Problem Statement

- All search tools allow searching by regular expression
  - Advanced search string syntax is hard, getting it right is harder
- No sharing of search terms among LE investigators
  - E.g. each investigator must come up with common terms for drugs, child porn, etc. on their own.

Solution

- Automated generation and testing of regular expressions
- LE Repository of search expressions
  - Searchable repository
  - Allow for comments on effectiveness of search terms
- Integrate into existing LE tools
  - EnCase, FTK, X-Ways, and others

Regular Expression Generator

- Browse and search for regular expressions
- Generate regular expressions with LESSA RegEx Generator
  - Create regular expressions for EnCase and FTK
  - Generate sample strings or use your own strings for testing

Keyword Lists

- Browse and search for keywords
- Share keywords by adding to lists or creating new lists
- Vote and comment on effectiveness of keywords

Export into Existing Tools

- Regular expressions and keywords can be downloaded and imported into existing tools
  - EnCase
  - FTK
  - X-Ways

Impact

- LE has a resource for search strings
  - RegEx Generator makes it easy to create regular expressions
  - Keyword repository allows LE to share and rate keywords
- Hosted on Electronic Crime Technology Center of Excellence website
  - www.ectcoe.net

Research sponsored by the National Institute of Justice