Reverse Engineering Format File Database BKD Polban 2018

Tjan Swi Hong

Jurusan Teknik Elektro, Politeknik Negeri Bandung, Bandung 40012
E-mail : tjansh@polban.ac.id

ABSTRAK

BKD adalah kewajiban dosen melaksanakan pendidikan, penelitian, dan pengabdian. Dosen Polban membuat laporan BKD menggunakan aplikasi PROGRAM_BKD_14_NOV_2017.exe dan data DATA_BKD_14_NOV_2017.ext dengan memasukkan data secara manual. Pekerjaan ini menyita waktu, padahal data yang diperlukan sudah tersedia. Proses manual berkurang jika dibuat aplikasi yang mengolah data menjadi file BKD. Masalahnya file data BKD tidak dapat dibuka oleh aplikasi lain dan struktur database tidak diketahui. Format file harus dicari supaya datanya dapat dibaca dan ditulis. Metode yang digunakan untuk mendapatkan format file database BKD yaitu *reverse engineering* dengan tahapan: Analisa format file, analisa *field* database, merangkum hasil Analisa. Analisa format file menggunakan pendekatan file ekstensi dan *file signature*. File ditampilkan dalam bentuk hexadesimal dan ASCII menggunakan xxd. Analisa *field* database membandingkan data yang dimasukkan di aplikasi secara manual dengan isi database dan isi file yang ditampilkan menggunakan SQLiteStudio dan xxd. Format file didapat dengan merangkum hasil analisa. File database BKD adalah file database SQLite 3 dengan nama file internal ds.dat kemudian dikompres dengan format zip berekstensi ext. Database terdiri dari tabel cek dan xy. Tabel cek menyimpan data asesor. Tabel xy menyimpan data informasi PT, informasi dosen, asesor, serta kinerja pengajaran, penelitian, pengabdian dan pendukung dengan pembeda tipe *record* di *field* a.

Kata Kunci
Reverse Engineering, Format File

1. PENDAHULUAN

BKD (Beban Kerja Dosen) adalah salah satu kewajiban dosen untuk melaksanakan Pendidikan, penelitian, dan pengabdian kepada masyarakat yang harus dilaporkan secara rutin. Pelaporan BKD di Polban menggunakan aplikasi PROGRAM_BKD_14_NOV_2017.exe dan file data DATA_BKD_14_NOV_2017.ext. Dengan aplikasi ini dosen memasukkan data diri, memasukkan satu satu data pengajaran, penelitian, dan pengabdian, serta mengunggah lampiran lampiran SK dan bukti kerja. Pekerjaan ini menyita waktu, padahal data yang diperlukan seperti pengajaran sudah tersedia di jurusan. Jika ada aplikasi yang dapat mengolah data pengajaran, penelitian dan pengabdian menjadi file BKD, akan mengurangi banyak proses manual data entri. Masalahnya yaitu file data BKD tidak dapat dibuka oleh aplikasi lain dan struktur database tidak diketahui. Format file harus dicari supaya datanya dapat dibaca dan ditulis.

Riset yang berhubungan termasuk pendekatan untuk menganalisis file biner, file log, spesifik database, dan database SQLite. Pehnack menjelaskan cara *reverse engineering* untuk menganalisis file biner [1]. Schuster menemukan format file event log Microsoft Vista dengan membandingkan file log dalam bentuk biner dan text [2]. Zelenyuk menjelaskan Langkah Langkah *reverse engineering* file database [3], sedangkan Tjan menjelaskan *reverse engineering* file database SCADA dengan membandingkan data sebenarnya dengan data mentah file [4]. Nemetz, Schmitt dan Freiling membuat standar forensik analisis untuk menganalisis file SQLite [5].

2. METODA

Tahapan *reverse engineering* yang dilakukan untuk mendapatkan format file database BKD: Analisa format file menggunakan file ekstensi dan *file signature* sehingga file dapat dibaca dan ditulis, analisa *field* database dengan cara membandingkan isi database dengan tampilan dari program BKD sehingga didapat peta penyimpanan data di masing masing *field*, merangkum hasil Analisa menjadi format file database BKD.

3. HASIL DAN ANALISA

Analisa format file menggunakan pendekatan file ekstensi dan *file signature*. File ditampilkan dalam bentuk hexadesimal dan ASCII menggunakan xxd. Analisa *field* database membandingkan data yang dimasukkan di aplikasi secara manual dengan isi database dan isi file yang ditampilkan menggunakan SQLiteStudio dan xxd. Format file didapat dengan merangkum hasil analisa.

3.1. Analisa Format File

Analisa format file dilakukan dengan tahapan:

- Tentukan tipe file menggunakan file ekstensi
- Jika tidak berhasil, tentukan tipe file menggunakan *file signature* atau *magic number*.

- Jika berhasil, tes membuka file menggunakan perangkat lunak standar
- Jika tidak berhasil, lakukan analisa lebih detail

File ekstensi biasanya dapat digunakan untuk menentukan format file. Data BKD menggunakan ekstensi ext, akan tetapi tidak ditemukan standar yang berhubungan dengan database untuk tipe file ini [6].

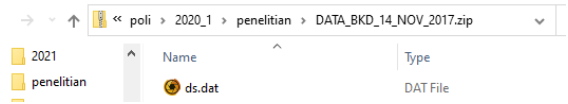
Tahap berikutnya mencari tipe file menggunakan *file signature* atau *magic number*. File dibuka menggunakan perangkat lunak xxd sehingga dapat ditampilkan dalam bentuk hexadesimal dan ASCII lihat

Gambar *1*. Data hexadesimal 50 4B 03 04 cocok dengan *file signature* file zip atau turunannya [7].

File diganti nama menjadi ekstensi zip, dan dibuka menggunakan Windows Explorer. File berhasil dibuka dan di dalamnya terdapat file ds.dat. Lihat Gambar 2.

```
C:> xxd -g1 -l16 -u -c8 DATA_BKD_14_NOV_2017.ext
0000000: 50 4B 03 04 14 00 02 00  PK......
0000008: 08 00 81 66 6E 4B D9 5D  ...fnK.]
```

Gambar 1. *xxd data file BKD ASCII*



Gambar 2. *Unzip file data BKD*

File berekstensi dat digunakan untuk macam macam tipe file termasuk video, registry, database dan dokumen [8].

```
C:> xxd -g1 -l16 -u -c8 ds.dat
0000000: 53 51 4C 69 74 65 20 66  SQLite f
0000008: 6F 72 6D 61 74 20 33 00  ormat 3.
```

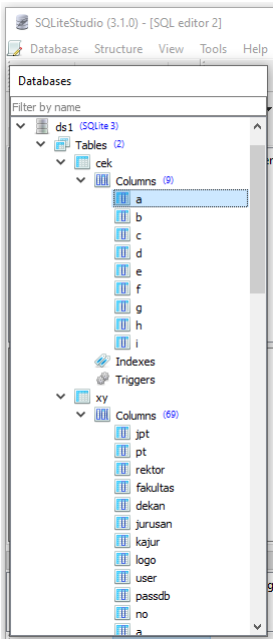
Gambar 3. *xxd file ds.dat ASCII*

Karena tidak dapat ditentukan dari file ekstensinya, tahap berikutnya mencari tipe file menggunakan *file signature* atau *magic number*. File dibuka menggunakan perangkat lunak xxd sehingga dapat ditampilkan dalam bentuk hexadesimal dan ASCII lihat Gambar 3. Data hexadesimal 53 51 4C 69 74 65 20 66 6F 72 6D 61 74 20 33 00 cocok dengan *file signature* file SQLite database yang biasanya berekstensi db, sqlite, atau sqlitedb [7].

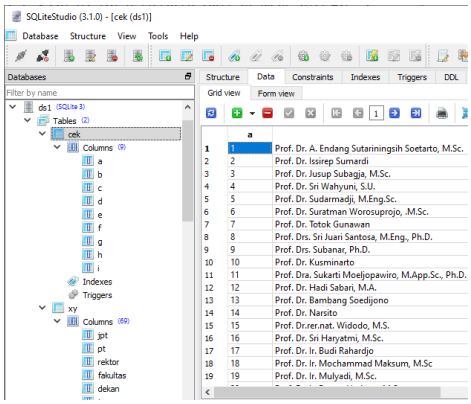
File diganti nama dengan ekstensi sqlite dan dibuka dengan SQLiteStudio. File berhasil dibuka, terdapat dua tabel yaitu cek dan xy. Lihat Gambar 4.

Tabel cek berisi data asesor, sedangkan tabel xy kosong. Lihat Gambar 5 dan Gambar 6.

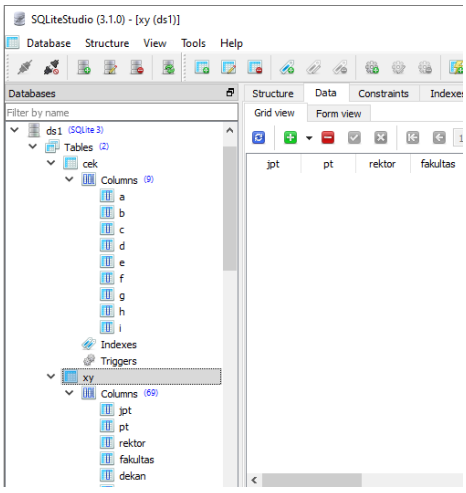
Jadi format file data BKD adalah file database SQLite 3 dengan ekstensi dat yang di kompres menggunakan format zip dengan ekstensi ext.



Gambar 4. *ds.sqlite di SQLiteStudio*



Gambar 5. Isi tabel cek



Gambar 6 Isi tabel xy

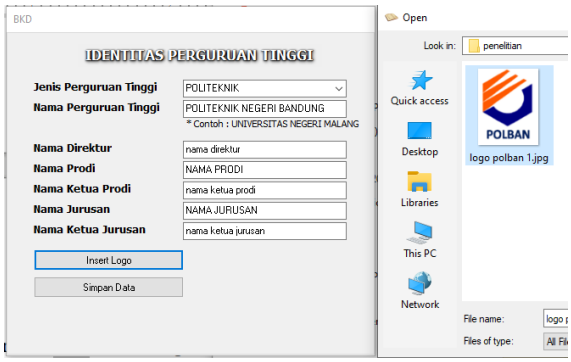
3.2. Analisa Field Database

Field database ditentukan dengan mengisi data di aplikasi BKD kemudian disimpan, membandingkan isi data aplikasi dengan data *record* di database.
Lihat Gambar 7 dan Gambar 8, data BKD di aplikasi terdiri dari:

- Identitas perguruan tinggi
- Identitas dosen
- Kinerja bidang pendidikan
- Kinerja bidang penelitian
- Kinerja bidang pengabdian masyarakat
- Kinerja penunjang lainnya
- Kewajiban khusus

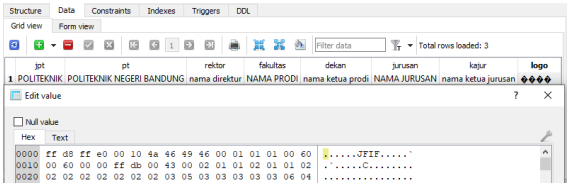
Field diisi dengan data yang mudah untuk diidentifikasi. Contoh data untuk identitas perguruan tinggi lihat Gambar 8. Data terdiri dari pilihan misalnya jenis perguruan tinggi, isian misalnya nama prodi, dan gambar misalnya "insert logo".

Gambar 7. Menu utama aplikasi BKD



Gambar 8. Sampel pengisian data identitas PT

Hasil data yang disimpan di database dapat dilihat pada Gambar 9. Tabel xy, *field* jpt berisi Jenis PT, pt berisi nama PT, rektor berisi nama Direktur, fakultas berisi nama Prodi, dekan berisi nama ketua prodi, jurusan berisi nama Jurusan dan kajur berisi nama Ketua Jurusan. Isi file logo disimpan sebagai data biner di *field* logo. Gambar 9 isi *field* logo dalam hexadisimal dan Gambar 10 isi file logo menggunakan xxd berisi data yang sama.

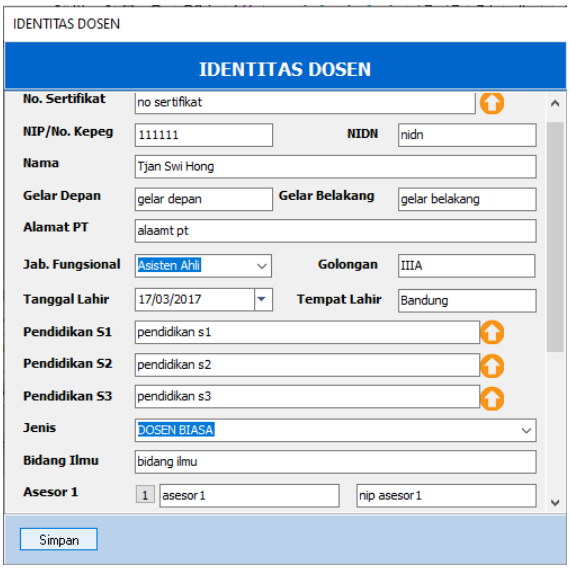


Gambar 9. Isi database identitas perguruan tinggi

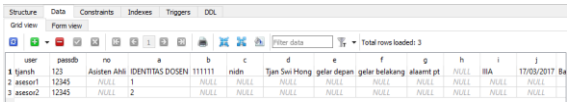
```
C:> xxd -g1 -l32 -u -c8 "logo polban 1.jpg"
0000000: FF D8 FF E0 00 10 4A 46  ......JF
0000008: 49 46 00 01 01 01 00 60  IF.....`
0000010: 00 60 00 00 FF DB 00 43  .`.....C
0000018: 00 02 01 01 02 01 01 02  ........
```

Gambar 10. *xxd file logopolban 1.jpg*

Identitas dosen diisi dengan sampel data seperti Gambar 11. Hasil data disimpan di database seperti Gambar 12. Ada tiga *record* pada tabel xy. *Record* pertama berisi identitas dosen, sedangkan dua *record* lagi informasi asesor 1 dan asesor 2. *Field* user dan passdb berisi username dan password. *Field* a menunjukkan tipe *record*, "IDENTITAS DOSEN" untuk identitas dosen, "1" untuk asesor 1 dan "2" untuk asesor 2. Data NIP, NIDN, nama, gelar depan, gelar belakang, alamat PT masing-masing disimpan di *field* b, c, d, e, f dan g.

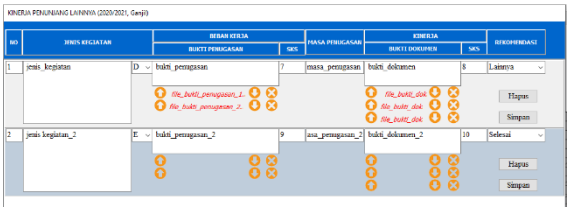


Gambar 11. Sampel pengisian identitas dosen

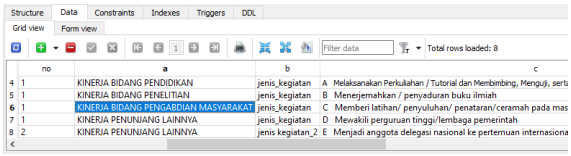


Gambar 12. Isi database tabel xy identitas dosen

Data isian kinerja bidang pendidikan, bidang penelitian, bidang pengabdian dan penunjang hampir sama. Gambar 13 adalah sampel isian untuk kinerja di aplikasi BKD. Gambar 14 isi database tabel xy dengan sampel data kinerja bidang pendidikan, bidang penelitian, bidang pengabdian dan penunjang.

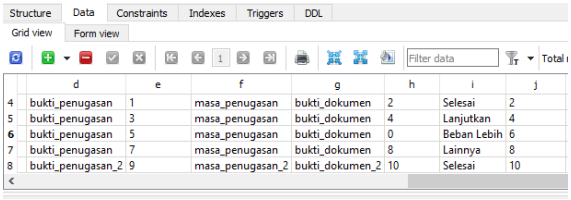


Gambar 13. Sample pengisian kinerja



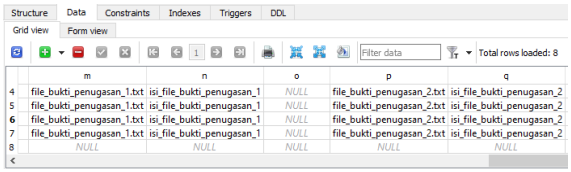
Gambar 14. Isi database tabel xy kinerja

Field no berisi nomor kegiatan pada data entri kinerja. *Field* a, menunjukkan tipe *record* untuk masing masing kinerja. *Field* b dan c menunjukkan jenis kegiatan.



Gambar 15. Isi database tabel xy kinerja d-j

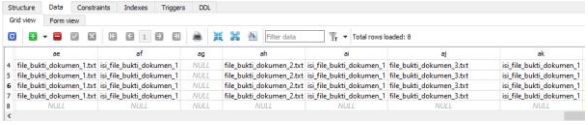
Field d sampai dengan j Gambar 15 berisi data beban kerja, kinerja dan rekomendasi. *Field* d, e, f berisi data beban kerja berupa bukti penugasan, sks dan masa penugasan. *Field* g, h, i, j berisi kinerja berupa bukti dokumen, sks kinerja terhitung, rekomendasi, dan sks kinerja. Catatan dari data di atas, jika rekomendasi "Beban Lebih", maka *field* h (sks kinerja terhitung) akan berisi 0.



Gambar 16. Isi database tabel xy kinerja m-q

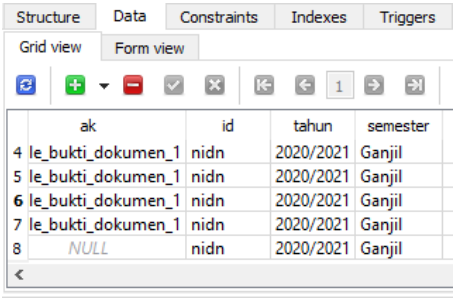
Field m, n, p dan q Gambar 16 berisi data unggah bukti penugasan. *Field* m dan p berisi nama file sedangkan *field* n dan q adalah isi file bukti penugasan.

Field ae sampai dengan ak Gambar 17 berisi data unggah bukti dokumen kinerja. *Field* ae, ah, dan aj berisi nama file sedangkan *field* af, ai dan ak adalah isi file bukti dokumen kinerja.



Gambar 17. Isi database tabel xy kinerja ae-ak

Semua data tadi dibedakan dengan data NIDN dosen serta tahun dan semester pelaporan kinerja. Lihat Gambar 18.



	ak	id	tahun	semester
4	le_bukti_dokumen_1	nidn	2020/2021	Ganjil
5	le_bukti_dokumen_1	nidn	2020/2021	Ganjil
6	le_bukti_dokumen_1	nidn	2020/2021	Ganjil
7	le_bukti_dokumen_1	nidn	2020/2021	Ganjil
8	NULL	nidn	2020/2021	Ganjil

Gambar 18. Isi database tabel xy kinerja id tahun semester

3.3. Rangkuman Hasil Perbandingan

SQLite berisi tabel cek dan xy. Tabel cek berisi data asesor sedangkan semua data yang dimasukkan manual disimpan di tabel xy.

Tabel xy berisi berbagai informasi dengan pembeda *field* a (tipe *record*), *field* id (NIDN dosen) serta *field* tahun, semester (tahun dan semester pelaporan). Detail tipe *record* lihat Tabel 1.

Tabel 1. *Field a tipe record*

No	*Field* a (tipe *record*)	Data yang disimpan
1	IDENTITAS DOSEN	identitas PT dan identitas dosen
2	1	asesor1
3	2	asesor2
4	KINERJA BIDANG PENDIDIKAN	kinerja bidang pendidikan
5	KINERJA BIDANG PENELITIAN	kinerja bidang penelitian
6	KINERJA BIDANG PENGABDIAN MASYARAKAT	kinerja bidang pengabdian
7	KINERJA PENUNJANG LAINNYA	kinerja penunjang

Detail *field* untuk penyimpanan kinerja dapat dilihat Tabel 2 .

Tabel 2. *Field penyimpanan kinerja*

No	*Field*	Data yang disimpan
1	b dan c	Jenis kegiatan
2	d, e dan f	Beban kerja
3	g, h, i dan j	Kinerja
4	m, n, p dan q	File Unggah bukti penugasan
5	ae, af, ah, ai, aj, dan ak	File Unggah bukti kinerja

4. KESIMPULAN

File database BKD Polban 2018 adalah file database SQLite 3 dengan nama file internal ds.dat kemudian dikompres dengan format zip dengan ekstensi ext.

File database terdiri dari dua tabel yaitu cek dan xy. Tabel cek menyimpan data asesor sedangkan data yang di entri oleh dosen disimpan di tabel xy.

Tabel xy menyimpan data informasi PT, informasi dosen, asesor, serta kinerja pengajaran, penelitian, pengabdian dan pendukung. Ciri *record* disimpan di *field* a. Satu kelompok data dibedakan dengan *field* id (NIDN) dan tahun/semester (tahun dan semester pelaporan). *Field* yang digunakan untuk menyimpan data kinerja yaitu: Jenis kegiatan b dan c; Beban kerja d, e dan f; Kinerja g, h, i dan j; File unggah bukti penugasan m, n, p dan q; dan File unggah bukti kinerja ae, af, ah, ai, aj, dan ak.

Format file database BKD sudah ditemukan, sehingga aplikasi yang mengolah data menjadi file BKD dapat dibuat.

UCAPAN TERIMA KASIH

Terima kasih kami ucapkan kepada Jurusan Teknik Elektro Politeknik Negeri Bandung yang telah mendukung penyelesaian penelitian ini.

DAFTAR PUSTAKA

[1] A. Pehnack, "How to Approach Binary File Format Analysis Essential knowledge for reverse engineering," Chicago, 2015.

[2] A. Schuster, "Introducing the Microsoft Vista event log file format," *Digital Investigation*, Vols. 4, Suppement, p. S65 – S72, 2007.

[3] S. Zelenyuk, "Database Reverse Engineering, Part 2: Main Approaches," 6 January 2018. [Online]. Available: https://medium.com/@MorteNoir/database-reverse-engineering-part-2-main-approaches-ae9355b2d429.

[4] S. H. Tjan, "Reverse Engineering Megadata MD3000 Database File Format," in *International Seminar of Science and Applied Technology (ISSAT 2020)*, Bandung, 2020.

[5] S. Nemetz, S. Schmitt and F. Freiling, "A standardized corpus for SQLite database forensics," *Digital Investigation*, Vols. 24, Supplement, pp. S121-S130, 2018.

[6] "EXT file extension - Norton Commander extension," [Online]. Available: https://www.file-extensions.org/ext-file-extension. [Accessed 27 07 2021].

[7] "File Signatures," [Online]. Available: https://www.filesignatures.net/. [Accessed 27 07 2021].

[8] "Search File-Extensions.org Search string: "dat"," [Online]. Available: https://www.file-extensions.org/search/?searchstring=dat&searchtype=2. [Accessed 27 07 2021].