February 6, 2012 Development Center of AthTek Software

We have just released new versions of <u>AthTek NetWalk</u>, with many new features included. You can now download AthTek NetWalk Free Trial Edition to try the new features yourself, and you will find AthTek NetWalk has greatly enhanced its <u>packet analyzing</u> functions for easily troubleshooting.

Download Free Home Edition V2.2.42

What's new?

1. Support to capture up to 8G trace file.

In the previous versions, AthTek NetWalk can open up to 4GB packet files, but only capture 256MB packet files. With AthTek NetWalk v2.2.42, users are allowed to capture up to 8GB packet files in one time! This means even you leave AthTek NetWalk to **capture packets** for a long time, it still will be a single large complete trace file.

2. Enhance the event trigger.

Now you can set it to be time-based trigger, filter-based trigger and event-based trigger. This means you can make AthTek NetWalk to be intelligent in <u>network monitoring</u> and **packet capturing**. You can set the packet capturing length, or set the packet filter for capturing, or even to set it

based on event types.

pture Options						
General Trigger						
Time Based						
Start Trigger						
9:00:00	V	Use data also	2012/ 2/ 7	 		
Stop Trigger						
17:00:00 🚖		Use data also	2012/ 2/ 7	* *		
Filter Based						
Start Trigger: Remo	ve Multi	cast				
Start nigger. Remo	ve Mala	cast				
Stop Trigger: Remo	ve DNS					
Event Based						
Start Trigger: 🚹 🚺	K	Stop Trigger:	+			
ICMP destination networ ICMP redirect	'k unknown	ICMP router ad ICMP network	unreachable			
Syn storm High physical utilization		ICMP destination unreachable ICMP router solicitation				
ARP too many replies wi	thout reque			-		
Repeat Trigger						
Repeat Trigger						

3. Show events in hosts, flows, application nodes and connection charts for easier troubleshooting.

In the new version, we add several flags to show the event levels of all the network communications. For example, green stands for informational events; yellow stands for minor events; orange stands for major events; red stands for severe events. This will greatly help in fast locate the suspicious connections

in troubleshooting.

		Cler	t	Server Tot	al Bytes	Events	Duration
192.193.204	001 <> 192.168.68.45/1414	192.193.204	1 192.16	8.68.45	260,924	0	00:00:1
10.205.32. 47 <> 23.230/5000 10.204.16. 1 <> 10.105/55308 10.204.16. 0 <> 6.43/4242 64.157.238 449 <> 154.23/7280 10.200.10. 14 <> 17.166/4001 10.200.10. 15 <> 17.213/5001		10.005.32.13	3 15.128	23.230	806	0	00:00:1
		10.304.16.22	10.200	10.200. 10.20 172.32.		0	00:00:17 00:00:17 00:00:01 00:00:00 00:00:00
		10.204.16.12	4 10.2			0	
		64.157.238.1	4 172.32			1	
		10.200.10.10	0 10.204	17.066	130 0		
		10.200.10.10	0 10.204	10.204.17.213		130 0	
10.201.131	655 <> 170 27.77/2301	10 301 131 23	1 172.27	207.77	1,198	0	00:00:1
10.207, 174 $6263 < 40.11.68/1530$ 10.200, 10. $14 < ->$ 17.166/4001 10.205, 32. $49 < ->$ 12.3.230/5000 172, 32, 54. $81 < -> 6$ 238.150/15001 10.200, 10. $15 < ->$ 17.213/5001 172, 21, 252 301 $< ->$ 1.31.135/2763 10.201, 131 579 $< ->$.30.241/2301 172, 27, 34. 01 $< ->$ 131.135/2807 10.201, 131 833 $< ->$.95.99/2301 10.200, 10. 17 $< ->$ 17.166/4001 10.201, 131 311 $< ->$ 5.195.200/2301		10.307.174.2	6 140.24	140.240 10.204. 15.128.2 64.157.23		3	00:00:0
		10, 200, 10, 10	0 10.204			0	00:00:0
		10.205,32,12	5 15.128			0	00:00:1
		170.12.54.23	64.157.2			0	
		10. 200. 10. 10	0 10.204	17.213	2,011 0	0	00:00:0
		1 252.16	1 10.201.1	10.201.13 172.26.3 10.201.13 172.27.		0	0 00:00:
		10 201 131.23	1 172.26			0	
		170.27,34.21				0	
		10 200 131.13	8 172.2			0	00:00:0
		10, 200, 10, 10	0 10.204			0	00:00:0
		10.201.131.15		172.25.195.200	130 0 634 0	0	00:00:0
tistics Conne	ction Chart Events						
Length	10.207.174.216	140.240.11.68	Delta Time	Rel. Time		Abs. Time	1
			Delta Time 0.000000000	Rel. Time	2008-0	Abs. Time 4-02 07:54:5	
Length	10.207.174.216	2499 Win=2144 Len=0 MSS					9.1673700
Length 81 60	10.207.174.216 16263 > 1530 (97N) Sec-2339 1530 > 16383 (57N, ACK) Sec- 1530 > 16263 (57N, ACK) Sec-	2499 Win=2144 Len=0 MSS	0.000000000	0.000000000	2008-0	4-02 07:54:5	9, 167370 9, 199434
Length 81 60 08 60 99 60	10.207.174.216 16263 > 1530 (97N) Sec-2339 1530 > 16383 (57N, ACK) Sec- 1530 > 16263 (57N, ACK) Sec-	2499 Win=2144 Len=0 MSS 1736634960 Ack=23392500 1738834960 Ack=23392500 Asmission	0.000000000	0.000000000	2008-0	4-02 07:54:5 4-02 07:54:5	9.167370 9.199434 9.694249
Length 81 60 28 60 99 60 24 60	10.207.174.216 16263 > 1530 [Smi] Seq=2330 1530 > 16263 [Smi, ACK] Seq= 1530 > 16263 [Smi, ACK] Seq= 16263 > 1530 [ACK] Seq=2330	2499 Win=2144 Len=0 MSS 1736634960 Ack=23392500 1738834960 Ack=23392500 Asmission	0.000000000	0.00000000 0.032064000 0.526879000	2008-0 2008-0 2008-0	4-02 07:54:5 4-02 07:54:5 4-02 07:54:5	9. 1673700 9. 1994340 9. 6942490 9. 8858890
Length 81 60 28 60 99 60 24 60	10.207.174.216 16263 > 1530 (SYN) Sec-2330 1530 > 16263 (SYN, ACK) Sec- 1530 > 16263 (SYN, ACK) Sec- 16263 > 1530 (ACK) Sec- 16263 > 1530 (PSH, ACK) Sec-	2499 Win=2144 Len=0 MSS 1739834960 Ack=23392500 1738834960 Ack=23392500 1738834960 Ack=1738834961 Win=	0.000000000 0.032064000 0.494815000 0.191640000	0.000000000 0.032064000 0.526879000 0.718519000	2008-0 2008-0 2008-0 2008-0	4-02 07:54:5 4-02 07:54:5 4-02 07:54:5 4-02 07:54:5	9. 1673700 9. 1994340 9. 6942490 9. 8858890 0. 9260 160

4. Add an advanced event tab.

Besides the Statistic Event and Packet Tab, we add a new Advanced Tab in AthTek NetWalk v2.2.42. The Advanced Tab is set for analyzing some complex and typical events. It will synthesize various <u>packet sniffing</u> results and recalculate the relations between each traffic nodes. Finally it will tell you which part is safe and which other is suspicious.

🕒 Event	Manager			
: 🛨 -	📝 🚍 🗶 🖪 🖪 🖂 🗞 I	Q Search	🛞 🔞	
19 Stat	istic Events	Advanced Eve	ents	
Enabled	Name	Severity	Layer	Action
V	DNS No Such Name	Informational	Application Layer	Global Action
1	DNS Format Error	🥚 Minor 🔪 🖊	Application Laver	Global Action
V	DNS Slow Response	S Minor Crea	ate Packet Event	
V	DNS Server Failure	\varTheta Major		1
~	DNS Not Implemented	Informa G	eneral	
2	DNS Refused	😑 Minor	Name: Untitled event	
1	DNS Not Authoritative	😑 Minor		
1	DNS Name Out Of Zone	🔵 Informa 🛛 S	everity: 🕒 Information	nal 👻 Belongs to: Application Layer 👻
1	HTTP Bad Request	😑 Minor		
1	HTTP Unauthorized	Severe	Action: Global Action	▼ [Please set an action.]
V	HTTP Forbidden Access	😑 Major	-	
1	HTTP Page Not Found	🥚 Minor 🛛 🔾	ondition	
V	HTTP Method Not Allowed	🔵 Informa 🛛 ,	a a a 1	
1	HTTP Not Acceptable	🔵 Informa 🍐	🌯 • 🥵 • 🤧 🛛 🖉	
4	HTTP Proxy Authentication Required	😑 Minor	A	
1	HTTP Request Timeout	😑 Minor	Å	
1	HTTP Conflict	Severe	No Rule	
1	HTTP Length Required	😑 Minor	No Rule	
1	HTTP Request-URI Too Long	Severe		
1	HTTP Unsupported Media Type	Informa		•
1	HTTP Internal Server Error	Severe		
V	HTTP Not Implemented	😑 Major		
1	HTTP Bad Gateway	\varTheta Major		
1	HTTP Service Unavailable	\varTheta Major		
V	HTTP Gateway Timeout	\varTheta Major		
1	HTTP Version Not Supported	😑 Minor		
V	IP Checksum Error	\varTheta Major		
V	UDP Checksum Error	🥮 Major		OK Cancel Help
1	TCP Checksum Error	😑 Major 🧲	metomonopore cayer	
V	TCP Connection Slow Setup	Informational	Net&Transport Layer	Global Action
4	TCP Retransmission	\varTheta Major	Net&Transport Layer	Global Action

5. Upgrade Wireshark core program. Upgrade Wireshark from v1.6.1 to v1.6.5.