

Trends in dForensics, Feb/2013

JK Kim

proneer

proneer@gmail.com

<http://forensic-proof.com>

Security is a people problem...





FORENSIC-PROOF (forensic-proof.com/) (cont'd)

▪ 파일시스템 터널링을 주의하자 (Pay Attention to the File System Tunneling)

• 파일시스템 터널링

- ✓ 짧은 시간(기본 15초)안에 폴더에 동일한 이름으로 파일이 생성되면 생성시간을 변경하지 않음
- ✓ FAT, NTFS 에서 기본적으로 지원
- ✓ 파일을 삭제하거나 파일 이름 변경 → 캐시에 저장
- ✓ 파일 생성 시 캐시를 검색하여 동일한 파일이름이 있으면 캐시 정보를 복원

• 파일시스템 터널링을 사용하는 이유

- ✓ 임시 파일을 사용하는 프로그램의 동일성 유지를 위해

FORENSIC-PROOF (forensic-proof)

- 파일시스템 터널링을 주의하자

```
C:\WINDOWS\system32\cmd.exe

C:\Tunneling>echo > file1

C:\Tunneling>dir /tc
Volume in drive C has no label.
Volume Serial Number is 941C-9471

Directory of C:\Tunneling

02/08/2013  08:41 PM    <DIR>          .
02/08/2013  08:41 PM    <DIR>          ..
02/08/2013  08:42 PM                13 file1
                    1 File(s)                13 bytes
                    2 Dir(s)  6,156,234,752 bytes free

C:\Tunneling>echo %time%
20:44:16.07

C:\Tunneling>ren file1 file2

C:\Tunneling>dir /tc
Volume in drive C has no label.
Volume Serial Number is 941C-9471

Directory of C:\Tunneling

02/08/2013  08:41 PM    <DIR>          .
02/08/2013  08:41 PM    <DIR>          ..
02/08/2013  08:42 PM                13 file2
                    1 File(s)                13 bytes
                    2 Dir(s)  6,156,218,368 bytes free

C:\Tunneling>echo > file1

C:\Tunneling>dir /tc
Volume in drive C has no label.
Volume Serial Number is 941C-9471

Directory of C:\Tunneling

02/08/2013  08:41 PM    <DIR>          .
02/08/2013  08:41 PM    <DIR>          ..
02/08/2013  08:42 PM                13 file1
02/08/2013  08:42 PM                13 file2
                    2 File(s)                26 bytes
                    2 Dir(s)  6,156,218,368 bytes free

C:\Tunneling>echo %time%
20:44:33.57

C:\Tunneling>_
```



FORENSIC-PROOF (forensic-proof.com/)

▪ 파일시스템 터널링을 주의하자 (Pay Attention to the File System Tunneling)

• 파일시스템 터널링 설정

✓ HKLM\SYSTEM\ControlSet00\Control\FileSystem\MaximumTunnelEntryAgeInSeconds → 생성

- Data: 초 (캐시 유지 시간)

• 파일시스템 터널링 활성화/비활성화

✓ HKLM\SYSTEM\ControlSet00\Control\FileSystem\MaximumTunnelEntries → 생성

- Data : 0 (비활성화), 1 (활성화)

• 파일시스템 흔적이 터널링에 의한 것인지, 공격자의 의도적인 행위인지를 고려



FORENSIC FOCUS (articles.forensicfocus.com/) (cont'd)

What are 'gdocs'? Google Drive Data – Part 2

My Drive - Google Drive

https://drive.google.com/#my-drive

Facebook Twitter HanRSS Gmail FORENSIC-PROOF F-INSIGHT Nate Daum Naver CYB3RCRIM3: 4th ...

+Jin Kook Search Images Maps Play YouTube News Gmail Drive Calendar More

Google

Drive

New folder

Sort

CREATE

My Drive

Shared with me

Starred

Recent

More

Download Google Drive

5% full
[Upgrade storage](#)

Meet your Drive

My Drive is the home for all your files. With Google Drive for your PC, you can sync files from your computer to **My Drive**.

Download Google Drive for PC

Then, go for a spin

- Explore the left hand navigation.
- Create Google Docs and more.
- See files at a glance with the new grid view.
- Get the Google Drive mobile app.

My Drive

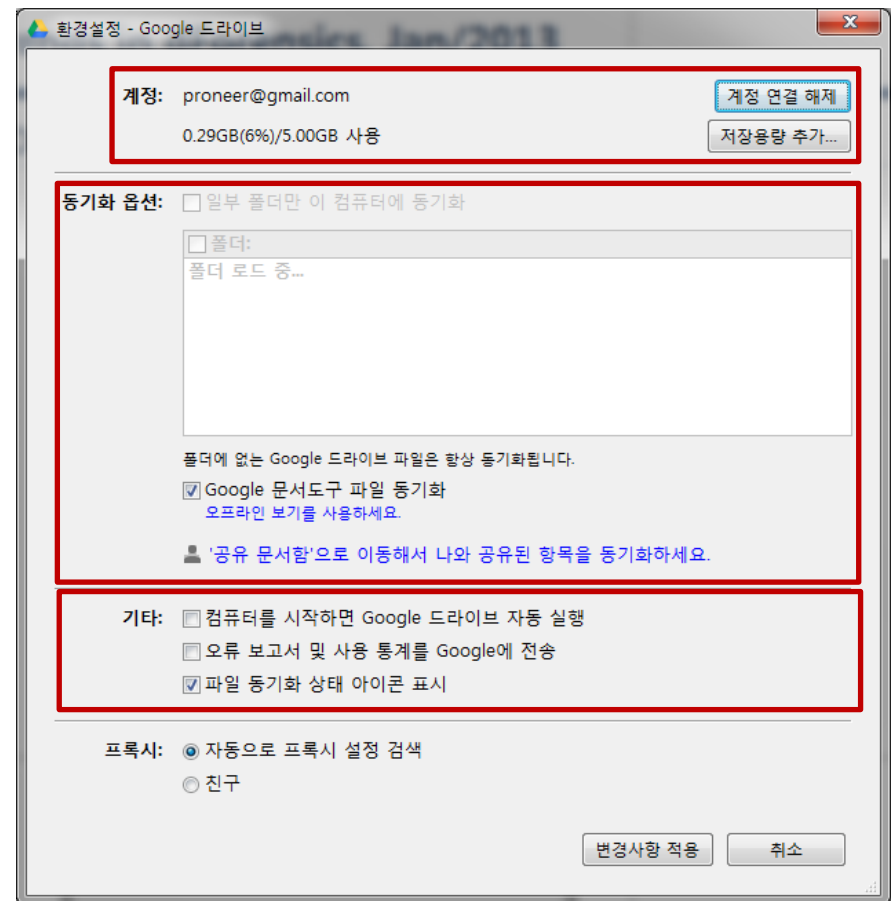
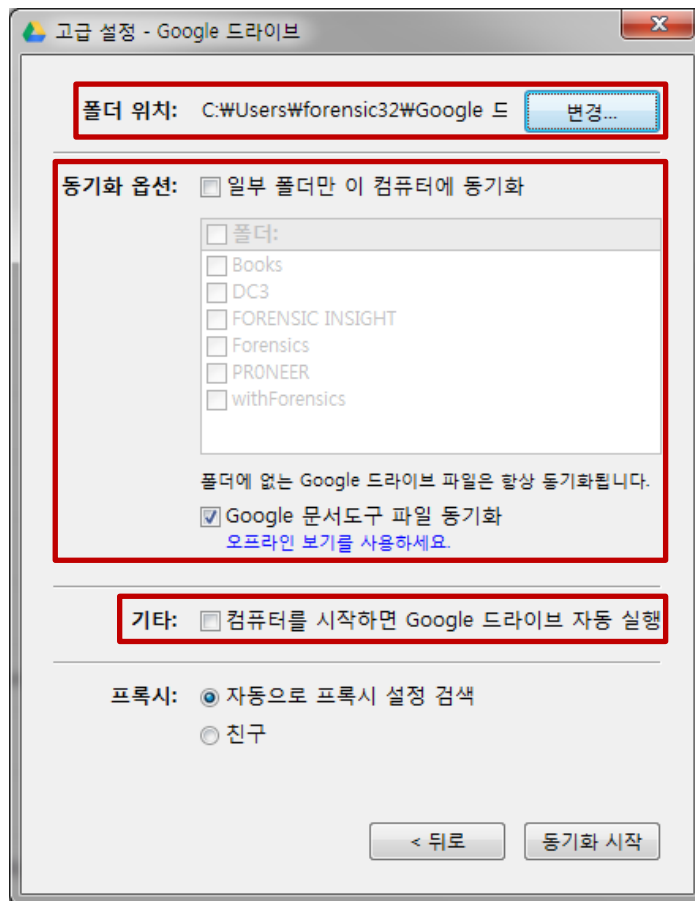
<input type="checkbox"/>	TITLE	OWNER	LAST MODIFIED
<input type="checkbox"/>	☆ Books	me	6/14/12 me
<input type="checkbox"/>	☆ FORENSIC INSIGHT	me	11/8/12 me
<input type="checkbox"/>	☆ Forensics	me	7/14/12 me
<input type="checkbox"/>	☆ PRONEER	me	9/25/12 me
<input type="checkbox"/>	☆ CODEGATE 2012	me	2/25/12 me
<input type="checkbox"/>	☆ P dc-12-raggo.ppt	me	8/27/11 me



FORENSIC FOCUS (articles.forensicfocus.com/) (cont'd)

What are 'gdocs'? Google Drive Data – Part 2

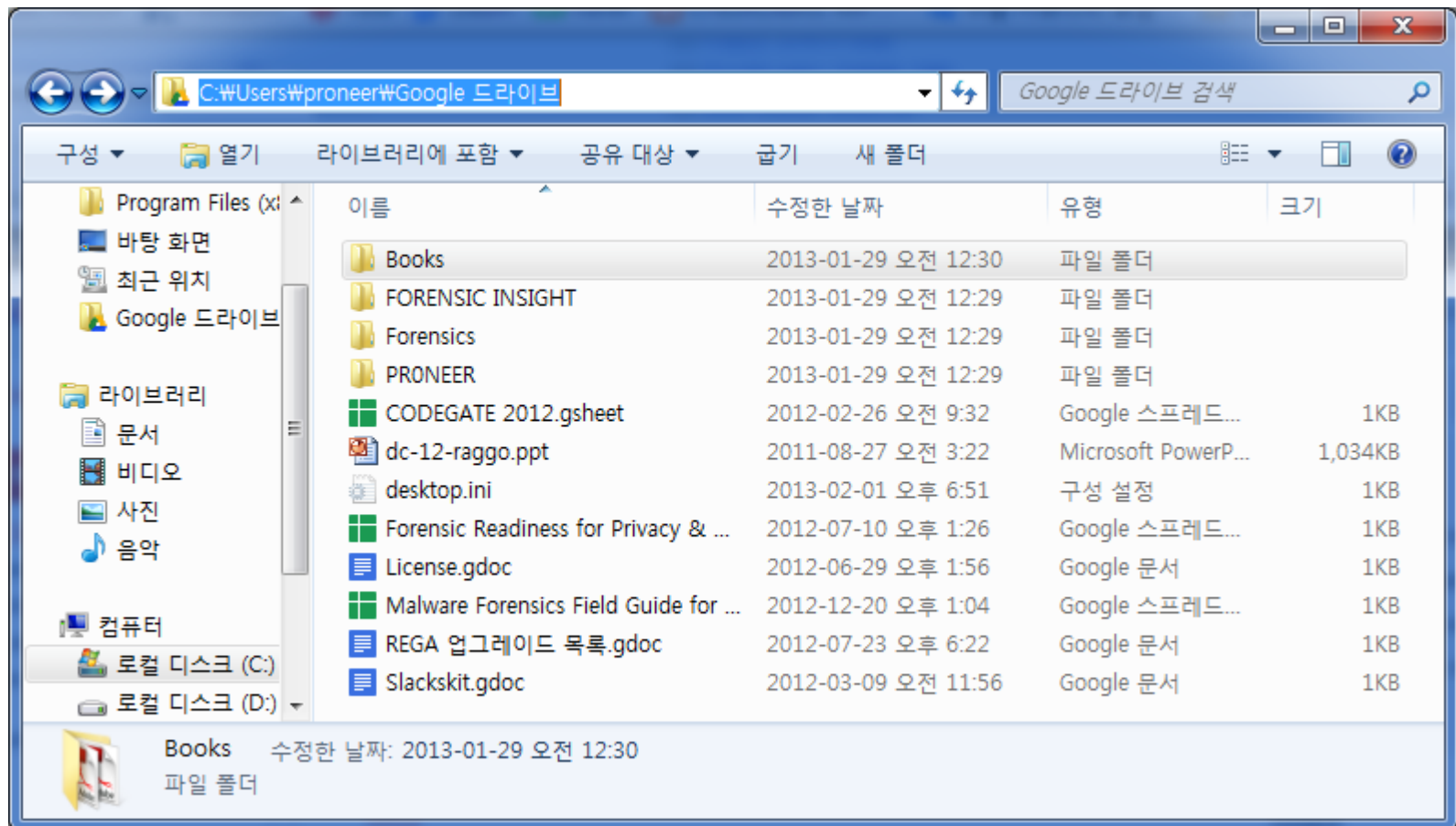
설치 시, 설치 후 설정





FORENSIC FOCUS (articles.forensicfocus.com/) (cont'd)

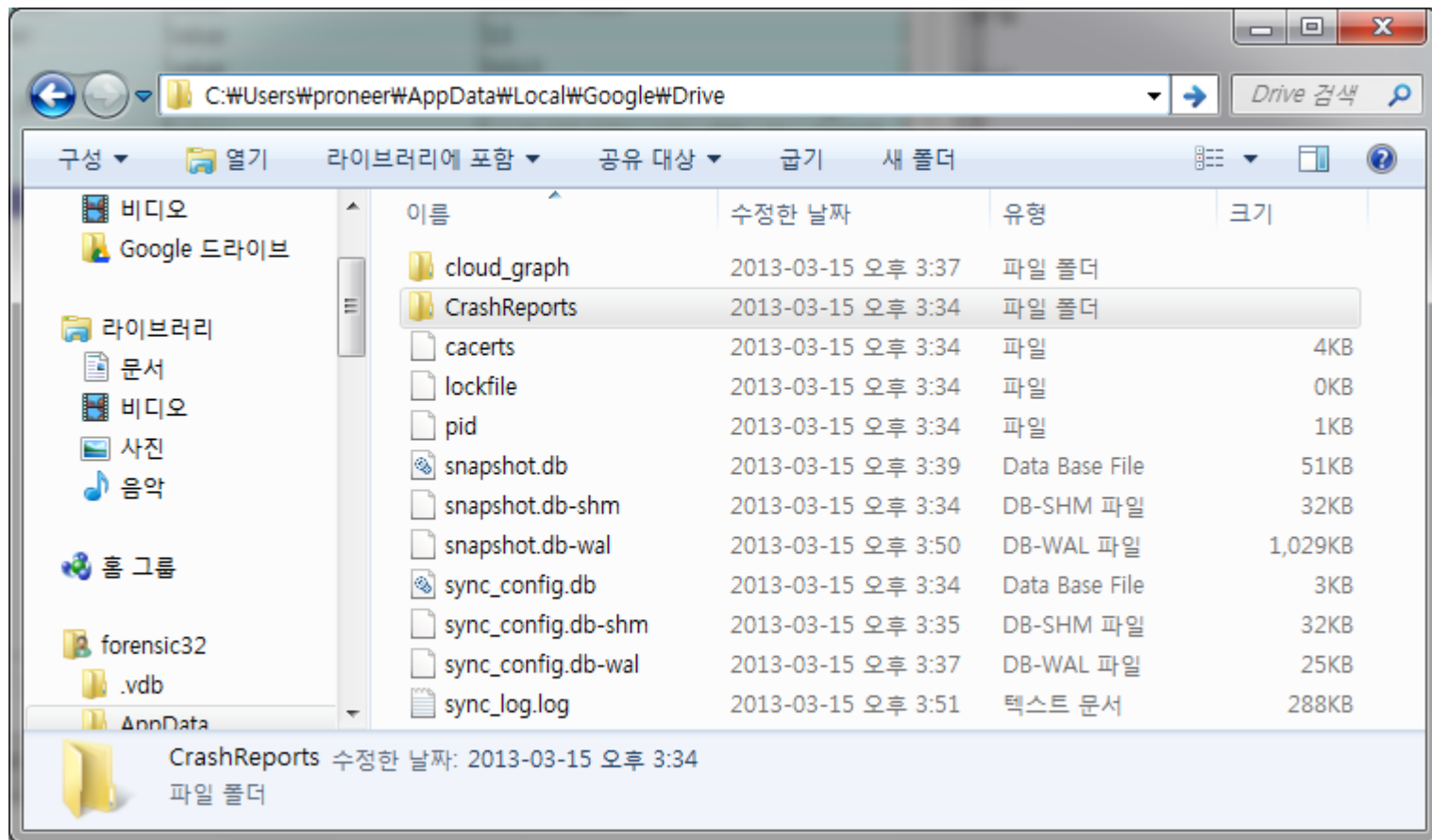
- What are 'gdocs'? Google Drive Data – Part 2
 - %UserProfile%\Google Drive → **gdoc, gsheet, gslides**





FORENSIC FOCUS (articles.forensicfocus.com/) (cont'd)

- What are 'gdocs'? Google Drive Data – Part 2
 - %UserProfile%\AppData\Local\Google\Drive → **로그 및 설정 정보**





FORENSIC FOCUS (articles.forensicfocus.com/) (cont'd)

▪ What are 'gdocs'? Google Drive Data – Part 2

- %UserProfile%\AppData\Local\Google\Drive ➔ **로그 및 설정 정보**

파일/폴더명	저장 정보
cloud_graphW	구글 드라이브 클라우드 리소스 ID
CrashReportsW	충돌 보고서
cacerts	CAcert 인증서
lockfile	잠긴 파일
pid	프로세스 ID
snapshot.db	클라우드, 로컬 파일/폴더 정보 생성/수정 시간, 파일/폴더명, 리소스 ID, URL, 크기, 체크섬, 공유여부, 매핑정보 등
sync_config.db	로컬 싱크 경로, 이메일, 버전 등
sync_log.log	싱크 로그



FORENSIC FOCUS (articles.forensicfocus.com/) (cont'd)

▪ What are 'gdocs'? Google Drive Data – Part 2

• 레지스트리 아티팩트

정보	경로
확장자 연결 정보	HKEY_CLASSES_ROOT\gdoc, .gdraw, .gform, .glink, .gnote, .gscrip, gsheets, gslides, gtable
설치여부, 인증 토큰	HKEY_CURRENT_USER\Software\Google\Drive
자동시작 여부	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
제품명, 설치시간, 설치경로, 상세버전 등	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\WS-1-5-18\Products\{Product GUID}\InstallProperties
제품명, 설치시간, 설치경로, 상세버전 등	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{GUID}



FORENSIC FOCUS (articles.forensicfocus.com/)

▪ What are 'gdocs'? Google Drive Data – Part 2

- 논의 사항

- ✓ 조사 대상에 자동 동기화 설정이 되어 있다면??
- ✓ 사용자명과 패스워드를 이용해 접근 권한을 얻어야 할지??
- ✓ 재판관할권 문제



Recover.co.il (cont'd)

▪ Hiding Data in Hard-Drive's Service Areas (<http://www.recover.co.il/SA-cover/SA-cover.pdf>)

- 서비스 영역

- ✓ HDD 상의 논리적인 영역으로 제조사에 의해 생성
- ✓ LBA(Logical Block Address) 범위 밖의 영역으로 표준 ATA 명령으로 접근 불가
- ✓ HDD가 복잡해짐에 따라 그런 복잡함을 컨트롤하기 위한 소프트웨어와 데이터로 구성
- ✓ 서비스 영역 데이터 ➔ 보통 안정성을 위해 백업본 유지
 - Detect management module
 - S.M.A.R.T(Self-Monitoring, Analysis and Reporting Technology) data module
 - Self-test module
 -



Recover.co.il (cont'd)

- **Hiding Data in Hard-Drive's Service Areas** (<http://www.recover.co.il/SA-cover/SA-cover.pdf>)
 - 서비스 영역 접근
 - ✓ HDD I/O 포트에 VSC(Vendor Specific Commands)를 보내어 접근
 - ✓ VSC는 HDD 제조사마다 제각각이고 공개하지 않음
 - ✓ 제조사에서 HDD 기능을 조작하기 위해 도구를 공개하기도 함
 - WD(Western Digital) – widle3.exe (open source, **idle3**)
 - HDDHACKR
 - ✓ **PC3000** – 서비스 영역을 접근하여 데이터 복구 시도



Recover.co.il (cont'd)

▪ Hiding Data in Hard-Drive's Service Areas (<http://www.recover.co.il/SA-cover/SA-cover.pdf>)

- 서비스 영역 크기 ➔ 서비스 영역과 모듈 크기는 제조사마다 제각각

✓ WD2500KS-00MJB0 (WD Hawk family, 250 GB, Firmware 02AEC)

- 6개의 표면을 사용 (헤드 0 ~ 5) ➔ 각 표면의 예약된 영역은 대략 23 MB
- 헤드 0,1에 매핑된 플래터 표면에 2개의 서비스 영역(원본, 백업본) 존재, 각각 6 MB
- 헤드 2 ~ 5에 매핑된 예약된 영역은 사용되지 않음
- 전체 예약된 영역 141 MB 중 12 MB를 서비스 영역으로 사용

✓ WD10EACS-00ZJB0 (WD Hulk family, 1 TB)

- 8개의 표면을 사용 (헤드 0 ~ 7) ➔ 각 표면의 예약된 영역은 대략 56 MB
- 헤드 0,1에 매핑된 플래터 표면에 2개의 서비스 영역(원본, 백업본) 존재, 각각 26 MB
- 헤드 2 ~ 7에 매핑된 예약된 영역은 사용되지 않음
- 전체 예약된 영역 450 MB 중 52 MB를 서비스 영역으로 사용



Recover.co.il (cont'd)

- **Hiding Data in Hard-Drive's Service Areas** (<http://www.recover.co.il/SA-cover/SA-cover.pdf>)
 - **VSC로만 접근 가능한 추가적인 예약 영역**
 - ✓ HDD 플래시 칩의 부트 스트래핑 공간 (보통 1 MB)
 - ✓ HDD LBA 범위 밖의 사용되지 않는 트랙
 - ✓ 헤드가 비활성화되어 있는 디스크 표면
 - **데이터 은닉과 파괴 (Data Hiding and Sanitation)**
 - ✓ 예약된 영역은 HDD VSC에 의해서만 접근 가능
 - ✓ 데이터 영구삭제 도구나 포렌식 도구는 해당 영역에 접근이 불가능



Recover.co.il (cont'd)

▪ Hiding Data in Hard-Drive's Service Areas (<http://www.recover.co.il/SA-cover/SA-cover.pdf>)

• 개념 증명 (Proof of Concept)

✓ WD 250 GB Hawk family

- 6개의 표면으로 구성, 면당 64 트랙, 트랙당 720 섹터
- 서비스 영역에 할당된 초기 2개의 표면은 제외
- 나머지 4개 표면의 예약 영역 활용 → 4 X 64 X 720 X 512 bytes
- POC 코드는 데이터 손실, HDD 실패를 유발할 수 있으므로 주의해서 사용

✓ 테스트 과정

1. 94 MB의 랜덤 파일을 생성하고 MD5 해시 계산
2. 서비스 영역에 파일 쓰기
3. dd /dev/zero를 이용해 전체 HDD 영구삭제
4. 서비스 영역에서 파일을 읽어 MD5 해시 계산 후 초기 해시값과 비교



Recover.co.il

- **SA-cover-poc.c** (<http://www.recover.co.il/SA-cover/SA-cover-poc.c>)

```
root@Shafan1:~/SA# dd if=/dev/urandom count=184320 > random-
file ; md5sum random-file
184320+0 records in
184320+0 records out
94371840 bytes (94 MB) copied, 12.8187 s, 7.4 MB/s
Obaca7245e1efa160512a6217c13a7b0 random-file
root@Shafan1:~/SA# ./SA-cover-poc -p 0x0170 -w ./random-file
using port address: 0x0170
Model: WDC WD2500KS-00MJB0
S/N: WD-WCANK5391702
F/W Ver: 02.01C03
LBA24:268435455 LBA48:488397168
Service area sectors-per-track (720)
Service area tracks (64)
Num of heads(6)
Unused reversed space (94371840 bytes)
writing head(2) track(-1)
writing head(2) track(-2)
writing head(2) track(-3)
....
writing head(5) track(-62)
writing head(5) track(-63)
writing head(5) track(-64)
```

```
root@Shafan1:~/SA# dd if=/dev/zero of=/dev/sdb bs=1M
dd: writing '/dev/sdb': No space left on device
238476+0 records in
238475+0 records out
250059350016 bytes (250 GB) copied, 4732.86 s, 52.8 MB/s
root@Shafan1:~/SA# ./SA-cover-poc -p 0x0170 -r after-dding-dev-
zero
using port address: 0x0170
Model: WDC WD2500KS-00MJB0
S/N: WD-WCANK5391702
F/W Ver: 02.01C03
LBA24:268435455 LBA48:488397168
Service area sectors-per-track (720)
Service area tracks (64)
Num of heads(6)
Unused reversed space (94371840 bytes)
reading head(2) track(-1)
reading head(2) track(-2)
....
reading head(5) track(-62)
reading head(5) track(-63)
reading head(5) track(-64)
root@Shafan1:~/SA# md5sum after-dding-dev-zero
Obaca7245e1efa160512a6217c13a7b0 after-dding-dev-zero
```



Learn Powershell (learn-powershell.net) (cont'd)

- **Write** to an Existing File Without Updating LastWriteTime or LastAccessTimestamps Using PowerShell

```
PS C:\temp> New-Item -Path C:\temp -Name "testfile.txt" -Type "file"

디렉터리: C:\temp

Mode                LastWriteTime         Length Name
----                -
-a---          2013-03-16 오전 2:43             0 testfile.txt

PS C:\temp> Get-Item .\testfile.txt | Select Name,CreationTime,LastWriteTime,LastAccessTime,Length

Name                : testfile.txt
CreationTime         : 2013-03-16 오전 2:43:59
LastWriteTime        : 2013-03-16 오전 2:43:59
LastAccessTime       : 2013-03-16 오전 2:43:59
Length               : 0

PS C:\temp> Get-Date

2013년 3월 16일 토요일 오전 2:45:09
```



Learn Powershell (learn-powershell.net) (cont'd)

- **Write** to an Existing File Without Updating LastWriteTime or LastAccessTimestamps Using PowerShell

```
관리자: Windows PowerShell

PS C:\temp> "forensic insight" | Write-File -File .\testfile.txt
PS C:\temp> Get-Item .\testfile.txt | Select Name,CreationTime,LastWriteTime,LastAccessTime,Length

Name           : testfile.txt
CreationTime    : 2013-03-16 오전 2:43:59
LastWriteTime   : 2013-03-16 오전 2:43:59
LastAccessTime  : 2013-03-16 오전 2:43:59
Length          : 19

PS C:\temp> "append text" | Write-File -File .\testfile.txt -Append
PS C:\temp> Get-Item .\testfile.txt | Select Name,CreationTime,LastWriteTime,LastAccessTime,Length

Name           : testfile.txt
CreationTime    : 2013-03-16 오전 2:43:59
LastWriteTime   : 2013-03-16 오전 2:43:59
LastAccessTime  : 2013-03-16 오전 2:43:59
Length          : 32

PS C:\temp> Get-Date

2013년 3월 16일 토요일 오전 2:46:33
```



Learn Powershell (learn-powershell.net) (cont'd)

▪ Write to an Existing File Without Updating LastWriteTime or LastAccessTimestamps Using PowerShell

• Write-File.ps1 스크립트 다운로드

✓ <http://gallery.technet.microsoft.com/scriptcenter/Write-or-Clear-a-File-49b5afdf>


Script Center

Search TechNet with Bing

United States (English) Sign in

[Home](#) [Library](#) [Learn](#) [Downloads](#) **Repository** [Community](#) [Forums](#) [Blog](#)

Script Center > Repository > Operating System > Write or Clear a File Without Updating LastAccess or LastWrite timestamps


 Download Windows Server 2012

Write or Clear a File Without Updating LastAccess or LastWrite timestamps

This function will allow you to edit an existing file without updating the LastWrite or LastAccess timestamp. Another neat thing is that if you are using the FileSystemWatcher .Net class to track a directory, it will not trip the Changed event at all. This uses a Win32 API to p

Quick Access

[My Contributions](#)
[Upload a contribution](#)
[Browse Script Requests](#)


Boe Prox

Download

Write-File.ps1

Ratings

★★★★★ (0)

Last Updated

2/16/2013

Downloaded

51 times






License

[TechNet Terms of Use](#)

Favorites

[Add To Favorites](#)

Share It:

Category

Operating System

Sub Category

.NET Framework

Tags

Powershell, Pinvoke, Win32 API, file stream

Report Abuse to Microsoft



Learn Powershell (learn-powershell.net)

▪ Read File Without Updating LastAccess TimeStamp using PowerShell

- Get-FileContent.ps1 스크립트 다운로드

✓ <http://gallery.technet.microsoft.com/scriptcenter/Read-file-without-updating-15eb9cb8>


Script Center

Search TechNet with Bing

United States (English) Sign in

[Home](#) [Library](#) [Learn](#) [Downloads](#) **Repository** [Community](#) [Forums](#) [Blog](#)

Script Center > Repository > Operating System > Read file without updating LastAccess timestamp

 Download Windows Server 2012


Read file without updating LastAccess timestamp

This function allows you to read a file and not update the LastAccess timestamp if it is enabled. This function uses the same Win32API that I used in my script to write to files without updating the timestamp. I also use a StreamReader to read the data with a given encoding to

Download

Get-FileContent.ps1

Ratings	★★★★★ (0)	Last Updated	2/18/2013
Downloaded	27 times	License	TechNet Terms of Use
Favorites	Add To Favorites	Share It:	Email Twitter LinkedIn Google+ Facebook
Category	Operating System		
Sub Category	.NET Framework		
Tags	Powershell, Pinvoke, Win32 API, file stream		
Report Abuse to Microsoft			



Boe Prox

Quick Access

[My Contributions](#)

[Upload a contribution](#)

[Browse Script Requests](#)



Password hashes dump tools

Tool	Command line	GUI	Local	Remote	SAM	Controls hidden. Press ESC to show controls. Dismiss		Credential manager	Protected storage	Autologin	Logon sessions
Cain & Abel	No	Yes	Yes	Yes. See notes	Yes (in-memory and from reg files)	Yes	Yes (in-memory and from reg files)	Yes locally No remotely	Yes locally No remotely	Yes (via LSA secrets)	No
pwdump2	Yes	No	Yes	No	Yes (in-memory)	No	No	No	No	No	No
pwdump6	Yes. See notes	No	Yes	Yes	Yes (in-memory)	Yes	No	No	No	No	No
pwdump7	Yes	No	Yes	No	Yes (from registry files). See notes	No	No	No	No	No	No
PowerDump	Yes	No	Yes	No	Yes (from registry files). See notes	No	No	No	No	No	No
fqdump	Yes	No	Yes	Yes	Yes (in-memory)	Yes	No	No	Unreliable. See notes	No	No
PWDumpX	Yes	No	Yes	Yes	Yes (in-memory)	Yes	Yes (in-memory)	No	No	Yes (via LSA secrets)	No
gsecdump	Yes	No	Yes	No	Yes (in-memory). See notes	No	Yes (in-memory)	No	No	Yes (via LSA secrets)	Yes (dump). See notes
carrot	Yes. See notes	No	Yes	No	Yes (from registry files). See notes	No	No	Unreliable. See notes	Yes	Yes	No
Metasploit smart_hashdump (post module)	Yes	No	Yes	Yes	Yes (local users in-memory and from reg files; domain users in-memory). See notes	No	No	No	No	No	No
Metasploit hashdump (post module)	Yes	No	Yes	Yes	Yes (from registry files). See notes	No	No	No	No	No	No
Metasploit hashdump (script)	Yes	No	Yes	Yes	Yes (from registry files). See notes	No	No	No	No	No	No
Metasploit hashdump (command)	Yes	No	Yes	Yes	Yes (in-memory). See notes	No	No	No	No	No	No



Others (cont'd)

▪ **Mandiant**

- Mandiant Exposes APT1 – One of China's Cyber Espionage Units & Releases 3,000 Indicators
- Threat Actors Using Mandiant APT1 Report as a Spear Phishing Lure
- Threat Actors Using Mandiant APT1 Report as a Spear Phishing Lure: The Nitty Gritty
- Netizen Research Bolsters APT1 Attribution

▪ **SANS Computer Forensics**

- Intro to Report Writing for Digital Forensics
- Report Writing for Digital Forensics: Part II

▪ **viaForensics**

- **OSDF Conference** – YAFFS2 Support for The Sleuth Kit



Others (cont'd)

▪ EDD AND FORENSICS

- **Auto-Generating OpenIOCs** – ioc_creator.py
- **Automating OpenIOC with Splunk** – IOC Splunker.py

▪ Journey Into Incident Response

- **Links for Toolz** – Custom Googles, Useful Public Resources, Malware Downloaders and Scappers, IDX Information and Parsers, Memory Forensics

▪ Hexacorn

- Beyond good ol' Run key
- Beyond good ol' Run key, Part 2
- Beyond good ol' Run key, Part 3



Others

- **Another Forensics Blog**

- Finding and Reverse Engineering Deleted SMS Messages

- **Bernardo Damele A. G.**

- Dump Windows password hashes efficiently – Part 1
- Dump Windows password hashes efficiently – Part 2
- Dump Windows password hashes efficiently – Part 3
- Dump Windows password hashes efficiently – Part 4
- Dump Windows password hashes efficiently – Part 5
- Dump Windows password hashes efficiently – Part 6



dForensics Tools (cont'd)

▪ williballenthin.com

- **INDXParse** – NTFS INDX 파서
- **phthon-registry** – 파이썬 레지스트리 모듈
- **python-evtx** – EVTX 이벤트 로그 파서
- **Shellbags** – Shellbags 파서

▪ NirSoft

- **NirLauncher** – NirSoft의 150여개 도구를 포터블 형태로 통합한 도구

▪ Tools Yard

- **Unhide Forensics Tool** – 숨긴 프로세스/포트 확인
- **Password Cracker Tool Hashkill** – GPU를 지원하는 패스워드 크랙 도구



dForensics Tools

- **Mach-O File Format Template for 010 Editor**
 - Mach-O 010 에디터 템플릿
- **Unpack.py**
 - WinAppDbg를 사용한 악성코드 자동 언팩 스크립트

