SI5 – Administration des Réseaux
Troubleshooting Computer Networks

# TD : traceroute, SmokePing, et Dépannage

## 1 traceroute depuis un opérateur grand public

Un traceroute depuis une machine derrière un accès chez opérateur grand public donne :

```
root@Ubuntu:~# traceroute -I www.unice.fr
traceroute to www.unice.fr (134.59.204.1), 30 hops max, 60 byte packets
1 192.168.0.254 (192.168.0.254) 5.212 ms 5.058 ms *
2 * * *
3 * * *
4 * * *
5 * * *
6 * lyon-crs16-1-be1008.intf.routers.proxad.net (212.27.59.153) 25.561 ms *
7 th2-crs16-1-be2001.intf.routers.proxad.net (212.27.59.29) 35.708 ms 36.191 ms *
8 * * *
9 renater.routers.proxad.net (212.27.38.206) 41.948 ms 41.850 ms 41.743 ms
10 te0-0-0-3-paris1-rtr-001.noc.renater.fr (193.51.189.37) 64.037 ms 64.126 ms 64.481 ms
11 te0-3-1-0-lyon1-rtr-001.noc.renater.fr (193.51.189.126) 57.268 ms 57.664 ms 53.579 ms
12 te1-1-marseille1-rtr-021.noc.renater.fr (193.51.189.18) 45.334 ms 53.356 ms 53.287 ms
13 te1-2-sophia-rtr-021.noc.renater.fr (193.51.189.26) 53.181 ms 53.051 ms 51.727 ms
14 unsa-vl601-gi8-4-sophia-rtr-021.noc.renater.fr (193.51.181.141) 51.200 ms 49.509 ms 49.423 ms
15 * * *
16 * * *
17 webs.unice.fr (134.59.204.1) 49.541 ms 50.164 ms 51.937 ms
```

Le même avec l'option `-N` qui contrôle le nombre de paquets envoyé simultanément donne :

```
root@Ubuntu:~# traceroute -I www.unice.fr -N 1
traceroute to www.unice.fr (134.59.204.1), 30 hops max, 60 byte packets
1 192.168.0.254 (192.168.0.254) 1.170 ms 3.064 ms 1.657 ms
2 82.238.189.254 (82.238.189.254) 19.207 ms 19.377 ms 23.285 ms
3 78.254.5.190 (78.254.5.190) 24.038 ms 27.957 ms 21.017 ms
4 ant06-1-v902.intf.nra.proxad.net (78.254.254.154) 21.559 ms 22.918 ms 22.097 ms
5 nice-6k-1-v900.intf.nra.proxad.net (78.254.254.158) 21.304 ms 22.428 ms 21.042 ms
6 lyon-crs16-1-be1008.intf.routers.proxad.net (212.27.59.153) 27.997 ms 28.290 ms 32.009 ms
7 th2-crs16-1-be2001.intf.routers.proxad.net (212.27.59.29) 36.053 ms 35.206 ms 35.322 ms
8 aub-6k-1-po21.intf.routers.proxad.net (212.27.50.138) 36.613 ms 34.503 ms 35.170 ms
9 renater.routers.proxad.net (212.27.38.206) 33.867 ms 35.671 ms 33.866 ms
10 te0-0-0-3-paris1-rtr-001.noc.renater.fr (193.51.189.37) 53.208 ms 68.097 ms 88.138 ms
11 te0-3-1-0-lyon1-rtr-001.noc.renater.fr (193.51.189.126) 50.172 ms 44.771 ms 49.871 ms
12 te1-1-marseille1-rtr-021.noc.renater.fr (193.51.189.18) 48.383 ms 45.060 ms 47.141 ms
13 te1-2-sophia-rtr-021.noc.renater.fr (193.51.189.26) 49.811 ms 45.614 ms 50.350 ms
14 unsa-vl601-gi8-4-sophia-rtr-021.noc.renater.fr (193.51.181.141) 46.011 ms 47.599 ms 48.147 ms
15 * * *
16 * * *
17 webs.unice.fr (134.59.204.1) 44.690 ms 48.601 ms 46.574 ms
```

**Question #1 :**
Quelle politique applique les routeurs 2-5 d'après vous et les routeurs 15 et 16 ?

**Question #2 :**
Interpréter maintenant ce qui se passe lorsqu'on fait un traceroute en envoyant des paquets TCP ? On discutera notamment ce que fait le routeur 9.

```
root@Ubuntu:~# traceroute -T www.unice.fr -N 1 -q 1
traceroute to www.unice.fr (134.59.204.1), 30 hops max, 60 byte packets
1 192.168.0.254 (192.168.0.254) 1.038 ms
2 82.238.189.254 (82.238.189.254) 17.519 ms
3 78.254.5.190 (78.254.5.190) 20.959 ms
4 ant06-1-v902.intf.nra.proxad.net (78.254.254.154) 23.586 ms
5 nice-6k-1-v900.intf.nra.proxad.net (78.254.254.158) 22.454 ms
6 lyon-crs16-1-be1008.intf.routers.proxad.net (212.27.59.153) 30.742 ms
7 th2-crs16-1-be2001.intf.routers.proxad.net (212.27.59.29) 35.093 ms
8 aub-6k-1-po21.intf.routers.proxad.net (212.27.50.138) 30.039 ms
9 *
10 te0-0-0-3-paris1-rtr-001.noc.renater.fr (193.51.189.37) 47.897 ms
11 te0-3-1-0-lyon1-rtr-001.noc.renater.fr (193.51.189.126) 53.583 ms
12 te1-1-marseille1-rtr-021.noc.renater.fr (193.51.189.18) 43.391 ms
13 *
14 unsa-vl601-gi8-4-sophia-rtr-021.noc.renater.fr (193.51.181.141) 48.166 ms
15 *
16 *
17 webs.unice.fr (134.59.204.1) 48.522 ms
```

**Question #3 :**
Que se passe-t-il si on envoie une sonde UDP maintenant ? (Observez que l'utilisateur interrompt le programme traceroute à la ligne 19.)

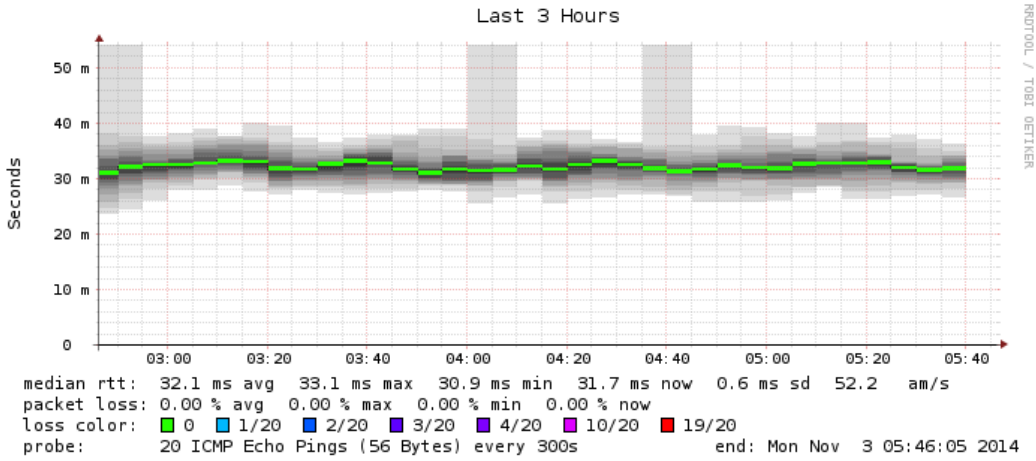
```
root@Ubuntu:~# traceroute -U www.unice.fr -N 1 -q 1
traceroute to www.unice.fr (134.59.204.1), 30 hops max, 60 byte packets
1 192.168.0.254 (192.168.0.254) 1.433 ms
2 82.238.189.254 (82.238.189.254) 24.093 ms
3 78.254.5.190 (78.254.5.190) 22.891 ms
4 ant06-1-v902.intf.nra.proxad.net (78.254.254.154) 17.799 ms
5 nice-6k-1-v900.intf.nra.proxad.net (78.254.254.158) 36.700 ms
6 lyon-crs16-1-be1008.intf.routers.proxad.net (212.27.59.153) 26.789 ms
7 th2-crs16-1-be2001.intf.routers.proxad.net (212.27.59.29) 32.527 ms
8 aub-6k-1-po21.intf.routers.proxad.net (212.27.50.138) 34.369 ms
9 *
10 te0-0-0-3-paris1-rtr-001.noc.renater.fr (193.51.189.37) 61.513 ms
11 te0-3-1-0-lyon1-rtr-001.noc.renater.fr (193.51.189.126) 46.766 ms
12 te1-1-marseille1-rtr-021.noc.renater.fr (193.51.189.18) 49.793 ms
13 *
14 unsa-vl601-gi8-4-sophia-rtr-021.noc.renater.fr (193.51.181.141) 54.150 ms
15 *
16 *
17 *
18 *
19 *^C
```

# 2 SmokePing

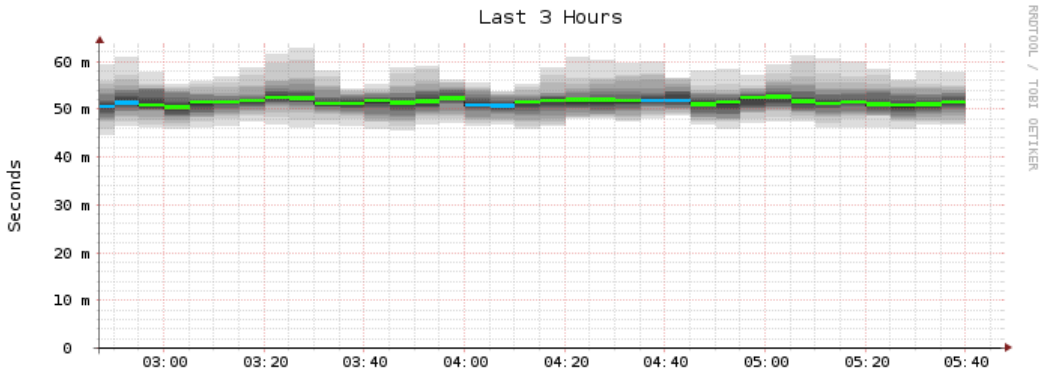
Dans cet exercice, nous allons analyser les graphes fournis par SmokePing qui ont été obtenus depuis une machine qui est raccordée via un accès ADSL. SmokePing a été paramétré pour fournir les indicateurs suivants :

- Niveau réseau
  - ping vers kheops.unice.fr
  - ping vers resolver DNS de l'opérateur
- Niveau application
  - DNS
    - Interrogation du resolver DNS de l'opérateur pour résoudre www.google.fr
    - Interrogation du resolver ouvert de Google (8.8.8.8) pour résoudre kheops.unice.fr
  - HTTP
    - téléchargement page kheops.unice.fr
  - HTTPs
    - téléchargement page d'accueil de kheops.unice.fr

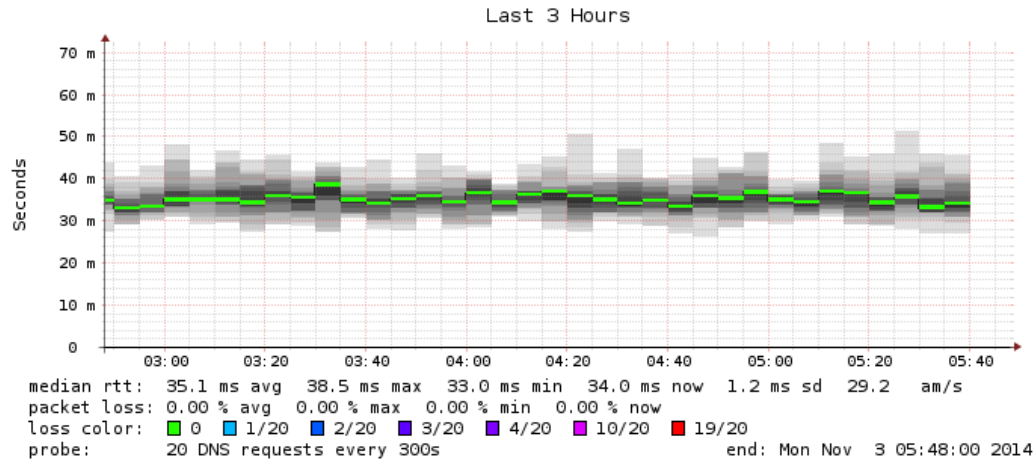
## Ping of Local_DNS



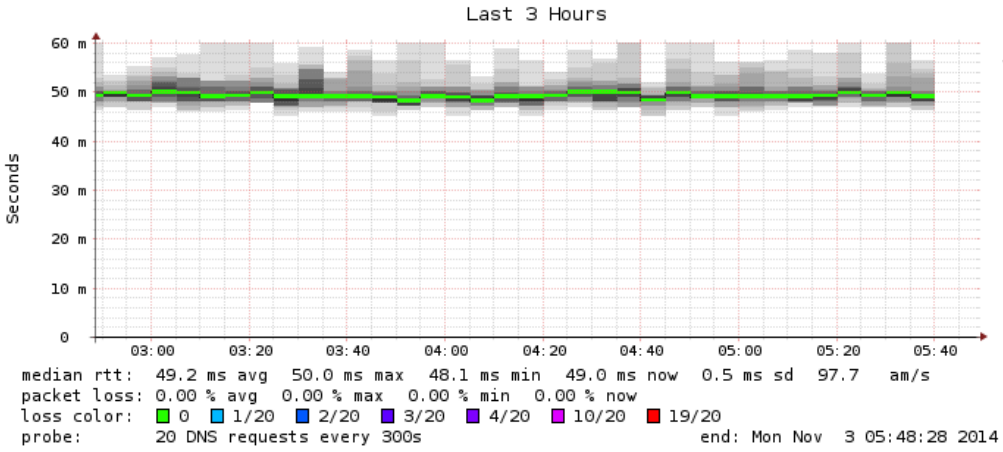

## Ping of kheops



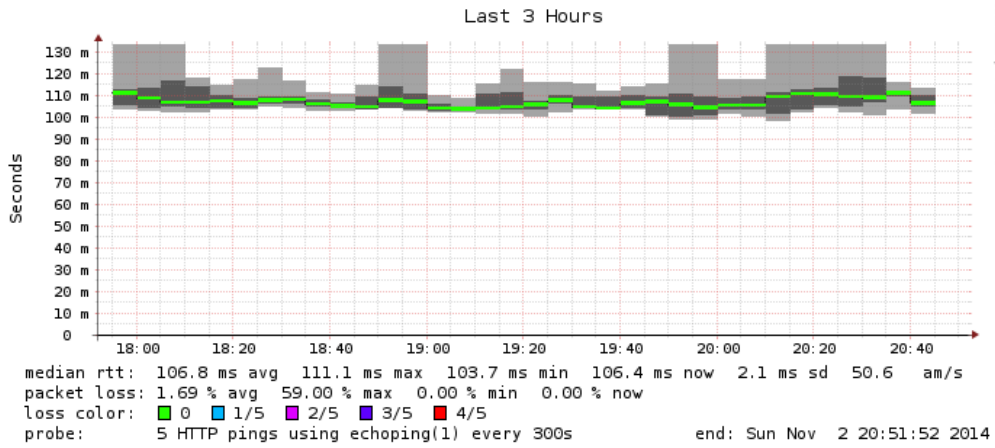
# DNS lookup for Google from the DNS of ISP



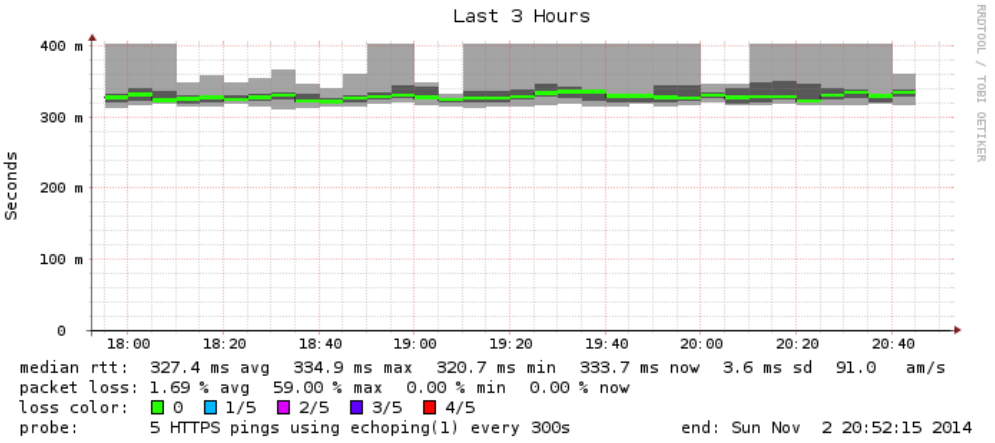

# DNS lookup for kheops from Google open DNS



# HTTP for Kheops




# HTTPs for Kheops




**Question #4 :**
En quoi peut-on dire que SmokePing est une généralisation de ping ?

## 2.1 Accès ADSL

Toutes les mesures effectuées passent au travers du lien d'accès ADSL. Voici un traceroute effectué depuis la machine.

```
g@~:traceroute www.google.fr
traceroute to www.google.fr (74.125.136.94), 64 hops max, 52 byte packets
 1  192.168.0.254 (192.168.0.254)  3.227 ms  1.499 ms  1.618 ms
 2  82.238.189.254 (82.238.189.254)  22.462 ms  22.608 ms  23.447 ms
 3  78.254.5.190 (78.254.5.190)  57.356 ms  28.126 ms  34.682 ms
 4  ant06-1-v902.intf.nra.proxad.net (78.254.254.154)  22.296 ms  21.869 ms  22.433 ms
```

```
 5  nice-6k-1-v900.intf.nra.proxad.net (78.254.254.158)  23.228 ms  22.856 ms  23.427 ms
 6  marseille-crs8-1-be1006.intf.routers.proxad.net (194.149.160.137)  26.911 ms  26.948 ms  28.392
 7  p11-crs16-1-be1102.intf.routers.proxad.net (78.254.249.6)  36.027 ms  35.220 ms  35.947 ms
 8  th2-9k1-be1001.intf.routers.proxad.net (78.254.249.6)  35.185 ms  36.780 ms  35.656 ms
 9  * ix-15-547.tcore1.pvu-paris.as6453.net (195.219.241.173)  76.658 ms  76.883 ms
10  * * *
11  72.14.239.145 (72.14.239.145)  88.513 ms  88.723 ms  91.281 ms
12  * * 209.85.245.81 (209.85.245.81) 86.731 ms
13  209.85.245.87 (209.85.245.87) 85.224 ms  86.358 ms
    216.239.51.112 (216.239.51.112)  87.183 ms
14  72.14.236.135 (72.14.236.135)  108.451 ms
    209.85.240.220 (209.85.240.220)  88.782 ms  98.841 ms
15  209.85.255.85 (209.85.255.85)  91.499 ms
    216.239.48.104 (216.239.48.104)  90.741 ms
    209.85.255.87 (209.85.255.87)  91.015 ms
16  216.239.49.38 (216.239.49.38)  90.906 ms
    216.239.49.28 (216.239.49.28)  92.234 ms
    216.239.49.38 (216.239.49.38)  91.763 ms
17  * * *
18  * ea-in-f94.1e100.net (74.125.136.94)  92.919 ms  91.183 ms
```

**Question #5 :**
Quel est le RTT sur le lien d'accès ADSL ?

**Question #6 :**
Comment ce résultat varie en fonction de l'accès ADSL d'après vous (opérateur, distance, qualité du lien) ?

## 2.2 DNS

**Question #7 :**
Qu'est-ce qu'un resolver DNS ?

**Question #8 :**
Quelle est la part de la latence d'accès au serveur par rapport au temps de résolution DNS du serveur ?

**Question #9 :**
Relier le temps de résolution en lui-même avec le schéma typique de résolution DNS.

**Question #10 :**
Y a-t-il du caching DNS ?

## 2.3 HTTP

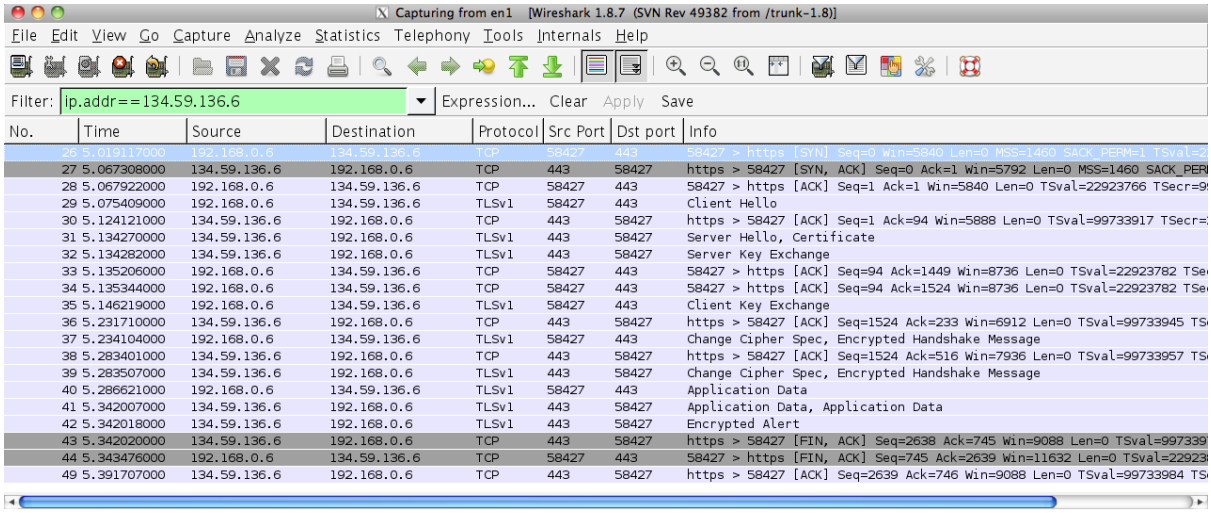
**Question #11 :**
Faites un diagramme temporel correspondant au téléchargement de l'objet demandé.

**Question #12 :**
Faites le lien entre le diagramme précédent, le temps de ping et le temps du HTTPping pour kheops.

## 2.4 HTTPs

**Question #13 :**
Quel est le surcout du HTTPs par rapport au HTTP ?

**Question #14 :**
Voici les traces wiresharks pour kheops. Relier le surcout en temps avec les échanges réseau et le temps de ping.




---

# 3 Analyse d'une trace de communication avec un serveur Web

Ouvrez la trace `http_espn.pcap` avec **Wireshark**. Il s'agit de trafic lié au téléchargement de la page d'entrée d'un site Web.

**Question #15 :**
Quelle est la composition de la trace en terme de protocoles UDP/TCP d'une part et d'applications au dessus de ces 2 couches transports d'autre part ? Utilisez la fonction *protocol hierarchy* du menu *statistics*.

Faire un filtre sur le port 80 TCP seulement. Réouvrir *protocol hierarchy*. On veut comprendre pourquoi la fraction de trafic HTTP est si faible alors que le port 80 est le port HTTP. Pour se faire, **analysez la connexion sur le port 38433**.

**Question #16 :**
A quoi servent les 3 premiers paquets TCP ?

**Question #17 :**
Combien d'objets sont demandés par le client ?

Analysez le contenu des paquets TCP *avec des données*, envoyés depuis le serveur vers le client en réponse à la requête HTTP (le GET).

**Question #18 :**
Où se situe le 200 OK dans les données ?
(Utilisez la sous-fenêtre d'en bas de Wireshark, pas la fenêtre intermédiaire.)

**Question #19 :**
Quelle trame Wireshark marque comme HTTP (dans la fenêtre intermédiaire) et quelles trames marque-t-il comme TCP ?

**Question #20 :**
Quelle est la logique derrière ce choix ?
(Réfléchissez comme un développeur...)

Effacez le filtre. Utilisez la fonction *conversations* du menu *statistics*.

**Question #21 :**
Combien il y a-t-il de conversations au niveau IP, TCP et UDP dans cette trace ?

**Question #22 :**
En analysant le niveau Ethernet, déduisez où est faite la capture et à quoi correspondent ces 2 adresses MAC.

Concentrons-nous maintenant sur le trafic DNS. Créez un filtre pour ne récupérer **que** *les demandes de résolutions DNS*. Pour cela, il faut se placer sur un paquet DNS où il y a une requête, puis sur le champ dans l'en-tête applicative où apparaît le code qui indique que c'est une requête et faire un *click droit* et *Prepare a Filter* puis *Selected*.

**Question #23 :**
Quel filtre a été créé ?

**Question #24 :**
Combien de demande de résolution DNS trouvez-vous ?
(Wireshark indique le nombre de paquets filtrés dans la barre en bas.)

Passons maintenant aux requêtes HTTP. Pour les trouver, nous allons utiliser la fonction *HTTP/Requests* du menu *Statistics*. Appuyez directement sur le bouton *Create Stats*.

**Question #25 :**
Interprétez les 2 premières colonnes du résultat ?

**Question #26 :**
En quoi ce résultat est compatible avec l'analyse DNS faite précédemment ?

**Question #27 :**
Créez un filtre pour calculer le nombre d'objets effectivement téléchargés (en filtrant sur le bon code réponse HTTP du serveur en utilisant à nouveau le *Prepare As* filtered puis *Selected*). Combien il y en a-t-il ?

**Question #28 :**
Expliquez la différence de 2 objets entre les questions #25 et #27 en regardant tous les codes réponses du serveur (et pas seulement les 200 OK).
(Ne tenez pas compte du troisième élément.)

# 4 Dépannage réseau

Vous êtes administrateur/ingénieur réseau. Un de vos utilisateurs n'arrive pas à accéder à Internet. En revanche, il arrive à accéder aux ressources internes (serveurs de données, mail, imprimantes, etc.). Vous avez capturé la trace `nowebaccess1.pcap` sur le commutateur d'attachement (swich) de la machine de l'utilisateur.

Quelques informations sur le réseau :

- l'adresse IP de la machine de l'utilisateur est 172.16.0.8 et les serveurs DNS configurés sur la machine sont 4.2.2.2 et 4.2.2.1 ;
- le réseau de l'entreprise se situe dans la plage d'adresse 172.16.0.0/24 ;
- ne tenez pas compte des messages[1] "bad internet checksum" au niveau IP.

**Question #29 :**
Que se passe-t-il dans la trace ?

**Question #30 :**
A votre avis, pourquoi l'utilisateur ne peut pas accéder à Internet ? Donnez-lui une explication possible du problème.

Un autre utilisateur se plaint de ne pas pouvoir accéder à certains sites Web (mais pas tous). Vous capturez à nouveau une trace de trafic qui s'appelle `nowebaccess3.pcap`.

**Question #31 :**
Que se passe-t-il dans la trace ?

**Question #32 :**
A votre avis, pourquoi l'utilisateur ne peut pas accéder à ce service en particulier ?

**Question #33 :**
Expliquez ce choix de configuration fait dans le réseau à l'utilisateur (de manière succinte).

1. Ils proviennent du fait que la capture s'est faite sur une machine où le calcul de la somme de contrôle est déporté sur la carte physique. Wireshark capture avant que ce soit effectué, et croit donc à un erreur dans le paquet.