Muhammad Izham Bin Norhamadi  
B032020039

# Task 1

**Evidence Report for Project:** C10frag

**Project Number:** C10frag

**Project Description:**

**Image Files:**

**File Name:** C:\Users\Acer\Documents\kerja\BITS3443 Digital Forensics\W10\C10frag.eve

Image File Type: DFT Image

File Number: C10frag

Technician Name: Joe Friday

Date: 02/06/2007

Time: 21:29:01

Checksum: e549fa1ab8c66792ccc1b23990b0afba

Checksum Validated: Yes

Compressed image: No

Time Zone Information:

Time Zone: (GMT-08:00) Pacific Time (US & Canada); Tijuana (Pacific Standard Time)

Daylight savings (summertime) was in effect: Yes

Time Zone information obtained automatically from remote system/image.

Hard Disk: A:\

Volume Name: NO NAME

Volume Serial Number : 2F5F-13FD

File System: FAT12

Bytes Per Sector: 512

Total Clusters: 2847

Sectors per cluster: 1

Total Sectors: 2880

Hidden Sectors: 0

Total Capacity: 1440 KB

Start Sector: 0

End Sector: 0

**Disks:**

**Evidence of Interest:**

Total Evidence Items of Interest: 13

Hard Disk: A:\

List of Files:

C:\Users\Acer\Documents\kerja\BITS3443 Digital Forensics\W10\C10frag.eve\78-list.xls

MD5 Checksum: 8C2226B745BECF04150580F0F6AC8353

Deleted: 01/18/2003 15:31

MFT &STANDARD\_INFO entry modified: Not available

MFT $FILE\_NAME entry modified: Not available

**Cluster Chain:**

Start Cluster End Cluster Total Clusters

33 (21) 87 (57) 55

Investigator's comments: Recovered hidden .jpg file

C:\Users\Acer\Documents\kerja\BITS3443 Digital Forensics\W10\C10frag.eve\shellback2.005

MD5 Checksum: 1A8705E2079502FE29F542B5301768AD

Deleted: 01/18/2003 15:34

MFT &STANDARD\_INFO entry modified: Not available

MFT $FILE\_NAME entry modified: Not available

**Cluster Chain:**

Start Cluster End Cluster Total Clusters

961 (3C1) 1062 (426) 102

Investigator's comments: Recovered hidden .jpg file

C:\Users\Acer\Documents\kerja\BITS3443 Digital Forensics\W10\C10frag.eve\shellback2.006

MD5 Checksum: 6701E072FB0CF7E79F60DF01567C6785

Deleted: 01/18/2003 15:35

MFT &STANDARD\_INFO entry modified: Not available

MFT $FILE\_NAME entry modified: Not available

**Cluster Chain:**

Start Cluster End Cluster Total Clusters

1067 (42B) 1168 (490) 102

Investigator's comments: Recovered hidden .jpg file

C:\Users\Acer\Documents\kerja\BITS3443 Digital Forensics\W10\C10frag.eve\wshellback4.jpg

MD5 Checksum: 4C17DBF21835D82872CFF5E66670ECFE

Deleted: 01/18/2003 16:20

MFT &STANDARD\_INFO entry modified: Not available

MFT $FILE\_NAME entry modified: Not available

**Cluster Chain:**

Fragmented File

Start Cluster End Cluster Total Clusters

1067 (42B) 1168 (490) 102

1312 (520) 1326 (52E) 15

2484 (9B4) 2495 (9BF) 12

2756 (AC4) 2770 (AD2) 15

Investigator's comments: Recovered hidden .jpg file

No EXIF information is available

C:\Users\Acer\Documents\kerja\BITS3443 Digital Forensics\W10\C10frag.eve\images\0Pict0033.jpg

MD5 Checksum: C233FF5CD4598D264D871E123D376D84

Deleted: 01/18/2003 16:20

MFT &STANDARD\_INFO entry modified: Not available

MFT $FILE\_NAME entry modified: Not available

**Cluster Chain:**

Fragmented File

Start Cluster End Cluster Total Clusters

1328 (530) 1429 (595) 102

2771 (AD3) 2773 (AD5) 3

Investigator's comments: Recovered hidden .jpg file

No EXIF information is available

C:\Users\Acer\Documents\kerja\BITS3443 Digital Forensics\W10\C10frag.eve\images\åHELLB~1.008

MD5 Checksum: 8301AB73C84B0F80486271D9EC4C942C

Deleted: 01/18/2003 15:36

MFT &STANDARD\_INFO entry modified: Not available

MFT $FILE\_NAME entry modified: Not available

**Cluster Chain:**

Start Cluster End Cluster Total Clusters

1328 (530) 1429 (595) 102

Investigator's comments: Recovered hidden .jpg file

C:\Users\Acer\Documents\kerja\BITS3443 Digital Forensics\W10\C10frag.eve\images\zPict0013.xif

MD5 Checksum: 14EA712CFAF99D3D5D6E953A096DF3A9

Created: 01/18/2003 16:02 Modified: 01/18/2003 14:59 Last Accessed: 01/18/2003 00:00

MFT &STANDARD\_INFO entry modified: Not available

MFT $FILE\_NAME entry modified: Not available

**Cluster Chain:**

Fragmented File

Start Cluster End Cluster Total Clusters

474 (1DA) 478 (1DE) 5

691 (2B3) 787 (313) 97

847 (34F) 948 (3B4) 102

961 (3C1) 1062 (426) 102

1947 (79B) 2073 (819) 127

2130 (852) 2231 (8B7) 102

2678 (A76) 2755 (AC3) 78

Investigator's comments: Recovered hidden .jpg file

C:\Users\Acer\Documents\kerja\BITS3443 Digital Forensics\W10\C10frag.eve\images\0Pict0014.jpg

MD5 Checksum: A3E6EAD48448B5925CE3D5186F776535

Deleted: 01/18/2003 15:58

MFT &STANDARD\_INFO entry modified: Not available

MFT $FILE\_NAME entry modified: Not available

**Cluster Chain:**

Start Cluster End Cluster Total Clusters

33 (21) 126 (7E) 94

Investigator's comments: Recovered hidden .jpg file

No EXIF information is available

C:\Users\Acer\Documents\kerja\BITS3443 Digital Forensics\W10\C10frag.eve\images\shellback2.024

MD5 Checksum: 12C0ABDE2F90EC020D6D9BEF4A3D1A89

Deleted: 01/18/2003 15:42

MFT &STANDARD\_INFO entry modified: Not available

MFT $FILE\_NAME entry modified: Not available

**Cluster Chain:**

Start Cluster End Cluster Total Clusters

2678 (A76) 2755 (AC3) 78

Investigator's comments: Recovered hidden .jpg file

C:\Users\Acer\Documents\kerja\BITS3443 Digital Forensics\W10\C10frag.eve\Archive\invoice1.xls

MD5 Checksum: B21F44878AE567A0D0C478D232DBC77E

Deleted: 01/18/2003 15:38

MFT &STANDARD\_INFO entry modified: Not available

MFT $FILE\_NAME entry modified: Not available

**Cluster Chain:**

Start Cluster End Cluster Total Clusters

1925 (785) 1971 (7B3) 47

Investigator's comments: Recovered hidden .jpg file

C:\Users\Acer\Documents\kerja\BITS3443 Digital Forensics\W10\C10frag.eve\Archive\shellback2.008

MD5 Checksum: 57481036C3716ACB725590053DEC71A8

Deleted: 01/18/2003 15:38

MFT &STANDARD\_INFO entry modified: Not available

MFT $FILE\_NAME entry modified: Not available

**Cluster Chain:**

Start Cluster End Cluster Total Clusters

1972 (7B4) 2073 (819) 102

Investigator's comments: Recovered hidden .jpg file

C:\Users\Acer\Documents\kerja\BITS3443 Digital Forensics\W10\C10frag.eve\Archive\shellback2.009

MD5 Checksum: 8EF3C32681549D225C0162C38B614031

Deleted: 01/18/2003 15:39

MFT &STANDARD\_INFO entry modified: Not available

MFT $FILE\_NAME entry modified: Not available

**Cluster Chain:**

Start Cluster End Cluster Total Clusters

2130 (852) 2231 (8B7) 102

Investigator's comments: Recovered hidden .jpg file

C:\Users\Acer\Documents\kerja\BITS3443 Digital Forensics\W10\C10frag.eve\oscar

MD5 Checksum: 3586B0D4C65B09C4B6A5893DA7AB68EF

Deleted: 01/18/2003 15:07

MFT &STANDARD\_INFO entry modified: Not available

MFT $FILE\_NAME entry modified: Not available

**Cluster Chain:**

Fragmented File

Start Cluster End Cluster Total Clusters

476 (1DC) 478 (1DE) 3

691 (2B3) 693 (2B5) 3

Investigator's comments: Recovered hidden .jpg file

C:\Users\Acer\Documents\kerja\BITS3443 Digital Forensics\W10\C10frag.eve, Hard Disk A:\ : Evidence of Interest: 13

# Task 2

**Evidence Report for Project:** C10carve

**Project Number:** C10carve

**Project Description:**

**Image Files:**

**File Name:** C:\Users\Acer\Documents\kerja\BITS3443 Digital Forensics\W10\C10Carve.eve

Image File Type: DFT Image

File Number: C10frag

Technician Name: Joe Friday

Date: 02/06/2007

Time: 21:34:19

Checksum: 59c4af4782fc383b7f18b584594f42ec

Checksum Validated: Yes

Compressed image: No

Time Zone Information:

Time Zone: (GMT-08:00) Pacific Time (US & Canada); Tijuana (Pacific Standard Time)

Daylight savings (summertime) was in effect: Yes

Time Zone information obtained automatically from remote system/image.

Hard Disk: G:\

Volume Name: NO NAME

Volume Serial Number : 2D31-1BED

File System: FAT16

Bytes Per Sector: 512

Total Clusters: 51283

Sectors per cluster: 4

Total Sectors: 205569

Hidden Sectors: 63

Total Capacity: 102784 KB

Start Sector: 0

End Sector: 0

**Disks:**

**Evidence of Interest:**

Total Evidence Items of Interest: 7

Hard Disk: G:\

List of Files:

C:\Users\Acer\Documents\kerja\BITS3443 Digital Forensics\W10\C10Carve.eve\Pictures\Friends\gametour5.txt

MD5 Checksum: 82199FA995265C3FC54B04DD89A153DC

Deleted: 02/04/2007 20:19

MFT &STANDARD\_INFO entry modified: Not available

MFT $FILE\_NAME entry modified: Not available

**Cluster Chain:**

Start Cluster End Cluster Total Clusters

727 (2D7) 1138 (472) 412

Investigator's comments: Similar file located on first USB drive

C:\Users\Acer\Documents\kerja\BITS3443 Digital Forensics\W10\C10Carve.eve\Pictures\Friends\åICT0037.JPG

MD5 Checksum: 68A713955B06D9FF18AB11770B7F3803

Deleted: 02/04/2007 20:19

MFT &STANDARD\_INFO entry modified: Not available

MFT $FILE\_NAME entry modified: Not available

**Cluster Chain:**

Start Cluster End Cluster Total Clusters

727 (2D7) 814 (32E) 88

Investigator's comments: Similar file located on first USB drive

No EXIF information is available

C:\Users\Acer\Documents\kerja\BITS3443 Digital Forensics\W10\C10Carve.eve\Pictures\Friends\gametour1.txt

MD5 Checksum: E61611D933646773D295F291D2E9A196

Created: 02/04/2007 20:19 Modified: 08/05/2001 09:22 Last Accessed: 02/05/2007 00:00

MFT &STANDARD\_INFO entry modified: Not available

MFT $FILE\_NAME entry modified: Not available

**Cluster Chain:**

Fragmented File

Start Cluster End Cluster Total Clusters

19915 (4DCB) 21962 (55CA) 2048

21963 (55CB) 23066 (5A1A) 1104

Investigator's comments: Similar file located on first USB drive

C:\Users\Acer\Documents\kerja\BITS3443 Digital Forensics\W10\C10Carve.eve\Pictures\Friends\gametour2.txt

MD5 Checksum: FD157F6D9B79BE120614B185A6E01518

Created: Modified: Last Accessed:

MFT &STANDARD\_INFO entry modified: Not available

MFT $FILE\_NAME entry modified: Not available

**Cluster Chain:**

Start Cluster End Cluster Total Clusters

Investigator's comments: Additional similar files in USB drive

C:\Users\Acer\Documents\kerja\BITS3443 Digital Forensics\W10\C10Carve.eve\Pictures\Friends\gametour3.txt

MD5 Checksum: 55A9B71E30F2FF6549CF73EFC94257DA

Created: Modified: Last Accessed:

MFT &STANDARD\_INFO entry modified: Not available

MFT $FILE\_NAME entry modified: Not available

**Cluster Chain:**

Start Cluster End Cluster Total Clusters

Investigator's comments: Additional similar files on USB drive

C:\Users\Acer\Documents\kerja\BITS3443 Digital Forensics\W10\C10Carve.eve\Pictures\Friends\gametour4.txt

MD5 Checksum: B28199BF44E3DD164F98752868529566

Created: Modified: Last Accessed:

MFT &STANDARD\_INFO entry modified: Not available

MFT $FILE\_NAME entry modified: Not available

**Cluster Chain:**

Start Cluster End Cluster Total Clusters

Investigator's comments: Additional similar files on USB drive

C:\Users\Acer\Documents\kerja\BITS3443 Digital Forensics\W10\C10Carve.eve\Pictures\Friends\gametour6.txt

MD5 Checksum: D16BFF738B47D57C77E01C9E9F6BFBDB

Created: Modified: Last Accessed:

MFT &STANDARD\_INFO entry modified: Not available

MFT $FILE\_NAME entry modified: Not available

**Cluster Chain:**

Start Cluster End Cluster Total Clusters

Investigator's comments: Additional similar files on USB drive

C:\Users\Acer\Documents\kerja\BITS3443 Digital Forensics\W10\C10Carve.eve, Hard Disk G:\ : Evidence of Interest: 7

**Clusters of Interest:**

**File Signature Mismatch:**

**Search Results:**

-----------------------------------------------------------------

Image File Name: C:\Users\Acer\Documents\kerja\BITS3443 Digital Forensics\W10\C10Carve.eve

-----------------------------------------------------------------

Keyword: zzzz

Hits: 6

-----------------------------------------------------------------

List of data files in which search patterns found:

Pictures\Vacations\TEMP\PublicDomain\SPEC.PDF

Pictures\House\åSCF0327.JPG

Pictures\Friends\gametour5.txt

Pictures\Friends\SPEC.PDF

Pictures\Friends\åICT0037.JPG

Recycled\Df73.JPG

List of words found:

fgzzzz

zzzz

-----------------------------------------------------------------

# Task 3

|  |  |  |  |
| --- | --- | --- | --- |
|  | Spider.bmp | Spider.jpg | Spider2.bmp |
| **Size** | 1.03mb | 48.5kb | 1.03mb |
| **Header** | 42 4D | FF D8 | 42 4D |
| **Trailer** | 83 00 | FF D9 | 84 00 |
| **Compression** |  | JPEG, quality: 80, subsampling ON (2x2) |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | Flower.gif | Flower.jpg | Flower2.gif |
| **Size** | 318kb | 98.8kb | 324kb |
| **Header** | 47 49 | FF D8 | 47 49 |
| **Trailer** | 00 3B | FF D9 | 00 3B |
| **Compression** | LZW | JPEG, quality: 80, subsampling ON (2x2) | LZW |

|  |  |  |  |
| --- | --- | --- | --- |
|  | Cartoon.bmp | Cartoon.gif | Cartoon2.bmp |
| **Size** | 18.2kb | 10.4kb | 18.2kb |
| **Header** | 42 4D | 47 49 | 42 4D |
| **Trailer** | 00 00 | 00 3B | FD FD |
| **Compression** |  | LZW |  |

Based on the comparison, converting BMP to JPG to BMP doesn’t affect the file size. Converting GIF to JPG to GIF increases the size and converting BMP to GIF to BMP affects a small file size because of lossless compression.

# Task 5

Comparing Mission.bmp and Mission-steg.bmp...

Compare error at OFFSET EE

file1 = 75

file2 = 74

Compare error at OFFSET 19B

file1 = 1E

file2 = 1F

Compare error at OFFSET 27F

file1 = 34

file2 = 35

Compare error at OFFSET 2AD

file1 = 4E

file2 = 4F

Compare error at OFFSET 3B6

file1 = 89

file2 = 88

Compare error at OFFSET 41A

file1 = 55

file2 = 54

Compare error at OFFSET 479

file1 = 9A

file2 = 9B

Compare error at OFFSET 4BF

file1 = 95

file2 = 94

Compare error at OFFSET 5D2

file1 = 5D

file2 = 5C

Compare error at OFFSET 6D1

file1 = 1B

file2 = 1A

10 mismatches - ending compare

n

There are 10 mismatches between Mission.bmp and Mission-steg.bmp, a few differences in bit by one. Mission-steg.bmp also contains a lot more hexadecimal values compared to Mission.bmp.