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 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 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

🗄 🦳 🔂 data	1255_vm 8 Regular File	2/1/2018 6:30:5	PackageKit	16397	8 Regular File	2/9/2018 9:37:3
in in the se	1259 48 Regular File	2/1/2018 6:36:0		16401	16 Regular File	2/1/2018 8:51:2
	1259_fsm 24 Regular File	2/1/2018 6:30:5	ackups	174	8 Regular File	2/1/2018 6:30:5
11563	1259 vm 8 Regular File	2/1/2018 6:36:0	🖃 🫅 data	175	8 Regular File	2/1/2018 6:31:0
11564	1417 0 Regular File	2/1/2018 6:30:5	🚊 🛅 base	2328	0 Regular File	2/1/2018 6:30:5
- 16389	1418 0 Regular File	2/1/2018 6:30:5		2600	8 Regular File	2/1/2018 6:30:5
☐ 16394	16395 8 Regular File	2/1/2018 8:51:2		2600_fsm 2	24 Regular File	2/1/2018 6:30:5
alobal	16307 8 Regular File	2/0/2018 0:17:1	11564	2600_vm	8 Regular File	2/1/2018 6:30:5
	16401 16 Regular File	2/3/2010 3.17.1		2601	8 Regular File	2/1/2018 6:30:5
		2/1/2010 0:01:2		2601_fsm 2	24 Regular File	2/1/2018 6:30:5
E D ng multivact	174 8 Regular File	2/1/2018 0:30:5	iglobal	2601_vm	8 Regular File	2/1/2018 6:30:5
pg_montact	1 1/5 8 Regular File	2/1/2018 6:31:0	pg_clog	2602	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···	pg_log	<u>ີ 2602 fsm</u>	24 Regular File	2/1/2018 6:30:5
rces ×	led0 9E 02 00 00 00 00 00 00-00 00 00 00 00 00 00	00	terret in the second s	lec0 02 00 00 00 13 54 65 72-72	51 6E 63 65 03 00	00 ····Terrance···
athlEila Ontiona	lee0 06 00 03 80 02 29 18 00-01 00 00 00 0F 53 74	65 ····) ····Ste	Sources ×	led0 9E 02 00 00 00 00 00 00-00	00 00 00 00 00 00	00
	16IU 76 65 6E 13 41 62 6F 6F-74 6D 61 6E 00 00 00	00 Ven Abootman · · · ·	Dath ICila	lee0 06 00 03 80 02 29 18 00-01)0 00 00 0F 53 74	65 · · · · ·) · · · · · · · Ste
	1f10 0F 00 03 00 00 00 00 00 00 00 00 00 00 00	6F 500	empauriplie Opuons	16IU /6 65 6E 13 41 62 6E 6E-/4 0	3D 61 6E 00 00 00	00 ven Abootman · · · ·
	1f20 74 74 11 44 69 63 68 60-61 6F 00 00 00 00 00	00 tt.Dickman		1f10 05 00 03 00 02 05 18 00-05	00 00 00 00 00 00 00 00 00 00 00 53 63	6F
	1f30 9D 02 00 00 00 00 00 00-03 00 00 00 00 00 00			1f20 74 74 11 44 69 63 6B 6D-61	6E 00 00 00 00 00 00	00 tt.Dickman
	1f40 04 00 03 00 02 09 18 00-04 00 00 08 52 69	63Bic		1f30 9D 02 00 00 00 00 00 00-03	00 00 00 00 00 00	00
	1f50 6B 31 54 68 65 50 72 6F-75 64 43 61 6E 61 64	69 k1TheProudCanadi		1f40 04 00 03 00 02 09 18 00-04)0 00 00 0B 52 69	63 ····Ric
	1f60 61 6E 4D 6E 75 6E 74 69-65 00 00 00 00 00 00	00 anMountie · · · · · ·		1f50 6B 31 54 68 65 50 72 6F-75	54 43 61 6E 61 64	69 klTheProudCanadi
	1f70 9D 02 00 00 00 00 00 00-02 00 00 00 00 00 00	00		1f60 61 6E 4D 6F 75 6E 74 69-65	00 00 00 00 00 00	00 anMountie · · · · · ·
	1f80 03 00 03 00 02 09 18 00-03 00 00 00 11 50 68	69Phi		1f70 9D 02 00 00 00 00 00 00-02	00 00 00 00 00 00	00
	1f90 6C 6C 69 70 03 00 00 00-9D 02 00 00 9E 02 00	00 11ip		1f80 03 00 03 00 02 09 18 00-03)0 00 00 11 50 68	69 · · · · · Phi
	1fa0 01 00 00 00 00 00 00 00-07 00 03 40 02 05 18	00		1f90 6C 6C 69 70 03 00 00 00-9D)2 00 00 9E 02 00	00 11ip
	1fb0 02 00 00 00 13 54 65 72-72 61 6E 63 65 19 61	6E · · · · · Terrance · an		1fa0 01 00 00 00 00 00 00 00 00-07	JU U3 40 U2 U5 18 C1 CE C2 CE 10 C1	CE
	1fc0 64 20 50 68 69 6C 6C 69-70 00 00 00 00 00 00	00 d Phillip · · · · ·		1100 02 00 00 00 13 54 65 72-72 0	00 00 00 00 00 00 00 01 05 03 03 19 01	00 d Phillip
>	1fd0 9D 02 00 00 9E 02 00 00-00 00 00 00 00 00 00	00		1fd0 9D 02 00 00 9E 02 00 00-00		00
1 1 1	1fe0 06 00 03 40 02 05 18 00-01 00 00 00 11 53 74	65 · · · @ · · · · · · · · Ste		1fe0 06 00 03 40 02 05 18 00-01	00 00 00 11 53 74	65ß
Remove <u>A</u> ll <u>C</u> reate Image	1ff0 70 68 65 6E 13 41 62 6F-6F 74 6D 61 6E 00 00	00 phen ·Abootman · · ·	ove Remove <u>A</u> ll ⊆reate Image	1ff0 70 68 65 6E 13 41 62 6F-6F	74 6D 61 6E 00 00	00 phen Abootman · · ·
x Value Int Custom Conte	Cursor pos = 0		Hex Value Int Custom Conte	Cursor pos = 0; clus = 4253196; log sec = 3402	25568; phy sec = 34027	616
nsaction.ad1/Custom Content Image([Multi]) [AD1]/\\.\PHYSICALDRIVE3:VolGroup-ly_root [51200MB]:NONAME [ext4]/[root]/vafrom atta						

Screenshot of Update Transaction

Screenshot of Delete Transaction

