

작성자	김서영
분석 일자	2024.05.15.
작성 일자	2024.05.17~2024.05.18.
분석 대상	evidence02.pcap
문서 버전	2.0
작성자 E-mail	<a href="mailto:sykim1802@naver.com">sykim1802@naver.com</a>

0. 목차

1. 문제 .....3

2. 분석 도구 .....3

3. 환경 .....3


4. Write-Up.....4

5. Flag..... 11

6. 별도 첨부 ..... 12

7. Reference ..... 13

### 1. 문제

URL	<a href="#">Puzzle #2: Ann Skips Bail – Network Forensics Puzzle Contest (forensicscontest.com)</a>
문제 내용	<p>After being released on bail, Ann Dercover disappears! Fortunately, investigators were carefully monitoring her network activity before she skipped town.</p> <p>"We believe Ann may have communicated with her secret lover, Mr. X, before she left," says the police chief. "The <u>packet capture</u> may contain clues to her whereabouts."</p> <p>You are the forensic investigator. Your mission is to figure out what Ann emailed, where she went, and recover evidence including: (별도첨부)</p>
문제 파일	 <b>evidence02.pcap</b>
문제 유형	Network forensics
난이도	2 / 3

### 2. 분석 도구

도구명	다운로드 링크	Version
Wireshark	<a href="#">Wireshark · Download</a>	4.2.4 x64
HxD	<a href="#">HxD - Freeware Hex Editor and Disk Editor   mh-nexus</a>	2.5.0.0

### 3. 환경

OS
Windows11 x64

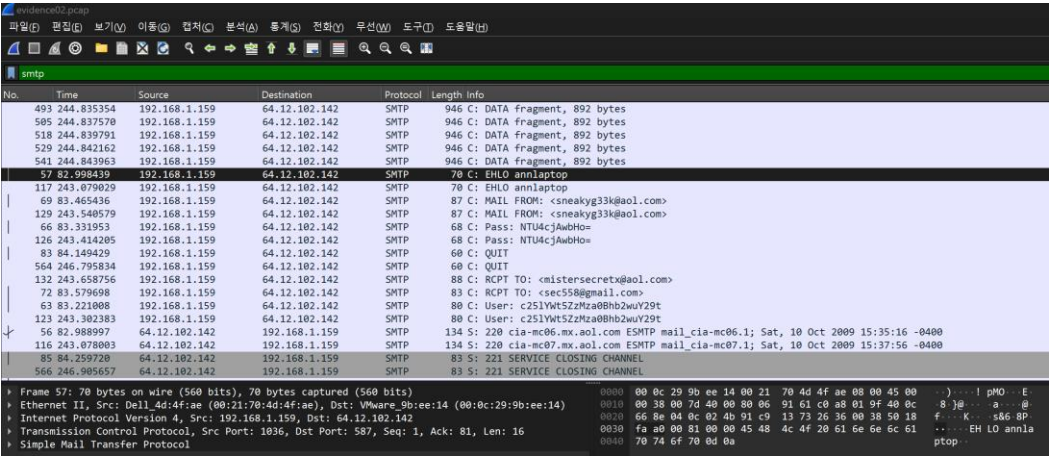
## 4. Write-Up

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

문제 내용에서 Ann의 이메일 활동에 대해 물어보고 있다.

이메일을 전송할 때는 SMTP(Simple Mail Transfer Protocol, 단순 메일 전송 프로토콜)를 이용한다.

따라서 Wireshark에서 evidence.pcap를 연 후 SMTP만 검색해보았다.

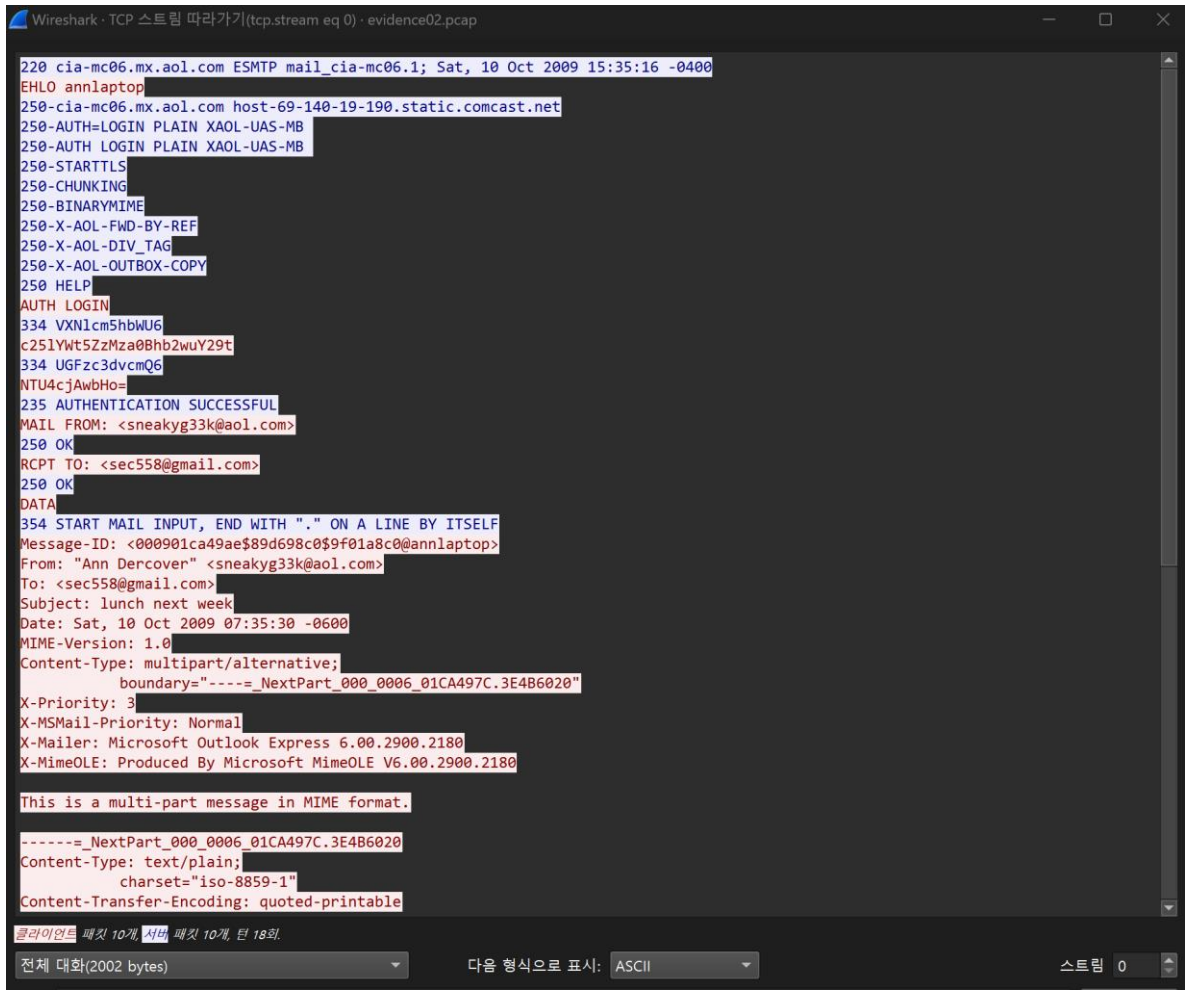


No.	Time	Source	Destination	Protocol	Length	Info
493	244.835354	192.168.1.159	64.12.102.142	SMTP	946	C: DATA fragment, 892 bytes
505	244.837579	192.168.1.159	64.12.102.142	SMTP	946	C: DATA fragment, 892 bytes
518	244.839791	192.168.1.159	64.12.102.142	SMTP	946	C: DATA fragment, 892 bytes
529	244.842162	192.168.1.159	64.12.102.142	SMTP	946	C: DATA fragment, 892 bytes
541	244.843963	192.168.1.159	64.12.102.142	SMTP	946	C: DATA fragment, 892 bytes
57	82.998439	192.168.1.159	64.12.102.142	SMTP	70	C: EHLO annlaptop
117	243.079029	192.168.1.159	64.12.102.142	SMTP	70	C: EHLO annlaptop
69	83.465436	192.168.1.159	64.12.102.142	SMTP	87	C: MAIL FROM: <sneakyg33k@aol.com>
129	243.540579	192.168.1.159	64.12.102.142	SMTP	87	C: MAIL FROM: <sneakyg33k@aol.com>
66	83.331953	192.168.1.159	64.12.102.142	SMTP	68	C: Pass: NTU4cjAwBHo=
126	243.414205	192.168.1.159	64.12.102.142	SMTP	68	C: Pass: NTU4cjAwBHo=
83	84.149429	192.168.1.159	64.12.102.142	SMTP	60	C: QUIT
564	246.795834	192.168.1.159	64.12.102.142	SMTP	60	C: QUIT
132	243.658756	192.168.1.159	64.12.102.142	SMTP	80	C: RCPT TO: <mistersecretx@aol.com>
72	83.579608	192.168.1.159	64.12.102.142	SMTP	83	C: RCPT TO: <sec558@gmail.com>
63	83.221008	192.168.1.159	64.12.102.142	SMTP	80	C: User: c251YwT5ZzHza08hb2wvY29t
123	243.302383	192.168.1.159	64.12.102.142	SMTP	80	C: User: c251YwT5ZzHza08hb2wvY29t
56	82.988997	64.12.102.142	192.168.1.159	SMTP	134	S: 220 cia-mc06.mx.aol.com ESMTP mail_cia-mc06.1; Sat, 10 Oct 2009 15:35:16 -0400
116	243.078003	64.12.102.142	192.168.1.159	SMTP	134	S: 220 cia-mc07.mx.aol.com ESMTP mail_cia-mc07.1; Sat, 10 Oct 2009 15:37:56 -0400
85	84.259728	64.12.102.142	192.168.1.159	SMTP	83	S: 221 SERVICE CLOSING CHANNEL
566	246.905657	64.12.102.142	192.168.1.159	SMTP	83	S: 221 SERVICE CLOSING CHANNEL

[사진 1] SMTP 검색

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

[WHS-2] .iso



[사진 2] tcp 스트림(1)

```
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
```

[사진 3] 이메일 수신자, 발신자, 내용, 발신 일자

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

```
AUTH LOGIN  
334 VXN1cm5hbWU6  
c251YWt5ZzZma0Bhb2wuY29t  
334 UGFzc3dvcmQ6  
NTU4c jAwbHo=  
235 AUTHENTICATION SUCCESSFUL
```

[사진 4] 로그인 흔적

[WHS-2] .iso

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

**Base64 형식에서 디코딩**  
데이터를 입력하고 디코딩 버튼을 누르기만 하면 됩니다.

VXNlcm5hbWU6  
c25lYWt5ZzZmZa0Bhb2wuY29t  
UGFzc3dvcmQ6  
NTU4cjAwbHo=

인코딩된 2진수의 경우(이미지, 문서 등), 이 페이지 아래쪽으로 약간 더 내려가셔서 파일 업로드 양식을 사용해 보세요.

UTF-8 소스 문자 세트.

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

☒ 라이브 모드 끄기 입력하거나 붙여넣으면서 실시간으로 디코딩합니다(UTF-8 문자 세트만 지원).

< 디코딩 > 데이터를 아래 영역으로 디코딩합니다.

Username:sneakyg33k@aol.comPassword:558r00lz

[사진 5] base64 decoder 결과(Base64 디코딩 및 인코딩 - 온라인 (base64decode.org))

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

```
DATA
354 START MAIL INPUT, END WITH "." ON A LINE BY ITSELF
Message-ID: <000901ca49ae589d698c039f01a8c0@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
```

[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.

```
Wireshark - TCP 스트림 따라가기(tcp.stream eq 1) - evidence02.pcap
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
AUTH LOGIN
334 VXN1cm5hbWU6
c251YWt5ZzZmZa08hb2wuY29t
334 UGFzc3dvcmQ6
NTU4c3AwbHo=
235 AUTHENTICATION SUCCESSFUL
MAIL FROM: <sneakyg33k@aol.com>
250 OK
RCPT TO: <mistersecretx@aol.com>
250 OK
```

[사진 7] tcp 스트림 (2)

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

```
-----_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
```

[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 비밀 애인이라고 볼 수 있었다.

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

```
<!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>

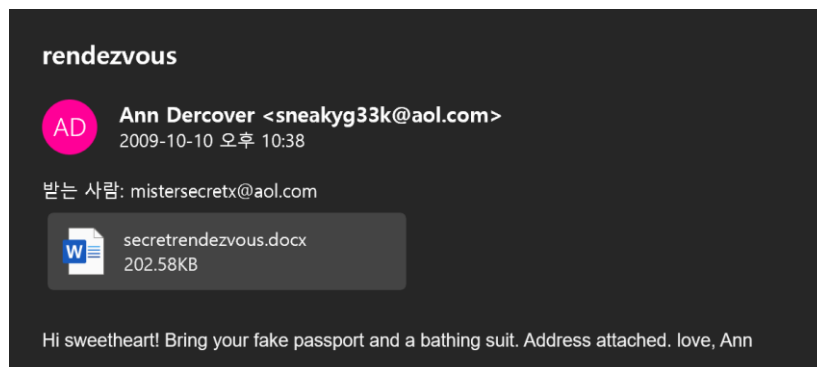
-----_NextPart_001_000E_01CA497C.9DEC1E70--

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

[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

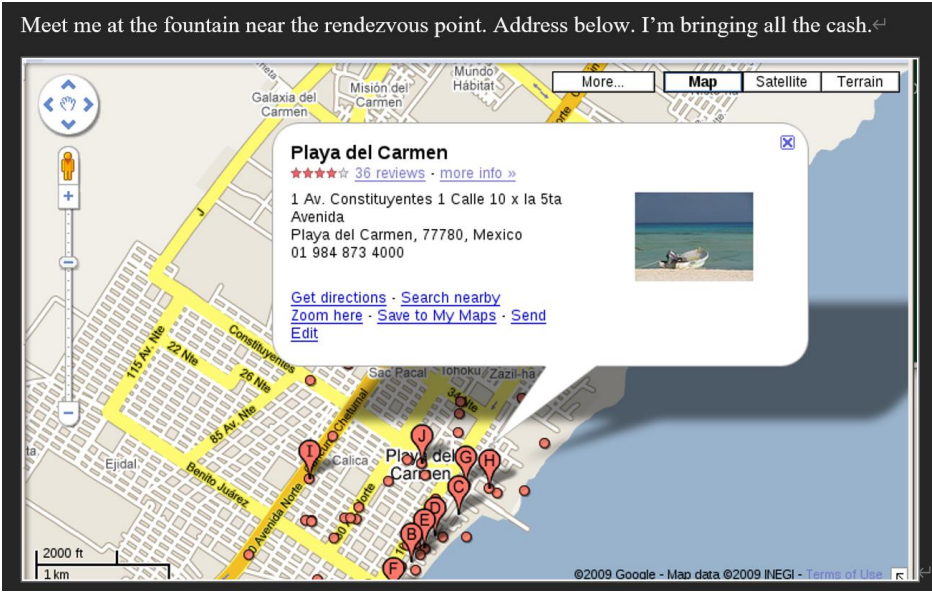
sans02.eml로 저장하니 secretrendezvous.docx파일을 열고 저장할 수 있었다.

```
C:\Users\김서영\Desktop\화이트햇\.iso 임시프로젝트>certutil -hashfile secretrendezvous.docx MD5
MD5의 secretrendezvous.docx 해시 :
9e423e11db88f01bbff81172839e1923
CertUtil: -hashfile 명령이 성공적으로 완료되었습니다.
```

[사진 11] secretrendezvous.docx의 MD5 값

secretrendezvous.docx를 다운 받아 cmd창에서 MD5값을 구하였다.





[사진 12] secretrendezvous.docx 내용

- Ann과 비밀 애인의 rendezvous point의 주소를 확인했다.
- 마지막으로, secretrendezvous.docx 내 이미지 파일의 MD5 값을 구하기 위해 HxD 로 docx 파일을 연 후 PNG 헤더 시그니처와 푸터 시그니처를 찾았다.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000D90	60	ED	56	80	4C	F6	02	00	4C	F6	02	00	15	00	00	00	`iveLô..Lô.....
00000DA0	77	6F	72	64	2F	6D	65	64	69	61	2F	69	6D	61	67	65	word/media/image
00000DB0	31	2E	70	6E	67	89	50	4E	47	0D	0A	1A	0A	00	00	00	l.pngPNG.....
00000DC0	0D	49	48	44	52	00	00	02	F4	00	00	01	B7	08	02	00	.IHDR...ô.....

[사진 13] PNG파일의 헤더 시그니처

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
000303E0	9C	9C	9C	DB	97	8F	3A	8C	92	84	33	FF	17	A3	F1	4C	œœœœŮ—.:Œ'„3ÿ.ŒŒL
000303F0	2A	58	5E	E8	05	00	00	00	00	49	45	4E	44	AE	42	60	*X^è.....TENDØB
00030400	82	50	4B	03	04	14	00	06	00	08	00	00	00	21	00	96	PK.....!.-

[사진 14] PNG파일의 푸터 시그니처

파일 시그니처를 바탕으로 PNG 파일에 해당되는 블록만 선택하여 다시 저장한 후 HxD 로 MD5 값을 확인하였다.

[WHS-2] .iso

secretrendezvous.docx

sans02.png

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG.....IHDR
00000010	00	00	02	F4	00	00	01	B7	08	02	00	00	00	54	9A	56	...ô.....TšV
00000020	1E	00	00	00	03	73	42	49	54	08	08	08	DB	E1	4F	E0	.....sBIT...ŮáOà
00000030	00	00	00	19	74	45	58	74	53	6F	66	74	77	61	72	65	....tEXtSoftware
00000040	00	67	6E	6F	6D	65	2D	73	63	72	65	65	6E	73	68	6F	.gnome-screensho
00000050	74	EF	03	BF	3E	00	00	20	00	49	44	41	54	78	9C	EC	tī.¿>... .IDATxœì

결과

체크섬

검색 (0개의 검색 결과)

C:\Users\김서영\Desktop\화이트햇\iso

템프로젝트\sans02.png

알고리즘	체크섬	사용방법
MD-5	AADEACE50997B1BA24B09AC2EF1940B7	

[사진 15] PNG파일의 MD5값

## 5. Flag

1. sneakyg33k@aol.com
2. 558r00lz
3. mistersecret@aol.com
4. fake passport, a bathing suit
5. secretrendezvous.docx
6. 9e423e11db88f01bbff81172839e1923
7. Playa del Carmen, Mexico
8. AADEACE50997B1BA24B09AC2EF1940B7

## 6. 별도 첨부

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?



## 7. Reference

- [\[네트워크\] 응용 계층 \(velog.io\)](https://velog.io)
- [File Signatures \(garykessler.net\)](https://garykessler.net)