X-Ray Vision for Databases

James Wagner, Alexander Rasin, Karen Heart, Jonathan Grier
CNS Award #1656268

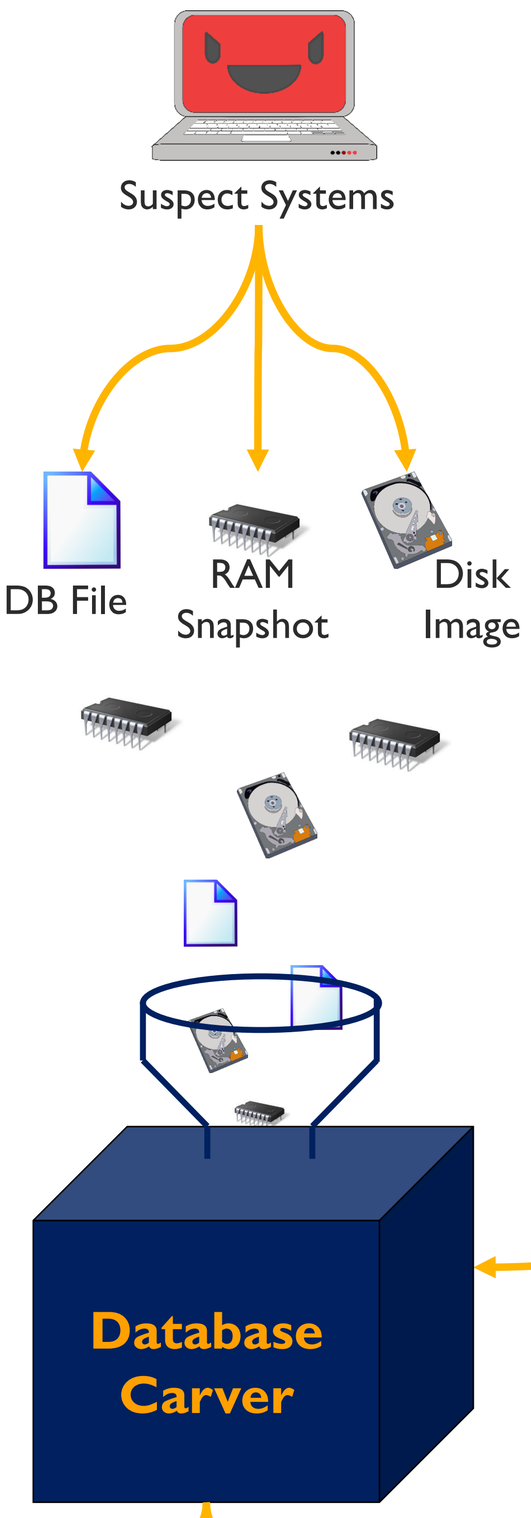
DePaul

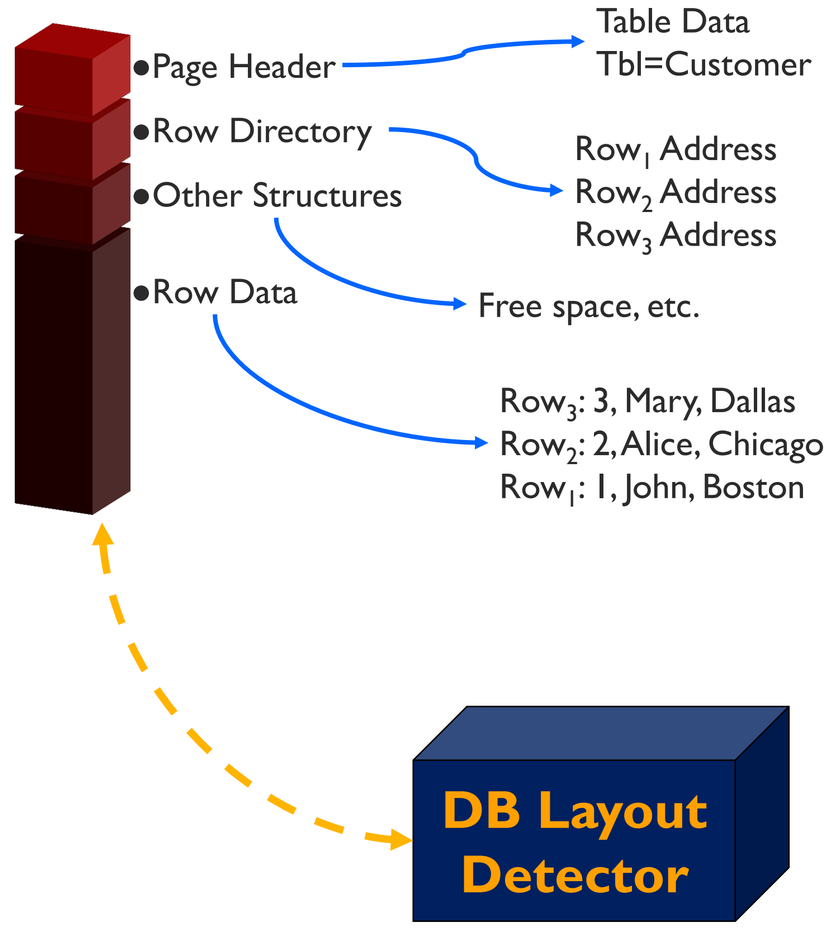
GRIER FORENSICS

Databases Management Systems (DBMSes) Are Everywhere
- Personal Cell Phone Data
- Web Browsers
- Banking Transactions
- Employee Records

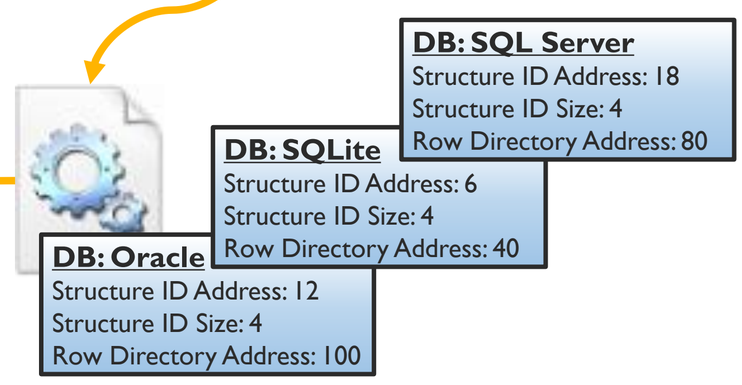
DBMSes in a Digital Investigation
- Incomplete or corrupt storage
- DB file carving
  - not supported by current forensic tools
  - files must still be parsed

Supported DBMSes
- Apache Derby
- DB2
- Firebird
- Maria DB
- MySQL
- Oracle
- PostgreSQL
- SQLite
- SQL Server





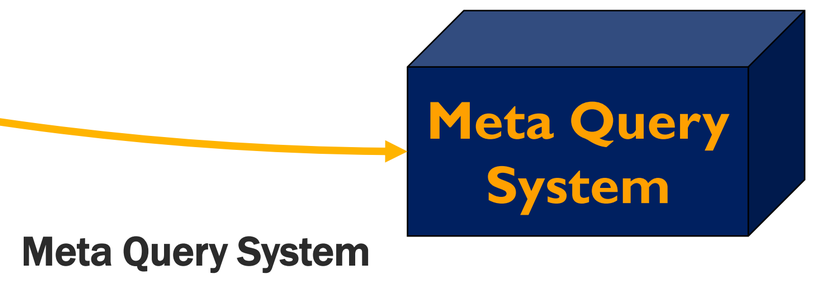
Automated DB Layout Detector
- Deconstructs storage at the page level
- Automates learns storage parameters
- Performed on a trusted system



Parameter File

Database Carver
- Reconstructs database data and meta data using parameters
- A universal data carving tool
- Generalized approach to database forensics

Database Carver Output
- Table data, indexes, materialized views
- Deleted records, tables, and files
- System data and meta data



Meta Query System
- A system for querying reconstructed data
  - query the user data
  - query data not available in original DB
- Ex. Return all deleted Customer records.

DB Carver Output (SQLite on Android)

Active Rows

```
**********************************************************
Page Address: 2726696960|Page Type: Table|Record Cnt: 20
----------------------------------------------------------
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 |34
  +   |   380| NULL|344|When ur free call me plz|344|1
  +   |   381| NULL|345|Cancel that...I talked w Tracey|3
          ...
  +   |   389| NULL|353|They said it could take six hours
  +   |   400| NULL|364|Drop car off tomorrow pm. Work or
  +   |   401| NULL|365|Ok|365|1
  -   |  NULL| NULL|NULL|Just let him out before u leave.
```

Deleted Row

Internal RowID

DB Detective
- Use storage for audit log verification
- Unattributed delete of **record #4** indicates tampering