Projet Sécurité 182



**Rapport de projet**

Zeqiri Amir – CIN3B

ETML, Vennes – A13

32 Périodes

Maître : M. Bourahla

Table des matières

[1 Introduction 3](#_Toc208996845)

[1.1 Schéma 3](#_Toc208996846)

[2 Présentation de WireShark 4](#_Toc208996847)

[3 Analyse et identification des trames du service DHCP 4](#_Toc208996848)

[4 Analyse et identification des trames du service DNS 4](#_Toc208996849)

[5 Analyse et identification des trames du service AD 4](#_Toc208996850)

[6 Problèmes rencontrés 4](#_Toc208996851)

[7 Sources & Aides 4](#_Toc208996852)

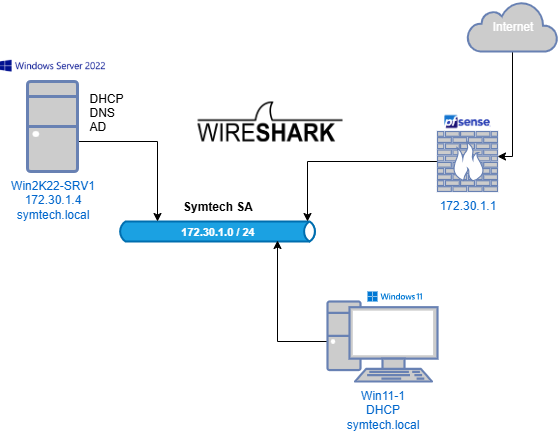
[8 Conclusion 4](#_Toc208996853)

# Introduction

Analyse du trafic réseau avec Wireshark

Dans le cadre du module 182 à l’ETML, nous devons réaliser un projet où l’objectif est de mettre en place une petite infrastructure et d’analyser le trafic réseau avec Wireshark. Le but est de voir comment fonctionnent certains services important comme DHCP, DNS et Active Directory, et de repérer les trames, protocoles et ports utilisés pendant leurs échanges.  
  
Le projet se fait dans un contexte pratique : une entreprise valaisanne de sécurité souhaite observer ce qui se passe sur le réseau quand ses services serveurs sont activés. Pour cela, nous avons installé un poste Windows 11 et un serveur Windows Server 2022, puis capturer le trafic Wireshark.  
  
Ce travail nous permet de mettre en pratique ce qu’on a appris sur les protocoles et les services réseau, mais aussi de mieux comprendre comment analyser et diagnostiquer un réseau, ce qui est une compétence utile en informatique et en sécurité.

## Schéma



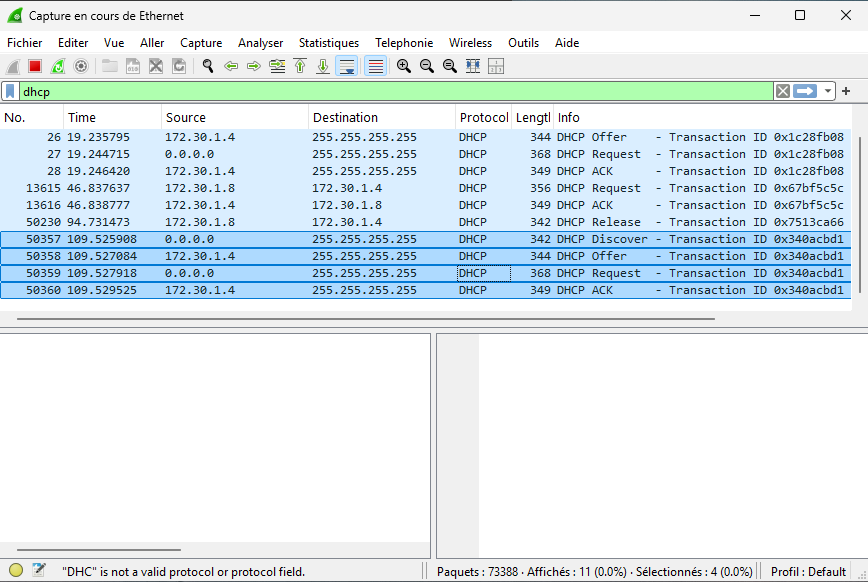
# Présentation de WireShark

Wireshark est un logiciel gratuit qui sert à analyser le trafic réseau. Avec lui, je peux capturer les paquets qui passent sur une carte réseau et les regarder en détail. Ça permet de voir quels protocoles sont utilisés, quelles machines discutent entre elles et quelles infos elles s’échangent.

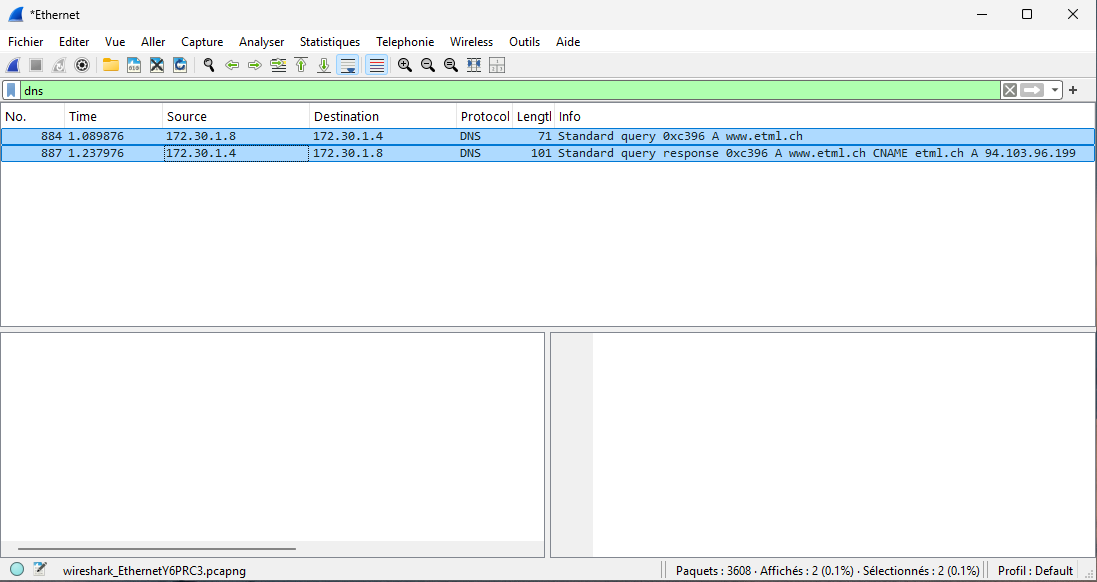
C’est un outil souvent utilisé par les admins réseaux et les personnes qui travaillent en sécurité, car il aide à trouver des problèmes de communication ou à vérifier que tout fonctionne comme prévu.

Dans mon projet, j’utilise Wireshark pour voir directement les trames envoyées et reçues par les services DHCP, DNS et Active Directory. C’est donc l’outil principal qui me permet d’analyser le trafic entre mon poste Windows 11 et mon serveur Windows Server 2022.

# Analyse et identification des trames du service DHCP

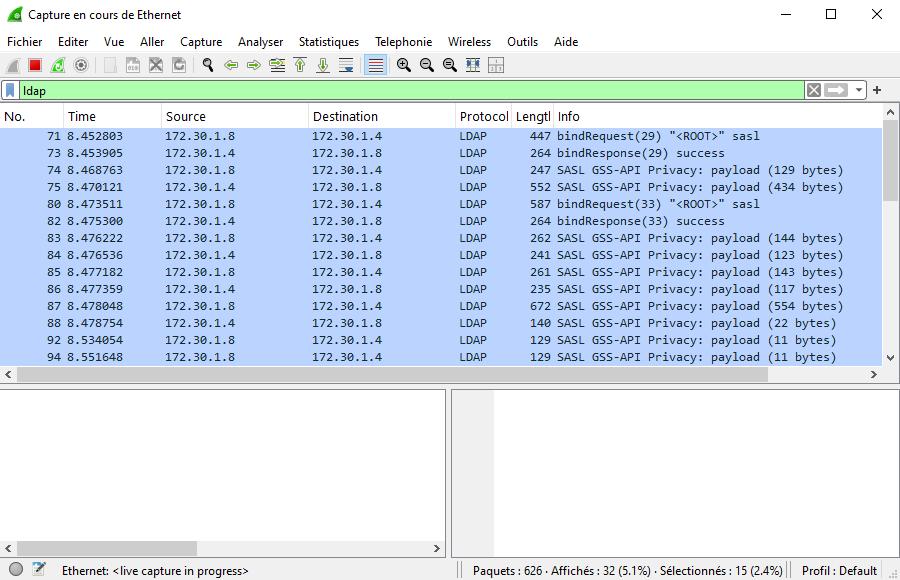


# Analyse et identification des trames du service DNS

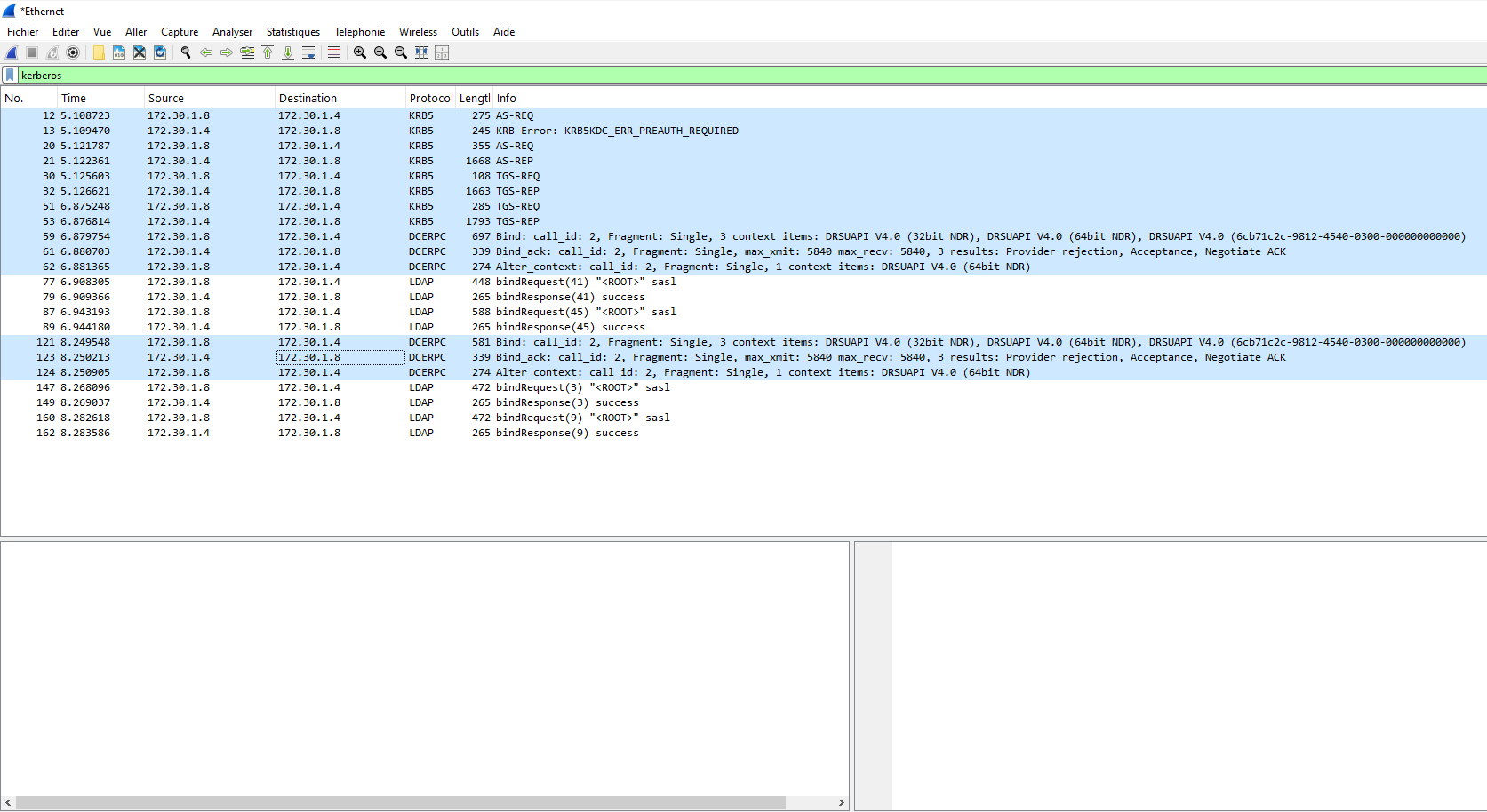


# Analyse et identification des trames du service AD

## LDAP



## Kerberos



## DNS

# Problèmes rencontrés

Problèmes rencontrés

# Sources & Aides

[Lien](file:///C:\Users\amizeqiri\Desktop\GitHub\P_Bulles_docker2\Lien) : Lien

# Conclusion

Conclusion