History

v1.1.0

- Swapped the MIME parser from OpenPop to a slightly modified version of MimeKit (MimeKitLite). This allows for the correct differentiation between in-line parts (e.g. images, PGP sigs) and true attachments
- Modified the data storage to use Alternate Data Streams (ADS) so that all of the different output data can be stored in one file per session
- Added Session and and Packet parser interfaces e.g. HTTP and DNS so far
- Added Processor interface e.g. SMTP
- Added logging using NLog and this.Log libraries
- Added logging to all exception handlers
- Fixed bug where if only one item showing in list, then you cannot select it to view session details
- Updated the TCP session parsing code using the current Wireshark code (epan/follow.c). This identified 4 bugs introduced in the porting.
- Fixed bug in the import window which resulted in databases that were appended to without warning the user
- Fixed bug where the new sessions were not displayed if multiple imports were performed without restarting the application
- Changed HTML parser from HtmlAgilityPack to AngleSharp
- Changed the GZIP decoder from DotNetZip to the MS one due to it being poorly implemented compared to the latest MS version
- Modified the session processing to be multi-threaded
- Implemented multi-threaded session parsing
- Modified the SMTP output so that the CSV is correctly formed when there are multiple recipients
- Added new SMTP output that shows the recipients associated with a particular MD5 hash and subject
- Removed the Ionic zip file library and replaced with System.IO.Compression.FileSystem
- Modified the SMTP processing so that all unzipped files have ".safe" appended to the filename to prevent accidental execution. Thanks DannyF
- Modified the SMTP processing so that the email addresses from the TO parts
- Modified the SMTP CSV to include a header
- Added option to manually perform GZIP decoding so that specific sessions can be decoded when the HTTP parser has been turned off. This will also parse the HTTP Host header and all of the HTTP methods called in the TCP session, the parsed data will then be displayed in the list.
- Add HTTP file extractor which uses file signatures to determine what should be extracted out (zip, exe, gz, doc, xls, docx, xlsx, pdf, rar, winzip)
- Remove the gzip header if we process it using the HTTP session processor else it will error the next time around
- Outputs the start timestamp, end timestamp and number of packets processed to the output directory (Log.txt)
- Moved the URL export to a new URL extractor

v1.0.10

- Added the Date field from the MIME parsing to the various output files
- Fixed an bug where the *.urls files might not exist. Thanks CalG

v1.0.9

- Added SMTP MIME parsing. Use the Processors->SMTP menu item to run.

v1.0.8

- Modified the HTTP request regex to match URL's starting with a fully qualified host name e.g. "http://www.blah.com/index.html" rather than "/index.html"
- Modified the HTTP response regex to match response descriptions that contain a space e.g. 404 NOT FOUND
- Added HTML "A HREF" tag matching and extracting
- Move all HTTP parsing from the packet level parser to the session parser, so in theory it should be quicker
- Modified the HTTP parsing so that it stores an MD5 of the parsed data e.g. link, URL etc, which is then used to ensure that no duplicates are output
- Modified the HTTP method regex to support CONNECT methods
- Modified the HTTP method regex to support URL's that begin with https://

v1.0.7

- Added export all of the extracted URLS. The export will also export a uniqued list of URL's. Use the File->Export->URL's menu item

v1.0.6

- Updated the HEX and HTML display's so that an extra line break is added when the sessions traffic changes direction, so that there is clear delineation between the traffic directions
- Added URL parsing. All URL's are extracted from HTTP sessions and are displayed on the new URL's tab
- Fixed a potential null object exception when changing the options
- Updated the error handling to log errors to the users local AppData directory for the application rather than the application directory

v1.0.5

- Regressed the Winpcap dependencies from 4.1.2980 to 4.1.0.2100

v1.0.4

- Modified the HTTP header regexes to deal with HTTP servers that don't put spaces after the Host header name
- Modified to allow the user to disable the HTTP parsing during processing. Use the toolbar button to set
- Modified to stop processing sessions after a user configurable session size. Use the toolbar drop down.
- Modified allow the processing of only sessions that are from IP's (both source and destination) that are not in the RFC 1918 private ranges e.g. remote connections. Use the toolbar button to set
- Added Geo IP locations using the MaxMind GeoLite data (http://www.maxmind.com)
- Updated the session reconstruction code from the wireshark code e.g. /epan/follow.c
- Updated Winpcap dependencies from 4.1.0.2100 to 4.1.2980
- Removed the protobuf storage to increase the processing speed
- Modified to process the FIN packets from a TCP session so that sessions can be completed earlier

v1.0.3

- Added more user feedback whilst the parsing starts up
- Changed the thread invoking from Task.Factory.StartNew to new Thread since it seems to hang on servers
- Corrected the installer to include the missing Winpcap binaries
- Added HTTP method parsing
- Added ability to extract unique source/destination IP addresses. Accessed via context menu
- Added automatic gzip decoding to HTTP requests. This can be disabled via the settings
- Added the ability to export the base HEX for a session
- Modified the file storage to use protobufs so one file is created per session rather than the 3 previously
- Fixed the Q/A key events as they didn't work when the data is sorted by a column

v1.0.2

- Removed awesomium for HTML display

v1.0.1

- Modified the database creation to prevent file locking, which can stop the creation of subsequent databases during a continuous run of the application
- Moved the database deletion/creation to the Parser object e.g. background thread
- Moved the SQL CE database access from PetaPoco to NPoco
- Update awesomium to v1.7.0.5
- Modified the key presses so that the selected session is always in view
- Parses out the Host header for display on main list

v1.0.0

- Added Size column to list view
- Loading of session data now occurs on a background thread

v0.0.1

- Initial release