

# Wireshark 2.x– Les Fondamentaux



Ce cours est destiné aux personnes concernées par l'administration des réseaux informatiques. Aucune durée minimale d'activité professionnelle n'est demandée.

## OBJECTIF

Wireshark est un outil fondamental et puissant pour aider les techniciens et les ingénieurs en charge de réseaux et de serveurs. Mais il est nécessaire de prendre le temps de l'approprier.

A l'issue de cette formation l'apprenant sera capable d'utiliser Wireshark pour une analyse en profondeur des flux réseaux et la détection des principales sources de dysfonctionnement des réseaux. Cette analyse portera essentiellement sur Ethernet en mode filaire, IP, TCP et UDP ainsi que les protocoles majeurs utilisés en TCP/IP.

Cette formation permettra également aux participants connaissant un peu Wireshark dans sa version 1.x non seulement d'améliorer leurs techniques de capture et d'analyse mais aussi d'approprier la nouvelle interface et les nouvelles fonctionnalités de la version 2.

Une formation complémentaire de 3 jours, uniquement tournée vers l'analyse des problèmes et des performances sur un réseau filaire, est aussi disponible. Elle nécessite d'avoir acquis les connaissances fondamentales décrites ci-après.

## CONTENU

- L'interface de Wireshark
- Comment capturer un flux réseau
- Comment créer et utiliser de filtres de capture pour ne garder que les trames intéressantes
- Comment gérer les préférences et les options de capture
- Comment colorer les trames pour mieux identifier les flux
- Comment créer et utiliser les filtres d'affichage pour se concentrer sur les flux pertinents
- Utiliser et formater les différents horodatages
- Comment créer de nouvelles colonnes avec des informations contenues dans les trames

- Comment utiliser les profils pour changer rapidement les réglages mis en œuvre selon le cas à traiter (analyse TCP, DNS, http, recherche de problèmes de performance)
- Sauvegarde et impression des captures
- Exemples concrets d'analyse de flux
- Comment exploiter les principales statistiques et les principaux graphiques à des fins de diagnostic
- Présentation succincte des outils en lignes de commande

## PRE-REQUIS

- Connaissances de base sur les réseaux et TCP/IP
- Être à l'aise avec un PC sous Windows (7, 8 ou 10)
- Les connaissances en sécurité informatique sont un plus mais ne sont pas obligatoires

## DATES ET LIEUX

Formation en classe virtuelle

Durée : 2 jours -14h00 (9h30-17h30)

Planning : [WireShark \(infinigate.fr\)](http://WireShark.infinigate.fr)

## INSCRIPTION

Connectez-vous sur notre site  
[www.infinigate.fr/trainings](http://www.infinigate.fr/trainings)

Si vous avez des questions sur le contenu de la formation, les prérequis, et les modalités d'accès aux personnes en situation de handicap, contactez-nous :  
[info@infinigate.fr](mailto:info@infinigate.fr)

