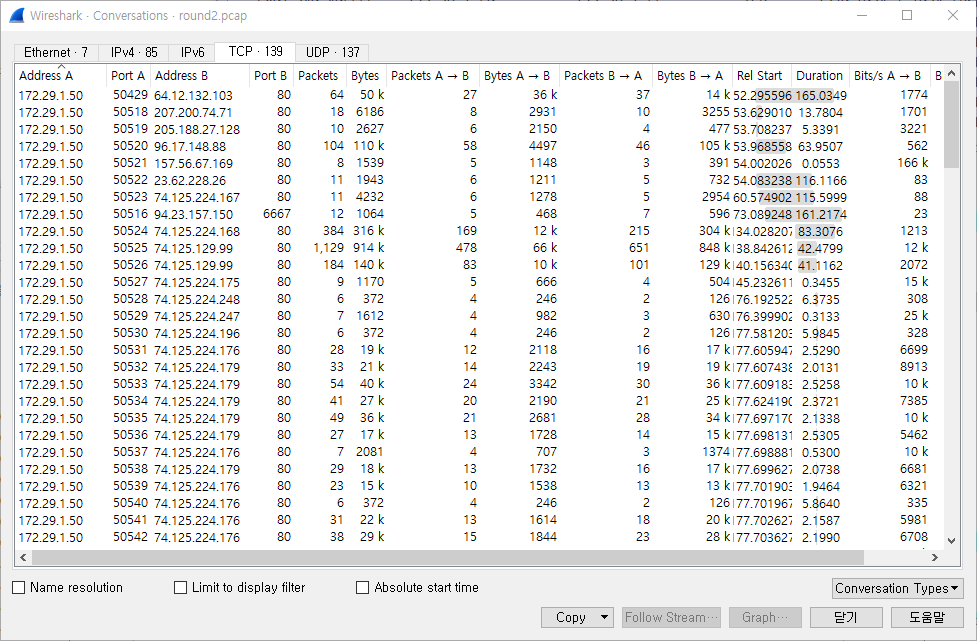
CTF-D.com

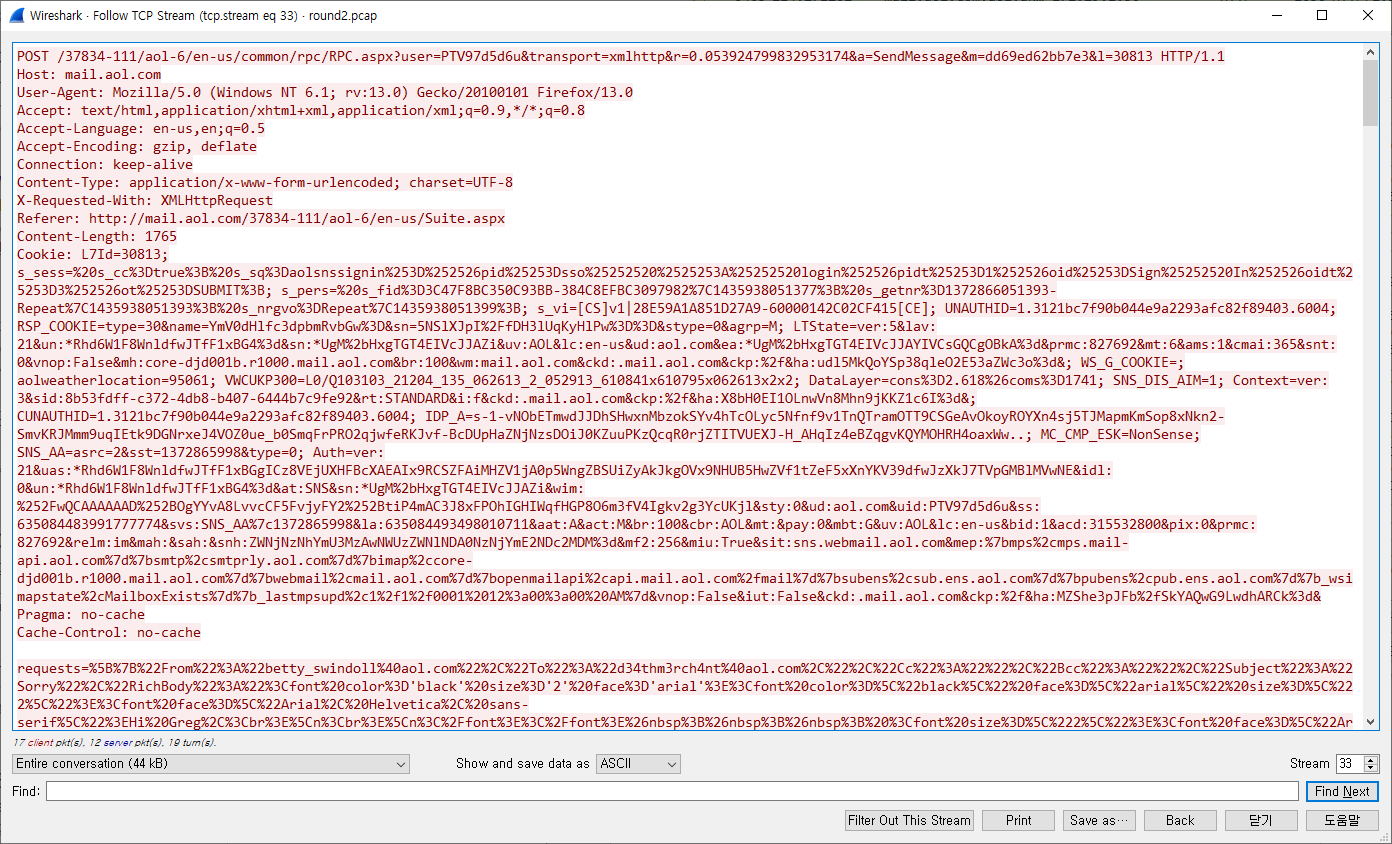
network

2번 문제

1. [Wireshark]-[Statistics]-[Conversations]

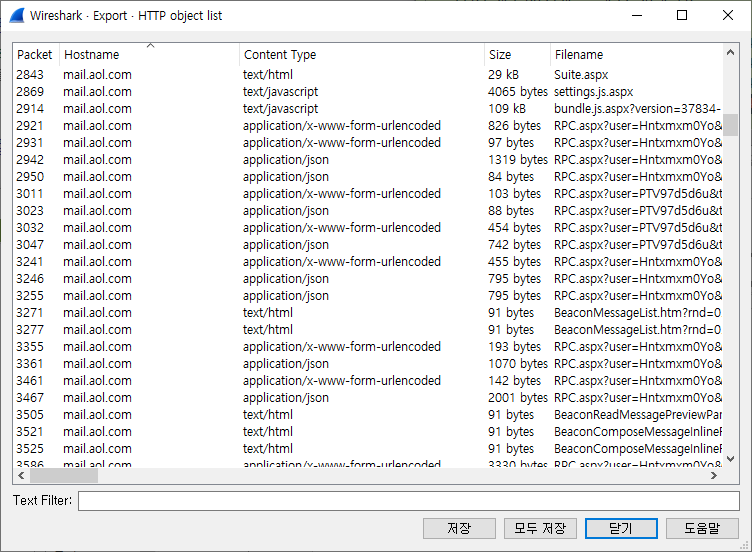


[Follow TCP Stream] 해줘도 몬지 잘 모르겠다.

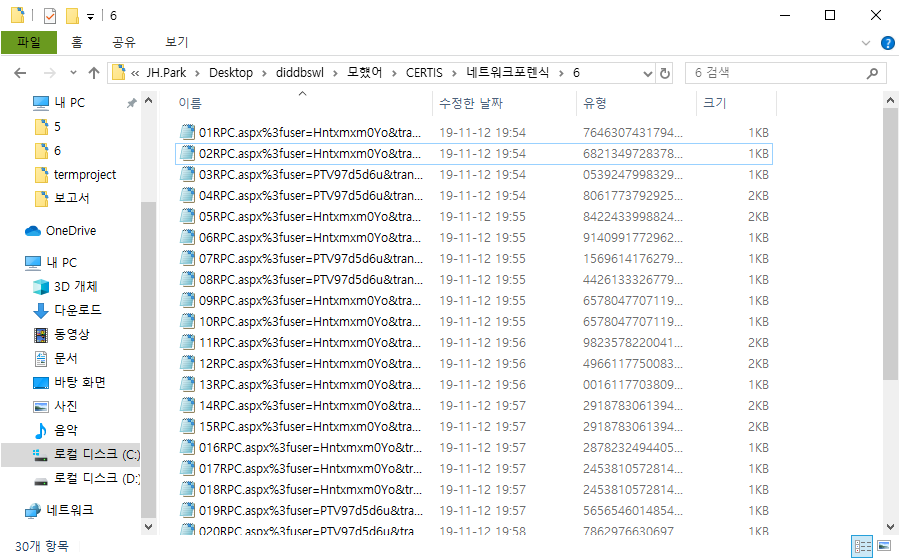


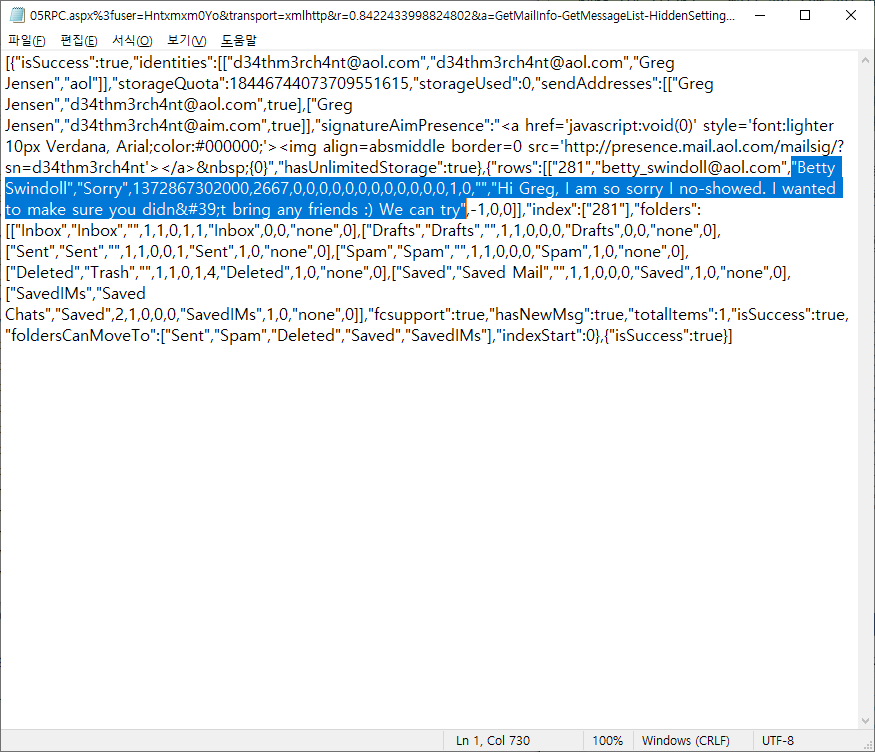
포트 80번으로 통신한 내용이 많다. HTTP를 분석해보자

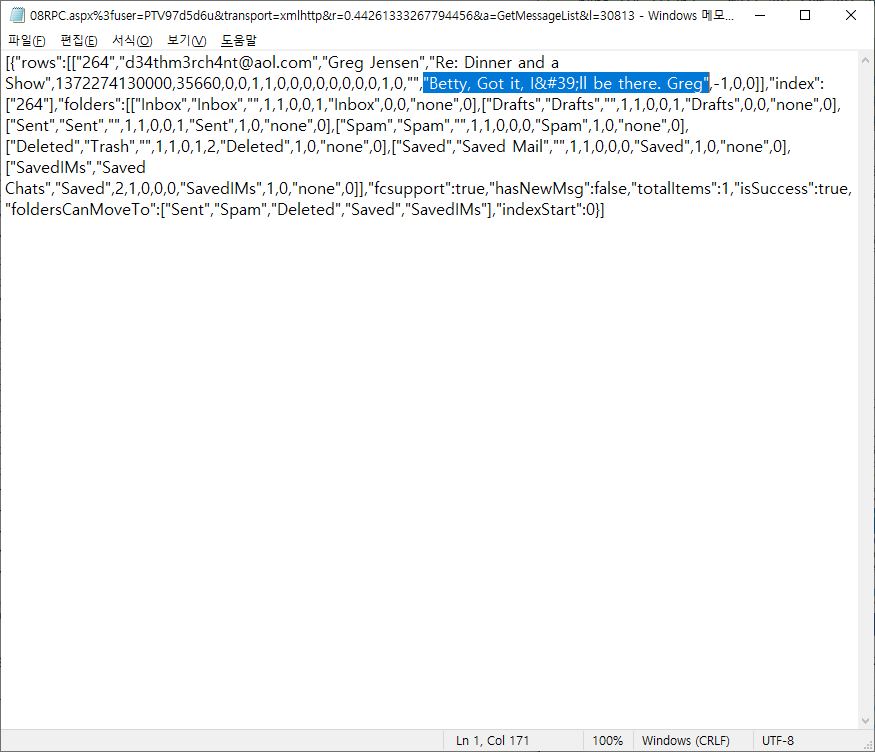
2. [File]-[Export]-[HTTP]

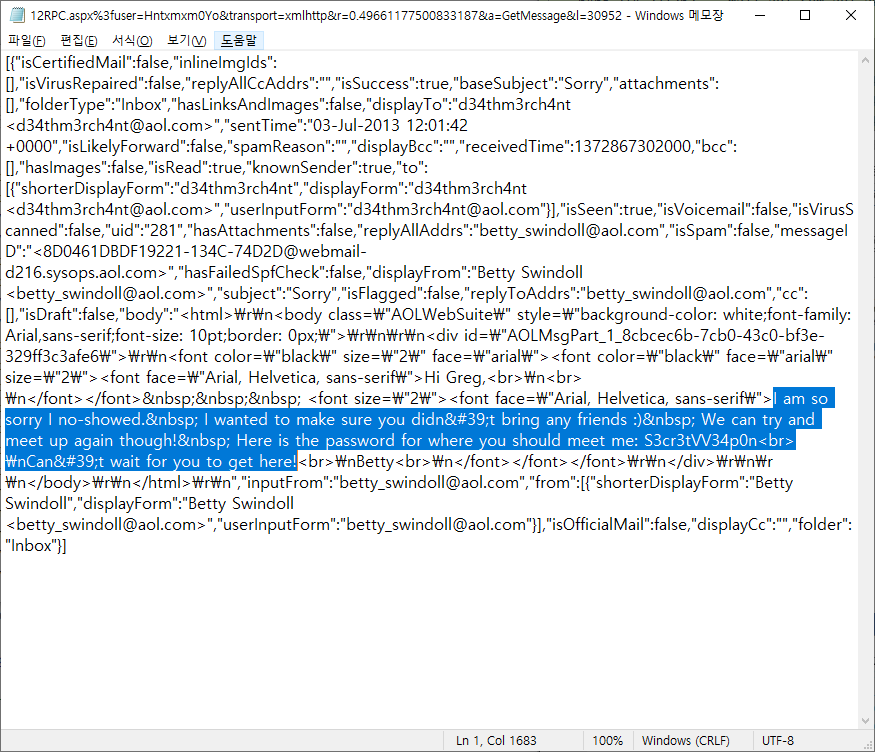


mail.aol.com이 눈에 띄어서 text/html 파일을 다 저장했다.







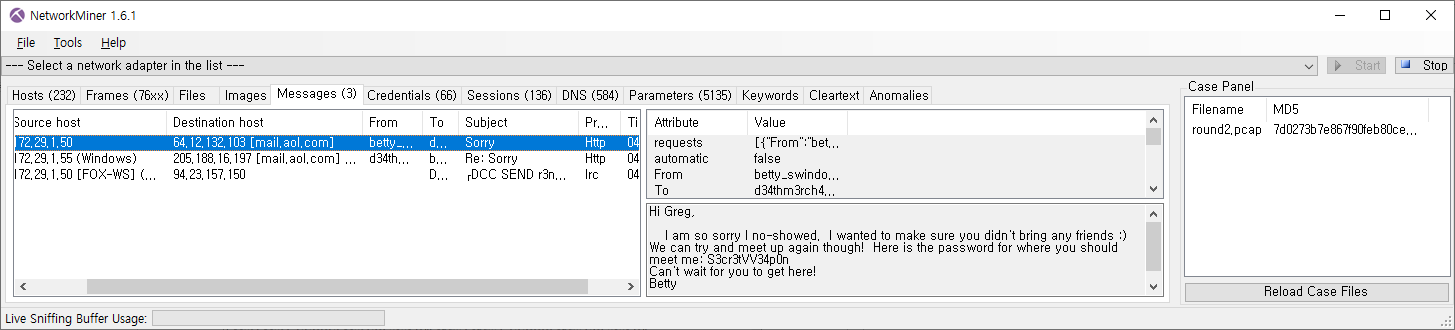


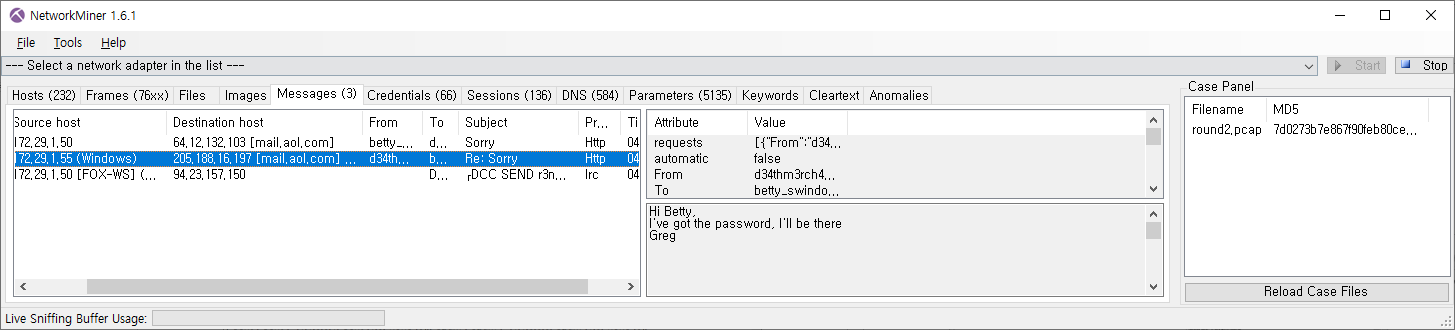
메일을 주고받은 내용이 담긴 파일도 있다. 그 중 만날 장소의 패스워드를 가르쳐주는 메일이 있었다.

Password: S3cr3tVV34p0n

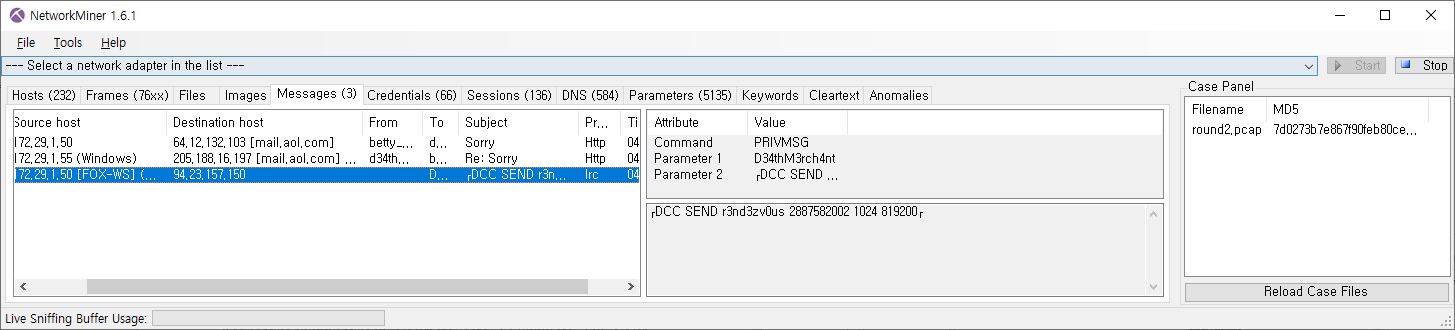
3. 모르겠어서 민혁햄한테 HELP

🡪 NetworkMiner 사용





훨씬 깔끔하게 보인다. 근데 내가 이전에 찾은 정보랑 동일하다.

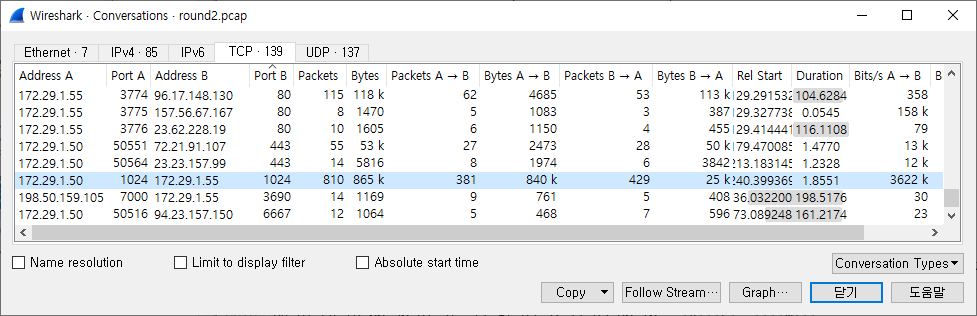


마지막 정보는

DCC SEND r3nd3zv0us 2887582002 1024 819200

DCC SEND <filename> <host> <port>

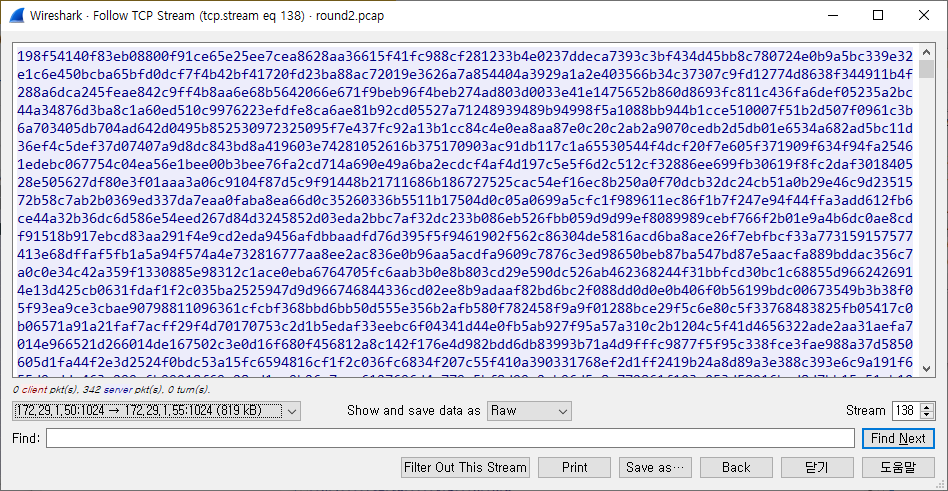
4. port가 1024인 것 찾기



이제 모르겠어서 롸업 봐야겠다

<https://chp747.tistory.com/13>

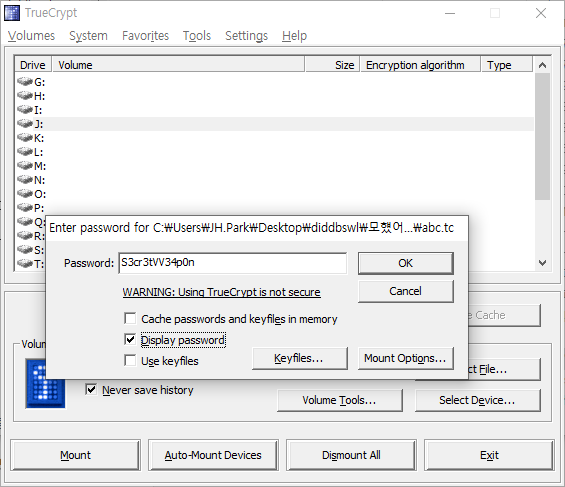
5. 파일 추출해서 분석

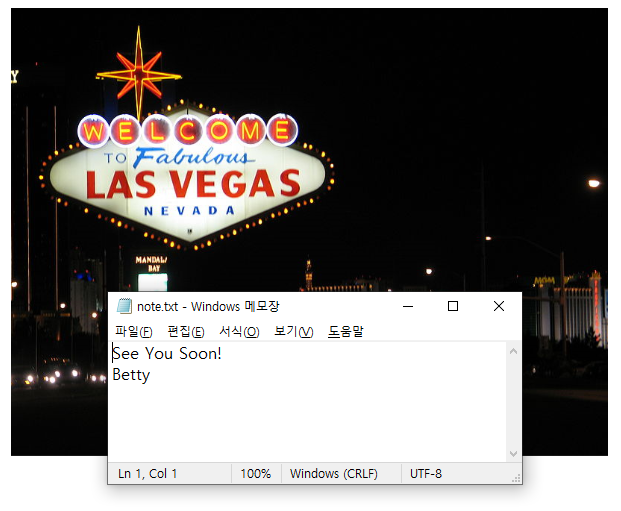


파일 용량을 819kB로 맞추고 추출해준다.

그럼 tc 파일을 얻을 수 있다는데 나는 형식이 없다,,

truecrypt로 파일을 열어준다.





라스베가스 참 좋지

답: LAS VEGAS