

ANALISI STATICA BASICA

Traccia:

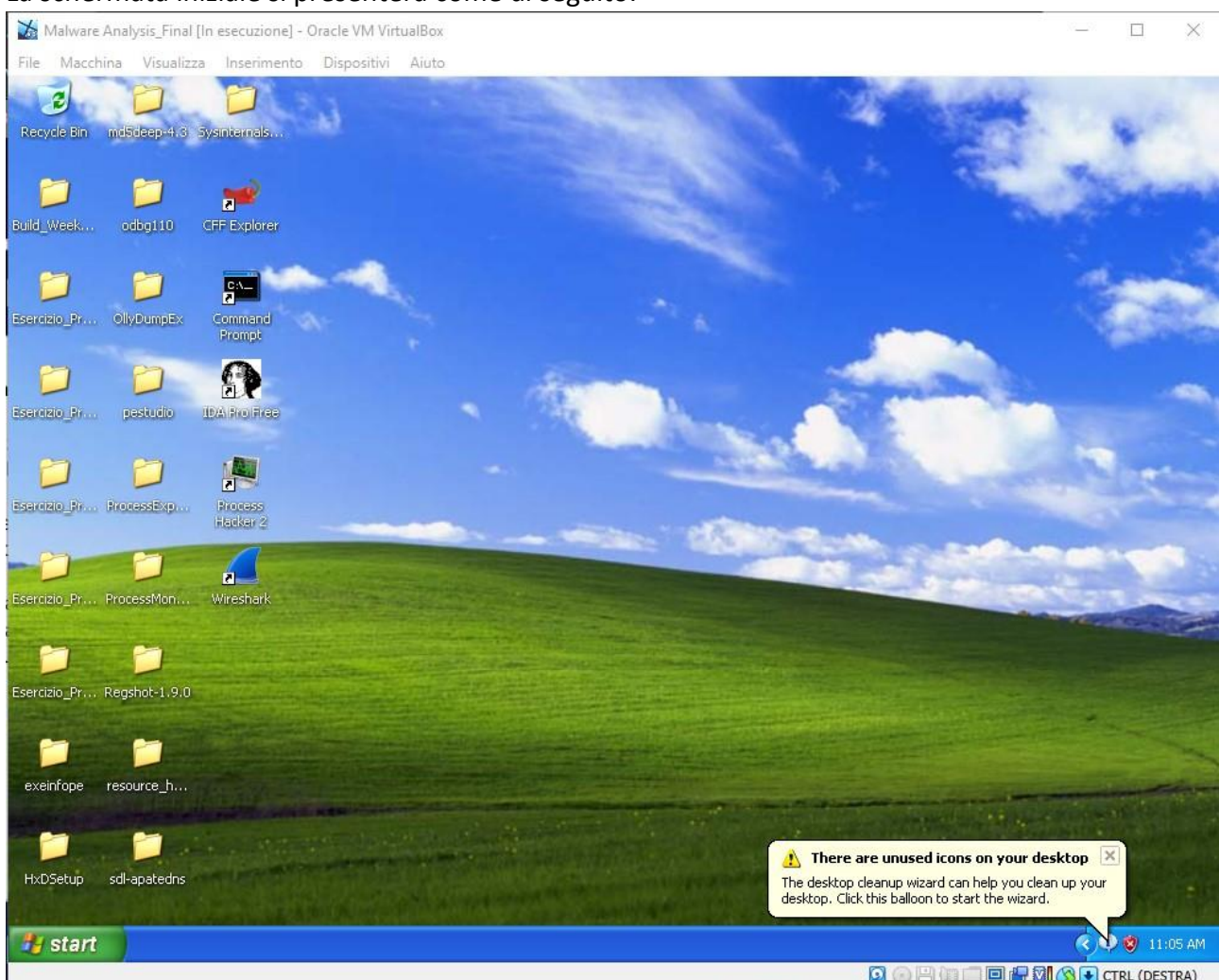
Nella lezione teorica del mattino, abbiamo visto come recuperare informazioni su un malware tramite l'analisi statica basica.

Con riferimento al file eseguibile contenuto nella cartella «**Esercizio_Pratico_U3_W2_L1**» presente sul desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

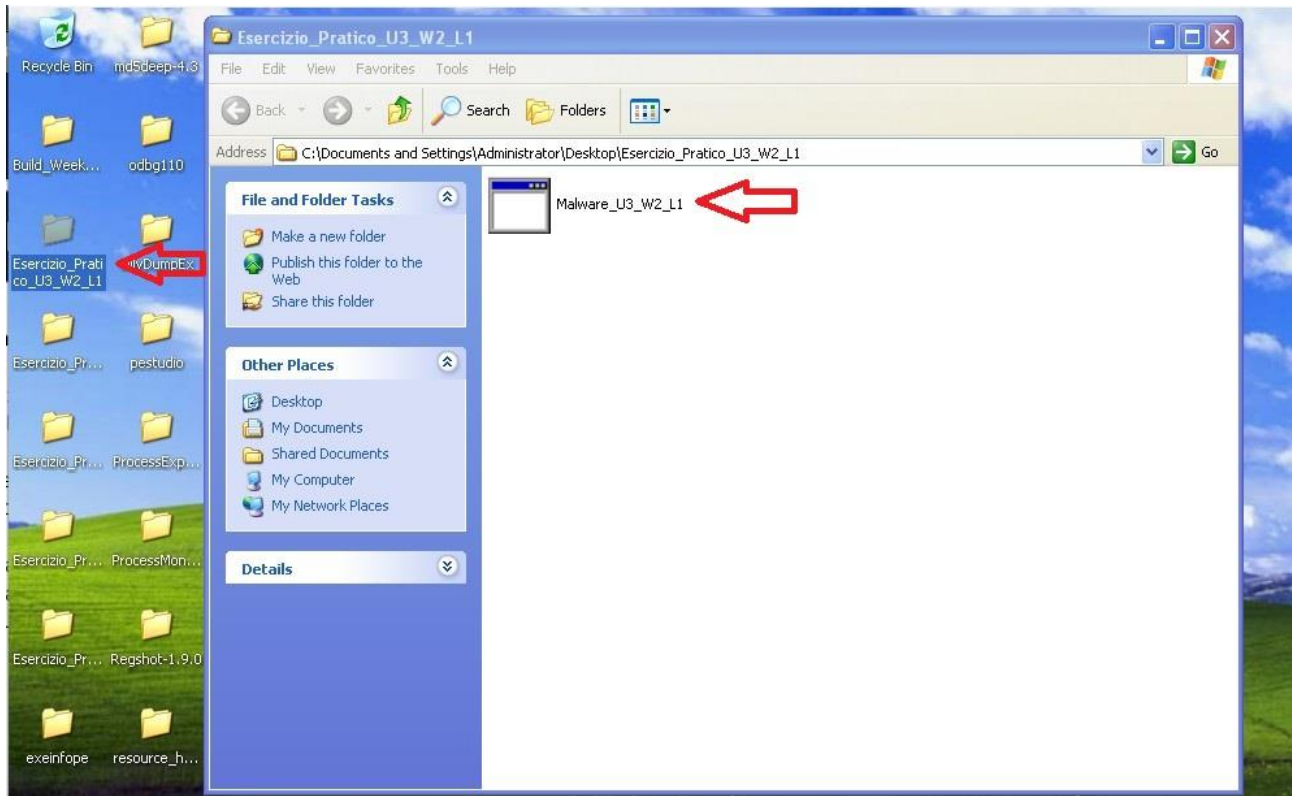
- Indicare le **librerie importate** dal malware, fornendo una **descrizione** per ognuna di esse
- Indicare le **sezioni** di cui si compone il malware, fornendo una **descrizione** per ognuna di essa
- Aggiungere una **considerazione finale** sul malware in analisi in base alle informazioni raccolte

Data la traccia, come prima cosa siamo andati ad importare la macchina virtuale su VirtualBox per poi avviarla.

La schermata iniziale si presenterà come di seguito:



Siamo andati ad aprire quindi la cartella indicata contenente il file eseguibile:

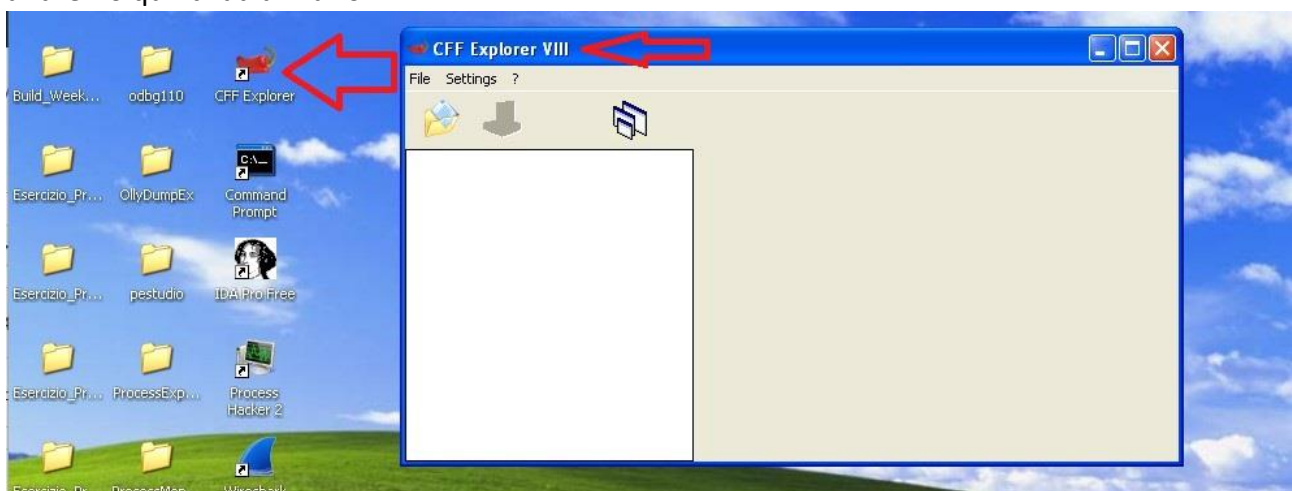


Andremo così ad iniziare la nostra **analisi statica basica** che consiste nell'esaminare un eseguibile senza vederne le istruzioni che lo compongono (quindi senza eseguirlo), con lo scopo di confermare se un dato file sia malevolo e fornire informazioni generiche circa le sue funzionalità.

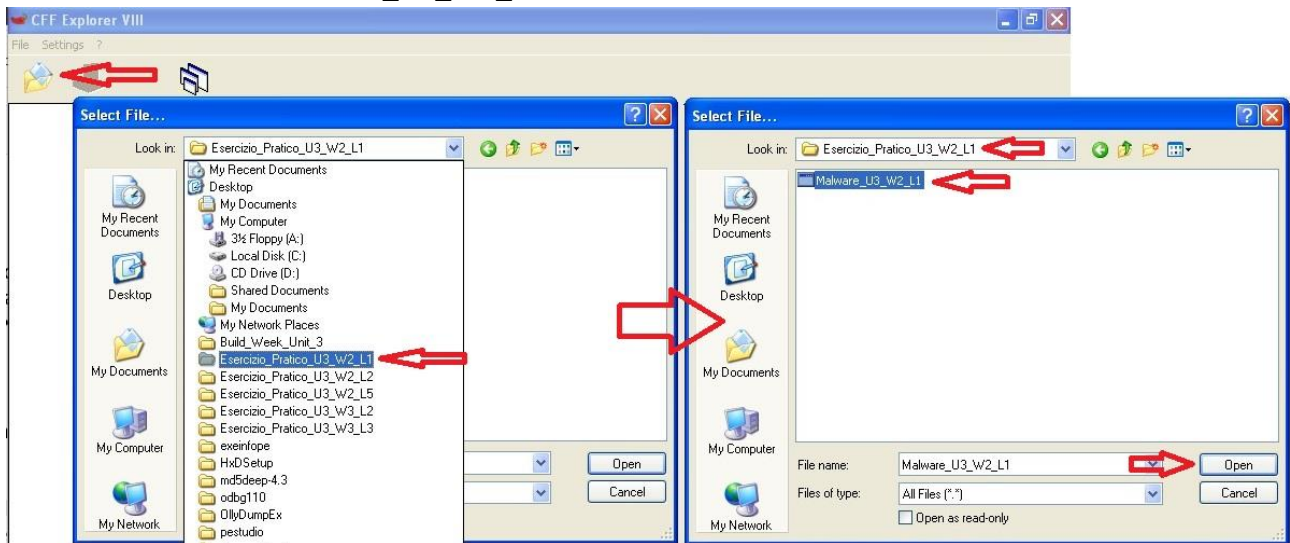
Windows utilizza per la maggior parte dei file eseguibili in formato **PE (Portable Execution)**. Questo formato contiene al suo interno delle informazioni necessarie al sistema operativo per capire come gestire il codice del file, come le **librerie**.

Le informazioni circa le librerie e le funzioni richieste dall'eseguibile sono contenute nell'header del formato PE. Controllare quali sono le librerie e le funzioni importate ed esportate è fondamentale per capire lo scopo del malware.

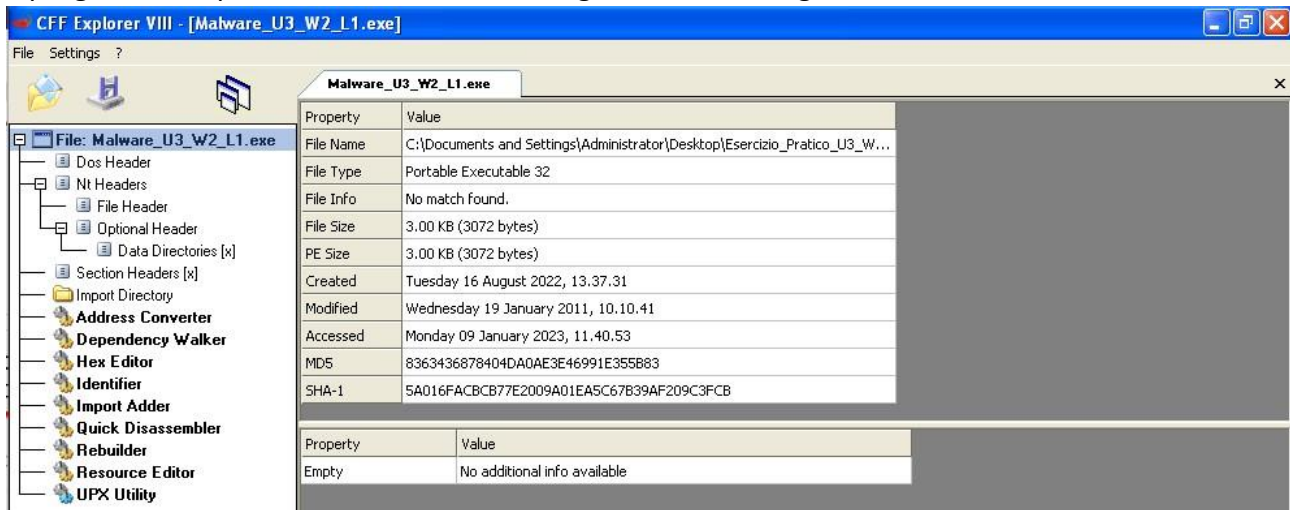
Per farlo, possiamo utilizzare il tool **CFF Explorer**, già presente sulla nostra macchina virtuale; andremo quindi ad avviarlo:



Andremo ora a scegliere il nostro eseguibile da esaminare cliccando sull'icona della cartella e selezionando il file "Malware_U3_W2_L1".



Il programma ci presenterà una descrizione generale dell'eseguibile:



Per controllare le librerie e le funzioni importate ci sposteremo su "Import Directory", dove il pannello ci darà informazioni circa le librerie importate, mentre per ogni libreria il pannello

inferiore mostrerà una lista delle funzioni richieste all'interno della libreria stessa.

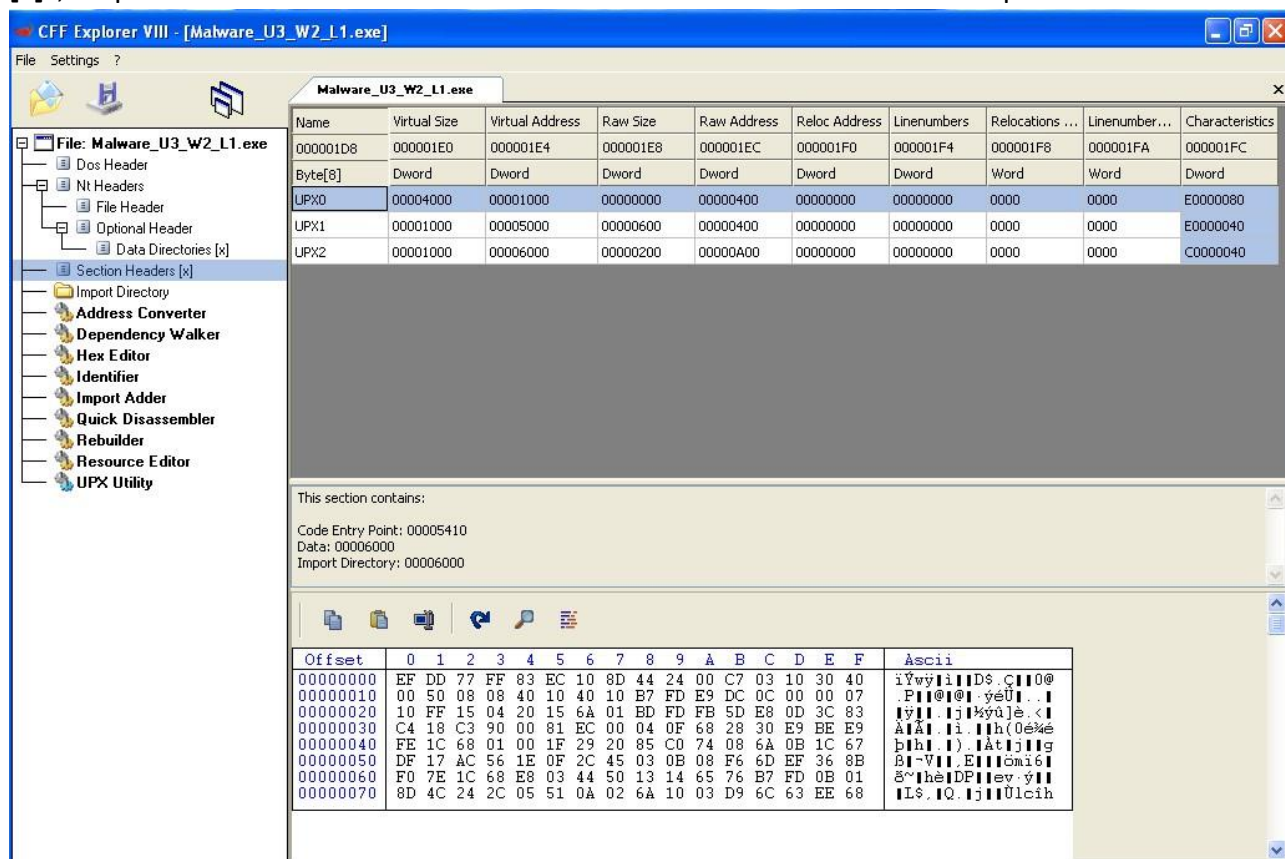
| Module Name | Imports | OFTs | TimeDateStamp | ForwarderChain | Name RVA | FTs (IAT) |
|--------------|--------------|----------|---------------|----------------|----------|-----------|
| 00000A98 | N/A | 00000A00 | 00000A04 | 00000A08 | 00000A0C | 00000A10 |
| szAnsi | (nFunctions) | Dword | Dword | Dword | Dword | Dword |
| KERNEL32.DLL | 6 | 00000000 | 00000000 | 00000000 | 00006098 | 00006064 |
| ADVAPI32.dll | 1 | 00000000 | 00000000 | 00000000 | 000060A5 | 00006080 |
| MSVCRT.dll | 1 | 00000000 | 00000000 | 00000000 | 000060B2 | 00006088 |
| WININET.dll | 1 | 00000000 | 00000000 | 00000000 | 000060BD | 00006090 |

| OFTs | FTs (IAT) | Hint | Name |
|-------|-----------|------|----------------|
| Dword | Dword | Word | szAnsi |
| N/A | 000060C8 | 0000 | LoadLibraryA |
| N/A | 000060D6 | 0000 | GetProcAddress |
| N/A | 000060E6 | 0000 | VirtualProtect |
| N/A | 000060F6 | 0000 | VirtualAlloc |
| N/A | 00006104 | 0000 | VirtualFree |
| N/A | 00006112 | 0000 | ExitProcess |

Potremo vedere che le **librerie importate** saranno:

- **KERNEL32.DLL**: libreria piuttosto comune che contiene le funzioni principali per interagire con il sistema operativo, manipolazione file e gestione della memoria. In questo caso possiamo vedere, ad esempio, che la libreria utilizza funzioni come **LoadLibrary** e **GetProcAddress**, utilizzate per caricare funzioni aggiuntive durante l'esecuzione del programma.
- **ADVAPI32.dll**: libreria che contiene le funzioni per interagire con i servizi ed i registri del sistema operativo Microsoft.
- **MSVCRT.dll**: libreria che contiene funzioni per la manipolazione delle stringhe, dell'allocazione memoria e altro, come chiamate per input/output in stile linguaggio C.
- **WININET.dll**: libreria che contiene funzioni per l'implementazione di protocolli di rete come GTP, FTP, NTP.

Andremo ora a vedere le sezioni di cui si compone il malware spostandoci su “**Section Headers [x]**”, in quanto l’header del formato PE fornisce anche le sezioni di cui si compone il software.



Com’è possibile vedere in “Section Headers [x]” saranno visibili come sezioni **UPX0**, **UPX1** e **UPX2** al posto di .text, .data, .rsrc ecc. UPX (Ultimate Packer for eXecutables) è un packer eseguibile gratuito e open source che supporta un numero di formati di file da diversi sistemi operativi. UPX è utilizzato per ridurre la dimensione del file di Portable Executables di circa il 50% -70%. Viene spesso utilizzato anche dagli attori delle minacce per aggiungere uno strato di offuscamento al loro malware. La versione predefinita ha un flag "decompress" che recupererà il codice originale.

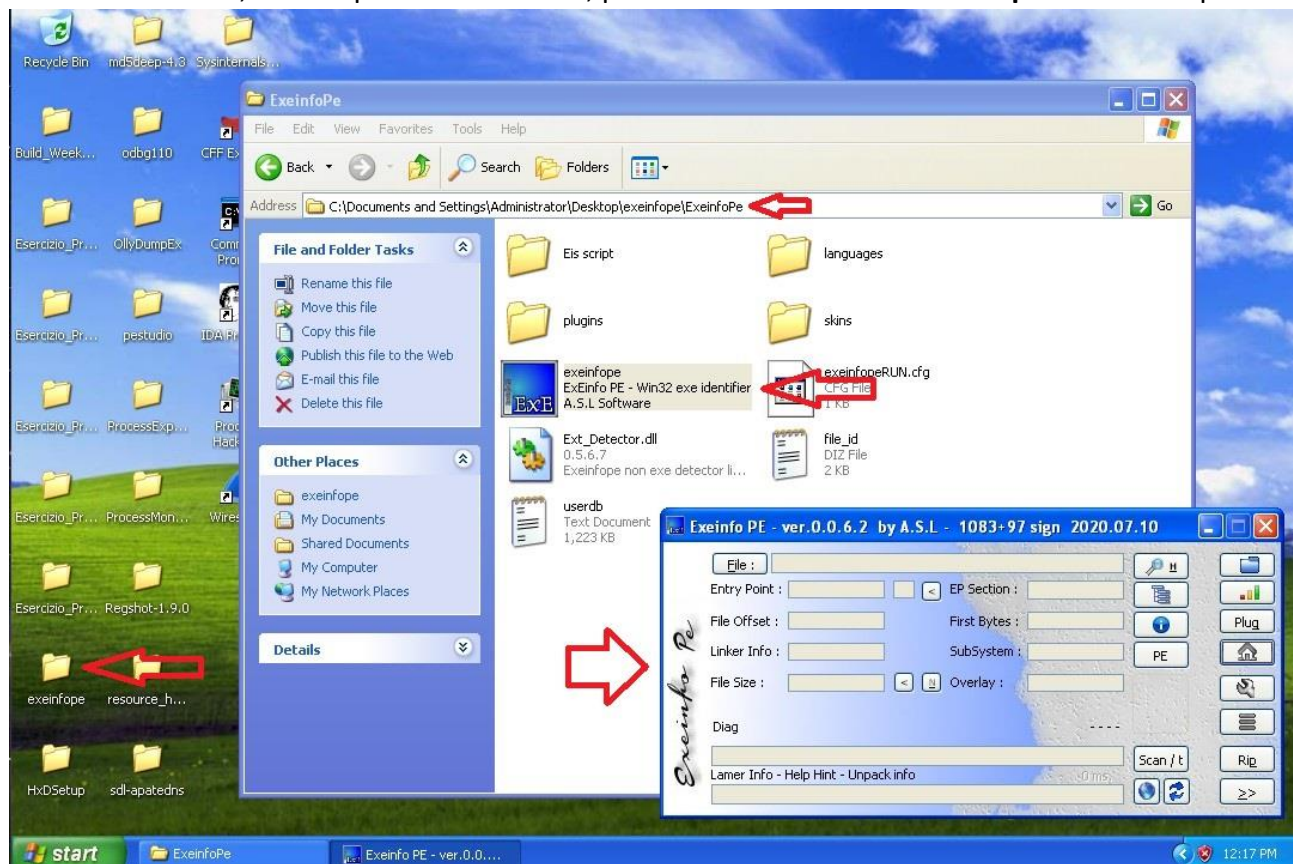
Tramite il link <https://kamransaifullah.medium.com/practical-malware-analysis-chapter-1-lab-1-2-solution-7db0acb0ad0> siamo riusciti a comprendere che UPX0, UPX1 e UPX2 si riferiscono di fatto alle sezioni del file PE:

- **.text:** sezione contenente le istruzioni che la CPU eseguirà una volta che il software verrà avviato.
- **.data:** sezione contenente i dati e le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma.
- **.rdata:** sezione che include generalmente le informazioni circa le librerie e le funzioni importate ed esportate dall’eseguibile.

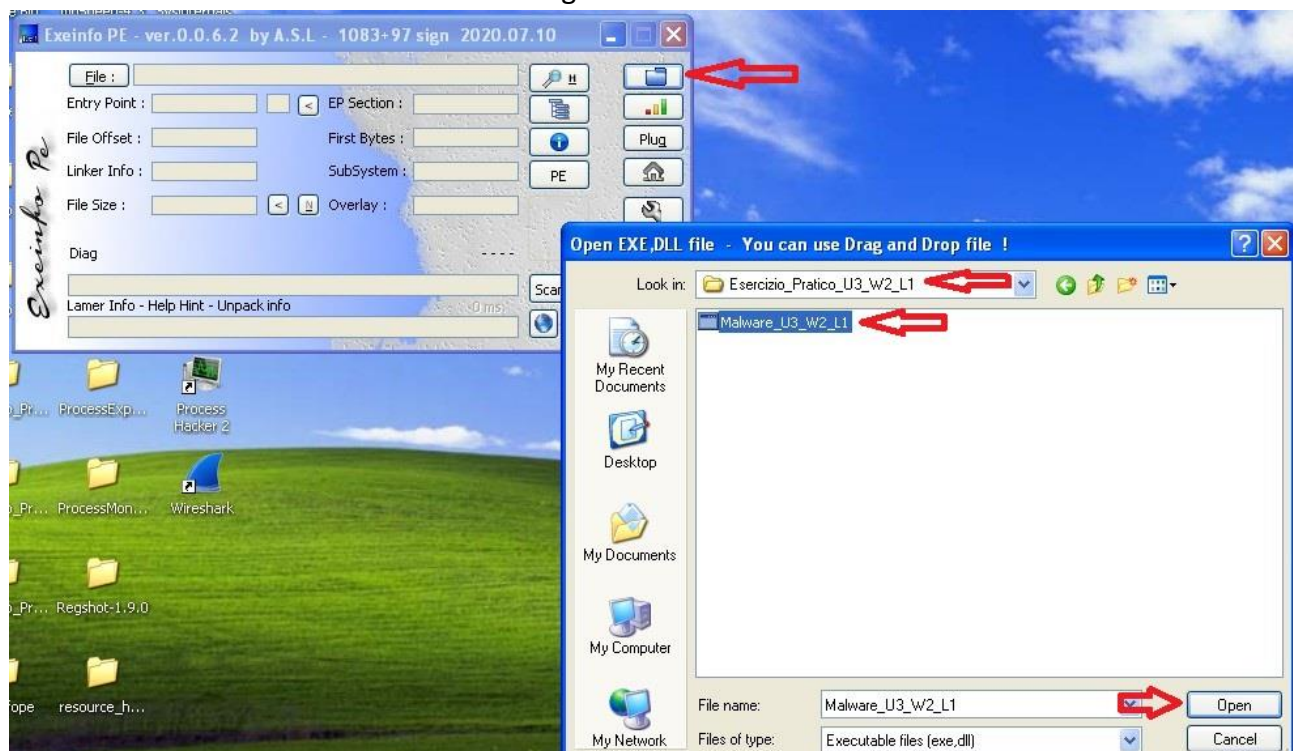
Questa schermata ci riporterà non solo il nome delle sezioni ma anche altre informazioni quali:

- **Virtual Size:** che indica lo spazio allocato per la sezione durante il processo di caricamento dell’eseguibile in memoria.
- **Raw Size:** indica lo spazio occupato dalla sezione quando è sul disco.

Le informazioni possono essere recuperate utilizzando altri tool, sempre presenti sulla nostra macchina virtuale, uno di questi è **ExeinfoPE**, presente nella cartella “**exeinfope**” sul Desktop.



Una volta avviato andremo a caricare l'eseguibile cliccando sull'icona della cartella in alto a destra:



The screenshot displays the Exeinfo PE v0.0.6.2 application window. The main pane shows detailed file information for "Malware_U3_W2_L1.exe".

| Field | Value |
|-----------------------------------------------------------------------------------------------------------------|---------------------------------------|
| File : | Malware_U3_W2_L1.exe |
| Entry Point : | 00005410 oo < EP Section : UPX1 |
| File Offset : | 00000810 First Bytes : 60.BE.00.50.40 |
| Linker Info : | 6.00 SubSystem : Win Console |
| File Size : | 00000C00h Overlay : NO 00000000 |
| Image is 32bit executable RES/OVL : 0 / 0 % 2011 | |
| UPX 0.89 - 3.xx -> Markus & Laszlo ver. [3.04] <- from file. (sign like Lamer Info - Help Hint - Unpack info | |
| Big sec. 2 [UPX1], unpack "upx.exe -d" from http://upx.github.io or | |

A red arrow points to the "Sections viewer" tab at the bottom.

Sections viewer : [Malware_U3_W2_L1.exe] 3 sections - alignment : 1000h

| Nr | Virtual offset | Virtual size | RAW Data offset | RAW size | Flags | Name | First bytes (hex) | First Ascii 20h bytes | sect. Stats |
|-------|----------------|--------------|-----------------|----------|----------|------|----------------------------|-----------------------|-------------|
| 01 | 00001000 | 00004000 | 00000400 | 00000000 | E0000080 | UPX0 | ! Z E R O S I Z E ! | ? w □ D\$ □□0@... d' | |
| 02 ep | 00005000 | 00001000 | 00000400 | 00000600 | E0000040 | UPX1 | EF DD 77 FF 83 EC 10 8D 44 | | |
| 03 im | 00006000 | 00001000 | 00000A00 | 00000200 | C0000040 | UPX2 | 00 00 00 00 00 00 00 00 | | |

Below the sections viewer, there are fields for "Overlay" (No overlay data), "End of file" (a long string of zeros), and "Section status" (03, Executable, Readable, Writable). A "Clip" button is also present.

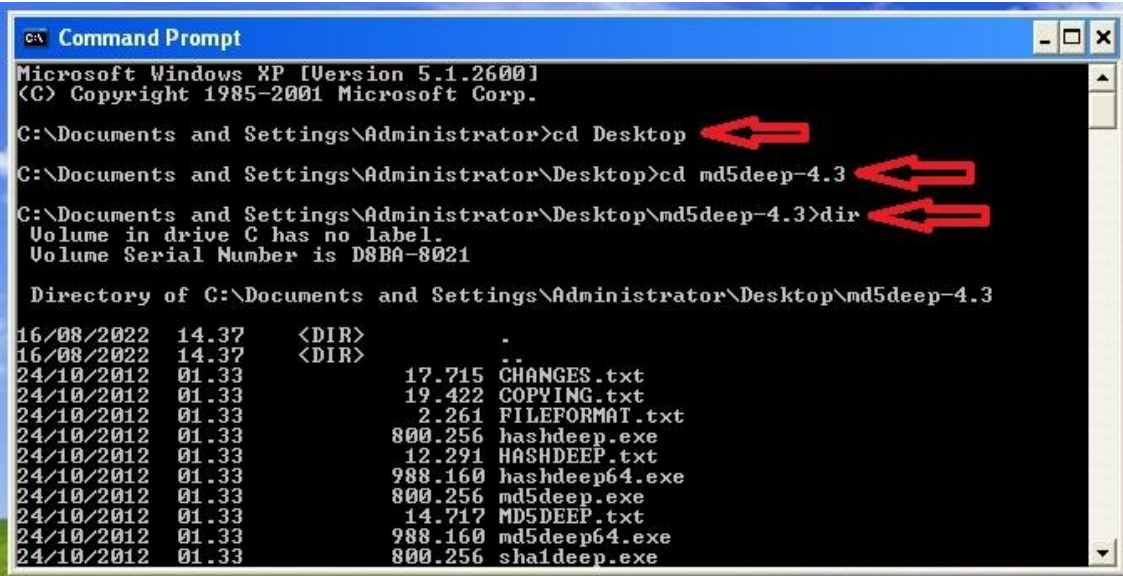

At the bottom, it states: "> RAW decimal size : 512 bytes = 0.50 kb = 0.00 MB <

Usualmente, quando si analizza un potenziale malware la prima cosa da fare è assicurarsi che sia un malware, per farlo si può controllare la sua **firma (file signature)** e vedere se essa sia nota. Siti come **VirusTotal** permettono di caricare un file eseguibile e controllarne la reputazione controllando nei database dei software antivirus.

Alternativamente si può calcolare l'**hash** del malware, ovvero una stringa alfanumerica unica per identificare file. Per farlo si può usare l'utilità **md5deep**, presente anch'essa sulla nostra macchina virtuale all'interno della cartella "md5deep-4.3".

Alternativamente si può calcolare l'**hash** del malware, ovvero una stringa alfanumerica unica per identificare file. Per farlo si può usare l'utility **md5deep**, presente anch'essa sulla nostra macchina virtuale all'interno della cartella "md5deep-4.3".

Per l'utilizzo del tool da riga di comando andremo quindi ad aprire il **Command Prompt**, ci sposteremo nella directory contenente il tool tramite il comando "**cd**" e "**dir**".



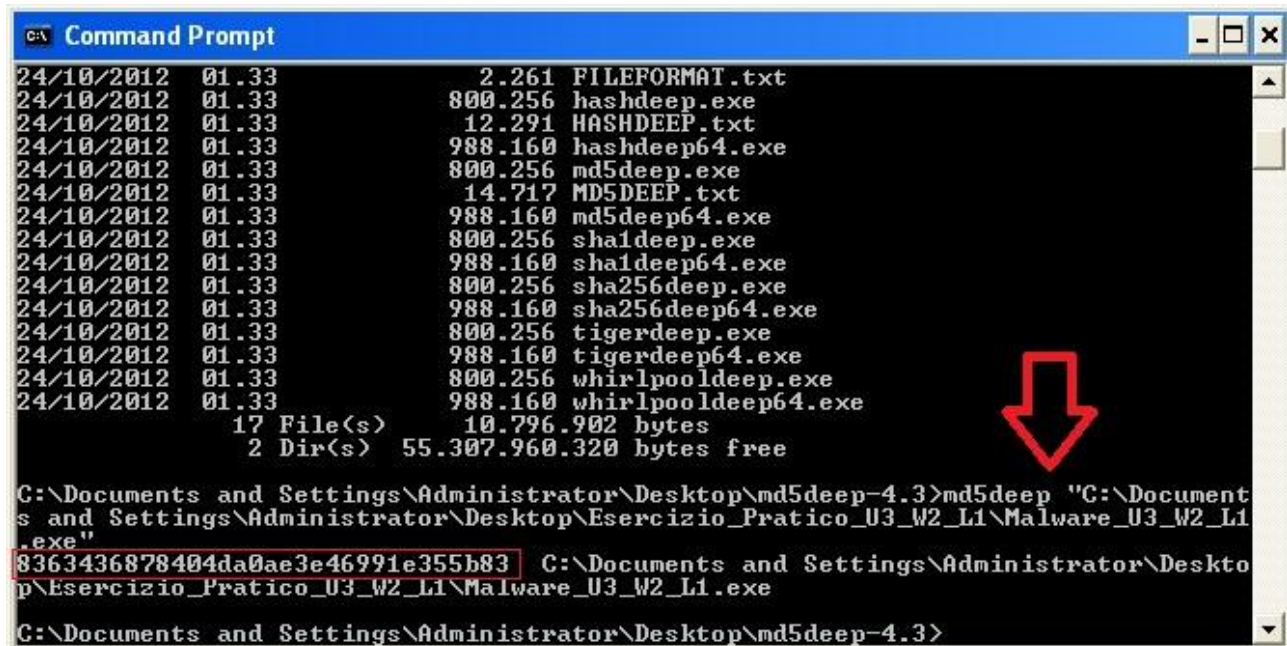
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>cd Desktop
C:\Documents and Settings\Administrator\Desktop>cd md5deep-4.3
C:\Documents and Settings\Administrator\Desktop\md5deep-4.3>dir
Volume in drive C has no label.
Volume Serial Number is D8BA-8021

Directory of C:\Documents and Settings\Administrator\Desktop\md5deep-4.3

16/08/2022  14.37    <DIR>          -
16/08/2022  14.37    <DIR>          -
24/10/2012  01.33             17.715  CHANGES.txt
24/10/2012  01.33             19.422  COPYING.txt
24/10/2012  01.33              2.261  FILEFORMAT.txt
24/10/2012  01.33            800.256  hashdeep.exe
24/10/2012  01.33            12.291  HASHDEEP.txt
24/10/2012  01.33           988.160  hashdeep64.exe
24/10/2012  01.33            800.256  md5deep.exe
24/10/2012  01.33            14.717  MD5DEEP.txt
24/10/2012  01.33           988.160  md5deep64.exe
24/10/2012  01.33            800.256  sha1deep.exe
```

Per lanciare il comando useremo la sintassi "**md5deep percorso_del_file_eseguibile**" ed il programma ci fornirà l'hash seguita dal path del file stesso per il quale è stato calcolato l'hash.



```
24/10/2012  01.33              2.261  FILEFORMAT.txt
24/10/2012  01.33            800.256  hashdeep.exe
24/10/2012  01.33            12.291  HASHDEEP.txt
24/10/2012  01.33           988.160  hashdeep64.exe
24/10/2012  01.33            800.256  md5deep.exe
24/10/2012  01.33            14.717  MD5DEEP.txt
24/10/2012  01.33           988.160  md5deep64.exe
24/10/2012  01.33            800.256  sha1deep.exe
24/10/2012  01.33           988.160  sha1deep64.exe
24/10/2012  01.33            800.256  sha256deep.exe
24/10/2012  01.33           988.160  sha256deep64.exe
24/10/2012  01.33            800.256  tigerdeep.exe
24/10/2012  01.33           988.160  tigerdeep64.exe
24/10/2012  01.33            800.256  whirlpooldeep.exe
24/10/2012  01.33           988.160  whirlpooldeep64.exe
      17 File(s)      10.796.902 bytes
      2 Dir(s)  55.307.960.320 bytes free

C:\Documents and Settings\Administrator\Desktop\md5deep-4.3>md5deep "C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L1\Malware_U3_W2_L1.exe"
8363436878404da0ae3e46991e355b83 C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L1\Malware_U3_W2_L1.exe
C:\Documents and Settings\Administrator\Desktop\md5deep-4.3>
```

Una volta recuperato l'hash esso si potrà utilizzare come se fosse un'etichetta per l'identificazione del malware, si potrà condividere con altri analisti della sicurezza per aiutarli nell'identificazione del malware o si potrà cercarlo online (ad esempio su VirusTotal) per confermare che sia un

malware e trovare informazioni riguardo il suo comportamento.

c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6

53 / 71

53 security vendors and no sandboxes flagged this file as malicious

c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6

3.00 KB
Size

2023-01-04 20:55:55 UTC
4 days ago

Lab01-02.exe

peexe checks-disk-space via-tor detect-debug-environment idle long-sleeps upx checks-user-input

EXE

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 30 +

Basic properties ⓘ

| | |
|---------------------|------------------------------------------------------------------|
| MD5 | 8363436878404da0ae3e46991e355b83 |
| SHA-1 | 5a016facbcb77e2009a01ea5c67b39af209c3fcb |
| SHA-256 | c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6 |
| Vhash | 03303e07d1019z601pz1bz |
| Authentihash | c0dd97382560a28cc053de86b9505ea78390147de7021744eb49d9b55e3d152f |
| Imphash | 096aa05b8a2e1f2dc66fc73a1a978a7b |
| Rich PE header hash | 0560c88b0c8133e98d13ab271ab4c687 |
| SSDEEP | 48:atUKzxRhviNZEVtfn4m3ZUJSSeJY8JTalcLoBgs:0UKXktb4KOJzcK |

VirusTotal ci darà la conferma che il file eseguibile si tratta di un malware (Trojan) secondo 53/71 antivirus.

<https://www.virustotal.com/gui/file/c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6/detection>

Nel caso di malware si potrebbero recuperare informazioni dalle stringhe contenute all'interno degli eseguibili. L'utility da riga di comando "**strings**", presente sulla macchina all'interno della cartella "SysinternalsSuite", permette di trovare tutte le stringhe utilizzate all'interno di un eseguibile. Andremo quindi a lanciare l'utility tramite il comando "**strings percorso_del_file_eseguibile**".

```
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>cd Desktop
C:\Documents and Settings\Administrator\Desktop>cd SysinternalsSuite
C:\Documents and Settings\Administrator\Desktop\SysinternalsSuite>strings "C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L1\Malware_U3_W2_L1.exe"

Strings v2.51
Copyright (C) 1999-2013 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
Rich
UPX0
UPX1
UPX2
3.04
UPX!
AI3
h<0
L$,
QII
" z
RU$
u+W
.hP
t=p
sHR
!Pd
S'
a\Y
tEE
DnM
;0I
PQ6
<23h
MalService
shGL345
http://w
warean
ysisbook.co
om#Int6net Explo!r 8FEI
.0<
SystemTimeToFile
GetMo
NaA
Cvg
*Waitab'r
Process
OpenMu$x

ZSB+
For$
ing
ObjectU4
!Urtb
CtrlDisp ch
SCM
8_e
Xcpt
mArg
sus
5nm0_
t_fd
i9H
m<e
?.p
vty
dll137n
olfp
PEL
dW!6
.4t
!B\ .rd
e.&
0'0
~s
u A
Glu
PTj
XPtPSW
KERNEL32.DLL
ADVAPI32.dll
MSUCRT.dll
WININET.dll
LoadLibraryA
GetProcAddress
VirtualProtect
VirtualAlloc
VirtualFree
ExitProcess
CreateServiceA
exit
InternetOpenA

C:\Documents and Settings\Administrator\Desktop\SysinternalsSuite>
```

L'output di strings rivela spesso molte stringhe non significative, sarà il ruolo dell'analista di sicurezza controllarle dettagliatamente per trovare quelle più significative.

Tramite le nostre analisi siamo arrivati alla conclusione che il malware sia un **Trojan**, un malware che si nasconde all'interno di un altro programma apparentemente utile e innocuo: l'utente, eseguendo o installando quest'ultimo programma, attiva inconsapevolmente anche il codice del Trojan nascosto.

Nel nostro caso il Trojan conterrà al suo interno librerie in grado di interagire col sistema operativo, modificare file, registri di sistemi e protocolli di rete.