Paper Review

Database Forensic Analysis with DBCarver

Gurpreet Singh

February 11, 2018

CS4414

Jot notes

Abstract

- Forensics needs to be effective on databases that are configured incorrectly and have no protection techniques integrated in them. Sometimes they don't even have logging
- Paper talks about a tool called DBCarver.
- Reconstructs database context from a database image without using any log or system data.
- Uses page carving to reconstruct both query-able data and deleted data.
- Allows investigators to conduct new types of analysis on the data

Introduction

- Since most large applications use databases, large scale cyber crime almost always involves databases.
- A related concept is file carving, which retrieves files from storage on a file system even if they are deleted or corrupted
- Relational databases store data in pages
- We can reconstruct pages to retrieve data
- Targets extracting data maintained by the running database instead of recovering original
- Paper considers two scenarios, database is good or bad
-

Summary

Strengths and Weaknesses