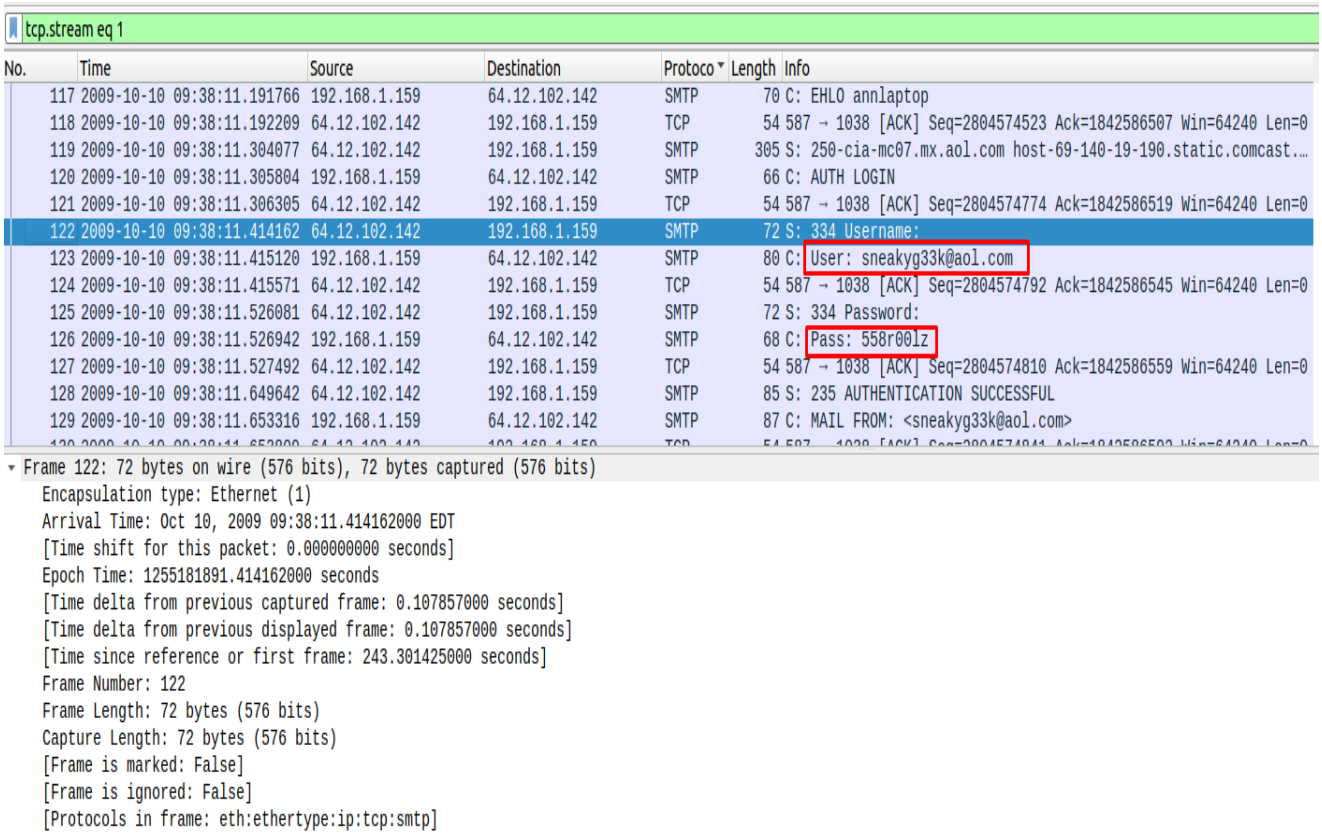
BİL420/BİL520 Siber Güvenliğe Giriş

1. What is Ann’s e-mail address?



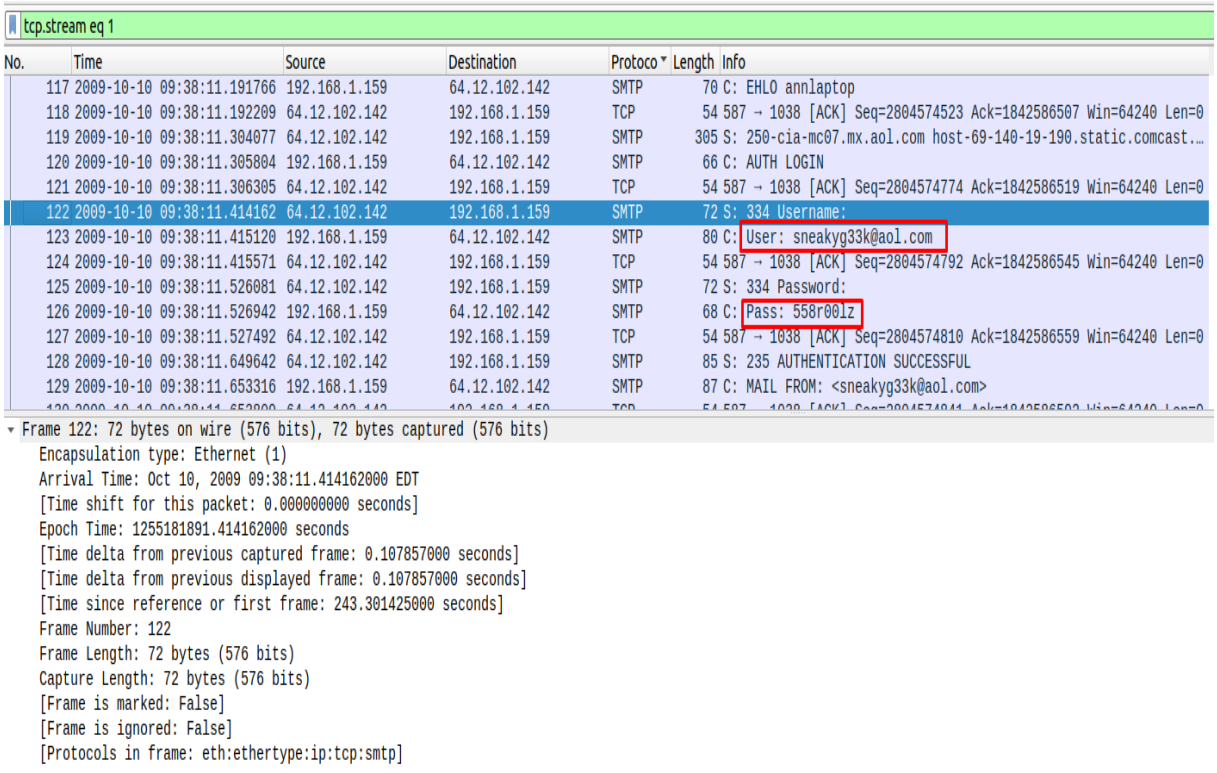
tcp.stream eq 1

No.	Time	Source	Destination	Protoco	Length	Info
117	2009-10-10 09:38:11.191766	192.168.1.159	64.12.102.142	SMTP	70	C: EHLO annlaptop
118	2009-10-10 09:38:11.192209	64.12.102.142	192.168.1.159	TCP	54	587 → 1038 [ACK] Seq=2804574523 Ack=1842586507 Win=64240 Len=0
119	2009-10-10 09:38:11.304077	64.12.102.142	192.168.1.159	SMTP	305	S: 250-cia-mc07.mx.aol.com host-69-140-19-190.static.comcast.…
120	2009-10-10 09:38:11.305804	192.168.1.159	64.12.102.142	SMTP	66	C: AUTH LOGIN
121	2009-10-10 09:38:11.306305	64.12.102.142	192.168.1.159	TCP	54	587 → 1038 [ACK] Seq=2804574774 Ack=1842586519 Win=64240 Len=0
122	2009-10-10 09:38:11.414162	64.12.102.142	192.168.1.159	SMTP	72	S: 334 Username:
123	2009-10-10 09:38:11.415120	192.168.1.159	64.12.102.142	SMTP	80	C: User: sneakyg33k@aol.com
124	2009-10-10 09:38:11.415571	64.12.102.142	192.168.1.159	TCP	54	587 → 1038 [ACK] Seq=2804574792 Ack=1842586545 Win=64240 Len=0
125	2009-10-10 09:38:11.526081	64.12.102.142	192.168.1.159	SMTP	72	S: 334 Password:
126	2009-10-10 09:38:11.526942	192.168.1.159	64.12.102.142	SMTP	68	C: Pass: 558r00lz
127	2009-10-10 09:38:11.527492	64.12.102.142	192.168.1.159	TCP	54	587 → 1038 [ACK] Seq=2804574810 Ack=1842586559 Win=64240 Len=0
128	2009-10-10 09:38:11.649642	64.12.102.142	192.168.1.159	SMTP	85	S: 235 AUTHENTICATION SUCCESSFUL
129	2009-10-10 09:38:11.653316	192.168.1.159	64.12.102.142	SMTP	87	C: MAIL FROM: <sneakyg33k@aol.com>

```
▾ Frame 122: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 10, 2009 09:38:11.414162000 EDT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1255181891.414162000 seconds
    [Time delta from previous captured frame: 0.107857000 seconds]
    [Time delta from previous displayed frame: 0.107857000 seconds]
    [Time since reference or first frame: 243.301425000 seconds]
    Frame Number: 122
    Frame Length: 72 bytes (576 bits)
    Capture Length: 72 bytes (576 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:smtp]
```

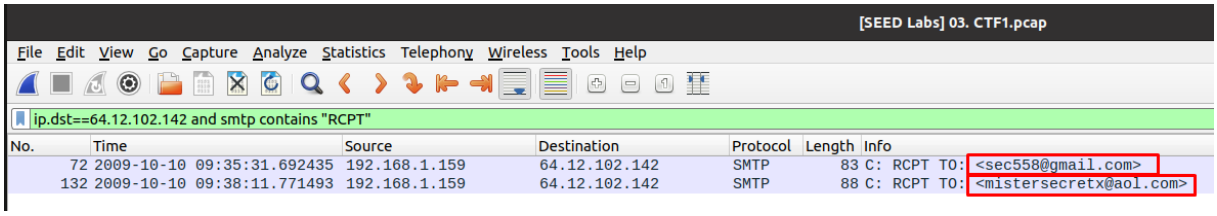
Ann’s mail address is sneakyg33k@aol.com

2. What is Ann’s e-mail password?



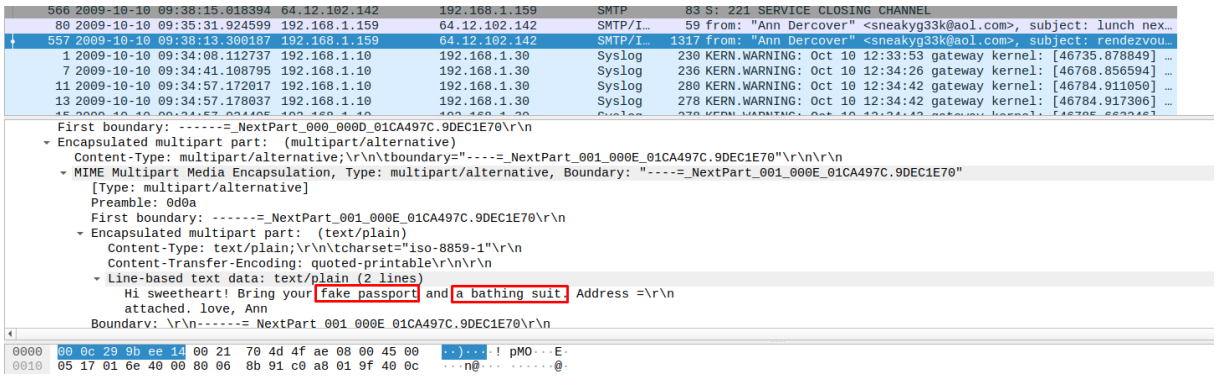
Ann's password is 558r00lz

3. What are the e-mail addresses that Ann sent e-mail?



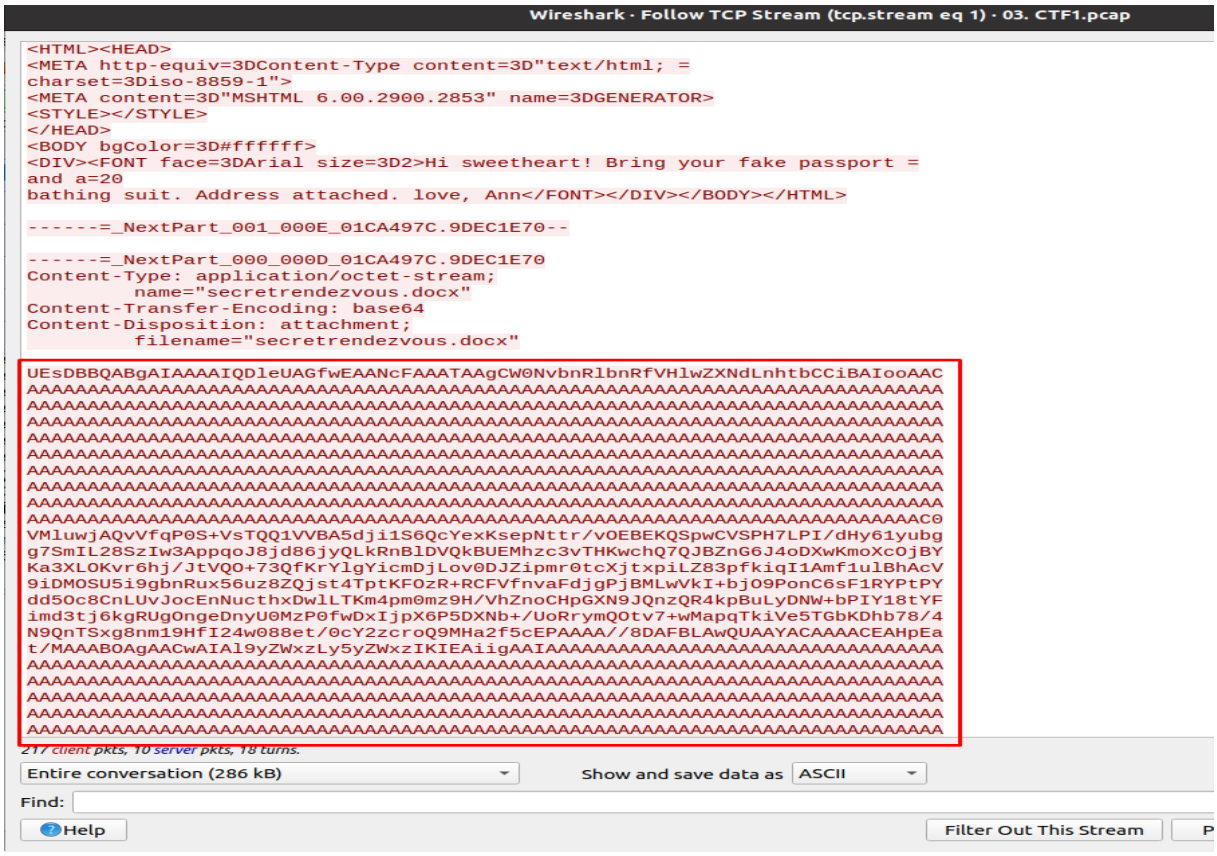
Addresses are sec558@gmail.com and mistersecretx@aol.com

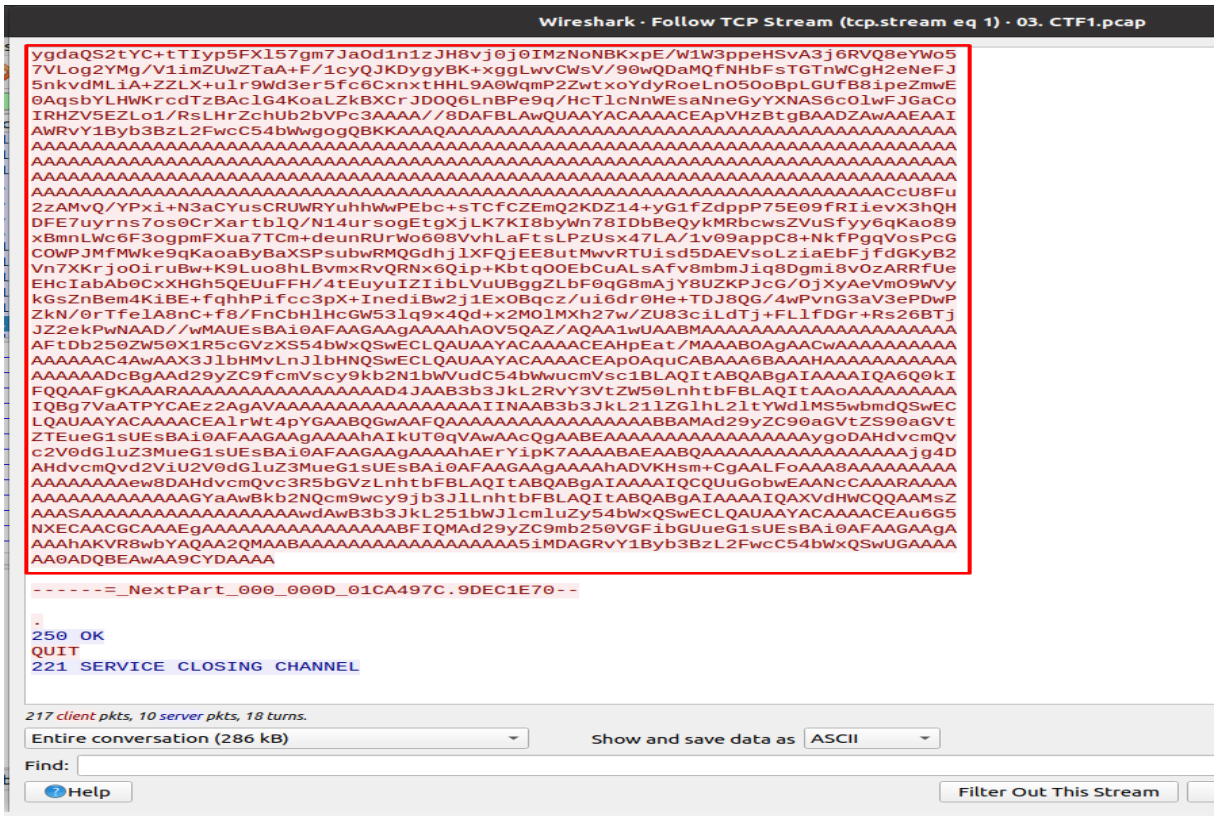
4. What are the two things Ann requested from her friend to bring?



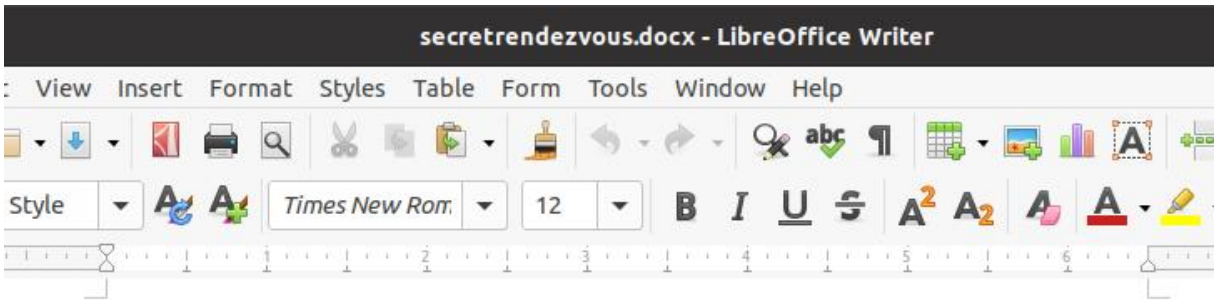
Two things are "your fake passport" and "a bathing suit".

5. Which country is the meeting place according to the attached document?

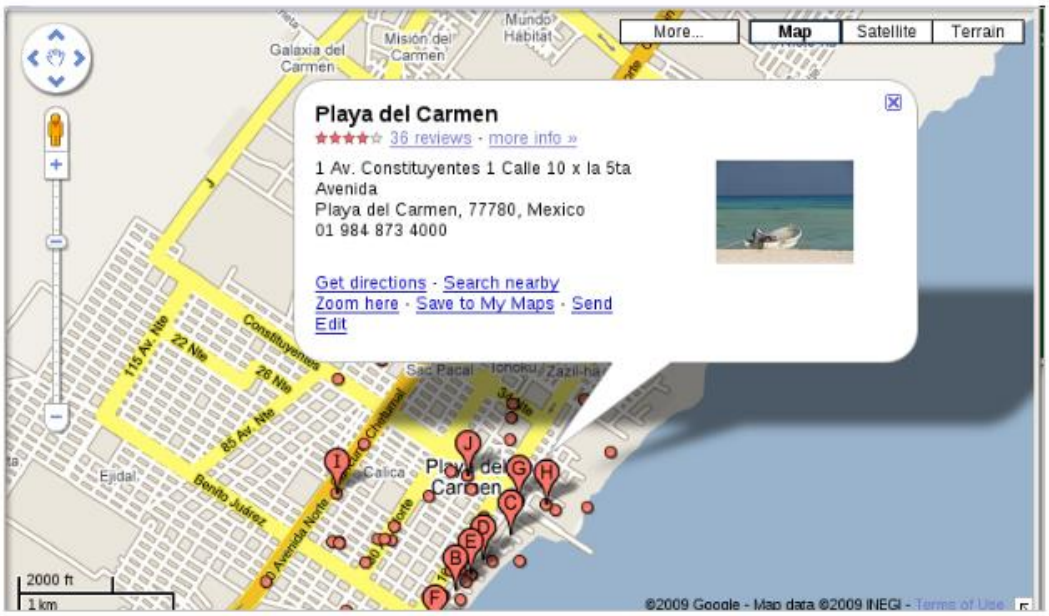




Kırmızı kare işaretli alanın başından sonuna kadar decode from base64 yapıp docx uzantılı bir dosya oluşturmamız gerekiyor gerçek dosya içeriğine ulaşabilmek için

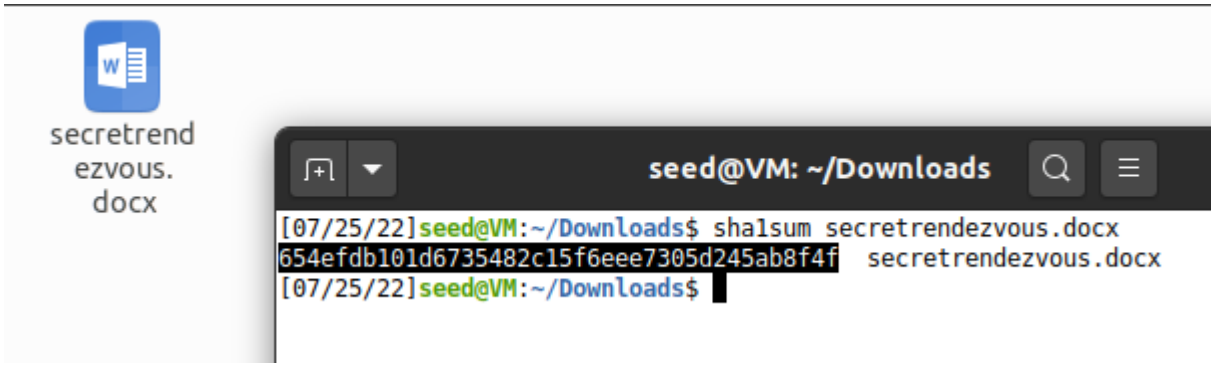


Meet me at the fountain near the rendezvous point. Address below. I'm bringing all the cash.



Buluşma yeri yukarda gözüktüğü gibidir.

6. What is the SHA1 value of the file sent as an e-mail attachment?



SHA1 value is "654efdb101d6735482c15f6eee7305d245ab8f4f"