EXAMEN, BASES DES RESEAUX M2102

Nom..... Prénom..... Groupe.....

<u>Consignes</u> : vous avez 1 heure et demi (1h 30 min) pour répondre aux questions ci-dessous.

Vous avez le droit aux imprimés des CMs (avec des notes pertinentes aux cours) de ce module et le bouquin Récapitulation Réseaux, mais rien d'autre en tant que matériel supplémentaire. Ceci veut dire en particulier : pas de sac-à-dos, pas de portable, pas de calculatrice, pas de téléphone portable. Il n'est pas permis non plus d'avoir écrit des problèmes et solutions dans leur entier comme « note de cours ».

Lisez attentivement chaque question avant d'y répondre et faites attention à tout détail qui peut vous donner un indice sur la bonne réponse.

NOTES : Cet examen contient des questions courtes et des questions plus longues. Les énoncés sont, dans la mesure possible, indépendantes, donc si vous n'arrivez pas répondre à une question, vous aurez la possibilité de passer à la prochaine.

Les points indiqués à côté des questions donnent un bilan sur 28 points.

Les questions bonus vous peuvent donner des points en plus. Si votre score (avec bonus) dépasse 28, alors ce surplus pourra compenser un score bas dans les TPs.

NOTE / 28

NOTE EXAMEN (90%) /20

TP NOTE (10%) /20

NOTE MODULE /20

Question I : Les adresses MAC et IP

1. **(1 point)** Expliquez les différences entre les adresses MAC et les adresses IP.
2. **(1 point)** Quel est le rôle d'un serveur DHCP ?
3. **(3 points)** Votre entreprise achète la plage d'adresses 123.45.66.0/23. On vous demande de découper ce réseau de manière à répondre aux besoins d'adressage des différents sites de l'entreprise :

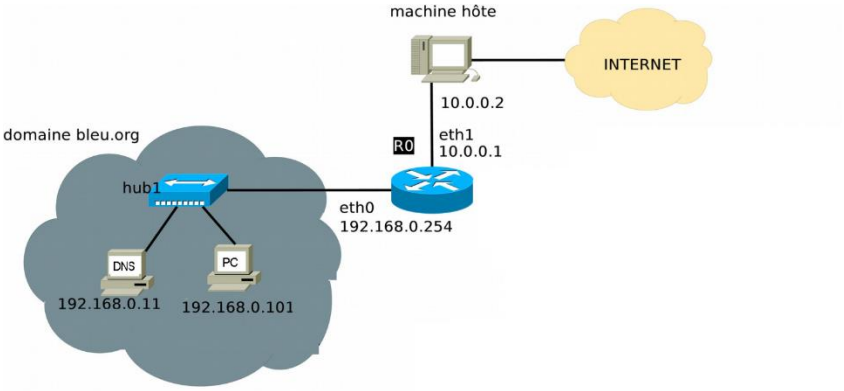
   200 machines pour le siège social
   100 machines pour la filiale en Belgique
   110 machines pour la filiale en Allemagne

   Expliquez la méthodologie que vous allez adopter. De plus, pour chaque sous-réseau obtenu, indiquez :

   a. Son numéro de réseau, en utilisant une notation CIDR et en donnant le masque réseau (Netmask)
   b. L'adresse de broadcast de chaque sous-réseau
   c. Le nombre de machines que l'on peut adresser
   d. La première adresse utilisable
   e. La dernière adresse utilisable

Question II : IP Forwarding

Pour cette question, on utilisera le schéma suivant. Nous avons notamment trois machines : une qu'on appelle DNS, une autre qu'on appelle PC, et une machine hôte située dans un réseau de classe B. L'outil « hub 1 » est un switch.



Répondez aux questions suivantes :

1. **(0.5 points)** Quelle est le rôle de la machine R0 dans cette topologie ?

2. **(0.75 points)** Quelles commandes faut-il utiliser sur R0 pour lui attribuer la configuration IP nécessaire ?
3. **(1.5 points)** Nous voulons que les machines du domaine bleu.org puissent se connecter à la machine hôte. Ces deux machines n'ont qu'une carte réseau, avec une interface qui s'appelle eth0. Donnez les commandes qui font en sort que :
    - Les adresses IP données dans la figure soient attribuées aux bonnes machines
    - Les machines DNS et PC puissent se connecter à la machine hôte

4. Nous voulons également faire en sort que la machine PC utilise la machine DNS pour ses requêtes DNS. Répondez aux questions suivantes :
    a. **(1 point)** Quel est le rôle du protocole DNS ?
    b. **(1.25 points)** Quel fichier faut-il modifier, comment, et sur quelle machine pour que PC puisse utiliser la machine DNS pour ses requêtes DNS ?
    c. **(1 point)** Quelle est la différence entre le protocole DNS et le protocole ARP (pensez à son rôle, quand les protocoles sont-ils utilisés, etc.) ?

5. **(1 point)** Que faut-il encore faire pour que les machines du domaine bleu.org puissent joindre l'Internet ? Donnez la commande/les commandes à utiliser et le nom de la machine/des machines sur laquelle/lesquelles il faut mettre cette commande/ces commandes.

Question III : Les protocoles réseau

1. **(2 points)** Expliquez les rôles respectifs des 4 couches les plus basses du modèle OSI : notamment la couche physique, liaison, réseau et transport.
2. **(1 point)** Expliquez la notion d'encapsulation dans le contexte des protocoles réseau.
3. **(0.5 points)** Quel est le rôle d'une commande de ping ?
4. **(1 point)** Donnez la commande ping entre deux machines PCA (adresse IP 172.16.2.36, adresse MAC f6:84:e8:d1:3b:b5) et PCB (adresse IP 172.16.2.85, adresse MAC a2:36:67:5a:12:11) ? Et si on veut faire exactement trois pings d'une machine vers l'autre ?
5. **(1 point)** Si on veut repérer une commande ping sur un logiciel comme Wireshark, sous quel protocole va-t-on trouver cette commande ? Donnez l'encapsulation de cette commande.
6. **(1 point)** Dans l'annexe, vous allez trouver des en-têtes spécifiques aux divers protocoles réseau. Complétez la trame suivante, sachant que ce message a été envoyé de PCB vers PCA.

    __ __ __ __ __ __ __ __ __ __ __ __ 08 00 45 00
    00 54 00 00 40 00 40 01 c5 24 __ __ __ __ __ __
    __ __ 08 00 2f 56 03 02 00 a0 52 01 2e f0 01 00
    08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17
    18 19 1a 1b 1c 1d 1e 1f 20 21 22
7. **(Bonus, 2 points)** Indiquez à quoi correspondent les fragments de trame indiquées en jaune ci-dessus.

Question IV : Le protocole SSH

Cette question concerne un protocole utilisé pour connecter deux ordinateurs de façon sécurisée, notamment le protocole SSH.

1. **(0.5 point)** Expliquez la notion de port et son utilité.
2. La commande `netstat -tn` sur une certaine machine donne la capture suivante :

```
# netstat -tn
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0    236 139.162.151.198:22      78.116.61.143:45364     ESTABLISHED
tcp        0      0 139.162.151.198:443     78.116.61.143:51657     FIN_WAIT2
tcp        0      0 139.162.151.198:80      78.116.61.143:51654     FIN_WAIT2
tcp        0      0 139.162.151.198:443     78.116.61.143:51655     FIN_WAIT2
tcp        0      0 139.162.151.198:443     78.116.61.143:51658     ESTABLISHED
```

   Sachant que le port 22 est dédié aux connections SSH, le port 80 est dédié aux connections HTTP et le port 443 est dédié aux connections HTTPS (HTTP sécurisé), expliquez :
   a. **(0.5 points)** Quelle est l'adresse IP de cette machine ?
   b. **(1 point)** Dans quelles connexions cette machine est-elle impliquée au présent et quels sont leurs statuts ?
   c. **(0.5 points)** Qui est le client et qui est le serveur dans les connections représentées sur les lignes 1 et 5 ?
   d. **(1 point)** Que signifie la mention `tcp` en début de chaque ligne ?

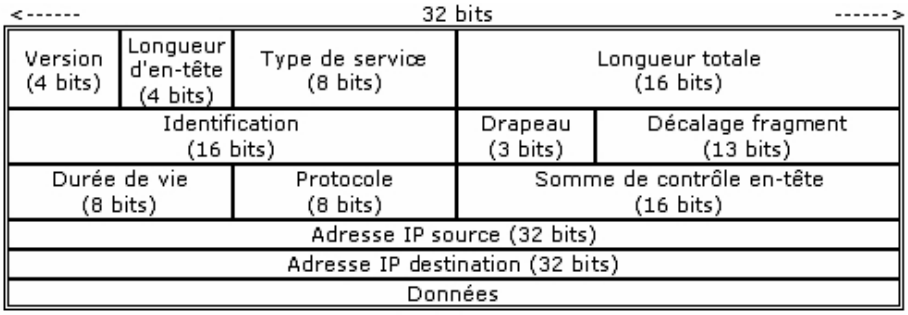
3. Regardez la capture dans l'annexe B de ce document. Répondez aux questions suivantes :
   a. **(1 point)** Décrivez ce que signifient des trois messages inclus dans le carré rouge (les messages indexés 3 à 5) -- pensez aussi à spécifier les adresses du client/du serveur, les ports utilisés.
   b. **(1 point)** La capture est coupée au message 22. Supposez que le message suivant (numéro 23 dans la capture) est envoyé par la machine 192.168.1.97 vers la machine 128.93.193.13. De quel port vers quel port cette transmission va-t-elle ? Quelles sont les valeurs de Seq et Ack pour ce message ?
   c. **(1 point)** Et si le message suivant va en sens inverse ?

4. Regardez la capture dans l'annexe C de ce document, qui détaille le message 49 sur une capture Wireshark. Répondez aux questions suivantes :
   a. **(2 points)** Quelle information est cachée par les blocs bleus ? (dans la partie protocoles)
   b. **(1 point)** Les blocs rouges (en bas) indiquent des contenus chiffrés, notamment les données envoyées dans le message 49. Quelle information contient le reste du message (non capturé dans les blocs rouges ?)
   c. **(Bonus, 1.5 points)** Pour la partie du message qui n'est pas contenue dans les blocs rouges indiquez la séparation entre les différents protocoles utilisés par ce message (vous pouvez utiliser comme référence l'annexe A).

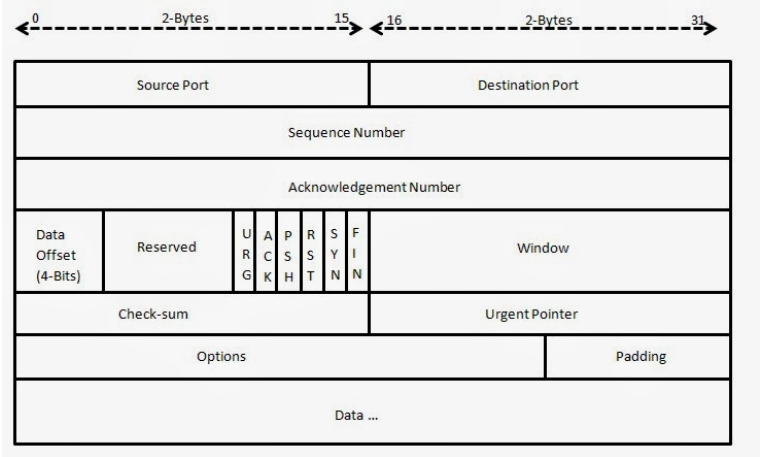
ANNEXE A

Bit 0 - 7	Bit 8 - 15	Bit 16 - 23	Bit 24 - 31
Type de message	Code	Somme de contrôle	
Bourrage ou données			
Données (*optionnel et de longueur variable*)			

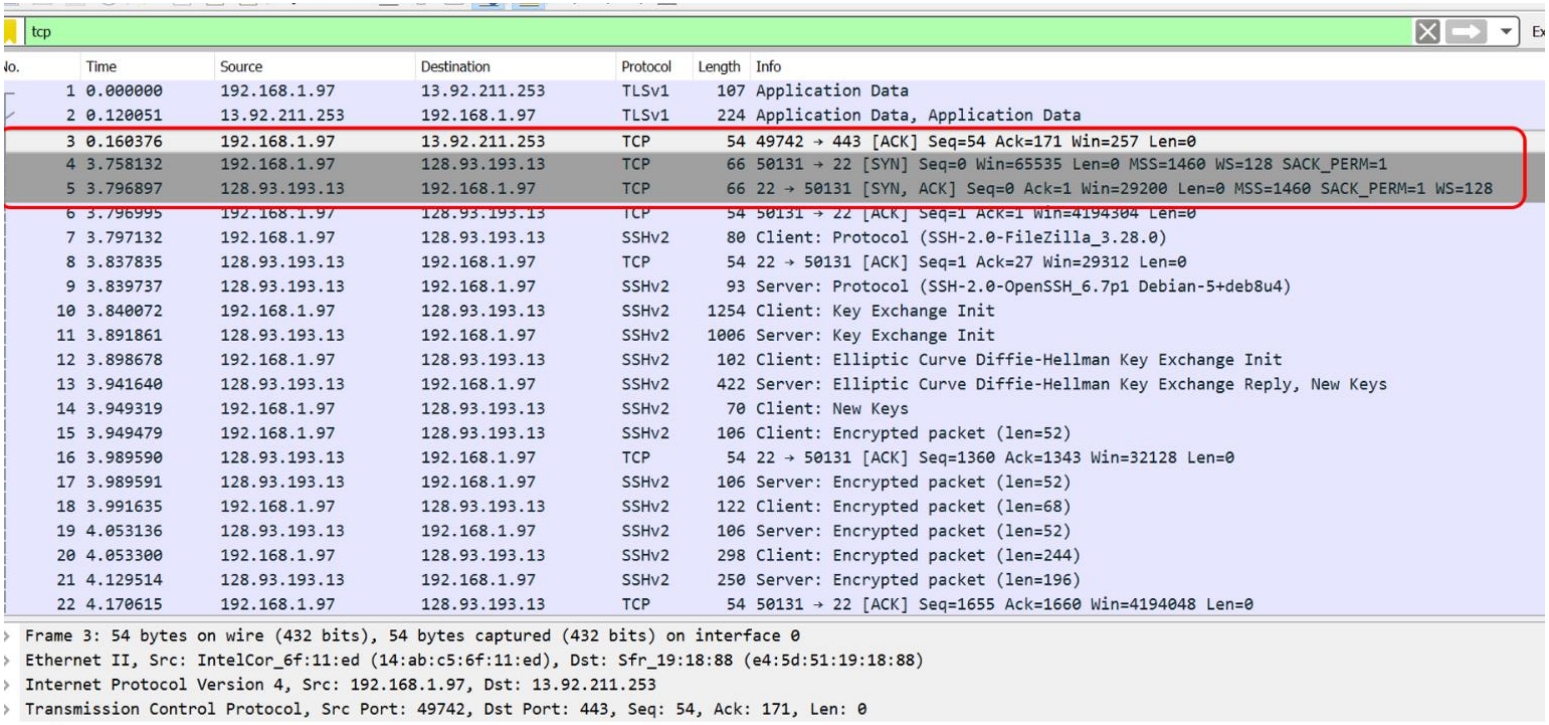
En-tête du protocole ICMP



En-tête du protocole IP



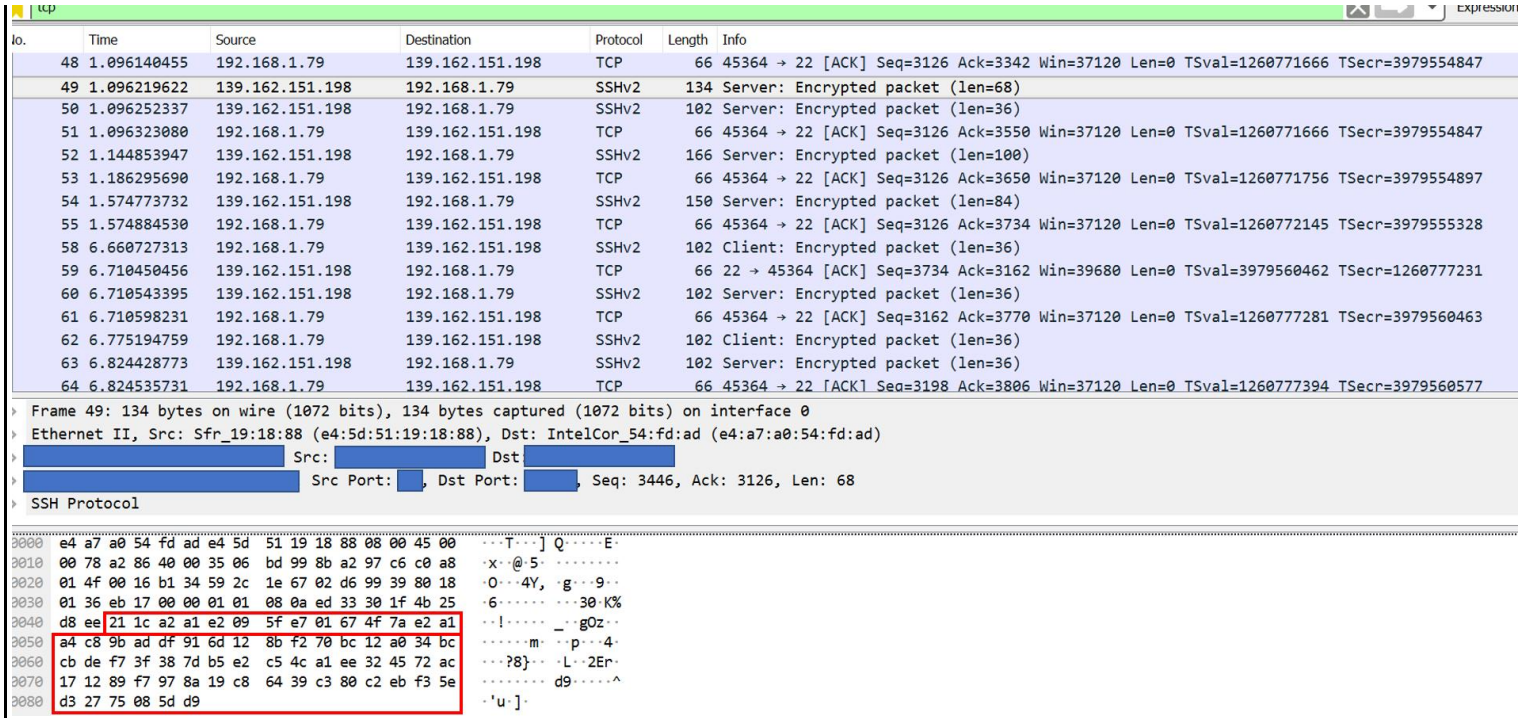
En-tête du protocole TCP



tcp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.97	13.92.211.253	TLSv1	107	Application Data
2	0.120051	13.92.211.253	192.168.1.97	TLSv1	224	Application Data, Application Data
3	0.160376	192.168.1.97	13.92.211.253	TCP	54	49742 → 443 [ACK] Seq=54 Ack=171 Win=257 Len=0
4	3.758132	192.168.1.97	128.93.193.13	TCP	66	50131 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1
5	3.796897	128.93.193.13	192.168.1.97	TCP	66	22 → 50131 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
6	3.796995	192.168.1.97	128.93.193.13	TCP	54	50131 → 22 [ACK] Seq=1 Ack=1 Win=4194304 Len=0
7	3.797132	192.168.1.97	128.93.193.13	SSHv2	80	Client: Protocol (SSH-2.0-FileZilla_3.28.0)
8	3.837835	128.93.193.13	192.168.1.97	TCP	54	22 → 50131 [ACK] Seq=1 Ack=27 Win=29312 Len=0
9	3.839737	128.93.193.13	192.168.1.97	SSHv2	93	Server: Protocol (SSH-2.0-OpenSSH_6.7p1 Debian-5+deb8u4)
10	3.840072	192.168.1.97	128.93.193.13	SSHv2	1254	Client: Key Exchange Init
11	3.891861	128.93.193.13	192.168.1.97	SSHv2	1006	Server: Key Exchange Init
12	3.898678	192.168.1.97	128.93.193.13	SSHv2	102	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
13	3.941640	128.93.193.13	192.168.1.97	SSHv2	422	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys
14	3.949319	192.168.1.97	128.93.193.13	SSHv2	70	Client: New Keys
15	3.949479	192.168.1.97	128.93.193.13	SSHv2	106	Client: Encrypted packet (len=52)
16	3.989590	128.93.193.13	192.168.1.97	TCP	54	22 → 50131 [ACK] Seq=1360 Ack=1343 Win=32128 Len=0
17	3.989591	128.93.193.13	192.168.1.97	SSHv2	106	Server: Encrypted packet (len=52)
18	3.991635	192.168.1.97	128.93.193.13	SSHv2	122	Client: Encrypted packet (len=68)
19	4.053136	128.93.193.13	192.168.1.97	SSHv2	106	Server: Encrypted packet (len=52)
20	4.053300	192.168.1.97	128.93.193.13	SSHv2	298	Client: Encrypted packet (len=244)
21	4.129514	128.93.193.13	192.168.1.97	SSHv2	250	Server: Encrypted packet (len=196)
22	4.170615	192.168.1.97	128.93.193.13	TCP	54	50131 → 22 [ACK] Seq=1655 Ack=1660 Win=4194048 Len=0

ANNEXE B



No.	Time	Source	Destination	Protocol	Length	Info
48	1.096140455	192.168.1.79	139.162.151.198	TCP	66	45364 → 22 [ACK] Seq=3126 Ack=3342 Win=37120 Len=0 TSval=1260771666 TSecr=3979554847
49	1.096219622	139.162.151.198	192.168.1.79	SSHv2	134	Server: Encrypted packet (len=68)
50	1.096252337	139.162.151.198	192.168.1.79	SSHv2	102	Server: Encrypted packet (len=36)
51	1.096323080	192.168.1.79	139.162.151.198	TCP	66	45364 → 22 [ACK] Seq=3126 Ack=3550 Win=37120 Len=0 TSval=1260771666 TSecr=3979554847
52	1.144853947	139.162.151.198	192.168.1.79	SSHv2	166	Server: Encrypted packet (len=100)
53	1.186295690	192.168.1.79	139.162.151.198	TCP	66	45364 → 22 [ACK] Seq=3126 Ack=3650 Win=37120 Len=0 TSval=1260771756 TSecr=3979554897
54	1.574773732	139.162.151.198	192.168.1.79	SSHv2	150	Server: Encrypted packet (len=84)
55	1.574884530	192.168.1.79	139.162.151.198	TCP	66	45364 → 22 [ACK] Seq=3126 Ack=3734 Win=37120 Len=0 TSval=1260772145 TSecr=3979555328
58	6.660727313	192.168.1.79	139.162.151.198	SSHv2	102	Client: Encrypted packet (len=36)
59	6.710450456	139.162.151.198	192.168.1.79	TCP	66	22 → 45364 [ACK] Seq=3734 Ack=3162 Win=39680 Len=0 TSval=3979560462 TSecr=1260777231
60	6.710543395	139.162.151.198	192.168.1.79	SSHv2	102	Server: Encrypted packet (len=36)
61	6.710598231	192.168.1.79	139.162.151.198	TCP	66	45364 → 22 [ACK] Seq=3162 Ack=3770 Win=37120 Len=0 TSval=1260777281 TSecr=3979560463
62	6.775194759	192.168.1.79	139.162.151.198	SSHv2	102	Client: Encrypted packet (len=36)
63	6.824428773	139.162.151.198	192.168.1.79	SSHv2	102	Server: Encrypted packet (len=36)
64	6.824535731	192.168.1.79	139.162.151.198	TCP	66	45364 → 22 [ACK] Seq=3198 Ack=3806 Win=37120 Len=0 TSval=1260777394 TSecr=3979560577

```
▸ Frame 49: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface 0
▸ Ethernet II, Src: Sfr_19:18:88 (e4:5d:51:19:18:88), Dst: IntelCor_54:fd:ad (e4:a7:a0:54:fd:ad)
▸ [redacted] Src: [redacted] Dst [redacted]
▸ [redacted] Src Port: [redacted], Dst Port: [redacted], Seq: 3446, Ack: 3126, Len: 68
▸ SSH Protocol
```

```
0000  e4 a7 a0 54 fd ad e4 5d  51 19 18 88 08 00 45 00   ···T···] Q·····E·
0010  00 78 a2 86 40 00 35 06  bd 99 8b a2 97 c6 c0 a8   ·x··@·5· ········
0020  01 4f 00 16 b1 34 59 2c  1e 67 02 d6 99 39 80 18   ·O···4Y, ·g···9··
0030  01 36 eb 17 00 00 01 01  08 0a ed 33 30 1f 4b 25   ·6····· ···30·K%
0040  d8 ee 21 1c a2 a1 e2 09  5f e7 01 67 4f 7a e2 a1   ··!····· _··gOz··
0050  a4 c8 9b ad df 91 6d 12  8b f2 70 bc 12 a0 34 bc   ·····m· ··p···4·
0060  cb de f7 3f 38 7d b5 e2  c5 4c a1 ee 32 45 72 ac   ···?8}·· ·L··2Er·
0070  17 12 89 f7 97 8a 19 c8  64 39 c3 80 c2 eb f3 5e   ········ d9·····^
0080  d3 27 75 08 5d d9                                 ·'u·]·
```

ANNEXE C