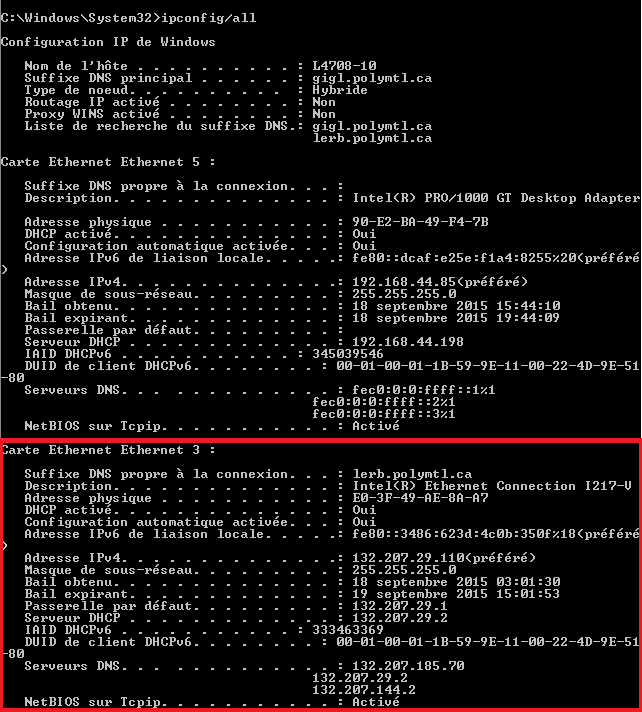
|  |  |
| --- | --- |
| Département de génie informatique et génie logiciel | TP1 : WireSHARK collecte et ANALYSE D’INFORMATION  Chargé de laboratoire : Mauricio Mendoza Medellin  Theo Chapon  Matricule : 1810945 |

# 1.4 Rappel et description avec ipconfig /all



- **Hostname** : L4708-10

- **Nom des suffixes DNS** : gigl.polymtl.ca et lerb.polymtl.ca

- **Nombre d’interfaces réseaux** : Il y a 2 interfaces physiques et 13 interfaces logiques

**Carte Intel I217-V :**

**Addresse MAC:** E0-3F-49-AE-8A-A7

La carte provient de la compagnie ASUSTek COMPUTER INC

E0-3F-49 (hex) ASUSTek COMPUTER INC.

E03F49 (base 16) ASUSTek COMPUTER INC.

15,Li-Te Rd., Peitou, Taipei 112, Taiwan

Taipei Taiwan 112

TW

Source : http://standards-oui.ieee.org/oui.txt

**Adresse IPv4 :**132.207.29.110

**Masque réseau** : 255.255.255.0

Cette adresse a été obtenue par le serveur DHCP

**Adresse IPv6** : fe80::3486:623d:4c0b:350f

**Serveur DHCP** : 132.207.29.2

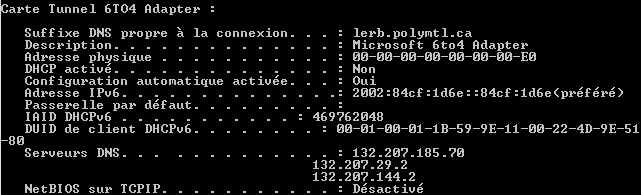
**Serveur DNS** : 132.207.185.70

132.207.29.2

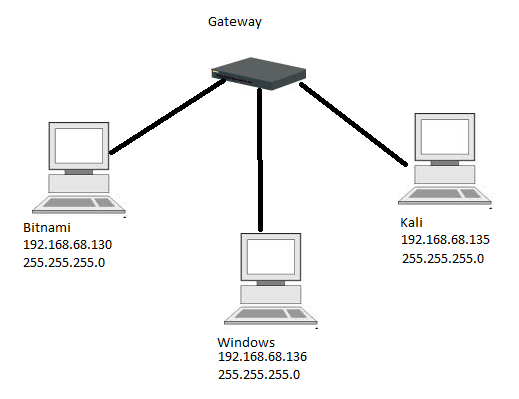
132.207.144.2

**Server Wins** : Non trouvé

**Adresse du tunnel 6to4 adapter (IPV6)** : 2002:84cf:1d6e::84cf:1d6e



# 1.5 Partie A General



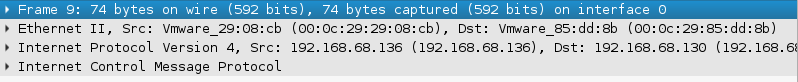
# 1.6 Partie B TCP/UDP

1. Lors d’un ping –t, la trame est envoyée en broadcast, c’est-à-dire que toutes les machines présentes sur le réseau vont recevoir le ping. C’est pourquoi la machine Kali reçoit la trame ICMP.
2. On peut voir les couches 2, 3 et 4 du modèle OSI :

- Ethernet II : couche de liaison qui fournit des informations concernant l’identification physique (MAC)

- Internet Protocol : couche réseau qui fournit des informations concernant l’identification logique de machine (adresse IP). On remarque que la version du protocole IP utilisée est la 4.

- Internet Control Message Protocol : couche de transport. Dans notre cas, ICMP.



1. Sur l’image précédente, on voit que l’adresse MAC des cartes réseaux des machines source et destination ont les 3 premiers octets qui sont identiques (00-0C-29). Cela indique qu’elles proviennent du même fabriquant.

REMARQUE : La carte réseau de la machine Kali provient elle aussi du même constructeur.

00-0C-29 (hex) VMware, Inc.

000C29 (base 16) VMware, Inc.

3401 Hillview Avenue

Palo Alto CA 94304

US

Source : http://standards-oui.ieee.org/oui.txt

1. Le OUI 00-0c-0c appartient à Cisco :

00-0C-0C (hex) APPRO TECHNOLOGY INC.

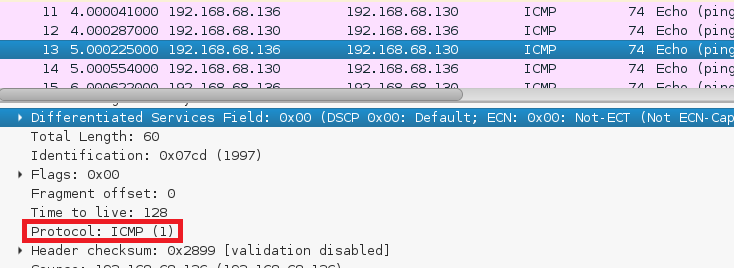
000C0C (base 16) APPRO TECHNOLOGY INC.

13F, No. 66 Chung-Cheng Rd,

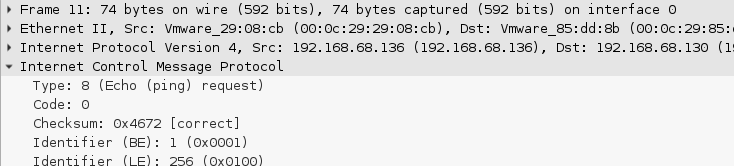
Hsin-Chuang Taipei 242

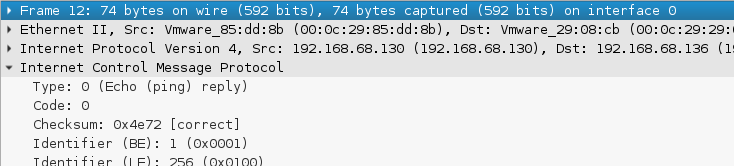
TW

1. Les paquets envoyés sont bien ICMP

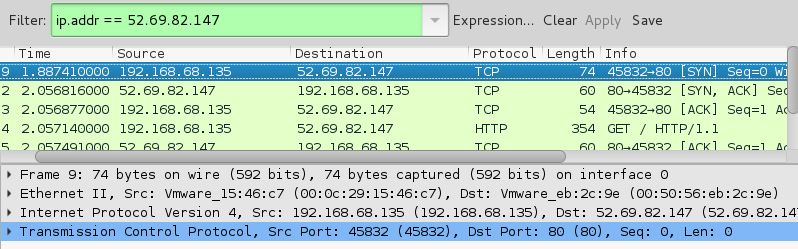


1. Les requêtes ICMP en request sont de Type : 8 et celles en reply sont de Type : 0.



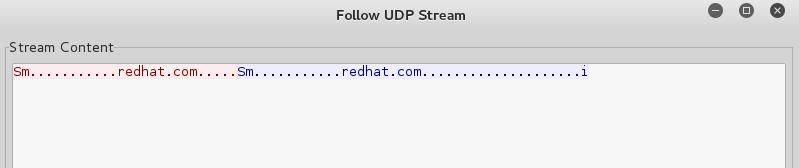


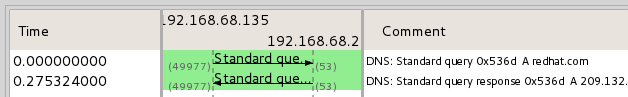
1. On peut facilement remarquer les 3 paquets qui servent à la synchronisation (SYN, SYN ACK et ACK).



1. Les avantages de Quick UDP est la rapidité de la synchronisation et donc de la connexion ainsi que sa polyvalence (broadcast, multicast).

En revanche, l’utilisation d’UDP ne permet pas de garantir la réception des paquets. On évite donc de l’utiliser lors de connexion sécurisé.

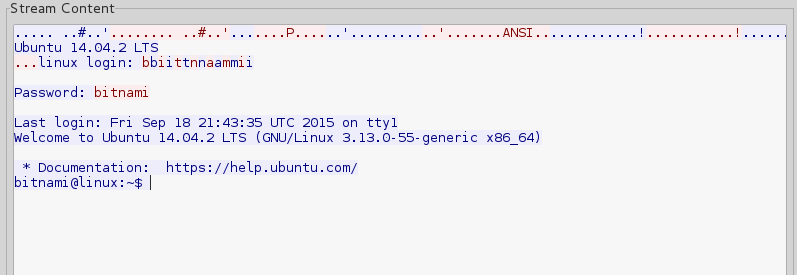




# 1.7 Partie B Telnet

On peut voir en clair (pas de cryptage) la communication entre Window 7 et Bitnami, donc on peut récupérer l’identifiant et le mot de passe.

Pour cela, on utilise l’option Follow TCP stream de Wireshark.

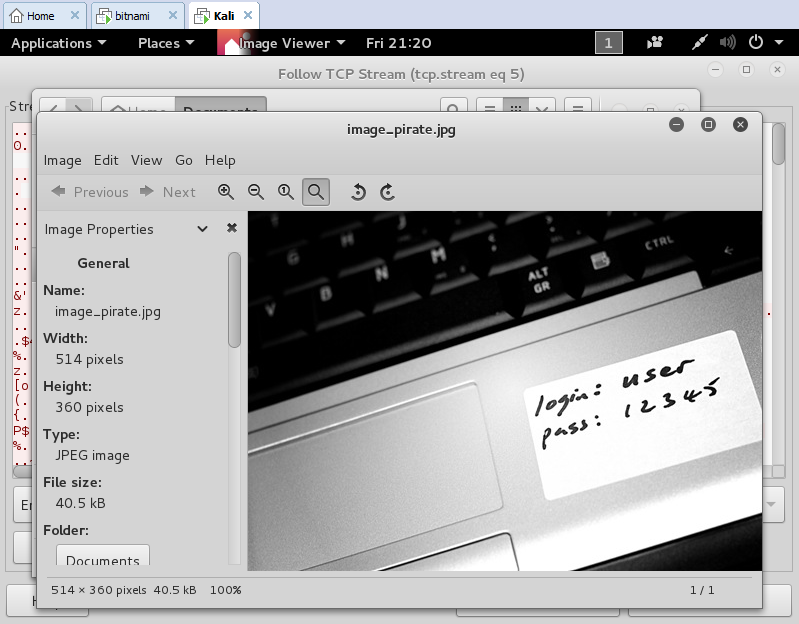


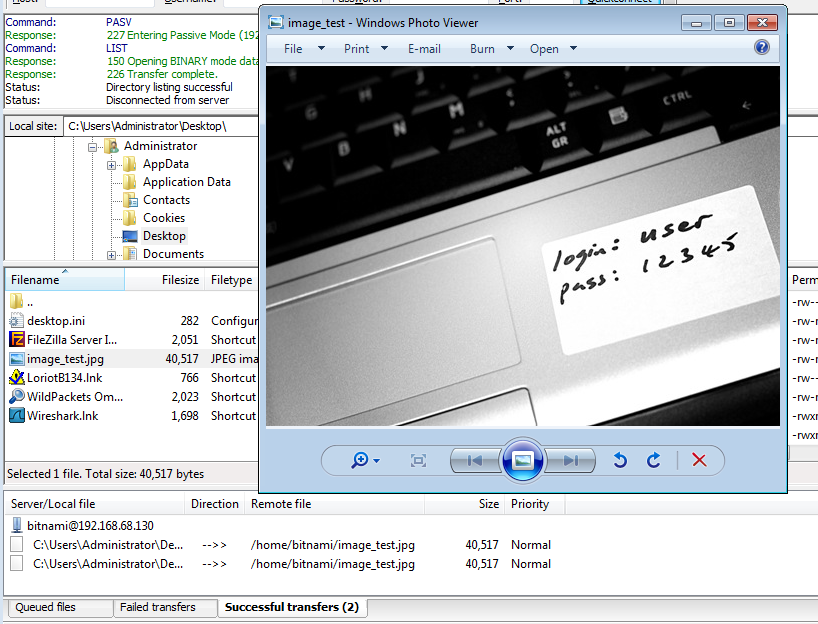
# 1.8 Partie C FTP

1. On retrouve le même problème pour FTP que pour TELNET. On peut voir l’id et le mot de passe pour se connecter.



1. En utilisant l’analyseur de flux à partir du premier FTP-DATA, on peut voir le fichier encoder. Pour le récupérer l’image, il suffit de l’enregistrer au bon format (dans notre cas, jpeg). Pour cela, il faut regarder l’entête (JFIF pour jpeg).





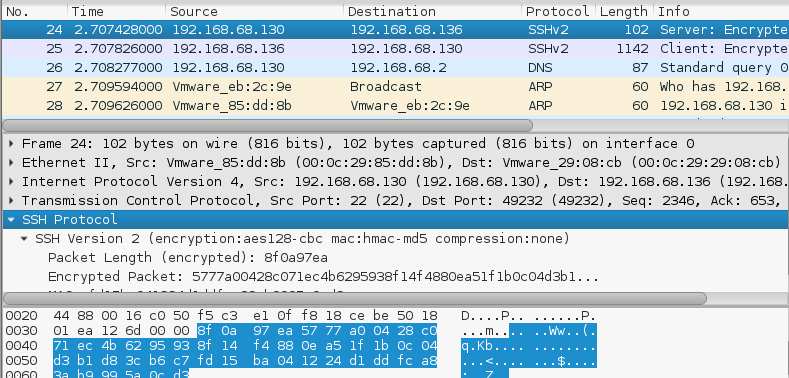
# 1.9 Partie D SSH

1. SSH est un protocole qui encrypte les données qui sont envoyées. Si l’on veut pouvoir récupérer les données, il faut posséder la clé.

De plus, on peut voir ;

- le cryptage utilisé : aes128-cbc et hmac-md5

- le paquet encrypté et sa longueur

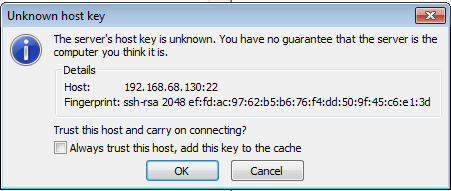


On voit que les données sont encryptées et que l’on ne peut pas les décrypter sans la clé.

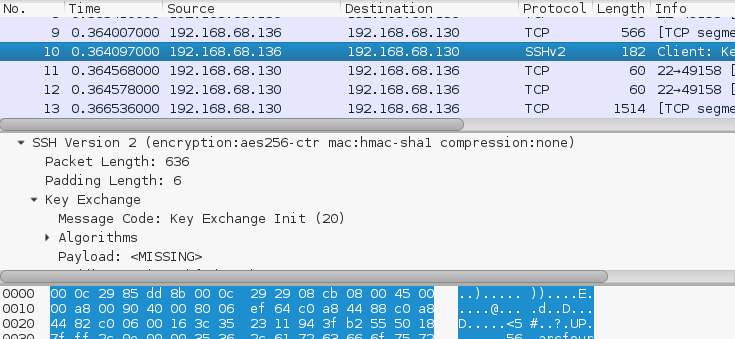


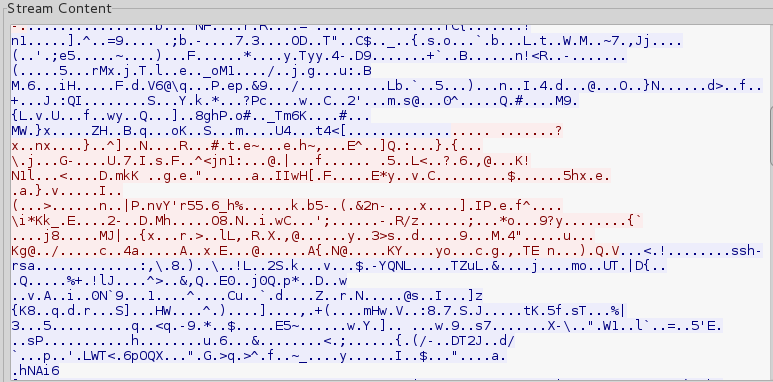
# 1.10 Partie D SFTP

1. Comme c’est la première fois que l’on se connecte à ce server, Filezilla nous fournit le fingerprint afin de vérifier l’authenticité du serveur.



1. Comme pour SSH, on voit bien que les paquets sont encryptés. Sur les premiers paquets, on peut récupérer des informations supplémentaires concernant le payload et l’échange des clés publiques.





c) En entreprise, Wireshark va servir pour effectuer de la surveillance sur les paquets, les informations et les utilisateurs du réseau. Il permet de vérifier que les données sensibles ou représentant un risque sont bien encryptées avec les bons protocoles. Il permet aussi de vérifier la destination des données.