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

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		

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	

File04

	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) XMill compressed XML	

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	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 Imager		D0 CF 11 E0 A1 B1	No footer

		1A E1 An Object Linking and Embedding (OLE) format known as Compound Binary File format by Microsoft used by Microsoft Office	
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 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 Imager			No footer
HexEdit			No footer
TrID: Marco Pontello 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

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 = >

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	FF D9
TrID:	100%	Note: not a real mp3 file	

	matching MP3	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

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

Ex5:

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

Queue file 'Unititled1.ods'

Ex6: (more info)

1)replaced a character where the value is unknown or unrepresentable in Unicode

2) http://xdSa5Xcrrrxxxolc.onion/