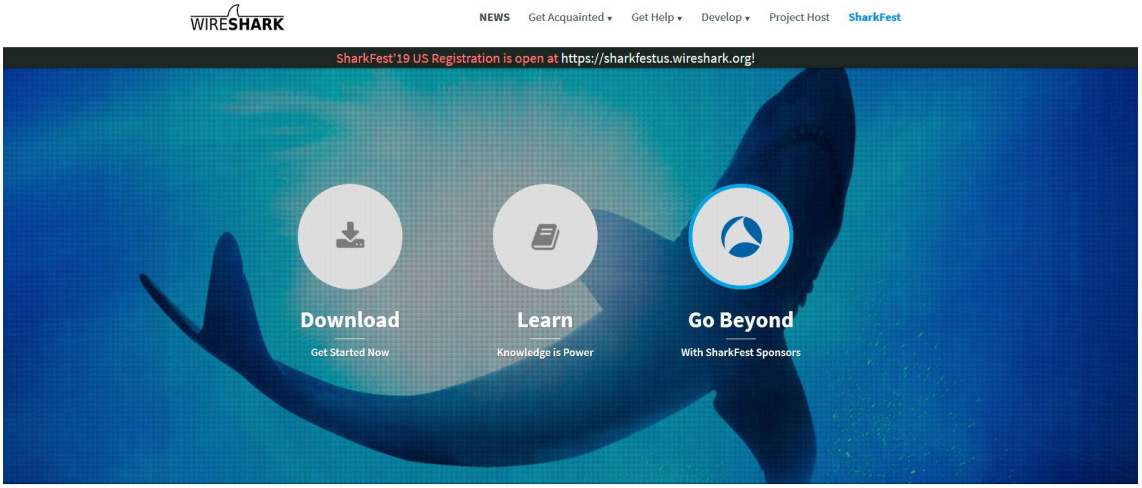
■#10_WireShark インストール

1. WireShark とは

Wireshark（ワイヤシャーク）は、ネットワーク・アナライザ・ソフトウェアで、IP、DHCP など 800 以上のプロトコルを解析できる機能があり、Windows、Linux、BSD、macOS 他幅広い環境で利用できます。



https://www.wireshark.org/

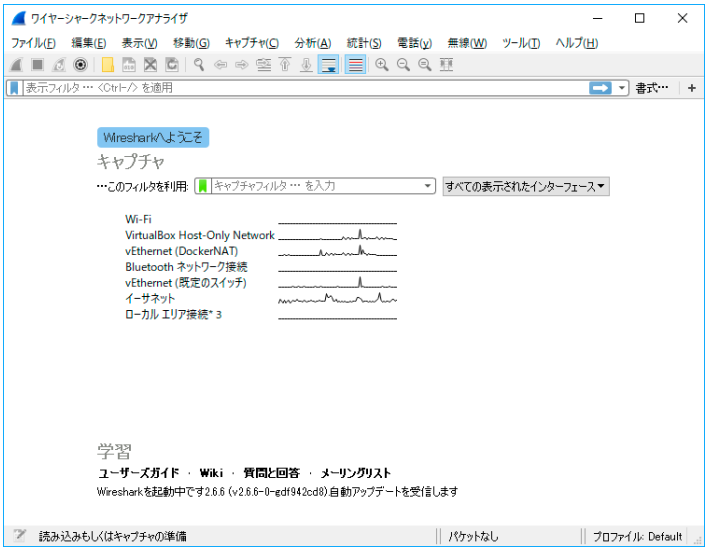
2. インストール

上記ページの “download” をクリックし。Windows64bit 版のインストーラーをダウンロードし実行します。
インストールは基本、オプションを触らず、そのまま “next” でインストール完了します。

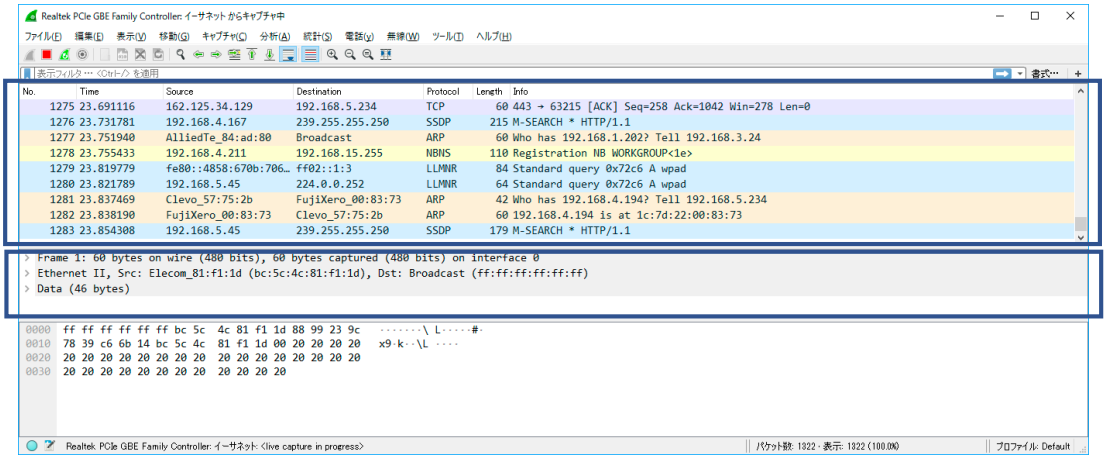
ダウンロードサイト：https://www.wireshark.org/#download

3. 動作確認

インストールが完了したら。起動してみましょう。起動すると下記のような画面が出るはずです。
一覧に表示されるインターフェイスは、利用環境によって異なります。この場合有線のイーサネットで接続しているため、イーサネットの部分をダブルクリックします。皆さんは Wi-fi でしょうか。



そうすると下記のような画面になるはずです。



次々と文字が出てきますね、これがキャプチャされた内容になります。この中には、目的外の情報も含まれているため、任意にフィルタリングしながら、目的のデータを探ることになります。

4. キャプチャできる内容。

LAN アナライザにはいくつか種類があります。主に下記の 3 種類になります。

区分	特徴	
ハードウェア LAN アナライザ	長所	物理的に接続し計測するため、ケーブル品質のチェックや、エラーフレームの測定が可能
	短所	統計やレポートの出力形式やパケット分析に対しての柔軟性が低い
商用ソフトウェア LAN アナライザ	長所	全体的な使い勝手、機能が優れている場合が多い
	短所	NIC ドライバでキャプチャする必要性があり、それよりも会のレイヤのトラブルシュートが困難である。また一般的に高価であり個人での運用は難しい
OSS ソフトウェア LAN アナライザ	長所	ソフトウェアの改変や機能アップが多く、一部の機能では商用をしのぐものもある。 また OSS であるため無償で利用可能
	短所	インターフェイスが独特であったり、UI の改変に一貫性が無い場合がある。 機能的には商用 LAN アナライザ同様の短所あり。

WireShark は OSS(Open Source Software)で、GPL ライセンスで公開されています。