
ESIEA MS-SIS

# Rapport de Projet
# Lecteur de fichier Pcap

*Auteur :*
Vincent CLÉMENT

6 novembre 2016

# Table des matières

# Chapitre 1

# Présentation du projet

## 1.1 Introduction

.Dans le cadre de la formation mastère spécialisé de l'esiea, il nous était demandé d'écrire un programme capable de lire des fichiers pcap. Le programme doit respecter un cahier des charges qui implique d'utiliser le langage de programmation Java qui est orienté objet. Il ne doit pas contenir d'interface graphique, simplement une interface en console. L'utilisation d'une API, autre que l'API standard Java est interdite. Les différents protocoles devront être detecté par le programme, une option donné au programme permet de choisir le protocole que l'on souhaite afficher.

— Ethernet ;
— ARP ;
— IP ;
— TCP ;
— UDP ;
— ICMP ;
— DHCP ;
— HTTP ;
— DNS.

Dans ce projet, je n'ai pas implémenter tout les protocoles. Il me manque les protocoles de couche 5 à 7 (DHCP, HTTP, DNS)

## 1.2 Présentation du fichier Pcap

La première chose a effectué lors de l'ouverture du fichier pcap, est l'extraction du "Global Header" du fichier. Il contient plusieurs informations essentielles à la compréhension du fichier, notamment l'encodage des informations binaire. Si Les informations sont codés selon la norme "Big-Endian" dans ce cas, on accepte d'ouvrir le fichier, sinon on le rejette. Pour la norme Little-Endian il faut inverser chaque octet.

La figure ci-dessous montre comment est composé le fichier pcap.


Dans ce fichier, chaque paquet est composé de deux choses :

— Un Header Pcap ;
— Un Packet Data.

Le header donne les informations de base du paquet. Les données correspondent au paquet réseau. Pour commencer, j'ai créé un objet pour rassembler les informations contenu dans le pcap header, et un second objet qui correspond au donnée. Ensuite dans chaque objet, il existe un attribut qui a pour type un tableau d'octets et qui contient les informations du fichier pcap. Ensuite une methode permet d'extraire les octets qui nous intéresse pour les analyser. Par exemple, on peut utliser cette méthode pour extraire les 4 premiers octets et vérifier que ces octets sont égaux à "d4c3b2a1".

## 1.3 Les différents objets du projet

Les réseaux sont construit autour du modèle OSI, lui-même divisé en 7 couches. Pour ce projet, j'ai créé un objet par couche. Les informations contenu dans l'objet "Header Pcap" contiennent les données sur la première couche de ce modèle. Sur chaque couche, j'ai créé plusieurs méthodes permettant de récuperer les informations intéressante. Puis ensuite, j'ai créé plusieurs objets par protocoles. Certains protocoles comme TCP et UDP héritent de la classe "Couche4".