COMP 3355

Lab 2
Network capture and scanning

Wireshark & Nmap

Introduction to Packet Capture

- What is packet capture?

- Packet capture is a process of collecting packets which will be processed and used later for further purposes

Introduction to Wireshark

- Wireshark is a free and open-source packet capture analyzer.
- Used for network troubleshooting, analysis, software and communications protocol development, and education.
- Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets.

Introduction to Wireshark

Wireshark can:

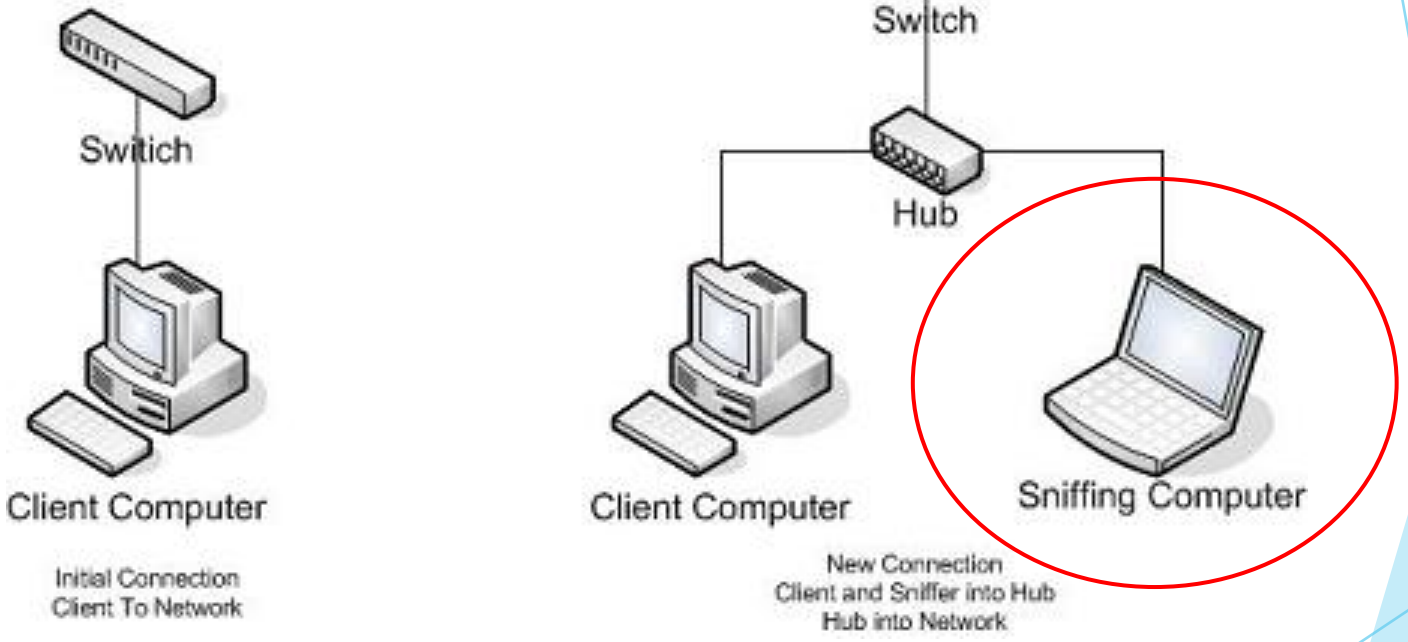
1. Capture the **incoming** and **outgoing** traffic of the network interface

2. Capture all communications within a Network

It allows the user to put network interface controllers into promiscuous mode.

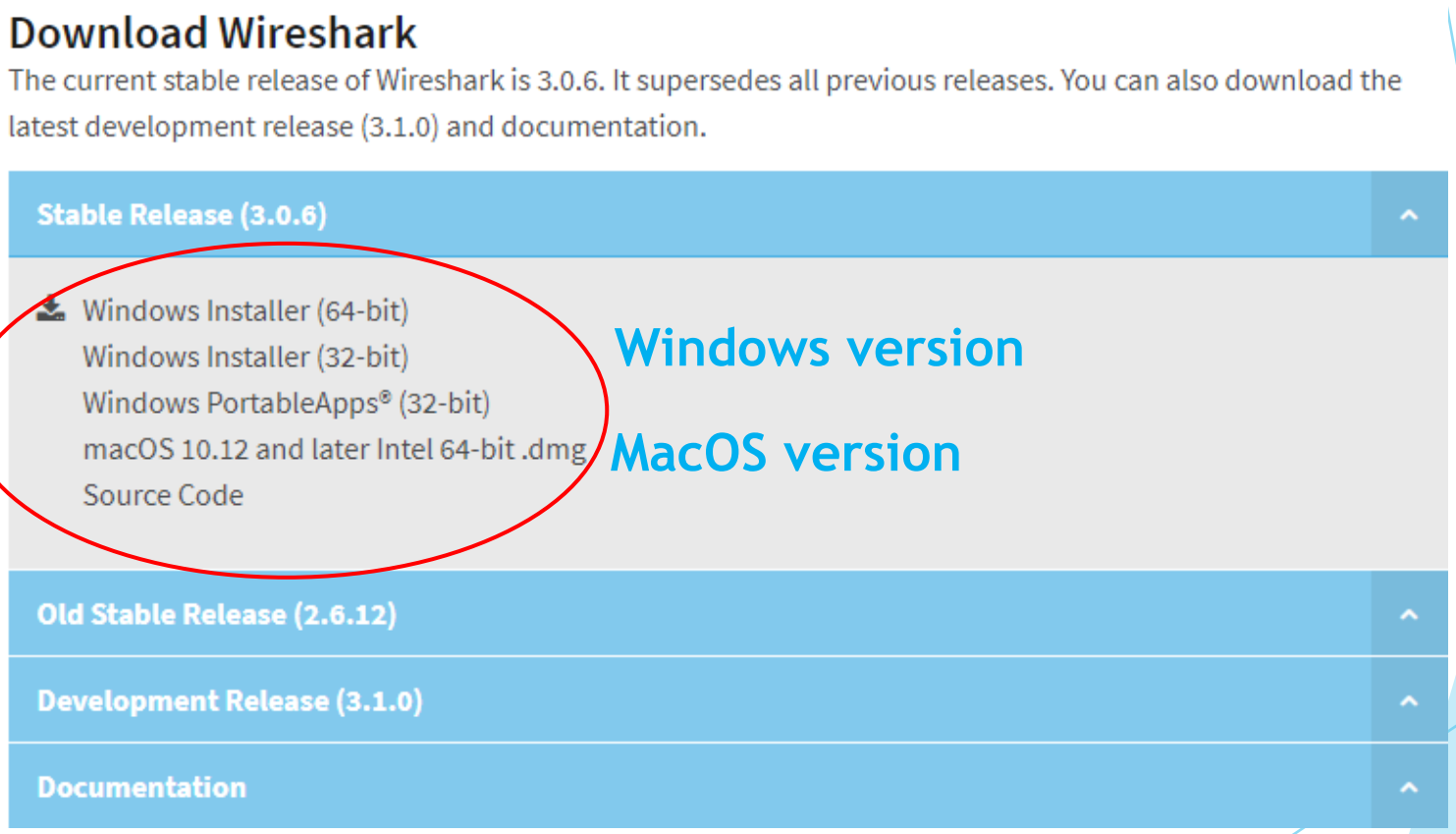
See all traffic visible on that interface, not just traffic addressed to one of the interface's configured addresses and broadcast/multicast traffic.

Capture network traffic within a internal network



How to install Wireshark

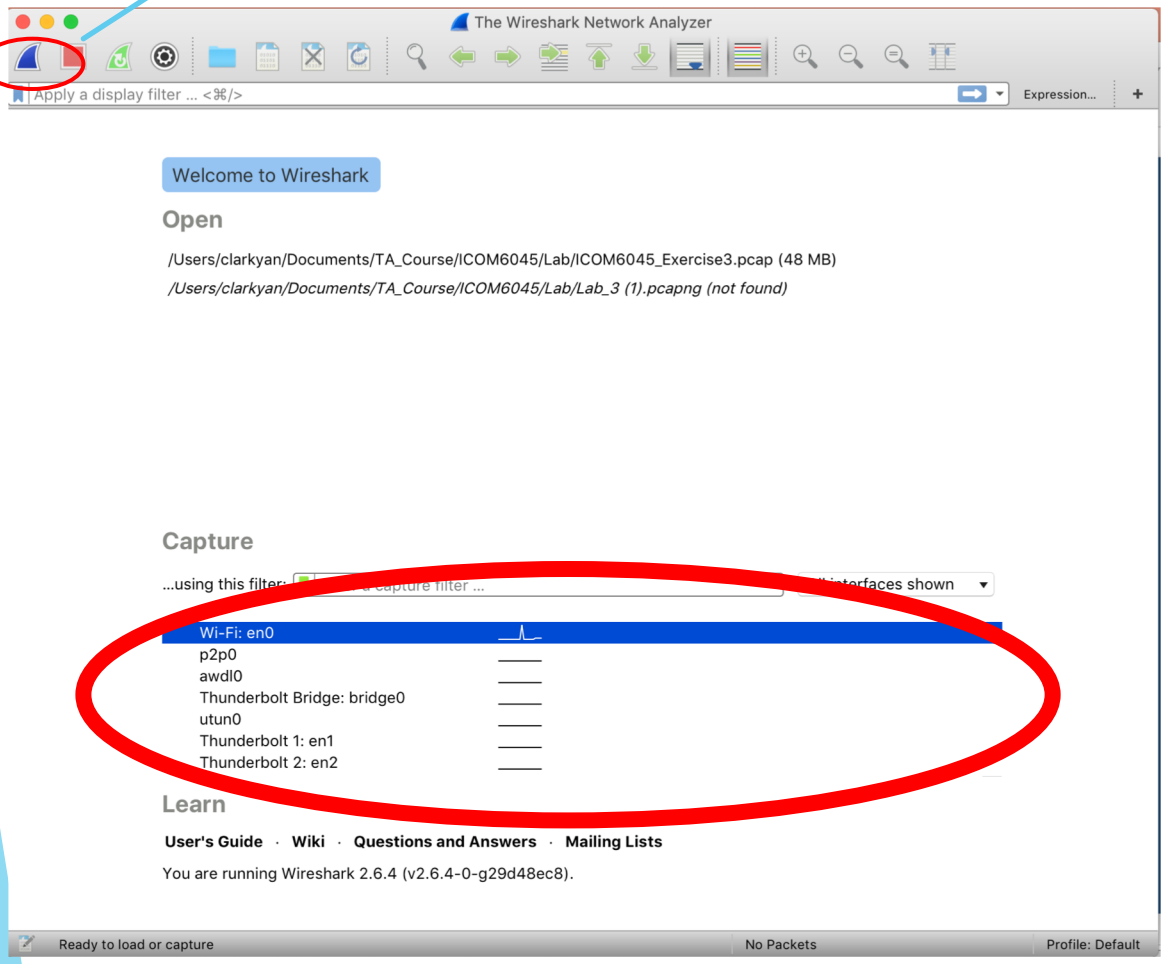
- Open the browser and go to the website https://www.wireshark.org/download.html



Select a version and click to download the software

Capture Packet using Wireshark

Press “Start”



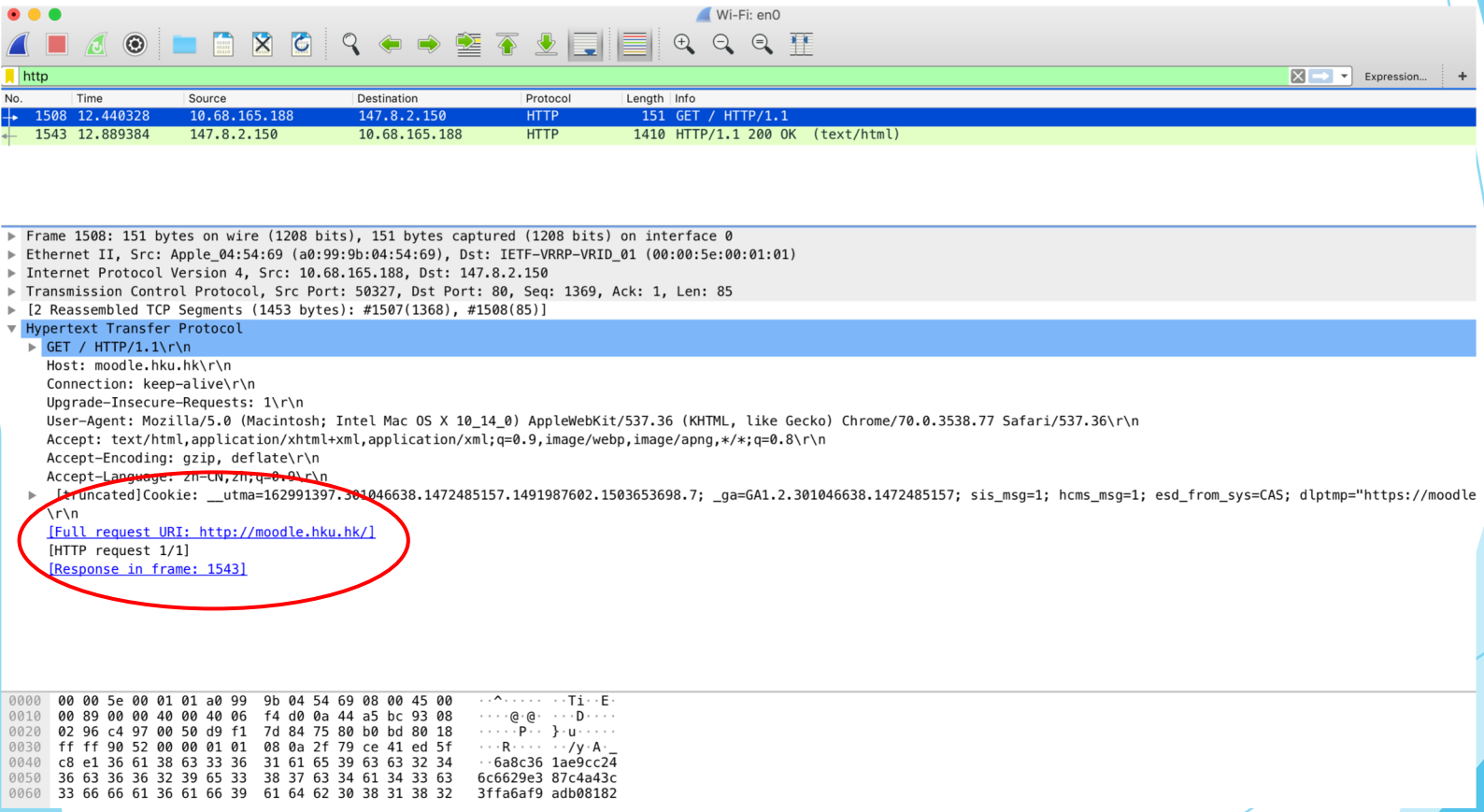
Try it!

Select the Network interface

Try the following scenario

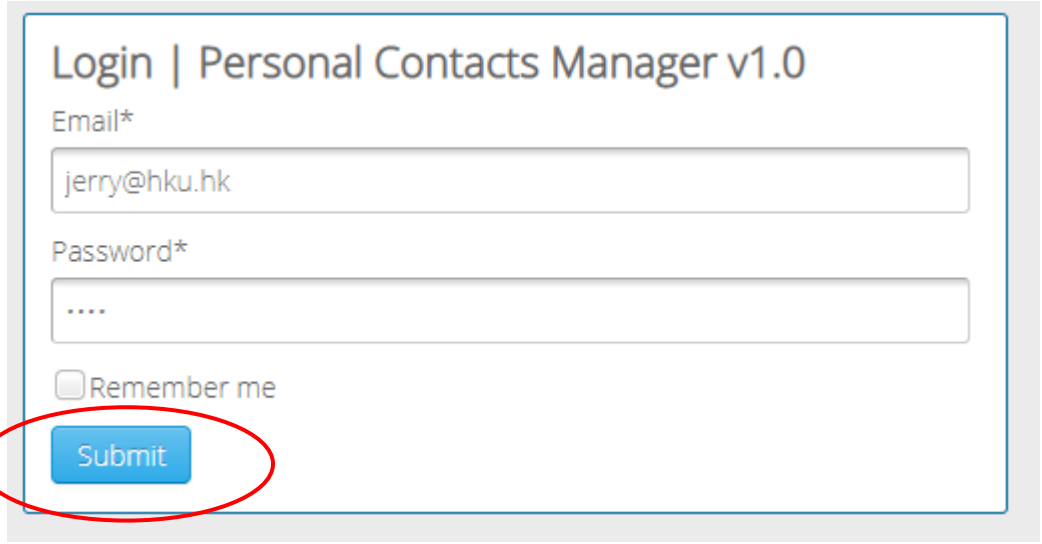
- Start capture packet in Wireshark
- Open your web browser, access http://moodle.hku.hk/
- Stop the packet capture

- Use ”http” filter to find all http requests
- After selecting the GET information



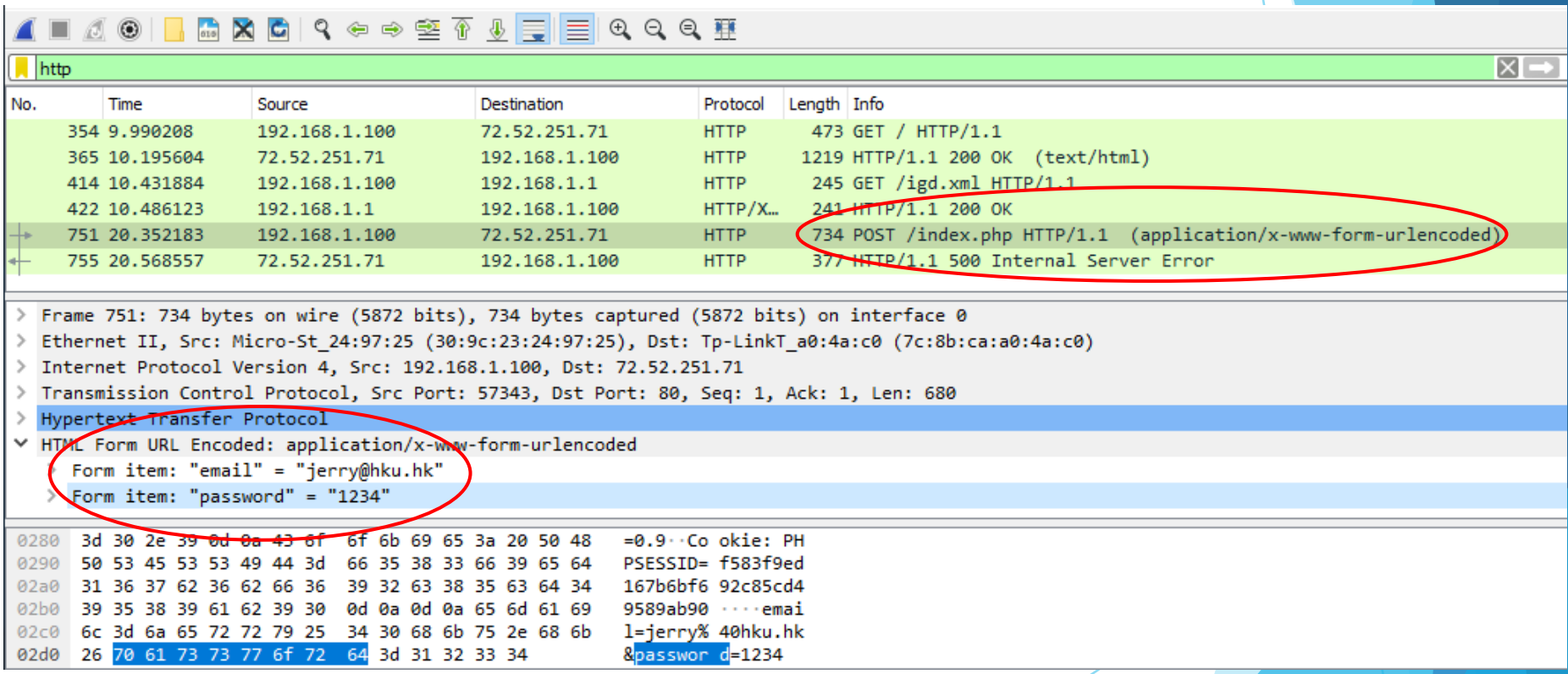
Try the following scenario

- Start capture packet in Wireshark
- Open your web browser, access http://www.techpanda.org/



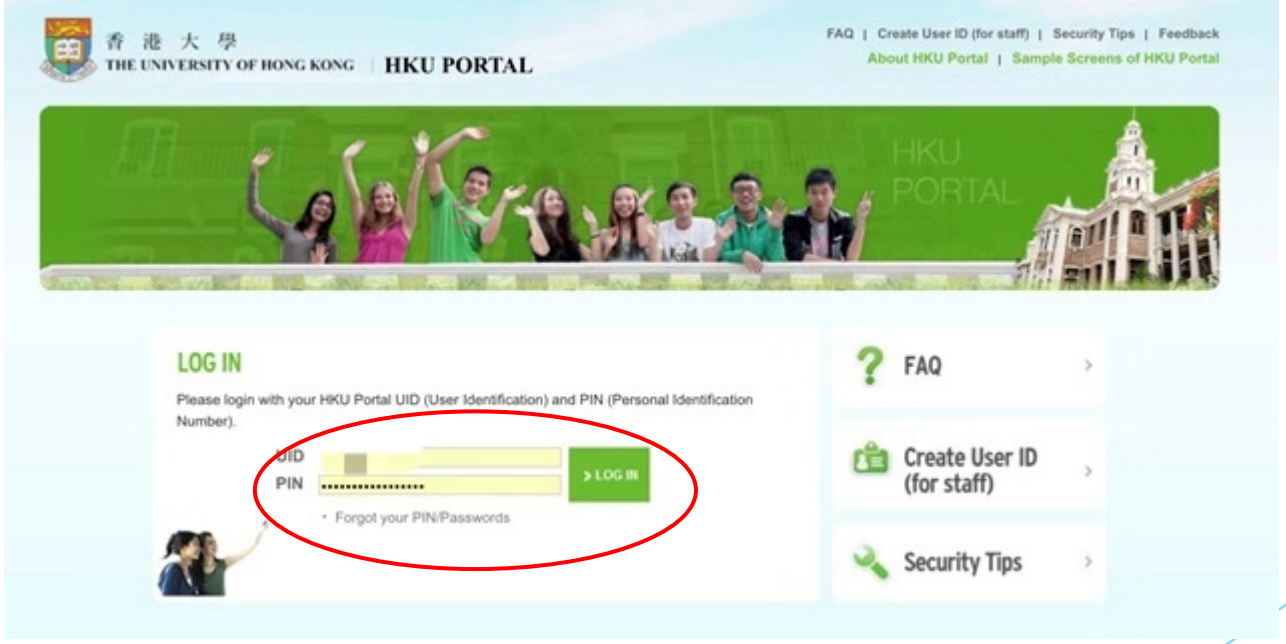
Click "Submit" Here!

- Stop the packet capture
- Use ”http” filter to find all http requests
- After selecting the POST information



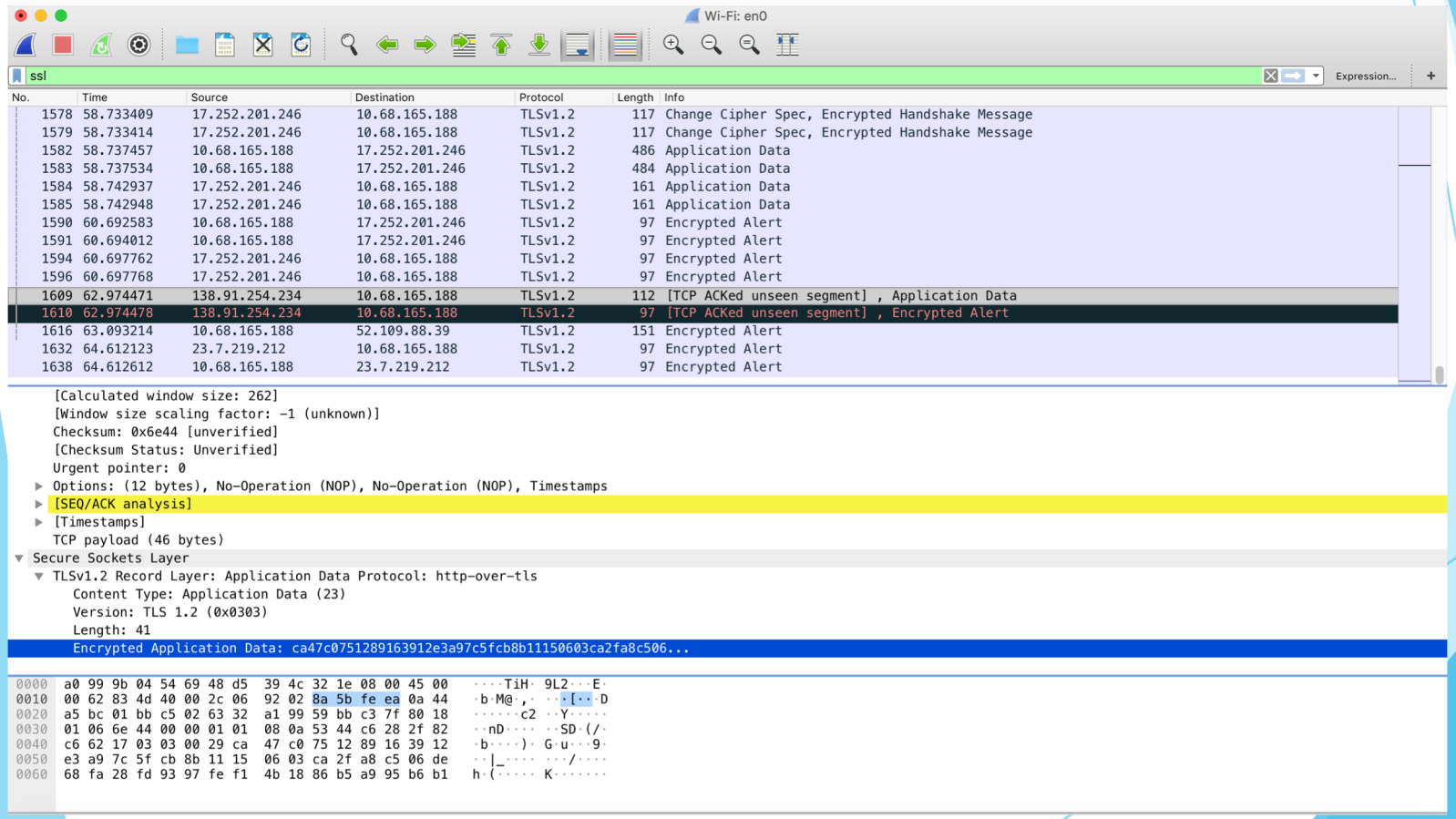
Try the following scenario

- Start capture packet in Wireshark
- Open your web browser, access https://hkuportal.hku.hk



Click "Login In" Here!

- Stop the packet capture
- Use ”ssl” filter to find all https requests
- Can you find the record? Why and Why not?



NMAP - the Network MAPper

- In order to crack into a computer system, an attacker has to find a target machine, and then find out what ports the machine is listening on before a system can be compromised.
- By using scanners such as Nmap, the attacker are able to sweep networks and look for vulnerable targets.
- Once these targets are identified, an intruder is able to scan for listening ports.
- https://nmap.org/

Ping Sweep: Which hosts are up?

- Intruders are able to sweep entire networks by looking for targets with Nmap. This is usually done with a ping scan by using the "-sP" flag.
- Nmap will allow you to specify networks with wild cards, such as 10.6.1.*, meaning from 10.6.1.0 to 10.6.1.255.
- E.g.: nmap –sP 147.8.178.*

```
Tianyis-MacBook-Pro:~ wang$ nmap -sP 147.8.178.*
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-05 11:16 HKT
Nmap scan report for www2.cs.hku.hk (147.8.178.79)
Host is up (0.0097s latency).
Nmap scan report for waterman-nat1.cs.hku.hk (147.8.178.109)
Host is up (0.0056s latency).
Nmap scan report for host-178-116.cs.hku.hk (147.8.178.116)
Host is up (0.0044s latency).
Nmap scan report for host-178-172.cs.hku.hk (147.8.178.172)
Host is up (0.0052s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 24.81 seconds
```

Port Scanning: Any vulnerable services available?

- TCP Scanning
  - When an attacker is using TCP connect scans, Nmap will open connections to interesting ports on the target host
  - E.g.: nmap –sT localhost

```
[Tianyis-MacBook-Pro:~ wang$ nmap -sT localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-05 11:25 HKT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00025s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 973 closed ports, 26 filtered ports
PORT    STATE SERVICE
631/tcp open  ipp
```

Port Scanning: Any vulnerable services available?

- UDP Scanning
  - Using the UDP scan “-sU” an attacker can determine what ports are open to UDP on a host. Nmap will send a 0-byte UDP packet to each port. If the host returns a "port unreachable" message, that port is considered closed.
  - E.g.: nmap –sU localhost

```
Tianyis-MacBook-Pro:~ wang$ sudo nmap -sU localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-05 11:30 HKT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000098s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 997 closed ports
PORT     STATE         SERVICE
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
5353/udp open|filtered zeroconf
```

May Need Root Privileges

OS Fingerprinting: Which OS is Running on the host?

- Often an intruder may be more familiar with exploits for a particular operating system, and may be looking for machines he's able to compromise easily. A common option is TCP/IP fingerprinting with **the "-O" option** to determine the remote operating system.
- Nmap accomplishes this by sending different types of probes to the host, which will narrow the target operating system.
- E.g.: nmap –O localhost
- May Need Root Privileges

CVE detection using Nmap

- CVE: Common Vulnerabilities and Exposures
- One of Nmap's greatest features that not all the network and systems administrators know about is something called "Nmap Scripting Engine" (known as NSE).
- Using NSE is crucial in order to automate system and vulnerability scans.
- E.g.: nmap -Pn --script vuln localhost

```
PORT    STATE SERVICE
631/tcp open  ipp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
| http-phpmyadmin-dir-traversal:
|   VULNERABLE:
|   phpMyAdmin grab_globals.lib.php subform Parameter Traversal Local File Inclusion
|     State: UNKNOWN (unable to test)
|     IDs:  CVE:CVE-2005-3299
|       PHP file inclusion vulnerability in grab_globals.lib.php in phpMyAdmin 2.6.4 and
2.6.4-pl1 allows remote attackers to include local files via the $__redirect parameter, p
ossibly involving the subform array.
'
```

CVE (Anc

```
[root@securitytrails:~]nmap -Pn --script vuln 192.168.1.105
Starting Nmap 7.60 ( https://nmap.org ) at 2018-10-01 09:46 -03
Pre-scan script results:
| broadcast-avahi-dos:
| Discovered hosts:
| 224.0.0.251
| After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).
Nmap scan report for 192.168.1.105
Host is up (0.00032s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
80/tcp open http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.
|
| Disclosure date: 2009-09-17
| References:
| http://ha.ckers.org/slowloris/
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
1900/tcp open upnp
20005/tcp open btx
49152/tcp open unknown
49153/tcp open unknown
```

Reference

- Security arrangement with mobile app development https://www.pcpd.org.hk/mobileapps/files/Sharing_of_Security_Arrangement_with_Mobile_App_De.pdf

- NIST - Vetting the Security of Mobile Applications https://www.nist.gov/publications/vetting-security-mobile-applications

- Testing Website http://aavtrain.com

Thanks!