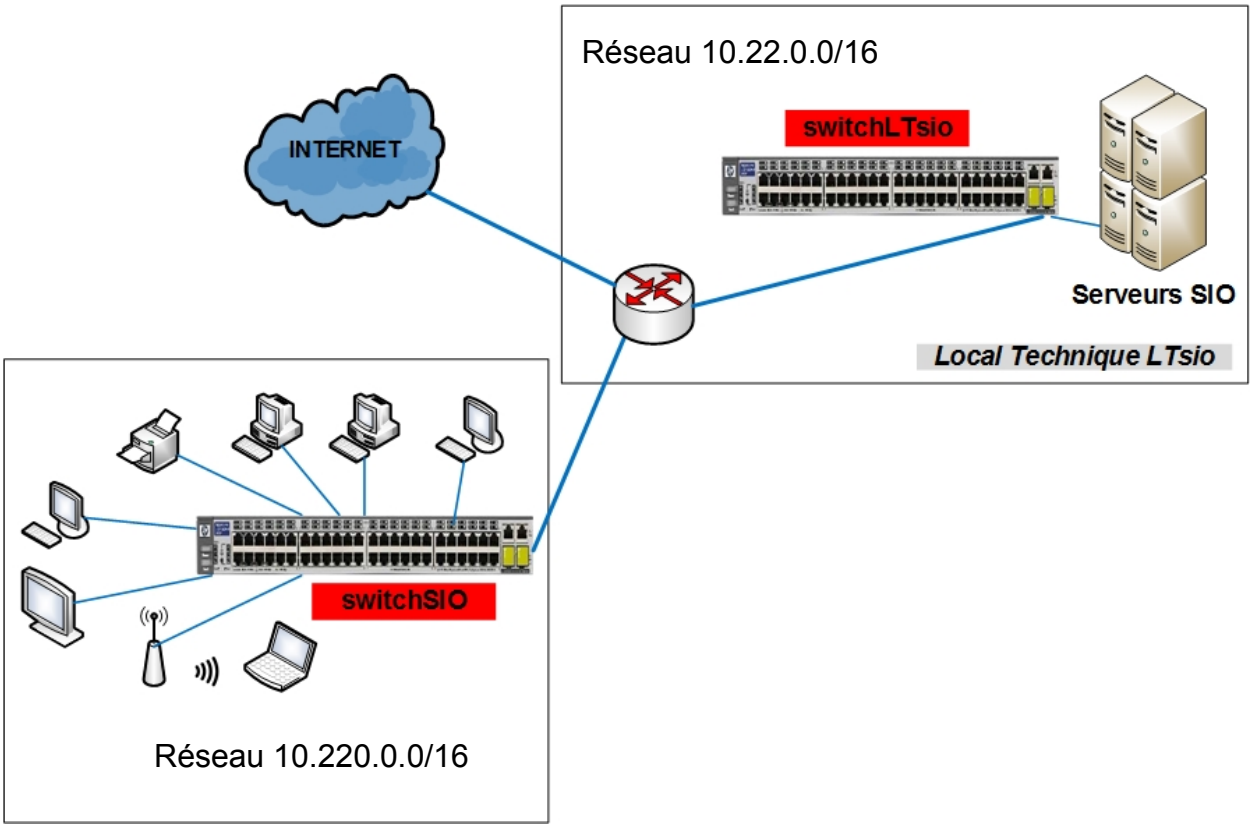
TP 5.2 Service et transport de paquets – Activité pratique
Analyse de la communication entre un client et un serveur FTP

Contexte de travail

Les serveurs (machines virtuelles) sont situées dans la ferme des serveurs dans le local technique des BTS SIO.

L'étudiant a accès à un serveur d'adresse IP 10.22.30.100 sur lequel il trouvera notamment le service FTP déjà configuré.



Les postes clients (postes Windows Seven et Ubuntu) sont situés dans la classe et disposent :

- d''un navigateur comme chrome ou firefox
- d'une application cliente FTP comme filezilla
- d'un outil sniffer : Wireshark

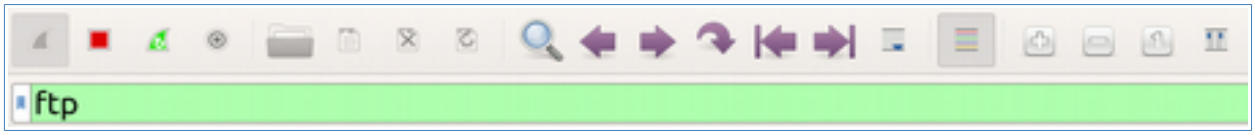
Le serveur FTP configuré n'est pas accessible de manière anonyme mais avec le compte « ***btssio*** » qui a pour mot de passe « ***mdpbtssio*** ». Un fichier nommé « ***texteSecret.txt*** » a été déposé dans le dossier « ftp ».

L'échange entre le client et le serveur FTP pour récupérer ce fichier va faire l'objet d'une analyse de trame.

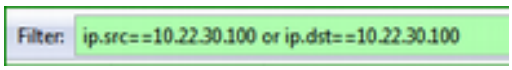
1 Préparation de l'analyse de trame

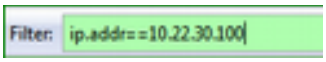
Sur votre poste client, lancez Wireshark.

Pour limiter le nombre de trames capturées, il vaut mieux restreindre les trames que l'on veut afficher en mettant en place un filtre dans l'analyseur de trame ; par exemple, si l'on veut filtrer les trames « FTP » ou incluant les transferts de données FTP « ftp or ftp-data » :

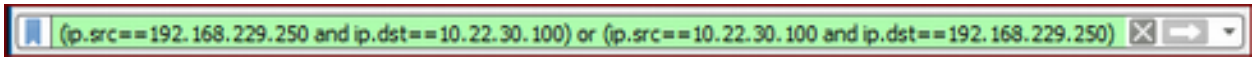


Ou pour ne visualiser que les communication ip avec un serveur d'adresse 10.22.30.100.





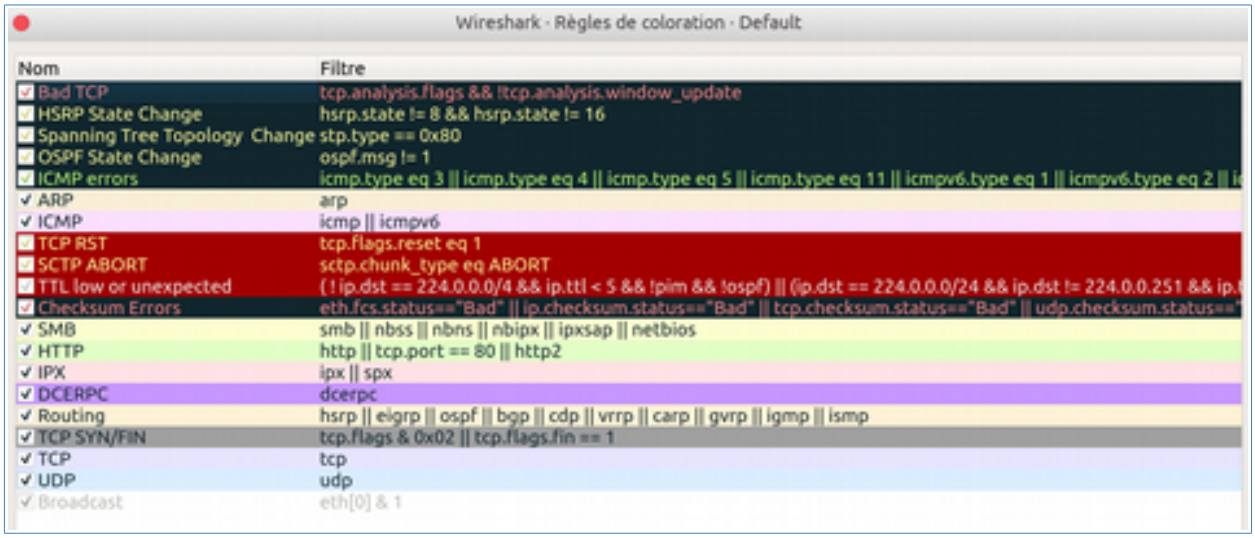
Ou encore uniquement entre une adresse IP (192.168.229.250) et le serveur d'adresse 10.22.30.100.



Ou plus simplement (pas très algorithmique mais équivalent au filtre précédent sous wireshark)

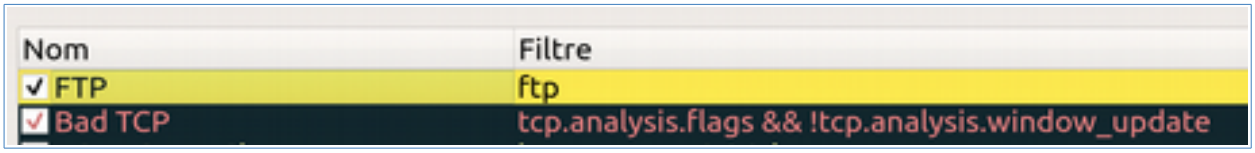
De nombreuses trames sont enregistrées. Afin de mettre en évidence certaines trames ou types de trames, il est possible d'ajouter (et/ou de modifier) des couleurs à celles déjà assignées par défaut.

On accède aux couleurs via le menu « Vue » puis « *Coloring Rules* » *:*



Par défaut les trames FTP sont colorées en gris clair comme n'importe quelle trame TCP spécifique (HTTP, en revanche, est distingué), nous allons donc les différencier par une autre couleur :

1. *Cliquez sur le « + » en bas à gauche de la fenêtre pour ajouter une règle de coloration* ⇒ ***Une nouvelle ligne vient s'insérer avant toutes les autres.*** Quand une ligne est sélectionné, il est possible de la modifier.
2. *Remplacer « New coloring rule » par le nom de la nouvelle règle (par exemple* ***FTP****).*
3. *Saisissez « ftp » dans la colonne « filtre ».*
4. *Choisissez une couleur de fond (jaune fluo par exemple) (et éventuellement une couleur de police.*



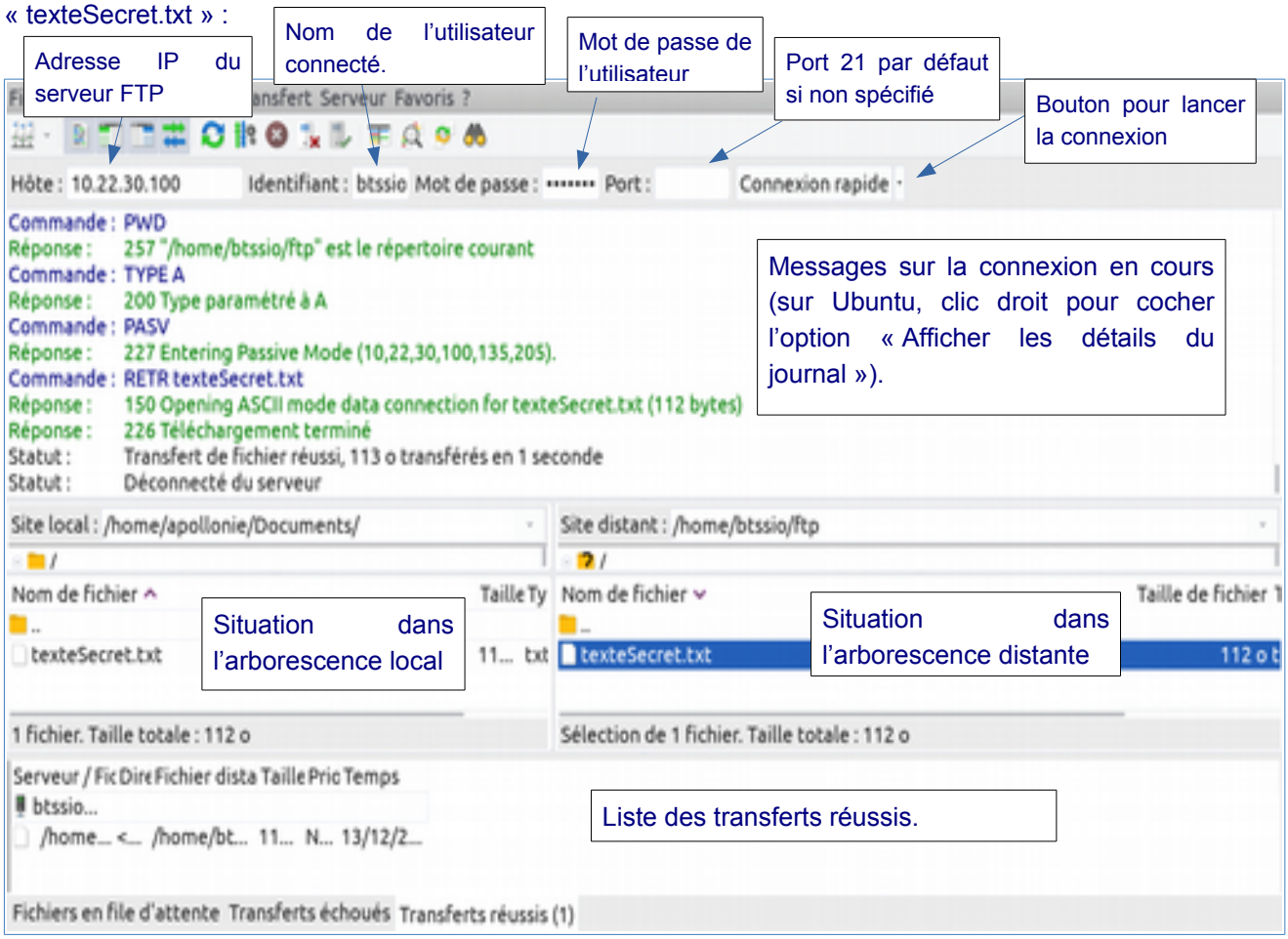
5. *Cliquez sur OK pour valider.*

2 L'échange FTP et l'écoute d'une connexion FTP

- Démarrez la capture de trame **juste avant** de vous connecter au serveur FTP (voir ci-après)

- À partir d'un client FileZilla :
  - Connectez-vous au serveur FTP (la capture de trame doit démarrer à ce moment **juste avant).**
  - Transférez le fichier "texteSecret.txt" présent dans le répertoire "ftp".

La copie d'écran ci-dessous montre l'interface du client FileZilla après « download » du fichier « texteSecret.txt » :



- Stopper la capture de trame lorsque le transfert est terminé.

- Enregistrez votre capture (captureFTP) afin de pouvoir y revenir si besoin.

- Repérez les trames de connexion du service FTP et du même coup les quelques trames qui précèdent ((commandes FTP : USER et PASS), comme le montre l'extrait sur la figure suivante) :

Source	Destination	Protocol	Lengt	Info
10.220.203.1	10.22.30.100	TCP	74	33410 → 21 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_
10.22.30.100	10.220.203.1	TCP	74	21 → 33410 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS
10.220.203.1	10.22.30.100	TCP	66	33410 → 21 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=12
10.22.30.100	10.220.203.1	FTP	124	Response: 220 ProFTPD 1.3.5b Server (Debian) [::ffff:
10.220.203.1	10.22.30.100	TCP	66	33410 → 21 [ACK] Seq=1 Ack=59 Win=29312 Len=0 TSval=1
10.220.203.1	10.22.30.100	FTP	76	Request: AUTH TLS
10.22.30.100	10.220.203.1	TCP	66	21 → 33410 [ACK] Seq=59 Ack=11 Win=29056 Len=0 TSval=
10.22.30.100	10.220.203.1	FTP	98	Response: 500 commande AUTH non comprise
10.220.203.1	10.22.30.100	FTP	76	Request: AUTH SSL
10.22.30.100	10.220.203.1	FTP	98	Response: 500 commande AUTH non comprise
10.220.203.1	10.22.30.100	FTP	79	Request: USER btssio
10.22.30.100	10.220.203.1	FTP	103	Response: 331 Mot de passe requis pour btssio
10.220.203.1	10.22.30.100	FTP	82	Request: PASS mdpbtssio
10.22.30.100	10.220.203.1	FTP	103	Response: 230 Utilisateur btssio authentifi\303\251

La correction qui suit est faite en fonction de l'analyse de trame représentée ci-dessus.

Préalable : Adresses IP et adresses MAC utilisées

Q1. Complétez le tableau ci-dessous retraçant les adresses IP et adresses MAC utilisées lors de l'échange en ce qui concerne les 2 premières trames ? *Vous fournirez toutes les explications nécessaires quant aux adresse MAC utilisées.*

	Trame 1		Trame 2	
	IP/MAC	Matériel correspondant	IP/MAC	Matériel correspondant
IP source				
IP destination				
Mac source				
Mac dest.				

Les premières requêtes TCP

Q2. Combien de requêtes TCP ont eu lieu avant l'instruction USER ?

Q3. De quoi s'agit-il ?

Q4. Sélectionnez chaque trame TCP et complétez le tableau ci après.

		@IP	**Port**	**FLAG**	**N° Séquence**	**N° ACK**
Trame 1	Source					
	Dest					
Trame 2	Source					
	Dest					
Trame 3	Source					
	Dest					

Q5. Dans la première trame, par quelle valeur en Hexa est représentée le port destination du service FTP ? Expliquez à quoi cela correspond.

L'échange FTP : la connexion au serveur FTP

Q6. Combien de requêtes FTP ont eu lieu avant l'instruction USER ? Qui s'adresse à qui ?

Q7. Voit-on le nom de l'utilisateur en clair (pour la commande USER) ?

Q8. Quelle est la réponse du serveur FTP à la commande USER ?

Q9. Voit-on le mot de passe de l'utilisateur en clair (dans la commande PASS) ?

Q10. Quelle est la réponse du serveur FTP à la commande PASS ?

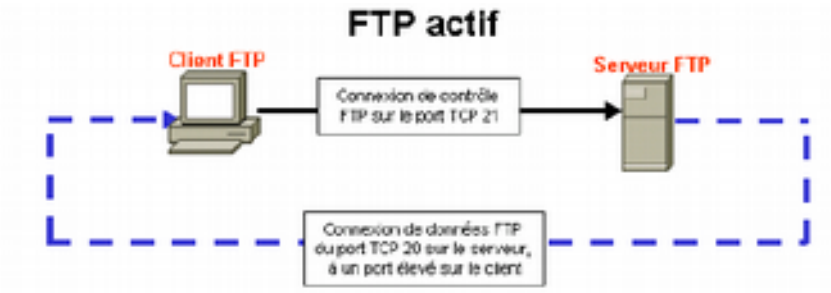
Q11. Y a-t-il d'autres trames qui s'intercalent entre les requêtes FTP ? Si oui, À quoi correspondent-elles ?

Remarque : Un client FTP s'authentifie toujours auprès du serveur FTP, même si l'authentification est ouverte à tout le monde. Dans ce dernier cas, un utilisateur anonyme (en règle générale nommé « Anonymous ») est utilisé par défaut.

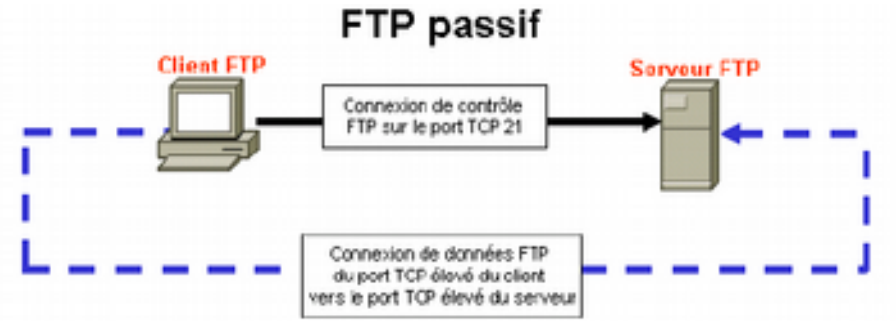
L'échange FTP : le transfert de données

Lors du transfert de données ou avec une simple liste de répertoires, un nouveau port est ouvert. Il s'agit du mode de transfert. **Ce mode peut être actif ou passif**.

En mode de transfert actif, un client démarre une session FTP avec le serveur sur le port 21 standard de TCP. Pour le transfert des données, le serveur lance une connexion à partir du port 20 standard de TCP vers un port élevé d'un client, un numéro de port supérieur à 1023.



En mode de transfert passif, un client démarre une session FTP avec le serveur sur le port 21 standard de TCP. Il s'agit de la même connexion utilisée en mode de transfert actif. Pour le transfert des données, cependant, deux modifications majeures interviennent. Dans ce mode, **c'est le client** (et pas le serveur) **qui établit la connexion** des données avec le serveur. Et des ports élevés sont utilisés aux deux extrémités de la connexion.



Cette nouvelle connexion FTP nécessaire à l'échange de données véhicule des trames « FTP-DATA ».

De manière à les mettre en évidence, colorer les trames FTP-DATA en mauve.

Q12. Combien de trames FTP-DATA contient votre analyse de trame ? Qui s'adresse à qui ?

Q13. Quel est le contenu de cette (ces) trame(s) ?

Wireshark intègre des « facilités » pour analyser les trames. Via le menu *Analyser/Suivre/Flux*, il est aussi possible d'avoir une analyse visuelle et rapide du contenu des trames.

Q14. Quelles adresses IP source et destination avec quels ports source et destination sont utilisés lors de l'envoi du fichier pour la commande FTP DATA ?

Q15. S'agit-il d'un transfert en mode « actif » ou « passif ». Justifiez votre réponse.

Q16. Pourquoi le(s) trame(s) FTP-DATA sont-elles aussi précédées de trois trames TCP ?

Q17. Examinez plus particulièrement une trame, par exemple la trame du transfert du fichier texte.
a) Quel est le 1er en-tête ? que contient-il ?

b) Quel est le second en-tête ? que contient-il ?

c) Quel est le troisième en-tête ? que contient-il ?

d) En déduire quoi est encapsulé dans quoi et comment fonctionne l'encapsulation.

Les dernières requêtes TCP (fermeture de la connexion)

il est possible de fermer un échange FTP à l'aide d'une connexion en trois ou quatre étapes. Quand une machine n'a plus de données à envoyer, elle envoie un segment FIN à l'autre machine (ce FIN peut aussi être accompagné d'un ACK). Si cette dernière n'a plus de données à envoyer, elle peut répondre soit avec 2 trames (un segment ACK puis par un autre segment FIN, ACK) soit par une seule trame définissant les indicateurs FIN et ACK . La première machine à l'origine de la fermeture de connexion répond alors par un segment ACK.

Q18. À quoi reconnaissez-vous les requêtes de fermeture de connexion ?

Q19. À l'issue du transfert de fichier, qui est à l'origine de la fermeture de session ?

Q20. À l'issue du transfert du fichier, combien y a-t-il de requête pour la fermeture de connexion ?

Q21. Complétez le diagramme de séquence ci-dessous illustrant les trames de fermeture de session

Ordinateur client Ordinateur Serveur