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.

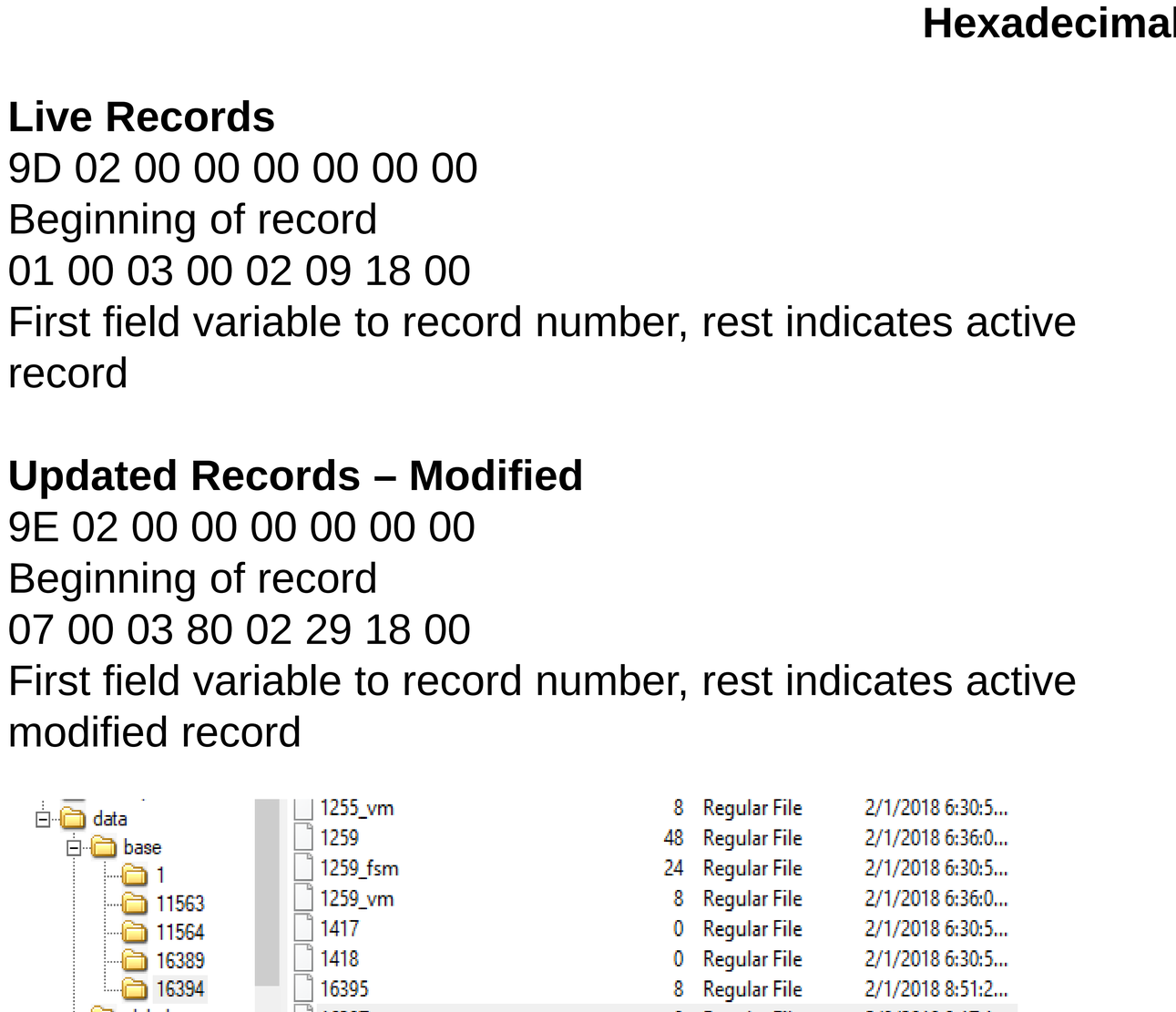
Hexadecimal Meanings

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

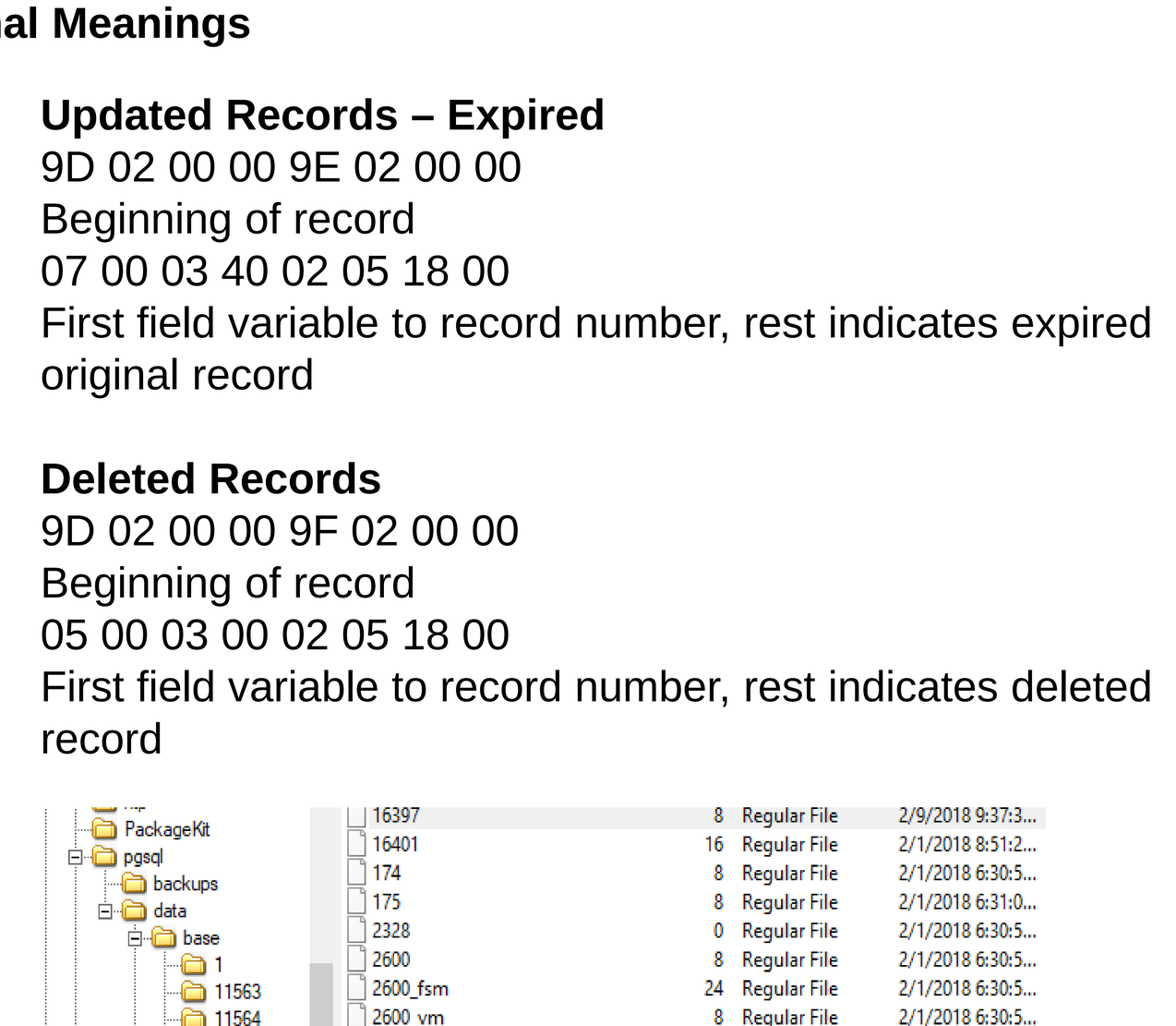
Updated Records – Modified
9E 02 00 00 00 00 00 00
Beginning of record
07 00 03 80 02 29 18 00
First field variable to record number, rest indicates active modified record

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



Screenshot of Update Transaction



Screenshot of Delete Transaction