École Polytechnique de Montréal

Département de génie informatique

INF8402 - Sécurité des réseaux fixes et mobiles

Automne 2015

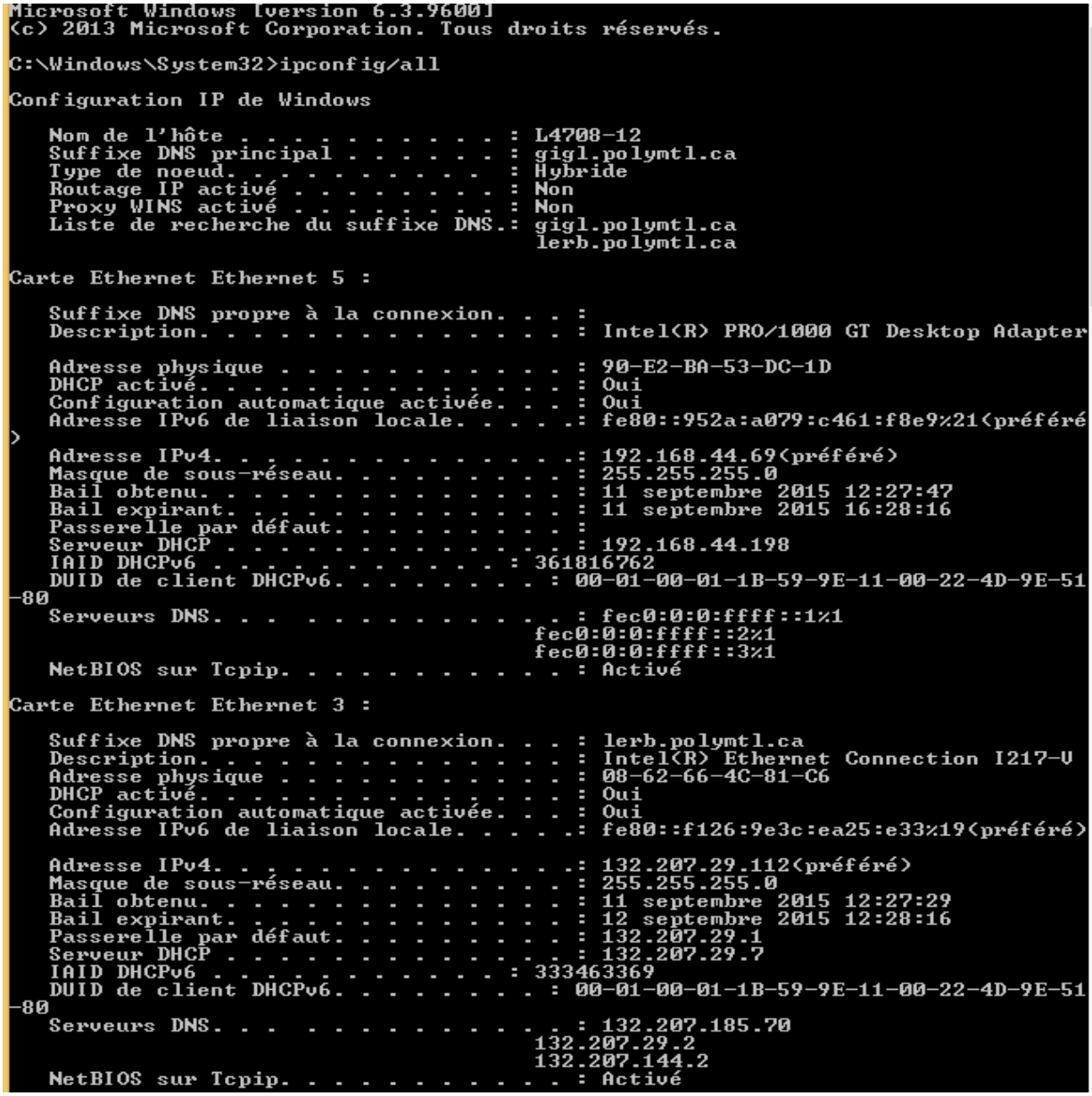
Travail Pratique N°1 : WIRESHARK COLLECTE ET ANALYSE D'INFORMATION

Equipe No 16

Informations générales

Public cible	Étudiants de 2e et 3e cycle de génie informatique
Titre du cours	**INF8402 - Sécurité des réseaux fixes et mobiles**
Session	Automne 2015
Date et lieu de réalisation	Laboratoire de réseautique (L-4708)
Taille de chaque équipe	4 étudiants
Chargé du laboratoire	(Mauricio.Mendoza---Medellin@polymtl.ca)
Étudiants	Ivan Christopher Koupa Lendouba : 1394313 Sara Farshadfar : 1760128 Mohamad Nour Tamer : 1755044

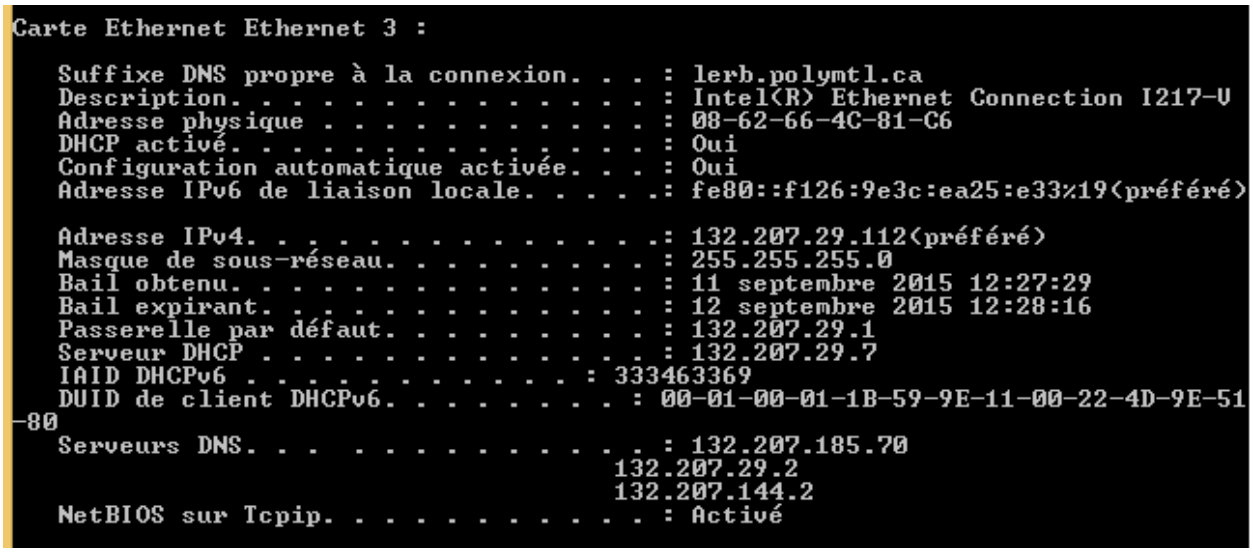
1.4 Rappel et description avec ipconfig /all



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. Tous droits réservés.

C:\Windows\System32>ipconfig/all

Configuration IP de Windows

   Nom de l'hôte . . . . . . . . . . . . : L4708-12
   Suffixe DNS principal . . . . . . . . : gigl.polymtl.ca
   Type de noeud. . . . . . . . . . . . . : Hybride
   Routage IP activé . . . . . . . . . . : Non
   Proxy WINS activé . . . . . . . . . . : Non
   Liste de recherche du suffixe DNS.: gigl.polymtl.ca
                                       lerb.polymtl.ca

Carte Ethernet Ethernet 5 :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . . . . . . . . . . : Intel(R) PRO/1000 GT Desktop Adapter

   Adresse physique . . . . . . . . . . . : 90-E2-BA-53-DC-1D
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::952a:a079:c461:f8e9%21(préféré
)
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.44.69(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Bail obtenu. . . . . . . . . . . . . . : 11 septembre 2015 12:27:47
   Bail expirant. . . . . . . . . . . . . : 11 septembre 2015 16:28:16
   Passerelle par défaut. . . . . . . . . :
   Serveur DHCP . . . . . . . . . . . . . : 192.168.44.198
   IAID DHCPv6 . . . . . . . . . . . : 361816762
   DUID de client DHCPv6. . . . . . . . : 00-01-00-01-1B-59-9E-11-00-22-4D-9E-51
-80
   Serveurs DNS. . .  . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé

Carte Ethernet Ethernet 3 :

   Suffixe DNS propre à la connexion. . . : lerb.polymtl.ca
   Description. . . . . . . . . . . . . . : Intel(R) Ethernet Connection I217-V
   Adresse physique . . . . . . . . . . . : 08-62-66-4C-81-C6
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::f126:9e3c:ea25:e33%19(préféré)

   Adresse IPv4. . . . . . . . . . . . . .: 132.207.29.112(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Bail obtenu. . . . . . . . . . . . . . : 11 septembre 2015 12:27:29
   Bail expirant. . . . . . . . . . . . . : 12 septembre 2015 12:28:16
   Passerelle par défaut. . . . . . . . . : 132.207.29.1
   Serveur DHCP . . . . . . . . . . . . . : 132.207.29.7
   IAID DHCPv6 . . . . . . . . . . . : 333463369
   DUID de client DHCPv6. . . . . . . . : 00-01-00-01-1B-59-9E-11-00-22-4D-9E-51
-80
   Serveurs DNS. . .  . . . . . . . . . . : 132.207.185.70
                                       132.207.29.2
                                       132.207.144.2
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé
```

- Hostname : L4708-12
- Nom de suffixe DNS : gigl.polymtl.ca
- Nombre d'interface réseau : 15

Carte Intel I217-V :



- **Addresse physique MAC:** 08-62-66-4C-81-C6
  Il s'agit de la compagnie ASUSTek COMPUTER INC.
- **Adresse IPv4 :**132.207.29.112
- **Masque réseau** : 255.255.255.0
  Cette adresse a été obtenue par le serveur DHCP
- **Adresse IPv6** : fe80::f126:9e3c:ea25:e33
- **Serveur DHCP** : 132.207.29.7
- **Serveur DNS** : 132.207.185.70
  132.207.29.2
  132.207.144.2
- **Server Wins** : n'est pas spécifié

Interfaces virtuelles pour VMware " Le tunnel 6to4 adapter "

```
Carte Tunnel 6TO4 Adapter :

   Suffixe DNS propre à la connexion. . . : lerb.polymtl.ca
   Description. . . . . . . . . . . . . . : Microsoft 6to4 Adapter
   Adresse physique . . . . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP activé. . . . . . . . . . . . . . : Non
   Configuration automatique activée. . . : Oui
   Adresse IPv6. . . . . . . . . . . . . .: 2002:84cf:1d70::84cf:1d70(préféré)
   Passerelle par défaut. . . . . . . . . :
   IAID DHCPv6 . . . . . . . . . . . : 150994944
   DUID de client DHCPv6. . . . . . . . : 00-01-00-01-1B-59-9E-11-00-22-4D-9E-51
-80
   Serveurs DNS. . .  . . . . . . . . . . : 132.207.185.70
                                    132.207.29.2
                                    132.207.144.2
   NetBIOS sur TCPIP. . . . . . . . . . . : Désactivé
```

- **Adresse du tunnel 6to4 adapter :** 2002 :84cf :1d70 ::84cf :1d70

1.5 Partie A Général

- **Adresse de Windows 7** : 192.168.68.129
- **Adresse de Bitnami :** 192.168.68.130
- **Adresse de Kali :** 192.168.68.131

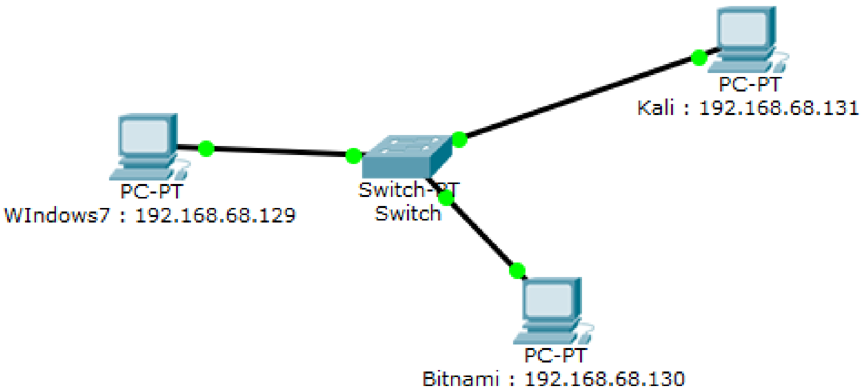
Pinging the Windows machine has failed because of the firewall, so we can make sure that Kali machine is on the same network by running the arp command

```
root@kali:~# arp -a
? (192.168.68.254) at 00:50:56:f9:40:95 [ether] on eth0
? (192.168.68.130) at 00:0c:29:a3:45:e5 [ether] on eth0
? (192.168.68.129) at 00:0c:29:bd:95:34 [ether] on eth0
? (192.168.68.2) at 00:50:56:eb:2c:9e [ether] on eth0
root@kali:~#
```

Runing the command « sudo ufw disable » on Bitnami

```
linux login: bitnami
Password:
Last login: Thu Sep 10 20:04:45 UTC 2015 on tty1
Welcome to Ubuntu 14.04.2 LTS (GNU/Linux 3.13.0-55-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
bitnami@linux:~$ sudo
sudo        sudoedit    sudoreplay
bitnami@linux:~$ sudo
sudo        sudoedit    sudoreplay
bitnami@linux:~$ sudo ufw disable
[sudo] password for bitnami:
Firewall stopped and disabled on system startup
bitnami@linux:~$ _
```

Une graphique de la configuration des équipes



1.6 Partie B TCP/UDP

1- Ping avec l'option –t (ping encontinu) au Bitnami

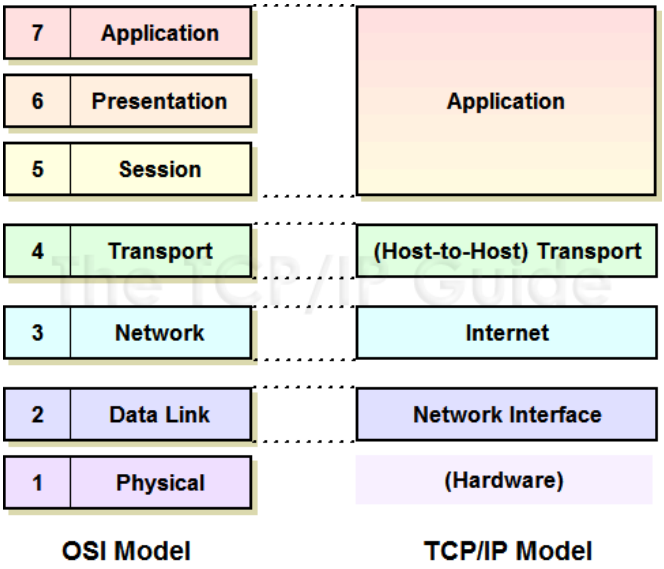
```
C:\Users\Administrator>ping 192.168.68.130 -t

Pinging 192.168.68.130 with 32 bytes of data:
Reply from 192.168.68.130: bytes=32 time<1ms TTL=64
Reply from 192.168.68.130: bytes=32 time<1ms TTL=64
Reply from 192.168.68.130: bytes=32 time<1ms TTL=64
Reply from 192.168.68.130: bytes=32 time<1ms TTL=64
Reply from 192.168.68.130: bytes=32 time<1ms TTL=64
Reply from 192.168.68.130: bytes=32 time<1ms TTL=64
Reply from 192.168.68.130: bytes=32 time<1ms TTL=64
Reply from 192.168.68.130: bytes=32 time<1ms TTL=64
Reply from 192.168.68.130: bytes=32 time<1ms TTL=64
Reply from 192.168.68.130: bytes=32 time<1ms TTL=64
Reply from 192.168.68.130: bytes=32 time<1ms TTL=64
```

2- Les trames ICMP (Ping).

1	0.000000000	192.168.68.129	192.168.68.130	ICMP	74	Echo (ping
2	0.000099000	192.168.68.130	192.168.68.129	ICMP	74	Echo (ping
5	1.000736000	192.168.68.129	192.168.68.130	ICMP	74	Echo (ping
6	1.000817000	192.168.68.130	192.168.68.129	ICMP	74	Echo (ping
7	1.999816000	192.168.68.129	192.168.68.130	ICMP	74	Echo (ping
8	1.999900000	192.168.68.130	192.168.68.129	ICMP	74	Echo (ping
9	3.000208000	192.168.68.129	192.168.68.130	ICMP	74	Echo (ping
10	3.000215000	192.168.68.130	192.168.68.129	ICMP	74	Echo (ping
11	4.000786000	192.168.68.129	192.168.68.130	ICMP	74	Echo (ping

3- If you're trying to capture network traffic that's *not* being sent to or from the machine running Wireshark, i.e. traffic between “ Windows & Bitnami) you will have to capture in "promiscuous mode", and, on a switched Ethernet network, Wireshark provide us with this feature.

4- Couches du modèle OSI



As you can see, there are three OSI layers showing (Layer 2 & 3 & 4)

```
▸ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▸ Ethernet II, Src: Vmware_bd:95:34 (00:0c:29:bd:95:34), Dst: Vmware_a3:45:e5 (00:0c:29:a3:45
▸ Internet Protocol Version 4, Src: 192.168.68.129 (192.168.68.129), Dst: 192.168.68.130 (192
▸ Internet Control Message Protocol
```

5- Les champs de l’entête Ethernet

```
▾ Ethernet II, Src: Vmware_a3:45:e5 (00:0c:29:a3:45:e5), Dst: Vmware_bd:95:34 (00:0c:29:bd:95:34)
  ▾ Destination: Vmware_bd:95:34 (00:0c:29:bd:95:34)
      Address: Vmware_bd:95:34 (00:0c:29:bd:95:34)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: Vmware_a3:45:e5 (00:0c:29:a3:45:e5)
      Address: Vmware_a3:45:e5 (00:0c:29:a3:45:e5)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IP (0x0800)
```

It’s the same manufacturer (Vmware).

6- recherche pour **00-0c-0c**, à qui appartient ce OUI

```
00-0C-0C    (hex)              APPRO TECHNOLOGY INC.
000C0C      (base 16)          APPRO TECHNOLOGY INC.
                               13F, No. 66 Chung-Cheng Rd,
                               Hsin-Chuang  Taipei  242
                               TW
```

By looking for the **00-0c-0c** it seems that is not Cisco related OUI & what has been found for cisco is the below screen shot

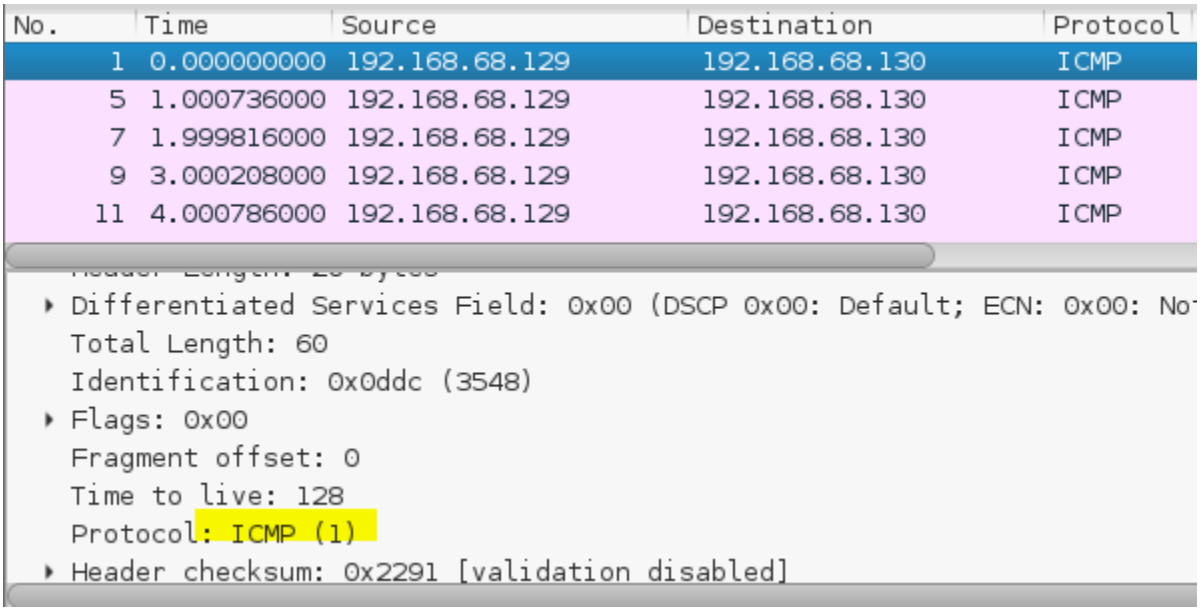
```
F4-CF-E2    (hex)              Cisco Systems, Inc
F4CFE2      (base 16)          Cisco Systems, Inc
                               170 West Tasman Drive
                               San Jose  CA  95134
                               US

50-1C-BF    (hex)              Cisco Systems, Inc
501CBF      (base 16)          Cisco Systems, Inc
                               170 West Tasman Drive
                               San Jose  CA  95134
                               US
```

7- Filtrer les paquets pour icmp seulement et vérifier les valeurs des champs type pour les trames request et reply.

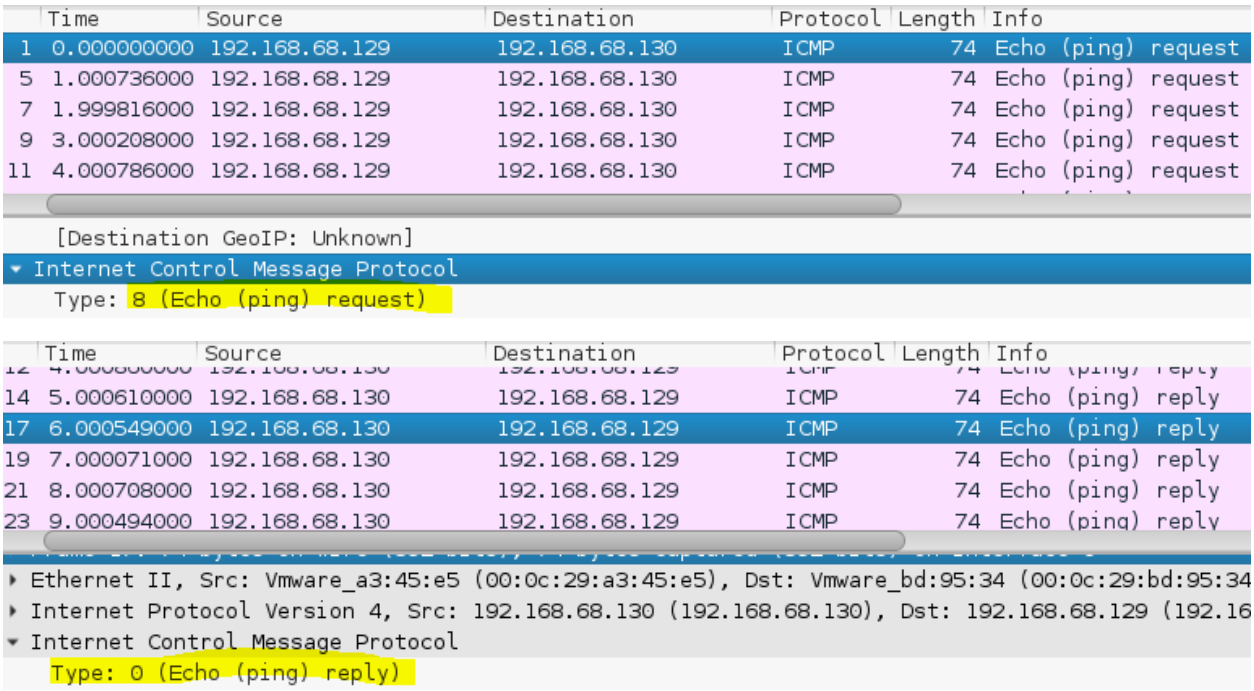
As you can see from the below screen shots the ICMP value of 1 for both the request & reply packet

No.	Time	Source	Destination	Protocol
6	1.000817000	192.168.68.130	192.168.68.129	ICMP
8	1.999900000	192.168.68.130	192.168.68.129	ICMP
10	3.000215000	192.168.68.130	192.168.68.129	ICMP
12	4.000860000	192.168.68.130	192.168.68.129	ICMP
14	5.000610000	192.168.68.130	192.168.68.129	ICMP

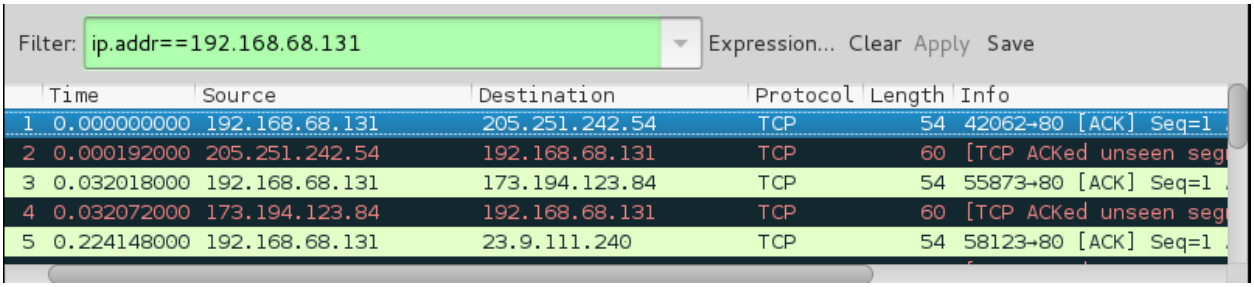
```
▸ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: No
  Total Length: 60
  Identification: 0x8b8d (35725)
▸ Flags: 0x00
  Fragment offset: 0
  Time to live: 64
  Protocol: ICMP (1)
▸ Header checksum: 0xe4df [validation disabled]
```



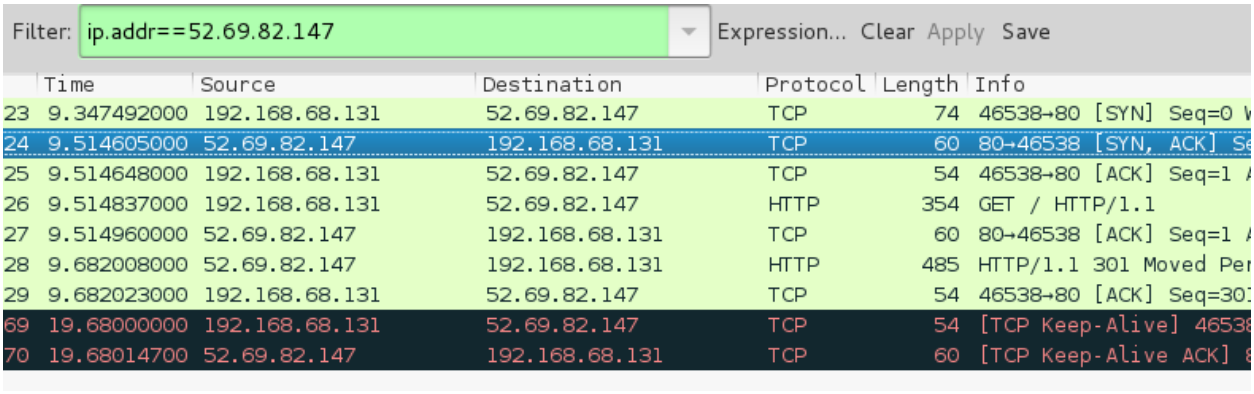
8- Packets type



9- Filtrez sur adresse ip

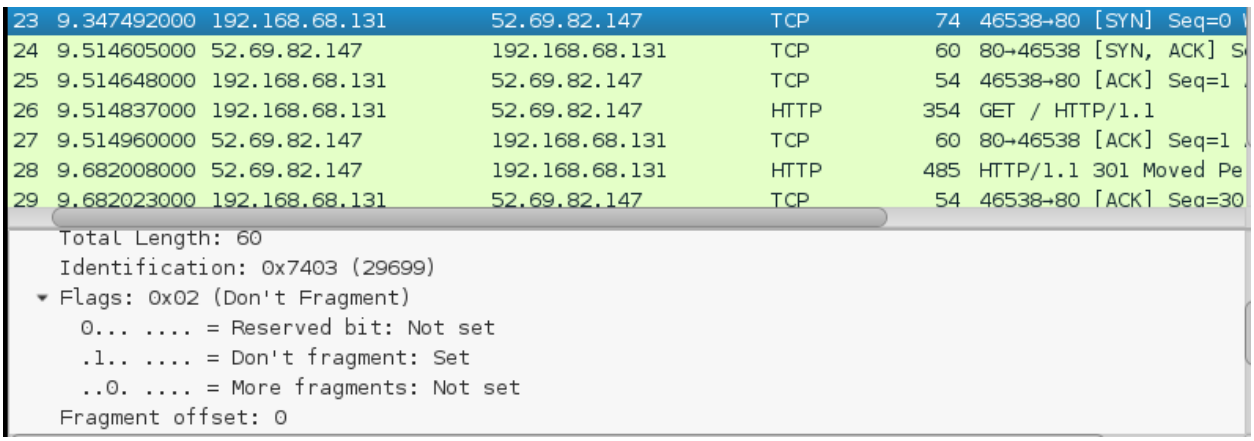


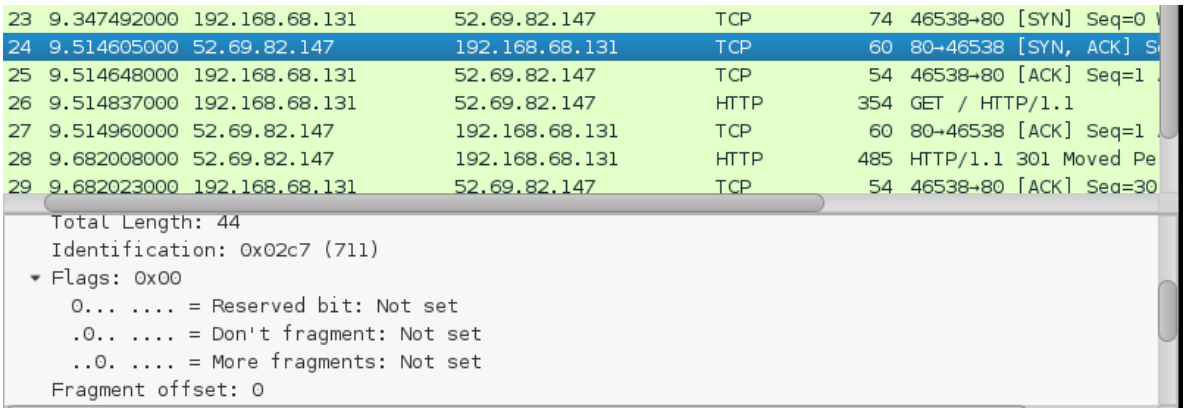
10-Filtrez l'adresse de toyota.jp

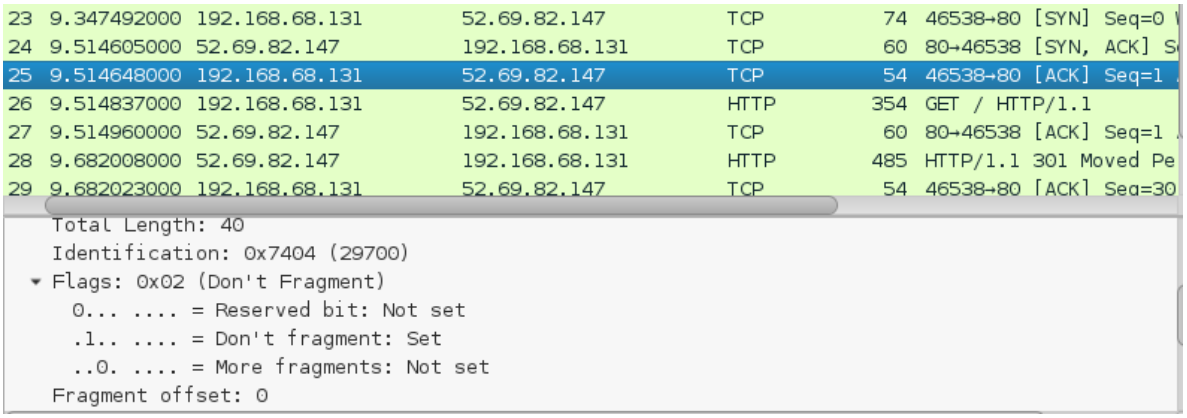


11-Identifiez le premier 3 paquets connexion.(As you can see packets 23,24,25)

By looking at those three packets, you will see the TCP 3 way handshakes (SYN, SYN ACK, ACK).

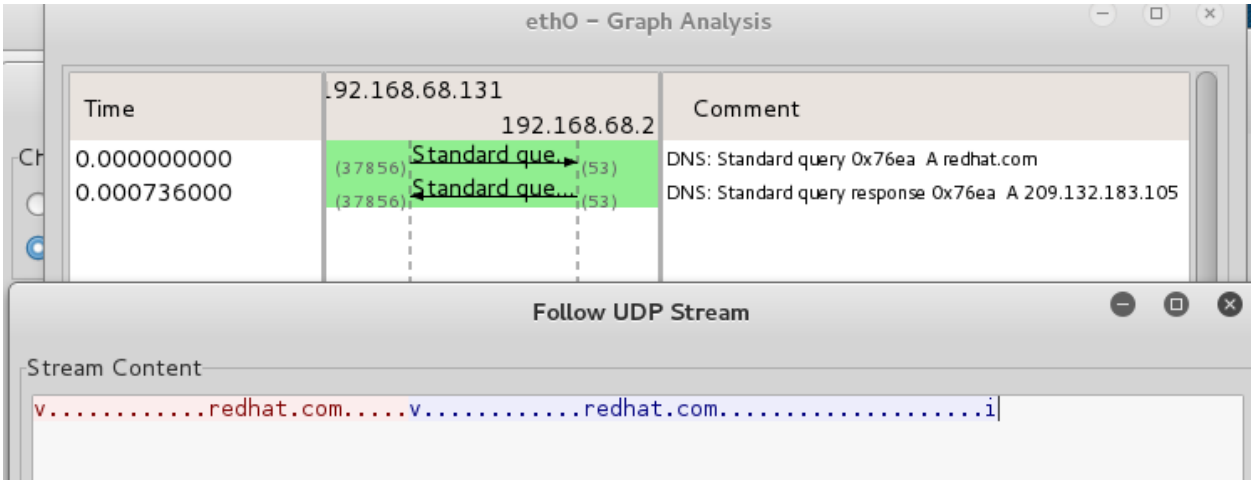






12- TCP vs UDP

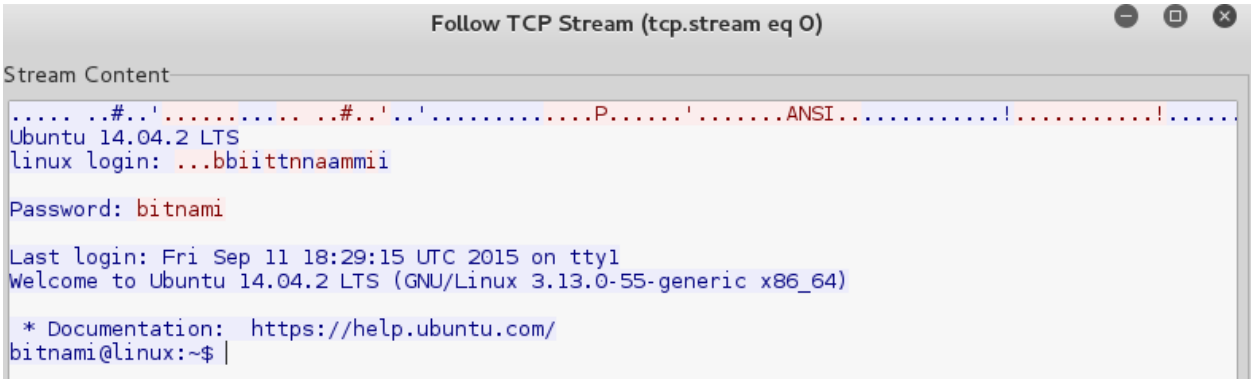
TCP is suited for applications that require high reliability, and transmission time is relatively less critical.	UDP is suitable for applications that need fast, efficient transmission, such as games. UDP's stateless nature is also useful for servers that answer small queries from huge numbers of clients.



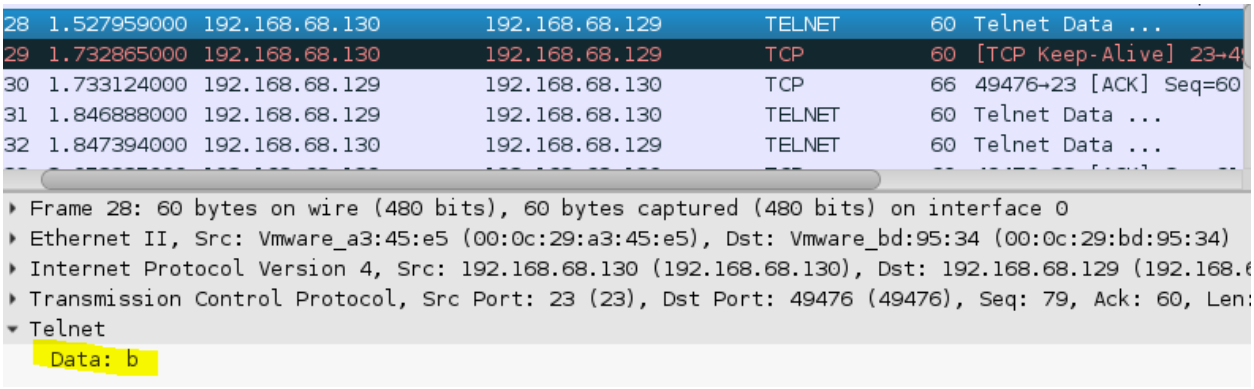
1.7 Partie B TELNET

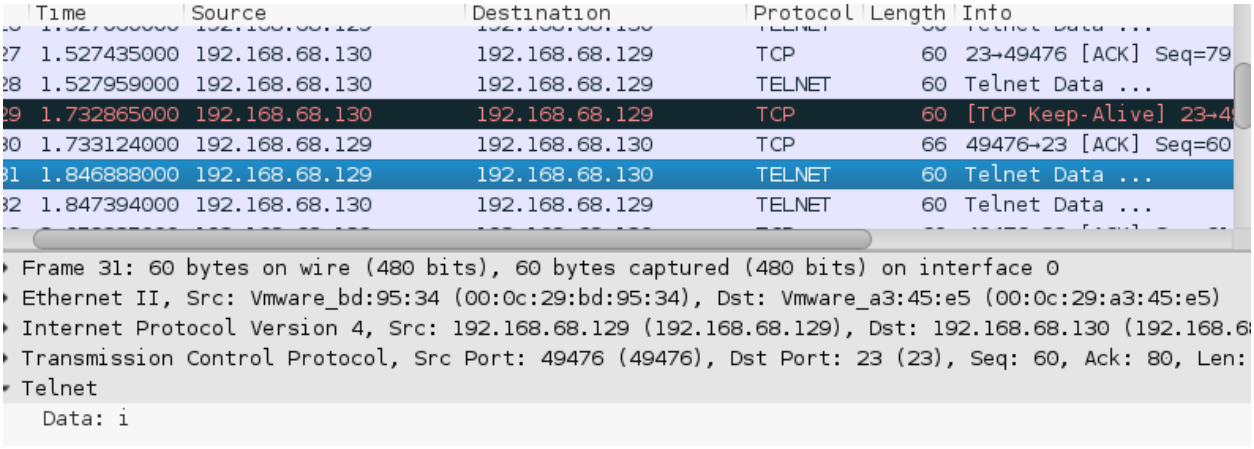
1- Connecting to Bitnami from Windows machine using Telnet with a username/password : bitnami/Bitnami

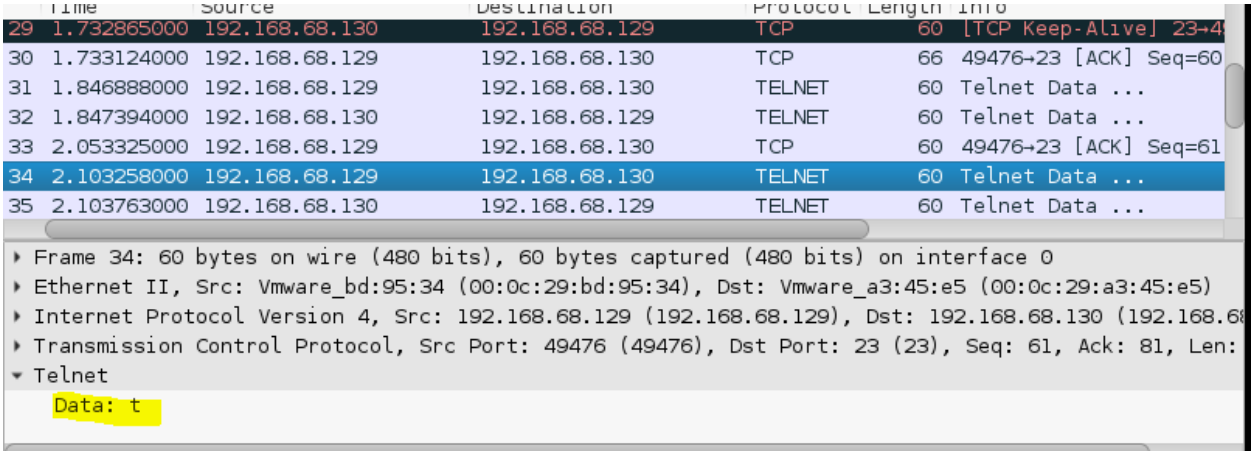
As you can see that the password has been sent as a clear text which make the Telnet protocol unsecure to be used



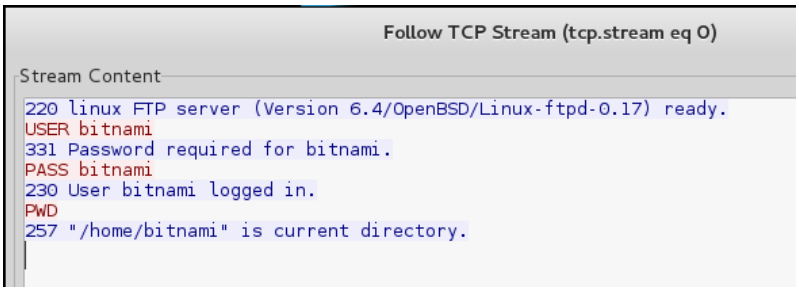
2- As you can see from the below screen shot how Wireshark is able to sniff & interpret the Telnet traffic





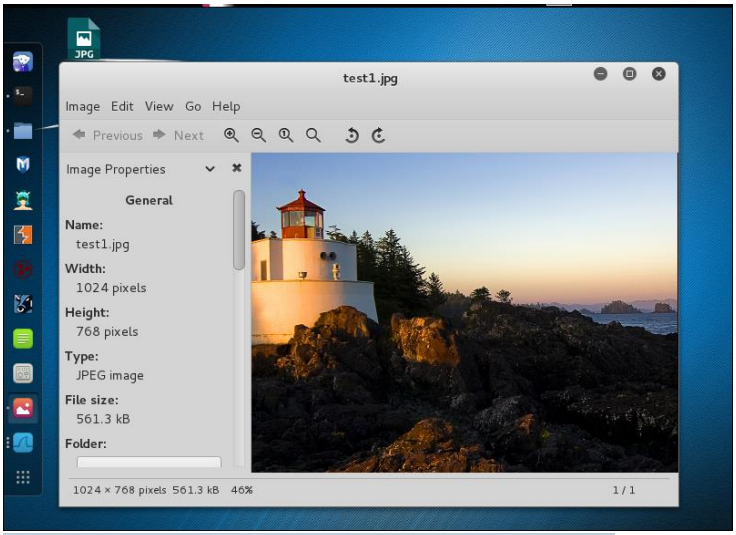


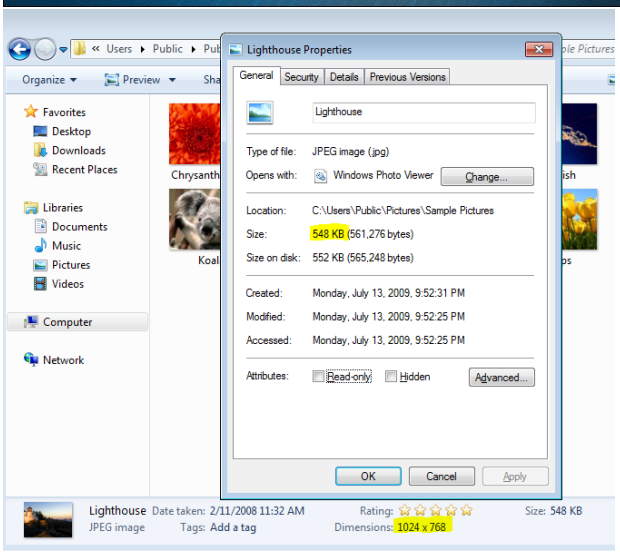
1.8 Partie C FTP



En ce qui a trait au transfert du nom de l'utilisateur et du mot de passe, le protocole FTP et Telnet sont équivalent car nous sommes en mesure de consulter ces données en claire sur le réseau.

Nous sommes en mesure de consulter l'image transférée par FTP à travers la machine Kali tel que présenté dans les captures d'écran suivantes.

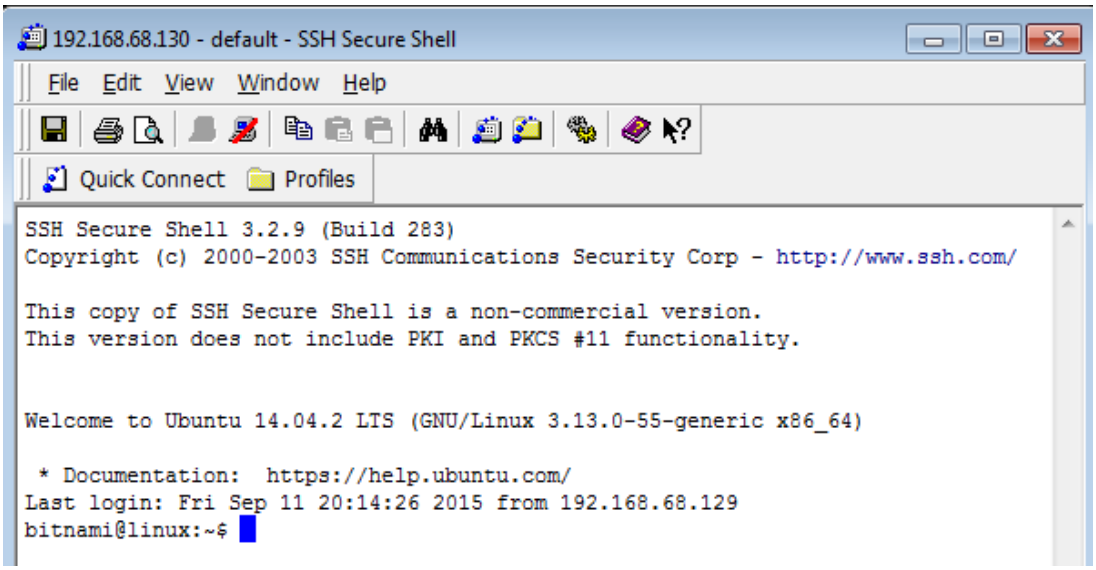




En consultant les propriétés de l'image sur la machine Windows et sur la machine Kali, nous constatons que les attributs sont assez équivalents, donc l'image se voit très peu altérée.

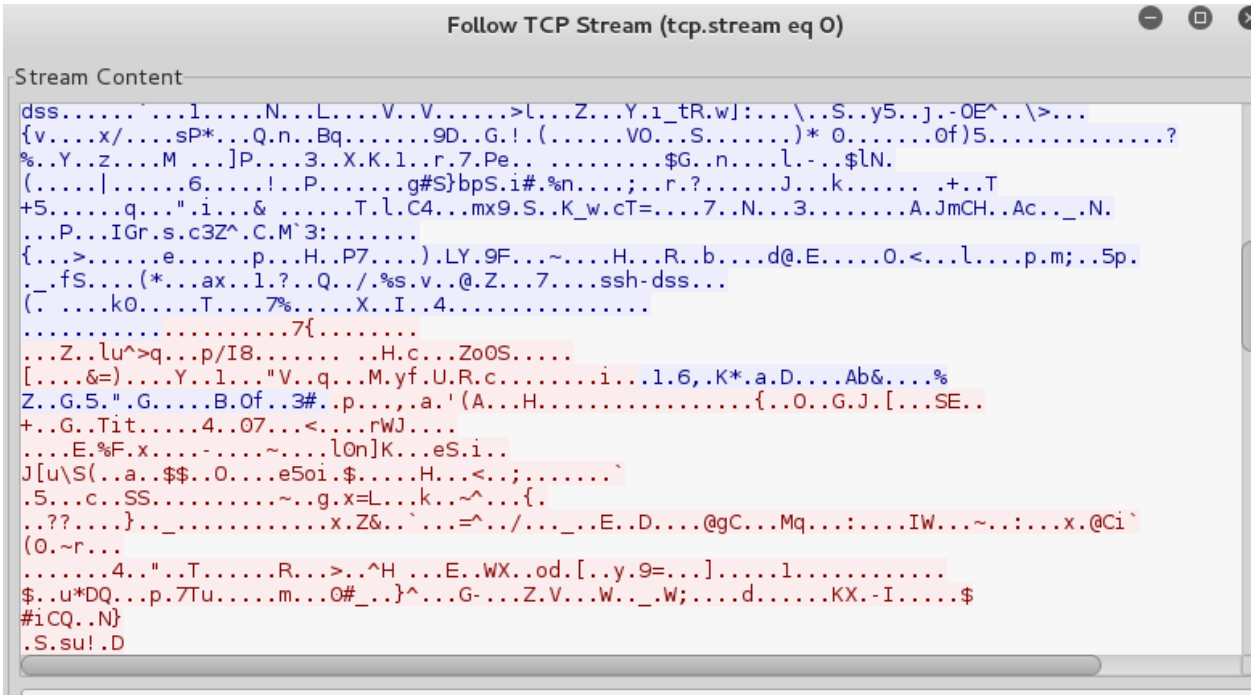
1.9 Partie D SSH

1- Connecting to Bitnami from Windows machine using SSH with a username/password : bitnami/Bitnami

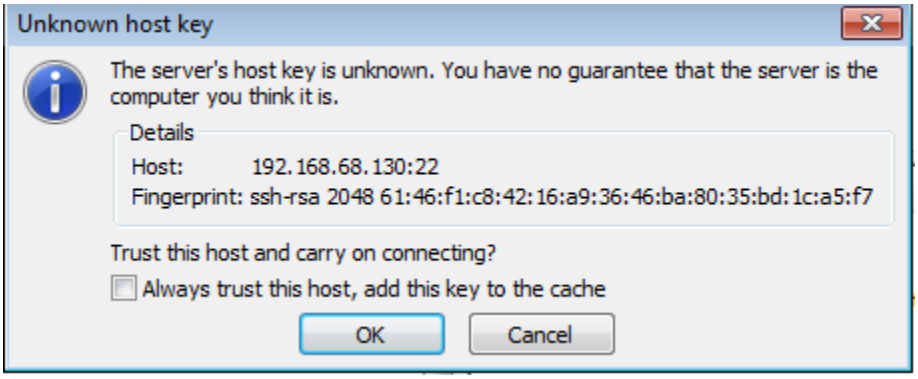


2- SSH is an encrypted way of communication based on encrypting the Sent data using the Public key which has been already send by the destination target which will decrypted the data using his private key associated with the sent public key

Source	Destination	Protocol	Length	Info
192.168.68.130	192.168.68.129	SSHv2	95	Server: Protocol (SSH-2.0-OpenSSH_6.6
192.168.68.129	192.168.68.130	SSHv2	98	Client: Protocol (SSH-1.99-3.2.9 SSH
192.168.68.130	192.168.68.129	TCP	60	22→49478 [ACK] Seq=42 Ack=45 Win=2924
192.168.68.129	192.168.68.130	SSHv2	390	Client: Ignore, Key Exchange Init
192.168.68.130	192.168.68.129	TCP	60	22→49478 [ACK] Seq=42 Ack=381 Win=302
192.168.68.130	192.168.68.129	TCP	1514	[TCP segment of a reassembled PDU]
192.168.68.130	192.168.68.129	SSHv2	242	Server: Key Exchange Init
192.168.68.129	192.168.68.130	TCP	60	49478→22 [ACK] Seq=381 Ack=1690 Win=6
192.168.68.129	192.168.68.130	SSHv2	214	Client: Ignore, Diffie-Hellman Key Ex
192.168.68.130	192.168.68.129	SSHv2	710	Server: Diffie-Hellman Key Exchange R
192.168.68.129	192.168.68.130	TCP	60	49478→22 [ACK] Seq=541 Ack=2346 Win=6
192.168.68.129	192.168.68.130	SSHv2	86	Client: Ignore, New Keys
192.168.68.130	192.168.68.129	TCP	60	22→49478 [ACK] Seq=2346 Ack=573 Win=3
192.168.68.129	192.168.68.130	SSHv2	134	Client: Encrypted packet (len=80)



1.10 Partie D SFTP



Il s'agit de la clé publique du serveur avec laquelle le client va chiffrer les données à envoyer vers celui-ci.

Toute l'information qui circule est encryptée. Mais nous pouvons voir le processus d'échange de clé initialisé afin de rendre la connexion sécurisée.

.Pour analyser la sécurité d'une entreprise en utilisant Wireshark, nous nous assurerons qu'aucune information sensible ne transite par les protocoles FTP et Telnet, mais bien par un dispositif sécurisé tel que SFTP ou SSH.