Wireshark 分析機能入門

大量パケットの分析方法

hebikuzure



◎実践 パケット解析——Wiresharkを使った トラブルシューティング

- http://www.oreilly.co.jp/books/9784873113517/
- ISBN978-4-87311-351-7

インストール

公式サイトからダウンロードしてインス トールしましょう

http://www.wireshark.org/

Download Wireshark

Get Wireshark

The current stable release of Wireshark is 1.4.0. It supersedes all previous releases, including all releases of Ethereal. You can also download the latest development release (1.4.0rc2) and documentation.





◎最新バージョンを利用しましょう

- セキュリティ修正が含まれます
- 古いバージョンは攻撃対象になります

 現在の最新版は 1.6.1 (7/18 リリース)
 Windows 環境では同梱のWinPcap を利用 しましよう

WinPcapの注意事項

◎WinPcap 4.1 以降のバージョンでは NPF サービスが自動起動に設定されます

- [管理者として実行] しなくてもパケット キャプ チャができます
- 自動起動で問題がある場合は、以下のレジストリ キーで設定が変更できます
 HKLM¥SYSTEM¥CurrentControlSet¥services¥ NPF¥Start
 - 0x1 : SERVICE_SYSTEM_START
 - 0x2 : SERVICE_AUTO_START
 - 0x3 : SERVICE_DEMAND_START



• How To Set Up a Capture http://wiki.wireshark.org/CaptureSetup Security http://wiki.wireshark.org/Security OPlatform-Specific information about capture privileges http://wiki.wireshark.org/CaptureSetup/ CapturePrivileges

Wiresharkの分析機能

Expert Info Composite 機能
対話 (Conversations) 統計機能
終端 (Endpoint) 統計機能
IO Graph 機能

分析機能の利用

◎個々のパケットの解析の繰り返しでは抽出するのが困難な大量のデータ

特異パケットを自動抽出マクロ的分析データの可視化

キャプチャデータの概要表示

Statistics] – [Summary]

Wireshark: Summary - 0 X File Name: C:\Users\Murachi\Documents\Network Monitor 3\Captures\IE_Download.pcap Length: 54450311 bytes Wireshark/tcpdump/... - libpcap Format: Encapsulation: Ethernet Packet size limit: 65535 bytes Time 2011-07-16 21:25:08 First packet: Last packet: 2011-07-16 21:25:32 Elapsed: 00:00:23 Capture Interface: unknown Dropped packets: unknown Capture filter: unknown Display Display filter: none Ignored packets: 0 Traffic Captured Displayed Marked Packets 54203 54203 0 Between first and last packet 23.782 sec Avg. packets/sec 2279.131 Avg. packet size 988.562 bytes Bytes 53583039 Avg. bytes/sec 2253062.662 Avg. MBit/sec 18.025 Help Close

特異パケットの抽出

●Expert Info Composite 機能

○[Analyze] – [Expert Info Composite] または ここをクリック

0030 40 e6 c2 81 00 00 47 45 54 20 2f 6d 79 2e 6e 61 @....GE T /my.na 6d 65 3f 5f 3d 31 33 31 31 31 36 32 32 34 33 39 0040 me?_=131 11622439 33 34 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 34 HTTP/ 1.1.. Hos 0050 74 3a 20 62 2e 68 61 74 65 6e 61 2e 6e 65 2e 6a 0060 t: b.hat ena.ne.j 70 Od Oa 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 0070 p..Conne ction: ƙ eep-aliv e..x-Req 0080 65 65 70 2d 61 6c 69 76 65 0d 0a 58 2d 52 65 71 0090 75 65 73 74 65 64 2d 57 69 74 68 3a 20 58 4d 4c uested-W ith: XML 48 74 74 70 52 65 71 75 65 73 74 0d 0a 55 73 65 00a0 HttpRequ est..Use 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 r-Agent: Mozilla 00b0 2f 35 2e 30 20 28 57 69 20 36 2e 31 3b 20 57 4f 6e 64 6f /5.0 (Wi ndows NT 00c0 77 73 20 4e 54 ood0 57 36 34 29 20 41 70 70 6.1; WO W64) App 00e0 6c 65 57 65 62 4b 69 74 2f 35 33 34 2e 33 30 20 lewebKit /534.30 Intel(R) 82578DM Gigabit Network Conne... Packets: 1009 Displayed: 1009 Marked: 0

Expert Info Composite

◎特異情報があるパケットが分類されて表示 される

Wireshark: 2180 Expert Info	5		
Errors: 3 (1218) Warnings: 0 (0) Notes: 3 (23)	Chats: 266 (939) Details: 2180	
Group	Summary	 Count 	•
Checksum IPv4	Bad checksum		1197
🗄 Malformed GIF image	Malformed Packet	: (Exception occurred)	20
Malformed HTTP	Malformed Packet	: (Exception occurred)	1
Help			<u>C</u> lose

Expert Info Composite - $\mathbf{Error}\ \normalize{\mathcal{F}}\ \mathcal{T}$

◎不正パケット、チェックサム エラーなど

チェックサムエラーは Checksum Offload のためで、問題ない場合がほとんど

🗖 Wireshark: 2180 Expert Info	3		
Errors: 3 (1218) Warnings: 0	0) Notes: 3 (23) Chats: 266	5 (939) Details: 2180	
Group Protocol	Summary	 Count 	•
Checksum IPv4	Bad checksum		1197
🗉 Malformed GIF image	Malformed Packet (Excepti	ion occurred)	20
Malformed HTTP	Malformed Packet (Excepti	on occurred)	1
<u>H</u> elp			Close

チェックサムエラーの抑止(1)

- ●キャプチャ時、NIC の Checksum Offload を無効にする
 - ・基本的にネットワーク ドライバー側の設定
 - Windows なら[デバイス マネージャー] からネッ トワーク アダプターのプロパティーを開いて設定 できる

チェックサムエラーの抑止(2)

[Edit] – [Preference] – [Protocols] で [IPv4] (または [IPv6])の [Validate the IPv4 checksum if possible] を無効にする

🔀 Wireshark: Preferences - F	Profile: D	efault		
ARUBA_ERM	*	□ Internet Protocol Version 4		
ASN1		Decode IPv4 TOS field as DiffServ field:	\checkmark	
ATM		Reassemble fragmented IPv4 datagrams:		
ATMTCP	=			
ATP		Show IPv4 summary in protocol tree		
Banana		Validate the IPv4 checksum if possible:		
BAT		Support packet-capture from 1P TSO-enabled hardware.	V	
BATADV		Enable GeoIP lookups:		
BEEP				
BER		Interpret Reserved flag as Security flag (RFC 3514):		
BGP				

Expert Info Composite - Warnings タブ

●sequence number の不一致、Window サ イズの問題、fast retransmission など

Wireshark: 18976 Expert Inf	OS	
Errors: 3 (18283) Warnings: 5	(61) Notes: 129 (500) Chats: 32 (132) Details: 18976	
Group Protocol	Previous segment lost (common at car	14
	Window is full	2
	Fast retransmission (suspected)	6
	Out-Of-Order segment	38
	Zero window	1
Help		<u>C</u> lose

Expert Info Composite - $\operatorname{Notes} otin \mathcal{T}$

◎再送、重複 ACK、特異な TTL、アプリ ケーション レベルのエラーなど

Wireshark: 1	8976 Expert Inf	os				×
Errors: 3 (1828	33) Warnings: 5	(61) Notes: 129 (500)	Chats: 32 (132)	Details: 18976		
Group 📢	Protocol (Summary	4	Count	•	*
Sequence	ТСР	Duplicate ACK (#122)			1	
	ТСР	Duplicate ACK (#123)			1	
	тср	Duplicate ACK (#124)			1	
	тср	Duplicate ACK (#125)			1	
	тср	Duplicate ACK (#126)			1	
🗉 Sequence	IPv4	"Time To Live" only 4			2	
Packet:	54183	3			1	
Packet:	54195	5			1	Ŧ
<u>H</u> elp					Close	

Expert Info Composite - Chats タブ

●リクエスト/レスポンスごとに分類

🗖 Wireshark: 18976 Expert Inf	DS				23
Errors: 3 (18283) Warnings: 5	(61) Notes: 129 (500)	Chats: 32 (132)	Details: 18976		
Group (Protocol (Summary	•	Count	•	*
	GET /downloads/info.a	spx?na=41&Srcl	F	1	Ξ
	GET /dcs8kzhcc00000	ww68ffquzt0_6o5	5	1	
	GET /downloads/ja-jp/	/confirmation.asp	1	1	
	HTTP/1.1 302 Found¥	r¥n		1	
	Connection establish r	equest (SYN): se	2	7	
	HTTP/1.1 200 OK¥r¥n			22	
	Connection finish (FIN)		20	
	Connection establish a	cknowledge (SYI	1	8	Ŧ
Help				<u>C</u> lose	

●分析情報のあるすべてのパケットを表示

- Miresha	ırk: 18976 Expe	rt Infos		
Errors: 3	(18283) Warnir	ngs: 5 (61) Not	es: 129 (50	0) Chats: 32 (132) Details: 18976
No	 Severity 	Group Group	Protocol	Summary
	1 Error	Checksum	IPv4	Bad checksum
	2 Error	Checksum	IPv4	Bad checksum
	4 Error	Checksum	IPv4	Bad checksum
	4 Note	Sequence	ТСР	Retransmission (suspected)
	8 Error	Checksum	IPv4	Bad checksum
	8 Chat	Sequence	HTTP	GET /downloads/info.aspx?na=41&SrcFamilyId=0A391A
	9 Error	Checksum	IPv4	Bad checksum
	9 Chat	Sequence	HTTP	GET /dcs8kzhcc00000ww68ffquzt0_6o5q/dcs.gif?&dcsdat
	10 Error	Checksum	IPv4	Bad checksum
<u>H</u> elp		-		<u>C</u> lose

マクロ的分析

●対話 (Conversations) 統計機能

◎終端 (Endpoint) 統計機能

Top N分析 / パレート分析に 利用できる

対話 (Conversations) 統計機能

Statistics] – [Conversations]

Conversations: IE_Download.pcap

Ethernet: 13 Fibre (Channel FDD1 IPv4:	28 IPv6: 6	IPX JXTA	NCP RSVP SCT	P TCP: 41 To	ken Ring UDP: 2	6 USB WLAN					
Ethernet Conversations												
Address A	Address B	Packets (Bytes (Packets A→B ◀	Bytes A→B ◀	Packets A←B ◀	Bytes A←					
00:1b:8b:11:a0:0d	6c:62:6d:a5:b0:d0	54 136	53 566 867	35 864	52 526 605	18 272	1 040					
6c:62:6d:a5:b0:d0	ff:ff:ff:ff:ff	6	685	6	685	0						
00:d0:2b:30:b5:1a	33:33:00:00:00:0d	1	136	1	136	0						
00:1b:8b:11:a0:0d	01:00:5e:7f:ff:fa	20	6 932	20	6 932	0	=					
33:33:00:00:00:0c	6c:62:6d:a5:b0:d0	6	2 048	0	0	6	2					
01:00:5e:7f:ff:fa	6c:62:6d:a5:b0:d0	6	1 952	0	0	6	1					
00:00:74:fd:d2:07	6c:62:6d:a5:b0:d0	16	3 382	10	2 870	6						
33:33:00:01:00:03	6c:62:6d:a5:b0:d0	2	174	0	0	2						
01:00:5e:00:00:fc	6c:62:6d:a5:b0:d0	1	67	0	0	1						
00:13:d3:ff:c4:44	33:33:ff:5a:f9:11	1	86	1	86	0	-					
•							•					

Name resolution

Limit to display filter

Help

Close

Conversations – Ethernet タブ

◎送信元/宛先 MAC アドレスの組み合わせ ごとの情報を表示

Conversations: IE_	Download.pcap					[- 0 8			
Ethernet: 13 Fibre	Channel FDD1 IPv4:	28 IPv6: 6	IPX JXTA	NCP RSVP SCT	P TCP: 41 To	ken Ring UDP: 26	USB WLAN			
Ethernet Conversations										
Address A	Address B	Packets (Bytes (Packets A→B ◀	Bytes A→B ◀	Packets A←B ◀	Bytes A←			
00:1b:8b:11:a0:0d	6c:62:6d:a5:b0:d0	54 136	53 566 867	35 864	52 526 605	18 272	1 040			
6c:62:6d:a5:b0:d0	ff:ff:ff:ff:ff	6	685	6	685	0				
00:d0:2b:30:b5:1a	33:33:00:00:00:0d	1	136	1	136	0				
00:1b:8b:11:a0:0d	01:00:5e:7f:ff:fa	20	6 932	20	6 932	0	=			
33:33:00:00:00:0c	6c:62:6d:a5:b0:d0	6	2 048	0	0	6	2			
01:00:5e:7f:ff:fa	6c:62:6d:a5:b0:d0	6	1 952	0	0	6	1			
00:00:74:fd:d2:07	6c:62:6d:a5:b0:d0	16	3 382	10	2 870	6				
33:33:00:01:00:03	6c:62:6d:a5:b0:d0	2	174	0	0	2				
01:00:5e:00:00:fc	6c:62:6d:a5:b0:d0	1	67	0	0	1				
00:13:d3:ff:c4:44	33:33:ff:5a:f9:11	1	86	1	86	0	-			
4										

Conversations – IPv4 タブ

●送信元/宛先 IP アドレスの組み合わせごと に情報を表示

Conversations:	IE_Download.pca	þ						Σ
Ethernet: 13 Fib	ore Channel FDD1	IPv4: 28 I	Pv6:6 IPX	JXTA NCP RSVP	SCTP TCP: 4	1 Token Ring U	DP: 26 USB W	VLAN
			IPv4	Conversations				
Address A	Address B	Packets (Bytes (Packets A→B ◀	Bytes A→B (Packets A←B ◀	Bytes A←B ◀	F 🔺
65.55.122.235	192.168.1.14	4	244	0	0	4	244	
74.125.153.125	192.168.1.14	2	121	1	66	1	55	Ξ
192.168.1.14	255.255.255.255	1	124	1	124	0	0	
192.168.1.14	207.46.19.254	100	93 321	38	21 558	62	71 763	
192.168.1.14	208.92.236.184	20	5 872	10	3 998	10	1 874	
65.55.122.234	192.168.1.14	6	366	0	0	6	366	
192.168.1.1	192.168.1.14	33	8 636	18	7 347	15	1 289	
143.90.194.26	192.168.1.14	53 815	53 370 631	35 690	52 377 057	18 125	993 574	
65.55.5.232	192.168.1.14	3	1 832	1	1 065	2	767	
143.90.194.43	192.168.1.14	12	8 711	6	6 057	6	2 654	-
•							Þ	

Conversations – TCP タブ

◎送信元 IP・PORT / 宛先 IP・PROT の組み 合わせごとに情報を表示

🗖 Conversations: IE_Download.pcap

Ethernet: 13 F	ibre Chanr	rel FDD1 IPv4: 2	8 IPv6: 6	IPX JXTA	NCP RSVP	SCTP TCP: 41	Token Ring U	DP: 26 USB WLAN
Address A	Port A 🖣	Address B	Port B 🖣	Packets (Bytes (Packets A→B ◀	Bytes A→B ◀	Packets A←B ▲
65.55.122.235	2492	192.168.1.14	2492	4	244	0	0	
192.168.1.14	56465	74.125.153.125	5222	2	121	1	55	-
192.168.1.14	57270	207.46.19.254	80	11	9 395	5	5 164	1
192.168.1.14	57300	208.92.236.184	80	7	2 787	3	1 916	
192.168.1.14	57269	207.46.19.254	80	25	23 499	10	5 420	1
65.55.122.234	2492	192.168.1.14	2492	6	366	0	0	1
192.168.1.14	57302	143.90.194.26	80	3	186	2	120	
192.168.1.14	57303	143.90.194.26	80	53 812	53 370 445	18 123	993 454	35 68
192.168.1.14	57268	207.46.19.254	80	4	3 183	2	2 528	1
192.168.1.14	57267	207.46.19.254	80	5	4 417	2	2 551	
•								4

Conversation List

●特定のプロトコルだけのリストを作成する 場合は

[Statistics] – [Conversation List]

からプロトコルを選択する

プロトコル階層の分析

[Statistics] – [Protocol Hierarchy]

📶 Wireshark: Protocol Hierarchy Statistics						
Display	filter: none					
Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Pack 🔺
🗆 Frame	100.00 %	54203	100.00 %	53583039	18.025	
Ethernet	100.00 %	54203	100.00 %	53583039	18.025	
Internet Protocol Version 4	99.96 %	54182	99.99 %	53579771	18.023	
Transmission Control Protocol	99.86 %	54125	99.97 %	53565742	18.019	18
Data	0.02 %	10	0.00 %	610	0.000	
Jabber XML Messaging	0.00 %	1	0.00 %	55	0.000	
Hypertext Transfer Protocol	66.06 <mark>%</mark>	35805	98.06 %	52543350	17.675	35
Line-based text data	0.01 %	6	0.01 %	6763	0.002	
Compuserve GIF	0.01 %	4	0.01 %	4048	0.001	
Malformed Packet	0.00 %	1	0.00 %	1434	0.000	
Media Type	0.01 %	3	0.01 %	4370	0.001	
Portable Network Graphics	0.01 %	4	0.01 %	5804	0.002	
Malformed Packet	0.01 %	4	0.01 %	5804	0.002	
Malformed Packet	0.00 %	1	0.00 %	60	0.000	
Secure Sockets Layer	0.04 %	21	0.02 %	8331	0.003	
User Datagram Protocol	0.11 %	57	0.03 %	14029	0.005	



◎IO Graph 機能 ◎[**Statistics**] – [IO Graphs]



IO Graph





◎XAxis:X軸(横軸)の調整

- Tick interval
 プロット 単原回時間/
 - プロット間隔時間の調整
- Pixels per tick プロット表示間隔の調整
- View as time of day
- 表示時間フォーマットの変更



◎X Axisの設定





●YAxis:Y軸(縦軸)の調整

- Unit
 - 表示単位の切り替え Packet 数, Byte数, Bit数, Advanced
- Scale
 - 目盛のスケールの切り替え



●YAxisの設定



グラフ データの追加

- [Graphs] セクション [Filter]
 Display Filter と同じ書式でフィルタを 設定する
- ◎[Graph n] ボタンで表示/非表示を切替え

Graph 4 Color Filter: ip.addr==74.125.235.170



◎[Graphs] セクション – [Filter]



グラフの保存

●[Save] ボタン

作成したグラフを画像として保存できる

📶 Wireshark: Sa	ave Graph As	23
<u>N</u> ame:		
Save in <u>f</u> older:	🛅 Captures	-
<u>■</u> Browse for other folders		
File type: png	•	
	<u>S</u> ave <u>C</u> a	ncel

TCPストリームの可視化

●TCP Stream Graph 機能

●[Statistics] - [TCP Stream Graph] - 作成するグラフの種類を選択

TCP Stream Graph





◎Graph Control ウィンドウの [Graph Type] タブで切り替えできる

📶 Graph 7 - Control - W 🗖 🔲 🔀		
Zoom Magnify Origin Cross Graph type		
Graph type:		
Round-trip Time		
Throughput		
Time/Sequence (Stevens'-style)		
Time/Sequence (tcptrace-style)		
Window Scaling		
Init on change		
<u>H</u> elp <u>C</u> lose		

Round Trip Time Graph



Throughput Graph



Time/Sequence (Stevens)



Time/Sequence (tcptrace)



Window Scaling





Wireshark User's Guide http://www.wireshark.org/docs/ wsug_html_chunked/ Wireshark Wiki http://wiki.wireshark.org/FrontPage Wireshark University http://www.wiresharktraining.com/