



UNIVERSITÀ
degli STUDI
di CATANIA

Dipartimento di Matematica e Informatica
Corso di Laurea Triennale in Informatica

Digital Forensics
A.A. 2019/2020

ANALISI FORENSE

ALIBI INFORMATICO



Studentesse:

Francesca Ragazzi

Matricola: X81000697

Clizia Giorgia Manganaro

Matricola: X81000716

INDICE

Premessa 3

1. Software e strumenti utilizzati..... 3

2. Creazione Alibi..... 4

3. Occultamento Prove 5

4. Analisi Forense 7

5. Software e strumenti utilizzati 7

6. Conclusioni 9

7. Referenze 10

PREMESSA:

In una bigia giornata dell'aprile 2020, Jessica Fante in preda ad una crisi rancorosa nei confronti della sua ex amica di infanzia decise di vendicarsi per una faccenda amorosa avvenuta 10 anni prima.

Dopo aver premeditato per anni la sua vendetta decise di approfittare della corsa delle 22:00 p.m. della vittima per prenderla di soppiatto e commettere l'atto estremo.

Nel suo piano studiato alla perfezione decise di creare un finto alibi utilizzando gli strumenti informatici per difendersi da una eventuale accusa in tribunale utilizzando una estensione di Google Chrome che consente di generare uno script contenente una serie di sequenze automatizzate di azioni che verranno lanciate per la fascia oraria in cui commetterà il crimine, e dichiarerà di essere stata in casa in quell'arco temporale mentre navigava online su vari social Network, in particolare di essersi addormentata guardando una serie su Prime Video^[1].

Nel momento in cui commette il crimine lascerà il telefono a casa per evitare di produrre ulteriori tracce.

1. STRUMENTI E SOFTWARE UTILIZZATI:

1. PC Asus VivoBook S15 S510UN OS: Windows 10 Home
2. DéjàClick^[2] for Google Chrome
3. Browser Google Chrome

2. DéjàClick^[2] è uno strumento di registrazione e riproduzione che consente di creare script di monitoraggio basati sulle operazioni dell'utente per riprodurre attività del browser. È un'estensione gratuita che può essere collegato sia a Google Chrome che a Mozilla Firefox.

L'estensione permette di eseguire sequenze di operazioni, precedentemente prestabilite sul browser, pur non essendo fisicamente davanti alla macchina. Lo script generato verrà salvato in formato .xml a cui potranno essere apportate delle modifiche in futuro.



2. CREAZIONE ALIBI

Al fine di difendersi da una eventuale accusa, Jessica decide di creare un alibi da presentare in tribunale a sua difesa.

Prima di uscire da casa fa partire uno script di automatismi creato tramite DejaClick^[2].

La sera antecedente, la sospettata ha provveduto a registrare la sequenza di operazioni che saranno mandate in esecuzione il giorno successivo, che prevedono la navigazione in vari Social Network, siti web ed infine la visione di una serie tv su Prime Video. Le istruzioni verranno eseguite sequenzialmente in modo da simulare un comportamento umano a tutti gli effetti, con tempi di attesa variabili, errori di scrittura e autocorrezioni. Al termine dell'esecuzione dello script, l'accusata provvede alla disinstallazione dell'estensione DejaClick, alla cancellazione dei file associati all'estensione (chiave di registro) e alla distruzione di tutte le possibili tracce che possono essere state lasciate, inoltre, viene cancellata la cronologia relativa all'estensione ma non relativa alla cronologia della navigazione automatizzata che sarà parte fondamentale della dimostrazione dell'alibi.

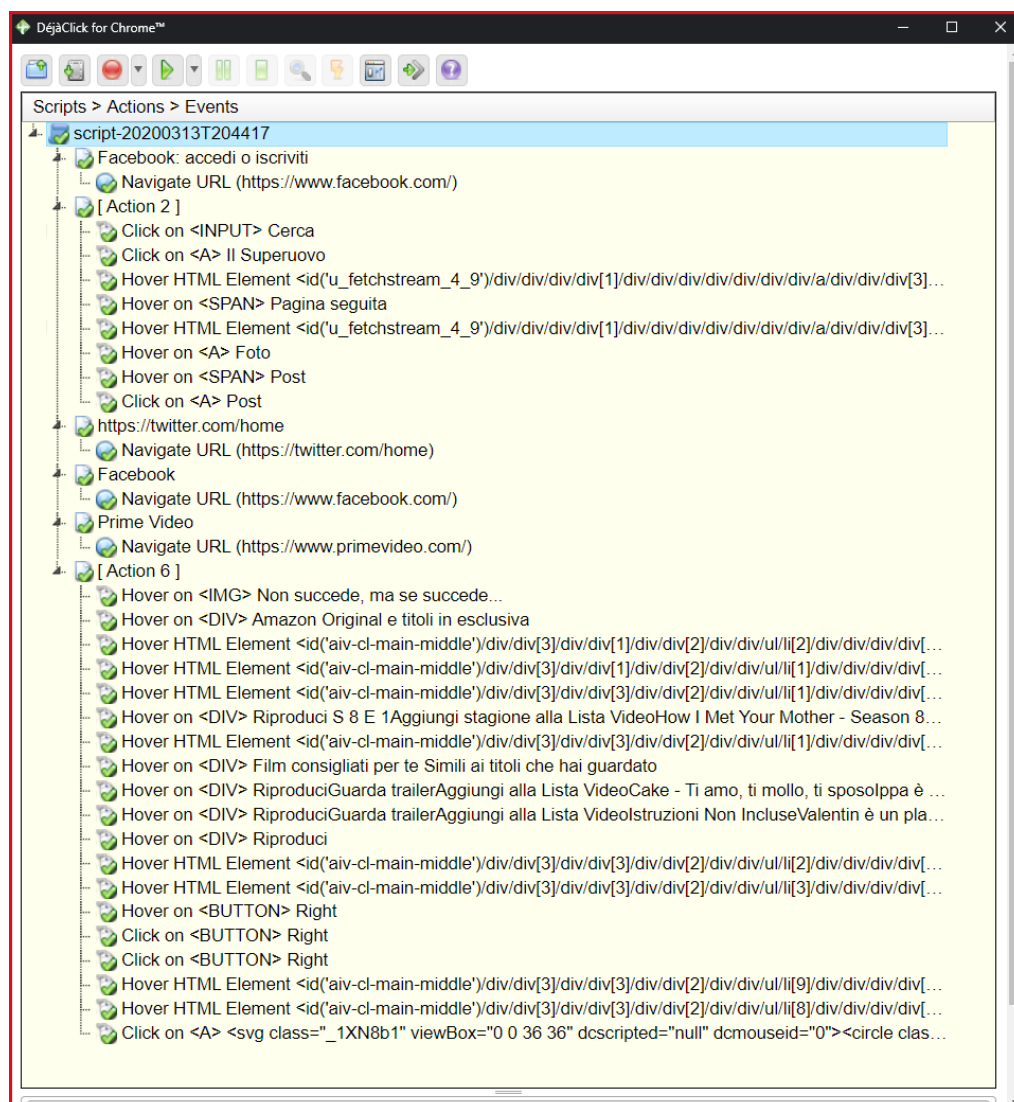


Figura-1 Script creato con DejaClick.

3. OCCULTAMENTO PROVE

- Su Google Chrome selezionando Altri Strumenti/Estensioni/Modalità sviluppatore e successivamente, cliccando su dettagli dell'estensione recuperiamo l'ID relativo a DejaClick for Chrome.
- Una volta memorizzato l'ID, eliminiamo l'estensione da Google Chrome e chiudiamo il browser.

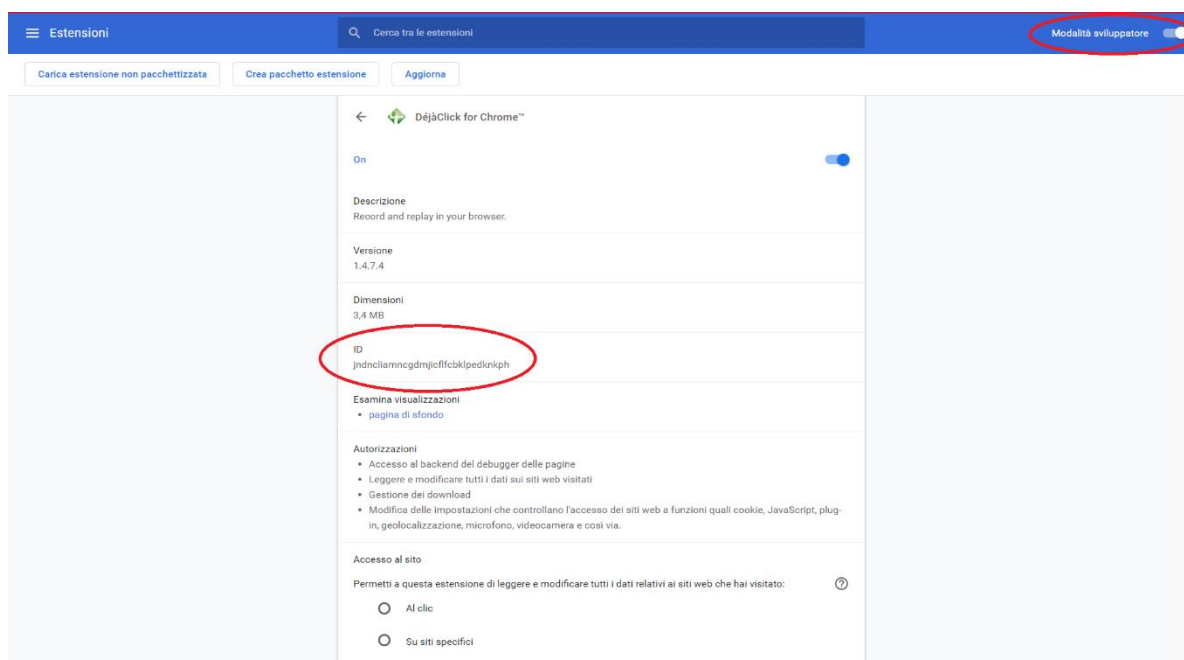


Figura-2 Screen finestra estensione Dejaclick su Google Chrome.

- Aprendo l'Editor del registro di sistema, dalla barra di ricerca di Windows, facciamo clic su Modifica/Trova e dalla finestra è necessario incollare l'ID dell'estensione di Chrome, quindi fare clic sul pulsante Trova successivo.

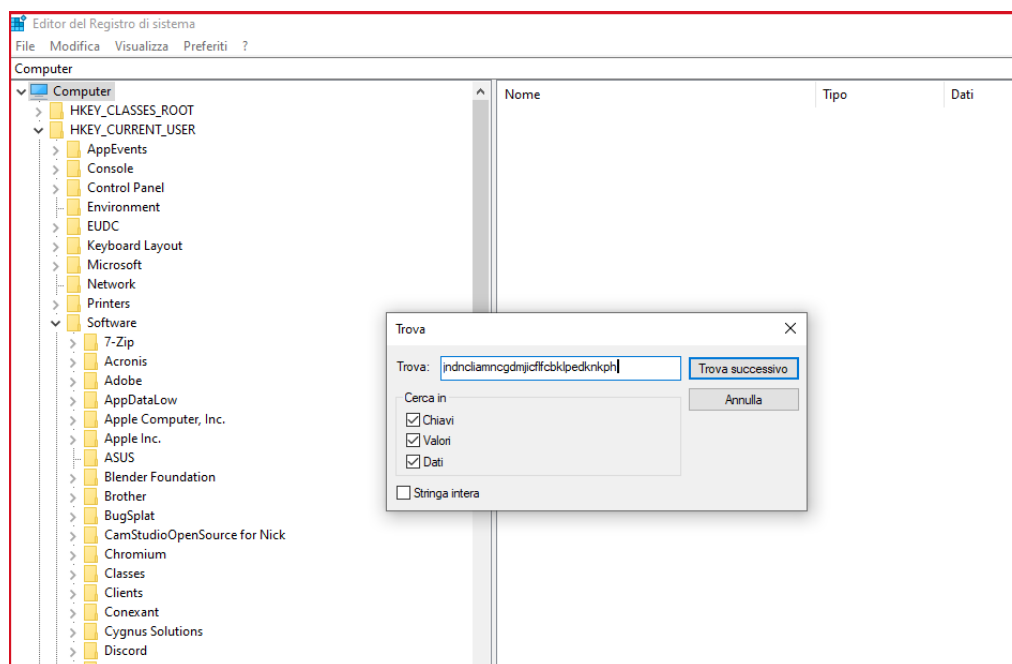


Figura-3 Finestra dell'Editor di registro di sistema.

- È possibile eliminare la chiave di registro che corrisponde al valore dei dati dell'ID, facendo semplicemente clic con il tasto destro del mouse sulla chiave di registro e selezionare Elimina.

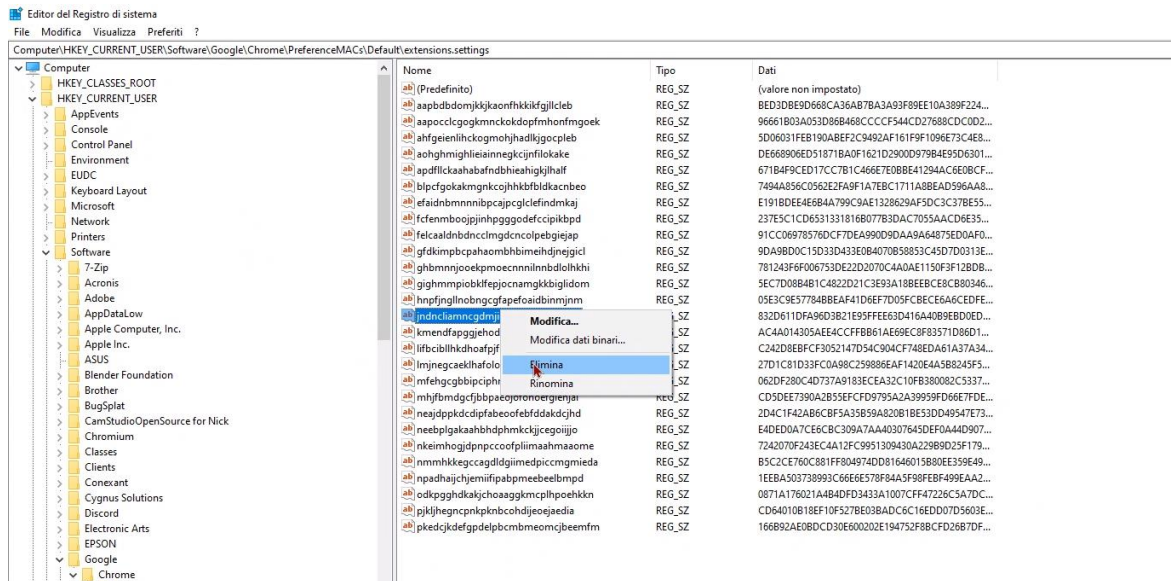


Figura-4 Eliminazione chiave di registro.

- Fare clic sul pulsante Sì per rimuovere la voce del registro.
- Per la rimozione dei file associativi è necessario andare nel percorso *C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions* ed eliminare la cartella nominata con codice ID relativo all'estensione.
- Al percorso *C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications* eliminiamo la cartella con codice ID relativo all'estensione.
- Eliminiamo il file *.xml* dello script memorizzato.
- Eliminiamo i file recenti cliccando tasto destro su Accesso rapido/Opzioni e nella sezione privacy clicchiamo su cancella.

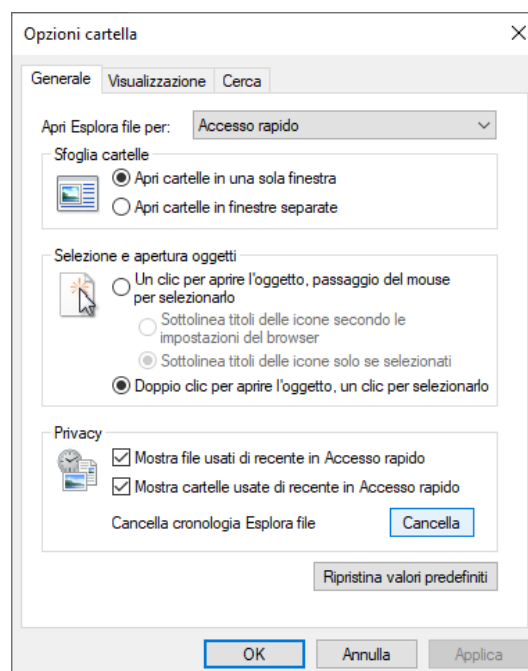


Figura-5 Eliminazione File recenti.

4. ANALISI FORENSE

Per procedere con l'analisi forense viene sequestrato il pc (Asus VivoBook S15 S510UN OS: Windows 10 Home) della sospettata, in modo tale da ottenere i dati in modo completo con interferenze minime sui dati originali sotto esame, in dettaglio utilizzando le Best Practices per tutte le fasi della consulenza tecnica. È da evidenziare che l'analisi potrebbe risultare particolarmente difficile in quanto i software non sono stati installati nel sistema e non si rilevano tracce nel file di registro. Le uniche evidenze che potrebbero essere rinvenute riguardano l'elenco degli ultimi file aperti e nella cartella dei file prefetch.

Il tecnico può solo verificare la credibilità dell'evidenza accertandosi che il sistema di rilevazione non abbia evidenziato falle tecnologiche tali da rendere non ammissibile giuridicamente la prova informatica.

Inoltre, il pc analizzato ha un sistema di riconoscimento di impronte digitali che consente di accedere al device solamente in presenza della sospettata, è dunque possibile dimostrare scientificamente l'associazione con l'individuo escludendo la presenza di complici.

5. STRUMENTI E SOFTWARE UTILIZZATI

1. PC Asus VivoBook S15 S510UN OS: Windows 10 Home
2. LastActivityView^[3]
3. BrowsingHistoryView^[4]
4. ChromeCacheView^[5]
5. RegScanner^[6]

2. LastActivityView^[3] è un tool per il OS Windows che raccoglie informazioni da varie fonti su un sistema in esecuzione e visualizza un registro delle azioni eseguite dall'utente e degli eventi verificatisi sul computer. L'attività visualizzata da LastActivityView include:

- esecuzione di file .exe;
- finestra di dialogo Apri/Salva;
- apri file/cartella da Explorer o altro software;
- installazione software, arresto/avvio del sistema;
- arresto dell'applicazione o del sistema;
- connessione/disconnessione della rete e altro.

3. BrowsingHistoryView^[4] è un tool che legge i dati cronologici di diversi browser Web (Mozilla Firefox, Google Chrome, Internet Explorer, Microsoft Edge, Opera) e consente di guardare la cronologia di navigazione di tutti i profili utente in un sistema in esecuzione visualizzandola in una tabella che include le seguenti informazioni:

- URL visitato;
- titolo;
- tempo di visita;
- conteggio visite;
- Browser Web;
- profilo utente.

4. ChromeCacheView^[5] è un tool 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.

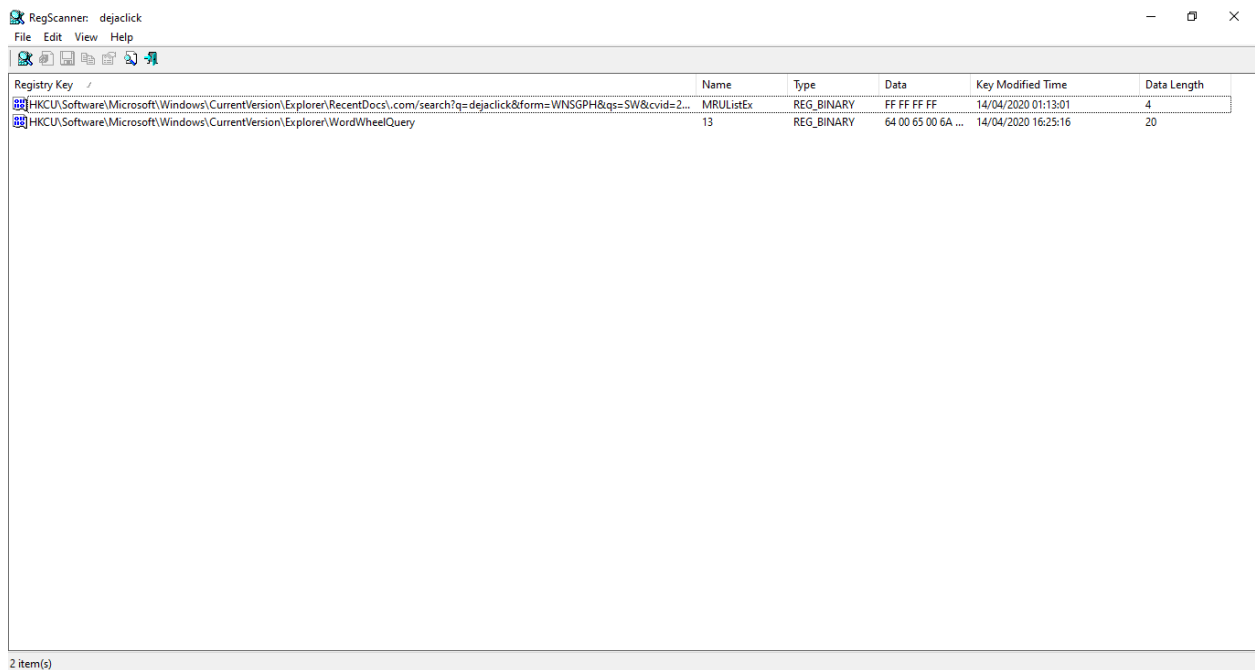
5. RegScanner^[6] è un tool progettato per semplificare le ricerche nel registro che consente di specificare le chiavi di base e i valori che si vogliano controllare, quindi si possono cercare solo i valori DWORD in KEY_LOCAL_MACHINE e HKEY_CURRENT_USER, **è possibile eseguire ricerche di stringa con distinzione tra maiuscole e minuscole**. Inoltre, **è in grado di esaminare solo le chiavi del Registro di sistema che sono state modificate nel periodo di tempo specificato**.

6. CONCLUSIONI

Dopo aver effettuato l'analisi forense è stato possibile rinvenire tramite RegScanner delle modifiche relative ad una chiave di registro dell'estensione DéjàClick, di conseguenza l'alibi dichiarato dalla sospettata Jessica Fante non è ammissibile giuridicamente.

Vengono riportate in figura le evidenze digitali ricavate tramite il tool sopracitato.

L'imputata pertanto viene dichiarata colpevole del crimine.



Registry Key	Name	Type	Data	Key Modified Time	Data Length
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\com/search?q=dejaclick&form=WNSGPH&q=SW&cvid=2...	MRUListEx	REG_BINARY	FF FF FF FF	14/04/2020 01:13:01	4
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery	13	REG_BINARY	64 00 65 00 6A ...	14/04/2020 16:25:16	20

Figura-6 Evidenze digitali finto alibi relativo ad una modifica di una chiave di registro dell'estensione DejaClick.

7. REFERENZE

- [1] <https://www.primevideo.com/>
- [2] <https://smartbear.com/product/alertsite/features/dejaclick/>
- [3] https://www.nirsoft.net/utils/computer_activity_view.html
- [4] https://www.nirsoft.net/utils/browsing_history_view.html
- [5] https://www.nirsoft.net/utils/chrome_cache_view.html
- [6] <https://www.nirsoft.net/utils/regscanner.html>