

CERIAS

The Center for Education and Research in Information Assurance and Security

Decoding the Hexadecimal Representation of a PostgreSQL Database Table

Joseph Balazs, Dr. Marcus Rogers, Dr. John Springer, Dr. Dawn Laux

Abstract

Database forensics is an inadequately researched subfield of Digital Forensics. Existing documentation and literature contains a gap for the meaning of the hexadecimal representation of records within a table for the PostgreSQL database management system. In order to determine the indications between active and inactive records, the meanings had to be resolved. Simple testing was done on a table to insert, update, and delete records. A hex interpreter was used to analyze the differences between the records at the file system layer.

Hexadecimal Meanings

Live Records

9D 02 00 00 00 00 00 00

Beginning of record

01 00 03 00 02 09 18 00

First field variable to record number, rest indicates active record

Updated Records – Modified

9E 02 00 00 00 00 00 00

Beginning of record

07 00 03 80 02 29 18 00

First field variable to record number, rest indicates active modified record

Updated Records – Expired

9D 02 00 00 9E 02 00 00

Beginning of record

07 00 03 40 02 05 18 00

First field variable to record number, rest indicates expired original record

Deleted Records

9D 02 00 00 9F 02 00 00

Beginning of record

05 00 03 00 02 05 18 00

First field variable to record number, rest indicates deleted record

File Name	Size	Type	Modification Date
1255_vm	8	Regular File	2/1/2018 6:30:5...
1259	48	Regular File	2/1/2018 6:36:0...
1259_fsm	24	Regular File	2/1/2018 6:30:5...
1259_vm	8	Regular File	2/1/2018 6:36:0...
1417	0	Regular File	2/1/2018 6:30:5...
1418	0	Regular File	2/1/2018 6:30:5...
16395	8	Regular File	2/1/2018 8:51:2...
16397	8	Regular File	2/9/2018 9:17:1...
16401	16	Regular File	2/1/2018 8:51:2...
174	8	Regular File	2/1/2018 6:30:5...
175	8	Regular File	2/1/2018 6:31:0...

```

lec0 02 00 00 00 13 54 65 72-72 61 6E 63 65 03 00 00 .....Terrance...
led0 9E 02 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
lee0 06 00 03 80 02 29 18 00-01 00 00 00 0F 53 74 65 .....).....Ste
lef0 76 65 6E 13 41 62 6F 6F-74 6D 61 6E 00 00 00 00 ven·Abootman...
lf00 9D 02 00 00 00 00 00 00-04 00 00 00 00 00 00 .....
lf10 05 00 03 00 02 09 18 00-05 00 00 00 0D 53 63 6F .....Sco
lf20 74 74 11 44 69 63 6B 6D-61 6E 00 00 00 00 00 00 tt·Dickman...
lf30 9D 02 00 00 00 00 00 00 00-03 00 00 00 00 00 00 .....
lf40 04 00 03 00 02 09 18 00-04 00 00 00 0B 52 69 63 .....Ric
lf50 6B 31 54 68 65 50 72 6F-75 64 43 61 6E 61 64 69 klTheProudCanadi
lf60 61 6E 4D 6F 75 6E 74 69-65 00 00 00 00 00 00 00 anMountie...
lf70 9D 02 00 00 00 00 00 00 00-02 00 00 00 00 00 00 .....
lf80 03 00 03 00 02 09 18 00-03 00 00 00 11 50 68 69 .....Phi
lf90 6C 6C 69 70 03 00 00 00-9D 02 00 00 9E 02 00 00 llip...
lfa0 01 00 00 00 00 00 00 00 00-07 00 03 40 02 05 18 00 .....@...
lfb0 02 00 00 00 13 54 65 72-72 61 6E 63 65 19 61 6E .....Terrance·an
lfc0 64 20 50 68 69 6C 6C 69-70 00 00 00 00 00 00 00 d Phillip...
lfd0 9D 02 00 00 9E 02 00 00-00 00 00 00 00 00 00 .....
lfe0 06 00 03 40 02 05 18 00-01 00 00 00 11 53 74 65 ...·@.....Ste
lff0 70 68 65 6E 13 41 62 6F-6F 74 6D 61 6E 00 00 00 phen·Abootman...

```

Screenshot of Update Transaction

File Name	Size	Type	Modification Date
16397	8	Regular File	2/9/2018 9:37:3...
16401	16	Regular File	2/1/2018 8:51:2...
174	8	Regular File	2/1/2018 6:30:5...
175	8	Regular File	2/1/2018 6:31:0...
2328	0	Regular File	2/1/2018 6:30:5...
2600	8	Regular File	2/1/2018 6:30:5...
2600_fsm	24	Regular File	2/1/2018 6:30:5...
2600_vm	8	Regular File	2/1/2018 6:30:5...
2601	8	Regular File	2/1/2018 6:30:5...
2601_fsm	24	Regular File	2/1/2018 6:30:5...
2601_vm	8	Regular File	2/1/2018 6:30:5...
2602	24	Regular File	2/1/2018 6:30:5...
2602_fsm	24	Regular File	2/1/2018 6:30:5...

```

lec0 02 00 00 00 13 54 65 72-72 61 6E 63 65 03 00 00 .....Terrance...
led0 9E 02 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
lee0 06 00 03 80 02 29 18 00-01 00 00 00 0F 53 74 65 .....).....Ste
lef0 76 65 6E 13 41 62 6F 6F-74 6D 61 6E 00 00 00 00 ven·Abootman...
lf00 9D 02 00 00 9F 02 00 00-00 00 00 00 00 00 00 .....
lf10 05 00 03 00 02 05 18 00-05 00 00 00 0D 53 63 6F .....Sco
lf20 74 74 11 44 69 63 6B 6D-61 6E 00 00 00 00 00 00 tt·Dickman...
lf30 9D 02 00 00 00 00 00 00 00-03 00 00 00 00 00 00 .....
lf40 04 00 03 00 02 09 18 00-04 00 00 00 0B 52 69 63 .....Ric
lf50 6B 31 54 68 65 50 72 6F-75 64 43 61 6E 61 64 69 klTheProudCanadi
lf60 61 6E 4D 6F 75 6E 74 69-65 00 00 00 00 00 00 00 anMountie...
lf70 9D 02 00 00 00 00 00 00 00-02 00 00 00 00 00 00 .....
lf80 03 00 03 00 02 09 18 00-03 00 00 00 11 50 68 69 .....Phi
lf90 6C 6C 69 70 03 00 00 00-9D 02 00 00 9E 02 00 00 llip...
lfa0 01 00 00 00 00 00 00 00 00-07 00 03 40 02 05 18 00 .....@...
lfb0 02 00 00 00 13 54 65 72-72 61 6E 63 65 19 61 6E .....Terrance·an
lfc0 64 20 50 68 69 6C 6C 69-70 00 00 00 00 00 00 00 d Phillip...
lfd0 9D 02 00 00 9E 02 00 00-00 00 00 00 00 00 00 .....
lfe0 06 00 03 40 02 05 18 00-01 00 00 00 11 53 74 65 ...·@.....Ste
lff0 70 68 65 6E 13 41 62 6F-6F 74 6D 61 6E 00 00 00 phen·Abootman...

```

Screenshot of Delete Transaction