



UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Analisi forense di file nel sistema operativo Windows

Analisi di tools e creazione di software contenitore

Informatica Forense
Ruffo Sara
Mat. 699859
a.a. 2019/2020

Sommario

Introduzione	4
Descrizione generale del progetto	4
Glossario.....	4
Inquadramento.....	5
Uso nell'informatica forense	6
Proprietà di file	6
Jumplist	7
Dispositivi usb	9
• Classe di archiviazione di massa (MSC):	9
• Picture Transfer Protocol (PTP):.....	9
• Media Transfer Protocol (MTP):	9
Shellbags	12
Shimcache	13
Appcache.....	14
Prefetch	16
Superfetch	17
Analisi tools	17
JumpListView v1.16	17
Descrizione	17
Requisiti di sistema	17
JumpListView Columns	18
USBDeview v2.85.....	19
Descrizione	19
Requisiti di sistema	19
Problemi noti	20
USBDeview Columns	20
BrowsingHistoryView v2.35.....	21
Descrizione	21
Requisiti di sistema	22
Problemi noti	23
Opzioni Avanzate	23
Lettura Cronologia precedente	25
ShellBags Explorer 1.3.3.0	25
Descrizione	25
Requisiti di Sistema.....	26
Vista ad albero	26

Time zone support	27
AppCompatCacheParser 1.4.3.1	27
Descrizione	27
Requisiti di sistema	28
ChromeCacheView v2.00.....	28
Descrizione	28
Requisiti di sistema	29
WinPrefetchView v1.35	29
Descrizione	29
Requisiti di sistema	31
SuperFetchTree	31
Descrizione	31
Uso.....	32
Requisiti di sistema	33
Ulteriori funzioni	33
Proprietà dei file	33
Descrizione	33
Uso.....	33
Risultato	36
Proprietà file .LNK.....	36
Unione file CSV	37
Sistema	38
Come eseguire	38
Aggiornamento.....	38
Tools Nirsoft	38
Tools Eric Zimmerman	40
Altri tools	42
SuperFetchTree	42

Introduzione

Scopo di questo documento

Lo scopo che si prefigge questo documento è di spiegare cosa il progetto dovrà offrire, rappresentandolo come una scatola nera e descrivendo il suo comportamento esterno.

Descrizione generale del progetto

L'obiettivo principale del presente progetto è la ricerca e l'analisi dei tools esistenti per la creazione di un cruscotto interattivo che consenta l'analisi forense di proprietà di file, jumplist, proprietà file .LNK, proprietà dispositivi USB, cronologia Browser, shellbags, shimcache, appcache, prefetch e superfetch.

Glossario

Jumplist: Rappresenta un elenco di elementi e attività visualizzato come menu in un pulsante della barra delle applicazioni. Permettono di accedere rapidamente, al massimo con un paio di clic, ai file ed alle cartelle che si utilizzano più spesso.

File .LNK: I file LNK sono file di scorciatoia associati a Windows e sviluppati da Microsoft Corporation. LNK è un acronimo di LINK. I file LNK (conosciuti anche come collegamenti di shell) vengono utilizzati come riferimento a un file originale. Contiene proprietà di base come: Tipo di file, posizione, dimensione, nonché il programma che apre il file di destinazione

Dispositivi USB: Dispositivi che utilizzano l'interfaccia normalizzata USB, nonché standard industriale di comunicazione seriale.

Cronologia Browser: Funzione che memorizza e visualizza in ordine cronologico le pagine visitate con un browser durante la navigazione in Internet o le ricerche effettuate in un motore di ricerca.

Shellbags: Un set di chiavi del registro di sistema che memorizza i dettagli di una cartella visualizzata, ad esempio dimensioni, posizione e icona.

Shimcache: Shimcache, noto anche come AppCompatCache , è un componente dell'Application Compatibility Database , creato da Microsoft (a partire da Windows XP) e utilizzato dal sistema operativo per garantire

la retrocompatibilità dei vecchi binari con le nuove versioni dei sistemi operativi Microsoft

Appcache: Noto anche come Application Cache (AppCache) viene usata per specificare le risorse che il browser deve memorizzare nella cache e rendere disponibili per gli utenti offline. Le applicazioni in cache si caricano e funzionano correttamente anche se gli utenti cliccano sul tasto refresh del browser quando sono offline

Prefetch: Il prefetch è una funzionalità, introdotta in Windows XP e ancora utilizzata in Windows 10, che memorizza dati specifici sulle applicazioni eseguite per aiutarli ad avviarsi più velocemente. Il prefetch è un algoritmo che aiuta ad anticipare i mancati cache (volte in cui Windows richiede dati che non sono memorizzati nella cache del disco) e li memorizza sul disco rigido per un facile recupero.

Superfetch: Superfetch è una funzione che tenta di determinare quali applicazioni verranno avviate e quindi carica tutti i file e i dati necessari in memoria. Entrambe queste funzionalità richiedono alcune operazioni di lettura e scrittura per funzionare.

Inquadramento

Il presente progetto prevede le seguenti fasi:

- Identificazione delle necessità forensi;
- Analisi dei tools prescelti;
- Integrazione con funzioni necessarie;
- Sviluppo del programma e generazione del file eseguibile.

Uso nell'informatica forense

Proprietà di file

Le proprietà dei file prendono il nome di metadati. Essi sono spesso descritti come "dati sui dati" e vengono utilizzati per fornire informazioni su un file o documento specifico.

L'informatica forense li utilizza per analizzare le attività di dispositivi digitale. Di solito, la maggior parte dei campi dei metadati sono nascosti e non visibili o accessibili all'utente finale.

Individui malevoli potrebbero alterare o eliminare i metadati per nascondere le proprie attività. Quando questo avviene, si evidenziano incoerenze tra i vari punti che possono rivelare indizi di manomissione delle prove o distruzione.

Esempi di metadati includono

- Nome del file
- Estensione del file
- Dimensione del file
- Data dell'ultimo accesso
- Data di creazione
- Data dell'ultima modifica

I metadati sono importanti indipendentemente dal tipo di indagine in cui si è coinvolti. Ad esempio, i metadati delle cartelle cliniche elettroniche sono fondamentali quando si indaga se un medico ha modificato la cartella clinica di un paziente.¹

<https://www.forensicon.com/resources/articles/what-is-metadata/>

Jumplist

Jump Lists è una nuova funzionalità dei sistemi operativi Windows. È stata introdotta a partire da Windows 7.

Mostra i file e le attività utilizzate più di recente o più frequentemente da un utente. Sono simili alle scorciatoie in quanto portano l'utente direttamente ai file o alle directory.

Sono diversi dai normali *Accessi Rapidi* in quanto le informazioni visualizzate sono differenti per ogni applicazione. Ad esempio, Internet Explorer utilizzerà Jump List per visualizzare i siti Web visitati di frequente; i prodotti Microsoft Office come Excel, PowerPoint e Word, invece, mostreranno i documenti aperti più di recente.

Il contenuto e le attività specificate di questi sono gestiti dall'applicazione specifica responsabile per quel file di destinazione specifico.

Gli Jump List contengono diversi tipi di informazioni per ciascun tipo di applicazione e per ogni azione (es. Apertura, aggiornamento, eliminazione, ecc.) sul file.

Dal punto di vista dell'utente, le Jump List aumentano l'efficienza fornendo un rapido accesso ai file, dal punto di vista di un investigatore forense, le Jump Lists sono un buon indicatore di quali file sono stati aperti di recente o quali siti Web sono stati visitati frequentemente.

Essendo relativi ai prodotti Windows, esistono limitati analisi di ricerca nell'area del valore forense dei dati degli Jump List.

Barnett è stato il primo ad analizzare il valore forense dei dati degli Jump List di Windows. Nel suo esperimento non ha usato alcuno strumento forense per computer. L'autore ha utilizzato un PC con Windows 7 con vari browser Web per scaricare immagini da un sito Web. Quindi la quantità e il tipo di informazioni archiviate dagli Jump List sono state confrontate manualmente per diversi browser Web.

In Windows 7, i dettagli dei file a cui si accede, sono conservati all'interno di file di archiviazione strutturati che sono essi stessi memorizzati nel profilo dell'utente. I file sono denominati con 16 cifre esadecimali, noti come AppID, seguiti da due estensioni di file nascoste denominate automaticDestinations e customDestinations. Il primo set memorizza le informazioni sull'utilizzo dei file di dati. Gli articoli vengono ordinati in

base a quello usato più di recente (Most Recently Used - MRU) o in base a quello usato più di frequente (Most Frequently Used - MFU), a seconda dell'applicazione.²

Dispositivi usb

Ottenere informazioni sui dispositivi USB collegati al momento o nel passato a un sistema può essere fondamentale per alcune indagini.

Le pen drive USB sono il mezzo più utilizzato da malintenzionati per il furto di dati e la propagazione di malware. Pertanto, i manufatti correlati possono essere una parte essenziale di molte indagini.

Lo scopo principale dell'analisi forense dell'unità USB è identificare i dispositivi collegati e trovare delle seguenti informazioni al riguardo come: tempo di connessione e rimozione, file copiati sul o dal dispositivo, file e software aperti ed eseguiti dall'unità collegata.

Tra i vari tipo di dispositivi USB, quella che viene utilizzato maggiormente per scopi di archiviazione è la classe di archiviazione di massa (MSC).

- **Classe di archiviazione di massa (MSC):**
 - Utilizzato da chiavette USB, lettori mp3, alcuni smartphone
 - Su Windows, è riconosciuto come driver del disco rigido o dispositivo con memoria rimovibile
 - I file possono essere copiati da o verso l'unità
- **Picture Transfer Protocol (PTP):**
 - I dispositivi supportati sono: telecamere, alcuni smartphone
 - Può essere utilizzato in caso di download di immagini o video da una memoria esterna
 - L'utente può scaricare file dall'unità ma non può caricare nulla su di esso (unidirezionale)
- **Media Transfer Protocol (MTP):**
 - Tecnicamente un successore di PTP
 - Spostamento di file bidirezionale (da / verso l'unità)
 - Può essere utilizzato in caso di tipi di file diversi da PTP
 - Dispositivi supportati: fotocamere, smartphone

<https://commons.erau.edu/cgi/viewcontent.cgi?article=1317&context=adfsf>

Un consorzio di sette aziende iniziò lo sviluppo di USB nel 1994: Compaq, Hewlett-Packard, IBM, Microsoft, NEC e Nortel.

L'obiettivo era rendere più semplice il collegamento di dispositivi esterni ai PC, affrontando i problemi di usabilità delle interfacce esistenti e semplificando la configurazione software di tutti i dispositivi collegati a USB, oltre a consentire una maggiore velocità dati per dispositivi esterni.

Quando si analizza in modo forense un computer, è necessario tenere conto anche dei vari dispositivi che vi sono, o vi sono stati, collegati.

Pertanto, non è possibile ignorare pen drive, schede di memoria collegate tramite adattatori USB, dischi rigidi rimovibili, penne, TV, videogiochi e qualsiasi altra cosa ad esso collegata.

Come specificato dall'organizzazione USB, ogni dispositivo USB deve avere un identificatore di codice univoco basato su tre campi: VendorID, ProductID e Serial-String.

Tuttavia, Windows utilizza VendorId, ProductID e BcdDevice (numero di revisione) per comporre le chiavi di registro che devono essere ricercate nel database del Registro di sistema per garantire l'utilizzo del dispositivo USB. Il campo USB bInterfaceClass, bInterfaceSubClass e bInterfaceProtocol influenzano anche il modo in cui Windows gestisce il dispositivo e il suo driver.

Il modo migliore per verificare se un dispositivo USB è stato collegato a un computer Windows è cercare nel registro tramite l'identificatore univoco USB.

Cronologia browser

Durante l'analisi forense, non bisogna tralasciare le informazioni che si potrebbero ricavare dai browser presenti sul dispositivo. I browser contengono una moltitudine di informazioni che si potrebbero rivelare utili ai fini dell'indagine.

Le informazioni che possono essere estratte da un browser sono contenute negli artefatti, quali cronologia di navigazione, segnalibri, elenco di file scaricati, dati della cache ... ecc.

Questi artefatti sono file memorizzati all'interno di cartelle specifiche nel sistema operativo e ogni browser memorizza i suoi file in una posizione diversa rispetto ad altri browser e hanno tutti nomi diversi, ma tutti

tendono ad archiviare lo stesso tipo di dati.

Gli artefatti più comunemente memorizzati dai browser sono:

- **Cronologia di navigazione:** contiene dati sulla cronologia di navigazione dell'utente. Può essere utilizzato venire a conoscenza dei siti visitati dall'utente e della data/ora in cui questo è avvenuto
- **Completamento automatico dei dati:** sono i dati suggeriti dal browser in base a ciò che è più spesso ricercato dall'utente. Può essere utilizzato unitamente alla cronologia di navigazione per ottenere maggiori informazioni.
- **Cache:** durante la navigazione di siti Web, il browser salva nella cache vari tipi di dati (immagini, file javascript ... ecc.). Questo avviene per varie ragioni come ad esempio, per accelerare il tempo di caricamento dei siti Web. Questi file presenti nella cache possono essere un'ottima fonte di informazioni durante un'indagine forense.

La principale fonte di prove viene comunque considerato il database cronologico del profilo dell'utente e le principali aree di interesse per gli investigatori sono:

- **URL:** la tabella degli URL contiene la cronologia di navigazione di base che contiene una singola istanza per tutti gli URL visitati, un timestamp per l'ultima volta visitata e un contatore per il numero di volte visitate.
- **VISITE:** la tabella delle visite è unica per i browser che utilizzano Chromium. Contiene più record per lo stesso URL, uno per ogni volta che la pagina viene visitata. Un utente può avere diversi record per "google.com" e la tabella delle visite verrà elencata ogni volta che è stata visitata a cui viene aggiunto un timestamp aggiuntivo ogni volta che la pagina è stata visitata.³

Shellbags

Gli shellbag sono file di formato proprietario Microsoft che sono stati resi disponibili a partire da Windows XP ma solo recentemente sono diventati popolari. Sempre solo attualmente il loro potenziale valore forense sta iniziando ad essere apprezzato.

Gli shellbag aiutano a tenere traccia di viste, dimensioni e posizioni di una finestra di una cartella se visualizzate tramite Esplora risorse; questo include cartelle di rete e dispositivi rimovibili.

La posizione, la vista o le dimensioni di una determinata finestra della cartella potrebbero non essere utili per un'indagine. La loro validità si accresce corredandole con una serie di artefatti aggiuntivi creati da Windows durante la memorizzazione di queste proprietà nel registro.

Così si viene a formare una visione approfondita della cartella, della cronologia di navigazione e dei dettagli per qualsiasi cartella che, per vari motivi, potrebbe non esistere più su un sistema.

I shellbags sono strutturati in un formato simile alla gerarchia Windows Explorer. Ogni cartella è numerata e rappresenta una cartella genitore o un figlio di quella precedente. All'interno di ciascuna di queste cartelle si trovano le chiavi MRUListEx, NodeSlot e NodeSlots:

- MRUListEx contiene un valore di 4 byte che indica l'ordine in cui è stato effettuato l'ultimo accesso a ciascuna cartella figlio nella gerarchia BagMRU. Ad esempio, se una determinata cartella ha tre cartelle secondarie etichettate 0, 1 e 2 e la cartella 2 era l'ultima a cui si accedeva, MRUListEx elencherà prima la cartella 2 seguita dall'ordine di accesso corretto per le cartelle 0 e 1
- Il valore NodeSlot corrisponde alla particolare impostazione di visualizzazione memorizzata per quella cartella. Combinando i dati di entrambe le posizioni, gli investigatori sono venuti a conoscenza dei dettagli di una determinata cartella e come sono stati visualizzati dall'utente
- NodeSlots si trova solo nella sottochiave root BagMRU e viene aggiornato ogni volta che viene creato un nuovo shellbag

L'aggiunta di shellbag ad un'analisi aiuterà a ricostruire una sequenza temporale di eventi. Sebbene un'analisi corretta della shellbag possa essere impegnativa, i dati inclusi negli artefatti possono essere fondamentali per le indagini.

Dal punto di vista anti-forense, l'assenza di voci ShellBag può suggerire la pulizia del sistema e una particolare conoscenza informatica da parte dell'utente analizzato.⁴

Shimcache

Windows Shimcache, noto anche come AppCompatCache, è stato creato da Microsoft a partire da Windows XP ed è utilizzato dal sistema operativo Windows per identificare i problemi di compatibilità delle applicazioni.

Gli Shimcache, e nello specifico i loro indicatori, possono essere usati dagli investigatori forensi per eseguire comparazioni con altre origini dati, come il file AmCache.hve e i file di prefetch.

Shimcache memorizza vari metadati di file in base al sistema operativo, ad esempio:

- Percorso completo del file
- Dimensione del file
- Standard_Information (SI) con l'ora dell'ultima modifica
- Ora dell'ultimo aggiornamento di Shimcache
- Flag di esecuzione del processo

Shimcache non conserva tutti i dati che salva nel corso del tempo ma esegue il “roll” dei dati, cioè sostituisce i dati più vecchi con i dati più recenti. In base al sistema operativo varia la quantità di dati conservati.

<https://www.magnetforensics.com/blog/forensic-analysis-of-windows-shellbags/>

<https://www.dfir.training/windows/amcache/207-lifars-amcache-and-shimcache-forensics/file>

A partire da Windows Vista, Microsoft incorporato nello Shimcache la categoria "Flag di esecuzione del processo" per ogni voce memorizzata.

L'informatico forense è facilitato dal flag di esecuzione del processo, ove presente, rende più facile per l'investigatore determinare se una voce è stata eseguita o meno o se questa voce è stata aggiunta a seguito di un'attività diversa dall'esecuzione del file, come la navigazione interattiva di una directory. Queste voci possono essere facilmente individuate osservando se il Flag di esecuzione del processo è contrassegnato come FALSO.

Dalla lettura del white paper di Andrew Davis " *Sfruttare la cache di compatibilità delle applicazioni nelle indagini forensi* ", sappiamo ogni volta che viene eseguita un'applicazione con metadati univoci, verrà creata una voce Shimcache corrispondente. In altre parole, le nuove voci vengono create quando i metadati di un file esistente vengono modificati e rieseguiti.

Il valore di Shimcache per gli investigatori può essere problematico se non analizzato attentamente. È importante riconoscere che questa risorsa è alquanto volatile e dovrebbe essere preservata non appena le indagini lo consentiranno.

In una situazione ideale, Shimcache di un sistema è in grado di fornire ottime prove a sostegno del collegamento con reperti del file system, Registro di sistema, log degli eventi, e il traffico di rete. ⁵

Appcache

Application Cache (AppCache) consente l'esecuzione offline delle applicazioni basate sul Web. Gli sviluppatori possono specificare le risorse per la cache del browser, rendendole disponibili per l'applicazione anche se non è possibile stabilire una connessione al server. Queste risorse si caricano e funzionano correttamente anche se gli utenti fanno clic sul pulsante Aggiorna quando sono offline.⁶

I browser Web conservano le informazioni relative ai siti visitati, ai download, alla cronologia delle ricerche, ai cookie e alle informazioni sulla

https://www.fireeye.com/blog/threat-research/2015/06/caching_out_the_val.html

<https://www.html5rocks.com/en/tutorials/appcache/beginner/>

cache in una posizione predefinita nella macchina del sospettato. Esistono molti browser disponibili in IT World. I principali sono Internet Explorer, Google Chrome e Mozilla Firefox. Essendo Google Chrome uno dei browser web più popolari, è importante analizzare i file del browser lasciati da questo browser al momento dell'indagine di informatica informatica.

Prendiamo ad esempio il browser Google Chrome.

Un computer Windows memorizza i file del browser creati da Google Chrome in "OS Drive: \\ Users \ Username \ AppData \ local \ Google \ Chrome \ UserData \ Default \". Oltre a questo percorso profilo predefinito, potrebbero esserci altre cartelle in "... Google \ Chrome \ UserData \\" corrispondenti a ciascun profilo aggiuntivo creato dall'utente. Le pagine e le immagini memorizzate nella cache a cui un utente accede tramite il browser Web Google Chrome sono archiviate in una cartella denominata "Cache" presente all'interno di questi percorsi del profilo. Google Chrome salva i dettagli forensi del browser in diversi file come segnalibri, cookie, sessione corrente, schede correnti, cronologia, ultima sessione, ultime schede, predittore di azioni di rete, preferenze, collegamenti visitati e siti principali. Queste informazioni sono archiviate in file separati creati nei percorsi del profilo.

La memorizzazione nella cache è il processo di creazione di un archivio temporaneo per i contenuti a cui si accede frequentemente in siti Web visitati come html, immagini, script java ecc.

Questo archivio temporaneo consente di evitare il ri-download di oggetti in siti Web visualizzati in precedenza. Di solito la cartella cache contiene almeno cinque file, un file indice e quattro file di dati. Il file indice contiene indirizzi che puntano a un file di dati con elementi memorizzati nella cache. I file di dati che memorizzano i dati memorizzati nella cache sono denominati come data_0, data_1, data_2 e data_3. I file di dati possono anche essere chiamati come file di blocco poiché i dati memorizzati nella cache sono allocati in blocchi di dimensioni fisse. La dimensione massima del blocco allocato per il file di dati è 16 Kb e se la dimensione del contenuto supera, Chrome lo salva in un file esterno. Il nome del file esterno inizia con "f_". Il file indice ha tre parti, un'intestazione, i dati dell'ultimo utilizzo (LRU) e una tabella hash. La dimensione dell'intestazione è di 256 byte e la dimensione dei dati LRU è di 112 byte. La dimensione della tabella hash è menzionata nella variabile membro "size table" presente nell'intestazione. I

dati LRU vengono utilizzati per lo sfratto [6] che aiuta il browser a eliminare le vecchie voci quando lo spazio disponibile per l'archiviazione della cache è pieno. La tabella hash è un bucket contenente indirizzi cache, che punta ai dati effettivi memorizzati nella cache all'interno dei file di dati. Un esempio di file di indice è mostrato in Fig.2. I file di dati o i file di blocco memorizzano le informazioni come blocchi con dimensioni predefinite. Se la dimensione delle informazioni della cache è inferiore a 16 KB, le informazioni vengono salvate in uno dei file di dati in base alla dimensione del blocco. Le dimensioni dei dati predefinite dei file sono mostrate nella Tabella III. Se la dimensione è superiore a 16 KB, verrà memorizzata come file separato. In questo caso, tutti i dati che devono essere memorizzati nella cache vengono memorizzati come file con un nome `f_#####`, dove # è il numero esadecimale che identifica il file come `f_000001`, `f_000002` ecc.

Informazioni forensi rilevanti riguardanti il profilo di navigazione web dell'utente possono essere ottenute analizzando questi file⁷

Prefetch

I file di prefetch sono ottimi manufatti per investigatori forensi che cercano di analizzare le applicazioni che sono state eseguite su un sistema. Windows crea un file di prefetch quando un'applicazione viene eseguita da una posizione particolare per la prima volta. Questo è usato per velocizzare il caricamento delle applicazioni. Per gli investigatori, questi file contengono alcuni dati preziosi sulla cronologia delle applicazioni di un utente su un computer.

La prova dell'esecuzione del programma può essere una risorsa preziosa per gli investigatori forensi. Possono provare che un sospetto ha avviato un programma come CCleaner per coprire eventuali potenziali illeciti. Se da allora il programma è stato cancellato, potrebbe ancora esistere un file di prefetch sul sistema per fornire prove dell'esecuzione. Un altro uso prezioso dei file di prefetch è nelle indagini sui malware che possono aiutare gli esaminatori a determinare quando è stato eseguito un programma dannoso. Combinando questo con alcune analisi di base della sequenza temporale, gli investigatori possono identificare eventuali file dannosi aggiuntivi che

<https://sci-hub.tw/10.1109/ICCIC.2017.8524272>

sono stati scaricati o creati sul sistema e aiutano a determinare la causa principale di un incidente.

I file di prefetch sono tutti denominati in un formato comune in cui è elencato il nome dell'applicazione, quindi un hash di otto caratteri del percorso in cui è stata eseguita l'applicazione, seguito dall'estensione .PF. Ad esempio, il file di prefetch per calc.exe verrà visualizzato come CALC.EXE-oFE8F3A9.pf, dove oFE8F3A9 è un hash del percorso da cui è stato eseguito il file. Questi file sono tutti memorizzati nella cartella ROOT / Windows / Prefetch.

Il calcolo del percorso originale dell'applicazione dall'hash fornito nel file di prefetch è relativamente semplice, ma può richiedere molto tempo. A seconda della versione di Windows da cui è stato estratto il file, viene utilizzata una diversa funzione di hashing.

L'analisi dei file di prefetch è relativamente semplice. Oltre al nome e al percorso menzionati in precedenza, i file di prefetch contengono dettagli sul numero di volte in cui l'applicazione è stata eseguita, dettagli sul volume, nonché informazioni di data e ora in cui la prima e l'ultima applicazione sono state eseguite. Per Windows 8 e versioni successive, i file di prefetch ora contengono fino a otto timestamp per l'ultima esecuzione di un'applicazione, offrendo agli investigatori diversi timestamp aggiuntivi per aiutare a costruire una sequenza temporale di eventi su un sistema.⁸

Superfetch

SuperFetch è stato sul radar forense sin dalle versioni di anteprima di Windows Vista. È l'aggiornamento dei Prefetch ma promette di ottimizzare in modo proattivo la memoria dell'applicazione in termini di tempo e scenari di utilizzo. È importante notare che non sostituisce il servizio Prefetch. Microsoft ha scelto di continuare a utilizzarlo in Windows 8.1 e Windows 10.

SuperFetch è costituito da una serie di file di database "Ag *.db" situati nella cartella % SystemRoot% \ Prefetch. È estremamente complesso con una varietà di diversi formati di intestazione per diversi database, versioni e

<https://www.magnetforensics.com/blog/forensic-analysis-of-prefetch-files-in-windows/>

architetture (x86 e x64) dei sistemi operativi Microsoft. Sui sistemi con unità SSD, potrebbe essere disattivato per impostazione predefinita (simile a Prefetch). Ci sono ancora molte lacune nella conoscenza dei SuperFetch.

SuperFetch tiene traccia degli "scenari di prestazione" ed è specificamente progettato per anticipare le applicazioni eseguite di frequente dopo l'attività del sistema come modalità standby, ibernazione e cambio rapido utente. Registra il set di pagine di memoria utilizzate per un lungo periodo di tempo, consentendo di modellare il comportamento degli utenti e prendere decisioni migliori su quando precaricare i dati delle applicazioni in memoria. Sono questi i database, che registrano ciò che è stato caricato in passato, da cui si possono ricavare le seguenti informazioni:

- Nomi eseguibili dell'applicazione
- Conteggio dell'esecuzione
- Conteggio in primo piano
- File di supporto (include i percorsi completi di una vasta gamma di file mappati in memoria, tra cui DLL, file zip, documenti, file di database e file e cartelle presenti su supporti rimovibili, Cestino, cartelle temporanee e Volume Shadow Copie e volumi crittografati)
- Volumi accessibili (esempio: HardDiskVolume)
- Informazioni sul percorso completo che forniscono dati su cartelle presenti su vari volumi di accesso da parte del sistema
- Tempi di attività dell'applicazione
- Data / ora (dal database AgAppLaunch - scopo sconosciuto ma sembra non essere collegato in modo affidabile al tempo di esecuzione nei test)

Mentre le informazioni sui tempi memorizzati da SuperFetch devono ancora essere verificate per la sua affidabilità, presumibilmente potrebbero aiutare a identificare l'attività delle applicazioni che si verificano in momenti strani. Per esempio: è normale vedere l'applicazione del database aziendale accessibile durante il fine settimana?⁹

<https://digital-forensics.sans.org/blog/2015/01/28/whats-new-in-windows-application-execution>

Analisi tools

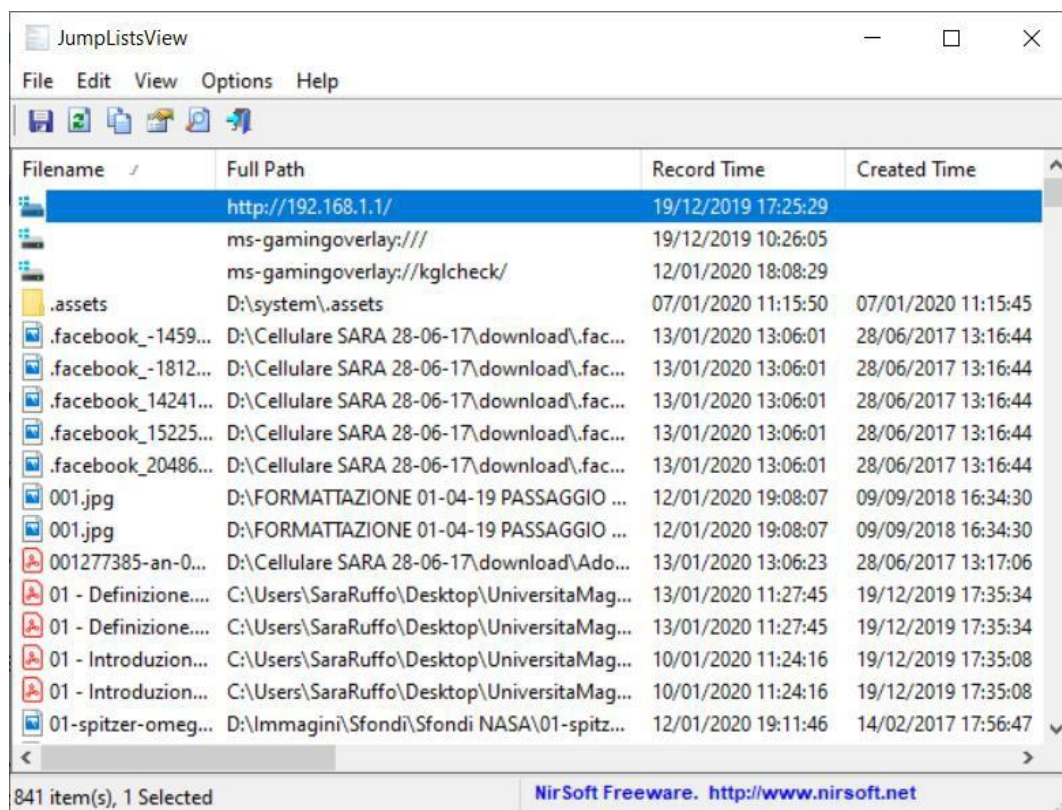
Verranno ora analizzati i tool selezionati e usati nel software.

JumpListView v1.16

Descrizione

JumpListView è un semplice strumento che visualizza le informazioni memorizzate dalla funzione 'Jump Lists' di Windows 7 e Windows 8. Per ogni record trovato nei Jump List, vengono visualizzate le seguenti informazioni: Il nome file che l'utente ha aperto, la data / ora dell'evento di apertura del file, l'ID dell'applicazione utilizzata per aprire il file, la dimensione / il tempo / gli attributi del file nel momento in cui il file è stato aperto e altro ancora ...

Puoi anche esportare i record Jump Jump list nel file CSV / xml / html.



Requisiti di sistema

Questa utility funziona su Windows 7, Windows 8 e Windows 10. Sono supportati sia sistemi a 32 che a 64 bit. Nella versione precedente di Windows, la funzione 'Jump Lists' non esiste, e quindi JumpListView non visualizzerà alcun dato, ma ... Puoi ancora leggere i dati dal disco rigido

esterno contenente l'installazione di Windows 7/8 usando la finestra "Opzioni avanzate".

Le informazioni delle jump list sono archiviate nelle seguenti cartelle:

C: \ Users \ [Profilo utente] \ AppData \ Roaming \ Microsoft \ Windows \ Recenti \ AutomaticDestinations

C: \ Users \ [Profilo utente] \ AppData \ Roaming \ Microsoft \ Windows \ recenti \ CustomDestinations

Attualmente JumpListView legge solo le informazioni dalla cartella AutomaticDestinations.

JumpListView Columns

- Nome file e percorso completo: il nome file che probabilmente l'utente ha aperto.
- Ora record: specifica la data / ora in cui l'utente ha probabilmente aperto il nome file specificato.
- Ora di creazione, Ora modificata, Ora di accesso, Attributi del file e Dimensione del file: specifica la data / ora, gli attributi e la dimensione del file, come registrato nel momento in cui l'utente ha aperto il file. Tenere presente che l'ora / la dimensione / gli attributi correnti del file potrebbero essere diversi. Inoltre, per alcuni dei record, queste informazioni su tempo / dimensioni / attributi non sono disponibili.
- ID voce: l'ID interno del record.
- ID applicazione: specifica l'ID delle applicazioni utilizzate per aprire il nome file specificato. Significa che se vedi 2 record con lo stesso ID applicazione, entrambi i file sono stati aperti dalla stessa applicazione.

Attualmente JumpListView non è in grado di rilevare l'applicazione, ma è possibile trovare alcuni ID di applicazione comuni su Internet.

Questa utility è rilasciata come freeware.¹⁰

https://www.nirsoft.net/utils/jump_lists_view.html

USBDeview v2.85

Descrizione

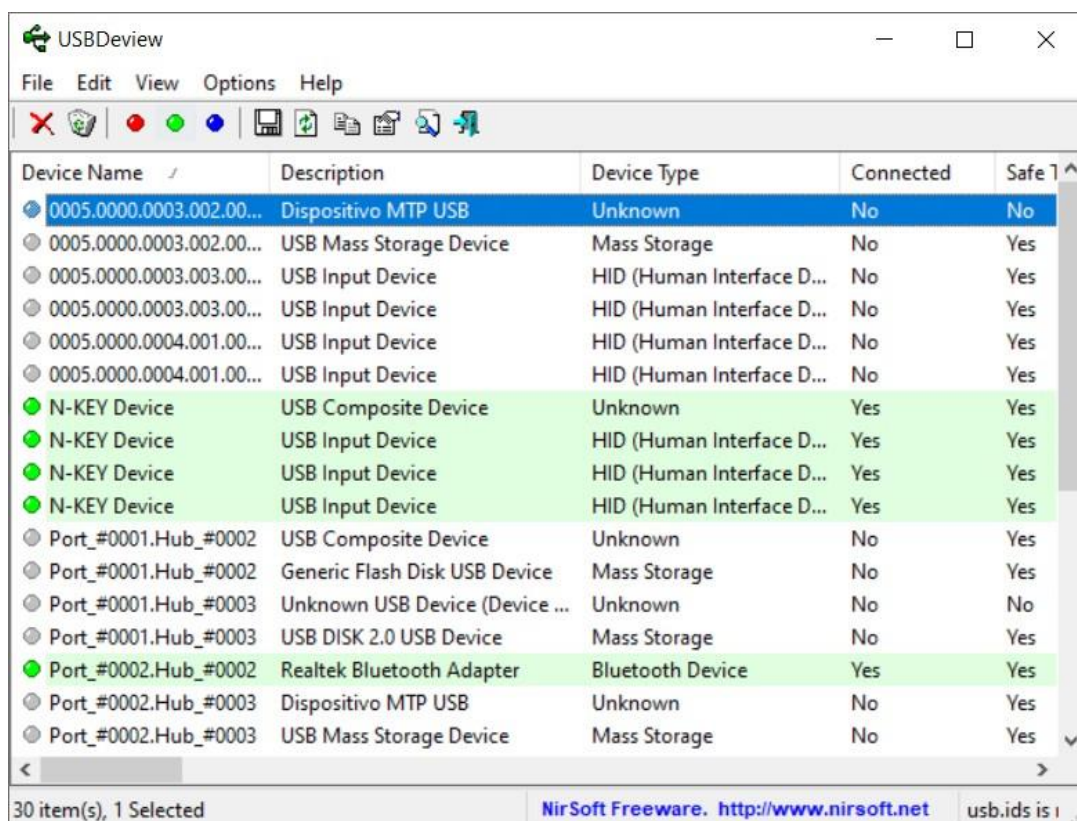
USBDeview è una piccola utility che elenca tutti i dispositivi USB che sono attualmente collegati al computer, nonché tutti i dispositivi USB utilizzati in precedenza.

Per ogni dispositivo USB, vengono visualizzate informazioni estese: Nome / descrizione dispositivo, tipo di dispositivo, numero di serie (per dispositivi di archiviazione di massa), la data / ora in cui è stato aggiunto il dispositivo, VendorID, ProductID e altro.

USBDeview consente anche di disinstallare i dispositivi USB utilizzati in precedenza, scollegare i dispositivi USB attualmente collegati al computer, nonché per disabilitare e abilitare i dispositivi USB.

È inoltre possibile utilizzare USBDeview su un computer remoto, purché si acceda a quel computer con l'utente amministratore.

Puoi anche esportare i recordlist nel file CSV / xml / html.



The screenshot shows the USBDeview application window. It has a menu bar (File, Edit, View, Options, Help) and a toolbar with various icons. Below the toolbar is a table listing USB devices. The table has five columns: Device Name, Description, Device Type, Connected, and Safe to Remove. The first row is selected, showing a device with ID 0005.0000.0003.002.00... described as 'Dispositivo MTP USB'. Other rows include various USB Mass Storage Devices, HID (Human Interface Devices), and a Realtek Bluetooth Adapter. The status bar at the bottom indicates '30 item(s), 1 Selected' and provides the NirSoft Freeware website URL.

Device Name	Description	Device Type	Connected	Safe to Remove
0005.0000.0003.002.00...	Dispositivo MTP USB	Unknown	No	No
0005.0000.0003.002.00...	USB Mass Storage Device	Mass Storage	No	Yes
0005.0000.0003.003.00...	USB Input Device	HID (Human Interface D...	No	Yes
0005.0000.0003.003.00...	USB Input Device	HID (Human Interface D...	No	Yes
0005.0000.0004.001.00...	USB Input Device	HID (Human Interface D...	No	Yes
0005.0000.0004.001.00...	USB Input Device	HID (Human Interface D...	No	Yes
N-KEY Device	USB Composite Device	Unknown	Yes	Yes
N-KEY Device	USB Input Device	HID (Human Interface D...	Yes	Yes
N-KEY Device	USB Input Device	HID (Human Interface D...	Yes	Yes
N-KEY Device	USB Input Device	HID (Human Interface D...	Yes	Yes
Port_#0001.Hub_#0002	USB Composite Device	Unknown	No	Yes
Port_#0001.Hub_#0002	Generic Flash Disk USB Device	Mass Storage	No	Yes
Port_#0001.Hub_#0003	Unknown USB Device (Device ...	Unknown	No	No
Port_#0001.Hub_#0003	USB DISK 2.0 USB Device	Mass Storage	No	Yes
Port_#0002.Hub_#0002	Realtek Bluetooth Adapter	Bluetooth Device	Yes	Yes
Port_#0002.Hub_#0003	Dispositivo MTP USB	Unknown	No	Yes
Port_#0002.Hub_#0003	USB Mass Storage Device	Mass Storage	No	Yes

Requisiti di sistema

Questa utility funziona su Windows 2000, Windows XP, Windows 2003, Windows Vista, Windows Server 2008, Windows 7, Windows 8 e Windows

10. Sono supportati sia i sistemi a 32 bit che a 64 bit. Windows 98 / ME non è supportato.

Problemi noti

- Per disabilitare / abilitare gli elementi USB su sistemi x64, è necessario utilizzare anche la versione x64 di USBDeview.
- La colonna "Data di creazione" non visualizza i valori corretti su Windows 7/8 / Vista / 2008.
- Alcuni dispositivi USB con driver non valido potrebbero causare il blocco di USBDeview. Per aggirare questo problema, è necessario disattivare l'opzione "Recupera alimentazione USB / Informazioni sulla versione":
USBDeview.exe / RetrieveUSBPower o

USBDeview Columns

- **Nome dispositivo:** specifica il nome del dispositivo. Per alcuni dispositivi, questa colonna può visualizzare un nome senza significato, ad esempio "Dispositivo USB". Se il nome del dispositivo non ha significato, prova a guardare la colonna Descrizione.
- **Descrizione del dispositivo:** la descrizione del dispositivo.
- **Tipo di dispositivo:** il tipo di dispositivo, in base al codice di classe USB.
- **Connesso:** specifica se il dispositivo è attualmente collegato al computer. Se il dispositivo è collegato, è possibile utilizzare l'opzione "Disconnect Selected Devices" (F9) per disconnettere il dispositivo.
- **Sicuro da scollegare:** specifica se è sicuro scollegare il dispositivo dalla presa USB senza prima disconnetterlo. Se il valore di questa colonna è falso e si desidera scollegare il dispositivo, è necessario innanzitutto disconnettere il dispositivo utilizzando l'opzione "Disconnect Selected Devices" (F9) dell'utilità USBDeview o utilizzando l'utilità "Unplug or Eject Hardware" del sistema operativo Windows.
- **Lettera di unità:** specifica la lettera di unità del dispositivo USB. Questa colonna è rilevante solo per i dispositivi di memoria

flash USB e per le unità CD / DVD USB. Tenere presente che USBDeview non è in grado di rilevare le lettere di unità dei dischi rigidi USB.

- **Numero di serie:** specifica il numero di serie del dispositivo. Questa colonna è rilevante solo per i dispositivi di archiviazione di massa (dispositivi di memoria flash, unità CD / DVD e dischi rigidi USB).
- **Data di creazione:** specifica la data / ora di installazione del dispositivo. Nella maggior parte dei casi, questo valore di data / ora rappresenta l'ora in cui è stato collegato per la prima volta il dispositivo alla porta USB. Tuttavia, tenere presente che in alcune circostanze questo valore potrebbe essere errato. Inoltre, su Windows 7, questo valore viene inizializzato con la data / ora corrente ad ogni riavvio.
- **Data ultima connessione / disconnessione:** specifica l'ultima volta che è stato collegato / scollegato il dispositivo. Questo valore di data viene perso quando si riavvia il computer.
- **VendorID / ProductID:** specifica VendorID e ProductID del dispositivo.
- **Classe / sottoclasse / protocollo USB:** specifica la classe / sottoclasse / protocollo del dispositivo in base alle specifiche USB.
- **Hub / Porta:** specifica il numero di hub e il numero di porta a cui è stato collegato il dispositivo. Questo valore è vuoto per i dispositivi di archiviazione di massa.

Questa utility è rilasciata come freeware.¹¹

BrowsingHistoryView v2.35

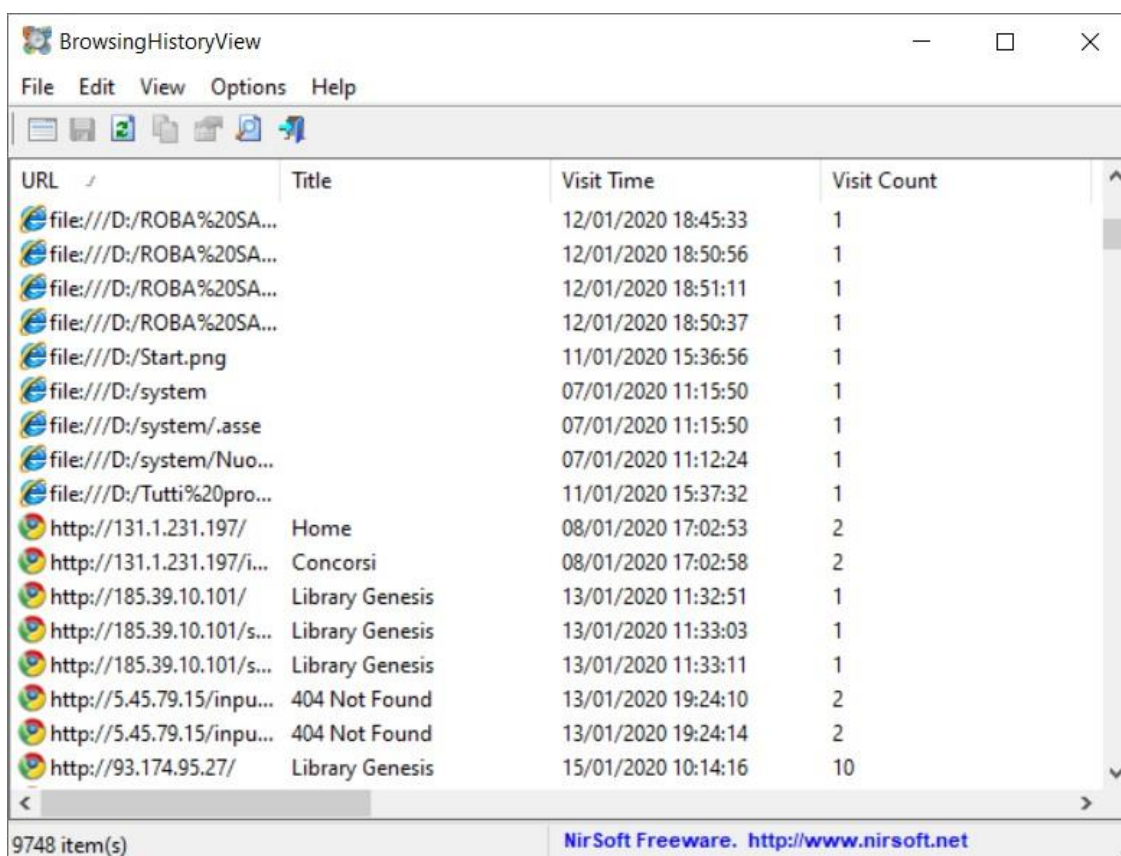
Descrizione

BrowsingHistoryView è un'utilità che legge i dati della cronologia di 4 diversi browser Web (Internet Explorer, Mozilla Firefox, Google Chrome e Safari) e visualizza la cronologia di navigazione di tutti questi browser Web in una tabella.

https://www.nirsoft.net/utils/usb_devices_view.html

La tabella della cronologia di navigazione include le seguenti informazioni: URL visitato, Titolo, Tempo di visita, Conteggio visite, Browser Web e Profilo utente. BrowsingHistoryView consente di visualizzare la cronologia di navigazione di tutti i profili utente in un sistema in esecuzione, nonché di ottenere la cronologia di navigazione da un disco rigido esterno.

Puoi anche esportare la cronologia di navigazione nel file csv / html / xml dall'interfaccia utente o dalla riga di comando, senza visualizzare alcuna interfaccia utente.



The screenshot shows the BrowsingHistoryView application window. It has a menu bar (File, Edit, View, Options, Help) and a toolbar with icons for file operations. The main area displays a table of browsing history items. The table has four columns: URL, Title, Visit Time, and Visit Count. The data is sorted by Visit Time in descending order. The bottom status bar shows '9748 item(s)' and the NirSoft Freeware logo with the website URL.

URL	Title	Visit Time	Visit Count
file:///D:/ROBA%20SA...		12/01/2020 18:45:33	1
file:///D:/ROBA%20SA...		12/01/2020 18:50:56	1
file:///D:/ROBA%20SA...		12/01/2020 18:51:11	1
file:///D:/ROBA%20SA...		12/01/2020 18:50:37	1
file:///D:/Start.png		11/01/2020 15:36:56	1
file:///D:/system		07/01/2020 11:15:50	1
file:///D:/system/.asse		07/01/2020 11:15:50	1
file:///D:/system/Nuo...		07/01/2020 11:12:24	1
file:///D:/Tutti%20pro...		11/01/2020 15:37:32	1
http://131.1.231.197/	Home	08/01/2020 17:02:53	2
http://131.1.231.197/i...	Concorsi	08/01/2020 17:02:58	2
http://185.39.10.101/	Library Genesis	13/01/2020 11:32:51	1
http://185.39.10.101/s...	Library Genesis	13/01/2020 11:33:03	1
http://185.39.10.101/s...	Library Genesis	13/01/2020 11:33:11	1
http://5.45.79.15/inpu...	404 Not Found	13/01/2020 19:24:10	2
http://5.45.79.15/inpu...	404 Not Found	13/01/2020 19:24:14	2
http://93.174.95.27/	Library Genesis	15/01/2020 10:14:16	10

Requisiti di sistema

Questa utility funziona su qualsiasi versione di Windows, a partire da Windows 2000 fino a Windows 10. Sono supportati sia sistemi a 32 bit che x64.

Sono supportati i seguenti browser Web:

- Internet Explorer (versione 4.00 e successive)
- Mozilla Firefox (versione 3.00 e successive)
- Microsoft Edge

- Google Chrome
- Safari
- Opera (versione 15 o successiva, basata sul browser Web Chrome)

Problemi noti

- "Conteggio visite" sul browser Web Internet Explorer: la colonna "Conteggio visite" viene presa "così com'è" dal file cronologico di Internet Explorer. Sfortunatamente, Internet Explorer tende a gonfiare eccessivamente il numero di "Visit Count", il che significa che non si può presumere che il numero di "Visit Count" rappresenti il numero effettivo di volte in cui l'utente ha visitato il sito Web specificato. Questa osservazione è rilevante solo per Internet Explorer.
- Limitazioni e problemi con la lettura della cronologia di IE10, IE11 e Microsoft Edge: le versioni 10 e 11 di Internet Explorer memorizzano i dati della cronologia all'interno di WebCacheV01.dat e questo file viene bloccato dal sistema operativo la maggior parte delle volte, anche quando IE è chiuso.
Per sbloccare il file del database della cronologia, è necessario attivare l'opzione "Arresta automaticamente l'attività cache di IE10 / IE11 / Edge". Se si utilizza l'opzione "Carica cronologia da computer remoto" - BrowsingHistoryView interromperà l'attività cache di IE10 / IE11 / Edge sul sistema remoto specificato, in modo da poter vedere la cronologia di IE10 / IE11 / Edge da remoto.

Opzioni Avanzate

Le opzioni avanzate consentono di:

- **Filtrare per data / ora visita:** consente di caricare la cronologia dall'ultimo numero di giorni / ore o da un intervallo di data / ora specifico.

- **Browser Web:** BrowsingHistoryView caricherà la cronologia solo dai browser Web selezionati. Ad esempio, se si desidera ottenere solo la cronologia di navigazione di Internet Explorer, è necessario selezionare la casella di controllo "Internet Explorer" e deselezionare tutti gli altri.
- **Caricare la cronologia da:** consente di scegliere l'origine dati della cronologia di navigazione:
 - **Caricare la cronologia dal sistema corrente (Tutti gli utenti):** se si sceglie questa opzione, BrowsingHistoryView esegue la scansione di tutti i profili utente sul sistema (C: \ Documents and Settings o C: \ Users) e carica i dati della cronologia da essi.
 - **Caricare la cronologia dal sistema in esecuzione corrente (solo utente corrente):** se si sceglie questa opzione, BrowsingHistoryView carica solo la cronologia di navigazione dell'utente attualmente connesso.
 - **Caricare la cronologia dalla cartella dei profili specificata:** se si sceglie questa opzione, BrowsingHistoryView esegue la scansione di tutti i profili utente nella cartella specificata.
 - **Caricare la cronologia da profilo specificato:** se si sceglie questa opzione, BrowsingHistoryView carica la cronologia dalla cartella del profilo specificato.
 - **Caricare la cronologia dalle cartelle personalizzate specificate:** se si sceglie questa opzione, è necessario specificare le cartelle.
 - **Caricare la cronologia da file della cronologia specificati:** se scegli questa opzione, si deve specificare il file della cronologia di ogni browser Web che si desidera caricare.
 - **Caricare la cronologia da computer remoto:** consente di caricare la cronologia di navigazione dal computer remoto sulla rete. Bisogna tenere presente che questa opzione funziona solo quando si dispone dell'accesso di amministratore completo al computer remoto.

Lettura Cronologia precedente

Se il disco rigido ha una o più copie shadow, si può visualizzare la cronologia memorizzata all'interno di queste copie shadow selezionando l'opzione "Carica cronologia dalla cartella dei profili specificati" nella finestra "Opzioni avanzate" e quindi scegliendo il percorso desiderato per la copia shadow.

All'interno delle copie shadow è possibile trovare elementi della cronologia precedenti che non esistono nel sistema corrente, nonché elementi della cronologia che sono stati eliminati.

La funzione copie shadow funziona solo a partire da Windows Vista.

Questa utility è rilasciata come freeware.¹²

ShellBags Explorer 1.3.3.0

Descrizione

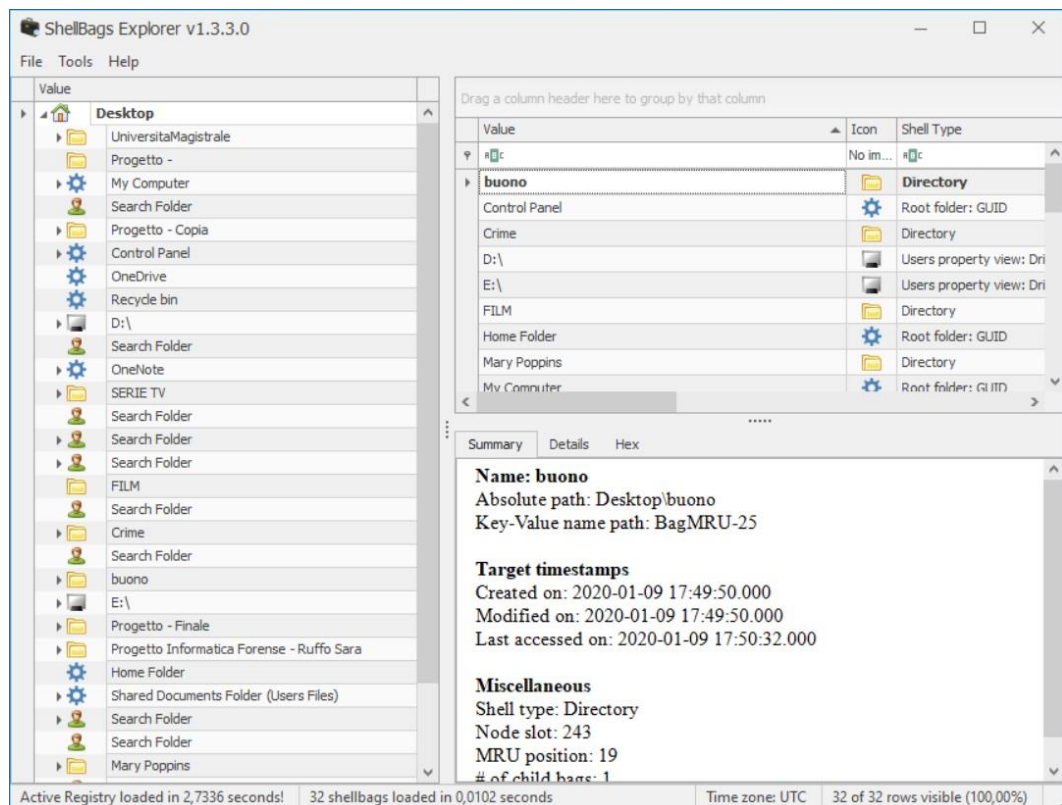
ShellBags Explorer include il supporto per tutti i blocchi di estensione noti e rilevamento automatico di blocchi sconosciuti, tipi di ShellBag sconosciuti, ecc.

- Interpreta i dati in vista esadecimale. Quando vengono selezionati valori esadecimali, i valori si aggiornano dalla posizione del cursore.
- Supporta per NTUser.dat e USRClass.dat
- Visualizza coerentemente dei dati per i sacchetti
- Ha la possibilità di visualizzare tutti i sacchetti in modo ricorsivo per ordinare, filtrare, ecc.
- Quando si utilizza lo strumento da riga di comando, la possibilità di ingerire più hive del Registro di sistema e rimuovere duplicati ShellBags. Ciò consente una visione completa dell'accesso alla directory che abbraccia la gamma di dati in tutti gli hive del Registro di sistema.
- Ha la possibilità di mostrare a quali directory è stato effettuato l'accesso su supporti CD e DVD (e quindi mostrare quali lettere di unità erano dispositivi ottici)

https://www.nirsoft.net/utils/browsing_history_view.htm

SBE è stato progettato con caratteristiche e capacità come il rilevamento GUID sconosciuto, i disallineamenti dei blocchi di estensione, ecc. Ed è stato utilizzato per fornire informazioni significative, precedentemente sconosciute, alle specifiche del formato per gli elementi della shell. Segnalando automaticamente anomalie nel processo di decodifica, queste anomalie possono essere segnalate allo sviluppatore del programma per migliorare le capacità di SBE e quindi il processo forense in cui SBE viene utilizzato.

Puoi anche esportare i dati in un file CSV / xml / html.



Requisiti di Sistema

ShellBags Explorer richiede l'installazione di Microsoft .net framework versione 4.6 full runtime o successiva.

Vista ad albero

La vista ad albero mostra un Windows Explorer come rappresentazione dei dati ShellBag. Ci sono menu in Strumenti per espandere e contrarre automaticamente tutti i nodi.

Time zone support

Come la sua controparte GUI, SBECmd può adattare tutte le date e gli orari al fuso orario selezionato dall'utente. Il fuso orario predefinito è UTC, ma è possibile selezionare un fuso orario diverso.

Il programma è stato sviluppato da Eric Zimmerman.¹³

AppCompatCacheParser 1.4.3.1

Descrizione

Il programma serve per analizzare gli Shimcache

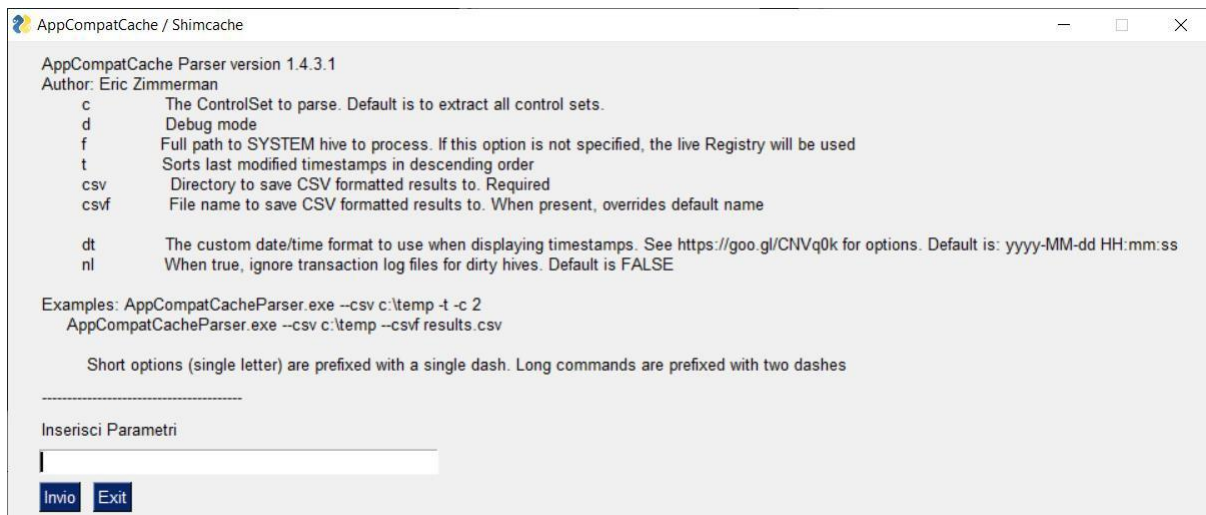
Il programma è privo di interfaccia grafica e funziona da riga di comando. I comandi sono i seguenti.

- **c** Il ControlSet da analizzare. L'impostazione predefinita è estrarre tutti i set di controllo.
- **d** Modalità debug
- **f** Percorso completo verso l'hive SYSTEM da elaborare. Se questa opzione non viene specificata, verrà utilizzato il registro live
- **t** Ordina gli ultimi timestamp modificati in ordine decrescente
- **csvf** Nome del file in cui salvare i risultati in formato CSV. Se presente, sostituisce il nome predefinito
- **dt** Il formato personalizzato di data / ora da utilizzare quando si visualizzano i timestamp.
- **nl** Se vero, ignora i file di registro delle transazioni per hive sporchi. L'impostazione predefinita è FALSA

Un'opzione richiesta è **-s**, per far sì che il programma sappia dove salvare le cose. Se si omette l'opzione **-h**, viene scaricato il registro live.

Tutti gli orari sono UTC.

<https://ericzimmerman.github.io/#!index.md>



Requisiti di sistema

AppCompatCache (shimcache) parser. Supporta Windows 7 (x86 and x64), Windows 8.x, and Windows 10

Il programma è stato sviluppato da Eric Zimmerman.¹⁴

ChromeCacheView v2.00

Descrizione

ChromeCacheView è una piccola utility che legge la cartella cache del browser Web Google Chrome e visualizza l'elenco di tutti i file attualmente memorizzati nella cache. Per ogni file di cache, vengono visualizzate le seguenti informazioni: URL, Tipo di contenuto, Dimensione del file, Ora dell'ultimo accesso, Ora di scadenza, Nome del server, Risposta del server.

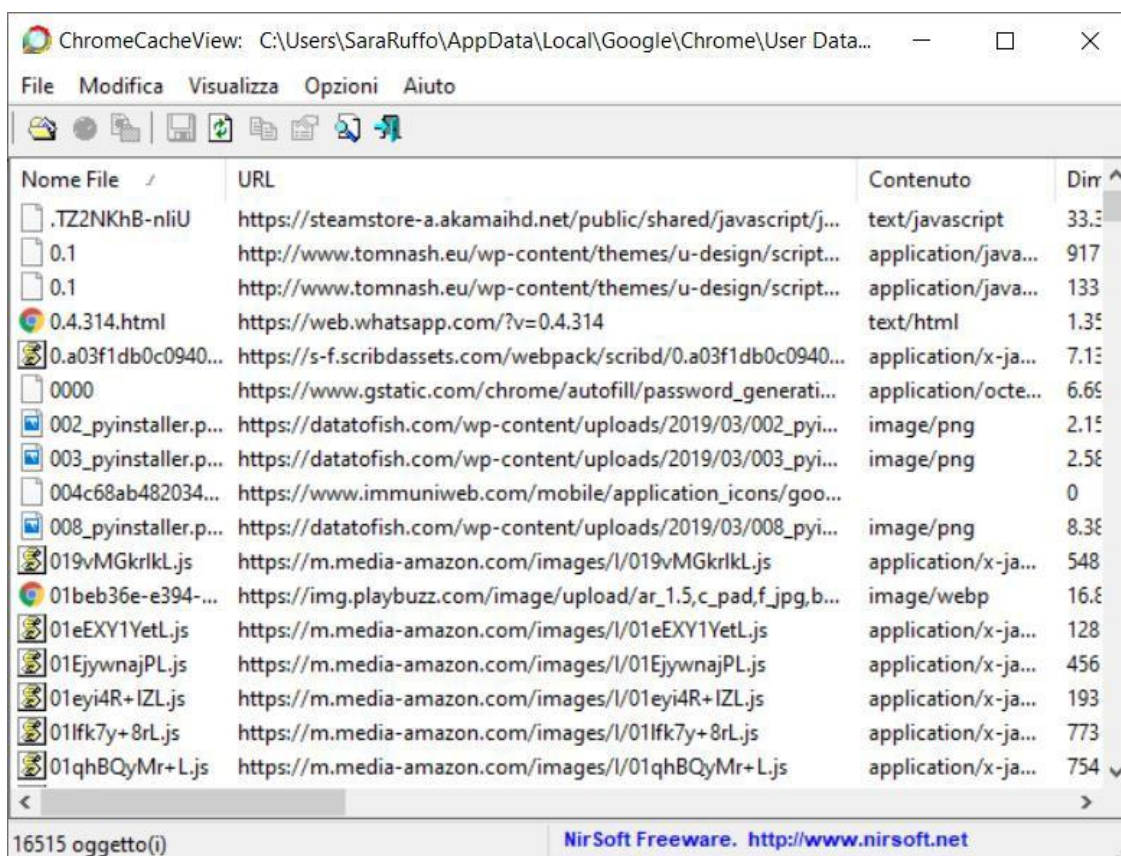
È possibile selezionare facilmente uno o più elementi dall'elenco cache, quindi estrarre i file in un'altra cartella o copiare l'elenco degli URL negli Appunti.

Nella finestra principale viene visualizzato l'elenco dei file attualmente memorizzati nella cache dell'utente predefinito di Google Chrome.

È possibile selezionare uno o più file cache dall'elenco, quindi esportare l'elenco in file di testo / html / xml / csv (opzione 'Salva elementi selezionati'), copiare l'elenco URL negli appunti (Ctrl + U), copiare l'intera tabella dei file di cache (Ctrl + C), quindi incollarlo in Excel o nel foglio di

<https://ericzimmerman.github.io/#!index.md>

calcolo di OpenOffice. Si può anche estrarre i file effettivi dalla cache e salvarli in un'altra cartella.



Requisiti di sistema

Questa utility funziona su qualsiasi versione di Windows, a partire da Windows 2000 fino a Windows 7/8/2008/10

Questa utility è rilasciata come freeware.¹⁵

WinPrefetchView v1.35

Descrizione

Ogni volta che si esegue un'applicazione nel sistema, un sistema di prefetch che contiene informazioni sui file caricati dall'applicazione viene creato dal sistema operativo Windows. Le informazioni nel file Prefetch vengono utilizzate per ottimizzare il tempo di caricamento dell'applicazione al successivo avvio.

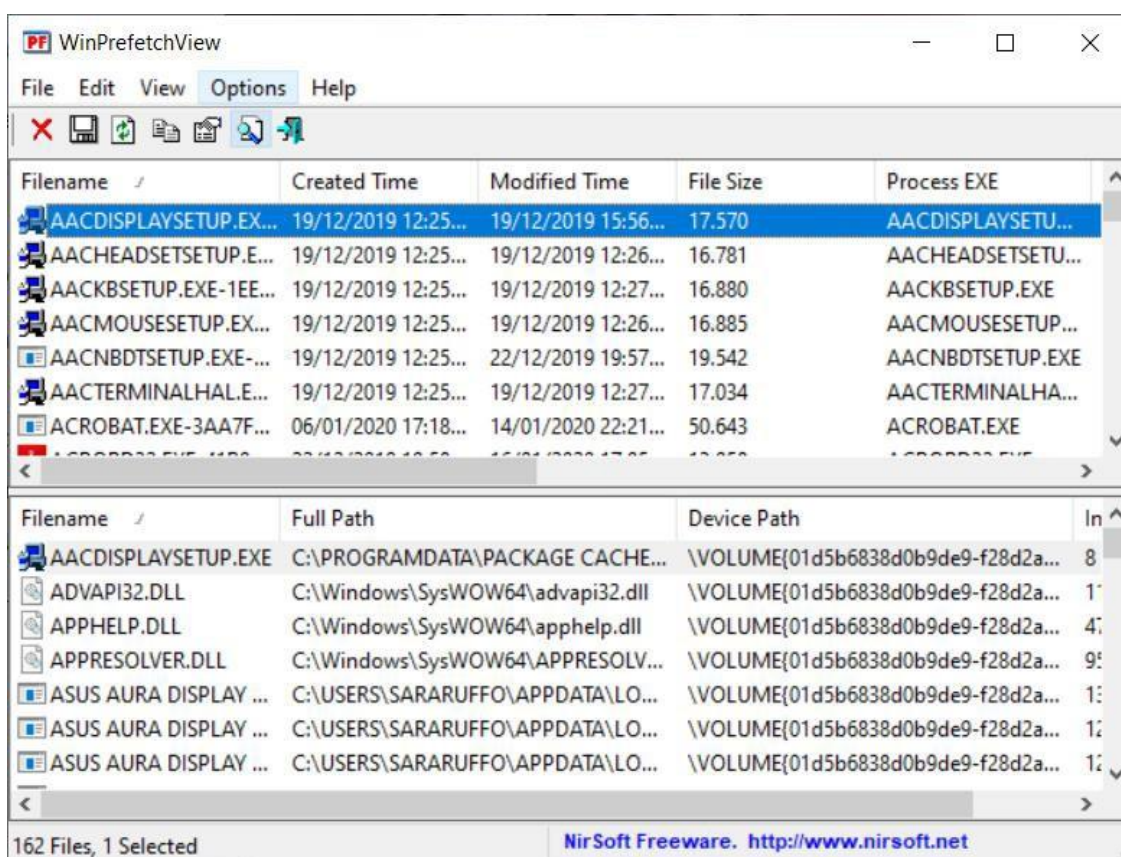
https://www.nirsoft.net/utills/chrome_cache_view.html

WinPrefetchView è una piccola utility che legge i file Prefetch memorizzati nel tuo sistema e visualizza le informazioni in essi memorizzate. Analizzando questi file, si può sapere quali file utilizza ogni applicazione e quali file vengono caricati all'avvio di Windows.

La finestra principale di WinPrefetchView contiene 2 riquadri: il riquadro superiore visualizza l'elenco di tutti i file Prefetch nel sistema. Quando si seleziona un file nel riquadro superiore, nel riquadro inferiore viene visualizzato l'elenco dei file memorizzati all'interno del file Prefetch selezionato, che rappresentano i file caricati dall'applicazione nei tempi precedenti in cui è stato utilizzato.

WinPrefetchView consente inoltre di eliminare i file Prefetch selezionati. Tuttavia, che anche quando viene eliminato un file Prefetch, verrà nuovamente creato dal sistema operativo appena verrà eseguito di nuovo lo stesso programma.

Puoi anche esportare i dati in un file CSV / xml / html.



Requisiti di sistema

Questa utility funziona su qualsiasi versione di Windows, a partire da Windows XP fino a Windows 10. Le versioni precedenti di Windows sono irrilevanti per questa utility, perché non usano i file Prefetch.

Questa utility è rilasciata come freeware.¹⁶

SuperFetchTree

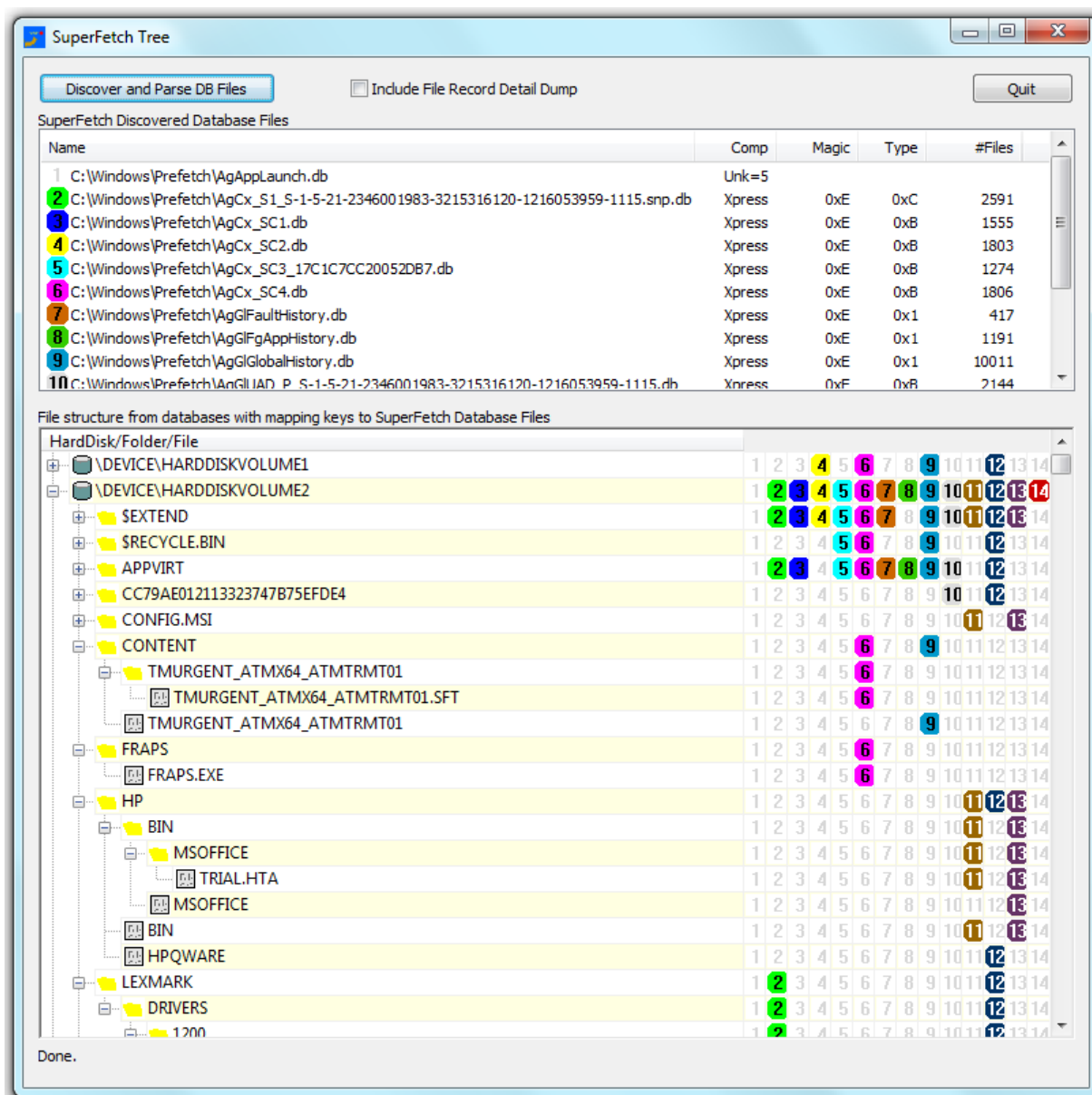
Descrizione

Questo strumento è stato scritto per studiare le informazioni archiviate da SuperFetch nei suoi file database. Al momento, questi sono ancora oggetto di indagine in quanto non conosciamo ancora completamente il formato di questi file. Microsoft non documenta il formato attualmente, ma questo strumento rappresenta lo sforzo migliore fino ad oggi per estrarre informazioni su di essi.

Le versioni recenti dei file dei sistemi operativi Microsoft Windows leggono i modelli dall'uso del sistema e quindi preparano gli scenari per determinati eventi e li memorizzano in una serie di file "DB" nella cartella Windows \ Prefetch. Il contenuto di questi file contiene informazioni tali che quando si verifica un evento implementato, il servizio SuperFetch memorizzerà nella cache determinati file nella cache degli elenchi di standby nella RAM, in previsione della loro necessità.

Questi file DB sono di un formato non documentato e compressi.

https://www.nirsoft.net/utils/win_prefetch_view.html



Uso

SuperFetchTree è uno strumento GUI. Individua e analizza tutti i file db SuperFetch e visualizza un elenco combinato con informazioni con codice colore su quali file fanno riferimento a questo elenco. Fornisce una struttura ad albero grafica e identifica in modo accurato a quali database un determinato file o cartella ha fatto riferimento

Se si seleziona la casella di controllo, verranno visualizzati ulteriori dettagli di ciascuna voce - al momento però non comprendiamo il formato di tali dettagli.

Questo strumento individuerà automaticamente tutti i file db nella cartella C: \ Windows \ Prefetch e li analizzerà facendo clic sul pulsante. Se si

desidera visualizzare i dettagli aggiuntivi per i file nella vista ad albero, selezionare la casella di controllo dump dei dettagli prima di fare clic sul pulsante Scopri e analizza.

È, al momento, l'unico tools che permette di analizzare i superfetch di Windows 10 da pc con sistema operativo Windows 10.

Requisiti di sistema

È l'unico tools che permette di analizzare i superfetch di Windows 10 da pc con sistema operativo Windows 10.¹⁷

Questa utility funziona su qualsiasi versione di Windows, a partire da Windows Vista fino Windows 10.

Ulteriori funzioni

Ulteriori funzioni non afferenti a nessun tools sono state implementate nel software.

Proprietà dei file

Descrizione

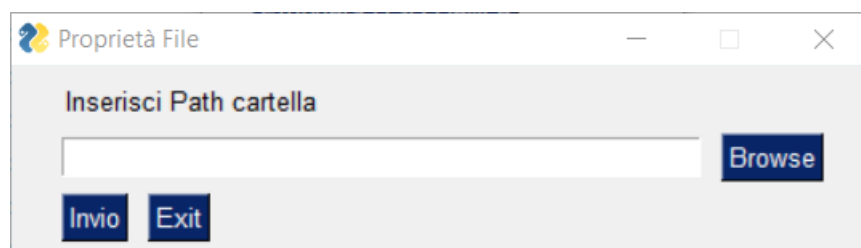
Questa funzione permette di visualizzare a schermo le proprietà dei file contenuti nella cartella selezionata.

Le caratteristiche dei file che verranno visualizzate sono:

- Il path del file.
- La data di ultima modifica;
- La data di creazione;
- La data di ultimo accesso.

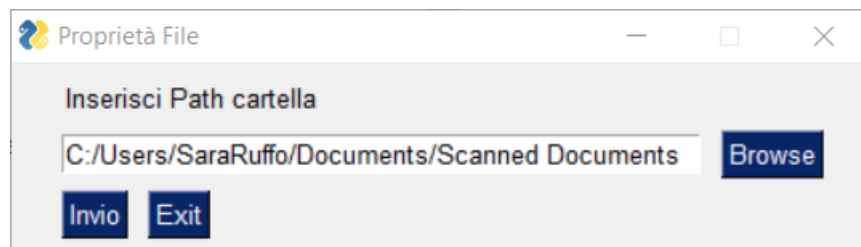
Uso

La funzione proprietà file permette all'utente di scegliere una cartella contenente i file da analizzare.

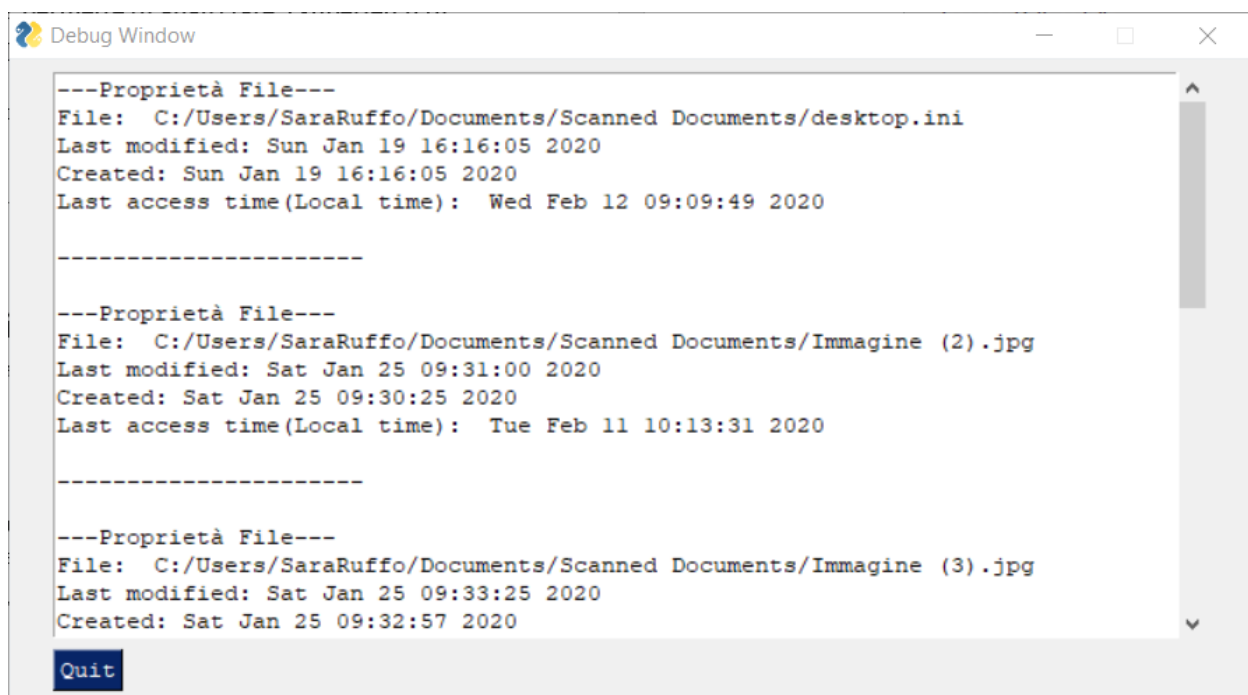


http://www.tmurgent.com/Tools/SuperFetch_Tools/SuperFetch_Tools.pdf

L'utente può selezionare la cartella attraverso il pulsante Browser, oppure incollando il path della cartella nell'apposito campo di testo



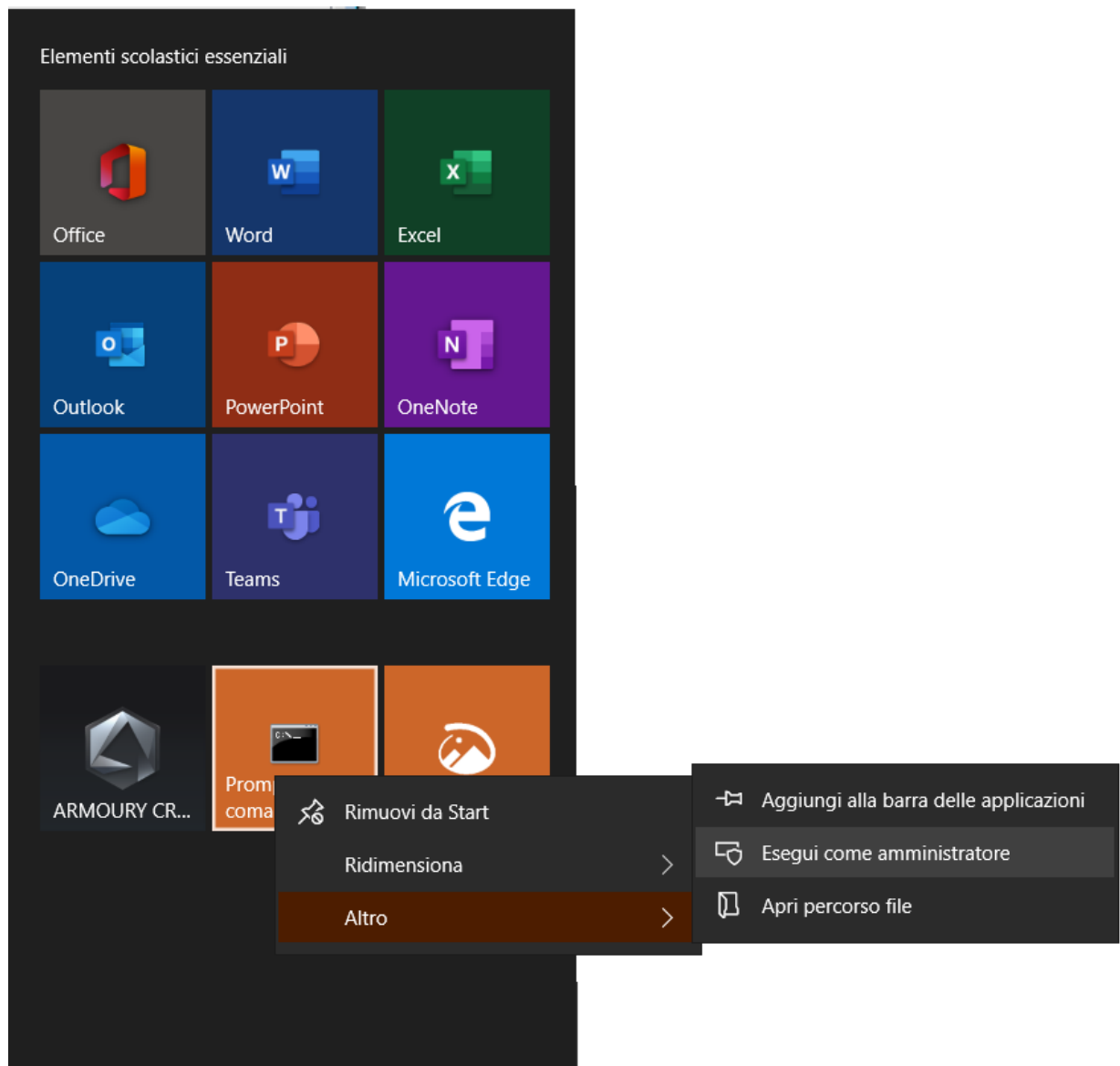
Una volta selezionata la cartella, verranno visualizzati a schermo le caratteristiche dei file in essa presenti.



Per poter visualizzare la *Data di ultimo* accesso (Last access time – data e orario sono basati sull'orario del sistema), è necessario che venga abilitata la visualizzazione dell'ultimo accesso a file e cartelle su Windows

Le operazioni da effettuare su Windows per abilitare la visualizzazione dell'ultimo accesso sono le seguenti:

1. Avviare il Prompt dei Comandi come Amministratore



2. Nel prompt digitare *fsutil behavior set disablelastaccess 0*

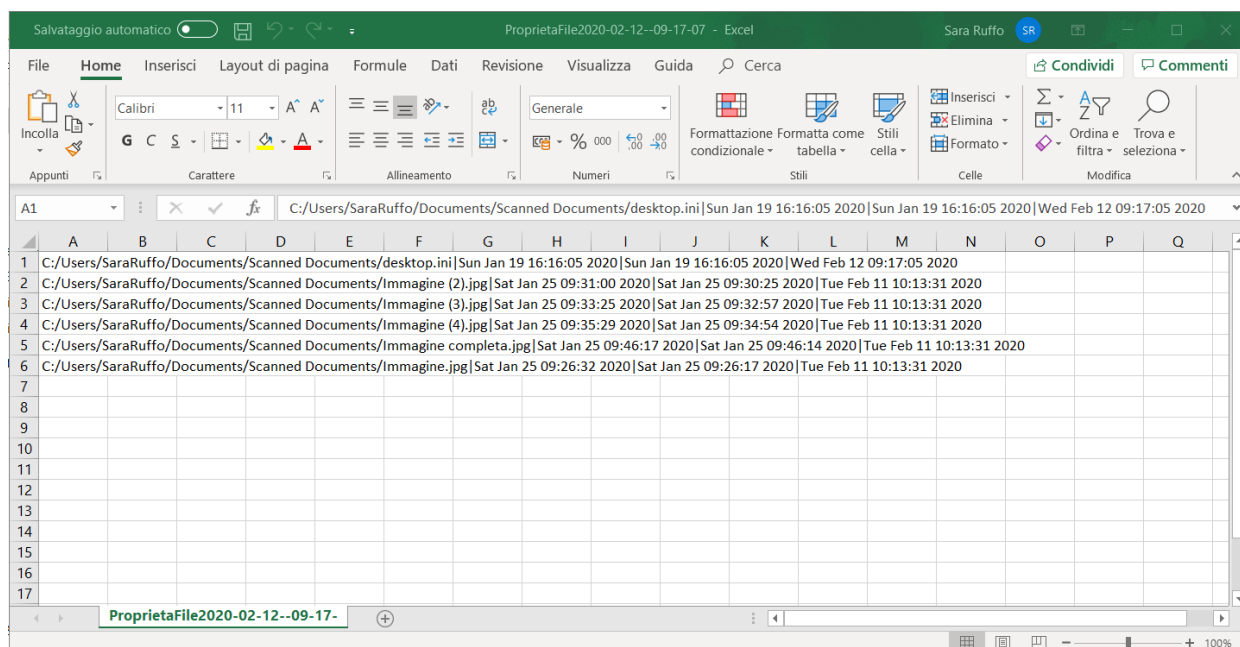
```
Amministratore: Prompt dei comandi
Microsoft Windows [Versione 10.0.18363.592]
(c) 2019 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Windows\system32>fsutil behavior set disablelastaccess 0
```

3. Premere invio e riavviare il computer.

Risultato

In seguito alla conferma da parte dell'utente, il programma stampa a video l'elenco delle caratteristiche dei file presenti nella cartella selezionata e genera un file .CSV, nella locazione del file eseguibile, contenente i dati visualizzati



Proprietà file .LNK

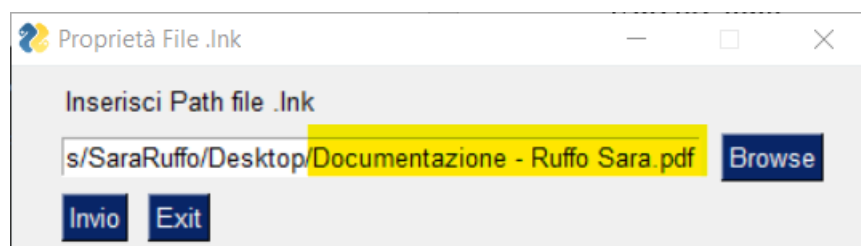
Descrizione

La funzione proprietà file .LNK permette all'utente di scegliere un file collegamento (.lnk) di cui visualizzare il link di destinazione.

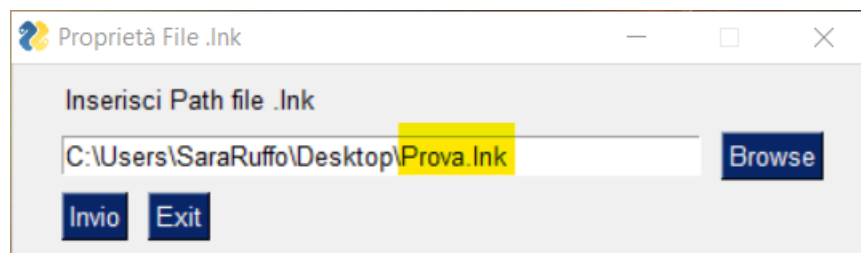
Uso

L'utente può:

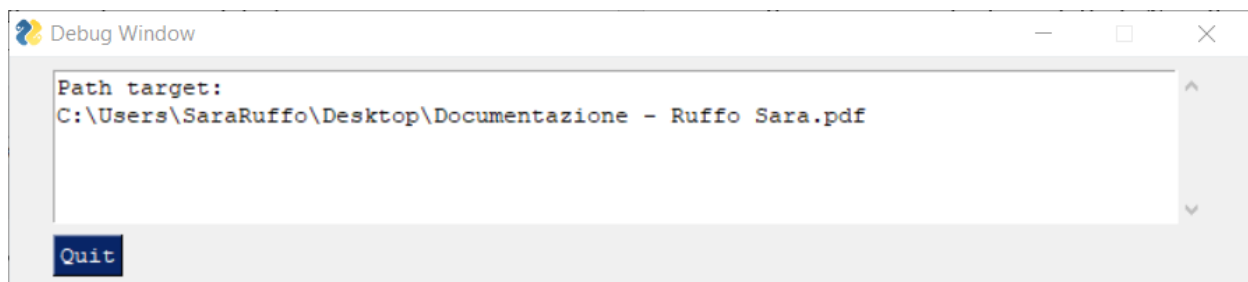
- Selezionare il file attraverso il pulsante Browser. In questo caso verrà visualizzato nel campo testo direttamente il path di destinazione del collegamento.



- Incollare il path del file nell'apposito campo di testo.



In questo caso bisognerà premere invio per poter visualizzare il path di destinazione del file .lnk

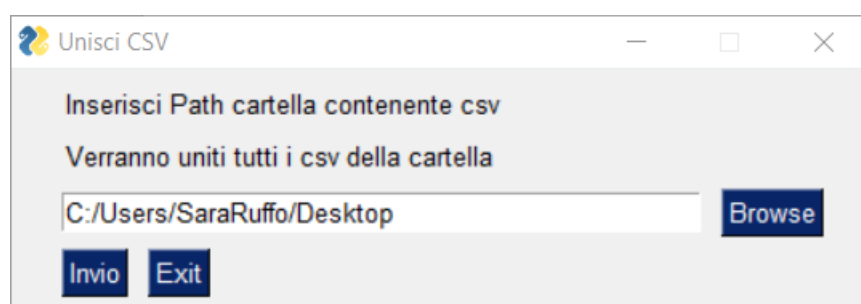


Unione file CSV

Questa funzione permette all'utente di unire i file CSV presenti nella cartella selezionata in un unico file XLSX in cui ogni file CSV è contenuto in un foglio XLSX.

Uso

L'utente potrà scrivere il path della cartella contenente i file .csv da unire oppure potrà usare il pulsante Browser per navigare all'interno delle cartelle e selezionare la cartella.



Risultato

Verrà generato un file unico nella cartella contenente i file CSV unificati nominato `[gg-mm-aaaa]combined_CSV.xlsx`.

Sistema

Il software è stato sviluppato e testato su sistema operativo Windows 10 e browser Chrome Versione 79.0.3945.117.

Il programma è stato sviluppato nel linguaggio di programmazione python 3.7

Come eseguire

Il programma è fornito sotto forma di file .exe nominato Progetto_Ruffo.exe. Per avviare il programma è sufficiente eseguire questo file.

Aggiornamento

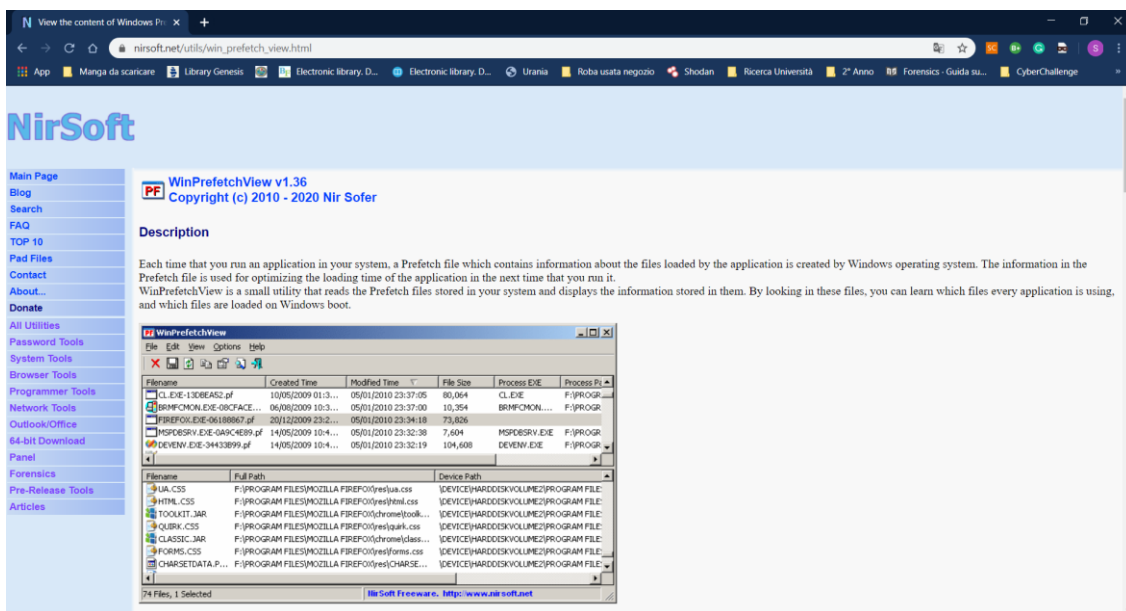
I tools precedentemente descritti potrebbero subire degli aggiornamenti nel corso del tempo.

Tools Nirsoft

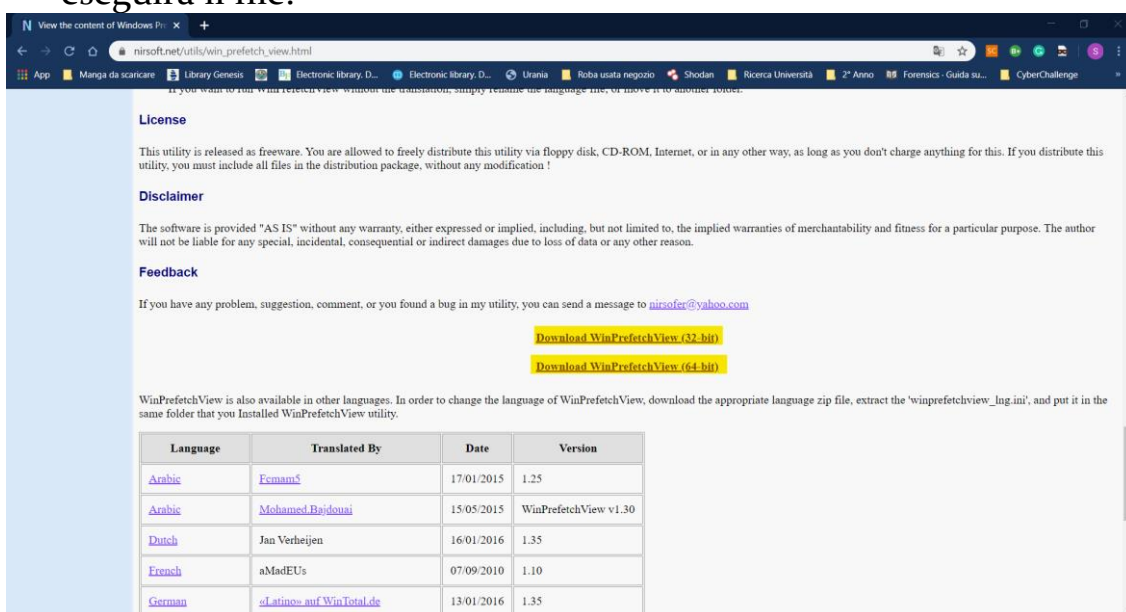
I seguenti tools sono realizzati da Nirsoft, quindi la procedura di aggiornamento è la stessa.

Per aggiornare i tools prodotti da Nirsoft, è necessario:

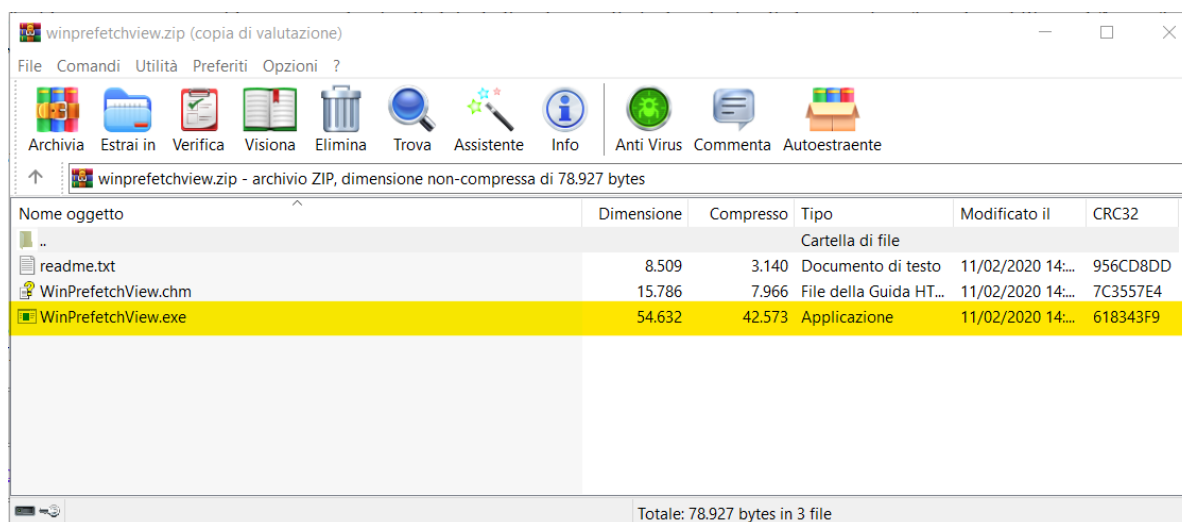
1. Aprire il browser prescelto, e visualizzare la pagina web del tools da aggiornare.
Ad esempio, nel caso di WinPrefetchView - https://www.nirsoft.net/utils/win_prefetch_view.html - la pagina che sarà visualizzata è la seguente:



2. Cliccare sul link del download presente in fondo alla pagina scegliendo la tipologia di eseguibile compatibile con il PC che eseguirà il file.



3. Il file .zip così scaricato conterrà il file .exe prescelto



4. Ora sarà sufficiente estrarre il file .exe e copiarlo nella directory contenente il file eseguibile .exe del programma principale - C:\Users\[UTENTE]\Progetto Informatica Forense - Ruffo Sara\PySimpleGui
5. Solo nel caso del tool ChromeCacheView è necessario copiare nella directory l'intera cartella estratta invece del solo file .exe.

I tools Nirsoft utilizzati in questo programma sono:

- JumpListView - https://www.nirsoft.net/utils/jump_lists_view.html
- USBDeview - https://www.nirsoft.net/utils/usb_devices_view.html
- BrowsingHistoryView - https://www.nirsoft.net/utils/browsing_history_view.html
- ChromeCacheView - https://www.nirsoft.net/utils/chrome_cache_view.html
- WinPrefetchView - https://www.nirsoft.net/utils/win_prefetch_view.html

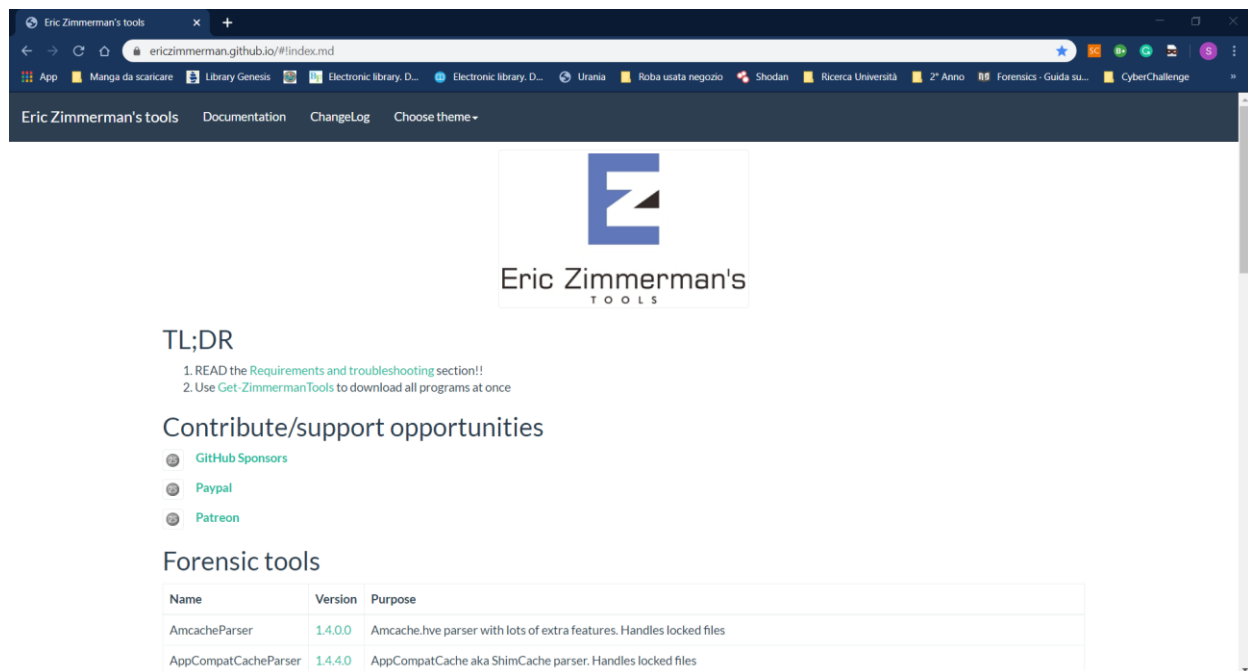
Tools Eric Zimmerman

I seguenti tools sono realizzati da Eric Zimmerman, quindi la procedura di aggiornamento è la stessa.

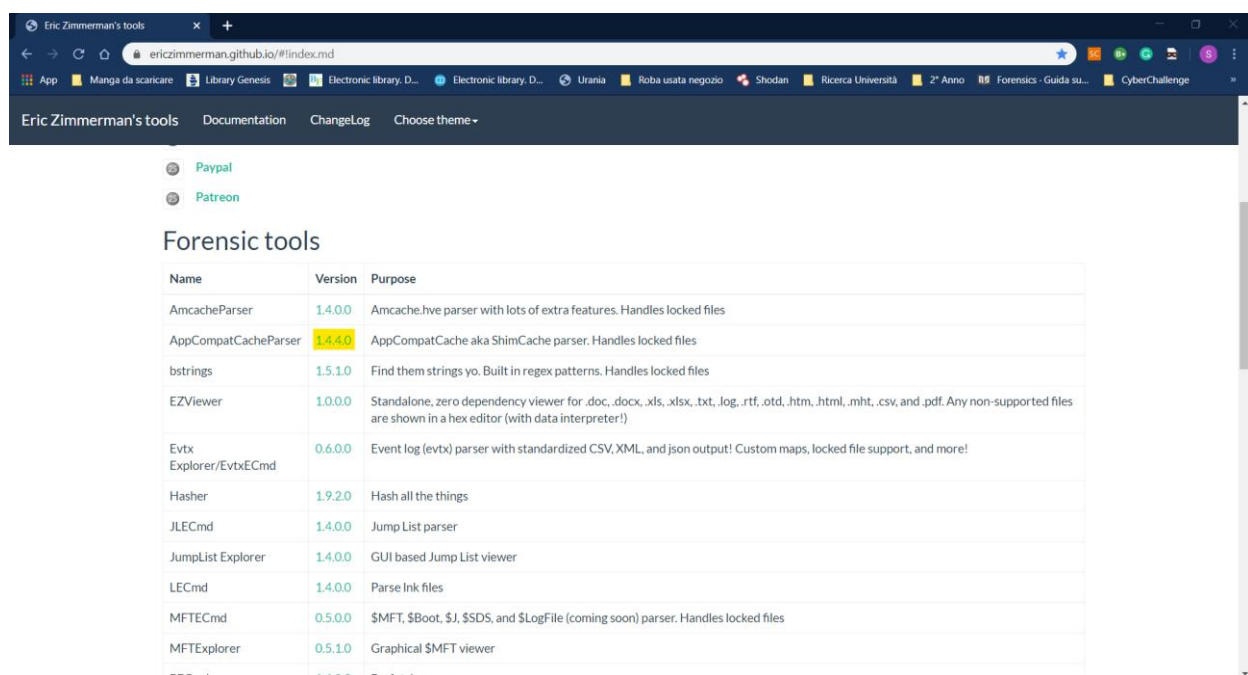
Per aggiornare i tools prodotti da Eric Zimmerman, è necessario:

1. Aprire il browser prescelto, e visualizzare la pagina web dei tools prodotti da Eric Zimmerman - <https://ericzimmerman.github.io>

La pagina è la stessa per entrambi i tools.



2. È necessario ricercare nella pagina il nome del tool che si vuole aggiornare e cliccare sul codice della versione corrente



3. Verrà così avviato il download di un file .zip contenente dell'ultima versione rilasciata del programma.

- a. Per l'aggiornamento di ShellBags Explorer sarà sufficiente estrarre la cartella contenuta nel file .zip appena scaricato e copiarlo nella directory contenente il file eseguibile .exe del programma principale - C:\Users\[UTENTE]\...\Progetto

Informatica Forense - Ruffo Sara\PySimpleGui

- b. Per l'aggiornamento di AppCompatCacheParser sarà necessario estrarre il file .exe contenuto nel file .zip appena scaricato e copiarlo nella directory contenente il file eseguibile .exe del programma principale - C:\Users\[UTENTE]\...\Progetto Informatica Forense - Ruffo Sara\PySimpleGui

I tools Eric Zimmerman utilizzati in questo programma sono:

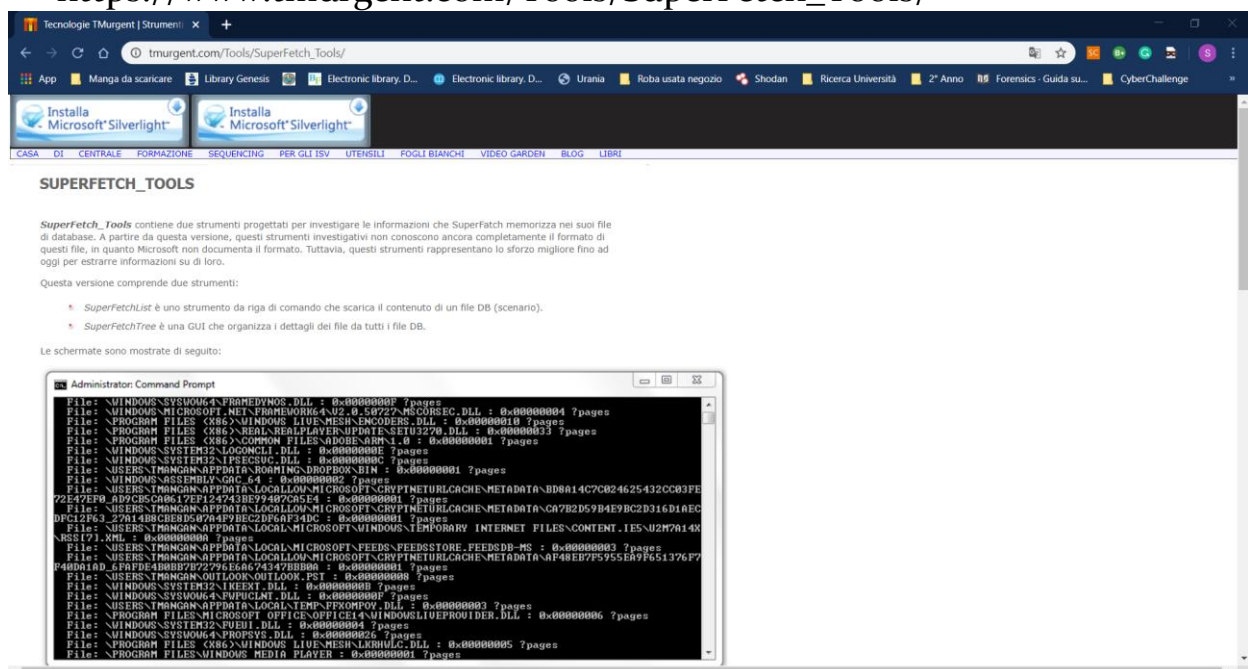
- ShellBags
- AppCompatCacheParser

Altri tools

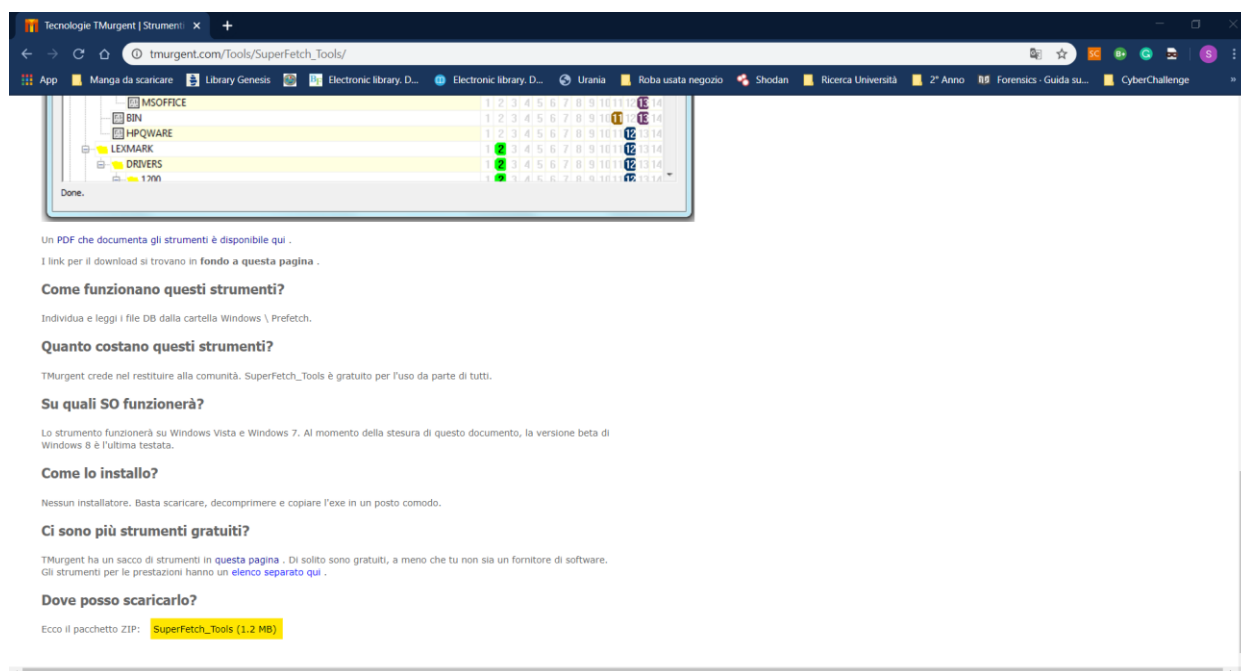
SuperFetchTree

Per aggiornare il tool SuperFetchTree è necessario:

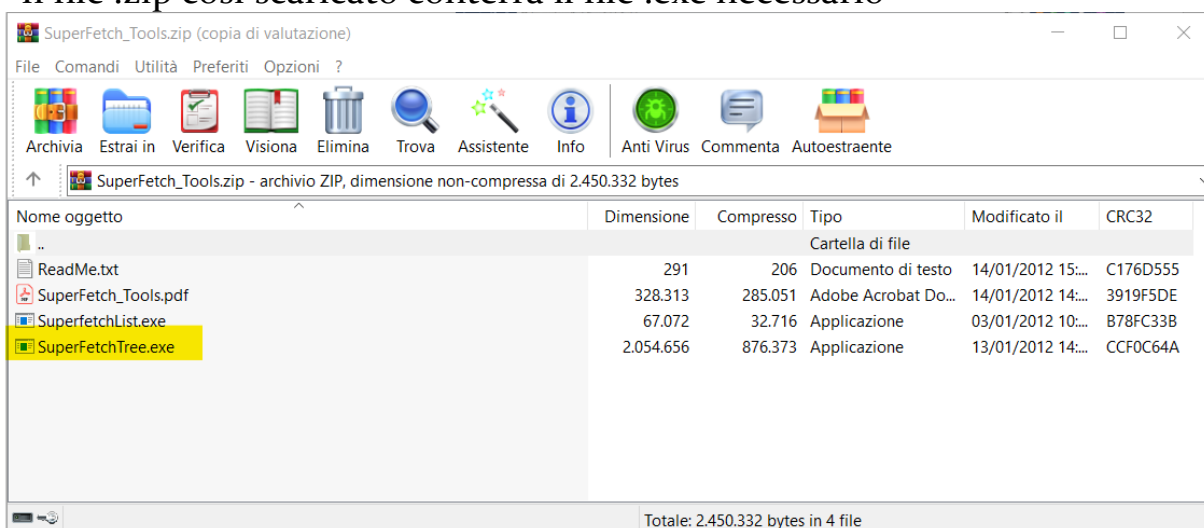
1. Aprire il browser prescelto, e visualizzare la pagina web del tool - https://www.tmurgent.com/Tools/SuperFetch_Tools/



2. Cliccare sul link del download presente in fondo alla pagina.



3. Il file .zip così scaricato conterrà il file .exe necessario



4. È ora necessario estrarre il file SuperFetchTree.exe contenuto nel file .zip appena scaricato e copiarlo nella directory contenente il file eseguibile .exe del programma principale - C:\Users\[UTENTE]\...\Progetto Informatica Forense - Ruffo Sara\PySimpleGui