DIFO 2017 - Lab 1 Report

Group number: Group 14

Group members: Wisam Faik, Md Piar Hossain, Cecilia To

# Exercise 1 - Hashing

**Objective:** Acquire data as acquisition to ensure the integrity of evidence as read-only.

**Chain-of-custody**: generated hash values for all evidence acquired.

Our objective for this exercise was to find the hash values of all four files.

* **What files (and/or folders) did you hash?**

’hello’, ’hello(2)’, ’hello(3)’ and ’hello(4)’ files were all hashed using md5deep64.exe, sha256deep64.exe and whirlpooldeep64.exe.

The commands used were:

i) this is using md5deep64:

> C:\...path…\md5deep64.exe hello

da5c61e1edc0f18337e46418e48c1290 ” hello”

> C:\...path…\md5deep64.exe ”hello (2)”

cdc47d670159eef60916ca03a9d4a007 ”hello (2)”

> C:\...path…\md5deep64.exe ”hello (3)”

cdc47d670159eef60916ca03a9d4a007 ”hello (3)”

> C:\...path…\md5deep64.exe ”hello (4)”

da5c61e1edc0f18337e46418e48c1290 ” hello”

ii) this is using sha256deep64:

> C:\...path…\sha256deep64.exe hello

fad878bd261840a4ea4a8277c546d4f46e79bbeb60b059cee41f8b50e28d0e88 C:\...path…\hello

> C:\...path…\sha256deep64.exe “hello (2)”

1316543942a8c6cd754855500cd37068edbbd8b31c4979d2825a4e799fed6102 “C:\...path…\hello (2)”

> C:\...path…\sha256deep64.exe “hello (3)”

60d13913155644883f130b85eb24d778314014c9479aedb5f6323bf38ad3a451 “C:\...path…\hello (3)”

> C:\...path…\sha256deep64.exe “hello (4)”

1c4ff4e490b15b2b214f26c5654decccbcbea9eb900f88649dc7b1e42341be56 “C:\...path…\hello (4)”

iii) this is using whirlpooldeep64:

> C:\...path…\whirlpooldeep64.exe “C:\...path…\hello”

>1f4388f4a81a6cfacde955cf5fd84c4e76f12876db3356e2a84efda91f8c44407b3626b770d9752f9b0aa05927e7fb7c66e07ea96ea47ece2ca78a40cedb9d7e

> C:\...path…\whirlpooldeep64.exe “C:\...path…\hello (2)”

aae0a840704962b3026cf5b2058aa1a3d7752e6d562e0a843ce0abf7107666fb475ac45df08587c468f7754847f2be4cebd1172dedfebfaa6527c8da2b1bc364

> C:\...path…\whirlpooldeep64.exe “C:\...path…\hello (3)”

959593fe62721c9d058831eaa742f103d1b853b43a81a94dd30cc89a6dafb6926b64bdd7b0ef16a4c566601f81af95988fb952720482562a6269728ef5f5d5fb

> C:\...path…\whirlpooldeep64.exe “C:\...path…\hello (4)”

4324731f2340b0d5ce741f566abd7ebf8a1c18a15e4835bd8c25bdc974ec275a6e088982422456060bf145d7013cd0aa8ac1b62ee3f8149bfd6490e6a5a95efa

* **Which algorithms did you choose?**

Initially, we only used md5 algorithms and we noticed using md5, the ’hello’ with ’hello (4) files have same the hash values where ’hello (2)’ with ’hello (3)’ files have the same hash values. Because of this finding, we decided to use sha256 and whirlpool algorithms to ensure and confirm if these files truly have the same hash values. While using sha256 and whirlpool algorithms, we discovered the hash values were not the same for all four files.

The algorithms chosen for hashing ’hello’, ’hello(2)’, ’hello(3)’ and ’hello(4)’ were sha256, whirlpool and md5. The reason algorithm sha256 and whirlpool generated different hash values because sha256 digests input message length up to 264 bits in length and whirlpool digests input message length up to 2256 which results into different hash values for all four files. Whirlpool generates 512 bits length and sha256 generates 256 bits length.

* **Suppose you would need to calculate the hash sums of several files and folders, how could you do that using the tools and resources provided? Provide a description and exact commands.**

According to the <http://md5deep.sourceforge.net/>, ’-r’ flag can be used to hash all files within a folder recursively. This ’–r’ option doesn’t hash the folder but only the files inside a folder.

Command used:

> C:\..input path…\whirlpooldeep64.exe -t -r C:\..input folder path > output\_whirlpool.txt

Output\_test.txt looks like this:

1f4388f4a81a6cfacde955cf5fd84c4e76f12876db3356e2a84efda91f8c44407b3626b770d9752f9b0aa05927e7fb7c66e07ea96ea47ece2ca78a40cedb9d7e 2017:09:14:12:27:34 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hashing\test\hello

959593fe62721c9d058831eaa742f103d1b853b43a81a94dd30cc89a6dafb6926b64bdd7b0ef16a4c566601f81af95988fb952720482562a6269728ef5f5d5fb 2017:09:14:12:27:34 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hashing\test\hello (3)

aae0a840704962b3026cf5b2058aa1a3d7752e6d562e0a843ce0abf7107666fb475ac45df08587c468f7754847f2be4cebd1172dedfebfaa6527c8da2b1bc364 2017:09:14:12:27:34 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hashing\test\hello (2)

4324731f2340b0d5ce741f566abd7ebf8a1c18a15e4835bd8c25bdc974ec275a6e088982422456060bf145d7013cd0aa8ac1b62ee3f8149bfd6490e6a5a95efa 2017:09:14:12:27:34 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hashing\test\hello (4)

> C:\..input path… \md5deep64.exe -t –r C:\..input folder path > output\_md5.txt

Output\_test.txt looks like this:

da5c61e1edc0f18337e46418e48c1290 2017:09:14:12:27:34 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hashing\test\hello

cdc47d670159eef60916ca03a9d4a007 2017:09:14:12:27:34 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hashing\test\hello (2)

cdc47d670159eef60916ca03a9d4a007 2017:09:14:12:27:34 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hashing\test\hello (3)

da5c61e1edc0f18337e46418e48c1290 2017:09:14:12:27:34 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hashing\test\hello (4)

> C:\..input path… \shar256deep64.exe –r C:\..input folder path > output\_md5.txt

Output\_test.txt looks like this:

fad878bd261840a4ea4a8277c546d4f46e79bbeb60b059cee41f8b50e28d0e88 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hashing\test\hello

1316543942a8c6cd754855500cd37068edbbd8b31c4979d2825a4e799fed6102

C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hashing\test\hello (2)

60d13913155644883f130b85eb24d778314014c9479aedb5f6323bf38ad3a451 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hashing\test\hello (3)

1c4ff4e490b15b2b214f26c5654decccbcbea9eb900f88649dc7b1e42341be56 C:\Users\cs2lab\Desktop\Shared\_Folder\DiFo2017\Lab1\Exercise1\_Hashing\test\hello (4)

* **Come up with an efficient way to match hash sums – so that you can automatically identify files that might (or might not be) of interest. Describe how you did this and which exact programs you used, and reflect upon why this might be useful for a forensic examiner in their work life.**

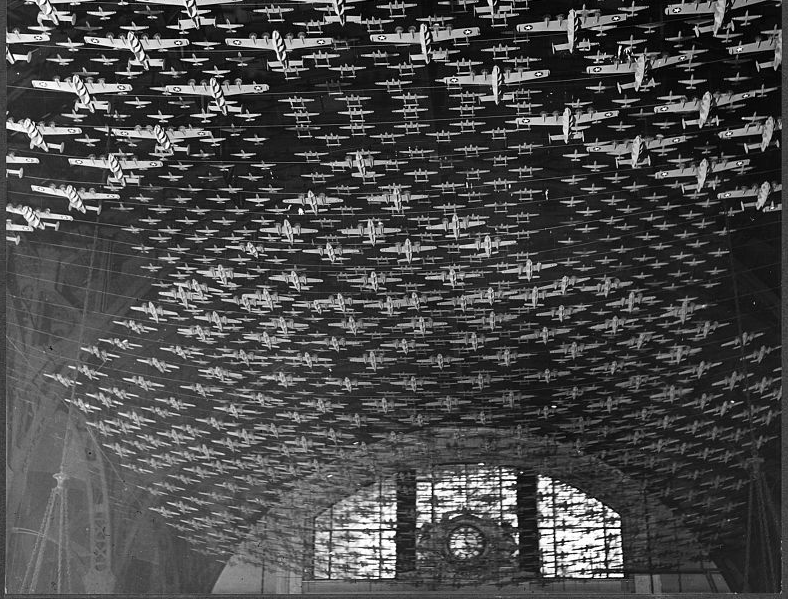
We used the ‘-m’ with md5deep64.exe,(sha256 & whirlpool)

# Exercise 2 - File Headers

We used these TrID, FTK Imager, HexEdit and Exiftool tools to identify the filer header and footer information. All twelve files were identified by using the Gary Kessler File Signature Table, http://www.garykessler.net/library/file\_sigs.html.

With File: 01

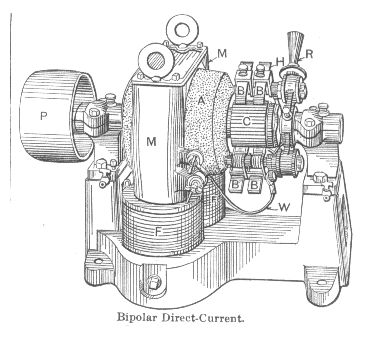
Result file 01: We were able to identify this file to be a JPEG file because the file header hexadecimal values (FF D8 FF E0 00 10 4A 46 49 46 00) matched from Gary Kessler File Signature table . But with TrID, it provided matching based on percentage of accuracy. There were four matching found for file 01 using TrID. 38.1 % and 28.6% of JPG file matching but there were also 23.8% and 9.5% matching to MP3 file. See table below.



|  |  |  |  |
| --- | --- | --- | --- |
| Tools | 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 | N/A | N/A |
| Exiftool | Photoshop cs3 | N/A | N/A |

With File: 02

Result file 02: We were able to identify this file to be a GIF file:



see table below.

|  |  |  |  |
| --- | --- | --- | --- |
| Tools | 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 | N/A | N/A |
| ExifTool | GIP | N/A | N/A |

With File: 03

Result file 03: We were able to identify this file to be an internet shortcut because according Gary Kessler File Signature Table, there was no file type matching the file header hexadecimal information we retrieved from FTK Imager and HexEdit. See table below.

|  |  |  |  |
| --- | --- | --- | --- |
| Tools | File type | header | Footer/trailer |
| FTK Imager  URL=http://www.dc3.mil/challenge/  Modified=70C990463628CB0139 | N/A | 5B 49 6E 74 65 72 6E 65 | No footer |
| HexEdit  www.dc3.mil/challenge/..Modified=70C990463628VB0139 | Read only File | 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 | N/A |
| ExifTool | Unknown | N/A | N/A |

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

With File: 04

Result file 04: We were able to identify this file to be a PK Zip file. See table below.

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

With File: 05

Result file 05: We were able to identify this file to be an XPI file….???. See table below.

|  |  |  |  |
| --- | --- | --- | --- |
|  | File type | header | Footer/trailer |
| FTK Imager | 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 – XPI  ZIP compression  Autodesk FLIC Image File extension | N/A |

With File: 06

Result file 06: We were able to identify this file to be

|  |  |  |  |
| --- | --- | --- | --- |
|  | 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 | N/A |

File07

|  |  |  |  |
| --- | --- | --- | --- |
|  | File type | header | Footer/trailer |
| FTK Imager | HTTP | 68 74 74 70 | No footer |
| HexEdit | HTTP | 68 74 74 70 | N/A |
| 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 | N/A |

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 | N/A |

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 – Anti Forensics

Objective: To acquire the c.mp3 and Suspicious\_File evidences by using scalpel tool from Kali. Scalpel will automatically perform file carving on these two files.

**Acquisition:**

1. From Kali(linux) commands used for c.mp3 file:

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

Resulted with extraction of c.mp3 file into one JPG and three of PGP files. See appendix 1(c.mp3).

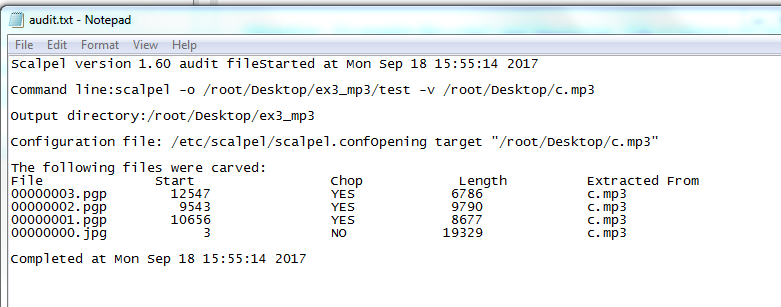


Figure 1: Summary Scalpel report on c.mp3 file.

* The 00000000.jpg file was a picture of Keira Knightley



Figure 2: Result of 00000000.jpg file.

* Three PGP files were not able to decrypt using this GpgEX tool.
* PGP files not able to decrypt because GpgEX tool requires a key to decrypt a pgp file.
* Foremost tool on Kali:
* Foremost -o /root/Desktop/ex3\_mp3/test –i /root/Desktop/c.mp3
* Extraction result was only one file. It was a 00000000.jpg file. Opening this extracted 0000000.jpg file revealed it was the same picture as from scalpel extracted 0000000.jpg file.

**Analysis:**

1. Windows: we used HexEdit and TrID to analyze further this c.mp3. It appeared to be that the c.mp3 file header has been modified with ’49 44 33’ to hide the real file type which was JFIF. But according to TrID, it reported 100% matching to mp3 file.

|  |  |  |  |
| --- | --- | --- | --- |
| Tools | File type | header | Footer/trailer |
| 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) | | 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 |  |

Malwaretracker.com/doc.php was used to analyze further of c.mp3 file:

Md5: 670a8c0db494ced4882e44b27dbd6af2

Sha1: c5e6e5e1715e90879829264c88ad83160bbe358c

Sha256:

Content/type: audio ID3 type verion 2.255.216

Analysis time: 5.2s

Result: clean

Virustotal.com was used to analyze further of c.mp3 file:

Md5: 670a8c0db494ced4882e44b27dbd6af2

Sha1: c5e6e5e1715e90879829264c88ad83160bbe358c

FileType: MP3

ID3Size 0

MIMETYPE audio/mpeg

Warning: invalid ID3 header

**Summary** of c.mp3 file:

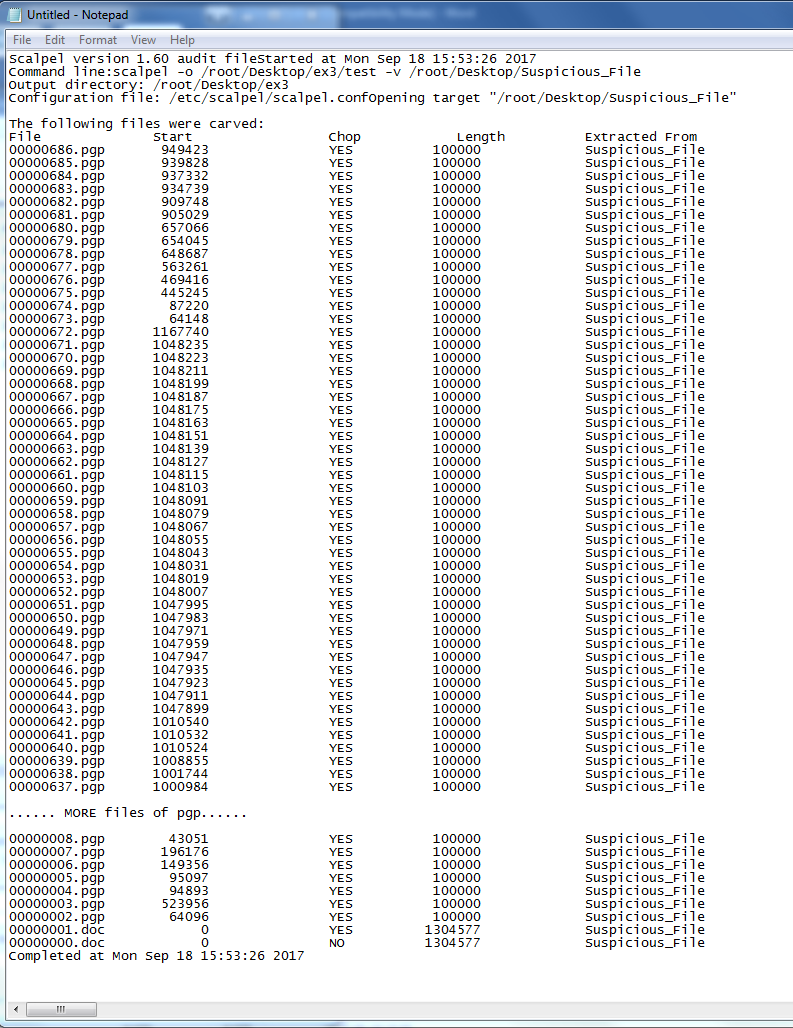
It appeared to be an image JPEG file but not a mp3 file. Based on the Virustotal.com warning message, the invalid ID3 header confirmed with HexEdit that the first 3 bytes of header information were modified to be a mp3 file.

**Acquisition:**

1. Scalpel from Kali(linux) commands used for Suspicious\_File file:

* scalpel –o /root/Desktop/ex3\_mp3/test –v /root/Desktop/ Suspicious\_File

Resulted with extraction of Suspicious\_File file into 687 files where two were doc files and the rest were PGP files. See appendix 2 (Suspicious\_File).



* With PGP files, we downloaded Elcomsoft Forensic Disk Decryptor to try to decrypt PGP files. But this tool also asked for the keys to these PGP files to decrypt them. We could not process further.
* Foremost tool on Kali:

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

* Foremost extracted into one OLE file (00000000.ole).
* We used Malwaretracker and Virustotal to analyze 00000000.ole file and the results were same as

**Analysis:**

suspicious\_file

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

Malwaretracker.com/doc.php redirected to this: cryptam.com:

Name of file: Susicious\_File

md5: 63017bb2a213fa440191b204929ab0f7

sha1: f454953c6ae4496b21d2e4c1006842aff60b90eb

sha256: cec6534e8ddc4f5f9e9b2a0cedb438a8419a5ffd08ecfe059467630f624d5b1a

ssdeep: 24576:ATgRvu+fNB53r3j1HXQ+5ql8ie+i0QMv4RhDHd91S1etww4qEyY9c4jC1CV+E4cY:ATgRvu+fNB53r3j1HA+5ql8iePd91YeX

signature hits:

2638: string. This program cannot be run in DOS mode

1244080: string.LoadLibraryA

1243996: string.GetModuleHandleA

1244048: string.GetCommandLineA

1246706: string.GetSystemMetrics

1243770: string.GetProcAddress

1243712: string.EnterCriticalSection

1243400: string.CloseHandle

1244398: string.CreateFileA

1247318: string.RegOpenKeyExA

1081060: string.user32.dll

1163676: string.KERNEL32

1161103: string.ExitProcess

1246846: string.GetMessageA

1246552: string.CreateWindowExA

dropped.file exe 91babceabb2263975b0c4309e82ca977 / 1302016 bytes / @ 2560

Also, Malwaretracker.com provided more details on the Suspicious\_File when we looked at the link to ‘decrypted raw strings’ option. From the decrypted raw string info, it revealed that there were several files with the word ‘copyright’ such as:

*- Copyright (C) 1998, Thomas G. Lane*

*- deflate 1.1.3 Copyright 1995-1998 Jean-loup Gailly*

*- inflate 1.1.3 Copyright 1995-1998 Mark Adler*

*- Copyright (c) 1992-2001 by P.J. Plauger, licensed by Dinkumware, Ltd. ALL RIGHTS RESERVED.*

*- Copyright 2003 - 2004 PopCap Games, Inc.*

Additionally, we found these URL of:

*- http://www.popcap.com/win32updatecheck2.php?prod=*

*- http://www.popcap.com/register.php?theGame=*

*- http://www.microsoft.com/directx*

*- http://www.popcap.com/beta\_validate.php?prod=*

*- http://store.gamehouse.com/buyzuma.jsp?AID=%AFFIL%&amp;D=%DAYS%&amp;M=%MINUTES%*

And these information:

* *OriginalFilename*
* *Zuma.exe*
* *ProductName*
* *Zuma Deluxe*
* *ProductVersion*
* *1.0.0.1*
* *SpecialBuild*
* *Presented by GameHouse*

We also discovered there were random information such as:

* TimeZoneName=Arab Standard Time
* Names of months but May, June and July months were missing
* Names of days
* Instructions
* names of players and characters
* names of sounds files
* names of image files

and many more…..

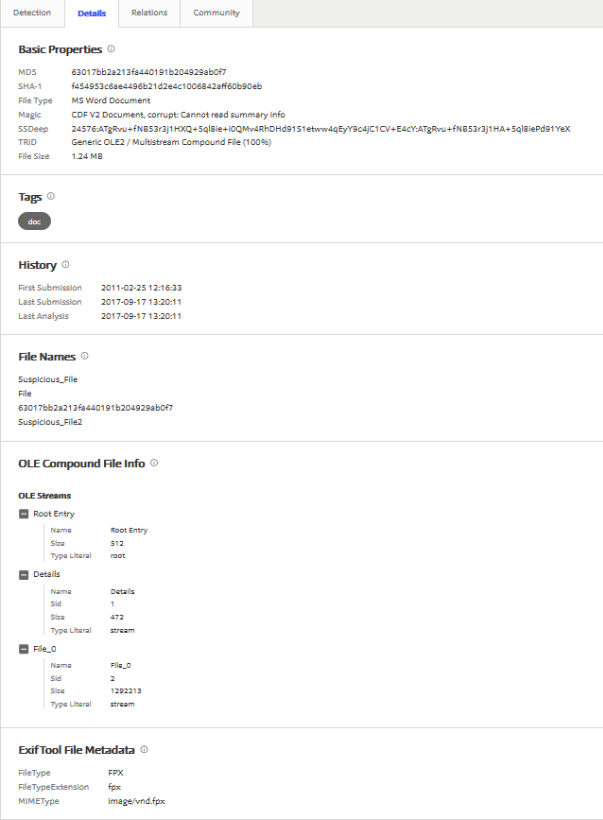
Virustotal.com:

Generic OLE2 Multistream Compound File

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

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

Details tab:



**Summary** of Suspicious\_File: it appeared to contain multiple files where we did not try to carve these files except when using Scalpel on a Linux system (Kali). This was where 687 files were carved.

See appendix 2

# Exercise 4 - Acquisition

See DIFO2017\_Lab1\_Report\_Group14\_Ex4.pdf

# Exercise 5 - Cracking

# Exercise 6 - Steganography

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec a diam lectus. Sed sit amet ipsum mauris. Maecenas congue ligula ac quam viverra nec consectetur ante hendrerit. Donec et mollis dolor. Praesent et diam eget libero egestas mattis sit amet vitae augue. Nam tincidunt congue enim, ut porta lorem lacinia consectetur. Donec ut libero sed arcu vehicula ultricies a non tortor. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean ut gravida lorem. Ut turpis felis, pulvinar a semper sed, adipiscing id dolor. Pellentesque auctor nisi id magna consequat sagittis. Curabitur dapibus enim sit amet elit pharetra tincidunt feugiat nisl imperdiet. Ut convallis libero in urna ultrices accumsan. Donec sed odio eros. Donec viverra mi quis quam pulvinar at malesuada arcu rhoncus. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. In rutrum accumsan ultricies. Mauris vitae nisi at sem facilisis semper ac in est.

Appendix 1: c.mp3

root@kali:~/Desktop/test# scalpel -o /root/Desktop/test/output\_mp3/ -v /root/Desktop/test/c.mp3

Scalpel version 1.60

Written by Golden G. Richard III, based on Foremost 0.69.

Output directory: "/root/Desktop/test/output\_mp3"

Configuration file: "/etc/scalpel/scalpel.conf"

Coverage maps directory: "/root/Desktop/test/output\_mp3"

Opening target "/root/Desktop/test/c.mp3"

Total file size is 19332 bytes

Image file pass 1/2.

Read 19332 bytes from image file.

/root/Desktop/test/c.mp3: 100.0% |\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*| 18.9 KB 00:00 ETAA jpg header was found at : 3

Memory reallocation performed, total header storage = 101

A jpg footer was found at : 19330

Memory reallocation performed, total footer storage = 101

A pgp header was found at : 10656

Memory reallocation performed, total header storage = 101

A pgp header was found at : 9543

Memory reallocation performed, total header storage = 101

A pgp header was found at : 12547

Allocating work queues...

Work queues allocation complete. Building carve lists...

Carve lists built. Workload:

art with header "\x4a\x47\x04\x0e" and footer "\xcf\xc7\xcb" --> 0 files

art with header "\x4a\x47\x03\x0e" and footer "\xd0\xcb\x00\x00" --> 0 files

gif with header "\x47\x49\x46\x38\x37\x61" and footer "\x00\x3b" --> 0 files

gif with header "\x47\x49\x46\x38\x39\x61" and footer "\x00\x3b" --> 0 files

jpg with header "\xff\xd8\xff\xe0\x00\x10" and footer "\xff\xd9" --> 1 files

png with header "\x50\x4e\x47\x3f" and footer "\xff\xfc\xfd\xfe" --> 0 files

bmp with header "\x42\x4d\x3f\x3f\x00\x00\x00" and footer "" --> 0 files

tif with header "\x49\x49\x2a\x00" and footer "" --> 0 files

tif with header "\x4d\x4d\x00\x2a" and footer "" --> 0 files

avi with header "\x52\x49\x46\x46\x3f\x3f\x3f\x3f\x41\x56\x49" and footer "" --> 0 files

mov with header "\x3f\x3f\x3f\x3f\x6d\x6f\x6f\x76" and footer "" --> 0 files

mov with header "\x3f\x3f\x3f\x3f\x6d\x64\x61\x74" and footer "" --> 0 files

mov with header "\x3f\x3f\x3f\x3f\x77\x69\x64\x65\x76" and footer "" --> 0 files

mov with header "\x3f\x3f\x3f\x3f\x73\x6b\x69\x70" and footer "" --> 0 files

mov with header "\x3f\x3f\x3f\x3f\x66\x72\x65\x65" and footer "" --> 0 files

mov with header "\x3f\x3f\x3f\x3f\x69\x64\x73\x63" and footer "" --> 0 files

mov with header "\x3f\x3f\x3f\x3f\x70\x63\x6b\x67" and footer "" --> 0 files

mpg with header "\x00\x00\x01\xba" and footer "\x00\x00\x01\xb9" --> 0 files

mpg with header "\x00\x00\x01\xb3" and footer "\x00\x00\x01\xb7" --> 0 files

fws with header "\x46\x57\x53" and footer "" --> 0 files

doc with header "\xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00" and footer "\xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00" --> 0 files

doc with header "\xd0\xcf\x11\xe0\xa1\xb1" and footer "" --> 0 files

pst with header "\x21\x42\x4e\xa5\x6f\xb5\xa6" and footer "" --> 0 files

dbx with header "\xcf\xad\x12\xfe\xc5\xfd\x74\x6f" and footer "" --> 0 files

idx with header "\x4a\x4d\x46\x39" and footer "" --> 0 files

mbx with header "\x4a\x4d\x46\x36" and footer "" --> 0 files

wpc with header "\x3f\x57\x50\x43" and footer "" --> 0 files

htm with header "\x3c\x68\x74\x6d\x6c" and footer "\x3c\x2f\x68\x74\x6d\x6c\x3e" --> 0 files

pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0d" --> 0 files

pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0a" --> 0 files

mail with header "\x41\x4f\x4c\x56\x4d" and footer "" --> 0 files

pgd with header "\x50\x47\x50\x64\x4d\x41\x49\x4e\x60\x01" and footer "" --> 0 files

pgp with header "\x99\x00" and footer "" --> 1 files

pgp with header "\x95\x01" and footer "" --> 0 files

pgp with header "\x95\x00" and footer "" --> 2 files

pgp with header "\xa6\x00" and footer "" --> 0 files

txt with header "\x2d\x2d\x2d\x2d\x2d\x42\x45\x47\x49\x4e\x20\x50\x47\x50" and footer "" --> 0 files

rpm with header "\xed\xab" and footer "" --> 0 files

wav with header "\x52\x49\x46\x46\x3f\x3f\x3f\x3f\x57\x41\x56\x45" and footer "" --> 0 files

ra with header "\x2e\x72\x61\xfd" and footer "" --> 0 files

ra with header "\x2e\x52\x4d\x46" and footer "" --> 0 files

dat with header "\x72\x65\x67\x66" and footer "" --> 0 files

dat with header "\x43\x52\x45\x47" and footer "" --> 0 files

zip with header "\x50\x4b\x03\x04" and footer "\x3c\xac" --> 0 files

java with header "\xca\xfe\xba\xbe" and footer "" --> 0 files

max with header "\x56\x69\x47\x46\x6b\x1a\x00\x00\x00\x00" and footer "\x00\x00\x05\x80\x00\x00" --> 0 files

pins with header "\x50\x49\x4e\x53\x20\x34\x2e\x32\x30\x0d" and footer "" --> 0 files

Carving files from image.

Image file pass 2/2.

/root/Desktop/test/c.mp3: 100.0% |\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*| 18.9 KB 00:00 ETAOPENING /root/Desktop/test/output\_mp3/pgp-34-0/00000003.pgp

CLOSING /root/Desktop/test/output\_mp3/pgp-34-0/00000003.pgp

OPENING /root/Desktop/test/output\_mp3/pgp-34-0/00000002.pgp

CLOSING /root/Desktop/test/output\_mp3/pgp-34-0/00000002.pgp

OPENING /root/Desktop/test/output\_mp3/pgp-32-0/00000001.pgp

CLOSING /root/Desktop/test/output\_mp3/pgp-32-0/00000001.pgp

OPENING /root/Desktop/test/output\_mp3/jpg-4-0/00000000.jpg

CLOSING /root/Desktop/test/output\_mp3/jpg-4-0/00000000.jpg

Processing of image file complete. Cleaning up...

Done.

Scalpel is done, files carved = 4, elapsed = 0 seconds.

Appendix 2: Suspicious\_File

1. edit the scalpel.conf file to so that would allow scalpel carve any file type.

root@kali:~# vi /etc/scalpel/scalpel.conf

root@kali:~# scalpel -o /root/Desktop/test -v /root/Desktop/test/Suspicious\_File

Scalpel version 1.60

Written by Golden G. Richard III, based on Foremost 0.69.

Output directory: "/root/Desktop/test"

Configuration file: "/etc/scalpel/scalpel.conf"

Coverage maps directory: "/root/Desktop/test"

1. root@kali:~# scalpel -o /root/Desktop/test/output/ -v /root/Desktop/test/Suspicious\_File

Scalpel version 1.60

Written by Golden G. Richard III, based on Foremost 0.69.

Output directory: "/root/Desktop/test/output"

Configuration file: "/etc/scalpel/scalpel.conf"

Coverage maps directory: "/root/Desktop/test/output"

Opening target "/root/Desktop/test/Suspicious\_File"

Total file size is 1304576 bytes

Image file pass 1/2.

Read 1304576 bytes from image file.

/root/Desktop/test/Suspicious\_File: 100.0% |\*\*\*\*\*\*\*\*\*\*\*\*| 1.2 MB 00:00 ETAA doc header was found at : 0

Memory reallocation performed, total header storage = 101

A doc footer was found at : 0

Memory reallocation performed, total footer storage = 101

A doc header was found at : 0

Memory reallocation performed, total header storage = 101

A pgp header was found at : 64096

Memory reallocation performed, total header storage = 101

A pgp header was found at : 523956

A pgp header was found at : 94893

Memory reallocation performed, total header storage = 101

A pgp header was found at : 95097

A pgp header was found at : 149356

A pgp header was found at : 196176

A pgp header was found at : 262143

A pgp header was found at : 856818

A pgp header was found at : 982885

A pgp header was found at : 1108369

A pgp header was found at : 1204055

A pgp header was found at : 1217347

A pgp header was found at : 1223699

A pgp header was found at : 1237111

A pgp header was found at : 1277062

A pgp header was found at : 18771

Memory reallocation performed, total header storage = 101

.......(nOTE: we removed the pgp header info due to redundency).....

A pgp header was found at : 146124

A pgp header was found at : 146126

A pgp header was found at : 146287

Memory reallocation performed, total header storage = 201

A pgp header was found at : 146289

A pgp header was found at : 146461

A pgp header was found at : 150171

A pgp header was found at : 150194

.......(nOTE: we removed the pgp header info due to redundency).....

A pgp header was found at : 373603

A pgp header was found at : 373646

A pgp header was found at : 373707

Memory reallocation performed, total header storage = 301

A pgp header was found at : 374113

A pgp header was found at : 374267

.......(nOTE: we removed the pgp header info due to redundency).....

A pgp header was found at : 521256

A pgp header was found at : 521564

Memory reallocation performed, total header storage = 401

A pgp header was found at : 521648

A pgp header was found at : 523777

.......(nOTE: we removed the pgp header info due to redundency).....

A pgp header was found at : 610528

A pgp header was found at : 610530

A pgp header was found at : 610631

A pgp header was found at : 610633

Memory reallocation performed, total header storage = 501

A pgp header was found at : 610698

A pgp header was found at : 610700

A pgp header was found at : 610760

.......(nOTE: we removed the pgp header info due to redundency).....

A pgp header was found at : 728136

A pgp header was found at : 728143

A pgp header was found at : 728150

Memory reallocation performed, total header storage = 601

A pgp header was found at : 728157

A pgp header was found at : 728164

A pgp header was found at : 729555

.......(nOTE: we removed the pgp header info due to redundency).....

A pgp header was found at : 924127

A pgp header was found at : 924177

A pgp header was found at : 924196

Memory reallocation performed, total header storage = 701

A pgp header was found at : 925296

A pgp header was found at : 925298

.......(nOTE: we removed the pgp header info due to redundency).....

A pgp header was found at : 1048223

A pgp header was found at : 1048235

A pgp header was found at : 1167740

A pgp header was found at : 64148

Memory reallocation performed, total header storage = 101

A pgp header was found at : 87220

A pgp header was found at : 445245

A pgp header was found at : 469416

A pgp header was found at : 563261

A pgp header was found at : 648687

A pgp header was found at : 654045

A pgp header was found at : 657066

A pgp header was found at : 905029

A pgp header was found at : 909748

A pgp header was found at : 934739

A pgp header was found at : 937332

A pgp header was found at : 939828

A pgp header was found at : 949423

Allocating work queues...

Work queues allocation complete. Building carve lists...

Carve lists built. Workload:

art with header "\x4a\x47\x04\x0e" and footer "\xcf\xc7\xcb" --> 0 files

art with header "\x4a\x47\x03\x0e" and footer "\xd0\xcb\x00\x00" --> 0 files

gif with header "\x47\x49\x46\x38\x37\x61" and footer "\x00\x3b" --> 0 files

gif with header "\x47\x49\x46\x38\x39\x61" and footer "\x00\x3b" --> 0 files

jpg with header "\xff\xd8\xff\xe0\x00\x10" and footer "\xff\xd9" --> 0 files

png with header "\x50\x4e\x47\x3f" and footer "\xff\xfc\xfd\xfe" --> 0 files

bmp with header "\x42\x4d\x3f\x3f\x00\x00\x00" and footer "" --> 0 files

tif with header "\x49\x49\x2a\x00" and footer "" --> 0 files

tif with header "\x4d\x4d\x00\x2a" and footer "" --> 0 files

avi with header "\x52\x49\x46\x46\x3f\x3f\x3f\x3f\x41\x56\x49" and footer "" --> 0 files

mov with header "\x3f\x3f\x3f\x3f\x6d\x6f\x6f\x76" and footer "" --> 0 files

mov with header "\x3f\x3f\x3f\x3f\x6d\x64\x61\x74" and footer "" --> 0 files

mov with header "\x3f\x3f\x3f\x3f\x77\x69\x64\x65\x76" and footer "" --> 0 files

mov with header "\x3f\x3f\x3f\x3f\x73\x6b\x69\x70" and footer "" --> 0 files

mov with header "\x3f\x3f\x3f\x3f\x66\x72\x65\x65" and footer "" --> 0 files

mov with header "\x3f\x3f\x3f\x3f\x69\x64\x73\x63" and footer "" --> 0 files

mov with header "\x3f\x3f\x3f\x3f\x70\x63\x6b\x67" and footer "" --> 0 files

mpg with header "\x00\x00\x01\xba" and footer "\x00\x00\x01\xb9" --> 0 files

mpg with header "\x00\x00\x01\xb3" and footer "\x00\x00\x01\xb7" --> 0 files

fws with header "\x46\x57\x53" and footer "" --> 0 files

doc with header "\xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00"

and footer "\xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00" --> 1 files

doc with header "\xd0\xcf\x11\xe0\xa1\xb1" and footer "" --> 1 files

pst with header "\x21\x42\x4e\xa5\x6f\xb5\xa6" and footer "" --> 0 files

dbx with header "\xcf\xad\x12\xfe\xc5\xfd\x74\x6f" and footer "" --> 0 files

idx with header "\x4a\x4d\x46\x39" and footer "" --> 0 files

mbx with header "\x4a\x4d\x46\x36" and footer "" --> 0 files

wpc with header "\x3f\x57\x50\x43" and footer "" --> 0 files

htm with header "\x3c\x68\x74\x6d\x6c" and footer "\x3c\x2f\x68\x74\x6d\x6c\x3e" --> 0 files

pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0d" --> 0 files

pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0a" --> 0 files

mail with header "\x41\x4f\x4c\x56\x4d" and footer "" --> 0 files

pgd with header "\x50\x47\x50\x64\x4d\x41\x49\x4e\x60\x01" and footer "" --> 0 files

pgp with header "\x99\x00" and footer "" --> 2 files

pgp with header "\x95\x01" and footer "" --> 13 files

pgp with header "\x95\x00" and footer "" --> 656 files

pgp with header "\xa6\x00" and footer "" --> 14 files

txt with header "\x2d\x2d\x2d\x2d\x2d\x42\x45\x47\x49\x4e\x20\x50\x47\x50" and footer "" --> 0 files

rpm with header "\xed\xab" and footer "" --> 0 files

wav with header "\x52\x49\x46\x46\x3f\x3f\x3f\x3f\x57\x41\x56\x45" and footer "" --> 0 files

ra with header "\x2e\x72\x61\xfd" and footer "" --> 0 files

ra with header "\x2e\x52\x4d\x46" and footer "" --> 0 files

dat with header "\x72\x65\x67\x66" and footer "" --> 0 files

dat with header "\x43\x52\x45\x47" and footer "" --> 0 files

zip with header "\x50\x4b\x03\x04" and footer "\x3c\xac" --> 0 files

java with header "\xca\xfe\xba\xbe" and footer "" --> 0 files

max with header "\x56\x69\x47\x46\x6b\x1a\x00\x00\x00\x00" and footer "\x00\x00\x05\x80\x00\x00" --> 0 files

pins with header "\x50\x49\x4e\x53\x20\x34\x2e\x32\x30\x0d" and footer "" --> 0 files

Carving files from image.

Image file pass 2/2.

/root/Desktop/test/Suspicious\_File: 100.0% |\*\*\*\*\*\*\*\*\*\*\*\*|

1.2 MB 00:00 ETAOPENING /root/Desktop/test/output/pgp-35-0/00000686.pgp

CLOSING /root/Desktop/test/output/pgp-35-0/00000686.pgp

OPENING /root/Desktop/test/output/pgp-35-0/00000685.pgp

CLOSING /root/Desktop/test/output/pgp-35-0/00000685.pgp

OPENING /root/Desktop/test/output/pgp-35-0/00000684.pgp

CLOSING /root/Desktop/test/output/pgp-35-0/00000684.pgp

.......(nOTE: we removed pgp files due to redundency).....

OPENING /root/Desktop/test/output/pgp-33-0/00000010.pgp

CLOSING /root/Desktop/test/output/pgp-33-0/00000010.pgp

OPENING /root/Desktop/test/output/pgp-33-0/00000009.pgp

CLOSING /root/Desktop/test/output/pgp-33-0/00000009.pgp

OPENING /root/Desktop/test/output/pgp-33-0/00000008.pgp

CLOSING /root/Desktop/test/output/pgp-33-0/00000008.pgp

OPENING /root/Desktop/test/output/pgp-33-0/00000007.pgp

CLOSING /root/Desktop/test/output/pgp-33-0/00000007.pgp

OPENING /root/Desktop/test/output/pgp-33-0/00000006.pgp

CLOSING /root/Desktop/test/output/pgp-33-0/00000006.pgp

OPENING /root/Desktop/test/output/pgp-33-0/00000005.pgp

CLOSING /root/Desktop/test/output/pgp-33-0/00000005.pgp

OPENING /root/Desktop/test/output/pgp-33-0/00000004.pgp

CLOSING /root/Desktop/test/output/pgp-33-0/00000004.pgp

OPENING /root/Desktop/test/output/pgp-32-0/00000003.pgp

CLOSING /root/Desktop/test/output/pgp-32-0/00000003.pgp

OPENING /root/Desktop/test/output/pgp-32-0/00000002.pgp

CLOSING /root/Desktop/test/output/pgp-32-0/00000002.pgp

OPENING /root/Desktop/test/output/doc-21-0/00000001.doc

CLOSING /root/Desktop/test/output/doc-21-0/00000001.doc

OPENING /root/Desktop/test/output/doc-20-0/00000000.doc

CLOSING /root/Desktop/test/output/doc-20-0/00000000.doc

Processing of image file complete. Cleaning up...

Done.

Scalpel is done, files carved = 687, elapsed = 1 seconds.