


Lycée d'enseignement général et technologique international Victor Hugo COLOMIERS		
Architecture matérielle & OS	Les réseaux informatiques	
	Activité Pratique	
Nom : _____		Prénom : _____
		Date : _____

1 Objectifs

Découvrir et étudier :

- le concept de protocole réseau, le rôle et le fonctionnement des protocoles IP et TCP
- le modèle OSI et le concept d'encapsulation

2 Protocole, encapsulation et Modèle OSI

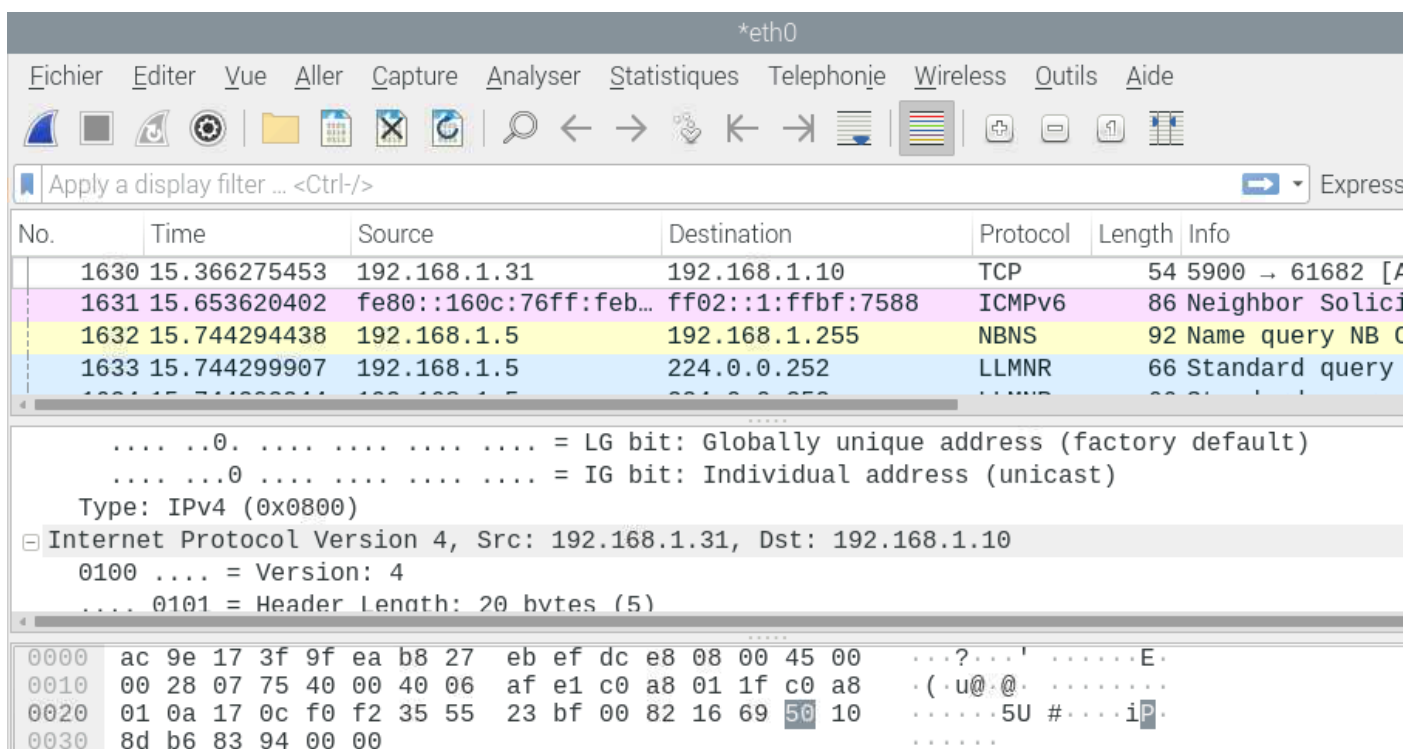
Nous allons illustrer ces trois concepts dans le contexte des réseaux informatiques. Pour rappel, ces concepts sont abordés dans le document intitulé « Cours_Decouverte_Réseaux_2019_V1.pdf ». Sa lecture est un prérequis pour les activités suivantes.

Nous utiliserons l'outil « Wireshark » dans la suite des activités pratiques proposées.




2.1 Découverte d'un analyseur de protocole

« Wireshark » est un analyseur de protocole (sniffer) gratuit et open-source, utilisable sur les systèmes Windows et Linux et MAC OS.

L'interface de « Wireshark » est constituée de trois fenêtres principales:



La fenêtre la plus haute liste les trames capturées dont elle résume les caractéristiques (une couleur par protocole). En cliquant sur une trame de cette fenêtre, vous modifiez le contenu des deux autres.

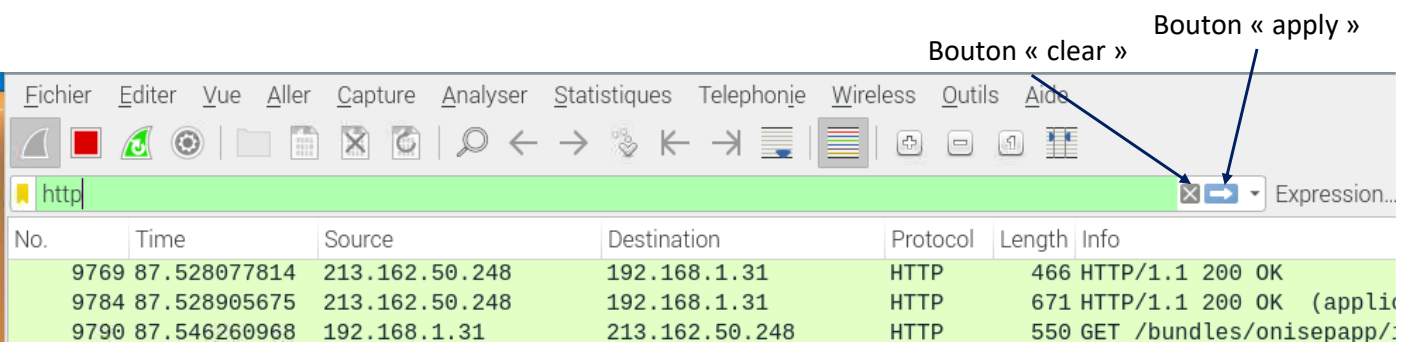
Lycée d'enseignement général et technologique international Victor Hugo COLOMIERS		
Architecture matérielle & OS	Les réseaux informatiques	
	Activité Pratique	

La fenêtre du milieu décrit précisément le contenu de la trame sélectionnée dans la fenêtre précédente. Les champs constituant la trame et les protocoles associés à chaque couche, ainsi que diverses informations fournies par le logiciel, y sont présentés dans une structure arborescente reprenant le modèle en couches OSI (ou le modèle TCP-IP suivant le nombre de couches présentes).

La fenêtre du bas contient les données (exprimées en hexadécimal) portées par la trame sélectionnée. Les champs sélectionnés dans l'arbre de la fenêtre du milieu y sont affichés surlignés.

Afin de ne pas afficher toutes les trames qui circulent sur le réseau, vous pouvez utiliser un filtre à la capture (Ex : l'analyseur ne capture que les trames issues de l'adresse IP 192.168.1.31 avec le protocole de transport UDP) ou un filtre à l'affichage (toutes les trames sont capturées mais seules les trames TCP sont affichées).

Le filtre d'affichage est plus simple d'emploi, il est activé à l'aide du bouton « Filtrer » sous la barre des icônes. Vous accédez alors à la boîte de dialogue dédiée à la construction de filtres d'affichage. La fenêtre à sa droite vous permet de composer un filtre directement ou d'en choisir un prédéfini. Attention, le filtre doit être activé en cliquant sur le bouton « Apply ». Un clic sur le bouton « Clear » désactive le filtre d'affichage en cours d'utilisation. L'aide intégrée (F1) explique la syntaxe des filtres d'affichage (section 6.3 « Filtering Packets While Viewing »).



Bouton « clear »

Bouton « apply »

No.	Time	Source	Destination	Protocol	Length	Info
9769	87.528077814	213.162.50.248	192.168.1.31	HTTP	466	HTTP/1.1 200 OK
9784	87.528905675	213.162.50.248	192.168.1.31	HTTP	671	HTTP/1.1 200 OK (appli
9790	87.546260968	192.168.1.31	213.162.50.248	HTTP	550	GET /bundles/onisepapp/:

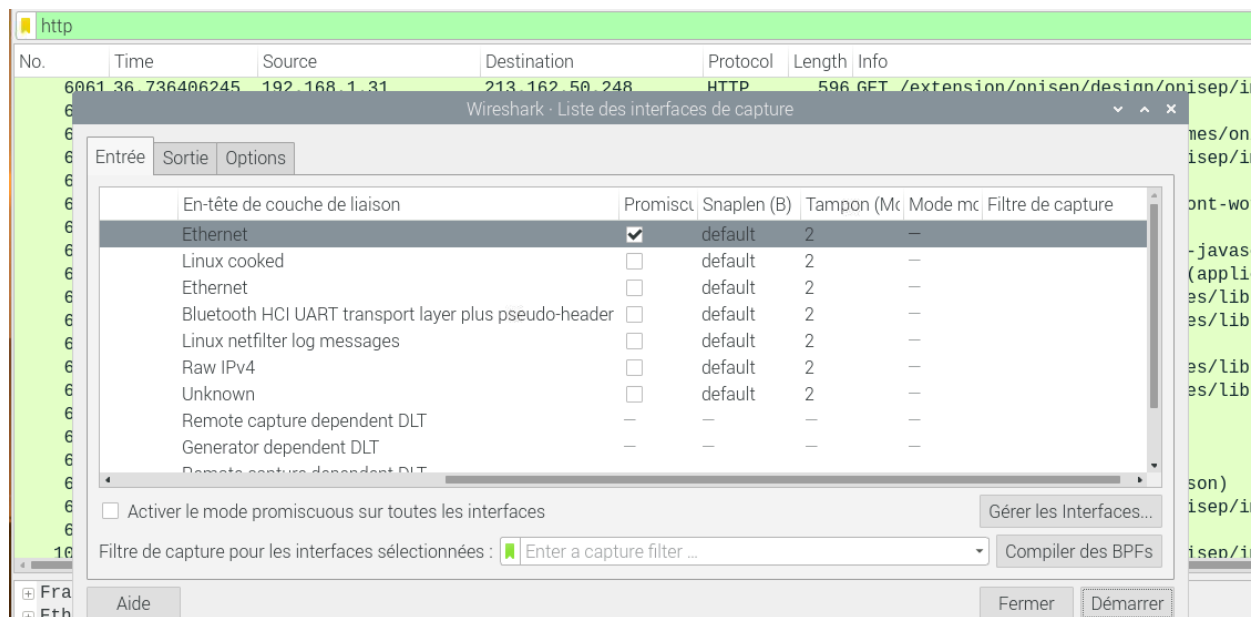
Pour lancer une capture, sélectionnez « Options » dans le menu « Capture ». La fenêtre « Capture options » s'affiche. Elle vous permet de définir les options à utiliser lors de la capture :

- interface sur laquelle est réalisée la capture
- utilisation d'un filtre de capture
- limitation du nombre de trames capturées
- durée de la capture,
- résolution de nom à l'affichage.

2.2 Analyse des couches du modèle OSI

a.

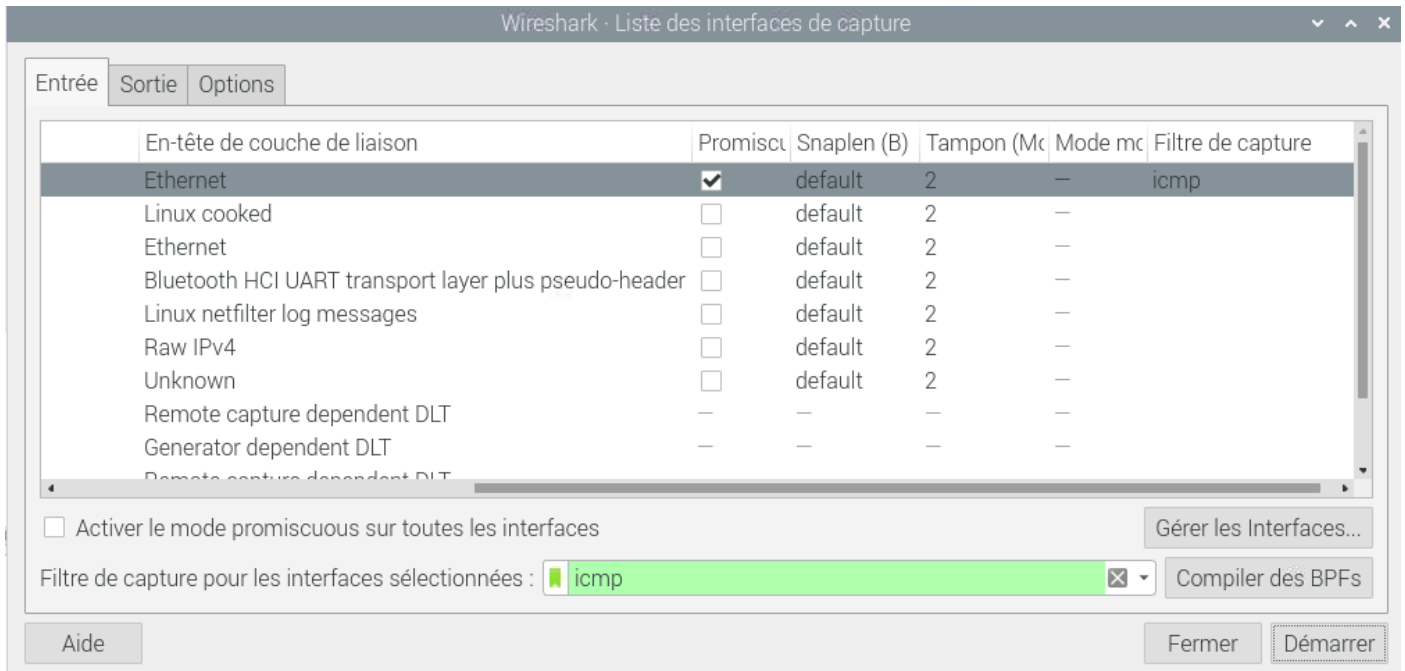
I. Configurer « Wireshark » de la façon suivante :



II. Démarrez la capture avec le bouton



III. Ouvrez le navigateur « Chromium » et rendez-vous sur le site internet de l'ONISEP en saisissant l'URL www.onisep.fr dans la barre d'URL



```
pi@raspberrypinsi:~ $ ping 192.168.1.11
PING 192.168.1.11 (192.168.1.11) 56(84) bytes of data.
64 bytes from 192.168.1.11: icmp_seq=1 ttl=128 time=0.637 ms
64 bytes from 192.168.1.11: icmp_seq=2 ttl=128 time=0.782 ms
64 bytes from 192.168.1.11: icmp_seq=3 ttl=128 time=0.668 ms
64 bytes from 192.168.1.11: icmp_seq=4 ttl=128 time=0.763 ms
64 bytes from 192.168.1.11: icmp_seq=5 ttl=128 time=0.923 ms
64 bytes from 192.168.1.11: icmp_seq=6 ttl=128 time=0.694 ms
64 bytes from 192.168.1.11: icmp_seq=7 ttl=128 time=0.696 ms
^C
--- 192.168.1.11 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 269ms
rtt min/avg/max/mdev = 0.637/0.737/0.923/0.093 ms
pi@raspberrypinsi:~ $
```



Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.11	192.168.1.11	ICMP	98	Echo (ping) request id=0x00000000
2	0.000550413	192.168.1.11	192.168.1.31	ICMP	98	Echo (ping) reply id=0x00000000
3	1.062903830	192.168.1.31	192.168.1.11	ICMP	98	Echo (ping) request id=0x00000000
4	1.063603929	192.168.1.11	192.168.1.31	ICMP	98	Echo (ping) reply id=0x00000000
5	2.102783332	192.168.1.31	192.168.1.11	ICMP	98	Echo (ping) request id=0x00000000
6	2.103402130	192.168.1.11	192.168.1.31	ICMP	98	Echo (ping) reply id=0x00000000
7	3.142865649	192.168.1.31	192.168.1.11	ICMP	98	Echo (ping) request id=0x00000000
8	3.143544187	192.168.1.11	192.168.1.31	ICMP	98	Echo (ping) reply id=0x00000000
9	4.182820837	192.168.1.31	192.168.1.11	ICMP	98	Echo (ping) request id=0x00000000
10	4.183687758	192.168.1.11	192.168.1.31	ICMP	98	Echo (ping) reply id=0x00000000
11	5.183918984	192.168.1.31	192.168.1.11	ICMP	98	Echo (ping) request id=0x00000000
12	5.184554866	192.168.1.11	192.168.1.31	ICMP	98	Echo (ping) reply id=0x00000000
13	6.262787838	192.168.1.31	192.168.1.11	ICMP	98	Echo (ping) request id=0x00000000
14	6.263425126	192.168.1.11	192.168.1.31	ICMP	98	Echo (ping) reply id=0x00000000

Checksum: 0x2da0 [correct]
[Checksum Status: Good]
Identifier (BE): 2270 (0x08de)
Identifier (LE): 56840 (0xde08)
Sequence number (BE): 1 (0x0001)
Sequence number (LE): 256 (0x0100)

```

0000  b8 27 eb ef dc e8 ac 9e 17 3f 9f ea 08 00 45 00  .'. . . . . ? . . . . E.
0010  00 54 56 08 00 00 80 01 61 26 c0 a8 01 0b c0 a8  .TV. . . . . a& . . . .
0020  01 1f 00 00 2d a0 08 de 00 01 99 4c 0a 5e 33 d3  . . . . . L.^3.

```


Victor Hugo

A faire vous-même : analyse d'un protocole

a. Appliquez un filtre d'affichage afin de ne visualiser que les trames contenant le protocole « http » puis lancez une capture. A l'aide du navigateur « Chromium », connectez-vous au site web « www.terminales2019-2020.fr ». Arrêtez la capture.

b. Développez dans la fenêtre du milieu le protocole « http ». Quelle est la première commande HTTP relevée ? A quoi correspond-elle ? Retrouvez dans l'en-tête http les différentes informations : nom du site demandé (URL), version du navigateur utilisé, langage accepté.

[illegible]



- c. Analysez la première réponse du serveur web interrogé. Quel est le type du serveur web ? Combien reste-t-il d'octets après l'en-tête http ? A quoi correspondent-t-il ?

.....
.....
.....
.....
.....

- d. Quel est l'intérêt d'indiquer dans l'en-tête http la date et l'heure et une information de type « Last-Modified » ?

.....
.....
.....
.....

Victor Hugo



Interaction
Homme-
Machine

Les réseaux informatiques

Activité Pratique

Victor Hugo

- b. A l'aide du cours sur les réseaux informatiques et de la commande « man ifconfig », répondez aux questions suivantes :

Quel est le rôle de la commande « ifconfig » ?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Si vous envoyez un PDU vers un autre système, quelle interface réseau sera utilisée ?

.....

.....

Quelle est votre adresse IP ?

.....

.....

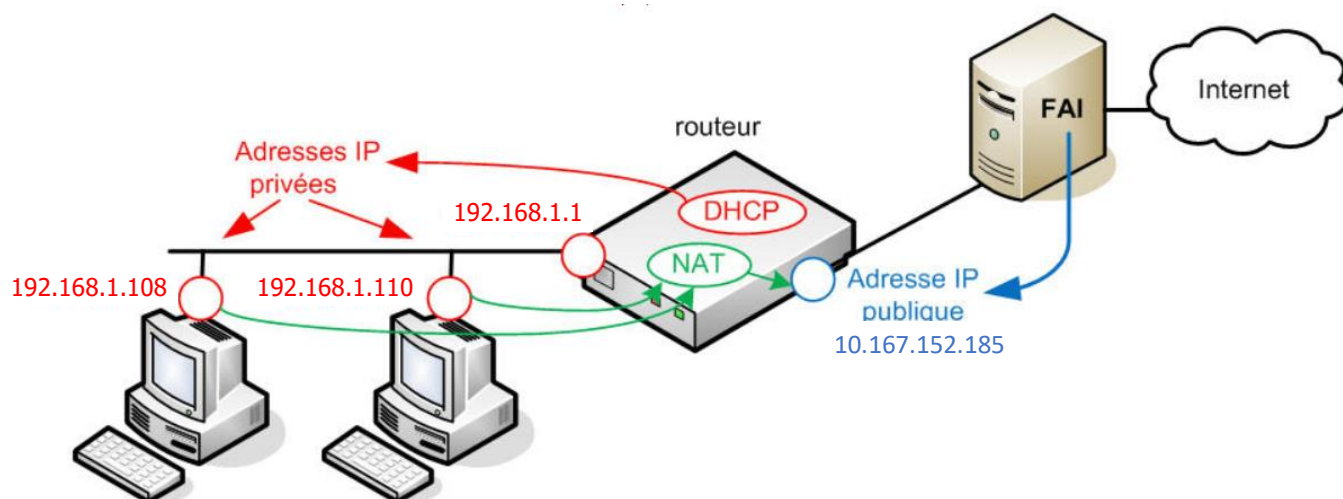
De quel type d'adresse s'agit-il ? Expliquez.

.....

.....

.....

.....





Interaction
Homme-
Machine

Les réseaux informatiques

Activité Pratique



Quelle est l'adresse de votre réseau ou sous-réseau ? Justifiez la valeur du masque.

.....

.....

L'adresse de votre routeur est 10.167.152.185. Quelle est sa classe ?

.....

.....

4 Test de connectivité

Vous allez tester la connectivité de votre machine au réseau en utilisant la commande « ping ».

- Afin de connaître la commande, entrez la commande « man ping »
- Vérifiez que le protocole IP est opérationnel sur votre machine en tapant la commande :
ping -c 3 « 127.0.0.1 ». Que signifie l'option « -c 3 » ?

.....

.....

.....

.....

- A l'aide d'internet, expliquez le résultat obtenu

.....

.....

.....

.....

- Comment pourriez-vous vérifier que votre adresse IP est opérationnelle à l'aide de la commande ping ? Comment évaluez-vous le résultat ?

.....

.....

.....

.....

- e. Que désigne le terme « passerelle ». La commande « route » vous permet d'obtenir l'adresse de votre passerelle. Quelle est cette adresse ? Parvenez-vous à l'atteindre ?

.....
.....
.....
.....
.....

- f. Comment pouvez-vous envoyer 5 paquets à une autre machine (celle d'un autre binôme ?) à l'aide de la commande ping ?



.....
.....
.....
.....
.....

- g. L'URL www.onisep.fr possède l'adresse IP « 213.162.50.248 ». Tentez de joindre ce serveur en lui envoyant 5 paquets « ECHO_REQUEST ». A quoi correspondent les valeurs de temps renvoyées lors de cette commande ? Comparez-les avec ceux constatés lors de la commande exécutée en f. Justifiez.

.....
.....
.....
.....
.....

- h. L'URL www.huawei.cn possède l'adresse IP « 185.176.76.132 ». Tentez de joindre ce serveur en lui envoyant 5 paquets « ECHO_REQUEST ». A quoi correspondent les valeurs de temps renvoyées lors de cette commande ? Comparez-les avec ceux constatés lors de la commande exécutée précédemment. Justifiez.

.....
.....
.....
.....
.....

Lycée d'enseignement général et technologique international Victor Hugo COLOMIERS		
Interaction Homme- Machine	Les réseaux informatiques	
	Activité Pratique	

- b. Identifiez et commentez la ligne indiquant comment joindre une machine de votre réseau local ainsi que la ligne indiquant comment joindre une machine distante.



.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

- c. La commande « traceroute » permet de suivre les chemins qu'un paquet de données (paquet IP) va prendre pour aller de la machine locale à une autre machine connectée au réseau IP. Relever l'itinéraire d'accès à une Raspberry Pi de la salle 113. Justifiez les valeurs obtenues.

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

- d. Relever l'itinéraire d'accès à www.onisep.fr et www.huawei.cn . Si besoin, utilisez la commande « traceroute -T + <adresse IP> ». Faites un « man traceroute » afin de comprendre l'option « -T ». Expliquez. Justifiez les valeurs obtenues.

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Lycée d'enseignement général et technologique international Victor Hugo COLOMIERS		
Interaction Homme- Machine	Les réseaux informatiques	
	Activité Pratique	

- e. Relevez l'adresse IP d'une machine qui appartient à un des deux itinéraires obtenus précédemment. Puis en vous rendant sur le site <http://www.ripe.net/whois>, taper l'adresse IP et analysez le résultat obtenu.

.....
.....
.....
.....
.....
.....

**** Fin du document ****