ShimCache

91913232 김우종

Contents

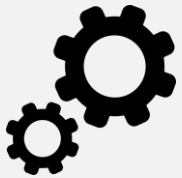
What is ShimCache?

ShimCache 정의

- AppCompatCache로 불리기도 함
- 응용 프로그램 간 호환성을 제어하고 문제 해결을 위해 만든 파일
  - 악성코드 실행 시 호환성 문제 발생하기 때문에 침해분석에 활용한다.
- 모든 실행 파일의 경로, 크기, 마지막 수정 시간 등의 정보를 저장한다.
- 프리패치와 비슷한 응용프로그램의 실행 정보를 저장한다.
  - 하지만 프리패치는 한정적이라 사라질 가능성이 있다.

ShimCache Forensic's perspective

실행 파일의 이름, 경로 정보를 확인



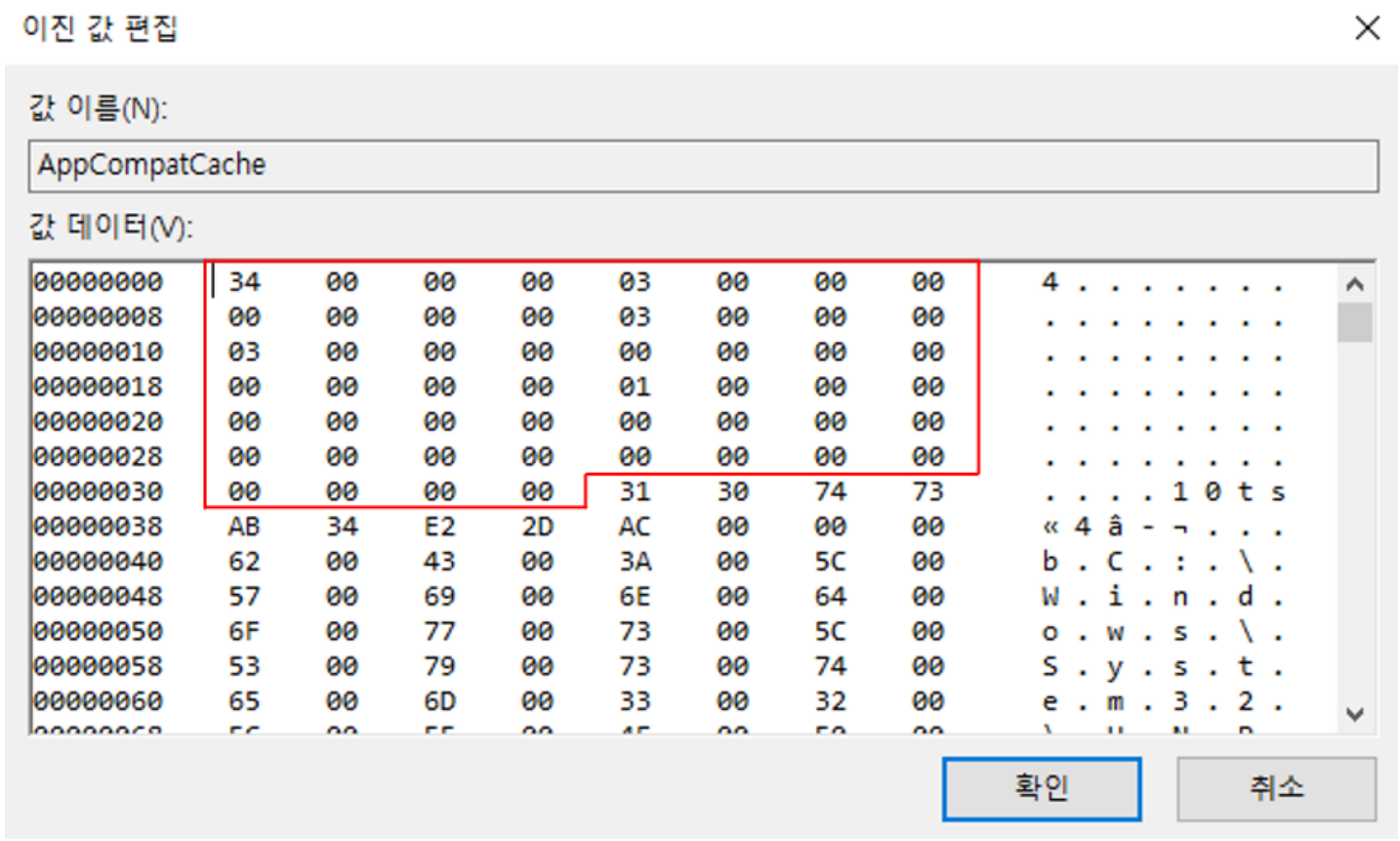
마지막 수정 시간 확인

침해사고 분석에 활용 가능

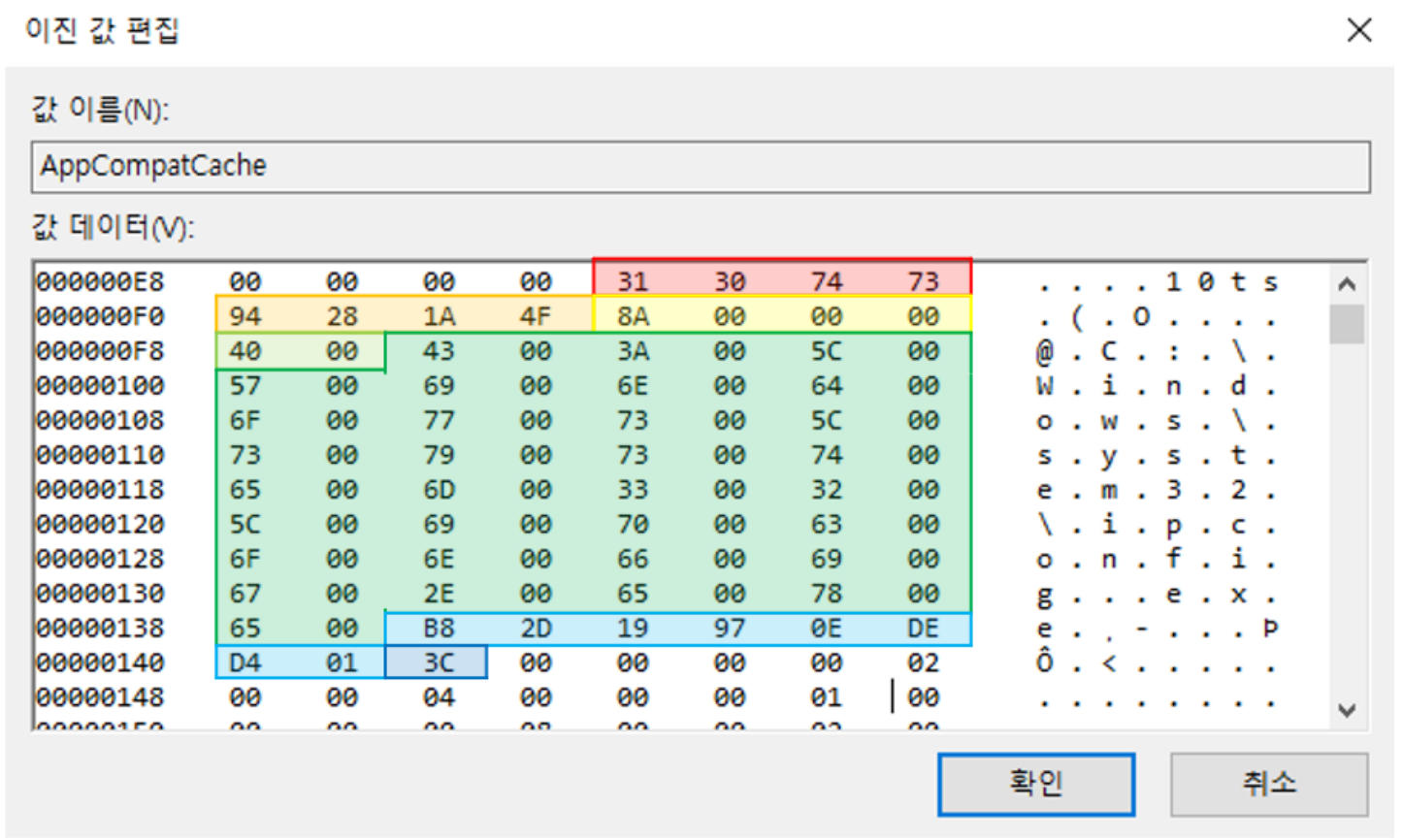
ShimCache Registry Path

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache

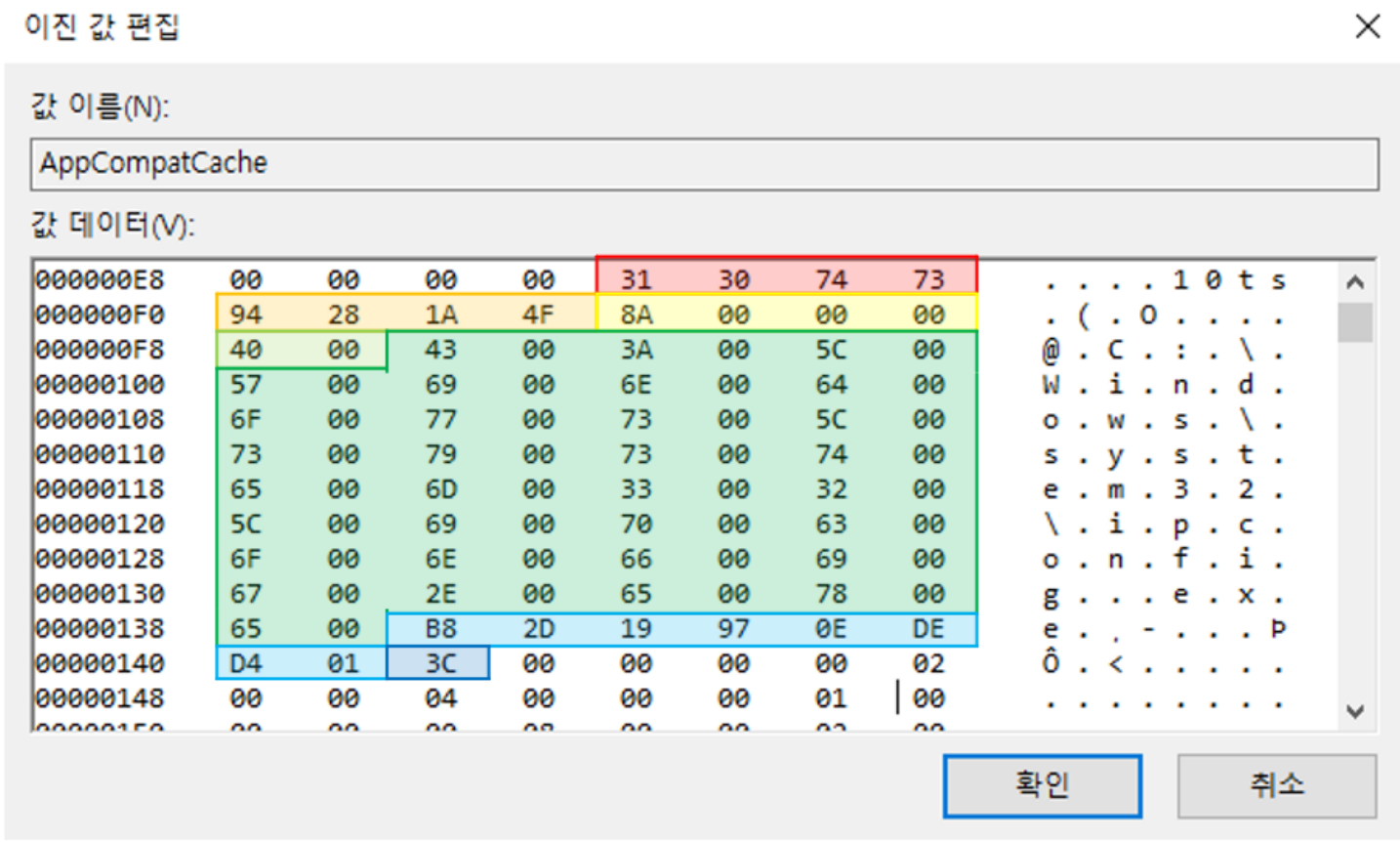
ShimCache Structure (Header)



ShimCache Structure (Entry)



오프셋	길이	설명
0x00 ~ 0x03	4byte	10ts (시그니처)
0x04 ~ 0x07	4byte	Unknown
0x08 ~ 0x1B	4byte	엔트리 크기
0x1C ~ 0x1D	2byte	경로 길이
0x1E ~ 0x??	가변byte	파일 경로
0x?? ~ 0x?? + 8	8byte	마지막 수정 시간
0x?? + 8 ~ 0x?? + 9	1byte	데이터 길이
0x?? + 9 ~	데이터 길이byte	데이터



ShimCache Parser

QnA