# Wireshark 分析機能入門

大量パケットの分析方法

hebikuzure

# 本日の参考書

- 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/

# 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
  - 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

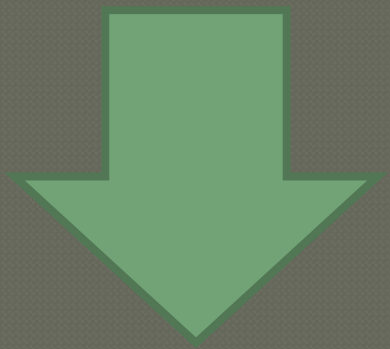
- **How To Set Up a Capture**
  http://wiki.wireshark.org/CaptureSetup
- **Security**
  http://wiki.wireshark.org/Security
- **Platform-Specific information about capture privileges**
  http://wiki.wireshark.org/CaptureSetup/CapturePrivileges

# 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

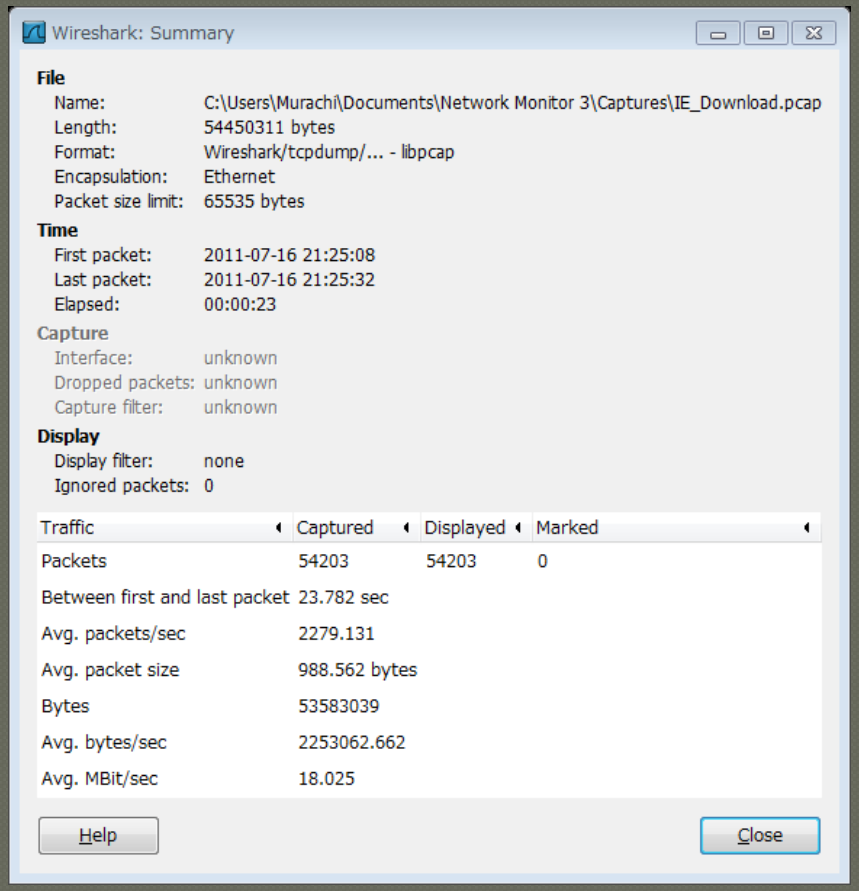
- 個々のパケットの解析の繰り返しでは抽出するのが困難な大量のデータ



特異パケットを自動抽出
マクロ的分析
データの可視化

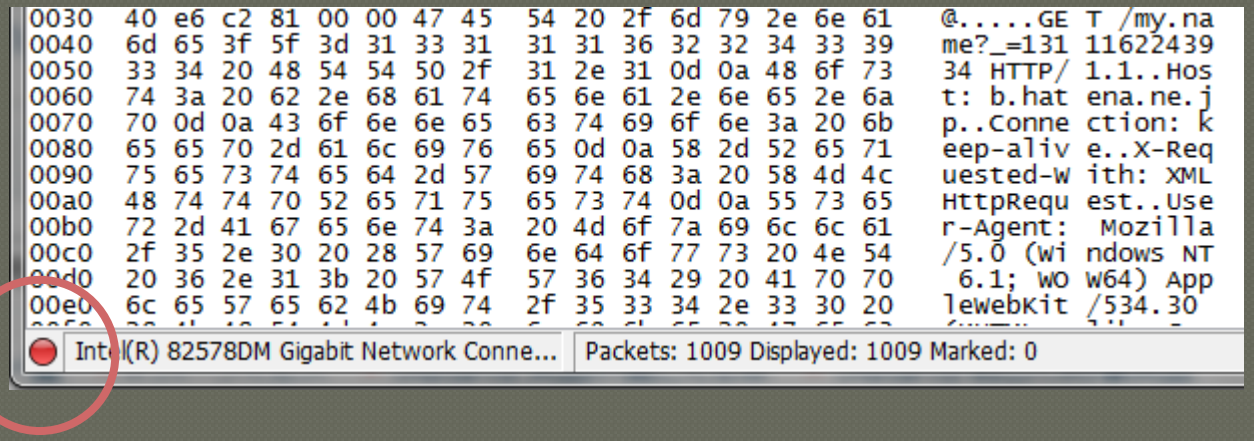
# キャプチャ データの概要表示

- [Statistics] – [Summary]



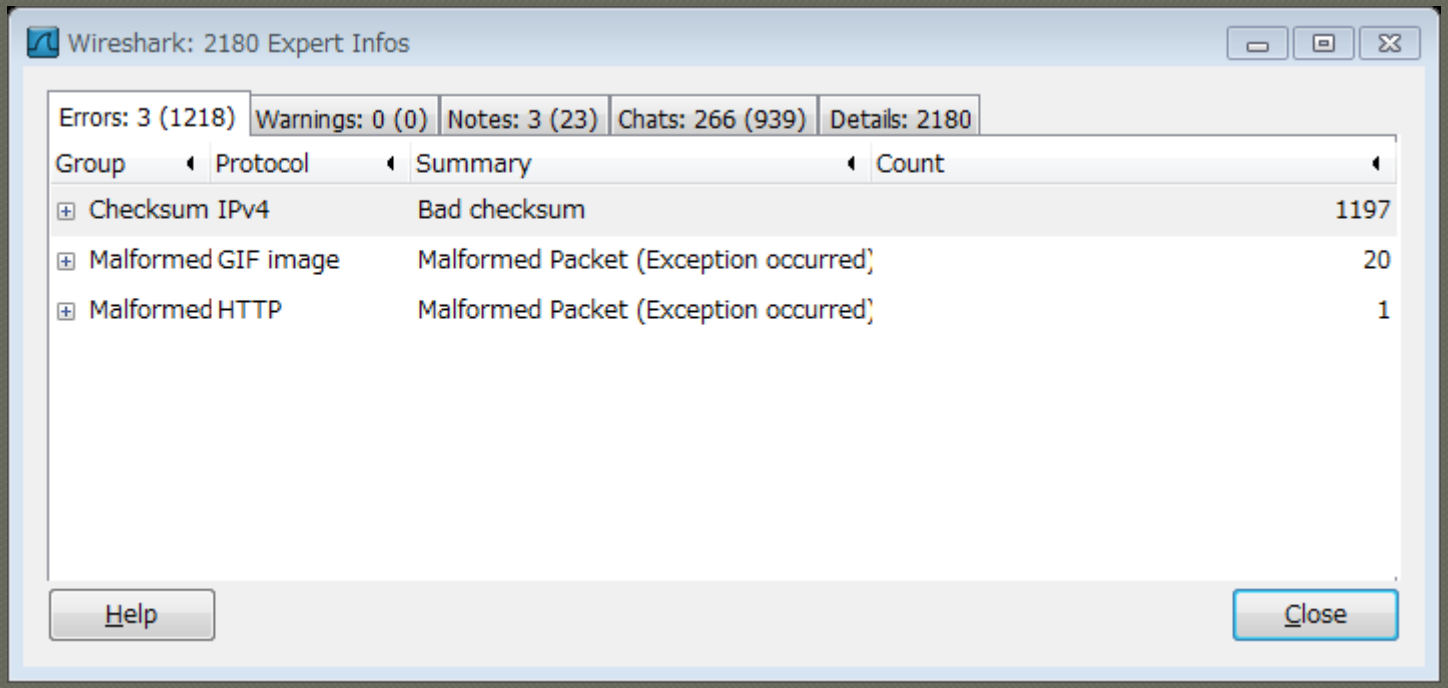
# 特異パケットの抽出

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



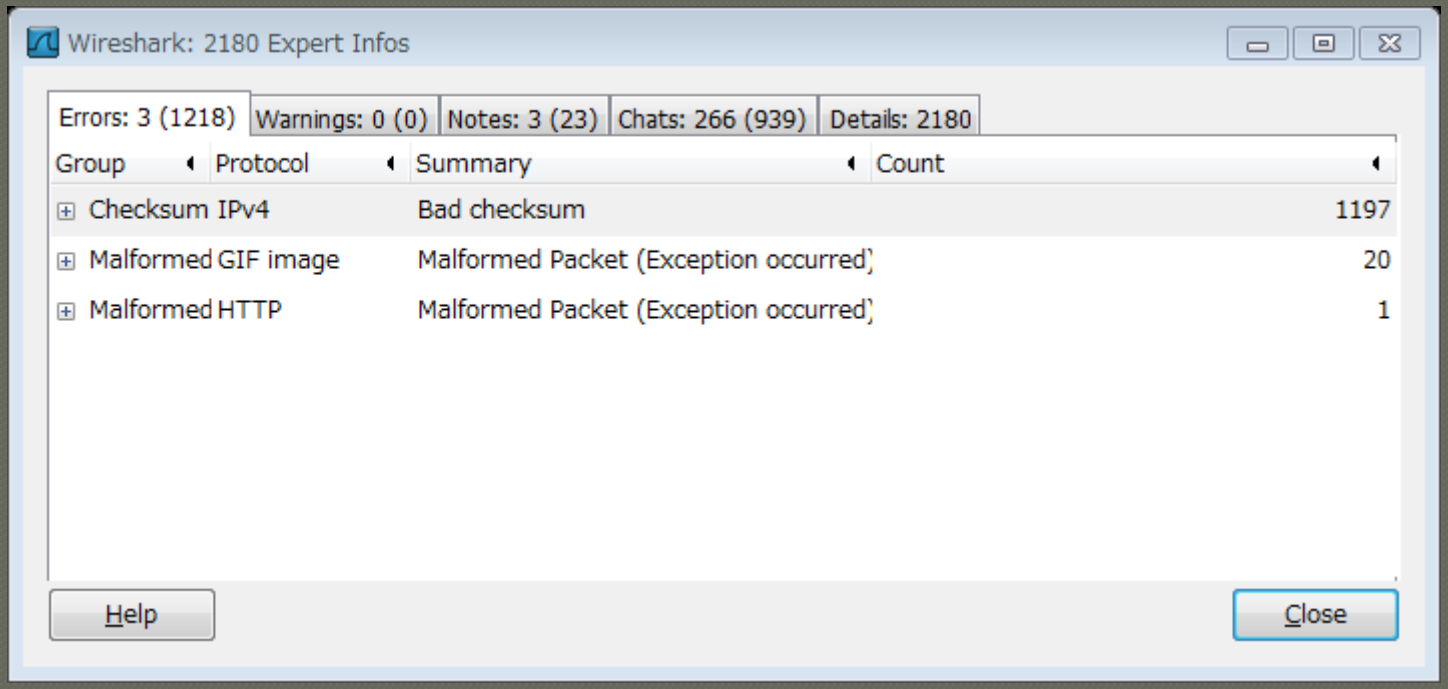
# Expert Info Composite

- 特異情報があるパケットが分類されて表示される



# Expert Info Composite - Error タブ

- 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

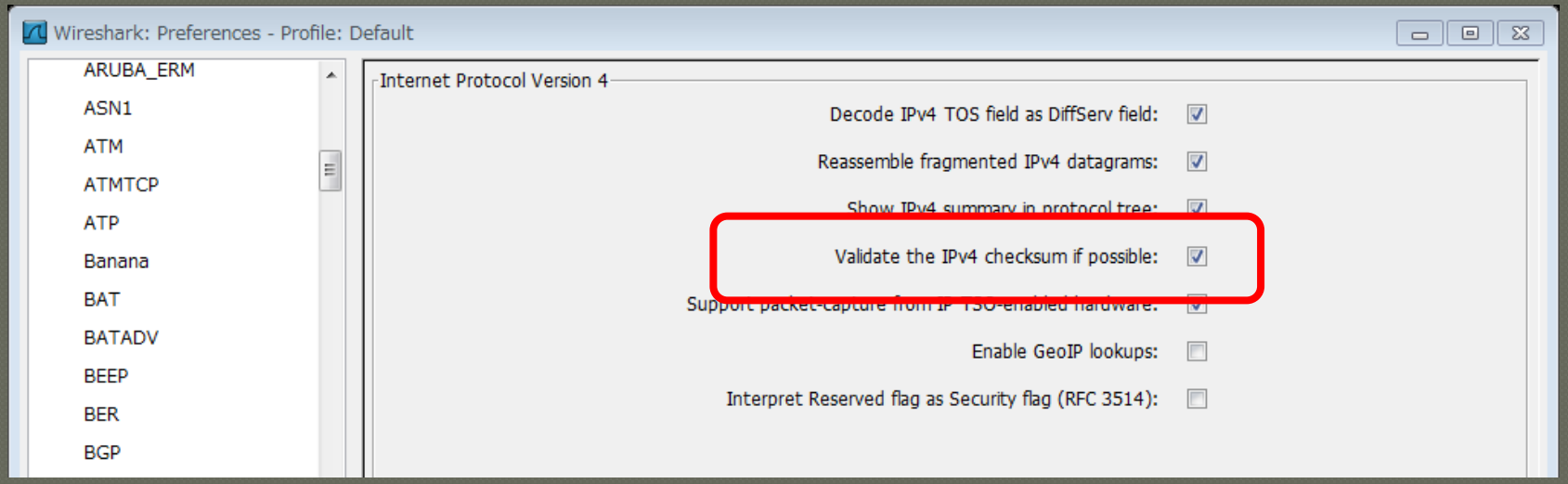


# チェックサム エラーの抑止（1）

- 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

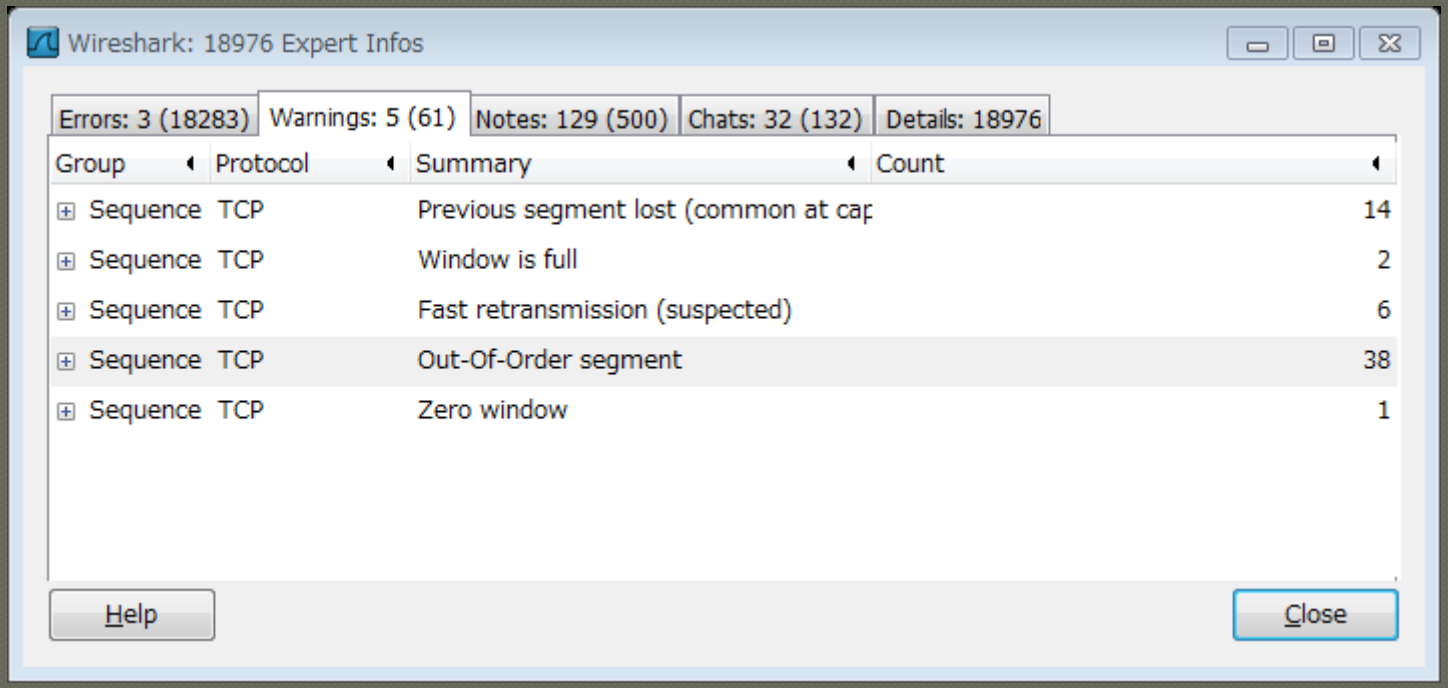
# チェックサムエラーの抑止（2）

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



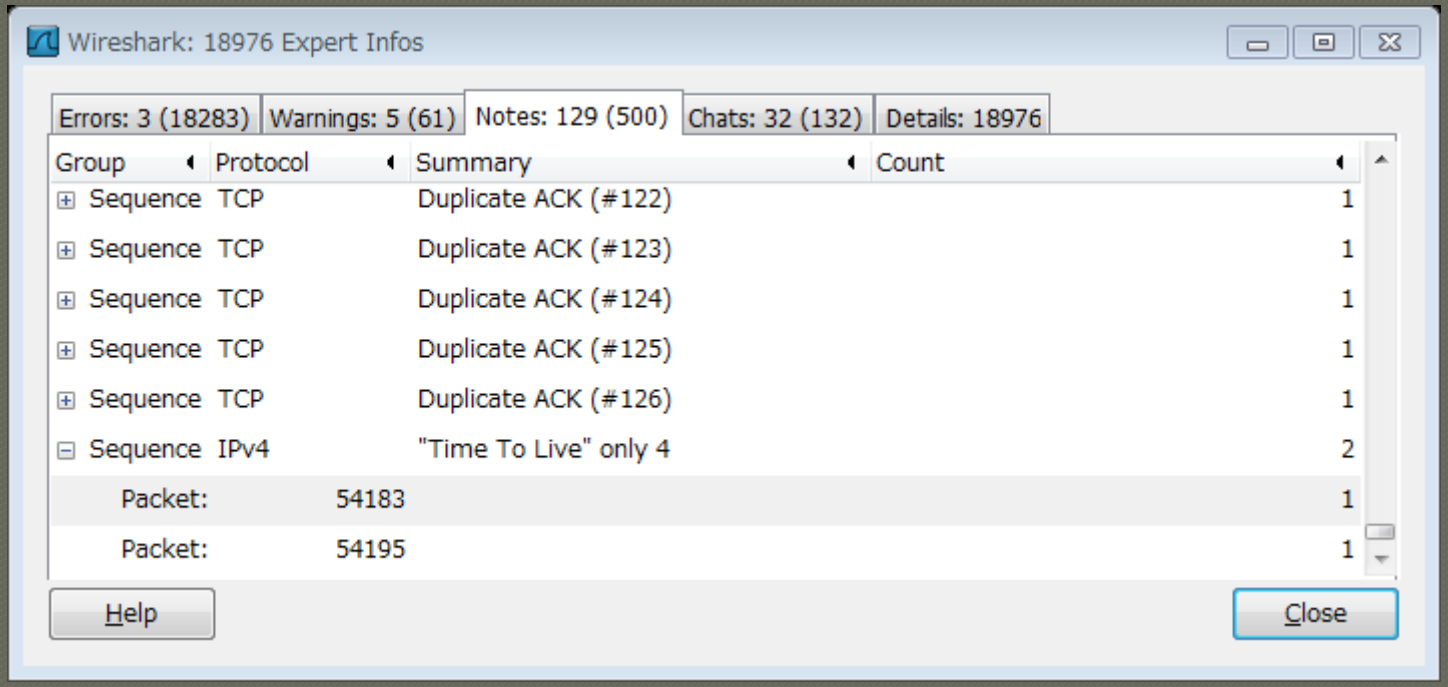
# Expert Info Composite - Warnings タブ

- sequence number の不一致、Window サイズの問題、fast retransmission など



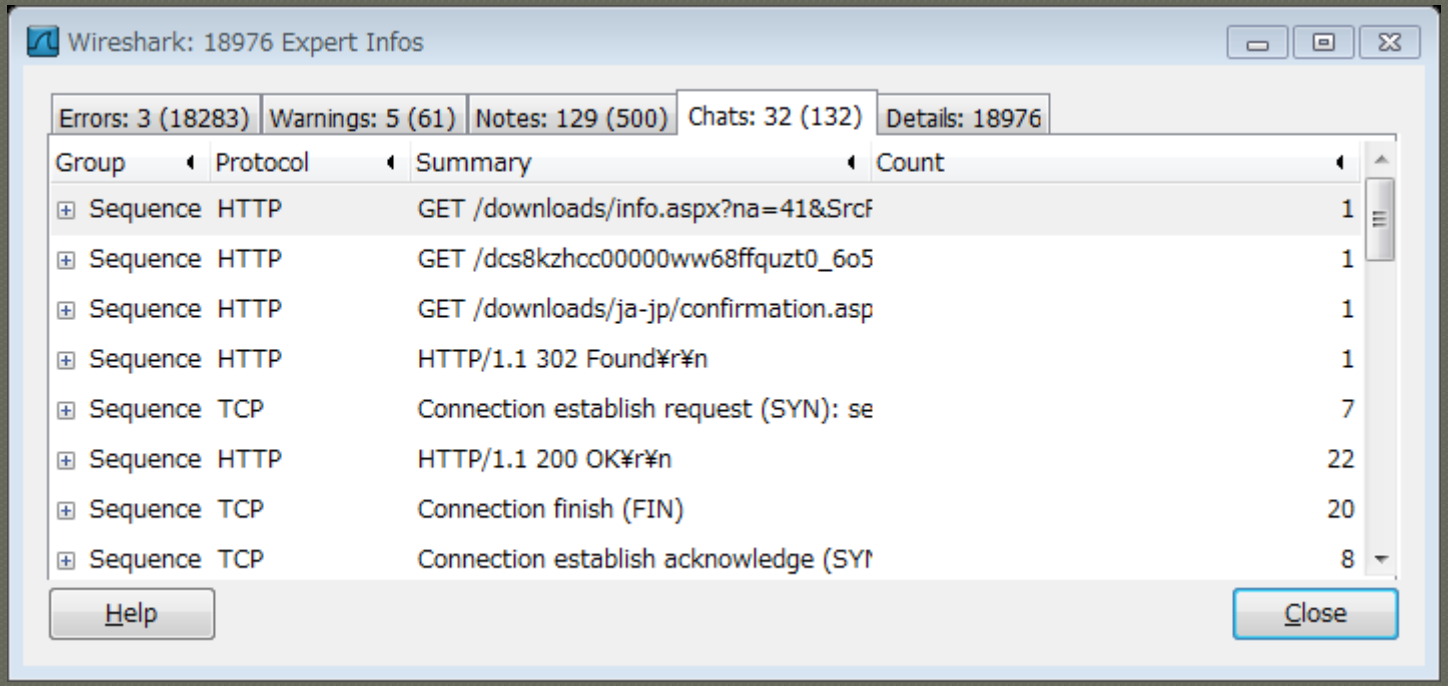
# Expert Info Composite - Notes タブ

- 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



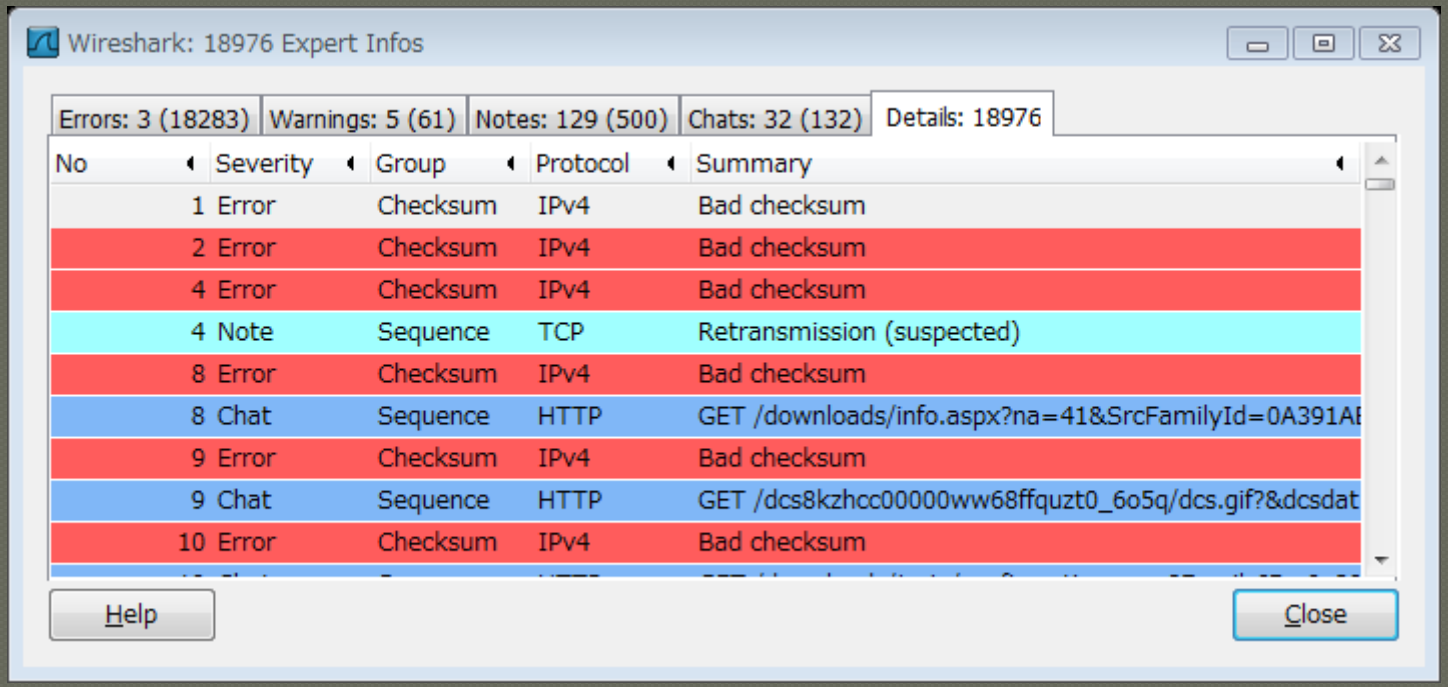
# Expert Info Composite - Chats タブ

- リクエスト/レスポンスごとに分類



# Expert Info Composite - Details タブ

- 分析情報のあるすべてのパケットを表示



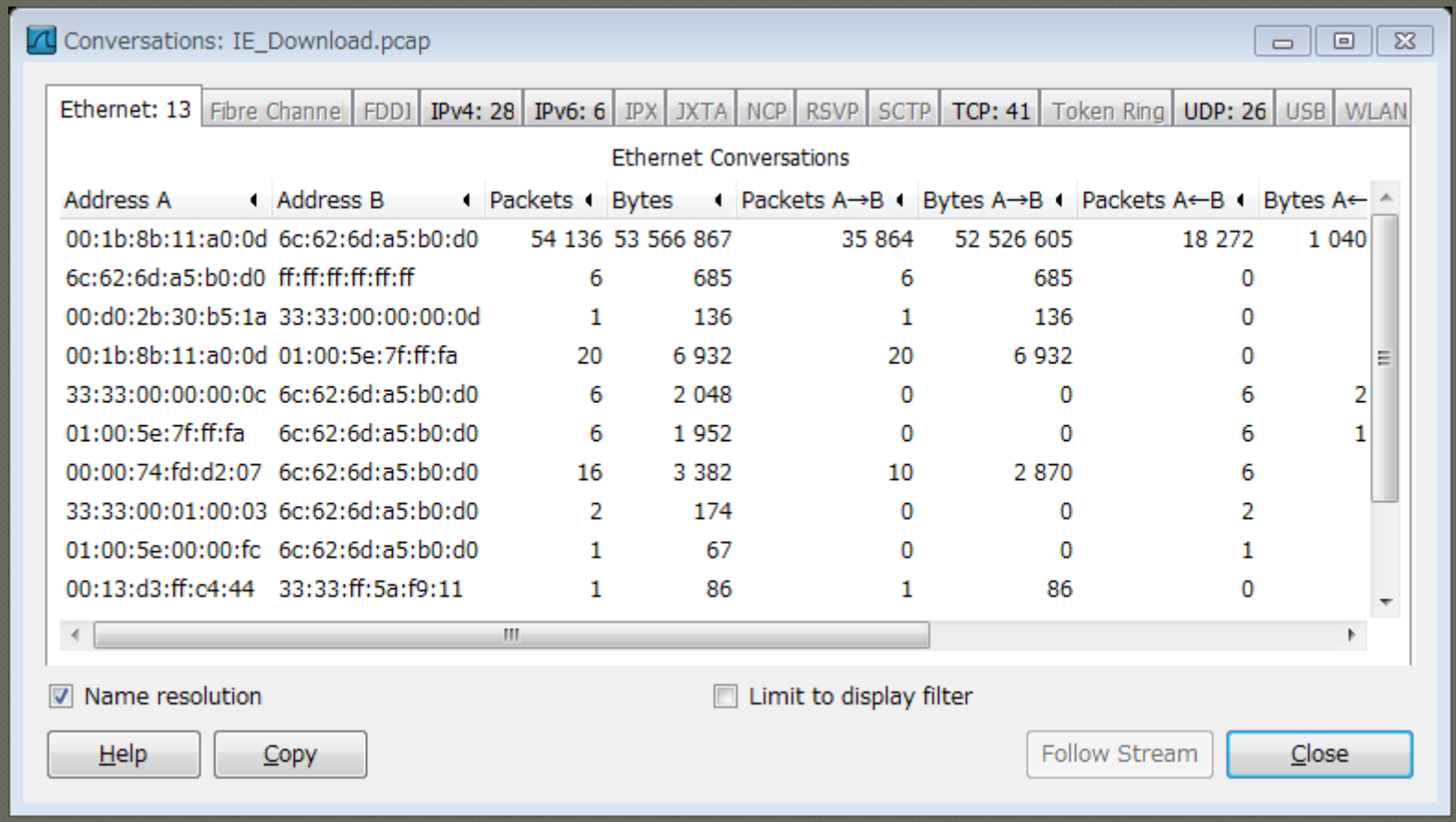
# マクロ的分析

- 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

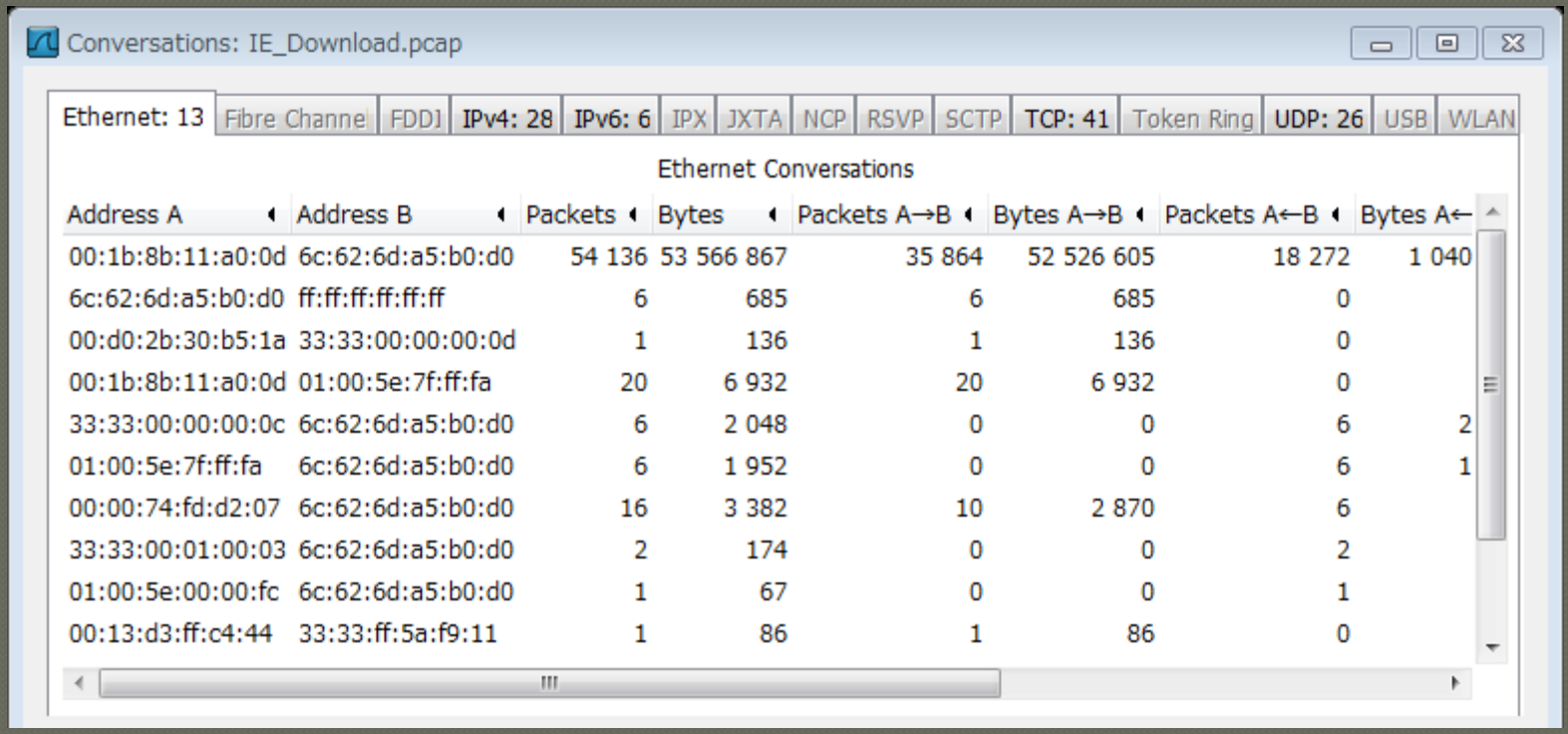
# 対話 (Conversations) 統計機能

- [Statistics] – [Conversations]



# Conversations – Ethernet タブ

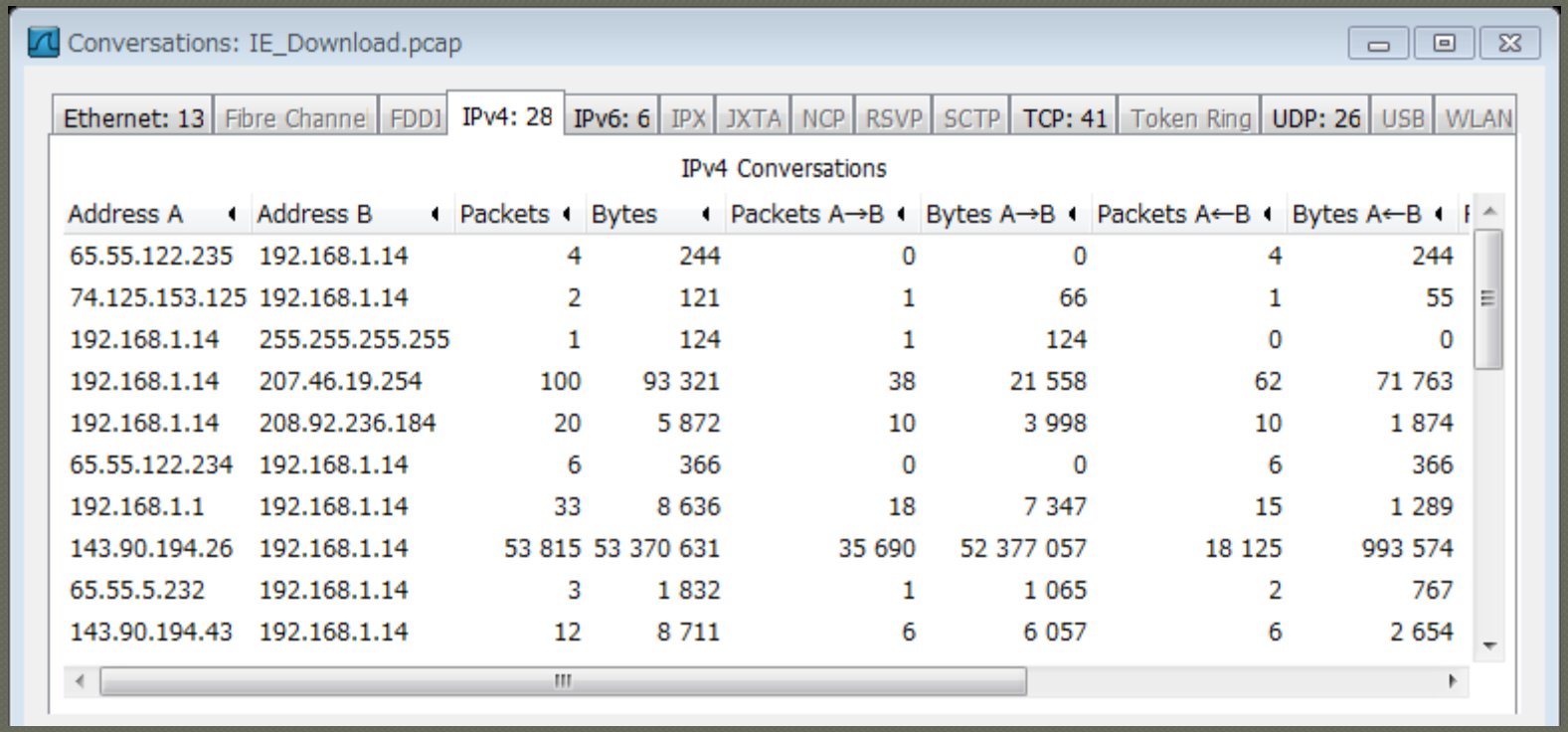
- 送信元/宛先 MAC アドレスの組み合わせごとの情報を表示




| 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: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 | |

# Conversations – IPv4 タブ

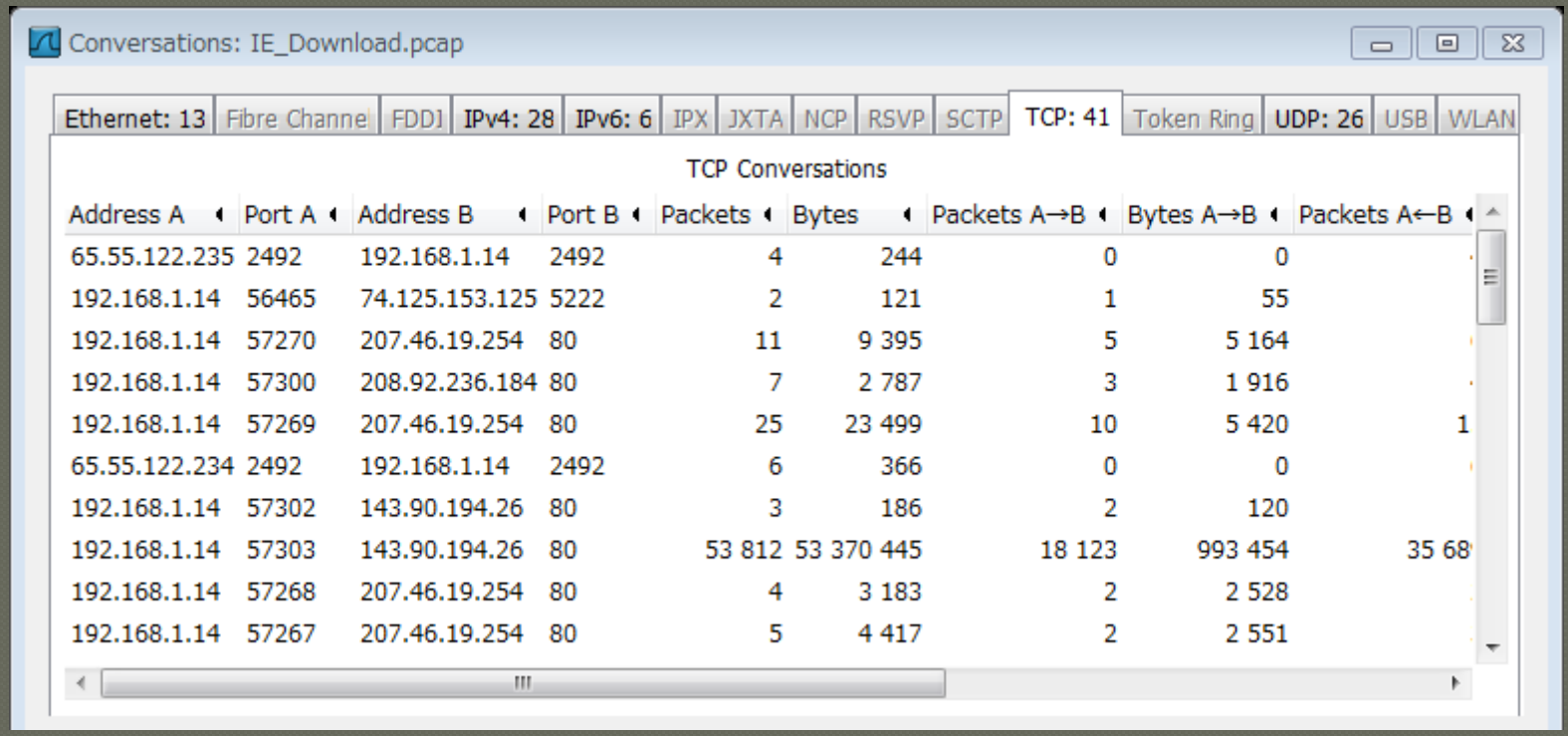
- 送信元/宛先 IP アドレスの組み合わせごとに情報を表示




| Address A | Address B | Packets | Bytes | Packets A→B | Bytes A→B | Packets A←B | Bytes A←B |
|---|---|---|---|---|---|---|---|
| 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 |
| 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 |

# 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




| 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 | |
| 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 | |
| 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 | |
| 192.168.1.14 | 57267 | 207.46.19.254 | 80 | 5 | 4 417 | 2 | 2 551 | |

# Conversation List

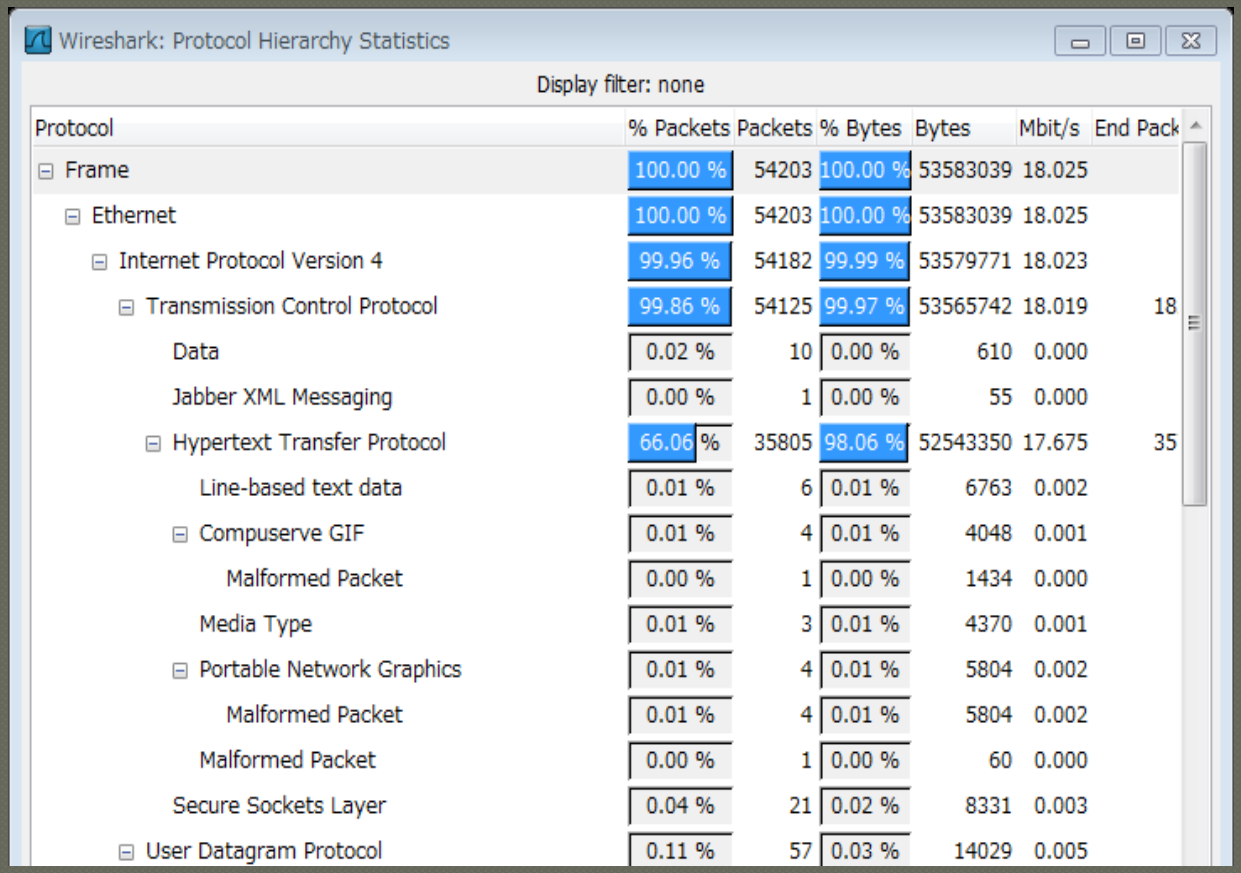
- 特定のプロトコルだけのリストを作成する場合は

  [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

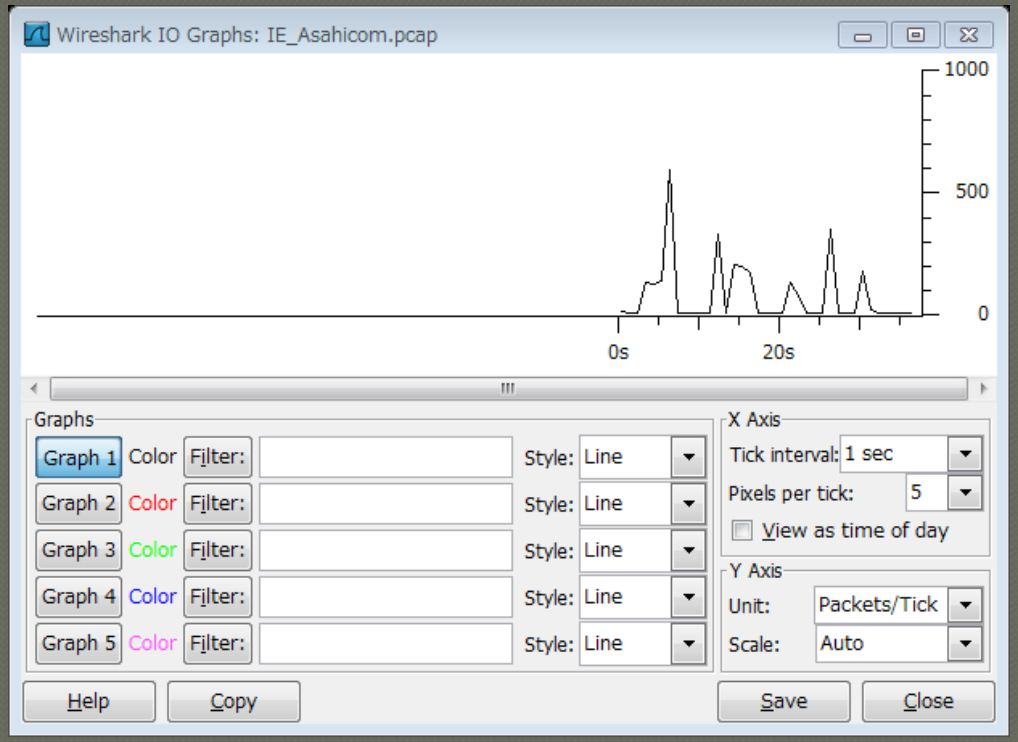
- **[Statistics]** – [Protocol Hierarchy]



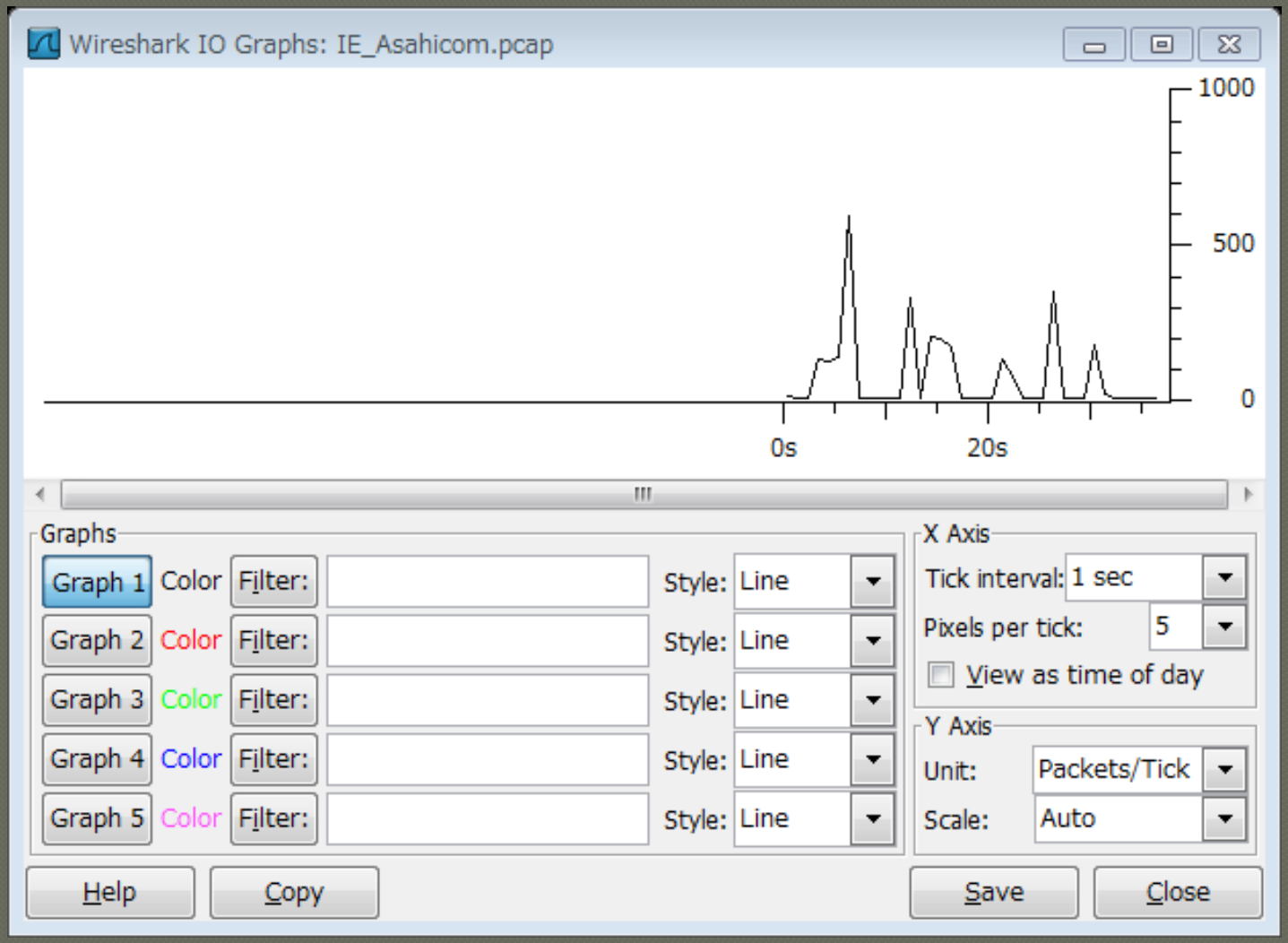

| Protocol | % Packets | Packets | % Bytes | Bytes | Mbit/s | End Pack |
|---|---|---|---|---|---|---|
| Frame | 100.00 % | 54203 | 100.00 % | 53583039 | 18.025 | |
| Ethernet | 100.00 % | 54203 | 100.00 % | 53583039 | 18.025 | |
| Internet Protocol Version 4 | 99.96 % | 54182 | 99.99 % | 53579771 | 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 % | 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 | |

# データの可視化

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



# IO Graph

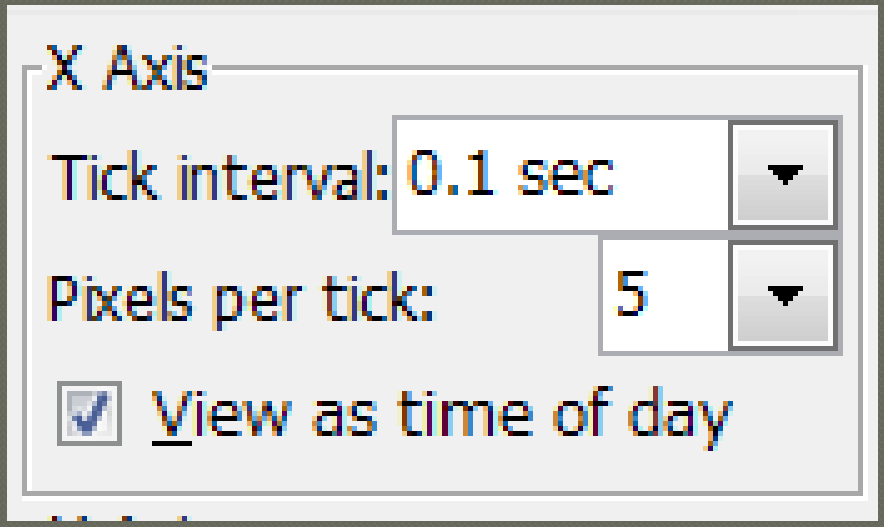

Wireshark IO Graphs: IE_Asahicom.pcap
1000
500
0
0s
20s
Graphs
Graph 1
Color
Filter:
Style:
Line
Graph 2
Color
Filter:
Style:
Line
Graph 3
Color
Filter:
Style:
Line
Graph 4
Color
Filter:
Style:
Line
Graph 5
Color
Filter:
Style:
Line
X Axis
Tick interval:
1 sec
Pixels per tick:
5
View as time of day
Y Axis
Unit:
Packets/Tick
Scale:
Auto
Help
Copy
Save
Close

# X 軸の調整

- X Axis : X 軸（横軸）の調整
  - Tick interval
    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

- X Axis の設定

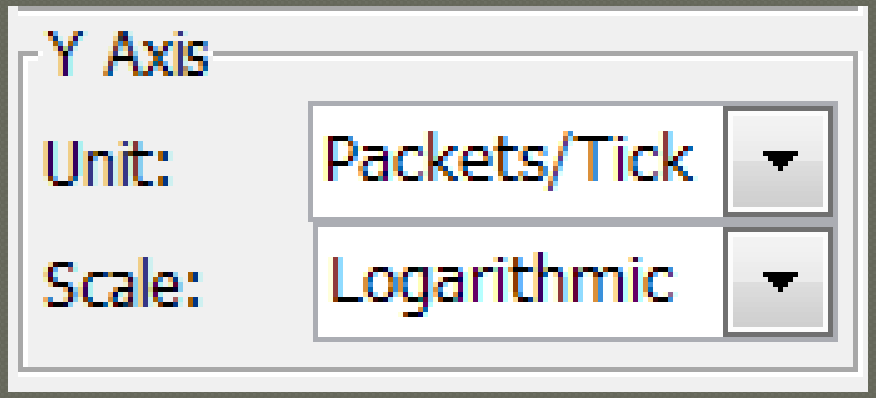


# Y 軸の調整

- **Y Axis :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**

# Y Axis

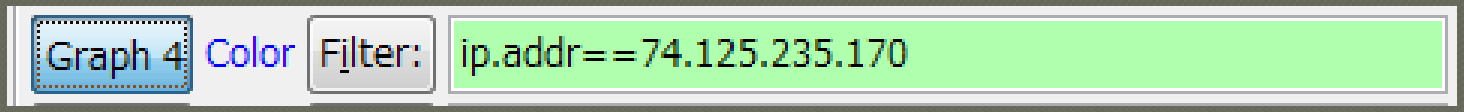
- Y Axis の設定



# グラフ データの追加

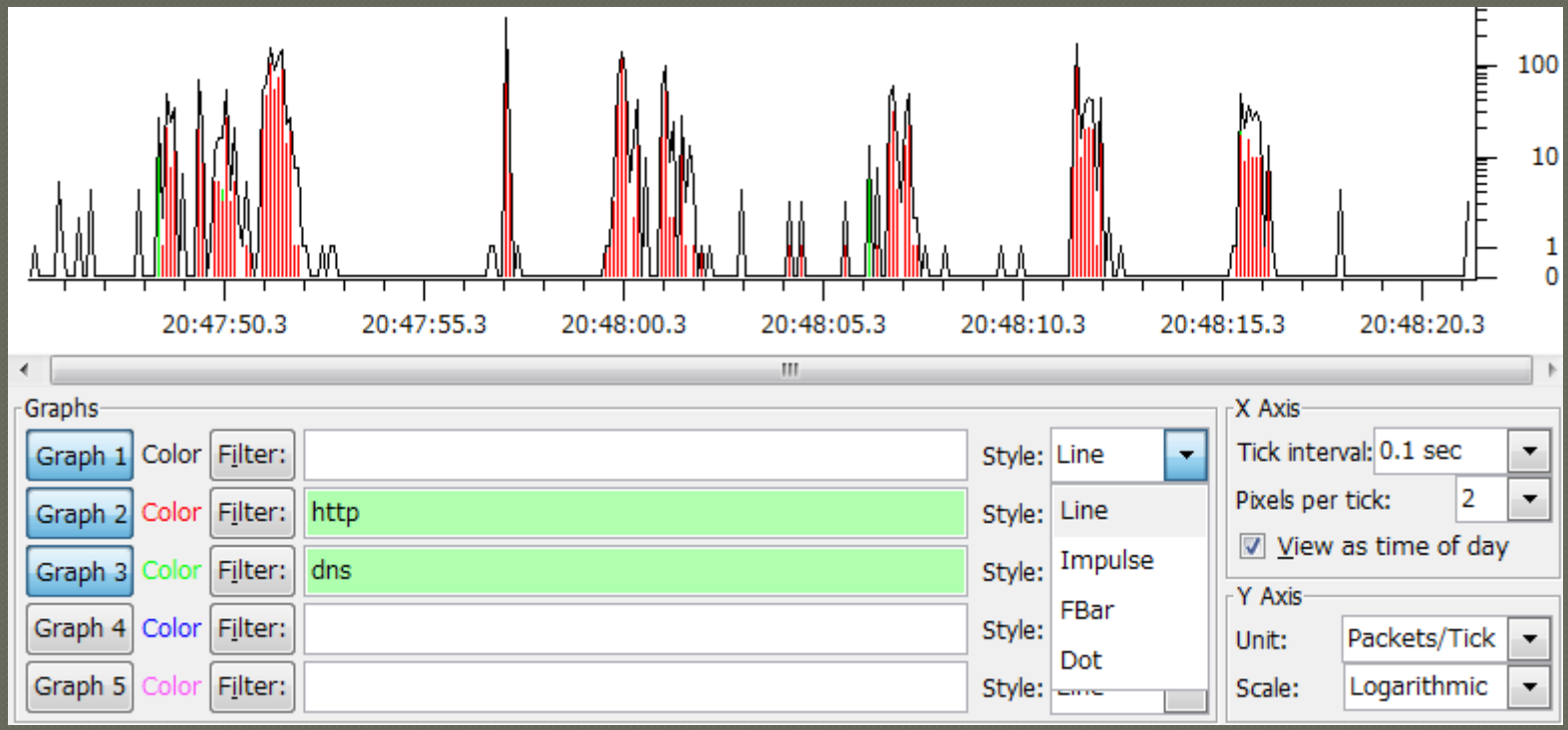
- [Graphs] セクション – [Filter]
- Display Filter と同じ書式でフィルタを設定する

- [Graph n] ボタンで表示/非表示を切替え



# グラフ種類の変更

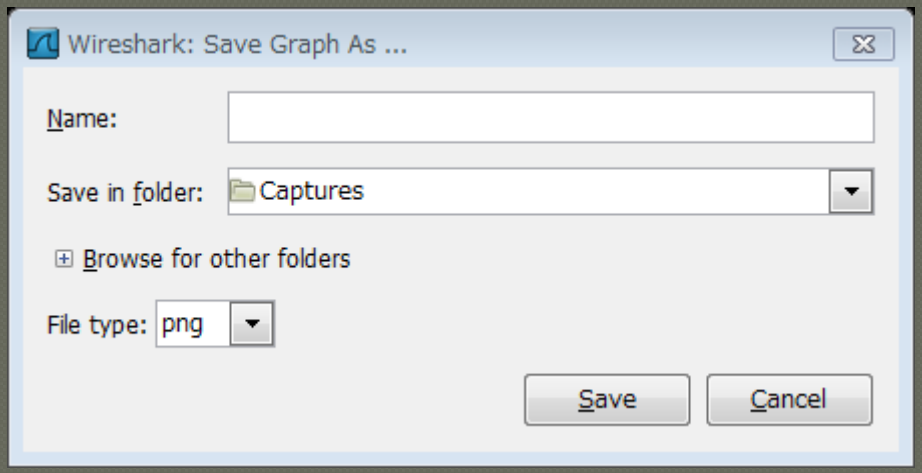
- [Graphs] セクション – [Filter]



# 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

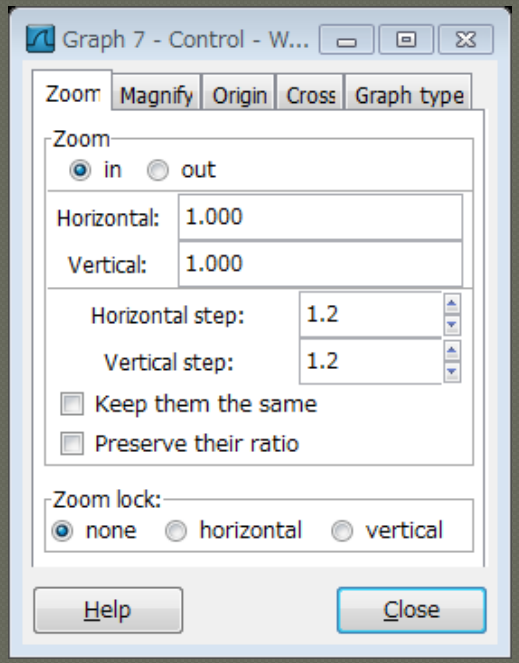


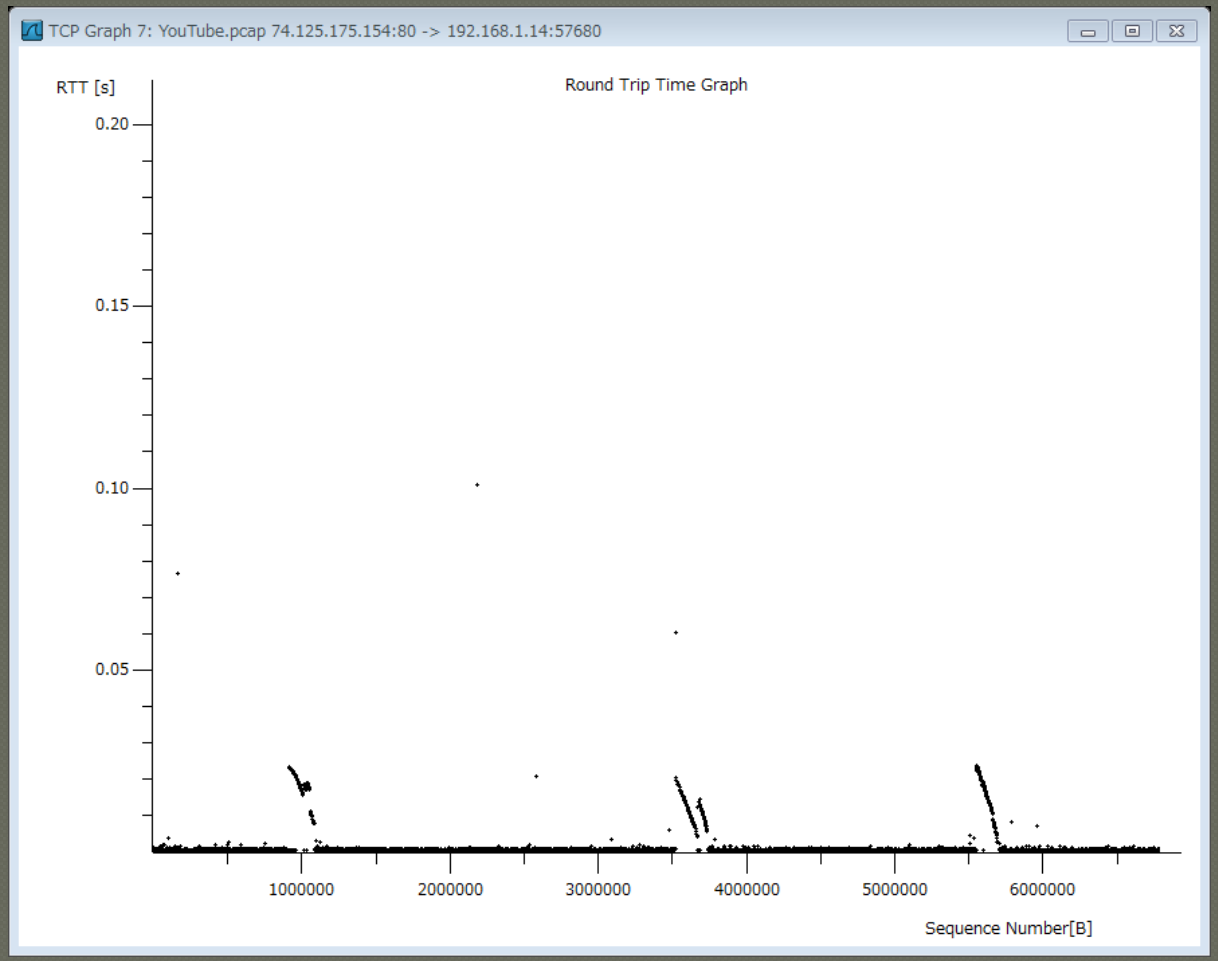
# TCP ストリームの可視化

- TCP Stream Graph 機能

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

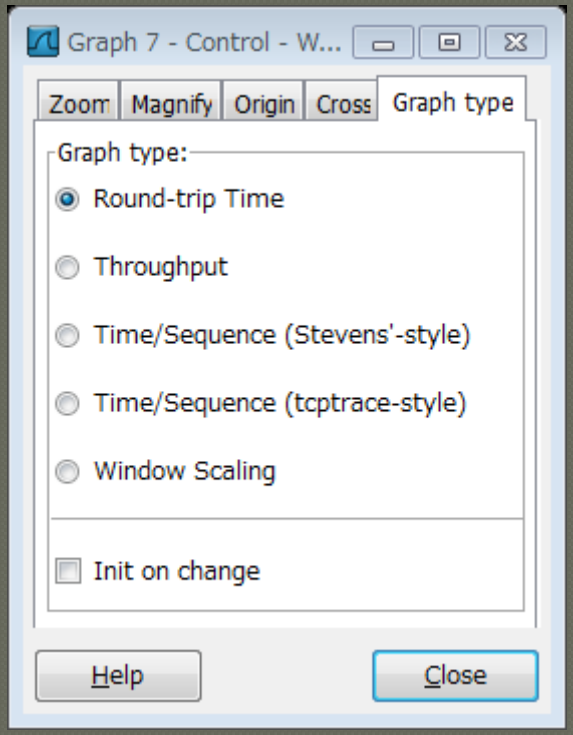
# TCP Stream Graph



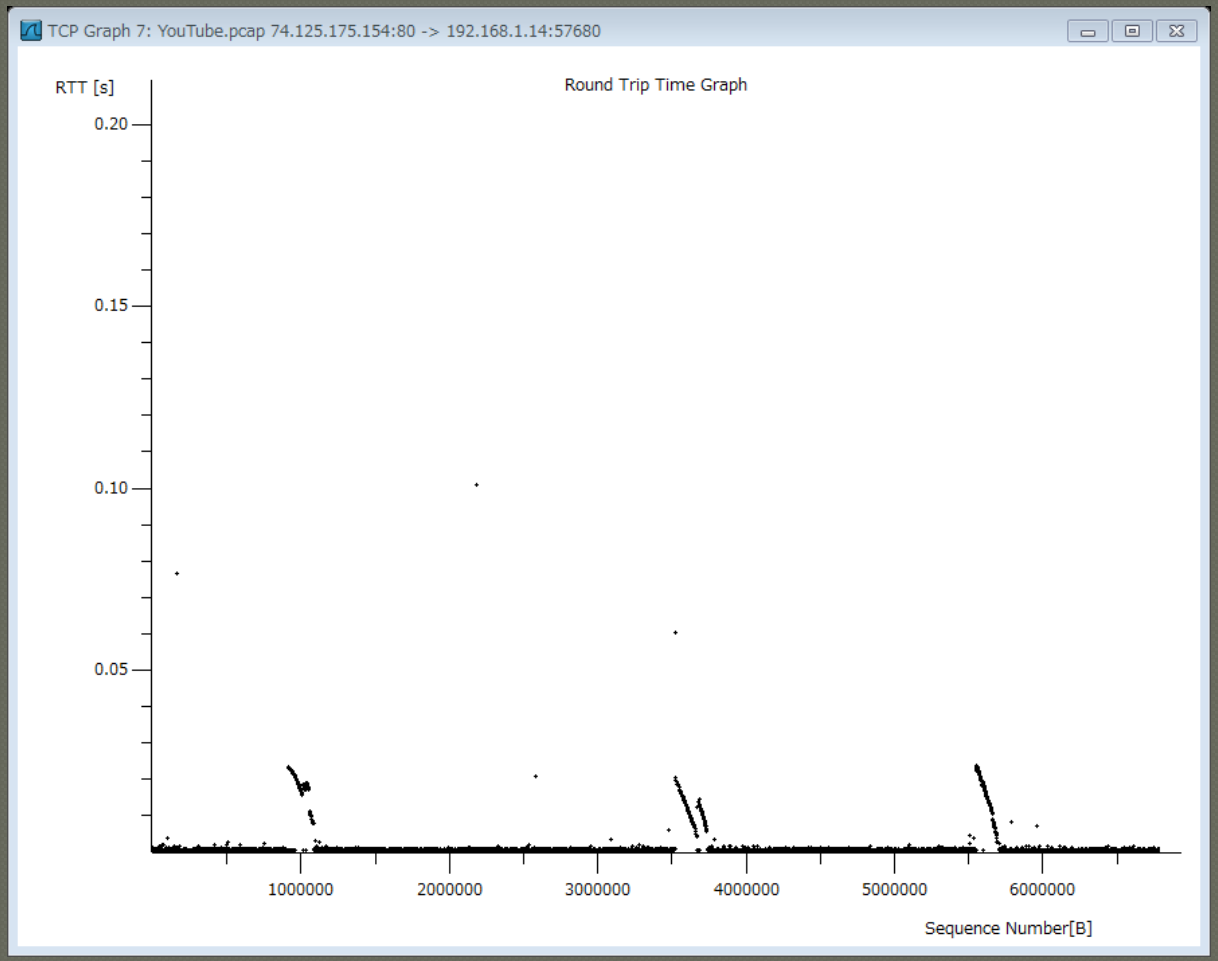



# グラフ種類の変更

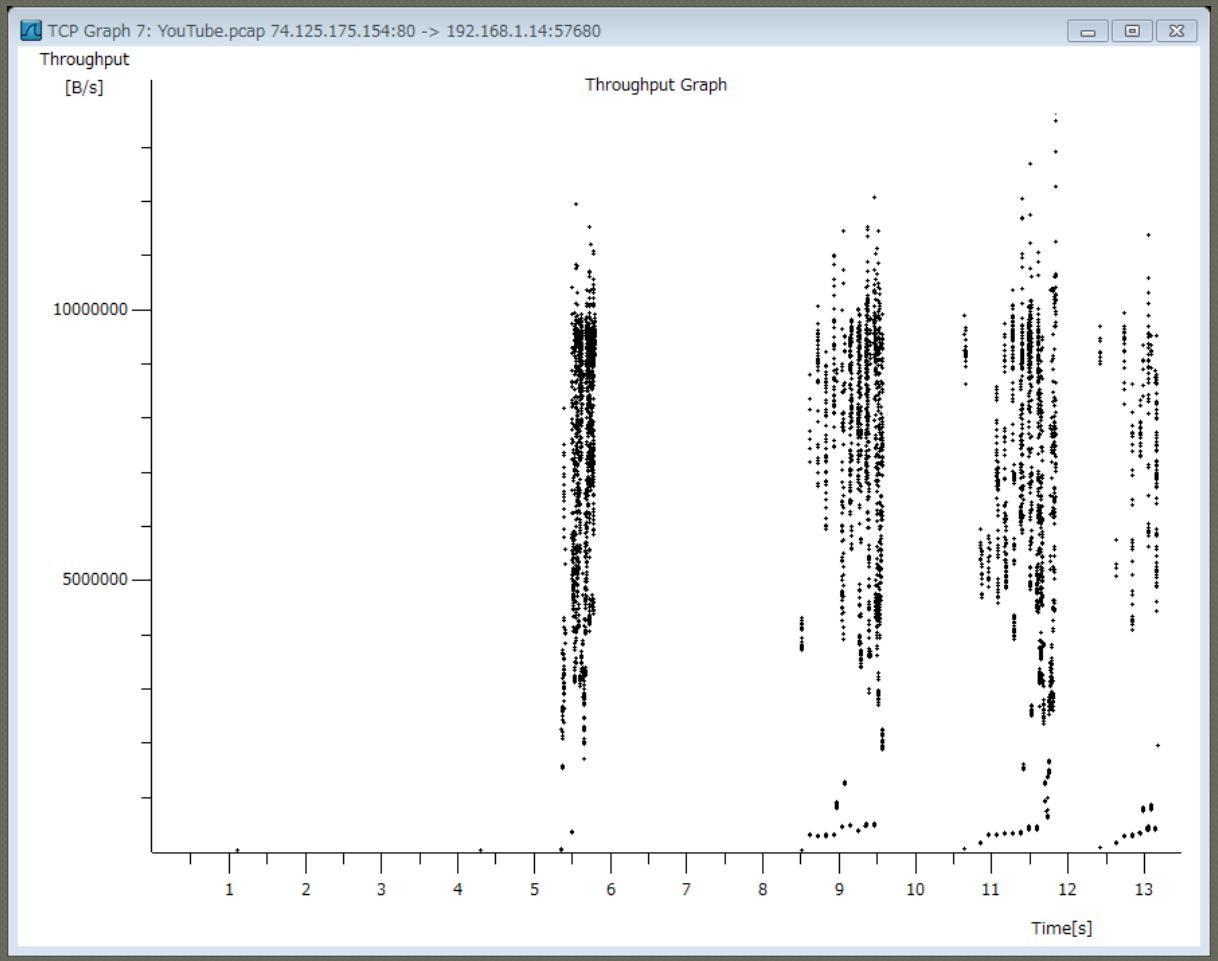
- Graph Control ウィンドウの
  [Graph Type] タブで切り替えできる



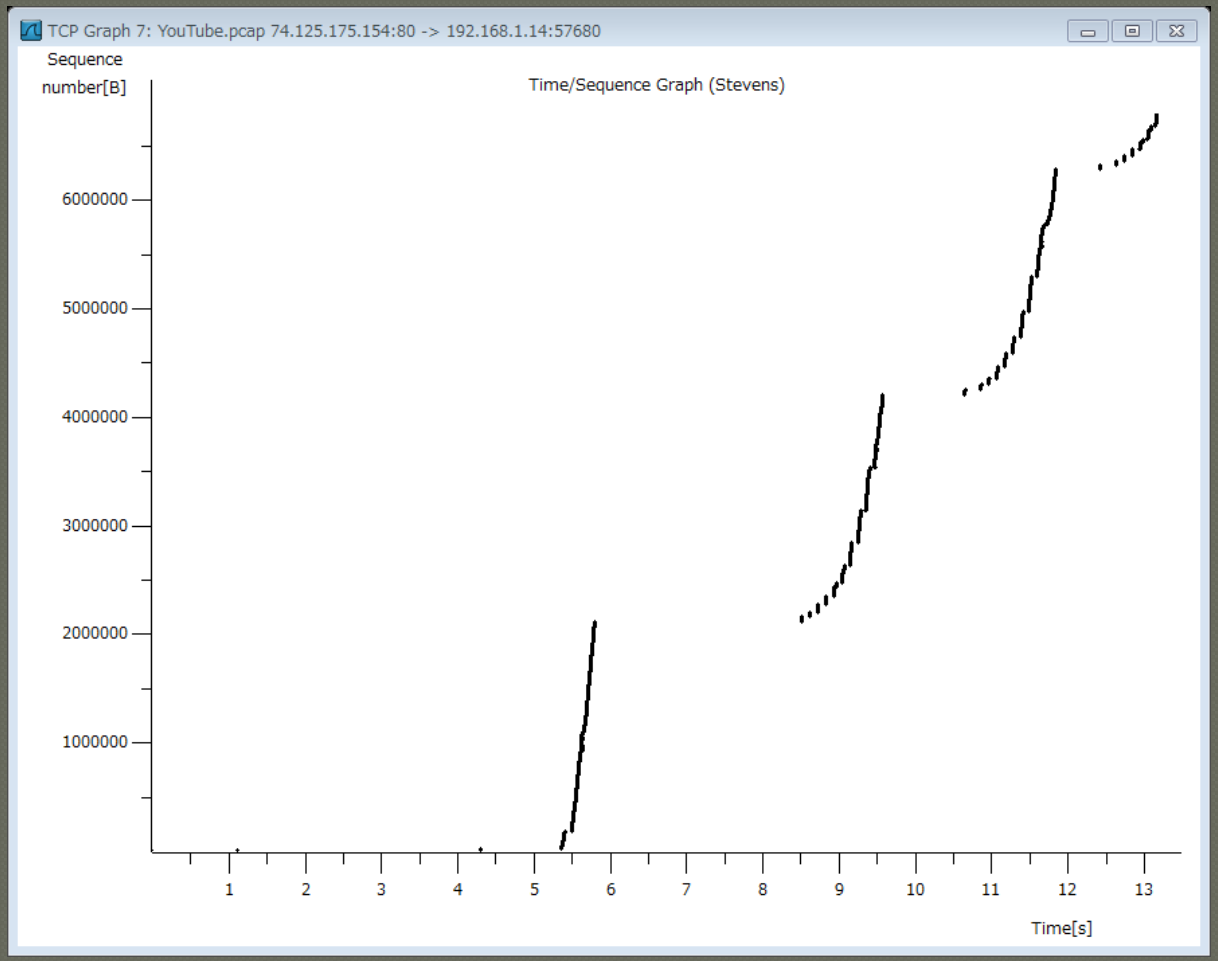
# Round Trip Time Graph



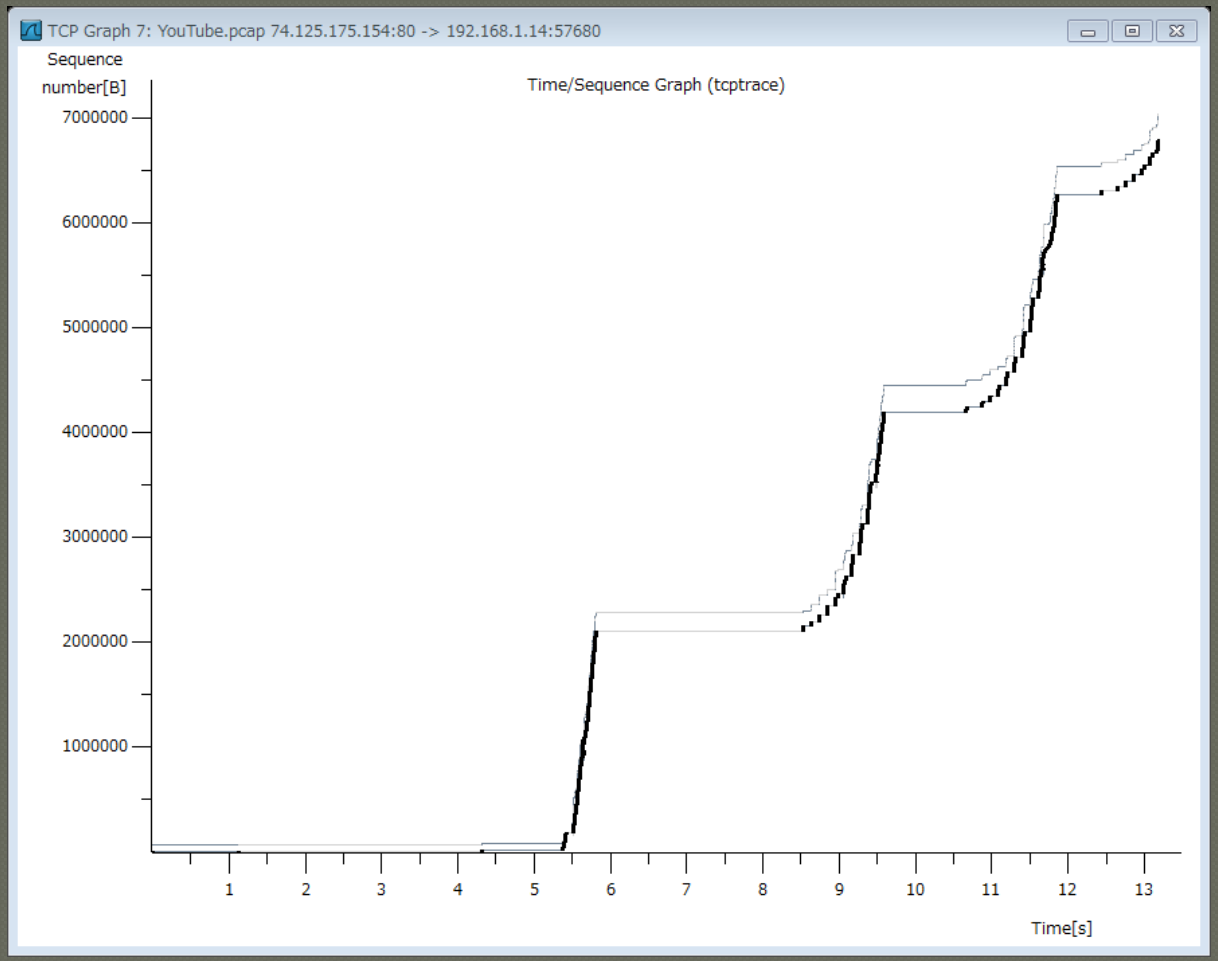
# Throughput Graph



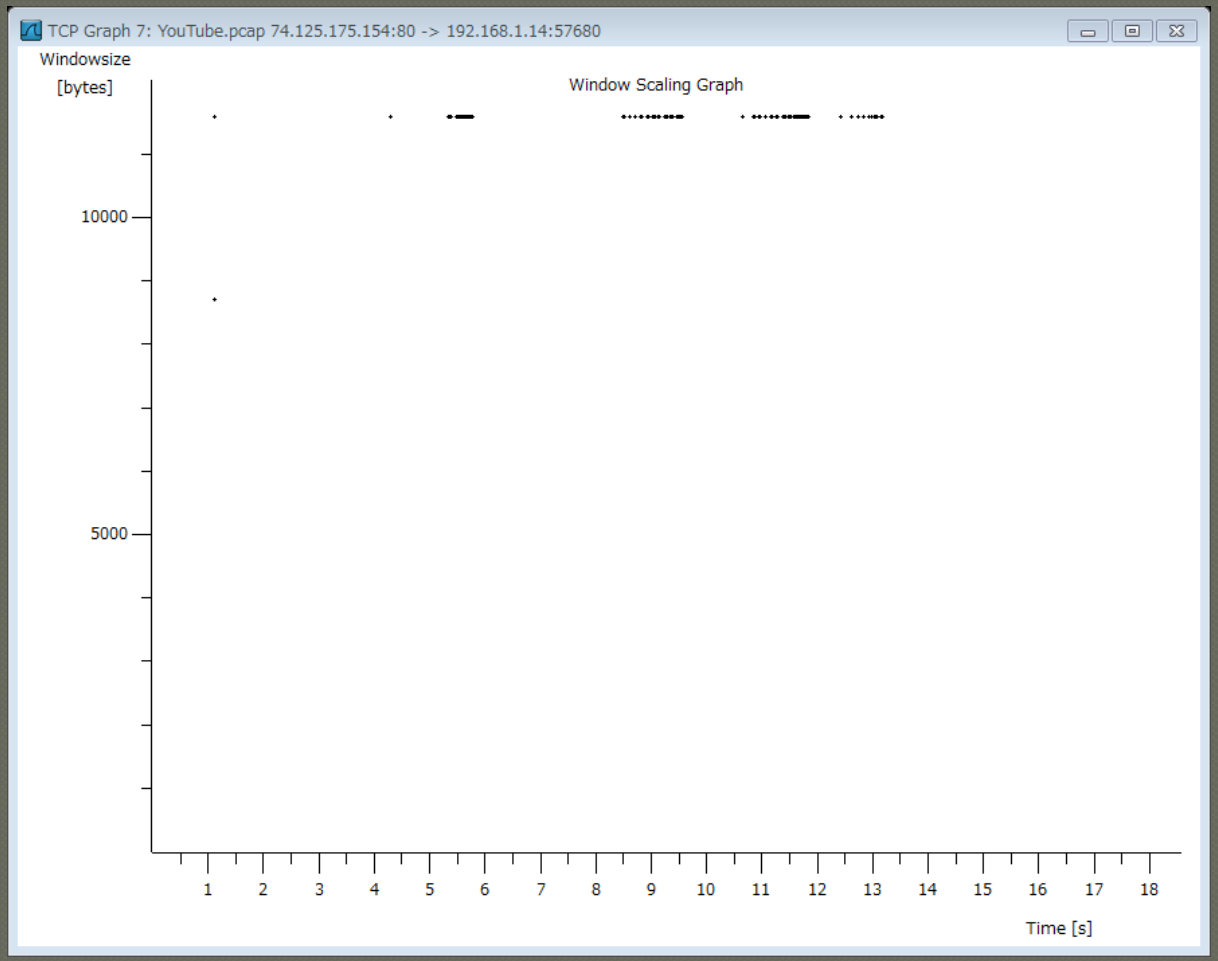
# Time/Sequence (Stevens)



# Time/Sequence (tcptrace)



# Window Scaling



# 参考資料

- **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/