

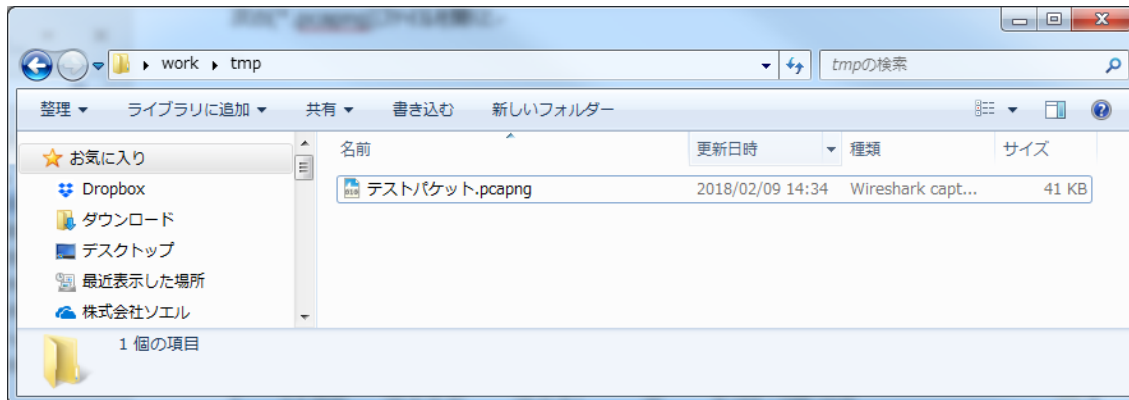
Wireshark の使い方

作成日: 2018/03/12

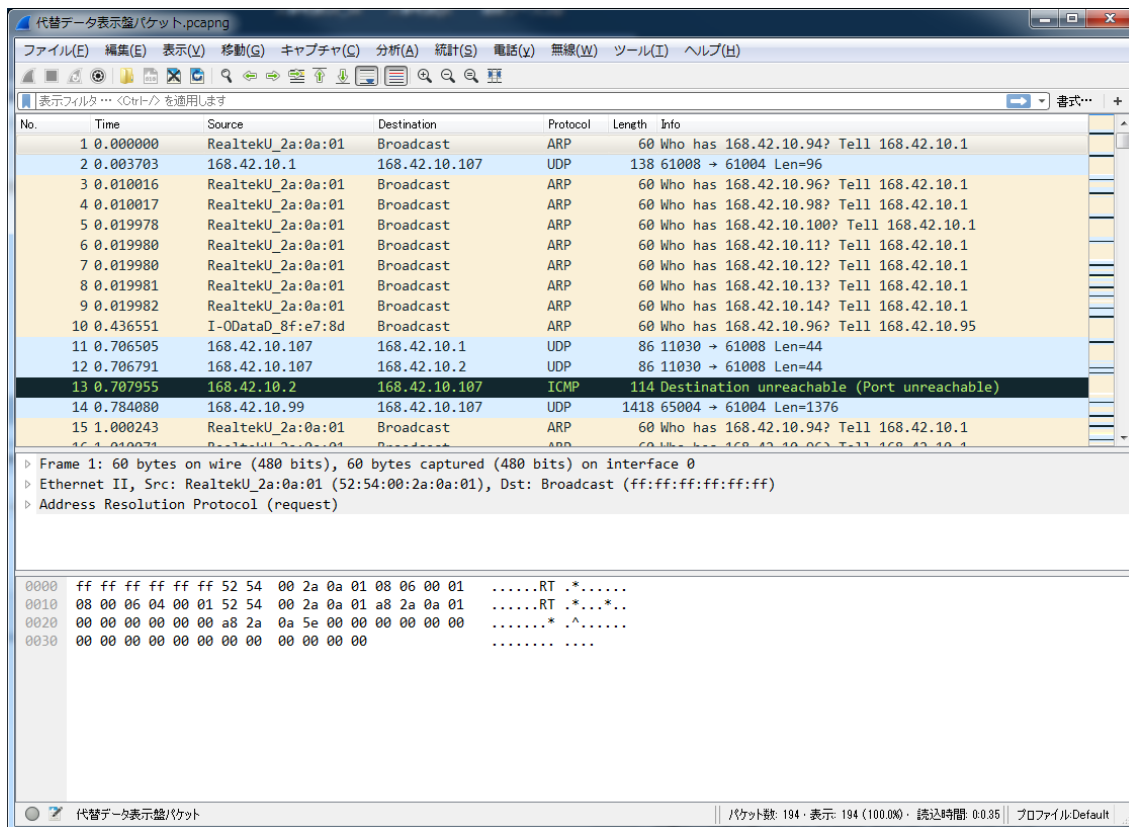
作成者: 小木曾

Wireshark のログファイルの確認

次の(*.pcapng)ファイルを開くと



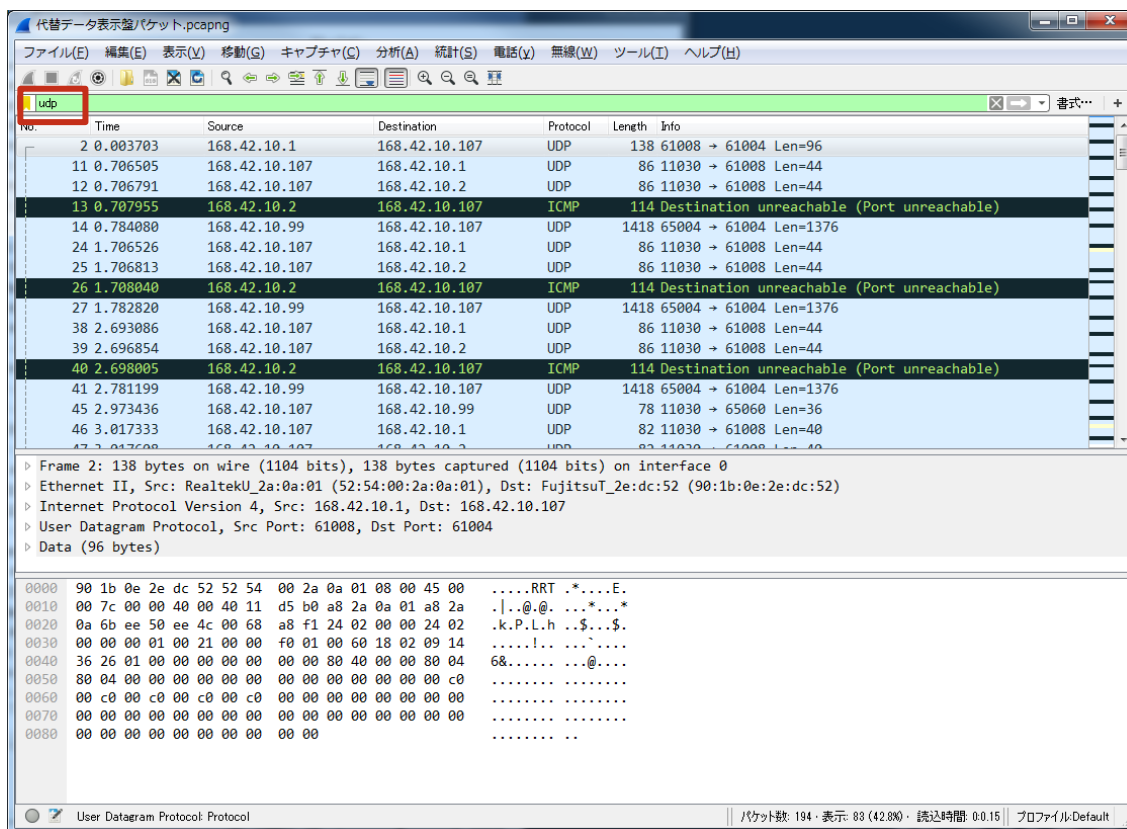
Wireshark では次のように表示されます。



通信情報の絞込み

ここで、全体の中から UDP 通信だけ確認してみましょう。

表示フィルタ…と記述されたところに、udp と入力し、Enter を押します。すると UDP 通信だけが、抽出されます。



データの確認

一番上のパネルの説明を行います。

Time は、データ記録からの時間

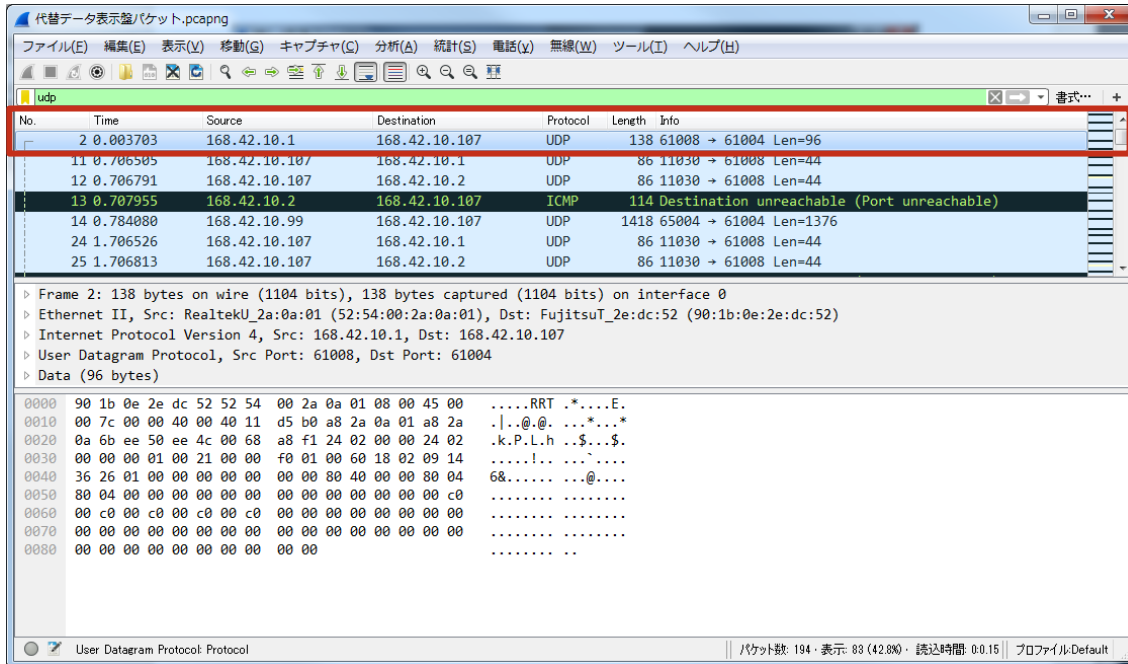
Source は、送信元の IP アドレス

Destination は、送信先の IP アドレス

Length は、通信データの Byte 数

通信の内容を詳しく確認するために、このパネルから確認したい通信情報を選択します。

ここでは、No.2 のデータを使い説明します。



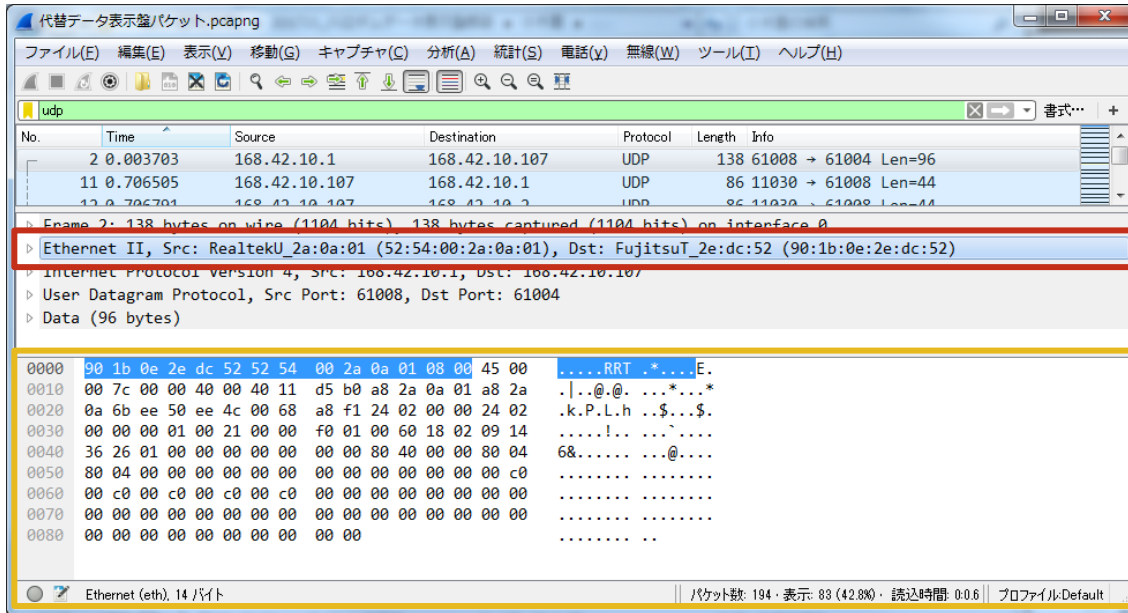
このログファイルの記録は、ローカル IP アドレス 168.42.10.107 で行われています。No.2 は 168.42.10.1 から、UDP のデータが送信されてきました。

UDP 通信データのフォーマットは以下です。

		イーサネットヘッダ 14byte		IPヘッダ 20byte						UDPヘッダ 8byte								
プリアンブル	SYN C	宛先 M A C アドレス	宛先 M A C アドレス	* 全 データ長	* 識 別子	* 生 存 時 間	* 1 1 H	* チ ェ ッ ク サ ム	* 送 信 元 I P ア ド レ ス	* 4 バ イ ト	* 宛 先 I P ア ド レ ス	* 4 バ イ ト	* 送 信 元 ポ ー ト	* 宛 先 ポ ー ト	* U D P デ ー タ 長	* チ ェ ッ ク サ ム	* デ ー タ	* チ ェ ッ ク コ ー ド
		6 バ イ ト	6 バ イ ト															

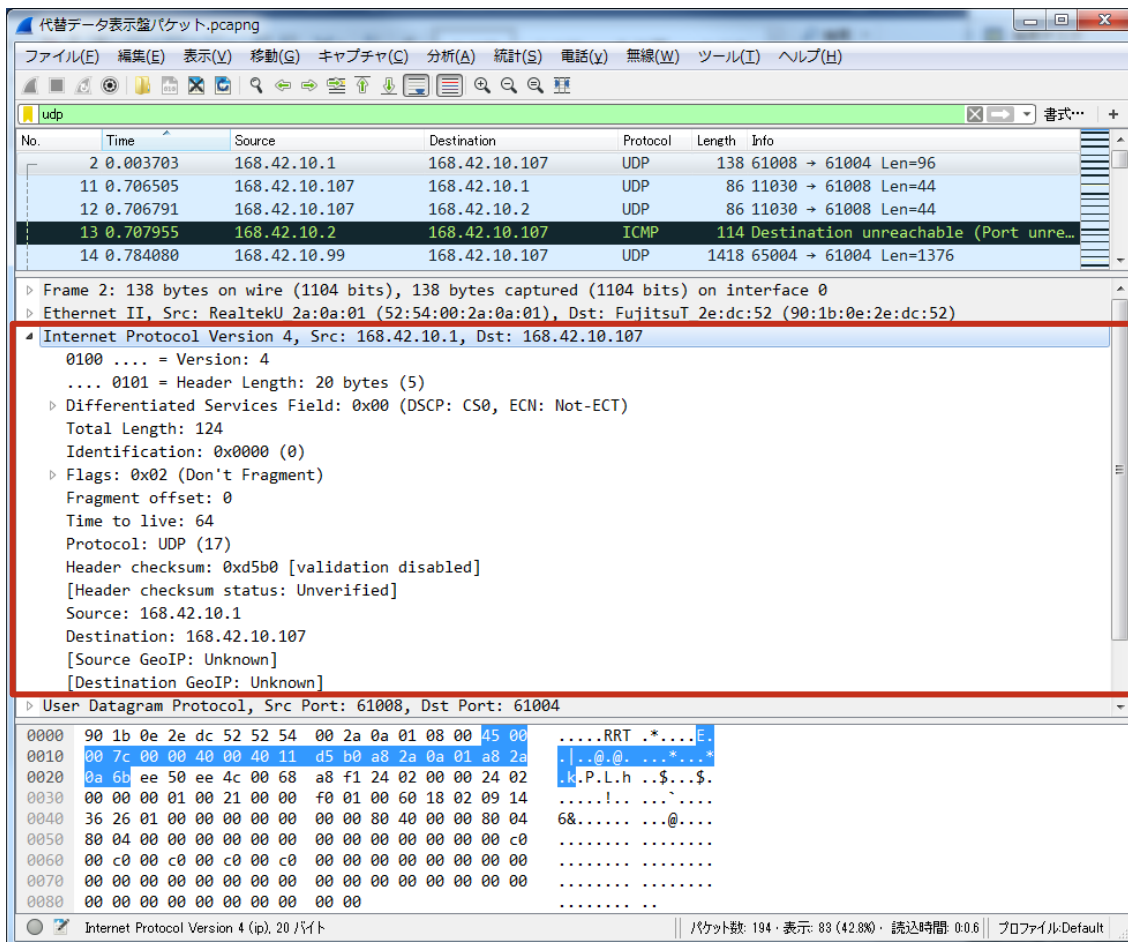
イーサネットヘッダ確認

二番目のパネルの Ethernet II という行を選択してください。三番目のパネルで 1 部分が反転すると思います。黄色で囲まれたところには、送信されたデータ全体が表示されています。その中で、青く反転したところがイーサネットヘッダです。16 進数の 2 文字、1byte ごとに区切られて表示されています。



IP ヘッダの確認

二番目のパネルの Internet Protocol ~ を展開してください。IP ヘッダの内容が可視化されています。



UDP ヘッダの確認

通信にどのポートが使用されたかを確認します。

The screenshot shows the Wireshark interface with a packet capture file named '代替データ表示盤/パケット.pcapng'. The main packet list pane shows four packets. The fourth packet, at time 13.0.707955, is an ICMP message (Type 3, Code 3) from 168.42.10.2 to 168.42.10.107, labeled 'Destination unreachable (Port unreach...)'. The packet details pane is expanded to show the 'User Datagram Protocol' section, indicating a source port of 61008 and a destination port of 61004. Below this, the raw data is displayed in hexadecimal and ASCII. The ASCII portion shows the characters 'RRT.*...E.' followed by a line of dots, and then 'k.P.L.h...\$...\$.' followed by another line of dots. The status bar at the bottom indicates 'User Datagram Protocol (udp), 8 バイト' and 'パケット数: 194 · 表示: 83 (42.8%) · 読み込み時間: 0:0.6 | プロファイル: Default'.

No.	Time	Source	Destination	Protocol	Length	Info
2	0.003703	168.42.10.1	168.42.10.107	UDP	138	61008 → 61004 Len=96
11	0.706505	168.42.10.107	168.42.10.1	UDP	86	11030 → 61008 Len=44
12	0.706791	168.42.10.107	168.42.10.2	UDP	86	11030 → 61008 Len=44
13	0.707955	168.42.10.2	168.42.10.107	ICMP	114	Destination unreachable (Port unreach...)

Frame 2: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface 0
Ethernet II, Src: RealtekU_2a:0a:01 (52:54:00:2a:0a:01), Dst: FujitsuT_2e:dc:52 (90:1b:0e:2e:dc:52)
Internet Protocol Version 4, Src: 168.42.10.1, Dst: 168.42.10.107
User Datagram Protocol, Src Port: 61008, Dst Port: 61004
Source Port: 61008
Destination Port: 61004
Length: 104
Checksum: 0xa8f1 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
Data (96 bytes)

```
0000  90 1b 0e 2e dc 52 52 54 00 2a 0a 01 08 00 45 00  ....RRT.*...E.
0010  00 7c 00 00 40 00 40 11 d5 b0 a8 2a 0a 01 a8 2a  ..|.@.@...*...*
0020  0a 6b ee 50 ee 4c 00 68 a8 f1 24 02 00 00 24 02  .k.P.L.h...$...$
0030  00 00 00 01 00 21 00 00 f0 01 00 60 18 02 09 14  .....!.....
0040  36 26 01 00 00 00 00 00 00 00 80 40 00 00 80 04  6&.....@....
0050  80 04 00 00 00 00 00 00 00 00 00 00 00 00 c0  .....
0060  00 c0 00 c0 00 c0 00 c0 00 00 00 00 00 00 00  .....
0070  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  .....

```

User Datagram Protocol (udp), 8 バイト | パケット数: 194 · 表示: 83 (42.8%) · 読み込み時間: 0:0.6 | プロファイル: Default

データの確認

The screenshot shows the Wireshark interface with a packet capture named '代替データ表示盤パケット.pcapng'. The main display area shows a list of packets. Packet 13 is selected, which is an ICMP message of type 114 (Destination unreachable) from 168.42.10.2 to 168.42.10.107. The packet details pane shows the structure of the frame, including Ethernet II, Internet Protocol Version 4, and User Datagram Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII, with the ASCII portion containing the text '.....RRT.*....E.'.

No.	Time	Source	Destination	Protocol	Length	Info
2	0.003703	168.42.10.1	168.42.10.107	UDP	138	61008 → 61004 Len=96
11	0.706505	168.42.10.107	168.42.10.1	UDP	86	11030 → 61008 Len=44
12	0.706791	168.42.10.107	168.42.10.2	UDP	86	11030 → 61008 Len=44
13	0.707955	168.42.10.2	168.42.10.107	ICMP	114	Destination unreachable (Port unreach...)

▶ Frame 2: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface 0
 ▶ Ethernet II, Src: RealtekU_2a:0a:01 (52:54:00:2a:0a:01), Dst: FujitsuT_2e:dc:52 (90:1b:0e:2e:dc:52)
 ▶ Internet Protocol Version 4, Src: 168.42.10.1, Dst: 168.42.10.107
 ▶ User Datagram Protocol, Src Port: 61008, Dst Port: 61004
 ▶ Data (96 bytes)

```

0000  90 1b 0e 2e dc 52 52 54 00 2a 0a 01 08 00 45 00  .....RRT.*....E.
0010  00 7c 00 00 40 00 40 11 d5 b0 a8 2a 0a 01 a8 2a  .|. @. . . * . . *
0020  0a 6b ee 50 ee 4c 00 68 a8 f1 24 02 00 00 24 02  .k.P.L.h ..$...$.
0030  00 00 00 01 00 21 00 00 f0 01 00 60 18 02 09 14  .....!.....
0040  36 26 01 00 00 00 00 00 00 00 80 40 00 00 80 04  6&..... @.....
0050  80 04 00 00 00 00 00 00 00 00 00 00 00 00 00 c0  .....
0060  00 c0 00 c0 00 c0 00 c0 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  .....
  
```

Data (data), 96 バイト | パケット数: 194 · 表示: 83 (42.8%) · 読み込み時間: 0:0.6 | プロファイル: Default