침해사고 당한 컴퓨터에 대한 Live Disk Data 수집 자동화 IR 스크립트

**LDDC**

**(Live Disk Data Collector)   
TEST REPORT**

Team \_ Digital Forensic Study

**목차**

[**1.** **테스트 개요** 2](#_Toc158744847)

[**1.1.** **테스트 목적** 2](#_Toc158744848)

[**1.2.** **테스트 PC 환경** 2](#_Toc158744849)

[**1.3.** **테스트 셋** 2](#_Toc158744850)

[**2.** **상세 테스트 내용** 2](#_Toc158744851)

[**2.1.** **입력 시험** 3](#_Toc158744852)

[**2.2.** **분석 시험** 3](#_Toc158744853)

[**3.** **테스트** 4](#_Toc158744854)

[**3.1.** **입력 시험 결과** 4](#_Toc158744855)

[**3.2.** **분석 시험 결과** 9](#_Toc158744856)

# **테스트 개요**

침해사고대응을 위한 라이브 상태의 디스크 데이터 수집 자동화 IR 스크립트(이하 ‘LDDC’)를 테스트하고자 한다. 라이브 디스크 데이터를 수집하고 분석하는 IR 스크립트를 개발하여 스크립트의 효율성, 정확성 및 신뢰성을 평가한다.

## **테스트 목적**

LDDC IR 스크립트의 수집 및 분석 기능 정확성 평가

LDDC IR 스크립트의 안정성 및 신뢰성 평가

## **테스트 PC 환경**

|  |  |  |
| --- | --- | --- |
|  | **PC1** | **PC2** |
| **OS** | Windows 11 Home | Windows 11 Pro |
| **프로세서** | Intel i7 9th Gen | Intel i5 13th Gen |
| **IDE** | VsCode | VsCode |

## **테스트 셋**

|  |  |  |
| --- | --- | --- |
| **Live Disk Data** | **TestSet1** | **TestSet2** |
| **OS** | Windows 11 Home | Windows 11 Pro |

# **상세 테스트 내용**

테스트 진행은 다음과 같은 방법으로 진행되며, 입력 시험과 분석 시험으로 나누어 진행한다.

1. 테스트 PC에서 LDDC실행
2. 실행된 LDDC에서 선택적으로 라이브 디스크 데이터 수집
3. 수집된 테스트 PC의 라이브 디스크 데이터 검증 및 스크립트 제작 흐름도 평가
4. LDDC의 성능, 속도 및 정확성 평가
5. 사용자 경험 향상을 위한 피드백 수집

## **입력 시험**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **일련 번호** | **테스트 번호** | **테스트 항목** | **상세 설명** | **담당자** |
| 1 | 111 | LDDC 실행 및 interface 테스트  (set 변수, :REDO) | 정상적인 LDDC 실행 여부와 선택 interface 정상 표시 여부 확인 | 김민서, 최원혁 |
| 2 | 121 | all data정상 작동 여부 테스트  (:1) | 1번 all data 정상 작동 여부, 흐름 및 수집 완료 확인 + 초기 interface로 돌아가는지 확인 | 김민서, 최원혁 |
| 3 | 131 | Volatile data 정상 작동 여부 테스트  (:2) | 2번 Volatile data 정상 작동 여부, 흐름 및 수집 완료 확인 + 초기 interface로 돌아가는지 확인 | 김민서, 최원혁 |
| 4 | 141 | non-volatile data정상 작동 여부 테스트  (:3) | 3번 non-volatile data정상 작동 여부, 흐름 및 수집 완료 확인 + 초기 interface로 돌아가는지 확인 | 김민서, 최원혁 |
| 5 | 151 | Program end 정상 작동 여부 테스트  (:4) | 4번 Program end 정상 작동 여부 확인 + LDDC 종료 여부 확인 | 김민서, 최원혁 |

## **분석 시험**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **일련 번호** | **테스트 번호** | **테스트 항목** | **상세 설명** | **담당자** |
| 1 | 211 | All data데이터 출력 파일 확인 | LDDC가 All data에 설정된 모든 라이브 디스크 데이터를 정상적으로 출력했는지 파일 확인 | 김민서, 최원혁 |
| 2 | 221 | Volatile data데이터 출력 파일 확인 | LDDC가 Volatile data에 설정된 모든 라이브 디스크 데이터를 정상적으로 출력했는지 파일 확인 | 김민서, 최원혁 |
| 3 | 231 | non-volatile data데이터 출력 파일 확인 | LDDC가 non-volatile data에 설정된 모든 라이브 디스크 데이터를 정상적으로 출력했는지 파일 확인 | 김민서, 최원혁 |

# **테스트**

## **입력 시험 결과**

|  |  |  |  |
| --- | --- | --- | --- |
| **테스트 번호** | **테스트 종류** | **테스트 항목** | **담당자** |
| 111 | 단위 테스트 | 실행 및 interface | 김민서, 최원혁 |
| **테스트 목적** | | | |
| 정상적인 LDDC 실행 여부 및 선택 interface 정상 표시 여부 확인 | | | |
| **테스트 환경** | | | |
| Windows 11 | | | |
| **테스트 케이스** | | | |
| 1. LDDC 실행 | | | |
| **테스트 결과** | | | |
| LDDC 정상적으로 실행되었으며, interface 또한 정상적으로 구현됨. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **테스트 번호** | **테스트 종류** | **테스트 항목** | **담당자** |
| 121 | 단위 테스트 | All data정상 작동 여부 | 김민서, 최원혁 |
| **테스트 목적** | | | |
| 1번 All data정상 작동 여부, 흐름 및 수집 완료 확인 + 초기 interface로 돌아가는지 확인 | | | |
| **테스트 환경** | | | |
| Windows 11 | | | |
| **테스트 케이스** | | | |
| 1. LDDC 실행 후 ‘1’ (All data) 입력 2. 디스크 데이터 파일 정상적으로 추출되었는지 확인 3. 초기 interface로 돌아갔는지 확인 | | | |
| **테스트 결과** | | | |
| LDDC 정상적으로 실행됨.  ‘1’ 입력 시 전체적인 라이브 디스크 데이터 (vol, nonvol) 정상적으로 추출됨.  초기 interface로 정상적으로 돌아감. | | | |

| **테스트 번호** | **테스트 종류** | **테스트 항목** | **담당자** |
| --- | --- | --- | --- |
| 131 | 단위 테스트 | Volatile data정상 작동 여부 | 김민서, 최원혁 |
| **테스트 목적** | | | |
| 2번 Volatile data정상 작동 여부, 흐름 및 수집 완료 확인 + 초기 interface로 돌아가는지 확인 | | | |
| **테스트 환경** | | | |
| Windows 11 | | | |
| **테스트 케이스** | | | |
| 1. LDDC 실행 후 ‘2’ (Volatile data) 입력 2. 디스크 데이터 파일 정상적으로 추출되었는지 확인 3. 초기 interface로 돌아갔는지 확인 | | | |
| **테스트 결과** | | | |
| LDDC 정상적으로 실행됨.  ‘2’ 입력 시 휘발성 라이브 디스크 데이터 (vol) 정상적으로 추출됨.  초기 interface로 정상적으로 돌아감. | | | |

| **테스트 번호** | **테스트 종류** | **테스트 항목** | **담당자** |
| --- | --- | --- | --- |
| 141 | 단위 테스트 | non-volatile data정상 작동 여부 | 김민서, 최원혁 |
| **테스트 목적** | | | |
| 3번non-volatile data정상 작동 여부, 흐름 및 수집 완료 확인 + 초기 interface로 돌아가는지 확인 | | | |
| **테스트 환경** | | | |
| Windows 11 | | | |
| **테스트 케이스** | | | |
| 1. LDDC 실행 후 ‘3’ (non-volatile data) 입력 2. 디스크 데이터 파일 정상적으로 추출되었는지 확인 3. 초기 interface로 돌아갔는지 확인 | | | |
| **테스트 결과** | | | |
| LDDC 정상적으로 실행됨.  ‘3’ 입력 시 비휘발성 라이브 디스크 데이터 (nonvol) 정상적으로 추출됨.  초기 interface로 정상적으로 돌아감. | | | |

| **테스트 번호** | **테스트 종류** | **테스트 항목** | **담당자** |
| --- | --- | --- | --- |
| 151 | 단위 테스트 | Program end정상 작동 여부 | 김민서, 최원혁 |
| **테스트 목적** | | | |
| 4번 Program end 정상 작동 여부 확인 + LDDC 종료 여부 확인 | | | |
| **테스트 환경** | | | |
| Windows 11 | | | |
| **테스트 케이스** | | | |
| 1. LDDC 실행 후 ‘4’ (Program end) 입력 2. LDDC 정상 종료되는지 확인 | | | |
| **테스트 결과** | | | |
| ‘4’ 입력 시 LDDC가 정상 종료됨. | | | |

## **분석 시험 결과**

|  |  |  |  |
| --- | --- | --- | --- |
| **테스트 번호** | **테스트 종류** | **테스트 항목** | **담당자** |
| 211 | 단위 테스트 | All data데이터 출력 파일 확인 | 김민서, 최원혁 |
| **테스트 목적** | | | |
| LDDC가 All data에 설정된 모든 라이브 디스크 데이터를 정상적으로 출력했는지 파일 확인 | | | |
| **테스트 환경** | | | |
| Windows 11 | | | |
| **테스트 케이스** | | | |
| 1. LDDC 실행 후 ‘1’ (All data) 입력. 2. 설계된 명령어에 맞게 디스크 데이터 파일 추출되었는지 확인 | | | |
| **테스트 결과** | | | |
| 휘발성 및 비휘발성 디스크 데이터에 해당하는 명령어들이 정상적으로 실행됨.  휘발성 및 비휘발성 디스크 데이터 파일들이 정상적으로 출력됨.  **logonAccount, net, process, Prefetch, cache, cookie, eventlog, mft, quicklaunch, recent, registry**에 해당하는 파일들이 모두 정상적으로 출력됐고 내용도 정상적인 것을 확인. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **테스트 번호** | **테스트 종류** | **테스트 항목** | **담당자** |
| 221 | 단위 테스트 | Volatile data데이터 출력 파일 확인 | 김민서, 최원혁 |
| **테스트 목적** | | | |
| LDDC가 Volatile data에 설정된 모든 라이브 디스크 데이터를 정상적으로 출력했는지 파일 확인 | | | |
| **테스트 환경** | | | |
| Windows 11 | | | |
| **테스트 케이스** | | | |
| 1. LDDC 실행 후 ‘2’ (Volatile data) 입력. 2. 설계된 명령어에 맞게 디스크 데이터 파일 추출되었는지 확인 | | | |
| **테스트 결과** | | | |
| 휘발성 디스크 데이터에 해당하는 명령어들이 정상적으로 실행됨.  휘발성 디스크 데이터 파일들이 정상적으로 출력됨.  **logonAccount, net, process**에 해당하는 파일들이 모두 정상적으로 출력됐고 내용도 정상적인 것을 확인. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **테스트 번호** | **테스트 종류** | **테스트 항목** | **담당자** |
| 231 | 단위 테스트 | non-volatile data데이터 출력 파일 확인 | 김민서, 최원혁 |
| **테스트 목적** | | | |
| LDDC가 non-volatile data에 설정된 모든 라이브 디스크 데이터를 정상적으로 출력했는지 파일 확인 | | | |
| **테스트 환경** | | | |
| Windows 11 | | | |
| **테스트 케이스** | | | |
| 1. LDDC 실행 후 ‘3’ (non-volatile data) 입력. 2. 설계된 명령어에 맞게 디스크 데이터 파일 추출되었는지 확인 | | | |
| **테스트 결과** | | | |
| 비휘발성 디스크 데이터에 해당하는 명령어들이 정상적으로 실행됨.  비휘발성 디스크 데이터 파일들이 정상적으로 출력됨.  **Prefetch, cache, cookie, eventlog, mft, quicklaunch, recent, registry**에 해당하는 파일들이 모두 정상적으로 출력됐고 내용도 정상적인 것을 확인. | | | |