Wireshark で見る プロトコル

プロトコルの特徴を知る

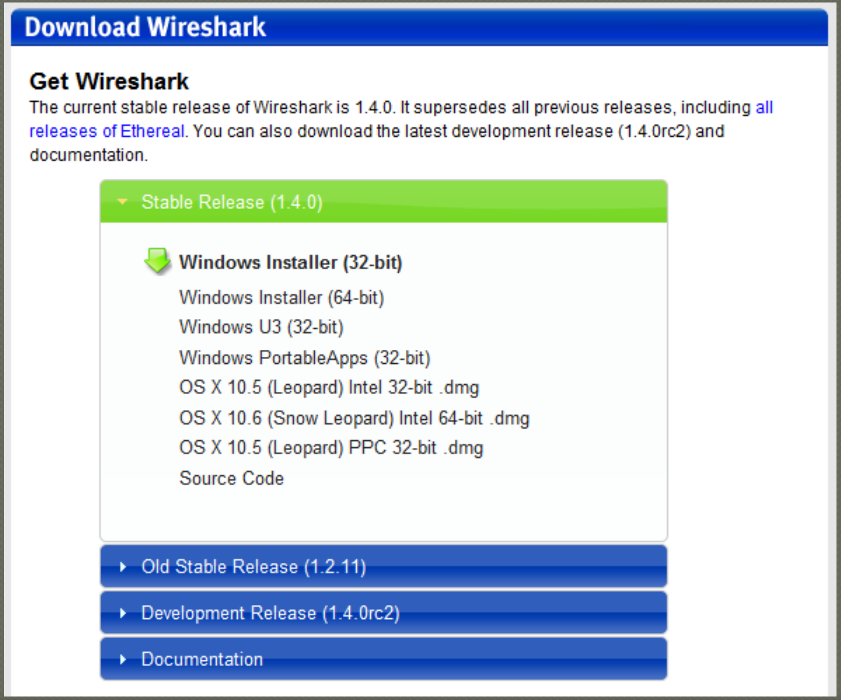
hebikuzure

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/



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

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

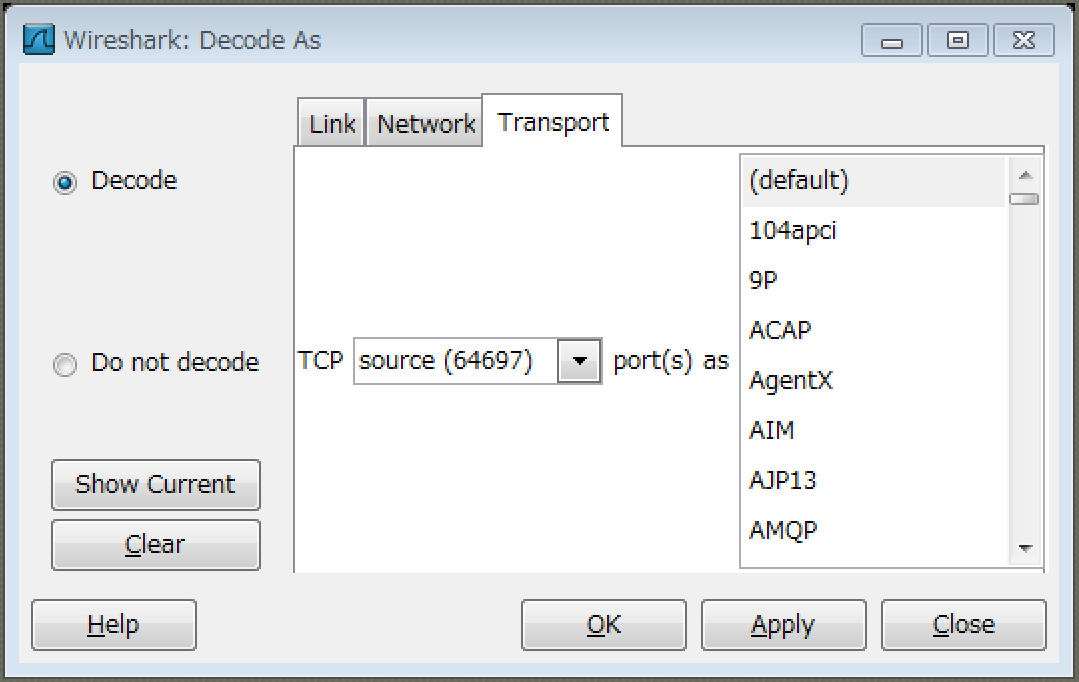
- 正しく解析されない場合も多い
- 特にトランスポート層で既定のポート以外を使い通信を行っている場合
- ex.
  - 81番ポートでHTTP
  - 443番ポート以外でのHTTPS

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

● Decode

○ Do not decode

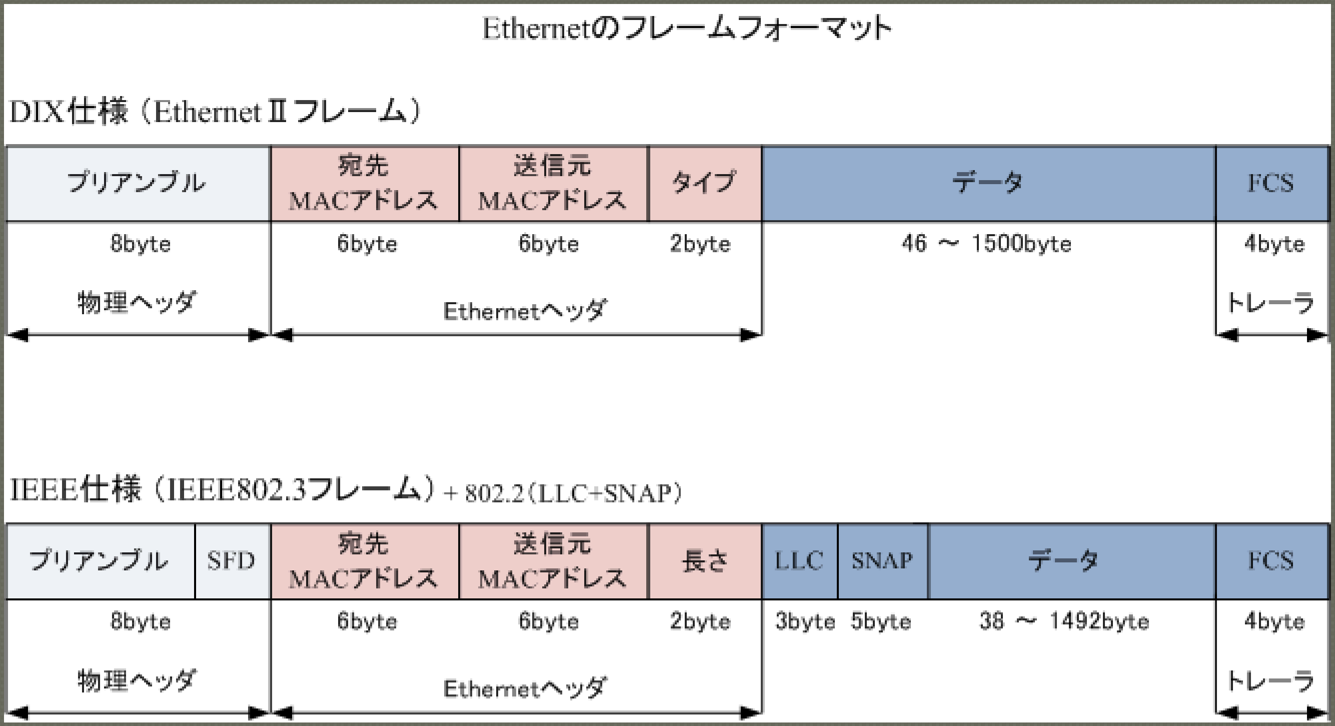
TCP source (64697) port(s) as (default)

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（Ethernet Ⅱ フレーム）

プリアンブル	宛先 MACアドレス	送信元 MACアドレス	タイプ	データ	FCS
8byte	6byte	6byte	2byte	46 〜 1500byte	4byte
物理ヘッダ	Ethernetヘッダ				トレーラ

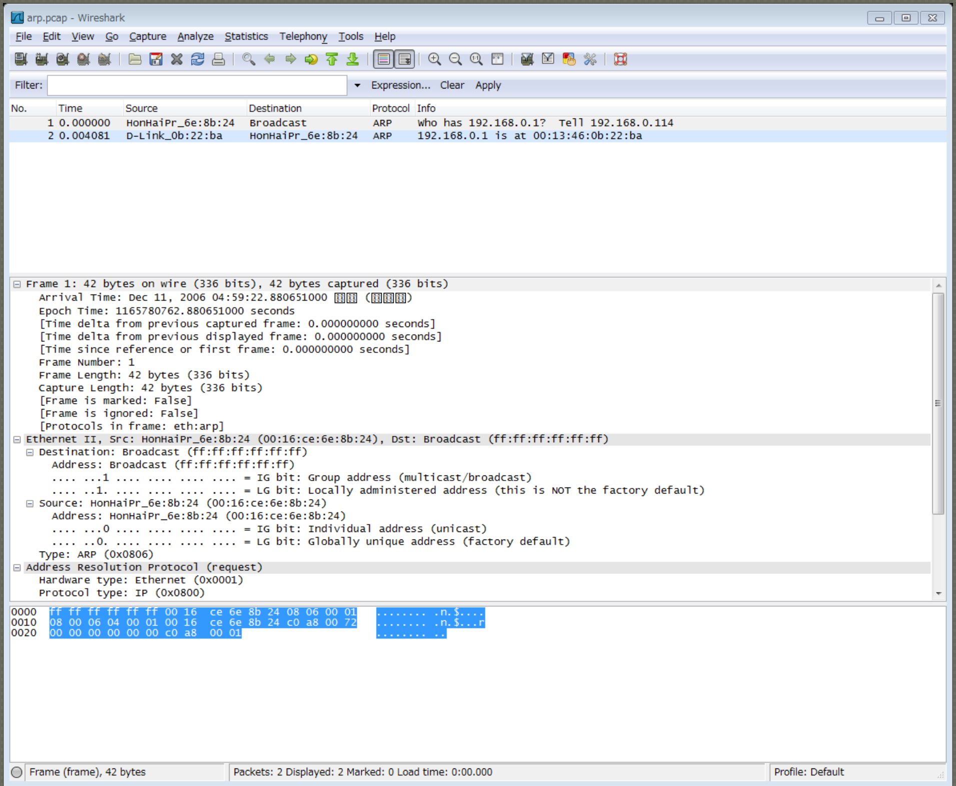
IEEE仕様（IEEE802.3フレーム）+ 802.2（LLC+SNAP）

プリアンブル	SFD	宛先 MACアドレス	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		Ethernet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


arp.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

```
No.   Time      Source             Destination        Protocol Info
    1 0.000000  HonHaiPr_6e:8b:24  Broadcast          ARP      Who has 192.168.0.1?  Tell 192.168.0.114
    2 0.004081  D-Link_0b:22:ba    HonHaiPr_6e:8b:24  ARP      192.168.0.1 is at 00:13:46:0b:22:ba
```

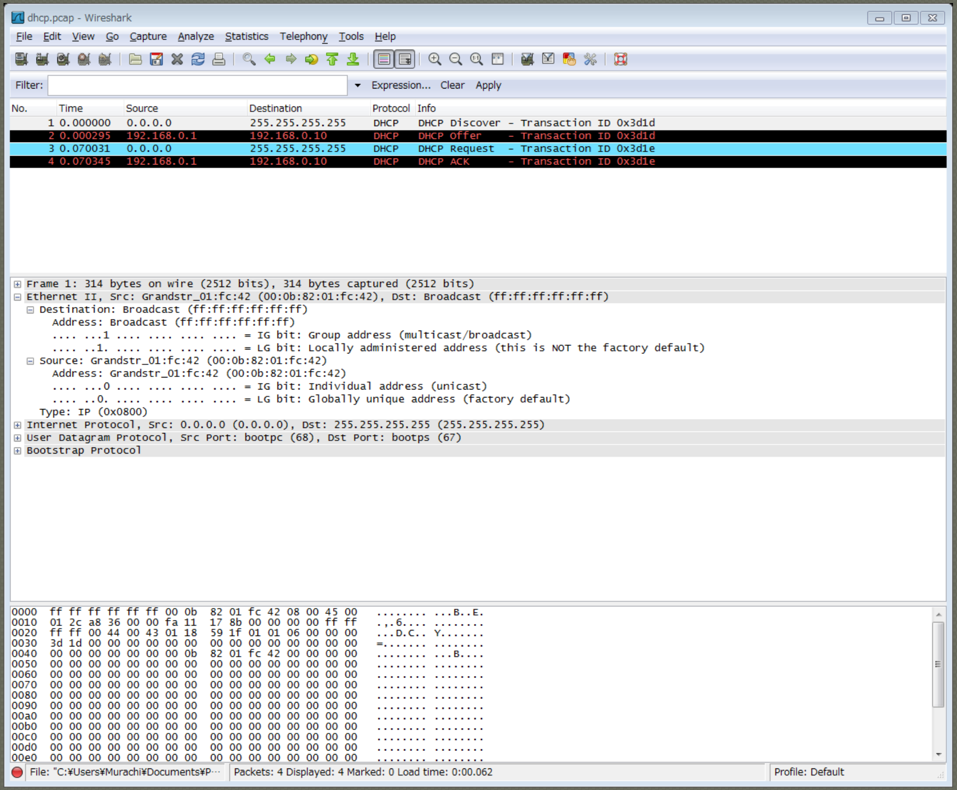
```
⊟ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
    Arrival Time: Dec 11, 2006 04:59:22.880651000 □□ (□□□□)
    Epoch Time: 1165780762.880651000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 42 bytes (336 bits)
    Capture Length: 42 bytes (336 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:arp]
⊟ Ethernet II, Src: HonHaiPr_6e:8b:24 (00:16:ce:6e:8b:24), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊟ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
  ⊟ Source: HonHaiPr_6e:8b:24 (00:16:ce:6e:8b:24)
      Address: HonHaiPr_6e:8b:24 (00:16:ce:6e:8b:24)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: ARP (0x0806)
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
```

```
0000  ff ff ff ff ff ff 00 16  ce 6e 8b 24 08 06 00 01   ........ .n.$....
0010  08 00 06 04 00 01 00 16  ce 6e 8b 24 c0 a8 00 72   ........ .n.$...r
0020  00 00 00 00 00 00 c0 a8  00 01                     ........ ..
```

Frame (frame), 42 bytes | Packets: 2 Displayed: 2 Marked: 0 Load time: 0:00.000 | Profile: Default

DHCP

- Discover ⇒ Offer ⇒ Request ⇒ ACK
  - dhcp.pcap



```
No.     Time        Source         Destination      Protocol Info
      1 0.000000    0.0.0.0        255.255.255.255  DHCP     DHCP Discover - Transaction ID 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 0x3d1e
      4 0.070345    192.168.0.1    192.168.0.10     DHCP     DHCP ACK      - Transaction ID 0x3d1e
```

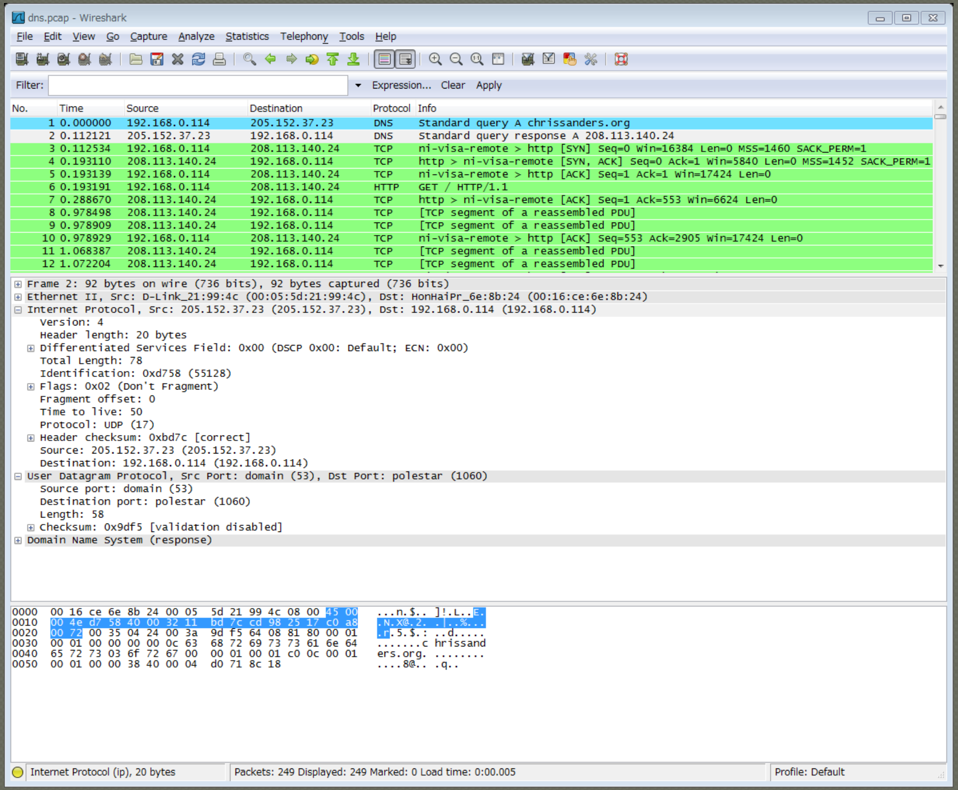
```
⊞ Frame 1: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits)
⊟ Ethernet II, Src: Grandstr_01:fc:42 (00:0b:82:01:fc:42), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊟ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
  ⊟ Source: Grandstr_01:fc:42 (00:0b:82:01:fc:42)
      Address: Grandstr_01:fc:42 (00:0b:82:01:fc:42)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
⊞ Bootstrap Protocol
```

```
0000  ff ff ff ff ff ff 00 0b  82 01 fc 42 08 00 45 00   ........ ...B..E.
0010  01 2c a8 36 00 00 fa 11  17 8b 00 00 00 00 ff ff   .,.6.... ........
0020  ff ff 00 44 00 43 01 18  59 1f 01 01 06 00 00 00   ...D.C.. Y.......
0030  3d 1d 00 00 00 00 00 00  00 00 00 00 00 00 00 00   =....... ........
0040  00 00 00 00 00 00 00 0b  82 01 fc 42 00 00 00 00   ........ ...B....
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

File: "C:¥Users¥Murachi¥Documents¥P··· Packets: 4 Displayed: 4 Marked: 0 Load time: 0:00.062

DNS

- UDP でダメなら TCP
  - dns.pcap



dns.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

```
No.  Time        Source          Destination     Protocol Info
   1 0.000000    192.168.0.114   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=1460 SACK_PERM=1
   4 0.193110    208.113.140.24  192.168.0.114   TCP      http > ni-visa-remote [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1452 SACK_PERM=1
   5 0.193139    192.168.0.114   208.113.140.24  TCP      ni-visa-remote > http [ACK] Seq=1 Ack=1 Win=17424 Len=0
   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]
  10 0.978929    192.168.0.114   208.113.140.24  TCP      ni-visa-remote > http [ACK] Seq=553 Ack=2905 Win=17424 Len=0
  11 1.068387    208.113.140.24  192.168.0.114   TCP      [TCP segment of a reassembled PDU]
  12 1.072204    208.113.140.24  192.168.0.114   TCP      [TCP segment of a reassembled PDU]
```

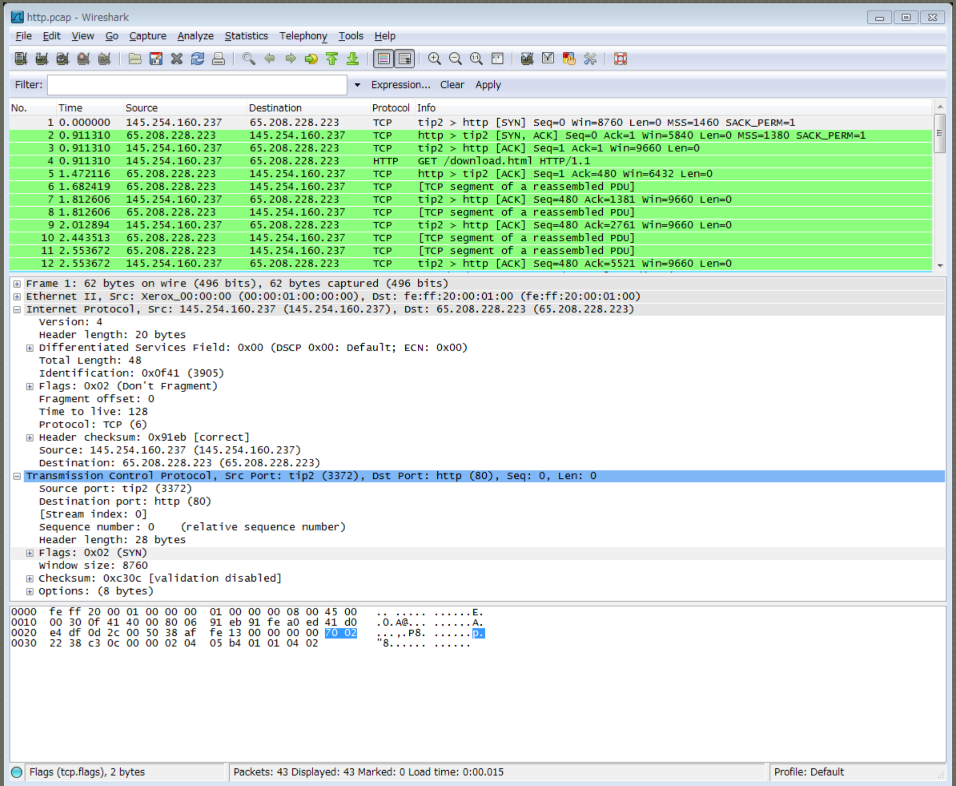
```
⊞ Frame 2: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
⊞ Ethernet II, Src: D-Link_21:99:4c (00:05:5d:21:99:4c), Dst: HonHaiPr_6e:8b:24 (00:16:ce:6e:8b:24)
⊟ Internet Protocol, Src: 205.152.37.23 (205.152.37.23), Dst: 192.168.0.114 (192.168.0.114)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 78
    Identification: 0xd758 (55128)
  ⊞ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 50
    Protocol: UDP (17)
  ⊞ Header checksum: 0xbd7c [correct]
    Source: 205.152.37.23 (205.152.37.23)
    Destination: 192.168.0.114 (192.168.0.114)
⊟ User Datagram Protocol, Src Port: domain (53), Dst Port: polestar (1060)
    Source port: domain (53)
    Destination port: polestar (1060)
    Length: 58
  ⊞ Checksum: 0x9df5 [validation disabled]
⊞ Domain Name System (response)
```

```
0000  00 16 ce 6e 8b 24 00 05  5d 21 99 4c 08 00 45 00   ...n.$.. ]!.L..E.
0010  00 4e d7 58 40 00 32 11  bd 7c cd 98 25 17 c0 a8   .N.X@.2. .|..%...
0020  00 72 00 35 04 24 00 3a  9d f5 64 08 81 80 00 01   .r.5.$.: ..d.....
0030  00 01 00 00 00 00 0c 63  68 72 69 73 73 61 6e 64   .......c hrissand
0040  65 72 73 03 6f 72 67 00  00 01 00 01 c0 0c 00 01   ers.org. ........
0050  00 01 00 00 38 40 00 04  d0 71 8c 18               ....8@.. .q..
```

Internet Protocol (ip), 20 bytes | Packets: 249 Displayed: 249 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 - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

```
No.   Time      Source           Destination      Protocol Info
    1 0.000000  145.254.160.237  65.208.228.223   TCP      tip2 > http [SYN] Seq=0 Win=8760 Len=0 MSS=1460 SACK_PERM=1
    2 0.911310  65.208.228.223   145.254.160.237  TCP      http > tip2 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1
    3 0.911310  145.254.160.237  65.208.228.223   TCP      tip2 > http [ACK] Seq=1 Ack=1 Win=9660 Len=0
    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  TCP      [TCP segment of a reassembled PDU]
    7 1.812606  145.254.160.237  65.208.228.223   TCP      tip2 > http [ACK] Seq=480 Ack=1381 Win=9660 Len=0
    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 2.553672  145.254.160.237  65.208.228.223   TCP      tip2 > http [ACK] Seq=480 Ack=5521 Win=9660 Len=0
```

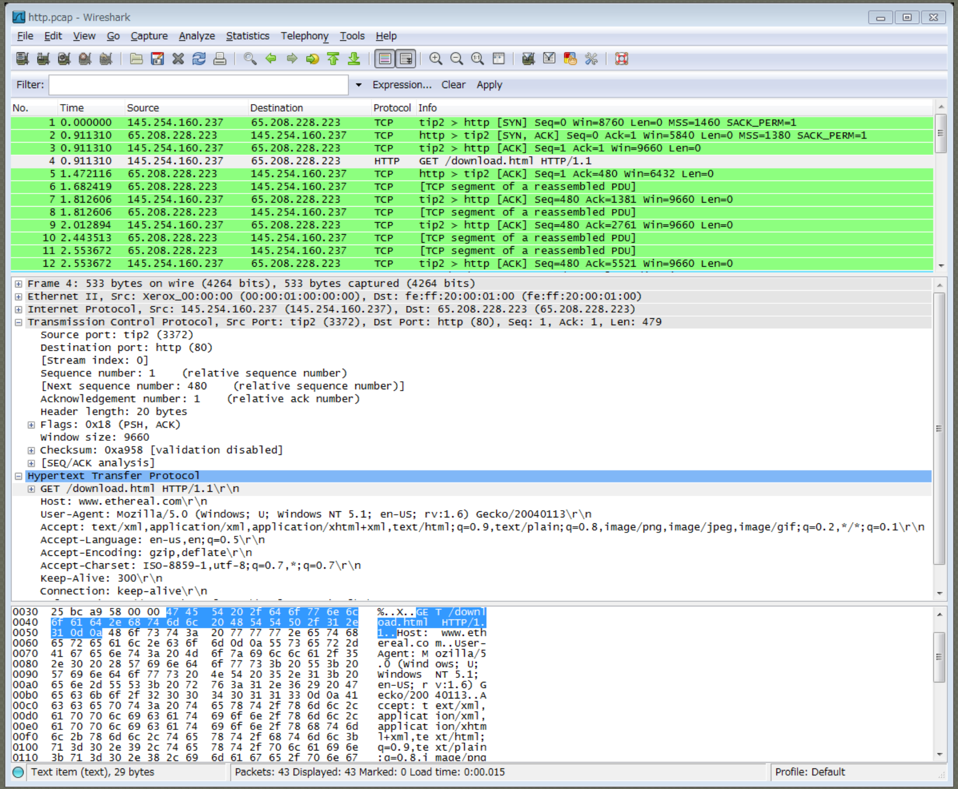
```
⊞ Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
⊞ Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
⊟ Internet Protocol, Src: 145.254.160.237 (145.254.160.237), Dst: 65.208.228.223 (65.208.228.223)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 48
    Identification: 0x0f41 (3905)
  ⊞ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
  ⊞ Header checksum: 0x91eb [correct]
    Source: 145.254.160.237 (145.254.160.237)
    Destination: 65.208.228.223 (65.208.228.223)
⊟ Transmission Control Protocol, Src Port: tip2 (3372), Dst Port: http (80), Seq: 0, Len: 0
    Source port: tip2 (3372)
    Destination port: http (80)
    [Stream index: 0]
    Sequence number: 0    (relative sequence number)
    Header length: 28 bytes
  ⊞ Flags: 0x02 (SYN)
    Window size: 8760
  ⊞ Checksum: 0xc30c [validation disabled]
  ⊞ Options: (8 bytes)
```

```
0000  fe ff 20 00 01 00 00 00  01 00 00 00 08 00 45 00   .. ..... ......E.
0010  00 30 0f 41 40 00 80 06  91 eb 91 fe a0 ed 41 d0   .0.A@... ......A.
0020  e4 df 0d 2c 00 50 38 af  fe 13 00 00 00 00 70 02   ...,.P8. ......p.
0030  22 38 c3 0c 00 00 02 04  05 b4 01 01 04 02         "8...... ......
```

Flags (tcp.flags), 2 bytes | Packets: 43 Displayed: 43 Marked: 0 Load 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


http.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression...
Clear
Apply

```
No.   Time      Source           Destination      Protocol Info
    1 0.000000  145.254.160.237  65.208.228.223   TCP      tip2 > http [SYN] Seq=0 Win=8760 Len=0 MSS=1460 SACK_PERM=1
    2 0.911310  65.208.228.223   145.254.160.237  TCP      http > tip2 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1
    3 0.911310  145.254.160.237  65.208.228.223   TCP      tip2 > http [ACK] Seq=1 Ack=1 Win=9660 Len=0
    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  TCP      [TCP segment of a reassembled PDU]
    7 1.812606  145.254.160.237  65.208.228.223   TCP      tip2 > http [ACK] Seq=480 Ack=1381 Win=9660 Len=0
    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 2.553672  145.254.160.237  65.208.228.223   TCP      tip2 > http [ACK] Seq=480 Ack=5521 Win=9660 Len=0
```

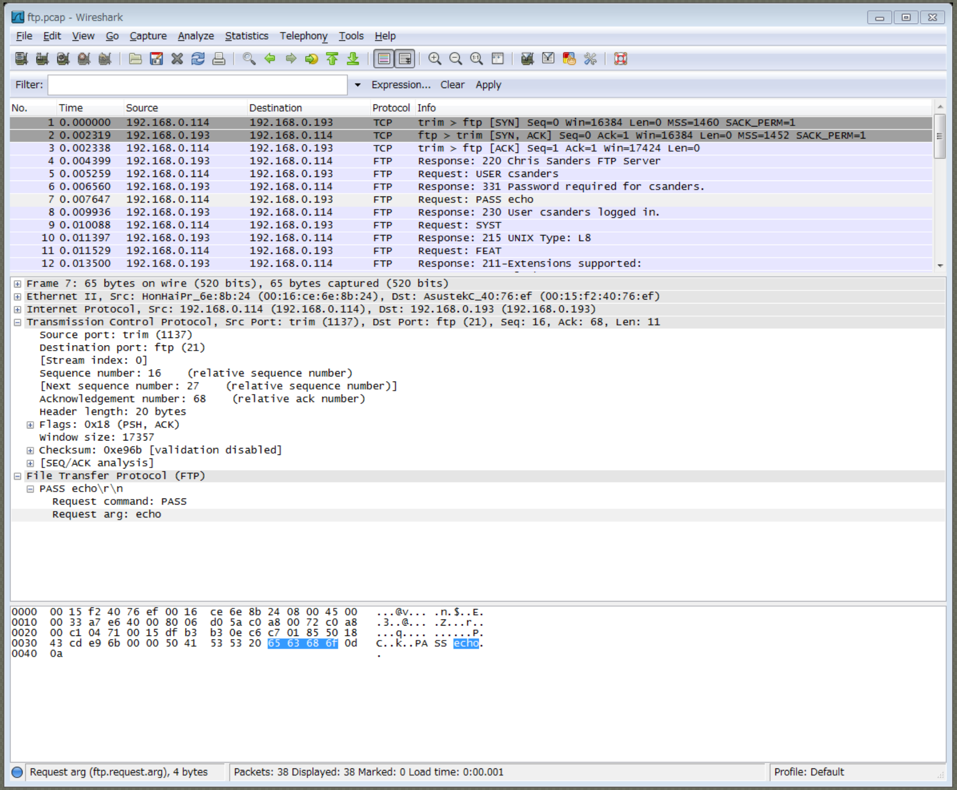
```
⊞ Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)
⊞ Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
⊞ Internet Protocol, Src: 145.254.160.237 (145.254.160.237), Dst: 65.208.228.223 (65.208.228.223)
⊟ Transmission Control Protocol, Src Port: tip2 (3372), Dst Port: http (80), Seq: 1, Ack: 1, Len: 479
    Source port: tip2 (3372)
    Destination port: http (80)
    [Stream index: 0]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 480    (relative sequence number)]
    Acknowledgement number: 1    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x18 (PSH, ACK)
    Window size: 9660
  ⊞ Checksum: 0xa958 [validation disabled]
  ⊞ [SEQ/ACK analysis]
⊟ Hypertext Transfer Protocol
  ⊞ GET /download.html HTTP/1.1\r\n
    Host: www.ethereal.com\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113\r\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=0.2,*/*;q=0.1\r\n
    Accept-Language: en-us,en;q=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
```

```
0030  25 bc a9 58 00 00 47 45  54 20 2f 64 6f 77 6e 6c   %..X..GE T /downl
0040  6f 61 64 2e 68 74 6d 6c  20 48 54 54 50 2f 31 2e   oad.html  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 77 77 77 2e 65 74 68   1..Host:  www.eth
0060  65 72 65 61 6c 2e 63 6f  6d 0d 0a 55 73 65 72 2d   ereal.co m..User-
0070  41 67 65 6e 74 3a 20 4d  6f 7a 69 6c 6c 61 2f 35   Agent: M ozilla/5
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   Windows  NT 5.1;
00a0  65 6e 2d 55 53 3b 20 72  76 3a 31 2e 36 29 20 47   en-US; r v:1.6) G
00b0  65 63 6b 6f 2f 32 30 30  34 30 31 31 33 0d 0a 41   ecko/200 40113..A
00c0  63 63 65 70 74 3a 20 74  65 78 74 2f 78 6d 6c 2c   ccept: t ext/xml,
00d0  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 6d 6c 2c   applicat ion/xml,
00e0  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 68 74 6d   applicat ion/xhtm
00f0  6c 2b 78 6d 6c 2c 74 65  78 74 2f 68 74 6d 6c 3b   l+xml,te xt/html;
0100  71 3d 30 2e 39 2c 74 65  78 74 2f 70 6c 61 69 6e   q=0.9,te xt/plain
0110  3b 71 3d 30 2e 38 2c 69  6d 61 67 65 2f 70 6e 67   ;q=0.8,i mage/png
```

Text item (text), 29 bytes | Packets: 43 Displayed: 43 Marked: 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 - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

```
No.   Time       Source          Destination     Protocol Info
    1 0.000000   192.168.0.114   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   192.168.0.114   192.168.0.193   FTP      Request: PASS echo
    8 0.009936   192.168.0.193   192.168.0.114   FTP      Response: 230 User csanders logged in.
    9 0.010088   192.168.0.114   192.168.0.193   FTP      Request: SYST
   10 0.011397   192.168.0.193   192.168.0.114   FTP      Response: 215 UNIX Type: L8
   11 0.011529   192.168.0.114   192.168.0.193   FTP      Request: FEAT
   12 0.013500   192.168.0.193   192.168.0.114   FTP      Response: 211-Extensions supported:
```

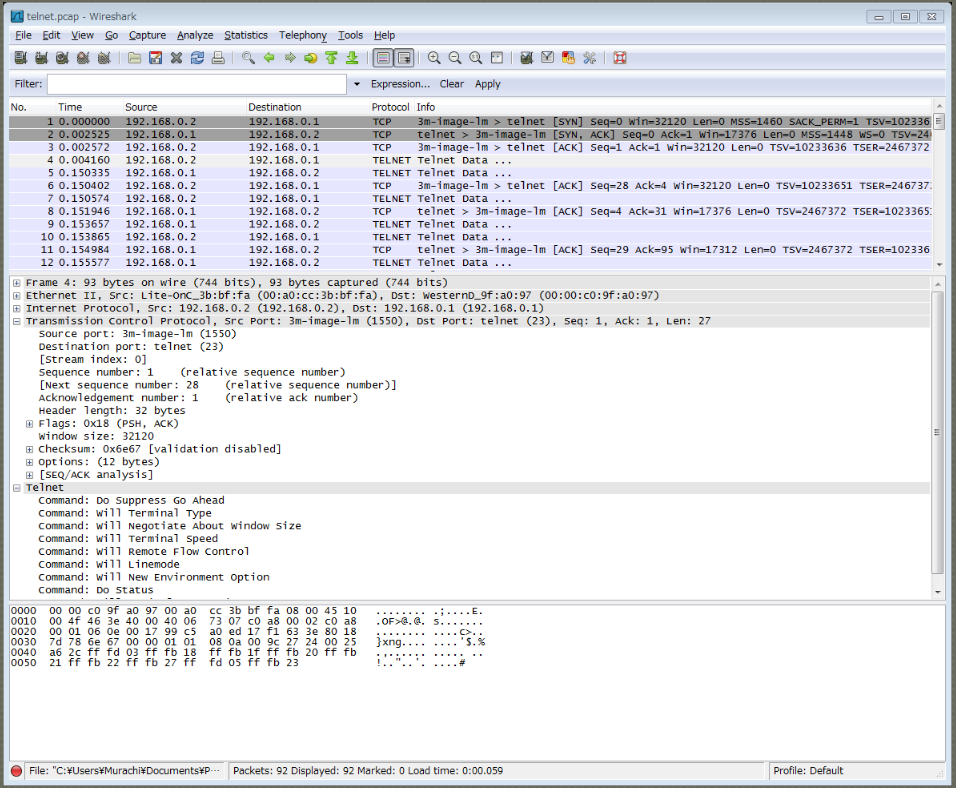
```
⊞ Frame 7: 65 bytes on wire (520 bits), 65 bytes captured (520 bits)
⊞ Ethernet II, Src: HonHaiPr_6e:8b:24 (00:16:ce:6e:8b:24), Dst: AsustekC_40:76:ef (00:15:f2:40:76:ef)
⊞ Internet Protocol, Src: 192.168.0.114 (192.168.0.114), Dst: 192.168.0.193 (192.168.0.193)
⊟ Transmission Control Protocol, Src Port: trim (1137), Dst Port: ftp (21), Seq: 16, Ack: 68, Len: 11
    Source port: trim (1137)
    Destination port: ftp (21)
    [Stream index: 0]
    Sequence number: 16    (relative sequence number)
    [Next sequence number: 27    (relative sequence number)]
    Acknowledgement number: 68    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x18 (PSH, ACK)
    Window size: 17357
  ⊞ Checksum: 0xe96b [validation disabled]
  ⊞ [SEQ/ACK analysis]
⊟ File Transfer Protocol (FTP)
  ⊟ PASS echo\r\n
      Request command: PASS
      Request arg: echo
```

```
0000  00 15 f2 40 76 ef 00 16  ce 6e 8b 24 08 00 45 00   ...@v... .n.$..E.
0010  00 33 a7 e6 40 00 80 06  d0 5a c0 a8 00 72 c0 a8   .3..@... .Z...r..
0020  00 c1 04 71 00 15 df b3  b3 0e c6 c7 01 85 50 18   ...q.... ......P.
0030  43 cd e9 6b 00 00 50 41  53 53 20 65 63 68 6f 0d   C..k..PA SS echo.
0040  0a                                                 .
```

● Request arg (ftp.request.arg), 4 bytes | Packets: 38 Displayed: 38 Marked: 0 Load time: 0:00.001 | Profile: Default

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



telnet.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

```
No.   Time      Source        Destination   Protocol Info
    1 0.000000  192.168.0.2   192.168.0.1   TCP      3m-image-lm > telnet [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSV=102336
    2 0.002525  192.168.0.1   192.168.0.2   TCP      telnet > 3m-image-lm [SYN, ACK] Seq=0 Ack=1 Win=17376 Len=0 MSS=1448 WS=0 TSV=24
    3 0.002572  192.168.0.2   192.168.0.1   TCP      3m-image-lm > telnet [ACK] Seq=1 Ack=1 Win=32120 Len=0 TSV=10233636 TSER=2467372
    4 0.004160  192.168.0.2   192.168.0.1   TELNET   Telnet Data ...
    5 0.150335  192.168.0.1   192.168.0.2   TELNET   Telnet Data ...
    6 0.150402  192.168.0.2   192.168.0.1   TCP      3m-image-lm > telnet [ACK] Seq=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 ...
    8 0.151946  192.168.0.1   192.168.0.2   TCP      telnet > 3m-image-lm [ACK] Seq=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 ...
   10 0.153865  192.168.0.2   192.168.0.1   TELNET   Telnet Data ...
   11 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
   12 0.155577  192.168.0.1   192.168.0.2   TELNET   Telnet Data ...
```

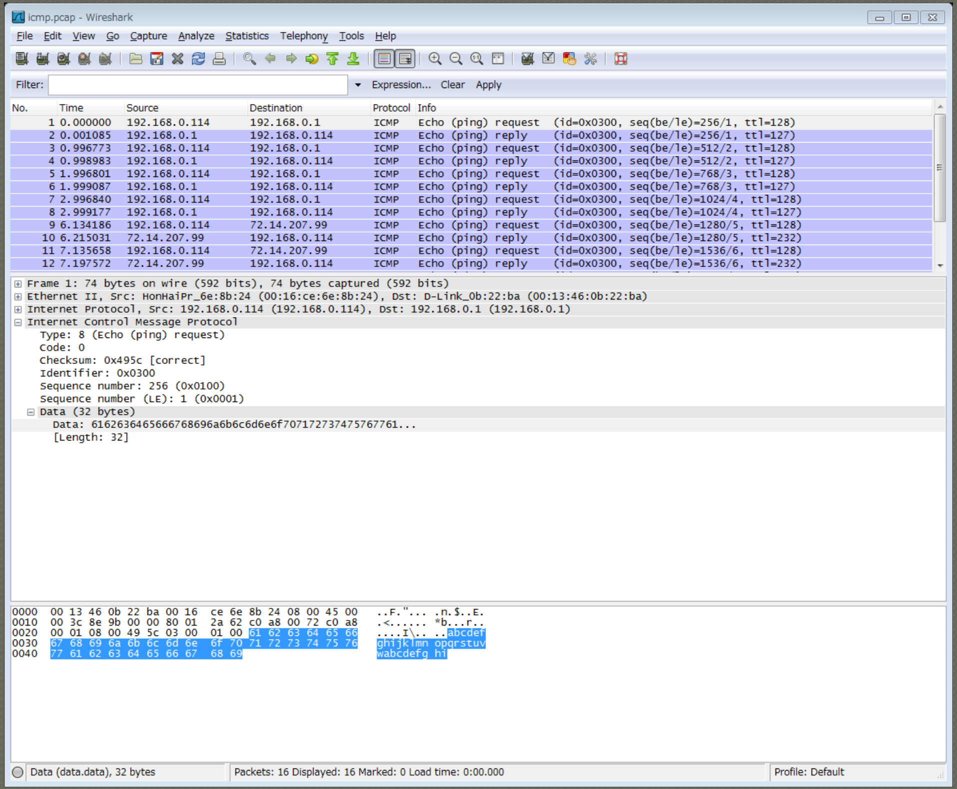
```
⊞ Frame 4: 93 bytes on wire (744 bits), 93 bytes captured (744 bits)
⊞ Ethernet II, Src: Lite-OnC_3b:bf:fa (00:a0:cc:3b:bf:fa), Dst: WesternD_9f:a0:97 (00:00:c0:9f:a0:97)
⊞ Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
⊟ Transmission Control Protocol, Src Port: 3m-image-lm (1550), Dst Port: telnet (23), Seq: 1, Ack: 1, Len: 27
    Source port: 3m-image-lm (1550)
    Destination port: telnet (23)
    [Stream index: 0]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 28    (relative sequence number)]
    Acknowledgement number: 1    (relative ack number)
    Header length: 32 bytes
  ⊞ Flags: 0x18 (PSH, ACK)
    Window size: 32120
  ⊞ Checksum: 0x6e67 [validation disabled]
  ⊞ Options: (12 bytes)
  ⊞ [SEQ/ACK analysis]
⊟ Telnet
    Command: Do Suppress Go Ahead
    Command: Will Terminal Type
    Command: Will Negotiate About Window Size
    Command: Will Terminal Speed
    Command: Will Remote Flow Control
    Command: Will Linemode
    Command: Will New Environment Option
    Command: Do Status
```

```
0000  00 00 c0 9f a0 97 00 a0  cc 3b bf fa 08 00 45 10   ........ .;....E.
0010  00 4f 46 3e 40 00 40 06  73 07 c0 a8 00 02 c0 a8   .OF>@.@. s.......
0020  00 01 06 0e 00 17 99 c5  a0 ed 17 f1 63 3e 80 18   ........ ....c>..
0030  7d 78 6e 67 00 00 01 01  08 0a 00 9c 27 24 00 25   }xng.... ....'$.%
0040  a6 2c ff fd 03 ff fb 18  ff fb 1f ff fb 20 ff fb   .,...... ..... ..
0050  21 ff fb 22 ff fb 27 ff  fd 05 ff fb 23            !..".'. ....#
```

File: "C:¥Users¥Murachi¥Documents¥P··· Packets: 92 Displayed: 92 Marked: 0 Load time: 0:00.059 Profile: Default

ICMP

- ユーティリティ プロトコル
  - icmp.pcap



```
No.   Time       Source          Destination      Protocol Info
    1 0.000000   192.168.0.114   192.168.0.1      ICMP   Echo (ping) request  (id=0x0300, seq(be/le)=256/1, ttl=128)
    2 0.001085   192.168.0.1     192.168.0.114    ICMP   Echo (ping) reply    (id=0x0300, seq(be/le)=256/1, ttl=127)
    3 0.996773   192.168.0.114   192.168.0.1      ICMP   Echo (ping) request  (id=0x0300, seq(be/le)=512/2, ttl=128)
    4 0.998983   192.168.0.1     192.168.0.114    ICMP   Echo (ping) reply    (id=0x0300, seq(be/le)=512/2, ttl=127)
    5 1.996801   192.168.0.114   192.168.0.1      ICMP   Echo (ping) request  (id=0x0300, seq(be/le)=768/3, ttl=128)
    6 1.999087   192.168.0.1     192.168.0.114    ICMP   Echo (ping) reply    (id=0x0300, seq(be/le)=768/3, ttl=127)
    7 2.996840   192.168.0.114   192.168.0.1      ICMP   Echo (ping) request  (id=0x0300, seq(be/le)=1024/4, ttl=128)
    8 2.999177   192.168.0.1     192.168.0.114    ICMP   Echo (ping) reply    (id=0x0300, seq(be/le)=1024/4, ttl=127)
    9 6.134186   192.168.0.114   72.14.207.99     ICMP   Echo (ping) request  (id=0x0300, seq(be/le)=1280/5, ttl=128)
   10 6.215031   72.14.207.99    192.168.0.114    ICMP   Echo (ping) reply    (id=0x0300, seq(be/le)=1280/5, ttl=232)
   11 7.135658   192.168.0.114   72.14.207.99     ICMP   Echo (ping) request  (id=0x0300, seq(be/le)=1536/6, ttl=128)
   12 7.197572   72.14.207.99    192.168.0.114    ICMP   Echo (ping) reply    (id=0x0300, seq(be/le)=1536/6, ttl=232)
```

```
⊞ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
⊞ Ethernet II, Src: HonHaiPr_6e:8b:24 (00:16:ce:6e:8b:24), Dst: D-Link_0b:22:ba (00:13:46:0b:22:ba)
⊞ Internet Protocol, Src: 192.168.0.114 (192.168.0.114), Dst: 192.168.0.1 (192.168.0.1)
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x495c [correct]
    Identifier: 0x0300
    Sequence number: 256 (0x0100)
    Sequence number (LE): 1 (0x0001)
  ⊟ Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677761...
      [Length: 32]
```

```
0000  00 13 46 0b 22 ba 00 16  ce 6e 8b 24 08 00 45 00   ..F."... .n.$..E.
0010  00 3c 8e 9b 00 00 80 01  2a 62 c0 a8 00 72 c0 a8   .<...... *b...r..
0020  00 01 08 00 49 5c 03 00  01 00 61 62 63 64 65 66   ....I\.. ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

```
○ Data (data.data), 32 bytes | Packets: 16 Displayed: 16 Marked: 0 Load time: 0:00.000 | Profile: Default
```

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/