

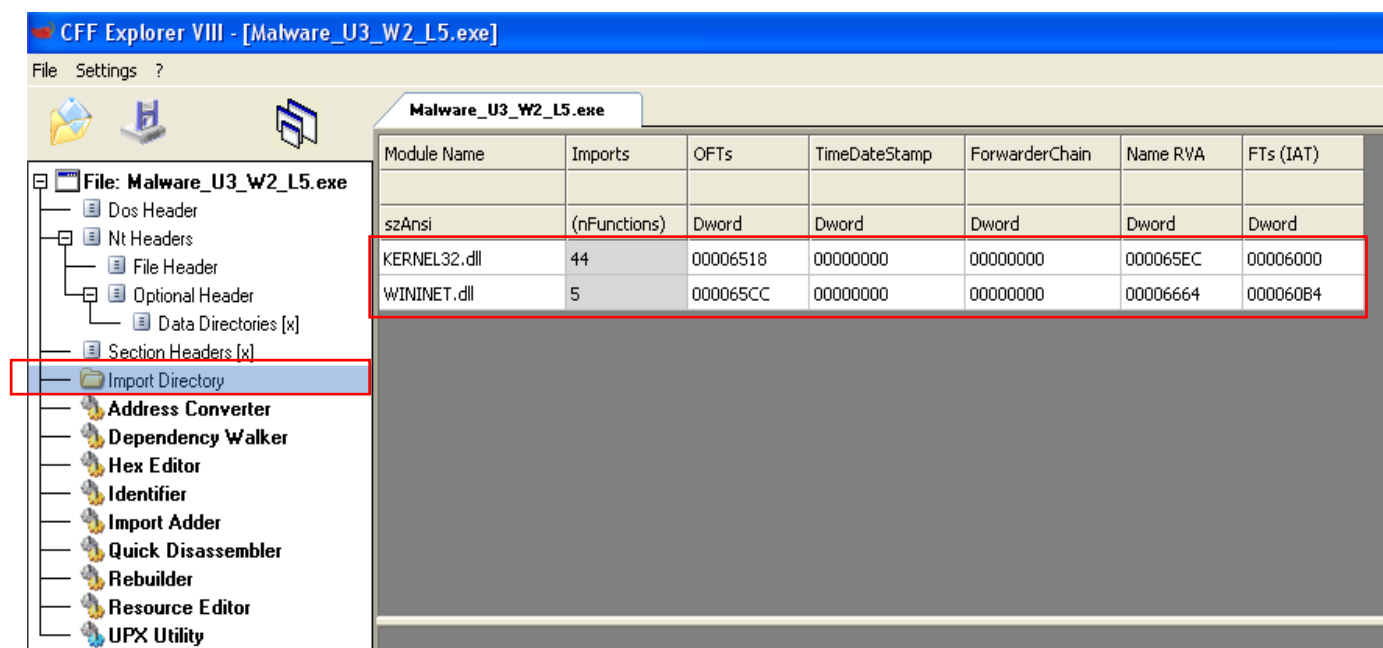
## PROGETTO

## Analisi Malware\_U3\_W2\_L5

Per eseguire l'analisi di questo malware, utilizzo il programma **CFF Explorer**.

Importo il file eseguibile contenente il malware all'interno del tool e ne analizzo il contenuto.

Per prima cosa, analizzo le librerie importate da questo malware andando nel menù **"import directory"**.



Da qui si possono notare le due librerie importate:

- **KERNEL32.dll**: libreria che contiene le funzioni principali per interagire con il sistema operativo e svolgere varie operazioni a basso livello. Svolge un ruolo chiave nella creazione e nell'esecuzione di applicazioni Windows.
- **WININET.dll**: libreria che contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP. Viene comunemente utilizzata da browser web, programmi di download, client FTP e altre applicazioni che richiedono la comunicazione su Internet.

Analizzando più nello specifico la libreria KERNEL32.dll, si possono notare, tra le funzioni richieste, le funzioni **LoadLibraryA** e **GetProcAddress**. Questo implica che la modalità di importazione di tale libreria è a tempo di esecuzione, cioè l'eseguibile richiama la libreria solamente quando ha necessità di utilizzare una determinata funzione. È una tecnica usata dai malware per risultare meno invasivi e rilevabili.

KERNEL32.dll	44	00006518	00000000	00000000	000065EC	00006000
WININET.dll	5	000065CC	00000000	00000000	00006664	000060B4

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
000067E4	000067E4	0175	GetVersionExA
000067F4	000067F4	019D	HeapDestroy
00006802	00006802	019B	HeapCreate
00006810	00006810	02BF	VirtualFree
0000681E	0000681E	019F	HeapFree
0000682A	0000682A	022F	RtlUnwind
00006836	00006836	02DF	WriteFile
00006842	00006842	0199	HeapAlloc
0000684E	0000684E	00BF	GetCPInfo
0000685A	0000685A	00B9	GetACP
00006864	00006864	0131	GetOEMCP
00006870	00006870	02BB	VirtualAlloc
00006880	00006880	01A2	HeapReAlloc
0000688E	0000688E	013E	GetProcAddress
000068A0	000068A0	01C2	LoadLibraryA
000068B0	000068B0	011A	GetLastError

Nella libreria WININET.dll, invece, si può notare la funzione **InternetGetConnectedState** che ha lo scopo di verificare se la macchina su cui è in esecuzione il programma ha accesso ad internet.

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00006664	N/A	000064F0	000064F4	000064F8	000064FC	00006500
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	44	00006518	00000000	00000000	000065EC	00006000
WININET.dll	5	000065CC	00000000	00000000	00006664	000060B4

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
00006640	00006640	0071	InternetOpenUrlA
0000662A	0000662A	0056	InternetCloseHandle
00006616	00006616	0077	InternetReadFile
000065FA	000065FA	0066	InternetGetConnectedState
00006654	00006654	006F	InternetOpenA

Successivamente mi sposto nel menù “**Section Headers**” per visualizzare le sezioni di cui si compone il file eseguibile.

CFF Explorer VIII - [Malware\_U3\_W2\_L5.exe]

File Settings ?

Malware\_U3\_W2\_L5.exe

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	00004A78	00001000	00005000	00001000	00000000	00000000	0000	0000	60000020
.rdata	0000095E	00006000	00001000	00006000	00000000	00000000	0000	0000	40000040
.data	00003F08	00007000	00003000	00007000	00000000	00000000	0000	0000	C0000040

File: Malware\_U3\_W2\_L5.exe

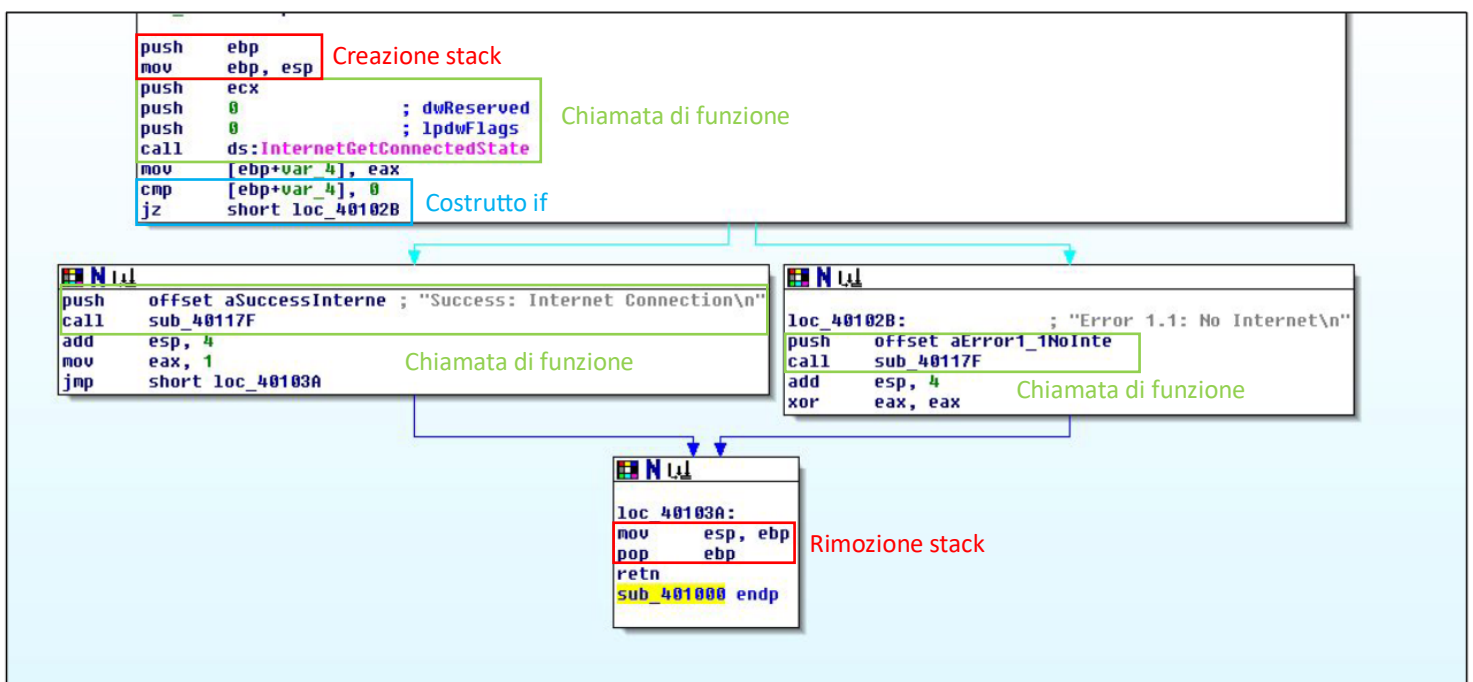
- Dos Header
- Nt Headers
- File Header
- Optional Header
- Data Directories [x]
- Section Headers [x]**
- Import Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

- **.text**: contiene le istruzioni che la CPU eseguirà una volta che il software sarà avviato. È l'unica sezione di un file eseguibile che viene eseguita dalla CPU.
- **.rdata**: include le informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile.
- **.data**: contiene dati/variabili globali del programma eseguibile che devono essere disponibili da qualsiasi parte del programma.

Si possono anche notare ulteriori informazioni dalla schermata delle sezioni come:

- **Virtual size**: dimensione dello spazio allocato per la sezione durante il processo di caricamento dell'eseguibile in memoria
- **Raw size**: dimensione dello spazio occupato dalla sezione quando è sul disco.

## Analisi codice assembly



Analizzando nel complesso il codice fornitoci, esso sembra verificare lo stato della connessione internet della macchina e successivamente stampa un messaggio a schermo in base al risultato ottenuto: "success: internet connection" nel caso di connessione, "error 1.1: no internet" in caso di non connessione.

Essendo però questa solo una parte del codice di un ipotetico malware, si può ipotizzare che esso abbia bisogno di una connessione ad internet per svolgere alcune operazioni.

In conclusione, posso ipotizzare che il malware in questione sia un downloader, un trojan o una backdoor.

Analizzo qualche riga del codice:

- **Call ds:InternetGetConnectedState:** viene chiamata la funzione InternetGetConnectedState. ds indica che la funzione è situata nella sezione di dati del programma.
- **Push offset aSuccessInternet ; "Success: Internet Connection\n":** viene messo l'indirizzo della stringa "Success: Internet Connection\n" in cima allo stack.
- **Jmp short loc\_40103A:** viene effettuato un salto incondizionato a loc\_40103A. viene eseguito il salto ignorando le istruzioni successive fino all'etichetta specificata.
- **Xor eax,eax:** viene eseguita un'operazione di XOR tra il registro eax e se stesso. Viene impostato il registro eax a zero.
- **Retn sub 401000 endp:** ritorna alla subroutine. Il comando serve per ripristinare l'indirizzo di ritorno dallo stack e per riprendere l'esecuzione del codice principale.

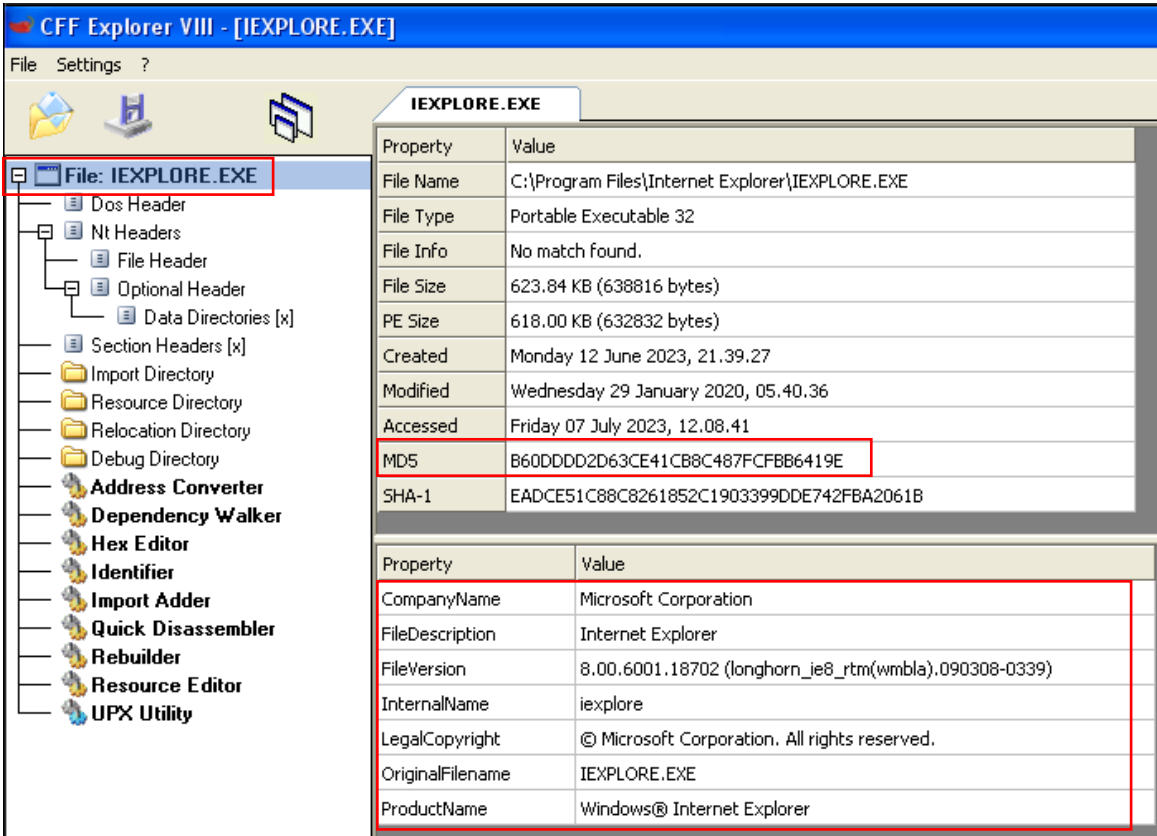
## BONUS: analisi file sospetto IEXPLORE.EXE

Dopo aver ricevuto una segnalazione da un dipendente di un programma sospetto, inizio l'analisi di tale programma se si tratta di un possibile malware oppure è un programma non maligno.

Trattandosi del programma IEXPLORER.exe contenuto nella cartella C:\Program Files\Internet Explorer, potrei già dire al dipendente che si tratta di un programma sano essendo ben conosciuto e distribuito ufficialmente da Microsoft. Eseguo, però, un'analisi più approfondita sia per avvalorare maggiormente il mio pensiero, sia perché in alcuni casi i malware potrebbero nascondersi dietro a programmi all'apparenza "innocenti".

Avvio quindi il tool **CFF EXPLORER**, apro l'eseguibile IEXPLORER.exe e vedo che nella parte inferiore del programma ci sono tutte le informazioni note riguardo tale eseguibile come il nome della compagnia che lo ha rilasciato, la descrizione, il nome del prodotto, ecc.

Mi appunto, inoltre, l'hash MD5 dell'eseguibile che utilizzerò in seguito per un'ulteriore analisi: B60DDDD2D63CE41CB8C487FCFBB6419E



The screenshot displays the CFF Explorer VIII interface for the file IEXPLORE.EXE. The left sidebar shows a tree view of file components, with 'File: IEXPLORE.EXE' selected. The main pane on the right is divided into two sections. The top section, titled 'IEXPLORE.EXE', lists various properties such as File Name, File Type, File Size, PE Size, Created, Modified, Accessed, MD5, and SHA-1. The MD5 hash is highlighted with a red box. The bottom section, also titled 'IEXPLORE.EXE', lists additional properties like CompanyName, FileDescription, FileVersion, InternalName, LegalCopyright, OriginalFilename, and ProductName. This section is also highlighted with a red box.

Property	Value
File Name	C:\Program Files\Internet Explorer\IEXPLORE.EXE
File Type	Portable Executable 32
File Info	No match found.
File Size	623.84 KB (638816 bytes)
PE Size	618.00 KB (632832 bytes)
Created	Monday 12 June 2023, 21.39.27
Modified	Wednesday 29 January 2020, 05.40.36
Accessed	Friday 07 July 2023, 12.08.41
MD5	B60DDDD2D63CE41CB8C487FCFBB6419E
SHA-1	EADCE51C88C8261852C1903399DDE742FBA2061B

Property	Value
CompanyName	Microsoft Corporation
FileDescription	Internet Explorer
FileVersion	8.00.6001.18702 (longhorn_ie8_rtm(wmbla).090308-0339)
InternalName	iexplore
LegalCopyright	© Microsoft Corporation. All rights reserved.
OriginalFilename	IEXPLORE.EXE
ProductName	Windows® Internet Explorer



This screenshot shows the VirusTotal analysis interface for the file IEXPLORE.EXE. On the left, a green circular progress indicator shows 0 detections out of 70 engines. A red box highlights this indicator. The main header area contains a green checkmark icon and the text "No security vendors and no sandboxes flagged this file as malicious", which is also enclosed in a red box. Below the header, the file's SHA-256 hash is displayed: b18a0d4beba606bf30f5010ba3c72abafac8d5f303a8fbc24d77f7b78b7866e. A red box highlights the filename "IEXPLORE.EXE". To the right of the hash, the file size is listed as 623.84 KB and the last analysis date is 15 days ago. At the bottom, a row of analysis categories is shown: peexe, via-for, overlay, runtime-modules, signed, detect-debug-environment, ide, direct-cpu-clock-access, and checks-user-input.

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 20 +

### Basic properties ①



**HYBRID**  
ANALYSIS

Q IP, Domain, Hash..

 Request Report Deletion

whitelisted

[Link](#)
[Twitter](#)
[E-Mail](#)

[Link](#)
[Twitter](#)
[E-Mail](#)

[Link](#)
[Twitter](#)
[E-Mail](#)

✓ Up-to-date

VirusTotal

CLEAN

### Multi Scan Analysis

Last Update: 07/07/2023 12:48:58 (UTC)

View Details: 

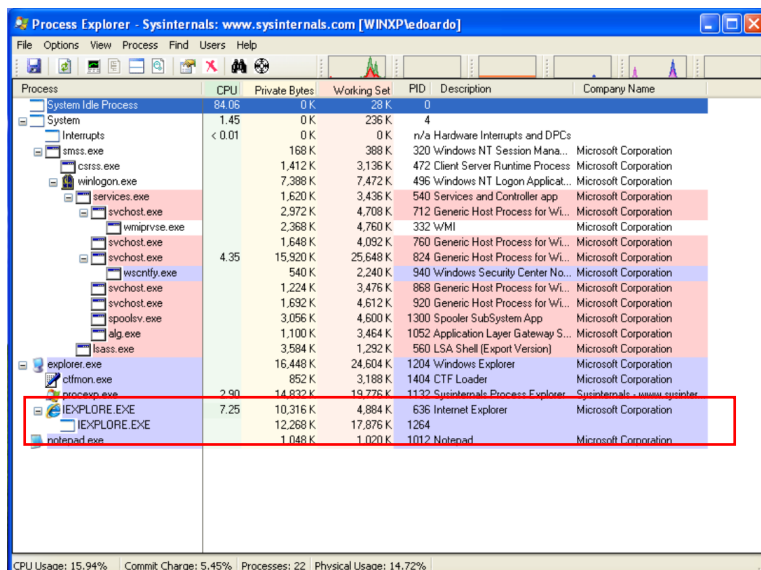
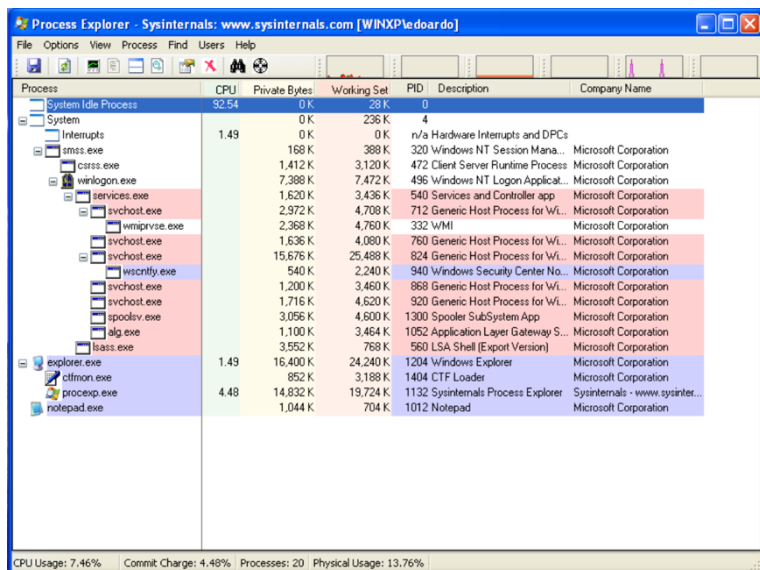
Visit Vendor: 

 GET STARTED WITH A FREE TRIAL

Da questa schermata risulta, nuovamente, un programma non sospetto e risulta pure in whitelist. Inoltre, tutti i risultati degli antivirus confermano che il file è pulito.

Non volendo però presentare al dipendente solo una ricerca sul web, continuo l'analisi aiutandomi con qualche tool per avere maggiori conferme.

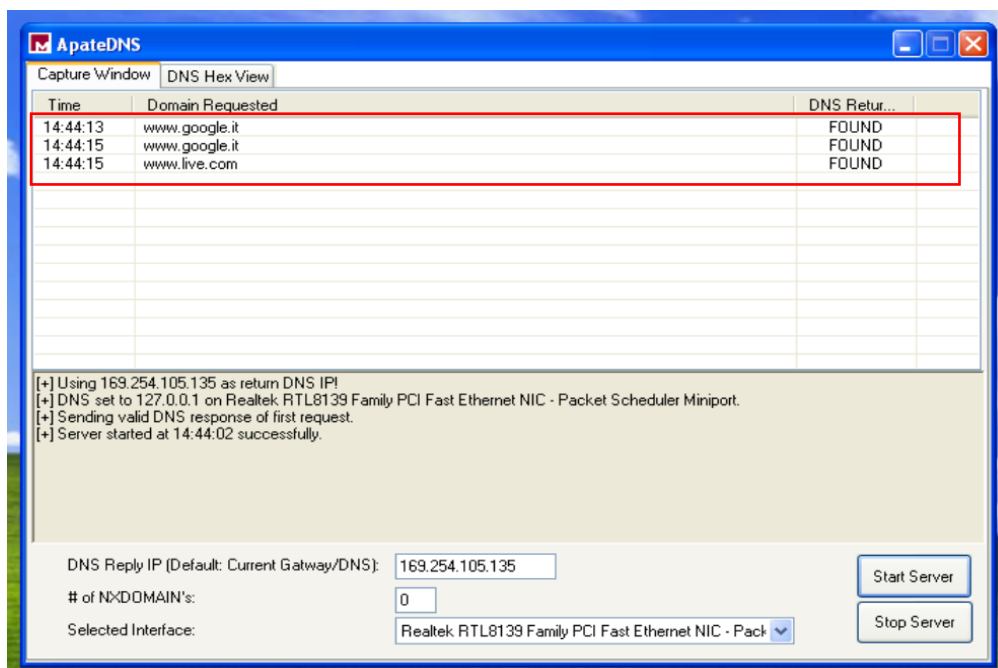
Avvio il tool **Process Explorer** e salvo un'istantanea del risultato, successivamente avvio il programma IEXPLORER.exe ed eseguo nuovamente un'istantanea di procexp per analizzare i processi creati.



Dalle schermate ottenute si può notare come all'apertura di Internet Explorer si crei solo il suo processo e non anche altri processi sospetti.

Questo conferma ulteriormente il fatto che sia un file sano.

Successivamente avvio il tool **ApatDNS** per verificare il traffico di rete generato dal file e poter controllare se, in modo nascosto, cerca di raggiungere indirizzi sospetti, di creare qualche tipo di connessione malevola o di scaricare qualcosa di indesiderato.



Anche in questo caso, però, trovo solo riscontri positivi sulla natura del file segnalatomi dal dipendente.

Dopo tutte queste analisi, posso comunicare al dipendente che il file che ha segnalato è pulito e non nasconde niente di sospetto e che quindi può usarlo tranquillamente.