LDDC

(LIVE DISK DATA COLLECTOR) TEST REPORT

김민서, 김우리, 박혜미, 최원혁

침해사고 당한 컴퓨터에 대한 Live Disk Data 수집 자동화 IR 스크립트

목차

1.	테스트	트 개요	2
		테스트 목적	
		테스트 셋	
2.		테스트 내용	
		입력 시험	
	2.2.	분석 시험	3
3.	테스트	<u> </u>	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	정상적인 LDDC 실행	김우리
'	111			검구니
		(set 변수, :REDO)	여부와 선택 interface 정상	
			표시 여부 확인	
2	121	all data 정상 작동 여부 테스트	1 번 all data 정상 작동	김민서,
		(:1)	여부, 흐름 및 수집 완료	최원혁
			확인 + 초기 interface 로	
			돌아가는지 확인	
3	131	Volatile data 정상 작동 여부 테스트	2 번 Volatile data 정상	김민서,
		(:2)	작동 여부, 흐름 및 수집 최원학	
			완료 확인 + 초기	
			interface 로 돌아가는지	
			확인	
4	141	non-volatile data 정상 작동 여부	3 번 non-volatile	김민서,
		테스트	data 정상 작동 여부, 흐름	최원혁
		(:3)	및 수집 완료 확인 + 초기	
			interface 로 돌아가는지	
			확인	
5	151	Program end 정상 작동 여부 테스트	4 번 Program end 정상	박혜미
		(:4)	작동 여부 확인 + LDDC	
			종료 여부 확인	

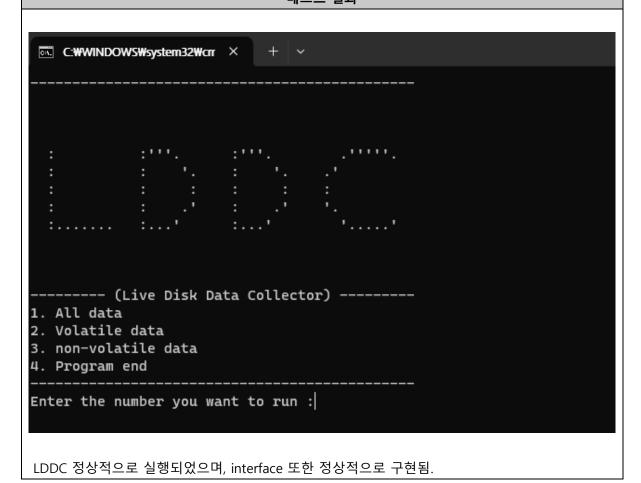
2.2.분석 시험

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

3. 테스트

3.1. 입력 시험 결과

테스트 번호	테스트 종류	테스트 항목	담당자	
111	단위 테스트	실행 및 interface	김우리	
	테스트	<u>목</u> 적		
정상적	인 LDDC 실행 여부 및 선	택 interface 정상 표시 여	부 확인	
	테스트	환경		
	Windo	ows 11		
	테스트	케이스		
1. LDDC 실행				
테스트 결과				



테스트 번호	테스트 종류	테스트 항목	담당자
121	단위 테스트	All data 정상 작동	김민서, 최원혁
		여부	

1 번 All data 정상 작동 여부, 흐름 및 수집 완료 확인 + 초기 interface 로 돌아가는지 확인

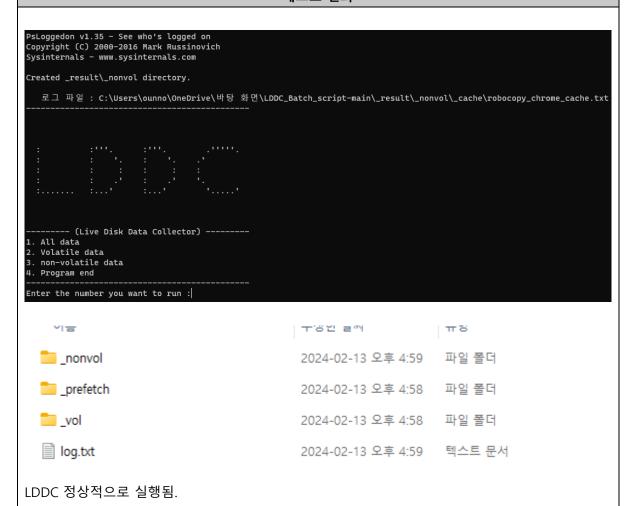
테스트 환경

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



'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	김민서, 최원혁
		작동 여부	

2 번 Volatile data 정상 작동 여부, 흐름 및 수집 완료 확인 + 초기 interface 로 돌아가는지 확인

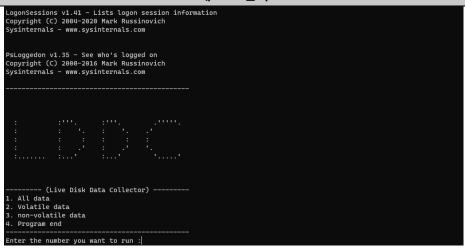
테스트 환경

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



== _vol	2024-02-13 오후	5:04 파일 폴더
log.txt	2024-02-13 오후	5:04 텍스트 문서
이름	수정한 날짜	유형
alogonAccount	2024-02-13 오후 5:0)4 파일 폴더
net	2024-02-13 오후 5:0)3 파일 폴더
process	2024-02-13 오후 5:0)4 파일 폴더

LDDC 정상적으로 실행됨.

'2' 입력 시 휘발성 라이브 디스크 데이터 (vol) 정상적으로 추출됨.

초기 interface 로 정상적으로 돌아감.

테스트 번호	테스트 종류	테스트 항목	담당자
141	단위 테스트	non-volatile data 정상	김민서, 최원혁
		작동 여부	

3 번 non-volatile data 정상 작동 여부, 흐름 및 수집 완료 확인 + 초기 interface 로 돌아가는지 확인

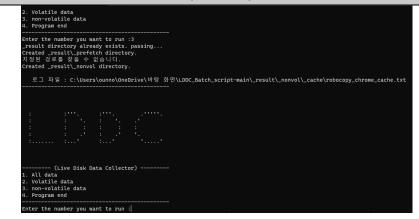
테스트 환경

Windows 11

테스트 케이스

- 1. LDDC 실행 후 '3' (non-volatile data) 입력
- 2. 디스크 데이터 파일 정상적으로 추출되었는지 확인
- 3. 초기 interface 로 돌아갔는지 확인

테스트 결과



nonvol

2024-02-13 오후 5:13 파일 폴더

prefetch

2024-02-13 오후 5:12 파일 폴더

____cache

2024-02-13 오후 7:06 파일 폴더

a_cookie

2024-02-13 오후 7:06 파일 폴더 2024-02-13 오후 7:06 파일 폴더

== _eventlog

2024-02-13 오후 7:06 파일 폴더

nft _mft

2024-02-13 エー 7:00 세달 달

auicklaunch

2024-02-13 오후 7:06 파일 폴더

2024-02-13 오후 7:06 파일 폴더

== _registry

2024-02-13 오후 7:06 파일 폴더

LDDC 정상적으로 실행됨.

'3' 입력 시 비휘발성 라이브 디스크 데이터 (nonvol) 정상적으로 추출됨.

초기 interface 로 정상적으로 돌아감.

테스트 번호	테스트 종류	테스트 항목	담당자
151	단위 테스트	Program end 정상	박혜미
		작동 여부	

4 번 Program end 정상 작동 여부 확인 + LDDC 종료 여부 확인

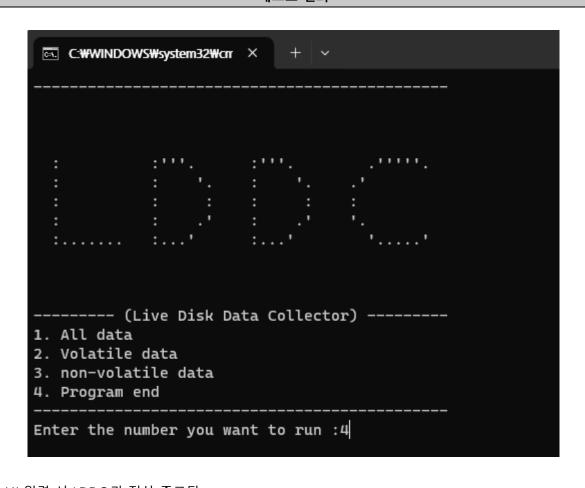
테스트 환경

Windows 11

테스트 케이스

- 1. LDDC 실행 후 '4' (Program end) 입력
- 2. LDDC 정상 종료되는지 확인

테스트 결과



'4' 입력 시 LDDC 가 정상 종료됨.

3.2.분석 시험 결과

테스트 번호	테스트 종류	테스트 항목	담당자	
211	단위 테스트	All data 데이터 출력	김민서, 최원혁	
	PII A I	파일 확인		
IDDC 7F All data 0ll		트 목적 크 데이터를 정상적으로 ∄	출련해느지 파익 화이	
EBBC 1 7 m data 3 m		<u> </u>		
	W	/indows 11		
		. 케이스		
	′1′ (All data) 입력. 에 맞게 디스크 데이터 파	이 ᄎ추디어느지 하이		
2. 글세션 6명의				
arn tut	테스트	트 결과		
arp.txt	logonsessions.txt			
getmac.txt	netlocalgroup.txt			
ipconfig.txt	5.700 SS	VIE		
net.txt	netlocal group administrator		d_files.txt	
netstat.txt	netsession.txt	Listdlls.txt		
route.txt	netuser.txt	ps.txt		
tcpvcon.txt	PsLoggedon.txt	tasklist tasklist		
	-		20	
E-1		COMPONENTS	2024-02	
== ReadyBoot		DEFAULT	2024-02	
010EDITOR.EXE-F90AI	D38B.pf	Default User_NTUSER.DAT	2024-02	
121.0.6167.161_121.0	0.6167.140-7D9A	Default User_USRCLASS.DA	AT 2024-02	
AI.EXE-517C04F0.pf		Default_NTUSER.DAT	2024-02	
AM_DELTA_PATCH_1.	403.3248.0.E-409	Default_USRCLASS.DAT	2024-02	
하바서 미 비하바서 디	V크 데이터에 체다치느 미		해 되	
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 파	일들이 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

LDDC 가 Volatile data 에 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 arp.txt logonsessions.txt getmac.txt netlocalgroup.txt 기급 ipconfig.txt netlocalgroupadministrators.txt handle_opened_files.txt net.txt netsession.txt Listdlls.txt netstat.txt netuser.txt ps.txt route.txt PsLoggedon.txt tasklist tcpvcon.txt

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 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					
	ReadyBoot				
	010EDITOR.EXE-F90				
	010EDITOR.EXE-F90	.0.6167.140-7D9A			
	010EDITOR.EXE-F90 121.0.6167.161_121 AI.EXE-517C04F0.pf	I.0.6167.140-7D9A			
	010EDITOR.EXE-F90	I.0.6167.140-7D9A			
	010EDITOR.EXE-F90 121.0.6167.161_121 AI.EXE-517C04F0.pf	I.0.6167.140-7D9A			
	010EDITOR.EXE-F90 121.0.6167.161_121 AI.EXE-517C04F0.pf AM_DELTA_PATCH_	1.0.6167.140-7D9A 1.403.3248.0.E-409 수정			
	□ 010EDITOR.EXE-F90 □ 121.0.6167.161_121 □ AI.EXE-517C04F0.pf □ AM_DELTA_PATCH_ 이름	1.0.6167.140-7D9A 1.403.3248.0.E-409 수정			

	Application.evtx	2024-02		
■ GigabyteEngine.evtx		2024-02		
# HardwareEvents.evtx		2024-02		
lnternet Explorer.evtx		2024-02		
	smft \$	2024-C		
	user Pinned			
	Chrome			
	Microsoft Edge □			
	WHS_1st_biweekly_report.docx(2)	2023-11-05 ⊆		
	🗾 바탕 화면	2024-02-12 5		
	🔂 연습문제_풀이-qkqxld777.ppt	2023-11-20 ⊆		
	🏚 차량 네트워크 보안 Handout.docx	2024-02-03 ⊆		
	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.				