



Confidential Document

## Title

*XCZ Company Hacking Incident*

## Description

### Korean

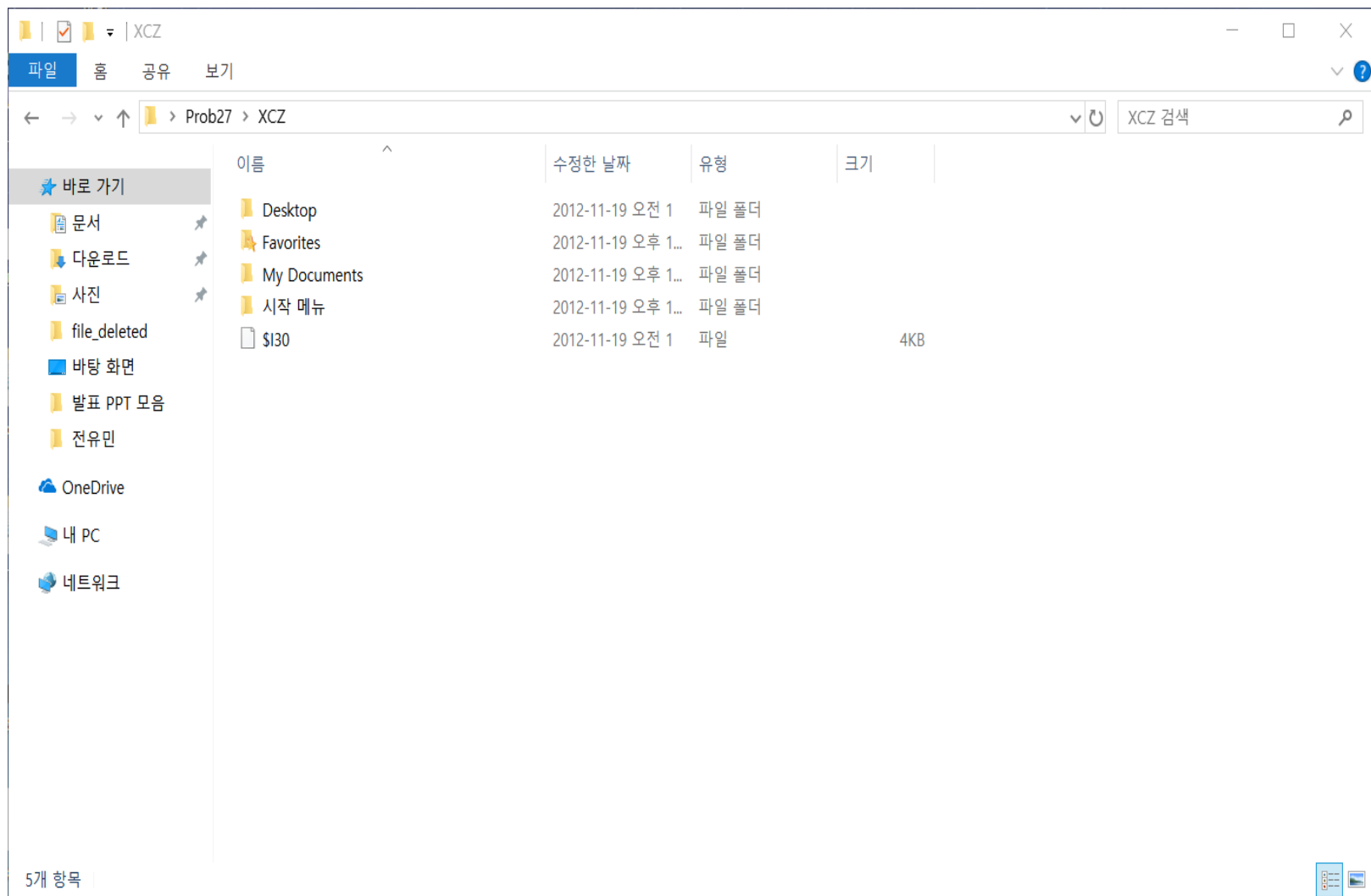
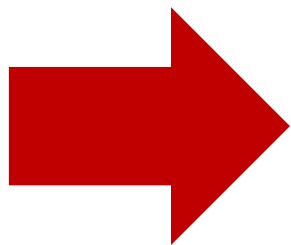
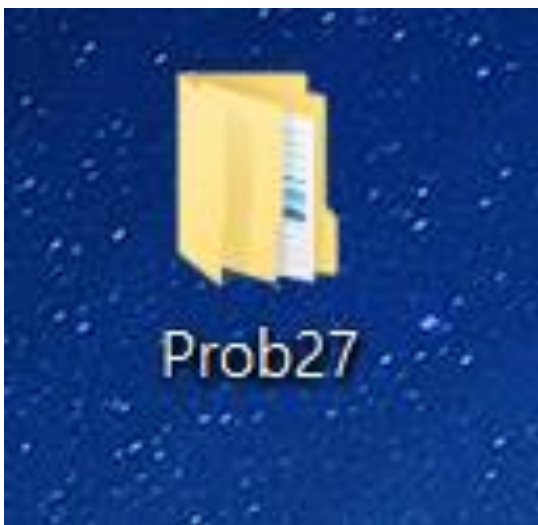
어느 날 해커 'FORENSER' 는 BOSS 의 명령을 받고 계획까지 치밀하게 세운 뒤,  
"XCZ" 라는 회사의 내부에 침입하여 기밀문서를 찾아 외부로 유출하는 과정 중 현장에서 발각되었다.  
조사 중에서도 죄의식을 느끼지 못하고 질문에 답하지 않고 물어보았자 시간을 버리는 일이었다.  
결국 참다 못해 직접 나서서 찾기로 하였다.  
증거를 찾을 수 있는 단서는 'FORENSER' 가 가지고 있던 하드디스크 하나. 나는 일단 하드디스크에서 증거가 될 수 있을만한 것을 추려내었다.  
키 값을 찾으세요.

### English

One day, hackers under the command of the BOSS 'FORENSER' plan densely built after  
Were caught in the field of intrusion by a company called "XCZ" internal confidential document leaked to the external.  
It was a waste of time do not feel guilty survey among the questions asked without answer.  
Eventually was impatient to go out and find.  
Clues can be found in the the evidence 'FORENSER' one hard disk. I had to cull evidence from one hard disk to be.  
Find the key.

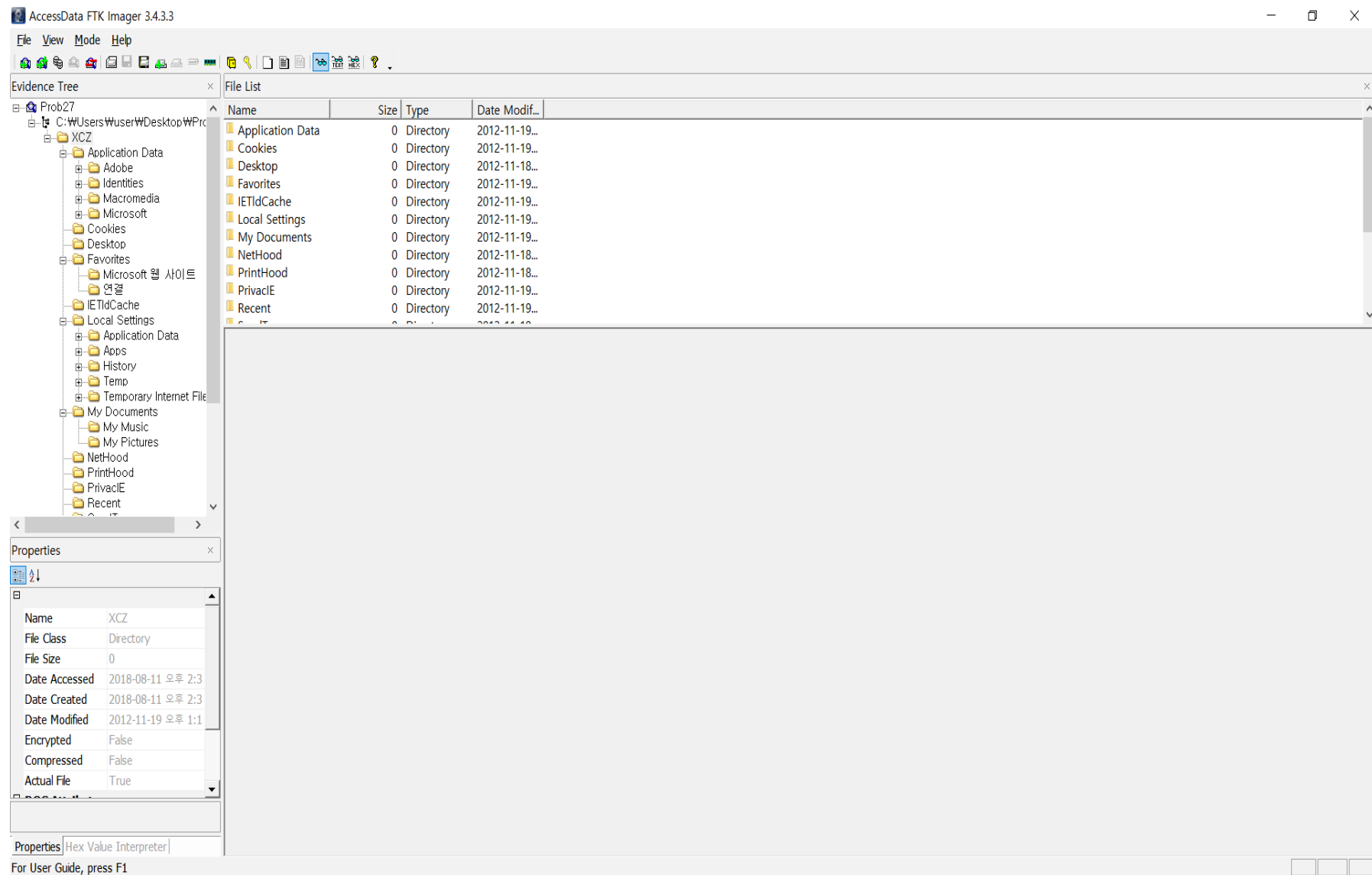
[Prob27.7z](#)

# XCZ.KR Prob 27 (Digital Forensic)





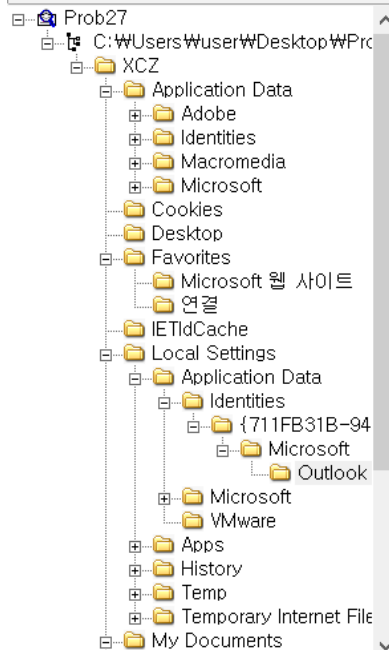
# FTK Imager







## Evidence Tree



## Properties

Name	Outbox.dbx
File Class	Regular File
File Size	142,036
Date Accessed	2018-08-11 오후 2:3
Date Created	2018-08-11 오후 2:3
Date Modified	2012-11-18 오후 4:3
Encrypted	False
Compressed	False
Actual File	True

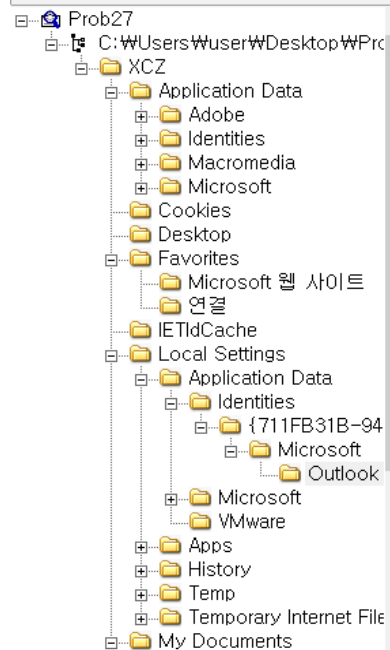
## File List

Name	Size	Type	Date Modif...
\$I30	4	Regular File	2012-11-18...
Folders.dbx	74	Regular File	2012-11-18...
Inbox.dbx	75	Regular File	2012-11-18...
Offline.dbx	10	Regular File	2012-11-18...
Outbox.dbx	139	Regular File	2012-11-18...

```
02aa0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
02ab0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
02ac0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
02ad0 00 00 00 00 D4 2A 00 00-48 00 00 28 28 4D 53 .....
02ae0 47 43 4F 4C 5F 46 4C 41-47 53 20 26 20 41 52 46 .....
02af0 5F 57 41 54 43 48 29 20-21 3D 20 30 20 7C 7C 20 .....
02b00 28 4D 53 47 43 4F 4C 5F-46 4C 41 47 53 20 26 20 .....
02b10 41 52 46 5F 49 47 4E 4F-52 45 29 20 21 3D 20 30 .....
02b20 29 00 00 00 24 2B 00 00-00 B4 02 00 00 00 11 01 .....
02b30 80 02 00 00 81 89 40 01-02 00 00 84 D4 EA 00 .....
02b40 05 08 00 00 06 0F 00 00-08 17 00 00 0D 1E 00 00 .....
02b50 0E 27 00 00 00 03 00 00-91 B1 94 00 12 37 00 00 .....
02b60 13 3F 00 00 14 4B 00 00-1A 59 00 1B 69 00 00 .....
02b70 1C 72 00 00 C0 DE 91 FD-AA C5 CD 01 73 65 63 .....
02b80 65 74 00 1A B2 96 FD AA-C5 CD 01 73 65 63 72 .....
02b90 74 00 46 4F 52 45 4E 53-45 52 00 46 4F 52 45 .....
02ba0 53 45 52 40 78 63 7A 2E-6B 72 00 C0 DE 91 FD .....
02bb0 C5 CD 01 42 4F 53 53 40-78 63 7A 2E 6B 72 00 .....
02bc0 42 4F 53 53 40 78 63 7A-2E 6B 72 3E 00 46 4F .....
02bd0 45 4E 53 45 52 40 78 63-7A 2E 6B 72 00 30 30 .....
02be0 30 30 30 30 31 00 F8 01-00 00 01 00 AF A8 00 .....
02bf0 00 00 00 B1 94 00 00 AF A8-00 00 05 00 00 00 00 .....
02c00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
02c10 00 00 00 00 00 00 00 00-00 00 02 00 00 00 00 .....
02c20 00 00 00 00 00 00 00 00-00 00 AF A8 03 00 AF A8 .....
02c30 01 00 73 01 00 00 B1 94-00 00 00 00 00 00 00 .....
02c40 00 00 01 00 00 00 00 00-00 00 00 00 00 00 00 .....
02c50 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
02c60 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
02c70 00 00 00 00 00 00 00 00-00 00 AF A8 00 00 AF A8 .....
02c80 03 00 00 00 00 00 00 00-00 00 00 00 00 2C 06 .....
02c90 00 00 80 94 00 00 84 05-00 00 00 00 00 00 04 00 .....
02ca0 00 00 57 05 00 00 00 00-00 00 00 00 00 00 00 .....
02cb0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
02cc0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
02cd0 00 00 00 00 00 00 AF A8-03 00 AF A8 04 00 00 00 .....
02ce0 00 00 00 00 00 00 00 00-00 00 68 03 00 24 05 .....
02cf0 00 00 0E 03 00 00 00 00-00 00 04 00 00 E1 02 .....
02d00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
```



## Evidence Tree



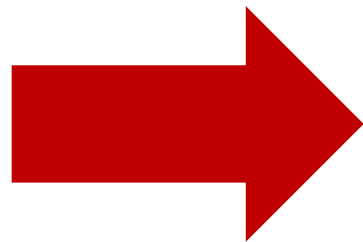
## Properties

Name	Outbox.dbx
File Class	Regular File
File Size	142,036
Date Accessed	2018-08-11 오후 2:3
Date Created	2018-08-11 오후 2:3
Date Modified	2012-11-18 오후 4:3
Encrypted	False
Compressed	False
Actual File	True

## File List

Name	Size	Type	Date Modif...
\$I30	4	Regular File	2012-11-18...
Folders.dbx	74	Regular File	2012-11-18...
Inbox.dbx	75	Regular File	2012-11-18...
Offline.dbx	10	Regular File	2012-11-18...
Outbox.dbx	139	Regular File	2012-11-18...

```
0eab0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
0eac0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
0ead0 00 00 00 00 D4 EA 00 00-00 02 00 00 00 02 00 .....
0eae0 E4 EC 00 00 46 72 6F 6D-3A 20 22 46 4F 52 45 45 .....
0eaf0 53 45 52 22 20 3C 46 4F-52 45 4E 53 45 52 40 .....
0eb00 63 7A 2E 6B 72 3E 0D 0A-54 6F 3A 20 3C 42 4F 52 .....
0eb10 53 40 78 63 7A 2E 6B 72-3E 0D 0A 53 75 62 6A .....
0eb20 63 74 3A 20 73 65 63 72-65 74 0D 0A 44 61 74 .....
0eb30 3A 20 4D 6F 6E 2C 20 31-39 20 4E 6F 76 20 32 .....
0eb40 31 32 20 30 31 3A 33 37-3A 32 35 20 2B 30 39 .....
0eb50 30 0D 0A 4D 49 4D 45 2D-56 65 72 73 69 6F 6E .....
0eb60 20 31 2E 30 0D 0A 43 6F-6E 74 65 6E 74 2D 54 .....
0eb70 70 65 3A 20 6D 75 6C 74-69 70 61 72 74 2F 6D .....
0eb80 78 65 64 3B 0D 0A 09 62-6F 75 6E 64 61 72 79 3D .....
0eb90 22 2D 2D 2D 2D 2D 3F 4E-65 78 74 50 61 72 74 5F .....
0eba0 30 30 30 5F 30 30 33-5F 30 31 43 44 43 35 46 .....
0ebb0 36 2E 36 44 37 45 34 31-42 30 22 0D 0A 58 2D 50 .....
0ebc0 72 69 6F 72 69 74 79 3A-20 33 0D 0A 58 2D 4D 53 .....
0ebd0 4D 61 69 6C 2D 50 72 69-6F 72 69 74 79 3A 20 4E .....
0ebe0 6F 72 6D 61 6C 0D 0A 58-2D 4D 61 69 6C 65 72 3A .....
0ebf0 20 4D 69 63 72 6F 73 6F-66 74 20 4F 75 74 6C 6F .....
0ec00 6F 6B 20 45 78 70 72 65-73 73 20 36 2E 30 30 2E .....
0ec10 32 39 30 30 2E 35 39 33-31 0D 0A 58 2D 4D 69 6D .....
0ec20 65 4F 4C 45 3A 20 50 72-6F 64 75 63 65 64 20 42 .....
0ec30 79 20 4D 69 63 72 6F 73-6F 66 74 20 4D 69 6D 65 .....
0ec40 4F 4C 45 20 56 36 2E 30-30 2E 32 39 30 30 2E 35 .....
0ec50 39 39 34 0D 0A 0D 0A 54-68 69 73 20 69 73 20 61 .....
0ec60 2D 6D 75 6C 74 69 2D 70-61 72 74 20 6D 65 73 73 .....
0ec70 61 67 65 20 69 6E 20 4D-49 4D 45 20 66 6F 72 6D .....
0ec80 61 74 2E 0D 0A 0D 0A 2D-2D 2D 2D 2D 2D 3D 5F 4E .....
0ec90 65 78 74 50 61 72 74 5F-30 30 30 5F 30 30 30 33 .....
0eca0 5F 30 31 43 44 43 35 46-36 2E 36 44 37 45 34 31 .....
0ecb0 42 30 0D 0A 43 6F 6E 74-65 6E 74 2D 54 79 70 65 .....
0ecc0 3A 20 6D 75 6C 74 69 70-61 72 74 2F 61 6C 74 65 .....
0ecd0 72 6E 61 74 69 76 65 3B-0D 0A 09 62 6F 75 6E 64 .....
0ece0 61 72 79 3D E4 EC 00 00-00 02 00 00 00 02 00 .....
0ecf0 F4 E2 00 00 22 2D 2D 2D-2D 3D 5F 4E 65 78 74 50 .....
0ed00 61 72 74 5F 30 30 31 5F-30 30 30 34 5F 30 31 43 .....
0ed10 44 43 35 46 36 2E 36 44-37 45 34 31 42 30 22 0D .....
0ed20 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
```



# DBX???

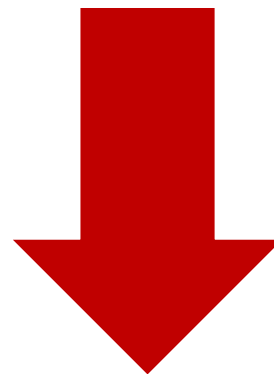
Export Files...

DBX파일

Microsoft Outlook Express 데이터 파일 확장자

Outlook Express

Microsoft에서 제공하는 이메일 클라이언트 프로그램





# Mail Viewer

(IDX, MBX, DBX)

Open Wizard

[ Open what? ]

☒ **Mozilla Thunderbird message database** Browse current TB store

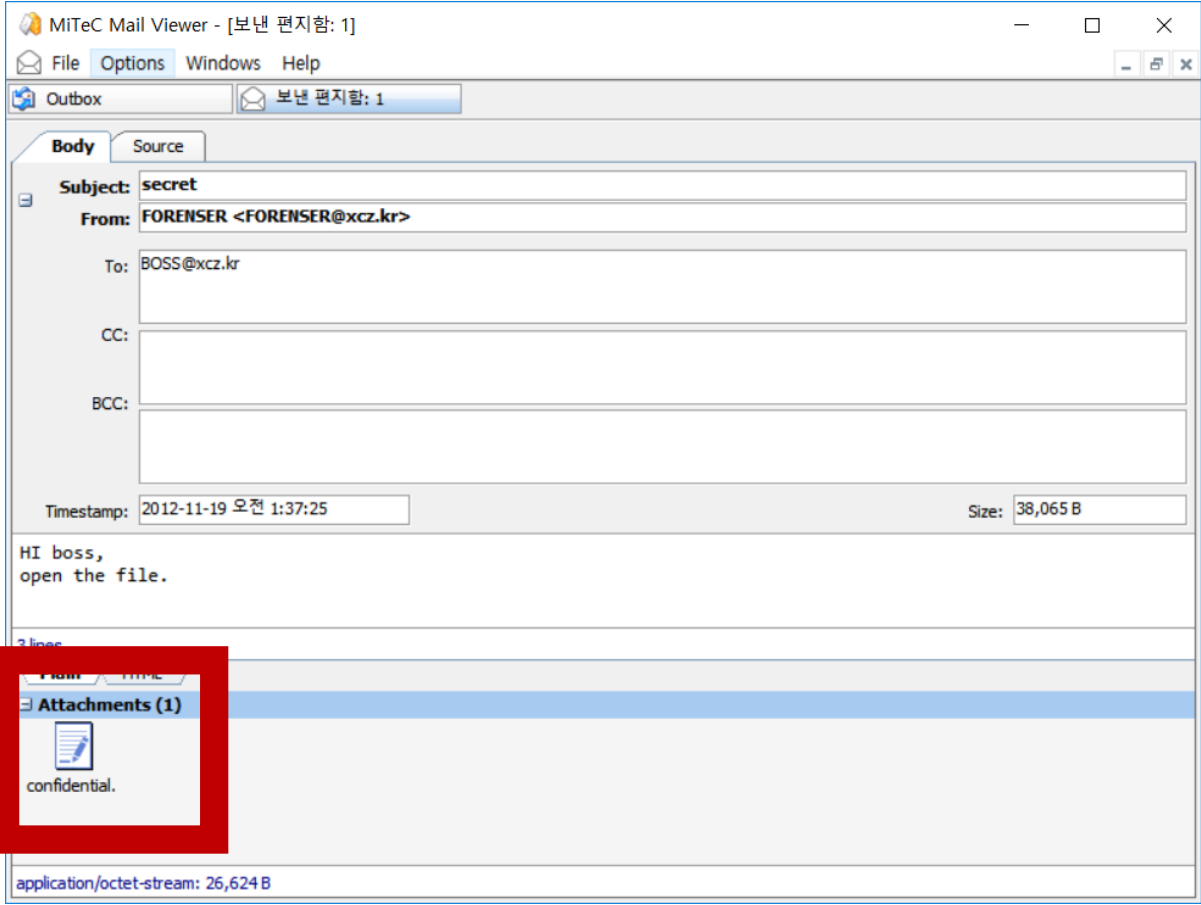
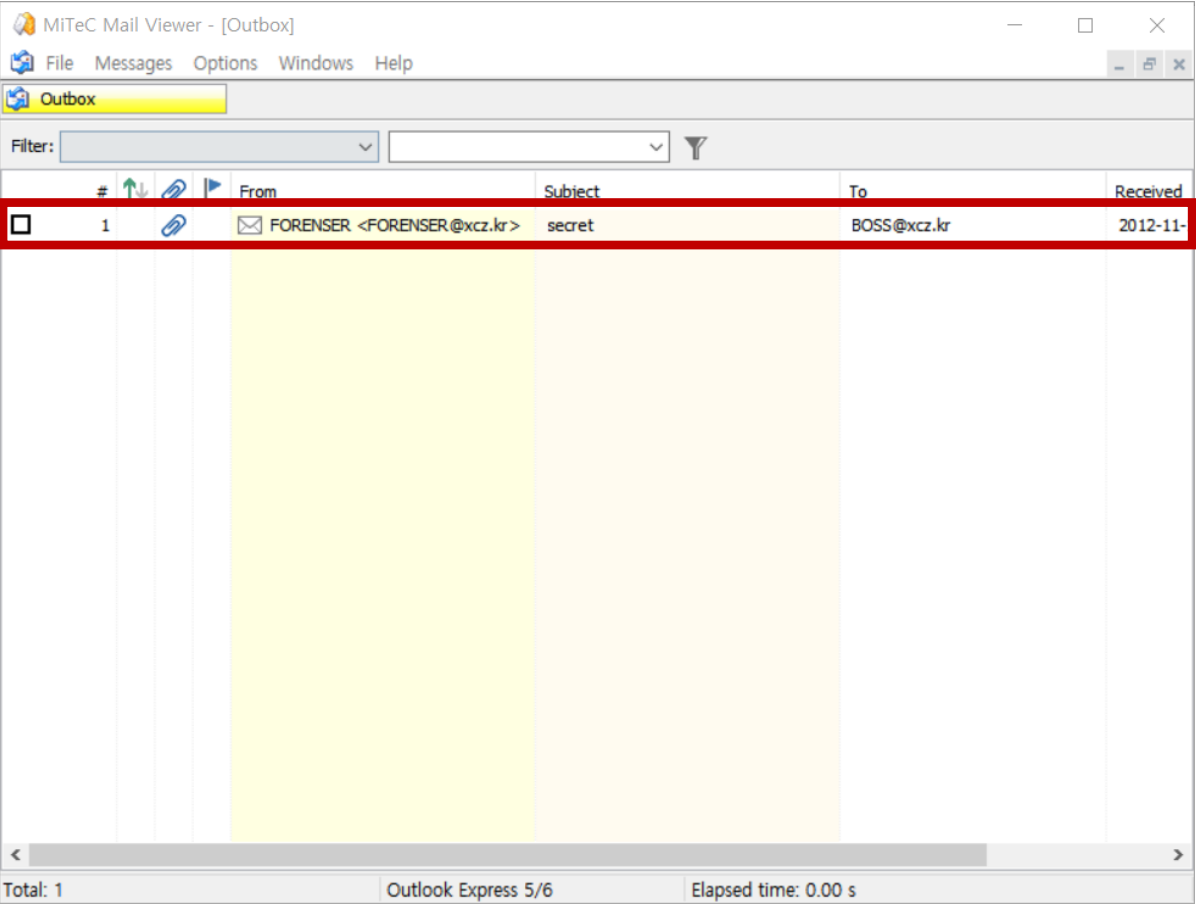
☐ **Folder containing e-mail files (EML)** Browse current Win/Live Mail store

☐ **Single EML file**

☒ **Outlook Express message database** Browse current OE store

☒ Evaluate attachment presence

OK Cancel





Boss! Long time no see!

The meantime, how are you?

Difference, but have gotten to the boss you ordered X CZ company's confidential documents.

We will bring together the hard disk.

I'll see you soon find! Boss!

----- Confidential document -----

10.21 Site Open - Admin : (Reset & UNLIMIT)

10.21 New Prob! - [Prob1 ~ Prob20]

10.21 Facebook sharing feature Open!

10.21 New Prob! - [Prob1 ~ Prob20]

10.21 Facebook sharing feature Open!

10.22 New Web Prob21[300]

10.23 New Forensic Prob22[250]

10.27 New Trivia Prob23[200]

11.03 Naver search engine X CZ.KR were registered.

11.04 New Forensic Prob24[200]

11.04 New Trivia Prob25[250]

11.18 New Crypto Prob26[150]

11.19 New Forensic Prob27[150]

???

번역

즉석 번역 사용 안함

영어 한국어 독일어 언어 감지



한국어 영어 일본어

번역하기

Boss! Long time no see!  
The meantime, how are you?

Difference, but have gotten to the boss you ordered X CZ company's confidential documents.

We will bring together the hard disk.  
I'll see you soon find! Boss!

----- Confidential document -----

10.21 Site Open - Admin : (Reset & UNLIMIT)  
10.21 New Prob! - [Prob1 ~ Prob20]  
10.21 Facebook sharing feature Open!  
10.22 New Web Prob21[300]  
10.23 New Forensic Prob22[250]  
10.27 New Trivia Prob23[200]  
11.03 Naver search engine X CZ.KR were registered.  
11.04 New Forensic Prob24[200]  
11.04 New Trivia Prob25[250]  
11.18 New Crypto Prob26[150]  
11.19 New Forensic Prob27[150]

보스! 오랜만 이네!  
그동안, 잘 지냈니?

차이점은 있지만 X CZ 회사에 대한 상사에게 알려 주었습니다.

우리는 하드 디스크를  
나눈 다음

----- Confidential document -----  
10.21 Site Open - Admin : (Reset & UNLIMIT)  
10.21 New Prob! - [Prob1 ~ Prob20]  
10.21 Facebook sharing feature Open!  
10.22 New Web Prob21[300]  
10.23 New Forensic Prob22[250]  
10.27 New Trivia Prob23[200]  
11.03 Naver search engine X CZ.KR were registered.  
11.04 New Forensic Prob24[200]  
11.04 New Trivia Prob25[250]  
11.18 New Crypto Prob26[150]  
11.19 New Forensic Prob27[150]

10.21 Site Open - Admin : (Reset & UNLIMIT)  
10.21 New Prob! - [Prob1 ~ Prob20]  
10.21 Facebook sharing feature Open!  
10.22 New Web Prob21[300]  
10.23 New Forensic Prob22[250]  
10.27 New Trivia Prob23[200]  
11.03 Naver search engine X CZ.KR were registered.  
11.04 New Forensic Prob24[200]  
11.04 New Trivia Prob25[250]  
11.18 New Crypto Prob26[150]  
11.19 New Forensic Prob27[150]

☆ 📄 🔊 🔍

수정 제한하기



656/5000

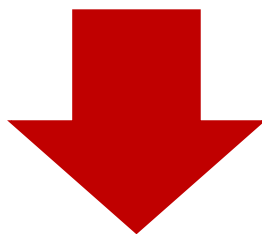
boseul olaenman inel

11.04 New Forensic Prob24[200]

11.04 New Trivia Prob25[250]

11.18 New Crypto Prob26[150]

11.19 New Forensic Prob27[150]



11.04 New Forensic Prob24[200]

11.04 New Trivia Prob25[250]

11.18 New Crypto Prob26[150]

11.19 New Forensic Prob27[150] auth key is



# CLEAR!!!

Thank You