system NTFS, di un dead system. Tali metadati sono reperiti da una immagine forense (denominata Win10.dd), acquisita dal disco fisso (circa 20GB), di un dead system simulato (ospitato su una macchina virtuale), equipaggiato con il sistema operativo Microsoft Windows 10
2. Cronologia del browser Google Chrome, estrapolata dal relativo file (memorizzato nel suddetto dead system). Il file relativo alla cronologia è stato acceduto dal drive «virtuale» (contrassegnato dalla lettera E:), sul quale è stato effettuato il mounting, in modalità «sola lettura», della suddetta immagine forense

Per la realizzazione di questa super timeline, verrà utilizzato il tool fls della suite The Sleuth Kit (TSK).

#### Istruzioni per creare una supertimeline

a) fls -z Europe/Rome -f ntfs -r -m C: Win10.dd > InfoFileSystem.body: Il tool fls elenca tutti i file e le directory, presenti all'interno di un file system, esplicitando, per ciascuno di essi, diverse informazioni. Nell'esempio, fls è stato utilizzato per i timestamp (in formato MACB) di tutti i file/directory. I parametri forniti sono i seguenti:

- -z Europe/Rome: Specifica il fuso orario (timezone): Europa/Roma
- -f: Specifica il tipo di file system: NTFS
- -r: Specifica che il contenuto delle directory deve essere considerato ricorsivamente (es., contenuto di directory all'interno di altre directory, e così via)
- C: Specifica che i file devono essere considerati a partire dalla cartella C:
- Win10.dd: L'immagine da cui ottenere le informazioni sui file
- InfoFileSystem.body: Il file in cui verrà memorizzato l'output (nel formato denominato body (specificato dall'opzione -m)

b) log2timeline esempio3.plaso "E : \[...] \ History"

c) log2timeline esempio3.plaso InfoFileSystem.body Le due esecuzioni del tool log2timeline, del framework Plaso, fanno riferimento al medesimo file di output (esempio3.plaso), al quale vengono aggiunte informazioni provenienti dal file, relativo alla cronologia di Chrome (istruzione b)), informazioni provenienti dal file system (istruzione c)). Si ricorda che tali informazioni sono state ottenute, tramite il tool fls, dall'istruzione a)

d) psort -z Europe/Rome -o XLSX -w FileCronologia.xlsx esempio3.plaso. Viene infine eseguito il tool psort, al fine di convertire il file esempio3.plaso (in formato Plaso), in formato XLSX (opzione -o XLSX). Anche in questo caso è utilizzato il fuso orario Europa/Roma (opzione -z) Europe/Rome

3. Analisi (parziale) Versione Preprocessata del File Prodotto. Il file prodotto è costituito da oltre un milione di entry. Sono stati infatti estrapolati 1.039.826 di eventi. Il suddetto file è stato preliminarmente preprocessato ed esemplificato, in modo da renderlo più fruibile, ed è strutturato come segue: In nero e grassetto sono riportati, esclusivamente, i file (ed i relativi timestamp), potenzialmente rilevanti, per la definizione di un possibile scenario investigativo [informazioni estrapolate dalla Fonte 1.]. In ciano e grassetto sono riportate alcune informazioni, in maniera sintetica, in merito ad alcuni eventi [Fonte 1.]. In rosso scuro e grassetto sono riportati gli URL visitati (ed i relativi timestamp), estrapolati dalla Fonte 2. Il file preprocessato è organizzato in una tabella, costituita dalle seguenti tre colonne:

- Ora: riporta l'ora in cui si è verificato l'evento (gli eventi di interesse, si sono verificati tutti nella stessa data)
- Descrizione: riporta una breve descrizione testuale dell'evento (ad esempio, visita di un URL)
- Path oppure URL: specifica il path nel file system o l'URL, coinvolto nell'evento

Da questa fase si può analizzare se le tracce di timeline siano coerenti tra di loro.

### La cartella Prefetch introduzione

Nel nostro esempio si nota che c'è la creazione di un file all'interno di una cartella denominata prefetch. La cartella *C : \Windows \Prefetch* fa riferimento ad una cartella speciale di Windows, denominata appunto Prefetch. Questa cartella viene utilizzata da Windows per incrementare le performance di sistema, effettuando un pre-caricamento di alcune «parti» di codice delle applicazioni usate più comunemente. Dal punto di vista forense, la cartella Prefetch è molto utile, al fine di individuare quali applicativi sono stati utilizzati nel sistema. Esempio: nel nostro caso viene creato un file dal nome MSPAINT.EXE-76E10B24.pf, all'interno della cartella *C : \Windows \Prefetch*.

Ogni «parte» di applicazione/processo viene mappata in un file, il cui nome ha il seguente formato:  
<NOMEFILE\_ESEGUITIBILE>-<VALORE\_HASH>.pf

### C:/\$Recycle.Bin

La cartella C:/\$Recycle.Bin è la cartella che Windows utilizza per il Cestino. Se al suo interno viene creato un nuovo file vuol dire che l'utente abbia spostato nel Cestino un file (per «eliminarlo»), pertanto, potrebbe essere utile approfondire di cosa si tratti e soprattutto delineare delle possibili ipotesi/motivazioni. Quando un file viene «eliminato» (spostato nel Cestino), il S.O., lo rinomina, senza alterarne l'estensione, e lo sposta nella cartella \$Recycle.Bin, quindi, anche dal «nuovo nome del file», è possibile individuare l'estensione del file «eliminato» [nell'esempio, l'estensione è: .png , si tratta verosimilmente di una immagine, in formato PNG. Esempio: *C : \\$Recycle.Bin \ S - 1 - 5 - 21 - 3031900839 - 921391284 - 2575565698 - 1001 \ \$R33G7OQ.png*. NOTA:S.... è il secure IDentifier (SID) dell'utente. Il SID è un identificativo univoco associato a ciascun utente all'interno del sistema.

### Possibile scenario

Dalle osservazioni e le informazioni precedenti, potrebbe essere possibile delineare uno scenario verosimile degli eventi, sufficientemente accurato, in riferimento alla (piccola) porzione della super timeline analizzata:

1. Navigazione Web sulla pagina Eventi del Dipartimento di Informatica (DI) dell'Università di Salerno
2. Visita alla pagina dedicata di un evento archiviato (già svoltosi)
3. Avvio del programma Microsoft Paint
4. Visualizzazione/Creazione di una immagine (probabilmente tramite Paint)
5. Cancellazione di una immagine PNG (probabilmente l'immagine di cui sopra)
6. Creazione (verosimilmente automatica) di un collegamento rapido (.lnk) ad un file il cui nome è DigitalForensics (non è nota l'estensione del file al quale il collegamento fa riferimento)
7. La navigazione Web prosegue con la visita ad altri URL, relativi ad altre pagine del suddetto Dipartimento

## Timeline con Autopsy [Versione Windows]

La versione per Microsoft Windows, del tool Autopsy, fornisce diverse opzioni per la gestione della super timeline e una GUI molto ben realizzata ed user-friendly.

### Visualizzazione mediante Timeline Explore

Timeline Explorer è un software, sviluppato da Eric Zimmerman, che permette la visualizzazione di timeline/super timeline. Le timeline di input devono essere in formato XLS o in formato CSV (Comma-Separated Values). Possono essere ottenute come output da vari tool (The Sleuth Kit, Volatility, Plaso, ecc.). Visualizza le righe con colori diversi, in base alla tipologia di evento.

## 6.3 Mounting di Immagini Forensi

### 6.3.1 Linux

#### Mounting con formato EWF

1. In primo luogo, è necessario creare una cartella, mediante mkdir, in cui verrà effettuato il mounting dell'immagine forense.

```
# mkdir /mnt/puntodimount
```

2. Utilizzare il comando ewfmount, nel modo seguente: ewfmount <nome\_immagine\_EWF> <cartella>
3. Posizionandosi nella cartella /mnt/puntodimount (utilizzata con il comando precedente), sarà possibile individuare il file ewf1
4. È possibile utilizzare il comando mmfs (della suite The Sleuth Kit – TSL), sul file ewf1, per individuare le informazioni sulle partizioni, ecc. (le informazioni sono estratte dal MBR).
5. Supponiamo di voler effettuare il mounting della Partizione 1. Creiamo prima una cartella, in cui andare ad effettuare il mounting della Partizione 1, denotata /mnt/partizione1. Utilizziamo poi il comando mount, di Linux, nel modo seguente:

```
# mount -o ro,loop,show_sys_files,streams_interface=windows,offset=1048576 -t ntfs ewf1 /mt/partizione1/
```

Con -o si specificano delle opzioni per il mounting. L'opzione ro, si riferisce al mounting, in modalità sola lettura (read-only). Il valore del campo offset (ovvero, 1048576), esprime un numero di byte, ed è calcolato nel modo seguente:  $2048 \times 512 = 1048576$ , dove 2048 è il settore di inizio della Partizione 1 e 512 è la dimensione, in termini di byte, di un settore. Con -t ntfs si fa invece riferimento al fatto che si sta effettuando il mounting di un file system NTFS.

6. Spostandosi nella cartella /mnt/partizione1, sarà possibile visionare il contenuto della Partizione 1, di cui si è effettuato il mounting
7. Se vogliamo caricare una nuova partizione per prima cosa si deve fare l'unmounting della partizione1 nel nostro caso: rm -r /mnt/partizione1/, si procede come prima.

#### Mounting con formato RAW

1. Utilizzando il comando mmfs (della suite The Sleuth Kit – TSL), si ottengono informazioni sul file 10-ntfs-disk.dd, per individuare le informazioni sulle partizioni, ecc. (le informazioni sono estratte dal MBR). Si procede poi come nel caso di ewf.

### 6.3.2 Windows

Il tool OSFMount permette di effettuare il mounting (anche in sola lettura) di immagini forensi, in sistemi Windows-based. Il mounting verrà effettuato su un disco «virtuale», al quale può essere associato un riferimento logico (costituito una lettera mnemonica, non in uso dal sistema). Esempi: E:, F:. Sviluppato da PassMark, è gratuitamente scaricabile ed è appositamente progettato per lavorare con la suite PassMark OSForensics<sup>tm</sup>. Ma può essere utilizzato anche come utility stand-alone.

# Capitolo 7

## Importanza degli Artefatti di Windows

Un sistema operativo è un software particolarmente complesso ed articolato. Se adeguatamente supportato, è in continua evoluzione con miglioramenti sulla sicurezza, aggiunta di nuove funzionalità, ecc.. Durante l'esecuzione di un S.O., vengono utilizzate diverse strutture. Alcune sono direttamente accessibili (o parzialmente accessibili) dall'utente. Altre strutture sono accessibili ed utilizzabili esclusivamente al S.O. All'interno di tali strutture, possono esservi diversi artefatti (file, stringhe di testo, ecc.), i quali vengono memorizzati dal S.O., per diversi obiettivi. Migliorare l'esperienza dell'utente e/o agevolare alcune azioni dell'utente. Migliorare le performance di sistema. Ricordare alcune azioni dell'utente, per fornire adeguati suggerimenti, in futuro, ottimizzando l'operatività dell'utente stesso.

### 7.1 Alcune fonti di artefatti

#### 7.1.1 Fase di Boot di Windows

La fase di boot di un computer è una fase potenzialmente rilevante, per l'investigazione forense. Possibilità di identificare i file modificati durante il processo di boot, per cui, anche in caso di eventuali avvii accidentali, è possibile determinare quali siano i file alterati dal S.O. Possibilità di esaminare i processi di avvio, al fine di individuare eventuali software malevoli.

Principali fasi di boot:

- BIOS (Basic Input-Output System): Permette l'intermediazione tra l'hardware e il S.O. Contiene una sequenza di istruzioni che è indispensabile per l'avvio del S.O. e per far sì che il S.O. possa controllare correttamente l'hardware. Le istruzioni sono generalmente memorizzate all'interno di una memoria ROM (Read-Only Memory)/PROM (Programmable ROM). A partire dal 2017, il BIOS è stato sostituito con l'UEFI (Unified Extensible Firmware Interface). L'UEFI estende le funzionalità del BIOS e fornisce una GUI più avanzata, rispetto a quella fornita dal BIOS, per la configurazione del sistema.

Durante questa fase di inizializzazione: vengono eseguite le seguenti operazioni:

Identificazione dei dispositivi hardware

Inizializzazione dei suddetti dispositivi

Power-On Self Test (POST): Fase di testing automatico, che permette di verificare il corretto funzionamento delle componenti e delle periferiche hardware. Caricamento del codice del BIOS. Test dell'integrità del suddetto codice. Individuazione della causa che ha portato all'avvio del processo di POST (accensione, ripresa dallo stand-by, ecc.). Individuazione della RAM. Determinazione delle dimensioni. Fase di verifica. Individuazione dei dispositivi di sistema e dei bus. Fase di catalogazione ed inizializzazione. Eventuale avvio del BIOS della scheda video. Lettura delle impostazioni relative alla configurazione di avvio.

Il CMOS (Complementary Metal-Oxide Semiconductor) è un semiconduttore che svolge la funzione di una piccolissima RAM e contiene le impostazioni del BIOS. Assorbe poca energia elettrica e deve necessariamente essere alimentato da una batteria (se la batteria si scarica, le impostazioni del BIOS, vengono tipicamente resettate a quelle di fabbrica)

Identificazione del dispositivo di avvio e lettura del Master Boot Record (MBR)

Avvio del Boot Manager, denominato Windows Boot Manager nel S.O. Windows (Bootmgr.exe)

Il Windows Boot Manager ha il compito di individuare il loader di Windows (Winload.exe), nella partizione di boot di Windows

Inizia poi la fase successiva: Loader del S.O. (OS Loader)

- Loader del S.O.: L'eseguibile Windows Loader (Winload.exe) effettua le seguenti operazioni:  
Avvia i driver essenziali e minimali per la lettura di dati dal disco fisso (o dal supporto di memorizzazione prescelto). Inizializza il sistema ad un punto in cui il Kernel di Windows può iniziare la sua esecuzione. Al momento dell'avvio del Kernel, vengono caricati in memoria, i seguenti elementi: Registro di sistema, alcuni Driver. Vengono caricati in memoria tutti i driver, che sono necessari nelle fasi successive. Tali driver sono contrassegnati come BOOT\_START.
- Inizializzazione del S.O.: Nella fase di inizializzazione del S.O., viene eseguita la maggior parte delle operazioni di avvio. Questa fase può essere suddivisa in quattro sotto-fasi principali:

Inizializzazione del Kernel: In questa fase vengono inizializzate tutte le strutture dati e le componenti del Kernel. Viene poi inizializzato il Plug and Play (PnP) manager, il quale inizializza i driver, contrassegnati come BOOT\_START (tali driver sono stati precedentemente caricati in memoria)

Inizializzazione della Sessione: Il controllo passa al gestore di sessione: processo smss.exe, smss.exe provvede a: inizializzare il registro (caricato in memoria, precedentemente), inizializzare i dispositivi ed i driver (non contrassegnati come BOOT\_START). Avvia alcuni processi relativi a sottosistemi del S.O.

Inizializzazione di accesso a Windows (Winlogon): Il controllo passa al gestore del logon (Winlogon.exe). Appare la schermata di logon (autenticazione), vengono avviati determinati servizi, vengono avviati eventuali script per la gestione di privilegi (Group Policy), ecc.

Inizializzazione dell'Interfaccia Grafica (Explorer): Viene avviato il Desktop Window Manager (DWM), il quale provvede all'avvio dell'ambiente desktop, visualizzandolo per la prima volta (nella fase di boot)

Loader del S.O. e inizializzazione del S.O fanno parte del codice windows.

- PostBoot: La fase di PostBoot include lo svolgimento di diverse attività in background, che devono essere avviate, sebbene il desktop risulti visualizzato ed utilizzabile, ad esempio: avvio di servizi, avvio di programmi in background (ad es., DropBox, OneDrive, ecc.), aggiunta di tray icon (icone nell'area vicino l'orologio di Windows), ecc.

### 7.1.2 Analisi del Registro di Sistema

Il registro di sistema è una componente di Windows, che memorizza molteplici informazioni, alle quali il S.O. fa continuamente riferimento, durante l'utilizzo. Ad esempio, vengono memorizzati:

- Settaggi e preferenze di Windows stesso e di eventuali applicazioni installate
- Settaggi e preferenze degli utenti
- Settaggi e preferenze dell'hardware del sistema

Inoltre, il registro di sistema, tiene traccia di alcune attività degli utenti. Dal punto di vista forense, il registro di sistema è potenzialmente una enorme risorsa. In esso, infatti, sono contenuti migliaia di valori. Windows fornisce il tool Editor del Registro di sistema, il quale permette di visualizzare e modificare il registro di sistema. Utilizzabile soltanto in un live system. Il registro ha una specifica struttura gerarchica. Presenta cinque chiavi radice (root keys). All'interno di ogni chiave radice, sono presenti delle sotto-chiavi (sub-keys). Ciascuna sotto-chiave, può contenere, a sua volta, altre sotto-chiavi e/o valori (values). Ogni valore è costituito da tre elementi: Nome del valore (Prima Colonna), Dati contenuti nel valore (Terza Colonna), Tipo dei dati, contenuti nel valore (Seconda Colonna), es: Stringhe (REG\_SZ, REG\_EXPAND\_SZ, ...), numeri (REG\_DWORD, ...), dati binari (REG\_BINARY), ecc..

## HKEY\_CLASSES\_ROOT

La chiave radice HKEY\_CLASSES\_ROOT (talvolta, chiamata anche HKCR, per brevità), definisce il comportamento di Windows, in risposta ad alcune azioni eseguite dall'utente, tramite Esplora Risorse. Esplora Risorse è una componente della UI di Windows, che permette di «navigare» nel file system, svolgere operazioni sui file (ad esempio, rinominare un file), ecc.

Esempio di Azioni dell'Utente:

1. Click su determinati tasti di Esplora Risorse, i quali si attivano, alla selezione di un file
2. Click su determinate entry del menu contestuale, associato ad un file (tale menu si apre mediante un click, con il tasto destro del mouse, su un file, tramite Esplora Risorse)
3. Doppio click su un file, tramite Esplora Risorse

All'interno di HKEY\_CLASSES\_ROOT, è possibile individuare una sotto-chiave, per ognuna delle estensioni, note al sistema. Ciascuna di tali sotto-chiavi ha il medesimo nome dell'estensione a cui fa riferimento. Esempio: La sotto-chiave .png definisce il comportamento di Windows, in risposta alle azioni dell'utente, effettuate su file con estensione .png (tramite Esplora Risorse).

Esempio: In un live system, si intende individuare quale programma è utilizzato da Windows, in risposta all'azione di apertura di file con estensione .docx (eseguita dall'utente, tramite Esplora Risorse):

1. In primo luogo, individuare la sotto-chiave .docx, all'interno della chiave radice HKEY\_CLASSES\_ROOT.
2. Selezionare la sotto-chiave .docx (cliccando su di essa), per visualizzarne i valori
3. Considerare il contenuto (elemento Dati) del valore denominato (Predefinito), che è uguale a: Word.Document.12
4. Individuare la sotto-chiave denominata Word.Document.12, contenuta sempre nella chiave-radice HKEY\_CLASSES\_ROOT. Espandere la suddetta sotto-chiave, fino al seguente percorso di registro: [...] \Word.Document.12\shell\Open\command. NOTA: shell fa riferimento all'interfaccia grafica di Windows ed Open all'azione di apertura del file.
5. Nel contenuto (elemento Dati) del valore (Predefinito), è specificato, in questo caso, il percorso (nel file system) relativo all'eseguibile del programma, utilizzato da Windows, per l'apertura dei file con estensione .docx: *C :\ProgramFiles(x86)\MicrosoftOffice\Root\Office16\WINWORD.EXE*

## HKEY\_LOCAL\_MACHINE

La chiave radice HKEY\_LOCAL\_MACHINE (o HKLM) contiene informazioni sulla configurazione della macchina. Tale chiave radice è indipendente dall'utente autenticato.

La chiave radice HKEY\_LOCAL\_MACHINE contiene cinque sotto-chiavi:

- System: contiene settaggi, preferenze ed informazioni del sistema, come, ad esempio, il nome della macchina, il fuso orario, le interfacce di rete, i dispositivi di memorizzazione collegati al sistema, ecc.
- Software: contiene settaggi e preferenze, relative ad applicazioni installate ed a servizi installati, nel sistema
- SAM: Acronimo di Security Account Manager (SAM). Contiene informazioni di sicurezza, in merito agli utenti ed a eventuali gruppi di utenti. Contiene tutte le informazioni relative ad i permessi degli utenti, forniti dall'amministratore. Contiene il nome utente (username), il SID (acronimo di Secure ID: si tratta di un identificativo univoco associato a ciascun utente) e le relative password (crittografate) degli utenti. Per ragioni di sicurezza, Windows non permette l'accesso a questa sotto-chiave (essa appare vuota), sul sistema in uso. Può essere però estratta, dalla macchina in uso, ed analizzata su un'altra macchina.
- Security: contiene eventuali policy di sicurezza. Analogamente alla sotto-chiave SAM, anche questa chiave non può essere direttamente acceduta, sul sistema in uso.
- Hardware: Informazioni, settaggi ed impostazioni dei dispositivi collegati al sistema. Tali informazioni sono memorizzate in fase di boot.

Esempio: In un live system, si intende conoscere la tipologia del dispositivo di memorizzazione (ad esempio, penna USB, disco fisso, ecc.), collegato al sistema, al quale è stata associata la lettera E:

1. Al percorso *HKEY\_LOCAL\_MACHINE\SYSTEM\MountedDevices*, è possibile individuare tutti i dispositivi di memorizzazione, che sono collegati al sistema o che sono stati collegati, precedentemente
2. Viene mostrato la lista dei dispositivi di memorizzazione. Ciascuna lettera è un riferimento logico ad un dispositivo o ad una unità di memorizzazione, collegata al sistema (o che è stata collegata, precedentemente)
3. Effettuando un doppio click, sul valore evidenziato (riferito al dispositivo di memorizzazione, associato alla lettera E:), verrà aperta nuova schermata, la quale permetterà la visualizzazione e/o la modifica del contenuto (elemento Dati). **NOTA:** Trattandosi di dati binari (elemento Tipo uguale a REG\_BINARY), verranno mostrate due rappresentazioni (esadecimale e testuale).
4. Dalla rappresentazione testuale, è possibile individuare la stringa «USB STOR Disk», la quale indica che la tipologia del dispositivo è una penna (o un dispositivo similare), collegato ad una porta USB del sistema. Inoltre, è possibile individuare le stringhe «Jet Flash» e «Transcend», le quali si riferiscono rispettivamente al modello del dispositivo USB ed alla marca

## HKEY\_CURRENT\_USER

In Windows, a ciascun utente è associato un profilo. Un profilo specifica la configurazione e le preferenze, per Windows stesso e per eventuali altri software, relative ad un determinato utente. Ad esempio, lo sfondo del desktop, i colori degli elementi dell'interfaccia grafica, la dimensione delle finestre, le impostazioni del mouse, ecc. Inoltre, a ciascun profilo è associata una cartella di profilo, in cui l'utente può memorizzare i suoi file (ad esempio, documenti, immagini, video, download, ecc.) Il percorso di tale cartella è tipicamente il seguente: *C :\Users\ <NomeUtente>*. Quando un utente

effettua l'autenticazione con successo, Windows ne caricherà il relativo profilo. In tal modo, l'utente autenticato potrà fruire del suo ambiente operativo (Windows ed eventuali altri software), in accordo alla sua configurazione e preferenze, e potrà fruire dei suoi file.

La configurazione e le preferenze, relative al profilo dell'utente autenticato, sono memorizzate nella chiave radice HKEY\_CURRENT\_USER (o HKCU). In tale chiave radice, inoltre, potrebbero essere presenti anche tracce di attività dell'utente autenticato.

## HKEY\_USERS

La chiave radice HKEY\_USERS (o HKU) memorizza le configurazioni e le preferenze, relative ai profili degli utenti autenticati, nel sistema. In questo esempio, sono presenti cinque sotto-chiavi, relative ai



profili degli utenti autenticati, nel sistema:

- Quattro fanno riferimento ad utenti «speciali» di Windows. Tali utenti sono gestiti/utilizzati dal S.O. e servono per eseguire servizi o altre attività di sistema.
- Una fa riferimento all'utente (autenticato) [NOTA: è riportato il relativo SID]. Tutti gli utenti (non «speciali»), hanno un SID che inizia per S-1-5-21. Tramite ciò è stato possibile dedurre che la sotto-chiave, evidenziata in verde, facesse riferimento ad un utente (non «speciale»).
- La sotto-chiave .DEFAULT memorizza la configurazione e le preferenze, in riferimento al profilo di un utente «speciale», denominato utente di Default. Quando viene creato un nuovo utente, esso non avrà alcun profilo, pertanto, Windows ne creerà uno nuovo, che sarà una copia del profilo dell'utente di Default (includendo la configurazione e le preferenze). In tal modo, potrà essere fornito un ambiente operativo di base, al nuovo utente, il quale potrà essere personalizzato, successivamente. **NOTA:** La copia del profilo, discussa sopra, verrà eseguita solo quando il nuovo utente effettuerà la prima autenticazione.
- La sotto-chiave S-1-5-18, fa riferimento al profilo dell'utente «speciale» di Windows, denominato Sistema (System)
- La sotto-chiave S-1-5-19, fa riferimento al profilo dell'utente «speciale» di Windows, denominato Servizio Locale (LocalService)
- La sotto-chiave S-1-5-20, fa riferimento al profilo dell'utente «speciale» di Windows, denominato Servizio di Rete (NetworkService)
- La chiave che inizia con SID S-1-5-21 (*HKEY\_USERS\<SIDUtenteAutenticato>*) memorizza quindi la configurazione e le preferenze, relative al profilo dell'utente autenticato. Contiene le stesse informazioni della chiave radice HKEY\_CURRENT\_USER, discussa precedentemente.

## HKEY\_CURRENT\_CONFIG

HKEY\_CURRENT\_CONFIG (o HCC) è un alias che fa riferimento alla chiave radice HKEY\_LOCAL\_MACHINE (HKLM). Memorizza informazioni riguardanti il profilo hardware, utilizzato dalla macchina, all'avvio del sistema.

## 7.2 Analisi del Registro di Sistema

Nella seguente tabella, sono riportate alcune corrispondenze tra chiavi radici ed i percorsi degli hive file, nel file system. Queste informazioni sono rilevanti, poiché da una immagine forense (acquisita da

<b>HKEY_CURRENT_USER</b>	
È memorizzato nell'hive file <b>NTUSER.DAT</b> , il quale è localizzato all'interno della cartella di profilo, dell'utente autenticato (posizione tipica: <b>C:\Users\&lt;NomeUtente&gt;</b> )	
<b>HKEY_LOCAL_MACHINE</b>	
<b>System</b>	<b>C:\Windows\System32\config\System</b>
<b>SAM</b>	<b>C:\Windows\System32\config\SAM</b>
<b>Security</b>	<b>C:\Windows\System32\config\Security</b>
<b>Software</b>	<b>C:\Windows\System32\config\Software</b>

un dead system o da un live system) è possibile accedere ai vari hive file, al fine di effettuare l'analisi forense del registro.

### 7.2.1 Tool RegRipper

Per l'analisi degli hive file di registro, è possibile utilizzare il tool RegRipper. Oltre l'eseguibile, è necessario scaricare anche i plugin di RegRipper. I plugin vanno memorizzati tutti nella cartella plugin. La sua interfaccia grafica contiene: Percorso dell'hive file, relativo al segmento di registro, che si intende analizzare, percorso del report, che genererà RegRipper, in output, al termine della fase di elaborazione, selezione del profilo adeguato per il parsing dell'hive file, da analizzare, log della fase di elaborazione. All'interno del file generato da RegRipper si possono trovare diverse informazioni utili.

#### comdlg32

Le informazioni, potenzialmente utili, sono state individuate all'interno di una sezione del report, relativa ad una libreria di Windows, denominata Common Dialog Box library (comdlg32). Tale libreria contiene un insieme di finestre di dialogo, prefabbricate e pronte all'uso, utilizzabili dalle applicazioni, mediante le API, fornite dalla libreria stessa. La libreria comdlg32 memorizza, nel registro, alcune tracce delle azioni, eseguite dall'utente, ai fini di agevolare eventuali azioni analoghe, che, presumibilmente, saranno rieseguite in futuro, dall'utente stesso. È verosimile supporre che Microsoft Paint abbia invocato le API, della libreria comdlg32, in seguito ad azioni effettuate dell'utente (ciò ha fatto sì che siano state salvate delle tracce, all'interno del registro) Ad esempio, l'utente ha richiesto di aprire o salvare un file, di conseguenza, Paint ha mostrato la relativa finestra di dialogo (Open o Save As) e, tramite essa, l'utente ha selezionato il file. Il report di RegRipper è suddiviso in varie sezioni, pertanto, prima di proseguire con l'analisi, ci soffermeremo sull'organizzazione strutturale di una sua sezione.

```

comdlg32 v.20180702

Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32
LastWrite Time Sat Feb  9 18:39:15 2019 (UTC)
CIDSzMRU
LastWrite: Sat Feb  9 18:39:15 2019
Note: All value names are listed in MRUListEx order.

mspaint.exe

```

[...]

LastWrite Time è un timestamp e specifica la data e l'ora, in cui è avvenuta l'ultima modifica di ComDlg32. Sotto-chiave CIDSzMRU (contenuta nella sotto-chiave principale, ComDlg32) utilizzata dalla libreria Common Dialog Box, per la memorizzazione di specifiche informazioni, potenzialmente utili. Mspaint.exe contenuto del/i valore/i presente/i all'interno della sotto-chiave CIDSzMRU.

```

LastVisitedPidlMRU
LastWrite: Sat Feb  9 18:39:15 2019
Note: All value names are listed in MRUListEx order.

```

**mspaint.exe - My Computer\CLSID/Desktop**

In merito alla sotto-chiave LastVisitedPidlMRU, RegRipper ne riporta il contenuto, mediante un elenco, in cui ogni item ha il seguente formato:  $p_i - c_i$ .  $p_i$  è un programma che ha mostrato, recentemente, all'utente, una finestra di dialogo Open o Save As. L'ultimo file che l'utente ha selezionato (tramite una finestra di dialogo, mostrata dal programma  $p_i$ ), è localizzato nella cartella  $c_i$ . In questo caso, è presente un unico item e specifica che Microsoft Paint (mspaint.exe) ha mostrato, all'utente, una finestra di dialogo Open o Save As. Inoltre, l'ultimo file, che l'utente ha selezionato (tramite una finestra di dialogo, mostrata da Paint), è localizzato nella cartella del Desktop.

**mspaint.exe - My Computer \ CLSID/Desktop**: L'obiettivo di LastVisitedPidlMRU è di agevolare le azioni dell'utente: quando l'utente vorrà nuovamente aprire/salvare un file, un dato programma mostrerà la finestra di dialogo Open o Save As, in cui sarà pre-selezionata, automaticamente (proprio per agevolare l'azione dell'utente), la cartella, in cui è localizzato l'ultimo file selezionato dall'utente, in precedenza.

Grazie alle tracce della libreria Common Dialog Box, è possibile identificare l'utilizzo di Microsoft Paint, alle ore 18:39:15 (09/02/2019).

### OpenSavePidlMRU

La sottochiave OpenSavePidlMRU memorizza i percorsi dei file selezionati, mediante una finestra di dialogo Open oppure Save As, della libreria comdlg32. Grazie a questa sotto-chiave, una finestra di dialogo Open/Save As, sarà in grado di fornire le seguenti funzionalità, all'utente:

1. Mostrare la lista dei file recenti ovvero, i file che sono stati aperti/salvati recentemente dall'utente.
2. Funzionalità di auto-completamento dell'input: l'utente inizia a scrivere, nell'apposita area, il nome di un file, utilizzato di recente, e gli vengono forniti suggerimenti, in base al suo input, per completare automaticamente il nome del file, che sta scrivendo

## 7. Importanza degli Artefatti di Windows

---

```
UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time Sat Feb 9 10:35:18 2019 (UTC)

{9E04CAB2-CC14-11DF-BB8C-A2F1DED72085}

{A3D53349-6E61-4557-8FC7-0028EDCEEBF6}

{B267E3AD-A825-4A09-82B9-EEC22AA3B847}

{BCB48336-4DDD-48FF-BB0B-D3190DACB3E2}

{CAA59E3C-4792-41A5-9909-6A6A8D32490E}

{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
Sat Feb 9 18:38:39 2019 Z
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\mspaint.exe (8)
```



Nella sezione del report, denominata UserAssist, sono riportate informazioni in merito agli applicativi eseguiti recentemente, nel sistema. Nello specifico, è stata individuata una traccia di esecuzione di Microsoft Paint alle 18:38:39 (09/02/2019) pertanto, è possibile supporre che il suddetto software sia stato avviato alle 18:38:39.

{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7} è un GUID (Globally Unique Identifier). Un GUID è un identificativo univoco globale ed è utilizzato da Windows, al fine di identificare determinate tipologie di componenti software (incluse, alcune cartelle di sistema, ecc.). Ogni GUID è composto da 16 byte, rappresentati in esadecimale. In questo caso, il GUID, evidenziato in blu, associato a mspaint.exe, è riferito alla cartella di sistema: *C : \Windows \ System32*

### Un possibile scenario

L'utente avvia Microsoft Paint alle 18:38:39. L'utente intende salvare un file, tramite Microsoft Paint, **NOTA:** È possibile supporre che si tratti di un salvataggio, poiché si è supposto che l'utente abbia creato una immagine. A seguito dell'azione, effettuata dall'utente (ad esempio, un click sul pulsante «Salva»), Microsoft Paint mostra una finestra di dialogo Save As, per il salvataggio di file. È possibile supporre che la chiusura della suddetta finestra sia avvenuta alle 18:39:15. È possibile inoltre ipotizzare che la chiusura di Paint sia avvenuta alle 18:39:17. Possibile Ipotesi: Microsoft Paint aggiorna la lista delle immagini recenti, per gli utilizzi futuri del software stesso, probabilmente alla chiusura dell'applicazione (sarebbero opportune ulteriori verifiche a riguardo).

## 7.3 Analisi dei Registri degli Eventi

Durante l'esecuzione di un software complesso, come il S.O., accadono innumerevoli eventi. La natura degli eventi è vastissima. La maggior parte di essi è registrata dal S.O., mediante un sistema di memorizzazione, denominato Event Logging. Gli eventi vengono memorizzati all'interno di registri degli eventi (detti anche event log o, più semplicemente, log), tali registri contengono informazioni importanti, derivanti dal software e dall'hardware. Le informazioni sono provenienti anche da applicativi, oltre che dal S.O., al fine di notificare eventuali informazioni all'utente. I registri possono essere utilizzati anche per la realizzazione di super timeline. Tutti gli eventi, in Windows, sono gestiti e memorizzati dal servizio Event Logging (Event Logging Service). Gli eventi sono tutti registrati in ordine cronologico, in tal modo, è possibile individuare: eventuali criticità/problems nell'ambito del S.O. e della sicurezza, attività dell'utente, utilizzo di risorse del sistema. È necessario sottolineare, però, che le informazioni registrate, sono dipendenti dalla configurazione del S.O. Ad esempio, è possibile disabilitare completamente il logging degli eventi.

Possibili Informazioni Utili per l'Investigazione Forense fornite da un singolo Evento, memorizzato all'interno di un Registro:

- Tipologia: tramite alcune informazioni, relative ad un evento, come l'ID dell'evento (Event ID) e/o categoria dell'evento (Event Category), è possibile individuare la tipologia di un evento.
- Data e ora: per ciascun evento, viene riportato un timestamp, utile per contestualizzare la finestra temporale, in cui un certo evento ha avuto luogo.
- Elementi Coinvolti/Acceduti:
  - Utenti: vengono specificati gli utenti, coinvolti in un certo evento. **NOTA:** Si fa riferimento anche agli utenti «speciali» di Windows (ad esempio, l'utente speciale Sistema, l'utente speciale Servizio di Rete, ecc.), poiché alcuni eventi sono riferiti ad azioni svolte direttamente da Windows, tramite gli utenti speciali.
  - Altri sistemi: in ambiente di rete, i registri hanno solitamente molteplici riferimenti ad account di sistemi remoti. Nelle versioni più recenti di Windows, viene mantenuto anche l'indirizzo IP, all'interno dei log.
  - Risorse: in base alla granularità della configurazione, i log possono riportare diverse informazioni in relazione a molteplici risorse del S.O.

Sono memorizzati in file con estensione .evtx, dal sistema di Event Logging. La cartella in cui sono memorizzati è tipicamente la seguente: *C :\Windows\System32\WinEvt\Logs*. Il percorso di tale cartella può comunque essere modificata dal registro di sistema. Inoltre, è anche possibile impostare che i log vengano inviati ad un host remoto. Quindi, bisogna considerare anche l'eventuale possibilità che non tutti i log siano memorizzati all'interno della macchina, che si sta analizzando.

### 7.3.1 Principali categorie di log

- Registro di Applicazione (Application Log): è uno spazio utilizzato dalle applicazioni, che intendono registrare degli eventi significativi. Esempio: un anti-virus potrebbe voler memorizzare eventi come l'individuazione di un malware.
- Registro di Sicurezza (Security Log): vengono registrati eventi relativi a controlli sulle politiche di accesso e di sicurezza locali e di gruppo.
- Installazione (Setup): vengono memorizzate informazioni relative a Windows ed all'installazione di aggiornamenti. Esempio: aggiornamenti di sicurezza, installazione di patch, ecc.
- Registro degli Eventi di Sistema (System Log): regista principalmente informazioni riguardanti le operazioni di sistema e la manutenzione di Windows, Esempio: fallimento dell'avvio di un servizio, in fase di boot della macchina.
- Eventi Inoltrati (Forwarded Events): regista eventi provenienti da computer remoti.

### 7.3.2 Registro eventi sicurezza

Prima che un utente possa eseguire una determinata operazione, sono necessari, talvolta, dei controlli di sicurezza (es: controllo dei privilegi), i controlli di sicurezza vengono memorizzati nel registro degli eventi di sicurezza.

Possibili Motivi per cui viene Memorizzato un Evento di Sicurezza:

Tipo di Evento	Descrizione
<b>Errore (Critical/Error)</b>	Notifica di un problema significativo <ul style="list-style-type: none"> <li><i>Esempio:</i> Perdita di dati</li> </ul>
<b>Avviso (Warning)</b>	Notifica di un problema non significativo <ul style="list-style-type: none"> <li><i>Esempio:</i> Spazio in esaurimento</li> </ul>
<b>Informazioni (Information)</b>	Notifica di una operazione eseguita con successo <ul style="list-style-type: none"> <li><i>Esempio:</i> Corretto avvio di un servizio</li> </ul>
<b>Controllo Riuscito (Success Audit)</b>	Notifica che un controllo, relativo allo svolgimento di una certa operazione, ha avuto <b>esito positivo</b> <ul style="list-style-type: none"> <li><i>Esempio:</i> Autenticazione con successo di un utente</li> </ul>
<b>Controllo Fallito (Failure Audit)</b>	Notifica che un controllo, relativo allo svolgimento di una certa operazione, ha avuto <b>esito negativo</b> <ul style="list-style-type: none"> <li><i>Esempio:</i> Accesso ad una risorsa, senza avere permessi (accesso negato)</li> </ul>

### 7.3.3 Il tool Visualizzatore Event

Il tool Visualizzatore Eventi (Event Viewer) è un tool integrato in Windows, permette di visualizzare tutti i registri del sistema in uso. Gli eventi sono visualizzati in maniera molto dettagliata. Il principale svanataggio è che l'analisi del registro può essere particolarmente complessa, per via di una interfaccia utente molto dettagliata, ma al contempo complessa. Si accede al tool dal pannello di controllo. Di un evento è possibile controllare la tipologia, la sua data e ora, la sua origine, l'identificativo e la sua categoria. È possibile anche generare un file xml con le precedenti informazioni.

### 7.3.4 Esportazione dei Registri

Affinché possa essere svolta un'analisi dei registri, è necessario preliminarmente esportarli. La modalità di esportazione, varia in virtù del fatto che ci si trovi a lavorare su un:

- Live System: quando si lavora con un live system, è necessario considerare che i file di log, sono costantemente utilizzati.
  - Prima possibilità: Utilizzare il tool Visualizzatore Eventi e cliccare, con il tasto destro, sul registro di interesse. Selezionare la voce «Salva tutti gli eventi con nome...», verrà fornita la possibilità di esportare il log, in diversi formati: formato utilizzato per i file di log (.evtx), file XML (.xml), file testuale (.txt) e file CSV (.csv)
  - Seconda possibilità: acquisire una immagine forense del disco fisso in cui sono memorizzati i log. Una volta acquisita l'immagine forense, si può trattare il sistema, in maniera offline, come se si trattasse un dead system.

- Dead System: recuperare i file di log (.evtx), dall'apposita cartella. I file .evtx sono in formato binary XML, pertanto, non possono essere analizzati direttamente. Vi sono però diversi tool che permettono l'analisi dei file di log degli eventi

### 7.3.5 Il tool FullEventLogView

Il tool FullEventLogView è sviluppato da NirSoft ed è gratuitamente scaricabile, prevede la visualizzazione dei registri degli eventi, da diverse fonti: Computer locale, Computer remoto sulla rete, File .evtx. Permette anche l'esportazione dei registri, in diversi formati (fra cui, il formato HTML). Disponibile unicamente per sistemi Windows-based 32 bit e 64 bit. Fornisce una pratica e semplice interfaccia grafica, ma è possibile specificare determinate opzioni anche tramite linea di comando. FullEventLogView avvia automaticamente il reperimento di informazioni sugli eventi all'interno del sistema in uso, tale operazione può essere fermata, cliccando su Stop.

## 7.4 La Cartella Prefetch

Al primo avvio di un dato programma P, Windows ne analizzerà il comportamento, nell'arco dei primi 10 secondi di esecuzione registrerà le informazioni in merito ai file utilizzati da P, per il suo avvio. Tali informazioni saranno memorizzate, in un apposito file (detto file di prefetch), associato al programma P, che verrà memorizzato nella cartella Prefetch. Al successivo avvio di P, grazie al file di prefetch, associato a P (creato al primo avvio di P), Windows sarà in grado di precaricare, in memoria, i file che P utilizzerà, per l'avvio. In tal modo, sarà possibile ridurre i tempi di avvio di P.

Tipicamente, ad ogni programma è associato un file di prefetch, il quale contiene le seguenti informazioni:

- Il nome dell'eseguibile del programma
- Il percorso, nel file system, dell'eseguibile
- Numero di volte che il programma è stato eseguito, utile, ad esempio, per individuare il programma più utilizzato dall'utente
- Data e ora delle esecuzioni recenti del programma
- Una lista di file utilizzati dal programma, per il suo avvio

La cartella Prefetch è tipicamente la seguente: *C : \Windows \Prefetch*, oppure, più in generale: <CartellaWindows>\Prefetch. I file di prefetch hanno estensione .pf. Il nome di un file prefetch ha la seguente struttura: <NOME\_ESEGUIBILE>-<VALORE\_HASH>.pf.

Da Windows 8 in poi, la cartella Prefetch può contenere fino a 1024 file di prefetch (associati ad altrettanti eseguibili). Invece, da Windows XP a Windows 7, tale cartella poteva contenere al massimo 128 file di prefetch. Quando il limite massimo di file prefetch è raggiunto, Windows elimina i file di prefetch più datati, per fare spazio ai nuovi.

La funzionalità di prefetching (pre-caricamento) può essere anche utilizzata per ridurre i tempi, relativi alla fase di boot di Windows (funzionalità denominata ReadyBoot). Dal registro di sistema è possibile specificare il comportamento del prefetching, nelle seguenti modalità:

1. Disabilitazione totale del prefetching
2. Abilitazione del prefetching solo per migliorare le performance di avvio delle applicazioni
3. Abilitazione del prefetching solo per migliorare le performance di boot di Windows
4. Abilitazione di entrambi i punti 2. e 3.

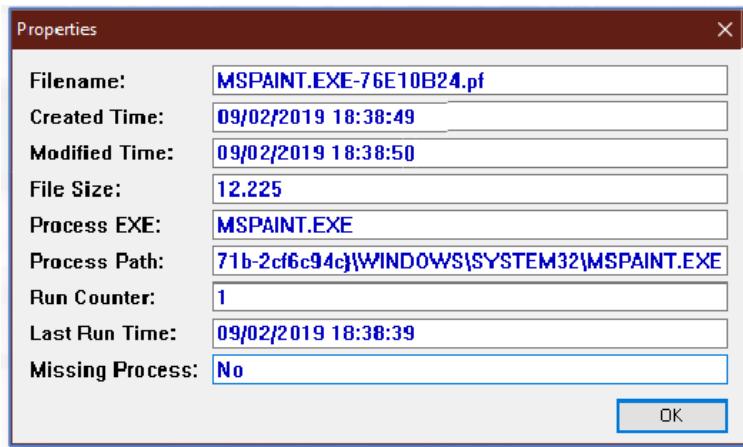
Un file potenzialmente interessante, contenuto all'interno della cartella Prefetch, è il file layout.ini (non è un file di prefetch). layout.ini contiene una lista di file, i quali sono utilizzati con maggior frequenza, dal S.O., nell'ambito delle operazioni di prefetching. Tale file è tipicamente utilizzato per ottimizzare la deframmentazione del disco fisso. I file dovrebbero essere memorizzati in locazioni contigue del disco fisso, per ottimizzare le performance degli accessi ad essi.

### 7.4.1 Il tool WinPrefetchView

Permette di visualizzare tutti i file, contenuti nella cartella Prefetch di Windows. Per ciascun file di prefetch, permette di visualizzarne tutti i dettagli. Di default, visualizza i file di prefetch del sistema in cui il tool è avviato. Tuttavia, tramite delle opportune opzioni a linea di comando, è possibile specificare anche una cartella specifica (o un file di prefetch specifico):

```
WinPrefetchView.exe /folder E:\Windows\Prefetch
```

Disponibile unicamente per sistemi Windows-based. Esempio di informazioni su di un eseguibile:



## 7.5 Attività Pianificate di Windows

All'interno del S.O., possono esservi installate diverse applicazioni, che necessitano di eseguire determinate attività (tasks), in un preciso orario/una precisa data e/o con una determinata frequenza (es: aggiornamenti). Tali attività sono dette attività pianificate (scheduled tasks). Sono memorizzate tipicamente nella seguente cartella: *C :\ Windows \ System32 \ Tasks*. Ciascuna attività pianificata è memorizzata in un file XML, il quale contiene diverse informazioni, fra cui: Chi ha creato l'attività pianificata (autore), quale è la data e/o l'ora in cui l'attività verrà eseguita, eventualmente, la frequenza con cui l'attività verrà ripetuta, Il percorso relativo all'eseguibile o al comando, che verrà eseguito dall'attività. Le attività programmate possono anche essere definite dall'utente (es: invio di un email alle 12).

Analisi delle attività pianificate:

- Live System: l'analisi delle attività pianificate, in un live system, può avvenire mediante il tool (integrato in Windows), denotato come utilità di Pianificazione (Task Scheduler). Il tool è accessibile dal Pannello di Controllo (Utilità di pianificazione).
- Dead System: l'analisi delle attività pianificate, in un dead system, può avvenire mediante l'ispezione dei file XML, associati alle attività pianificate, presenti nella relativa cartella (accedendovi dall'immagine forense, acquisita dal dead system). Es:

```

<Triggers>
  <CalendarTrigger>
    <StartBoundary>2018-12-20T13:12:35</StartBoundary>
    <Repetition>
      <Interval>PT1H</Interval>
      <Duration>P1D</Duration>
    </Repetition>
    <ScheduleByDay>
      <DaysInterval>1</DaysInterval>
    </ScheduleByDay>
  </CalendarTrigger>
</Triggers>

```

## 7.6 La Cache delle Miniature

Al fine di migliorare l'esperienza utente, Windows, tramite la componente Esplora Risorse, agevola la visualizzazione del contenuto delle cartelle. Se richiesto dall'utente, vengono visualizzate delle piccole anteprime di eventuali immagini, contenute all'interno di una cartella. Queste anteprime vengono dette miniature o thumbnail (abbreviato thumb).

Tuttavia, la visualizzazione di una miniatura, relativa ad una certa immagine  $I$ , è una operazione abbastanza onerosa. Infatti, per poter mostrare una miniatura, all'utente, il S.O. deve effettuare diversi passi, fra cui:

- Leggere il file, relativo all'immagine  $I$
- Effettuare il caricamento in memoria di  $I$
- Eventuale Decompressione di  $I$
- Elaborare l'immagine  $I$
- Esecuzione di diverse operazioni, più o meno complesse, su  $I$  (ad esempio, downsizing di  $I$ , ecc.), al fine di generare la miniatura
- Generare la miniatura  $I_M$  per  $I$
- Mostrare, all'utente, la miniatura  $I_M$

Per migliorare le performance e rendere, conseguentemente, più gradevole l'esperienza utente, il S.O. utilizza una cache delle miniature.

### 7.6.1 Idee di Base del Funzionamento

La prima volta, in cui è necessario mostrare, all'utente, la miniatura  $I_M$ , per una certa immagine  $I$ , il S.O. la genera, come indicato precedentemente, e la mostra all'utente. Inoltre, la miniatura generata viene memorizzata all'interno della cache delle miniature. Le successive volte, in cui sarà necessario mostrare, all'utente, la miniatura  $I_M$ , dell'immagine  $I$ , il S.O. la reperirà direttamente dalla cache delle miniature. Ciò riduce notevolmente i tempi, poiché non è più necessario leggere il file, relativo ad  $I$ , effettuare operazioni su  $I$ , ecc.

**Osservazione:** Pertanto, anche se una immagine  $I$ , venisse eliminata, potrebbe essere recuperata la sua miniatura, memorizzata dal S.O., all'interno della cache delle miniature.

Nella pratica, Windows memorizza le miniature in diverse cache. Una miniatura viene memorizzata in una determinata cache, in base alla sua risoluzione. L'obiettivo è di mostrare, all'utente, una

miniatura, nella risoluzione più adeguata possibile (in base alle preferenze dell'utente, ecc.) Ogni cache è caratterizzata da un file, il cui nome ha il seguente formato: thumbcache\_N.db. All'interno di thumbcache\_N.db, saranno memorizzate tutte le miniatures, aventi una risoluzione pari a  $N \times M$ ,  $Q \times N$  o  $N \times N$  pixel (dove  $M$  e  $Q$  sono minori di  $N$ ).

**Esempio:** Ad esempio, nel file thumbcache\_256.db, saranno memorizzate tutte le miniatures con risoluzione pari a  $256 \times 100$ ,  $200 \times 256$ ,  $256 \times 256$ , ecc.

Le cache di miniatures, sono memorizzate al seguente percorso

C:\Users\<NomeUtente>\AppData\Local\Microsoft\Windows\Explorer

Dove <NomeUtente> è lo username dell'utente.

## 7.7 Il tool Thumbcache Viewer

Thumbcache Viewer è un ottimo strumento per l'analisi delle cache delle miniatures. Il software è Open-Source ed è gratuitamente scaricabile. Disponibile unicamente per sistemi Windows-based a 32 bit e 64 bit. Fornisce una semplice e funzionale interfaccia grafica. È inoltre possibile specificare determinate opzioni anche tramite linea di comando.

### 7.7.1 Esempio di utilizzo

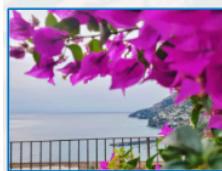
Verrà considerato il seguente scenario:

- Memorizzazione di tre immagini fotografiche (caratteristiche nella prossima slide), su un sistema, equipaggiato con il S.O. Windows 10
- Visualizzazione del contenuto delle cartelle, contenenti le suddette immagini, mediante Esplora Risorse, richiedendo di mostrare le miniatures
- Eliminazione delle tre immagini. NOTA: Si suppone che non sia possibile ripristinare tali immagini, mediante processi di file recovery, normale utilizzo del sistema, spegnimento del sistema per simulare un dead system, acquisizione dell'immagine forense del disco fisso.



#### • Immagine Fotografica 1

- Risoluzione:  $4032 \times 3024$
- Formato: JPEG (estensione .jpg)
- Dimensione: ~1 MB



#### • Immagine Fotografica 2

- Risoluzione:  $1080 \times 810$
- Formato: JPEG (estensione .jpg)
- Dimensione: ~80 KB



#### • Immagine Fotografica 3

- Risoluzione:  $4032 \times 3024$
- Formato: JPEG (estensione .jpg)
- Dimensione: ~1 MB

Utilizzando Thumbcache Viewer, verrà effettuata l'analisi di thumbcache\_768.db (acceduto dall'immagine forense, discussa nello scenario precedente). Gli obiettivi sono recuperare le miniatura, relative alle tre immagini fotografiche e ottenere eventuali ulteriori informazioni in merito a tali immagini. Aprendo il file sul tool vengono estratte 7 miniature dal file.

Per memorizzare le minuature: selezionare tutte le miniature nella lista e cliccare sulla voce "Save Selected...", dal menù contestuale che appare cliccando con il tasto destro.

Caratteristiche delle Miniature estratte dal file thumbcache\_768.db



2 e 7 sono miniatura di cartelle. **Nota:** Alcune miniature sono identiche (varia esclusivamente il nome del file, il contenuto è identico). Possibile spostamento o copia, da parte dell'utente, del file dell'Immagine Fotografica 1 (o della cartella che lo contiene) da una locazione ad un'altra. Osservando le miniatura delle cartelle, è possibile notare che l'Immagine Fotografica 1 e l'Immagine Fotografica 2 erano probabilmente contenute in cartelle diverse (poiché abbiamo due miniatura di cartelle). All'interno di tali cartelle, inoltre, non erano presenti altre immagine (infatti, è visibile una singola immagine per ciascuna cartella).

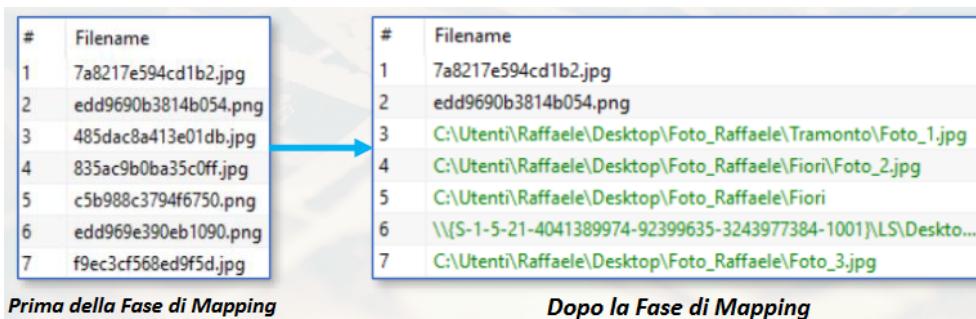
Abbiamo visto che è possibile recuperare le varie miniatura di immagini, dai file di cache. Le miniatura forniscono tipicamente una idea dell'immagine originale, benché non ne conservino tipicamente tutti i dettagli visivi. Possono comunque essere memorizzate in più risoluzioni (a seconda delle preferenze dell'utente, ecc.). Inoltre, il formato e l'estensione potrebbero rimanere invariati rispetto ai file originali (non è però detto che questo avvenga in tutti i casi). Tuttavia, non è stato possibile individuare i percorsi "originali" delle immagini, rappresentate dalle miniatura (poiché esso non è contenuto nei file di cache). I nomi assegnati alle miniatura, infatti, sono riportati come una sequenza di caratteri alfanumerici.

I nomi assegnati alle miniatura non sono casuali, ma si tratta di nomi potenzialmente significativi. Al fine di velocizzare la ricerca di file, Windows, per molteplici cartelle, utilizza dei meccanismi di indicizzazione. Tale indicizzazione avviene tipicamente in automatico, tramite il servizio Windows Search (WSearch). **Idea Base:** Durante l'indicizzazione, viene effettuato anche un mapping, ove a molteplici file, nel sistema, viene associato un indice. Il suddetto mapping viene mantenuto in un database, in formato chiamato ESE (Extensible Storage Engine) database. Il database è memorizzato nel file Windows.edb localizzato nella seguente cartella: C :\ProgramData\Microsoft\Search\Data\Applcaions\Windows.

Sfruttando il database Windows.edb, il tool Thumbcache Viewer permette di risalire ai percorsi, nel file system, delle immagini, rappresentate dalle miniature. Il nome assegnato ad una miniatura potrebbe essere un indice ed, in caso positivo, esso risulterebbe riferito all'immagine, rappresentata dalla miniatura stessa, quindi, tramite il suddetto indice è possibile provare ad individuare il percorso, nel file system, dell'immagine rappresentata. Dopo aver estratto le miniature dal file thumbcache\_768.db, è possibile cliccare sulla voce "Map File Paths..." dal menu Tools, e si aprirà la finestra di dialogo per la selezione del database Windows.edb. All'interno di questa finestra selezioniamo Include Folders e Retrieve Extended Information per avere informazioni più accurate (i filtri, nel campo di testo, sono già specificati dal tool e specificano i vari formati delle immagini). Cliccando su scan avviamo la fase di mapping

### Dopo la fase di mapping

Lista delle Miniature, dopo la Fase di Mapping:



#	Filename
1	7a8217e594cd1b2.jpg
2	edd9690b3814b054.png
3	485dac8a413e01db.jpg
4	835ac9b0ba35c0ff.jpg
5	c5b988c3794f6750.png
6	edd969e390eb1090.png
7	f9ec3cf568ed9f5d.jpg

#	Filename
1	7a8217e594cd1b2.jpg
2	edd9690b3814b054.png
3	C:\Utenti\Raffaele\Desktop\Foto_Raffaele\Tramonto\Foto_1.jpg
4	C:\Utenti\Raffaele\Desktop\Foto_Raffaele\Fiori\Foto_2.jpg
5	C:\Utenti\Raffaele\Desktop\Foto_Raffaele\Fiori
6	\\\\$-1-5-21-4041389974-92399635-3243977384-1001\LS\Desktop...
7	C:\Utenti\Raffaele\Desktop\Foto_Raffaele\Foto_3.jpg

Thumbcache Viewer ha indicato che è riuscito ad effettuare il mapping di 6 file, tuttavia, dalla lista si evince che i file mappati sono solo 5. **Possibile ipotesi:** Come supposto precedentemente, l'Immagine Fotografica 1 è stata probabilmente spostata da una locazione ad un'altra di conseguenza, il suo indice, potrebbe essere associato a due percorsi diversi (e Thumbcache Viewer ha riportato solo il più recente o comunque solo uno dei due percorsi), si tratta ovviamente di una ipotesi che deve essere eventualmente approfondita, se necessario, analizzando, con maggior dettaglio, anche il funzionamento dell'indicizzazione di Windows.

## 7.8 Analisi dei collegamenti

Un collegamento rapido (detto anche scorciatoia, shortcut, link o collegamento) è un file che ha il solo compito di «puntare» ad un altro file. Ad esempio, può puntare ad un documento, all'eseguibile di un programma, ecc. L'obiettivo di un collegamento è di semplificare l'accesso al file/programma a cui punta. Il collegamento, infatti, può essere tenuto in un punto più accessibile, dell'interfaccia grafica del S.O. Esempi: Desktop, Menù Start, Ecc. I file di collegamento hanno estensione .lnk .

I collegamenti, automaticamente creati da Windows, in riferimento ai documenti utilizzati, di recente, dall'utente, vengono, in genere, memorizzati nelle due seguenti cartelle:

```
C:\Users\<NomeUtente>\AppData\Roaming\Microsoft\Windows\Recent
C:\Users\<NomeUtente>\AppData\Roaming\Microsoft\Office\Recent
```

Un collegamento memorizza diverse informazioni, relative al file a cui punta:

- Data e ora di creazione/ultima modifica/ultimo acceso
- Nome

- Percorso
- Dimensione
- Informazioni sul dispositivo di memorizzazione, in cui è localizzato il suddetto file

**Nota:** Un collegamento (creato automaticamente da Windows o comunque creato dall'utente) non viene (automaticamente) eliminato, nel caso in cui il file, puntato da tale collegamento, venga eliminato. Questa caratteristica può essere estremamente utile, soprattutto in particolari scenari.

### **Esempio**

L'utente (su cui eventualmente si sta investigando) ha visionato un documento di testo, sul suo PC, dotato del S.O. Windows. Tale documento è stato visionato da un dispositivo di memorizzazione esterno (ad esempio, una penna USB), che l'utente ha scollegato dal PC e, successivamente, distrutto (o comunque il dispositivo non è più leggibile/accessibile dagli investigatori). Windows ha creato automaticamente il collegamento al suddetto documento. Il collegamento riporta anche informazioni in merito al dispositivo di memorizzazione, su cui era memorizzato il file, puntato dal collegamento stesso pertanto, è comunque possibile dimostrare che è stato aperto/utilizzato un documento, memorizzato su un certo dispositivo (ad esempio, una penna USB), poiché il collegamento non viene (automaticamente) eliminato anche se il file, di fatto, non è più accessibile, poiché il dispositivo è stato scollegato.

In virtù delle considerazioni precedenti, relative alle informazioni, fornite dal file system, sul collegamento (.lnk) possiamo supporre che:

- La data/ora di creazione del collegamento potrebbe far riferimento alla data/ora in cui il file (a cui il collegamento punta) è stato aperto per la prima volta
- La data/ora dell'ultima modifica del collegamento potrebbe far riferimento alla data/ora in cui il file (a cui il collegamento punta) è stato aperto per l'ultima volta
- Se la data/ora di creazione e la data/ora dell'ultima modifica del collegamento coincidono, si potrebbe supporre che il file (a cui il collegamento punta) è stato aperto solo una volta, dalla locazione specificata dal collegamento

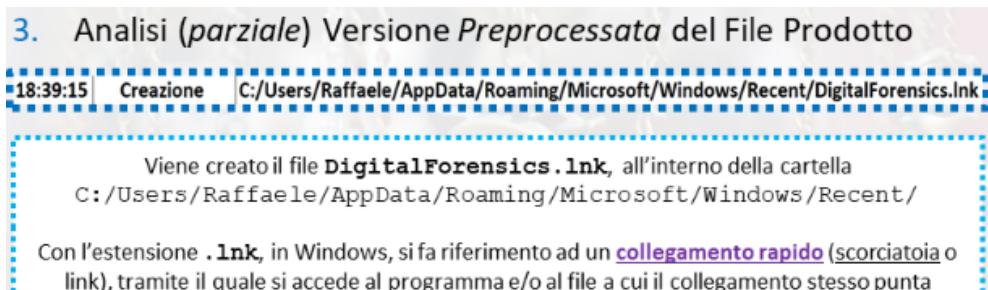
### 7.8.1 ExifTool

ExifTool è uno strumento a linea di comando. Permette di effettuare lettura, modifica e scrittura dei metadati di molteplici tipologie di file, fra cui i file .lnk

```
> "exiftool(-k).exe" [input]
```

[input]: Parametro che permette di specificare il percorso del file di input.

#### Esempio di utilizzo



Tramite ExifTool, analizziamo il file di collegamento, denominato DigitalForensics.lnk. DigitalForensics.lnk è acceduto dall'immagine forense, utilizzata per l'Esempio di Utilizzo 3 dell'Argomento 5 (Super Timeline). Gli obiettivi sono:

- L'individuazione di conferme alle ipotesi, precedentemente redatte
- L'individuazione di eventuali ulteriori informazioni, incluse informazioni sul file, a cui il collegamento punta

```
ExifTool Version Number      : 11.27
File Name                  : DigitalForensics.lnk
Directory                  : E:/Users/Raffaele/AppData/Roaming/Microsoft/Windows/Recent
File Size                   : 686 bytes
File Modification Date/Time : 2019:02:09 19:39:15+01:00
File Access Date/Time       : 2019:02:09 19:39:15+01:00
File Creation Date/Time    : 2019:02:09 19:39:15+01:00
File Permissions            : rw-rw-rw-
File Type                  : LNK
File Type Extension        : lnk
MIME Type                  : application/octet-stream
Flags                      : IDList, LinkInfo, RelativePath, WorkingDir, Unicode, NoKnownFolderTracking
File Attributes             : Archive
Create Date                : 2019:02:09 19:39:15+01:00
Access Date                : 2019:02:09 19:39:15+01:00
Modify Date                : 2019:02:09 19:39:15+01:00
Target File Size           : 2448
Icon Index                 : (none)
Run Window                 : Normal
Hot Key                    : (none)
Target File DOS Name       : DigitalForensics.png
Drive Type                 : Fixed Disk
Volume Label               :
Local Base Path            : C:/Users/Raffaele/Desktop/DigitalForensics.png
Relative Path              : ..\..\..\..\Desktop\DigitalForensics.png
Working Directory          : C:/Users/Raffaele/Desktop
Machine ID                 : desktop-64e4ls7
```

Dall'analisi osserviamo che:

- Il file DigitalForensics.lnk, relativo al collegamento, dalla dimensione di 686 byte, acceduto dall'immagine forense (montata, in sola lettura, sul drive virtuale, a cui è stata contrassegnata la lettera E:)
- il file è di tipo LNK (collegamento) ed ha estensione .lnk

- Dalle informazioni sul file DigitalForensics.lnk, è possibile osservare che la data e l'ora di creazione e la data e l'ora dell'ultima modifica coincidono (ovvero, le 18:39:15 del 09/02/2019). **NOTA:** Tutte le informazioni sugli orari, del presente esempio, sono riportate con un'ora in più, per un errore di redazione dell'esempio. Pertanto è possibile supporre che il file (a cui il collegamento punta) è stato aperto solo una volta, dalla locazione specificata dal collegamento.

Tutte le informazioni riportate successivamente, riguarderanno il file a cui il collegamento punta e non il file DigitalForensics.lnk. Il file puntato ha la seguente locazione: *C :\Users\Raffaele\Desktop\DigitalForensics.png*. Scompriamo che le informazioni sono coerenti con le ipotesi discusse precedentemente. DigitalForensics.png (il file a cui il collegamento punta) era memorizzato su un disco fisso (valore Fixed Disk di Drive Type), il quale non aveva etichetta del volume (Volume Label). Possiamo osservare che DigitalForensics.png (il file a cui il collegamento punta), è stato creato alle 18:39:15 del 09/02/2019. Anche questa informazione è coerente. È possibile inoltre notare come DigitalForensics.png (il file puntato dal collegamento), dopo la creazione, non sia stato più acceduto/modificato (data/ora della creazione, dell'ultima modifica, dell'ultimo accesso coincidono). È inoltre possibile conoscere la dimensione (in byte) del file DigitalForensics.png (file puntato dal collegamento): 2448 byte ( 2 KB), dal valore Target File Size. Ultima informazione, potenzialmente utile, anche per analisi successive, che è possibile osservare, è l'ID della macchina: desktop-64e41s7 (valore di Machine ID).

## 7.9 Il cestino virtuale

i recenti S.O. non prevedono (di default) la "cancellazione diretta" di file e/o directory, effettuata dall'utente, tramite l'interfaccia grafica. Un file/directory cancellato viene prima spostato nel Cestino virtuale (Recycle Bin). Per eliminare i file definitivamente è necessario svuotarlo. Dal cestino è anche possibile ripristinare i file.

La cartella associata al Cestino è memorizzata nella root della partizione di sistema (ad esempio, *C :\*). Il nome e la struttura della cartella sono dipendenti dalla versione di Windows. Da Windows XP fino a prima di Windows Vista RECYCLER. Da Windows Vista in poi (incluso Windows 10) \$Recycle.Bin.

### 7.9.1 RECYCLER

All'interno della cartella RECYCLER, vi è una sottocartella, per ciascuno degli utenti del sistema. Il nome di ciascuna sottocartella è l'identificativo dell'utente (User ID), a cui tale sottocartella fa riferimento. Una sottocartella di RECYCLER, associata ad uno specifico utente, conterrà esclusivamente i file cancellati (spostati nel Cestino), dall'utente ad essa associato. I file cancellati però non mantengono il proprio nome, bensì hanno un nome sequenziale: DC1, DC2, DC3, e così via. Vi è un file, denominato INFO2, il quale specifica il mapping tra i file in tale sottocartella (che iniziano con DC1, DC2, ecc.) ed i relativi percorsi dei file originali. Questo file è utilizzato da Windows, anche per soddisfare eventuali azioni di ripristino da parte dell'utente inoltre, vengono specificate le informazioni sulla data e l'ora della cancellazione.

### 7.9.2 \$Recycle.Bin

All'interno della cartella \$Recycle.Bin, vi è una sottocartella, per ciascuno degli utenti del sistema. Il nome di ciascuna sottocartella è l'identificativo SID dell'utente (Secure ID), a cui tale sottocartella fa riferimento. Una sottocartella di \$Recycle.Bin, associata ad uno specifico utente, conterrà esclusiva-

mente i file cancellati (spostati nel Cestino), dall'utente ad essa associato. Nello specifico, per ogni file cancellato, vengono generati due file:

1. File che memorizza il contenuto del file cancellato. Il nome inizia per \$R, seguito da una stringa random
2. File che memorizza le informazioni in merito al file cancellato (detto anche file indice). Utilizzato da Windows, anche per soddisfare eventuali azioni di ripristino da parte dell'utente. Il nome inizia per \$I, seguito dalla medesima stringa random, del file \$R (file 1.)

Quando un file viene cancellato definitivamente dal Cestino, vengono cancellati entrambi i file associati (file \$R e file \$I). **Nota:** Quando si lavora con un dead system, si ha a disposizione esclusivamente l'immagine forense, pertanto, è necessario considerare il file INFO2 (nel caso della cartella RECYCLER), oppure, i file \$I (nel caso della cartella \$Recycle.Bin), per estrarre informazioni utili.

### 7.9.3 Tool Rifiuti2

Rifiuti2 è un tool Open-Source che analizza il cestino dei S.O. Windows ed estrae diverse informazioni, fra cui:

- Data e ora della cancellazione di ciascun file
- Path del file originale
- Dimensione dei file cancellati

Rifiuti2 è utilizzabile dal terminale di Kali Linux, mediante due comandi:

- rifiuti: Specifico per la cartella RECYCLER. Da Windows XP fino a prima di Windows Vista. Utilizzo (sintassi semplificata): rifiuti <file\_INFO2>.
- rifiuti-vista: Specifico per la cartella \$Recycle.Bin. Da Windows Vista in poi (incluso Windows 10). Utilizzo (sintassi semplificata): rifiuti-vista <directory\_o\_file>.

#### Esempio 1 di utilizzo con RECYCLER

Eseguiamo il comando:

```
> rifiuti INFO2-sample1
```

```
root@kali:~/Scrivania# rifiuti INFO2-sample1
INFO2 File: INFO2-sample1

INDEX  DELETED TIME      DRIVE NUMBER  PATH          SIZE
44     10/28/2008 16:53:42  2   C:\DOCUMENTS\ALLUSE-1\Desktop\#e000~1.LNK    4
096
45     11/03/2008 16:01:59  2   C:\Documents and Settings\Administrator\Desktop
\wongsir_url.txt        4096
46     11/06/2008 10:20:58  2   C:\Documents and Settings\Administrator\Desktop
\dd-wrt.v24 mini_wrt54g.bin 2912256
47     11/13/2008 13:08:39  2   C:\Documents and Settings\Administrator\Desktop
\theme\.svn             765952
48     11/13/2008 13:11:33  2   C:\Documents and Settings\Administrator\Desktop
\Config Client          5812224
49     11/13/2008 13:11:36  2   C:\Documents and Settings\Administrator\Desktop
\Config Client.7z         1847296
```

### Esempio 2 di utilizzo con RECYCLER

Eseguiamo il comando:

> rifiuti INFO2-sample2

#### Esempio di utilizzo con \$Recycle.Bin

Tramite Rifiuti2, analizziamo i file contenuti nel Cestino, estraendoli dalla stessa immagine forense, utilizzata per l'Esempio di Utilizzo 3 dell'Argomento 5 (Super Timeline).

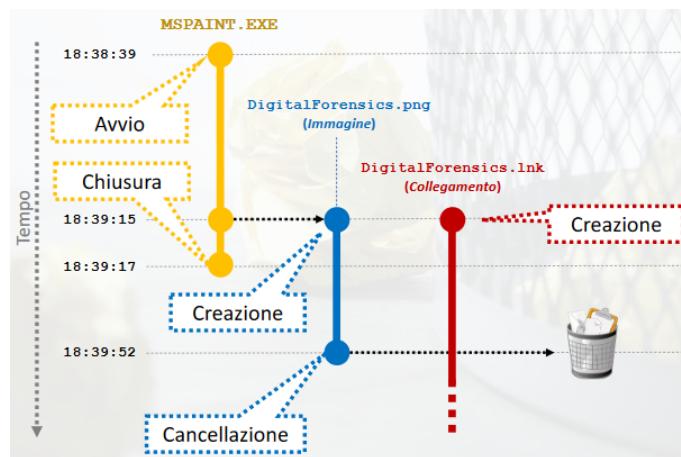
Eseguiamo il comando:

> rifiuti-vista cestino\_win/

```
root@kali:~/Scrivania# rifiuti-vista cestino_win/
Recycle bin path: 'cestino_win/'
Version: 2
Index Deleted Time Size Path
$133G700.png 2019-02-09 18:39:52 nps 2448 jeanC:\Users\Raffaele\Desktop\DigitalForensics.png
```

Il Cestino contiene un unico file cancellato, che fa riferimento al file DigitalForensics.png (come osservabile, dal path). Le informazioni reperite sono le seguenti:

- Cancellato alle 18:39:52 (09/02/2019)
  - Dimensione pari a 2448 byte (informazione coerente con quanto osservato precedentemente)
  - Il file indice è denominato \$I33G70Q.png



## 7.10 Analisi delle Copie Shadow

Una copia shadow (letteralmente, copia ombra), detta anche punto di ripristino, shadow copy o volume shadow copy (VSS), è una copia di backup dei file di Windows (e non solo). La particolarità di tali copie è che esse vengono generate, in maniera trasparente all'utente, durante l'utilizzo normale del sistema. Le copie shadow vengono utilizzate, al fine di ripristinare il sistema, nel caso in cui si siano riscontrate problematiche. Dal punto di vista forense, le copie shadow sono particolarmente importanti, soprattutto negli scenari in cui un sospetto ha cercato di eliminare delle tracce.

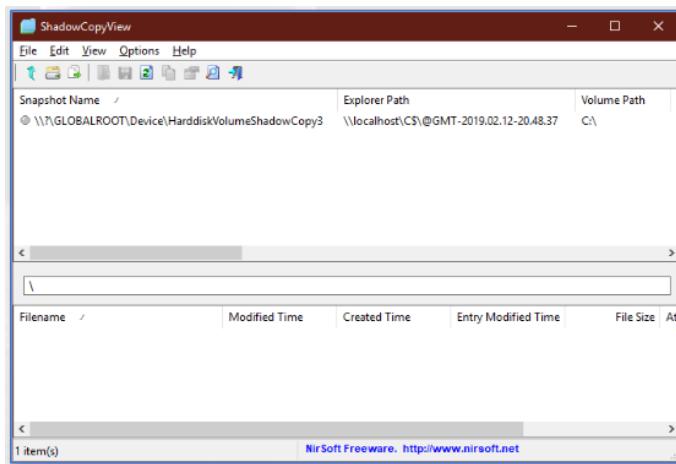
### 7.10.1 Svantaggi/Limiti

Una copia shadow potrebbe però non contenere informazioni utili, per l'investigazione forense, inoltre, anche individuando dei file, potenzialmente rilevanti, l'investigatore sarà in grado di visualizzare esclusivamente una versione di tali file (snapshot), non viene fornito un servizio di versioning dei file. Il servizio per la creazione di copie shadow è attivo di default, nella partizione in cui è installato il S.O., tuttavia, è possibile disattivare tale servizio. La creazione di una copia shadow può avvenire: periodicamente, oppure prima che si installi del software, il quale potrebbe danneggiare il sistema (driver, ecc.). Le copie shadow vengono tipicamente sovrascritte dal S.O. In generale, quindi le copie shadow sono degli artefatti utili principalmente al S.O., in caso di necessità di ripristino.

L'utente ha comunque la possibilità di creare un punto di ripristino, dalla finestra Proprietà del sistema (Tab: Protezione Sistema), accessibile da Pannello di Controllo → Sistema → Protezione Sistema.

### 7.10.2 Il tool ShadowCopyView

Il tool ShadowCopyView consente di navigare all'interno di una copia shadow, permettendo all'investigatore di visionare i vari file in essa contenuti: possibilità di utilizzo da penna USB (utile nei live system), interfaccia grafica semplice ed intuitiva, gratuitamente scaricabile e disponibile per sistemi Windows-based (32 bit e 64 bit). Sviluppato da NirSoft.

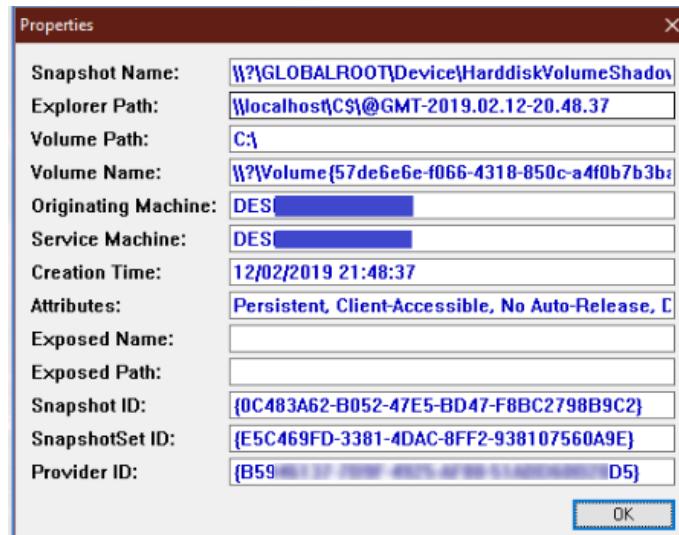


Selezionare la copia shadow desiderata, per visionare i file e le cartelle estratte da essa:



Possibilità di copiare il file o la directory selezionata all'interno di una cartella qualsiasi del sistema in uso (per effettuarne l'analisi). Possibilità di visualizzazione dei file, relativi alla copia shadow selezionata, nell'Esplora Risorse di Windows (per maggiore praticità).

Proprietà di una Shadow Copy:



Possibilità di ricerca di file/directory mediante la ricerca tramite parole chiave.

# Capitolo 8

# Network Forensics

La network forensics è un ramo della digital forensics, si occupa degli aspetti forensi riguardanti le reti (computer, apparati di rete, ecc.). Principalmente, la network forensics viene eseguita sui live system, viene acquisito il traffico raw, prodotto dalle interfacce di rete di un dispositivo informatico: pacchetti, eventuali log, ecc. Tale traffico viene poi analizzato.

## 8.1 Il tool Xplico

Xplico è un tool Open Source che permette l'analisi forense di traffico di rete. L'acquisizione del traffico di rete può essere eseguita mediante Xplico stesso o mediante tool esterni (ad esempio, Wireshark, Ettercap, ecc.). **NOTA:** Wireshark ed Ettercap sono direttamente disponibili in Kali Linux e Parrot Linux. Xplico permette di analizzare file che contengono acquisizioni di rete, i quali hanno generalmente estensione .pcap (packet capture).

Tantissimi protocolli di rete sono supportati da Xplico, fra cui:

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Hypertext Transfer Protocol (HTTP)
- File Transfer Protocol (FTP)
- Internet Message Access Protocol (IMAP)
- Simple Mail Transfer Protocol (SMTP)
- Post Office Protocol (POP3)
- Ecc.

Fornisce una interfaccia intuitiva e web-based.

All'interno del traffico di rete possiamo trovare tracce molto utili per le indagini, ad esempio: indirizzi Web di Siti Visitati, contenuto di E-mail, chat di Social Network, pacchetti VoIP e file stampati.

In caso di errore di installazione aggiungere la seguente riga

```
deb http://http.kali.org/kali kali-rolling main non-free contrib  
al file sources.list, nella cartella /etc/apt
```

Prima di avviare Xplico è necessario specificare i seguenti comandi, dal Terminale di Kali Linux:

```
> service apache2 start
> service xplico start
```

### 8.1.1 Esempio di utilizzo

Per gli esempi di utilizzo delle prossime slide, verranno utilizzati tre file, in formato PCAP. I file PCAP memorizzano traffico di rete, acquisito precedentemente. Utilizzeremo i seguenti tre file:

1. xplico.org\_sample\_capture\_web\_must\_use\_xplico\_nc.cfg.pcap
2. freeswitch4560\_tosipphone\_ok.pcap
3. smtp.pcap

#### Esempio di Utilizzo 1 - HTTP & Web

Alla creazione di un nuovo caso vengono richieste le seguenti informazioni:

- La metodologia di acquisizione: File con dati di rete, precedentemente acquisiti (file con estensione .pcap)
- Acquisizione diretta del traffico, mediante Xplico, dall'interfaccia di rete
- Il nome del caso
- Eventuali riferimenti esterni

Una volta creato un caso è possibile selezionandolo creare una nuova sessione. Apriamo la sessione appena creata e elaboriamo il file. In questo esempio, utilizzeremo il file, denominato: xplico.org\_sample\_capture\_web\_must\_use\_xplico\_nc.cfg.pcap.



Ora verranno spiegate tutte le sezioni:

- Sessione dei Dati: vengono mostrate alcune informazioni sui dati acquisiti, fra cui:
    - Data e ora dell'inizio dell'acquisizione
    - Data e ora della fine dell'acquisizione
    - Host da cui è stata effettuata l'acquisizione
- Nel nostro esempio l'intervallo di acquisizione è di circa 33 secondi.

- HTTP: viene riportato il numero di pacchetti POST, il numero di pacchetti GET, il numero di pacchetti relativi ad immagini e video (nell'esempio, non è stato individuato nessun pacchetto di questo tipo)
- E-mail: riporta il numero di e-mail ricevute, inviate e non lette, individuate nel traffico analizzato (nell'esempio, non è stata rilevata alcuna e-mail)
- Web Mail: viene indicato il numero di e-mail (gestite mediante client Web) ricevute, inviate e non lette, individuate nel traffico analizzato (nell'esempio, non è stata rilevata alcuna e-mail)
- Facebook Chat/Paltalk: vengono riportate le statistiche relative alla chat di Facebook (ed altra chat Paltalk) ed ai relativi utenti identificati (nell'esempio, non è stata individuata alcuna informazione)
- Sconosciuti: vengono riportate le statistiche in relazione ad artefatti/oggetti sconosciuti (non decodificati). Nello specifico, sono stati identificati diversi artefatti testuali ed oggetti denominati Dig

È possibile approfondire gli artefatti sconosciuti mediante le sezioni del menù

- TCP-UDP: vengono mostrate tutte le connessioni effettuate verso un host. Sono mostrate data e ora in cui una connessione è stata effettuata, indirizzo di destinazione(ip e porta), il protocollo usato, la durata della connessione e il numero di byte generato dalla connessione. Se un dato è evidenziato con un colore rosso scuro è possibile ottenere ulteriori dettagli. Esempio: Cliccando sul link relativo all'indirizzo IP di destinazione (ovvero 74.125.77.100) della prima connessione, verrà scaricato un file testuale con il contenuto del/dei pacchetto/i

HTTP/1.1 200 OK			
Date: Wed, 09 Dec 2009 17:42:46 GMT	10	373	
Content-Length: 35	d	251	
Pragma: no-cache	13	104	
Cache-Control: private, no-cache, no-cache=Set-Cookie, proxy-revalidate	13	496	
Expires: Wed, 19 Apr 2000 11:43:00 GMT	6	038	
Last-Modified: Wed, 21 Jan 2004 19:50:30 GMT	6	81	
Content-Type: image/gif	7	643	
Server: Golfe			
X-XSS-Protection: 0			

Esempio: Cliccando poi sul link info.xml e su pcap, si aprirà una pagina contenente ancora altri dettagli in relazione alla connessione in esame.

- Dig: In questa sezione vengono mostrati diversi file, con una data e ora, il nome del file, il tipo, la loro dimensione e il loro file info.xml.

### 8.1.2 VoIP

Voice over IP (VoIP) definisce un insieme di protocolli, il segnale analogico, prodotto dalla voce, viene convertito in un segnale digitale, il quale viene incapsulato in pacchetti, ciò permette di effettuare chiamate telefoniche, mediante le infrastrutture di rete.

La comunicazione mediante VoIP è:

- Real-time
- Bi-direzionale

Le linee telefoniche sono generalmente su rete PSTN (Public Switched Telephone Network).

Una telefonata VoIP ha due fasi principali:

1. Setup: viene instaurata una sessione. In questa fase può essere utilizzato uno dei seguenti protocolli: H.323, SIP (Session Initiation Protocol), ecc.
2. Flusso Audio: Se chiamante e chiamato hanno accettato la sessione, (instaurata nella fase di setup), viene avviato il flusso audio (ovvero, la telefonata). Il protocollo utilizzato è tipicamente RTP (Real-Time Protocol)

## Protocollo SIP

Il protocollo SIP (Session Initiation Protocol) permette di iniziare, modificare e terminare sessioni per: chiamate telefoniche, conferenze con più flussi multimediali (ad esempio, conferenze telefoniche). L'identificativo (telefonico) è associato all'utente, non al terminale, analogia con l'e-mail (associata all'utente). L'identificativo è nel formato Uniform Resource Identifier (URI), esempio: sip:rpizzolante@unisa.it, sip:+39089546445454@gateway.com, sip:pincopallino@1.2.3.4.

Protocollo di tipo client-server con scambio di messaggi testuali, analogia con il protocollo HTTP.

- Creazione della sessione: instaurare la sessione per una chiamata, impostando adeguati parametri, ecc.
- Gestione di una sessione: trasferimento di una sessione, modifiche ai parametri della sessione, invocazione dei servizi

### Esempio di Utilizzo 2 - VoIP

In questo esempio, utilizzeremo il file, denominato: freeswitch4560\_tosipphone\_ok.pcap.

HTTP	MMS	E-mail	FTP - TFTP - HTTP di file	Web Mail
Post 0	Numeri 0	Ricevute 0	Connessioni 0 - 0	Totale 0
Get 0	Contenuto 0	Inviate 0	Scaricato 0 - 0	Ricevute 0
Video 0	Video 0	Non lette 0/0	Caricato 0 - 0	Inviate 0
Immagini 0	Immagini 0		HTTP 0	
<hr/>				
Facebook Chat / Paltalk		IRC/Paltalk Exp/Msn/Yahoo!	Dns - Arp - ICMPv6	NNTP
Utenti 0	Chat 0/0	Server 0	DNS res 0	Gruppi 0
		Canali 0/0/0	ARP/ICMPv6 0/0	Articoli 0
<hr/>				
Feed & Printed files		WhatsApp	Telnet / Systog	Sconosci.
Numero 0	Pdf 0	Connection 0	Connessioni 0/0	Testi 0/1
				Dig 0

Come è possibile osservare, sono state individuate 2 chiamate, tramite servizio VoIP (con il protocollo SIP). Nel menù nella sezione VoIP in SIP possiamo ottenere più informazioni.

Data	Da	A	Durata
2007-10-31 12:14:23	"FreeSwitch" <sip:5555551212@192.168.1.111>	<sip:6580@192.168.1.12>	0:0:0
2007-10-31 12:14:23	"FreeSwitch" <sip:5555551212@192.168.1.111>	<sip:6580@192.168.1.12>	0:0:19

Sono state effettuate due chiamate da "Freeswitch" <sip:5555551212@192.168.1.111> (colonna denominata Da) a <sip:6580@192.168.1.12> (colonna denominata A) della durata rispettivamente di 0 secondi e 19 secondi (entrambe le comunicazioni sono state effettuate alle ore 12:14:23 del giorno 31/10/2007, come si evince dalla colonna Data). Cliccando sulla durata possiamo ottenere più informazioni. Per esempio il contenuto di alcuni pacchetti SIP (file cmd.txt), per esempio tramite il valore di user-agenti si può individuare il modello degli apparati che hanno effettuato la comunicazione.

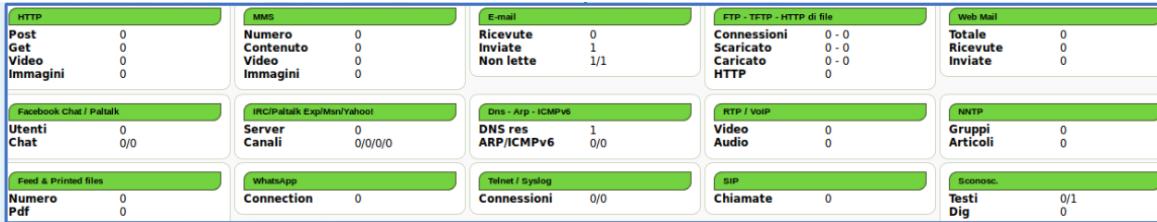
### 8.1.3 Protocolli E-mail

Esistono diversi protocolli per inviare un email:

- Simple Mail Transfer Protocol (SMTP): utilizza la porta 25 ed è usato per inviare le email
- Post Office Protocol (POP3): utilizza la porta 110 ed è usato per la ricezione di e-mail: permette di effettuarne il download dal server e-mail al client
- Internet Message Access Protocol (IMAP): utilizza la porta 143 ed è utilizzato per la ricezione di e-mail: permette di effettuarne il download dal server e-mail al client, ma una copia delle e-mail è lasciata sul server, in modo da permettere l'accesso anche da altri client (ad esempio, client Web, ecc.)

### Esempio di Utilizzo 3 - E-mail

In questo esempio, utilizzeremo il file, denominato smtp.pcap.



Come è possibile osservare dalla sezione E-mail, Xplico ha individuato una e-mail. Per vederne il contenuto andiamo nella sezione poste/email. È stata individuata una e-mail (dove non è stato specificato l'oggetto), inviata da gurpartap@patriots.in (colonna Mittente) a raj\_deol2002in@yahoo.co.in (colonna Ricevitori), avente dimensione, in termini di byte, pari a 14544. Cliccando sull'oggetto dell'email (denominato -(no subject)-) è possibile visionare il contenuto della e-mail.



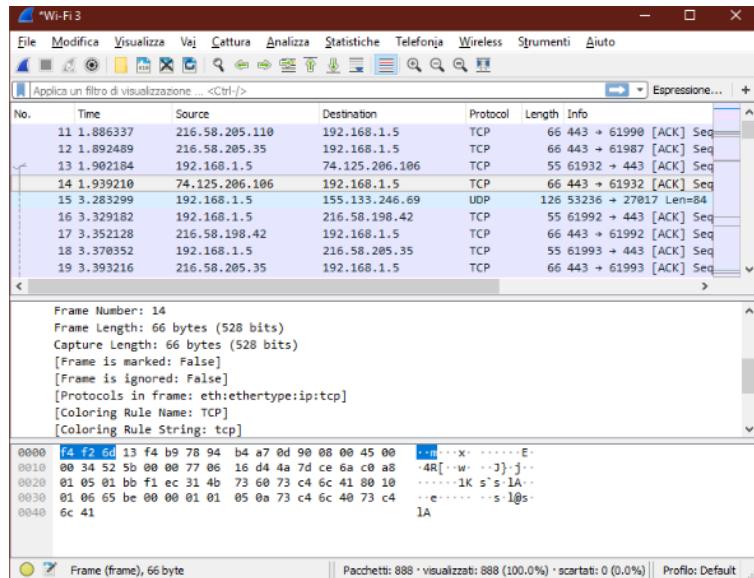
Viene fornita la possibilità di scaricare l'email in formato EML, il quale è un formato standard, in accordo alla RFC 5322, e può essere aperto da diversi client e-mail. Cliccando sul nome di un allegato (news.txt nel nostro caso), è possibile scaricarlo e/o visionarlo.

## 8.2 Acquisizione Traffico di Rete - Wireshark

Wireshark è uno sniffer di traffico di rete. È in grado di catturare il traffico di rete, in modalità promiscua<sup>7</sup>.

Wireshark permette la definizione di filtri per l'acquisizione del traffico ad esempio, acquisizione di pacchetti di determinati protocolli, da determinati host, ecc.

### 8.2.1 Esempio di Utilizzo



Nella schermata possiamo notare:

- Elenco dei pacchetti acquisiti: Per ciascun pacchetto (uno per ciascuna riga), vengono riportate diverse informazioni, tra cui:
  - Numero e timestamp (time) del pacchetto
  - Indirizzo IP sorgente e destinazione
  - Protocollo (per facilitare la visualizzazione, le righe relative a pacchetti con diversi protocolli, vengono riportate di colore diverso)
  - Dimensioni (in termini di byte)
  - Ulteriori informazioni
- Dettagli ed informazioni aggiuntive del pacchetto selezionato (in questo caso il pacchetto numero 14)
  - Contenuto del pacchetto selezionato (in questo caso il pacchetto numero 14): Byte-per-byte in esadecimale (a sinistra) e Byte-per-byte in ASCII (a destra).
  - Dettagli ed informazioni (schermata estesa) aggiuntive del pacchetto selezionato.

<sup>7</sup>Nella modalità promiscua, tutto il traffico osservato, da una interfaccia, viene passato alla CPU (si tratta di una modalità di controllo) ed è quindi possibile memorizzarlo

# Capitolo 9

## Anti-Forensics

L'Anti-Forensics (AF) è una collezione di strumenti e tecniche atte a mettere in difficoltà gli strumenti forensi, gli investigatori ed il normale svolgimento dell'indagine. Gli obiettivi principali sono:

- Evitare che vengano individuate alcune tracce di eventi, che hanno avuto luogo
- Interrompere la raccolta di informazioni
- Aumentare il tempo necessario, per lo svolgimento di una indagine
- Innescare dubbi sul report di una indagine
- Forzare i tool forensi a rilevare la propria presenza
- Sovvertire gli strumenti forensi (ovvero, utilizzarli come tool per l'anti-forensics)
- Effettuare un attacco diretto all'investigatore forense
- Non lasciare tracce dell'esecuzione di un tool per l'anti-forensics

### 9.1 Principali categorie per le tecniche anti-forensics

#### 9.1.1 Nascondere/Eliminare le Evidenze

Per esempio pulire una superficie per eliminare le impronte digitali, pulire le orme delle scarpe per nascondere una fuga, ecc.

#### Sovrascrittura di Dati e Metadati

Esistono tool che permettono di sovrascrivere dati potenzialmente rilevanti, per l'indagine, in tal modo, tali informazioni vengono perse. Questi tool operano tipicamente in tre modalità:

1. Sovrascrittura dell'intero dispositivo di memorizzazione
2. Sovrascrittura di singoli file
3. Sovrascrittura dell'unallocated space, il quale potrebbe contenere file eliminati (ma ancora presenti sul dispositivo di memorizzazione)

Alcuni tool permettono di sovrascrivere i timestamp, contenuti nei metadati del file system:

- Data/ora dell'ultimo accesso a un file
- Data/ora di creazione di un file

- Data/ora dell'ultima modifica a un file
- Data/ora dell'ultima modifica ai metadati del file

Tali metadati potrebbero essere utilizzati per la realizzazione di timeline tradizionali. In questo scenario, l'ordine degli eventi, riportati nella timeline, potrebbe risultare alterato.

Il tool **Attribute Changer** è un software gratuito, permette, in maniera semplice, di modificare i metadati di un file. Si integra all'interno dell'interfaccia utente di Windows (Esplora Risorse), facendo un click, con il tasto destro, su un certo file, verrà mostrato il relativo menu contestuale, il quale permetterà la modifica dei metadati, è possibile mantenere un rapporto (log), in cui si tiene traccia di ogni modifica ai metadati di un certo file. Il log è esportabile in un foglio elettronico.

Un altro tool per la Sovrascrittura di Metadati è **Timestomp** (Metasploit). Permette di sovrascrivere i metadati, relativi al file system NTFS.

### Crittografia e Information Hiding

La crittografia e gli approcci di information hiding (occultamento di dati), possono essere utilizzati contro la maggior parte delle tecniche forensi. La crittografia è particolarmente efficace, per nascondere dati, tuttavia, i dati crittografati sono facilmente rilevabili, infatti, i dati crittografati hanno un'entropia elevata. Inoltre, diversi tool per la crittografia, inglobano metadati o header particolari, all'interno dei file e ciò contribuisce a renderli riconoscibili.

In questa categoria, possiamo individuare le seguenti tecniche per l'anti-forensics:

- File System Crittografato: effettua la cifratura dei file. La cifratura viene effettuata quando i file vengono memorizzati sul dispositivo di memorizzazione. I file vengono decifrati, solo quando vi è necessità di effettuare delle operazioni su di essi (ad esempio, lettura/scrittura del file, ecc.). Un investigatore, quindi, non può analizzare i file, contenuti in un file system siffatto, poiché essi sono cifrati.
- Protocolli di rete crittografati: Il traffico di rete può essere crittografato, al fine di proteggerlo dall'analisi forense. Esistono diversi protocolli che permettono di crittografare il contenuto del traffico:
  - Secure Sockets Layer (SSL)
  - Secure SHell (SSH)
 L'idea di base è che i pacchetti di rete, vengono cifrati ed incapsulati. Esiste poi l'onion routing, il quale fa uso di nodi intermediari, grazie ai quali è possibile proteggere il traffico di rete, da eventuali analisi
- Information Hiding: Mediante le tecniche di information hiding è possibile nascondere informazioni, in diverse tipologie di file.

Esistono tool che permettono di nascondere dati, all'interno delle strutture del file system o del S.O. Esempi:

- Slacker (Metasploit): è in grado di nascondere dati all'interno dello slack space, nel file system FAT oppure NTFS
- StegoMFT: è in grado di nascondere dati all'interno della Master File Table (MFT), del file system NTFS

### 9.1.2 Minimizzare le evidenze lasciate dai tools per l'AF

Esempi nel Mondo Fisico: pulire le tracce lasciate da un'arma del delitto, polvere da sparo, residui, ecc.

#### Memory Injection

Sfruttando le vulnerabilità di buffer overflow, è possibile iniettare codice malevolo, nello spazio di indirizzi di un programma vittima, in esecuzione. In tal modo, il comportamento del programma «vittima», viene alterato. Tradizionalmente, i buffer overflow sono utilizzati come punto di ingresso in un sistema remoto. In questo scenario, l'attaccante è in grado di memorizzare i tool per l'AF, sul sistema remoto.

#### Live CD, Penne USB bootable e Virtual Machine

Live CD, penne USB bootable e macchine virtuali possono essere utilizzati come strumenti per l'anti-forensics. In genere, tali strumenti lasciano poche tracce.

- Live CD: un Live CD è un supporto di memorizzazione di sola lettura (ad esempio, un CD-ROM, un DVD-ROM, ecc.), permette l'avvio e l'esecuzione di un S.O., senza che il S.O. venga effettivamente installato sulla macchina
- Penne USB bootable: analogamente ai Live CD, una penna USB bootable permette di avviare ed eseguire un S.O., senza che esso venga installato sulla macchina. La principale differenza consiste nel fatto che è possibile effettuare operazioni di scrittura, in tali dispositivi. In tal modo, ad esempio, un attaccante potrebbe memorizzare dei file, creati direttamente sul S.O., che è stato avviato dalla penna USB<sup>8</sup>
- Macchine Virtuali: Si tratta di un S.O. «client», il quale viene eseguito in un programma (ad esempio, VMWare, Oracle VirtualBox, ecc.). Il sistema che esegue il suddetto programma e, conseguentemente, il S.O. client, viene detto sistema host. Sul sistema host, vengono memorizzati gli «stati» del S.O. client ed un piccolo insieme di file (file di configurazione, ecc.). A seguito dello svolgimento di un attacco e/o di azioni malevoli, sul S.O. client, il malintenzionato dovrebbe solo cancellare in modo sicuro (minimizzando le tracce della cancellazione) i file associati alla macchina virtuale

#### Accessi anonimi e memorizzazioni anonime

Un malintenzionato potrebbe utilizzare diversi account anonimi o falsi, su vari servizi di Cloud storage online. Al momento della creazione di un nuovo account, viene fornita una significativa quantità di spazio. I malintenzionati potrebbero utilizzare lo spazio, fornito dai suddetti account, al fine di memorizzare dei tool per l'AF ed eventuali informazioni acquisite.

---

<sup>8</sup>Con un Live CD o una penna USB bootable, è possibile quindi utilizzare un certo PC, per effettuare eventuali attacchi, non lasciando alcuna traccia (o lasciandone pochissime) del suddetto attacco

### 9.1.3 Sfruttare bug dei tool per l'investigazione forense

#### Mancato controllo dei dati di input

I tool forensi, dovrebbero svolgere adeguati controlli sull'input, onde evitare di incorrere in potenziali attacchi. Ad esempio, attacchi di buffer overflow, ecc. Gli attacchi ai suddetti tool, potrebbero arrecare problemi ed errori, durante lo svolgimento dell'indagine forense.

#### Attacchi Denial of Service (DoS)

L'utilizzo di risorse (CPU, memoria RAM, spazio su disco, ecc.), da parte di alcuni tool forensi, è dipendente dai dati di input. In questi casi, le suddette risorse potrebbero essere soggette ad attacchi di tipo DoS (Denial-of-Service). Mediante tecniche di compressione dati, è possibile produrre un particolare attacco DoS, denominato compression bombs attack. In dettaglio, vengono realizzati particolari file compressi, denominati compression bomb, analizzando questi file, alcuni tool forensi devono utilizzare notevoli quantitativi di risorse, soprattutto, in termini di spazio del disco. Un esempio di compression bomb è il file denominato 42.zip, di circa 44 KB. Questo file contiene 16 file zippati, ciascuno di tali file contiene ancora 16 file zippati, ciascuno di tali file contiene ancora 16 file zippati, ciascuno di tali file contiene ancora 16 file zippati, ciascuno di tali file contiene ancora 16 file zippati, ciascuno di tali file contiene ancora 16 file zippati, ciascuno di tali file contiene ancora 16 file zippati, ciascuno dei quali contiene un file da 4.3 GB. La dimensione del file alla fine è di 4.5 PetaByte (PB).

#### Euristiche Fragili

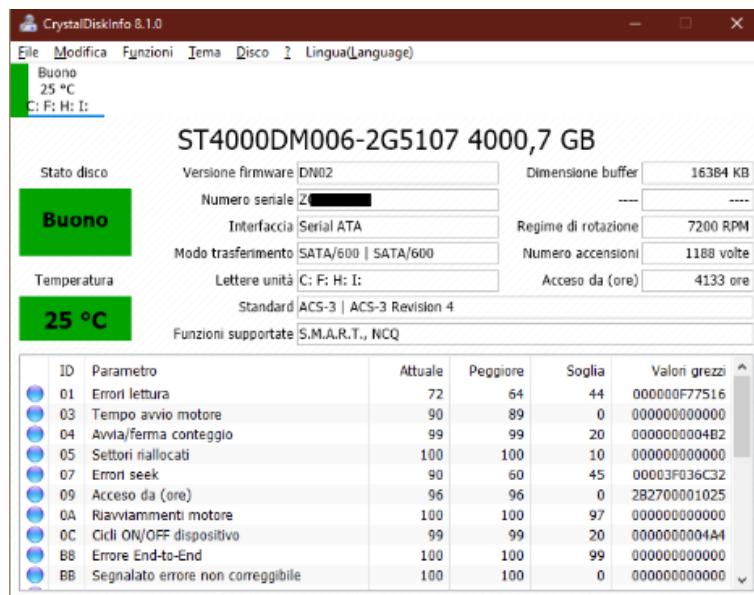
Alcuni tool forensi, necessitano di conoscere la tipologia di file, al fine di permettere una elaborazione efficiente ed efficace. In genere, per identificare la tipologia di un file, i tool si basano sull'header di un file. Tecniche per l'Anti-Forensics. Conoscendo le heuristiche utilizzate, un attaccante può sfruttarle in maniera maliziosa, ad esempio, l'attaccante può alterare l'header di un file (prima di eliminarlo), probabilmente, tale file potrebbe non essere ripristinato dai tool di file recovery.

### 9.1.4 Rilevare l'utilizzo di tool per l'investigazione forense

#### Contrastare l'analisi forense mediante la tecnologia S.M.A.R.T.

La maggior parte dei dischi fissi, integra una tecnologia chiamata S.M.A.R.T. S.M.A.R.T. è l'acronimo di Self-Monitoring, Analysis and Reporting Technology. Mediante questa tecnologia, il disco fisso monitora sé stesso (self-monitoring), fornendo diverse informazioni diagnostiche: il numero totale accensioni, il tempo totale di attività (ovvero, il tempo in cui il disco è stato utilizzato), eventuali temperature elevate raggiunte dal dispositivo, altri attributi, specificati dal produttore.

Esempio di informazioni S.M.A.R.T., fornite dal software gratuito CrystalDiskInfo



La tecnologia S.M.A.R.T. prevede un comando, denominato DISABLE, per disabilitare il tracciamento delle informazioni diagnostiche, tuttavia, sperimentalmente, è stato osservato che solo alcuni modelli lo implementino. Inoltre, in alcuni casi, anche se tale comando è implementato e viene utilizzato, la tecnologia S.M.A.R.T. continua a tener traccia del tempo di attività e del numero di accensioni. I tool per l'Anti-Forensics possono trarre beneficio dalle informazioni, fornite dalla tecnologia S.M.A.R.T. Infatti, tramite tali informazioni, è possibile cercare di capire se sono già stati utilizzati determinati tool per l'analisi forense. **Esempio:** un aumento significativo del tempo di attività del disco fisso, potrebbe indicare che è stato utilizzato un tool per l'acquisizione di una immagine forense

#### Contrastare la Network Forensics

Molti tool per la network forensics acquisiscono il traffico, utilizzando un'interfaccia di rete, in modalità promiscua. In genere, gli host, che effettuano il monitoring della rete, non dovrebbero essere in grado di trasmettere sulla rete che stanno monitorando. Tuttavia, nella pratica, i suddetti host, non sono spesso configurati correttamente, pertanto, è possibile identificare (ed, eventualmente, attaccare) questi host, analizzando le loro risposte a pacchetti malformati

## 9.2 Alcune Contromisure

Alcune delle tecniche anti-forensi possono essere semplicemente superate, migliorando i tool forensi • Ad esempio, utilizzando controlli più rigidi dell'input, ecc. Inoltre, è possibile mettere in difficoltà i tool, per la sovrascrittura dei dati/metadati, memorizzando questi ultimi in supporti di sola lettura:

- CD-ROM/DVD-ROM
- Ecc.

I suddetti supporti, ad esempio, un volta scritti, non possono essere alterati (si suppone, inoltre, che l'attaccante non vi abbia accesso fisico).

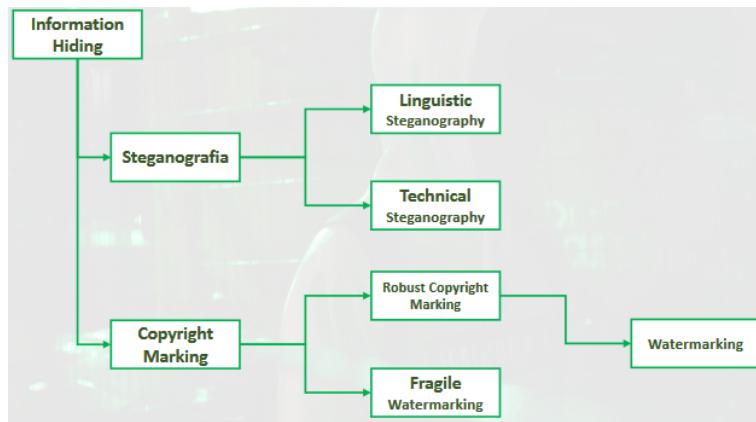
Un'altra possibilità è quella di inviare dei log (relativi ai dati memorizzati, nel file system) ad un host remoto a cui si ha accesso.

I compression bombs attacks potrebbero essere evitati, un tool forense potrebbe avvisare l'investigatore di comportamenti potenzialmente anomali. Per esempio se la decompressione di un file richiede un tempo più lungo di una certa soglia oppure se la dimensione dei dati estratti supera una certa soglia.

La crittografia dei file ed, in generale, i file system crittografati, sono, in generale, un problema per gli investigatori forensi. Tuttavia, in alcuni casi, è stato possibile recuperare password e/o chiavi crittografiche, utilizzando spyware, key logger e altre tecniche.

## 9.3 Information Hiding | Cenni e Richiami

Mediante le tecniche di information hiding è possibile nascondere informazioni, in diverse tipologie di file.



### 9.3.1 Esempio Didattico 1 | Information Hiding in File RTF

Il formato Rich Text Format (RTF) permette di memorizzare documenti di testo formattati. Un file, in formato RTF, può essere aperto da Microsoft WordPad, Microsoft Word ed altri editor/visualizzatori di file RTF. All'interno di un file RTF è possibile nascondere delle informazioni. RTF utilizza un linguaggio di markup simile ad HTML, è molto improbabile che si vada a visionare il sorgente di un file RTF. Ciò facilita l'information hiding, all'interno dei file RTF.

```

{\rtf1\ansi\ansicpg1252\deff0\nouicompat\de
flang1040{\fonttbl{\f0\fnil\fcharset0
Calibri;}}
{\*\generator Riched20
  
```

```

10.0.17763}\viewkind4\uc1
\pard\sa200\s1276\slmult1\f0\fs22\lang16
Ciao, \i nascondo\i0 un \ul\b
segreto\ulnone\b0 !\par
\par
\par
}

```

Sorgente del file secreto.rtf. **Nota:** Il sorgente di un file RTF, può essere visionato aprendo tale file, mediante un semplice editor di testi (come, ad esempio, Microsoft Blocco Note). \i indica l'inizio di un testo formattato in italico, \i0 indica la fine di un testo formattato in italico. Il «sorgente» deve necessariamente iniziare con l'header {\rtf e deve terminare con il footer }, tutte le informazioni dopo il footer, non vengono considerate, dai visualizzatori/editor di file RTF (come, ad esempio, Microsoft WordPad, ecc.) Le informazioni dopo il footer, infatti, saranno totalmente ignorate.

### 9.3.2 Esempio Didattico 2 | Information Hiding in File EXE

Consideriamo un certo eseguibile (EXE), E.exe, per sistemi basati su Microsoft Windows. Alteriamo uno o più byte di E.exe, al fine di nascondere informazioni in tali byte. È conveniente alterare dei byte «poco significativi» (per evitare di alterare il normale comportamento del programma stesso). Esempio: I byte di una stringa costante, utilizzata raramente e solo in caso di errori gravi, nell'esecuzione del programma. Per semplicità, salviamo la versione dell'eseguibile, che nasconde informazioni, nel file E1.exe. Si otterrà il seguente risultato:

E1.exe sarà eseguito normalmente da Windows

L'hash (calcolato, ad esempio, con MD5) del file E.exe, sarà ovviamente diverso dall'hash del file E1.exe

Verranno effettuati i seguenti passi:

1. Scrittura di un semplice programma in linguaggio C (per semplicità, verranno definite due stringhe costanti, non utilizzate nell'esecuzione del programma)
2. Compilazione del suddetto programma: L'output della compilazione, ovvero, l'eseguibile, sarà memorizzato nel file E.exe
3. Salvataggio dell'eseguibile modificato (che nasconde informazioni), nel file E1.exe
4. Cancellazione di E.exe e normale utilizzo/esecuzione del file E1.exe

```

1 #include <stdio.h>
2
3 int main(int argc, char *argv [])
4 {
5     char *stringa1 = "Digital ";
6     char *stringa2 = "Forensics";
7
8     printf("Ciao, Mondo!!!!");
9
10 }

```

"Digital " (8 byte) e "Forensics" (9 byte) sono due stringhe costanti, che non verranno utilizzate, in fase di esecuzione, ma che saranno comunque contenute all'interno dell'eseguibile. Il loro valore esadecimale può essere modificato senza portare ad un cambiamento dell'exe, ma il valore hash del file cambierà.

# Capitolo 10

## Digital Image Forensics

È una branca del Digital Forensics che si occupa dell'estrazione di prove processuali da immagini digitali( Source Camera Identification (SCI)). Riveste un ruolo fondamentale nelle indagini per pedopornografia , rappresenta la differenza tra una condanna per possesso di materiale pedopornografico ed una per produzione.

### 10.1 Source Camera Identification (SCI)

Un problema comune nel mondo dell'Image forensics è l'avere una o più foto digitali incognite e una sola macchina fotografica. Noi da questi elementi vogliamo sapere se quella macchina ha scattato quella foto e se qualcuno ha alterato quella foto. Per far questo ci viene in aiuto la teoria dei segnali.

#### Rumore nelle foto

All'interno di una macchina fotografica è presente un sensore(CCD).È fatto di silicio e contiene imperfezioni dovute al materiale ed al processo di lavorazione. Le fluttuazioni nei valori dei pixel nei punti in cui ci sono queste imperfezioni sono costanti. Possono essere utilizzati per identificare il CCD che ha scattato la foto che contiene quello specifico rumore (1,2,3). Questo rumore si chiama Pixel Non-Uniformity (PNU). Estrarre il PNU non è facile non esiste un modo "diretto" di estrarre il PNU. La foto contiene anche rumore proveniente da altre fonti, ad esempio rumore elettrico, disturbi da freddo o caldo eccessivo, rumore magnetico. Sappiamo però ottenere una foto senza rumore! Si usa un filtro che, in maniera statistica, elimina le lq fluttuazioni nei valori dei pixel. Questo processo si chiama denoising.

#### Estrazione del rumore

Il PNU si ottiene per sottrazione: come primo passo applichiamo un filtro wavelet alla foto digitale  $i$  (denoising), Otteniamo così l'immagine filtrata  $F_I$ . Il rumore residuo lo otteniamo sottraendo all'immagine originale l'immagine filtrata  $Rn = I - F_I$ . Ma questo ancora non ci basta! Abbiamo detto prima che l'immagine contiene altro rumore oltre al PNU, questo si chiama Residual Noise (RN).

#### 10.1.1 Impronta digitale della camera

Per ottenere l'impronta di una camera innanzitutto dobbiamo scattare un certo numero di foto con quella camera (sperimentalmente l'ideale è almeno 60). Quindi se ne calcola la media  $Rp = \frac{\sum_i Rn_i}{|i|}$ . Questa media è chiamata Reference Pattern (RP).

### 10.1.2 Incastriamo il colpevole

Ora abbiamo un Rn per la foto I di cui vogliamo identificare la camera sorgente e un Rp per la camera D. Calcoliamo la correlazione (distanza) tra i due  $C_{DI} = \text{corr}(Rp_D, Rn_I)$ . Calcoliamo una soglia di accettazione  $\theta$  usando la tecnica di Newman-Pearson. Se  $C_{DI} > \theta$  allora I è stata scattata usando D.