

The importance of Network Forensics tools are increasing as the cyber crimes related to computer network are increasing at a rapid rate. Network Session Analyser (NeSA) is a network forensics tool for analysing network packets. NeSA accepts packet dump file in the **pcap** format, generated using any third party packet capturing tool.

To help the novice users, an easy filter expression building facility is added. Time zone based analysis is incorporated into NeSA to make it capable of analysing dumps collected from different time zones. Rebuilt files can be exported for future references. It has a good Hex Viewer which also indicates the data communication direction using different colours.

Regular expression based search is available to locate the evidence and evidence related items. The analysis state of a file can be saved and the analysis can be resumed from that point at a later time.

Features

- Loads pcap formatted dump files and rebuilds TCP sessions
- Extracts files from HTTP, FTP, SMTP and POP3 protocols
- Built in Hex View, Thumbnail View, File View and Mail View
- Powerful filter for filtering TCP sessions as well as packets
- Regular expression based search capability
- Supports port customisation based on Application layer protocol
- Time Zone can be changed for Time Zone based Analysis