Microsoft

Taipei Interoperability Protocols Plugfest

2014

Microsoft Message Analyzer
Packet Analysis at a Higher Level

Neil B Martin

Test Manager WSSC- Interop and Tools

Microsoft Corporation

Microsoft

Content

- Packet Analyzer - review
- Abstracting views of protocols
- Alternative data sources
  - ETW
  - Remote Capture
  - Bluetooth
  - USB
  - Evtx
  - Logs files

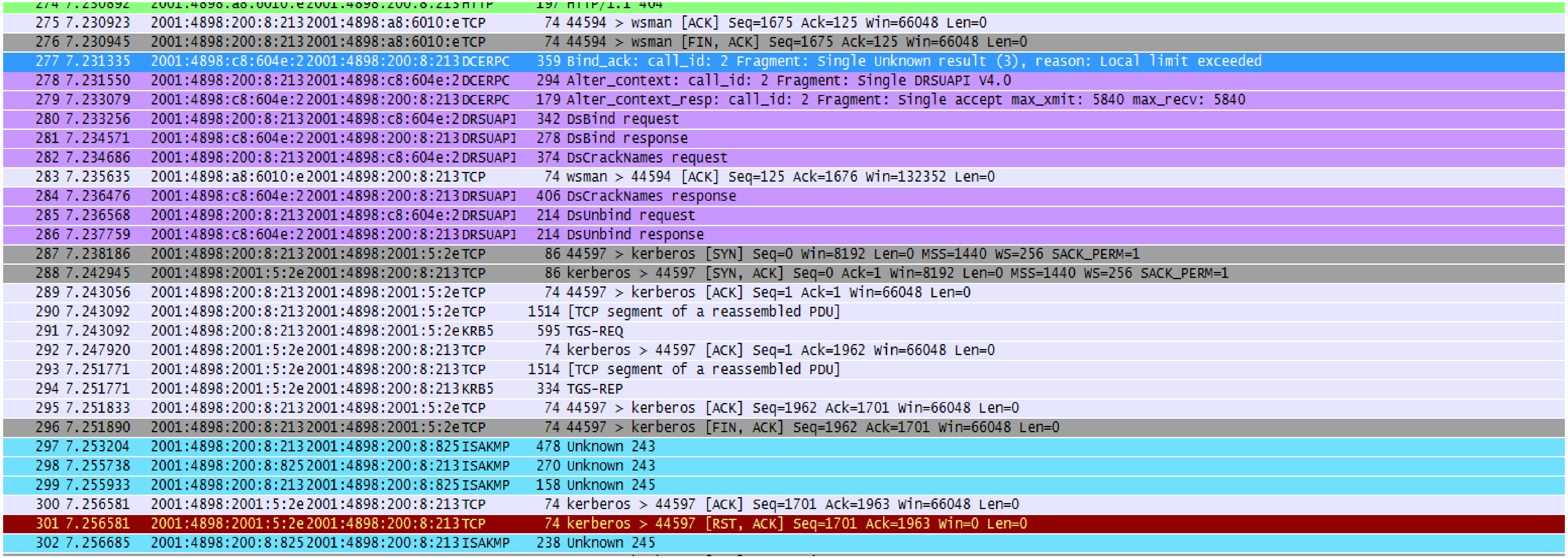
Message Analyzer – What is it?

- A packet analyzer is a computer program or a piece of computer hardware that can intercept and log traffic passing over all or part of a network
- Packet analyzers capture network packets in real time and display them in human-readable format

Dissectors

- WireShark, Microsoft NetMon 3.4
- These tools are dissectors
  - If they recognize a packet they dissect it and display the inner fields of the packet
  - The parsers are written based on the protocol specifications or in some cases through reverse engineering of the protocols when no specification is available

Dissectors

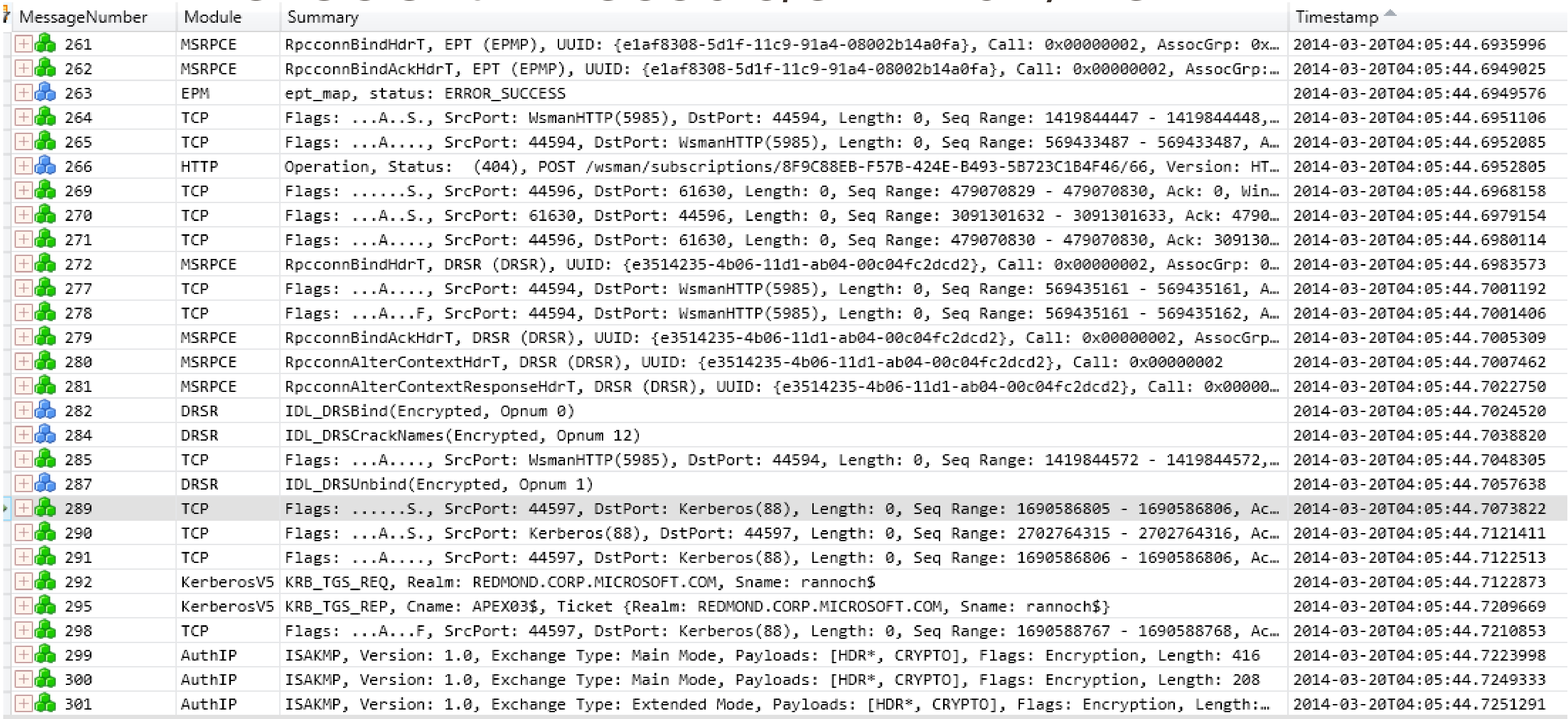


```
274 7.230892   2001:4898:a8:6010:e 2001:4898:200:8:213 HTTP     197 HTTP/1.1 404
275 7.230923   2001:4898:200:8:213 2001:4898:a8:6010:e TCP       74 44594 > wsman [ACK] Seq=1675 Ack=125 Win=66048 Len=0
276 7.230945   2001:4898:200:8:213 2001:4898:a8:6010:e TCP       74 44594 > wsman [FIN, ACK] Seq=1675 Ack=125 Win=66048 Len=0
277 7.231335   2001:4898:c8:604e:2 2001:4898:200:8:213 DCERPC   359 Bind_ack: call_id: 2 Fragment: Single Unknown result (3), reason: Local limit exceeded
278 7.231550   2001:4898:200:8:213 2001:4898:c8:604e:2 DCERPC   294 Alter_context: call_id: 2 Fragment: Single DRSUAPI V4.0
279 7.233079   2001:4898:c8:604e:2 2001:4898:200:8:213 DCERPC   179 Alter_context_resp: call_id: 2 Fragment: Single accept max_xmit: 5840 max_recv: 5840
280 7.233256   2001:4898:200:8:213 2001:4898:c8:604e:2 DRSUAPI  342 DsBind request
281 7.234571   2001:4898:c8:604e:2 2001:4898:200:8:213 DRSUAPI  278 DsBind response
282 7.234686   2001:4898:200:8:213 2001:4898:c8:604e:2 DRSUAPI  374 DsCrackNames request
283 7.235635   2001:4898:a8:6010:e 2001:4898:200:8:213 TCP       74 wsman > 44594 [ACK] Seq=125 Ack=1676 Win=132352 Len=0
284 7.236476   2001:4898:c8:604e:2 2001:4898:200:8:213 DRSUAPI  406 DsCrackNames response
285 7.236568   2001:4898:200:8:213 2001:4898:c8:604e:2 DRSUAPI  214 DsUnbind request
286 7.237759   2001:4898:c8:604e:2 2001:4898:200:8:213 DRSUAPI  214 DsUnbind response
287 7.238186   2001:4898:200:8:213 2001:4898:2001:5:2e TCP       86 44597 > kerberos [SYN] Seq=0 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1
288 7.242945   2001:4898:2001:5:2e 2001:4898:200:8:213 TCP       86 kerberos > 44597 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1
289 7.243056   2001:4898:200:8:213 2001:4898:2001:5:2e TCP       74 44597 > kerberos [ACK] Seq=1 Ack=1 Win=66048 Len=0
290 7.243092   2001:4898:200:8:213 2001:4898:2001:5:2e TCP     1514 [TCP segment of a reassembled PDU]
291 7.243092   2001:4898:200:8:213 2001:4898:2001:5:2e KRB5     595 TGS-REQ
292 7.247920   2001:4898:2001:5:2e 2001:4898:200:8:213 TCP       74 kerberos > 44597 [ACK] Seq=1 Ack=1962 Win=66048 Len=0
293 7.251771   2001:4898:2001:5:2e 2001:4898:200:8:213 TCP     1514 [TCP segment of a reassembled PDU]
294 7.251771   2001:4898:2001:5:2e 2001:4898:200:8:213 KRB5     334 TGS-REP
295 7.251833   2001:4898:200:8:213 2001:4898:2001:5:2e TCP       74 44597 > kerberos [ACK] Seq=1962 Ack=1701 Win=66048 Len=0
296 7.251890   2001:4898:200:8:213 2001:4898:2001:5:2e TCP       74 44597 > kerberos [FIN, ACK] Seq=1962 Ack=1701 Win=66048 Len=0
297 7.253204   2001:4898:200:8:213 2001:4898:200:8:825 ISAKMP   478 Unknown 243
298 7.255738   2001:4898:200:8:825 2001:4898:200:8:213 ISAKMP   270 Unknown 243
299 7.255933   2001:4898:200:8:213 2001:4898:200:8:825 ISAKMP   158 Unknown 245
300 7.256581   2001:4898:2001:5:2e 2001:4898:200:8:213 TCP       74 kerberos > 44597 [ACK] Seq=1701 Ack=1963 Win=66048 Len=0
301 7.256581   2001:4898:2001:5:2e 2001:4898:200:8:213 TCP       74 kerberos > 44597 [RST, ACK] Seq=1701 Ack=1963 Win=0 Len=0
302 7.256685   2001:4898:200:8:825 2001:4898:200:8:213 ISAKMP   238 Unknown 245
```

Microsoft Message Analyzer

- Dissection and Abstraction
  - We want to allow a higher level of abstraction view of protcols
  - Pattern Matching
    - Match up request/response pairs where possible
    - Called an operation
  - Different Viewers and Charts
- Addressing many of the challenges of diagnosing modern networks
  - Protocol Validation
    - Identify packets that do not match the specification
  - Data capture from multiple sources
    - NDIS, Bluetooth, USB, Windows Firewall Layer, Web Proxy
  - Header only network capture
    - Reduce data in volume scenarios
  - Correlation of data across multiple data sources and logs
    - Load and display multiple data source

Microsoft Message Analyzer

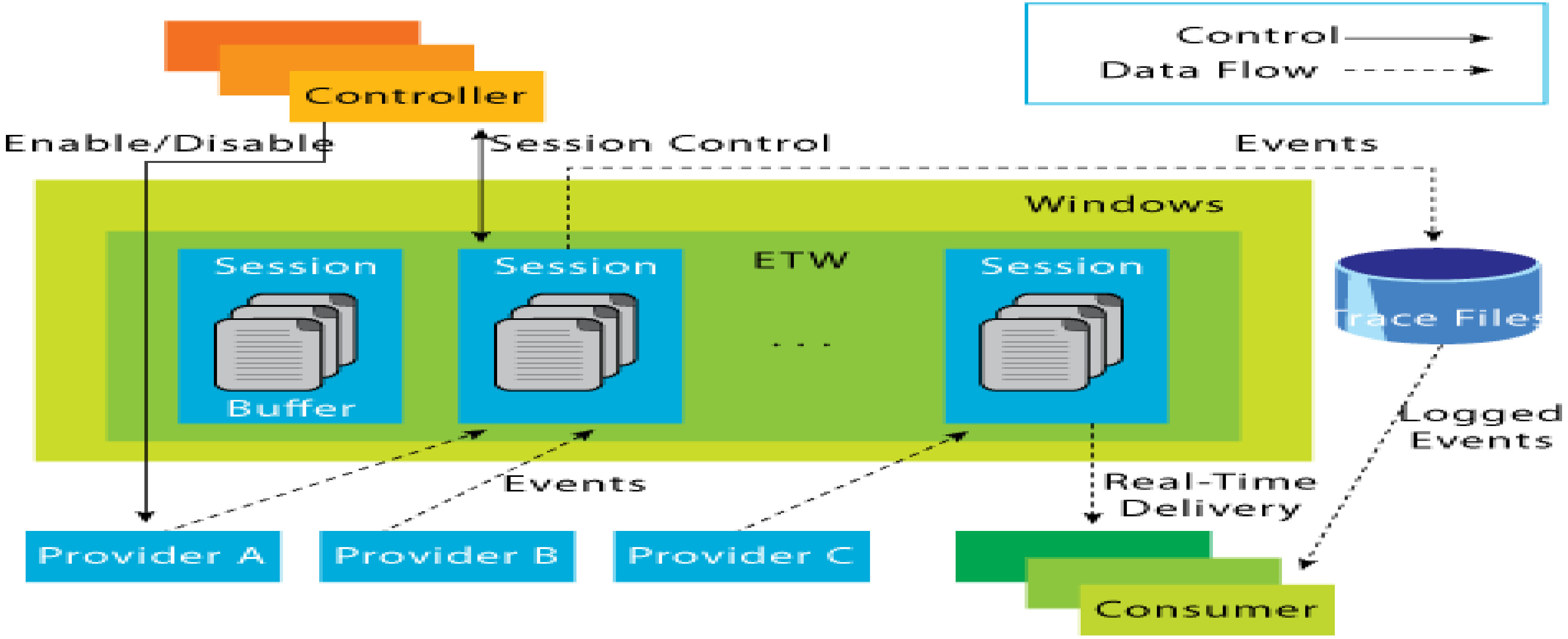


MessageNumber	Module	Summary	Timestamp
261	MSRPCE	RpcconnBindHdrT, EPT (EPMP), UUID: {e1af8308-5d1f-11c9-91a4-08002b14a0fa}, Call: 0x00000002, AssocGrp: 0x…	2014-03-20T04:05:44.6935996
262	MSRPCE	RpcconnBindAckHdrT, EPT (EPMP), UUID: {e1af8308-5d1f-11c9-91a4-08002b14a0fa}, Call: 0x00000002, AssocGrp:…	2014-03-20T04:05:44.6949025
263	EPM	ept_map, status: ERROR_SUCCESS	2014-03-20T04:05:44.6949576
264	TCP	Flags: ...A..S., SrcPort: WsmanHTTP(5985), DstPort: 44594, Length: 0, Seq Range: 1419844447 - 1419844448,…	2014-03-20T04:05:44.6951106
265	TCP	Flags: ...A...., SrcPort: 44594, DstPort: WsmanHTTP(5985), Length: 0, Seq Range: 569433487 - 569433487, A…	2014-03-20T04:05:44.6952085
266	HTTP	Operation, Status: (404), POST /wsman/subscriptions/8F9C88EB-F57B-424E-B493-5B723C1B4F46/66, Version: HT…	2014-03-20T04:05:44.6952805
269	TCP	Flags: ......S., SrcPort: 44596, DstPort: 61630, Length: 0, Seq Range: 479070829 - 479070830, Ack: 0, Win…	2014-03-20T04:05:44.6968158
270	TCP	Flags: ...A..S., SrcPort: 61630, DstPort: 44596, Length: 0, Seq Range: 3091301632 - 3091301633, Ack: 4790…	2014-03-20T04:05:44.6979154
271	TCP	Flags: ...A...., SrcPort: 44596, DstPort: 61630, Length: 0, Seq Range: 479070830 - 479070830, Ack: 309130…	2014-03-20T04:05:44.6980114
272	MSRPCE	RpcconnBindHdrT, DRSR (DRSR), UUID: {e3514235-4b06-11d1-ab04-00c04fc2dcd2}, Call: 0x00000002, AssocGrp: 0…	2014-03-20T04:05:44.6983573
277	TCP	Flags: ...A...., SrcPort: 44594, DstPort: WsmanHTTP(5985), Length: 0, Seq Range: 569435161 - 569435161, A…	2014-03-20T04:05:44.7001192
278	TCP	Flags: ...A...F, SrcPort: 44594, DstPort: WsmanHTTP(5985), Length: 0, Seq Range: 569435161 - 569435162, A…	2014-03-20T04:05:44.7001406
279	MSRPCE	RpcconnBindAckHdrT, DRSR (DRSR), UUID: {e3514235-4b06-11d1-ab04-00c04fc2dcd2}, Call: 0x00000002, AssocGrp…	2014-03-20T04:05:44.7005309
280	MSRPCE	RpcconnAlterContextHdrT, DRSR (DRSR), UUID: {e3514235-4b06-11d1-ab04-00c04fc2dcd2}, Call: 0x00000002	2014-03-20T04:05:44.7007462
281	MSRPCE	RpcconnAlterContextResponseHdrT, DRSR (DRSR), UUID: {e3514235-4b06-11d1-ab04-00c04fc2dcd2}, Call: 0x00000…	2014-03-20T04:05:44.7022750
282	DRSR	IDL_DRSBind(Encrypted, Opnum 0)	2014-03-20T04:05:44.7024520
284	DRSR	IDL_DRSCrackNames(Encrypted, Opnum 12)	2014-03-20T04:05:44.7038820
285	TCP	Flags: ...A...., SrcPort: WsmanHTTP(5985), DstPort: 44594, Length: 0, Seq Range: 1419844572 - 1419844572,…	2014-03-20T04:05:44.7048305
287	DRSR	IDL_DRSUnbind(Encrypted, Opnum 1)	2014-03-20T04:05:44.7057638
289	TCP	Flags: ......S., SrcPort: 44597, DstPort: Kerberos(88), Length: 0, Seq Range: 1690586805 - 1690586806, Ac…	2014-03-20T04:05:44.7073822
290	TCP	Flags: ...A..S., SrcPort: Kerberos(88), DstPort: 44597, Length: 0, Seq Range: 2702764315 - 2702764316, Ac…	2014-03-20T04:05:44.7121411
291	TCP	Flags: ...A...., SrcPort: 44597, DstPort: Kerberos(88), Length: 0, Seq Range: 1690586806 - 1690586806, Ac…	2014-03-20T04:05:44.7122513
292	KerberosV5	KRB_TGS_REQ, Realm: REDMOND.CORP.MICROSOFT.COM, Sname: rannoch$	2014-03-20T04:05:44.7122873
295	KerberosV5	KRB_TGS_REP, Cname: APEX03$, Ticket {Realm: REDMOND.CORP.MICROSOFT.COM, Sname: rannoch$}	2014-03-20T04:05:44.7209669
298	TCP	Flags: ...A...F, SrcPort: 44597, DstPort: Kerberos(88), Length: 0, Seq Range: 1690588767 - 1690588768, Ac…	2014-03-20T04:05:44.7210853
299	AuthIP	ISAKMP, Version: 1.0, Exchange Type: Main Mode, Payloads: [HDR*, CRYPTO], Flags: Encryption, Length: 416	2014-03-20T04:05:44.7223998
300	AuthIP	ISAKMP, Version: 1.0, Exchange Type: Main Mode, Payloads: [HDR*, CRYPTO], Flags: Encryption, Length: 208	2014-03-20T04:05:44.7249333
301	AuthIP	ISAKMP, Version: 1.0, Exchange Type: Extended Mode, Payloads: [HDR*, CRYPTO], Flags: Encryption, Length:…	2014-03-20T04:05:44.7251291

Data Capture from Multiple Sources

- Message Analyzer captures ETW
  - ETW - Event Trace for Windows
- Message Capture from:
  - Traditional NDIS traffic from the Network Adapter
  - Windows Filtering Platform 9aka Firewall)
  - Web proxy
  - USB ports
  - Bluetooth
  - Windows SMB Client
  - Windows SMB Server ……

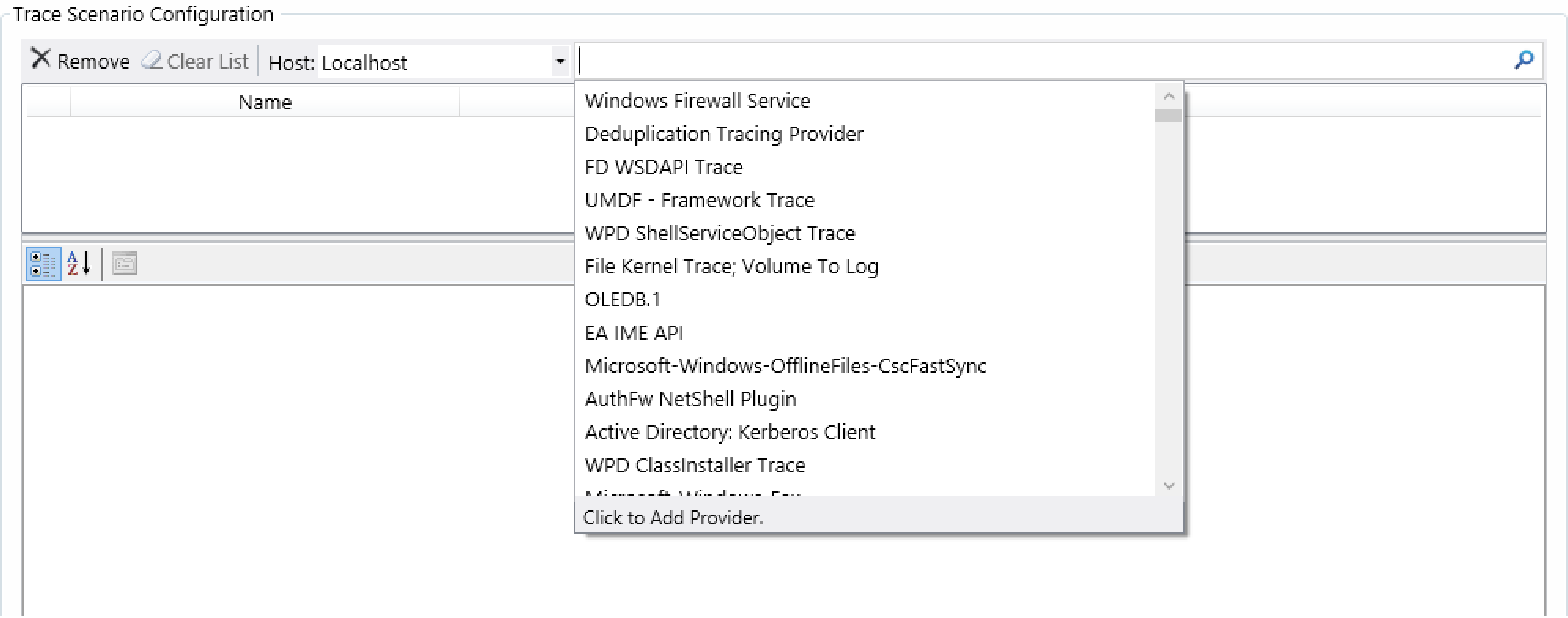
Event Tracing for Windows -ETW



Event Tracing for Windows

- Event Tracing for Windows ETW
- **High-resolution (<<100μs)** logging infrastructure allows any component to tell the outside world what it is currently doing by firing ETW events.
- A powerful diagnostic **tool** to log every methods/lines inside the code with reasonable performance for debugging/troubleshooting.
- MSDN on ETW http://msdn2.microsoft.com/en-us/library/bb968803(VS.85).aspx

Event Tracing for Windows -ETW



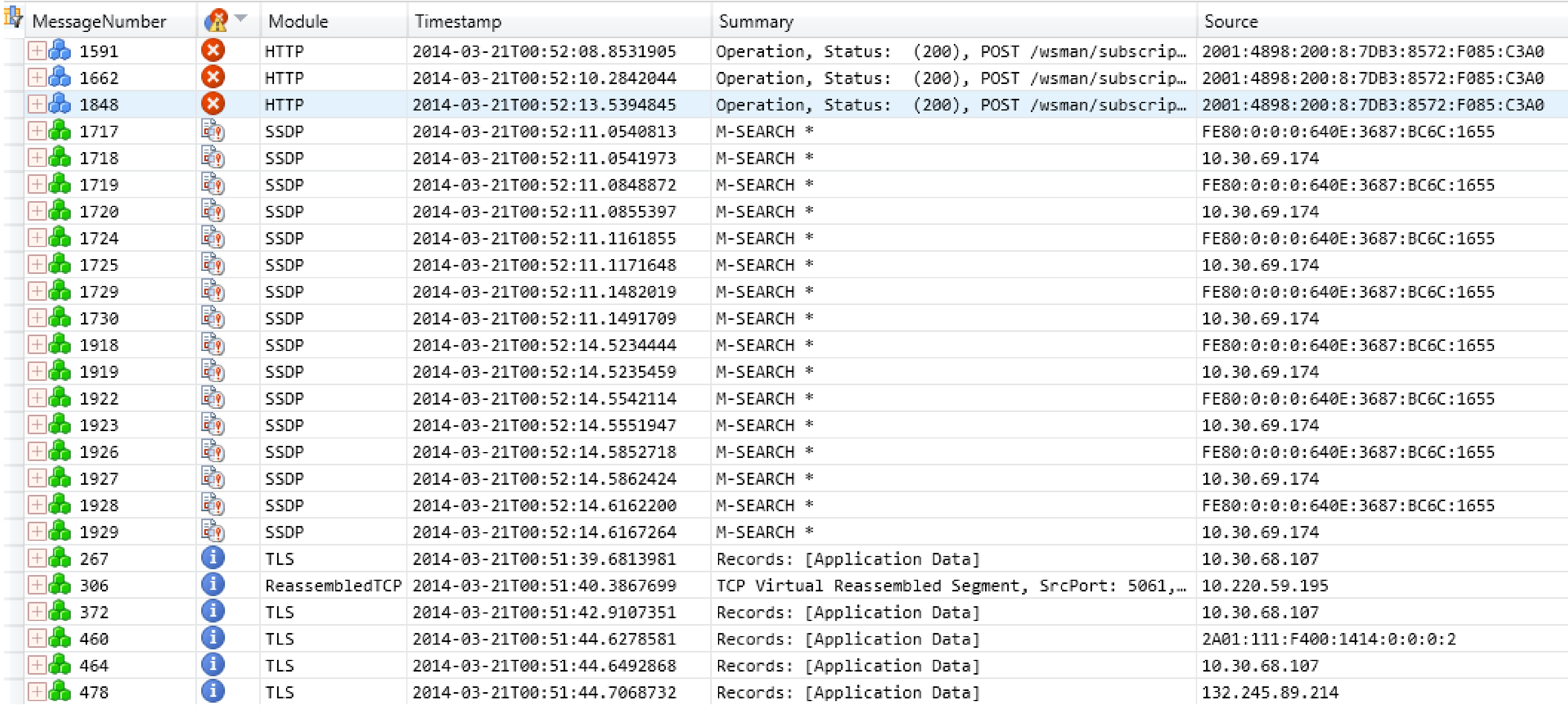
Trace Scenario Configuration

Windows Firewall Service
Deduplication Tracing Provider
FD WSDAPI Trace
UMDF - Framework Trace
WPD ShellServiceObject Trace
File Kernel Trace; Volume To Log
OLEDB.1
EA IME API
Microsoft-Windows-OfflineFiles-CscFastSync
AuthFw NetShell Plugin
Active Directory: Kerberos Client
WPD ClassInstaller Trace

Click to Add Provider.

All Windows ETW Sources are available to Message Analyzer

Rapid Diagnostics

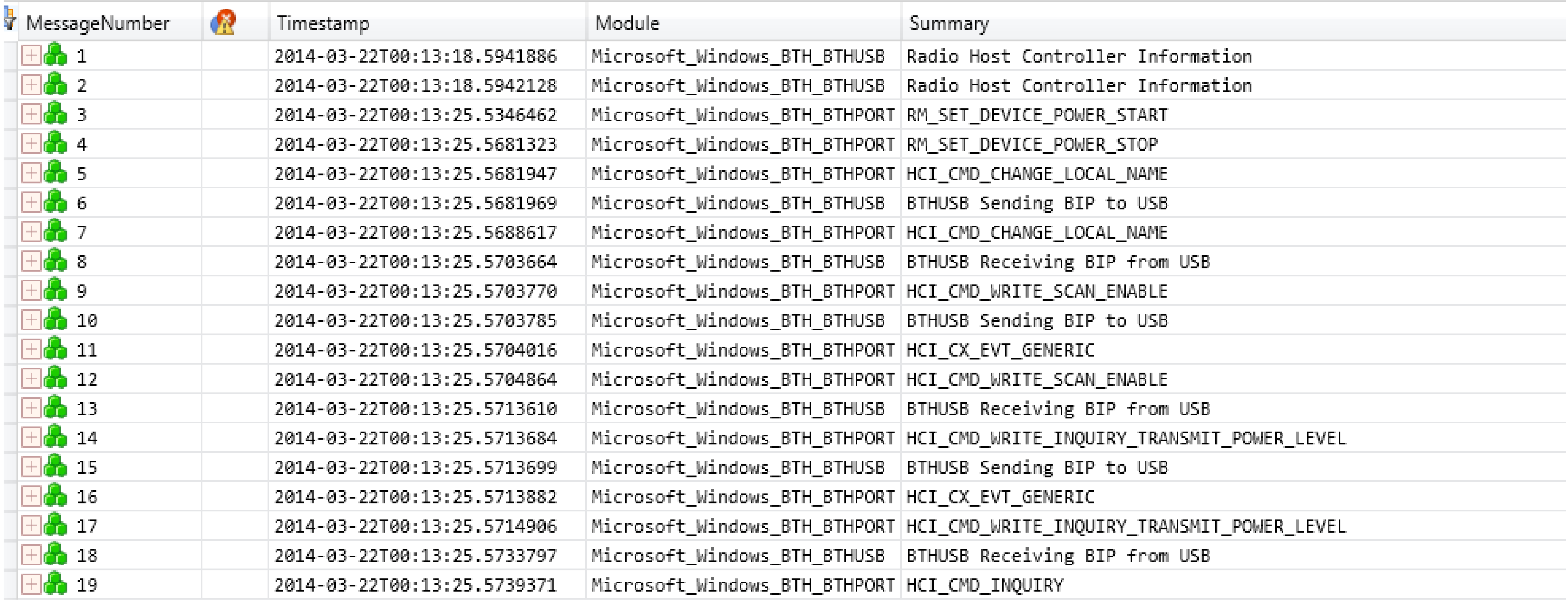


MessageNumber		Module	Timestamp	Summary	Source
1591	✖	HTTP	2014-03-21T00:52:08.8531905	Operation, Status: (200), POST /wsman/subscrip…	2001:4898:200:8:7DB3:8572:F085:C3A0
1662	✖	HTTP	2014-03-21T00:52:10.2842044	Operation, Status: (200), POST /wsman/subscrip…	2001:4898:200:8:7DB3:8572:F085:C3A0
1848	✖	HTTP	2014-03-21T00:52:13.5394845	Operation, Status: (200), POST /wsman/subscrip…	2001:4898:200:8:7DB3:8572:F085:C3A0
1717	?	SSDP	2014-03-21T00:52:11.0540813	M-SEARCH *	FE80:0:0:0:640E:3687:BC6C:1655
1718	?	SSDP	2014-03-21T00:52:11.0541973	M-SEARCH *	10.30.69.174
1719	?	SSDP	2014-03-21T00:52:11.0848872	M-SEARCH *	FE80:0:0:0:640E:3687:BC6C:1655
1720	?	SSDP	2014-03-21T00:52:11.0855397	M-SEARCH *	10.30.69.174
1724	?	SSDP	2014-03-21T00:52:11.1161855	M-SEARCH *	FE80:0:0:0:640E:3687:BC6C:1655
1725	?	SSDP	2014-03-21T00:52:11.1171648	M-SEARCH *	10.30.69.174
1729	?	SSDP	2014-03-21T00:52:11.1482019	M-SEARCH *	FE80:0:0:0:640E:3687:BC6C:1655
1730	?	SSDP	2014-03-21T00:52:11.1491709	M-SEARCH *	10.30.69.174
1918	?	SSDP	2014-03-21T00:52:14.5234444	M-SEARCH *	FE80:0:0:0:640E:3687:BC6C:1655
1919	?	SSDP	2014-03-21T00:52:14.5235459	M-SEARCH *	10.30.69.174
1922	?	SSDP	2014-03-21T00:52:14.5542114	M-SEARCH *	FE80:0:0:0:640E:3687:BC6C:1655
1923	?	SSDP	2014-03-21T00:52:14.5551947	M-SEARCH *	10.30.69.174
1926	?	SSDP	2014-03-21T00:52:14.5852718	M-SEARCH *	FE80:0:0:0:640E:3687:BC6C:1655
1927	?	SSDP	2014-03-21T00:52:14.5862424	M-SEARCH *	10.30.69.174
1928	?	SSDP	2014-03-21T00:52:14.6162200	M-SEARCH *	FE80:0:0:0:640E:3687:BC6C:1655
1929	?	SSDP	2014-03-21T00:52:14.6167264	M-SEARCH *	10.30.69.174
267	ⓘ	TLS	2014-03-21T00:51:39.6813981	Records: [Application Data]	10.30.68.107
306	ⓘ	ReassembledTCP	2014-03-21T00:51:40.3867699	TCP Virtual Reassembled Segment, SrcPort: 5061,…	10.220.59.195
372	ⓘ	TLS	2014-03-21T00:51:42.9107351	Records: [Application Data]	10.30.68.107
460	ⓘ	TLS	2014-03-21T00:51:44.6278581	Records: [Application Data]	2A01:111:F400:1414:0:0:0:2
464	ⓘ	TLS	2014-03-21T00:51:44.6492868	Records: [Application Data]	10.30.68.107
478	ⓘ	TLS	2014-03-21T00:51:44.7068732	Records: [Application Data]	132.245.89.214

Remote Capture

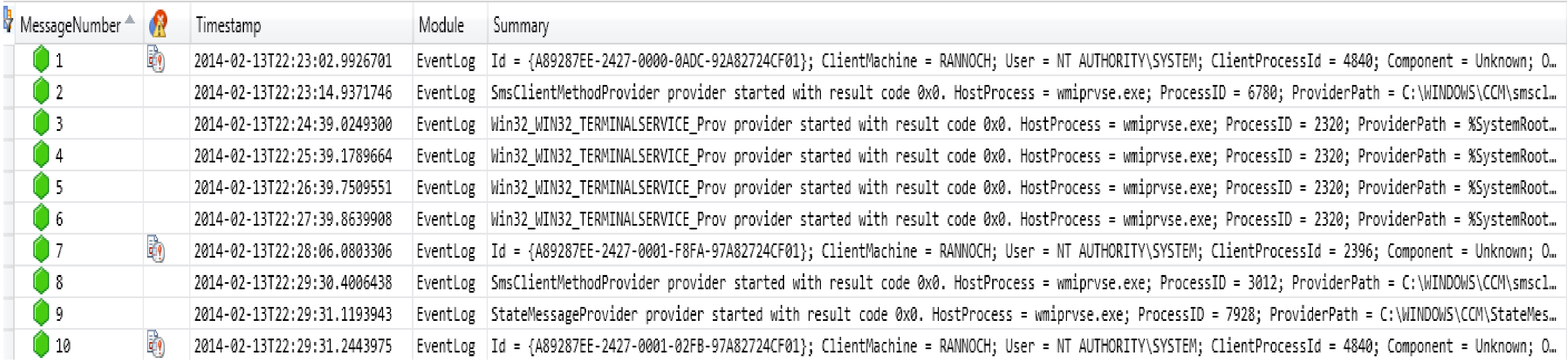
- Capability to perform remote capture
  - Select machine and give credentials
  - Collect data via ETW from NIC on remote machine

BlueTooth and USB



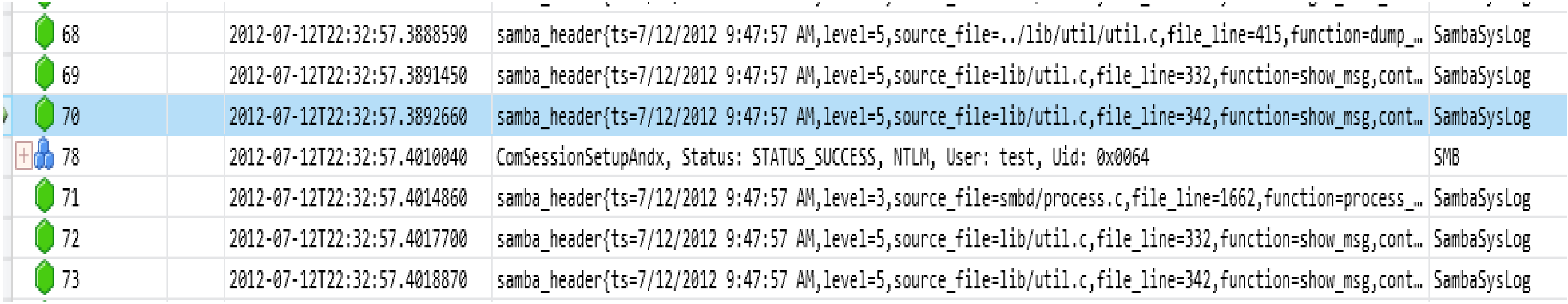
MessageNumber		Timestamp	Module	Summary
1		2014-03-22T00:13:18.5941886	Microsoft_Windows_BTH_BTHUSB	Radio Host Controller Information
2		2014-03-22T00:13:18.5942128	Microsoft_Windows_BTH_BTHUSB	Radio Host Controller Information
3		2014-03-22T00:13:25.5346462	Microsoft_Windows_BTH_BTHPORT	RM_SET_DEVICE_POWER_START
4		2014-03-22T00:13:25.5681323	Microsoft_Windows_BTH_BTHPORT	RM_SET_DEVICE_POWER_STOP
5		2014-03-22T00:13:25.5681947	Microsoft_Windows_BTH_BTHPORT	HCI_CMD_CHANGE_LOCAL_NAME
6		2014-03-22T00:13:25.5681969	Microsoft_Windows_BTH_BTHUSB	BTHUSB Sending BIP to USB
7		2014-03-22T00:13:25.5688617	Microsoft_Windows_BTH_BTHPORT	HCI_CMD_CHANGE_LOCAL_NAME
8		2014-03-22T00:13:25.5703664	Microsoft_Windows_BTH_BTHUSB	BTHUSB Receiving BIP from USB
9		2014-03-22T00:13:25.5703770	Microsoft_Windows_BTH_BTHPORT	HCI_CMD_WRITE_SCAN_ENABLE
10		2014-03-22T00:13:25.5703785	Microsoft_Windows_BTH_BTHUSB	BTHUSB Sending BIP to USB
11		2014-03-22T00:13:25.5704016	Microsoft_Windows_BTH_BTHPORT	HCI_CX_EVT_GENERIC
12		2014-03-22T00:13:25.5704864	Microsoft_Windows_BTH_BTHPORT	HCI_CMD_WRITE_SCAN_ENABLE
13		2014-03-22T00:13:25.5713610	Microsoft_Windows_BTH_BTHUSB	BTHUSB Receiving BIP from USB
14		2014-03-22T00:13:25.5713684	Microsoft_Windows_BTH_BTHPORT	HCI_CMD_WRITE_INQUIRY_TRANSMIT_POWER_LEVEL
15		2014-03-22T00:13:25.5713699	Microsoft_Windows_BTH_BTHUSB	BTHUSB Sending BIP to USB
16		2014-03-22T00:13:25.5713882	Microsoft_Windows_BTH_BTHPORT	HCI_CX_EVT_GENERIC
17		2014-03-22T00:13:25.5714906	Microsoft_Windows_BTH_BTHPORT	HCI_CMD_WRITE_INQUIRY_TRANSMIT_POWER_LEVEL
18		2014-03-22T00:13:25.5733797	Microsoft_Windows_BTH_BTHUSB	BTHUSB Receiving BIP from USB
19		2014-03-22T00:13:25.5739371	Microsoft_Windows_BTH_BTHPORT	HCI_CMD_INQUIRY

Evtx File



MessageNumber		Timestamp	Module	Summary
1		2014-02-13T22:23:02.9926701	EventLog	Id = {A89287EE-2427-0000-0ADC-92A82724CF01}; ClientMachine = RANNOCH; User = NT AUTHORITY\SYSTEM; ClientProcessId = 4840; Component = Unknown; O…
2		2014-02-13T22:23:14.9371746	EventLog	SmsClientMethodProvider provider started with result code 0x0. HostProcess = wmiprvse.exe; ProcessID = 6780; ProviderPath = C:\WINDOWS\CCM\smscl…
3		2014-02-13T22:24:39.0249300	EventLog	Win32_WIN32_TERMINALSERVICE_Prov provider started with result code 0x0. HostProcess = wmiprvse.exe; ProcessID = 2320; ProviderPath = %SystemRoot…
4		2014-02-13T22:25:39.1789664	EventLog	Win32_WIN32_TERMINALSERVICE_Prov provider started with result code 0x0. HostProcess = wmiprvse.exe; ProcessID = 2320; ProviderPath = %SystemRoot…
5		2014-02-13T22:26:39.7509551	EventLog	Win32_WIN32_TERMINALSERVICE_Prov provider started with result code 0x0. HostProcess = wmiprvse.exe; ProcessID = 2320; ProviderPath = %SystemRoot…
6		2014-02-13T22:27:39.8639908	EventLog	Win32_WIN32_TERMINALSERVICE_Prov provider started with result code 0x0. HostProcess = wmiprvse.exe; ProcessID = 2320; ProviderPath = %SystemRoot…
7		2014-02-13T22:28:06.0803306	EventLog	Id = {A89287EE-2427-0001-F8FA-97A82724CF01}; ClientMachine = RANNOCH; User = NT AUTHORITY\SYSTEM; ClientProcessId = 2396; Component = Unknown; O…
8		2014-02-13T22:29:30.4006438	EventLog	SmsClientMethodProvider provider started with result code 0x0. HostProcess = wmiprvse.exe; ProcessID = 3012; ProviderPath = C:\WINDOWS\CCM\smscl…
9		2014-02-13T22:29:31.1193943	EventLog	StateMessageProvider provider started with result code 0x0. HostProcess = wmiprvse.exe; ProcessID = 7928; ProviderPath = C:\WINDOWS\CCM\StateMes…
10		2014-02-13T22:29:31.2443975	EventLog	Id = {A89287EE-2427-0001-02FB-97A82724CF01}; ClientMachine = RANNOCH; User = NT AUTHORITY\SYSTEM; ClientProcessId = 4840; Component = Unknown; O…

External Logs



```
68   2012-07-12T22:32:57.3888590   samba_header{ts=7/12/2012 9:47:57 AM,level=5,source_file=../lib/util/util.c,file_line=415,function=dump_…   SambaSysLog
69   2012-07-12T22:32:57.3891450   samba_header{ts=7/12/2012 9:47:57 AM,level=5,source_file=lib/util.c,file_line=332,function=show_msg,cont…   SambaSysLog
70   2012-07-12T22:32:57.3892660   samba_header{ts=7/12/2012 9:47:57 AM,level=5,source_file=lib/util.c,file_line=342,function=show_msg,cont…   SambaSysLog
78   2012-07-12T22:32:57.4010040   ComSessionSetupAndx, Status: STATUS_SUCCESS, NTLM, User: test, Uid: 0x0064                                    SMB
71   2012-07-12T22:32:57.4014860   samba_header{ts=7/12/2012 9:47:57 AM,level=3,source_file=smbd/process.c,file_line=1662,function=process_…   SambaSysLog
72   2012-07-12T22:32:57.4017700   samba_header{ts=7/12/2012 9:47:57 AM,level=5,source_file=lib/util.c,file_line=332,function=show_msg,cont…   SambaSysLog
73   2012-07-12T22:32:57.4018870   samba_header{ts=7/12/2012 9:47:57 AM,level=5,source_file=lib/util.c,file_line=342,function=show_msg,cont…   SambaSysLog
```

Microsoft Message Analyzer

- Powerful, extensible viewing and analysis
- Browse, Select, View
  - Browse for messages from various sources (live, or stored)
  - Select a set of messages from those sources by characteristic(s)
  - View messages in a provided viewer, configure or build your own
- A new high-level grid view
  - High level “Operations” view with automatic re-assembly
  - “Bubbling up” of errors in the stack to the top level
  - Ability to drill down the stack to underlying messages and/or packets
  - On the fly grouping, filtering, finding, or sorting by any message property
  - Payload rendering
- Validation of message structures, behavior, and architecture
  - Does the protocol comply with the specifications?

Windows Protocols

- Over 450 published specifications for Windows Protocols

  (as of Windows 8.1)

  (http://msdn.microsoft.com/en-us/library/gg685446.aspx)

  Available online and as PDF

  Continue to publish new documents with each release of Windows

- Continue to develop tools and technology to aid with the development of protocol documents, parsers and test technology

Download and Join our Community

How to get MA: http://www.microsoft.com/en-us/download/details.aspx?id=40308

How to get help: Blog, Operating Guide, Technet Forum for Message Analyzer

- We invite you to Explore Message Analyzer
- Connect Community
  - https://connect.microsoft.com/site216/

Questions and Answers