Network Administration/System Administration Homework #0

B10202012 劉仲楷

Acknowledgement 這份作業有參考 ChatGPT，但都是用自己的話寫出。

Network Administration

I Short Answer

1. 自上而下分別是（參考 Kurose 與 Ross 撰寫的課本）

名稱	功能	應用服務	網路設備	常見問題解析
Application	support network applications	HTTP	Proxy	憑證過期
Transport	process-process data transfer	TCP	防火牆	封包遺失
Network	routing of datagrams from source to destination	IPv4	router	IP Spoofing
Link	data transfer between neighboring network elements	Ethernet	switch	MAC 位址衝突
Physical	bits “on the wire”	光纖傳輸	光纖	硬體故障、電磁干擾

2. (a) VLAN 是 Link Layer 的技術，用來將一個或多個 switch(es)，也就是實體網路，分成一個或多個邏輯子網路。好處是方便管理，因為不受硬體限制，也提升網路安全。

   (b) Gateway 用來連結不同網路，讓不同 protocol 或不同子網能溝通。例如不同 AS 之間就需要透過 gateway router 傳輸封包。

   (c) Switches 用來建立 LAN（區域網路），讓同一網段的設備能溝通；routers 則用來連接網路，並選擇連接起點和終點的最佳路徑。因此 switches 比較著重在 link layer 而 routers 則是 network layer。

   (d) Broadcast storm 是當有很多需要廣播的封包時，會造成交通壅塞。Switching loop 則是當封包的路徑是 loop 時，封包就無法到達終點，進而導致交通壅塞。相同的地方是兩個都會造成交通壅塞；不同的地方是起因不同。解決 broadcast storm 的方法是規劃好可以廣播的範圍（LAN）或是額外付出成本控制；解決 switching loop 的方法是利用 spanning tree protocol（STP）以及檢查實體網路拓撲用沒有環。

3. NAT 用來轉換內部私有 IP 以及外部公開 IP。例如家用網路利用多臺主機但同一個 IP 網址上網，則需要這個轉譯裝置才知道哪個封包傳給哪個主機/外面的IP。另一個應用是在內網架設伺服器使用 port forwarding 技術，這樣能隱藏內部主機的實際 IP，外部看不到內部結構，進而降低直接攻擊內部主機的風險。

4. 因為 IPv4 不夠用，換成 IPv6 就夠用了。IPv6 有 128 bits，因此完全夠用，遠超過未來需求。同時有兩個版本是因為很多應用不支援 IPv6，因為對使用者來說換成 IPv6 的好處不大，但要保證相容性的前提下，只好並行。

5. 相同的是都是 transport layer protocol。不同的是 TCP 是 connection-oriented，建立連線要 three-way handshake，並有 reliability、congestion control 等機制；而 UDP 是 connectionless，因此沒有上述的保證，但也因此封包小、延遲低。UDP 適合即時影音串流、DNS 等情境，而 TCP 適合 HTTPS、SMTP、SFTP 等。

6. - Access Point, AP：用來提供 Wi-Fi 無線連線。
   - Router：連接 WAN、LAN；Switch：組成 LAN
   - 防火牆：過濾惡意流量
   - DNS 伺服器：domain name 和 IP 轉換；DHCP：自動分配 IP
   - CA：簽發憑證，提供認證

7. - 在 eno0 設定 public IP（140.112.30.1），並且把 140.112.30.254 設為 唯一的 default gateway
   - 在 eno1 設定 private，不要設 default gateway
   - 加入靜態路由例如：

     ```
     ip route add 172.16.0.0/16 via 172.16.0.1 dev eno1
     ip route add 10.0.0.1 via 172.16.0.1 dev eno1
     ```

8. (a) Trunk mode 可以讓不同 VLAN 的流量通過；access mode 則只能讓單一 VLAN 通過。Access mode 通常用來連接 PC 等單一 VLAN；Trunk mode 則用來連接 switch、router 等。Access mode 只轉發 untagged 的封包；trunk mode 對於不是 native VLAN 的封包都會加上 802.1Q tag。Native VLAN 則在該 trunk 上不加 tag 傳送的封包會被歸到這個 VLAN。

   (b) 如下表所示，native VLAN 改成 999 當黑洞。

Port	Mode (trunk/access)	Native VLAN	Tagged VLAN(s)
1	trunk	999	10, 20, 30
2	access	10	-
3	access	20	-
4	access	30	-

   (c) 伺服器在單一實體 NIC（例如 eth0）上建立三個 VLAN 子介面，各自對應 VLAN 10/20/30，並在子介面上設定對應網段的 IP。

II Command Line Utilities

1. (a) 140.112.8.116
   (b) 140.112.30.26

2. (a) meow1.csie.ntu.edu.tw
   (b) smtps.ntu.edu.tw

III 網路連線與 WireShark

1. (a) TCP 用來做 end-to-end 的溝通。它將 application layer 的 data 切成 segment，透過 network layer 傳輸，在接收端再重新組合。此外，它有 reliability、congestion control、connection-oriented 等特色。

   (b)
   - Source Port：用來標示發送端的應用程式。例如一台瀏覽器開啓網頁，會隨機使用一個臨時 port 來和伺服器溝通。
   - Destination Port：用來標示接受端的應用程式。例如 HTTP 通常是 80，HTTPS 是 443。
   - Sequence Number：用來記錄一個封包在整個 stream 中的位置，讓接收端照 sequence number 的順序重組被切割的資料，並偵測遺失封包。
   - Checksum：用來檢查傳輸資料有沒有 1 bit 錯誤。
   - Acknowledgment Number：告訴發送端已經收到的最後一個 正確封包的 sequence number 的下一個。例如 0-100 已經接收到，但 99 checksum 不符，則為 99。或是都正確接收，則為 101。

   (c) TCP 需要 three-way handshake 因為 1. 確保雙方的收發能力、2. 正常同步 initial sequence number，避免重複用舊的連線資料。

   i. SYN（Client 到 Server）：Client 端送出 SYN 封包，需要附上 initial sequence number（ISN_C）。用來告訴伺服器客戶端的位置（IP）、應用程式（port）以及初始序號。

   ii. SYN + ACK（Server 到 Client）：Server 回覆一個包含 SYN 和 ACK 的封包。其中 SYN 含有自己的 initial sequence number（ISN_S），ACK 用來回覆收到客戶端的 SYN，並回覆 ISN_C + 1。用來告訴客戶端已經收到請求，可以建立連線，並提供自己的初始序號。

   iii. ACK（Client 到 Server）：Client 回覆 ACK 封包，包含 ISN_S + 1，用來回覆已經收到伺服器的初始序號了。

2. (a) ICMP 用來做錯誤回報，而不是資料傳輸。IMCP 依附在 IP，在 network layer，而 TCP/UDP 在 transport layer，因此 IMCP 沒有 port 的概念

   (b)
   - Echo Request：請對方回覆以測試是否能到達目的地
   - Echo Reply：回覆 Echo Request，也就是目的地能到達
   - Destination Unreachable：當 router 或 server 發現封包無法送達時，用來回報，並說明原因，如 ip 或 port 不可達。

   (c) 當使用 `ping` 時，系統會產生一個 ICMP Echo Request 封包，送到目標 IP。若正常運作，目標會回覆一個 ICMP Echo Reply 封包。`ping` 根據是否收到回覆以及回覆內容判斷是否可抵達、RTT 等。

3. (a) SSL/TLS 是用來建立在 application layer 之上的資安 protocol，用來保證資料傳輸的機密性（confidentiality）, 完整性（integrity）以及身份認證（authentication）。它透過非對稱加密及 key exchange 確保機密性，MAC 或 HMAC 確保完整性，以憑證用來做身份認證。

   (b) 在 TLS handshake 後，client 會產生一個隨機數字，成為 pre-master secret key，再透過伺服器的 public key 加密後傳給伺服器。伺服器收到後，雙方再利用 pre-master secret key 交換各自隨機數，即可計算出相同的 master secret key。最後會利用 master secret key 產生 session keys，用來加密各 session 的傳輸資料。Wireshark 會需要 pre-master secret key 是因為 session key

會被 master secret 加密。如果有 pre-master secret，就能按照 TLS protocol 推得 master secret，再得到 session keys。

(c) HTTP 傳輸明文，用 TCP Port 80。HTTPS 是 HTTP 透過 SSL/TLS加密傳輸，用 TCP Port 443。HTTP 容易被竊聽或被 MitM attack。因此 HTTPS 透過前兩題所說的方式保證各 sessions 的機密性、完整性及身份認證。

(d) i. course8pz3.aca.ntu.edu.tw（臺大課程網）。透過 Statistics > IPv4 Statistics 可以看到只有 172.20.10.2 和 140.112.161.137，並且透過 info 欄位看到 client hello，再看到 destination 就能知道 140.112.161.137 是 server 端。最後透過 `nslookup` 知道這個 IP 的 domain name。

ii. A. 解密：Edit > Preferences > Protocols > TLS 設定 pre-master secret key。此時點擊右下角有 Decrypted TLS 可看到解密後的明文。

B. 篩選 HTTP，ip.src 篩 172.20.10.2，ip.dst 篩 140.112.161.137

C. 看到 Info 欄位含有 /search/quick?... 並截取後面文字

D. 貼在 https://course.ntu.edu.tw 的最後並在瀏覽器搜尋

E. 得到結果為「網路管理」及「蔡欣穆」，所以是網路管理。

4. (a) 如下圖所示，我 `ping` 了 8.8.8.8。可以看到 echo request destination 和 echo reply source 為 8.8.8.8。

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	140.112.243.115	8.8.8.8	ICMP	98	Echo (ping) request id=0x7d3a, seq=1/256, ttl=64 (reply in 2)
2	0.001835304	8.8.8.8	140.112.243.115	ICMP	98	Echo (ping) reply id=0x7d3a, seq=1/256, ttl=117 (request in 1)
3	1.001276976	140.112.243.115	8.8.8.8	ICMP	98	Echo (ping) request id=0x7d3a, seq=2/512, ttl=64 (reply in 4)
4	1.002881358	8.8.8.8	140.112.243.115	ICMP	98	Echo (ping) reply id=0x7d3a, seq=2/512, ttl=117 (request in 3)
5	2.003393899	140.112.243.115	8.8.8.8	ICMP	98	Echo (ping) request id=0x7d3a, seq=3/768, ttl=64 (reply in 6)
6	2.005268226	8.8.8.8	140.112.243.115	ICMP	98	Echo (ping) reply id=0x7d3a, seq=3/768, ttl=117 (request in 5)
7	3.004800833	140.112.243.115	8.8.8.8	ICMP	98	Echo (ping) request id=0x7d3a, seq=4/1024, ttl=64 (reply in 8)
8	3.006542434	8.8.8.8	140.112.243.115	ICMP	98	Echo (ping) reply id=0x7d3a, seq=4/1024, ttl=117 (request in 7)
9	4.005811582	140.112.243.115	8.8.8.8	ICMP	98	Echo (ping) request id=0x7d3a, seq=5/1280, ttl=64 (reply in 10)
10	4.007171006	8.8.8.8	140.112.243.115	ICMP	98	Echo (ping) reply id=0x7d3a, seq=5/1280, ttl=117 (request in 9)

Figure 1: `ping` 指令的 ICMP 封包

(b) 擷取封包後在 filter 欄位篩選 http，並在 Hypertext Transfer Protocol 下展開，找到 Host、Connection 等 HTTP Header。

```
▸ Frame 14234: 443 bytes on wire (3544 bits), 443 bytes captured (3544 bits) on interface
▸ Ethernet II, Src: CompalInform_63:be:90 (08:8f:c3:63:be:90), Dst: cc:6a:33:2a:35:c7 (cc
▸ Internet Protocol Version 4, Src: 140.112.243.115, Dst: 34.223.124.45
▸ Transmission Control Protocol, Src Port: 36706, Dst Port: 80, Seq: 1, Ack: 1, Len: 377
▾ Hypertext Transfer Protocol
  ▸ GET /online HTTP/1.1\r\n
    Host: shininggoodastoundinglight.neverssl.com\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:136.0) Gecko/20100101 Firefox/136.0\r\
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Sec-GPC: 1\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Priority: u=0, i\r\n
    \r\n
    [Full request URI: http://shininggoodastoundinglight.neverssl.com/online]
    [HTTP request 1/3]
    [Response in frame: 14255]
    [Next request in frame: 14257]
```

Figure 2: neverssl 的連線資訊

System Administration

I 想變强的捷兔

1. Dockerfile 如下所示。

```
FROM python:3.12-alphine
WORKDIR /home/nasa/
COPY secret .
RUN python3 secret_script.py && rm secret_script.py
ENTRYPOINT ["sh"]
```

   FROM 用來指定 container 的 base image；WORKDIR 是工作目錄，接下來的 COPY、RUN、ENTRYPOINT 都在此目錄下執行。COPY 將 `secret` 複製到 container；RUN 在 build 時執行 `secret_script.py` 並刪掉。ENTRYPOINT 進入 shell。

2. RUN 在 build time 執行；ENTRYPOINT 在 runtime 執行。如果合併，則每次啓動都會執行 `secret_script.py`，且刪掉。但如果上次刪掉，則這次沒有這份檔案就執行不了，就會報錯。

3. ENTRYPOINT 是固定執行入口；CMD 則是預設執行的命令或參數，所以可以把 ENTRYPOINT 換成 CMD，只是較容易被覆蓋。同時有 ENTRYPOINT 和 CMD 會變成：例如

   ```
   ENTRYPOINT ["python3"]
   CMD ["app.py"]
   ```

   則預設會執行 `python3 app.py`

使用

```
docker image ls
```

可以看到唯一的 image 是 test。再使用

```
docker run -it test
```

啓動，結果如 fig. 3。 最後使用

```
base64 -d \$(find / -name "holiday.txt")
```

找到 `FLAG{J3T2h011DAY!!}`

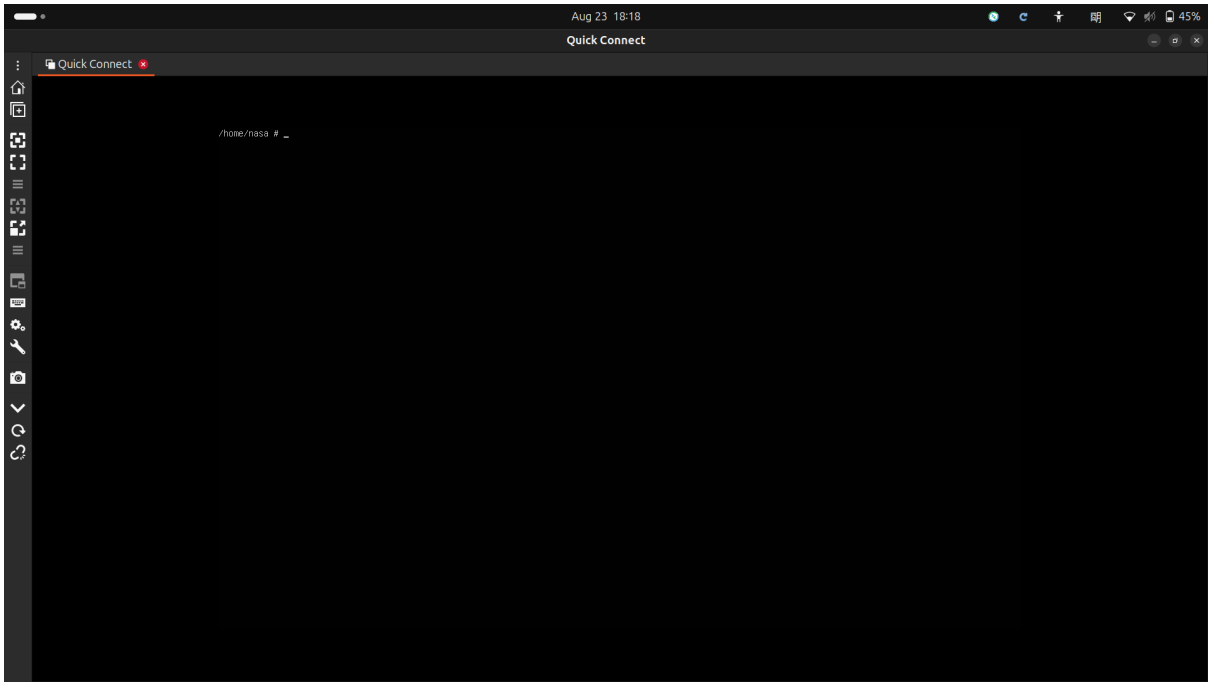

Figure 3: 進入 Docker Shell 圖

II RSA

1. 明文是 `FLAG{RSA_15_V3RY_FUN_7O_P14Y_42OUND}`，程式碼如下所示。

```
from Crypto.Util.number import bytes_to_long, long_to_bytes
import base64
...
cipher_bytes = base64.b64decode(cipher)
c = bytes_to_long(cipher_bytes)
n = pow(c, d, N)
m = long_to_bytes(n)
print(m)
```

2. 利用下列程式碼即可取得結果如 fig. 4。

```
openssl pkey -in private.pem -pubout
```

```
joshua@joshua-Aspire-A514-55:~/nasa$ openssl pkey -in private.pem -pubout
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDw9Zqs6jtKCRX3yzr4quzNt118
5Mva3JAczVCpklxhtwgiOw8Z+oJyuR4vz1SXtynx2ESySLsNJ+nXN6P/EStm6/Hl
B6BkAmNUT+HNB+rkLSs5lirdOQ+l4VAlJwUuo98Ua0LKIgMxbQb28+xU+HP/hVkM
A4cxF7OKpT8+g9ChPwIDAQAB
-----END PUBLIC KEY-----
joshua@joshua-Aspire-A514-55:~/nasa$
```

Figure 4: `private.pem` 對應公鑰

3. 最低八位數是 83d0a13f。利用解題工具如 fig. 5。

```python
from Crypto.PublicKey import RSA
with open("private.pem", "rb") as f:
    data = f.read()
    mykey = RSA.import_key(data)
print(hex(mykey.n)[-8:])
```

Figure 5: `private.pem` 的 n

III The Web

1.
   - HTTP：HyperText Transfer Protocol，是一種 Application layer 的 protocol。用來約定瀏覽器和伺服器的資料傳輸方式。
   - HTML：HyperText Markup Language，一種標記語言，用來記錄網頁結構與內容。
   - URL：Uniform Resource Locator（統一資源定位器），用來指定網路資源位置與存取方式。例如 https://example.com/index.html：https 是使用協定；example.com 是網域名；index.html 是資源路徑。

2. (a) 結果如 fig. 6 所示。

欄位	內容
請求方法	GET
請求目標路徑	/
HTTP 協定版本	HTTP/1.1
請求標頭	Host: www.csie.ntu.edu.tw
	User-Agent: curl/8.5.0
	Accept: */*
回應狀態碼與訊息	301 Moved Permanently
HTTP 協定版本	HTTP/1.1
回應標頭	Date: Sat, 23 Aug 2025 12:55:05 GMT
	Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
	Location: https://www.csie.ntu.edu.tw/
	Content-Length: 236
	Content-Type: text/html; charset=iso-8859-1
回應主體	`<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">`
	`<html><head>`
	`<title>301 Moved Permanently</title>`

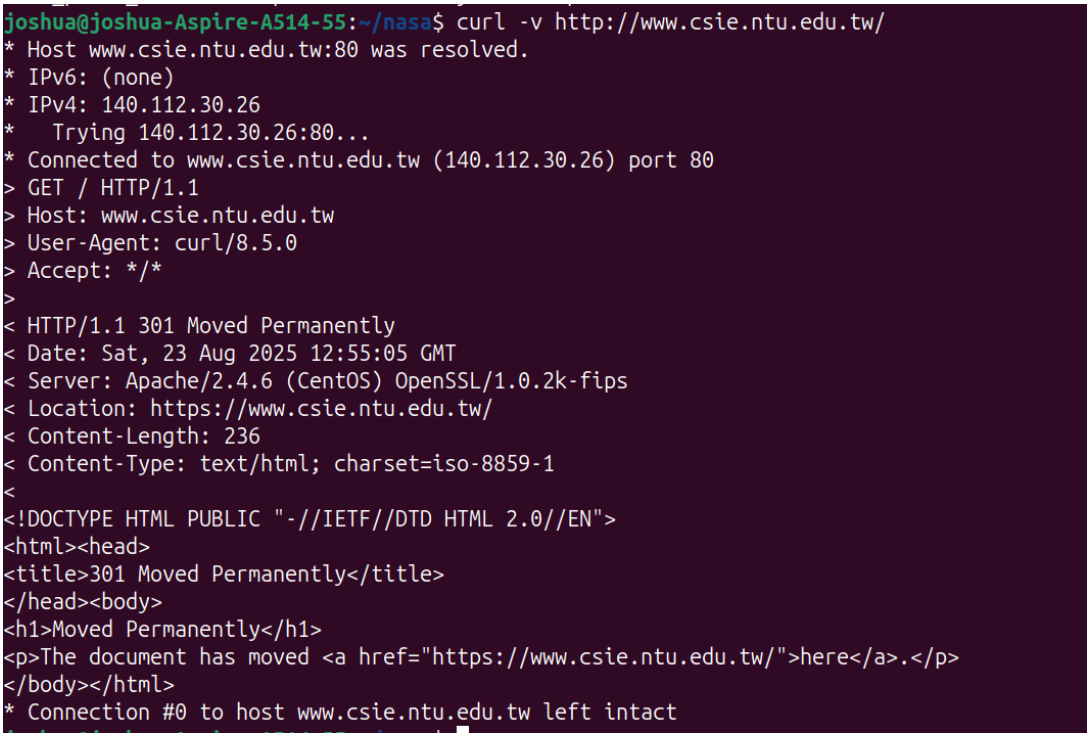

Figure 6: `curl` 執行結果

(b) 回應是 301 Moved Permanently，意義是請求的資源已經被永久移動到新的 URL。利用到 Location 標頭資訊，指出新的資源位置（新的 URL）。

(c) 使用的技術是虛擬主機 (Virtual Hosting)，也就是同一台伺服器 (同一個 IP) 運行多個網站，目的是為了節省 IPv4 位址資源，因此允許多個網域名稱對應到同一個伺服器。利用送出 header 裡的 host 辨別要連到的網站。

3. `FLAG{54v3_50_p0und5_p3r_p3r50n}`。先透過各

   ```
   curl -v ws6.csie.ntu.edu.tw:21080/discount
   ```

   找到 ws6.csie.ntu.edu.tw 的 IP：140.112.30.187，再手動設定 host。

   ```
   curl -v --header "Host: jet2holidays.csie.ntu.edu.tw" \
     http://140.112.30.187:21080/discount
   ```

4. (a) 使用 `curl -v https://www.csie.ntu.edu.tw/`

欄位	內容
TLS 版本	TLSv1.2
Cipher suite	ECDHE-RSA-AES128-GCM-SHA256
憑證主體	C=TW; ST=Taiwan; L=Taipei; O=National Taiwan University CN=*.csie.ntu.edu.tw
憑證發行者	C=TW; O=TAIWAN-CA; CN=TWCA Secure SSL Certification Authority
憑證到期日	Nov 3 15:59:59 2025 GMT

(b) 憑證（certificate）能確保連線對象是被認證的。若使用者信任憑證發行者（此為 TWCA），則利用非對稱加密，主體公佈公鑰並保留私鑰以供使用者連線時認證，防止 MitM 攻擊。

(c) TLS1.3 支援 1-RTT（false start）以及 0-RTT（early application data），縮短建立安全連線所需時間。TLS1.3 只支援擁有 forward secrecy 的密碼學演算法，並移除了不安全的演算法（SHA-1、MD5...）

(d) 例如釣魚網站，攻擊者取得了一張合法的憑證（例如 Let's Encrypt），並建立了和真實網站幾乎一樣的假網站，且 URL 只有一點點不一樣，則使用者還是會被騙。因為 HTTPS 只保證「傳輸過程加密」與「伺服器身份與憑證匹配」，並不保證其他的安全性。

IV Unix

使用下列指令得到 `FLAG{HAHAHAHAHA_MY_NAME_IS_FLASHPAW_HAHAHAHAHA}`

```
unzip bag.zip
strings clue.png | grep -o 'FLAG{[^}]*}'
```

接下來 `unzip temple.zip`，輸入 flag，進入資料夾後

```
find . -type f -print0 | xargs -0 du -b | sort -nr | head
```

即可找到最大的檔案並執行

```
./big_room13/small_room0/tinyroom16/statue.sh
```

會看到

> WOW! I AM SURPRISED YOU FOUND THE REAL ME!!!

進入該資料夾後，用 `ls -a` 即可看到 `.wall.inscription` 再使用

```
cowsay -f hellokitty.cow "$(cat .wall.inscription | tr 'a-z' 'n-za-m')" | lolcat
```

即可得到 fig. 7。

Figure 7: 召喚喵王