

Lampiran

Lampiran Data curving pada kartu media



Lampiran history chat BBM yang terhapus





Lampiran Case Information pada kartu media

CASE INFORMATION

Jan 29, 2013

FTK Version Version 1.50 DEMO, build 04.09.08

Case Number 03

Case Location C:\Users\Hanung\Desktop\shortcut\Hanung Raditya Kusuma\skripsi hanung\Tahapan-tahapan FTK imager\03-bb-email-forensic\

Case Description

Report Created Jan 29, 2013 10:41pm

Forensic Examiner Hanung

Agency esa unggul

Address Purati

Phone 08568283794

Fax 3324232

Email dzhadul@gmail.com

Comments Forensic

Investigator Hanung Raditya Kusuma

Agency www

Address

Phone

Fax

Email

Comments

Access Data Forensic Toolkit

Lampiran File Overview pada kartu media

Tabel FILE OVERVIEW

Jan 29,2013

Kategori File	List File	Amount
Evidence items	Evidence items	1
File items	Total File Items	340
	Flagged Thumbnails	0
	Other thumbnails	7
File Status	KFF alert files	0
	Bookmark items	0
	Bad Extensions	1
	Encrypted Files	0
	From E-mail	0
	Deleted Files	34
	From Recyclebin	0
	Duplicate items	2

	OLE subitems	0
	Flagged ignore	0
	KFF ignorable	0
File Category	Documents	0
	Spreadsheets	0
	Database	0
	Graphic	7
	E-mail messages	0
	Executables	0
	Archives	0
	Folders	32
	Slack/free space	146
	Other Known type	0
	Unknown type	155

Lampiran Evicence List

EVIDENCE LIST

Jan 29,2013

Display Name: case03-email-bb\BLACKBERRY-FAT16
Evidence File Name: case03-email-bb.E01
Evidence Path: C:\Users\Hanung\Desktop\shortcut\Hanung Raditya
 Kusuma\skripsi hanung\Tahapan-tahapan FTK imager
Identification Name/Number: 033
Evidence Type: FAT16
Added: 1/28/2013 5:11:07 PM
Children: 340
Descendants: 340
Investigator's Name: Hanung Raditya Kusuma
Comment:

Lampiran CaseLog pada kartu media

CASELOG.TXT

1/28/2013 5:11:07 PM -- FTK Version 1.50 DEMO
build 04.09.08

Examiner's Machine:

Phys Mem: Total: 2,147,483,647
Available: 1,389,031,424 Used: 758,452,223
Virt Mem: Total: 2,147,352,576
Available: 1,837,674,496 Used: 309,678,080
Page File Available: 3,763,265,536

1/28/2013 5:11:07 PM -- AccessData PRTK5 EFS
integration unavailable: AccessData PRTK 5 is
not installed

1/28/2013 5:11:07 PM -- New case started by
investigator Hanung Raditya Kusuma using FTK
version 1.50 DEMO build 04.09.08

Case Name: 03-bb-email-forensic

Case Number: 03

Case Folder:

C:\Users\Hanung\Desktop\shortcut\Hanung Raditya
Kusuma\skripsi hanung\Tahapan-tahapan FTK
imager\03-bb-email-forensic

Description:

Case Log Options (NOT Case Agent Logging
Options):

Log case and evidence events: Yes

Log error messages: Yes

Log bookmarking events: Yes

Log searching events: Yes

Log special searching events: Yes

Log other events: Yes

Log extended information: Yes

Processes to be performed:

File Extraction: Yes

File Identification: Yes

MD5 Hash: Yes
 SHA1 Hash: No
 KFF (Known File Filter): Yes
 Entropy Test: Yes
 Full Text Index: Yes
 Prerender Thumbnails: Yes
 File Listing Database: Yes
 HTML File Listing: Yes
 Decrypt EPS Files: Unavailable
 Default Case Refinement Settings:

Add files only if they satisfy BOTH the
 file status and the file type criteria as
 follows:

File Status Criteria:
 Deletion status: any
 Encryption status: any
 From email status: any
 Duplicate status: any
 OLE stream status: any

File Type Criteria:
 documents: yes
 spreadsheets: yes
 databases: yes
 . graphics: yes
 email messages: yes
 executables: yes
 archives: yes
 folders: yes
 other recognized: yes
 unknown: yes

Default Index Refinement Settings:

Don't index KFF ignorable files

Index files only if they satisfy BOTH
 the file status and the file type criteria as
 follows:

File Status Criteria:
 Deletion status: any
 Encryption status: any
 From email status: any
 Duplicate status: any

```

1/28/2013 5:11:07 PM -- Adding to database...
1/28/2013 5:11:07 PM -- Filtering...
1/28/2013 5:11:07 PM -- Indexing 302
characters... (Index size: 20 KB)
1/28/2013 5:11:07 PM -- File name: case03-email-
bb\BLACKBERRY-FAT16\BlackBerry
Type: Folder
1/28/2013 5:11:07 PM -- Adding to database...
1/28/2013 5:11:07 PM -- Filtering...
1/28/2013 5:11:07 PM -- Indexing 216
characters... (Index size: 20 KB)
1/28/2013 5:11:08 PM -- File name: case03-email-
bb\BLACKBERRY-FAT16\BlackBerry\music
Type: Folder
1/28/2013 5:11:08 PM -- Adding to database...
1/28/2013 5:11:08 PM -- Filtering...
1/28/2013 5:11:08 PM -- Indexing 23
characters... (Index size: 21 KB)
1/28/2013 5:11:08 PM -- File name: case03-email-
bb\BLACKBERRY-FAT16\BlackBerry\music\Media Sync
Type: Folder
1/28/2013 5:11:08 PM -- Adding to database...
1/28/2013 5:11:08 PM -- Filtering...
1/28/2013 5:11:08 PM -- Indexing info only...
(Index size: 21 KB)
1/28/2013 5:11:08 PM -- Indexing 33
characters... (Index size: 25 KB)
1/28/2013 5:11:08 PM -- File name: case03-email-
bb\BLACKBERRY-FAT16\tmp\bbm_1351889976139.tmp
Type: Unknown File Type
1/28/2013 5:11:08 PM -- Adding to database...
1/28/2013 5:11:08 PM -- File name: case03-email-
bb\BLACKBERRY-
FAT16\tmp\bbm_1354168250509.tmp.rem
1/28/2013 5:11:08 PM -- Identifying...
1/28/2013 5:11:08 PM -- Hashing and Entropy
Test...
1/28/2013 5:11:08 PM -- MD5:
685A876945D8696A9EA8B366D526703B
Type: Unknown File Type

```

```
1/28/2013 5:11:08 PM -- Adding to database...
1/28/2013 5:11:08 PM -- Indexing info only...
(Index size: 26 KB)
1/28/2013 5:11:08 PM -- File name: case03-email-
bb\BLACKBERRY-
FAT16\tmp\bbm_1354248497903.tmp.rem
1/28/2013 5:11:08 PM -- Identifying...
1/28/2013 5:11:08 PM -- Hashing and Entropy
Test...
1/28/2013 5:11:08 PM -- MD5:
B610C87BE0318C36FA5CC909C90FF0B4
Type: Unknown File Type
1/28/2013 5:11:08 PM -- Adding to database...
1/28/2013 5:11:08 PM -- Indexing info only...
(Index size: 26 KB)
1/28/2013 5:11:08 PM -- File name: case03-email-
bb\BLACKBERRY-FAT16\tmp\bbm_1351338632340.tmp
Type: Unknown File Type
1/28/2013 5:11:08 PM -- Adding to database...
1/28/2013 5:11:08 PM -- File name: case03-email-
bb\BLACKBERRY-FAT16\tmp\bbm_1351338639736.tmp
Type: Unknown File Type
1/28/2013 5:11:08 PM -- Adding to database...
1/28/2013 5:11:08 PM -- File name: case03-email-
bb\BLACKBERRY-FAT16\tmp\bbm_1351338645959.tmp
1/28/2013 5:11:29 PM -- Indexing info only...
(Index size: 69 KB)
1/28/2013 5:11:29 PM -- File name: case03-email-
bb\BLACKBERRY-FAT16\DriveFreeSpace29
C:\Users\Hanung\Desktop\shortcut\Hanung Raditya
Kusuma\skripsi hanung\Tahapan-tahapan FTK
imager\03-bb-email-forensic\ using FTK version
1.50 DEMO build 04.09.08
```


