**그래픽, 클립아트, 그림, 디자인이(가) 표시된 사진

자동 생성된 설명**

**[XCZ Company Hacking Incident] Write-Up**

|  |  |
| --- | --- |
| **작성자** | 김서영 |
| **분석 일자** | 2024.05.18. |
| **작성 일자** | 2024.05.18. |
| **분석 대상** | Prob27.7z |
| **문서 버전** | 1 |
| **작성자 E-mail** | [sykim1802@naver.com](mailto:sykim1802@naver.com) |

1. **목차**

[**1.** **문제** 3](#_Toc165902295)

[**2.** **분석 도구** 3](#_Toc165902296)

[**3.** **환경** 3](#_Toc165902297)

[**4.** **Write-Up** 4](#_Toc165902298)

[**5.** **Flag** 7](#_Toc165902299)

[**6.** **별도 첨부** 8](#_Toc165902300)

[**7.** **Reference** 9](#_Toc165902301)

# **문제**

|  |  |
| --- | --- |
| **URL** | [Prob27 (xcz.kr)](http://xcz.kr/START/prob/prob27.php) |
| **문제**  **내용** | 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. |
| **문제**  **파일** |  |
| **문제**  **유형** | Disk forensics |
| **난이도** | 1 / 5 |

# **분석 도구**

|  |  |  |
| --- | --- | --- |
| **도구명** | **다운로드 링크** | **Version** |
| Autopsy | [Autopsy - Download](https://www.autopsy.com/download/) | 4.21.0 |
| Mail Viewer | [MiTeC Homepage](https://www.mitec.cz/mailview.html) | 2.5.1.0 |
|  |  |  |

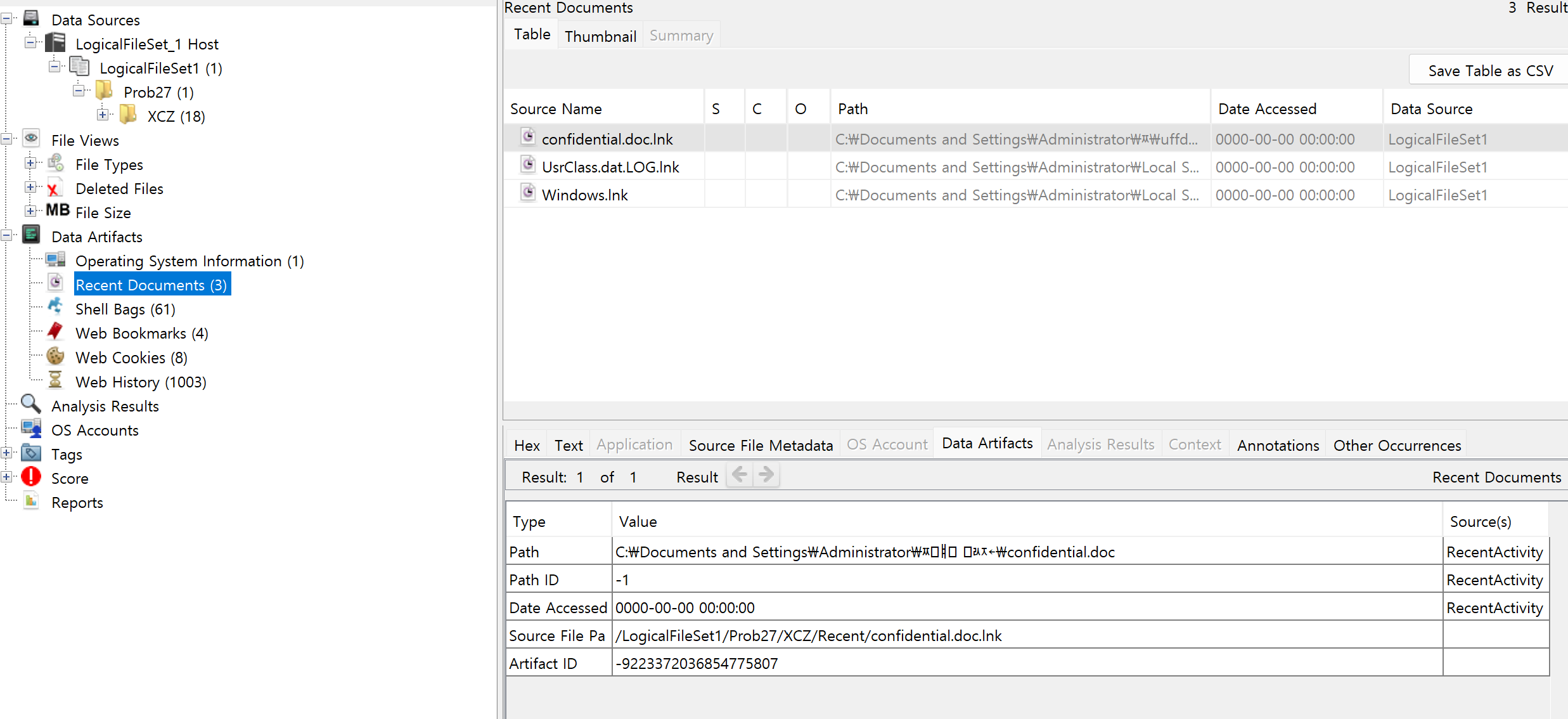
# **환경**

|  |
| --- |
| **OS** |
| Windows11 x64 |

# **Write-Up**

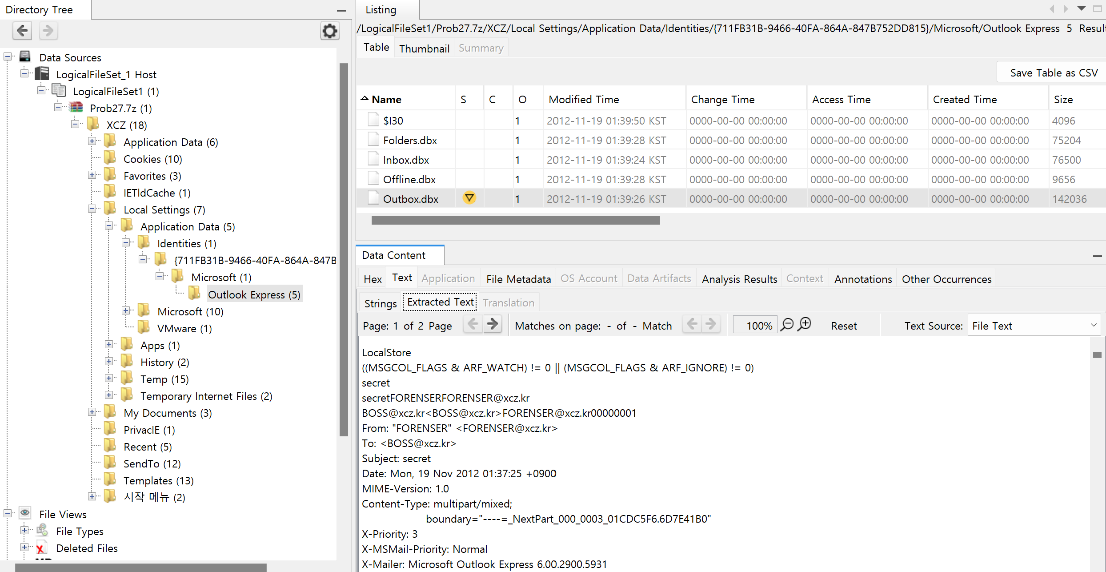
|  |  |
| --- | --- |
| **파일명** | Prob27.7z |
| **용량** | 15,648kb |
| **SHA256** | d1e528b350ab1623711b668f48c316c9e38811f1b073f91e2a30a1b88786c7b6 |
| **Timestamp** | ‎ 2024‎-05‎-17‎ 11:42:03 |

1. 문서 양이 많지 않아서 문서들 목록을 먼저 보게 되었다.



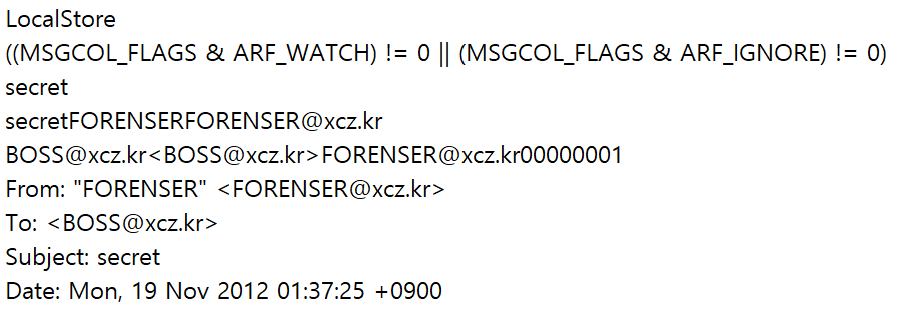
[사진 1] Data Artifacts – Recent Documents

최근 문서 기록에 “Confidential.doc.lnk”가 남아있었다. Confidential(기밀)이라는 제목이 확 눈에 들어왔고, 링크가 남아있다는 뜻은 Confidential.doc가 어딘가 있음을 의미하기에 파일 찾기에 몰두했다.



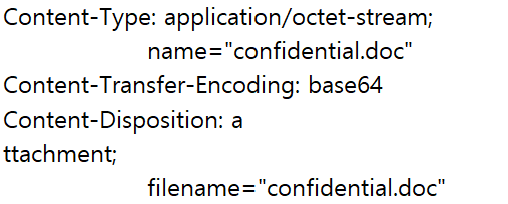
[사진 2] 수상한 dbx 파일

숫자로 시작하는 파일 내부에서 outlook express 폴더를 찾았다. 기록과 텍스트 내용을 자세히 살펴보았다.



[사진 3] 수신자와 발신자

문제 내용에서 나온 해커 “Forenser”의 이름이 나왔고, 그가 발신자이다. 또한, 문제내용과 일치하게 수신자는 BOSS다.



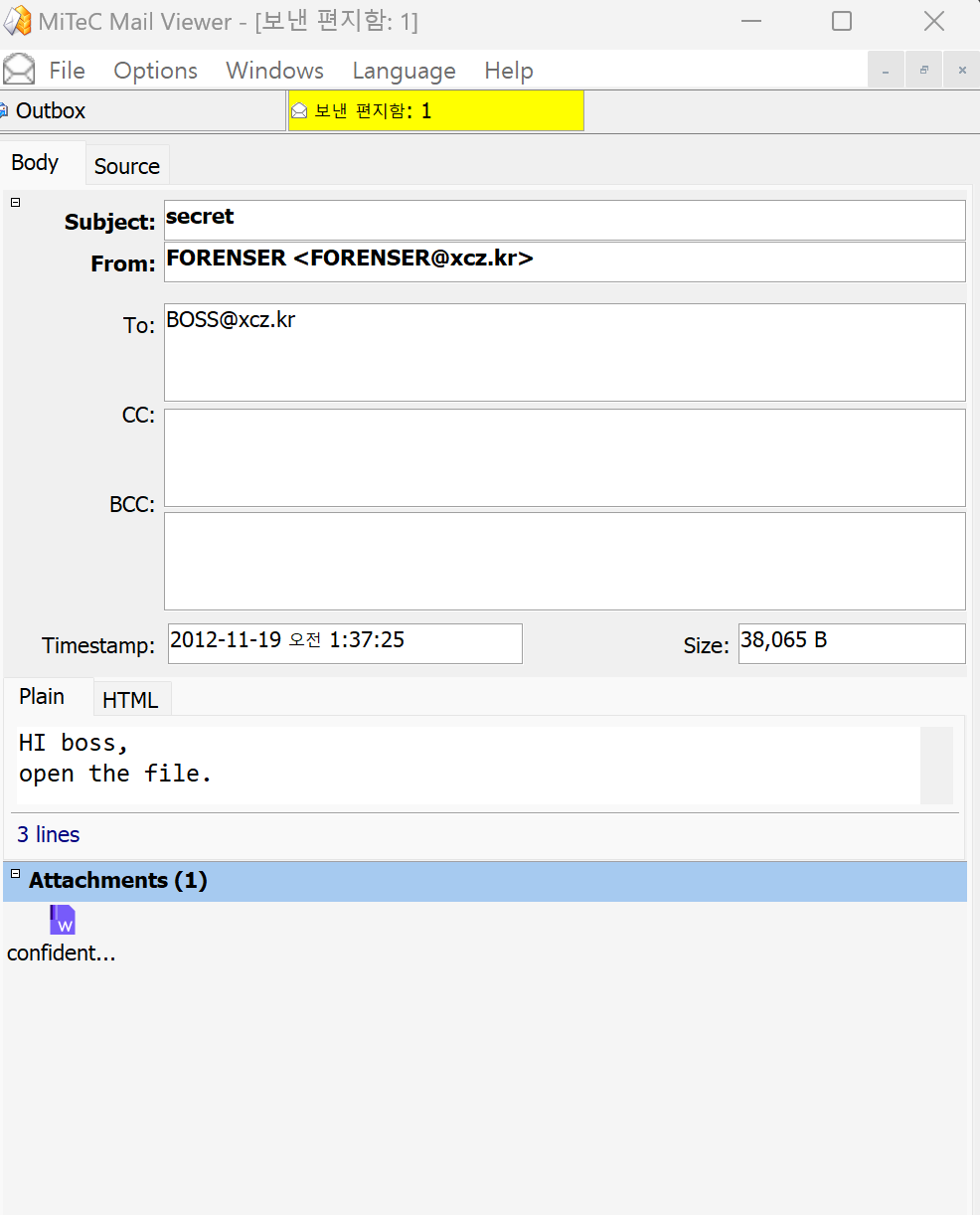
[사진 4] confidential.doc가 첨부되어 있다는 증거

Attachment – “confidential.doc”가 [사진 3]의 아래에 나와있어 결정적인 증거라고 확신했다. 이 이메일을 추출하여 열어보면 confidential.doc도 함께 열릴 것으로 추측된다.

Outbox.dbx를 추출하여 확장자명은 .eml로 바꿔준 후 Outlook 메일 프로그램으로 열려고 시도했다.

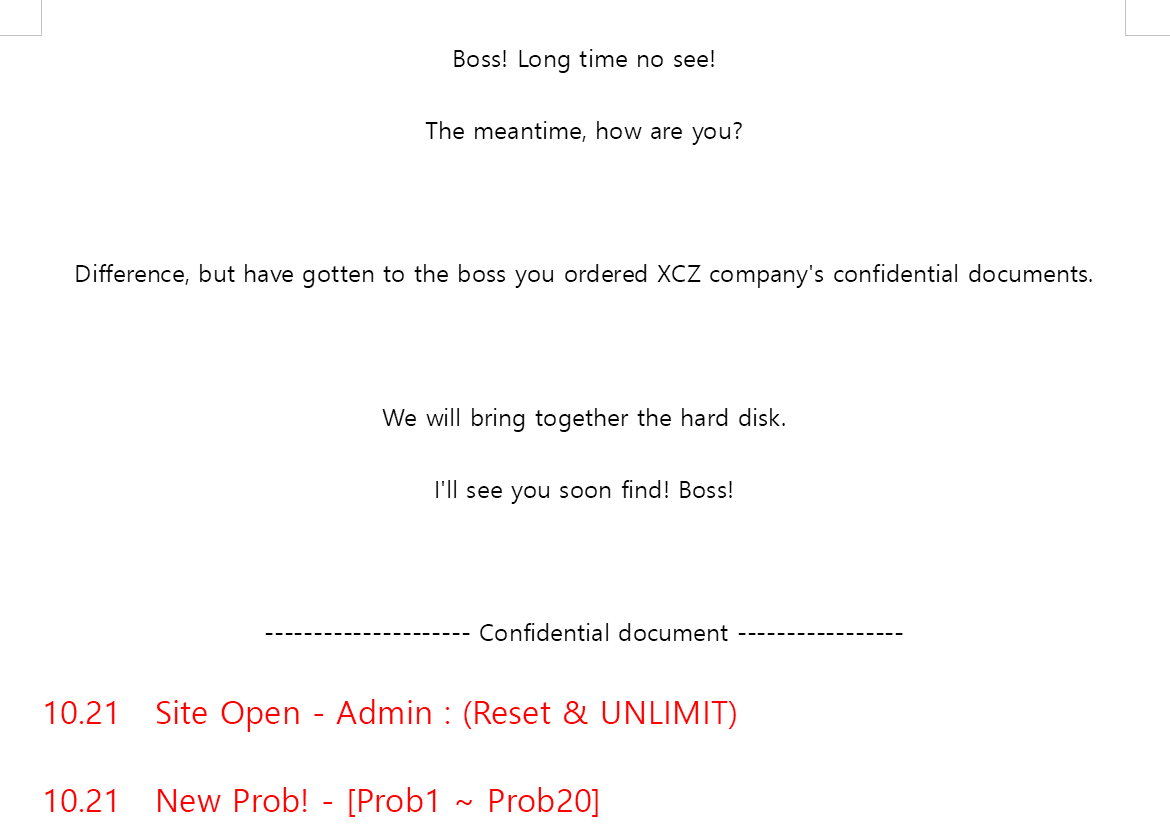
하지만, 확장자명을 바꾸는 건 역시나 한계가 뚜렷했다. 수신자와 발신자만 명시되어 있고, subject에 secret이 빠져있고, confidential.doc를 다운받아서 여는 것은 불가능했다.

따라서 DBX viewer를 다운 받아 [사진 2]의 Outbox.dbx를 열어보았고,



[사진 5] Outbox.dbx로 이메일 복원

첨부파일인 confidential.doc를 열면,



[사진 6] confidential.doc 내용

맨 아래 빨간색 글자 옆을 드래그 한 후, 글씨 색을 바꾸면 key값을 구할 수 있다.

# **Flag**

Flag = Out10OkExpr3s5M4i1

# **별도 첨부**

# **Reference**