pcapFS Mounting Network Data for On-the-Fly Analysis

Fraunhofer Institute for Communication, Information Processing and Ergonomics

> OSDFCon 2018 October 17th

Jan-Niclas Hilgert* Martin Lambertz jan-niclas.hilgert@fkie.fraunhofer.de martin.lambertz@fkie.fraunhofer.de



Wireshark is great, but

	ply a display filter <		In a stanta		Destand		Expression.
	Source		Destination	Destination Port	Protocol	Host	Info
	172.16.133.57 172.16.133.57	53807	68.64.21.62 68.64.21.62	1853 1853	UDP UDP		53807-1853 Len=1126 53807-1853 Len=1126
	172.16.133.57	53807 53807		1853	UDP		53807→1853 Len=1126 53807→1853 Len=52
	96.43.146.176	443	68.64.21.62 172.16.133.82	61228	TCP		443→61228 [ACK] Seg=1 Ack=1 Win=9659 Len=0
	172.16.133.56	445	68.64.21.42	1853	UDP		443→61226 [ACK] Seq=1 ACK=1 W11=9659 Left=0 49514→1853 Len=125
	68.64.21.62	1853	172.16.133.57	53807	UDP		49514→1655 Len=125 1853→53807 Len=25
	96.43.146.176	443	172.16.133.82	61228	TCP		443→61228 [ACK] Seg=1 Ack=1107 Win=10765 Len=0
	96.43.146.176	443	172.16.133.82	60073	TCP		443→60073 [ACK] Seq=1 Ack=1 Win=65535 Len=0
	172.16.133.49	58246	68.64.21.41	1853	UDP		58246→1853 Len=125
	172.16.133.103	63406	216.115.222.200		TCP		63406→443 [SYN] Seg=0 Win=8192 Len=0 MSS=1460 WS=256 SACK
	172.16.133.43	57700	172.16.139.250	5440	HTTP	172.16.139.250:5440	GET /CSIS/CSISISAPI.dll/?request?aaeb6985-26fc-48a7-a5f8-
	68.64.21.41	1853	172.16.133.60	63861	UDP	1/2.10.139.230.3440	1853→63861 Len=125
	172.16.133.43	57700	172.16.139.250	5440	TCP		[TCP Retransmission] 57700→5440 [PSH, ACK] Seg=1 Ack=1 Wi
	67.217.94.135	8200	172.16.133.60	63862	ADP		[ICF Retraismission] 5/700-5440 [FSN, ACK] Seq-1 ACK-1 WI
	67.217.94.155	8200	172.16.133.53	55702	ADP		
	67.217.94.204	8200	172.16.133.114	49321	ADP		
	172.16.133.53	49292	172.16.139.250	5500	TCP		49292→5500 [ACK] Seg=1 Ack=1 Win=256 Len=0
	172.16.133.53	49292	172.16.139.250		ТСР		[TCP Dup ACK 17#1] 49292-5500 [ACK] Seq=1 Ack=1 Win=256 Len
	157.56.242.198	49292	172.16.133.57	60589	TCP		443-60589 [ACK] Seg=1 Ack=1 Win=2203 Len=0
	172.16.133.114	55270	67.217.65.49	443	TCP		55270→443 [ACK] Seq=1 Ack=1 Win=257 Len=0
	172.16.133.43	57700	172.16.139.250	5440	тср		57700→5440 [ACK] Seq=212 Ack=183 Win=16379 Len=0
	172.16.133.43	57700	172.16.139.250	5440	ТСР		57700→5440 [ACK] Seq=212 Ack=184 Win=16379 Len=0
	172.16.133.43	57700	172.16.139.250	5440	тср		57700→5440 [ACK] Seq=212 Ack=183 Win=16379 Len=0
	172.16.133.43	57700	172.16.139.250	5440	TCP		57700→5440 [ACK] Seq=212 Ack=185 Win=16379 Len=0
	172.16.133.43	57700	172.16.139.250		TCP		57700→5440 [FIN, ACK] Seq=212 Ack=164 win=16379 Len=0
	ame 1: 1168 byte:						57700-5440 [11N, ACK] SEQ-212 ACK-104 WIN-10579 LEN-0
						2:d0 (00:90:7f:3e:02:d0	2)
	•				-	21.62 (68.64.21.62)	
	er Datagram Proto				, 031. 00.04.	21.02 (00.04.21.02)	
	ta (1126 bytes)	July Sil	10111 JJ007, DSI	10101 1055			
P Da	(1120 by(C3)						
0000			9f d4 90 db 08		E.		
	04 82 fd 44 00				.@^9D@		
	15 3e d2 2f 07 1a 0f df bb 0d		43 4f c5 b8 2b 88 50 11 77 f1		=.n CO+		
	ec 3a 88 65 92		45 11 ac 84 4a		.&x EJo		
	6a c6 90 ce 5f				X.c \$S@.0U		
	ec 25 37 44 42						



Wireshark is great, but

1. Usability

Apply a display filter						Expression
Fime Source		t Destination	Destination Port	Protocol	Host	Info
201 172.16.133.57	53807	68.64.21.62	1853	UDP		53807→1853 Len=1126
01 172.16.133.57	53807	68.64.21.62	1853	UDP		53807→1853 Len=1126
01 172.16.133.57	53807	68.64.21.62	1853	UDP		53807→1853 Len=52 443-61228 [ACK] Seq=1 Ack=1 Win=9659 Len=0 49514→1853 Len=125 1853→53807 Len=25 443-61228 [ACK] Seq=1 Ack=1107 Win=10765 Len=0 443-60073 [ACK] Seq=1 Ack=1 Win=65535 Len=0
01 96.43.146.176	443	172.16.133.82	61228	TCP		443→61228 [ACK] Seq=1 Ack=1 Win=9659 Len=0
01 172.16.133.56	49514	68.64.21.42	1853	UDP		49514→1853 Len=125
01 68.64.21.62	1853	172.16.133.57	53807	UDP		1853→53807 Len=25
01 96.43.146.176	443	172.16.133.82	61228	TCP		443→61228 [ACK] Seq=1 Ack=1107 Win=10765 Len=0
01 96.43.146.176	443	172.16.133.82	60073	TCP		443→60073 [ACK] Seq=1 Ack=1 Win=65535 Len=0
01 172.16.133.49	58246	68.64.21.41	1853	UDP		58246→1853 Len=125
01 172.16.133.103	63406	216.115.222.200	443	ТСР		63406→443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_
01 172.16.133.43	57700	172.16.139.250	5440	HTTP	172.16.139.250:5440	GET /CSIS/CSISISAPI.dll/?request?aaeb6985-26fc-48a7-a5f8-2
01 68.64.21.41	1853	172.16.133.60	63861	UDP		1853→63861 Len=125
01 172.16.133.43	57700	172.16.139.250	5440	ТСР		[TCP Retransmission] 57700→5440 [PSH, ACK] Seq=1 Ack=1 Win
01 67.217.94.135	8200	172,16,133,60	63862	ADP		
01 67.217.94.156	8200					
01 67.217.94.204	8200	_			70	
01 67.217.94.204 01 172.16.133.53	8200 49292		Dac	kat	c. 70	
01 67.217.94.204 01 172.16.133.53 01 172.16.133.53	8200 49292 49292	F	Pac	ket	s [.] 79	1615 ^{56 Len=0}
01 67.217.94.204 01 172.16.133.53 01 172.16.133.53 01 157.56.242.198	8200 49292 49292 443	F	Pac	ket	s: 79	1615 ^{56 Len=0} 3 Len=0 7 Len=0 7 Len=0
01 67.217.94.204 01 172.16.133.53 01 172.16.133.53 01 157.56.242.198 01 172.16.133.114	8200 49292 49292 443 55270	F	Pac	ket	s: 79	7 Len=0
01 67.217.94.204 01 172.16.133.53 01 172.16.133.53 01 157.56.242.198 01 172.16.133.114 01 172.16.133.43	8200 49292 49292 443 55270 57700	F	Pac	ket	s: 79	7 Len=0 in=16379 Len=0
01 67.217.94.156 01 67.217.94.204 01 172.16.133.53 01 172.16.133.53 01 157.56.242.198 01 172.16.133.114 01 172.16.133.43 01 172.16.133.43	8200 49292 49292 443 55270 57700 57700	_			s: 79	7 Len=0 in=16379 Len=0 in=16379 Len=0
01 67.217.94.204 01 172.16.133.53 01 172.16.133.53 01 157.56.242.198 01 172.16.133.114 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43	8200 49292 49292 443 55270 57700 57700 57700	172.16.139.250	5440	тср	s: 79	7 Len=0 in=16379 Len=0 in=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=183 Win=16379 Len=0
11 67.217.94.204 11 172.16.133.53 01 172.16.133.53 01 157.56.242.198 01 172.16.133.114 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43	8200 49292 49292 443 55270 57700 57700 57700 57700 57700	172.16.139.250 172.16.139.250	5440 5440	TCP TCP	s: 79	7 Len=0 in=16379 Len=0 in=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=183 Win=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=184 Win=16379 Len=0
11 67.217.94.204 11 172.16.133.53 11 172.16.133.53 11 157.56.242.198 11 172.16.133.114 11 172.16.133.43 11 172.16.133.43 11 172.16.133.43 11 172.16.133.43 11 172.16.133.43 11 172.16.133.43 11 172.16.133.43	8200 49292 443 55270 57700 57700 57700 57700 57700 57700	172.16.139.250 172.16.139.250 172.16.139.250	5440 5440 5440	TCP TCP TCP	s: 79	7 Len=0 in=16379 Len=0 in=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=183 Win=16379 Len=0
01 67.217.94.204 01 172.16.133.53 01 172.16.133.53 01 157.56.242.198 01 172.16.133.114 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43	8200 49292 443 55270 57700 57700 57700 57700 57700 57700 57700 57700	172.16.139.250 172.16.139.250 172.16.139.250 172.16.139.250 (9344 bits), 116	5440 5440 5440 8 bytes captur	TCP TCP TCP red (9344 bits)		7 Len=0 in=16379 Len=0 in=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=183 Win=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=184 Win=16379 Len=0 57700→5440 [FIN, ACK] Seq=212 Ack=184 Win=16379 Len=0
01 67.217.94.204 01 172.16.133.53 01 157.56.242.198 01 157.56.242.198 01 172.16.133.114 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 Prame 1: 1168 byt Ethernet II, Src:	8200 49292 443 55270 57700 57700 57700 57700 57700 57700 es on wire Apple_d4:	172.16.139.250 172.16.139.250 172.16.139.250 (9344 bits), 116 90:db (14:10:9f:d	5440 5440 5440 8 bytes captur 14:90:db), Dst:	TCP TCP TCP red (9344 bits) Watchgua_3e:02	2:d0 (00:90:7f:3e:02:d0	7 Len=0 in=16379 Len=0 in=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=183 Win=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=184 Win=16379 Len=0 57700→5440 [FIN, ACK] Seq=212 Ack=184 Win=16379 Len=0
01 67.217.94.204 01 172.16.133.53 01 175.56.242.198 01 157.56.242.198 01 172.16.133.414 01 172.16.133.43 02 172.16.133.43 03	8200 49292 443 55270 57700 57700 57700 57700 57700 57700 es on wire Apple_d4: Version 4	172.16.139.250 172.16.139.250 172.16.139.250 (9344 bits), 116 90:db (14:10:9f:d , Src: Sean.local	5440 5440 5440 38 bytes captur 14:90:db), Dst: (172.16.133.5	TCP TCP TCP red (9344 bits) Watchgua_3e:02		7 Len=0 in=16379 Len=0 in=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=183 Win=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=184 Win=16379 Len=0 57700→5440 [FIN, ACK] Seq=212 Ack=184 Win=16379 Len=0
01 67.217.94.204 01 172.16.133.53 01 172.16.133.53 01 157.56.242.198 01 172.16.133.414 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 02 11.6.133.43 03 11.6.133.43 04 11.6.133.43 05 11.6.133.43 05 11.6.133.43 05 1	8200 49292 443 55270 57700 57700 57700 57700 57700 57700 es on wire Apple_d4: Version 4	172.16.139.250 172.16.139.250 172.16.139.250 (9344 bits), 116 90:db (14:10:9f:d , Src: Sean.local	5440 5440 5440 38 bytes captur 14:90:db), Dst: (172.16.133.5	TCP TCP TCP red (9344 bits) Watchgua_3e:02	2:d0 (00:90:7f:3e:02:d0	7 Len=0 in=16379 Len=0 in=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=183 Win=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=184 Win=16379 Len=0 57700→5440 [FIN, ACK] Seq=212 Ack=184 Win=16379 Len=0
01 67.217.94.204 01 172.16.133.53 01 172.16.133.53 01 157.56.242.198 01 172.16.133.414 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 02 11.6.133.43 03 11.6.133.43 04 11.6.133.43 05 11.6.133.43 05 11.6.133.43 05 1	8200 49292 443 55270 57700 57700 57700 57700 57700 57700 es on wire Apple_d4: Version 4	172.16.139.250 172.16.139.250 172.16.139.250 (9344 bits), 116 90:db (14:10:9f:d , Src: Sean.local	5440 5440 5440 38 bytes captur 14:90:db), Dst: (172.16.133.5	TCP TCP TCP red (9344 bits) Watchgua_3e:02	2:d0 (00:90:7f:3e:02:d0	7 Len=0 in=16379 Len=0 in=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=183 Win=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=184 Win=16379 Len=0 57700→5440 [FIN, ACK] Seq=212 Ack=184 Win=16379 Len=0
01 67.217.94.204 01 172.16.133.53 01 172.16.133.53 01 157.56.242.198 01 172.16.133.114 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43	8200 49292 443 55270 57700 57700 57700 57700 57700 57700 es on wire Apple_d4: Version 4	172.16.139.250 172.16.139.250 172.16.139.250 (9344 bits), 116 90:db (14:10:9f:d , Src: Sean.local	5440 5440 5440 38 bytes captur 14:90:db), Dst: (172.16.133.5	TCP TCP TCP red (9344 bits) Watchgua_3e:02	2:d0 (00:90:7f:3e:02:d0	7 Len=0 in=16379 Len=0 in=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=183 Win=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=184 Win=16379 Len=0 57700→5440 [FIN, ACK] Seq=212 Ack=184 Win=16379 Len=0
21 67.217.94.204 21 172.16.133.53 31 172.16.133.53 31 157.56.242.198 31 172.16.133.414 31 172.16.133.43 31 172.16.133.43 31 172.16.133.43 31 172.16.133.43 31 172.16.133.43 31 172.16.133.43 31 172.16.133.43 31 172.16.133.43 31 172.16.133.43 31 172.16.133.43 31 172.16.133.43 31 172.16.133.43 31 172.16.133.43 31 172.16.133.43 31 172.16.133.43 31 172.16.133.43 32 11 33 11 34 11 35 11 36 11 37 11 38 11 39 11 39 11 39	8200 49292 443 55270 57700 57700 57700 57700 57700 57700 es on wire Apple_d4: Version 4	172.16.139.250 172.16.139.250 172.16.139.250 (9344 bits), 116 90:db (14:10:9f:d , Src: Sean.local	5440 5440 5440 38 bytes captur 14:90:db), Dst: (172.16.133.5	TCP TCP TCP red (9344 bits) Watchgua_3e:02	2:d0 (00:90:7f:3e:02:d0	7 Len=0 in=16379 Len=0 in=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=183 Win=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=184 Win=16379 Len=0 57700→5440 [FIN, ACK] Seq=212 Ack=184 Win=16379 Len=0
01 67.217.94.204 01 172.16.133.53 01 172.16.133.53 01 157.56.242.198 01 172.16.133.114 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 Frame 1: 1168 byt Ethernet II, Src: Internet Protocol User Datagram Pro Data (1126 bytes)	8200 49292 443 55270 57700 57700 57700 57700 57700 57700 57700 es on wire Apple_d4: Version 4 tocol, Src	172.16.139.250 172.16.139.250 172.16.139.250 (9344 bits), 116 90:db (14:10:9f:d , Src: Sean.local Port: 53807, Dst	5440 5440 5440 8 bytes captur 14:90:db), Dst: (172.16.133.5 Port: 1853	TCP TCP TCP ed (9344 bits) Watchgua_3e:07 7), Dst: 68.64	2:d0 (00:90:7f:3e:02:d0	7 Len=0 in=16379 Len=0 in=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=183 Win=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=184 Win=16379 Len=0 57700→5440 [FIN, ACK] Seq=212 Ack=184 Win=16379 Len=0
01 67.217.94.204 01 172.16.133.53 01 172.16.133.53 01 157.56.242.198 01 157.56.242.198 01 172.16.133.414 01 172.16.133.43 02 11.68 byt Ethernet II, Src: Internet Protocol User Datagram Pro Data (1126 bytes) <td>8200 49292 443 55270 57700 57700 57700 57700 57700 57700 es on wire Apple_d4: Version 4 tocol, Src</td> <td>172.16.139.250 172.16.139.250 172.16.139.250 (9344 bits), 116 90:db (14:10:9f:d , Src: Sean.local Port: 53807, Dst</td> <td>5440 5440 5440 38 bytes captur 14:90:db), Dst: (172.16.133.5 Port: 1853 00 45 00></td> <td>TCP TCP TCP red (9344 bits) Watchgua_3e:02 7), Dst: 68.64</td> <td>2:d0 (00:90:7f:3e:02:d0</td> <td>7 Len=0 in=16379 Len=0 in=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=183 Win=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=184 Win=16379 Len=0 57700→5440 [FIN, ACK] Seq=212 Ack=184 Win=16379 Len=0</td>	8200 49292 443 55270 57700 57700 57700 57700 57700 57700 es on wire Apple_d4: Version 4 tocol, Src	172.16.139.250 172.16.139.250 172.16.139.250 (9344 bits), 116 90:db (14:10:9f:d , Src: Sean.local Port: 53807, Dst	5440 5440 5440 38 bytes captur 14:90:db), Dst: (172.16.133.5 Port: 1853 00 45 00>	TCP TCP TCP red (9344 bits) Watchgua_3e:02 7), Dst: 68.64	2:d0 (00:90:7f:3e:02:d0	7 Len=0 in=16379 Len=0 in=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=183 Win=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=184 Win=16379 Len=0 57700→5440 [FIN, ACK] Seq=212 Ack=184 Win=16379 Len=0
01 67.217.94.204 01 172.16.133.53 01 172.16.133.53 01 172.16.133.53 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 Frame 1: 1168 byt Ethernet II, Src: Internet Protocol User Datagram Pro Data (1126 bytes) 0000 00 90 7f 3e 02 010 04 82 fd 44 00	8200 49292 443 55270 57700 57700 57700 57700 57700 57700 57700 57700 57700 200 57700 200 200 200 200 200 200 200 200 200	172.16.139.250 172.16.139.250 172.16.139.250 (9344 bits), 116 90:db (14:10:9f:d , Src: Sean.local Port: 53807, Dst 9f d4 90 db 08 (ee 5e ac 10 85 3	5440 5440 5440 8 bytes captur 4:90:db), Dst: . (172.16.133.5 : Port: 1853 00 45 00> 39 44 40D	TCP TCP TCP red (9344 bits) Watchgua_3e:02 7), Dst: 68.64	2:d0 (00:90:7f:3e:02:d0	7 Len=0 in=16379 Len=0 in=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=183 Win=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=184 Win=16379 Len=0 57700→5440 [FIN, ACK] Seq=212 Ack=184 Win=16379 Len=0
01 67.217.94.204 01 172.16.133.53 01 172.16.133.53 01 172.16.133.53 01 172.16.133.53 01 172.16.133.14 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 Frame 1: 1168 Ethernet II, Src: Internet Protocol User Datagram Pro Data (1126 bytes) 000 00 90 7f 3e 02 010 04 82 fd 44 00 020 15 3e d2 2f 07	8200 49292 443 55270 57700 57700 57700 57700 57700 57700 57700 57700 es on wire Apple_d4: Version 4 tocol, Src	172.16.139.250 172.16.139.250 172.16.139.250 (9344 bits), 116 90:db (14:10:9f:d , Src: Sean.local Port: 53807, Dst 9f d4 90 db 08 0 ee 5e ac 10 85 3 43 4f c5 b8 2b 0	5440 5440 5440 58 bytes captur 14:90:db), Dst: . (172.16.133.5 : Port: 1853 00 45 00> 39 44 40D dd d0 cc .>/	TCP TCP TCP red (9344 bits) Watchgua_3e:02 7), Dst: 68.64 E. E. E. E. 	2:d0 (00:90:7f:3e:02:d0	7 Len=0 in=16379 Len=0 in=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=183 Win=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=184 Win=16379 Len=0 57700→5440 [FIN, ACK] Seq=212 Ack=184 Win=16379 Len=0
01 67.217.94.204 01 172.16.133.53 01 172.16.133.53 01 157.56.242.198 01 157.56.242.198 01 172.16.133.114 01 172.16.133.414 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 Frame 1: 1168 byt Ethernet II, Src: Internet Protocol User Datagram Pro Data (1126 bytes) 0000 00 90 7f 3e 00 010 04 82 df 00 020 15 8e d2 2f 00 030 1a 0f df bb 00	8200 49292 443 55270 57700 57700 57700 57700 57700 57700 57700 es on wire Apple_d4: Version 4 tocol, Src 40 14 10 00 40 11 3d 04 6e 0f 05 70	172.16.139.250 172.16.139.250 172.16.139.250 (9344 bits), 116 90:db (14:10:9f:d , Src: Sean.local Port: 53807, Dst 9f d4 90 db 088 (ee 5e ac 10 85 3 43 4f c5 b8 2b (88 50 11 77 f1 b	5440 5440 5440 58 bytes captur 14:90:db), Dst: (172.16.133.5 Port: 1853 00 45 00> 39 44 40D dd d0 cc .>./ b1 95 e2	TCP TCP TCP ed (9344 bits) Watchgua_3e:02 7), Dst: 68.64 E. @^9D@ /.=.n CO+ p.P.w	2:d0 (00:90:7f:3e:02:d0	7 Len=0 in=16379 Len=0 in=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=183 Win=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=184 Win=16379 Len=0 57700→5440 [FIN, ACK] Seq=212 Ack=184 Win=16379 Len=0
01 67.217.94.204 01 172.16.133.53 01 172.16.133.53 01 157.56.242.198 01 157.56.242.198 01 172.16.133.53 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 01 172.16.133.43 Frame 1: 1168 byt Ethernet II, Src: Internet Protocol User Datagram Pro Data (1126 bytes) 000 00 90 7f 3e 02 011 12 6 bytes 15 3e d2 2f 07 020 15 3e d2 2f 07 030 1a 0f df bb 00 030 1a 0f df bb 00 04 ec 3a 88 65 92	8200 49292 443 55270 57700 57700 57700 57700 57700 57700 57700 es on wire Apple_d4: Version 4 tocol, Src 2 4 d0 14 10 0 00 40 11 3 d0 46 0 of 05 70 2 aa 26 78	172.16.139.250 172.16.139.250 172.16.139.250 (9344 bits), 116 90:db (14:10:9f:d , Src: Sean.local Port: 53807, Dst 9f d4 90 db 08 0 ee 5e ac 10 85 3 43 4f c5 b8 2b 0	5440 5440 5440 58 bytes captur 14:90:db), Dst: (172.16.133.5 Port: 1853 00 45 00> 39 44 40D dd d0 cc .>./ b1 95 e2 6f aa 9b .:.e	TCP TCP TCP red (9344 bits) Watchgua_3e:02 7), Dst: 68.64 E. E. E. E. 	2:d0 (00:90:7f:3e:02:d0	7 Len=0 in=16379 Len=0 in=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=183 Win=16379 Len=0 57700→5440 [ACK] Seq=212 Ack=184 Win=16379 Len=0 57700→5440 [FIN, ACK] Seq=212 Ack=184 Win=16379 Len=0



Wireshark is great, but

1. Usability

2. Performance

			IIG WIL	ii laige	capture fil	les	wiki.wireshark.
🧧 🔳 🔬 🔘		×	U	U	•		
Apply a display filter	. <%/>	If you h	ave a lar	rge captu	re file e $\sigma > 1$	00MB, Wireshark wil	I become slow whil
Time Source	Source Port	t De		•	•		
201 172.16.133.57	53807	Ioading	, filtering	g and alik	e actions.		
201 172.16.133.57	53807	68					
201172.16.133.5720196.43.146.176	53807 443	172.16.133.82	61228	TCP		443→61228 [ACK] Seq=1 Ack=1 Win=9	0650 Lon-0
201 172.16.133.56	49514	68.64.21.42	1853	UDP		49514→1853 Len=125	
201 68.64.21.62	1853	172.16.133.57	53807	UDP		1853→53807 Len=25	
201 96.43.146.176	443	172.16.133.82	61228	TCP		443→61228 [ACK] Seq=1 Ack=1107 Wi	in=10765 Len=0
201 96.43.146.176	443	172.16.133.82	60073	TCP		443→60073 [ACK] Seq=1 Ack=1 Win=6	65535 Len=0
201 172.16.133.49	58246	68.64.21.41	1853	UDP		58246→1853 Len=125	
201 172.16.133.103		216.115.222.200		ТСР		63406→443 [SYN] Seq=0 Win=8192 Le	
201 172.16.133.43	57700	172.16.139.250	5440	HTTP	172.16.139.250:5440	GET /CSIS/CSISISAPI.dll/?request?	?aaeb6985-26†c-48a7-a5†8-2
20168.64.21.41201172.16.133.43	1853 57700	172.16.133.60 172.16.139.250	63861 5440	UDP TCP		1853→63861 Len=125 [TCP Retransmission] 57700→5440	[DCH ACK] Sec-1 Ack-1 Win
201 67.217.94.135	8200	172.16.133.60	63862	ADP			[FSH, ACK] SEQ=1 ACK=1 WIN
201 67.217.94.156	8200			1121			
	8200						
201 67.217.94.204			1	1		10 210	56 Len=0
201 67.217.94.204 201 172.16.133.53 201 172.16.133.53	8200 49292 49292		bc	tim		19 210	56 Len=0] Seq=1 Ack=1 Win=256 Le
201 67.217.94.204 201 172.16.133.53 201 172.16.133.53 201 157.56.242.198	8200 49292 49292 49292 443	Lo	ad	tim	ne: 0:	19.210] Seq=1 Ack=1 Win=256 Le 03 Len=0
201 67.217.94.204 201 172.16.133.53 201 172.16.133.53 201 157.56.242.198 201 172.16.133.114	8200 49292 49292 49292 443 55270	Lo	ad	tim	ne: 0:	19.210] Seq=1 Ack=1 Win=256 Le 03 Len=0 7 Len=0
201 67.217.94.204 201 172.16.133.53 201 172.16.133.53 201 157.56.242.198 201 172.16.133.114 201 172.16.133.43	8200 49292 49292 443 55270 57700	Lo	ad	tim	ne: 0:	19.210	<pre> Seq=1 Ack=1 Win=256 Le 03 Len=0 7 Len=0 in=16379 Len=0 </pre>
201 67.217.94.204 201 172.16.133.53 201 172.16.133.53 201 157.56.242.198 201 172.16.133.114 201 172.16.133.43 201 172.16.133.43	8200 49292 49292 443 55270 57700 57700				ne: 0:		<pre>) Seq=1 Ack=1 Win=256 Le 03 Len=0 7 Len=0 in=16379 Len=0 in=16379 Len=0</pre>
201 67.217.94.204 201 172.16.133.53 201 172.16.133.53 201 157.56.242.198 201 172.16.133.114 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43	8200 49292 49292 443 55270 57700 57700 57700	172.16.139.250	5440	ТСР	ne: 0:	57700→5440 [ACK] Seq=212 Ack=183	j Seq=1 Ack=1 Win=256 Le 03 Len=0 7 Len=0 in=16379 Len=0 in=16379 Len=0 Win=16379 Len=0
201 67.217.94.204 201 172.16.133.53 201 172.16.133.53 201 157.56.242.198 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43	8200 49292 49292 443 55270 57700 57700	172.16.139.250 172.16.139.250	5440 5440		ne: 0:	57700→5440 [ACK] Seq=212 Ack=183 57700→5440 [ACK] Seq=212 Ack=184	j Seq=1 Ack=1 Win=256 Le 03 Len=0 7 Len=0 in=16379 Len=0 win=16379 Len=0 Win=16379 Len=0
201 67.217.94.204 201 172.16.133.53 201 172.16.133.53 201 157.56.242.198 201 172.16.133.414 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43	8200 49292 49292 443 55270 57700 57700 57700 57700 57700	172.16.139.250 172.16.139.250 172.16.139.250	5440 5440 5440	TCP TCP TCP	ne: 0:	57700→5440 [ACK] Seq=212 Ack=183	j Seq=1 Ack=1 Win=256 Le 03 Len=0 7 Len=0 in=16379 Len=0 win=16379 Len=0 Win=16379 Len=0
201 67.217.94.204 201 172.16.133.53 201 172.16.133.53 201 157.56.242.198 201 172.16.133.414 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43	8200 49292 49292 443 55270 57700 57700 57700 57700 57700	172.16.139.250 172.16.139.250 172.16.139.250 (9344 bits), 116	5440 5440 5440 8 bytes captur	TCP TCP TCP red (9344 bits)	1e: 0:	57700→5440 [ACK] Seq=212 Ack=183 57700→5440 [ACK] Seq=212 Ack=184 57700→5440 [FIN, ACK] Seq=212 Ack	j Seq=1 Ack=1 Win=256 Le 03 Len=0 7 Len=0 in=16379 Len=0 win=16379 Len=0 Win=16379 Len=0
201 67.217.94.204 201 172.16.133.53 201 172.16.133.53 201 157.56.242.198 201 172.16.133.114 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 Erame 1: 1168 byt Ethernet II, Src:	8200 49292 49292 443 55270 57700 57700 57700 57700 57700 57700 ces on wire Apple_d4:5	172.16.139.250 172.16.139.250 172.16.139.250 172.16.139.250 (9344 bits), 116 90:db (14:10:9f:d	5440 5440 5440 8 bytes captur 4:90:db), Dst:	TCP TCP TCP red (9344 bits) : Watchgua_3e:0		57700→5440 [ACK] Seq=212 Ack=183 57700→5440 [ACK] Seq=212 Ack=184 57700→5440 [FIN, ACK] Seq=212 Ack	j Seq=1 Ack=1 Win=256 Le 03 Len=0 7 Len=0 in=16379 Len=0 win=16379 Len=0 Win=16379 Len=0
201 67.217.94.204 201 172.16.133.53 201 172.16.133.53 201 157.56.242.198 201 172.16.133.114 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 Frame 1: 1168 byt Ethernet II, Src: Internet Protocol User Datagram Pro	8200 49292 49292 443 55270 57700 57700 57700 57700 57700 57700 57700 (es on wire Apple_d4:5 Version 4 otocol, Src	172.16.139.250 172.16.139.250 172.16.139.250 (9344 bits), 116 90:db (14:10:9f:d , Src: Sean.local	5440 5440 5440 8 bytes captur 4:90:db), Dst: (172.16.133.5	TCP TCP TCP red (9344 bits) : Watchgua_3e:0	2:d0 (00:90:7f:3e:02:d6	57700→5440 [ACK] Seq=212 Ack=183 57700→5440 [ACK] Seq=212 Ack=184 57700→5440 [FIN, ACK] Seq=212 Ack	j Seq=1 Ack=1 Win=256 Le 03 Len=0 7 Len=0 in=16379 Len=0 win=16379 Len=0 Win=16379 Len=0
201 67.217.94.204 201 172.16.133.53 201 172.16.133.53 201 157.56.242.198 201 172.16.133.114 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 ≥ Frame 1: 1168 byt ► Ethernet II, Src:	8200 49292 49292 443 55270 57700 57700 57700 57700 57700 57700 57700 (es on wire Apple_d4:5 Version 4 otocol, Src	172.16.139.250 172.16.139.250 172.16.139.250 (9344 bits), 116 90:db (14:10:9f:d , Src: Sean.local	5440 5440 5440 8 bytes captur 4:90:db), Dst: (172.16.133.5	TCP TCP TCP red (9344 bits) : Watchgua_3e:0	2:d0 (00:90:7f:3e:02:d6	57700→5440 [ACK] Seq=212 Ack=183 57700→5440 [ACK] Seq=212 Ack=184 57700→5440 [FIN, ACK] Seq=212 Ack	j Seq=1 Ack=1 Win=256 Le 03 Len=0 7 Len=0 in=16379 Len=0 win=16379 Len=0 Win=16379 Len=0
201 67.217.94.204 201 172.16.133.53 201 172.16.133.53 201 157.56.242.198 201 172.16.133.114 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 ≥01 172.16.133.43 ≥01 172.16.133.43 ≥01 172.16.133.43 ≥01 172.16.133.43 ≥01 172.16.133.43	8200 49292 49292 443 55270 57700 57700 57700 57700 57700 57700 57700 (es on wire Apple_d4:5 Version 4 otocol, Src	172.16.139.250 172.16.139.250 172.16.139.250 (9344 bits), 116 90:db (14:10:9f:d , Src: Sean.local	5440 5440 5440 8 bytes captur 4:90:db), Dst: (172.16.133.5	TCP TCP TCP red (9344 bits) : Watchgua_3e:0	2:d0 (00:90:7f:3e:02:d6	57700→5440 [ACK] Seq=212 Ack=183 57700→5440 [ACK] Seq=212 Ack=184 57700→5440 [FIN, ACK] Seq=212 Ack	j Seq=1 Ack=1 Win=256 Le 03 Len=0 7 Len=0 in=16379 Len=0 win=16379 Len=0 Win=16379 Len=0
201 67.217.94.204 201 172.16.133.53 201 172.16.133.53 201 157.56.242.198 201 172.16.133.114 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 Frame 1: 1168 byt Ethernet II, Src: Internet Protocol User Datagram Pro	8200 49292 49292 443 55270 57700 57700 57700 57700 57700 57700 57700 (es on wire Apple_d4:5 Version 4 otocol, Src	172.16.139.250 172.16.139.250 172.16.139.250 (9344 bits), 116 90:db (14:10:9f:d , Src: Sean.local	5440 5440 5440 8 bytes captur 4:90:db), Dst: (172.16.133.5	TCP TCP TCP red (9344 bits) : Watchgua_3e:0	2:d0 (00:90:7f:3e:02:d6	57700→5440 [ACK] Seq=212 Ack=183 57700→5440 [ACK] Seq=212 Ack=184 57700→5440 [FIN, ACK] Seq=212 Ack	j Seq=1 Ack=1 Win=256 Le 03 Len=0 7 Len=0 in=16379 Len=0 win=16379 Len=0 Win=16379 Len=0
201 67.217.94.204 201 172.16.133.53 201 172.16.133.53 201 157.56.242.198 201 157.56.242.198 201 157.56.242.198 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 Solt 172.16.133.43 Solt 172.16.133.43 Solt 172.16.133.43 Solt 172.16.133.43 Solt Solt Solt Solt Solt Solt Solt Solt Solt Solt	8200 49292 443 55270 57700 57700 57700 57700 57700 57700 57700 ces on wire Apple_d4:5 Version 4, otocol, Src	172.16.139.250 172.16.139.250 172.16.139.250 (9344 bits), 116 90:db (14:10:9f:d , Src: Sean.local Port: 53807, Dst	5440 5440 5440 8 bytes captur 4:90:db), Dst: (172.16.133.5 Port: 1853 00 45 00:	TCP TCP TCP red (9344 bits) : Watchgua_3e:0 57), Dst: 68.64 >E.	2:d0 (00:90:7f:3e:02:d6	57700→5440 [ACK] Seq=212 Ack=183 57700→5440 [ACK] Seq=212 Ack=184 57700→5440 [FIN, ACK] Seq=212 Ack	j Seq=1 Ack=1 Win=256 Le 03 Len=0 7 Len=0 in=16379 Len=0 win=16379 Len=0 Win=16379 Len=0
201 67.217.94.204 201 172.16.133.53 201 172.16.133.53 201 157.56.242.198 201 172.16.133.114 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 Ethernet II, Src: Internet Protocol User Datagram Pro Data (1126 bytes) 20000 00 90 7f 3e 02 0010 04 82 fd 44 00	8200 49292 49292 443 55270 577000 577000 57700000000	172.16.139.250 172.16.139.250 172.16.139.250 (9344 bits), 116 90:db (14:10:9f:d , Src: Sean.local Port: 53807, Dst 9f d4 90 db 08 0 ee 5e ac 10 85 3	5440 5440 5440 8 bytes captur 4:90:db), Dst: (172.16.133.5 Port: 1853 00 45 00 39 44 40	TCP TCP TCP red (9344 bits) : Watchgua_3e:0 57), Dst: 68.64 >E. D@^9D@	2:d0 (00:90:7f:3e:02:d6	57700→5440 [ACK] Seq=212 Ack=183 57700→5440 [ACK] Seq=212 Ack=184 57700→5440 [FIN, ACK] Seq=212 Ack	j Seq=1 Ack=1 Win=256 Le 03 Len=0 7 Len=0 in=16379 Len=0 win=16379 Len=0 Win=16379 Len=0
201 67.217.94.204 201 172.16.133.53 201 172.16.133.53 201 157.56.242.198 201 172.16.133.114 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 Ethernet II, Src: Internet Protocol User Datagram Pro Data (1126 bytes) 0000 00 90 7f 3e 02 0010 04 82 fd 44 00 0020 15 3e d2 2f 07	8200 49292 49292 443 55270 57700 57000 57000 57000 57000 57000 57000 57000 57000 57000 57000 57000 57000 57000 57000 57000 57000 570000 5700000000	172.16.139.250 172.16.139.250 172.16.139.250 (9344 bits), 116 90:db (14:10:9f:d , Src: Sean.local Port: 53807, Dst 9f d4 90 db 08 0 ee 5e ac 10 85 3 43 4f c5 b8 2b 0	5440 5440 8 bytes captur 4:90:db), Dst: (172.16.133.5 Port: 1853 00 45 00 39 44 40 dd d0 cc .>.	TCP TCP TCP red (9344 bits) : Watchgua_3e:0 57), Dst: 68.64	2:d0 (00:90:7f:3e:02:d6	57700→5440 [ACK] Seq=212 Ack=183 57700→5440 [ACK] Seq=212 Ack=184 57700→5440 [FIN, ACK] Seq=212 Ack	j Seq=1 Ack=1 Win=256 Le 03 Len=0 7 Len=0 in=16379 Len=0 win=16379 Len=0 Win=16379 Len=0
201 67.217.94.204 201 172.16.133.53 201 172.16.133.53 201 172.16.133.53 201 172.16.133.14 201 172.16.133.43 201 172.16.134 201 172.16.134 201 172.16.134 201 172.16.134	8200 49292 49292 443 55270 57700 57700 57700 57700 57700 57700 ces on wire Apple_d4:5 Version 4, otocol, Src 2 d0 14 10 0 00 40 11 7 3d 04 6 d 0f 05 70 2 aa 26 78	172.16.139.250 172.16.139.250 172.16.139.250 (9344 bits), 116 90:db (14:10:9f:d , Src: Sean.local Port: 53807, Dst 9f d4 90 db 08 (ee 5e ac 10 85 3 43 4f c5 b8 2b (88 50 11 77 f1 1 45 11 ac 84 4a (5440 5440 5440 8 bytes captur 4:90:db), Dst: (172.16.133.5 Port: 1853 00 45 00 39 44 40 dd d0 cc 51 95 e2 61 aa 9b	TCP TCP TCP red (9344 bits) : Watchgua_3e:0 57), Dst: 68.64 >E. D@^9D@	2:d0 (00:90:7f:3e:02:d6	57700→5440 [ACK] Seq=212 Ack=183 57700→5440 [ACK] Seq=212 Ack=184 57700→5440 [FIN, ACK] Seq=212 Ack	j Seq=1 Ack=1 Win=256 Le 03 Len=0 7 Len=0 in=16379 Len=0 win=16379 Len=0 Win=16379 Len=0
201 67.217.94.204 201 172.16.133.53 201 172.16.133.53 201 157.56.242.198 201 172.16.133.114 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 201 172.16.133.43 Ethernet II, Src: Internet Protocol User Datagram Pro Data (1126 bytes) 0000 00 90 7f 3e 02 0010 04 82 fd 44 00 0020 15 3e d2 2f 07 0030 1a 0f df bb 00 0040 ec 3a 88 65 92 0050 6a c6 90 ce 51	8200 49292 49292 443 55270 5770 57700 57000 57000 57000 57000 57000 57000 57000 57000 57000 5700000000	172.16.139.250 172.16.139.250 172.16.139.250 (9344 bits), 116 90:db (14:10:9f:d , Src: Sean.local Port: 53807, Dst 9f d4 90 db 08 0 ee 5e ac 10 85 43 4f c5 b8 2b 0 88 50 11 77 f1 45 11 ac 84 4a 0 24 53 40 19 30 3	5440 5440 8 bytes captur 4:90:db), Dst: (172.16.133.5 Port: 1853 00 45 00 39 44 40 dd d0 cc .>. b1 95 e2 6f aa 9b 55 18 eb j.	TCP TCP TCP red (9344 bits) : Watchgua_3e:0 57), Dst: 68.64 >E. D@. ^9D@ /.=.n CO+ p. P.W e&x EJO X.c \$S@.0U.	2:d0 (00:90:7f:3e:02:d6	57700→5440 [ACK] Seq=212 Ack=183 57700→5440 [ACK] Seq=212 Ack=184 57700→5440 [FIN, ACK] Seq=212 Ack	j Seq=1 Ack=1 Win=256 Le 03 Len=0 7 Len=0 in=16379 Len=0 win=16379 Len=0 Win=16379 Len=0
201 67.217.94.204 201 172.16.133.53 201 172.16.133.53 201 172.16.133.53 201 172.16.133.14 201 172.16.133.43 201 172.16.134 201 172.16.134 201 172.16.134 201 172.16.134	8200 49292 49292 443 55270 5770 57700 57000 57000 57000 57000 57000 57000 57000 57000 57000 5700000000	172.16.139.250 172.16.139.250 172.16.139.250 (9344 bits), 116 90:db (14:10:9f:d , Src: Sean.local Port: 53807, Dst 9f d4 90 db 08 0 ee 5e ac 10 85 43 4f c5 b8 2b 0 88 50 11 77 f1 45 11 ac 84 4a 0 24 53 40 19 30 3	5440 5440 8 bytes captur 4:90:db), Dst: (172.16.133.5 Port: 1853 00 45 00 39 44 40 dd d0 cc .>. b1 95 e2 6f aa 9b 55 18 eb j.	TCP TCP TCP red (9344 bits) : Watchgua_3e:0 57), Dst: 68.64 >E. D@. ^9D@ /.=.n CO+ p. P.w e&x EJo.	2:d0 (00:90:7f:3e:02:d6	57700→5440 [ACK] Seq=212 Ack=183 57700→5440 [ACK] Seq=212 Ack=184 57700→5440 [FIN, ACK] Seq=212 Ack	j Seq=1 Ack=1 Win=256 Le 03 Len=0 7 Len=0 in=16379 Len=0 win=16379 Len=0 Win=16379 Len=0



wiki wirochark org

Wireshark is great, but

1. Usability

- 2. Performance
- 3. Resources

					Wireshark · Export · H	TTP object list	
				bigFlows.pcap			Wireshark · Export · HTTP object list
		XC	Packet	Hostname	Content Type	Size	Filename
Annhu e dienleu filter	- 9-2 /		133015	www.nbc.com	image/jpeg		smash_top_hudson_01.jpg
Apply a display filter <			133154	www.nbc.com	image/jpeg		jlg_top_kaiser_02a.jpg
e Source		Destination	133287	www.nbc.com	image/jpeg		goon_lf_whitford_01.jpg
1 172.16.133.57	53807	68.64.21.6	133384	www.nbc.com	image/jpeg		snl_lf_waltz.jpg
1 172.16.133.57	53807	68.64.21.6	133465	www.nbc.com	image/jpeg		cap_lf_cast.jpg
1 172.16.133.57	53807	68.64.21.6	133542	www.nbc.com	image/jpeg		otr_768_mandel_01.jpg
1 96.43.146.176	443	172.16.133	133649	www.nbc.com	image/jpeg		rev_lf_rev-returns_01.jpg
1 172.16.133.56	49514	68.64.21.4	133724	www.nbc.com	image/jpeg		bl lf ali.jpg
1 68.64.21.62	1853	172.16.133	133819	www.nbc.com	image/jpeg		days_lf_weekly-preview.jpg
1 96.43.146.176	443	172.16.133	133940	www.nbc.com	image/jpeg		rev_lf_wheatley_03.jpg
1 96.43.146.176	443	172.16.133	134027	www.nbc.com	0 111 0		
1 172.16.133.49	58246	68.64.21.4	134027	www.nbc.com www.nbc.com	image/jpeg image/jpeg		snl-new-cropped-proto-custom_51.jpg
1 172.16.133.103	63406	216.115.22	134066	www.nbc.com www.nbc.com	image/jpeg image/png		icons-s5b32d4f9ff-3.png
1 172.16.133.43	57700	172.16.139	134327				sweetsansonair-heavy-webfont.ttf
1 68.64.21.41	1853	172.16.133	134327	www.nbc.com	application/x-font-ttf		· · · · · · · · · · · · · · · · · · ·
l 172.16.133.43	57700	172.16.139	134474	www.nbc.com	application/x-font-ttf		
67.217.94.135	8200	172,16,133	134808	www.nbc.com	image/jpeg		otr_top_cannon_01.jpg?01AD=3IHTRArnolg7OcEyRN
67.217.94.156	8200	172.16.133		www.nbc.com	image/gif		handtinytrans.gif
67.217.94.204	8200	172.16.133	134930	www.nbc.com	image/png		arrow-home-white.png
172.16.133.53	49292	172.16.139	135341	www.nbc.com	application/x-font-ttf		sweetsansonair-medium-webfont.ttf
L 172.16.133.53	49292	172.16.139	135989	www.nbc.com	image/png		arrow-home-blue.png
l 157.56.242.198	49292	172.16.133	137028	www.nbc.com	text/html	30 kB	
			137067	www.nbc.com	text/html		dropdowns-site.html
1 172.16.133.114	55270	67.217.65.	138305	www.nbc.com	text/html		footer-global.shtml
1 172.16.133.43	57700	172.16.139	142007	www.nbc.com	text/html	1566 bytes	
1 172.16.133.43	57700	172.16.139	142073	www.nbc.com	application/json		listTopVideos?timePeriod=HOURLY&fromRow=0&to
1 172.16.133.43	57700	172.16.139	142085	www.nbc.com	image/jpeg	7024 bytes	5 = = ,,,,
1 172.16.133.43	57700	172.16.139	142123	www.nbc.com	image/jpeg		bl_224_face-your-fears_01.jpg
1 172.16.133.43	57700	172.16.139	142126	www.nbc.com	image/jpeg		dec_224_press-conference_01.jpg
Frame 1: 1168 byte			142134	www.nbc.com	image/gif	4916 bytes	
Ethernet II, Src:	Apple_d4:9	0:db (14:10	142171	www.nbc.com	image/gif		logo-localstations.gif
Internet Protocol	Version 4,	Src: Sean.	142215	www.nbc.com	image/jpeg		logo-theweatherchannel.jpg
User Datagram Prot	ocol, Src	Port: 53807	142389	www.nbc.com	image/jpeg		zeebox_190.jpg
Data (1126 bytes)			142390	www.nbc.com	text/html	1414 bytes	3
			142449	www.nbc.com	image/jpeg		Fallon-iphone-app-promo.jpg
			142476	www.nbc.com	image/jpeg	26 kB	NBCApp.jpg
00 00 90 7f 3e 02 10 04 82 fd 44 00 20 15 3e d2 2f 07	00 40 11 3d 04 6e	9f d4 90 d ee 5e ac 1 43 4f c5 b	Help				Save All Close Save
30 1a 0f df bb 0d 40 ec 3a 88 65 92 50 6a c6 90 ce 5f 60 ec 25 37 44 42	aa 26 78 58 ea 63	45 11 ac 8 24 53 40 1	7 f1 b1 95 e2 4 4a 6f aa 9b 9 30 55 18 eb c 05 18 a4 83	p.P.w .:.e&x EJo jX.c \$5@.0U .%7DB			
2 bigFlows							isplayed: 791615 (100.0%) · Load time: 0:19.210 Profile: I



Wireshark is great, but

1. Usability

- 2. Performance
- 3. Resources
- How else can you access a pcap?

			• • •		Wireshark · Export · H	TTP object list	
				bigFlows.pcap			Wireshark · Export · HTTP object list
		XC					
			Packet	Hostname	Content Type	Size	Filename
Apply a display filter <	:		133015	www.nbc.com	image/jpeg		smash_top_hudson_01.jpg
me Source	Source Port	Destination	133154	www.nbc.com	image/jpeg		jlg_top_kaiser_02a.jpg
01 172.16.133.57	53807	68.64.21.6	133287	www.nbc.com	image/jpeg		goon_lf_whitford_01.jpg
01 172.16.133.57	53807	68.64.21.6	133384	www.nbc.com	image/jpeg		snl_lf_waltz.jpg
01 172.16.133.57	53807	68.64.21.6	133465	www.nbc.com	image/jpeg		cap_lf_cast.jpg
01 96.43.146.176	443	172.16.133	133542	www.nbc.com	image/jpeg		otr_768_mandel_01.jpg
01 172.16.133.56	49514	68.64.21.4	133649	www.nbc.com	image/jpeg		rev_lf_rev-returns_01.jpeg
01 68.64.21.62	1853	172.16.133	133724	www.nbc.com	image/jpeg		bl_lf_ali.jpg
01 96.43.146.176	443	172.16.133	133819	www.nbc.com	image/jpeg		days_lf_weekly-preview.jpg
01 96.43.146.176	443	172.16.133	133940	www.nbc.com	image/jpeg		rev_lf_wheatley_03.jpg
01 172.16.133.49	58246	68.64.21.4	134027	www.nbc.com	image/jpeg		grim_lf_preview.jpg
01 172.16.133.103	63406	216.115.22	134066	www.nbc.com	image/jpeg		snl-new-cropped-proto-custom_51.jpg
01 172.16.133.43	57700	172.16.139	134185	www.nbc.com	image/png		icons-s5b32d4f9ff-3.png
01 68.64.21.41		172.16.133	134327	www.nbc.com	application/x-font-ttf	58 kB	sweetsansonair-heavy-webfont.ttf
	1853		134474	www.nbc.com	application/x-font-ttf	59 kB	sweetsansonair-regular-webfont.ttf
01 172.16.133.43	57700	172.16.139	134808	www.nbc.com	image/jpeg	157 kB	otr_top_cannon_01.jpg?01AD=3IHTRArnolg7OcEyRN
01 67.217.94.135	8200	172.16.133	134882	www.nbc.com	image/gif	37 bytes	handtinytrans.gif
01 67.217.94.156	8200	172.16.133	134930	www.nbc.com	image/png	1245 bytes	arrow-home-white.png
01 67.217.94.204	8200	172.16.133	135341	www.nbc.com	application/x-font-ttf	59 kB	sweetsansonair-medium-webfont.ttf
01 172.16.133.53	49292	172.16.139	135989	www.nbc.com	image/png	1243 bytes	arrow-home-blue.png
01 172.16.133.53	49292	172.16.139	137028	www.nbc.com	text/html	30 kB	dropdowns-global.shtml
01 157.56.242.198	443	172.16.133	137067	www.nbc.com	text/html	1497 bytes	dropdowns-site.html
01 172.16.133.114	55270	67.217.65.4	138305	www.nbc.com	text/html	8307 bytes	footer-global.shtml
01 172.16.133.43	57700	172.16.139	142007	www.nbc.com	text/html	1566 bytes	products.php?v=nbc&ecid=PRF-NBC-102769&pa=F
01 172.16.133.43	57700	172.16.139	142073	www.nbc.com	application/json	13 kB	listTopVideos?timePeriod=HOURLY&fromRow=0&tc
01 172.16.133.43	57700	172.16.139	142085	www.nbc.com	image/jpeg	7024 bytes	goon_224_whitford_01.jpg
01 172.16.133.43	57700	172.16.139	142123	www.nbc.com	image/jpeg	11 kB	bl_224_face-your-fears_01.jpg
01 172.16.133.43	57700	172.16.139	142126	www.nbc.com	image/jpeg		dec_224_press-conference_01.jpg
Frame 1: 1168 byte			142134	www.nbc.com	image/gif	4916 bytes	
Ethernet II, Src: /			142171	www.nbc.com	image/gif	6468 bytes	logo-localstations.gif
Internet Protocol			142215	www.nbc.com	image/jpeg	-	logo-theweatherchannel.jpg
User Datagram Proto			142389	www.nbc.com	image/jpeg		zeebox_190.jpg
Data (1126 bytes)	JUUL, SIL	FUIL: 55007	142390	www.nbc.com	text/html		products.php?v=nbc&cnt=3&thumbnailImgsize=778
Data (1120 Dytes)			142449	www.nbc.com	image/jpeg	-	Fallon-iphone-app-promo.jpg
			142476	www.nbc.com	image/jpeg		NBCApp.jpg
			142470	www.iibc.com	inuge/jpeg	20 110	100/100.000
000 00 90 7f 3e 02	d0 14 10	9f d4 90 d					
	00 40 11	ee 5e ac 1	Help				Save All Close Save
020 15 3e d2 2f 07	3d 04 6e	43 4f c5 b					
030 1a Of df bb Od			f1 b1 95 e2	p .P.w			
040 ec 3a 88 65 92			4a 6f aa 9b	.:.e&x EJo			
050 6a c6 90 ce 5f			30 55 18 eb	jX.c \$S@.0U			
060 ec 25 37 44 42	es da 32	er eg að 80	18 a4 83	.%7DB			
bigFlows						Packets: 791615 · D	isplayed: 791615 (100.0%) · Load time: 0:19.210 Profile: E





20180706.pcap

- File systems organize unstructured data and make them available to the user
 - Create a file system for pcaps

Name	Date Modified
67.217.94.135	Today at 22:49
67.217.94.156	Today at 22:49
67.217.94.204	Today at 22:49
68.64.21.41	Today at 22:49
68.64.21.62	Today at 22:48
96.43.146.176	Today at 23:03
67.217.94.204	Today at 23:03
👼 HTTPData.jpg	Today at 23:03
68.64.21.41	Today at 22:50
172.16.133.43	Today at 22:50
172.16.133.58	Today at 22:50
172.16.133.43	Today at 23:02
172.16.133.57	Today at 22:48
172.16.133.58	Today at 22:48
172.16.133.103	Today at 22:49



- File systems organize unstructured data and make them available to the user
 - Create a file system for pcaps
- Create a structure, which can be used when accessing the same network capture again
 - Create an index file keeping track of the files in the file system





20180706.index

20180706.pcap

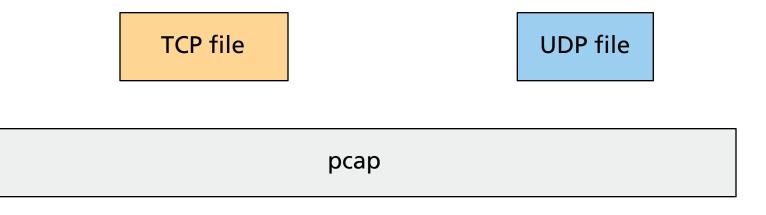
🛑 😑 🛑 🚞 pca	pFileSystem
) ♣ • ⚠
Name	Date Modified
67.217.94.135	Today at 22:49
67.217.94.156	Today at 22:49
67.217.94.204	Today at 22:49
68.64.21.41	Today at 22:49
68.64.21.62	Today at 22:48
96.43.146.176	Today at 23:03
67.217.94.204	Today at 23:03
📄 HTTPData.jpg	Today at 23:03
68.64.21.41	Today at 22:50
172.16.133.43	Today at 22:50
172.16.133.58	Today at 22:50
172.16.133.43	Today at 23:02
172.16.133.57	Today at 22:48
172.16.133.58	Today at 22:48
172.16.133.103	Today at 22:49



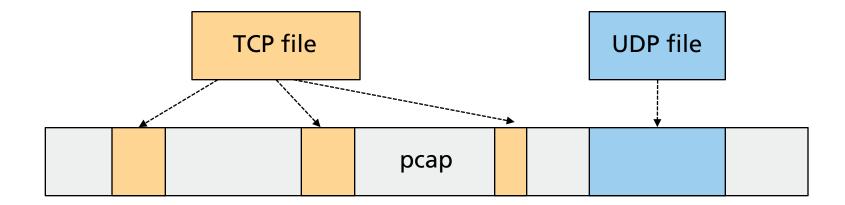
- File systems organize unstructured data and make them available to the user
 - Create a file system for pcaps
- Create a structure, which can be used when accessing the same network capture again
 - Create an index file keeping track of the files in the file system
- Extracting data in order to process it creates unnecessary overhead
 - Point directly into the data in the pcap

20180706.index	010101 011010 011100 20180706.pcap			
🛑 🕘 🛑 💼 pcapF	leSystem			
	☆ ~ ①			
Name	Date Modified			
67.217.94.135	Today at 22:49			
67.217.94.156	Today at 22:49			
67.217.94.204	Today at 22:49			
68.64.21.41	Today at 22:49			
68.64.21.62	Today at 22:48			
▼ ■ 96.43.146.176	Today at 23:03			
▼ 🛅 67.217.94.204	Today at 23:03			
HTTPData.jpg	Today at 23:03			
▶ 💼 68.64.21.41	Today at 22:50			
172.16.133.43	Today at 22:50			
172.16.133.58	Today at 22:50			
▶	Today at 23:02			
172.16.133.57	Today at 22:48			
▶	Today at 22:48			
172.16.133.103	Today at 22:49			





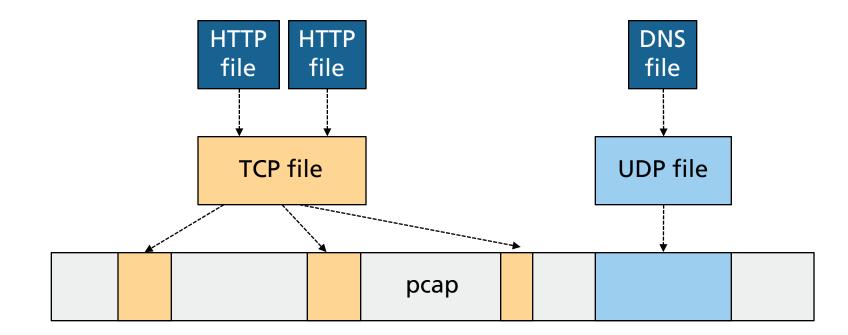




TCP and UDP files point directly into the pcap

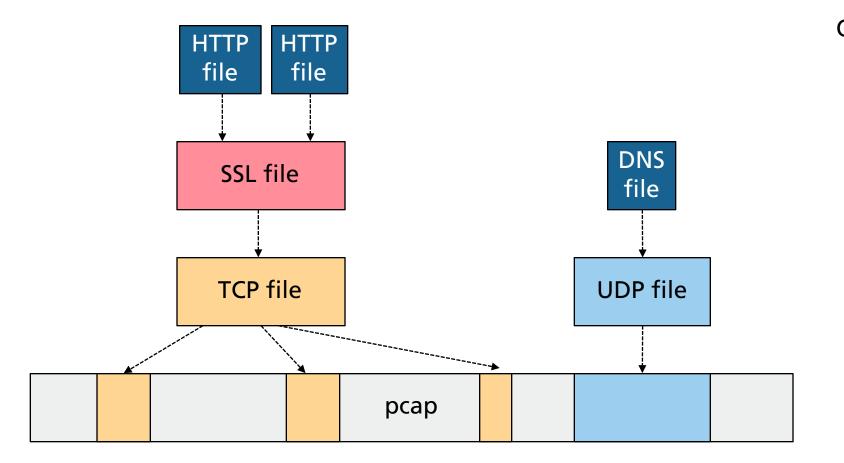


11 © Fraunhofer FKIE



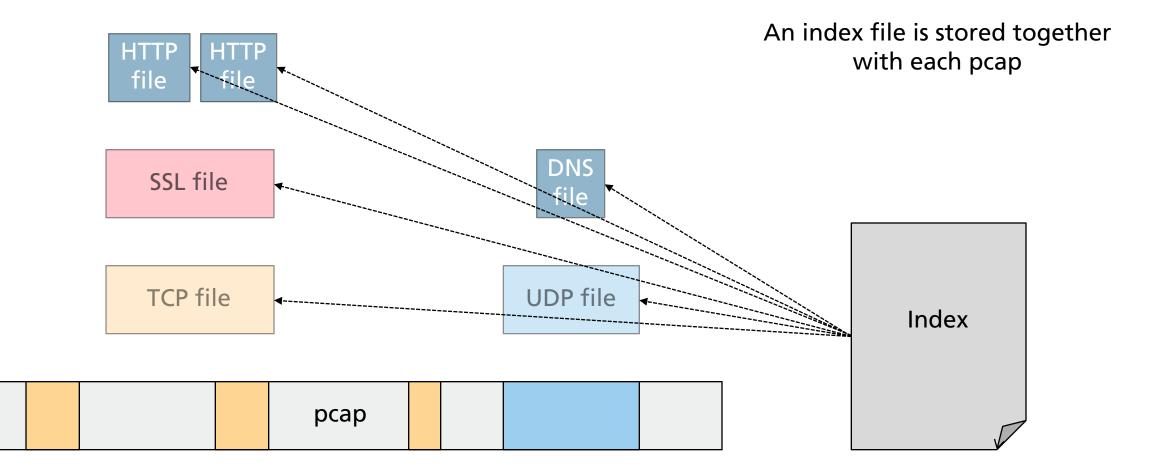
Application protocols can then point into the TCP and UDP files





Other protocols add new virtual layers in between







- pcapFS is a FUSE module mounting captured network data as a virtual file system
 - Filesystem in Userspace is part of the Linux kernel and available for multiple operating systems including FreeBSD, OpenBSD and MacOS
 - Another "pcapFS" was already released as part of the PyFlag framework by Michael Cohen
 - Unfortunately deprecated and not maintained S
- Index files can be stored in memory or on disk for future mounts
- Protocols are implemented by virtual file classes





Demo



- Usability
 - Data is presented using the virtual file system
 - Its hierarchy can be specified using multiple sorting options
- Performance
 - First mount of a pcap creates an index file
 - Browsing through the mounted data takes almost no time
 - Mounting with a used index is significantly faster than Wireshark
- Resources
 - Files in pcapFS point directly into the pcap or other virtual files
 - They are only extracted on demand



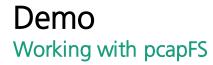


Demo



- pcapFS supports mounting of split pcap files
- File system level tools can be used on the mounted data without any extraction
- Metadata can be preprocessed and displayed as an own file as for example:
 - HTTP header
 - DNS requests and responses (e.g. as JSON)
- Missing data in streams can easily be padded for reconstruction

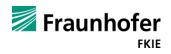




Demo



- Decryption of data by providing the corresponding key files
 - More cipher suites for SSL will be added in the future
 - Key files can be implemented for multiple protocols
- Configuration files force a protocol decoding on files with specified properties:
 - e.g. XOR dstPort 31489 protocol http



Summary

- pcapFS gives investigators the possibility to
 - quickly take a look at the relevant data of a network capture
 - order the data by different criteria
 - use file system level tools for their analysis
- Keeping an index file for each pcap significantly increases the performance of analyzing pcaps
- Using virtual files eliminates the overhead of extracting data out of pcaps



Future Plans

Add support for more protocols (wishes are more than welcome!)

- Particularly add support for other cipher suites in SSL
- BitTorrent, HTTP2, SMB
- Add support for more metadata
 - e.g. SSL certificates
- Make use of Symbolic Links (e.g. reverse connections)
- Add support for pcapng



Thanks for your attention!

https://github.com/fkie-cad/pcapfs

jan-niclas.hilgert@fkie.fraunhofer.de

