

Wireshark 入門

キャプチャしたパケットの表示

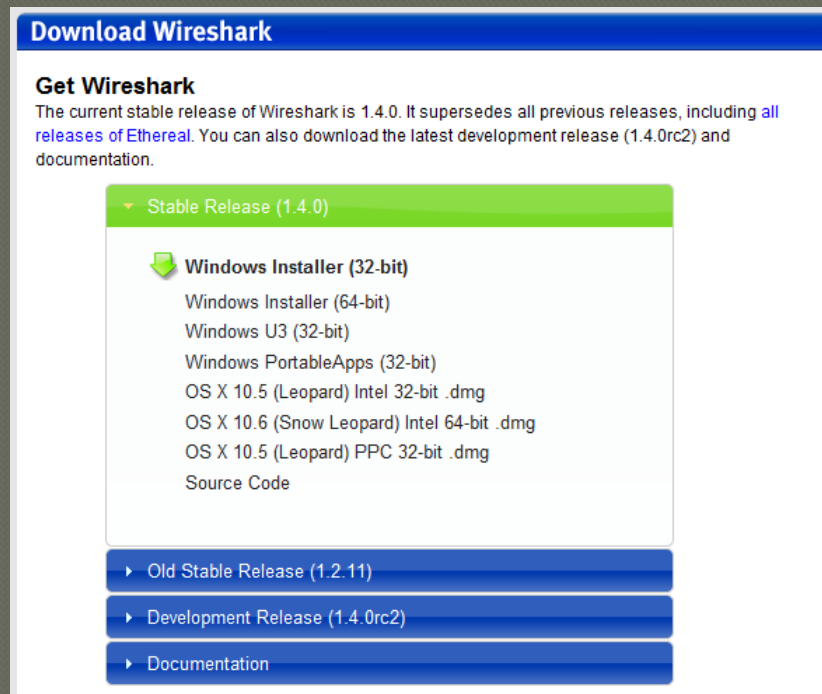
hebikuzure

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/>



The screenshot shows the 'Download Wireshark' page. At the top, there is a blue header with the text 'Download Wireshark'. Below this, the section 'Get Wireshark' is displayed. The text states: '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.' Below the text, there is a green bar with a dropdown arrow and the text 'Stable Release (1.4.0)'. Underneath this bar, a list of download options is shown, including 'Windows Installer (32-bit)', 'Windows Installer (64-bit)', 'Windows U3 (32-bit)', 'Windows PortableApps (32-bit)', 'OS X 10.5 (Leopard) Intel 32-bit .dmg', 'OS X 10.6 (Snow Leopard) Intel 64-bit .dmg', 'OS X 10.5 (Leopard) PPC 32-bit .dmg', and 'Source Code'. At the bottom of the page, there are three blue buttons with white text: 'Old Stable Release (1.2.11)', 'Development Release (1.4.0rc2)', and 'Documentation'.

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.

Stable Release (1.4.0)

- Windows Installer (32-bit)
- Windows Installer (64-bit)
- Windows U3 (32-bit)
- Windows PortableApps (32-bit)
- OS X 10.5 (Leopard) Intel 32-bit .dmg
- OS X 10.6 (Snow Leopard) Intel 64-bit .dmg
- OS X 10.5 (Leopard) PPC 32-bit .dmg
- Source Code

Old Stable Release (1.2.11)

Development Release (1.4.0rc2)

Documentation

注意事項

- ◎ 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

参考情報

- ◎ **How To Set Up a Capture**

<http://wiki.wireshark.org/CaptureSetup>

- ◎ **Security**

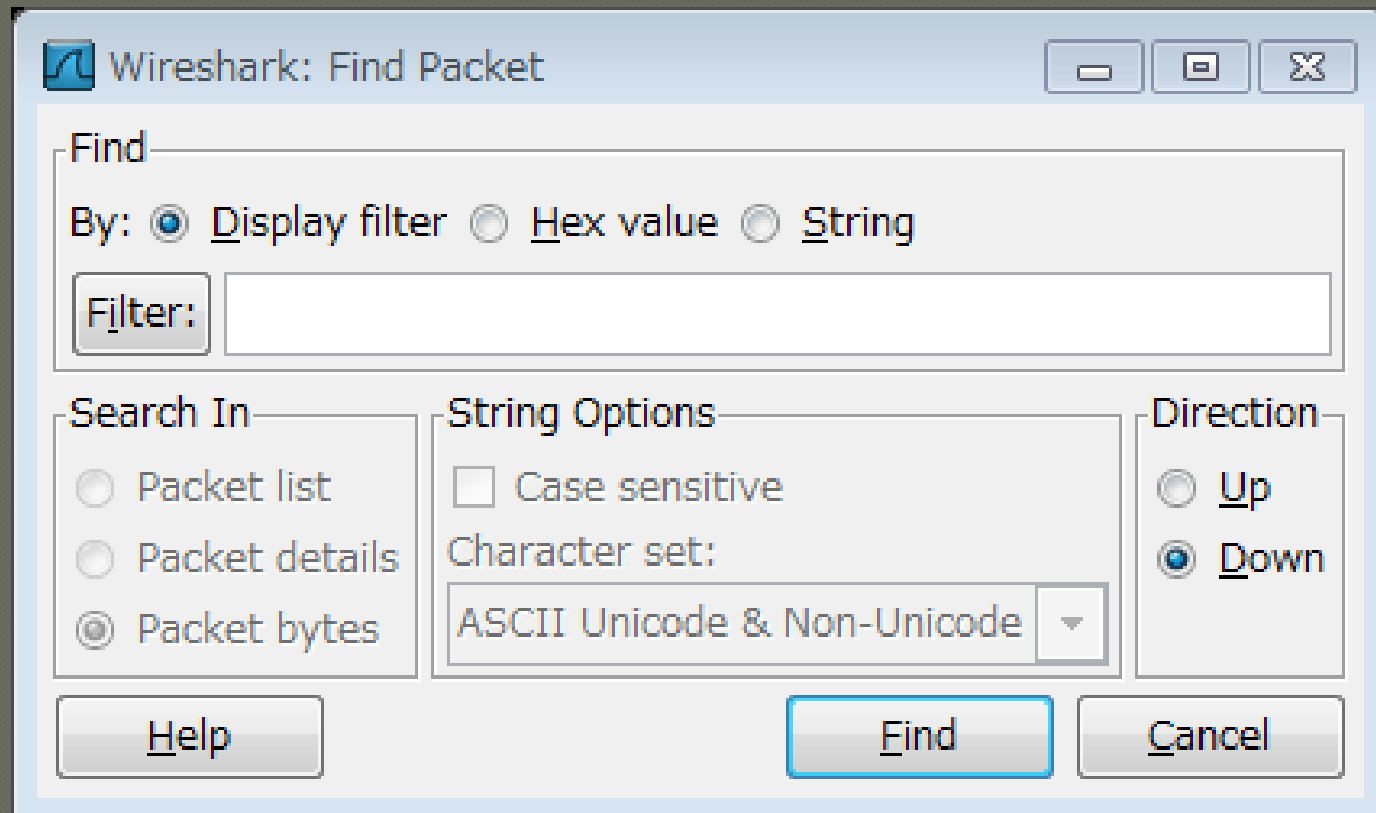
<http://wiki.wireshark.org/Security>

- ◎ **Platform-Specific information about capture privileges**

<http://wiki.wireshark.org/CaptureSetup/CapturePrivileges>

パケットの検索

- [Edit] -> [Find Packet]



時間の表示形式

The screenshot shows the Wireshark interface with the 'View' menu open and 'Time Display Format' selected. The menu lists various time display options and their keyboard shortcuts. The background shows a packet capture with several TCP and HTTP packets.

Option	Shortcut
Date and Time of Day: 1970-01-01 01:02:03.123456	Ctrl+Alt+1
Time of Day: 01:02:03.123456	Ctrl+Alt+2
Seconds Since Epoch (1970-01-01): 1234567890.123456	Ctrl+Alt+3
Seconds Since Beginning of Capture: 123.123456	Ctrl+Alt+4
Seconds Since Previous Captured Packet: 1.123456	Ctrl+Alt+5
Seconds Since Previous Displayed Packet: 1.123456	Ctrl+Alt+6
Automatic (File Format Precision)	
Seconds: 0	
Deciseconds: 0.1	
Centiseconds: 0.12	
Milliseconds: 0.123	
Microseconds: 0.123456	
Nanoseconds: 0.123456789	
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
- ◎ 基準にしたいパッケージをクリックして [Edit] -> [Set Time Reference] (Ctrl + T)
 - 基準にしたパッケージ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

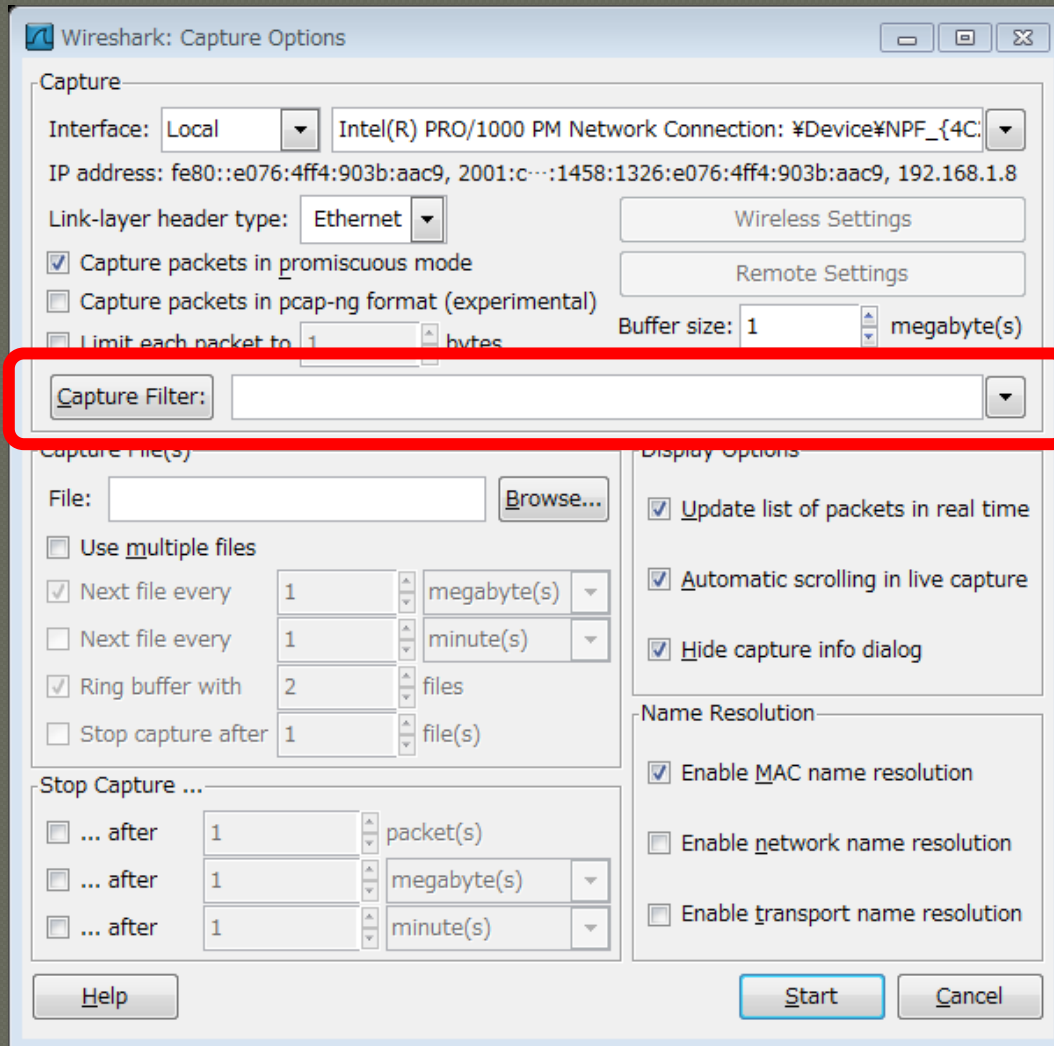
◎ キャプチャ フィルタ

- 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

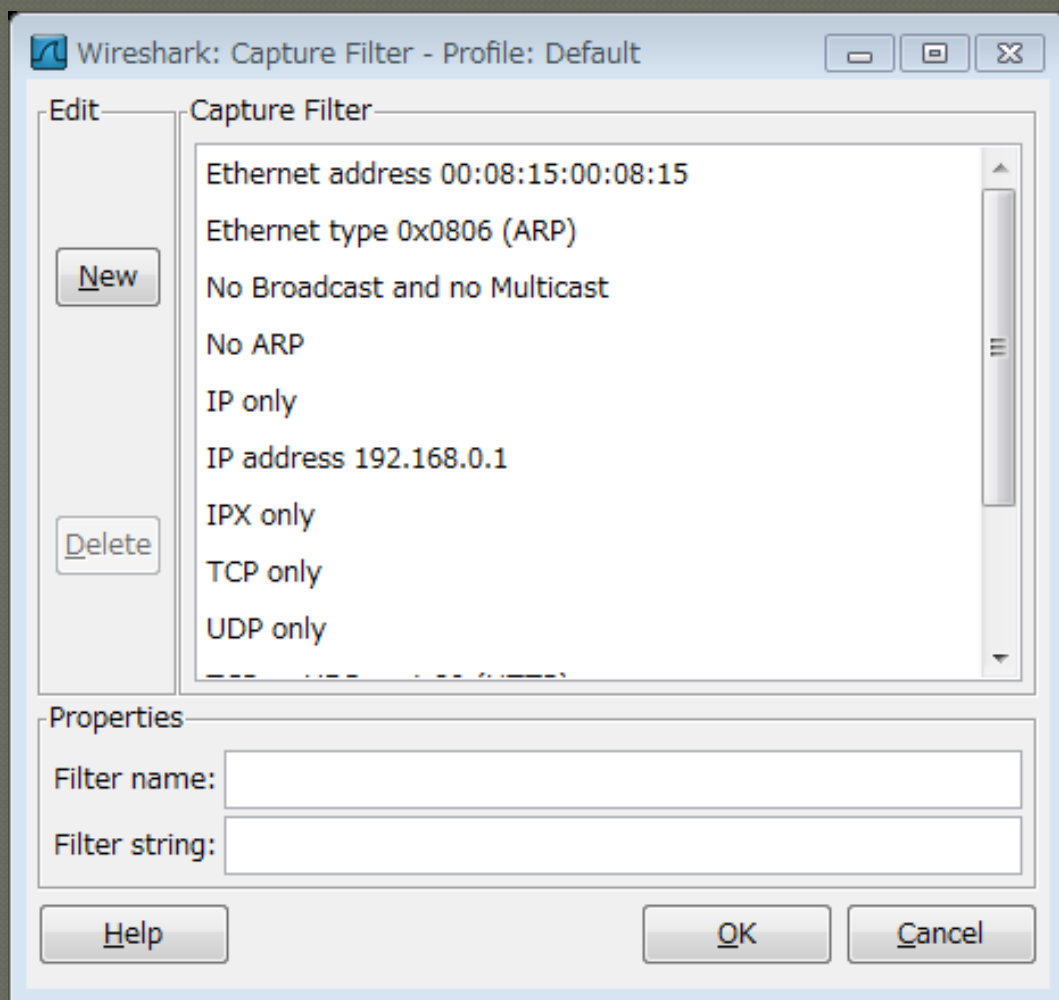
◎ ディスプレイ フィルタ

- 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



キャプチャフィルタの作成



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

2011_02_15.cap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

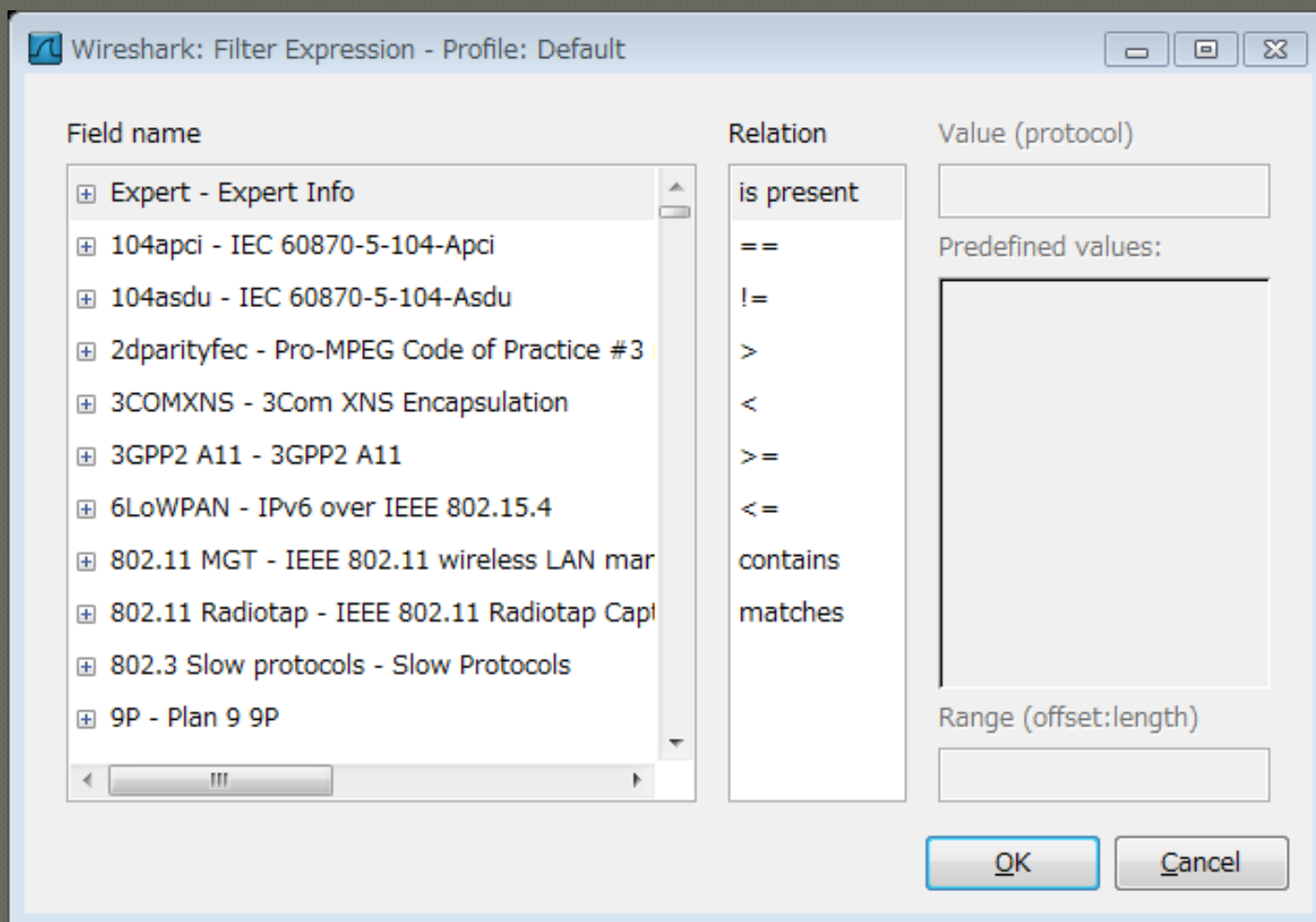
Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
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	TCP	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	TCP	80 > 64697 [ACK] Seq=1 Ack=928 win=7416 Len=0
6	0.067496	211.131.226.15	192.168.1.8	HTTP	HTTP/1.1 200 OK (text/html)
7	0.067496	211.131.226.15	192.168.1.8	HTTP	Continuation or non-HTTP traffic
8	0.067496	211.131.226.15	192.168.1.8	HTTP	Continuation or non-HTTP traffic
9	0.067496	211.131.226.15	192.168.1.8	HTTP	Continuation or non-HTTP traffic
10	0.067496	211.131.226.15	192.168.1.8	HTTP	Continuation or non-HTTP traffic
11	0.067496	211.131.226.15	192.168.1.8	HTTP	Continuation or non-HTTP traffic
12	0.067781	192.168.1.8	211.131.226.15	TCP	64697 > 80 [ACK] Seq=928 Ack=8485 win=65044 Len=0
13	0.077561	211.131.226.15	192.168.1.8	HTTP	Continuation or non-HTTP traffic
14	0.079120	211.131.226.15	192.168.1.8	HTTP	Continuation or non-HTTP traffic
15	0.079120	211.131.226.15	192.168.1.8	HTTP	Continuation or non-HTTP traffic
16	0.079120	211.131.226.15	192.168.1.8	HTTP	Continuation or non-HTTP traffic

Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)

- Ethernet II, Src: AsustekC_cf:be:af (00:13:d4:cf:be:af), Dst: NecAcces_11:a0:0d (00:1b:8b:11:a0:0d)
- Internet Protocol, Src: 192.168.1.8 (192.168.1.8), Dst: 211.131.226.15 (211.131.226.15)
- Transmission Control Protocol, Src Port: 64697 (64697), Dst Port: 80 (80), Seq: 0, Len: 0
 - Source port: 64697 (64697)
 - Destination port: 80 (80)
 - [Stream index: 0]
 - Sequence number: 0 (relative sequence number)
 - Header length: 28 bytes
 - Flags: 0x02 (SYN)
 - window size: 8192
 - Checksum: 0x7766 [validation disabled]
 - Options: (8 bytes)

ディスプレイフィルタの作成



比較演算子

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

論理演算子

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

フィルタの例

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

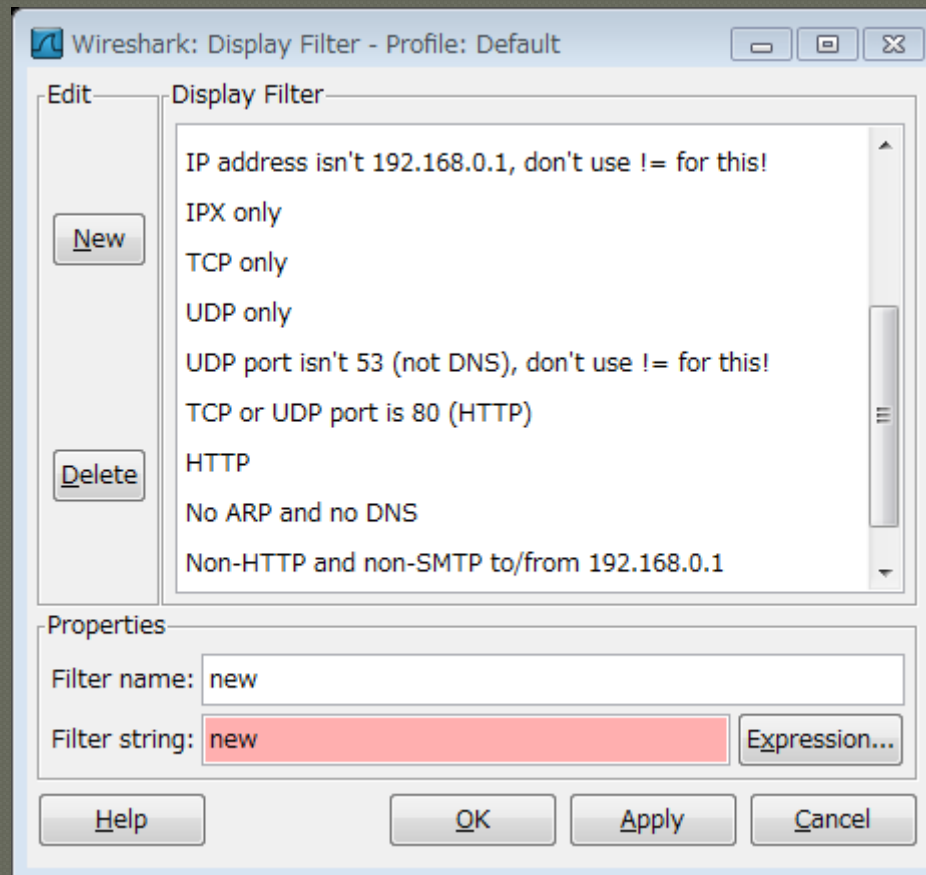
よくある間違い

- ◎ `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]



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.](http://wiki.wireshark.org/DisplayFilters)

Wireshark の名前解決

◎ MAC アドレス

- MAC アドレス ⇒ 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

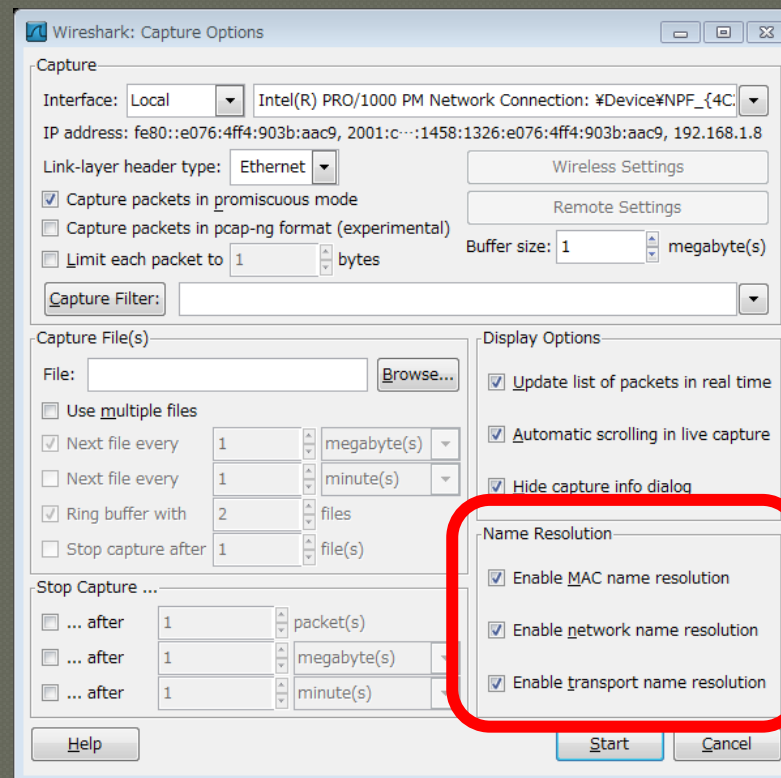
- ポート番号 ⇒ プロトコル名 (well-known ports)

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）

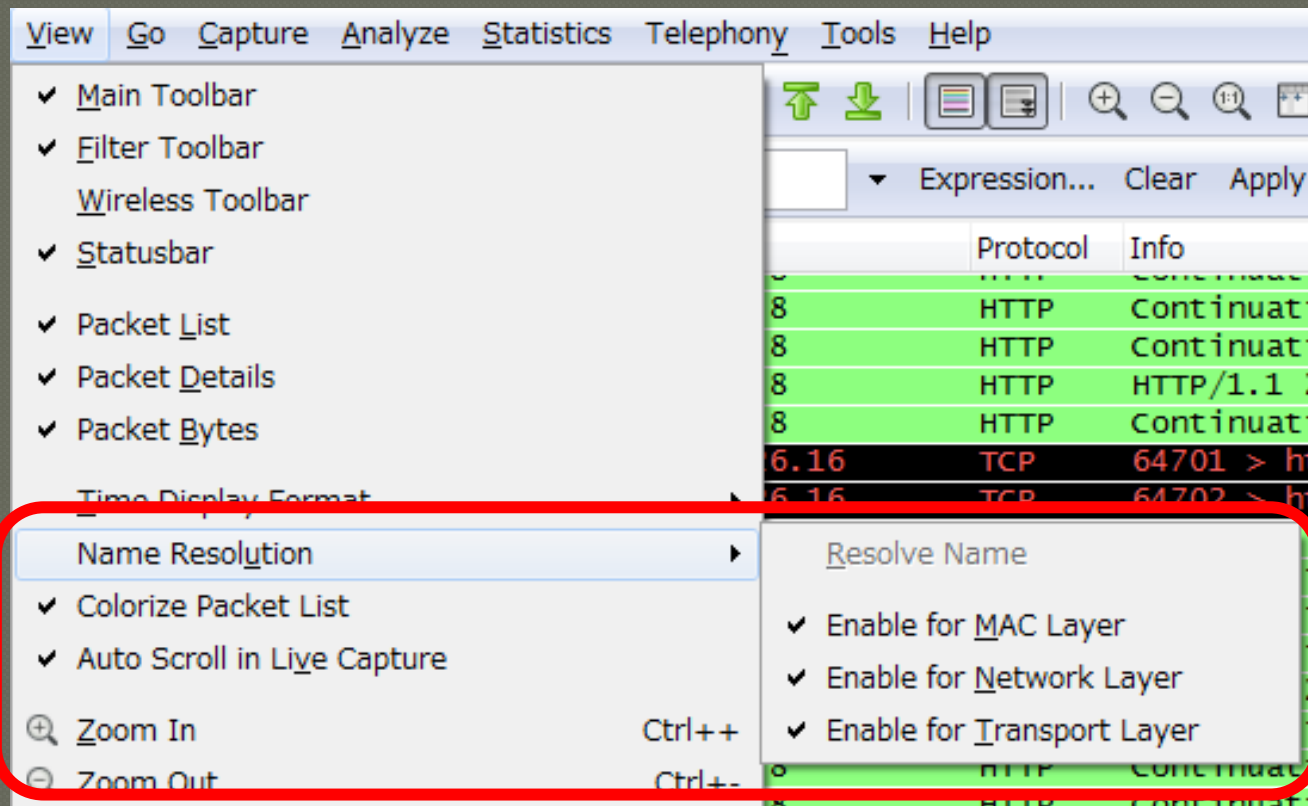
名前解決・キャプチャ時の設定

◎ [Capture] – [Options] の “Name Resolution” セクション



名前解決・表示時の設定

◎ [View] – [Name Resolution]



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

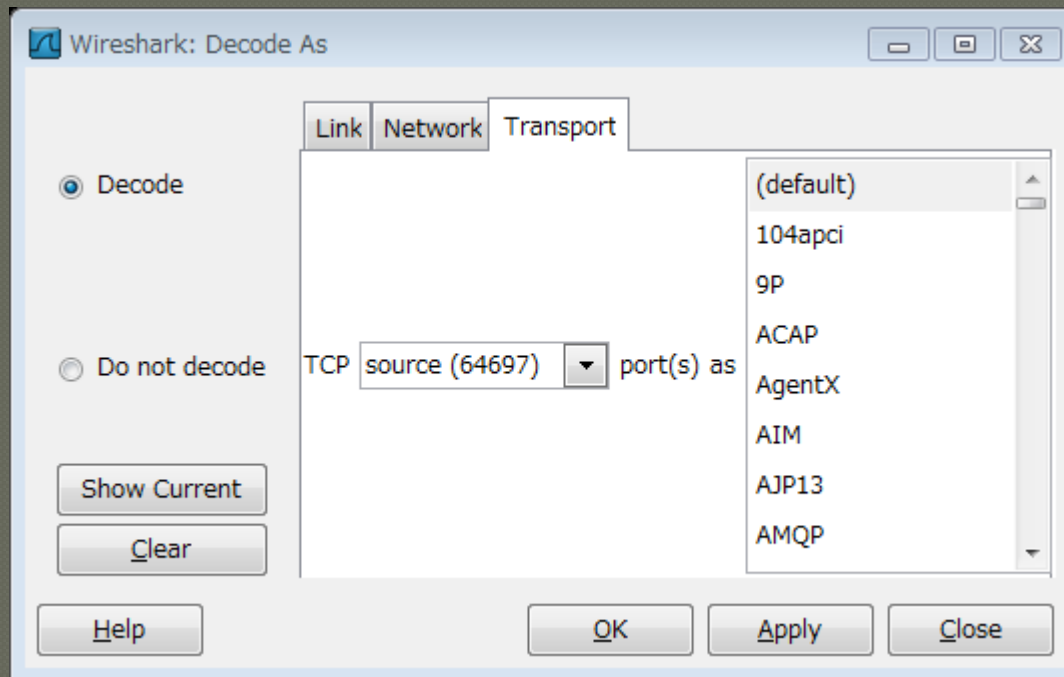
- ◎ 正しく解析されない場合も多い
- ◎ 特にトランスポート層で既定のポート以外を使い通信を行っている場合
- ◎ ex.
 - 81番ポートで HTTP
 - 443番ポート以外での HTTPS

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

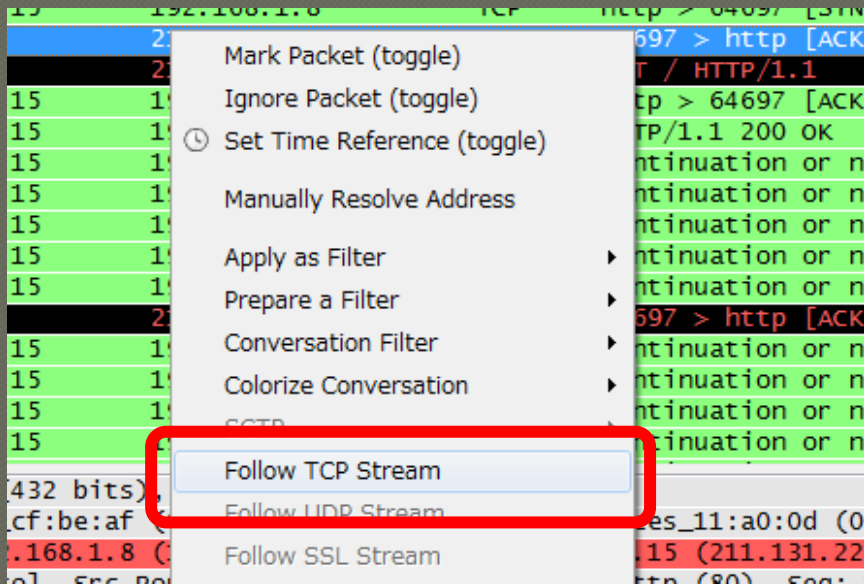
- 指定するパケットを右クリック
- [Decode as...] を選択
- プロトコルを指定



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]



Follow TCP Stream

The screenshot shows a window titled "Follow TCP Stream" with a "Stream Content" pane. The pane displays an HTTP request and response. The request is a GET for a page on www.asahi.com. The response is an HTTP/1.1 200 OK from an Apache server, with content type text/html and gzip encoding. Below the headers, the start of the HTML body is visible, including a meta charset declaration and a link to a page on asahi.com.

```
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; ebNewBandwidth_.www.asahi.com=1686%3A1297769203290;
__utmz=261975709.1297769205.19.14.utmcsr=home.att.ne.jp|utmccn=(referral)|utmcmd=referral|utmctt=/
gold/hebikuzure/link/bookmark.html; __utma=261975709.505929985.1279864839.1297591984.1297769205.19;
__utmb=261975709.1.10.1297769205; IMPASEG=S0%3D10198/S1%3D10876/S2%3D10130/S3%3D10127/S4%3D11132/S5%
3D11135/S6%3D11136/S7%3D10451/S8%3D11279/S9%3D10474/S10%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

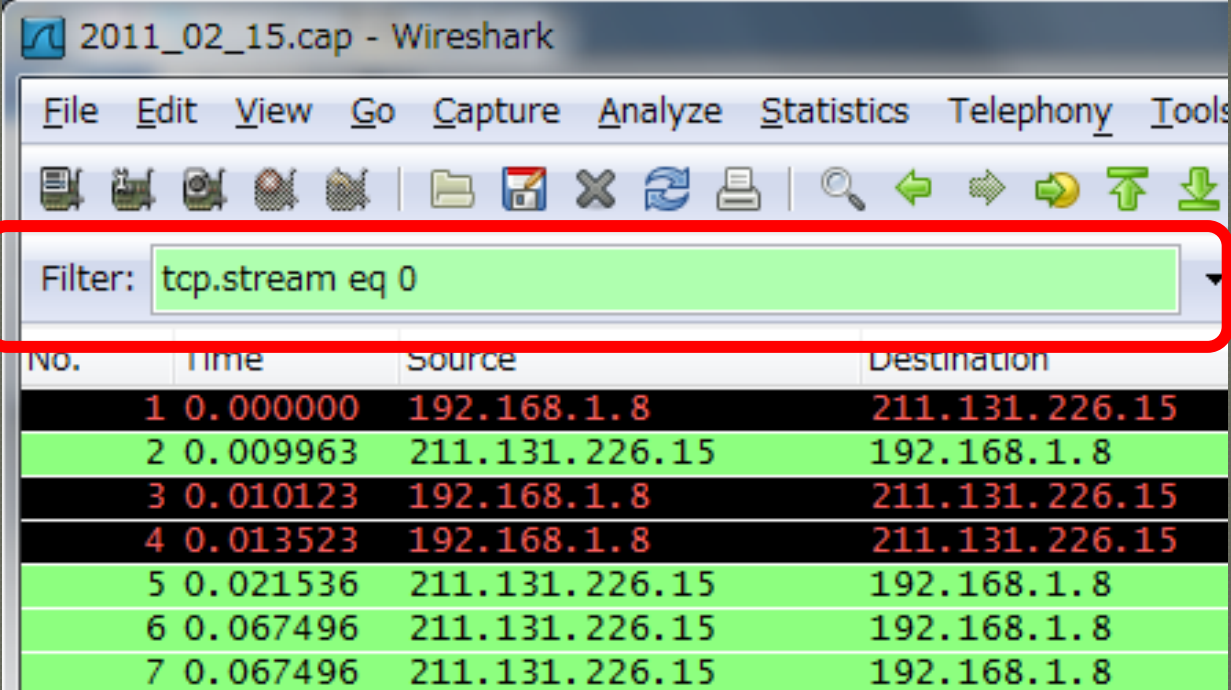
.....}.{.G.....a...6.....!!..d..}...4.....?f..'.....%
[.....!..OCH.9.....w.zf.....H.s...4.....].hw2.8...\.s...p...]....o..|.....
~...=G.rh/..A.Co...o.c.4...c4.z.U.....#.....}. "4...00.....a4.?~.xu..i5.9l<.m.....Ye..
```

Find Save As Print Entire conversation (36078 bytes) ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close

TCP Stream のフィルタ

- “Follow TCP Stream” を行くと、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

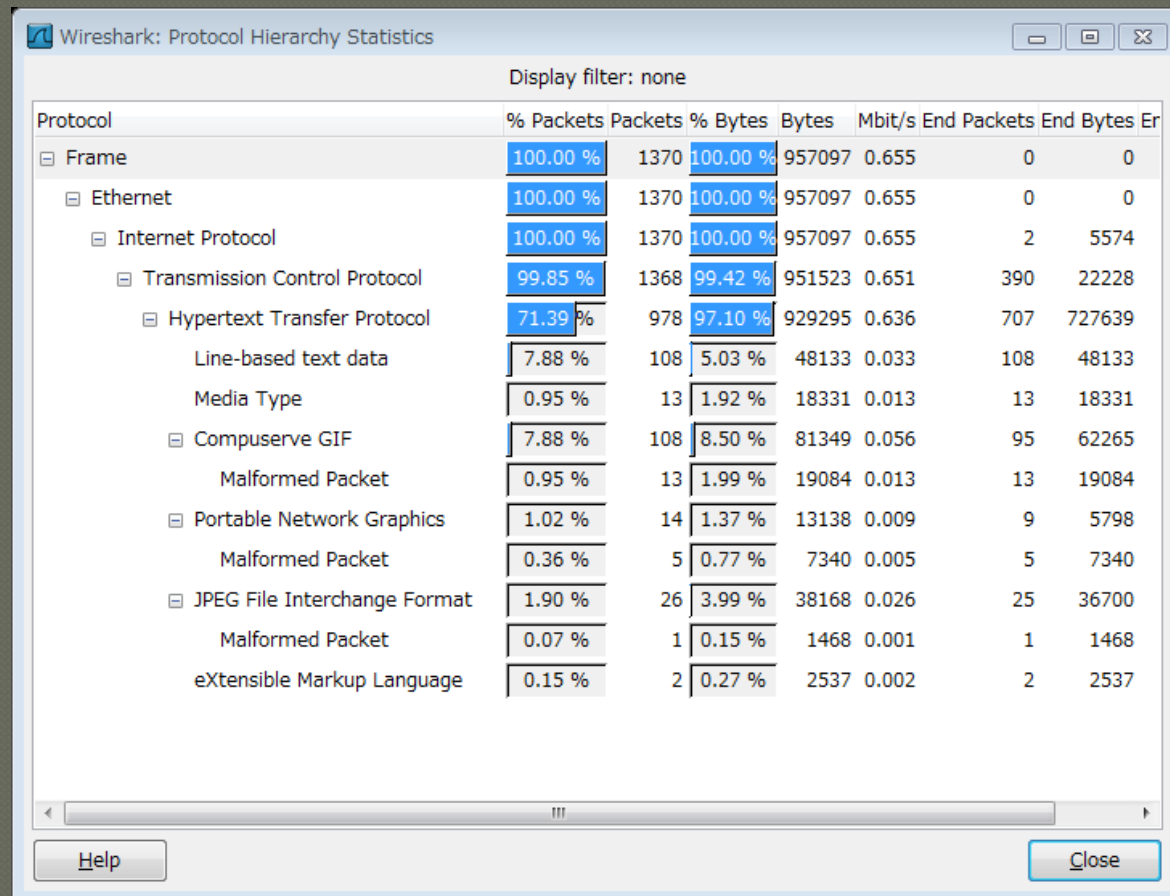
File Edit View Go Capture Analyze Statistics Telephony Tools

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]



Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	Er
[-] 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	

Help Close

エンドポイントの確認

◎ [Statistics] – [Endpoints]

The screenshot shows a window titled "Endpoints: 2011_02_15.cap" with a tabbed interface. The "IPv4: 16" tab is selected, displaying a table of IPv4 endpoints. The table has columns for Address, Packets, Bytes, Tx Packets, Tx Bytes, Rx Packets, Rx Bytes, Latitude, and Longitude. Below the table are checkboxes for "Name resolution" (checked) and "Limit to display filter" (unchecked). At the bottom, there are buttons for "Help", "Copy", "Map", and "Close".

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Latitude	Longitude
192.168.1.8	1 368	951 523	553	161 065	815	790 458	-	-
211.131.226.15	228	207 956	149	177 465	79	30 491	-	-
59.106.108.72	340	116 839	168	54 876	172	61 963	-	-
211.131.226.16	538	458 276	341	409 182	197	49 094	-	-
220.213.234.196	20	4 534	10	2 302	10	2 232	-	-
143.90.194.26	107	108 863	78	104 497	29	4 366	-	-
74.125.235.78	51	25 581	28	21 965	23	3 616	-	-
143.90.194.25	7	1 789	3	766	4	1 023	-	-
203.169.10.232	7	1 388	3	489	4	899	-	-
115.69.195.172	12	3 000	6	1 938	6	1 062	-	-
216.223.0.209	7	1 155	4	985	3	170	-	-

Conversations

○ [Statistics] – [Conversations]

Conversations: 2011_02_15.cap

Ethernet: 1 | Fibre Channel | FDDI | IPv4: 15 | IPv6 | IPX | JXTA | NCP | RSVP | SCTP | TCP: 44 | Token Ring | UDP | USB | WLAN

IPv4 Conversations

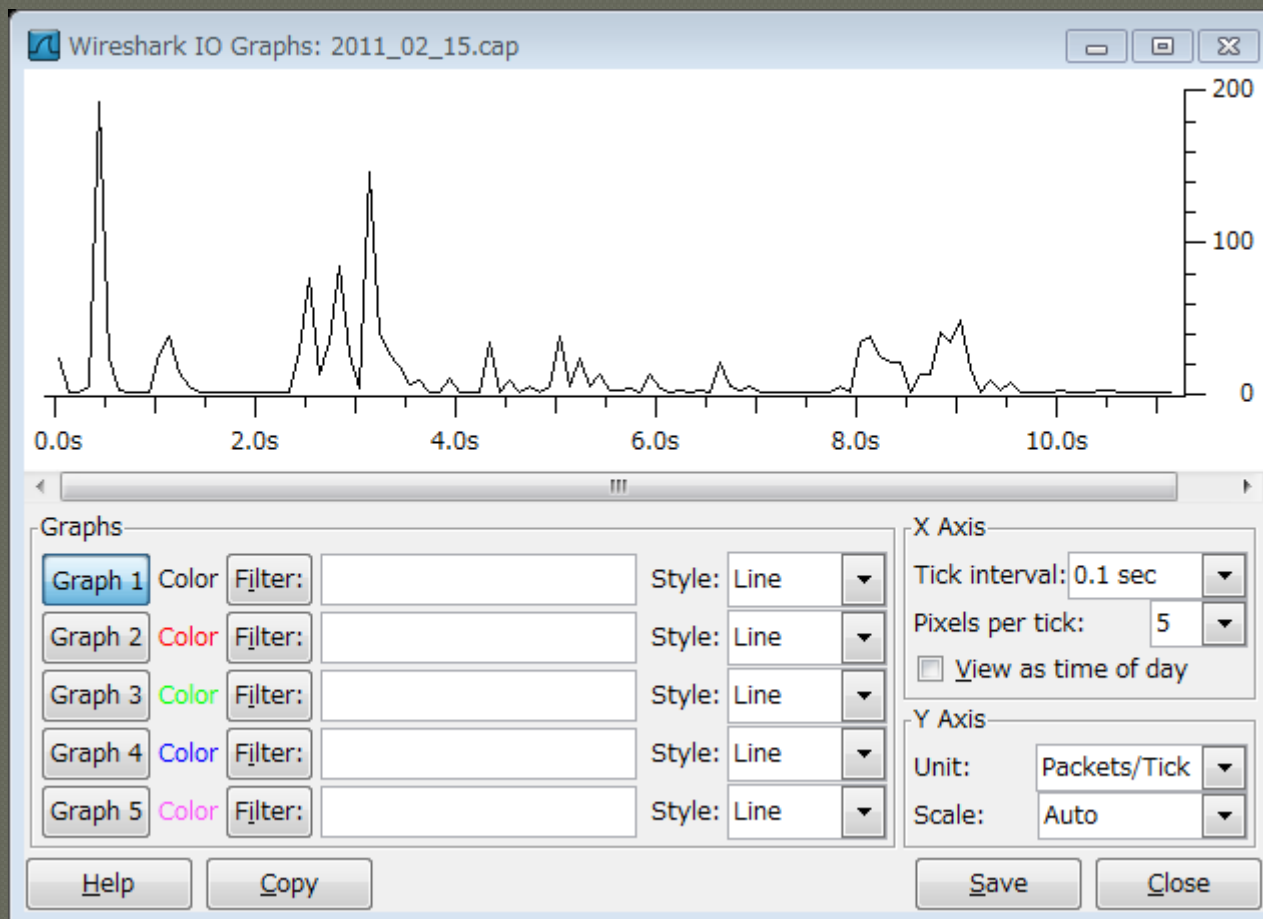
Address A	Address B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B
192.168.1.8	211.131.226.15	228	207 956	79	30 491	149	177 465
59.106.108.72	192.168.1.8	340	116 839	168	54 876	172	61 963
192.168.1.8	211.131.226.16	538	458 276	197	49 094	341	409 182
192.168.1.8	220.213.234.196	20	4 534	10	2 232	10	2 302
143.90.194.26	192.168.1.8	107	108 863	78	104 497	29	4 366
74.125.235.78	192.168.1.8	51	25 581	28	21 965	23	3 616
143.90.194.25	192.168.1.8	7	1 789	3	766	4	1 023
192.168.1.8	203.169.10.232	7	1 388	4	899	3	489
115.69.195.172	192.168.1.8	12	3 000	6	1 938	6	1 062
192.168.1.8	216.223.0.209	7	1 155	3	170	4	985

Name resolution Limit to display filter

Help Copy Follow Stream Close

IO グラフ

◎ [Statistics] – [IO Graphs]



參考資料

- ◎ **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/>