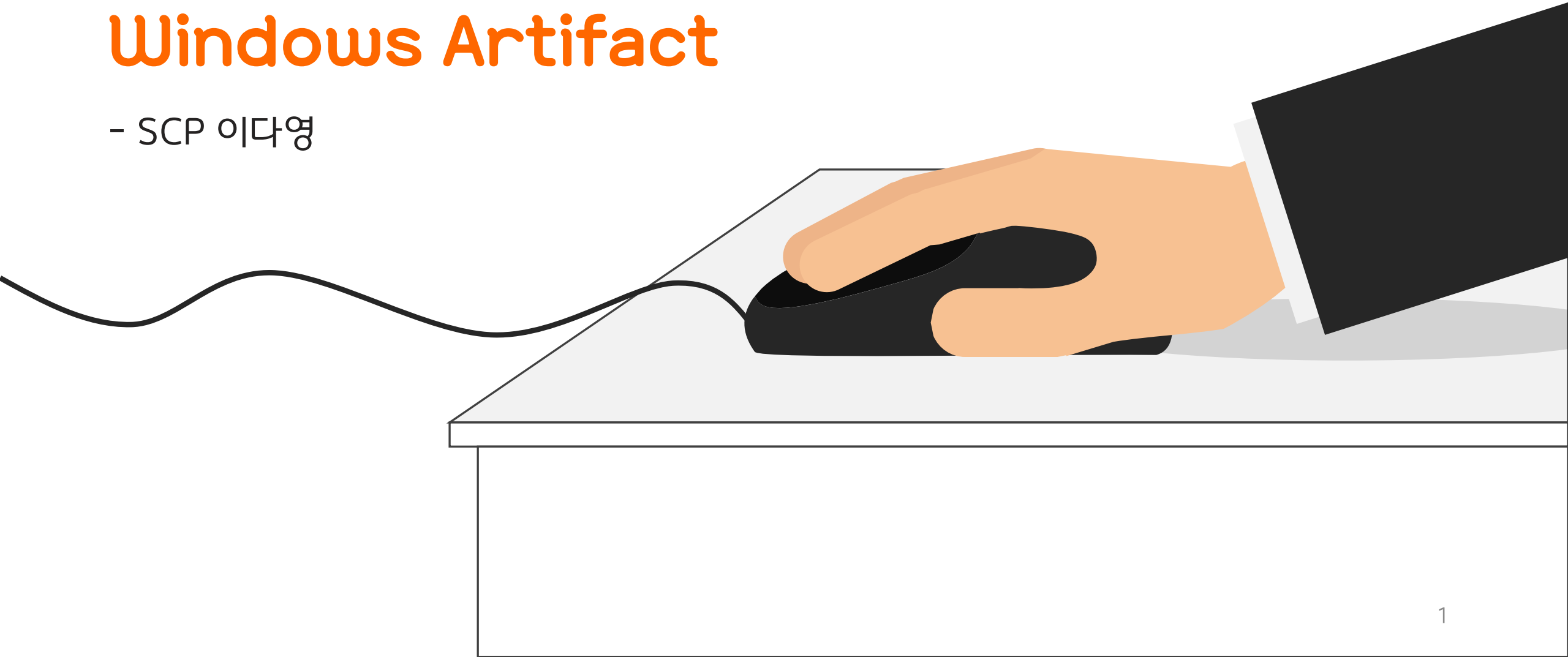


Windows Artifact

- SCP 이다영



Artifact



: 애플리케이션이나 운영체제를 사용하면서 생성되는 흔적

[생성 증거]

Windows Artifact



: 윈도우가 가지고 있는 특유의 기능들과
그 기능을 구현하는데 필요한 요소들로부터 찾을 수 있는 여러가지 정보

Artifact 종류



1. 웹 아티팩트

2. 이벤트 로그

3. 프리페치

4. LNK(Windows Shortcut)

5. 점프리스트

6. 레지스트리

7. 썸네일

8. 휴지통

1. 웹 아티팩트



: 웹에서 사용한 기록이 사용자의 컴퓨터에 남는 것








- 웹 아티팩트 종류

- (1) Web History
- (2) Cache
- (3) Cookie
- (4) Download File List

1. 웹 아티팩트 - Web History



: 사용자가 직접 방문한 웹 사이트의 접속 기록

오늘 - 2021년 5월 24일 월요일			
<input type="checkbox"/>	오후 2:12	 Web Artifcact : 네이버 블로그	m.blog.naver.com
<input type="checkbox"/>	오후 2:12	 Web Artifcact : 네이버 블로그	m.blog.naver.com
<input type="checkbox"/>	오후 2:12	 Web Artifcact : 네이버 블로그	m.blog.naver.com
<input type="checkbox"/>	오후 2:12	 웹 아티팩트란/ - Google 검색	www.google.com
<input type="checkbox"/>	오후 2:09	 [로그란] What is LOG DATA? : 네이버 블로그	m.blog.naver.com
<input type="checkbox"/>	오후 2:09	 [로그란] What is LOG DATA? : 네이버 블로그	m.blog.naver.com
<input type="checkbox"/>	오후 2:09	 [로그란] What is LOG DATA? : 네이버 블로그	m.blog.naver.com

1. 웹 아티팩트 - Chace



- : 웹 사이트 접속 시, 방문 사이트로부터 자동으로 전달받는 데이터
- 악성 파일을 다운로드 하거나 악성 페이지에 접근하는데 이용되기도 한다.

 chapter1.jpg	_dk_https://joongbu.ac.kr https://joongbu.ac.kr https://ccs.jo...	image/jpeg	8,128	2021-05-24 오후 ...
 chapter1.jpg	_dk_https://joongbu.ac.kr https://joongbu.ac.kr https://ccs.jo...	image/jpeg	8,173	2021-05-24 오후 ...
 chapter10.jpg	_dk_https://joongbu.ac.kr https://joongbu.ac.kr https://ccs.jo...	image/jpeg	13,778	2021-05-24 오후 ...
 chapter10.jpg	_dk_https://joongbu.ac.kr https://joongbu.ac.kr https://ccs.jo...	image/jpeg	15,078	2021-05-24 오후 ...
 chapter11.jpg	_dk_https://joongbu.ac.kr https://joongbu.ac.kr https://ccs.jo...	image/jpeg	12,556	2021-05-24 오후 ...
 chapter11.jpg	_dk_https://joongbu.ac.kr https://joongbu.ac.kr https://ccs.jo...	image/jpeg	13,677	2021-05-24 오후 ...
 chapter12.jpg	_dk_https://joongbu.ac.kr https://joongbu.ac.kr https://ccs.jo...	image/jpeg	11,831	2021-05-24 오후 ...
 chapter12.jpg	_dk_https://joongbu.ac.kr https://joongbu.ac.kr https://ccs.jo...	image/jpeg	12,241	2021-05-24 오후 ...
 chapter13.jpg	_dk_https://joongbu.ac.kr https://joongbu.ac.kr https://ccs.jo...	image/jpeg	12,558	2021-05-24 오후 ...
 chapter13.jpg	_dk_https://joongbu.ac.kr https://joongbu.ac.kr https://ccs.jo...	image/jpeg	6,298	2021-05-24 오후 ...

1. 웹 아티팩트 - Cookie



- : 웹 사이트 접속 시, 자동으로 사용자 저장 장치에 저장되는 텍스트 데이터
- 사용자 기반 서비스를 제공할 수 있게 한다.



최근 본 상품



1. 웹 아티팩트 - Download File List



: 웹에서 사용자가 직접 다운로드한 파일의 정보 기록

	<div>Inter.zip</div> <div>https://fonts.google.com/download?family=Inter</div> <div>폴더 열기</div>	×
	<div>shop.svg</div> <div>https://icons.getbootstrap.com/assets/icons/shop.svg</div> <div>폴더 열기</div>	×

2. 이벤트 로그



: 윈도우의 운용 과정에서 발생하는 특정 동작(이벤트)을 체계적으로 기록한 바이너리 로깅 시스템




* 로그

어떤 루트를 통해 어떻게 접속하고 어떠한 행위를 하였는지,
어떤 명령어로 어떤 행동을 했는지 기록되는 데이터

2. 이벤트 로그



제어판 > 관리 도구 > 이벤트 뷰어 > Windows 로그

키워드	날짜 및 시간	원본	이벤트 ID	작업 범주
 감사 성공	2021-05-24 오후 2:45:00	Microsoft Windo...	4798	User Account Management
 감사 성공	2021-05-24 오후 2:45:00	Microsoft Windo...	4672	Special Logon
 감사 성공	2021-05-24 오후 2:45:00	Microsoft Windo...	4624	Logon

2. 이벤트 로그



Windows Vista and above Events	
General Event Descriptions	General Event IDs
Account and Group Activities	4624, 4625, 4648, 4728, 4732, 4634, 4735, 4740, 4756
Application Crashes and Hangs	1000 and 1002
Windows Error Reporting	1001
Blue Screen of Death (BSOD)	1001
Windows Defender Errors	1005, 1006, 1008, 1010, 2001, 2003, 2004, 3002, 5008
Windows Integrity Errors	3001, 3002, 3003, 3004, 3010 and 3023
EMET Crash Logs	1 and 2
Windows Firewall Logs	2004, 2005, 2006, 2009, 2033
MSI Packages Installed	1022 and 1033
Windows Update Installed	2 and 19
Windows Service Manager Errors	7022, 7023, 7024, 7026, 7031, 7032, 7034
Group Policy Errors	1125, 1127, 1129
AppLocker and SRP Logs	865, 866, 867, 868, 882, 8003, 8004, 8006, 8007
Windows Update Errors	20, 24, 25, 31, 34, 35
Hotpatching Error	1009
Kernel Driver and Kernel Driver Signing Errors	5038, 6281, 219
Log Clearing	104 and 1102
Kernel Filter Driver	6
Windows Service Installed	7045
Program Inventory	800, 903, 904, 905, 906, 907, 908
Wireless Activities	8000, 8001, 8002, 8003, 8011, 10000, 10001, 11000, 11001, 11002, 11004, 11005, 11006, 11010, 12011, 12012, 12013
USB Activities	43, 400, 410
Printing Activities	307

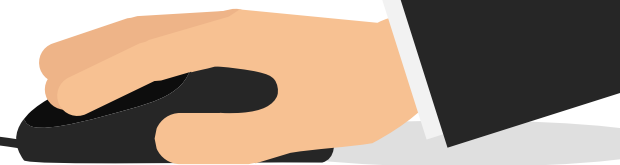
3. 프리페치




: 윈도우에서는 실행 파일이 사용하는
시스템 자원 정보를 특정 파일에 저장한다.

- 윈도우 부팅 시 프리페치 파일을 모두 메모리에 로드하여 실행 속도를 향상시킨다.
- 획득 가능 정보
 - (1) 실행 파일 이름
 - (2) 실행 파일 경로 해쉬값
 - (3) 실행 파일 마지막 실행 시간
 - (4) 실행 파일 실행 횟수
 - (5) 참조목록

3. 프리페치



 HWP.EXE-1659D1F0.pf











Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	17	00	00	00	53	43	43	41	11	00	00	00	4C	CE	03	00SCCA....LÎ..
00000010	48	00	57	00	50	00	2E	00	45	00	58	00	45	00	00	00	H.W.P...E.X.E...
00000020	60	6B	DC	04	80	F8	FF	FF	00	00	00	00	00	00	00	00	`kÛ.€øÿÿ.....
00000030	3D	00	00	00	80	FA	FF	FF	00	00	00	00	00	00	00	00	=...€úÿÿ.....
00000040	00	00	00	00	00	00	00	00	AE	38	EA	02	F0	D1	59	16@8ê.ðÑY.
00000050	00	00	00	00	F0	00	00	00	40	01	00	00	F0	28	00	00ð...@...ð(..
00000060	D2	39	00	00	C8	DE	02	00	3C	BC	00	00	08	9B	03	00	Ò9..ÈË..<4...>..
00000070	01	00	00	00	44	33	00	00	47	00	00	00	01	00	00	00D3..G.....
00000080	D6	6C	A6	69	07	69	D6	01	00	00	00	00	00	00	00	00	Öl;i.iÖ.....
00000090	00	00	00	00	00	00	00	00	03	00	00	00	01	00	00	00

실행 파일 이름: HWP.EXE

3. 프리페치

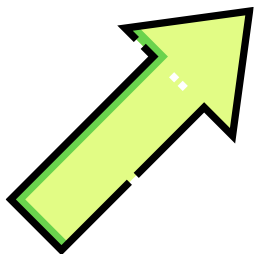


HWP.EXE-1659D1F0.pf

Filename	Full Path	Device Path	Index
 NTDLL.DLL	C:\Windows\System32\ntdll.dll	\DEVICE\HARDDISKVOLUME2\WIND...	0
 WOW64.DLL	C:\WINDOWS\SYSTEM32\WOW64.DLL	\DEVICE\HARDDISKVOLUME2\WIND...	1
 WOW64WIN.DLL	C:\WINDOWS\SYSTEM32\WOW64WI...	\DEVICE\HARDDISKVOLUME2\WIND...	2
 WOW64CPU.DLL	C:\WINDOWS\SYSTEM32\WOW64CP...	\DEVICE\HARDDISKVOLUME2\WIND...	3
 KERNEL32.DLL	C:\Windows\System32\kernel32.dll	\DEVICE\HARDDISKVOLUME2\WIND...	4
 KERNEL32.DLL	C:\Windows\SysWOW64\kernel32.dll	\DEVICE\HARDDISKVOLUME2\WIND...	5
 USER32.DLL	C:\Windows\System32\user32.dll	\DEVICE\HARDDISKVOLUME2\WIND...	6
 NTDLL.DLL	C:\Windows\SysWOW64\ntdll.dll	\DEVICE\HARDDISKVOLUME2\WIND...	7
 APISETSCHEMA.DLL	C:\Windows\System32\APISETSCHE...	\DEVICE\HARDDISKVOLUME2\WIND...	8
 KERNELBASE.DLL	C:\Windows\SysWOW64\KERNELBAS...	\DEVICE\HARDDISKVOLUME2\WIND...	9

참조 목록

4. LNK(Shortcut)



: 바로가기 파일(링크 파일)이라고도 불리며, 응용 프로그램, 디렉터리, 파일 등의 객체를 참조하는 파일

- 링크 대상 파일에 관한 생성, 접근, 수정 시간 정보 및 원본 위치 등에 관한 기록을 포함한다.

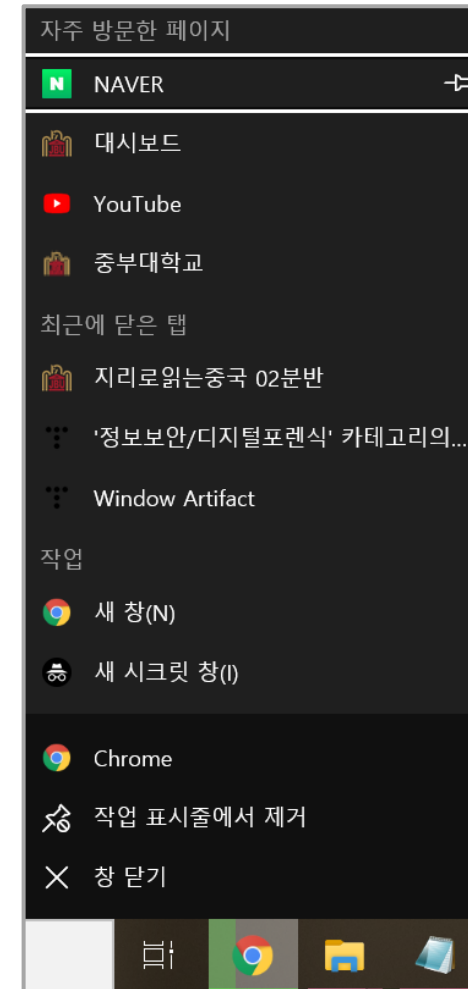


5. 점프리스트



: LNK의 확장형






- 최근 항목
- 자주 사용하는 항목
- 작업
- 사용자 고정



5. 점프리스트



%UserProfile%\AppData\Roaming\Microsoft
Windows\Recent\AutomaticDestinations

이름	수정한 날짜	유형	크기
 1b6ebacd7cd2f25a.automaticDestinations-ms	2021-05-23 오후 5:51	AUTOMATICDESTIN...	3KB
 1c7a9be1b15a03ba.automaticDestinations-ms	2020-12-21 오후 10:56	AUTOMATICDESTIN...	6KB
 1ced32d74a95c7bc.automaticDestinations-ms	2021-05-22 오후 12:02	AUTOMATICDESTIN...	151KB
 1f1f846f76251ea8.automaticDestinations-ms	2020-03-11 오전 1:09	AUTOMATICDESTIN...	37KB
 1fcde67b18651c69.automaticDestinations-ms	2020-10-19 오후 1:10	AUTOMATICDESTIN...	2KB

5. 점프리스트



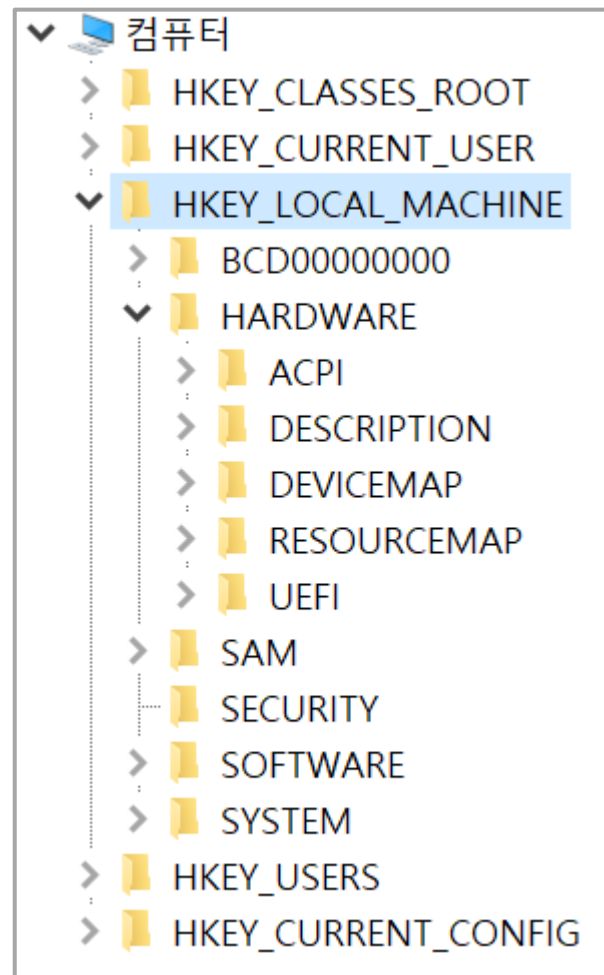
Filename	Full Path	Record Time	Created Time	Modified Time
 0222보완.md	C:\Users\djssl\Desktop\0222보완.md	2021-02-26 오후 ...	2021-02-22 오후 ...	2021-02-22 오후 ...
 0222보완.md	C:\Users\djssl\Desktop\0222보완.md	2021-02-22 오후 ...	2021-02-22 오후 ...	2021-02-22 오후 ...
 0223_web.md	C:\Users\djssl\Desktop\0223_web.md	2021-03-06 오후 ...	2021-02-23 오후 ...	2021-02-23 오후 ...
 0223_web.md	C:\Users\djssl\Desktop\0223_web.md	2021-02-24 오후 ...	2021-02-23 오후 ...	2021-02-23 오후 ...
 02주차_객체지...	C:\Users\djssl\Desktop\2학년 1학기\객...	2021-04-23 오후 ...	2021-03-20 오후 ...	2021-03-20 오후 ...
 02주차_객체지...	C:\Users\djssl\Desktop\2학년 1학기\객...	2021-04-23 오후 ...	2021-03-20 오후 ...	2021-03-20 오후 ...
 03 (1).7z	C:\Users\djssl\Downloads\03 (1).7z	2020-09-10 오후 ...	2020-09-10 오후 ...	2020-09-10 오후 ...

6. 레지스트리



: 시스템 구성 정보를 저장한 데이터 베이스

- 윈도우를 이용할 때 필요한 모든 정보들이 담겨있다.



6. 레지스트리



컴퓨터\HKEY_LOCAL_MACHINE\SYSTEM\Setup			
이름	종류	데이터	
(기본값)	REG_SZ	(값 설정 안 됨)	
CloneTag	REG_MULTI_SZ	Sat Dec 07 09:18:25 2019	
CmdLine	REG_SZ		
Compact	REG_DWORD	0x00000001 (1)	
LastMigrationScope	REG_DWORD	0x00000005 (5)	
OOBEInProgress	REG_DWORD	0x00000000 (0)	
OsLoaderPath	REG_SZ	₩	
RemoveWindowsOld	REG_DWORD	0x00000000 (0)	
RespecializeCmdLine	REG_SZ	Sysprep₩sysprep.exe /respecialize /quiet	
RestartSetup	REG_DWORD	0x00000000 (0)	
RollbackActive	REG_DWORD	0x00000000 (0)	
SetupPhase	REG_DWORD	0x00000000 (0)	
SetupSupported	REG_DWORD	0x00000001 (1)	
SetupType	REG_DWORD	0x00000000 (0)	
SystemPartition	REG_SZ	₩Device₩HarddiskVolume1	
SystemSetupInProgress	REG_DWORD	0x00000000 (0)	
UninstallSourceVersion	REG_SZ	10.0.18363	
Upgrade	REG_DWORD	0x00000000 (0)	
WorkingDirectory	REG_SZ	C:₩WINDOWS₩Panther	

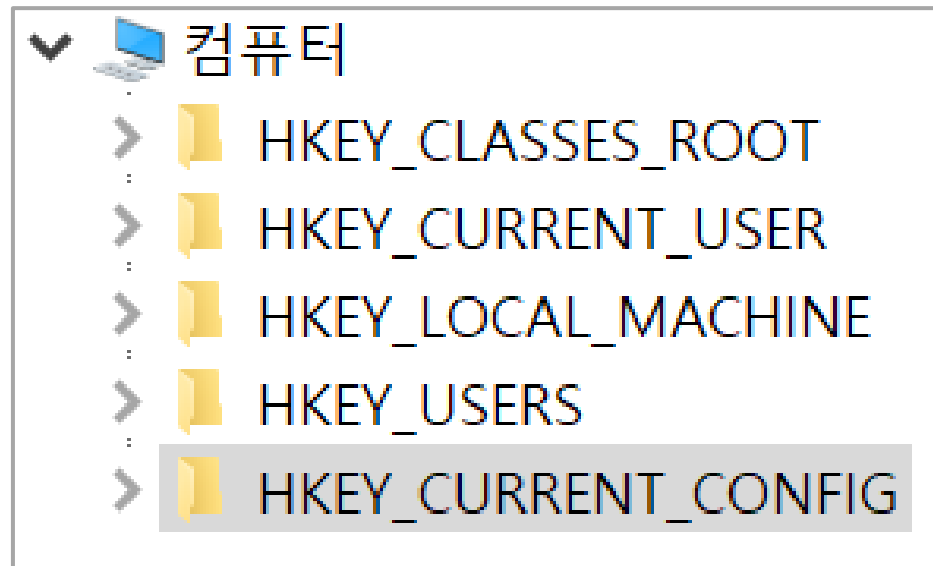
Key

Value

Data
Type

Data

6. 레지스트리



Root Key


6. 레지스트리 - 기본 시스템 정보



운영체제 이름

 ProductName	REG_SZ	Windows 10 Home
---	--------	-----------------


사용자

 RegisteredOwner	REG_SZ	djssl286@naver.com
---	--------	--------------------

운영체제 세부버전

 BuildLabEx	REG_SZ	19041.1.amd64fre.vb_release.191206-1406
--	--------	---

운영체제 설치 날짜

 InstallDate	REG_DWORD	0x60265a9b (1613126299)
---	-----------	-------------------------

-> 2021.2.12 오후 7:38:19

6. 레지스트리 - 기본 시스템 정보



업데이트 기록

✓ 기능 업데이트(1)

Windows 10, 버전 2004의 기능 업데이트

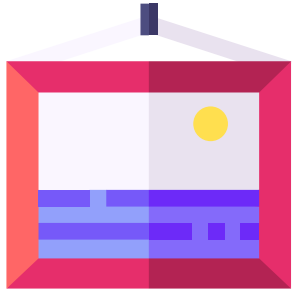
2021-02-12에 설치 성공

6. 레지스트리



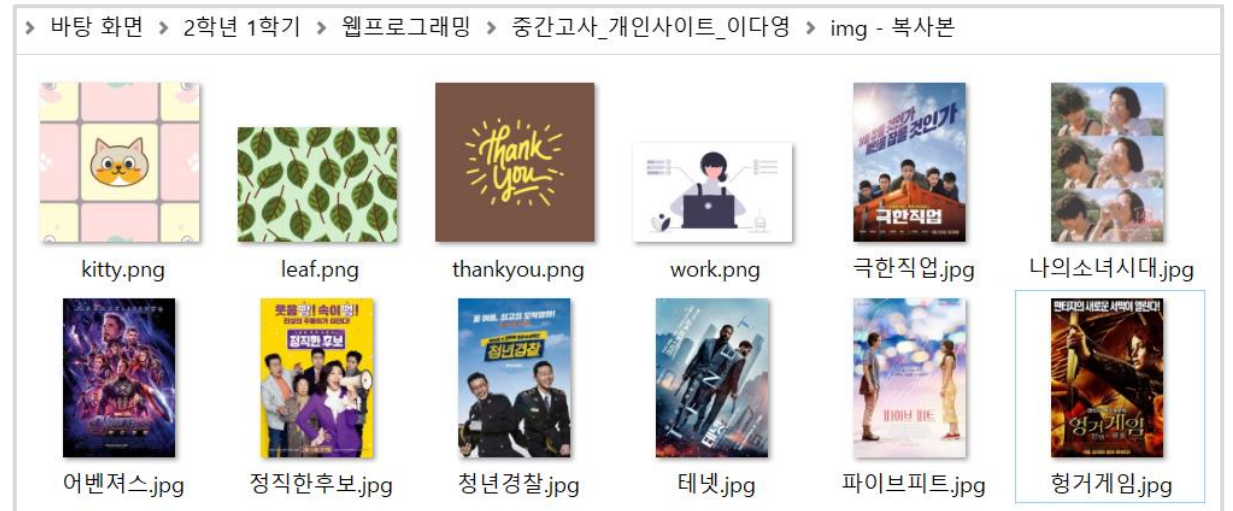
- 시스템 마지막 종료 시각
- 표준 시간대
- 날짜 변경 흔적
- 응용 프로그램 사용 로그
- 검색어 목록
- 최근 열어본 파일
- USB 장치 연결 정보

7. 썸네일



: 윈도우 미디어 파일에 대한 미리보기 데이터베이스 파일







- 원본 파일이 삭제되더라도
한 번 저장된 썸네일은 삭제되지 않는다.



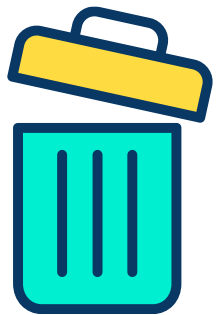
7. 썸네일



%UserProfile%\AppData\Local\Microsoft\Windows\Explorer

이름	수정한 날짜	유형
 thumbcache_96.db	2021-05-23 오후 1:01	Data Base File
 thumbcache_256.db	2021-05-25 오후 12:12	Data Base File
 thumbcache_768.db	2021-05-13 오후 11:32	Data Base File
 thumbcache_1280.db	2021-05-20 오후 4:40	Data Base File
 thumbcache_1920.db	2021-05-13 오후 11:32	Data Base File
 thumbcache_2560.db	2021-05-13 오후 11:32	Data Base File

8. 휴지통



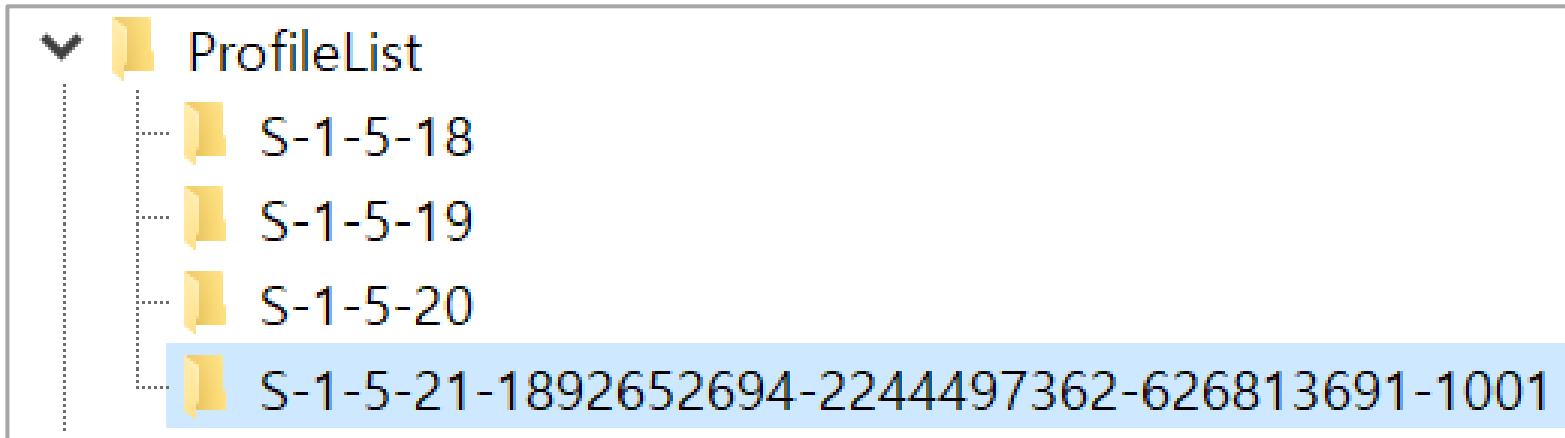
: 윈도우에서 파일을 삭제할 경우,
기본적으로 삭제된 파일은 휴지통 영역으로 이동

- 최대 크기를 넘지 않을 경우, 삭제한 파일 모두 복구 가능하다.
- 최대 크기를 넘길 경우, 오래된 파일부터 차례로 삭제된다.
- 사용자 SID(Security ID)별로 폴더가 존재한다.

8. 휴지통



₩HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft
₩Windows NT₩CurrentVersion₩ProfileList



감사합니다 😊

