



# SessionViewer

## About

woanware is the name for a set of tools and applications I have written. The majority of the tools/applications are related to networking, network security, application security or digital forensic tasks.

## **Introduction**

## History

### 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