2019.5 第 1 版

パケットモニター(Wireshark)の使い方

1. Wireshark とは

ネットワーク上（LAN ケーブルに流れている）のパケットを取得して、その中の情報を画面に表示するソフトウェア（LAN アナライザーまたはパケットモニター）の１つに Wireshark がある。Wireshark は、非常に高機能なオープンソース（ソースコードが公開されている）の LAN アナライザで、誰でも自由にコンピュータにインストールして利用することができる。（公式サイト http://www.wireshark.org）

＜主な利用目的＞

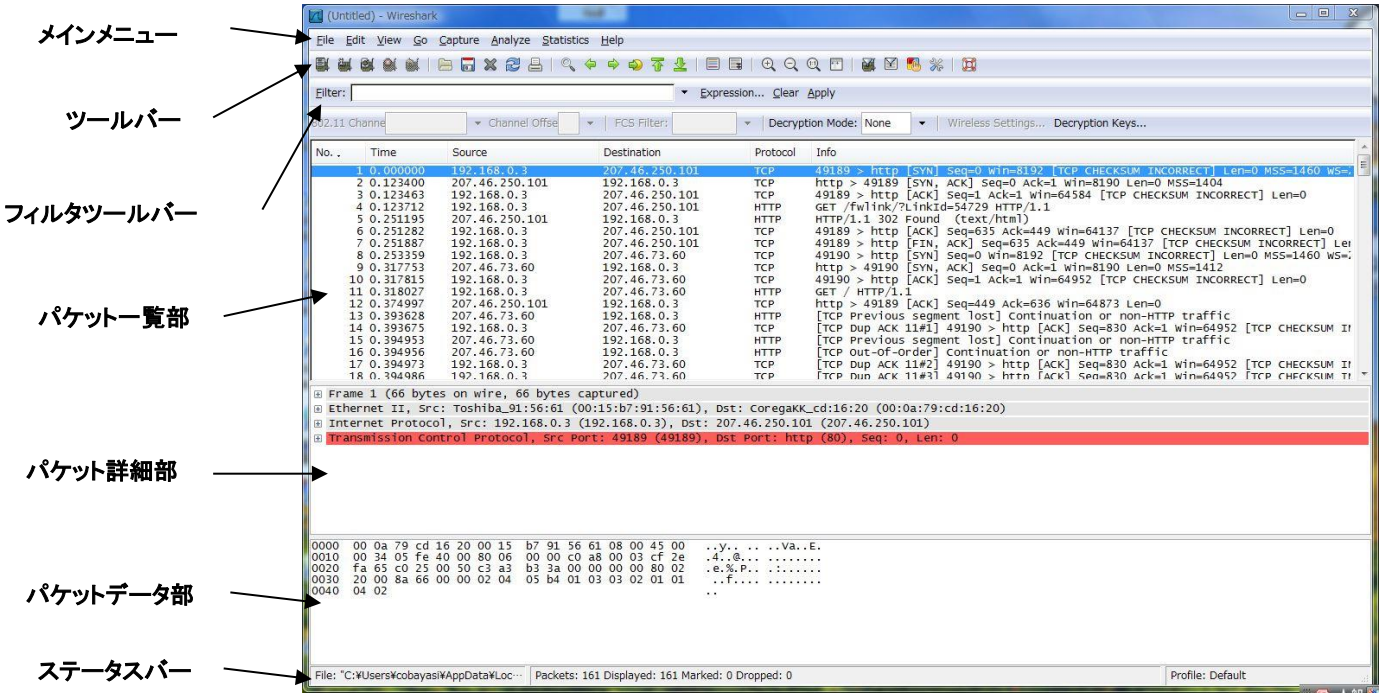
- ネットワーク管理者がネットワークのトラブルを解決するため
- セキュリティ技術者がセキュリティの問題を解決するため
- 開発技術者がプロトコルの実装についてデバッグ（誤り確認）するため
- ネットワークプロトコルの内部について学習するため

＜主な機能＞

- ネットワークインタフェースから送出されるパケットをキャプチャ（取得する）する
- パケットの内容を詳細表示する
- パケットキャプチャしたデータを開いたり保存したりできる
- 他の LAN アナライザが取得したキャプチャデータを変換して読み込み、書き出しができる
- さまざまな条件でパケットを絞り込んで検索できる
- 特定のパケットのみ色づけできる
- さまざまな統計情報を作成できる

2. ユーザインタフェース

Wireshark は、パケットをキャプチャするための様々なメニューやツールバーで構成されている。また、右クリックで呼び出したサブメニューで、オプションなどを指定することができる。ここでは、キャプチャしたパケットを解析するために必要な Wireshark の画面構成などについて述べる。



＜画面構成と各部の名称＞

[メインメニュー]

Wireshark の様々な機能を呼び出すために使用され、以下の項目がある。

メインメニューの項目と主機能

項 目 名	主 な 機 能
File	ファイルの開閉・保存・結合・印刷など
Edit	パケット検索・強調表示
View	ツールバーや画面表示、パケットの色分け
Go	特定パケットの表示
Capture	キャプチャの開始・終了、キャプチャフィルタ(キャプチャ時の絞り込み)の編集
Analyze	表示フィルタ(絞り込み表示)の作成・編集、パケット解析
Statistics	パケット数の一覧やプロトコル分布などの統計情報の表示
Help	ヘルプ機能

[ツールバー]

よく使う機能をボタン化してある

[フィルタツールバー]

パケットを絞り込む(フィルタ機能)ときに使用する

[パケット一覧部]

キャプチャしたパケットを一覧にして表示する。1つのパケットを1行で表示し、簡単な説明(info)がつけられる。ここでクリックして選択した1つのパケットの詳細な内容が、[パケット詳細部]に表示される。

パケット一覧部・表示内容

項 目 名	内 容
No.	キャプチャした順番を示す番号
Time	キャプチャした時刻
Source	送信元アドレス
Destination	宛先アドレス
Protocol	プロトコルの名称
info	パケットの概要

[パケット詳細部]

[パケット一覧部]で選択したパケットの詳細内容(解析内容)を表示する。また、ヘッダやレイヤに付けられている⊞印をクリックすると、詳細な解析内容が表示される。

[パケットデータ部]

[パケット一覧部]で選択したパケットの内容を、16 進数や ASCII コードなどで表示する。より細かく解析する時に利用する。

[ステータスバー]

現在のプログラムの状態やパケットキャプチャに関する情報が表示される。通常、左側には現在の Wireshark の状態及びキャプチャファイルや選択したフィールドの内容が、右側には現在選択しているパケットの番号が表示されている。

3. キャプチャ操作とパケット表示

ここでは、web サーバー(PC1)からサンプルホームページをダウンロードするときにやり取りされるパケットを例に取って、キャプチャの操作手順とパケットの表示と確認方法を説明する。

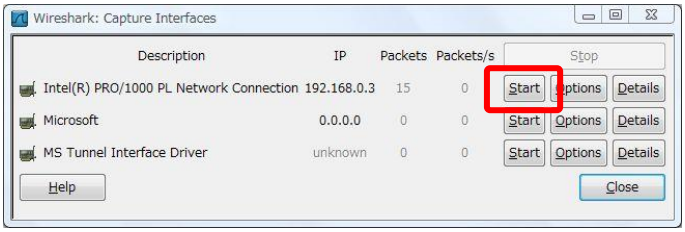
＜キャプチャ操作手順＞

① デスクトップの下に示すアイコンをダブルクリックして Wireshark を起動する。

Wireshark のアイコン

② ツールバーの[interfaces]ボタン（一番左にあるボタン）を押して、キャプチャインタフェース画面を表示させる。

③ 使用している通信アダプタ(LAN カード)を選択して[Start]ボタンを押す。この時点でキャプチャが開始されるので、何らかのパケットが表示される



キャプチャ画面

④ ブラウザを起動させ、web サーバー(PC1)のアドレスを指定して、ホームページを表示させる。ホームページのダウンロードが終了したら、ツールバーの[Stop]ボタン（左から4番目のボタン）を押す。

＜パケットの表示＞

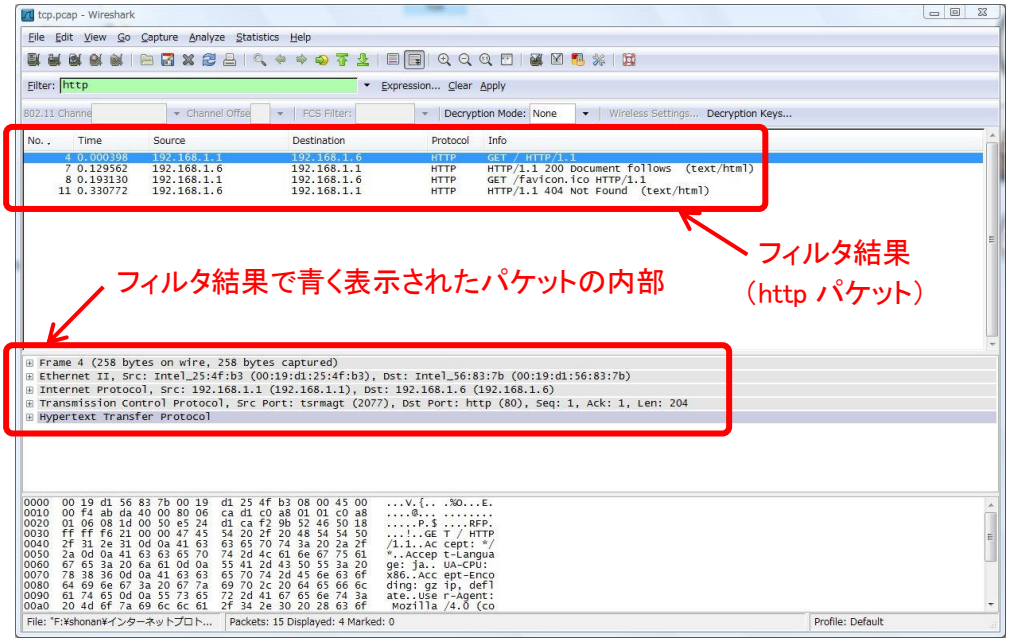
キャプチャ終了直後は、目的以外のパケットが表示されているので、表示フィルタを使って絞り込みを行う。今回は、http プロトコルのみを表示するために、以下の通りにフィルタツールバーのボックスに http を入力する。

フィルタ入力画面

http を入力し終わるとボックスが緑色に変わるので、Enter キーを押すとパケット一覧部に、以下のように http プロトコルのみが表示される。

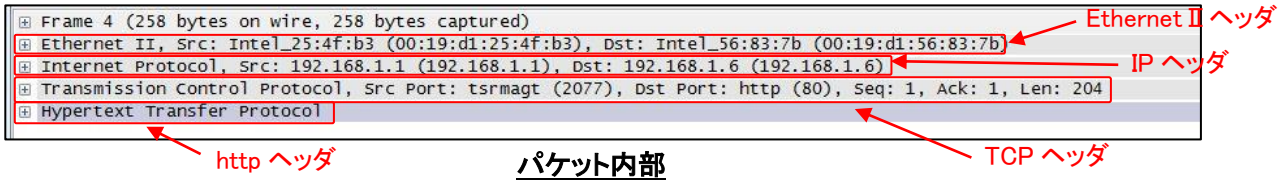
＜パケット（各ヘッダ）の確認＞

ここでは、表示されたパケットヘッダの構成を確認する方法について、1つのパケットを例に挙げて説明する。



フィルタ結果表示

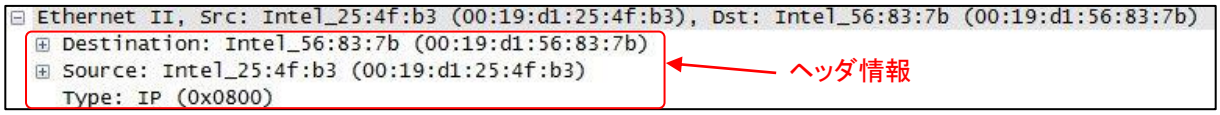
表示されているパケットで[info]の列で GET /http/1.1 と表示されているパケットを選び、パケット詳細部の表示内容を確認する。



パケット内部

上図（パケット内部）の[Ethernet Ⅱ][Internet Protocol][Transmission Control Protocol][Hypertext Transfer Protocol]は、パケットの**ヘッダ**と呼ぶ部分で複数の要素から構成されており、重要な役割を果たしている。また、最上部の[Frame]は、フレーム情報（プロトコルの構成やサイズなど）を表している。

＊Ethernet Ⅱ ヘッダ（※行頭のプラス印＋をクリックするとヘッダ情報が表示する）

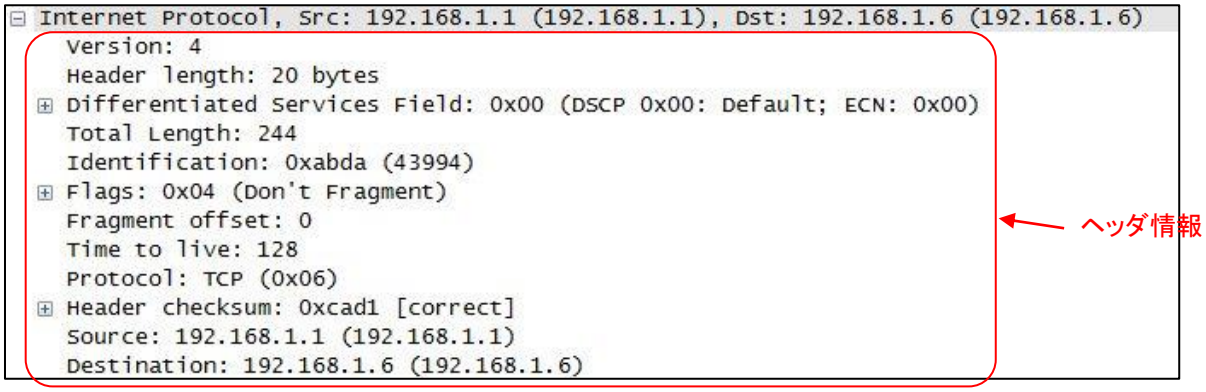


Ethernet Ⅱ ヘッダ情報

Ethernet Ⅱ ヘッダの主要素と内容

Destination	宛先 LAN カードの MAC アドレス
Source	送信元 LAN カードの MAC アドレス
Type	上位プロトコルタイプ（ヘッダ形式）

＊IP ヘッダ（※行頭のプラス印＋をクリックするとヘッダ情報が表示する）

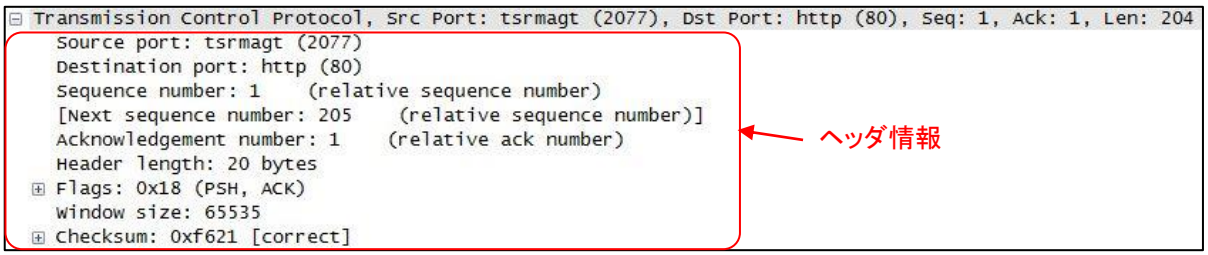


IP ヘッダ情報

IP ヘッダの主要素と内容

Vertion	バージョン（通常は 4）
Header length	ヘッダサイズ（通常は 20 バイト）
Differentiated Service Field	パケット優先度（プロトコル優先度）
Total Length	IP パケットサイズ（単位：バイト）
Identification	パケット識別情報
Flags	パケット分割識別子
Fragment offset	パケット分割位置
Time to live	パケットの寿命
Protocol	上位プロトコルタイプ
Header checksum	パケット破損確認情報
Source	送信元 IP アドレス
Destination	宛先 IP アドレス

＊TCP ヘッダ（※行頭のプラス印＋をクリックするとヘッダ情報が表示する）

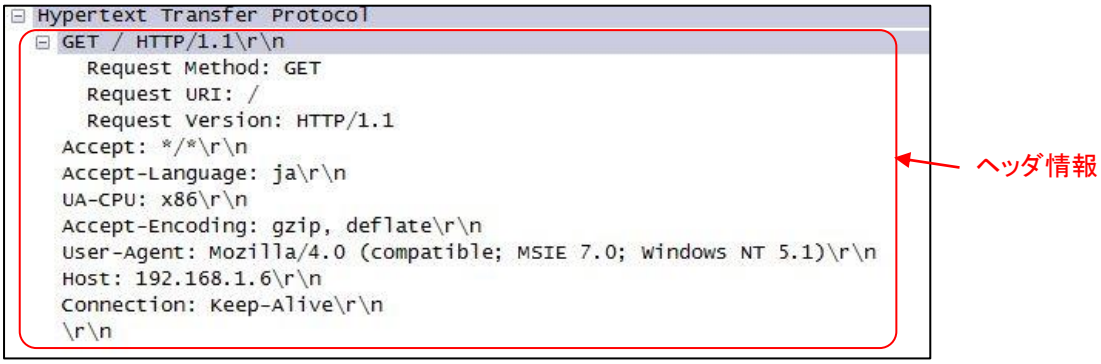


TCP ヘッダ情報

TCP ヘッダの主要素と内容

Source port	送信元ポート番号
Destination port	宛先ポート番号
Sequence number	順序番号（パケットの順番）
Acknowledgement number	応答確認番号（受け取ったパケットの順番）
Header length	ヘッダサイズ（通常 20 バイト）
Flages	TCP 通信制御のための識別子
Windows size	受信バッファサイズ（単位：バイト）
Checksum	パケット破損確認情報

＊http ヘッダ（※行頭のプラス印＋をクリックするとヘッダ情報が表示する）



httpヘッダ情報

TCP ヘッダの主要素と内容

GET	要求メソッド（Web ページ取得）
Accept	Web ブラウザの書式
Accept-Language	Web ブラウザの利用言語
UA-CPU	使用 CPU（コード形式）
Accept-Encoding	Web ブラウザのデータ形式
User-Agent	Web ブラウザの種類やバージョン
Host	Web サーバーの情報（IP アドレス）
Connection	Web サーバーの接続情報