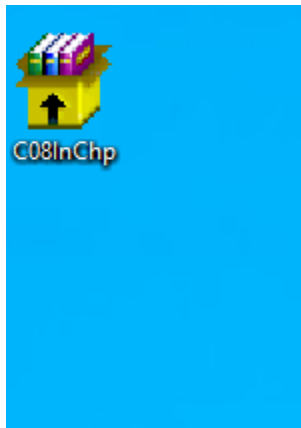


Task 1:



In this step, I have moved the chapter 8.exe file to my Windows VM.

New Case Information

Steps

1. Case Information
2. Optional Information

Case Information

Case Name:

Base Directory:

Case Type: ☒ Single-User ☐ Multi-User

Case data will be stored in the following directory:

< Back Next > Finish Cancel Help

In this step, I am creating a new case.

EXIF Metadata

Table Thumbnail Summary






Save Table as CSV

Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Date Created	Device Model	Device Make	File Path
IMG_1345.jpg				File	Not Notable				2009-04-05 18:39:04 PDT	Canon PowerShot SD670 IS	Canon	/img_C08InChp.dd/Homework/IMG_1345.jpg
Odyssey1.txt				File	Not Notable				2001-08-07 11:50:49 PDT	Dimage Z330 Zoom	Minolta Co., Ltd	/img_C08InChp.dd/Homework/Odyssey1.txt
RBATWNR.jpg				File	Not Notable				2009-04-05 18:39:04 PDT	Canon PowerShot SD670 IS	Canon	/img_C08InChp.dd/\$RECYCLE.BIN/RBATWNR
_R2WHGRN.txt				File	Not Notable				2001-08-07 11:50:49 PDT	Dimage Z330 Zoom	Minolta Co., Ltd	/img_C08InChp.dd/\$RECYCLE.BIN/_R2WHGR
R0006332.jpg				File	Not Notable				2009-04-05 18:39:04 PDT	Canon PowerShot SD670 IS	Canon	/img_C08InChp.dd/\$CarvedFiles/1/R0006332




















< >

Data Content

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Date Created	Device Model	Device Make	File Path
 _MG_1345.jpg				File	Not Notable				2009-04-05 18:39:04 PDT	Canon PowerShot SD870 IS	Canon	/img_C08InChp.dd/Homework/_MG_1345.jpg
 _Odyssey11.txt				File	Not Notable				2001-08-07 11:50:49 PDT	Damage 2330 Zoom	Minolta Co., Ltd	/img_C08InChp.dd/Homework/Odyssey11.txt
 _RBA1_MG_1345.jpg				File	Not Notable				2009-04-05 18:39:04 PDT	Canon PowerShot SD870 IS	Canon	/img_C08InChp.dd/RECYCLE.BIN/_RBA1N
 _R2WHGRN.txt				File	Not Notable				2001-08-07 11:50:49 PDT	Damage 2330 Zoom	Minolta Co., Ltd	/img_C08InChp.dd/RECYCLE.BIN/_R2WHG
 _f0006352.jpg				File	Not Notable				2009-04-05 18:39:04 PDT	Canon PowerShot SD870 IS	Canon	/img_C08InChp.dd/ScavedFiles/1/f0006352

Data Content									
Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Page:	1	of 2	Page: < →	Go to Page:	1	Jump to Offset:		Launch in HxD	
0x00000000:	FF D8 FF E0	00 10 4A 4E	49 4E 00 01	01 01 00 78JFIF....X				
0x00000010:	00 78 00 00	FF E1 03 1C	45 78 69 6E	00 00 45 49	..x.....Exif..II				
0x00000020:	2A 00 08 00	00 00 0B 00	0E 01 02 00	0A 00 00 00	*.....				
0x00000030:	92 00 00 00	0F 01 02 00	12 00 00 00	9C 00 00 00				
0x00000040:	10 01 02 00	12 00 00 00	AE 00 00 00	12 01 03 00				
0x00000050:	01 00 00 00	01 00 00 00	1A 01 05 00	01 00 00 00				
0x00000060:	C0 00 00 00	1B 01 06 00	01 00 00 00	C8 00 00 00				
0x00000070:	28 01 03 00	01 00 00 00	02 00 97 02	31 01 02 00	(.....1.....				
0x00000080:	0A 00 00 00	D0 00 00 00	32 01 02 00	14 00 00 002.....				
0x00000090:	DA 00 00 00	13 02 03 00	01 00 00 00	02 09 97 02				

Keyword search		33 results								
Table	Thumbnail	Summary								
Save Table as CSV										
Name	Keyword Preview	Location	Modified Time	Change Time	Access Time	Created Time				
 _RANH86F.txt	at once, there are «fifty» two chosen youths f	/img_C08InChp.dd/\$RECYCLE.BIN/_RANH86F.txt	2007-02-01 13:11:50 PST	0000-00-00 00:00:00	2017-07-10 00:00:00 PDT	2017-07-10 17:54:13 PT				
 Unalloc_4_1536000_10485760	le work, and on the «fifty» calypso sent him fr	/img_C08InChp.dd/\$Unalloc/Unalloc_4_1536000_1048...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				
 _R8ATNM9.jpg	«fifif» pexicanoncanon p	/img_C08InChp.dd/\$RECYCLE.BIN/_R8ATNM9.jpg	2017-07-10 17:50:56 PDT	0000-00-00 00:00:00	2017-07-10 00:00:00 PDT	2017-07-10 17:55:54 PT				
 _5.XLS	ocks of sheep, with «fifty» head in each flock.	/img_C08InChp.dd/Accounts/GovernmentDATA/_5.XLS	2007-02-01 13:33:28 PST	0000-00-00 00:00:00	2017-07-10 00:00:00 PDT	2017-07-10 17:53:53 PT				
 f0000192.txt	le work, and on the «fifty» calypso sent him fr	/img_C08InChp.dd/\$CarvedFiles/1/f0000192.txt	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				
 _51.XLS	zzzz«zfif»«exif» minol	/img_C08InChp.dd/Accounts/GovernmentDATA/_51...	2007-02-01 13:34:06 PST	0000-00-00 00:00:00	2017-07-10 00:00:00 PDT	2017-07-10 17:53:53 PT				
 f0000280.txt	at table, there are «fifty» maid servants in th	/img_C08InChp.dd/\$CarvedFiles/1/f0000280.txt	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				
 f0000784.txt	at once, there are «fifty» two chosen youths f	/img_C08InChp.dd/\$CarvedFiles/1/f0000784.txt	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				
 f0001008.txt	n though there were «fifty» bands of men surrou	/img_C08InChp.dd/\$CarvedFiles/1/f0001008.txt	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				
 Odyssey05.txt	le work, and on the «fifty» calypso sent him fr	/img_C08InChp.dd/Homework/Odyssey05.txt	2007-02-01 13:03:44 PST	0000-00-00 00:00:00	2017-07-10 00:00:00 PDT	2017-07-10 17:54:13 PT				
 _R63H7RL.txt	n though there were «fifty» bands of men surrou	/img_C08InChp.dd/\$RECYCLE.BIN/_R63H7RL.txt	2007-02-01 13:13:54 PST	0000-00-00 00:00:00	2017-07-10 00:00:00 PDT	2017-07-10 17:54:13 PT				
 Odyssey07.txt	at table, there are «fifty» maid servants in th	/img_C08InChp.dd/Homework/Odyssey07.txt	2007-02-01 13:04:44 PST	0000-00-00 00:00:00	2017-07-10 00:00:00 PDT	2017-07-10 17:54:13 PT				
 gametour2.exe	zzzz«zfif»«exif» minol	/img_C08InChp.dd/Vacation Pictures/gametour2.exe	2001-08-05 07:50:24 PDT	0000-00-00 00:00:00	2017-07-10 00:00:00 PDT	2017-07-10 17:55:39 PT				
 gametour3.exe	zzzz«zfif»«exif» minol	/img_C08InChp.dd/Vacation Pictures/gametour3.exe	2001-08-07 04:51:44 PDT	0000-00-00 00:00:00	2017-07-10 00:00:00 PDT	2017-07-10 17:55:39 PT				
 _REVVHBl.txt	le work, and on the «fifty» calypso sent him fr	/img_C08InChp.dd/\$RECYCLE.BIN/_REVVHBl.txt	2007-02-01 13:03:44 PST	0000-00-00 00:00:00	2017-07-10 00:00:00 PDT	2017-07-10 17:54:13 PT				
 gametour4.exe	zzzz«zfif»«exif» minol	/img_C08InChp.dd/Vacation Pictures/gametour4.exe	2001-08-08 08:23:54 PDT	0000-00-00 00:00:00	2017-07-10 00:00:00 PDT	2017-07-10 17:55:39 PT				
 Odyssey12.txt	ocks of sheep, with «fifty» head in each flock.	/img_C08InChp.dd/Homework/Odyssey12.txt	2007-02-01 13:09:18 PST	0000-00-00 00:00:00	2017-07-10 00:00:00 PDT	2017-07-10 17:54:13 PT				
 _NTONY-1.TXT	thee a hundred and «fifty» ways: therefore	/img_C08InChp.dd/\$OrphanFiles/_NTONY-1.TXT	2007-02-01 19:51:50 PST	0000-00-00 00:00:00	2007-02-06 00:00:00 PST	2007-02-06 15:20:57 PT				
 _RH2IF84.txt	at table, there are «fifty» maid servants in th	/img_C08InChp.dd/\$RECYCLE.BIN/_RH2IF84.txt	2007-02-01 13:04:44 PST	0000-00-00 00:00:00	2017-07-10 00:00:00 PDT	2017-07-10 17:54:13 PT				
Data Content										
Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results				
Pages: 1 of 13	Page	Go to Page: 1	Jump to Offset	Annotations	Other					

The screenshot shows the Immunity Debugger interface. The main window displays the disassembly of the executable 'gametour2.exe'. The assembly code is shown in a table with columns for Offset(h), hex, mnemonics, and comments. The 'Special editors' pane on the right is open, showing the 'Data inspector' tab. This pane lists various data types and their values, such as Int8, UInt8, Int16, and pointers to memory locations. The 'Byte order' section shows 'Little endian' selected, and the 'Hexadecimal basis' section is unchecked.

Offset(h)	hex	mnemonics	comments
00000000	7A 7A 7A 0A 00 10 7A 46	jmpz .z.FFF....x	
00000010	00 78 00 00 FF E1 03 1C	js .x.yA..ExiF..II	
00000020	2A 00 08 00 00 0B 00 0E	0E 02 00 0A 00 00	
00000030	92 00 00 00 0F 01 02 00	12 00 00 9C 00 00	
00000040	10 01 02 00 12 00 00 AE	00 12 01 03 00	
00000050	01 00 00 01 01 00 08 00	1A 01 05 00 01 00	
00000060	C0 00 00 00 1B 01 05 00	01 00 00 C8 00 00	
00000070	28 01 03 00 01 00 00 02	00 97 02 31 01 02 00	
00000080	0A 00 00 00 D0 00 00 32	01 02 00 14 00 00	
00000090	DA 00 00 00 13 02 03 01	00 00 00 02 00 97 02	
000000A0	69 87 04 00 01 00 00 0E	00 00 00 00 00 00 00	
000000B0	20 20 20 20 20 20 20 20	20 20 20 4D 69 6E 6F 6C 74	
000000C0	61 20 43 6F 2C 20 4C 74	6D 20 44 69 6D 61 20 4C 74	
000000D0	67 65 20 32 33 33 30 20	5A 6F 6F 6D 20 48 00	
000000E0	00 01 01 00 00 48 00 00	00 01 00 00 20 20	
000000F0	20 20 20 20 20 20 20 20	32 30 31 3A 30 38 3A	
00000100	30 35 20 31 34 3A 35 30	3A 30 37 10 10 27 08	
00000110	03 00 04 00 00 B4 01 00	00 00 00 07 04 00	
00000120	00 30 32 31 30 03 00 02	00 14 00 00 BC 01	
00000130	00 00 04 50 02 00 14 00	00 00 D0 01 00 01 91	
00000140	07 00 04 00 00 01 02 03	00 00 02 91 05 00 01 00	
00000150	00 E4 01 00 00 01 92 0A	00 01 00 00 EC 01	
00000160	00 02 52 05 00 01 00 00	00 F4 01 00 04 92	
00000170	0A 01 01 00 00 FC 01 00	00 09 92 03 00 01 00	
00000180	00 01 00 00 00 0A 92 05	00 01 00 00 04 02	
00000190	00 7C 92 07 00 08 01 00	00 0C 02 00 00 A0	
000001A0	07 04 00 00 30 31 30 01	00 A0 03 00 01 00	
000001B0	00 01 00 00 00 02 A0 04	01 00 00 00 80 03	
000001C0	00 03 A0 04 01 01 00 00	58 02 00 00 00 00	
000001D0	00 64 04 00 64 00 64 00	32 30 31 3A 30	
000001E0	38 3A 30 35 20 31 34 3A	35 30 3A 30 37 00 32	
000001F0	30 31 3A 30 38 3A 30 35	20 31 34 3A 35 30 3A 30	

Special editors

Data inspector

Binary (8 bit)	Value
Int8	122
UInt8	122
Int16	31354
UInt16	31354
Int24	8026746
UInt24	8026746
Int32	2054847098
UInt32	2054847098
Int64	5078389124054547066
UInt64	5078389124054547066
LEB128	-6
ULEB128	122
AnsiChar / char_t	z
WideChar / char16_t	z
UTF-8 code point	z (U+007A)
Single (float32)	3.25139583610295E35
Double (float64)	3.303815300226569E31
OLETIME	Invalid
FILETIME	Invalid
DOS date	3/26/2041

Byte order

☒ Little endian ☐ Big endian

☐ Hexadecimal basis (for integral numbers)


Offset(h): 0

Overwrite

In this step, I have downloaded HxD and opened the gametour2.exe file.

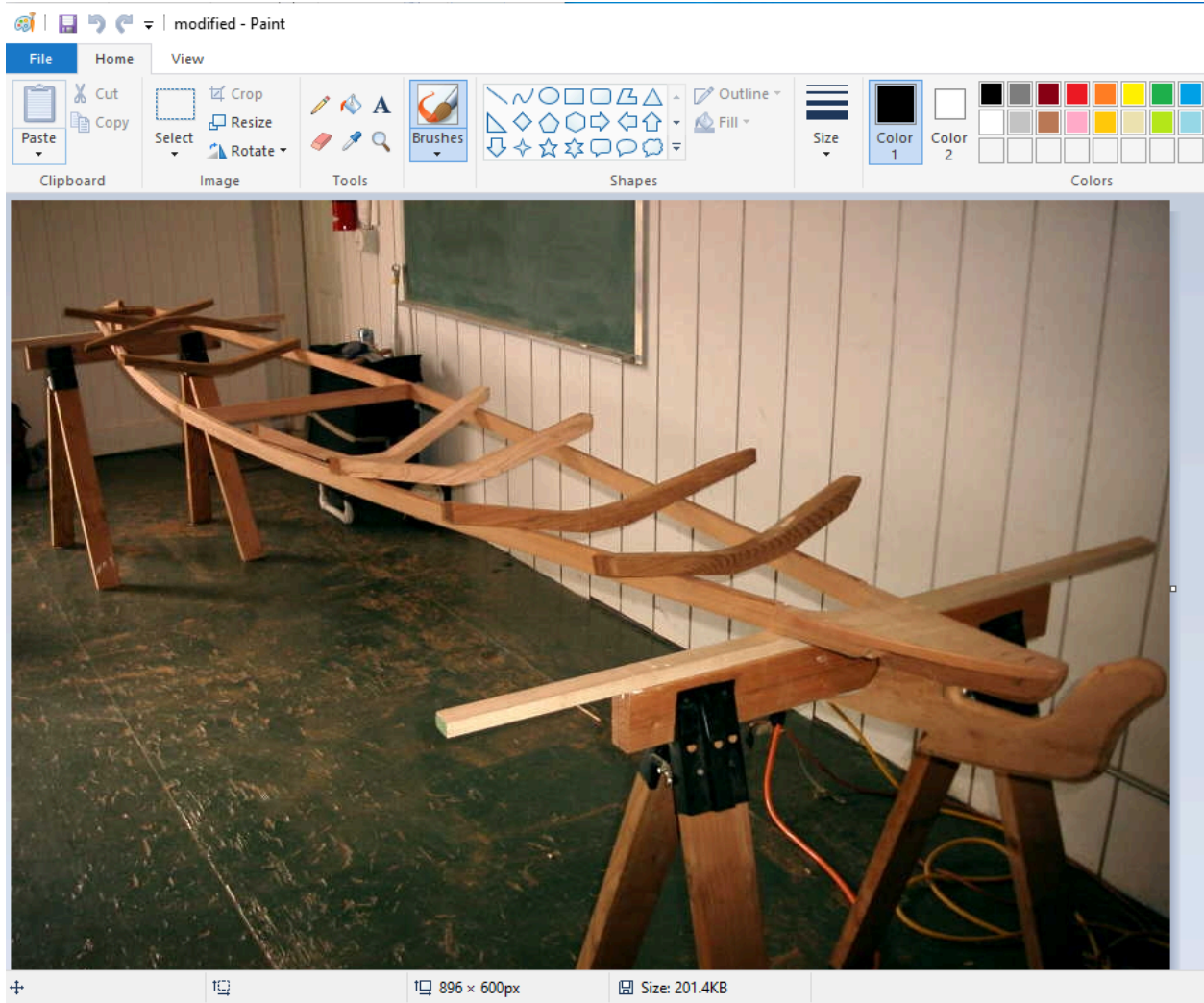
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	FF	D8	DD	E0	00	10	7A	46	49	46	00	01	01	01	00	78	ÿøÝà.zFIF.....x
00000010	00	78	00	00	FF	E1	03	1C	45	78	69	66	00	00	49	49	.x..ÿá..Exif..II
00000020	2A	00	08	00	00	00	0B	00	0E	01	02	00	0A	00	00	00	*.....
00000030	92	00	00	00	0F	01	02	00	12	00	00	00	9C	00	00	00	'.....æ...
00000040	10	01	02	00	12	00	00	00	AE	00	00	00	12	01	03	00©.....
00000050	01	00	00	00	01	00	08	00	1A	01	05	00	01	00	00	00
00000060	C0	00	00	00	1B	01	05	00	01	00	00	00	C8	00	00	00	À.....È...
00000070	28	01	03	00	01	00	00	00	02	00	97	02	31	01	02	00	(.....-..l...
00000080	0A	00	00	00	00	00	00	00	32	01	02	00	14	00	00	00Ð...2.....

Here I have replaced the first 4 bytes with the JFIF header values.

 gametour2.exe

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	FF	D8	DD	E0	00	10	4A	46	49	46	00	01	01	01	00	78	ÿøÝà..JFIF.....x
00000010	00	78	00	00	FF	E1	03	1C	45	78	69	66	00	00	49	49	.x..ÿá..Exif..II
00000020	2A	00	08	00	00	00	0B	00	0E	01	02	00	0A	00	00	00	*.....
00000030	92	00	00	00	0F	01	02	00	12	00	00	00	9C	00	00	00	'.....æ...
00000040	10	01	02	00	12	00	00	00	AE	00	00	00	12	01	03	00©.....

I have replaced the z in ZFIF to J and see that the 6th byte has changed.



I have saved the modified file and can now view it in paint.

Task 2:

```
timothyd@ubuntu:~$ echo "Launch Codes: 123123" > secret.txt
```

In this step, I am creating a secret message and storing it in a file.

```
timothyd@ubuntu:~$ steghide embed -ef secret.txt -cf city.jpeg
Enter passphrase:
Re-Enter passphrase:
embedding "secret.txt" in "city.jpeg"... done
```

In this step, I have embedded the password into the jpeg file that I downloaded from the internet.

```
need to get 213 kB of archives.
After this operation, 701 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu jammy/universe amd64 libmcrypt4 amd64 2.5.8-7 [213 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu jammy/universe amd64 steghide amd64 0.5.1-15 [213 kB]
Fetched 213 kB in 1s (237 kB/s)
Selecting previously unselected package libmcrypt4.
Reading database ... 255366 files and directories currently installed.)
Preparing to unpack .../libmcrypt4_2.5.8-7_amd64.deb ...
Unpacking libmcrypt4 (2.5.8-7) ...
Selecting previously unselected package steghide.
Preparing to unpack .../steghide_0.5.1-15_amd64.deb ...
Unpacking steghide (0.5.1-15) ...
Setting up libmcrypt4 (2.5.8-7) ...
Setting up steghide (0.5.1-15) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.6) ...
timothyd@ubuntu:~$ echo "Launch Codes: 123123" > secret.txt
timothyd@ubuntu:~$ steghide embed -ef secret.txt -cf city.jpeg
Enter passphrase:
Re-Enter passphrase:
steghide: could not open the file "city.jpg".
timothyd@ubuntu:~$ steghide embed -ef secret.txt -cf city.jpeg
Enter passphrase:
Re-Enter passphrase:
steghide: could not open the file "city.jpeg".
timothyd@ubuntu:~$ ls
base64  dns.txt  Downloads  key.gpg  message.txt.sig  my.log  originalfile  plain.txt  Public  snap  Videos
Desktop  Documents  inspec_4.18.114-1_amd64.deb  message.txt  Music  my.log-  Pictures  plain.txt.enc  secret.txt  Templates
timothyd@ubuntu:~$ ls
base64  Desktop  Documents  inspec_4.18.114-1_amd64.deb  message.txt  Music  my.log-  Pictures  plain.txt  plain.txt.enc  secret.txt  Templates  Videos
city.jpeg  dns.txt  Downloads  key.gpg  message.txt.sig  my.log  originalfile  plain.txt  Public  snap  Templates  Videos
timothyd@ubuntu:~$ steghide embed -ef secret.txt -cf city.jpeg
Enter passphrase:
Re-Enter passphrase:
embedding "secret.txt" in "city.jpeg"... done
timothyd@ubuntu:~$ eog city.jpeg
```

I have opened the image and there seems to be no noticeable difference in the image.

```
timothyd@ubuntu:~$ steghide extract -sf city.jpeg
Enter passphrase:
the file "secret.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "secret.txt".
timothyd@ubuntu:~$ cat secret.txt
Launch Codes: 123123
timothyd@ubuntu:~$
```

I then have extracted the secret file and am outputting the message.