EnCase Timeline Report EnScript
This script gathers file information on all or selected files/folders and presents it in a timeline view. The user can select the timeframe to check and output either HTML or tab-delimited text format. The script checks Created, Modified, and Accessed times and puts files in order according to these fields. If a file was both Created and Accessed during the specified time period, the file will be listed twice, once with Created highlighted and once with Accessed highlighted.

Distribute to anyone who would like a copy, but make sure bug reports come directly to me so it can be fixed for everyone.

REQUIREMENTS
-EnCase Version 6.8.1 and above

-For Records output – 6.5+

-Please overwrite all files from previous script versions or use the EnPack

Known issues
If opening tab delimited file in Excel (tested in v2003), Excel clips the "seconds" field by default from the time display and the column must be formatted to include this. Recommended format is 'yyyy-mm-dd hh:mm:ss', 'mm/dd/yyyy hh:mm:ss', or similar depending on your viewing preference.

If copying text from the HTML view, use the IE version, as the zero width space character from the FireFox version will be copied as a character even though it is not visible.

Options
- **Start Date** - the beginning (minimum) date and time to check, typically entered in the format "mm/dd/yy hh:mm:ss" (no quotes) e.g. "07/13/05 10:30:11"

- **Stop Date** - the ending (maximum) date and time to check, typically entered in the format "mm/dd/yy hh:mm:ss" (no quotes) e.g. "07/14/05 10:30:11"

- **Investigator Name** - Enter your name here to add to the document heading e.g. "Joe Q. Investigator"

- **Title of Report** - Enter the report title here to add to the document heading e.g. "EnCase Timeline Report for Case 1234"

- **Output Path** - Enter a directory / folder name to send the output to, default is your case Export folder plus "\TimelineReport", if the folder exists, the script automatically renames to "\TimelineReport - 1", "\TimelineReport - 2", etc. e.g. "C:\Case1234\Export\TimelineReport"

- **Create Records** - Only available in version 6.5 and higher. Creates records in the Records View of EnCase 6. (Beta feature)

- **Create Bookmarks** - Bookmarks all entries that match the selected time range in order (as selected by sort settings). This will not bookmark any entry that does not have a Starting Extent (EnCase is incapable of performing this function), though those entries will show up in text and HTML output. A nice side effect of this output option is being able to

blue check all bookmarks, right click, and choose "Tag Selected Files" to immediately view the files in question within EnCase.
Checked by default

- **Create TSV report** - Outputs a tab delimited format text file with the extension .xls
  Checked by default

  - o Text Options
    - ▪ **Entries per file** – Maximum number of entries allowed in an output file before that file will be closed and a new one opened to continue the output
      65500 by default

- **Create HTML Report** - Outputs an HTML format document and a CSS stylesheet
  Checked by default

  - o HTML Options
    - ▪ **Version for IE** - Outputs an HTML file not including HTML v4 code ​(zero width space). IE incorrectly interprets ​ and displays a square box character instead. IE version output will usually require horizontal scrolling to view all fields.
      Checked by default

    - ▪ **Version for FireFox** - Outputs an HTML file replacing every backslash character "\" with "\​". The zero width space character allows Firefox to properly break the line and wrap to the next line without introducing a visible space.
      Checked by default

    - ▪ **Entries per file** – Maximum number of entries allowed in an output file before that file will be closed and a new one opened to continue the output
      10000 by default

- **Include current time in heading?** - Adds the date and time that the script is executed to the output heading
  Checked by default

- **Include criteria in heading?** - Adds the Start Date and Stop Date to the output heading
  Checked by default

- **Sort Order**
  - o **Ascending** - Sorts output with minimum / lowest / oldest date first (top) and maximum / highest / most recent date last (bottom
    Selected by default

  - o **Descending** - Sorts output with maximum / highest / most recent date first (top) and minimum / lowest / oldest date last (bottom)
    Not selected by default

- **Check only selected files?** - This will only check the files/folders you have selected for dates in range instead of checking the whole case
  Not checked by default

- **Time Options**
  - o **Check Created time?** - Will include Created dates/times in report
    Checked by default

  - o **Check Written time?** - Will include last Written (AKA Modified) dates/times in report
    Checked by default

  - o **Check Accessed time?** - Will include last Accessed dates/times in report
    Checked by default

  - o **Check Entry Modified time?** - Will include the entry modified dates/times in report
    Not checked by default

  - o **Check Deleted time?** - Will include the Recycle Bin records deleted dates/times in report
    Checked by default

- **Output Fields** – Select the list of fields you would like to appear in the report. Applies <u>only</u> to the tab-separated values (TSV) text output.

  - o **UP** – Moves the currently selected field up in the output list

  - o **DN** – Moves the currently selected field down in the output list

Geoff Black, EnCE
geoff@geoffblack.com
http://www.geoffblack.com/forensics