

Surface Analysis

Surface Analysis Tools

Tool name	Description
CFF Explorer	PE Editor, Viewer
PE Studio	PE Viewer
StudPE	PE Editor, Viewer
PE Insider	PE Viewer
pefile	Python PE Editor, Viewer
Viper	Surface analysis framework

Surface Analysis Tools – CFF Explorer

CFF Explorer VIII - [notepad.exe]

File Settings ?

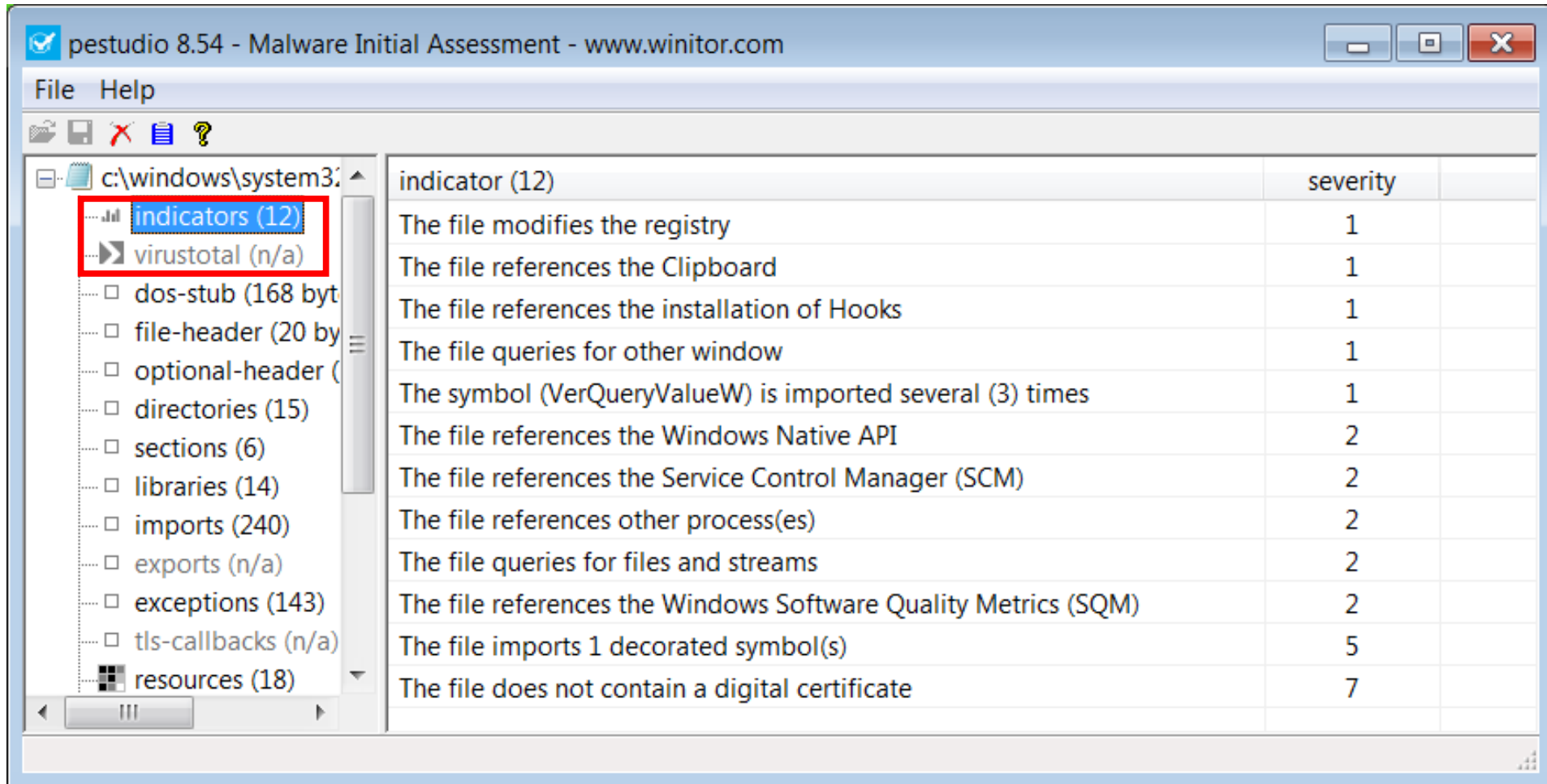
notepad.exe

File: notepad.exe

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

Member	Offset	Size	Value	Meaning
Magic	00000100	Word	020B	PE64
MajorLinkerVersion	00000102	Byte	09	
MinorLinkerVersion	00000103	Byte	00	
SizeOfCode	00000104	Dword	0000A800	
SizeOfInitializedData	00000108	Dword	00025800	
SizeOfUninitializedD...	0000010C	Dword	00000000	
AddressOfEntryPoint	00000110	Dword	00003570	.text
BaseOfCode	00000114	Dword	00001000	
ImageBase	00000118	Qword	0000000100000000	
SectionAlignment	00000120	Dword	00001000	
FileAlignment	00000124	Dword	00000200	
MajorOperatingSystem...	00000128	Word	0006	
MinorOperatingSystem...	0000012A	Word	0001	

Surface Analysis Tools – PE Studio



Scenario 1 Labs

The Result of Persistence Analysis

- We found two binaries from the host Client-Win10-1.

	Persistence Type	Name	Image to Execute	Registered Date	Access Right
Persistence A	Scheduled Task	SxS	C:\Windows\SvS.DLL,GnrkQr	2018-03-14 22:50:28 (JST)	Privilege
Persistence B	WMI	AddinManager Monitor	C:\Windows\addins\Addins Manager.exe	2018-03-20 18:40:27 (JST)	Privilege

- If you have not extracted them, you can find them as a zip file in the following folder.
 - E:\Artifacts\scenario1_malware\malware.zip
 - Password: infected

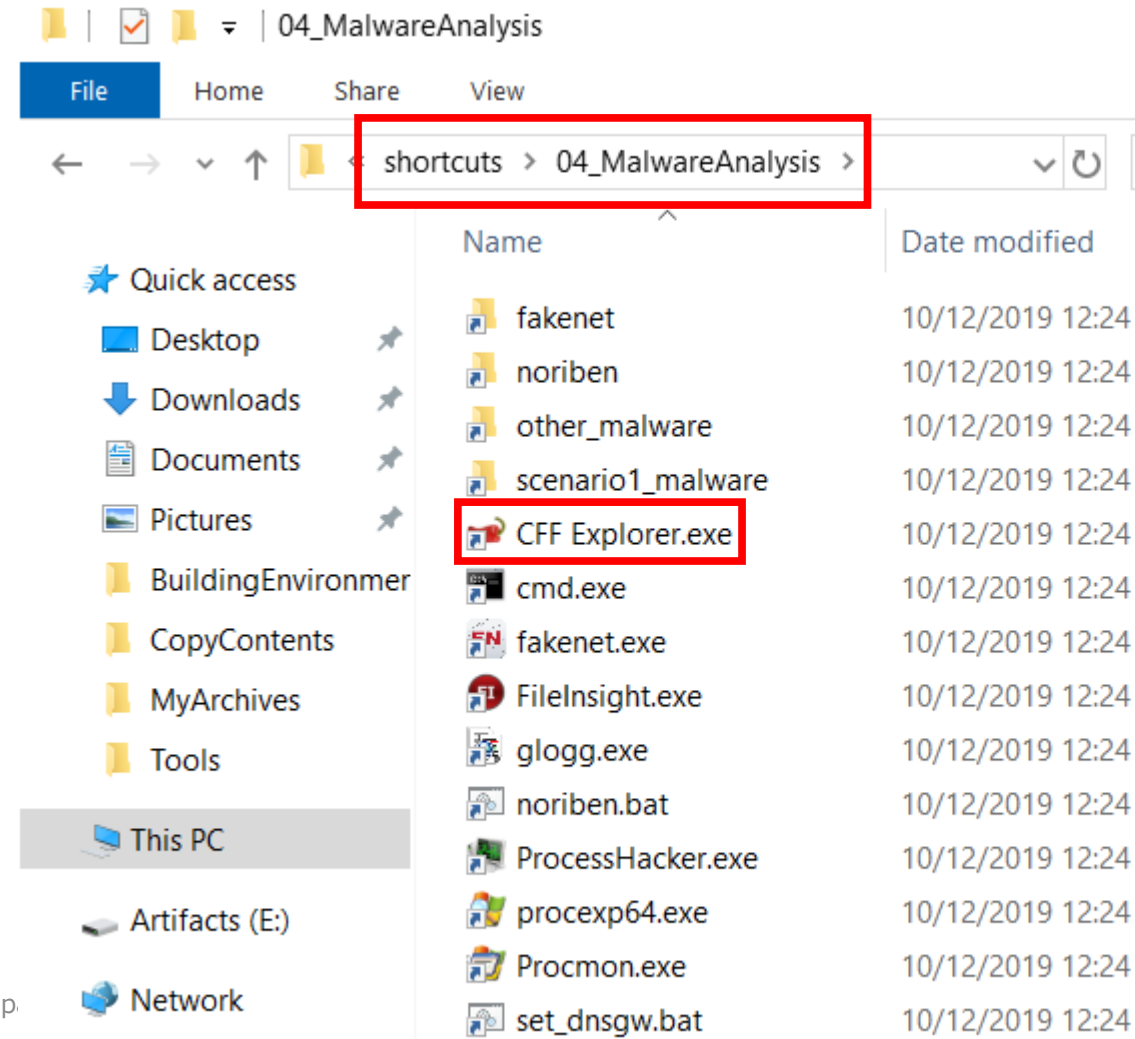
Scenario 1 Labs:

Surface Analysis for SvS.DLL

Scenario 1 Labs:

Surface Analysis for SvS.DLL (1)

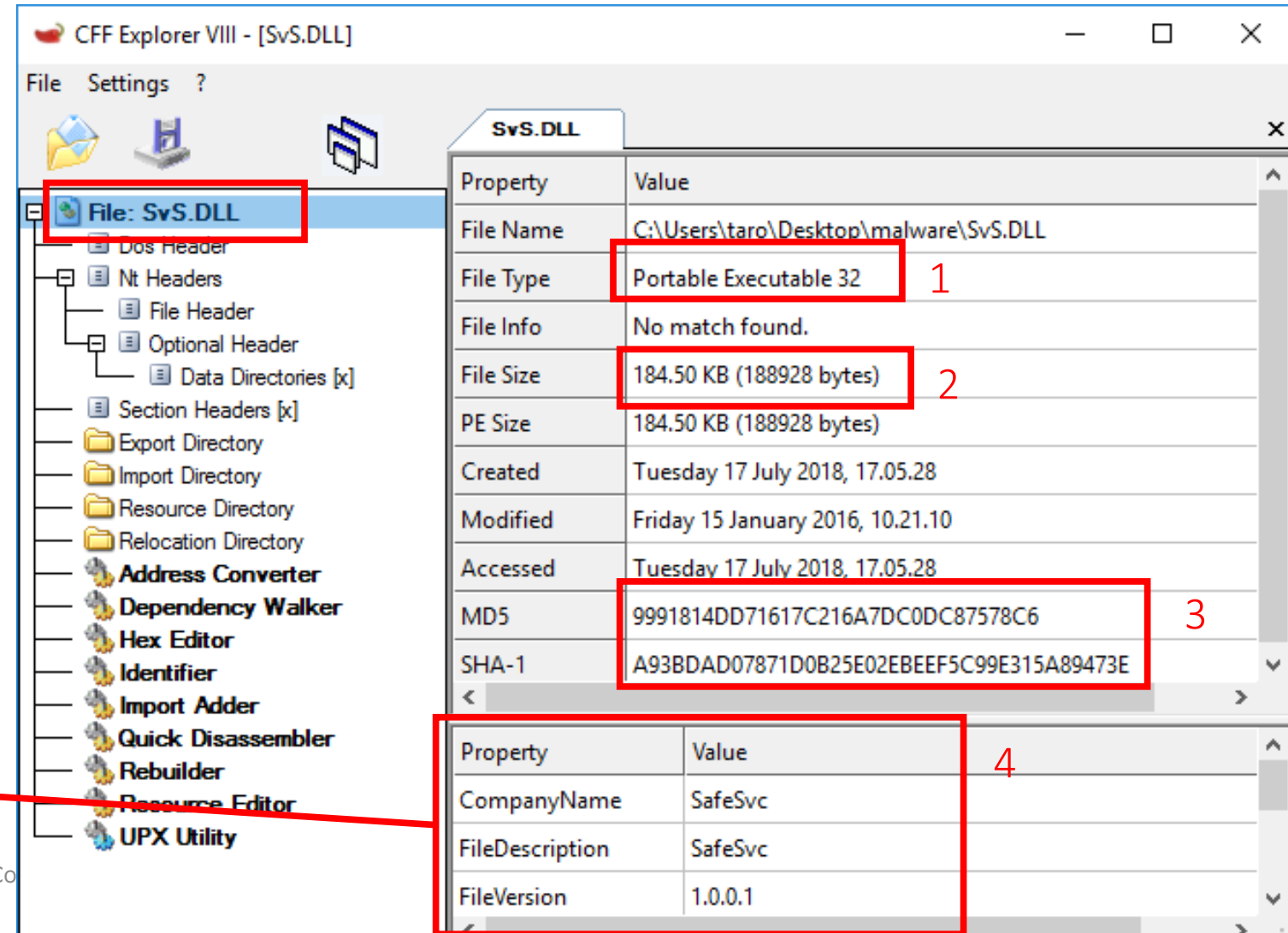
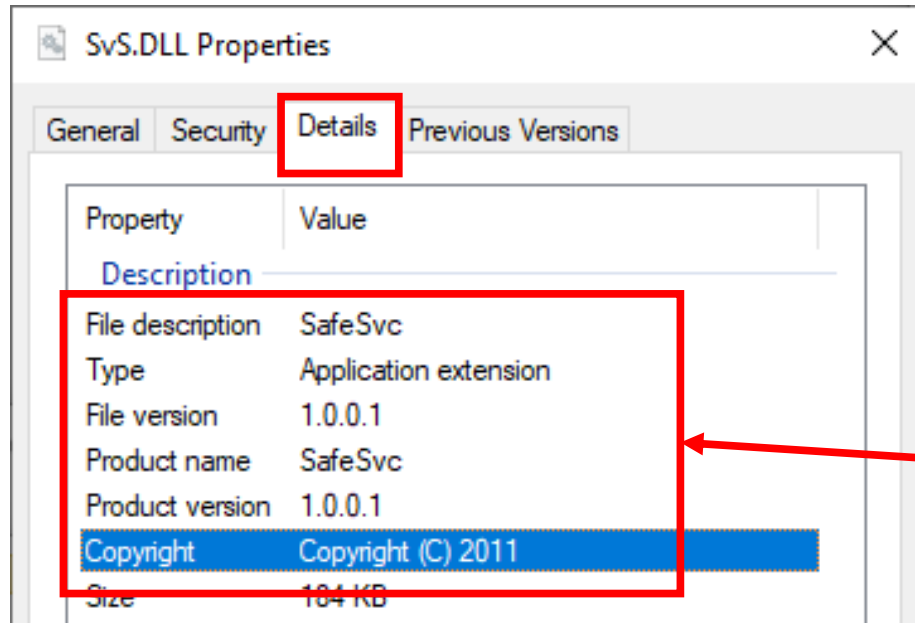
- Open “CFF Explorer”
 - Path: Shortcuts\04_MalwareAnalysis
- Drag and drop SvS.DLL onto it.
 - If you forgot to extract the malware, you can find it in the following path.
 - E:\Artifacts\scenario1_malware\malware.zip
 - Password: infected



Scenario 1 Labs:

Surface Analysis for SvS.DLL (2)

- Click the file name on the left pane.
- We can see :
 - File type
 - File size
 - MD5/SHA1 hashes
 - File Properties



Scenario 1 Labs: Surface Analysis for

- Click “File Header” on the left pane.
- Click “Click here” on the “Characteristics” field.
- You can find that:
 1. This file is a DLL
 2. This file is a 32 bit binary.

CFF Explorer VIII - [SvS.DLL]

File Settings ?

SvS.DLL

Member	Offset	Size	Value	Meaning
Machine	000000D4	Word	014C	Intel 386
NumberOfSections	000000D6	Word	0005	
TimeDateStamp	000000D8	Dword	4EE21DCE	
PointerToSymbolTa...	000000DC	Dword	00000000	
NumberOfSymbols	000000E0	Dword	00000000	
SizeOfOptionalHea...	000000E4	Word	00E0	
Characteristics	000000E6	Word	2102	Click here

Characteristics

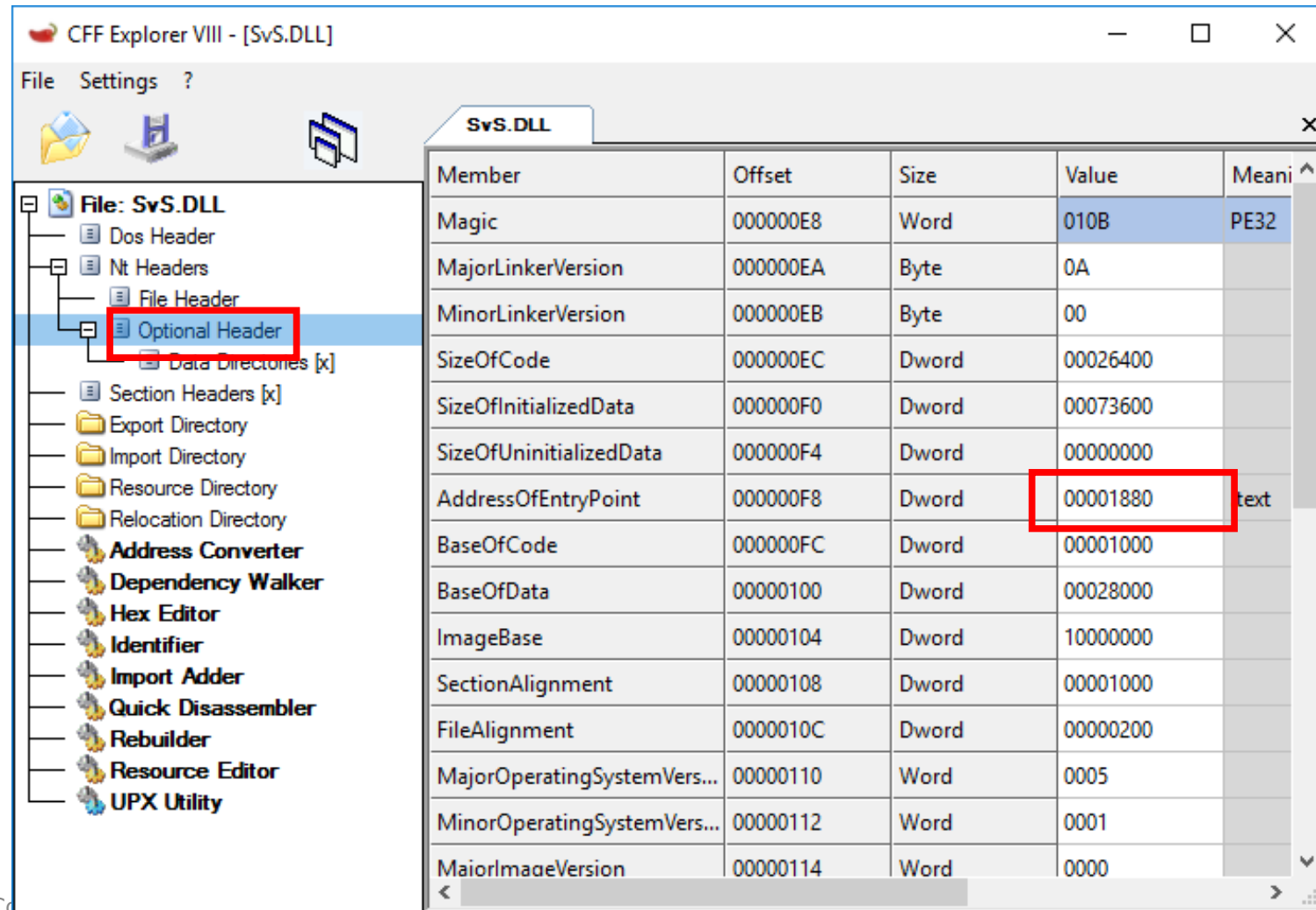
- ☒ File is executable
- ☒ File is a DLL
- ☐ System File
- ☐ Relocation info stripped from file
- ☐ Line numbers stripped from file
- ☐ Local symbols stripped from file
- ☐ Aggressively trim working set
- ☐ App can handle >2gb address space
- ☐ Bytes of machine word are reversed (low)
- ☒ 32 bit word machine
- ☐ Debugging info stripped from file in .DBG file
- ☐ If Image is on removable media, copy and run from the swap
- ☐ If Image is on Net, copy and run from the swap file
- ☐ File should only be run on a UP machine
- ☐ Bytes of machine word are reversed (high)

OK Cancel

Scenario 1 Labs:

Surface Analysis for SvS.DLL (4)

- Click “Optional Header” on the left pane.
- You can find:
 1. Offset of the entry point for this file is 0x1880.
 - This is the starting point of the code for this binary.



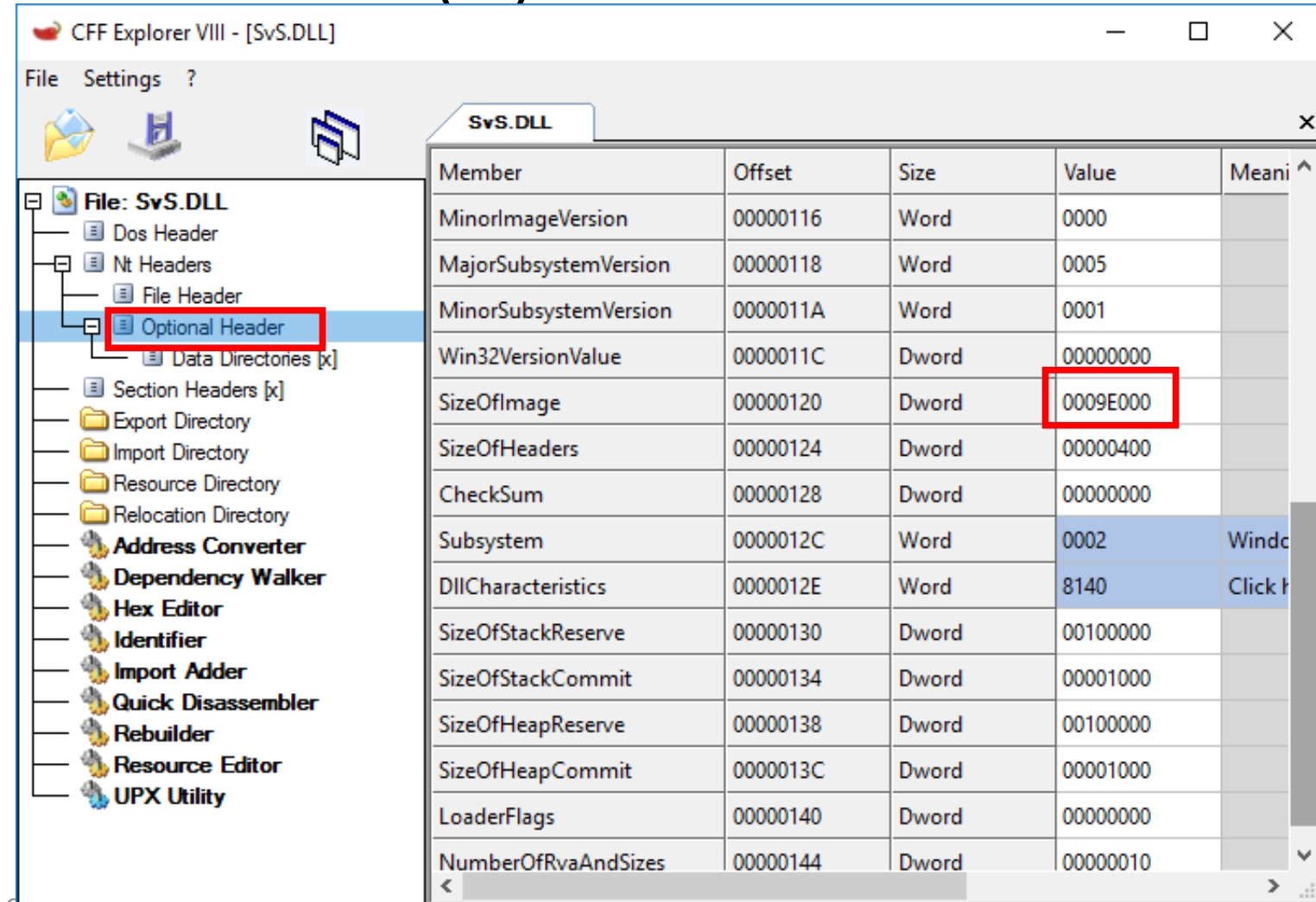
The screenshot shows the CFF Explorer VIII interface for the file SvS.DLL. The left pane displays the file structure, with the 'Optional Header' section highlighted in blue and a red box around it. The right pane shows a table of the optional header fields.

Member	Offset	Size	Value	Meani
Magic	000000E8	Word	010B	PE32
MajorLinkerVersion	000000EA	Byte	0A	
MinorLinkerVersion	000000EB	Byte	00	
SizeOfCode	000000EC	Dword	00026400	
SizeOfInitializedData	000000F0	Dword	00073600	
SizeOfUninitializedData	000000F4	Dword	00000000	
AddressOfEntryPoint	000000F8	Dword	00001880	text
BaseOfCode	000000FC	Dword	00001000	
BaseOfData	00000100	Dword	00028000	
ImageBase	00000104	Dword	10000000	
SectionAlignment	00000108	Dword	00001000	
FileAlignment	0000010C	Dword	00000200	
MajorOperatingSystemVers...	00000110	Word	0005	
MinorOperatingSystemVers...	00000112	Word	0001	
MaiorImageVersion	00000114	Word	0000	

Scenario 1 Labs:

Surface Analysis for SvS.DLL (5)

- You can also find:
 - Image size on memory is 0x9e000.



CFF Explorer VIII - [SvS.DLL]

File Settings ?

SvS.DLL

Member	Offset	Size	Value	Meaning
MinorImageVersion	00000116	Word	0000	
MajorSubsystemVersion	00000118	Word	0005	
MinorSubsystemVersion	0000011A	Word	0001	
Win32VersionValue	0000011C	Dword	00000000	
SizeOfImage	00000120	Dword	0009E000	
SizeOfHeaders	00000124	Dword	00000400	
Checksum	00000128	Dword	00000000	
Subsystem	0000012C	Word	0002	Windows Common-Object Model
DllCharacteristics	0000012E	Word	8140	Click to view details
SizeOfStackReserve	00000130	Dword	00100000	
SizeOfStackCommit	00000134	Dword	00001000	
SizeOfHeapReserve	00000138	Dword	00100000	
SizeOfHeapCommit	0000013C	Dword	00001000	
LoaderFlags	00000140	Dword	00000000	
NumberOfRvaAndSizes	00000144	Dword	00000010	

Scenario 1 Labs:

Surface Analysis for SvS.DLL (6)

- Click “Section Headers”.
- The section names and the number seem to be normal.

The screenshot shows the CFF Explorer VIII interface for the file SvS.DLL. The left pane displays a tree view of the file's structure, with 'Section Headers [x]' selected and highlighted by a red rectangle. The right pane displays a table of section headers, also with a red rectangle highlighting the first five rows. The table columns are Name, Virtual Size, Virtual Address, Raw Size, Raw Address, and Relative Virtual Address (partially visible). The bottom of the interface shows a hex editor with an offset row and a data row.

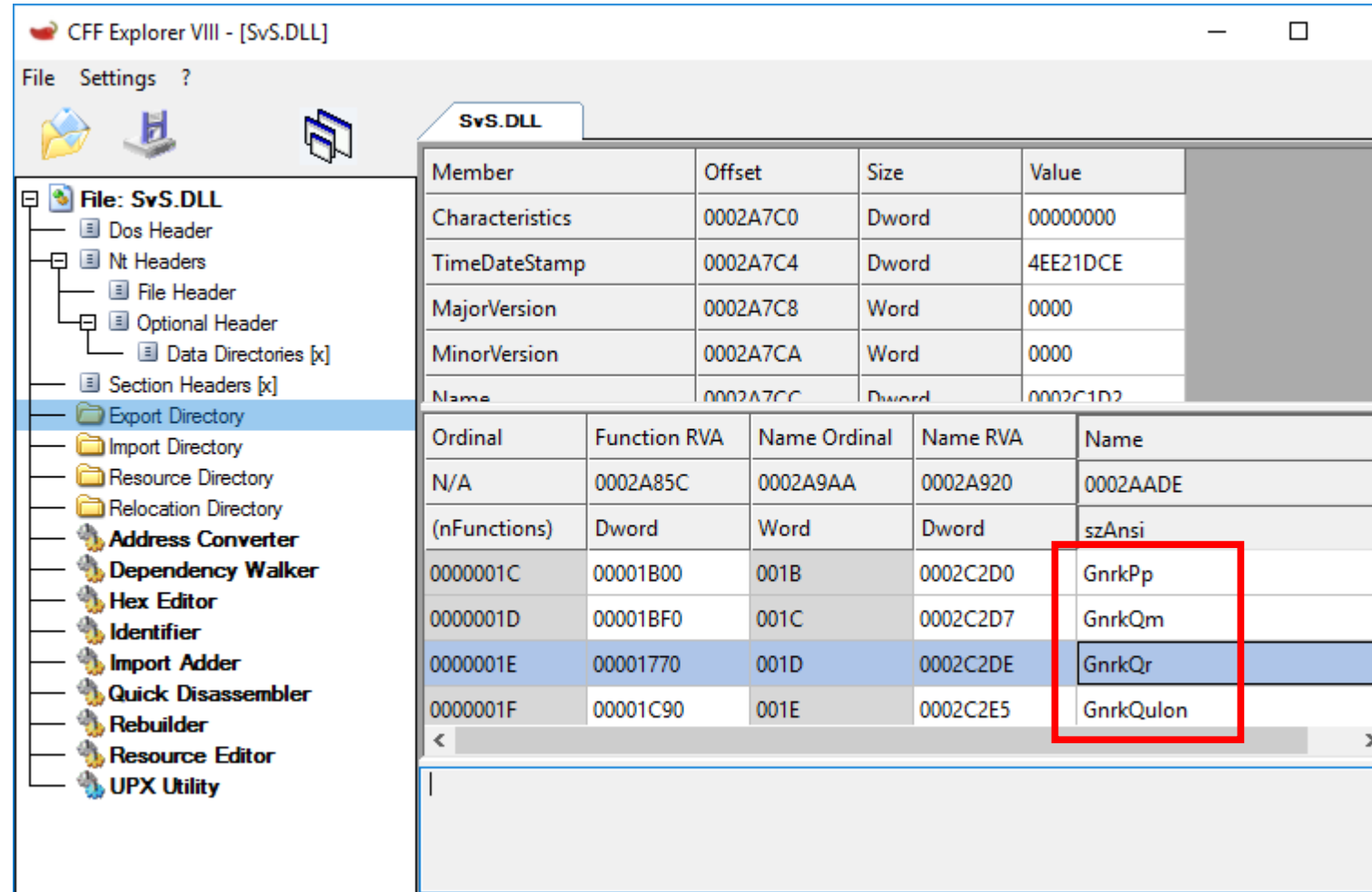
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Relative Virtual Address
Byte[8]	Dword	Dword	Dword	Dword	Dword
.text	00027000	00001000	00026400	00000400	00000000
.rdata	00005000	00028000	00004400	00026800	00000400
.data	0006D000	0002D000	00000A00	0002AC00	00000400
.rsrc	00001000	0009A000	00000400	0002B600	00000400
.reloc	000026FC	0009B000	00002800	0002BA00	00000400

Offset: 0 1 2 3 4 5 6 7 8 9 A B C D E F

Scenario 1 Labs:

Surface Analysis for SvS.DLL (7)

- Click “Export Directory” on the left pane.
- It looks unusual as many non human-readable APIs are exported.
 - “GnrkQr”, which is used for persistence, is also exported.



The screenshot shows the CFF Explorer VIII interface for the file SvS.DLL. The left pane displays the file's structure, with the 'Export Directory' selected. The right pane shows a table of exported functions. The table has columns for Ordinal, Function RVA, Name Ordinal, Name RVA, and Name. The function 'GnrkQr' is highlighted in blue, and a red box is drawn around the 'Name' column for the functions 'GnrkPp', 'GnrkQm', 'GnrkQr', and 'GnrkQulon'.

Member	Offset	Size	Value
Characteristics	0002A7C0	Dword	00000000
TimeStamp	0002A7C4	Dword	4EE21DCE
MajorVersion	0002A7C8	Word	0000
MinorVersion	0002A7CA	Word	0000
Name	0002A7CC	Dword	0002C1D2

Ordinal	Function RVA	Name Ordinal	Name RVA	Name
N/A	0002A85C	0002A9AA	0002A920	0002AADE
(nFunctions)	Dword	Word	Dword	szAnsi
0000001C	00001B00	001B	0002C2D0	GnrkPp
0000001D	00001BF0	001C	0002C2D7	GnrkQm
0000001E	00001770	001D	0002C2DE	GnrkQr
0000001F	00001C90	001E	0002C2E5	GnrkQulon

Scenario 1 Labs:

Surface Analysis for SvS.DLL (8)

- Click “Import Directory” on the left pane.
- It imports only four modules.

CFF Explorer VIII - [SvS.DLL]

File Settings ?

SvS.DLL

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name
0002A2A2	N/A	00029D90	00029D94	00029D98	000
szAnsi	(nFunctions)	Dword	Dword	Dword	Dw
KERNEL32.dll	40	0002B688	00000000	00000000	000
USER32.dll	30	0002B72C	00000000	00000000	000
GDI32.dll	17	0002B640	00000000	00000000	000
ADVAPI32.dll	18	0002B5F4	00000000	00000000	000

Left Pane:

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

Right Pane:

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
0002BA6C	0002BA6C	0112	EnumTimeFormatsW
0002BA80	0002BA80	02B2	GlobalAddAtomW
0002BA52	0002BA52	04CE	TryEnterCriticalSection
0002BA46	0002BA46	02CB	HeapAlloc

Scenario 1 Labs:

Surface Analysis for SvS.DLL (9)

- Open cmd.exe and check readable strings on this binary.
 - Execute this command.

```
strings -n 10 C:\Users\taro\Desktop\malware\SvS.DLL
```

- -n: Minimum string length
- Then, we can find a remarkable string.

```
CONNECT live.net:443 HTTP/1.0
```

Is this a malicious server?

Scenario 1 Labs:

Surface Analysis for SvS.DLL - Summary

The result of the surface analysis for SvS.DLL

Characteristics	Result
File type	Portable Executable 32 (32 bit binary)
File size	184.50 KB (188928 bytes)
MD5 hash	9991814DD71617C216A7DC0DC87578C6
SHA1 hash	A93BDAD07871D0B25E02EBEEF5C99E315A89473E
PE characteristics	32 bit / DLL
Address of entry point	0x1880
Size of image	0x9e000 (647,168)
Import table	Only four modules and there is no TCP/IP related module.
Export table	Ugly API names
Notable strings	CONNECT live.net:443 HTTP/1.0

Scenario 1 Labs:

Surface Analysis for SvS.DLL – Summary (Cont.)

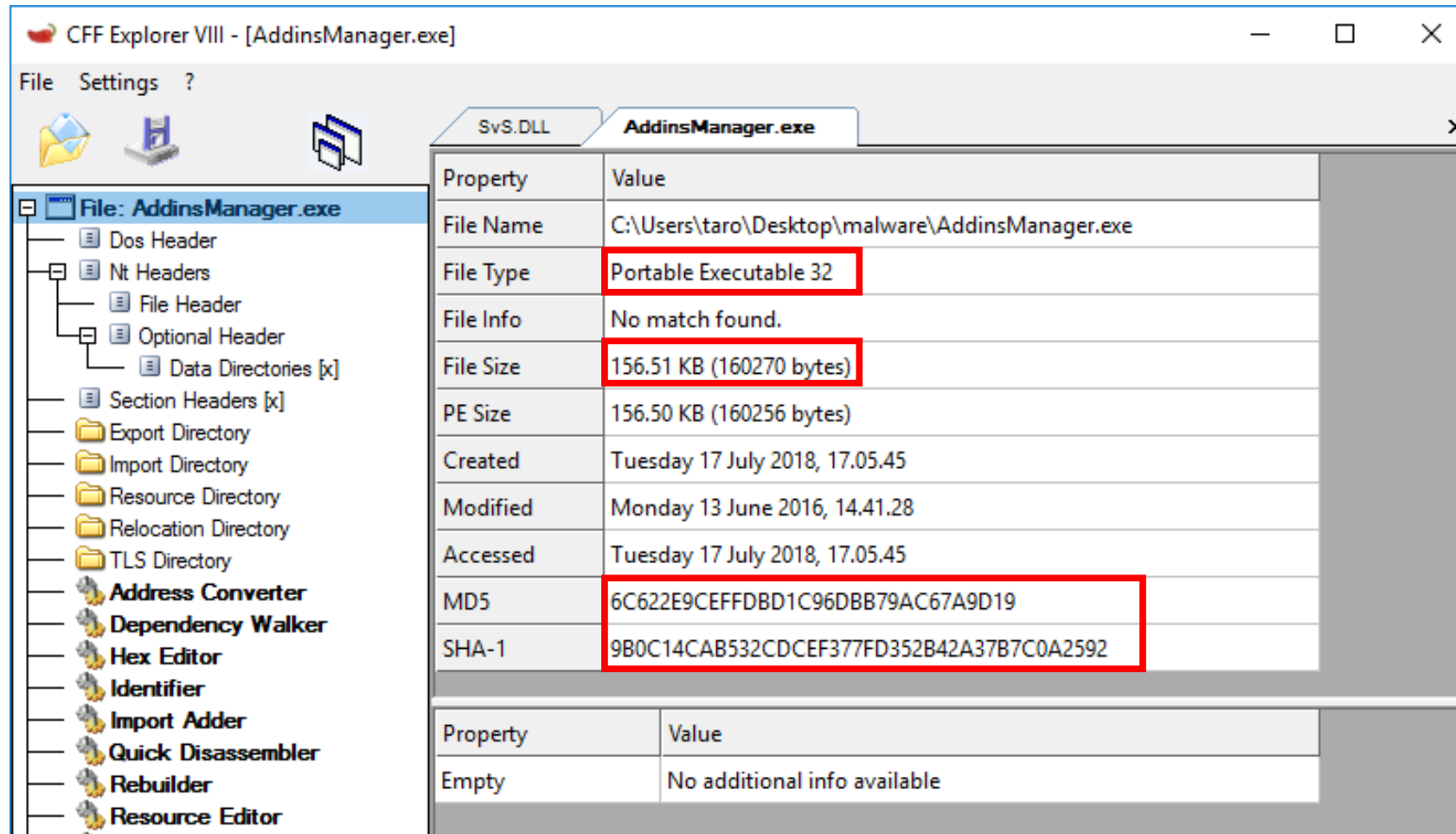
- This file might communicate with an external host as the readable strings contained a sign of HTTP communication. In spite of it, this binary does not load any TCP/IP related DLLs such as WS2_32, wsock32, WinHttp or WinInet.
- Therefore, it might be packed or obfuscated.

Scenario 1 Labs: Surface Analysis for AddinsManager.exe

Scenario 1 Labs:

Surface Analysis for AddinsManager.exe (1)

- Drag and drop AddinsManager.exe onto CFF explorer.



CFF Explorer VIII - [AddinsManager.exe]

File Settings ?

File: AddinsManager.exe

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

Property	Value
File Name	C:\Users\taro\Desktop\malware\AddinsManager.exe
File Type	Portable Executable 32
File Info	No match found.
File Size	156.51 KB (160270 bytes)
PE Size	156.50 KB (160256 bytes)
Created	Tuesday 17 July 2018, 17.05.45
Modified	Monday 13 June 2016, 14.41.28
Accessed	Tuesday 17 July 2018, 17.05.45
MD5	6C622E9CEFFD8D1C96DBB79AC67A9D19
SHA-1	9B0C14CAB532CDCEF377FD352B42A37B7C0A2592

Property	Value
Empty	No additional info available

Scenario 1 Labs: Surface Analysis for

- Click “File Header” on the left pane.
- Click “Click here” on the “Characteristics” field.
- You can find that:
 1. This file is an EXE, and not a DLL.
 2. This file is a 32 bit binary.

The screenshot displays the CFF Explorer VIII interface for the file AddinsManager.exe. The left pane shows the file's structure, with 'File Header' selected and highlighted by a red box. The right pane shows a table of file headers. The 'Characteristics' field is highlighted with a red box, and a red box labeled 'Click here' is positioned over it. A 'Characteristics' dialog box is open, showing a list of file characteristics. The 'File is executable' and '32 bit word machine' checkboxes are checked and highlighted with red boxes.

Member	Offset	Size	Value	Meaning
Machine	00000084	Word	014C	Intel 386
NumberOfSections	00000086	Word	000B	
TimeDateStamp	00000088	Dword	3534352E	
PointerToSymbolTa...	0000008C	Dword	00027200	
NumberOfSymbols	00000090	Dword	00000000	
SizeOfOptionalHea...	00000094	Word	00E0	
Characteristics	00000096	Word	030E	Click here

Characteristics

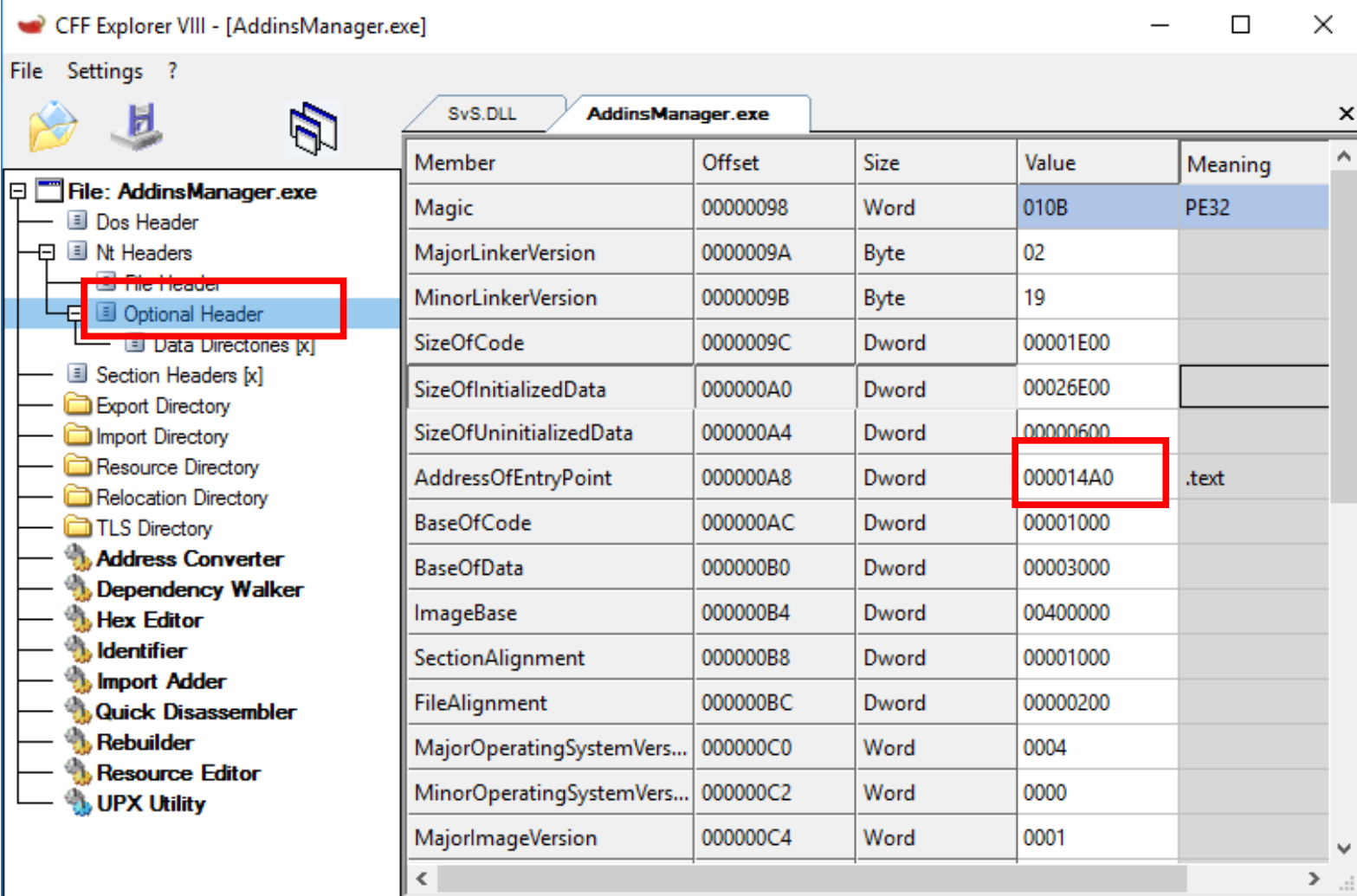
- ☒ File is executable
- ☐ File is a DLL
- ☐ System File
- ☐ Relocation info stripped from file
- ☒ Line numbers stripped from file
- ☒ Local symbols stripped from file
- ☐ Agressively trim working set
- ☐ App can handle >2gb address space
- ☐ Bytes of machine word are reversed (low)
- ☒ 32 bit word machine
- ☒ Debugging info stripped from file in .DBG file
- ☐ If Image is on removable media, copy and run from the swap
- ☐ If Image is on Net, copy and run from the swap file
- ☐ File should only be run on a UP machine
- ☐ Bytes of machine word are reversed (high)

OK Cancel

Scenario 1 Labs:

Surface Analysis for AddinsManager.exe (3)

- Click “Optional Header” on the left pane.
- You can find:
 - Offset of the entry point of this file is 0x14a0.



CFF Explorer VIII - [AddinsManager.exe]

File Settings ?

SvS.DLL AddinsManager.exe

File: AddinsManager.exe

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

Member	Offset	Size	Value	Meaning
Magic	00000098	Word	010B	PE32
MajorLinkerVersion	0000009A	Byte	02	
MinorLinkerVersion	0000009B	Byte	19	
SizeOfCode	0000009C	Dword	00001E00	
SizeOfInitializedData	000000A0	Dword	00026E00	
SizeOfUninitializedData	000000A4	Dword	00000600	
AddressOfEntryPoint	000000A8	Dword	000014A0	.text
BaseOfCode	000000AC	Dword	00001000	
BaseOfData	000000B0	Dword	00003000	
ImageBase	000000B4	Dword	00400000	
SectionAlignment	000000B8	Dword	00001000	
FileAlignment	000000BC	Dword	00000200	
MajorOperatingSystemVersion	000000C0	Word	0004	
MinorOperatingSystemVersion	000000C2	Word	0000	
MajorImageVersion	000000C4	Word	0001	

Scenario 1 Labs:

Surface Analysis for AddinsManager.exe (4)

- You can also find:
 1. Image size on memory is 0x2F000.

CFF Explorer VIII - [AddinsManager.exe]

File Settings ?

SvS.DLL AddinsManager.exe

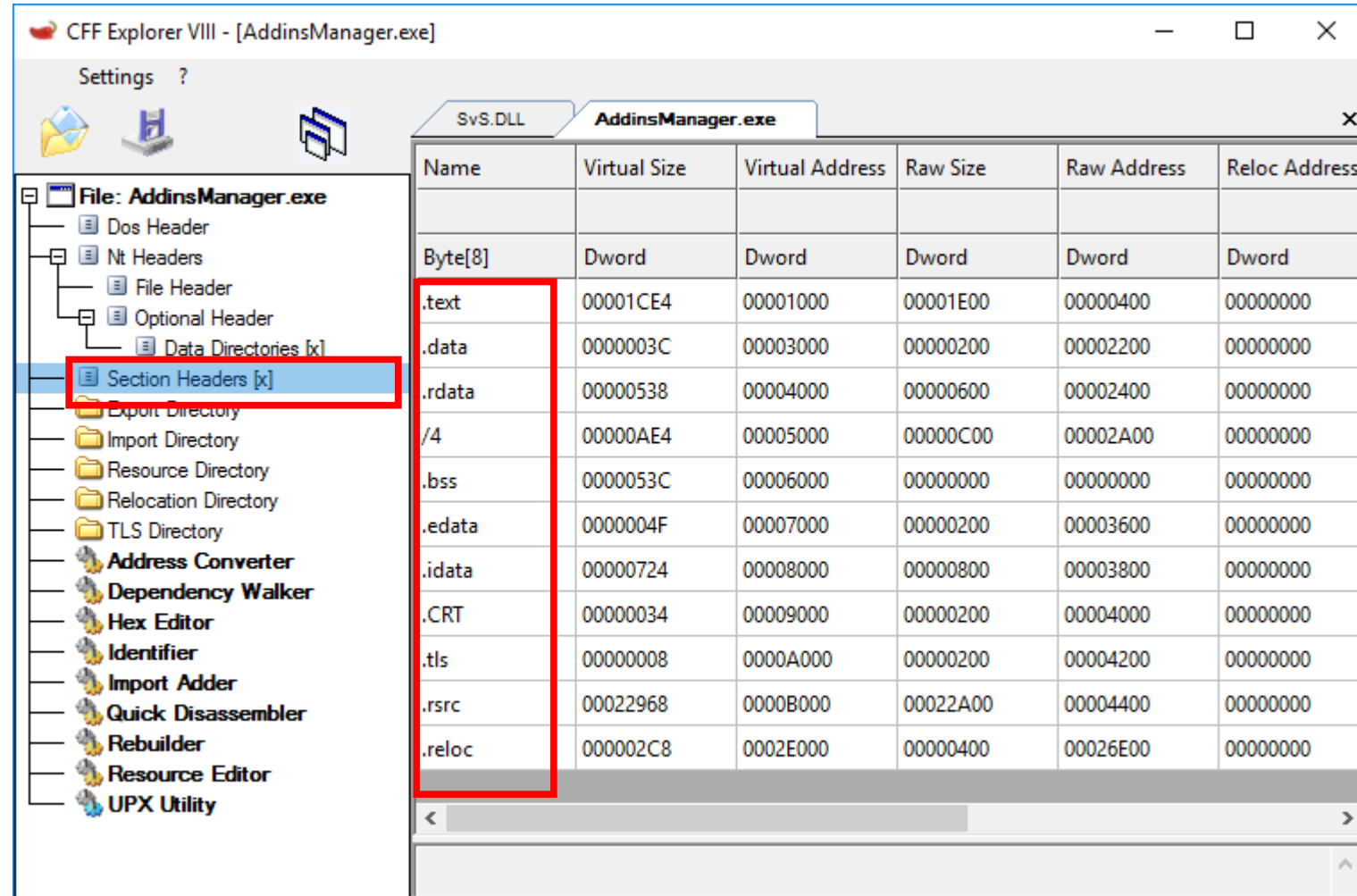
Member Offset Size Value Meaning

MinorImageVersion	000000C6	Word	0000	
MajorSubsystemVersion	000000C8	Word	0004	
MinorSubsystemVersion	000000CA	Word	0000	
Win32VersionValue	000000CC	Dword	00000000	
SizeOfImage	000000D0	Dword	0002F000	
SizeOfHeaders	000000D4	Dword	00000400	
Checksum	000000D8	Dword	0002F21B	
Subsystem	000000DC	Word	0002	Windows GUI
DllCharacteristics	000000DE	Word	0000	Click here
SizeOfStackReserve	000000E0	Dword	00200000	
SizeOfStackCommit	000000E4	Dword	00001000	
SizeOfHeapReserve	000000E8	Dword	00100000	
SizeOfHeapCommit	000000EC	Dword	00001000	
LoaderFlags	000000F0	Dword	00000000	
NumberOfRvaAndSizes	000000F4	Dword	00000010	

Scenario 1 Labs:

Surface Analysis for AddinsManager.exe (5)

- Click “Section Headers”.
- One of the section names “/4” looks strange and the number of sections seems to be greater than the number of typical binaries.



CFF Explorer VIII - [AddinsManager.exe]

Settings ?

File: AddinsManager.exe

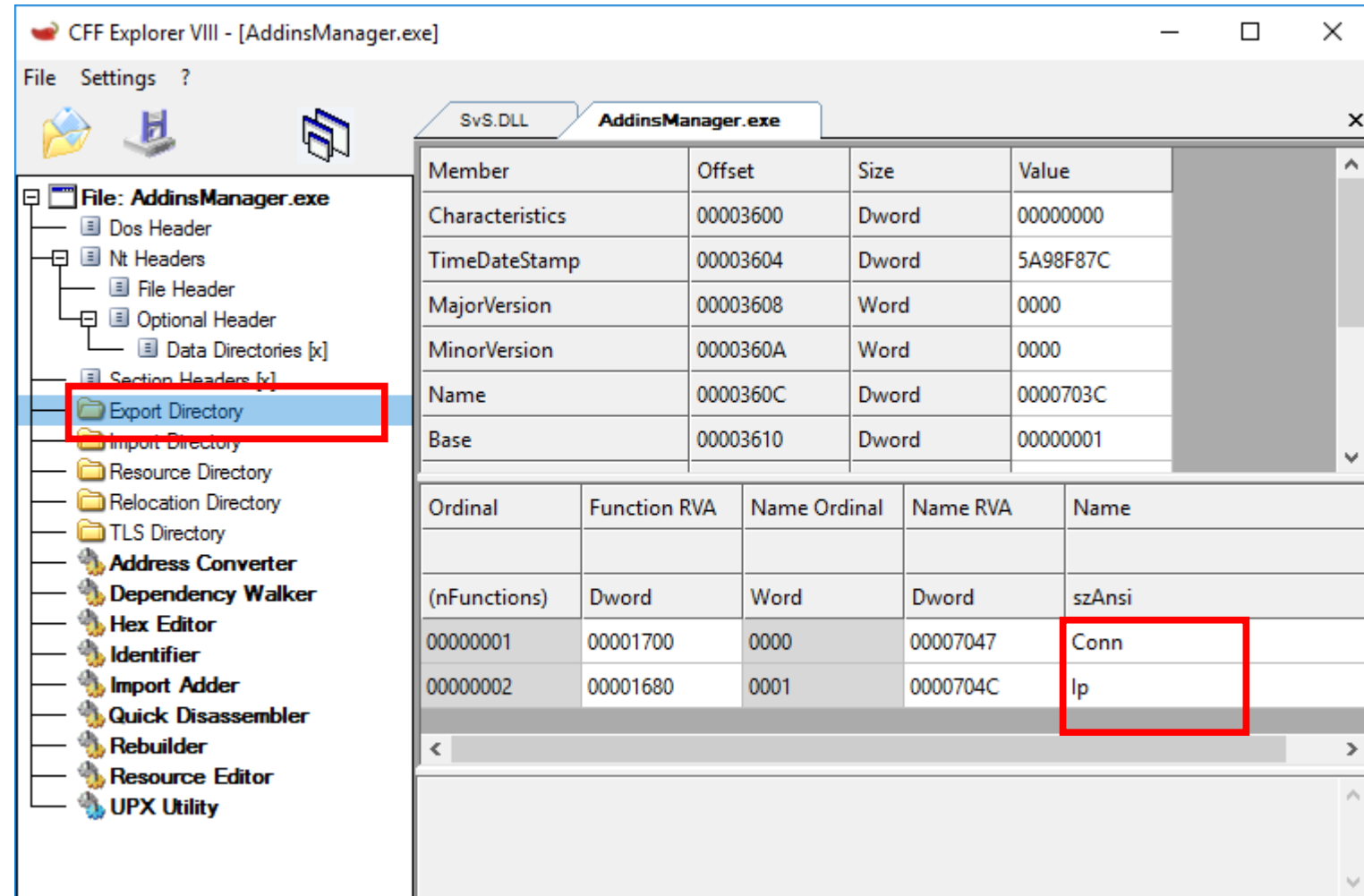
- Dos Header
- Nt Headers
- File Header
- Optional Header
- Data Directories [x]
- Section Headers [x]**
- Export Directory
- Import Directory
- Resource Directory
- Relocation Directory
- TLS Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler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

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address
Byte[8]	Dword	Dword	Dword	Dword	Dword
.text	00001CE4	00001000	00001E00	00000400	00000000
.data	0000003C	00003000	00000200	00002200	00000000
.rdata	00000538	00004000	00000600	00002400	00000000
/4	00000AE4	00005000	00000C00	00002A00	00000000
.bss	0000053C	00006000	00000000	00000000	00000000
.edata	0000004F	00007000	00000200	00003600	00000000
.idata	00000724	00008000	00000800	00003800	00000000
.CRT	00000034	00009000	00000200	00004000	00000000
.tls	00000008	0000A000	00000200	00004200	00000000
.rsrc	00022968	0000B000	00022A00	00004400	00000000
.reloc	000002C8	0002E000	00000400	00026E00	00000000

Scenario 1 Labs:

Surface Analysis for AddinsManager.exe (6)

- Click “Export Directory” on the left pane.
- It looks unusual. This is not a DLL, but it exports two APIs.



CFF Explorer VIII - [AddinsManager.exe]

File Settings ?

SvS.DLL AddinsManager.exe

Member Offset Size Value

Characteristics	00003600	Dword	00000000
TimeDateStamp	00003604	Dword	5A98F87C
MajorVersion	00003608	Word	0000
MinorVersion	0000360A	Word	0000
Name	0000360C	Dword	0000703C
Base	00003610	Dword	00000001

Ordinal Function RVA Name Ordinal Name RVA Name

(nFunctions)	Dword	Word	Dword	szAnsi
00000001	00001700	0000	00007047	Conn
00000002	00001680	0001	0000704C	Ip

Scenario 1 Labs:

Surface Analysis for AddinsManager.exe (7)

- Click “Import Directory” on the left pane.
- It imports only four modules.
- It loads WSOCK32.DLL.
 - It might communicate with external hosts.

CFF Explorer VIII - [AddinsManager.exe]

Settings ?

File: AddinsManager.exe

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

Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name
00003F18	N/A	0000383C	00003840	00003844	000
szAnsi	(nFunctions)	Dword	Dword	Dword	Dw
KERNEL32.dll	29	00008064	00000000	00000000	000
msvcrt.dll	25	000080DC	00000000	00000000	000
USER32.dll	1	00008144	00000000	00000000	000
WSOCK32.DLL	5	0000814C	00000000	00000000	000

OFTs	FTs (IAT)	Hint	Name
00003954	00003A54	00003DE4	00003DE6
Dword	Dword	Word	szAnsi
000085E4	000085E4	0026	connect
000085EE	000085EE	003D	recv
000085F6	000085F6	0043	send

Scenario 1 Labs:

Surface Analysis for AddinsManager.exe (8)

- Open cmd.exe and check readable strings on this binary.

```
strings -n 10 C:\Users\taro\Desktop\malware\AddinsManager.exe
```

- -n: Minimum string length
- We can find several remarkable strings.

```
outlook.net  
CONNECT %s:%d HTTP/1.1  
HTTP/  
200  
Conn
```

Is this a malicious server?

Scenario 1 Labs: Surface Analysis for AddinsManager.exe - Summary

The result of the surface analysis for AddinsManager.exe

Characteristics	Result
File type	Portable Executable 32 (32 bit binary)
File size	156.51 KB (160270 bytes)
MD5 hash	6C622E9CEFFDBD1C96DBB79AC67A9D19
SHA1 hash	9B0C14CAB532CDCEF377FD352B42A37B7C0A2592
PE characteristics	32 bit / EXE
Address of entry point	0x14A0
Size of image	0x2f000 (192,512)
Import table	It might communicate with external hosts because it loads WSOCK32.DLL.
Export table	It exports two APIs in spite of a executable file.
Notable strings	outlook.net, CONNECT %s:%d HTTP/1.1, HTTP/, 200 and Conn

Scenario 1 Labs: Surface Analysis for AddinsManager.exe – Summary (Cont.)

- This file might communicate with an external host as imported APIs and readable strings indicate.
- The section names look strange. Therefore, this file might be obfuscated or packed.