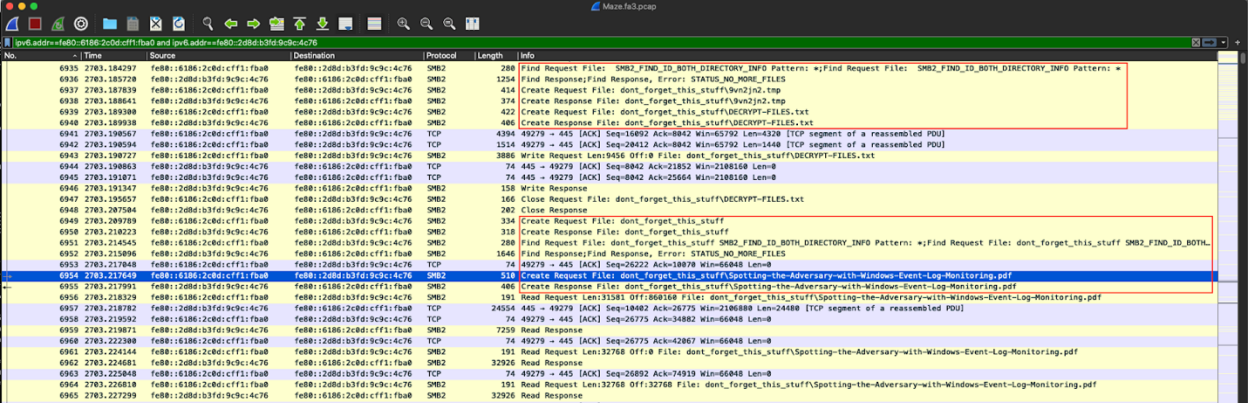
Maze.fa3.pcap
ipv6.addr==fe80::6186:2c0d:cff1:fba0 and ipv6.addr==fe80::2d8d:b3fd:9c9c:4c76
No. Time Source Destination Protocol Length Info
6935 2703.184297 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 SMB2 280 Find Request File: SMB2_FIND_ID_BOTH_DIRECTORY_INFO Pattern: *;Find Request File: SMB2_FIND_ID_BOTH_DIRECTORY_INFO Pattern: *
6936 2703.185720 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 SMB2 1254 Find Response;Find Response, Error: STATUS_NO_MORE_FILES
6937 2703.187839 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 SMB2 414 Create Request File: dont_forget_this_stuff\9vn2jn2.tmp
6938 2703.188641 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 SMB2 374 Create Response File: dont_forget_this_stuff\9vn2jn2.tmp
6939 2703.189300 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 SMB2 422 Create Request File: dont_forget_this_stuff\DECRYPT-FILES.txt
6940 2703.189938 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 SMB2 406 Create Response File: dont_forget_this_stuff\DECRYPT-FILES.txt
6941 2703.190567 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 TCP 4394 49279 → 445 [ACK] Seq=16092 Ack=8042 Win=65792 Len=4320 [TCP segment of a reassembled PDU]
6942 2703.190594 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 TCP 1514 49279 → 445 [ACK] Seq=20412 Ack=8042 Win=65792 Len=1440 [TCP segment of a reassembled PDU]
6943 2703.190727 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 SMB2 3886 Write Request Len:9456 Off:0 File: dont_forget_this_stuff\DECRYPT-FILES.txt
6944 2703.190863 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 TCP 74 445 → 49279 [ACK] Seq=8042 Ack=21852 Win=2108160 Len=0
6945 2703.191071 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 TCP 74 445 → 49279 [ACK] Seq=8042 Ack=25664 Win=2108160 Len=0
6946 2703.191347 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 SMB2 158 Write Response
6947 2703.195657 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 SMB2 166 Close Request File: dont_forget_this_stuff\DECRYPT-FILES.txt
6948 2703.207504 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 SMB2 202 Close Response
6949 2703.209789 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 SMB2 334 Create Request File: dont_forget_this_stuff
6950 2703.210223 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 SMB2 318 Create Response File: dont_forget_this_stuff
6951 2703.214545 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 SMB2 280 Find Request File: dont_forget_this_stuff SMB2_FIND_ID_BOTH_DIRECTORY_INFO Pattern: *;Find Request File: dont_forget_this_stuff SMB2_FIND_ID_BOTH…
6952 2703.215896 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 SMB2 1646 Find Response;Find Response, Error: STATUS_NO_MORE_FILES
6953 2703.217048 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 TCP 74 49279 → 445 [ACK] Seq=26222 Ack=10070 Win=66048 Len=0
6954 2703.217649 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 SMB2 510 Create Request File: dont_forget_this_stuff\Spotting-the-Adversary-with-Windows-Event-Log-Monitoring.pdf
6955 2703.217991 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 SMB2 406 Create Response File: dont_forget_this_stuff\Spotting-the-Adversary-with-Windows-Event-Log-Monitoring.pdf
6956 2703.218329 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 SMB2 191 Read Request Len:31581 Off:860160 File: dont_forget_this_stuff\Spotting-the-Adversary-with-Windows-Event-Log-Monitoring.pdf
6957 2703.218782 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 TCP 24554 445 → 49279 [ACK] Seq=10402 Ack=26775 Win=2106880 Len=24488 [TCP segment of a reassembled PDU]
6958 2703.219592 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 TCP 74 49279 → 445 [ACK] Seq=26775 Ack=34802 Win=66048 Len=0
6959 2703.219871 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 SMB2 7259 Read Response
6960 2703.222300 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 TCP 74 49279 → 445 [ACK] Seq=26775 Ack=42067 Win=66048 Len=0
6961 2703.224144 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 SMB2 191 Read Request Len:32768 Off:0 File: dont_forget_this_stuff\Spotting-the-Adversary-with-Windows-Event-Log-Monitoring.pdf
6962 2703.224681 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 SMB2 32926 Read Response
6963 2703.225048 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 TCP 74 49279 → 445 [ACK] Seq=26892 Ack=74919 Win=66048 Len=0
6964 2703.226810 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 SMB2 191 Read Request Len:32768 Off:32768 File: dont_forget_this_stuff\Spotting-the-Adversary-with-Windows-Event-Log-Monitoring.pdf
6965 2703.227299 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 SMB2 32926 Read Response