Laboratoire ADR

Introduction au logiciel Wireshark

Objectif

Installation du logiciel Wireshark

Utilisation du logiciel pour l’analyse de réseaux

Définir des filtres pour la visualisation de trames

Matériels/Logiciels

Wireshark

Les questions à répondre

Les parties qui demandent des captures d’écran ou des réponses sont marquées en police blanche sur fond bleu :

Illustration

Informations générales

La compréhension des protocoles de réseau peut souvent être grandement approfondie en voyant les protocoles en action et en jouant avec les protocoles. Les analyseurs de réseaux permettent d’observer la séquence des messages échangés entre deux entités homologues et donc de voir des protocoles en action.

Dans ce laboratoire, vous devez installer le logiciel de capture et d’analyse de réseaux Wireshark dans une machine virtuelle ou dans votre ordinateur. Un rapport sera soumis par élève.

Le rapport est dû le soir du laboratoire suivant. Une semaine supplémentaire peut être donnée si la date de rendu coïncide avec un TE de la classe.

Découvrir le logiciel Wireshark

Wireshark est un programme informatique libre de droits qui permet de capturer et d’analyser les trames transmises par les interfaces de communication du terminal sur lequel il s’exécute ou par d’autres systèmes lorsque le milieu de transmission est partagé, comme par exemple dans le cas de 802.11. Si les trames ne sont pas chiffrées, le contenu peut donc être lu par l’utilisatrice ou l’utilisateur de Wireshark à des fins, par exemple, de dépannage.

Installation

Allez sur le site <https://www.wireshark.org> et suivez les instructions pour télécharger et installer le logiciel.

Utilisation

Les instructions suivantes sont basées sur une version de Wireshark pour Windows. Elles ne seront donc pas applicables directement si vous utilisez d’autres systèmes d’exploitation (Linux ou Mac OSX) ou si la version de Windows que vous utilisez est différente. Cependant, les instructions devraient être suffisamment similaires pour que vous puissiez les utiliser.

Depuis le menu Démarrer, lancer l'application Wireshark. Vous verrez apparaître une fenêtre similaire à celle-ci (mais pas forcément identique puisque, encore un fois, elle dépendra de la version et du système d’exploitation) :

Graphical user interface, application

Description automatically generated

Capture de paquets

Pour capturer des paquets, vous pouvez cliquer sur le bouton bleu en forme d’aileron de requin dans la barre d’outils.

Lorsque vous aurez capturer quelques trames, arrêter la capture avec le bouton carré rouge dans la barre d’outils (à côté de l’aileron).

1. Montrez une capture d’écran. Voici un exemple pour illustrer l’aspect général de ce que vous devriez voir :

Graphical user interface, application, Word

Description automatically generated

Ouverture d’un fichier de capture existant :

Les paquets capturés par Wireshark peuvent être sauvegardés dans des fichiers. Deux tels fichiers sont disponibles sur le site du cours dans la page de téléchargements Labo.

Téléchargez-les et notez leur emplacement sur votre machine avant de continuer.

Ouvrez d’abord le fichier appelé « Capture ADR.pcapng » avec Wireshark (File -> open dans la barre de menus).

Wireshark affichera les trames contenues dans le fichier (qui correspondent à des trames capturées dans un réseau 802.11) comme ci-dessous.

Graphical user interface, text, application

Description automatically generated

2. Montrez à l’aide d’une capture d’écran le résultat de l’ouverture du fichier sur votre ordinateur.

En plus de la barre de menus et la barre d’outils montrées avec des flèches à la figure ci-dessus, la fenêtre est divisée en trois parties marquées 1, 2 et 3 à la figure ci-dessus.

3. Décrivez les informations données par chacune des parties (cherchez les informations dans le menu « help » ou par Internet).

Première partie : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Deuxième partie : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Troisième partie : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Filtres d’affichage Wireshark

Les captures contiennent un grand nombre de paquets. Il est possible de spécifier quels paquets sont affichés en utilisant un filtre d’affichage (ou filtre de post-capture).

La sélection peut se faire sur par différentes méthodes dont :

• en tapant le nom d’un protocole : par exemple icmp

• en utilisant les valeurs des champs des entêtes : par exemple le type et/ou subtype des trames 802.11

• par la présence ou par l’absence d’un champ dans les entêtes

Les filtres d’affichage peuvent être introduits dans la fenêtre de la barre d’outils des filtres qui se trouve en dessous de la barre d’outils (voir figure à la section 3).

Vous pouvez aussi sélectionner un champ dans les détails d’un paquet, puis avec clic droit : Apply as filter…

Introduisez un filtre en tapant « icmp » (sans les guillemets) dans la fenêtre de la barre d’outils de filtres.

4. Montrez une capture d’écran du résultat.

Le paquet le plus commun est le paquet « beacon », qui est transmis dans les réseaux basés sur infrastructure environ dix fois par seconde. Cherchez par Internet le filtre pour ne pas afficher les beacons. Appliquez-le et montrez une capture d’écran dans laquelle le filtre ainsi que la liste de paquets résultante soit visible.

5. Montrez une capture d’écran.

Vous pouvez créer des filtres avec des opérateurs logiques « or » ou « and ». Nous allons les utiliser dans le prochain labo.

Les champs dans les trames et le calcul du temps de transmission

Ouvrez maintenant le fichier de capture appelé « Single frame.pcapng ».

Wireshark décode et affiche les entêtes des couches successives dans le panneau du milieu (numéro 2 dans la figure de la section 6 ci-dessus).

La figure ci-dessous vous montre la relation entre ce qui est affiché par Wireshark pour le paquet de la capture que vous venez d’ouvrir, la trame MAC 802.11 et les différentes couches ou protocoles dont les entêtes sont décodés.



Les trois premières lignes du panneau du milieu dans Wireshark (identifié par le numéro 1 dans la figure ci-dessus) contiennent respectivement

1) des informations globales sur le paquet,

2) le Radiotap header et

3) la Radio 802.11 information.

A partir de la quatrième ligne, Wireshark vous présente l’encapsulation des différents protocoles en commençant par l’entête la plus extérieur de la trame (MAC) :

la quatrième ligne décode l’encapsulation MAC 802.11, la cinquième décode l’entête LLC, la sixième décode l’entête IP et ainsi de suite.

6. En explorant le contenu décodé par Wireshark pour les différentes entêtes et en utilisant les premières lignes (Frame, Radiotap header et 802.11 radio information), déterminer :

1. La longueur en octets du NPDU (PDU du protocole IP)
2. Le débit nominal de la transmission de cette trame transmission
3. Si le préambule long ou court est utilisé
4. Calculez le temps de transmission du paquet incluant l’entête PLCP (seulement le paquet, pas de DIFS, SIFS ou autre)
5. La valeur calculée correspond-elle au temps de transmission affiché dans le « 802.11 Radio information » ?
6. Dans radio information, il y a deux temps en µs appelés Start et End. Est-ce que la différence de ces deux valeurs correspond à la durée que vous avez calculée ? Sinon, pourquoi ?