분석 파일 : USB Image.001

사용 Tool :

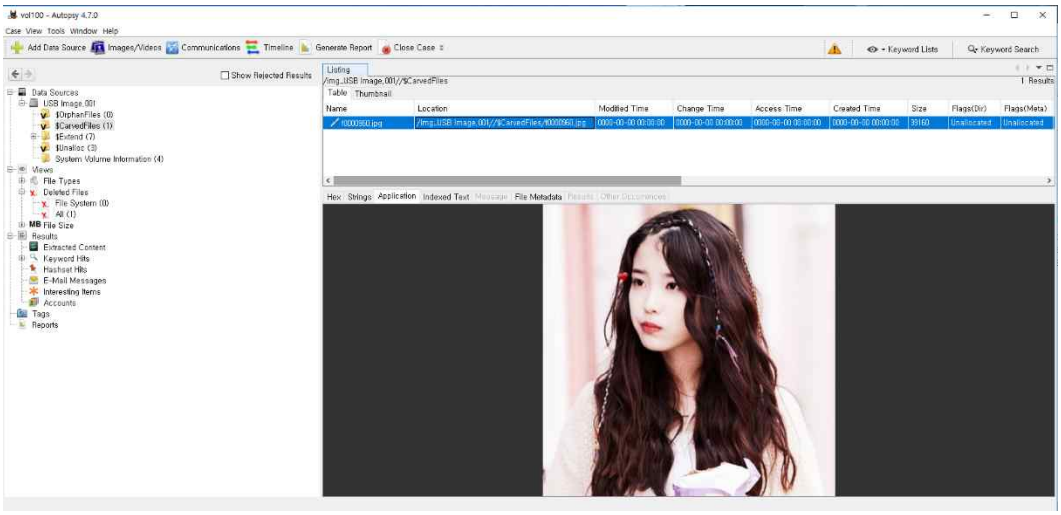
Autopsy : https://www.sleuthkit.org/autopsy/

Winhex : https://www.x-ways.net/winhex/

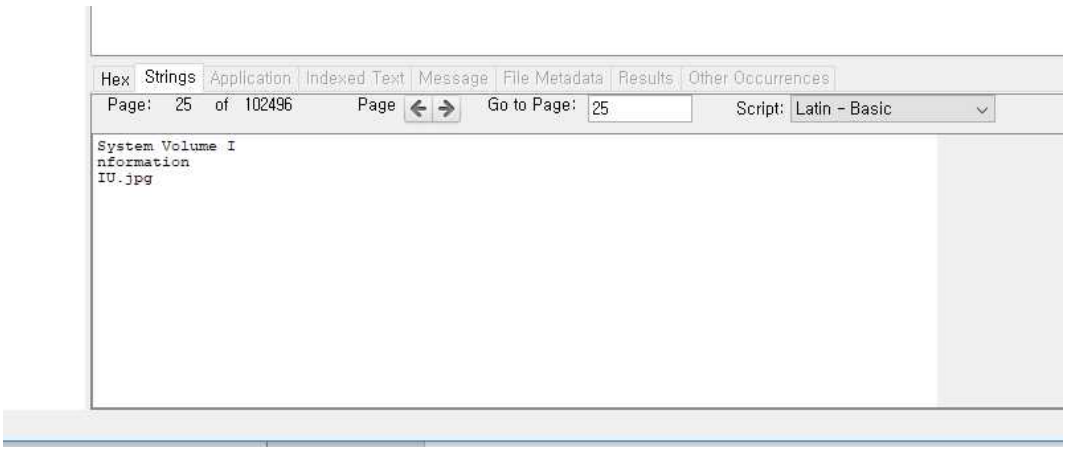
처음으로 USB의 구조를 확인하기 위해 Autopsy와 Winhex을 사용하였고 MFT구조를 가지는 NTFS시스템을 사용하고 있는 것을 확인하였다.

하지만 빠른 포맷을 통해 포맷을 하였고 이전에는 현재 파일 시스템과 다른 파일시스템을 사용하였다고 사용자는 진술 하였다.

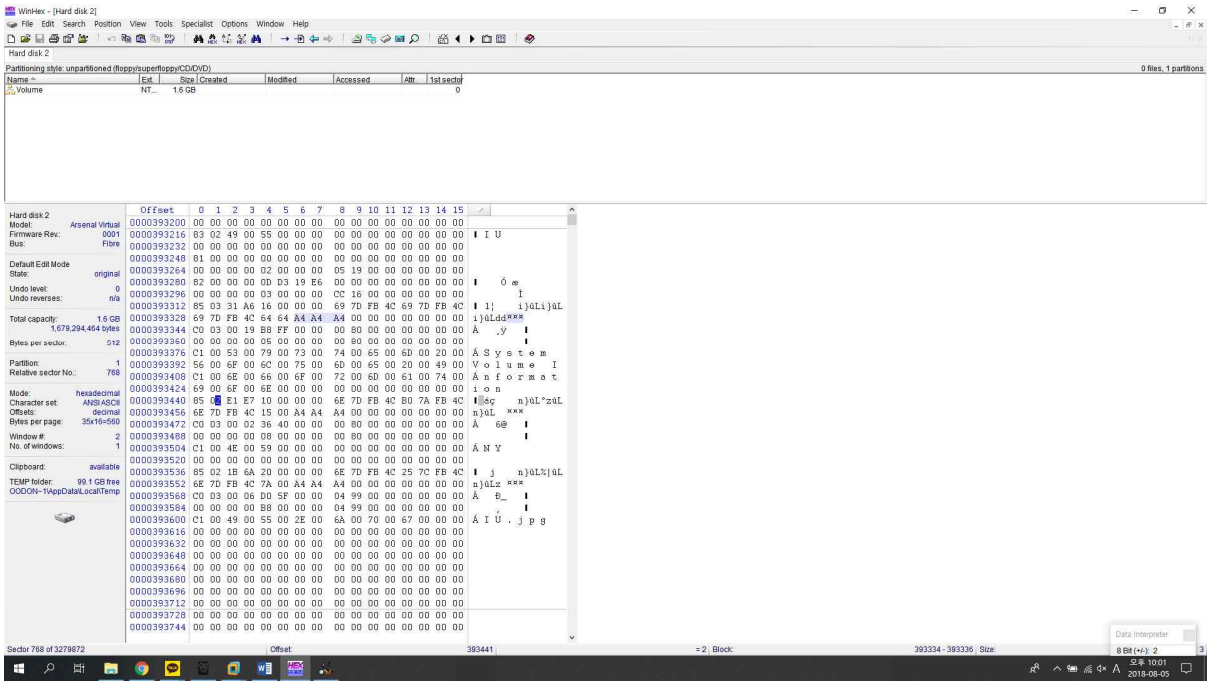
Autopsy 카빙기능을 이용하여 할당되지 않은 영역중 IU이미지로 보이는 JPG파일을 찾아내었고



또한 Autopsy을 이용하여 String값으로 찾아보던 중 아래의 키워드를 찾아내었다.



Winhex를 통해 키워드 검색을 하였고. exFAT Directory Structure구조가 보이는 섹터를 찾았다.



IU이미지의 Directory Entry

```
85 02 1B 6A 20 00 00 00  6E 7D FB 4C 25 7C FB 4C  ▌  j     n}ûL%|ûL
6E 7D FB 4C 7A 00 A4 A4  A4 00 00 00 00 00 00 00  n}ûLz ¤¤¤
C0 03 00 06 D0 5F 00 00  04 99 00 00 00 00 00 00  À   Ð_   ▌
00 00 00 00 B8 00 00 00  04 99 00 00 00 00 00 00      ¸    ▌
C1 00 49 00 55 00 2E 00  6A 00 70 00 67 00 00 00  Á I U . j p g
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Convert Unix timestamp

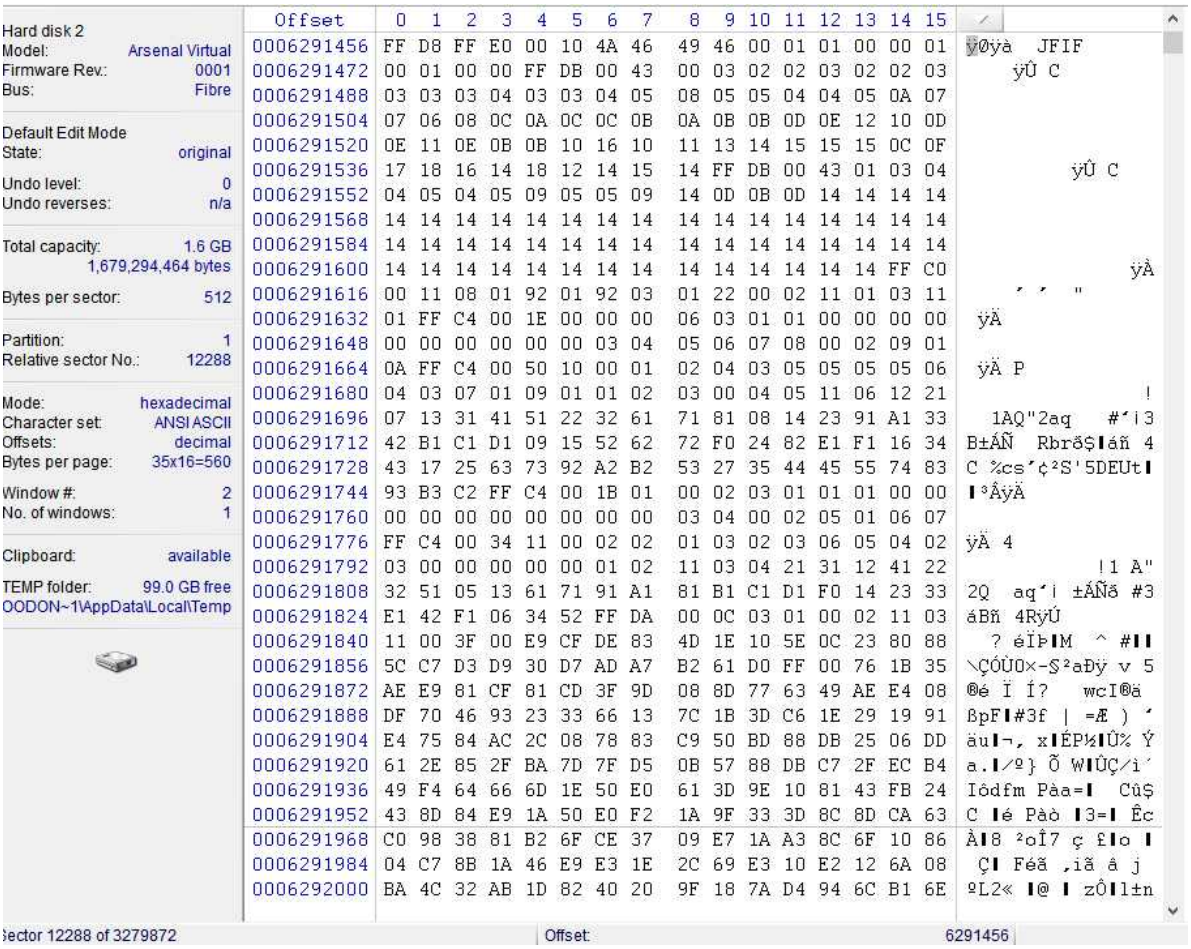
CreateTime : 4CFB7D6E -> 2010년 12월 5일 8:54:22

Last Modified Time : 4CFB7C25 -> 2010년 12월 5일 8:48:53

Last Accessed Time : 4CFB7D6E -> 2010년 12월 5일 8:54:22

First Cluster : B8 -> (184 * 8)(1472섹터) +64(섹터) = (1536 * 8)(12288섹터)

IU.jpg의 실질데이터 영역



Hard disk 2
Model: Arsenal Virtual
Firmware Rev.: 0001
Bus: Fibre

Default Edit Mode
State: original

Undo level: 0
Undo reverses: n/a

Total capacity: 1.6 GB
1,679,294,464 bytes

Bytes per sector: 512

Partition: 1
Relative sector No.: 12288

Mode: hexadecimal
Character set: ANSI ASCII
Offsets: decimal
Bytes per page: 35x16=560

Window #: 2
No. of windows: 1

Clipboard: available

TEMP folder: 99.0 GB free
OODON~1\AppData\Local\Temp

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0006291456	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	00	00	01
0006291472	00	01	00	00	FF	DB	00	43	00	03	02	02	03	02	02	03
0006291488	03	03	03	04	03	03	04	05	08	05	05	04	04	05	0A	07
0006291504	07	06	08	0C	0A	0C	0C	0B	0A	0B	0B	0D	0E	12	10	0D
0006291520	0E	11	0E	0B	0B	10	16	10	11	13	14	15	15	15	0C	0F
0006291536	17	18	16	14	18	12	14	15	14	FF	DB	00	43	01	03	04
0006291552	04	05	04	05	09	05	05	09	14	0D	0B	0D	14	14	14	14
0006291568	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14
0006291584	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14
0006291600	14	14	14	14	14	14	14	14	14	14	14	14	14	14	FF	C0
0006291616	00	11	08	01	92	01	92	03	01	22	00	02	11	01	03	11
0006291632	01	FF	C4	00	1E	00	00	00	06	03	01	01	00	00	00	00
0006291648	00	00	00	00	00	00	03	04	05	06	07	08	00	02	09	01
0006291664	0A	FF	C4	00	50	10	00	01	02	04	03	05	05	05	05	06
0006291680	04	03	07	01	09	01	01	02	03	00	04	05	11	06	12	21
0006291696	07	13	31	41	51	22	32	61	71	81	08	14	23	91	A1	33
0006291712	42	B1	C1	D1	09	15	52	62	72	F0	24	82	E1	F1	16	34
0006291728	43	17	25	63	73	92	A2	B2	53	27	35	44	45	55	74	83
0006291744	93	B3	C2	FF	C4	00	1B	01	00	02	03	01	01	01	00	00
0006291760	00	00	00	00	00	00	00	00	03	04	00	02	05	01	06	07
0006291776	FF	C4	00	34	11	00	02	02	01	03	02	03	06	05	04	02
0006291792	03	00	00	00	00	00	01	02	11	03	04	21	31	12	41	22
0006291808	32	51	05	13	61	71	91	A1	81	B1	C1	D1	F0	14	23	33
0006291824	E1	42	F1	06	34	52	FF	DA	00	0C	03	01	00	02	11	03
0006291840	11	00	3F	00	E9	CF	DE	83	4D	1E	10	5E	0C	23	80	88
0006291856	5C	C7	D3	D9	30	D7	AD	A7	B2	61	D0	FF	00	76	1B	35
0006291872	AE	E9	81	CF	81	CD	3F	9D	08	8D	77	63	49	AE	E4	08
0006291888	DF	70	46	93	23	33	66	13	7C	1B	3D	C6	1E	29	19	91
0006291904	E4	75	84	AC	2C	08	78	83	C9	50	BD	88	DB	25	06	DD
0006291920	61	2E	85	2F	BA	7D	7F	D5	0B	57	88	DB	C7	2F	EC	B4
0006291936	49	F4	64	66	6D	1E	50	E0	61	3D	9E	10	81	43	FB	24
0006291952	43	8D	84	E9	1A	50	E0	F2	1A	9F	33	3D	8C	8D	CA	63
0006291968	C0	98	38	81	B2	6F	CE	37	09	E7	1A	A3	8C	6F	10	86
0006291984	04	C7	8B	1A	46	E9	E3	1E	2C	69	E3	10	E2	12	6A	08
0006292000	BA	4C	32	AB	1D	82	40	20	9F	18	7A	D4	94	6C	B1	6E

Sector 12288 of 3279872 | Offset: 6291456

파일명 : IU.jpg

MD5 : 9da42a4e002946ebec3f7b6b51020813