**그래픽, 클립아트, 그림, 디자인이(가) 표시된 사진

자동 생성된 설명**

**[Ann Skips Bail] Write-Up**

|  |  |
| --- | --- |
| **작성자** | 김서영 |
| **분석 일자** | 2024.05.15. |
| **작성 일자** | 2024.05.17~2024.05.18. |
| **분석 대상** | evidence02.pcap |
| **문서 버전** | 1 |
| **작성자 E-mail** | [sykim1802@naver.com](mailto:sykim1802@naver.com) |

1. **목차**

[**1.** **문제** 3](#_Toc165902295)

[**2.** **분석 도구** 3](#_Toc165902296)

[**3.** **환경** 3](#_Toc165902297)

[**4.** **Write-Up** 4](#_Toc165902298)

[**5.** **Flag** 10](#_Toc165902299)

[**6.** **별도 첨부** 11](#_Toc165902300)

[**7.** **Reference** 12](#_Toc165902301)

# **문제**

|  |  |
| --- | --- |
| **URL** | [Puzzle #2: Ann Skips Bail – Network Forensics Puzzle Contest (forensicscontest.com)](https://forensicscontest.com/2009/10/10/puzzle-2-ann-skips-bail) |
| **문제**  **내용** | 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: |
| **문제**  **파일** |  |
| **문제**  **유형** | Network forensics |
| **난이도** | 2 / 5 |

# **분석 도구**

|  |  |  |
| --- | --- | --- |
| **도구명** | **다운로드 링크** | **Version** |
| Wireshark | [Wireshark · Download](https://www.wireshark.org/download.html) | 4.2.4 x64 |
| HxD | [HxD - Freeware Hex Editor and Disk Editor | mh-nexus](https://mh-nexus.de/en/hxd/) | 2.5.0.0 |
|  |  |  |

# **환경**

|  |
| --- |
| **OS** |
| Windows11 x64 |

# **Write-Up**

|  |  |
| --- | --- |
| **파일명** | evidence02.pcap |
| **용량** | 328kb |
| **SHA256** | 290f495df4d30038e0db638ac9a0ee24afd9c708acbf1bd86bec9f0c45fc061c |
| **Timestamp** | ‎2024-05-15 13:54:35 |

1. What is Ann’s email address?

2. What is Ann’s email password?

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

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

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

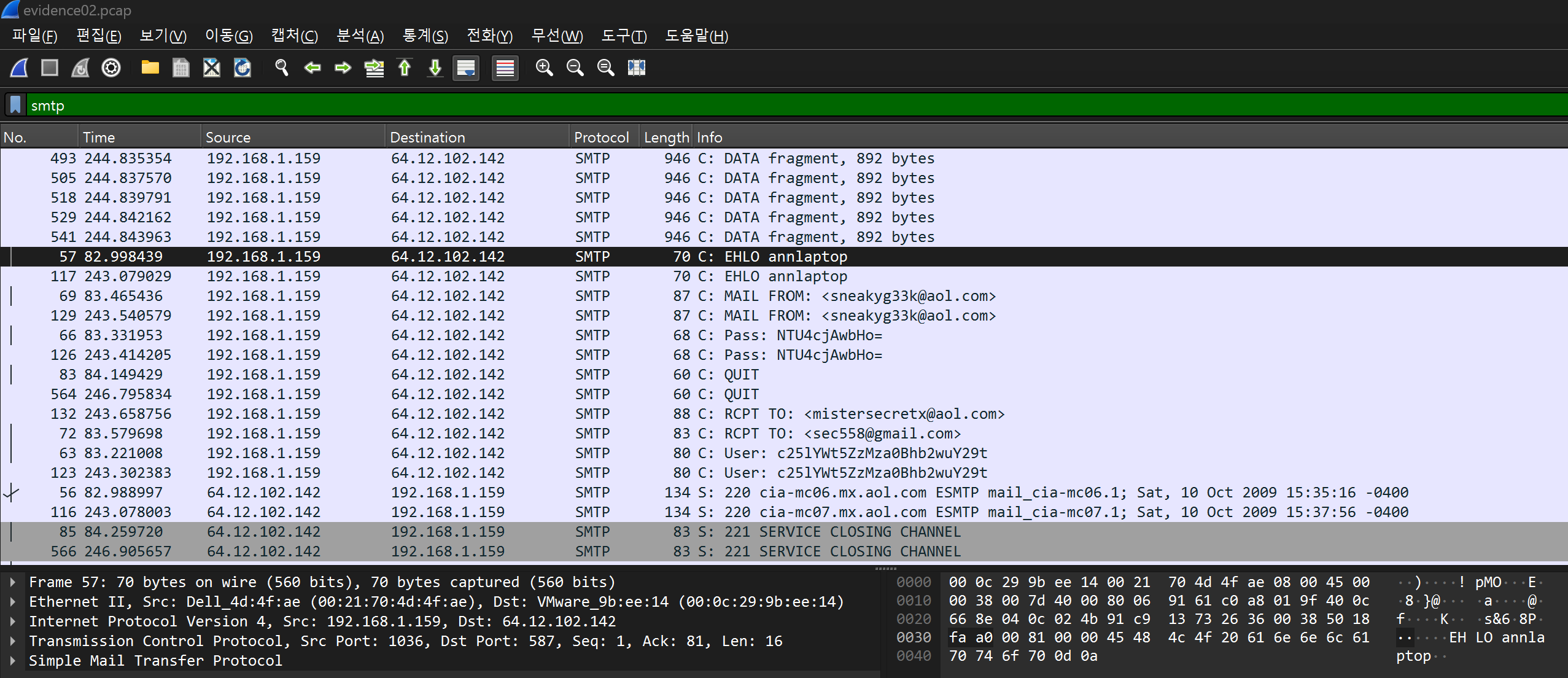
6. What is the MD5sum of the attachment Ann sent to her secret lover?

7. In what CITY and COUNTRY is their rendez-vous point?

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

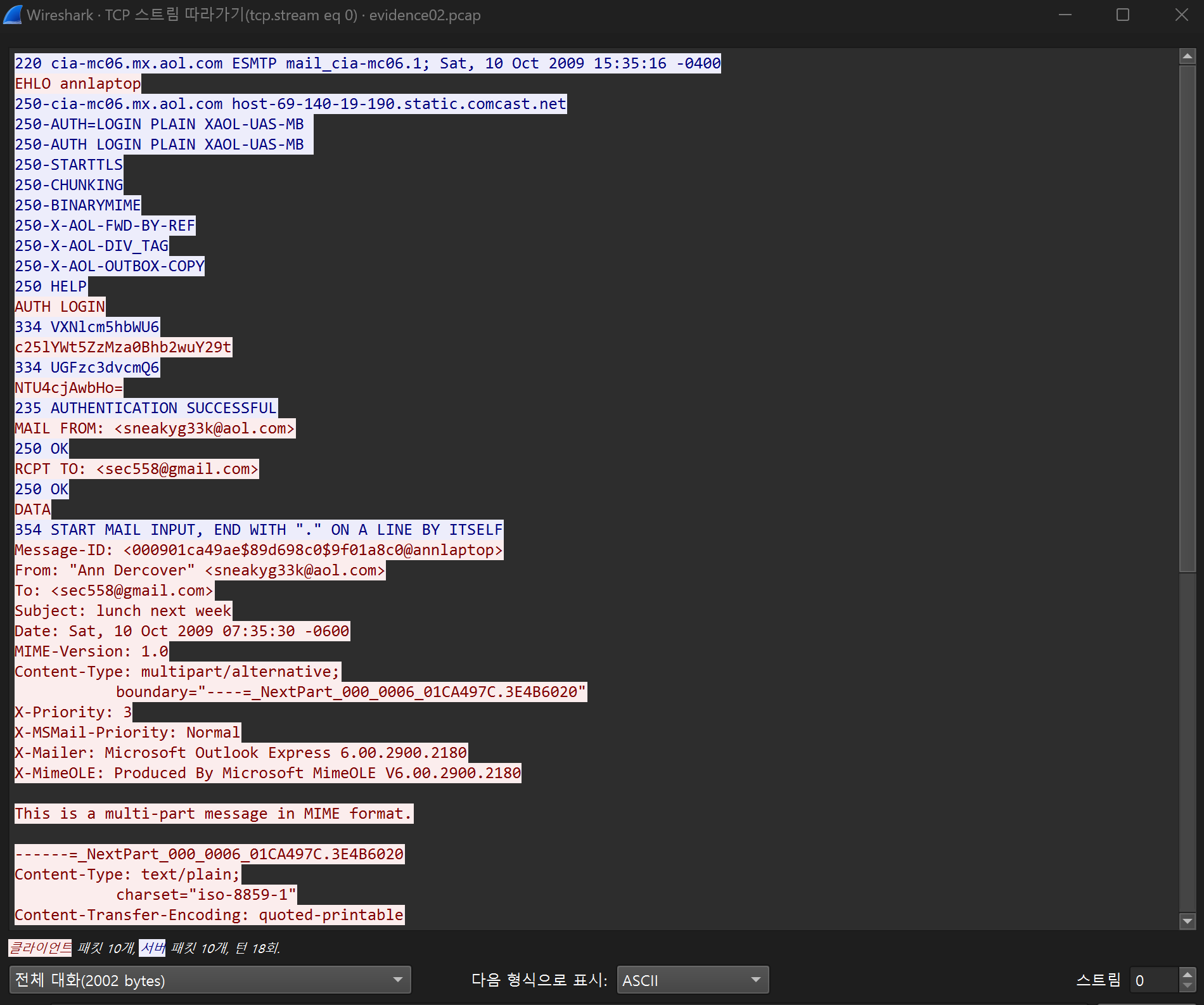
문제 내용에서 Ann의 이메일 활동에 대해 물어보고 있다.

이메일을 전송할 때는 SMTP(Simple Mail Transfer Protocol, 단순 메일 전송 프로토콜)을 이용한다. 따라서 Wireshark에서 evidence.pcap를 연 후 SMTP만 검색해보았다.

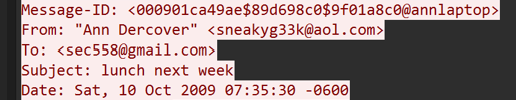


[사진 1] SMTP 검색

[사진 1]에서 선택된 패킷을 따라가기-tcp 스트림으로 열어보았다.

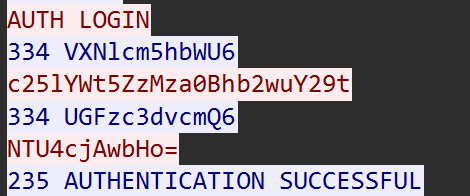


[사진 2] tcp 스트림(1)



[사진 3] 이메일 수신자, 발신자, 내용, 발신 일자

1. [사진 3]에서 발신자 Ann의 이메일 주소는 sneakyg33k@aol.com임을 알 수 있다.



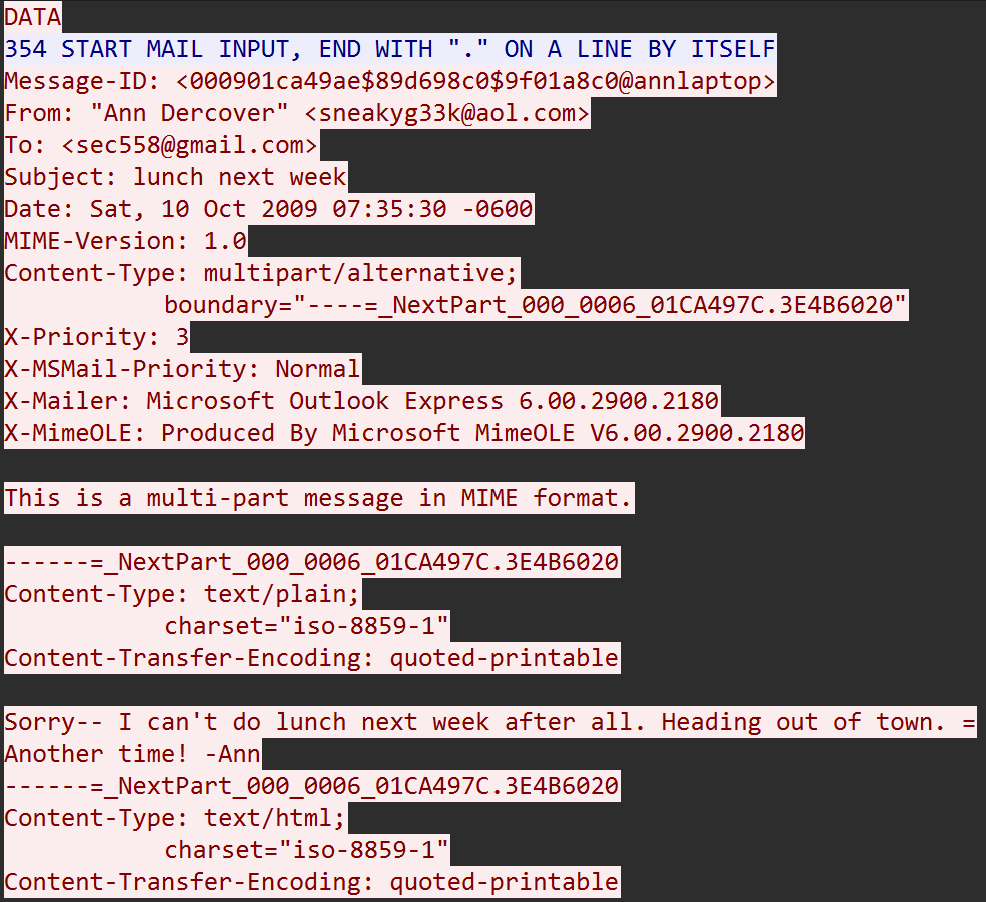
[사진 4] 로그인 흔적

2. [사진 4]에서 위쪽엔 LOGIN과 아래엔 Authentication Successful이 있는 것을 보고 로그인이 성공적으로 이루어졌음을 알려주는 패킷이라고 생각했다.



[사진 5] base64 decoder 결과([Base64 디코딩 및 인코딩 - 온라인 (base64decode.org)](https://www.base64decode.org/ko/))

Base64 decoder에 디코딩한 결과, Ann의 이메일 비밀번호는 558r00lz임을 알아냈다.

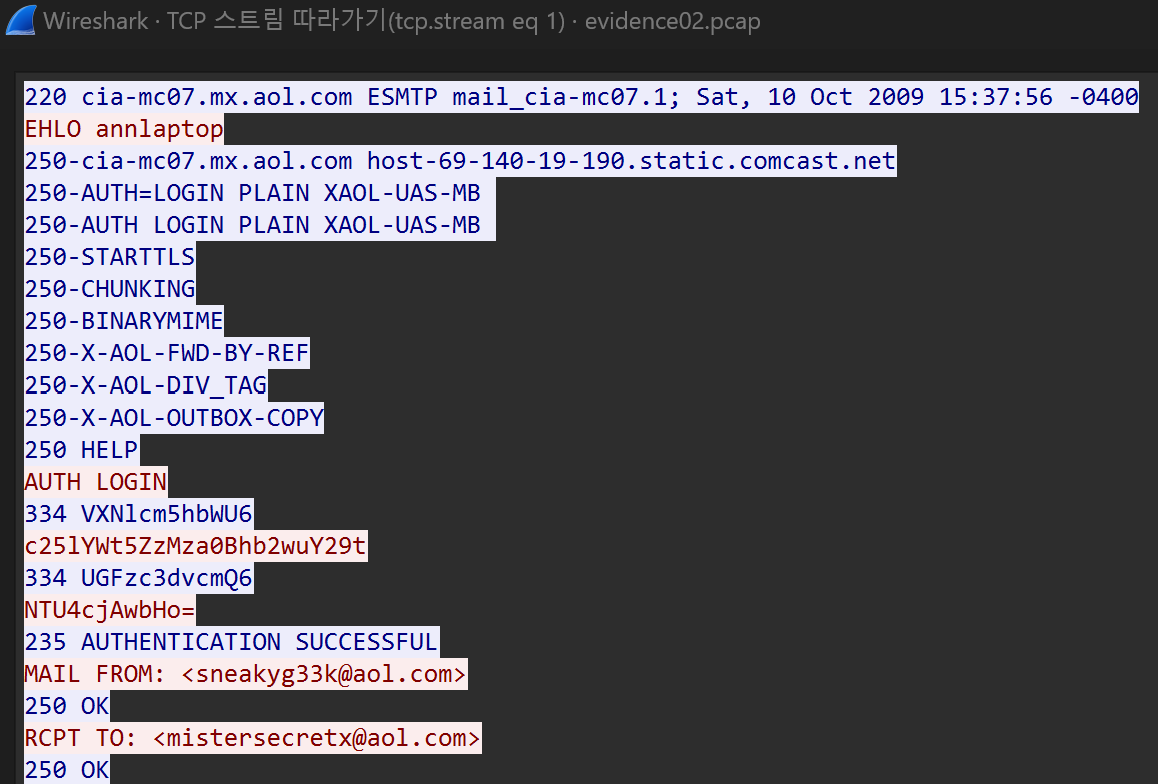


[사진 6] 수신자 sec558에게 보낸 이메일 내용

3. 처음에 수신자 sec558@gmail.com을 Ann의 비밀애인이라고 생각했다.

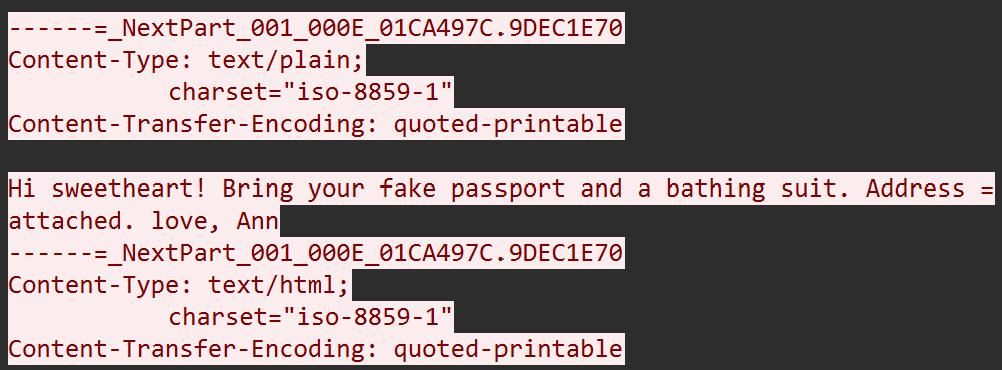
하지만, 이메일 내용이 다음주 점심 약속을 취소하자는 얘기였다.

애인 사이의 대화라고 생각하기에 확신이 서지 않아 다른 TCP 스트림이 존재하는지 찾아보았다.



[사진 7] tcp 스트림 (2)

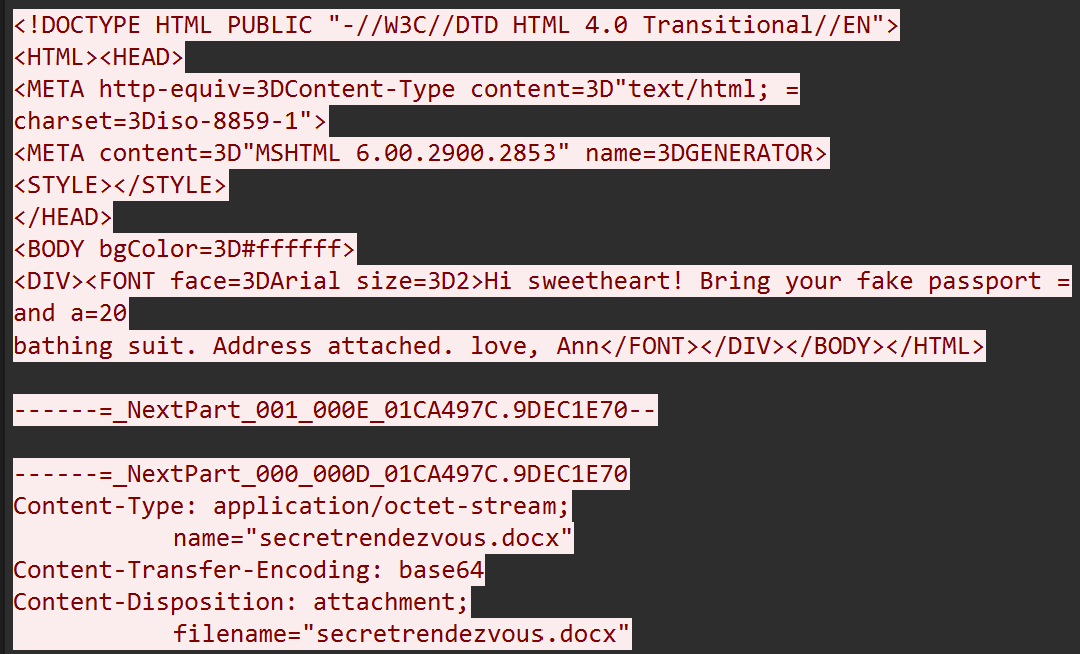
또 다른 tcp 스트림을 찾았고, 수신자의 이메일이 mistersecret@aol.com으로 달랐다.



[사진 8] 수신자 mistersecret에게 보낸 이메일 내용

mistersecret@aol.com에게 보낸 내용의 시작에서 수신자를 “sweetheart”라고 지칭하는 것으로 보아, [사진 6] 속의 이메일 수신자 sec558@gmail.com보다 mistersecret@aol.com이 유력하게 비밀애인이라고 볼 수 있었다.

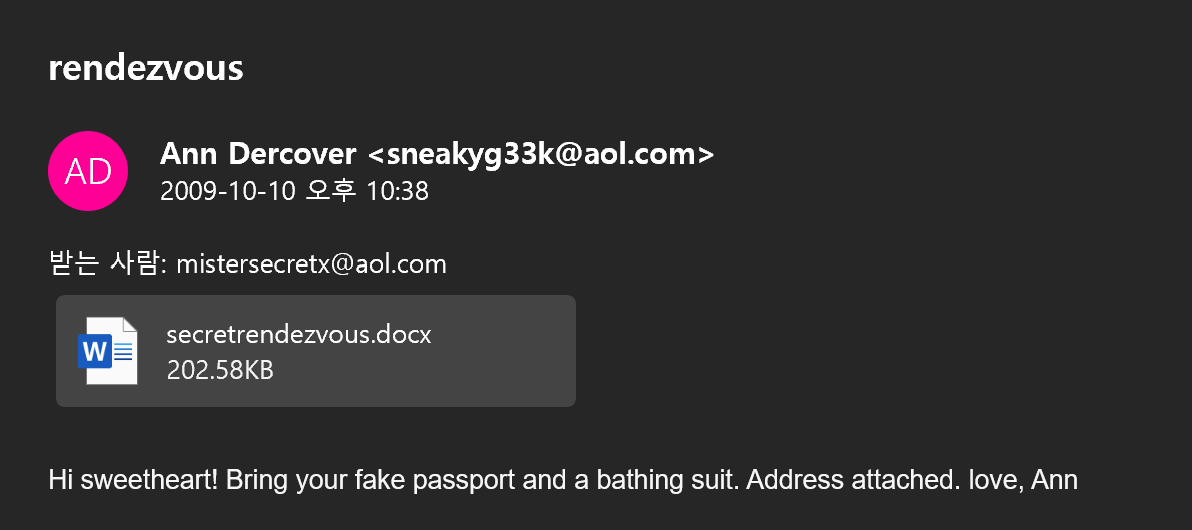
4. 또한, [사진 8]에서 Ann이 그에게 fake passport와 a bathing suit를 가져오라고 했음을 알 수 있었다.



[사진 9] attachment의 파일 이름

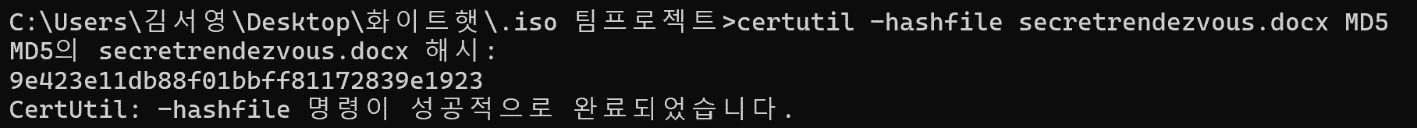
5. [사진 7]의 tcp 스트림을 아래로 내려보니 이메일에 첨부되어 있는 attachment의 파일 이름은 secretrendezvous.docx임을 찾을 수 있었다.

6. Tcp 스트림 창으로 얻을 수 있는 정보가 더 이상 없다고 판단하여, 해당 패킷을 raw 형태로 변환 후 확장자명 .eml로 저장했다. 이렇게 하면 이메일 프로그램에서 열어볼 수 있기 때문이다.



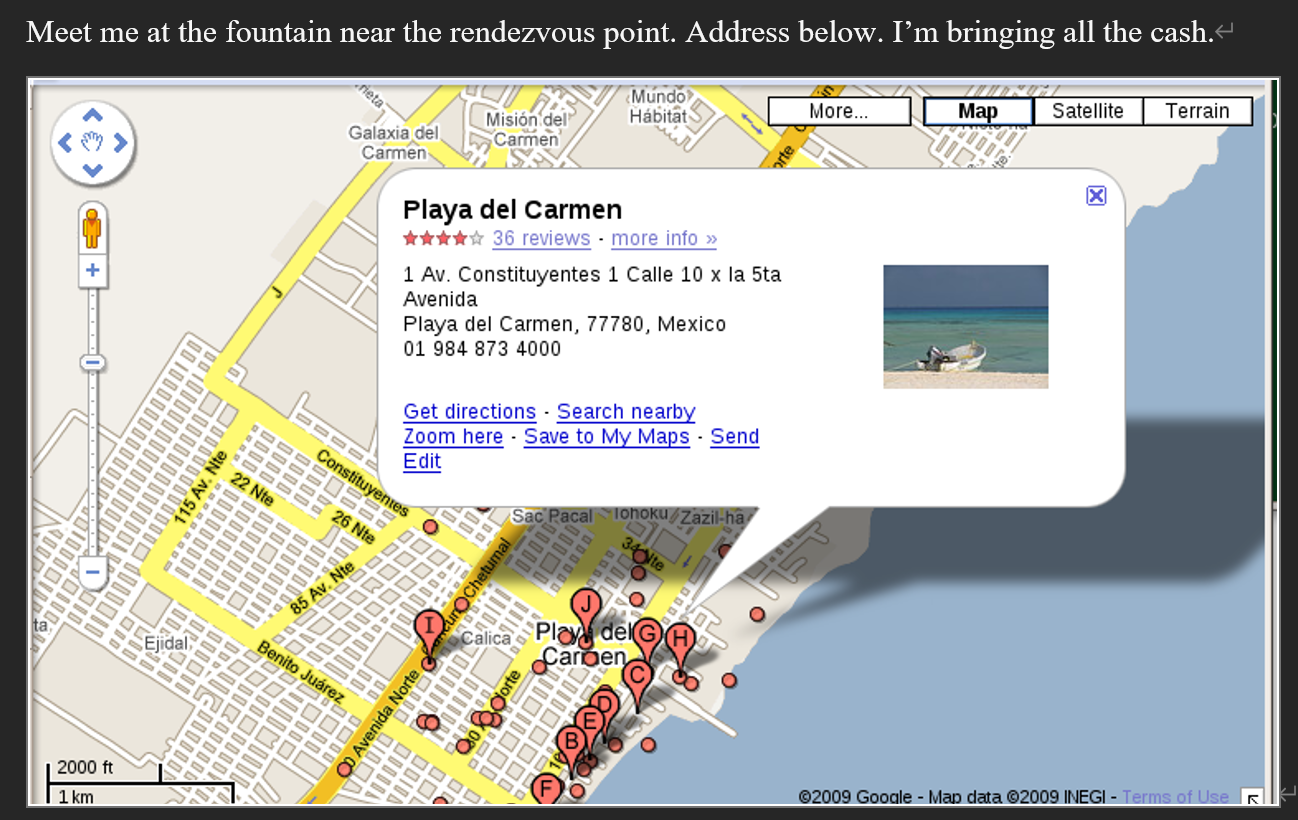
[사진 10] sans02.eml로 저장 후 열린 이메일

sans02.eml로 저장하니 secretrendezvous.docx파일을 열고 저장할 수 있었다.



[사진 11] secretrendezvous.docx의 MD5 값

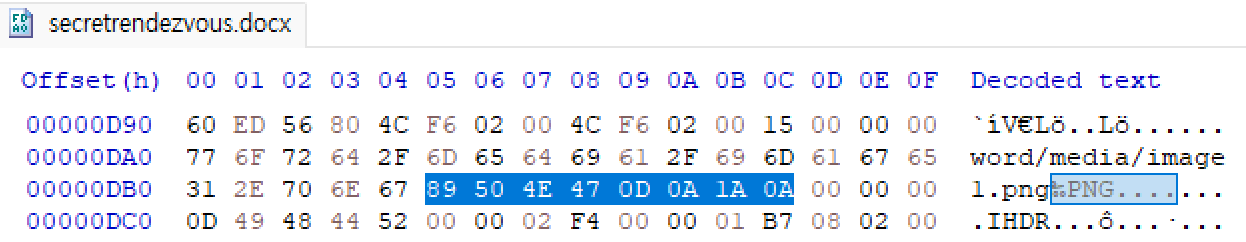
secretrendezvous.docx를 다운 받아 cmd창에서 MD5값을 구하였다.



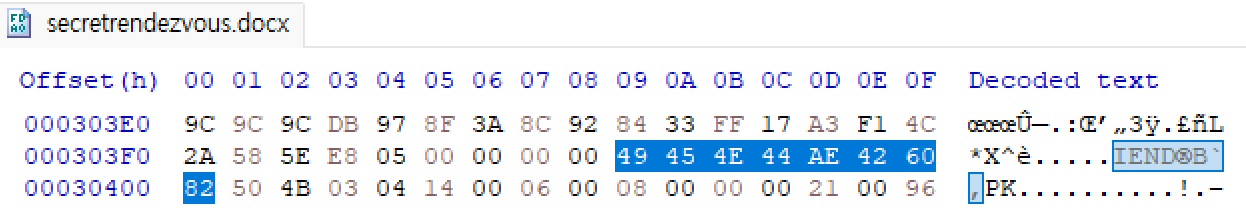
[사진 12] secretrendezvous.docx 내용

7. Ann과 비밀 애인의 rendezvous point의 주소를 확인했다.

8. 마지막으로, secretrendezvous.docx 내 이미지 파일의 MD5값을 구하기 위해 HxD로 docx파일을 연 후 PNG 헤더 시그니처와 푸터 시그니처를 찾았다.

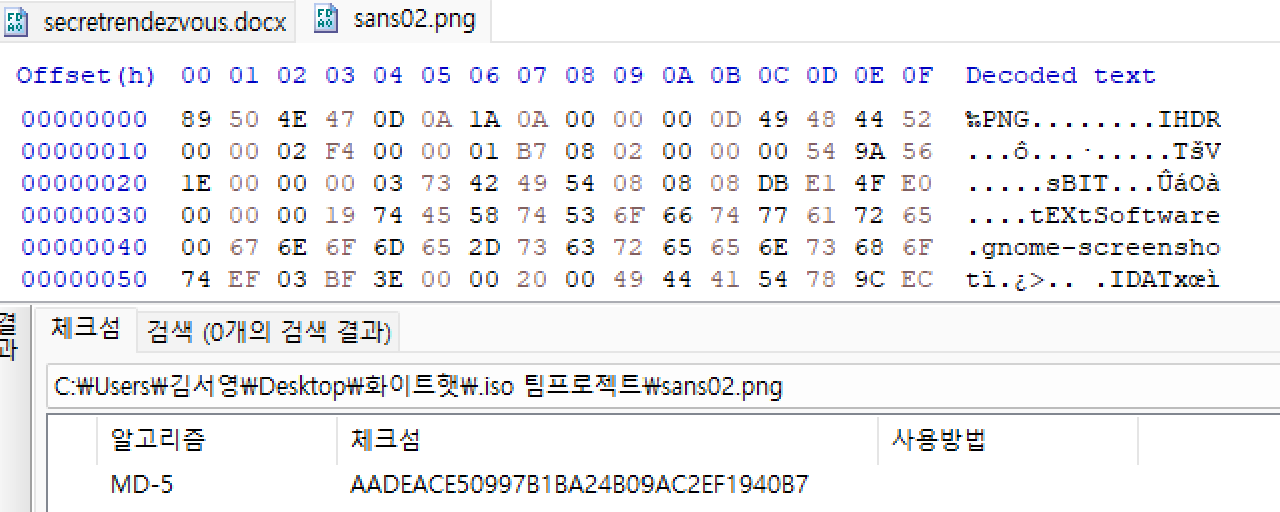


[사진 13] PNG파일의 헤더 시그니처



[사진 14] PNG파일의 푸터 시그니처

파일 시그니처를 바탕으로PNG파일에 해당되는 블록만 선택하여 다시 저장한 후 HxD로 MD5값을 확인하였다.



[사진 15] PNG파일의 MD5값

# **Flag**

1. What is Ann’s email address? - sneakyg33k@aol.com

2. What is Ann’s email password? - 558r00lz

3. What is Ann’s secret lover’s email address? - mistersecret@aol.com

4. What two items did Ann tell her secret lover to bring? - fake passport, a bathing suit

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

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

- 9e423e11db88f01bbff81172839e1923

7. In what CITY and COUNTRY is their rendez-vous point? - Playa del Carmen, Mexico

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

- AADEACE50997B1BA24B09AC2EF1940B7

# **별도 첨부**

# **Reference**

* [[네트워크] 응용 계층 (velog.io)](https://velog.io/@gndan4/%EB%84%A4%ED%8A%B8%EC%9B%8C%ED%81%AC-%EC%9D%91%EC%9A%A9-%EA%B3%84%EC%B8%B5)
* [File Signatures (garykessler.net)](https://www.garykessler.net/library/file_sigs.html)