User authentication in TransbaseCD RDBMS

Research Seminar in Cryptography

September 7, 2016

TransbaseCD RDBMS

TransbaseCD RDBMS

TransbaseCD RDBMS

transbase®
the SQL engine

"Transbase CD is a variant of the SQL database system that stores the database contents in ROM files. These are typically distributed on media like DVDs in large quantities. Transbase CD supports mechanisms for online distribution of partial updates."

`https://www.transaction.de/en/products/technologies/transbase-cd.html`

TransbaseCD RDBMS

transbase®
the SQL engine

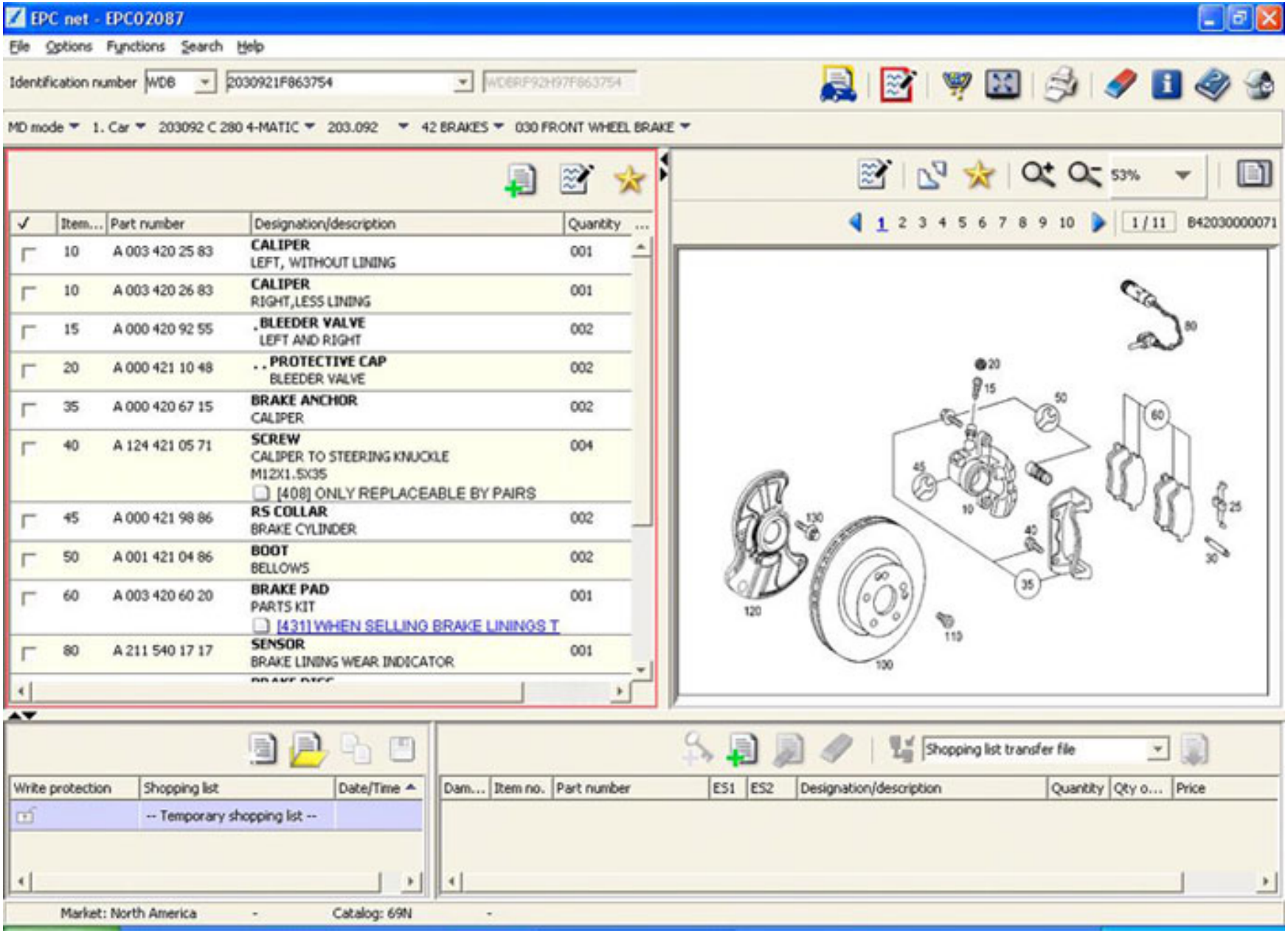
"Transbase CD is a variant of the SQL database system that stores the database contents in ROM files. These are typically distributed on media like DVDs in large quantities. Transbase CD supports mechanisms for online distribution of partial updates."

`https://www.transaction.de/en/products/technologies/transbase-cd.html`

Used by Daimler AG to distribute Service Manuals and Electronic Parts Catalogs to workshops and dealers.

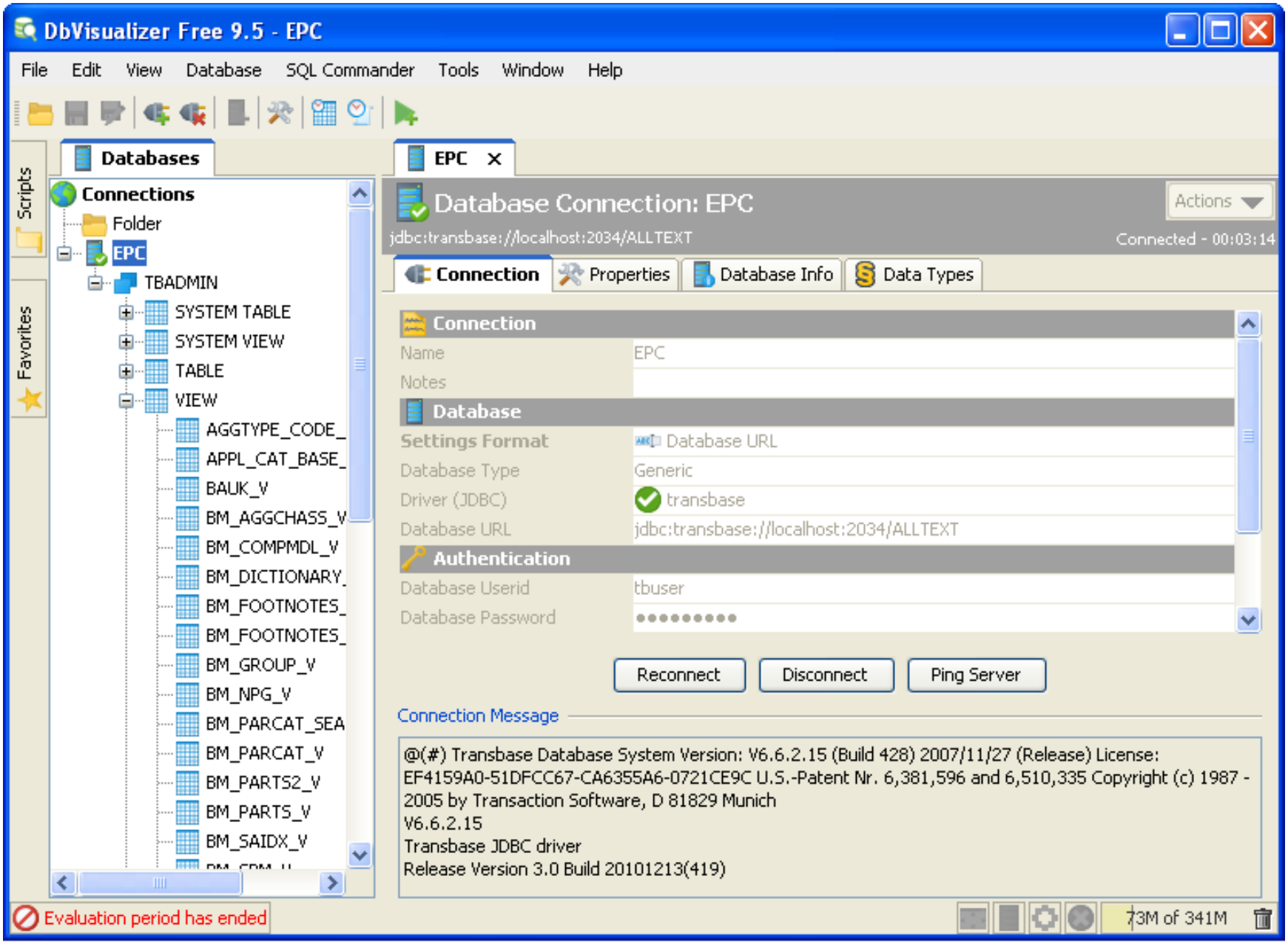
Mercedes-Benz EPC

Mercedes-Benz EPC

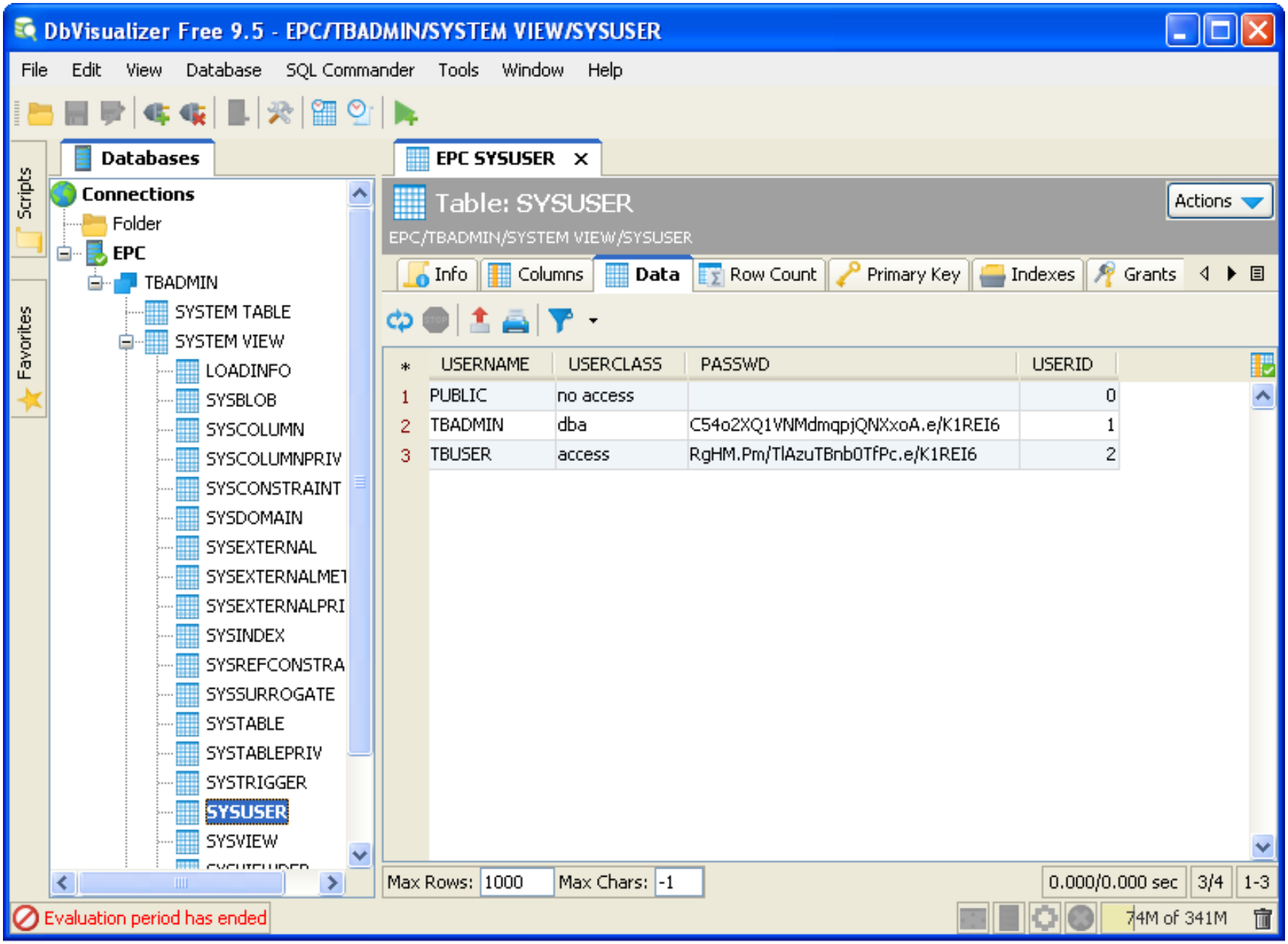


Connecting using JDBC driver

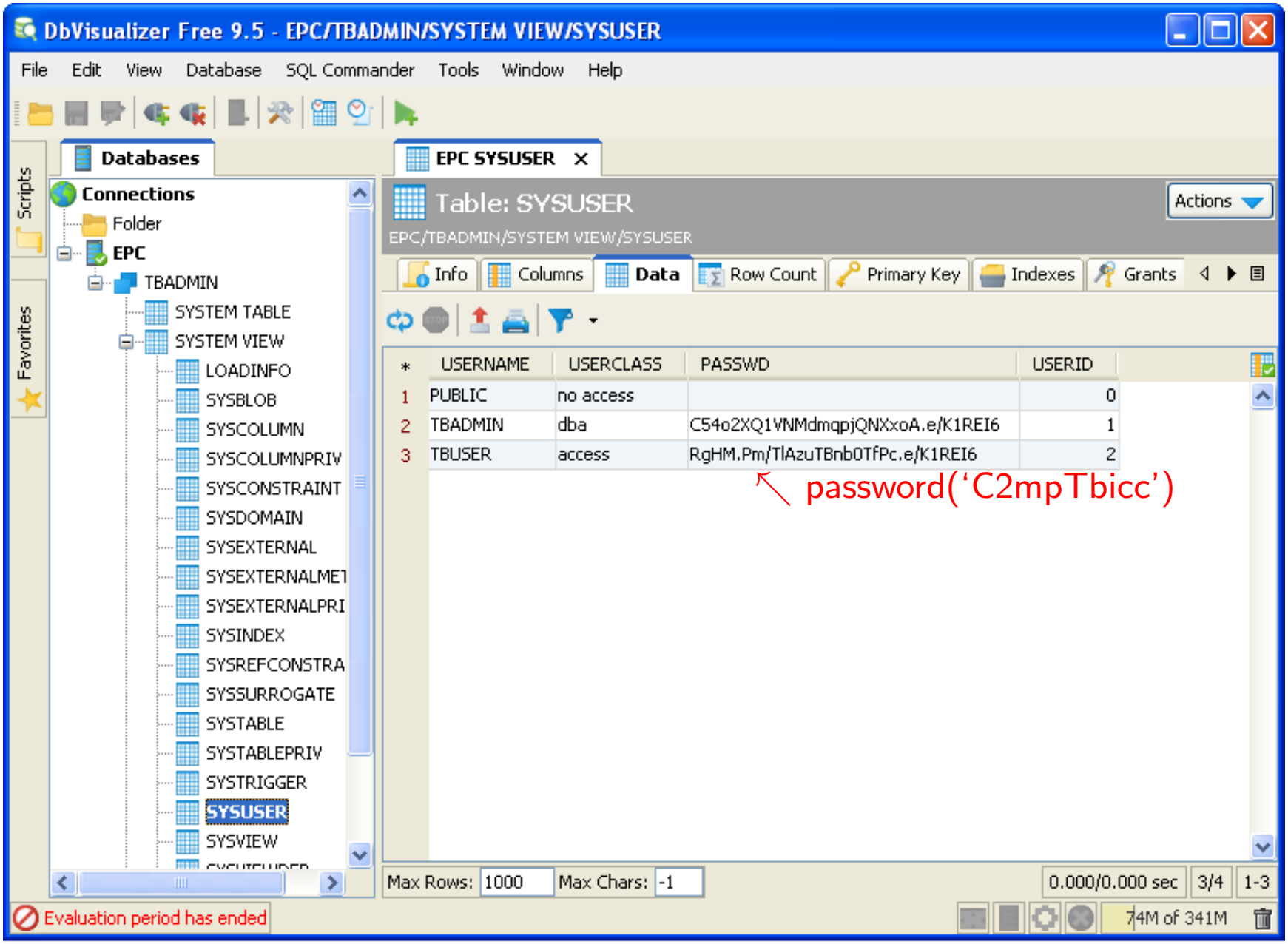
Connecting using JDBC driver



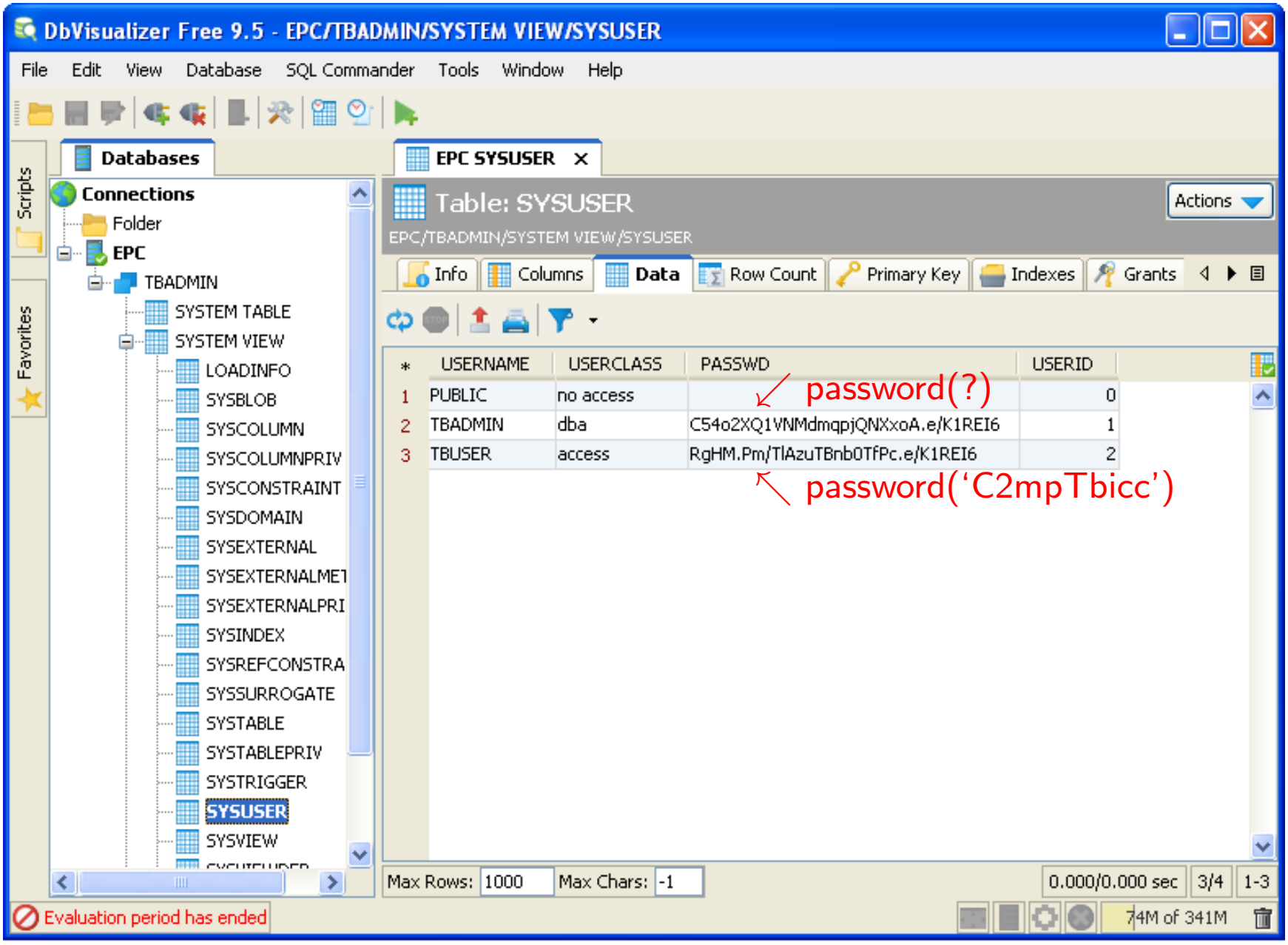
Connecting using JDBC driver



Connecting using JDBC driver



Connecting using JDBC driver



Research questions

Research questions

- How to reset “tbadmin” password having read-write access to database?

Research questions

- How to reset “tbadmin” password having read-write access to database?
  - Such feature officially not documented

Research questions

- How to reset “tbadmin” password having read-write access to database?
  - Such feature officially not documented
  - Requires reverse-engineering password data structure

Research questions

- How to reset “tbadmin” password having read-write access to database?
  - Such feature officially not documented
  - Requires reverse-engineering password data structure
  - Has “tbadmin” wider access to data in the db?

Research questions

- How to reset “tbadmin” password having read-write access to database?
  - Such feature officially not documented
  - Requires reverse-engineering password data structure
  - Has “tbadmin” wider access to data in the db?
- Is it possible to sniff password from db connection?

Research questions

- How to reset “tbadmin” password having read-write access to database?
  - Such feature officially not documented
  - Requires reverse-engineering password data structure
  - Has “tbadmin” wider access to data in the db?
- Is it possible to sniff password from db connection?
  - Reverse-engineer JDBC driver (`tbjdbc.jar`)

Research questions

- How to reset “tbadmin” password having read-write access to database?
  - Such feature officially not documented
  - Requires reverse-engineering password data structure
  - Has “tbadmin” wider access to data in the db?
- Is it possible to sniff password from db connection?
  - Reverse-engineer JDBC driver (`tbjdbc.jar`)
  - Document authentication protocol

Research questions

- How to reset "tbadmin" password having read-write access to database?
  - Such feature officially not documented
  - Requires reverse-engineering password data structure
  - Has "tbadmin" wider access to data in the db?
- Is it possible to sniff password from db connection?
  - Reverse-engineer JDBC driver (`tbjdbc.jar`)
  - Document authentication protocol

Available:

- VirtualBox VM image with Windows XP and TransbaseCD (MB EPC) installed