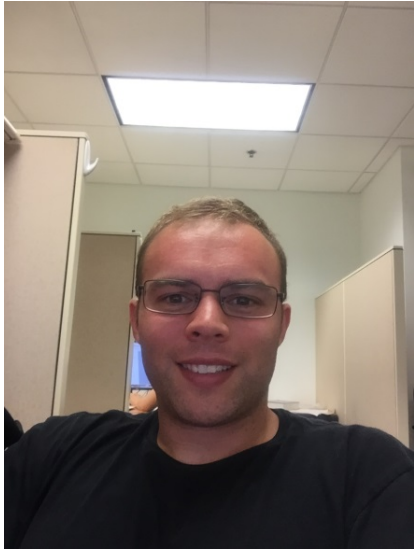




for Databases





James Wagner



Alexander Rasin



Jonathan Grier



Tanu Malik



Karen Heart



Motivation

- Data is a valuable asset
- Data breaches
 - More than 85% go undetected^[1]
 - 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)



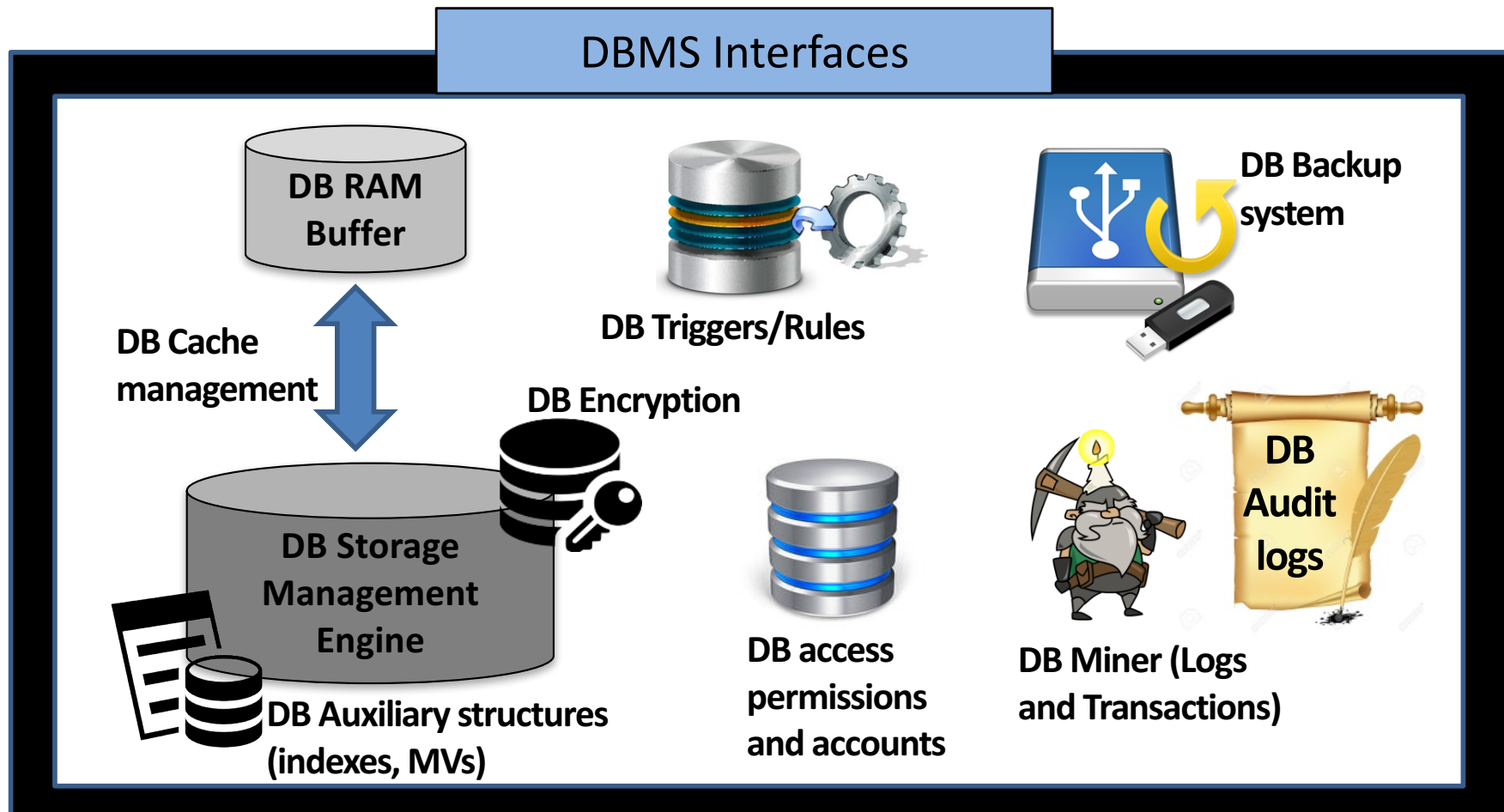
DBMS is a BlackBox



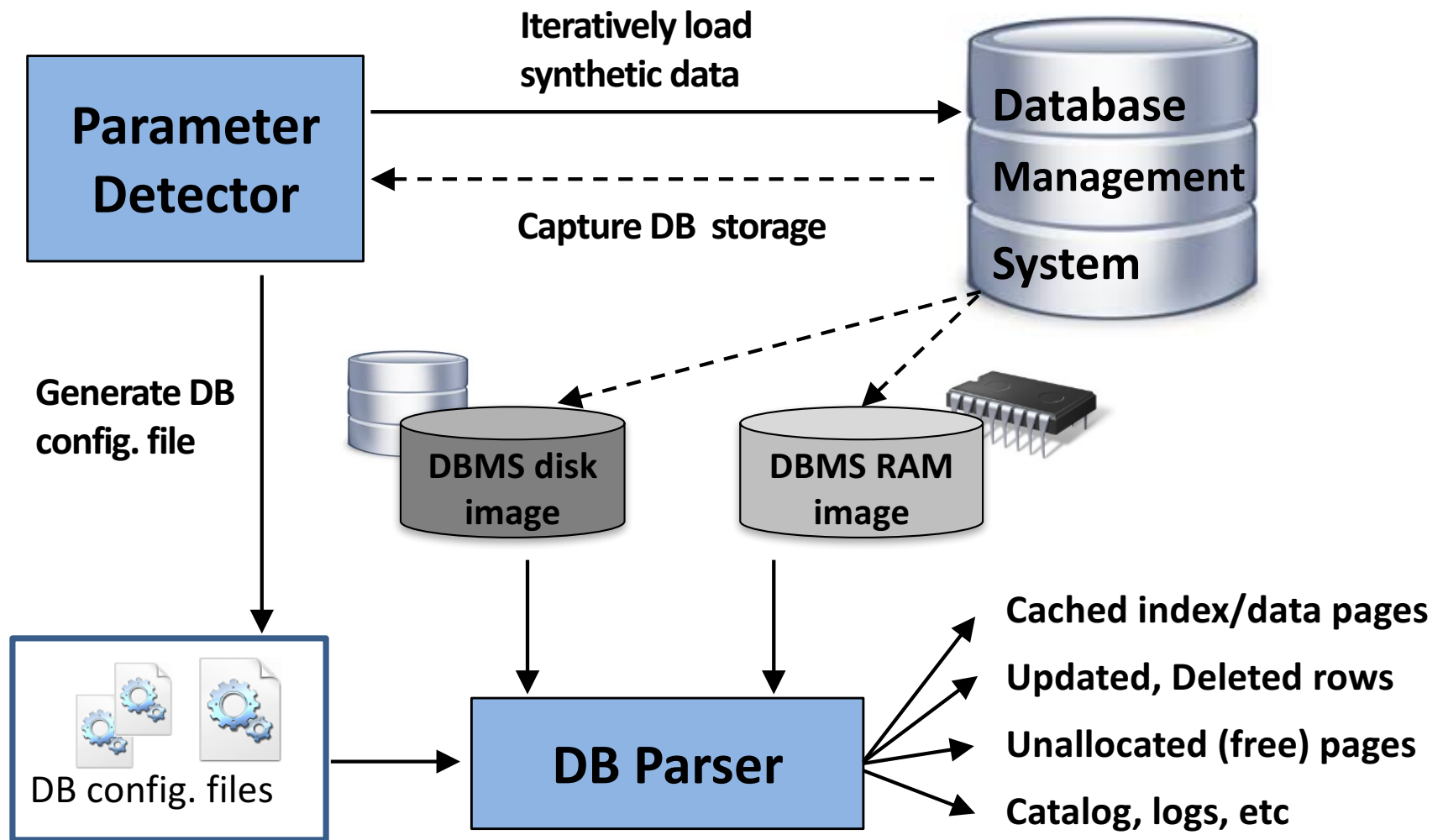
DBMS: The Inner World

**Current investigative tools
do not work on DBMSes**

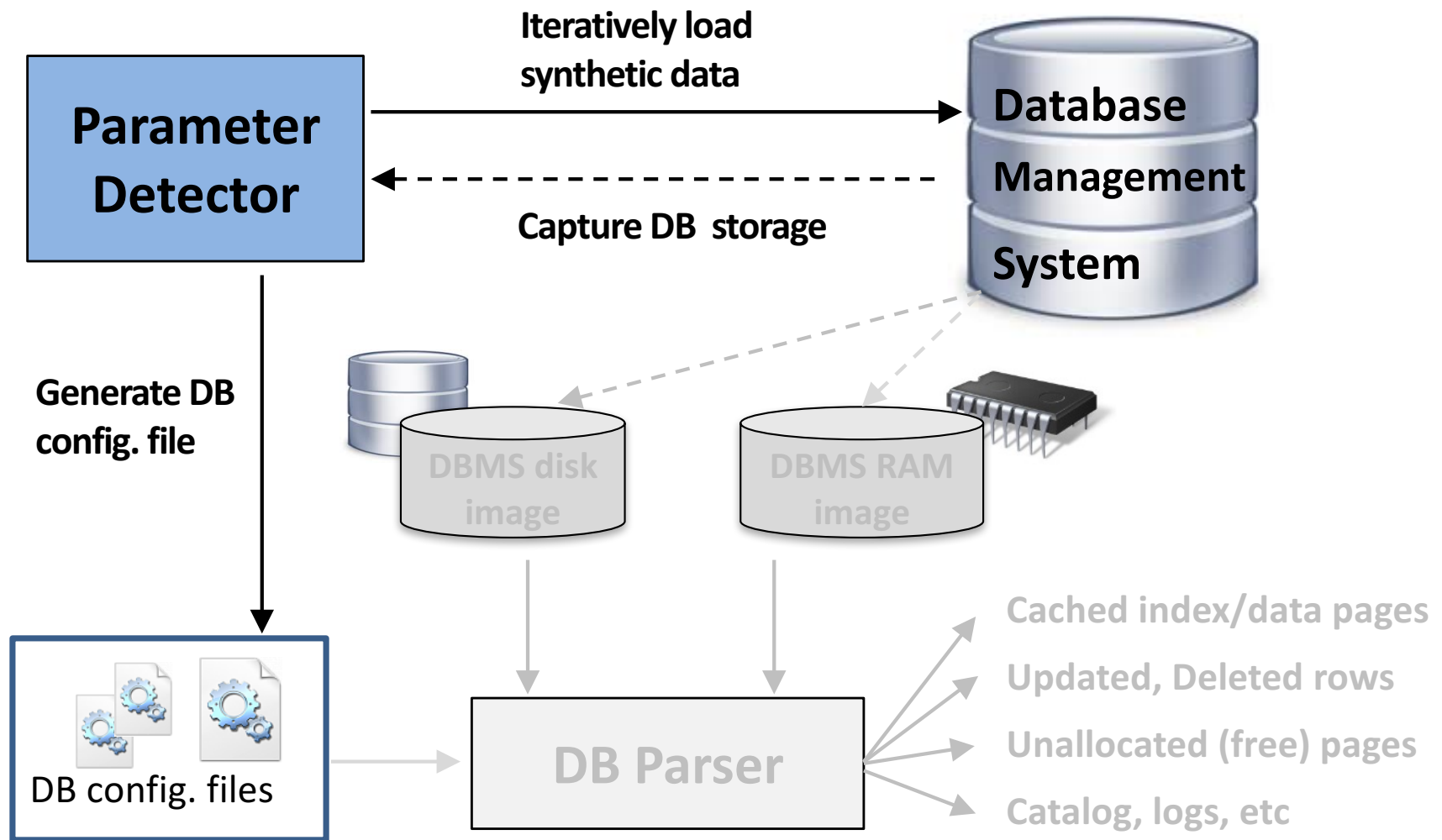
**Database files are
meaningless without DBMS**



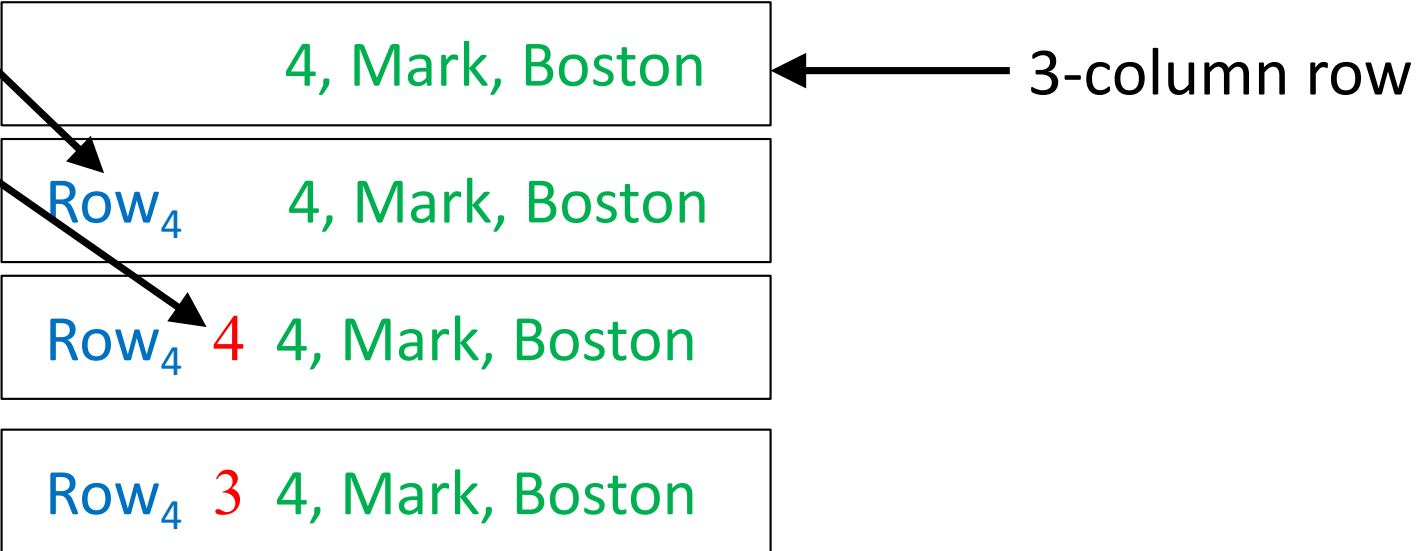
DBCarter Architecture



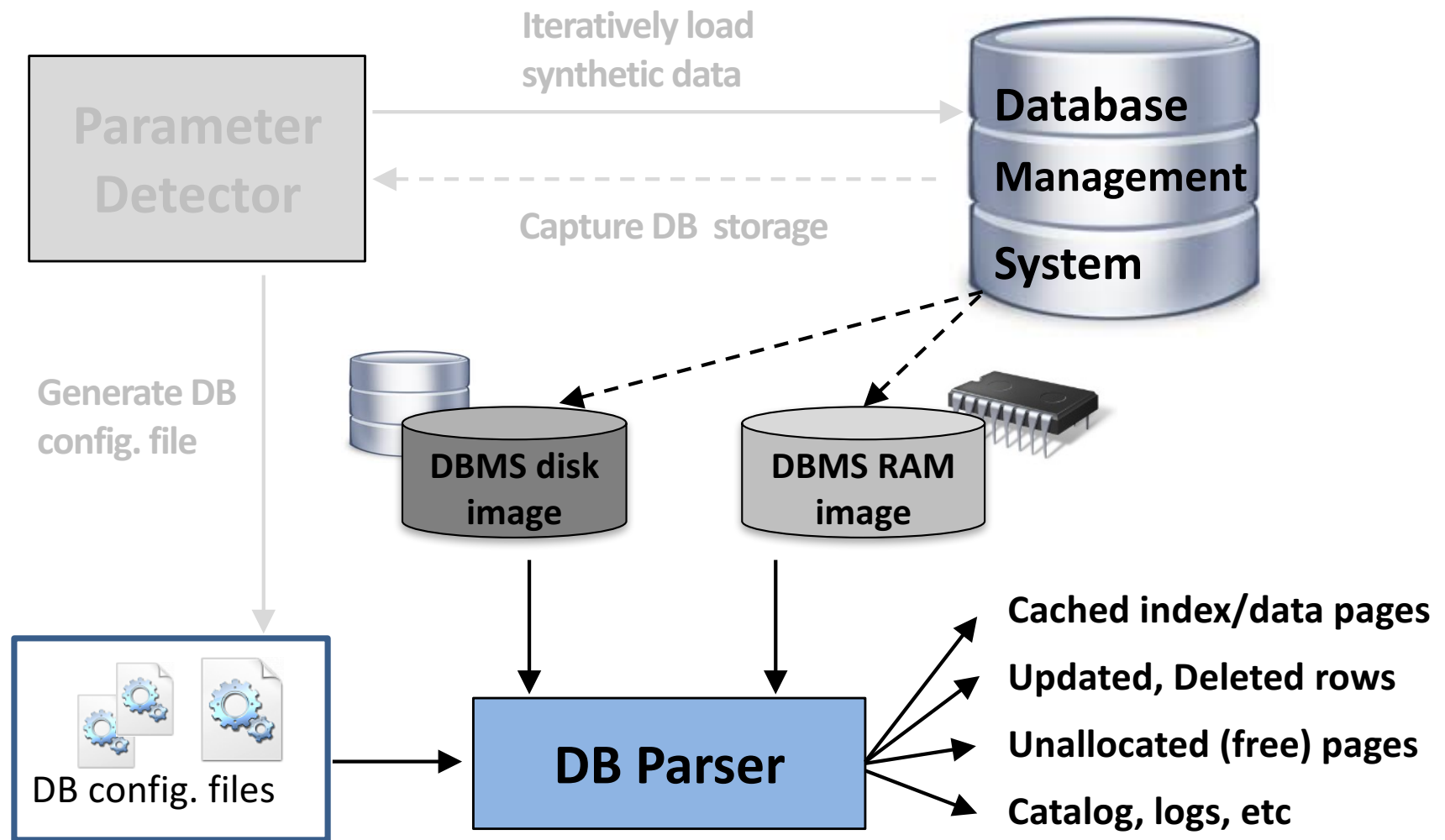
DBCarter Architecture



	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)

Page Address: **2726696960** Page Type: Table|Record Cnt: **20**|Structure ID:

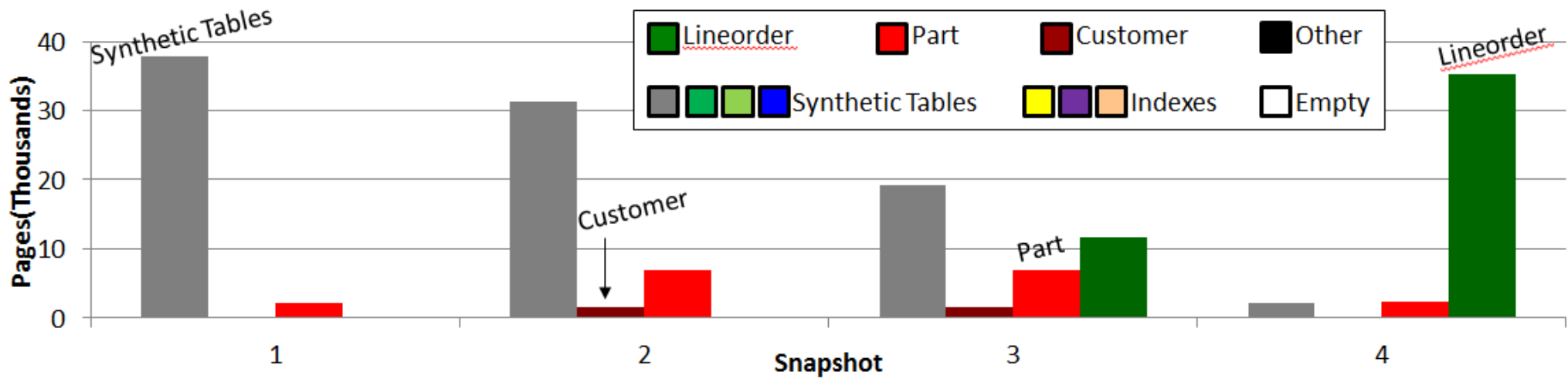
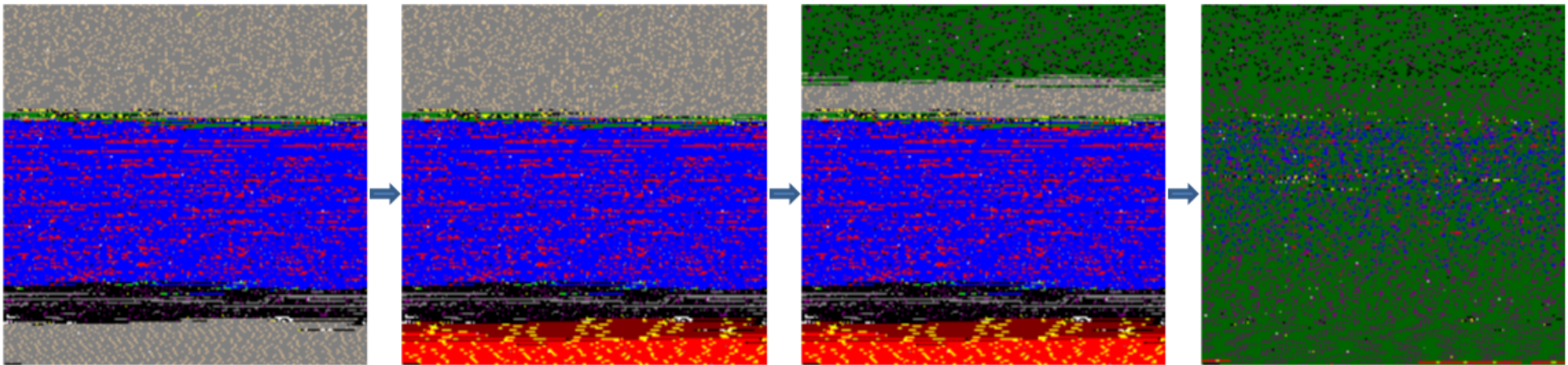
**Number of
Active Rows**

Status	RowID	Data
+	361	NULL 325 Going to our house today 325 1
+	362	NULL 326 Maybe later why 326 1
+	363	NULL 327 Before 3:30 327 1
+	364	NULL 328 Ya 328 1
+	366	NULL 330 Ok 330 1
+	367	NULL 331 Moms walking him hes cranky 331 1
+	368	NULL 332 Ok 332 1
+	379	NULL 343 Will email you a form to sign 343 1
+	380	NULL 344 When ur free call me plz 344 1
+	381	NULL 345 Cancel that...I talked w Tracey 345 1
	...	
+	389	NULL 353 They said it could take six hours 353 1
+	400	NULL 364 Drop car off tomorrow pm. Work on it we
+	401	NULL 365 Ok 365 1
-		1 NULL NULL ..Just let him out before u leave. N

**Internal
RowID**

**Deleted
Row**

Oracle RAM Snapshots



Insider Threats (Log Tampering)

Log File

*T1, DELETE FROM Customer
WHERE City = 'Chicago';*

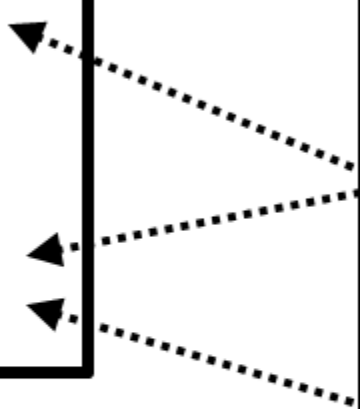
*T2, DELETE FROM Customer
WHERE Name LIKE 'Chris%';*



**UNATTRIBUTED
DELETE**

DBCarver Output

Del. Flag	Page Type: Table Structure: Customer
x	1, Christine, Chicago
✓	2, George, New York
x	3, Christopher, Seattle
x	4, Thomas, Austin
✓	5, Mary, Boston



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