



STORAGE DEVELOPER CONFERENCE

SNIA ■ SANTA CLARA, 2015

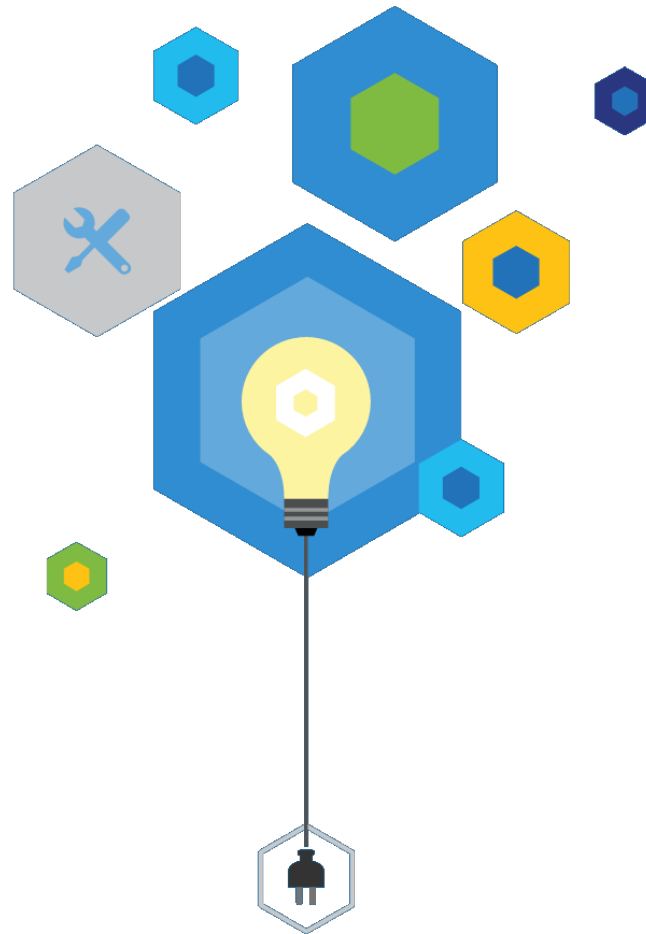
# Microsoft Message Analyzer: New Looks and New Tricks

**Paul Long**  
**Microsoft**

# What is Message Analyzer?

- ❑ Protocol Analysis
- ❑ Protocol Validation
- ❑ Log File Analyzer
- ❑ Deep Data Inspection and Correlation
- ❑ Packet Capture and Event Tracing Collector

# Demo – Inspection and Correlation



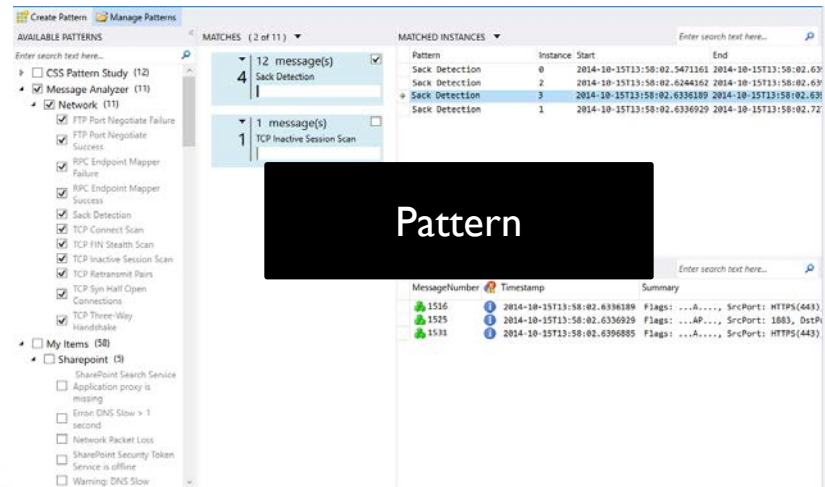
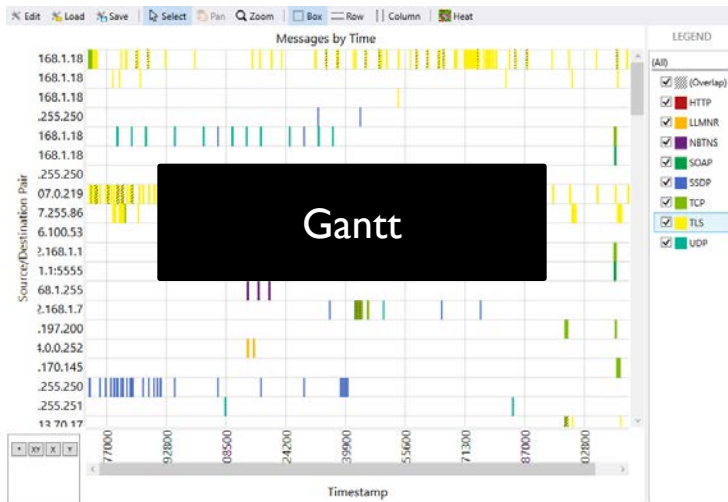
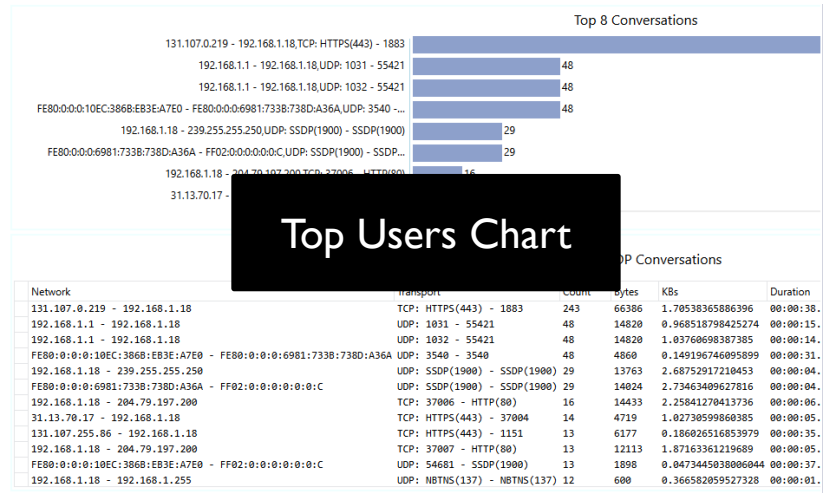
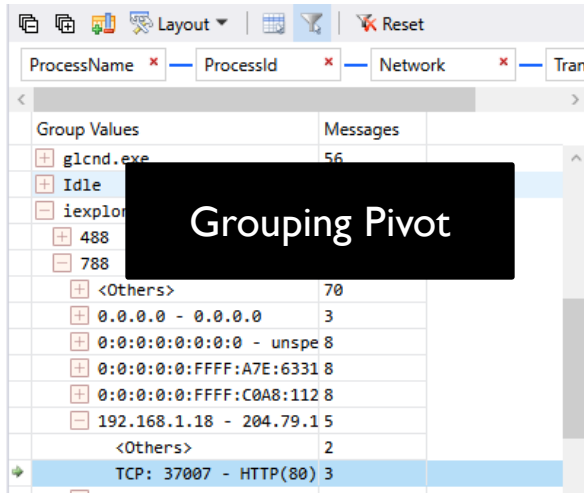
# What's Different with Message Analyzer?

- ❑ Message Reassembly and Operations
  - ❑ Reduces Noise
  - ❑ Increasing Filtering performance
  - ❑ Simplifies Application Troubleshooting
  - ❑ Simplifies Performance Troubleshooting

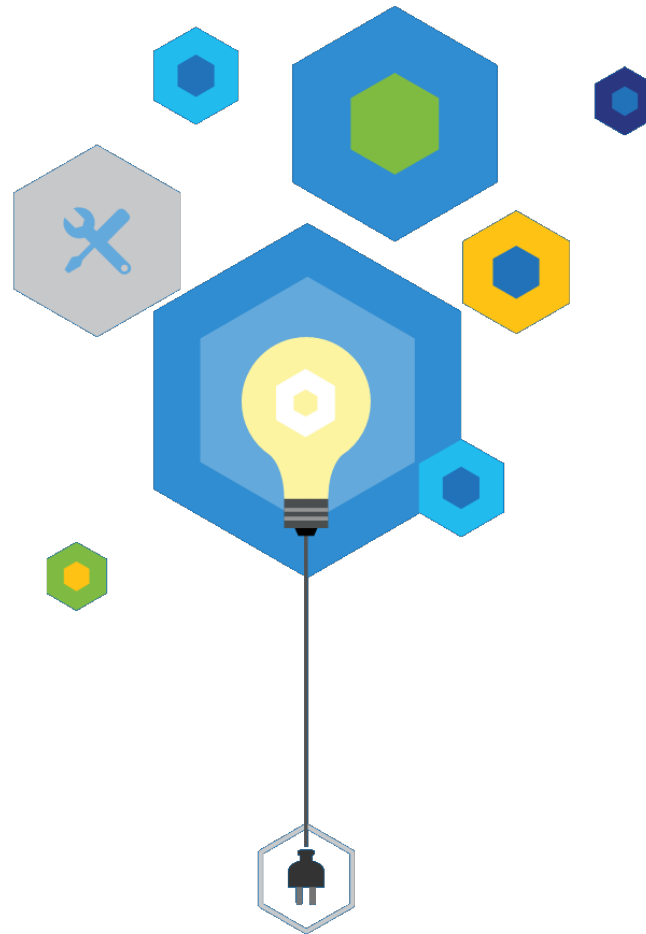
# What's Unique About Message Analyzer?

- ❑ Read more than just Network Traces
  - ❑ Text Log Files (IIS, NetLogon, SambaSysLog)
  - ❑ Event Logs and Tracing (EVTX and ETL)
  - ❑ PowerShell
  - ❑ CSV/TSV
  - ❑ SQL Databases
  - ❑ Azure Tables

# What's Unique About Message Analyzer?



# Demo – Pattern Match TCP Sequences

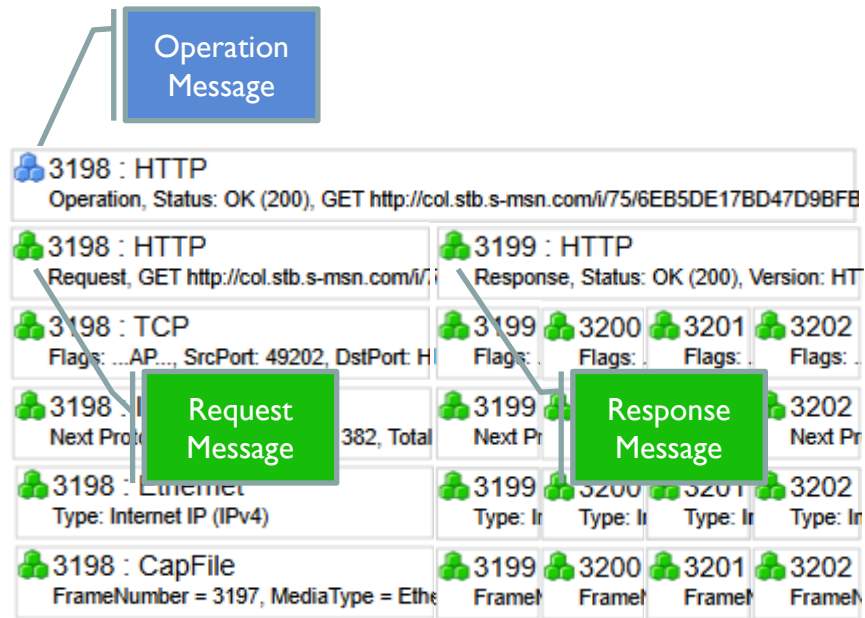


# Messages are Coalesced

- ❑ **Operations** – Group related messages, like Requests and Responses
- ❑ **Automatic Reassembly** – Fragments for IP, TCP, HTTP, and others are automatically reassembled and stored as a tree
- ❑ **Protocol is Validated** – Protocols can be Analyzed and Simulated which allows us to identify differences from the specification.



# Operations and Reassembly



# Network Monitor View

Microsoft Network Monitor 3.4 - E:\Users\Paul\Documents\Work\Captures\MessageMonitorDemos\HTTP\HTTPGoodOnlyBoot\_OneHTTP.cap

File Edit View Frames Filter Experts Tools Help

New Capture Open Capture Save As Reassemble Layout Parser Profiles Options How Do I

HTTPGoodOnlyBoot\_OneHTTP.cap Start Page Parsers

Network Convers...

- All Traffic
- Other Traffic
- IPv4 (65.53.6.120)

Display Filter

Apply Remove History Load Filter

Save Filter Clear Text

Frame Summary

Find Color Rules Aliases Columns

Frame Number	Time Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
1	13:42:59.0639260	0.0000000		65.53.6.120	65.53.63.31	HTTP	HTTP:Request, GET http://col.stb.s-msn.com/i/75/6EB5DE17BD47D99FB0A0232E81BB54.jpg
2	13:42:59.0861538	0.0222278		65.53.63.31	65.53.6.120	HTTP	HTTP:Response, HTTP/1.1, Status: Ok, URL: http://col.stb.s-msn.com/i/75/6EB5DE17BD47D
3	13:42:59.0861538	0.0222278		65.53.63.31	65.53.6.120	TCP	TCP:[Continuation to #2]Flags=...A..., SrcPort=HTTP(80), DstPort=49202, PayloadLen=14
4	13:42:59.0861538	0.0222278		65.53.63.31	65.53.6.120	TCP	TCP:[Continuation to #2]Flags=...AP..., SrcPort=HTTP(80), DstPort=49202, PayloadLen=5
5	13:42:59.0864245	0.0224985		65.53.6.120	65.53.63.31	TCP	TCP:Flags=...A..., SrcPort=49202, DstPort=HTTP(80), PayloadLen=0, Seq=1450402713, Win=0

Frame Details

Frame: Number = 1, Captured Frame Length = 453, MediaType = ETHERNET

- Ethernet: Etype = Internet IP (IPv4), DestinationAddress: [00-07-B3-29-F8-6C]
- Ipv4: Src = 65.53.6.120, Dest = 65.53.63.31, Next Protocol = TCP, PacketLength = 453
- Tcp: Flags=...AP..., SrcPort=49202, DstPort=HTTP(80), PayloadLen=399, Seq=1450402713, Win=0
- Http: Request, GET http://col.stb.s-msn.com/i/75/6EB5DE17BD47D99FB0A0232E81BB54.jpg

Hex Details

Decode As	Width	Prot Off: 0 (0x00)	Frame Off: 0 (0x00)
0000	00 07 B3 29 F8 00 00 03 FF 10 C8 68 0A		
0010	01 B7 01 7E 40 00 80 06 2F C2 41 35 0A		
0020	3F 1F C0 32 00 50 56 73 62 0A 61 31 A0		
0030	40 29 D3 D7 00 00 47 45 54 20 68 74 7A		
0040	2F 63 6F 6C 2E 73 74 62 2E 73 2D 6D 7A		
0050	6F 6D 2F 69 2F 37 35 2F 36 45 42 35 4A		
0060	42 44 34 37 44 39 42 46 42 30 41 30 3A		
0070	38 31 42 42 35 34 2E 6A 70 67 20 48 5A		
0080	31 2E 31 0D 0A 41 63 63 65 70 74 3A 2A		
0090	0D 0A 52 65 66 65 72 65 72 3A 20 68 7A		
00A0	2F 2F 77 77 77 2E 6D 73 6E 2E 63 6F 61		
00B0	63 69 64 3D 69 65 68 70 0D 0A 41 63 6A		
00C0	2D 4C 61 6E 67 75 61 67 65 3A 20 65 61		

Version 3.4.2350.0

Displayed: 5 Captured: 5 Focused: 1 Selected: 1

# Wireshark View

The screenshot displays the Wireshark interface with a packet capture of an HTTP GET request. The main pane shows a list of packets, with packet 4 selected. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Source Port	Destination Port	Info
1	0.000000000	65.53.6.120	65.53.63.31	HTTP	49202	80	80 GET http://col.stb.s-msn.com/i/75/6EB5DE17BD47
2	0.022227800	65.53.63.31	65.53.6.120	TCP	80	49202	49202 [TCP segment of a reassembled PDU]
3	0.000000000	65.53.63.31	65.53.6.120	TCP	80	49202	49202 [TCP segment of a reassembled PDU]
4	0.000000000	65.53.63.31	65.53.6.120	HTTP	80	49202	49202 HTTP/1.1 200 OK (JPEG JFIF image)
5	0.000270700	65.53.6.120	65.53.63.31	TCP	49202	80	49202-80 [ACK] Seq=400 Ack=3433 win=16425 Len=

The packet details pane for the selected packet (Frame 4) shows the following layers:

- Frame 4: 566 bytes on wire (4528 bits), 566 bytes captured (4528 bits)
- Ethernet II, Src: Cisco\_29:f8:00 (00:07:b3:29:f8:00), Dst: Microsof\_10:c8:68 (00:03:ff:10:c8:68)
- Internet Protocol Version 4, Src: 65.53.63.31 (65.53.63.31), Dst: 65.53.6.120 (65.53.6.120)
- Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49202 (49202), Seq: 2921, Ack: 400, Len: 512
- [3 Reassembled TCP Segments (3432 bytes): #2(1460), #3(1460), #4(512)]
- Hypertext Transfer Protocol**
- JPEG File Interchange Format

The packet bytes pane shows the raw data of the selected packet, with a hex dump and ASCII representation. The ASCII representation shows the start of an HTTP response, including the status line: "HTTP/1.1 200 OK (JPEG JFIF image)".

File: "E:\Users\Paul\Documents\Work\Captures\MessageMonitorDemos\HTTP\HTTPGood..." | Packets: 5 · Displayed: 5 (100.0%) · Load time: 0:00.000 | Profile: Default

# Message Analyzer View

The screenshot shows the Microsoft Message Analyzer application. Three callout boxes highlight key features:

- Limit Noise:** Points to the 'Tools' menu.
- Measure Performance:** Points to the 'Performance' menu.
- Visualize Data:** Points to the 'Field Chooser' pane on the right.

The main interface displays a table of messages with columns: MessageNumber, Timestamp, TimeElapsed, ResponseTime, Source, Destination, Module, and Summary. Below the table is the 'Message Stack 1' pane showing a detailed view of the message layers (HTTP, TCP, IPv4, Ethernet, CapFile). The 'Details 1' pane shows the message details, including Method (GET), Uri, Version (HTTP/1.1), StatusCode (200), ReasonPhrase (OK), ContentType (image/jpeg), and Payload. The 'Field Data' pane on the right shows a preview of the image data.

# Filtering Differences



2908 : HTTP Operation, Status: OK (200), GET http://www.msn.com/?ocid=ehp, Version: HTTP/1.1	
2908 : HTTP Request: GET http://www.msn.com/?ocid=ehp	2927 : HTTP Response, Status: OK (200), Version: HT
2908 : TCP Flags: AP, Src, SeqP	2916 : TCP Flags: A, SeqP
2908 : IPv4 Next Protocol: TCF	2916 : IPv4 Next Protocol: TCF
2908 : Ethernet Type: Internet IP (I)	2916 : Ethernet Type: Internet IP (I)
2900 : CapFile FrameNumber = 2	2916 : CapFile FrameNumber = 2

3139 : HTTP Operation, Status: OK (200), GET http://col.stb.s-msn.com/766D3131720D146FD85	
3139 : HTTP Request: GET http://col.stb.s-msn.com/766D3131720D146FD85	3163 : HTTP Response, Status: OK (200), Version: HT
3139 : TCP Flags: AP, SrcPort: 48202, DstPort: H	3163 : TCP Flags: A, SeqP
3139 : IPv4 Next Protocol: TCP, Packet ID: 366, Total	3163 : IPv4 Next Protocol: TCP, Packet ID: 366, Total
3139 : Ethernet Type: Internet IP (IPv4)	3163 : Ethernet Type: Internet IP (IPv4)
3139 : CapFile FrameNumber = 3139, MediaType = Ethe	3163 : CapFile FrameNumber = 3139, MediaType = Ethe
























3178 : HTTP Operation, Status: OK (200), GET http://ads2.msads.net/CIS/61000/000/000/017003/	
3178 : HTTP Request: GET http://ads2.msads.net/CIS/61000/000/000/017003/	3179 : HTTP Response, Status: OK (200), Version: HT
3178 : TCP Flags: AP, SrcPort: 48202, DstPort: H	3179 : TCP Flags: A, SeqP
3178 : IPv4 Next Protocol: TCP, Packet ID: 376, Total	3179 : IPv4 Next Protocol: TCP, Packet ID: 376, Total
3178 : Ethernet Type: Internet IP (IPv4)	3179 : Ethernet Type: Internet IP (IPv4)
3178 : CapFile FrameNumber = 3177, MediaType = Ethe	3179 : CapFile FrameNumber = 3177, MediaType = Ethe

3134 : HTTP Operation, Status: OK (200), GET http://col.stb.s-msn.com/30/413380/2FE8F238E6E	
3134 : HTTP Request: GET http://col.stb.s-msn.com/30/413380/2FE8F238E6E	3141 : HTTP Response, Status: OK (200), Version: HT
3134 : TCP Flags: AP, SrcPort: 49198, DstPort: H	3141 : TCP Flags: A, SeqP
3134 : IPv4 Next Protocol: TCP, Packet ID: 362, Total	3141 : IPv4 Next Protocol: TCP, Packet ID: 362, Total
3134 : Ethernet Type: Internet IP (IPv4)	3141 : Ethernet Type: Internet IP (IPv4)
3134 : CapFile FrameNumber = 3133, MediaType = Ethe	3141 : CapFile FrameNumber = 3133, MediaType = Ethe
























# Filtering Difference

Filtering **always** applies to the entire tree. If any node in the tree contains a match, top level message is returned. Even when operations are hidden.

 3198 : HTTP Operation, Status: OK (200), GET http://col.stb.s-msn.com/i/75/6EB5DE17BD47D9BFB				
 3198 : HTTP Request, GET http://col.stb.s-msn.com/i/7		 3199 : HTTP Response, Status: OK (200), Version: HT		
 3198 : TCP Flags: ...AP..., SrcPort: 49202, DstPort: H	 3199	 3200	 3201	 3202
 3198 : IPv4 Next Protocol: TCP, Packet ID: 382, Total	 3199	 3200	 3201	 3202
 3198 : Ethernet Type: Internet IP (IPv4)	 3199	 3200	 3201	 3202
 3198 : CapFile FrameNumber = 3197, MediaType = Eth	 3199	 3200	 3201	 3202

# Viewpoints

Viewpoints let you see messages at layers in the stack. A TCP viewpoint let's you see all TCP fragments.

















 <b>3198 : HTTP</b> Operation, Status: OK (200), GET http://col.stb.s-msn.com/i/75/6EB5DE17BD47D9BFB					
 <b>3198 : HTTP</b> Request, GET http://col.stb.s-msn.com/i/7		 <b>3199 : HTTP</b> Response, Status: OK (200), Version: HT			
 <b>3198 : TCP</b> Flags: ...AP..., SrcPort: 49202, DstPort: H		 <b>3199</b>	 <b>3200</b>	 <b>3201</b>	 <b>3202</b>
 <b>3198 : IPv4</b> Next Protocol: TCP, Packet ID: 382, Total		 <b>3199</b>	 <b>3200</b>	 <b>3201</b>	 <b>3202</b>
 <b>3198 : Ethernet</b> Type: Internet IP (IPv4)		 <b>3199</b>	 <b>3200</b>	 <b>3201</b>	 <b>3202</b>
 <b>3198 : CapFile</b> FrameNumber = 3197, MediaType = Eth		 <b>3199</b>	 <b>3200</b>	 <b>3201</b>	 <b>3202</b>



# Viewpoint Filter

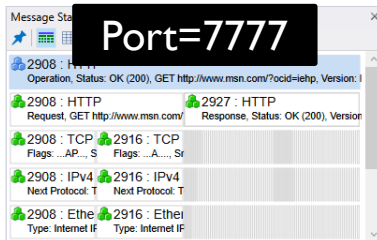
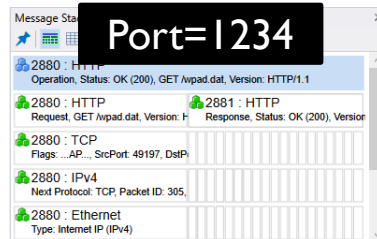
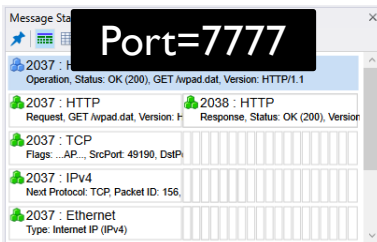
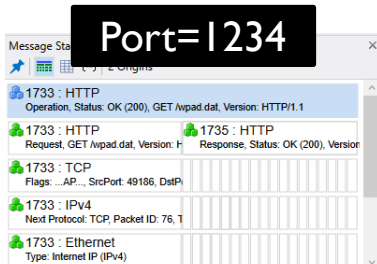
Viewpoint filters let you apply a filter at the top row under the viewpoint (blue line).

---

 3198 : TCP Flags: ...AP..., SrcPort: 49202, DstPort: H	 3199 Flags: ..	 3200 Flags: ..	 3201 Flags: ..	 3202 Flags: ..
 3198 : IPv4 Next Protocol: TCP, Packet ID: 382, Total	 3199 Next Pr	 3200 Next Pr	 3201 Next Pr	 3202 Next Pr
 3198 : Ethernet Type: Internet IP (IPv4)	 3199 Type: In	 3200 Type: In	 3201 Type: In	 3202 Type: In
 3198 : CapFile FrameNumber = 3197, MediaType = Ethe	 3199 FrameN	 3200 FrameN	 3201 FrameN	 3202 FrameN



# Filtering is Fast



View Filter: TCP.Port==1234

Requires looking at  
4 messages

Viewpoint Filter: TCP.SequenceNumber==1234

Requires looking at  
only the TCP  
fragments in the 2  
resulting Messages

# What's New with Message Analyzer

- ❑ Comparison Tools
- ❑ UI Workflow Improvements
- ❑ Parse As support
- ❑ Performance Improvements

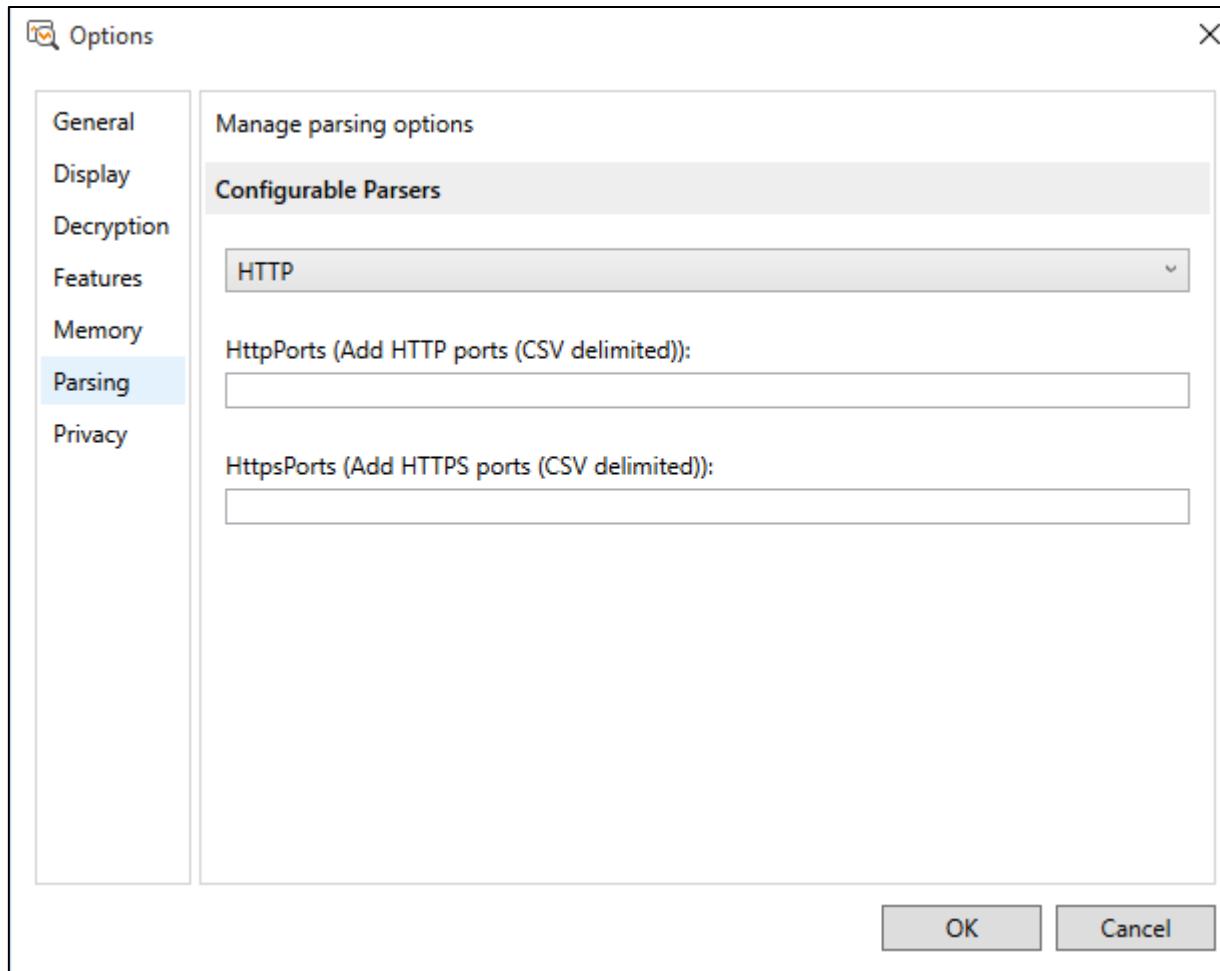
# Demo – Comparison Tools

Compare Fields (Preview) ×

Baseline: SMBPerf192.168.1.5Bad:106 , Current: SMBPerf192.168.1.5Bad:108

Field	Baseline	Current
Header.ProtocolId	4266872130	4266872130
Header.StructureSize	64	64
Header.CreditCharge	1	1
Header.Status.Sev	STATUS_SEVERITY_SUCCESS(0)	STATUS_SEVERITY_SUCCESS(0)
Header.Status.C	False	False
Header.Status.N	False	False
Header.Status.Facility	0	0
Header.Status.Code	0	0
Header.Command	SMB2SessionSetup(1)	SMB2SessionSetup(1)
Header.Credit	31	1
Header.Flags.SMB2FlagsServerToRedir	0	0
Header.Flags.SMB2FlagsAsyncCommand	0	0
Header.Flags.SMB2FlagsRelatedOperat...	0	0
Header.Flags.SMB2FlagsSigned	0	0
Header.Flags.SMB2FlagsPriorityMask	0	0
Header.Flags.SMB2FlagsDFSOperations	0	0
Header.Flags.SMB2FlagsReplayOperati...	0	0
Header.NextCommand	0	0
Header.MessageId	2	3
Header.Reserved2	65279	65279
Header.TreeId	0	0
Header.SessionId	0	4398046511125
Header.Signature	binary[0,0,0,0,0,0,0,0,0,0,0,0,0,0,0]	binary[0,0,0,0,0,0,0,0,0,0,0,0,0,0,0...

# Demo – Parse As



# Upcoming Features

To be updated later

# Useful Links

- ❑ Blog: <http://blogs.technet.com/MessageAnalyzer>
  - ❑ Latest Download
  - ❑ Videos
  - ❑ Support Forums