

MISE EN PLACE D'UN
ENVIRONNEMENT DE TRAVAIL
PERSONNEL

GEORDY BALOU

BTS SIO SISSR

CFA INGETIS PARIS



SOMMAIRE

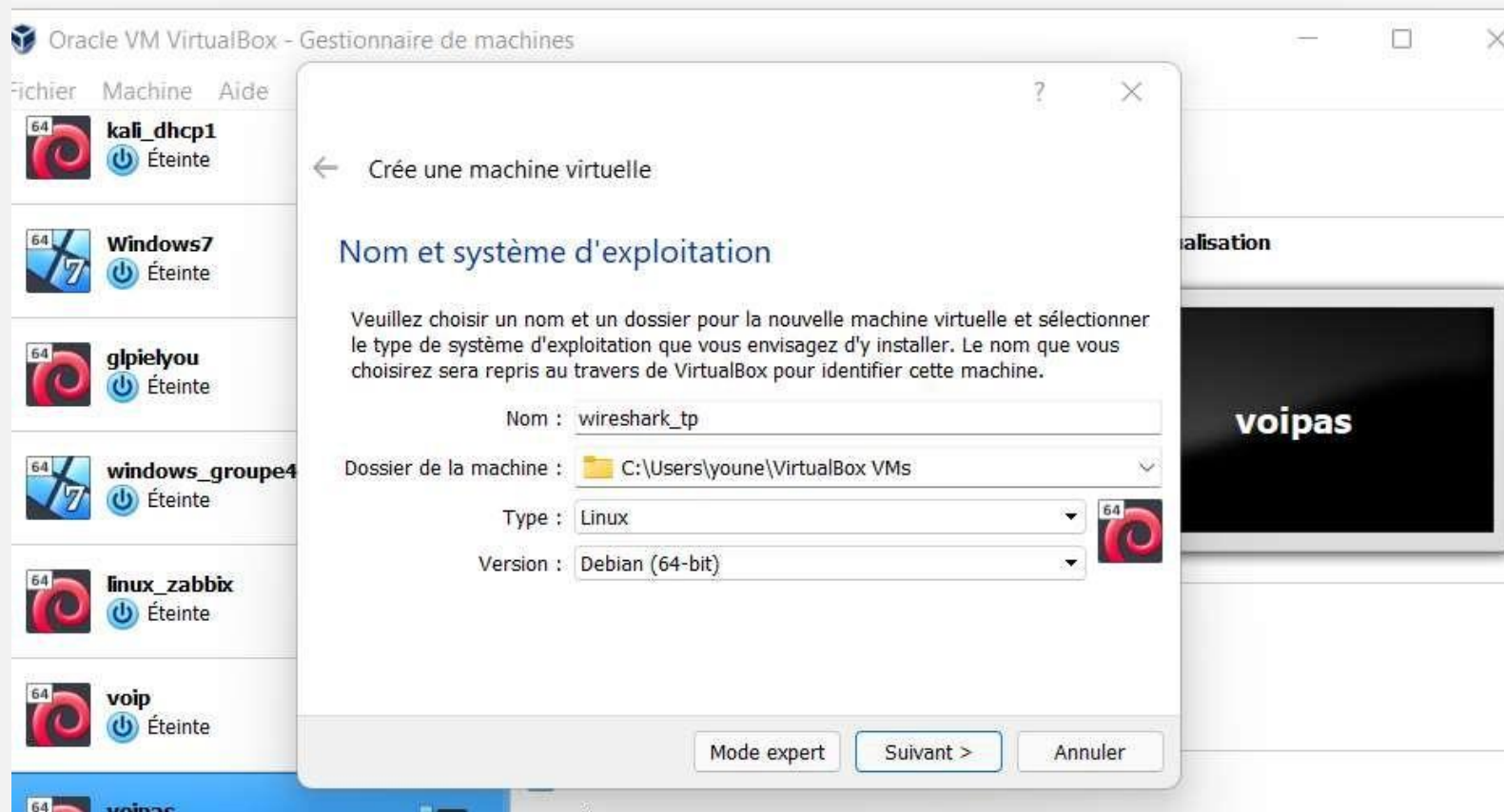
- Définition
- Installation
- wireshark

DÉFINITION

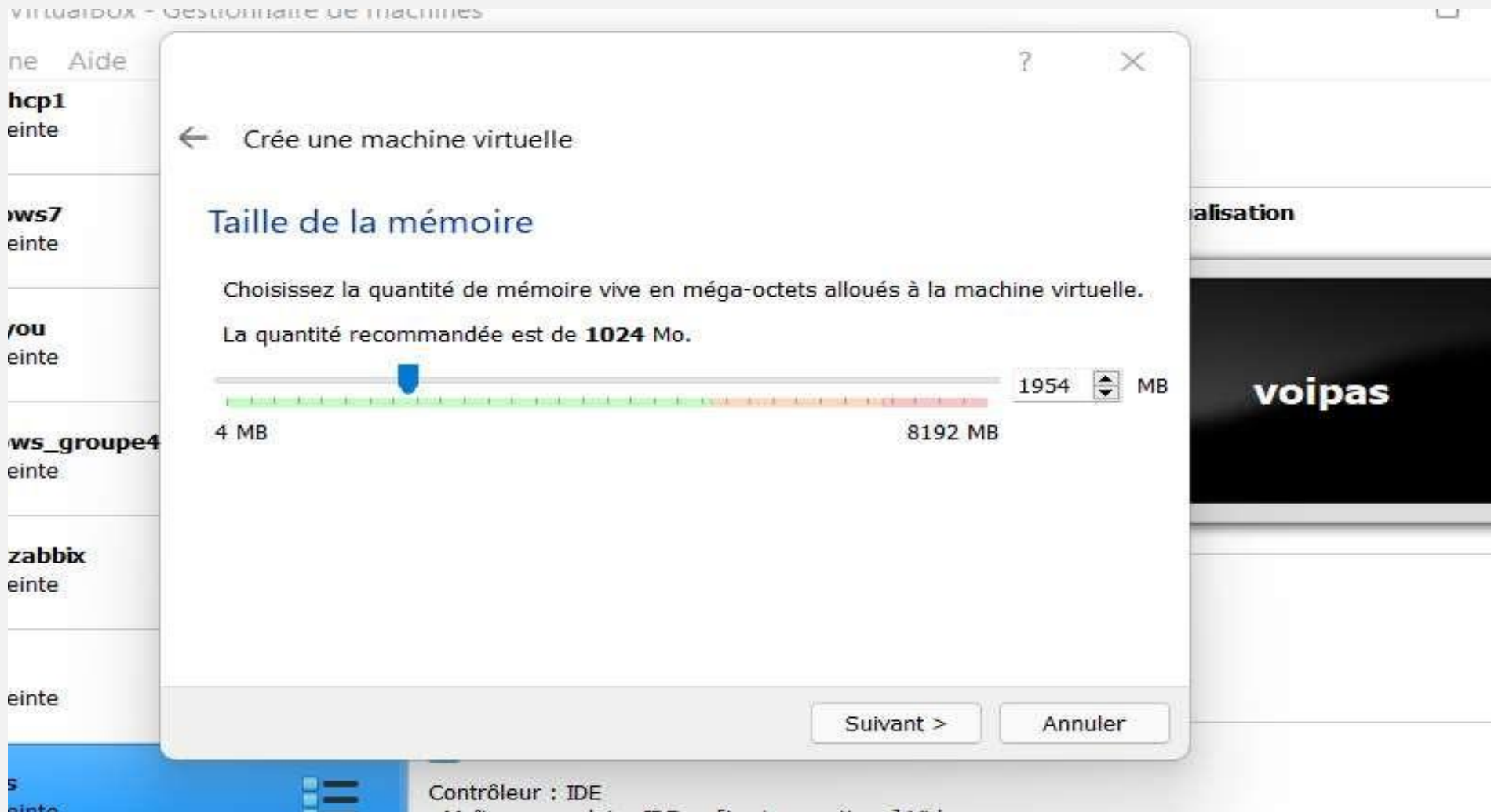
- Un environnement d'apprentissage personnel est un système ou un écosystème qui aident des apprenants à construire, organiser eux-mêmes leur apprentissage. C'est un environnement qui rend l'apprenant capable dans son processus d'apprentissage
-
- Afin de mettre en place cet environnement régulièrement je fais des travaux pratiques afin pratiquer et ainsi de mieux connaître mon cours alors pour cet fois j'ai choisi de vous présenter mon travaux pratiques sur Wireshark qui est un analyseur de paquets libre et gratuit. Il est utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro-ingénierie.
-
- J'ai choisi Wireshark car c'est un outil souvent utiliser dans la cyber sécurité et qui permet d'encadrer les paquets qui transit au sein du réseau.

INSTALLATION

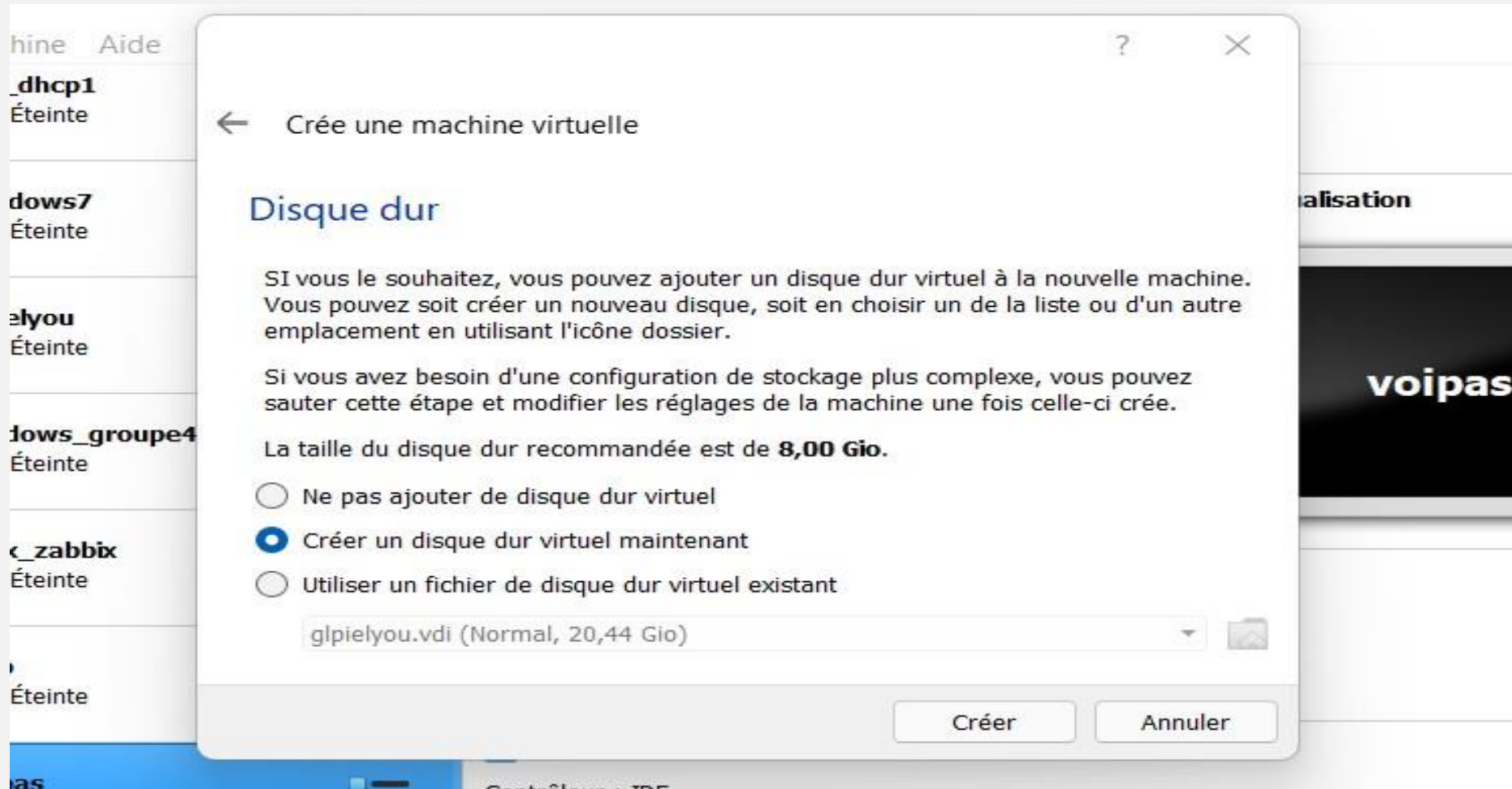
- Dans un premier temps nous allons créer une machine virtuelle avec virtualbox qui est un hyperviseur de type 2

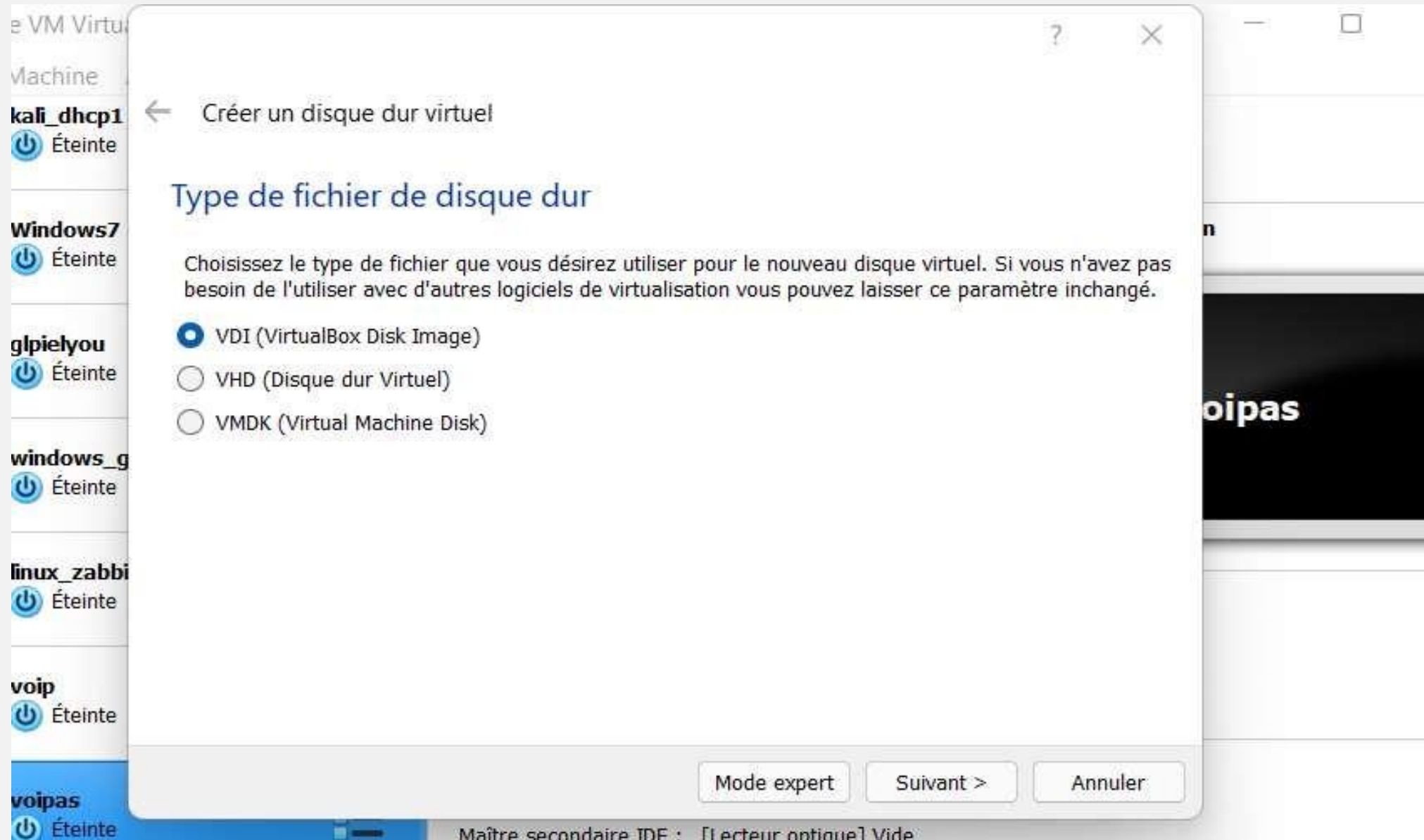


- On configure la mémoire de la machine virtuelle :



- Ensuite on configure le disque dur :





← Créer un disque dur virtuel

Stockage sur disque dur physique

Veillez choisir si le nouveau fichier de disque dur virtuel doit croître au fur et à mesure (allocation dynamique) ou bien s'il doit être créé à sa taille maximale (taille fixe).

Un fichier de disque dur **alloué dynamiquement** n'utilisera d'espace sur votre disque dur physique qu'au fur et à mesure qu'il se remplira (jusqu'à une **taille fixe maximale**), **cependant il ne se réduira pas automatiquement lorsque de l'espace sur celui-ci sera libéré.**

Un fichier de disque dur à **taille fixe** sera plus long à créer sur certains systèmes mais sera souvent plus rapide à utiliser.

- ☒ Dynamiquement alloué
- ☐ Taille fixe

Suivant >

Annuler

← Créer un disque dur virtuel

Emplacement du fichier et taille

Veuillez saisir un nom pour le nouveau fichier de disque dur virtuel dans la boîte ci-dessous ou cliquez sur l'icône dossier pour choisir un autre dossier dans lequel le créer.

C:\Users\youne\VirtualBox VMs\wireshark_tp\wireshark_tp.vdi



Choisissez la taille du disque dur virtuel en mégaoctets. Cette taille est la limite de la quantité de données de fichiers qu'une machine virtuelle sera capable de stocker sur le disque dur.

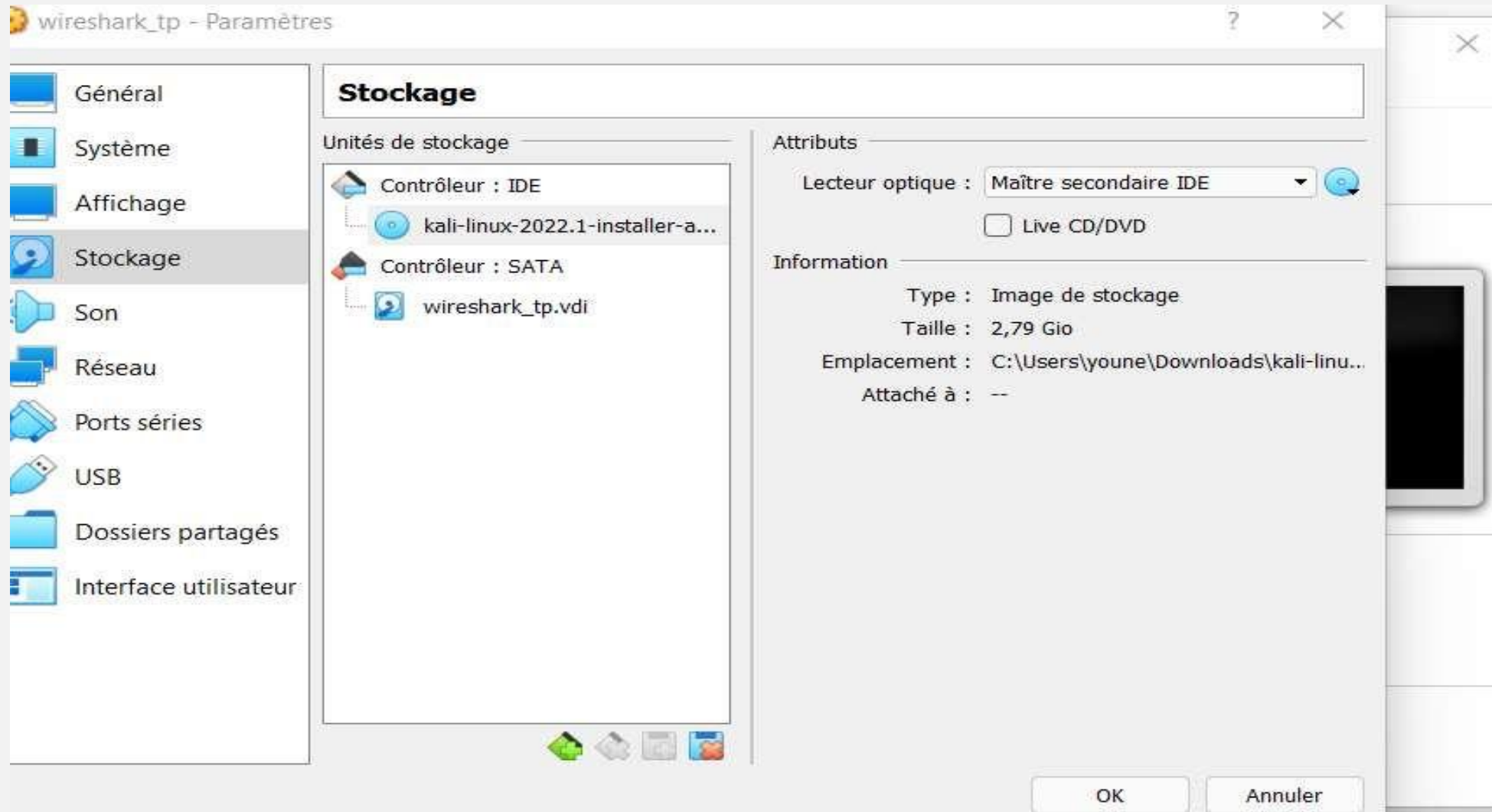


Créer

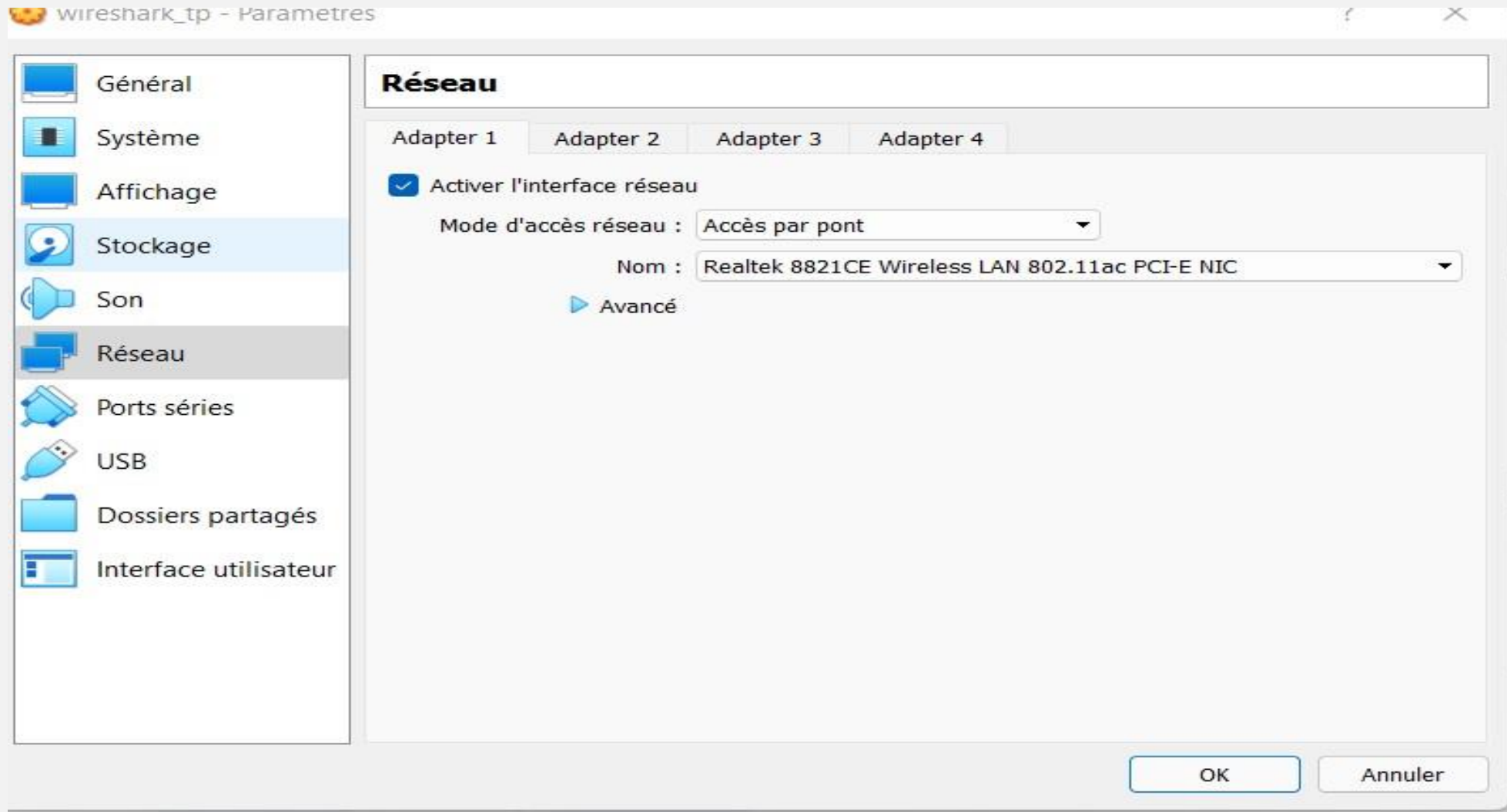
Annuler

Maître secondaire IDE : [Lecteur optique] Vide
Contrôleur : SATA

- Dans la configuration de la machine nous allons dans stockage pour mettre l'iso



- Egalement on change le mode d'accès réseau par « accès par pont »



- On démarre la machine puis on gère l'installation



Configurer le réseau

Veuillez indiquer le nom de ce système.

Le nom de machine est un mot unique qui identifie le système sur le réseau. Si vous ne connaissez pas ce nom, demandez-le à votre administrateur réseau. Si vous installez votre propre réseau, vous pouvez mettre ce que vous voulez.

Nom de machine :

Créer les utilisateurs et choisir les mots de passe

Un bon mot de passe est composé de lettres, chiffres et signes de ponctuation. Il devra en outre être changé régulièrement.

Mot de passe pour le nouvel utilisateur :

☐ **Afficher le mot de passe en clair**

Veuillez entrer à nouveau le mot de passe pour l'utilisateur, afin de vérifier que votre saisie est correcte.

Confirmation du mot de passe :

☐ **Afficher le mot de passe en clair**

Partitionner les disques

Si vous continuez, les modifications affichées seront écrites sur les disques. Dans le cas contraire, vous pourrez faire d'autres modifications.

Les tables de partitions des périphériques suivants seront modifiées :

SCSI2 (0,0,0) (sda)

Les partitions suivantes seront formatées :

partition n° 1 sur SCSI2 (0,0,0) (sda) de type ext4

partition n° 5 sur SCSI2 (0,0,0) (sda) de type swap

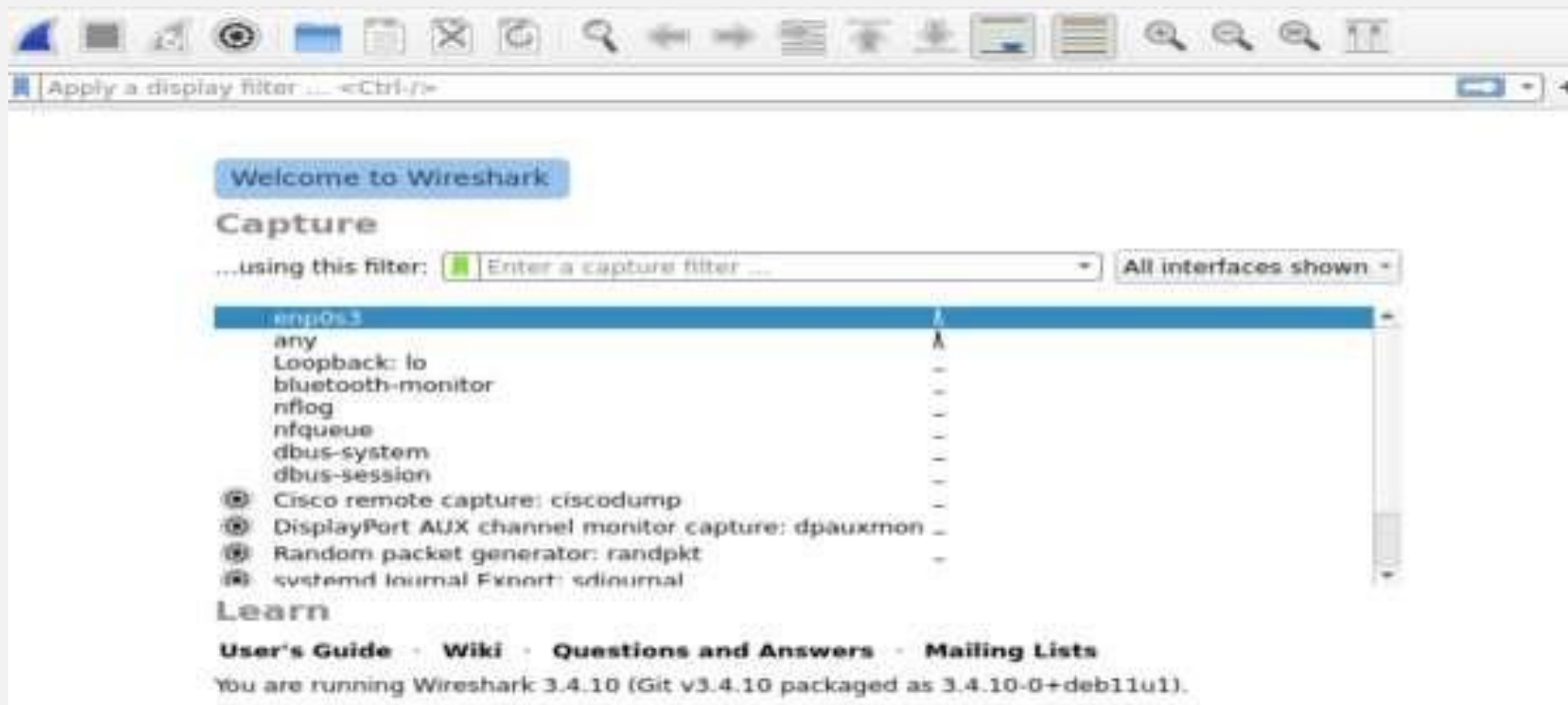
Faut-il appliquer les changements sur les disques ?

☐ Non

☒ **Oui**

WIRESHARK

- Après avoir installé la machine virtuelle nous allons utiliser wireshark afin de comprendre ce logiciel
- Voici la page d'accueil de wireshark



- Ensuite lorsqu'on appuie sur enp0s3 puis sur démarrer on verra les transmissions de paquets au sein du réseau :

Capture en cours de enp0s3

Echier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
4466	13.360411953	2a00:1450:4007:818::	2a01:cb08:191:4700::	TCP	86	443 → 45708 [ACK] Seq=8445217
4467	13.360412013	2a00:1450:4007:818::	2a01:cb08:191:4700::	TCP	86	443 → 45708 [FIN, ACK] Seq=8445217
4468	13.360412050	2a00:1450:4007:818::	2a01:cb08:191:4700::	TCP	86	443 → 45708 [ACK] Seq=8445218
4469	13.360429793	2a01:cb08:191:4700::	2a00:1450:4007:818::	TCP	86	45708 → 443 [ACK] Seq=1492 Ack=
4470	13.3604300820	Sagemcom_31180/cb	IEEE 1545.1-Control	ieee1545	66	Topology discovery
4471	15.120390143	2a01:cb08:191:4700::	2001:41d0:1004:b27::	NTP	110	NTP Version 4, client
4472	15.120390913	Sagemcom_31180/cb	Broadcast	homePL	20	PLC Management
4473	15.120400002	2001:41d0:1004:b27::	2a01:cb08:191:4700::	NTP	110	NTP Version 4, server

Frame 1: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface enp0s3, id 0

Ethernet II, Src: PcsCompu_38:08:28 (08:00:27:30:08:28), Dst: IPv6mcast_16 (33:33:00:00:00:16)

Internet Protocol Version 6, Src: fe80::a00:27ff:fe30:828, Dst: ff02::15

Internet Control Message Protocol v6

```

0000  33 33 00 00 00 16 08 00  27 30 08 28 85 dd 00 00  33 00 00 00 00 00 00 00
0010  00 00 00 00 4c 00 01 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0020  27 ff fe 30 08 28 ff 02  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0030  00 00 00 00 00 00 16 3a 00  05 02 00 00 01 00 8f 00  00 00 00 00 00 00 00 00
0040  8b fd 00 00 00 03 04 00  00 00 ff 02 00 00 00 00  00 00 00 00 00 00 00 00
0050  00 00 00 00 00 01 ff 17  9e 17 04 00 00 00 ff 02  00 00 00 00 00 00 00 00
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 fb 04 00  00 00 00 00 00 00 00 00
0070  00 00 ff 02 00 00 00 00  00 00 00 00 00 00 01 ff 30  00 00 00 00 00 00 00 00
0080  08 28
  
```

- Afin de montrer que lorsqu'on divulgue des informations dans un site non sécurisé
- A l'aide d'un logiciel comme wireshark nous pouvons voir en claire ces informations :
-
- Nous allons sur le site : <http://dev.knl.im/wireshark/> et nous mettrons un identifiant et un mot de passe : admin et password



- A l'aide de Wireshark nous allons pouvoir obtenir énormément d'informations sur cette transmission de paquets, notamment l'identifiant et le mot de passe :

Apply a display filter ... <Ctrl-/>							
No.	Time	Source	Destination	Protocol	Length	Info	
10	3.336163793	192.168.1.35	46.105.38.206	TCP	66	39398 → 80	[ACK]
11	3.336415353	192.168.1.35	46.105.38.206	HTTP	595	POST /wireshark	
12	3.382004844	46.105.38.206	192.168.1.35	TCP	66	80 → 39398	[ACK]
13	3.382004894	46.105.38.206	192.168.1.35	HTTP	296	HTTP/1.1 200 OK	
14	3.382076577	192.168.1.35	46.105.38.206	TCP	66	39398 → 80	[ACK]
Source: PcsCompu 30:08:28 (08:00:27:30:08:28)							
Type: IPv4 (0x0000)							
Internet Protocol Version 4, Src: 192.168.1.35, Dst: 46.105.38.206							
0100 = Version: 4							
.... 0101 = Header Length: 20 bytes (5)							
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)							
01f0	72 65 72 3a 20 68 74 74 70 3a 2f 2f 64 65 76 2e	rer: htt p://dev.					
0200	6b 6e 6c 2e 69 6d 2f 77 69 72 65 73 68 61 72 6b	kml.img & Ireshark					
0210	2f 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63	/- Upgra de-Insec					
0220	75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d	ure-Requ ests: 1					
0230	0a 0d 0a 75 73 65 72 6e 61 6d 65 3d 61 64 6d 69	-- usern ame=admi					
0240	6e 26 70 61 73 73 77 6f 72 64 3d 70 61 73 73 77	n&passwo rd=passw					
0250	6f 72 64	ord					