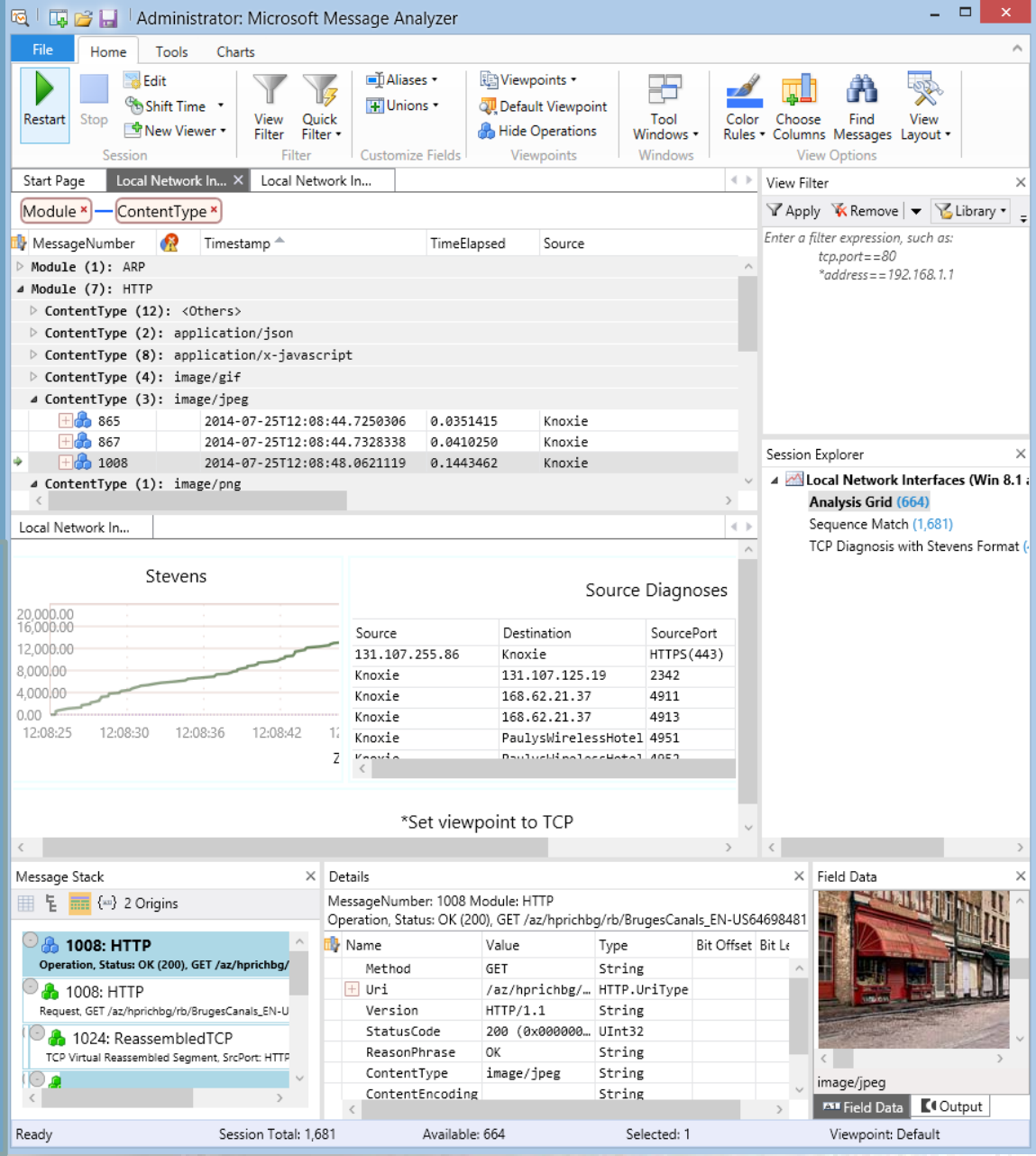
SDC
STORAGE DEVELOPER CONFERENCE
SNIA ■ SANTA CLARA, 2014

Evolution of Message Analyzer and Windows Interoperability

Paul Long
Microsoft

What is Message Analyzer?

blogs.technet.com/MessageAnalyzer

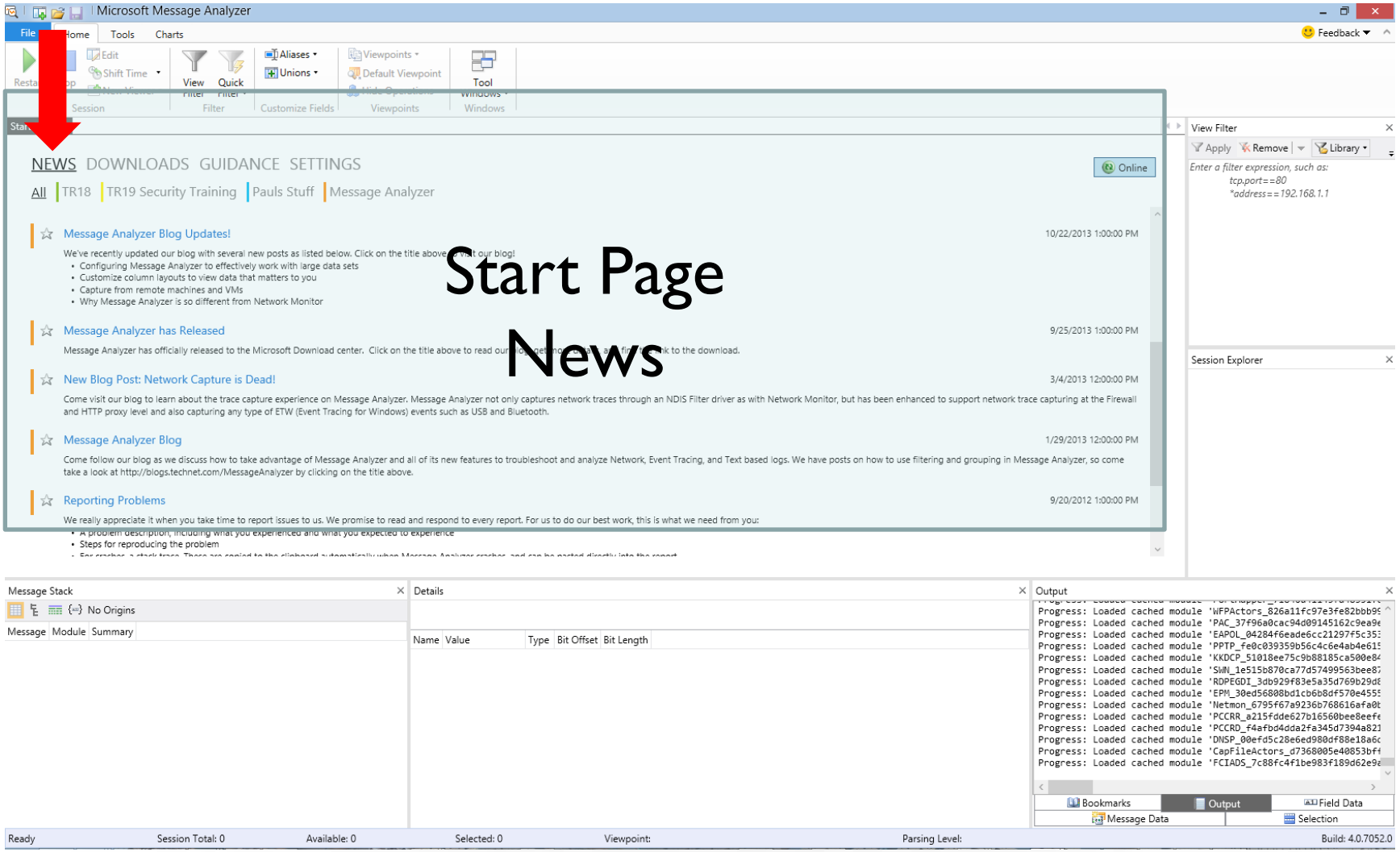


Usual Suspects

What is Message Analyzer

- Protocol and Log File Analysis Tool
  - Correlation across traces and logs
  - Visualize Data
- Trace Collection Tool
  - Remote and Local
  - ETW events

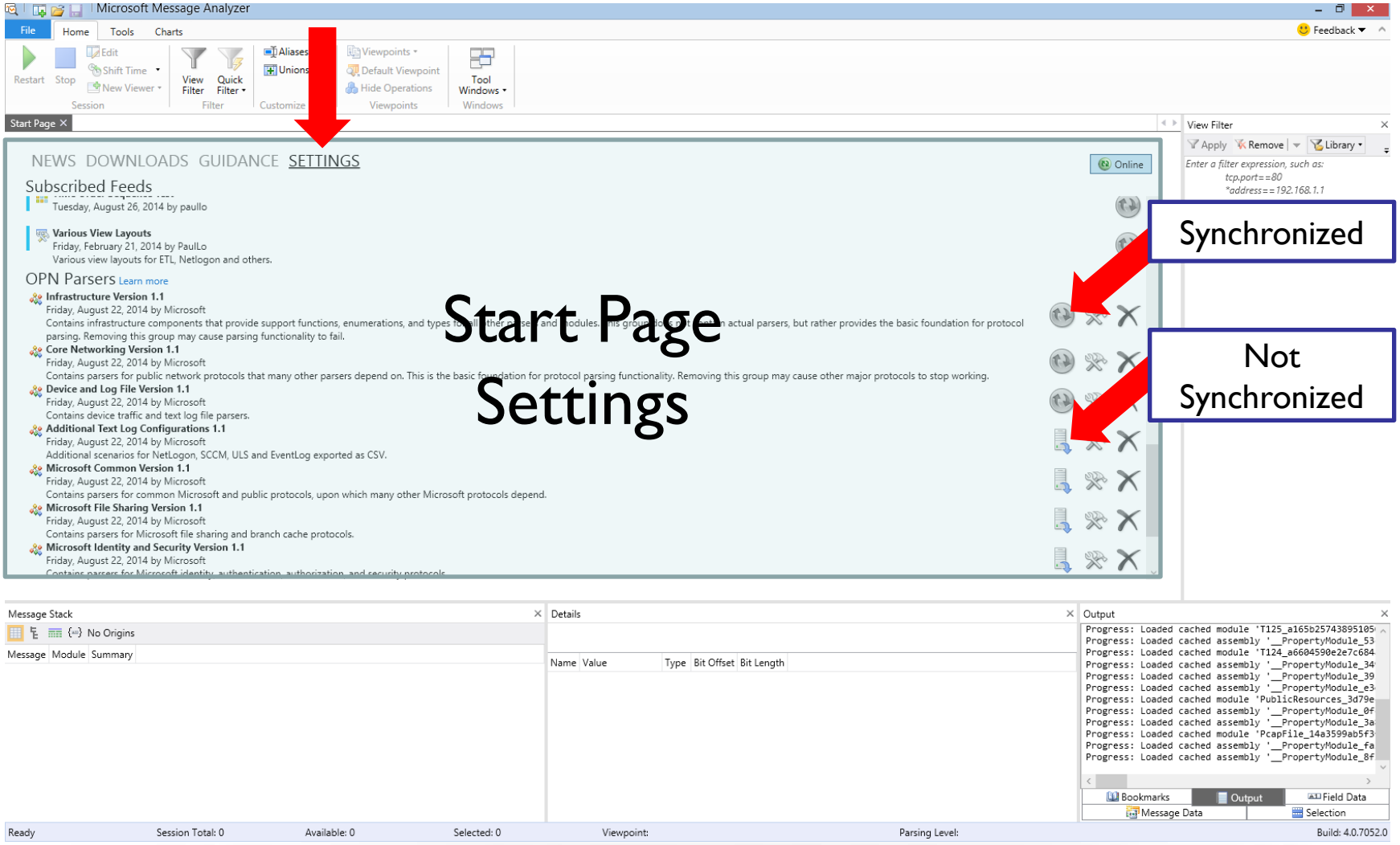
Demo: A quick tour



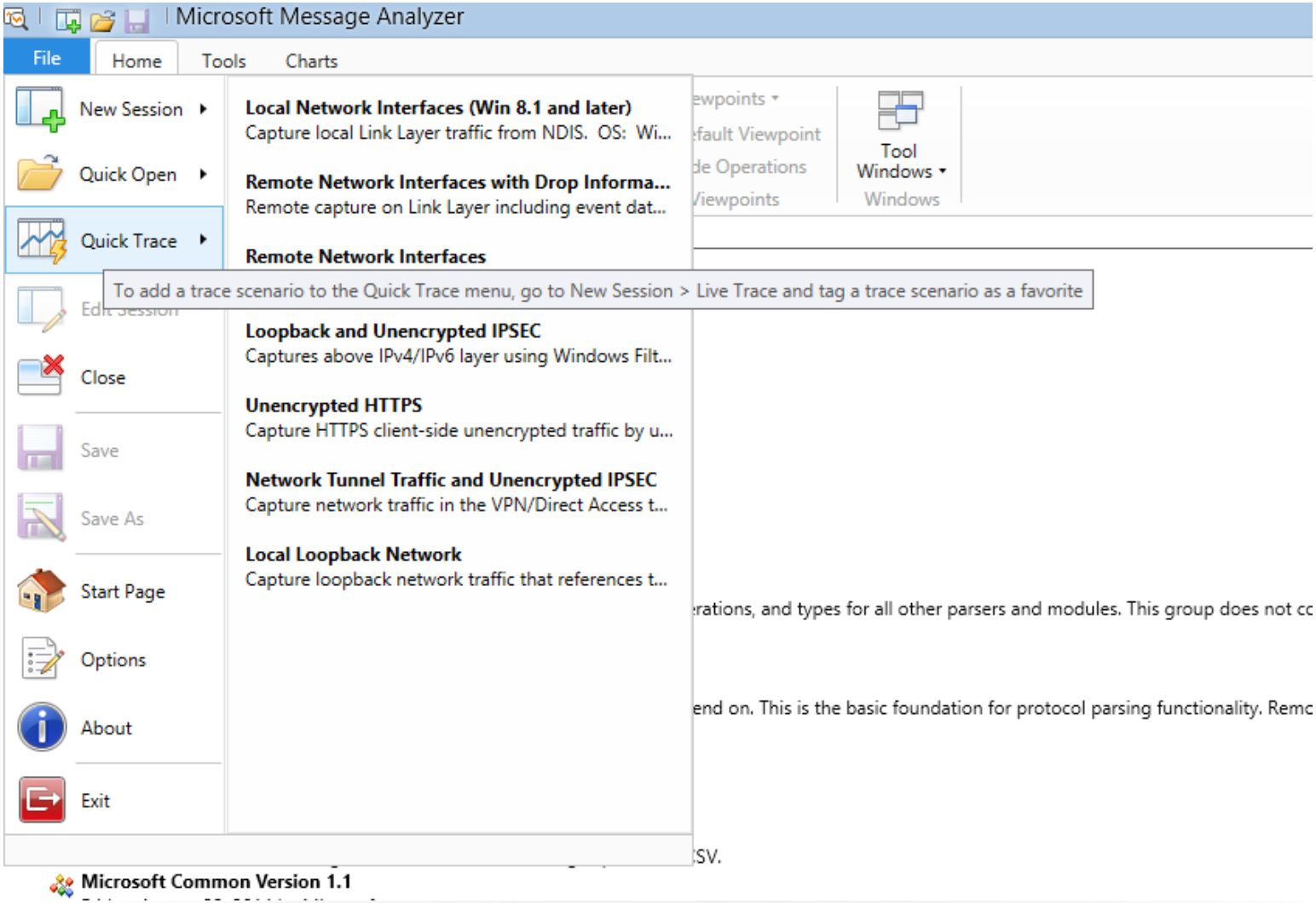
Start Page

News

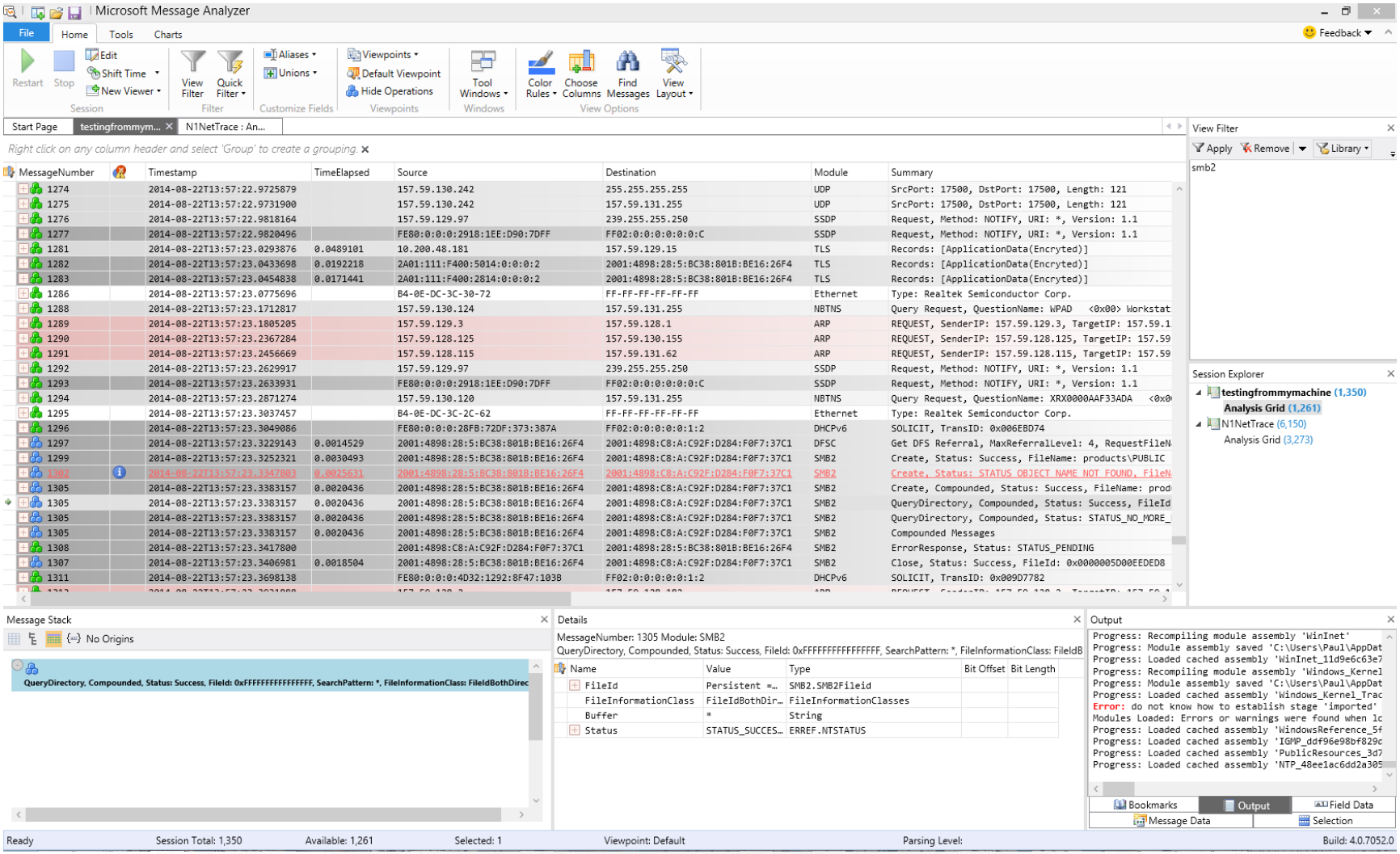
Demo: A quick tour



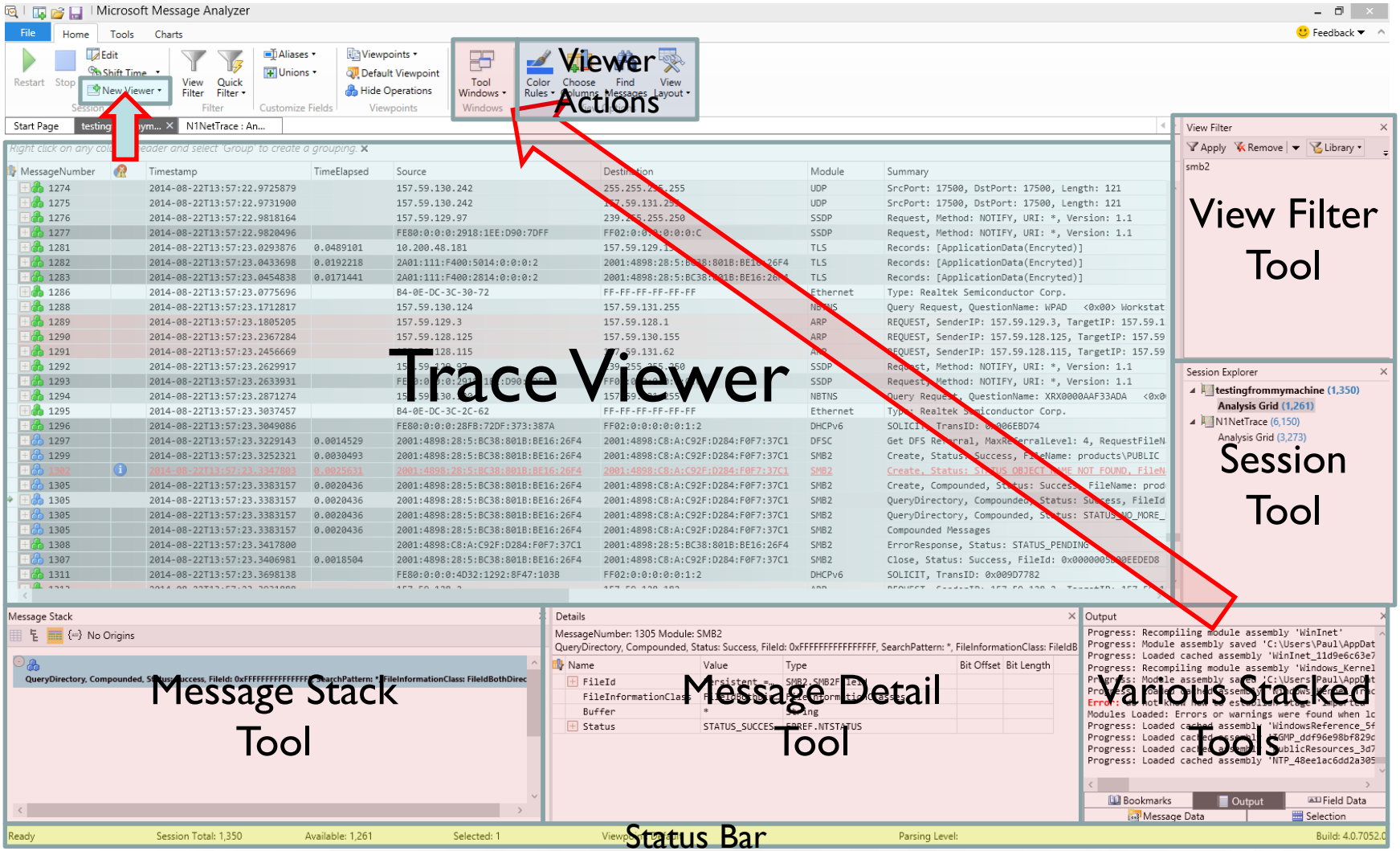
Demo: A quick tour



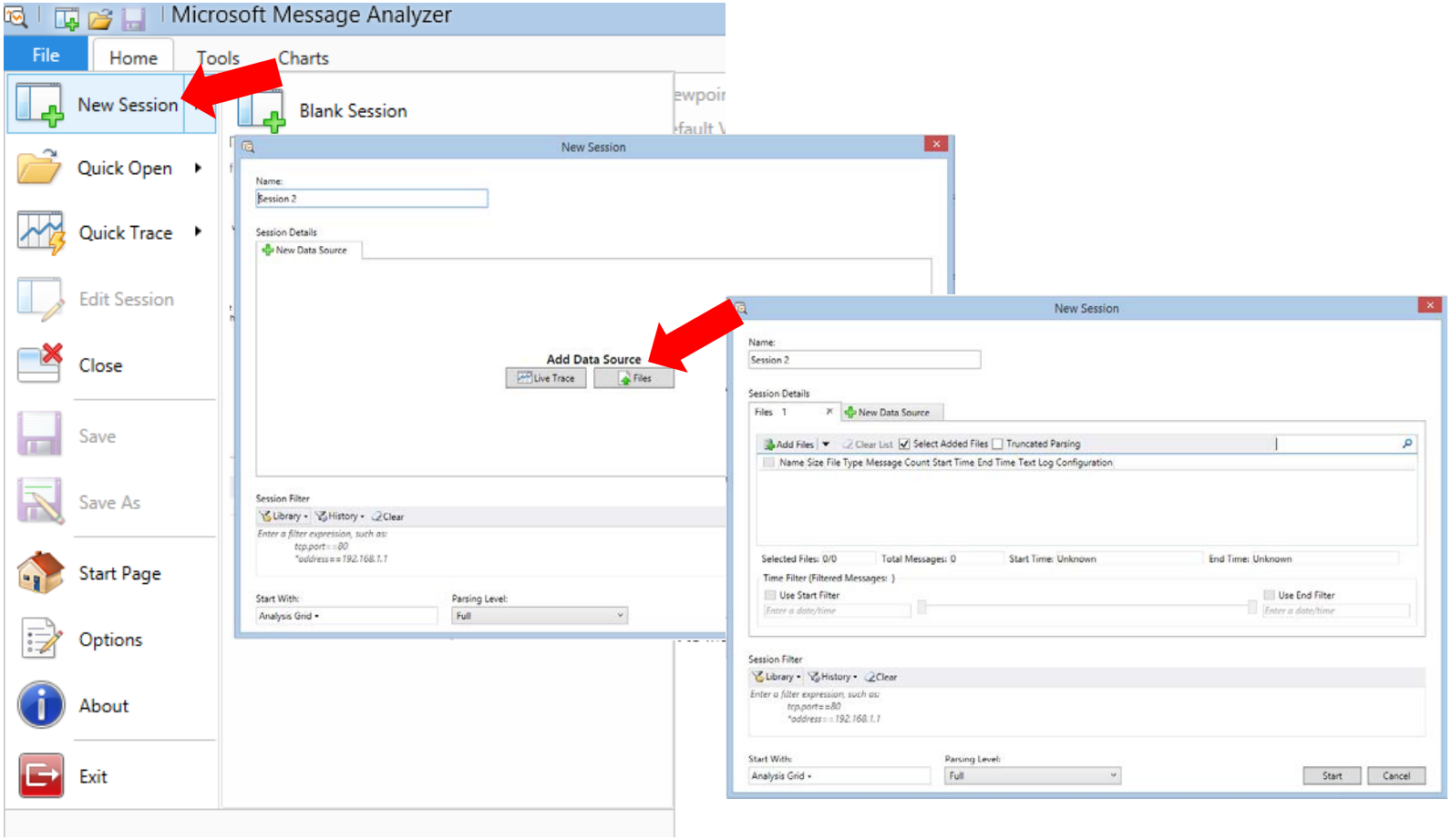
Demo: A quick tour



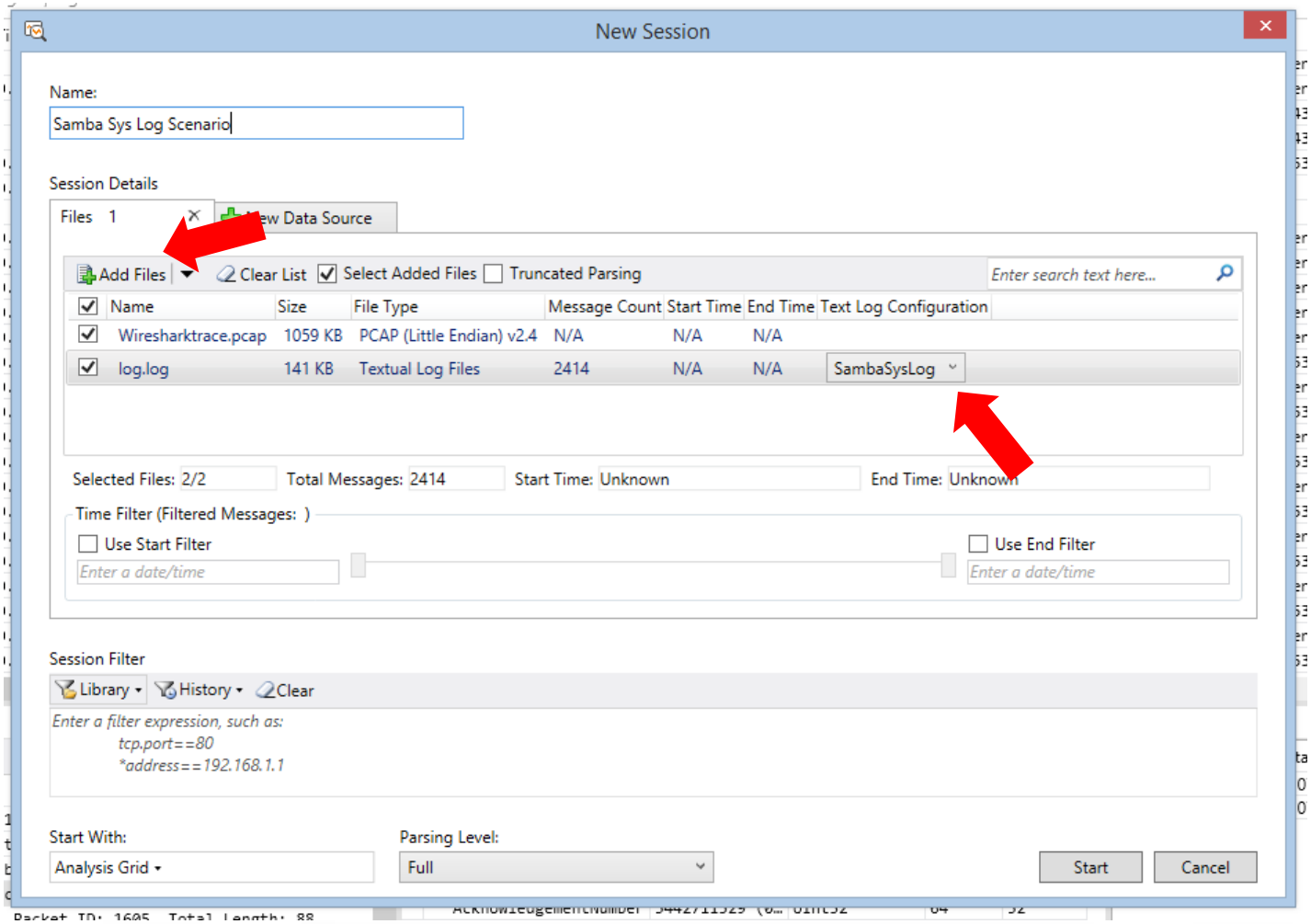
Demo: A quick tour

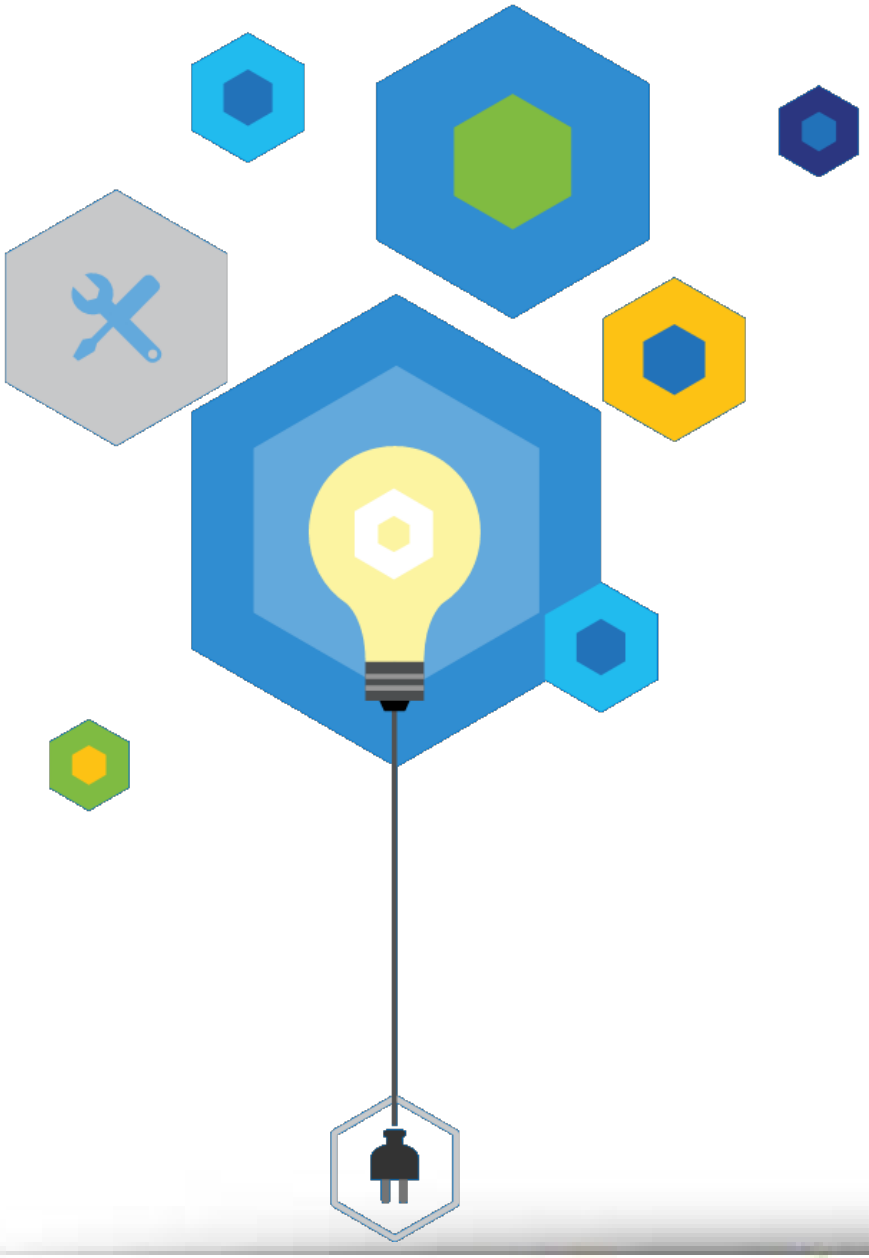


Demo: A quick tour



Demo: A quick tour



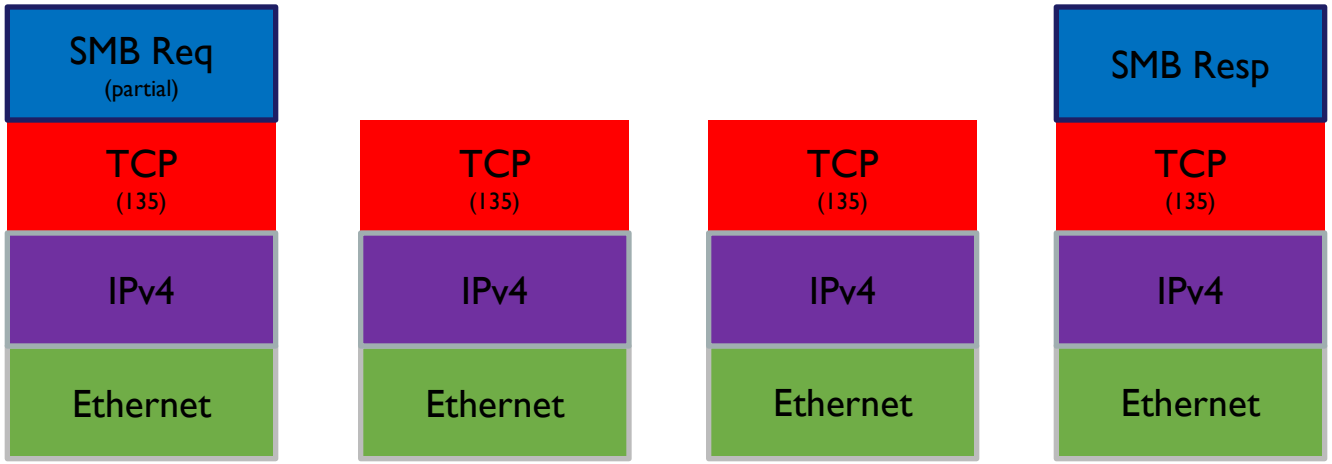


Demo: Correlation with Multiple Logs

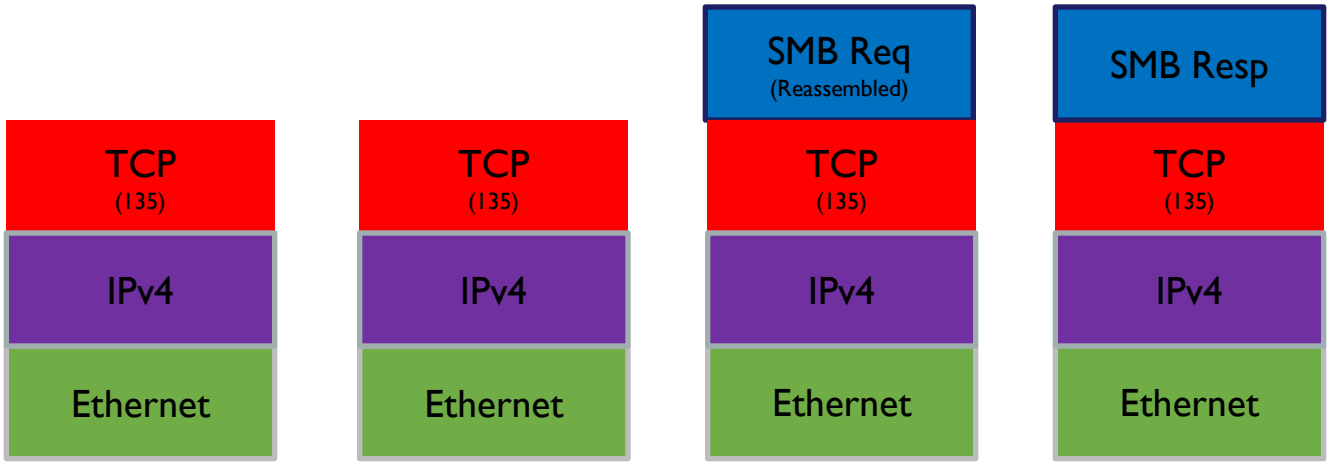
Differences

- Fully Reassemble
  - TCP, HTTP and all layers
  - Fragments hidden
- Group Operations
  - Request/Response
  - Measure response times
- Automatic Diagnoses
  - TCP diagnosis show as info
  - Validation and Protocol Behavior

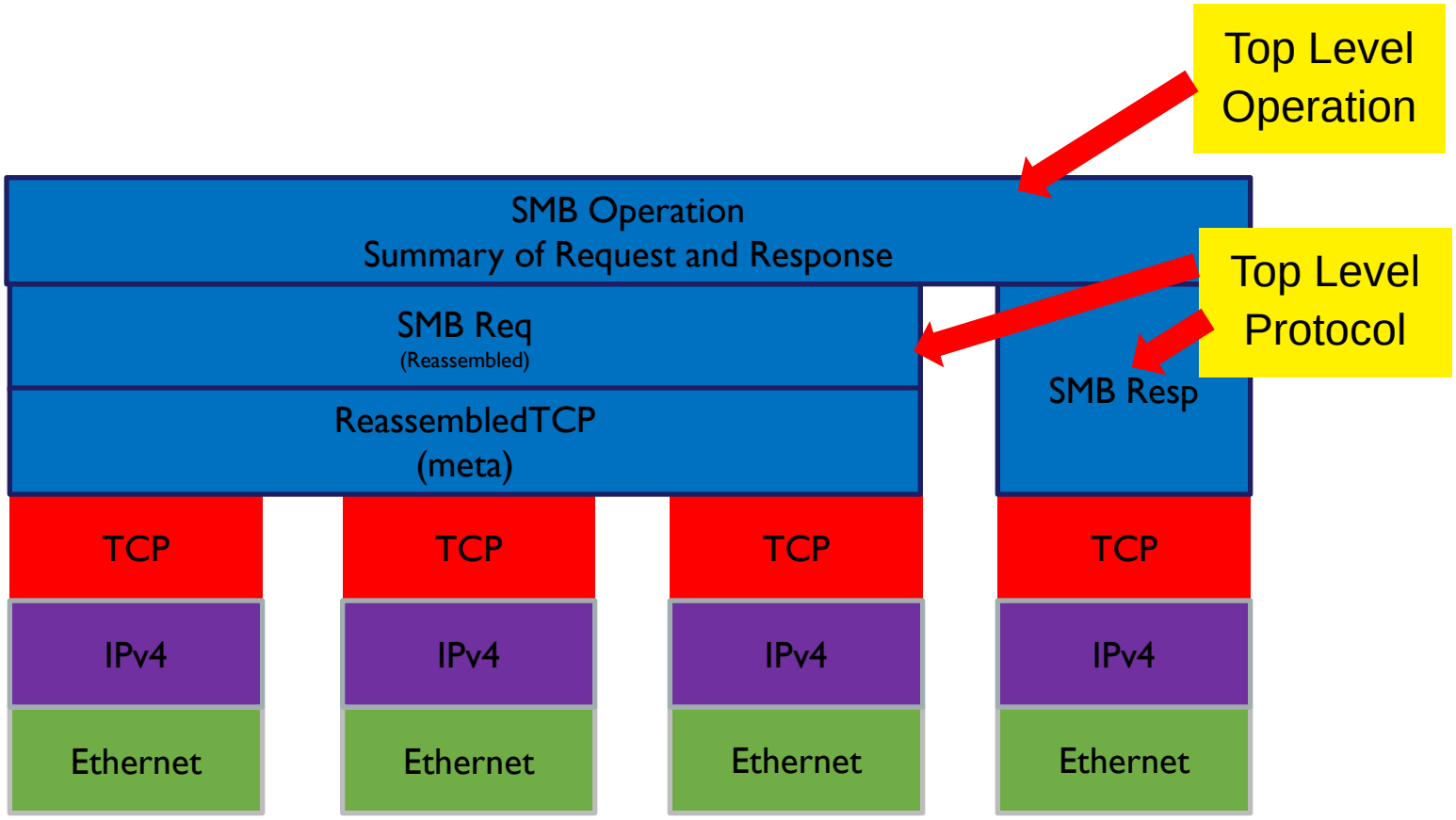
Differences – Netmon

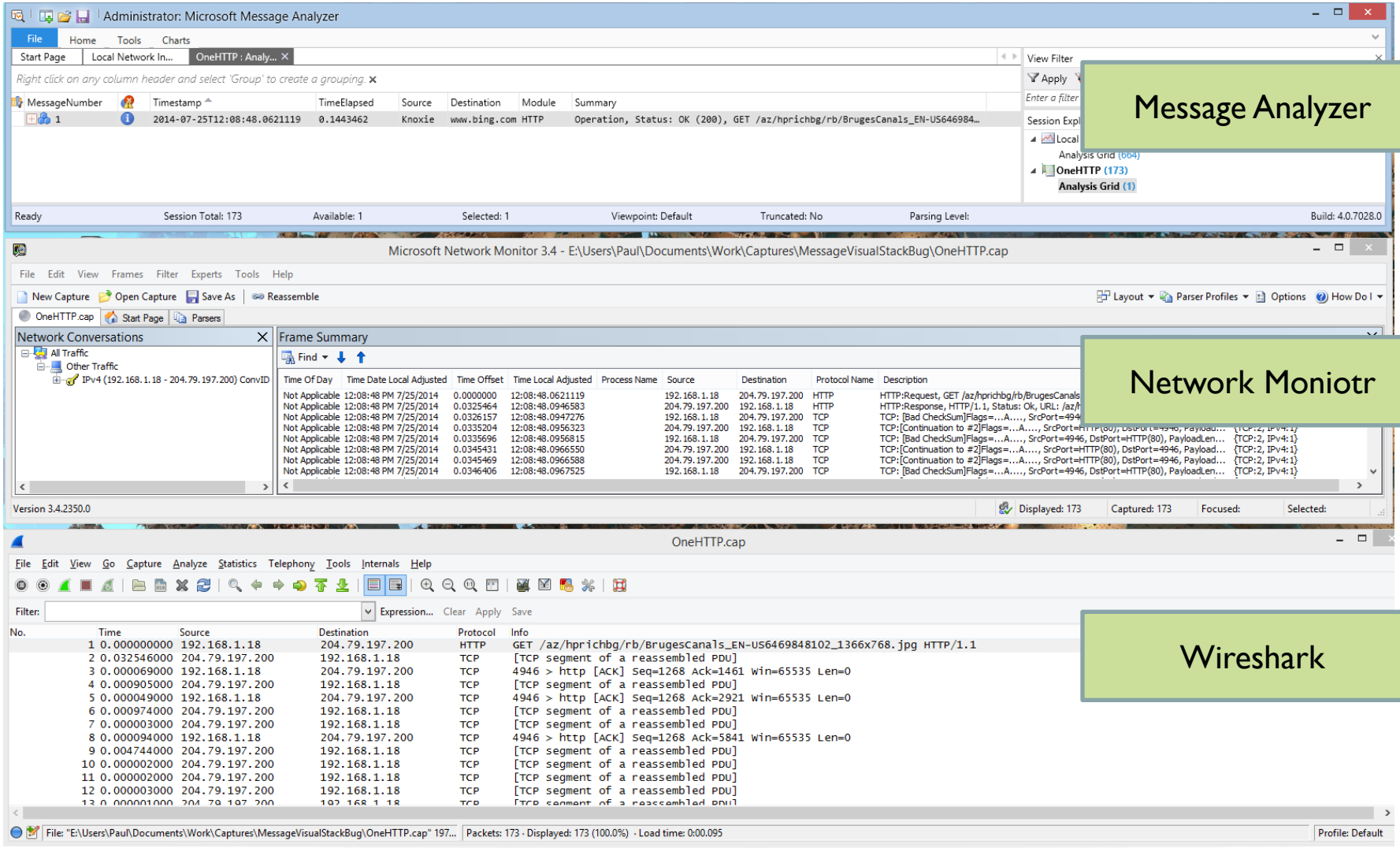


Differences – Wireshark

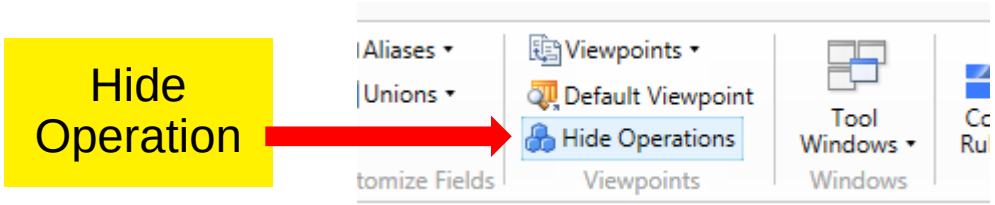


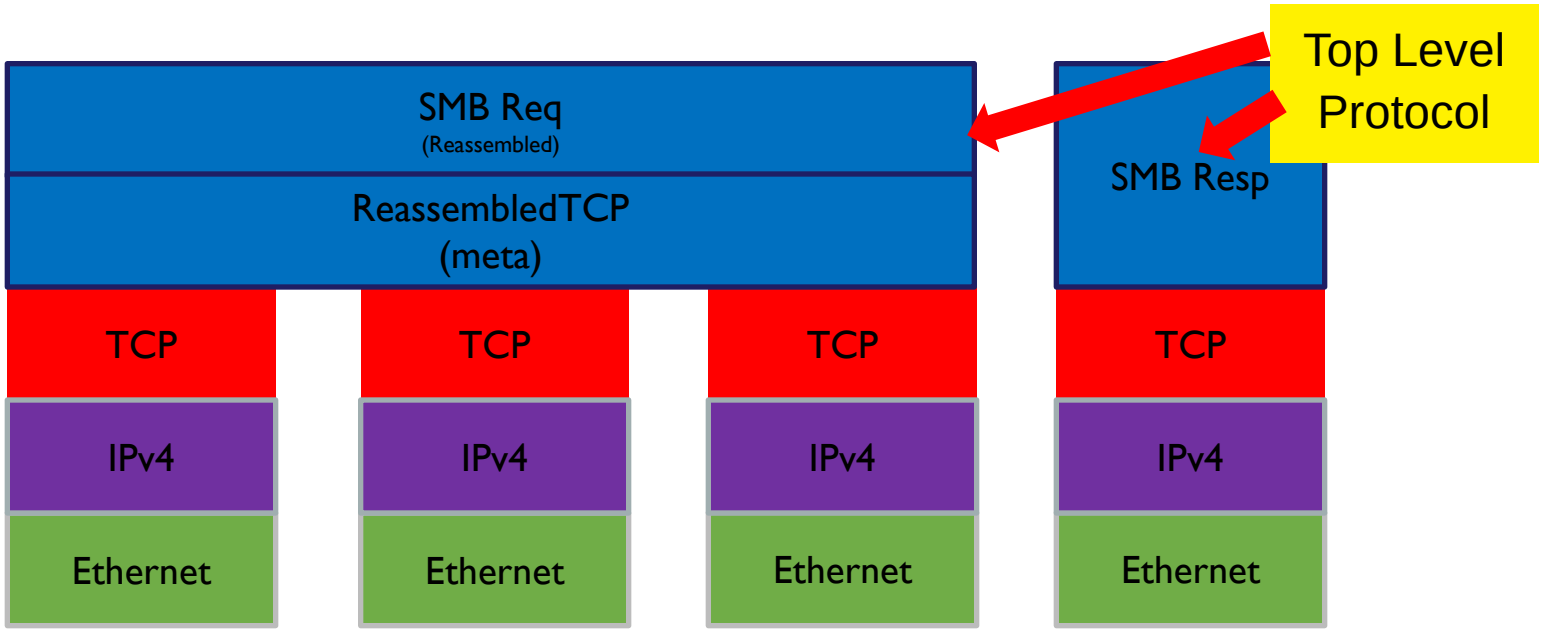
Differences – Message Analyzer



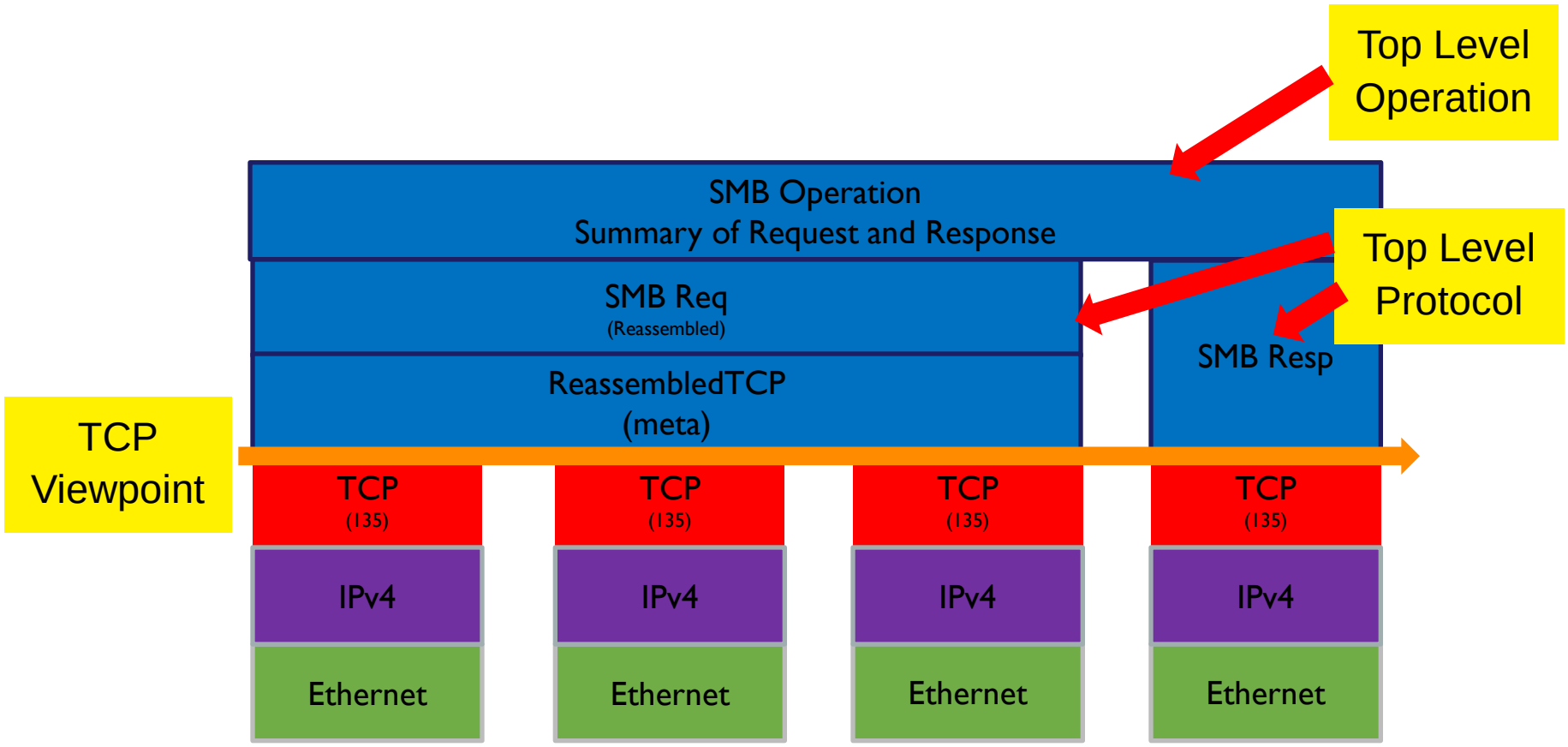


Differences – Message Analyzer

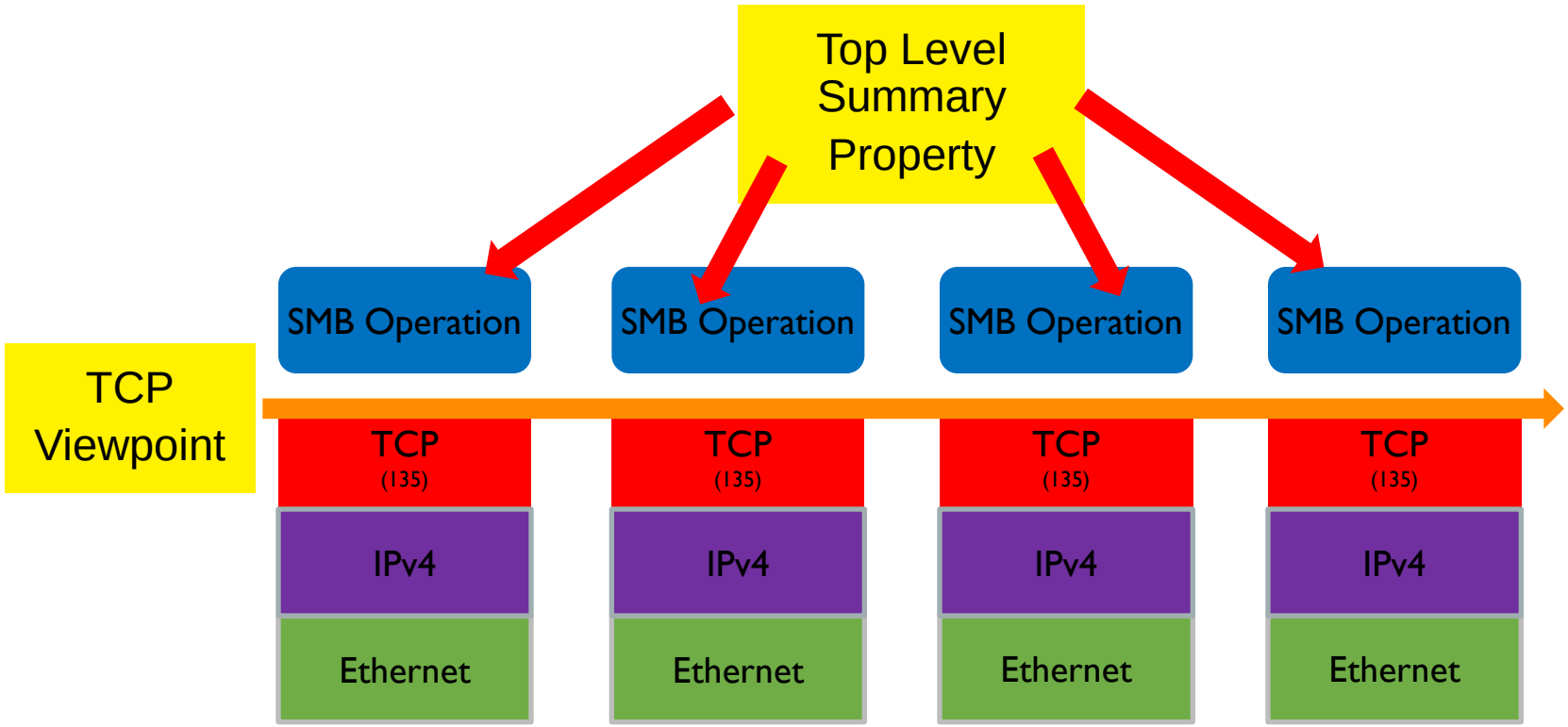




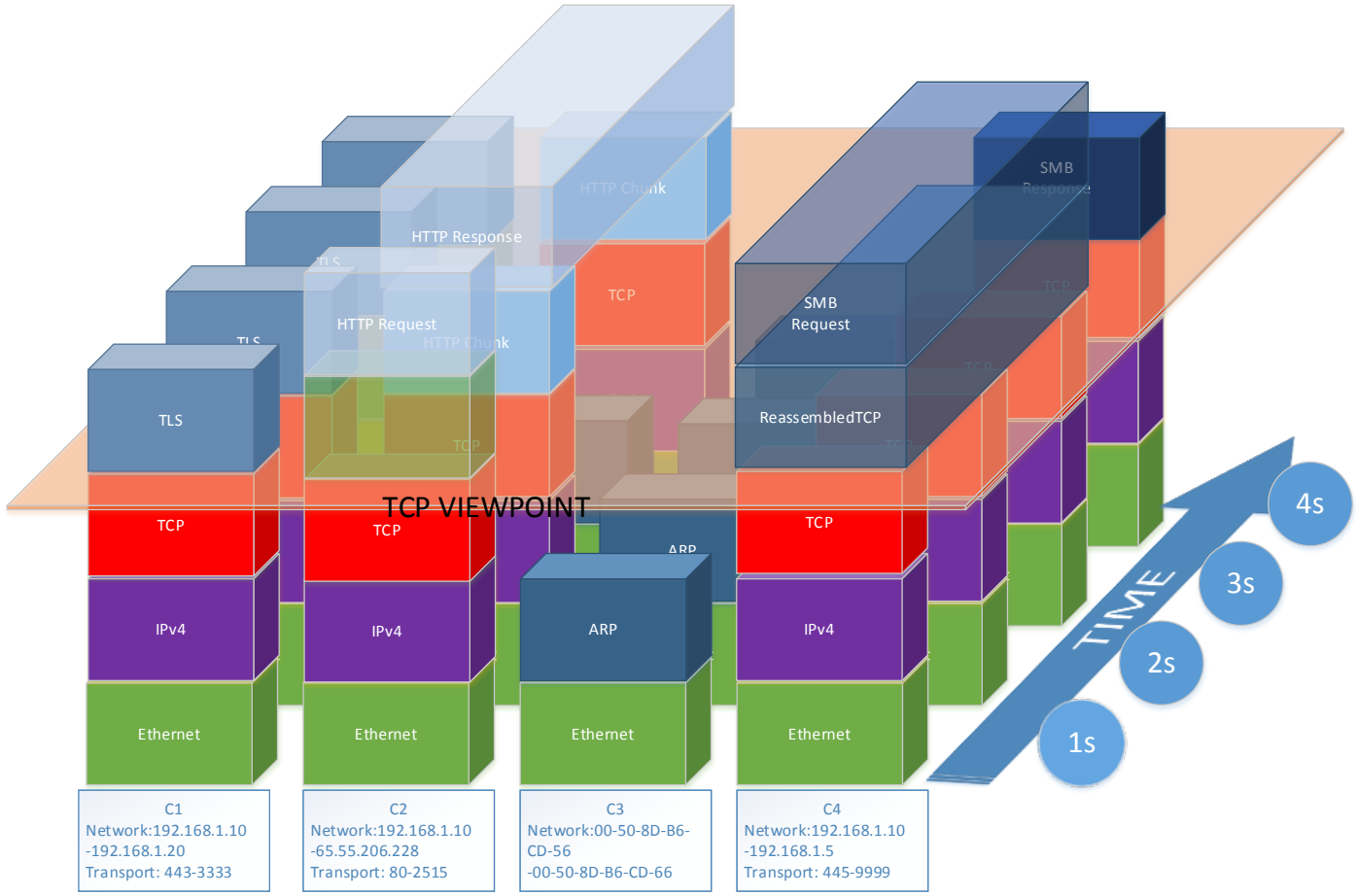
Differences – Message Analyzer



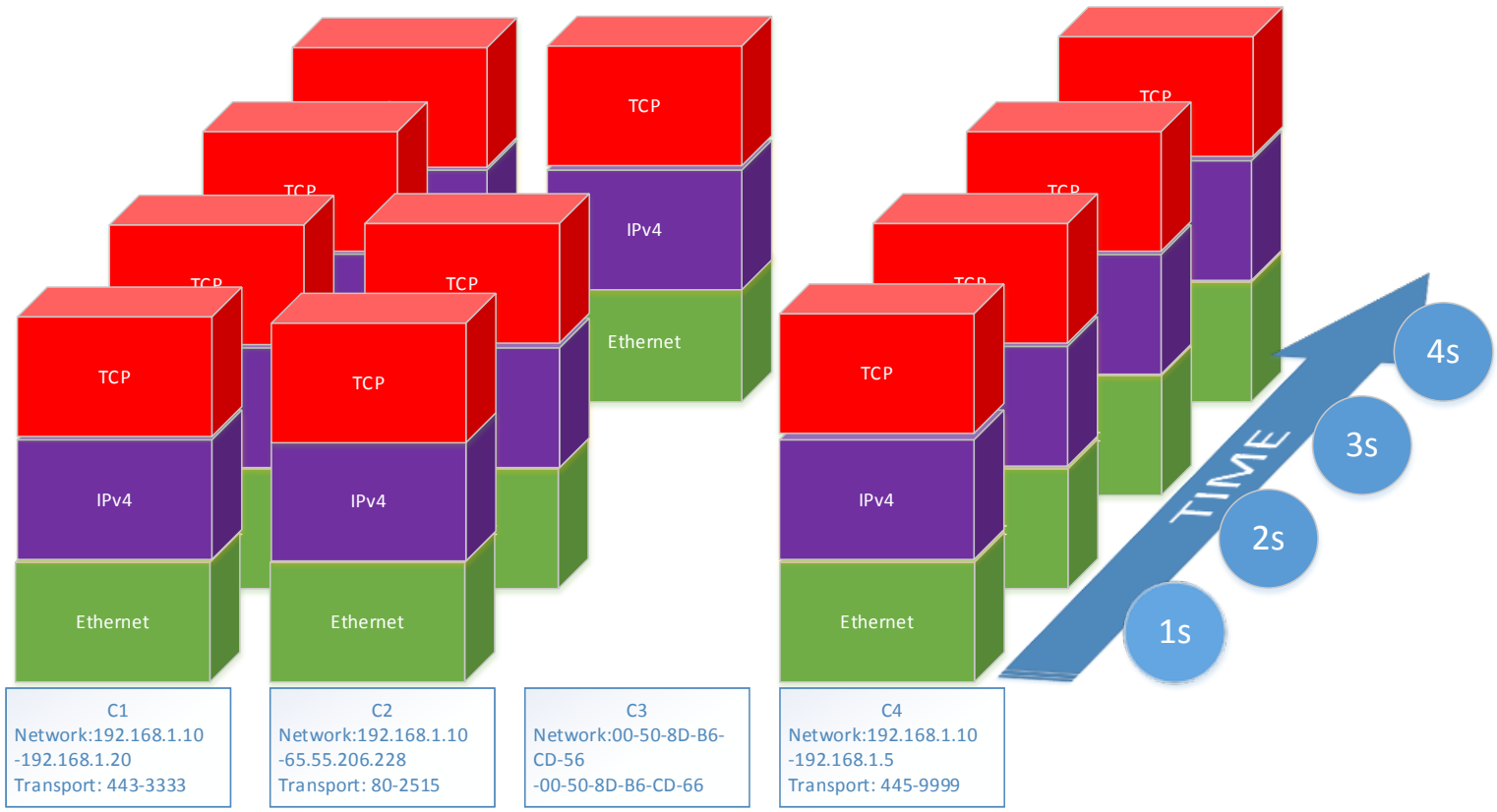
Differences – Message Analyzer



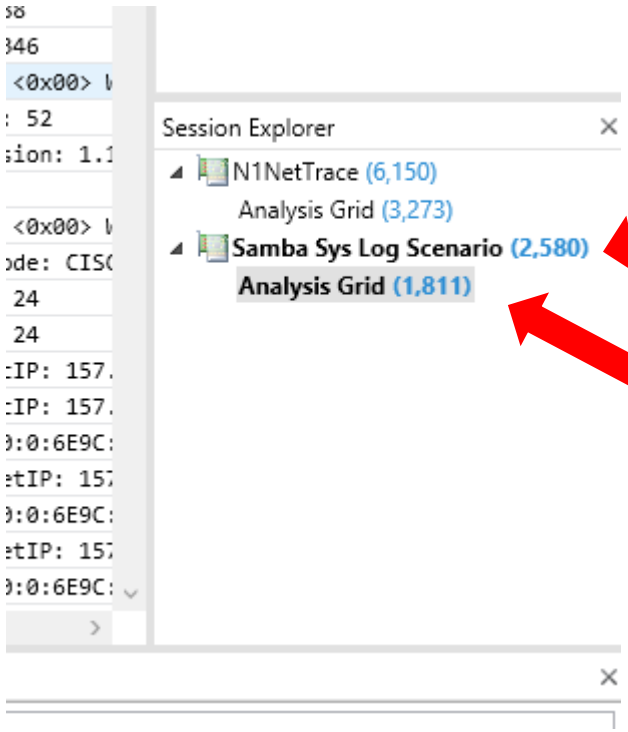
Differences – Message Analyzer in 3D



Differences – Message Analyzer in 3D



Differences: Session Explorer



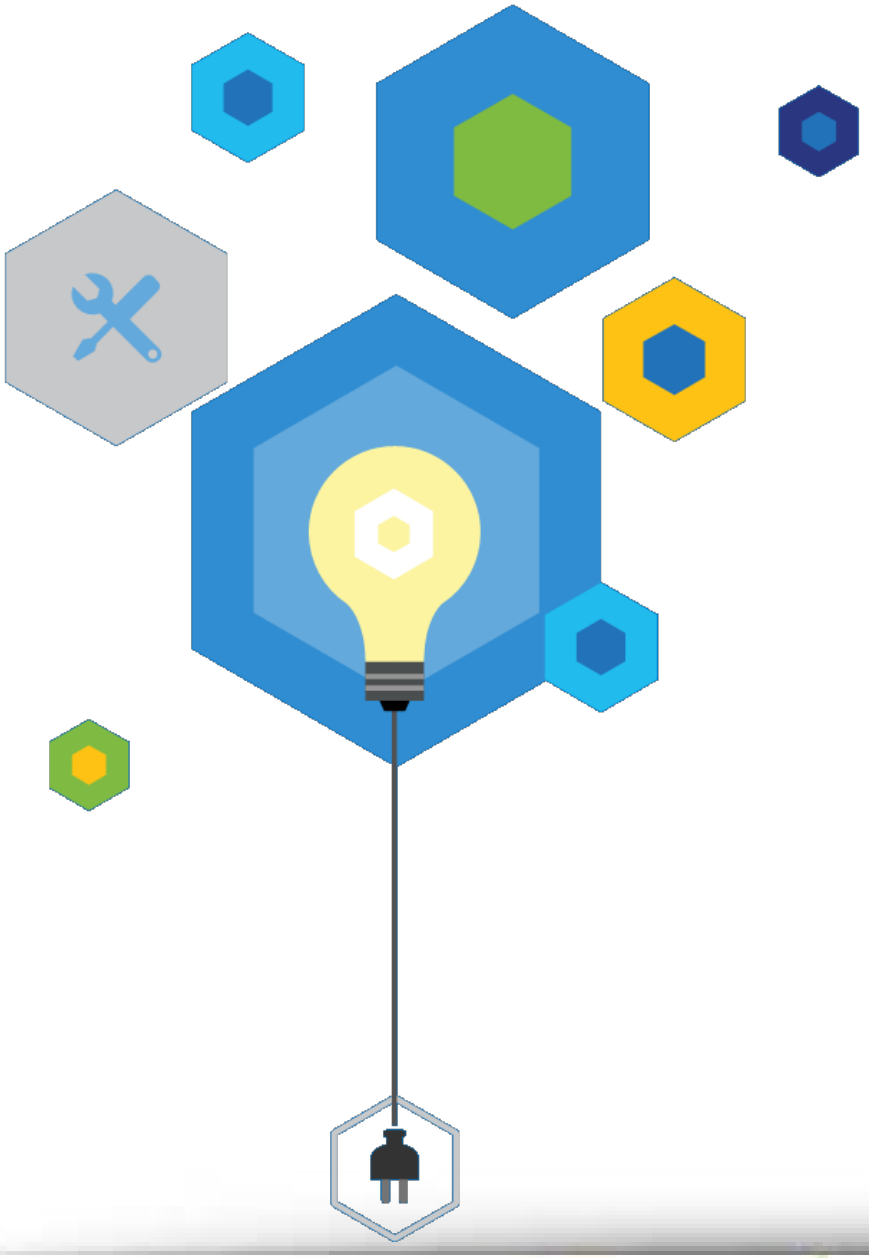
Total number of messages at the bottom. For a .cap or .pcap. This is what Netmon/Wireshark display

Total Number after data is reassembled and summarized with operations.

Encrypted Tracing

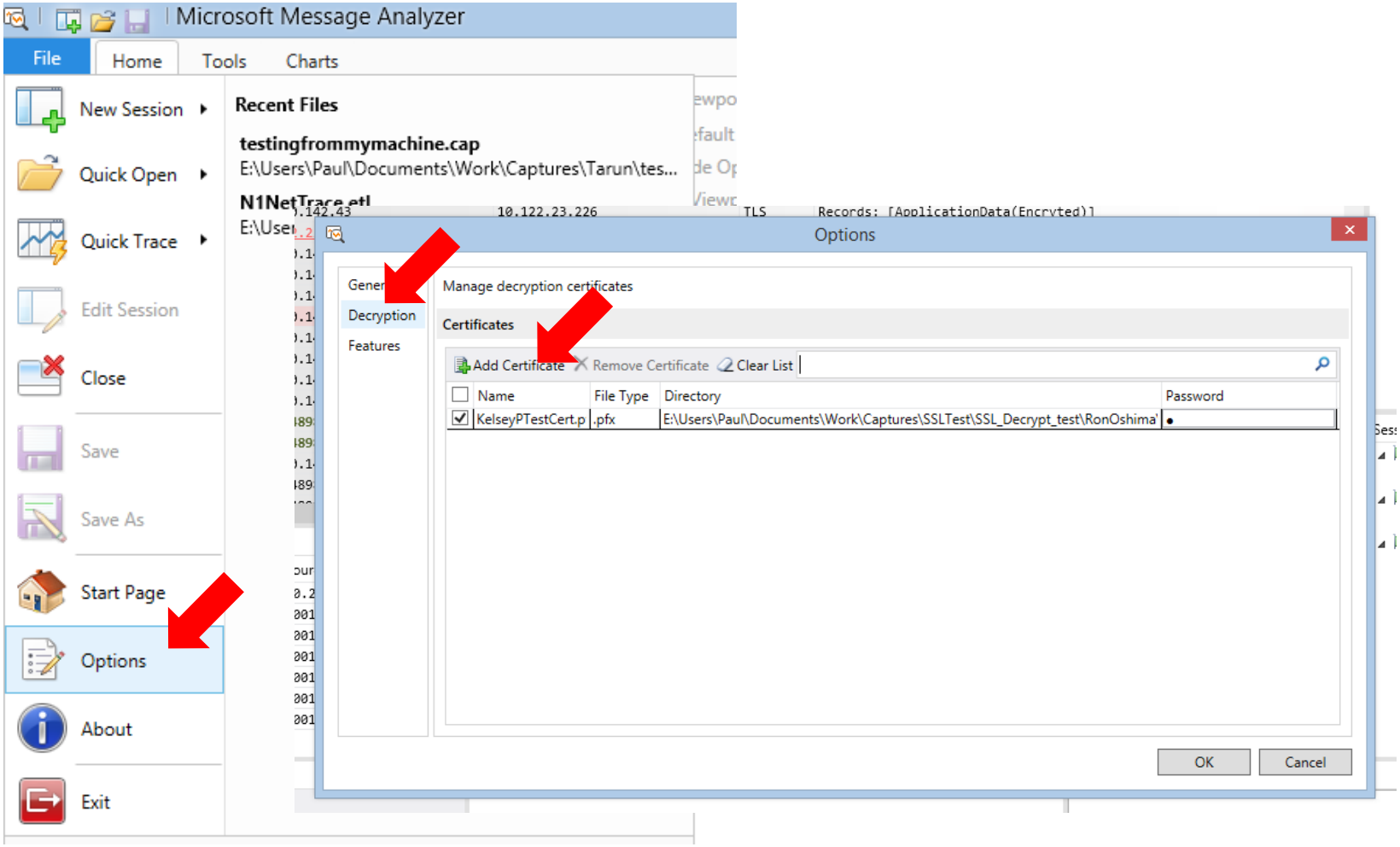
Dealing with Encrypted Traffic

- Capture before encryption
  - HTTPs
  - IPSEC
  - SMB
  - SMB Direct
- Decrypt a trace afterwards

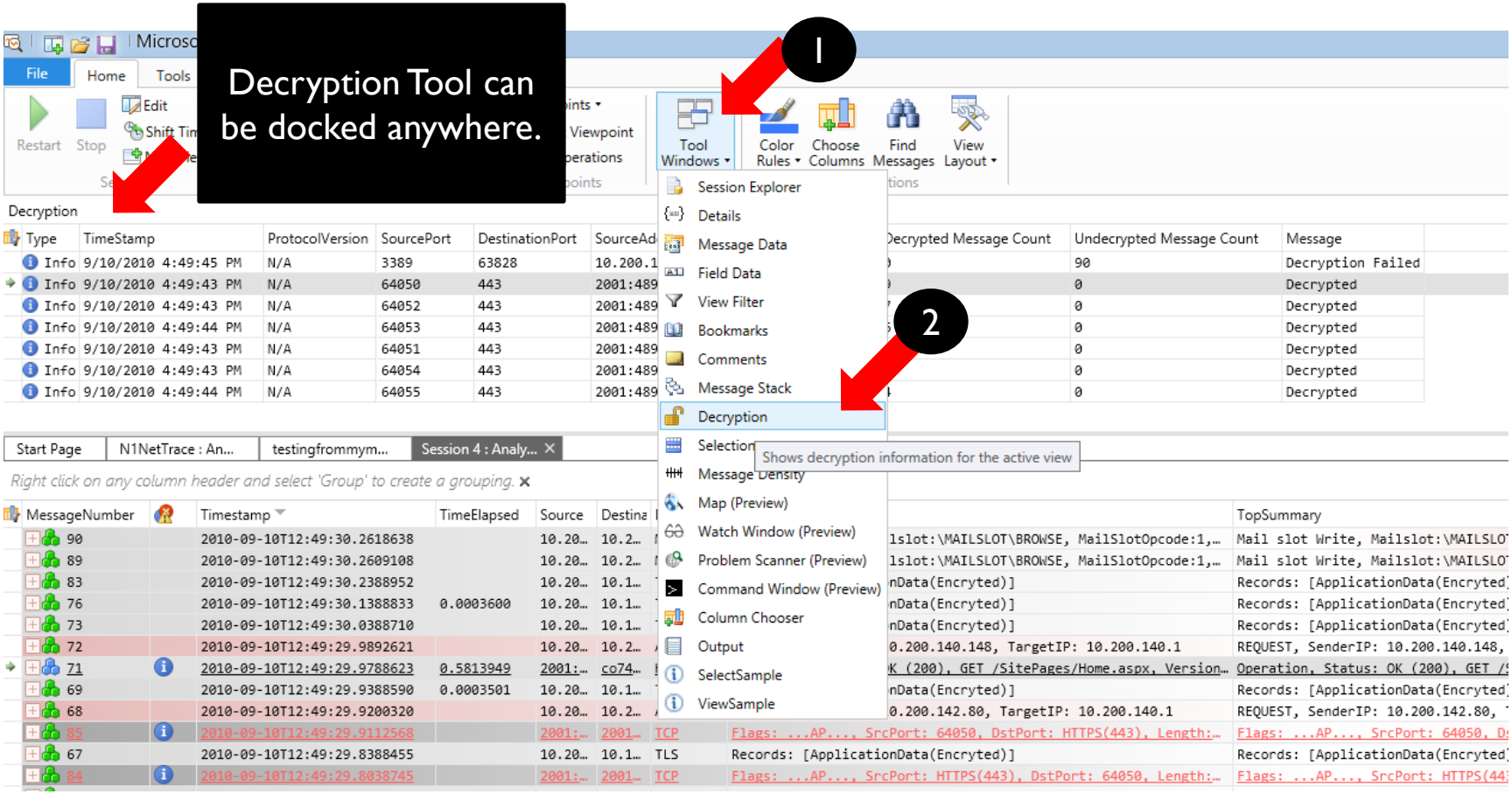


Demo:
Post Decryption

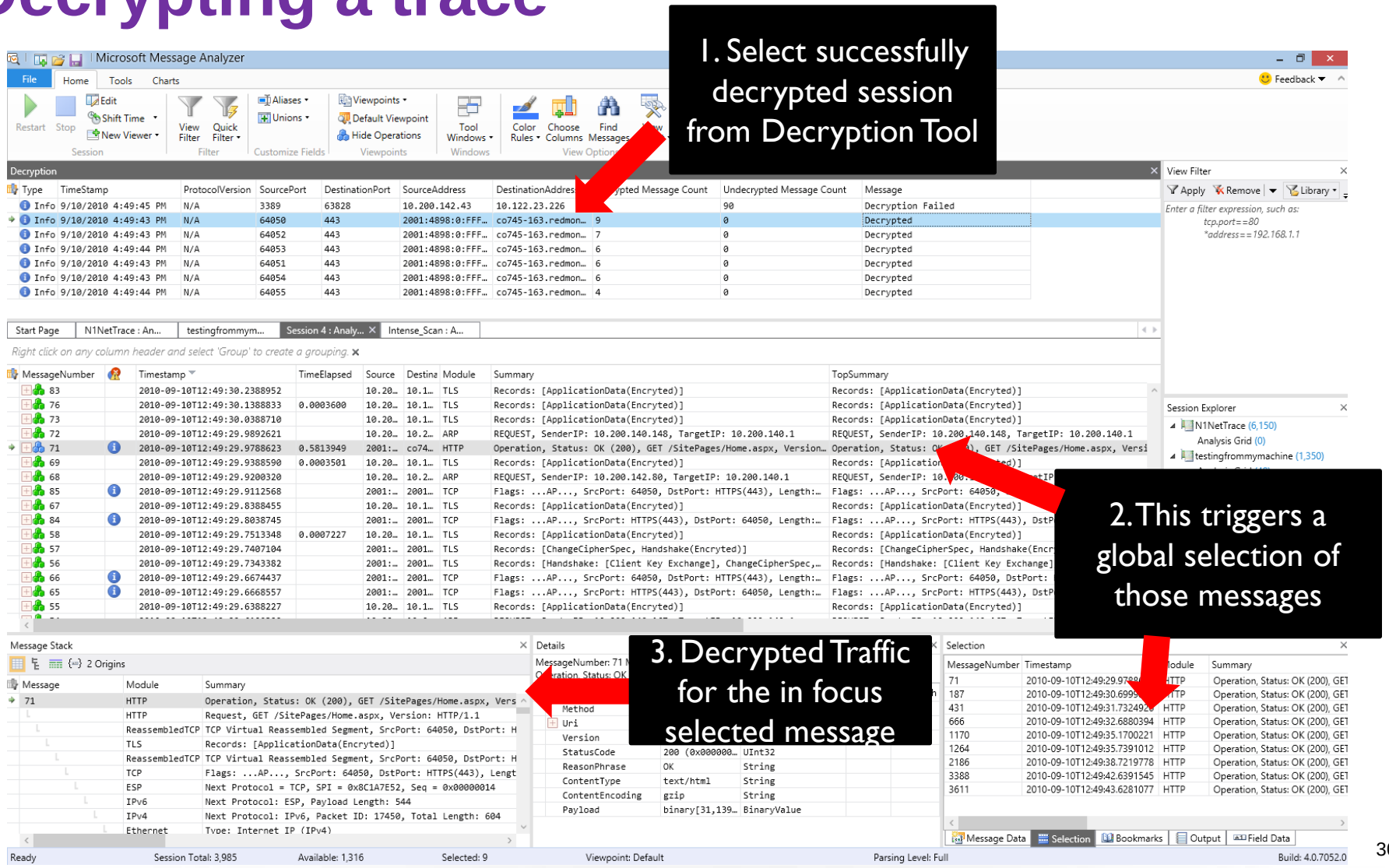
Decrypting a trace



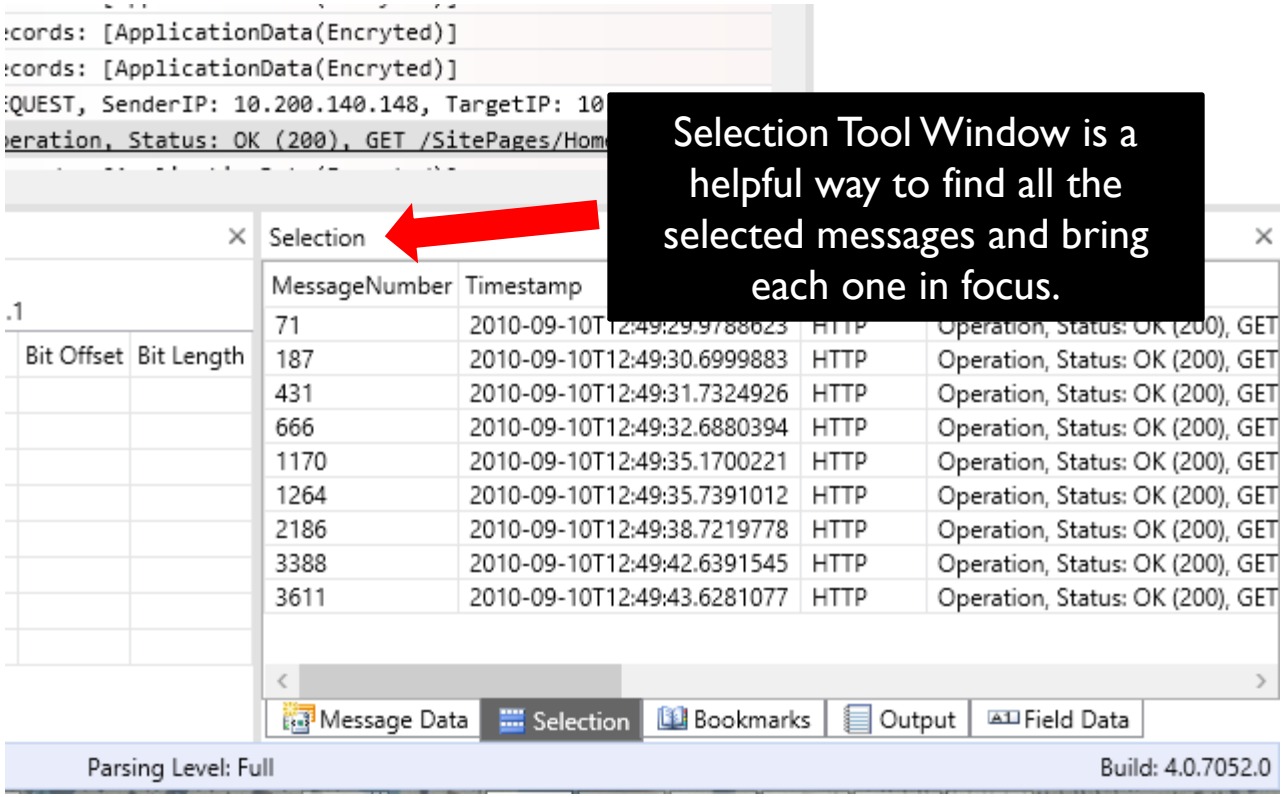
Decrypting a trace



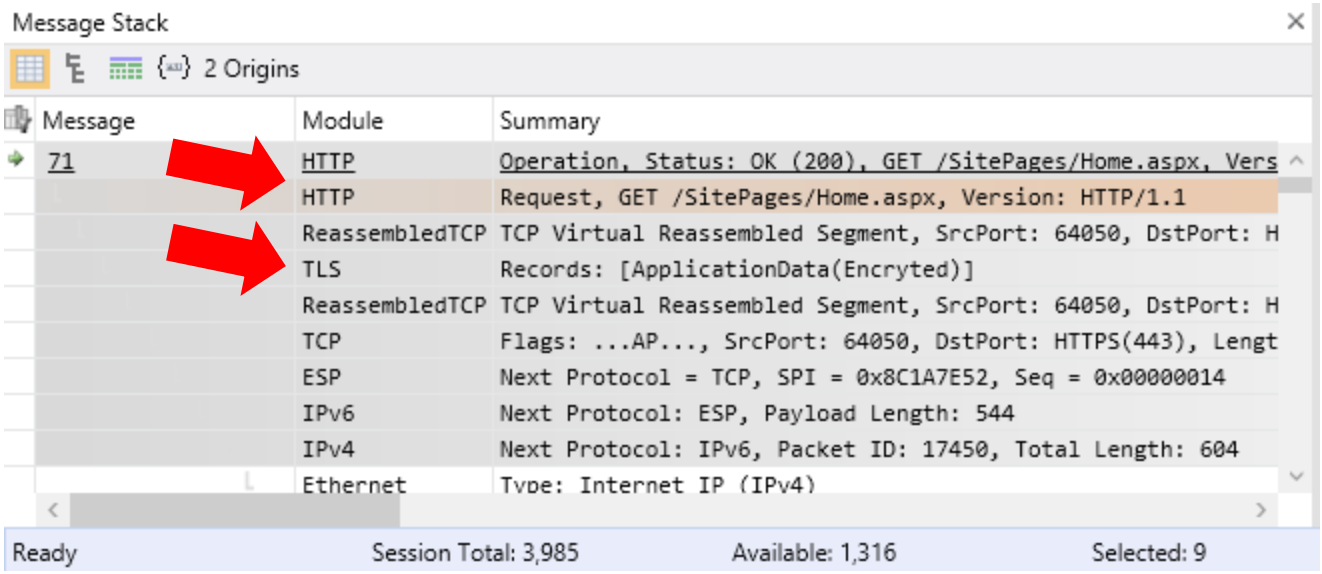
Decrypting a trace



Decrypting a trace



Decrypting a trace



Questions?

Resources

- http://blogs.technet.com/MessageAnalyzer
- http://social.technet.microsoft.com/Forums/en-US/home?forum=messageanalyzer
- http://connect.Microsoft.com/Site216