

REPORT

S10-L5

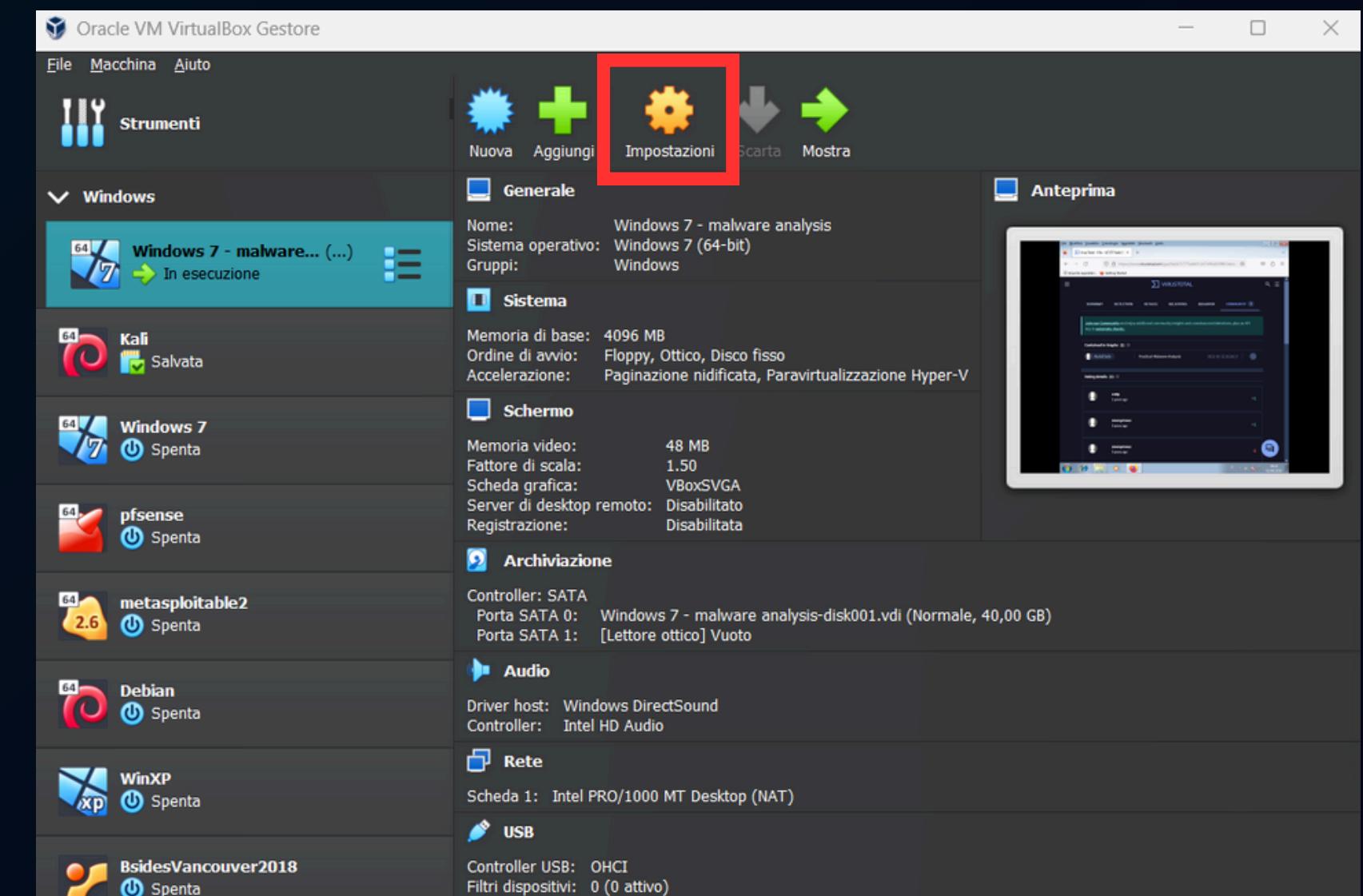
Traccia:

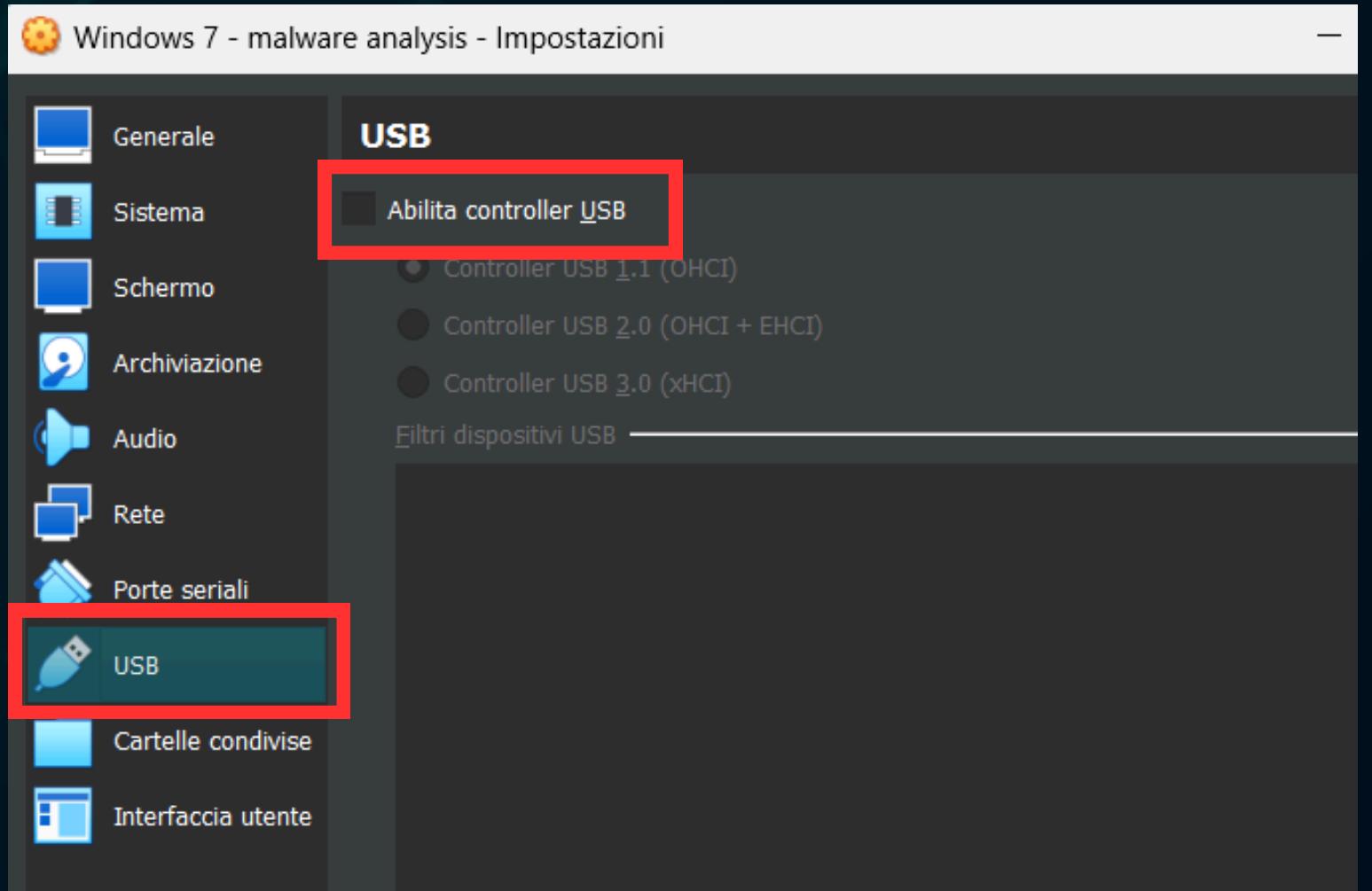
Con riferimento al file Malware_U3_W2_L5 presente all'interno della cartella «Esercizio_Pratico_U3_W2_L5 » sul desktop della macchina virtuale dedicata per l'analisi dei malware, rispondere ai seguenti quesiti:

- 1- Quali librerie vengono importate dal file eseguibile ? Fare anche una descrizione.
- 2- Quali sono le sezioni di cui si compone il file eseguibile del malware? Fare anche una descrizione.

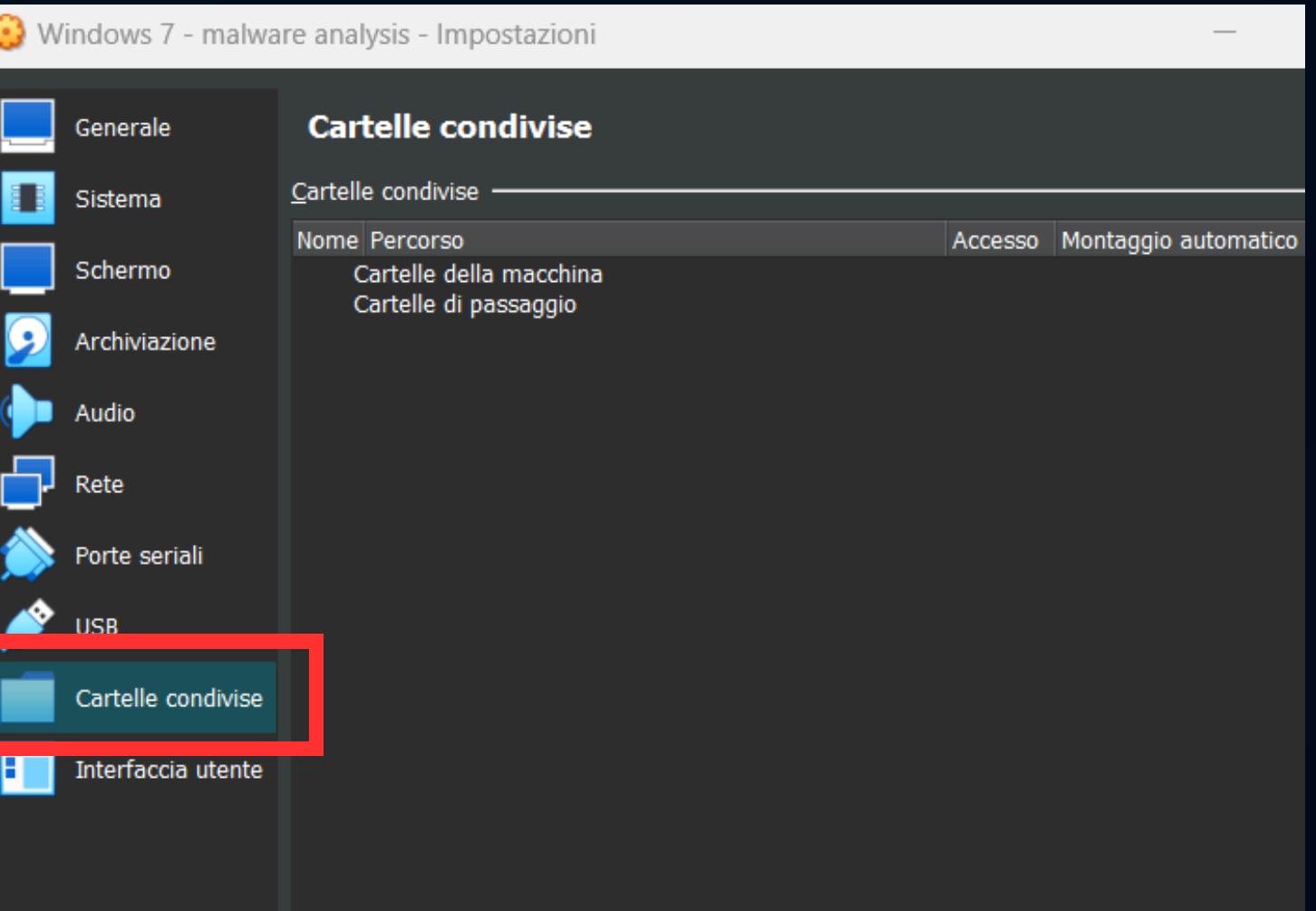
Prima di analizzare il file per verificare se è un malware devo prima impostare correttamente il mio laboratorio virtuale per non creare eventuali danni alla rete o al pc.

Da VirtualBox selezionando la macchina Windows7 e andando su impostazioni vado a disabilitare le porte USB, eliminare le cartelle condivise e cambiare la rete in rete interna.

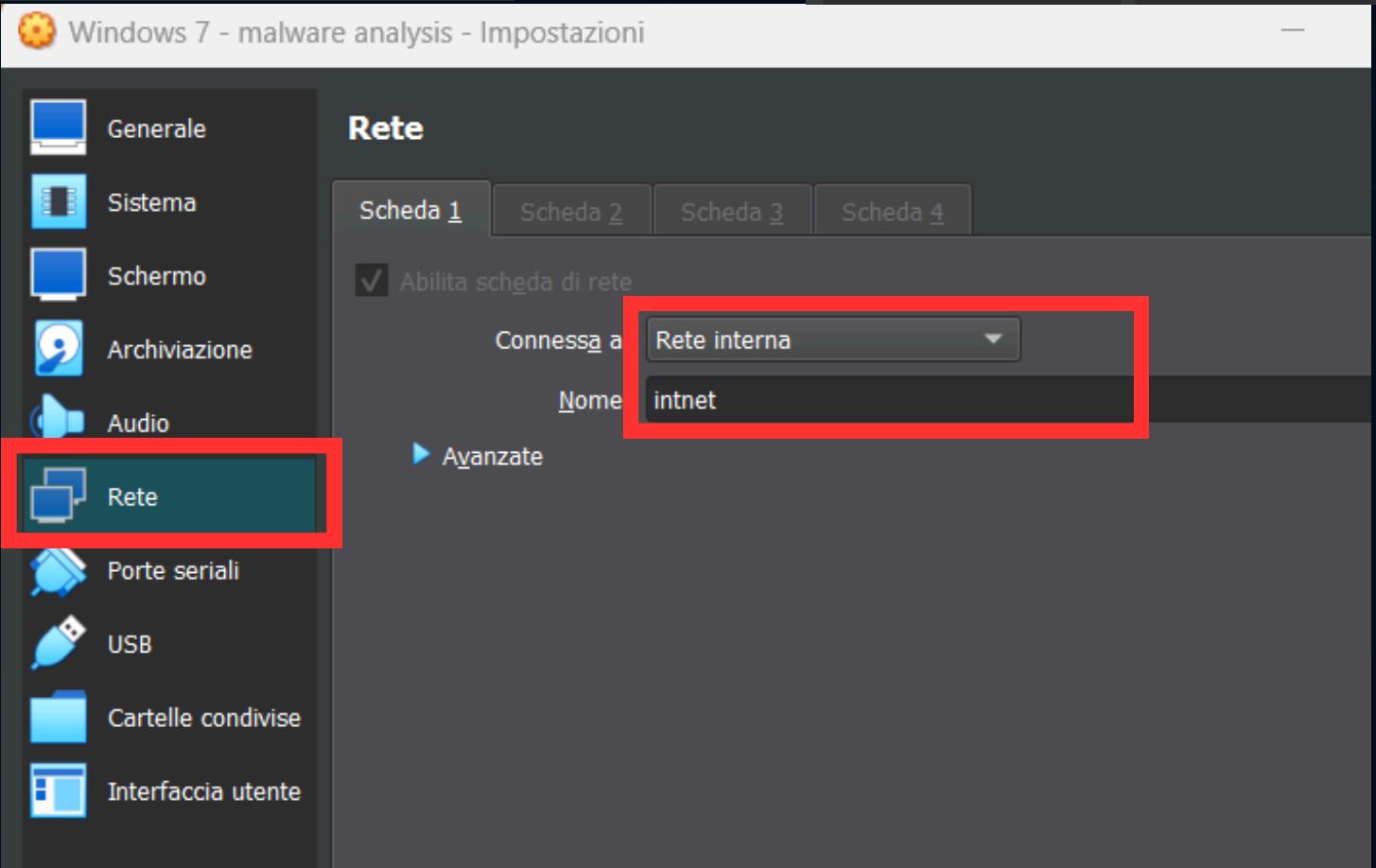




1-Disabilito controller USB

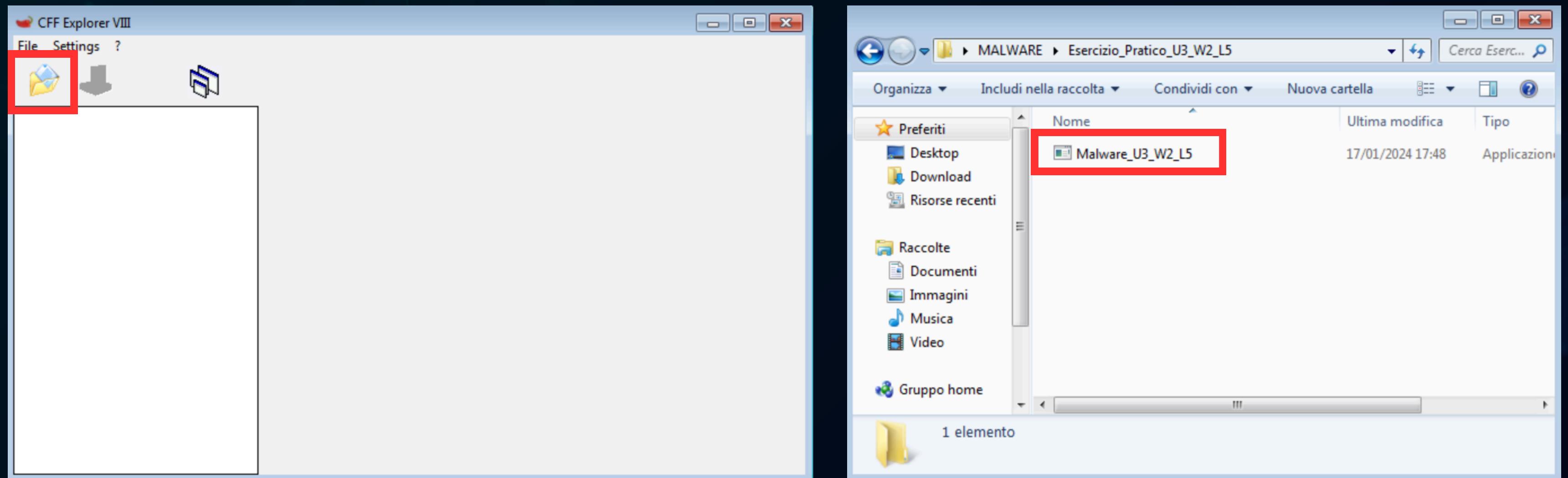


2-Rimuovo cartelle condivise

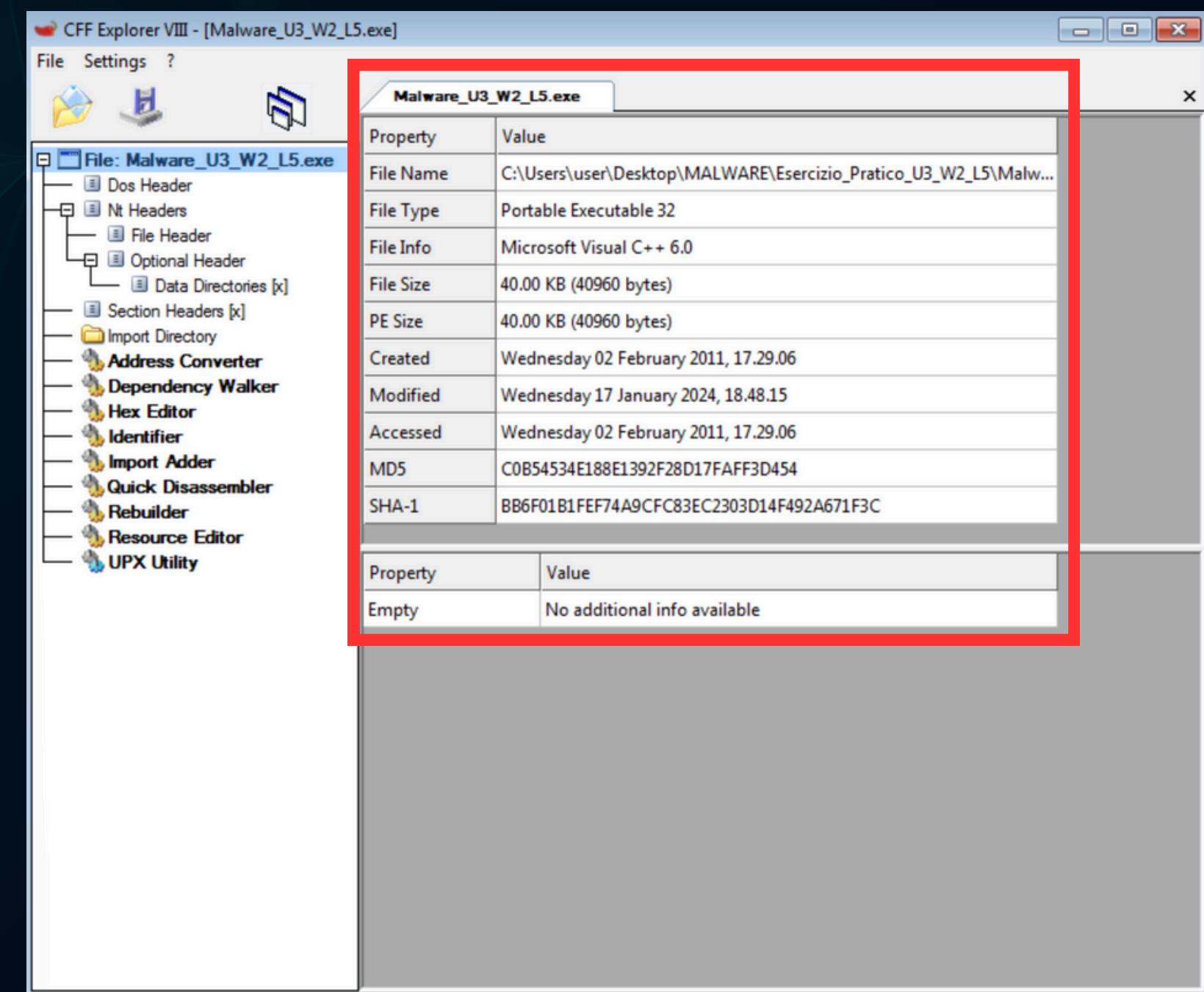


3- Rete interna

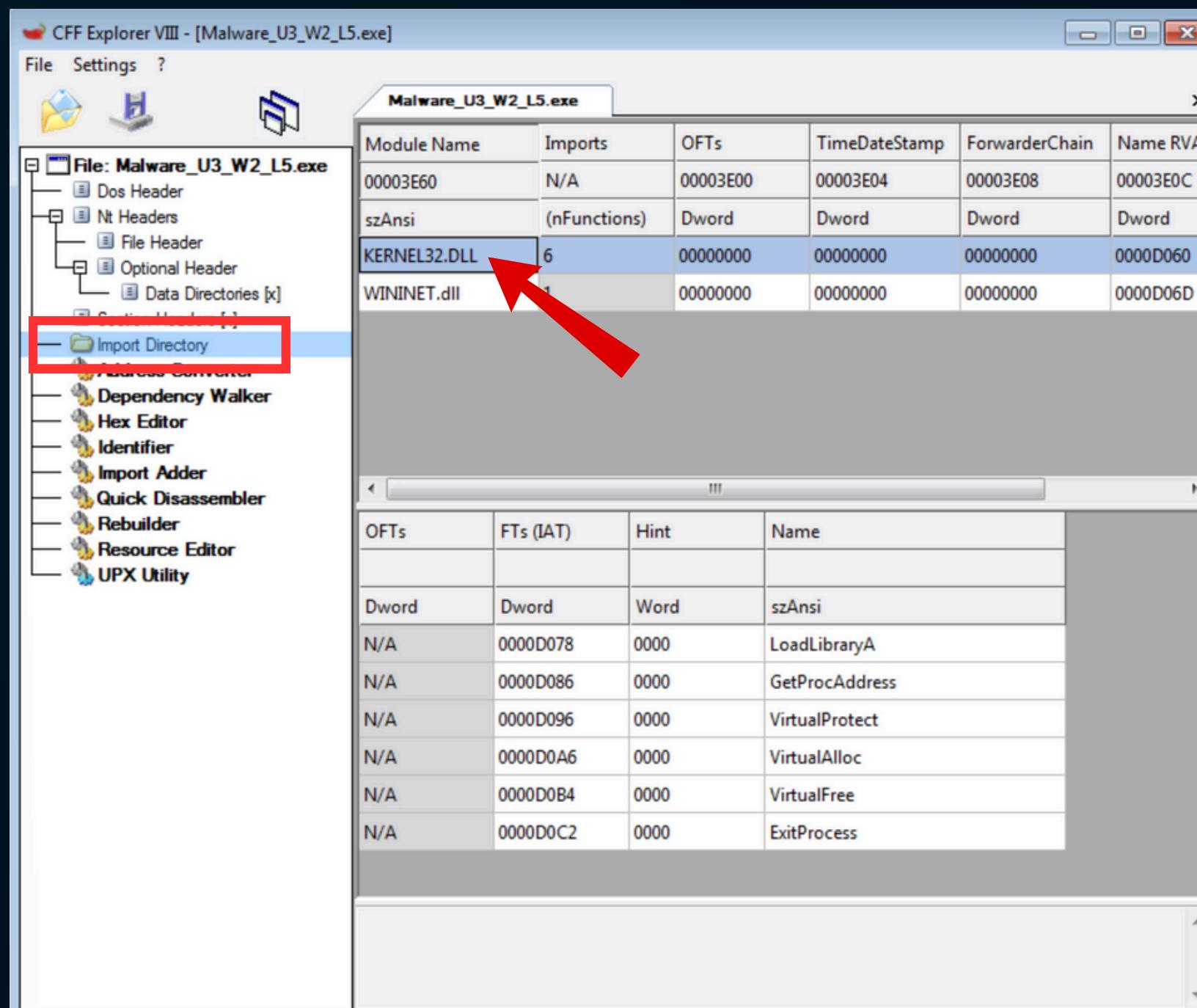
Per analizzare il malware utilizzo il programma CFF Explorer VIII che si presenta come in figura, andando a cliccare sull'icona della cartella posso aprire il file di mio interesse, Malware_U3_W2_L5



All'apertura mi verranno mostrate alcune informazioni generali riguardo il file come il tipo (Portable Executable 32), il linguaggio in cui è stato scritto (C++), le varie date di creazione, modifica e accesso e l'hash MD5, molto importante per verificare con altri programmi se si tratta di un malware. L'hash md5 si sarebbe potuto calcolare anche utilizzando il tool md5deep.

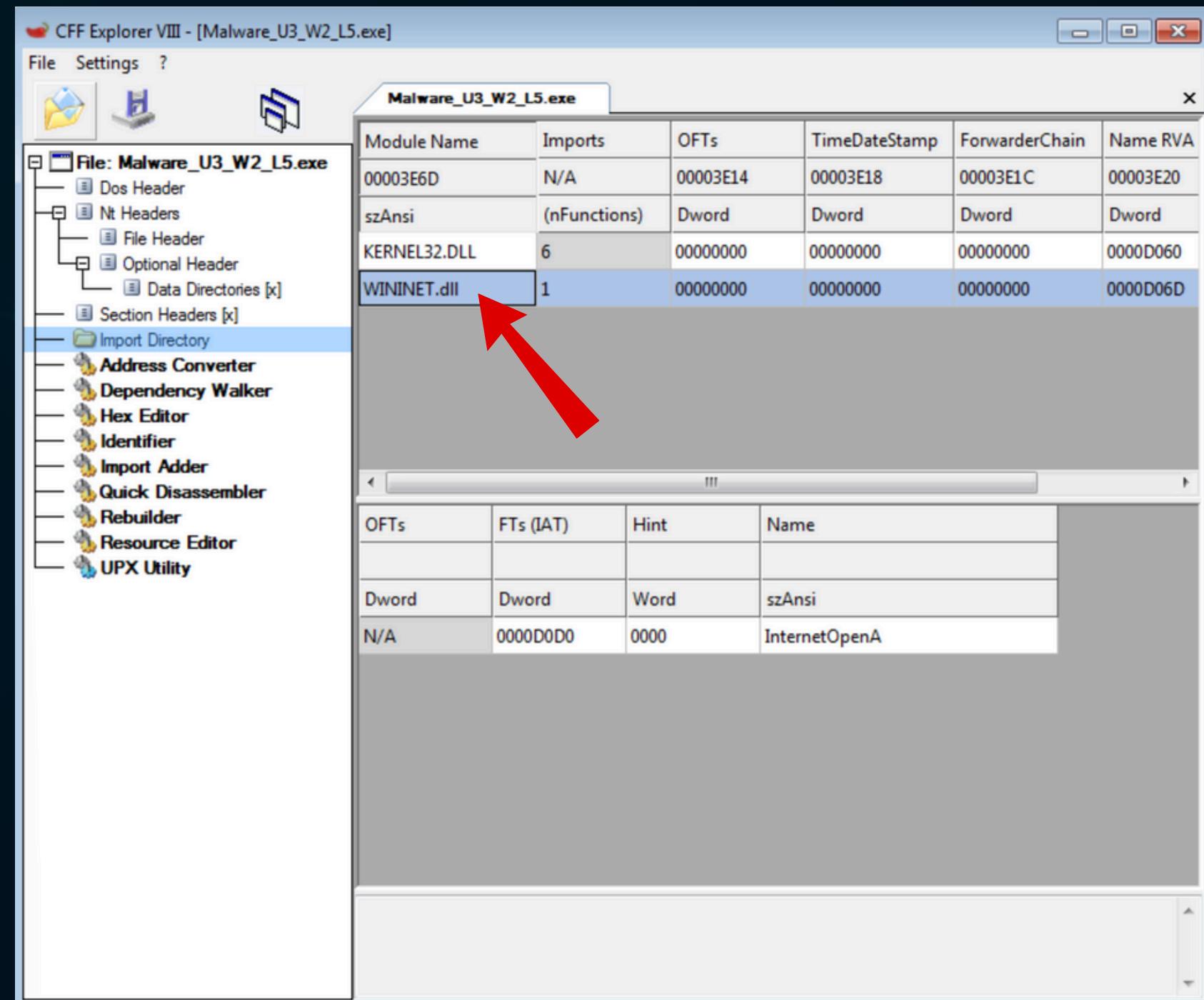


Andiamo ora ad analizzare le librerie importate dal malware andando nella sezione “Import Directory”. Possiamo notare due librerie importate: KERNEL32.DLL e WININET.dll



Kernel32.dll è una libreria dinamica fondamentale per il sistema operativo Windows. Essa fornisce un'interfaccia tra le applicazioni e il kernel del sistema operativo, offrendo una vasta gamma di funzioni per gestire operazioni di basso livello come:

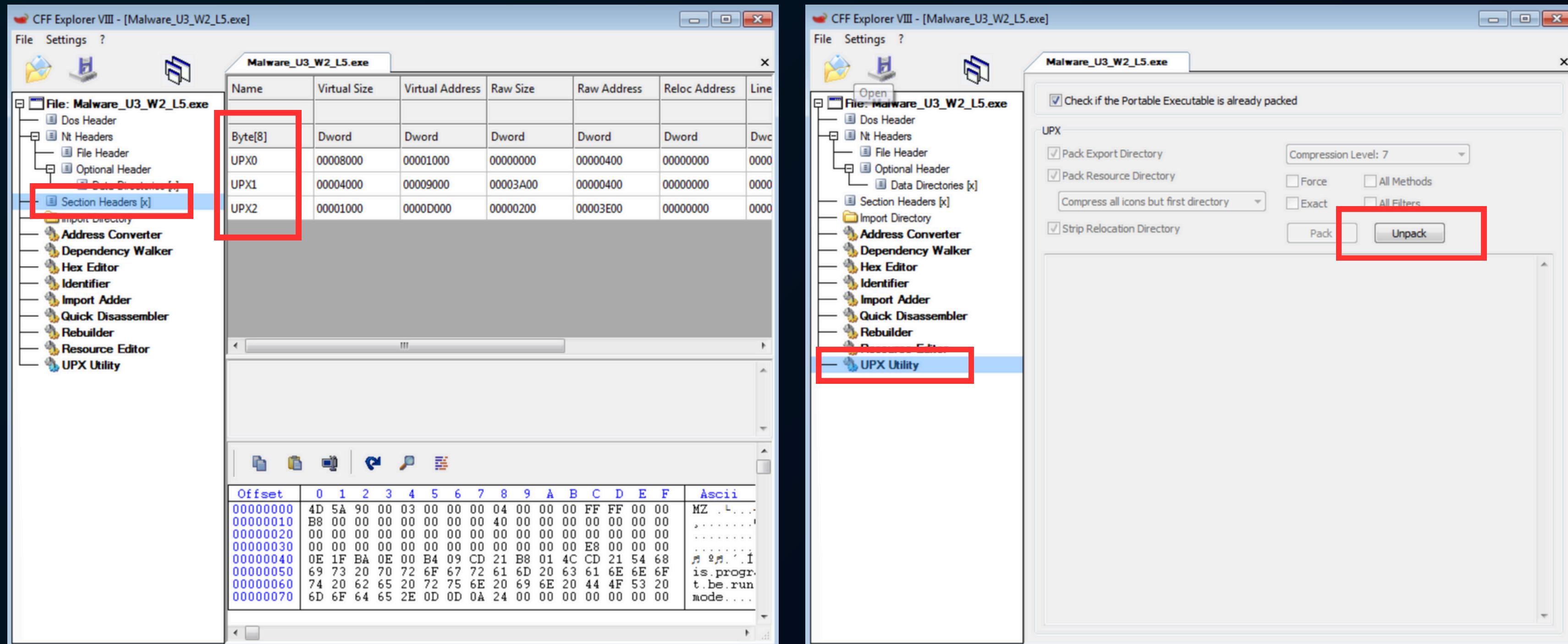
- Gestione della memoria: allocazione, deallocazione, protezione della memoria.
- Input/Output: gestione dei file, operazioni di lettura/scrittura, accesso al disco.
- Processi e thread: creazione, terminazione, sincronizzazione, gestione dei processi e dei thread.
- Gestione del tempo: timer, sleep, wait.
- Interazione con il sistema operativo: informazioni sul sistema, gestione degli errori, registrazione eventi.



WININET.dll è una libreria dinamica fondamentale per le applicazioni Windows che necessitano di interagire con Internet. Essa fornisce un'interfaccia per accedere alle risorse web utilizzando i protocolli HTTP e FTP. Funzionalità principali di WININET.dll:

- HTTP e FTP: Gestisce le richieste e le risposte per i protocolli HTTP e FTP, consentendo il download e l'upload di file.
- Cookie: Supporta la gestione dei cookie, inclusi la creazione, la lettura e la scrittura.
- Autenticazione: Fornisce meccanismi di autenticazione per accedere a risorse protette.
- Proxy: Supporta la configurazione e l'utilizzo dei proxy per l'accesso alla rete.
- Cache: Gestisce la cache delle risorse web per migliorare le prestazioni.

Andiamo ora ad analizzare le sezioni che compongono il malware andando alla voce “Section Headers”. Nel caso le sezioni fossero compresse per rendere l’analisi del malware più difficile, bisogna andare alla voce UPX Utility e cliccare su Unpack così da decomprimerle e andare a leggerne il contenuto.



CFF Explorer VIII - [Malware_U3_W2_L5.exe]

File Settings ?

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

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Line
000001E0	000001E8	000001EC	000001F0	000001F4	000001F8	0000
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dwc
.text	00004A78	00001000	00005000	00001000	00000000	0000
.rdata	0000095E	00006000	00001000	00006000	00000000	0000
.data	00003F08	00007000	00003000	00007000	00000000	0000

This section contains:

Code Entry Point: 000011B0

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	55	8B	EC	51	6A	00	6A	00	FF	15	C0	60	40	00	89	45	U iQj.j.
00000010	FC	83	7D	FC	00	74	14	68	48	70	40	00	E8	5E	01	00	ü }ü.tqh
00000020	00	83	C4	04	B8	01	00	00	00	EB	0F	68	30	70	40	00	.JÄ,
00000030	E8	4A	01	00	00	83	C4	04	33	C0	8B	E5	5D	C3	CC	CC	èJ .. Ä
00000040	55	8B	EC	81	EC	10	02	00	00	6A	00	6A	00	6A	00	6A	U i i+.
00000050	00	68	F4	70	40	00	FF	15	C4	60	40	00	89	45	F4	6A	.hôp@.ýL
00000060	00	6A	00	6A	00	6A	00	68	C4	70	40	00	8B	45	F4	50	j:j.j.h
00000070	FF	15	B4	60	40	00	89	45	F0	83	7D	F0	00	75	1E	68	ýL @ E

.rdata include generalmente le informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile

.text contiene le istruzioni (le righe di codice) che la CPU eseguirà una volta che il software sarà avviato. Generalmente questa è l'unica sezione di un file eseguibile che viene eseguita dalla CPU, in quanto tutte le altre sezioni contengono dati o informazioni a supporto.

CFF Explorer VIII - [Malware_U3_W2_L5.exe]

File Settings ?

File: Malware_U3_W2_L5.exe

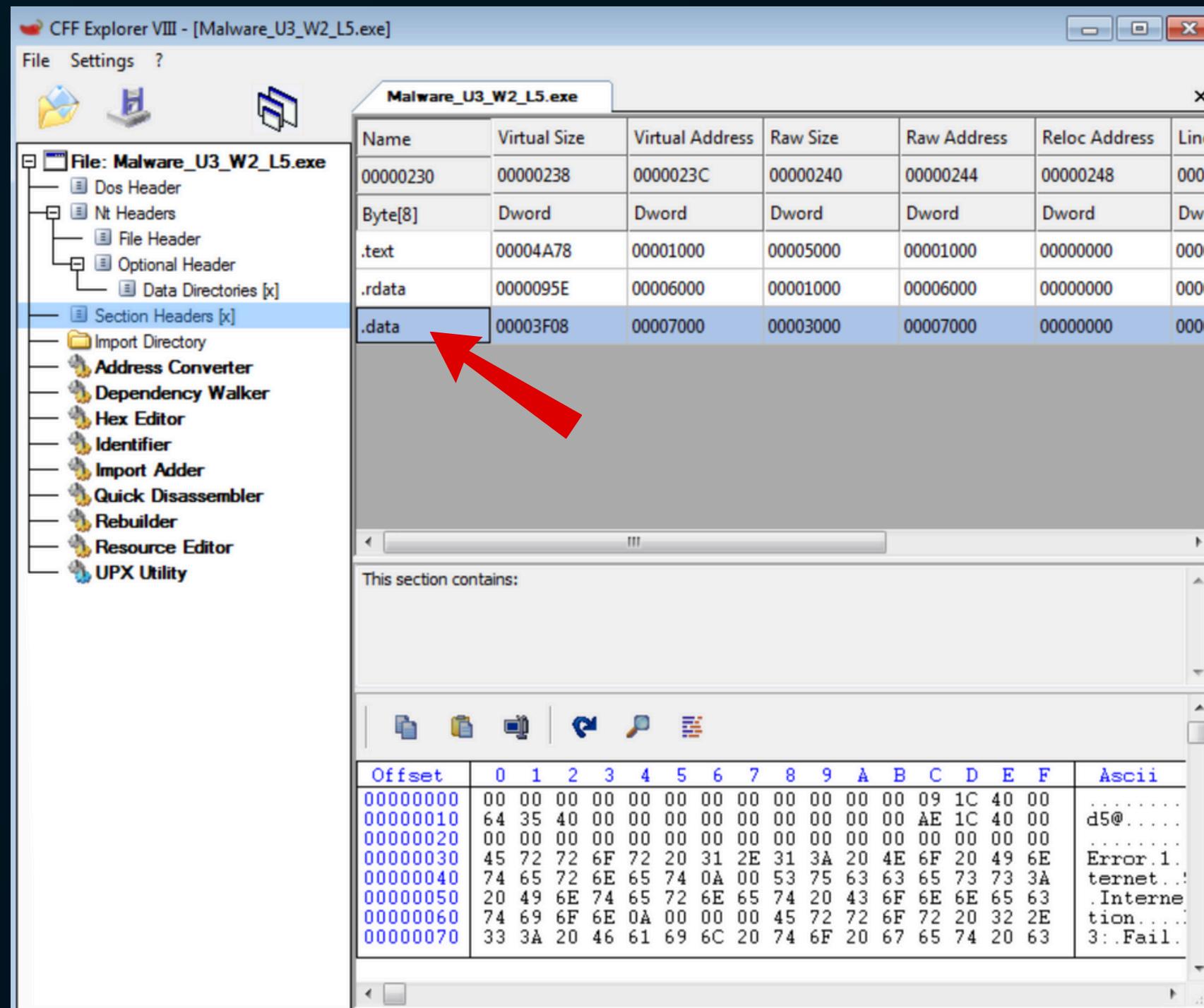
- Dos Header
- Nt Headers
 - File Header
 - Optional Header
 - Data Directories [x]
- Section Headers [x]
- Import Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Line
00000208	00000210	00000214	00000218	0000021C	00000220	0000
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dwc
.text	00004A78	00001000	00005000	00001000	00000000	0000
.rdata	0000095E	00006000	00001000	00006000	00000000	0000
.data	00003F08	00007000	00003000	00007000	00000000	0000

This section contains:

Data: 00006000
Import Directory: 000064DC

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	FE	65	00	00	06	66	00	00	14	66	00	00	24	66	00	00	be..-f..
00000010	34	66	00	00	42	66	00	00	50	66	00	00	66	66	00	00	4f..Bf..
00000020	78	66	00	00	84	66	00	00	92	66	00	00	A4	66	00	00	xf..lf..
00000030	B8	66	00	00	D2	66	00	00	E6	66	00	00	00	67	00	00	,f..Öf..
00000040	1A	67	00	00	30	67	00	00	48	67	00	00	60	67	00	00	-g..Ög..
00000050	70	67	00	00	7E	67	00	00	8C	67	00	00	9E	67	00	00	pg..~g..
00000060	B0	67	00	00	CA	67	00	00	DA	67	00	00	E8	67	00	00	*g..Eg..
00000070	F4	67	00	00	02	68	00	00	OC	68	00	00	18	68	00	00	ög..ñh..



.data: contiene tipicamente i dati / le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma. Una variabile si dice globale quando non è definita all'interno di un contesto di una funzione, ma bensì è globalmente dichiarata ed è di conseguenza accessibile da qualsiasi funzione all'interno dell'eseguibile.

Successivamente è possibile inserire il file su VirusTotal per verificare se il malware è già stato analizzato in passato e quindi inserito nel database dei file malevoli. In questo caso vediamo che si tratta effettivamente di un malware, probabilmente di un Trojan.

The image shows two screenshots of the VirusTotal website. The left screenshot shows the 'SUMMARY' tab with a red arrow pointing to a message: '40/74 security vendors flagged this file as malicious'. The right screenshot shows the 'DETECTION' tab with a red arrow pointing to the threat label 'trojan.r002c0pdm21/ymacco'. Both screenshots include a 'Community' section at the top.

VirusTotal - File - b71777edb21

VIRUSTOTAL

SUMMARY DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 7

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

40/74 security vendors flagged this file as malicious

40 / 74

Community Score

b71777edb21167c96d20ff803cbcb25d24b94b3652db2f286dc6efd3d8416a

Malware_U3_W2_L5.exe

Importa segnalibri... Getting Started

VIRUSTOTAL

SUMMARY DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 7

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat trojan.r002c0pdm21/ymacco Threat categories trojan Family labels r002c0pdm21

label

Security vendors' analysis Do you want to automate checks?

Alibaba	! Trojan:Win32/Generic.2cc376c1
AliCloud	! Trojan:Win/Ymacco.AMH1
Antiy-AVL	! Trojan/Win32.BTSGeneric
Avast	! Win32:PUP-gen [PUP]
AVG	! Win32:PUP-gen [PUP]
CrowdStrike Falcon	! Win/malicious_confidence_100% (W)
Cylance	! Unsafe
DeepInstinct	! MALICIOUS
DrWeb	! Trojan.MulDrop7.63090
Elastic	! Malicious (moderate Confidence)
ESET-NOD32	! Win32/Agent.WOO
Fortinet	! W32/Agent.WOO!tr

Importa segnalibri... Getting Started

Su VirusTotal possiamo reperire molte informazioni riguardo il file, alcune le avevamo già evidenziate con CFF Explorer come le sezioni, le librerie importate e l'hash del file

The image shows two side-by-side screenshots of the VirusTotal analysis interface for the file b71777edbf21167c96d20ff803cbcb2.

Left Screenshot (Basic Properties):

- Basic properties:**
 - MD5: c0b54534e188e1392f28d17faff3d454
 - SHA-1: bb6f01b1fef74a9fcf83ec2303d14f492a671f3c
 - SHA-256: b71777edbf21167c96d20ff803cbcb25d24b94b3652db2f286dc6efd3d8416a
 - Vhash: 044036651d1az2crz5bz
 - Authentihash: a8ca4bd7f0eeeca509d0cab34b123894fb81ccfdadeafde39228f9e660522686
 - Imphash: 30146c4b4aedc56db4852f147883b9a0
 - Rich PE header hash: 684f866cc4786b48eedc2e55578ee968
 - SSDEEP: 384:5PvvWL94iMg9IVrpf6lXT2pCcea0dNDJXdhcYfydyNugreAWoWv:ubvONpf6FT2Qvh...
 - TLSH: T1C0036C2779E14077C482C6B090B6CF2AFB7B663303528187CB542A5A3E319E5EA36...
 - File type: Win32 EXE (executable, windows, win32, pe, pexe)
 - Magic: PE32 executable (console) Intel 80386, for MS Windows
 - TrID: Win32 Executable MS Visual C++ (generic) (36.8%) | Microsoft Visual C++ compiled ex...
 - DetectItEasy: PE32 | Compiler: EP:Microsoft Visual C/C++ (6.0 (1720-9782)) [EXE32] | Compiler: Mi...
 - Magika: PEBIN
 - File size: 40.00 KB (40960 bytes)
 - PEiD packer: Microsoft Visual C++
- History:** Creation Time: 2011-02-02 21:29:05 UTC

Right Screenshot (File Details):

- Header:**
 - Target Machine: Intel 386 or later processors and compatible processors
 - Compilation Timestamp: 2011-02-02 21:29:05 UTC
 - Entry Point: 4528
 - Contained Sections: 3
- Sections:** A table showing file sections with columns: Name, Virtual Address, Virtual Size, Raw Size, Entropy, MD5, and Chi2. The sections listed are .text, .rdat, a, and .data.
- Imports:** A list showing imports from KERNEL32.dll and WININET.dll.

In conclusione il malware effettua anche delle connessioni a domini e IP probabilmente malevoli

VIRUSTOTAL

Domain	Detections	Created	Registrar
132.155.190.20.in-addr.arpa	2 / 93	-	-
150.32.88.40.in-addr.arpa	0 / 93	-	-
16.155.190.20.in-addr.arpa	1 / 93	-	-
24.78.0.192.in-addr.arpa	0 / 93	-	-
25.78.0.192.in-addr.arpa	1 / 93	-	-
29.91.21.72.in-addr.arpa	1 / 93	-	-
48.193.43.104.in-addr.arpa	1 / 93	-	-
login.live.com	0 / 93	1994-12-28	CSC CORPORATE DOMAINS, INC.
practicalmalwareanalysis.com	0 / 93	2011-01-22	GoDaddy.com, LLC
prda.aadg.msidentity.com	0 / 93	2016-03-21	MarkMonitor Inc.
r3.o.lencr.org	0 / 93	2020-06-29	CloudFlare, Inc.
windowsupdate.s.llnwi.net	0 / 93	2013-07-31	GoDaddy.com, LLC
www.microsoft.com	0 / 93	1991-05-02	MarkMonitor Inc.
www.practicalmalware-analysis.com	3 / 93	2011-01-22	GoDaddy.com, LLC
x1.o.lencr.org	0 / 93	2020-06-29	CloudFlare, Inc.

Contacted IP addresses (48) ⓘ

IP	Detections	Autonomous System	Country
104.65.174.220	0 / 93	20940	US
104.80.88.81	0 / 93	20940	US
104.80.88.97	0 / 93	20940	US
104.98.118.138	0 / 93	20940	US
104.98.118.155	0 / 93	20940	US
104.99.72.226	0 / 93	20940	US
114.114.114.114	2 / 93	21859	CN
13.107.4.50	8 / 93	8068	US
15.197.142.173	1 / 93	16509	US
192.0.78.24	0 / 93	2635	US

Esercizio 2: Identificare i costrutti noti, ipotizzare il comportamento della funzionalità implementata e fare una tabella per spiegare il significato delle singole righe di codice

```
1 push    ebp
2 mov     ebp, esp
3 push    ecx
4 push    0; dwReserved
5 push    0; lpdwFlags
6 call    ds:InternetGetConnectedState
7 mov     [ebp+var_4], eax
8 cmp     [ebp+var_4], 0
9 jz      short loc_40102B
10 push   offset aSuccessInterne ;
11 call   sub_40105F
12 add    esp, 4
13 mov    eax, 1
14 jmp    short loc_40103A
15 loc_40102B:
16 push   offset aError1_1NoInte
17 call   sub_40117F
18 add    esp, 4
19 xor    eax, eax
20 loc_40103A:
21 mov    esp, ebp
22 pop    ebp
23 retn
24 sub_401000 endp
```

Differenza tra codice assembly x86 e C

```
1 #include <windows.h>
2
3 int CheckInternetConnection() {
4     DWORD dwFlags = 0;
5     DWORD dwReserved = 0;
6
7     if (InternetGetConnectedState(&dwFlags, &dwReserved)) {
8         # c'è connessione
9         return 1;
10    } else {
11        # non c'è connessione
12        return 0;
13    }
14 }
```

Costrutti

1	push	ebp	Creazione del frame di stack
2	mov	ebp, esp	
3	push	ecx	
4	push	0; dwReserved	Le due istruzioni di push mi preparano i parametri necessari alla funzione
5	push	0; lpdwFlags	
6	call	ds:InternetGetConnectedState	Chiamata a funzione InternetGetConnectedState
7	mov	[ebp+var_4], eax	
8	cmp	[ebp+var_4], 0	
9	jz	short loc_40102B	Salto condizionale se condizione vera (if in C)
10	push	offset aSuccessInterne ;	Il push mi prepara il parametro per la funzione
11	call	sub_40105F	Chiamata a funzione (connessione presente)
12	add	esp, 4	Pulizia stack e setta valore ritorno a 1
13	mov	eax, 1	
14	jmp	short loc_40103A	Salto se la condizione precedente è falsa
15	loc_40102B:		
16	push	offset aError1_1NoInte	push del parametro che serve alla funzione
17	call	sub_40117F	Chiamata a funzione (connessione assente)
18	add	esp, 4	Pulizia stack e setta valore ritorno a 1
19	xor	eax, eax	
20	loc_40103A:		
21	mov	esp, ebp	Rimozione del frame di stack
22	pop	ebp	
23	retn		Termine della subroutine e ritorno al codice che l'ha invocata
24	sub_401000	endp	

- Azioni sullo stack
- Salti
- Chiamate

```
1 push    ebp
2 mov     ebp, esp
3 push    ecx
4 push    0; dwReserved
5 push    0; lpdwFlags
6 call    ds:InternetGetConnectedState
7 mov     [ebp+var_4], eax
8 cmp     [ebp+var_4], 0
9 jz      short loc_40102B
10 push   offset aSuccessInterne ;
11 call   sub_40105F
12 add    esp, 4
13 mov    eax, 1
14 jmp    short loc_40103A
15 loc_40102B:
16 push   offset aError1_1NoInte
17 call   sub_40117F
18 add    esp, 4
19 xor    eax, eax
20 loc_40103A:
21 mov    esp, ebp
22 pop    ebp
23 retn
24 sub_401000 endp
```

La funzione InternetGetConnectedState svolge l'operazione di verifica di connessione di rete e salva il risultato della verifica in una variabile locale:

- Se la connessione è attiva, chiama la funzione sub_40105F e restituisce il valore 1
- Se la connessione non è attiva, chiama la funzione sub_40117F e restituisce il valore 0

Il codice non fornisce le definizioni delle funzioni sub_40105F e sub_40117F, quindi non possiamo determinare esattamente cosa fanno. Tuttavia, possiamo fare alcune supposizioni basate sui loro nomi:

- sub_40105F: viene chiamata quando c'è una connessione a Internet e potrebbe eseguire azioni come visualizzare un messaggio di successo, avviare un'altra applicazione o connettersi a un server.
- sub_40117F: Probabilmente viene chiamata quando non c'è connessione a Internet e potrebbe eseguire azioni come visualizzare un messaggio di errore, tentare di riconnettersi o terminare l'applicazione.

Analisi del codice

push	ebp	Salva il valore del base pointer (ebp) sullo stack per poterlo ripristinare in seguito
mov	ebp, esp	Imposta il base pointer (ebp) al valore dello stack pointer (esp) per creare un nuovo frame di stack per questa funzione.
push	ecx	Salva il valore del registro ecx sullo stack per poterlo ripristinare in seguito
push	0; dwReserved	Push due valori zero sullo stack come parametri per la funzione InternetGetConnectedState. Questi parametri rappresentano rispettivamente dwReserved (un valore riservato) e lpdwFlags (un puntatore a un valore di flag)
push	0; lpdwFlags	
call	ds:InternetGetConnectedState	Chiama la funzione Windows API InternetGetConnectedState per verificare la presenza di una connessione internet. Il risultato della chiamata viene restituito nel registro eax
mov	[ebp+var_4], eax	Salva il valore restituito da InternetGetConnectedState nella variabile locale var_4 (situata a 4 byte dal base pointer).

cmp [ebp+var_4], 0

Confronta il valore della variabile var_4 con zero. Se il valore è zero, significa che non c'è connessione internet

jz short loc_40102B

Se il confronto precedente è uguale a zero (non c'è connessione), salta all'indirizzo di memoria loc_40102B

push offset aSuccessInterne ;

Pushed l'indirizzo della stringa "aSuccessInterne" sullo stack come parametro per una successiva chiamata di funzione

call sub_40105F

Chiama la funzione sub_40105F, passando come parametro l'indirizzo della stringa "aSuccessInterne"

add esp, 4

Rimuove il parametro passato alla funzione sub_40105F dallo stack

mov eax, 1

Imposta il valore del registro eax a 1 (codice di ritorno di successo connessione)

jmp short loc_40103A

Salta all'indirizzo di memoria loc_40103A, che è il punto di ritorno della funzione.

loc_40102B:	Etichetta di salto per il caso di assenza di connessione
push offset aError1_1NoInte	Push l'indirizzo della stringa aError1_1NoInte sullo stack
call sub_40117F	Chiama la funzione sub_40117F, per gestire il caso di assenza di connessione
add esp, 4	Rimuove il parametro passato alla funzione sub_40117F dallo stack
xor eax, eax	Imposta il valore di ritorno della funzione a 0 (indicando no connection)
loc_40103A:	Etichetta per il punto di ricongiunzione dopo la gestione dei casi di successo o fallimento
mov esp, ebp	Ripristina il valore del puntatore allo stack esp
pop ebp	Ripristina registro base ebp ai valori salvati all'inizio della funzione
ret	Ritorna alla funzione principale
sub_401000 endp	Fine della definizione della subroutine

BONUS

Per prima ho utilizzato il tool md5deep per calcolare l'hash del file "iexplore.exe" per confrontarlo e verificarne l'integrità online. Avvio il cmd ed eseguo il seguente codice:

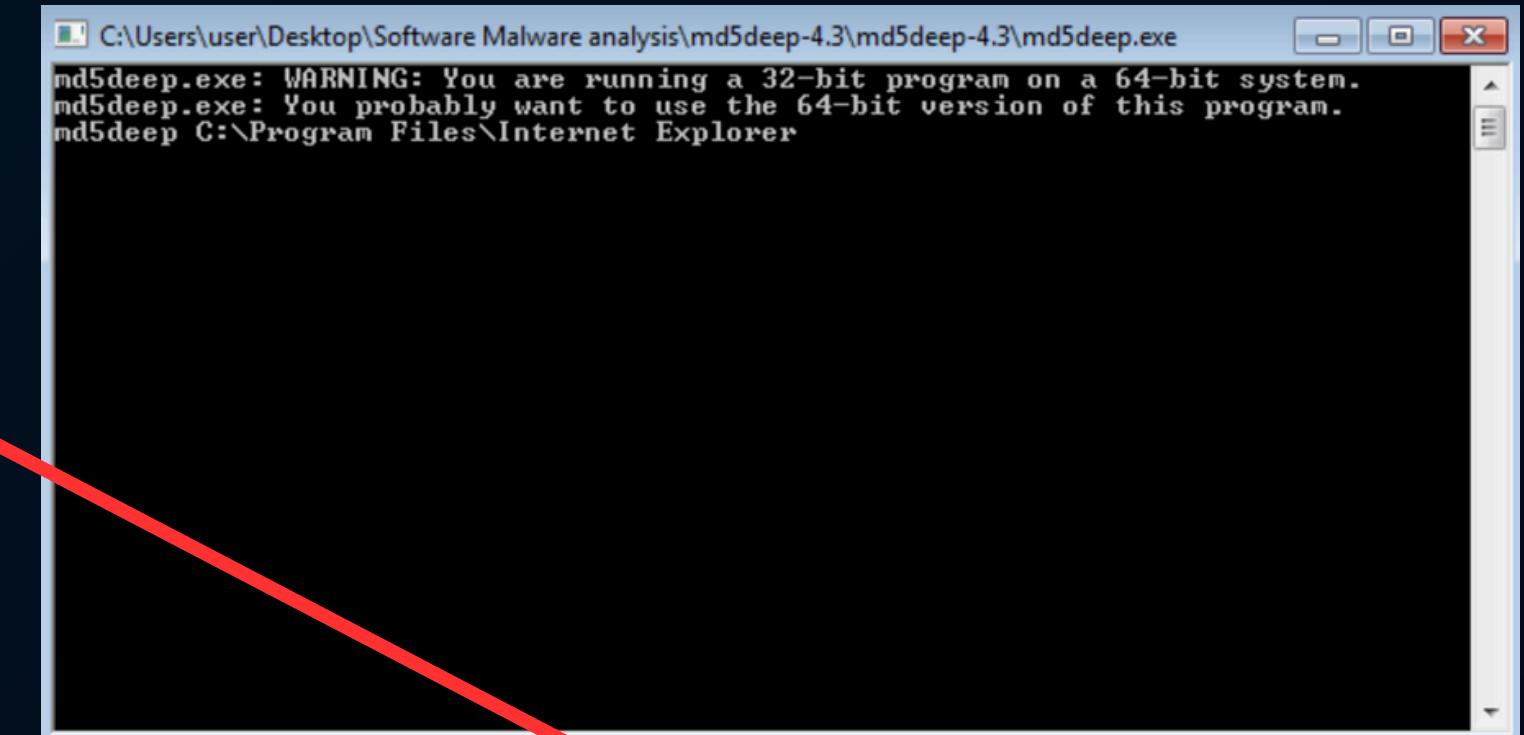
md5deep "C:\Program Files\Internet Explorer\iexplore.exe"

Come messaggio ricevo l'hash del file e vado ad inserirlo ad esempio su

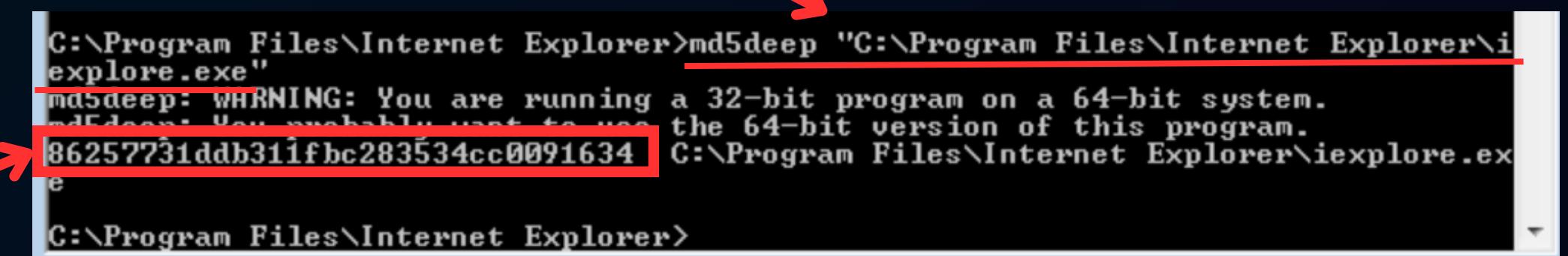
<https://opentip.kaspersky.com/>

oppure

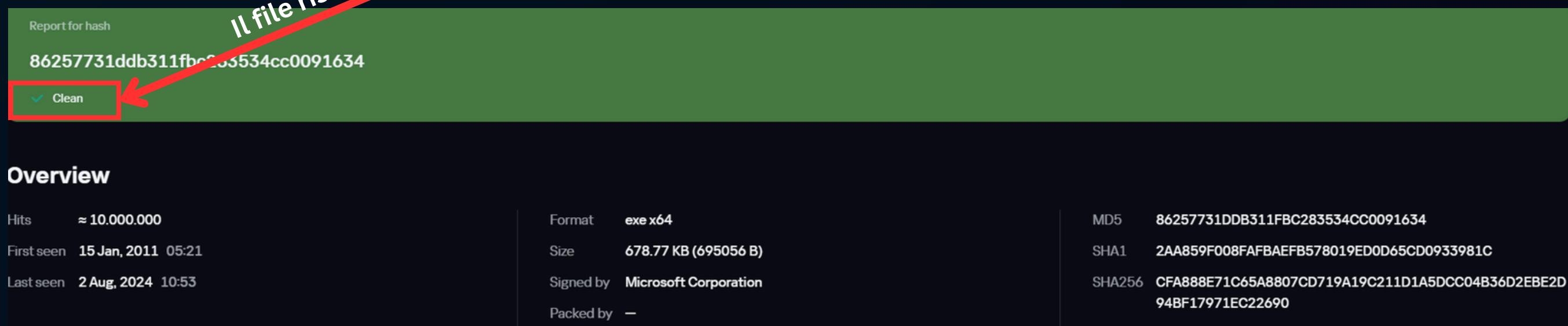
<https://www.virustotal.com/gui/home/upload>



```
C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3\md5deep-4.3\md5deep.exe
md5deep.exe: WARNING: You are running a 32-bit program on a 64-bit system.
md5deep.exe: You probably want to use the 64-bit version of this program.
md5deep C:\Program Files\Internet Explorer
```



```
C:\Program Files\Internet Explorer>md5deep "C:\Program Files\Internet Explorer\iexplore.exe"
md5deep: WARNING: You are running a 32-bit program on a 64-bit system.
md5deep: You probably want to use the 64-bit version of this program.
86257731ddb311fbc283534cc0091634 C:\Program Files\Internet Explorer\iexplore.exe
C:\Program Files\Internet Explorer>
```



Report for hash
86257731ddb311fbc283534cc0091634

Clean

Overview

Hits	~10.000.000
First seen	15 Jan, 2011 05:21
Last seen	2 Aug, 2024 10:53
Format	exe x64
Size	678.77 KB (695056 B)
Signed by	Microsoft Corporation
Packed by	-
MD5	86257731DDB311FBC283534CC0091634
SHA1	2AA859F008FAFBBAEFB578019ED0D65CD0933981C
SHA256	CFA888E71C65A8807CD719A19C211D1A5DCC04B36D2EBE2D 94BF17971EC22690

Possiamo fare anche una scansione su VirusTotal che infatti ci dice che il file è legittimo, lo possiamo notare anche dalle Signature Validation, molto importanti e sono tutte Windows

VIRUSTOTAL

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

	Do you want to automate checks?
Lionic	!
Acronis (Static ML)	Undetected
AhnLab-V3	Undetected
Alibaba	Undetected
AliCloud	Undetected
ALYac	Undetected
Antiy-AVL	Undetected
Arcabit	Undetected
Avast	Undetected
AVG	Undetected
Avira (no cloud)	Undetected
Baidu	Undetected
BitDefender	Undetected
BitDefenderTheta	Undetected
Bkav Pro	Undetected

Basic properties	
MD5	86257731ddb311fbc283534cc0091634
SHA-1	2aa859f008fafbaefb578019ed0d65cd0933981c
SHA-256	cfa888e71c65a8807cd719a19c211d1a5dcc04b36d2ebe2d94bf17971ec22690
Vhash	065066651d15156550d8z381d1z31z57z7170309fz
Authentihash	cb2b877464a17ecc18fba8e72b550efb6d0bff6dd3266f98b78962b9aa3a9b1b
Imphash	2b84b899b6f300d0016ed11889c0ae02
Rich PE header has...	9305e490a8b829c41a61650bbecdb45c
SSDeep	12288:VxrPX+pd167QhE0s7+jM+M6ugRfMMkIM7ovX+pd167QhE0u7+F:TE6Ehg7mM+M6...
TLSH	T14AE49D42F3C0A4D6D4AA46704A77DB741663BC7998144B2F32A8B65F3D313C36936...
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32+ executable (GUI) x86-64, for MS Windows
TrID	Windows Control Panel item (generic) (58.9%) Microsoft Visual C++ compiled execut...
DetectItEasy	PE64 Compiler: Microsoft Visual C/C++ (15.00.30729) [LTCG/C++] Linker: Microsof...
Magika	CT_PEBIN
File size	678.77 KB (695056 bytes)

Signature info

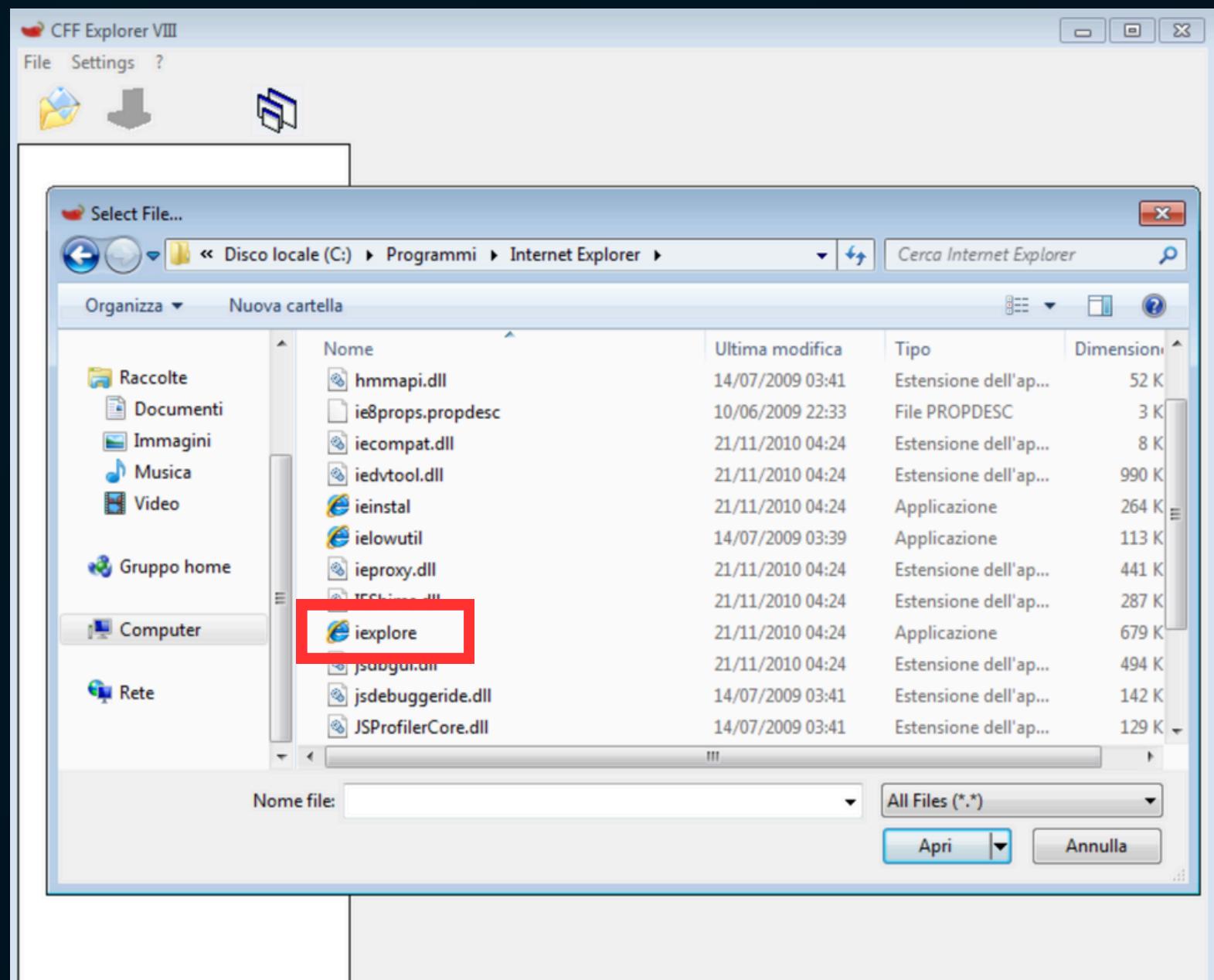
Signature Verification

Signed file, valid signature

File Version Information

Copyright	© Microsoft Corporation. All rights reserved.
Product	Windows® Internet Explorer
Description	Internet Explorer
Original Name	IEXPLORE.EXE
Internal Name	iexplore
File Version	8.00.7601.17514 (win7sp1_rtm.101119-1850)
Date signed	2010-11-20 12:28:00 UTC

Aprendo il file su CFF Explorer sembra non si tratti di un malware...



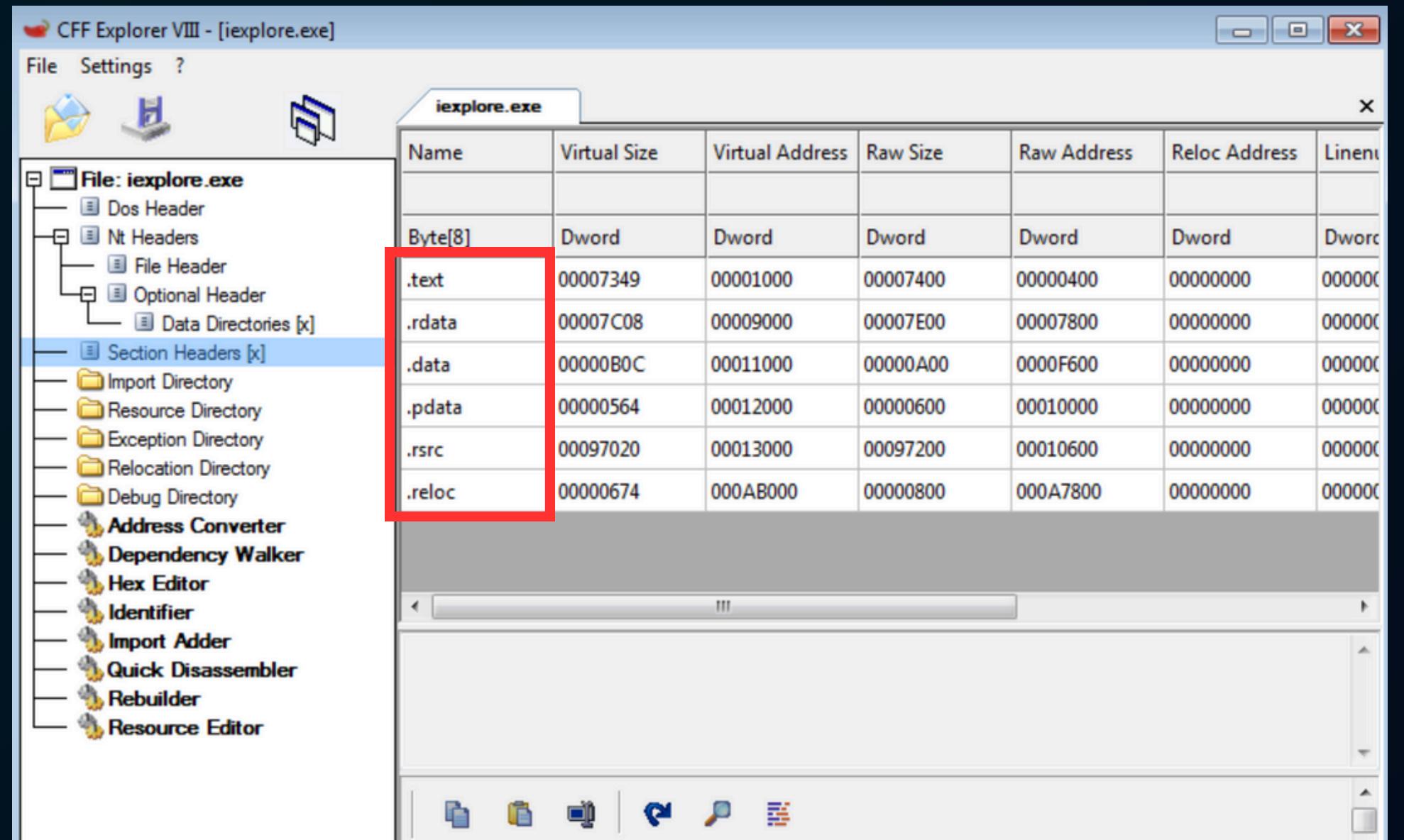
Property	Value
File Name	C:\Program Files\Internet Explorer\iexplore.exe
File Type	Portable Executable 64
File Info	Microsoft Visual C++ 8.0 (DLL)
File Size	678.77 KB (695056 bytes)
PE Size	672.00 KB (688128 bytes)
Created	Sunday 21 November 2010, 05.24.43
Modified	Sunday 21 November 2010, 05.24.43
Accessed	Sunday 21 November 2010, 05.24.43
MD5	86257731DDB31FBC283534CC0091634
SHA-1	2AA859F008FAFBABE5B578019ED0D65CD0933981C

Property	Value
CompanyName	Microsoft Corporation
FileDescription	Internet Explorer
FileVersion	8.00.7601.17514 (win7sp1_rtm.101119-1850)
InternalName	iexplore
LegalCopyright	© Microsoft Corporation. All rights reserved.
OriginalFilename	IEXPLORE.EXE
ProductName	Windows® Internet Explorer

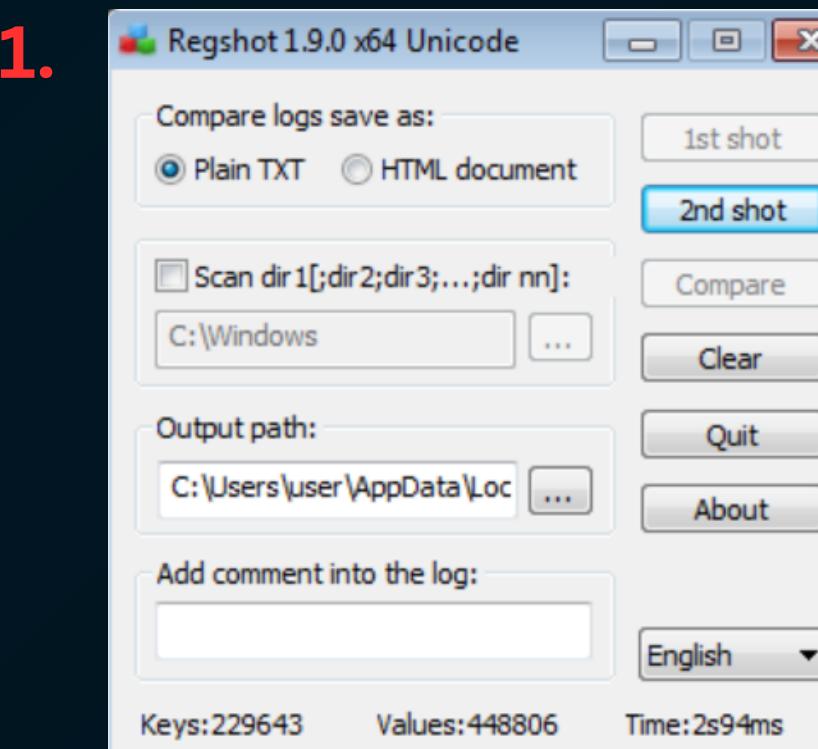
Vengono importate diverse librerie ma sono tutte necessarie al programma per funzionare, ad esempio:

Module Name	Imports	OFTs	TimeStamp
szAnsi	(nFunctions)	Dword	Dword
ADVAPI32.dll	13	0000F6B8	FFFFFF
KERNEL32.dll	56	0000F728	FFFFFF
USER32.dll	9	0000F8F0	FFFFFF
msvcrt.dll	29	0000F940	FFFFFF
ntdll.dll	3	0000FA30	FFFFFF
SHLWAPI.dll	23	0000FA50	FFFFFF
SHELL32.dll	7	0000FB10	FFFFFF
ole32.dll	5	0000FB50	FFFFFF
iertutil.dll	14	0000FB80	FFFFFF
urlmon.dll	3	0000FBF8	FFFFFF

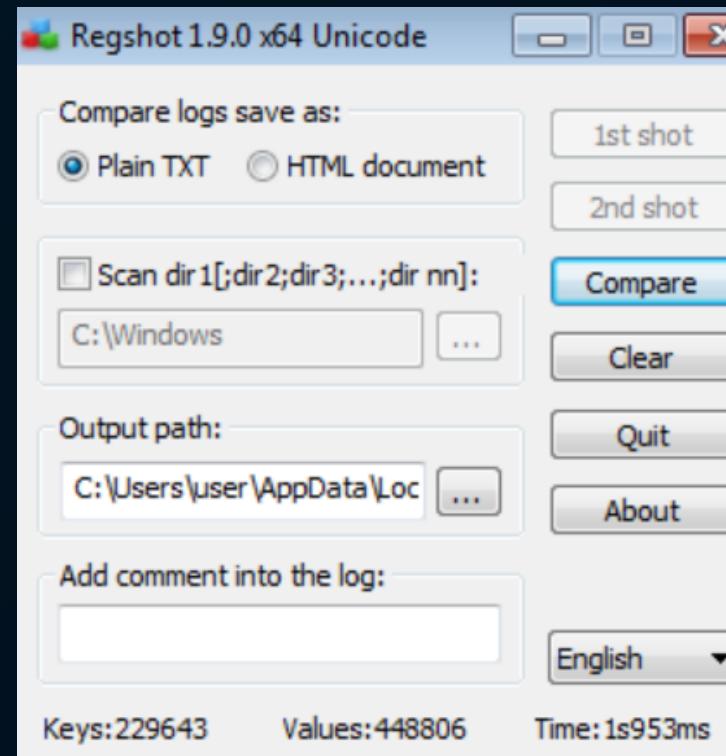
- Kernel32.dll: Fornisce funzioni di base per l'interazione con il sistema operativo, come la gestione della memoria e l'accesso ai file.
- User32.dll: Fornisce funzioni per l'interazione con la finestra dell'utente, come la creazione di finestre, la gestione degli eventi e la visualizzazione di elementi grafici.
- Gdi32.dll: Fornisce funzioni per la grafica bidimensionale, come il disegno di linee, forme e testo.
- Comdlg32.dll: Fornisce funzioni per le comuni finestre di dialogo, come la finestra "Apri" e la finestra "Salva con nome".
- Shell32.dll: Fornisce funzioni per l'interfaccia utente di Windows Explorer e per l'interazione con il desktop.
- Ole32.dll: Fornisce funzioni per la creazione e la gestione di oggetti COM (Component Object Model).
- Wininet.dll: Fornisce funzioni per la connessione a Internet e la gestione delle richieste HTTP.



Anche nelle sezioni che compongono il programma non si
non niente di strano, ci sono normali sezioni del programma
come .text, .rdata, .data, .pdata, .rsrc, .reloc.



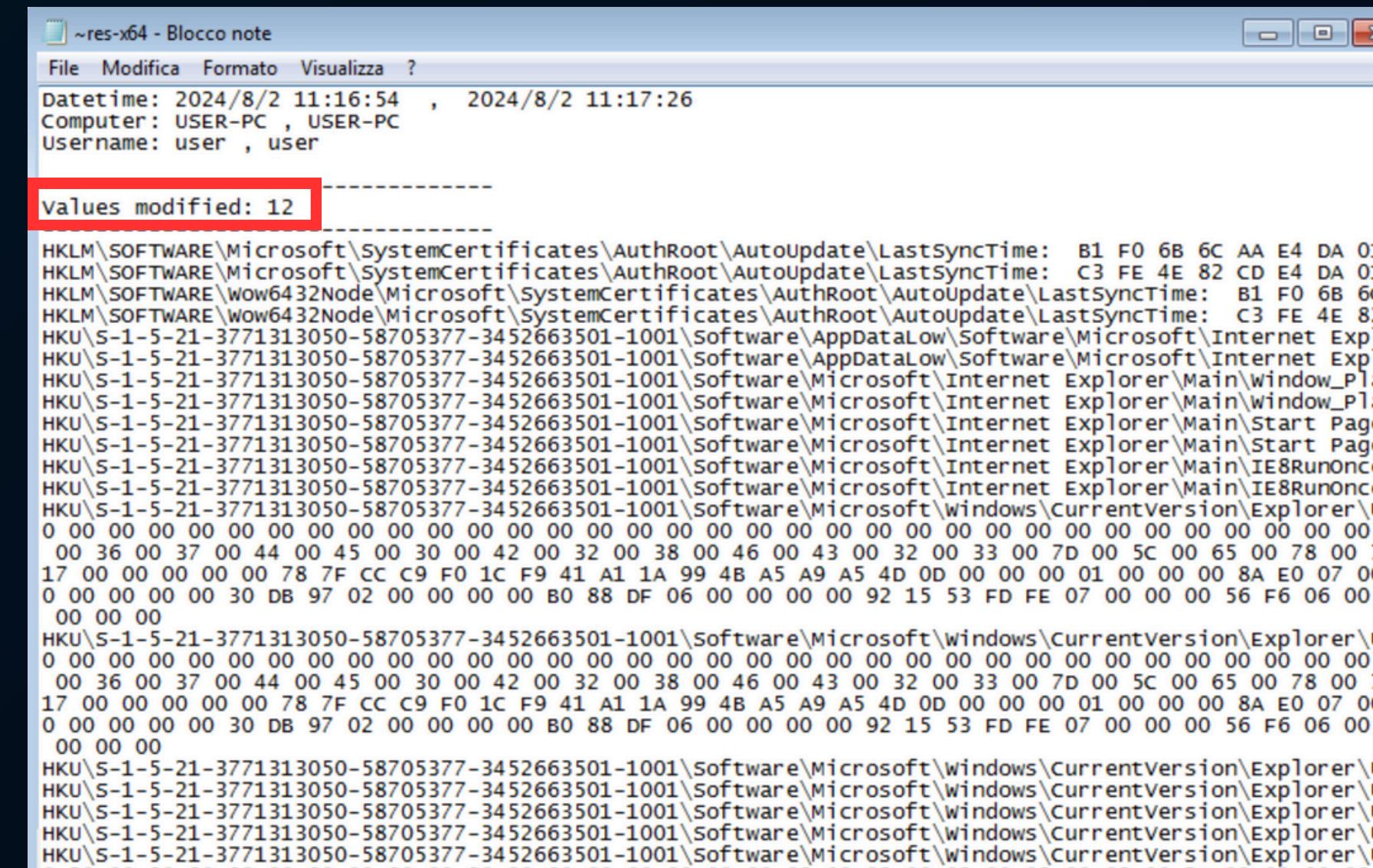
2.

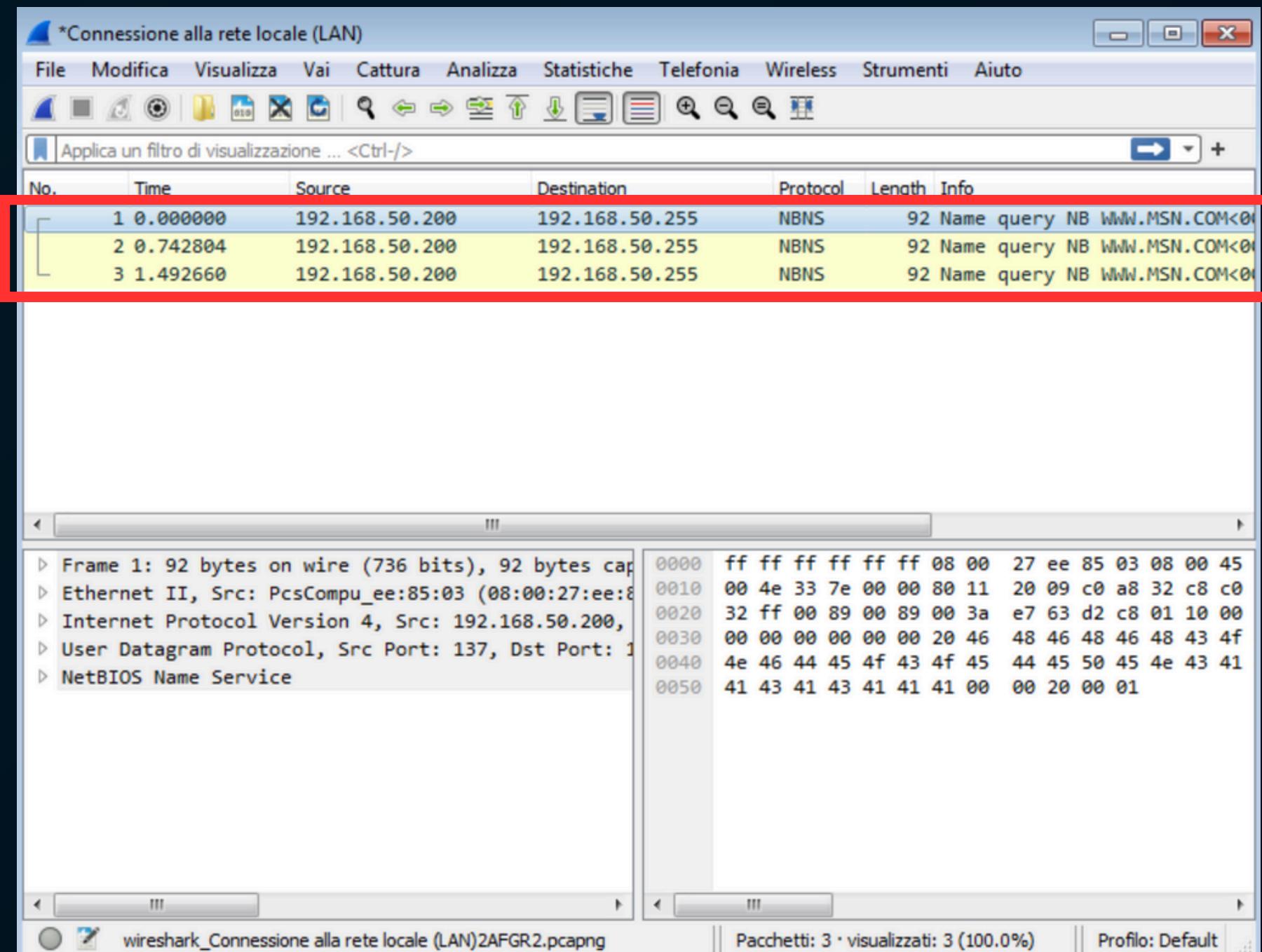


Utilizzo RegShot per una scansione delle chiavi di registro

Le chiavi di registro modificate da Internet Explorer possono variare a seconda delle impostazioni e delle estensioni installate. Alcune delle chiavi più comuni includono:

- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer: Questa chiave contiene le impostazioni specifiche dell'utente per Internet Explorer, come la pagina iniziale, i bookmark e le preferenze di sicurezza.
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer: Questa chiave contiene le impostazioni di Internet Explorer a livello di sistema.

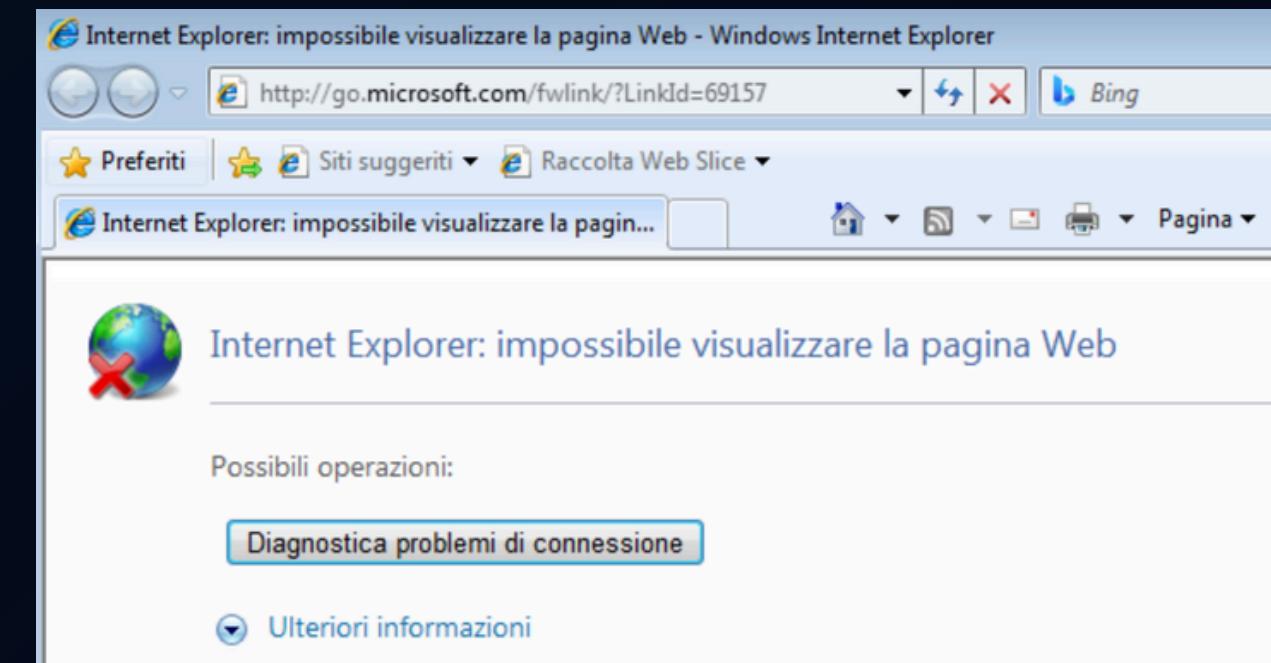




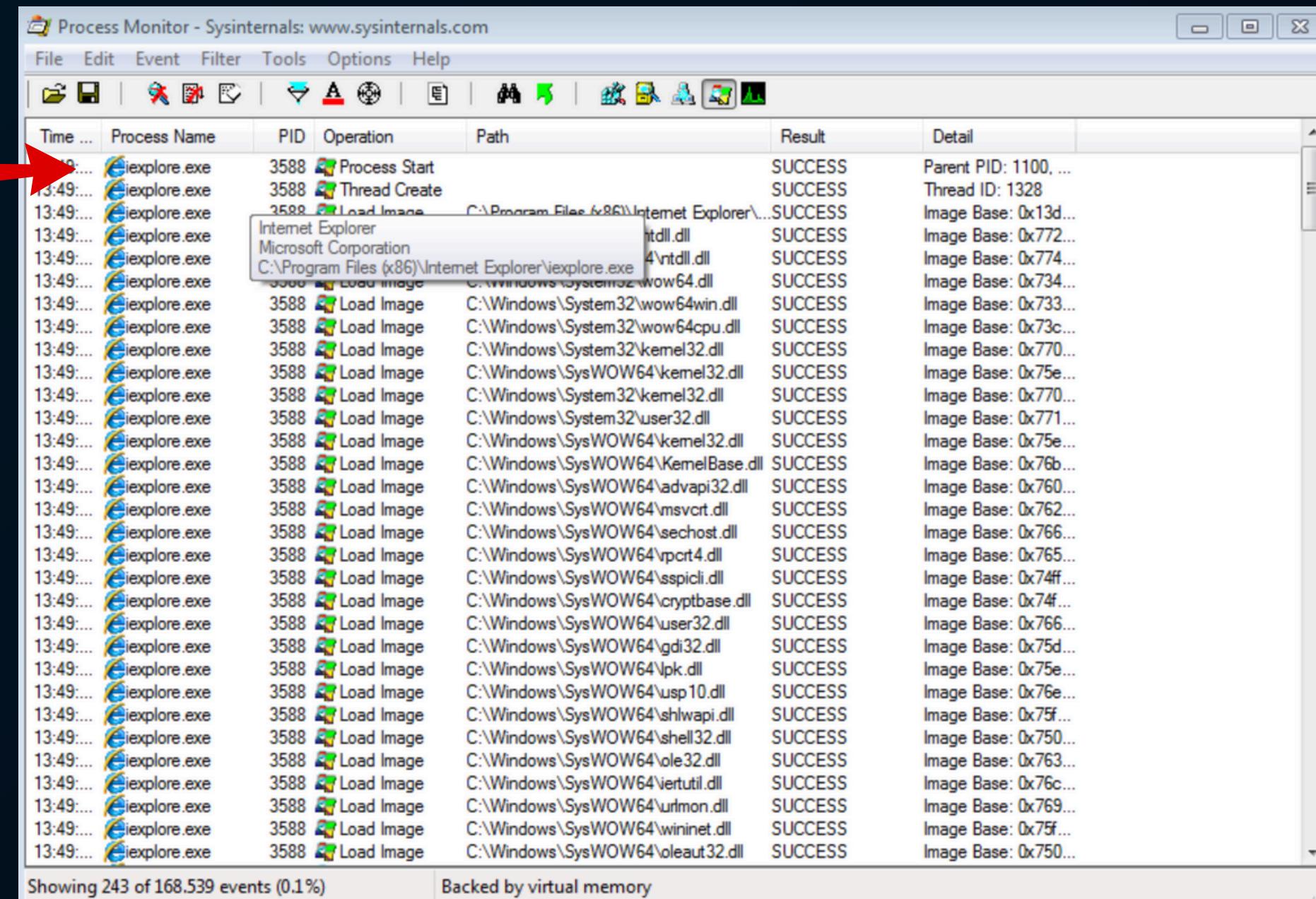
Utilizzando Wirshark possiamo notare che non viene effettuata nessuna connessione a domini malevoli o richieste ad IP “strani”

Il significato di questi pacchetti è il seguente:

- Name Query indica che si tratta di una richiesta di risoluzione di un nome. In altre parole, il tuo dispositivo sta "chiedendo" a un server qual è l'indirizzo IP associato al nome di dominio "www.msn.com".
- NB sta per "NetBIOS". NetBIOS è un protocollo di rete più vecchio, utilizzato principalmente in ambienti Windows, per la denominazione di dispositivi e servizi all'interno di una rete locale. Tuttavia, viene spesso utilizzato anche per la risoluzione di nomi DNS.
- www.msn.com: È il nome di dominio che vuoi risolvere.



Utilizzando Process Monitor posso notare che non vengono avviate chiamate per avviare altri programmi al di fuori di iexplore, ma vengono eseguiti solo i processi a lui necessari (parecchi)



A screenshot of the Process Monitor application window. The title bar reads "Process Monitor - Sysinternals: www.sysinternals.com". The main window displays a table of events. A red arrow points to the first event in the list, which is "iexplore.exe 3588 Process Start". The table has columns for Time, Process Name, PID, Operation, Path, Result, and Detail. The "Operation" column shows various system calls like "Thread Create", "Load Image", and "Process Start" for the "iexplore.exe" process. The "Path" column shows the file paths for these operations, such as "C:\Program Files\Internet Explorer\iexplore.exe" for the process start and "C:\Windows\System32\wow64.dll" for a load operation. The "Result" column is mostly "SUCCESS", and the "Detail" column provides additional information like parent PID and image base addresses.

Time	Process Name	PID	Operation	Path	Result	Detail
13:49:...	iexplore.exe	3588	Process Start		SUCCESS	Parent PID: 1100, ...
13:49:...	iexplore.exe	3588	Thread Create		SUCCESS	Thread ID: 1328
13:49:...	iexplore.exe	3588	Load Image	C:\Program Files\Internet Explorer\iexplore.exe	SUCCESS	Image Base: 0x13d...
13:49:...	iexplore.exe	3588	Load Image	ntdll.dll	SUCCESS	Image Base: 0x722...
13:49:...	iexplore.exe	3588	Load Image	4\ntdll.dll	SUCCESS	Image Base: 0x774...
13:49:...	iexplore.exe	3588	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x734...
13:49:...	iexplore.exe	3588	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x733...
13:49:...	iexplore.exe	3588	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x73c...
13:49:...	iexplore.exe	3588	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x770...
13:49:...	iexplore.exe	3588	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x75e...
13:49:...	iexplore.exe	3588	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x770...
13:49:...	iexplore.exe	3588	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x771...
13:49:...	iexplore.exe	3588	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x75e...
13:49:...	iexplore.exe	3588	Load Image	C:\Windows\SysWOW64\kernelBase.dll	SUCCESS	Image Base: 0x76b...
13:49:...	iexplore.exe	3588	Load Image	C:\Windows\SysWOW64\advapi32.dll	SUCCESS	Image Base: 0x760...
13:49:...	iexplore.exe	3588	Load Image	C:\Windows\SysWOW64\msvcr.dll	SUCCESS	Image Base: 0x762...
13:49:...	iexplore.exe	3588	Load Image	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Image Base: 0x766...
13:49:...	iexplore.exe	3588	Load Image	C:\Windows\SysWOW64\pctrl4.dll	SUCCESS	Image Base: 0x765...
13:49:...	iexplore.exe	3588	Load Image	C:\Windows\SysWOW64\sspicl.dll	SUCCESS	Image Base: 0x74f...
13:49:...	iexplore.exe	3588	Load Image	C:\Windows\SysWOW64\cryptbase.dll	SUCCESS	Image Base: 0x74...
13:49:...	iexplore.exe	3588	Load Image	C:\Windows\SysWOW64\user32.dll	SUCCESS	Image Base: 0x766...
13:49:...	iexplore.exe	3588	Load Image	C:\Windows\SysWOW64\gdi32.dll	SUCCESS	Image Base: 0x75d...
13:49:...	iexplore.exe	3588	Load Image	C:\Windows\SysWOW64\pk.dll	SUCCESS	Image Base: 0x75e...
13:49:...	iexplore.exe	3588	Load Image	C:\Windows\SysWOW64\usp10.dll	SUCCESS	Image Base: 0x76e...
13:49:...	iexplore.exe	3588	Load Image	C:\Windows\SysWOW64\shlwapi.dll	SUCCESS	Image Base: 0x75f...
13:49:...	iexplore.exe	3588	Load Image	C:\Windows\SysWOW64\shell32.dll	SUCCESS	Image Base: 0x750...
13:49:...	iexplore.exe	3588	Load Image	C:\Windows\SysWOW64\ole32.dll	SUCCESS	Image Base: 0x763...
13:49:...	iexplore.exe	3588	Load Image	C:\Windows\SysWOW64\iertutil.dll	SUCCESS	Image Base: 0x76c...
13:49:...	iexplore.exe	3588	Load Image	C:\Windows\SysWOW64\urlmon.dll	SUCCESS	Image Base: 0x769...
13:49:...	iexplore.exe	3588	Load Image	C:\Windows\SysWOW64\wininet.dll	SUCCESS	Image Base: 0x75f...
13:49:...	iexplore.exe	3588	Load Image	C:\Windows\SysWOW64\oleaut32.dll	SUCCESS	Image Base: 0x750...

Dopo queste evidenze si può affermare che il programma non è un malware ma il browser web legittimo Internet Explorer