Wireshark & Iperf

NA 有線組 林子傑

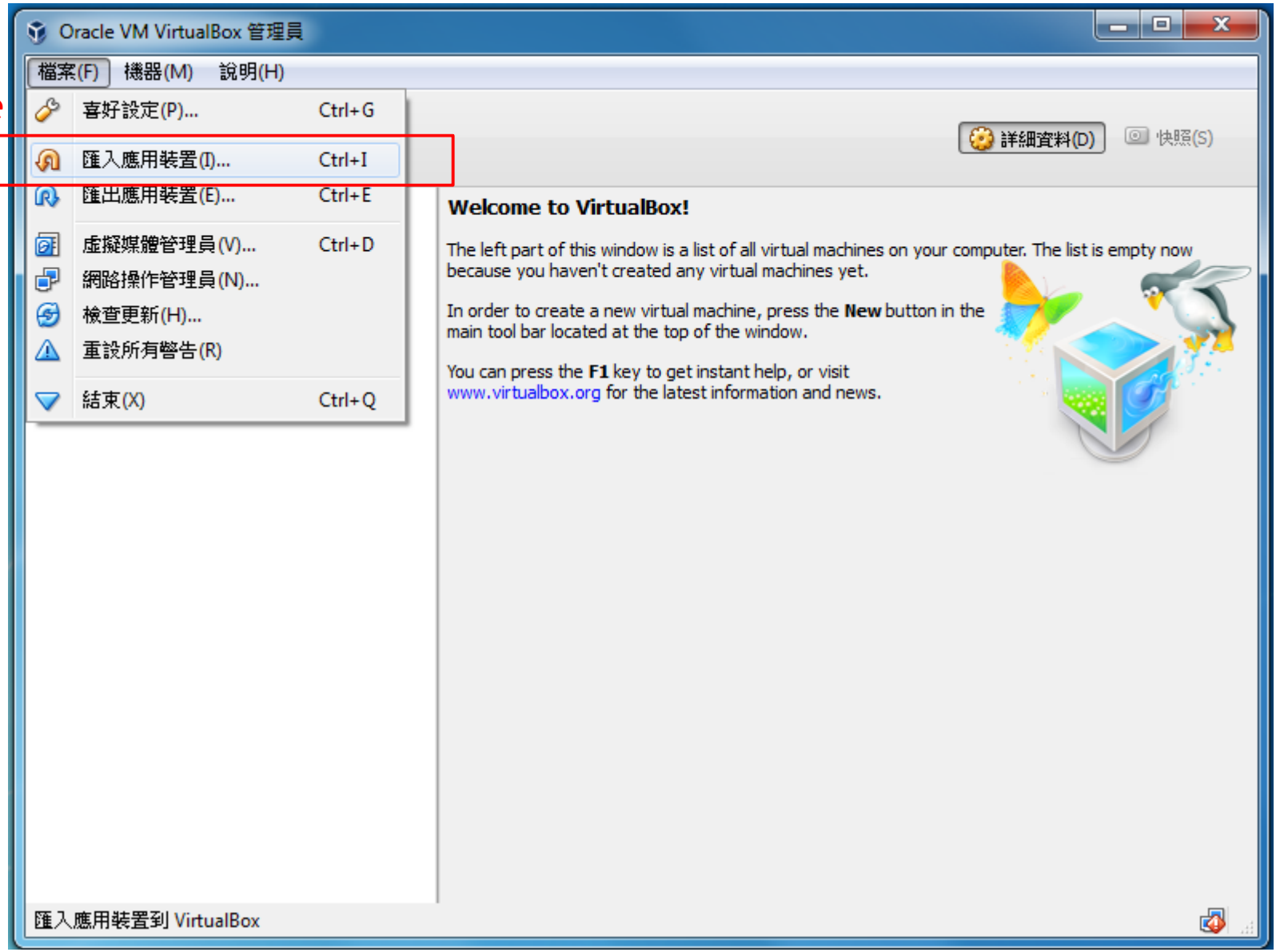
Intro

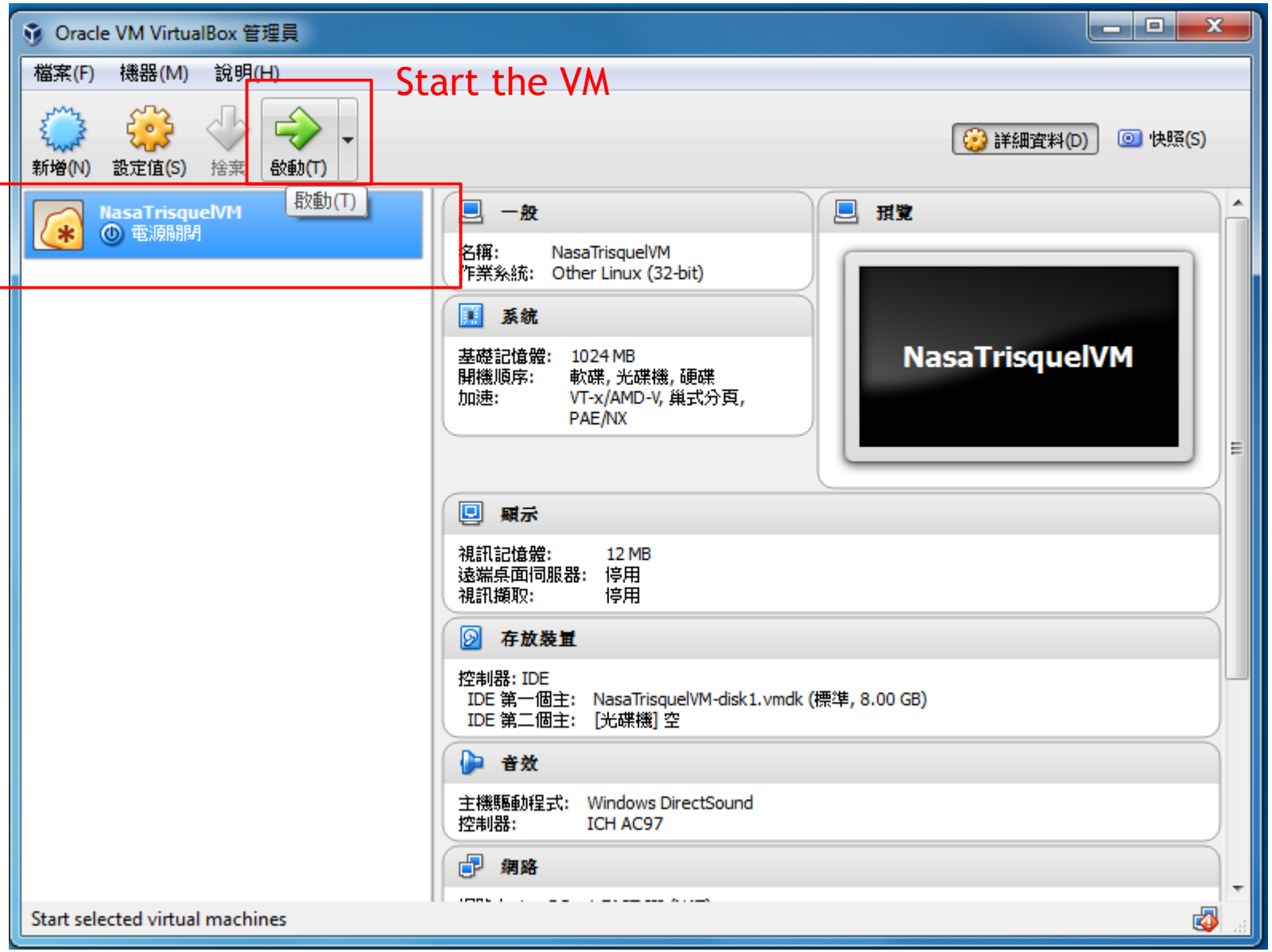
- What is “Wireshark”?
  - A software tool that sniffs the network traffic transmitted from your own PC.
- What is “iperf”?
  - A software tool that examines the network bandwidth between 2 hosts.

Get a VM!

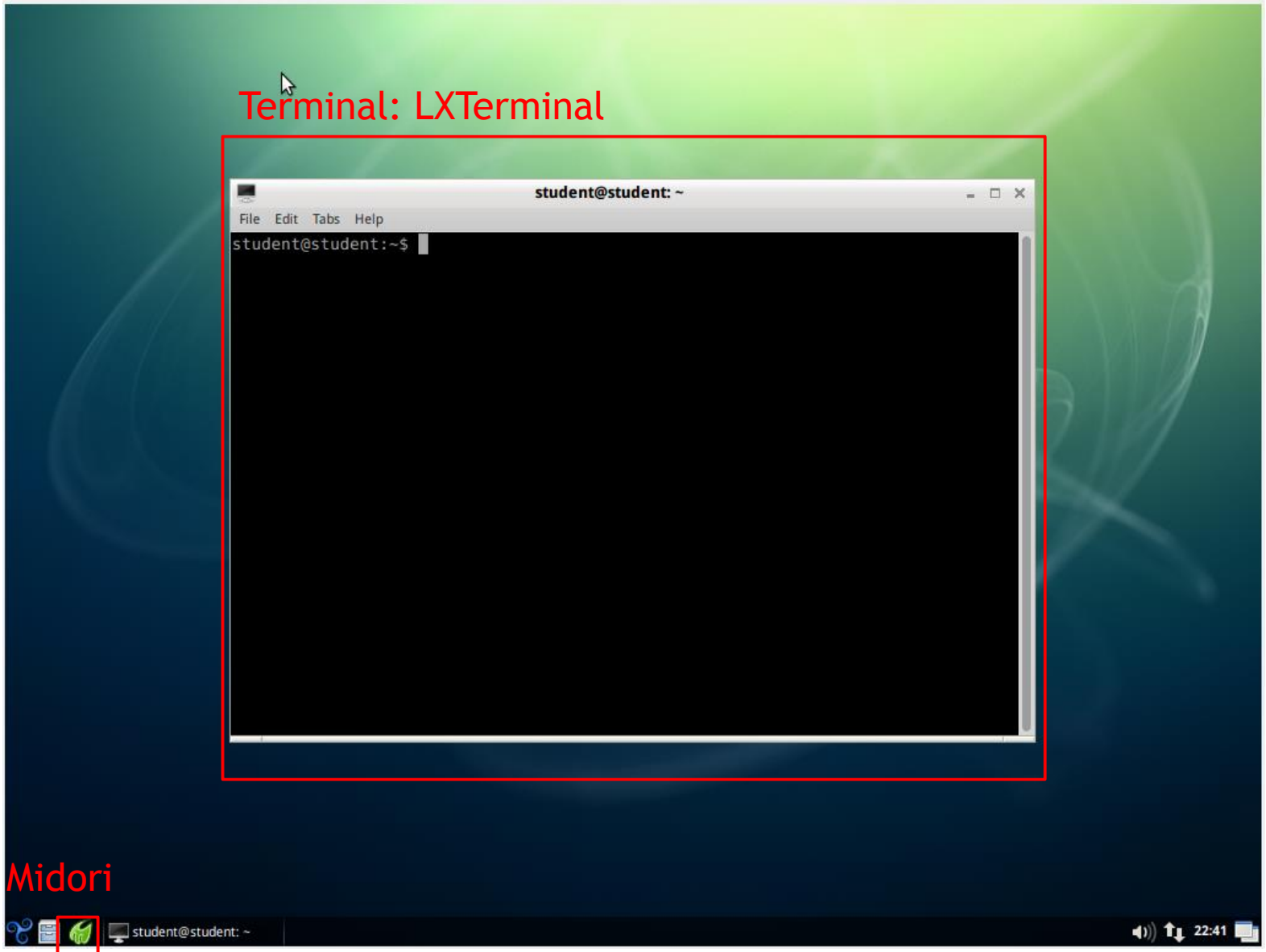
- Why experiment in VM?
  - Wireshark needs to privileged mode to do traffic sniffing.
  - Install any package you want!
  - Backup & Recovery
- How?
  - Import the VM image provided by TAs.
  - Install by yourself.

Import a VM image




Oracle VM VirtualBox 管理員
檔案(F)
機器(M)
說明(H)
Start the VM
新增(N)
設定值(S)
捨棄
啟動(T)
詳細資料(D)
快照(S)
NasaTrisquelVM
電源關閉
一般
名稱: NasaTrisquelVM
作業系統: Other Linux (32-bit)
系統
基礎記憶體: 1024 MB
開機順序: 軟碟, 光碟機, 硬碟
加速: VT-x/AMD-V, 巢式分頁, PAE/NX
預覽
NasaTrisquelVM
顯示
視訊記憶體: 12 MB
遠端桌面伺服器: 停用
視訊擷取: 停用
存放裝置
控制器: IDE
IDE 第一個主: NasaTrisquelVM-disk1.vmdk (標準, 8.00 GB)
IDE 第二個主: [光碟機] 空
音效
主機驅動程式: Windows DirectSound
控制器: ICH AC97
網路
Start selected virtual machines

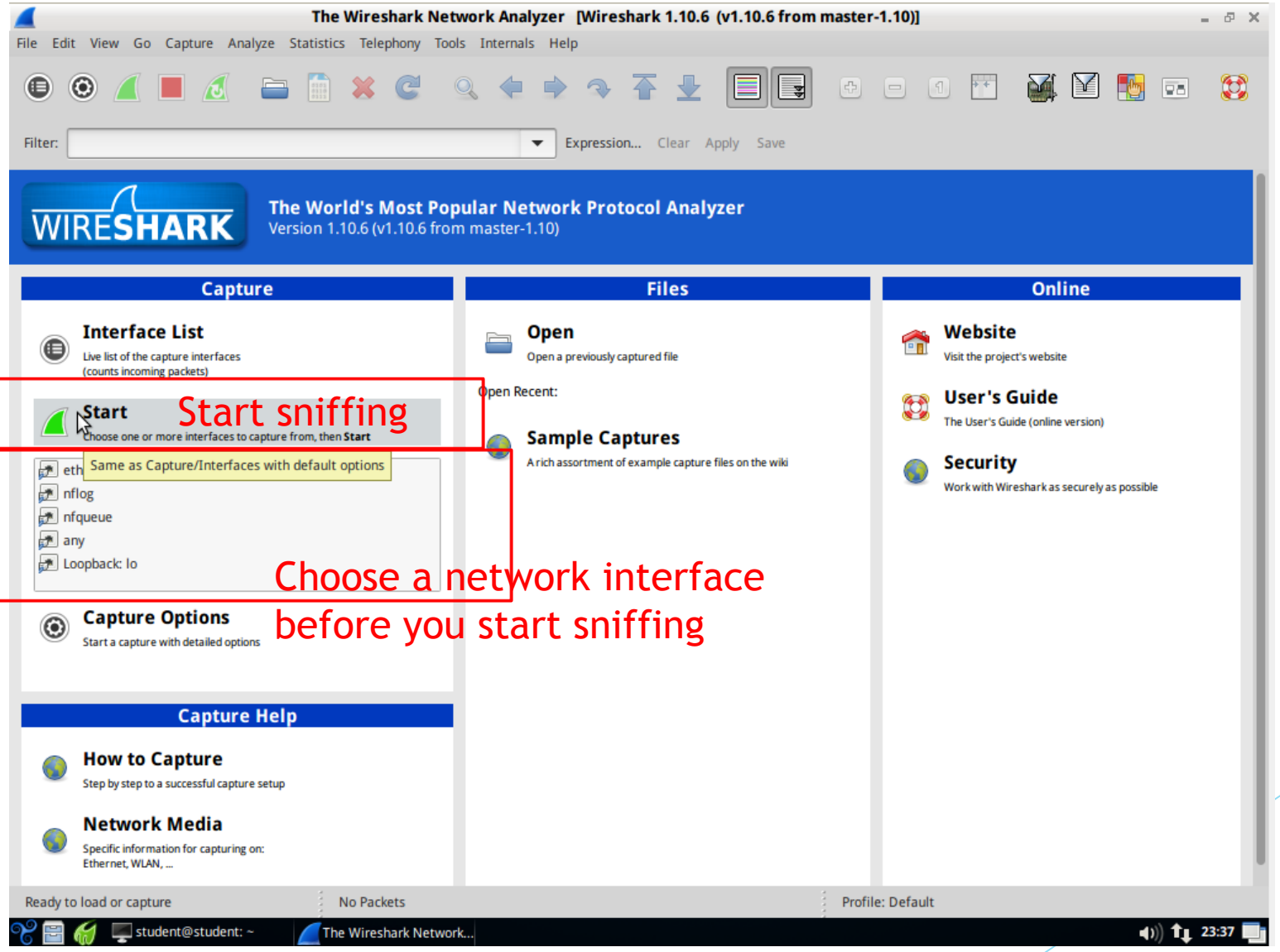
OS: Trisquel Linux



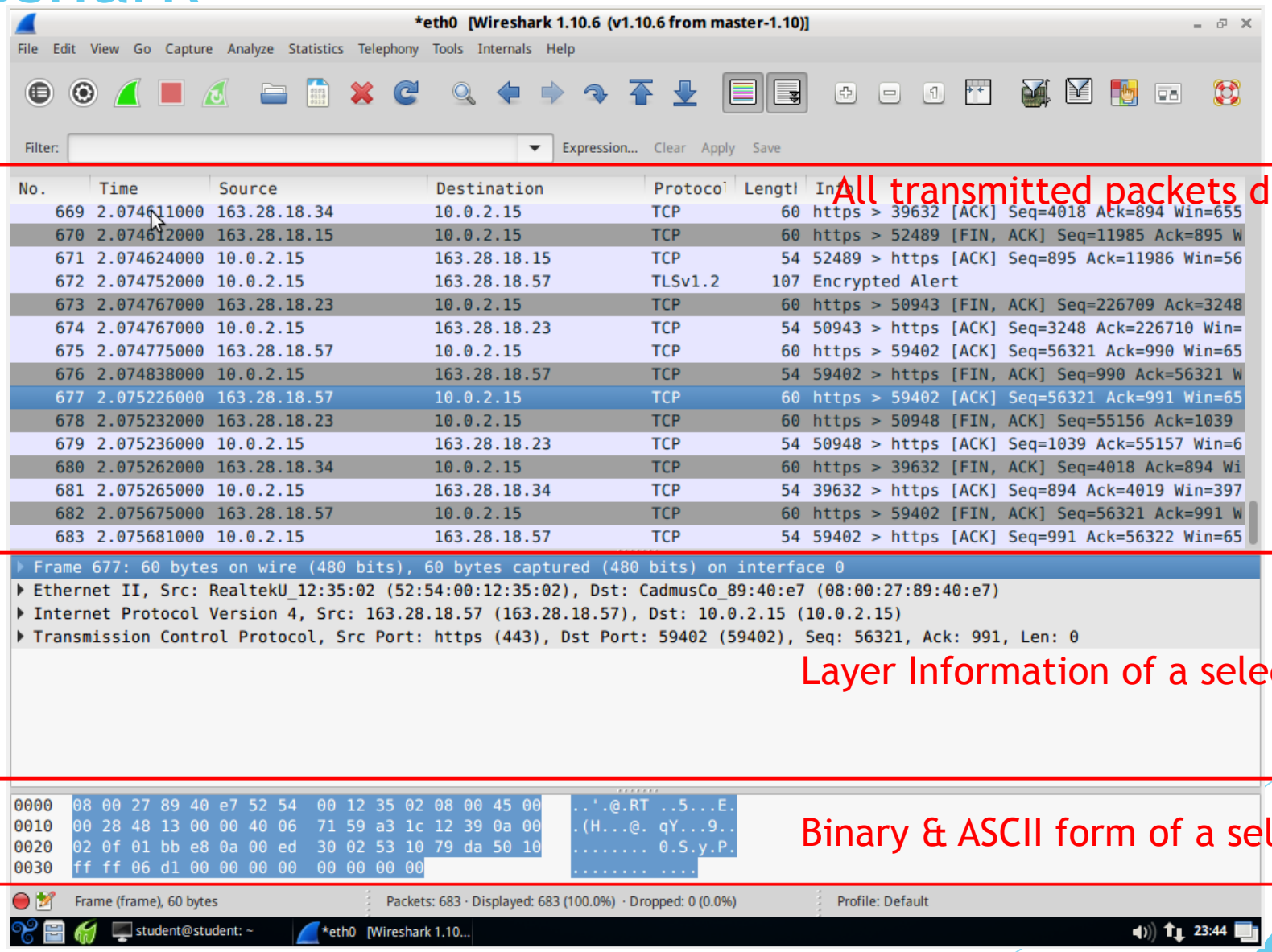
Our VM Enviroment:

- OS: Trisquel Linux (A branch from Ubuntu, light-weight OS)
- Account/Password: student/student
- Default Browser: Midori (Not Firefox or Chrome!)
- Shortcut for Terminal: Ctrl+Alt+T
- Install “Wireshark”:
  - sudo apt-get install wireshark
- Install “iperf”:
  - sudo apt-get install iperf

Wireshark


The Wireshark Network Analyzer [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.10.6 (v1.10.6 from master-1.10)
Capture
Interface List
Live list of the capture interfaces
(counts incoming packets)
Start
Choose one or more interfaces to capture from, then Start
Same as Capture/Interfaces with default options
eth
nflog
nfqueue
any
Loopback: lo
Capture Options
Start a capture with detailed options
Files
Open
Open a previously captured file
Open Recent:
Sample Captures
A rich assortment of example capture files on the wiki
Online
Website
Visit the project's website
User's Guide
The User's Guide (online version)
Security
Work with Wireshark as securely as possible
Capture Help
How to Capture
Step by step to a successful capture setup
Network Media
Specific information for capturing on:
Ethernet, WLAN, ...
Ready to load or capture
No Packets
Profile: Default
student@student: ~
The Wireshark Network...
23:37
Start sniffing
Choose a network interface
before you start sniffing

Wireshark



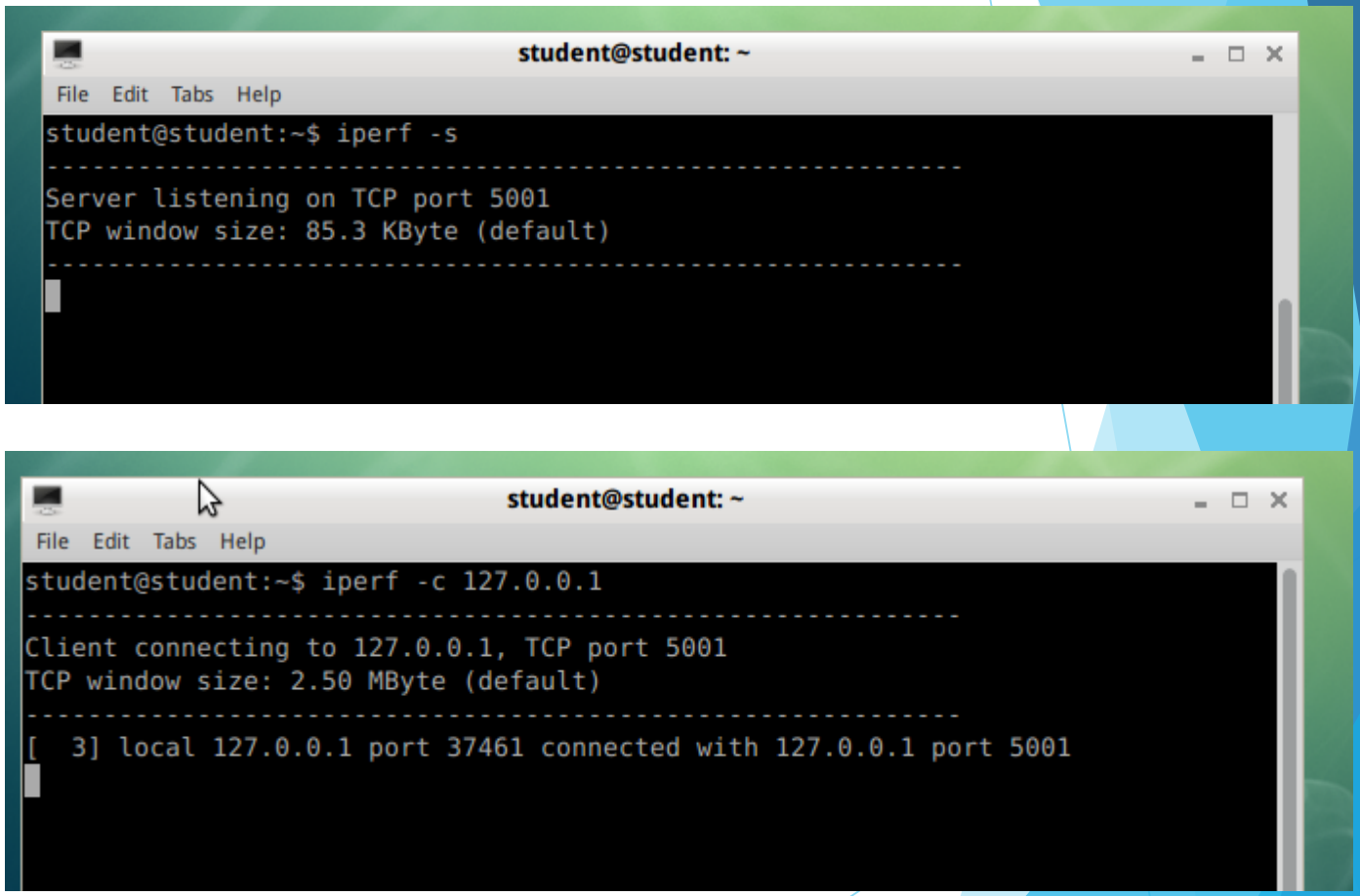
All transmitted packets during sniffing

Layer Information of a selected packet

Binary & ASCII form of a selected packet

Iperf

- It’s a cmd-line utility, Not GUI
- Server-side command:
  - iperf -s
- Client-side command:
  - iperf –c <Server’s IP>



Exercise 1

- Start sniffing the network traffic with Wireshark
- Try to login to 104 Job Bank with any string for Account/Password, e.g. your Student ID
- Stop sniffing and find the transmitted packet.
- Find the Account/Password string you typed previously.

Exercise 2

- Find a partner, and test the bandwidth between your VMs using “iperf”.
- In our VM environment, is server-side IP accessible from the client-side?
  - Hint 1: Adjust your VM’s network interface to “Bridged” not “NAT”!!
  - Hint 2: Google it or Ask TAs!!