

# ANALYSE RESEAU AVEC WIRESHARK

**Programme** (Mis à jour le 16/02/2024)

## Introduction à Wireshark

- Démarrer une capture
- Utiliser les Timestamps
- Configurer les règles de coloration
- Sauvegarde et exportation
- Changer les préférences au niveau protocoles

## Utiliser les filtres de capture

- Configurer un filtre de capture
- Configurer un filtre Ethernet
- Filtrage Host et Network
- Filtrage TCP/UDP

## Utiliser les filtres d'affichages

- Filtrage Ethernet, ARP, Host, Network
- Filtrage de protocoles spécifiques
- Utilisation des opérateurs de filtrage

## Utiliser les outils de statistiques

- Hiérarchie de protocole
- Flow graph
- Conversations
- TCP Stream

## Analyse de flux Ethernet

- Broadcast (Erreur/storm)
- VLAN et VLAN Tagging
- Spanning Tree
- WIFI

## Analyse ARP, IP

- ARP Request Reply
- Fragmentation
- Routage IP
- Adresse IP dupliquée
- DHCP

## Analyse TCP/UDP

- Problème de connexion TCP
- Retransmission TCP
- Reset TCP

## Analyse HTTP et DNS

- Filtrage trafic DNS
- Filtrage trafic HTTP
- Filtrage trafic HTTPS SSL/TLS

## Analyse complémentaire : Fonctions réseaux

### Référence

THIS3211

### Durée

3 jours / 21 heures

### Prix HT / stagiaire

2175€

### Objectifs pédagogiques

- Identifier les causes les plus fréquentes de disfonctionnement dans les réseaux TCP/IP
- Savoir filtrer du trafic (capture / affichage)
- Création de profils personnalisés
- Connaître les règles de coloration, de graphiques, des interprétations terrains ainsi que les fonctionnalités clés des communications TCP/IP
- Comprendre le comportement normal/anormal de l'ARP, DNS, IP, TCP, UDP, ICMP, et HTTP/HTTPS, Etc...
- Maîtriser les techniques de capture de trafic et le placement de l'analyseur
- Comprendre le fonctionnement et l'analyse des protocoles en Téléphonie sur IP ainsi que l'Ethernet Industriel avec ModBus TCP et les protocoles de commutation et routage IP.

### Niveau requis

- Avoir de bonnes connaissances en Réseaux TCP / IP

### Public concerné

- Ce cours s'adresse à toute personne intéressée par le dépannage et l'optimisation des réseaux TCP/IP et l'analyse le trafic réseau avec Wireshark

### Formateur

Les formateurs intervenants pour Themanis sont qualifiés par notre Responsable Technique Olivier Astre pour les formations informatiques et bureautiques et par Didier Payen pour les formations management.

### Conditions d'accès à la formation

Délai : 3 mois à 1 semaine avant le démarrage de la formation dans la limite des effectifs indiqués

### Moyens pédagogiques et techniques

Salles de formation (les personnes en situation de handicap peuvent avoir des besoins spécifiques pour suivre la formation. N'hésitez pas à nous contacter pour en discuter) équipée d'un ordinateur de dernière génération par stagiaire, réseau haut débit et vidéo-projection UHD

Documents supports de formation projetés  
Apports théoriques, étude de cas concrets et exercices

Mise à disposition en ligne de documents supports à la suite de la formation

- Fonctionnement et analyse du protocole de signalisation SIP
- Fonctionnement et analyse des protocoles RTP/RTCP
- Analyse du protocole ModBus TCP et de ses usages
- Analyse du fonctionnement des protocoles réseaux de niveau 2 et 3

## **Conclusion**