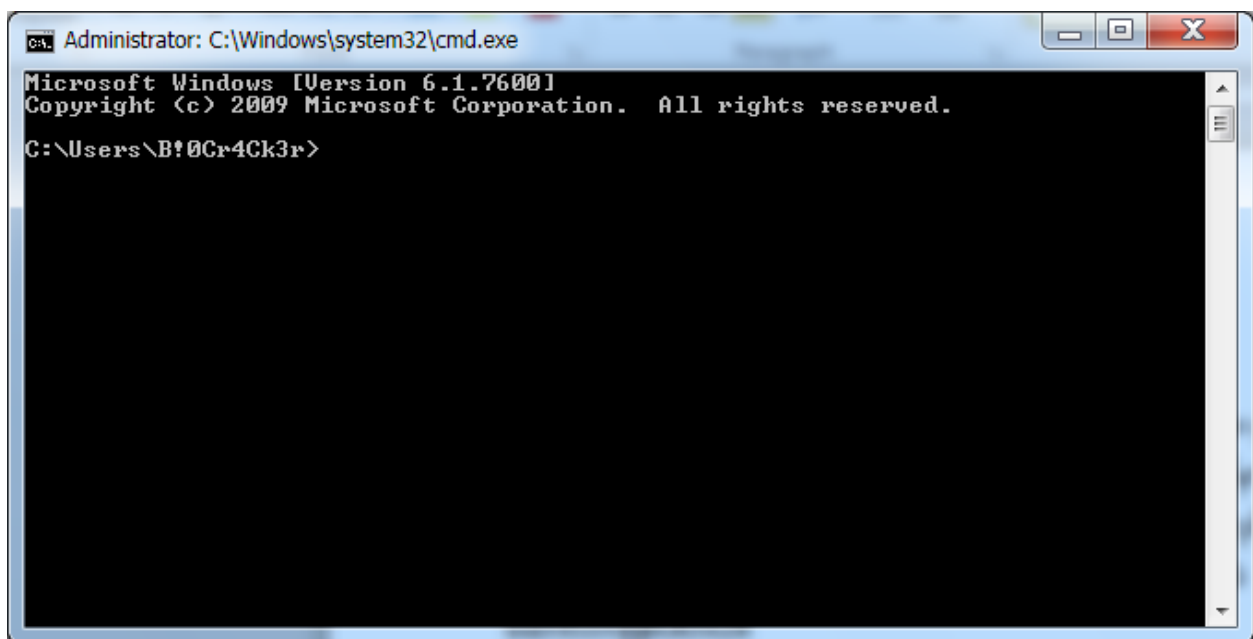


Windows7 ပေါ်မှ DOS Command များအကြောင်း တစ်စုံတစ်ရာစာတမ်း

DOS Command ဆိုတာကတော့ ကျွန်တော်တို့ Microsoft Window မှာ Services ပိုင်းတွေအတွက် အဓိက အသုံးများကြပါတယ်။ သူကတော့ ကျွန်တော်တို့ လက်ရှိ ဝင်းဒိုးပေါ်မှာ GUI (Graphical User Interface) Mode မှာမဟုတ်ဘဲ CLI (Command Line Interface) Mode ထဲမှာ လုပ်ဆောင်ရတာဖြစ်ပါတယ်။ Command Prompt ဆိုတာတော့ကြားဖူးကြမှာပါ။ ဟုတ်ပါတယ် အဲဒီနောက်ခံ အမဲရောင်နဲ့ အောက်ကပုံအတိုင်းလုပ် ဆောင်တာဖြစ်ပါတယ်။



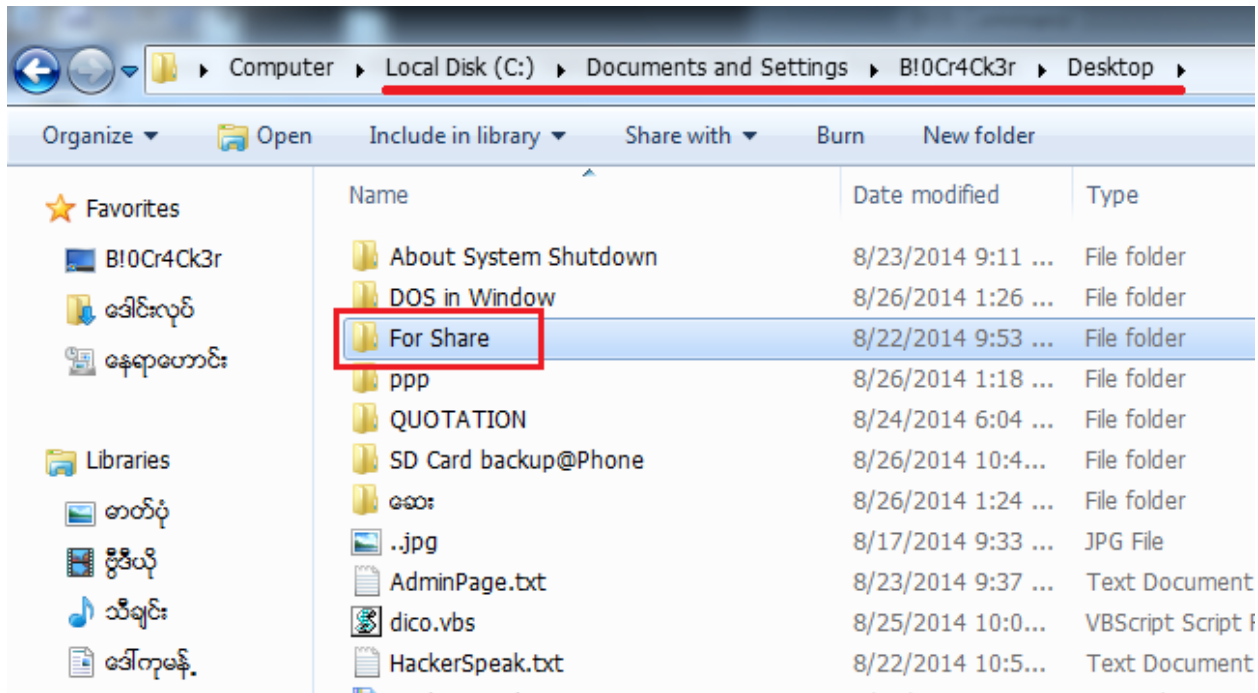
ကဲ ..လိုတိုရှင်းနဲ့ ထိထိရောက်ရောက်ပဲရှင်းပြပါမယ်ဗျာ

" cd "

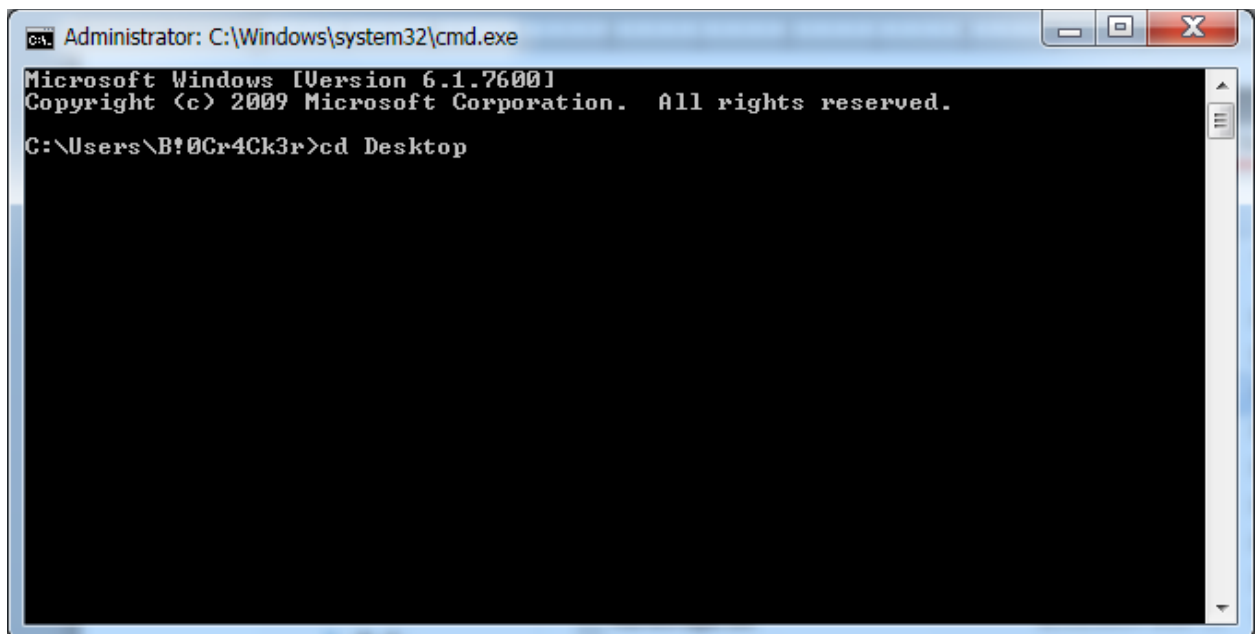
Cd ဆိုတဲ့ Command ကတော့ ကျွန်တော်တို့ Directory တွေထဲဝင်မယ်၊ ထွက်မယ်ဆိုတဲ့အခါမှာသုံးတာဖြစ်ပါတယ်။ Directory ဆိုတာကလည်း ကျွန်တော်တို့ Folder တွေကိုခေါ်ဆိုခြင်းဖြစ်ပါတယ်။ နောက်တစ်ချက်က မိမိက ဝင်ချင်တဲ့ ဖိုင်တွေရဲ့ Location ကိုလည်း သိရမှာဖြစ်ပါတယ်။ ဆိုလိုတာကတော့ ပတ်လမ်းပေါ့....ဥပမာ အားဖြင့် Desktop ပေါ်က ဖိုင်တစ်ခုထဲဝင်ချင်ဆယ်ဆိုပါစို့...



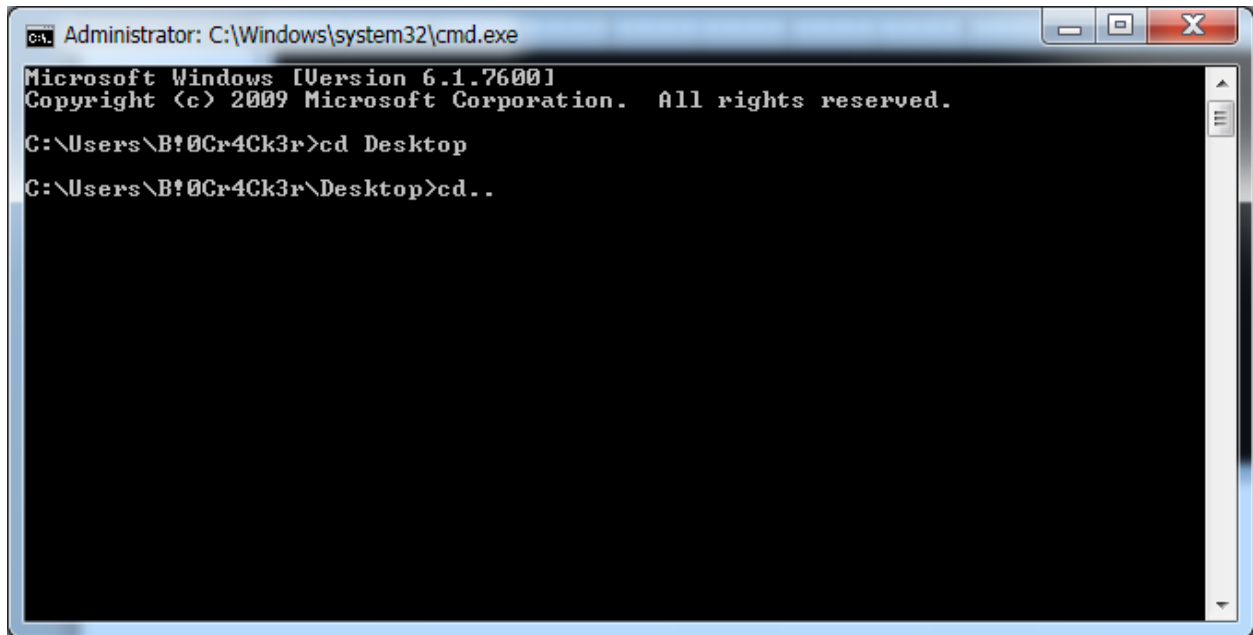
အခုကျွန်တော်က Desktop ပေါ်က အနီရောင်အကွက်လေးလုပ်ထားတဲ့ For Share ဆိုတဲ့ Folder ထဲကိုဝင် မယ်ဆိုပါစို့။ သူ့ရဲ့ပတ်လမ်းကိုသိရပါမယ်။ဒီတော့ ပတ်လမ်းဘယ်လိုသွားရမလည်း ဆိုတာ သိဖို့ အတွက်က တော့



အထက်ပါပုံအတိုင်း My Computer ကိုဖွင့်လိုက်ပါ အနီရောင်လိုင်းကလေးအတိုင်းပေ... C: Location
 ထဲက နေ Documents and Settings ထဲက B!0Cr4Ck3r (လက်ရှိ User Folder) ထဲကနေ Desktop
 ဆိုတဲ့အဆင့် အတိုင်းသွားလိုက်တဲ့အခါမှာလည်း အောက်က လေးထောင့်ကွက်လေးကအတိုင်း For
 Share ဆိုတဲ့ Folder ထဲကိုရောက်သွားနိုင်ပါတယ်။ ဒါပေမယ့် Command လိုင်းထဲမှာကတော့



အောက်ပါလိပ်စာအတိုင်းပေါ့..... ဒီတော့ cd ဆိုတဲ့အကြောင်းလေးပြောဖို့ကျန်နေပြီနဲ့တူတယ်။
ဖိုဒါတစ်ခုကို ဝင်ချင်တယ်ဆိုရင် >cd (ဝင်ချင်တဲ့ဖိုဒါနာမည်) ဆိုရင် သူက အဲဒီဖိုဒါထဲကို ရောက်ပါမယ်။
ပြန်ထွက်ချင်တယ် ဆိုရင်တော့



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\B!0Cr4Ck3r>cd Desktop
C:\Users\B!0Cr4Ck3r\Desktop>cd..
```

အထက်ပါပုံအတိုင်း >cd.. ဆိုပြီးရိုက်ရပါမယ်။ ဒါကတော့ နောက်က ဖိုဒါပတ်လမ်းတစ်ခုဆီကို
ပြန်ထွက်တာ ဖြစ်ပါတယ်။ အကယ်လို့များ C: ဆိုတဲ့ root နေရာကိုတိုက်ရိုက်သွားချင်တယ်ဆိုရင်တော့
>cd\ ဆိုပြီး ရိုက်ရ ပါမယ်။

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\B!0Cr4Ck3r>cd Desktop
C:\Users\B!0Cr4Ck3r\Desktop>cd..
C:\Users\B!0Cr4Ck3r>cd\
```

အထက်ပါပုံအတိုင်းရိုက်လိုက်တဲ့အခါမှာတော့

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

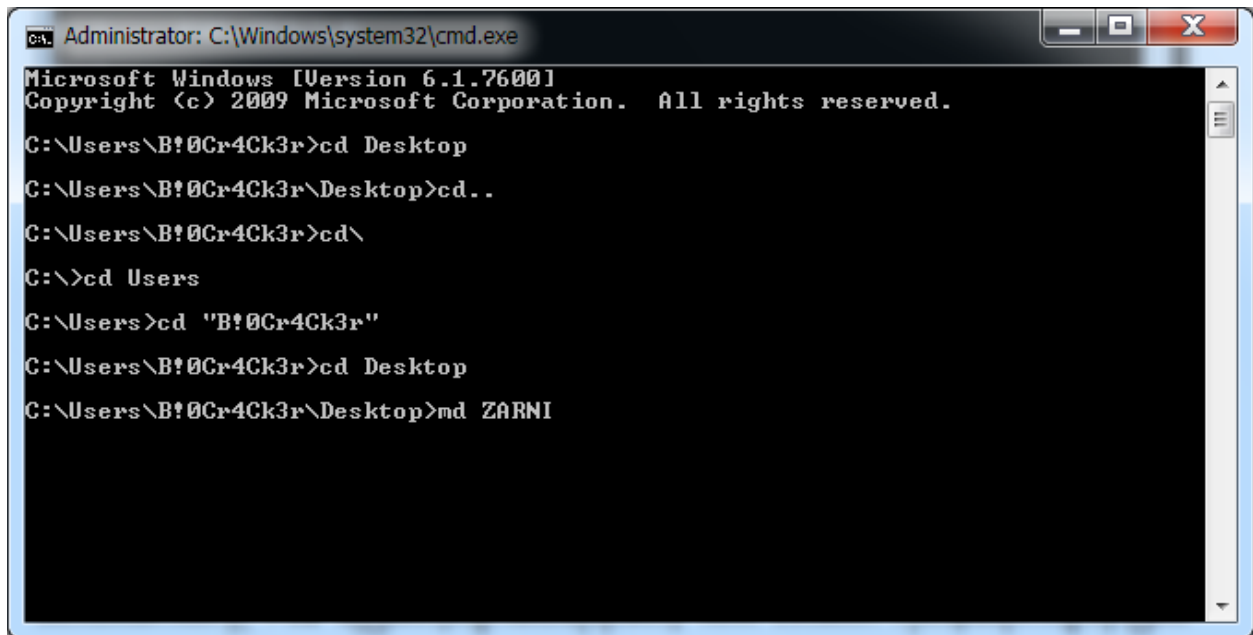
C:\Users\B!0Cr4Ck3r>cd Desktop
C:\Users\B!0Cr4Ck3r\Desktop>cd..
C:\Users\B!0Cr4Ck3r>cd\
C:\>_
```

အထက်ပါပုံအတိုင်း Root Location ကိုတန်းရောက်သွားပါတယ်။ ဒါကတော့ cd command မှာသုံးတဲ့အသုံး နှုန်းပါပဲ... အဲ Linux နဲ့ ယှဉ်ပြီးပြောရရင်တော့။ ကျွန်တော်တို့ ဖိုင်တစ်ခုထဲဝင်ချင်ရင် >cd (Folder) ဆိုပြီး ဝင်တာလည်းတူပါတယ်။ ပြန်ထွက်တဲ့အခါမှာတော့ >cd .. ဆိုပြီးဖြစ်ပါတယ်။

မတူပါဘူး cd.. မှာ Space ခြား ပါတယ်။အကယ်လို့ >cd ဆိုပြီးတော့ပဲရိုက်မယ်ဆိုရင်တော့ Root Location ကိုတန်းရောက်သွားမှာဖြစ်ပါ တယ်။

“ rd & md or mkdir ”

rd ဆိုတာကတော့ Remove Directory ဖြစ်ပြီး md ဆိုတာကတော့ Make Directory ဖြစ်ပါတယ်။ ဘယ်လို သုံးရမလည်းဆိုတာကို ပုံလေးနဲ့ ဆက်ပြပါမယ်။ဥပမာတစ်ခု ကျွန်တော်တို့က Desktop ပေါ်မှာ ZARNI ဆို တဲ့ Folder လေးတစ်ခုတည်ပါမယ်။ဒီတော့ ကျွန်တော်တို့က Desktop Location ကိုအရင်ဝင်ဂျပိမယ် ပြီးသွားရင် တော့ >md ZARNI ဆိုပြီး ရိုက်လိုက်ပါမယ်။



```
C:\> Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\B!0Cr4Ck3r>cd Desktop
C:\Users\B!0Cr4Ck3r\Desktop>cd..
C:\Users\B!0Cr4Ck3r>cd\
C:\>cd Users
C:\Users>cd "B!0Cr4Ck3r"
C:\Users\B!0Cr4Ck3r>cd Desktop
C:\Users\B!0Cr4Ck3r\Desktop>md ZARNI
```

ဒီလိုဆိုရင်သင့်ရဲ့ Desktop ပေါ်မှာ စစ်ကြည့်လိုက်ပါ

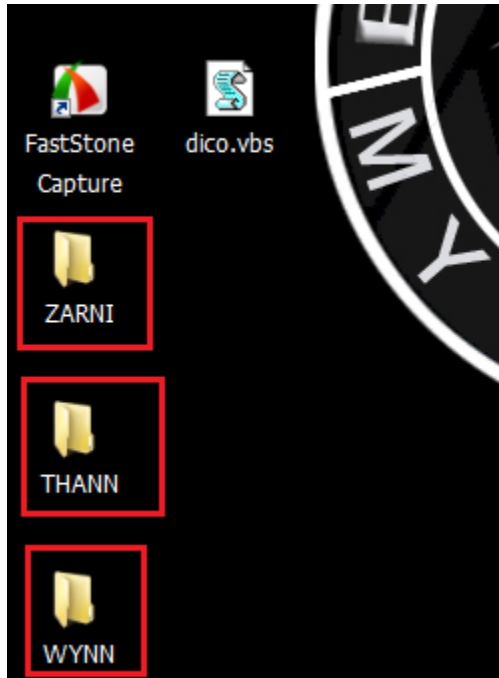


Desktop ပေါ်မှာ **ZARNI** ဆိုတဲ့ ဖိုဒါရောက်နေပါမယ်။ ဒါကတော့ GUI Mode ပေါ်မှာဆိုရင် Right Click နှိပ် တယ်။ ပြီးသွားရင် New ထဲကနေ Folder ဆိုပြီး မိမိ နှစ်သက်ရာ နာမည်ပေးတာနဲ့ အတူတူ ပါပဲ။ဟုတ်ပြီး နောက် တစ်ချက်ပြောပါမယ်။ အကယ်လို့ သင်ဟာ **ZARNI THANN WYNN** လို့နာမည်ပေးချင်တယ်ဆို ရင် ကျွန်တော်တို့က

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\B!0Cr4Ck3r>cd Desktop
C:\Users\B!0Cr4Ck3r\Desktop>cd..
C:\Users\B!0Cr4Ck3r>cd\
C:\>cd Users
C:\Users>cd "B!0Cr4Ck3r"
C:\Users\B!0Cr4Ck3r>cd Desktop
C:\Users\B!0Cr4Ck3r\Desktop>md ZARNI
C:\Users\B!0Cr4Ck3r\Desktop>md ZARNI THANN WYNN
```

အထက်ပါပုံအတိုင်းရိုက်လို့မရပါဘူး ။ ဘာကြောင့်လည်းမေးလာရင် ပုံနဲ့ လက်တွေ့ပြပါမယ်။ အကယ်
လို့ သင်ဟာ အဲဒီလိုရိုက်လိုက်မယ်ဆိုရင် သင့်ရဲ့ Desktop ပေါ်မှာ



အပေါ်ကပုံအတိုင်း **ZARNI** ကတစ်ခု **THANN** ကတစ်ခု **WYNN** တစ်ခုဆိုပြီး ဖိုဒါ ဂရုဖြစ်သွားပါမယ်
ဘာကြောင့် လည်းဆိုတော့ ကျွန်တော်တို့က CLI Mode ထဲမှာ Space ခြားပြီး ဖိုဒါနာမည်ပေးမယ်ဆိုရင်
double cots တွေထည့် ပေးရပါမယ်။ ရိုက်ရမှာက `>md "ZARNI THANN WYNN"` ဆိုပြီးတော့


```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

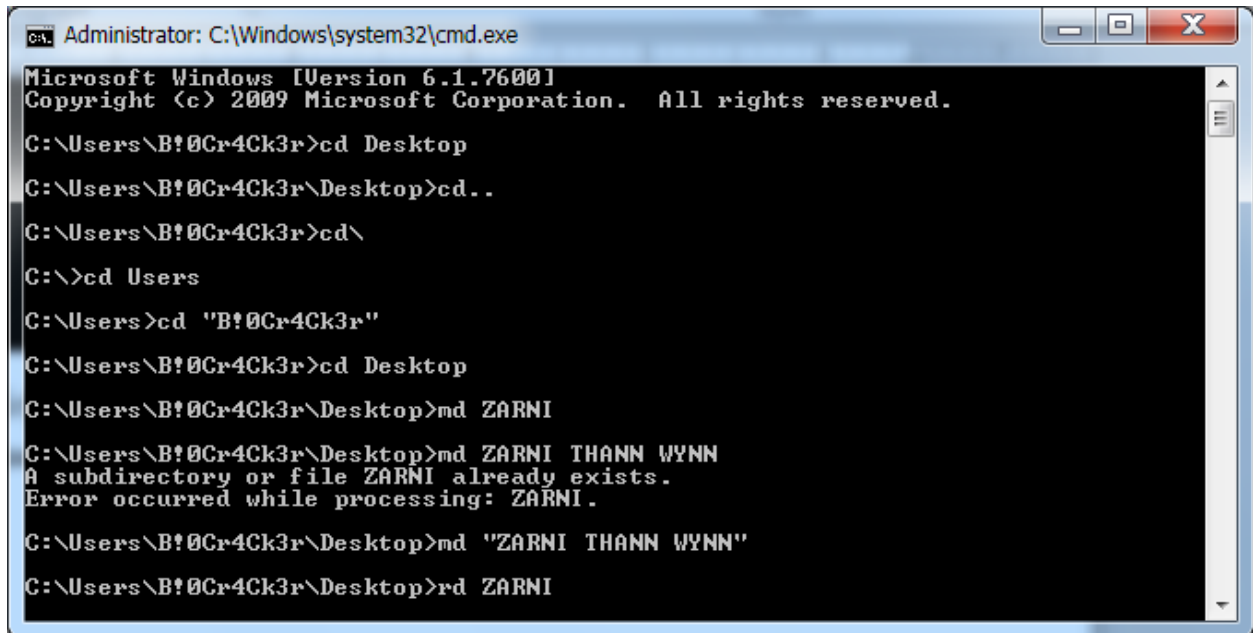
C:\Users\B!0Cr4Ck3r>cd Desktop
C:\Users\B!0Cr4Ck3r\Desktop>cd..
C:\Users\B!0Cr4Ck3r>cd\
C:\>cd Users
C:\Users>cd "B!0Cr4Ck3r"
C:\Users\B!0Cr4Ck3r>cd Desktop
C:\Users\B!0Cr4Ck3r\Desktop>md ZARNI
C:\Users\B!0Cr4Ck3r\Desktop>md ZARNI THANN WYNN
A subdirectory or file ZARNI already exists.
Error occurred while processing: ZARNI.
C:\Users\B!0Cr4Ck3r\Desktop>md "ZARNI THANN WYNN" _
```

အထက်ပါပုံအတိုင်းဖြစ်ပါတယ်။ ဒါမှ သင့်ရဲ့ Desktop ပေါ်မှာလည်း



အထက်ပါပုံအတိုင်းသင်လိုချင်တဲ့ ZARNI THANN WYNN ဆိုတဲ့ နာမည်နဲ့ရရှိမှာဖြစ်ပါတယ်။
ကဲဒီလောက်ဆို ရင် md Command အကြောင်း သိပြီထင်ပါတယ်။ ဒါဆိုရင် rd Command

အကြောင်းဆက်ပြောပါမယ်။ **rd** ဆိုတာကတော့ Remove Directory ဖြစ်ပါတယ်။ ဒီတော့ ကျွန်တော် တို့က ခုနက တည်ဆောက်ထားတဲ့ Folder တွေကိုပြန်ဖျက်ပြပါမယ်။ အရင်ဆုံး **ZARNI** ဆိုတဲ့ ဖိုဒါကိုဖျက် ပါမယ်။ ရိုက်ရမှာက **>rd ZARNI** ဆိုပြီး



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\B!\0Cr4Ck3r>cd Desktop
C:\Users\B!\0Cr4Ck3r\Desktop>cd..
C:\Users\B!\0Cr4Ck3r>cd\
C:\>cd Users
C:\Users>cd "B!\0Cr4Ck3r"
C:\Users\B!\0Cr4Ck3r>cd Desktop
C:\Users\B!\0Cr4Ck3r\Desktop>md ZARNI
C:\Users\B!\0Cr4Ck3r\Desktop>md ZARNI THANN WYNN
A subdirectory or file ZARNI already exists.
Error occurred while processing: ZARNI.
C:\Users\B!\0Cr4Ck3r\Desktop>md "ZARNI THANN WYNN"
C:\Users\B!\0Cr4Ck3r\Desktop>rd ZARNI
```

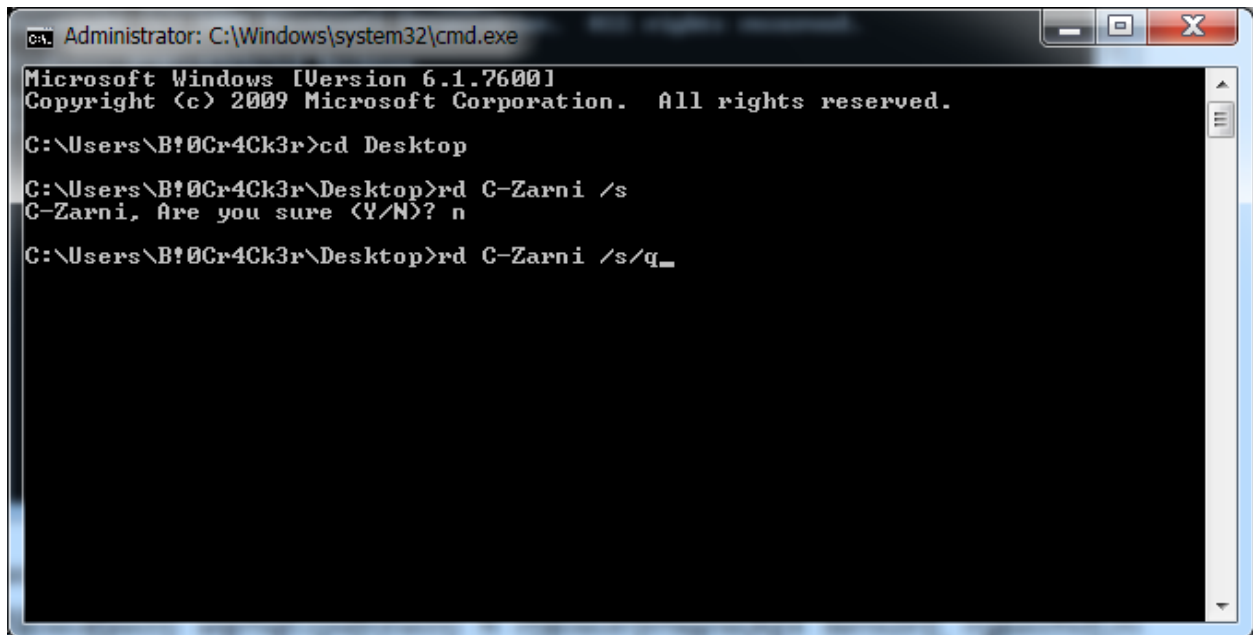
အထက်ပါပုံအတိုင်းရိုက်လိုက်တဲ့အခါမှာ သင့်ရဲ့ Desktop ပေါ်မှာ **ZARNI** ဆိုတဲ့နာမည် နဲ့ခပ်ချော ချောကောင် လေးတစ်ယောက်ရဲ့ နာမည်နဲ့ ဖိုဒါကမရှိတော့ပါဘူး။ အလားတူပဲ အခြား Folder တွေ ကိုဖျက် ချင်တယ်ဆိုရင် လည်း

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\B!0Cr4Ck3r\Desktop>cd..
C:\Users\B!0Cr4Ck3r>cd\
C:\>cd Users
C:\Users>cd "B!0Cr4Ck3r"
C:\Users\B!0Cr4Ck3r>cd Desktop
C:\Users\B!0Cr4Ck3r\Desktop>md ZARNI
C:\Users\B!0Cr4Ck3r\Desktop>md ZARNI THANN WYNN
A subdirectory or file ZARNI already exists.
Error occurred while processing: ZARNI.
C:\Users\B!0Cr4Ck3r\Desktop>md "ZARNI THANN WYNN"
C:\Users\B!0Cr4Ck3r\Desktop>rd ZARNI
C:\Users\B!0Cr4Ck3r\Desktop>rd THANN
C:\Users\B!0Cr4Ck3r\Desktop>rd WYNN
C:\Users\B!0Cr4Ck3r\Desktop>rd "ZARNI THANN WYNN"
```

ဒီအတိုင်းပဲ >rd THANN , >rd WYNN , >rd "ZARNI THANN WYNN" ဆိုပြီးရိုက်ပြီးဖျက် နိုင်ပါတယ်။
rd မှာထပ်ပြီး နောက်ဆက်တွဲ Parameter တွေရှိပါသေးတယ် သူကတော့ /s နဲ့ /q ပဲဖြစ်ပါတယ်။
ဘယ်လို အနေ အထားမှာလည်းဆိုတော့ ကျွန်တော်တို့ဖျက်မယ့် Folder ထဲက ဖိုင်တစ်ခုခုက အခြား
Process တစ်ခုခုမှာ သုံး နေမယ်ဆိုရင် လုံးဝ rd တစ်ခုတည်းနဲ့ ဖျက်လို့မရပါဘူး ဒါကြောင့် ကျွန်တော်
တို့က >rd (ဖျက်ချင်သော ဖိုဒါနာမည်) /s လို့ရိုက်ပါမယ်။ဒါဆိုရင်

```
Administrator: C:\Windows\system32\cmd.exe - rd C-Zarni /s
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\B!0Cr4Ck3r>cd Desktop
C:\Users\B!0Cr4Ck3r\Desktop>rd C-Zarni /s
C-Zarni, Are you sure (Y/N)?
```

အထက်ပါအတိုင်း သေချာသလား Yes or No မေးပါလိမ့်မယ် ဒါဆိုရင် ကျွန်တော်တို့က ဖျက်မယ်ဆိုရင် Y ကိုနှိပ်ပေးပြီးတော့ မဖျက်ချင်ဘူးဆိုရင်တော့ N ကိုနှိပ်ပေးလိုက်ရမှာပေါ့ဗျာ။ အကယ်လို့ ကျွန်တော်တို့က ပြန်မမေးစေချင်ဘူး တစ်ခါတည်းတန်းဖျက်မယ် ဘယ် Process ထဲမှာပဲ ယူပြီး Run နေ Run နေ ဖျက်ကိုဖျက် မယ်ဆိုရင်တော့ သုံးရမယ့် Command က

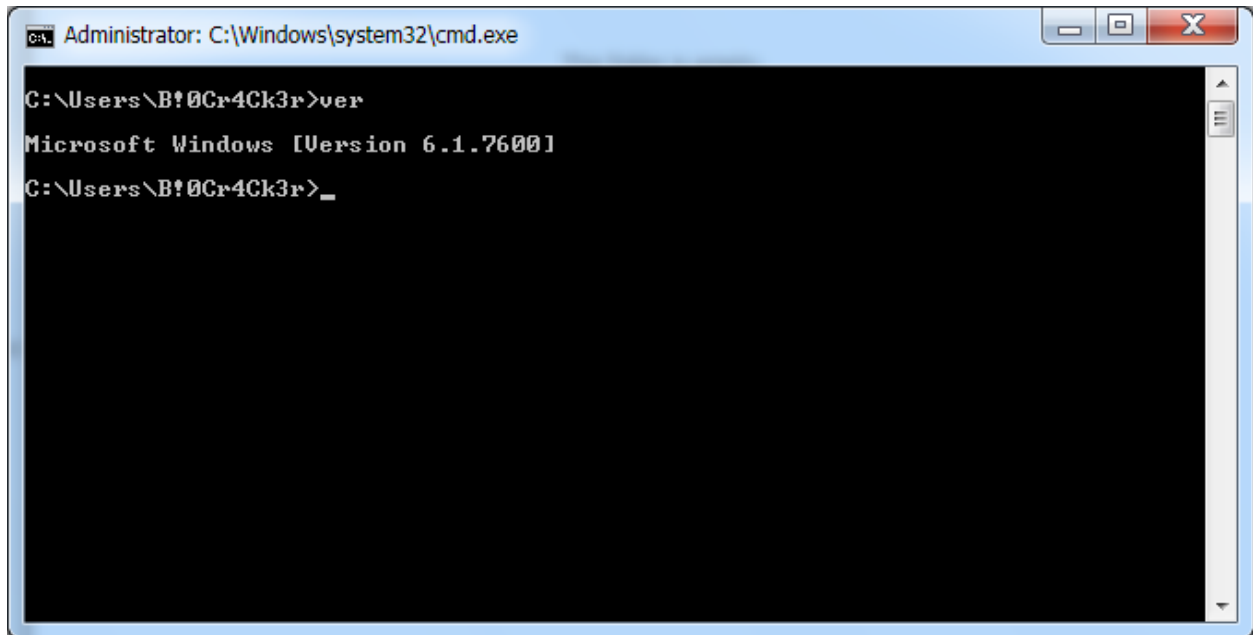


```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\B!0Cr4Ck3r>cd Desktop
C:\Users\B!0Cr4Ck3r\Desktop>rd C-Zarni /s
C-Zarni, Are you sure (Y/N)? n
C:\Users\B!0Cr4Ck3r\Desktop>rd C-Zarni /s/q_
```

အထက်ပါပုံအတိုင်း >rd C-Zarni /s/q ဆိုပြီး နောက်က Parameter နှစ်ခုကိုကပ်ပေးလိုက်ပါ။ ဒါဆိုရင် သင့်ကို ဘာမှ မေးမှာမဟုတ်တော့ပဲ တန်းဖျက်သွားပါလိမ့်မယ်။

“ver”

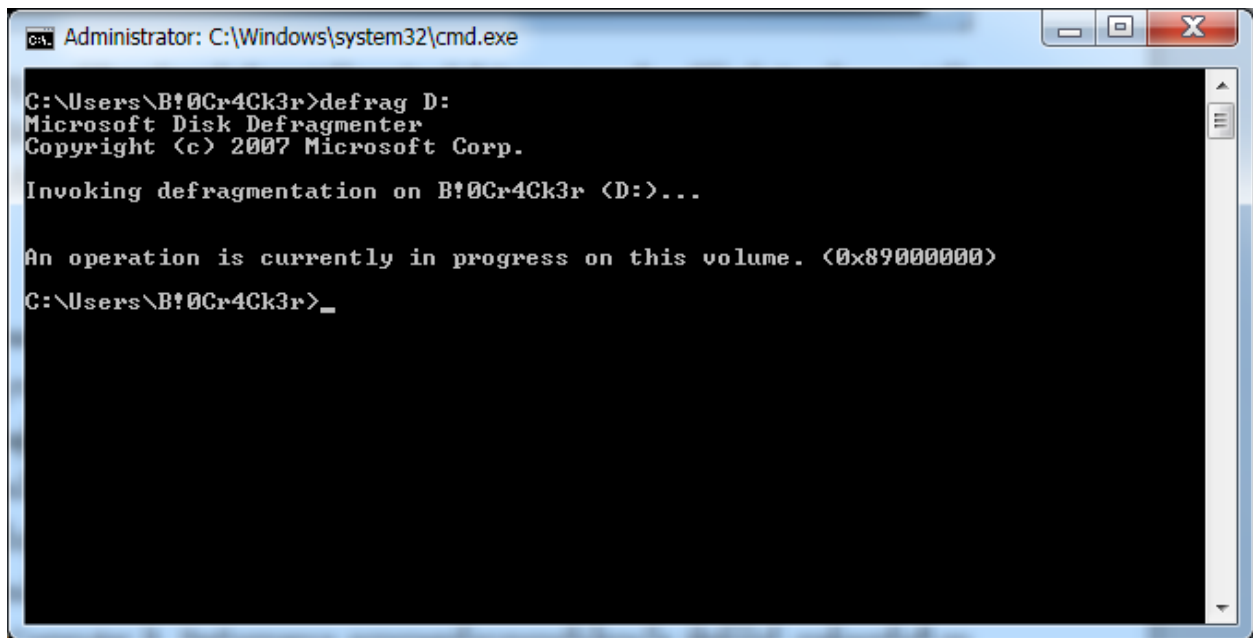


```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\B!0Cr4Ck3r>ver
Microsoft Windows [Version 6.1.7600]
C:\Users\B!0Cr4Ck3r>_
```

Ver ဆိုတာကတော့ လက်ရှိ ကျွန်တော်တို့အသုံးပြုနေတဲ့ ဝင်းဒိုးရဲ့ Version ကို ဖော်ပြချင်တဲ့အခါမှာ အသုံးပြုတာဖြစ်ပါတယ်။ GUI Mode မှာဆိုရင်တော့ My Computer ကို Right Click နှိပ်ပြီး Properties ထဲဝင်ကြည့်ရင်အလွယ်တကူသိရှိနိုင်ပါတယ်။

“defrag”

Defrag ဆိုတာကတော့ ကျွန်တော်တို့ Defragmentation လုပ်တာပဲဖြစ်ပါတယ်။ ဆိုလိုတာကတော့ HDD မှာ ကျွန်တော်တို့က Data တွေကိုထည့်လိုက် ၊ ဖျက်လိုက်၊ နှင့် နေရာတိုင်းမှာ သိမ်းဆည်းထားကြတာဖြစ်ပါတယ်။ ဥပမာအနေဖြင့်ဆိုရင် လုပ်ငန်းတစ်ခုမှ ဖိုင်တွဲတွေထားတဲ့ စင်တစ်ခုပေါ်မှာ သုံးစွဲသူက မိမိလိုချင်တဲ့ ဖိုင်တွဲကိုယူသုံးတယ်၊ ပြီးတော့ပြန်ထားတယ် ။ နောက်လူကလည်း အလားတူပဲ ဒီလိုယူသုံးတယ်။ ပြန်ထားတယ်။ ဒီလိုနဲ့ ဖိုင်တွဲတွေတင်ထားတဲ့စင်က ကြာလာတာနဲ့အမျှ သပ်ရပ်မှုမရှိတော့ပဲ ဖရိုဖရဲဖြစ်နေတဲ့ ပုံစံမျိုး ဖြစ်သွားတတ်ပါတယ်။ ဒါကြောင့် HDD ကလည်း ထိုနည်းအတိုင်းပါပဲ ကြာလာနဲ့အမျှ ဖိုင်တွေက HDD မှာ ဖရိုဖရဲတွေဖြစ်ပြီး Computer ရဲ့ Performance တွေကျဆင်းလာတတ်ပါတယ်။ ဒါကြောင့် ကျွန်တော်တို့က Defragment လုပ်ပေးရတာပါ။ ဘာ Command ကိုရိုက်ရမလည်းဆိုတော့ **>defrag D:** ဆိုပြီးရိုက်လိုက်ပါမယ်။



အပေါ်ပုံကတော့ D Partition ကို Defrag လုပ်တာပါ။ သို့.နောက်မှာတွဲရမယ့် Parameter တွေကတော့

/A Perform analysis on the specified volumes.

/C Perform the operation on all volumes.

/E Perform the operation on all volumes except those specified.

/H Run the operation at normal priority (default is low)

/M Run the operation each volumes in parallel in the background.

/T Track an operation already in progress on the specified volumes.

/U Print the progress of the operation on the screen.

/V Print verbose output containing the fragmentation statistics.

/X Perform free space consolidation on the specified volumes.

တို့.ဖြစ်ပါတယ် အသုံးပြုပုံ ဥပမာတွေကတော့

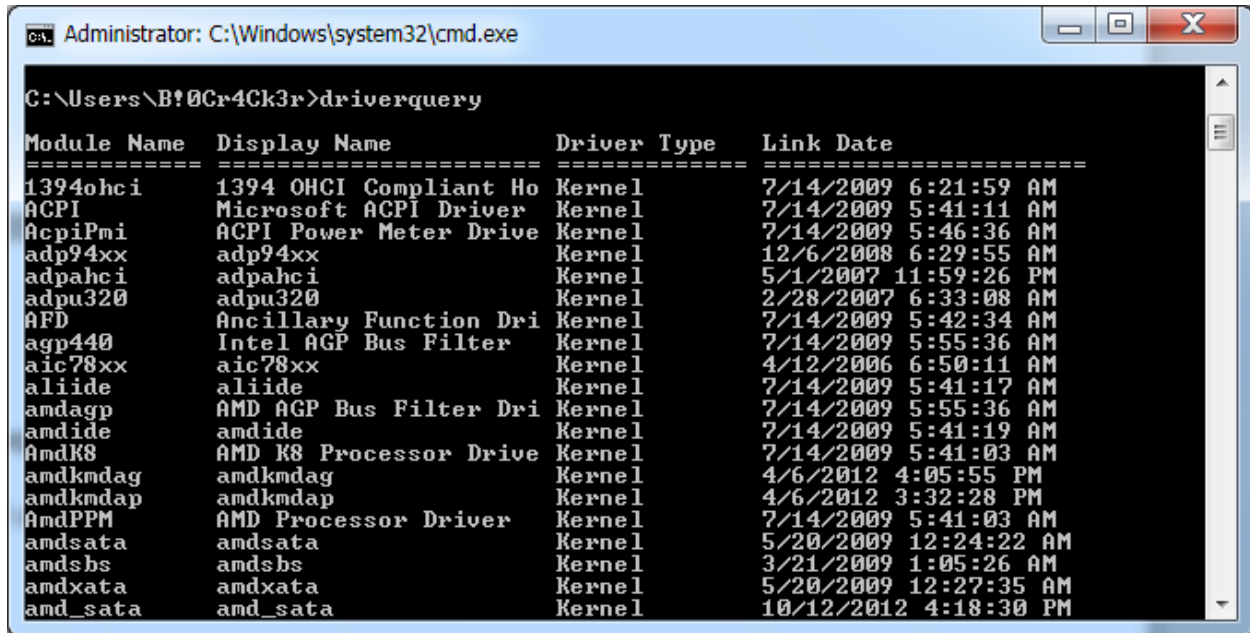
defrag C: /U /V

defrag C: D: /M

defrag C:\mountpoint /A /U

defrag /C /H /V တို့ပဲဖြစ်ပါတယ်။

“drivequery”



```
Administrator: C:\Windows\system32\cmd.exe

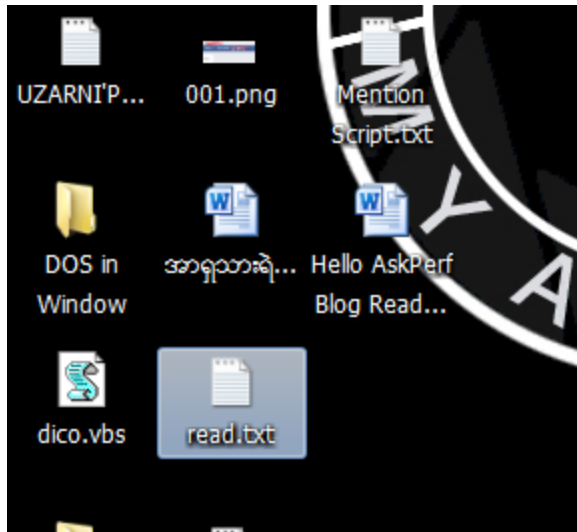
C:\Users\B!0Cr4Ck3r>driverquery

Module Name      Display Name      Driver Type      Link Date
=====
1394ohci         1394 OHCI Compliant Ho Kernel          7/14/2009 6:21:59 AM
ACPI             Microsoft ACPI Driver Kernel          7/14/2009 5:41:11 AM
AcpiPmi          ACPI Power Meter Drive Kernel          7/14/2009 5:46:36 AM
adp94xx          adp94xx           Kernel          12/6/2008 6:29:55 AM
adpahci          adpahci           Kernel          5/1/2007 11:59:26 PM
adpu320          adpu320           Kernel          2/28/2007 6:33:08 AM
AFD              Ancillary Function Dri Kernel          7/14/2009 5:42:34 AM
agp440           Intel AGP Bus Filter Kernel          7/14/2009 5:55:36 AM
aic78xx          aic78xx           Kernel          4/12/2006 6:50:11 AM
aliide           aliide            Kernel          7/14/2009 5:41:17 AM
amdagp           AMD AGP Bus Filter Dri Kernel          7/14/2009 5:55:36 AM
amdide           amdide            Kernel          7/14/2009 5:41:19 AM
AmdK8            AMD K8 Processor Drive Kernel          7/14/2009 5:41:03 AM
amdkmdag         amdkmdag          Kernel          4/6/2012 4:05:55 PM
amdkmdap         amdkmdap          Kernel          4/6/2012 3:32:28 PM
AmdPPM           AMD Processor Driver Kernel          7/14/2009 5:41:03 AM
amdsata          amdsata           Kernel          5/20/2009 12:24:22 AM
amdsbs           amdsbs            Kernel          3/21/2009 1:05:26 AM
amdxtata         amdxtata          Kernel          5/20/2009 12:27:35 AM
amd_sata         amd_sata          Kernel          10/12/2012 4:18:30 PM
```

Drivequery ဆိုတာကတော့ လက်ရှိ သင့်ရဲ့ ကွန်ပျူတာထဲက HDD ထဲမှာရှိသော Driver Type တွေနဲ့ Module name တွေကိုသိချင်တဲ့အခါမှာသုံးတာဖြစ်ပါတယ်။

“copy”

Copy Command ကတော့ ကျွန်တော်တို့ Copy လုပ်ချင်တဲ့အခါမှာ သုံးပါတယ်။ GUI Mode မှာဆိုရင်တော့ Ctrl+C လို့လုပ်ပြီး ထားချင်တဲ့နေရာမှာ Ctrl+V ဆိုပြီးလုပ်ဆောင်ရတာပါ။ ဒီ Command Line ထဲမှာဘယ်လိုရိုက်ရမလည်းဆိုတော့ ဥပမာ ကျွန်တော်က Desktop ပေါ်က read.txt ဆိုတဲ့ဖိုင်ကို



D ဆိုတဲ့ Data Partition ထဲကိုကူးယူချင်တာပါ။ ဒီတော့ဂိုက်ရမယ့် Command ကတော့

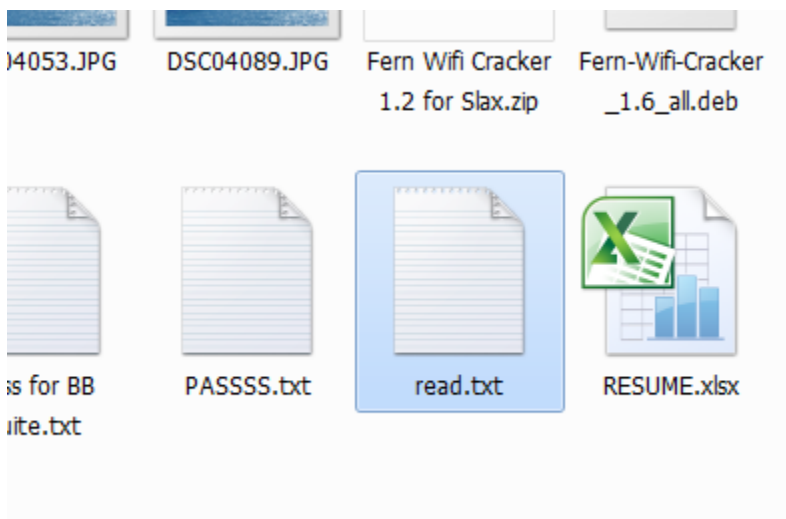
```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\B!0Cr4Ck3r>copy C:\Users\%username%\Desktop\read.txt d:\read.txt
```

ဆိုပြီးတော့ဖြစ်ပါတယ်။ ဒီနေရာမှာတစ်ခုချင်းစီရှင်းပြပေးပါမယ်။ **B!0Cr4Ck3r>** ဆိုတာကတော့ သင်လက်ရှိဖွင့်လှက်တဲ့အချိန်မှာ သင့်ရဲ့ Username ကိုပြနေမှာပါ။ ဒီနောက်မှာ စပြီးကော်ပီကူးဖို့အတွက် **copy** ဆိုတဲ့ Command ကို စတင်အသုံးပြုလိုက်ပါတယ်။ ဒီနောက် Desktop ရဲ့ Location ကိုရောက်အောင်အရင်သွားရပါမယ်။ ဒီတော့ ကျွန်တော်တို့က **C:\User\%username%\Desktop** ဆိုပြီးတော့ပေါ့။ **%username%** ဆိုတာကတော့ Owner name ကိုကိုယ်စားပြုတာပါ။ Desktop နေရာရောက်ပြီဆိုရင် ကျွန်တော်တို့က **read.txt** ဆိုတဲ့ဖိုင်ကိုကူးမှာဖြစ်တဲ့အတွက်ကြောင့် ရိုက်လိုက်တာပါ။ ဒီနော့ မိမိကူးယူမယ့် Desination ကိုသတ်မှတ်ပေးရမှာဖြစ်ပါတယ်။


```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\B!0Cr4Ck3r>copy C:\Users\%username%\Desktop\read.txt d:\read.txt
1 file(s) copied.
C:\Users\B!0Cr4Ck3r>
```

ကျွန်တော်တို့က D Partition ထဲမှာ ကူးယူချင်တာဖြစ်တဲ့အတွက်ကြောင့် d:\read.txt ဆိုပြီးရိုက်ပေးလိုက်တာ ပါ။ ဒါဆိုရင်တော့ သင့်ကွန်ပျူတာ D Partition ထဲမှာ



Read.txt ဆိုပြီးရောက်နေမှာဖြစ်ပါတယ်။ ဒီနည်းအတိုင်းပဲ မိမိကူးယူချင်သော ဖိုင်များကိုအလွယ်တကူ Source နဲ့ Desination ကို သတ်မှတ်ပြီးကူးယူနိုင်ပါတယ်။

"type"

Type ဆိုတာကတော့ မိမိကြည့်ချင်တဲ့ဖိုင်တွေကို အထူးသဖြင့် Window ထဲက အရေးကြီးတဲ့ System File တွေကိုကြည့်ချင်တဲ့အခါမှာသုံးတာပါ။ ဥပမာ ကျွန်တော်တို့က C: အောက်က System File အချို့ကိုကြည့် ချင်သောအခါမှာ...

-autoexec.bat

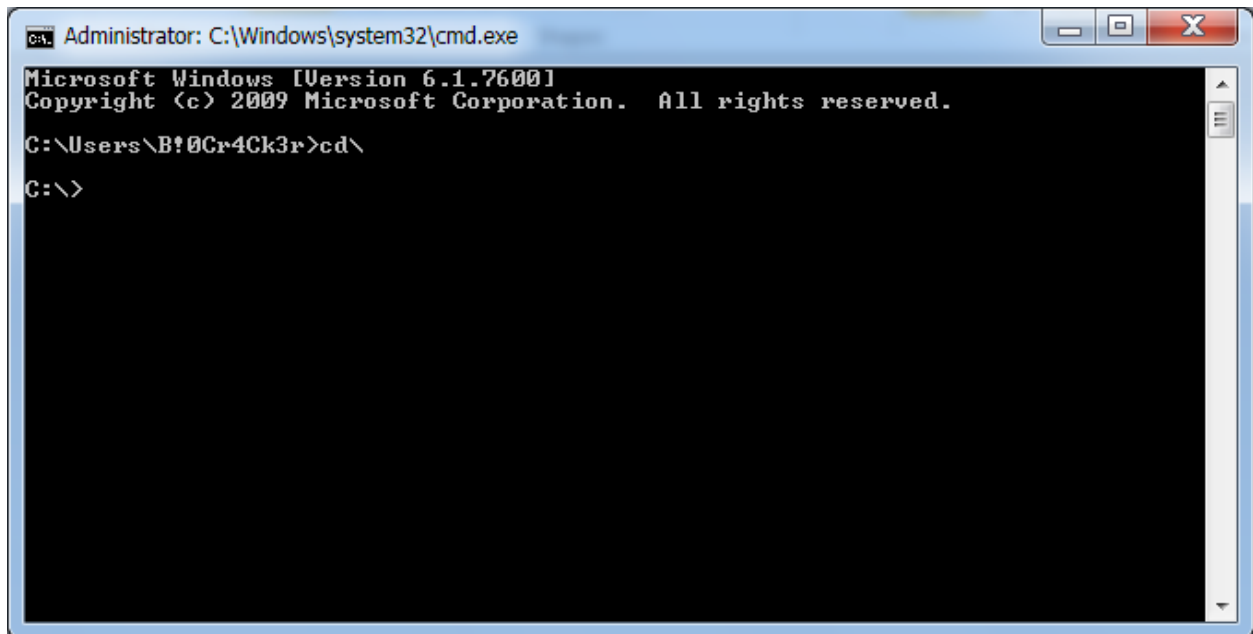
config.sys

hiberfil.sys

IO.SYS

MSDOS.SYS

pagefile.sys စတဲ့ဖိုင်တွေကိုနမူနာကြည့်ပြပါမယ်။



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\B!0Cr4Ck3r>cd\
C:\>
```

အထက်ပါပုံအတိုင်းကတော့ လက်ရှိရောက်နေတဲ့ Location ကနေ ကျွန်တော်တို့ကြည့်ချင်တဲ့ Root Partition C: ထဲကိုရောက်အောင်သွားဖို့အတွက် >cd\ ဆိုပြီးရိုက်လိုက်ပါတယ်။ ဒီနောက်တော့

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\B!0Cr4Ck3r>cd\

C:\>type autoexec.bat
REM Dummy file for NTUDM
C:\>type config.sys
FILES=40

C:\>type hiberfil.sys
The process cannot access the file because it is being used by another process.
C:\>type IO.SYS

C:\>type MSDOS.SYS

C:\>type pagefile.sys
The process cannot access the file because it is being used by another process.
C:\>_
```

ကျွန်တော်တို့က တစ်ခုချင်းစီကိုတိုက်ပြီးကြည့်လို့ရပါတယ်။ အချို့ကတော့ အခြား Process မှာ Run နေတယ်လို့ပြပြီး အချို့ဖိုင်တွေမှာကတော့ သူ့ထဲက ဒေတာတွေကိုပြပါမယ်။

“hostname”

```
Administrator: C:\Windows\system32\cmd.exe

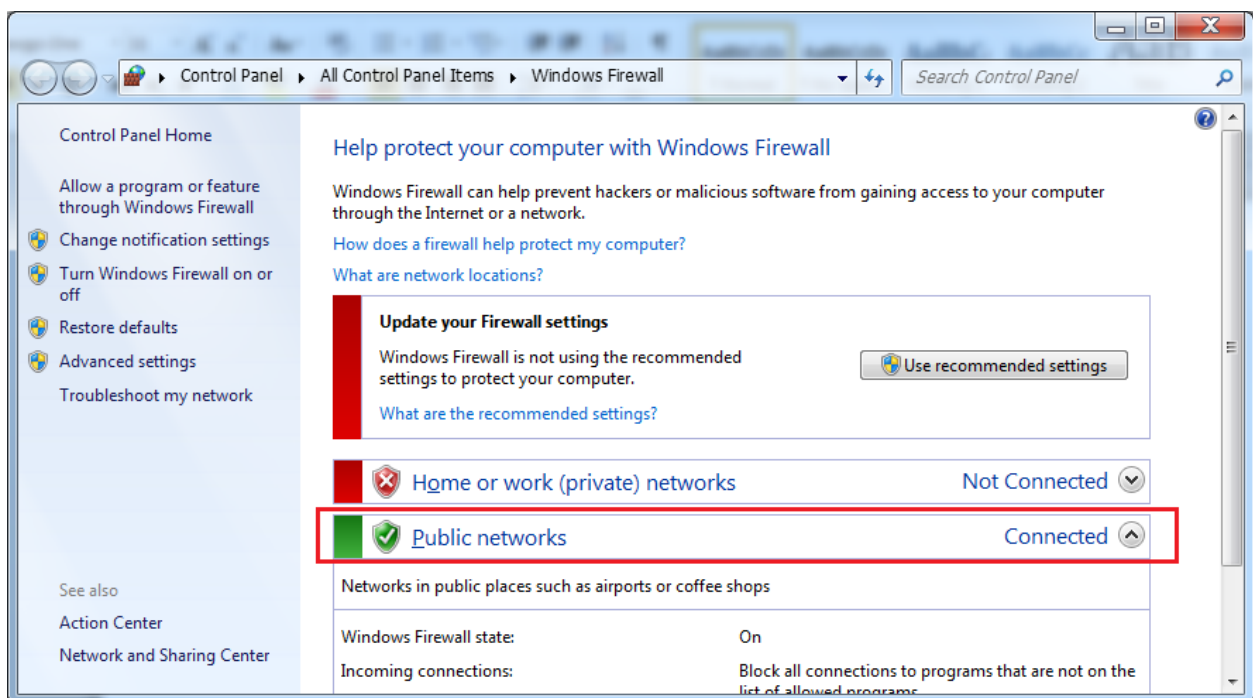
C:\>hostname
B!0Cr4Ck3r-PC

C:\>_
```

Hostname ဆိုတာကတော့လက်ရှိ မိမိကွန်ပျူတာရဲ့ အမည်နာမကို သိချင်သော အခါမှာအသုံးပြုတာဖြစ်ပါတယ်။

“netsh ”

Netsh ဆိုတဲ့ Command ကတော့ မိမိကွန်ပျူတာ Network အတွက် Configure လုပ်တဲ့ အဓိက Command တစ်ခုဆိုလည်းမမှားပါဘူး။ဥပမာတစ်ခုဖြင့်ပြသရသော ကျွန်တော်တို့ Network မှာ Security ပိုင်းအတွက် Window Firewall ကို Enable လုပ်ပေးထားရပါတယ်။ သို့ပေမယ့် LAN ထဲမှာ Gaming လုပ်တာတွေ၊ Sharing လုပ်တာတွေအတွက် ဒီ Window Firewall Service ကို Enable လုပ်ထားမယ်ဆိုရင် Error တက်တတ် ပါတယ်။ ဒါကြောင့် အများစုက Diasble လုပ်ထားရပါတယ်။ ပုံမှန် GUI Mode မှာဆိုရင်တော့ Run Box ထဲမှာ Firewall.cpl လို့ရိုက်လိုက်ပြီး Change Firewall Setting ထဲမှာ သွားပြီး Disable လုပ်ပေးရပါတယ်။



ဒါပေမယ့် ကျွန်တော်တို့က DOS ထဲကနေသွားတဲ့အခါမှာတော့ ရိုက်ရမယ့် Command က

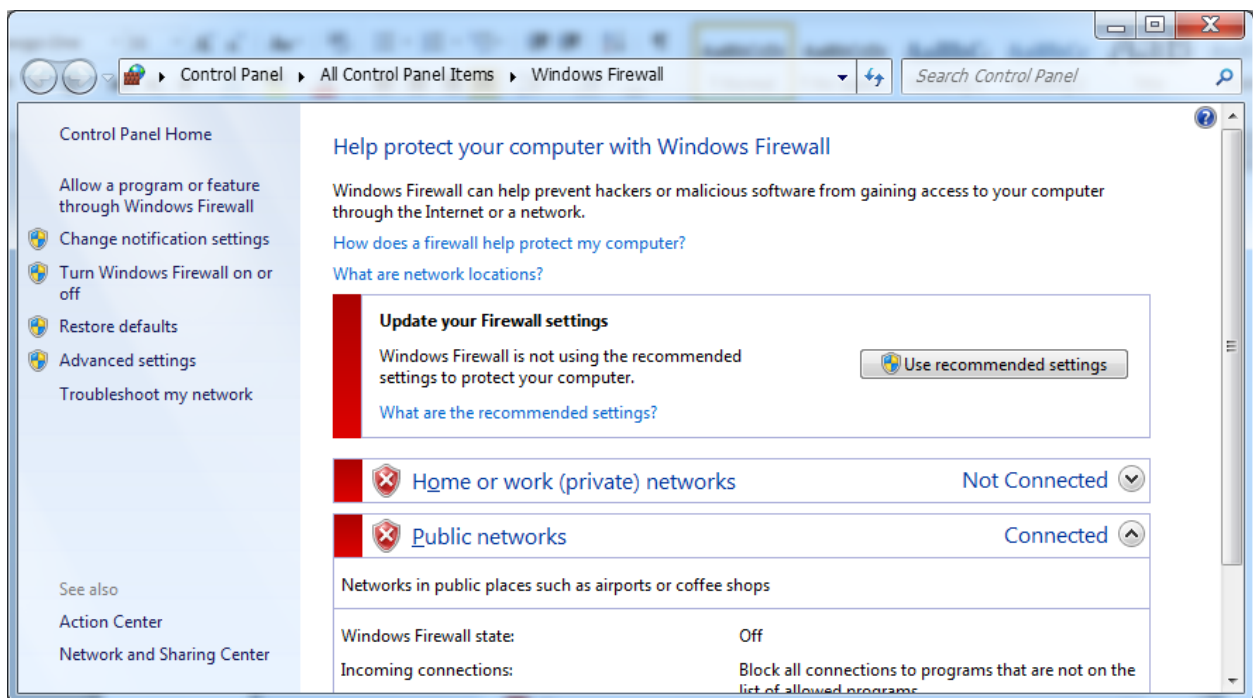
```
Administrator: CristianoZarni
C:\>netsh firewall set opmode disable

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at http://go.microsoft.com/fwlink/?linkid=121488 .

Ok.

C:\>_
```

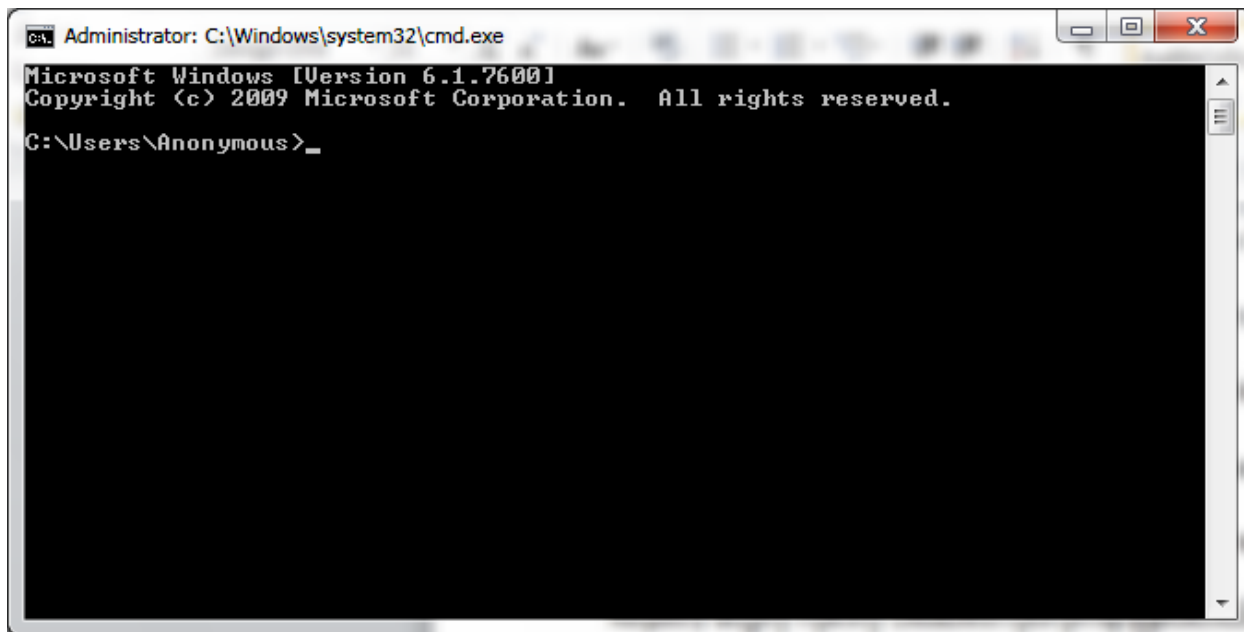
အထက်ပါပုံအတိုင်းမှ >netsh firewall set opmode disable ဆိုပြီးရိုက်ပေးလိုက်တဲ့အခါမှာတော့



အထက်ပါပုံအတိုင်း Disable ဖြစ်သွားပါမယ်။ အကယ်လို ကျွန်တော်တို့က Enable ပြန်လုပ်ချင်တယ်ဆိုရင်တော့ >netsh firewall set opmode enable ဆိုပြီးပြန်ရိုက်ပေးလိုက်ရုံပါပဲ။

Window ရဲ့ Process List တွေကို TaskManager မဟုတ်တဲ့ နေရာကနေကြည့်မယ်

အခုပြောမယ့်အကြောင်းအရာကတော့ ကျွန်တော်တို့ GUI (Graphical User Interface)ဖြစ်တဲ့ Command Line Interface ကနေ သွားပြီး Window Background မှာ Run နေတဲ့ Porcess List ကိုကြည့် တဲ့နည်းဖြစ်ပါတယ်။ ဒီအနေအထားက ဘယ်လိုအနေအထားမှာ အထောက် အကူဖြစ် စေနိုင်သလည်းဆိုတော့ Window ကို Virus ကိုက်သွားတဲ့အနေအထားမှာ အရမ်းအသုံးဝင်မှာဖြစ်ပါတယ်။ ဘာလို့လည်းဆိုတော့ Virus Detected ဖြစ်သွားပီဆိုရင် အထူးသဖြင့် သူက Window ရဲ့ Taskmanager, Group Policy,Registry တွေကို လုံးဝကို Disabled လုပ်လိုက်မှာဖြစ်ပါတယ်။ ကျွန်တော်တို့ဆီမှာProcess hacker လိုမျိုး Portable ဖြစ်တဲ့ Process List ကြည့်နိုင်တဲ့ ကောင်လေး အဆင်သင့်ရှိနေရင်တော့ အကြောင်းမဟုတ်ပေမယ့် အဆင် သင့်မဖြစ် တဲ့အခါမျိုးမှာတော့ အခုပြောမယ့် နည်းလမ်းလေးက အရမ်းအသုံးဝင်မယ်လို့မျှော်လင့်ပါ တယ်။ ကဲ ပထမ တစ်မျိုးစလိုက်ရအောင် အရင်ဆုံးကျွန်တော်တို့က Keyboard ကနေပီးတော့ RUN Box ကိုခေါ်လိုက်မှာဖြစ်ပါ တယ်။ (Win+R) ထို့နောက်တော့ "cmd" လို့ရိုက်လိုက်ပါမယ်။ ဒါဆိုရင်တော့အောက်ပါပုံအတိုင်းပေါ်လာရင်



ကျွန်တော်တို့ထပ်ရိုက်ရမယ့် Command ကတော့ " tasklist" ဖြစ်ပါတယ်

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Anonymous>tasklist

Image Name                      PID Session Name        Session#    Mem Usage
=====
System Idle Process             0 Services             0           24 K
System                          4 Services             0          816 K
smss.exe                       304 Services             0          748 K
csrss.exe                      540 Services             0         2,988 K
csrss.exe                      620 Console              1          8,304 K
wininit.exe                    628 Services             0         3,232 K
services.exe                  676 Services             0         8,432 K
lsass.exe                     692 Services             0         7,252 K
lsm.exe                        700 Services             0         2,972 K
winlogon.exe                   756 Console              1          6,916 K
svchost.exe                   844 Services             0         6,460 K
DFServ.exe                    896 Services             0         6,200 K
svchost.exe                    964 Services             0         6,832 K
atiesrxx.exe                  1028 Services            0         2,940 K
svchost.exe                   1104 Services             0        12,176 K
svchost.exe                   1192 Services             0        49,668 K
svchost.exe                   1216 Services             0        22,668 K
audiodg.exe                   1296 Services             0        19,856 K
```

ဒီလိုဆိုရင် သူက Window ရဲ့ နောက်ခံမှာ Run နေမယ့် Process တွေအကုန်လုံးကိုဖော်ပြပေးမှာဖြစ်ပါတယ်။ ဒါဆိုရင် ကျွန်တော်တို့က ဥပမာ Virus Process တစ်ခုခုကို ပိတ်ချင်တဲ့အခါမှာရိုက်ရမယ့် Command ကတော့ “taskkill /f /im PROCESS.EXE /t” ဖြစ်ပါတယ်

```
Administrator: C:\Windows\system32\cmd.exe

wmplayer.exe                   956 Console              1       37,684 K
OSPPSUC.EXE                   1328 Services             0         5,808 K
OSPPSUC.EXE                   2360 Services             0         3,752 K
conhost.exe                   2908 Services             0         2,300 K
OSPPSUC.EXE                   3736 Services             0        11,596 K
PDFXCview.exe                 2320 Console              1        28,012 K
WINWORD.EXE                   3768 Console              1       52,480 K
SearchProtocolHost.exe        2728 Services             0         6,640 K
SearchFilterHost.exe          988 Services             0         6,776 K
cmd.exe                       1156 Console              1         2,468 K
conhost.exe                   3928 Console              1         4,056 K
tasklist.exe                  3780 Console              1         4,268 K
WmiPrvSE.exe                   852 Services             0         4,696 K

C:\Users\Anonymous>taskkill /f /im wmplayer.exe /t_
```

အပေါ်မှာပြထားတဲ့ Command မှာ PROCESS.EXE ဆိုတာကတော့ မိမိက ရပ်ချင်တဲ့ Process ရဲ့ နာမည်ကို ဆိုလိုတာဖြစ်ပါတယ်။ အခုကျွန်တော်က ဥပမာအနေနဲ့ WindowMedia Player ကို ပိတ်တာ ကိုရိုက်လိုက်ပါ တယ်။ ဒီနေရာမှာကျွန်တော်တစ်ခုပြောချင်တာကတော့ taskkill ဆိုတာကတော့ လက်ရှိ Run နေတဲ့ Process ကို ပိတ်ချင်တာဖြစ်ပြီးတော့ /f ဆိုတာကတော့ Force ကိုရည်ညွှန်းတာဖြစ်ပါတယ်။ နောက်တစ်ခုကတော့/im ဆိုတာကလည်း Image ဆိုတာကိုရည်ညွှန်းတာဖြစ်ပါတယ်။ ဆိုလိုတာကတော့ တစ်ခြား Process Area တွေမှာ ၎င်း Process က Run နေမယ်ဆိုရင်လည်း ၎င်းကိုပိတ်ဖို့ အတွက် ရည်ညွှန်းတာ ဖြစ်ပါတယ်။ ဒီနောက်နေရာဖြစ်တဲ့ wmplayer.exe ဆိုတာကတော့ Window Media Player အလုပ်လုပ်နေတဲ့ Process Name ဖြစ်ပါတယ်။ဒီကောင်ကိုပိတ်ချင်တဲ့အတွက်ကြောင့် ကျွန်တော် တို့က wmplayer.exe ဆိုပြီးရိုက်လိုက် တာဖြစ်ပါတယ်။ နော်ကဆုံးတစ်ခုဖြစ်ပါတယ်။ကတော့ /t ဖြစ်ပါ တယ်။ သူကတော့ Terminated ဆိုတာ ဖြစ်ပါတယ်။ သူကတော့ ဘယ်နေရာတွေ ဘယ်လိုတွေပဲ အလုပ် လုပ်နေပစေ လုံးဝဖြတ်တောက် ပြစ်မယ်လို့ပြောတာဖြစ်ပါတယ်။ ဒီလောက်ဆိုရင်တော့ သာမန် Command Line ကနေ Process List နဲ့ Process Kill လုပ်တဲ့ အကြောင်းကို အကြမ်းဖျဉ်း သိ လောက် ပီလို့ ယူစပါရစေ။ မရှင်းလင်းတာများကိုလည်း ကျွန်တော်ကို ဆက်လက်မေးမြန်းနိုင်ပါတယ်။ အခုနောက် တစ်ခုပြောမှာဖြစ်ပါတယ်။ သူကတော့ WMIC Command ဖြစ်ပါတယ်။ဒီ Command ကတော့ အသေးစိတ်လေ့လာမယ်ဆိုရင် နည်းနည်းကြမ်းတယ်ပျ ကျွန်တော်အချိန်ရရင်လည်း ဒီ Command အကြောင်းလေးကို အသေးစိတ်ပြောပြချင်ပါသေးတယ်။ သူက ဘယ် လောက်ထိစွမ်းသ လည်းဆိုရင် Hardware တွေကိုတောင် ကမောက်ကမဖြစ်အောင်လုပ်နိုင်တယ်လို့ စာဖတ်ဖူးပါတယ်။ :P ကဲဆက်လိုက် ရအောင်ဗျာ နောက်ထပ် Process List ကိုကြည့်ဖို့နည်းကတော့ သာမန် ကျွန်တော်တို့ CMD ကိုခေါ် လိုက်ပါမယ်။ဒါဆိုရင်တော့အောက်ပါပုံအတိုင်းပေါ်လာပါမယ်။


```
Administrator: C:\Windows\system32\cmd.exe - wmic
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Anonymous>wmic
wmic:root\cli>
```

ဒီအချိန်မှာ လုံးဝကို kernel Mode ထဲကိုဝင်သွားတာဖြစ်ပါတယ်။ ပီးနောက်ထပ်ရိုက်ရမယ့် Command ကတော့ process ဆိုတာဖြစ်ပါတယ်။

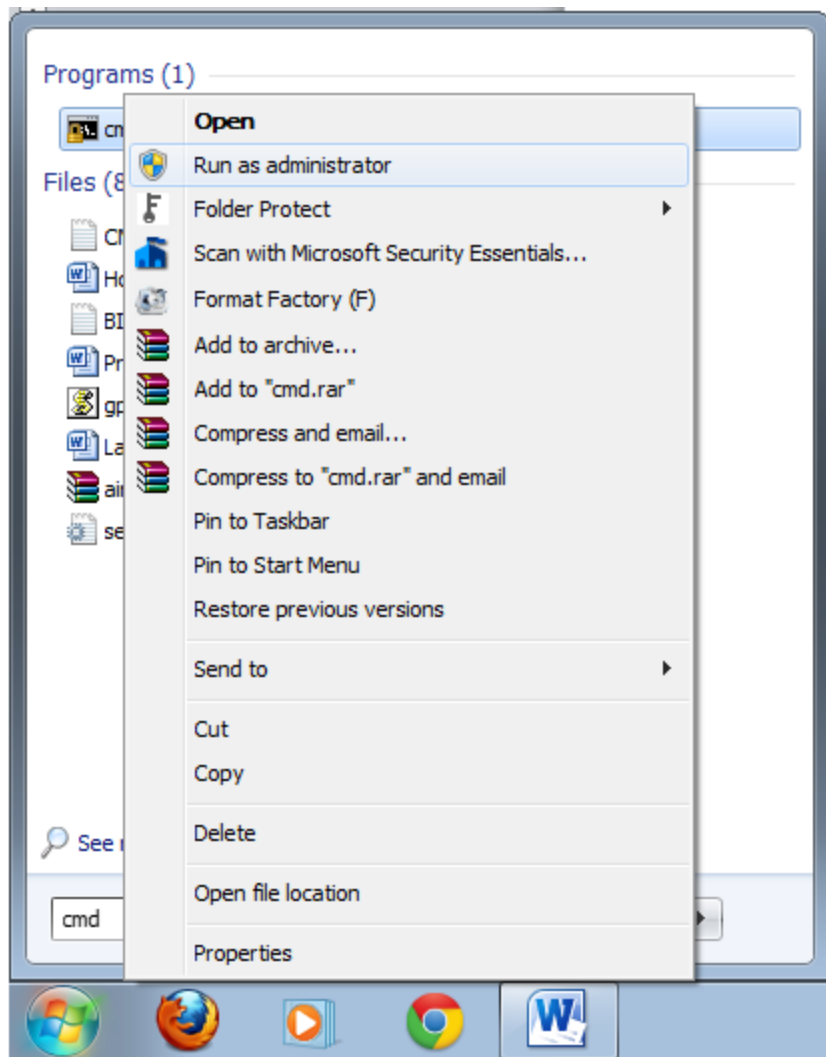
```
Administrator: C:\Windows\system32\cmd.exe - wmic
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Anonymous>wmic
wmic:root\cli>process
Caption                               CommandLine
System Idle Process
System
smss.exe
csrss.exe
csrss.exe
wininit.exe
services.exe
lsass.exe
lsass.exe
lsass.exe
winlogon.exe
svchost.exe
DFSServ.exe
svchost.exe
atiesrxx.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
audiodg.exe
svchost.exe
```

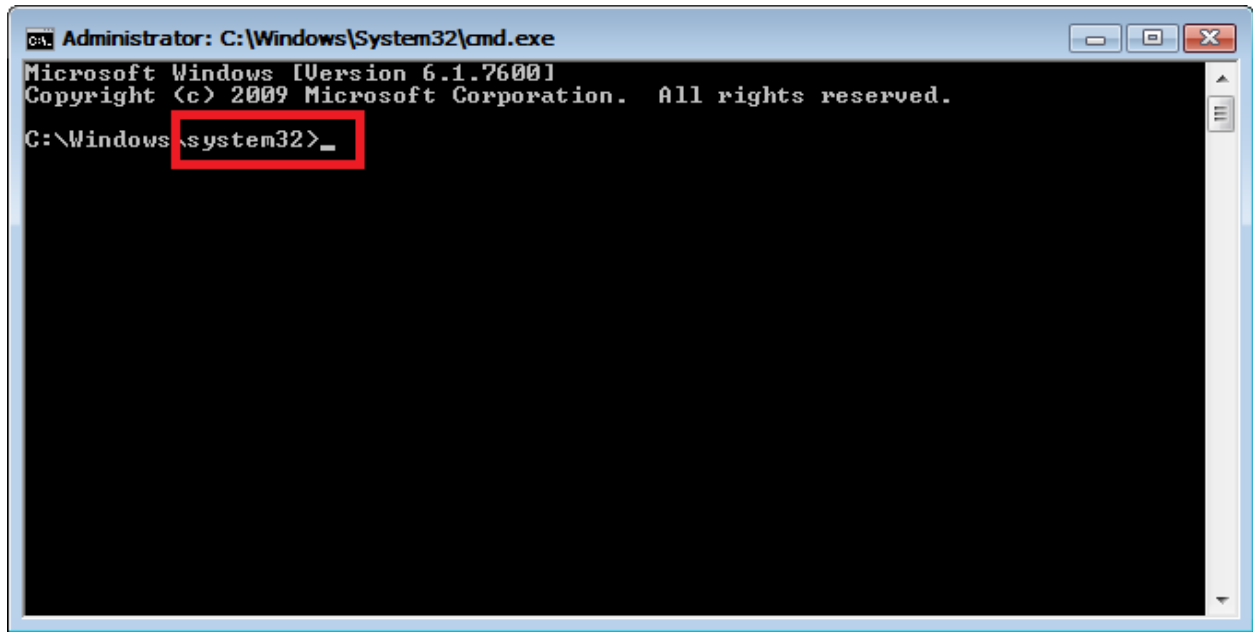
အထက်ပါပုံအတိုင်းရိုက် လိုက်မယ်ဆိုရင်တော့ သူက လက်ရှိ Wwindow မှာ Runနေသမျှ Process အားလုံး ကို ဖော်ပြပေးမှာဖြစ်ပါတယ်။

Shortcut Virus ကို Command Line ကနေသတ်မယ်

Shortcut Virus ကို Remover ဖြင့် အလွယ်တကူသတ်လို့ရနိုင်ပါတယ်။ ဒါပေမယ့် ကျွန်တော်ကတော့ ကျွန်တော်ကြုံတွေ့ရတဲ့ Customer Site ထဲမှ အဖြစ်အပျက်များ ဇာတ်လမ်းသွားအ ရနည်းနည်းတော့ရှင်း ပြချင်ပါသေးတယ်။ ဒီလိုမျှ တစ်ရက် ကျွန်တော် Services အတွက် Customer Site နှစ်ခုကို Run ပီးတော့ အပြန် နောက်ထပ်စိုက်ခံတစ်ခုက အရေးကြီးလို့ ဖုန်းလှမ်းဆက်ခေါ်တော့ကျွန်တော် ရောက်သွား တယ် ဟို ရောက်တော့ External Stick တွေအကုန်လုံးမှာ Shortcut Virus တွေဝင်နေ တာကိုတွေ့ လိုက် တယ်။ အို..... လွယ်လွယ်လေးပေါ့ ဆိုပီး ကျွန်တော်လည်းရှိသမျှ Stick တွေထုတ် လိုက် တယ်။ ကံဆိုးတာ က Shortcut Virus Remover က မရှိတော့ဘူး ကျွန်တော်ပျောက်သွားတဲ့ Stick ထဲ ပါသွားတယ်။ ဒါနဲ့ ဖုန်းထဲကနေအင်တာနက်ဖွင့်ပီးတော့ဒေါင်းမယ်လုပ်ပြန်တော့လည်းကျွန်တော်ချစ်သောမြန်မာ့ ဆက်သွယ် ရေးက ကော်နပ်ရှင်ကျနေ တယ် ဒါနဲ့ လာထားအာဘွားအဲလေ.. ဓာတ်ရှင်ကားတွေနဲ့ မှားကုန်ပီ။။ လာထားဆိုပီး Command Line ထဲကနေသတ်မယ်ဆိုပီး Customer ဆီမှာရှိသမျှ Stick တွေအကုန်လုံး ကိုထိုးပလိုက်တယ်။ ပီးတော့အောက်ပါ ပုံအတိုင်းမှ

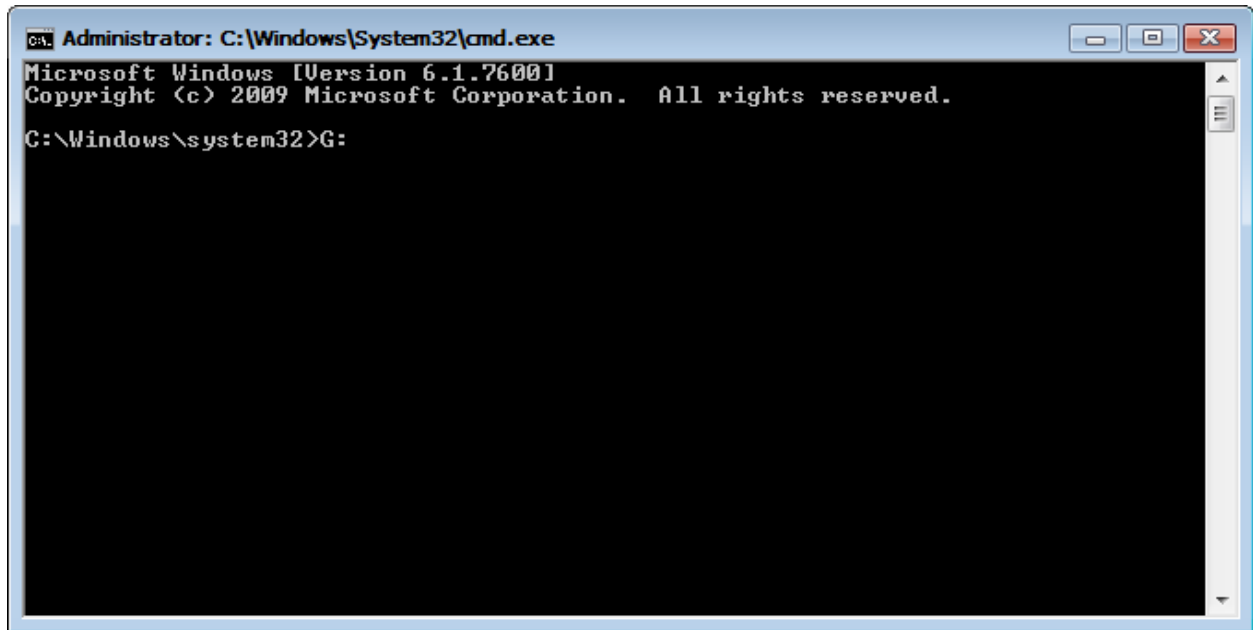


Start ထဲမှာ "cmd" လို့ရှိက်မီး Right Click ထောက် Run as administrator အနေဖြင့် ဖွင့်လိုက်ပါတယ်။



```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>
```

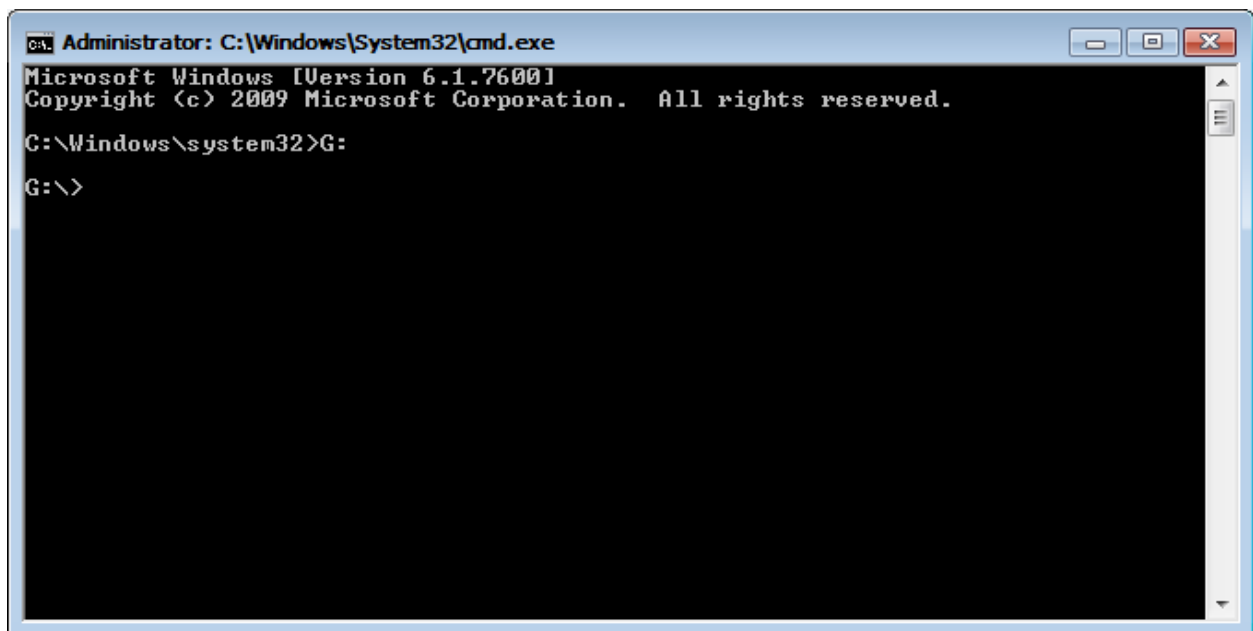
ဒီနေရာမှာတစ်ခုပြောချင်တာက ပုံမှန် Run Box ထဲကနေ "cmd" လို့ရိုက်ရင် သူက User Level အနေဖြင့် သွားပီး User Location ကိုပဲပြမှာဖြစ်ပါတယ်။ အခုကျွန်တော်တို့က Run as administrator အနေဖြင့် သွားထား တဲ့အတွက်ကြောင့် System Location ကိုပြနေတာဖြစ်ပါတယ်။ ဘာကွာသလည်းဆိုတော့ သင်ဟာ သာမန် run box ထဲကနေသာရိုက်လိုက်ရင် နောက်ပိုင်းလုပ် ဆောင်ချက်တွေကို ဘာမှလုပ်လို့ရမှာ မဟုတ် တော့ လို့ပါကဲဆက်သွားရအောင်ဒီနောက်တော့ Shortcut Virus ဝင်နေတဲ့ Stick ရဲ့ Drive Letter ကိုရိုက် ထည့် လိုက်ပါမယ်။



```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>G:
```

ကျွန်တော့်ဆီမှာဝင်နေတာက Drive Letter G ပါ ဒါကြောင့် G: ဟုရိုက်လိုက်ပါတယ်။ ပီးနောက် Enter ကိုနှိပ်လိုက်ပါတယ်။ထိုအခါအမှာတော့အောက်ပါအတိုင်း သင့် Stick ထဲကိုရောက်သွားပါပီ။



```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>G:
G:\>
```

ထိုအခါ သင်အရင်ဆုံးရိုက်ရမယ့် Command က >del *.lnk /s/f/a ဆိုပီးတော့ဖြစ်ပါတယ်။ အောက်ပါပုံအတိုင်းပေါ့...

```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>G:
G:\>del *.lnk /s/f/a
```

ပီးရင်တော့ Enter ကိုနှိပ်လိုက်ပါ ဒါဆိုရင် သင့် Stick ထဲမှာရှိသမျှ Shortcouteတွေအကုန်လုံးကို ဖျက်ပလိုက် ပါမယ်။ထိုနောက် ထပ်မံရိုက်ရမယ့် Command ကတော့ >del *.tmp /s/f/a ဖြစ်ပါတယ်။ ဒါကတော့ တစ်ခါတည်း TEMP ဖိုင်တွေကိုပါဖျက်ပလိုက်တာပါ။ နောက်တစ်ခါထပ်ရိုက်ရမှာကတော့>del *.db /s/f/a ဖြစ်ပါတယ် သူလည်း Temporary တွေကိုဖျက်ပလိုက်တာပါ။ဒီလိုမျိုးတွေ ဖျက်ပီးသွားပီဆိုရင်တော့ သင့် Stick ထဲမှာ Hidden ဖြစ်နေတဲ့ ဖိုင်တွေကိုဖော်ဖို့အတွက် ရိုက်ရမယ့် Command ကတော့>attrib -s -h -r *.* ဆိုပီးအရင်ရိုက်လိုက်ပါမယ်။ ဒါကတော့ ဖိုင်တွေကိုဖော်ဖို့အတွက် ဖြစ်ပါတယ်။ ထို့နောက်တော့ >dir /ah ဆိုပီးရိုက်လိုက်တဲ့ အခါမှာတော့ ပျောက်နေတဲ့ Folder တွေကို အစဉ်လိုက်ဖော်ပြပေးပါမယ်။ ၎င်းဖိုလ်ဒါနာ မည်တွေကိုမှတ်သားပီးတော့ ပြန်ဖော်ရမယ့် Command က>attrib -s -h -r [Folder Name] ဖြစ်ပါတယ် Foler Name ဆိုတာက တော့သင် dir /ah လို့ရိုက်လိုက်တဲ့အချိန်မှာဖော်ပြပေးတဲ့ Folder Listတွေထဲ ကဖြစ်ပါတယ်။ ကဲ ဒီလောက်ဆိုရင် အဆင်ပြေလောက်မယ်လို့မျှော်လင့်ကြည့်ပါတယ်။ ဒီ Post မှာ ကျွန်တော် တစ်ခု ထူးခြား အောင်လုပ်ထားပါတယ်။ အဲဒါကတော့ နောက်ပိုင်းပုံတွေကိုဆက်မထည့်ထားတာပါ။ ကျွန်တော့ ကိုအားပေးတဲ့ ကျွန်တော့ စာဖတ် ပရိတ်သတ်ရဲ့ နားလည်နိုင်မှုစွမ်းရည်လေးကို သိချင်လို့ပါ အဆင်မပြေ ဘူးဆိုရင် အချိန်မရွေးမေးမြန်းနိုင်ပါတယ်။ စာမေးလို့ ဘယ်တော့မှစိတ်မဆိုးတတ်ပါဘူး

ကျွန်တော့်ကို အသက် မေးရင်သာ စိတ်ဆိုးတာပါ။ ကျွန်တော်က အခုမှ ၁၈ နှစ်တောင်မပြည့် သေးပါ ဘူးခင်ဗျာ....

Batch File ကို Command Line ထဲကနေဘယ်လိုရေးမလည်း

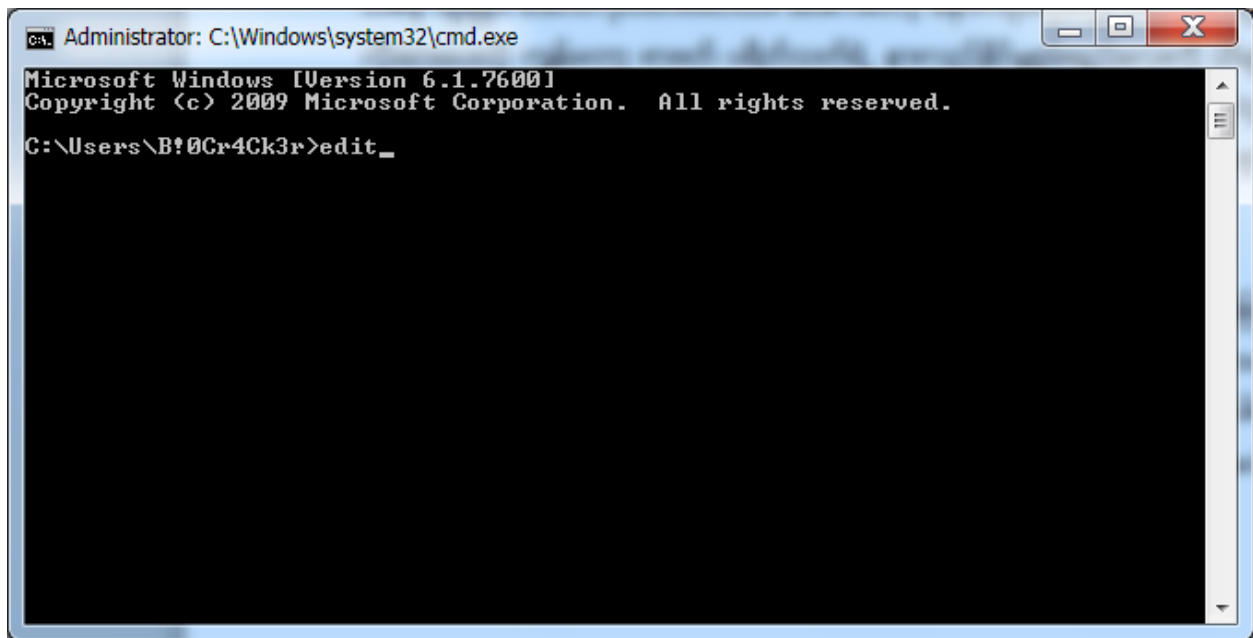
လွယ်ပါတယ်။အခုပြောမယ့် Level ကို ကျွန်တော်က အမြင့်ပိုင်း Level သမားအဖြစ်သတ်မှတ်လိုက်ပါမယ်။ ဘာလို့လည်းဆိုတော့ Batch File Programming ကိုအနည်းနဲ့ အများသိထားတယ် လို့ပဲ သတ်မှတ် လိုက်ပါ သည်။ပုံမှန်ဆိုရင် Batch File Programming ကို Notepad ထဲကနေရေး တာများပါတယ်။ အခု ကျွန်တော်က သူများနဲ့မတူအောင် Command Prompt ထဲကနေရေးပြီး လုပ်ဆောင်တာကိုပြမယ်။ ဥပမာ တစ်ခုအနေနဲ့ ကျွန်တော်က

@echo off

Shutdown -s -t 300

Msg * your computer has been hacked by B!0Cr4Ck3r

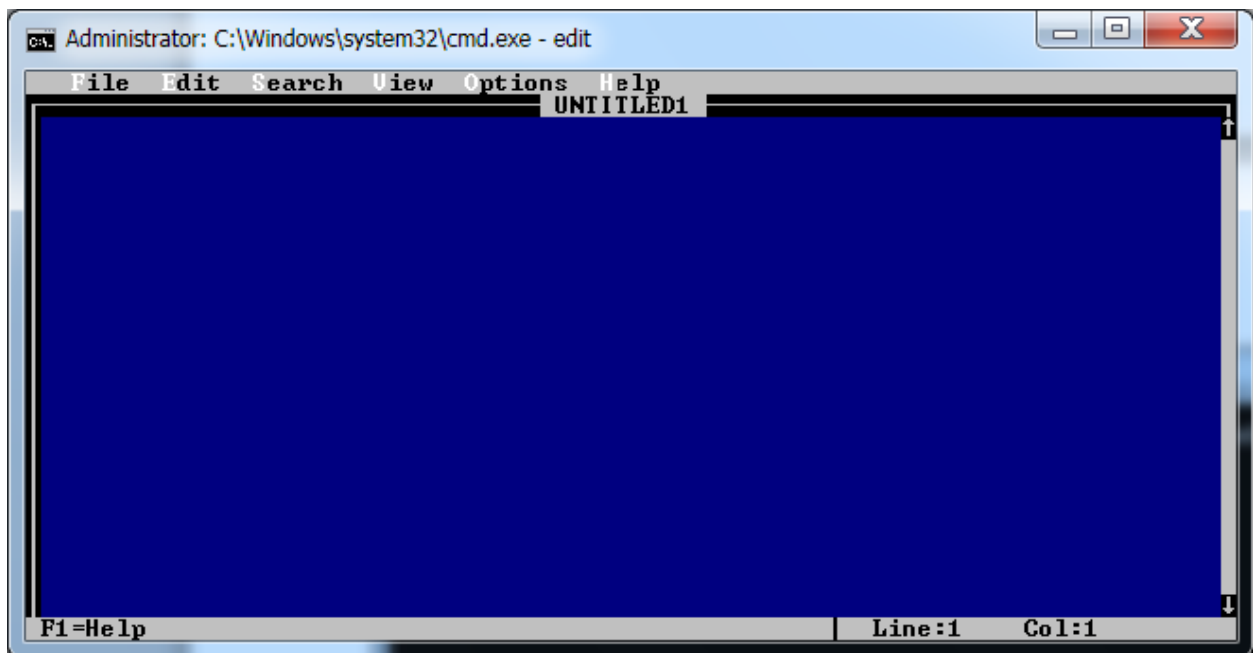
ဆိုတဲ့ ဟာလေးကို ပုံမှန်ဆိုရင် Notepad ထဲမှာကူးထည့်ပြီး *.bat အဖြစ်သိမ်းဆည်းရပါတယ်။ သို့ပေ သော်လည်း ကျွန်တော်က Comman Prompt ကိုဖွင့်လိုက်ပါပြီ



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

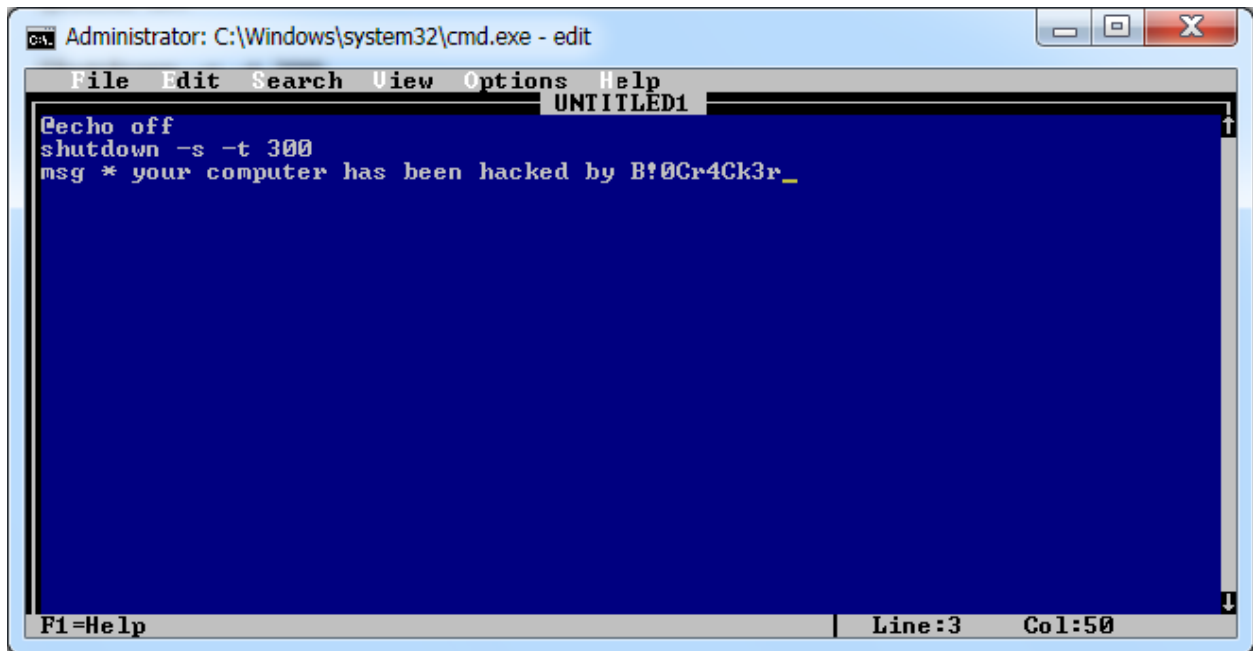
C:\Users\B!0Cr4Ck3r>edit_
```

ထို့နောက်အထက်ပါပုံအတိုင်း **edit** ဆိုတာကိုရိုက်လိုက်ပါတယ်။ ဒါဆိုရင်တော့အောက်ပါပုံအတိုင်း

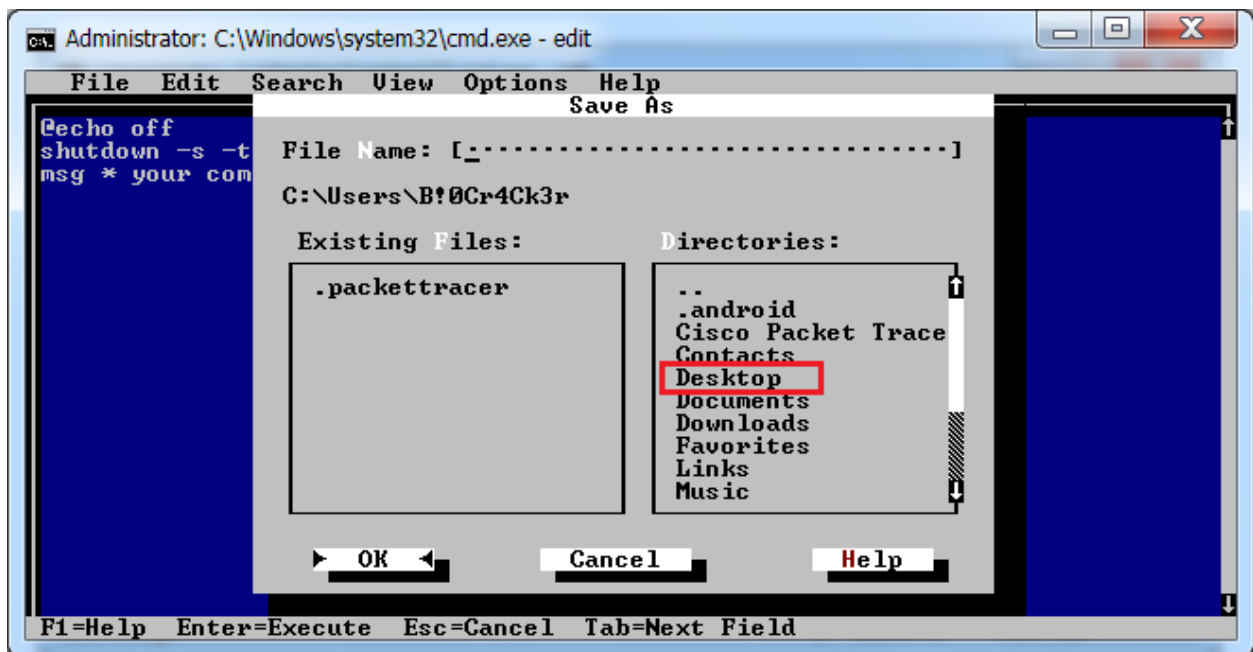


```
Administrator: C:\Windows\system32\cmd.exe - edit
File Edit Search View Options Help
UNTITLED1
F1=Help | Line:1 Col:1
```

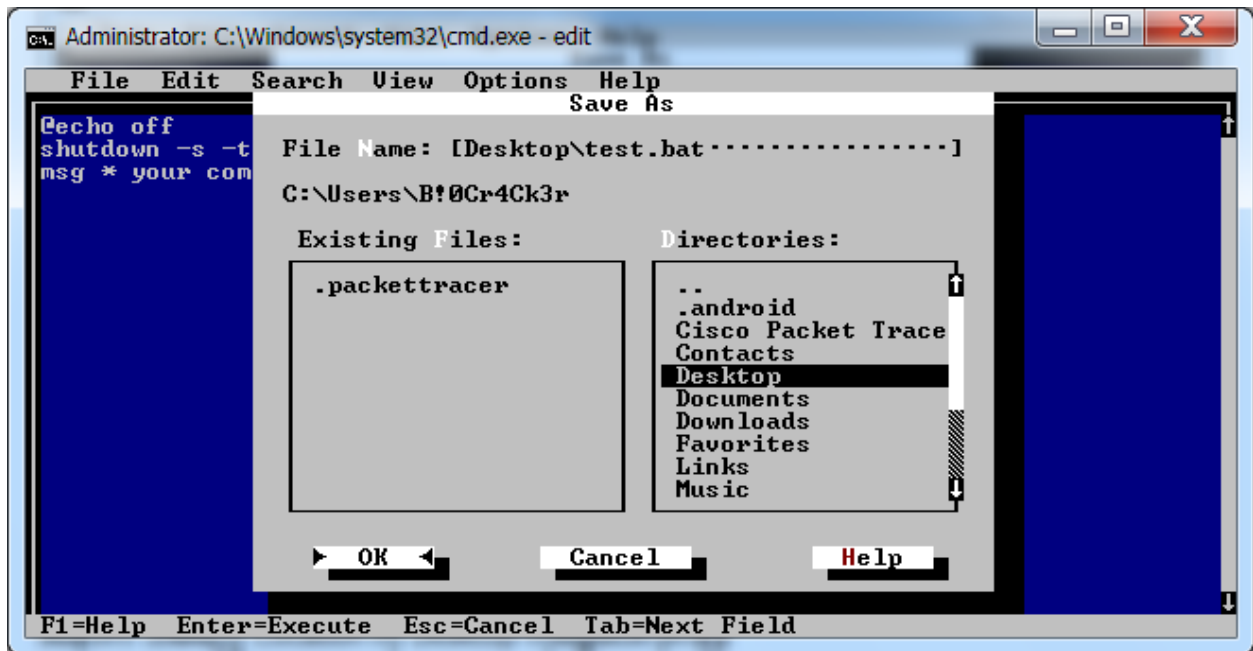
ပေါ်လာပါပြီ ဒါဆိုရင် ခုနက Code တွေကိုအဲဒီထဲမှာရိုက်ပါမယ်။



ထို့နောက် Alt + F + S ကိုနှိပ်လိုက်ပါမယ်။



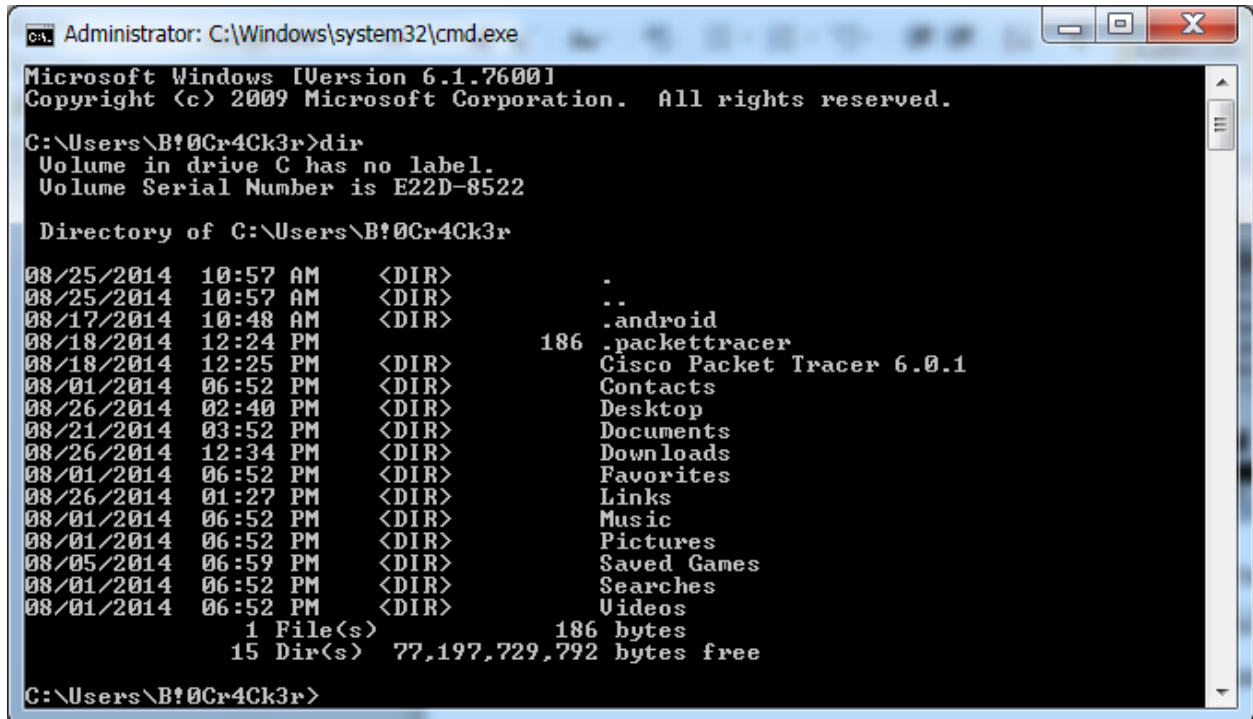
ဒီနောက် သိမ်းမည့် Location ကို Desktop ကိုရွေးပေးလိုက်ပြီး



ဖိုင်နာမည်ကိုတော့မိမိစိတ်ကြိုက်ပေးနိုင်ပါတယ် ကျွန်တော်ကတော့ test.bat ဆိုပြီးပေးပြီး Save လုပ်လိုက် ပါတယ်။ ထို့နောက်တော့ Alt + F + X ကိုနှိပ်ပြီးထွက်လိုက်ပါတယ်။ ဒါဆိုရင်တော့ သင့်ရဲ့ Desktop ပေါ်မှာ test.bat ဆိုတဲ့ဖိုင်လေးရောက်နေပါမယ်။ ကဲဒီလောက်ဆိုအဆင်ပြေမယ်ထင်ပါတယ်။

" dir "

Dir ဆိုတာကတော့ Directory (Folder) ကိုခေါ်ဆိုခြင်းဖြစ်ပါတယ်။သူ့ကိုဘယ်လိုသုံးရသလည်းဆိုတော့ ကျွန်တော်တို့ Command Prompt ထဲမှာ



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\B!\0Cr4Ck3r>dir
Volume in drive C has no label.
Volume Serial Number is E22D-8522

Directory of C:\Users\B!\0Cr4Ck3r

08/25/2014  10:57 AM    <DIR>          .
08/25/2014  10:57 AM    <DIR>          ..
08/17/2014  10:48 AM    <DIR>          .android
08/18/2014  12:24 PM             186 .packettracer
08/18/2014  12:25 PM    <DIR>          Cisco Packet Tracer 6.0.1
08/01/2014  06:52 PM    <DIR>          Contacts
08/26/2014  02:40 PM    <DIR>          Desktop
08/21/2014  03:52 PM    <DIR>          Documents
08/26/2014  12:34 PM    <DIR>          Downloads
08/01/2014  06:52 PM    <DIR>          Favorites
08/26/2014  01:27 PM    <DIR>          Links
08/01/2014  06:52 PM    <DIR>          Music
08/01/2014  06:52 PM    <DIR>          Pictures
08/05/2014  06:59 PM    <DIR>          Saved Games
08/01/2014  06:52 PM    <DIR>          Searches
08/01/2014  06:52 PM    <DIR>          Videos
               1 File(s)              186 bytes
              15 Dir(s)  77,197,729,792 bytes free

C:\Users\B!\0Cr4Ck3r>
```

Dir လိုက်ရှိုက်လိုက်တယ်ဆိုရင် လက်ရှိရောက်နေတဲ့ Location ထဲက ဖိုင်တွေကိုကြည့်ချင် သုံးရတာဖြစ်ပါတယ်။ Linux မှာဆိုရင်တော့ " ls " ပေါ့.....။ dir မှာပဲ Hidden တွေကိုပြစေချင်တယ်ဆိုရင် "dir /ah" ဆိုပြီး

```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\B!0Cr4Ck3r>dir /ah
Volume in drive C has no label.
Volume Serial Number is E22D-8522

Directory of C:\Users\B!0Cr4Ck3r

08/01/2014  06:52 PM    <DIR>          AppData
08/01/2014  06:52 PM    <JUNCTION>     Application Data [C:\Users\B!0Cr4Ck3r\AppData\Roaming]
08/01/2014  06:52 PM    <JUNCTION>     Cookies [C:\Users\B!0Cr4Ck3r\AppData\Roaming\Microsoft\Windows\Cookies]
08/01/2014  06:52 PM    <JUNCTION>     Local Settings [C:\Users\B!0Cr4Ck3r\AppData\Local]
08/01/2014  06:52 PM    <JUNCTION>     My Documents [C:\Users\B!0Cr4Ck3r\Documents]
08/01/2014  06:52 PM    <JUNCTION>     NetHood [C:\Users\B!0Cr4Ck3r\AppData\Roaming\Microsoft\Windows\Network Shortcuts]
08/26/2014  03:13 PM             1,835,008 ntuser.dat
08/26/2014  03:13 PM             262,144 ntuser.dat.LOG1
08/01/2014  06:52 PM              0 ntuser.dat.LOG2
08/01/2014  06:57 PM             65,536 NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0b
cd1824}.TM.blf
08/01/2014  06:57 PM             524,288 NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0b
cd1824}.TMContainer000000000000000001.regtrans-ms
08/01/2014  06:57 PM             524,288 NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0b
cd1824}.TMContainer000000000000000002.regtrans-ms
08/13/2014  10:26 PM             65,536 ntuser.dat{7222ae4f-22f6-11e4-ae35-74e543
00c19b}.TM.blf
```

ရိုက်မယ်ဆိုရင်ဖြစ်ပြီးအကယ်လို့များ များတယ်ဆိုရင် "dir /ah /p" လို့ရိုက်ရင်

```
Administrator: C:\Windows\system32\cmd.exe - dir /ah /p

Volume Serial Number is E22D-8522

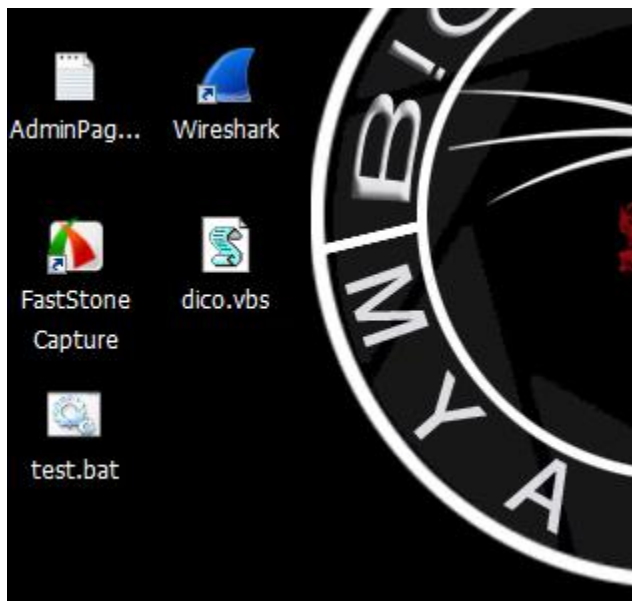
Directory of C:\Users\B!0Cr4Ck3r

08/01/2014  06:52 PM    <DIR>          AppData
08/01/2014  06:52 PM    <JUNCTION>     Application Data [C:\Users\B!0Cr4Ck3r\AppData\Roaming]
08/01/2014  06:52 PM    <JUNCTION>     Cookies [C:\Users\B!0Cr4Ck3r\AppData\Roaming\Microsoft\Windows\Cookies]
08/01/2014  06:52 PM    <JUNCTION>     Local Settings [C:\Users\B!0Cr4Ck3r\AppData\Local]
08/01/2014  06:52 PM    <JUNCTION>     My Documents [C:\Users\B!0Cr4Ck3r\Documents]
08/01/2014  06:52 PM    <JUNCTION>     NetHood [C:\Users\B!0Cr4Ck3r\AppData\Roaming\Microsoft\Windows\Network Shortcuts]
08/26/2014  03:13 PM             1,835,008 ntuser.dat
08/26/2014  03:13 PM             262,144 ntuser.dat.LOG1
08/01/2014  06:52 PM              0 ntuser.dat.LOG2
08/01/2014  06:57 PM             65,536 NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0b
cd1824}.TM.blf
08/01/2014  06:57 PM             524,288 NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0b
cd1824}.TMContainer000000000000000001.regtrans-ms
08/01/2014  06:57 PM             524,288 NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0b
cd1824}.TMContainer000000000000000002.regtrans-ms
08/13/2014  10:26 PM             65,536 ntuser.dat{7222ae4f-22f6-11e4-ae35-74e543
00c19b}.TM.blf
08/13/2014  10:26 PM             524,288 ntuser.dat{7222ae4f-22f6-11e4-ae35-74e543
00c19b}.TMContainer000000000000000001.regtrans-ms
Press any key to continue . . .
```

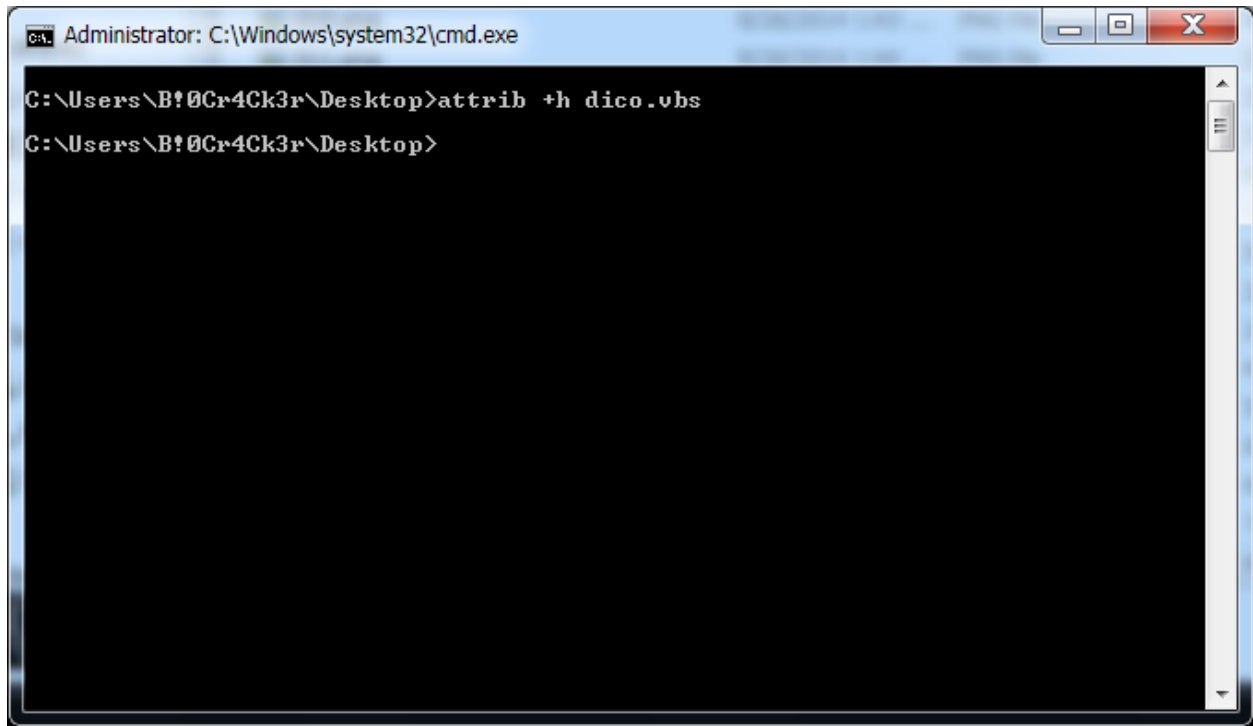
Pause လုပ်ပြီး ဖော်ပြပေးမှာဖြစ်ပါတယ်။ နောက်ထပ်ဟာတွေကြည့်ချင်ရင်တော့ Press any key to continue... ဆိုတဲ့အတွက်ကြောင့် ခလုတ်တစ်ခုခုကိုနှိပ်ပြီးဆက်ဖတ်နိုင်ပါတယ်။ သူနဲ့ တွဲပြီးရှိက်တဲ့ Parameter တွေကတော့ /b , /c , /d , /l , /n , /o , /q , /q , /r , /s တို့ဖြစ်ပါတယ်။ဒါတွေကို တော့ မိမိဘာသာပဲစမ်းသပ်ကြည့်ပါနော်....

“attrib”

Attrib ဆိုတာကတော့ attribute command ပဲဖြစ်ပါတယ်။ သူ့ကိုကတော့ ဖိုင်တွေကိုဖော်ချင်တာ ဖွက်ချင်တာတွေလုပ်ဆောင်တဲ့အခါမှာအဓိကသုံးပါတယ်။ ကဲလက်တွေ့ကြည့်ရအောင် ကျွန်တော်တို့က Desktop Location ကနေပဲပြမယ်ဗျာ



အထက်ပါပုံအတိုင်း မှာ ကျွန်တော်က disco.vbs ဆိုတဲ့ဖိုင်ကိုဖွက်ချင်တယ်ဆိုပါစို့။ ရှိက်ရမယ့် Command က



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\B!0Cr4Ck3r\Desktop>attrib +h disco.vbs
C:\Users\B!0Cr4Ck3r\Desktop>
```

>**attrib +h disco.vbs** ဆိုပြီးတော့ဖြစ်ပါတယ် ဒါဆိုရင် သင့်ရဲ့ disco.vbs ဆိုတဲ့ဖိုင်က Hidden ဖြစ်သွား ပါလိမ့်မယ်။ ပြန်ဖော်ချင်တယ်ဆိုရင်တော့ >**attrib -h disco.vbs** ဆိုပြီးရိုက်လိုက်ရင်ရပါတယ်။ ဒီနေရာမှာ အဓိပ္ပာယ်တော်ပြောမယ်။ ၎င်း attrib နှင့်တွဲတဲ့ Parameter တွေပဲဖြစ်ပါတယ်။

+ = Set an attribute

- = Clears an attribute

R = Read-only file attribute

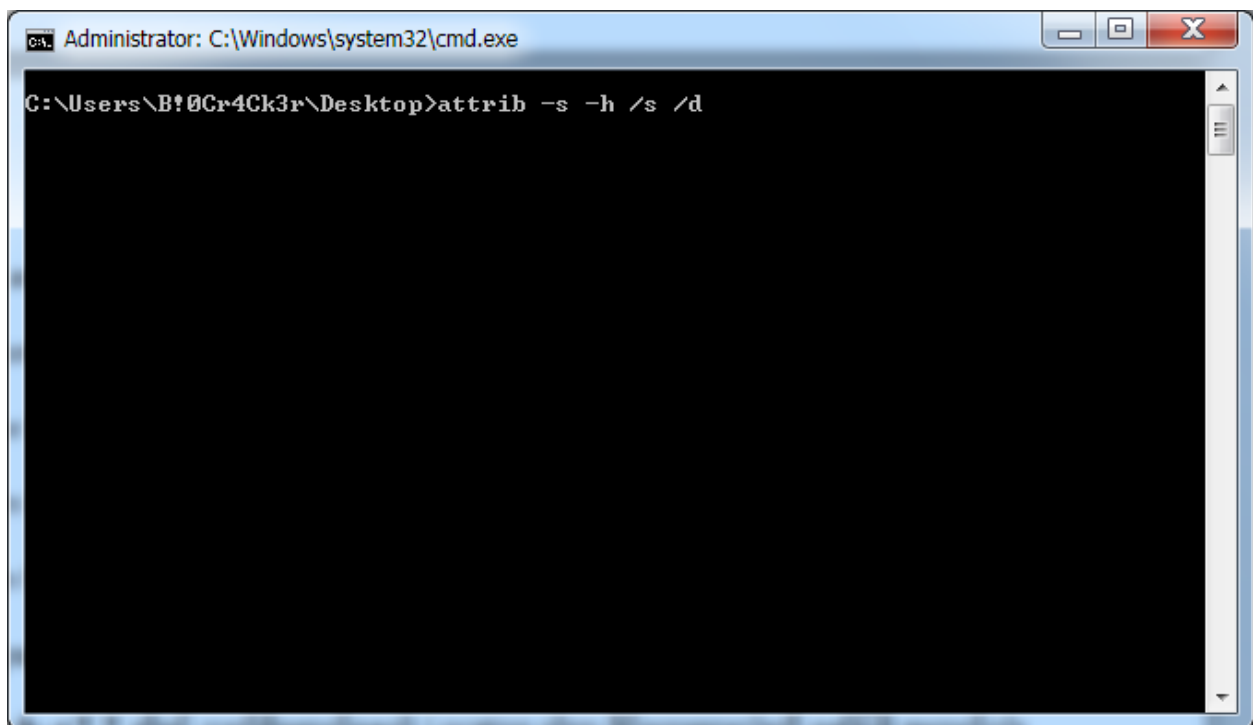
A = Archive file attribute

S = System file attribute

H = Hidden file attribute

တွေကတော့အဓိကပေါ့။ အဲ သူနဲ့ အများဆုံးတွဲပြီးကျွန်တော်သုံးတဲ့ Command တွေကတော့

>attrib -s -h -r *.* ဆိုရင် လက်ရှိရောက်နေတဲ့ Location ထဲက ဖိုင်တွေအားလုံးကို ဖော်ပြဖို့အတွက်သုံး တာဖြစ်ပါတယ်။ ဒီနေရာမှာတစ်ခုပြောချင်တာက ဖိုင်နဲ့ ဖိုဒါလုံးဝမတူပါဘူး ဆိုတာ ကိုမှတ်ထားရပါမယ်။ အကယ်လို့များ သင်ဟာလက်ရှိရောက်နေတဲ့ Location မှာ ဖိုင်တွေကော၊ ဖိုဒါတွေကော Hidden ဖြစ်နေလို့ ဒီ Command ကိုသုံးမယ်ဆိုရင် File တွေပဲ ပေါ်မှာဖြစ်ပြီး Folder တွေ ပေါ်မှာမဟုတ်ပါဘူး။ အကယ်လို့များ သင်ဟာ ဖိုင်တွေကော၊ ဖိုဒါတွေကော တစ်ပြိုင်နက်တည်း ပေါ်ချင် တယ်ဆိုရင်တော့ရိုက်ရမယ့် Command က

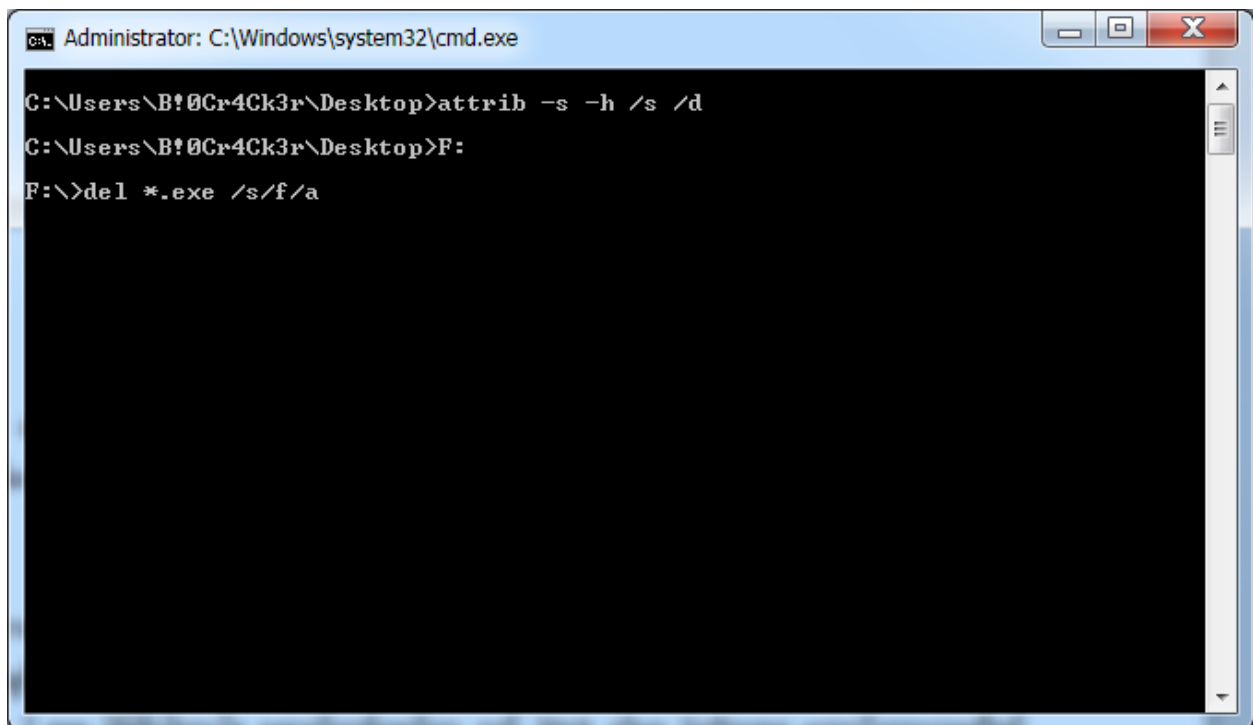


```
C:\Users\B!0Cr4Ck3r\Desktop>attrib -s -h /s /d
```

အထက်ပါပုံအတိုင်းမှ >attrib -s -h /s /d ဆိုပြီးတော့ဖြစ်ပါတယ်။ ဒီ Command ကို အထူးသဖြင့် ကျွန်တော် သုံးတာကတော့ Memory Stick ထဲမှာ ဖိုင်တွေပျောက်သွားတယ်လို့ ပြောကြ တဲ့ သူ တွေနဲ့တွေ့ရင် အများဆုံး သုံးပါတယ်။ ဆိုလိုတာက Shortcut Virus ကိုကံသွားတယ်ဆိုရင် ဒီ Command ကိုသုံးခြင်းဖြင့် ရှိသမျှ ဖိုင်တွေ၊ ဖိုဒါတွေအကုန်လုံးပေါ်လာမှာဖြစ်ပါတယ်။

" del "

Del ဆိုတာကတော့ Delete Command ပဲဖြစ်ပါတယ်။ ကီးဘုတ်က Del Key ပေါ့ဗျာ.... သူ့မှာကတော့ Virus တွေကိုဖျက်ချင်တဲ့အခါမှာ ဆိုလိုတာက သင့်ရဲ့ Memory Stick ထဲမှာ Virus ကိုက်နေတယ်ပေါ့ဗျာ။ Virus ဆိုတာကတော့ *.exe ပဲဖြစ်ပါတယ်။ နောက်တစ်ချက်က သင့် Stick ထဲမှာ Software မထည့်ထားဘူးဆိုရင် တော့ရိုက်ရမယ့် Command က သင့်ရဲ့ Drive Letter ထဲကိုအရင်ဆုံးဝင်ထားပါပြီးသွားရင်



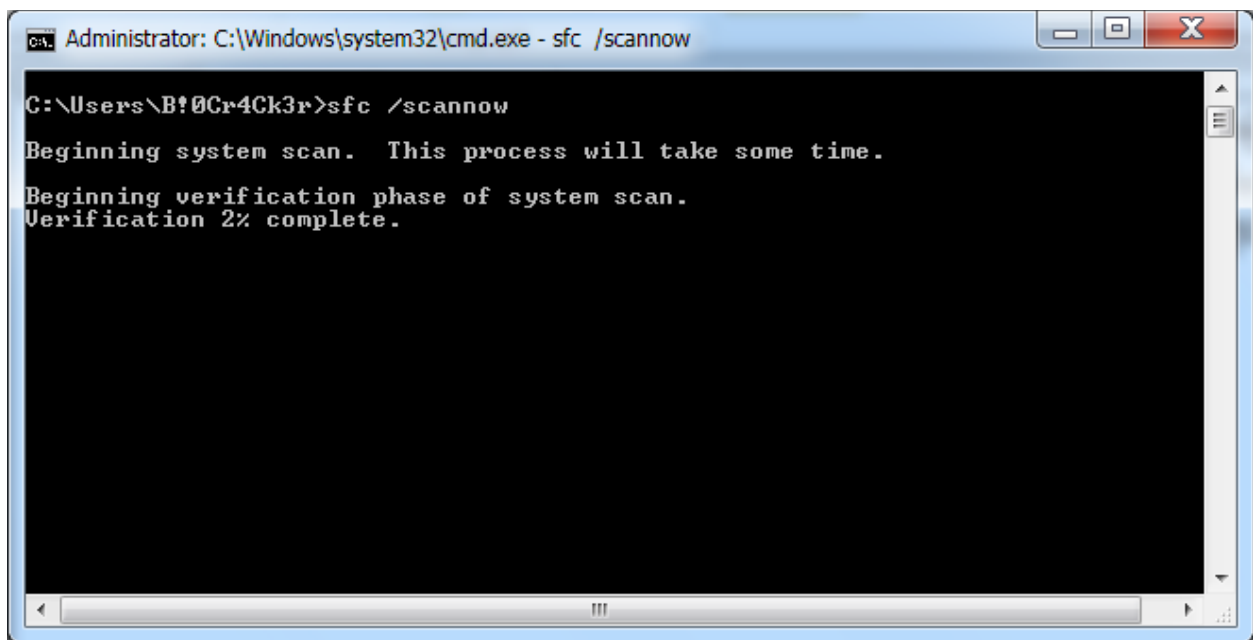
```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\B!0Cr4Ck3r\Desktop>attrib -s -h /s /d
C:\Users\B!0Cr4Ck3r\Desktop>F:
F:\>del *.exe /s/f/a
```

အထက်ပါအတိုင်းမှ >del *.exe /s/f/a ဆိုပြီးရိုက်ရပါမယ်။ ပါဝင်တဲ့ Parameter တွေကိုရှင်းပြရရင်တော့ /s ဆိုတာကတော့ Process တစ်ခုခုမှာ ယူပြီး Run နေတယ်ဆိုရင်တောင် သူက Terminate လုပ်နိုင်ဖို့အတွက် သုံးတာဖြစ်ပါတယ်။ /f ကတော့ force ပေးတာဖြစ်ပါတယ်။ /a ကတော့ Achrive

အတွက်သုံးတာဖြစ်ပါတယ်။ အကယ်လို့ သင်ဟာ GUI Mode ကနေ Shift+Del နဲ့ ဖျက်မယ်ဆိုရင် ၎င်းက Process တစ်ခုခုမှာ ယူပြီး Run နေတယ်ဆိုရင် လုံးဝဖျက်လို့မရပါဘူး။ ဒါပေမယ့် ဒီအတိုင်းသာ သင်ဖျက်ချင်တဲ့ဖိုင်ကို ဒီအတိုင်းလေးရိုက် ပြီးသုံးမယ်ဆိုရင် လုံးဝကိုပျက်သွားမှာဖြစ်ပါတယ်။

“ sfc ”

Sfc ဆိုတာကတော့ ကျွန်တော်တို့ ဘယ်အချိန်မှာ အများဆုံးသုံးရသလည်းဆိုတော့ ကွန်ပျူတာ Services သမားတွေ Customer Site ထဲရောက်သွားတဲ့အချိန်မှာအများဆုံးသုံးပါတယ်။ သူ့အတွက် သုံးရတဲ့ Parameter ကလည်းသိပ်မများပါဘူး မများပါဘူးဆိုတဲ့ထဲမှာမှ ကျွန်တော်အများဆုံးသုံးဖြစ်တဲ့ Command လေး တစ်ခုကိုတော့ပြောပါမယ်။



```
Administrator: C:\Windows\system32\cmd.exe - sfc /scannow

C:\Users\B!0Cr4Ck3r>sfc /scannow

Beginning system scan. This process will take some time.
Beginning verification phase of system scan.
Verification 2% complete.
```

အထက်ပါပုံအတိုင်းပေါ့.... >sfc /scannow ပဲဖြစ်ပါတယ် ဘာကြောင့်ဒီ Command ရိုက်ရသလည်း ဆိုတာ ရှင်းပြခွင့်ပြုပါနော် (အာဇာနည် လေသံဖြင့်)။ ကျွန်တော်တို့လိုပုံမှန် End User (ကွန်ပျူတာကိုင်တတ်ရုံလူမျိုး) တွေကတော့ ကွန်ပျူတာကို သုံးတယ်ဆိုရုံပဲသုံးကြတယ်

တစ်ပတ်တစ်ကြိမ်၊ သို့မဟုတ် တစ်လတစ်ကြိမ်လည်း မိမိကွန်ပျူတာကို Maintaining , Cleanning , Checking မလုပ်ဖြစ်တတ်ကြပါဘူး။ ဒီလိုအနေအထားမှာ HDD (Hard Disk Drive) တွေက ဖိုင်းတွေဖရိုဖရဲဖြစ်ပြီး စက်က Data တွေဖွင့်တဲ့အခါမှာလေးလံတာမျိုးတွေကြုံဖူး ကြမှာပါ။ ဒီလိုအနေအထားတစ်ခုမှာ ဒီ Command ရိုက်လိုက်မယ်ဆိုရင် လက်ရှိ HDD မှာဖြစ်ပျက်နေ Error တွေကို Scan စစ်မယ်၊ ပြီးတော့ Repair လုပ်မယ်ဖြစ်ပါတယ်။ ဒီ Command က တစ်ပတ်တစ်ကြိမ်လောက် ရိုက်ပေးသင့်ပါတယ်။ သူနဲ့ တွဲတဲ့အခြား Command တွေကတော့

/verifyonly ကတော့ ဖိုင်းတွေကို Verify လုပ်ရုံပါပဲ

/scanfile ကတော့ဖိုင်းတွေကိုစစ်ပြီး ပြင်လို့ရရင်ပြင်ပေးပါတယ်။

/verifyfile ကလည်း File တွေကိုပဲ သီးသန့် Verify လုပ်ပေးတာပါ။

/offbootdir ကတော့ Boot Directory ကို Offline အနေဖြင့် Repair လုပ်ပေးပါတယ်။

/offwindir တွေပဲဖြစ်ပါတယ်။ ဥပမာအားဖြင့်

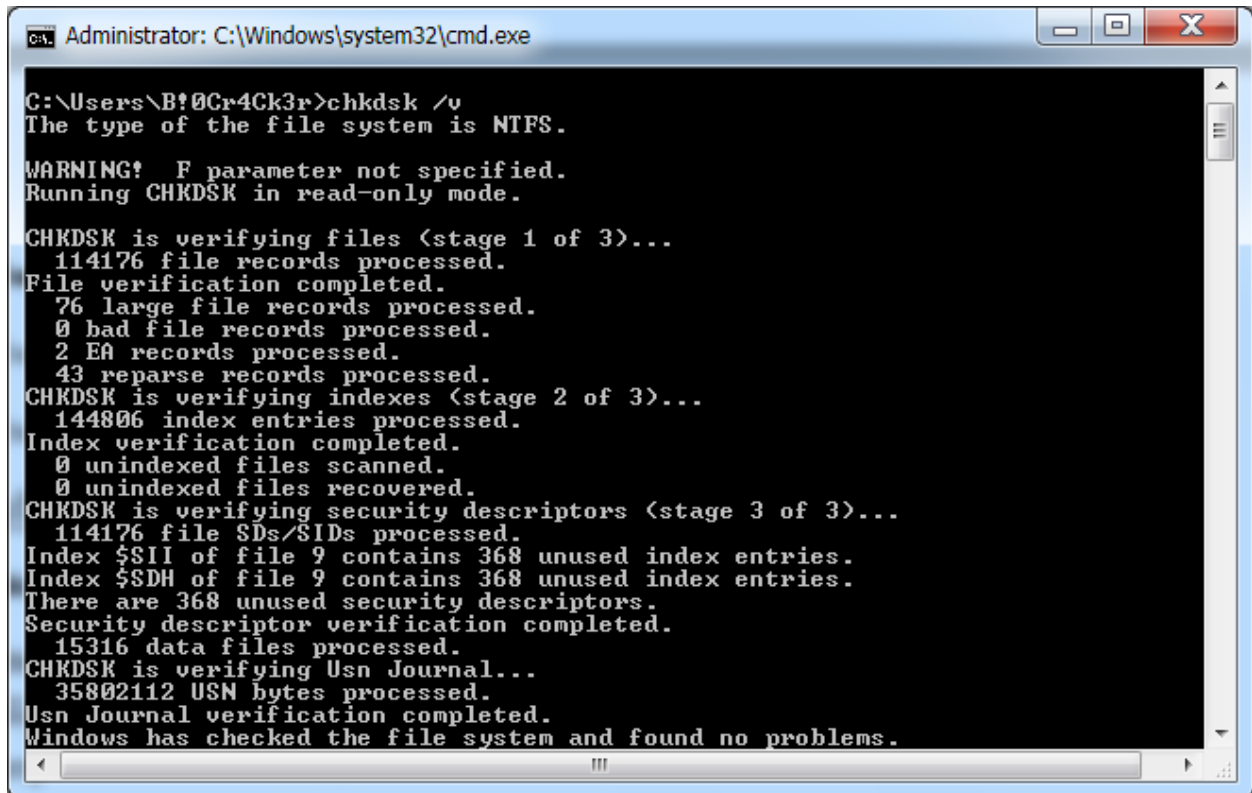
sfc /verifyfile=c:\windows\system32\kernel132.dll

sfc /scanfile=d:\windows\system32\kernel132.dll /offbootdir=d:\ /offwindir d:\windows

စသည်ဖြင့် ဖြစ်ပါတယ်။ စမ်းကြည့်မှ သိပါမယ်။

“chkdsk”

Chkdsk ဆိုတာကတော့ Check Disk Services Mode ဖြစ်ပါတယ်။ ဒီ Command ကိုလည်း ကျွန်တော်တို့ အပေါ်မှာရှင်းပြပေးခဲ့တဲ့ sfc အသွင်းသင်္ကေတတူပါတယ်။ သူ့ကိုကျွန်တော်အများ ဆုံးသုံး ဖြစ်တဲ့ Parameter တွေ ကတော့



```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\B!0Cr4Ck3r>chkdsk /v
The type of the file system is NTFS.

WARNING! F parameter not specified.
Running CHKDSK in read-only mode.

CHKDSK is verifying files (stage 1 of 3)...
114176 file records processed.
File verification completed.
76 large file records processed.
0 bad file records processed.
2 EA records processed.
43 reparse records processed.
CHKDSK is verifying indexes (stage 2 of 3)...
144806 index entries processed.
Index verification completed.
0 unindexed files scanned.
0 unindexed files recovered.
CHKDSK is verifying security descriptors (stage 3 of 3)...
114176 file SDs/SIDs processed.
Index $SII of file 9 contains 368 unused index entries.
Index $SDH of file 9 contains 368 unused index entries.
There are 368 unused security descriptors.
Security descriptor verification completed.
15316 data files processed.
CHKDSK is verifying Usn Journal...
35802112 USN bytes processed.
Usn Journal verification completed.
Windows has checked the file system and found no problems.
```

အထက်ပါပုံအတိုင်း >chkdsk /v ဖြစ်ပါတယ်။ သူနဲ့အခြားတွဲသုံးတဲ့ Parameter တွေကတော့

/F Fix လုပ်ဖို့ဖြစ်ပါတယ်။ ဒါပေမယ့် Computer ကို Restart ချပြီးပြန်တက်လာမှ လုပ်မှာပါ

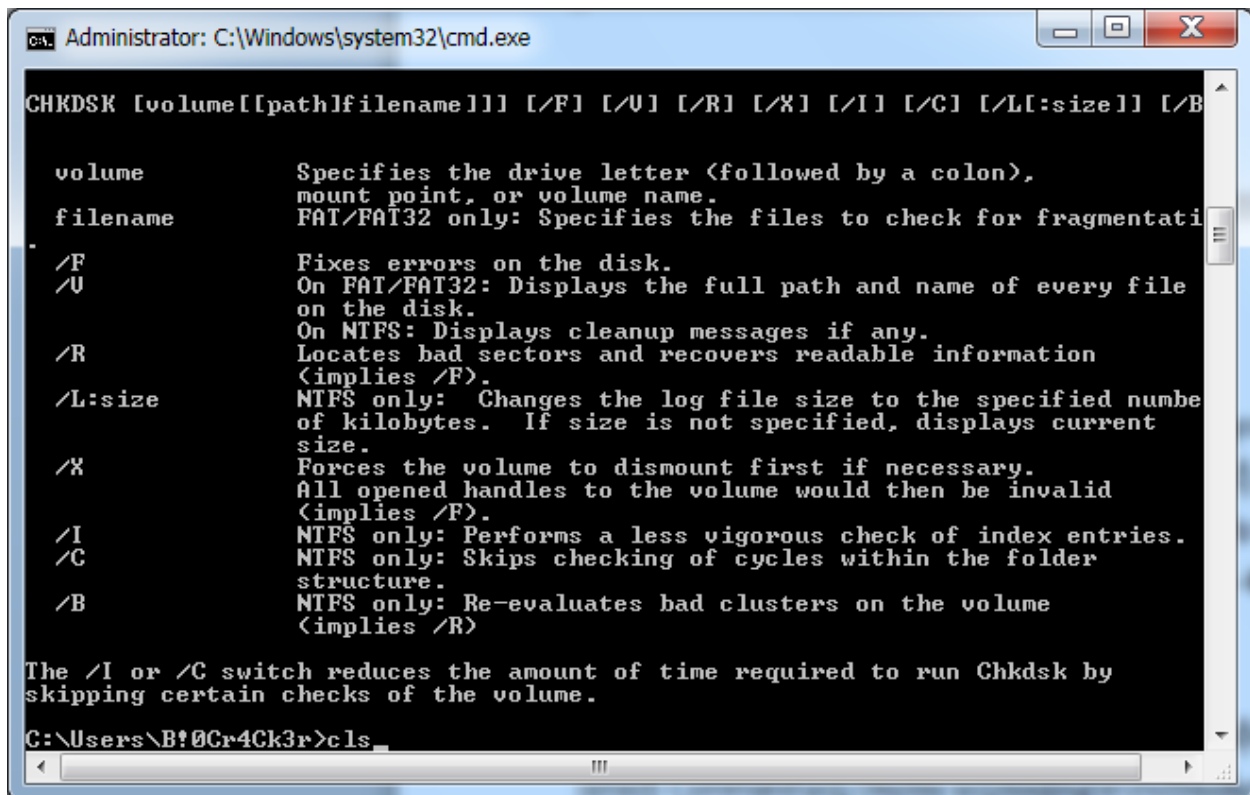
/V ကတော့ရှိသမျှ File System တွေအကုန်လုံးအတွက် တစ်ခါတည်း Scan and repair လုပ်ပါတယ်

အခြား Command တွေအကုန်လုံးကလည်း အလားတူပါပဲ နောက်တစ်ခါ System ပြန်တက်လာမှ လုပ်ဆောင် တာဖြစ်ပါတယ်။ အသေးစိတ်သိရှိရန်အတွက် >chkdsk /? သို့မဟုတ် >help chkdsk လို့ရှိုက်ပြီး အသေး စိတ်ဝင်ရောက်ဖတ်ရှုနိုင်ပါတယ်။ Linux မှာဆိုရင်တော့ Help Function အတွက်

#man (သိချင်သော Command) သို့မဟုတ် #(သိချင်သော Command) --help ဆိုပြီးရိုက်ရှာလို့လွယ်ကူပါတယ်။

“ cls ”

Cls ဆိုတာကတော့ Clear Screen လို့အဓိပ္ပာယ်ရပါတယ်။ ဆိုလိုတာက Command Prompt ထဲမှာ မိမိရိုက် ထားတဲ့ Command တွေ Display တွေအရမ်းများလာတဲ့အခါမှာ မြင်ကွင်းရှင်းအောင်အတွက် cls ဆိုတာလေးကို



```
Administrator: C:\Windows\system32\cmd.exe

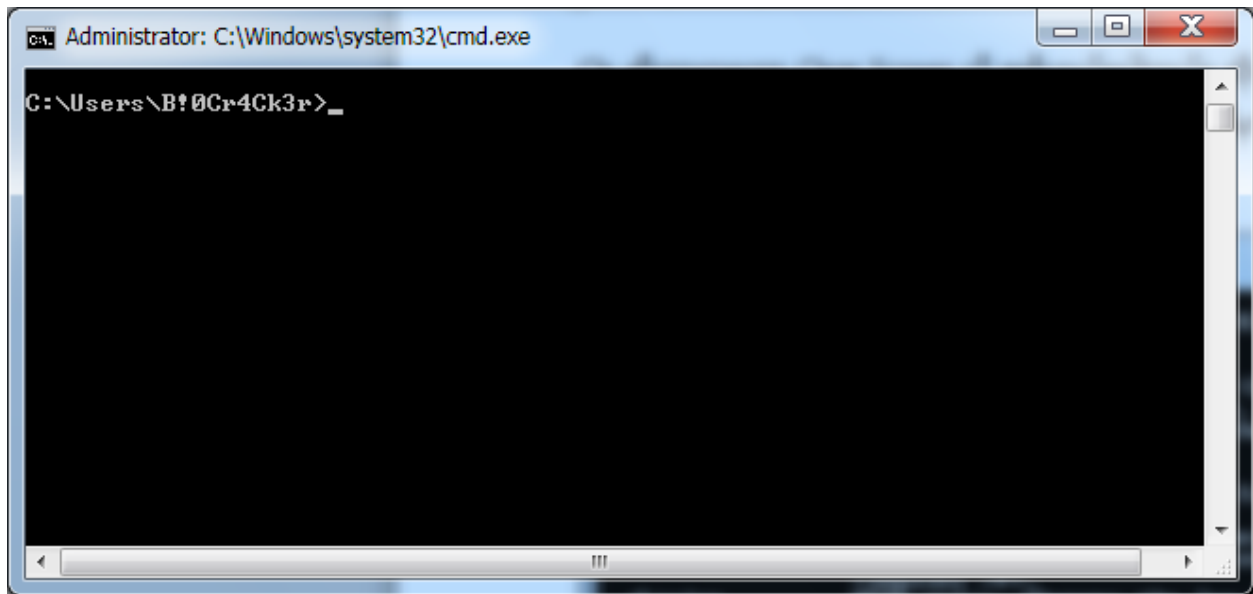
CHKDSK [volume[[path]filename]] [/F] [/U] [/R] [/X] [/I] [/C] [/L[:size]] [/B]

volume          Specifies the drive letter <followed by a colon>,
                 mount point, or volume name.
filename         FAT/FAT32 only: Specifies the files to check for fragmentati
-
/F              Fixes errors on the disk.
/U              On FAT/FAT32: Displays the full path and name of every file
                 on the disk.
                 On NTFS: Displays cleanup messages if any.
/R              Locates bad sectors and recovers readable information
                 <implies /F>.
/L[:size]       NTFS only: Changes the log file size to the specified numbe
                 of kilobytes. If size is not specified, displays current
                 size.
/X              Forces the volume to dismount first if necessary.
                 All opened handles to the volume would then be invalid
                 <implies /F>.
/I              NTFS only: Performs a less vigorous check of index entries.
/C              NTFS only: Skips checking of cycles within the folder
                 structure.
/B              NTFS only: Re-evaluates bad clusters on the volume
                 <implies /R>

The /I or /C switch reduces the amount of time required to run Chkdsk by
skipping certain checks of the volume.

C:\Users\B!0Cr4Ck3r>cls
```

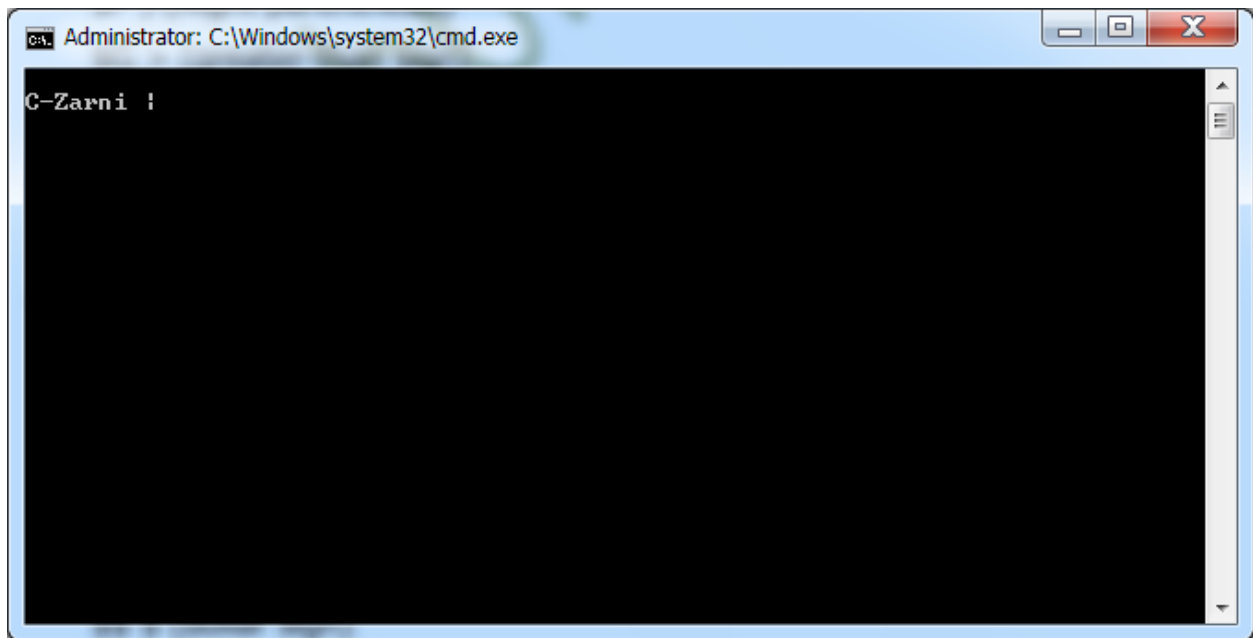
ရိုက်လိုက်မယ်ဆိုရင်



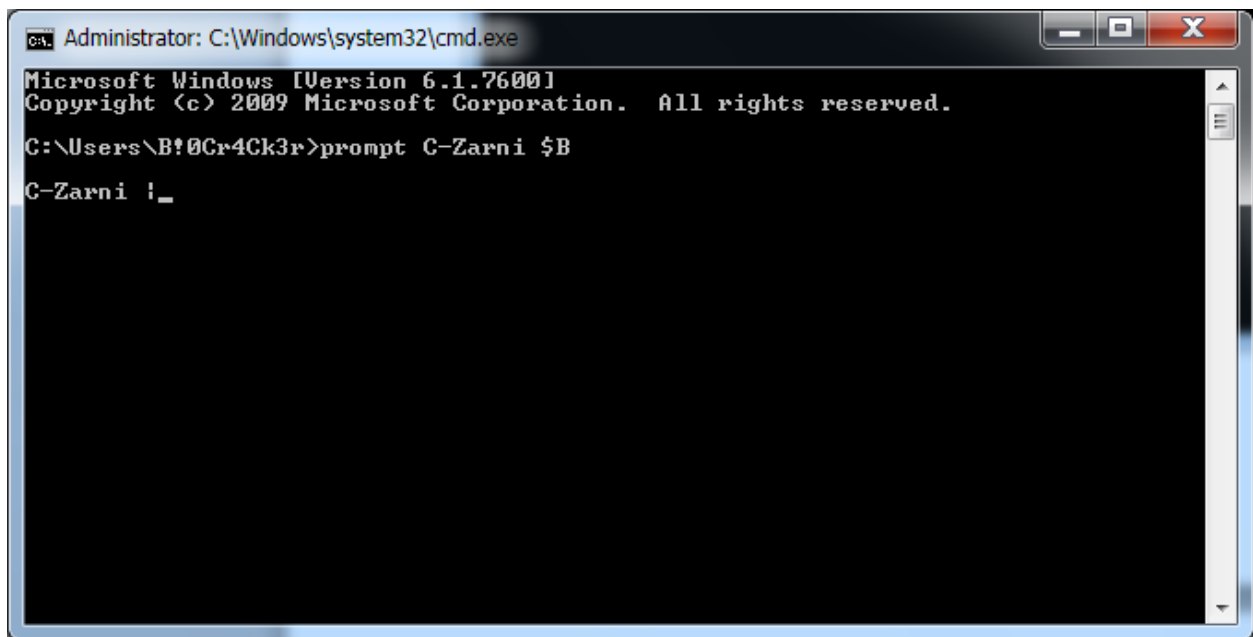
အထက်ပါပုံအတိုင်းရှင်းလင်းသွားတာကိုတွေ့ရမှာပါ။ Linux ဘက်မှာဆိုရင်တော့ **#clear** သို့မဟုတ် **Ctrl+L** ဖြစ်ပါတယ်။

“prompt”

Prompt ဆိုတာကတော့ ကျွန်တော်တို့ Command Prompt ထဲမှာ ပုံမှန်ဆိုရင် လက်ရှိ ရောက်နေတဲ့ Location တွေနဲ့ ဖော်ပြပေးပါတယ်။ ဒါပေမယ့် ကျွန်တော်တို့က အကွန့်တက်ပြီး လက်ရှိရောက်နေတဲ့ Location တွေကိုမဖော်ပြချင်ဘူး ဥပမာ ဘယ်လိုပဲ **cd** ရိုက်ရိုက် **cd..** ပဲရိုက်ရိုက် **cd** ပဲရိုက်ရိုက်ပေါ့



အထက်ပါပုံအတိုင်းပဲ Location နေရာမှာပြနေအောင်လုပ်လို့ ရပါတယ်။ဒီလိုလုပ်ဖို့ ကတော့ ကျွန်တော်တို့ ရိုက်ရမယ့် Command ကတော့ >prompt C-Zarni \$B ဆိုပြီး



အထက်ပါပုံအတိုင်းရိုက်လိုက်ပါမယ် ဒါဆိုရင် သင်ဟာ ဘယ် Location ထဲကိုပဲဝင်ဝင် ပထမပြခဲ့တဲ့ ပုံအတိုင်း ပဲ ပြနေမှာဖြစ်ပါတယ်။ \$ နဲ့ တွဲသုံးရမယ့် Command တွေကတော့

\$A & (Ampersand)

\$B | (Pipe)

\$C ((Left parenthesis)

\$D (Current Date)

\$E Escape code

\$F) (Right parenthesis)

\$G > (greater-than sign)

\$H Backspace

\$L < (less-than sign)

\$N Current Drive

\$P Current drive and path

\$Q = (equal sign)

\$S Space

\$T Current time

\$V Windows XP version Number

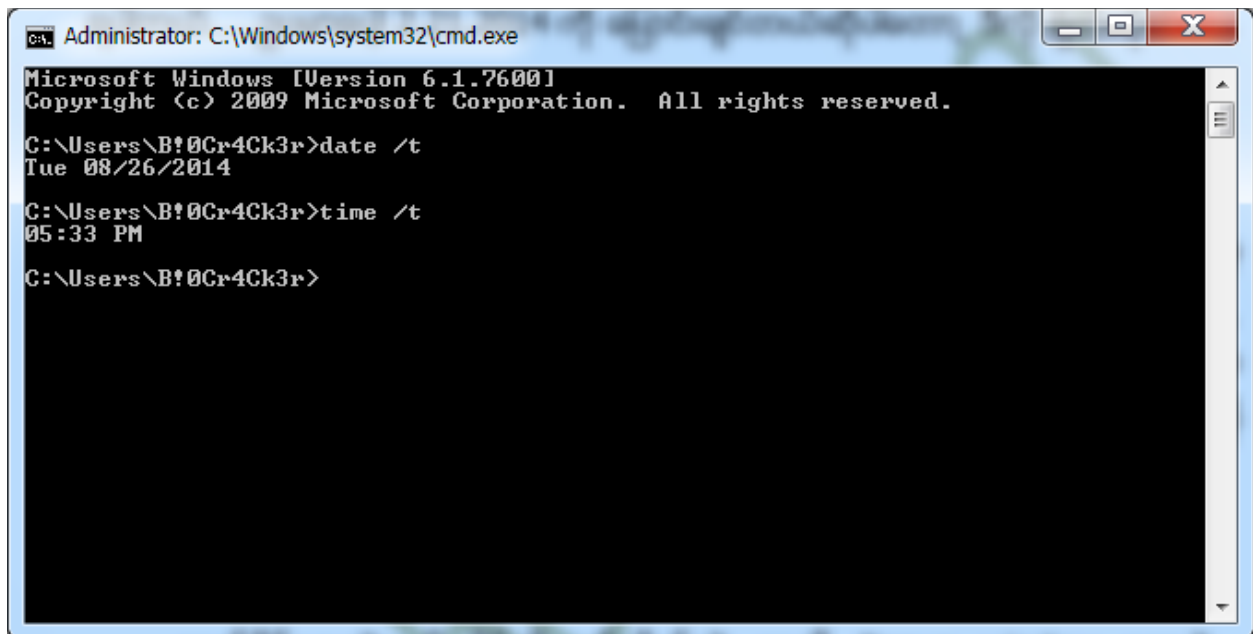
\$_ Carriage return and linefeed

\$ \$ (dollar sign)

တို့ပဲဖြစ်ပါတယ်။ မိမိနှစ်သက်ရာလေးတွေကိုရွေးချယ်စမ်းသပ်အသုံးပြုကြည့်နိုင်ပါတယ်။

“ Current Date and Current Time”

လက်ရှိရောက်နေတဲ့အချိန်ရယ်၊ ရက်စွဲရယ်ကို သိရှိနိုင်ဖို့ကတော့ ကျွန်တော်တို့ရိုက်ရမယ့် Command က



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\B!\0Cr4Ck3r>date /t
Tue 08/26/2014

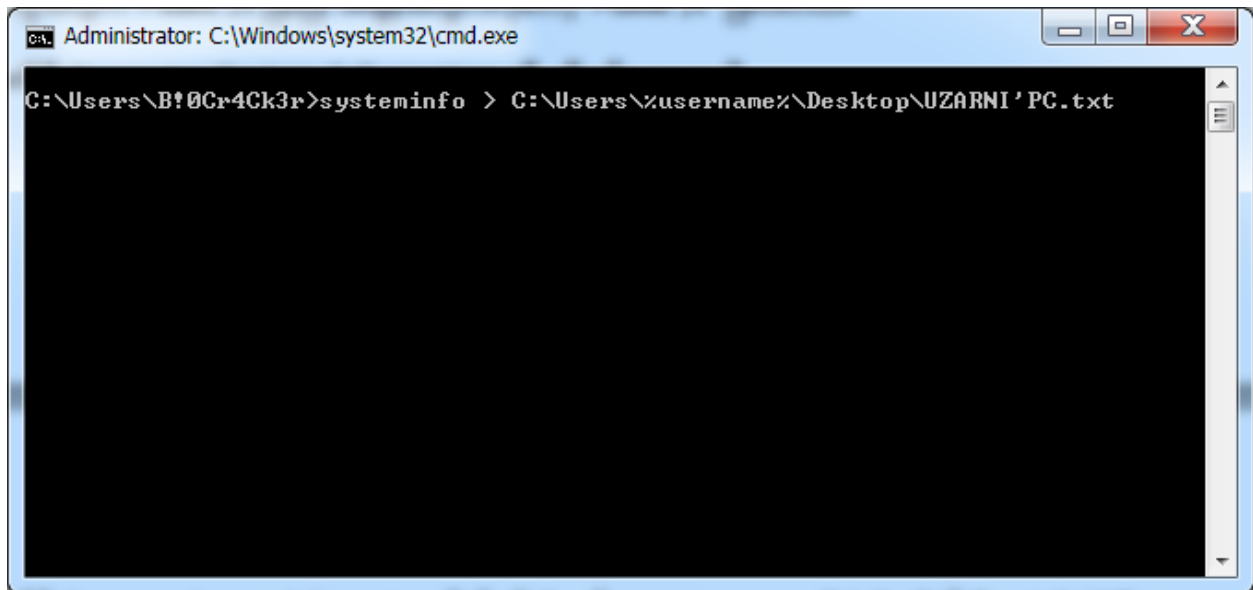
C:\Users\B!\0Cr4Ck3r>time /t
05:33 PM

C:\Users\B!\0Cr4Ck3r>
```

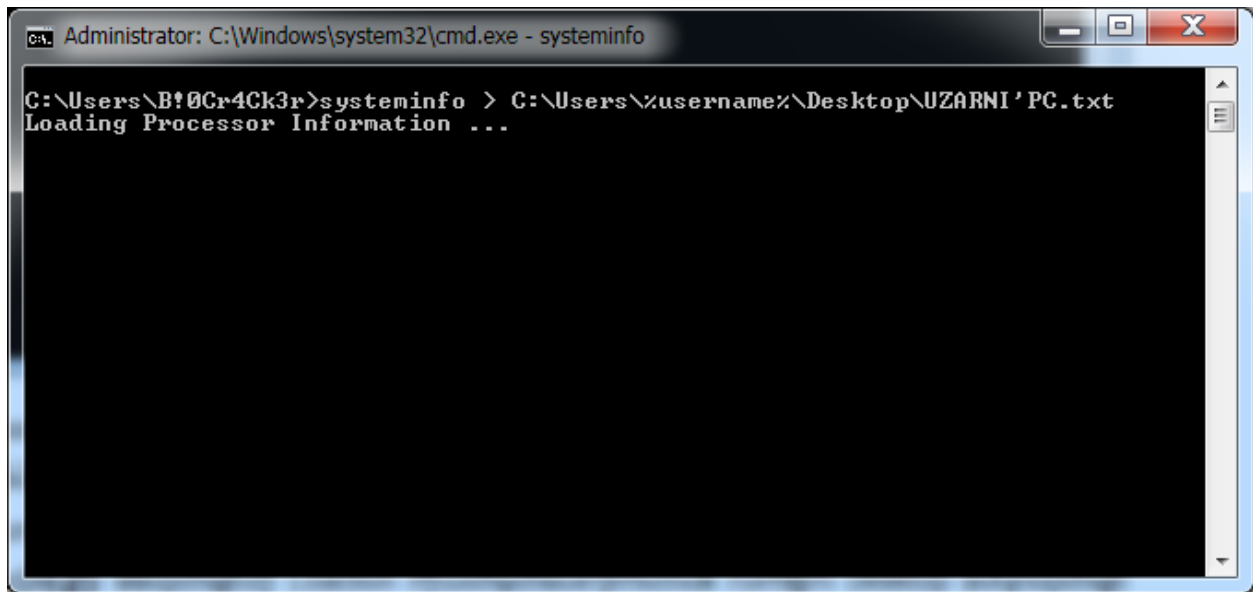
ရက်စွဲအတွက် `>date /t` ဖြစ်ပြီး အချိန်အတွက်ကိုတော့ `>time /t` ဖြစ်ပါတယ်။

လက်ရှိ Computer System Information ကို သိချင်သောအခါ

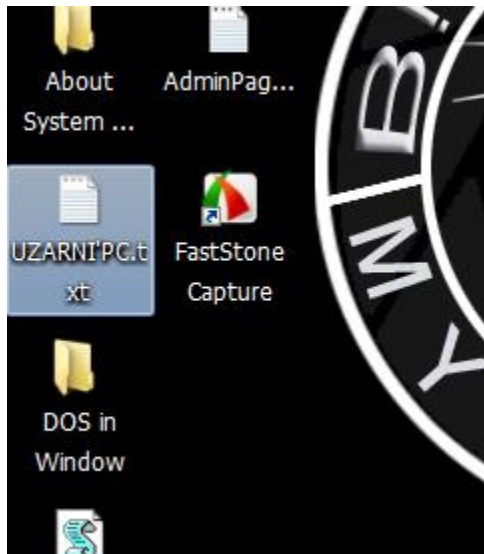
လက်ရှိ Computer System Information ကိုသိချင်တဲ့အခါမှာ အများစုကတော့ “dxdiag” တို့၊ “msinfo32” တို့စသဖြင့် ရိုက်ပြီး ကြည့်ကြပါတယ်။ ကျွန်တော်တို့က အဲဒီလိုရိုက်မနေတော့ဘူး တစ်ခါတည်း Text ဖိုင်နဲ့ ထုတ်လိုက်ပါမယ်။ ဘယ်လိုလုပ်ရမလည်းဆိုတော့ ရိုက်ရမယ့် Command က



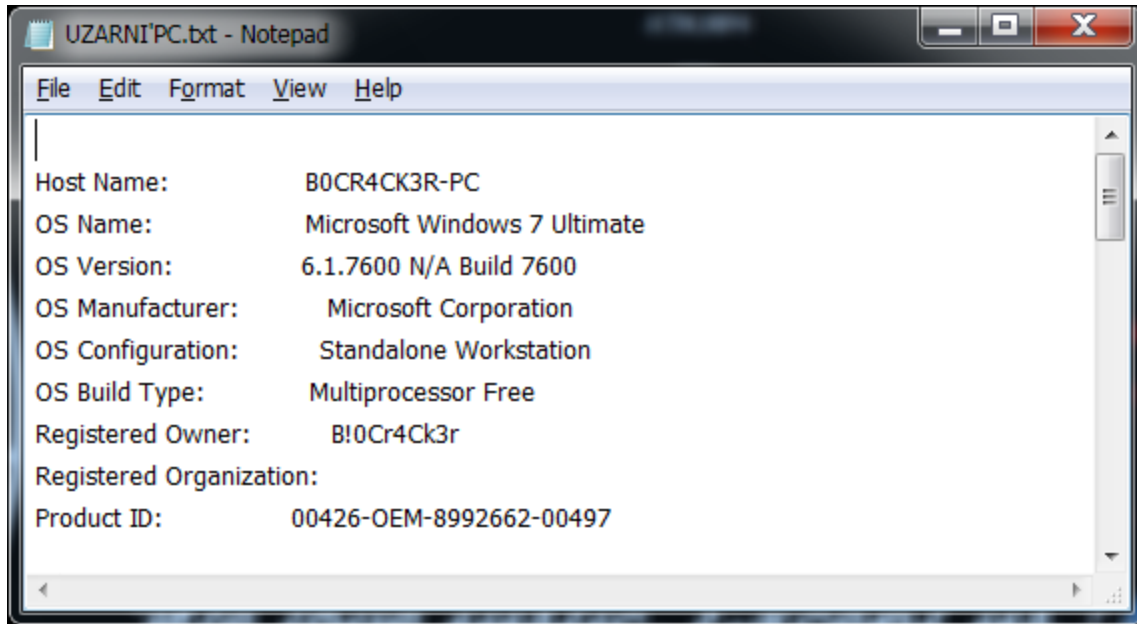
အထက်ပါပုံအတိုင်း >systeminfo > C:\Users\%username%\Desktop\UZARNI'PC.txt ဆိုပြီး ဖြစ်ပါတယ်။ တစ်ချက်ရှင်းပြပေးပါမယ်။ >systeminfo ဆိုတာကတော့ System ရဲ့ Information ကိုသိချင် သောကြောင့်ရိုက်ရခြင်းဖြစ်ပါတယ်။ ကျွန်တော်တို့က Output ထုတ်ချင်သောကြောင့် Greater-than ကို အသုံးပြုပြီး မိမိထုတ်ချင်တဲ့ Location ကိုသတ်မှတ်ပေးလိုက်တာပါ။ လက်ရှိက Desktop ပေါ်မှာထုတ်ချင် သောကြောင့်Desktop Location ရဲ့ ပတ်လမ်းက C:\User\လက်ရှိ Username\Desktop\ လို့ရိုက်လိုက်ပါတယ်။ %username% ဆိုပြီးဘာကြောင့်ရိုက်ရသလည်းဆိုတော့ ကွန်ပျူတာ တစ်လုံးနှင့်တစ် လုံးကို နာမည်ပေးထားတာခြင်းမတူညီကြပါဘူး။ ဒါကြောင့် ဘယ်လိုပဲ နာမည်ပေးထား ပေးထား User Directory ကိုရောက်စေရန် သုံးလိုက်ခြင်းဖြစ်ပါတယ်။ နောက်ဆုံးက UZARNI'PC.txt ဆိုတာကတော့ Text ဖိုင်ထုတ်တဲ့အခါမှာ နာမည်ကိုတွဲသတ်မှတ်လိုက်ခြင်းဖြစ်ပါတယ်။ ဒီအခါမှာတော့



အထက်ပါပုံအတိုင်းသင့်ကွန်ပျူတာ စနစ်တစ်ခုလုံးက အချက်အလက်တွေကို Processing လုပ်နေပြီး သင့်ရဲ့ Desktop ပေါ်မှာ



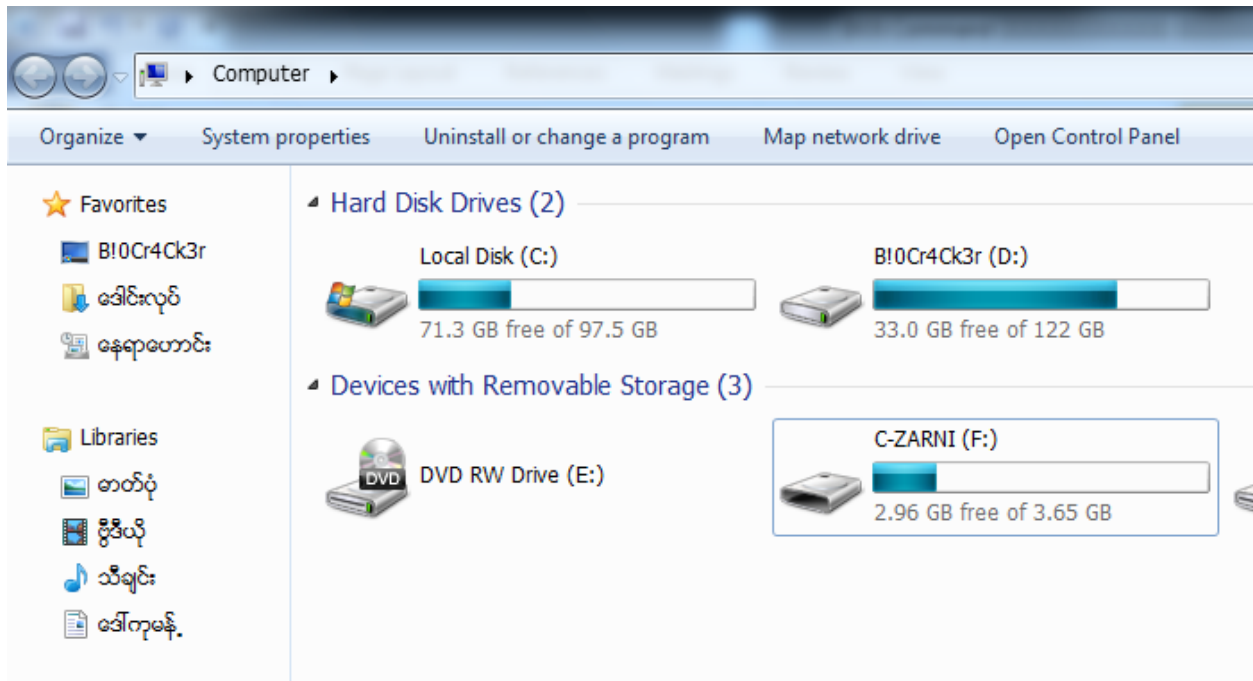
အထက်ပါပုံအတိုင်းဖော်ပြပေးနေမှာဖြစ်ပါတယ် ၎င်းဖိုင်ကိုဖွင့်လိုက်တဲ့အခါမှာတော့



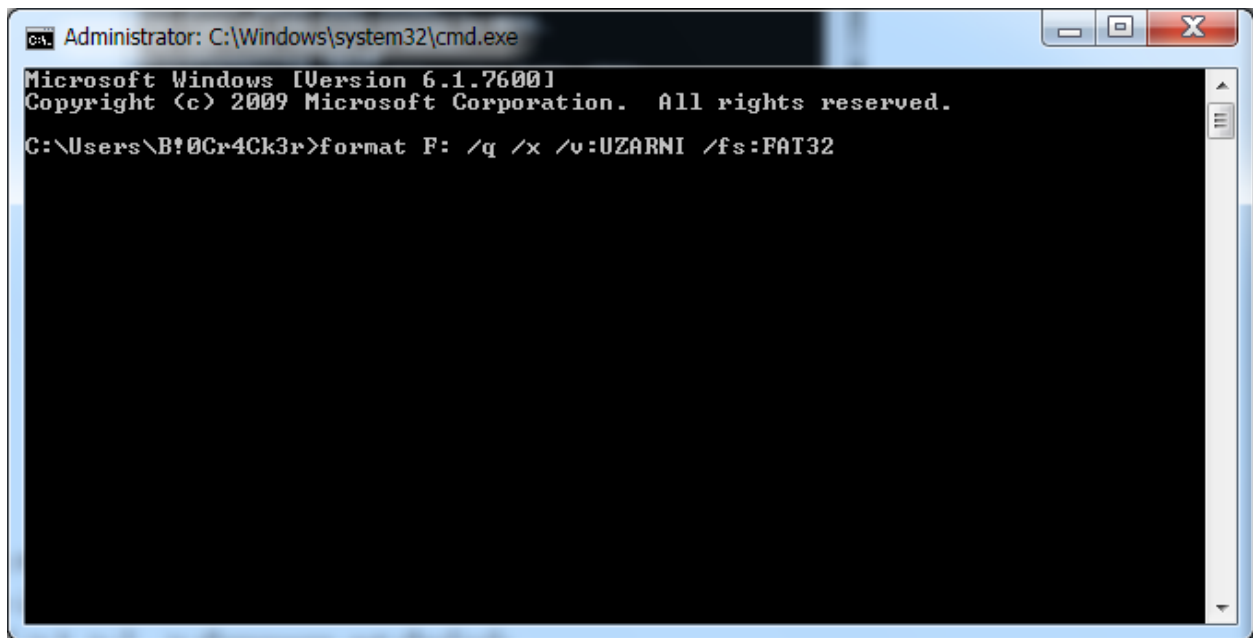
အထက်ပါပုံအတိုင်း သင့် ကွန်ပျူတာစနစ်တစ်ခုလုံးက အချက်အလက်တွေကိုအသေးစိတ်ဖော်ပြပေးပါလိမ့်မယ်။

“format”

Format ဆိုတာကတော့ အားလုံးသိတဲ့အတိုင်းပဲ လက်ရှိ Partition သို့မဟုတ် Stick တို့ကို Data Erase လုပ်ပလိုက်တာပဲဖြစ်ပါတယ်။ ကဲစလိုက်ရအောင်သင်က Memory Stick ကို GUI Mode ကနေမဟုတ်ပဲ CLI Mode ထဲကနေ Format ချချင်တဲ့အခါမှာ အရင်ဆုံး သင်သိရမှာက သင် Format ချမယ့် Memory Stick ရဲ့ Drive Letter ကို လုံးဝသိရမှာဖြစ်ပါတယ်။ ဘယ်လိုသိနိုင်မလည်း ?... လွယ်ပါတယ် သင့် Computer ထဲကို Stick ဖြင့် ချိတ်ဆက်လိုက်ပါ ထို့နောက် My Computer ကိုဖွင့်လိုက်ပါ



အခု ကျွန်တော် Format ချပြမယ့် Stick ရဲ့ နာမည်က C-Zarni ဆိုတဲ့ ဟာဖြစ်ပါတယ်။ သူ့ရဲ့ ဘေးမှာ (F:) ဆိုပြီးတွေ့ရမှာပါ။ ဒါကို Drive Letter လိုက် ခေါ်ပါတယ်။ (C:) ဆိုရင် System Partition ဖြစ်ပြီး (D:) ဆိုတာကတော့ Data Partition ဖြစ်ပါတယ်။ (E:) ကတော့ ODD (Optical Disk Drive) ပါ။ ဒါဆိုရင် ဘယ် Drive က ဘာ Drive letter ဆိုတာကို ရိပ်မိလောက်ပြီထင်ပါတယ်။ ကဲ ဒီတော့ ကျွန်တော့်က (F:) ကိုသုံးပါ တော့မယ်။အရင်ဆုံး Command Prompt ထဲမှာ ကျွန်တော်တို့ ရိုက်ရမယ့် Command ကတော့

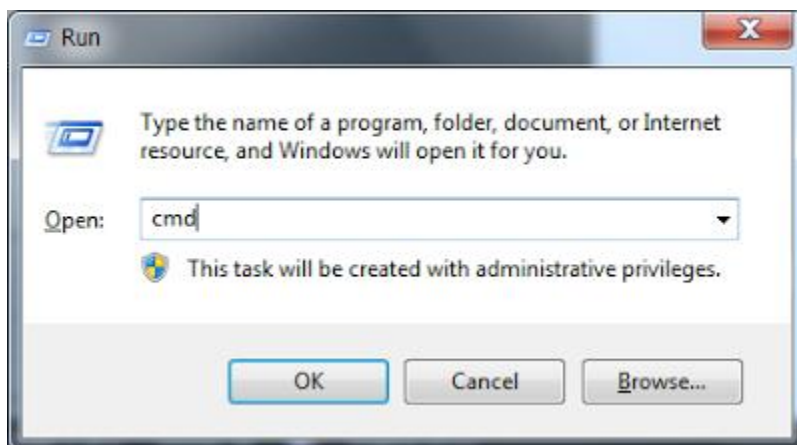
A screenshot of a Windows command prompt window. The title bar reads "Administrator: C:\Windows\system32\cmd.exe". The window content shows the following text: "Microsoft Windows [Version 6.1.7600] Copyright (c) 2009 Microsoft Corporation. All rights reserved. C:\Users\B!0Cr4Ck3r>format F: /q /x /v:UZARNI /fs:FAT32". The command prompt is open, and the command has been entered but not yet executed.

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\B!0Cr4Ck3r>format F: /q /x /v:UZARNI /fs:FAT32
```

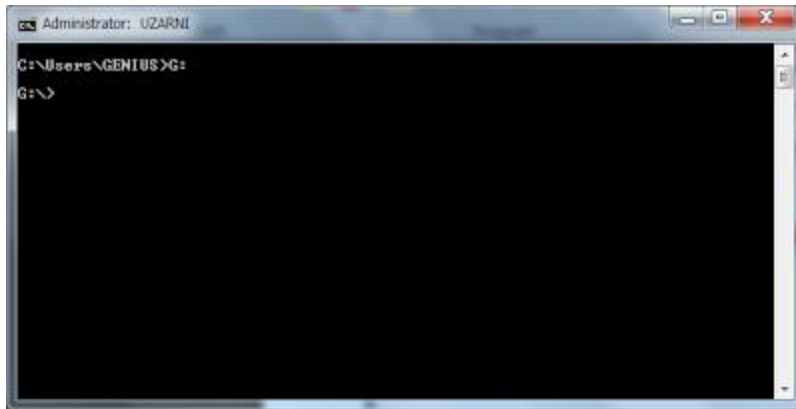
>format F: /q /x /v:UZARNI /fs:FAT32 ဆိုပြီးတော့ဖြစ်ပါတယ်။ ဒီမှာသုံးသွားတဲ့ Command နဲ့ Parameter တွေအကြောင်းရှင်းပြပါမယ်။ >format ကတော့ Format ချဖို့ဖြစ်ပြီး F: ကတော့ သင်္ကေတရှိ Format ချမယ့် Drive ရဲ့ Letter ဖြစ်ပါတယ်။ /q ကတော့ Quick ကိုညွှန်းတာဖြစ်ပါတယ်။ ဘာကြောင့်သုံးရသလည်းဆိုတော့တစ်ခါတစ်လေ Stick မှာ Bad Sector တွေ Error ရှိနေတဲ့အခါမျိုးမှာ အဲဒီအရာတွေကို Skip လုပ်သွားဖို့အတွက်ဖြစ်ပါတယ်။ /x ကတော့ Drive ကို Format မချခင် Dismount လုပ်တဲ့သဘောပါ။ ထို့နောက် /V: ကတော့ Format ချပြီးသွားလင် ထို Stick ကို နာမည်တစ်ခါတည်းပေးလို့ရအောင်လုပ်တဲ့ Parameter ပါ။ UZARNI ဆိုတာကတော့ Drive ရဲ့နာမည်ကိုခပ်ချောချောကောင်လေးတစ်ယောက်ရဲ့ နာမည် ပေး လိုက်တာပါ။ /fs: ဆိုတာကတော့ File System ကိုသတ်မှတ်ဖို့အတွက် အသုံးပြုတာဖြစ်ပါတယ်။ FAT32 ဆိုတာကတော့ အသုံးပြုမယ့် File System ဖြစ်ပါတယ်။ ကျွန်တော်တို့က Memory Stick ဖြစ်တဲ့အတွက် ကြောင့် File System ကို FAT32 သုံးစွဲရပါမယ်။

လုံးဝဖျက်လိုမရတဲ့ Folder တွေ Command Line ထဲကနေတည်မယ်။

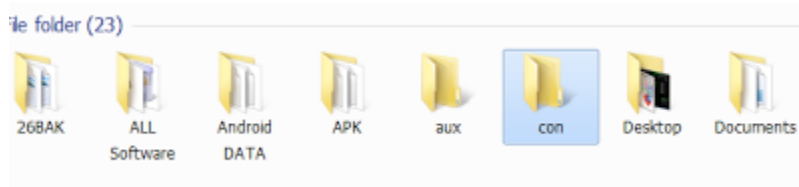
သင့်ကွန်ပျူတာရဲ့ Data Partition ထဲမှာ ဘယ်လိုမှဖျက်လိုမရတဲ့ Folder တည်မယ် မတည်ခင် တစ်ခုမှတ်ထားရမှာက ဒီနည်းဟာ CLI Mode ကနေသွားမှာပါ။သူ့ကို Effectဖြစ်ဖို့က System Partition ကိုရှောင်ရမှာဖြစ်ပါတယ်။ ဘာလို့လည်းဆိုတော့ဒီနည်းဟာ System Partition မှာအလုပ်မ လုပ်ပါဘူး။ ကဲစလိုက်ရအောင်လားဗျာ..ထုံးစံအတိုင်းပေါ့ကျွန်တော်တို့က CLI ကနေ လုပ်မှာဆိုတော့ ကီးဘုတ်ကနေ Run ကိုခေါ်လိုက်ပီး "cmd"လို့ရိုက်လိုက်ကြတာပေါ့။



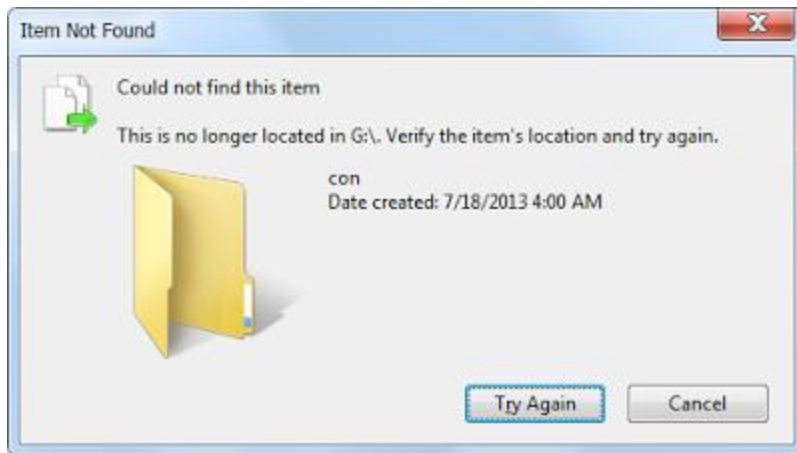
ပြီးသွားရင် အနီးတားခေါက်လိုက်ပါ။ဒီနောက်မှာတော့မိမိတို့ကွန်ပျူတာမှာရှိတဲ့ DataPartition ကို သတ်မှတ်မှာဖြစ်ပါတယ် ကျွန်တော့်ကွန်ပျူတာထဲမှာကတော့ G: & Z:ဆိုပီးရှိပါတယ် ကျွန်တော်က G: မှာလုပ်ဆောင်မှာဖြစ်ပါတယ်။ဒါကြောင့် ပေါ်လာတဲ့ CLI Mode မှာ "G:" လို့ရိုက်လိုက်ပါမယ်



ဒါဆိုရင် သင့်ကွန်ပျူတာက Data Partition ထဲရောက်သွားပါပြီ။ ဒီတော့ကျွန်တော်တို့က ဖိုဒါတည်ရအောင် ဆိုတော့က ဖိုဒါတည်မယ်ဆိုရင် သုံးဂုမယ့် Command က "md"(Make Directory) ဖြစ်ပါတယ်။ဒါကြောင့်ကျွန်တော်တို့က G:\>md con\ လို့ရိုက်လိုက်ပါမယ် ဒါဆိုရင်သင့်မိုင်ကွန်ပျူတာမှာလည်း con ဆိုတဲ့ Folder ကပေါ်လာမှာဖြစ်ပါတယ်။



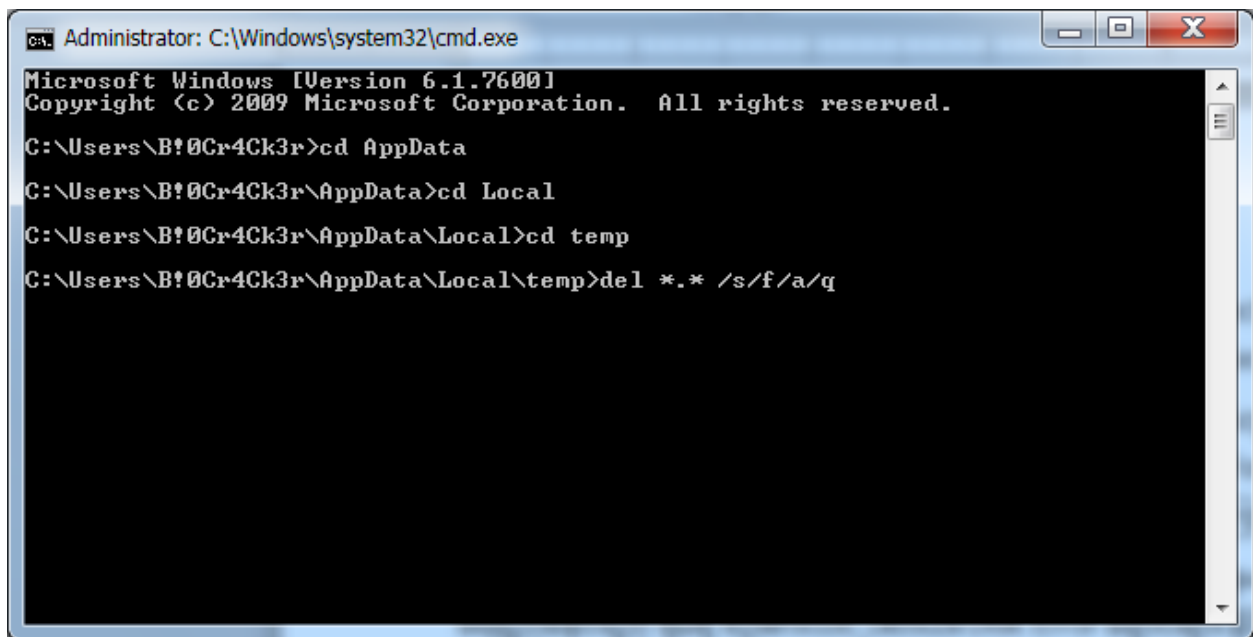
ဒီအခါကျွန်တောတို့ကစမ်းပြီး ဖျက်ကြည့်ရအောင် ။ဆိုတော့ ကီးဘုတ်ကနေ ထုံးစံအတိုင်းပေါ့ဖျက်မယ်ဆိုမှတော့ Del Key ကိုနှိပ်လိုက်ပါမယ်။ဒါဆိုရင်အောက်ပါ ပုံအတိုင်းဖျက်လို့မရဘူးဆိုတဲ့ Error Message ပြလာမှာဖြစ်ပါတယ်။



ကြိုက်သလောက်ဖျက်ပါ။ သာမန်ဖျက်ရုံလောက်နဲ့ ဘယ်လိုနည်းနဲ့မှမပျက်နိုင်ပါဘူးကီးဘုတ်ကနေ Shift+Del နဲ့လည်းဖျက်လို့မရပါဘူး။ဒါပေမယ့်သူ့ကိုပြန်ဖျက်ချင်တယ်ဆိုရင်တော့ CLI ကနေပဲ ရိုက်ရမယ့် Command က `G:>rd con\` ဆိုပြီး ပြန်ရိုက်လိုက်ပါ။Rd (Remove Directory) ခံပြီးပြန်ရိုက်လိုက်တဲ့အခါကျရင်တော့ပြန်ပျက်သွားမှာဖြစ်ပါတယ်။ထိုကဲ့သို့သောဖိုဒါများကိုတည်ရင်အခုက နှုတ်တော်ဖော်ပြထားတဲ့ အမည်များကိုသာသုံးရမှာဖြစ်ပါတယ်။ *con, aux, lpt1, lpt2, lpt3, lpt4, lpt5, lpt6, lpt7, lpt8 နှင့် lpt9*တို့ပဲဖြစ်ပါတယ်။ မိမိက စိတ်ကြိုက်နာမည်ပေးလျှင် အလွယ်တကူဖျက်လို့ရပါတယ်ဥပမာ `G:>md zarni\` ဆိုရင် ဖိုဒါကတော့တည်သွားမယ် ဒါပေမယ့်သူ့ကိုဖျက်တဲ့အခါ (ပုံမှန် Del Key ကိုသုံး၍ဖျက်ခြင်း) ပျက်သွားမှာဖြစ်ပါတယ်။

Browsing ရဲ့ Temp ဖိုင်တွေကို တစ်ချက်တည်းနဲ့ရှင်းမယ်

ကျွန်တော်တို့ Browsing Data cache တွေ၊ Program temporary file တွေနှင့် အခြားမလိုအပ်တဲ့ဖိုင်တွေအများစုရှိတဲ့နေရာကတော့ C:\Users\%username%\AppData\Local\temp\ ထဲမှာ အများဆုံးတည်ရှိကြတာပါ။ ဒီလိုရှိတဲ့နေရာထဲက ဟာတွေကို ကျွန်တော်တို့က CLI Mode ထဲကနေဖျက်ချင် တဲ့အခါမှာ တော့ အရင်ဆုံး cmd ကိုဖွင့်လိုက်ပါ ပြီးသွားရင်



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\B!0Cr4Ck3r>cd AppData
C:\Users\B!0Cr4Ck3r\AppData>cd Local
C:\Users\B!0Cr4Ck3r\AppData\Local>cd temp
C:\Users\B!0Cr4Ck3r\AppData\Local\temp>del *.* /s/f/a/q
```

အထက်ပါပုံအတိုင်း

>cd AppData

>cd Local

>cd temp

>del *.* /s/f/a/q

ဆိုပြီးကိုက်လိုက်ပါမယ်။ ဒါဆိုရင်သင်အခုလက်ရှိသုံးနေတဲ့ အဓိက Browser တွေရဲ့ Cache တွေကိုရှင်းလင်း သွားမှာဖြစ်ပါတယ်။ ဒီနေရာမှာ Parameter တွေကိုရှင်းပြပါမယ်။

>**del** ဆိုတာကတော့ Delete Command ဖြစ်ပါတယ်။ *.* ဆိုတာကတော့ [dot] ရဲ့အရှေ့က * ကတော့ မသိသော File Name ကိုယ်စားပြုပြီး [dot] ရဲ့အနောက်က * ကတော့ မသိသော File Extention ကိုဆို လိုတာဖြစ်ပါတယ်။ ထို့နောက် Parameter တွေအကြောင်းဆက်ရှင်းပြခွင့်ပြုပါ (အာဇာနည်လေသံဖြင့်) **/s** ဆိုတာကတော့ Deleter specified ဖြစ်ပါတယ်။ **/f** ကတော့ Force Deleting ကိုကိုယ် စားပြတာဖြစ်ပါတယ်။ **/a** ကတော့ ဖျက်မယ့်ဗိုင်းကို attribute ပေါ်မှာ အခြေခံပြီးအလုပ်လုပ်အောင် သတ်မှတ်တာဖြစ်ပါတယ်။ **/q** ကတော့ Quick mode ဖြစ်ပါတယ်။ အမေးအမြန်းမရှိ မြန်မြန်ဖျက်ဆိုတဲ့ အဓိပ္ပါယ်ရပါတယ်။

How to Hack the BIOS Password using by CMD Mode ?



ကျွန်တော်တို့ Password တွေကိုကျော်ကြတဲ့နည်းပေါင်းစုံတွေထဲမှာမှ အခုကျွန်တော်ပြောချင်တာက BIOS Password ကိုကျော်မယ့်နည်းလေးပါ။ Desktop Computer မှာဆိုရင်တော့ရှေးမရှိဘူးပေါ့ CMOS Battery ကိုဖြုတ်ပီး မိနစ် ၃၀ လောက်ထားလိုက်ရင် BIOS Password က ပြုတ်သွားပါလိမ့်မယ်နောက် တစ်နည်းကတော့ CMOS Jumper လေးကို နေရာရွှေ့ပေးလိုက်ရုံပေါ့....



စတိုင်ပတ်မှာကတော့ Laptop Computer တွေအတွက်ပါLaptop ကျတော့ CMOS Battery ကို အချို့ ဖက်တွေမှာကဖြုတ်ဖို့လွယ်ကူပေမယ့် အချို့စက်တွေမှာက ဖြုတ်ဖို့ခက်ခဲပါတယ်။ ဒါပေမယ့် ဘာဘက်ထ ရှိမှမဖြုတ်ပဲ ကျွန်တော်တို့က လက်ရှိတက်နေတဲ့ ဝင်းဒိုးပေါ်ကနေပဲ CLI Mode ထဲကနေ အသုံးပြုပြီး BIOS Password ကိုဖြုတ်ချမှာဖြစ်ပါတယ်။

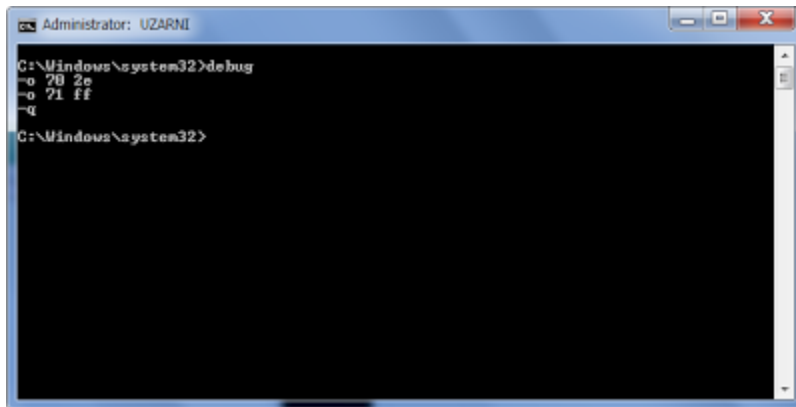
ကဲရိုက်ရမှာက

_o 70 2e

_o 71 ff

_q

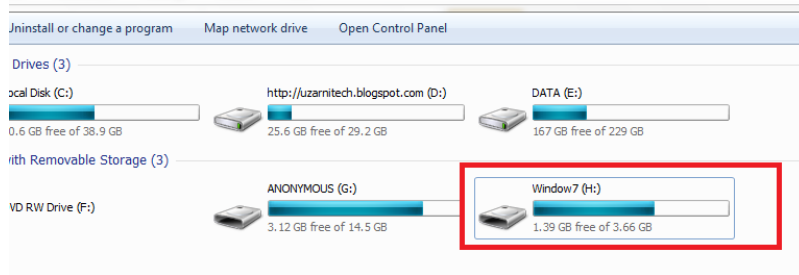
လို့ရှိက်ရမှာဖြစ်ပါတယ်။ အောက်ကပုံအတိုင်းပေါ့ ၀= အင်္ဂလိပ်အက္ခရာအို ပါအောက်ကပုံအတိုင်းပေါ့...



ပီးသွားရင် ကျွန်တော်တို့က စက်ကို Restart တစ်ချက်ချပြီး BIOS ထဲဝင်ကြည့်လိုက်ပါ BIOS Password က Clear ဖြစ်နေတာကိုတွေ့ရပါလိမ့်မယ်။

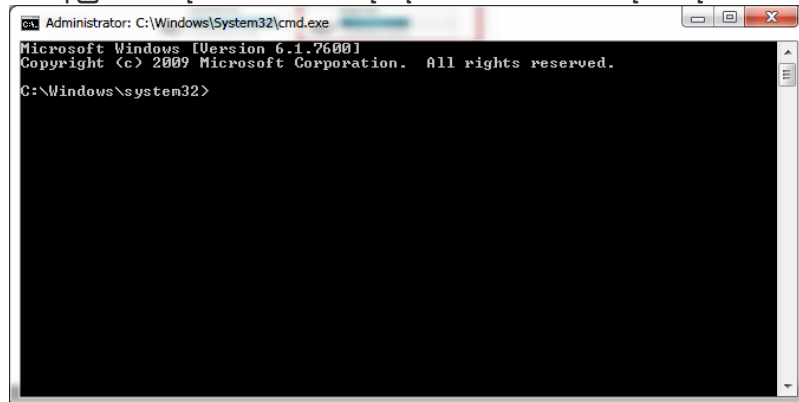
ဘာ Software မှမသုံးပဲ USB Stick ဖြင့် ဝင်းဒိုးတင်နည်း

ကျွန်တော်တို့ Window Installation မှာ အများစုက CD or DVD ဖြင့်တင်ကြတာ များပါတယ်။ ဒီလိုအနေအထားကလည်း Object (မိမိ တင်မယ့် စက်မှာ) CD or DVD Rom ပါနေမှပဲဖြစ်မှာပါ။ အကယ် လို့ မပါဘူးဆိုရင်တော့ USB Stick ဖြင့် တင်တဲ့နည်း လမ်း ပေါင်းစုံရှိပါတယ်။ ဂရုတော်တော်များများမှာလည်း ရေးထားတာကို အလွယ်တကူရှာဖွေတွေ့ရှိနိုင်မှာပါ။ ထိုနည်းတွေ ကလည်း Window ကို အရင်ဆုံး ISO လုပ်ပီးမှ ကြားခံဖြစ်သော Program တစ်ခုခုဖြင့် Stick ကို Bootable ဖြစ်အောင် အရင်လုပ်ပီးတော့မှ ဆွဲထည့်တဲ့ နည်းတွေများပါတယ်။ အခုကျွန်တော် ပြောမယ့်အကြောင်းအရာလေး ကတော့ Window CD တစ်ချပ်ပဲရှိပါစေ ရပါတယ်။ ကြားခံ ဘာ Software မှ မလိုပဲ Command Line ထဲကနေ USB Stick ကို Bootable ဖြစ်အောင် MBR (Master Boot Record)တွေ၊ Partition တွေသတ်မှတ်ပီး အလွယ်ဆုံးလုပ်ဆောင်စေပီးနောက် ဝင်းဒိုးအခွေ ထဲမှ ဒေတာအားလုံးကို ကော်ပီ Paste လုပ်လိုက်ရုံနဲ့ ရမယ့်နည်း ဖြစ်ပါတယ်။ ဒီနည်းကိုလုပ်ဆောင်ဖို့အတွက် Memory Stick ရဲ့ Size ကတော့ အနည်းဆုံး 4GB ရှိဖို့လိုအပ်ပါမယ်။ ကဲစလိုက်ရ အောင်လားဗျာ...အရင်ဆုံး သင့် USB ကို ကွန်ပျူတာနဲ့ ဆက်သွယ် လိုက်ပါ။

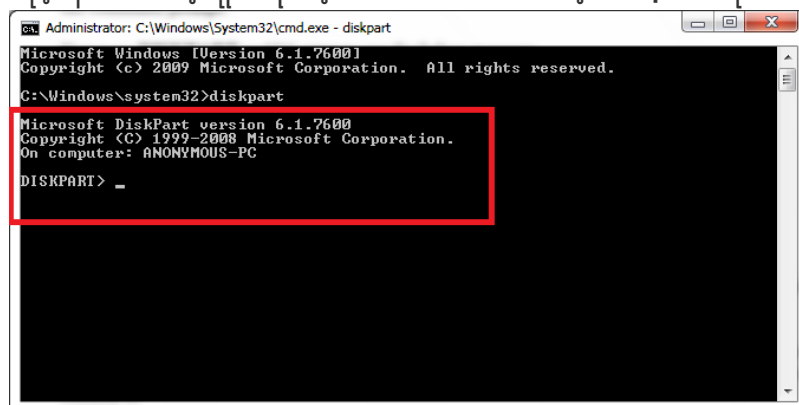


ဒီနောက်တော့ သင့်ရဲ့ Drive Letter, Size တို့ကို တိကျသေချာ စွာမှတ်သားထားဖို့လိုပါတယ်။ အရမ်းလည်းအရေးကြီးပါတယ်။ အကယ်လို့ Driveletter and size ကို မှားယွင်းသွားတယ်ဆိုရင် ဝင်းဒိုးရဲ့ စနစ်တစ်ခုလုံးကိုပါထိခိုက်နိုင်လို့ပါ (အရမ်းအရေးကြီး)။

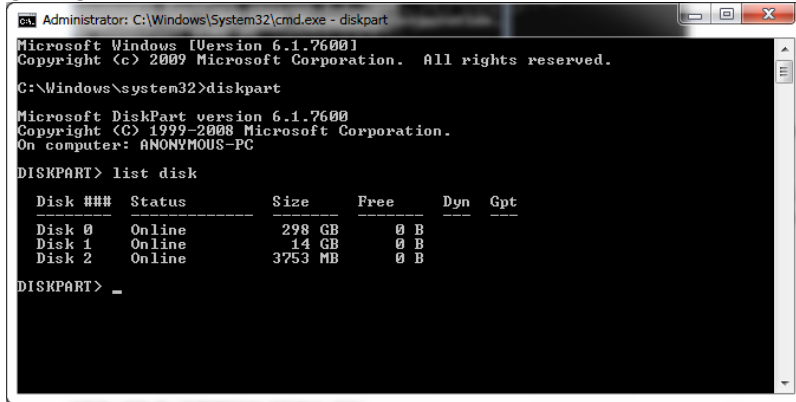
ထို့နောက် ကျွန်တော်တို့က Start ထဲမှာ run လို့ရှိကိစီး Right Click နှိပ်၍ run as administrator အနေဖြင့် ဝင်လိုက်ပါမယ်။ ဒါဆို ရင်တော့ အောက်ပါပုံအတိုင်းပေါ်လာမှာဖြစ်ပါတယ်။



ထို့နောက်တော့ ရိုက်ရမယ့် Command ကတော့ diskpart ဆိုတာ ဖြစ်ပါတယ်။



၃၈၈၈၈၈၈၈.လောက်စောင့်ပြီး **DISKPART>** - ဆိုတာဖြစ်တဲ့အထိ တစ် ချက်စောင့်လိုက်ပါမယ်။ အထက်ပါပုံ အတိုင်းပေါ့.... ပီးသွားရင်တော့ ကျွန်တော်တို့က လက်ရှိ ဝင်းဒိုးမှာ Detected ဖြစ်နေတဲ့ Drive တွေ ကိုကြည့်မှာဖြစ်တဲ့အတွက်ကြောင့်ရိုက်ရမယ့် Command ကတော့ **List disk** ဖြစ်ပါတယ် အောက်ပါ ပုံအတိုင်းပေါ့..



```
Administrator: C:\Windows\System32\cmd.exe - diskpart
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>diskpart

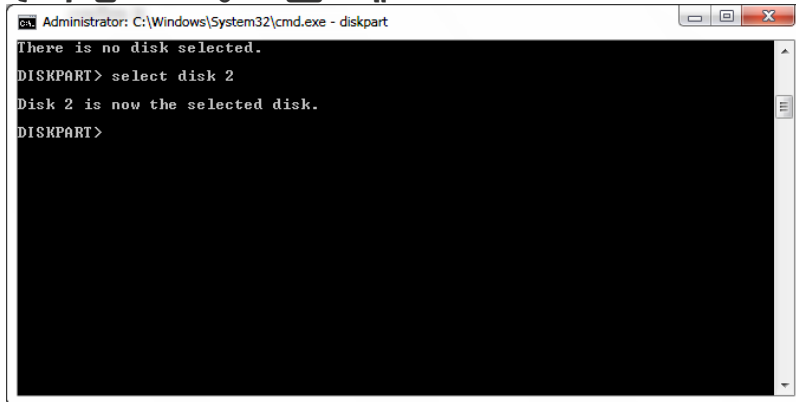
Microsoft DiskPart version 6.1.7600
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: ANONYMOUS-PC

DISKPART> list disk

   Disk ###        Status       Size         Free        Dyn  Gpt
   -----        -
   Disk 0            Online          298 GB         0 B
   Disk 1            Online          14 GB         0 B
   Disk 2            Online        3753 MB         0 B

DISKPART> _
```

အထက်ပါပုံအတိုင်းမှာ သေချာရှင်းပြချင်ပါတယ်။ ဘာလို့လည်း ဆိုတော့ ဒီနေရာမှာ ကျွန်တော် တစ်ခါတုန်းက စမ်းတုန်းကဆို Disk ရွေးချယ်မှုမှားယွင်းသွားတာကြောင့် ဝင်းဒိုးက လုံးဝကို ဒေါင်းသွား တယ်ဗျ။ ဘယ်လိုမှလည်း Recover လုပ်လို့မရတော့လို့ ဝင်းဒိုး ပြန် တင်ရတဲ့အနေ အထား အထိအောင်ရောက်သွားလို့ ဒီနေရာက အ အရမ်းအရေးကြီးပါတယ်။ ဒါကြောင့် မိမိရဲ့ Window တင်မယ့် Disk ကို သေချာအောင် ကြည့်စေလိုပါတယ်။ အထက်ပါပုံအတိုင်းနဲ့ ကျွန်တော်ရှင်းပြပါမယ်။ အခုလက်ရှိ Disk အရ 0, 1 , 2 ဆိုပြီးရှိ ပါတယ်။ 0 ဆိုတာကတော့ ကျွန်တော့် ကွန်ပျူတာထဲမှာရှိတဲ့ HDD Size 320 ကိုညွှန်းတာဖြစ်ပါတယ်။ Disk 1 ကတော့ 16GB ရှိတဲ့ Memory Stick တစ်ခုဖြစ်ပြီး၊ Disk 2 ဆိုတာကတော့ ကျွန်တော် ဝင်းဒိုး တင်ဖို့စမ်းသပ်မယ့် Stick ဖြစ်ပြီး Size အားဖြင့် 4GB သာရှိ ပါတယ်။ ဒါကြောင့် ကျွန်တော်ကတော့ Disk 2 နဲ့ အလုပ်လုပ် မှာ ။ သင်တို့ကတော့ မိမိ Drive ရဲ့ Size ကို သေချာစစ်ဖို့လိုပီးရွေးချယ် ရမှာဖြစ်ပါတယ်။ကဲဆက်လိုက်ရအောင်ကျွန်တော်က Disk 2 ကိုရွေး ချယ်မှာဖြစ်တဲ့အတွက်ကြောင့် ရိုက်မယ့် Command က **select disk 2** ဆိုပြီးဖြစ်ပါတယ်။



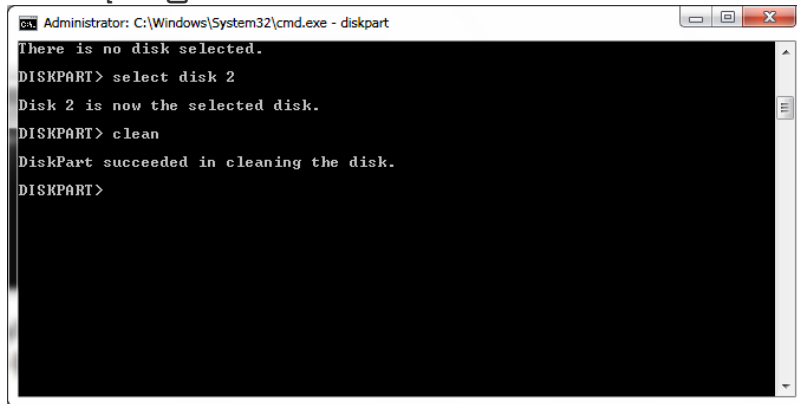
```
Administrator: C:\Windows\System32\cmd.exe - diskpart
There is no disk selected.

DISKPART> select disk 2

Disk 2 is now the selected disk.

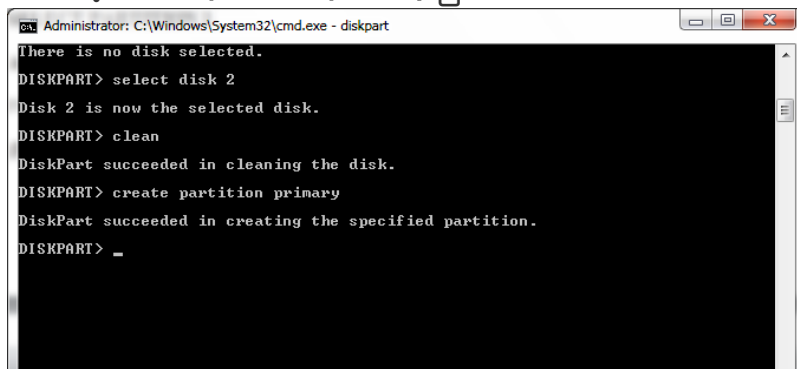
DISKPART>
```

ဒါဆိုရင်တော့ Disk 2 ကိုရွေးချယ်ပီးသွားပီဖြစ်ပါတယ်။ဒီနောက် ဆက် ရိုက်ရမယ့် Command ကတော့ **clean** ဆိုတာဖြစ်ပါတယ်။



```
Administrator: C:\Windows\System32\cmd.exe - diskpart
There is no disk selected.
DISKPART> select disk 2
Disk 2 is now the selected disk.
DISKPART> clean
DiskPart succeeded in cleaning the disk.
DISKPART>
```

ဒါဆိုရင်တော့ ကျွန်တော်တို့က Stick ထဲက ဒေတာတွေကို ဖျက်စီး လိုက်တဲ့အ ပိုင်းဖြစ်ပါ တယ်။ဘာကြောင့်လည်းဆိုတော့ MBR သတ်မှတ်ဖို့ဖြစ်ပါတယ်။ထို့နောက်ထပ်မံရိုက်ရမယ့် Command ကတော့ **create partition primary** ဖြစ်ပါတယ်။



```
Administrator: C:\Windows\System32\cmd.exe - diskpart
There is no disk selected.
DISKPART> select disk 2
Disk 2 is now the selected disk.
DISKPART> clean
DiskPart succeeded in cleaning the disk.
DISKPART> create partition primary
DiskPart succeeded in creating the specified partition.
DISKPART> _
```

ဒီအပိုင်းကတော့သင့်ရဲ့ Stick ကို Partititon တစ်ခုအဖြစ် လုပ်ဆောင် တဲ့အပိုင်းဖြစ်ပါတယ်။ ထို့နောက် ကျွန်တော်တို့ဆက် ရိုက်ရမယ့် Command ကတော့ **select partition 1** ဆိုတာဖြစ် ပါတယ်။

```
Administrator: C:\Windows\System32\cmd.exe - diskpart

Disk 0 Online 298 GB 0 B
Disk 1 Online 14 GB 0 B
Disk 2 Online 3753 MB 0 B

DISKPART> select disk 2
Disk 2 is now the selected disk.
DISKPART> clean
DiskPart succeeded in cleaning the disk.
DISKPART> create partition primary
DiskPart succeeded in creating the specified partition.
DISKPART> select partition 1
Partition 1 is now the selected partition.
DISKPART>
```

ထို့နောက် ဆက်လက်ပီးတော့ရှိက်ရမယ့် Command က **active** ဆိုတာဖြစ်ပါတယ်။

```
Administrator: C:\Windows\System32\cmd.exe - diskpart

Disk 0 Online 298 GB 0 B
Disk 1 Online 14 GB 0 B
Disk 2 Online 3753 MB 0 B

DISKPART> select disk 2
Disk 2 is now the selected disk.
DISKPART> clean
DiskPart succeeded in cleaning the disk.
DISKPART> create partition primary
DiskPart succeeded in creating the specified partition.
DISKPART> select partition 1
Partition 1 is now the selected partition.
DISKPART> active
DiskPart marked the current partition as active.
DISKPART>
```

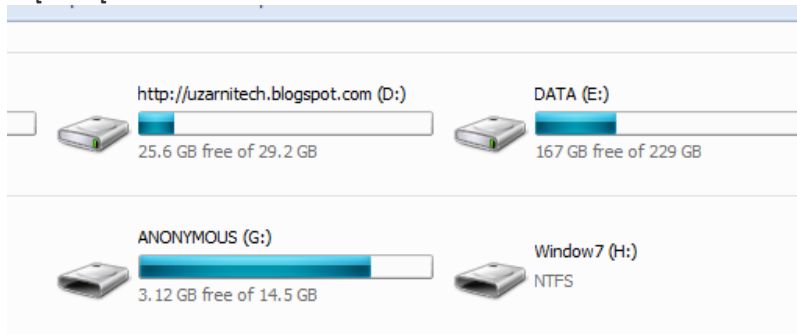
ဒါကတော့ အခုလက်ရှိသင်ရွေးချယ်သတ်မှတ်ထားတဲ့ Partition ကို အသက်ဝင်အောင် လုပ်လိုက်တာ ဖြစ်ပါတယ်။ထို့နောက်ရှိက်ရမှာက **Format fs=ntfs** ဆိုတာဖြစ်ပါတယ်။

```
Administrator: C:\Windows\System32\cmd.exe - diskpart

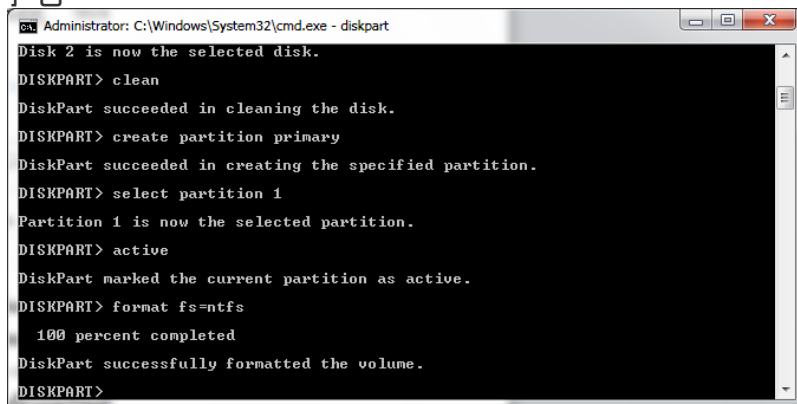
Disk 2 Online 3753 MB 0 B

DISKPART> select disk 2
Disk 2 is now the selected disk.
DISKPART> clean
DiskPart succeeded in cleaning the disk.
DISKPART> create partition primary
DiskPart succeeded in creating the specified partition.
DISKPART> select partition 1
Partition 1 is now the selected partition.
DISKPART> active
DiskPart marked the current partition as active.
DISKPART> format fs=ntfs
3 percent completed
```


ဒါကတော့ အခုလက်ရှိ Partition ကို NTFS File System အဖြစ် Format ချလိုက်တာဖြစ်ပါတယ်။
ဒီအချိန်မှာ သင်ဟာ My Computer ထဲမှာသွားကြည့်တဲ့အခါမှာတော့ သင့်ရဲ့ Stick ကအောက်
ပါပုံအတိုင်း



Busy Mode အနေဖြင့် ပြနေမှာပါ။ Formatting လုပ်နေတဲ့အချိန်မှာ အနည်းဆုံး ၁၀ မိနစ်နဲ့ ၁၅
မိနစ်ကြားမှာကြာတဲ့အတွက်ကြောင့် သင်ဟာ ဆေးလိပ်သောက်တတ်သူဆိုရင် အပြင်မှာ ဆေးလိပ်တစ်
လိပ် လောက် သွားသောက်ချိန်ရပါတယ်။ :P အားလုံးပီးသွားတဲ့အခါ မှာတော့အောက်ပါပုံအတိုင်း ပေါ်လာ
မှာဖြစ်ပါတယ်။



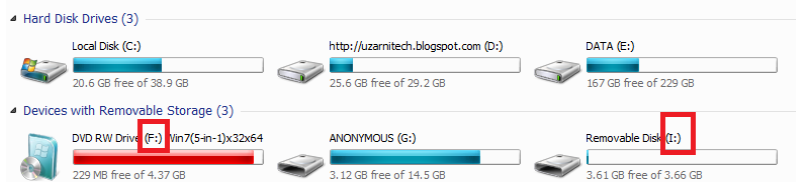
ဒါဆိုရင်တော့ သင့်ရဲ့ Stick ကို Formated ဖြစ်သွားပါပြီ ထို့နောက် ထပ်ရိုက် ရမယ့် Command ကတော့
assign ဖြစ်ပါတယ်။

```

Administrator: C:\Windows\System32\cmd.exe - diskpart
DiskPart succeeded in cleaning the disk.
DISKPART> create partition primary
DiskPart succeeded in creating the specified partition.
DISKPART> select partition 1
Partition 1 is now the selected partition.
DISKPART> active
DiskPart marked the current partition as active.
DISKPART> format fs=ntfs
    100 percent completed
DiskPart successfully formatted the volume.
DISKPART> assign
DiskPart successfully assigned the drive letter or mount point.
DISKPART>

```

ထို့နောက် တော့ လုပ်ဆောင်ချက် တစ်ဆင့်ပီးသွားပီဖြစ်တဲ့အတွက် ကြောင့် exit လို့ရိုက်လိုက်ပါမယ်။ ဒီနေရာမှာ လုပ်ဆောင်ချက် ပြီးသွား ပီဆိုပီးတော့ မပိတ်လိုက် ပဲနဲ့ Minimize ခဏလုပ် ထားလိုက်ပါ။ ကျွန်တော် တို့လုပ်ဆောင်ရ မယ့်အပိုင်းတွေကျန် ပါသေးတယ်။ ထို့နောက် သင့်ရဲ့ CD Drive ထဲကို ဝင်းဒိုး 7 သို့မဟုတ် Window 8 အခွေကိုထည့်လိုက်ပါမယ်။ ကျွန်တော်က တော့ Window7 ကို ထည့်လိုက် ပါတယ်။ ဒီနေရာမှာ တစ်ခု မှတ်ထားရမှာက (အရေးကြီး) သင့်ရဲ့ CD Drive Letter နဲ့ သင့်ရဲ့ Memory Stick Drive Letter တို့ပဲဖြစ်ပါတယ်။ ကျိန်းသေ အောင် ကျွန်တော်တို့က My Computer ထဲကနေသွားကြည့်ထား ပါမယ်။



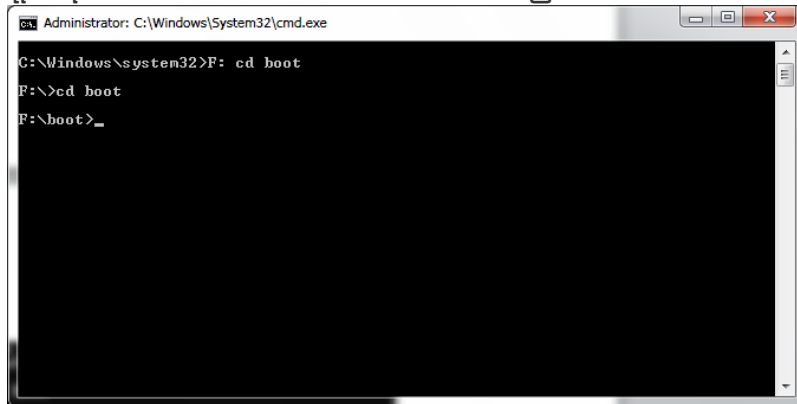
CD Drive ရဲ့ Drive Letter က အနီရောင်အကွက်ထဲက F ဖြစ်ပီး တော့ သင့် Stick ရဲ့ Drive Letter ကတော့ I ဖြစ်ပါတယ်။ ဒီတော့ ကျွန်တော်တို့ရိုက်ရမယ့် Command ကတော့ F: CD BOOT ဖြစ် ပါတယ်။

```

Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32\F: cd boot
F:\>

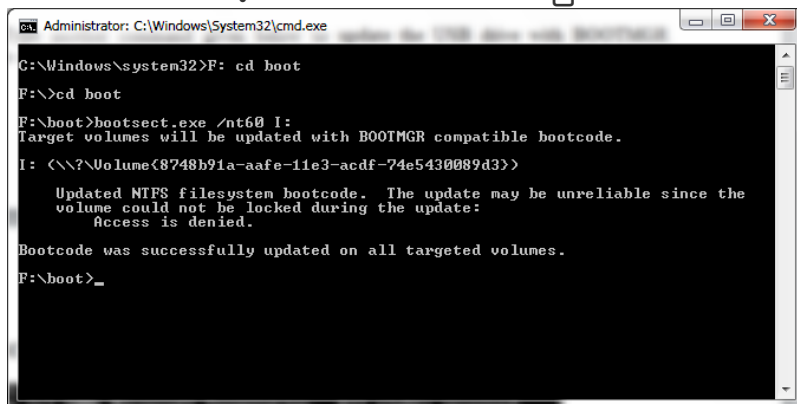
```

ဒါဆိုရင်သူက Drive Letter F (CD ROM) ထဲကိုရောက်သွားပါပြီ။ ဒီနောက်တော့ ကျွန်တော်တို့ ထပ်ပီး ရိုက်ရမယ့် Command ကတော့ **CD BOOT** ဖြစ်ပါတယ်။



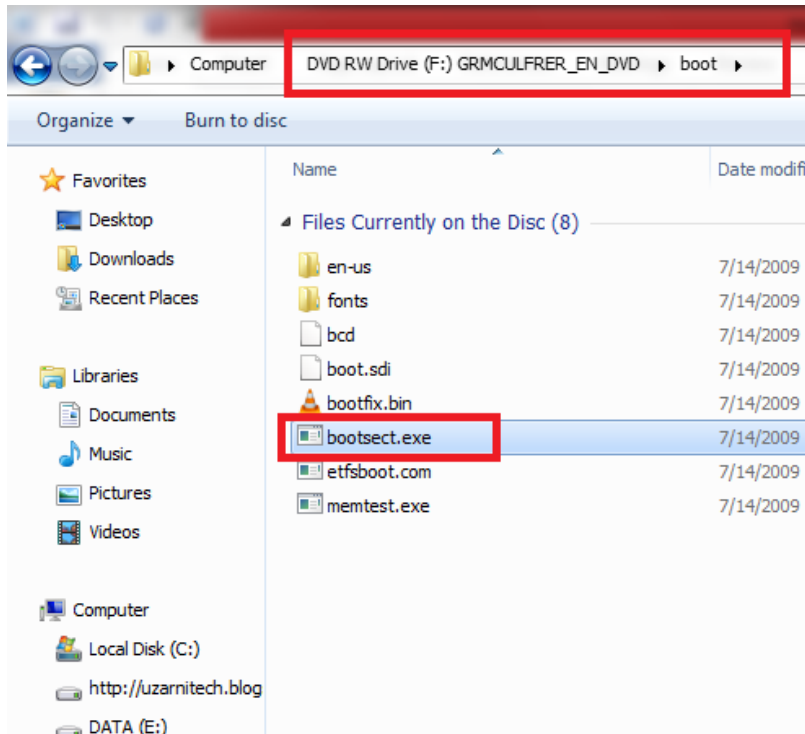
```
Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32>F: cd boot
F:\>cd boot
F:\boot>_
```

ဒါဆိုရင်တော့ အခွေထဲမှာရှိတဲ့ Boot Location ထဲကိုရောက်သွား ပါပြီ။ထို့နောက် ဆက်ရိုက်ရမယ့် Command ကတော့ **bootsect.exe /nt60 I:** ဖြစ်ပါတယ်။



```
Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32>F: cd boot
F:\>cd boot
F:\boot>bootsect.exe /nt60 I:
Target volumes will be updated with BOOTMGR compatible bootcode.
I: <\\?\Volume{8748b91a-aafe-11e3-acdf-74e5430089d3}>
    Updated NTFS filesystem bootcode. The update may be unreliable since the
    volume could not be locked during the update:
    Access is denied.
Bootcode was successfully updated on all targeted volumes.
F:\boot>_
```

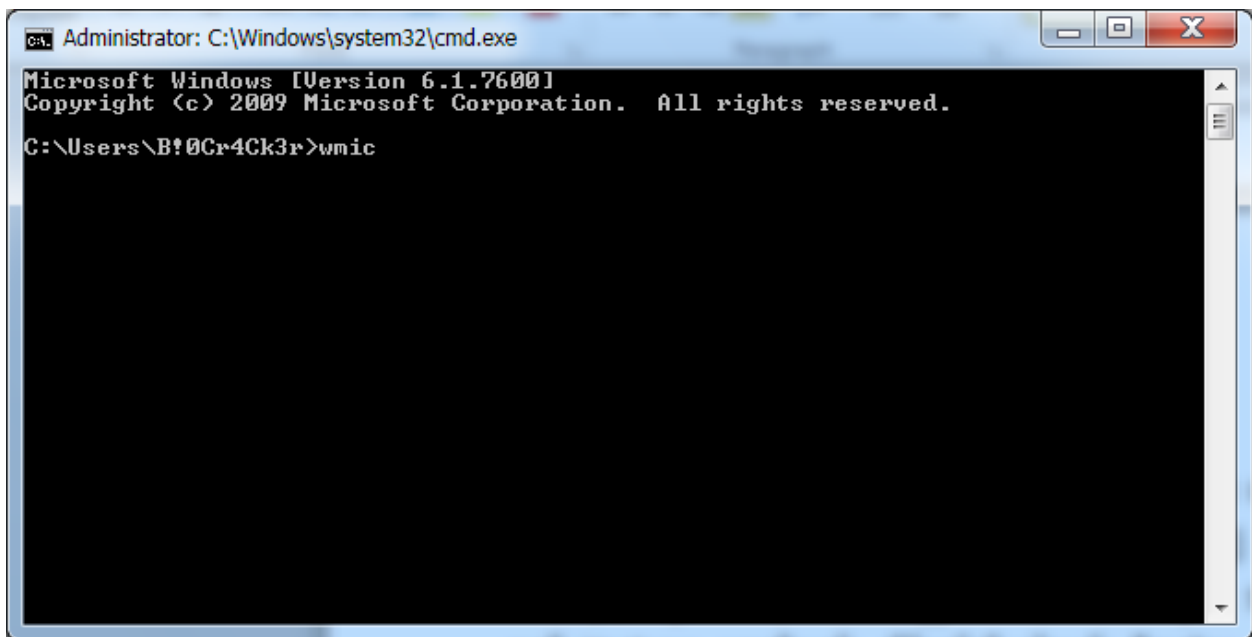
ဆိုလိုတာကတော့



အထက်ပါပုံအတိုင်းမှာ F:/boot ဆိုတဲ့ Folder ထဲက bootsect.exe ကိုအသုံးပြုပြီး သင့်ရဲ့ USB Stick ကို BOOTMGR ကို compatible ဖြစ်အောင် လုပ်ဆောင်လိုက်တာဖြစ်ပါတယ်။ ဒါမှလည်း သင့်ရဲ့ Stick က Bootable ဖြစ်ပြီး အထဲမှ Data တွေကိုဖတ်နိုင်မှာဖြစ်ပါတယ်။ ဒီအဆင့်တွေအားလုံးပီး သွားပါဆိုရင် တော့သင့်ရဲ့ Stick ထဲကို ဝင်းဒိုး အခွေထဲမှာပါတဲ့ Data တွေအားလုံးကို ရှိရှိ သာမန် Copy လုပ်ပြီး Pate လုပ်လိုက်ပါ။ ဒါဆိုရင်တော့ သင့်ရဲ့ Stick ထဲမှာ Window 7 Installation အတွက် အားလုံးအဆင်သင့်ဖြစ်သွားပါ ပီ။ ကျွန်တော်တို့က ၎င်း Stick ဖြင့်ဝင်းဒိုးတင်ချင်တဲ့အခါမှာတော့ BIOS ထဲမှာ First Boot Device ကို USB Stick ကိုရွေးချယ်ပေးပြီး Post တက်ခြင်းဖြင့် ဝင်းဒိုး စနစ်ကြီးတစ်ခုလုံးကို အခွေဖြင့် သွင်းသလို လုပ်ဆောင်နိုင်မှာဖြစ်ပါတယ်။

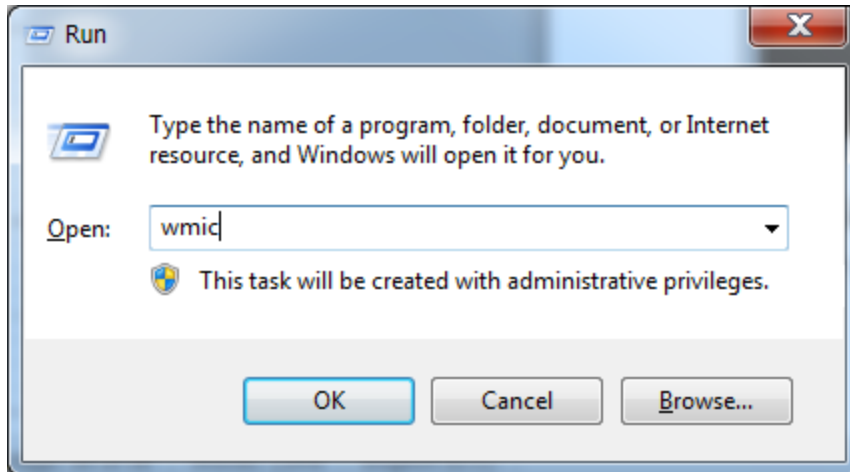
WMIC (Window Mangement Instrumentation Command)

Windows Management Instrumentation Command ဆိုတာကတော့ ကျွန်တော်တို့ ကွန်ပျူတာ စနစ်ကြီးထဲမှာ ရှိတဲ့အချက်အလက်တွေ၊ Remote Computer ရဲ့အချက်အလက်တွေကိုဖော်ပြပေးတဲ့ Command ဖြစ်ပါတယ်။တို့ပြင် အဲဒီစက်တွေကိုလှမ်းပြီး Configuration လုပ်နိုင်တာတွေကိုလည်းလုပ်လုပ်ဆောင်နိုင်ပါတယ်။ ဒီ WMIC ကတော့ အဓိကအားဖြင့် Vista/Windows 7, Windows XP Professional, တို့မှာပဲအလုပ်လုပ်ပြီးတော့ WindowXP Home Version မှာလုံးဝအလုပ်မလုပ်ပါဘူး။ ဒီ Command က ဘာတွေအထိလုပ်ဆောင်လုပ်ရသလည်းဆိုတော့ အဓိကအားဖြင့် Kernal Mode ထဲမှာဝင်ရောက်လုပ် ဆောင်ရတဲ့အတွက် အရမ်း သတိလည်းထားသင့်ပါတယ်။ သူက Software ကိုလည်းထိန်းချုပ်လို့ရနိုင် သလို Hardware တွေကိုလည်း ထိန်းချုပ်လို့ရပါတယ်။ ဒီအထဲကမှ အသုံးများတဲ့ Command အချို့ကို ပုံလေးတွေနဲ့ အသေးစိတ်ကောက်နှုတ်ဖော်ပြပေးပါမယ်။အရင်ဆုံး WMIC ထဲကိုဝင်ရောက်နိုင်ဖို့အတွက် ကိုကျွန်တော်တို့က Run ထဲကနေ cmd လို့ရှိက်ပြီး Command Prompt ပေါ်လာမှ

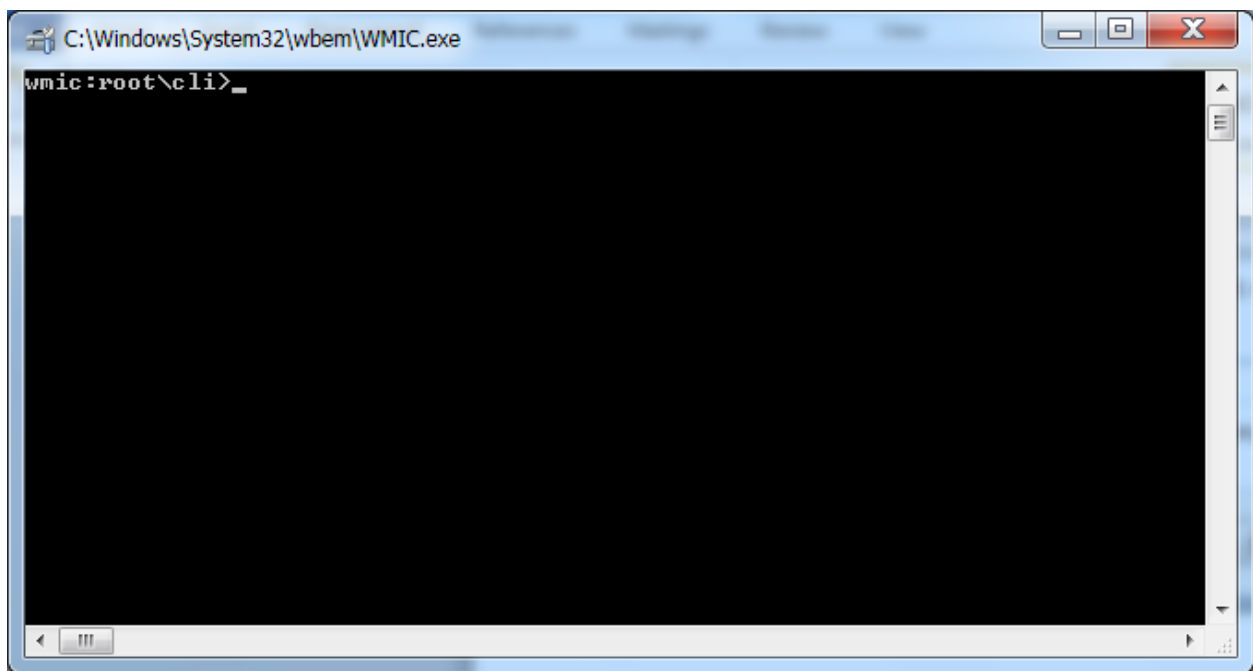
A screenshot of a Windows Command Prompt window. The title bar reads "Administrator: C:\Windows\system32\cmd.exe". The window content shows the following text: "Microsoft Windows [Version 6.1.7600] Copyright (c) 2009 Microsoft Corporation. All rights reserved. C:\Users\B!0Cr4Ck3r>wmic". The command prompt is currently at the end of the "wmic" command line.

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\B!0Cr4Ck3r>wmic
```

အထက်ပါပုံအတိုင်း " wmic " လို့ရှိက်ပြီးတော့လည်းဝင်ရောက်နိုင်သလို Run Box ထဲမှာပဲ တန်းပြီးတော့

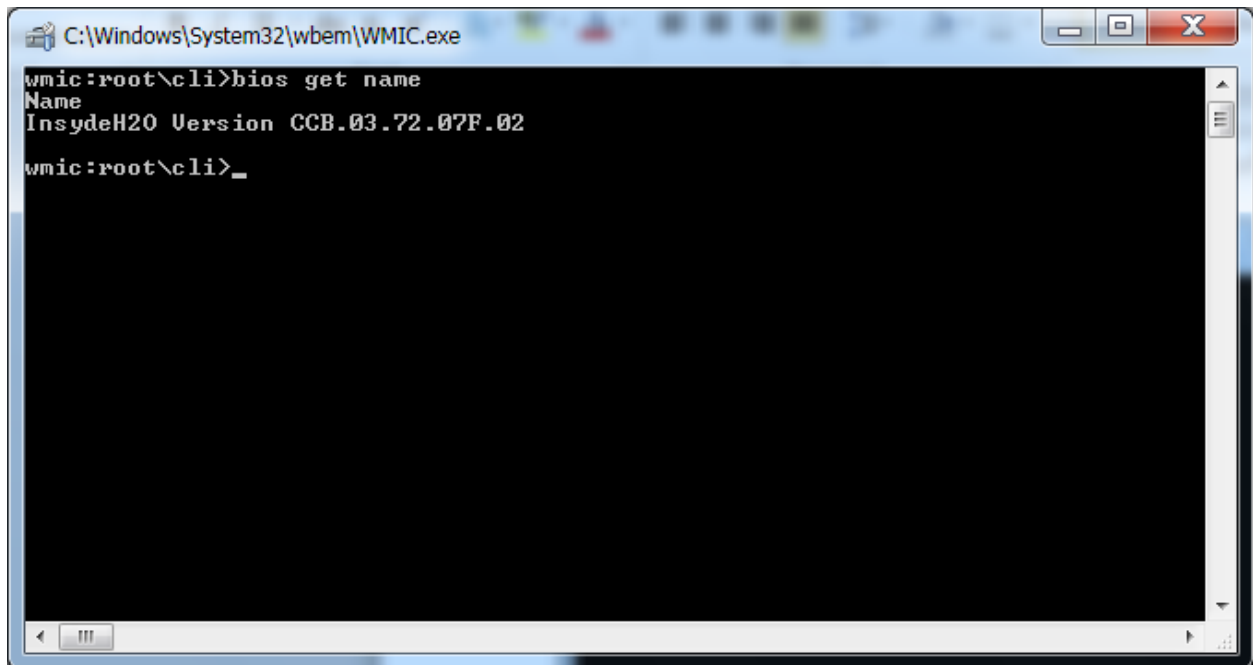


“wmic” လိုရိုက်ပြီးအထက်ပါပုံအတိုင်းဝင်လိုက်မယ်ဆိုရင်အောက်ပါပုံအတိုင်း



တန်းပြီးရောက်သွားမှာပါ။ ကဲစလိုက်ရအောင် အသုံးများတဲ့ Command လေးတွေအကြောင်းပေါ့....

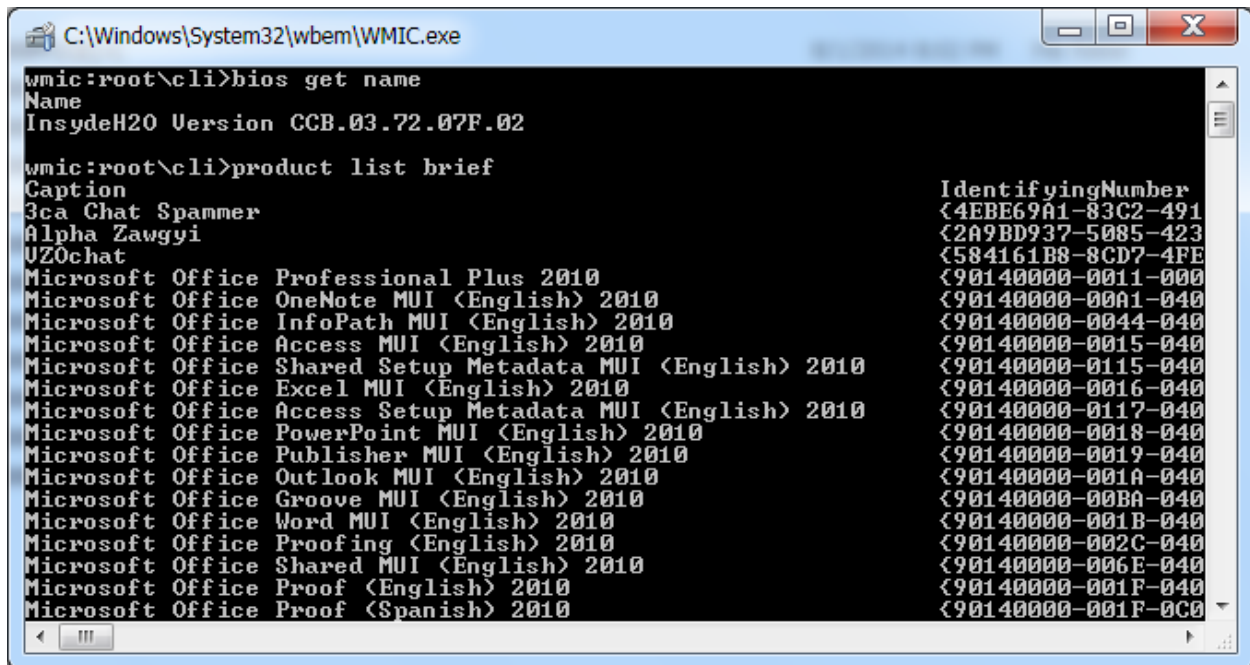
“ bios get name”



```
C:\Windows\System32\wbem\WMIC.exe
wmic:root\cli>bios get name
Name
InsydeH2O Version CCB.03.72.07F.02
wmic:root\cli>
```

bios get name ဆိုတာကတော့ သင့် Computer ရဲ့ BIOS အမည်နဲ့ Version ကိုသိချင်သောအခါမှာ အသုံးပြုသော Command ဖြစ်ပါတယ်။ ဘာကြောင့် မိမိ BIOS Version ကိုသိရမလည်းဆိုတော့ တစ်ခါတစ်လေမှာ ကျွန်တော်တို့ MB (Mother Board) ကသက်တမ်းကြာလာတဲ့အခါမှာ အထူးသဖြင့် မိမိ အသုံးပြုနေတဲ့ Mother Board မှာပါဝင်သော BIOS Chip ရဲ့ Version က နိမ့်လာတဲ့အခါမှာ နောက်ပိုင်း အသစ်ထွက်လာတဲ့ Software တွေနဲ့ Match အဖြစ်တာမျိုးတွေ၊ Hardware တွေထပ်စိုက်တဲ့ အခါမှာ အဆင်မပြေတာမျိုးတွေဖြစ်တတ်ပါတယ်။ BIOS ကိုဘယ်လို Update လုပ်ရမလည်းဆိုတာကို တော့ အလျဉ်းသင့်လျှင်ထပ်မံဖော်ပြပေးပါ့မယ်။

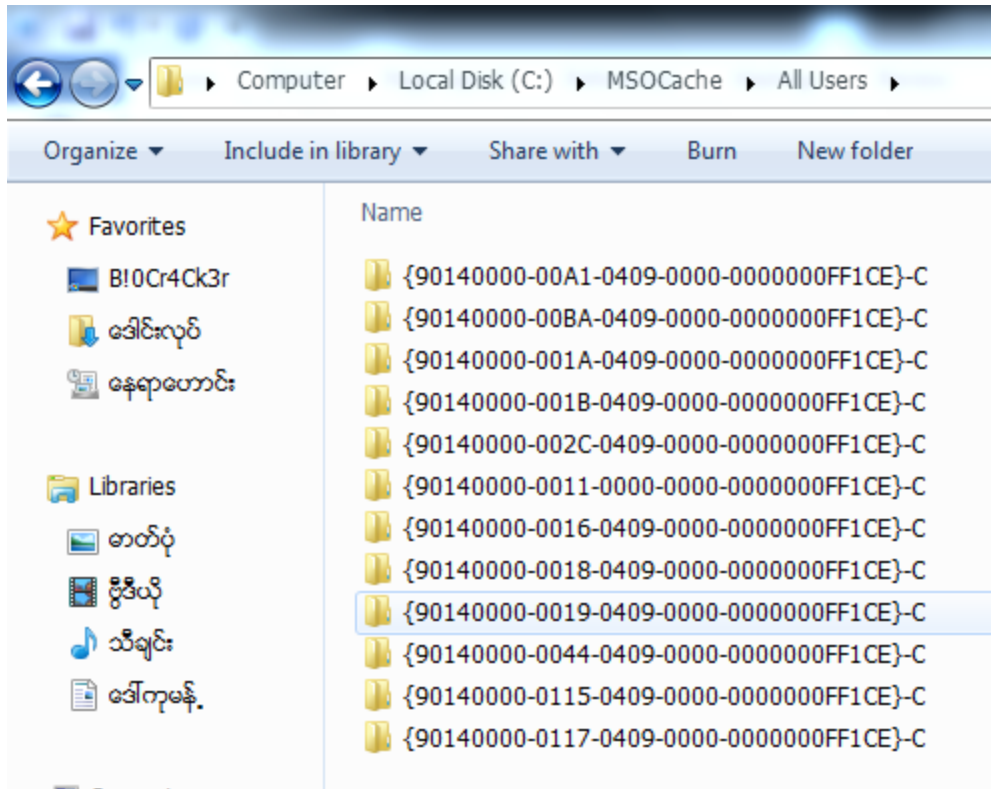
“ product list brief”



```
wmic:root\cli>bios get name
Name
InsydeH20 Version CCB.03.72.07F.02

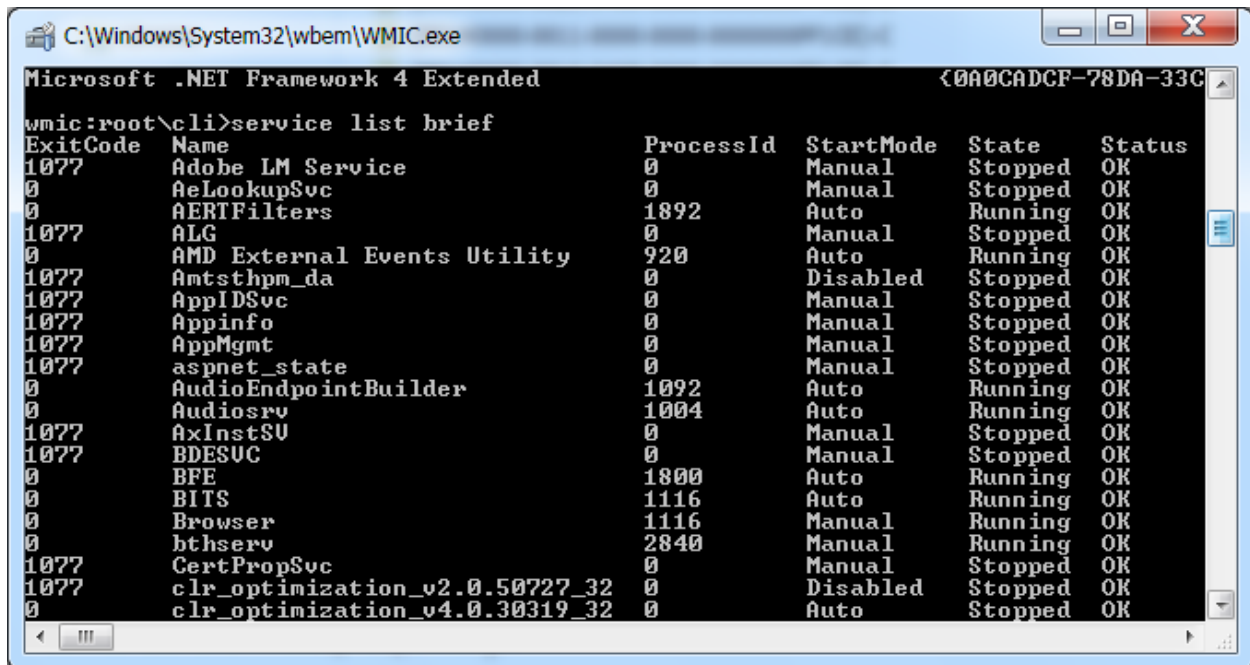
wmic:root\cli>product list brief
Caption                                                    IdentifyingNumber
3ca Chat Spammer                                           <4EBE69A1-83C2-491
Alpha Zawgyi                                               <2A9BD937-5085-423
UZ0chat                                                    <584161B8-8CD7-4FE
Microsoft Office Professional Plus 2010                  <90140000-0011-000
Microsoft Office OneNote MUI (English) 2010             <90140000-00A1-040
Microsoft Office InfoPath MUI (English) 2010            <90140000-0044-040
Microsoft Office Access MUI (English) 2010              <90140000-0015-040
Microsoft Office Shared Setup Metadata MUI (English) 2010 <90140000-0115-040
Microsoft Office Excel MUI (English) 2010                <90140000-0016-040
Microsoft Office Access Setup Metadata MUI (English) 2010 <90140000-0117-040
Microsoft Office PowerPoint MUI (English) 2010           <90140000-0018-040
Microsoft Office Publisher MUI (English) 2010            <90140000-0019-040
Microsoft Office Outlook MUI (English) 2010              <90140000-001A-040
Microsoft Office Groove MUI (English) 2010               <90140000-00BA-040
Microsoft Office Word MUI (English) 2010                 <90140000-001B-040
Microsoft Office Proofing (English) 2010                 <90140000-002C-040
Microsoft Office Shared MUI (English) 2010               <90140000-006E-040
Microsoft Office Proof (English) 2010                    <90140000-001F-040
Microsoft Office Proof (Spanish) 2010                    <90140000-001F-0C0
```

Product list brief ဆိုတာကတော့ သင့်စက် Install လုပ်ထားတဲ့ Software တွေရဲ့ အမည်အချို့နဲ့ identifying Number တွေကိုဖော်ပြပေးတာဖြစ်ပါတယ်။ ဒီနေရာမှာတစ်ခုပြောချင်တာက အနောက်က Identifying Number တွေဆိုတာကိုပဲဖြစ်ပါတယ်။ ဒါတွေကတော့ သင်တို့ စက်ထဲမှာ သင်ကတော့ မိမိစက်ကို Program တွေကို အသုံးပြုလိုက်တာပဲ ဒါပေမယ့် အခုဒီ List ထဲမှာပြထားတဲ့ Number တွေထဲက လက်ရှိသုံးနေတဲ့ Program တွေရဲ့ Cache တွေကော သုံးခဲ့တဲ့ Program တွေရဲ့ Cache တွေကို သိမ်းထားတဲ့နေရာလေးတစ်ခုရှိပါတယ်။ အဲဒီနေရာကတော့ကျွန်တော်တို့



အထက်ပါပုံအတိုင်း C:\MSOCache\All Users ထဲမှာရှိနေပါတယ်။ ဒီနေရာက ဟာတွေကတော့ သင့်အတွက် မလိုအပ်တဲ့ Cache File တွေပဲဖြစ်ပါတယ်။ထိုစဉ်အားလုံးကို Select All ပေးပြီး Shift Delete လုပ်နိုင်ပါတယ်။

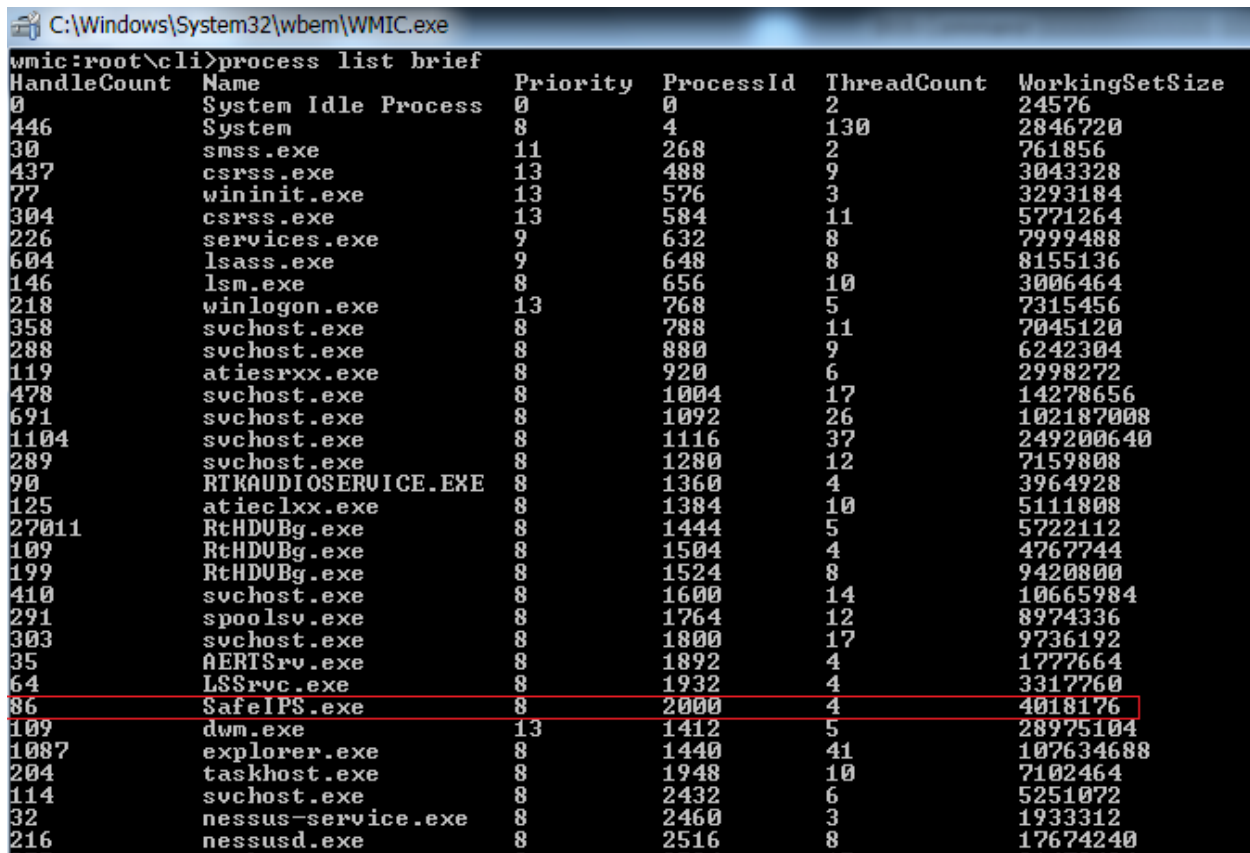
“ service list brief”



```
Microsoft .NET Framework 4 Extended
wmic:root\cli>service list brief
ExitCode Name ProcessId StartMode State Status
1077 Adobe LM Service 0 Manual Stopped OK
0 AelookupSvc 0 Manual Stopped OK
0 AERTIFilters 1892 Auto Running OK
1077 ALG 0 Manual Stopped OK
0 AMD External Events Utility 920 Auto Running OK
1077 Amtsthp_da 0 Disabled Stopped OK
1077 AppIDSvc 0 Manual Stopped OK
1077 Appinfo 0 Manual Stopped OK
1077 AppMgmt 0 Manual Stopped OK
1077 aspnet_state 0 Manual Stopped OK
0 AudioEndpointBuilder 1092 Auto Running OK
0 Audiosrv 1004 Auto Running OK
1077 AxInstSU 0 Manual Stopped OK
1077 BDESVC 0 Manual Stopped OK
0 BFE 1800 Auto Running OK
0 BITS 1116 Auto Running OK
0 Browser 1116 Manual Running OK
0 bthserv 2840 Manual Running OK
1077 CertPropSvc 0 Manual Stopped OK
1077 clr_optimization_v2.0.50727_32 0 Disabled Stopped OK
0 clr_optimization_v4.0.30319_32 0 Auto Stopped OK
```

Service List Brief ကတော့ သင့်စက်ထဲမှာ လက်ရှိ Run နေတဲ့ Services Mode တွေအကုန်လုံးကို ဖော်ပြပေးထားတာဖြစ်ပါတယ်။ ဆိုလိုတာကတော့ ကျွန်တော်တို့ GUI Mode ထဲမှာ Services.msc ထဲက နေ သွားကြည့်သလိုပါပဲ ဘယ် Services တွေကတော့ Run နေတယ်။ ဘယ် Services တွေက တော့ ရပ်နေ တယ်ဆိုတာကိုအပြင် ထို Services များအတွက် Code တွေကအစဖော်ပြပေးတာဖြစ် ပါ တယ်။

“process list brief”



C:\Windows\System32\wbem\WMIC.exe					
wmic:root\cli>process list brief					
HandleCount	Name	Priority	ProcessId	ThreadCount	WorkingSetSize
0	System Idle Process	0	0	2	24576
446	System	8	4	130	2846720
30	smss.exe	11	268	2	761856
437	csrss.exe	13	488	9	3043328
77	wininit.exe	13	576	3	3293184
304	csrss.exe	13	584	11	5771264
226	services.exe	9	632	8	7999488
604	lsass.exe	9	648	8	8155136
146	lsmon.exe	8	656	10	3006464
218	winlogon.exe	13	768	5	7315456
358	svchost.exe	8	788	11	7045120
288	svchost.exe	8	880	9	6242304
119	atiesrxx.exe	8	920	6	2998272
478	svchost.exe	8	1004	17	14278656
691	svchost.exe	8	1092	26	102187008
1104	svchost.exe	8	1116	37	249200640
289	svchost.exe	8	1280	12	7159808
90	RTKAUDIOSERVICE.EXE	8	1360	4	3964928
125	atieclxx.exe	8	1384	10	5111808
27011	RtHDUBg.exe	8	1444	5	5722112
109	RtHDUBg.exe	8	1504	4	4767744
199	RtHDUBg.exe	8	1524	8	9420800
410	svchost.exe	8	1600	14	10665984
291	spoolsv.exe	8	1764	12	8974336
303	svchost.exe	8	1800	17	9736192
35	ALERTSvc.exe	8	1892	4	1777664
64	LSSrv.exe	8	1932	4	3317760
86	SafeIPS.exe	8	2000	4	4018176
109	dwm.exe	13	1412	5	28975104
1087	explorer.exe	8	1440	41	107634688
204	taskhost.exe	8	1948	10	7102464
114	svchost.exe	8	2432	6	5251072
32	nessus-service.exe	8	2460	3	1933312
216	nessusd.exe	8	2516	8	17674240

Process list brief ဆိုတာကတော့ သင့်စက်ထဲမှာလက်ရှိ Run နေတဲ့ Process တွေအားလုံးကိုဖော်ပြပေးမှာပါ။ Process List ကို GUI Mode ကနေကြည့်ချင်တဲ့အခါမှာတော့ ကျွန်တော်တို့က TaskManager ကိုခေါ်ပြီးကြည့်ရပါတယ်။ TaskManager ထဲမှာ မဖော်ပြပေးနိုင်တဲ့ အခြားသော Process တွေကို ကျွန်တော်တို့ ဒီ WMIC ရဲ့ process list brief ထဲမှာဖော်ပြပေးနိုင်ပါတယ်။ အထက်ပါပုံအတိုင်းမှာ အနီရောင်လေးထောင့်ကွက်ထဲကဟာလိုမျိုးပေါ့... အဲဒီမှာတစ်ခုပြောချင်တာက ကျွန်တော်တို့ GUI ရဲ့ TaskManager ထဲမှာ Process End လုပ်ချင်တယ်ဆိုရင် မိမိရပ်ချင်တဲ့ Process ကို Select ပေး End Process Tree လုပ်လိုကရင် ရပါတယ်။ ဒီမှာကတော့ Process ကို Kill လုပ်ချင်တယ်ဆိုရင် အနီရောင်ကွက် လေးထဲက အတိုင်းမှ ProcessID ကိုမှတ်ရမှာပါ အဲဒီမှာ ဥပမာအနေနဲ့ SafeIPS.exe ဆိုတာကိုကျွန်တော်က ရပ်ချင်တာပါ။ အဲဒီကောင်ရဲ့ ProcessID ကတော့ “2000” ဖြစ်ပါတယ်။ ဒီတော့ ကျွန်တော်တို့က အဲဒီကောင်ကိုရပ်ဖို့က

```
C:\Windows\System32\wbem\WMIC.exe
wmic:root\cli>process delete
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="0"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="4"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="268"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="488"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="576"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="584"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="632"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="648"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="656"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="768"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="788"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="880"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="920"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="1004"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="1092"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="1116"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="1280"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="1360"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="1384"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="1444"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="1504"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="1524"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="1600"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="1764"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="1800"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="1892"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="1932"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="2000"' (Y/N/?)? y
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="1412"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="1440"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="1948"' (Y/N/?)? n
Delete '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="2432"' (Y/N/?)? n
```

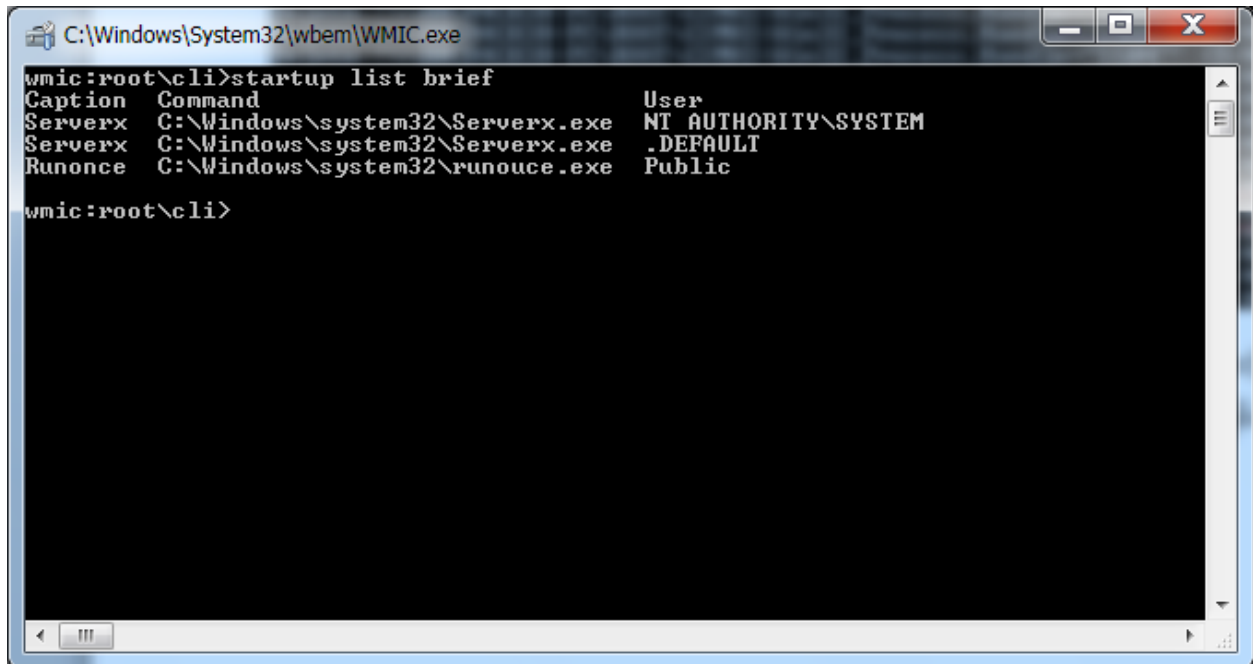
ကျွန်တော်တို့က process delete ဆိုပြီးဂိုက်လိုက်ပါမယ်။ ထို့နောက် မိမိသတ်မှတ်ထားတဲ့ 2000 ဆိုတာ မရောက်မချင်း "n" ဆိုတာကိုပဲနှိပ်ပြီး ရောက်လာပြီဆိုရင်တော့ "Y" ကိုနှိပ်ပေးလိုက်ရမှာဖြစ်ပါတယ်။ နောက်တစ်နည်းကတော့ ကျွန်တော်တို့က

```
C:\Windows\System32\wbem\WMIC.exe
wmic:root\cli>process where name="explorer.exe" call terminate
Execute '\\B0CR4CK3R-PC\ROOT\CIMV2:Win32_Process.Handle="1440"'->terminate() (Y/N/?)? y
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
    ReturnValue = 0;
};
wmic:root\cli>
```

Explorer.exe ကို ရပ်ချင်တယ်ဆိုရင် ကျွန်တော်တို့ရိုက်ရမယ့် Command က

"process where name="explorer.exe" call terminate" ဆိုပြီးရိုက်လိုက်ပါမယ်။ ဒါဆိုရင်သူက အဲဒီ Process ကို တစ်ကယ် Terminate လုပ်မှာလားလို့ မေးပါလိမ့်မယ်။ ဒီအခါမှာ ကျွန်တော်တို့က "Y" ကို ရွေးပေးလိုက်ပါမယ်။

" startup list brief"

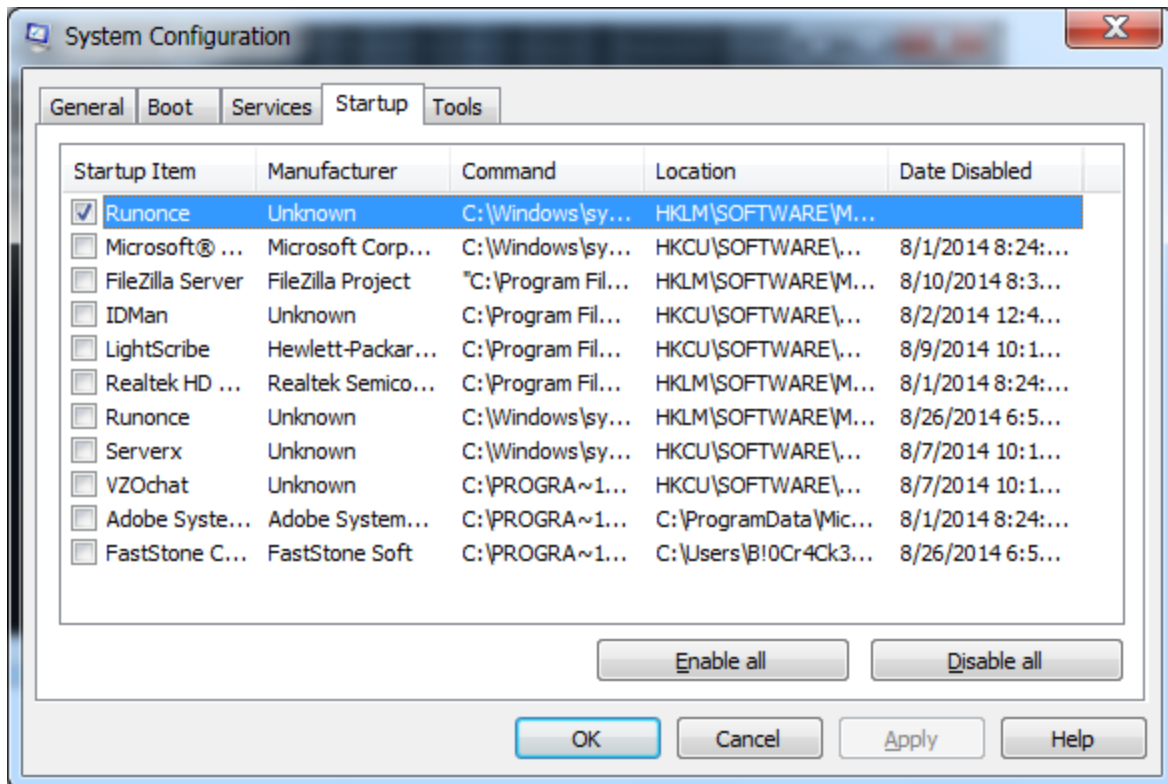


```
wmic:root\cli>startup list brief
```

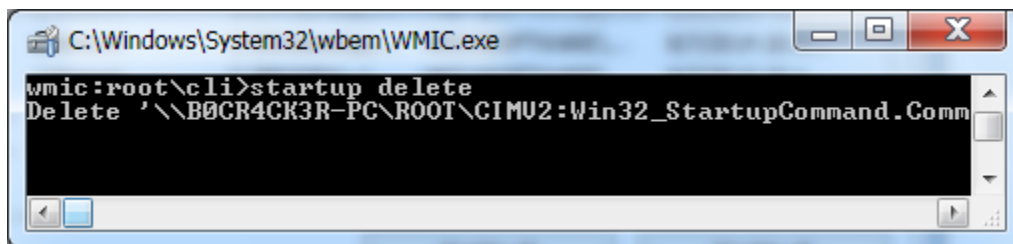
Caption	Command	User
Serverx	C:\Windows\system32\Serverx.exe	NT AUTHORITY\SYSTEM
Serverx	C:\Windows\system32\Serverx.exe	.DEFAULT
Runonce	C:\Windows\system32\runouce.exe	Public

```
wmic:root\cli>
```

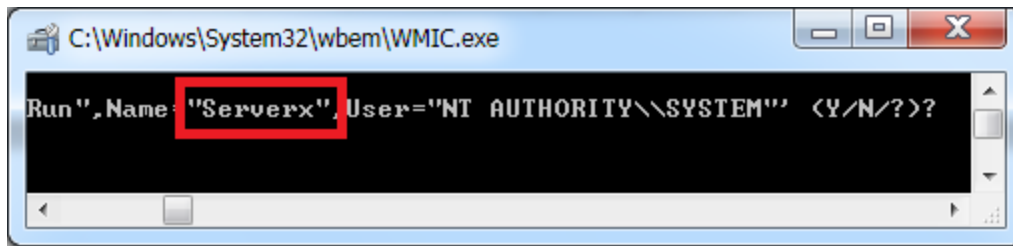
Startup list brief ဆိုတာကတော့ ကျွန်တော်တို့ ဝင်းဒိုးပေါ်က msconfig လို့ရိုက်ပြီး Start up ထဲမှာပါ တဲ့အတိုင်း



အထက်ပါပုံအတိုင်းမှ ဝင်းဒိုးတက်တက်ချင်းမှာ Run မယ့် Services တွေကိုဖော်ပြပေးတာမျိုးနဲ့ အလားသဏ္ဌာန် တူပါတယ်။တစ်ခါတစ်လေ ကျွန်တော်တို့က ဝင်းဒိုးပေါ်ကနေ အဲဒီ Startup တွေကိုဘယ်လိုပိတ်ပိတ် ပိတ်လို့မရတာမျိုးတွေကြုံဖူးကြမှာပါ။ ဒီလိုအခါမှာတော့ ကျွန်တော်တို့က ဒီထဲကနေ ရှိကရမယ့် Command ကတော့ **startup delete** ဆိုပြီးဖြစ်ပါတယ်။ ဒါဆိုရင်တော့

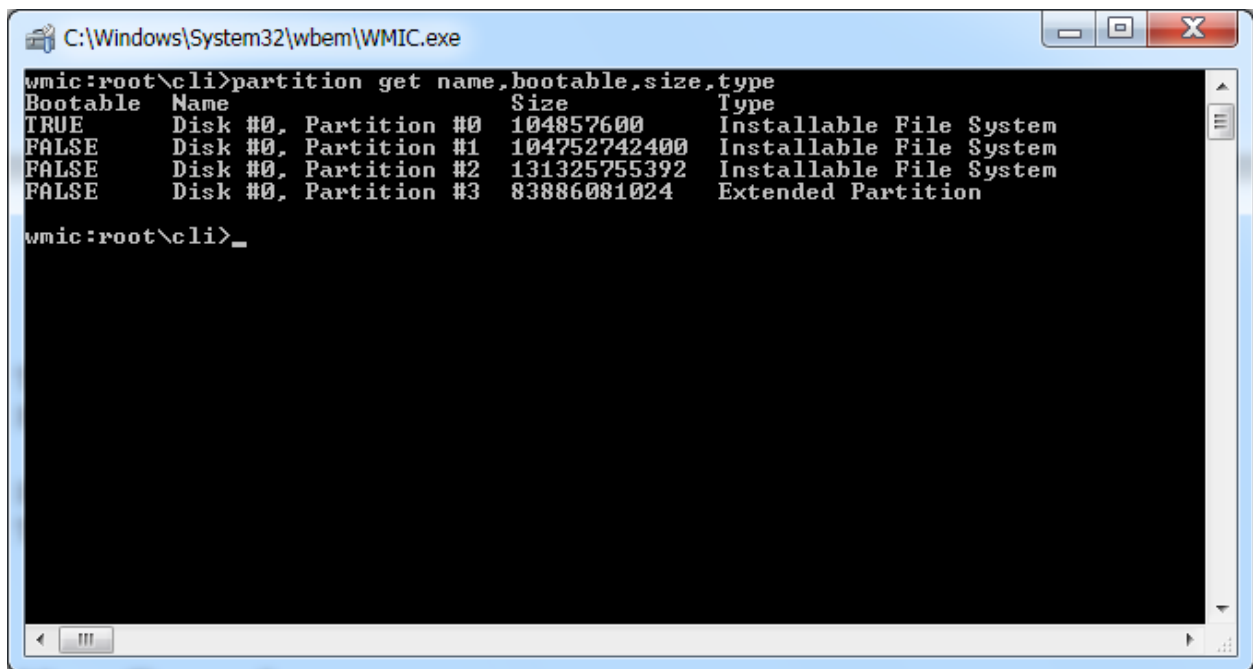


အထက်ပါပုံအတိုင်း startup delete လို့ဂိုက်လိုက်ပါမယ်။ ဒီအခါမှာ အောက်နားလေးက Scroll Bar လေးကိုဆွဲလိုက်ပါ မိမိ ဖျက်ချင်တဲ့ ဟာလားဆိုတာသေချာစစ်ပါ။ အပေါ်မှာပြထားတဲ့ Process ၃ ခုဟုတ်မဟုတ်ဆိုတာကိုပေါ့



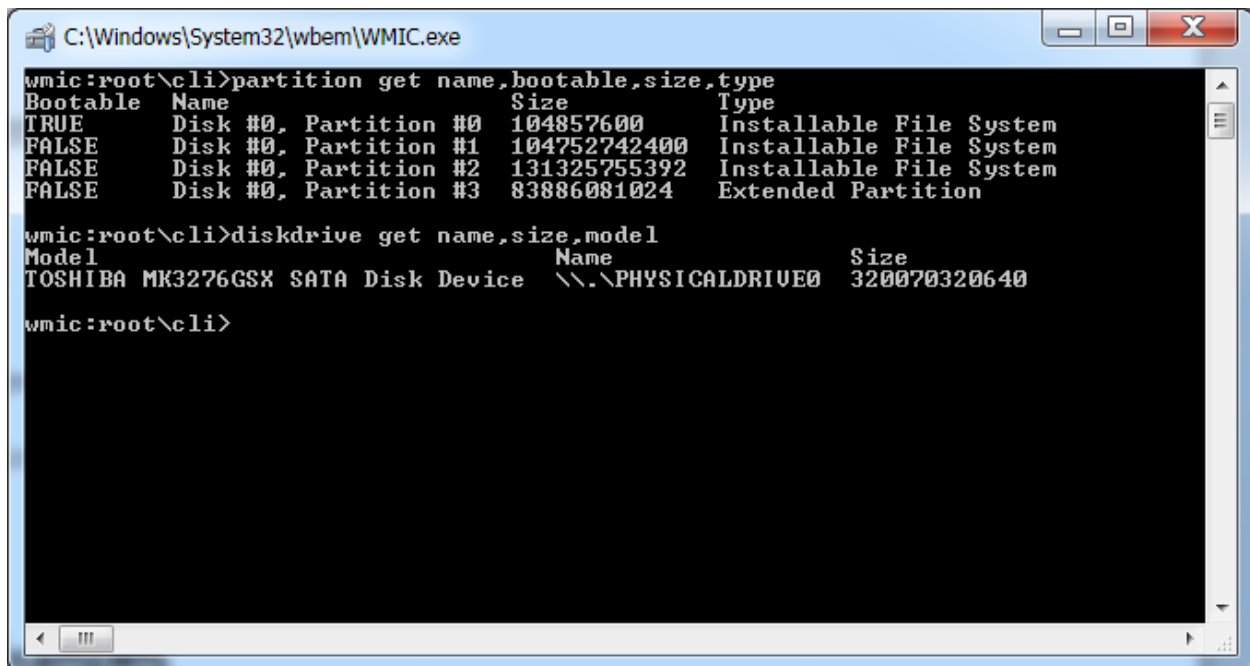
ဟုတ်တယ်ဆိုရင်တော့ ကျွန်တော်တို့က Y ကိုနှိပ်ပေးလိုက်ပါမယ်။ ဒီနည်းနဲ့အခြားသော Process တွေကိုလည်း ဖျက်နိုင်ပါတယ်။

“ Boot File ဘယ်နားမှာရှိသလည်းနဲ့ Partition တွေ Size တွေဘယ်လောက်ရှိသလည်း”



ကျွန်တော်တို့ မိမိကွန်ပျူတာ System ရဲ့ HDD မှာ Partition ဘယ်နှခုရှိသလည်း Boot Partition ကဘယ်မှာလည်း Size တွေဘယ်လောက်ရှိသလည်းနာမည်တွေကဘာလည်းကြည့်ချင်တဲ့အခါမှာအဓိကသုံးပါတယ်။ ရိုက်ရမယ့် Command ကတော့

“partition get name,bootable,size,type” ဆိုပြီးတော့ဖြစ်ပါတယ်။ အထက်ပါပုံအတိုင်းပေါ့။နောက်ထပ်တစ်ချက်ကတော့

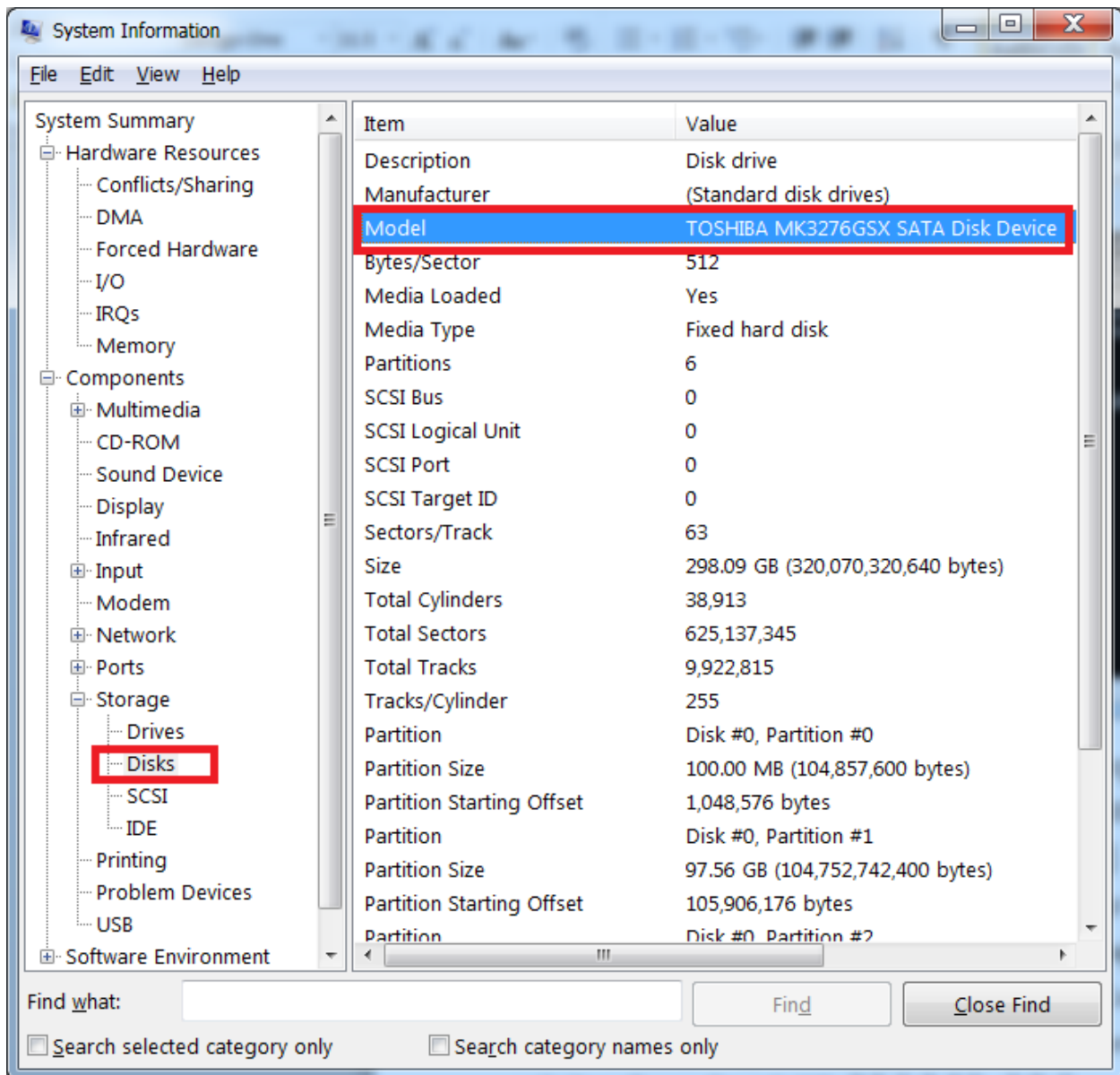


```
wmic:root\cli>partition get name,bootable,size,type
Bootable Name Size Type
TRUE Disk #0, Partition #0 104857600 Installable File System
FALSE Disk #0, Partition #1 104752742400 Installable File System
FALSE Disk #0, Partition #2 131325755392 Installable File System
FALSE Disk #0, Partition #3 83886081024 Extended Partition

wmic:root\cli>diskdrive get name,size,model
Model Name Size
TOSHIBA MK3276GSX SATA Disk Device \\.\PHYSICALDRIVE0 320070320640

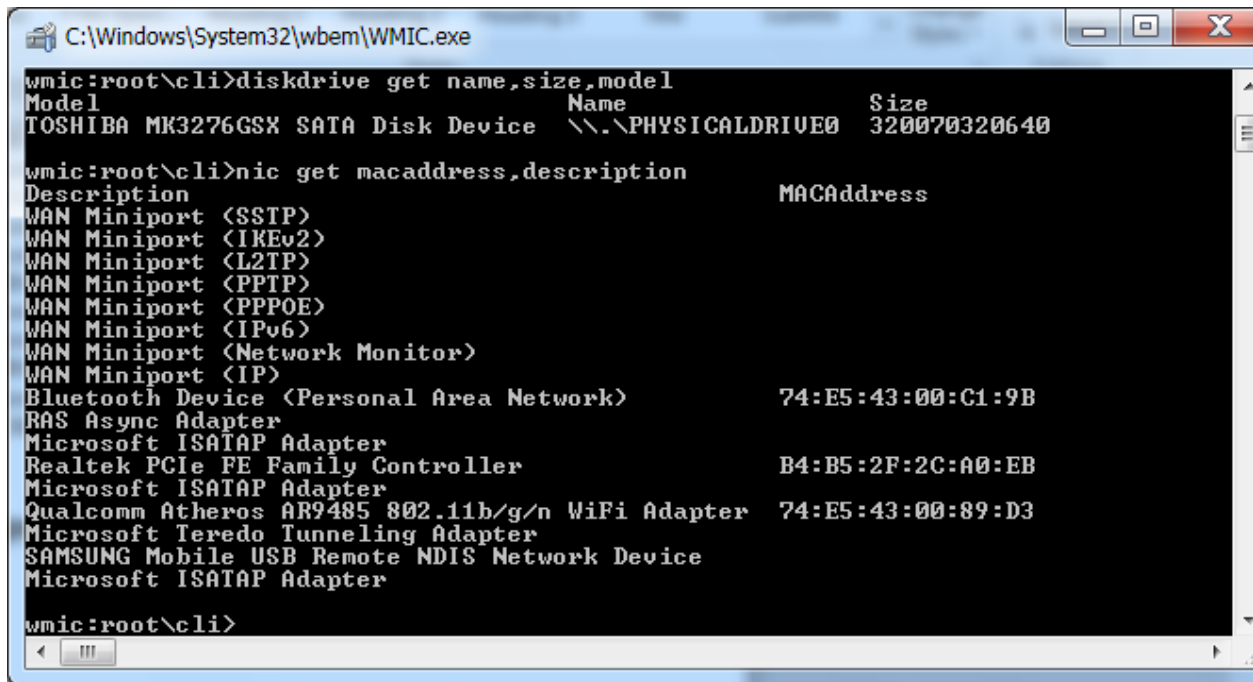
wmic:root\cli>
```

ကျွန်တော်တို့က လက်ရှိ HDD ရဲ့ နာမည် Modle နံပါတ်တွေ Size တွေကိုသိချင်တဲ့အခါမှာသုံးပါတယ်။ အထက်ပါပုံအတိုင်းမှာတော့ Model ဆိုတဲ့နေရာမှာ TOSHIBA MK3276GSX SATA လို့ပြပြီး Size မှာကတော့ ကျွန်တော့် HDD က 320GB ရှိတဲ့အတွက်ကြောင့် Size နေရာမှာ 320070320640 လို့ပြတာ ဖြစ်ပါတယ်။ တစ်ကယ်ဆိုရင် Desktop မှာပဲဖြစ်ဖြစ်၊ Laptop မှာပဲဖြစ်ဖြစ် Model Number တွေ Size ရှိတယ် Disk ရဲ့ Size ကိုတော့ "diskmgmt.msc" ထဲကနေကြည့်လို့နိုင်ပါတယ်။အများသတိမထားမိတဲ့ အချက်ကလေးတစ်ခုရှိပါတယ်။ မိမိ စက်ထဲက Hardware Component တွေရဲ့ အသေးစိတ် အချက်အလက်တွေကိုကြည့်ဖို့နည်းပါ။ အခု ကျွန်တော်အပေါ်က Command နဲ့ပဲ ယှဉ်ပြီးပြောပြပေးပါ့ မယ်။အရင် ဆုံး Run ထဲကနေ "msinfo32" လို့ရှိုက်လိုက်ပါ။ ဒါဆိုရင်



အထက်ပါပုံအတိုင်းမှ လိပ်စာအတိုင်းလည်းသွားရောက်စစ်ဆေးနိုင်ပါတယ်။

“nic”



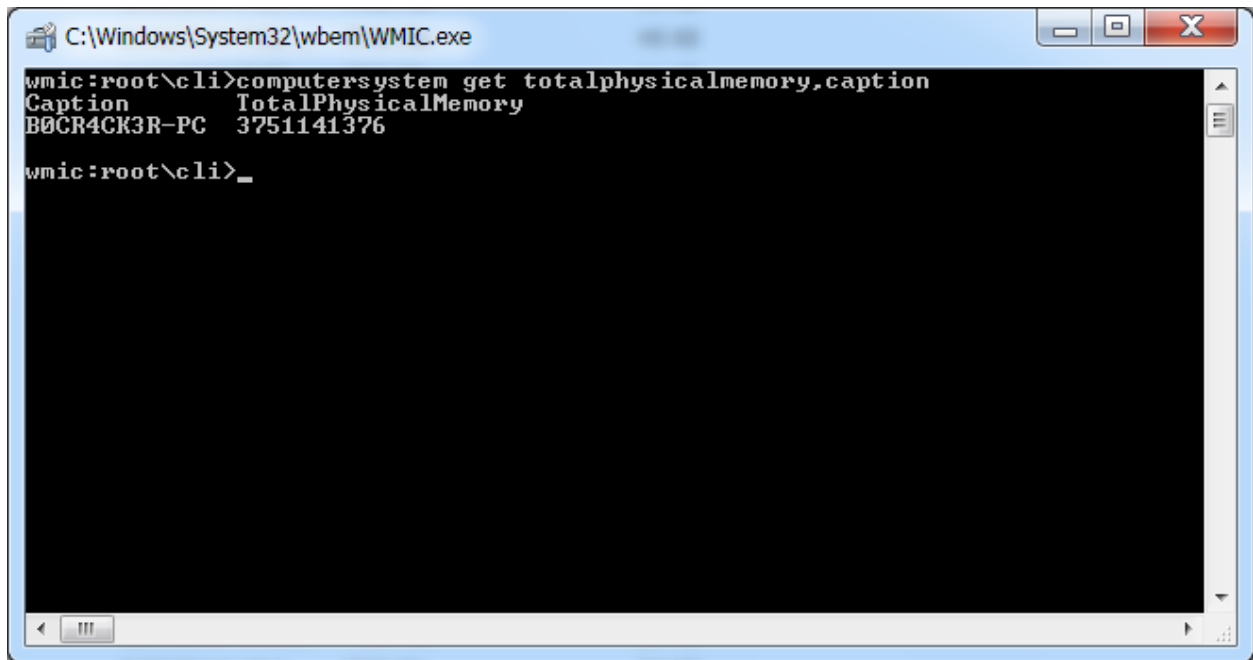
```
C:\Windows\System32\wbem\WMIC.exe
wmic:root\cli>diskdrive get name,size,model
Model Name Size
TOSHIBA MK3276GSX SATA Disk Device \\.\\PHYSICALDRIVE0 320070320640

wmic:root\cli>nic get macaddress,description
Description MACAddress
WAN Miniport (SSTP)
WAN Miniport (IKEv2)
WAN Miniport (L2TP)
WAN Miniport (PPTP)
WAN Miniport (PPPOE)
WAN Miniport (IPv6)
WAN Miniport (Network Monitor)
WAN Miniport (IP)
Bluetooth Device (Personal Area Network) 74:E5:43:00:C1:9B
RAS Async Adapter
Microsoft ISATAP Adapter
Realtek PCIe FE Family Controller B4:B5:2F:2C:A0:EB
Microsoft ISATAP Adapter
Qualcomm Atheros AR9485 802.11b/g/n WiFi Adapter 74:E5:43:00:89:D3
Microsoft Teredo Tunneling Adapter
SAMSUNG Mobile USB Remote NDIS Network Device
Microsoft ISATAP Adapter

wmic:root\cli>
```

Nic ဆိုတာကတော့ အများသိတဲ့အတိုင်းပဲ Network Interface Card ပဲဖြစ်ပါတယ်။ NIC နဲ့ပတ်သက်ပြီး ဘာတွေလုပ်လို့ရသလည်းဆိုတော့ အပေါ်က Command အတိုင်း “nic get macaddress,description” ဆိုပြီးရှိုက်လိုက်တဲ့အခါမှာတော့ သင့်စက်ရဲ့ Network Card ရဲ့ MAC Address တွေ အသေးစိတ် အကြောင်းအရာတွေကိုဖော်ပြပေးမှာဖြစ်ပါတယ်။

“computersystem”



```
C:\Windows\System32\wbem\WMIC.exe
wmic:root\cli>computersystem get totalphysicalmemory,caption
Caption          TotalPhysicalMemory
B0CR4CK3R-PC     3751141376
wmic:root\cli>
```

ဒီ Command ကတော့ ကျွန်တော်တို့ ကွန်ပျူတာမှာရှိတဲ့ Physical Memory ရဲ့ ပမာဏကိုကြည့်ချင် တဲ့အခါမှာသုံးတာဖြစ်ပါတယ်။ရိုက်ရမယ့် Command ကတော့

“computersystem get totalphysicalmemory,caption” ဖြစ်ပါတယ်။ ဒါဆိုရင်တော့လက်ရှိ သင့် ကွန်ပျူတာရဲ့ Memory ရဲ့ ပမာဏကိုအတိအကျဖော်ပြပေးမှာဖြစ်ပါတယ်။ GUI ပေါ်မှာဆိုရင်တော့ My Computer ကို Right Click ထောက်ပြီး Properties ထဲဝင်ကြည့်ရင်ရပါတယ်။

“cpu get”

```
Administrator: C:\Windows\system32\cmd.exe - wmic
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\B!0Cr4Gk3r>wmic
wmic:root\cli>cpu get MaxClockSpeed
MaxClockSpeed
1300

wmic:root\cli>
```

Cpu get MaxClockSpeed ဆိုတာကတော့ လက်ရှိသင့်ကွန်ပျူတာမှာ အလုပ်လုပ်နေတဲ့ CUP ရဲ့ Speed ကိုဖော်ပြပေးစေချင်တဲ့အခါမှာသုံးတာဖြစ်ပါတယ်။

“cpu list”

```
Administrator: Cristiano Zarni - wmic
C:\Users\B!0Cr4Gk3r>wmic
wmic:root\cli>cpu list
AddressWidth  Architecture  Availability  Caption  Conf
32            9              3             x64 Family 20 Model 2 Stepping 0

wmic:root\cli>
```

Cpu list ဆိုတာကတော့ လက်ရှိ သင့် ကွန်ပျူတာထဲမှာ ရှိသော CPU (Central Processing Unit) ရဲ့ အသေးစိတ် အချက်အလက်တွေဖြစ်သော

Current Clock Speed လက်ရှိ CPU ရဲ့ Clock Speed...

Current Voltage လက်ရှိ CPU မှာ လုပ်ဆောင်နေတဲ့ Voltage တွေကိုအသေးစိတ်ဖော်ပြပေးတယ်။

Data Width ဆိုတာကတော့သင့် OS အတွက် Run နိုင်တဲ့ စနစ်ကိုဖော်ပြတာပါ။ဥပမာ- 64 လား 32 လား

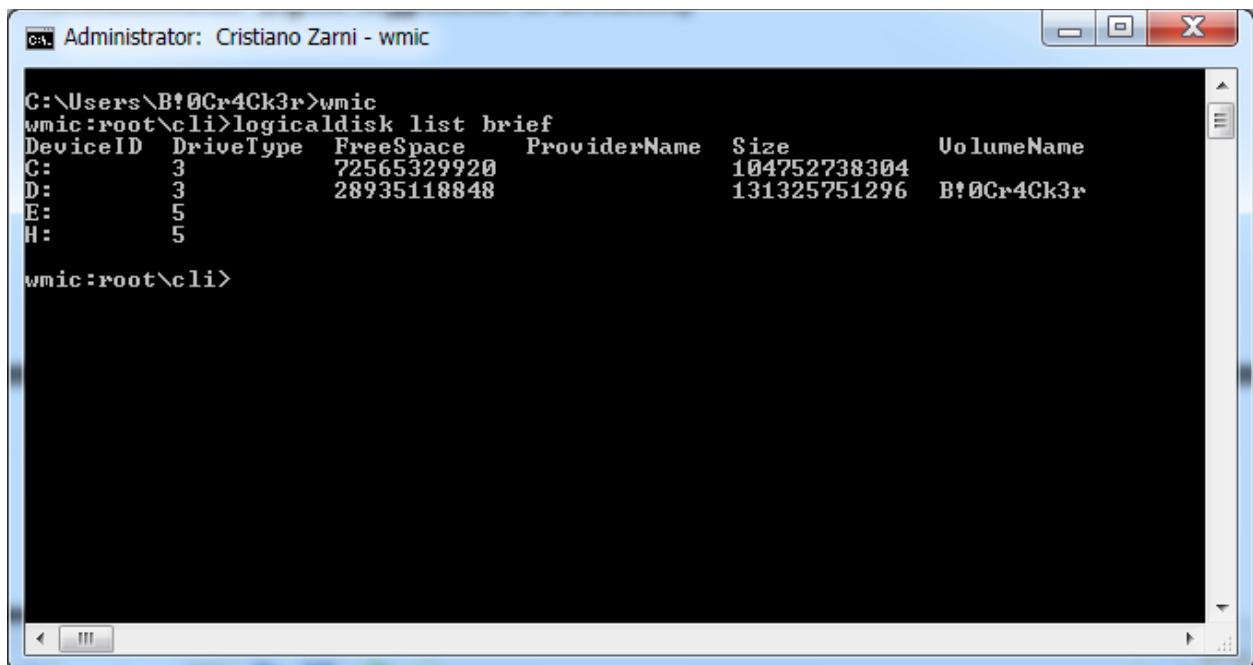
L2 Cache Size Level 2 Cache ရဲ့ သိမ်းဆည်းနိုင်မှုပမာဏကိုဖော်ပြပေးမှာပါ။

Product Name Detail သင့် CPU ကိုဘယ်ကထုတ်တယ် ဘာ အမျိုးအစားလည်းဖော်ပြပေးပါတယ်။

Processor Type သင့် CPU ရဲ့ Support လုပ်နိုင်တဲ့ Type ကိုဖော်ပြပေးတာဖြစ်ပါတယ်။

Socket Type ကတော့ CPU ရဲ့ Socket Type တွေကို အသေးစိတ်ဖော်ပြပေးတာပါ။ ဥပမာ ကျွန် တော် တို့က Desktop မှာဆိုရင် CPU အတွက် MB တွေမှာ Socket Type တွေရှိပါတယ်။ Socket A, Socket 7, PGA (Pin Grid Array), LGA (Land Grid Array) စသဖြင့် ရှိသလို သင့် စက်မှာ ဘာ Socket လည်းဆို တာကို သိရှိနိုင်ပါတယ်။

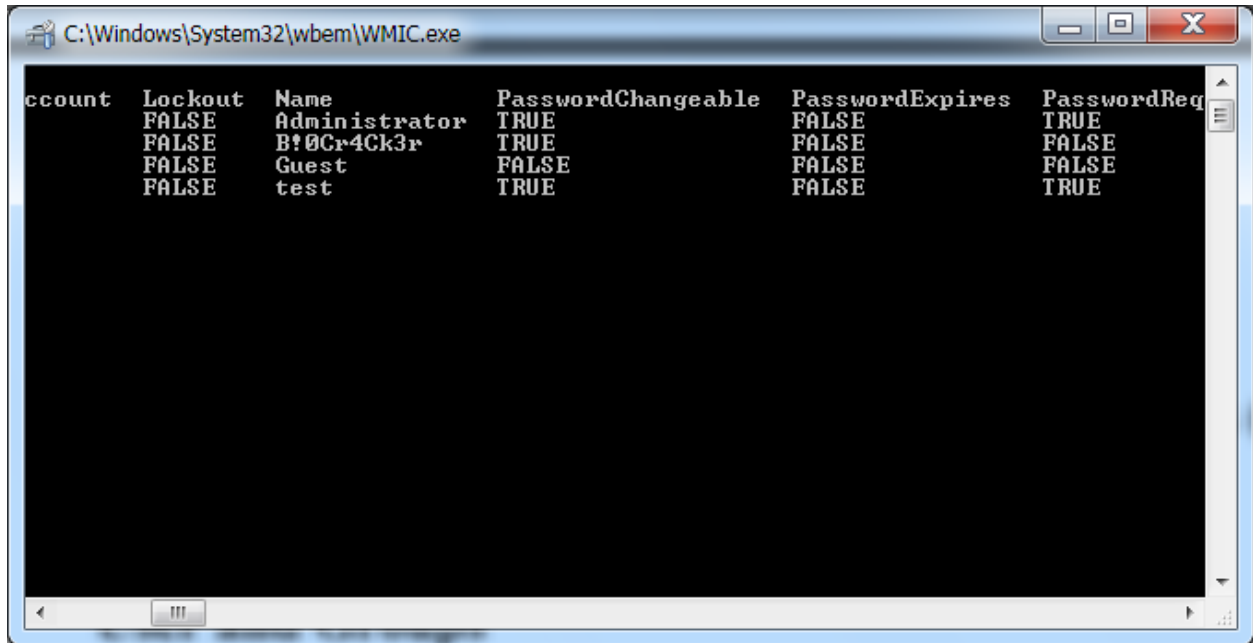
“logicaldisk list brief”



```
C:\Users\B!0Cr4Ck3r>wmic
wmic:root\cli>logicaldisk list brief
DeviceID DriveType FreeSpace ProviderName Size VolumeName
C:        3          72565329920      104752738304
D:        3          28935118848       131325751296  B!0Cr4Ck3r
E:        5
H:        5
wmic:root\cli>
```

Logicaldisk list brief ဆိုတာကတော့ သင့် စက်ထဲမှာရှိသော HDD ရဲ့ Partition ပိုင်းထားတာတွေကိုက အစ အသေးစိတ်ဖော်ပြပေးပါတယ်။

“useraccount list”



Useraccount list ဆိုတာကတော့ သင့်ကွန်ပျူတာမှာ User Account ဖွင့်ထားတာတွေကိုအသေးစိတ် ဖော်ပြပေးမှာဖြစ်ပါတယ်။ Administrator Account Type လား၊ Guest Account Type လား၊ Password ပေးထားလား၊ မပေးထားဘူးလားဆိုတာကအစ အသေးစိတ်ဖော်ပြပေးပါတယ်။

“qfe”

```
Administrator: C:\Windows\system32\cmd.exe - wmic
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\B!0Cr4Ck3r>wmic
wmic:root\cli>qfe get description,installedOn
Description      InstalledOn
Update           8/1/2014

wmic:root\cli>_
```

Qfe get description,installedOn ဆိုတာကတော့ သင့်ကွန်ပျူတာဝင်းဒိုးစနစ်ကြီးကို ဘယ်နေ့က Update လုပ်လိုက်သလည်းဆိုတာကိုသိချင်တဲ့အခါမှာသုံးပါတယ်။ ဒီ Command ကလည်း သင့်အတွက် အရေးကြီးပါတယ်။ ဆိုလိုတာက အချို့ Customer Site တွေမှာ Window Guniue Error တက်တာကို ကြုံဖူးကြမှာပါ။ ဒီလိုတက်တယ်ဆိုတာ ကျွန်တော်တို့က Licence Verssion မဟုတ်ပဲ Cracked Version ကို အသုံးပြုကြတဲ့အခါ အွန်လိုင်းချိတ်ဆက်ထားပြီး Window Update လုပ်မိတဲ့အချိန်မျိုးမှာဖြစ်သွားတတ် တာပါ။ ဒါကြောင့် ဘယ်နေ့ Update လုပ်လိုက်သလည်းဆိုတာကိုအလွယ်တကူသိရှိနိုင်အောင်ဖြစ်ပါ တယ်။