Advantech AE Technical Share Document

Date	2015/04/28	SR#	1-2040686313							
Category	□FAQ ■SOP	FAQ SOP Related OS N/A								
Abstract	ADAM-60XX and ADAM-6	ADAM-60XX and ADAM-62XX_How to use Wireshark to collect the packet								
Keyword	ADAM-6K, ADAM-62XX, Wireshark, Collect packet									
Related										
Product	ADAM-6K, ADAM-62XX and ADAM-5000(L)/TCP									

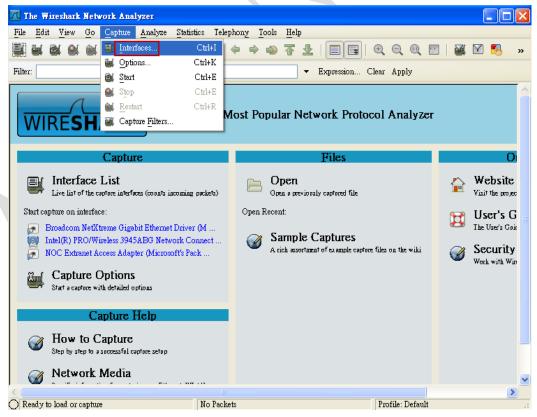
Problem Description:

This documentation shows how to use third-party software Wireshark to collect the Ethernet packet.

Brief Solution - Step by Step:

[Steps]

Step1: Launch WireShark, click "Capture" and then select "Interface ..."



<u>Step2</u>: Select "Options" to set up the conditions for packet capturing.

Wireshark: Capture Interfaces						
	Description		IP	Packets	Packets/s	Stop
🔊 Realtek 10/100/1000 Ethemet NIC		(Microsoft's Packet Scheduler)	172.18.2.21	130	6	Start Options Details
Help						Close

<u>Step3</u>: Change "Buffer Size" to adjust the temporary storage space for Ethereal Packets.

Capture Interface: Local 🗸	Realtek 10/100/1000 Ethen	net NIC (Microsoft's
IP address: 172.18.2.21		·····
	met 🔽	Wireless Settings
Capture packets in promisc	uous mode	Remote Settings
Capture packets in pcap-ng	format (experimental)	Buffer size: 1300 🗘 megabyte(s)
Limit each packet to 1	🗘 bytes	
Capture Filter:		
Capture File(s)		Display Options
File:	Browse	Update list of packets in real time
🔲 Use multiple files		
✓ Next file every 1	megabyte(s)	Automatic scrolling in live capture
Next file every 1	minute (s)	✓ Hide capture info dialog
Ring buffer with 2	🗘 files	Name Resolution
Stop capture after 1	🗘 file(s)	
Stop Capture		Enable MAC name resolution
after 1	packet(s)	Enable network name resolution
after 1	megabyte(s)	Enable transport name resolution
after 1	minute(s)	
Help		Start Cancel

AD\ANTECH

Enabling an Intelligent Planet

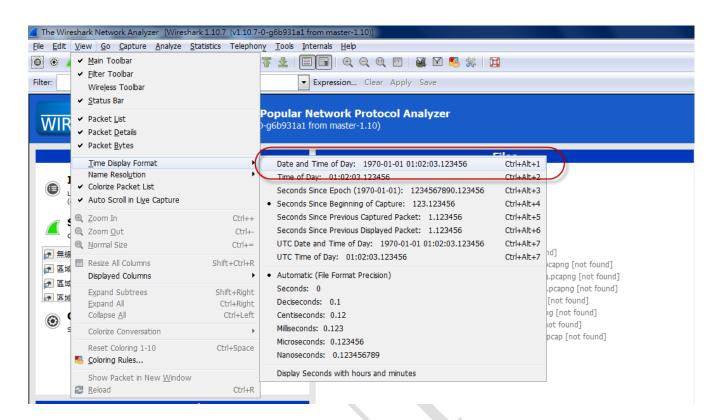
<u>Step4</u>: Select "Use multiple files" to set up conditions for file saving.

📶 Wireshark: Capture Options	
Capture	
Interface: Local 🗸 Realtek 10/100/1000 Ethernet	NIC (Microsoft's 💌
IP address: 172.18.2.21	
Link-layer header type: Ethernet 💌	Wireless Settings
Capture packets in promiscuous mode	Remote Settings
Capture packets in pcap-ng format (experimental)	Buffer size: 300 🛟 megabyte(s)
Limit each packet to 1 🗘 bytes	
Capture Filter:	•
Capture File(s)	Display Options
File: Browse	✓ Update list of packets in real time
☑ Use multiple files	
Next file every 1 megabyte(s)	Automatic scrolling in live capture
✓ Next file every 1	✓ Hide capture info dialog
✓ Ring buffer with 20	Name Resolution
Stop capture after 1 file(s)	
Stop Capture	Enable MAC name resolution
🔲 after 🚺 🗘 packet(s)	Enable network name resolution
🗌 after 🛛 1 💭 megabyte(s) 🗸 🗸	
🔲 after 1 🔅 minute (s) 🗸	Enable transport name resolution
Help	Start Cancel
litte	Caller

Next file every 1 day is to save Ethereal file after one day of capturing.

Ring buffer with 20 files means Wireshark will only hold last 20 files at a time.

<u>Step5</u>: Select "Date and Time of Day" as the data format.



AD\ANTECH

Enabling an Intelligent Planet

<u>Step6</u>: Click "Start" to begin capturing packet

Capture			
Interface: Local	~	Realtek 10/100/1000 Et	hemet NIC (Microsoft's 💌
IP address: 172.18.2.	21		
Link-layer header typ	e: Ether	met 💌	Wireless Settings
Capture packets i	n promiscu	aous mode	Remote Settings
Capture packets i		format (experimental)	Buffer size: 300 🗢 megabyte(s)
Capture Filter:			•
Capture File(s)			Display Options
Tal.			
File:		Bro	wse Update list of packets in real time
 ✓ Use multiple files 		Bro	
	1	(Brown) (Brown	Image: Wideling of the second seco
Use multiple files	1		Automatic scrolling in live capture
Use multiple files Next file every	1	🗘 megabyte(s)	Automatic scrolling in live capture Hide capture info dialog
 ✓ Use multiple files Next file every ✓ Next file every 	1 1 20	 megabyte(s) day(s) 	Automatic scrolling in live capture Hide capture info dialog Name Resolution
 Use multiple files Next file every Next file every Ring buffer with 	1 1 20	<pre> megabyte(s) day(s) files </pre>	Automatic scrolling in live capture Hide capture info dialog
 Use multiple files Next file every Next file every Ring buffer with Stop capture after 	1 1 20	<pre> megabyte(s) day(s) files </pre>	Automatic scrolling in live capture Hide capture info dialog Name Resolution
 Use multiple files Next file every Next file every Ring buffer with Stop capture after Stop Capture 	1 1 20	 me gabyte (s) day(s) files file (s) 	Automatic scrolling in live capture Hide capture info dialog Name Resolution Enable MAC name resolution

Step7: Communication packets are captured and shown on the screen

1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2	5 2.82 6 3.14 7 3.29 8 4.03 9 5.35 0 5.41 1 5.41	2074 2461 2527 4026 4047 8835 9620 3373 6123 4507 5867 2425				Source 1/2. 172. 172. 172. 172. 172. BayN BayN 172. 172.	18.2 20.1 18.2 20.1 20.1 18.2 etwo 18.2 20.1 etwo	.43 .233 .233 .233 .43 _6e:e _6e:e .43 .233	ec:71		Destination 1/2.20.: 172.18. 172.18. 172.18. 172.20.: Bay-Net Bay-Net 172.20.: 172.18. 172.20.: 172.18.	Clear Appl 1.233 2.43 1.233 2.43 1.233 works-(: 1.233	Synopti	Protocol DCERPC DCERPC DCERPC DCERPC DCERPC TCP SONMP	Info Rec Res Res Res Sol Sol Sol
No 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2	8 2.14 9 2.14 0 2.14 1 2.14 2 2.14 3 2.14 4 2.82 5 2.82 6 3.14 7 3.29 8 4.03 9 5.35 0 5.41 1 5.41	2074 2461 2527 4026 4047 8835 9620 3373 6123 4507 5867 2425				172. 172. 172. 172. 172. BayN BayN 172. 172. BayN	18.2 20.1 18.2 20.1 20.1 18.2 etwo 18.2 20.1 etwo 20.1	.233 .43 .233 .43 .6e:e .6e:e .43 .233			Destination 1/2.20.: 172.18. 172.18. 172.18. 172.18. 172.20.: Bay-Net Bay-Net 172.20.:	1.233 2.43 1.233 2.43 2.43 1.233 works-(: works-(: 1.233	Synopti	DCERPC DCERPC DCERPC DCERPC TCP SONMP SONMP DCERPC	Rec Rec Rec Rec Sol Sol Rec
1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2	8 2.14 9 2.14 0 2.14 1 2.14 2 2.14 3 2.14 4 2.82 5 2.82 6 3.14 7 3.29 8 4.03 9 5.35 0 5.41 1 5.41	2074 2461 2527 4026 4047 8835 9620 3373 6123 4507 5867 2425				172. 172. 172. 172. 172. BayN BayN 172. 172. BayN	18.2 20.1 18.2 20.1 20.1 18.2 etwo 18.2 20.1 etwo 20.1	.233 .43 .233 .43 .6e:e .6e:e .43 .233			1/2.20. 172.18. 172.20. 172.18. 172.18. 172.20. Bay-Net Bay-Net 172.20.	2.43 1.233 2.43 2.43 1.233 works-(works-(1.233		DCERPC DCERPC DCERPC DCERPC TCP SONMP SONMP DCERPC	Rec Rec Rec Rec Sol Sol Rec
1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2	9 2.14 0 2.14 1 2.14 2 2.14 3 2.14 4 2.82 5 2.82 6 3.14 7 3.29 8 4.03 9 5.35 0 5.41 1 5.41	2074 2461 2527 4026 4047 8835 9620 3373 6123 4507 5867 2425				172. 172. 172. 172. BayN BayN 172. 172. BayN	20.1 18.2 20.1 20.1 18.2 etwo etwo 18.2 20.1 etwo	.233 .43 .233 .43 .6e:e .6e:e .43 .233			172.18. 172.20. 172.18. 172.18. 172.20. Bay-Net Bay-Net 172.20.	2.43 1.233 2.43 2.43 1.233 works-(works-(1.233		DCERPC DCERPC DCERPC TCP SONMP SONMP DCERPC	Res Res Res pc Sof Sof Res
1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 2	0 2.14 1 2.14 2 2.14 3 2.14 4 2.82 5 2.82 6 3.14 7 3.29 8 4.03 9 5.35 0 5.41 1 5.41	2461 2527 4026 4047 8835 9620 3373 6123 4507 5867 2425				172. 172. 172. BayN BayN 172. 172. BayN	18.2 20.1 20.1 18.2 etwo etwo 18.2 20.1 etwo	.43 .233 .43 _6e:e _6e:e .43 .233			172.20. 172.18. 172.18. 172.20. Bay-Net Bay-Net 172.20.	1.233 2.43 2.43 1.233 works-(works-(1.233		DCERPC DCERPC TCP SONMP SONMP DCERPC	Rec Res pc Sof Sof Rec
1: 1 1 1 1 1 2 2: 2 2 2	1 2.14 2 2.14 3 2.14 4 2.82 5 2.82 6 3.14 7 3.29 8 4.03 9 5.35 0 5.41 1 5.41	2527 4026 4047 8835 9620 3373 6123 4507 5867 2425				172. 172. BayN BayN 172. 172. BayN	20.1 20.1 18.2 etwo etwo 18.2 20.1 etwo	233 233 43 6e:e 6e:e 43 233			172.18. 172.18. 172.20. Bay-Net Bay-Net 172.20.	2.43 2.43 1.233 works-(: works-(: 1.233		DCERPC DCERPC TCP SONMP SONMP DCERPC	Re: Re: pc Sof Sof Rei
1 1 1 1 1 1 2 2 2 2 2 2	2 2.14 3 2.14 4 2.82 5 2.82 6 3.14 7 3.29 8 4.03 9 5.35 0 5.41 1 5.41	4026 4047 8835 9620 3373 6123 4507 5867 2425				172. 172. BayN BayN 172. 172. BayN	20.1 18.2 etwo etwo 18.2 20.1 etwo	.233 .43 _6e:e _6e:e .43 .233			172.18. 172.20. Bay-Net Bay-Net 172.20.	2.43 1.233 works-(: works-(: 1.233		DCERPC TCP SONMP SONMP DCERPC	Re: pc Sof Sof Re(
1 1 1 1 1 2 2 2 2 2	3 2.14 4 2.82 5 2.82 6 3.14 7 3.29 8 4.03 9 5.35 0 5.41 1 5.41	4047 8835 9620 3373 6123 4507 5867 2425				172. BayN BayN 172. 172. BayN	18.2 etwo etwo 18.2 20.1 etwo	.43 _6e:e _6e:e .43 .233			172.20. Bay-Net Bay-Net 172.20.	1.233 works-(: works-(: 1.233		TCP SONMP SONMP DCERPC	pc 501 501 Re(
1, 1 1 1 2 2 2 2 2	4 2.82 5 2.82 6 3.14 7 3.29 8 4.03 9 5.35 0 5.41 1 5.41	8835 9620 3373 6123 4507 5867 2425				BayN BayN 172. 172. BayN	etwo etwo 18.2 20.1 etwo	_6e:e _6e:e .43 .233			Bay-Net Bay-Net 172.20.	works-(: works-(: 1.233		SONMP SONMP DCERPC	501 501 Re(
1 1 1 2 2 2 2 2	5 2.82 6 3.14 7 3.29 8 4.03 9 5.35 0 5.41 1 5.41	9620 3373 6123 4507 5867 2425				BaýN 172. 172. BayN	etwo 18.2 20.1 etwo	_6e:e .43 .233			Bay-Net 172.20.3	works-(: 1.233		SONMP DCERPC	SOI Re(
1 1 1 2 2: 2 2 2	6 3.14 7 3.29 8 4.03 9 5.35 0 5.41 1 5.41	3373 6123 4507 5867 2425				172. 172. BayN	18.2 20.1 etwo	.43 .233	ec:71		172.20.3	1.233	Synopti	DCERPC	Red
1 1 2 2 2 2 2	7 3.29 8 4.03 <mark>9 5.35</mark> 0 5.41 1 5.41	6123 4507 5867 2425				172. BayN	20.1 etwo	233							
1 2 2: 2: 2 2	8 4.03 9 5.35 0 5.41 1 5.41	4507 <mark>5867</mark> 2425				BayN	etwo.				172.18.	2 42		TCP	
1 2: 2: 2	<mark>9 5.35</mark> 0 5.41 1 5.41	5867 2425						6e:e							753
2:	0 5.41 1 5.41	2425				172			20:71	-	Spannin		(for-br		COL
2: 2 2	1 5.41										172.18.			BROWSER	
2							18.2				172.20.3			TCP	rki
2							20.1				172.18.			TCP	bla
	2 5.91						18.2				172.20.3			TCP	re
2.	3 5.91						20.1		-		172.18.		20 I	TCP	bla
	4 6.04	2716				BayN	etwo.	_6e:e	20:71	-	Spannin	g-tree-	(tor-br	STP	COL
															>
± Fram	e 1 (6	i0 byt	es on	wire,	60 byt	es c	aptu	red)							
± IEEE	802.3	Ethe	rnet												
± Logi															
± Span				.1											
≖ ⊃hau	ning i	iee P	TUCUCU												
000 0	01 80 (cZ 00	00 00	00 e0	7b 6	e ec	71 (0 26	42 4	42		. {n.q.&	\$BB		
	03 00 0			80 00				d bo				{P			
020 0	00 1d 8	30 00	00 e0	7b 6e				01 01				n .q			
030 0	02 00 0			00 00	00 0	0 OŌ	00								

<u>Step8</u>: Move to "Capture" and choose "Stop" to terminate the monitoring

ile <u>F</u>	Edit J	View	Go	Cap	ture 🧧	nalyz	ze <u>S</u>	tatistic	s T	eleph	ony	T	ools	He	lp												
	1		i	Ð	Interfac	:es		(Ctrl+I			¢		T	⊉				Ð	Q	11	**	Ň	¥ 🗹		>	>
			_	١.	Options			С	trl+K	E					1	_		_									
Filter:				8	Start			0	trl+E	L					•	Ex	pression	C	lear	App	ly						
No	T	lime		9	Stop			C	trl+E	se							Destina	tion					Pro	tocol	Ir	nfo	^
11	L48 9	95.67	898	ŝ	Restart			C	trl+R	.1	8.2	2.4	3				172.2	20.1		1			TC	P	Ť	10	
	L49 9		353		-				unix			2.4					172.2						TC			ТC	
	L50 9				Capture	e Filte	rs					1.1					172.1						TC			ТC	
	L51 9					_	_	_		s co,							CDP/\								-	ev	
	L52 9													:c:7	1		Spanr					or-b				on	
	L53 9									2.1							255.2		25				UD			ou	
		98.57								2.1								255.	25	5.25			UD			ou	
	L55 9									2.1							255.2						UD			ou	
	L56 9									2.1				_			255.2						UD			ou	
	L57 9													:c:7			Spann									on	
	L58 1													<:7			Spann									on	
	L59 1													c:7	1		Spann				-(T)	or-p				on	
	L60 1									2.1							172.2						TC			TC	
	161 1									2.2				7	-1		172.1				(TC			TC	
	L62 1 L63 1													:C:7			Bay-N									ON	
	L63 I L64 1													c:7			Bay-N Spann									ON a	
LL	104 1	.05.0	318/						Bd	уме	u wu	1_0	e:e	:c:7	T		Sparin	nng	9- U	ree-	-(1)	ur-n	r. 51	Р		on	\geq
																										>	
🗄 Fra	ame 1	L (60) byt	:es	on v	vire	e, 6	0 by	/tes	ca	pti	ure	ed)														
+ IEE	EE 80)2.3	Ethe	ern	et																						
± Loc	gical	l-Lir	ik ca	ont	rol																						
+ Spa	-					1																					
- ope		'g ''																									
																						-					
0000		80 c							6e (42				• • •		۰, ď.							
010 020) 00) e0				e0) 71 (· · ·		.{P.							
020					fa =				00 (0T	UT.	14	00			.{r		9	• • •						
030	V2	00 0			ιd	00	~~	00	00 (20						• • • • •	•••	• •	•••							
							-										-	_	-								
		UL 137 L	man Chi.	mhit	t Ethern	at Dwi	ver A	A	Packa	to: 11	64 I	Diopl	hered	· 116	A Ma	rbad	• El		1 Pm	ofile:	Defe	the					

<u>Step9</u>: Go to "File" and select "Save" to save data into a file. After that, please send the file to us for further analysis.

Dpen Open Re		<u>Capture</u> Ctrl+	Analyze	Statisti		•	þ	<u>T</u> oo =	2	_	l [Ð,		0, 🖻	3	¥ 🗹	•	
Merge										•	Ex	pression	ь С	lear	Apply					
💥 <u>C</u> lose		Ctrl+1	₩		Sou	urce					1	Destina	tion				F	rotocol	I	nfo
ave 🖥		Ctrl+	S				.68.	1.10)			255.	255.	255	. 255		L	JDP	S	Jou
					19	2.1	.68.	1.10	2			255.3	255.	255	.255		L L	JDP	5	sou
\overline 🚮 Save <u>A</u> s.		Shift+Ctrl+	15					1.10)			255.3						JDP		sou
File Set								.44				255.3						JDP		Sou
THE SET			- L					_6e:							ee-(for-l				on
Export			- H								8:2	ff02				from 1		HCPV6		50]
					Baj	yne	TWC	_6e:	:ec:	110	0.2	5pani ff02	nnng	-tr	ee-(for-l		STP DHCPV6	-	ion
📇 Print		Ctrl+	-P					6e:			0:2					for-l				or Ior
			_					_6e;										SONMP		SON
🐔 Quit		Ctrl+	Q					_0e; _6e;										SONMP		SON SON
1424	185.6396	17	_					_6e:				Span	nina	-tr	ee-(for-l	hr 9	STP		ion
	185.8799							.43				172.						ICP		TC
	185.8810							.100)			172.						TCP		ΤC
1427 :	186.0571	.37			fe	80:	:f0	84:0	:94	428	8:2	ff02	::1:	2				HCPV6	S	501
	187.6507							_6e:		71						for-l				on
1429 :	189.1519	43			19	2.1	.68.	1.10)			255.3	255.	255	.255		. U	JDP	S	Sou
<																				>
											-	_	_	_	_		_		_	-
🗄 Frame			wire,	60 b	ytes	Ca	apti	ur edj)											
∃ IEEE 8																				
🗄 Logica	l-Link ⊂	iontrol																		
🗄 Spanni	ng Tree	Protoco	1																	
	-																			
0000 01	80 c2 00	0 00 00	00.00	7b	6e (20	71	00.7	6.4	<u>э</u> и	2			In	.q.&	.00				
					e0 7										.ч.∝ {р					
	1d 80 00				71 8								.{n	.a						
		0 ff fa			00 0						-			1						

ADVANTECH Enabling

Enabling an Intelligent Planet

<u>Step 10</u>: To save files with corresponding date and time by selecting "Browse"

📶 Wireshark: Capture Options 📃 🗖 🗙
Capture
Interface: Local 🗸 Realtek 10/100/1000 Ethemet NIC (Microsoft's 💌
IP address: 172.18.2.21
Link-layer header type: Ethemet 🗸 Wireless Settings
Capture packets in promiscuous mode Remote Settings
Capture packets in pcap-ng format (experimental) Buffer size: 300 🔅 megabyte(s)
Limit each packet to 1 bytes
Capture Filter: not tcp port 3389
Capture File(s) Display Options
File: Update list of packets in real time
✓ Use multiple files
Next file every 1 C megabyte(s) Automatic scrolling in live capture
V Next file every 1 day(s) V Hide capture info dialog
Ring buffer with . 20 C files
Stop capture after 1 C file (s)
Stop Capture
after 1 packet(s) Enable network name resolution
after 1 🗘 megabyte(s) 🗸
after 1 1 minute (s) Enable transport name resolution
Help Start Cancel

Step 11: Assign a file name and directory to save the files

🗖 Wireshark:	Specify a Capture File 🛛 🗙
Name:	test
Save in folder:	🖻 My Documents 💽
🗄 Browse for (ther folders
	OK Cancel

AD\ANTECH

Enabling an Intelligent Planet

Step 12: Click "Start" to start capturing packets

Capture -						
Interface:	Local	~ R	ealtek 10/100/1000 Ethe	met NIC	(Mic	rosoft's 💌
IP address	172.18.2.21					
Link-laye	r header type:	Etheme	t 🔽	W	ireless Settings	
Captu	ue packets in p	romiscuo	us mode	Re	mote Settings	
-	ue packets in p each packet to		rmat (experimental)	Buffer size:	300 🗘	megabyte(s)
Capture	Filter: not to	p port 33	89			
Capture Fi	le (s)			Display Opt	tions	
File: an	d Settings\peter	.kuoMy	Documents/test Brow	98 🔽 Update	list of packets	in real time
🗸 Use m	ultiple files				-	
Next i	file every 1	2	me gabyte (s)	Autom	atic scrolling in	a live capture
V Next i	file every 1		🗘 day(s)	V Hide o	apture info dial	og
Ring	buffer with	20	🗘 files	Name Reso	hation	
Stop o	apture after 1		C file(s)			
Stop Captu	ure			Enable	MAC name re	solution
	r 1		pecket(s)	Enable	network name	resolution
🗌 afte			me gabyte(s)			
… eft	r 1		See and the Part of the See		transport name	

Step 13: Files will be saved with data and time on the filename

Year 2011 Month 11 Date 25 Time 17:34:01

1322_D1.83_BFC0C9C9	7,668 KB
1322_D1.83_BFD6F8AF	7,668 KB
🐴 ACP Exam - 20110919-1	1,810 KB
➡CSRC架構圖	47 KB
🔁 Doc1 Comm - ICOM Card vs Serial Device	396 KB
🔁 EKI-1222-assy-wall-mount_10252011 M	67 KB
🔁 EKI-1351_1352_Manual_Ed2	4,120 KB
🔁 EKI-6311G_Manual_v1.0_090105	1,944 KB
🔁 EKI-6311GN901T_String_Table_20110831	195 KB
EKI-6311GN901T_String_Table_20111011	194 KB
🔁 eLearning - Giving Scores	937 KB
🛀 important question (6)	1,337 KB
🔁 SYS.CONFIG	81 KB
📷 test_00010_20111125173431	3 KB
📷 test_00011_20111125173441	2 KB
📷 test_00012_20111125173451	3 KB
📾 test_00013_20111125173501	3 KB
atest_00014_20111125173511	1 KB