썸네일/아이콘 캐시 포렌식

JK Kim

@pr0neer

forensic-proof.com

proneer@gmail.com

개요

1. 썸네일 소개
2. 썸네일 분석
3. 아이콘 캐시 소개
4. 아이콘 캐시 분석

썸네일 소개

썸네일 소개

썸네일이란?

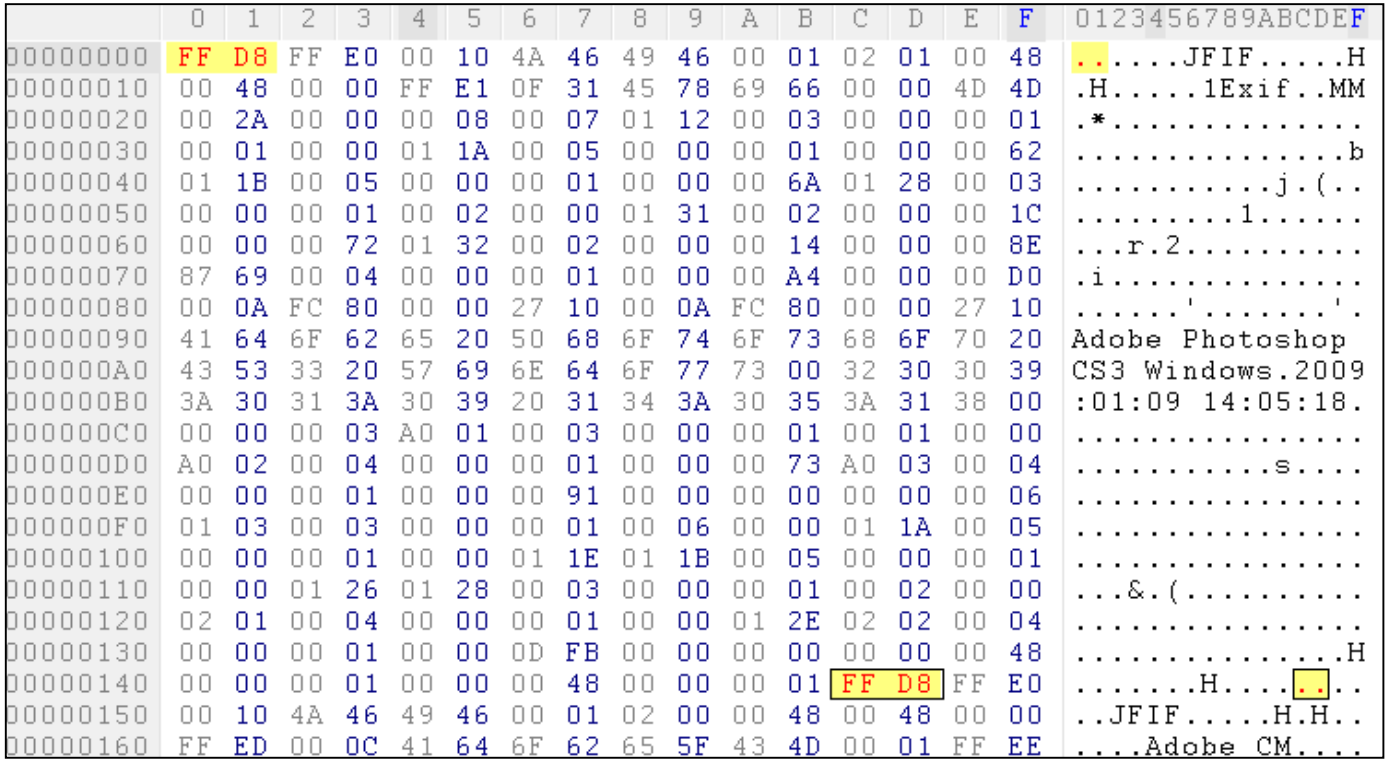
- 그래픽 이미지를 축소한 것으로 많은 양의 이미지를 빠르게 탐색하기 위한 것
- 윈도우 폴더 미리보기 기능에 사용
- 초기 방문 시 썸네일을 캐시해두고 재방문 시 캐시된 데이터 보여줌 ➔ 성능 향상
- 한번 저장된 썸네일은 원본 파일이 삭제되더라도 삭제되지 않음

- **썸네일 변화**
  - **윈도우 2K** : ADS(Alternative Data Stream)
  - **윈도우 XP** : Thumbs.db (폴더별)
  - **윈도우 Vista 이후** : Thumbcache_##.db (중앙집중식)

썸네일 소개

썸네일이란?

- **썸네일 지원 파일**
  - JPEG, BMP, GIF, TIF, PDF, HTM, PDF, PPTX, DOCX 등



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	02	01	00	48	......JFIF.....H
00000010	00	48	00	00	FF	E1	0F	31	45	78	69	66	00	00	4D	4D	.H.....1Exif..MM
00000020	00	2A	00	00	00	08	00	07	01	12	00	03	00	00	00	01	.*..............
00000030	00	01	00	00	01	1A	00	05	00	00	00	01	00	00	00	62	...............b
00000040	01	1B	00	05	00	00	00	01	00	00	00	6A	01	28	00	03	...........j.(..
00000050	00	00	00	01	00	02	00	00	01	31	00	02	00	00	00	1C	.........1......
00000060	00	00	00	72	01	32	00	02	00	00	00	14	00	00	00	8E	...r.2..........
00000070	87	69	00	04	00	00	00	01	00	00	00	A4	00	00	00	D0	.i..............
00000080	00	0A	FC	80	00	00	27	10	00	0A	FC	80	00	00	27	10	......'.......'.
00000090	41	64	6F	62	65	20	50	68	6F	74	6F	73	68	6F	70	20	Adobe Photoshop
000000A0	43	53	33	20	57	69	6E	64	6F	77	73	00	32	30	30	39	CS3 Windows.2009
000000B0	3A	30	31	3A	30	39	20	31	34	3A	30	35	3A	31	38	00	:01:09 14:05:18.
000000C0	00	00	00	03	A0	01	00	03	00	00	00	01	00	01	00	00	....
000000D0	A0	02	00	04	00	00	00	01	00	00	00	73	A0	03	00	04	...........s....
000000E0	00	00	00	01	00	00	00	91	00	00	00	00	00	00	00	06	....
000000F0	01	03	00	03	00	00	00	01	00	06	00	00	01	1A	00	05	....
00000100	00	00	00	01	00	00	01	1E	01	1B	00	05	00	00	00	01	....
00000110	00	00	01	26	01	28	00	03	00	00	00	01	00	02	00	00	...&.(..........
00000120	02	01	00	04	00	00	00	01	00	00	01	2E	02	02	00	04	....
00000130	00	00	00	01	00	00	0D	FB	00	00	00	00	00	00	00	48	...............H
00000140	00	00	00	01	00	00	00	48	00	00	00	01	FF	D8	FF	E0	.......H.......
00000150	00	10	4A	46	49	46	00	01	02	00	00	48	00	48	00	00	..JFIF.....H.H..
00000160	FF	ED	00	0C	41	64	6F	62	65	5F	43	4D	00	01	FF	EE	....Adobe CM....

윈도우 XP 썸네일

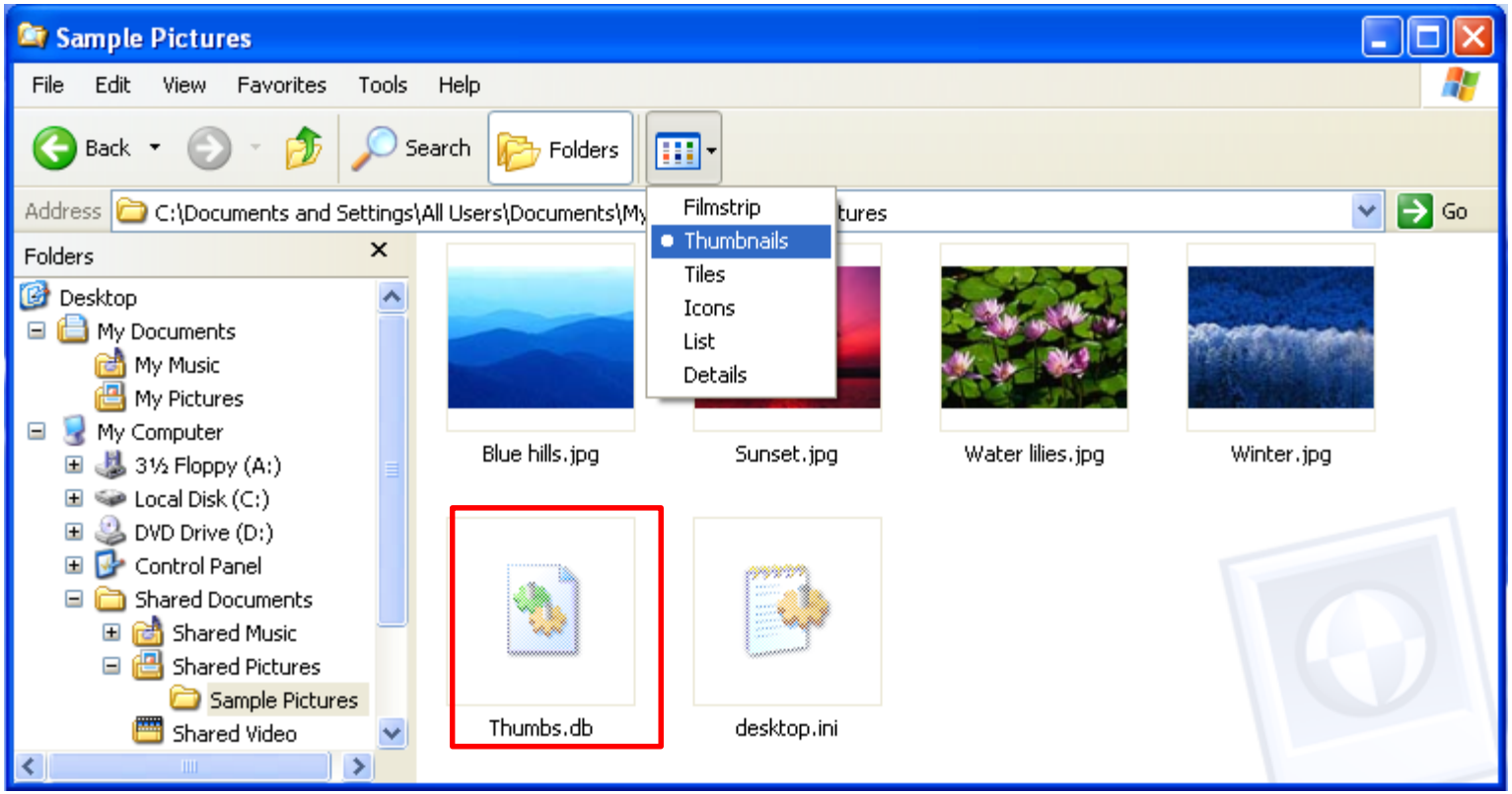
- **XP 썸네일**
  - 각 폴더마다 미리보기 수행 시 "Thumbs.db" 파일 생성

- **썸네일 픽셀 크기**
  - XP 썸네일 크기는 기본 **96x96**

  - **레지스트리 설정**
    - ✓ **Key** : HKEY_USER₩<USER SID>₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer
    - ✓ **Value** : ThumbnailSize 생성 (DWORD, 0x20~0x64)

윈도우 XP 썸네일

- **[Explorer] ➔ [View] ➔ [Thumbnails]**
  - [내 그림]폴더의 미리보기 ➔ 기본 4개의 파일 존재



썸네일 소개

윈도우 XP 썸네일

Microsoft Compound Document File Format

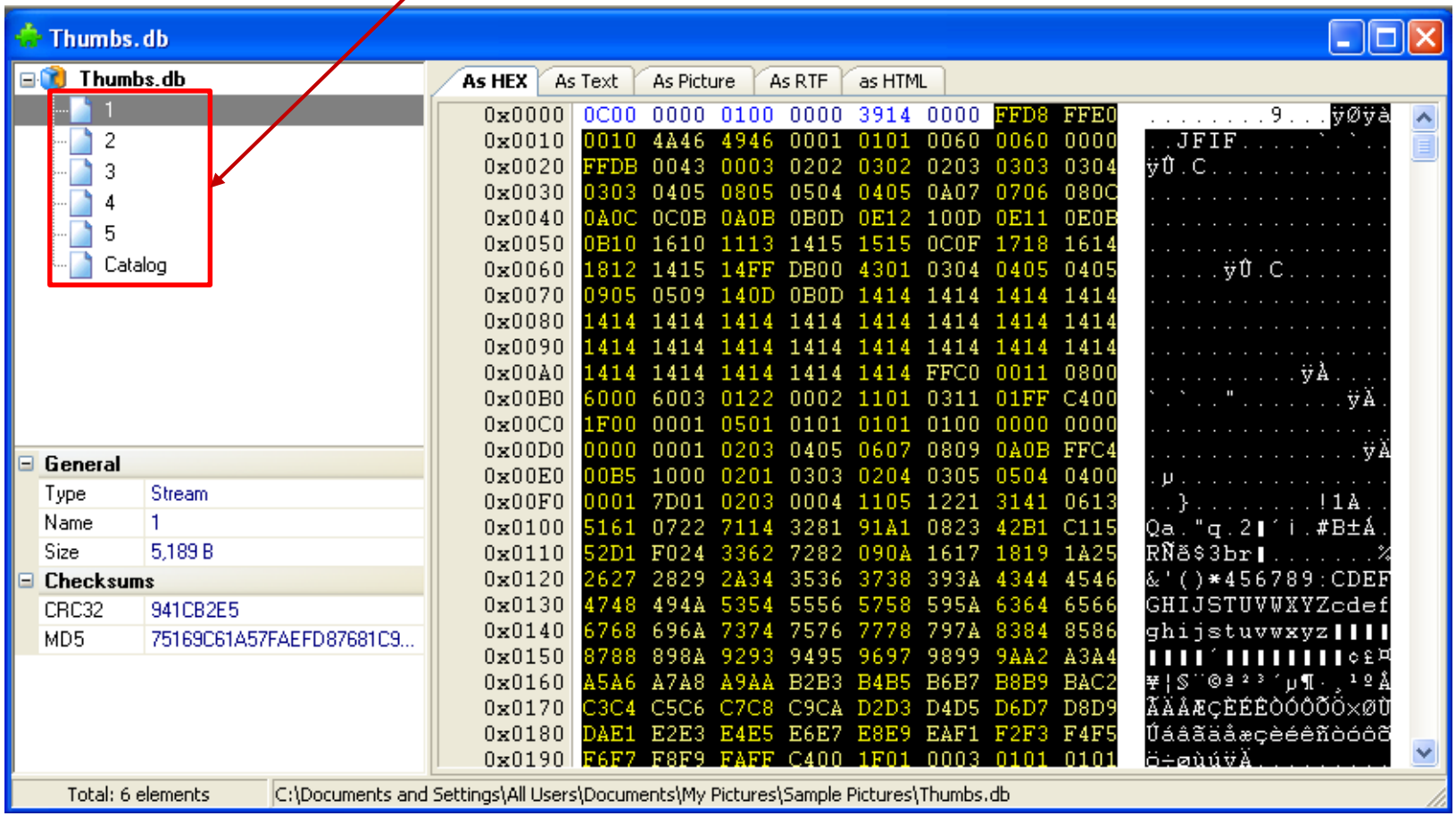
- **Thumbs.db**

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
001AF2000	D0	CF	11	E0	A1	B1	1A	E1	00	00	00	00	00	00	00	00
001AF2010	00	00	00	00	00	00	00	00	3E	00	03	00	FE	FF	09	00
001AF2020	06	00	00	00	00	00	00	00	00	00	00	00	01	00	00	00
001AF2030	01	00	00	00	00	00	00	00	00	10	00	00	0C	00	00	00
001AF2040	02	00	00	00	FE	FF	FF	FF	00	00	00	00	00	00	00	00
001AF2050	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
001AF2060	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
001AF2070	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
001AF2080	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
001AF2090	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
001AF20A0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
001AF20B0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
001AF20C0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
001AF20D0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
001AF20E0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
001AF20F0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
001AF2100	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
001AF2110	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
001AF2120	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
001AF2130	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
001AF2140	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
001AF2150	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
001AF2160	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
001AF2170	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
001AF2180	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
001AF2190	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
001AF21A0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
001AF21B0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF

썸네일 소개

윈도우 XP 썸네일

- **Thumbs.db ➔ SSView**
  - [내 그림] 폴더의 Thumbs.db에 저장된 썸네일이 5개인 이유는?

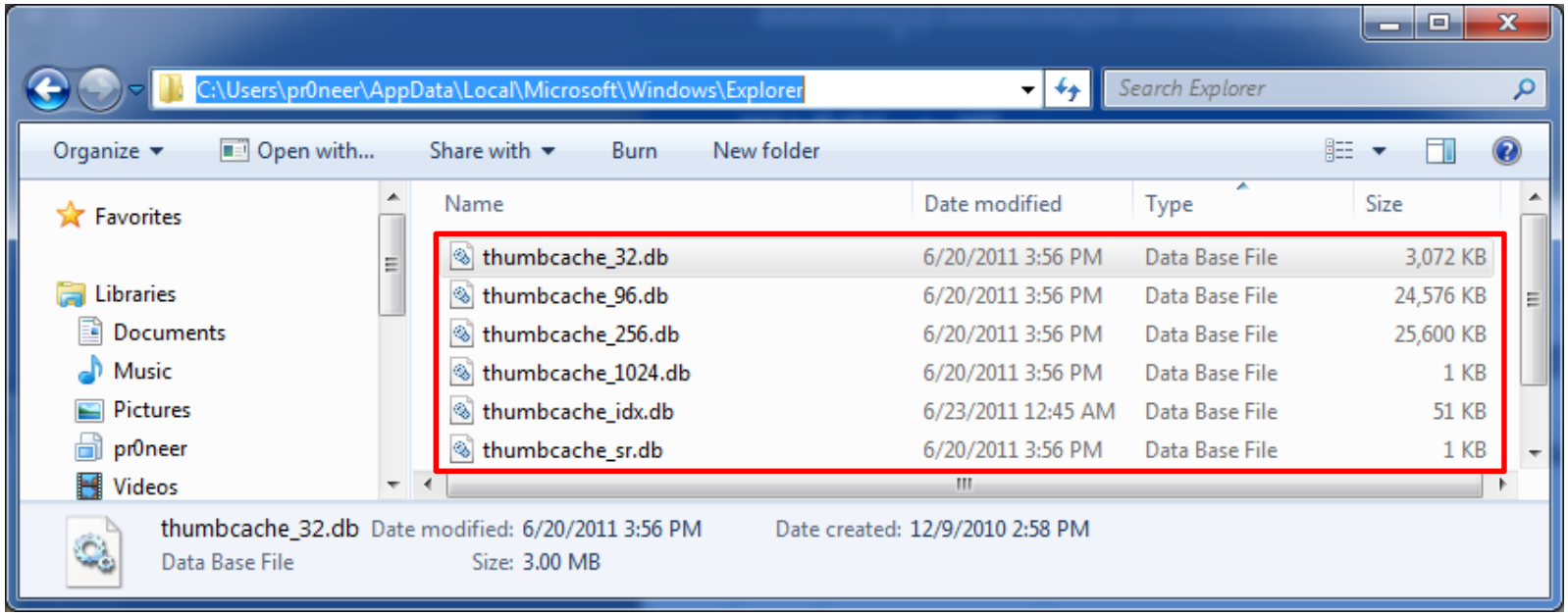


윈도우 XP 썸네일

- **Thumbnail Database Viewer**
  - [미리보기 폴더] 내용도 썸네일이 생성됨

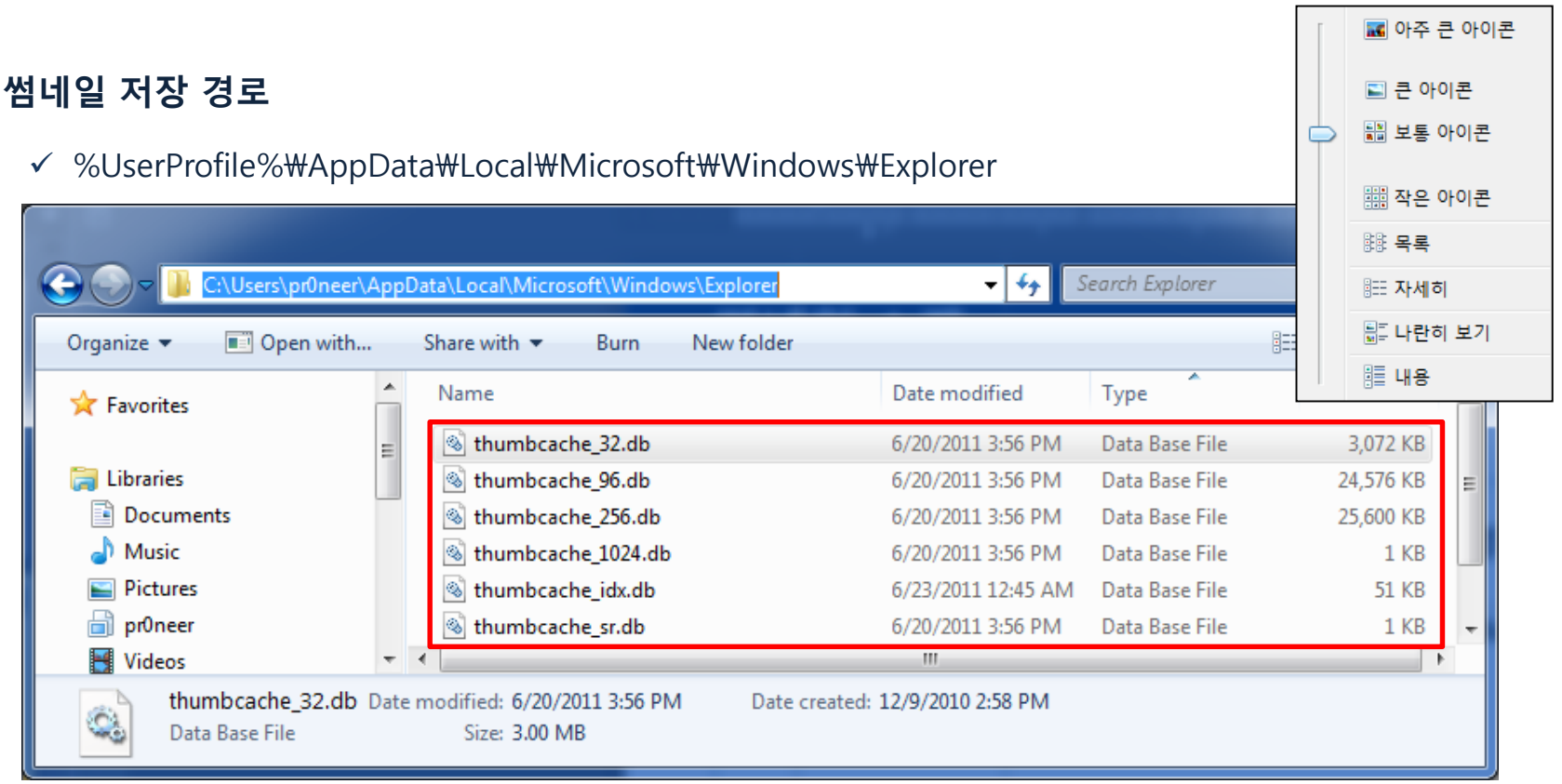
윈도우 Vista/7 썸네일

- **각 폴더의 Thumbs.db 파일 외에 추가적인 썸네일 캐쉬 사용**
  - %UserProfile%₩AppData₩Local₩Microsoft₩Windows₩Explorer



윈도우 Vista/7 썸네일

- **Vista/7 썸네일**
  - 시스템의 모든 썸네일은 크기 별로 중앙집중화되어 관리됨
  - 보통 아이콘(32x32), 큰 아이콘(96x96), 아주 큰 아이콘(256x256)
  - **썸네일 저장 경로**
    - ✓ %UserProfile%₩AppData₩Local₩Microsoft₩Windows₩Explorer

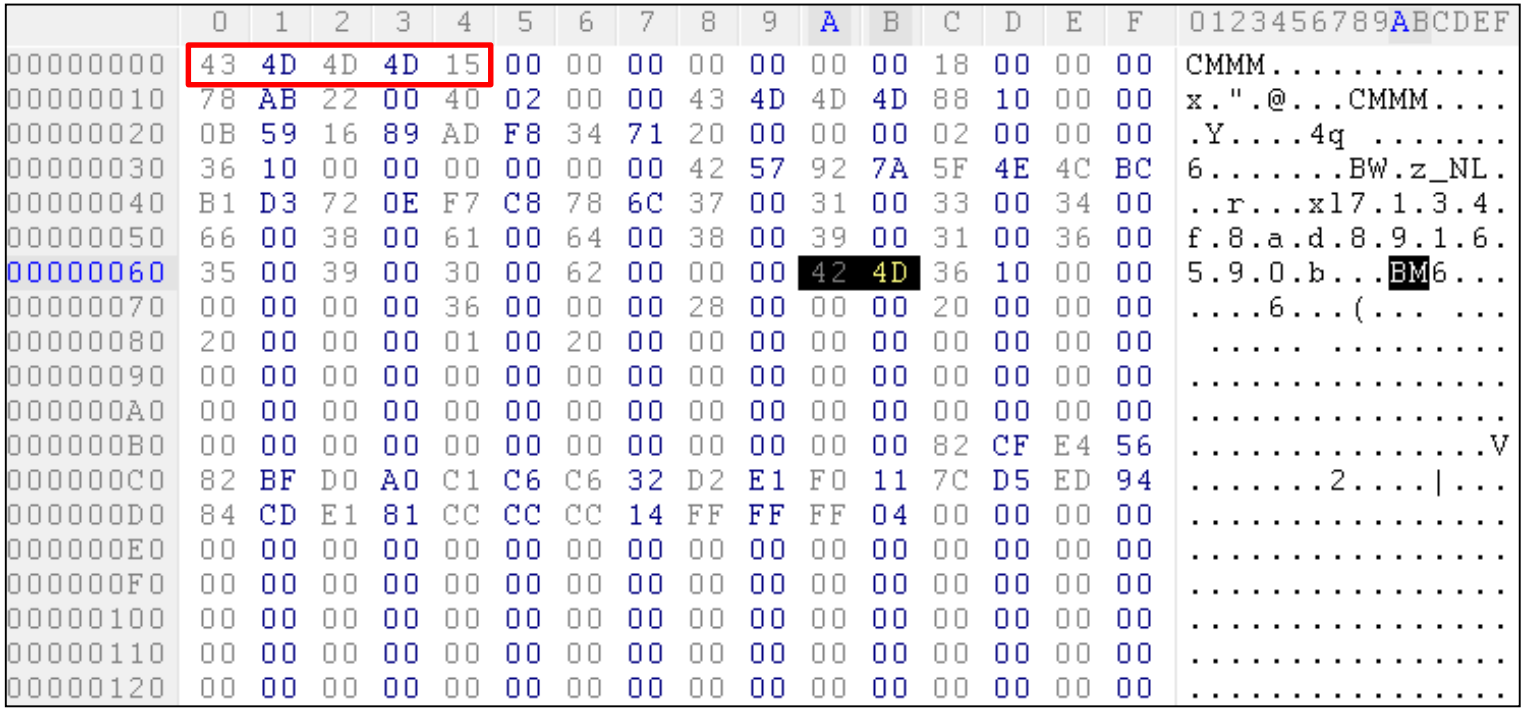


윈도우 Vista/7 썸네일

- **Thumbcache 분류**
  - **Thumbcache_idx.db**
    - ✓ 썸네일의 인덱스 정보
  - **Thumbcache_sr.db**
    - ✓ 알 수 없음
  - **Thumbcache_32.db**
    - ✓ 32x32 픽셀보다 작은 썸네일이 저장되며 모두 BMP 형식
  - **Thumbcache_96.db**
    - ✓ 32x32 ~ 96x96 픽셀 사이의 썸네일이 저장되며 모두 BMP 형식
  - **Thumbcache_256.db**
    - ✓ 96x96 ~ 256x256 픽셀 사이의 썸네일이 저장되며 JPEG 또는 PNG
  - **Thumbcache_1024.db**
    - ✓ 256x256 ~ 1024x2014 픽셀 사이의 썸네일이 저장되며 모두 JPEG

윈도우 Vista/7 썸네일

- **thumbcache_###.db 구조**
  - XP의 CDF 구조가 아닌 고유한 파일 형식
  - 헤더를 제외하고는 연속적으로 썸네일 저장 ➔ 단순 카빙으로도 추출 가능

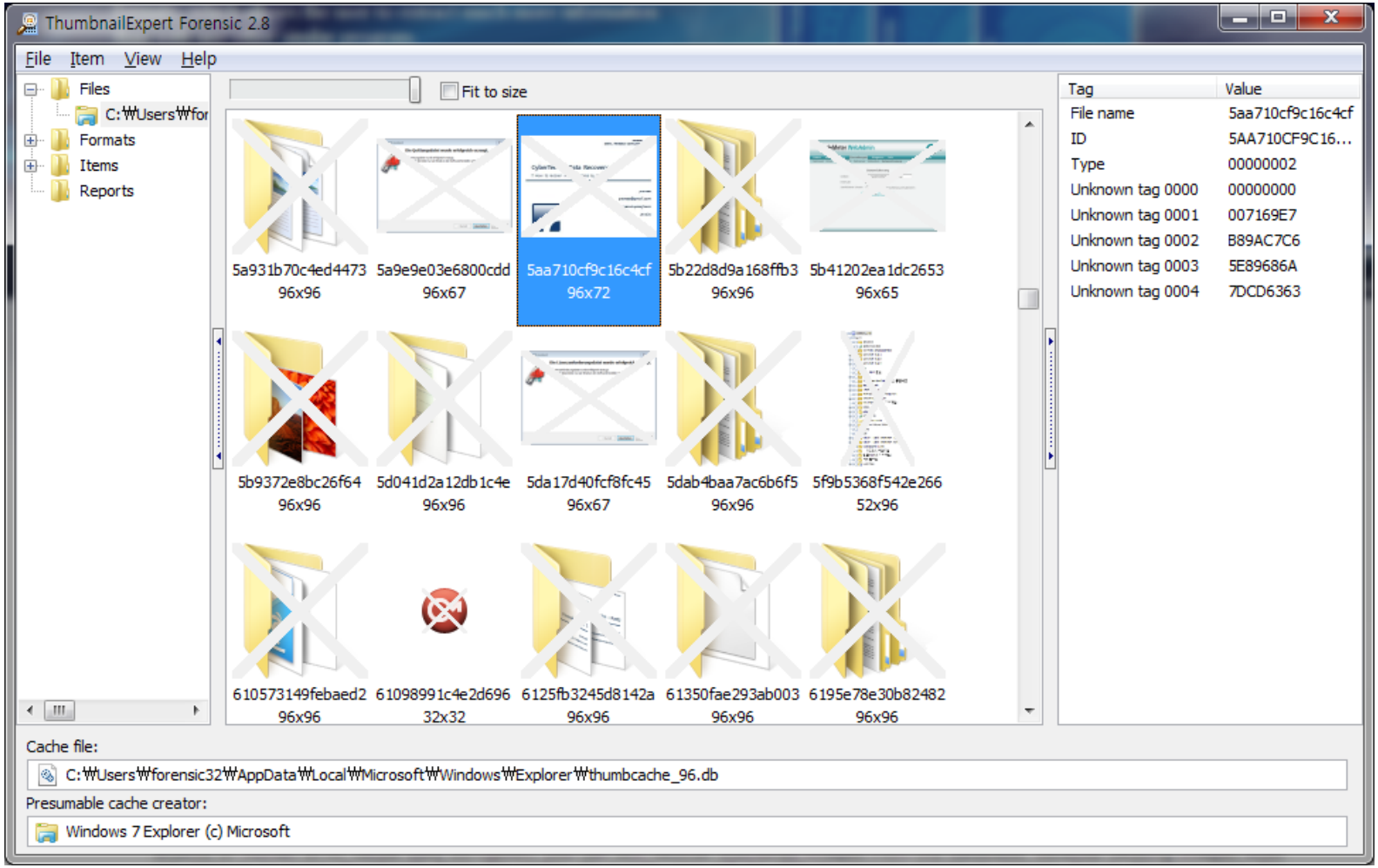


	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
00000000	43	4D	4D	4D	15	00	00	00	00	00	00	00	18	00	00	00	CMMM.....
00000010	78	AB	22	00	40	02	00	00	43	4D	4D	4D	88	10	00	00	x."..@...CMMM....
00000020	0B	59	16	89	AD	F8	34	71	20	00	00	00	02	00	00	00	.Y....4q .....
00000030	36	10	00	00	00	00	00	00	42	57	92	7A	5F	4E	4C	BC	6.......BW.z_NL.
00000040	B1	D3	72	0E	F7	C8	78	6C	37	00	31	00	33	00	34	00	..r...xl7.1.3.4.
00000050	66	00	38	00	61	00	64	00	38	00	39	00	31	00	36	00	f.8.a.d.8.9.1.6.
00000060	35	00	39	00	30	00	62	00	00	00	42	4D	36	10	00	00	5.9.0.b...BM6...
00000070	00	00	00	00	36	00	00	00	28	00	00	00	20	00	00	00	....6...(... ...
00000080	20	00	00	00	01	00	20	00	00	00	00	00	00	00	00	00	....
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	82	CF	E4	56	V
000000C0	82	BF	D0	A0	C1	C6	C6	32	D2	E1	F0	11	7C	D5	ED	94	.....2....|...
000000D0	84	CD	E1	81	CC	CC	CC	14	FF	FF	FF	04	00	00	00	00	.....
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

썸네일 분석

썸네일 분석 도구

- **ThumbnailExpert Forensic** – http://www.thumbnailexpert.com/



썸네일 활용하기

- **그래픽, 동영상, 문서 파일의 존재 유무**
  - 파일 미리보기 시 자동 썸네일되기 때문에 특정 파일의 존재 유무 판단

- **저작물, 권리 문서 확인**
  - 문서 파일의 경우 첫 페이지가 썸네일되기 때문에 문서의 내용 확인 가능
  - 그래픽, 동영상의 경우 원본 저작물의 썸네일과 조사 대상 시스템의 썸네일 비교

- **음란물 조사**
  - 음란물 열람 시 자동 썸네일되기 때문에 아청법 조사에 활용

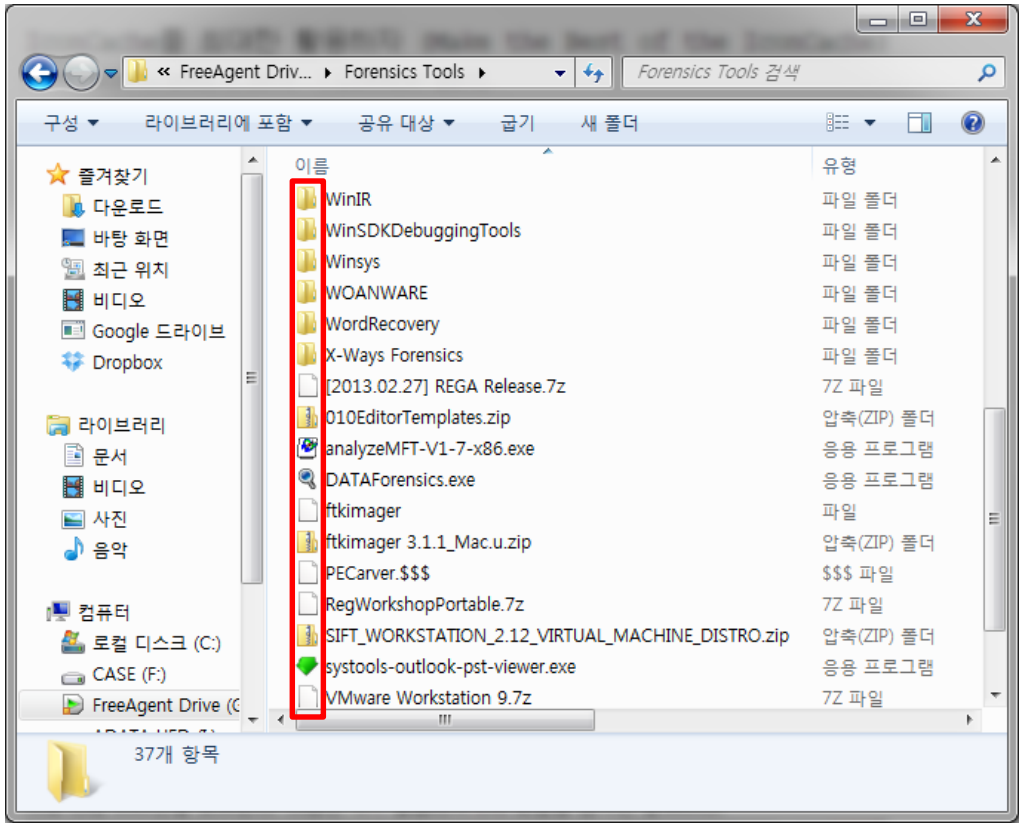
실습 #1

- 썸네일 흔적 확인하기

아이콘 캐시 소개

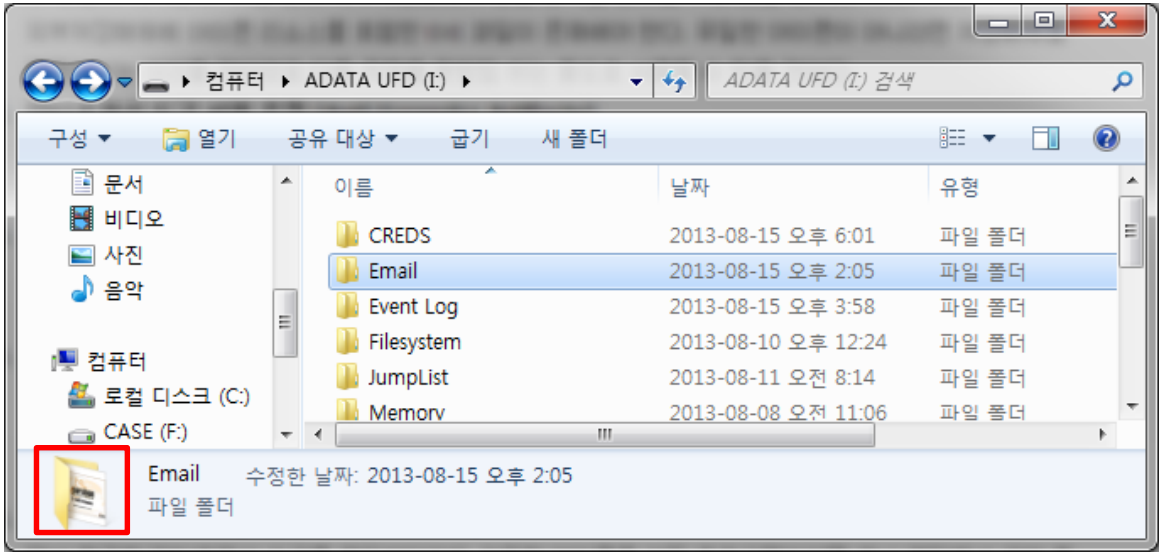
아이콘 캐시란?

- **탐색기 아이콘**
  - 탐색기는 파일 형식에 따라 다양한 아이콘을 표현
  - 아이콘도 미리 캐시해둔 후 재방문 시 빠르게 로드



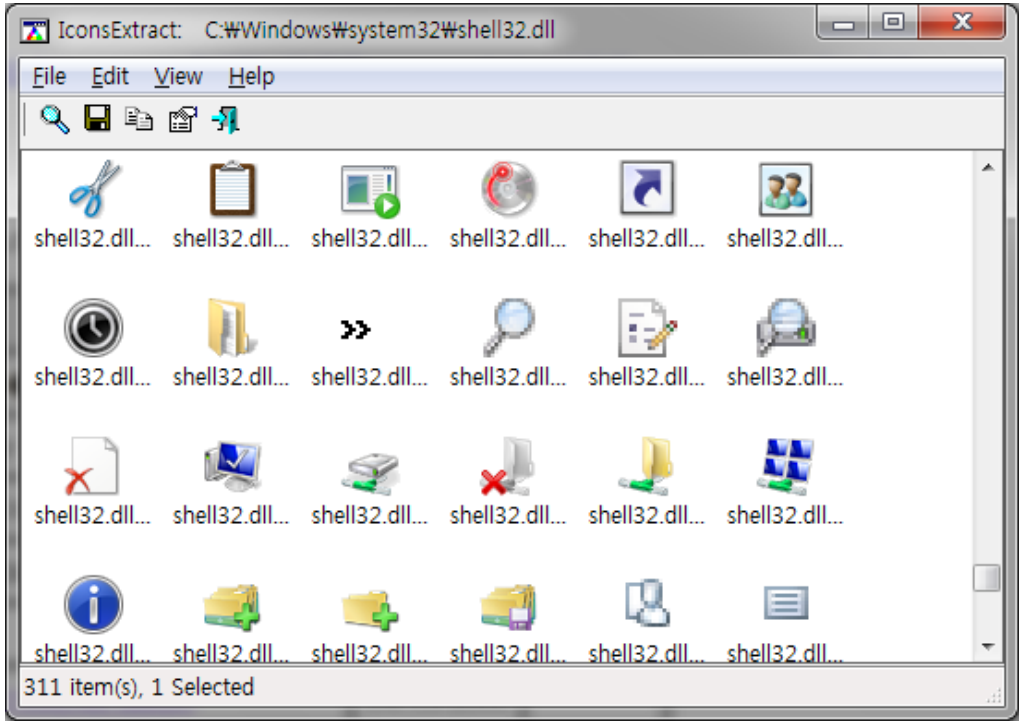
아이콘 캐시란?

- **아이콘 캐시 시점**
  - 폴더 내용 확인 시 로드되는 아이콘 캐시됨
  - 인터넷에서 다운로드 받을 경우, 폴더 내용을 확인하지 않더라고 캐시됨
  - 폴더 내용을 확인하지 않더라도 "수정 시간"을 기준으로 최근 2개의 아이템 캐시됨



아이콘 가져오기

- **각 유형별 가져오기**
  - 폴더, 파일 등 윈도우 탐색기 기본 아이콘 ➔ %SystemRoot%₩system32₩shell32.dll
  - 워드, 엑셀, 파워포인트, 한글 ➔ 각 응용프로그램 실행 파일의 리소스 영역
  - 실행 파일 ➔ 실행 파일의 리소스 영역



아이콘 캐시하기

- **운영체제 별 아이콘 캐시**
  - **윈도우 9x/NT4/2K**
    - ✓ %SystemDrive%₩Windows₩**ShellIconCache**
    - ✓ %SystemDrive%:₩Winnt₩**ShellIconCache**
  - **윈도우 XP**
    - ✓ %UserProfile%₩Local Settings₩Application Data₩**IconCache.유**
  - **윈도우 Vista/7**
    - ✓ %UserProfile%₩AppData₩Local₩**IconCache.db**

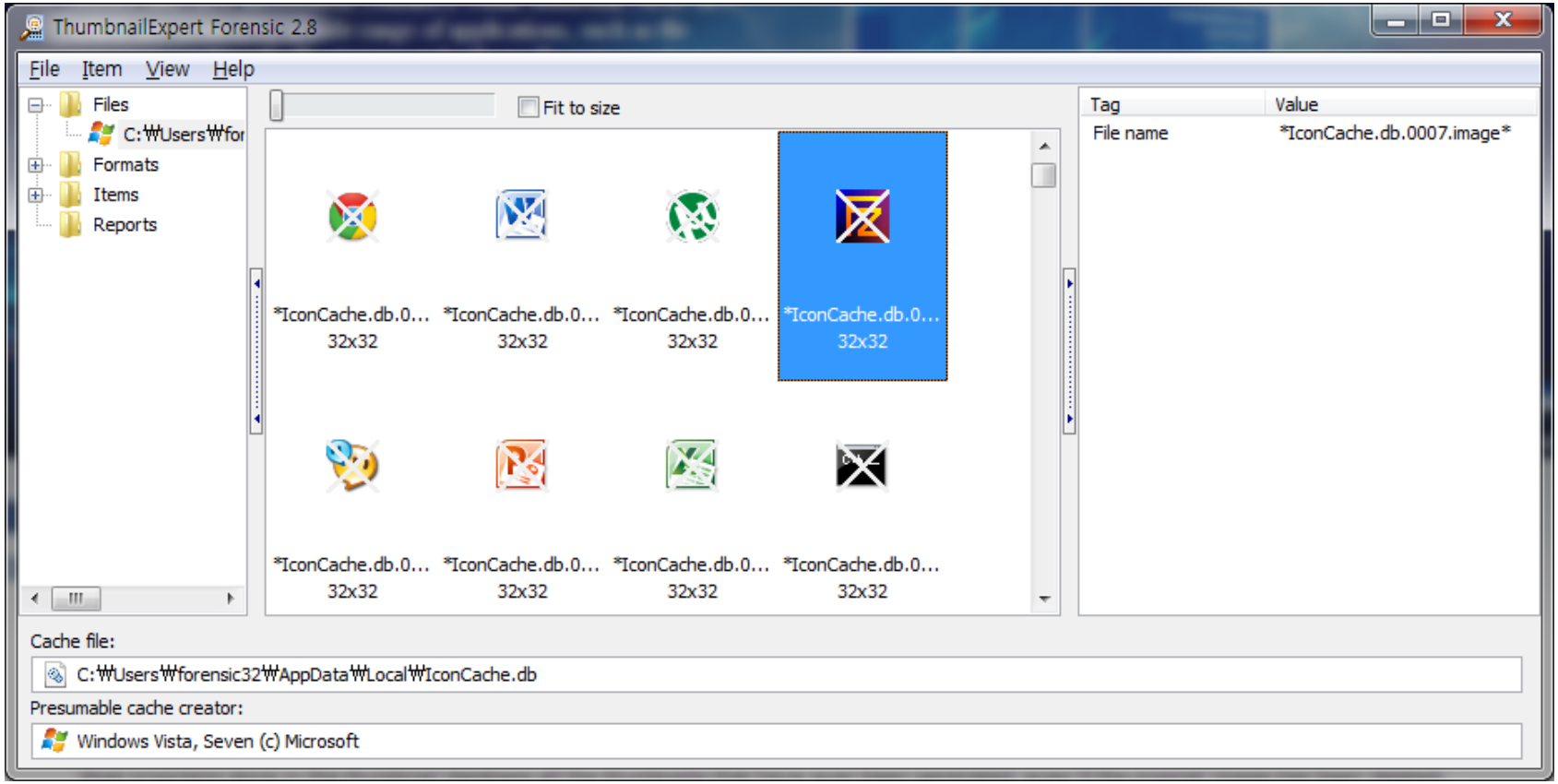
아이콘 캐시 분석

아이콘 캐시 동작

- **메모리와 아이콘 캐시**
  - **윈도우 시작 시 아이콘 캐시를 메모리에 로드**
    - ✓ 기본 500개 아이콘 캐시
    - ✓ 설정된 값 초과 시 아이콘이 검게 나오는 등의 이상 현상
    - ✓ 레지스트리 아이콘 캐시 개수 설정
      - **Key** : HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer
      - **Value** : Max Cached Icons (String, 100-4096) (Default 500)
  - **윈도우 종료 시 아이콘 캐시 업데이트**
    - ✓ 재부팅 전에는 새롭게 캐시된 내용 확인 불가능

분석 도구

- **ThumbnailExpert** – http://www.thumbnailexpert.com/



아이콘 캐시 활용하기

- **외부저장장치/광학드라이브 사용 흔적**
  - 외부저장장치의 유일한 실행 파일이 존재할 경우, 아이콘 캐시를 통해 연결 확인
  - XP의 경우, 경로 정보를 이용해 외부저장장치 및 광학드라이브 연결 확인

- **안티 포렌식 도구 사용 흔적**
  - 전문 안티포렌식 도구는 대부분 고유한 아이콘 사용

- **악성코드 흔적**
  - 애드웨어류와 같이 아이콘을 보유하고 있는 악성코드 흔적 확인

- **프로그램 사용 흔적**
  - 안티 포렌식 도구 이외에 고유한 아이콘을 가진 프로그램이라면 흔적 확인 가능

아이콘 캐시 분석

실습 #2

- 아이콘 캐시 흔적 확인하기

질문 및 답변