




작성자	허은정
분석 일자	2024-05-09
작성 일자	2024-05-09
분석 대상	PDF
문서 버전	1
작성자 E-mail	dmswjd4315@yonsei.ac. kr

0. 목차

- 1. 문제3
- 2. 분석 도구3
- 3. 환경3
- 4. Write-Up.....4
- 5. Flag..... 12
- 6. 별도 첨부 13
- 7. Reference 14

1. 문제

URL	http://suninatas.com/challenge/web31/web31.asp
문제 내용	<p>*안내: 본 PDF 파일은 PC에 유해한 작업을 하지 않습니다. 단순 문제 풀이용입니다. 악성코드가 첨부된 PDF를 분석하여 Flag를 찾으세요.</p> <p>인증키 형식: lowercase(MD5(Flag))</p>
문제 파일	<div>  <div> Hello_SuNiNaTaS. pdf </div> </div>
문제 유형	File forensics
난이도	2/ 5

2. 분석 도구

도구명	다운로드 링크	Version
PDF stream Dumper	http://sandsprite.com/blogs/index.php?uid=7&pid=57	v0.9.624

3. 환경

OS
Window 11 64-bit

4. Write-Up

파일명	Hello_SuNiNaTaS.pdf
용량	24.6KB (25,232 바이트)
SHA256	d1d3fd81952ffab1d52509a0d6dd7bcd27017e082ec99d4b0c4a0004577c4fdf
Timestamp	2024-05-09 16:06:49

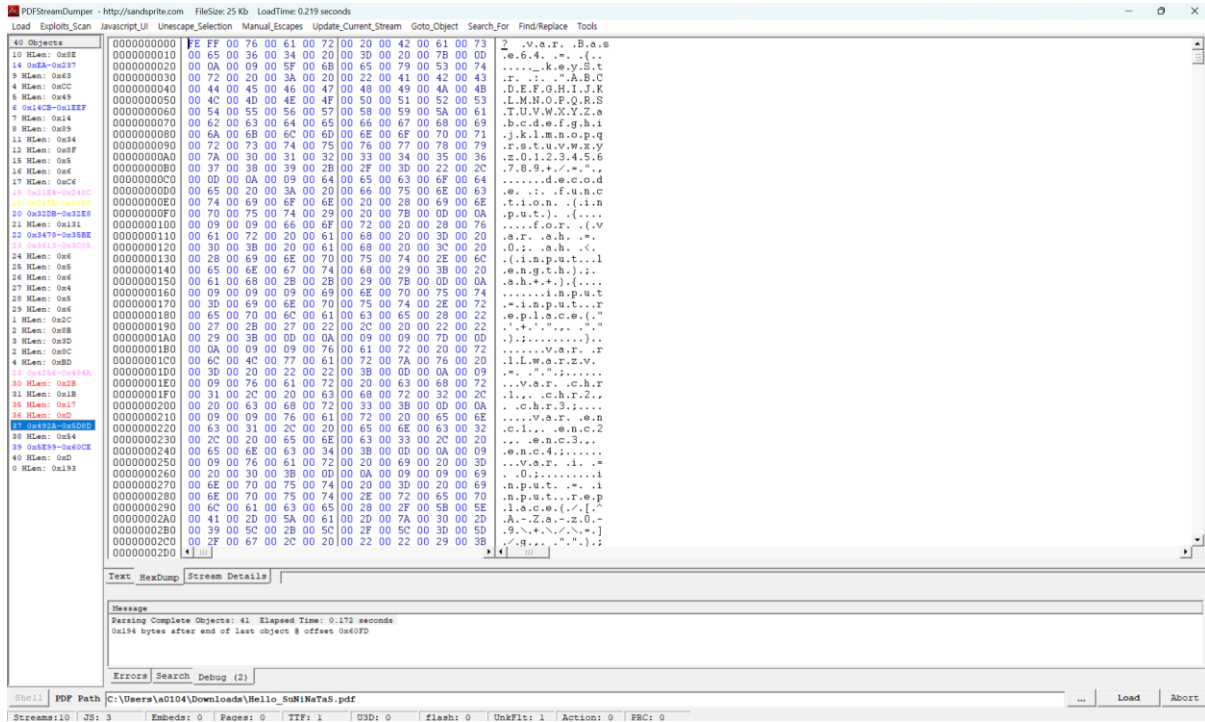
문제를 보면 PDF 가 존재하여 다운로드 받았습니다.



[사진 1] 문제 PDF 내용

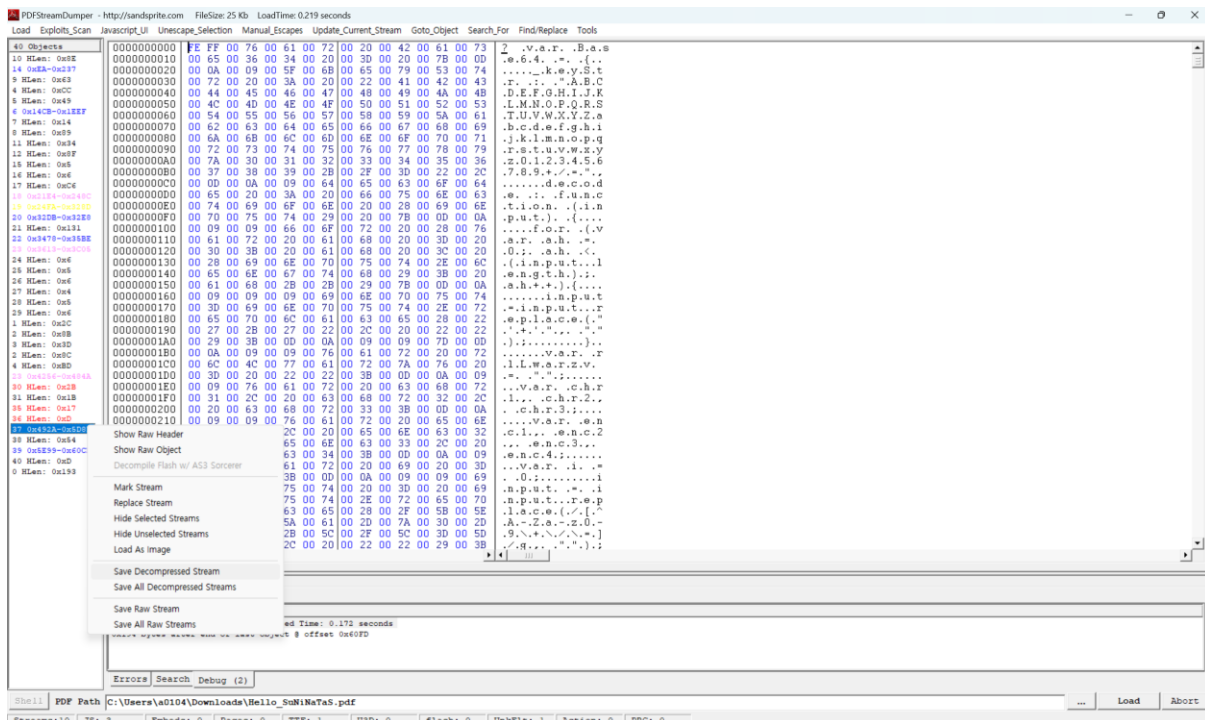
문제파일을 다운 받은 후 열면 [사진 1]과 같은 내용이 나오고 다른 문제점을 찾지 못하였다. 이를 봤을 때 pdf를 분석할 프로그램이 필요할 것이라 생각하여 pdf Steam Dumper를 이용하였다.

[WHS-2] .iso



[사진 2] pdf Stream Dumper을 활용하여 본 Hello_SuNiNaTas.pdf

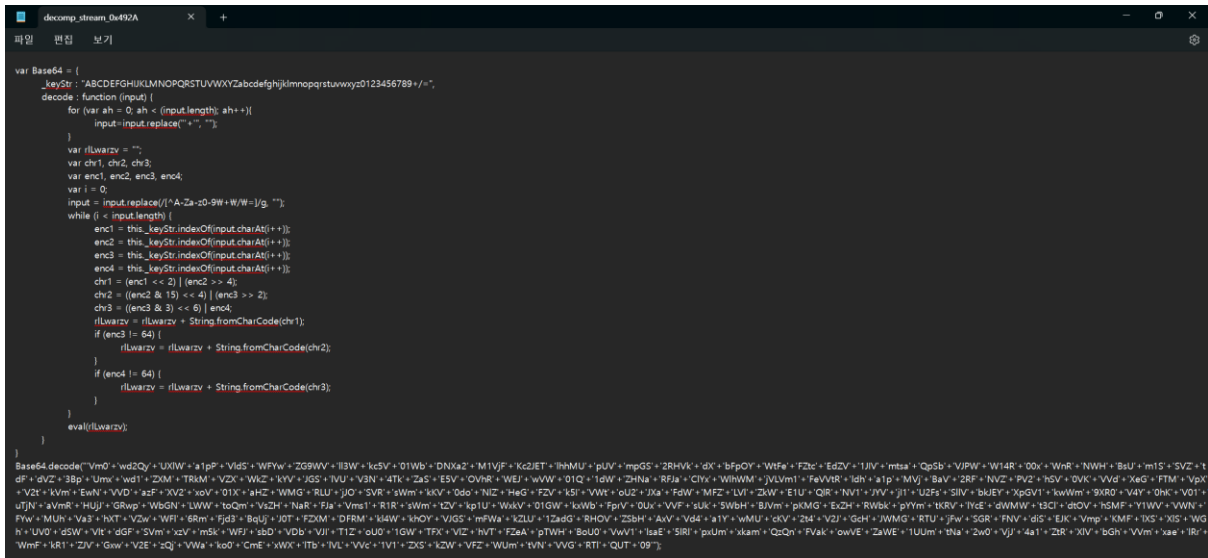
Pdf Steam Dumper을 활용하여 Hello_SuNiNaTas를 본 결과, 37번째 object에서 자바스크립트 코드가 있다는 것을 확인할 수 있었습니다.



[사진 3] 37번 object Save Decompressed Steam

[WHS-2] .iso

[사진 4] 추출한 txt문서



```

var Base64 = {
  _keyStr: "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=",
  decode: function (input) {
    for (var ah = 0; ah < (input.length); ah++) {
      input = input.replace(" ", "");
    }
    var rLuarzrv = "";
    var chr1, chr2, chr3;
    var enc1, enc2, enc3, enc4;
    var i = 0;
    input = input.replace(/[\t\r\n\A-Za-z0-9\W\/=]/g, "");
    while (i < input.length) {
      enc1 = this._keyStr.indexOf(input.charAt(i));
      enc2 = this._keyStr.indexOf(input.charAt(i+1));
      enc3 = this._keyStr.indexOf(input.charAt(i+2));
      enc4 = this._keyStr.indexOf(input.charAt(i+3));
      chr1 = (enc1 << 2) | (enc2 >> 4);
      chr2 = ((enc2 & 15) << 4) | (enc3 >> 2);
      chr3 = ((enc3 & 3) << 6) | enc4;
      rLuarzrv = rLuarzrv + String.fromCharCode(chr1);
      if (enc3 != 64) {
        rLuarzrv = rLuarzrv + String.fromCharCode(chr2);
      }
      if (enc4 != 64) {
        rLuarzrv = rLuarzrv + String.fromCharCode(chr3);
      }
      i = i + 4;
    }
    eval(rLuarzrv);
  }
}

Base64.decode("Vm0dw2QyUXlWapPVldSWFYwZG9WVlI3Wkc5V01WbDNXa2M1VjFKc2JETlhhMUUpUVmpGS2RHVkdXbFp0YWtFeFZtcEdZV1JlVmtsaQpSbVJPWW14R00xWnRnWHBsUm1SSVZtdFdVZ3BpUmxwd1ZXMT RkMVZXWkZkYVJGS1VUV3N4TkZaSE5V0VhRWEJwVW01Q1dWZHNaRFJaClYxWIhWMjVlVW1FeVvtRldha1pMVjBaV2RFNVZPV2hSV0VKVvdXegFTMpXV2tkVmEwNVVDazFXV2xoV01XaHZWMGRlUjJ0SVRsWmkKV0doNlZHeGFZVks1VWtoU2JXaFdwMFZLVlZkWE1UQlRNV1JYVj1lU2FsSl1VbkJEYXpGV1kwWm9XROV4Y0hkV01uTjNaVmRHUjJGRWpWbGNLWWtoQmVsZHNaRFJaVms1R1RsWmtZVkp1UWxkV01GWkxWbFprVOUxVVFfSuk5WbHBjVmpKMGEZHRWbKpYYmtKRVIYcEdWMMt3CldtOVhSMFY1WVWNFYwUUhVa3hXTVZwWF16RmFjd3BqUjJ0TFZXMDFRMk14Wkh0YVVGSmFWakZLU1ZadGRHOVZSbHAXVVd4a1YwMUckV2t4V2JGcHJWMGRtUjFwSGRFNVdiSEJKVmpKMFIxSXlSWGhUV0dSWWltdGFVmxzVm5kWFJsbDVDVbVJlT1ZoU01GWTfXVlZhVTFZeApTWHBoU0VwV1lsaE5lRlpxUmXkamQzQhFvakowVEZaWE1UUmNa2w0VjJ4a1ZtRXlVbGhVmxae1RrWmFkR1ZJVGVxwV2EzQjVWakoOCmExWXITb1VLVvc1V1ZXSkZWfZWUmtVNVVGRt1QUT09")

```

[사진 5] 추출한 txt 문서 내용

37번째 object를 Save Decompressed Steam 한 후, 파일을 메모장에서 열어본 결과 위의 코드 부분은 base64 디코딩 코드임을 확인하였고

Vm0dw2QyUXlWapPVldSWFYwZG9WVlI3Wkc5V01WbDNXa2M1VjFKc2JETlhhMUUpUVmpGS2RHVkdXbFp0YWtFeFZtcEdZV1JlVmtsaQpSbVJPWW14R00xWnRnWHBsUm1SSVZtdFdVZ3BpUmxwd1ZXMT RkMVZXWkZkYVJGS1VUV3N4TkZaSE5V0VhRWEJwVW01Q1dWZHNaRFJaClYxWIhWMjVlVW1FeVvtRldha1pMVjBaV2RFNVZPV2hSV0VKVvdXegFTMpXV2tkVmEwNVVDazFXV2xoV01XaHZWMGRlUjJ0SVRsWmkKV0doNlZHeGFZVks1VWtoU2JXaFdwMFZLVlZkWE1UQlRNV1JYVj1lU2FsSl1VbkJEYXpGV1kwWm9XROV4Y0hkV01uTjNaVmRHUjJGRWpWbGNLWWtoQmVsZHNaRFJaVms1R1RsWmtZVkp1UWxkV01GWkxWbFprVOUxVVFfSuk5WbHBjVmpKMGEZHRWbKpYYmtKRVIYcEdWMMt3CldtOVhSMFY1WVWNFYwUUhVa3hXTVZwWF16RmFjd3BqUjJ0TFZXMDFRMk14Wkh0YVVGSmFWakZLU1ZadGRHOVZSbHAXVVd4a1YwMUckV2t4V2JGcHJWMGRtUjFwSGRFNVdiSEJKVmpKMFIxSXlSWGhUV0dSWWltdGFVmxzVm5kWFJsbDVDVbVJlT1ZoU01GWTfXVlZhVTFZeApTWHBoU0VwV1lsaE5lRlpxUmXkamQzQhFvakowVEZaWE1UUmNa2w0VjJ4a1ZtRXlVbGhVmxae1RrWmFkR1ZJVGVxwV2EzQjVWakoOCmExWXITb1VLVvc1V1ZXSkZWfZWUmtVNVVGRt1QUT09

해당 문자열을 Base64 디코딩해 주는 사이트에서 돌려보았습니다.

[WHS-2] .iso

Decode from Base64 format

Simply enter your data then push the decode button.

Vm0wd2QyUXlWa1pPVIldSWFYwZG9WVlI3Wkc5V01WbDNXa2M1VjFKc2JETlhMUUpUVmpGS2RHVkdXbFpOYWtFeFZtcEdZV1JlVmtsAqSbVJPWW14R00xWnRNWHBsUm1SSVZtdFdVZ3BpUmxwd1ZXMTRkMVZXWkZkYVJGSiVUV3N4TkZaSE5VOvhRWEJwVW01Q1dWZHNARFJaCIYxWlhWMjVlVn1FeVtRidha1pMVjBaV2RfNVZPV2hSV0VKVvdXGFTMVpXV2tkVmEwNVVDazFXV2xoV01XaHZWMGRlUjJOSVRSWmkKV0doNIZHeGFZVn5lVWtoU2JXaFdWMFZLVIZkWE1UQIRNV1JYVjI1U2FsSIlVbkJEYXpGV1kwWm9XR0V4Y0hkV01uTjNaVmRHUjJGRwpWbGNLWWtoQmVsZHNARFJaVms1R1RsWmtZVkp1UWxkV01GWkxWbFprV0UxVVF5Uk5WbHBjVmpKMGExZHRWbKpYYmtKRVIYcEdWMWt3CldtOVhSMFY1WVVVNFYwMUhVa3hXTVZwWFI6RmFjd3BqUjJ0TFZXMDFRMkl4WkhOYVJGSmFWakZLU1ZadGRHOVZSbHAXVvd4a1YwMUcKV2t4V2JGcHJWMGRtUjFwSGRfNVdiSEJkVmpKMFIxSXlSWGhUV0dSWVltdGF5VmxzVm5kWFJsbDVBbVJIT1ZoU01GWTFXVIZhVTFZeApTWHBoU0VwV1IsaE5lRlpxUmxkamQzQnFvakowVEZaWE1UUmtna2w0VjJ4a1ZlRXlVbGhVmxaelRlRmFkr1ZJVGxwV2EzQjVWako0CmExWXTbVlVlc1V1ZXSkZWVfZWUmtVNVVGRTlQUtO9

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8

Source character set.

☐

Decode each line separately (useful for when you have multiple entries).

Live mode OFF

Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE >

Decodes your data into the area below.

Vm0wd2QyVkZOVWRXV0doVYwZG9WMVl3Wkc5V1JsbDNXa1JTVjFKdGVGWlZNaKExVmpGYWRHVkIiRmROYmxGM1ZtMxpIRmRlVmtWUgpiRlpwVW14d1VWZFdaRFJUTWsxNFZHNu9XQXBpUm5CWVdsZDRZV1ZXV25KVmEYUmFWakZLV0ZWdE5VOWhRWEJUWWxaS1ZWWkdVa05UCk1WWlhWMWWhV0dKR2NITIZlWGh6VGxaYVNHUkhSbWhWV0VKVvdXMTBtMWRXV25SaJYUnBDazFWY0ZoWGEhcHJWMnN3ZVdGR2FGVlcYkhBelDsZDRZVn5lZGZlZkYVJlUjQldWMFZLVIZkWE1UQIRNVlplVjJ0a1dtVnJXbkJEYXpGV1kwWm9XR0V5YUUV4V01HUkxWMVpXYzFacwpjR2tLVW01Q2lxZHNARFJaVjFKSVZldG9VRlp1UWxkV01GWkxWbFprV0dSR1pHdE5WbHBjVjJ0YyWlyRXhTWGRYYmtaRVlsVndXRlI5CmRHOvhSMFY1WVVVaU1YxSXphSEpWYlhlNeFzQldjd3BqUjJ0TFZXMTRkMkl4V2xkVmEyUlhUVIZzTkZadGVlTlplWa3B5VjJ4a1YySnUKUW5WVWJFVTVVRkU5UFE9PQ==

[사진 6] Base64 디코딩

Decode from Base64 format

Simply enter your data then push the decode button.

SSBhbSBzb3JyeSwgVGhpcyBpcyBub3QgS2V5fiEh

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8

Source character set.

☐

Decode each line separately (useful for when you have multiple entries).

Live mode OFF

Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE >

Decodes your data into the area below.

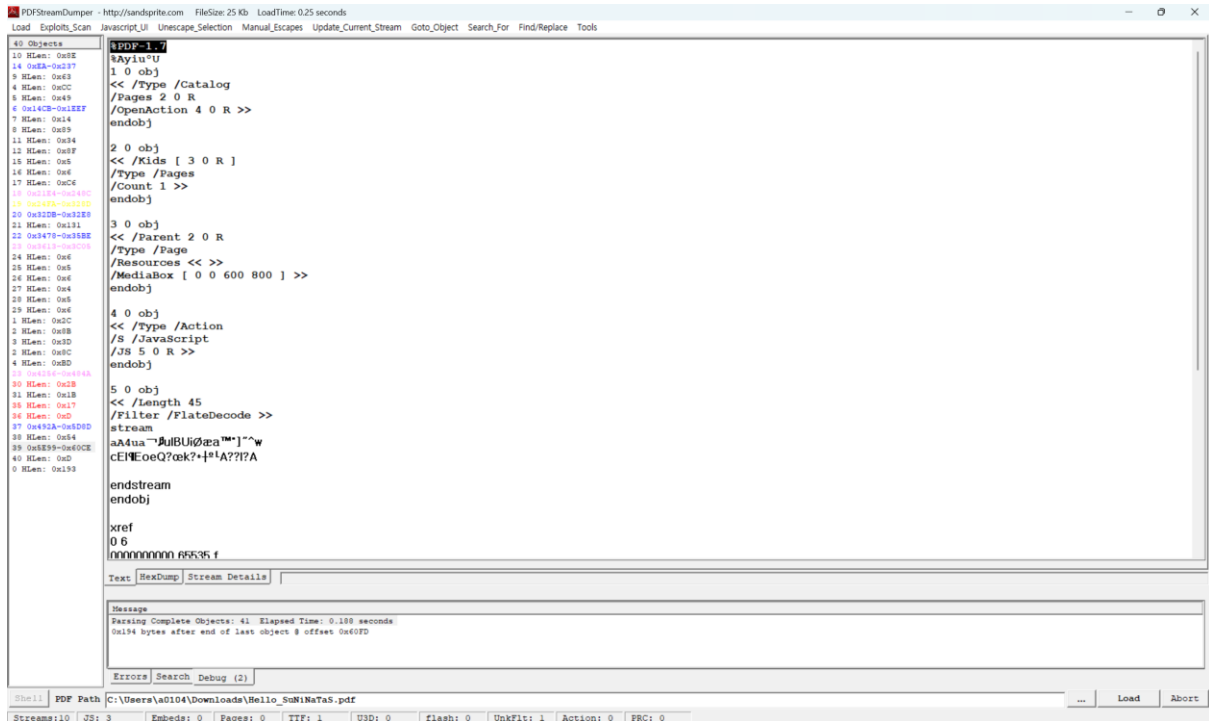
I am sorry, This is not Key~!!

7

[WHS-2] .iso

[사진 7] Base64 디코딩 결과

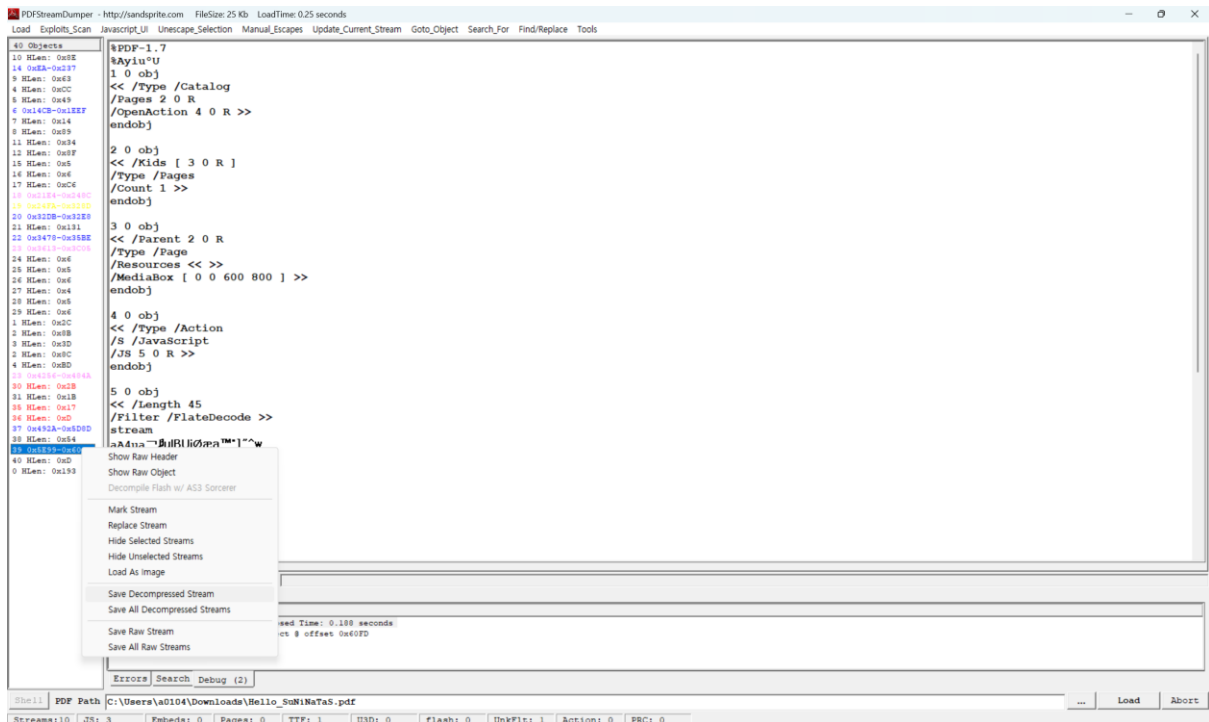
Base64를 계속 복호화 시도해본 결과 다음과 같은 문구가 나오게 되었고 이를 통해 이것은 key 값이 아니라는 것을 알게 되었습니다. 따라서, 다시 PDFStreamDumper로 돌아가보았습니다.



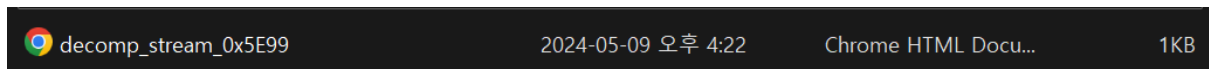
[사진 8] 39 object 내용

39번째 object에서 PDF 헤더를 확인할 수 있었고 이를 통해 PDF 안에 PDF가 하나 더 있다는 것을 알게 되었습니다.

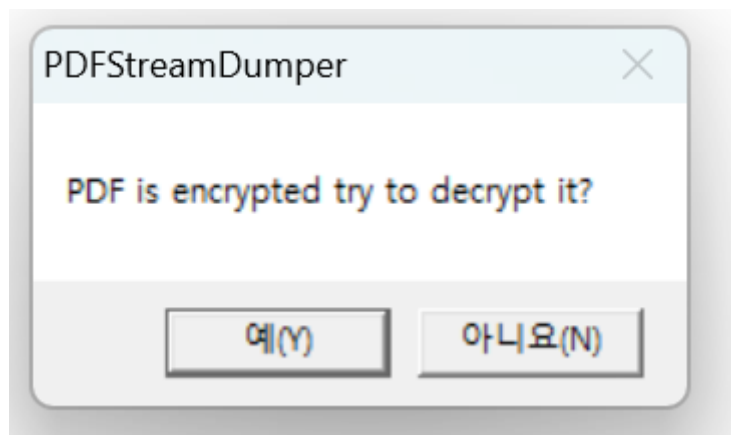
[WHS-2] .iso



[사진 9] 39 object Save Decompressed Stream




[사진 10] 추출한 PDF



[사진 11] 추출한 PDF를 PDF Steam Dumper에 연 사진

39번째 object도 save Decompressed Stream을 한 후, PDF Stream Dumper로 열어보았더니 PDF가 잠겨 있다는 것을 알 수 있습니다.

PDF 잠금 해제




파일 선택

▼

또는 PDF를 여기로 끌어 놓으세요

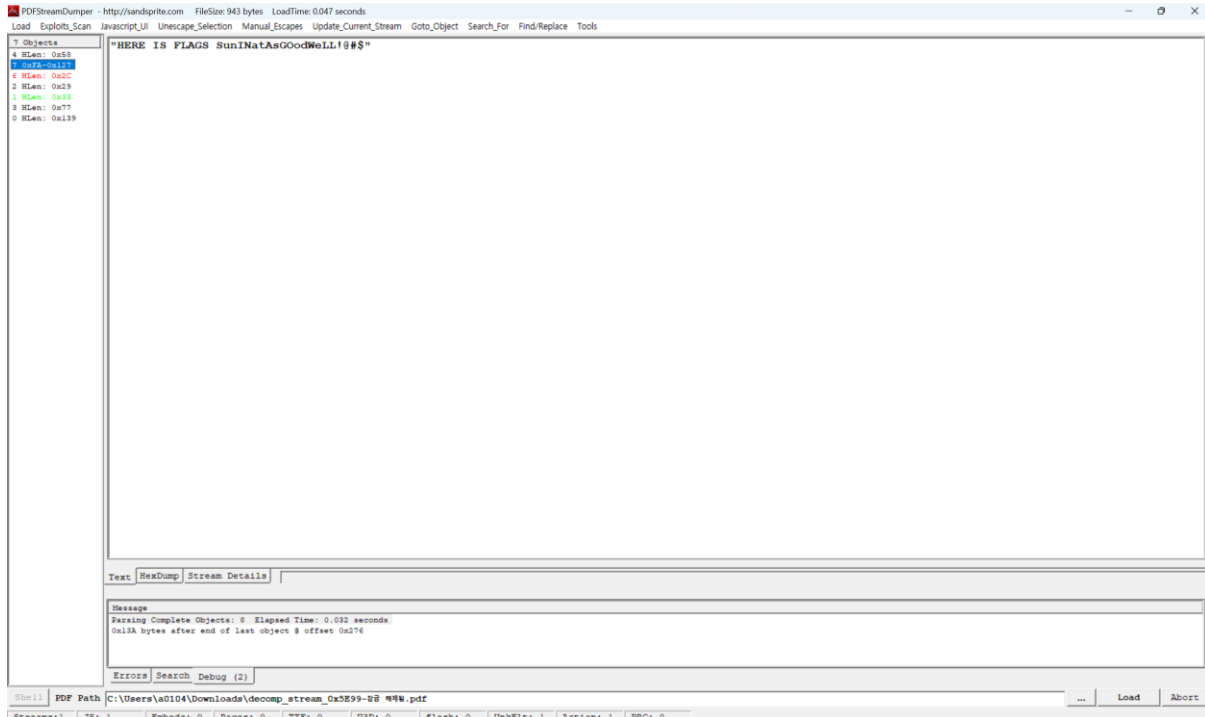
- 파일 크기 제한 및 광고 워터마크 없음 - PDF에 설정된 불필요한 비밀번호를 제거할 수 있는 무료 온라인 비밀번호 제거 툴로, 사용법도 간단합니다.
- 가입이 필요 없음
 - PDF 파일을 몇 초 만에 잠금 해제
 - TLS 암호화를 통해 안전하게 문서 처리

[사진 12] PDF 잠금 푼 사이트

 decomp_stream_0x5E99-잠금 해제됨	2024-05-09 오후 4:23	Chrome HTML Docu...	1KB
---	--------------------	---------------------	-----

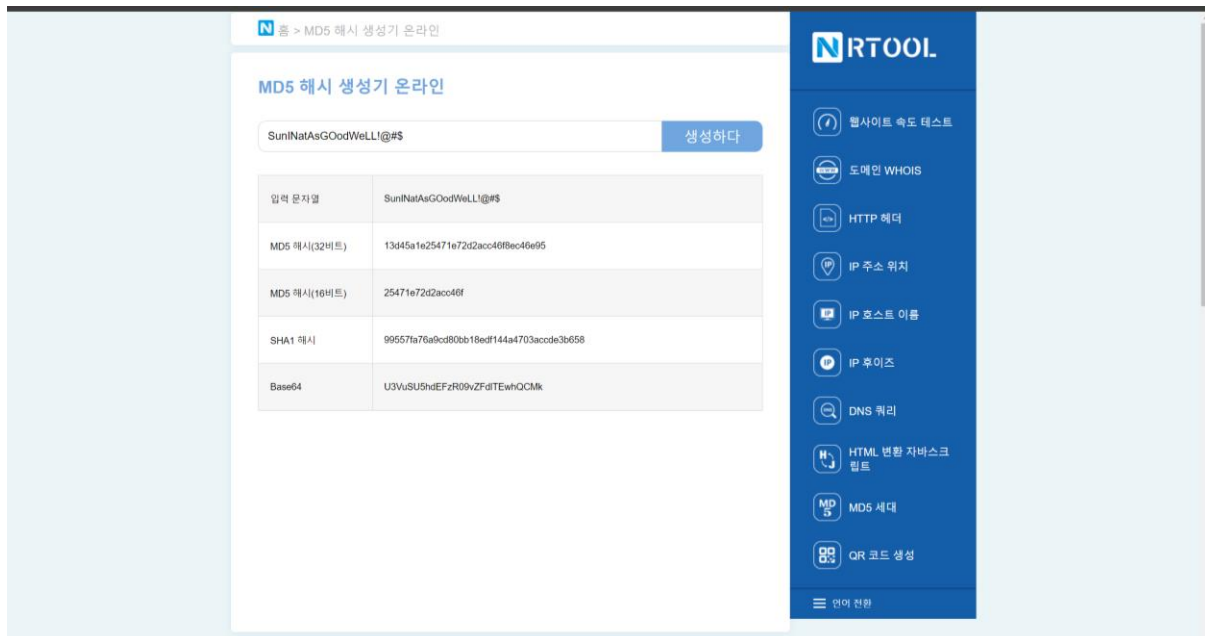
[사진 13] 잠금 풀린 PDF

[WHS-2] .iso



[사진 14] 해당 PDF를 PDF Stream Dumper로 연 내용

[사진12]를 통해 잠긴 PDF 파일을 풀고, 다시 PDF Stream Dumper을 이용하여 확인해보았습니다. 해당 PDF의 7번째 object에서 Flag 값을 찾을 수 있었습니다.



[사진 15] flag값을 MD5시킨 결과

해당 flag값인 `SunINatAsGooDWeLL!@#$`을 [사진15]에서 MD5 인코딩 시켜보면 `13d45a1e25471e72d2acc46f8ec46e95`라는 auth key가 나오게 됩니다.

5. Flag

13d45a1e25471e72d2acc46f8ec46e95

6. 별도 첨부

7. Reference

- [URL]