논리적 쓰기방지 및 이미지 생성

포렌식 실습

컴퓨터보안 실습



SeoulTech UCS Lab

Ubiquitous Computing & Security Laboratory

디지털포렌식 절차



논리적 쓰기 방지

1. 레지스트리 수정을 통한 쓰기 방지



레지스트리 수정 - NTFS파일시스템(Win7) 레지스트리 수정 [오타나면 안됨] Key: HKLM\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies Name : WriteProtect Value : 0x0000000(쓰기방지 해제), 0x00000001(쓰기방지 설정) Dword 생성

논리적 쓰기 방지



레지스트리 수정 - NTFS파일시스템(Win7) 레지스트리 수정 [오타나면 안됨] Key: HKLM\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies Name : WriteProtect Value : 0x0000000(쓰기방지 해제), 0x00000001(쓰기방지 설정) Dword 생성

논리적 쓰기 방지



레지스트리 수정 - NTFS파일시스템(Win7) 레지스트리 수정 [오타나면 안됨] Key: HKLM\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies Name : WriteProtect Value : 0x0000000(쓰기방지 해제), 0x0000001(쓰기방지 설정) Dword 생성

논리적 쓰기 방지



레지스트리 수정 - NTFS파일시스템(Win7) 레지스트리 수정 [오타나면 안됨] Key: HKLM\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies Name : WriteProtect Value : 0x0000000(쓰기방지 해제), 0x00000001(쓰기방지 설정) Dword 생성

논리적 쓰기 방지

2. 자동 실행 방지

이 이 이 아파	양목 • 🚱 🔍 🕫 • 제어판 • 모든 제어핀	1 항목 🕨 자동 실형
컴퓨터 설정 변경	각 유형의 미디어나 장치	지를 산입할 때 발생되는 동작을 선택하십시오. 실 ^{형 사용(1)} 체크 해제
🖌 Flash Player	의 비사 🕑 오디오 CD	기본값선택
🐯 RemoteApp 및 데스크통 연결 🚭 Windows Live 언어 설정	🥞 V 🕡 향상된 오디오 CD	기본값선택
國 관리 도구	🏲 판 🕮 DVD 동영상	o DVD 비디오 재생 - Media+ Player 10
 ⑦ 기본 프로그램 쯔 디스블레이 	1월 (년 향상된 DVD 동영상	기본값선택
 값 바탕 화면 가젯 및 색 관리 	· · · · · · · · · · · · · · · · · · ·	기본값선택
19 시스템	a ∧ 📧 사진	 행 매 번 확인
한 음성 인식 ····································	1 전 표 비디오 파일	기본값 선택
· 전원 음 · · · · · · · · · · · · · · · · · ·	📠 🚛 🕗 오디오 파일	기본값 선택
물 볼더 옵 자동으로 음악을 재생하고 사전 고 소프트웨어를 설치하고 게임 이드로 CD DVD 및 자기에	민을 보 명을 할 🚯 빈 CD	기본값 선택
기본 설정을 변경합니다.	네만 한 빈 DVD	기본값 선택
	💮 빈 BD	기본값 선택
	🐻 혼합 몬텐츠	🔞 매 번 확인

제어판 - 자동실행

모든 미디어 및 장치에 자동 실행 사용 체크 해제

1. 이미징 도구 AccessData FTK Imager 3.1.3 설치 및 실행



1) 파일 - Create Disk Image

2. 원본 이미지 선택



- 1) 파일 Create Disk Image
- 2) Physical Dirve 선택
- 3) 증거 드라이브 선택

3. 이미지 포맷 설정

Image Source	Select Image Type
WW.WPHYSICALDRIVE3	
Starting Evidence Number: 1 Image Destination(s)	Please Select the Destination Image Type
	C SMART
	G EON
	C AFF
Add Edit Bemove	
Add Overflow Location	
Verify images after they are created Create directory lictics of all files in the image after they are created	< 뒤로(<u>B</u>) 다음(<u>N</u>) > 취소 도움말
Create greatery isoligs of an ines in the image and they are created	

- 1) 파일 Create Disk Image
- 2) Physical Dirve 선택
- 3) 증거 드라이브 선택
- 4) Add 선택, 파일 포맷 E01으로 설정

4. 증거 정보 입력

Evidence Item Information Case Number: Evidence Number: Unique Description: Examiner: Notes:	사건번호 증거번호 특징 검사자	Select Image Destination Image Destination Folder F:\Forensic Image Filename (Excluding Extension) Itest Image Fragment Size (MB) For Raw, E01, and AFF formats: 0 = do not fragment Compression (0=None, 1=Fastest,, 9=Smallest) Use AD Encryption	Browse
 < 뒤로(<u>B</u>)) CHB(N) > <u>C</u> ancel <u>H</u> elp	< 뒤로(<u>B</u>) <u>F</u> inish <u>C</u> ancel	<u>H</u> elp

┃ 분할 이미지 크기

- 1) 파일 Create Disk Image
- 2) Physical Dirve 선택
- 3) 증거 드라이브 선택
- 4) Add 선택, 파일 포맷 E01으로 설정
- 5) 증거 정보입력, 파일 위치 설정

5. 이미징

age source	
W. WPHYSICALDRIVE3	Creating Image
Starting Evidence Number: 1 age Destination(s)	Image Source: WW.WPHYSICALDRIVE3
WForensicWtest [E01]	Destination: F:\Forensic\Ftest
	Status: Creating image
	Progress
Add Edit Remove	Floor
Add Canada and Landa	Estimated time left
erify images after they are created 🗌 Precalculate Progress Statistics	Cancel

- 1) 파일 Create Disk Image
- 2) Physical Dirve 선택
- 3) 증거 드라이브 선택
- 4) Add 선택, 파일 포맷 E01으로 설정
- 5) 증거 정보입력, 파일 위치 설정
- 6) 이미징 작업 진행

5. 정보 확인

▶ 로컬 디스크 (F:) ▮	Forensic +		
인쇄 굽기	새 롤더		800 💌
	이름 ^ 수	:정한 날짜	유형
	🕌 test 2	013-06-24 오전	파일 폴더
	Viet text E01 2	013-06-24 오전	EnCase Evidence
	📋 test.E01.txt 2	013-06-24 오전	텍스트 문서
	test.E02 2	013-06-24 오전	E02 파일
	(iii) test.E01 - 메모장		0
	파일(F) 편집(E) 서식(O) 보기(V) 도용	}말(H)	
	Tracks per Dylinder: 255 Sectors per Track: 63 Bytes per Sector: 512 Sector Count: 15,814,656 [Physical Drive Information] Drive Nodel: LGE USB Drive USB De Drive Serial Number: AADOODDODOOD Drive Interface Type: USB Removable drive: True Source data size: 7722 MB Sector count: 15814655 [Computed Hashes] MD5 checksum: 58b0d849ea7ddaf5 SHA1 checksum: 73c628418eD0507 Image Information: Acquisition started: Mon Jun 24 Acquisition finished: Mon Jun 24	vice 0485 06850cc190 6e9c1alc1103cd5 1 00:07:04 2013 1 00:14:03 2013	7 e9dfdaaf6
	F:₩Forensic♥test.E01 F:₩Forensic♥test.E02 Image Verification Results: Verification started: Non Jun 24 Verification finished: Non Jun 24 MD5 checksum: 58b0d849ea7dda15 SHA1 checksum: 73c828418e0d9507 verified	00:14:03 2013 00:14:45 2013 078d6cb690cc190 6e9c1a1c1103cd5	7 : verified e9dfdaaf6 :

*.txt로 증거 이미지 정보 확인 파일정보 중 MD5, SHA1 등 무결성을 확인할 수 있는 해시값 확인

실습 과제

증거물 USB에 대한 사본 이미지 생성 및 무결성 입증

1. 증거물 USB의 파일 변경, 훼손 없이 사본 이미징 작업이 완료되어야 함

Case Number:	20150513
Evidence Number:	0
Unique Description:	none
Examiner:	'학번'
Notes:	

2. 이미지 파일 포맷은 E01으로 설정

3. 'USB 번호', '생성된 사본 이미지 파일 정보(.txt) 내용'을 복사하여 bgwon214@gmail.com</u>로 제출

참고문헌

◆ 정보 보안 개론[개정3판], 양대일 저, 한빛미디어, 2018, 1.
◆ 디지털 포렌식 개론(2판), 이상진 저, 이룬 출판사, 2015. 5.
◆ 컴퓨터보안, William Stalling 저, 한티미디어, 2016. 8
◆ 정보보안과 사이버 해킹의 기초, 김경신 저, 2016. 8

