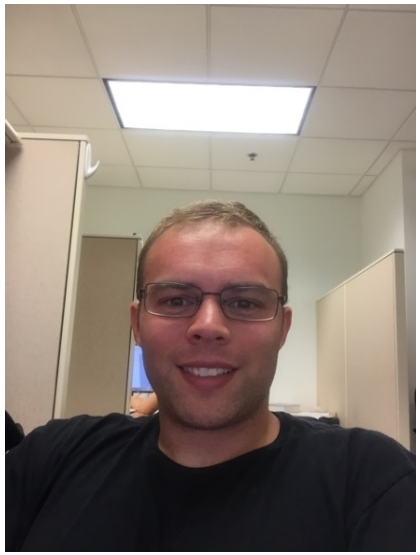
for Databases

DePaul

GRIER FORENSICS



James Wagner

Alexander Rasin

Jonathan Grier

Tanu Malik

Karen Heart

Motivation

- Data is a valuable asset
- Data breaches
  - More than 85% go undetected[]
  - Average detection time is 210 days[2]

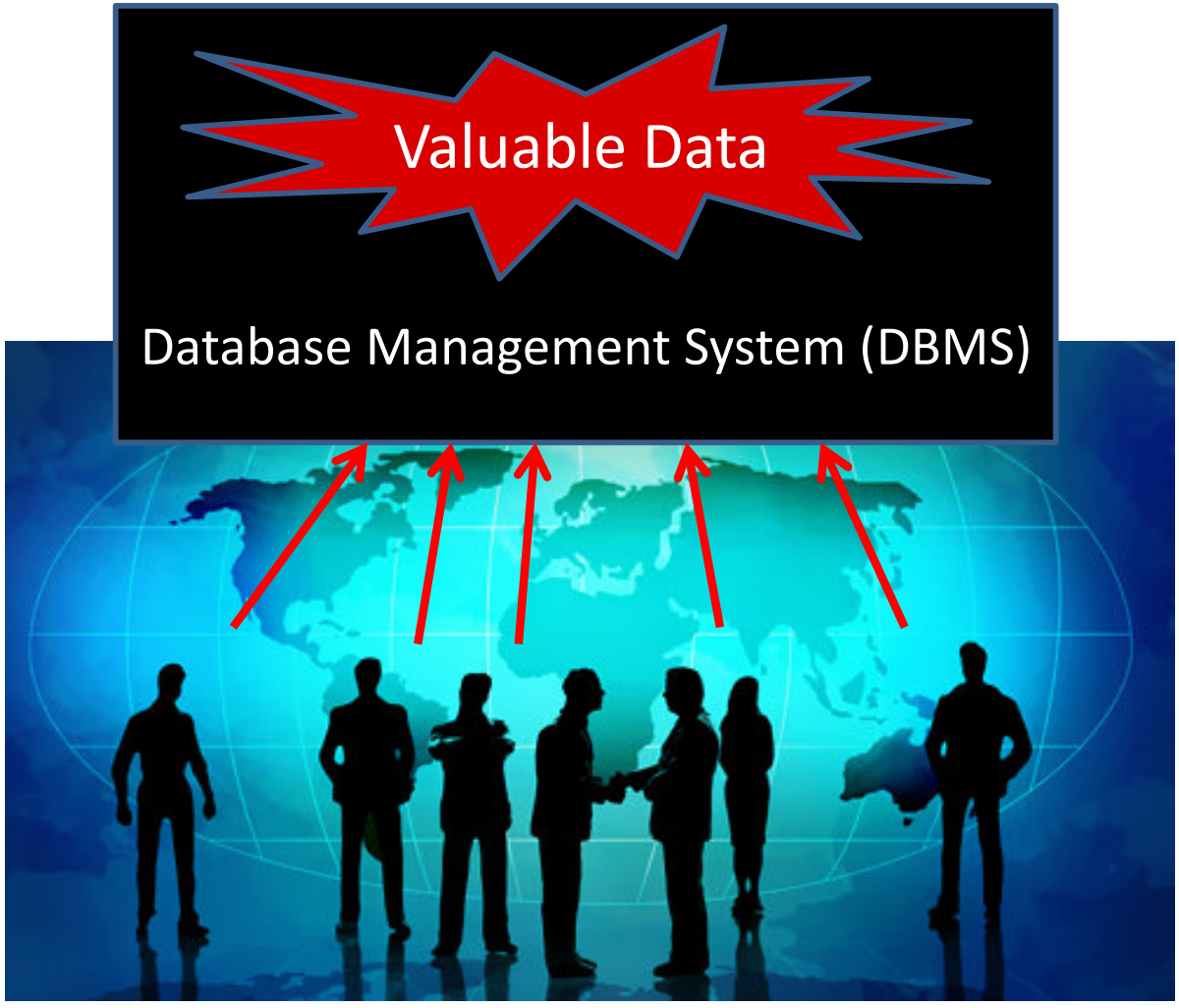
[1] E. Ouellet and P. E. Proctor. Magic quadrant for content-aware data loss prevention. Technical Report, 2012.

[2] T. TrustWave. global security report, 2013. http://www.trustwave.com/2013GSR, 2013.

DBMSes are Everywhere

- The obvious
  - Financial data
  - Website back-end
- The less obvious
  - Mobile phones (SQLite)
  - Human Resources (PeopleSoft)
  - Web-browsers (SQLite)

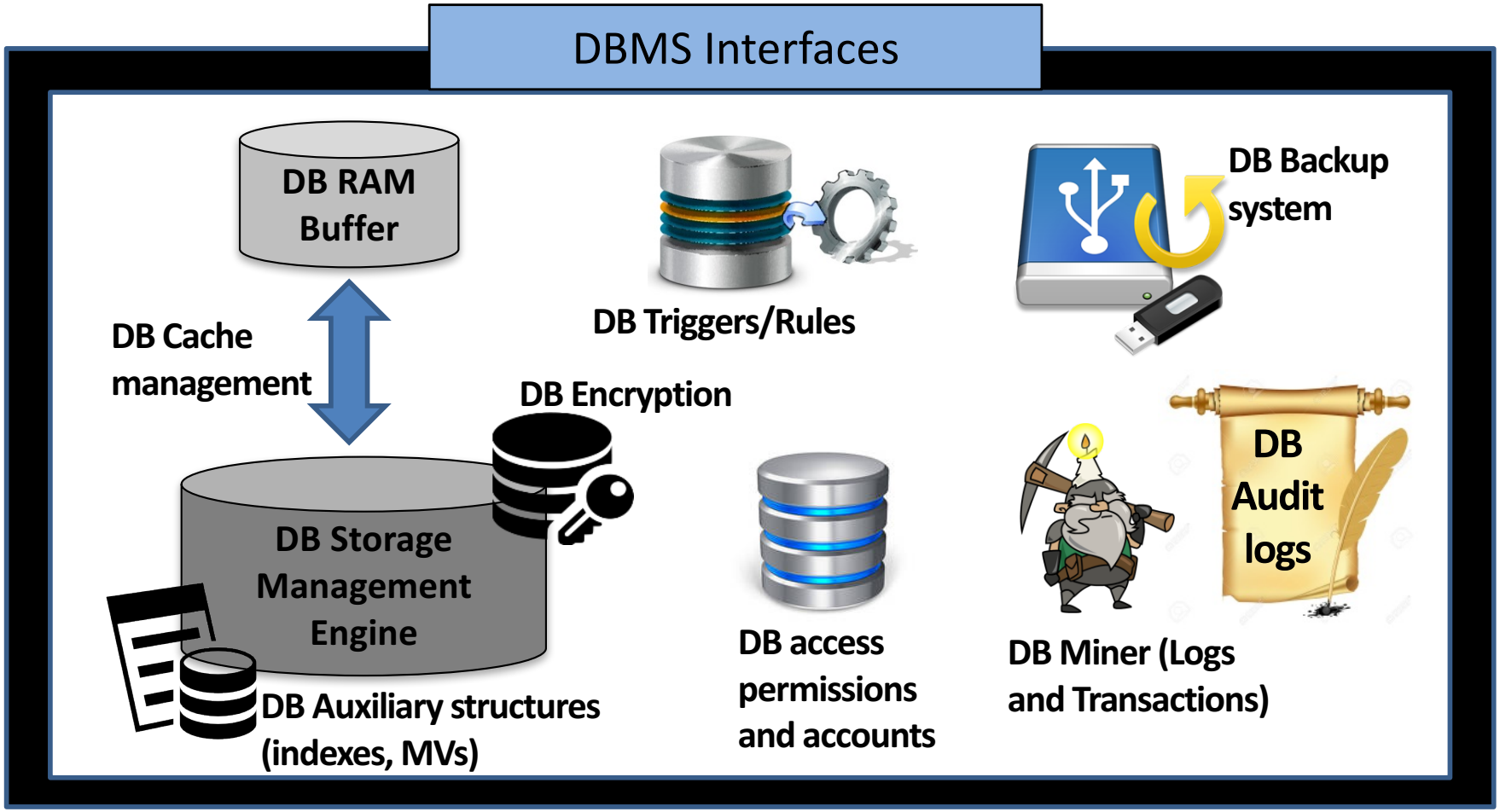
DBMS is a BlackBox



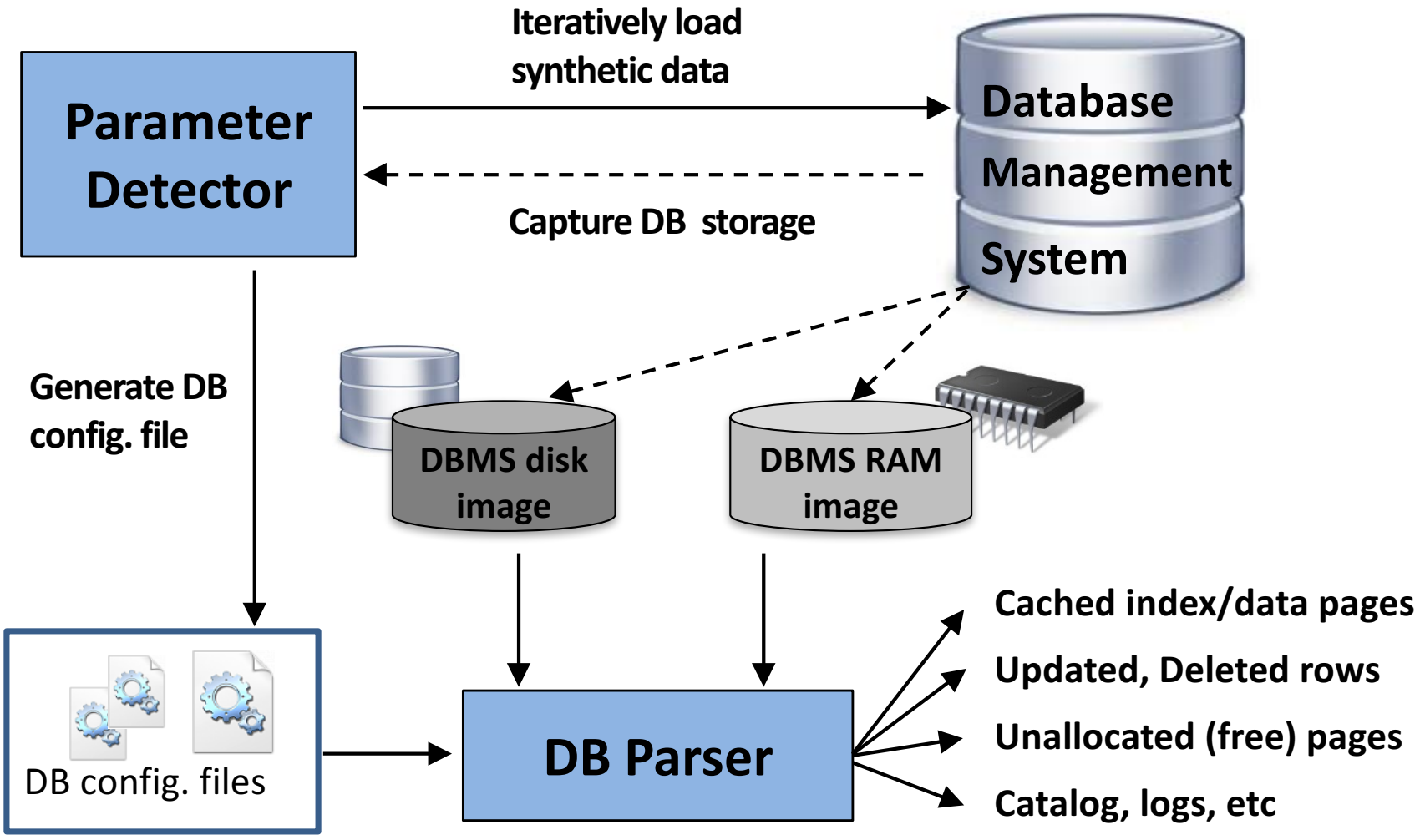
DBMS: The Inner World

Current investigative tools do not work on DBMSes

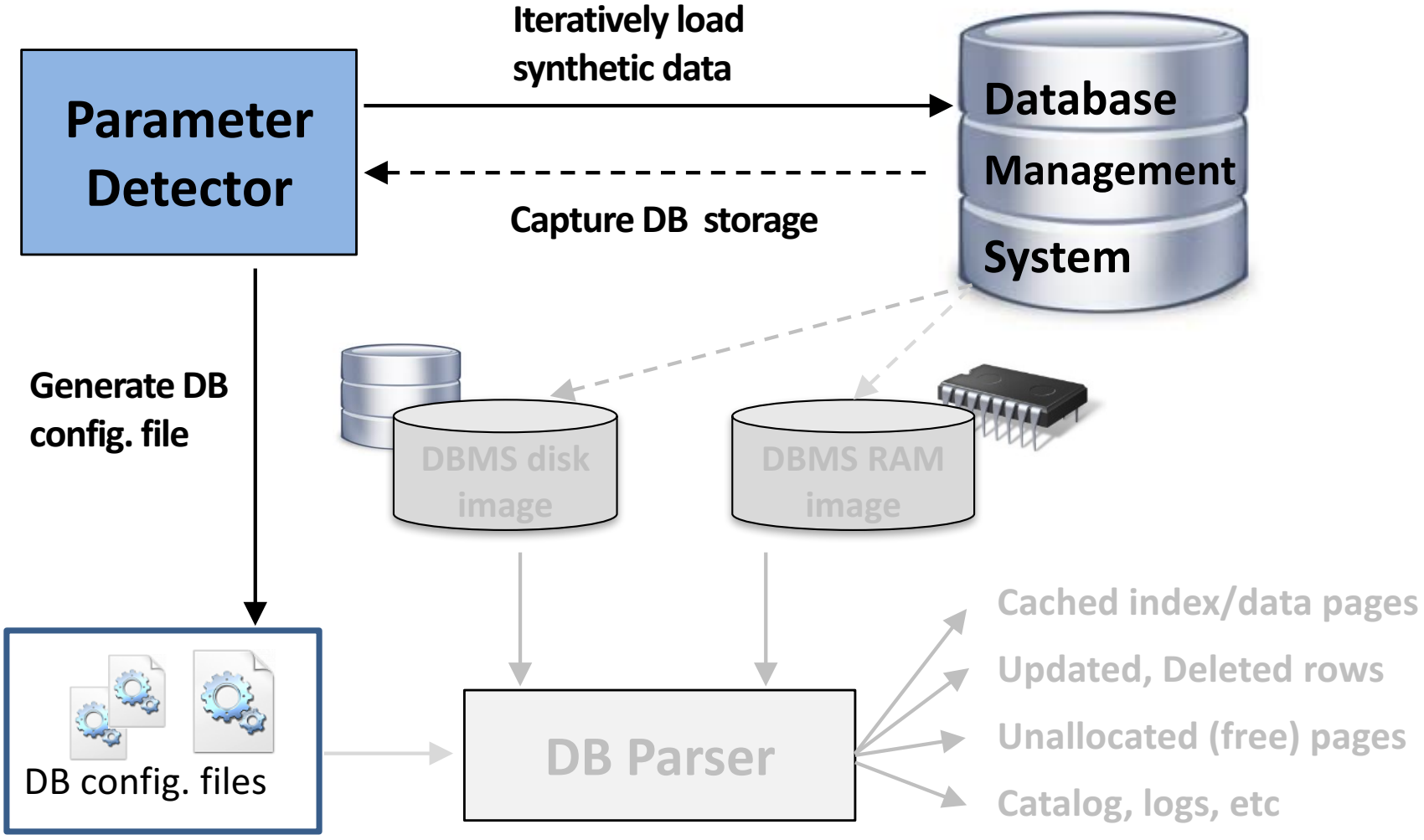
Database files are meaningless without DBMS



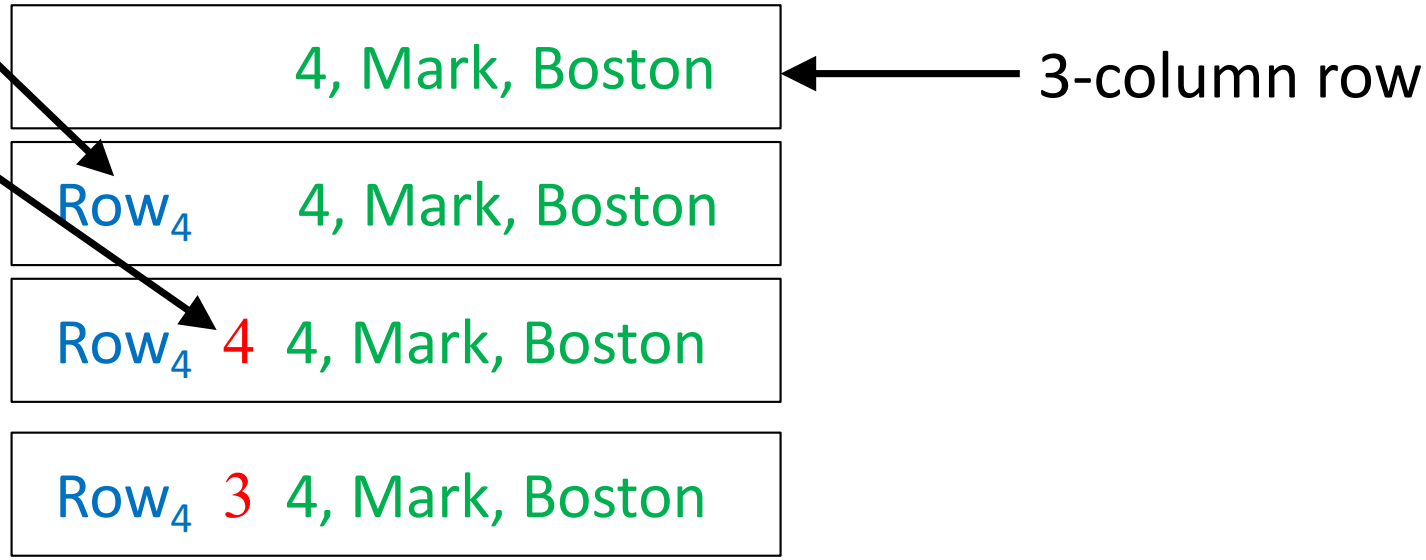
DBCarver Architecture



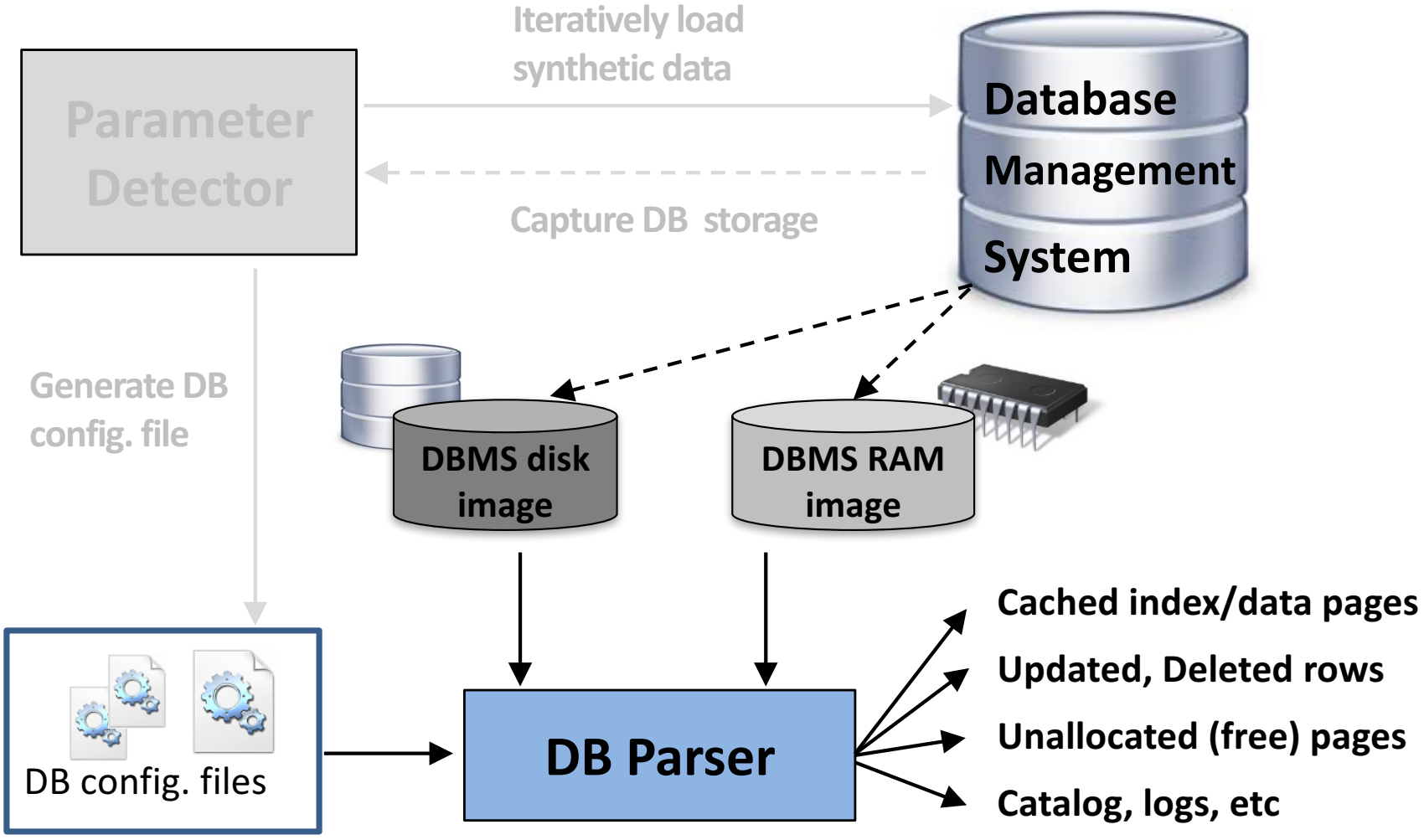
DBCarver Architecture



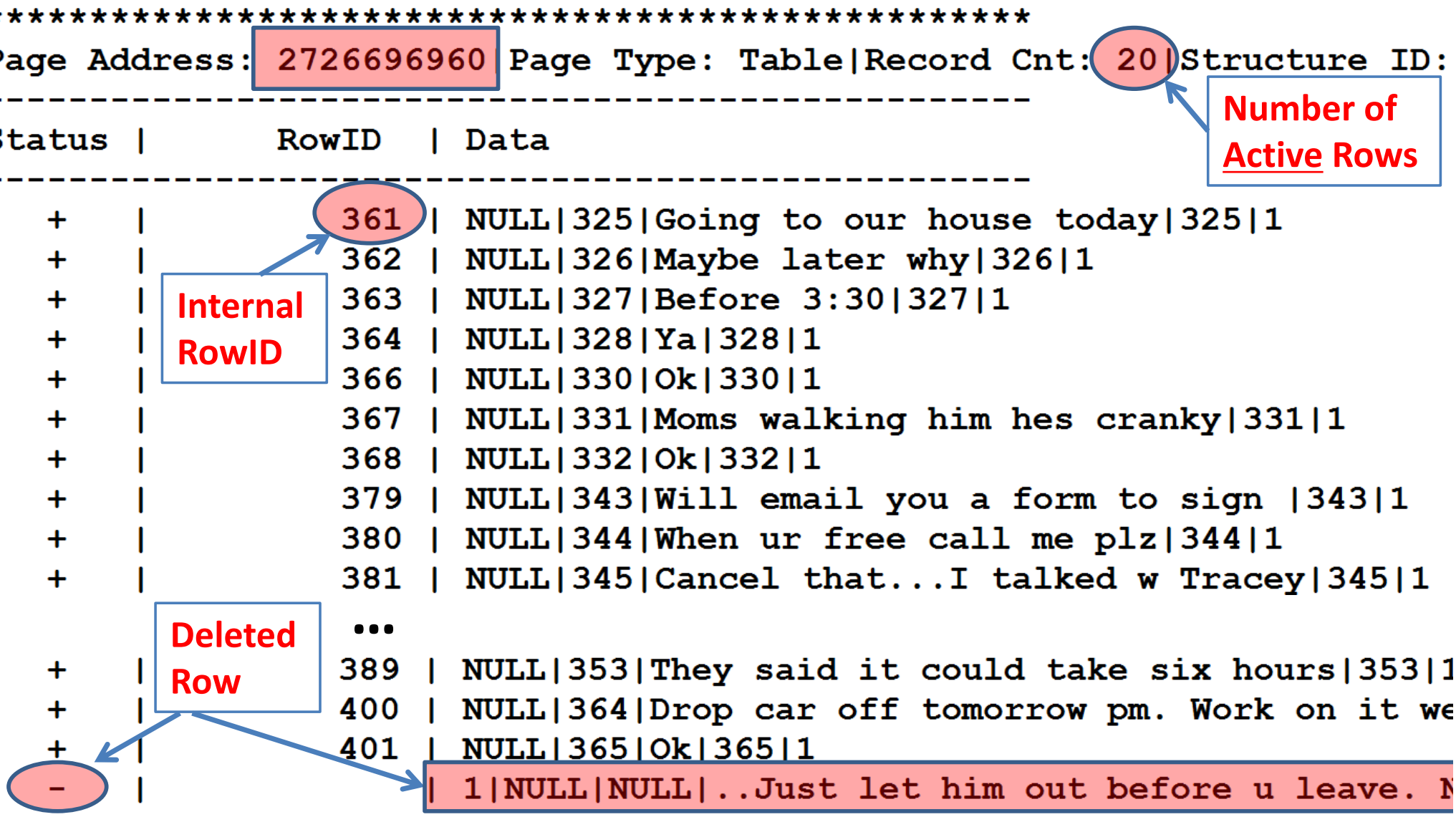
	Oracle	PostgreSQL	SQLite	Firebird	DB2	SQLServer	MySQL	Apache Derby
Structure Identifier	Yes	No	Yes					No
Unique Page ID	Yes							No
Row Dir. Sequence	Top-to-bottom insertion					Bottom-to-top insertion		
Row Identifier	No	Yes	No			Yes		
Column Count	Yes		No		Yes	No		Yes



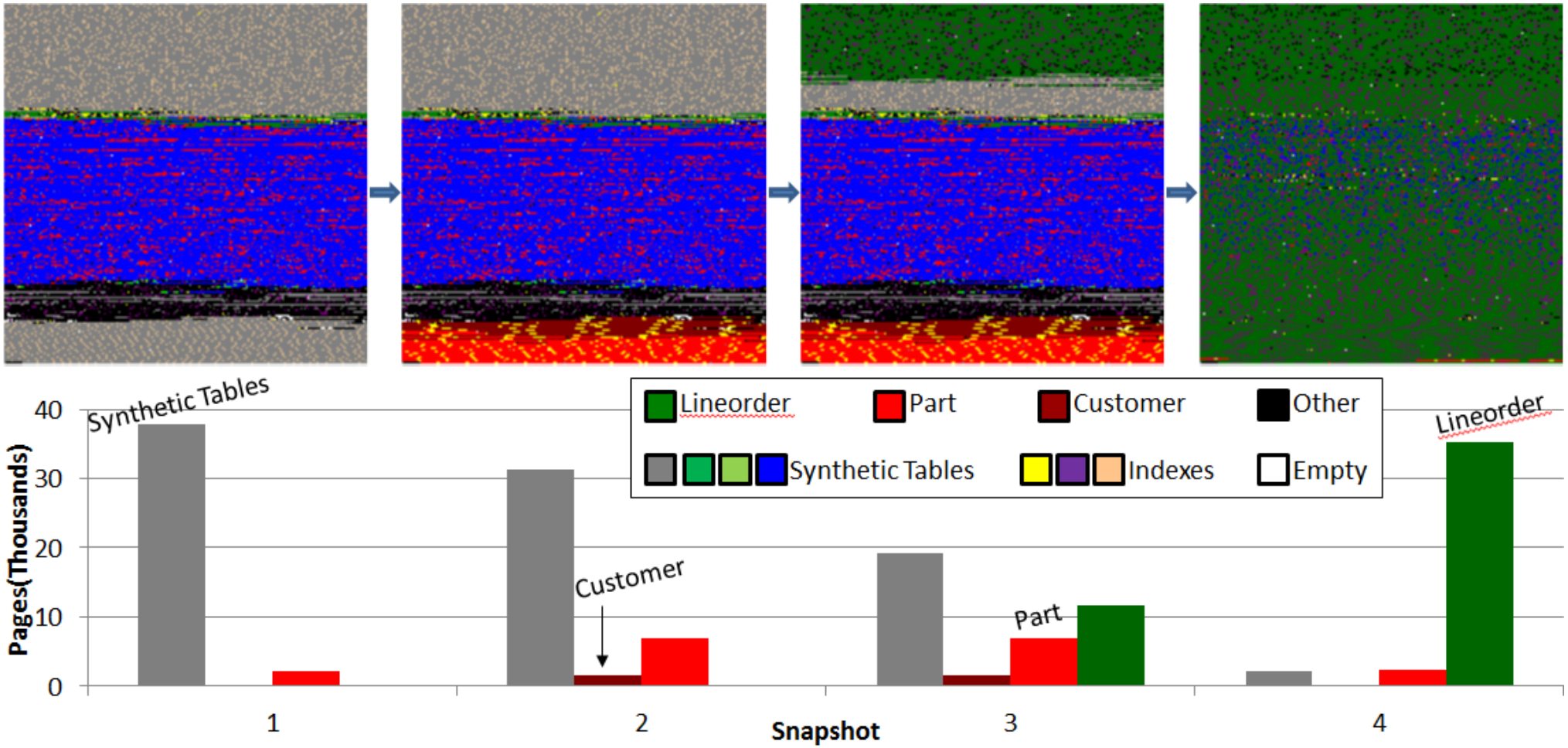
DBCarver Architecture



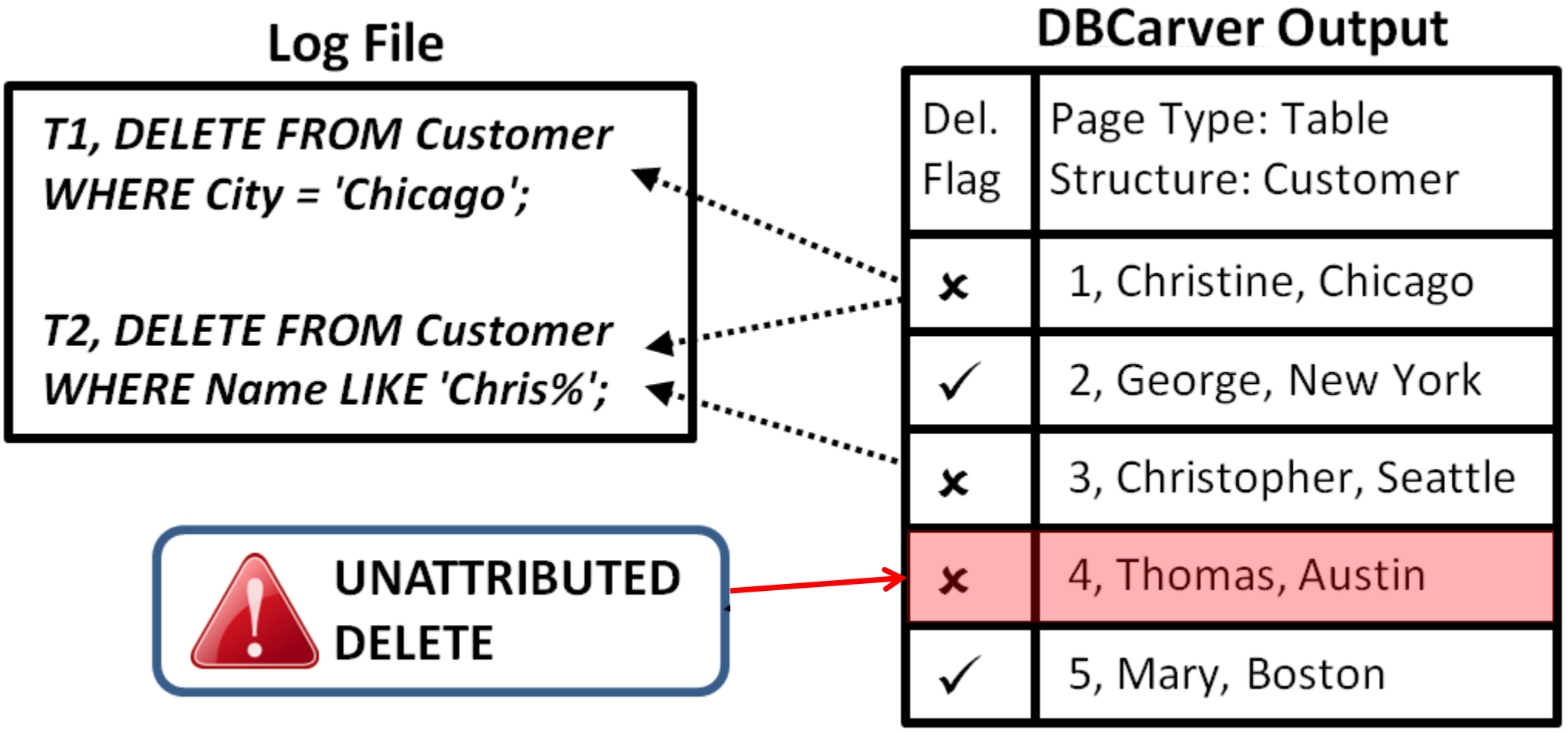
DBCarver Output (SQLite on Android)



Oracle RAM Snapshots



Insider Threats (Log Tampering)



Use Cases and Collaborations

Contact Us

- Available during break at 4:00
- Alexander Rasin
  - DePaul University, 312-362-7008, arasin@depaul.edu
- Jonathan Grier
  - Digital Forensics consultant
- Karen Heart
  - Litigation attorney – so we are also interested in all associated legal / evidential issues