[포렌식툴 분석 보고서]

[PDFStreamDumper]

작성일	2025.05.26
작성자	김신아
검토자	김예은

목차

Ⅰ. 툴 기본 정보

항목	내용
툴 이름	pdfstreamdumper
분석 카테고리	파일 사용/조작, 사용자 행위
사용 버전	v0.9.624
다운로드 경로	https://sandsprite.com/blogs/index.php?uid=7&pid=57
지원 포맷	PDF문서 포맷 , 임베디드 JavaScript , 스크립트 스트림 등

[표1. 툴 기본 정보]

Ⅱ. 툴 소개 및 목적

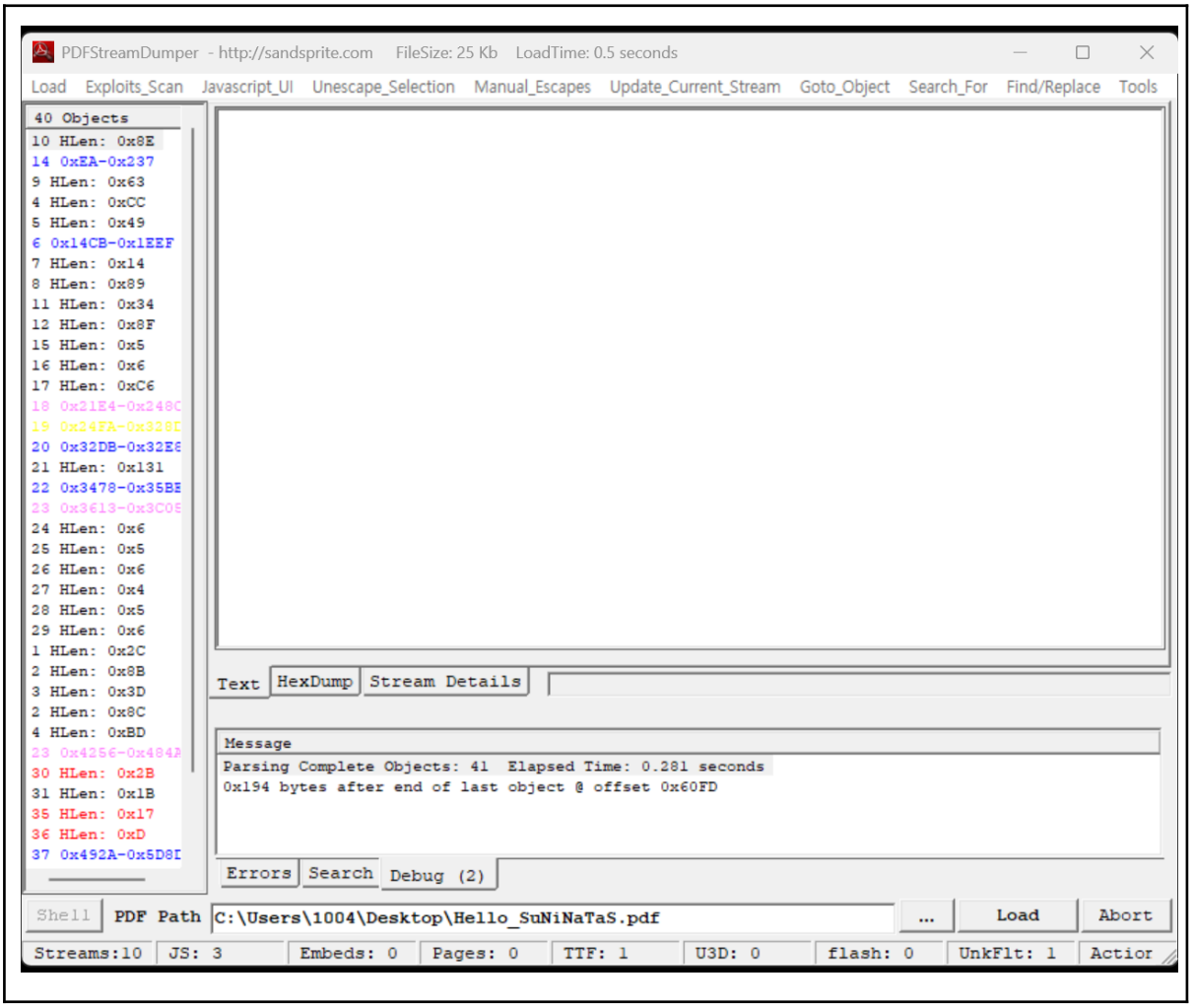
1. 악성 PDF 문서를 정적 분석하기 위한 도구이다.
2. PDF 내부에 숨겨진 JavaScript, 임베디드 객체, exploit 코드 등을 탐지하고 분석할 수 있는 기능 제공한다.

Ⅲ. 설치 매뉴얼

1. 지원 운영체제 : Windows 운영체제 전용 도구
2. 설치 방식
    1) 최신 버전 PDFStreamDumper.zip 파일을 클릭하여 다운로드
    2) .zip 파일을 원하는 위치에 압축 해제
    3) 압축을 푼 폴더 내에서 PDFStreamDumper.exe 실행 파일 클릭하여 실행

Ⅳ. 주요 기능 및 사용법

기능1. PDF 오브젝트 구조 분석



[그림1. PDF 오브젝트 구조 분석 화면]

1) PDFStreamDumper는 PDF 파일의 내부 오브젝트 구조를 계층적으로 분석할 수 있다.

2) 사용법

(1) PDF 파일 열기 (File > Open PDF)

(2) 좌측 패널에서 오브젝트 리스트 확인

(3) 각 오브젝트 클릭 시 상세 정보 및 연결 구조 확인 가능

기능2. 스트림 분석

1) PDF 내부의 스트림 객체를 디코딩 및 분석하여 악성 코드 여부를 확인한다.

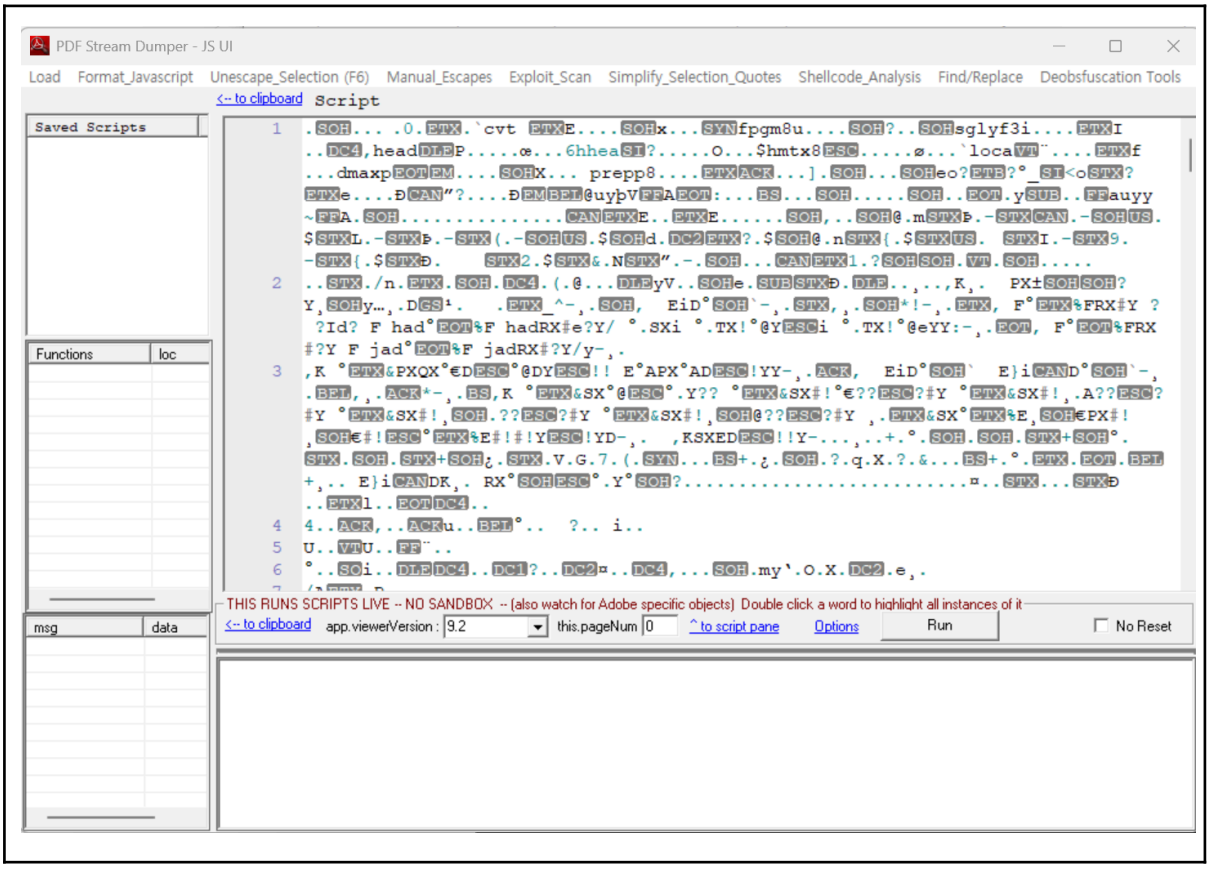
2) 사용법

(1) 분석 대상 스트림 선택

(2) 상단 메뉴에서 Stream > Dump Stream 선택

(3) 스트림 내용이 자동 디코딩되어 확인 가능

기능3. JavaScript 분석



[그림2. JavaScript 코드 분석 화면]

1) PDF에 포함된 JavaScript 코드의 존재 여부 및 내용을 확인할 수 있다.

2) 사용법

(1) JavaScript 포함 오브젝트 선택

(2) JS Analysis 탭에서 스크립트 코드 자동 추출

(3) Suspicious 항목 표시로 의심 코드 식별

기능4. Exploit 스캔

1) 알려진 취약점을 악용하는 exploit을 탐지하는 기능이다.

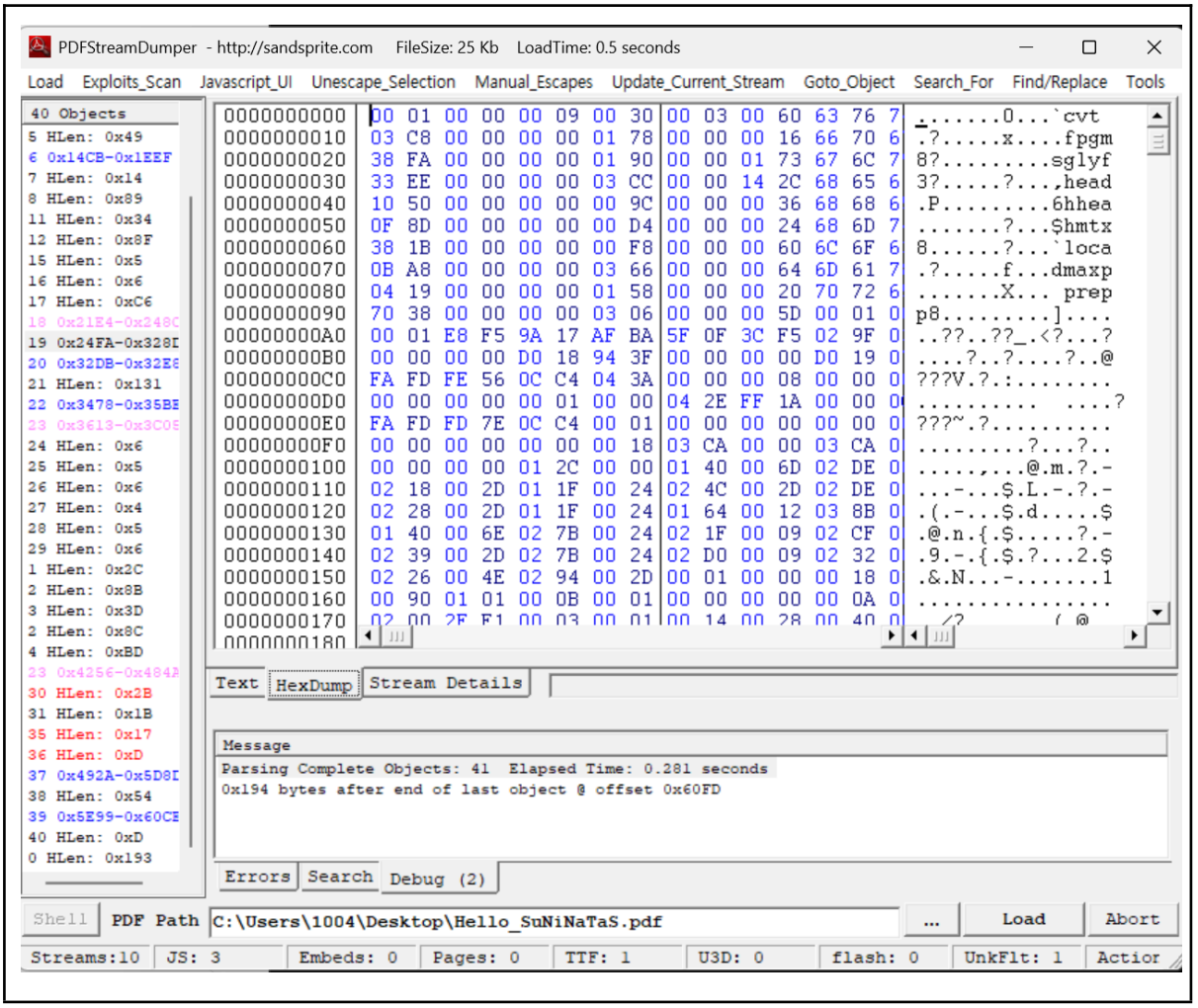
2) 사용법

(1) Tools > Scan for Known Exploits 클릭

(2) 자동 스캔 후 결과 리스트 제공

(3) 발견된 exploit 코드 위치와 설명 표시됨

기능5. Hex Viewer 및 파일 추출



[그림3. Hex Viewer 및 파일 추출 화면]

1) PDF 내 바이너리 데이터를 Hex 뷰로 확인하고 임베디드 파일을 추출할 수 있다.
2) 사용법
    (1) 오브젝트 선택 후 Hex View 탭 클릭
    (2) 필요한 데이터 범위 선택 후 Extract 기능 사용
    (3) 추출된 파일은 로컬로 저장 가능

Ⅴ. 참고 자료

[1] https://hackingstudypad.tistory.com/340