

# SMB3 Offload Data Transfer (ODX) Network traffic examples

Companion to the presentation from  
the Storage Developer Conference  
by Gordon Ross, Sep. 2016

# Open src (call 16)

The image shows a Wireshark capture window titled "copy-sparse2.snoop". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar with various icons. A display filter is set to "sharing violation sa258666". The packet list pane shows three packets:

No.	Time	Source	Destination	Protocol	Length	Info
15	4.450931	10.10.0.153	10.10.1.57	SMB2	131	Create Response, Error: STATUS_OBJECT_NAME_NOT_FOUND
16	4.451590	10.10.1.57	10.10.0.153	SMB2	282	Create Request File: sparse1
17	4.452175	10.10.0.153	10.10.1.57	SMB2	330	Create Response File: sparse1

The packet details pane for packet 16 is expanded, showing the following structure:

- Frame 16: 282 bytes on wire (2256 bits), 282 bytes captured (2256 bits)
- Ethernet II, Src: Vmware\_ed:15:81 (00:0c:29:ed:15:81), Dst: Vmware\_96:2a:f7 (00:0c:29:96:2a:f7)
- Internet Protocol Version 4, Src: 10.10.1.57, Dst: 10.10.0.153
- Transmission Control Protocol, Src Port: 49186, Dst Port: 445, Seq: 798, Ack: 707, Len: 228
- NetBIOS Session Service
- SMB2 (Server Message Block Protocol version 2)
  - SMB2 Header
    - Create Request (0x05)
      - StructureSize: 0x0039
        - Oplock: Batch oplock (0x09)
        - Impersonation: Impersonation (2)
        - Create Flags: 0x0000000000000000
      - Access Mask: 0x00120089
      - File Attributes: 0x00000000
      - Share Access: 0x00000005, Read, Delete
      - Disposition: Open (if file exists open it, else fail) (1)
      - Create Options: 0x00200044
    - Filename: sparse1
      - Offset: 0x00000078
      - Length: 14
    - ExtraInfo SMB2\_CREATE\_DURABLE\_HANDLE\_REQUEST SMB2\_CREATE\_QUERY\_MAXIMAL\_ACCESS\_REQUEST SMB2\_CREATE\_QUERY\_ON\_DISK\_ID
      - Offset: 0x00000088
      - Length: 88
        - Chain Element: SMB2\_CREATE\_DURABLE\_HANDLE\_REQUEST "DhNq"
        - Chain Element: SMB2\_CREATE\_QUERY\_MAXIMAL\_ACCESS\_REQUEST "MxAc"
        - Chain Element: SMB2\_CREATE\_QUERY\_ON\_DISK\_ID "QFid"

# Open src (reply 17)

The image shows a Wireshark capture window titled "copy-sparse2.snoop". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help), a toolbar with various icons, and a display filter set to "sharing violation sa258666".

No.	Time	Source	Destination	Protocol	Length	Info
16	4.451590	10.10.1.57	10.10.0.153	SMB2	282	Create Request File: sparse1
17	4.452175	10.10.0.153	10.10.1.57	SMB2	330	Create Response File: sparse1
18	4.452477	10.10.1.57	10.10.0.153	SMB2	370	GetInfo Request FILE_INFO/SMB2_FILE_EA_INFO File: s...

The packet details pane for frame 17 shows the following structure:

- Frame 17: 330 bytes on wire (2640 bits), 330 bytes captured (2640 bits)
- Ethernet II, Src: Vmware\_96:2a:f7 (00:0c:29:96:2a:f7), Dst: Vmware\_ed:15:81 (00:0c:29:ed:15:81)
- Internet Protocol Version 4, Src: 10.10.0.153, Dst: 10.10.1.57
- Transmission Control Protocol, Src Port: 445, Dst Port: 49186, Seq: 707, Ack: 1026, Len: 276
- NetBIOS Session Service
- SMB2 (Server Message Block Protocol version 2)
  - SMB2 Header
  - Create Response (0x05)
    - StructureSize: 0x0059
    - Oplock: Batch oplock (0x09)
    - Response Flags: 0x00
    - Create Action: The file existed and was opened (1)
    - Create: May 23, 2016 11:45:49.752778600 Pacific Daylight Time
    - Last Access: May 23, 2016 11:49:31.084749100 Pacific Daylight Time
    - Last Write: May 23, 2016 11:45:49.753670200 Pacific Daylight Time
    - Last Change: May 23, 2016 11:45:49.753670200 Pacific Daylight Time
    - Allocation Size: 1879048704
    - End Of File: 1879048196
    - File Attributes: 0x00000020
    - GUID handle File: sparse1
      - File Id: fe835580-00fd-0000-0300-000000000000
      - [Frame handle opened: 17]
    - ExtraInfo SMB2\_CREATE\_QUERY\_MAXIMAL\_ACCESS\_REQUEST SMB2\_CREATE\_QUERY\_ON\_DISK\_ID SMB2\_CREATE\_DURABLE\_HANDLE\_REQUEST
      - Offset: 0x00000098
      - Length: 120
      - Chain Element: SMB2\_CREATE\_QUERY\_MAXIMAL\_ACCESS\_REQUEST "MxAc"
      - Chain Element: SMB2\_CREATE\_QUERY\_ON\_DISK\_ID "0e1d"

# Open dst (call 39)

The image shows a Wireshark capture window titled "copy-sparse2.snoop". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar with various analysis tools. A display filter is set to "sharing violation sa258666". The packet list pane shows three packets:

No.	Time	Source	Destination	Protocol	Length	Info
38	4.483827	10.10.0.153	10.10.1.57	SMB2	342	GetInfo Response;GetInfo Response;GetInfo Response
39	4.484296	10.10.1.57	10.10.0.153	SMB2	338	Create Request File: sparse1 - Copy (3)
40	4.485163	10.10.0.153	10.10.1.57	SMB2	330	Create Response File: sparse1 - Copy (3)

The packet details pane for packet 39 shows the following structure:

- Frame 39: 338 bytes on wire (2704 bits), 338 bytes captured (2704 bits)
- Ethernet II, Src: Vmware\_ed:15:81 (00:0c:29:ed:15:81), Dst: Vmware\_96:2a:f7 (00:0c:29:96:2a:f7)
- Internet Protocol Version 4, Src: 10.10.1.57, Dst: 10.10.0.153
- Transmission Control Protocol, Src Port: 49186, Dst Port: 445, Seq: 2963, Ack: 2954, Len: 284
- NetBIOS Session Service
- SMB2 (Server Message Block Protocol version 2)
  - SMB2 Header
    - Create Request (0x05)
      - StructureSize: 0x0039
        - Oplock: Batch oplock (0x09)
        - Impersonation: Impersonation (2)
        - Create Flags: 0x0000000000000000
      - Access Mask: 0x0017019f
      - File Attributes: 0x00000020
      - Share Access: 0x00000000
      - Disposition: Create (if file exists fail, else create it) (2)
      - Create Options: 0x00000044
      - Filename: sparse1 - Copy (3)
        - Offset: 0x00000078
        - Length: 36
      - ExtraInfo SMB2\_CREATE\_DURABLE\_HANDLE\_REQUEST SMB2\_CREATE\_ALLOCATION\_SIZE SMB2\_CREATE\_QUERY\_MAXIMAL\_ACCESS\_REQUEST SMB2\_CREATE\_QUERY
        - Offset: 0x000000a0
        - Length: 120
          - Chain Element: SMB2\_CREATE\_DURABLE\_HANDLE\_REQUEST "DhNq"
          - Chain Element: SMB2\_CREATE\_ALLOCATION\_SIZE "AlSi"
          - Chain Element: SMB2\_CREATE\_QUERY\_MAXIMAL\_ACCESS\_REQUEST "MvAc"

# Open dst (reply 40)

The image shows a Wireshark capture window titled "copy-sparse2.snoop". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help), a toolbar with various icons, and a display filter set to "sharing violation sa258666".

No.	Time	Source	Destination	Protocol	Length	Info
39	4.484296	10.10.1.57	10.10.0.153	SMB2	338	Create Request File: sparse1 - Copy (3)
40	4.485163	10.10.0.153	10.10.1.57	SMB2	330	Create Response File: sparse1 - Copy (3)
41	4.486025	10.10.1.57	10.10.0.153	SMB2	178	Ioctl Request FSCTL_SRV_REQUEST_RESUME_KEY File: sp...

The detailed view of frame 40 shows the following structure:

- Frame 40: 330 bytes on wire (2640 bits), 330 bytes captured (2640 bits)
- Ethernet II, Src: Vmware\_96:2a:f7 (00:0c:29:96:2a:f7), Dst: Vmware\_ed:15:81 (00:0c:29:ed:15:81)
- Internet Protocol Version 4, Src: 10.10.0.153, Dst: 10.10.1.57
- Transmission Control Protocol, Src Port: 445, Dst Port: 49186, Seq: 2954, Ack: 3247, Len: 276
- NetBIOS Session Service
- SMB2 (Server Message Block Protocol version 2)
  - SMB2 Header
    - Create Response (0x05)
      - StructureSize: 0x0059
        - Oplock: Batch oplock (0x09)
      - Response Flags: 0x00
        - Create Action: The file did not exist but was created (2)
        - Create: Jun 3, 2016 07:47:22.046473800 Pacific Daylight Time
        - Last Access: Jun 3, 2016 07:47:22.046473800 Pacific Daylight Time
        - Last Write: Jun 3, 2016 07:47:22.046473800 Pacific Daylight Time
        - Last Change: Jun 3, 2016 07:47:22.046473800 Pacific Daylight Time
        - Allocation Size: 1879048704
        - End Of File: 0
      - File Attributes: 0x00000020
    - GUID handle File: sparse1 - Copy (3)
      - File Id: fe835870-00fd-0000-0400-000000000000
      - [Frame handle opened: 40]
    - ExtraInfo SMB2\_CREATE\_QUERY\_MAXIMAL\_ACCESS\_REQUEST SMB2\_CREATE\_QUERY\_ON\_DISK\_ID SMB2\_CREATE\_DURABLE\_HANDLE\_REQUEST
      - Offset: 0x00000098
      - Length: 120
        - Chain Element: SMB2\_CREATE\_QUERY\_MAXIMAL\_ACCESS\_REQUEST "MxAc"
        - Chain Element: SMB2\_CREATE\_QUERY\_ON\_DISK\_ID "0e5d"

# Read src (call 45)

The image shows a Wireshark capture window titled 'copy-sparse2.snoop'. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar with various icons. A display filter is set to 'sharing violation sa258666'. The packet list pane shows four packets:

No.	Time	Source	Destination	Protocol	Length	Info
44	4.486898	10.10.0.153	10.10.1.57	SMB2	126	SetInfo Response
45	4.487251	10.10.1.57	10.10.0.153	SMB2	210	Ioct1 Request FSCTL_OFFLOAD_READ File: sparse1
46	4.514585	10.10.0.153	10.10.1.57	SMB2	698	Ioct1 Response FSCTL_OFFLOAD_READ File: sparse1
47	4.531139	10.10.1.57	10.10.0.153	TCP	60	49186→445 [ACK] Seq=3635 Ack=4094 Win=2053 Len=0

The packet details pane for packet 45 is expanded, showing the following structure:

- Frame 45: 210 bytes on wire (1680 bits), 210 bytes captured (1680 bits)
- Ethernet II, Src: Vmware\_ed:15:81 (00:0c:29:ed:15:81), Dst: Vmware\_96:2a:f7 (00:0c:29:96:2a:f7)
- Internet Protocol Version 4, Src: 10.10.1.57, Dst: 10.10.0.153
- Transmission Control Protocol, Src Port: 49186, Dst Port: 445, Seq: 3479, Ack: 3450, Len: 156
- NetBIOS Session Service
- SMB2 (Server Message Block Protocol version 2)
  - SMB2 Header
  - Ioct1 Request (0x0b)
    - StructureSize: 0x0039
    - Function: FSCTL\_OFFLOAD\_READ (0x00094264)
    - GUID handle File: sparse1
    - Max Ioctl In Size: 0
    - Max Ioctl Out Size: 528
    - Flags: 0x00000001
    - In Data
      - Offset: 0x00000078
      - Length: 32
      - Size: 32
      - Flags: 0x00000000
      - TokenTimeToLive: 0
      - Reserved: 00000000
      - FileOffset: 0
      - CopyLength: 1880096768
    - Out Data: NO DATA
      - Offset: 0x00000078
      - Length: 0

# Read src (reply 46)

The screenshot shows a Wireshark window titled "copy-sparse2.snoop". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help), a toolbar with various icons, and a display filter set to "sharing violation sa258666".

No.	Time	Source	Destination	Protocol	Length	Info
44	4.486898	10.10.0.153	10.10.1.57	SMB2	126	SetInfo Response
45	4.487251	10.10.1.57	10.10.0.153	SMB2	210	Ioctl Request FSCTL_OFFLOAD_READ File: sparse1
46	4.514585	10.10.0.153	10.10.1.57	SMB2	698	Ioctl Response FSCTL_OFFLOAD_READ File: sparse1
47	4.531139	10.10.1.57	10.10.0.153	TCP	60	49186→445 [ACK] Seq=3635 Ack=4094 Win=2053 Len=0

Packet 46 details:

- Frame 46: 698 bytes on wire (5584 bits), 698 bytes captured (5584 bits)
- Ethernet II, Src: Vmware\_96:2a:f7 (00:0c:29:96:2a:f7), Dst: Vmware\_ed:15:81 (00:0c:29:ed:15:81)
- Internet Protocol Version 4, Src: 10.10.0.153, Dst: 10.10.1.57
- Transmission Control Protocol, Src Port: 445, Dst Port: 49186, Seq: 3450, Ack: 3635, Len: 644
- NetBIOS Session Service
- SMB2 (Server Message Block Protocol version 2)
  - SMB2 Header
    - Ioctl Response (0x0b)
      - StructureSize: 0x0031
        - unknown: 0000
      - Function: FSCTL\_OFFLOAD\_READ (0x00094264)
      - GUID handle File: sparse1
      - In Data: NO DATA
      - Out Data
        - Offset: 0x00000070
        - Length: 528
        - Size: 528
        - Flags: 0x00000000
        - TransferLength: 268435456
      - Token (IdType 0x10001)
        - TokenType: 0x00010001
        - Reserved: 0000
        - TokenIdLength: 32
        - TokenId: Opaque Data

# Write dst (call 48)

The screenshot shows a Wireshark capture window titled "copy-sparse2.snoop". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help), a toolbar with various icons, and a display filter set to "sharing violation sa258666".

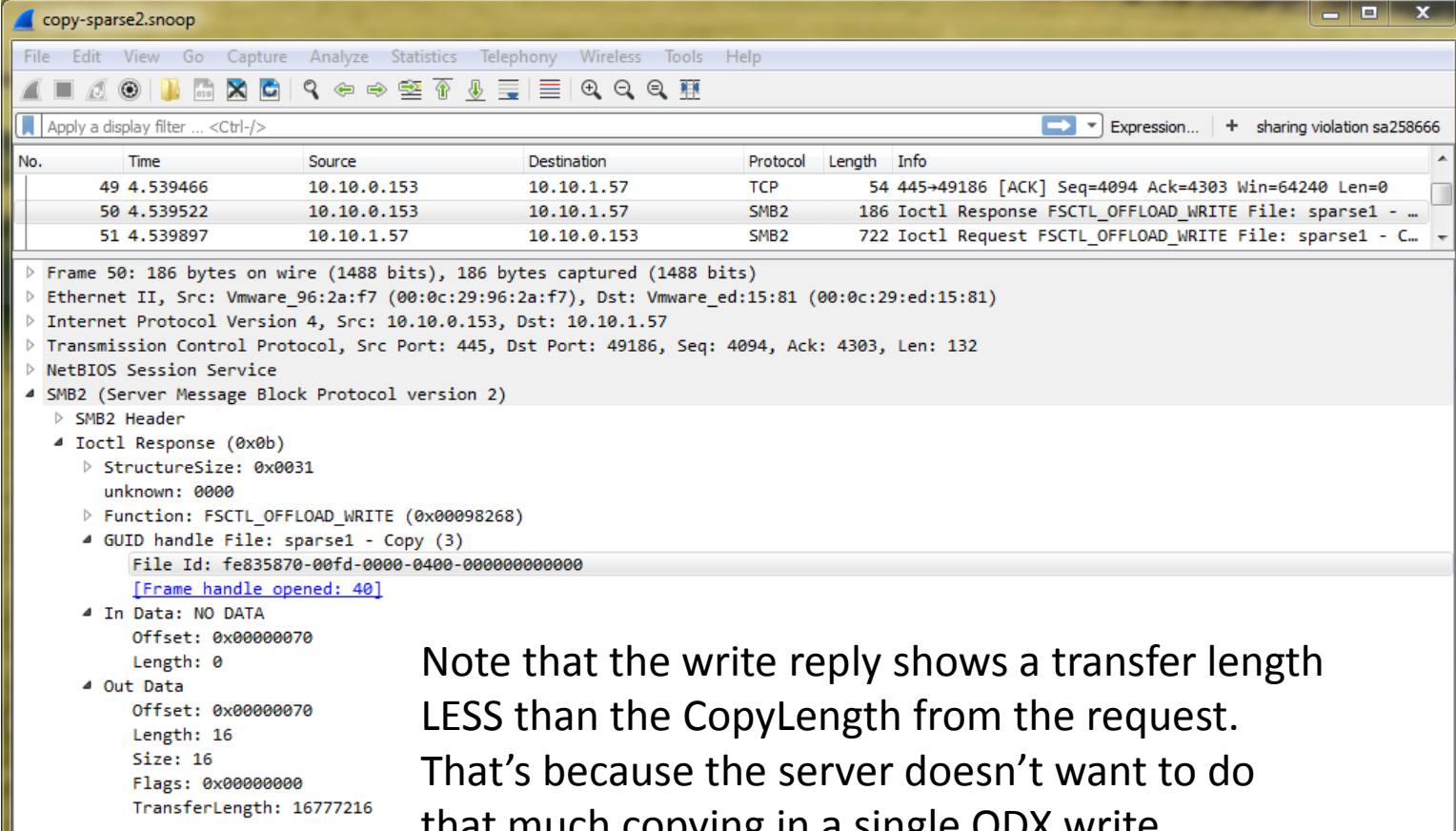
No.	Time	Source	Destination	Protocol	Length	Info
47	4.531139	10.10.1.57	10.10.0.153	TCP	60	49186→445 [ACK] Seq=3635 Ack=4094 Win=2053 Len=0
48	4.533356	10.10.1.57	10.10.0.153	SMB2	722	Ioctl Request FSCTL_OFFLOAD_WRITE File: sparse1 - C...
49	4.539466	10.10.0.153	10.10.1.57	TCP	54	445→49186 [ACK] Seq=4094 Ack=4303 Win=64240 Len=0

The packet details pane for packet 48 shows the following structure:

- Ethernet II, Src: Vmware\_ed:15:81 (00:0c:29:ed:15:81), Dst: Vmware\_96:2a:f7 (00:0c:29:96:2a:f7)
- Internet Protocol Version 4, Src: 10.10.1.57, Dst: 10.10.0.153
- Transmission Control Protocol, Src Port: 49186, Dst Port: 445, Seq: 3635, Ack: 4094, Len: 668
- NetBIOS Session Service
- SMB2 (Server Message Block Protocol version 2)
  - SMB2 Header
    - Ioctl Request (0x0b)
      - StructureSize: 0x0039
      - Function: FSCTL\_OFFLOAD\_WRITE (0x00098268)
      - GUID handle File: sparse1 - Copy (3)
        - Max Ioctl In Size: 0
        - Max Ioctl Out Size: 16
      - Flags: 0x00000001
      - In Data
        - Offset: 0x00000078
        - Length: 544
        - Size: 544
        - Flags: 0x00000000
        - FileOffset: 0
        - CopyLength: 268435456
        - TokenOffset: 0
        - Token (IdType 0x10001)
          - TokenType: 0x00010001
          - Reserved: 0000
          - TokenIdLength: 32
          - TokenId: Opaque Data
      - Out Data: NO DATA



# Write dst (reply 50)

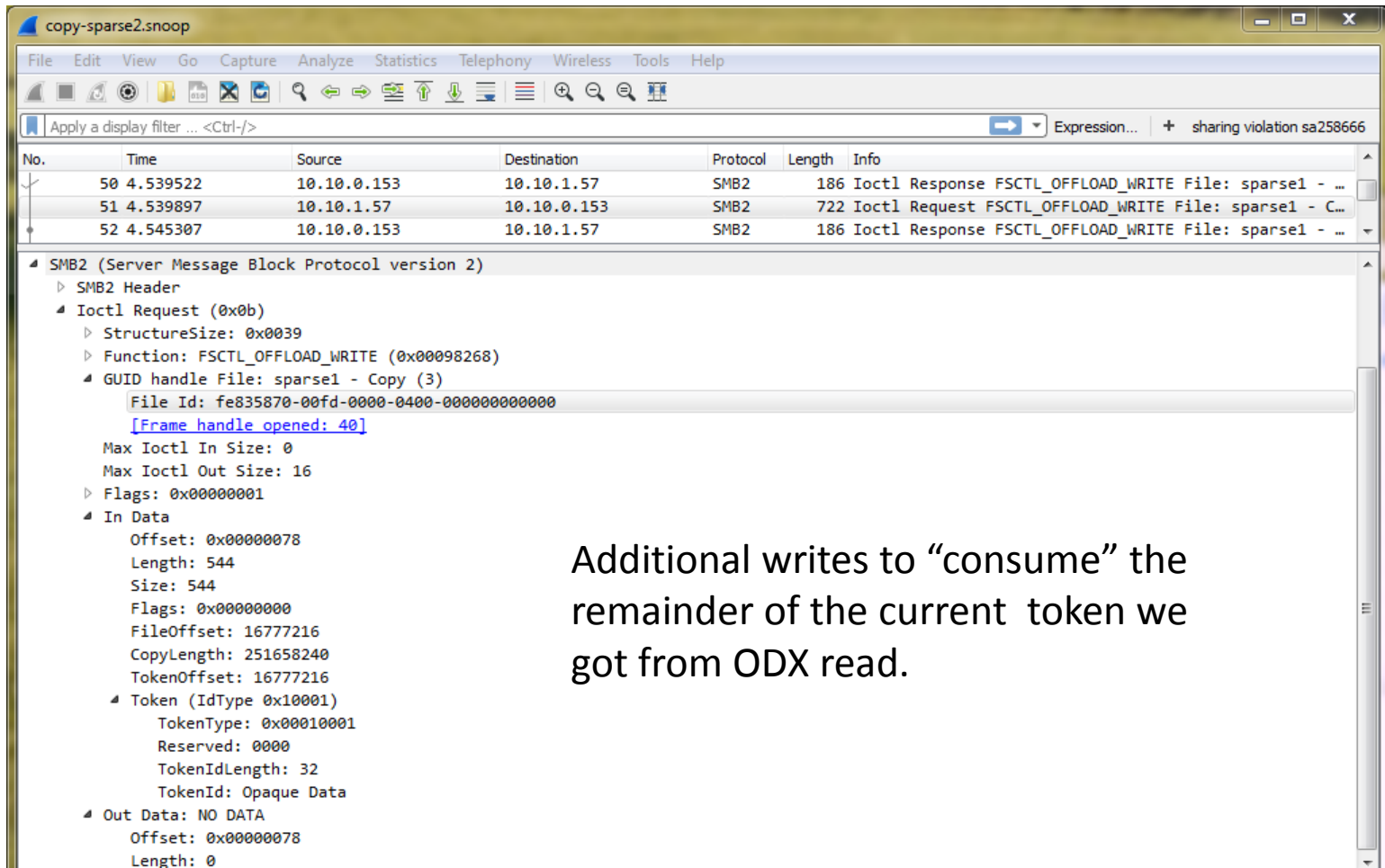


The screenshot shows a Wireshark capture of network traffic. The main pane displays a list of captured packets. Packet 50 is highlighted, showing it is an SMB2 Ioctl Response from 10.10.0.153 to 10.10.1.57. The details pane for packet 50 shows the SMB2 header and the Ioctl Response structure. The 'GUID handle File: sparse1 - Copy (3)' is expanded to show the 'File Id: fe835870-00fd-0000-0400-000000000000'. The 'In Data' section shows 'NO DATA' with an offset of 0x00000070 and a length of 0. The 'Out Data' section shows an offset of 0x00000070, a length of 16, a size of 16, and a transfer length of 16777216 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
49	4.539466	10.10.0.153	10.10.1.57	TCP	54	445->49186 [ACK] Seq=4094 Ack=4303 Win=64240 Len=0
50	4.539522	10.10.0.153	10.10.1.57	SMB2	186	Ioctl Response FSCTL_OFFLOAD_WRITE File: sparse1 - ...
51	4.539897	10.10.1.57	10.10.0.153	SMB2	722	Ioctl Request FSCTL_OFFLOAD_WRITE File: sparse1 - C...

Note that the write reply shows a transfer length LESS than the CopyLength from the request. That's because the server doesn't want to do that much copying in a single ODX write.

# Write dst (call 51)



The screenshot shows a Wireshark capture window titled "copy-sparse2.snoop". The main pane displays a list of network packets. Packet 51 is selected, and its details pane is expanded to show SMB2 protocol information.

No.	Time	Source	Destination	Protocol	Length	Info
50	4.539522	10.10.0.153	10.10.1.57	SMB2	186	Ioctl Response FSCTL_OFFLOAD_WRITE File: sparse1 - ...
51	4.539897	10.10.1.57	10.10.0.153	SMB2	722	Ioctl Request FSCTL_OFFLOAD_WRITE File: sparse1 - C...
52	4.545307	10.10.0.153	10.10.1.57	SMB2	186	Ioctl Response FSCTL_OFFLOAD_WRITE File: sparse1 - ...

The details pane for packet 51 shows the following structure:

- SMB2 (Server Message Block Protocol version 2)
  - SMB2 Header
    - Ioctl Request (0x0b)
      - StructureSize: 0x0039
      - Function: FSCTL\_OFFLOAD\_WRITE (0x00098268)
      - GUID handle File: sparse1 - Copy (3)
        - File Id: fe835870-00fd-0000-0400-000000000000
        - [Frame handle opened: 40]
      - Max Ioctl In Size: 0
      - Max Ioctl Out Size: 276
      - Flags: 0x00000001
      - In Data
        - Offset: 0x00000078
        - Length: 544
        - Size: 544
        - Flags: 0x00000000
        - FileOffset: 16777216
        - CopyLength: 251658240
        - TokenOffset: 16777216
        - Token (IdType 0x10001)
          - TokenType: 0x00010001
          - Reserved: 0000
          - TokenIdLength: 32
          - TokenId: Opaque Data
      - Out Data: NO DATA
        - Offset: 0x00000078
        - Length: 0

Additional writes to “consume” the remainder of the current token we got from ODX read.

# Write dst (reply 52)

copy-sparse2.snoop

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... + sharing violation sa258666

No.	Time	Source	Destination	Protocol	Length	Info
50	4.539522	10.10.0.153	10.10.1.57	SMB2	186	Ioctl Response FSCTL_OFFLOAD_WRITE File: sparse1 - ...
51	4.539897	10.10.1.57	10.10.0.153	SMB2	722	Ioctl Request FSCTL_OFFLOAD_WRITE File: sparse1 - C...
52	4.545307	10.10.0.153	10.10.1.57	SMB2	186	Ioctl Response FSCTL_OFFLOAD_WRITE File: sparse1 - ...

▶ Frame 52: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits)

- ▶ Ethernet II, Src: Vmware\_96:2a:f7 (00:0c:29:96:2a:f7), Dst: Vmware\_ed:15:81 (00:0c:29:ed:15:81)
- ▶ Internet Protocol Version 4, Src: 10.10.0.153, Dst: 10.10.1.57
- ▶ Transmission Control Protocol, Src Port: 445, Dst Port: 49186, Seq: 4226, Ack: 4971, Len: 132
- ▶ NetBIOS Session Service
- ▶ SMB2 (Server Message Block Protocol version 2)
  - ▶ SMB2 Header
    - ▶ Ioctl Response (0x0b)
      - ▶ StructureSize: 0x0031  
unknown: 0000
      - ▶ Function: FSCTL\_OFFLOAD\_WRITE (0x00098268)
      - ▶ GUID handle File: sparse1 - Copy (3)
        - File Id: fe835870-00fd-0000-0400-000000000000
        - [Frame handle opened: 40]
    - ▶ In Data: NO DATA  
Offset: 0x00000070  
Length: 0
    - ▶ Out Data  
Offset: 0x00000070  
Length: 16  
Size: 16  
Flags: 0x00000000  
TransferLength: 16777216

Again, server elected to copy less than the requested size. Client issues more writes until the current ODX read token is consumed.

# Write dst (many)

copy-sparse2.snoop

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... + sharing violation sa258666

No.	Time	Source	Destination	Protocol	Length	Info
72	4.829299	10.10.0.153	10.10.1.57	SMB2	186	Ioctl Response FSCTL_OFFLOAD_WRITE File: sparse1 - ...
73	4.829751	10.10.1.57	10.10.0.153	SMB2	722	Ioctl Request FSCTL_OFFLOAD_WRITE File: sparse1 - C...
74	4.829788	10.10.0.153	10.10.1.57	TCP	54	445→49186 [ACK] Seq=5150 Ack=9647 Win=64240 Len=0
75	4.870514	10.10.0.153	10.10.1.57	SMB2	186	Ioctl Response FSCTL_OFFLOAD_WRITE File: sparse1 - ...
76	4.871213	10.10.1.57	10.10.0.153	SMB2	722	Ioctl Request FSCTL_OFFLOAD_WRITE File: sparse1 - C...
77	4.906316	10.10.1.57	10.10.0.153	TCP	722	[TCP Retransmission] 49186→445 [PSH, ACK] Seq=9647 ...
78	4.906409	10.10.0.153	10.10.1.57	TCP	54	445→49186 [ACK] Seq=5282 Ack=10315 Win=64240 Len=0
79	4.908235	10.10.0.153	10.10.1.57	SMB2	186	Ioctl Response FSCTL_OFFLOAD_WRITE File: sparse1 - ...
80	4.908649	10.10.1.57	10.10.0.153	SMB2	722	Ioctl Request FSCTL_OFFLOAD_WRITE File: sparse1 - C...
81	4.908723	10.10.0.153	10.10.1.57	TCP	54	445→49186 [ACK] Seq=5414 Ack=10983 Win=64240 Len=0
82	4.962437	10.10.0.153	10.10.1.57	SMB2	186	Ioctl Response FSCTL_OFFLOAD_WRITE File: sparse1 - ...
83	4.963113	10.10.1.57	10.10.0.153	SMB2	722	Ioctl Request FSCTL_OFFLOAD_WRITE File: sparse1 - C...
84	4.998119	10.10.0.153	10.10.1.57	SMB2	186	Ioctl Response FSCTL_OFFLOAD_WRITE File: sparse1 - ...
85	4.998770	10.10.1.57	10.10.0.153	SMB2	722	Ioctl Request FSCTL_OFFLOAD_WRITE File: sparse1 - C...
86	5.028927	10.10.0.153	10.10.1.57	TCP	54	445→49186 [ACK] Seq=5678 Ack=12319 Win=64240 Len=0
87	5.038162	10.10.0.153	10.10.1.57	SMB2	186	Ioctl Response FSCTL_OFFLOAD_WRITE File: sparse1 - ...
88	5.038716	10.10.1.57	10.10.0.153	SMB2	722	Ioctl Request FSCTL_OFFLOAD_WRITE File: sparse1 - C...
89	5.097324	10.10.0.153	10.10.1.57	SMB2	186	Ioctl Response FSCTL_OFFLOAD_WRITE File: sparse1 - ...
90	5.097766	10.10.1.57	10.10.0.153	SMB2	722	Ioctl Request FSCTL_OFFLOAD_WRITE File: sparse1 - C...
91	5.108789	10.10.0.153	10.10.1.57	TCP	54	445→49186 [ACK] Seq=5942 Ack=13655 Win=64240 Len=0
92	5.150889	10.10.0.153	10.10.1.57	SMB2	186	Ioctl Response FSCTL_OFFLOAD_WRITE File: sparse1 - ...
93	5.151570	10.10.1.57	10.10.0.153	SMB2	722	Ioctl Request FSCTL_OFFLOAD_WRITE File: sparse1 - C...
94	5.184491	10.10.0.153	10.10.1.57	SMB2	186	Ioctl Response FSCTL_OFFLOAD_WRITE File: sparse1 - ...
95	5.185196	10.10.1.57	10.10.0.153	SMB2	210	Ioctl Request FSCTL_OFFLOAD_READ File: sparse1
96	5.185414	10.10.0.153	10.10.1.57	SMB2	698	Ioctl Response FSCTL_OFFLOAD_READ File: sparse1

StructureSize: 0x0039  
Function: FSCTL\_OFFLOAD\_READ (0x00094264)  
GUID handle File: sparse1  
File Id: fe835580-00fd-0000-0300-000000000000  
[\[Frame handle opened: 17\]](#)

