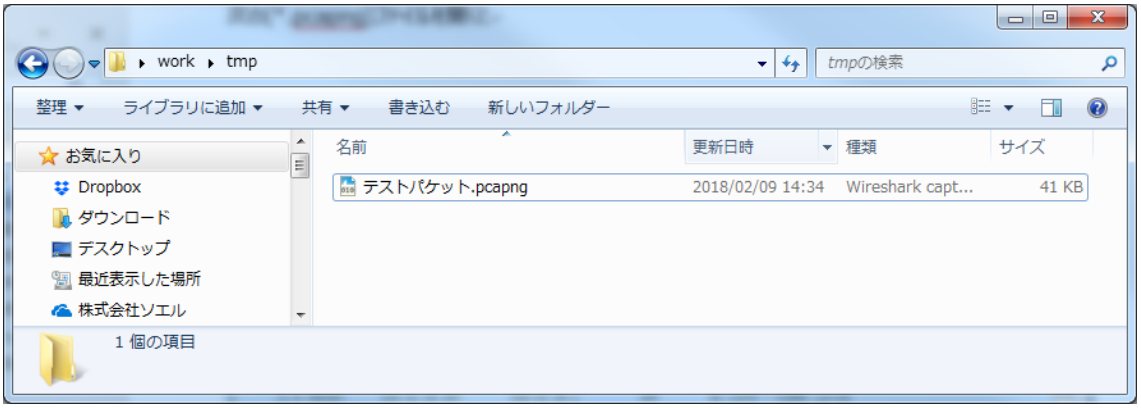
Wireshark の使い方

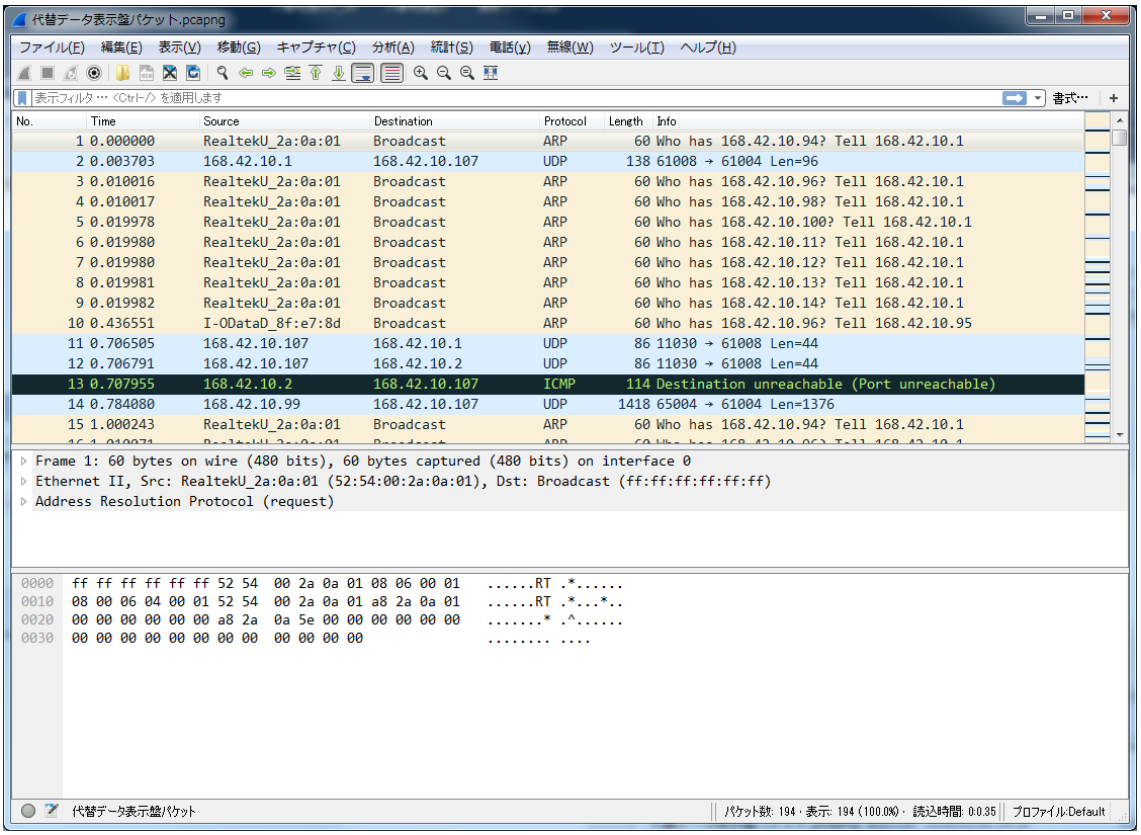
作成日: 2018/03/12
作成者: 小木曽

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。

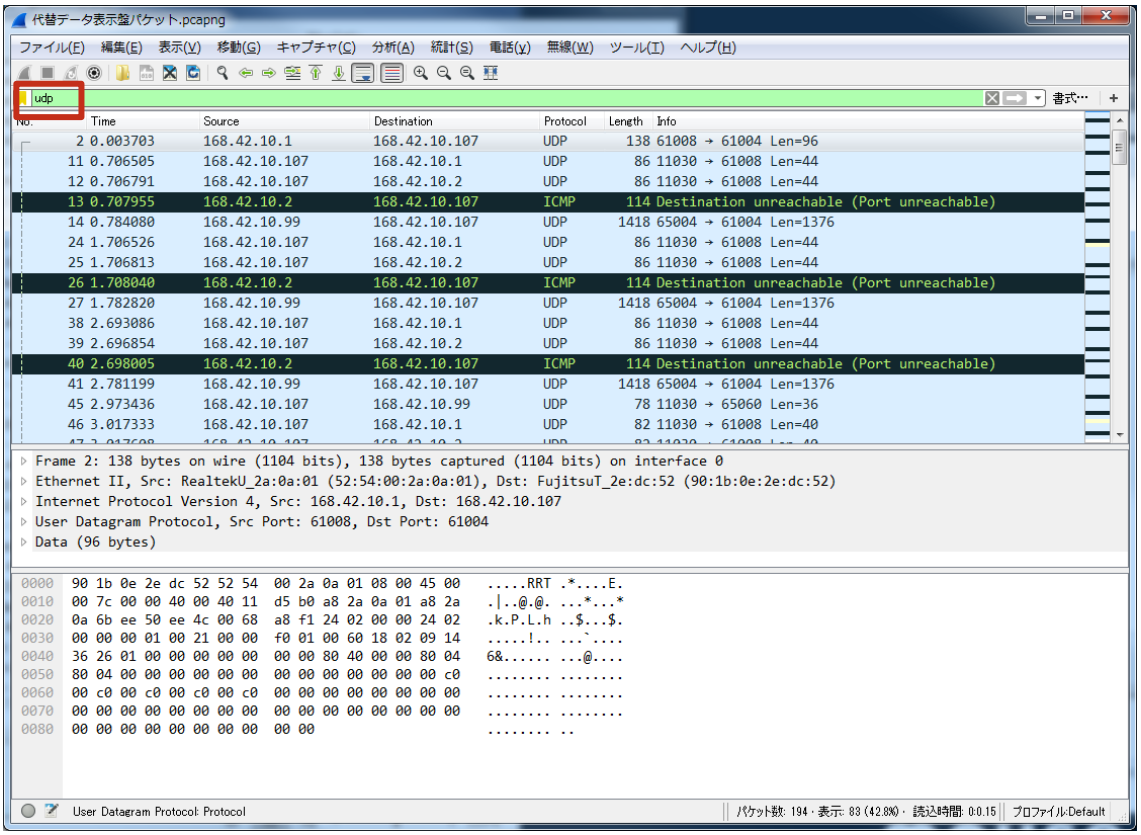


sowel 株式会社ソエル

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

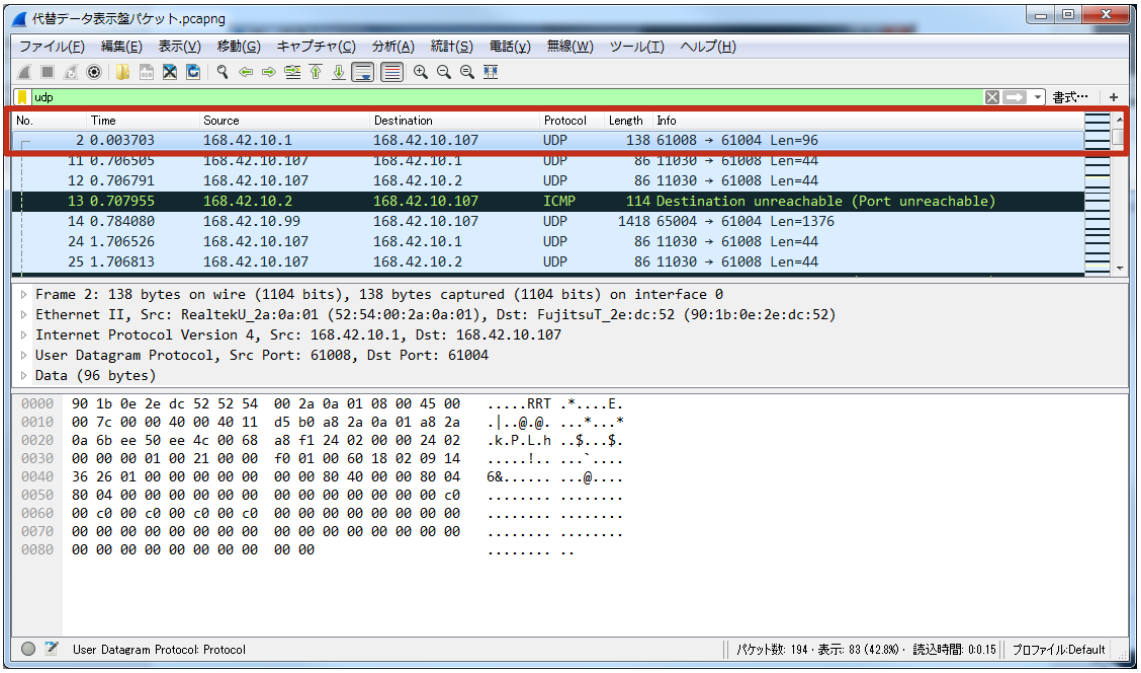
Source は、送信元の IP アドレス

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。



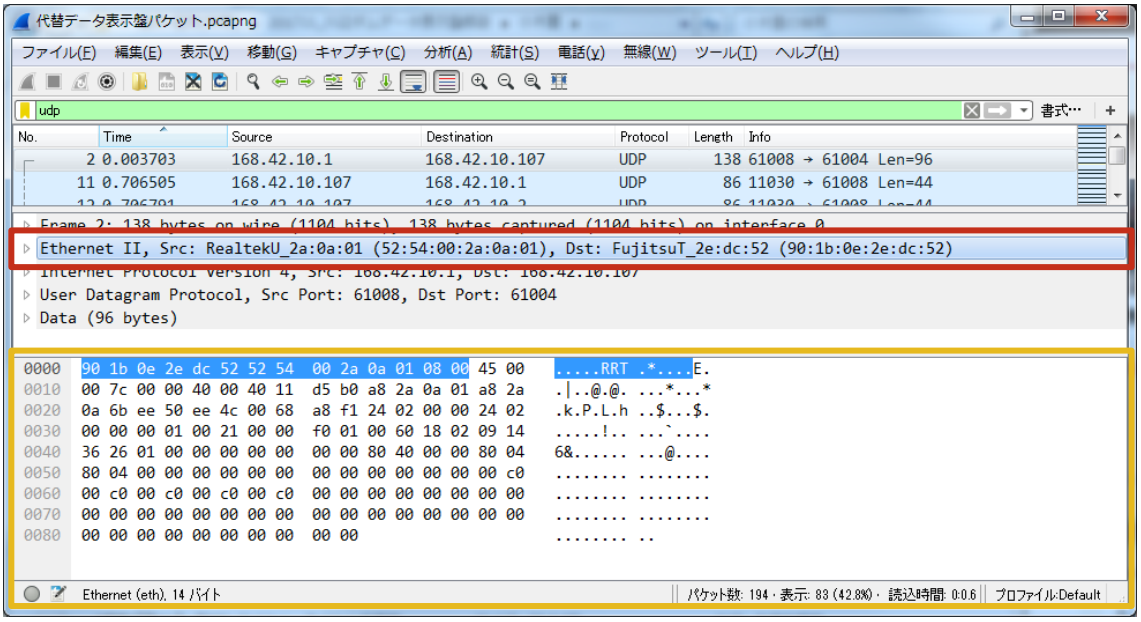
このログファイルの記録は、ローカル IP アドレス 168.42.10.107 で行われています。No.2 は 168.42.10.1 から、UDP のデータが送信されてきました。

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	SYNC	宛先MACアドレス 6バイト	宛先元MACアドレス 6バイト	タイプ	*	全データ長	識別子	*	生存時間	チェックサム	送信元IPアドレス 4バイト	宛先IPアドレス 4バイト	送信元ポート	宛先ポート	UDPデータ長	チェックサム	データ	チェックコード
					*				11H									

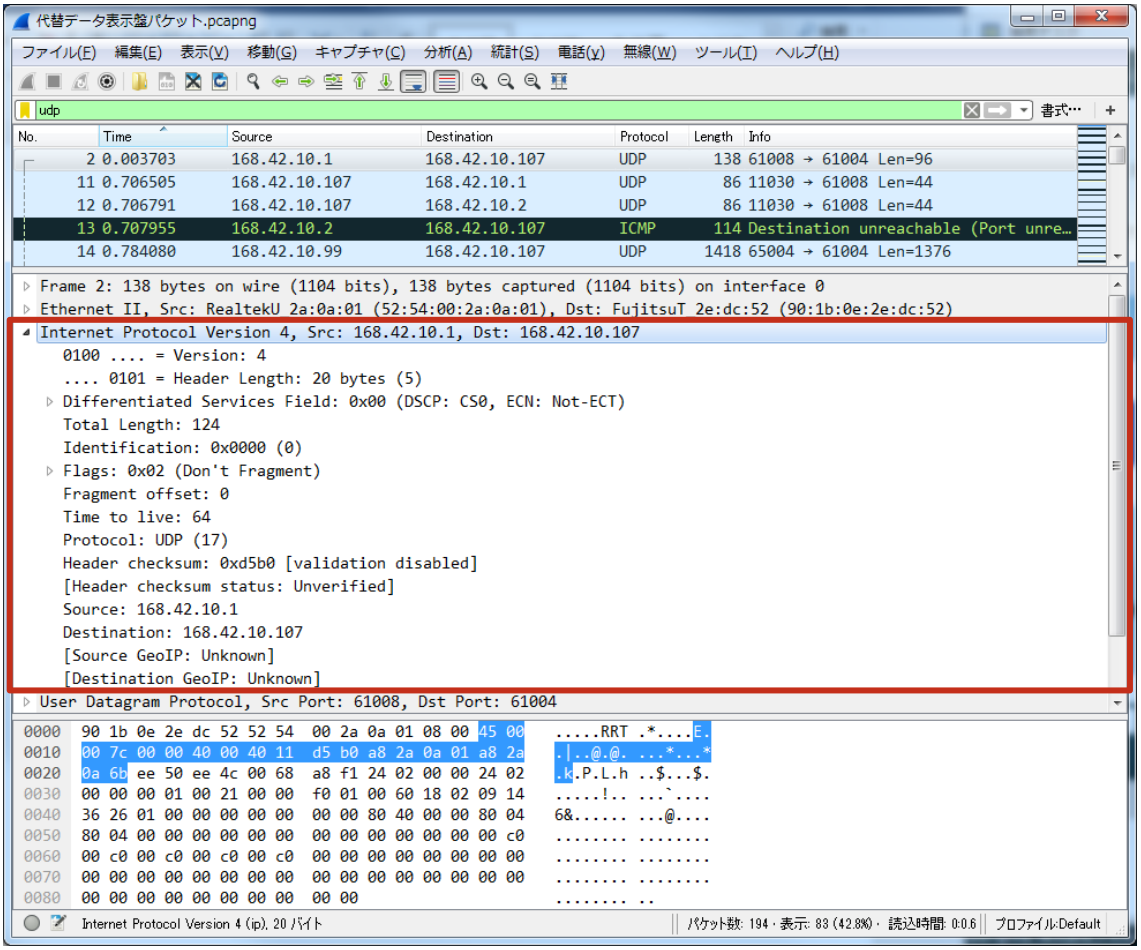
イーサネットヘッダ確認

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。



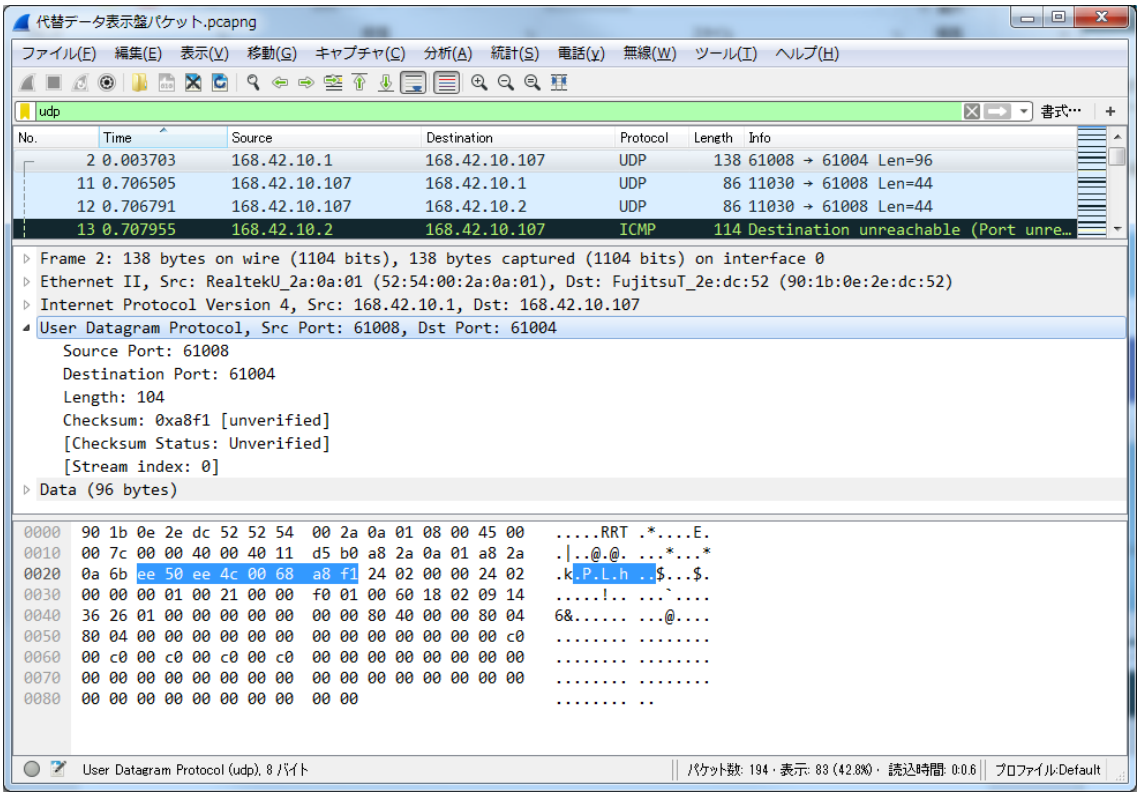
IP ヘッダの確認

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。



データの確認