Contribution ID: **482** Type: **not specified**

Correlating Memory, Persistent, and Runtime Evidence in Redis

Tuesday, 2 December 2025 16:30 (30 minutes)

Databases are an important source of digital evidence, but most forensic methods and tools are focused on relational database systems. In-memory NoSQL databases, such as Redis are harder to investigate because persistence files and logs record only part of the activity, and volatile evidence exists in memory. This paper presents a technique and parser to bring multiple Redis sources: memory snapshots, RDB, AOF, MONITOR, ACL logs, and SLOWLOG together. Three experiments were carried out. The first tested recovery of short and long values from memory, showing that command arguments can be extracted from an offset even when not preserved in persistence. The second measured coverage across individual sources and demonstrates that combining them gives a broader view of the investigation. The third examine a master-replica scenario, where the parser recovers missing operations by matching memory with monitor logs. Our findings show that cross-source artifact correlation improve completeness in Redis forensic analysis.

Presenting Author

Email

Student or Postdoc?

Institute

Registered for the conference?

CHPC User

CHPC Research Programme

Primary author: ZIA, Muhammad Abdul Moiz

Presenters: Dr ADEDAYO, Mary O. (Applied Computer Science, The University of Winnipeg); ZIA, Muhammad Abdul Moiz

Session Classification: ISSA