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

Network Conversations

SMB (TID:0x3003, PID:0x04BC, MID:0xBC43) ConvID = 33
SMB (FileName: \Shares_B\PDD\TechPub@#92) ConvID = 34
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

SMB:R; Transact2, Find First2, Both Directory Info (NT)
TCP:[Continuation to #123]Flags=...AP..., SrcPort=Microsoft-DS

NbtSS:NbtSS Continue payload
TCP:[Continuation to #18714]Flags=...A....,
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: 426688142 (0x196EE59E)
- Flags: 80 (0x50)
- Flags: ...AP...
  - Window: 65535 (scale factor 0x0) = 65535
  - Checksum: 0x8A05, Good
  - UrgentPointer: 0 (0x0)
- TcpContinuationData: Binary Large Object (264 Bytes)
Filtering Tips for SMB/SMB2 Traffic
Standard Filters SMB/SMB2

- Standard Filters are Built Into Network Monitor
- Currently 3 available Standard Filters for SMB
- 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
Many others, to find type “Property.SMB” and use Intellisense.
- Any Property can be added as a column in Column Chooser.

---

<table>
<thead>
<tr>
<th>SMB File Name</th>
<th>SMB File ID</th>
<th>SMB Command</th>
<th>SMBMID</th>
<th>Frame ...</th>
<th>Time Offset</th>
<th>Process Name</th>
<th>Source</th>
<th>Destin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nicktestweb1\copy_2_of_file-1.pdf@#3487</td>
<td>64 (0x40)</td>
<td>255 (0xFF)</td>
<td>416 (0x1140)</td>
<td>3487</td>
<td>0.234375</td>
<td>192.168.102.11</td>
<td>192.16</td>
<td></td>
</tr>
<tr>
<td>Nicktestweb1\copy_2_of_file-1.pdf@#3487</td>
<td>64 (0x40)</td>
<td>255 (0xFF)</td>
<td>416 (0x1140)</td>
<td>3488</td>
<td>0.234375</td>
<td>192.168.102.61</td>
<td>192.16</td>
<td></td>
</tr>
<tr>
<td>Nicktestweb1\copy_2_of_file-1.pdf@#3487</td>
<td>64 (0x40)</td>
<td>50 (0x32)</td>
<td>4480 (0x1180)</td>
<td>3489</td>
<td>0.234375</td>
<td>192.168.102.11</td>
<td>192.16</td>
<td></td>
</tr>
<tr>
<td>Nicktestweb1\copy_2_of_file-1.pdf@#3487</td>
<td>64 (0x40)</td>
<td>50 (0x32)</td>
<td>4480 (0x1180)</td>
<td>3490</td>
<td>0.234375</td>
<td>192.168.102.61</td>
<td>192.16</td>
<td></td>
</tr>
<tr>
<td>Nicktestweb1\copy_2_of_file-1.pdf@#3487</td>
<td>64 (0x40)</td>
<td>50 (0x32)</td>
<td>4608 (0x1200)</td>
<td>3493</td>
<td>0.234375</td>
<td>192.168.102.11</td>
<td>192.16</td>
<td></td>
</tr>
<tr>
<td>Nicktestweb1\copy_2_of_file-1.pdf@#3487</td>
<td>64 (0x40)</td>
<td>50 (0x32)</td>
<td>4608 (0x1200)</td>
<td>3494</td>
<td>0.234375</td>
<td>192.168.102.61</td>
<td>192.16</td>
<td></td>
</tr>
</tbody>
</table>
Locating SMB/SMB2 Errors Trace with Color Filters
Filter will find any frame with an SMB error.

```python
```
Filter will find any frame with an SMB2 error.

SMB2Header.Status != 0
AND
smb2.SMB2Header.Status != 259
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://connect.microsoft.com](http://connect.microsoft.com) – Latest Betas, Beta support Forums and Bug Reporting