Exercise 2:

File01: FF D8 FF E0

|  |  |  |  |
| --- | --- | --- | --- |
|  | File type | header | Footer/trailer |
| FTK imager | JFIF - JPEG | FF D8 FF E0 00 10 4A 46 49 46 00 | FF D9 |
| HexEdit | JFIF - JPEG | FF D8 FF E0 00 10 4A 46 49 46 00 | FF D9 |
| TrID  : Marco Pontello, marcopon@gmail.com | 38.1% matching JPG  28.6% matching JPG  23.8% matching MP3  9.5% matching MP3 | FF D8 FF E0 00 10 4A 46 49 46 00 | FF D9 |
| ExitTool | Photoshop cs3 |  |  |

File02

|  |  |  |  |
| --- | --- | --- | --- |
|  | File type | header | Footer/trailer |
| FTK Imager | GIF87a bitmap | 47 49 46 38 37 61 67 01 39 | 00 3B (.;) |
| HexEdit | GIF87a bitmap | 47 49 46 38 37 61 67 01 39 | 00 3B (.;) |
| TrID:  Marco Pontello  marcopon@gmail.com | 60% matching GIF,  30% matching GIF |  |  |
| ExifTool | GIP |  |  |

File03

|  |  |  |  |
| --- | --- | --- | --- |
|  | File type | header | Footer/trailer |
| FTK Imager | Internet URL | 5B 49 6E 74 65 72 6E 65 | No footer |
| HexEdit  www.dc3.mil/challenge/..Modified=70C990463628VB0139 | Internet URL | 5B 49 6E 74 65 72 6E 65 | No footer |
| TrID:  Marco Pontello  marcopon@gmail.com | 91.7% matching URL;  8.3% matching INI | Windows URL shortcut  INI Generic Configuration |  |
| ExifTool |  |  |  |

Note: [InternetShortcut] URL=http://www.dc3.mil/challenge/..Modified=70C990463628VB0139File04

|  |  |  |  |
| --- | --- | --- | --- |
|  | File type | header | Footer/trailer |
| FTK Imager | PKZIP | 50 4B 03 04 | 50 4B |
| HexEdit | PKZIP | 50 4B 03 04 | 50 4B  00 00 00 = … |
| TrID:  Marco Pontello  marcopon@gmail.com | 100% matching ZIP | PKZIP compressed archive |  |

File05

|  |  |  |  |
| --- | --- | --- | --- |
|  | File type | header | Footer/trailer |
| FTK Imager | XPI | 50 4B 03 04 | 00 00 00 = … |
| HexEdit | XPI | 50 4B 03 04 | 00 00 00 = … |
| TrID:  Marco Pontello  marcopon@gmail.com | 66.6% = XPI,  33% = ZIP,  0.1% = CEL | Mozilla Firefox Browser extension – XPI  ZIP compression  Autodesk FLIC Image File extension |  |

File06

|  |  |  |  |
| --- | --- | --- | --- |
|  | File type | header | Footer/trailer |
| FTK Imager | XML  (DMG file) | Got: 78 01 63 60  From garykessler:  78 01 73 0D 62 62 60 | No footer |
| HexEdit | XML  (DMG file) | Got: 3C 3F 78 01 63 60  From garykessler:  3C 3F 78 01 73 0D 62 62 60 | No footer |
| TrID:  Marco Pontello  marcopon@gmail.com | 50% DMG  50% XMI | Disk Image (Macintosh) compressed XML  XMill is an efficient XML data compressor |  |

File07

|  |  |  |  |
| --- | --- | --- | --- |
|  | File type | header | Footer/trailer |
| FTK Imager | HTTP | 68 74 74 70 | No footer |
| HexEdit | HTTP | 68 74 74 70 |  |
| TrID:  Marco Pontello  marcopon@gmail.com | 100% RPM Package generic | Maybe a RedHat Package Manager file since seeing several files nested inside from reading the hex |  |

File08

|  |  |  |  |
| --- | --- | --- | --- |
|  | File type | header | Footer/trailer |
| FTK Imager | ITSF | 49 54 53 46  gary:  Microsoft Compiled HTML Help File | No footer |
| HexEdit | ITSF | 49 54 53 46  gary:  Microsoft Compiled HTML Help File | No footer |
| TrID:  Davide “Airex” Airaghi  airex”AT”Tiscali”DOT”.it | 100% CHM file | Microsoft Compiled HTML Help File | No footer |

File09

|  |  |  |  |
| --- | --- | --- | --- |
|  | File type | header | Footer/trailer |
| FTK Imager | MThd  MIDI | 4D 54 68 64  gary:  Musical Instrument Digital Interface (MIDI) sound file | No footer |
| HexEdit | MThd  MIDI | 49 54 53 46  gary:  Musical Instrument Digital Interface (MIDI) sound file | No footer |
| TrID:  Marco Pontello  marcopon@gmail.com | 100% MIDI | MIDI Music  URL: www.midi.org | No footer |

File10

|  |  |  |  |
| --- | --- | --- | --- |
|  | File type | header | Footer/trailer |
| FTK Imager | A readme file from Microsoft File Checksum Integrity | 4D 69 63 72 6F 73 6F 66  gary:  Microsoft | No footer |
| HexEdit | A readme file from Microsoft File Checksum Integrity | 4D 69 63 72 6F 73 6F 66  gary:  Microsoft | No footer |
| TrID:  nothing | 0.0% matched |  | No footer |

Note: it seems to be a FCIV (File Checksum Integrity Verifier V2.05) readme file which is a text file and txt has no file header info but when we do txt as extension, it opens up ok as readme file

File11

|  |  |  |  |
| --- | --- | --- | --- |
|  | File type | header | Footer/trailer |
| FTK Imager |  | D0 CF 11 E0 A1 B1 1A E1  An Object Linking and Embedding (OLE) format known as Compound Binary File format by Microsoft used by Microsoft Office | No footer |
| HexEdit |  | D0 CF 11 E0 A1 B1 1A E1  An Object Linking and Embedding (OLE) format known as Compound Binary File format by Microsoft used by Microsoft Office | No footer |
| TrID:  Marco Pontello  [marcopon@gmail.com](mailto:marcopon@gmail.com)  URL  http://office.microsoft.com | 36% DOC  33.7 % XLS  21.3% DOC  9% | Microsoft Word Doc  Microsoft Excel sheet  Microsoft Word doc (old ver)  Generic OLE2/Multistream Compound File | No footer |

Note: rename the file to 11.doc and it opens up as a windows word doc.

File12

|  |  |  |  |
| --- | --- | --- | --- |
|  | File type | header | Footer/trailer |
| FTK Imager |  |  | No footer |
| HexEdit |  | 64 38 3A 61 | No footer |
| TrID:  Marco Pontello  [marcopon@gmail.com](mailto:marcopon@gmail.com)  URL  http://office.microsoft.com | 57.7% TORRENT  42.3%  TORRENT | Bit Torrent Link (Trackerless)  Bit Torrent Link | No footer |
| ExifTool | Torrent | Note: file extension: torrent |  |

File exte

Note: with the hex found these info: http://old-releases.ubuntu.com/releases/9.10/

Ubunte CD release from 2009

name29:[ubuntu-9.10-desktop-amd64.iso](http://old-releases.ubuntu.com/releases/9.10/ubuntu-9.10-desktop-amd64.iso)

Exercise 3 file carving:

<http://resources.infosecinstitute.com/file-carving/#gref>

suspicious\_file

|  |  |  |  |
| --- | --- | --- | --- |
|  | File type | header | Footer/trailer |
| FTK | OLECF (?) | D0 CF 11 E0 A1 B1 1A E1 |  |
| HexEdit |  |  |  |
| TrID: | 100% OLE2 | Generic OLE2 Multistream Compound File |  |

Malwaretracker.com/doc.php:

Result: walware[150]

Embedded executable: found

Virustotal.com:

Generic OLE2 Multistream Compound File

Detection: CAT-QuickHeal OLE.Win32.Agent.EB => might be a trojan

NANO-Antivirus Virus.Win32.Gen.ccmw = >

Details tab:

See png file

Scalpel from Kali(linux):

1) scalpel –o /root/Desktop/ex3\_mp3/test –v /root/Desktop/c.mp3

2) able to extract to JPG and PGP files.

3) JPG file was Keira Knighty picture,

4) PGP files not able to decrypt because GpgEX application was not able to

1. scalpel –o /root/Desktop/ex3\_mp3/test –v /root/Desktop/Suspicious\_File
2. able to extract to PGP files
3. PGP files not able to decrypt because GpgEX application was not able to

Elcomsoft Forensic Disk Decryptor:

Downloaded for tried version and still not able to decrypt PGP

c.mp3

|  |  |  |  |
| --- | --- | --- | --- |
|  | File type | header | Footer/trailer |
| FTK |  |  |  |
| HexEdit | JFIF | 49 44 33 FF D8 FF E0 00 10 4A 46 49 46 49 46 00  ‘4A 46 49 46’ = JFIF  Gary:   |  |  |  | | --- | --- | --- | | FF D8 FF E0 xx xx 4A 46 49 46 00 |  | ÿØÿà..JF IF. | | JFIF, JPE, JPEG, JPG |  | [JPEG/JFIF graphics file](http://www.jpeg.org/public/jfif.pdf" \t "_blank) | | FF D9 |
| TrID: | 100% matching MP3 | Note: not a real mp3 file  49 44 33 : only read the 3 bytes from header info and assume it is mp3 |  |

|  |  |
| --- | --- |
| Offset at: | Header info |
|  |  |
|  |  |
|  |  |

Malwaretracker.com/doc.php:

Md5: 670a8c0db494ced4882e44b27dbd6af2

Sha1: c5e6e5e1715e90879829264c88ad83160bbe358c

Sha256:

Content/type: audio ID3 type verion 2.255.216

Analysis time: 5.2s

Result: clean

Virustotal.com

Md5: 670a8c0db494ced4882e44b27dbd6af2

Sha1: c5e6e5e1715e90879829264c88ad83160bbe358c

FileType: MP3

ID3Size 0

MIMETYPE audio/mpeg

Warning: invalid ID3 header

Foremost – got one file - extracted into OLE file

> foremost –i /root/Desktop/ex3/Suspicious\_file –o /root/Desktop/test

Structure storage viewer

Ex4:

1. will perform hashing on evidence file by using md5deep64
2. open from FTK Imager: Oracle VM VirtualBox Disk Image converted image from winxp.raw

3)use dd (path ex: dd if=/dev/zero of=/dev/sdb bs=8k) to do data dump of the winxp.vdi

3074048+0 records in

3074048+0 records out

1573912576 byes copied 255.919s (6.2M per second during copy);

4min 26sec

the plan:

-acquire image and convert to raw image so that we can analyze the data inside raw image

from winxp.vdi – is the Oracle virtual box image

1. acquire the image by using (bit by bit copy) to convert to a raw image from cmd do:

c:\Program Files\Oracle\VirtualBox>vboxmanage.exe internalcommands converttoraw c:\Users\cs2lab\Desktop\img\winxp.vdi c:\Users\cs2lab\Desktop\img\winxp\_img.raw

Converting image “C:\Users\cs2lab\Desktop\img” 214748364801 bytes (20480MB) to raw….

1. Chain of custody:

use sha1deep64 for hash for both the image and the copied image for verification of the hash value where the hash generated for the copied took a little longer. The hashes are different due to file size the copied is raw file with large file size of 20GB compare to the original 1.5GB. Plus the extension is the not same.

1. Md5deep64 to hash both the original and copied raw – takes a bit longer .
2. FTK image, add evidence of the copied raw image. (attach picture: first\_step.png)
3. See a folder named as “Chris Hemsworth”
4. Mount image as physical&logical with read only drive letter E:

Partition 1[204465MB] HPFS/NTFS

Where the drive is 18611GB free where 2.65 GB is used

1. go to Documents and Settings found as “Chris Hemsworth” folder, try to open, get permission deny.
2. Program Files folder found ‘xerox/nwwia’ folder is part of the Windows Image Acquisition service. It’s not a virus/malware of any kind.
3. From All Users folder, HexEdit of one of the playlist from My Music where My Picture folder is empty
4. Found secedit.sdb Security folder
5. exporting unallocated space
6. Windows/system32/spool/Printers access denied
7. Chris Hemsworth folder from FTK Imager:

Acquisition date is the day ‘we’ forensics engineer acquired the image into raw to start our analysis of this image - 2017/09/20 date started

Sector: sector count = 41913522 \* 512 per sector = 2.14597e10 bytes

2.14597e10 / 1024 = 20956761 kilobytes / 1024 = 20,465.5869 megabytes / 1024 = 19.9859247 gigabytes

(from FTK imager: 20465MB)

From FTK imager: use Verify Drive/Image feature to verify the hash = matched

- exported as image for EO1

From EnCase: add the E01 image and start verifying

Picture: sys\_info to get filesystem and volume, root\_time\_date.png,sector.png

Ex5:

Used AccessData Passwood Recovery to crack password on this ‘untitled.docx’ started 18:13:48 2017/09/15

2.3.1: PRTK takes too long to crack these files. Ex: Cass pdf file took over 24hrs.

‘Untitled1.ods’ , ‘Untitled1.doc’

1. password was cracked for casssh.pdf is ‘01frid’ and it opens up an image
2. ‘Untitled1.ods’
3. ‘Untitled1.doc’

Ex6: (more info)

-both files seem to be same, but the hast info are the not same. The file header hex info are the same but the content are the same.

- hash info using md5deep64:

c1l.png: 601450fd443v42f4ece0e3f001ed73b3

header info: 50 4E 47 0D 0A 1A 0A

footer info: 49 45 4E 44 AE 42 60 82

c2l.png: b914…..

header info: 50 4E 47 0D 0A 1A 0A

footer info: 49 45 4E 44 AE 42 60 82

Meta data:

Date created: 9/19/2017 3:48PM

Modified date: 8/9/2017 2:36PM

18,428 bytes – C1l.png

18,459 bytes– C2l.png

HexEdit:

c1l.png has IHDR, sBIT, pHYs, IDAT, IDAT, IDAT, IEND

Critical IDAT splits into three chunks where each chunk contains image data

sBIT pHY – between IDAT – might be something to think about

c2l.png has IHDR, IDAT, IEND (hidden message in the IDAT)

- Tools used:

exiftool, md5deep64, tweakPNG, rizzy.py

from kali:

1) run python rizzy.py – open GUI: get image button and provide the image file of c1l.png, select decode option, start

a) see c1l.png we took

replaced a character where the value is unknown or unrepresentable in Unicode – utf-8 error

b) get <http://xdSa5Xcrrrxxxolc.onion/>

as url hidden

2) stepic.py to check png files

a) \FF this is same error as UFT-8

b) get <http://xdSa5Xcrrrxxxolc.onion/>

68 74 74 70 3a 2f 2f 78 64 53 61 35 58 63 72 72 72 78 78 78 6f 6c 63 2e 6f 6e 69 6f 6e 2f

786453613558637272727878786f6c632e6f6e696f6e