Analyzing SMB/SMB2 with Network Monitor 3

Who are you?

- Paul Long - Technical Evangelist for Network Monitor
- Networking Specialist in CPR Support group for Microsoft for 15 years
- Blog on http://blogs.technet.com/netmon

What you will learn

- Where SMB/SMB2 Documentation Is
- How to Organizing Traffic with Conversations
- Understand Reassembly and Fragmentation
- Filtering Tips for SMB/SMB2 Traffic
- How to Locate SMB/SMB2 Errors with Color Filters
- Demo: SMB/SMB2 Trace Examples

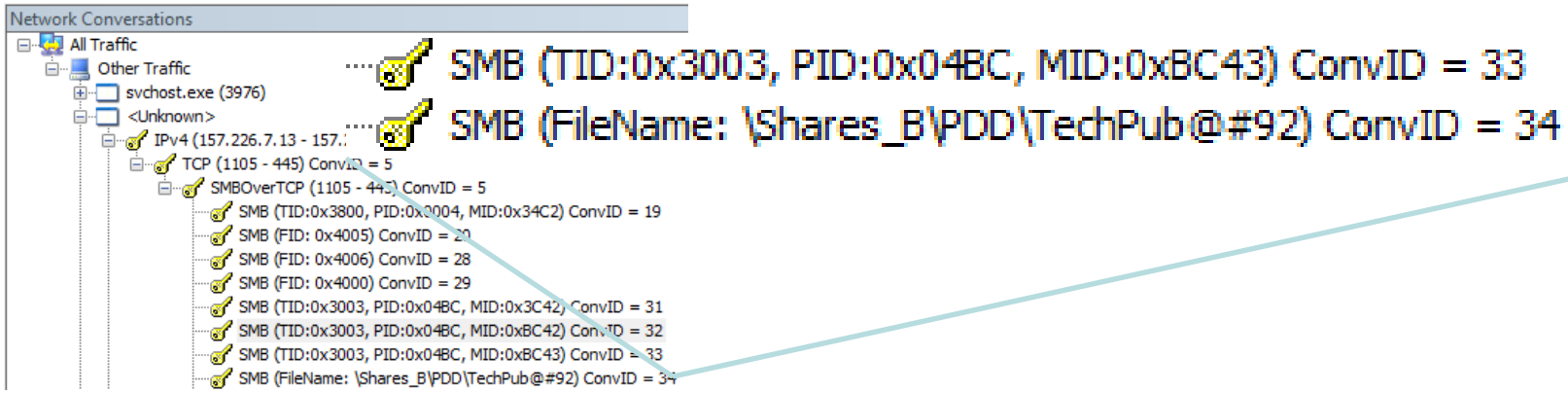
Documentation of SMB/SMB2

- Microsoft Open Specifications
- Bing "MS-SMB" or "MS-SMB2"
- How Protocols Work Together
  - MS-SYS
  - MS-PROTO
  - MS-SECO
- Open Protocol Forums

Organizing Traffic with Conversations

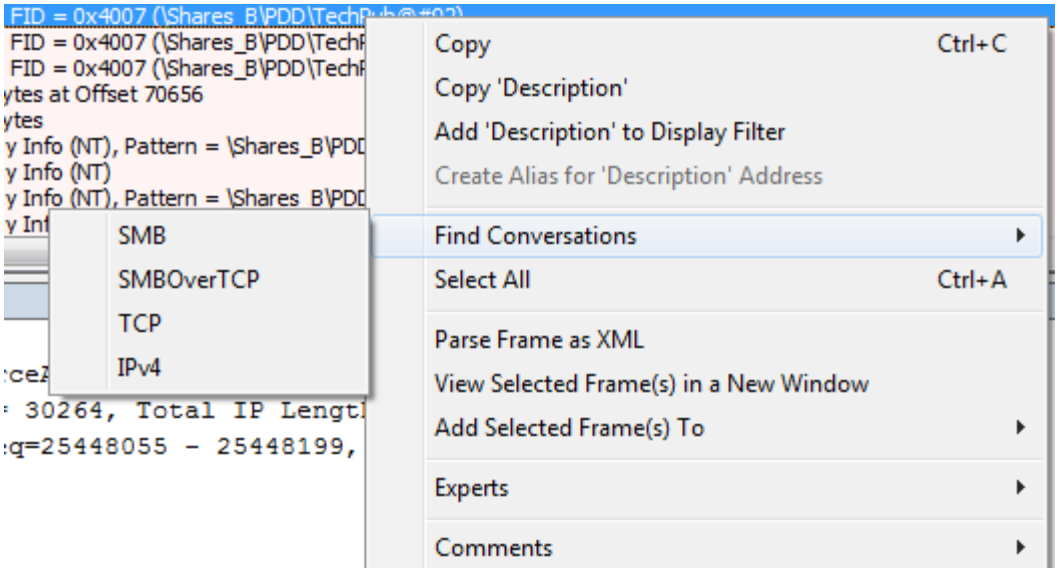
The Conversation Tree

- Organizes Network Traffic by Grouping Like Traffic
- For SMB, this means
  - by File ID or File Name
  - SMB Transaction



Conversation Tree Tricks

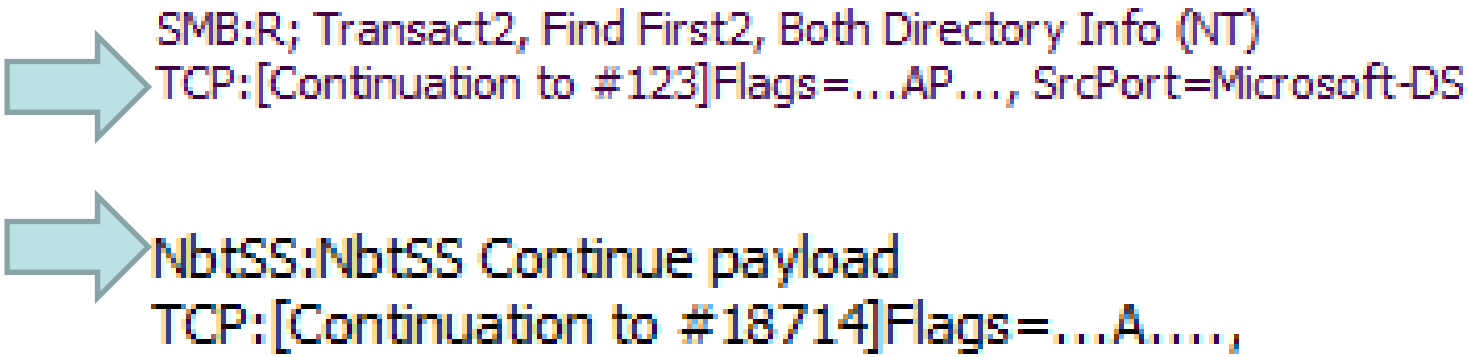
- Click on Tree Node to Filter Traffic
- Right Click Frame to Locate Conversation



Understanding Reassembly and Fragmentation

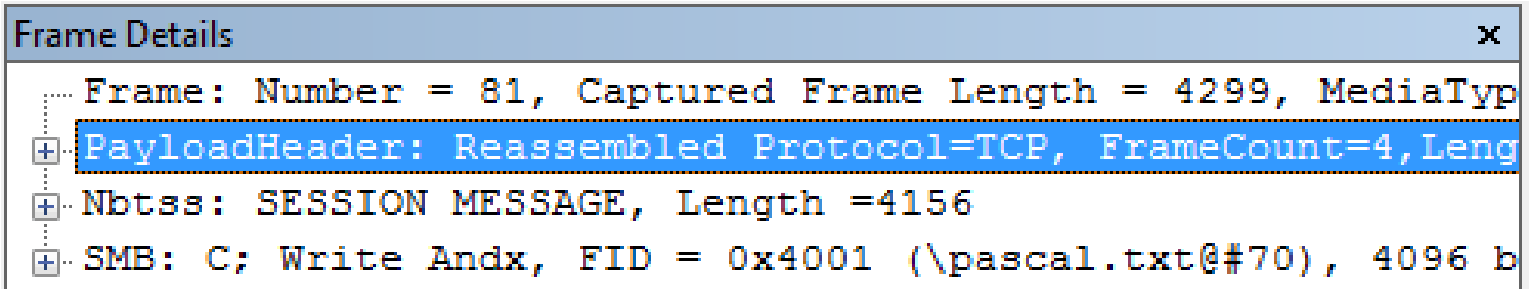
SMB/SMB2 and Fragmentation

- SMB/SMB2 Big, Ethernet Frames Small
- TCP/NBTSS can Fragment Data
  - Continuation frames are a key
- Network Monitor does NOT reassemble by default



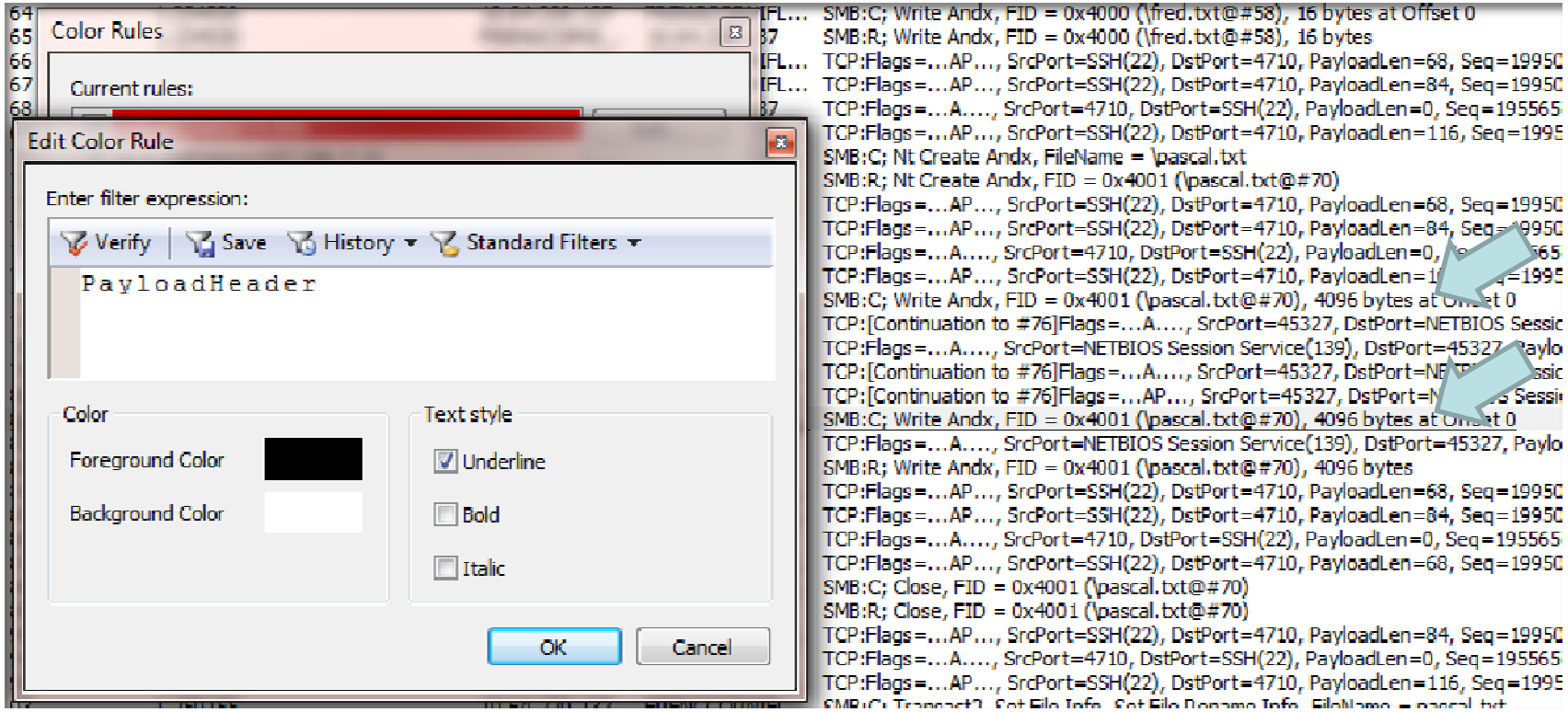
Reassembling with Network Monitor

- Press Reassemble Button
  - Only Available on Saved Traces
- New Window Appears, New Frames are Inserted
- New Frames have PayloadHeader Prepended to Top



Working With Reassembled Trace

- Newly Inserted Frame Follows Fragmented Data
- Color Filter Makes Finding Frames Easier



Mid Frame Fragmentation

- Network Monitor Can't Deal with Mid Frame Fragmentation
- Occurs when NBTSS or TCP Streams Two SMB Commands Together
- Can use "Decode As"
- Filter to Find (or Color Filter)

```
(!smb AND !smb2)
AND
(ContainsBin(FrameData, HEX, "FF 53 4D 42")
OR
ContainsBin(FrameData, HEX, "FE 53 4D 42"))
```

Mid Frame Fragmentation Example

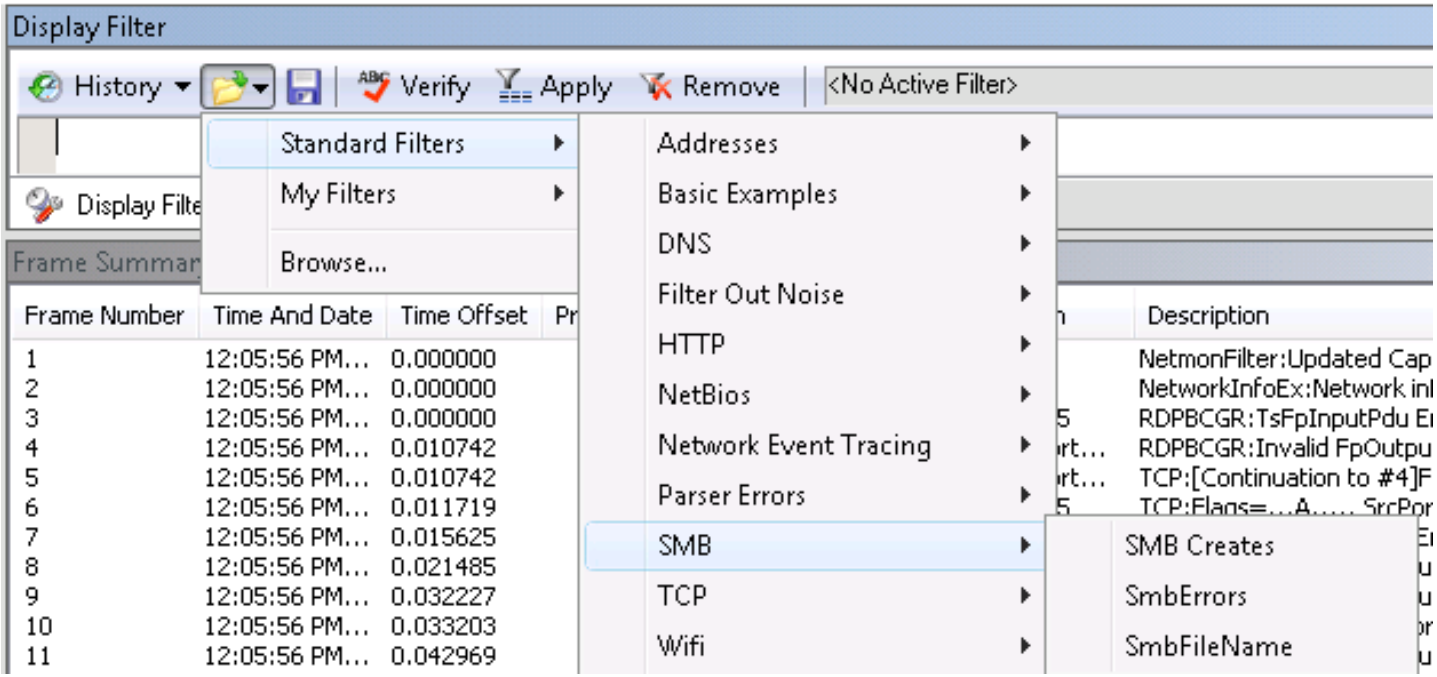

```
Tcp: [Continuation to #17813]Flags=...AP..., SrcPort=2055, DstPort=NETBIOS Session Service(139
    SrcPort: 2055
    DstPort: NETBIOS Session Service(139)
    SequenceNumber: 1263282351 (0x4B4C28AF)
    AcknowledgementNumber: 426698142 (0x196EE59E)
  + DataOffset: 80 (0x50)
  + Flags: ...AP...
    Window: 65535 (scale factor 0x0) = 65535
    Checksum: 0xBAA5, Good
    UrgentPointer: 0 (0x0)
    TcpContinuationData: Binary Large Object (264 Bytes)
```

```
0070   B5 2D 8E 2A 3D 2C E7 25 D1 91 B3 09 04 1C 98 96  µ- *=,ç%Ñ ³...
0080   76 EA 4E 78 FF E2 1D 78 2C B8 C0 3B 4B 20 16 A8  vêNxÿâ.x,¸À;K .¨
0090   18 BF C9 40 B4 02 1C 12 76 EB C7 14 F5 33 97 00  .¿É@´...vëÇ.õ3 .
00A0   6C 81 AB E1 3E 62 5F 1B D6 C1 2A 24 D5 91 4D ED  l «á>b_.ÖÁ*$Õ Mí
00B0   44 C8 23 7C A0 8E 55 D9 CF EC 7E 46 F9 54 38 8A  DÈ#|  UÙÏì~FùT8
00C0   64 04 63 1E 7D 5D 80 28 CF F9 40 60 01 AC C6 51  d.c.}] (Ïù@`.¬ÆQ
00D0   AD 5A 8E AB 38 19 E2 B6 3F 54 09 70 29 19 10 45  -Z «8.â¶?T.p)..E
00E0   9F 33 B0 02 56 7C EB 76 43 BD 43 0E 68 86 FB CC   3°.V|ëvC½C.h ûÌ
00F0   7E 15 00 00 00 48 FF 53 4D 42 32 00 00 00 00 18  ~....HÿSMB2.....
0100   17 C8 00 00 00 00 00 00 00 00 00 00 00 00 40 00  .È............@.
0110   E4 0B 40 00 41 52 0F 04 00 00 00 02 00 28 00 00  ä.@.AR.......(..
0120   00 00 00 00 00 00 00 00 00 04 00 44 00 00 00 00  ...........D....
0130   00 01 00 07 00 07 00 00 00 00 45 00 EC 03        ..........E.ì.
```

Filtering Tips for SMB/SMB2 Traffic

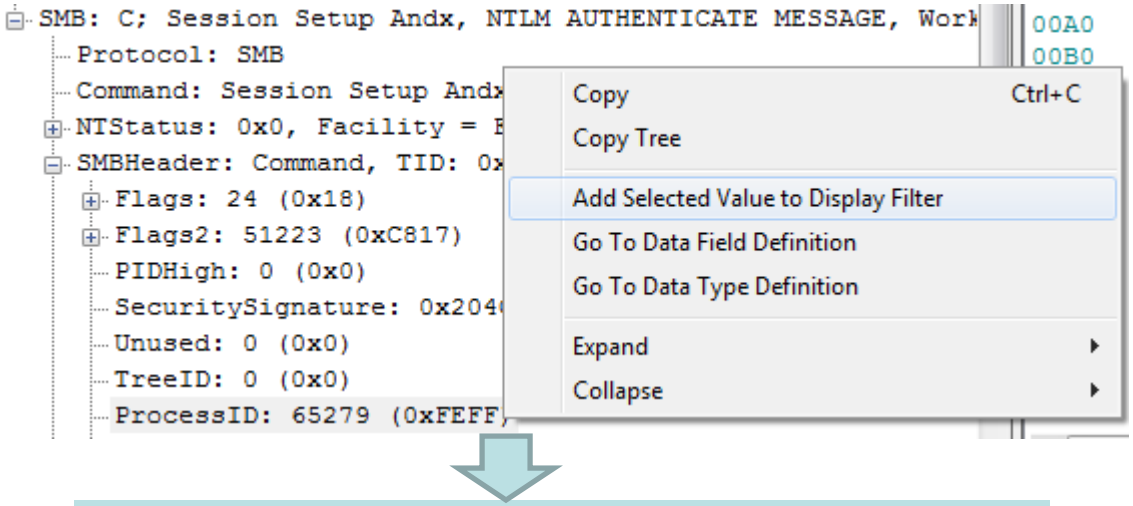
Standard Filters SMB/SMB2

- Standard Filters are Built Into Network Monitor
- Currently 3 available Standard Filters for SMB



Right Click add to Filter

- Click any field in Frame Details to create a filter that finds other frames with the same info.
- Great way to learn how to create filters!



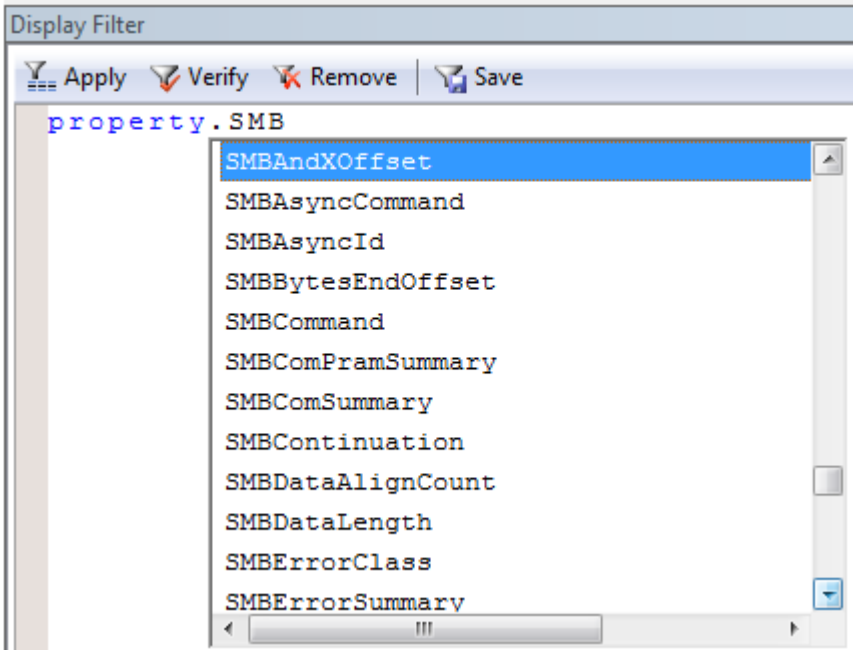
SMB.SMBHeader.ProcessID == 0xfeff

Properties of Interest for SMB/SMB2

- Properties are Meta Data defined by the Parser
  - Property.SMBFileName.contains(".txt")
  - Property.SMBCommand == 0x72
  - Property.SMBMID == 0x40
  - SMB File ID
    - Property.SMBFileID == 0x4000
  - SMB2 File ID
    - Property.SMBFileIDPersistent
    - Property.SMBFileIDVolatile

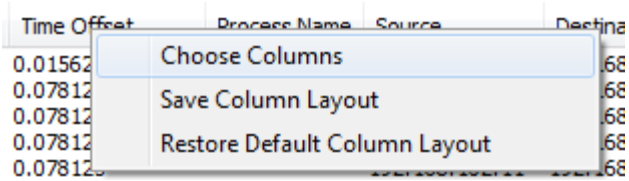
Properties of Interest for SMB/SMB2

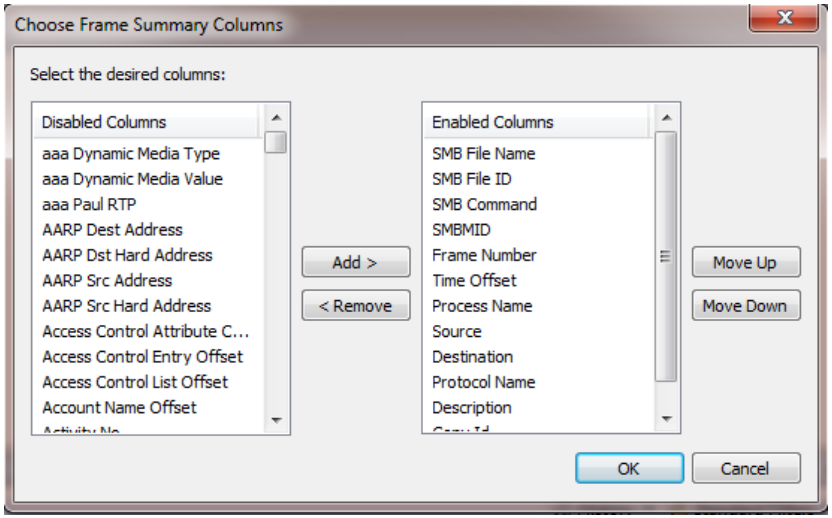
- Many others, to find type "Property.SMB" and use Intellisense.



Properties As Columns

- Any Property can be added as a column in Column Chooser





SMB File Name	SMB File ID	SMB Command	SMBMID	Frame ...	Time Offset	Process Name	Source	Destin
\nicktestweb1\copy_2_of_file-1.pdf@#3487		255 (0xFF)	4416 (0x1140)	3487	0.234375		192.168.102.11	192.16
\nicktestweb1\copy_2_of_file-1.pdf@#3487	64 (0x40)	255 (0xFF)	4416 (0x1140)	3488	0.234375		192.168.102.61	192.16
\nicktestweb1\copy_2_of_file-1.pdf@#3487	64 (0x40)	50 (0x32)	4480 (0x1180)	3489	0.234375		192.168.102.11	192.16
\nicktestweb1\copy_2_of_file-1.pdf@#3487	64 (0x40)	50 (0x32)	4480 (0x1180)	3490	0.234375		192.168.102.61	192.16
\nicktestweb1\copy_2_of_file-1.pdf@#3487	64 (0x40)	50 (0x32)	4608 (0x1200)	3493	0.234375		192.168.102.11	192.16
\nicktestweb1\copy_2_of_file-1.pdf@#3487	64 (0x40)	50 (0x32)	4608 (0x1200)	3494	0.234375		192.168.102.61	192.16

Locating SMB/SMB2 Errors Trace with Color Filters

Color Filter for SMB Errors

- Filter will find any frame with an SMB error.

```
(smb.DOSError.Error != 0 AND smb.DOSError.Error != 22)
OR
(smb.NTStatus.Code != 0 && smb.NTStatus.Code!= 22)
```

```
SMB:R; Nt Create Andx - NT Status: System - Error, Code = (34) STATUS_ACCESS_DENIED
SMB:C; Nt Create Andx, FileName = \01_Publishing\SC2000_1-2_Prepublishing\GER\IU_About_Title_SC2000_1-2_GER.doc
SMB:R; Nt Create Andx - NT Status: System - Error, Code = (97) STATUS_PRIVILEGE_NOT_HELD
SMB:C; Nt Create Andx, FileName = \01_Publishing\SC2000_1-2_Prepublishing\GER\IU_About_Title_SC2000_1-2_GER.doc
```

Color Filter for SMB2 Errors

- Filter will find any frame with an SMB2 error.

```
SMB2Header.Status != 0
AND
smb2.SMB2Header.Status != 259
```

```
SMB2:R  TREE CONNECT (0x3), TID=0x1
DFSC:Get DFS Referral Request, FileName: \ns401_89\fs3, MaxReferralLevel: 4
SMB2:R  - NT Status: System - Error, Code = (14) STATUS_NO_SUCH_DEVICE IOCTL (0xb)
SMB2:C  TREE CONNECT (0x3), Path=\\ns401_89\fs3
SMB2:R  TREE CONNECT (0x3), TID=0x2
SMB2:C  TREE DISCONNECT (0x4), TID=0x1
```

Demos

Demo: Trace Examples

- Trouble Shooting a Delayed Write Failure
- Looking at SMB Oplocks

Network Monitor 3

NM3 is a protocol analyzer and network capture tool. Features such as Process Tracking and the Conversation Tree allow you to quickly locate traffic.

- http://www.microsoft.com/downloads Latest released version.
- http://blogs.technet.com/netmon - Includes general help topics and training videos.
- http://social.technet.microsoft.com/Forums/en/netmon - Public Support Forums
- http://www.CodePlex.com/NMParsers - Open Source Parsers and latest parser version.
- http://www.CodePlex.com/NMExperts - Experts Landing Page
- http://connect.microsoft.com – Latest Betas, Beta support Forums and Bug Reporting