CRYPTARSI

Encode and query encrypted data sets

Cryptarsi is on Github: http://github.com/bivol/cryptarsi Authors: Delyan Delchev @delian and Atanas Tchobanov @bivolbg

Key features

- Uses AES 256 encryption;
- Javascript implementation;
- User and password never travel in clear text even without https;
- All data is stored and travels encrypted;

Key features

- Encoding is done in the browser (Firefox, Chrome);
- Uses indexedDB for large locally stored data;
- Generates flat text files for web based deployment;
- Supports text, pdf, images and audio files;

Documents

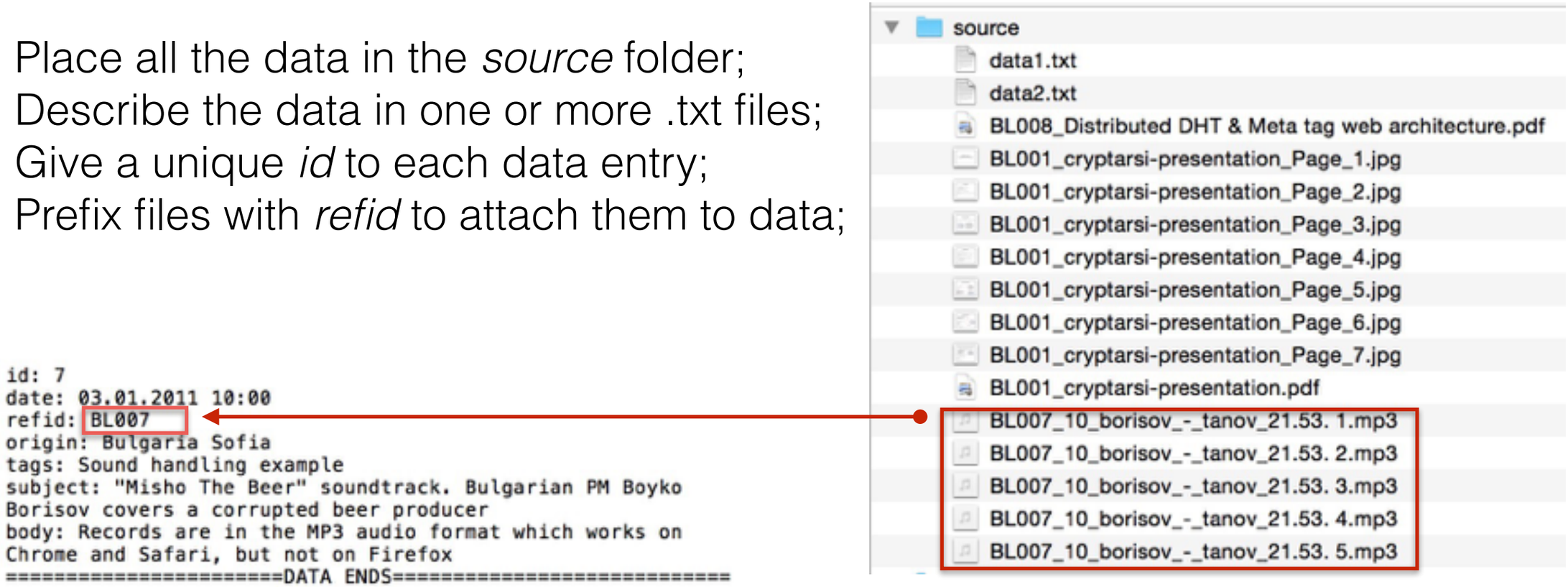
- Cryptarsi accepts UTF8 text documents + attached files;
- Each text document starts with id: UniqueID;
- Each text document ends by ==========DATA ENDS==========
- Many documents can be combined in a single text file.

Attachments

- Attached files types: PNG, JPG, MP3, OGG, PDF;
- The files attached to each document are named RefID_filename;
- Files without RefID prefix are attached to the *Welcome* page;

Prepare your data

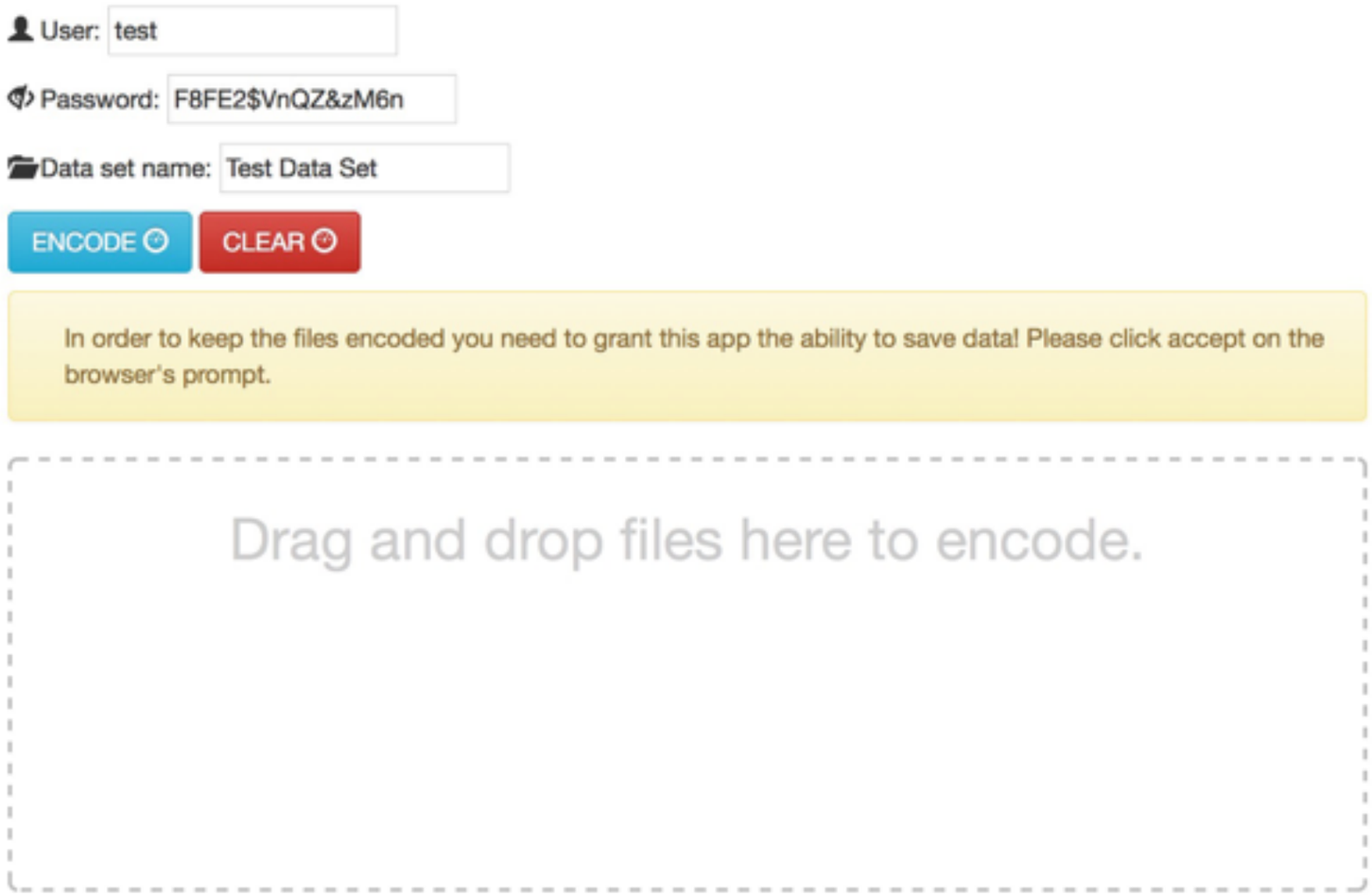
- Place all the data in the *source* folder;
- Describe the data in one or more .txt files;
- Give a unique *id* to each data entry;
- Prefix files with *refid* to attach them to data;



- Text description will be indexed and searchable. Make it precise and detailed;
- Files without prefix are attached to the *Welcome* page;
- PDF, JPG, PNG, MP3 and OGG files accepted;

Cryptarsi is on Github: http://github.com/bivol/cryptarsi Authors: Delyan Delchev @delian and Atanas Tchobanov @bivolbg

Encode your data



- Open the encoding page;
- Enter the username, a **complex password** and the data set name;
- Drag and drop files from the *source* directory;

Cryptarsi is on Github: http://github.com/bivol/cryptarsi Authors: Delyan Delchev @delian and Atanas Tchobanov @bivolbg

The query process

- Data is indexed;
- Data and indexes are encrypted with user/pass and stored locally;
- Query words are encrypted with user/pass;
- For each query word the encrypted index file is retrieved and decrypted in RAM;
- Data files found in the index file are retrieved and decrypted in RAM;
- Cross set search is operated in decrypted data text for complex queries (ex: +word1 +word2 -word3);

Cryptarsi is on Github: http://github.com/bivol/cryptarsi Authors: Delyan Delchev @delian and Atanas Tchobanov @bivolbg

Case studies

- Personal encrypted storage of sensitive data;
- Share copies of encrypted, searchable data set;
- Web deployment for cooperative work on large encrypted data sets;