## Wireshark で見る プロトコル

#### プロトコルの特徴を知る

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

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	
	Link Network Transport	
Oecode		(default)
		104apci
		9P
o De est de se de		ACAP
Do not decode	ICP source (64697)  port(s) as	AgentX
		AIM
Show Current		AJP13
Clear		AMQP
<u>H</u> elp	<u> </u>	<u>Apply</u> <u>Close</u>

#### プロトコルの特徴・パターンを知る

# ●代表的なプロトコルのパケット内容を知る =正常な動作のパターンを知る ●『正常』を知れば『異常』に気づきやすい

#### ◎自動解析されなかったプロトコルを推定す る場合にも必要な経験

#### Ethernet フレーム フォーマット

Ethernetのフレームフォーマット											
DIX仕様(Eth	ernet	<b>Iフレーム</b> )									
プリアンブノ	L	宛先 MAC <b>ア</b> ドレス	送信元 MACアドレス	タイプ		データ	FCS				
8byte		6byte	6byte	2byte	4	6 ~ 1500byte	4byte				
物理ヘッダ	,	E	thernetヘッダ				トレーラ				
				-							
IEEE仕様 (IEEE802.3フレーム) + 802.2(LLC+SNAP)											
プリアンブル SFD		宛先 MAC <b>ア</b> ドレス	送信元 MACアドレス	長さ	LLC SNAP データ		FCS				
8byte		6byte	6byte	2byte	3byte 5byte	38 ~ 1492byte	4byte				
物理ヘッダ		E	thernetヘッダ				トレーラ				

●プリアンブルとトレーラはWiresharkで は表示されない

#### ARP

#### ●ネットワーク層(MACアドレス)とデー タリンク層(IPアドレス)のプロトコル

arp.pcap

<pre>jie</pre>	🗓 arp.pcap - Wireshark	X
Iter:       • • • • • • • • • • • • • • • • • • •	Elle Edit View Go Capture Analyze Statistics Telephony Iools <u>H</u> elp	
Iter:       • Expression Clear Apply         2. Time       Source       Destination         10.000000 homHaiFr_6e:8b:24       Protocol Info         2.0.004081       D-Link_0b:22:ba       HonHaiFr_6e:8b:24         Prame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)         Arrival Time: Dec 11, 2006 04:59:22.88051000 Esconds         [Inter delta from previous Captured frame: 0.000000000 seconds]         [Inter delta from previous displayed frame: 0.00000000 seconds]     <	꽃 날 살 삶 삶   >> 27 X 27 음   (), ~ ~ ~ ~ ~ ~ 2	
2.         Time         Source         Destination         Protocol Info           1.0.000000         HordLast         ARP         Moho has 192.168.0.17         Tell 192.168.0.114           2.0.004081         D-Link_Ob:22:ba         HonHaiPr_6e:8b:24         ARP         192.168.0.1         is at 00:13:46:0b:22:ba           Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)         Arrival Time: oc. 11, 2006 04:59:22.880651000 Seconds         Is at 00:13:46:0b:22:ba           Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)         Arrival Time: oc. 11, 2006 04:59:22.880651000 Seconds           [Trime delta from previous captured frame: 0.00000000 seconds]         Is at 165780762.880651000 seconds           [Trime delta from previous captured frame: 0.000000000 seconds]         Is at at a from previous captured frame: 0.000000000 seconds]           [Trime delta from previous captured frame: 0.000000000 seconds]         Is at at a from previous captured frame: 0.00000000 seconds]           [Trime since reference or first frame: 0.000000000 seconds]         Is at at a from previous captured frame: 0.000000000 seconds]           [Trame is marked: ralse]         [Protoci Inf Frame: stars 17 at 30.00000000 seconds]           [Trame is marked: ralse]         [Frame is informed: ralse]           [Protoci In frame: etherapt         155874 (00:150:ce:68:8b:24), 051: Broadcast (ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:	Filter:   Filter:   Expression Clear Apply	
<pre>1 0.000000 HomHaiPr_Ge:8b:24 Broadcast ARP who has 192.168.0.17 Tell 192.168.0.114 2 0.004081 D-Link_Ob:22:ba HomHaiPr_Ge:8b:24 ARP 192.168.0.1 is at 00:13:46:0b:22:ba Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) Arrival Time: Dec II, 2006 04:59:22.880651000 [EME] (EMENDED) Epoch Time: 1165780762.880651000 [EME] (EMENDED) Epoch Time: 11678780762.880651000 [EME] (EMENDED) Epoch Time: 11678780762.880651000 [EME] (EMENDED) Epoch Time: 1167878780782.880651000 [EME] (EMENDED) Epoch Time: 1167878787878787878787878787878787878787</pre>	Io. Time Source Destination Protocol Info	
<pre>20.0040s1 D-LINC_00:22:ba HonHalPF_be:80:24 ARP 192.168.0.1 is at 00:13:46:00:22:ba Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) Arrival Time: Dec 11, 2006 04:59:22.880651000 [mm (Immun) Arrival Time: Dec 11, 2006 04:59:22.880651000 [mm (Immun) Time delta from previous captured frame: 0.00000000 seconds] [Time sine reference or first frame: 0.00000000 seconds] [Tame is imarked: ralse] [Prame is ignored: False] [Prame is ignored: False] [Prate is ignored: False] [Prate is formarked: ralse] [Prate: I, Src: HonHalPF_6e:8b:24 (00:16:ce:6e:8b:24), DSt: Broadcast (ff:ff:ff:ff:ff:ff) Address: Broadcast (ff:ff:ff:ff:ff:ff) Address: Broadcast (ff:ff:ff:ff:ff:ff:ff) Address: Broadcast (ff:ff:ff:ff:ff:ff:ff) Address: Broadcast (ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:</pre>	1 0.000000 HonHaiPr_6e:8b:24 Broadcast ARP who has 192.168.0.17 Tell 192.168.0.114	
<pre>Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) Arrival Time: Dec 11, 2006 04:39:22, 88051000 Execonds [Inde delta from previous captured frame: 0.00000000 seconds] [Time delta from previous captured frame: 0.00000000 seconds] [Time since reference of fisplayed frame: 0.00000000 seconds] [Time since reference of fisplayed frame: 0.00000000 seconds] [Time since of fisplayed frame: 0.00000000 seconds] [Trame Length: 42 bytes (336 bits) [Erame is inarked: ralse] [Prateotis in frame: etharp] Ethernet II, Src: HonHalfPr Ge:8b:24 (00:16:ce:6e:8b:24), Dst: Broadcast (ff:ff:ff:ff:ff:ff:ff:</pre>		
<pre>Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) Arrival Time: Dec 11, 2006 04:59:22, 880651000 [UIII] (UIIII]] Epoch Time: 1165780762, 880651000 seconds [Time delta from previous captured frame: 0.00000000 seconds] [Time since reference or first frame: 0.00000000 seconds] [Frame tameted: False] [Frame tameted: False] [Frame is ignored: False] [Prateous in frame: eth:arp] Ethernet II, Src: HonHaiPr-Ge:80:24 (00:16:ce:6e:8b:24), Dst: Broadcast (ff:ff:ff:ff:ff) Address: Broadcast (ff:ff:ff:ff:ff:ff) address: Broadcast (ff:ff:ff:ff:ff:ff:ff) address: Broadcast (ff:ff:ff:ff:ff:ff:ff:ff) address: Broadcast (ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:</pre>		
Arrival Time: Dec 11, 2006 04:59:22.880651000 [EM] (EMENDER)         Epoch Time: 1165780762.880651000 seconds         [Time delta from previous captured frame: 0.00000000 seconds]         [Time delta from previous displayed frame: 0.00000000 seconds]         [Trame target frame: 10,00000000 seconds]         [Frame tamekd: False]         [Prame ta marked: False]         [Protocols in frame: etc.targ]         Bestination is Broadcast (ff:ff:ff:ff:ff:ff:ff)         Address: Broadcast (ff:ff:ff:ff:ff:ff)         Source: HonHaiPr_6e:8b:24 (00:16:ce:6e:8b:24)		
<pre>Prame 1: 42 bytes on wine (350 bits); 42 bytes taplured (350 bits) Arrival Time: bet 11, 2006 bits); 24 bytes taplured (350 bits) Epoch Time: 1165780762.880651000 Bits); Epoch Time: 1165780762.880651000 Bits); End ta from previous displayed frame: 0.00000000 seconds] [Time detta from previous displayed frame: 0.00000000 seconds] [Time detta from previous displayed frame: 0.00000000 seconds] Frame large Number: 1 Frame target reference or first frame: 0.00000000 seconds] [Time since reference or first frame: 0.00000000 seconds] Frame target reference or first frame: 0.00000000 seconds] Frame target reference or first frame: 0.00000000 seconds] [Time since reference or first frame: 0.00000000 seconds] Frame target reference or first frame: 0.00000000 seconds] Frame target reference or first frame: 0.00000000 seconds] [Trame is marked: False] [Frame is marked: False] [Frame is marked: False] [Protocols in frame: eth:arg] Ethernet II. Src: Hondwing feeRbiz4 (00:16:ce:6e:8b:24), bst: Broadcast (ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:</pre>	- France 1, 12 losses an oder (226 loss). 12 losses entroned (226 loss)	
Epoch Time: 1165780762.880651000 seconds         [Time delta from previous captured frame: 0.00000000 seconds]         [Time since reference or first frame: 0.00000000 seconds]         Frame Number: 1         Frame Length: 42 bytes (336 bits)         Capture Length: 42 bytes (336 bits)         [Irame is ignored: False]         [Prame is ignored: False]         [Prate is in frame: eth:arp]         Ebstinations Broadcast (ff:ff:ff:ff:ff:ff)         Address: Broadcast (ff:ff:ff:ff:ff:ff:ff)         Address: Broadcast (ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:	Arrival Time: Dec 11, 2006 04:59:22.880651000 [[[[] ([[[[[[]]]])	
<pre>[Time deita from previous captured frame: 0.00000000 seconds] [Time deita from previous displayed frame: 0.00000000 seconds] [Time since reference or first frame: 0.00000000 seconds] [Frame since reference or first frame: 0.00000000 seconds] [Frame is marked: False] [Frame is marked: False] [Frame is marked: False] [Protocols in frame: eth:arp] Ethernet II, Src: HonHairF.Ges&amp;B:24 (00:16:ce:6e:8b:24), Dst: Broadcast (ff:ff:ff:ff:ff:ff)</pre>	Epoch Time: 1165780762.880651000 seconds	
<pre>time since ref profiles first firmme: 0.00000000000000000000000000000000000</pre>	[Time delta from previous captured frame: 0.00000000 seconds]	
Frame Number: 1         Frame Number: 1         Frame Number: 1         Frame Length: 42 bytes (336 bits)         Capture Length: 42 bytes (336 bits)         [Frame is marked: False]         [Frame is marked: False]         [Protocols in frame: ethicarp]         Obstinations Broadcast (ff:ff:ff:ff:ff:ff)         Address: Broadcast (ff:ff:ff:ff:ff:ff:ff)         Source: unnalPr_SetBb:24 (00:16:ce:66:8b:24)         Source: unnalPr_SetBb:24 (00:16:ce:66:8b:24)         address: HonHaifF (setBb:24 (setBb:24)         address: Hon	[Time derica from previous displayed frame: 0.00000000 seconds]	
<pre>Frame Length: 42 bytes (336 bits) [Frame is marked: False] [Frame is marked: False] [Frame is inpred: False] [Protocols in frame: eth:arp] Ethernet II, Src: HonHairF.Ges&amp;B:24 (00:16:ce:6e:8b:24), Dst: Broadcast (ff:ff:ff:ff:ff) Destination: Broadcast (ff:ff:ff:ff:ff) Address Broadcast (ff:ff:ff:ff) = TG bit: Group address (multicast/broadcast)</pre>	Frame Number: 1	
Capture Length: 42 bytes (36 bits) [Frame is ignored: FAISe] [Frame is ignored: FAISe] [Frame is ignored: FAISe] [Frame is in frame: ether.arg) Ethernet II, Src: HonMair_Ge:Bb:(40):IS:ce:Ge:Bb:24), Dst: Broadcast (ff:ff:ff:ff:ff:ff) Address: Broadcast (ff:ff:ff:ff:ff) Address: HonMair_Ge:Bb:24 (00:IS:ce:Ge:Bb:24) Address: HonMair_Ge:Bb:24 (00:IS:ce:Ge:Bb:24) 	Frame Length: 42 bytes (336 bits)	
<pre>[Frame is Markeu, Faise] [Frame is fighted to be added to be</pre>	Capture Length: 42 bytes (336 bits)	
<pre>[Protocols in frame: eth:arp] Ethernet II. Src: HowHairn GesBb:24 (00:16:ce:6e:8b:24), bst: Broadcast (ff:ff:ff:ff:ff:ff) Destination: Broadcast (ff:ff:ff:ff:ff:ff) Address: Broadcast (ff:ff:ff:ff:ff) </pre>	LFrame is marked: False]	
<pre>Ethernet II, Src: HomHairr_Ge:Bb:24 (00:16:cc:6c:Bb:24), Dst: Broadcast (ff:ff:ff:ff:ff:ff) Destination: Broadcast (ff:ff:ff:ff:ff:ff:ff)</pre>	[Protocols in frame: eth:arp]	
□ Destination: Broadcast (ff:ff:ff:ff:ff:ff) Address: Broadcast (ff:ff:ff:ff:ff:ff) 	Ethernet II, Src: HonHaiPr_6e:8b:24 (00:16:ce:6e:8b:24), Dst: Broadcast (ff:ff:ff:ff:ff:ff)	
Address: Broadcast (f:f:f:f:f:f:f:f:f:f:f:f:f:f:f:f:f:f:f:	Destination: Broadcast (ff:ff:ff:ff:ff:ff)	
<pre></pre>	Address: Broadcast (ff:ff:ff:ff:ff:ff)	
Source: HonHaiPr_Set8b24 (00:15:ce:6e:8b:24) Address: HonHaiPr_GebB24 (00:15:ce:6e:8b:24) 0		
Address: HomHaiPr_Ge:8b:24 (00:16:ce:6e:8b:24)        0      0        0	Source: HonHaipr. 6e:8b:24 (00:16:ce:6e:8b:24)	
I G bit: Individual address (unicast) 	Address: HonHaiPr_6e:8b:24 (00:16:ce:6e:8b:24)	
	0 = IG bit: Individual address (unicast)	
Iype: AAP (UXOBOD) Address Resolution Protocol (request) Hardware type: IP (UXOBOD) Protocol type: IP (UXOBOD)		
Hardware type: Ethernet (0x0001) Protocol type: IP (0x0800)	IVPE: ARP (UXU806) Address Pesolution Protocol (request)	
Protocol type: IP (0x0800)	Hardware type: Ethernet (0x001)	
	Protocol type: IP (0x0800)	
	010 08 00 06 04 00 01 00 16 <u>ce 6e 8b 24 c0 a8 00 72</u>	
10 08 00 06 04 00 01 00 16 ce 6e 8b 24 c0 a8 00 72	120 00 00 00 00 00 00 c0 as 00 01	
10 08 00 06 04 00 01 00 16 ce 6e 8b 24 c0 a8 00 72		
10 05 00 06 04 00 01 00 16 ce 6e 8b 24 c0 a8 00 72 20 00 00 00 00 00 00 c0 a8 00 01		
110 08 00 06 04 00 01 00 16 ce 68 8b 24 c0 a8 00 72		
bio os do de da do di do la co año 16 ce de 85 24 co año 072 20 00 00 00 00 00 00 co año 00 01		
110 05 00 06 04 00 01 00 16 ce 6e 8b 24 c0 a8 00 72 20 00 00 00 00 00 00 00 a8 00 01		
bio os do de da do di do fié ce de 85 24 co as do 72 20 00 00 00 00 00 00 co as do 01		
jio jas do de da do di do in co jas do di do di do di do di as do 72 jio joo do do do do do do do do di		
jio os do de do di do fi do di do di do di 26 ce de 85 24 co as do 72	Prome (frame) 43 hitse Packeter 3 Displayed 3 Marked 0 Land times 0/00 000	Profiles Default
100       00 <t< td=""><td>Priame (name), 42 bytes Packets: 2 Displayed: 2 Marked: 0 Load time: 0:00,000</td><td>Prome: Default</td></t<>	Priame (name), 42 bytes Packets: 2 Displayed: 2 Marked: 0 Load time: 0:00,000	Prome: Default

#### DHCP

#### • Discover $\Rightarrow$ Offer $\Rightarrow$ Request $\Rightarrow$ ACK

dhcp.pcap

	p.pcap - wiresi				
Elle	Edit <u>V</u> iew <u>G</u> o	<u>Capture</u> Analyze	Statistics Telephony Tools	, Help	
<b>e</b> i		🖻 🛃 🗙 😂 🗧	🔍 🗢 🛸 🌍 ዥ 👱	🗏 📑   Q, Q, Q, 💟   🕷 🗹 🥵 %   📜	
Filter:			-	Expression Clear Apply	
	Time	Course	Destination	Purchased to fa	
10.	1 0 000000	Source	255 255 255 255	Protocol Info DHCPDHCP_DiscoverTransaction_TD_0x3d1d	
	2 0.000295	192.168.0.1	192.168.0.10	DHCP DHCP Offer - Transaction ID 0x3d1d	
	3 0.070031	0.0.0.0	255.255.255.255	DHCP DHCP Request - Transaction ID 0x3dle	
_	4 0.0/0345	192.168.0.1	192.168.0.10	DHCP DHCP ACK - Transaction ID 0x3dle	
e Fra Eth D S	ume 1: 314 b hernet II, S kestination: Address: B 1 cource: Gran Address: G	ytes on wire (251 rc: grandstr_01.f Broadcast (ff:ff roadcast (ff:ff: dstr_01:fc:42 (00 randstr_01:fc:42	<pre>2 bits), 314 bytes cap c:42 (00:0b:82:01:fc:4 :ff:ff:ff:ff)  = IG bit: Group add  = LG bit: Locally ? :0b:82:01:fc:42) (00:0b:82:01:fc:42) = TG bit: Tofdidius</pre>	stured (2512 bits) 12), DSt: Broadcast (ff:ff:ff:ff:ff;ff) dress (multicast/broadcast) administered address (this is NOT the factory default) al address (unicast)	
	0.		= LG bit: Globally	unique address (factory default)	
т	ype: IP (Ox	0800)			
E Int Use	ernet Proto Protagram	col, Src: 0.0.0.0 Protocol. Src Por	(0.0.0.0), Dst: 255.2 t: bootpc (68), Dst Pc	255.255.255 (255.255.255.255) ort: bootps (67)	
Boo	tstrap Prot	oco1			
200	ff ff ff ff f	F ff ff 00 0b 82	01 fc 42 08 00 45 00	D C	
000 010	ff ff ff ff ff 01 2c a8 36	ffff000b 82 50000fa11 17	01 fc 42 08 00 45 00 8b 00 00 00 00 ff ff	······	
000 010 020 030	ff ff ff ff ff 01 2c a8 30 ff ff 00 44 3d 1d 00 00	F ff ff 00 0b 82 5 00 00 fa 11 17 4 00 43 01 18 59 0 00 00 00 00 00 00	01 fc 42 08 00 45 00 8b 00 00 00 00 ff ff 1f 01 01 06 00 00 00 00 00 00 00 00 00 00 00 01 fc 10 00 00 00 00 00		
000 010 020 030 040 050	ff ff ff ff ff 01 2c a8 36 ff ff 00 44 3d 1d 00 00 00 00 00 00 00 00 00 00	f ff ff 00 0b         82           5 00 00 fa 11         17           4 00 43 01 18         59           0 00 00 00 00         00           0 00 00 00 00         00           0 00 00 00 00         00           0 00 00 00 00         00	01 fc 42 08 00 45 00 8b 00 00 00 00 ff ff 1f 01 01 06 00 00 00 00 00 00 00 00 00 00 01 fc 42 00 00 00 00 00 00 00 00 00 00		
0000 010 020 030 040 050 060	ff ff ff ff ff 01 2c a8 36 ff ff 00 44 3d 1d 00 00 00 00 00 00 00 00 00 00 00 00 00	ff         ff         f0         00         82           5         00         00         fa         11         17           4         00         43         01         18         59           0         00         00         00         00         00           0         00         00         00         00         00           0         00         00         00         00         00           0         00         00         00         00         00	01 fc 42 08 00 45 00 8b 00 00 00 00 ff ff 1f 01 01 06 00 00 00 00 00 00 00 00 00 00 01 fc 42 00 00 00 00 00 00 00 00 00 00 00 00 00	······	
0000 010 020 030 040 050 060 070 0800	ff ff ff ff ff 01 2c a8 36 ff ff 00 44 3d 1d 00 00 00 00 00 00 00 00 00 00 00 00 00	f         ff         ff         00         00         82           5         00         00         fa         11         17           4         00         43         01         18         59           0         00         00         00         00         00         00           0         00			
0000 0010 0020 0040 0050 0060 0070 0080 0090 00a0	ff         ff<	fffff000b         82           5000fa11         17           40043018         59           000000000000000000000000000000000000			
0000 0010 0020 0030 0040 0050 0050 0050 0050 0080 0090 0080 008	ff         ff         ff         ff         ff         ff         ff         00         43         1d         00<	fffff000b         82           5000         fall         11         17           4004301         118         59         0000         0000         0000           00000         00000         00000         000000         00000000         00000000         0000000000         0000000000         0000000	$\begin{array}{cccccccccccccccccccccccccccccccccccc$		
0000 0010 0020 0030 0050 0050 0050 0050 0050 005	ff         ff         ff         ff         ff         ff         ff         f0         44           3d         1d         00 </td <td>F ff ff 00         0b         82           5 00         00         fa         11         15           00         00         00         fa         11         15           00         00         00         00         60         60           00         00         00         00         60         60           00         <t< td=""><td><math display="block">\begin{array}{cccccccccccccccccccccccccccccccccccc</math></td><td></td><td></td></t<></td>	F ff ff 00         0b         82           5 00         00         fa         11         15           00         00         00         fa         11         15           00         00         00         00         60         60           00         00         00         00         60         60           00 <t< td=""><td><math display="block">\begin{array}{cccccccccccccccccccccccccccccccccccc</math></td><td></td><td></td></t<>	$\begin{array}{cccccccccccccccccccccccccccccccccccc$		

#### DNS

#### ● UDP でダメなら TCP

#### • dns.pcap

dns.pcap - Wiresha	ırk				
Eile Edit View G	o <u>C</u> apture <u>A</u> nalyze §	Statistics Telephony Tools	Help		
	🖻 🖬 🗙 😂 🗛	🔍 🗢 🔿 🐺 生		A Q Q M A M M M 🕺 🕺	
Filter:		•	Express	ion Clear Apply	
No. Time	Source	Destination	Protoco	l Info	
1 0.000000	192.168.0.114	205.152.37.23	DNS	Standard query A chrissanders.org	
2 0.112121	205.152.37.23	192.168.0.114	DNS	Standard query response A 208.113.140.24	
3 0.112534	192.168.0.114	208.113.140.24	TCP	ni-visa-remote > http [SYN] Seq=0 Win=16384 Len=0 MSS=3	1460 SACK_PERM=1
5 0 193110	192 168 0 114	208 113 140 24	TCP	<pre>ni_visa_remote &gt; http [ACK] Seq=0 ACK=1 Win=3840 t ni_visa_remote &gt; http [ACK] Seq=1 Ack=1 Win=17424 Len=(</pre>	) ) MSS=1452 SACK_PERM=1
6 0.193191	192.168.0.114	208.113.140.24	HTTP	GET / HTTP/1.1	
7 0.288670	208.113.140.24	192.168.0.114	TCP	http > ni-visa-remote [ACK] Seq=1 Ack=553 Win=6624 Len=	=0
8 0.978498	208.113.140.24	192.168.0.114	TCP	[TCP segment of a reassembled PDU]	
9 0.978909	208.113.140.24	192.168.0.114	TCP	[TCP segment of a reassembled PDU]	1.00-0
11 1. 068387	208 113 140 24	192,168,0,114	TCP	TCP segment of a reassembled PDU1	Len=o
12 1.072204	208.113.140.24	192.168.0.114	TCP	[TCP segment of a reassembled PDU]	
Header lengt Differentiat Total Length Identificati Fragment off Time to live Protocol: UD Header check Source: 205. Destination USer Datagram Source port Length: 58 @ Checksum: 0 Domain Name Sj	h: 20 bytes ed Services Field :: 78 on: 0xd758 (55128; (Don't Fragment) :set: 0 :: 50 PP (17) Isum: 0xbd7c [corr: 192.168.0.114 (1) Protocol, 5rc Porr domain (53) port: polestar (10 :gdf5 [validation rstem (response)	: 0x00 (DSCP 0x00: Def ) act] 2.37.23) 22.168.0.114) 2: domain (53), Dst Pe 0560) jisabled]	ault; i	ECN: 0x00) lestar (1060)	
0000 00 16 ce 6 0010 00 46 07 5 0020 00 72 00 3 0030 00 01 00 0 0040 65 72 73 0 0050 00 01 00 0	e         8b         24         00         05         5d           8         40         00         32         11         bd           5         04         20         32         31         bd           0         00	21 99 4c 08 00 15 00 7c cd 95 25 17 cd a8 75 64 08 18 00 01 72 69 73 73 61 6e 64 01 00 01 cd 0c 00 01 71 8c 18		S. ].L S 	
Internet Protocol #	(ip), 20 bytes	Packets: 249 Displayed: 24	) Marked:	0 Load time: 0:00.005	Profile: Default

#### TCP

## ● セッション確立 ⇒ 3 Way Handshake ● セッション切断 ⇒ FIN / RESET

http.pcap

📶 http	.pcap - Wiresha	ırk								X
Eile E	<u>E</u> dit <u>V</u> iew <u>G</u> o	<u>Capture</u> Analyze	Statistics Telephony Tools	<u>H</u> elp						
		🖻 🖥 🗶 😂 🖴	🔍 🌞 🛸 🎝 🚡 🚣		)		🗸 🖂 🥵 💥 i 😫			
Filter:			-	Expressio	on Clear A	oply				
No.	Time	Source	Destination	Protocol	Info					
	1 0.000000	145.254.160.237	65.208.228.223	TCP	tip2 > htt	[SYN]	Seq=0 Win=8760 L	en=0 MSS=1460 SACK_P	ERM=1	
	2 0.911310	65.208.228.223	145.254.160.237	TCP	http > tip	2 [SYN,	ACK] Seq=0 Ack=1	L Win=5840 Len=0 MSS=	1380 SACK_PERM=1	=
	3 0.911310	145.254.160.237	65.208.228.223	TCP	tip2 > htt	D [ACK]	Seq=1 Ack=1 Win-	-9660 Len=0		
	4 0.911310	145.254.160.237	65.208.228.223	HTTP	GET /down1	oad.htm	1 HTTP/1.1			
	5 1.472116	65.208.228.223	145.254.160.237	TCP	http > tip	2 [ACK]	Seq=1 Ack=480 W	in=6432 Len=0		
	6 1.682419	65.208.228.223	145.254.160.23/	TCP	LTCP segme	nt of a	reassembled PDU			
	7 1.812000	145.254.160.23/	05.208.228.223	TCP	tip2 > ntt	D LACKJ	Seq=480 ACK=138	L W1N=9660 Len=0		
	9 2 012804	145 254 160 227	65 208 228 222	TCP	tin2 > htt		Sec-180 Ack-2761	   win=9660   en=0		
1	0 2 443513	65 208 228 223	145 254 160 237	TCP	TCP segme	of of a	reassembled PDU	l will-sooo Lell-o		
1	1 2.553672	65,208,228,223	145,254,160,237	TCP	TCP segme	nt of a	reassembled PDU			
1	12 2.553672	145.254.160.237	65.208.228.223	TCP	tip2 > htt	D [ACK]	Seg=480 Ack=5521	L win=9660 Len=0		-
+ Fra	me 1: 62 by	tes on wire (496	Dits), 62 Dytes captur	ed (496	DITS)		666			
Eth Tot	ernet II, S	rc: xerox_00:00:0	160 227 (145 254 160	, DST: TE	e:TT:20:00:0	)1:00 (	(65 208 228 222)	0		
- Int	ernet proto	COI, SEC: 145.254	.100.237 (145.254.100.	237), DS	st: 05.208	28.223	(05.208.228.223)			
	ersion: 4	by 20 byter								
	ifforontiat	n: 20 bytes od Sonvisos Fiold	· 0×00 (DECD 0×00) Dof	Equilty Fo						
	otal Longth	• 49	. 0x00 (DSCF 0x00. DEI	aure, et	LN. 0X00)					
-	dentificati	001: 000E41 (2005)								
	lags: 0x02	(Don't Fragment)								
	ragment off	set: 0								
Ť	ime to live	128								
P	rotocol: TC	P (6)								
ΞH	eader checks	sum: 0x91eb [corr	ect]							
S	ource: 145.3	254.160.237 (145.)	254.160.237)							
D	estination:	65.208.228.223 (	65.208.228.223)							
🗆 Tra	nsmission Co	ontrol Protocol, :	Src Port: tip2 (3372),	, Dst Por	rt: http (8	)), Seq	: 0, Len: 0			
5	ource port:	tip2 (3372)								
D	estination p	port: http (80)								
0	Stream inde	x: 0]								
S	equence num	ber: 0 (relati	ve sequence number)							
н	leader lengt	h: 28 bytes								
🕀 F	lags: 0x02	(SYN)								
W	indow size:	8760								
E C	necksum: Ox	C30C [validation	disabledj							
• 0	perions: (8 )	byces)								
0000	fe ff 20 00	01 00 00 00 01	00 00 00 08 00 45 00		E.					
0010	00 30 Of 41	40 00 80 06 91	eb 91 fe a0 ed 41 d0	.0.A@.	A.					
0020	e4 df 0d 2d	: 00 50 38 at te		P	<sup>9</sup> 8					
0050	22 58 65 00	. 00 00 02 04 03	D4 01 01 04 02	0						
_										
Flag	gs (tcp.flags), 2	bytes	Packets: 43 Displayed: 43 M	farked: 0 L	.oad time: 0:00	.015			Profile: Default	

#### HTTP

## ●テキスト ベースのプロトコル ●HTTP レベルのキャプチャなら Wireshark

を使わずとも.....

http.pcap

M http.pcap - Wireshark		
Elle Edit View Go Capture Analyze Statistics Telephony Tool	Help	
Filter:	Expression Clear Apply	
No. Time Source Destination	Protocol Info	A
1 0.000000 145.254.160.237 65.208.228.223	TCP tip2 > http [SYN] Seq=0 Win=8760 Len=0 MSS=1460 SACK_F	1280 SACK DEDM 1
3 0.911310 145.254.160.237 65.208.228.223	TCP tip2 > http [ACK] Seq=0 ACK=1 Win=3840 Len=0 MSS=	ISOU SACK_PERMEI
4 0.911310 145.254.160.237 65.208.228.223	HTTP GET /download.html HTTP/1.1	
5 1.472116 65.208.228.223 145.254.160.237	TCP http > tip2 [ACK] Seq=1 Ack=480 Win=6432 Len=0	
6 1.682419 65.208.228.223 145.254.160.237 7 1 812606 145 254 160 227 65 208 228 223	TCP [TCP segment of a reassembled PDU]	
8 1.812606 65.208.228.223 145.254.160.237	TCP [TCP segment of a reassembled PDU]	
9 2.012894 145.254.160.237 65.208.228.223	TCP tip2 > http [ACK] Seq=480 Ack=2761 Win=9660 Len=0	
10 2.443513 65.208.228.223 145.254.160.237	TCP [TCP segment of a reassembled PDU]	
11 2.553672 65.208.228.223 145.254.160.237	TCP [TCP segment of a reassembled PDU]	
12 2.5550/2 145.254.100.25/ 05.208.228.225	Ter Cipz > heep [Ack] Seq=400 Ack=5521 With=5000 Een=0	•
■ Frame 4: 533 bytes on wire (4264 bits), 533 bytes ca ■ Thermat II Case Yearey 00:00:00 (00:00:01:00:00:00)	ptured (4264 bits)	*
Ethernet II, SrC: Xerox_00:00:00 (00:00:01:00:00:00)	237) DST: 65 208 228 223 (65 208 228 223)	
Transmission Control Protocol. Src Port: tip2 (3372)	. Dst Port: http (80). Seg: 1. Ack: 1. Len: 479	
Source port: tip2 (3372)		
Destination port: http (80)		
[Stream index: 0]		
[Next sequence number: 480 (relative sequence n	umber )]	
Acknowledgement number: 1 (relative ack number)		
Header length: 20 bytes		
		=
Window Size: 9660 Checksum: 0x2058 [validation disabled]		
[SEO/ACK analysis]		
Hypertext Transfer Protocol		
GET /download.html HTTP/1.1\r\n		
Host: www.ethereal.com/r/n	L op US, mul 5), cosko (20040112) n) n	
Accept: text/xml.application/xml.application/xhtml	<pre>xml.text/html:g=0.9.text/plain:g=0.8.image/png.image/ipeg.image/</pre>	ne/aif:a=0.2.*/*:a=0.1\r\n
Accept-Language: en-us,en;g=0.5\r\n		
Accept-Encoding: gzip,deflate\r\n		
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n		
Keep-Alive: 300\r\n Connection: keep-alive\r\n		
connection, keep-arrive (r (n		÷
0030 25 bc a9 58 00 00 47 45 54 20 2f 64 6f 77 6e 6c	%XGE T /downl	A.
0050 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 65 74 68	1Host: www.eth	
0060 65 72 65 61 6c 2e 63 6t 6d 0d 0a 55 73 65 72 2d 0070 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35	ereal.co mUser-	
0080 2e 30 20 28 57 69 6e 64 6f 77 73 3b 20 55 3b 20	.0 (Wind ows; U;	=
0090 57 69 6e 64 6f 77 73 20 4e 54 20 35 2e 31 3b 20 00a0 65 6e 2d 55 53 3b 20 72 76 3a 31 2e 36 29 20 47	Windows NT 5.1; en-US: r v:1 6) 6	
00b0 65 63 6b 6f 2f 32 30 30 34 30 31 31 33 0d 0a 41	ecko/200 40113A	
00c0 63 63 65 70 74 3a 20 74 65 78 74 2f 78 6d 6c 2c	ccept: t ext/xml, applicat ion/xml	
00e0 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d	applicat ion/xhtm	
0010 6c 2b 78 6d 6c 2c 74 65 78 74 2f 68 74 6d 6c 3b 0100 71 3d 30 2e 39 2c 74 65 78 74 2f 70 6c 61 69 6e	I+xmI,te xt/html; g=0.9.te xt/plain	
0110 3b 71 3d 30 2e 38 2c 69 6d 61 67 65 2f 70 6e 67	:a=0.8.i mage/png	*
Text item (text), 29 bytes Packets: 43 Displayed: 43 I	Aarked: 0 Load time: 0:00.015	Profile: Default

#### FTP

# ○これもテキストベースのプロトコル ○ユーザー名/パスワードは平文(-\_-;)

ftp.pcap

📶 ftp.pcap - Wireshar	k		
<u>File Edit View G</u> o	o <u>C</u> apture <u>A</u> nalyze <u>S</u>	tatistics Telephony <u>T</u> ools	Help
	🖻 🖥 🗶 😂 🖴	। 🔍 🗢 🛸 🥥 暮 👱	। 🗐 🗐 । Q. Q. Q. 🗹 । 👹 🖾 🍕 % । 💢
Filter:		•	Expression Clear Apply
No. Time	Source	Destination	Protocol Info
1 0.000000	192.168.0.114	192.168.0.193	TCP trim > ftp [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
2 0.002319	192.168.0.193	192.168.0.114	TCP ftp > trim [SYN, ACK] Seq=0 Ack=1 win=16384 Len=0 MSS=1452 SACK_PERM=1
3 0.002338	192.168.0.114	192.168.0.193	TCP trim > ftp [ACK] seq=1 Ack=1 win=17424 Len=0
4 0.004399	192.168.0.193	192.168.0.114	FTP Response: 220 Chris Sanders FTP Server
5 0.005259	192.168.0.114	192.168.0.193	FTP Request: USER csanders
6 0.006560	192.168.0.193	192.168.0.114	FTP Response: 331 Password required for csanders.
7 0.007647 8 0.000026	192.108.0.114	102.108.0.195	FTP Request: PASS echo
9.0.010088	192.108.0.114	192.108.0.114	ETP Deguise: Syst
10 0 011397	192 168 0 193	192 168 0 114	ETP Desnorse 215 UNTY Type 18
11 0.011529	192,168,0,114	192.168.0.193	FTP Request: FFAT
12 0.013500	192.168.0.193	192.168.0.114	FTP Response: 211-Extensions supported:
<ul> <li>■ Ethernet II, S</li> <li>■ Internet Proto</li> <li>■ Internet Proto</li> <li>■ Transmission C</li> <li>Source port:</li> <li>Destination</li> <li>[Stream inde Sequence num</li> <li>[Next sequen</li> <li>Acknowledgem</li> <li>Header lengt</li> <li>■ Flags: 0x18</li> <li>■ GisQAcK ana</li> <li>■ Flie Transfer</li> <li>■ PASS echo\r\ Request or Request or</li> </ul>	rc: HonHaiPr_Ge:Bb col, src: 192.168. ontrol Protocol, s trim (1137) port: ftp (21) x: 0] ber: 16 (relati ce number: 168 (relatice construction) ent number: 68 h: 20 bytes (PSH, ACK) 17357 e36b (validation d lysis] Protocol (FTP) n mmand: PASS g; echo	:24 (00:16;ce:de:bb:2 0.114 (192;CB.0.114) rc Port: trim (1137), ve sequence number) relative sequence num (relative ack number) isabled]	4), Dsr: Asujtekc_40:76:ef (00:15:f2:40:76:ef) , Dsr: 192.168.0133 (192.168.0133) Dst Port: ftp (21), seq: 16, Ack: 68, Len: 11 ber)]
0000 00 15 f2 4 0010 00 33 a7 e 0022 00 c1 04 7 0030 43 cd e9 6 0040 0a	0 76 ef 00 16 ce 6 40 00 80 06 d0 9 1 00 15 df b3 b3 0 0 00 00 50 41 53 9	6e 8b 24 08 00 45 00 5a c0 a8 00 72 c0 a8 De c6 c7 01 85 50 18 53 20 65 65 65 68 67 0d	@vn.S.E. 3@vZ.vr. q

#### Telnet

# ●またまたテキストベース ●ユーザー名/パスワードは平文(-\_-;)

telnet.pcap

📶 telne	t.pcap - Wiresh	ark				
Eile E	dit ⊻iew <u>G</u> o	Capture Analyze Sta	atistics Telephony <u>T</u> ools	Help		
	M 10 10	🖹 🖌 🎜 🖥	् 🗢 🛸 🍄 🛧 🚣		)  0, 0, 0, 12   👪 🖻 畅 %   😫	
Filter:			•	Expressi	on Clear Apply	
No.	Time	Source	Destination	Protocol	Info	A
	1 0.000000	192.168.0.2	192.168.0.1	TCP	3m-image-lm > telnet [SYN] Seq=0 Win=32120 Len=0 MSS=14	460 SACK_PERM=1 TSV=102336
	2 0.002525	192.168.0.1	192.168.0.2	TCP	telnet > 3m-image-Im [SYN, ACK] Seq=0 Ack=1 Win=17376 I	Len=0 MSS=1448 WS=0 TSV=24
	3 0.0025/2	192.168.0.2	192.168.0.1	TCP	3m-1mage-Im > teinet [ACK] seq=1 ACK=1 W1n=32120 Len=0	TSV=10233636 TSER=246/3/2
	5 0 150335	192.108.0.2	192.108.0.1	TELNET	Telnet Data	
	6 0.150402	192.168.0.2	192.168.0.1	TCP	3m-image-lm > telnet [ACK] Seg=28 Ack=4 Win=32120 Len=	0 TSV=10233651 TSER=246737
	7 0.150574	192.168.0.2	192.168.0.1	TELNET	Telnet Data	0 13V-10233031 13EK-240737.
	8 0.151946	192.168.0.1	192.168.0.2	TCP	telnet > 3m-image-lm [ACK] Seg=4 Ack=31 win=17376 Len=	0 TSV=2467372 TSER=1023365
	9 0.153657	192.168.0.1	192.168.0.2	TELNET	Telnet Data	
1	0 0.153865	192.168.0.2	192.168.0.1	TELNET	Telnet Data	
1	1 0.154984	192.168.0.1	192.168.0.2	TCP	telnet > 3m-image-lm [ACK] Seq=29 Ack=95 Win=17312 Len-	=0 TSV=2467372 TSER=102336
1	2 0.155577	192.168.0.1	192.168.0.2	TELNET	Telnet Data	-
E En al	no 1 · 03 hvrt	es on wire (744 bit	ts) 03 bytes captur	od (744	hits)	
E ETh	ernet II. Sr	c: Lite-OnC 3b:bf:1	fa (00:a0:cc:3b:bf:f	a). Dst	: WesternD 9f:a0:97 (00:00:c0:9f:a0:97)	
+ Tht	ernet Protoc	ol. src: 192,168.0.	.2 (192.168.0.2). DS	t: 192.	168.0.1 (192.168.0.1)	
🖃 Tra	smission Co	ntrol Protocol, Sr	c Port: 3m-image-1m	(1550).	Dst Port: telnet (23), Seg: 1, Ack: 1, Len: 27	
5	ource port:	3m-image-lm (1550)		(/,		
D	estination p	ort: telnet (23)				
0	stream index	: 0]				
S	equence numb	er: 1 (relative	sequence number)			
0	vext sequenc	e number: 28 (re	elative sequence num	ber)]		
A	knowledgeme	nt number: 1 (re	elative ack number)			
н	eader length	: 32 bytes				
🗉 F	lags: 0x18 (	PSH, ACK)				_
W	indow size:	32120				=
• C	necksum: 0x6	e67 [validation di	sabled]			
• O	otions: (12	bytes)				
	SEQ/ACK ana I	ysisj				
e ren	iet	uppress co thead				
	ommand: b0 5	Torminal Type				
	mmand: will	Negotiate About W	indow Size			
	ommand: will	Terminal Sneed	Indow Size			
	ommand: will	Remote Flow Contro	റി			
C C	ommand: will	Linemode				
- C	ommand: will	New Environment Or	ption			
c	ommand: Do S	tatus				
			1.5.5.00.00.15.10		-	
0000	00 00 c0 9f	a0 97 00 a0 cc 3b	b b t t a 08 00 45 10	0520	E.	
0020	00 01 06 0e	00 17 99 c5 a0 ed	17 f1 63 3e 80 18	.0F2@	··· ·····D···	
0030	7d 78 6e 67	00 00 01 01 08 0a	a 00 9c 27 24 00 25	}xng.		
0040	a6 2c ff fd	03 ff fb 18 ff fb	o 1f ff fb 20 ff fb	111111		
0050	21 11 10 22	11 10 27 11 TO 05	0 11 10 23			

#### ICMP

#### □ ユーティリティ プロトコル

icmp.pcap

icmp.pcap - Wiresha	ark							[	X
Elle Edit View Go	Capture Analyze Sta	itistics Telephony Iools	Help			<b>7 •</b> 40 1 •	2		
		~~~ <u>~</u>		વિવવ		= 🐝 👋 🗜	8		
Filter:		•	Expression	. Clear Ap	ply				
No. Time	Source	Destination	Protocol Inf	fo		(14.0+0200	see(he/le) 255/1 eel	128)	
2 0.001085	192.168.0.1	192.168.0.114	ICMP EC	ho (ping)	reply	(id=0x0300,	seq(be/le)=256/1, ttl seq(be/le)=256/1, ttl	=128)	
3 0.996773	192.168.0.114	192.168.0.1	ICMP EC	ho (ping)	request	(id=0x0300,	seq(be/le)=512/2, ttl	=128)	
4 0.998983	192.168.0.1	192.168.0.114	ICMP EC	ho (ping)	reply	(1d=0x0300, (id=0x0300	<pre>seq(be/le)=512/2, ttl seq(be/le)=768/3 ttl</pre>	=127) =128)	
6 1.999087	192.168.0.1	192.168.0.114	ICMP EC	ho (ping)	reply	(id=0x0300,	seq(be/le)=768/3, ttl	=127)	
7 2.996840	192.168.0.114	192.168.0.1	ICMP EC	ho (ping)	request	(id=0x0300,	seq(be/le)=1024/4, tt	1=128)	
9 6.134186	192.168.0.114	72.14.207.99	ICMP EC	ho (ping)	request	(id=0x0300,	seq(be/le)=1024/4, tt seq(be/le)=1280/5, tt	1=127)	
10 6.215031	72.14.207.99	192.168.0.114	ICMP EC	ho (ping)	reply	(id=0x0300,	seq(be/le)=1280/5, tt	1=232)	
11 7.135658	192.168.0.114	72.14.207.99	ICMP EC	ho (ping)	request	(1d=0x0300, (id=0x0300)	<pre>seq(be/le)=1536/6, tt seq(be/le)=1536/6, tt</pre>	(1=128) (1=232)	
B Internet Protoc Internet Contro Type: 8 (Echt Code: 0 Checksum: 0x/ Identifier: 0 Sequence num Sequence num B Data (32 bytt Data: 6162( [Length: 32	col, src: 192.168.0. bl Message Protocol o (ping) request) 195c [correct] 2x0300 2ber: 256 (0x0100) 2ber (LE): 1 (0x0001) 2s) 356465666768696a6b66 2]	.114 (192.168.0.114) ) c6d6e6f7071727374757	, Dst: 192	.168.0.1	(192.168.	0.1)			
0000 00 13 46 0b	122 ba 00 16 ce 66	8b 24 08 00 45 00	F. "	.n. SF.					
0010 00 35 89 90 0020 00 01 08 00 0030 00 01 08 00 0030 07 61 62 63	26 00 00 50 01 26 05 49 50 03 00 01 02 60 60 60 67 65 65	20 27 00 072 00 08 0 1 02 03 04 05 04 7 1 72 73 74 75 76	. <i\ ghijkimn wabcdefg</i\ 	hi opgrstuv hi					
O Data (data.data), 3	2 bytes P	ackets: 16 Displayed: 16 M	arked: 0 Load	d time: 0:00.	000			Profile: Default	



# 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/