



Prefetch

파일 실행 흔적

이
다
영

01

Artifact

아티팩트



: 애플리케이션이나 운영체제를 사용하면서 생성되는 흔적

[생성 증거]

윈도우에서는 실행 파일이 사용하는 시스템 자원 정보를 특정 파일에 저장함
프리페치 파일

→ 윈도우 부팅 시 프리페치 파일을 모두 메모리에 로드하여 실행 속도를 향상시킴



02 Prefetch

프리페치

모니터링 시간

부팅: 120초
응용 프로그램 시작: 10초

경로

“ C:\Windows\Prefetch\ ”

제한 개수

윈도우 7 - 128개
윈도우 8, 10 - 1024개
개수 초과시 오래된 프리페치
파일부터 삭제 →
새로운 프리페치 파일 생성

02 Prefetch

프리페치

프리페치 파일에서 획득 가능한 정보

- 실행 파일 이름
- 실행 파일 경로 해쉬값
- 실행 파일 마지막 실행 시간
- 실행 파일 실행 횟수
- 참조 목록

03

분석

프리페치 파일



HWP.EXE-1659D1F0.pf

▷ 0x00

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....Lİ..
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	`kÜ.€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..ÈP...<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

프리페치 버전: Windows Vista 또는 Windows 7

03

분석

프리페치 파일

▷ 0x04

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	`kÜ.€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..ÈP...<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

시그니처: SCCA (프리페치 파일(PF))

03

분석

프리페치 파일

▷ 0x10

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....Lİ..
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	`kÜ.€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..ÈP...<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

03

분석

프리페치 파일

▷ 0x4C

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..ÈP...<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 경로 해쉬 값: 0x1659D1F0

HWP.EXE-1659D1F0.pf

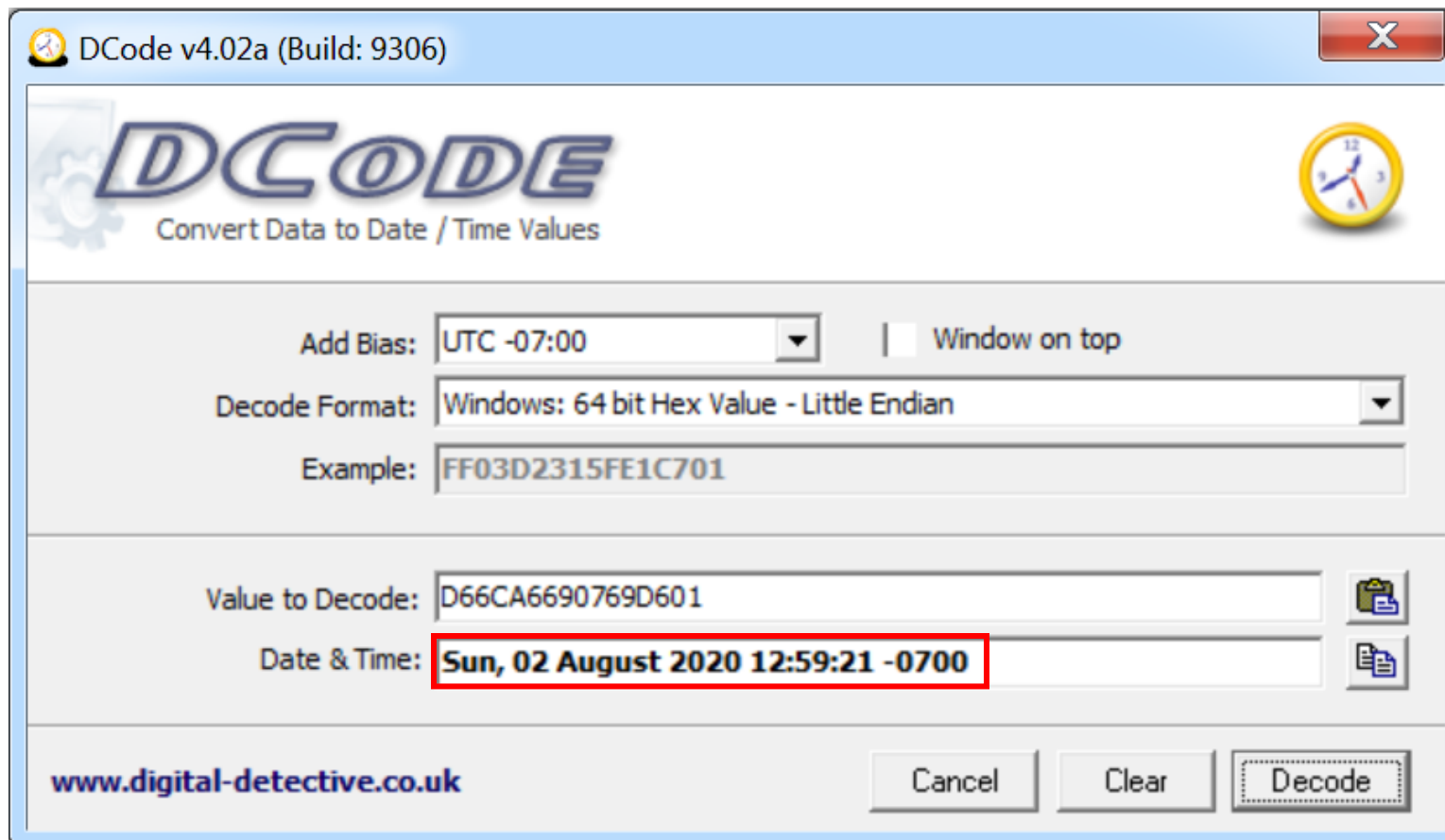
03

분석

프리페치 파일

▷ 0x80

Offset (h)	00	01	02	03	04	05
00000000	17	00	00	00	53	43
00000010	48	00	57	00	50	00
00000020	60	6B	DC	04	80	F8
00000030	3D	00	00	00	80	FA
00000040	00	00	00	00	00	00
00000050	00	00	00	00	F0	00
00000060	D2	39	00	00	C8	DE
00000070	01	00	00	00	44	33
00000080	D6	6C	A6	69	07	69 D6 01
00000090	00	00	00	00	00	00 00 03 00 00 00 01 00 00 00



실행 파일 마지막 실행 시간: 2020. 08. 02 (Sun) 12:59:21

03

분석

프리페치 파일

▷ 0x98

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..ÈP...<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 실행 횟수: 3



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
LOCALE.NLS	C:\Windows\System32\locale.nls	\DEVICE\HARDDISKVOLUME2\WIND...	10
HWP.EXE	C:\PROGRAM FILES (X86)\Hnc\Hwp8...	\DEVICE\HARDDISKVOLUME2\PROG...	11
USER32.DLL	C:\Windows\SysWOW64\user32.dll	\DEVICE\HARDDISKVOLUME2\WIND...	12






참조 목록

참조 목록 활용 (1)

: 실행한 파일 흔적

참조목록

Filename	Created Ti...	Modified Time
 WINWORD.EXE-AB6E...	2020-08-02 오...	2020-08-02 오...
 FILECOAUTH.EXE-9C...	2020-08-02 오...	2020-08-02 오...
 SVCHOST.EXE-3D60...	2020-08-02 오...	2020-08-02 오...
MUSNOTIFYICON.EXE...	2020-08-02 오...	2020-08-02 오...
 SIHCLIENT.EXE-98C4...	2020-08-02 오...	2020-08-02 오...
 UPFC.EXE-89D4FAEB....	2020-08-02 오...	2020-08-02 오...
 BACKGROUNDTASKH...	2020-08-02 오...	2020-08-02 오...
 BACKGROUNDTASKH...	2020-08-02 오...	2020-08-02 오...
 BACKGROUNDTASKH...	2020-08-02 오...	2020-08-02 오...
 BACKGROUNDTASKH...	2020-08-02 오...	2020-08-02 오...
 IGFEXT.EXE-56A281...	2020-08-02 오...	2020-08-02 오...
 RUNTIMEBROKER.EXE...	2020-08-02 오...	2020-08-02 오...
 DLLHOST.EXE-1BAE0...	2020-08-02 오...	2020-08-02 오...
 HANCONV.EXE-C62C...	2020-08-02 오...	2020-08-02 오...

Filename	Full Path
 WEBIO.DLL	C:\Windows\System32\webio.dll
 DNSAPI.DLL	C:\Windows\System32\dnsapi.dll
 NORMNFKC.NLS	C:\Windows\System32\normnfkc....
 RASADHLP.DLL	C:\Windows\System32\rasadhlp.dll
 이다영_92015300_대...	C:\Users\djssl\DOCUMENTS\이다...

03

분석

프리페치 파일

참조 목록 활용 (2)

: 외장 저장 장치 사용 흔적

참조목록

Filename	Created Time	Modified Ti...	File Size	Process EXE
HIMTRAYICON.EXE-1...	2020-08-02 오후 1:00	2020-08-02 오후 1:00	5,585	HIMTRAYICON.EXE
HWP.EXE-E327D425.pf	2020-08-02 오후 1:00	2020-08-02 오후 1:00	34,980	HWP.EXE
TEAMS.EXE-0F3D402...	2020-08-02 오후 1:00	2020-08-02 오후 1:00	16,189	TEAMS.EXE
DLLHOST.EXE-B74FD...	2020-08-02 오후 1:00	2020-08-02 오후 1:00	9,279	DLLHOST.EXE
SEARCHUI.EXE-B333...	2020-03-13 오후 1:00	2020-08-02 오후 1:00	87,188	SEARCHUI.EXE
DLLHOST.EXE-1BAE0...	2020-08-02 오후 1:00	2020-08-02 오후 1:00	4,408	DLLHOST.EXE
CONSENT.EXE-40419...	2020-03-13 오후 1:00	2020-08-02 오후 1:00	32,646	CONSENT.EXE
SEARCHFILTERHOST...	2020-08-02 오후 1:00	2020-08-02 오후 1:00	4,092	SEARCHFILTERHO..
AUDIODG.EXE-AB22E...	2020-08-02 오후 1:00	2020-08-02 오후 1:00	7,849	AUDIODG.EXE
SMARTSCREEN.EXE-E...	2020-08-02 오후 1:00	2020-08-02 오후 1:00	15,538	SMARTSCREEN.EXE
SEARCHPROTOCOLH...	2020-08-02 오후 1:00	2020-08-02 오후 1:00	4,580	SEARCHPROTOCOL...
SVCHOST.EXE-F952D...	2020-08-02 오후 1:00	2020-08-02 오후 1:00	12,477	SVCHOST.EXE
RUNTIMEBROKER.EXE...	2020-08-02 오후 1:00	2020-08-02 오후 1:00	15,991	RUNTIMEBROKER...
SVCHOST.EXE-73D0...	2020-08-02 오후 1:00	2020-08-02 오후 1:00	6,345	SVCHOST.EXE

Filename	Full Path	Device Path
ODTDOCGROUP.DFT	C:\PROGRAM FILES (X86)\WHNC\WH...	\\VOLUME{01d5385af3b93214-74f3...
XMLDOCGROUP.DFT	C:\PROGRAM FILES (X86)\WHNC\WH...	\\VOLUME{01d5385af3b93214-74f3...
(영어)3321이다영 17...		\\VOLUME{0000000000000000-f02...



감사합니다