Ann Skips Bail

After being released on bail, Ann Dercover disappears! Fortunately, investigators were carefully monitoring her network activity before she skipped town.

"We believe Ann may have communicated with her secret lover, Mr. X, before she left," says the police chief. "The packet capture may contain clues to her whereabouts."

You are the forensic investigator. Your mission is to figure out what Ann emailed, where she went, and recover evidence including:

1. What is Ann's email address?

Answer: Ann's email address captured from the packet is "sneakyg33k@aol.com".

2. What is Ann's email password?

Answer: Ann's email password captured from the packet is "**NTU4cjAwbHo=**" (Base64 encoded) which was decoded to human readable format "**558r00lz**".

3. What is Ann's secret lover's email address?

Answer: Ann's secret lover's email address captured from the packet is "**c25lYWt5ZzMza0Bhb2wuY29t**" (Base64 encoded) which was decoded to human readable format "mistersecretx@aol.com". Also, there is one another email address captured during the analysis of the packet. The email address is "sec558@gmail.com" and it is also coming from the same IP address (**64.12.102.142**) as of the email "mistersecretx@aol.com".

4. What two items did Ann tell her secret lover to bring?

Answer: The 2 item Ann asked her lover to get was a "**fake passport**" and "**bathing suit**". (Information acquired from Packet 557)

5. What is the NAME of the attachment Ann sent to her secret lover?

Answer: The attachment Ann sent to her lover was a Word document (.docx file) named "**secretrendezvous.docx**" (Information acquired from Packet 557)

6. What is the MD5sum of the attachment Ann sent to her secret lover?

Answer: The MD5 sum of the attached document is "**9e423e11db88f01bbff81172839e1923**"

```
C:\>certutil -hashfile E:\UBalt_Assignment\CYFI-620\secretrendezvous.docx MD5
MD5 hash of E:\UBalt_Assignment\CYFI-620\secretrendezvous.docx:
9e423e11db88f01bbff81172839e1923
CertUtil: -hashfile command completed successfully.
```

7. In what CITY and COUNTRY is their rendezvous point?

Answer: The rendezvous point was a city named "**Playa del Carmen**" located in "**Mexico**".

8. What is the MD5sum of the image embedded in the document?

Answer: The MD5 sum of the image embedded in document is "**aadeace50997b1ba24b09ac2ef1940b7**"

```
C:\>certutil -hashfile E:\UBalt_Assignment\CYFI-620\word\media\image1.png MD5
MD5 hash of E:\UBalt_Assignment\CYFI-620\word\media\image1.png:
aadeace50997b1ba24b09ac2ef1940b7
CertUtil: -hashfile command completed successfully.
```

MD5 (evidence02.pcap) = cfac149a49175ac8e89d5b5b5d69bad3

- By Mohit Dhabuwala
mohit.dhabuwala@ubalt.edu