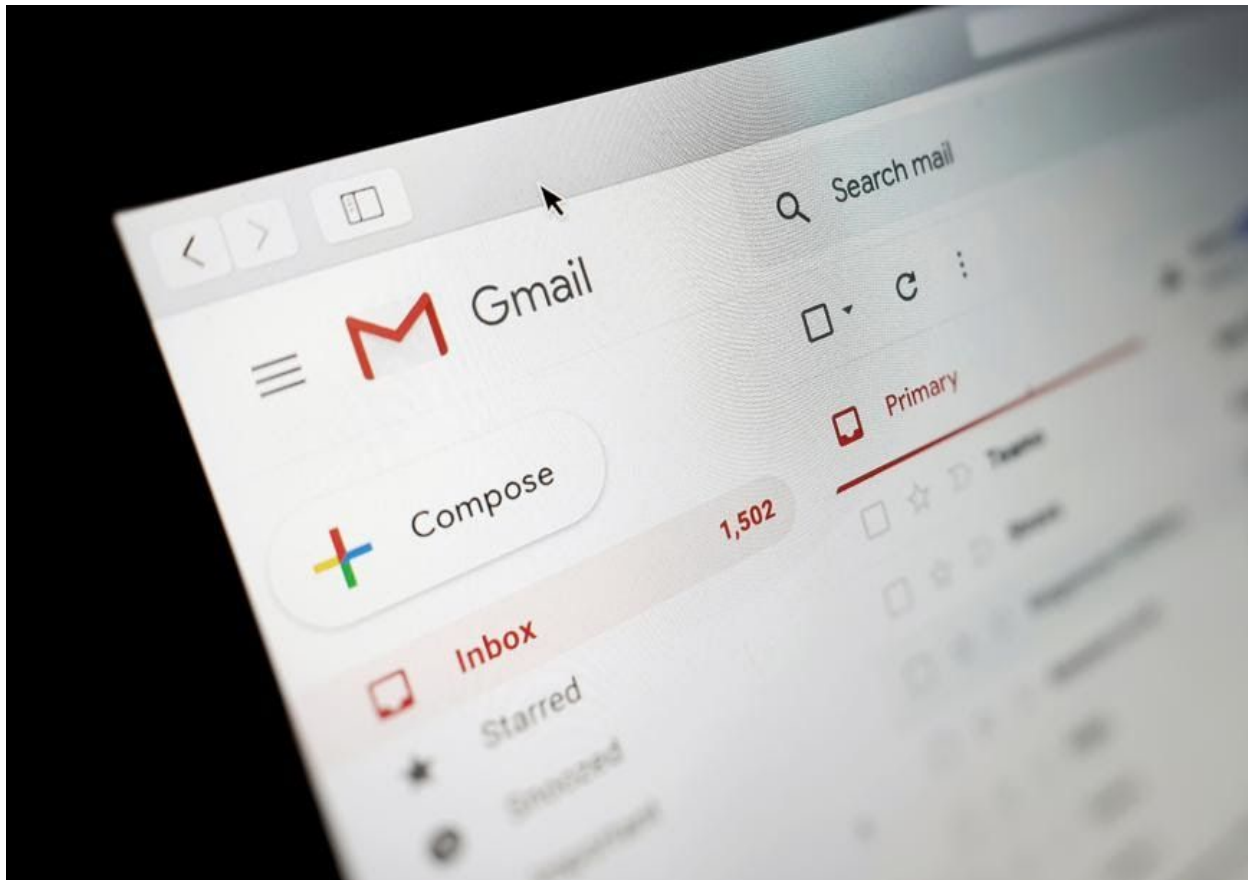


# GmailSending

## โปรแกรมส่งอีเมล Gmail



ชัญธิชา หาญศิริสถาพร 6010450349

ฉันทิกา บำรุง 6010451027

## Project 1: GmailSending

โปรแกรม GmailSending (เปลี่ยนจากที่เคยตอบใน quiz เรื่อง คำนวณ BMI)  
เป็นโปรแกรมที่ใช้ส่งอีเมลแบบง่ายๆด้วยภาษาโปรแกรม Python

วัตถุประสงค์ : ใช้ส่งอีเมลหาผู้รับ โดยไม่ต้องเข้า gmail ก็ส่งได้เหมือนกัน

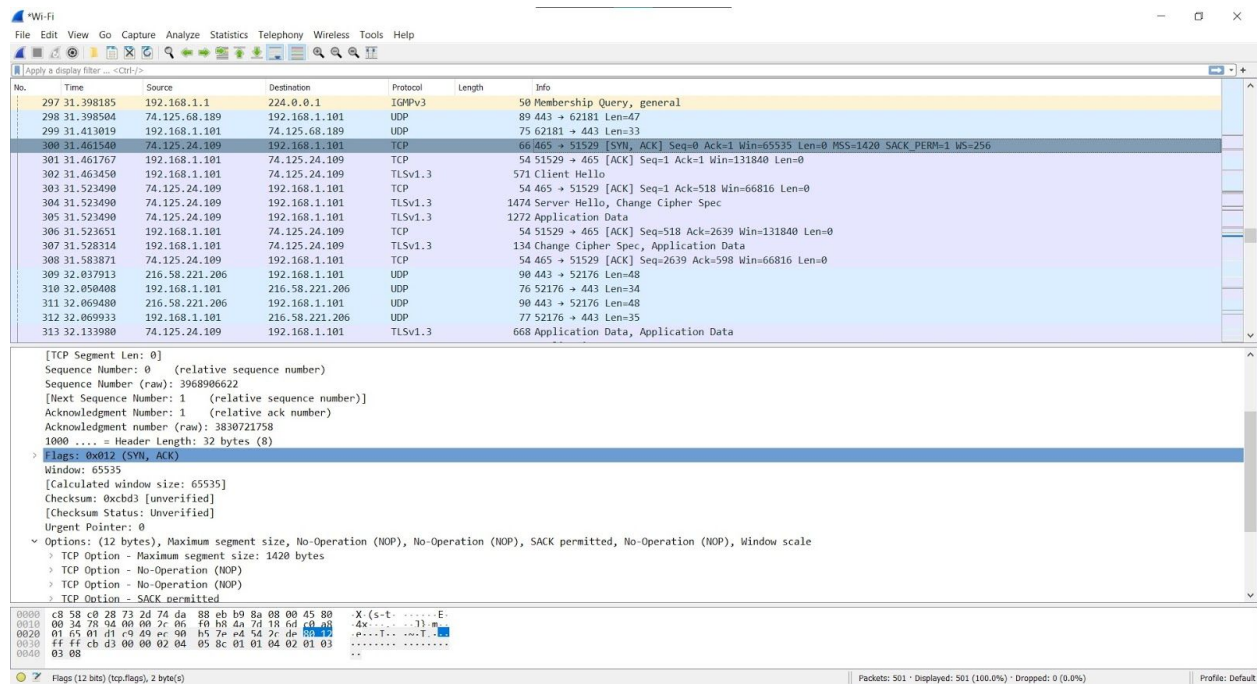
คุณลักษณะ : ส่งอีเมลผ่านโปรแกรม มีการตอบกลับเมื่อส่งสำเร็จ มีการปิดบัง password ให้  
โดยใช้ TCP( Transmission Control Protocol)

### ออกแบบ Application layer protocol

มีการใช้ SSL ที่ช่วยเพิ่มการรักษาความปลอดภัยในการรับส่งข้อมูลบนระบบเครือข่าย โดยอีเมล  
ที่ทำการส่งจะไม่ถูกแก้ไขเปลี่ยนแปลง และใช้ SMTP Gmail (smtp.gmail.com) ที่ใช้ส่ง  
email ในเครือข่ายอินเทอร์เน็ต

Source Code : ชื่อไฟล์ GmailSending\_Real

# Wireshark



## Flags:

ครั้งที่ 1 ผู้ส่งขอเริ่มติดต่อ > flags = SYN

ครั้งที่ 2 ผู้รับรับการติดต่อและพร้อมจะติดต่อ flags = SYN/ACK

ครั้งที่ 3 ผู้ส่งส่ง ACK กลับไปหาผู้รับ โดยมี socket, tcp ตามที่ตกลงไว้ คือ smtp, ssl

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl>F

No.	Time	Source	Destination	Protocol	Length	Info
416	35.969623	216.58.221.206	192.168.1.101	UDP	417	443 → 52176 Len=375
417	35.970491	192.168.1.101	216.58.221.206	UDP	82	52176 → 443 Len=40
418	35.970949	216.58.221.206	192.168.1.101	UDP	89	443 → 52176 Len=47
419	35.984916	192.168.1.101	216.58.221.206	UDP	76	52176 → 443 Len=34
420	36.025789	216.58.221.206	192.168.1.101	UDP	68	443 → 52176 Len=26
421	36.057242	52.114.36.46	192.168.1.101	TCP	66	443 → 51531 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1420 WS=256 SACK_PERM=1
422	36.057430	192.168.1.101	52.114.36.46	TCP	54	51531 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0
423	36.058143	192.168.1.101	52.114.36.46	TLSv1.2	571	Client Hello
424	36.235929	52.114.36.46	192.168.1.101	TCP	5734	443 → 51531 [ACK] Seq=1 Ack=518 Win=524800 Len=5680 [TCP segment of a reassembled PDU]
425	36.235929	52.114.36.46	192.168.1.101	TLSv1.2	134	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
426	36.235991	192.168.1.101	52.114.36.46	TCP	54	51531 → 443 [ACK] Seq=518 Ack=5761 Win=131840 Len=0
427	36.238534	192.168.1.101	52.114.36.46	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
428	36.238735	192.168.1.101	52.114.36.46	TLSv1.2	153	Application Data
429	36.239043	192.168.1.101	52.114.36.46	TLSv1.2	2155	Application Data
430	36.239105	192.168.1.101	52.114.36.46	TLSv1.2	161	Application Data
431	36.439933	52.114.36.46	192.168.1.101	TCP	54	443 → 51531 [ACK] Seq=5761 Ack=775 Win=524544 Len=0
432	36.439933	52.114.36.46	192.168.1.101	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message

[TCP Segment Len: 0]  
Sequence Number: 0 (relative sequence number)  
Sequence Number (raw): 2095915843  
[Next Sequence Number: 1 (relative sequence number)]  
Acknowledgment Number: 1 (relative ack number)  
Acknowledgment number (raw): 1745524357  
1000 .... = Header Length: 32 bytes (8)  
Flags: 0x012 (SYN, ACK)  
0000 .... = Reserved: Not set  
...0... = Nonce: Not set  
....0... = Congestion Window Reduced (CWR): Not set  
....0... = ECN-Echo: Not set  
....0... = Urgent: Not set  
....1... = Acknowledgment: Set  
....0... = Push: Not set  
....0... = Reset: Not set  
....1... = SYN: Set  
....0... = Fin: Not set

0010 00 34 88 42 40 00 70 06 67 34 34 72 24 2e c0 a8 -4 B@-p- g4Ar\$...  
0020 01 65 01 bb c9 4b 7c ed 23 43 68 0a 96 85 80 12 -e...K]- #Ch-----  
0030 ff ff ea b3 00 00 02 05 05 8c 01 03 03 08 01 01 .....  
0040 04 02 .....

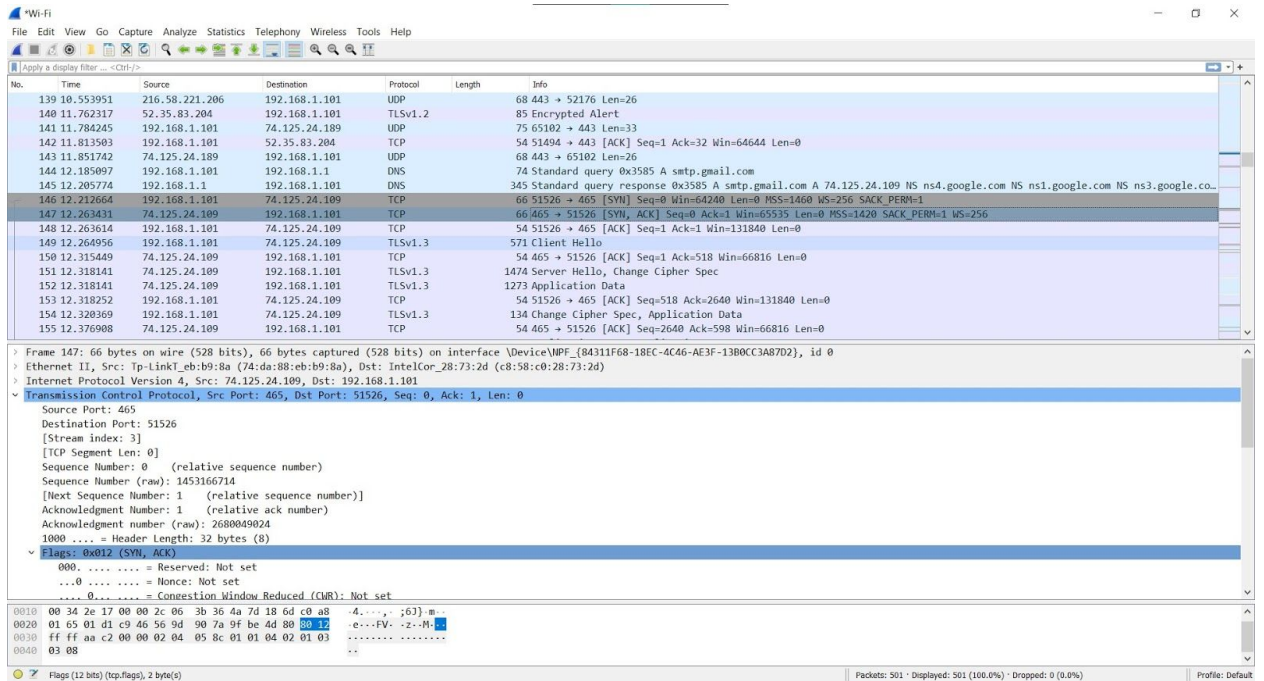
Flags (12 bits) (tcp.flags), 2 byte(s)

Packets: 501 · Displayed: 501 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

ตอน Handshake ครั้งที่ 2 หรือจังหวะ SYN/ACK จะเห็นว่า Flags = 0x012

มีเลข 1 โผล่มาอยู่ 2 ที่ คือ การ Handshake ครั้งที่ 2 ของ TCP Segment เอง



จะเห็นว่า ค่า sequence number บอกถึง three way handshake ด้วย

Host a (เรา) จะเริ่ม SYN จะมี SEQ = 0 ACK = 0

Host b (gmail) จะ SYN/ACK จะมี SEQ = 0 ACK = 1

Host a (เรา) จะ ACK จะมี SEQ = 1 ACK = 1