

Notice the TCP Min/Max Window summary info: immediate feedback on whether or not TCP Window size every scraped the bottom. And notice TCP Invalid Checksum total

OmniPeek - [Flow carbon-b-svif1:3260 <-> isis-1-iscsi-1:blackjack]

File Edit View Capture Send Monitor Tools Window Help

Start or Stop Capture

Client		carbon-b-svif1	isis-1-iscsi-1
Name		carbon-b-svif1	isis-1-iscsi-1
Network Address		10.111.42.51	10.111.42.37
Packets Sent		28,078	13,476
Bytes Sent		38,146,226	10,349,076
Average Size (Bytes)		1,358	767
First Packet Time		9:56:08.105250	9:56:08.104872
Last Packet Time		10:00:20.864485	10:00:20.864489
Routed Hops		0	0
TCP Min Window		65,535	52,983
TCP Max Window		65,535	65,535

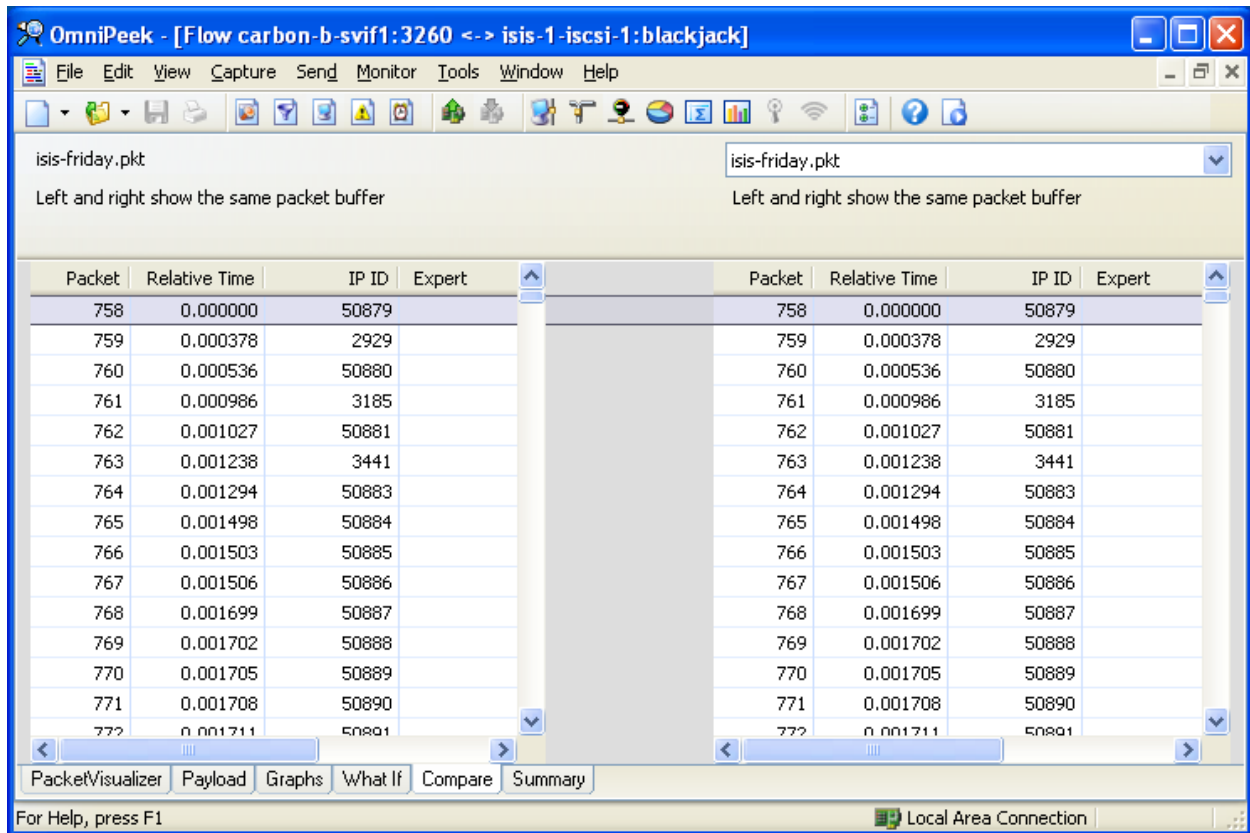
	Response Time	C->S bps	S->C bps
Best	0.000002	66,203,611.000	58,789,936.000
Worst	5.999360	282.000	755.000
Average	0.033675	10,165,388.000	6,254,727.000
Turns	7,112	28,078	13,476

Layer	Event	Count
Client/Server	Busy Network or Server	41
Client/Server	Low Server-to-Client Throughput	2
Client/Server	Slow Server Response Time	78
Transport	TCP Invalid Checksum	8

PacketVisualizer Payload Graphs What If Compare Summary

Starts or stops capture Local Area Connection

With a single trace, the display below is meaningless ... but consider what happens when you load separate traces into this display, one taken inside the firewall and one taken outside.



In the What If screen, you play with packet size, latency, contention, number of users, etc., and OmniPeek recalculates summary statistics (based on the current flow you are analyzing) to give you a glimpse at how performance and utilization might change.

OmniPeek - [Flow carbon-b-svif1:3260 <-> isis-1-iscsi-1:blackjack]

File Edit View Capture Send Monitor Tools Window Help

Protocol/Network

Avg send packet size: 1358

Avg receive packet size: 767

Latency (ms): 0

Contention (ms): 33

Application

Simultaneous users: 1

Packets per transaction: 3

Client processing (ms): 0

Server processing (ms): 0

Packet send: 2 to 1 receive ratio

Client/Server	Bits/sec	Max Pkts/sec	Utilization	Transaction Time (s...)
Client	32,000	2.21	75.13%	
Server	32,000	1.11	21.22%	0.903750
Client	56,000	3.77	73.13%	
Server	56,000	1.88	20.65%	0.530571
Client	64,000	4.27	72.48%	
Server	64,000	2.14	20.47%	0.468375
Client	128,000	7.98	67.71%	
Server	128,000	3.99	19.12%	0.250687
Client	224,000	12.71	61.63%	
Server	224,000	6.35	17.40%	0.157392
Client	256,000	14.10	59.84%	
Server	256,000	7.05	16.90%	0.141843
Client	384,000	18.95	53.60%	
Server	384,000	9.47	15.14%	0.105562
Client	512,000	22.88	48.54%	
Server	512,000	11.44	13.71%	0.087421
Client	768,000	28.87	40.84%	
Server	768,000	14.43	11.53%	0.069281
Client	1,024,000	33.22	35.24%	
Server	1,024,000	16.61	9.95%	0.060210
Client	1,536,000	39.11	27.66%	
Server	1,536,000	19.55	7.81%	0.051140
Client	2,048,000	42.91	22.76%	
Server	2,048,000	21.46	6.43%	0.046605
Client	4,000,000	50.04	13.59%	
Server	4,000,000	25.02	3.84%	0.039966
Client	10,000,000	55.81	6.15%	
Server	10,000,000	27.91	1.76%	0.035834
Client	16,000,000	57.57	3.91%	
Server	16,000,000	28.78	1.10%	0.034741
Client	45,000,000	59.49	1.44%	
Server	45,000,000	29.74	0.41%	0.033619
Client	100,000,000	60.09	0.66%	
Server	100,000,000	30.04	0.19%	0.033283
Client	155,520,000	60.28	0.42%	
Server	155,520,000	30.14	0.12%	0.033179
Client	622,080,000	60.52	0.11%	
Server	622,080,000	30.26	0.03%	0.033044
Client	1,000,000,...	60.55	0.07%	
Server	1,000,000,...	30.28	0.02%	0.033028

PacketVisualizer Payload Graphs What If Compare Summary

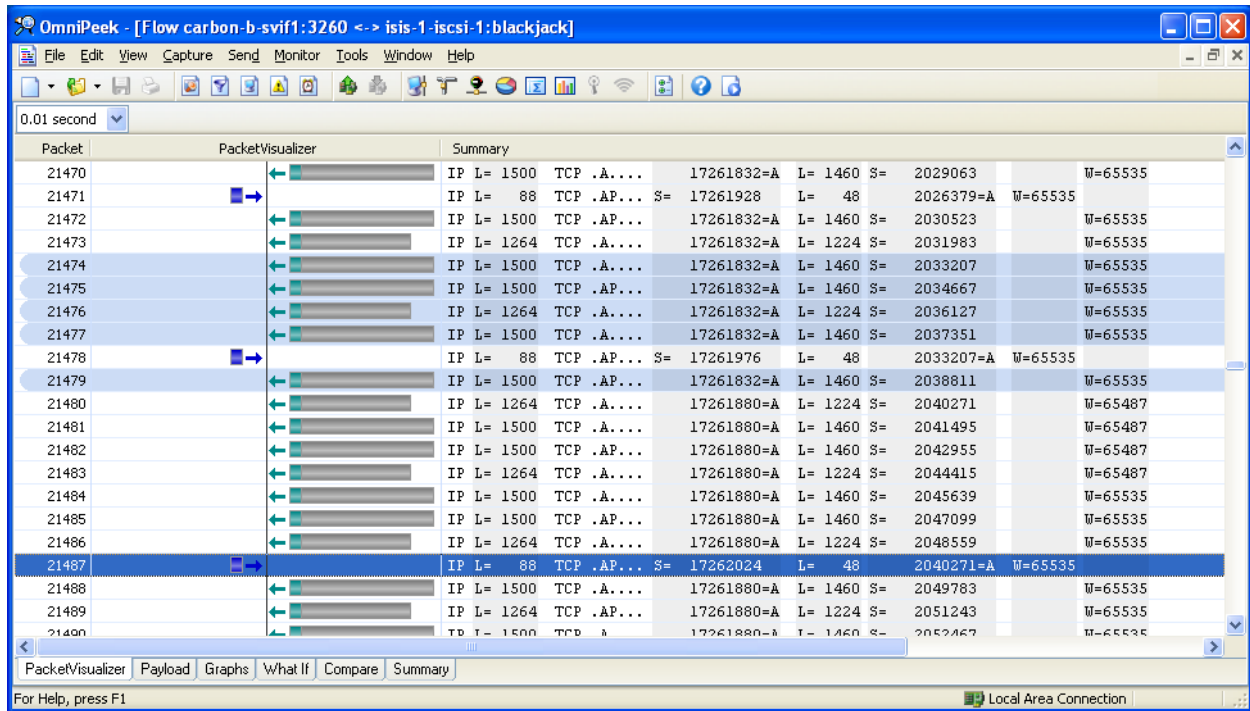
For Help, press F1 Local Area Connection

## PacketVisualizer summarizes IP length, TCP flags, TCP length, and Window size

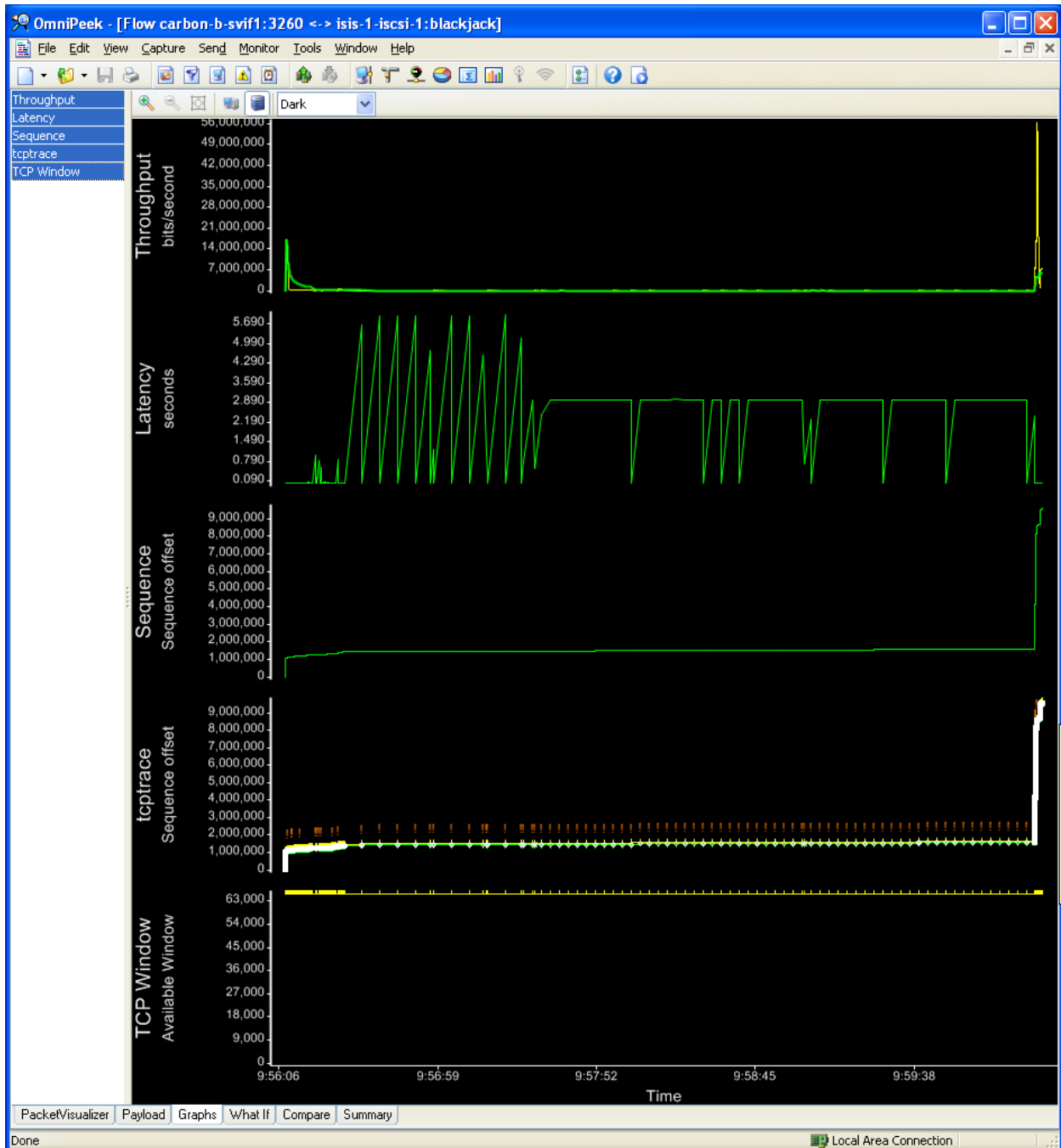
The screenshot shows the OmniPeek interface with the PacketVisualizer window open. The window displays a list of packets from packet 758 to 804. Each row represents a packet and includes a visual bar chart of its components, a summary of the IP and TCP headers, and the window size (W=).

Packet	PacketVisualizer	Summary
758		IP L= 88 TCP .AP... 0=A L= 48 S= 0 W=65535
759		IP L= 88 TCP .AP... S= 0 L= 48 48=A W=65535
760		IP L= 88 TCP .AP... 48=A L= 48 S= 48 W=65487
761		IP L= 88 TCP .AP... S= 48 L= 48 96=A W=65535
762		IP L= 376 TCP .AP... 48=A L= 336 S= 96 W=65535
763		IP L= 592 TCP .AP... S= 96 L= 552 432=A W=65535
764		IP L= 136 TCP .AP... 648=A L= 96 S= 432 W=64983
765		IP L= 1500 TCP .AP... 648=A L= 1460 S= 528 W=65223
766		IP L= 1500 TCP .A... 648=A L= 1460 S= 1988 W=65223
767		IP L= 848 TCP .AP... 648=A L= 808 S= 3448 W=65223
768		IP L= 1500 TCP .AP... 648=A L= 1460 S= 4256 W=65535
769		IP L= 1500 TCP .A... 648=A L= 1460 S= 5716 W=65535
770		IP L= 1456 TCP .A... 648=A L= 1416 S= 7176 W=65535
771		IP L= 1500 TCP .A... 648=A L= 1460 S= 8592 W=65535
772		IP L= 1500 TCP .A... 648=A L= 1460 S= 10052 W=65535
773		IP L= 1264 TCP .AP... 648=A L= 1224 S= 11512 W=65535
774		IP L= 1500 TCP .A... 648=A L= 1460 S= 12736 W=65535
775		IP L= 1500 TCP .A... 648=A L= 1460 S= 14196 W=65535
776		IP L= 1264 TCP .AP... 648=A L= 1224 S= 15656 W=65535
777		IP L= 1500 TCP .A... 648=A L= 1460 S= 16880 W=65535
778		IP L= 1500 TCP .A... 648=A L= 1460 S= 18340 W=65535
779		IP L= 1264 TCP .AP... 648=A L= 1224 S= 19800 W=65535
780		IP L= 1500 TCP .A... 648=A L= 1460 S= 21024 W=65535
781		IP L= 1500 TCP .A... 648=A L= 1460 S= 22484 W=65535
782		IP L= 1264 TCP .AP... 648=A L= 1224 S= 23944 W=65535
783		IP L= 1500 TCP .A... 648=A L= 1460 S= 25168 W=65535
784		IP L= 1500 TCP .A... 648=A L= 1460 S= 26628 W=65535
785		IP L= 1264 TCP .AP... 648=A L= 1224 S= 28088 W=65535
786		IP L= 1500 TCP .A... 648=A L= 1460 S= 29312 W=65535
787		IP L= 1500 TCP .A... 648=A L= 1460 S= 30772 W=65535
788		IP L= 160 TCP .AP... S= 648 L= 120 4256=A W=65535
789		IP L= 1264 TCP .AP... 648=A L= 1224 S= 32232 W=65535
790		IP L= 1500 TCP .A... 648=A L= 1460 S= 33456 W=65535
791		IP L= 1500 TCP .A... 648=A L= 1460 S= 34916 W=65535
792		IP L= 1264 TCP .AP... 648=A L= 1224 S= 36376 W=65535
793		IP L= 1500 TCP .A... 648=A L= 1460 S= 37600 W=65535
794		IP L= 1500 TCP .A... 648=A L= 1460 S= 39060 W=65535
795		IP L= 1264 TCP .AP... 648=A L= 1224 S= 40520 W=65535
796		IP L= 1500 TCP .A... 648=A L= 1460 S= 41744 W=65535
797		IP L= 1500 TCP .A... 648=A L= 1460 S= 43204 W=65535
798		IP L= 1264 TCP .AP... 648=A L= 1224 S= 44664 W=65535
799		IP L= 1500 TCP .A... 648=A L= 1460 S= 45888 W=65535
800		IP L= 1500 TCP .A... 648=A L= 1460 S= 47348 W=65535
801		IP L= 1264 TCP .AP... 648=A L= 1224 S= 48808 W=65535
802		IP L= 1500 TCP .A... 648=A L= 1460 S= 50032 W=65535
803		IP L= 1500 TCP .A... 648=A L= 1460 S= 51492 W=65535
804		IP L= 1264 TCP .AP... 648=A L= 1224 S= 52952 W=65535

In PacketVisualizer, clicking on a packet shows you ‘protocol-relatedness’, in this case I believe it shows you TCP ACK information (what packets have been ‘ACKed’ by the packet I’ve selected.)



Built-in graphing tool (I have a feature request in for graphing IP ident numbers). In this screen shot, I selected all five graphs for simultaneous display -- you can choose which one(s) you view. Mouse-over gives you details on a single packet. You can zoom in and out using mouse movements.



OK, but I'm trying to figure out why my iSCSI initiator (isis) keeps resetting its LUNs (hosted on carbon). Let's see if Expert has any suggestions.

**Flows analyzed:** 2    **Flows recycled:** 0  
**Events detected:** 386    **Packets dropped:** 0

Client Addr	Server Addr	Flows	Events	Packets	Bytes	Duration	Avg Respo...	TCP Status
carbon-b-svif1	isis-1-iscsi-1	1	129	41,554	48,495,302	0:04:12.759617	0.033675	
carbon-a-svif2	isis-1-iscsi-1	1	257	8,497	7,298,814	0:05:23.660997	0.152156	
3260 <-> 1027			257	8,497	7,298,814	0:05:23.660997	0.152156	Open
Busy Network or Server			40					
Low Server-to-Client Throughput			16				0.152156	
Low Client-to-Server Throughput			2				0.152156	
Slow Server Response Time			191				0.152156	
TCP Invalid Checksum			8				0.152156	

**Event Summary** | **Event Log** | **Node Details**

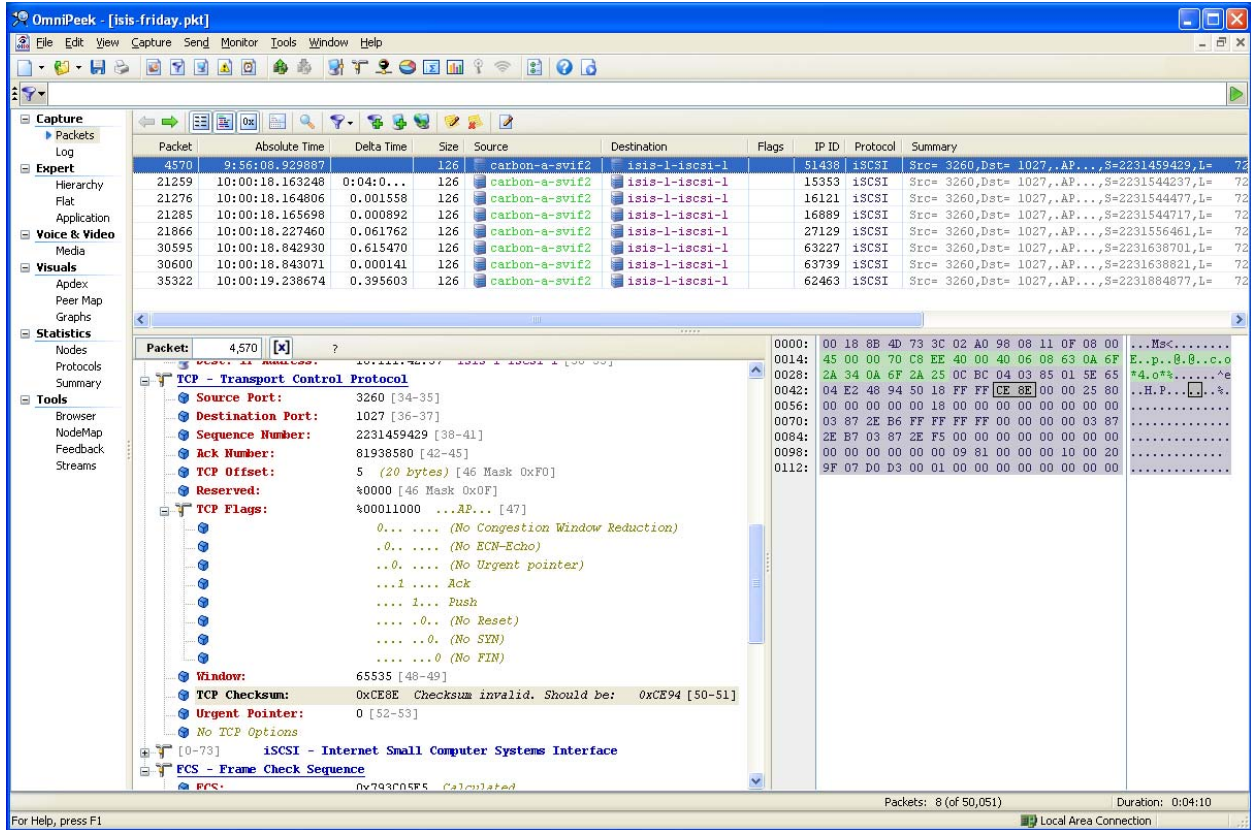
**Messages:** 386    0    386    0    0

Date/Time	Layer	Event	Source Addr	Dest Addr	Source Port	Dest Port	Packet
2/2/2008 9:54:57	Client/Server	Slow Server Response Time (0.272844 seconds from ...	isis-1-iscsi-1	carbon-a-svif2	1027	3260	6
2/2/2008 9:54:57	Client/Server	Slow Server Response Time (0.237452 seconds from ...	isis-1-iscsi-1	carbon-a-svif2	1027	3260	25
2/2/2008 9:54:57	Client/Server	Slow Server Response Time (0.199951 seconds from ...	isis-1-iscsi-1	carbon-a-svif2	1027	3260	36
2/2/2008 9:54:58	Client/Server	Slow Server Response Time (0.798576 seconds from ...	isis-1-iscsi-1	carbon-a-svif2	1027	3260	40
2/2/2008 9:54:59	Client/Server	Slow Server Response Time (0.299260 seconds from ...	isis-1-iscsi-1	carbon-a-svif2	1027	3260	85
2/2/2008 9:54:59	Client/Server	Slow Server Response Time (0.597742 seconds from ...	isis-1-iscsi-1	carbon-a-svif2	1027	3260	105
2/2/2008 9:55:00	Client/Server	Slow Server Response Time (0.905696 seconds from ...	isis-1-iscsi-1	carbon-a-svif2	1027	3260	116
2/2/2008 9:55:02	Client/Server	Busy Network or Server	isis-1-iscsi-1	carbon-a-svif2	1027	3260	123
2/2/2008 9:55:02	Client/Server	Slow Server Response Time (1.999431 seconds from ...	isis-1-iscsi-1	carbon-a-svif2	1027	3260	123
2/2/2008 9:55:03	Client/Server	Slow Server Response Time (0.999795 seconds from ...	isis-1-iscsi-1	carbon-a-svif2	1027	3260	125
2/2/2008 9:55:03	Client/Server	Slow Server Response Time (0.266669 seconds from ...	isis-1-iscsi-1	carbon-a-svif2	1027	3260	132
2/2/2008 9:55:04	Client/Server	Slow Server Response Time (0.732022 seconds from ...	isis-1-iscsi-1	carbon-a-svif2	1027	3260	136
2/2/2008 9:55:06	Client/Server	Slow Server Response Time (1.771596 seconds from ...	isis-1-iscsi-1	carbon-a-svif2	1027	3260	146
2/2/2008 9:55:06	Client/Server	Slow Server Response Time (0.217681 seconds from ...	isis-1-iscsi-1	carbon-a-svif2	1027	3260	150
2/2/2008 9:55:09	Client/Server	Busy Network or Server	isis-1-iscsi-1	carbon-a-svif2	1027	3260	155
2/2/2008 9:55:09	Client/Server	Slow Server Response Time (2.571007 seconds from ...	isis-1-iscsi-1	carbon-a-svif2	1027	3260	155
2/2/2008 9:55:09	Client/Server	Low Server-to-Client Throughput (10 kBytes/second)	isis-1-iscsi-1	carbon-a-svif2	1027	3260	155
2/2/2008 9:55:09	Client/Server	Slow Server Response Time (0.340497 seconds from ...	isis-1-iscsi-1	carbon-a-svif2	1027	3260	159
2/2/2008 9:55:12	Client/Server	Slow Server Response Time (2.974383 seconds from ...	isis-1-iscsi-1	carbon-a-svif2	1027	3260	166
2/2/2008 9:55:14	Client/Server	Slow Server Response Time (2.093188 seconds from ...	isis-1-iscsi-1	carbon-a-svif2	1027	3260	174
2/2/2008 9:55:15	Client/Server	Slow Server Response Time (0.905712 seconds from ...	isis-1-iscsi-1	carbon-a-svif2	1027	3260	181
2/2/2008 9:55:16	Client/Server	Slow Server Response Time (0.715969 seconds from ...	isis-1-iscsi-1	carbon-a-svif2	1027	3260	188
2/2/2008 9:55:18	Client/Server	Slow Server Response Time (2.269239 seconds from ...	isis-1-iscsi-1	carbon-a-svif2	1027	3260	198
2/2/2008 9:55:21	Client/Server	Slow Server Response Time (2.999404 seconds from ...	isis-1-iscsi-1	carbon-a-svif2	1027	3260	203
2/2/2008 9:55:21	Client/Server	Low Server-to-Client Throughput (1 kBytes/second)	isis-1-iscsi-1	carbon-a-svif2	1027	3260	203

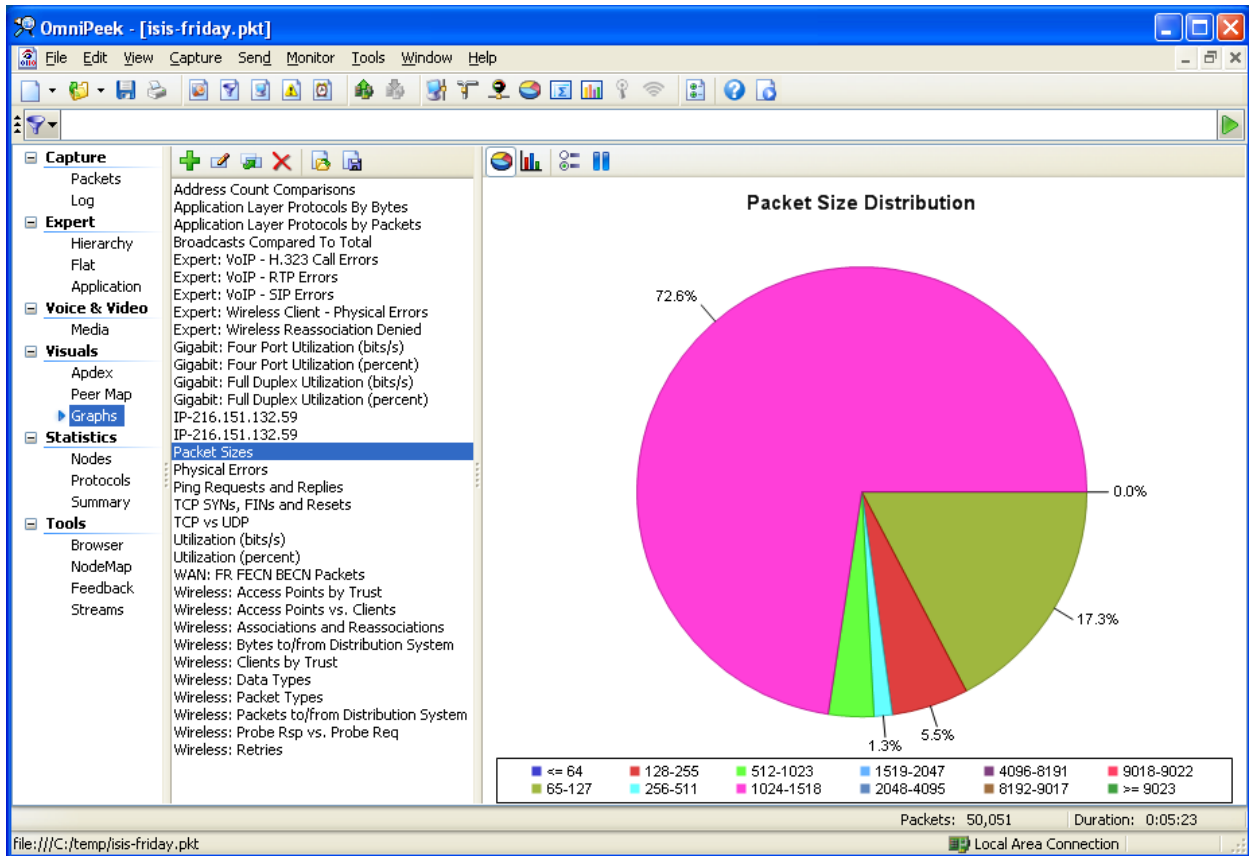
Packets: 50,051    Duration: 0:05:23

file:///C:/temp/isis-friday.pkt    Local Area Connection

TCP Checksum's invalid? Now, I was capturing with slicing as 128 bytes, so this smells like an analyzer bug to me (why did the analyzer fixate on these eight packets, given that virtually all these frames have a 'bad TCP Checksum?'). Still, let's go look at those packets. I right-click on the 'TCP Invalid Checksum' symptom and get a long menu, which includes 'Selected Related Packets'; I choose this and see the eight packets.



Built-in graphs based on entire trace



. You can build your own graphs, picking from an obscene number of variables.

New Graph: Pick a Statistic

- Statistic
- General**
  - Start Date
  - Start Time
  - Duration
- Network**
  - Total Bytes
  - Total Packets
  - Total Broadcast
  - Total Multicast
  - Average Utilization (percent)
  - Average Utilization (bits/s)
  - Current Utilization (percent)
  - Current Utilization (bits/s)
  - Max Utilization (percent)
  - Max Utilization (bits/s)
- Errors**
  - Total
  - CRC
  - Frame Alignment
  - Runt
  - Oversize
- Counts**
  - Physical Addresses
  - IP Addresses
  - IPv6 Addresses
  - AppleTalk Addresses
  - DECnet Addresses
  - IPX Addresses
  - Protocols
- Size Distribution**
  - <= 64
  - 65-127
  - 128-255
  - 256-511
  - 512-1023
  - 1024-1518
  - 1519-2047
  - 2048-4095
  - 4096-8191
  - 8192-9017
  - 9018-9022
  - >= 9023
- Expert**
  - Flows Analyzed (Total)
  - Flows Analyzed (Current)
  - Flows Analyzed (Recycled)
  - Node Pairs Analyzed (Total)
  - Node Pairs Analyzed (Current)
  - Node Pairs Analyzed (Recycled)
  - Packets Dropped
  - Busy Network or Server
  - Inefficient Client
  - Low Server-to-Client Throughput
  - Low Client-to-Server Throughput
  - Non-Responsive Client
  - Non-Responsive Server
  - One-Way Traffic
  - Slow Server Response Time
  - Apdex Score - Client Too Low
  - Apdex Task Ended - Tolerating User
  - Apdex Task Ended - Frustrated User
  - DHCP Low Lease Time
  - DHCP Multiple Server Response
  - DHCP Request Rejected
  - DHCP Request Storm

Units:

OK Cancel Help



New Graph: Pick a Statistic

- Statistic
- DHCP Request Storm
- DNS Slow Response Time
- DNS Error
- DNS Non-Existent Host or Domain
- FTP Slow Response Time
- HTTP Request Not Found
- HTTP Client Error
- HTTP Server Error
- HTTP Slow Response Time
- Kerberos Request Rejected
- LDAP Slow Response Time
- NFS Retransmission
- Oracle Logon Denied
- Oracle Slow Response Time
- Oracle TNS Connection Refused
- POP3 Login Failed
- POP3 Server Returned Error
- POP3 Slow Response Time
- SMB Logon or Access Denied
- SMB Command Rejected
- SMB Invalid Network Resource
- SMB Repeated or Looped Transaction
- SMB Excessive Transaction Loops
- SMTP Server Returned Error
- SMTP Slow Response Time
- SQL Server Failed Login
- SQL Server Client Error
- SQL Server Fatal Error
- SQL Server Resource Error
- SQL Server Slow Response Time
- Windows Master Browser Election
- NetBIOS (over IP) Session Refused
- H.225 RAS Reject
- H.225 Call Signaling (Q.931) - Call Dropped
- H.225 Call Signaling (Q.931) - Call Rejected
- H.245 Control Reject
- Low MOS-CQ
- Low R Factor Conversational
- MGCP - Transient Error
- MGCP - Permanent Error
- MGCP - Connection Deleted or Restart in Progress
- RTP Excessive Jitter Detected
- RTP Excessive Jitter Reported
- RTP Excessive Packet Loss Detected
- RTP Excessive Packet Loss Reported
- RTP Not Marked for QoS
- RTP Late Packet Arrival
- RTP Packet Out of Sequence
- SIP Post-Dial Delay Exceeded
- SIP Redirection
- SIP Client Authentication Required
- SIP Client Error
- SIP Server Error
- SIP Global Error
- RSVP Error
- TCP Connection Refused
- TCP Connection Lost
- TCP Inactive Connection Reset
- TCP Connection Reset
- TCP Too Many Retransmissions
- TCP Fast Retransmission (by ACK)
- TCP Fast Retransmission (by time)
- TCP Slow First Retransmission
- TCP Retransmission
- TCP Idle Too Long

Units:

OK Cancel Help

New Graph: Pick a Statistic

- Statistic
- TCP Idle Too Long
- TCP Invalid Checksum
- TCP Low Starting MSS
- TCP Repeated Connect Attempt
- TCP Slow Acknowledgement
- TCP Slow Segment Recovery
- TCP Triple Duplicate ACK
- TCP Low Window
- TCP Stuck Window
- TCP Zero Window
- TCP Segment Out of Sequence
- TCP Segment Outside Window
- TCP Segment Acked But Missing
- UDP Invalid Checksum
- IP Invalid Header Checksum
- IP Local Routing
- IP Network Duplicated Packet
- IP Low Time-To-Live
- IP Missing Fragment
- IP Packet w/CRC Frame Error
- IP Zero Address in Broadcast
- ICMP Network Unreachable
- ICMP Host Unreachable
- ICMP Protocol Unreachable
- ICMP Port Unreachable
- ICMP Fragmentation Needed
- ICMP Source Route Failed
- ICMP Host Unknown
- ICMP Net Unreachable TOS
- ICMP Host Unreachable TOS
- ICMP Comm Admin Prohibited
- ICMP Host Precedence Violation
- ICMP Precedence Cutoff
- ICMP Host Redirect
- ICMP Host TOS Redirect
- ICMP TTL Exceeded
- ICMP Fragmentation Time Exceeded
- ICMP Parameter Problem
- ICMP Obsolete Message
- 802.1X Dictionary Attack
- ARP Request Storm
- Broadcast Storm
- Multicast Storm
- Severe Broadcast Storm
- Severe Multicast Storm
- Spanning Tree Topology Change
- EAP Authentication Failure
- Too Many Physical Errors
- MAC Flooding
- Flow Tracker**
- Flows (all)
- Flows (current)
- Flows (recycled)
- Max
- Voice & Video**
- Calls (Total)
- Calls (Current)
- Calls (Recycled)
- Total Packet Loss %
- Voice Score Elements
- Voice Packet Loss %
- MOS-LQ
- MOS-CQ
- MOS-PQ
- R Factor Listening

Units: [dropdown]

OK Cancel Help

New Graph: Pick a Statistic



- Statistic
- R Factor Listening
- R Factor Conversational
- R Factor G.107
- AppleTalk Analysis**
- AARP Requests
- AARP Responses
- AARP Unanswered
- AARP Probes
- AppleTalk Broadcast/Multicast
- Email Analysis**
- SMTP Transfers Initiated
- SMTP Successful Transfers
- SMTP Failed Transfers
- FTP Analysis**
- FTP Transfers Initiated
- FTP Successful Transfers
- FTP Failed Transfers
- ICMP Analysis**
- Pings Unanswered
- ICMP Packets
- Ping Responses
- Ping Requests
- ICMP Router Advert
- ICMP Router Solicit
- ICMP Time Exceeded
- ICMP Param Problem
- ICMP Timestamp Req
- ICMP Timestamp Rsp
- ICMP Obsolete (?)
- ICMP Addr Mask Req
- ICMP Addr Mask Rsp
- ICMP Source Quench
- ICMP Net Redirect
- ICMP Host Redirect
- ICMP Net Srv Redirect
- ICMP Hst Srv Redirect
- ICMP Dest Unreach
- ICMP Net Unreach
- ICMP Host Unreach
- ICMP Proto Unreach
- ICMP Port Unreach
- ICMP Frag Needed
- ICMP Route Failed
- ICMP Net Unknown
- ICMP Host Unknown
- ICMP Net Prohibit
- ICMP Host Prohibit
- ICMP Net Srv Block
- ICMP Host Srv Block
- ICMP Comm Prohibited
- ICMP Host Violation
- ICMP Precedence Cutoff
- IP Analysis**
- TCP SYNs
- TCP FINs
- TCP RSTs
- ARP Requests
- ARP Responses
- ARPs Unanswered
- RARP Requests
- RARP Responses
- RARPs Unanswered
- NetWare Analysis**
- RIP Unanswered
- SAP Unanswered

Units:

New Graph: Pick a Statistic

- Statistic
- FTP Successful Transfers
- FTP Failed Transfers
- ICMP Analysis**
- Pings Unanswered
- ICMP Packets
- Ping Responses
- Ping Requests
- ICMP Router Advert
- ICMP Router Solicit
- ICMP Time Exceeded
- ICMP Param Problem
- ICMP Timestamp Req
- ICMP Timestamp Rsp
- ICMP Obsolete (?)
- ICMP Addr Mask Req
- ICMP Addr Mask Rsp
- ICMP Source Quench
- ICMP Net Redirect
- ICMP Host Redirect
- ICMP Net Srv Redirect
- ICMP Hst Srv Redirect
- ICMP Dest Unreach
- ICMP Net Unreach
- ICMP Host Unreach
- ICMP Proto Unreach
- ICMP Port Unreach
- ICMP Frag Needed
- ICMP Route Failed
- ICMP Net Unknown
- ICMP Host Unknown
- ICMP Net Prohibit
- ICMP Host Prohibit
- ICMP Net Srv Block
- ICMP Host Srv Block
- ICMP Comm Prohibited
- ICMP Host Violation
- ICMP Precedence Cutoff
- IP Analysis**
- TCP SYNs
- TCP FINs
- TCP RSTs
- ARP Requests
- ARP Responses
- ARPs Unanswered
- RARP Requests
- RARP Responses
- RARPs Unanswered
- NetWare Analysis**
- RIP Unanswered
- SAP Unanswered
- NCP Unanswered
- Newsgroup Analysis**
- Newsgroup Accesses
- VoIP Analysis**
- MGCP
- RTCP
- H.323
- G.723
- G.711
- SIP
- H.225
- H.245
- MEGACO
- Web**
- Web URLs

Units:

OK Cancel Help

But back to my trace. I've found a packet which the initiator emits at just about the same time as it logs the following message: "Initiator sent a task management command to reset the target." Here is how Surveyor decodes it:

Surveyor - Detail View [C:\Program Files\Finisar\Surveyor\CaptureFiles\Wdis\_module3\_auto\_02-01\_10\_00\_25.cap - 1 GBPS - ( 50051 frames total ) - Frame ID 757]

FID	BookMark	Abs Time	Delta [sec]	Size	Source	Destination	Summary
000753		02/01 09:56:06.698.860.280	0.905.812.280	618	isis-1-iscsi-1	carbon-b-svif1	iSCSI : SCSI command: Write(10), QTag:0x3872DE9, LUN:0x0e0F040000000000, LBA:0xC, Le...
000754		02/01 09:56:06.746.707.960	0.046.847.680	106	carbon-b-svif1	isis-1-iscsi-1	iSCSI : SCSI Response: Status:Good, QTag:0x3872DE9
000755		02/01 09:56:06.746.751.280	0.000.043.320	618	isis-1-iscsi-1	carbon-b-svif1	iSCSI : SCSI command: Write(10), QTag:0x3872DEA, LUN:0x0e0F040000000000, LBA:0xC, Le...
000756		02/01 09:56:06.746.778.880	0.001.027.600	106	carbon-b-svif1	isis-1-iscsi-1	iSCSI : SCSI Response: Status:Good, QTag:0x3872DEA
000757	Task Mgmt	02/01 09:56:08.104.872.760	1.359.893.880	106	isis-1-iscsi-1	carbon-a-svif2	iSCSI : Response - SCSI Task Management Response
000758		02/01 09:56:08.105.250.360	0.000.377.500	106	carbon-a-svif2	isis-1-iscsi-1	iSCSI : Response - SCSI Task Management Response
000759		02/01 09:56:08.105.408.160	0.000.157.800	106	isis-1-iscsi-1	carbon-a-svif2	iSCSI : Response - SCSI Task Management Response
000760		02/01 09:56:08.105.859.560	0.000.450.400	106	carbon-a-svif2	isis-1-iscsi-1	iSCSI : Response - SCSI Task Management Response
000761		02/01 09:56:08.105.899.480	0.000.040.520	394	isis-1-iscsi-1	carbon-a-svif2	iSCSI : SCSI command: Unknown, QTag:0x17A58782, LUN:0x0e0F040000000000, Len:4096
000762		02/01 09:56:08.106.110.280	0.000.210.800	610	carbon-a-svif2	isis-1-iscsi-1	iSCSI : SCSI Data (READ): Len:24, QTag:0x17A58782, Final:0, Offset:0
000763		02/01 09:56:08.106.166.960	0.000.055.680	154	isis-1-iscsi-1	carbon-a-svif2	iSCSI : Response - SCSI Task Management Response
000764		02/01 09:56:08.106.370.960	0.000.204.000	1518	isis-1-iscsi-1	carbon-a-svif2	iSCSI : SCSI command: Read(10), QTag:0x17A5878B, LUN:0x0e0F040000000000, LBA:0x42C8...
000765		02/01 09:56:08.106.375.000	0.000.004.040	1518	isis-1-iscsi-1	carbon-a-svif2	iSCSI : Response - Continuation of Data Segment (74 bytes)

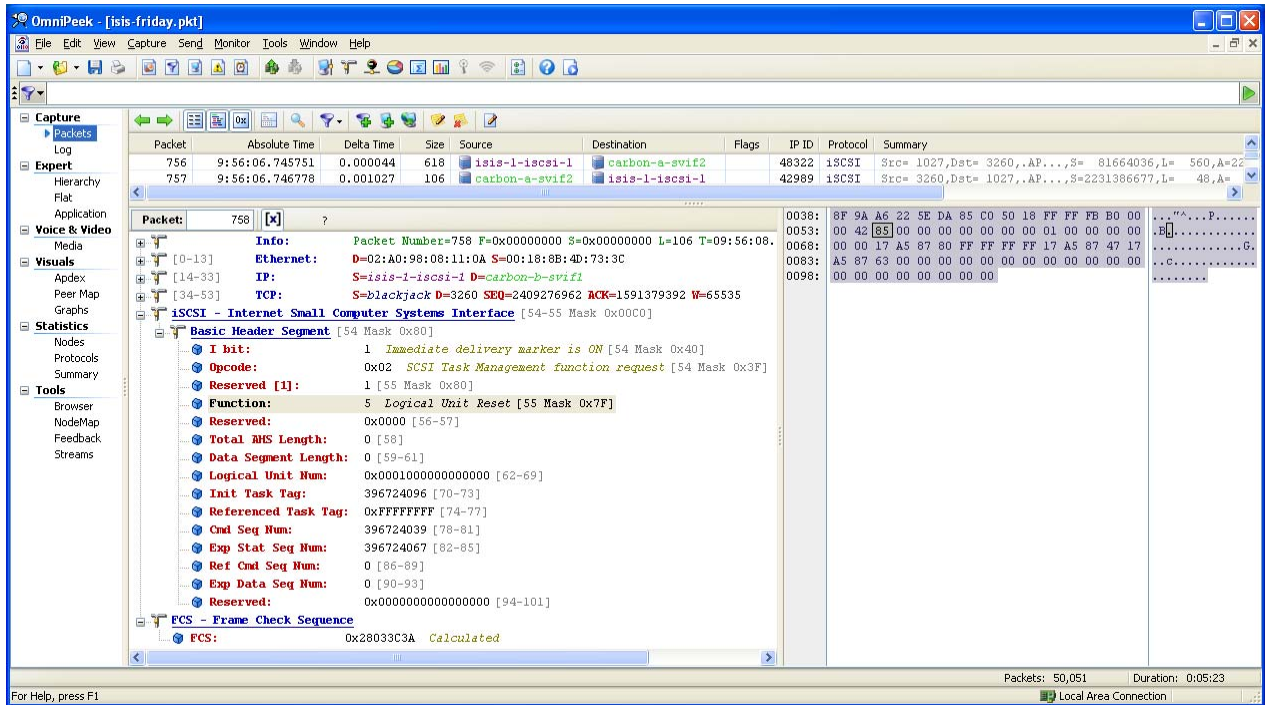
Detail View Frame ID 757, arrived at 02/01 09:56:08.104872, Frame Status: (Good Frame)

- Data Link Control (DLC)
- Internet Protocol (IP)
- Transmission Control Protocol (TCP)
- Internet Small Computer Systems Interface (ISCSI)
  - MS Code 0x42
    - 0... .. X bit: must = 1
    - 1.. .. I bit: must = 1
    - ..00 0010 SCSI Task Management Command
  - Flag/Reserved 0x85
    - 1... .. must = 1
    - ..00 0101 Reserved
    - Response 0 (Function Complete)
    - Qualifier 0 (Function Executed)
    - Reserved 000000000010000
    - Initiator Task Tag 0x00000000
    - Referenced Task Tag 0x17A58780
    - Status Sequence Number 4294967295
    - Expected Command SN 396724039
    - Maximum Command SN 396724067
    - Reserved 000000000000000000000000
  - Data/FCS
    - Data/Padding [4 bytes]
    - Frame Check Sequence 0x28033C3A (Correct)

Hex	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	ASCII
0000:	02	40	98	06	11	0A	00	18	88	40	73	3C	08	00	45	00	. . . . . M S C . . E .
0010:	00	58	C6	BF	00	00	80	06	0A	AB	0A	6F	2A	25	0A	6F	* X & L . . . . . S . 0 % 0
0020:	2A	33	04	01	0C	BC	8F	9A	A6	22	5E	DA	85	CD	50	18	* 3 . . . . . A U . A P .
0030:	FF	FF	FF	FF	00	00	42	83	00	00	00	00	00	00	00	01	. . B . . B . . . . .
0040:	00	00	00	00	00	00	17	A5	87	80	FF	FF	FF	FF	17	A5	. . . . . W . . . . .
0050:	87	47	17	A5	87	63	00	00	00	00	00	00	00	00	00	00	. G . W . C . . . . .
0060:	00	00	00	00	00	00	28	03	3C	3A							. . . . . [ . < .

Capture View Overview Servers Transactions Issues Clients / Ready Total Frames: 50051, Packets Analyzed: 50051 Capture/Display Filter: None

And here's how OmniPeek decodes it -- notice how OmniPeek presents the function (LUN Reset) along with the LUN number (1) ... now, perhaps Surveyor is correct (meaning, you just can't extract the function and the LUN number from this kind of packet); and perhaps OmniPeek is mistaken ... after all, I would like to think that Finisar can write a SCSI decode.



However, jumping to RFC3270, it seems to me that the format of this frame specifies the Function and the LUN number ... which suggests to me that what OmniPeek claims to be doing is at least theoretically possible

### 10.5. Task Management Function Request

Byte/	0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	
0   .   I	0x02	1   Function	Reserved	
4   TotalAHSLength	DataSegmentLength			
8   Logical Unit Number (LUN) or Reserved				
12				
16   Initiator Task Tag				
20   Referenced Task Tag or 0xffffffff				
24   CmdSN				
28   ExpStatSN				
32   RefCmdSN or Reserved				
36   ExpDataSN or Reserved				
40   Reserved				/

```

+ /
+-----+-----+-----+-----+
48| Header-Digest (Optional) |
+-----+-----+-----+-----+

```

### 10.5.1. Function

The Task Management functions provide an initiator with a way to explicitly control the execution of one or more Tasks (SCSI and iSCSI tasks). The Task Management function codes are listed below. For a more detailed description of SCSI task management, see [SAM2].

- 1 - ABORT TASK - aborts the task identified by the Referenced Task Tag field.
- 2 - ABORT TASK SET - aborts all Tasks issued via this session on the logical unit.
- 3 - CLEAR ACA - clears the Auto Contingent Allegiance condition.

Satran, et al.	Standards Track	[Page 129]
RFC 3720	iSCSI	April 2004

- 4 - CLEAR TASK SET - aborts all Tasks in the appropriate task set as defined by the TST field in the Control mode page (see [SPC3]).
- 5 - LOGICAL UNIT RESET
- 6 - TARGET WARM RESET
- 7 - TARGET COLD RESET
- 8 - TASK REASSIGN - reassigns connection allegiance for the task identified by the Referenced Task Tag field to this connection, thus resuming the iSCSI exchanges for the task.

Here's another example of why I appreciated OmniPeek's iSCSI decode. The Immediate Delivery flag in an iSCSI Basic Header Segment indicates a problem. When it is *\*not\** set, both analyzers portray this fact easily enough

Surveyor - Detail View - [C:\Program Files\Finisar\Surveyor\CaptureFiles\Wdis\_module3\_auto\_02-01 10\_0...

File Edit Configuration View Module Monitor Views Capture Views Tools Window Help

Display Filter:

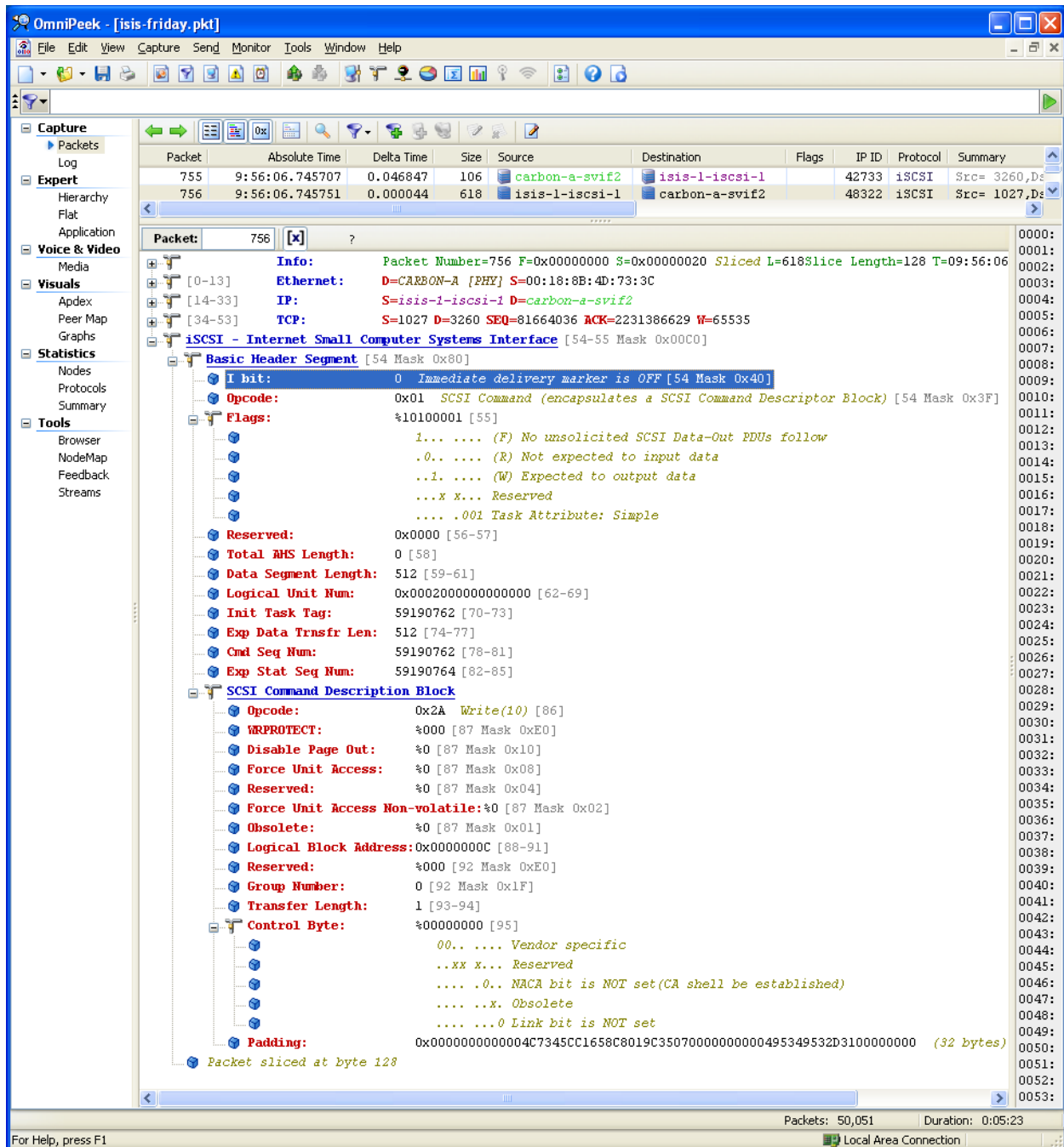
FID	BookMark	Abs Time	Delta [sec]	Size	Source	Destination
000754		02/01 09:56:06.745.707.960	0.046.847.680	106	carbon-b-svif1	isis-1-iscsi-1
000755		02/01 09:56:06.745.751.280	0.000.043.320	618	isis-1-iscsi-1	carbon-b-svif1
000756		02/01 09:56:06.746.778.880	0.001.027.600	106	carbon-b-svif1	isis-1-iscsi-1
000757	Task Mgmt	02/01 09:56:08.104.872.760	1.358.093.880	106	isis-1-iscsi-1	carbon-a-svif2
000758		02/01 09:56:08.105.250.360	0.000.377.600	106	carbon-a-svif2	isis-1-iscsi-1

**Detail View** Frame ID 755, arrived at 02/01 09:56:06.745751, Frame Status: (Good Frame)

- Data Link Control (DLC)
- Internet Protocol (IP)
- Transmission Control Protocol (TCP)
- Internet Small Computer Systems Interface (ISCSI)
  - BHS Opcode
    - 0x01
      - 0... .... X bit: Retry/Restart NOT set
      - .0.. .... I bit: Immediate delivery marker NOT set
      - ..00 0001 SCSI command (encapsulates a SCSI CDB)
    - Flags and Attributes
      - 0xA1
        - 1... .... F flag = 1
        - .0.. .... R flag: input data NOT expected
        - ..1. .... W flag: output data is expected
        - ...0 0... Reserved
        - .... .001 Task Attributes = 1 : Simple
      - Reserved 0
      - SCSI Command Reference No. 0
      - Total AHS Length 0
      - Data Segment Length 000200( 512 bytes )
      - Logical Unit Number 0002000000000000
      - Initiator Task Tag 0x03872DEA
      - Expected Data Transfer Length 512
      - Command Sequence Number 59190762
      - Expected Status SN 59190764
      - SCSI-CDB : Operation Code 0x2A (Write(10))
      - SCSI-CDB : LUN / Reserved 0x00
        - 000. .... LUN = 0
        - ...0 0000 Reserved
      - SCSI-CDB : Logical Block Address 0x0000000C
      - SCSI-CDB : Reserved 0x00
      - SCSI-CDB : Length 1
      - SCSI-CDB : Control 0x00
      - SCSI-CDB : Padding 000000000000
      - SCSI Command Data [26 bytes]

Capture View Overview Servers Transactions Issues Clients

Ready Total Frames: 50051, Packets Analyzed: 50051 Capture\Display Filter: Nc



But when the Immediate Delivery flag is set, Surveyor just tells you that the 'I' bit is set, whereas OmniPeek says that 'Immediate delivery marker is ON' ... I prefer the way OmniPeek represents this:

Surveyor - Detail View - [C:\Program Files\Finisar\Surveyor\CaptureFiles\Wdis\_module3\_auto\_02-01 10\_0...

File Edit Configuration View Module Monitor Views Capture Views Tools Window Help

Display Filter:

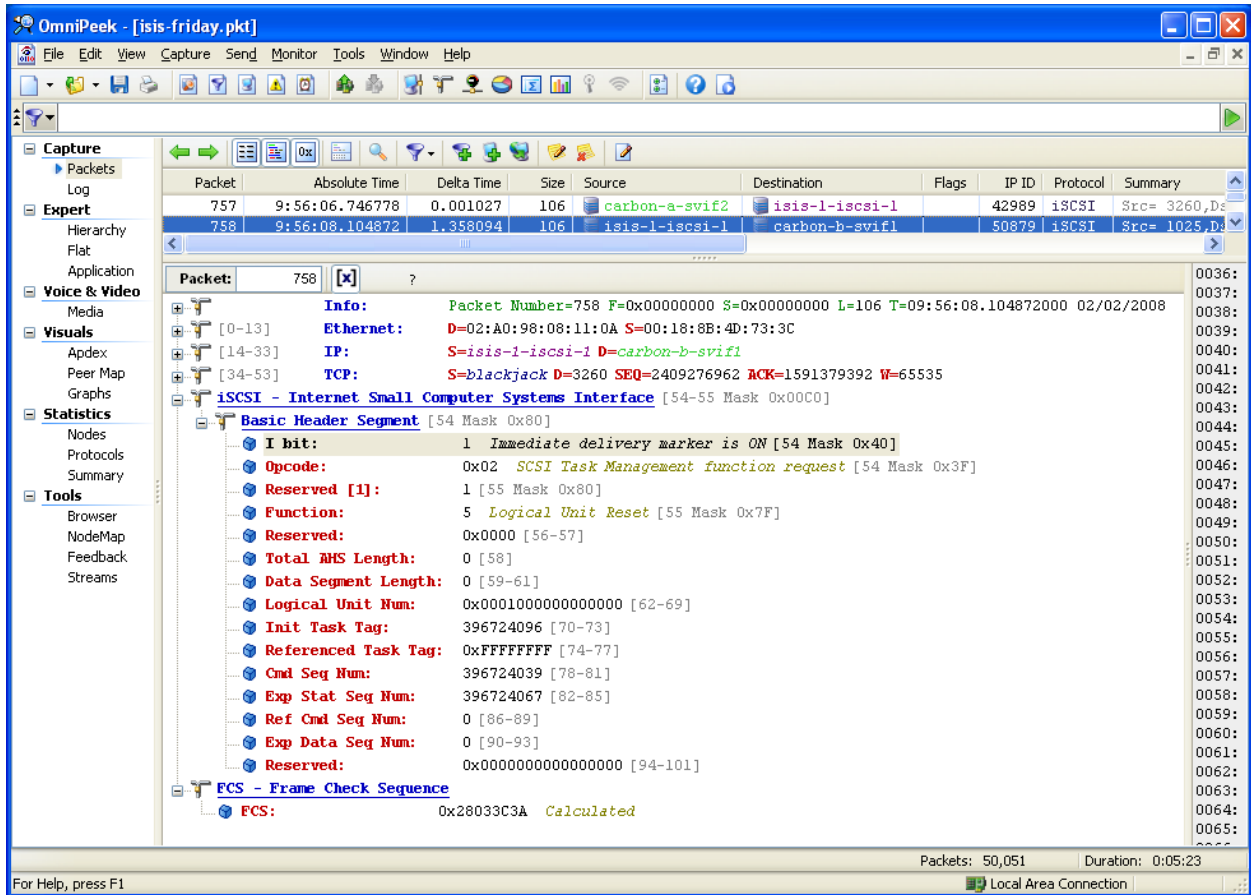
FID	BookMark	Abs Time	Delta [sec]	Size	Source	Destination
000754		02/01 09:56:06.745.707.960	0.046.847.680	106	carbon-b-svif1	isis-1-iscsi-1
000755		02/01 09:56:06.745.751.280	0.000.043.320	618	isis-1-iscsi-1	carbon-b-svif1
000756		02/01 09:56:06.746.778.880	0.001.027.600	106	carbon-b-svif1	isis-1-iscsi-1
000757	Task Mgmt	02/01 09:56:08.104.872.760	1.358.093.880	106	isis-1-iscsi-1	carbon-a-svif2
000758		02/01 09:56:08.105.250.360	0.000.377.600	106	carbon-a-svif2	isis-1-iscsi-1

Detail View Frame ID 757, arrived at 02/01 09:56:08.104872, Frame Status: (Good Frame)

- Data Link Control (DLC)
- Internet Protocol (IP)
- Transmission Control Protocol (TCP)
- Internet Small Computer Systems Interface (ISCSI)
  - BHS Opcode
    - 0x42
      - 0... .... X bit: must = 1
      - .1... .... I bit: must = 1
      - ..00 0010 SCSI Task Management Command
    - Flag/Reserved
      - 0x85
        - 1... .... must = 1
        - .000 0101 Reserved
      - Response 0 (Function Complete)
      - Qualifier 0 (Function Executed)
      - Reserved 00000000000010000
      - Initiator Task Tag 0x00000000
      - Referenced Task Tag 0x17A58780
      - Status Sequence Number 4294967295
      - Expected Command SN 396724039
      - Maximum Command SN 396724067
      - Reserved 000000000000000000000000
    - Data/FCS
      - Data/Padding [4 bytes]
      - Frame Check Sequence 0x28033C3A (Correct)

Capture View Overview Servers Transactions Issues Clients

Ready Total Frames: 50051, Packets Analyzed: 50051 Capture\Display Filter: Nc



There's an API so that you can extend the product; and a Web site hosting the plug-ins which people share.

WildPackets Developer Network - Browse Downloads - Mozilla Firefox 3 Beta 2

File Edit View History Bookmarks Tools Help

https://wpdn.wildpackets.com/browse.php

Getting Started Latest Headlines Google News Yahoo Mail Soma MIDAF TOC CenterNet Vox Util EMS FMS Serena Orwell

WildPackets - MyPeek WildPackets - MyPeek WildPackets View WildPackets Developer Network ...

WPDN WildPackets Developer Network [log in](#)

Home > Downloads [Documentation](#) [Community](#) [Downloads](#) [Support](#)

## Browse Downloads

### Browse By Category

**Downloads**

- Plug-ins
- Tools
- Remote Adapters

**Become a Member**

**Basic Membership**

Basic membership is free to all who want to join and includes the following benefits:

- Access to Documentation Library
- Post to Mailing List, Review Discussion Threads
- Limited Access to Plug-ins
- Share Content with Other Developers

[Sign Up](#)

**Maintenance Membership**

Maintenance membership requires an active maintenance contract for a WildPackets product and includes the following benefits:

- Full Access to Plug-ins
- Access to Source Code

If you are not a WildPackets Maintenance Customer but would like to purchase a Maintenance contract for your WildPackets product please [click here](#) for sales information.

[Sign Up](#)

**Plug-ins**

Some are real plug-ins. Others may be simple samples, much like the output from a Wizard, which a developer can copy and build upon for his own plug-in application.

**Tools**

Debuggers, test harnesses, and other utilities to aid development against the WildPackets platform.

**Remote Adapters**

Remote adapters make it possible to view packets in Peek from a remote device in real-time.

**Latest Submissions:**

- [QueryMe Plug-in](#)
- [FilterMe Plug-in](#)
- [DHCP Stats Plug-in](#)
- [Instant Messenger Plug-in](#)
- [VLAN Stats Plug-in](#)
- [SQLFilter Plug-in for MySQL](#)
- [Geiger Plug-in](#)
- [wan2lan Filter Plug-in](#)
- [Toolbar Plug-in](#)
- [Title Changer Plug-in](#)

[View All Plug-ins >>](#)

**Latest Submissions:**

- [Delphi Plug-in SDK](#)
- [Gnu Plug-in Wizard](#)
- [OmniPeek Plug-in Wizard](#)
- [OmniMapper](#)
- [pkt2mysql console program](#)
- [PeekRdr Sample Application](#)
- [Decoder Toolkit](#)
- [Forensics Filters](#)
- [Decoders](#)
- [pkt2sql Console Program](#)

[View All Tools >>](#)

**Latest Submissions:**

- [Remote TCPDump Adapter](#)
- [OmniSpectrum Interferer Adapter](#)

[View All Remote Adapters >>](#)

**Most Popular**

The Top 10 most popular submissions by vote.

- [Cisco AP Capture Adapter](#)
- [OmniPeek Plug-in Wizard](#)
- [OmniEngine Plug-in Wizard](#)
- [Decoder Toolkit](#)
- [WebStats](#)
- [Instant Messenger Plug-in](#)
- [Remote TCPDump Adapter](#)
- [Restart Plug-in](#)
- [QueryMe Plug-in](#)
- [FilterMe Plug-in](#)

[View All Downloads By Rating >>](#)

**Most Downloaded**

The Top 10 most downloaded submissions.

- [Google Map Plug-in](#)
- [Remote TCPDump Adapter](#)
- [SQLFilter Plug-in](#)
- [Instant Messenger Plug-in](#)
- [OmniPeek Plug-in Wizard](#)
- [Browser Plug-in](#)
- [Cisco AP Capture Adapter](#)
- [WebStats](#)
- [FilterMe Plug-in](#)
- [PeekPlayer Plug-in](#)

[View All Downloads By Most Downloaded >>](#)

Copyright © 2007 WildPackets, Inc - [Privacy Statement](#)  
All registered and unregistered trademarks are the sole property of their respective owners

[Documentation](#) | [Community](#) | [Downloads](#) | [Support](#)

Done wpdn.wildpackets.com

For this analysis, I ended up with Surveyor on one screen (I like the way their Summary line includes top-layer decode, iSCSI in this case) and OmniPeek in the other (for their fancy tools and their more detailed iSCSI decodes).