Exercise1 = > <https://ufile.io/8vq49> - (zip file)

Exercise 2:

File01: FF D8 FF E0

|  |  |  |  |
| --- | --- | --- | --- |
|  | File type | header | Footer/trailer |
| FTK | 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 |

File02

|  |  |  |  |
| --- | --- | --- | --- |
|  | File type | header | Footer/trailer |
| FTK | 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 |  |  |

File03

|  |  |  |  |
| --- | --- | --- | --- |
|  | File type | header | Footer/trailer |
| FTK | 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 |  |

File04

|  |  |  |  |
| --- | --- | --- | --- |
|  | File type | header | Footer/trailer |
| FTK | 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 | PK | 50 4B 03 04 | 00 00 00 = … |
| HexEdit | PK | 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  ZIP compression  Autodesk FLIC Image File extension |  |

File06

|  |  |  |  |
| --- | --- | --- | --- |
|  | File type | header | Footer/trailer |
| FTK | XML (maybe) | Got: 78 01 63 60  From garykessler:  78 01 73 0D 62 62 60 | No footer |
| HexEdit | XML (maybe) | 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)  XMill compressed XML |  |

File07

|  |  |  |  |
| --- | --- | --- | --- |
|  | File type | header | Footer/trailer |
| FTK | 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 | 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 | 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 | A readme file from Microsoft | 4D 69 63 72 6F 73 6F 66  gary:  Microsoft | No footer |
| HexEdit | A readme file from Microsoft | 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

File11

|  |  |  |  |
| --- | --- | --- | --- |
|  | File type | header | Footer/trailer |
| FTK |  | 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 |

File12

|  |  |  |  |
| --- | --- | --- | --- |
|  | File type | header | Footer/trailer |
| FTK |  |  | No footer |
| HexEdit |  |  | 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 |

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)