Wireshark Developer and User Conference

BI-8 Wireshark Software Case Studies

4:45p – 6:00p Mon June 25 2012

Megumi Takeshita Founder | ikeriri network service co., Itd.

SHARKFEST '12 UC Berkeley June 24-27, 2012

About Megumi Takeshita 竹下恵





- Founder, ikeriri network service co.,ltd ← Enterprize solution, nortel networks ←IS Bay Network
 - 10+ books about packet capturing, analysis, inspection, and consulting
 - Reseller of Riverbed Technology (former CACE technologies) and Metageek in Japan

Packet capturing Otaku (geek) from Ethereal, 1st Sharkfest !



before capturing

- Clear DNS C:¥>ipconfig /cleardns
- Stop firewalls, anti-spywares and others
- Stop service like UPnP(SSID), VPN and many

CONCEPTION 2015 2015 CONCEPTION AND Set TCP HF194152952 TCP HF194152952 TCP HF194152952 TCP HF194152952 TCP HF194152952	t ings¥takeshita>netsta 89:epnap HP1941520 89:aicrosoft ds. HP194 80:1064 HP1941529 89:3388 HP1941529 89:4444 HP1941529	t mall find "LISTEN" 200. Heriri, Localit LISTE 15295289, Keriri, Localit LISTE 289, Heriri, Localit LISTE 289, Heriri, Localit LISTE 289, Heriri, Localit LISTE	LING LISTENING UNG KING UNG
🗰 arskituszk			- 10
0:4Documents and Interface Statiut	Settings¥takeshita)netr ics Received	tat re Sent	
Bytes Thicast packets Nor-unicast packe Storen Discards Errors Unknown protocols	97344639 173391 ta 10690 0 0 92	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	
C: VDocuments and	Settings¥takoshita)aro		
Interface: 10.0.0 Internet Addres 10.0.0.1 10.0.0.5 10.0.0.6 10.0.0.10 10.0.0.104	.7 0.42 s Physical Address 00-10-db-41+30- 00-26-10-33-1a+ 00-16-db-ad-06- 00-21-5a-db-0d- 00-21-5a-db-0d- 00-21-5d-db-67-	Type D dynamic 6 dynamic 8 dynamic 4 dynamic 8 dynamic	
C: Wocurents and	Settings¥takeshita)		

- C:¥>netstat –a | find
 "LISTEN" ; netstat –ab
- Check NIC error, discards
 C:¥>netstat –e



Setting Wireshark

- Adding Wireshark program path into system variable (set Path=%Path%;C:¥Pro...)
- Check interface index number (thark –D)
- Add columns according to the field catching up
- To see latency, add fields tcp.time_delta
- Set Time display format previous displayed packet





Fragment

• Original frame

	Ethernetll (14)	IP (20)	ICMP (8)	Mess 150	age)0
• Fragment 1/2 in Ethernet MTU					
	Ethernetll (14)	IP(20) DF=0 MF=1 オフセット=	ICMP (8)	Message 1472	
 Fragment 2/2 in Ethernet MTU 					
		EthernetII (14)	IP(20) DF=0 MF=0	ICMP (8)	Message 28



SHARKFEST '12 | UC Berkeley | June 24–27, 2012

オノセット=

Testing packet size

ICMP • ping host –I message size (MTU-28) -f

EthernetII	IP	ICMP	message
(14)	(20)	(8)	MTU=1500->1472
TCP			
EthernetII	IP	ТСР	Segment size
(14)	(20)	(20)	MSS=1460
UDP			
EthernetII	IP	UDP	Datagram size
(14)	(20)	(8)	MTU=1500->1472

- NTT East MTU 1454Bytes (MSS 1414)
- NTT West FTTH MTU 1438Bytes (MSS 1398)
- GRE + IPsec (transport mode)1440
- GRE + IPsec (tunneling mode)1420



Check negotiation of TCP

See first 2 packet of 3way handshake (初期ウインドウサイズはOS等で指定)

- Window Size, SACK, MSS, Window Scaling
- Some router may rewrite this section via NAPT
- Follow TCP stream and Use coloring and Ctrl+Space

EXTERNAL OFFICE AND ADDRESS OF THE OWNER.	C BRITAN AND A REAL AND A
In he pay is care been been been been been be	
tyn - tynus. Cie ber	
Incase Non Incase Non	
St. New News Destates Proved Mr.	6
10.000000 172 16 6 13.202 12.51.3 TCP rsom > http [SYM	1 Seg=0 w1n=64240
20.002444 202 with manage 6.6.13 TCP http > rsom [5YM	, ACK] Seg-O Ack-1 win-sour Len-D MSS-
30.000033 172 ++++++] Seg=1 Ack=1 Win=64240 Len=0
4 0.037035 172 2.51.3 HTTP POST /rms/mall/b	asket/vc HTTP/1.1 (application/x-www-
50.002904 202 http > rsom [ACH] Seg=1 Ack=1004 Win=7021 Len=0
	a second field book
Frame 1 (66 by	
Ethernet TT S M49File (0t Imi Ofile)	
Totarnat Broto In 16 6 13 (1	201 Kreant: image/if image/v. http://iii
The second secon	second se
ITANSMISSION CONCION PROTOCOLI, SIC POP	application/essord v/s
- 100 F	Referer: http://item.rakuten.co.ip/nigari612/andipg700creamer/
	Accept-Language: ja
a ten junde den	Content-Type: application/x-www-form-urlencoded
	UA-CPU: x86
	Accept-Encoding: gzip, deflate
	User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR
	1,1,4322; NET CLR 2.0.50727)
	Host: order.step.rakuten.co.jp
0000 00 14 22 1c a2 99 00 0b 97 94 9f 1e 08 00 45 00	Content-Length: 78
0010 00 34 ed 36 40 00 80 06 5e 01 ac 10 06 0d ca 48	4 Contection: Reeparive
0020 33 26 0b 49 00 50 05 46 9b 06 00 00 00 00 80 02	38. Caller Control: no Caller diade3008160971-10175. e sectores e sectores (2000/2000/2000/2000/2000/2000/2000/200
0030 Ta TO 18 b6 00 00 02 04 05 b4 01 03 03 00 01 01	+ · · · bil
0040 04 02	** Tel men land on the second se
	The fact that th
1) / a "Hiseddauballourandane" / Amet 2 Parket 2 Mole 1	

SHARKFEST '12 | UC Berkeley | June 24–27, 2012

Using iperf and tfgen (made in Japan)

- Throughput ->iperf
- Traffic ->tfgen

TiGes	Contraction of the local division of the loc	- 0 ×
Eile Option Help		14.0560200
Utilization(kbps) :	4	Start
Destination :	127.0.0.1	SER
Time To Live Port:	16 echo	p
Traffic Pattern	Continuous and constant	
Period to update	0	
Utilization		×
	[QK	
Input bandwidth	utilization in kbps. Qancel	
4		

Input destination IP address	Cancel
127.0.0.1	
Time To Live 16	
Time To Live 16 UDP Port © Default port(echo)	(User definable)

Continuous and constant	<u>O</u> K
Continuous and random	Cancel
⊂ Brust and periodical	-
⊂ Burst and random	
Period to update utilization	

Overview of troubleshoot

- If we know the error obviously, see defference from OK and NG packet to see packet in micro range (field)
- No idea of trouble capture packet at more than 2 location to see packet in macro range (statistics)
- Expert Info say many things automatically
- Think of packet lost -> Ignore (Ctrl+I)



Expertize IO graph

- To see errors and counting the number of packet, set Y axis to packet/sec (histogram)
- To see performance and throughput, set Y axis to bit/sec (line)

聖 Wareshark ID Graphs. 株式は接続グラフprag	
	E.
	型 Wreshart ID Graphs 机建筑组成为97.36-00 型图图
T_1	
0.0s 20s 40s 6.0s	800
1	<u></u> 50000
Orack Color Fitter Divis Line + Tek entered (3) oc.	
Grach 2 Coles Filter (top analysis and Jost present) Stole (Files + Processor Table)	
Grach 1 Film Transition destants and Style Film + Yew as time of day	
Gran + Cher File Inperiodestation Style File + Y Asia	0x 20x
Graph & Pater Top and an and all pater Top	Capto XAce
State Arts	Augen 1 Color Fyler Style Leve - Text interval 1 in:
Hele Gree See	Shan Galard Sale Film State Dea + Picelager tak
	thrush 3 - Fyher Stole Line - T Store as the of the
	Drigh 4 One Filter Shie Line Y Avie
	Grunt B and Fyher Boyle Lee Well BracTex
	State Arte
	DW GRV Ser

SHARKFEST '12 | UC Berkeley | June 24–27, 2012

No sampling, non-sampling

 In old days we use sampling technologies like SNMP, MRTG, and many flow analysis such as Cisco NetFlow, sFlow, iFlow





 But small packet (64 bytes – 100 bytes) may be ignored. Some small packet is important symptom of analysis (ARP / TCP SYN / HTTP GET and others)

Actual capture rate

- Typical Intel's GigaNIC (e1000), typical Dell PowerEdge2850 / Xeon 2.8GHz RAM 1GB (PC3200, DDR2, 400MHz)
- Threadshould is 140Mbps in Frame size = 64



Another frame size

- Frame size = 200, actual rate 400Mbps
- Frame size = 1500 , <u>may be ok</u>, no problem.





SHARKFEST '12 | UC Berkeley | June 24–27, 2012

Ooops in non-sampling

- In case of frame size is 1500, there may be some drops (it is not non-sampling)
- Actually, customer want to see most highest point of traffic, so if the pcap file do not contains all packet (some ignored) no use.
- Off course please order TurboCap from us (^^)





For non-sampling inspection

- MMMM packets received by the application NNNN packets accepted by the filter and dumped to disk ummm
- Optimise I/O access flow packet -> IRQ -> SVC -> driver -> OS
- Use 6 cores Xeon-L5640 and 24GB RAM ! (power resolve things and no page files)
- Stop tcpdump and create program using pcap libraries in C/C++
- Pcap -> standard output -> FIFO -> SQLite
- 3 month no problem SHARKFEST '12 | UC Berkeley | June 24–27, 2012



Thank you



SHARKFEST '12 | UC Berkeley | June 24–27, 201