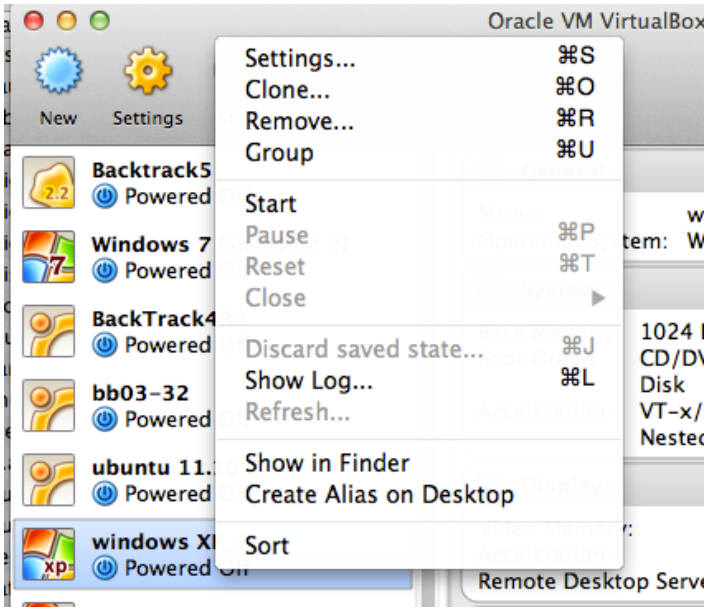
# Project 2: Melihat Segment dan Cluster menggunakan Hex Editor

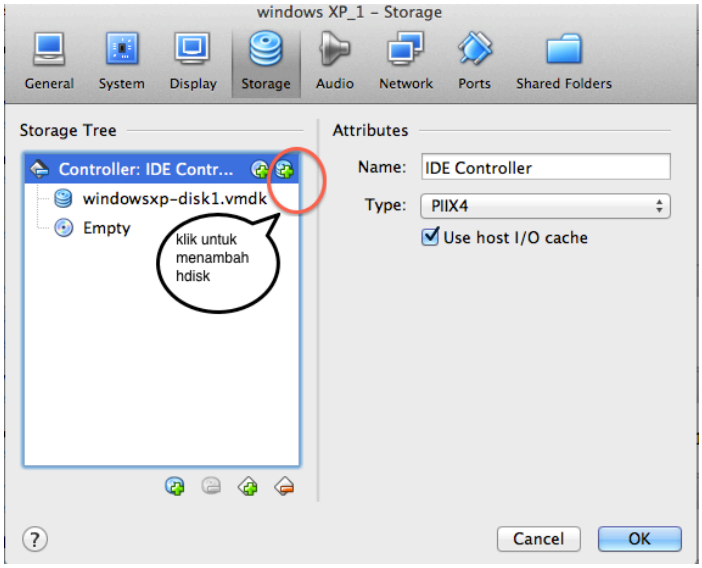
## Kebutuhan Project

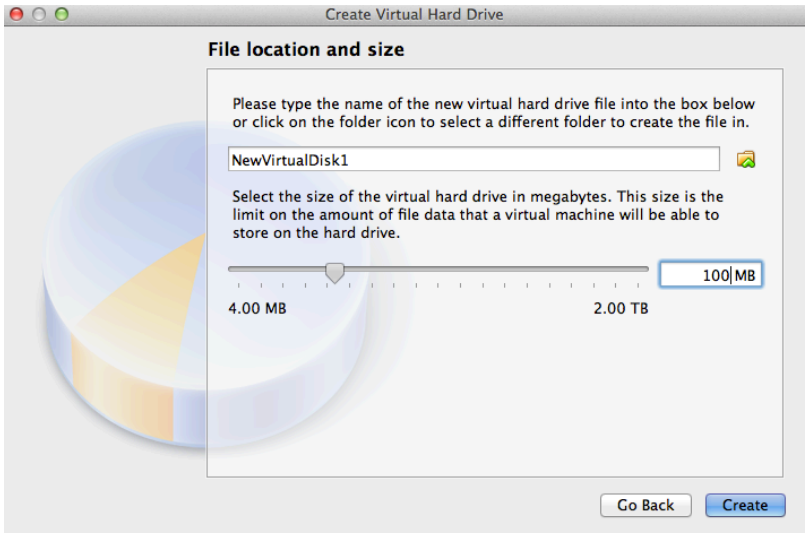
- Komputer virtual. Bisa menggunakan sembarang OS, dan bisa menggunakan software virtual apa saja seperti VirtualBox, Vmware, dll. Instruksi berikut mengasumsikan host yang diguanakan Backtrack 5 r3, VirtualBox, dan Guest OS menggunakan WinXPSP3, seperti yang disetup di lab Foresec.




## Menambahkan Small Hard Disk ke Komputer Virtual

1. Jalankan Virtualbox. Klik kanan pada icon Windows XP-SP3 dalam keadaan: "Powered Off", seperti terlihat di sebelah kanan.
2. Click "**Settings**". Pada kotak "Virtual Machine Settings", click icon **Storage...**. Kemudian klik icon hardisk di pojok kanan untuk menambah hardisk sperti di gambar.
3. Kemudian akan muncul pesan untuk menambah disk. Pilih Tab **"Create new disk".** Pilih **"VDI (VirtualBox Disk Image".** Kemudian klik Tombol "**Continue"** di pojok kiri bawah.
4. Selanjutnya pilih **"Dynamically allocated"**. Kemudian klik Tombol "**Continue"** di pojok kiri bawah.
5. Pada jendela **File location and size**, pada bagian ukuran hardisk, geser/isikan menjadi **100 MB,** seperti gambar di bawah.






6. Klik tombol **Create.** Maka akan kembali ke jendela setingan Windows-XP-SP3. Klik tombol OK di pojok kanan bawah. Maka jendela akan kembali ke jendela VirtualBox.

# Menjalankan Virtual Machine

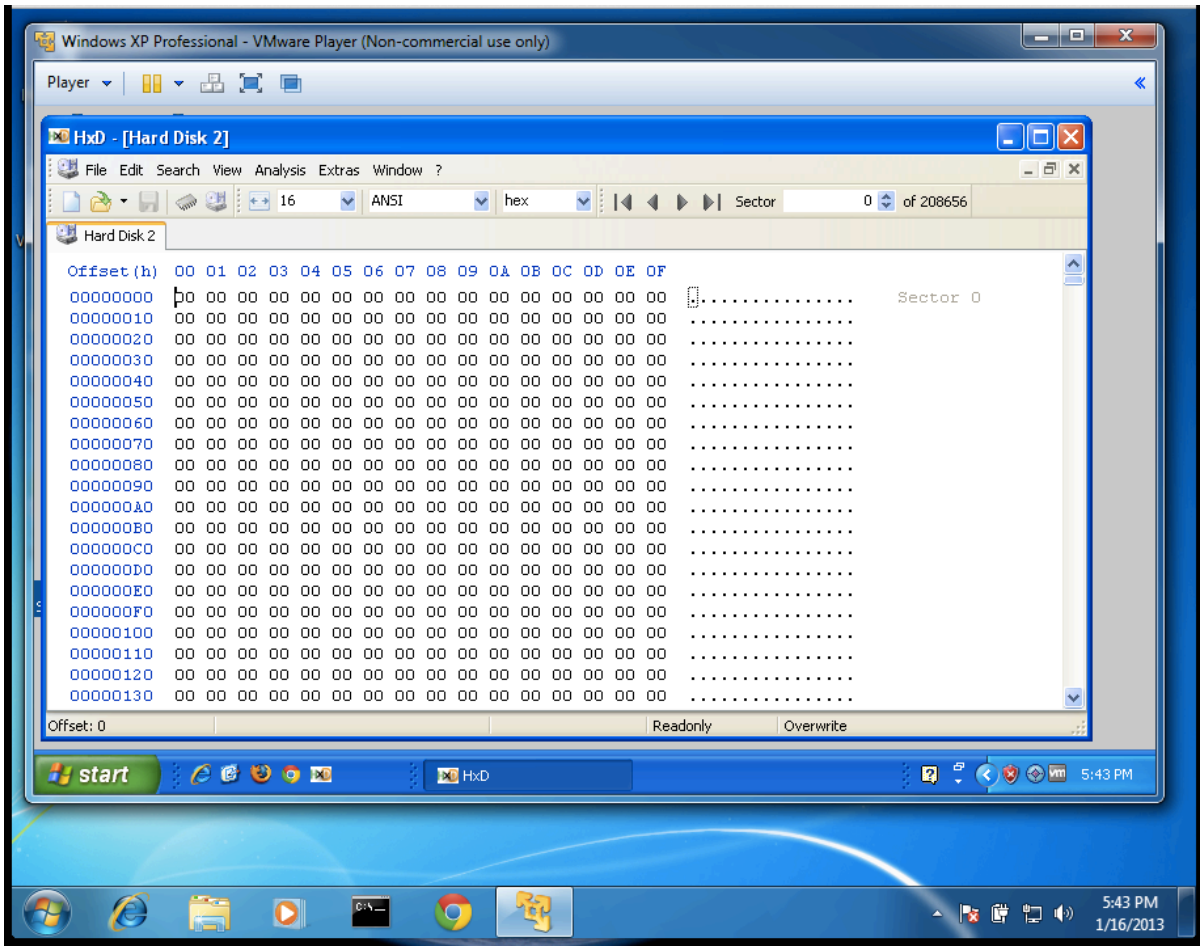
7. Di jendela VirtualBox double click icon Windows-XP-SP3, maka Windows XP akan segera berjalan.

# Download dan Install HxD

8. Pada komputer virtual WindowsXP-SP3, jalankan Web browser dan buka http://mh-nexus.de/en/hxd, atau bisa juga didownload melalui elearning.
9. Scroll down dan click link "**Download page**". Download dan install HxD versi bahasa Inggris. Biarkan saja dalam kondisi default options.

# Memeriksa Disk yang baru dibuat

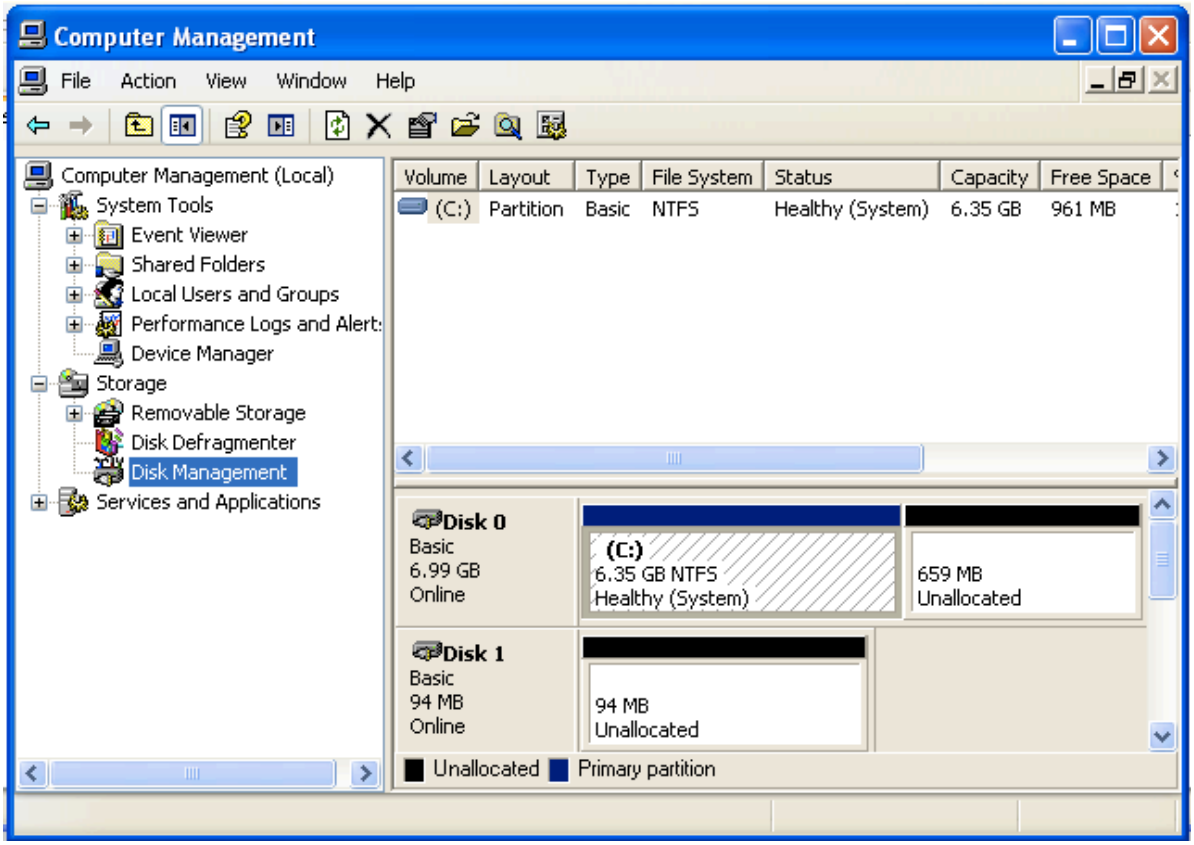
10. Pada komputer virtual, jika HxD tidak terbuka, click **Start**, "**All Programs**", "**HxD Hex Editor**", **HxD**.
11. Pada jendela HxD, click **Extras**, "**Open disk...**".
12. Pada kotak "Open disk", di bagian "Physical disks", click "**Hard Disk 2**", seperti terlihat di bawah. Click **OK**.




8. HxD memperlihatkan isi disk, seperti terlihat di bagian atas. Cari bagian berikut:
   - Tiap baris horizontal row terdiri dari 16 bytes, yang dilabeli dengan nilai Offset (h) value dalam bentuk hexadecimal di bagian atas.
   - Di sisi kiri, nilai terlihat dalam bentuk hexadecimal. Di sisi kanan, memperilihatkan nilai ASCII.
   - Karena hardisk yang digandeng merupakan hard disk baru, setiap byte masih kosong. Tidak ada informasi apapun di harddisk.
   - Disi kanan atas, perhatikan tampilan "Sector 0 of 208656". Tiap sector terdiri dari 512 bytes, sehingga jumlah total 208,656 x 512 bytes = 106,831,872 bytes. Hampir mendekati 00 million bytes, atau 0.1 GB.

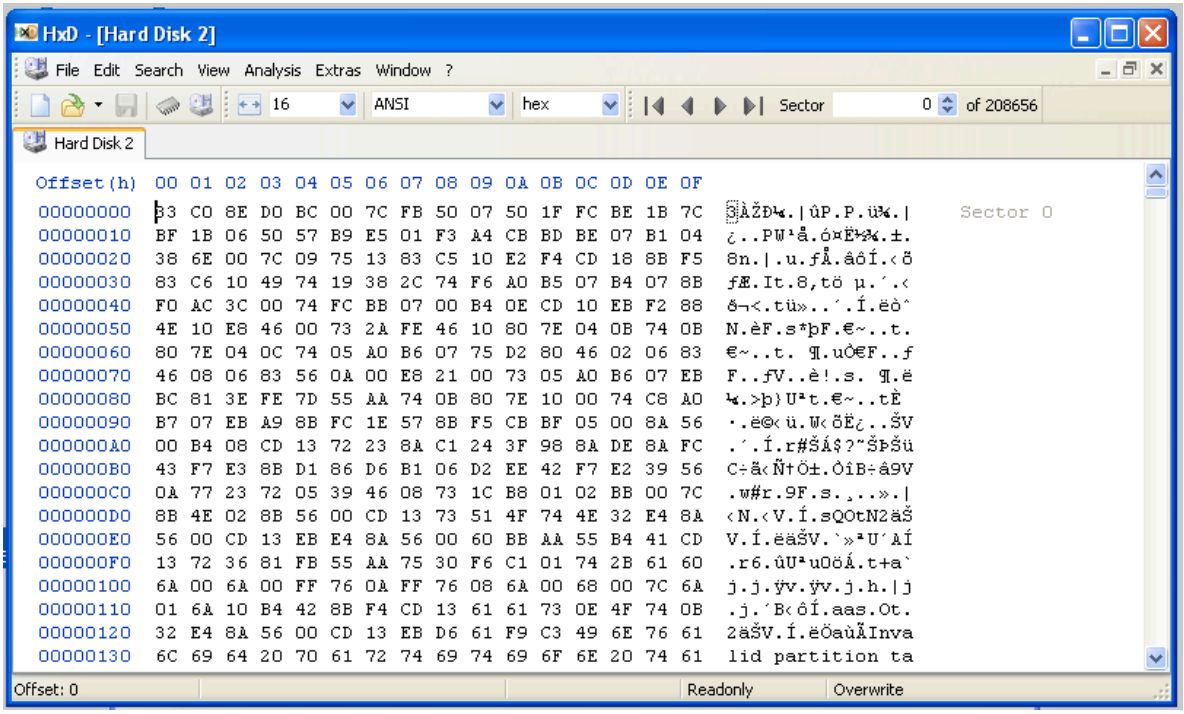
# Menginisiasi Disk

13. Pada jendela Windows virtual machine, click **Start**. Arahkan ke "**My Computer**" dan klik-kanan. Click **Manage**. Di bagian kiri "Computer Management", click "**Disk Management**". Muncul popup “itialize and Convert Disk Wizard" pops up. Click **Next**, **Next**, **Next**, dan **Finish**. Proses ini menulis Master Boot Record ke disk.
14. Maka selanjutnya  disk akan Nampak di Disk Management sebagai "Disk 1", berisi kurang lebih 100 MB alokasi space, seperti berikut.

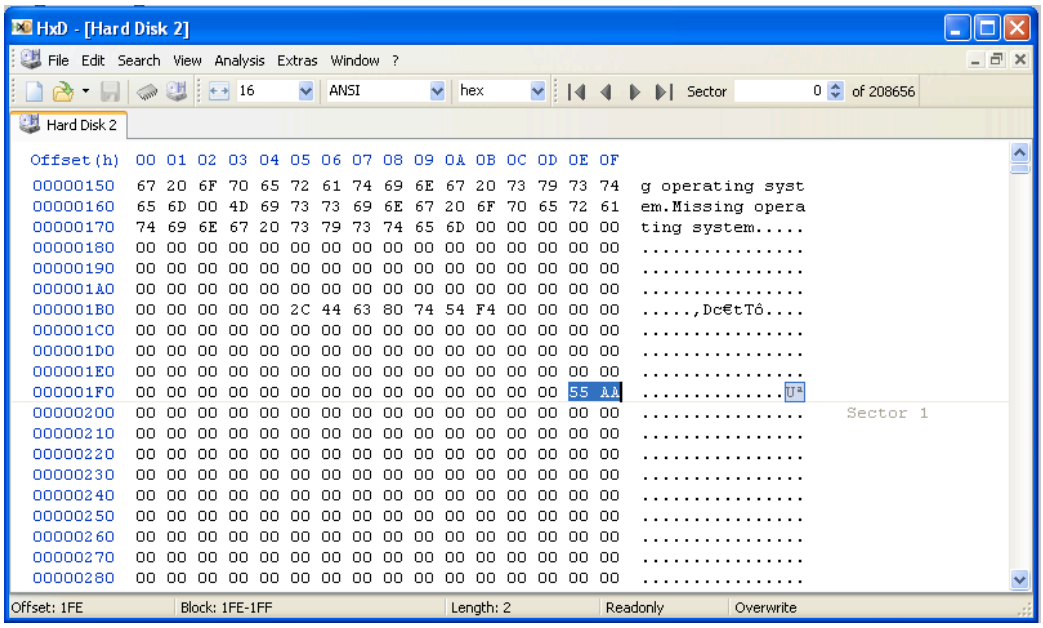



# Melihat Master Boot Record (MBR)

15. Pada HxD, click **View**, **Refresh**. Maka nilai Nonzero akan terlihat di sik, seperti berikut.



16. Scroll down hingga ke akhir sector pertama, lokasi 1FE dan 1FF, mak akan terlihat dua bytes terakhir adalah 55 dan AA, seperti di bawah ini. Bytes ke -200 dan seterusnya masih berisi nol.




Bagan berikut ini memperlihatkan fitur MBR (dari Wikipedia (http://en.wikipedia.org/wiki/Master_boot_record)).

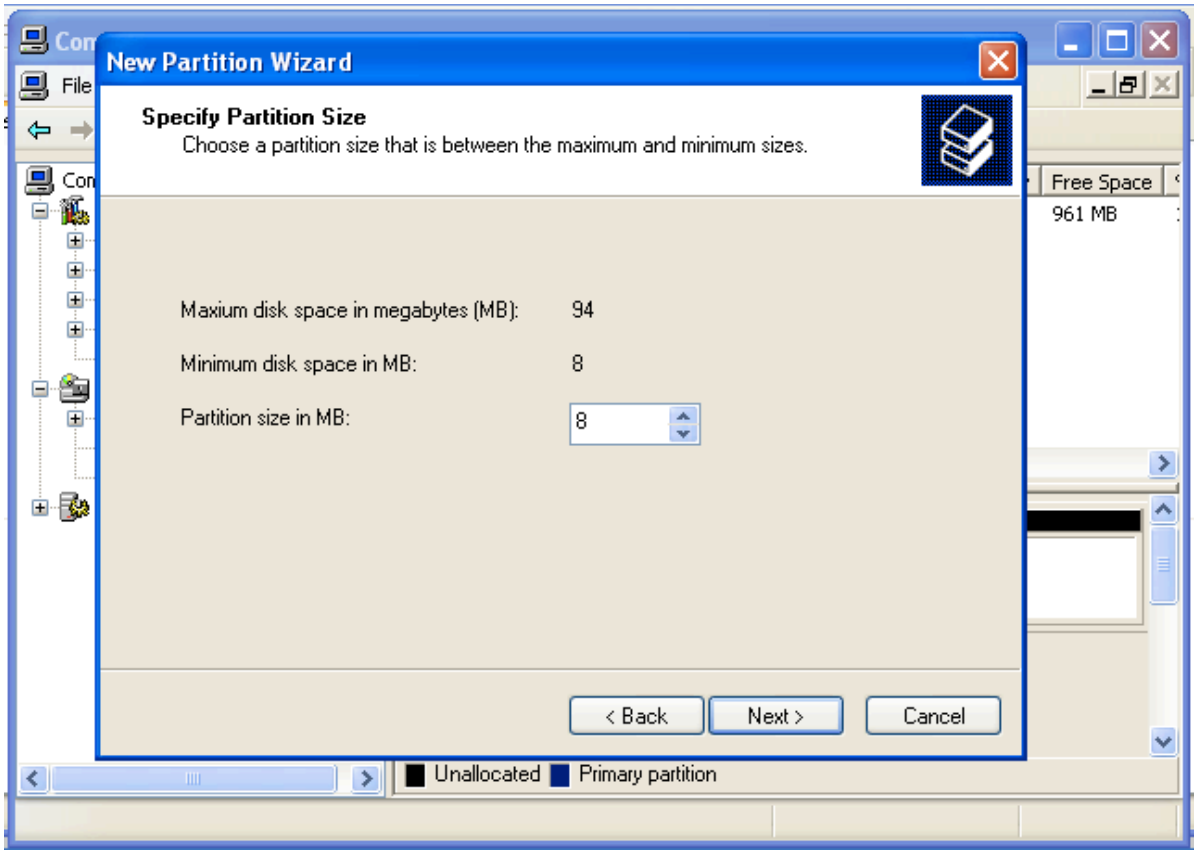
**Structure of a classical generic MBR**

| Address | | Description | | Size in bytes |
|---|---|---|---|---|
| Hex | Dec | | | |
| +000h | +0 | Bootstrap code area | | 446 |
| +1BEh | +446 | Partition entry #1 | *Partition table* (for primary partitions) | 16 |
| +1CEh | +462 | Partition entry #2 | | 16 |
| +1DEh | +478 | Partition entry #3 | | 16 |
| +1EEh | +494 | Partition entry #4 | | 16 |
| +1FEh | +510 | 55h | *Boot signature*[nb 1] | 2 |
| +1FFh | +511 | AAh | | |
| | | | **Total size: 446 + 4*16 + 2** | **512** |

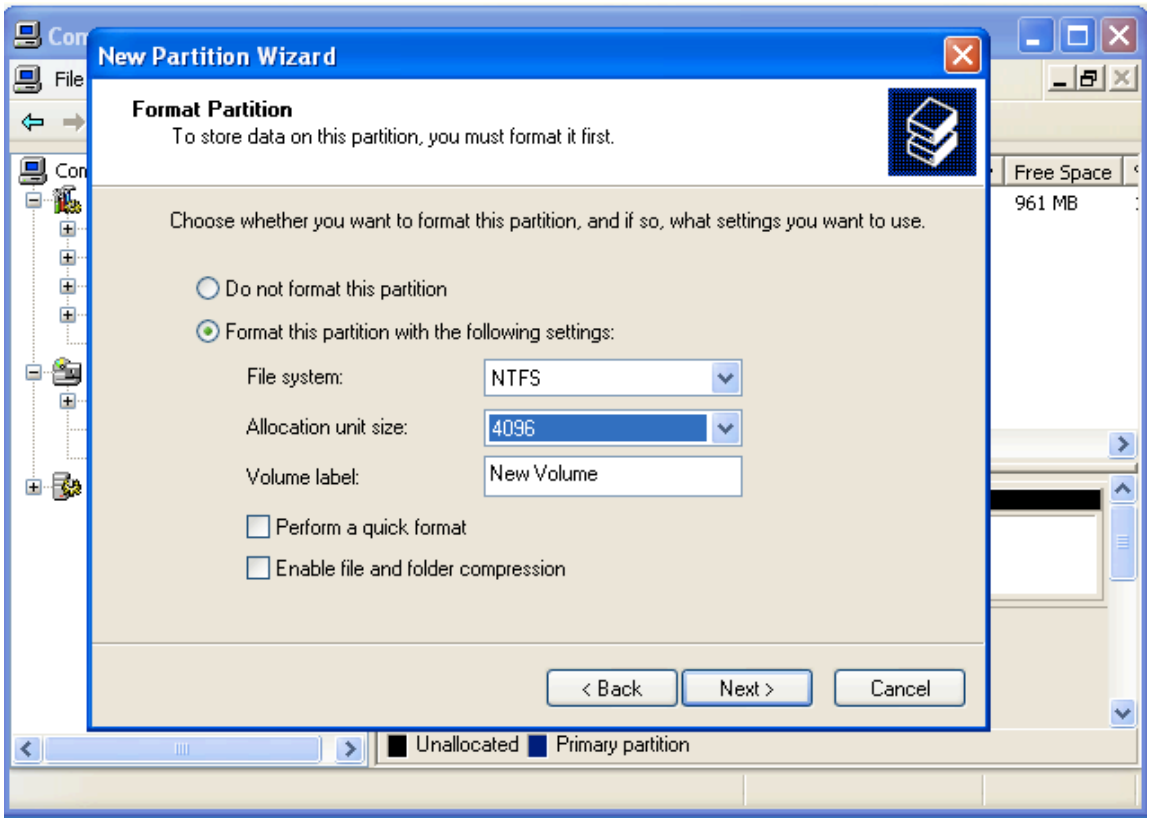
17. Cari fitur-fiturnya di jendela HxD:
    - **Start of Partition Table**: Lokasinya 01BC dan 01BD berisi nol
    - **Partition Table**: Lokasi 01BE hingga 01FD berisi 64 bytes nol. Terdapat empat records 16-byte, yang merupakan empat kemungkinan partisi pada Basic Disk. Karena tidak ada partisi pada disk, nilainya masih nol.
    - **End of Boot Sector**: Lokasi 01FE dan 01FF berisi 55 dan AA. Merupakan MBR Signature—yang merupakan akhir MBR, dan juga akhir Partition Table.

# Mempartisi Disk

18. Pada virtual machine, di "Disk Management", klik kanan area "**94 MB Unallocated**" Disk 1 dan click "**New Partition**".
19. Pada menu "Welcome to the New Partition Wizard", click **Next**.
20. Pada kotak "Select Partition Type", pilih default selection dari "Primary partition" dan click **Next**.
21. Pada kotak "Specify Partition Size", masukkan ukuran Partisi **8** seperti terlihat di bawah, dan click **Next**.

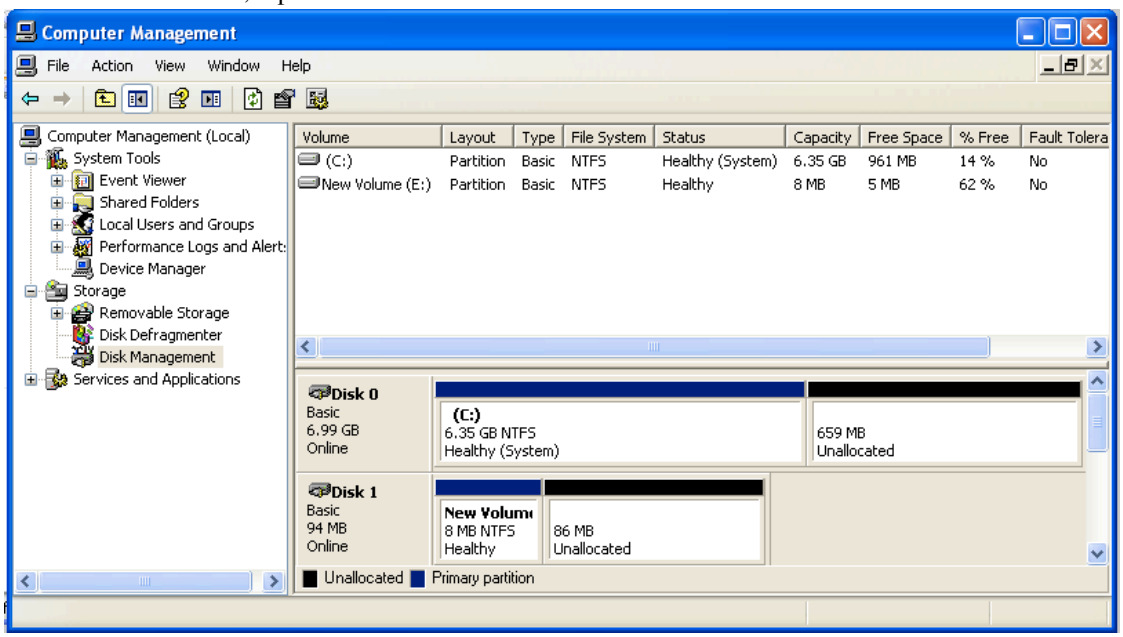



22. Pada kotak "Assign Drive Letter or Path", biarkan default selection E dan click **Next**.
23. Pada kotak "Format Partition", rubah "Allocation unit size" menjadi **4096**, seperti terlihat di bawah, dan click **Next**.



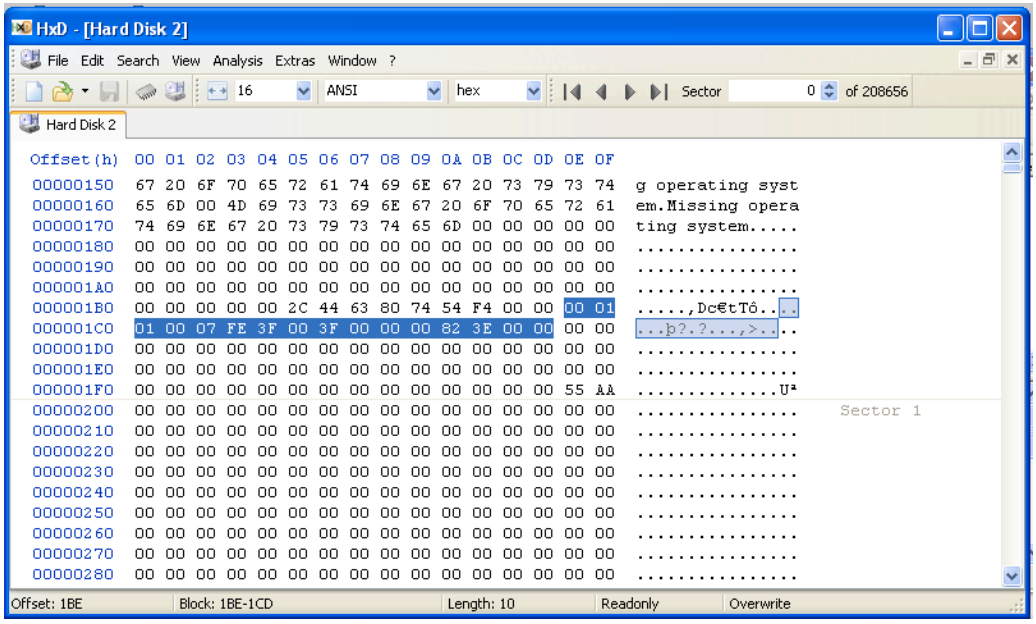

24. Pada kotak "Completing the New Partition Wizard", click **Finish**.

25. Setelah beberapa detik, Disk Manager akan terlihat ada New Volume (E:) partisi baru dengan ukuran 8 MB, seperti terlihat di bawah.



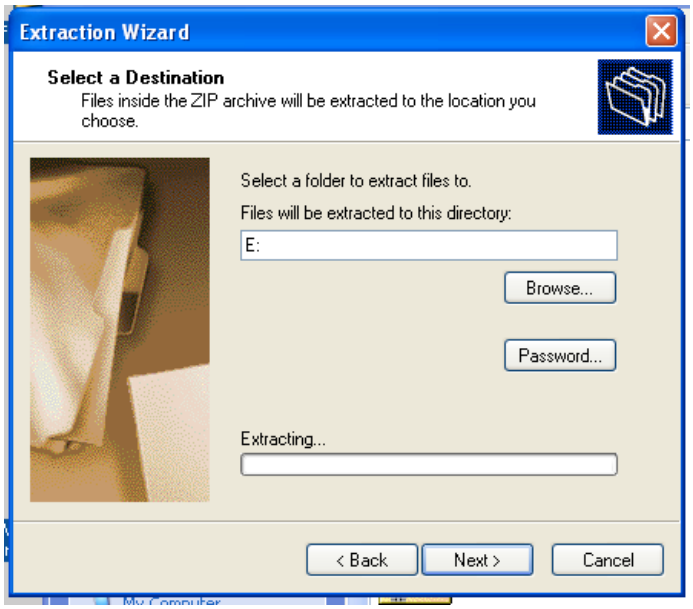
# Melihat Partition Table

26. Di HxD, click **View**, **Refresh**.
    Perhatikan pada record pertama dari partition table (dari hex 01BE hingga 01CD) sekarang berisi data, seperti yang di- highlighted di gambar di bawah ini.

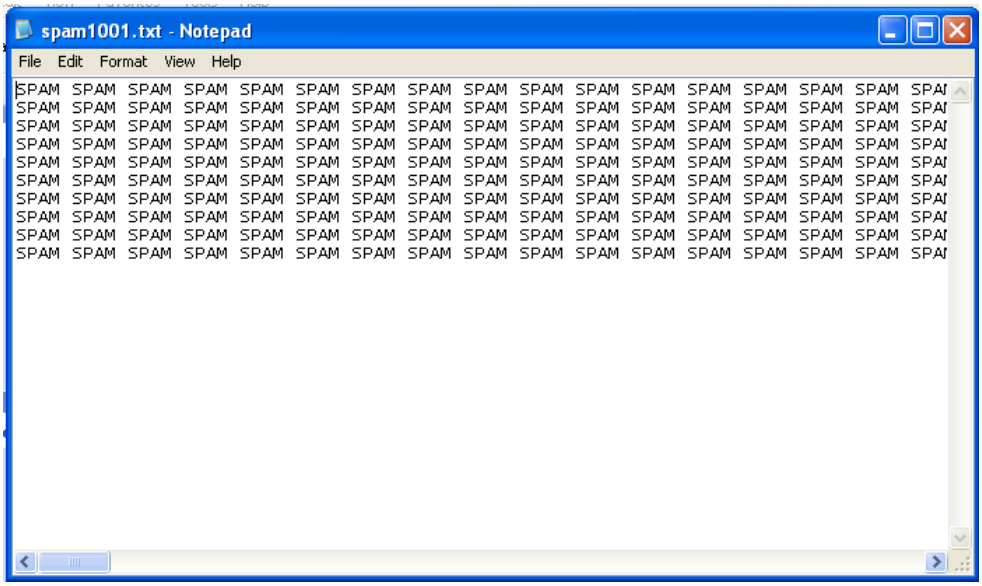



# Mengisi Partisi E: dengan Spam

27. Di komputer virtual, simpan **SPAM.zip** dari link di elearning.
28. Simpan file ke desktop.
29. Click link **EGGS.zip** di elearning dan simpan juga di desktop.
30. Di desktop, klik kanan file **SPAM.zip** dan click "**Extract All...**".
31. Pada kotak "Welcome to the Compressed (zipped) Folders Extraction Wizard", click **Next**.
32. Pada kotak "Select a Destination", masukkan direktori **E:**, seperti terlihat di bawah. Click **Next**.

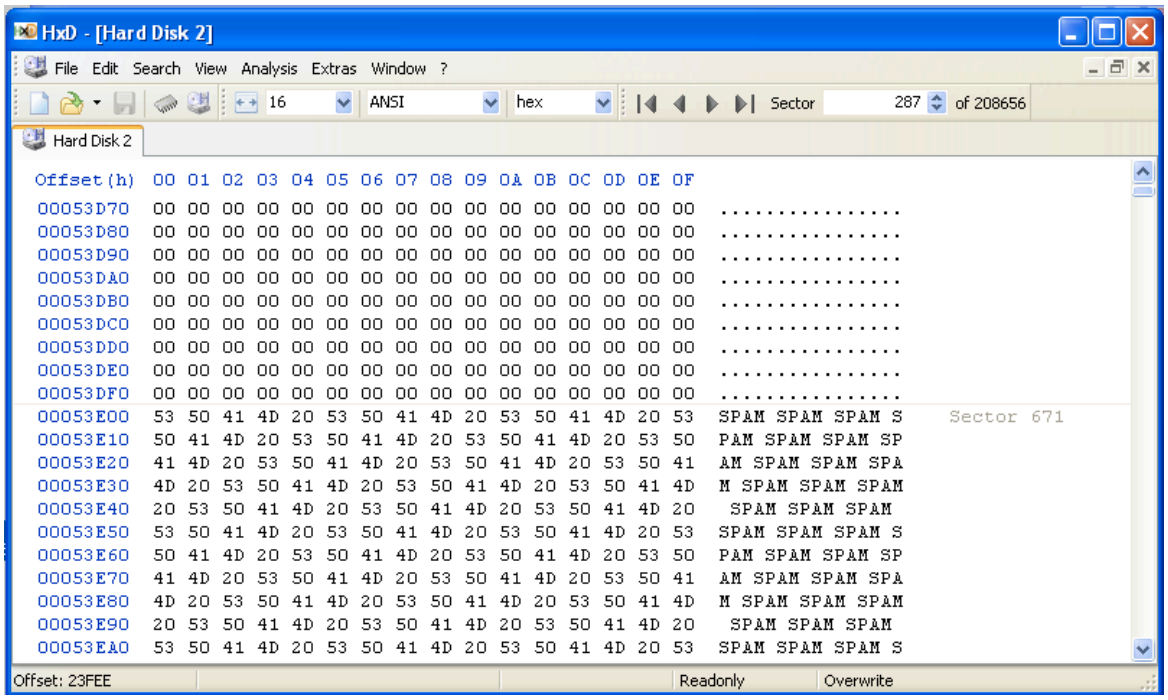


33. Setelah beberapa saat, akan muncul pop up pesan error, yang berisi "There is not enough space on the disk to extract the file". Click **OK**.
34. Pada kotak "Extraction Wizard", click **Cancel**.
35. Dari desktop komputer, click **Start**, "**My Computer**".
36. Double-click "**New Volume (E:)**".
37. Double-click folder **SPAM** untuk membukanya.
38. Akan terlihat banyak file yang bernama spam1001.txt, spam1002.txt, dst.
39. Double-click **spam1001.txt**.
    Seperti terlihat, file berisi tulisan SPAM berulang kali, seperti terlihat di bawah ini. Tiap file "spam" terdiri dari 10,000 characters.

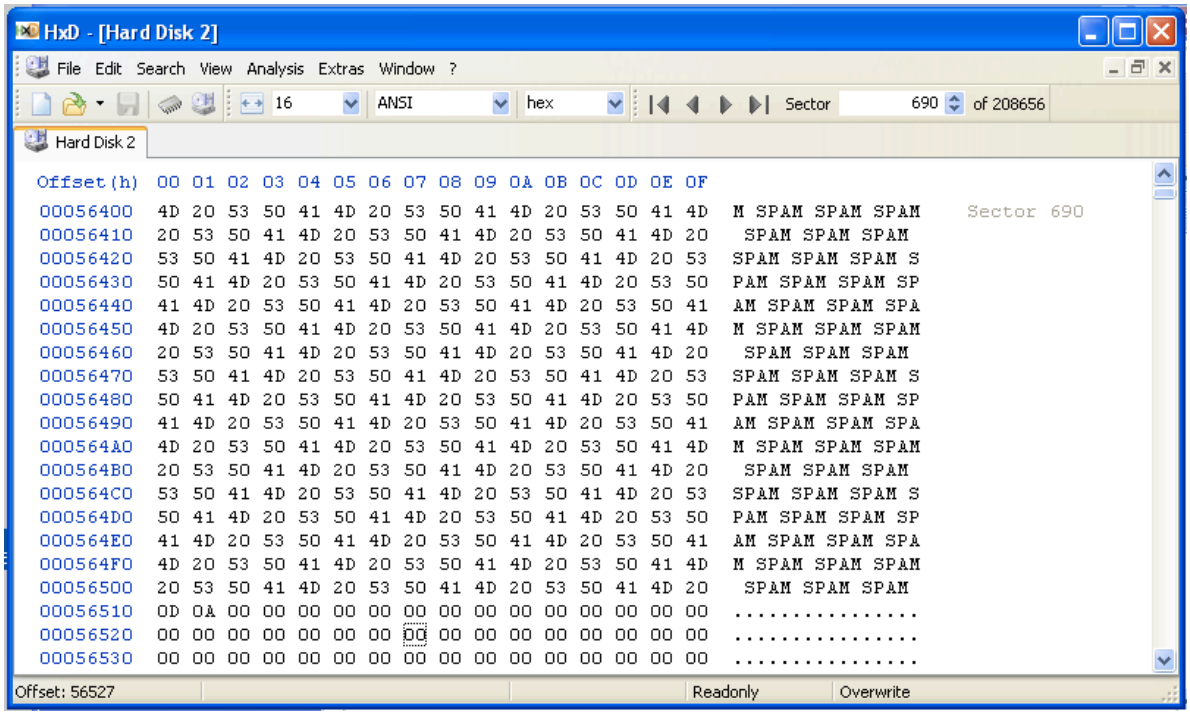



# Melihat Data SPAM yang Tersimpan

40. Di HxD, click **View**, **Refresh**.
41. Scroll down mouse sampai terlihat SPAM.
42. Scroll back dengan hati-hati untuk melihat awal block SPAM. Lokasi nya bisa saja berbeda. Seperti pada saat dijalankan, spam dimulai pada sector 671, seperti terlihat di bawah ini.




43. Tap key **PageDown** di keyboard sampai ketemu akhir text SPAM di file. Sebagai contoh yang dijalankan di sini, text berakhir di sector 714, seperti terlihat di bawah ini.




Format partisi dengan 4096-byte clusters, masing-masing terdiri dari 8 sector 512-byte. File spam berisi 10,000 karakter masing-masingnya, sehingga terdiri dari tiga clusters, seperti terlihat di bawah. Lihat clusters tersebut dan pastikan berisi data tersebut. Nomor Sector bisa saja berbeda, tapi pasti akan terlihat pola data pada 24 sectors yang berurutan.

```
CLUSTER 1   CLUSTER 2   CLUSTER 3
--- ----    --- ----    --- ----
671 SPAM    679 SPAM    687 SPAM
672 SPAM    680 SPAM    688 SPAM
673 SPAM    681 SPAM    689 SPAM
674 SPAM    682 SPAM    690 SPAM + 0
675 SPAM    683 SPAM    691 0
676 SPAM    684 SPAM    692 0
677 SPAM    685 SPAM    693 0
678 SPAM    686 SPAM    694 0
```

# Delete Files pada Drive E:

44. Di komputer Windows, click **Start**, "**My Computer**".
45. Double-click "**New Volume (E:)**".
46. Klik kanan folder **SPAM** dan click **Delete**.
47. Pada kotak "Confirm Folder Delete", click **Yes**.
48. Pop up "Confirm Folder Delete", yang memastikan filestersebut akan "permanently deleted". Click **Yes**.

# Melihat Data SPAM

49. Di HxD, click **View**, **Refresh**.
50. Scroll sampai ke 24 sectors yang sudah diperiksa sebelumnya, dan periksa semua text SPAM masih ada. Mendelete file tidak berarti menghapus data text.
51. Mendelete file hanya merubah records di Master File Table.

# Format Drive E:

52. Di komputer Windows, click **Start**, "**My Computer**".
53. Klik kanan "**New Volume (E:)**" dan click **Format...**.
54. Pada kotak "Format New Volume (E:)", pastikan kotak "Quick Format" tidak dicentang, dan kotak "Enable Compression" tidak dicentang.. Click **Start**. Pesan "Format New Volume (E:)" akan nampak "WARNING: Formatting will erase ALL data on this disk". Click **OK**.
55. Ketika pesan "Format Complete" muncul, click **OK**.

# Melihat Data SPAM

56. Pada HxD, click **View**, **Refresh**.
57. Scroll melewati 24 sectors yang sudah diperiksa sebelumnya, dan pastikan pesan SPAM text masih ada. Memformat disk juga tidak menghapus datanya.

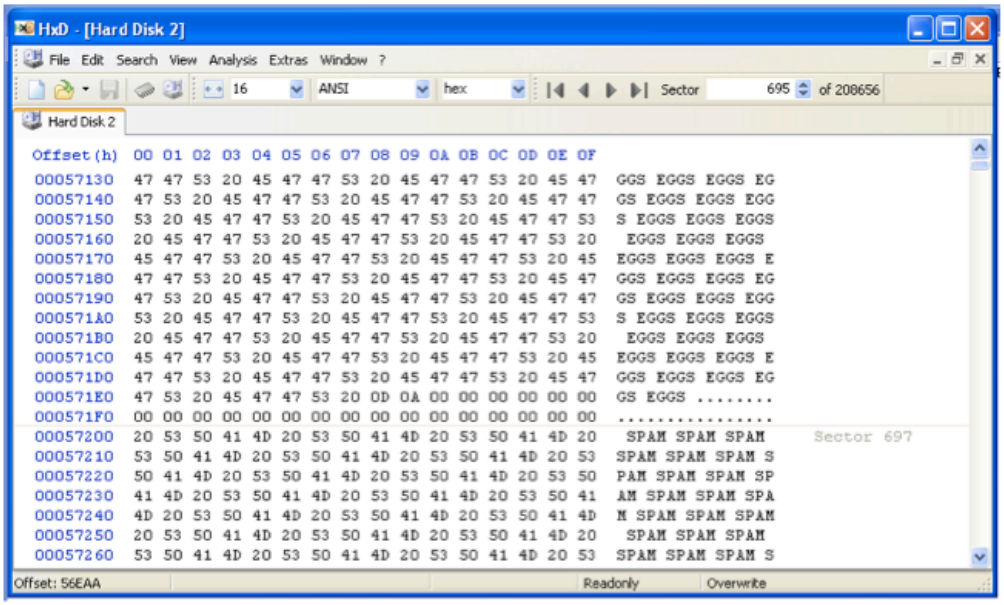
# Menambahkan File "EGGS" ke Partisi E:

58. Pada desktop, klik kanan file **EGGS.zip** dan click "**Extract All**".
59. Pada kotak "Welcome to the Compressed (zipped) Folders Extraction Wizard", click **Next**.

60. Pada kotak "Select a Destination", masukkan direktori **E:**. Click **Next**.
61. Ketika proses extraksi selesai, click **Finish**.
62. Jendela "New Volume (E:)" terbuka.
63. Double-click folder **EGGS** untuk membukanya.
64. Akan terlihat banyak file bertulisan "Copy (2) of eggs1001.txt", dll. Double-click satu dari file untuk membukanya.
65. Seperti yang terlihat, file yang berisi tulisan EGGS berulang kali, seperti terlihat di bawah. Terdapat total 1000 karakter di tiap file "eggs", lebih kecil dibandingakan file "spam".

# Melihat Data EGGS

66. Di HxD, click **View**, **Refresh**.
67. Scroll melewati 24 sectors yang sudah diperiksa sebelumnya, dan cari data EGGS. Jika perlu, scroll mouse, atau "Search" item menu, untuk mencari teks EGGS. Cari tempat dimana data EGGS berakhir, seperti terlihat berikut ini.




# Refleksi

Gambar ini memperlihatkan tiga hal penting:

- **Active data**: teks EGGS merupakan bagian file yang diacu di Master File Table
- **RAM Slack**: 22 Zeroes dia khir data EGGS berisikan nol ketika ditulis oleh modern operating systems. Pada Windows versions Win 95 Version B, area ini berisi data dari RAM, yang bisa saja berisi passwords atau informasi penting lainnya.
- **File Slack**: teks SPAM di ujung file "eggs" merupakan data lama, yang tertinggal pada active clusters

# Simpan Screen Image

68. Pastikan di layar terlihat tiga item penting: teks EGGS text, nol, dan teks SPAM. Tekan tombol printscreen untuk mengkopi seluruh data di layar. **GAMBAR YANG DI SUBMIT HARUS**

**GAMBAR FULL-SCREEN UNTUK MENDAPATKAN POIN SEMPURNA!** . Simpan dengan nama "**NamaKamu_Proj2a**".

# Observasi Sectors

Scroll sectors, dan pastikan pola di table bawah ini terlihat. Sektor yang saudara miliki mungkin berbeda, akan tetapi terdapat tiga sector berurutan yang isinya seperti ini.

| Sector | Contents | Technical Term |
|---|---|---|
| 695 | EGGS | Active data |
| 696 | EGGS + 0 | Active data + RAM Slack |
| 697 | SPAM | File Slack |

Pastikan untuk memahami istilah jenis data tersebut.

# Menghapus Disk

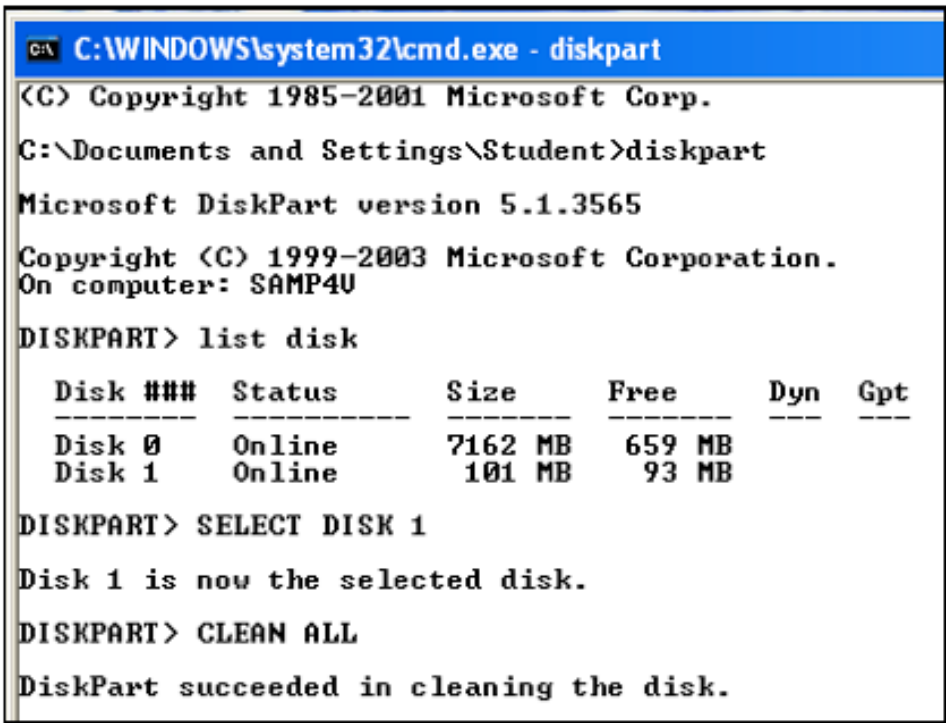
68. Sekarang kita menggunakan tool yang bisa benar-benar menghapus disk: DISKPART.
69. Di komputer Windows XP, tutup semua jendela, kecuali jendela HxD.
70. Click **Start**, **Run**.
71. Pada kotak Run, ketikkan **CMD** dan tekan tombol Enter.
72. Pada Command Prompt window, masukan perintah berikut diakhiri dengan Enter key:

    **DISKPART**

    Pada jendela Command Prompt window, masukan perintah berikut diakhiri dengan Enter key: key:

    **LIST DISK**

    Akan terlihat dua disks, sperti terlihat di gambar bawah. Disk 0 berupa disk system yang berisi Windows XP. Disk 1 disk 100 MB yang akan kita hapus.




73. Pada jendela Command Prompt window, kettikan perintah berikut diikuti dengan Enter key:
    **`SELECT DISK 1`**
    Pastikan pesan "Disk 1 is now the selected disk." HATI-HATI saat menggunakan tool ini – jika salah memilih disk maka GAME OVER. Pada jendela Command Prompt, masukkan perintah berikut diakhiri dengan Enter:
    **`CLEAN ALL`**

# Melihat Disk Kosong

74. Di HxD, click **View**, **Refresh**.
75. Semua teks SPAM dan EGGS habis.
76. Gulung ke atas dan periksa seluruh disk kosong—bahkan MBR juga hilang.

# Mengumpulkan Project

Kirim melalui elearning.

Last Modified: 11-3-2013