Architectures Réseaux Télécoms	Manuel : Analyseur réseau Wireshark	Création : **28/12/2006 15:20:00** Mise à jour : **04/05/200707 09:52:00 AM**
Auteur : David ROUMANET		

1.SOMMAIRE

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 0.99.4.

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 terminé, le **poste** devient une **sonde** réseau prête à fonctionner.

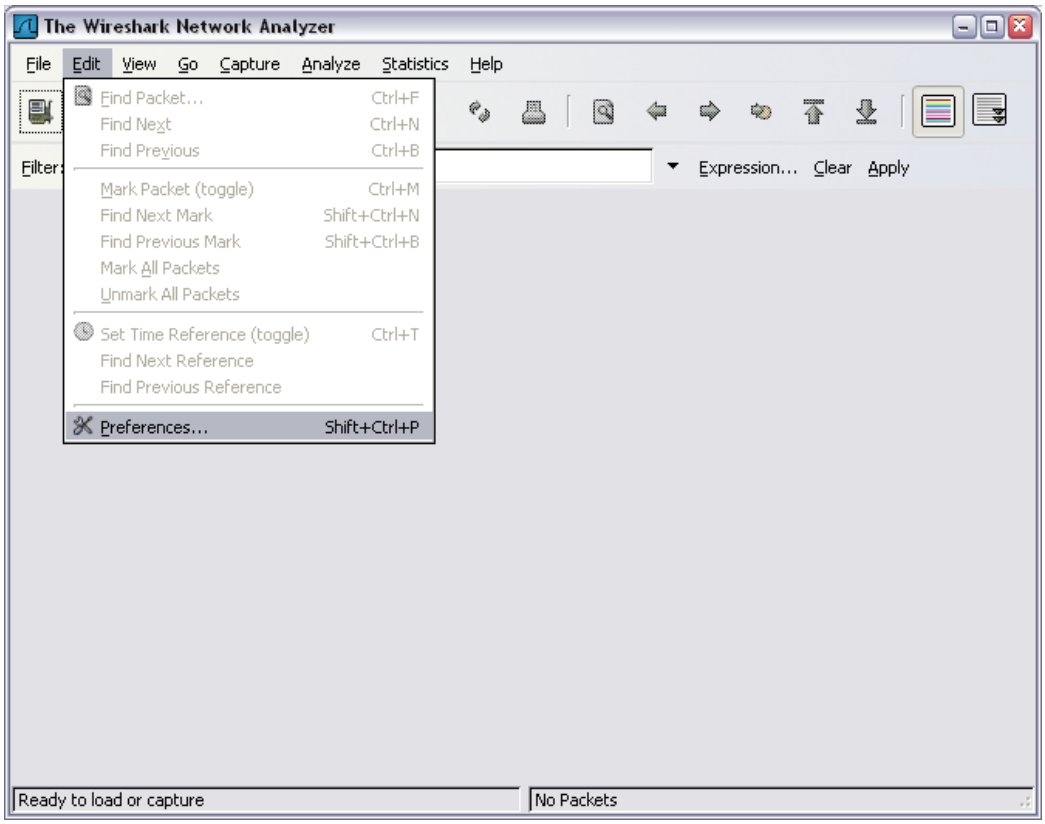
3.CAPTURE

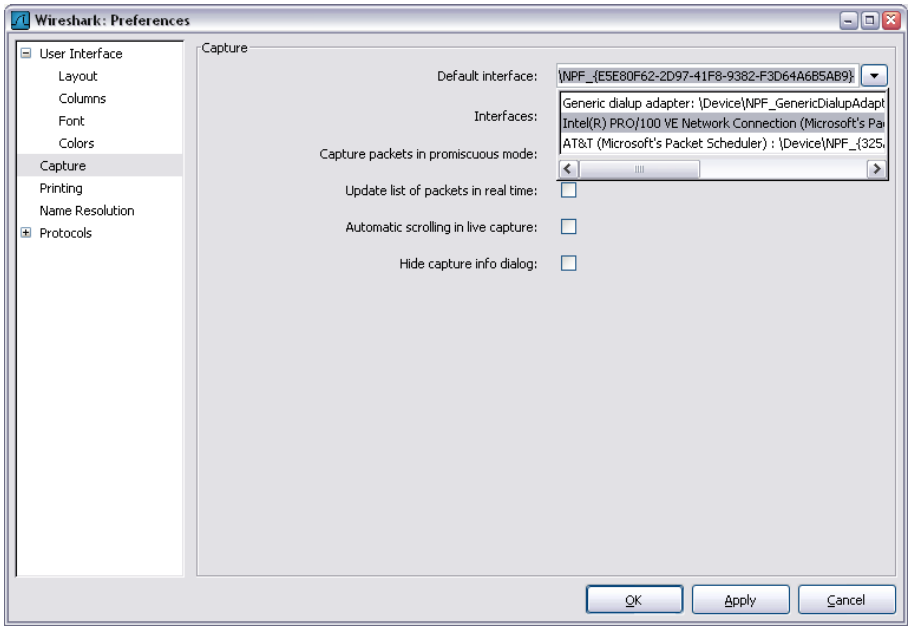
La première opération est la capture de trames. Cependant il y a plusieurs cas possibles :
- Capture en temps réel de manière manuelle (l'utilisateur démarre et arrête la capture)
- Capture avec limitations automatiques (dans le temps ou sur la taille…)
- Capture sur une période donnée avec rotation (utilisation d'un « buffer » circulaire)

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

3.1Edition des préférences

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





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

3.2Choisir les paramètres de capture

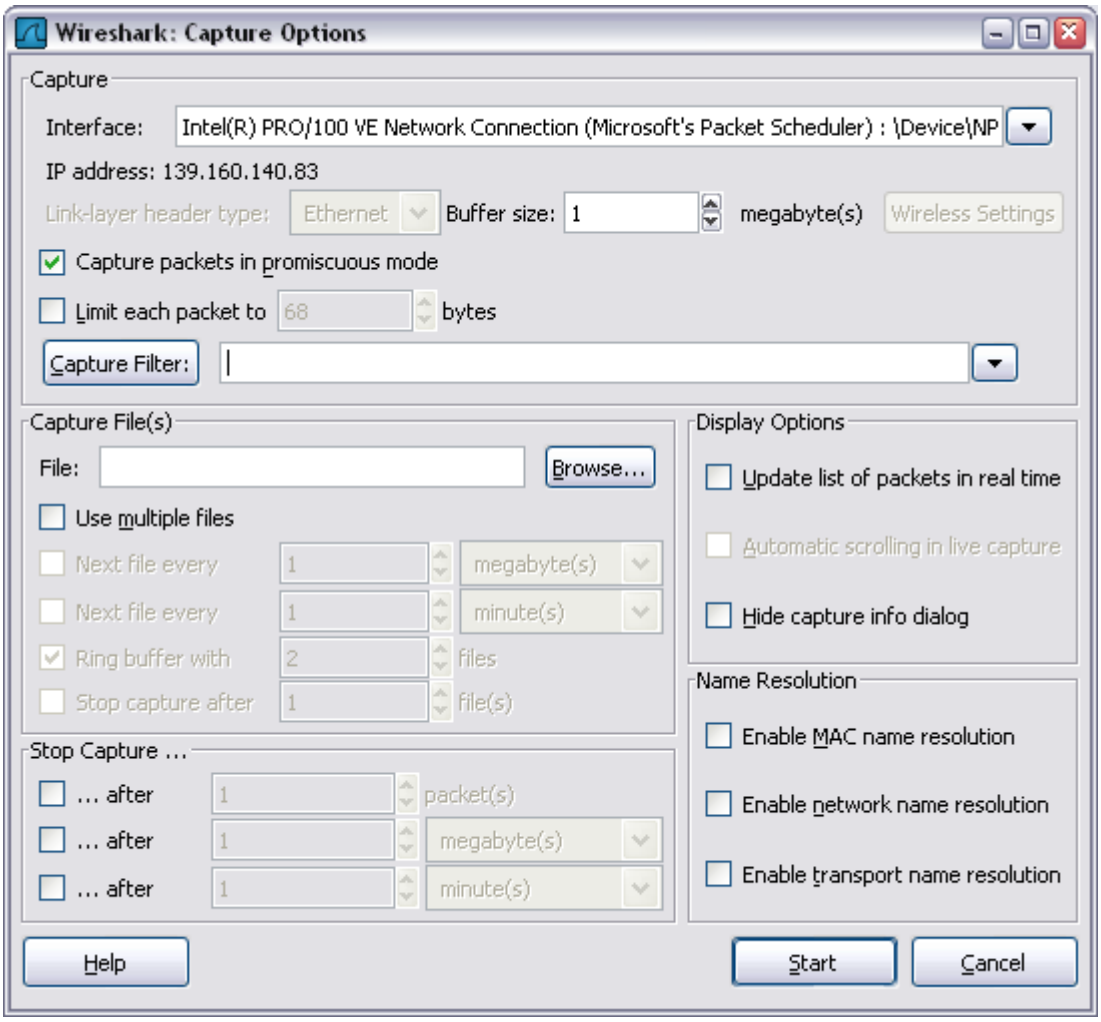
Pour faire une **capture manuelle**, il suffit de cliquer sur l'icône "Start a new live capture" ou dans le menu, choisir [Capture] [Start]… il suffira ensuite d'arrêter la capture en cliquant sur l'icône à sa droite.

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 ou 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.*

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]

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 ».

3.2.1Limitation 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 68 octets (entête TCP) et 132 (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.

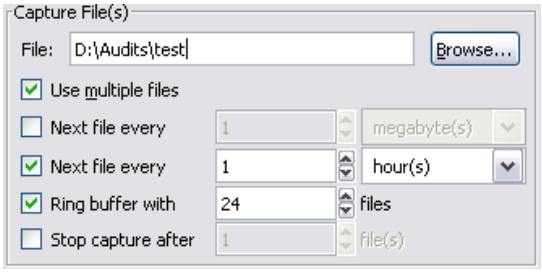
3.2.2Arrêt automatique sur seuil

Il est possible de limiter la capture sur 3 critères : nombre de paquets, taille de la capture et délai dans le temps. 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.

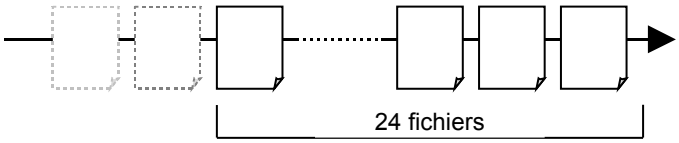
3.2.3Captures circulaires

C'est le mode le plus intéressant, surtout si la sonde dispose d'un espace disque suffisant. En effet, les problèmes réseaux sont souvents fugitifs et lorsque un incident survient, le temps d'activer une capture ne permet pas de trouver l'origine du problème. D'un autre coté, 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 24ème heure écoulée, Wireshark va supprimer le premier fichier de la liste et va créer un nouveau fichier.



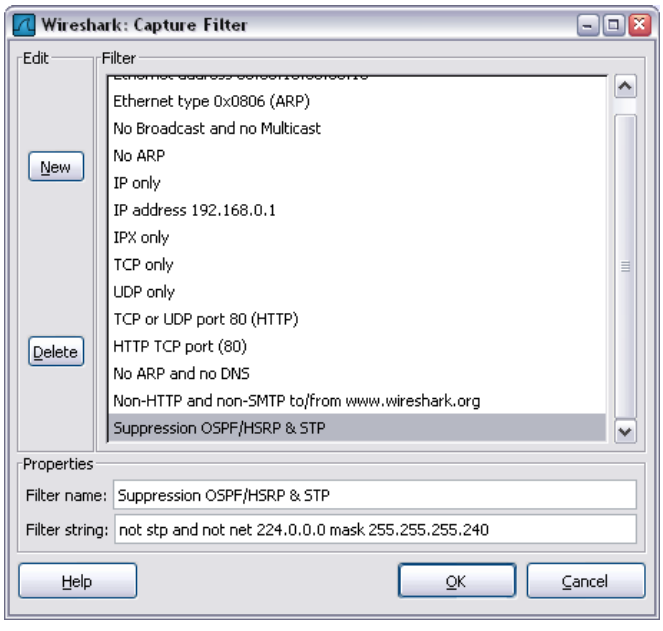
Avantages :

- 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 2Mo et 10Mo 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.

3.2.4Filtres de capture

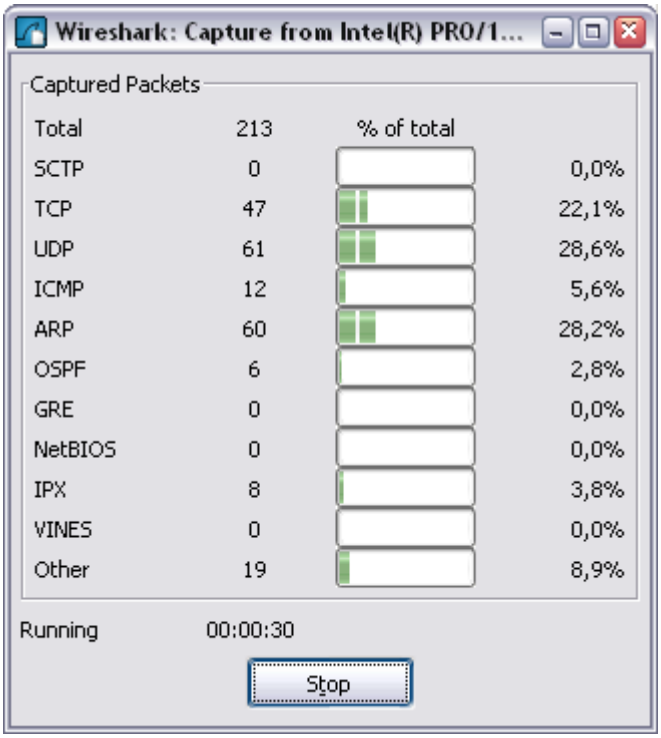
Si le flux à surveiller est bien identifié (serveur, plage réseau, numéros de ports), il est possible de n'enregistrer que les trames qui lui correspondent. Pour cela, Wireshark permet d'appliquer un filtre sur les paquets à enregistrer.



La syntaxe du filtre de capture est accessible en cliquant sur le bouton [Help]. Ce filtre permet de combiner plusieurs conditions (and et or) ainsi que d'inverser les filtres (not).

3.3Statistiques instantanées de capture

Une fois tous les paramètres de capture définis, la capture démarre. Wireshark affiche une boite de dialogue qui indique en temps réel la répartition des protocoles



4.ANALYSES

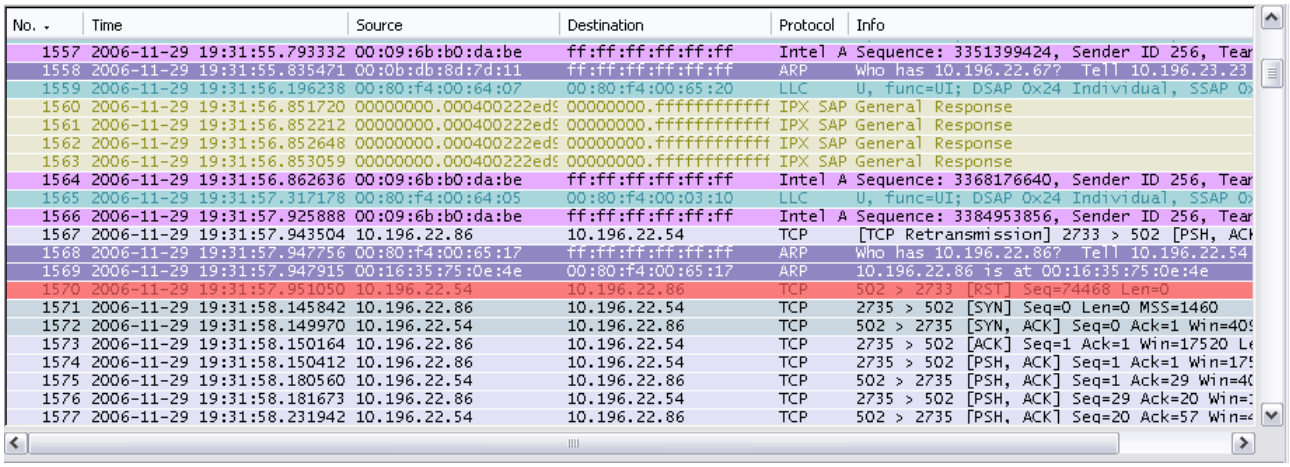
Une fois les captures effectuées, il est possible de faire le travail d'analyse. C'est la partie la plus complexe mais si les options de captures ont été judicieusement utilisées, ce travail ne sera pas trop long.

4.1Lecture des trames

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

4.1.1Fenêtre de résumé

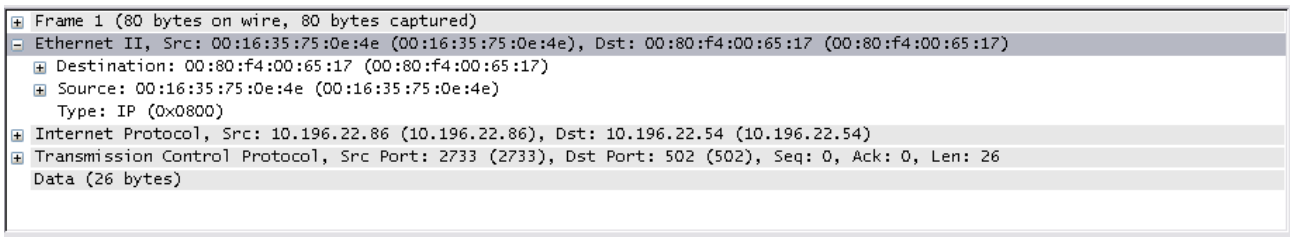
Dans cette fenêtre, Wireshark affiche un résumé des informations : adresses (niveau 3 ou par défaut niveau 2), estampillage horaire, protocole et description succinte. La coloration permet de retrouver rapidement certains protocoles (broadcast, requêtes ARP, etc.) et elle est personnalisable dans le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



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.

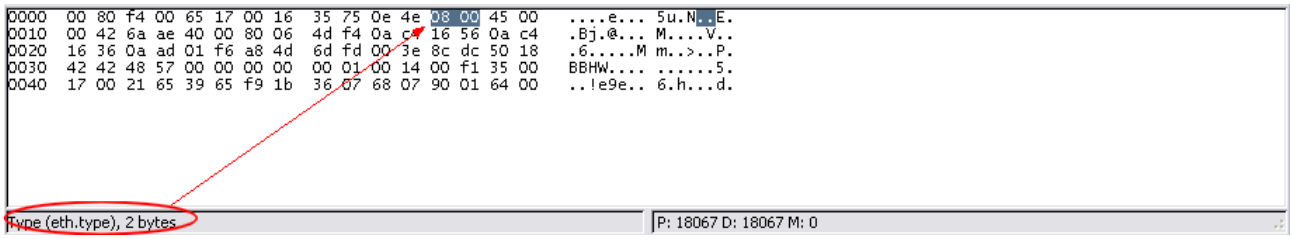
4.1.2Fenêtre d'arborescence de protocole

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.



4.1.3Fenêtre 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.

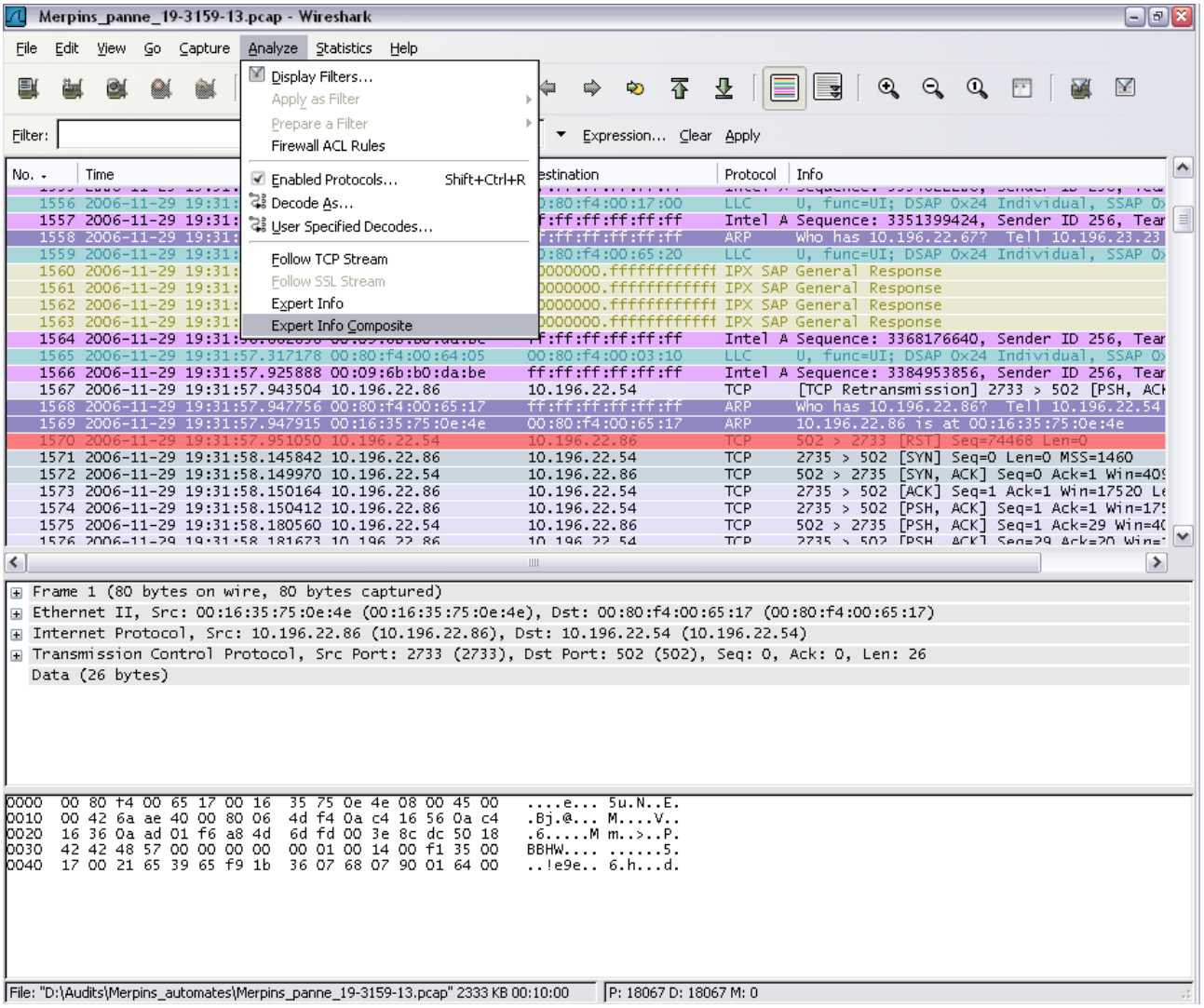


4.2Analyse rapide

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

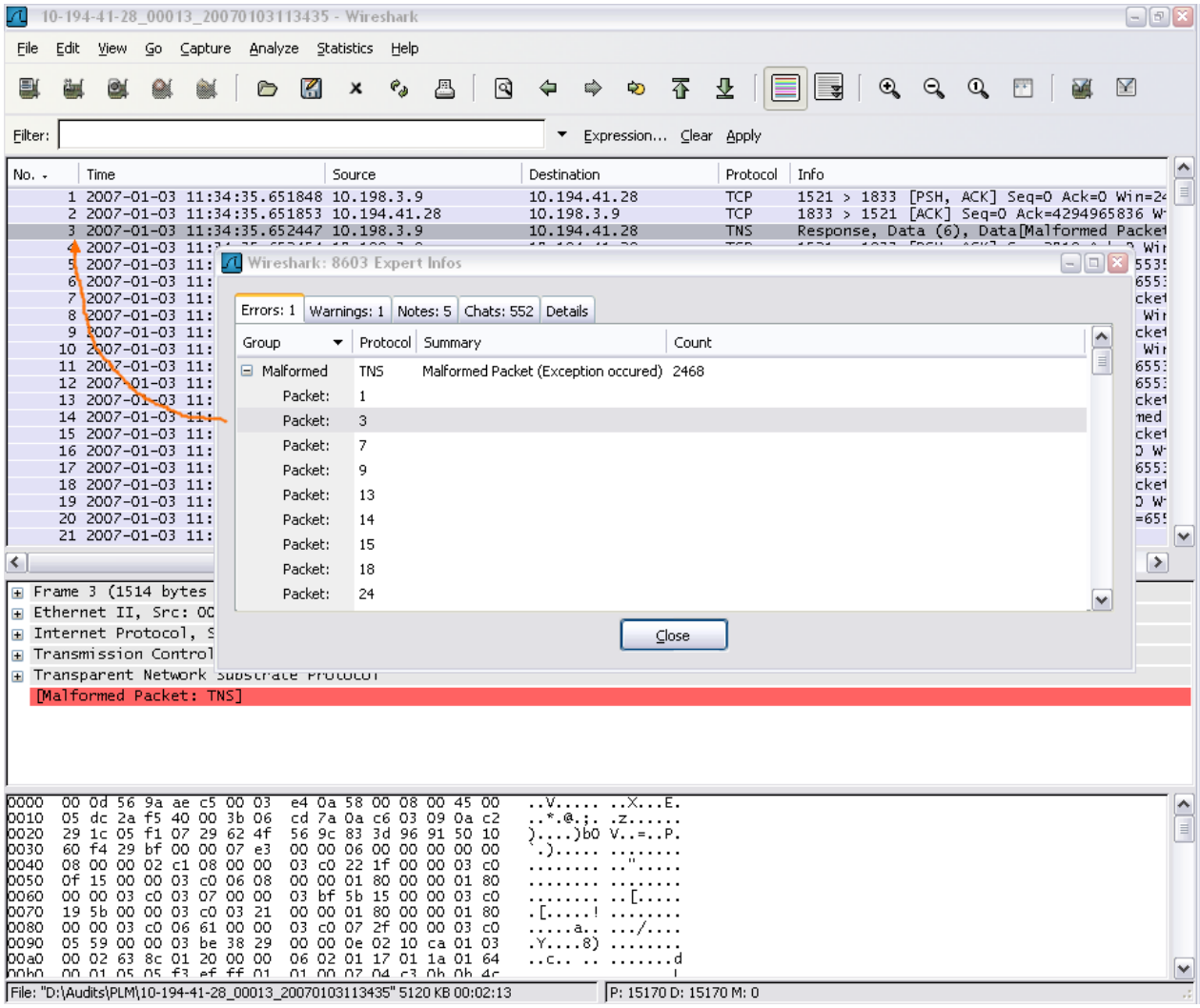
4.2.1Expert Info Composite

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 (flag) 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 mais pas forcément réels.
- 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.



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 condensé : 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…

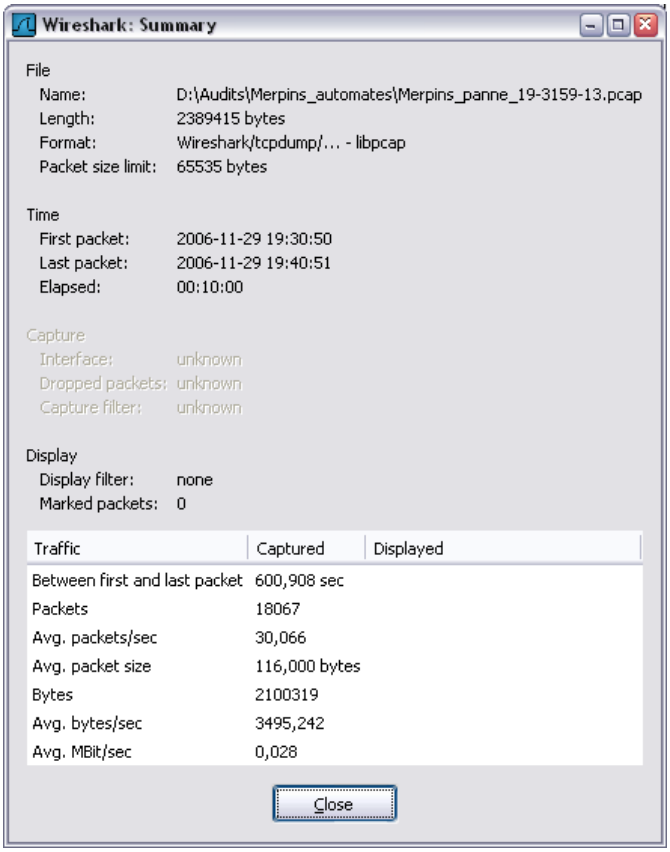
D'autres outils permettent l'analyse des protocoles utilisés et les temps de réponses ou bande passante.

4.3Analyse 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.

4.3.1Informations sur la capture

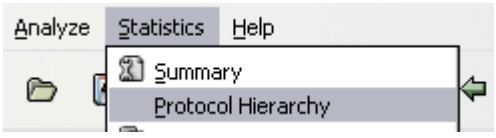
Wireshark affiche les informations sur le fichier de capture avec notamment le débit moyen lors de la capture. Pour cela, il faut aller dans le menu [Statistics] [Summary].



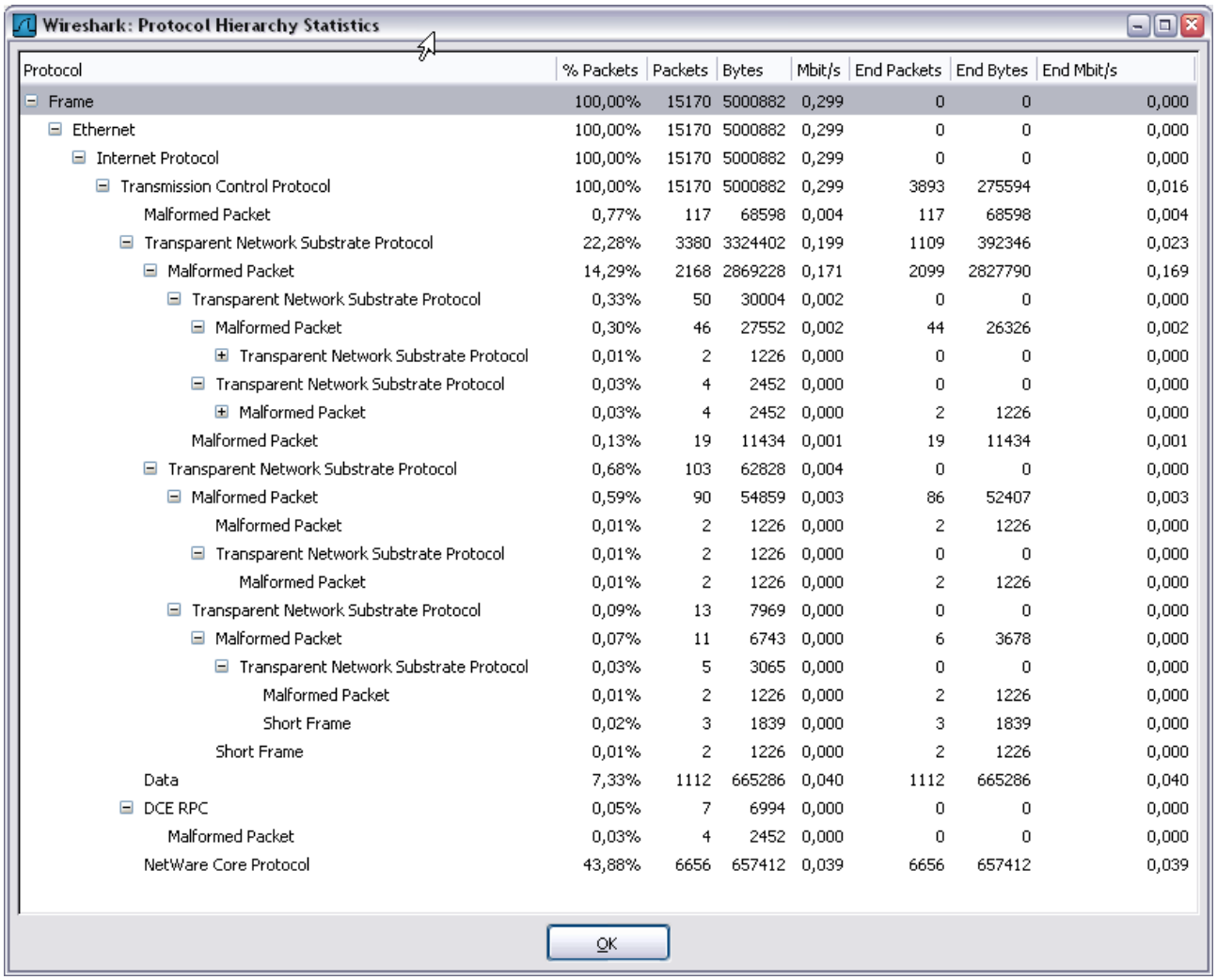
La durée de capture, ainsi que les dates de début et de fin sont indiquées de manière claire.

4.3.2Répartition 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.

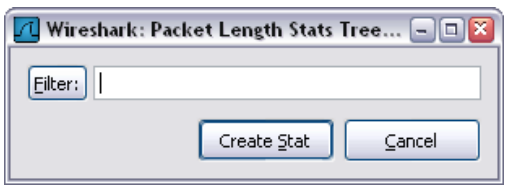


Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00%	15170	5000882	0,299	0	0	0,000
Ethernet	100,00%	15170	5000882	0,299	0	0	0,000
Internet Protocol	100,00%	15170	5000882	0,299	0	0	0,000
Transmission Control Protocol	100,00%	15170	5000882	0,299	3893	275594	0,016
Malformed Packet	0,77%	117	68598	0,004	117	68598	0,004
Transparent Network Substrate Protocol	22,28%	3380	3324402	0,199	1109	392346	0,023
Malformed Packet	14,29%	2168	2869228	0,171	2099	2827790	0,169
Transparent Network Substrate Protocol	0,33%	50	30004	0,002	0	0	0,000
Malformed Packet	0,30%	46	27552	0,002	44	26326	0,002
Transparent Network Substrate Protocol	0,01%	2	1226	0,000	0	0	0,000
Transparent Network Substrate Protocol	0,03%	4	2452	0,000	0	0	0,000
Malformed Packet	0,03%	4	2452	0,000	2	1226	0,000
Malformed Packet	0,13%	19	11434	0,001	19	11434	0,001
Transparent Network Substrate Protocol	0,68%	103	62828	0,004	0	0	0,000
Malformed Packet	0,59%	90	54859	0,003	86	52407	0,003
Malformed Packet	0,01%	2	1226	0,000	2	1226	0,000
Transparent Network Substrate Protocol	0,01%	2	1226	0,000	0	0	0,000
Malformed Packet	0,01%	2	1226	0,000	2	1226	0,000
Transparent Network Substrate Protocol	0,09%	13	7969	0,000	0	0	0,000
Malformed Packet	0,07%	11	6743	0,000	6	3678	0,000
Transparent Network Substrate Protocol	0,03%	5	3065	0,000	0	0	0,000
Malformed Packet	0,01%	2	1226	0,000	2	1226	0,000
Short Frame	0,02%	3	1839	0,000	3	1839	0,000
Short Frame	0,01%	2	1226	0,000	2	1226	0,000
Data	7,33%	1112	665286	0,040	1112	665286	0,040
DCE RPC	0,05%	7	6994	0,000	0	0	0,000
Malformed Packet	0,03%	4	2452	0,000	0	0	0,000
NetWare Core Protocol	43,88%	6656	657412	0,039	6656	657412	0,039

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

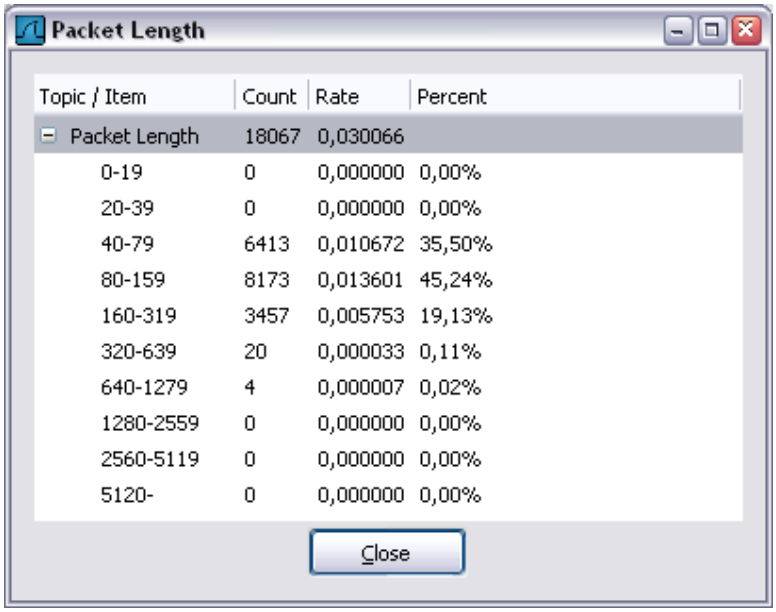
4.3.3Répartition des tailles de paquets

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…



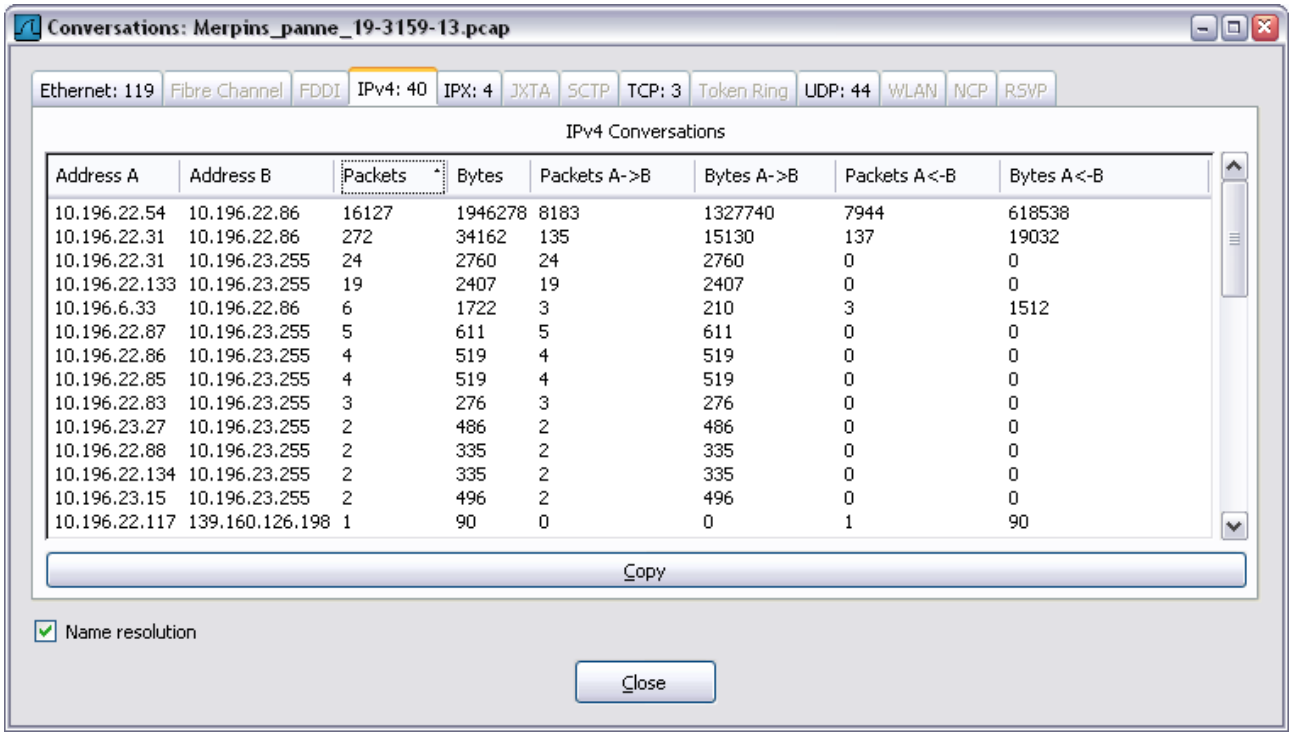
En cliquant sur le bouton [Create Stat], Wireshark ouvre une fenêtre contenant la répartition demandée par tranche.

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.



4.3.4Conversations

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



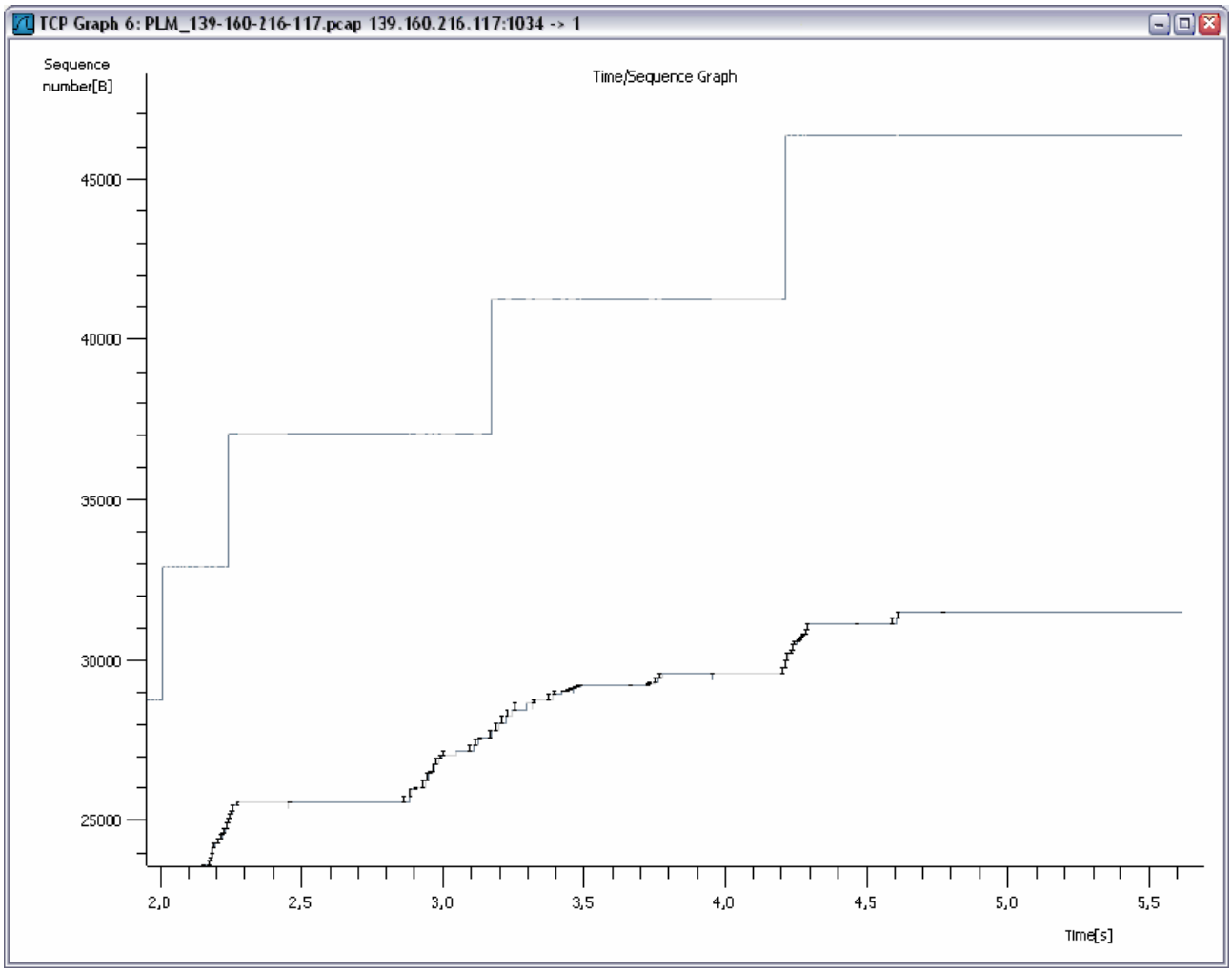
Les onglets permettent de choisir le type d'adressage (Ethernet, IPX, Ipv4) et même par protocoles (TCP ou UDP).

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].

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'.

4.4Analyse graphique "Time-Sequence" (tcptrace)

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



Les petits traits verticaux noirs (en forme de '**I**') sont des trames envoyés (du premier au dernier octet, donc la hauteur représente la longueur de la trame).

La courbe bleue qui semble suit les traits verticaux noirs correspond à l'accusé de réception des trames : séquence ACK. Elle indique le délai d'acquittement de chaque trame et lorsqu'il y a une retransmission, un petit trait vers le bas est ajouté (Duplicate ACK).