# Confidential Document

**Title**

*XCZ Company Hacking Incident*

**Description**

**Korean**

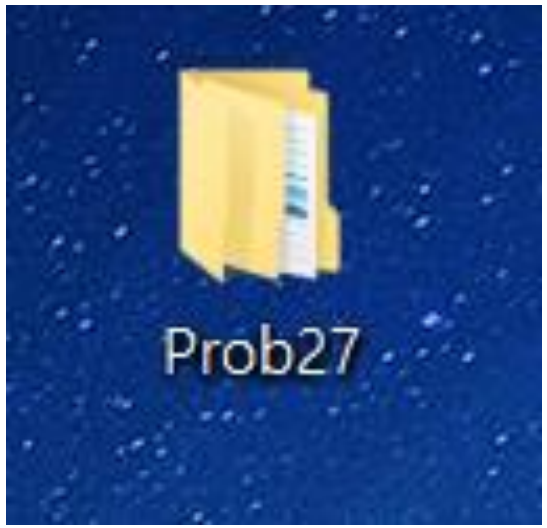
어느 날 해커 'FORENSER' 는 BOSS 의 명령을 받고 계획까지 치밀하게 세운 뒤,
"XCZ" 라는 회사의 내부에 침입하여 기밀문서를 찾아 외부로 유출하는 과정 중 현장에서 발각되었다.
조사 중에서도 죄의식을 느끼지 못하고 질문에도 답하지 않고 물어보았자 시간을 버리는 일이었다.
결국 참다 못해 직접 나서서 찾기로 하였다.
증거를 찾을 수 있는 단서는 'FORENSER' 가 가지고 있던 하드디스크 하나. 나는 일단 하드디스크에서 증거가 될 수 있을만한 것을 추려내었다.
키 값을 찾으세요.

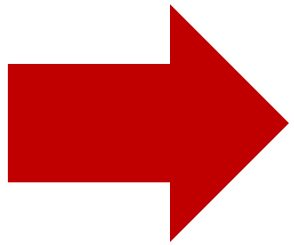
**English**

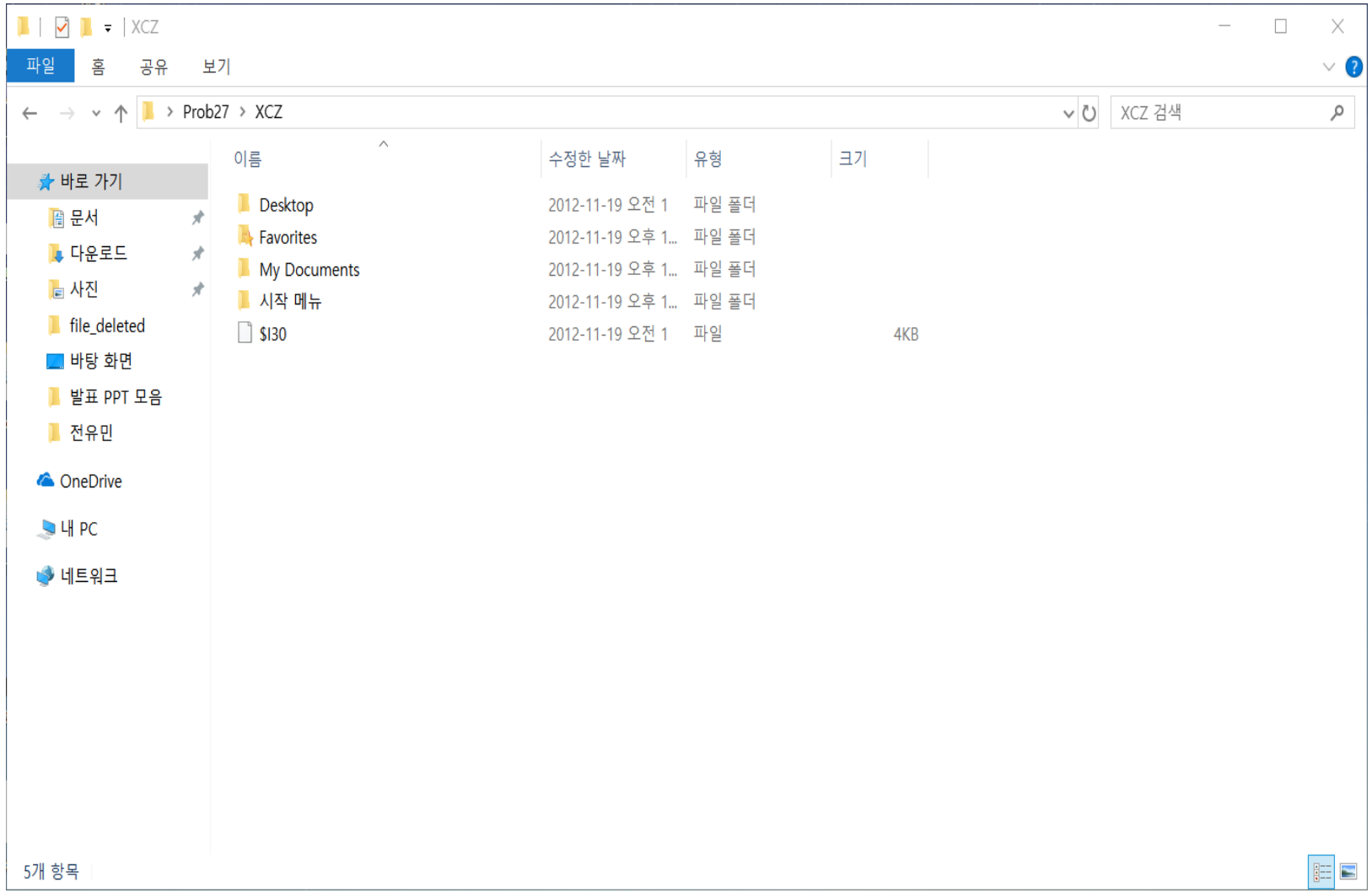
One day, hackers under the command of the BOSS 'FORENSER' plan densely built after
Were caught in the field of intrusion by a company called "XCZ" internal confidential document leaked to the external.
It was a waste of time do not feel guilty survey among the questions asked without answer.
Eventually 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.

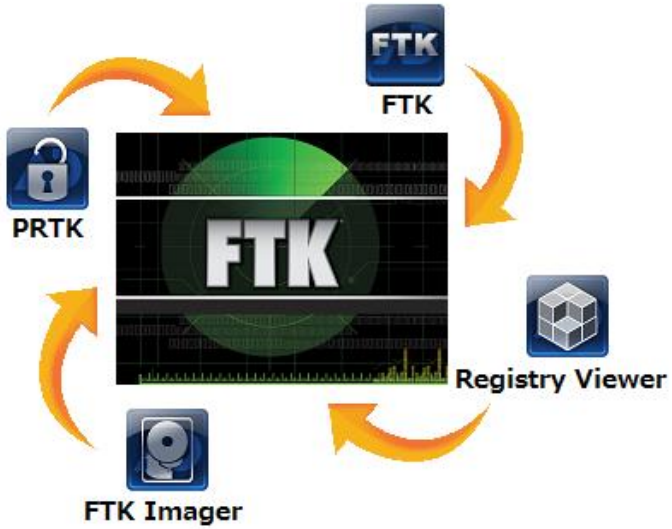
Prob27.7z

# XCZ.KR Prob 27 (Digital Forensic)


Prob27




XCZ
파일
홈
공유
보기
Prob27 › XCZ
XCZ 검색
바로 가기
문서
다운로드
사진
file_deleted
바탕 화면
발표 PPT 모음
전유민
OneDrive
내 PC
네트워크
이름
수정한 날짜
유형
크기
Desktop
2012-11-19 오전 1
파일 폴더
Favorites
2012-11-19 오후 1...
파일 폴더
My Documents
2012-11-19 오후 1...
파일 폴더
시작 메뉴
2012-11-19 오후 1...
파일 폴더
$I30
2012-11-19 오전 1
파일
4KB
5개 항목




# FTK Imager

AccessData FTK Imager 3.4.3.3

File View Mode Help

Evidence Tree

Prob27
C:₩Users₩user₩Desktop₩Pr
XCZ
Application Data
Adobe
Identities
Macromedia
Microsoft
Cookies
Desktop
Favorites
Microsoft 웹 사이트
연결
IETldCache
Local Settings
Application Data
Apps
History
Temp
Temporary Internet File
My Documents
My Music
My Pictures
NetHood
PrintHood
PrivacIE
Recent

File List

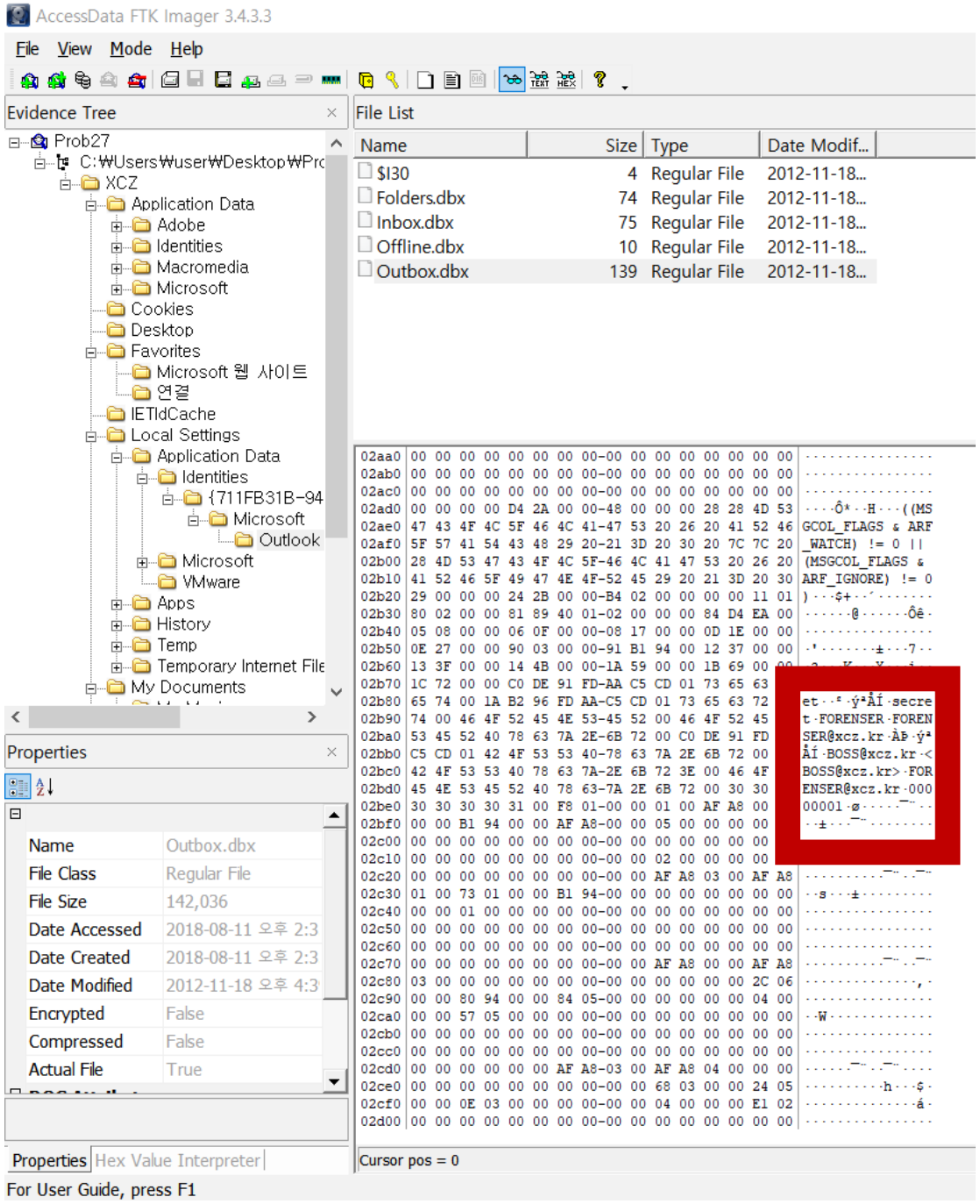
| Name | Size | Type | Date Modif... |
|---|---|---|---|
| Application Data | 0 | Directory | 2012-11-19... |
| Cookies | 0 | Directory | 2012-11-19... |
| Desktop | 0 | Directory | 2012-11-18... |
| Favorites | 0 | Directory | 2012-11-19... |
| IETldCache | 0 | Directory | 2012-11-19... |
| Local Settings | 0 | Directory | 2012-11-19... |
| My Documents | 0 | Directory | 2012-11-19... |
| NetHood | 0 | Directory | 2012-11-18... |
| PrintHood | 0 | Directory | 2012-11-18... |
| PrivacIE | 0 | Directory | 2012-11-19... |
| Recent | 0 | Directory | 2012-11-19... |

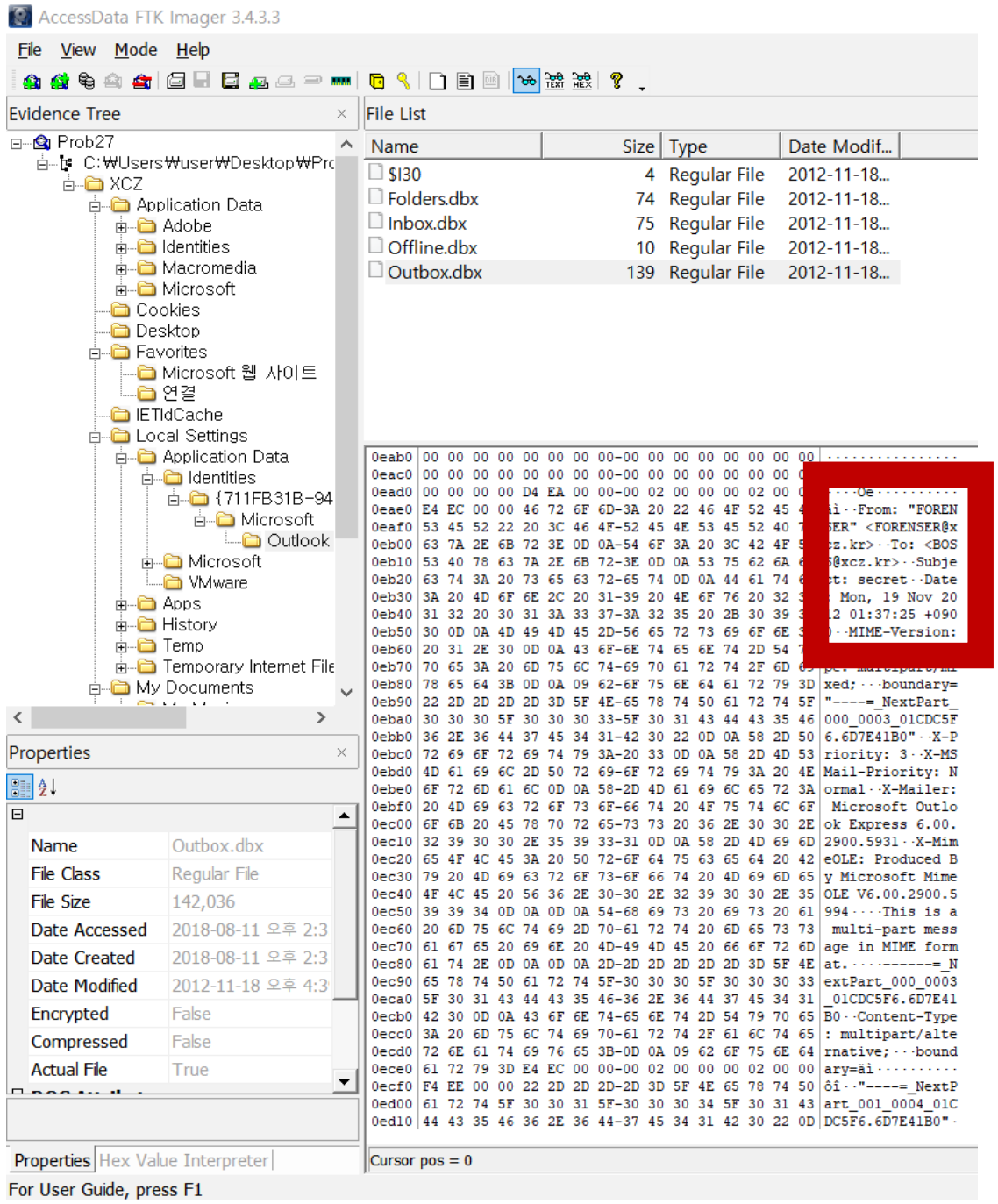
Properties

| | |
|---|---|
| Name | XCZ |
| File Class | Directory |
| File Size | 0 |
| Date Accessed | 2018-08-11 오후 2:3 |
| Date Created | 2018-08-11 오후 2:3 |
| Date Modified | 2012-11-19 오후 1:1 |
| Encrypted | False |
| Compressed | False |
| Actual File | True |

Properties | Hex Value Interpreter

For User Guide, press F1


AccessData FTK Imager 3.4.3.3
File View Mode Help
Evidence Tree
Prob27
C:₩Users₩user₩Desktop₩Pro
XCZ
Application Data
Adobe
Identities
Macromedia
Microsoft
Cookies
Desktop
Favorites
Microsoft 웹 사이트
연결
IETldCache
Local Settings
Application Data
Identities
{711FB31B-94
Microsoft
Outlook
Microsoft
VMware
Apps
History
Temp
Temporary Internet File
My Documents
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...
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
Properties Hex Value Interpreter
Cursor pos = 0
For User Guide, press F1


AccessData FTK Imager 3.4.3.3
File View Mode Help
Evidence Tree
Prob27
C:₩Users₩user₩Desktop₩Pro
XCZ
Application Data
Adobe
Identities
Macromedia
Microsoft
Cookies
Desktop
Favorites
Microsoft 웹 사이트
연결
IETldCache
Local Settings
Application Data
Identities
{711FB31B-94
Microsoft
Outlook
Microsoft
VMware
Apps
History
Temp
Temporary Internet File
My Documents
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...
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
Properties Hex Value Interpreter
Cursor pos = 0
For User Guide, press F1


DBX???

Export Files...

## DBX파일

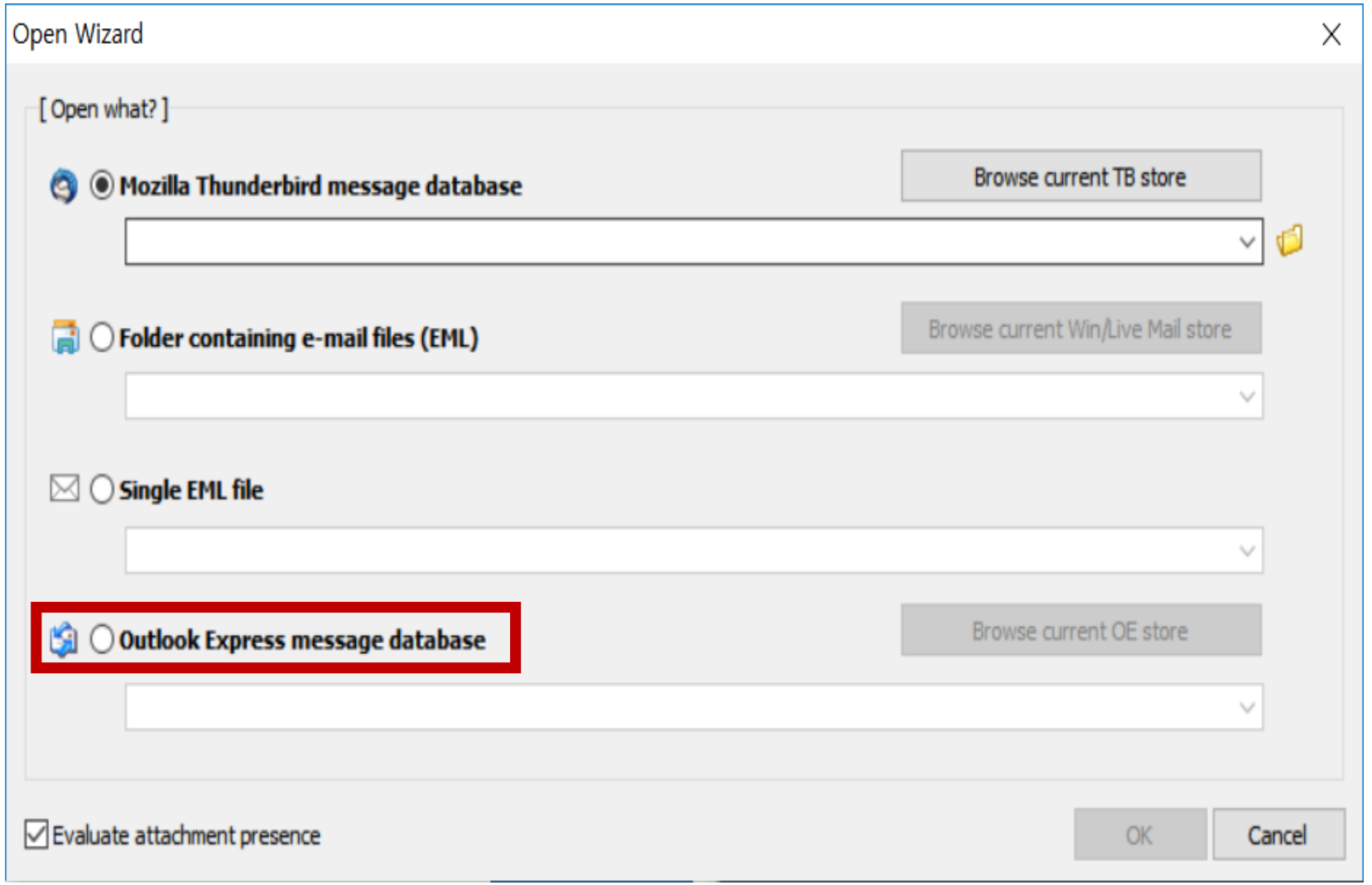
Microsoft Outlook Express 데이터 파일 확장자

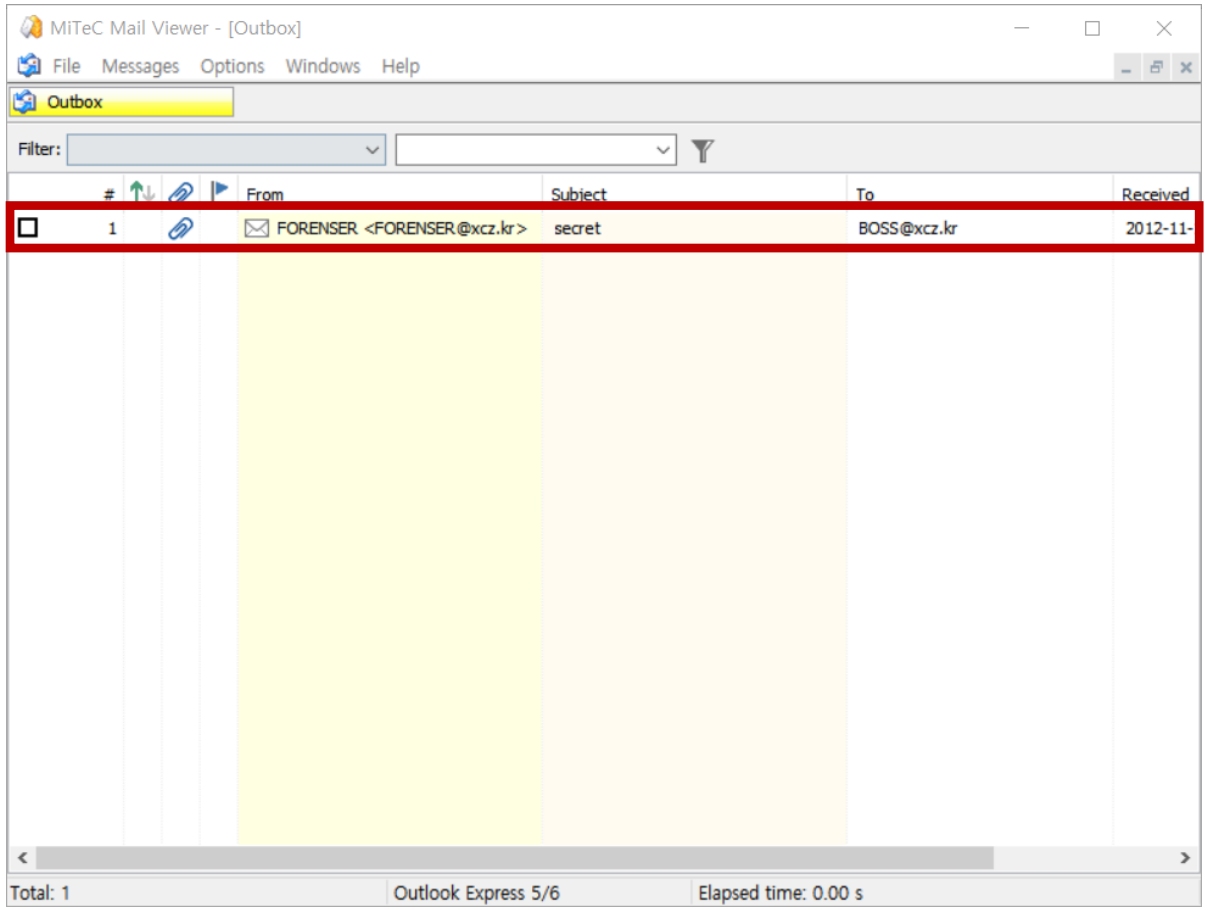
## Outlook Express

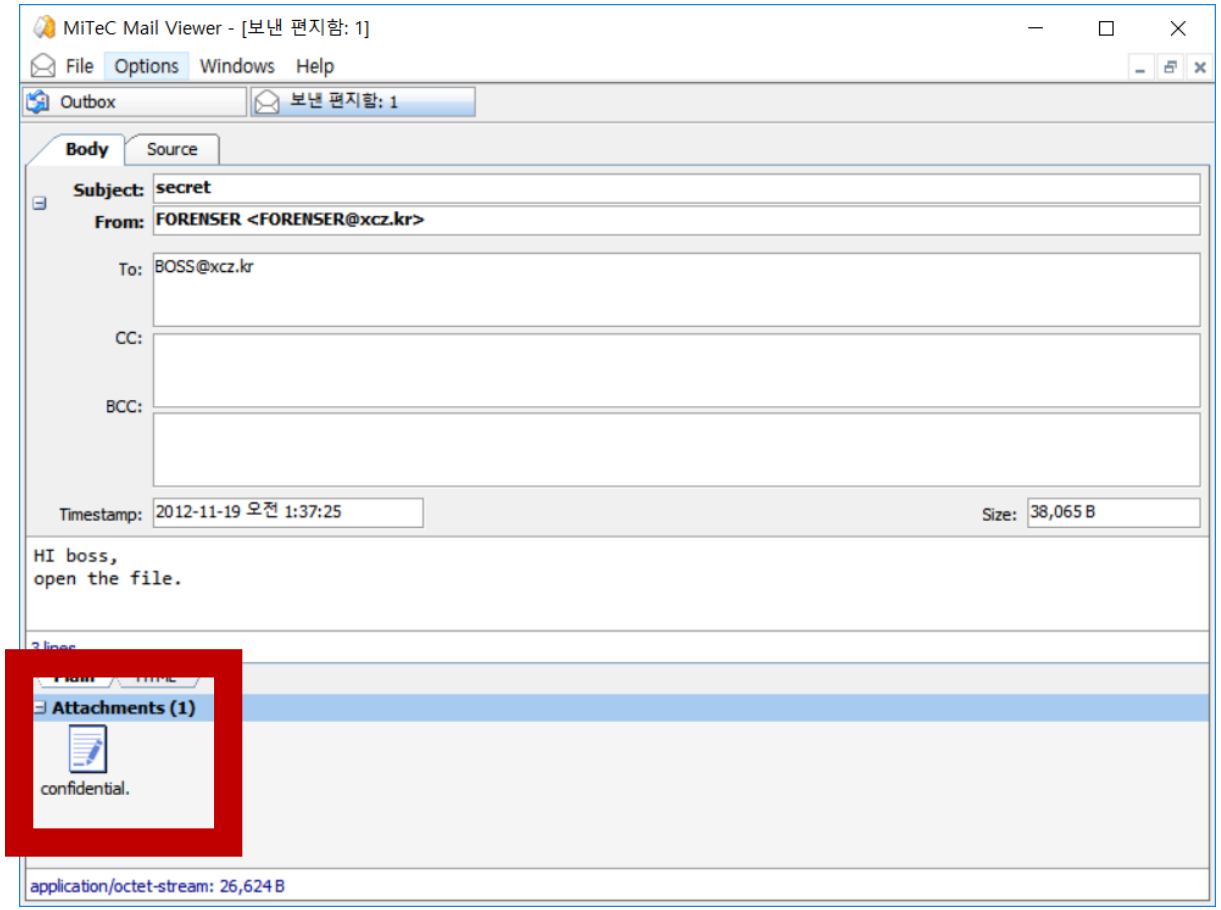
Microsoft에서 제공하는 이메일 클라이언트 프로그램

# Mail Viewer

(IDX, MBX, DBX)




MiTeC Mail Viewer - [Outbox]
File Messages Options Windows Help
Outbox
Filter:
# From Subject To Received
1 FORENSER <FORENSER@xcz.kr> secret BOSS@xcz.kr 2012-11-
Total: 1
Outlook Express 5/6
Elapsed time: 0.00 s


MiTeC Mail Viewer - [보낸 편지함: 1]
File Options Windows Help
Outbox
보낸 편지함: 1
Body Source
Subject: secret
From: FORENSER <FORENSER@xcz.kr>
To: BOSS@xcz.kr
CC:
BCC:
Timestamp: 2012-11-19 오전 1:37:25
Size: 38,065 B
HI boss,
open the file.
Attachments (1)
confidential.
application/octet-stream: 26,624 B

Boss! Long time no see!

The meantime, how are you?

Difference, but have gotten to the boss you ordered XCZ 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 XCZ.KR were registered.

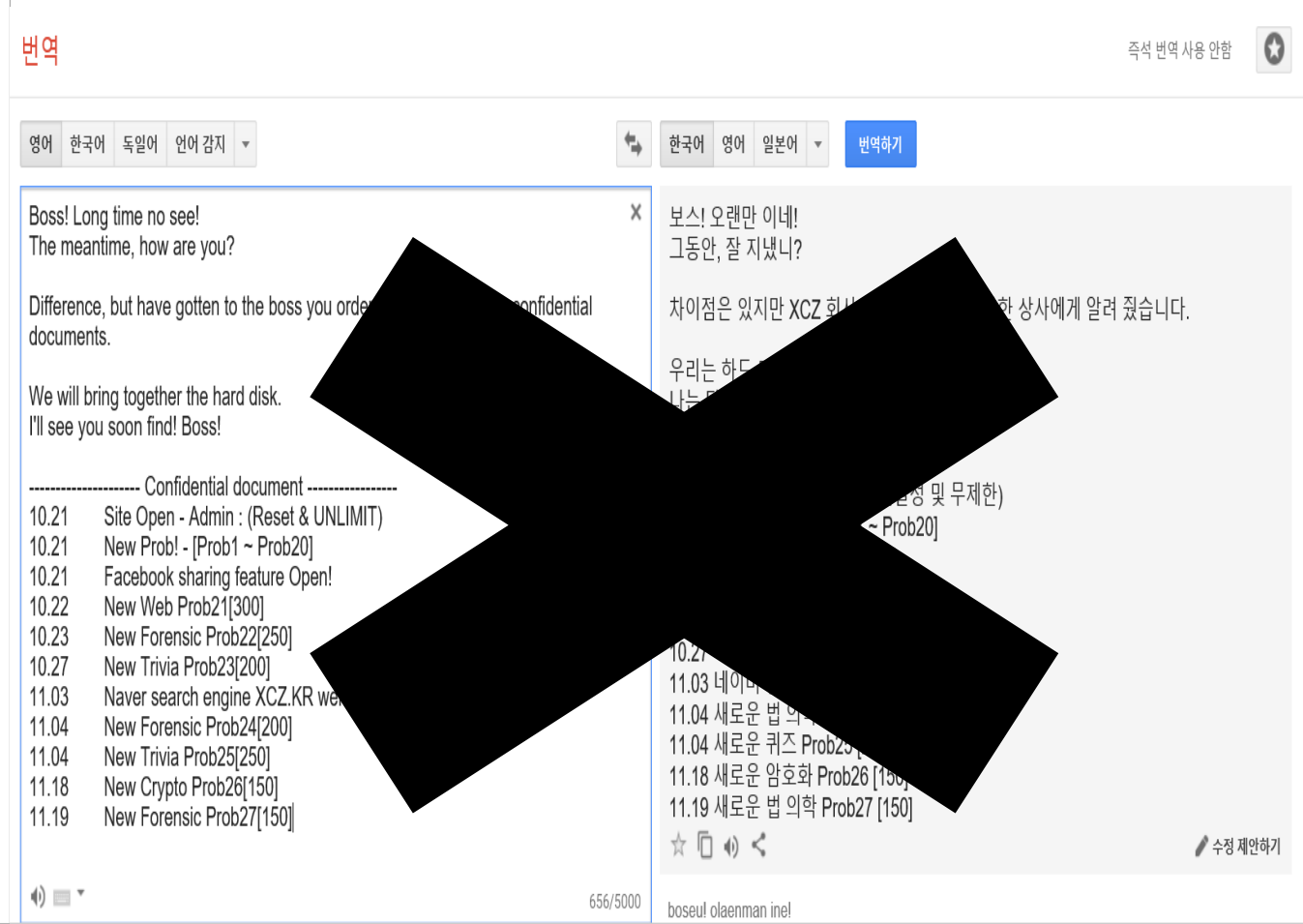
11.04 New Forensic Prob24[200]

11.04 New Trivia Prob25[250]

11.18 New Crypto Prob26[150]

11.19 New Forensic Prob27[150]

# ???

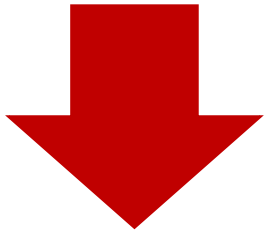


11.04 New Forensic Prob24[200]

11.04 New Trivia Prob25[250]

11.18 New Crypto Prob26[150]

11.19 New Forensic Prob27[150] [redacted]



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 [redacted]

# CLEAR!!!

# Thank You