

### How to merge Trace Files with ClearSight<sup>™</sup> Analyzer

### **Overview**

Due to the complexity of today's networks, it's often difficult to pinpoint where problems occur. These problems may be caused by one or more network elements: network device (router, switch, firewall, etc.) client, server, or application. In addition, these elements may reside in different network segments. Viewing data from one segment provides only a local perspective. Viewing data from multiple segments becomes a challenge since correlation often proves too tedious and time consuming. With ClearSight Analyzer (CSA), this challenge is overcome by its ability to create a combined "ladder" diagram using trace files from up to four different network segments. IT Professionals will then be able to visualize data in proper perspective where the order of frames as they are generated, forwarded, received, processed, and replied to by the different network elements are taken into account.

### How-to

This application note provides a methodology illustrating ClearSight Analyzer's Trace File Merge and Multi-Segment Analysis function. A general description of the function is given followed by a more detailed procedure.

A common first step in multi-segment analysis is to collect data from two or more (up to four) network segments and to save the data to respective trace files. The trace files may then be merged using the Trace File Merge function combined in CSA. The merged trace file will be displayed in a multisegment view showing how and how fast packet transverse through each segment. The input trace files may be one of the following commonly used format: .adc, .enc, or .pcap format. The resulting merged trace files will be in .adc format for use with the ClearSight Analyzer (or Network Time Machine).

#### Steps to merge two or more Trace Files

- Select Merge from the File menu. The ClearSight Analyzer Choose File(s) to Merge dialog box will appear.
- Navigate to the location of the file(s) you want to include. Click or Ctrl-Click on the specific trace files. The result will be similar to Figure 1.

Look in:  🙆	Trace		-	# 🛃 🔊
Name		Size	Туре	Date Modified
🛋 filter-4-fra	nes.adc	2 KB	ADC File	5/28/2008 3:1
🖌 merge time	adjusted.adc	264 KB	ADC File	5/28/2008 5:5
merge1.ad	u l	264 KB	ADC File	5/21/2008 5.5
seg-1.adc		135 KB	ADC File	5/21/2008 4:5
seq-2.adc		130 KB	ADC File	5/21/2008 4:5
<u>&lt;</u>	"seg-1.adc" "seg-2.a	dc"		
file Name:				

Figure 1: Choose Trace File(s) to Merge Dialog Box

**3.** Click Open. The ClearSight Analyzer File Merge dialog box will appear, with the file(s) you just selected included (see Figure 2). You can choose familiar names for the segments. To give a file a different segment name, double click in the Segment column for that file. Type in the new name or select a name from the drop-down list.

les Selected For Merge			Auto Sync
Filename	5	Cogmont	Time Offset.
Nocuments and Settings/liang/My Documents/Trace/seg-1.ac	lc	Segment1	
Documents and Settings/liang/Wy Documents/Trace/seg-2.ad	tc	Segment2	1

Figure 2: Trace Files Selected for Merge



## How to merge Trace Files with ClearSight Analyzer



- 4. If the time stamp for the first packet is not the same in all the trace files, you can enter an adjustment factor for any file in the Time Offset (sec) column (see Figure 2). By clicking Auto Sync, ClearSight Analyzer can calculate Time Offset automatically IF there is TCP Connection (SYN, SYN/ACK, and ACK) frame sequence; otherwise, you need to calculate offset(s) time manually. An example of how to calculate the adjustment is shown in page 3.
- **5.** Continue the process until you have gathered all the trace files that you want included. Up to four trace files may be specified. Then click the Merge button. The ClearSight Analyzer Save Merge To dialog box will appear (see Figure 3). Navigate to the location where you want to save the file, choose a name for the merged file, and click Save. The new merged trace file can now be opened in the ClearSight Analyzer.

😤 Save Merg	e To	
Save in:	Trace	- • • • • =
in filter-4-fra merge-tim merge1.ac seg-1.adc seg-2.adc	e-adjusted adr. Ic	
File <u>N</u> ame: Files of <u>Lyp</u> e:	merge1.adc ClearSight Files (.adc)	
		Save Cancel

Figure 3: Save Merge To Dialog Box

# Example on how to manually and calculate a time offset

In this section, how to calculate a time offset in detail. If there is TCP Connections (SYN, SYN/ACK, and ACK) frame sequence, CSA will calculate Time Offset automatically by clicking Auto Sync. However, you need to calculate time offset manually when there is no TCP Connection sequence.

- Open the merge1.adc trace file. In our example, we select a MGCP-VoIP application from the Main pane of the Detail tab. Then we select one of these flows, and view the multi-segment ladder display in the Conversation tab of the Statistics pane (see Figure 4).
- In the decode view, highlight 2 identical frames from 2 segments and check these frames on the left side (see Figure 5)
- Right mouse click on the chosen frames and choose Filter Checked Frames as shown in Figure 6.



Figure 4: Ladder View for Merge1.adc Trace File

192		alus	-	-	Src. A	-		1. 1.22	Len	Protocol	_			Summery	
	Seg Segae				43.12			1.116.19		MOCP	8072	Connerd, NTT			8[192.168.0.111
	Seg Segae					6.195		1.120.26	64	NOCP		Perponse, 21			**************
	Seg Secar							3.120.26	109	BOCP					18(71.243.120.2
	Seg Seme					10.26		1.116.19		DOCP		Response, 20			
	Seg Segae							1.116.19		ROCE					BI197.168.0.111
	Seg Segue			67.1	\$1.11	6.195	192.1	\$8.0.115	60	RCCP		Perponse, 30			
1 29 0	Seg Segar	1150		67.15	51.11	6.195	192.1	\$8.0.115	109	HOUP	HOCP,	Connand, RQS	T 47926-	\$769 110T	19(71.243.120.2
30 0	Seg Segae	nc.11		192.1	168.0	0.115	67.15	1.116.19	5 64	ROCP	MOCP.	Response, 20	0 47926	1769 GK	
	seg segue	15.28		71.24	43.12	10.26	\$7.15	1.116.195	5 219	NOCP	MGCP.	Connand, 281	9 65790	100T 2548	[192.168.0.115]
3 88 0				(7.1)		6 106	10. 20	30 001 0	102	work	MACON .	Fannand Pris	* *>< >>		10711 141 110
From EIN 1994	e 27 (110 II, MAC d , Stc Add std port , Command	bytes t 610 1 191	100- 108.0	20-58	242	18-10. A0311	HAC 5 67.15	C &ddr:		10+5 <b>7</b> -50					
Pose EIII 1 Direction Direction Direction	e 27 (110 II, MAC d , SEC Add Att port	bytes t 610 1 191	100- 108.0	20-58	242	18-10. A0311	HAC 5 67.15	C &ddr:		10-5 <b>7</b> -50					
Trane	e 27 (110 II, MAC d , SEC Add Att port	bytes t 610 1 191	100- 108.0	20-58	242	18-10. A0311	HAC 5 67.15	rc addr: 1.116.19 .115) M90	s CF 1.0	0-57-50		Text			
Trane Address	e 27 (110 II, MAC d , Sic Add are port , Command	bytes t 610 1 191	: 00- 168.0 6st 25231	20-58 115, port/ 261 1	0-06+ 242 207_	18-10, Addi: 7 19(192	MAC 5 67.15 .160.0	rc addr: 1.116.19 .115) M90	s CF 1.0	E F					
Prome ETE : 1994, 	e 27 (110 II, MAC d , Stc Add std port , Command 0 1 00 20 1	bytes t 610 1 191	: 00- 168.0 6st 25231	20-58 115, 00111 361 1 5 10	6 00	18-10, A0101 7 19(192 7 8	MAC 5 67.15 .160.0	A B	5 CF 1.0 C D D8 E0	E F		]Rh	_		
7 24 Frame	e 27 (110 II. MAC d ste port , Ceanacid 0 1 00 20 5	bytes nt edd 1 192 2 437 , NTFT 2 3 8 06	: 00- 168.0 6st 25231 4 18	20-52 115, 061 1 5 10 80 78	6 00	18-10, A0121 7 19(192 7 0 04 43	HAC 5 67.15 .160.0	A 0 37 30	C D C D C D C D C D C D C D C D C D C D	E F 43 68 . 43 97 .	£	1	_		
Trans T	e 27 (150 II, HAC d , SEC Add pre ports , Creanend 0 1 00 20 1 00 20 1 00 65 4 74 6 79 ( 35 32 1	bytes it add it 192 2437, NTFT 2437, NTFT 2437, NTFT 2437, NTFT 2537, NTFT 2537, NTFT 2537, NTFT 2537, NTFT	1 00- 168.0 dst 25231 4 18 60 69 33	20-58 115, 0011 3611 5 10 78 36	6 00 31	18-10, A0121 7 19[192 7 0 04 63 11 01 54 21 20 65	HAC 5 67.15 .160.0	A 0 37 30 48 54 48 54	C D C D C D C D C D C D C D C D C C C D C C C D C C C D C C C D C C C D C C C C	E F 45 68 . 43 97 J 20 32 4 40 58 5	[] []	1]Eh 1			
Trane T	e 27 (110 II, HAC d , SEC Add mer port , Commend 0 1 00 20 1 00 68 4 74 (5) 4 35 32 31 39 5	bytes it add it 192 2437, NTFT 2437, NTFTT 2437, NTFTT 2437, NTFTTT 2437, NTFTTT 2437, NTFTTTT 2437, NTFTTTTTTTTT 2437, NTFTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT	4 18 18 18 60 69 33 31	20-58 115, 0011 2611 2611 36 36 36	6 00 31 38	18-10, A032; 7 19(192 7 0 4 63 11 61 54 91 20 69 28 30	HAC 5 67.15 .160.0	A 0 37 30 42 54 31 31 31 31	CF 1.0 CF 1.0 CB E0 00 73 44 59 54 59 54 51 35 55	E F 43 68 - 43 97 - 20 32 8 20 45 1	[) [.[.T) 231361 ( 92.168.0	1]Kh TK 1.WTFY 2 10077_19[ 0.115] M			
Trans T	e 27 (110 II, HAC d , Stc Add mtr pot , Creaned 0 1 00 20 1 00 45 4 74 C3 35 32 31 39 3	bytes it add it 192 2437, NTFT 2437, NTFT 2437, NTFT 2437, NTFT 2537, NTFT 2537, NTFT 2537, NTFT 2537, NTFT	1 00- 168.0 dst 25231 4 18 60 69 33	5 10 5 10 78 34 22	6 00 31 38 30	18-10, A0121 7 19[192 7 0 04 63 11 01 54 21 20 65	HAC 5 67.15 .160.0	A 0 37 30 48 54 48 54	CF 1.0 CF 1.0 CB 80 CO 73 46 59 5F 31 35 55 31 30	E F 43 68 4 43 97 1 20 32 4 40 58 8 20 45 1 30 36 0	[] []	L_1Kh L			



Figure 6: Filter Checked Frames

- 4. You will see 4 frames are filtered out as shown in Figure 7.These frames are saved into a new trace file. Filter-4-frames.adc, by clicking Save As from the File menu. The Save Filtered Packets dialog box will appear and you need to choose No in order to save filtered trace files (see Figure 8).
- 5. The filter-4-frames.adc will come up with only four frames as shown in Figure 9. Frames 1 and 2 belong to Segment 2, while frames 3 and 4 belong to Segment 1. The next step is to figure out the time offset between the two segments.



**6.** There are two timing values that we need to consider: relative time and delta time, as shown in Figure 9 and Table 1. The four frames listed with respect to their relatives times are shown in Figure 10. The primary goal is to align the central line of Frame 1 and 2 to the central line of Frame 3 and 4. A central line as shown in Table 1 is half of the Delta time between the two consecutive frames.

ClearSi	ght Issues Probl	erma Decode	Reports			
0, 6	- 7 🔳 🔾 🕉	France: 4/242	8 Filter User Selected			
No.	Shakut	Sec. Addr	Det Astr	Len	Protocol	Simmary
11	(Seg Segarat2)	71,243,120,26	67.151.116.195	118	8002	MGCP, Command, MTPY 25231361 1507 18(192.168.0.115) M
12	(Seg Segment2)	67.151.116.195	71.243.120.26	64	8009	MGCP, Response, 200 25231361 CK
227	[Seg Segment1]	192.168.0.115	67.151.116.195	118	20029	MGCP, Command, MTFT 25231361 15WT 18(192.168.0.115) M
28	(Sep Sementi)	67, 151, 116, 195	192,168,0,115	60	MOCP	MGCP, Remonse, 200 25231361 GK





Figure 8: Save Filtered Packets

Hor	10	filter-4-frames	Lade 22								
Cle	urSight	Issues	Problems	Decode	Reports						
Q	ş.	V 🖬 🔇	33 1	Frames: 4 Fil	ter: None						
	Nb.	Status		Src. Add	Dat. Addr	Len	Protocol	Summary	Rol. Tene	Della Time	Abs. Time
	r.	Seg Tegment2]	.# 71.	243.120.26	67.151.116.195	118	MOCP	MOCP, Cosm	0.000000000	0.000000000	2008-05-07 08+54
22	t	Seg Segment2]	67.	151.116.195	71.243.120.26	64	MOCP	MOCP, Resp	0.004556000	0.004556008	2008-05-07 08:54
3	C	Seg Segment1]	193	2.168.0.115	67.151.116.195	110	MOCP	MOCP, Comm	8.990182000	8.985626008	2008-05-07 08:55
14	t	Seg Segment1]	67.	151.116.195	192.168.0.115	60	MOCP	MOCP, Resp	9.024793000	0.034611000	2008-05-07 08:55

Figure 9: Filter-4-frames.adc

### Calculate time offset

First, we align frame 1 to the t3 as shown in Figure 11. To align the central lines, we need to offset segment 2 by t6 - t5 =  $\Delta$ t4/2 -  $\Delta$ t2/2 (see Figure 12). Therefore, the correct time offset time to adjust Segment 2 to Segment 1 should be:

 $t = t3 + (\Delta t4 - \Delta t2) / 2 = 8.990182 + (0.034611 - 0.004556)/2 = 9.0052095$ 

	Relative Time (sec)	Delta Time (sec)
Frame No. 1	t1 = 0	∆t1 = 0
Frame No. 2	t2 = 0.004556	$\Delta t2 = t2 - t1 = 0.004556$
Frame No. 3	t3 = 8.990182	Δt3 = t3-t2 = 8.985626
Frame No. 4	t4 = 9.024793	Δt4 = t4-t3 = 0.034611
Central line of No.1 and No.2	t5 = Δt2 / 2	
Central line of No.3 and No.4	t6 = Δt4 / 2	

Table 1: Timing relationship between frames in trace files



Figure 10: Original Four Filtered Frames



Figure 11: Move Segment 2 to t3 (Step 1)







### Merge with the calculated time offset

Merge the original trace files again with the calculate time offset (see Figure 13). Then, we will get the new merged file shown in Figure 14.

(sec)
9.00520

Figure 13: File Merge with the Correct Time Offset



Figure 14: Merged Trace Files with Correct Offset

### **Summary**

This application note has shown how to use file merge function by ClearSight Analyzer. How to merge trace files is explained step by step in this application note. Moreover, how to calculate time offset is discussed in this note and example on how to merge trace files is described in detail.

Readers are encouraged to extend the basic methodology in this paper to include additional file merge features such as combined VoIP flows, non-VoIP applications and other multi-segment functions.

Contact your nearest Fluke Networks Engineer to help you extend the methodology in this paper to help you to get the most benefit out of your ClearSight Analyzer and file merge functions.

> Fluke Networks P.O. Box 777, Everett, WA USA 98206-0777

Fluke Networks operates in more than 50 countries worldwide. To find your local office contact details, go to www.flukenetworks.com/contact.

Contact Fluke Networks: Phone 800-283-5853 (US/Canada) or Email: info@flukenetworks.com. ©2010 Fluke Corporation. All rights reserved. Printed in U.S.A. 06/2010 3790785A D-ENG-N