

# ELEC S212

**Network Programming and Design**

## 2018 Autumn Presentation

**Assignment 4**

Please e-submit this assignment via the OLE

### by 27 April 2019, 23:59

**Preamble**

Dear ELEC S212 Students,

You must submit your answers to this assignment by the cut-off date: **27 April 2019**.

Please note that no assignment extension is allowed for the last assignment. So plan your time and start doing the assignment as soon as you can.

There are FOUR questions in this assignment. You should submit it and the associated files in zipped format and upload it to the OLE e-submission system.

Steven Choy

ELEC S212 Course Coordinator

WELL DONE!!

I am sure you will have better/good result for exam.

You have shown EXCELLENT understanding on network programming, network traffic analysis, network security, hacking; wired & wireless network design.

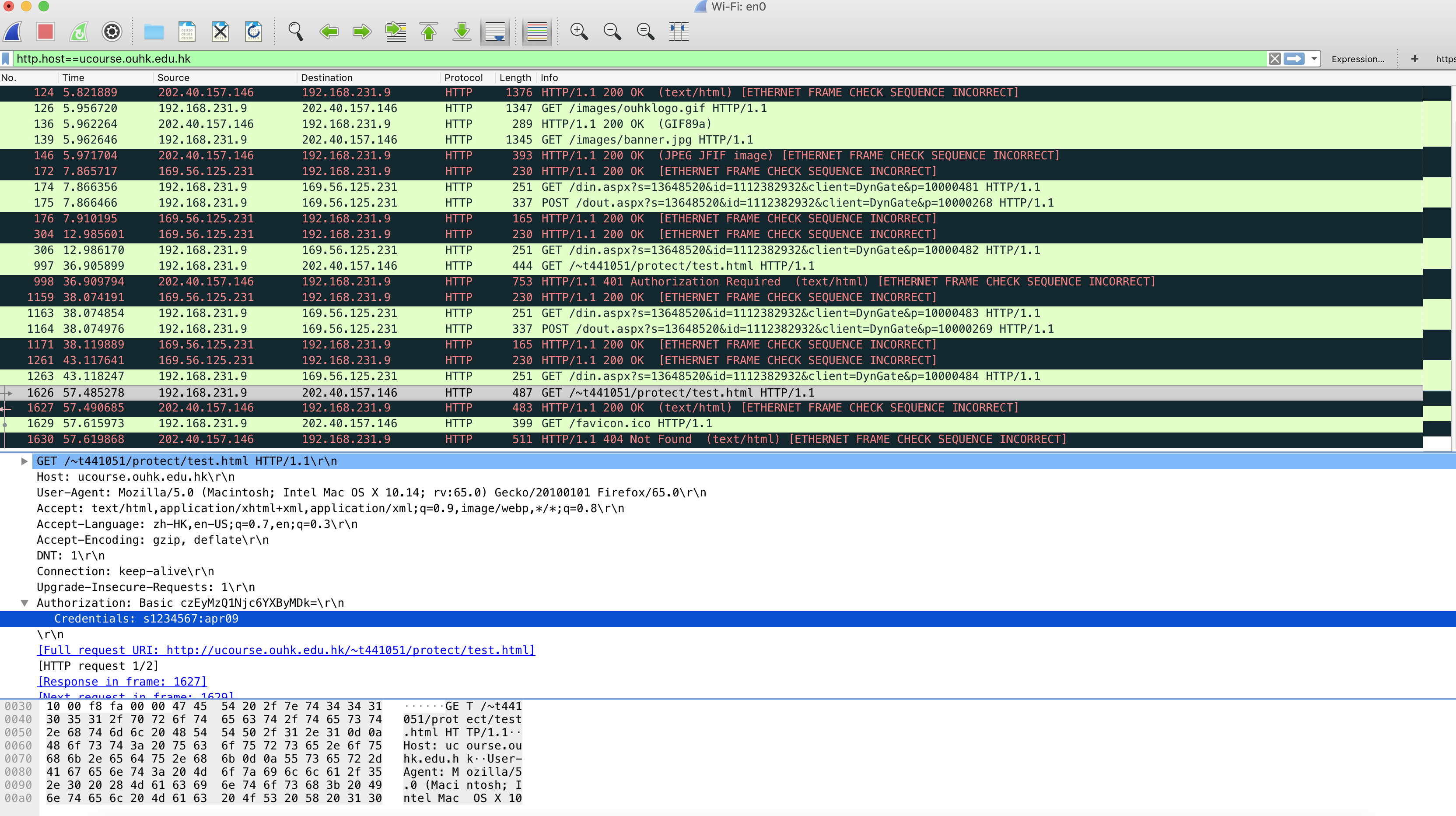
However, you are suggested to enhance:

1. Description of digital certificate
2. How to enhance a technical proposal for a wireless Café ordering system.

### Question 1

3 mark

1. The Highlighted column is the username login & password.



4 mark

Upload as an attachment.

4 mark

2. http
3. telnet
4. ftp
5. pop3

2 mark

1. http.request.method == “POST”

4 mark

(e)

Hub is the layer1 network devices, it will repeat bits out all ports except the incoming port. Therefore, the data copied to all ports.

However, switch is a layer 2 devices, an Ethernet switch consults a MAC address table to make a forwarding decision for each frame. When switch would like to packet sniffing, it needs to set the monitor port in switch

4 mark

**(F)**

Ethernet II, Source: 02:34:4d:59:6d:20

Ethernet II, Destination: 00:24:a5:73:64:f8  
Internet Protocol, Source: 192.168.11.3

Internet Protocol, Destination: 202.40.219.246

TCP, Source Port: 2436  
TCP, Destination Port: 80

4 mark

**(G)**

Ethernet II, Source: 00:24:a5:73:64:f8

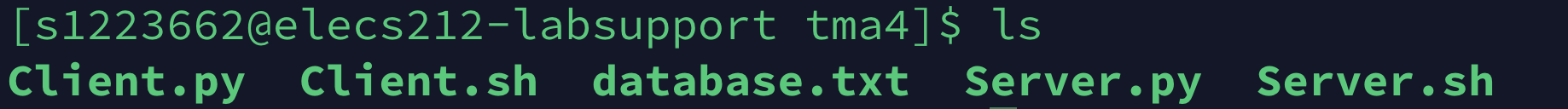
Ethernet II, Destination: 02:34:4d:59:6d:20  
Internet Protocol, Source: 202.40.219.246

Internet Protocol, Destination: 192.168.11.3

TCP, Source Port: 80   
TCP, Destination Port: 2436

mark

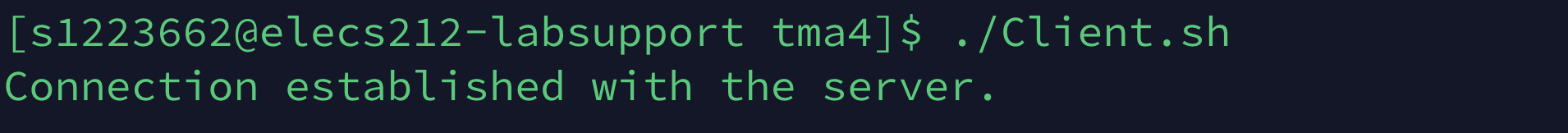
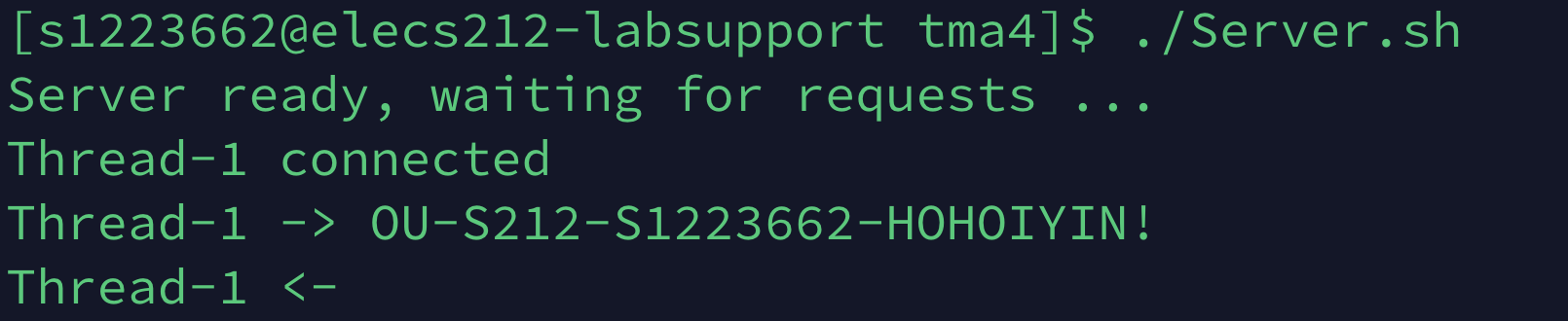
### Question 2 Dear sir, this is the python program. In labsupport tma4 folder, there are 5files.



**Step1: Launch server**

Run **./Server.sh**, it will display “Server ready, waiting for requests”.  


**Step2: Launch client**Run **./Client.sh**, it will display “Connection established with the server”.

  
  
**Step3: Connection Success**When the connection established, the server-side will send the greeting message.  


**## Available commands for client-side**

There is some function in client-side.

|  |  |
| --- | --- |
| Command | Description |
| HELLO | Say hello to the server, and the server respond with the pc-name. |
| LOGIN user password | Login the server. The username will be used in database.txt |
| LOGOUT | Logout of the server |
| CLOSE | Close connection to the server |

### #This is the demo of the command HELLO Command

|  |
| --- |
| Client |
|  |
| Server |
|  |

### LOGIN Command-1

|  |
| --- |
| Client |
|  |
| Server |
| N/A |

### LOGIN Command-2

|  |
| --- |
| Client (Login Failure) |
|  |
| Server |
|  |

### 

|  |
| --- |
| Client (Login Success) |
|  |
| Server |
|  |

### LOGOUT Command

|  |
| --- |
| Client (LOGOUT) |
|  |
| Server |
|  |

### CLOSE Command

|  |
| --- |
| Client |
|  |
| Server |
|  |

### Overall process

### 

### Question 3

3 mark

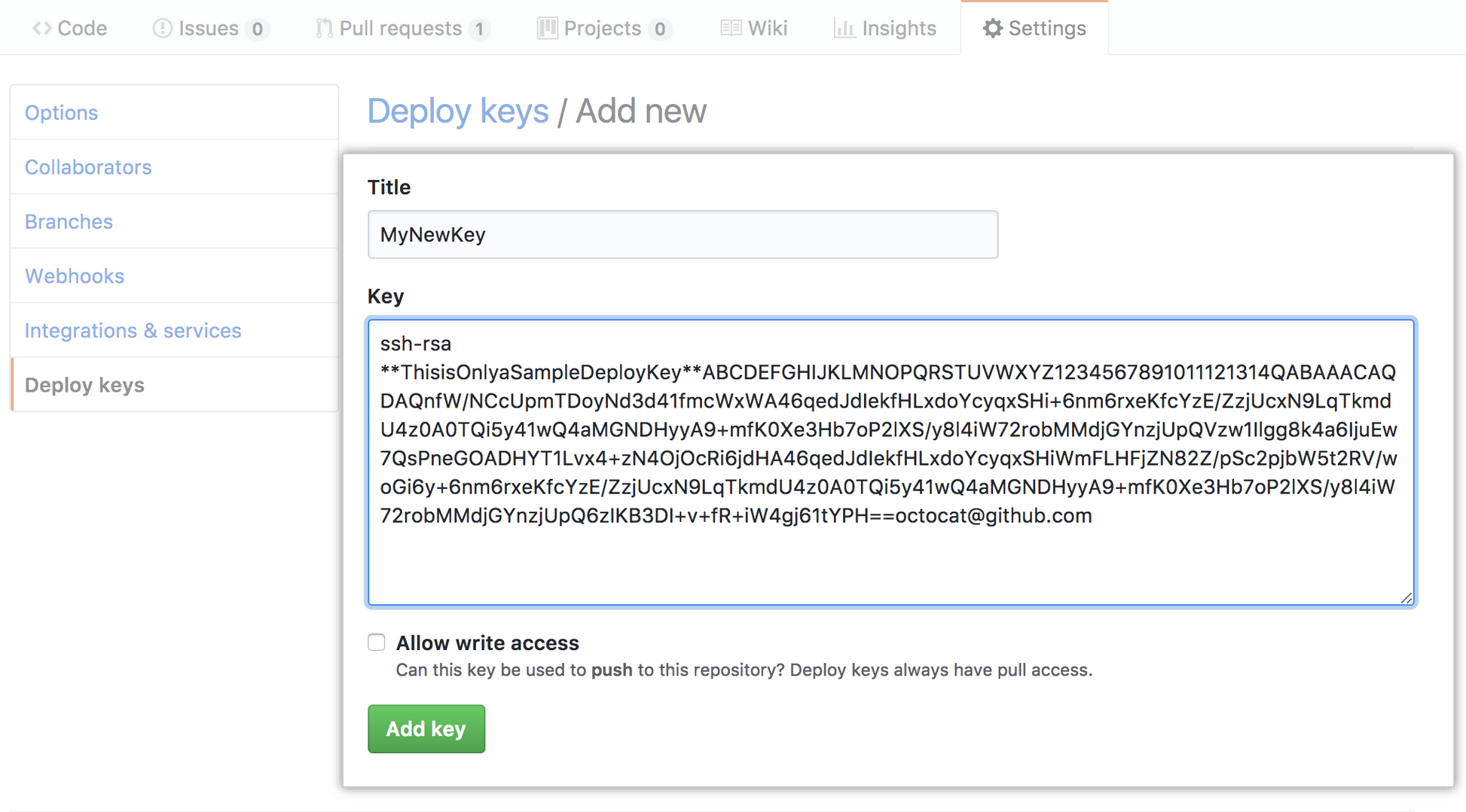
1. Asymmetric key encryption algorithm

Asymmetric key encryption means that each user has a pair of keys: public key & private key. The Public key can share with everyone, but private key should be kept it secret by owner.   
  
When the message is encrypted by one of the keys (whatever public key / private key), it must be decrypted with another key.   
  
Ether key can encrypt and either key can decrypt.

* Encrypt with public key and decrypt with private key
* Encrypt with private key and decrypt with public key  
    
  Example:  
  RSA (**Rivest–Shamir–Adleman**)

3 mark

1. Public key

Public key can share with everyone, and it used to encrypt data. The key can be generated by a software program.   
Example:  
The is the GitHub public key, SSH RSA key.   


3 mark

1. Certification authority (CA)

CA is everyone receives their certificates from one authority. It’s is hierarchical and single CA issues certs to intermediate CA.   
  
CA is responsible for verifying the identity of the key owner and for distributing the owner’s digital certificate for use by others.  
  
Example:  
The Postmaster General

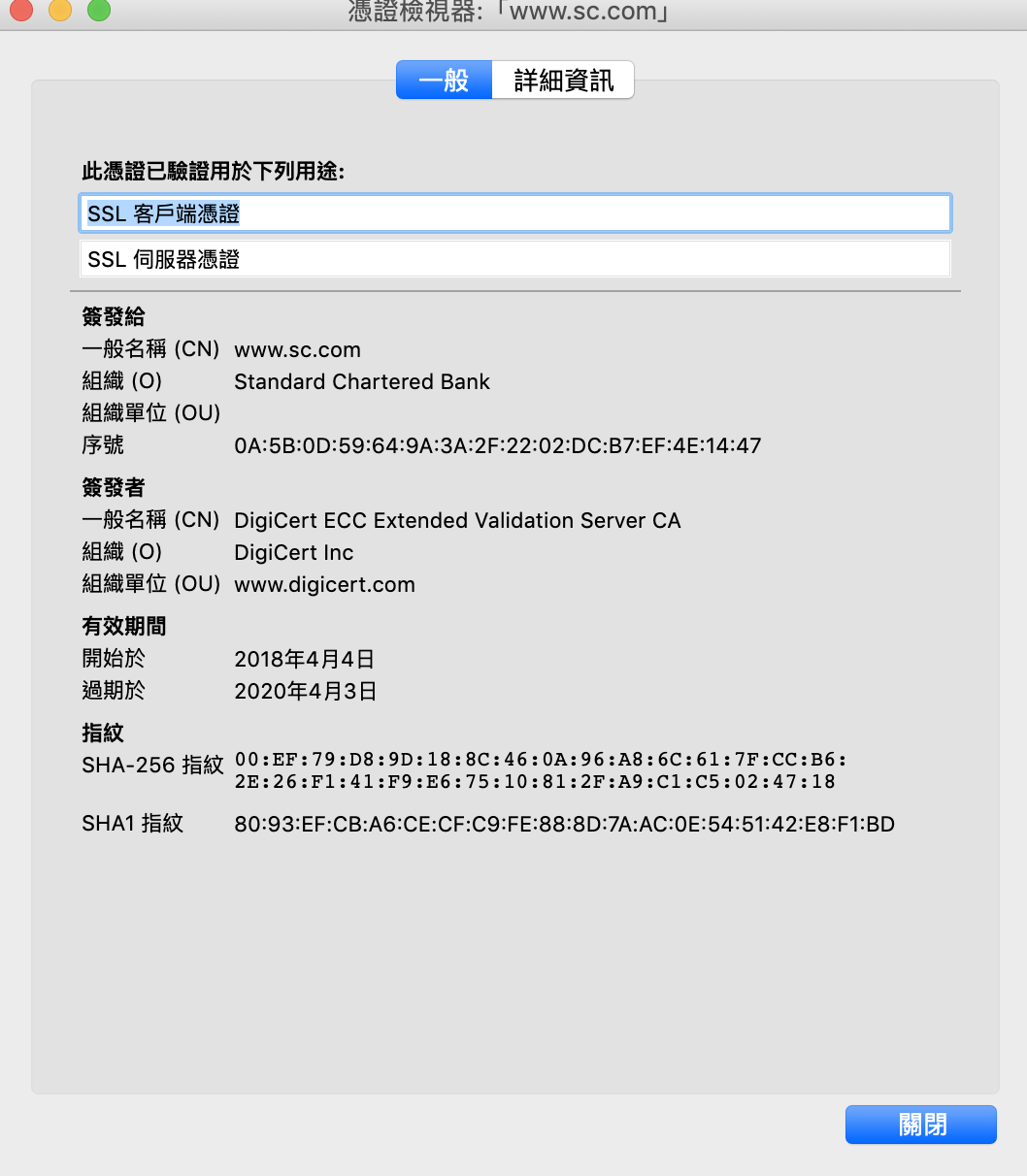
2 mark

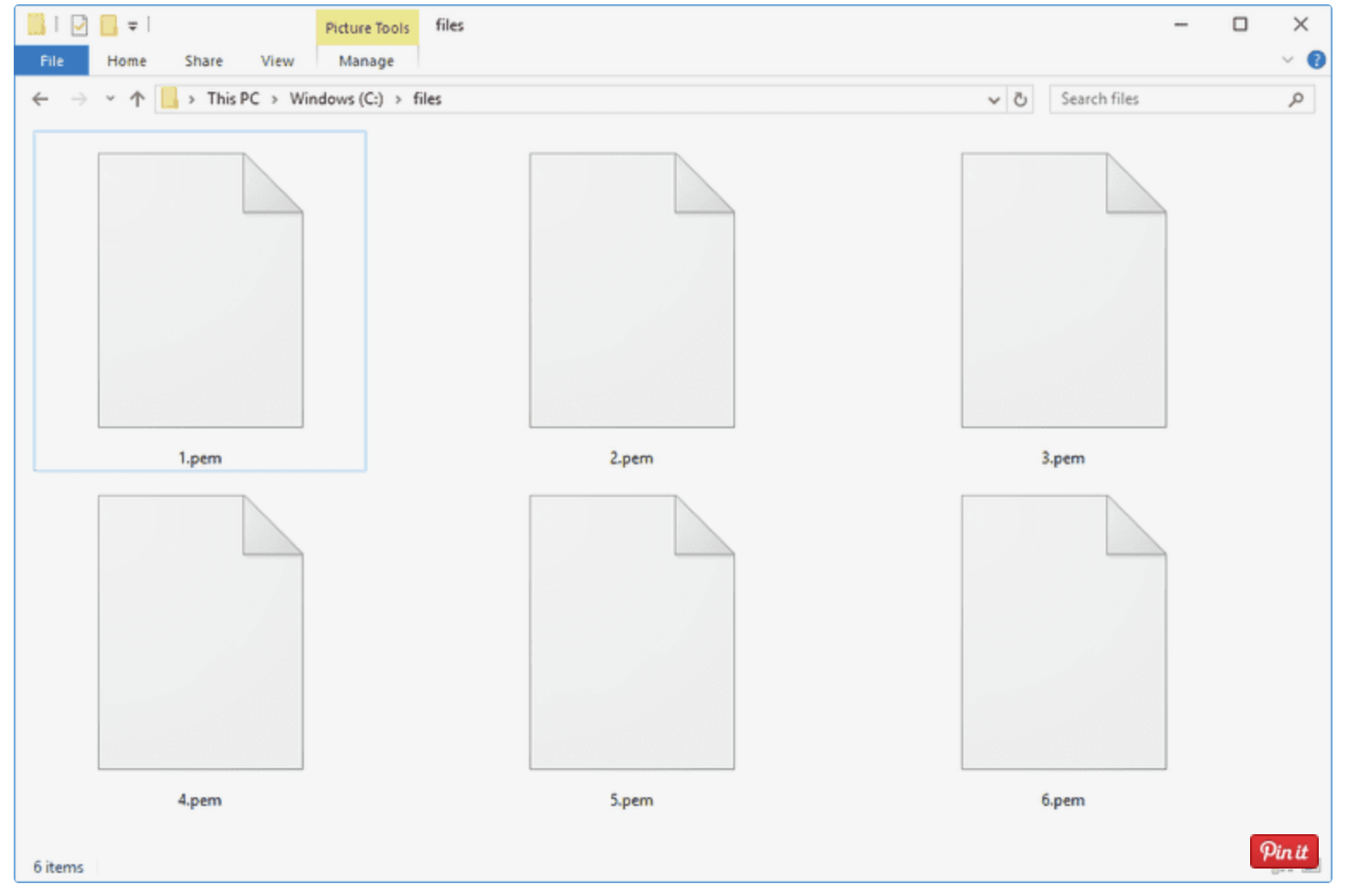
1. Digital certificates

A digital certificate is an electronic document issued and digitally signed by a certification authority to verify the identity of the certificate holder.   
  
Example:  


3 mark

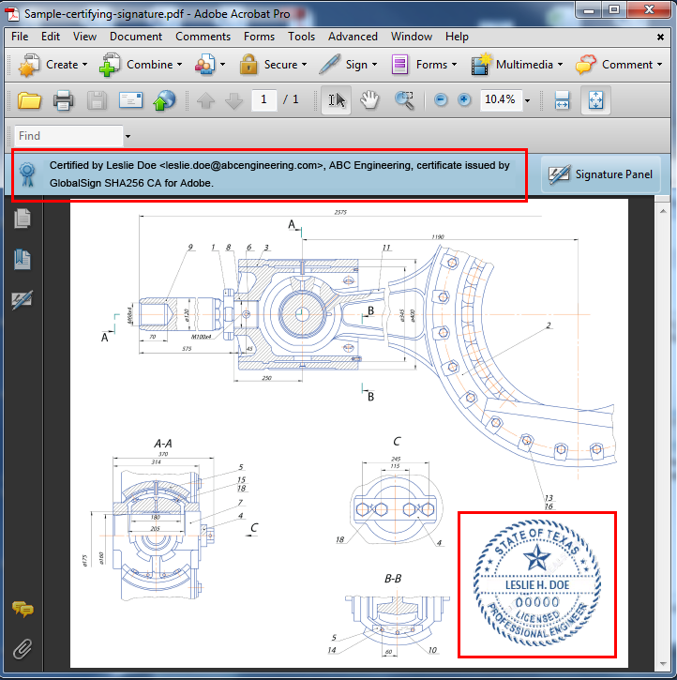
(e) X.509

X.509, is a certificate standard that defines what should be included in the certificate, such as owner name, expiration date of the public key, and so on.  
Common filename: .pem, .cer, .pfx   
Example:  




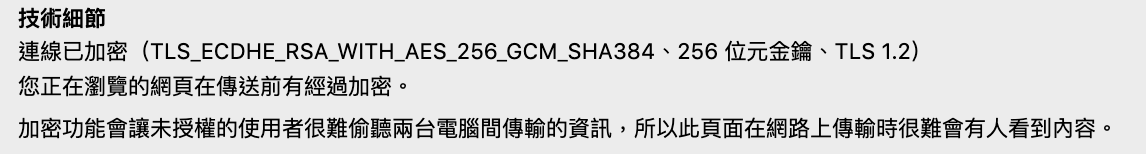
3 mark

1. Digital signature

Digital Signature is verifying the digital messages, software or documents. For file transfer, sensitive documents sharing, software distributions are being used.  
Certification: Proof the identity of the parties to the electronic transaction.  
Integrity: Make sure that the content of a message has not been altered.  
Authenticity: Any transaction can be tracked.  
  
  
Example:  


3 mark

1. Transport Layer Security

TLS is the latest industry standard cryptographic protocol. The successor to SSL.  
It authenticates the sever, client, and encrypts the data.  
  
A lots of website are now using HTTPS by default, regardless if sensitive data is going to be exchanged or not.   
  
  
Example:  
The Hang Seng Bank  
  


16 mark

### Question 4 Site Map 一張含有 文字, 地圖 的圖片 自動產生的描述

**Network Diagram  
一張含有 天空 的圖片

自動產生的描述**

**Café Background**

|  |  |
| --- | --- |
| Size | Medium retail chain |
| Number of employees | 50 (in office) 10 (in retail shop) |
| Client | 1. **Standalone Client – 6 (POS PC)**  |  |  | | --- | --- | | Benefit | Disadvantage | | Network Stability | Customer need to pay before the POS machine |  1. **Wireless Client - 10 (POS Terminal)**  |  |  | | --- | --- | | Benefit | Disadvantage | | Wireless, payment location is free | Wireless signal would be not stable | |
| How to order | |  | | --- | | PC Client / Wireless Client | | 1. Cashier identification function -  Cashier click the café POS application/apps, enter the correct ID & password. 2. Select the dial-in function 3. Click the table no. 4. Select number of customers 5. Redirect to Ordering Server, it will prompt the ordering screen, which can place the order (e.g. Breads/drink) and send it to the kitchen | |
| **How to bill** | |  | | --- | | PC Client / Wireless Client | | 1. Cashier identification function, cashier click the POS application/apps, enter the correct ID & password. 2. Select the dial-in function 3. Click the table no, confirm the receipt 4. Select pay button 5. Redirect to Billing Server, it will prompt the payment method screen, which can choose the payment type (cash/credit card/octopus) 6. After payment, screen will display the “Charge” and print receipt | |

**Software (Shop)**

|  |
| --- |
| POS System |
| Ordering system |
| Billing system |
| Inventory System |

**Hardware**

|  |  |
| --- | --- |
| **Set of ALL-IN-ONE POS PC** | **Set of ALL-IN-ONE Wireless Terminal** |
| 1. Touch Monitor and Computer 2. IC Card Reader 3. Thermal Receipt Printer 4. Barcode Scanner 5. Cash Drawer | 1. Touch Screen 2. IC Card Reader 3. Magnetic stripe card reader 4. Thermal printer |

**Network Related**

|  |  |
| --- | --- |
| Physical topology | Star |
| Transport method | Ethernet |
| Transmission speed and cable type | WAN Cable: Fiber  LAN Cable: Unshielded twisted Cat5e 1000Mbps |
| NOS | PC Client: Windows Wireless Client: Linux (Android) |
| Protocol for wired part and protocol for wireless part | Protocol for wired part: TCP/IP Protocol for wireless part: 802.11n/ac |

**IP Address Table (Office)**

|  |  |
| --- | --- |
| IP Range | 10.8.0.0 |
| IP Address | 10.8.0.1 ~ 10.8.0.255 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 10.8.0.254 |

**IP Address Table (Office’s Wireless Router)**

|  |  |
| --- | --- |
| IP Range | 10.8.10.0 |
| IP Address | 10.8.10.1 ~ 10.8.10.255 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 10.8.10.254 |

**IP Address Table (Shop)**

|  |  |
| --- | --- |
| IP Range | 10.8.1.0 |
| IP Address | 10.8.1.1 ~ 10.8.1.255 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 10.8.1.254 |

**IP Address Table (Shop – Wireless Devices)**

|  |  |
| --- | --- |
| IP Range | 10.8.11.0 |
| IP Address | 10.8.11.1 ~ 10.8.11.255 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 10.8.11.254 |

|  |  |  |
| --- | --- | --- |
| **IP** | **Name** | **Description** |
| 10.8.0.254 | Firewall (Office) | Connect to WAN |
| 10.8.1.254 | Firewall (Shop) | Connect to WAN |
| 10.8.10.254 | Access Point (office) | AP For wireless devices & guest network |
| 10.8.11.253 | Access Point1 | AP1 – Connect to POE switch port 1 For wireless devices & guest network  Setting: AP Bridge Point-to-Point |
| 10.8.11.254 | Access Point2 | AP2 – Connect to POE switch port 2  For wireless devices & guest network  Setting: AP Bridge Point-to-Point |

**Security**

|  |  |
| --- | --- |
| Firewall | IPsec VPN: Shop connect to Main Office, upload the data to Office server.  NAT, Access-list, IDS, IPS, DMZ |
| Switch | NAT, VLAN |

**Cost estimate (Shop)**

|  |  |  |
| --- | --- | --- |
| Device | Number | Cost |
| Firewall | 1 | $5000 |
| POE Switch | 1 | $3000 |
| POS All-In-One PC | 6 | $30000 |
| Wireless terminal | 10 | $20000 |
| Access Point | 2 | $5000 |
| Total Cost | $63000 | |

END OF Assignment 4