06 Wireshark 解 SMTP 的帳號和密碼解 base64 的編碼

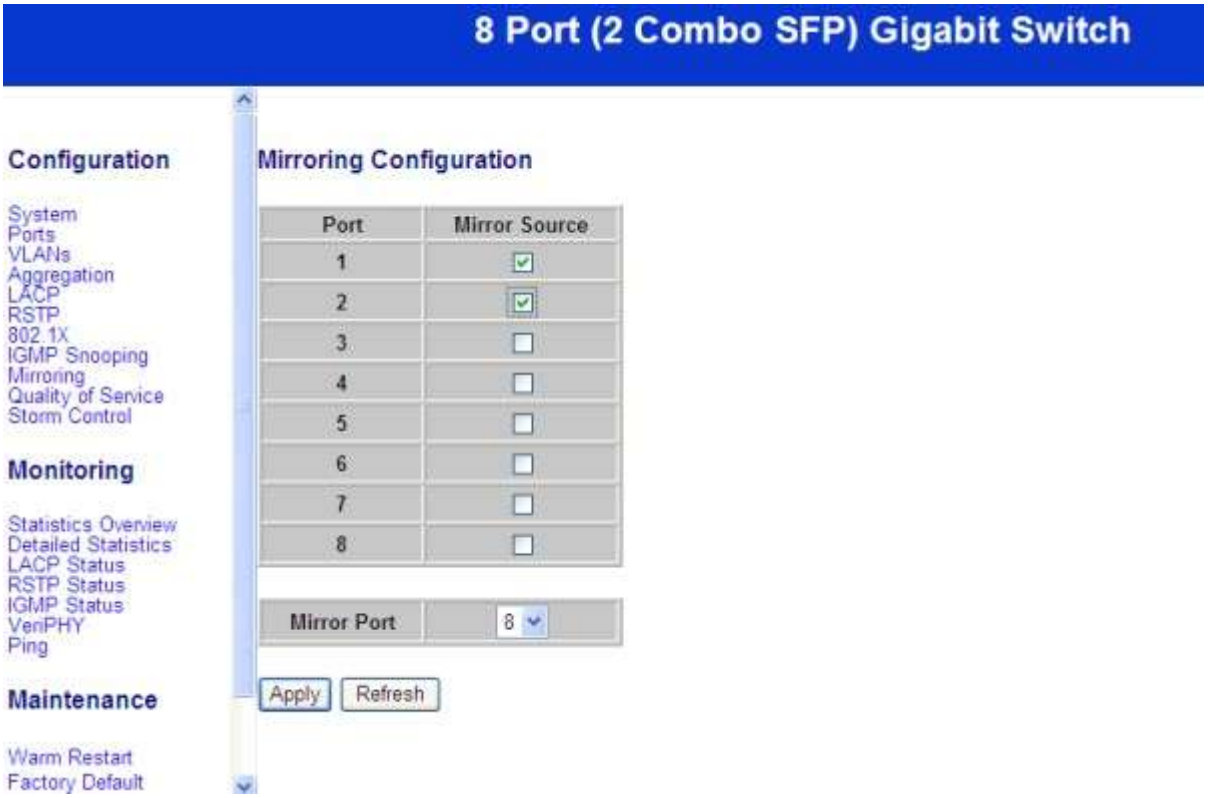
工具
UBS-5008 具有 Port Mirror 功能的 Switch Hub

一台 Windows 有安裝 Wireshark 的 Notebook

或是直接把 wireshark 安裝在 Exchnage Server 上面,不過此方法比較不建議
因爲搞不好那台 Server 有問題 XD

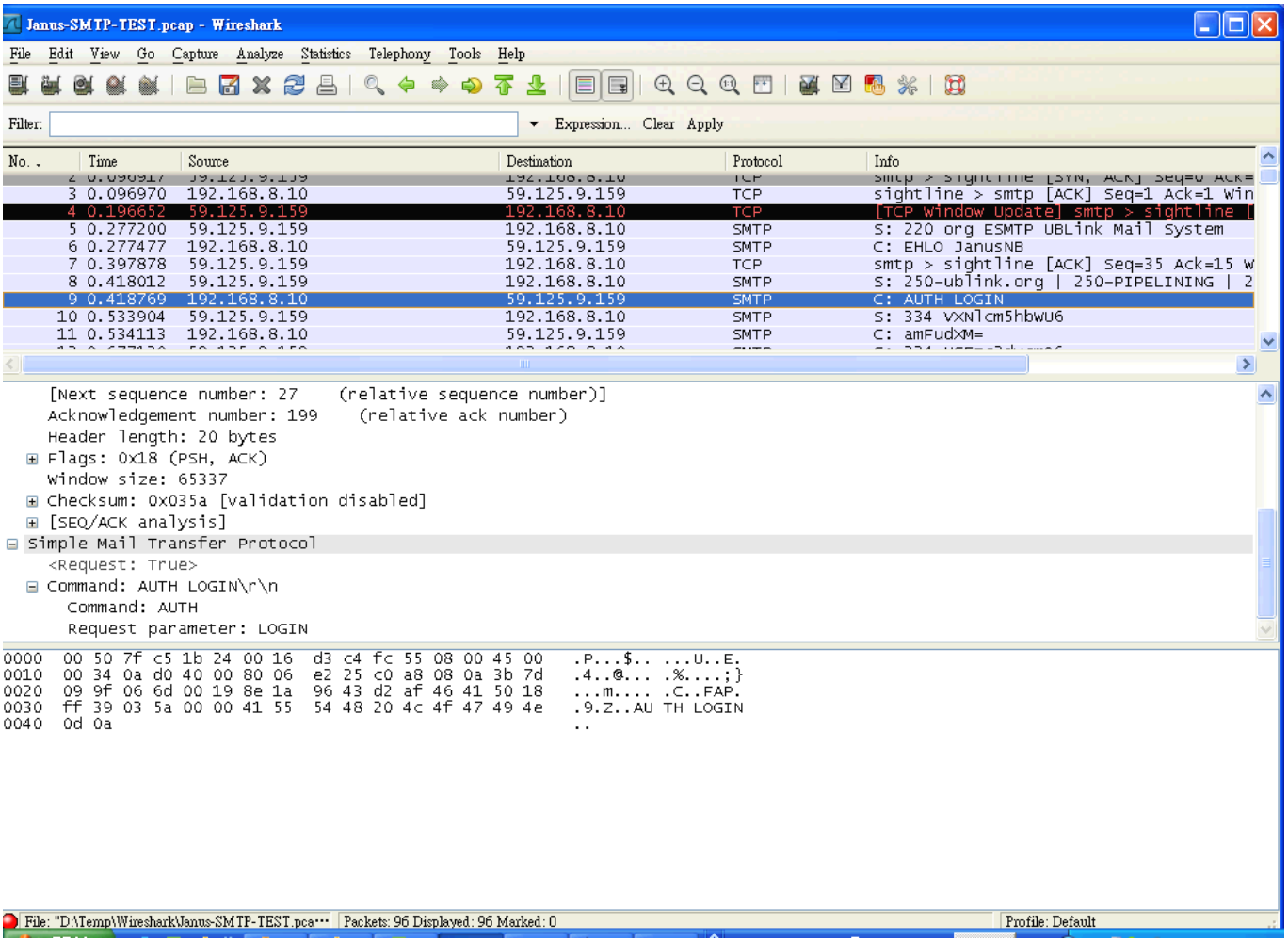
架構如下

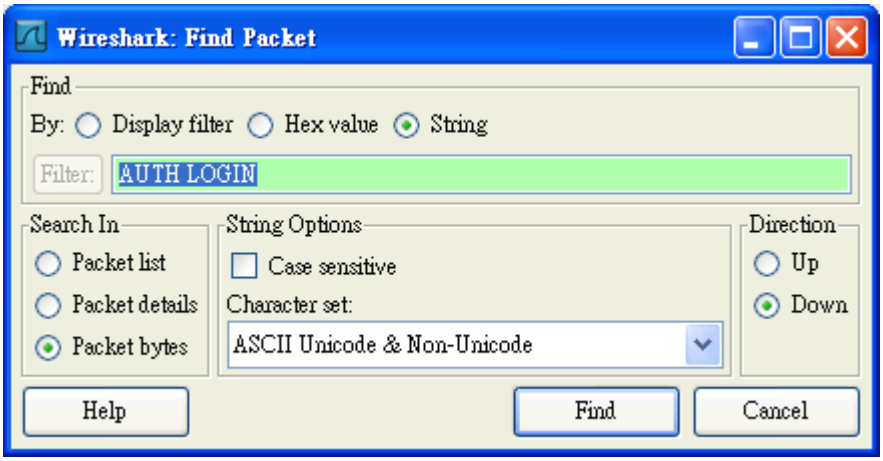
UBS-5008 設定如下



安裝 Wireshark 的 Notebook 裝在 Port 8
Mirror Port 1 的 Firewall 和 Port 2 的 Mail Server

Wireshark 抓一段 tcp port 25 的



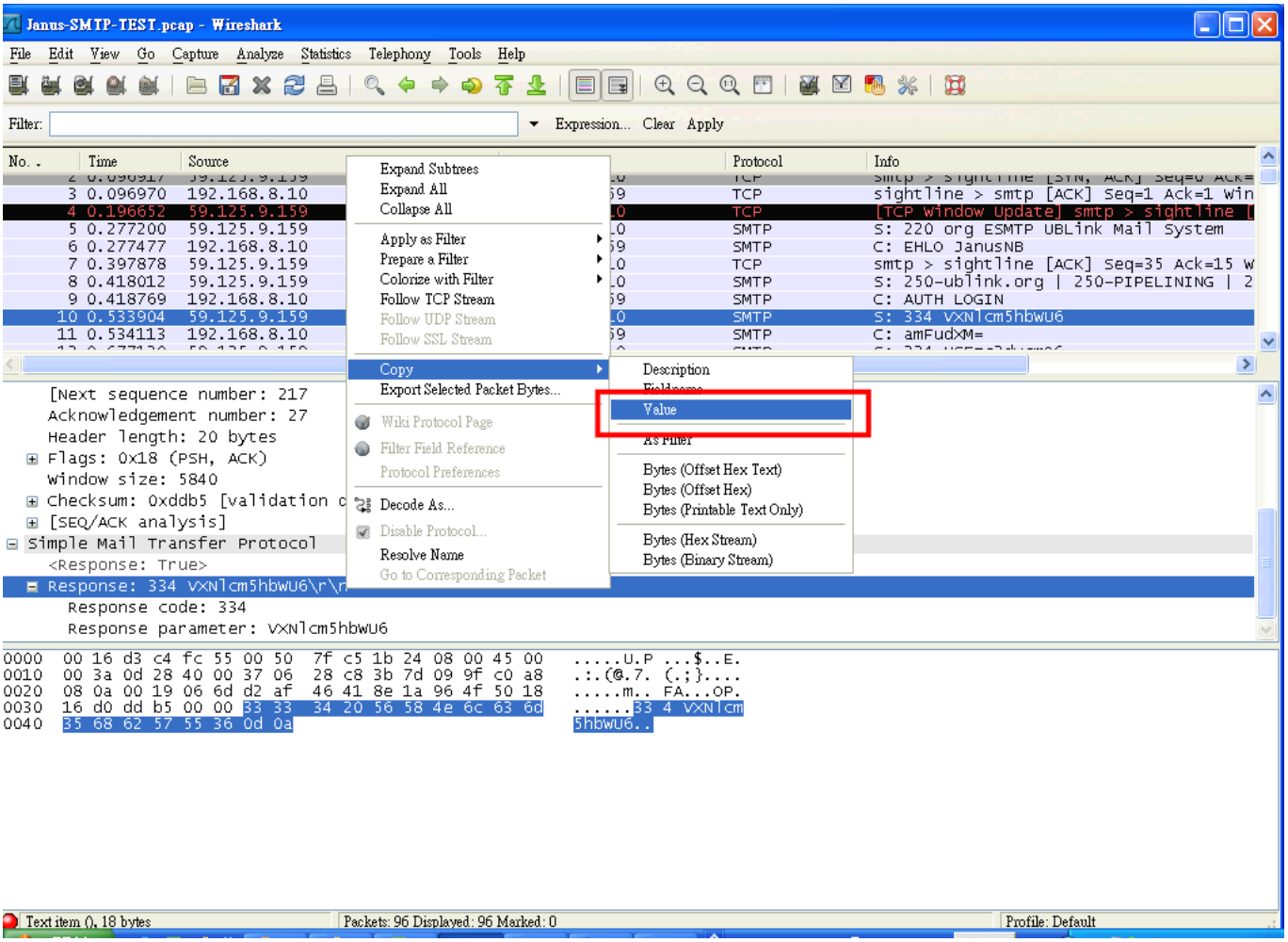


抓完之後

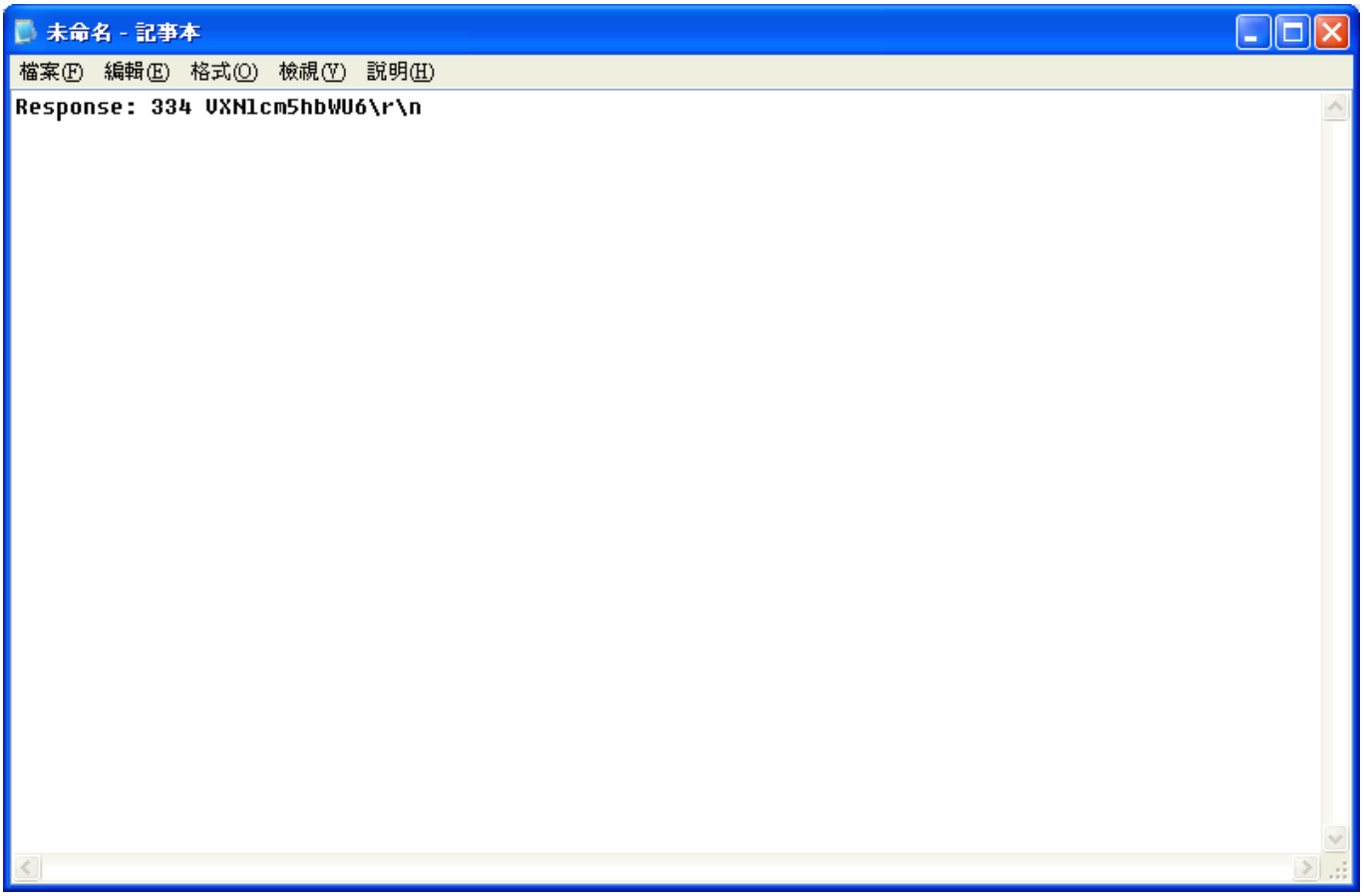
搜尋 String 是 AUTH LOGIN

AUTH LOGIN 是 Base64 的 Login 方法

直接找寄信最多的那一組


Janus-SMTP-TEST.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
No. Time Source Protocol Info
3 0.096970 192.168.8.10 TCP sightline > smtp [ACK] Seq=1 Ack=1 Win
4 0.196652 59.125.9.159 TCP [TCP Window Update] smtp > sightline [
5 0.277200 59.125.9.159 SMTP S: 220 org ESMTP UBLink Mail System
6 0.277477 192.168.8.10 SMTP C: EHLO JanusNB
7 0.397878 59.125.9.159 TCP smtp > sightline [ACK] Seq=35 Ack=15 W
8 0.418012 59.125.9.159 SMTP S: 250-ublink.org | 250-PIPELINING | 2
9 0.418769 192.168.8.10 SMTP C: AUTH LOGIN
10 0.533904 59.125.9.159 SMTP S: 334 VXNlcm5hbWU6
11 0.534113 192.168.8.10 SMTP C: amFudXM=
Expand Subtrees
Expand All
Collapse All
Apply as Filter
Prepare a Filter
Colorize with Filter
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Copy
Export Selected Packet Bytes...
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As...
Disable Protocol...
Resolve Name
Go to Corresponding Packet
Description
Value
As Filter
Bytes (Offset Hex Text)
Bytes (Offset Hex)
Bytes (Printable Text Only)
Bytes (Hex Stream)
Bytes (Binary Stream)
[Next sequence number: 217
Acknowledgement number: 27
Header length: 20 bytes
Flags: 0x18 (PSH, ACK)
Window size: 5840
Checksum: 0xddb5 [validation
[SEQ/ACK analysis]
Simple Mail Transfer Protocol
<Response: True>
Response: 334 VXNlcm5hbWU6\r\n
Response code: 334
Response parameter: VXNlcm5hbWU6
0000 00 16 d3 c4 fc 55 00 50 7f c5 1b 24 08 00 45 00 .....U.P ...$..E.
0010 00 3a 0d 28 40 00 37 06 28 c8 3b 7d 09 9f c0 a8 .:.(@.7. (.;}....
0020 08 0a 00 19 06 6d d2 af 46 41 8e 1a 96 4f 50 18 .....m.. FA...OP.
0030 16 d0 dd b5 00 00 33 33 34 20 56 58 4e 6c 63 6d ......33 4 VXNlcm
0040 35 68 62 57 55 36 0d 0a 5hbWU6..
Text item (), 18 bytes
Packets: 96 Displayed: 96 Marked: 0
Profile: Default

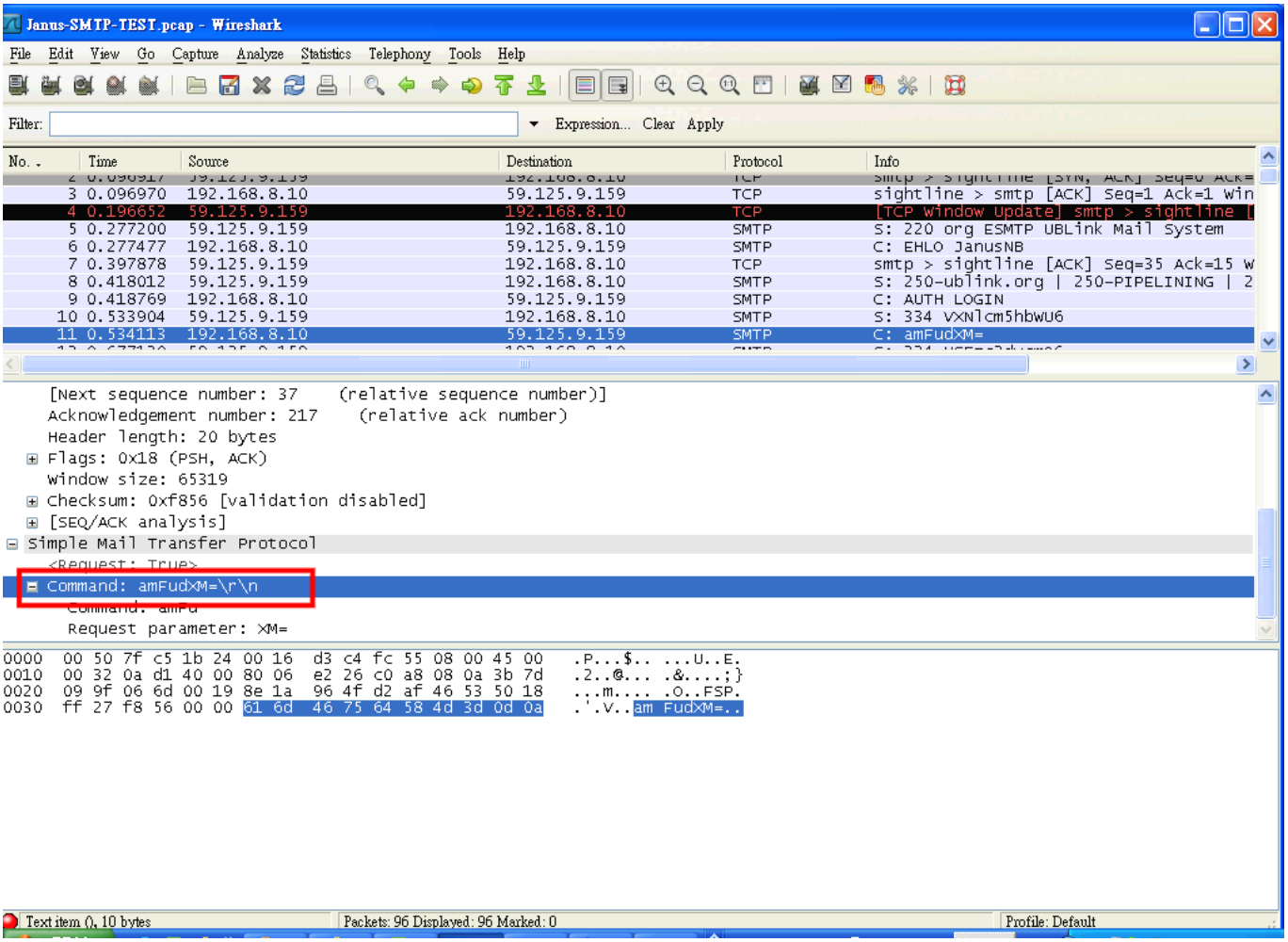
把他 Copy 到記事本



這一串解碼是 username

在這解碼

http://www.ublink.org/index.php/new/base64-.html



這一串才是 janus

Response: 334 VXNlcm5hbWU6\r\n 解出 Username:

Command: ZXJpYw==\r\n 解出 eric

Response: 334 UGFzc3dvcmQ6\r\n 解出 Password:

Command: MTIzNDU2\r\n 解出 123456

這樣就可以很快找到被 Relay 的帳號跟密碼了