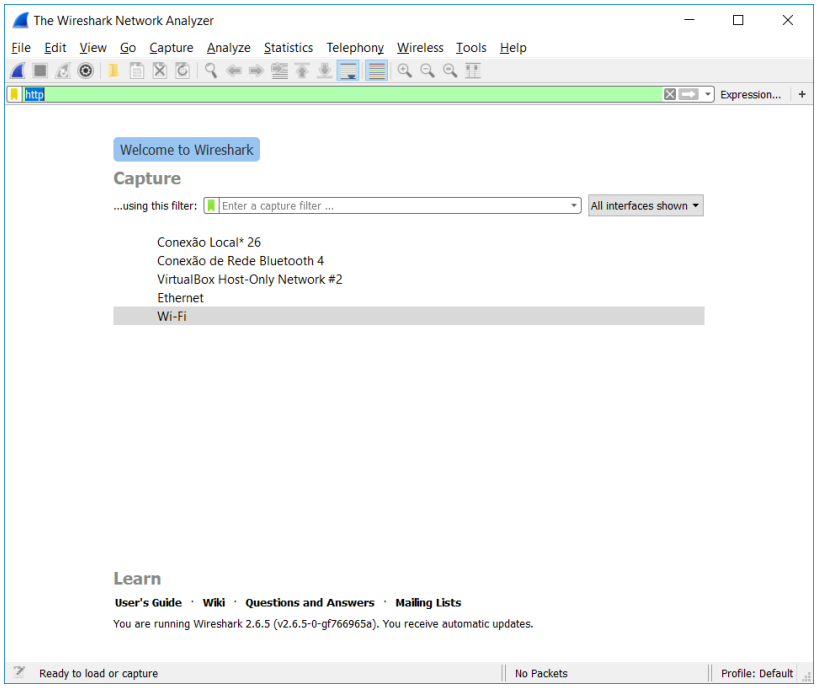
# TP Wireshark

Pour mieux comprendre les protocoles réseau, vous allez « voir les protocoles en action » et en « jouer avec les protocoles ». En d'autres termes, vous observerez la séquence des échanges de messages entre deux entités de protocole, les détails du fonctionnement du protocole, et ferez des protocoles pour effectuer certaines actions, puis observerez ces actions et leurs conséquences. Cela peut être fait dans des scénarios simulés ou dans un environnement réseau « réel » tel qu'Internet. Dans cette Wireshark TP, nous allons prendre cette dernière approche. Vous exécuterez diverses applications réseau dans différents scénarios à l'aide d'un ordinateur sur votre bureau, à la maison ou dans un laboratoire. Vous observerez les protocoles réseau de votre ordinateur « en action », interagissant et échangeant des messages avec des entités de protocole s'exécutant ailleurs sur Internet.

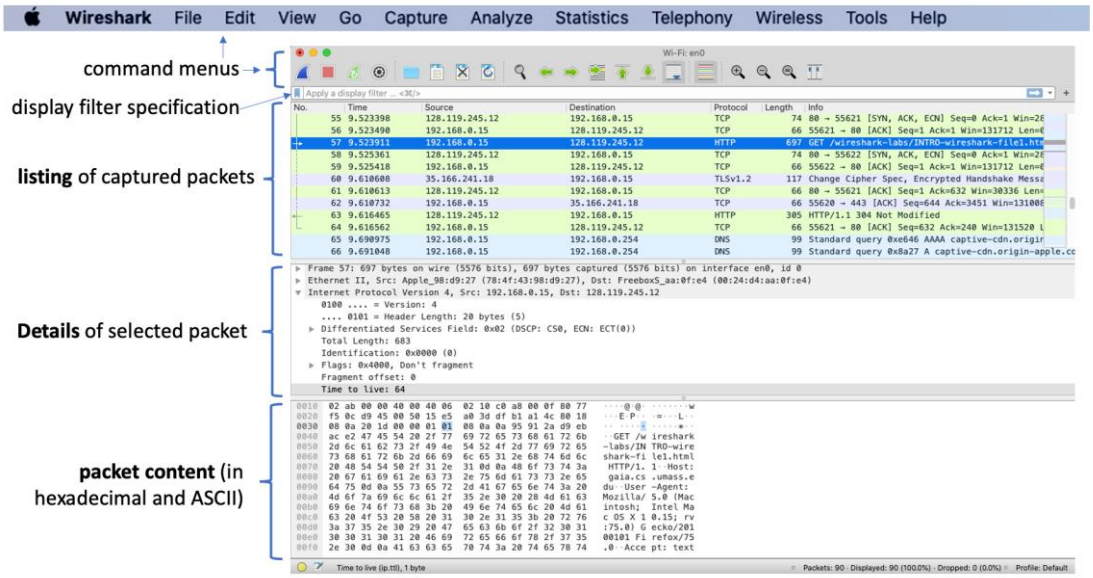
L'outil de base pour observer les messages échangés entre les entités de protocole en cours d'exécution est appelé un **renifleur de paquets**. Comme son nom l'indique, un renifleur de paquets copie passivement (« renifle ») les messages envoyés et reçus par votre ordinateur ; il affichera également le contenu des différents champs de protocole de ces messages capturés. Pour cette TP, vous utiliserez le renifleur de paquets Wireshark. Wireshark est un renifleur de paquets gratuit / shareware qui fonctionne sur les ordinateurs Windows, Linux / Unix et Mac. Les exercices Wireshark ci-dessous vous permettront d'explorer de nombreux protocoles Internet les plus importants.

**Pour commencer votre TP, vous devez télécharger et installer Wireshark. Vous pouvez le télécharger à [https://www.wireshark.org/#download](https://www.wireshark.org/#download).**

Lorsque vous exécutez le programme Wireshark, vous obtenez un écran de démarrage qui ressemble à l'écran ci-dessous. Dans cet écran, vous pouvez sélectionner l'interface que vous souhaitez surveiller (renifler).



Sélectionnez l'interface souhaitée (Ethernet, Wi-Fi, Bluetooth...) que vous allez utiliser, et vous aurez une interface comme celle que vous voyez dans l'image suivante (cette figure a été prise à partir d'une ancienne version de Wireshark). Cette image vous montre les principaux champs de Wireshark.



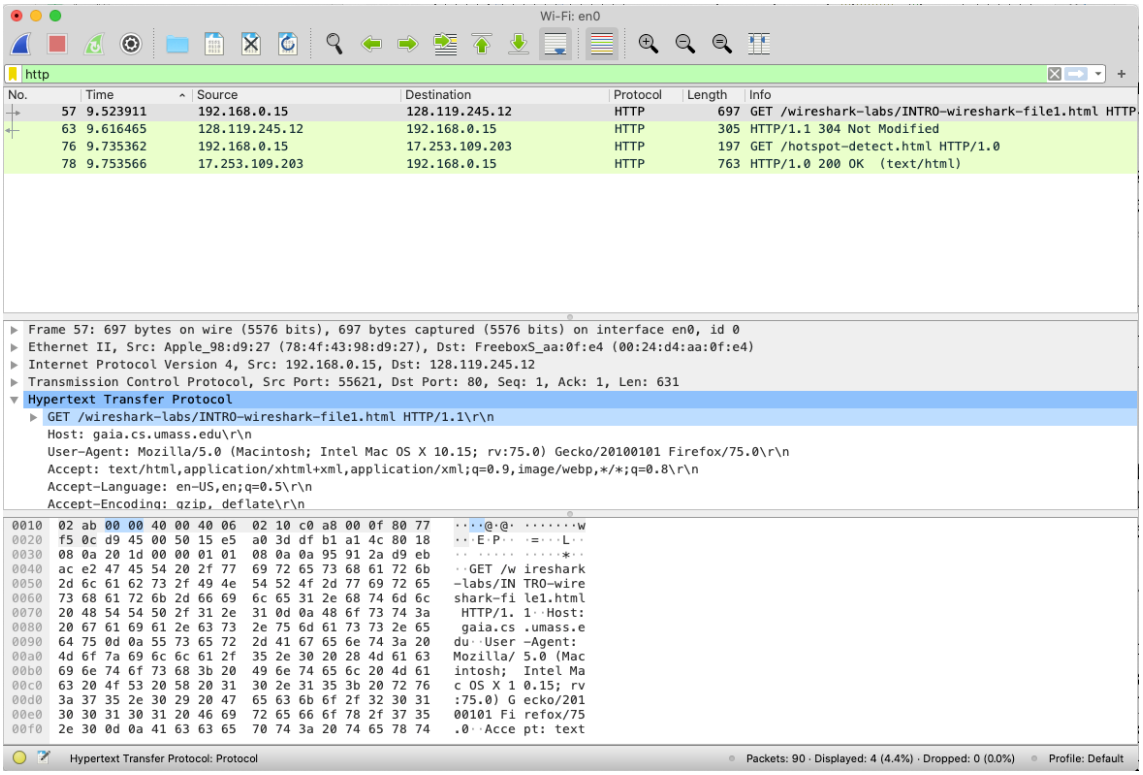

# Série de tests

La meilleure façon d'en apprendre davantage sur tout nouveau logiciel est de l'essayer ! Nous supposerons que votre ordinateur est connecté à Internet via une interface Ethernet filaire. En effet, je vous recommande de faire ce premier laboratoire sur un ordinateur doté d'une connexion Ethernet filaire, plutôt que d'une simple connexion sans fil. Procédez comme suit :

1. Démarrez un navigateur Web, qui affichera la page d'accueil sélectionnée.
2. Démarrez le logiciel Wireshark et sélectionnez l'interface que vous allez utiliser.
3. Une fois que vous commencez la capture de paquets, une fenêtre comme celle montrée ci-dessus apparaîtra et Wireshark commencera à capturer des paquets.
4. Pendant que Wireshark est en cours d'exécution, accédez à l'URL : http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html et affichez cette page dans votre navigateur.
5. Une fois que votre navigateur a affiché la page intro-wireshark-file1.html (il s'agit d'une simple ligne de félicitations), arrêtez la capture de paquets Wireshark en sélectionnant stop dans la fenêtre de capture Wireshark.
6. Tapez « http » (sans les guillemets, et en minuscules - tous les noms de protocole sont en minuscules dans Wireshark) dans la fenêtre de spécification du filtre d'affichage en haut de la fenêtre principale de Wireshark.
7. Recherchez le message HTTP GET qui a été envoyé de votre ordinateur au serveur HTTP gaia.cs.umass.edu. (Recherchez un message HTTP GET dans la partie « liste des paquets capturés » de la fenêtre Wireshark qui affiche « GET » suivi de l'URL gaia.cs.umass.edu que vous avez entrée. Lorsque vous sélectionnez le message HTTP GET, les informations de trame Ethernet, de datagramme IP, de segment TCP et d'en-tête de message HTTP

s'affichent dans la fenêtre d'en-tête de paquet2. En cliquant sur '+' et '-' pointant vers la droite et les pointes de flèche pointant vers le bas vers le côté gauche de la fenêtre de détails des paquets, minimisez la quantité d'informations Frame, Ethernet, Internet Protocol et Transmission Control Protocol affichées. Maximisez la quantité d'informations affichées sur le protocole HTTP. Votre écran Wireshark devrait maintenant ressembler à peu près comme indiqué ci-dessous. (Notez la quantité réduite d'informations de protocole pour tous les protocoles à l'exception de HTTP, et la quantité maximale d'informations de protocole pour HTTP dans la fenêtre d'en-tête de paquet).

Vous devriez voir quelque chose comme l'image ci-dessous :




8. **Vous êtes maintenant prêt à démarrer votre TP.**

# Exercices

Vous devez effectuer les exercices suivants sur Wireshark et fournir un rapport avec les réponses. Vous pouvez trouver tous les exercices et fichiers dont vous avez besoin sur le Moodle.