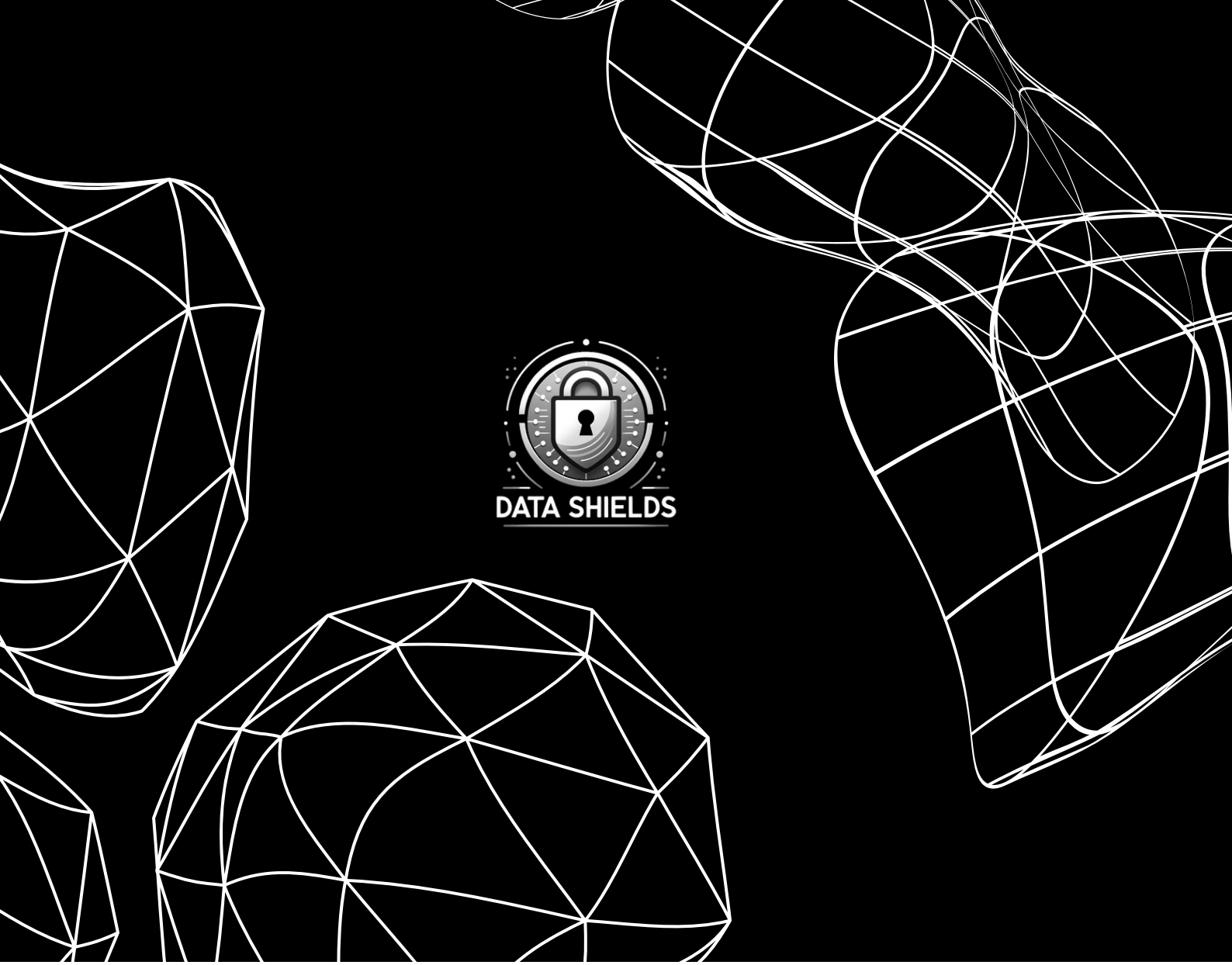


AFFIDABILITY ANALISYS

MARCO MALIZIA
DATASHIELDS

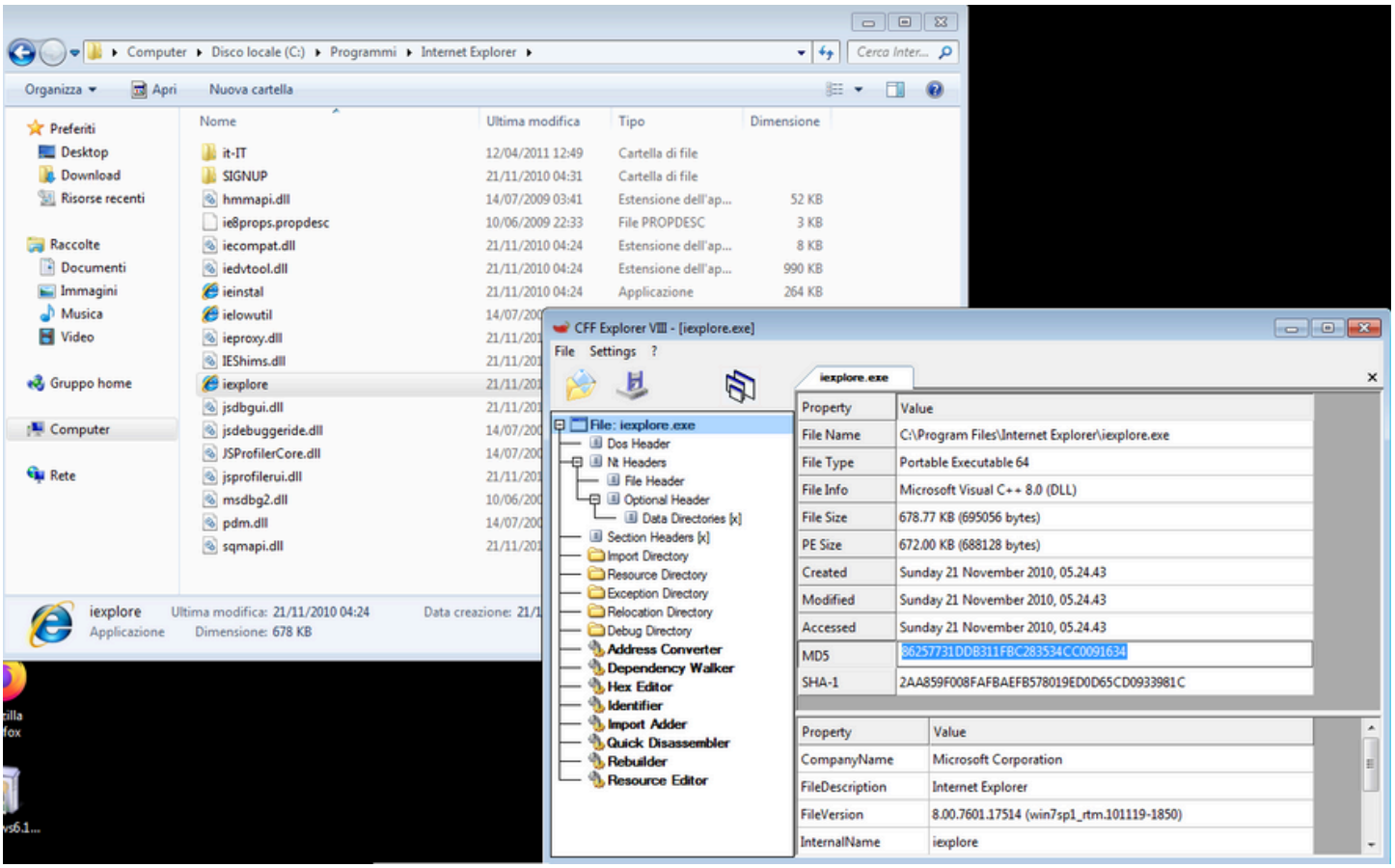
INCARICO

UN GIOVANE DIPENDENTE NEO ASSUNTO SEGNALA AL REPARTO TECNICO LA PRESENZA DI UN PROGRAMMA SOSPETTO. IL SUO SUPERIORE GLI DICE DI STARE TRANQUILLO MA LUI NON È SODDISFATTO E CHIEDE SUPPORTO AL SOC. IL FILE "SOSPETTO" È IEXPLORE.EXE CONTENUTO NELLA CARTELLA C :\PROGRAMMI\INTERNET EXPLORER (NO, NON RIDETE RAGAZZI)

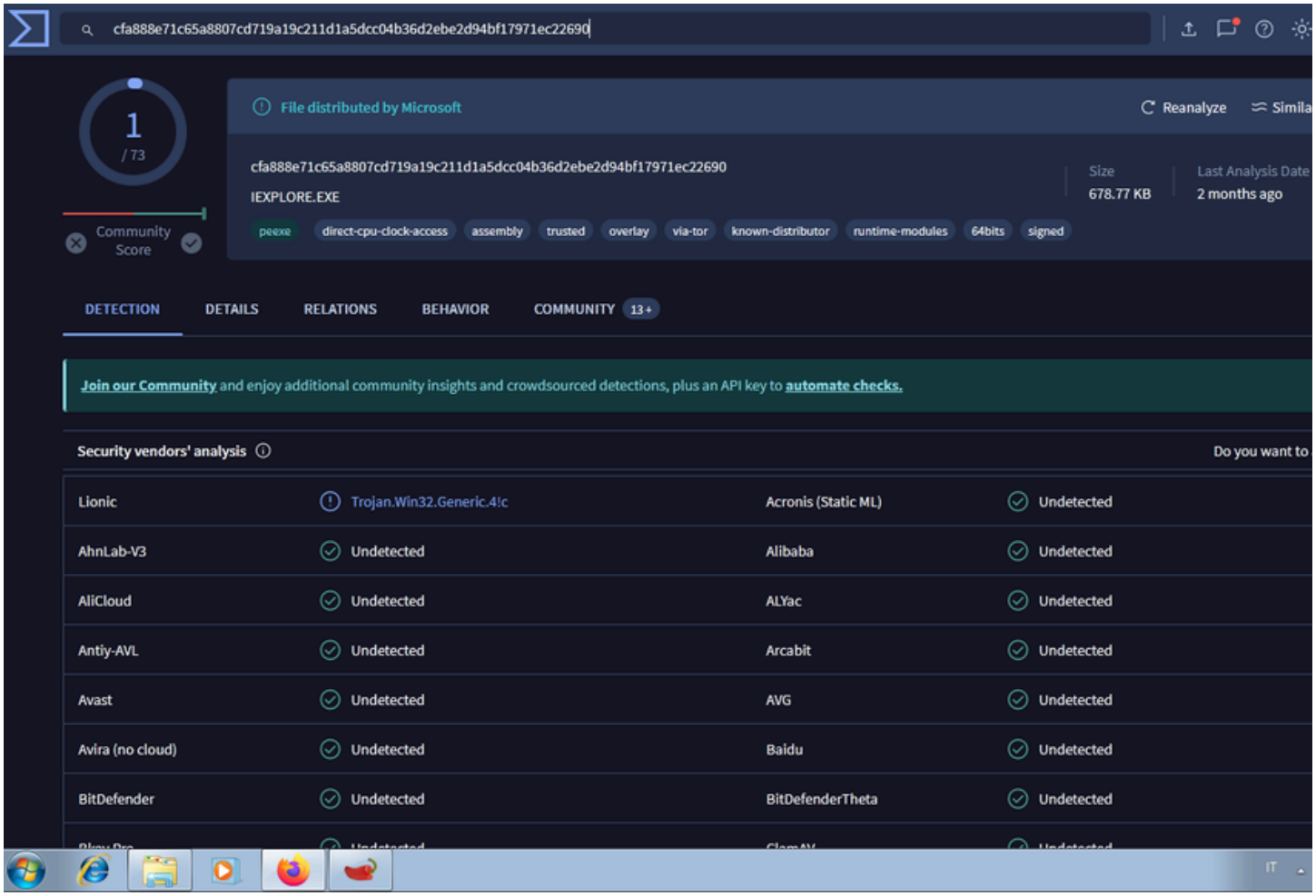
COME MEMBRO SENIOR DEL SOC TI È RICHIESTO DI CONVINCERE IL DIPENDENTE CHE ILFILE NON ÈMALIGNO. ESERCIZIO TRACCIA E REQUISITI POSSONO ESSERE USATI GLI STRUMENTI DI ANALISI STATICA BASICA E/O ANALISI DINAMICA BASICA VISTI A LEZIONE. NO DISASSEMBLY NO DEBUG O SIMILARI VIRUSTOTAL NON BASTA, OVVIAMENTE NON BASTA DIRE IEXPLORER È MICROSOFT QUINDI È BUONO, PUNTO.

VIRUSTOTAL

COME PRIMA ANALISI, ANDIAMO A CONSULTARE IL SERVIZIO **VIRUSTOTAL** COSI DA AVERE UN RISCONTRO ESPLICITO SULLA SICUREZZA DEL FILE OGGETTO. UNA VOLTO TROVATO IL FILE ALL'INTERNO DELLA DIRECTORY INDICATA PROCEDIAMO APRENDOLO CON **CFF EXPLORER.** ANDIAMO AD OTTENERE NELLA SEZIONE DI INFORMAZIONI DEL FILE IL CODICE HASH CHE INSERIREMO NEL PORTALE.



UNA VOLTA APERTO IL PORTALE DI VIRUSTOTAL PROCEDIAMO CON LA RICERCA ATTRAVERSO L'URL, INSERENDO IL CODICE HASH TROVATO IN PRECEDENZA.



NELL'IMMAGINE VEDIAMO IL RISCONTRO DELL'ANALISI DEL FILE DA PARTE DI MOLTEPLICI MOTORI ANTIVIRUS, CHE CONFERMANO L'INTEGRITÀ DEL FILE SOTTOLINEANDO LA SICUREZZA NELL'UTILIZZO.

ANALISI DINAMICA BASE

LA MAGGIOR PARTE DEI VENDOR IDENTIFICA IEXPLORE.EXE COME NON MALEVOLO. PROCEDIAMO CON UN'ANALISI DINAMICA DI BASE USANDO REGSHOT. QUESTO TOOL CATTURA DUE ISTANTANEE DEL REGISTRO DI SISTEMA E DEL FILE SYSTEM, CONSENTENDO DI CONFRONTARLE PER INDIVIDUARE LE MODIFICHE. QUESTE INFORMAZIONI SONO UTILI PER CAPIRE QUALI CHIAVI DI REGISTRO O FILE VENGONO ALTERATI DURANTE L'INSTALLAZIONE DI UN PROGRAMMA O ALTRE MODIFICHE AL SISTEMA. DOPO AVER EFFETTUATO UN PRIMO SHOT DEL REGISTO POSSIAMO PROCEDERE CON L’APERTURA DELL’ESEGUIBILE COSI DA POTER EFFETTARE IL SECONDO SHOT E CONFRONTARLI.

```
-----------------------------------
Keys deleted: 1
-----------------------------------
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Sett

-----------------------------------
Keys added: 2
-----------------------------------
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Sett
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Sett

-----------------------------------
Values deleted: 5
-----------------------------------
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Sett
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Sett
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Sett
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Sett
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Sett
```

```
-----------------------------------
Values added: 12
-----------------------------------
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Internet Explorer\Recovery\Active\{
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Internet Explorer\TypedURLs\url3: "
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Set
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Set
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Set
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Set
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Set
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Set
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Set
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Set
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Set
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Set

-----------------------------------
Values modified: 17
-----------------------------------
HKLM\SOFTWARE\Microsoft\Windows Search\Gather\Windows\SystemIndex\NewClientID: 0x00000002
HKLM\SOFTWARE\Microsoft\Windows Search\Gather\Windows\SystemIndex\NewClientID: 0x00000003
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\AppDataLow\Software\Microsoft\Internet Explor
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\AppDataLow\Software\Microsoft\Internet Explor
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Internet Explorer\Main\Window_Place
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Internet Explorer\Main\Window_Place
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Internet Explorer\Main\Start Page R
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Internet Explorer\Main\Start Page R
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Internet Explorer\Main\IE8RunOnceLa
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Internet Explorer\Main\IE8RunOnceLa
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Internet Explorer\Main\WindowsSearc
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Internet Explorer\Main\WindowsSearc
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Internet Explorer\TypedURLs\url1: "
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Internet Explorer\TypedURLs\url1: "
```

QUESTE SOLO LE DUE CHIAVI CHE SONO STATE AGGIUNTE:

1. HKU\S-1-5-21-3771313050-58705377-3452663501-1001\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\5.0\CACHE\EXTENSIBLE CACHE\MSHIST012024080220240803
2. HKU\S-1-5-21-3771313050-58705377-3452663501-1001\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\5.0\LOWCACHE\EXTENSIBLE CACHE\MSHIST012024080220240803

DOPO UNA RICERCA IN RETE POSSIAMO AFFERMARE CHE QUESTE CHIAVI SONO RELATIVE ALLA CACHE DI INTERNET EXPLORER, SPECIFICAMENTE ALLA CRONOLOGIA DI NAVIGAZIONE. INDICANO CHE IL BROWSER HA CREATO DELLE NUOVE VOCI NELLA CACHE, PROBABILMENTE PER MEMORIZZARE LA CRONOLOGIA DI NAVIGAZIONE RECENTE.

CONCLUSIONE

DOPO AVER EFFETTUATO DUE CONTROLLI SULL'ESEGUIBILE OGGETTO DI ANALISI, ABBIAMO RISCONTRATO DUE REPORT CHE CONFERMANO L'INTEGRITÀ DI **IEPLORER.EXE**, NEL CASO QUESTE DUE ANALISI NON BASTASSERO POTREMMO PROCEDERE CON UN'ANALISI SFTRUTTANDO IL SOFTWARE **CFF EXPLORER** ANALIZZANDO LE LIBRERIE, CON LE RISPETTIVE SEZIONI, IMPORTATE DALL'ESEGUIBILE.
VISTA L'AFFIDABILITÀ DEI DUE SECURITY CHECK AFFRONTATI POSSIAMO CONFERMARE AL COLLEGA CHE PUÒ CONTINUARE AD UTILIZZARE EXPLORER AUGURANDOGLI TANTA PAZIENZA NELL'ASPETTARE CHE SI CARICHINO LE PAGINE.