

<첫번째>

```
220 cia-mc06.mx.aol.com ESMTP mail_cia-mc06.1; Sat, 10 Oct 2009 15:35:16 -0400

EHLO annlaptop

250-cia-mc06.mx.aol.com host-69-140-19-190.static.comcast.net
250-AUTH=LOGIN PLAIN XAOL-UAS-MB
250-AUTH LOGIN PLAIN XAOL-UAS-MB
250-STARTTLS
250-CHUNKING
250-BINARYMIME
250-X-AOL-FWD-BY-REF
250-X-AOL-DIV_TAG
250-X-AOL-OUTBOX-COPY
250 HELP
```

## 1. 서버 접속

AOL 서버를 통해 이메일을 전송하는 과정을 보여주는 SMTP(단순 메일 전송 프로토콜)이다.

ESMTP : 확장된 SMTP 지원 의미 (기본 SMTP보다 다양한 기능 지원())

EHLO annlaptop : 클라이언트가 서버에 자신을 식별

220 cia-mc06.mx.aol.com ESMTP : 서버가 준비되었음을 나타내는 응답

250-cia-mc06.mx.aol.com host-69-140-19-190.static.comcast.net: 250은 SMTP 명령이 성공적으로 처리되었음을 나타낸다. AOL 서버(해당하는 SMTP 서버)와 클라이언트(Comcast 네트워크의 IP 주소) 사이의 연결이 이루어졌다는 것을 보여준다.

250-AUTH=LOGIN PLAIN XAOL-UAS-MB: 서버는 LOGIN, PLAIN, XAOL-UAS-MB 인증 방법을 지원. 클라이언트는 이 방법 중 하나를 사용하여 인증할 수 있다.

250-STARTTLS: 서버는 STARTTLS 명령을 지원하여 클라이언트와의 통신을 암호화된 세션으로 업그레이드할 수 있다. 이메일 통신의 보안을 강화하는 데 사용.

250-CHUNKING: 서버는 CHUNKING 명령을 지원. 이는 큰 이메일을 여러 조각으로 나눠 전송할 수 있게 하여 효율성을 높인다.

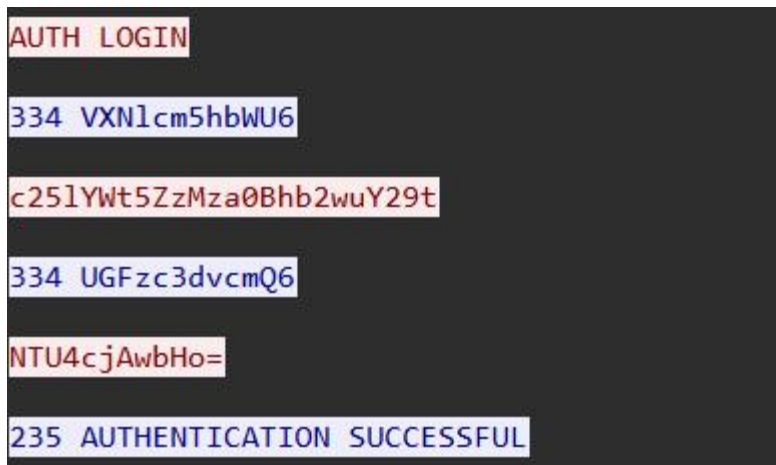
250-BINARYMIME: 이 명령은 이메일의 MIME 메시지를 바이너리 형식으로 전송할 수 있게 한다.

250-X-AOL-FWD-BY-REF: AOL의 특정 기능으로, 메일 전달과 관련된 추가 기능을 지원할 수 있음을 의미

250-X-AOL-DIV\_TAG: AOL 서버에서 이메일을 분류하거나 태그와 관련된 기능을 지원 가능

250-X-AOL-OUTBOX-COPY: 아웃박스에 복사본을 남기는 AOL 고유의 기능을 나타냄

250 HELP: HELP 명령을 사용하면 지원되는 명령 목록이나 서버 관련 도움말을 확인할 수 있다.



2. 서버 접속 계정 및 암호  
email: sneakyg33k@aol.com  
password: 558r00lz

AUTH LOGIN: 클라이언트가 SMTP 서버에 로그인 인증을 시도하기 위해 AUTH LOGIN 명령을 보냄

334 VXNlcm5hbWU6: 서버가 클라이언트에 사용자 이름을 요청하는 응답. VXNlcm5hbWU6는 BASE64로 인코딩된 Username:를 의미

### Base64 형식에서 디코딩

데이터를 입력하고 디코딩 버튼을 누르기만 하면 됩니다.

c25lYWt5ZzZmZa0Bhb2wuY29t

인코딩된 2진수의 경우(이미지, 문서 등), 이 페이지 아래쪽으로 약간 더

UTF-8 소스 문자 세트.

각 행을 개별적으로 디코딩하세요(여러 항목이 있을 때 도움이 됩니다).

라이브 모드 끄기 입력하거나 붙여넣으면서 실시간으로 디코딩

< 디코딩 > 데이터를 아래 영역으로 디코딩합니다.

sneakyg33k@aol.com

### Base64 형식에서 디코딩

데이터를 입력하고 디코딩 버튼을 누르기만 하면 됩니다.

NTU4cjAwbHo=

인코딩된 2진수의 경우(이미지, 문서 등), 이 페이지 아래쪽으로 약간 더 내

UTF-8 소스 문자 세트.

각 행을 개별적으로 디코딩하세요(여러 항목이 있을 때 도움이 됩니다).

라이브 모드 끄기 입력하거나 붙여넣으면서 실시간으로 디코딩합니

< 디코딩 > 데이터를 아래 영역으로 디코딩합니다.

558r00lz

BASE64 인코딩하여 서버에 전송했기 때문에 디코딩하면 실제 이메일 주소와 비밀번호 확인할 수 있다.

```

MAIL FROM: <sneakyg33k@aol.com>

250 OK

RCPT TO: <sec558@gmail.com>

250 OK

DATA

354 START MAIL INPUT, END WITH "." ON A LINE BY ITSELF

Message-ID: <000901ca49ae$89d698c0$9f01a8c0@annlaptop>
From: "Ann Dercover" <sneakyg33k@aol.com>
To: <sec558@gmail.com>
Subject: lunch next week
Date: Sat, 10 Oct 2009 07:35:30 -0600
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="-----_NextPart_000_0006_01CA497C.3E4B6020"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.2180
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180

This is a multi-part message in MIME format.

-----_NextPart_000_0006_01CA497C.3E4B6020
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

```

```

Sorry-- I can't do lunch next week after all. Heading out of town. =
Another time! -Ann
-----_NextPart_000_0006_01CA497C.3E4B6020
Content-Type: text/html;
        charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META http-equiv=3DContent-Type content=3D"text/html; =
charset=3Diso-8859-1">
<META content=3D"MSHTML 6.00.2900.2853" name=3DGENERATOR>
<STYLE></STYLE>
</HEAD>
<BODY bgColor=3D#ffffff>
<DIV><FONT face=3DArial size=3D2>Sorry-- I can't do lunch next week =
after all.=20
Heading out of town. Another time! -Ann</FONT></DIV></BODY></HTML>

-----_NextPart_000_0006_01CA497C.3E4B6020--
.

```

3. 메일전송 (sneakyg33k@aol.com에서 sec558@gmail.com으로 전송)

MAIL FROM: <[sneakyg33k@aol.com](mailto:sneakyg33k@aol.com)>: 클라이언트가 발신자 이메일 주소를 설정. 이 명령은 이메일이 sneakyg33k@aol.com에서 발송될 것임을 알 수 있다.

RCPT TO: <[sec558@gmail.com](mailto:sec558@gmail.com)>: 클라이언트가 수신자 이메일 주소를 설정합니다. 이 명령은 이메일이 sec558@gmail.com으로 전송될 것임을 알 수 있다.

Message-ID: 000901ca49ae\$89d698c0\$9f01a8c0@annlaptop: 이메일의 고유 식별자. 각 이메일에는 고유한 ID가 부여되어 추적 및 식별에 사용

From: "Ann Dercover" [sneakyg33k@aol.com](mailto:sneakyg33k@aol.com): 발신자의 이름과 이메일 주소. 이메일은 Ann Dercover라는 이름으로 sneakyg33k@aol.com에서 발송됨

To: [sec558@gmail.com](mailto:sec558@gmail.com): 수신자의 이메일 주소. 이 이메일은 sec558@gmail.com으로 보내졌다.

Subject: lunch next week: 이메일의 제목. 주제 : "lunch next week"

X-Priority: 3: 이메일의 우선순위. 3은 보통(Normal) 우선순위

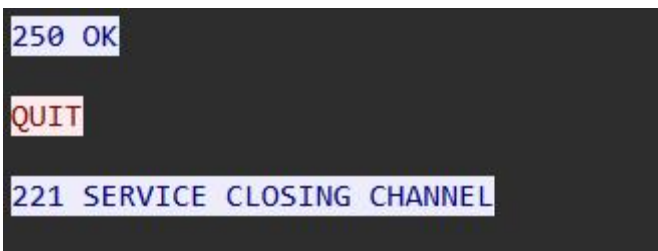
∴ 이메일 본문이 끝났음을 나타내는 단독 마침표

250 OK: 서버가 이메일 메시지를 성공적으로 수락했음을 나타내는 응답

QUIT: 클라이언트가 SMTP 세션을 종료하려고 시도

221 SERVICE CLOSING CHANNEL: 서버가 연결 종료 요청을 수락하고 세션을 닫는다는 응답

Sorry-- I can't do lunch next week after all. Heading out of town. Another time! -Ann



```
250 OK
QUIT
221 SERVICE CLOSING CHANNEL
```

4. 서버 종료

<두번째>

```
220 cia-mc07.mx.aol.com ESMTP mail_cia-mc07.1; Sat, 10 Oct 2009 15:37:56 -0400
EHLO annlaptop
250-cia-mc07.mx.aol.com host-69-140-19-190.static.comcast.net
250-AUTH=LOGIN PLAIN XAOL-UAS-MB
250-AUTH LOGIN PLAIN XAOL-UAS-MB
250-STARTTLS
250-CHUNKING
250-BINARYMIME
250-X-AOL-FWD-BY-REF
250-X-AOL-DIV_TAG
250-X-AOL-OUTBOX-COPY
250 HELP
```

서버접속

```
AUTH LOGIN
334 VXNlcm5hbWU6
c25lYWt5ZzMza0Bhb2wuY29t
334 UGFzc3dvcmQ6
NTU4cjAwbHo=
235 AUTHENTICATION SUCCESSFUL
```

서버 접속 계정 및 암호

MAIL FROM: <sneakyg33k@aol.com>

250 OK

RCPT TO: <mistersecretx@aol.com>

250 OK

DATA

354 START MAIL INPUT, END WITH "." ON A LINE BY ITSELF

Message-ID: <001101ca49ae\$e93e45b0\$9f01a8c0@annlaptop>

From: "Ann Dercover" <sneakyg33k@aol.com>

To: <mistersecretx@aol.com>

Subject: rendezvous

Date: Sat, 10 Oct 2009 07:38:10 -0600

MIME-Version: 1.0

Content-Type: multipart/mixed;

boundary="-----=\_NextPart\_000\_000D\_01CA497C.9DEC1E70"

X-Priority: 3

X-MSMail-Priority: Normal

X-Mailer: Microsoft Outlook Express 6.00.2900.2180

X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180

This is a multi-part message in MIME format.

메일전송 (sneakyg33k@aol.com에서 mistersecretx@aol.com으로 전송)

From: "Ann Dercover" <[sneakyg33k@aol.com](mailto:sneakyg33k@aol.com)>: 이메일 발신자의 이름과 이메일 주소. 발신자는 "Ann Dercover", 이메일 주소는 [sneakyg33k@aol.com](mailto:sneakyg33k@aol.com)

To: <[mistersecretx@aol.com](mailto:mistersecretx@aol.com)>: 이메일 수신자의 이메일 주소.

Subject: rendezvous (이메일 주제 : rendezvous)



```
-----=_NextPart_000_000D_01CA497C.9DEC1E70
Content-Type: multipart/alternative;
    boundary="-----=_NextPart_001_000E_01CA497C.9DEC1E70"

-----=_NextPart_001_000E_01CA497C.9DEC1E70
Content-Type: text/plain;
    charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

Hi sweetheart! Bring your fake passport and a bathing suit. Address =
attached. love, Ann
-----=_NextPart_001_000E_01CA497C.9DEC1E70
Content-Type: text/html;
    charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META http-equiv=3DContent-Type content=3D"text/html; =
charset=3Diso-8859-1">
<META content=3D"MSHTML 6.00.2900.2853" name=3DGENERATOR>
<STYLE></STYLE>
</HEAD>
<BODY bgColor=3D#ffffff>
<DIV><FONT face=3DArial size=3D2>Hi sweetheart! Bring your fake passport =
and a=20
bathing suit. Address attached. love, Ann</FONT></DIV></BODY></HTML>

-----=_NextPart_001_000E_01CA497C.9DEC1E70--

-----=_NextPart_000_000D_01CA497C.9DEC1E70
Content-Type: application/octet-stream;
    name="secretrendezvous.docx"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
    filename="secretrendezvous.docx"
```

[Follow Stream] 값에서는 서버 접속과 내용 중간 부분에 attachment 및 filename = secretrendezvous.docx라는 내용을 통해 파일이 첨부되었다라는 사실을 확인

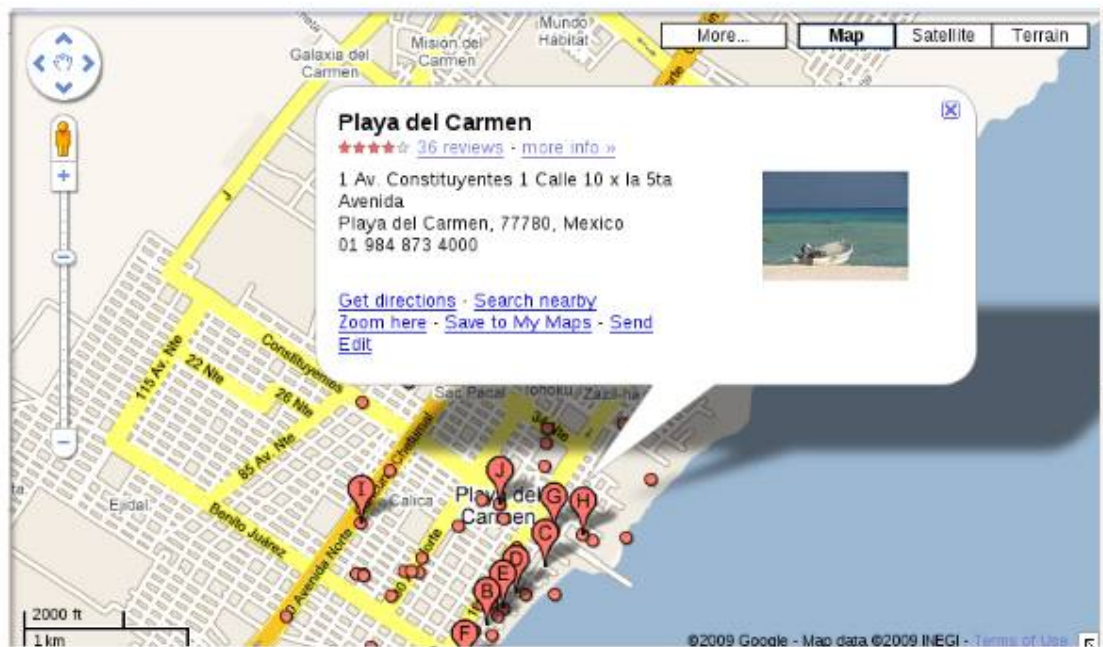
Hi sweetheart! Bring your fake passport and a bathing suit. Address attached. love, Ann

filename="secretrendezvous.docx"

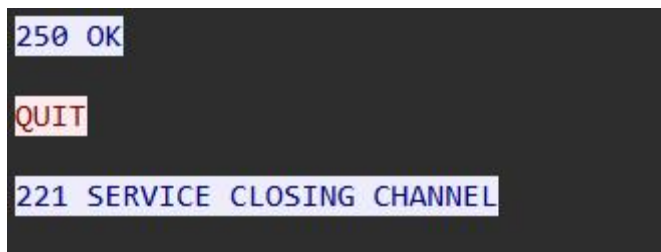
docx 파일로 인코딩 된 것을 확인



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



디코딩 하였더니 지도 추출



서버 종료

53~55

53	82.707578	192.168.1.159	64.12.102.142	TCP	62	1036 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
54	82.817457	64.12.102.142	192.168.1.159	TCP	58	587 → 1036 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
55	82.822388	192.168.1.159	64.12.102.142	TCP	54	1036 → 587 [ACK] Seq=1 Ack=1 Win=64240 Len=0

3-way handshaking을 통해 연결

56

220 : 서비스 준비 완료

cia-mc06.mx.aol.com : 메일 서버의 호스트 이름

ESMTP : SMTP의 한계를 보완한 확장 프로토콜, 이메일 전송을 위한 표준 프로토콜

mail\_cia-mc06.1 : 메일 서버의 식별자

Sat, 10 Oct 2009 15:35:16 -0400 : 메일 서버의 현재 시간

57

EHLO : Helo와 같은 의미(ESMTP에서는 Helo 대신 EHLO를 사용)

59

- 서버가 제공하는 기능과 옵션을 나열함.

- 250 : 성공을 의미(요청 수락)

- 250-cia-mc06.mx.aol.com host-69-140-19-190.static.comcast.net

: 클라이언트와 서버가 서로의 정보를 교환했음을 알려줌

- 250-AUTH=LOGIN PLAIN XAOL-UAS-MB (250-AUTH LOGIN PLAIN XAOL-UAS-MB)

LOGIN

: 간단한 사용자 이름과 비밀번호 기반 인증

PLAIN

: 사용자 이름과 비밀번호를 하나의 문자열로 결합해 전송

XAOL-UAS-MB

: AOL의 확장 인증 프로토콜

STARTTLS

: 이후부터 통신이 암호화

CHUNKING

: 데이터를 큰 덩어리로 나누어 처리할 수 있도록 하여, 메일 전송 효율성을 높이는 기능

BINARYMIME

: 바이너리 MIME(BINARYMIME) 형식을 지원함

X-AOL-FWD-BY-REF

: AOL에서 사용하는 확장 기능

이메일을 전달할 때, 원본 메시지를 복사하지 않고 참조만으로 전달하는 메커니즘

X-AOL-DIV\_TAG

: AOL에서 사용하는 확장 기능

이메일을 내부적으로 관리하거나, 태그를 추가해 메타데이터를 처리하는 데 사용

X-AOL-OUTBOX-COPY

: AOL의 독점 기능

클라이언트가 발송한 이메일의 복사본을 발신자의 아웃박스에 저장하는 기능

HELP : 서버의 추가 정보를 요청

60

Auth Login

: 클라이언트가 서버에 자신을 인증하기 위해 사용자 이름과 비밀번호를 보낼 준비가 되었음을 알리는 명령 / BASE64 인코딩된 사용자 정보로 이루어지며, 서버는 응답으로 사용자 이름과 비밀번호를 요청

62

334 : 클라이언트가 사용자 인증을 위한 정보를 제공할 차례

VXNlcm5hbWU6 : base64로 인코딩된 문자열

63, 66

User : c25lYWt5ZzMza0Bhb2wuY29t - 사용자 명

pass : NTU4cjAwbHo= - 비밀번호

65

334 : 서버가 클라이언트에게 인증 정보를 요청

UGFzc3dvcmQ6 : base64로 인코딩된 문자열

68

235 : 인증 성공을 나타내는 SMTP 응답 코드

AUTHENTICATION SUCCESSFUL : 클라이언트가 제공한 인증 정보와 일치해 인증이 성공적으로 이루어졌음을 의미

69

MAIL FROM : 이메일 발신자를 설정하는 명령

<[sneakyg33k@aol.com](mailto:sneakyg33k@aol.com)> : 이메일 주소가 발신자로 설정

71, 74, 82

250 : SMTP 명령이 성공적으로 처리되었음을 나타내는 상태 코드

OK : 그 명령이 정상적으로 실행되었음을 의미

72

RCPT TO : 이메일 수신자 주소를 설정하는 명령어

<[sec558@gmail.com](mailto:sec558@gmail.com)> : 수신 이메일 주소로 지정

75

DATA : 이메일 내용이 전송

77

354 : 이메일 본문을 시작하라는 서버의 응답 코드

START MAIL INPUT: 서버는 이제 이메일 본문 입력을 시작할 준비가 되었음

END WITH "." ON A LINE BY ITSELF : 마침표는 이메일 본문을 종료하는 신호로 사용

80

from: "Ann Dercover" sneakyg33k@aol.com, subject: lunch next week, (text/plain)  
(text/html) | . : 이메일의 헤더와 본문

83

QUIT : 클라이언트가 이메일 전송을 완료한 후 연결을 종료하려고 할 때 사용

85

221 : SMTP에서 "서비스 종료" 응답을 나타내는 코드

SERVICE CLOSING CHANNEL : 서버가 더 이상 클라이언트의 요청을 처리하지 않고, 연결을 종료할 준비가 되었음을 의미

해당 대화는 1036(client)와 587(server)가 대화하고 있음을 알 수 있다.

서버의 포트 번호를 통해 SMTP 프로토콜을 사용 중임을 알 수 있고 포트가 587인 SMTP는 클라이언트가 메일 서버에 이메일을 제출할 때 사용되는 표준 포트이며, STARTTLS를 사용해 암호화하고 SMTP 프로토콜의 확장을 통해 인증 및 보안을 강화한다. 25번 평문 SMTP보다 보안적으로 더 안전하며, 587보다 더 안전한 SMTP를 사용하고 싶다면 처음부터 SSL로 암호화가 적용되는 465번 포트(SMTPS)를 사용하면 된다.