Sciences numériques et technologie

Classe de seconde, enseignement commun

■ Internet

Contenus	Capacités attendues
Protocole TCP/IP : paquets, routage des paquets	Distinguer le rôle des protocoles IP et TCP. Caractériser les principes du routage et ses limites. Distinguer la fiabilité de transmission et l'absence de garantie temporelle.
Adresses symboliques et serveurs DNS	Sur des exemples réels, retrouver une adresse IP à partir d'une adresse symbolique et inversement.
Réseaux pair-à-pair	Décrire l'intérêt des réseaux pair-à-pair ainsi que les usages illicites qu'on peut en faire.
Indépendance d'internet par rapport au réseau physique	Caractériser quelques types de réseaux physiques : obsolètes ou actuels, rapides ou lents, filaires ou non. Caractériser l'ordre de grandeur du trafic de données sur internet et son évolution.

Liens Internet :	
Ressources élèves :	https://www.cybermalveillance.gouv.fr/nos-articles/video-phishing/ https://www.youtube.com/watch?v=N1fCXk1wQAw https://www.youtube.com/watch?v=jYYjYaXCy7k https://www.youtube.com/watch?v=qlFE8UGMYZ0
Ressources professeurs :	https://www.cybermalveillance.gouv.fr/contenus-de-sensibilisation/ https://www.cybermalveillance.gouv.fr/nos-articles/video-phishing/

CC BY NC SA

Inspiré du site : https://pixees.fr/informatiquelycee/n_site/snt.html
Inspiré du guide de Daniel Garmann et JP Toureau
Modifiée par Philippe PERENNES - pperennes@ac-caen.fr

Sciences numériques et technologie Classe de seconde, enseignement commun	THEME : Internet Activité : simulation des réseaux Capacités attendues : Distinguer le rôle des protocoles IP et TCP Caractériser les principes de routage et ses limites Sur des exemples réels, retrouver une adresse IP à partir d'une adresse symbolique et inversement	*Fiche élève* *Page 1/4*

ETAPE 1 : Qu'est-ce que l'hameçonnage ? ou phishing en anglais ?

Regarder la vidéo :

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

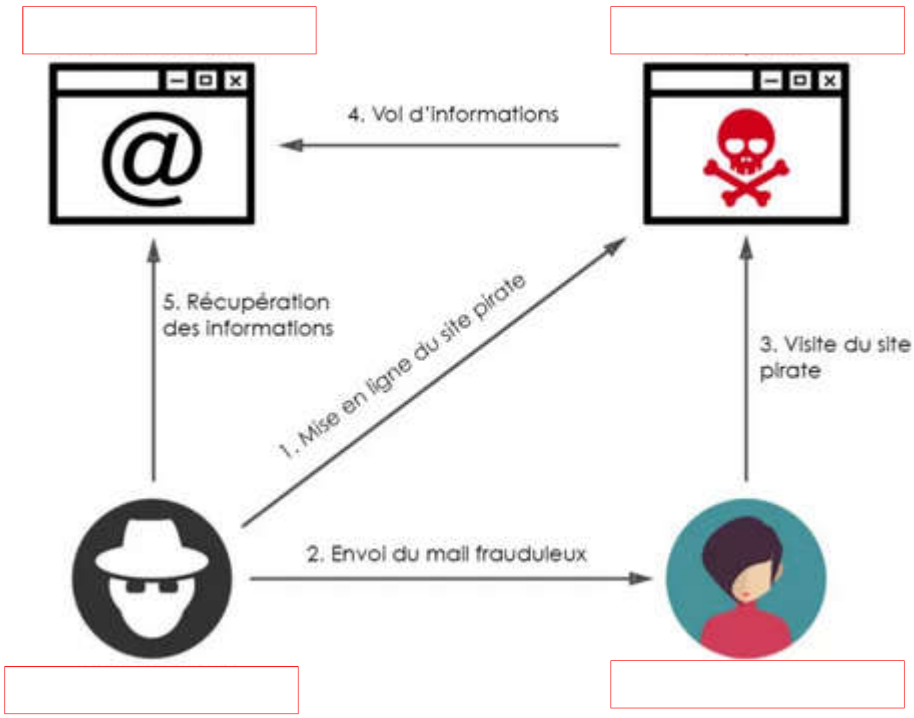
https://www.cybermalveillance.gouv.fr/nos-articles/video-phishing/

Quelle action de l'utilisateur peut déclencher cet hameçonnage ?

_____

_____

Compléter le dessin ci-dessous :



https://i1.wp.com/visionarymarketing.fr/blog/wp-content/uploads/2016/06/capture-d-ecran-06-57-2016_01.57.52.png?resize=584%2C469&ssl=1

Regarder la vidéo exemple :

https://www.youtube.com/watch?v=_iqoFbVLUHY

Que se passe-t-il dans cet exemple ? Est-ce que l'utilisateur s'en est rendu compte ?

_____

_____

ETAPE 2 : Lire l'article ci-dessous :

https://lexpansion.lexpress.fr/high-tech/piratage-des-noms-de-domaine-internet-subit-une-attaque-inedite_2063749.html

https://www.futura-sciences.com/tech/actualites/securite-tout-ce-vous-devez-savoir-piratage-dns-75150/

Expliquer de quel type d'attaque il s'agit :

_____

_____

_____

ETAPE 3 : Nous allons simuler une attaque du serveur DNS de Facebook : (schéma simplifié on image de nombreux routeurs—on en place un seul dans ce schéma)

Panique sur le web ce matin : Facebook était inaccessible suite à une panne de DNS touchant principalement l'Europe. Depuis 7h20 ce matin, impossible de se connecter sur son compte Facebook, du moins sur la version Internet du site puisque sa version mobile fonctionnait correctement. Heureusement, le bug est désormais réglé.

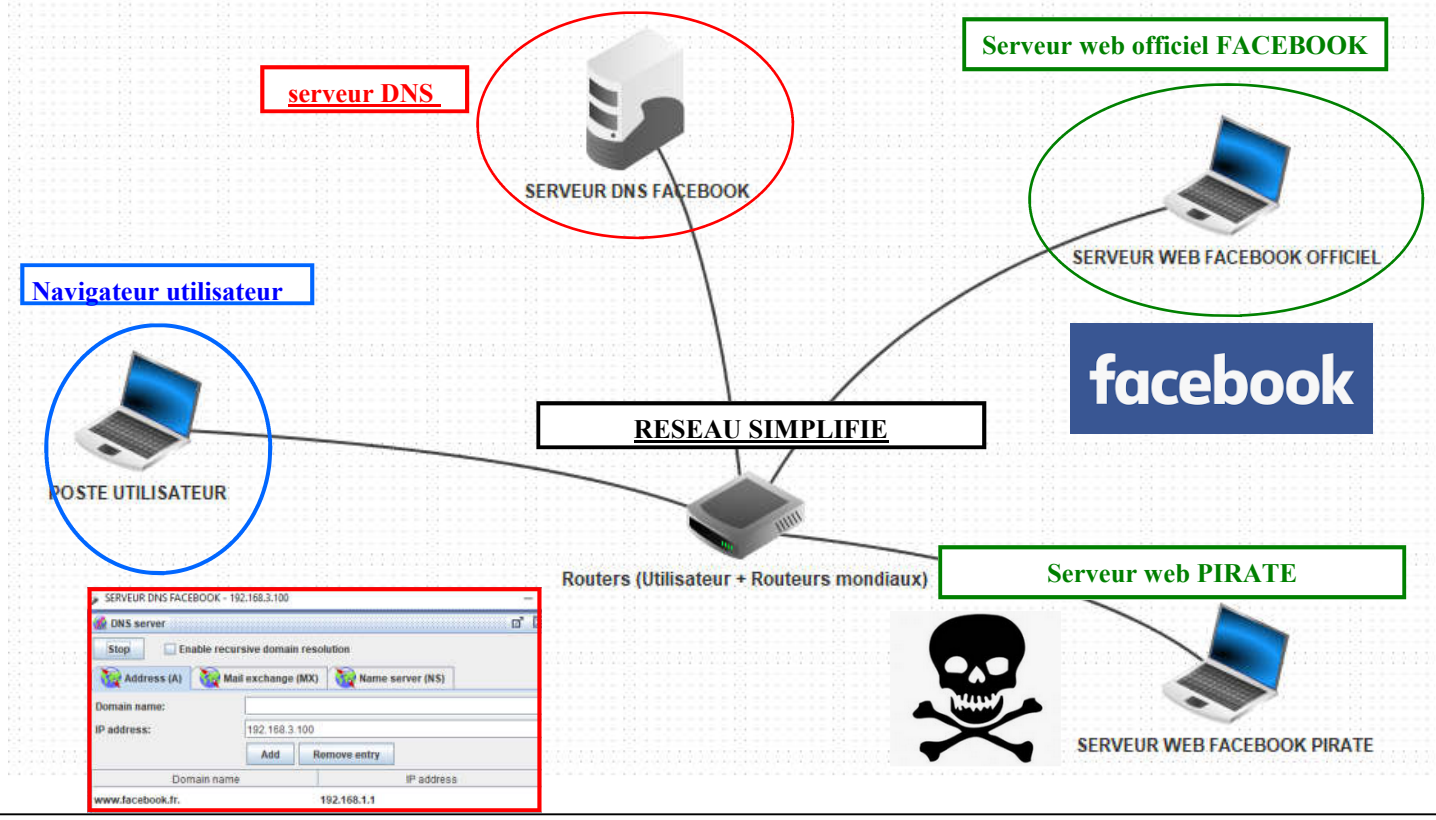
https://www.terrafemina.com/culture/culture-web/articles/11601-panne-de-dns-pour-facebook.html

Pour cela nous allons reprendre le schéma réseau ci-dessous :

Name	POSTE UTILISATEUR
MAC Address	11:3F:B4:CD:D6:23
IP address	192.168.0.1
Netmask	255.255.255.0
Gateway	192.168.0.254
Domain Name Server	192.168.3.100

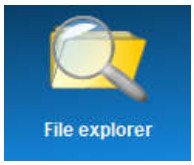
Name	SERVEUR DNS
MAC Address	12:13:4E:40:CD:17
IP address	192.168.3.100
Netmask	255.255.255.0
Gateway	192.168.3.254

Name	SERVEUR WEB FACEBOOK OFFICIEL
MAC Address	48:1C:72:59:5A:B5
IP address	192.168.1.1
Netmask	255.255.255.0
Gateway	192.168.1.254
Domain Name Server	192.168.3.100

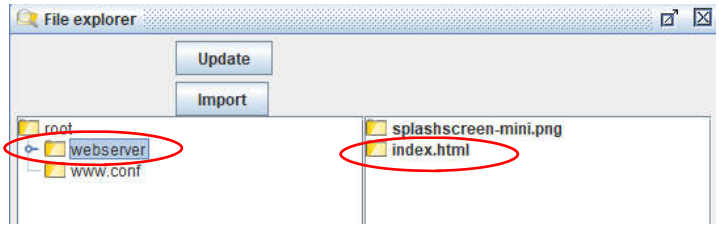


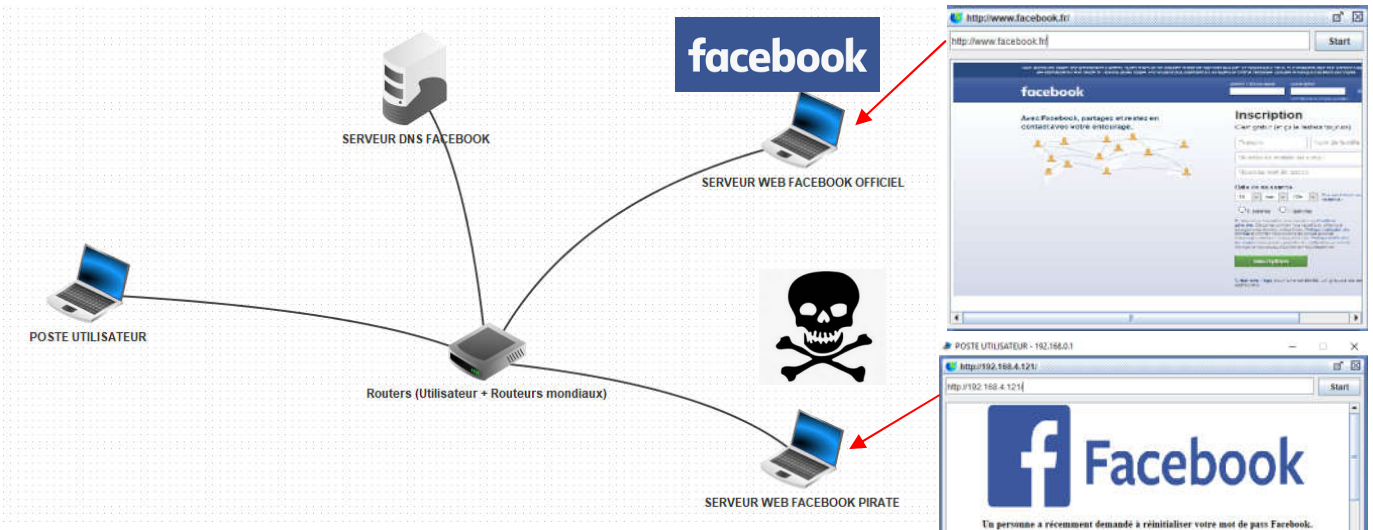
ETAPE 4 : Déposer les pages web sur les 2 serveurs web :

Installer sur les 2 postes - **serveur web** et **gestionnaire de fichiers**



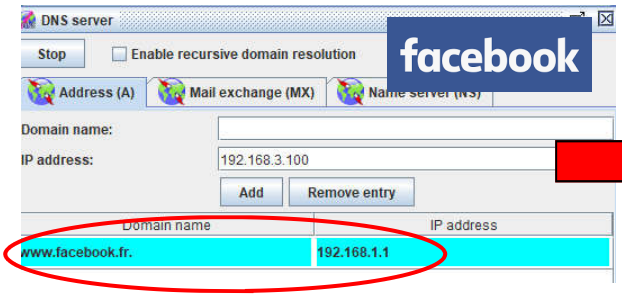
Grace au gestionnaire de fichiers déposer les pages web **index.html** dans **le serveur web**

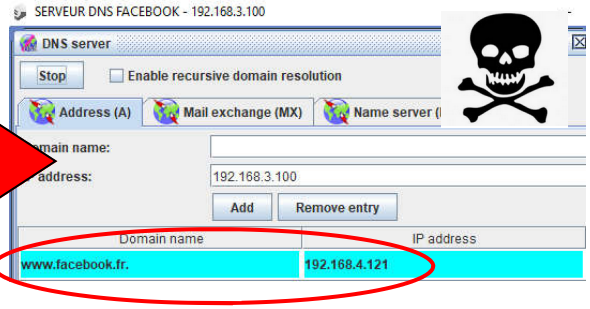




ETAPE 5 : Changer les paramètres du serveur DNS :

Association de _____ avec le serveur pirate _____





Faire le test sur le poste utilisateur avec le nom de domaine : www.facebook.fr

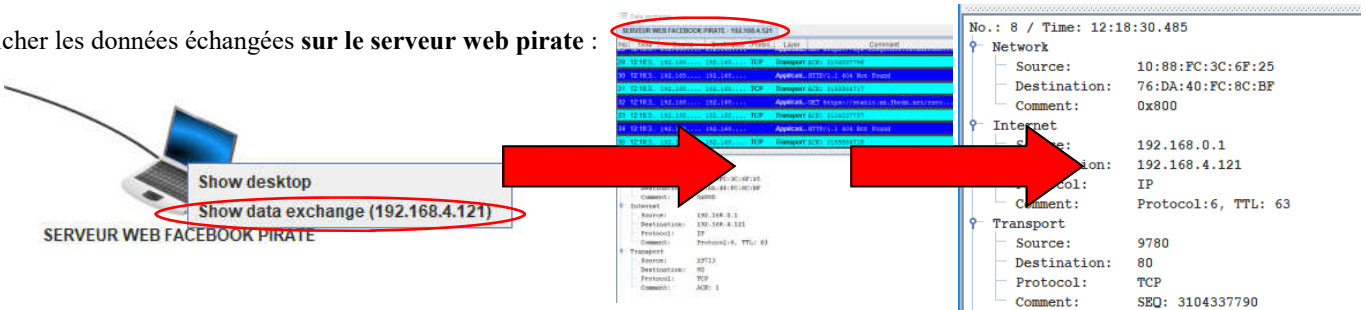
Synthèse :

La page web du nom de domaine www.facebook.fr est maintenant _____ grâce au _____ vers la page web _____.

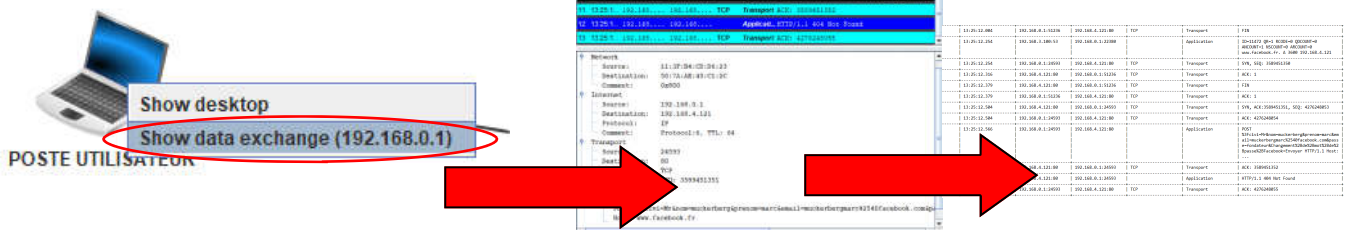
Nous allons pouvoir maintenant **récupérer les codes de connexion facebook de l'utilisateur.**

ETAPE 5 : Comment récupérer les codes de connexion facebook en analysant les couches réseaux :

Afficher les données échangées **sur le serveur web pirate** :



Afficher les données échangées **sur le poste utilisateur** :



Sur la couche **application POST** récupérer **les informations de connexion** :

Application	POST %3Fcivi=Mr&nom=muckerberg&prenom=marc&email=muckerbergmarc%2540facebook.com&passe=fondateur&Changement%2Bde%2Bmot%2Bde%2Bpasse%2BFacebook=Envoyer HTTP/1.1 Host: ...

&nom=muckerberg&prenom=marc&email=muckerbergmarc%2540facebook.com&passe=fondateur&C

Retrouver les informations de connexion :

Civilité : ○ Madame ○ Mademoiselle ○ Monsieur

Nom : Votre nom :

Prénom : Votre prénom :

Email : Votre email :

Mot de passe de connexion : Votre mot de passe :

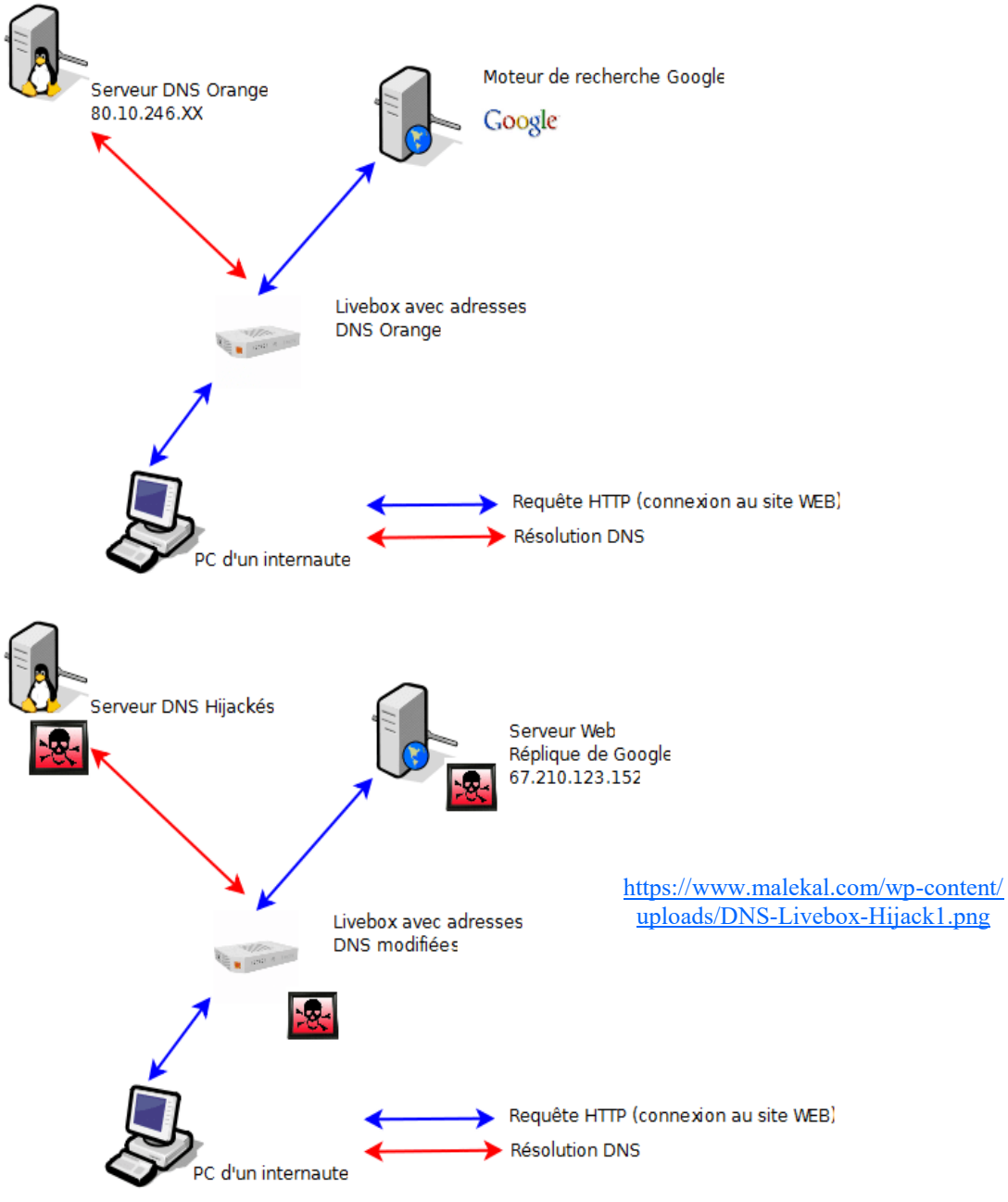
Historique Facebook :

Mark Elliot Zuckerberg, né le 14 mai 1984 à White Plains (État de New York), est un informaticien et chef d'entreprise américain. Il est le cofondateur du site web de réseau social Facebook dont il est le président-directeur général. Facebook a été créé en 2004 par Zuckerberg

Sciences numériques et technologie Classe de seconde, enseignement commun	THEME : Internet Activité : simulation des réseaux Capacités attendues : Distinguer le rôle des protocoles IP et TCP Caractériser les principes de routage et ses limites Sur des exemples réels, retrouver une adresse IP à partir d'une adresse symbolique et inversement	RESSOURCE 1

LE SERVEUR DNS :

ATTAQUE DU SERVEUR DNS :



https://www.malekal.com/wp-content/uploads/DNS-Livebox-Hijack1.png

PAGE WEB PIRATE—METHOD POST :

```
<form name="Changement de mot de passe Facebook" action="http://www.facebook.fr" method="get">
<center>
<img src="https://dyw7ncnq1en5l.cloudfront.net/optim/news/46/46727/f_facebook.png" align="center" height="150"
width="470">

<center>
<p>
        <b>Un personne a récemment demandé à réinitialiser votre mot de pass Facebook.</b>
</p>

<p>
        <b>Vous n'avez pas demandé ce changement ?</b>
</p>
<p>
        Changer de suite votre mot de passe
</p>
<p>
  <input type="radio" name="civi" value="Mme" /> Madame
  <input type="radio" name="civi" value="Mlle" /> Mademoiselle
  <input type="radio" name="civi" value="Mr" /> Monsieur
</p>
<p>
  Votre nom :<br />
  <input type="text" name="nom" value="" />
</p>
<p>
  Votre prénom :<br />
  <input type="text" name="prenom" value="" />
</p>
<p>
  Votre email :<br />
  <input type="text" name="email" value="" />
</p>
<p>
  Votre mot de passe :<br />
  <input type="password" name="passe" value="" />
</p>
<p>
  Confirmer votre mot de passe :<br />
  <input type="repassword" name="repasse" value="" />
</p>
<p>
  <input type="submit" value="Envoyer" />
  <input type="reset" value="Annuler" />
</p>
<a href="https://fr-fr.facebook.com/">Facebook © 2019</a>
        <img src="https://static.xx.fbcdn.net/rsrc.php/v3/yi/r/OBaVg52wtTZ.png" align="center">
<a href="https://fr-fr.facebook.com/">Facebook © 2019</a>
</form>
```

Sciences numériques et technologie Classe de seconde, enseignement commun	**THEME : Internet** **Activité : simulation des réseaux** **Capacités attendues :** **Distinguer le rôle des protocoles IP et TCP** **Caractériser les principes de routage et ses limites** **Sur des exemples réels, retrouver une adresse IP à partir d'une adresse symbolique et inversement**	*RESSOURCE 3*

No.	Time	Source	Destination	Protocol	Layer	Comment
1	13:25:12.004	192.168.0.1:22380	192.168.3.100:53		Application	ID=11472 QR=0 RCODE=0 QDCOUNT=1 ANCOUNT=0 NSCOUNT=0 ARCOUNT=0 www.facebook.fr. A IN
2	13:25:12.004	192.168.0.1:51236	192.168.4.121:80	TCP	Transport	FIN
3	13:25:12.254	192.168.3.100:53	192.168.0.1:22380		Application	ID=11472 QR=1 RCODE=0 QDCOUNT=0 ANCOUNT=1 NSCOUNT=0 ARCOUNT=0 www.facebook.fr. A 3600 192.168.4.121
4	13:25:12.254	192.168.0.1:24593	192.168.4.121:80	TCP	Transport	SYN, SEQ: 3589451350
5	13:25:12.316	192.168.4.121:80	192.168.0.1:51236	TCP	Transport	ACK: 1
6	13:25:12.379	192.168.4.121:80	192.168.0.1:51236	TCP	Transport	FIN
7	13:25:12.379	192.168.0.1:51236	192.168.4.121:80	TCP	Transport	ACK: 1
8	13:25:12.504	192.168.4.121:80	192.168.0.1:24593	TCP	Transport	SYN, ACK:3589451351, SEQ: 4276248053
9	13:25:12.504	192.168.0.1:24593	192.168.4.121:80	TCP	Transport	ACK: 4276248054
10	13:25:12.566	192.168.0.1:24593	192.168.4.121:80		Application	POST %3Fcivi=Mr&nom=muckerberg&prenom=marc&email=muckerbergmarc%2540facebook.com&pass=fondateur&Changement%2Bde%2Bmot%2Bde%2Bpasse%2BFacebook=Envoyer HTTP/1.1 Host: ...
11	13:25:12.816	192.168.4.121:80	192.168.0.1:24593	TCP	Transport	ACK: 3589451352
12	13:25:12.879	192.168.4.121:80	192.168.0.1:24593		Application	HTTP/1.1 404 Not Found
13	13:25:12.879	192.168.0.1:24593	192.168.4.121:80	TCP	Transport	ACK: 4276248055