[BOB7]포렌식_유동민_MBR/EBR

MBR

HxD - [C:\Users\YooDongMin\Desktop\강대명멘토\mbr_128.dd]

파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 기타 설정(X) 창 설정(W) ?

16 | ANSI | 10 진수 | 섹터 0 (262144 중)

mbr_128.dd

```
Offset(d)   00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
000000000   33 C0 8E D0 BC 00 7C 8E C0 8E D8 BE 00 7C BF 00   3ÀŽĐ¼.|ŽÀŽØ¾.|¿.
000000016   06 B9 00 02 FC F3 A4 50 68 1C 06 CB FB B9 04 00   .¹..üó¤Ph..Ëû¹..
000000032   BD BE 07 80 7E 00 00 7C 0B 0F 85 0E 01 83 C5 10   ½¾.€~..|..….ƒÅ.
000000048   E2 F1 CD 18 88 56 00 55 C6 46 11 05 C6 46 10 00   âñÍ.^V.UÆF..ÆF..
000000064   B4 41 BB AA 55 CD 13 5D 72 0F 81 FB 55 AA 75 09   ´A»ªUÍ.]r..ûUªu.
000000080   F7 C1 01 00 74 03 FE 46 10 66 60 80 7E 10 00 74   ÷Á..t.þF.f`€~..t
000000096   26 66 68 00 00 00 00 66 FF 76 08 68 00 00 68 00   &fh....fÿv.h..h.
000000112   7C 68 01 00 68 10 00 B4 42 8A 56 00 8B F4 CD 13   |h..h..´BŠV.<ôÍ.
000000128   9F 83 C4 10 9E EB 14 B8 01 02 BB 00 7C 8A 56 00   ŸƒÄ.žë.¸..».|ŠV.
000000144   8A 76 01 8A 4E 02 8A 6E 03 CD 13 66 61 73 1C FE   Šv.ŠN.Šn.Í.fas.þ
000000160   4E 11 75 0C 80 7E 00 80 0F 84 8A 00 B2 80 EB 84   N.u.€~.€..„Š.²€ë„
000000176   55 32 E4 8A 56 00 CD 13 5D EB 9E 81 3E FE 7D 55   U2äŠV.Í.]ëž.>þ}U
000000192   AA 75 6E FF 76 00 E8 8D 00 75 17 FA B0 D1 E6 64   ªunÿv.è..u.ú°Ñæd
000000208   E8 83 00 B0 DF E6 60 E8 7C 00 B0 FF E6 64 E8 75   èƒ.°ßæ`è|.°ÿædèu
000000224   00 FB B8 00 BB CD 1A 66 23 C0 75 3B 66 81 FB 54   .û¸.»Í.f#Àu;f.ûT
000000240   43 50 41 75 32 81 F9 02 01 72 2C 66 68 07 BB 00   CPAu2.ù..r,fh.».
000000256   00 66 68 00 02 00 00 66 68 08 00 00 00 66 53 66   .fh....fh....fSf
000000272   53 66 55 66 68 00 00 00 00 66 68 00 7C 00 00 66   SfUfh....fh.|..f
000000288   61 68 00 00 07 CD 1A 5A 32 F6 EA 00 7C 00 00 CD   ah...Í.Z2öê.|..Í
000000304   18 A0 B7 07 EB 08 A0 B6 07 EB 03 A0 B5 07 32 E4   . ·.ë. ¶.ë. µ.2ä
000000320   05 00 07 8B F0 AC 3C 00 74 09 BB 07 00 B4 0E CD   ...<ð¬<.t.».´.Í
000000336   10 EB F2 F4 EB FD 2B C9 E4 64 EB 00 24 02 E0 F8   .ëòôëý+Éädë.$.àø
000000352   24 02 C3 49 6E 76 61 6C 69 64 20 70 61 72 74 69   $.ÃInvalid parti
000000368   74 69 6F 6E 20 74 61 62 6C 65 2E 45 72 72 6F 72   tion table.Error
000000384   20 6C 6F 61 64 69 6E 67 20 6F 70 65 72 61 74 69    loading operati
000000400   6E 67 20 73 79 73 74 65 6D 00 4D 69 73 73 69 6E   ng system.Missin
000000416   67 20 6F 70 65 72 61 74 69 6E 67 20 73 79 73 74   g operating syst
000000432   65 6D 00 00 00 63 7B 9A 90 38 54 94 00 00 00 02   em...c{š.8T".....
000000448   03 00 07 8E 0C 02 80 00 00 00 00 A0 00 00 00 8E   ...Ž..€.... ...Ž
000000464   0D 02 07 1B 16 05 80 A0 00 00 00 A0 00 00 00 1B   .....€ ... ...
000000480   17 05 07 A7 20 07 80 40 01 00 00 A0 00 00 00 A7   ...§ .€@... ...§
000000496   21 07 05 FE 3F 0F 80 E0 01 00 00 10 02 00 55 AA   !..þ?.€à......Uª
000000512   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
000000528   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
000000544   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
000000560   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
000000576   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
000000592   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
000000608   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
000000624   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
000000640   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```
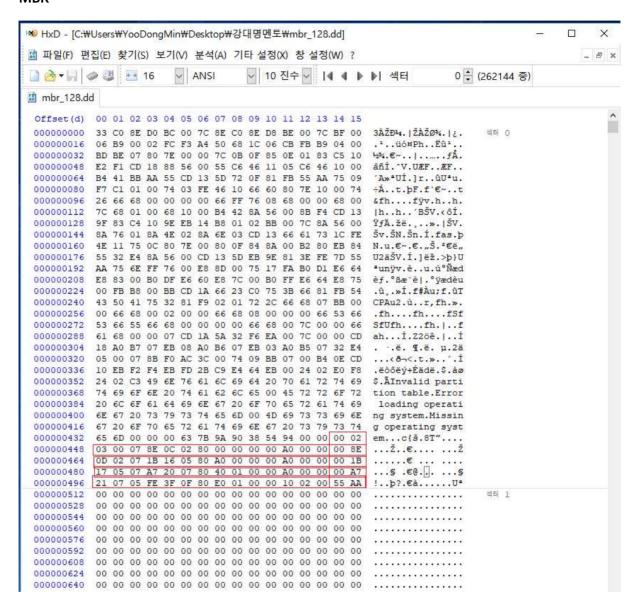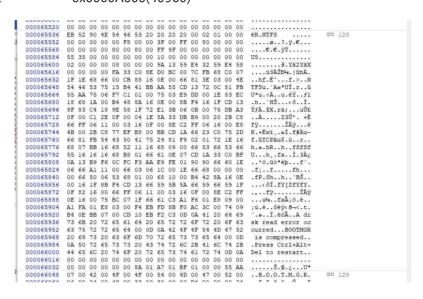
섹터 0

섹터 1

Partition 1) 00 02 03 00 07 8E 0C 02 80 00 00 00 00 A0 00 00

Partition Type :   0x07(NTFS)

Starting LBA Address: 0x00000080(128) 128섹터

Size in Sector :   0x0000A000(40960)

Partition 2) 00 8E 0D 02 07 1B 16 05 80 A0 00 00 00 A0 00 00

Partition Type :   0x07(NTFS)

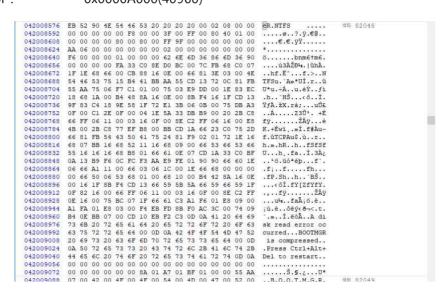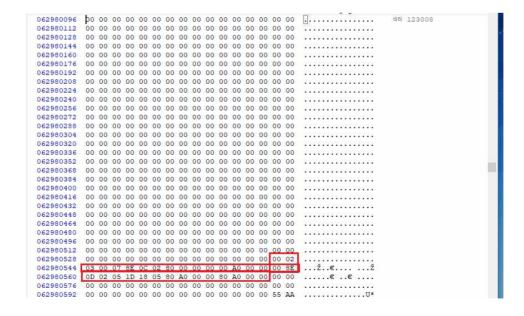Starting LBA Address: 0x0000A080(41088) 41088섹터

Size in Sector :   0x0000A000 (40960)

Partition 3) 00 1B 17 05 07 A7 20 07 80 40 01 00 00 A0 00 00

Partition Type :   0x07(NTFS)

Starting LBA Address: 0x00014080(82048) 82048섹터

Size in Sector :   0x0000A000(40960)

Extended Partition) 00 A7 21 07 05 FE 3F 0F 80 E0 01 00 00 10 02 00

Partition Type :   0x05(Microsoft Extended Partition)

Starting LBA Address: 0x0001E080(123008) 123008섹터

Size in Sector :   0x00021000(135168)

Partition 4) 00 02 03 00 07 8E 0C 02 80 00 00 00 00 A0 00 00

Partition Type :　　　　0x07(NTFS)

Starting LBA Address:　　0x00000080(128)　123008 + 128 = 123136섹터

Size in Sector :　　　　0x0000A000(40960)

Extended Partition) 00 8E 0D 02 05 1D 18 05 80 A0 00 00 80 A0 00 00

Partition Type :　　　　0x05(Microsoft Extended Partition)

Starting LBA Address:　　0x0000A080(41088) 123008 + 41088 = 164096섹터

Size in Sector :　　　　0x0000A080(41088)

Partition 5) 00 02 03 00 07 8E 0C 02 80 00 00 00 00 A0 00 00

Partition Type :　　　　　0x07(NTFS)

Starting LBA Address:　　0x00000080(128)　164096 + 128 = 164224섹터

Size in Sector :　　　　　0x0000A000(40960)

Extended Partition) 00 1D 19 05 05 2E 26 08 00 41 01 00 80 C0 00 00

Partition Type :　　　　　0x05(Microsoft Extended Partition)

Starting LBA Address:　　0x00014100(82176) 123008 + 82176 = 205184

Size in Sector :　　　　　0x0000C080(49280)

Partition 6) 00 02 03 00 07 11 0E 03 80 00 00 00 00 C0 00 00

Partition Type :   0x07(NTFS)

Starting LBA Address: 0x00000080(128) 205184 + 128 = 205312섹터

Size in Sector :   0x0000C000(49152

```
U643FFFU  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  yyyyyyyyyyyyyyyy
06440000  EB 52 90 4E 54 46 53 20 20 20 20 00 02 08 00 00  ëR.NTFS    .....
06440010  00 00 00 00 00 F8 00 00 3F 00 FF 00 80 00 00 00  .....ø..?.ÿ.€...
06440020  00 00 00 00 80 00 80 00 FF BF 00 00 00 00 00 00  ....€.€.ÿ¿......
06440030  00 08 00 00 00 00 00 00 02 00 00 00 00 00 00 00  ................
06440040  F6 00 00 00 01 00 00 00 9F AD 7F E4 D1 7F E4 1A  ö.......Ÿ..äÑ.ä.
06440050  00 00 00 00 FA 33 C0 8E D0 BC 00 7C FB 68 C0 07  ....ú3ÀŽÐ¼.|ûhÀ.
06440060  1F 1E 68 66 00 CB 88 16 0E 00 66 81 3E 03 00 4E  ..hf.Ëˆ...f.>..N
06440070  54 46 53 75 15 B4 41 BB AA 55 CD 13 72 0C 81 FB  TFSu.´A»ªUÍ.r..û
06440080  55 AA 75 06 F7 C1 01 00 75 03 E9 DD 00 1E 83 EC  Uªu.÷Á..u.éÝ..ƒì
06440090  18 68 1A 00 B4 48 8A 16 0E 00 8B F4 16 1F CD 13  .h..´HŠ...‹ô..Í.
064400A0  9F 83 C4 18 9E 58 1F 72 E1 3B 06 0B 00 75 DB A3  ŸƒÄ.žX.rá;...uÛ£
064400B0  0F 00 C1 2E 0F 00 04 1E 5A 33 DB B9 00 20 2B C8  ..Á.....Z3Û¹. +È
064400C0  66 FF 06 11 00 03 16 0F 00 8E C2 FF 06 16 00 E8  fÿ.......ŽÂÿ...è
064400D0  4B 00 2B C8 77 EF B8 00 BB CD 1A 66 23 C0 75 2D  K.+Èwï¸.»Í.f#Àu-
064400E0  66 81 FB 54 43 50 41 75 24 81 F9 02 01 72 1E 16  f.ûTCPAu$.ù..r..
064400F0  68 07 BB 16 68 52 11 16 68 09 00 66 53 66 53 66  h.».hR..h..fSfSf
06440100  55 16 16 16 68 B8 01 66 61 0E 07 CD 1A 33 C0 BF  U...h¸.fa..Í.3À¿
06440110  0A 13 B9 F6 0C FC F3 AA E9 FE 01 90 90 66 60 1E  ..¹ö.üó©éþ...f`.
06440120  06 66 A1 11 00 66 03 06 1C 00 1E 66 68 00 00 00  .f¡..f.....fh...
06440130  00 66 50 06 53 68 01 00 68 10 00 B4 42 8A 16 0E  .fP.Sh..h..´BŠ..
06440140  00 16 1F 8B F4 CD 13 66 59 5B 5A 66 59 66 59 1F  ...‹ôÍ.fY[ZfYfY.
06440150  0F 82 16 00 66 FF 06 11 00 03 16 0F 00 8E C2 FF  .‚..fÿ.......ŽÂÿ
06440160  0E 16 00 75 BC 07 1F 66 61 C3 A1 F6 01 E8 09 00  ...u¼..faÃ¡ö.è..
06440170  A1 FA 01 E8 03 00 F4 EB FD 8B F0 AC 3C 00 74 09  ¡ú.è..ôëý‹ð¬<.t.
06440180  B4 0E BB 07 00 CD 10 EB F2 C3 0D 0A 41 20 64 69  ´.»...Í.ëòÃ..A di
06440190  73 6B 20 72 65 61 64 20 65 72 72 6F 72 20 6F 63  sk read error oc
064401A0  63 75 72 72 65 64 00 0D 0A 42 4F 4F 54 4D 47 52  curred...BOOTMGR
064401B0  20 69 73 20 63 6F 6D 70 72 65 73 73 65 64 00 0D   is compressed..
064401C0  0A 50 72 65 73 73 20 43 74 72 6C 2B 41 6C 74 2B  .Press Ctrl+Alt+
064401D0  44 65 6C 20 74 6F 20 72 65 73 74 61 72 74 0D 0A  Del to restart..
064401E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
064401F0  00 00 00 00 00 00 8A 01 A7 01 BF 01 00 00 55 AA  ......Š.§.¿...Uª
06440200  07 00 42 00 4F 00 4F 00 54 00 4D 00 47 00 52 00  ..B.O.O.T.M.G.R.
```

섹터 205312

섹터 205313

)