Wireshark 入門

キャプチャしたパケットの表示

hebikuzure

本日のテキスト

◎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 Windows 環境では同梱のWinPcap を利用 しましょう

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

パケットの検索

[Edit] -> [Find Packet]

Wireshark: Find		
Find-		
By: () <u>D</u> isplay filte	er 🔘 <u>H</u> ex value 🔘 <u>S</u> tring	
F <u>i</u> lter:		
Search In	String Options	Direction
Packet list	Case sensitive	© <u>U</u> р
Packet details	Character set:	<u> </u>
Packet bytes	ASCII Unicode & Non-Unicode	-
<u>H</u> elp	<u> </u>	<u>C</u> ancel



◎右クリック -> [Mark Packet]

 \circ Ctrl + M

Destination Protocol Info 4697 > 80 [SYN] Seq=0 Win=8192 L Mark Packet (toggle) .15 0 > 64697 [SYN, ACK] Seq=0 Ack=1 Ignore Packet (toggle) 80 [ACK] Seq=1 Ack=1 Win= Set Time Reference (toggle) .15 64697 [ACK] Seq=1 Ack=928 Wi .15 (text/html) ттр/1.1 200 ок Manually Resolve Address .15 Previous segment lost] Conti .15 Previous seament lost Conti Apply as Filter .15 Previous segment lost Prepare a Filter .15 se .15 Conversation Filter revious se Colorize Conversation .15 nuation or non-HTTP SCTP .15 ous .15 Follow TCP Stream Previous sea ient lost .15 Previous seament lost Cont Follow UDP Stream (496 bits) Follow SSL Stream cf:be:af cces_11:a0:0d (00:1b:8b:11:a0:0d 6.15 (211.131.226.15) 2.168.1.8 Copy col, Src P 80 (80), Seq: 0, Len: 0 ැ Decode As... 📇 Print... Show Packet in New Window

時間の表示形式

2011_02	_15	i.cap - Wireshark				
<u>F</u> ile <u>E</u> dit	Vie	ew <u>G</u> o <u>C</u> apture <u>A</u> nalyze	Statistics Telepho	<u>ז ע</u> ר	<u>T</u> ools <u>H</u> elp	
	~	<u>M</u> ain Toolbar		T	👱 🗐 🗐 Đ, Q, 01, 17 ઍ 🗹 畅 % 💢	
Filter:	~	<u>F</u> ilter Toolbar			▼ Expression Clear Apply	
Theer.		<u>W</u> ireless Toolbar		-	Copression Color Approv	
No. Ti	~	<u>S</u> tatusbar			Protocol Info	
10.	,	Packet List		6.19	.5 TCP 64697 > 80 [SYN] Seq=0 Win=8192 Len=	0 MS
2 0. 3 0.	Ĵ	Packot Dotailo		。 6.1	10° 1	11=58 44 L
4 0.	Ť.	Packet Details		6.1	L5 HTTP GET / HTTP/1.1	
50.	×	Packet Bytes		8	ТСР 80 > 64697 [АСК] Seq=1 Ack=928 win=7	416
6 0. 7 0		<u>T</u> ime Display Format	۲.	[Date and Time of Day: 1970-01-01 01:02:03.123456 Ctrl+Alt-	+1 📘
8 0.		Name Resolution	•	٦	Time of Day: 01:02:03.123456 Ctrl+Alt-	+2
90.	~	Colorize Packet List		5	Seconds Since Epoch (1970-01-01): 1234567890.123456 Ctrl+Alt-	+3
$\begin{array}{c} 10 \ 0. \\ 11 \ 0. \end{array}$	~	Auto Scroll in Li <u>v</u> e Capture		• 9	Seconds Since Beginning of Capture: 123.123456 Ctrl+Alt	+4
12 0.	Ð	Zoom In	Ctrl++	5	Seconds Since Previous Captured Packet: 1.123456 Ctrl+Alt-	+5 🚺
13 0. 14 0.	Q	Zoom <u>O</u> ut	Ctrl+-	5	Seconds Since Previous Displayed Packet: 1.123456 Ctrl+Alt-	+6
15 0.	1	Normal Size	Ctrl+=	• /	Automatic (File Format Precision)	
16 0.	* *	Resize All Columns	Shift+Ctrl+R	5	Seconds: 0	-
		Displayed Columns	•	[Deciseconds: 0.1	
∃ Intern		Expand Subtrees	Shift+Right	C	Centiseconds: 0.12	
⊕ Transm		Expand All	Ctrl+Right	1	Milliseconds: 0.123	
		Collanse All	Ctrl+Left	1	Microseconds: 0.123456	
			Confecto	1	Nanoseconds: 0.123456789	
		Colorize Conversation	+		Dialay Cases do with house and minutes	
		Reset Coloring 1-10	Ctrl+Space	L	Display Seconds with hours and minutes Ctrl+Alt-	+0

時間の相対表示

- [Time Display Format] で [Second Since Beginning of Capture] を選択
 - この状態でキャプチャ開始からの相対時間を表示
- 基準にしたいパケットをクリックして
 [Edit] -> [Set Time Reference] (Ctrl + T)
 基準にしたパケットからの経過時間を表示

間隔の表示

- [Seconds Since Previous Captured Packet]
 - 直前にキャプチャしたパケットからの経過時間
- [Seconds Since Previous displayed Packet]
 - 表示されている直前のパケットからの経過時間

フィルタ

●キャプチャ フィルタ

- 特定の条件に合致したパケットだけキャプチャするためのフィルタ
- 条件に合致しないパケットは記録されない
- ◎ディスプレイ フィルタ
 - 特定の条件に合致したパケットだけ表示するためのフィルタ
 - 条件に合致しないパケットは表示されない
 - ・元のキャプチャ データは変更されない

キャプチャフィルタ

Wireshark: Capture Options					
Capture					
Interface: Local	▼ Intel	(R) PRO/1000 PM Netw	vork Connection: ¥Device¥NPF_{4C:		
IP address: fe80:	:e076:4ff4:903b	:aac9, 2001:c…:1458:	1326:e076:4ff4:903b:aac9, 192.168.1.8		
Link-layer header	r type: Etherne	et 💌	Wireless Settings		
Capture packe	ets in <u>p</u> romiscuol	us mode	Remote Settings		
Capture packe	ets in pcap-ng for	rmat (experimental)	Buffer size: 1 🚔 megabyte(s)		
Careburg Silbary					
Capture Filter:			Ľ		
Capture File(3)			Display Options		
File:		<u>B</u> rowse	Update list of packets in real time		
Use <u>m</u> ultiple fi	iles		Automatic corolling in live conture		
✓ Next file every	y 1	🔭 megabyte(s) 🔻	Automatic scrolling in live capture		
🗌 Next file every	y 1	minute(s)	☑ <u>H</u> ide capture info dialog		
☑ Ring buffer wit	th 2	files	Name Beschutien		
Stop capture a	after 1	[^] √ file(s)			
Stop Capture—			Enable MAC name resolution		
🔲 after 1	* *	packet(s)	Enable network name resolution		
🔲 after 1	* *	megabyte(s) -			
🔲 after 1	Å	minute(s) 👻	Enable transport name resolution		
Help			<u>S</u> tart <u>C</u> ancel		

キャプチャフィルタの作成

📶 Wireshark: Capture Filter - Profile: Default 💿 🖾						
Edit-	Capture Filter					
	Ethernet address 00:08:15:00:08:15					
	Ethernet type 0x0806 (ARP)					
New	No Broadcast and no Multicast					
	No ARP	8				
	IP only					
	IP address 192.168.0.1					
Delete	IPX only					
Delete	TCP only					
	UDP only					
Description						
Properties	S					
Filter nan	ne:					
Filter stri	ing:					
<u>H</u> elp	<u>O</u> K <u>C</u> ancel					

キャプチャフィルタの書式

- [not] primitive [and|or [not] primitive ...]
- ◎ 論理演算子は not、 and、 or
- ●例
 - tcp port 23 and host 10.0.0.5
 - tcp port 23 and not src host 10.0.0.5
- ●詳細はヘルプ参照のこと

ディスプレイフィルタ

201:	1_02_15.cap -	Wireshark				
<u>F</u> ile <u>E</u>	<u>E</u> dit <u>V</u> iew <u>G</u> o	o <u>C</u> apture <u>A</u> nalyze <u>S</u>	<u>S</u> tatistics Telephon <u>y</u> <u>T</u> ools <u>H</u>	<u>i</u> elp		
ev 2						
Filter:			▼ E	xpression	Clear Apply	
No	Time	Course	Destination	Drotocol	al Tafa	
IINO.	1 0.000000	192.168.1.8	211, 131, 226, 15	TCP	64697 > 80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 SACK PERM=1	
	2 0.009963	211.131.226.15	192.168.1.8	TCP	80 > 64697 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1414 SACK_PERM=1	
	3 0.010123	192.168.1.8	211.131.226.15	тср	64697 > 80 [ACK] Seq=1 Ack=1 Win=65044 Len=0	
	4 0.013523	192.168.1.8	211.131.226.15	HTTP	GET / HTTP/1.1	
	5 0.021536	211.131.226.15	192.168.1.8	тср	80 > 64697 [ACK] Seq=1 Ack=928 Win=7416 Len=0	
	6 0.06/496	211.131.226.15	192.168.1.8	HTTP	HTTP/1.1 200 OK (text/html)	
	7 0.067496 8 0.067496	211.131.220.13	192.108.1.8		Continuation or non-HITP traffic	
	9 0 067496	211.131.220.15	192.108.1.8	нттр	Continuation or non-HTTP traffic	
1	0 0.067496	211.131.226.15	192.168.1.8	нттр	Continuation or non-HTTP traffic	
1	1 0.067496	211.131.226.15	192.168.1.8	HTTP	Continuation or non-HTTP traffic	
1	2 0.067781	192.168.1.8	211.131.226.15	ТСР	64697 > 80 [АСК] Seq=928 Ack=8485 win=65044 Len=0	
1	3 0.077561	211.131.226.15	192.168.1.8	HTTP	Continuation or non-HTTP traffic	
1	4 0.079120	211.131.226.15	192.168.1.8	HTTP	Continuation or non-HTTP traffic	
1	5 0.079120	211.131.226.15	192.168.1.8	НТТР	Continuation or non-HTTP traffic	
1	6 0.079120	211.131.226.15	192.168.1.8	нттр	Continuation or non-HTTP traffic	
🖽 Fra	me 1: 62 by	tes on wire (496 b	oits), 62 bytes captured	(496 bi	pits)	
🕀 Eth	ernet II, S	rc: AsustekC_cf:be	e:af (00:13:d4:cf:be:af)	, Dst: N	NecAcces_11:a0:0d (00:1b:8b:11:a0:0d)	
🕀 🗄 🕀	ernet Proto	col, Src: 192.168.	1.8 (192.168.1.8), Dst:	211.131	31.226.15 (211.131.226.15)	
🛛 🗆 Tra	nsmission C	ontrol Protocol, S	Src Port: 64697 (64697),	Dst Port	ort: 80 (80), Seq: 0, Len: 0	
S S	ource port:	6469/ (6469/)				
r I	Stream inde	v· 01				
s	equence num	ber: 0 (relativ	/e sequence number)			
н	eader lengt	h: 28 bytes				
	lags: 0x02	(5YN)				
W	indow size:	8192				
. ⊕ C	hecksum: 0x	7766 [validation of	disabled]			
. ± 0	ptions: (8	bytes)				

ディスプレイフィルタの作成

Field name		Relation	Value (protocol)
	•	is present	
104apci - IEC 60870-5-104-Apci		==	Predefined values:
		!=	
		>	
		<	
		>=	
€ 6LoWPAN - IPv6 over IEEE 802.15.4		<=	
B02.11 MGT - IEEE 802.11 wireless LAN mar		contains	
802.11 Radiotap - IEEE 802.11 Radiotap Capi		matches	
⊕ 9P - Plan 9 9P			Range (offset:length)

<u>0</u>K

Cancel



== (eq): 等しい
!= (ne): 等しくない
> (gt): 大なり
< (lt): 小なり
>= (ge): 以上
<= (le): 以下



and (&&):論理積 or (||):論理和 xor (^^):排他的論理和 not (!):否定

フィルタの例

- ohost example.com
- host example.com and not (port 80)
 !dns
- onot broadcast and not multicast
- ip.dst==192.168.0.1

よくある間違い

- ip.addr == 1.2.3.4 で IP アドレスに
 1.2.3.4 を含むパケットを表示できる
 ○では、IP アドレスに 1.2.3.4 を含まない
 パケットを表示するフィルタは??
- □間違い:ip.addr!=1.2.3.4
 ○正解 :!(ip.addr == 1.2.3.4)

フィルタの保存

[Analyze] – [Display Filter]

Wireshark: Display Filter - Profile: Default					
Edit	Display Filter				
New	IP address isn't 192.168.0.1, don't use != for this! IPX only TCP only UDP only				
Delete	UDP port isn't 53 (not DNS), don't use != for this! TCP or UDP port is 80 (HTTP) HTTP No ARP and no DNS Non-HTTP and non-SMTP to/from 192.168.0.1				
Properties					
Filter nam	ne: new				
Filter stri	ng: new Expression				
<u>H</u> elp <u>OK</u> <u>A</u> pply <u>C</u> ancel					

ディスプレイフィルタの詳細

●ヘルプを参照

Wireshark Wiki Display Filter page http://wiki.wireshark.org/DisplayFilters.

Wiresharkの名前解決

●MAC アドレス

- MAC アドレス \Rightarrow IP アドレスに解決 (arp)
- MAC アドレスの上位3バイト ⇒ ベンダー名

● IP アドレス ・ IP アドレス ⇒ ホスト名(DNS)

●ポート番号 ・ポート番号 ⇒プロトコル名(well-known ports)

名前解決のデメリット

◎IP アドレスの名前解決のためキャプチャ時、キャプチャファイルを開く際に DNS アクセスが行われる

- ・トラフィックの増加
- ・処理時間の増加

◎ポート番号の名前解決では well-known ports 以外のトラフィックが正しく表示されない(かえって分かりにくくなる)

名前解決・キャプチャ時の設定

[Capture] – [Options] の "Name Resolution" セクション

🗖 Wireshark: Ca	apture (Options					
Capture							
Interface: Local 🔹 Intel(R) PRO/1000 PM Network Connection: ¥Device¥NP					work Connection: ¥Device¥NPF_{4C: 💌		
IP address: fe8	80::e07	5:4ff4:90)3b:a	ac9, 2001:c…:1458:	1326:e076:4ff4:903b:aac9, 192.168.1.8		
Link-layer head	der type	e: Ethe	rnet	•	Wireless Settings		
Capture pac	kets in	promiso	uous	mode	Remote Settings		
Capture pac	kets in	pcap-ng	forn	nat (experimental)	Buffer size: 1 megabyte(s)		
Limit each p	packet 1	to 1		🗸 bytes			
Capture Filter	:				.		
Capture File(s)					Display Options		
File:				Browse	☑ Update list of packets in real time		
Use <u>m</u> ultiple	e files						
✓ Next file ev	ery	1	1	megabyte(s) 👻	<u>Automatic scrolling in live capture</u>		
Next file ev	ery	1	1	minute(s) 🔻	Hide capture info dialog		
✓ Ring buffer	with	2	1	files	Name Resolution		
Stop captur	e after	1	4	file(s)			
Stop Capture					Enable MAC name resolution		
🔲 after	1		÷ pa	acket(s)	Enable network name resolution		
🔲 after	1		↓ m	negabyte(s)			
🔲 after	1		* m	ninute(s)	Enable transport name resolution		
<u>H</u> elp					<u>S</u> tart <u>C</u> ancel		

名前解決・表示時の設定

[View] – [Name Resolution]

<u>V</u> ie	w <u>G</u>	o <u>C</u> a	apture	<u>A</u> nalyze	Statistics	Telepho	n <u>y</u>	<u>T</u> ools	<u>H</u> e	lp				
~	<u>M</u> ain	Toolb	ar				1	_₽			Ð	Θ	11	++
ľ	<u>F</u> ilter <u>W</u> irel	Tooli ess T	oar oolbar					•	Exp	pression.		Clear	Арр	oly
- I	<u>S</u> tatı	ısbar								Protoco	ol	Info		
-	Pack	et <u>L</u> ist	t				8			HTTP		Cont	inua	ati
~	Pack	et <u>D</u> et	tails				8			HTTP		HTTP	/1.1	L 2
-	Pack	et <u>B</u> yt	es				8			HTTP		Cont	inua	ati
	Time	Dicol	av Forn	nat			6.	16 16		TCP		6470	$\frac{1}{2}$	ht ht
	Nam	e Res	, ol <u>u</u> tion			•		<u>R</u> esol	ve N	ame				
~	Color	ize Pa	icket Li	st				Enabl	e for	MAC La	ayer			
۲	Auto	Scroll	in Li <u>v</u> e	Capture			~	Enabl	e for	<u>N</u> etwor	rk Li	ayer		
Ð	<u>Z</u> oon	n In				Ctrl++	~	Enabl	e for	Transp	ort I	Layer		
Θ	Zoon	n Out				Ctrl+-	0		_	HITP		CONC	mue	Z

プロトコルの解析

●通常はWireshark が自動的に各フレーム (パケット)のプロトコルを解析して表示 してくれる

●リンク層、ネットワーク層、トランスポー
 ト層それぞれのプロトコルが解析される

自動解析の限界

●正しく解析されない場合も多い

◎特にトランスポート層で既定のポート以外 を使い通信を行っている場合

•ex.

- 81番ポートで HTTP
- 443番ポート以外での HTTPS

プロトコルの手動指定

プロトコルのデフォルトのポートを使用していないトラフィックは正しいプロトコルが推測されない場合が多い

●キャプチャ内容などからプロトコルが分かる場合は、手動でプロトコルを指定して表示させることができる

プロトコルの指定方法

●指定するパケットを右クリック ●[Decode as...]を選択 ●プロトコルを指定

Wireshark: Decode	As		x
	Link Network Transport		
Oecode		(default)	_
		104apci	
		9P	
o De est desede		ACAP	
Do not decode	TCP source (64697) rort(s) as	AgentX	
		AIM	
Show Current		AJP13	
Clear		AMQP	-
<u>H</u> elp	<u></u> K	<u>A</u> pply <u>C</u> lose	

TCP Stream の表示

○1つのTCPセッション中で送受信された データをまとめて表示する ○フレームを右クリック -

[Follow TCP Stream]

T. T.	.92.100.1.0	11CCP > 04097 [31N
2	Mark Packet (toggle)	697 > http [АСК] Г / НТТР/1.1
15 1	Ignore Packet (toggle)	tp > 64697 [АСК]
15 1	() Set Time Reference (toggle)	ГР/1.1 200 OK (
15 1		ntinuation or no
15 1	Manually Resolve Address	ntinuation or no
15 1		ntinuation or no
15 1	Apply as Filter	htinuation or no
15 1	Prenare a Filter	htinuation or no
2	i repare a riter	697 > http [АСК]
15 1	Conversation Filter	htinuation or no
15 1	Colorize Conversation	htinuation or no
15 1	CCTD	htinuation or no
15		rinuation or no
(422 hitc)	Follow TCP Stream	· ·
cf be af	Follow LIDP Stream	as 11:30:0d (0)
169 1 9	Fallow CGL Changes	15 (211 121 22)
.100.1.8 (Follow SSL Stream	15 (211.131.22)

Follow TCP Stream

Tellow TCP Stream
Stream Content
<pre>GET / HTTP/1.1 Host: www.asahi.com Connection: keep-alive Referer: http://home.att.ne.jp/gold/hebikuzure/link/bookmark.html Accept: application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5 User-Agent: Mozilla/5.0 (windows; U; windows NT 6.1; en-US) ApplewebKit/534.13 (KHTML, like Gecko) Chrome/9.0.597.98 safari/534.13 Accept-Encoding: gzip,deflate,sdch Accept-Language: ja,en-US;q=0.8,en;q=0.6 Accept-Charset: Shift_JIS,utf-8;q=0.7,*;q=0.3 Cookie: SC_Cut=55605079; ebNewBandWidthwww.asahi.com=1686%3A1297769203290; utmz=261975709.1297769205.19.14.utmcsr=home.att.ne.jp utmccn=(referral) utmcd=referral utmcct=/ gold/hebikuzure/link/bookmark.html; utma=261975709.505929885.1279864839.1297591984.1297769205.19:</pre>
utmb=261975709.1.10.1297769205; IMPASEG=50%3D10198/51%3D10876/52%3D10130/53%3D10127/54%3D11132/55% 3D11135/56%3D11136/57%3D10451/58%3D11279/59%3D10474/510%3D10080
HTTP/1.1 200 OK Server: Apache/2 Content-Type: text/html ETag: "5e35b4-ffa6-75f2b640" Vary: Accept-Encoding Content-Encoding: gzip Cache-Control: max-age=3 Expires: Tue, 15 Feb 2011 11:29:26 GMT Date: Tue, 15 Feb 2011 11:29:23 GMT Content-Length: 19637 Connection: keep-alive
Help Filter Out This Stream Close

TCP Stream のフィルタ

● "Follow TCP Stream"を行うと、そのスト リームだけ表示するフィルタが適用される

2011_02_15.cap -	Wireshark	_
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o	<u>Capture A</u> nalyze <u>S</u> tati	stics Telephon <u>y T</u> ools
	🖻 🛃 🗶 🛃 🗏 🤇	2, 🗢 🛸 🍛 ዥ 👱
Filter: tcp.stream eq	0	
No. Time	Source	Destination
1 0.000000	192.168.1.8	211.131.226.15
2 0.009963	211.131.226.15	192.168.1.8
3 0.010123	192.168.1.8	211.131.226.15
4 0.013523	192.168.1.8	211.131.226.15
5 0.021536	211.131.226.15	192.168.1.8
6 0.067496	211.131.226.15	192.168.1.8
7 0.067496	211.131.226.15	192.168.1.8

プロトコルの配分を確認する

Statistics] – [Protocol Hierarchy]

Help

🗖 Wireshark: Protocol Hierarchy Statistics								
	Display filt	er: none						
Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets E	End Bytes E	ir
🗆 Frame	100.00 %	1370	100.00 %	957097	0.655	0	0	
Ethernet	100.00 %	1370	100.00 %	957097	0.655	0	0	
Internet Protocol	100.00 %	1370	100.00 %	957097	0.655	2	5574	
Transmission Control Protocol	99.85 %	1368	99.42 %	951523	0.651	390	22228	
Hypertext Transfer Protocol	71.39 %	978	97.10 %	929295	0.636	707	727639	
Line-based text data	7.88 %	108	5.03 %	48133	0.033	108	48133	
Media Type	0.95 %	13	1.92 %	18331	0.013	13	18331	
Compuserve GIF	7.88 %	108	8.50 %	81349	0.056	95	62265	
Malformed Packet	0.95 %	13	1.99 %	19084	0.013	13	19084	
Portable Network Graphics	1.02 %	14	1.37 %	13138	0.009	9	5798	
Malformed Packet	0.36 %	5	0.77 %	7340	0.005	5	7340	
JPEG File Interchange Format	1.90 %	26	3.99 %	38168	0.026	25	36700	
Malformed Packet	0.07 %	1	0.15 %	1468	0.001	1	1468	
eXtensible Markup Language	0.15 %	2	0.27 %	2537	0.002	2	2537	

Close

エンドポイントの確認

Statistics] – [Endpoints]

C Endpoints: 2011_02_15.cap

Ethernet: 2	Fibr	e Channel	FDDI	IPv	4: 16	IPv6	IP	ATXL X	NCP	RSVP	SCT	P TCP: 59	Token Ring	UDP	USB	WL	AN
								IPv4 End	dpoint	s							
Address	•	Packets 4	Bytes	•	Tx Pa	ckets	• •	Tx Bytes	< R	k Packe	ts 🔹	Rx Bytes 🖣	Latitude 🖣	Longit	tude	•	*
192.168.1.8	}	1 368	951 5	523		55	53	161 0	65		815	790 458	-			-	
211.131.220	6.15	228	207 9	956		14	19	177 4	65		79	30 491	-			-	
59.106.108.	72	340	116 8	339		16	58	54 8	76		172	61 963	-			-	
211.131.220	5.16	538	458 2	276		34	41	409 1	82		197	49 094	-			-	=
220.213.234	4.196	5 20) 45	534		1	10	2 3	02		10	2 232	-			-	
143.90.194.	26	107	108 8	363		7	78	104 4	97		29	4 366	-			-	
74.125.235.	78	51	. 25 5	581		2	28	21 9	65		23	3 616	-			-	-
143.90.194.	25	7	17	789			3	7	66		4	1 023	-			-	
203.169.10.	232	7	13	388			3	4	89		4	899	-			-	
115.69.195.	172	12	2 3 0	000			6	19	38		6	1 062	-			-	
216.223.0.2	09	7	11	155			4	9	85		3	170	-			-	Ŧ

Name resolution

Limit to display filter

<u>H</u>elp

Map

Copy

23

Conversations

Follow Stream

23

Close

Statistics] – [Conversations]

Conversations: 2011_02_15.cap

Ethernet: 1	Fibre	ore Channel FDDI		Channel FDDI		Channel FDDI		e Channel FDDI		e Channel FDI		Channel FDI		Channel FDDI		IPv4: 15	IPv4: 15 IPv6 IPX JXTA		NCP	RSVP SCTP		TCP: 44		Token Ring	UDP	USB	WL	AN
IPv4 Conversations																												
Address A	▲ A	ddress B	•	Packets 4	Bytes	5 4	Packets	A->B	 ■ By 	/tes A->	·B∢	Pack	æts A<-B ◀	Bytes	A<-B	•	*											
192.168.1.8	2	11.131.22	26.15	228	207	956			79	30	491		149		177 4	65												
59.106.108.7	72 19	92.168.1.	8	340	116	839		1	68	54	876		172		61 9	63												
192.168.1.8	2	11.131.22	26.16	538	458	276		1	.97	49	094		341		409 1	82	=											
192.168.1.8	2	20.213.23	34.196	20	4	534			10	2	232		10		23	302												
143.90.194.2	26 19	92.168.1.	8	107	108	863			78	104	497		29		4 3	866												
74.125.235.7	78 19	92.168.1.	8	51	25	581			28	21	965		23		3.6	516												
143.90.194.2	25 19	92.168.1.	8	7	1	789			3		766		4		10)23												
192.168.1.8	20	03.169.10).232	7	1	388			4		899		3		4	189												
115.69.195.1	172 19	92.168.1.	8	12	3	000			6	1	938		6		10	62												
192.168.1.8	2	16.223.0.	209	7	1	155			3		170		4		9	85	Ŧ											
				111		_																						

Name resolution

Copy

Limit to display filter

<u>H</u>elp

IO グラフ

• [Statistics] – [IO Graphs]





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/