Invistigation forensics : how to find evidence from an oracle data base

Problem ment: In today’s technology-oriented world, information has become the lifeline of businesses. Be they banks or industries or small shops, information security has become crucial more than ever before. Since many employees, in one way or other, are connected and involved in information processing, security concerns have risen drastically. Thus, proper data integration and developing a contingency plan for the precise recovery of past data have become inevitable.

Literature Review:

Wright, P. M. (2005) practically evaluates the effectiveness of using LogMiner utility as an Oracle Forensics investigation tool. He typically started to assess the tool’s applicability by testing how rightly it creates a timeline and records the database actions that occurred in the past. Subsequently, the LogMiner’s transformation, interpretation and authenticity of Time Stamp data type were focused on.

Under the heading “ Scope of LogMiner testing” he defined that LogMiner could be used to analyze the Oracle generated redo log files containing information regarding the changes made for either recovering infected file(s)/corrupted data or tracking past actions. He further added that another method of ensuring database security is to regularly monitoring the Oracle built-in audit functions.

In order to check the reliability & validity of LogMiner, the researcher carried out the following three tests:

1. General forensic capability: Can the LogMiner utility produce a forensic timeline and

recover data?

2. Accuracy level: Precision of TIMESTAMP identified during test 1.

3. Find out source of inaccuracy: Is the inaccuracy fault lies in the LogMiner?

(1) General capability:

Results of test 1 showed that an index giving full time line was created disregarding the researcher's page count. Moreover, the column showing timestamp indicated an accuracy of one second while a timestamp by default shows one second with 6 decimal places. The data recovery phase also took place well. To ensure validity, the test was repeated 20 times and it yielded perfect results every time it ran.

(2) Level of Precision of Timestamp:

The reason Timestamp field was not showing decimal places for second could possibly be format mask or it may be defined right on the second or perhaps it was not a time field at all. Having run the query, it was found that the timestamp field was defined as Date field while the field was wrongly named as " Timestamp" which was misrepresenting in a forensics context. However lateron, a test was run creating a proper Timestamp field to see if LogMiner can store the decimal places. The test was run thrice – once after rebooting the system and the results were same in all instances.

(3) LogMiner's Imprecision or the logs themselves?

This test was aimed to determine what causes imperfection in reporting Timestamps – i. e. it is LogMiner or the redo logs that distorts the fractional decimals in a second. To test it timestamps were entered into the database – one with decimal places and another without and then analyzed the variance in the converted log. Having run the test, results showed that it was LogMiner that converted Timestamps into Dates causing distortion in fractional decimal places. The test was conducted multiple times and it yielded the same occurrence.

Conclusions

He concluded that all the tests were successfully conducted and results occurred as expected. LogMiner lets the analyst to run Structured Query Language (SQL) to the Oracle’s redo logs which are independent of database. The tool enables you to verify the information found on a normal dbf and enables you to recover the lost data.

References

Wright, P. M. (2005). Fight crime. Unravel incidents... one byte at a time: Oracle Database Forensics using LogMiner, SANS Institute, 1-39. Retrieved May 30, 2011, from http://computer-forensics. sans. org/community/papers/gcfa/oracle-database-forensics-logminer_159