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: 02/05/2007 00:00

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 00:00

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

Deleted: Deleted: 02/05/2007 00:00

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

Deleted: Deleted: 02/05/2007 00:00

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

Deleted: Deleted: 02/05/2007 00:00

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

Deleted: Deleted: 02/05/2007 00:00

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

Project Notes:

This Report was created by ProDiscover