

Wireless Ad Hoc Networks

Lab 1

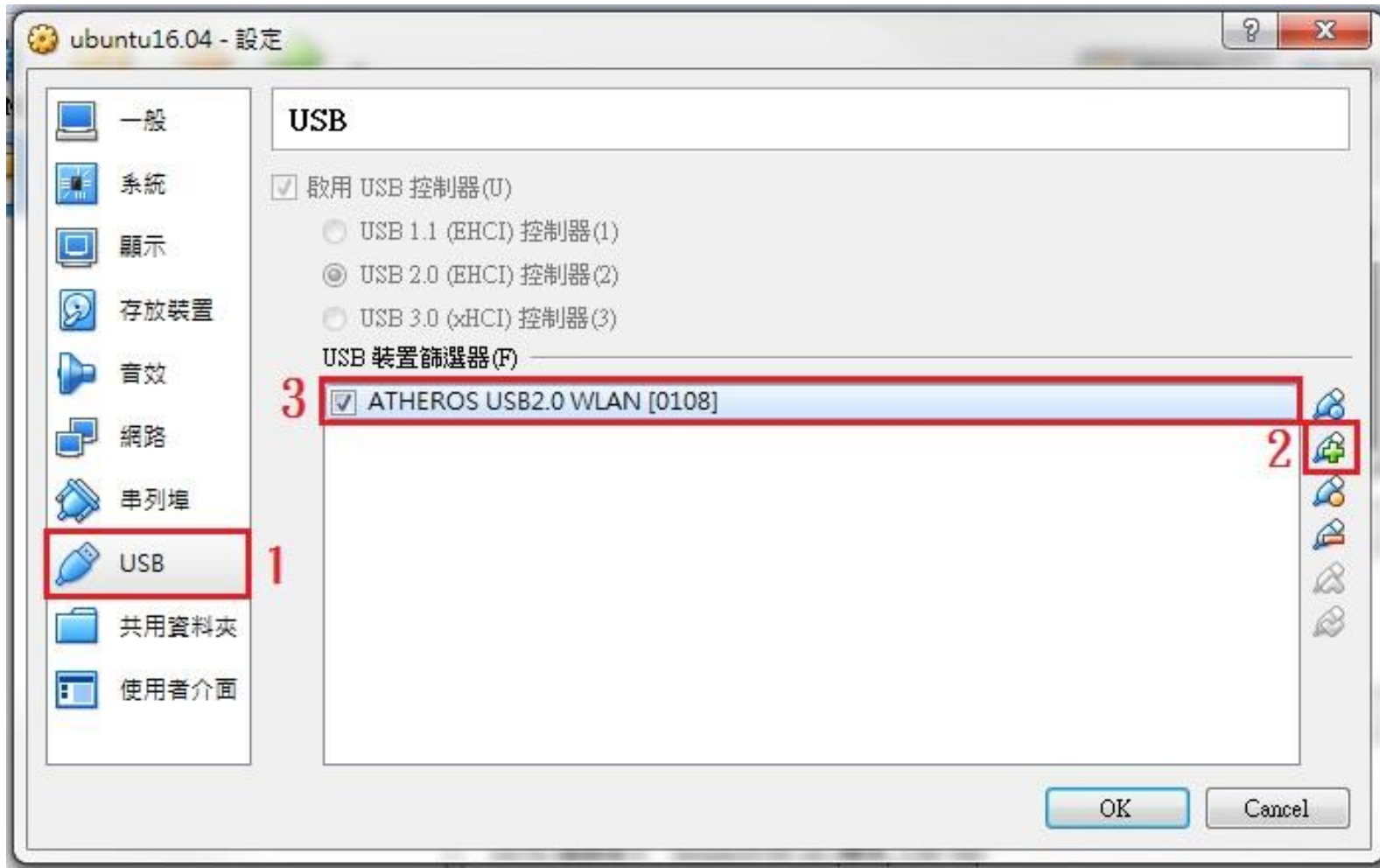
Wireshark

Packets Sniff Experiment

Open VM VirtualBox - Setting



Isolate wireless USB adapter



VirtualBox Start



Password : ImBun

Check wireless USB adapter has been driven or not?

1. Open terminal
2. *iwconfig*
3. Check wireless USB adapter has been driven.
(If not, change USB port.)

Check wireless USB adapter has been driven or not?

```
adhoc@adhoc: ~  
adhoc@adhoc:~$ iwconfig  
lo          no wireless extensions.  
  
wlan0       IEEE 802.11bgn  ESSID:off/any  
            Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm  
            Retry short limit:7   RTS thr:off   Fragment thr:off  
            Power Management:off  
  
eth0        no wireless extensions.  
  
adhoc@adhoc:~$
```

Packets Sniff Experiment

■ Lab Purpose

- Understand wireless network by capturing packets.

■ Equipments

- PC / NB (Root Password : **ImBun**)
- Atheros-chipset wireless NIC (support IEEE 802.11 b/g)
- Linux with iw (linux wireless package)
- Wireshark (network protocol analyzer)
- WiFi Access Point (Open Access / Encrypted)

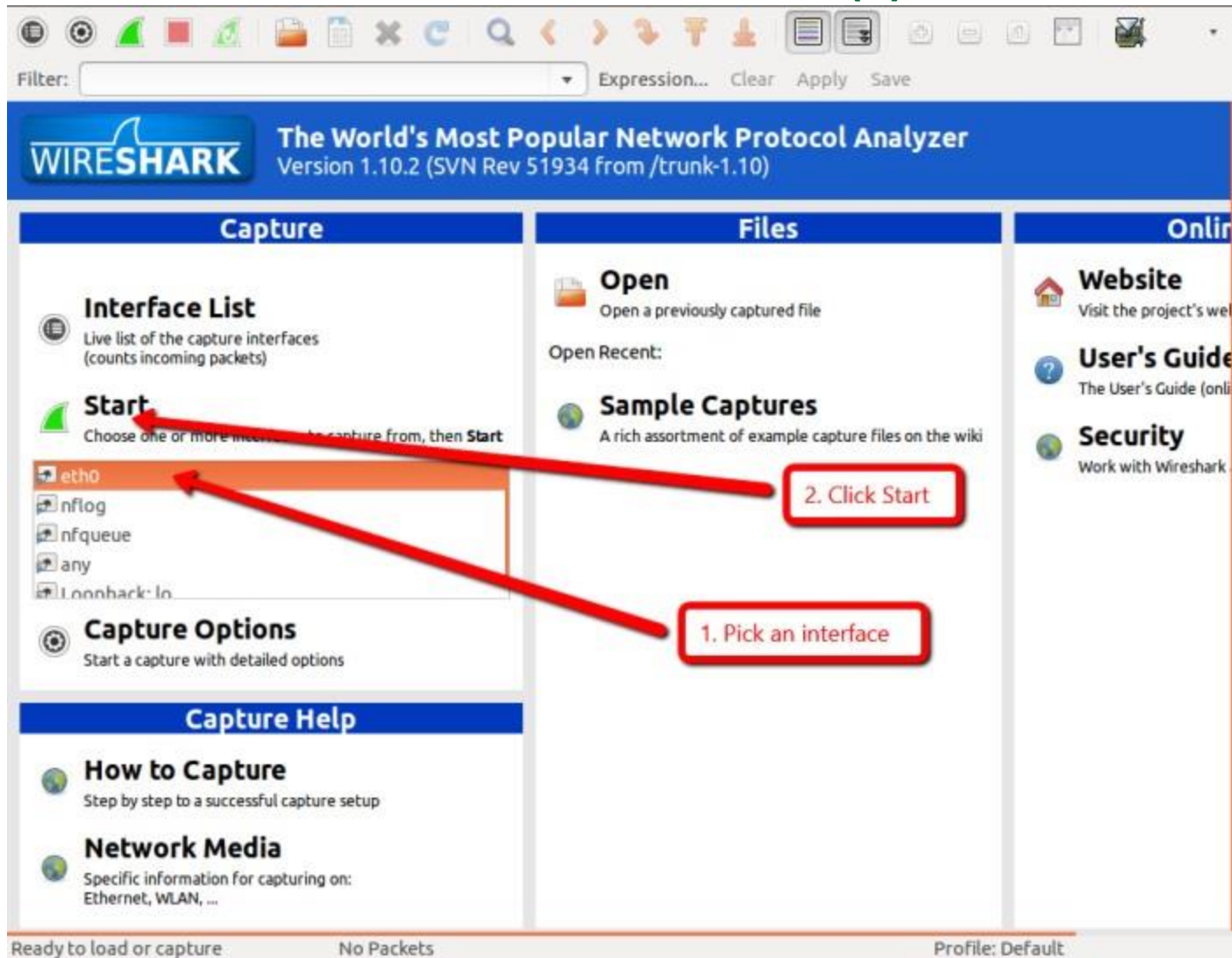
Wireshark Introduction

- A Free and Open-Source Packet Analyzer
- Available for UNIX and Windows
 - <https://www.wireshark.org/>
- Capture live packet data from a network interface
- Purpose:
 - *Network Administrators* : troubleshoot network problems
 - *Network Security Engineers* : examine security problems
 - *Developers* : debug protocol implementations
 - *People* : learn network protocol internals
- Installation on Ubuntu
 - `sudo apt-get install wireshark`
 - `sudo wireshark`

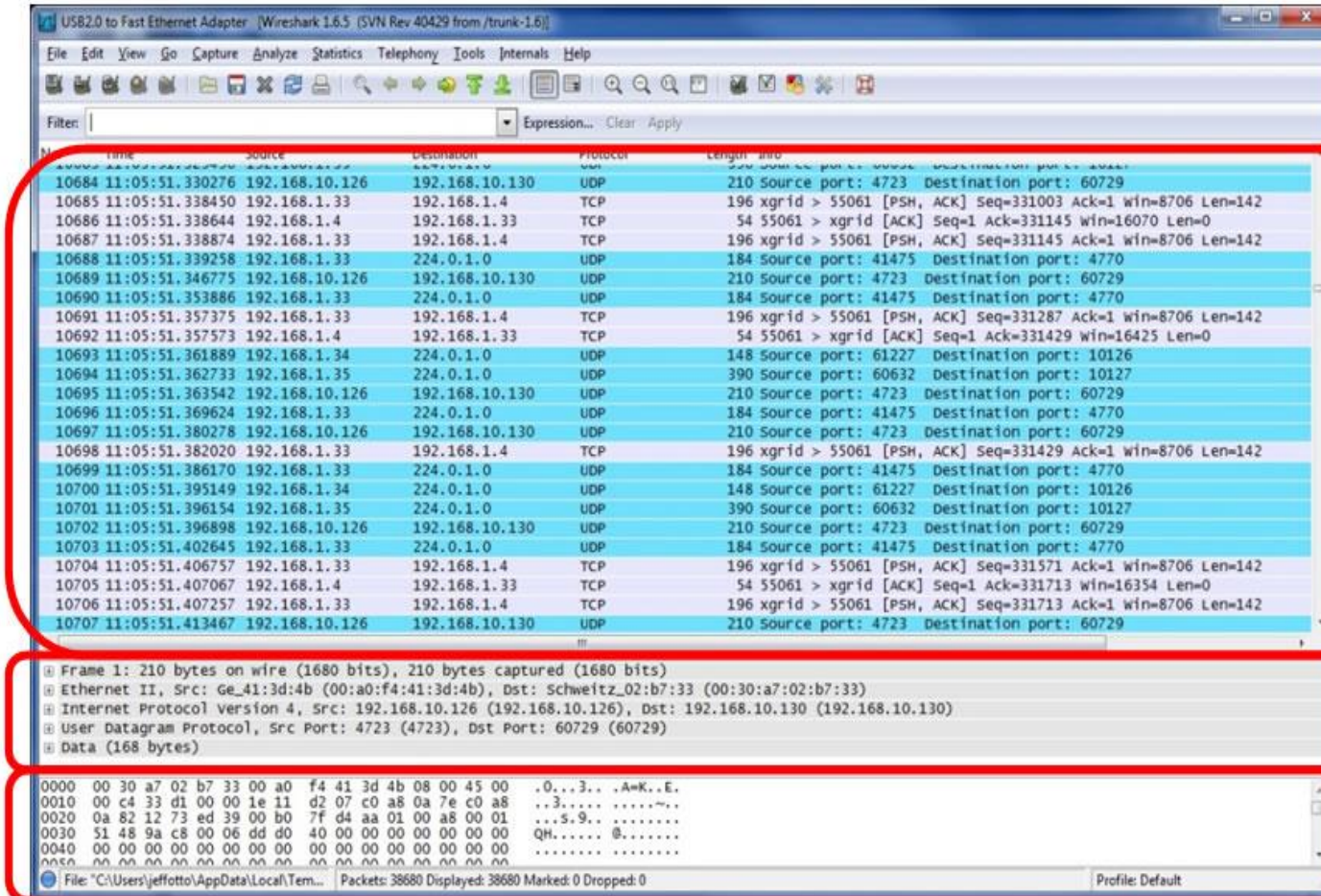
Wireshark Installation (from source)

- Package Download Link :
<https://1.as.dl.wireshark.org/src/wireshark-2.2.2.tar.bz2>
- Open the terminal, then type these commands:
 - ❑ Unpack the source file:
tar xaf wireshark-1.12.8.tar.bz2
 - ❑ Go to the Wireshark source directory:
cd wireshark-2.2.2
 - ❑ configure the source:
./configure
 - ❑ Build the source:
make
 - ❑ Install:
make install

Wireshark User Interface (I)



Wireshark User Interface (II)



Packet
capture

Packet
detail

Raw data

Linux Introduction w/ network command

- ifconfig - configure a network interface
 - Set IP address, MAC address ... etc

```
eth0      Link encap:Ethernet  HWaddr 00:26:18:37:B9:8D  
          inet addr:192.168.2.52  Bcast:192.168.2.255  Mask:255.255.255.0  
          inet6 addr: fe80::226:18ff:fe37:b98d/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:32487 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:2753 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:2504197 (2.3 MiB)  TX bytes:661455 (645.9 KiB)  
          Interrupt:17 Base address:0x4000
```

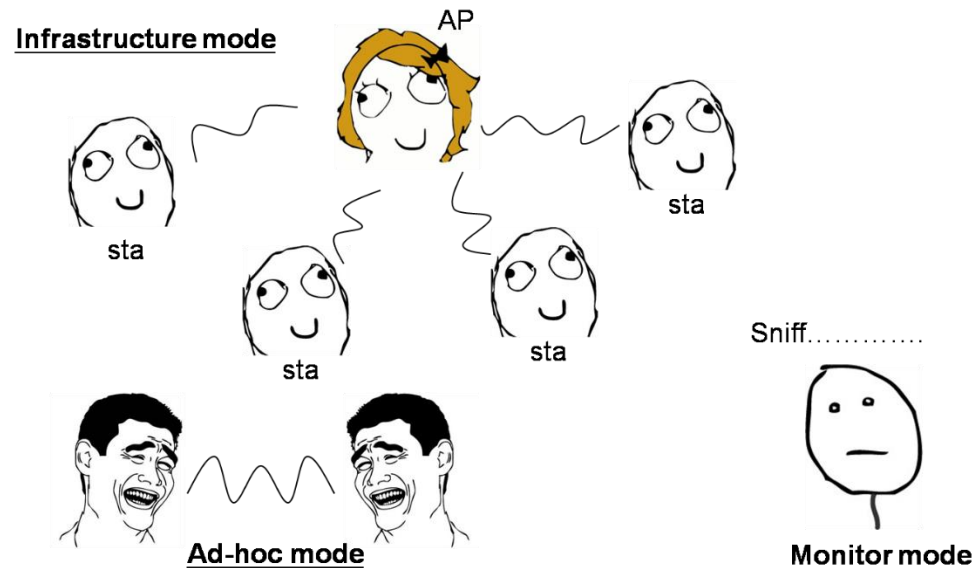
Linux Introduction w/ wireless network command

- iwconfig - configure a wireless network interface
 - Set ESSID, channel, rate ...etc

```
ath0 IEEE 802.11b ESSID:"" Nickname:""  
Mode:Managed Channel:0 Access Point: Not-Associated  
Bit Rate:0 kb/s Tx-Power:0 dBm Sensitivity=1/1  
Retry:off RTS thr:off Fragment thr:off  
Encryption key:off  
Power Management:off  
Link Quality=0/70 Signal level=-256 dBm Noise level=-256 dBm  
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0  
Tx excessive retries:0 Invalid misc:0 Missed beacon:0
```

Wireless Operating Modes

- Wi-Fi modes of operation (802.11 or Wi-Fi)
 - Station (STA) infrastructure mode
 - This mode is also called “ **Managed** ”
 - AccessPoint (AP) infrastructure mode
 - Ad-Hoc (IBSS) mode
 - Monitor (MON) mode (i.e, Sniff mode)
 - Don't need to connect any AP



Monitor mode – Wireless Channel

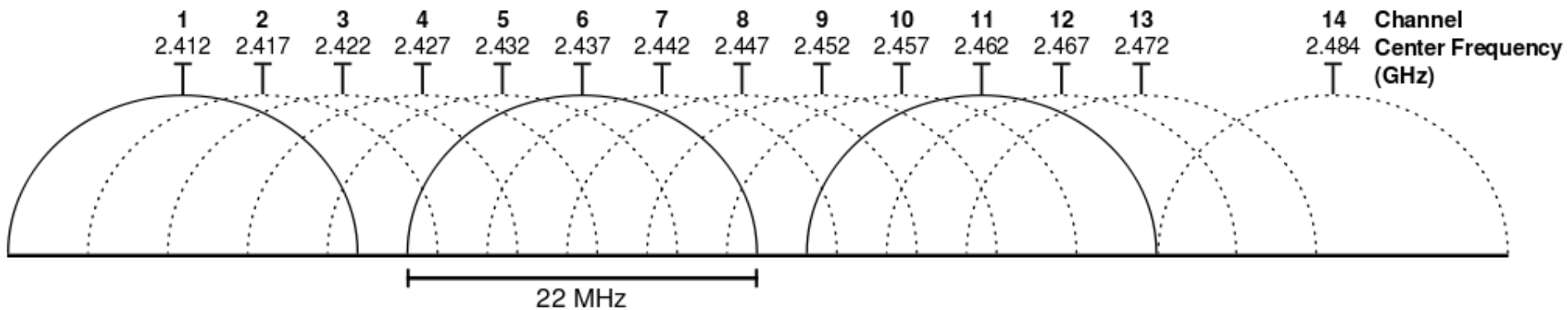






Fig. 2.4 GHz Wi-Fi channels (802.11b,g WLAN)

Packets Sniff Experiment

- [Step 1] Install Unix-like operating system. (Done For You)
- [Step 2] Download & install Wireshark. (Done For You)
- [Step 3] Switch the wireless NIC to monitor mode.
 - delete the normal *wlan#* interface if it's unused :
`iw dev`  (to list the available devices)
`sudo iw dev wlan# del`  (change # to the specific number)
 - add a monitor interface called *mon?* :
`sudo iw phy phy# interface add mon? type monitor`  (change ? to the a number)
 - enable the *mon?* interface using ifconfig :
`sudo ifconfig mon? up`
 - specify the wireless LAN frequency you want to capture on :
`sudo iwconfig mon? channel x`
or `sudo iw dev mon0 set freq 24yz`
- [Step 4] Open Wireshark to capture and observe the packets
 - `sudo wireshark`  (Use Wireshark with root authority)

Questions & Report

- TA will use our own devices to access Internet via an AP (Open Access/Encrypted).
- TA will generate HTTP, FTP, Telnet and SSH packets.
- Questions:
 - # Q1 :
Can you get any detail information from received packets for HTTP, FTP, Telnet and SSH via Open Access AP!?
(ex: username, password)
 - # Q2 :
Can you get any detail information from received packets for HTTP, FTP, Telnet and SSH via Encrypted AP!?
- You need to answer these questions and then write a full report with your thoughts or analysis(individual report).
 - Deadline : **2020 / 11 / 24**