



STORAGE DEVELOPER CONFERENCE

SNIA ■ SANTA CLARA, 2014



An abstract background graphic in the top right corner consists of a grid of small, semi-transparent colored circles. The colors transition from light yellow and green on the left to bright blue and cyan on the right, creating a sense of depth and motion.

Evolution of Message Analyzer and Windows Interoperability

Paul Long
Microsoft

What is Message Analyzer?

blogs.technet.com/MessageAnalyzer

Administrator: Microsoft Message Analyzer

File Home Tools Charts

Restart Edit Shift Time New Viewer View Filter Quick Filter Aliases Unions Viewpoints Default Viewpoint Hide Operations Tool Windows Color Rules Choose Columns Find Messages View Layout View Options

Start Page Local Network In... Local Network In...

Module x - ContentType x

MessageNumber Timestamp TimeElapsed Source

Module (1): ARP

Module (7): HTTP

- ContentType (12): <Others>
- ContentType (2): application/json
- ContentType (8): application/x-javascript
- ContentType (4): image/gif
- ContentType (3): image/jpeg
 - 865 2014-07-25T12:08:44.7250306 0.0351415 Knoxie
 - 867 2014-07-25T12:08:44.7328338 0.0410250 Knoxie
 - 1008 2014-07-25T12:08:48.0621119 0.1443462 Knoxie
- ContentType (1): image/png

Local Network In...

Session Explorer

Local Network Interfaces (Win 8.1) Analysis Grid (664) Sequence Match (1,681) TCP Diagnosis with Stevens Format (1)

Stevens

Source Diagnoses

Source	Destination	SourcePort
131.107.255.86	Knoxie	HTTPS(443)
Knoxie	131.107.125.19	2342
Knoxie	168.62.21.37	4911
Knoxie	168.62.21.37	4913
Knoxie	Pauly's Wireless Hotel	4951
Knoxie	Pauly's Wireless Hotel	4953

*Set viewpoint to TCP

Message Stack

Details

MessageNumber: 1008 Module: HTTP Operation, Status: OK (200), GET /az/hprichbg/rb/BrugesCanals_EN-US64698481

Name	Value	Type	Bit Offset	Bit Length
Method	GET	String		
Uri	/az/hprichbg/rb/BrugesCanals_EN-U	HTTP.UriType		
Version	HTTP/1.1	String		
Status Code	200 (0x000000)	UInt32		
Reason Phrase	OK	String		
Content Type	image/jpeg	String		
Content Encoding		String		

Field Data

image/jpeg

Field Data Output

Ready Session Total: 1,681 Available: 664 Selected: 1 Viewpoint: Default

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

The screenshot shows the Microsoft Message Analyzer interface. A red arrow points to the 'Start' button in the top-left corner of the main window. The main area displays a news feed titled 'Start Page News' with several items:

- Message Analyzer Blog Updates!** (10/22/2013 1:00:00 PM)
We've recently updated our blog with several new posts as listed below. Click on the title above to visit our blog!
 - Configuring Message Analyzer to effectively work with large data sets
 - Customize column layouts to view data that matters to you
 - Capture from remote machines and VMs
 - Why Message Analyzer is so different from Network Monitor
- Message Analyzer has Released** (9/25/2013 1:00:00 PM)
Message Analyzer has officially released to the Microsoft Download center. Click on the title above to read our blog post on the release and find the link to the download.
- New Blog Post: Network Capture is Dead!** (3/4/2013 12:00:00 PM)
Come visit our blog to learn about the trace capture experience on Message Analyzer. Message Analyzer not only captures network traces through an NDIS Filter driver as with Network Monitor, but has been enhanced to support network trace capturing at the Firewall and HTTP proxy level and also capturing any type of ETW (Event Tracing for Windows) events such as USB and Bluetooth.
- Message Analyzer Blog** (1/29/2013 12:00:00 PM)
Come follow our blog as we discuss how to take advantage of Message Analyzer and all of its new features to troubleshoot and analyze Network, Event Tracing, and Text based logs. We have posts on how to use filtering and grouping in Message Analyzer, so come take a look at <http://blogs.technet.com/MessageAnalyzer> by clicking on the title above.
- Reporting Problems** (9/20/2012 1:00:00 PM)
We really appreciate it when you take time to report issues to us. We promise to read and respond to every report. For us to do our best work, this is what we need from you:
 - A problem description, including what you experienced and what you expected to experience
 - Steps for reproducing the problem
 - For further analysis, traces are copied to the clipboard automatically when Message Analyzer crashes and can be pasted directly into the report

Below the news feed, there are three tabs: 'Message Stack', 'Details', and 'Output'. The 'Output' tab is currently selected and shows a list of loaded modules with their progress status:

Module	Progress
'WPPActors_826a1fc97e3f82bb95'	Loaded cached module
'PAC_37f96a0aca94fd091451629ea9e'	Loaded cached module
'EAPOL_04284f6eade6cc21297f5c35'	Loaded cached module
'PTP_Fe0c039359b56c4c6e4ab4e615'	Loaded cached module
'KKDCP_51018ee79c088185ca509e84'	Loaded cached module
'SIM_1e515b87077d57499563beeb87'	Loaded cached module
'RDP_EOD1_3db929f83e5a35d769b29d'	Loaded cached module
'EPM_30ed56808bd1c6b68df570e455'	Loaded cached module
'Netmon_6795f67a9236b768616aFa0t'	Loaded cached module
'PCCRRA_a215fdd6e27b16560be8eeef'	Loaded cached module
'PCCRD_f4afbd4dd62fa345d7394a821'	Loaded cached module
'DNSP_00effd5c28e6ed9800ff88e18a6c'	Loaded cached module
'CapFileActors_d7368005e40853bf1'	Loaded cached module
'FCIADS_7c88fc4f1be983f189d62e9a'	Loaded cached module

At the bottom of the interface, there are status bars for 'Ready', 'Session Total: 0', 'Available: 0', 'Selected: 0', 'Viewpoint:', 'Parsing Level:', and a timestamp 'Build: 4.0.7052.0'. The page number '5' is located in the bottom right corner.

Demo: A quick tour

The screenshot shows the Microsoft Message Analyzer interface. At the top, there's a ribbon menu with tabs like File, Home, Tools, and Charts. Below the ribbon, there's a toolbar with various icons for operations like Restart, Stop, View Filter, and Viewpoints. A large red arrow points down from the ribbon area towards the main content area.

The main content area is divided into two sections:

- Start Page**: This section contains a news feed with items like "Subscribed Feeds" and "OPN ParserS".
- SETTINGS**: This section is where the configuration changes are made.

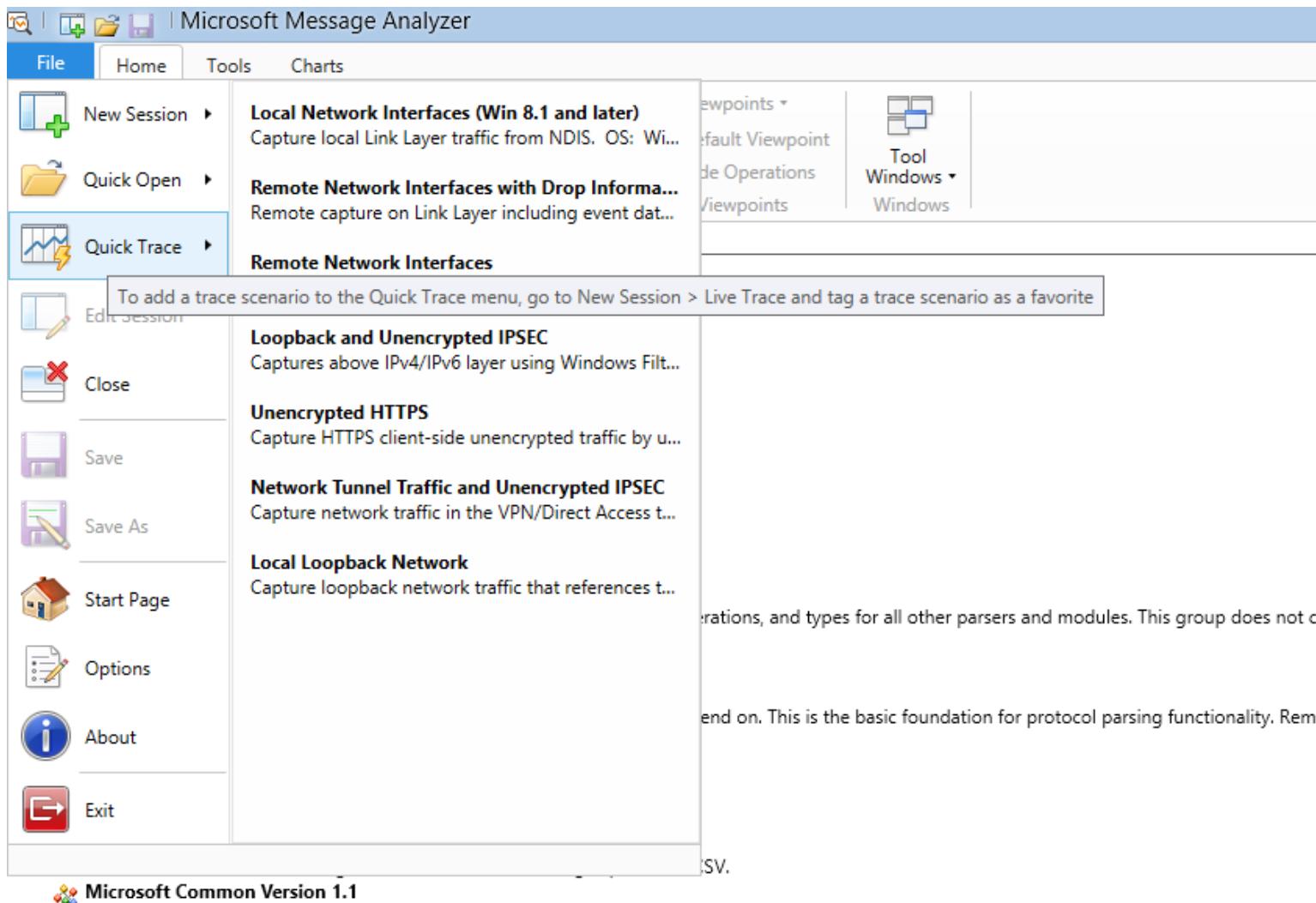
On the right side of the interface, there's a list of parser configurations, each with a status icon (green circle with "Online") and a delete icon (cross). Two specific items are highlighted with red arrows and boxes:

- Synchronized**: A green box surrounds the first item in the list.
- Not Synchronized**: A blue box surrounds the second item in the list.

At the bottom of the interface, there are several panes: "Message Stack", "Details", and "Output". The "Output" pane shows a list of assembly loading progress messages.

```
Progress: Loaded cached module 'T125_a165b25743895105'
Progress: Loaded cached assembly '__PropertyModule_53'
Progress: Loaded cached module 'T124_a6604590e2e7c684'
Progress: Loaded cached assembly '__PropertyModule_34'
Progress: Loaded cached assembly '__PropertyModule_39'
Progress: Loaded cached assembly '__PropertyModule_e3'
Progress: Loaded cached module 'PublicResources_3d79e'
Progress: Loaded cached assembly '__PropertyModule_0f'
Progress: Loaded cached module '__PropertyModule_3a'
Progress: Loaded cached module 'PcapFile_14a3599ab5f3'
Progress: Loaded cached assembly '__PropertyModule_fa
Progress: Loaded cached assembly '__PropertyModule_8f'
```

Demo: A quick tour



Demo: A quick tour

Microsoft Message Analyzer

File Home Tools Charts

Restart Stop Shift Time View Filter Quick Filter Aliases Unions Viewpoints Default Viewpoint Hide Operations Tool Windows Color Rules Choose Columns Find Messages View Layout View Options

Start Page testingfrommym... N1NetTrace: An...

Right click on any column header and select 'Group' to create a grouping. x

MessageNumber	Timestamp	TimeElapsed	Source	Destination	Module	Summary
1274	2014-08-22T13:57:22.9725879		157.59.130.242	255.255.255.255	UDP	SrcPort: 17500, DstPort: 17500, Length: 121
1275	2014-08-22T13:57:22.9731900		157.59.130.242	157.59.131.255	UDP	SrcPort: 17500, DstPort: 17500, Length: 121
1276	2014-08-22T13:57:22.9818164		157.59.129.97	239.255.255.250	SSDP	Request, Method: NOTIFY, URI: *, Version: 1.1
1277	2014-08-22T13:57:22.9820496		FE80:0:0:0:2918:1EE:D90:7DFF	FF02:0:0:0:0:0:C	SSDP	Request, Method: NOTIFY, URI: *, Version: 1.1
1281	2014-08-22T13:57:23.0293876	0.0489101	10.200.48.181	157.59.129.15	TLS	Records: [ApplicationData(Encrypted)]
1282	2014-08-22T13:57:23.0433698	0.0192218	2A01:111:F400:5014:0:0:2	2001:4898:28:5:BC38:801B:BE16:26F4	TLS	Records: [ApplicationData(Encrypted)]
1283	2014-08-22T13:57:23.0454838	0.0171441	2A01:111:F400:2814:0:0:2	2001:4898:28:5:BC38:801B:BE16:26F4	TLS	Records: [ApplicationData(Encrypted)]
1286	2014-08-22T13:57:23.0775696		B4-0E-DC-3C-30-72	FF-FF-FF-FF-FF-FF	Ethernet	Type: Realtek Semiconductor Corp.
1288	2014-08-22T13:57:23.1712817		157.59.130.124	157.59.131.255	NBTNS	Query Request, QuestionName: WPAD <0x00> Workstat
1289	2014-08-22T13:57:23.1805205		157.59.129.3	157.59.128.1	ARP	REQUEST, SenderIP: 157.59.129.3, TargetIP: 157.59.1
1290	2014-08-22T13:57:23.2367284		157.59.128.125	157.59.130.155	ARP	REQUEST, SenderIP: 157.59.128.125, TargetIP: 157.59
1291	2014-08-22T13:57:23.2456669		157.59.128.115	157.59.131.62	ARP	REQUEST, SenderIP: 157.59.128.115, TargetIP: 157.59
1292	2014-08-22T13:57:23.2629917		157.59.129.97	239.255.255.250	SSDP	Request, Method: NOTIFY, URI: *, Version: 1.1
1293	2014-08-22T13:57:23.2633931		FE80:0:0:0:2918:1EE:D90:7DFF	FF02:0:0:0:0:0:C	SSDP	Request, Method: NOTIFY, URI: *, Version: 1.1
1294	2014-08-22T13:57:23.2871274		157.59.130.120	157.59.131.255	NBTNS	Query Request, QuestionName: XRR0000AAF33ADA <0x0>
1295	2014-08-22T13:57:23.3037457		B4-0E-DC-3C-2C-62	FF-FF-FF-FF-FF-FF	Ethernet	Type: Realtek Semiconductor Corp.
1296	2014-08-22T13:57:23.3049086		FE80:0:0:0:28F8:72DF:373:387A	FF02:0:0:0:0:1:2	DHCPv6	SOLICIT, TransID: 0x006EBD74
1297	2014-08-22T13:57:23.3229143	0.0014529	2001:4898:28:5:BC38:801B:BE16:26F4	2001:4898:C8:A:C92F:D284:F0F7:37C1	DFS	Get DFC Referral, MaxReferralLevel: 4, RequestFileName
1299	2014-08-22T13:57:23.3252321	0.0030493	2001:4898:28:5:BC38:801B:BE16:26F4	2001:4898:C8:A:C92F:D284:F0F7:37C1	SMB2	Create, Status: Success, FileName: products\PUBLIC
1302	2014-08-22T13:57:23.3347803	0.0025631	2001:4898:28:5:BC38:801B:BE16:26F4	2001:4898:C8:A:C92F:D284:F0F7:37C1	SMB2	Create, Status: STATUS_OBJECT_NAME_NOT_FOUND, FileName
1305	2014-08-22T13:57:23.3383157	0.0020436	2001:4898:28:5:BC38:801B:BE16:26F4	2001:4898:C8:A:C92F:D284:F0F7:37C1	SMB2	Create, Compounded, Status: Success, FileName: prod
1305	2014-08-22T13:57:23.3383157	0.0020436	2001:4898:28:5:BC38:801B:BE16:26F4	2001:4898:C8:A:C92F:D284:F0F7:37C1	SMB2	QueryDirectory, Compounded, Status: Success, FileId
1305	2014-08-22T13:57:23.3383157	0.0020436	2001:4898:28:5:BC38:801B:BE16:26F4	2001:4898:C8:A:C92F:D284:F0F7:37C1	SMB2	QueryDirectory, Compounded, Status: STATUS_NO_MORE_
1308	2014-08-22T13:57:23.3417800		2001:4898:C8:A:C92F:D284:F0F7:37C1	2001:4898:28:5:BC38:801B:BE16:26F4	SMB2	Compounded Messages
1307	2014-08-22T13:57:23.3406981	0.0018504	2001:4898:28:5:BC38:801B:BE16:26F4	2001:4898:C8:A:C92F:D284:F0F7:37C1	SMB2	ErrorResponse, Status: STATUS_PENDING
1311	2014-08-22T13:57:23.3698138		FE80:0:0:0:4032:1292:8F47:103B	FF02:0:0:0:0:1:2	DHCPv6	Close, Status: Success, FileId: 0x0000005D00EEDED8
			157.59.129.2	157.59.129.2	NBTNS	SOLICIT, TransID: 0x00907782

Session Explorer

- testingfrommymachine (1,350)
 - Analysis Grid (1,261)
- N1NetTrace (6,150)
 - Analysis Grid (3,273)

Message Stack

No Origins

QueryDirectory, Compounded, Status: Success, Filed: 0xFFFFFFFFFFFFFF, SearchPattern: *, FileInformationClass: FileIdBothDir

Details

MessageNumber: 1305 Module: SMB2
QueryDirectory, Compounded, Status: Success, Filed: 0xFFFFFFFFFFFFFF, SearchPattern: *, FileInformationClass: FileIdBothDir

Name	Value	Type	Bit Offset	Bit Length
FileId	Persistent =	SMB2.SMB2FileId		
FileInformationClass	FileIdBothDir..FileInformationClasses			
Buffer	*	String		
Status	STATUS_SUCCE... ERREF.NTSTATUS			

Output

```
Progress: Recompiling module assembly 'WinInet'
Progress: Module assembly saved 'C:\Users\Paul\AppData\Local\Temp\WinInet\WinInet.dll'
Progress: Loaded cached assembly 'WinInet_11d9e6c63e7'
Progress: Recompiling module assembly 'Windows_Kernel'
Progress: Module assembly saved 'C:\Users\Paul\AppData\Local\Temp\Windows_Kernel\Windows_Kernel.dll'
Progress: Loaded cached assembly 'Windows_Kernel_Trace'
Error: do not know how to establish stage 'Imported'
Modules: Loaded: Errors or warnings were found when loading module 'WinInet.dll'
Progress: Loaded cached assembly 'WindowsReference_SF'
Progress: Loaded cached assembly 'IGW_ddf96e9Bdf829c'
Progress: Loaded cached assembly 'PublicResources_3d7'
Progress: Loaded cached assembly 'NTP_48ee1ac6d2a305'
```

Bookmarks Output Field Data

Message Data Selection

Ready Session Total: 1,350 Available: 1,261 Selected: 1 Viewpoint: Default Parsing Level: Build: 4.0.7052.0

Demo: A quick tour

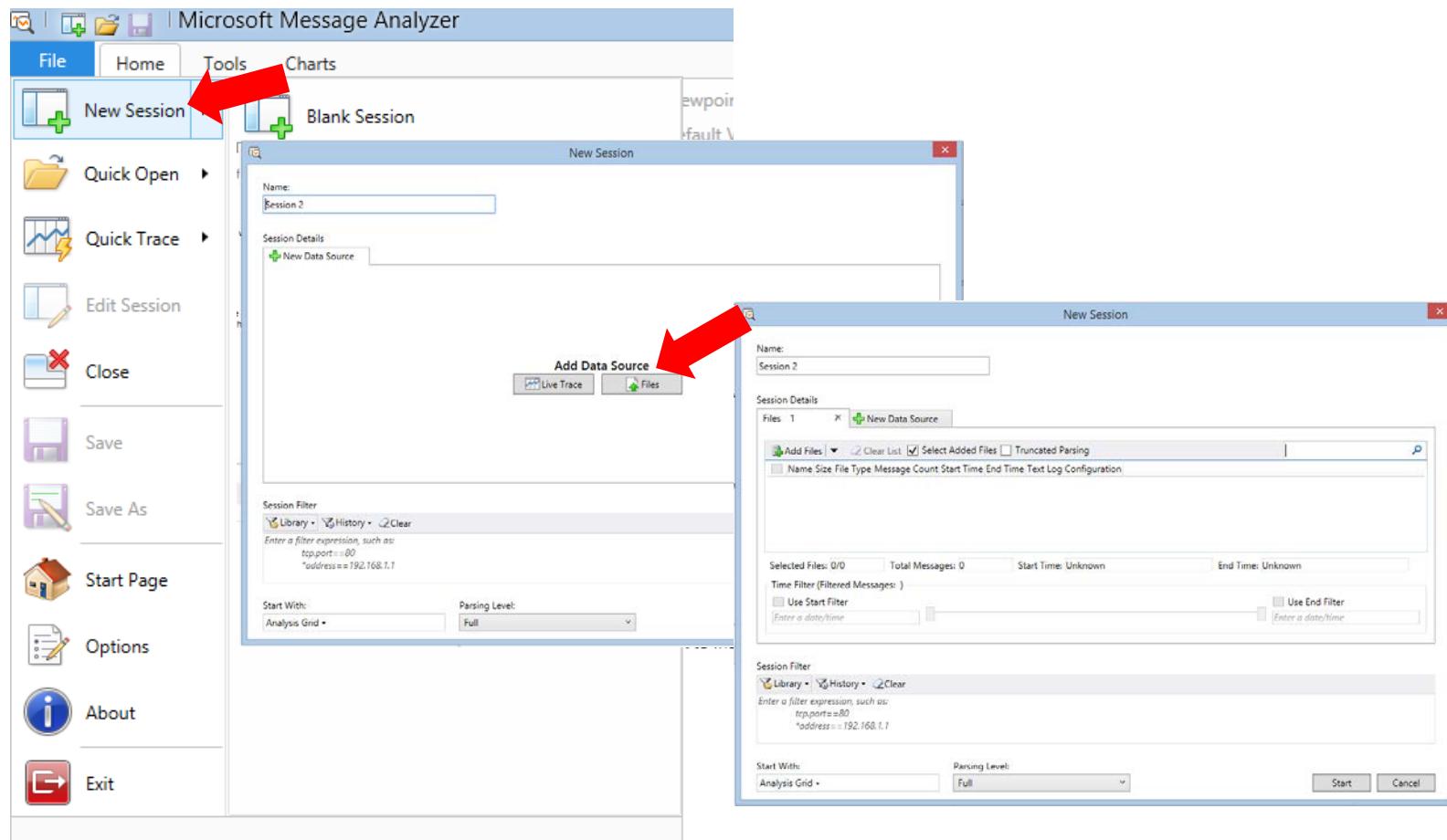
The screenshot shows the Microsoft Message Analyzer interface with several tools overlaid:

- Actions**: A red arrow points from the "Actions" button in the toolbar to the "View Filter Tool".
- Trace Viewer**: A large red arrow points from the "Message Number" column header to the "Session Explorer" pane.
- Message Stack Tool**: A red arrow points from the "Message Stack" tool in the bottom-left to the "Message Stack" tool in the bottom-right.
- Message Detail Tool**: A red arrow points from the "Details" table in the bottom-center to the "Message Detail" tool in the bottom-right.
- Various Stacked Tools**: A red arrow points from the "Output" pane in the bottom-right to the "Output" tab in the bottom-right.

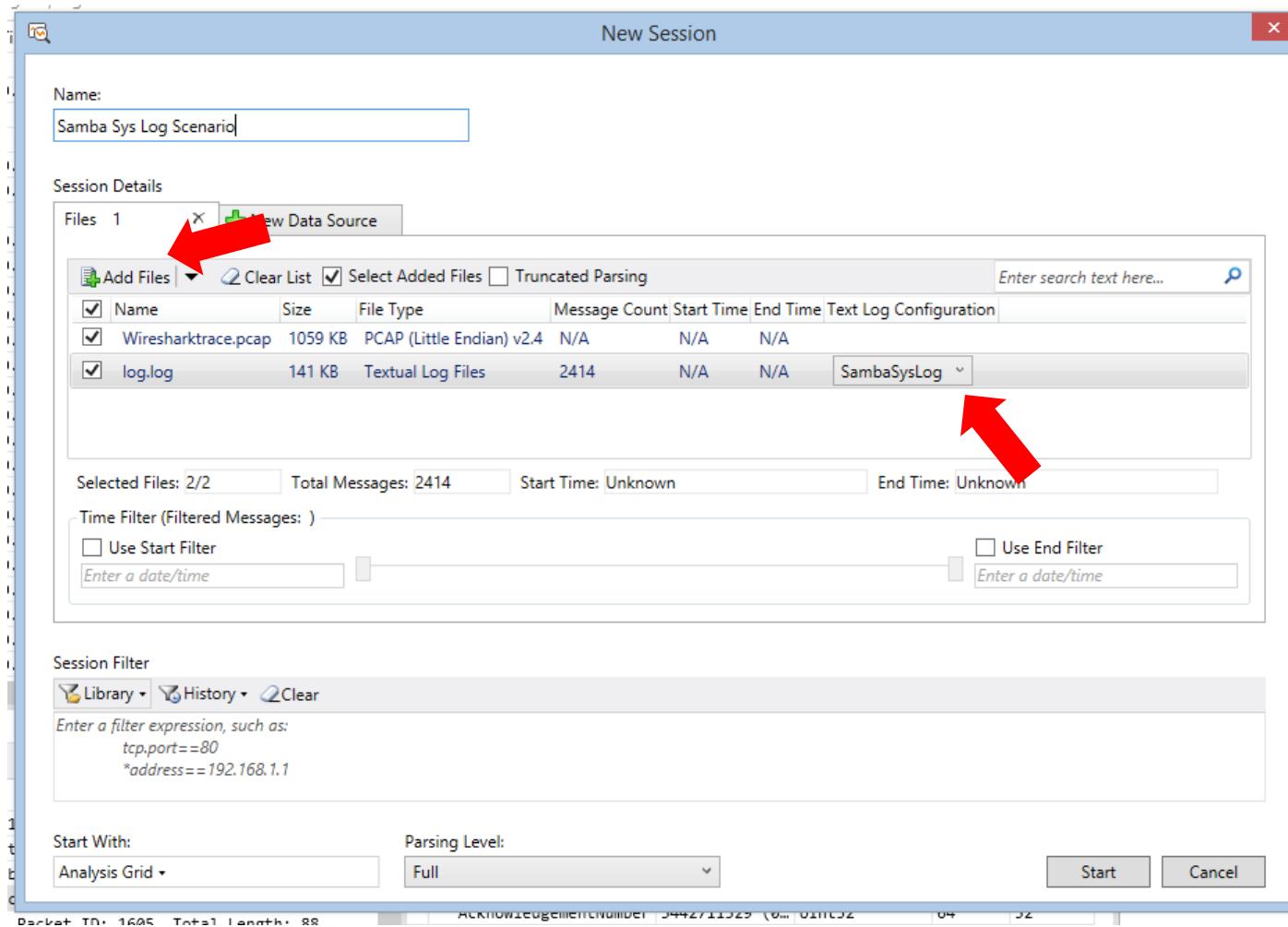
Key UI elements visible in the interface include:

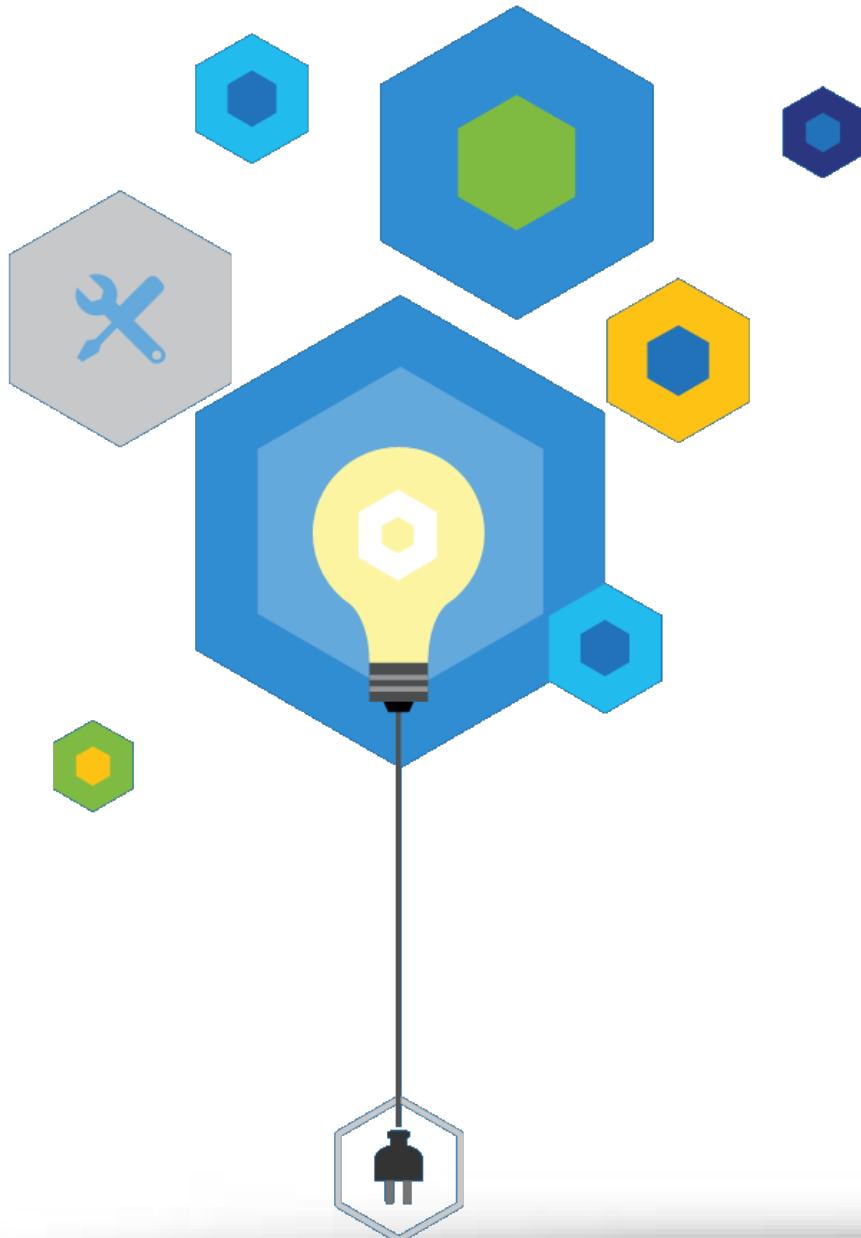
- Toolbar**: File, Home, Tools, Charts, Shift Time, New Viewer, Viewpoints, Windows, Viewer, Color, Choose, Find, View.
- Session Explorer**: Shows sessions like "testingfrommymachine (1,350)" and "N1NetTrace (6,150)".
- Analysis Grid**: Shows network traffic details with columns: MessageNumber, Timestamp, TimeElapsed, Source, Destination, Module, Summary.
- View Filter**: A floating window for filtering messages.
- Status Bar**: Session Total: 1,350, Available: 1,261, Selected: 1.

Demo: A quick tour



Demo: A quick tour





Demo: Correlation with Multiple Logs

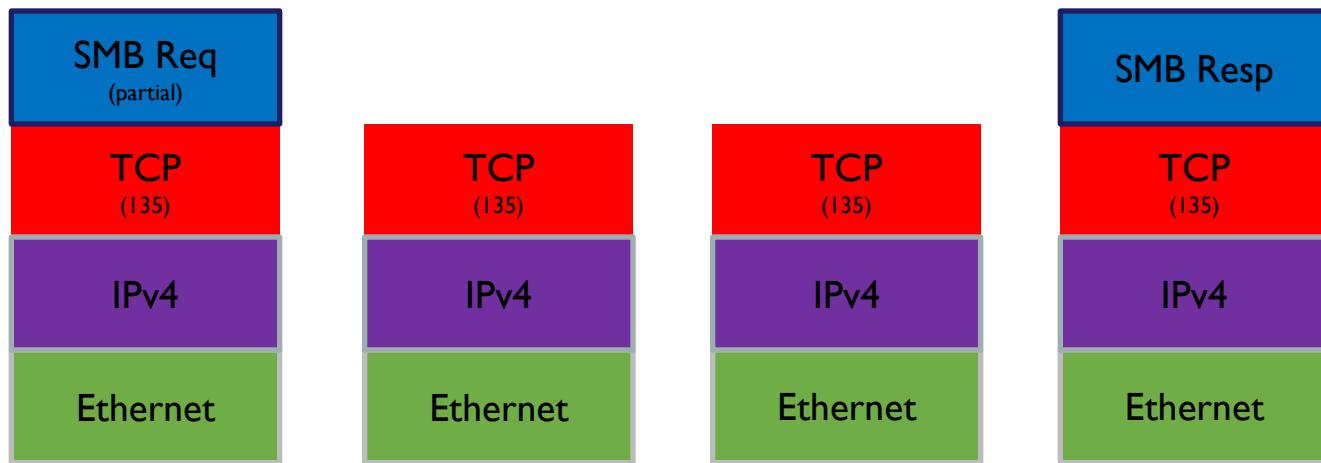


Differences

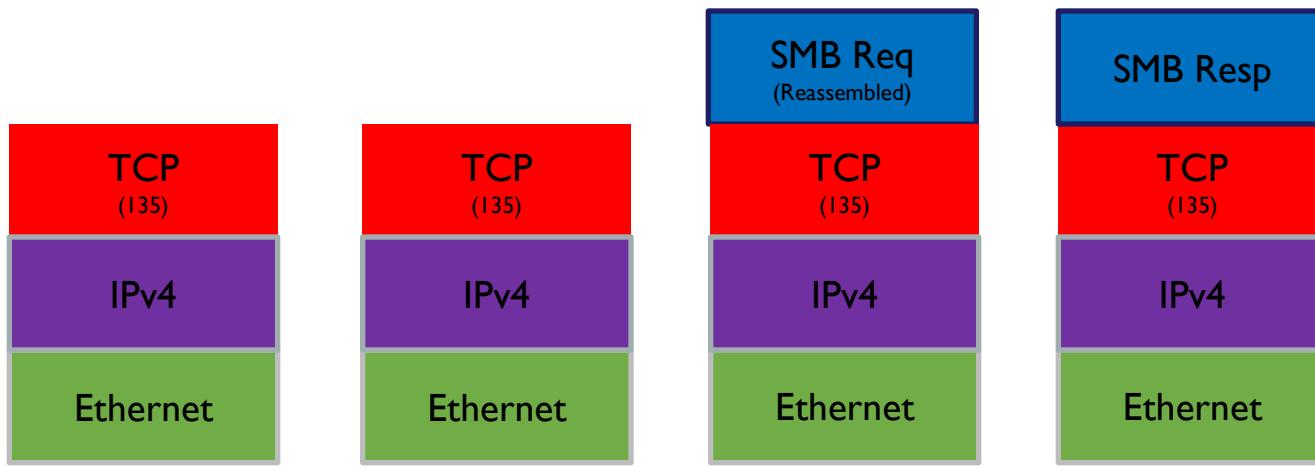


- **Fully Reassemble**
 - TCP, HTTP and all layers
 - Fragments hidden
- **Group Operations**
 - Request/Response
 - Measure response times
- **Automatic Diagnoses**
 - TCP diagnosis show as info
 - Validation and Protocol Behavior

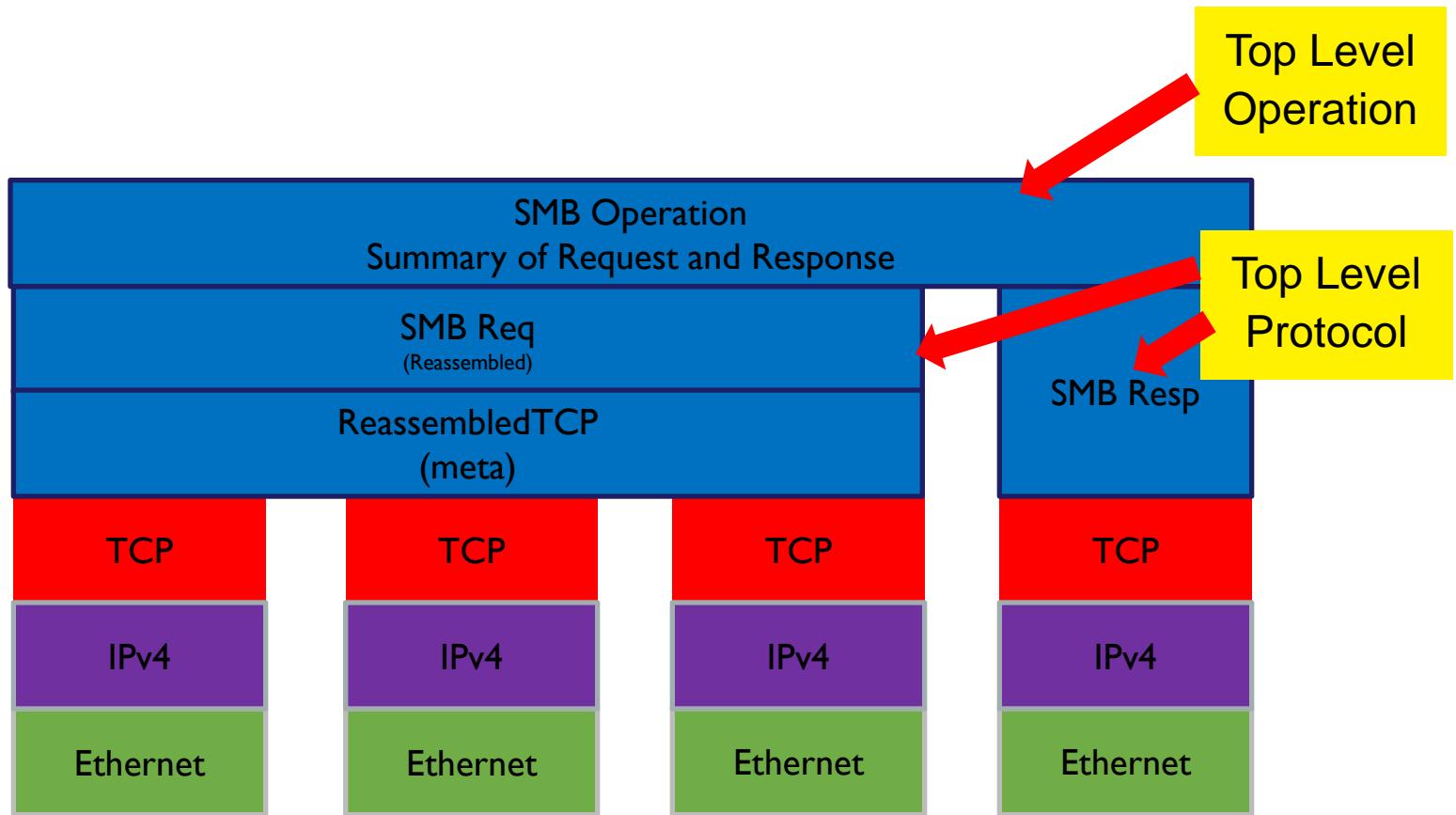
Differences – Netmon



Differences – Wireshark



Differences – Message Analyzer



Administrator: Microsoft Message Analyzer

File Home Tools Charts Start Page Local Network In... OneHTTP : Analy... X

Right click on any column header and select 'Group' to create a grouping. X

MessageNumber	Timestamp	TimeElapsed	Source	Destination	Module	Summary
1	2014-07-25T12:08:48.0621119	0.1443462	Knoxie	www.bing.com	HTTP	Operation, Status: OK (200), GET /az/hprichbg/rb/BrugesCanals_EN-US646984...

Ready Session Total: 173 Available: 1 Selected: 1 Viewpoint: Default Truncated: No Parsing Level: Build: 4.0.7028.0

Microsoft Network Monitor 3.4 - E:\Users\Paul\Documents\Work\Captures\MessageVisualStackBug\OneHTTP.cap

File Edit View Frames Filter Experts Tools Help

New Capture Open Capture Save As Reassemble

OneHTTP.cap Start Page Parsers

Network Conversations

- All Traffic
 - Other Traffic
 - IPv4 (192.168.1.18 - 204.79.197.200) ConvID

Frame Summary

Time Of Day	Time Date Local Adjusted	Time Offset	Time Local Adjusted	Process Name	Source	Destination	Protocol Name	Description
Not Applicable	12:08:48 PM 7/25/2014	0.0000000	12:08:48.0621119		192.168.1.18	204.79.197.200	HTTP	HTTP:Request, GET /az/hprichbg/rb/BrugesCanals_EN-US646984...
Not Applicable	12:08:48 PM 7/25/2014	0.0325464	12:08:48.0946583		204.79.197.200	192.168.1.18	HTTP	HTTP:Response, HTTP/1.1, Status: Ok, URL: /az/h...
Not Applicable	12:08:48 PM 7/25/2014	0.0326157	12:08:48.0947276		192.168.1.18	204.79.197.200	TCP	[Bad CheckSum]Flags=.,A...,SrvPort=494...
Not Applicable	12:08:48 PM 7/25/2014	0.0326204	12:08:48.0956323		204.79.197.200	192.168.1.18	TCP	TCP:[Continuation to #2]Flags=.,A...,SrvPort=494...
Not Applicable	12:08:48 PM 7/25/2014	0.0326596	12:08:48.0956815		192.168.1.18	204.79.197.200	TCP	[Bad CheckSum]Flags=.,A...,SrvPort=494...
Not Applicable	12:08:48 PM 7/25/2014	0.0345431	12:08:48.0966550		204.79.197.200	192.168.1.18	TCP	TCP:[Continuation to #2]Flags=.,A...,SrvPort=494...
Not Applicable	12:08:48 PM 7/25/2014	0.0345469	12:08:48.0966588		204.79.197.200	192.168.1.18	TCP	TCP:[Continuation to #2]Flags=.,A...,SrvPort=494...
Not Applicable	12:08:48 PM 7/25/2014	0.0346406	12:08:48.0967525		192.168.1.18	204.79.197.200	TCP	[Bad CheckSum]Flags=.,A...,SrvPort=494...

Version 3.4.2350.0 Displayed: 173 Captured: 173 Focused: Selected:

OneHTTP.cap

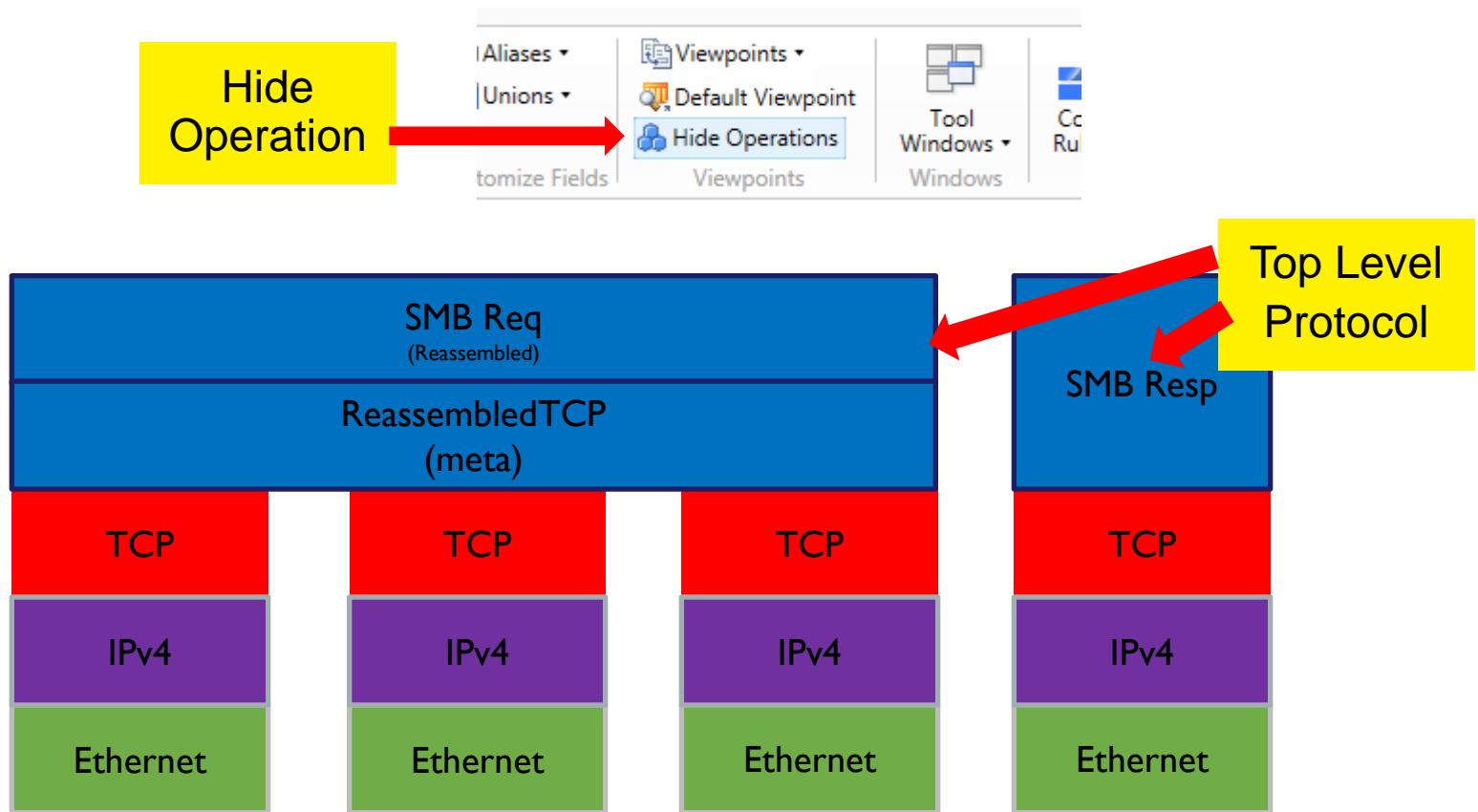
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter Expression... Clear Apply Save

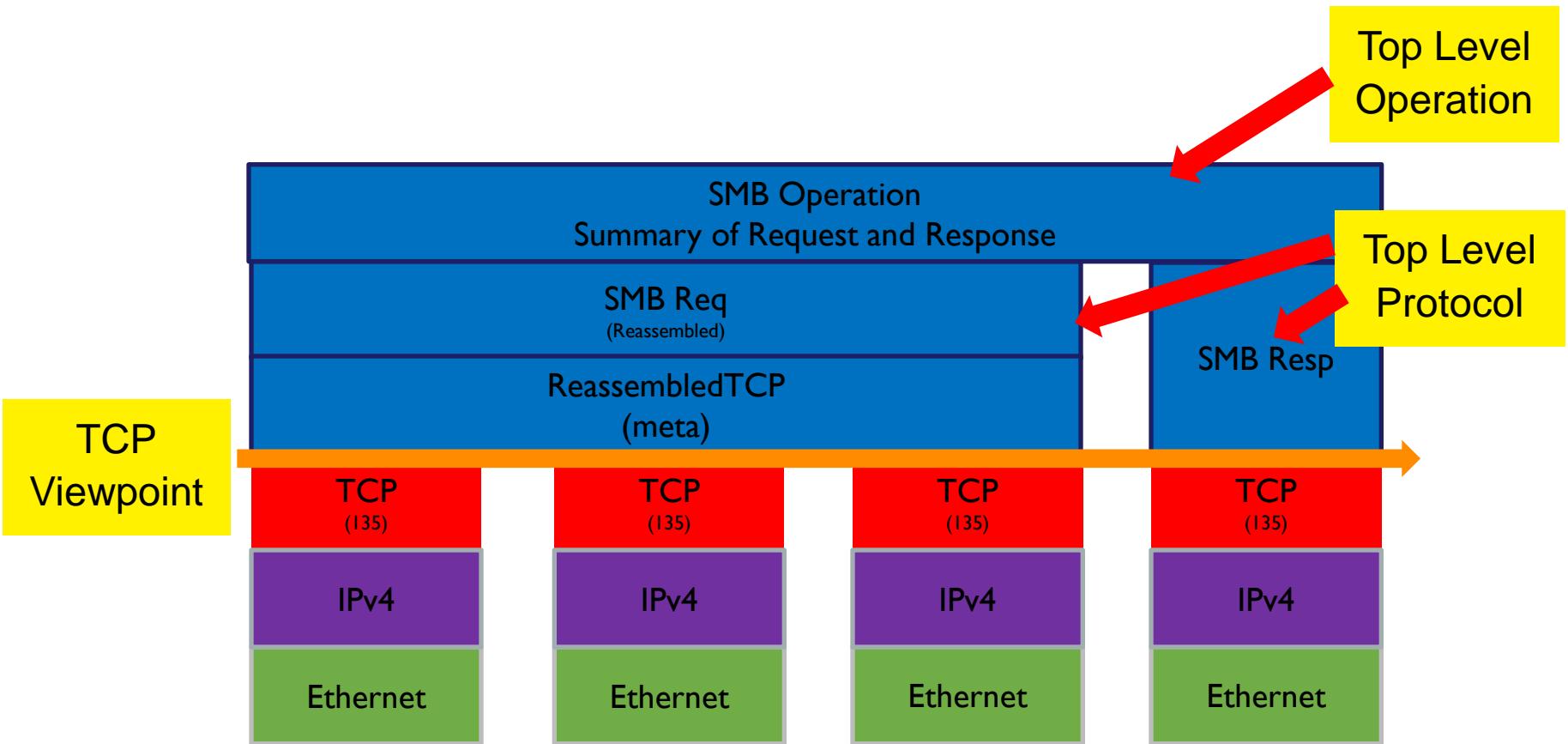
No.	Time	Source	Destination	Protocol	Info
1	0.000000000	192.168.1.18	204.79.197.200	HTTP	GET /az/hprichbg/rb/BrugesCanals_EN-US6469848102_1366x768.jpg HTTP/1.1 [TCP segment of a reassembled PDU]
2	0.032546000	204.79.197.200	192.168.1.18	TCP	4946 > http [ACK] seq=1268 Ack=1461 win=65535 Len=0
3	0.000069000	192.168.1.18	204.79.197.200	TCP	4946 > http [ACK] seq=1268 Ack=2921 win=65535 Len=0
4	0.000090500	204.79.197.200	192.168.1.18	TCP	[TCP segment of a reassembled PDU]
5	0.0000049000	192.168.1.18	204.79.197.200	TCP	4946 > http [ACK] seq=1268 Ack=2921 win=65535 Len=0
6	0.0000974000	204.79.197.200	192.168.1.18	TCP	[TCP segment of a reassembled PDU]
7	0.0000003000	204.79.197.200	192.168.1.18	TCP	[TCP segment of a reassembled PDU]
8	0.0000094000	192.168.1.18	204.79.197.200	TCP	4946 > http [ACK] seq=1268 Ack=5841 win=65535 Len=0
9	0.004744000	204.79.197.200	192.168.1.18	TCP	[TCP segment of a reassembled PDU]
10	0.0000002000	204.79.197.200	192.168.1.18	TCP	[TCP segment of a reassembled PDU]
11	0.0000002000	204.79.197.200	192.168.1.18	TCP	[TCP segment of a reassembled PDU]
12	0.0000003000	204.79.197.200	192.168.1.18	TCP	[TCP segment of a reassembled PDU]
13	0.000001000	204.79.197.200	192.168.1.18	TCP	[TCP segment of a reassembled PDU]

File: "E:\Users\Paul\Documents\Work\Captures\MessageVisualStackBug\OneHTTP.cap" 197... Packets: 173 - Displayed: 173 (100.0%) - Load time: 0:00.095 Profile: Default

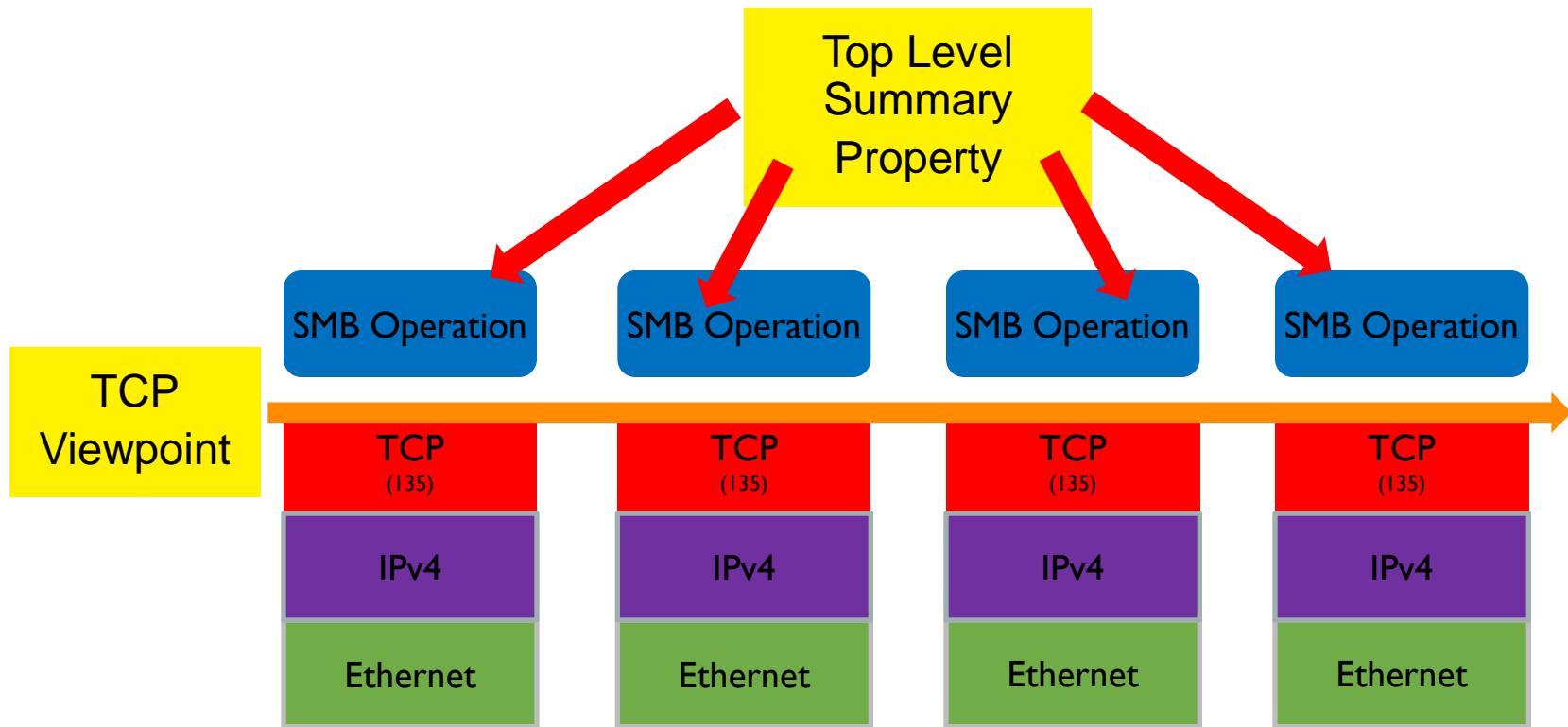
Differences – Message Analyzer



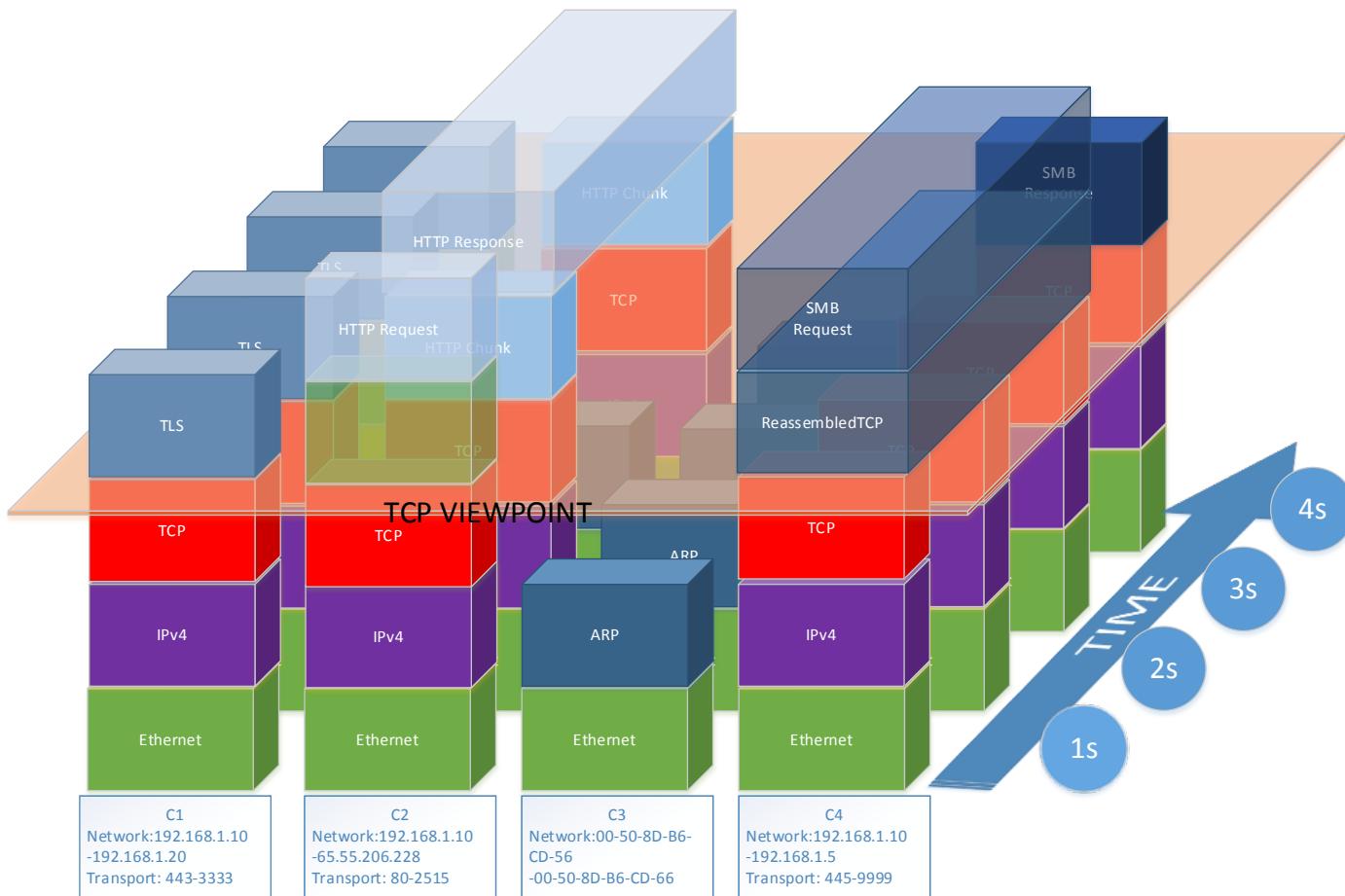
Differences – Message Analyzer



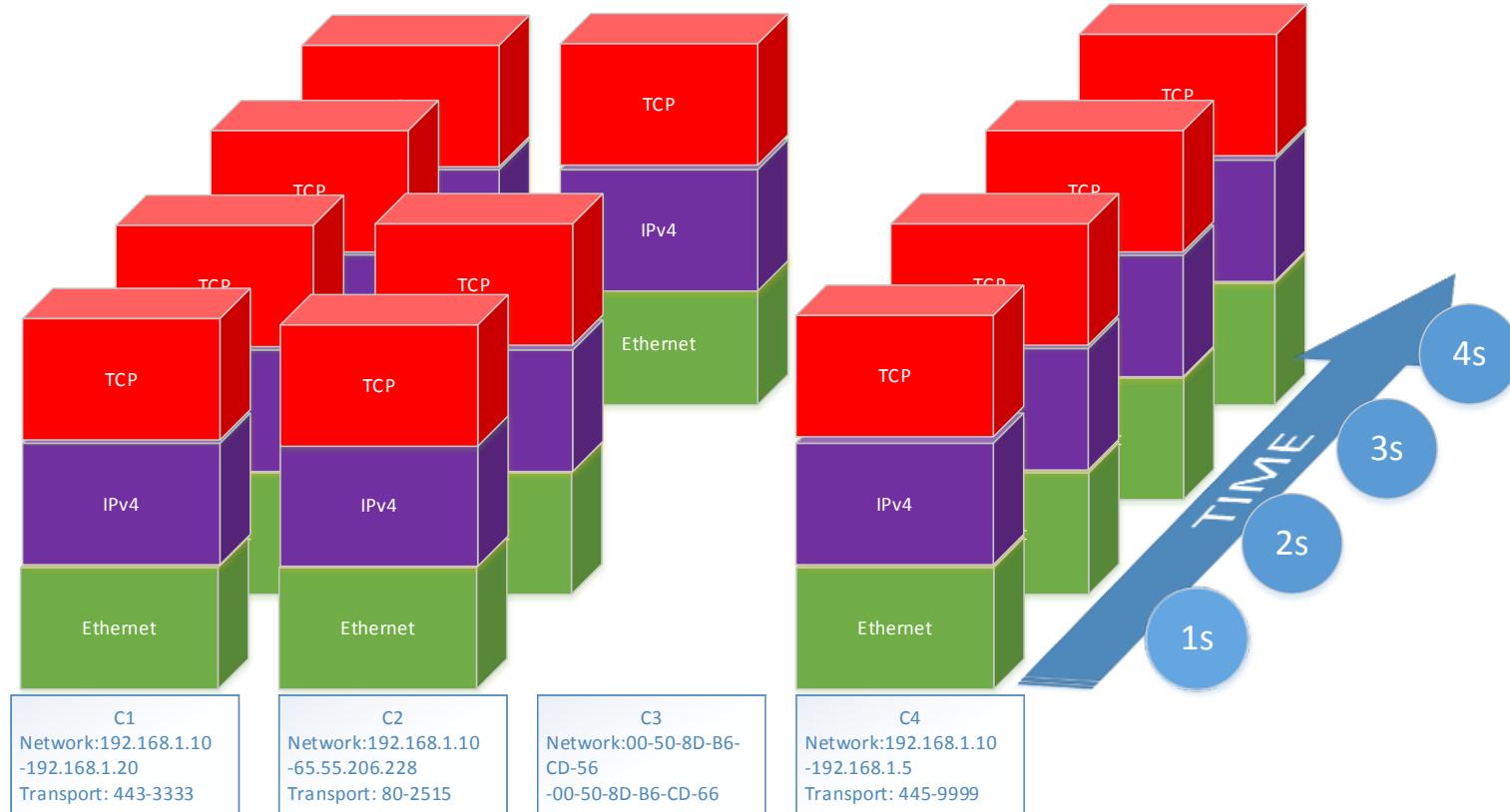
Differences – Message Analyzer



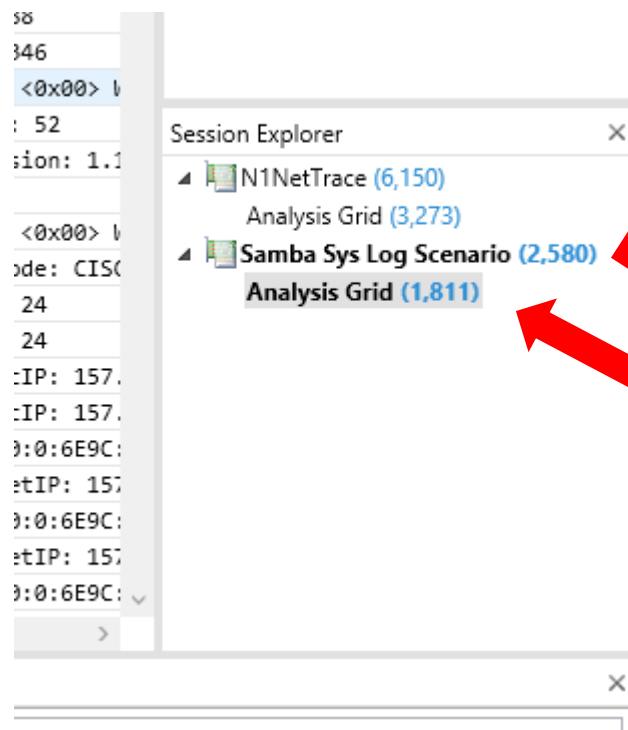
Differences – Message Analyzer in 3D



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

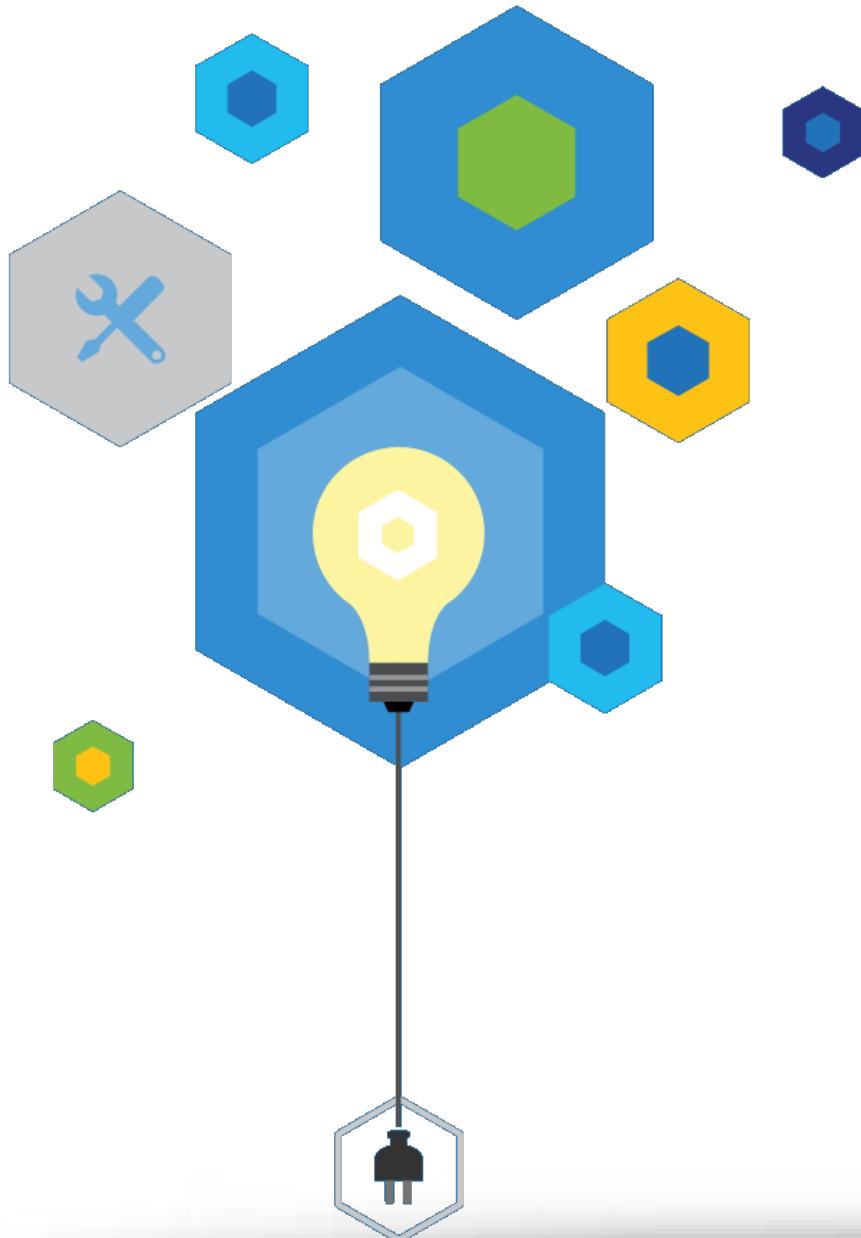
Total Number after data is reassembled and summarized with operations.



Encrypted Tracing

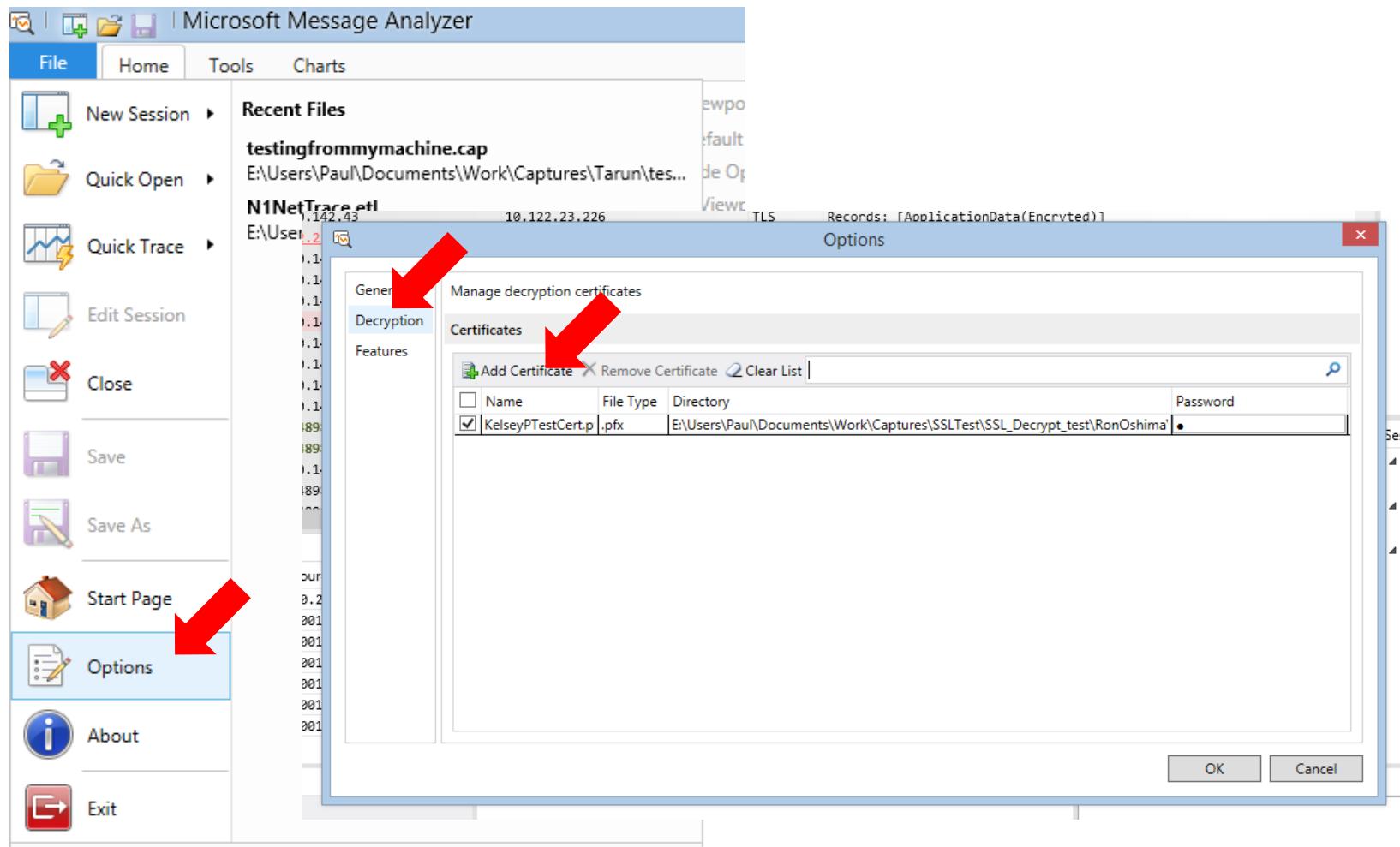
Dealing with Encrypted Traffic

- ❑ Capture before encryption
 - ❑ HTTPS
 - ❑ IPSEC
 - ❑ SMB
 - ❑ SMB Direct
- ❑ Decrypt a trace afterwards



Demo: Post Decryption

Decrypting a trace



Decrypting a trace

The screenshot shows the Microsoft NetworkMiner interface. A black callout box in the top-left corner contains the text "Decryption Tool can be docked anywhere." with a red arrow pointing to the left edge of the main window. In the top-right corner, there is a toolbar with several icons. A red arrow labeled '1' points to the "Tool Windows" icon. Another red arrow labeled '2' points to the "Decryption" icon in the dropdown menu that appears when the "Tool Windows" icon is clicked. The main pane displays two tables of network traffic data. The bottom table is titled "Decryption" and includes columns for "Decrypted Message Count", "Undecrypted Message Count", and "Message". The bottom-right section of the interface shows a preview of decrypted data, with a tooltip explaining it: "Shows decryption information for the active view".

Decryption Tool can be docked anywhere.

Decryption

Type	TimeStamp	ProtocolVersion	SourcePort	DestinationPort	SourceAd
i Info	9/10/2010 4:49:45 PM	N/A	3389	63828	10.200.1
i Info	9/10/2010 4:49:43 PM	N/A	64050	443	2001:489
i Info	9/10/2010 4:49:43 PM	N/A	64052	443	2001:489
i Info	9/10/2010 4:49:44 PM	N/A	64053	443	2001:489
i Info	9/10/2010 4:49:43 PM	N/A	64051	443	2001:489
i Info	9/10/2010 4:49:43 PM	N/A	64054	443	2001:489
i Info	9/10/2010 4:49:44 PM	N/A	64055	443	2001:489

Decrypted Message Count	Undecrypted Message Count	Message
90	0	Decryption Failed
0	0	Decrypted

Start Page N1NetTrace : An... testingfrommy... Session 4 : Analy... X

Right click on any column header and select 'Group' to create a grouping. X

Decryption

Shows decryption information for the active view

MessageNumber	Timestamp	TimeElapsed	Source	Destina
90	2010-09-10T12:49:30.2618638		10.20...	10.2...
89	2010-09-10T12:49:30.2609108		10.20...	10.2...
83	2010-09-10T12:49:30.2388952		10.20...	10.1...
76	2010-09-10T12:49:30.1388833	0.0003600	10.20...	10.1...
73	2010-09-10T12:49:30.0388710		10.20...	10.1...
72	2010-09-10T12:49:29.9892621		10.20...	10.2...
71	2010-09-10T12:49:29.9788623	0.5813949	2001...	c074...
69	2010-09-10T12:49:29.9388590	0.0003501	10.20...	10.1...
68	2010-09-10T12:49:29.9200320		10.20...	10.2...
85	2010-09-10T12:49:29.9112568		2001...	2001...
67	2010-09-10T12:49:29.8388455		10.20...	10.1...
84	2010-09-10T12:49:29.8038745		2001...	2001...

TopSummary
lslot:\MAILSLOT\BROWSE, MailSlotOpcode:1,... Mail slot Write, Mailslot:\MAILSLO
lslot:\MAILSLOT\BROWSE, MailSlotOpcode:1,... Mail slot Write, Mailslot:\MAILSLO
nData([Encrypted]) Records: [ApplicationData(Encrypted)]
nData([Encrypted]) Records: [ApplicationData(Encrypted)]
nData([Encrypted]) Records: [ApplicationData(Encrypted)]
0.200.140.148, TargetIP: 10.200.140.1 REQUEST, SenderIP: 10.200.140.148,
K (200), GET /SitePages/Home.aspx, Version: Operation_Status: OK (200), GET /
nData([Encrypted]) Records: [ApplicationData(Encrypted)]
0.200.142.80, TargetIP: 10.200.140.1 REQUEST, SenderIP: 10.200.142.80, .
Flags: ...AP..., SrcPort: 64050, DstPort: HTTPS(443), Length:... Flags: ...AP..., SrcPort: 64050, D:
Records: [ApplicationData(Encrypted)]
Flags: ...AP..., SrcPort: HTTPS(443), DstPort: 64050, Length:... Flags: ...AP..., SrcPort: HTTPS(44:

Decrypting a trace

Microsoft Message Analyzer

I. Select successfully decrypted session from Decryption Tool

View Filter

Session Explorer

2. This triggers a global selection of those messages

3. Decrypted Traffic for the in focus selected message

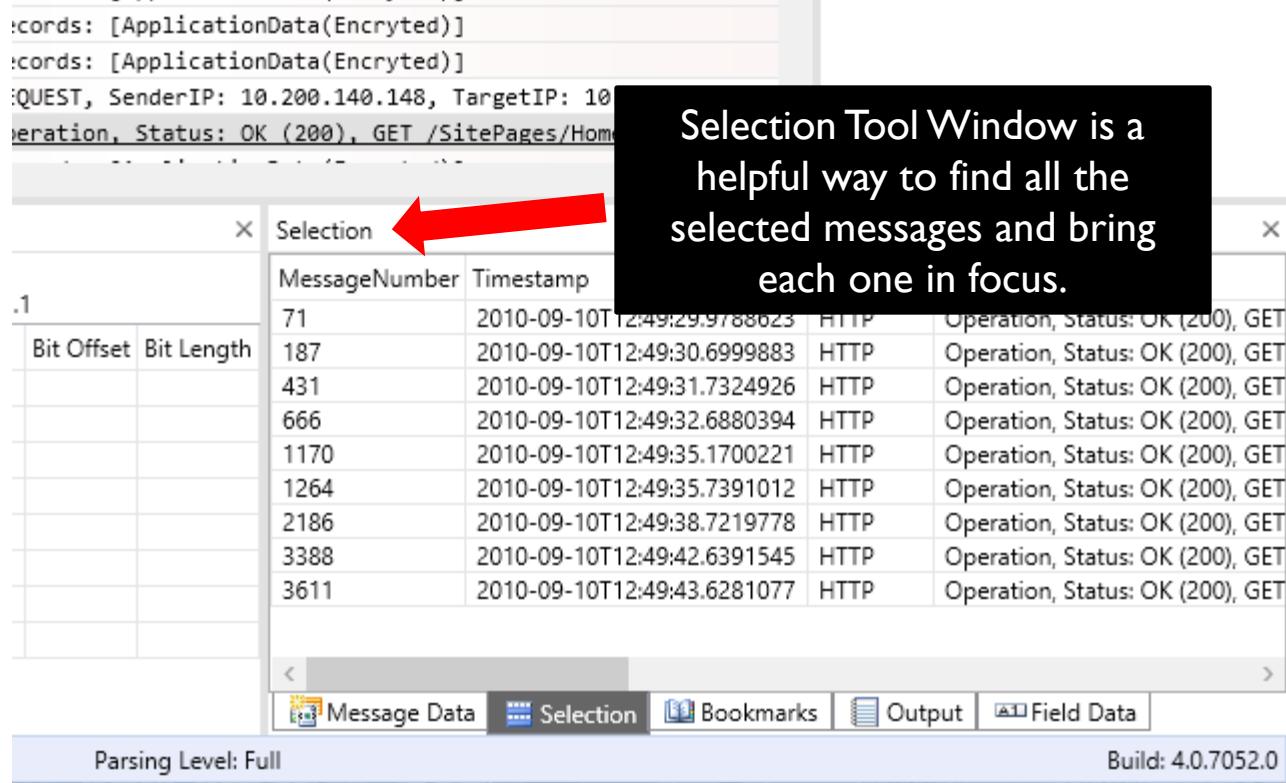
SDC 14

2014 Storage Developer Conference. © Microsoft. All Rights Reserved.

30

The screenshot shows the Microsoft Message Analyzer interface. A large black callout box labeled 'I. Select successfully decrypted session from Decryption Tool' has a red arrow pointing to a specific row in the 'Decryption' table. Another red arrow points to the same row in the main pane's list of messages. A third red arrow points to the detailed properties of the selected message in the bottom right pane. The interface includes tabs for Home, Tools, Charts, and various analysis tools like Viewpoints, Windows, and View Options. The 'Decryption' tool is open, showing a list of sessions with columns for Type, TimeStamp, ProtocolVersion, SourcePort, DestinationPort, SourceAddress, DestinationAddress, Encrypted Message Count, Undecrypted Message Count, and Message. One row is highlighted with a blue background. The main pane shows a list of messages with columns for MessageNumber, Timestamp, TimeElapsed, Source, Destina, Module, Summary, and TopSummary. The bottom pane shows a detailed view of the selected message, including its Method, Uri, Version, StatusCode, ReasonPhrase, ContentType, ContentEncoding, and Payload. The Session Explorer pane on the right lists sessions and analysis grids.

Decrypting a trace



The screenshot shows a software interface for managing network traces. At the top, there's a status bar with the text 'Records: [ApplicationData(Encrypted)]' repeated twice. Below this is a message list pane showing several log entries. A red arrow points from a callout box to the title bar of a window titled 'Selection'. The 'Selection' window contains a table with columns 'MessageNumber', 'Timestamp', and 'Operation, Status'. The table lists 11 messages, all of which are HTTP GET requests with status OK (200). The bottom of the interface includes tabs for 'Message Data', 'Selection' (which is currently active), 'Bookmarks', 'Output', and 'Field Data'. The status bar at the bottom also displays 'Parsing Level: Full' and 'Build: 4.0.7052.0'.

MessageNumber	Timestamp	Operation, Status
71	2010-09-10T12:49:29.9768623	HTTP Operation, Status: OK (200), GET
187	2010-09-10T12:49:30.6999883	HTTP Operation, Status: OK (200), GET
431	2010-09-10T12:49:31.7324926	HTTP Operation, Status: OK (200), GET
666	2010-09-10T12:49:32.6880394	HTTP Operation, Status: OK (200), GET
1170	2010-09-10T12:49:35.1700221	HTTP Operation, Status: OK (200), GET
1264	2010-09-10T12:49:35.7391012	HTTP Operation, Status: OK (200), GET
2186	2010-09-10T12:49:38.7219778	HTTP Operation, Status: OK (200), GET
3388	2010-09-10T12:49:42.6391545	HTTP Operation, Status: OK (200), GET
3611	2010-09-10T12:49:43.6281077	HTTP Operation, Status: OK (200), GET

Selection Tool Window is a
helpful way to find all the
selected messages and bring
each one in focus.

Decrypting a trace

Message Stack		
	Module	Summary
71	HTTP	Operation, Status: OK (200), GET /SitePages/Home.aspx, Vers
	HTTP	Request, GET /SitePages/Home.aspx, Version: HTTP/1.1
	ReassembledTCP	TCP Virtual Reassembled Segment, SrcPort: 64050, DstPort: H
	TLS	Records: [ApplicationData(Encrypted)]
	ReassembledTCP	TCP Virtual Reassembled Segment, SrcPort: 64050, DstPort: H
	TCP	Flags: ...AP..., SrcPort: 64050, DstPort: HTTPS(443), Lengt
	ESP	Next Protocol = TCP, SPI = 0x8C1A7E52, Seq = 0x00000014
	IPv6	Next Protocol: ESP, Payload Length: 544
	IPv4	Next Protocol: IPv6, Packet ID: 17450, Total Length: 604
	Ethernet	Type: Internet IP (IPv4)



Questions?

33

Resources

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