Labo Applications (90 min)

§0	Introduction	sudo ./c 2

Objectifs Comprendre l'utilité des protocoles RDP, SCP, SMB et LDAP dans un contexte d'entreprise

Session Ouvrir une **session Windows 7** administrateur : compte=**albert** password=**admin**

Action Copier sur le bureau le dossier partagé **\\10.2.1.1\doclabo\RSX\3_Applications**

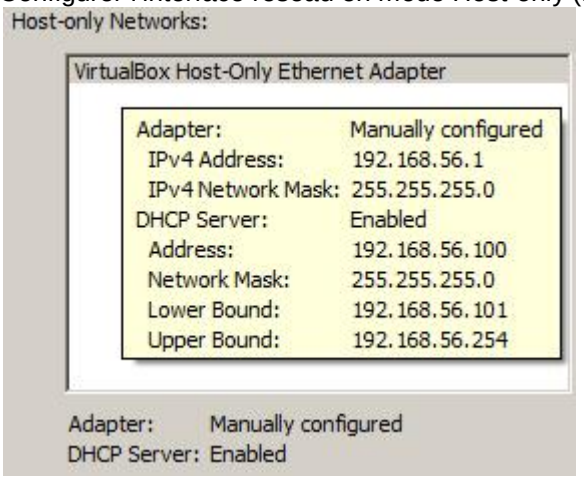
§1	Remote Desktop Protocol (MS Thin Client)	20 min

Objectif Accéder à un système XP depuis Win7 en mode GUI
Cette partie illustre l'accès distant que certains administrateurs utilisent depuis leur client Windows pour accéder aux serveurs Windows de l'entreprise

Etapes Utiliser le réseau en mode Host only
Créer un compte membre du groupe Utilisateurs du Bureau à distance
Autoriser l'accès distant sur XP
Tester

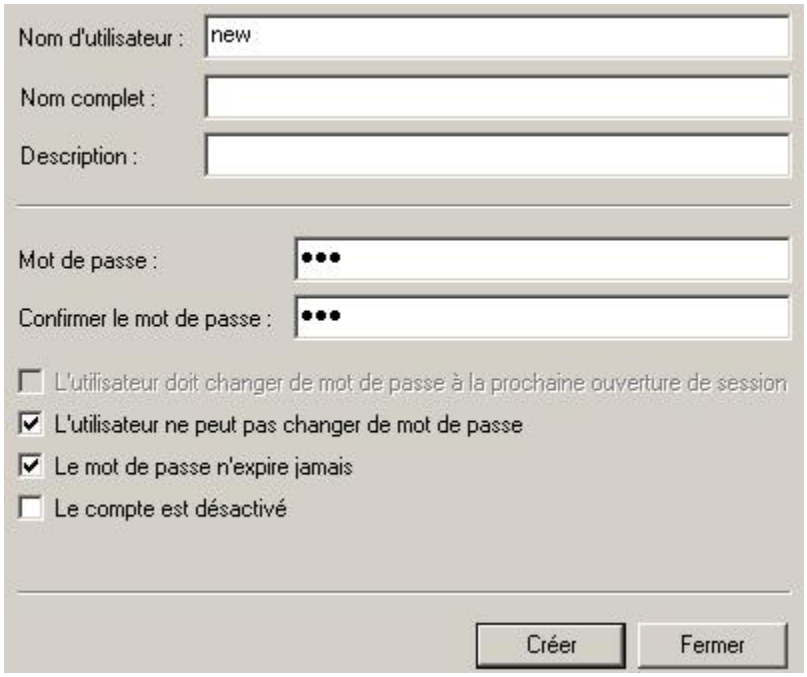
Action Lancer Vbox

a) Configurer l'interface réseau en mode Host-only (Files – Preferences – Network)



b) Importer **XP-SP3.ova**
Description → Username = Password = labo
Utiliser le réseau Host-only
Démarrer cette VM
Contrôler l'accès réseau à cette VM depuis Win7
XP – cmd – ipconfig → IP = 192.168.56.101
Win7 – cmd – ping 192.168.56.101

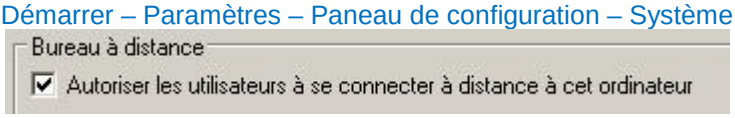
c) Créer un compte membre du groupe Utilisateurs du Bureau à distance
XP – Clic droit sur Poste de travail – Gérer
Utilisateurs et groupes locaux – Utilisateurs – Nouvel utilisateur



Propriétés du compte new – Membre de – Ajouter – Avancé – Rechercher

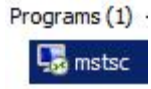
d) Autoriser l'accès distant sur XP

Démarrer – Paramètres – Paneau de configuration – Système – Utilisation à distance

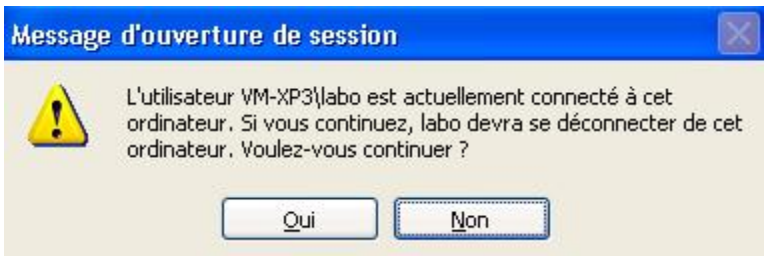


Dans **Choisir des utilisateurs distants**, contrôler que le compte créé y figure

e) Pouvez-vous établir une session mstsc depuis Win7 ?



Start -



XP (comme Win7 ou supérieur) ne supporte qu'une seule session

Vous devez accepter la déconnexion ou redémarrer XP pour autoriser l'accès distant depuis Win7

Session établie depuis Win7 avec Start – mstsc

f) Comment être certain d'avoir obtenue un accès distant ?

ipconfig

Remarques Cet accès GUI est habituellement utilisé par les administrateurs d'un serveur Microsoft
La licence MS Server (2003, 2008, 2013, …) autorise plusieurs clients distants alors que la licence MS client (Win8-Win7-Vista-XP) ne permet qu'une seule session locale ou distante

L'annexe 1 illustre le protocole Spice utilisé dans le monde Linux

§2	SCP (Secure Copy Protocol)	10 min

Objectif Tester l'accès SCP (Secure CoPy) depuis Win7
Cette partie illustre comment nous administrons le serveur 10.2.1.1 CentOS CLI du labo

Action **Arrêter (Power Off) la VM XP**
Importer **Samba_SELinux_disable.ova** (contrôler que le réseau de cette VM est bien en mode Host-only)
Etablir une session avec **Username = root password = rootroot**

a) Quelle est l'adresse IP du serveur Samba ?
ifconfig → 192.168.56.101 ou 102 (dépend de l'état de la VM XP)

b) Etablir une session SCP depuis Win7
Lancer putty pour tester

c) Lancer WinSCP depuis Win7

§3	Configuration du serveur Samba	10 min

Objectif Configurer un serveur de fichiers Linux – Samba
Cette partie illustre la configuration Samba-Linux permettant d'émuler un serveur de fichiers Windows
Tester depuis un client Win7

Etapes Utiliser **Samba_SELinux_disable.ova** du §2

Contrôler dans l'historique des commandes la présence de

- **`yum -y install samba`** Installer le paquet Samba

Désactiver SELinux
Créer le compte **jean**
Créer le dossier **/home/doc** qui sera accessible à **jean**
Donner les droits appropriés
Copier le fichier smb.conf

Corrigé

```
setenforce 0                          Désactiver SELinux
adduser jean
passwd jean
mkdir /home/doc
chmod -R 770 /home/doc
smbpasswd –a jean
copier /etc/samba/smb.conf            avec WinSCP (voir §2)
service smb start
service nmb start
```

a) A quoi sert **`mkdir /home/doc`** ?
b) A quoi sert **`chmod -R 770 /home/doc`** ?
c) A quoi sert **`smbpasswd –a jean`** ?
Contrôler au besoin vos réponses avec http://www.tdeig.ch/ITI2_Secu/Archives/33_Lab_Linux.pdf

d) Dans smb.conf, quelle est l'utilité de **`writable = yes`** ?
e) Dans smb.conf, quelle est l'utilité de **`browseable = yes`** ?
f) Dans smb.conf, quelle est l'utilité de **`valid users = jean`** ?

La doc Samba est volumineuse et indigeste
Liens utiles :

- http://christian.trillaud.free.fr/minal/samba.htm
- http://stephane.boireau.free.fr/informatique/samba/samba/samba_exemple5_mode_user.htm

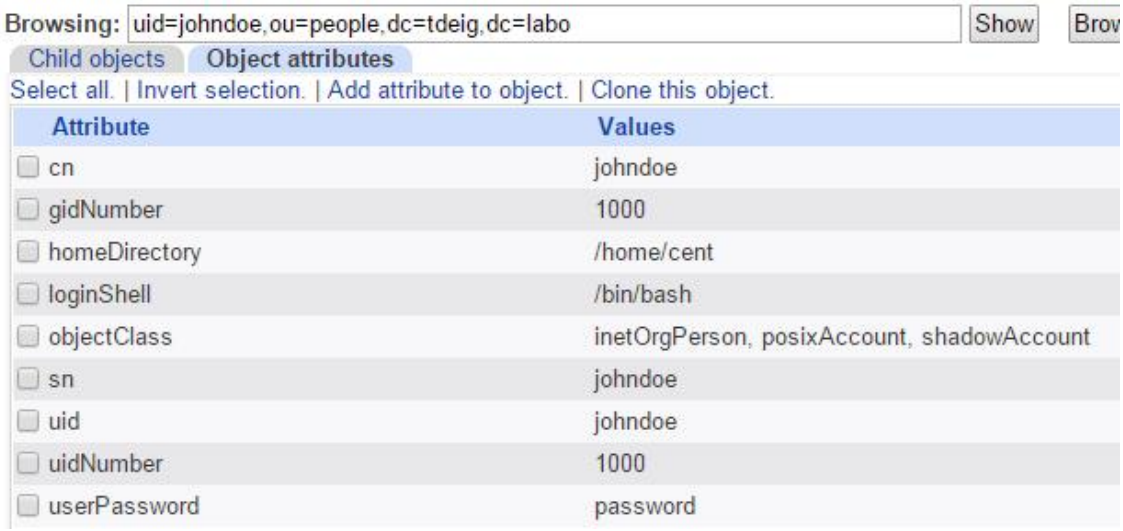
§4	Annuaire LDAP	10 min

Objectif Accéder aux champs d'un utilisateur
Cette partie illustre la notion d'annuaire
Tester avec le navigateur IE
Utiliser l'outil webmin → http://www.webmin.com/

Remarque La configuration utilisée pour ce serveur LDAP provient de
http://www.server-world.info/en/note?os=CentOS_6&p=ldap

Action **Arrêter (Power Off) la VM Samba_SELinux_disable**
Utiliser **LDAP_GL.ova** (**Username = root password = rootroot**)
Depuis Win7 :
Contrôler avec ping la connexion avec IP = 192.168.56.117
Accès avec Webmin **http://192.168.56.117:10000/**
Colonne de gauche : **Servers** – **LDAP Server**
Browse Database : cocher ou=people

a) Quels sont les champs du compte Johndoe



Attribute	Values
cn	johndoe
gidNumber	1000
homeDirectory	/home/cent
loginShell	/bin/bash
objectClass	inetOrgPerson, posixAccount, shadowAccount
sn	johndoe
uid	johndoe
uidNumber	1000
userPassword	password

Action Accéder à cet annuaire avec le navigateur IE (car Google Chrome ne supporte pas ldap://)
`ldap://192.168.56.117/dc=tdeig,dc=labo??sub?(sn=johndoe)`

Objectif Utiliser http://www.commentcamarche.net/contents/631-ldap-le-modele-d-information pour ajouter l'attribut **telephonenumber**
Tester avec IE

Action L'acquisition **LDAP.pcap** a été obtenue à partir de l'action précédente
Utiliser ce fichier pour répondre aux questions

b) Quel est le numéro de téléphone de Johndoe ?
Paquet 15

```
⊟ Lightweight Directory Access Protocol
  ⊟ LDAPMessage searchResEntry(3) "uid=johndoe,ou=people,dc=tdeig,dc=labo" [2 results]
      messageID: 3
    ⊟ protocolOp: searchResEntry (4)
      ⊟ searchResEntry
          objectName: uid=johndoe,ou=people,dc=tdeig,dc=labo
        ⊟ attributes: 9 items
          ⊞ PartialAttributeList item objectClass
          ⊞ PartialAttributeList item uid
          ⊞ PartialAttributeList item cn
          ⊞ PartialAttributeList item sn
          ⊞ PartialAttributeList item loginShell
          ⊞ PartialAttributeList item uidNumber
          ⊞ PartialAttributeList item gidNumber
          ⊞ PartialAttributeList item homeDirectory
          ⊟ PartialAttributeList item telephoneNumber
              type: telephoneNumber
            ⊟ vals: 1 item
                AttributeValue: 1234567890
```

§5	Samba-LDAP	20 min

Objectif

Accéder à un dossier partagé via une authentification LDAP
Test depuis un client CentOS

Etapes

Créer un dossier partagé
Utiliser l'outil SWAT (Samba Web Admin Tool) avec le **navigateur Chrome**
Créer un compte compatible avec Samba

Action

Contrôler que la VM **LDAP_GL** est active
Utiliser **SAMBA.ova** (**Username = root password = rootroot**)
Depuis Win7 : contrôler avec ping la connexion

Créer dossier partagé sur SAMBA

```
setenforce 0                    Désactiver SELinux
mkdir /home/partage
chmod -R 777 /home/partage
```

Depuis Win7 : accès à SWAT avec **192.168.56.xxx:901**

- Onglet SHARES
- Create Share = SMB
- Clic sur Create Share
- Modifier les champs :
  - path : /home/partage
  - available : Yes
- Sauver les modifications avec Commit Changes

- Vérifier dans l'onglet VIEW
- Voir balise SMB en bas de page

Sur SAMBA : créer le compte paul

```
smbldap-useradd -amg 513 -A 1 paul
smbldap-passwd paul
```

Utiliser **Client.ova** pour tester

```
smbclient //192.168.56.xxx/SMB -U paul
```

Ajouter un fichier et un dossier dans le partage
Tester l'accès

Parcourir la documentation
http://manpages.ubuntu.com/manpages/utopic/en/man8/smbldap-useradd.8.html

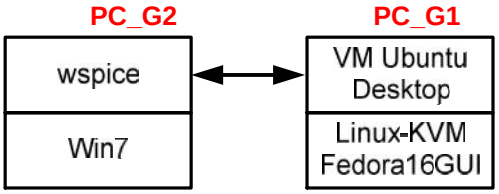
Tester avec le client Win7

Annexe 1 : Laboratoire VDI (Virtual Desktop Infrastructure)

0	Introduction	sudo ./c X

Ce travail de laboratoire a pour objectif l'étude de solution de VDI basées sur le protocole Open Source Spice developpé par Qumranet puis Red Hat.

Configuration pour ce travail pratique:



- **PC-Fedora16GUI** relié à l'intranet du labo
  labotd (compte utilisateur), password: labolabo
  root (compte administrateur), password: rootroot

- La machine virtuelle (VM) utilise le système d'exploitation **Ubuntu Desktop 12**
  labotd (compte utilisateur), password: labolabo
  root (compte administrateur), password: rootroot
  Elle se trouve sur le partage NFS dans **`/10.2.1.1/nfs_share/labo_vdi/`**

- La machine cliente utilise le système d'exploitation **Windows 7**
  albert(compte administrateur), password: admin

Documents utiles présents dans `\\10.2.1.1\doclabo\Virtu\VDI`

Le fichier **LS_VDI_miniLinux.pdf** décrit le développement, réalisé par Lionel Schaub en 2012, d'un client léger low cost basé sur CPU Atom – 2 GB RAM) sans disque mais avec clé USB et la distribution Linux Core Plus

http://www.linux-kvm.org/page/SPICE

1	Configuration	15 min

But 1.1 **Configurer Spice du côté serveur (Fedora 16 GUI)**

Action Ouvrir **Virtual Machine Manager** (VMM)
Créer une VM selon la procédure décrite au §1 du labo Linux-KVM
~~Démarrer cette VM~~

Afficher les paramètres de cette VM

Modifier les paramètres suivants

- Display VNC changer le type en **Spice - Apply**
- Video : **qxl - Apply**
- NIC: source device: **Host device em1: macvtap** **PC_G1**
  Device model: **virtio**
  source mode: **Bridge**
  Apply

But 1.2 **Modifier le fichier xml de la VM**

Action Dans un terminal avec les droits root
`virsh edit VM` L'éditeur utilisé est vi
Descendre jusqu' à la balise **`<graphics type='spice' autoport='yes' />`**
`i +Enter` pour modifier
`<graphics type='spice' port='5904' autoport='no' listen='0.0.0.0' />`
`Esc + : + wq + Enter` pour enregister

But 1.3 **Configurer Spice sur la VM Ubuntu Desktop**

Action : Démarrer cette VM puis typer
```
apt-get update
apt-get install spice-vdagent
```

But 1.4 **Configurer Spice du côté client Windows**

Action : Copier le dossier **wspice** sur le bureau
Lancer **…`\wspice\lib\spicec.exe`**

Host = adr IP de KVM
Port = 5904

Typer **`'shift + F11'`** pour passer en mode plein écran

2	Etude du flux Client-serveur	20 min

But 2.1 **Analyse du flux de donnée spice**

Remarque L'acquisition spice.pcap a été obtenue dans la configuration suivante :
PC Client Schaub
Diaporama Arm

Action Utiliser le menu Statistics de Wireshark

Q_2.1a Quel est le nombre de paquets capturés ?
Statistics/Summary

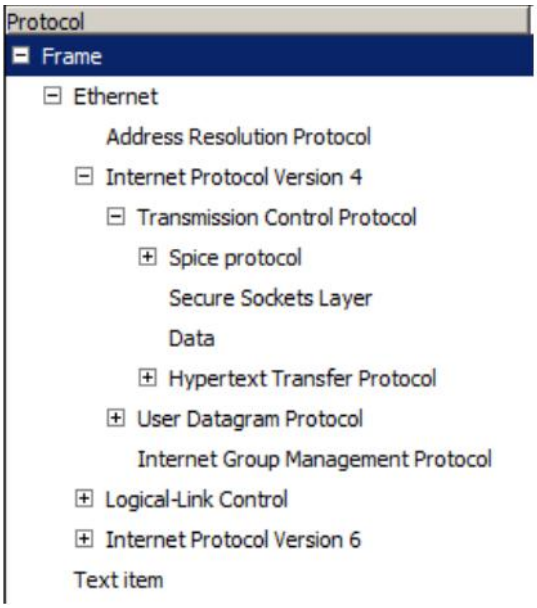
Display

Display filter:	none
Ignored packets:	0

Traffic	Captured	Displayed	Marked
Packets	53925	53925	0
Between first and last packet	153.569 sec		
Avg. packets/sec	351.146		
Avg. packet size	474.684 bytes		
Bytes	25597353		
Avg. bytes/sec	166683.388		
Avg. MBit/sec	1.333		

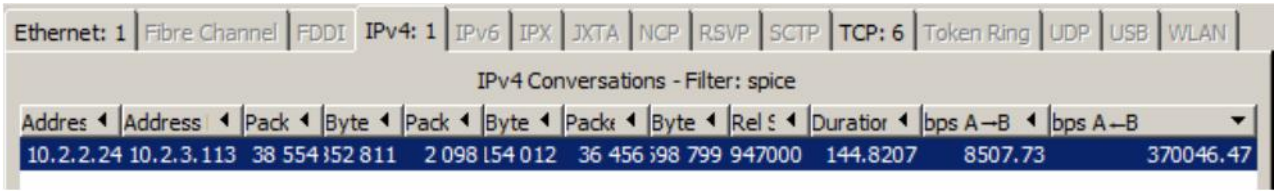
Q_2.1b Combien de temps a duré la capture ? Quel était le débit moyen ?
Dans Statistics/Summary, 153.569 secondes ou 2min30 avec un debit moyen de 1.333MBit/sec

Q_2.1c Quel est en l'hiérarchie des protocoles (l'empilement) utilisés dans cette capture ?
Dans Statistics/Protocol hierarchy, grace à ce menu on observe une dissection par couche OSI des données affichées



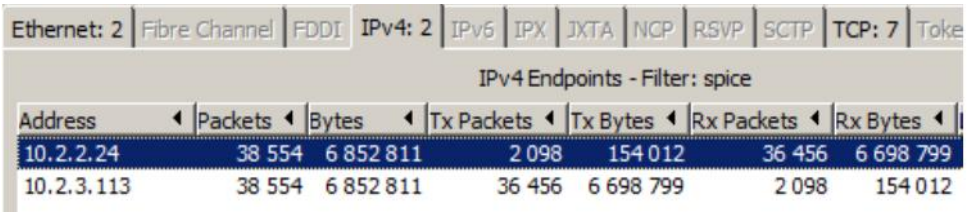
Action Appliquez le filtre "spice"

Q_2.1d Quel est le débit client-serveur puis serveur-client? Limiter la vue au filtre appliqué
Dans Statistics/Conversations, on peut lire les informations dans les colonnes bps. L'adresse du client ici etant 10.2.2.24 et celle du serveur 10.2.3.113



Q_2.1e Quel est le volume de données client-serveur reçu ? Limiter la vue au filtre appliqué

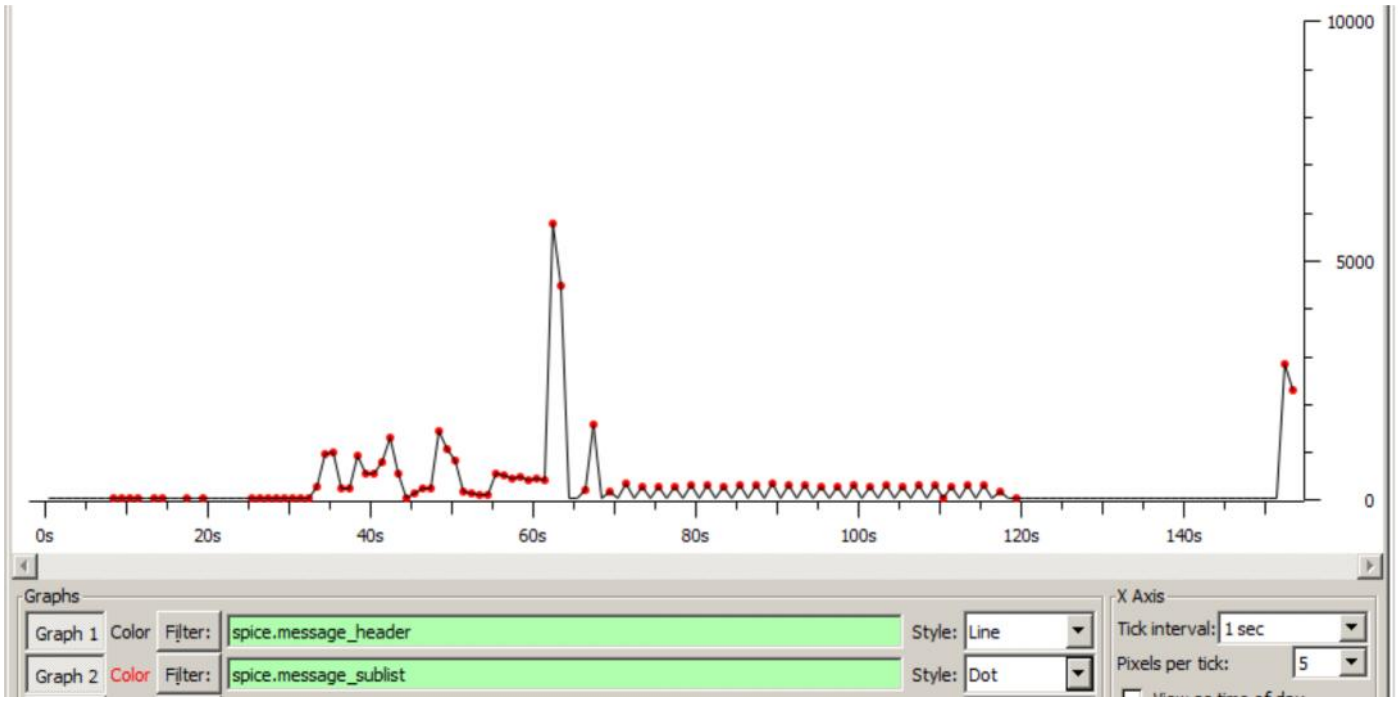
Dans Statistics/Endpoints, on peut lire les informations dans la colonne Rx Bytes

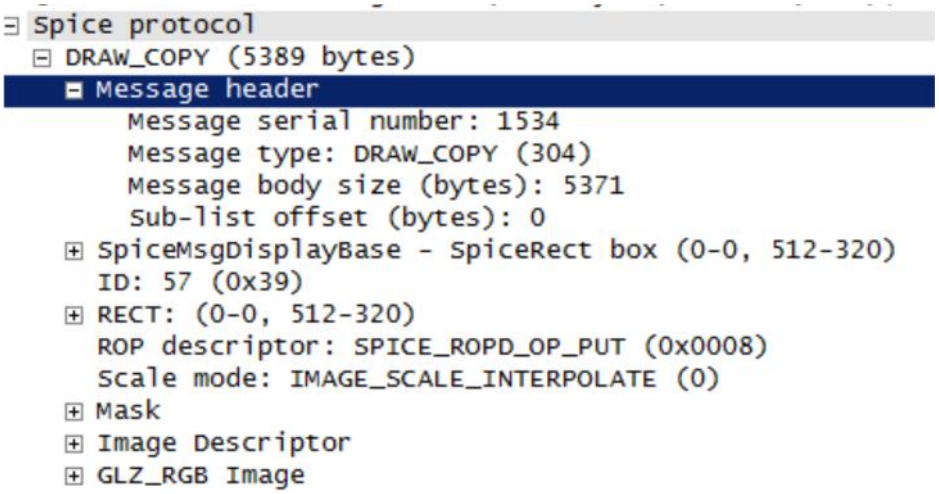


Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
10.2.2.24	38 554	6 852 811	2 098	154 012	36 456	6 698 799
10.2.3.113	38 554	6 852 811	36 456	6 698 799	2 098	154 012

Q_2.1f Tracez deux graphes en appliquant les filtre suivant:
spice.message_header(graph 1) et spice.message_sublist (graph2)
Que constatez-vous ?

Dans Statistics/IO Graphs, les deux graphes se superposent car le deuxieme filtre et inclut dans le 1er. Lorsqu'on clique sur un point du graph 1, on observe dans le resultat wireshark que message header et le premier niveau du protocole spice.





Remarque **Pour plus de détails sur le protocole spice voir le document:**
`/10.2.1.1/nfs_share/labo_vdi/documents/spice_protocol.pdf`