

1. SOMMAIRE

1. SOMMAIRE.....	2
2. OBJET.....	4
3. PRÉREQUIS.....	5
3.1 CONNAISSANCES.....	5
3.2 DIFFÉRENCE ENTRE COMMUTATEUR (SWITCH) ET RÉPÉTEUR (HUB).....	6
3.2.1 Répéteur.....	6
3.2.2 Commutateur.....	6
4. CAPTURES.....	7
4.1 ÉDITION DES PRÉFÉRENCES.....	7
4.2 CHOISIR LES PARAMÈTRES DE CAPTURE.....	8
4.2.1 Filtres de capture.....	9
4.2.2 Limitation de la taille des paquets.....	10
4.2.3 Arrêt automatique sur seuil.....	10
4.2.4 Captures circulaires.....	11
4.3 CAPTURES À DISTANCE.....	11
4.3.1 Environnement Linux.....	11
4.3.2 Environnement Microsoft.....	12
4.4 CAPTURE SUR PLUSIEURS INTERFACES.....	12
5. ANALYSES.....	14
5.1 LECTURE DES TRAMES.....	14
5.1.1 Fenêtre de résumé.....	14
5.1.2 Fenêtre d'arborescence de protocole.....	14
5.1.3 Fenêtre de vue des données.....	15
5.1.4 Réglages utiles.....	15
5.1.4.1 Affichage horaire.....	15
5.1.4.2 Choix des colonnes.....	15
5.2 ANALYSE RAPIDE.....	16
5.2.1 Expert Info Composite.....	16
5.2.2 Filtres d'affichage.....	17
5.2.3 Filtres d'affichage sur le grapheur.....	19
5.3 ANALYSE NORMALE.....	20
5.3.1 Informations sur la capture.....	20
5.3.2 Répartition des protocoles.....	20
5.3.3 Répartition des tailles de paquets.....	21
5.3.4 Conversations.....	22
5.4 ANALYSE GRAPHIQUE DE FLUX.....	23
5.5 ANALYSE TEXTE D'UN FLUX TCP OU UDP.....	24
5.6 ANALYSE GRAPHIQUE "TIME-SEQUENCE" (TCPTRACE).....	25
6. DIAGNOSTIC.....	27
6.1 TYPE DE PROTOCOLES.....	27
6.2 ARP.....	28
6.3 PROTOCOLES TCP OU UDP.....	28
6.3.1 DNS.....	28
6.4 ERREURS GÉNÉRALES.....	29
6.4.1 Zero Window.....	29
6.4.2 TCP Window Update.....	30
6.4.3 TCP ZeroWindowViolation.....	31
6.4.4 TCP ZeroWindowProbe.....	31

Guide d'utilisation de l'analyseur réseau Wireshark

6.4.5 <i>Windows is full</i>	31
6.4.6 <i>Bad Checksum IPv4</i>	31
6.4.7 <i>Duplicate ACK</i>	32
6.4.8 <i>Fast retransmit</i>	33
6.4.9 <i>TCP Retransmission</i>	33
6.4.10 <i>TCP Out-of-order</i>	33
6.4.11 <i>TCP Previous segment lost</i>	33
6.4.12 <i>BER error</i>	33
6.5 FLUX PARTICULIERS.....	33
6.5.1 <i>streaming</i>	33
6.5.2 <i>Spanning-tree</i>	36

2. OBJET

Le logiciel Wireshark (anciennement Ethereal) permet la capture et l'analyse de trames sur Ethernet.

Son utilité est indéniable pour contrôler le bon fonctionnement de réseau ou vérifier les trames transitant sur une interface d'un commutateur ou analyser les trafics inutiles ou ceux impactant les performances du réseau.

Voici un petit récapitulatif des capacités de Wireshark :

- Décoder les trames (niveau 2 et 3)
- Calculer le débit moyen sur la durée de la capture (Mbps)
- Tracer un graphe du trafic pour tout ou partie des flux capturés
- Afficher les temps de réponses des trames TCP (basé sur les acquittements)
- Indiquer les erreurs ou les alertes détectées (paquets perdus, retransmis, dupliqués...)
- Suivre un dialogue TCP (notamment HTTP)
- Donner les statistiques sur les tailles des trames réseaux
- Etc.

Pour cela, il suffit de l'installer sur un PC munit d'une interface réseau 100 Mbps ou plus et fonctionnant sous Windows ou Linux. La version décrite ici fonctionne sous Windows XP. Il s'agit de la version 1.6.

Récupérer la dernière version du programme sur le site <http://www.wireshark.org/>

Suivre les instructions d'installation (en particulier l'installation de WinPCAP s'il n'est pas déjà installé sur le poste).

Une fois l'installation terminée, le **poste** devient une **sonde** réseau prête à fonctionner.

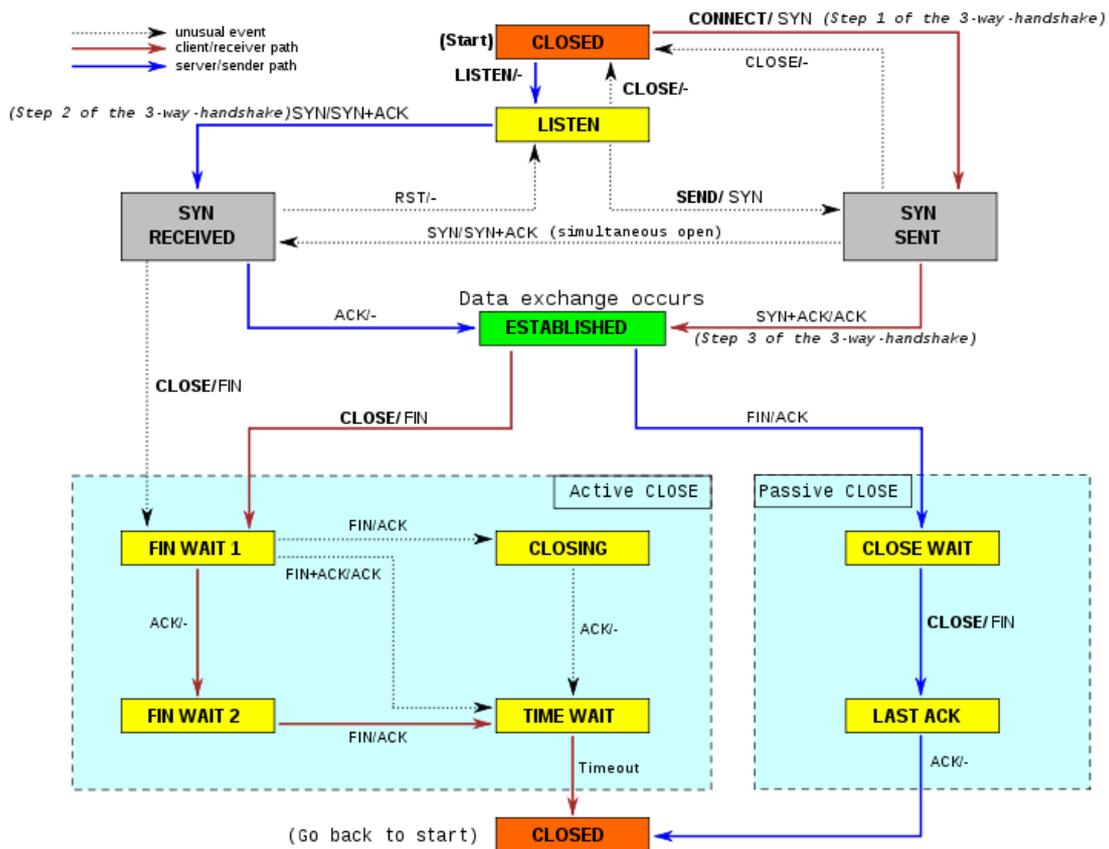
3. PRÉREQUIS

Bien que Wireshark fonctionne sur de nombreux systèmes d'exploitation (Windows, Linux, ...), d'autres éléments sont à prendre en compte pour permettre une capture dans de bonnes conditions.

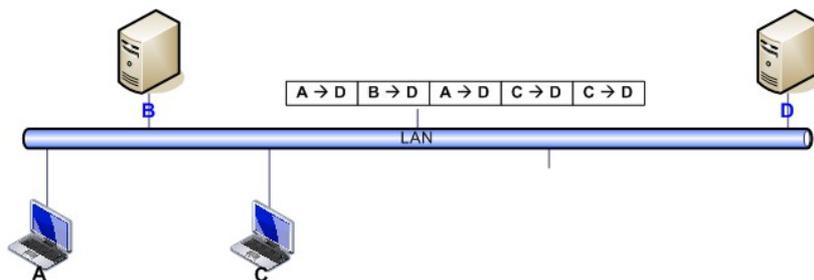
3.1 Connaissances

La connaissance des protocoles réseaux dans la théorie est un plus indéniable pour utiliser Wireshark.

Sans reprendre la description complète de TCP/IP, le schéma ci-dessous permet de lire l'état d'une connexion TCP (mode connecté du protocole IP).



Ce schéma permet de comprendre pourquoi un analyseur permet de trouver un problème réseau : en effet, les trames réseaux sont envoyés les unes après les autres mais un serveur ou un poste client reçoit également de nombreux autres flux. Les conversations ne sont donc pas continues dans le temps, comme le montre l'exemple ci-après. La machine « D » recevra plusieurs trames en provenance de « A », « B » et « C », que la couche « TCP » se chargera de remettre dans l'ordre.



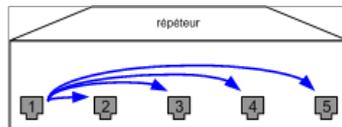
3.2 Différence entre commutateur (switch) et répéteur (hub)

Le placement de la sonde est important et pourtant, le choix du matériel et du point de collecte reste une des raisons de l'échec d'une analyse.

Désormais, il n'y presque plus que des commutateurs sur les réseaux. Ils sont rapides et semblent ne pas perturber les captures de paquets. Malheureusement, l'avantage principal des commutateurs sur les répéteurs devient un inconvénient pour les analyses réseaux.

3.2.1 RÉPÉTEUR

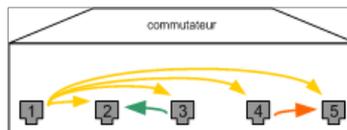
Le répéteur est un équipement actif qui reçoit un signal sur un port et le renvoie sur ses autres ports.



Les paquets sont émis simultanément sur l'ensemble des ports et si plusieurs machines communiquent en même temps, les règles du protocole CSMA/CD s'appliquent.

3.2.2 COMMUTATEUR

Le commutateur est un équipement actif doté d'une intelligence lui permettant de transmettre les trames directement à destination d'un port, à la condition qu'il retrouve l'adresse Ethernet (aussi appelée adresse MAC) de la machine destinataire sur un de ces ports. Il fonctionne donc au niveau 2 du modèle OSI. Pour les autres trames, il fonctionne comme un simple répéteur (ne pouvant pas déterminer le port de destination) : cela est vrai pour les trames de broadcast notamment.



De ce fait, capturer le flux du port 3 en étant sur le port 5 n'est pas directement possible. Il existe plusieurs méthodes malgré tout :

- ✦ **Port mirroring** : le commutateur réplique toutes les trames valides du port à surveiller sur le port où est connectée la sonde.
- ✦ **Network TAP** : il s'agit d'une solution de duplication des trames. Un TAP passif consiste en une sorte de multiprise physique (4 ports RJ45) qui peut fonctionner en 10/100 Mbps full-duplex. Un TAP actif est un répéteur capable de monter jusqu'à 10 Gbps mais est très coûteux.
- ✦ **ARP poisoning** : cette solution logicielle vient « tromper » le commutateur sur l'adresse MAC du destinataire. Cette solution n'est pas très propre en terme d'analyse.
- ✦ **ARP flooding** : cette solution consiste à saturer les tables ARP du commutateur pour l'obliger à broadcaster toutes les communications. Solution peu recommandable.

4. CAPTURES

La première opération est la capture de trames. Cependant il y a plusieurs cas possibles :

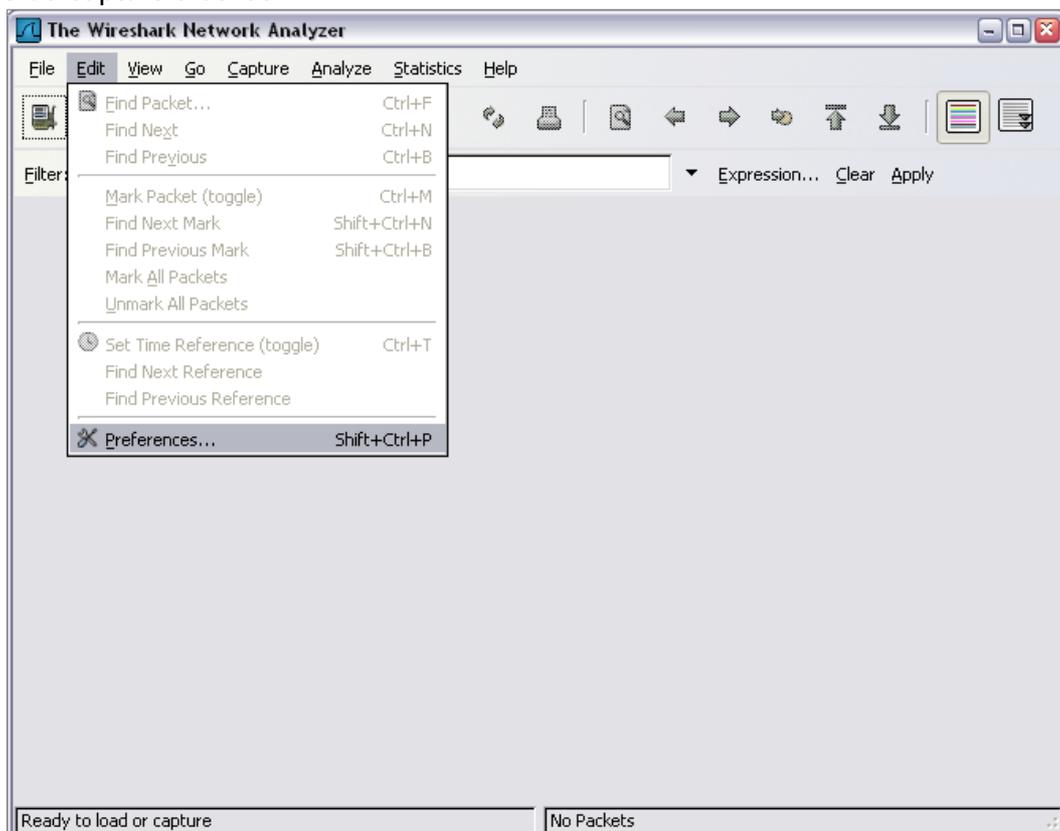
- Capture en temps réel de manière manuelle (l'utilisateur démarre et arrête la capture)
- Capture avec limitations automatiques (dans le temps ou sur la taille...)
- Capture sur une période donnée avec rotation (utilisation d'un « buffer » circulaire)
- Capture distante
- Capture sur plusieurs interfaces

D'autre part, il peut être utile de limiter les données capturées à celles qui sont en cause lors de l'analyse :

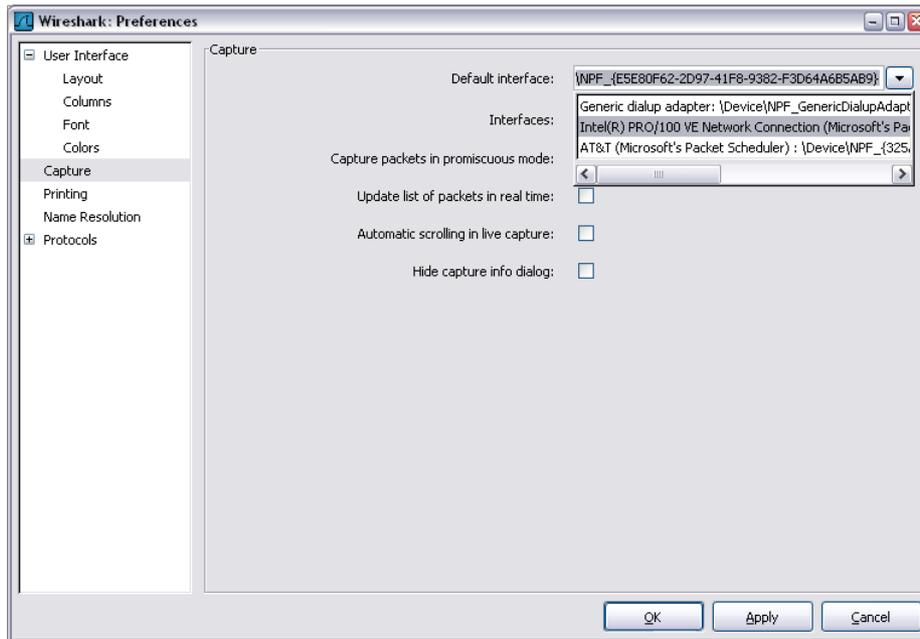
- Filtrage par protocoles
- Filtrage par adresses
- Limitation de la taille des paquets capturés

4.1 Édition des préférences

L'édition des préférences permet de choisir l'apparence de Wireshark mais aussi de choisir l'interface de capture à utiliser :



Guide d'utilisation de l'analyseur réseau Wireshark



Une fois les préférences modifiées, il est possible de procéder à notre première capture.

4.2 Choisir les paramètres de capture

Pour faire une **capture manuelle**, il suffit de cliquer sur l'icône "Start a new live capture" ou dans le menu, choisir [Capture] [Start]... il suffira ensuite d'arrêter la capture en cliquant sur l'icône à sa droite.



Cette option est intéressante pour tester le trafic et déterminer la quantité d'informations passant sur l'interface, cependant il est préférable de faire une capture automatisé.

Attention : la capture de trames sur un commutateur ne permet pas de voir tout le trafic mais seulement celui à destination du port où se trouve la sonde. En général, le seul trafic visible est constitué de broadcast (Ethernet, TCP/IP, Netbios, IPX...)

Pour analyser le trafic utile en provenance ou à destination d'un équipement particulier, il est nécessaire d'activer une fonction de mirroring ou monitoring. Consulter la documentation du fabricant du commutateur pour plus d'informations. En dernier recours, il peut-être nécessaire d'intercaler un répéteur (hub) entre l'équipement et la sonde.

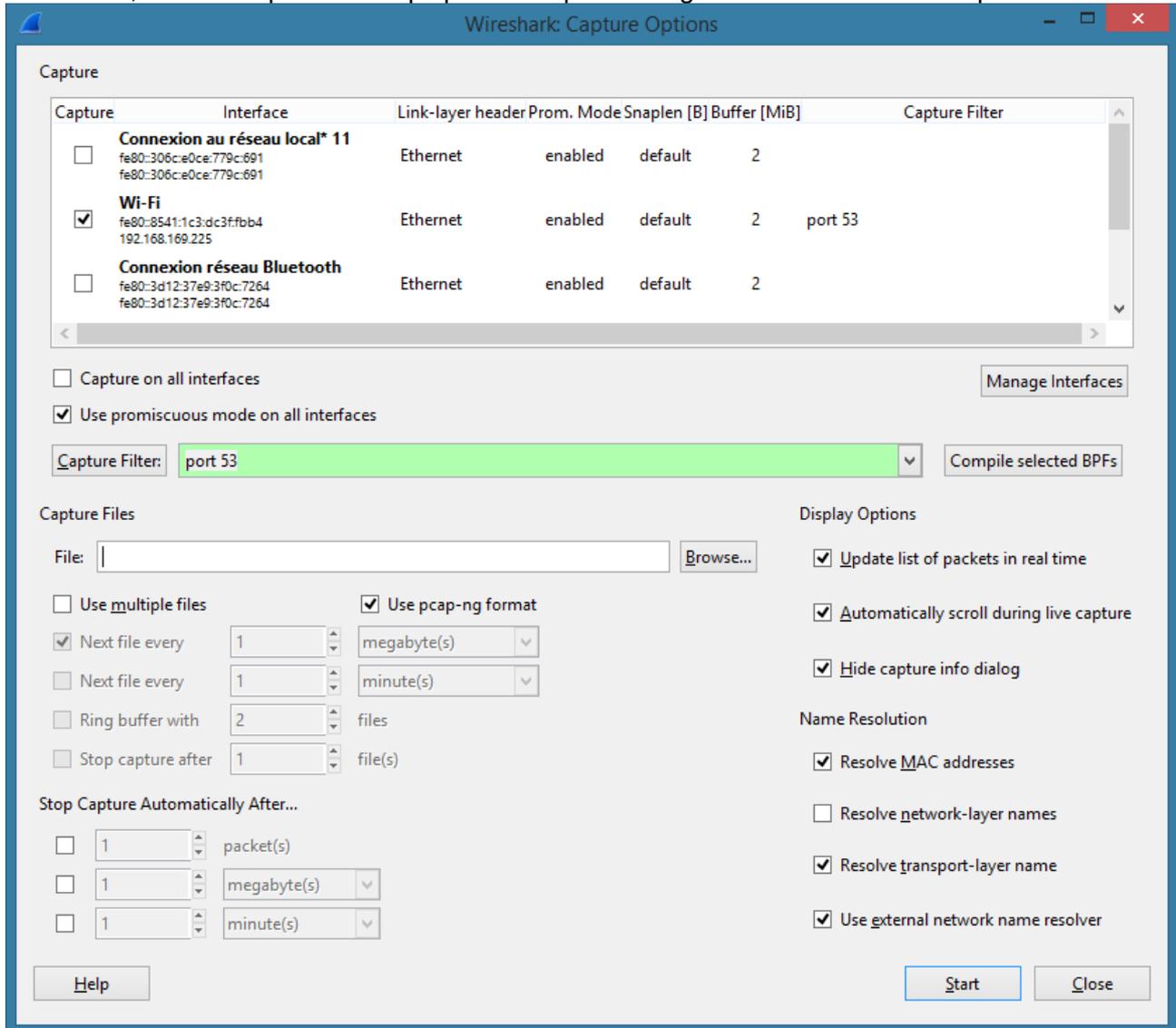
Commutateur Cisco : en mode config, taper la commande "monitor session 1 source..." puis "monitor session 1 destination ..."

Pour faire une **capture automatisée**, il faut cliquer sur l'icône "Show capture options..." ou dans le menu, choisir [Capture] [Options...] ou encore utiliser le raccourci-clavier [CTRL+K]



Guide d'utilisation de l'analyseur réseau Wireshark

Par défaut, l'interface présente la plupart des options en grisées car elles ne sont pas actives :



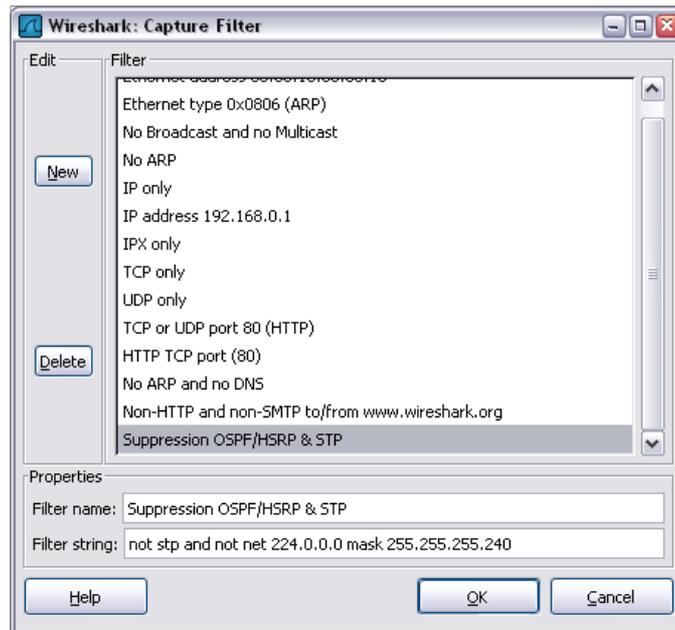
Il est primordial que la capture se fasse en mode « promiscuous ». D'autre part, si le poste n'est pas très puissant, il est préférable de désactiver la case « Update list of packets in real time ».

4.2.1 FILTRES DE CAPTURE

Il est possible de ne capturer qu'un certain type de flux. En activant ce filtre, seule les trames réseaux répondant aux critères du filtre seront enregistrées dans Wireshark. Par exemple, le filtre **port 53** permet de capturer seulement les paquets reçus et émis à destination du port TCP ou UDP 53 (ici, le protocole DNS). La couleur verte du champ indique que le filtre est valide.

Ce filtre est différent du filtre d'affichage (qui est utilisable après la capture).

Guide d'utilisation de l'analyseur réseau Wireshark

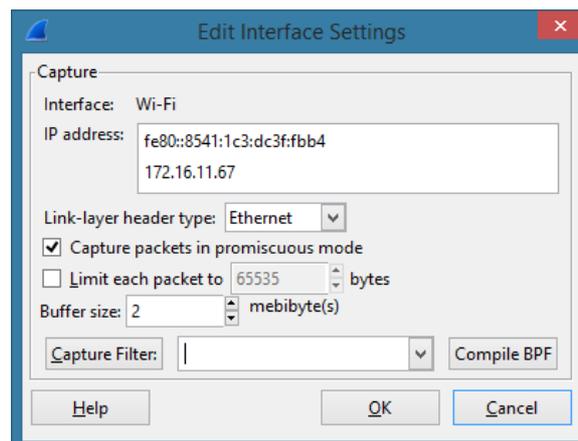


Il existe un certain nombre de filtres pré-définis (à titre d'exemple) mais il est tout à fait possible de créer les siens : la syntaxe autorise d'ailleurs l'utilisation de mots clés AND, OR, NOT...

4.2.2 LIMITATION DE LA TAILLE DES PAQUETS

L'analyse des trames se faisant généralement sur les premiers octets (les entêtes), il est utile de limiter la taille des paquets capturés à une taille maximum : pour cela, il suffit de cocher la case « Limit each packet to » et de choisir un nombre entre **60 octets** (minimum pour conserver l'entête TCP entier) et 512 (informations complémentaires pour des flux HTTP ou TNS par exemple). Cela n'a aucune influence sur les statistiques concernant les tailles de trames puisque cette information est inscrite dans l'entête des trames Ethernet.

Dans les nouvelles versions (1.8 et supérieure) de Wireshark, il faut double-cliquer sur l'interface et la boîte de dialogue suivante apparaît :



4.2.3 ARRÊT AUTOMATIQUE SUR SEUIL

Il est possible de limiter la capture sur 3 critères :

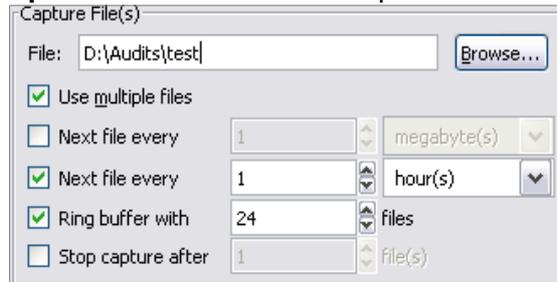
- Nombre de paquets,
- Taille de la capture,
- Délai dans le temps.

Guide d'utilisation de l'analyseur réseau Wireshark

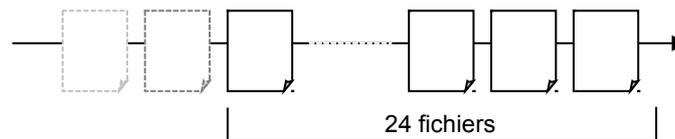
Ces trois critères peuvent être combinés. Cet arrêt automatique permet de limiter le travail d'analyse plus tard et de ne pas écraser un événement important.

4.2.4 CAPTURES CIRCULAIRES

C'est le mode le plus intéressant, surtout si la sonde dispose d'un espace disque suffisant. En effet, les problèmes réseaux sont souvent fugitifs et lorsqu'un incident survient, le temps d'activer une capture ne permet pas de trouver l'origine du problème. D'un autre côté, une capture linéaire permet de remonter dans l'historique des trames capturées mais la manipulation d'un fichier unique et souvent de **taille imposante et difficile**. La capture circulaire résout ces problèmes :



Dans l'exemple ci-dessus, Wireshark va créer 24 fichiers contenant chacun une heure de capture. Une fois la 24^{ème} heure écoulée, Wireshark va supprimer le premier fichier de la liste et va créer un nouveau fichier.



Avantages :

- Limiter le risque de dépassement de taille de disque,
- Conserver un historique sur 24 heures,
- Permettre la copie des fichiers intermédiaires (sauvegarde ou analyse sur autre poste),
- Localiser facilement un événement dans l'ensemble des fichiers.

Attention : la quantité de données capturées pouvant être très importante, il peut-être préférable de limiter chaque fichier à une taille comprise entre 5Mo et 20Mo afin de faciliter le travail d'analyse. En effet, l'utilisation des outils de Wireshark peut prendre beaucoup de temps sur un poste aux capacités limitées.

L'astuce pour déterminer le bon nombre de fichier pour effectuer la rotation est d'effectuer une première capture manuelle pour chronométrer combien de temps il faut pour remplir la taille choisie.

4.3 Captures à distance

Ce n'est pas uniquement lié à Wireshark mais aussi à WinPCAP dans les environnements Microsoft ou à l'utilisation de TShark via un tunnel SSH dans les environnements Linux.

4.3.1 ENVIRONNEMENT LINUX

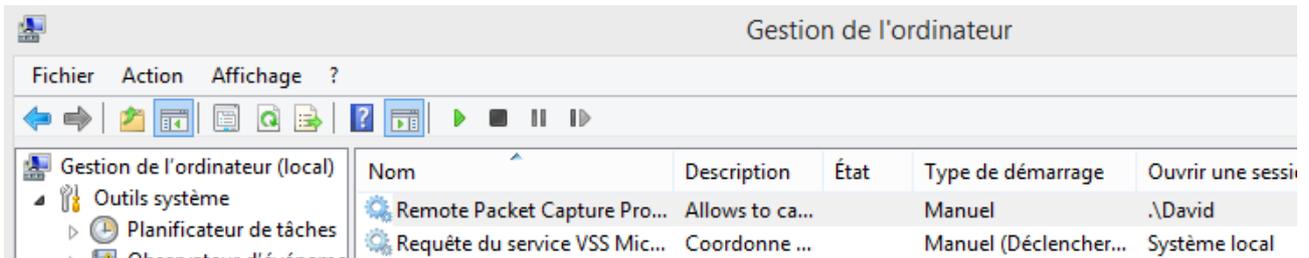
La ligne de commande suivante (à adapter en fonction des filtres attendus) :

```
ssh -l root <remote host> tshark -w - not not tcp port 22 | wireshark -k -i -
```

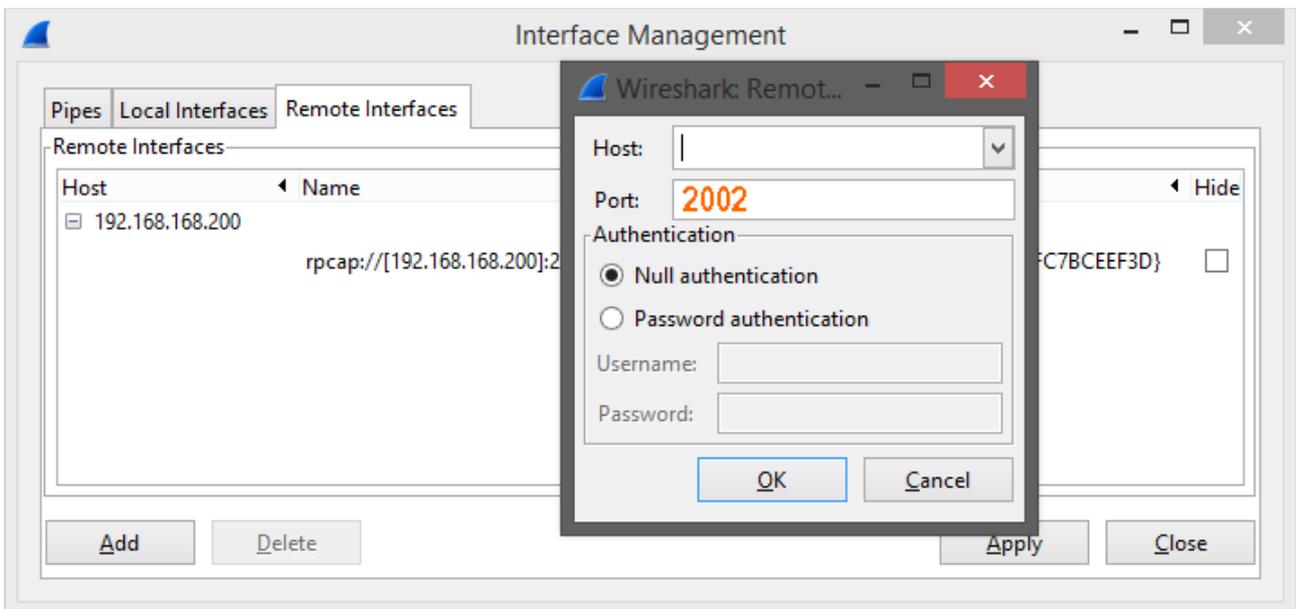
Guide d'utilisation de l'analyseur réseau Wireshark

4.3.2 ENVIRONNEMENT MICROSOFT

Sur la machine distante, il faut créer un compte de service pour l'utilisation de « Remote Packet Capture » puis démarrer le service.



Sur la machine locale, il faut déclarer la machine distante pour pouvoir accéder à ses interfaces. Cela se fait dans le menu [Capture] [Options...] (icône ) Cliquer sur le bouton [Manage Interfaces] et choisir l'onglet « Remote Interfaces » puis cliquer sur le bouton [Add]. Il faut alors saisir les paramètres de la boîte de dialogue (notamment choisir le port 2002 et cocher la case radio « Password Authentication »)



L'interface distante est désormais visible dans la boîte de dialogue habituelle.

4.4 Capture sur plusieurs interfaces

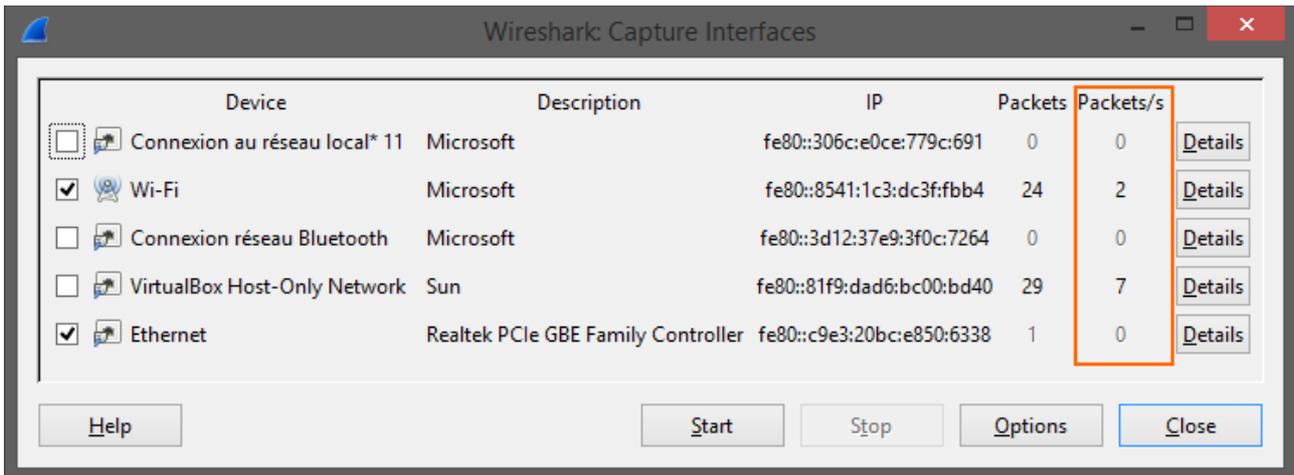
Les dernières versions de Wireshark permettent de capturer simultanément plusieurs interfaces : l'intérêt est de pouvoir tracer les flux en relation avec un service réseau d'une machine quelque soit son origine.

Les serveurs ont généralement plusieurs interfaces (parfois dédiés à la sauvegarde ou au NAS) mais aussi les postes de travail portable (Ethernet et Wi-Fi par exemple).

Pour cela, il suffit de sélectionner les interfaces à utiliser, dans le menu [Capture] [Interfaces...] ou bien en cliquant sur l'icône : 

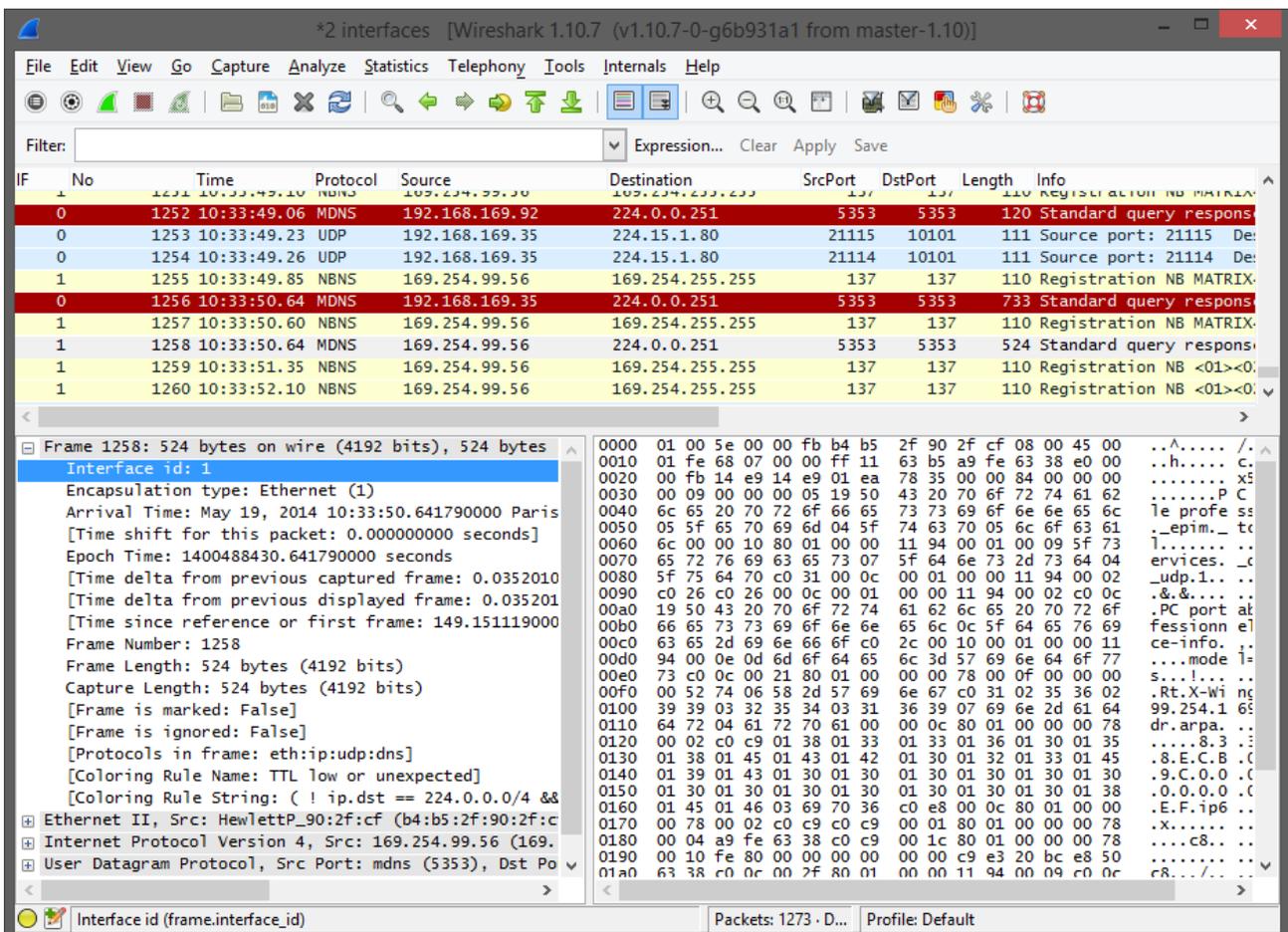
Ensuite il faut cocher les interfaces actives : la colonne de droite montre le nombre de paquets vus par seconde :

Guide d'utilisation de l'analyseur réseau Wireshark



La lecture nécessite une petite manipulation pour créer une colonne affichant l'interface d'origine :

1. Déplier la couche physique dans la fenêtre « Packet Details »
2. Sélectionner le premier champ « Interface ID : »
3. Clic droit, choisir « Apply as Column »



5. ANALYSES

Une fois les captures effectuées, il est possible de faire le travail d'analyse. C'est la partie la plus complexe mais si les options de captures ont été judicieusement utilisées, ce travail ne sera pas trop long.

5.1 Lecture des trames

L'affichage de Wireshark se décompose en fenêtre qu'il est possible de redimensionner :

5.1.1 FENÊTRE DE RÉSUMÉ

Dans cette fenêtre, Wireshark affiche un résumé des informations : adresses (niveau 3 ou par défaut niveau 2), estampillage horaire, protocole et description succincte. La coloration permet de retrouver rapidement certains protocoles (broadcast, requêtes ARP, etc.) et elle est personnalisable dans le menu [View] [Coloring Rules...].

No. -	Time	Source	Destination	Protocol	Info
1557	2006-11-29 19:31:55.793332	00:09:6b:b0:da:be	ff:ff:ff:ff:ff:ff	Intel A	Sequence: 3351399424, Sender ID 256, Tear
1558	2006-11-29 19:31:55.835471	00:0b:db:8d:7d:11	ff:ff:ff:ff:ff:ff	ARP	Who has 10.196.22.67? Tell 10.196.23.23
1559	2006-11-29 19:31:56.196238	00:80:f4:00:64:07	00:80:f4:00:65:20	LLC	U, func=UI; DSAP 0x24 Individual, SSAP 0x
1560	2006-11-29 19:31:56.851720	00000000.000400222ed5	00000000.ffffffffffff	IPX SAP	General Response
1561	2006-11-29 19:31:56.852212	00000000.000400222ed5	00000000.ffffffffffff	IPX SAP	General Response
1562	2006-11-29 19:31:56.852648	00000000.000400222ed5	00000000.ffffffffffff	IPX SAP	General Response
1563	2006-11-29 19:31:56.853059	00000000.000400222ed5	00000000.ffffffffffff	IPX SAP	General Response
1564	2006-11-29 19:31:56.862636	00:09:6b:b0:da:be	ff:ff:ff:ff:ff:ff	Intel A	Sequence: 3368176640, Sender ID 256, Tear
1565	2006-11-29 19:31:57.317178	00:80:f4:00:64:05	00:80:f4:00:03:10	LLC	U, func=UI; DSAP 0x24 Individual, SSAP 0x
1566	2006-11-29 19:31:57.925888	00:09:6b:b0:da:be	ff:ff:ff:ff:ff:ff	Intel A	Sequence: 3384953856, Sender ID 256, Tear
1567	2006-11-29 19:31:57.943504	10.196.22.86	10.196.22.54	TCP	[TCP Retransmission] 2733 > 502 [PSH, ACK]
1568	2006-11-29 19:31:57.947756	00:80:f4:00:65:17	ff:ff:ff:ff:ff:ff	ARP	Who has 10.196.22.86? Tell 10.196.22.54
1569	2006-11-29 19:31:57.947915	00:16:35:75:0e:4e	00:80:f4:00:65:17	ARP	10.196.22.86 1s at 00:16:35:75:0e:4e
1570	2006-11-29 19:31:57.951050	10.196.22.54	10.196.22.86	TCP	502 > 2733 [RST] Seq=74468 Len=0
1571	2006-11-29 19:31:58.145842	10.196.22.86	10.196.22.54	TCP	2735 > 502 [SYN] Seq=0 Len=0 MSS=1460
1572	2006-11-29 19:31:58.149970	10.196.22.54	10.196.22.86	TCP	502 > 2735 [SYN, ACK] Seq=0 Ack=1 Win=4096
1573	2006-11-29 19:31:58.150164	10.196.22.86	10.196.22.54	TCP	2735 > 502 [ACK] Seq=1 Ack=1 Win=17520 Len=0
1574	2006-11-29 19:31:58.150412	10.196.22.86	10.196.22.54	TCP	2735 > 502 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=0
1575	2006-11-29 19:31:58.180560	10.196.22.54	10.196.22.86	TCP	502 > 2735 [PSH, ACK] Seq=1 Ack=29 Win=4096
1576	2006-11-29 19:31:58.181673	10.196.22.86	10.196.22.54	TCP	2735 > 502 [PSH, ACK] Seq=29 Ack=20 Win=0
1577	2006-11-29 19:31:58.231942	10.196.22.54	10.196.22.86	TCP	502 > 2735 [PSH, ACK] Seq=20 Ack=57 Win=0

A partir de cette vue, il est possible de marquer des paquets : menu [Edit] [Mark packet (toggle)] ou séquence clavier [CTRL]+[M]. Cela permet lors d'une sauvegarde ou d'un export de limiter le nombre de trames sauvegardés.

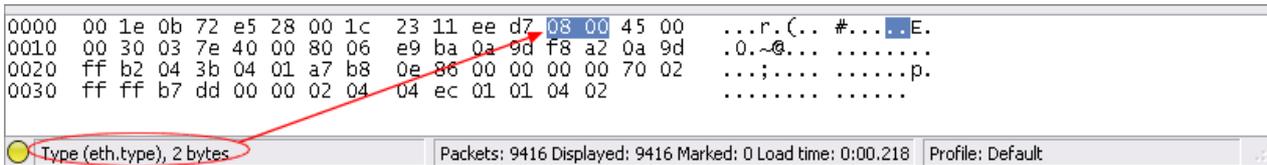
5.1.2 FENÊTRE D'ARBORESCENCE DE PROTOCOLE

Cette fenêtre détaille le paquet sélectionné dans la fenêtre de résumé : la trame est décomposée de manière hiérarchique, du plus bas niveau (frame) jusqu'au niveau du protocole le plus élevé connu par Wireshark.

+	Frame 1 (80 bytes on wire, 80 bytes captured)
-	Ethernet II, Src: 00:16:35:75:0e:4e (00:16:35:75:0e:4e), Dst: 00:80:f4:00:65:17 (00:80:f4:00:65:17)
+	Destination: 00:80:f4:00:65:17 (00:80:f4:00:65:17)
+	Source: 00:16:35:75:0e:4e (00:16:35:75:0e:4e)
	Type: IP (0x0800)
+	Internet Protocol, Src: 10.196.22.86 (10.196.22.86), Dst: 10.196.22.54 (10.196.22.54)
+	Transmission Control Protocol, Src Port: 2733 (2733), Dst Port: 502 (502), Seq: 0, Ack: 0, Len: 26
	Data (26 bytes)

5.1.3 FENÊTRE DE VUE DES DONNÉES

Cette fenêtre affiche les données brutes : chaque champ sélectionné dans la fenêtre d'arborescence de protocole et indiqué en inverse vidéo dans cette fenêtre. L'inverse est possible aussi. De plus, la barre d'état affiche également le type de donnée sélectionnée.



alertes (menu [Analyze] [Expert Info Composite]. BLEU = Chats, JAUNE = Warning, ROUGE = Errors

5.1.4 RÉGLAGES UTILES

Pour améliorer la lisibilité des trames dans la vue de résumé, voici deux réglages intéressants :

5.1.4.1 Affichage horaire

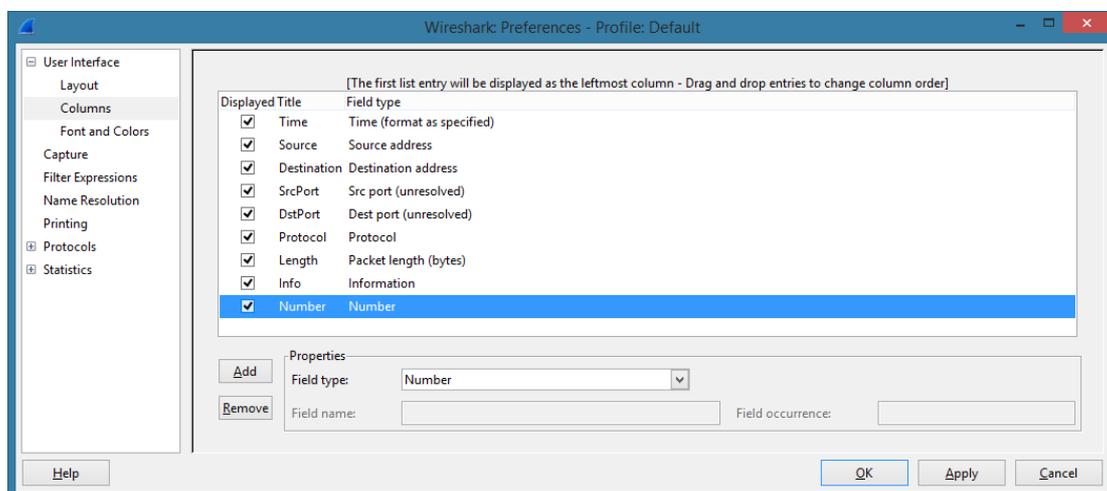
Dans le menu [View] [Time Display Format], choisir la représentation temporelle la plus pratique :

- **Time Of Day (CTRL+ Alt + 2)** permet un estampillage horaire permettant de comparer l'heure d'arrivée d'une trame avec un événement lié (appui d'un bouton, trame d'alerte SNMP, etc.)
- **Second Since beginning of Capture (CTRL + Alt + 3)** permet de mesurer le temps depuis le démarrage de la capture. L'affichage dans la colonne time est moins large, permettant ainsi de se positionner plus facilement dans les trames.
- **Second since Previous...** affiche le délai entre les trames : cette représentation est utile pour mesurer le délai de réponse à une trame ou lors d'échange de flux (calcul de latence).

Dans ce même menu, il est intéressant de limiter le nombre de décimales affichées (une résolution au centième de seconde sera généralement suffisant) pour limiter la largeur de la colonne « Time ».

5.1.4.2 Choix des colonnes

Dans le menu [Preferences], choisir l'onglet « Columns » ajouter les colonnes « Src Port » et « Dest Port »

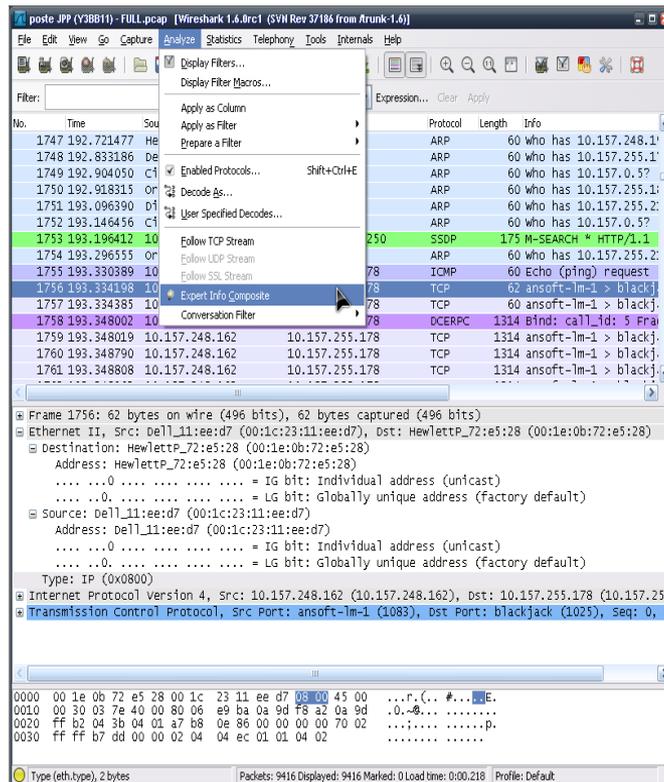


5.2 Analyse rapide

Pour obtenir rapidement des indications concernant les erreurs dans la capture, il faut utiliser le module expert.

5.2.1 EXPERT INFO COMPOSITE

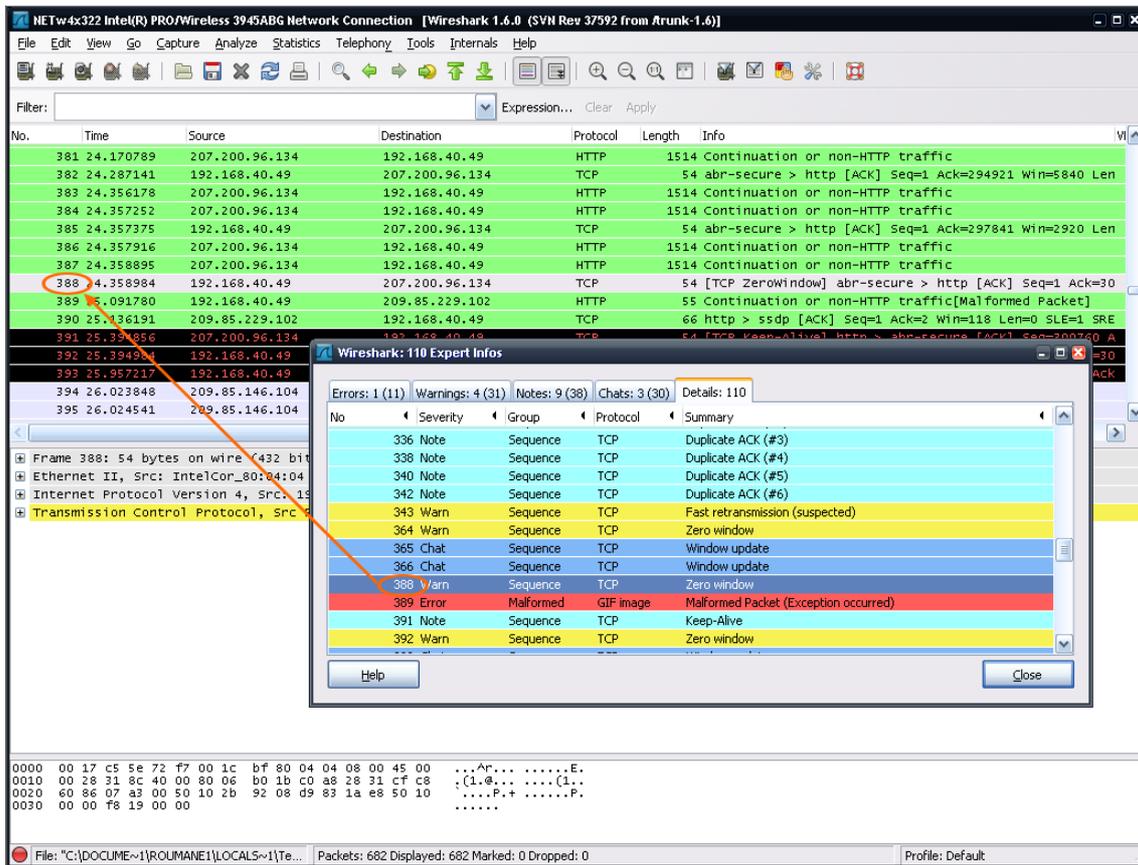
Ce module est accessible via le menu [Analyze] [Expert Info Composite]. Il permet une analyse rapide (bien que ce soit l'analyse la plus complexe).



Chaque trame va être analysée et les drapeaux (flags) ainsi que les numéros de séquences seront suivis. Le résultat est trié en 5 catégories :

- **ERRORS** : les problèmes réels comme des pertes de données. L'impact est donc visible.
- **WARNINGS** : les problèmes potentiels comme les trames malformées ou les BER.
- **NOTES** : les problèmes légers comme les retransmissions suspectées
- **CHAT** : le suivi des sessions (SYNchronisation, ReSeT, etc.)
- **Details** : est une vue des 4 catégories précédentes permettant de trier les données par type.

Guide d'utilisation de l'analyseur réseau Wireshark



En cliquant sur une erreur, le module affiche la trame dans le programme principal.

Attention : les onglets du module d'analyse expert indiquent le nombre de types d'erreurs reconnus. En cliquant sur l'onglet, chaque type d'erreur est affiché de manière condensée : il suffit d'explorer l'arborescence pour pouvoir afficher les trames.

Attention : le module d'analyse est une aide précieuse mais il ne permet pas un diagnostic à 100%. J'ai eu dans certains cas (protocole TNS d'Oracle) des messages « TNS unreassembled packets » qui étaient finalement dus à la multiplicité de requêtes simultanées : Wireshark n'est pas capable de différencier les différentes requêtes.

Parfois, Wireshark affiche un résultat erroné ou considère presque toutes les trames en erreurs. Le cas le plus classique est celui de l'erreur « Bad Checksum IPv4 ». Dans ce cas, il est utile de vérifier que l'interface Ethernet matériel est correctement configurée et éventuellement, désactiver l'option « Checksum offloading ».

D'autres outils permettent l'analyse des protocoles utilisés et les temps de réponses ou bande passante.

5.2.2 FILTRES D'AFFICHAGE

Wireshark permet de filtrer en temps réel l'affichage des trames. Cela peut être utile pour n'afficher que les flux en provenance d'une machine, suivre les échanges d'une machine en particulier ou lire les informations d'un protocole en particulier.

Guide d'utilisation de l'analyseur réseau Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
3884	312.129378	10.157.248.162	10.157.255.179	NSPI	154	NspiBind requ
3887	312.320258	10.157.248.162	10.157.255.179	TCP	60	trim > blackj
4044	320.989137	10.157.248.162	10.157.255.179	NSPI	202	NspiDNToEph r
4045	321.003297	10.157.248.162	10.157.255.179	NSPI	186	NspiGetProps
4046	321.005631	10.157.248.162	10.157.255.179	NSPI	282	NspiGetProps

L'expression est valide lorsque le champ est coloré en vert. Exemples de filtres classiques :

ip.addr == a.b.c.d	Afficher l'ensemble des flux de/vers l'adresse IP a.b.c.d (ou nom FQDN)
ip.addr == a.b.c.d/r	Il est également possible de fournir une plage IP (notation /24 par exemple)
ip.addr != a.b.c.d	Afficher toutes les trames sauf celles de/vers a.b.c.d
ip.src eq a.b.c.d ip.dst gt a.b.c.d	Autres variantes : ip.src et ip.dest pour choisir le sens du flux et eq, ne, gt...
tcp.port == nnnn	Afficher les trames correspondantes au protocole TCP n°nnnn

Mots clés :

Eq	,	==	Equal
Ne	,	!=	Not Equal
Gt	,	>	Greater Than
Lt	,	<	Less Than
Ge	,	>=	Greater than or Equal to
Le	,	<=	Less than or Equal to

Il y a aussi des filtres rapides :

Pour afficher tous les flux SSL, il est possible de taper directement 'SSL' dans la barre de saisie du filtre.

No.	Time	Source	Destination	Protocol	Length	Info
3	3.546412	192.168.40.49	195.47.241.4	SSL	302	Continuation Data
7	5.521439	192.168.40.49	195.47.241.4	SSL	302	Continuation Data
9	5.796824	192.168.40.49	195.47.241.4	SSL	206	Continuation Data

ssl	Flux de navigation sécurisé HTTPS ou SSL
dns	Requête de résolution de nom (DNS, port 53 UDP et TCP)
http	Flux de navigation (port 80 TCP)
imap	Flux de messagerie (port 143 TCP)
arp	Requête ARP (protocole de résolution d'adresse, couche 2 du modèle OSI)
stp	Protocole Spanning-Tree (protocole de niveau 2 pour les commutateurs)
...	

Certains protocoles nécessitent un peu plus de connaissance : n'afficher que les trames DHCP sur une capture, implique de savoir que DHCP est une option de BOOTP. Le filtre s'exprime comme suit :

bootp.option.type == 53

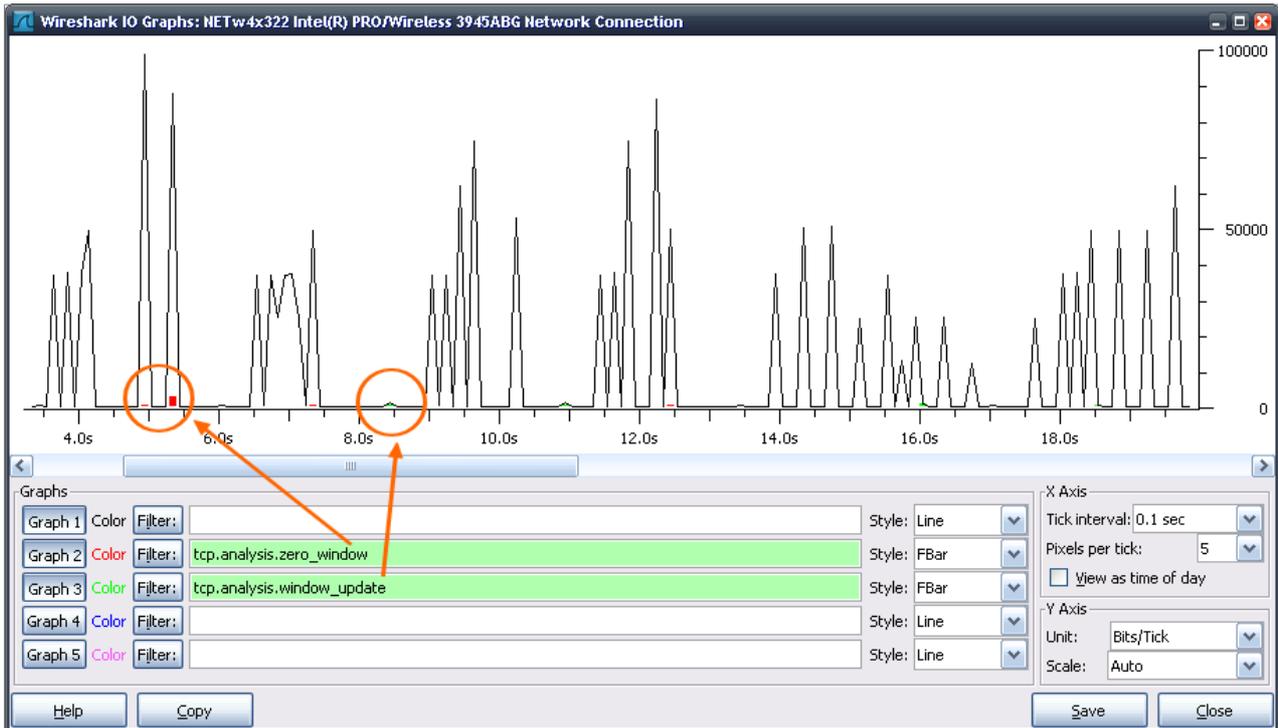
5.2.3 FILTRES D'AFFICHAGE SUR LE GRAPHEUR

Les filtres précédemment vus, sont également utilisables dans la fenêtre d'analyse graphique.

Pour y accéder, il suffit de ce rendre dans le menu [Statistics] [IO Graph].

Pour retrouver un débit en bits, il est préférable de modifier l'unité de l'échelle de l'axe Y (Y Axis).

- En cochant le bouton [GraphX] on active la couleur de graphique voulue
- En cliquant sur le bouton [Filter:] d'une ligne, on peut sélectionner un filtre existant
- En choisissant le style « Line », « Dot », « FBar », les événements s'affiche sous forme de lignes continues, de point ou de lignes verticales



Il est ainsi possible de mettre en relation un changement de débit avec un buffer mémoire saturé (gestion de congestion), des problèmes de retransmission ou d'autres messages d'erreurs.

tcp.analysis.zero_window	Trame de gestion de congestion (zero window)
tcp.analysis.duplicate_ack	Trame de gestion de retransmission
expert.message	Trame correspondante à une alerte dans le système expert composite de Wireshark
...	

5.3 Analyse normale

La qualification d'un réseau nécessite de pouvoir déterminer l'utilisation de celui-ci. Cela inclut l'utilisation de la bande passante, les protocoles présents ainsi que leur proportion, les temps de latence, la répartition des tailles de paquets, etc.

5.3.1 INFORMATIONS SUR LA CAPTURE

Wireshark affiche les informations sur le fichier de capture avec notamment le débit moyen lors de la capture. Pour cela, il faut aller dans le menu [Statistics] [Summary].

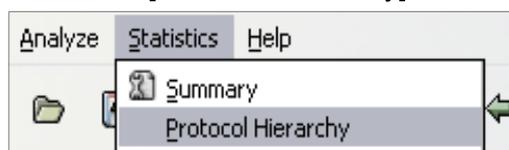


La durée de capture, ainsi que les dates de début et de fin sont indiquées de manière claire.

5.3.2 RÉPARTITION DES PROTOCOLES

Wireshark est capable de donner la répartition des protocoles sur une capture. Dans ce cas, plus la capture est grande, plus elle sera significative.

Dans le menu [Statistics], sélectionner [Protocol Hierarchy] :



Wireshark analyse alors l'ensemble des trames et fournit une table donnant le pourcentage d'utilisation sur le nombre totale de trame : ainsi le pourcentage de la sous-catégorie « Malformed Packet » sous « Transparent Network Substrate Protocol » se rapporte bien à la totalité des trames de la capture.

Guide d'utilisation de l'analyseur réseau Wireshark

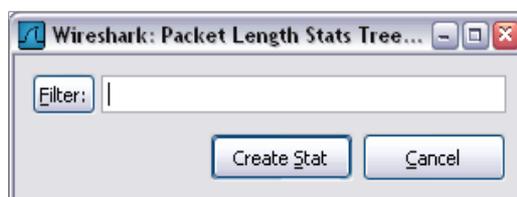
Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00 %	9416	100.00 %	948524	0.012	0	0	0.000
Ethernet	100.00 %	9416	100.00 %	948524	0.012	0	0	0.000
Address Resolution Protocol	59.57 %	5609	35.51 %	336806	0.004	5609	336806	0.004
Data	4.33 %	408	5.39 %	51160	0.001	408	51160	0.001
Logical-Link Control	30.03 %	1886	13.28 %	125959	0.002	0	0	0.000
Datagram Delivery Protocol	5.87 %	553	3.50 %	33180	0.000	0	0	0.000
Zone Information Protocol	5.87 %	553	3.50 %	33180	0.000	553	33180	0.000
Cisco Discovery Protocol	0.21 %	20	0.72 %	6855	0.000	20	6855	0.000
Spanning Tree Protocol	13.33 %	1255	8.36 %	79316	0.001	1255	79316	0.001
Dynamic Trunking Protocol	0.24 %	23	0.15 %	1426	0.000	23	1426	0.000
NetBIOS	0.18 %	17	0.32 %	3076	0.000	0	0	0.000
SMB (Server Message Block Protocol)	0.18 %	17	0.32 %	3076	0.000	0	0	0.000
SMB MailSlot Protocol	0.18 %	17	0.32 %	3076	0.000	0	0	0.000
Microsoft Windows Browser Protocol	0.18 %	17	0.32 %	3076	0.000	17	3076	0.000
VLAN Trunking Protocol	0.03 %	3	0.03 %	297	0.000	3	297	0.000
Internetnetwork Packet eXchange	0.15 %	14	0.17 %	1652	0.000	0	0	0.000
Service Advertisement Protocol	0.15 %	14	0.17 %	1652	0.000	14	1652	0.000
Data	0.01 %	1	0.02 %	157	0.000	1	157	0.000
DEC DNA Routing Protocol	1.43 %	135	0.85 %	8100	0.000	135	8100	0.000
Internet Protocol Version 4	13.22 %	1245	43.41 %	411721	0.005	0	0	0.000
User Datagram Protocol	5.56 %	524	7.11 %	67444	0.001	0	0	0.000
Data	3.30 %	311	2.44 %	23144	0.000	311	23144	0.000

👁 Il n'est – hélas – pas possible de copier les informations contenues dans cette fenêtre, ni même, les trier par colonnes.

5.3.3 RÉPARTITION DES TAILLES DE PAQUETS

Wireshark est capable d'afficher la répartition des paquets par taille. Dans le menu [Statistics], choisir [Packet Length...]

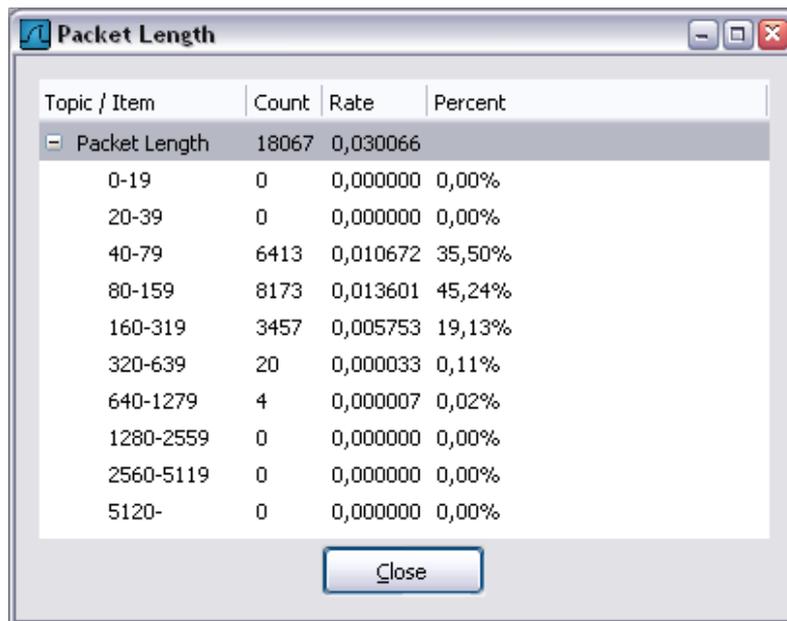
Une fenêtre s'affiche permettant de filtrer sur quels éléments la répartition doit être calculée : il n'est pas nécessaire de remplir le champ...



En cliquant sur le bouton [Create Stat], Wireshark ouvre une fenêtre contenant la répartition demandée par tranche.

👁 Comme pour la répartition hiérarchique de protocoles, il n'est – hélas – pas possible de copier les informations contenues dans cette fenêtre, ni même, les trier par colonnes.

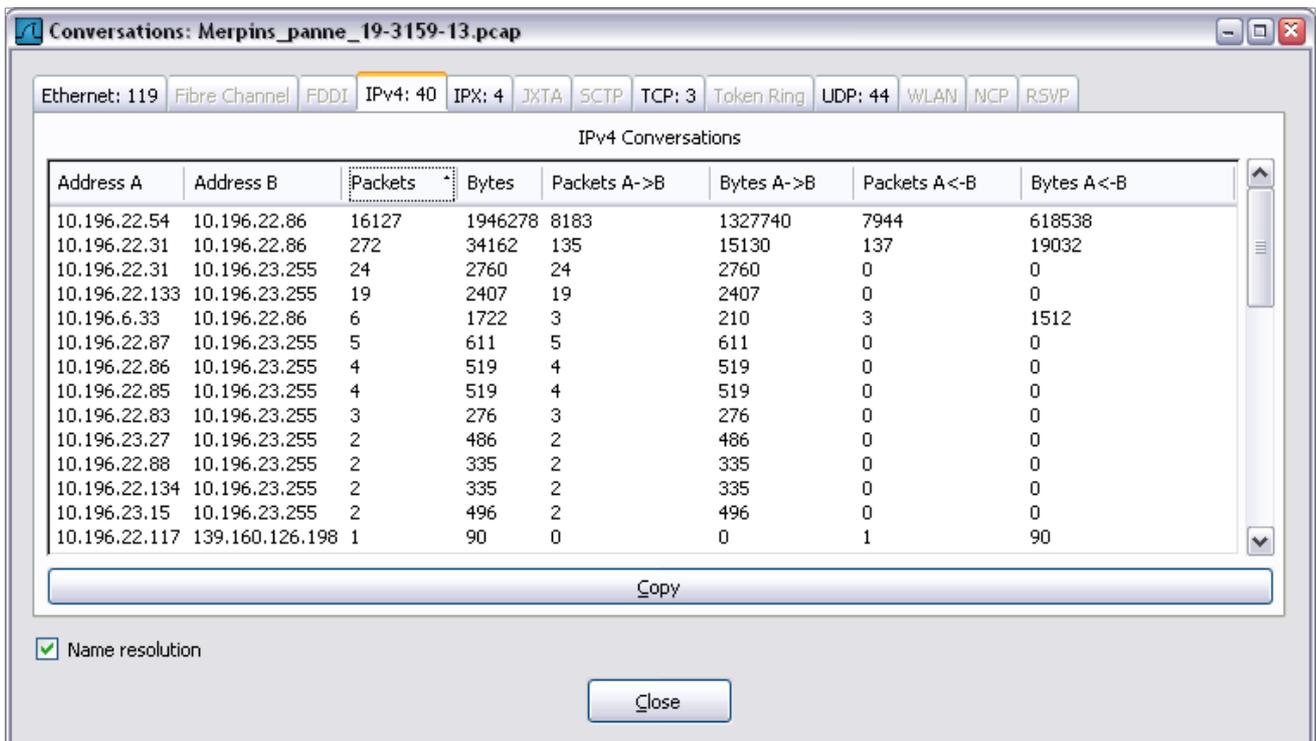
Guide d'utilisation de l'analyseur réseau Wireshark



Topic / Item	Count	Rate	Percent
Packet Length	18067	0,030066	
0-19	0	0,000000	0,00%
20-39	0	0,000000	0,00%
40-79	6413	0,010672	35,50%
80-159	8173	0,013601	45,24%
160-319	3457	0,005753	19,13%
320-639	20	0,000033	0,11%
640-1279	4	0,000007	0,02%
1280-2559	0	0,000000	0,00%
2560-5119	0	0,000000	0,00%
5120-	0	0,000000	0,00%

5.3.4 CONVERSATIONS

Wireshark est capable de montrer les conversations durant la capture, menu [Statistics] [Conversations].



Address A	Address B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B
10.196.22.54	10.196.22.86	16127	1946278	8183	1327740	7944	618538
10.196.22.31	10.196.22.86	272	34162	135	15130	137	19032
10.196.22.31	10.196.23.255	24	2760	24	2760	0	0
10.196.22.133	10.196.23.255	19	2407	19	2407	0	0
10.196.6.33	10.196.22.86	6	1722	3	210	3	1512
10.196.22.87	10.196.23.255	5	611	5	611	0	0
10.196.22.86	10.196.23.255	4	519	4	519	0	0
10.196.22.85	10.196.23.255	4	519	4	519	0	0
10.196.22.83	10.196.23.255	3	276	3	276	0	0
10.196.23.27	10.196.23.255	2	486	2	486	0	0
10.196.22.88	10.196.23.255	2	335	2	335	0	0
10.196.22.134	10.196.23.255	2	335	2	335	0	0
10.196.23.15	10.196.23.255	2	496	2	496	0	0
10.196.22.117	139.160.126.198	1	90	0	0	1	90

Les onglets permettent de choisir le type d'adressage (Ethernet, IPX, Ipv4) et même par protocoles (TCP ou UDP).

👁 Il est possible de trier les données par colonnes (en cliquant sur le titre de la colonne une fois ou deux fois pour changer l'ordre) et de copier le résultat dans le presse-papier (bouton [Copy]).

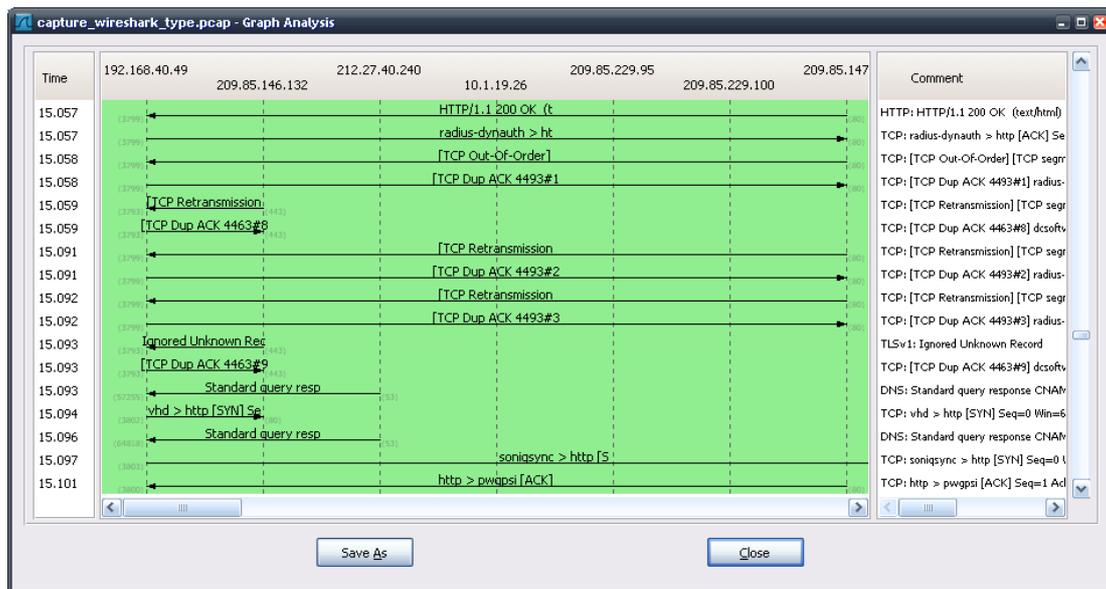
Guide d'utilisation de l'analyseur réseau Wireshark

👁 La troisième et la quatrième colonne (Packets et Bytes) sont respectivement la somme des colonnes 'Packets A->B + Packet B->A' et 'Bytes A->B + Bytes B-> A'.

5.4 Analyse graphique de flux

Cet outil permet d'afficher de manière graphique les échanges entre les différentes machines. Pour y accéder, il suffit de choisir dans le menu [Statistics] [Flow Graph...]

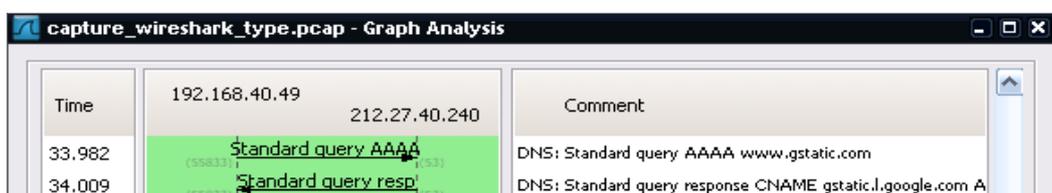
Un filtre s'affiche pour déterminer les options du graphique puis (après avoir cliqué sur [OK]) la fenêtre des flux s'ouvre.



L'échelle de temps est verticale (ascenseur à droite) tandis que les échanges sont affichés entre les machines de manière horizontale.

L'outil propose également une sauvegarde en mode texte (bouton [Save As])

L'intérêt de cet outil devient clair lorsqu'il est utilisé après un filtre. Il permet ainsi de lire les échanges dans le temps de manière pédagogique comme dans l'exemple ci-dessous pour une requête DNS :

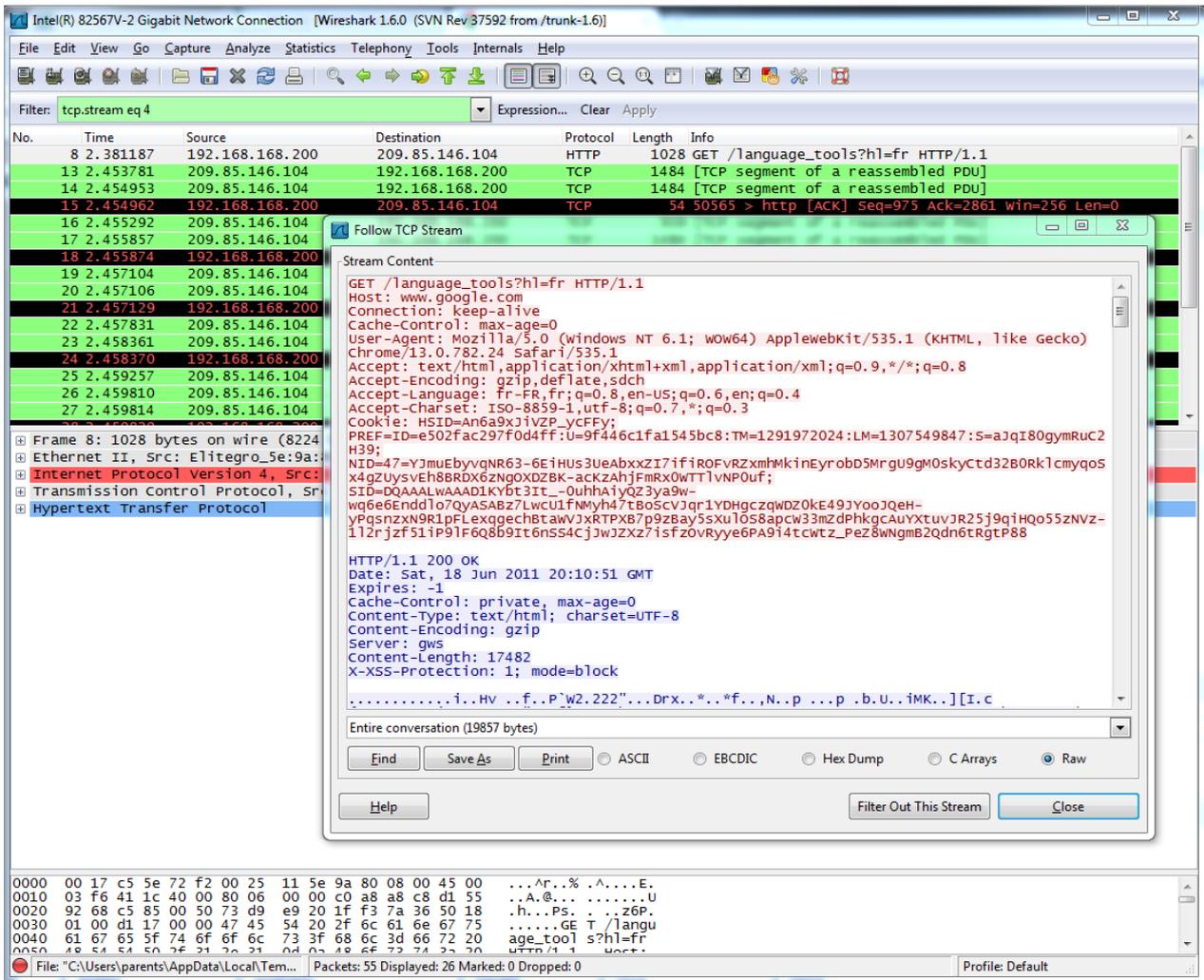


Les chiffres en grisés et entre parenthèses sur le graphique correspondent aux numéros de ports (UDP ou TCP).

5.5 Analyse texte d'un flux TCP ou UDP

Il existe une option qui permet de reconstituer un flux dans Wireshark. Cette option est particulièrement intéressante pour afficher un flux web au format HTTP par exemple.

Il faut d'abord cliquer sur une trame correspondante au flux à analyser. Ensuite, dans le menu [Analyse] choisir [Follow TCP stream].



Le flux apparaît avec deux couleurs :

- ▲ En **rouge** : le flux envoyé par le client vers le serveur
- ▲ En **bleu** : la réponse du serveur à la requête du client

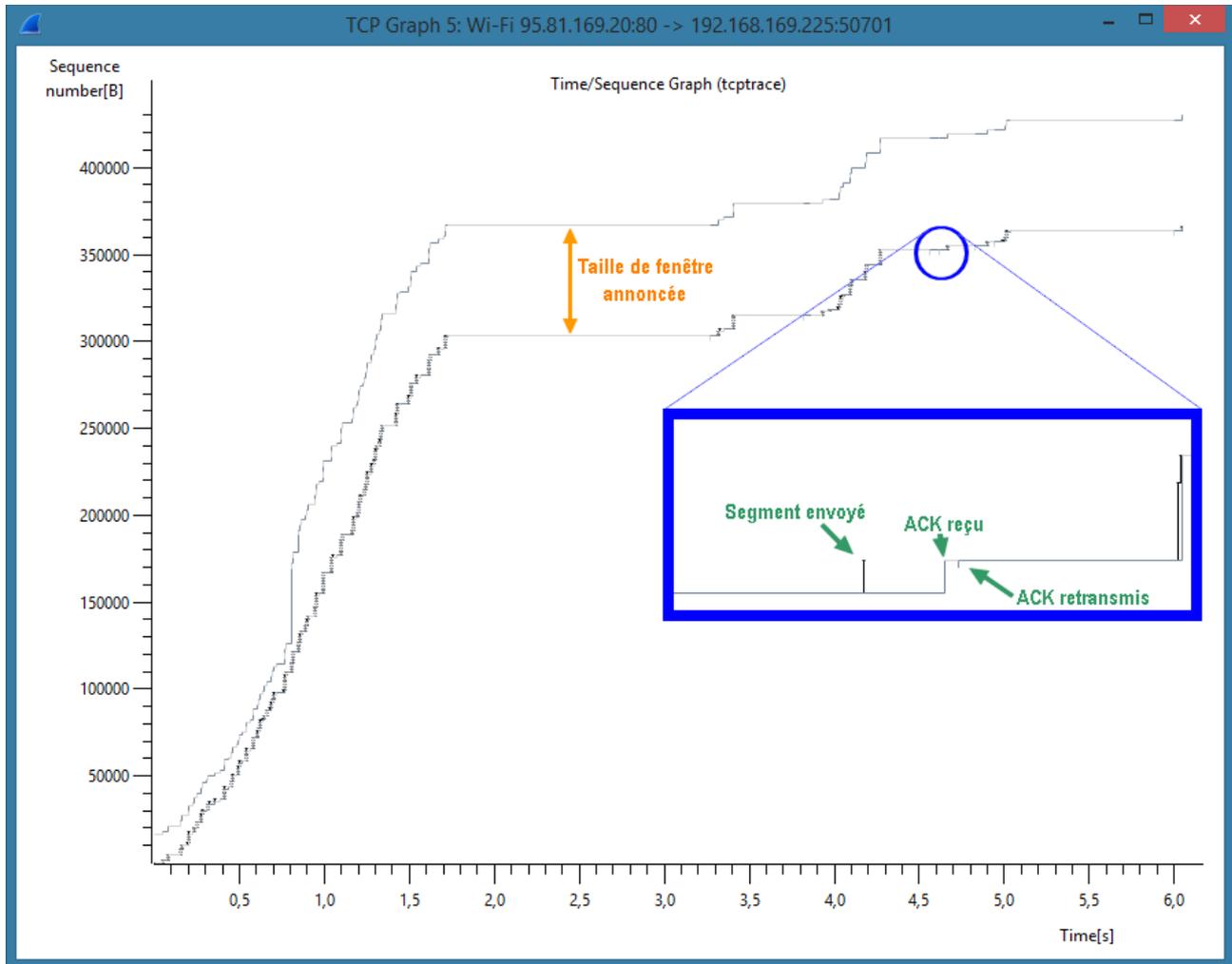
Grâce à cet outil, il est possible de lire quel navigateur web a été utilisé pour effectuer la requête (champ 'user-agent') ainsi que les options négociées.

En général, la réponse du serveur commence par 'HTTP/1.1 200 OK'.

A noter : la même option existe pour les flux UDP. Cliquer sur [Analyse] [Follow UDP stream]. Cela peut-être utilisé sur un flux SSDP ou DNS.

5.6 Analyse graphique "Time-Sequence" (tcptrace)

Cet outil graphique permet de voir rapidement la forme des échanges pour un flux sélectionné :



Ce graphe est une succession de traits noirs et de lignes bleues. Il est possible de zoomer dans ce graphe en cliquant sur le bouton du milieu de la souris. L'axe horizontal représente le temps tandis que l'axe vertical représente le numéro de séquence (en nombre relatif à la première trame).

Cette fonction est issue de l'outil tcptrace, disponible à l'adresse <http://www.tcptrace.org/> dont le fonctionnement est totalement décrit : l'outil s'avère cependant extrêmement complet et sa lecture reste difficile pour un néophyte.

Guide d'utilisation de l'analyseur réseau Wireshark

Il est possible de se déplacer dans le graphique ainsi que d'effectuer des zooms. Pour cela, il faut une souris avec 3 boutons, le bouton de milieu servant pour zoomer (en cliquant sur celui-ci). Le déplacement se fait en tenant le bouton droit de la souris enfoncée tout en déplaçant celle-ci.

En enfonçant la touche [CTRL] et en appuyant sur le bouton droit, une loupe apparaît, permettant de grossir une zone particulière du graphique.

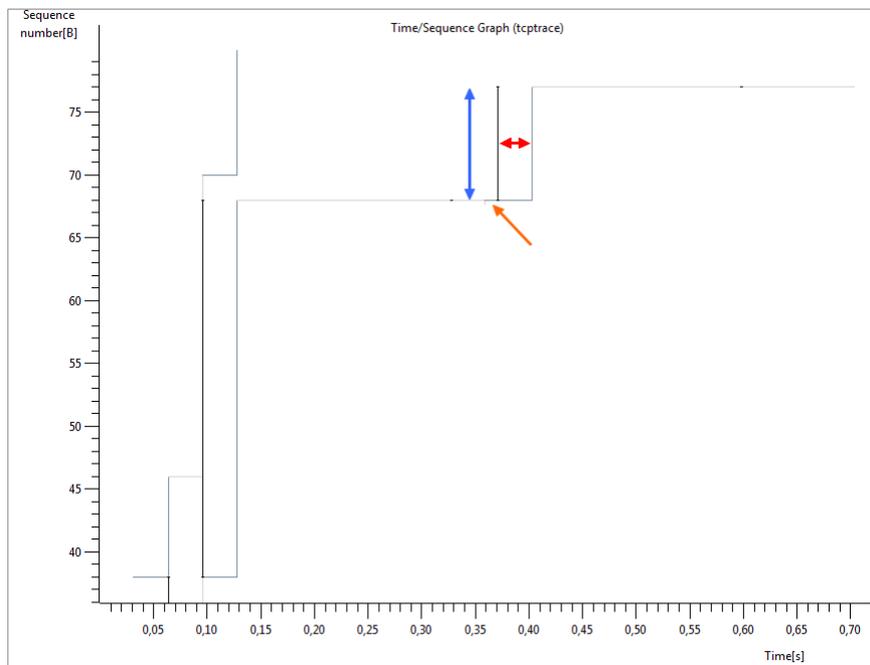
Enfin, les touches de raccourcis suivantes permettent les mêmes actions :

[CTRL] + [-] dézoomer

[CTRL] + [+] zoomer (sur les PC portables sans pavé numérique : [CTRL] + [Shift] + [+])

[Espace] permet de cliquer sur un segment graphique et de le retrouver dans la fenêtre principale des trames Wireshark.

Cette fonction est très complète et permet de suivre la conversation de manière graphique et ainsi de détecter des variations dans le temps ou des modifications de fenêtre.



La flèche **bleue** montre la hauteur du trait vertical noir (en forme de 'I') : il s'agit d'une trame envoyée (du premier au dernier octet, dont la hauteur représente l'écart du nombre de séquences).

La flèche **rouge** montre le temps écoulé entre l'émission des trames et la trame d'acquittement reçue.

La courbe la plus basse qui suit les traits verticaux noirs correspond à la réception des trames d'acquittement (ACK) du destinataire. La forme de la courbe ainsi constituée indique le débit : une courbe plutôt verticale montre un débit élevé tandis qu'une tendance horizontale montre un débit faible.

L'autre courbe bleue (au-dessus de la première courbe) correspond au mécanisme de fenêtre TCP (windows) : plus elle est haute, plus la quantité de trames à émettre avant un acquittement est importante.

6. DIAGNOSTIC

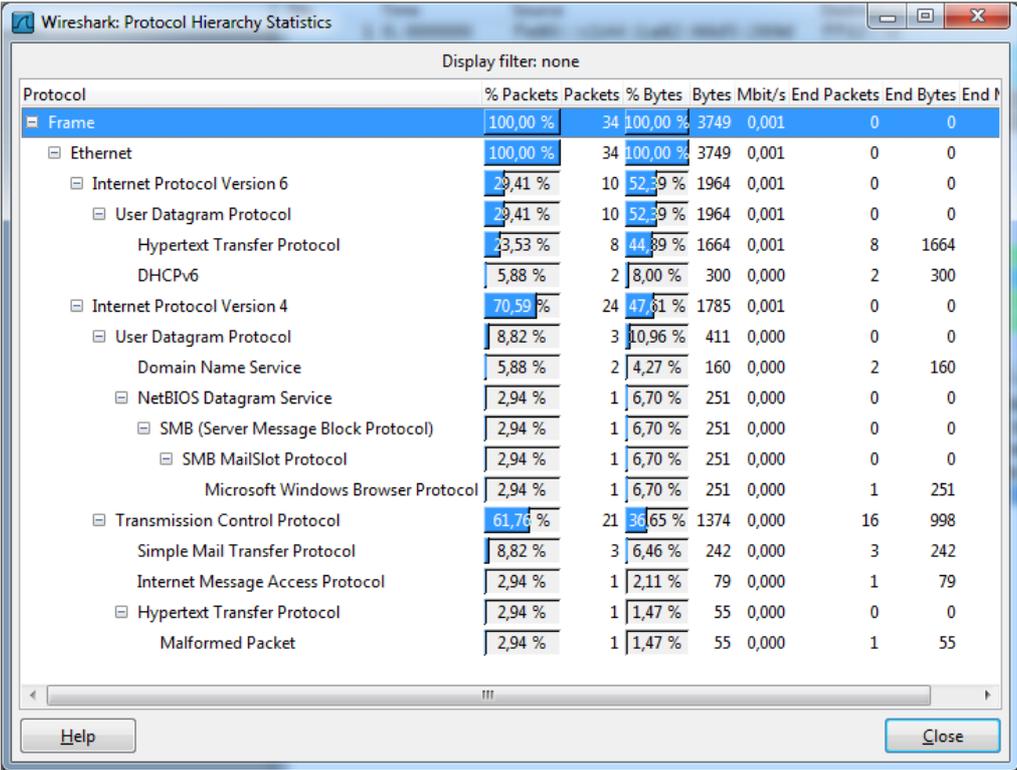
L'intérêt d'utiliser Wireshark est de faire de l'analyse réseau ou encore de l'audit : cet outil permet de contrôler les trames d'un flux et de les afficher.

Mais sans connaissance des protocoles affichés, les informations données par Wireshark ne sont pas facilement interprétables.

Cette partie est donc une aide au diagnostic, pour faciliter l'utilisation des nombreuses fonctions de Wireshark. Je n'ai pas la prétention de tout connaître et je souhaite rester humble : j'ai ajouté cette partie d'abord pour moi-même...

6.1 Type de protocoles

Depuis plusieurs années, le protocole IP s'est généralisé : il devrait donc être **rare** de rencontrer d'autres protocoles. Le passage par l'outil [Statistics] [Protocol Hierarchy] est donc une étape obligatoire :



Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End I
Frame	100,00 %	34	100,00 %	3749	0,001	0	0	
Ethernet	100,00 %	34	100,00 %	3749	0,001	0	0	
Internet Protocol Version 6	29,41 %	10	52,39 %	1964	0,001	0	0	
User Datagram Protocol	29,41 %	10	52,39 %	1964	0,001	0	0	
Hypertext Transfer Protocol	23,53 %	8	44,89 %	1664	0,001	8	1664	
DHCPv6	5,88 %	2	8,00 %	300	0,000	2	300	
Internet Protocol Version 4	70,59 %	24	47,61 %	1785	0,001	0	0	
User Datagram Protocol	8,82 %	3	10,96 %	411	0,000	0	0	
Domain Name Service	5,88 %	2	4,27 %	160	0,000	2	160	
NetBIOS Datagram Service	2,94 %	1	6,70 %	251	0,000	0	0	
SMB (Server Message Block Protocol)	2,94 %	1	6,70 %	251	0,000	0	0	
SMB MailSlot Protocol	2,94 %	1	6,70 %	251	0,000	0	0	
Microsoft Windows Browser Protocol	2,94 %	1	6,70 %	251	0,000	1	251	
Transmission Control Protocol	61,76 %	21	36,65 %	1374	0,000	16	998	
Simple Mail Transfer Protocol	8,82 %	3	6,46 %	242	0,000	3	242	
Internet Message Access Protocol	2,94 %	1	2,11 %	79	0,000	1	79	
Hypertext Transfer Protocol	2,94 %	1	1,47 %	55	0,000	0	0	
Malformed Packet	2,94 %	1	1,47 %	55	0,000	1	55	

Dans la figure ci-dessus, il n'y a que 2 protocoles majeurs présents : IPv6 et IPv4.

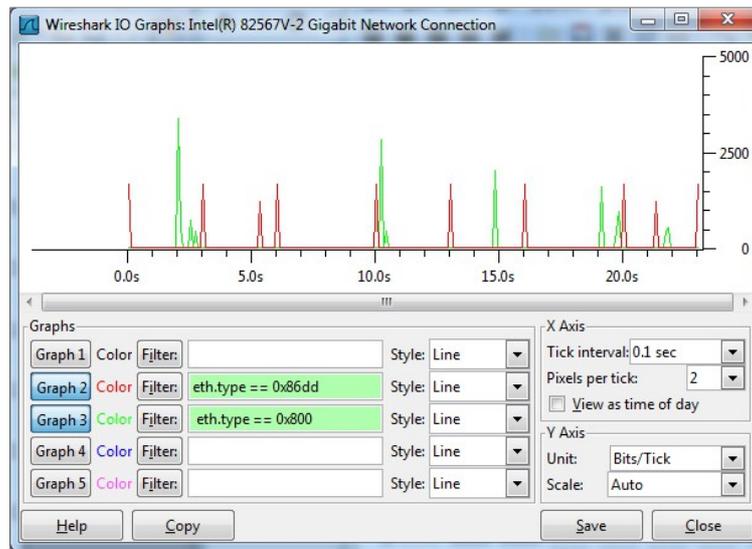
100% des trames capturées sont de type Ethernet :

- ⤴ 30% environ de type IPv6
- ⤴ 70% environ de type IPv4

Si le réseau audité ne fonctionne pas en IPv6, il y a une partie de la bande passante qui est utilisée de manière inutile.

Guide d'utilisation de l'analyseur réseau Wireshark

Il est également possible de contrôler le fonctionnement de ces protocoles avec l'outil [IO Graph] : les filtres sont alors basés sur le champ type de la trame Ethernet.



6.2 ARP

Le protocole ARP permet la résolution de l'adresse Ethernet une adresse IP. Généralement, une machine n'a qu'une seule adresse IP mais il y a des exceptions, notamment, le routeur (parfois nommé « passerelle par défaut »).

Il est donc fréquent lorsque les caches sont vides, de rencontrer deux trames ARP (demande et réponse).

Time	Protocol	Source	Destination	SrcPort	DstPort	Length	Info
11:02:42.26	ARP	HonHaiPr_a6:de:2d	Acrosser_15:e3:05			42	Who has 172.16.11.254? Tell 172.16.11.93
11:02:42.26	ARP	Acrosser_15:e3:05	HonHaiPr_a6:de:2d			56	172.16.11.254 is at 00:02:b6:15:e3:05

Il faut cependant surveiller que pour une même adresse IP, on ne trouve pas plusieurs adresses Ethernet, ce qui révélerait un problème (sécurité, duplication d'adresse IP, etc).

Wireshark est capable de vous montrer le cas d'une adresse dupliquée.

14:33:18.33	ARP	De11_8b:8f:43	Broadcast	60	Gratuitous ARP for 192.168.0.120 (Reply)
14:33:23.58	ARP	De11_8a:78:cb	Broadcast	60	Gratuitous ARP for 192.168.0.120 (Reply) (duplicate use of 192.168.0.120 detected!)

Le cas ci-dessus montre des requêtes ARP « gratuites » : ce type de requête est émise au démarrage d'un système afin de vérifier que son adresse IP n'est pas déjà utilisée.

6.3 Protocoles TCP ou UDP

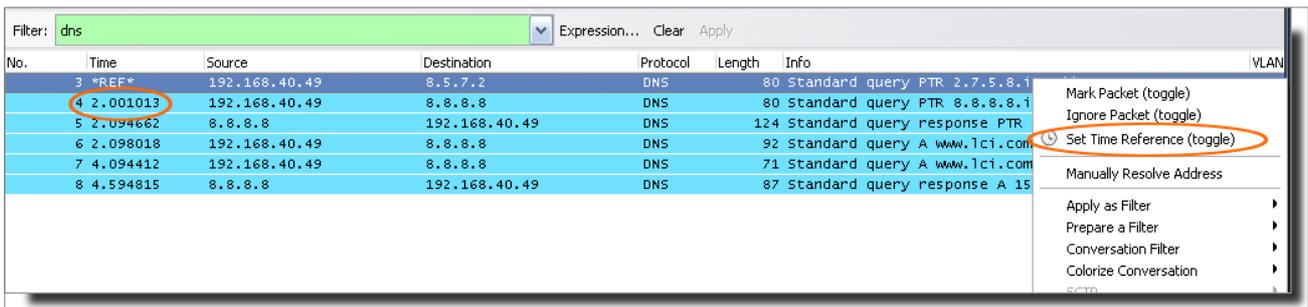
L'analyse de protocoles TCP ou UDP implique une bonne connaissance de leur fonctionnement... elle exige aussi une bonne connaissance de l'environnement dans lequel s'effectue l'analyse. Les performances réseaux dépendent également de la configuration des systèmes d'exploitation.

6.3.1 DNS

L'analyse des requêtes DNS permet de vérifier que les machines du réseau s'adressent au bon serveur DNS. En effet, un DNS externe peut répondre moins rapidement ou ne pas répondre sur les adresses locales. Un DNS inexistant ralentira les réponses au début de l'application : en effet, une fois le cache renseigné, la machine n'interroge plus le DNS.

Guide d'utilisation de l'analyseur réseau Wireshark

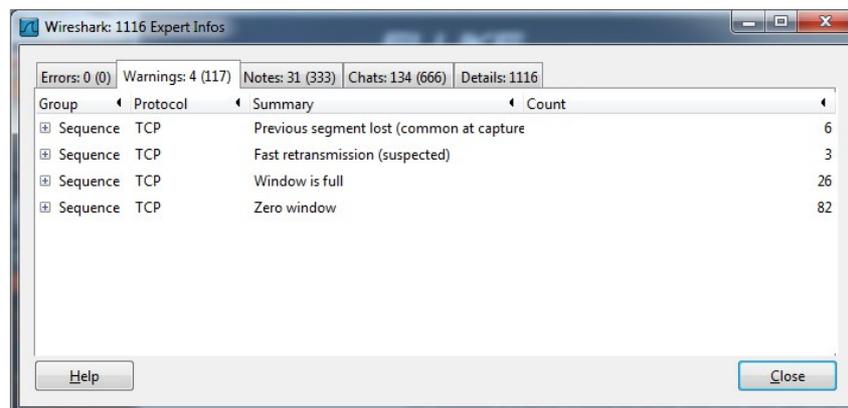
Un problème de performance uniquement au lancement d'une application doit faire suspecter un problème de DNS.



Dans cet exemple, la requête DNS part pour la destination 8.5.7.2... puis 2 secondes plus tard, la même requête est exécutée vers 8.8.8.8 qui répond presque instantanément. L'utilisation conjointe d'un filtre « DNS » ainsi que le marquage de la référence de temps sur la première requête (bouton droit sur la trame, choisir [Set the reference]) permet de mesurer le délai de réponse du serveur DNS.

6.4 Erreurs générales

Il existe plusieurs catégories d'erreurs et d'avertissements à surveiller. Pour cela, la première action est de lancer l'outil d'analyse [Analyze] [Expert Info Composite]



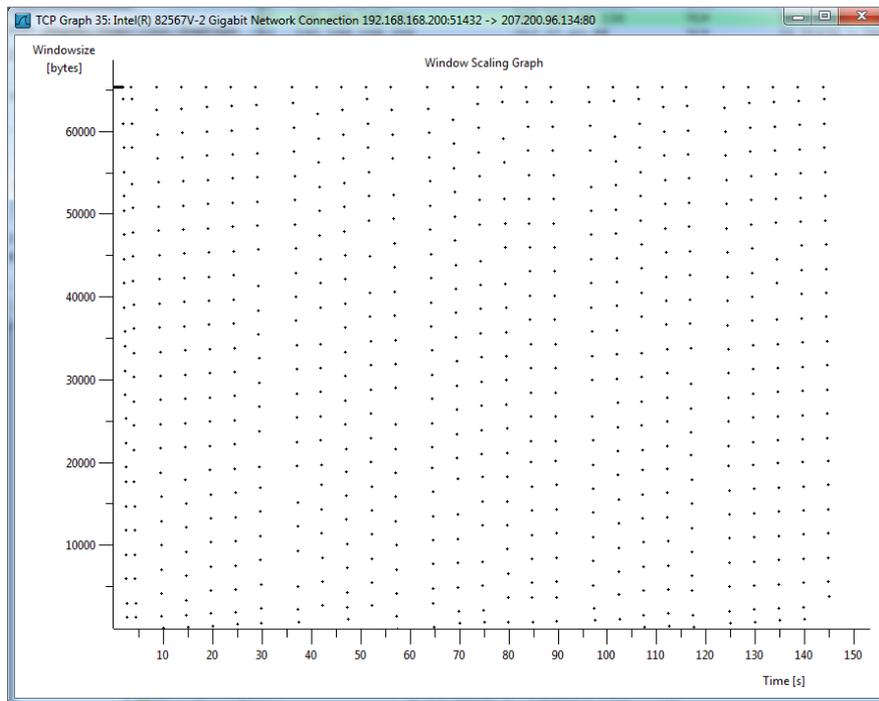
Les onglets sont classés de gauche (les erreurs les plus graves) à droite.

6.4.1 ZERO WINDOW

Ce type d'erreur signifie qu'une application sur la machine concernée est saturée et refuse de recevoir d'autres trames. Pour cela, elle réduit la fenêtre TCP à zéro.

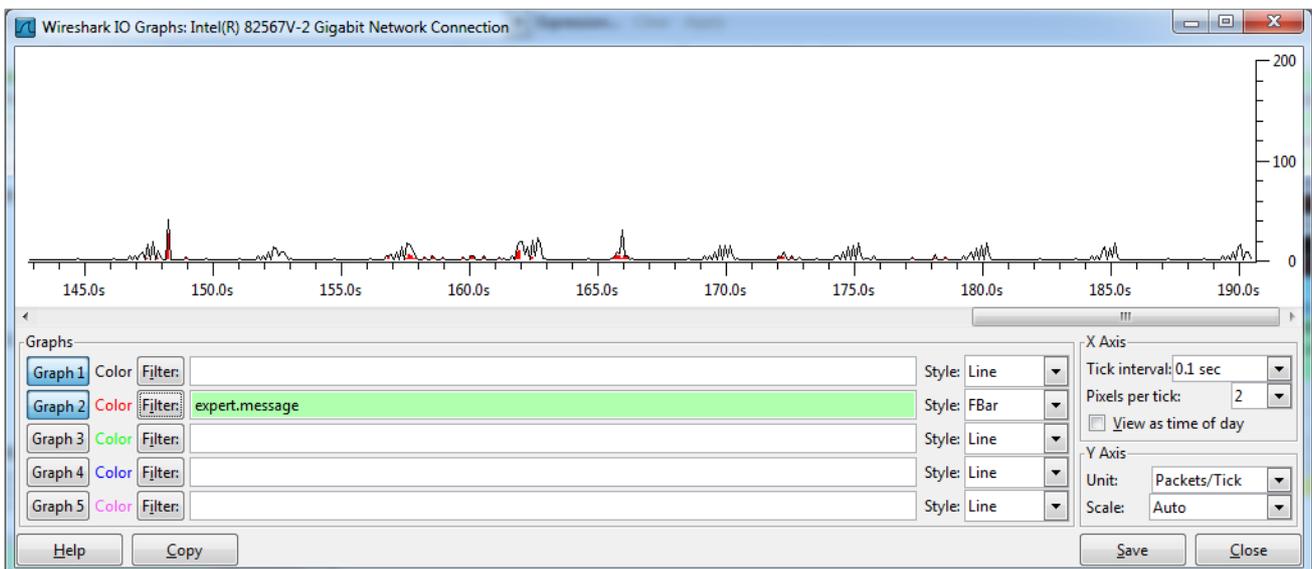
On peut également voir ce type de problème avec la fonction graphique [Statistics] [TCP stream graph] [Windows Scaling Graph] : en reliant les points verticalement on obtient une droite qui chute rapidement.

Guide d'utilisation de l'analyseur réseau Wireshark



Les raisons d'une erreur « Zero Window » sont multiples mais une surcharge de la machine émettrice est à envisager : trop de processus, CPU trop lente, application avec un buffer trop petit... ou parfois, certains programmes de streaming audio (type radio en ligne).

Un autre moyen d'analyser lorsque surviennent ces erreurs sont d'ajouter un filtre dans le module [IO Graph] :

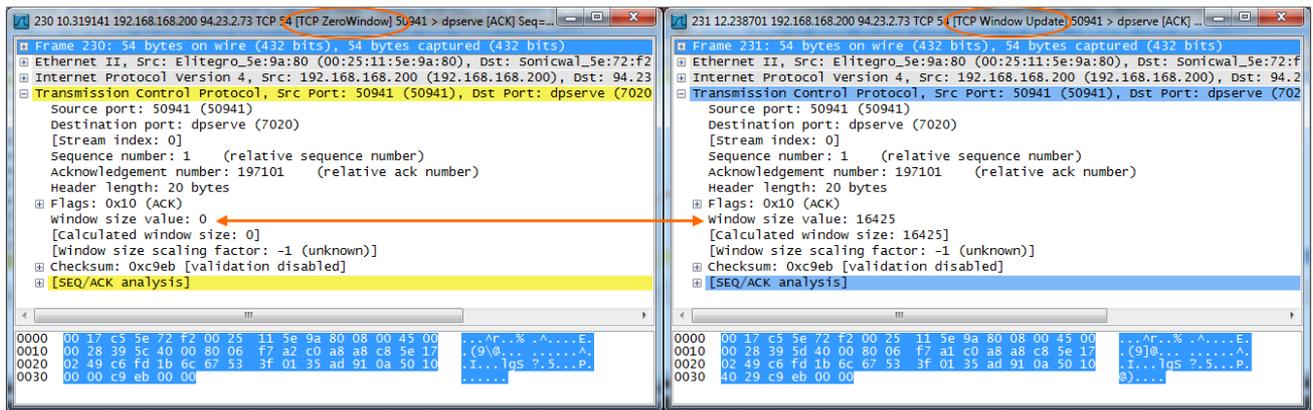


Le mécanisme de ZeroWindow est généralement suivi d'un message TCP Window Update.

6.4.2 TCP WINDOW UPDATE

Le destinataire indique ainsi qu'il est de nouveau prêt à recevoir une certaine quantité de données.

Guide d'utilisation de l'analyseur réseau Wireshark



6.4.3 TCP ZEROWINDOWVIOLATION

Cette erreur survient lorsque l'émetteur ignore l'information "Zero Window" du destinataire et continue à envoyer des trames de données.

6.4.4 TCP ZEROWINDOWPROBE

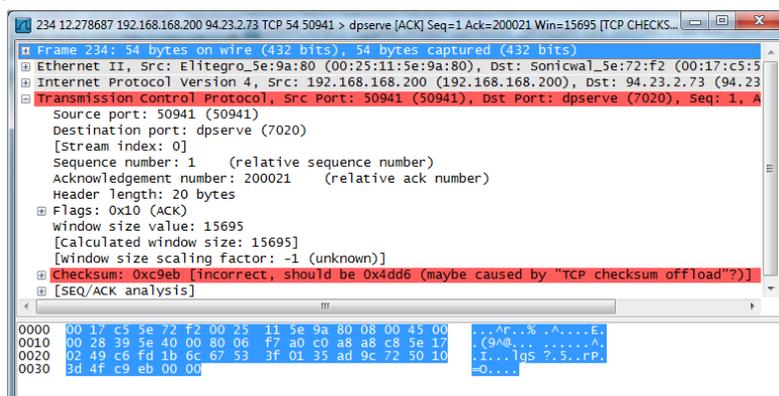
L'émetteur teste si la condition « Zero Window » est toujours active, en envoyant le prochain octet au destinataire. Il recevra soit une trame d'acquittement, soit une nouvelle trame « Zero Window » avec un délai deux fois plus grand.

6.4.5 WINDOWS IS FULL

Ce message est en relation avec l'erreur « Zero Window » mais dans ce cas, c'est l'émetteur qui – connaissant la capacité du buffer de la destination (grâce à l'erreur zero window) – prévient la destination qu'il n'enverra aucune donnée jusqu'à réception d'un acquittement (ACK) car cette trame remplira complètement le tampon mémoire du destinataire.

6.4.6 BAD CHECKSUM IPV4

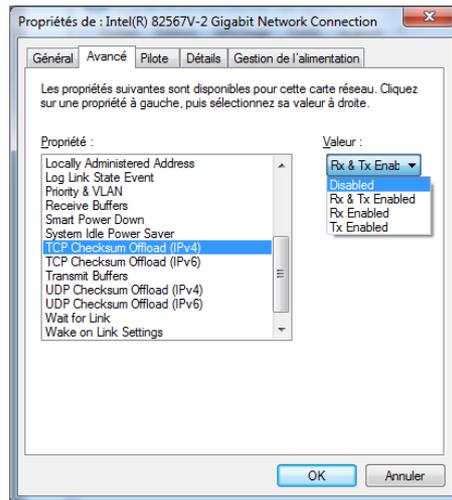
Wireshark calcule le checksum d'une trame et vérifie si ce calcul correspond à la valeur indiquée à la fin de la trame. En cas de différence, cela signifie que la trame a subi une modification (d'origine inconnue).



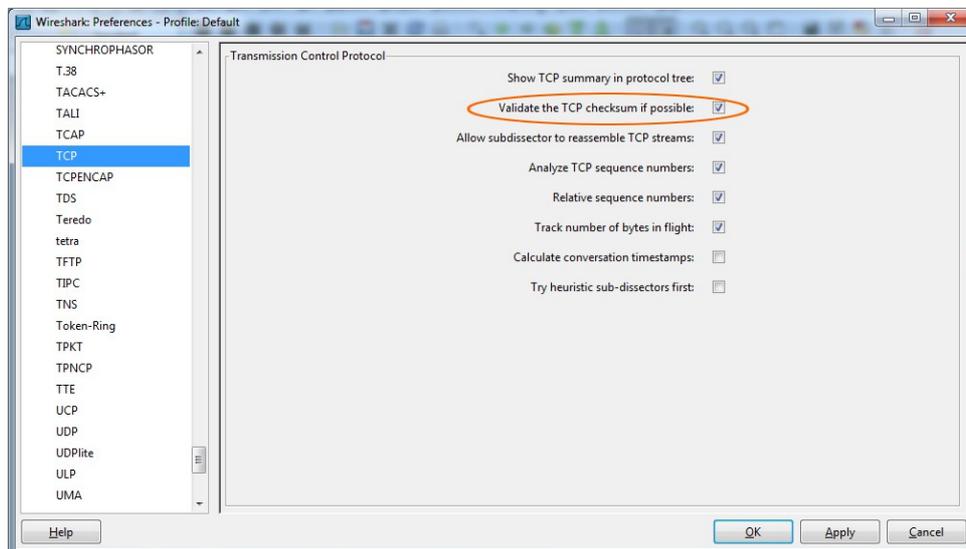
Si cette erreur arrive fréquemment en émission, il y a cependant une explication possible : les cartes réseaux récentes disposent d'une option « *Checksum offloading* » : cette option évite le calcul au niveau du driver réseau de la machine et c'est la carte qui effectue ce calcul. Le driver laisse donc le champ checksum vide (remplit de zéro), ce qui trompe l'analyseur.

Si Wireshark affiche systématiquement ce type d'erreur, il peut être utile de dé-valider cette fonction sur la carte réseau (propriétés carte réseau sous Windows).

Guide d'utilisation de l'analyseur réseau Wireshark



Une autre possibilité consiste à dévalider le contrôle de checksum dans wireshark : menu [Edit] [Preferences...] [Protocols], choisir TCP ou UDP et décocher "Validate XXX checksum..."



6.4.7 DUPLICATE ACK

Dans le cas où les trames arrivent dans le désordre, la destination prévient l'émetteur de ce fait en émettant une trame « Duplicate ACK ».

No.	Time	Source	Destination	Protocol	Length	Info
90	7.517669	10.202.103.72	10.17.7.76	TCP	1514	[TCP segment of a reassembled PDU]
91	7.517763	10.17.7.76	10.202.103.72	TCP	54	empire-empuma > blackjack [ACK] Seq=2191 Ack=3275 Win
92	7.518210	10.202.103.72	10.17.7.76	TCP	1506	[TCP Previous segment lost] [TCP segment of a reassembled PDU]
93	7.518291	10.17.7.76	10.202.103.72	TCP	66	[TCP Dup ACK 91#1] empire-empuma > blackjack [ACK] Seq=2191 Ack=3275 Win
94	8.000711	Atcatal_fb:1c:72	Spanning-tree-(for-bridg) STP	60	Conf. Root = 61440/4095/ff:ff:ff:ff:ff:ff Cost = 0	
95	9.000685	Atcatal_fb:1c:72	Spanning-tree-(for-bridg) STP	60	Conf. Root = 61440/4095/ff:ff:ff:ff:ff:ff Cost = 0	
96	9.082038	Cisco_22:78:9a	PVST+	64	Conf. Root = 49152/10/00:12:d9:22:78:80 Cost = 0 Po	
97	9.092024	10.202.103.72	10.17.7.76	TCP	1514	[TCP Retransmission] blackjack > empire-empuma [ACK] Seq=2191 Ack=3275 Win
98	9.092142	10.17.7.76	10.202.103.72	TCP	66	[TCP Dup ACK 91#2] empire-empuma > blackjack [ACK] Seq=2191 Ack=3275 Win
99	9.142306	10.202.103.72	10.17.7.76	DCERPC	1514	[TCP Retransmission] Response: call_id: 2 Fragment: 1
100	9.142326	10.17.7.76	10.202.103.72	TCP	54	empire-empuma > blackjack [ACK] Seq=2191 Ack=6187 Win
101	9.142717	10.202.103.72	10.17.7.76	TCP	1514	[TCP Retransmission] [TCP segment of a reassembled PDU]
102	9.192793	10.202.103.72	10.17.7.76	TCP	1514	blackjack > empire-empuma [ACK] Seq=6195 Ack=2191 Win

Cependant, le protocole TCP ne peut déterminer s'il s'agit d'une perte de trame ou d'un problème d'ordonnement. Un délai est donc appliqué pour permettre la réception d'un autre message « Duplicate ACK » qui permettra de vérifier s'il s'agit uniquement de 2 trames mal ordonnées ou bien si le désordre et les pertes sont plus graves.

Guide d'utilisation de l'analyseur réseau Wireshark

Wireshark indique donc par un comptage s'il s'agit du premier message ou plus : « TCP Dup ACK *trame#compteur* »

6.4.8 FAST RETRANSMIT

Dans le cas où l'émetteur reçoit des trames dont le numéro de séquence est supérieur au numéro de la trame d'acquittement, il peut retransmettre les trames manquantes avant la fin du timer d'acquittement.

Dans ce cas, les trames sont appelées "Fast Retransmission"

Dans tous les cas, les trames doivent être réémises dans un intervalle maximum de 3 fois "Duplicate ACK".

6.4.9 TCP RETRANSMISSION

Ce message intervient lorsque l'émetteur retransmet une trame après l'expiration du délai d'acquittement.

6.4.10 TCP OUT-OF-ORDER

Ce message survient lorsque une trame contient un numéro de séquence inférieur à la trame précédente reçue. Ce message n'est pas trop grave s'il survient de temps en temps : le protocole TCP ayant la capacité à réordonner les trames. Il s'agit donc seulement d'une information.

6.4.11 TCP PREVIOUS SEGMENT LOST

A l'inverse du message « TCP out-of-order », ce message survient lorsque une trame contient un numéro de séquence supérieur à la trame attendue (numéro de séquence prévu). Ce message est un bon indicateur des trames perdues et est souvent accompagné de l'évènement « TCP retransmission ».

6.4.12 BER ERROR

BER signifie **Bit Error Rate**. Une erreur BER correspond à un taux de bit en erreur sur un nombre bit total. Cette erreur étant très proche de la partie matérielle, sous Wireshark elle est souvent liée à une mauvaise analyse d'un protocole...

TCP_ACKed_lost_segment -

TCP Keep-Alive - Occurs when the sequence number is equal to the last byte of data in the previous packet. Used to elicit an ACK from the receiver.

TCP Keep-Alive ACK - Self-explanatory. ACK packet sent in response to a "keep-alive" packet.

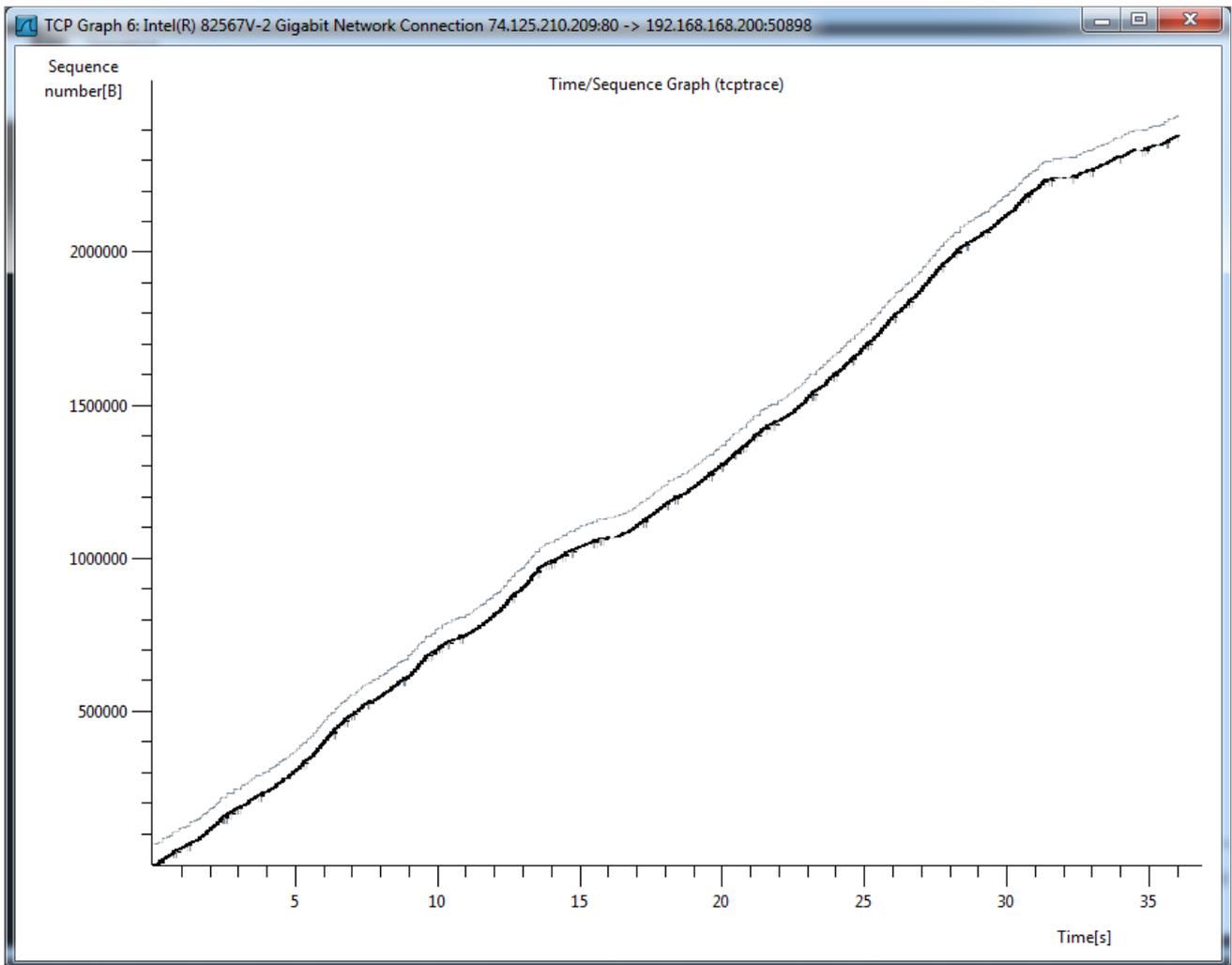
TCP DupACK - Occurs when the same ACK number is seen AND it is lower than the last byte of data sent by the sender. If the receiver detects a gap in the sequence numbers, it will generate a duplicate ACK for each subsequent packet it receives on that connection, until the missing packet is successfully received (retransmitted). A clear indication of dropped/missing packets.

6.5 Flux particuliers

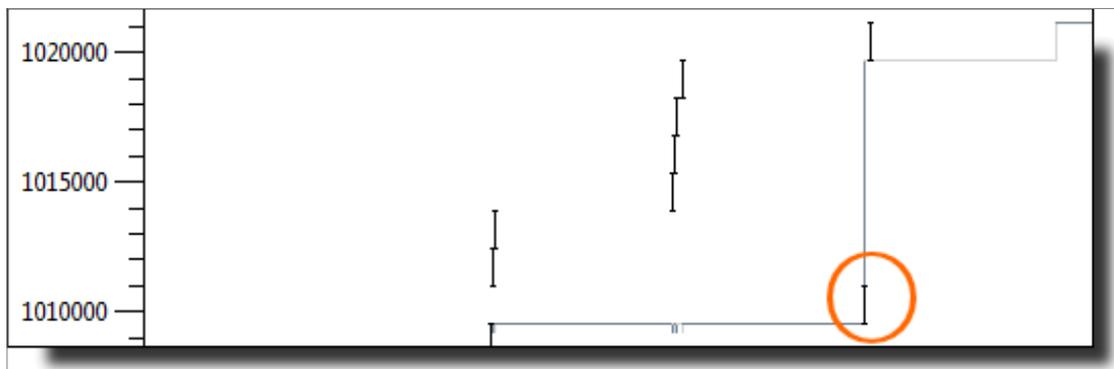
6.5.1 STREAMING

Il se caractérise par un accès régulier et (normalement) constant. L'outil « Time-sequence (tcptrace) est idéal pour établir le diagnostic :

Guide d'utilisation de l'analyseur réseau Wireshark



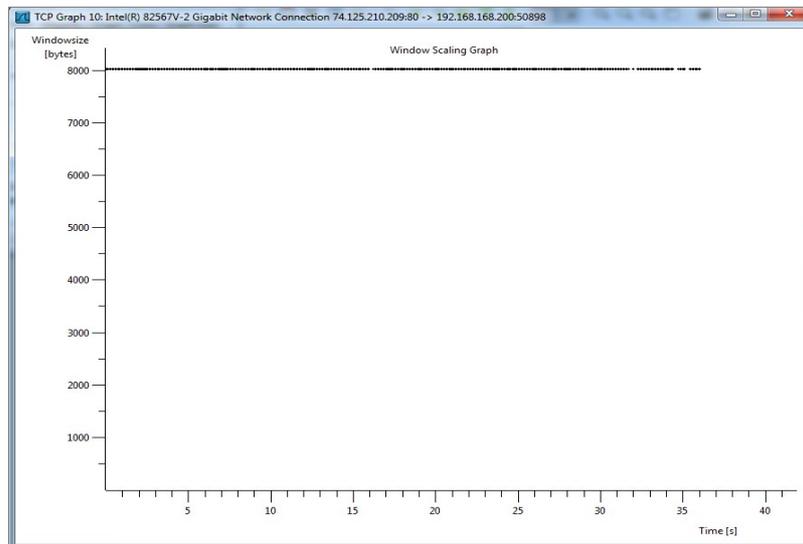
Dans ce graphe, il est possible de zoomer pour trouver les erreurs de retransmissions et vérifier l'ordre des séquences :



Ici, il est visible que la première trame a été ré-émise puisque son numéro de séquence est plus petit tandis que dans le temps, elle est plus à droite que les autres.

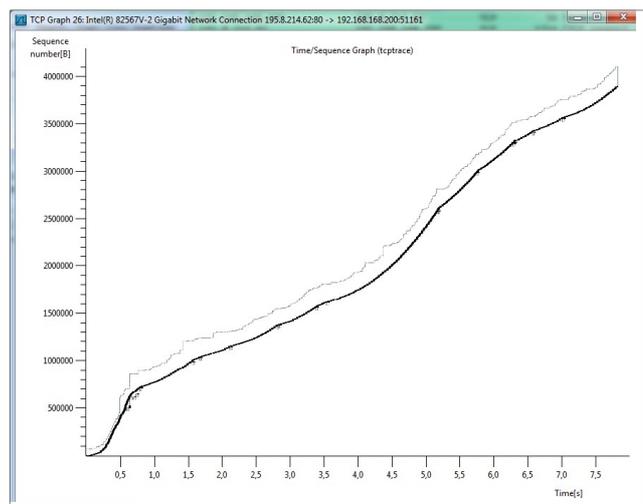
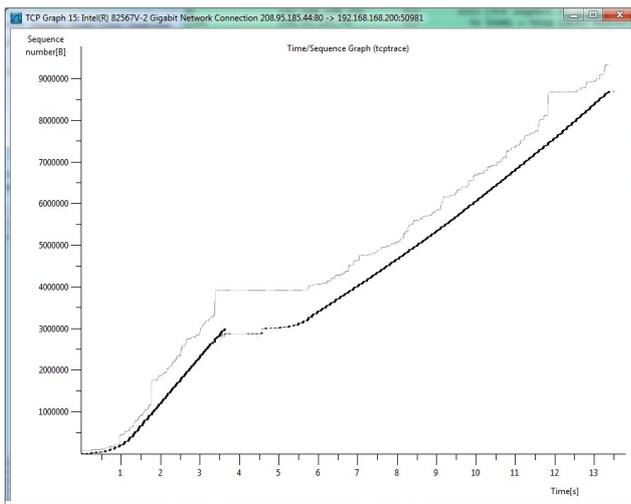
Un autre graphe permet de constater qu'il n'y a pas eu de congestion : [Statistics] [TCP Stream Graph] [Windows Scaling Graph] :

Guide d'utilisation de l'analyseur réseau Wireshark

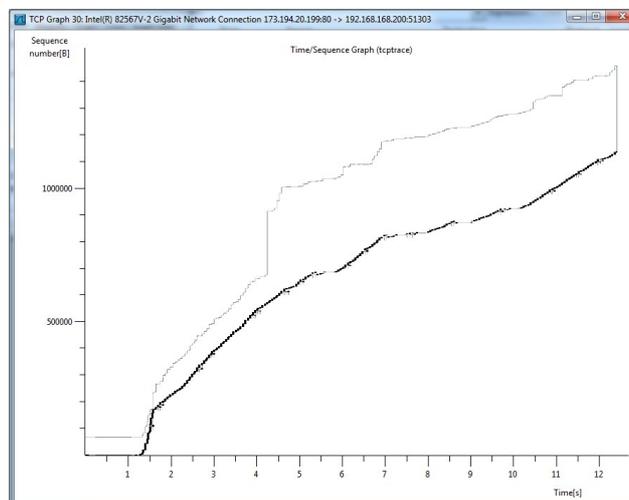


Le mécanisme de fenêtrage TCP a conservé une valeur constante de 8192 octets tout au long de la diffusion du flux.

Les images ci-après montrent un fonctionnement moins régulier du flux mais sans erreurs :

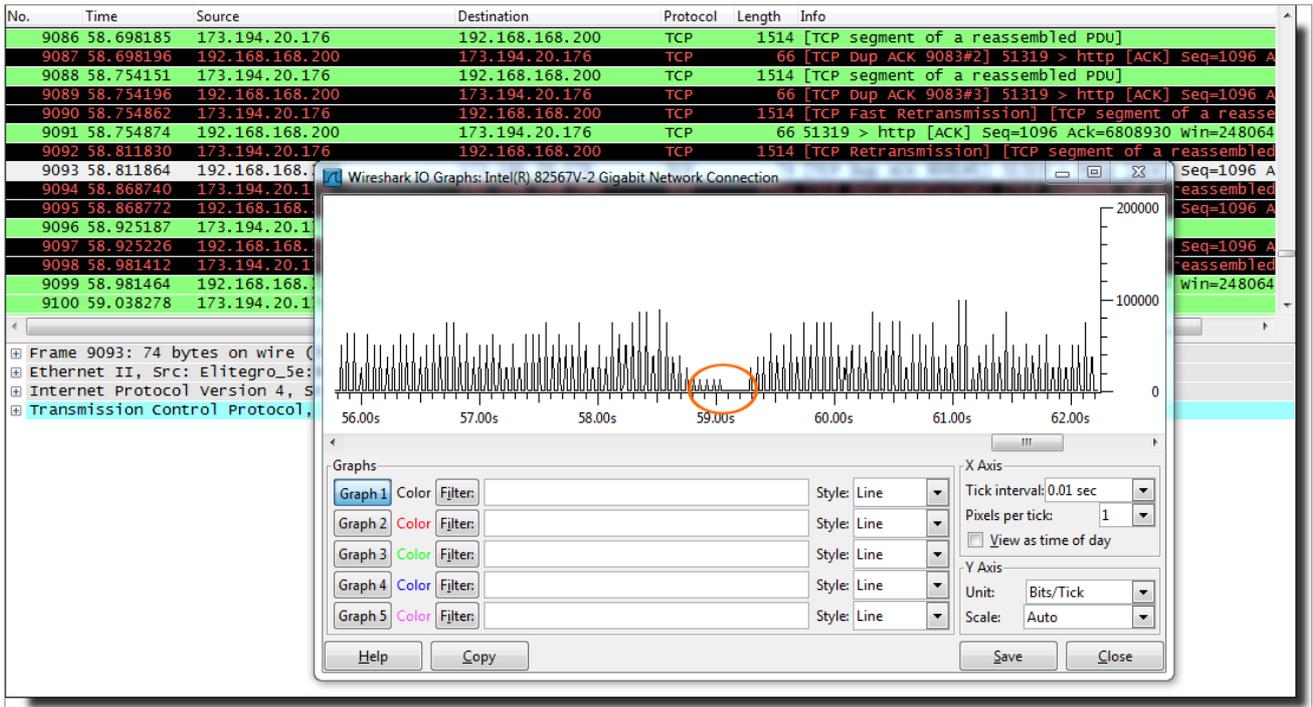


Enfin, un graphe contenant de nombreuses retransmissions :



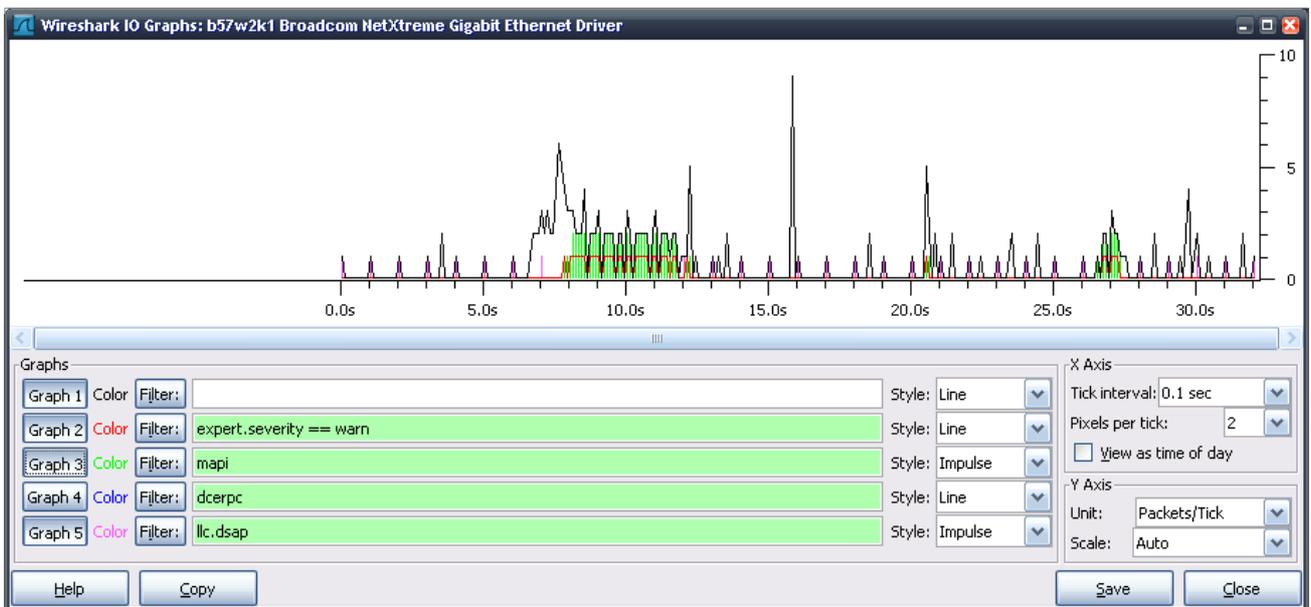
Guide d'utilisation de l'analyseur réseau Wireshark

Dans ce dernier cas, il est possible de vérifier les variations de débits : outil [Statistics] [IO Graph]



6.5.2 SPANNING-TREE

Les flux spanning-tree de type DSAP sont très constants : une trame est émise toute les secondes. Il est facile de le vérifier dans l'outil graphique « IO Graphs », en plaçant un filtre de type 'llc.dsap' et en choisissant un style 'impulse' (en rose sur le graphe).



Les trames font ici 480 octets, soit une charge globale de 3840 bits/s ce qui est relativement négligeable par rapport aux autres protocoles présents sur le graphe ci-dessus.