End-to-End Database Storage Analysis

CNF-1656268

PI: Alexander Rasin, co-PI: Jacob Furst, DePaul University

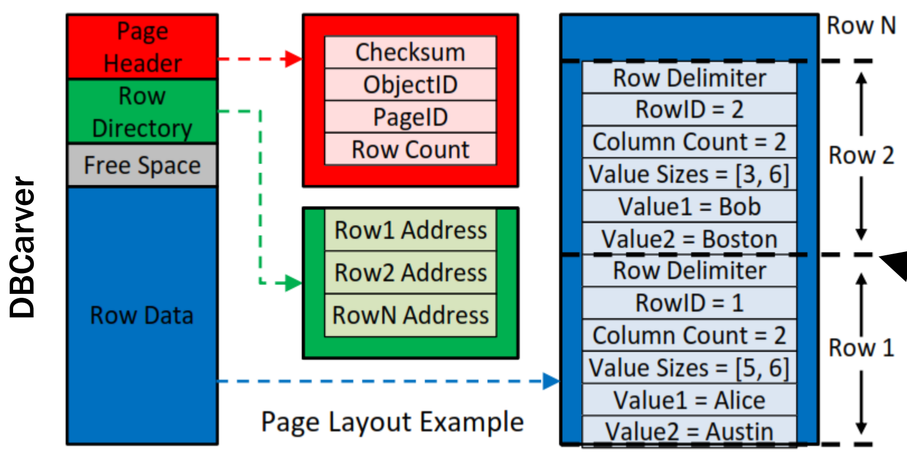
James Wagner (DePaul), Karen Heart (DePaul), Jonathan Grier (Grier Forensics)

Key Problems

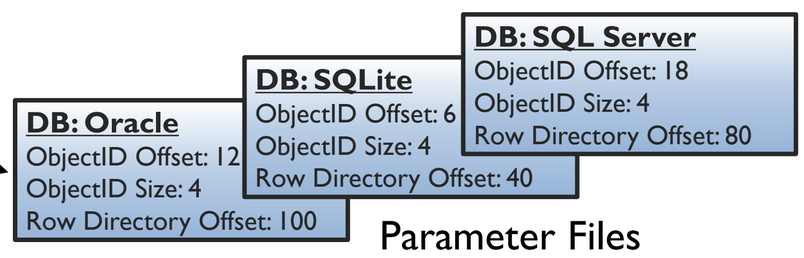
- Cyber-crimes involve data repositories, Database Management Systems (DBMS)
- Relational DBMS storage cannot be viewed/accessed directly
- The need for DBMS investigative tools:
  - Forensic analysis (independent evidence collection)
  - Intrusion detection (e.g., insider threat)
  - Evaluate performance reproducibility
  - Data retention compliance (e.g., secure delete)

Scientific Impact

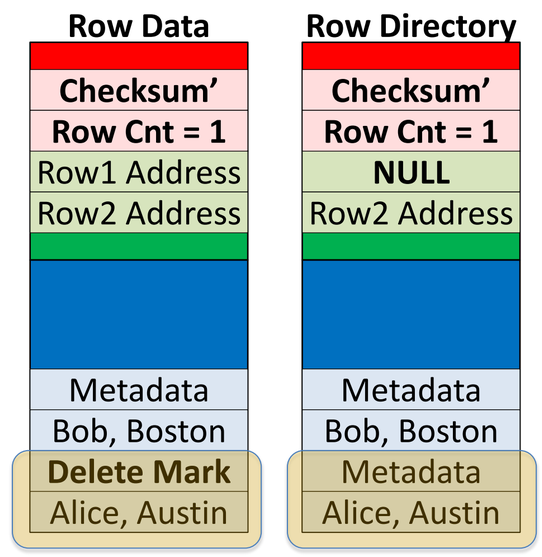
- Systematic approaches to reverse engineering system storage
  - Oracle, PostgreSQL, MySQL, SQLite, DB2, MS SQL Server, Firebird, Apache Derby, Maria DB
- Integrate database analysis with file-based forensic tools
- Augment access-monitoring tools with forensic artifacts
- Establish admissible evidence rules (e.g., presentable in court)

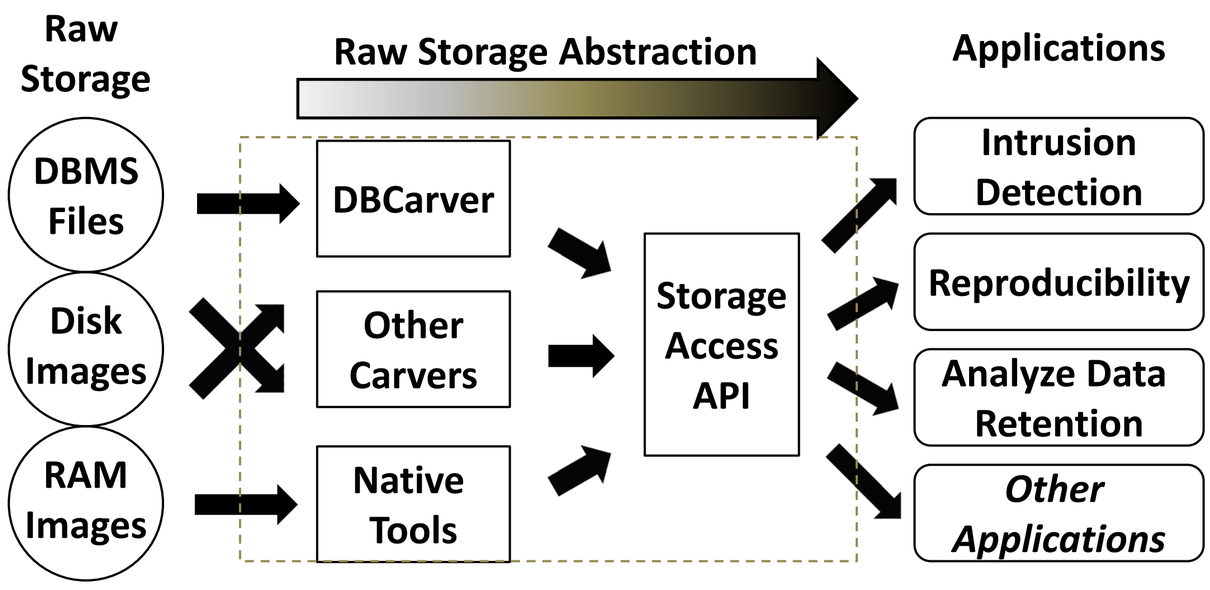


- Automatically determine page layout
- Deconstruct storage at the page level
- Page layout described in parameter files



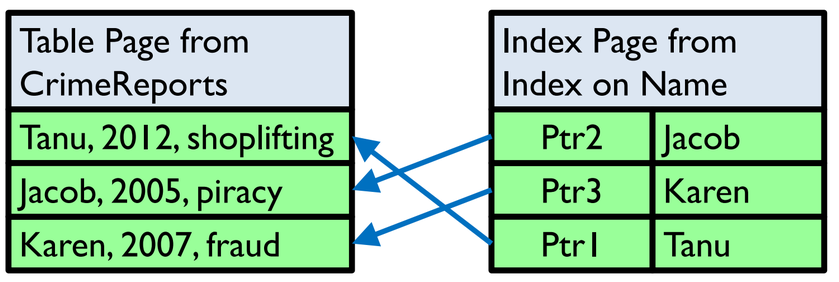
Mark Alice's deleted record in:





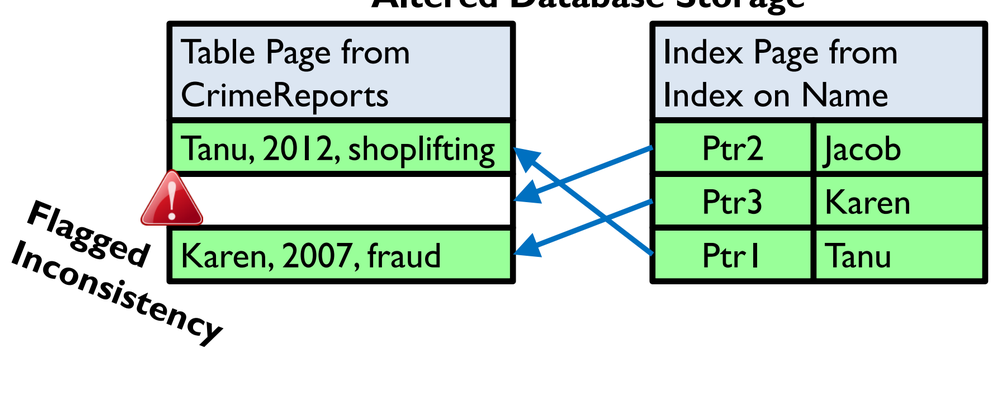
- Deleted records remain in storage
- Quantify deleted content via the API
- Validate data retention (e.g., secure delete)

Original Database Storage



- Jacob bribes a SysAdmin to erase his record
- SysAdmin has no DBMS account but:
  - Can modify the DB file on disk
  - Bypasses logging/access control

Altered Database Storage



Threat Scenarios (in untrusted environment)

- Data altering / evidence destruction – forensic investigation
  - DFRWS '15, DFRWS '16, CIDR '17, DFRWS '19
- Data theft / retained old data – evaluate data retention
- Database Admin altering records – audit log consistency
  - DFRWS '17
- System Admin altering DBMS files – audit DBMS files
  - EDBT '18, HST '18

- New tools for forensic analysts and data theft & tampering investigations
- Eliminate the 'blind spot' of current database monitoring tools
- Direct DBMS storage access for DB administrators and researchers
  - Security
  - Reproducibility
  - Performance

- Full understanding of DBMS storage
  - Advanced DB courses at DePaul
  - DFRWS '19 toolkit open-sourced
  - Storage benchmark under review (at CODASPY '20)
- Custom tutorial and course materials
  - Interactive web-based tutorials
  - Course on file / DB forensics, legal & procedural considerations

- Requests/Interest in our tools:
  - Regional Computer Forensic Lab (managed by FBI in Chicago)
  - Mandiant/FireEye
  - Royal Candian Mounted Police
  - MITRE
  - Individual researchers/teachers
- Forensic investigators mostly lack the ability to interpret DBMS files