

# KAÏNA-COM

## CATALOGUE DE FORMATION

### KR005 – L'outil wireshark - analyser les trames réseaux

---

#### Comprendre l'art d'analyser les flux réseaux



## KR005 – L'outil Wireshark - Analyser les trames réseaux

---

**Référence** KR005

---

**Niveau**

Débutant  
 Intermédiaire  
 Expert

---

**Nombre de jours** 2 jours

---

**Lieu de la formation** KAÏNA-COM  
LE CARRÉ HAUSSMANN II,  
6, allée de la Connaissance  
77127 Lieusaint - France

---

**Prix** 1.330 € HT

---

**Prérequis** Bonne connaissance des réseaux TCP/IP

---

**Public**

- Ingénieurs ou architectes
- Administrateurs système et réseau
- Développeurs
- Professionnels de la sécurité informatique

---

*Ce sujet continue à la page suivante*

## KR005 – L'outil Wireshark - Analyser les trames réseaux, suite

---

### Objectifs

Wireshark est un outil libre et gratuit qui permet de faire l'analyse de paquets et protocoles réseaux. Il est utilisé dans le dépannage, l'analyse de réseaux informatiques et le développement de protocoles.

Il facilite les captures, le décodage et l'analyse de paquets transmis sur tous les types de réseaux.

À l'issue de cette formation "l'outil wireshark - analyser les trames réseaux", vous serez en mesure de :

- Maîtriser l'outil wireshark
- Analyser les flux d'un réseau
- Diagnostiquer un problème réseau

---

*Ce sujet continue à la page suivante*

## KR005 – L'outil Wireshark - Analyser les trames réseaux, suite

**Contenu du cours**      Contenu du cours :

**Table 1: K005 - Contenu du cours**

Chapitre	Contenu
<b>Introduction</b>	<ul style="list-style-type: none"><li>• Objectifs</li><li>• Historique</li></ul>
<b>Fondamentaux</b>	<ul style="list-style-type: none"><li>• Méthodes de communications (unicast, multicast, broadcast)</li><li>• Les topologies et le contrôle d'accès</li><li>• Modèle de l'OSI</li><li>• Format d'une trame Ethernet</li><li>• Format d'un paquet IP</li></ul>
<b>Wireshark – Outil de trace</b>	<ul style="list-style-type: none"><li>• Description d'outil wireshark</li><li>• Installation d'un outil de trace (wireshark)</li><li>• L'écran de wireshark<ul style="list-style-type: none"><li>▪ Barre d'outils</li><li>▪ Zone de filtrage (comment appliquer un filtre)</li><li>▪ Zone d'affichage des paquets</li><li>▪ Zone d'affichage du contenu du paquet sélectionné</li><li>▪ Zone d'affichage du contenu du paquet sélectionné en hexadécimal</li></ul></li><li>• Barre d'état (accès au mode expert, aux annotations, affiche le nombre de paquets capturés et le profil en cours)</li></ul>

*Ce sujet continue à la page suivante*

## KR005 – L’outil Wireshark - Analyser les trames réseaux, suite

### Contenu du cours, suite

Chapitre	Contenu
<b>Fonctionnalités wireshark</b>	<ul style="list-style-type: none"><li>• Définition de paramètres généraux et personnels</li><li>• Définition de valeurs de temps et d'interprétation de résultats</li><li>• Création et application de filtres d'affichage</li><li>• Suivi des flux et réassemblage de données</li><li>• Personnalisation du profil wireshark</li><li>• Utilisation du système expert de wireshark</li></ul>
<b>L'analyse avec wireshark</b>	<ul style="list-style-type: none"><li>• L'analyse des trames :<ul style="list-style-type: none"><li>– TCP/IP</li><li>– ARP</li><li>– DHCP</li><li>– DNS</li><li>– HTTP</li><li>– FTP</li></ul></li><li>• Capture des communications réseaux en "clear text"</li><li>• Identifier qui veut se connecter au réseau</li><li>• Capturer et analyser le trafic d'un hôte ou d'un réseau</li></ul>
<b>Le dépannage avec wireshark</b>	<ul style="list-style-type: none"><li>• Identifier des délais anormaux</li><li>• Identifier des problèmes TCP</li><li>• Détecter des problèmes HTTP</li><li>• Détecter des erreurs applicatives</li><li>• Générer des graphiques</li><li>• Identifier des problèmes de buffer saturés</li><li>• Détecter des problèmes d'adresse IP dupliquées</li><li>• Identifier des problèmes liés au protocole DHCP</li></ul>

*Ce sujet continue à la page suivante*

## KR005 – L'outil Wireshark - Analyser les trames réseaux, suite

---

### Contenu du cours, suite

Chapitre	Contenu
<b>Utilisation de graphs</b>	<ul style="list-style-type: none"><li>• Maîtrise basique et avancée des fonctions de graph IO</li><li>• Graphs pour les problèmes de débit</li><li>• Graphs pour les problèmes de ralentissement</li><li>• Graphs sur les autres problèmes réseau</li></ul>
<b>Évaluation finale</b>	<ul style="list-style-type: none"><li>• Questions et réponses</li><li>• Examen final</li><li>• Évaluation du cours</li></ul>

---