Atelier Wireshark: Commencement

"Dis-moi et j'oublie. Montre-moi et je me souviens. Implique-moi et je comprendrai". proverbe chinois

---

La compréhension des protocoles réseau peut souvent être considérablement approfondie en "voyant les protocoles en action" et en "jouant avec les protocoles" - en observant la séquence de messages échangés entre deux entités de protocole, en approfondissant les détails du fonctionnement du protocole et en faisant en sorte que les protocoles effectuent certaines actions, puis observer ces actions et leurs conséquences. Cela peut être fait dans des scénarios simulés ou dans un environnement réseau "réel" tel qu'Internet. Dans les ateliers Wireshark que vous suivrez dans ce cours, vous exécuterez diverses applications réseau dans différents scénarios à l'aide de votre propre ordinateur. 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. Ainsi, vous et votre ordinateur ferez partie intégrante de ces ateliers. Vous observerez et vous apprendrez en pratiquant.

Dans ce premier atelier Wireshark, vous vous familiariserez avec Wireshark et ferez quelques captures et observations simples de paquets.

L'outil de base pour observer les messages échangés entre les entités de protocole d'exécution est appelé un "sniffeur" de paquets. Comme son nom l'indique, un sniffeur de paquets capture ("sniffe") les messages envoyés/reçus depuis/par votre ordinateur; il stockera et/ou affichera également généralement le contenu des divers champs de protocole dans ces messages capturés. Un sniffeur de paquets lui-même est passif. Il observe les messages envoyés et reçus par les applications et les protocoles exécutés sur votre ordinateur, mais n'envoie jamais de paquets de lui-même. De même, les paquets reçus ne sont jamais explicitement adressés au sniffeur de paquets. Au lieu de cela, un sniffeur de paquets reçoit une copie des paquets qui sont envoyés/reçus depuis/par l'application et les protocoles s'exécutant sur votre machine.

La Figure 1 montre la structure d'un sniffeur de paquets. À droite de la Figure 1 figurent les protocoles (dans ce cas, les protocoles Internet) et les applications (telles qu'un navigateur Web ou un client de messagerie) qui s'exécutent normalement sur votre ordinateur. Le sniffeur de paquets, illustré dans le rectangle en pointillés de la Figure 1, est un ajout au logiciel habituel de votre ordinateur et se compose de deux parties. La bibliothèque de capture de paquets qui reçoit une copie de chaque trame de la couche

liaison envoyée ou reçue par votre ordinateur via une interface donnée (couche liaison, telle qu'Ethernet ou WiFi).

Rappelez-vous (voir cours) que les messages échangés par des protocoles de couche supérieure tels que HTTP, FTP, TCP, UDP, DNS ou IP sont tous finalement encapsulés dans des trames de la couche liaison qui sont transmises sur des supports physiques tels qu'un câble Ethernet ou une liaison radio WiFi 802.11. La capture de toutes les trames de la couche liaison vous donne ainsi tous les messages envoyés/reçus via le lien surveillé depuis/par tous les protocoles et applications s'exécutant sur votre ordinateur.

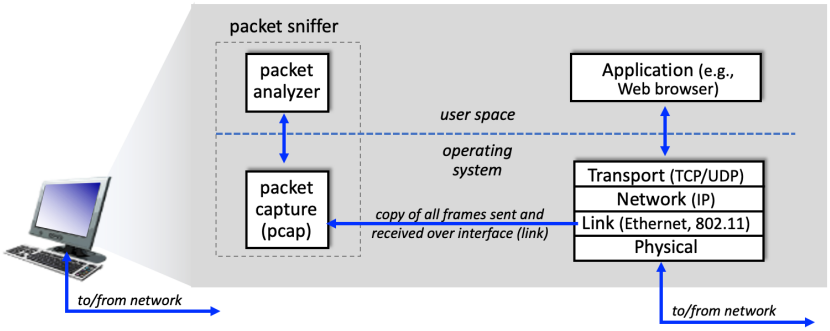

Figure 1: Structure d'un sniffeur de paquet

Le deuxième composant d'un sniffeur de paquets est l'analyseur de paquets, qui affiche le contenu de tous les champs d'un message d'un protocole donné. Pour ce faire, l'analyseur de paquets doit "comprendre" la structure de tous les messages échangés par les protocoles. Par exemple, supposons que nous souhaitions afficher les différents champs des messages échangés par le protocole HTTP sur la Figure 1. L'analyseur de paquets comprend le format des trames Ethernet et peut ainsi identifier le datagramme IP dans une trame Ethernet. Il comprend également le format de datagramme IP, de sorte qu'il peut extraire le segment TCP dans le datagramme IP. Enfin, il comprend la structure du segment TCP, de sorte qu'il peut extraire le message HTTP contenu dans le segment TCP. Enfin, il comprend le protocole HTTP et ainsi, par exemple, sait que les premiers octets d'un message HTTP contiendront la chaîne "GET", "POST" ou "HEAD".
Pour ces ateliers, nous utiliserons le sniffeur de paquets Wireshark [http://www.wireshark.org/], ce qui nous permettra d'afficher le contenu des messages envoyés/reçus depuis/par les protocoles à différents niveaux de la pile de protocoles. (Techniquement parlant, Wireshark est un analyseur de paquets qui utilise une bibliothèque de capture de paquets sur votre ordinateur. De plus, techniquement parlant, Wireshark capture les trames de la couche liaison comme illustré dans la Figure 1, mais utilise le terme générique "paquet" pour désigner les trames de la couche liaison, les datagrammes de la couche réseau, les segments de la couche transport et les messages de la couche application. Nous utiliserons donc ici le terme "paquet" moins précis pour respecter la convention Wireshark). Wireshark est un analyseur de protocole réseau gratuit qui s'exécute sur les ordinateurs Windows, Mac et Linux/Unix. C'est un analyseur de paquets idéal pour nos

ateliers - il est stable, dispose d'une large base d'utilisateurs et d'un support bien documenté qui comprend un guide de l'utilisateur (http://www.wireshark.org/docs/wsug_html_chunked/), des pages de manuel (http://www.wireshark.org/docs/man-pages/), et une FAQ détaillée (http://www.wireshark.org/faq.html), une fonctionnalité riche qui inclut la capacité d'analyser des centaines de protocoles, et une interface utilisateur bien conçue. Il fonctionne sur des ordinateurs utilisant des réseaux locaux sans fil Ethernet, série (PPP), 802.11 (WiFi) et de nombreuses autres technologies de couche liaison.

Obtenir Wireshark

Pour exécuter Wireshark, vous devez avoir accès à un ordinateur prenant en charge à la fois Wireshark et la bibliothèque de capture de paquets libpcap ou WinPCap. Le logiciel libpcap sera installé pour vous, s'il n'est pas installé dans votre système d'exploitation, lorsque vous installez Wireshark. Voir http://www.wireshark.org/download.html pour une liste des systèmes d'exploitation pris en charge et des sites de téléchargement.

Téléchargez et installez le logiciel Wireshark :

- Allez sur http://www.wireshark.org/download.html et téléchargez et installez Wireshark pour votre ordinateur.

La FAQ de Wireshark contient un certain nombre de conseils utiles et d'informations intéressantes, en particulier si vous rencontrez des difficultés pour installer ou exécuter Wireshark.

Exécuter Wireshark

Lorsque vous exécutez le programme Wireshark, vous obtenez un écran de démarrage qui ressemble à l'écran ci-dessous (Figure 2). Différentes versions de Wireshark auront des écrans de démarrage différents - alors ne paniquez pas si le vôtre ne ressemble pas exactement à la Figure 2 ! La documentation de Wireshark indique "*Comme Wireshark s'exécute sur de nombreuses plates-formes différentes avec de nombreux gestionnaires de fenêtres différents, différents styles appliqués et différentes versions de la boîte à outils GUI sous-jacente utilisée, votre écran peut être différent des captures d'écran fournies. Mais comme il n'y a pas de réelles différences de fonctionnalité, ces captures d'écran devraient toujours être bien compréhensibles*". Bien dit.

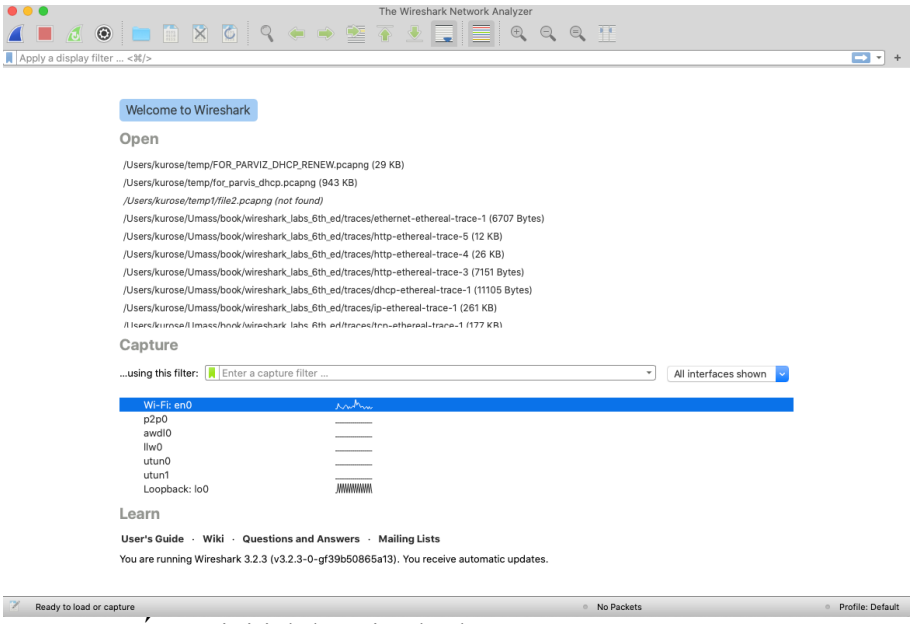

Figure 2: Écran initial de Wireshark

Il n'y a pas grand-chose de très intéressant sur cet écran. Mais notez que sous la section Capture, il y a une liste de soi-disant interfaces. L'ordinateur Mac dont nous prenons ces captures d'écran n'a qu'une seule interface - "Wi-Fi en0" (ombrée en bleu sur la Figure 2) qui est l'interface pour l'accès Wi-Fi. Tous les paquets vers/depuis cet ordinateur passeront par l'interface Wi-Fi, c'est donc ici que nous voudrons capturer les paquets. Sur un Mac, double-cliquez sur cette interface (ou sur un autre ordinateur, localisez l'interface sur la page de démarrage par laquelle vous obtenez une connectivité Internet, par exemple, probablement une interface WiFi ou Ethernet, et sélectionnez cette interface).

Prenons Wireshark pour un tour! Si vous cliquez sur l'une de ces interfaces pour démarrer la capture de paquets (c'est-à-dire pour que Wireshark commence à capturer tous les paquets envoyés vers/depuis cette interface), un écran comme celui sur la Figure 3 s'affichera, affichant des informations sur les paquets capturés. Une fois que vous démarrez la capture de paquets, vous pouvez l'arrêter en utilisant le menu déroulant Capture et en sélectionnant Arrêter (ou en cliquant sur le bouton carré rouge à côté de l'aileron Wireshark).

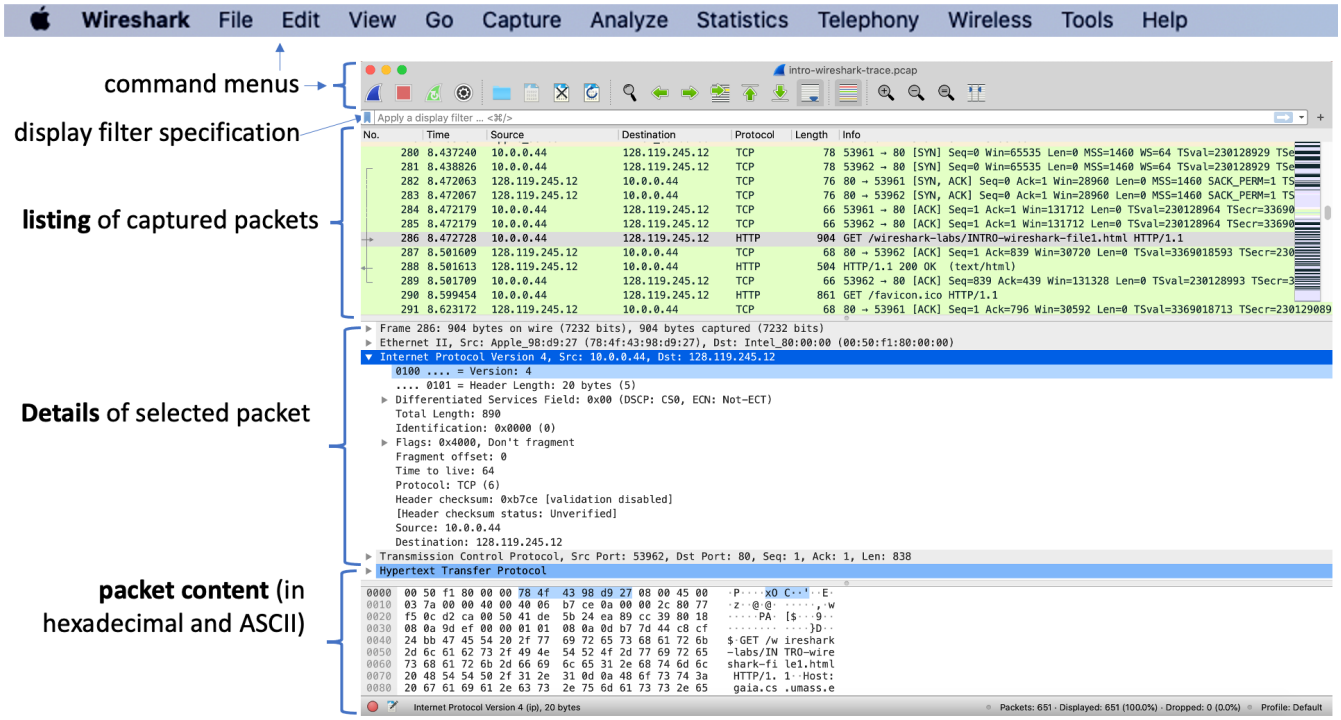

Figure 3: Fenêtre Wireshark, pendant et après la capture

Ceci a l'air plus intéressant ! L'interface Wireshark comporte cinq composants principaux :

- Les **menus de commande** sont des menus déroulants standard situés en haut de la fenêtre Wireshark (et sur un Mac en haut de l'écran également; la capture d'écran de la Figure 3 provient d'un Mac). Les menus Fichier et Capture nous intéressent maintenant. Le menu Fichier vous permet d'enregistrer les données de paquet capturées ou d'ouvrir un fichier contenant des données de paquet précédemment capturées et de quitter l'application Wireshark. Le menu Capture vous permet de commencer la capture de paquets.
- La **fenêtre de listing de paquets** affiche un résumé d'une ligne pour chaque paquet capturé, y compris le numéro de paquet (attribué par Wireshark; notez qu'il ne s'agit pas d'un numéro de paquet contenu dans l'en-tête d'un protocole), l'heure à laquelle le paquet a été capturé, les adresses source et de destination du paquet, le type de protocole et les informations spécifiques au protocole contenues dans le paquet. La liste des paquets peut être triée selon l'une de ces catégories en cliquant sur un nom de colonne. Le champ Type de protocole répertorie le protocole de niveau le plus élevé qui a envoyé ou reçu ce paquet, c'est-à-dire le protocole qui est la source ou le puits ultime pour ce paquet.
- La **fenêtre de détails d'en-tête de paquet** fournit des détails sur le paquet sélectionné (surligné) dans la fenêtre de liste de paquets. (Pour sélectionner un paquet dans la fenêtre de liste de paquets, placez le curseur sur le résumé d'une ligne du paquet dans la fenêtre de liste de paquets et cliquez avec le bouton gauche de la souris.). Ces détails incluent des informations sur la trame Ethernet (en supposant

que le paquet a été envoyé/reçu via une interface Ethernet) et le datagramme IP qui contient ce paquet. La quantité de détails Ethernet et de couche IP affichés peut être agrandie ou réduite en cliquant sur les cases plus/moins ou sur les triangles pointant vers la droite/vers le bas, à gauche de la trame Ethernet ou de la ligne de datagramme IP dans la fenêtre des détails du paquet. Si le paquet a été transporté via TCP ou UDP, les détails TCP ou UDP seront également affichés, qui peuvent également être étendus ou minimisés. Enfin, des détails sur le protocole de plus haut niveau qui a envoyé ou reçu ce paquet sont également fournis.

- La **fenêtre de contenu du paquet** affiche le contenu entier de la trame capturée, à la fois au format ASCII et hexadécimal.
- Vers le haut de l'interface utilisateur graphique de Wireshark, se trouve le **champ de filtre d'affichage de paquets**, dans lequel un nom de protocole ou d'autres informations peuvent être saisis afin de filtrer les informations affichées dans la fenêtre de liste de paquets (et donc l'en-tête de paquet et fenêtres de contenu des paquets). Dans l'exemple ci-dessous (Figure 5), nous utiliserons le champ de filtre d'affichage des paquets pour que Wireshark masque (et n'affiche pas) les paquets, à l'exception de ceux qui correspondent aux messages HTTP.

Tester Wireshark

La meilleure façon de découvrir un nouveau logiciel est de l'essayer ! Nous supposerons que votre ordinateur est connecté à Internet via une interface Ethernet filaire ou une interface Wi-Fi 802.11 sans fil. Procédez comme suit :

1. Démarrez votre navigateur Web préféré, qui affichera la page d'accueil que vous avez sélectionnée.

2. Démarrez le logiciel Wireshark. Vous verrez initialement une fenêtre similaire à celle illustrée à la figure 2. Wireshark n'a pas encore commencé à capturer les paquets.

3. Pour commencer la capture de paquets, sélectionnez le menu déroulant *Capture* et sélectionnez *Interfaces*. Cela entraînera l'affichage de la fenêtre "Wireshark : Capture Interfaces" (sur un PC) ou vous pouvez choisir Options sur un Mac. Vous devriez voir une liste d'interfaces, comme illustré dans les figures 4a (Windows) et 4b (Mac).

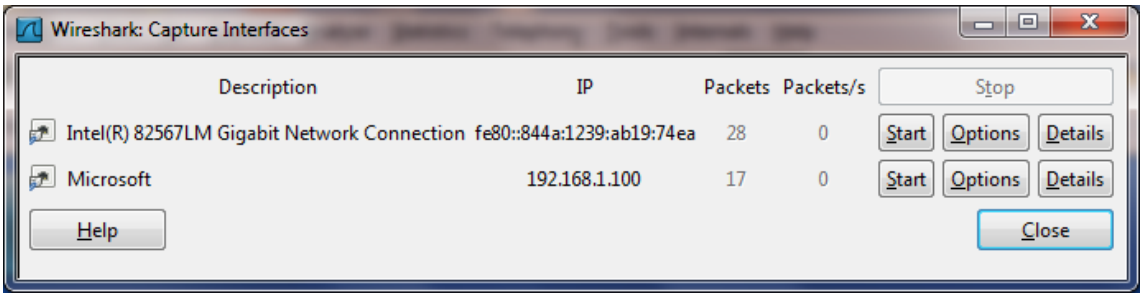

Figure 4a: Fenêtre interface de Capture de Wireshark, sur un ordinateur Windows

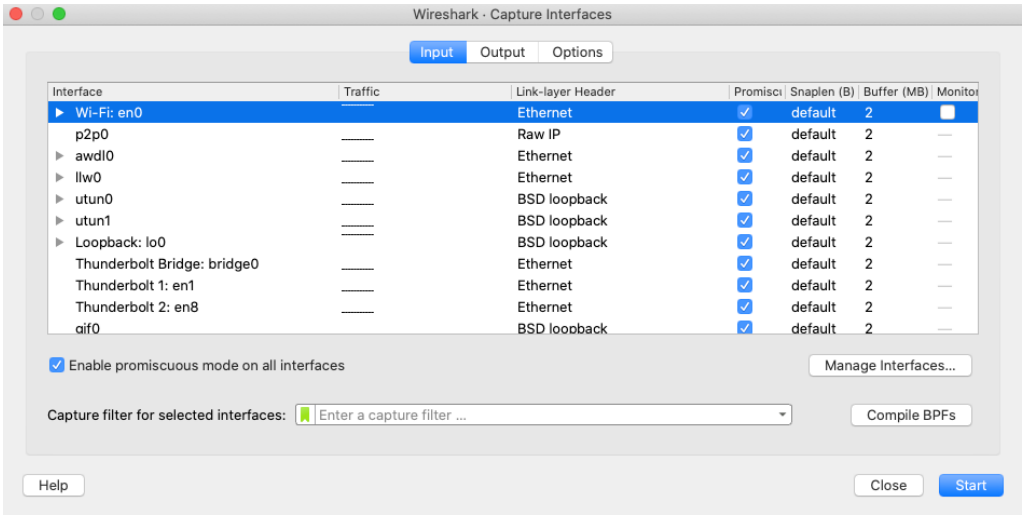

Figure 4b: Fenêtre interface de Capture de Wireshark, sur un Mac

4. Vous verrez une liste des interfaces sur votre ordinateur ainsi qu'un nombre de paquets qui ont été observés sur cette interface jusqu'à présent. Sur une machine Windows, cliquez sur Démarrer pour l'interface sur laquelle vous souhaitez commencer la capture de paquets (dans le cas de la figure 4a, la connexion réseau Gigabit). Sur une machine Windows, sélectionnez l'interface et cliquez sur Démarrer en bas de la fenêtre). La capture de paquets va maintenant commencer - Wireshark capture maintenant tous les paquets envoyés/reçus depuis/par votre ordinateur sur cette interface!

5. Une fois que vous avez commencé la capture de paquets, une fenêtre similaire à celle illustrée à la Figure 3 s'affiche. Cette fenêtre affiche les paquets capturés. En sélectionnant le menu déroulant Capture et en sélectionnant Arrêter, ou en cliquant sur le carré rouge Arrêter, vous pouvez arrêter la capture de paquets. Mais n'arrêtez pas encore la capture de paquets. Commençons par capturer quelques paquets intéressants. Pour ce faire, nous devrons générer du trafic réseau. Faisons-le à l'aide d'un navigateur Web, qui utilisera le protocole HTTP que nous étudierons en détail en classe pour télécharger le contenu d'un site Web.

6. Pendant que Wireshark est en cours d'exécution, saisissez l'URL : http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html et afficher

cette page dans votre navigateur. Afin d'afficher cette page, votre navigateur contactera le serveur HTTP sur gaia.cs.umass.edu et échangera des messages HTTP avec le serveur afin de télécharger cette page, comme indiqué dans cours. Les trames Ethernet ou WiFi contenant ces messages HTTP (ainsi que toutes les autres trames passant par votre adaptateur Ethernet ou WiFi) seront capturées par Wireshark.

7. 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. La fenêtre principale de Wireshark devrait maintenant ressembler à la Figure 3. Vous avez maintenant des données de paquets "live" qui contiennent tous les messages de protocole échangés entre votre ordinateur et d'autres entités du réseau ! Les échanges de messages HTTP avec le serveur Web gaia.cs.umass.edu doivent apparaître quelque part dans la liste des paquets capturés. Mais de nombreux autres types de paquets seront également affichés (voir, par exemple, les nombreux types de protocoles différents indiqués dans la colonne Protocole de la Figure 3). Même si la seule action que vous avez entreprise a été de télécharger une page Web, il y avait évidemment de nombreux autres protocoles en cours d'exécution sur votre ordinateur qui ne sont pas vus par l'utilisateur. Nous en apprendrons beaucoup plus sur ces protocoles au fur et à mesure que nous progressons dans le texte !

8. Tapez "http" (sans les guillemets et en minuscules - tous les noms de protocole sont en minuscules dans Wireshark, et assurez-vous d'appuyer sur votre touche Entrée/Retour) dans la fenêtre de spécification du filtre d'affichage en haut de l'écran principal (fenêtre Wireshark). Sélectionnez ensuite *Appliquer* (à droite de l'endroit où vous avez entré "http") ou appuyez simplement sur Retour. Ainsi, seuls les messages HTTP seront affiché dans la fenêtre de liste des paquets. La Figure 5 ci-dessous montre une capture d'écran après l'application du filtre http à la fenêtre de capture de paquets illustrée précédemment dans la Figure 3. Notez également que dans la fenêtre *Détails* du paquet sélectionné, nous avons choisi d'afficher le contenu détaillé du message d'application du protocole de transfert hypertexte qui a été trouvé dans le segment TCP, qui était à l'intérieur du datagramme IPv4 qui était à l'intérieur de la trame Ethernet II (WiFi). Se concentrer sur le contenu au niveau d'un message, d'un segment, d'un datagramme et d'une trame spécifiques nous permet de nous concentrer uniquement sur ce que nous voulons regarder (dans ce cas, les messages HTTP).

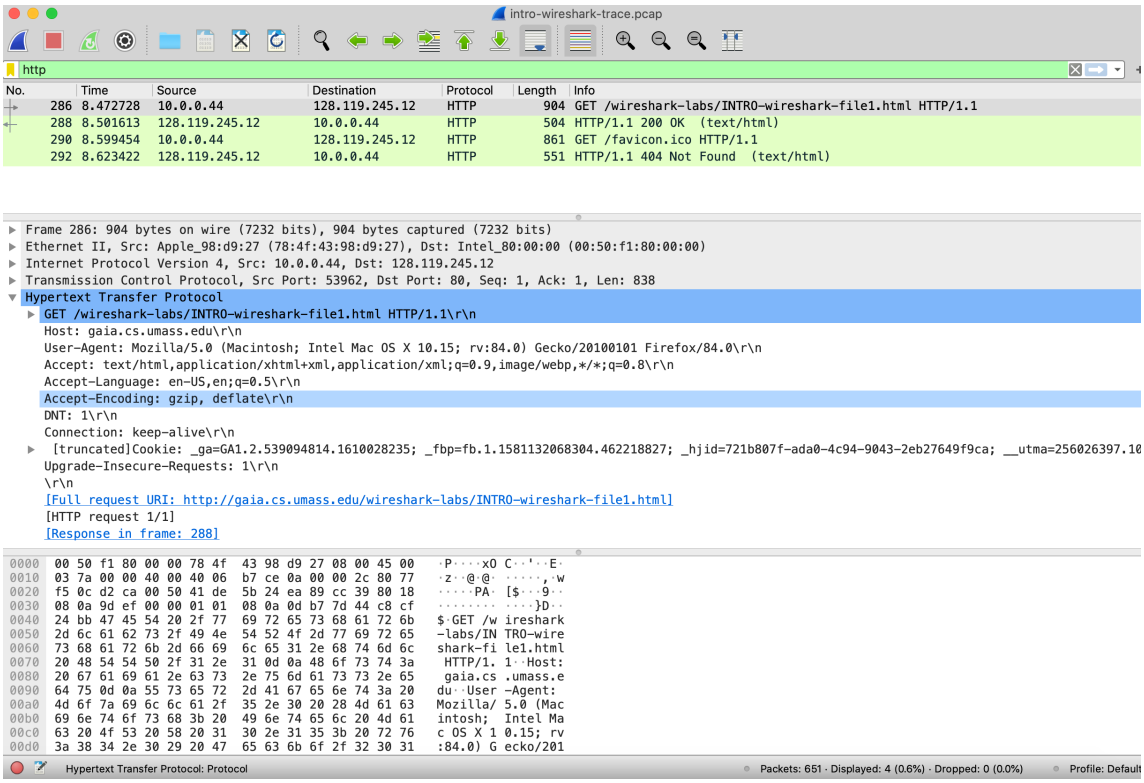

Figure 5: Détails du message HTTP qui contenait un GET de http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

9. Recherchez le message HTTP GET qui a été envoyé depuis 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 (voir les Figures 3 et 5) qui affiche "GET" suivi de l'URL gaia.cs.umass.edu que vous avez entrée. Lorsque vous sélectionnez le message HTTP GET, la trame Ethernet, le datagramme IP, le segment TCP et les informations d'en-tête de message HTTP seront affichés dans la fenêtre d'en-tête de paquet. En cliquant sur "+" et "-" et sur les flèches pointant vers la droite et vers le bas sur le côté gauche de la fenêtre des détails du paquet, vous réduisez la quantité d'informations sur les trames, Ethernet, Internet Protocol et Transmission Control Protocol affichées. Maximisez la quantité d'informations affichées sur le protocole HTTP. Votre affichage Wireshark devrait maintenant ressembler à peu près à la Figure 5. (Notez, en particulier, la quantité réduite d'informations de protocole pour tous les protocoles sauf HTTP, et la quantité maximisée d'informations de protocole pour HTTP dans la fenêtre d'en-tête de paquet).

10. Quitter Wireshark

Félicitations! Vous avez maintenant terminé le premier Atelier !

Répondez maintenant aux questions ci-dessous.

1. Parmi les protocoles suivants, lesquels sont affichés (c'est-à-dire répertoriés dans la colonne "protocole" de Wireshark) dans votre fichier de suivi : TCP, QUIC, HTTP, DNS, UDP, TLSv1.2 ?
2. Combien de temps s'est écoulé entre l'envoi du message HTTP GET et la réception de la réponse HTTP OK ? (Par défaut, la valeur de la colonne Heure dans la fenêtre de liste des paquets correspond à la durée, en secondes, écoulée depuis le début du traçage Wireshark. (Si vous souhaitez afficher le champ Heure au format heure du jour, sélectionnez Afficher le menu déroulant, puis sélectionnez Format d'affichage de l'heure, puis sélectionnez Heure du jour.)
3. Quelle est l'adresse Internet de gaia.cs.umass.edu (également connu sous le nom de www-net.cs.umass.edu) ? Quelle est l'adresse Internet de votre ordinateur ou (si vous utilisez le fichier de trace donné par le prof) de l'ordinateur qui a envoyé le message HTTP GET ?

Pour répondre aux deux questions suivantes, vous devrez sélectionner le paquet TCP contenant la requête HTTP GET. Le but de ces deux questions suivantes est de vous familiariser avec l'utilisation de la fenêtre "Détails du paquet sélectionné" de Wireshark (voir la Figure 3). Pour répondre à la première question ci-dessous, regardez dans la fenêtre "Détails du paquet sélectionné" basculez le triangle pour HTTP (votre écran devrait alors ressembler à la Figure 5); pour la deuxième question ci-dessous, vous devrez développer les informations sur la partie TCP (Transmission Control Protocol) de ce paquet.

4. Affichez les informations sur le message HTTP dans la fenêtre "Détails du paquet sélectionné" de Wireshark (voir la Figure 3 ci-dessus) afin que vous puissiez voir les champs dans le message de requête HTTP GET. Quel type de navigateur Web a émis la requête HTTP ? La réponse s'affiche à l'extrémité droite des informations après le champ "User-Agent :" dans l'affichage étendu du message HTTP. [Cette valeur de champ dans le message HTTP indique comment un serveur Web apprend le type de navigateur que vous utilisez.]
    - Firefox, Safari, Microsoft Internet Edge, ou autre

5. Affichez les informations sur le protocole de contrôle de transmission pour ce paquet dans la fenêtre "Détails du paquet sélectionné" de Wireshark (voir la Figure 3) afin que vous puissiez voir les champs du segment TCP transportant le message HTTP. Quel est le numéro de port de destination (le numéro suivant "Dest Port :" pour le segment TCP contenant la requête HTTP) auquel cette requête HTTP est envoyée ?

Et au final ...

6. Imprimez les deux messages HTTP (GET et OK) mentionnés à la question 2 ci-dessus. Pour ce faire, sélectionnez Imprimer dans le menu de commande Fichier Wireshark, puis sélectionnez les boutons radiaux "Paquet sélectionné uniquement" et "Imprimer tel qu'affiché", puis cliquez sur OK.