Bulk Extractor Viewer (*BEViewer*) Summary

June 7, 2012

1 The Main *BEViewer* Screen

A sample *BEViewer* screenshot showing a navigated Feature is shown in Figure 1.

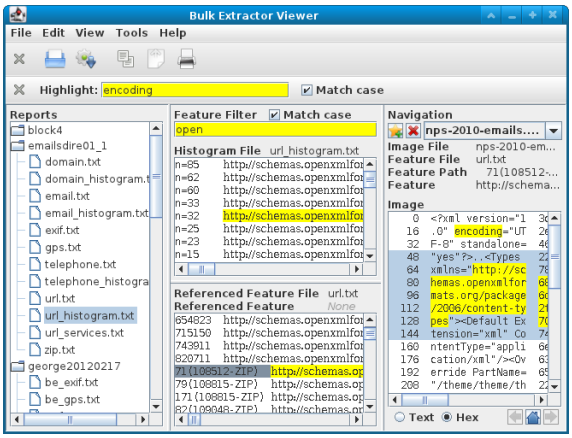

Figure 1: Sample *BEViewer* screenshot.

A blank *BEViewer* screenshot with areas labeled is shown in Figure 2.

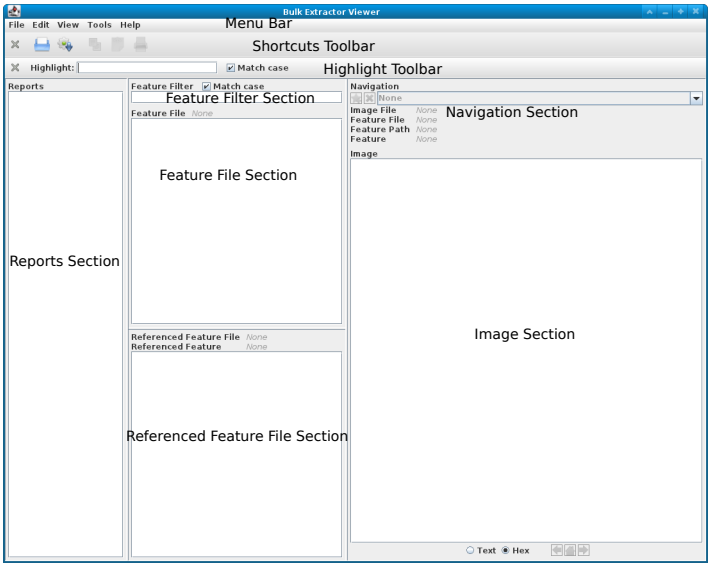

Figure 2: Blank *BEViewer* screenshot with sections annotated.

The main *BEViewer* screen is described in sections:

1.1 Menu Bar

Menus provide controls for *BEViewer* such as opening Reports, managing Bookmarks, copying ranges, configuring views, and running *bulk_extractor*:

- Use `File` to manage Reports, Bookmarks, and Work Settings, and to print or quit.
- Use `Edit` to Copy and to clear the Navigation history.
- Use `View` to set view parameters and to view properties.
- Use `Tools` to run *bulk_extractor*.
- Use `Help` for Help, version information, logs, and diagnostics.

1.2 Shortcuts Toolbar

The Shortcuts toolbar provides the following shortcuts:

- Open Report for browsing its Features.
- Run *bulk_extractor* to scan an Image and create Feature files containing Features from that Image.
- Copy a range of Features or a range of Image lines that have been selected by dragging the mouse over them.
- Export bookmarks to a file.
- Print the selected Feature range or Image range.

1.3 Highlight Toolbar

The Highlight toolbar allows typed text to be highlighted in the Feature and Image areas:

- Highlights show up in the Feature File listings and in the Image listing.
- Multple highlights may be issued by separating them with the | character.
- Unusual characters may be highlighted by entering their escaped octal sequences, for example `\000`.
- Click the Match case checkbox to match capitalization.

1.4 Reports Section

The Reports section is used to select Feature files from an opened Report.

- Hover over a Report folder to see the Report directory and the Image file associated with the Report.
- Hover over a Feature file or Histogram file to see the full path to it.
  - Feature files contain feature entries organized by filename.
  - Feature filenames ending in `_histogram.txt` contain histogram information.
  - Empty files and Stoplist files may be suppressed or shown.
- Click on a Report folder to see the Feature files within it.
- Click on a Feature file to view the Features within it.
- Click on a Histogram file to view the histogram entries in the Histogram listing and view the associated Feature file in the Referenced Feature file listing.
- When a folder or file is selected, you may use menu action `File | Close Report` to close it.

1.5 Feature Filter Section

The Feature Filter filters what Features are shown in the Feature file or Histogram file area.

- Type text to apply a filter.
- Click the Match case checkbox to match capitalization.

1.6 Feature File Section

If a Feature file is selected in the Reports section then its features are displayed:

- Click on a Feature to navigate to it.
- Drag on a range to select the range.
- Press the Escape key to deselect the range.

If a Histogram file is selected in the Reports section then the histogram entries associated with the Histogram file are displayed:

- Click on a Histogram entry to display the Features associated with this Histogram entry in the Referenced Feature File section.
- Press the Escape key to deselect the Histogram entry. Note that the Referenced Feature File section goes back to displaying all features instead of displaying the associated ones.
- Drag on a range to select the range.
- Press the Escape key to deselect the range.

Additionally:

- Type filter text to filter the set of features that are displayed.
- Type highlight text to highlight specific features.

1.7 Referenced Feature File Section

The Referenced Feature File section is only used when a Histogram file is selected in the Reports section. The Referenced Feature file shown is the Feature file corresponding to the Histogram file selected.

- Click on a Feature to navigate to it.
- Drag on a range to select the range.
- Press the Escape key to deselect the range.

The set of features displayed in the Referenced Feature File listing depends on whether a histogram entry is selected in the Histogram area:

- If no histogram is selected, all feature entries are shown in the Referenced Feature File listing.
- If a histogram entry is selected, only features matching that of the histogram entry are shown in the Referenced Feature File listing.

1.8 Navigation Section

The Navigation section controls which Feature is currently navigated to.

- Click the Bookmark button to bookmark the Feature that is currently navigated to.
- Click the Delete button to deselect the Feature that is currently navigated to and to delete it from the Navigation list.
- Select another feature in the Navigation list to navigate to that feature.
- The Image File, Feature File, Feature Path, and Feature labels indicate attributes about the feature that is currently navigated to.

1.9 Image Section

The Image section displays a page of the image associated with the feature that is currently navigated to.

- Drag on a range to select the range.
- Press the Escape key to deselect the range.
- Press the Text or Hex button to view the image as text or as hexadecimal bytes.
- Press the Forward, Reverse, and Home buttons to page forward and back in the image data.

1.10 Sample *BEViewer* Screenshot Explained

The sample screenshot shown in Figure 1 has the following going on:

1.10.1 Shortcuts Toolbar

The Shortcuts toolbar indicates the following:

- More Reports can be opened for browsing.
- The *bulk_extractor* scanner can be run.
- A range selection has been made in the Image section that may be copied to the System Clipboard.
- Features have been bookmarked and these bookmarks can be exported.
- A range selection has been made in the Image section that may be printed.

1.10.2 Highlight Toolbar

Highlighting is in effect because there is text, in this case `encoding`, in the highlight field.

- Highlighting is not shown in either Feature listing because the word `encoding` is not present in either of them.
- Highlighting is shown in the Image view.
- The highlighting case is set so that capitalization must match.

1.10.3 Reports Section

The Reports section indicates the following:

- Three reports are visible in the Reports tree, two of which are expanded.
- Within the `emailsdire01_1` Report, histogram feature file `url_histogram.txt` is selected.

1.10.4 Feature Filter Section

Feature filtering is in effect because there is text, in this case `open`, in the filter field.

- Feature filtering filters the features shown in the Feature File listing or the Histogram file listing.
- Feature filtering does not filter features shown in the Referenced Feature File listing.
- The filtering case is set so that capitalization must match.

1.10.5 Feature File Section

- In this example, the Feature File section contains features from Histogram file `url_histogram.txt` selected from the Reports pane.
- Only features containing text `open` are shown because the Feature File section is being filtered.
- No histogram entry is selected.
- One histogram entry is highlighted because it matches the feature that is selected in the Referenced Feature File area.

1.10.6 Referenced Feature File Section

- Referenced Feature file `url.txt` is shown because Histogram file `url_histogram.txt` is selected in the Reports section.
- The Feature at path `71(108512-ZIP)` is selected. As a result:
  - The feature is selected.
  - The feature's text is highlighted in the Feature File section, the Referenced Feature File section, and in the Image section.

1.10.7 Navigation Section

The Navigation section shows that a feature has been navigated to.

- The Navigation History drop-down box shows the feature that is navigated to.
- Navigation attributes indicate the Image file, Feature file, Feature path, and Feature text associated with the feature that is navigated to.

1.10.8 Image Section

- The Image section displays the page of image data corresponding to the selected Feature.
- A range of rows is selected and it may be copied to the System Clipboard or printed.
- Text `encoding` is highlighted as requested in the Highlight Toolbar.
- Feature text is highlighted because it is selected.
- A hexadecimal view of the image is displayed because the Hex view is selected as opposed to the Text view.
- Forward and back buttons are disabled because they are not useful: the un-zipped content at this path all fits on one page.

2 *BEViewer* Facilities

2.1 Generating Reports

bulk_extractor creates a report of features by running scanners on media images. A Report consists of:

- The directory containing the report.
- The `report.xml` text file that *bulk_extractor* creates when performing the scan.
- Text files, ending in `.txt`, containing features found during the *bulk_extractor* scan:
  - Feature files.
  - Histogram files generated from feature files, typically containing `_histogram` in their filename.
  - Stoplist files, if a stoplist is used, which contain features that have been excluded from the feature files. These end in `_stoplist.txt`.

Generate Reports by running the *bulk_extractor* scanner one of these ways:

- Click on the Run *bulk_extractor* button.
- Run *bulk_extractor* outside of *BEViewer* at the command prompt.
- Run *bulk_extractor* automatically when starting *BEViewer* by starting *BEViewer* using the `-r` option.

2.2 Managing Reports

BEViewer displays Features in Reports created by running the *bulk_extractor* scanner. Reports must be opened so that *BEViewer* can view their Features.

- Open Reports that have been created by *bulk_extractor*.
- Reports are opened automatically when they are created by running *bulk_extractor* from *BEViewer*.
- Close Reports to remove them from the Reports listing and from any Navigation history.

2.3 Bookmarks

Features may be bookmarked.

- Bookmarks are made by clicking on the Bookmark button.
- Bookmarked features may be exported to a file. Bookmark files show properties of bookmarked features along with their corresponding Image data.

2.4 Feature Formats

Features are extracted from their native encodings in the image. For example:

- Email addresses are often found in binary format or in UTF-16 format.
- IP addresses are obtained from specific bytes where surrounding bytes match an identifying pattern.

bulk_extractor scanners find these features, extract them, format them according to their type, then write them to their corresponding Feature file where they can be viewed directly, imported into Excel, or accessed by Python scripts and by *bulk_extractor*.

bulk_extractor formats features from Feature files based on their feature type for the following purposes:

- *bulk_extractor* reformats feature contents so that features may be displayed as a summary on one line.
- *bulk_extractor* creates a highlight template so that image bytes that map to features may be highlighted.

2.5 Highlighting

Highlighting in *BEViewer* comes from two sources:

- Text typed in the Highlighting Toolbar.
- Feature content associated with the currently selected feature.
  - For Feature views, feature highlighting consists of the formatted feature text.
  - For the Image view, feature highlighting is based on the highlighting template corresponding to the feature type.

Highlighting shows up in three places:

- The Feature File area.
- The Referenced Feature File area.

- The Image area.

To support highlighting of unusual characters and bytes, highlighting may be entered using escaped octal sequences, for example `\000`.

2.6 Work Settings

Work settings contain setting information about what Reports are currently opened and what Bookmarks are currently selected. Work settings allow you to add saved information to your work settings or to move them to another computer.

- Export Work Settings to a file.
- Import Work Settings from a file, augmenting existing work settings.
- Import Work Settings from a file, replacing existing work settings.

2.7 Clipboard

Copy information to the System Clipboard so that it may be pasted elsewhere.

- Copy a Feature, Histogram, or Image range selection.
- Copy the *BEViewer* runtime log so that it can be pasted into a failure report.

2.8 Printing Output

Print a feature or image range selection:

- Select a range and then click on the Print button to print the range.
- Press the Escape key to deselect the range.

2.9 Command-line Usage

BEViewer accepts input parameters when it is started from the command line:

- Type `-s "<scanner arguments>"`, quotes included, to start the *bulk_extractor* scanner with scanner arguments that are provided to *bulk_extractor*.
- Type `-clear_preferences` to reset all user preferences saved previously by *BEViewer*.