



# **LDDC**

## **(LIVE DISK DATA COLLECTOR)**

### **TEST REPORT**

Team \_ Digital Forensic Study

침해사고 당한 컴퓨터에 대한 Live Disk Data 수집 자동화 IR 스크립트

## 목차

1. 테스트 개요.....	2
1.1. 테스트 목적 .....	2
1.2. 테스트 PC 환경 .....	2
1.3. 테스트 셋 .....	2
2. 상세 테스트 내용.....	2
2.1. 입력 시험 .....	3
2.2. 분석 시험 .....	3
3. 테스트 .....	4
3.1. 입력 시험 결과 .....	4
3.2. 분석 시험 결과 .....	9

## 1. 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.

### 1.1. 테스트 목적

LDDC IR 스크립트의 수집 및 분석 기능 정확성 평가

LDDC IR 스크립트의 안정성 및 신뢰성 평가

### 1.2. 테스트 PC 환경

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

### 1.3. 테스트 셋

Live Disk Data	TestSet1	TestSet2
OS	Windows 11 Home	Windows 11 Pro

## 2. 상세 테스트 내용

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

- 1) 테스트 PC 에서 LDDC 실행
- 2) 실행된 LDDC 에서 선택적으로 라이브 디스크 데이터 수집
- 3) 수집된 테스트 PC 의 라이브 디스크 데이터 검증 및 스크립트 제작 흐름도 평가
- 4) LDDC 의 성능, 속도 및 정확성 평가
- 5) 사용자 경험 향상을 위한 피드백 수집

## 2.1.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 data 정상 작동 여부 테스트 (:1)	1 번 all data 정상 작동 여부, 흐름 및 수집 완료 확인 + 초기 interface 로 돌아가는지 확인	김민서, 최원혁
3	131	Volatile data 정상 작동 여부 테스트 (:2)	2 번 Volatile data 정상 작동 여부, 흐름 및 수집 완료 확인 + 초기 interface 로 돌아가는지 확인	김민서, 최원혁
4	141	non-volatile data 정상 작동 여부 테스트 (:3)	3 번 non-volatile data 정상 작동 여부, 흐름 및 수집 완료 확인 + 초기 interface 로 돌아가는지 확인	김민서, 최원혁
5	151	Program end 정상 작동 여부 테스트 (:4)	4 번 Program end 정상 작동 여부 확인 + LDDC 종료 여부 확인	김민서, 최원혁

## 2.2.분석 시험

일련 번호	테스트 번호	테스트 항목	상세 설명	담당자
1	211	All data 데이터 출력 파일 확인	LDDC 가 All data 에 설정된 모든 라이브 디스크 데이터를 정상적으로 출력했는지 파일 확인	김민서, 최원혁
2	221	Volatile data 데이터 출력 파일 확인	LDDC 가 Volatile data 에 설정된 모든 라이브 디스크 데이터를 정상적으로 출력했는지 파일 확인	김민서, 최원혁
3	231	non-volatile data 데이터 출력 파일 확인	LDDC 가 non-volatile data 에 설정된 모든 라이브 디스크 데이터를 정상적으로 출력했는지 파일 확인	김민서, 최원혁

### 3. 테스트

#### 3.1. 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			
 <p>LDDC 정상적으로 실행되었으며, interface 또한 정상적으로 구현됨.</p>			

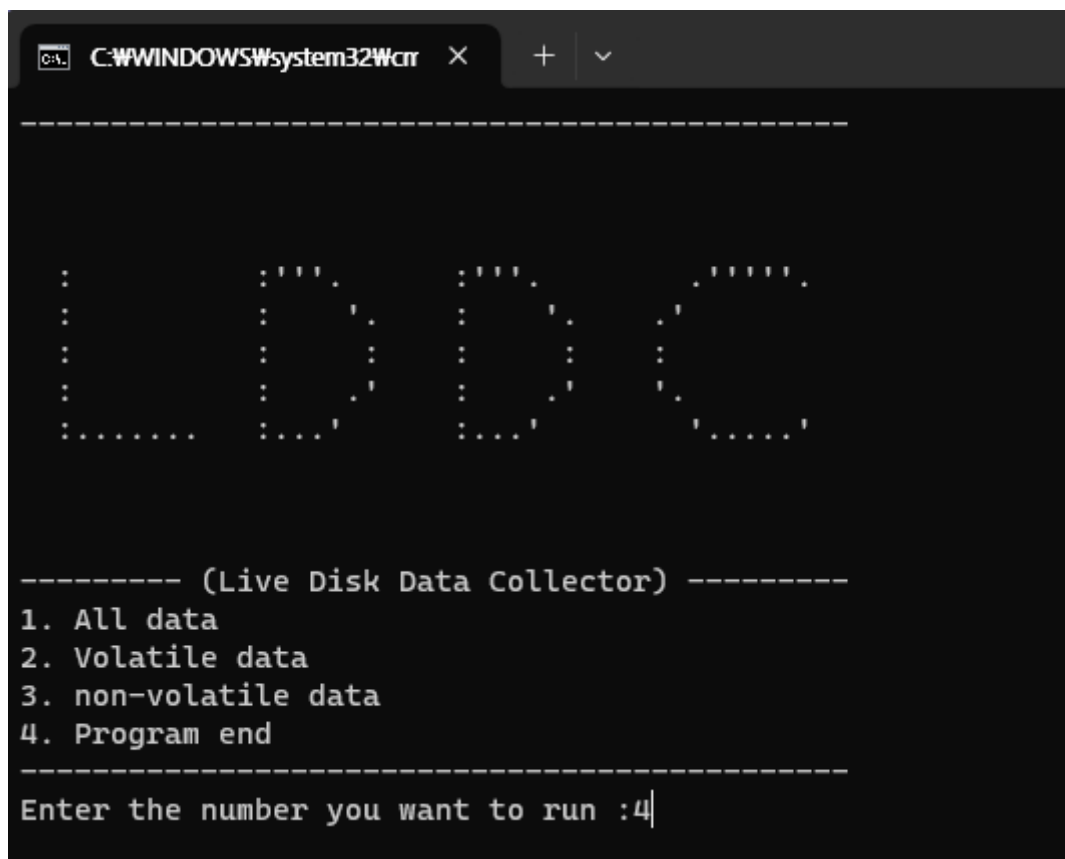
테스트 번호	테스트 종류	테스트 항목	담당자
121	단위 테스트	All data 정상 작동 여부	김민서, 최원혁
테스트 목적			
1 번 All data 정상 작동 여부, 흐름 및 수집 완료 확인 + 초기 interface 로 돌아가는지 확인			
테스트 환경			
Windows 11			
테스트 케이스			
1. LDDC 실행 후 '1' (All data) 입력 2. 디스크 데이터 파일 정상적으로 추출되었는지 확인 3. 초기 interface 로 돌아갔는지 확인			
테스트 결과			
<div> <div> PsLoggedon v1.35 - See who's logged on  Copyright (C) 2000-2016 Mark Russinovich  Sysinternals - www.sysinternals.com </div> <div> Created _result\_nonvol directory.   로그 파일 : C:\Users\ounno\OneDrive\바탕 화면\LDDC_Batch_script-main\_result\_nonvol\_cache\robocopy_chrome_cache.txt   <div> <div>LDDC</div> <div></div> </div> <div> (Live Disk Data Collector) 1. All data  2. Volatile data  3. non-volatile data  4. Program end </div> <div> Enter the number you want to run :  </div> </div> <div> <div> <div> <div>이름</div> <div>수집된 날짜</div> <div>파일</div> </div> <div> <div> <div>_nonvol</div> <div>_prefetch</div> <div>_vol</div> <div>log.txt</div> </div> <div> <div>2024-02-13 오후 4:59</div> <div>2024-02-13 오후 4:58</div> <div>2024-02-13 오후 4:58</div> <div>2024-02-13 오후 4:59</div> </div> <div> <div>파일 폴더</div> <div>파일 폴더</div> <div>파일 폴더</div> <div>텍스트 문서</div> </div> </div> </div> </div> </div>			
LDDC 정상적으로 실행됨. '1' 입력 시 전체적인 라이브 디스크 데이터 (vol, nonvol) 정상적으로 추출됨. 초기 interface 로 정상적으로 돌아감.			

테스트 번호	테스트 종류	테스트 항목	담당자
131	단위 테스트	Volatile data 정상 작동 여부	김민서, 최원혁
테스트 목적			
2 번 Volatile data 정상 작동 여부, 흐름 및 수집 완료 확인 + 초기 interface 로 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 interface 로 돌아갔는지 확인			
테스트 결과			
<div><div><div>LogonSessions v1.41 - Lists logon session information Copyright (C) 2004-2020 Mark Russinovich Sysinternals - www.sysinternals.com</div><div>PsLoggedon v1.35 - See who's logged on Copyright (C) 2000-2016 Mark Russinovich Sysinternals - www.sysinternals.com</div><div>----- :</div></div></div>			





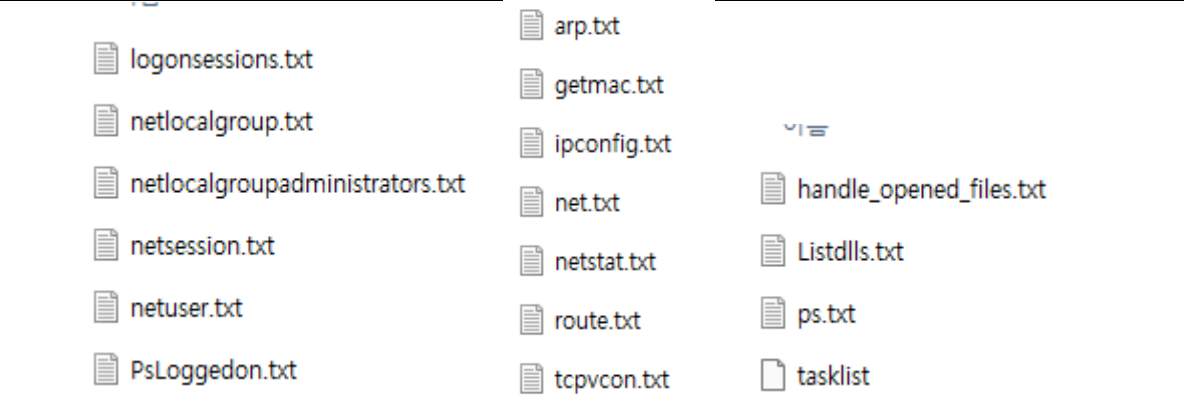
테스트 번호	테스트 종류	테스트 항목	담당자
151	단위 테스트	Program end 정상 작동 여부	김민서, 최원혁
테스트 목적			
4 번 Program end 정상 작동 여부 확인 + LDDC 종료 여부 확인			
테스트 환경			
Windows 11			
테스트 케이스			
<ol style="list-style-type: none"> <li>1. LDDC 실행 후 '4' (Program end) 입력</li> <li>2. LDDC 정상 종료되는지 확인</li> </ol>			
테스트 결과			

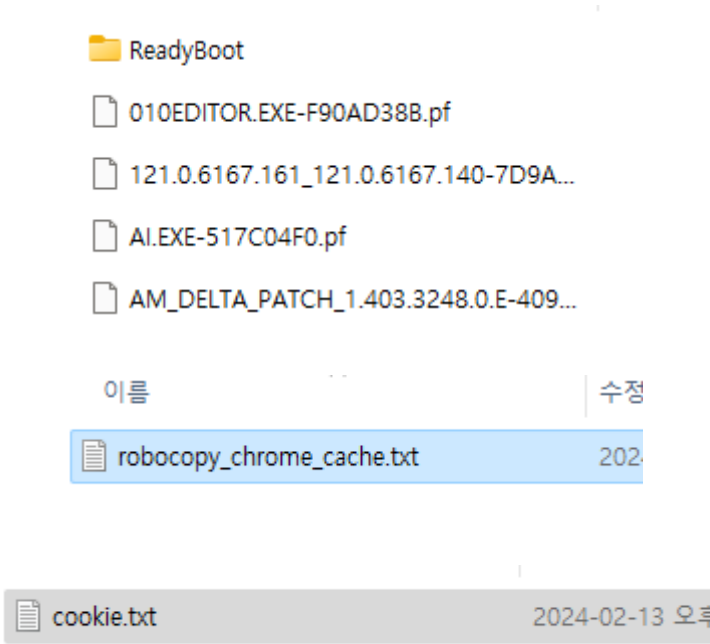




















'4' 입력 시 LDDC 가 정상 종료됨.

### 3.2. 분석 시험 결과

테스트 번호	테스트 종류	테스트 항목	담당자
211	단위 테스트	All data 데이터 출력 파일 확인	김민서, 최원혁
테스트 목적			
LDDC 가 All data 에 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			
<div> <div>  arp.txt                getmac.txt                ipconfig.txt                net.txt                netstat.txt                route.txt                tcpvcon.txt             </div> <div>  logonsessions.txt                netlocalgroup.txt                netlocalgroupadministrators.txt                netsession.txt                netuser.txt                PsLoggedon.txt             </div> <div>  handle_opened_files.txt                Listdlls.txt                ps.txt                tasklist             </div> </div> <div>  ReadyBoot            COMPONENTS            DEFAULT            Default User_NTUSER.DAT            Default User_USRCLASS.DAT            Default_NTUSER.DAT            Default_USRCLASS.DAT           2024-02         </div> <div>  010EDITOR.EXE-F90AD38B.pf            121.0.6167.161_121.0.6167.140-7D9A...            AI.EXE-517C04F0.pf            AM_DELTA_PATCH_1.403.3248.0.E-409...         </div>			
휘발성 및 비휘발성 디스크 데이터에 해당하는 명령어들이 정상적으로 실행됨. 휘발성 및 비휘발성 디스크 데이터 파일들이 정상적으로 출력됨. <b>logonAccount, net, process, Prefetch, cache, cookie, eventlog, mft, quicklaunch, recent, registry</b> 에 해당하는 파일들이 모두 정상적으로 출력됐고 내용도 정상적인 것을 확인.			

테스트 번호	테스트 종류	테스트 항목	담당자
221	단위 테스트	Volatile data 데이터 출력 파일 확인	김민서, 최원혁
테스트 목적			
LDDC 가 Volatile data 에 설정된 모든 라이브 디스크 데이터를 정상적으로 출력했는지 파일 확인			
테스트 환경			
Windows 11			
테스트 케이스			
<ol style="list-style-type: none"> <li>1. LDDC 실행 후 '2' (Volatile data) 입력.</li> <li>2. 설계된 명령어에 맞게 디스크 데이터 파일 추출되었는지 확인</li> </ol>			
테스트 결과			
 <p>휘발성 디스크 데이터에 해당하는 명령어들이 정상적으로 실행됨.</p> <p>휘발성 디스크 데이터 파일들이 정상적으로 출력됨.</p> <p><b>logonAccount, net, process</b> 에 해당하는 파일들이 모두 정상적으로 출력됐고 내용도 정상적인 것을 확인.</p>			

테스트 번호	테스트 종류	테스트 항목	담당자
231	단위 테스트	non-volatile data 데이터 출력 파일 확인	김민서, 최원혁
테스트 목적			
LDDC 가 non-volatile data 에 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			
			

 Application.evtx	2024-02
 GigabyteEngine.evtx	2024-02
 HardwareEvents.evtx	2024-02
 Internet Explorer.evtx	2024-02
 \$MFT	2024-02
 User Pinned	
 Chrome	
 Microsoft Edge	
 WHS_1st_biweekly_report.docx(2)	2023-11-05 5
 바탕 화면	2024-02-12 5
 연습문제_풀이-qkqxd777.ppt	2023-11-20 5
 차량 네트워크 보안 Handout.docx	2024-02-03 5
 COMPONENTS	2024-02
 DEFAULT	2024-02
 Default User_NTUSER.DAT	2024-02
 Default User_USRCLASS.DAT	2024-02
 Default_NTUSER.DAT	2024-02
 Default_USRCLASS.DAT	2024-02

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.