မျက်ပွင့် [illegible]

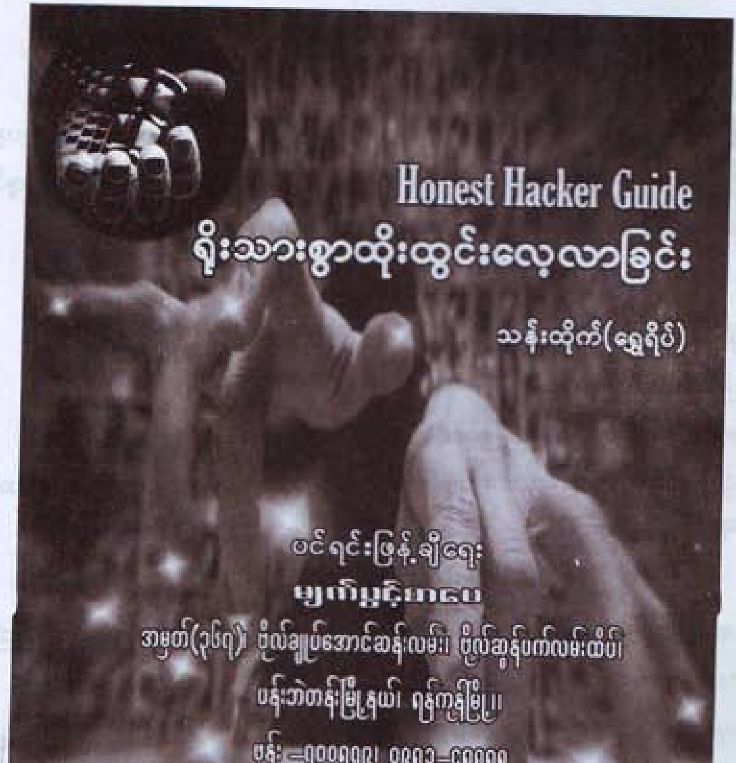
Honest Hacking Guide

ရိုးသားစွာထိုးထွင်းလေ့လာခြင်း

Honest Hacking

သန်းထိုက် (ရွှေဒိုမ်)

GOLDEN SHADE MEDIA Computer Technology


Honest Hacker Guide
ရိုးသားစွာထိုးထွင်းလေ့လာခြင်း
သန်းထိုက်(ရွှေရိပ်)
ပင်ရင်းဖြန့်ချိရေး
အမှတ်(၃၆၇)၊ ဗိုလ်ချုပ်အောင်ဆန်းလမ်း၊ ဗိုလ်ဆွန်ပက်လမ်းထိပ်၊
ပန်းဘဲတန်းမြို့နယ်၊ ရန်ကုန်မြို့။
goldenshadetech@gmail.com
http://thanhtikegs.weebly.com

မော်ကွန်းတစ်ခုရေးထိုးခြင်း

ကွယ်လွန်သွားပြီဖြစ်တဲ့ကျေးဇူးရှင် မွေးမေမေ၊
ကျွေးမွေးပညာသင်ပေးခဲ့တဲ့ ကျွေးဖေဖေ၊
ဘဝလက်တွဲဖော် ချစ်ဇနီးနှင့် လေးစားရသောအမိအဖ၊
ပညာအဖုံဖုံ နည်းအစုံဖြင့်သင်ယူခဲ့ရသော သင်မြင်ကြားဆရာများ၊
နိုင်ငံတကာရပ်ဝေးမြေခြားမှ သူငယ်ချင်းများ၊
အကူအညီပေးနေသော မိတ်ဆွေကောင်းများ၊
တစ်စုံတစ်ခုပေးခဲ့သောသူများ၊
တပည့်များ၊
အားလုံးအပါအဝင်
စာဖတ်ပရိသတ်များအားလုံးကို
ကျေးဇူးကမ္ဗည်းတင်ရေးထိုးအပ်ပါကြောင်း ----

သန်းထိုက်(ရွှေရိပ်)

မနေ့၊ တစ်နေ့ကလိုပါပဲသား . . . ချစ်လေးရယ်

သား နိုင်ငံရပ်ခြားကပြန်လာတော့ အမေရယ်မောပျော်ရွှင်နေခဲ့တယ် .....
သားပထမဆုံးစာအုပ်လေးထုတ်ဖို့စီစဉ်နေချိန် အမေနေမကောင်းတော်တော်ဖြစ်နေပြီနော် .....
အဲ့ဒီနေ့က အိပ်ယာပေါ်ကအမေ့ကို သားနောက်ဆုံးပြုစုခဲ့ရတာပါ .....
နောက်တစ်နေ့မှာ အမေ့ကိုဆေးရုံတင်လိုက်ပြီတဲ့ .....
သားရောက်တော့ အမေကဖက်လက်၊ ပိုက်တွေ၊ အပ်တွေ၊ စက်တွေအစုံနဲ့ပေါ့ .....
ပထမရက်နဲ့ ဒုတိယရက်မှာ အစ်မကြီးနဲ့ညီလေး၊ အစ်ကိုနဲ့မရီးတို့ စောင့်ခဲ့ကြတယ် .....
သုံးရက်မြောက်ညမှာ သားနဲ့အမေ့ချွေးမ ညအိပ်စောင့်ရမှာလေ .....
အမေသားတို့ကို ညစောင့်ပြုစုခွင့်တောင် မပေးခဲ့ဘူးနော် .....
သုံးရက်မြောက်မနက်မှာပဲ အမေသားတို့အားလုံးကိုထားခဲ့တယ် .....
အဲ့ဒီနေ့က အောက်တိုဘာလ ၁ ရက်နေ့ပေါ့ .....
ဆေးရုံရေခဲတိုက်သွားတဲ့လမ်းပေါ်မှာ အမေ့သက်ပျောက်အဝတ်ထုပ်လေးပိုက်ပြီး
မိုးရေတွေ တဖျောက်ဖျောက်နဲ့အတူ သားလည်းရောငိုနေခဲ့တယ် .....
အမေကစောင်ခေါင်းမြီးခြုံပြီး အေးစက်စက်အခန်းကျဉ်းထဲကျန်ခဲ့ရတယ် .....
သုသာန်မှာ သားဖက်ငိုတာကောအမေသိရဲ့လား၊ အပြင်မှာမိုးတွေရွာနေတယ်လေ .....
သားလက်နဲ့အမေ့ခန္ဓာကို မီးသဂြိုလ်စက်ထဲတွန်းထည့်ချိန် သားငိုဖို့မေ့နေတယ် .....
မြေပြင်ကထွက်ခွာသွားတဲ့အမေ့ကိုကောင်းကင်ပေါ်လှမ်းရှာမိတယ် .....
သားငိုဖို့သတိရတော့ ခေါင်းပေါ်မိုးစက်တွေကျနေပြီ .....
နှလုံးထဲအပေက သားဘေးမှာလေ အမေထွက်သွားခဲ့တာမယုံသလိုပေါ့ .....
အမေက မိုးရေစက်တွေနဲ့အတူထွက်ခွာသွားခဲ့တယ်လေ .....
သားဝမ်းနည်းမိဆုံးတစ်ခုကတော့ သားရတဲ့ပထမဆုံးစာမူခ အမေလုံးဝမစားခဲ့ရတာပါ .....
အမေ့ရည်မှန်း သားလျှော့ဒါန်းတာတွေ သာဓုခေါ်ပါအမေ .....

အမေ အောက်တိုဘာမိုးရေစက်တွေ တစ်ကျော့ပြန်လာပြီနော် .....
သားခေါင်းပေါ်မိုးရေစက်တွေကျလာပြန်ပြီ .....
ရင်ခွင်ထဲမှာ အောက်တိုဘာမိုးစက်တွေနဲ့အတူရောက်လာတဲ့ သမီးလေးကိုချီထားလို့ပေါ့ .....
မိုးရေစက်တွေနဲ့ သမီးလေးကိုမြင်တိုင်း သတိရလွမ်းနေရအဲပါအမေရယ် .....

၁ နှစ်ပြည့်အလွမ်းအမှတ်တရ
အမေချစ်တဲ့သား
သန်းထိုက်(ရွှေနိုင်)

ပထမဦးစွာသိရှိရန်မှာ ...

စာရေးသူအနေဖြင့် စာဖတ်ပရိသတ်ကြီးအား သိစေလိုသည်မှာ- ယခုရေးသား ထုတ်ဝေသည့် Honest Hacking စာအုပ်ကို မြန်မာဘာသာနည်းပညာစာပေဖွံ့ဖြိုး စေလိုသော ဖြူစင်သည့်စိတ်ကူးဖြင့်သာစီစဉ်ရေးသားထားပါတယ်။

မကောင်းစိတ်ဖြင့် ဖောက်ထွင်းမှုပြုလုပ်နိုင်သော Evil Mind Hacker, NonEthical Hacker တွေ၏ လုပ်ဆောင်ချက်များကို လုံးဝမရေးသားထားပါ။ နိုင်ငံတကာတွင် တွေ့ကြုံနေရသော Evil Mind Hacker တွေရဲ့ပညာရပ်တွေကို စာရေးသူလည်းမတတ်ကျွမ်းပါ။

ယခုစာအုပ်ကလေးဖြစ်မြောက်ရန် အချိန်များစွာပေးပြီးလေ့လာခဲ့တာတွေကိုသာ မြန်မာဘာသာ သင်ရိုးစာအုပ်လေးအဖြစ်ဖန်တီးရတာပါ။ စာရေးသူပေးထားသောအမည်ကပင် "ရိုးသားစွာထိုးထွင်းလေ့လာခြင်း(Honest Hacking)" ဖြစ်ပါတယ်။

စာဖတ်သူများအနေဖြင့် သာမန်စာအုပ်တွေမှာမပါရှိသလို၊ လေ့လာရန်လည်း မလွယ်ကူတဲ့ Windows System တွေကိုအတွင်းကျကျလေ့လာအသုံးချနိုင်ဖို့ဖြစ်ပါတယ်။ ဒါ့အပြင် အမှန်တကယ်လိုအပ်နေတဲ့ နည်းပညာဆိုင်ရာ အသုံးချဆော့ဖ်ဝဲလေးတွေကို အသုံးပြု နိုင်ရန်လမ်းညွှန်ထားတဲ့စာအုပ်လေးသာဖြစ်ပါတယ်။

ကွန်ပျူတာသုံးစွဲသူအများစုတွေ့ကြုံနေရတဲ့ Security Password ဆိုင်ရာပြဿနာ တွေကိုလည်း မိမိကိုယ်တိုင် ဖြေရှင်းနိုင်ဖို့ အသေးစိတ်လမ်းညွှန်ပေးထားသည်သာ ဖြစ်ပါတယ်။

ကွန်ပျူတာစက်ပြင်သင်တန်းကျောင်းတွေမှာမသင်တဲ့ဘာသာရပ်တွေမို့ စက်ပြင် ပညာရှင်များ လက်စွဲစာအုပ်ဖြစ်ဖို့လည်းဦးတည်ထားပါတယ်။

စာဖတ်သူများအနေဖြင့် ယခုစာအုပ်အား အမည်တစ်မျိုးဖြင့်အမှတ်မမှားသင့်ပါ။ စာအုပ်အမည်ကိုသေချာပြန်ဖတ်ကြည့်လိုက်ပါ။

" ရိုးသားစွာထိုးထွင်းလေ့လာခြင်း (Honest Hacking)"

ကျေးဇူးတင်လျှက်

သန်းထိုက် (ရွှေရိပ်)

goldenshadetech@gmail.com
http://thanhtikegs.weebly.com

စာရေးသူ၏နိဒါန်းပျိုးစကား

ယခုစာအုပ်လေးကိုထုတ်နိုင်ဖို့အားအတော်ယူခဲ့ရပါတယ်။ ယခုလတွေမှာ ကျန်းမာရေးကလည်း သိပ်မကောင်းတော့စာတစ်အုပ်ဖြစ်ဖို့ ပုံမှန်ထက် နှစ်ဆသုံးဆမကအားထုတ်ရပါတယ်။ စာရေးသူပထမဆုံး "အင်တာနက်သုံးလိပ်စာများ"စာအုပ်ထုတ်ဝေစဉ်ကပင် ကြော်ငြာခဲ့တဲ့စာအုပ်ဖြစ်ပေမယ့်လည်း အကြောင်းအမျိုးမျိုးကြောင့် ထုတ်ဝေဖို့ကြန့်ကြာခဲ့ပါတယ်။

အနယ်နယ်အရပ်ရပ်မှ ပရိသတ်တွေက စာရေးသူကို စာအုပ်မထွက်သေးဘူးလားလို့ တမေးတည်း မေးနေရတဲ့ စာအုပ်ကလေးပါ။ စာအုပ်အမည်ကိုလည်းခပ်ဆန်းဆန်းလေးဖြစ်အောင် "ရိုးသားစွာထိုးထွင်း လေ့လာခြင်း" [Honest Hacker Guide] လို့အမည်ပေးထားပါတယ်။

နိုင်ငံတကာမှာ Black Hacking လုပ်သူတွေကိုထိရောက်စွာအရေးယူဖမ်းဆီးနေတာတွေ သတင်း မီဒီယာတွေမှာ စာဖတ်သူတို့တွေ့မြင်ကြားသိနေရမယ်ထင်ပါတယ်။ အဆိုပါတွေကတော့ အများသူငှာကို စိတ်ဒုက္ခပေးသူတွေမို့ ဖမ်းဆီးခံရတာပါ။ ဘဏ်စာရင်းတွေကိုထိုးဖောက်ဝင်ရောက်မယ်။ Personal ဆိုင်ရာ လျှို့ဝှက်ချက်တွေကို ပိုင်ရှင်မသိအောင်ဝင်ရောက်ပြီး အများရှေ့မှာသိက္ခာကျရန်လွှင့်တင်မယ်။ အစရှိသဖြင့် အခြားသော မတရားမှုများစွာပြုလုပ်ခြင်းကြောင့်သာဖြစ်ပါတယ်။

စာရေးသူရဲ့ ယခုစာအုပ်မှာတော့ ကောင်းမွန်သောစိတ်ထားဖြင့် ကွန်ပျူတာဆိုင်ရာ နည်းပညာများကို ထိုးထွင်းလေ့လာဖို့အတွက် လမ်းညွှန်ရှင်းပြထားပါတယ်။ နာမည်မကြီးအသုံးနည်းတဲ့ အသုံးဝင် Program တွေကိုလည်း Installation ထည့်သွင်းပုံမှ အစရှင်းပြထားပါတယ်။

သာမန်အသုံးပြုသူတစ်ယောက်မှသည် အဆင့်မြင့်အသုံးပြုနေသူများအတွက် နည်းလမ်းအတိုများ၊ အဆင့်နည်းလုပ်ဆောင်ချက်များကို နားလည်လွယ်သောစကားပြောရေးနည်းဖြင့်ရှင်းပြထားပါတယ်။ အဓိက ကတော့ ပုံမှန်သုံးမဟုတ်တာတွေကိုရှင်းပြထားတာပါ။

ဆရာတစ်ယောက်ရဲ့စကားလေးတစ်ခွန်းပါ–

" လက်ညစ်ပတ်လျှင်ဆေးလို့ပြောင်တယ်......

စိတ်ညစ်ပတ်လျှင် ဆေးလို့မပြောင် ...... "

ကျေးဇူးတင်လျက်

သန်းထိုက် (ရွှေရိပ်)

goldenshadetech@gmail.com

ရိုးသားစွာထိုးထွင်းလေ့လာခြင်း

ပါဝင်သောအခန်းကဏ္ဍများ

အခန်း(၁)	**Hacker ဆိုသည်မှာ**
အခန်း(၂)	**Information Of Operation System**
အခန်း(၃)	**Windows Speed Hacking**
အခန်း(၄)	**Run Command Hacking**
အခန်း(၅)	**Windows Shortcut Key**
အခန်း(၆)	**Desktop Shortcut Icon Create & Hacking System Control**
အခန်း(၇)	**Hacking Group Policy**
အခန်း(၈)	**Hacking Registry Editor**
အခန်း(၉)	**Hacking Use Script Code**
အခန်း(၁၀)	**Guide For Hacker Editor**
အခန်း(၁၁)	**System Resource Hack**
အခန်း(၁၂)	**Email and Internet Hack**
အခန်း(၁၃)	**Internet Speed Hack**
အခန်း(၁၄)	**Hackr Using Weapons**
အခန်း(၁၅)	**System Security Hacking**

ရိုးသားစွာထိုးထွင်းလေ့လာခြင်း

အခန်း(၁)

Hacker ဆိုသည်မှာ

စဉ်	လေ့လာရန်	စာမျက်နှာ
၁။	Hacker ဆိုသည်မှာ	၂

အခန်း(၂)

Information Of Operation System

စဉ်	လေ့လာရန်	စာမျက်နှာ
၁။	Windows ဆိုသည်မှာ	၆
၂။	Windows ထုတ်ကုန်များကိုလေ့လာခြင်း	၈
၃။	Windows OS လုပ်ငန်းစဉ်	၁၂
၄။	Open Source များကိုလေ့လာခြင်း	၁၆

ရိုးသားစွာထိုးထွင်းလေ့လာခြင်း

အခန်း(၃)

Windows Speed Hacking

စဉ်	လေ့လာရန်	စာမျက်နှာ
၁။	Windows 7 အရှိန်မြင့်ရန် Hack လုပ်ခြင်း	၁၈

1# Search Indexing Feature
2# User Account Control
3# Extra Speed Booster
4# Turn off Unused Windows 7 Feature
5# Disable the Aero Peek and Aero Sanp Feature in Windows 7
6# Change the Power Plan To Maximun Performance
7# Software To Speed Up Windows 7
8# Disable Unwanted System Sounds in Windows 7
9# Disable Unwanted Start Up Items and Speed Up

အခန်း(၄)

Run Command Hacking

စဉ်	လေ့လာရန်	စာမျက်နှာ
၁။	Run Box မှတိုက်ရိုက်ဖွင့်နိုင်သော Command Key များကိုလေ့လာခြင်း	၂၈

ရိုးသားစွာထိုးထွင်းလေ့လာခြင်း

အခန်း(၅)

Windows Shortcut Key

စဉ်	လေ့လာရန်	စာမျက်နှာ
၁။	Windows Key နှင့်တွဲသုံးရသော Shortcut များကိုလေ့လာခြင်း	၃၆

အခန်း(၆)

Desktop Shortcut Icon Create & Hacking System Control

စဉ်	လေ့လာရန်	စာမျက်နှာ
၁။	Desktop ပေါ်တွင် Sleep Command ဖန်တီးခြင်း	၄၂
၂။	Desktop ပေါ်တွင် Shortcut Icon များကိုတည်ဆောက်ခြင်း Handy Shortcut Create Program	၄၄
၃။	Honest Hacker အသုံးချ System Process Control Good Mode Program	၄၇
၄။	အထောက်အပံ့ကောင်းသော Windows Winset Program ကိုလေ့လာခြင်း	၅၀
၅။	Windows Winset အသုံးကိုလေ့လာခြင်း	၅၅
၆။	လုံခြုံရေးစနစ်ဖန်တီးပေးသော Predator Program ကိုလေ့လာခြင်း	၆၁
၇။	USB Memory Stick and USB Drive ဖြင့်ကူးယူခြင်းအား ထိန်းချုပ်ခြင်း (USB Write Protect Program)	၆၈

ရှိုးသားစွာထိုးထွင်းလေ့လာခြင်း

အခန်း(၇)

Hacking Group Policy

စဉ်	လေ့လာရန်	စာမျက်နှာ
၁။	Group Policy ကိုလေ့လာခြင်း	၇၂
၂။	Group Policy ဖြင့် Start Menu ကိုထိန်းချုပ်ခြင်း	၇၅
၃။	Group Policy ဖြင့် System ပိုင်းကိုထိန်းချုပ်ခြင်း	၇၆
၄။	Group Policy ဖြင့် Internet Connection ကိုထိန်းချုပ်ခြင်း	၇၇
၅။	Group Policy ဖြင့် File Delete မပြုလုပ်ရန်ထိန်းချုပ်ခြင်း	၇၈
၆။	Registry Editor and Command Prompt ကိုထိန်းချုပ်ခြင်း	၇၉
၇။	Group Policy ဖြင့် Control Panel ကိုဖျောက်ထားခြင်း	၈၀

အခန်း(၈)

Hacking Registry Editor

စဉ်	လေ့လာရန်	စာမျက်နှာ
၁။	Hacker လက်သုံး Registry Editor အကြောင်းကို အတွင်းကျကျလေ့လာခြင်း	၈၂
၂။	Registry Backup ဦးစွာပြုလုပ်ထားခြင်း(ပထမနည်းလမ်း)	၈၃
၃။	Registry Backup ပြုလုပ်ခြင်း(ဒုတိယနည်းလမ်း)	၈၅
၄။	Registry Editor အတွင်းပိုင်းတည်ဆောက်ပုံကိုလေ့လာခြင်း	၈၇
၅။	Registry Editor အသုံးပြုနည်း	၈၈
၆။	Registry Editor ဝင်ရောက်ဖို့ရာ	၉၀
၇။	Control Panel အသုံးပြုခွင့်ပိတ်ထားခြင်း	၉၁
၈။	Control Panel အတွင်းမှ Add Remove Program အသုံးပြုခွင့်ပိတ်ထားခြင်း	၉၂

ရိုးသားစွာထိုးထွင်းလေ့လာခြင်း

အခန်း(၉)

Hacker Use Script Code

စဉ်	လေ့လာရန်	စာမျက်နှာ
၁။	Script Program ဆိုသည်မှာ	၁၀၀
၂။	Script Program ရေးဖို့သိထားရမည့်လုပ်ငန်းစဉ်များ	၁၀၀
၃။	Script Program အခြေခံ Code (Key Words)	၁၀၁
၄။	Registry Control Script Program ကိုရေးသားလေ့လာခြင်း	၁၀၄
၅။	.vbs Script ကိုထိုးထွင်းလေ့လာခြင်း	၁၀၆
၆။	Control System Enable Script Program ကိုရေးသားခြင်း	၁၀၈
၇။	Control System Disable Script Program အတွက်ပြင်ဆင်ရေးသားခြင်း	၁၁၂

အခန်း(၁၀)

Guide For Hacker Editor

စဉ်	လေ့လာရန်	စာမျက်နှာ
၁။	Guide For Hacker Editor	၁၁၈
၂။	Hacker Technique	၁၂၈

ရိုးသားစွာထိုးထွင်းလေ့လာခြင်း

အခန်း(၁၁)

System Resource Hack

စဉ်	လေ့လာရန်	စာမျက်နှာ
၁။	System Resource ကို Hacking လုပ်လေ့လာခြင်း	၁၃၀
၂။	Hacker Technique	၁၂၈

အခန်း(၁၂)

Email & Internet Hack

စဉ်	လေ့လာရန်	စာမျက်နှာ
၁။	Email များဖောက်ထွင်းမှုမှကာကွယ်ရန်	၁၃၄
၂။	Mail လုံခြုံရေးပြဿနာဖြေရှင်းနည်းလမ်းများ	၁၃၈
၃။	Internet Explorer သုံးသူများနှင့် ပြဿနာ	၁၄၁
၄။	Cookies တွေအစားခံရတဲ့အခါ	၁၄၃
၅။	Cookies Crack Program Code	၁၄၇
၆။	Gmail -GTalk ဆိုင်ရာအသုံးချလုပ်ဆောင်မှု	၁၅၁
၇။	Gmail သုံးသူတိုင်းလုပ်ဆောင်ဖို့ရာ	၁၅၄

အခန်း(၁၃)

Internet Speed Hack

စဉ်	လေ့လာရန်	စာမျက်နှာ
၁။	Internet Connection Speed Hack	၁၅၆
၂။	Speed Connect Program ကိုလေ့လာခြင်း	၁၅၈
၃။	Light Downloader Program ကိုအသုံးချလေ့လာခြင်း	၁၆၅
၄။	Honest Hacker တို့အတွက် Proxy ဆိုသည်မှာ	၁၇၃
၅။	Multi Proxy Program ကိုလေ့လာခြင်း	၁၇၇
၆။	My IP Address Program အသုံးပြုပြီး မိမိ IP Address ကိုလေ့လာခြင်း	၁၈၀

ဂိုးသားစွာထိုးထွင်းလေ့လာခြင်း

အခန်း(၁၄)

Hacker Using Weapons

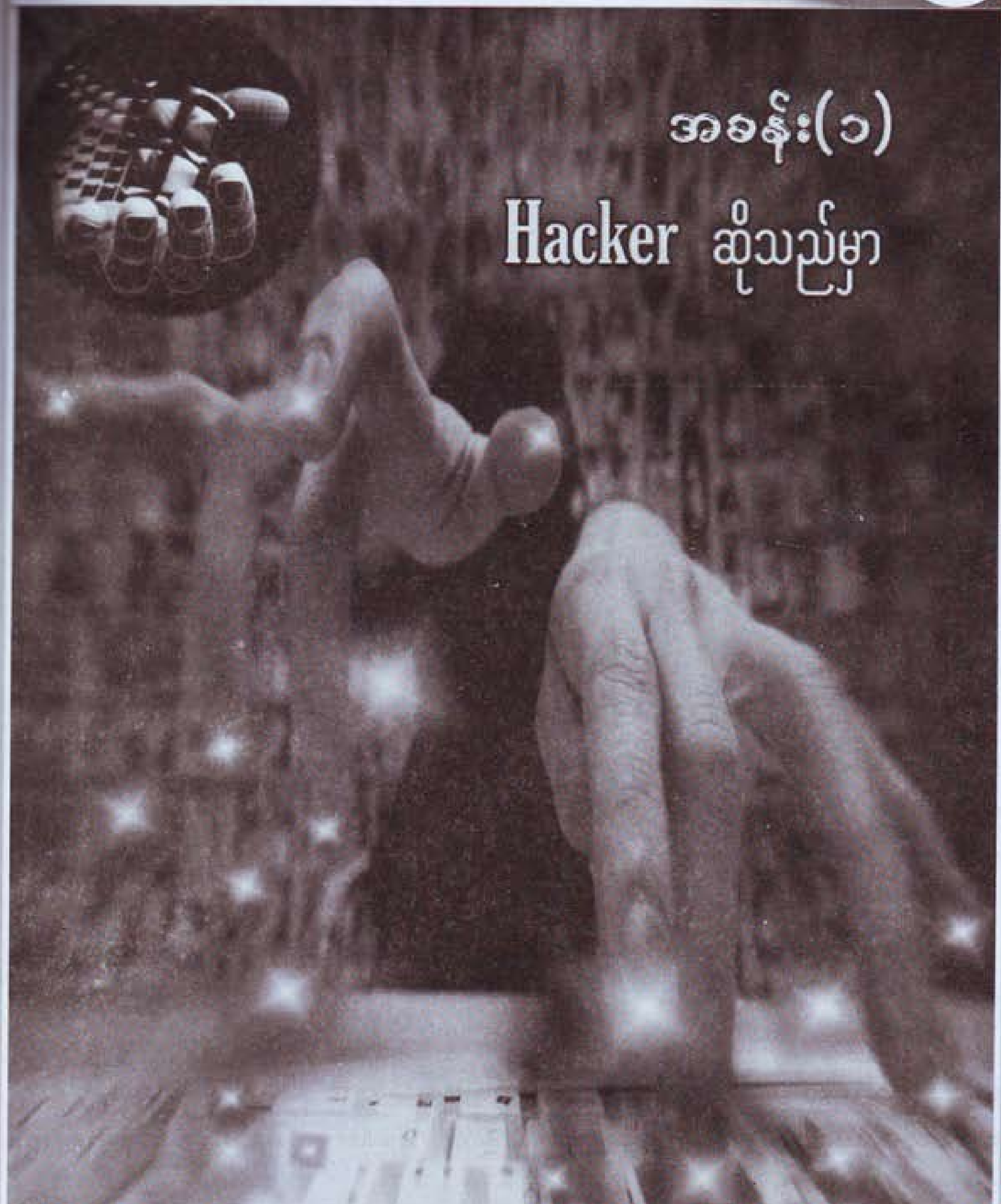
စဉ်	လေ့လာရန်	စာမျက်နှာ
၁။	Hacker အသုံးချ Website Hacking Code များကိုလေ့လာခြင်း	၁၈၂
၂။	c99 Shell ကိုလေ့လာခြင်း	၁၈၃
၃။	Web Attack တွင်သုံးသော Java Script စနစ်	၁၈၉
၄။	IP Scanner Script Code အသုံးချရယူခြင်း	၁၉၀
၅။	Internet ချိတ်ဆက်ထားသောကွန်ပျူတာကိုအဝေးမှ Hacking လုပ်ခြင်း (LogMeIn)	၁၉၁
၆။	Hacking Wifi Zone အတွက်သိသင့်စရာများ	၁၉၄
၇။	How to Hack WEP/WPA Wirless Network	၁၉၅
၈။	Anticipated Problems	၁၉၉
၉။	WPA Hacking	၂၀၀
၁၀။	Dial Up Connection မြန်ဖို့ဆိုတာ	၂၀၂

အခန်း(၁၅)

System Security Hacking

စဉ်	လေ့လာရန်	စာမျက်နှာ
၁။	Hiren's Boot CD ကိုလေ့လာခြင်း	၂၀၄
၂။	CMOS/BIOS Hack	၂၀၈
၃။	Admin Security ကိုထိုးဖောက်ခြင်း	၂၁၁
၄။	Deep Freeze နှင့်ပြဿနာအဖြာဖြာ	၂၁၅

အခန်း(၁)
Hacker ဆိုသည်မှာ



Hacker ဆိုသည်မှာ

Hacker လို့ဆိုလိုက်တာနဲ့ ကွန်ပျူတာတောက်တီးတောက်တဲ့သိသူမှ၊ ကျွမ်းကျင်ပညာရှင်အထိက အန္တရာယ်ရှိသောလူပုဂ္ဂိုလ်တစ်ယောက်အဖြစ်တန်းမြင်ပါလိမ့်မယ်။ ပြီးလျှင် လက်ထိပ်စော်နံနေမယ့် ရာဇဝတ်သားကောင်ဆိုပြီးတော့လည်း နှာခေါင်းရှုံ့နေပါလိမ့်မယ်။

ဥပမာစကားဆိုရသော် အရက်(သေရည်) ဆိုတာကောင်းသလား။ မကောင်းဘူးလား။ ကဲ--- စာဖတ်သူဘယ်လိုဖြေဆိုမလဲ။ အရက်ကြိုက်တဲ့အရက်ချစ်သူတွေကတော့ ကောင်းတယ်ဆိုမှာပဲ။ အရက်သမား အိမ်သူဇနီးမယားတွေကတော့မကောင်းဘူးလို့ဆိုလိမ့်မယ်။ စာဖတ်သူကကောင်းမါတယ်ဗျာ လို့တော့ သူတို့ရှေ့သွားမပြောမိစေနဲ့။ တစ်ခုခုပျံ့ဝဲရောက်လာလိမ့်မယ်။

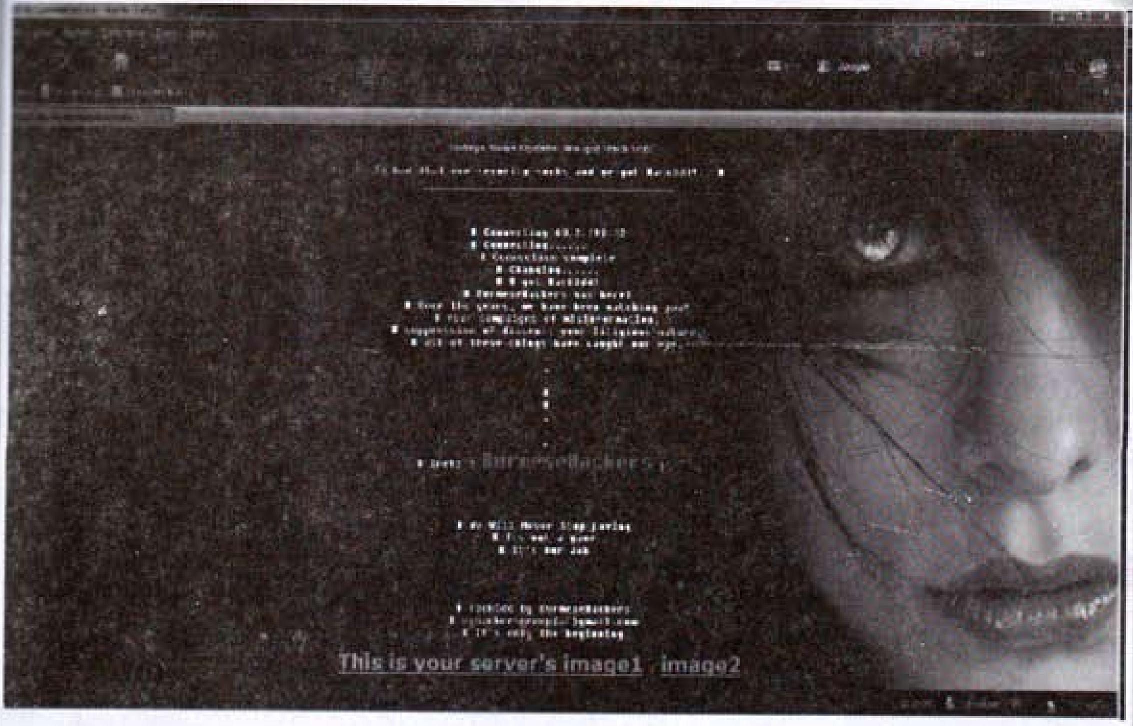
ဟုတ်ပါပြီ။ အဓိကဆိုလိုချင်တာကတော့ ကောင်းတဲ့အမြင်ရှိမှု၊ ကောင်းသောအသုံးရှိမှုပါပဲ။ အရက်(သေရည်)ကို မူးဖို့အတွက်သောက်ခဲ့သော် ဒါဟာမကောင်းတာ၊ ဒါပေမယ့် ဆေးဝါးဖော်စပ်ဖို့ ထည့်သွင်းတယ်၊ ဥပမာ–လိမ်းဆေးပေါ့။ ဒါဆိုကောင်းတယ်။

ဒီလိုပါပဲ ကွန်ပျူတာနည်းပညာဆိုင်ရာများအတွက် ကောင်းသောလုပ်ဆောင်ချက်ဖြင့် ထိုးထွင်း လေ့လာနေသူတွေရှိသလို၊ ဖျက်စီးလိုစိတ်၊ ဒုက္ခပေးလိုစိတ်၊ လူတွင်ကျယ်လုပ်လိုစိတ်တွေနဲ့ ထိုးဖောက် နှောက်ယှက်သူတွေလည်းရှိပါတယ်။

ယခုစာအုပ်ပြုစုနေစဉ်မှာပင် မြန်မာမှ Hacker က Georgia နိုင်ငံအစိုးရ၏ http://www.moh.gov.ge ကို Hack လုပ်လိုက်ပါတယ်။ ဘာတွေလုပ်လိုက်လဲဆိုတာကိုတော့ စာရေးသူလည်း မသိပါဘူး။ စာရေးသူ တွေ့လိုက်ရတာကတော့ WebPage ကိုပြင်ဆင်ထားပါတယ်။ ဘာတွေနှိုက်နှိုက်ချွတ်ချွတ်လုပ်လိုက်တယ်ဆိုတာကိုတော့ မသိရပါ။

မျက်နှာစာမှာတော့ Burmese Hacker လို့စာရေးထိုးထားပါတယ်။ တစ်ဖက်စာမျက်နှာမှာ အဆိုပါ WebPage ကိုကူးယူဖော်ပြထားပါတယ်။ ဒီလိုမျိုးတွေလုပ်ဆောင်သူကို အကြမ်းဖက် Hacke လို့ခေါ်ကြပါတယ်။

ဒါ့ကြောင့် စာရေးသူကတော့ အဆိုပါ Hacker မျိုးတွေကိုရှုတ်ချပါတယ်။ ယခုစာအုပ်မှာလည်း အဆိုပါကဲ့သို့သော အကြမ်းဖက်လုပ်ဆောင်ချက်မျိုးတွေအတွက် အထောက်အပံ့လုံးဝမပါရှိပါ။ စာရေးသူလည်းလုံးဝမတတ်ပါ။ ယခုစာအုပ်မှာတော့ Hacker တွေရဲ့လုပ်ဆောင်ချက်တွေကို သဘောတရားရှင်းပြထားတာပါရှိပါတယ်။



အခိုကဆိုလိုရင်းတောင်ပျောက်သွားတော့မယ်။ ဆက်ရလျှင် မြန်မာမှုပညာရှင်အများစုထဲမှာတော့ Hacker လုပ်လိုသူတွေရှိနေမှာပါ။ ၎င်းတို့အတွက်ယခုစာအုပ်လေးကရယ်မောစရာကောင်းနေမှာပါ။ ဒီ့ထက်ဆိုးလျှင် ဟာသစာအုပ်ဖတ်ရသလိုရယ်မောနေမယ်ထင်ပါတယ်။

Hacker ကိုဘာသာပြန်၊ အဓိပ္ပါယ်ဖွင့်ဆိုချက်များစွာရှိနေမှာပါ။ အခိုကဆိုလိုရင်းကတော့ ထိုးထွင်းသိမြင်ကျွမ်းကျင်သူလို့ဆိုရမှာပါ။ ကောင်းသည်၊ မကောင်းသည်ကတော့ အဆိုပါပုဂ္ဂိုလ်ရဲ့ ဗီဇစိတ်ရင်းပေါ်မူတည်ပါလိမ့်မယ်။

နိုင်ငံတကာဆောင်းပါးများ၊ မြန်မာ Blog များတွင် Hacker ဆိုတာကိုအမျိုးမျိုး ရှင်းလင်းချက်ထုတ်ကြပါတယ်။ စာရေးသူကိုလည်း အဆိုပါကိစ္စအတွက် ဝင်ရောက်ဆွေးနွေးပါဆိုလျှင် ယုန်ကလေးနာစေးနေတယ်လို့ဆိုရပါလိမ့်မယ်။

စာရေးသူကိုဆက်သွယ်ကြပါတယ်။ Hacker လုပ်ချင်လို့ သင်ပေးနိုင်မလားတဲ့။ စာရေးသူ ပြန်မေးခဲ့ပါတယ်။ Hacker ဆိုတာဘာတွေလုပ်တာလဲလို့။ အင်တာနက်ပေါ်မှာ အခြားသူတွေရဲ့ Blog, Website တွေ၊ Email တွေကိုဝင်ဖတ်၊ ဝင်ပြင်ချင်လို့ပါတဲ့။ ဒီလို နည်းပညာမျိုးတွေရှိနိုင်ပါတယ်။ ဒါပေမယ့် စာရေးသူမသိ၊ မတတ်ပါဘူး။ အင်တာနက်မျက်နှာတွေပေါ်မှာ Email ကို ထိုးဖောက်နိုင်တဲ့ ဆော့ဖ်ဝဲတွေကို ဒေါ်လာ-၁၀၀ နီးပါးနဲ့ရောင်းနေပါတယ်။ ကောင်းမကောင်း၊ လုပ်လို့ရမရကတော့ စာဖတ်သူ ငွေပေါ်လျှင်ဝယ်စမ်းသုံးကြည့်ပါလား။

Honest Hacker ဆိုတာသိပါသလား။ အဓိပ္ပါယ်ဖွင့်ဆိုကြည့်ပါဦး။ "ရိုးသားစွာထိုးဖောက်လေ့လာသူ" လို့စာရေးသူတော့ဆိုချင်ပါတယ်။ စာရေးသူကွန်ပျူတာလောကထဲဝင်ရောက်လာချိန်မှာ စက်ပြင်ဆင်ခြင်းကိုဦးစားပေးလေ့လာခဲ့ပါတယ်။ ပြီးတော့ Programming ဘာသာရပ်တွေကို လေ့လာပါတယ်။ အင်ဂျင်နီယာဘာသာရပ်တွေနဲ့၊ အနုပညာလုပ်ငန်းတွေကိုလည်း အလွတ်မပေးခဲ့ပါဘူး။ ဒီလိုနဲ့ စာရေးသူလုပ်ငန်းခွင်ဝင်ရောက်ချိန်မှာတွေ့ကြုံရတာတွေကတော့ Windows OS ရဲ့ လျှို့ဝှက်နက်နဲမှုတွေပါ။ စာရေးသူတို့ခေတ်အချိန်က Windows OS ဆိုလျှင် Windows 95 ကစသိတာပါ။ အဲ့ဒီအချိန်က DOS Command တွေဟာ စက်ပြင်ဆရာတွေရဲ့လက်နက်ကြီးတွေပါ။

ဒီလိုနဲ့တိုးတက်လာတဲ့အလျှောက် System ပိုင်းဆိုင်ရာပြဿနာတွေကိုဖြေရှင်းရပါတယ်။ Admin Password မေ့သွားတာတို့၊ အရေးကြီး Data တွေဖျက်မိတာတို့ကအစ System Command တွေ လုပ်မရတာအဆုံး၏ဖြေရှင်းပေးရပါတယ်။ ဟိုတစ်ချိန်ကတော့ CMOS/BIOS ကိုတောင်ပြန်လည် ရေးဆွဲပေးရပါတယ်။ ဒါတွေကို Hack or Crack လုပ်တယ်လို့ဆိုခဲ့ကြပါတယ်။

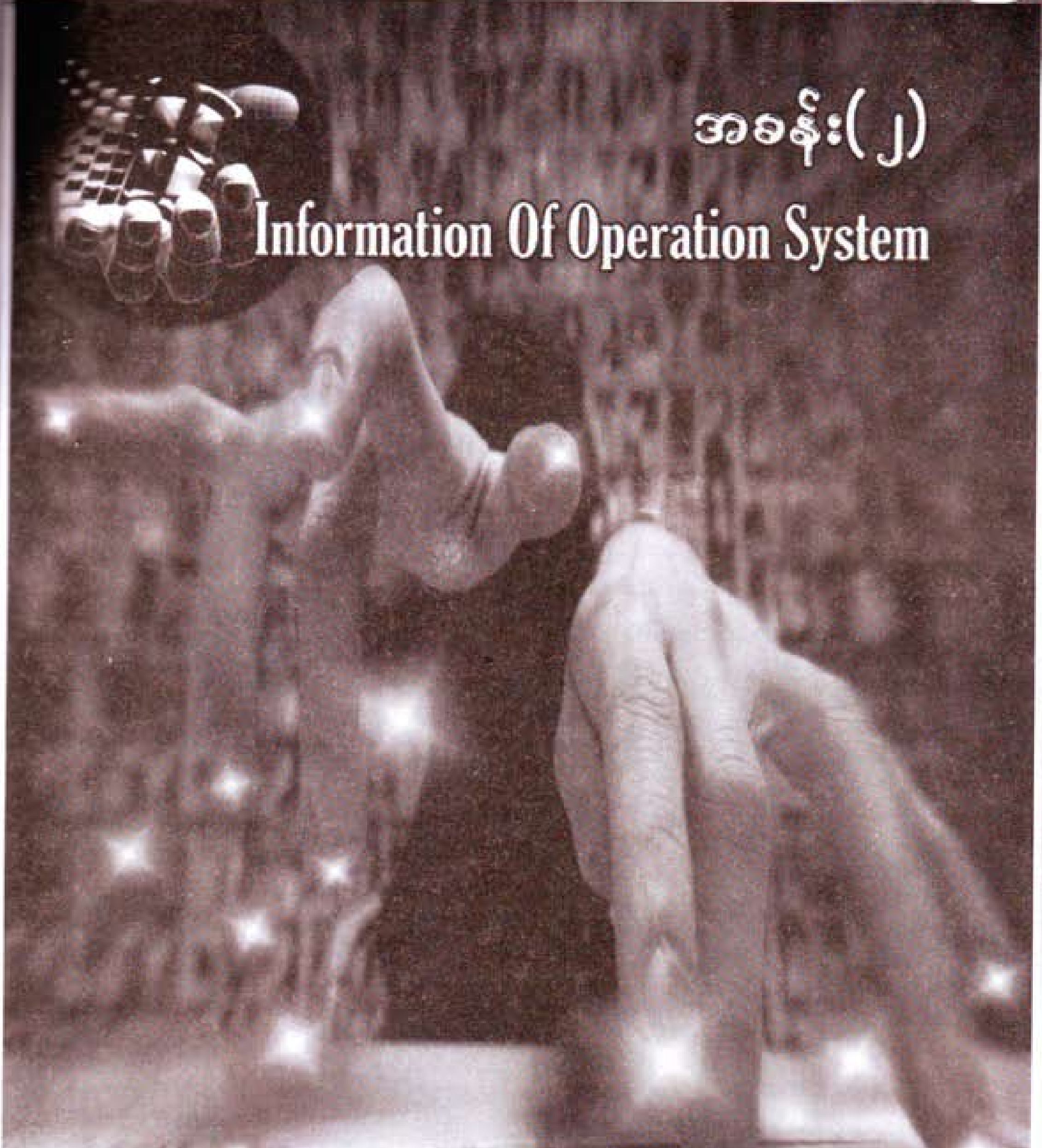
စာရေးသူရဲ့နည်းပညာခရီးလမ်းမှာတွေ့ကြုံရတာတွေ၊ သင်၊ မြင်၊ ကြား ဆရာများစွာရဲ့ ဗဟုသုတတွေကို တင်ပြချင်လို့ယခုစာအုပ်အား၊ ကွန်ပျူတာပညာရပ်ကို အတွင်းကျကျသိရှိ လေ့လာလိုသူတွေ၊ ကွန်ပျူတာဆိုင်ရာ ကျောင်းသားတွေ၊ စက်ပြုပြင်နေရတဲ့ စက်ပြင်ပညာရှင်ပေါက်စတွေ အတွက် ဦးတည်ရေးသားပါတယ်။

ဒါ့ကြောင့် Honest Hacker လို့စာအုပ်ကိုအမည်ပေးပြီး Windows OS ဆိုင်ရာတွေ၊ ကိုယ်ပိုင်သုံး အင်တာနက်ဆိုင်ရာတွေကိုသာ ရေးသားဖော်ပြရတာပါ။ တကယ့် Honest Hacker တစ်ယောက်ဖြစ်ဖို့ အတွက်ကတော့ အနည်းငယ်ပြည့်စုံသွားမှာပါ။ မိမိလက်ဝယ်ကြုံတွေ့လာရမယ့် ပိတ်ဆို့ခြင်းအခက်အခဲ တွေကိုကျော်လွှားဖို့ အထောက်အပံ့ကောင်းဖြစ်စေမှာပါ။

ပညာရှင်ဖြစ်ဖို့ထက် ပညာရပ်လေ့လာနိုင်ဖို့ဦးတည်ပြုစုရေးသားထားပါကြောင်း။

အခန်း(၂)

Information Of Operation System



goldenshadetech@gmail.com

http://thanhtikegs.weebly.com

Windows ဆိုသည်မှာ

Windows ဆိုတာတံခါးပေါက်လို့ဘာသာပြန်ဆိုတာဖြစ်လို့ ယခုလည်းကွန်ပျူတာတစ်လုံး စတင်ဖို့ ဝင်ရောက်ရမယ့်တံခါးပေါက်ဟာ Windows လို့သာမှတ်ယူလိုက်ပါ။ Operating System တွေကို အမျိုးအစားအမျိုးမျိုး ကိုအကျဉ်းချုပ်လေ့လာရလျှင်–

၁။ Microsoft မှဖန်တီးထုတ်လုပ်သော Windows Operating System

၂။ Apple မှဖန်တီးထုတ်လုပ်သော MAC Operationg System

၃။ Linux မှအခမဲ့အဖြစ်လွတ်လပ်စွာပြင်ဆင်ရေးသားနိုင်သော Ubuntu

တို့ဖြစ်ပါတယ်။

စာရေးသူယခုအဓိကထားရှင်းပြမှာကတော့ Windows စနစ်တွေအကြောင်းဖြစ်ပါတယ်။ Windows OS တွေကိုနာမည်ကျော် BillGate ပိုင်ဆိုင်တဲ့ Microsoft ကဖန်တီးထုတ်လုပ်ပါတယ်။ ကျန်ခဲ့ပြီဖြစ်တဲ့ သက္ကရာဇ်တွေနဲ့ Windows System တွေကိုကျော်လွှားပြီး ယခုနောက်ဆုံးထုတ် Windows 7 Version ကိုသာလေ့လာဖော်ပြသွားပါ့မယ်။

Windows 7 အခြေခံအသုံးပြုနည်းစာအုပ်တွေမြန်မာဘာသာနဲ့ မြန်မာမှုပညာရှင်တွေ ထုတ်ဝေခဲ့ပြီးဖြစ်လို့ အဆိုပါကဏ္ဍတွေကိုပြန်လည်မဖော်ပြတော့ပါ။ ယခုစာအုပ်မှာတော့ Windows 7 ကို အတွင်းကျကျလေ့လာနိုင်ဖို့ ဦးတည်ပြုစုရေးသားထားပါတယ်။

Windows 7 ဟာနောက်ဆုံးထုတ် Version လို့ဆိုပေမယ့် ယခင် Version တွေထက် သိပ်အပိုကြီး ဖြစ်မလာပါဘူး။ မြင်ကွင်းများနှင့် အမည်များ၊ အသုံးချပုံစံတစ်ချို့တို့သာပြောင်းလဲသွားတာပါ။ အနည်းငယ်အဆင့်မြင့်လာတာတော့ ရှိပါတယ်။

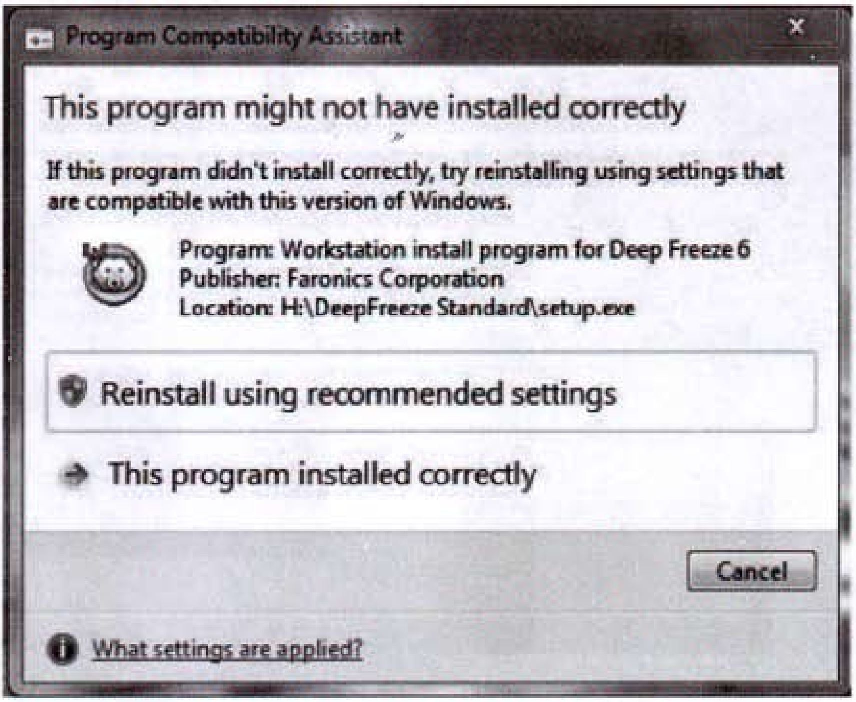
ဥပမာ– Virus တွေအဓိကပြန့်နှံ့စေတဲ့ AutoRun System ကိုထိန်းချုပ်ထားပါတယ်။ Program Install လုပ်ခြင်းတွေကို ခွင့်ပြုမိန့်ပေးနိုင်ဖို့စီစဉ်ခဲ့ပါတယ်။ နောက်ကွယ်မှအမြဲစောင့်ကြည့်ပေးနေသလို လိုအပ်လာလျှင် ချက်ခြင်းမေးခွန်းတွေထုတ်လာပါတယ်။ အဆိုးဆုံးအခြေအနေတစ်ရပ်ဖြစ်လာဖို့ မလွယ်တော့ပါဘူး။

စာရေးသူတွေ့မြင်ရတာကတော့ အသုံးပြုသူကို တရားခံဖြစ်စေတာပါ။ ဘာကိုဆိုလိုသလဲဆိုတော့ အသုံးပြုသူနှိပ်လိုက်တဲ့မေးခွန်းရဲ့အဖြေကြောင့်သာ ပျက်စီးရပါတယ်လို့ဆိုလာပါတယ်။ ရှင်းရှင်းပြောရလျှင် Virus Program တစ်ခုမောင်းနှင်ဖို့ စာဖတ်သူကမှားယွင်းပြီးခွင့်ပြုမိတာကြောင့် "ခင်ဗျားခွင့်ပြုလို့ ပျက်ရတာပါ" ဆိုပြီးတာဝန်ယူရပါလိမ့်မယ်။

ဒါကြောင့်စာဖတ်သူဟာ Windows 7 ပရိသတ်ဆိုလျှင် မေးလာတဲ့ အရေးကြီးမေးခွန်းတွေကို သတိထားဖြေဆိုရပါမယ်။ "မိမိလက်ဖြင့် မိမိဖျက်စီးမိပါတယ်" လို့မဖြစ်ပါစေနှင့်။ နောက်တစ်ခုကတော့ ယခုလိုသတိပေးလာတာကို အနှောက်အယှက်လို့ လုံးဝမယူဆပါနဲ့။ ဒီလိုတွေသတိပေးဖို့ စေတနာထား ဖန်တီးထားပါလားဆိုတာသတိရပါ။

Windows 7 ကိုကွန်ပျူတာစတင်သုံးသည်မှ ယနေ့အချိန်ထိ အကောင်းဆုံး၊ အအောင်မြင်ဆုံး အဆင့်မြင့်ဆုံးအဖြစ်သတ်မှတ်ရမှာပါ။ ဖန်တီးပုံကောင်းမွန်ခြင်း၊ သေသပ်စွာတည်ဆောက်ထားခြင်း တို့အပြင် လုံခြုံရေးစနစ်ကိုလည်းတိုးမြှင့်ထားတာကြောင့် အလွန်အောင်မြင်ခဲ့ပါတယ်။

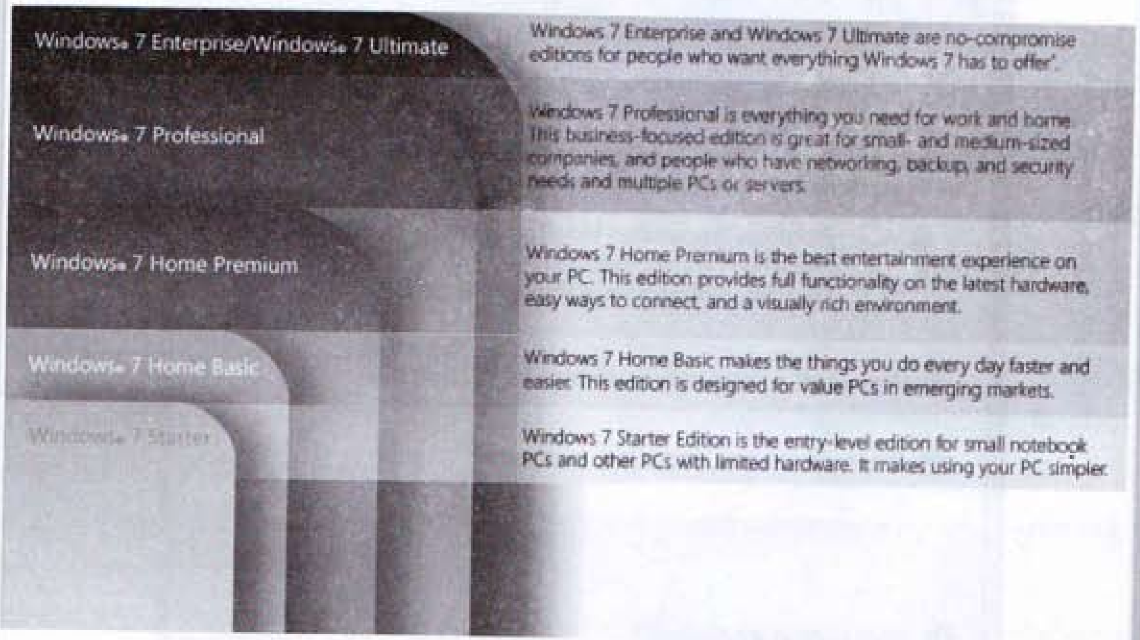
အလတ်စားအဆင့်ရှိ ကွန်ပျူတာတစ်လုံးပေါ်မှစတင်ရပ်တည်နိုင်တာကြောင့် သုံးစွဲသူပိုများ ရပါတယ်။



Windows 7 Editions ထုတ်ကုန်များကိုလေ့လာခြင်း

Windows 7 အားတန်ကြေးပေါ်မူတည်ပြီး၊ အဆင့်အတန်းမတူပဲ Windows Edition တွေကို ၅မျိုး ထုတ်လုပ်ဖြန့်ချိပါတယ်။ လူတန်းစားအမျိုးမျိုးအတွက်ခွဲခြားထုတ်လုပ်ရပါတယ်လို့ဆိုထားပါတယ်။ အဆင့်မြင့်ဆုံး Edition System ဟာဈေးအကြီးဆုံးဖြစ်ပါတယ်။ တန်ကြေးပေးတဲ့အလိုက် အမျိုးအစားပေါ်မူတည်ပြီး ရရှိမယ့်စွမ်းဆောင်ရည်လည်းကိုခွဲခြားရရှိမှာပါ။

ဘာပဲဖြစ်ဖြစ် ကွန်ပျူတာခေတ်တစ်လျှောက် အအောင်မြင်ဆုံး Operation System အဖြစ် Windows 7 ကမှတ်တိုင်ထူသွားပါပြီ။ သိပ်မကြာခင်နှစ်များမှာ ဒီ့ထက်ပိုကောင်းမယ့် Windows 8 ကအားယူနေပြန်ပါတယ်။



Windows 7 Stater

Windows 7 ကိုလုပ်ငန်းအသေးသုံးစေဖို့တန်ဖိုးနည်းဖန်တီးထားပါတယ်။ Notebook တွေ၊ PC တွေမှာတပ်ဆင်ထားတဲ့ Hardware တွေနဲ့ Windows 7 System ကိုသုံးနိုင်ရန် ကိုက်ညီမှုရှိမရှိကိုစစ်ဆေးဖို့၊ စမ်းသပ်ဖို့ထုတ်လုပ်ထားတာပါ။ ထုတ်ကုန်သစ်ဟာ သုံးဆွဲသူတွေအတွက် လုံခြုံရေးစနစ်ကောင်းမွန်ပြီး၊ ပြဿနာအနည်းဆုံးရှိဖို့ဆိုတာ ဟုတ်မဟုတ်စမ်းသပ်နိုင်ပါတယ်။ ဥရောပနိုင်ငံတွေမှာတော့ အခမဲ့ပေးသုံးကြပါတယ်။

Windows 7 Home Basic

Windows 7 ကိုကြိုက်နှစ်သက်သွားလို့ဝယ်သုံးဖို့ဆန္ဒရှိလာလျှင် တန်ဖိုးအနိမ့်ဆုံးဖြင့် ဝယ်ယူနိုင်ဖို့ဆိုတာထက် သာမန်သုံးသူတို့အတွက်ဆိုပြီး ထုတ်ထားတဲ့ထုတ်ကုန်ဖြစ်ပါတယ်။ Windows 7 Home Basic ကိုသာမန်ရုံးစနစ်များ၊ မိသားစုအိမ်သုံးများအတွက်သင့်လျော်ပါတယ်။ Netowrk ကိုလည်း အဆင့်မနိမ့်ပဲရရှိခံစားနိုင်ပါတယ်။ မျက်နှာစာတွေများများလိုချင်လို့ Monitor တွေကို ၂လုံးမက တွဲဖက်ချိတ်ဆက်သုံးဆွဲနိုင်ပါတယ်။

Windows 7 Home Premium

Windows 7 ကိုအဆင့်လည်းမြင့်တာလိုချင်တယ်၊ ငွေကြေးကိုလည်းချွေတာလိုတယ်ဆိုခဲ့လျှင် Windows 7 Home Premium Edition ကိုသာရွေးချယ်လိုက်ပါ။ Professional အဆင့်မဟုတ်ပေမယ့် အနိမ့်စားလည်းမဟုတ်ပါဘူး။ အိမ်တွေ၊ ရုံးတွေအတွက်တော့ မြင့်မားတဲ့စွမ်းဆောင်ရည်တွေရရှိမှာပါ။ Netowrk ဆိုင်ရာကိုလည်း စွမ်းရည်မြင့်မြင့်ခံစားရမှာပါ။

Windows 7 Professional

Windows 7 အတွက်အဆင့်မြင့်ထုတ်ကုန်တစ်ခုဖြစ်ပါတယ်။ Professional Edition လို့ဆိုထားသည့်အတိုင်း Professional User တစ်ယောက်အတွက် ထူးခြားပြီးအသုံးတည့်စရာတွေ ရရှိခံစားရမှာပါ။ Windows Server ကိုလည်းချိတ်ဆက်သုံးစွဲခွင့်ရရှိမှာပါ။ စာဖတ်သူကွန်ပျူတာဟာ Internet လိုင်းတွေ၊ Network လိုင်းတွေကြားထဲကူးလူးနေရတယ်ဆိုလျှင် Professional Edition ကိုသုံးစွဲသင့်ပါတယ်။

Windows 7 Enterprise and Ultimate

Windows 7 အတွက်အဆင့်မြင့်ဆုံးထုတ်ကုန်ဖြစ်ပါတယ်။ Professional Edition ထက်သာတာတွေရှိနေလို့ Professional User တစ်ယောက်အတွက် အကောင်းဆုံးစမ်းသပ်ခံ၊ အသုံးတော်ခံ Windows တစ်ခုဖြစ်စေမှာပါ။ လွတ်လပ်စွာထိန်းချုပ်ခွင့်တွေကို အားပါးတရရှိမှာဖြစ်သလို၊ လိုင်စင်ဖြင့်ဝယ်ယူသူတွေကတော့ အခြားခံစားခွင့်များစွာကို Microsoft မှထပ်မံရရှိပါလိမ့်မယ်။

တရားဝင်လိုင်စင်ဖြင့်ဝယ်ယူဖို့ဆိုတာ စာရေးသူတို့မြန်မာနိုင်ငံမှာ မဖြစ်နိုင်သေးပါဘူး။ Windows System Program တစ်ခုဟာ၊ ကွန်ပျူတာတစ်လုံးထက်ပိုမိုဈေးကြီးနေလို့ဖြစ်တာကတစ်ကြောင်း၊ နည်းပညာတိုးတက်ဖို့ အားယူနေရချိန်မှာ အလွယ်သုံး၊ အပေါများဆုံးတွေသာဖြစ်သင့်တာက တစ်ကြောင်းကြောင့် ကျပ်ငွေတစ်ထောင်ပတ်ဝန်းကျင်နှင့် အသုံးတည့်နေတာကိုက မြန်မာနည်းပညာသမားတွေကံကောင်းနေတာပါ။

ယခုဆိုလျှင် ကွန်ပျူတာလက်ဝယ်ပိုင်ဆိုင်မှုနှုန်းဟာ တဟုန်ထိုး ထိုးတက်လာနေတာကို စာဖတ်သူတွေ့မြင်မှာပါ။ ဒါ့ကြောင့်ယခုလိုအချိန်ဟာ မြန်မာနိုင်ငံမှ နည်းပညာလေ့လာနေသူတွေအတွက် အချိန်ကောင်းသာ ဖြစ်ပါတယ်။

Key Features	Starter	Home Premium	Professional	Enterprise/Ultimate
Join a Domain and Group Policy controls			✓	✓
Remote Desktop Host			✓	✓
Advanced Backup and Restore (Network Backup & Group Policy)			✓	✓
Encrypting File System			✓	✓
Windows Mobility Center (with Presentation Mode)			✓	✓
Offline Folders			✓	✓
BitLocker and BitLocker To Go				✓
AppLocker				✓
DirectAccess				✓
BranchCache				✓
Multilingual User Interface Packs				✓
Enterprise Search Scopes				✓
Virtual Desktop Infrastructure (VDI) Enhancements **				✓
Direct Boot from VHD				✓

Windows OS လုပ်ငန်းစဉ်

စာဖတ်သူဟာ Honest Hacker ဖြစ်ချင်လို့ ဒီစာအုပ်ကိုလေ့လာတာဆိုလျှင် OS တွေရဲ့ ရပ်တည်အသက်ဝင်နေပုံတွေကို သိရှိထားရပါမယ်။ Windows OS တွေကို ပညာရှင်များစွာစုပြီး တည်ဆောက်ရေးဆွဲပါတယ်။ ကွန်ပျူတာ Power Button ကိုစတင်ဖွင့်လိုက်သည်နှင့် အမာထည်လျှပ်စီးပြားများတွင် လျှပ်စစ်စတင်စီးဆင်းပြီး Windows OS လည်ပတ်နိုင်လောက်သော ပစ္စည်းများပြည့်စုံရဲ့လား၊ ကောင်းမွန်စွာ လည်ပတ်နေရဲ့လားဆိုတာ စတင်စစ်ဆေးပါတယ်။ ၄င်းကို Boot Startpping လုပ်တယ်လို့ဆိုတယ်။

တပ်ဆင်ထားသည့် Hardware ပိုင်းဆိုင်ရာများဖြစ်တဲ့ Processor(CPU), Memory, Graphic Display, Harddisk အစတပ်ဆင်ထားသမျှတို့ကိုကောင်းမွန်ကြောင်းအတည်ပြုချက်ရယူသည်ကို Power On Self Test (POST) လို့ခေါ်ကြပါတယ်။

ပြီးလျှင် Windows OS ၏စတင်ခြင်းအတွက် OS Boot ကိုရှာဖွေပါတယ်။ Harddisk မှာရှိလျှင် တန်းတက်သွားပြီး၊ Harddisk ပျက်နေလို့၊ ဒါမှမဟုတ် OS Boot မရှိလျှင် OS BootDisk တစ်ခုခုပေးဖို့ တောင်းဆိုလာပါလိမ့်မယ်။

ကွန်ပျူတာကိုစတင်ဖွင့်လိုက်သည်နှင့် Windows OS စတင်ရန်အတွက် Boot File တွေလိုအပ်ပါတယ်။ Windows OS အတွက်အရေးပါ System File တွေကတော့ -

IO.SYS
CONFIG.SYS
MSDOS.SYS
AUTOEXEC.BAT
NTDETECT.COM

တို့ဖြစ်ပါတယ်။

ဒီ့ထက်ပိုသိသင့်တဲ့ Essential Startup Process File တွေကိုလည်းလေ့လာထားသင့်ပါတယ်။ ၄င်းကို Boot or Root Directory လို့လည်းခေါ်ဆိုနိုင်ပါတယ်။

Essential Startup Process File အချို့ကို အောက်ဖက်မှာဖော်ပြထားပါတယ်။

Ntldr

Windows စတင်မှုအတွက် Boot.ini File ကိုဖတ်ပါတယ်။ Windows စတင်ရန်မရှိမဖြစ် Ntoskrnl.exe, Bootvid.dll, Hal.dll တွေကိုရှာဖွေမောင်းနှင်ပါတယ်။ ၄င်းတို့နှင့်အတူတကွ Device Driver တွေကိုလည်း ရှာဖွေမောင်းနှင်ရပါတယ်။

Boot.ini

Windows စတင်မှုအတွက် Install Control File ဖြစ်ပါတယ်။

Ntdetect.com

Ntldr စတင်မှုတွင်ပါဝင်လုပ်ဆောင်ပါတယ်။ တပ်ဆင်ထားတဲ့ Basic Device တွေကို Executes and Loading တွေကိုတာဝန်ယူပါတယ်။

Pagefile.sys

Memory, Physical RAM တွေကိုစစ်ဆေးအတည်ပြုပေးပါတယ်။ Windows OS လိုအပ်သော Memory ပမာဏနှင့် Application လုပ်ဆောင်မှုများကို ထိန်းချုပ်ရန်အတွက်ဖြစ်ပါတယ်။

Ntbootdd.sys

Ntldr စတင်မှုတွင်ပါဝင်လုပ်ဆောင်ပါတယ်။ Boot-Code တွေကို disk တွေပေါ်မှာထိန်းချုပ်စီစဉ်ပေးပါတယ်။ Boot System နဲ့ System Drives တွေကိုသဟဇာတဖြစ်အောင်စီမံပေးသူလဲဖြစ်ပါတယ်။

အထက်ပါ Essential Startup Process File တွေကို Hacker တွေ၊ Virus ရေးသူတွေဟာ မျက်စိကျကြပါတယ်။ စနစ်တစ်ခုလုံးရဲ့ အသက်သွေးကြောတွေဖြစ်နေလို့ပါ။

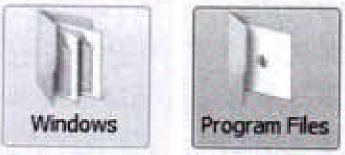
Windows Operation System File များရှိသောနေရာနှင့်အဓိက Control Files များကိုသိရှိထားသင့်ပါတယ်။ လိုအပ်လာလျှင် အလွယ်တကူ ရှာဖွေနိုင်မှာပါ။ စာဖတ်သူရဲ့ကွန်ပျူတာကို Windows OS ထည့်သွင်းထားလျှင်အောက်ဖော်ပြပါ Windows Operation System File များပါရှိနေပါလိမ့်မယ်။ Virus File ထင်ပြီး မှားဖျက်မိခြင်းမရှိစေရန်ဂရုပြုဖို့လိုပါတယ်။

စာဖတ်သူထည့်သွင်းထားတဲ့ Windows OS ဟာ Hard Disk Drive C: အောက်မှာရှိတယ်လို့ယူဆထားပါမယ်။ Drive C: ကိုဖွင့်ကြည့်တဲ့အခါ အောက်ပါအတိုင်းအဝါရောင် Folder များနှင့်ပုံမှန်ဖိုင်အချို့ကို တွေ့ရမှာပါ။

အထက်ပါပုံကဲ့သို့စာဖတ်သူကွန်ပျူတာမှာတွေ့မြင်ရမှာမဟုတ်ပါဘူး။ စာဖတ်သူများလေ့လာနိုင်စေရန် ကွယ်ဝှက်ထားသည်များကို စာရေးသူဖွင့်ပြထားခြင်းဖြစ်ပါတယ်။ အရောင်မှိန်နေတဲ့ Folder များနှင့် ဖိုင်များကို အလွယ်တကူမဖျက်မိစေရန်ကွယ်ဝှက်ထားပါတယ်။ ကွန်ပျူတာရဲ့စတင်မှုမှ ထိန်းချုပ်မှုအားလုံးအတွက် မရှိမဖြစ်ဖိုင်များဖြစ်နေလို့ပါ။ စာဖတ်သူတို့အတွက်အသုံးပြုနိုင်သောကြည့်ရှုမှုကိုမတားမြစ်ထားတဲ့ ဖိုင်တွေကိုတော့ ဒီတိုင်းထားရှိထားလို့ဖွင့်လှစ်လေ့လာနိုင်ပါတယ်။

မရှိမဖြစ်မပါမဖြစ် Folder တွေနဲ့၄င်းတို့အောက်မှ အရေးပါဖိုင်များကိုဆက်လက်လေ့လာပါမယ်။ Drive C: အောက်မှာအဓိကကျတဲ့ Folder ကြီးနှစ်ခုရှိပါတယ်။

Program Files Folder ကတော့ စာဖတ်သူထည့်သွင်းထားတဲ့လုပ်ငန်းအလိုက်အသုံးချ Application Program များကိုအစီအစဉ်တကျ အုပ်စုလိုက်ခွဲပြီးထားရှိရာနေရာဖြစ်ပါတယ်။



WINDOWS Folder ကတော့ Windows လုပ်ငန်းစဉ်များကိုစီမံရန် အုပ်စုဖွဲ့နေရာချထားတဲ့အပြင်၊ အရေးပါထပ်ဆင့် Folder များထပ်မံထားရှိပါတယ်။ ယခုစာဖတ်သူတွေ့ရမှာကတော့ WINDOWS Folder အောက်တွင်ထားရှိတဲ့အရေးပါ Folder များအောက်မှအဓိက System File များဖြစ်ပါတယ်။ ပထမဦးစွာသိထားသင့်သောအရေးပါဖိုင်များထားရှိတဲ့ Folder ကတော့ System32 ဖြစ်ပါတယ်။

System32 Folder အောက်ရှိအရေးပါဖိုင်များမှာ–

Ntoskrnl.exe Executive and kernel ဖိုင်တစ်ဖိုင်ဖြစ်ပါတယ်။

Ntkrnlpa.exe Windows အတွက် Physical Address Extension တွေကိုစီမံဖို့ မရှိမဖြစ်ဖိုင်တစ်ခုဖြစ်ပါတယ်။

Hal.dll Hardware abstraction layer အတွက်အဓိကအကျဆုံးဖိုင်တစ်ခု ဖြစ်ပါတယ်။ Virus တော်တော်များများမျက်စိကျ ဖျက်စီးတတ်တဲ့ ဖိုင်တစ်ခုဖြစ်ပါတယ်။ ၄င်းဖိုင်မရှိလျှင် ကွန်ပျူတာ တတ်မလာတော့ပါ။

Win32k.sys Kernel-mode part of the Win32 Subsystem အဖြစ်လုပ်ဆောင်ပါတယ်။ လက်တွဲညီစေဖို့တွဲဖက်လိုအပ်တဲ့ဖိုင်တစ်ခုလည်းဖြစ်ပါတယ်။

Ntdll.dll Windows အတွင်းပိုင်းတစ်ခုလုံးအတွက်အဓိကထောက်ပံ့နေတဲ့ စနစ်ဖိုင်ဖြစ်ပါတယ်။ ၄င်းဖိုင်ကိုလည်း Virus တွေဖျက်ဖို့အားထုတ်တတ်ကြပါတယ်။

Kernel32.dll, Advapi32.dll ,User32.dll ,Gdi32.dll

ဒီလေးဖိုင်ကတော့ Windows အတွက်အထောက်အပံ့ပြုနေတဲ့ Win32 subsystem DLLs File တွေဖြစ်ပါတယ်။

Hacker တွေရဲ့လုပ်ငန်းစဉ်ကျွမ်းကျင်မှုအတွက် အထောက်အပံ့လည်းရစေပါတယ်။

Open Source များကိုလေ့လာခြင်း

Open Source ဆိုတာ ယခုနှစ်ပိုင်းလူသိများလာတဲ့ လွတ်လပ်သော နည်းပညာဆိုင်ရာ လေ့လာစရာနေရာတွေဖြစ်လာပါတယ်။ လူသိအများဆုံး Open Source ကတော့ Linux ပဲဖြစ်ပါတယ်။ Windows OS တွေကြားထဲမှာ Microsoft Windows ဟာချုပ်ကိုင်မှုတွေနဲ့ တန်ကြေးမြင့်မြင့်ပေးရတာကြောင့် Linux OS ဟာအောင်မြင်မှုအထိုက်အလျှောက်ရလာပါတယ်။

သို့သော်လည်း လေ့လာရန်မလွယ်ကူခြင်း၊ တတ်ကျွမ်းသူနည်းပါးခြင်း၊ သင်တန်းရှားပါးခြင်းတို့ကြောင့် လေ့လာအသုံးပြုသူနည်းပါးခဲ့ပါတယ်။ ယခုနှစ်ပိုင်းမှာတော့ Ubuntu ကိုရေးထုတ်ခဲ့ပြီး မြန်မာမှ ကျွမ်းကျင်ပညာရှင်များက အထောက်အပံ့တွေပေးခဲ့ပါတယ်။ ဒါ့ကြောင့် ဒီနှစ်ပိုင်းမှာ Ubuntu ကိုသုံးလာသူတွေ များလာပါပြီ။

နာမည်ရခဲ့တဲ့ Open Source OS တွေကတော့–

Gentoo 2.6.24-gentoo-r5 GRUB 0.97

Ubuntu 2.6.24.3-debug GRUB 0.97

Debian 2.6.18-6-6861 GRUB 0.97

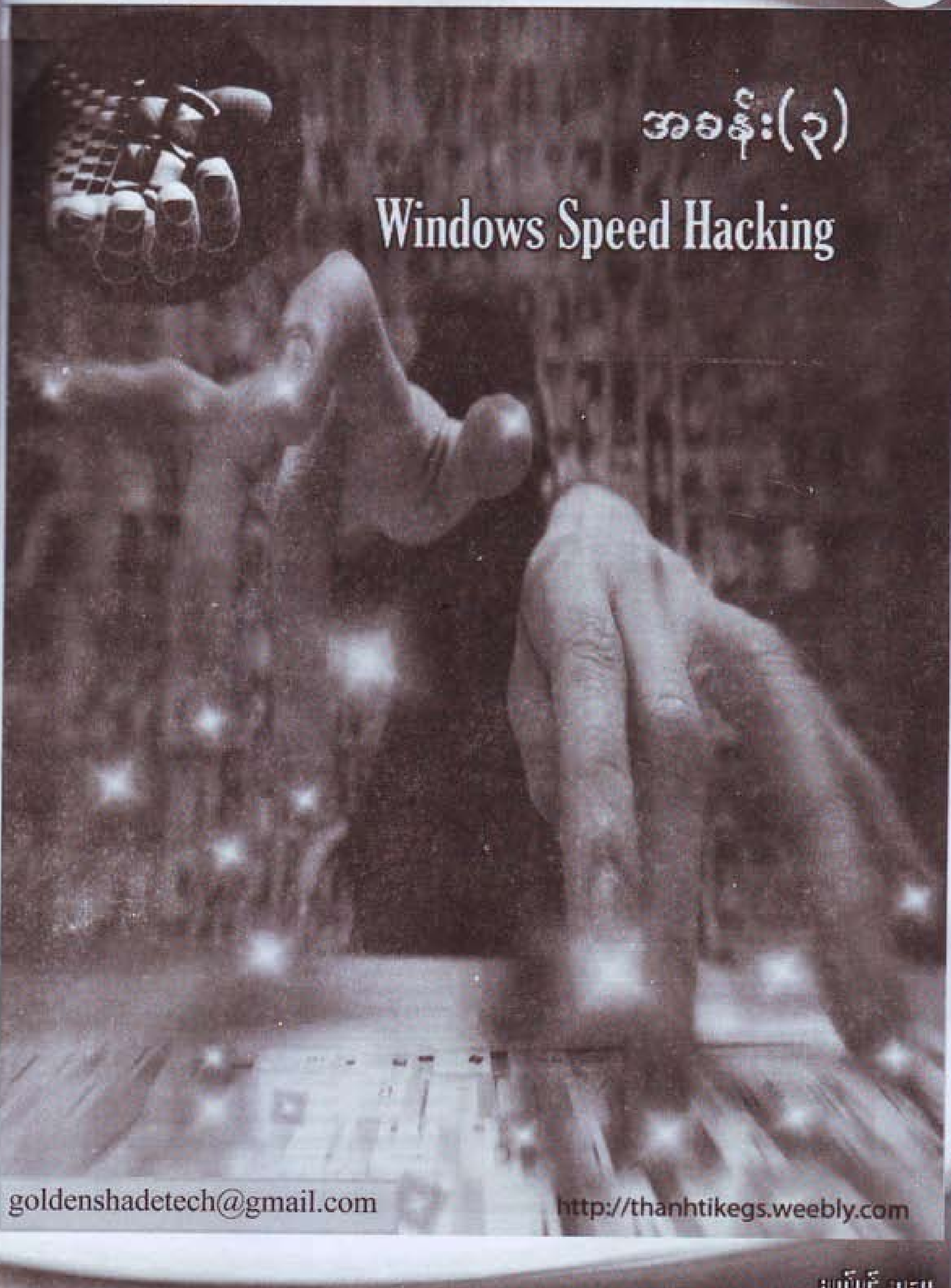
Fedora 2.6.25.9-76.fc9.i6862 GRUB 0.97

Office ပိုင်းဆိုင်ရာမှာလည်း Open Office.org 3.1 ထွက်ရှိလာပါတယ်။ လေ့လာနိုင်ရန် ယခုစာအုပ်နှင့်တွဲပါသော CD ထဲတွင်ထည့်သွင်းပေးထားပါတယ်။

Open Source Program တွေဟာ ရေးသားပုံ Programming Code တွေကိုပြန်လည်လေ့လာနိုင်သလို၊ မိမိစိတ်ကြိုက်ပြန်လည်ရေးသားပြုပြင်နိုင်ပါတယ်။ Programming ဘာသာရပ်လေ့လာနေသူများအတွက် လေ့လာသင့်သောစနစ်ဖြစ်ပါတယ်။

နိုင်ငံတကာမှ Hacker တွေဟာ Windows OS ကိုမသုံးကြပါဘူး။ Linux OS ကိုသာအသုံးပြုပြီး လေ့လာရှာဖွေစမ်းသပ်ကြပါတယ်။ ဒါ့ကြောင့် မြန်မာနိုင်ငံမှ ကွန်ပျူတာနည်းပညာအထူးပြုလေ့လာနေသူများအနေဖြင့် စမ်းသပ်သုံးစွဲသင့်ပါတယ်။

စာဖတ်သူများအတွက် Linux OS နှင့် Open Source Program များကိုအလွယ်လေ့လာနိုင်ဖို့ စာတစ်အုပ်အဖြစ်ထုတ်ဝေဖို့စီစဉ်ပါဦးမယ်။


အခန်း(၃)
Windows Speed Hacking
goldenshadetech@gmail.com
http://thanhtikegs.weebly.com

Windows 7 ကိုအရှိန်မြင့်ရန် Hack လုပ်ခြင်း

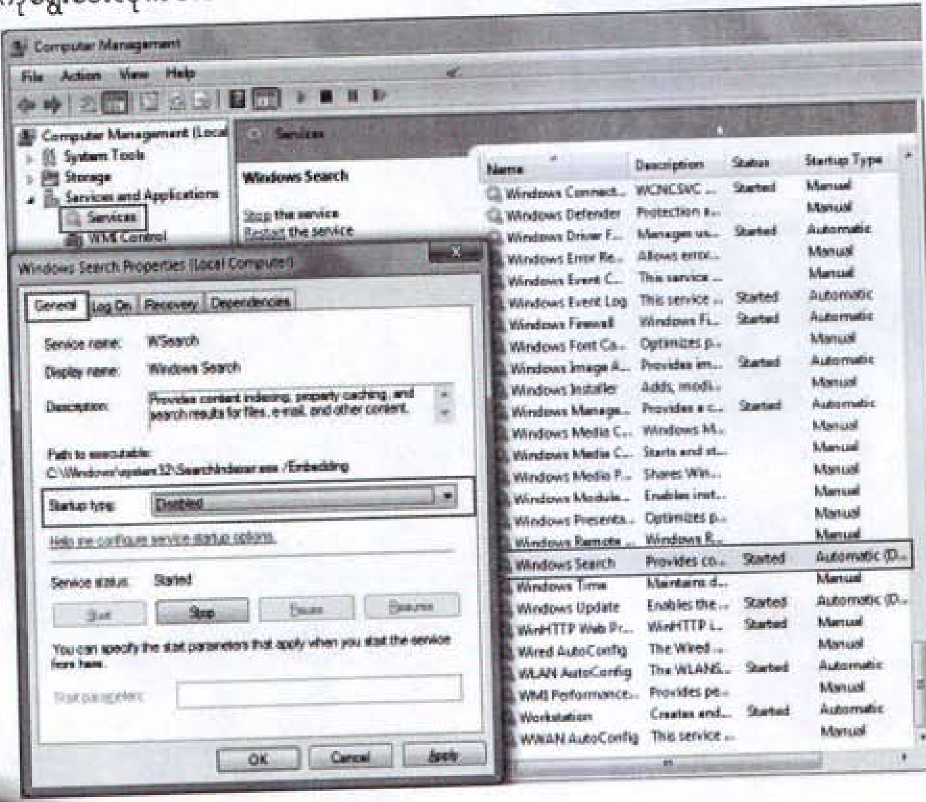
Windows 7 အသုံးပြုသူတွေဟာ Windows 7 ကိုအမြန်ဆုံးမဟုတ်တောင် အတော်ပင်မြန်ဆန်ဖို့ မျှော်လင့်နေကြမယ်ထင်ပါတယ်။ အမြန်နှုန်းမြှင့်တင်နည်းအများကြီးရှိပါတယ်။ ဒါကတော့ Windows ရဲ့လုပ်ဆောင်ချက်တွေကို လျှော့ချပြီး အမြန်နှုန်းကိုမြှင့်တင်နိုင်ပါတယ်။ အောက်ပါအတိုင်း အချက် (၉) ချက်ကို ပြုလုပ်ဆောင်ရွက်ရပါမယ်။

၁။ Search Indexing Feature ကိုပြင်ဆင်ခြင်း

၁- My Computer ကို Right Click နှိပ်ပြီး Manage ကိုရွေးပါ။

၂- Services and Applications အောက်မှ Services ကိုနှိပ်ပါ။ ညာဖက်ခြမ်းမှ Windows Search Property ကိုရွေးပြီးကလစ်နှစ်ချက်ဆင့်နှိပ်လိုက်ပါ။

၃- Windows Search Property Box မှ General Tab အောက်တွင် Startup Type အားဖွင့်ပြီး Disable ကိုရွေးပေးလိုက်ပါ။



၂။ User Account Control ကိုပြင်ဆင်ခြင်း

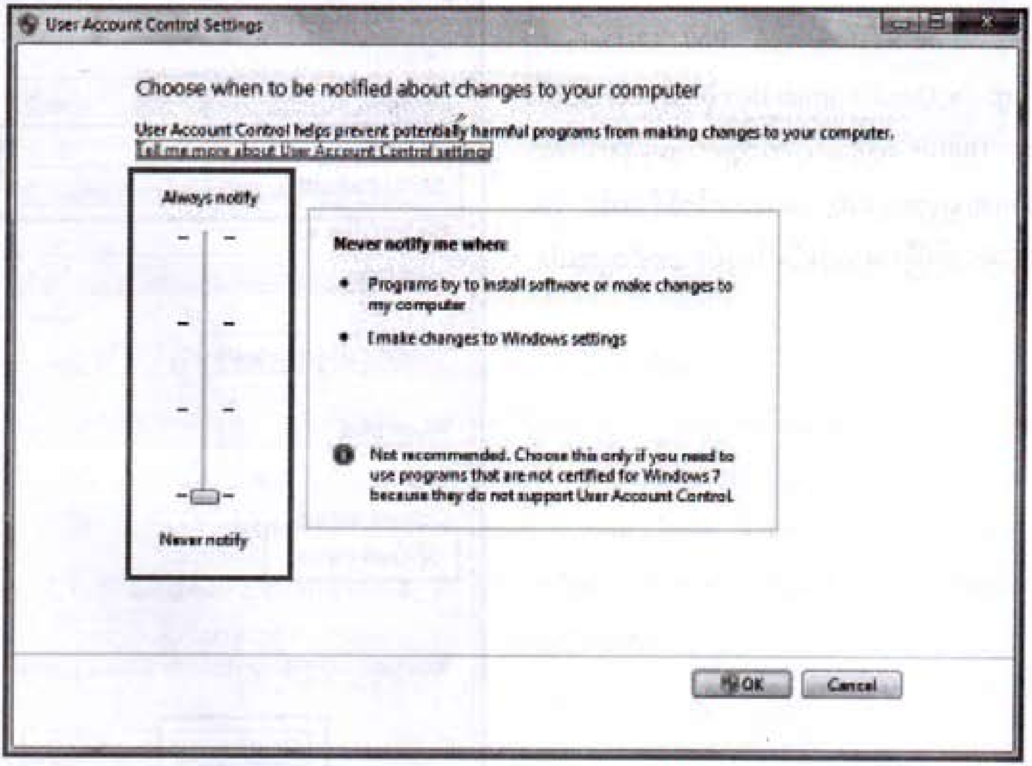
၁- Control Panel ကိုဖွင့်ပြီး User Accounts and Family Safety ကိုဖွင့်ပါ။ အတွင်းမှ User Account ကိုရွေးပါ။

၂- User Account Control settings ကိုနှိပ်ပါ။

၃- Always Notify နှင့် Never Notify Slider ဘားတန်းတွင် Never Notify နေရာသို့ ဆွဲချလိုက်ပါ။

OK Button ကိုနှိပ်လိုက်လျှင်ရပါပြီ။ ပြီးလျှင် ကွန်ပျူတာကို ပြန်လည်စတင်ရန် Reboot ပြုလုပ်ပါ။

သတိပြုရန်မှာ- အဆိုပါလုပ်ဆောင်ချက်ဟာ လိုင်စင်ဗားရှင်းသုံးသူများအတွက် အန္တရာယ် ရှိလာနိုင်ပါတယ်။ ကူးယူဗားရှင်းကိုသုံးသူများအတွက်ကတော့ သိပ်ပြဿနာမရှိနိုင်ပါဘူး။



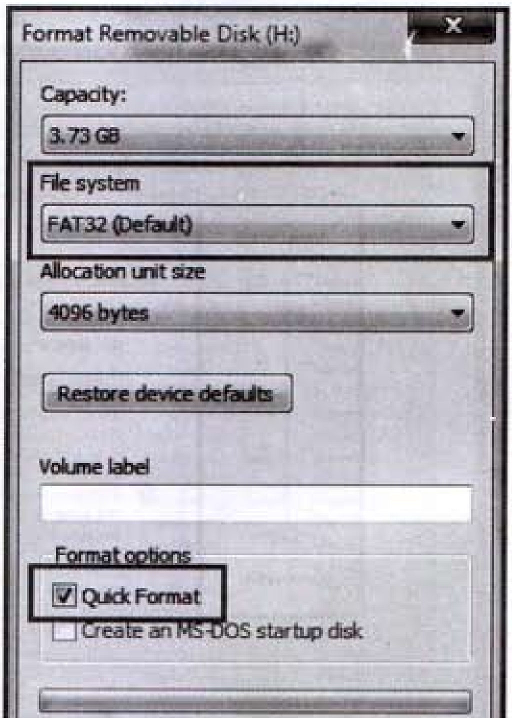
၃။ Extra Speed Booster ကိုအသုံးပြုခြင်း

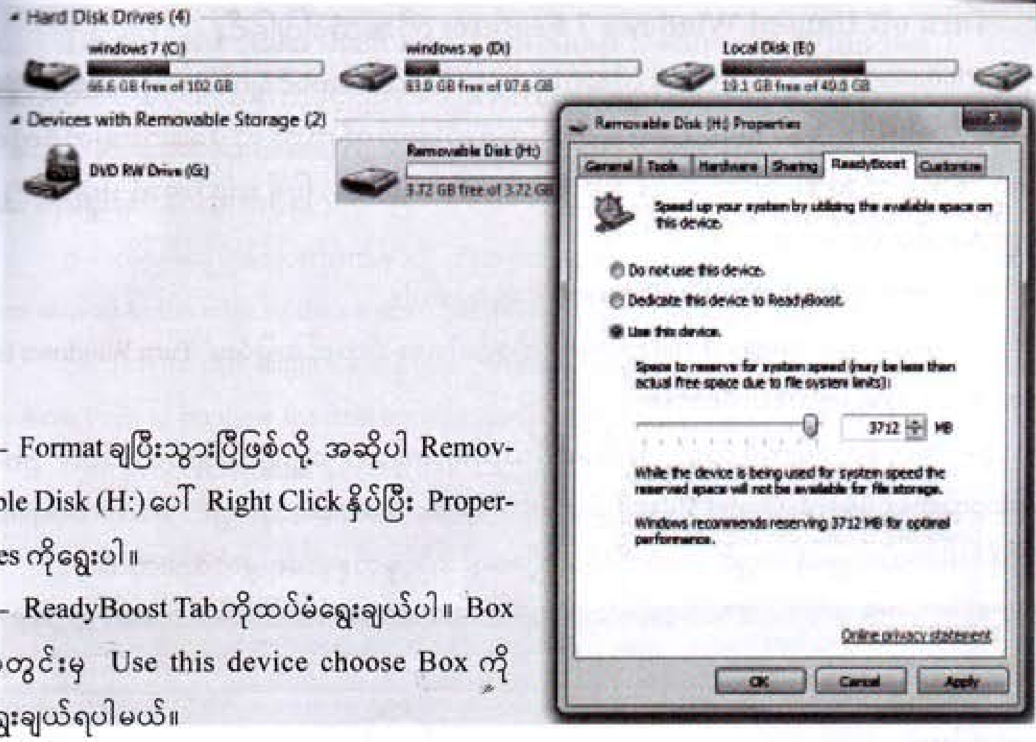
USB Drive/Pendrive တစ်ခုကိုအသုံးပြုပြီး Windows ကိုအရှိန်မြင့်တင်ဖို့လိုအပ်တဲ့အချိန်မှာ USB Drive/Pendrive တပ်ဆင်လိုက်တာနဲ့ လိုအပ်တဲ့အရှိန်တစ်ခုရလာမယ်ဆိုလျှင် သိပ်ကောင်းမယ်လို့ ထင်ကြတဲ့သုံးစွဲသူတွေအတွက် Windows 7 ကဖြည့်ဆီးပေးလိုက်ပါတယ်။

အဓိကကျတဲ့အချက်ကတော့ အဆိုပါ USB Drive/Pendrive ဟာ Memory Space 4.0 GB ရှိရပါမယ်။ USB Drive အတွင်းအခြားမှတ်စုများထားရှိလို့မရတော့ပါဘူး။ USB Booster သုံးရန် သီးသန့်ဖြစ်သွားပါလိမ့်မယ်။

၁- USB Drive/Pendrive ကို Format ချရပါမယ်။ My Computer => Removable Disk(H:) ပေါ် Right Click နှိပ်ပြီး Format ကိုရွေးပါ။

File System တွင် FAT 32(Default) ကိုရွေးပါ။ Quick Format Box မှာအမှတ်တပ်ပါ။ Start Button ကိုနှိပ်လိုက်လျှင် အမှန်တကယ် Format ချမှာလားလို့ မေးလာပါလိမ့်မယ်။ Ok, Yes သာဖြေပြီးအဆင့်လိုက်လုပ်ဆောင်သွားပါ။





၂– Format ချပြီးသွားပြီဖြစ်လို့ အဆိုပါ Removable Disk (H:)ပေါ် Right Click နှိပ်ပြီး Properties ကိုရွေးပါ။

၃– ReadyBoost Tab ကိုထပ်မံရွေးချယ်ပါ။ Box အတွင်းမှ Use this device choose Box ကို ရွေးချယ်ရပါမယ်။

၄– System Limits Slide ဘားတန်းကိုတော့ အသုံးပြု USB Stick ဟာ 4.0 GB (avg; 4000 MB) ဖြစ်တာကြောင့် Auto အနေဖြင့် System Limits 3712 MB ကိုပေးပါလိမ့်မယ်။ ပေးသည့် အတိုင်းသာ ရယူပါမယ်။

အဆင်သင့်ဖြစ်နေပြီဖြစ်လို့ OK Button ကိုသာနှိပ်လိုက်ပါ။

စာဖတ်သူအနေဖြင့် တစ်ချိန်ချိန်မှာ လက်ရှိသုံးနေတဲ့ကွန်ပျူတာကိုအရှိန်မြှင့်တင်လိုတဲ့အခါ အဆိုပါ USB Stick ကိုတပ်ဆင်လိုက်သည်နှင့် အရှိန် ၅–၁၀ ရာခိုင်နှုန်းနီးပါးမြင့်တက်လာပါလိမ့်မယ်။ စာရေးသူစမ်းသပ်ကြည့်သလောက်ကတော့ 8.0 GB မှာ System Limits 7712 MB ထိပေးထားတဲ့အတွက် ၂၀ မှ ၃၅ ရာခိုင်နှုန်းထိမြင့်တက်လာပါတယ်။ စာရေးသူလက်ရှိသုံးနေတဲ့ ကွန်ပျူတာပေါ်မှာ စမ်းသပ်လိုက်တာပါ။ ကွန်ပျူတာတပ်ဆင်ထားတာတွေကတော့ –

CPU - Dual Core 2.7 GHz

RAM - 2 GB

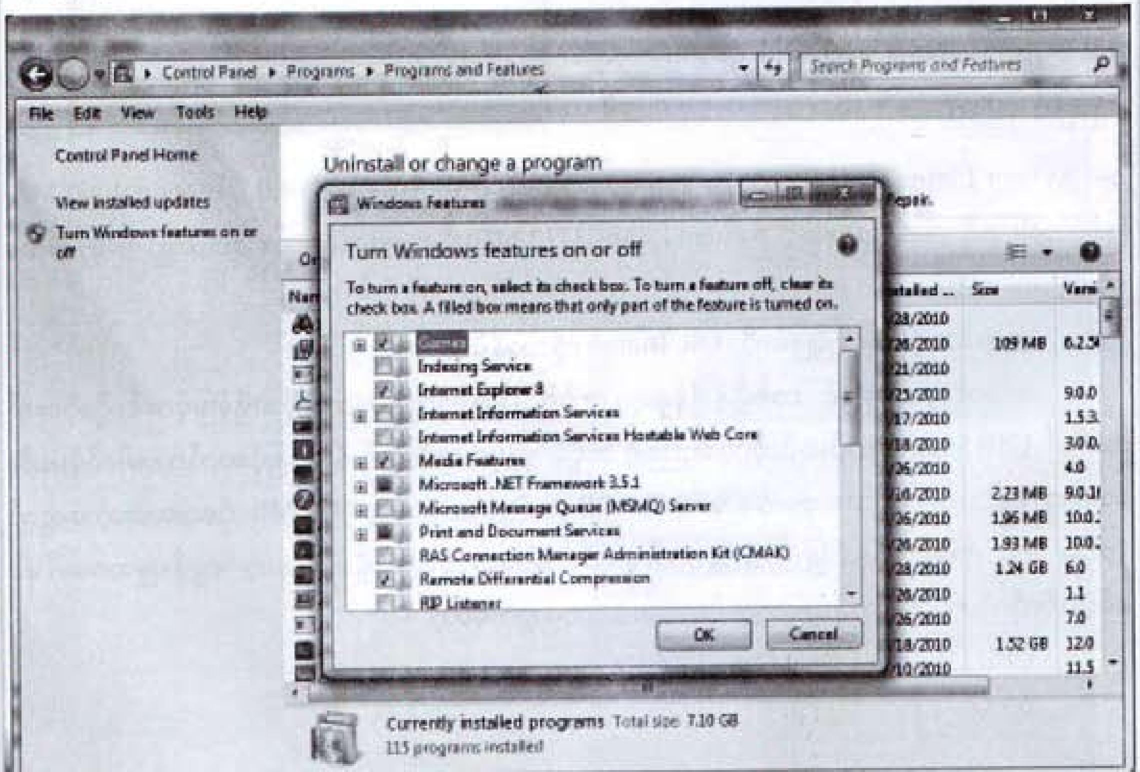
၄။ Turn off Unused Windows 7 Features ကိုအသုံးပြုခြင်း

Windows ကိုအရှိန်မြှင့်တင်ဖို့လိုအပ်တဲ့အောက်ပါလုပ်ဆောင်ချက်များကို အဆင့်လိုက် လုပ်ဆောင်သွားပါ။ သတိပြုရမည်ကတော့ အမှတ်ဖြုတ်လိုက်တဲ့လုပ်ဆောင်ချက်တွေကို ပြန်လည်စတင်တဲ့အခါ အသုံးပြုနိုင်မည်မဟုတ်တော့ပါ။ ပြန်လည်အသုံးပြုလိုလျှင် ပြန်လည်အမှတ်တပ်နိုင်ပါတယ်။

၁– Control Panel ကိုဖွင့်ပြီး Program ကိုရွေးချယ်ပါ။

၂– ထိုအောက်မှ Program and Features ကိုဖွင့်ပါ။ ဘယ်ဘက်အခြမ်းမှ Turn Windows features on or off ကိုရွေးချယ်နှိပ်လိုက်ပါ။

၃– အကုန်လုံးဖြုတ်ဖို့ထက် အသုံးမလိုသည်များကိုသာ ရွေးချယ်ဖြုတ်လိုက်ပါ။ ဥပမာ ဂိမ်းမဆော့လျှင် ထိပ်ဆုံးမှ Games Box ကိုဖြုတ်နိုင်ပါတယ်။ Internet မသုံးလျှင် Internet Explorer ကိုဖြုတ်နိုင်ပါတယ်။ ဖြစ်နိုင်လျှင် ဖြုတ်လိုက်သည့်စာရင်းကို မှတ်စုမှာရေးမှတ်ထားလိုက်ပါ။



၅။ Disable the Aero Peek and Aero Snap features in Windows 7

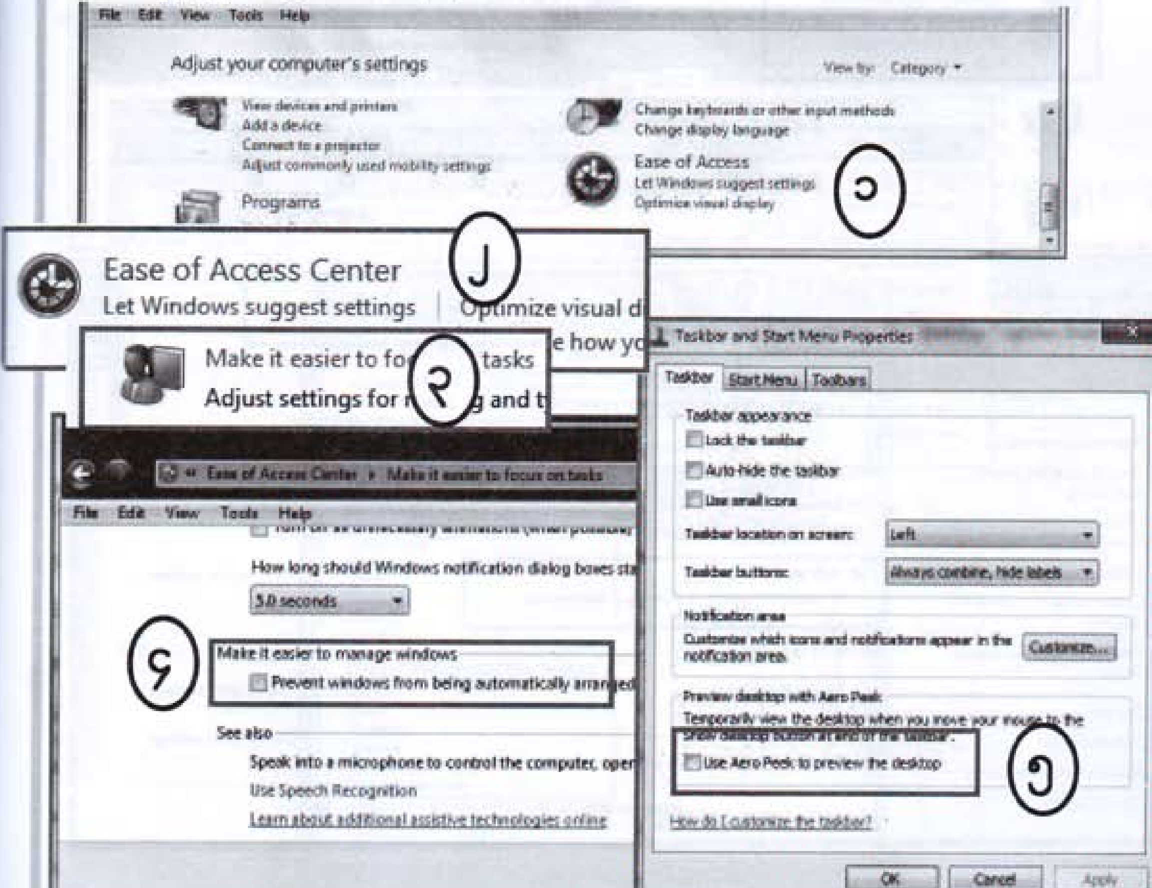
၁– Control Panel ကိုဖွင့်ပြီး Ease of Access ကိုရွေးချယ်ပါ။

၂– ထိုအောက်မှ Ease of Access Center ကိုဖွင့်ပါ။ ၎င်းအတွင်းမှ Make it easier to focus on tasks ကိုရွေးချယ်နှိပ်လိုက်ပါ။

၃– ထိုမြင်ကွင်းအောက်ဖက်နားရှိ Prevent windows from being automatically arranged when moved to the edge of the screen ကိုအမှတ်ဖြုတ်လိုက်ပါ။ Ok ဖြင့်ထွက်ပါ။

၄– Taskbar ပေါ် Right Click နှိပ်ပြီး Property ကိုရွေးချယ်ပါ။ ပြီးလျှင် Taskbar Tab အောက်မှ Use Aero Peek to preview the desktop ကိုအမှတ်ဖြုတ်လိုက်ပါ။

ကွန်ပျူတာကို Restart ချလိုက်ပါ။

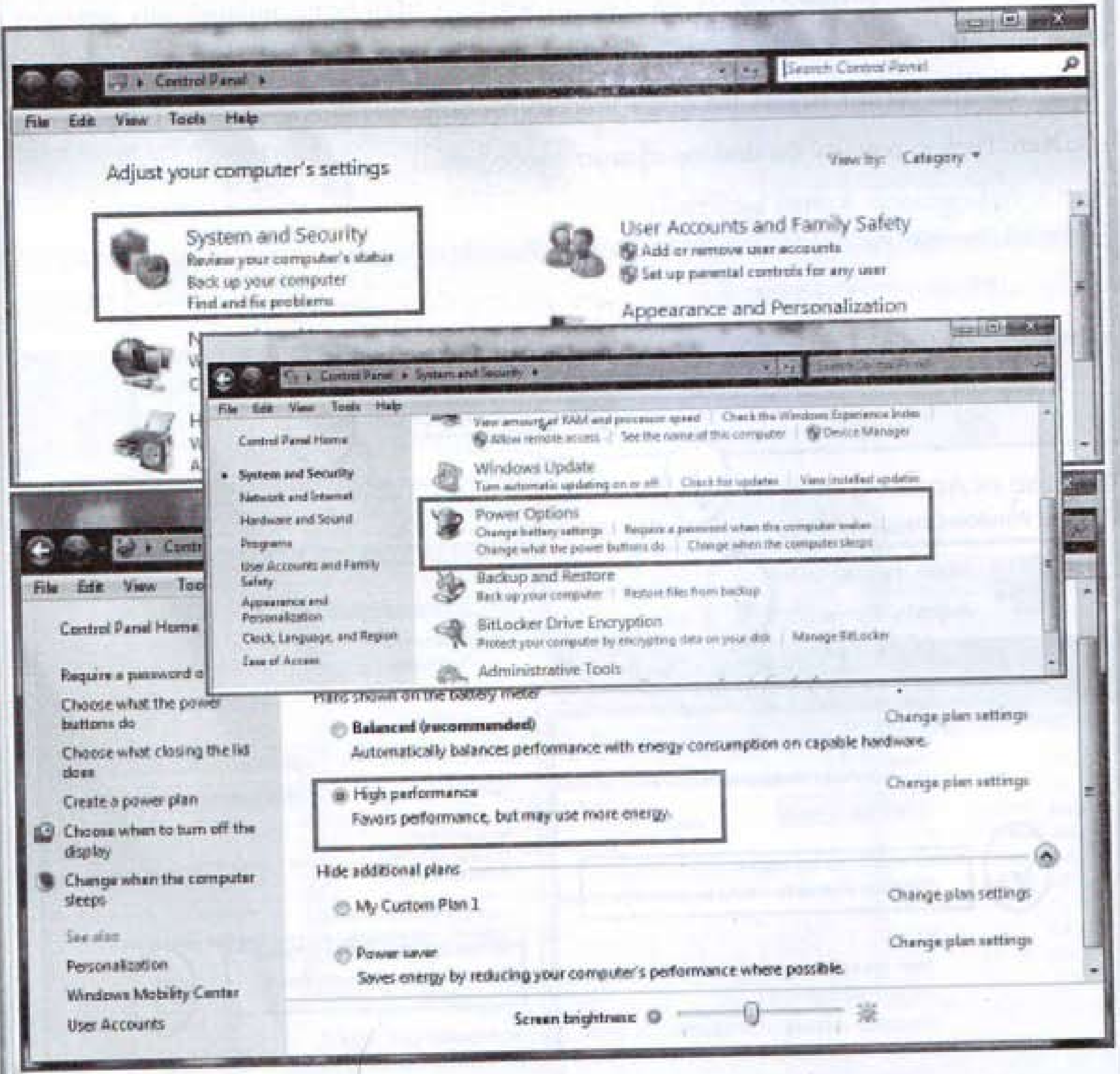


၆။ Change the Power Plan To Maximum Performance ကိုအသုံးပြုခြင်း

၁- Control Panel ကိုဖွင့်ပြီး System and Security ကိုရွေးချယ်ပါ။

၂- ထိုအောက်မှ Power Options ကိုဖွင့်ပါ။

၃- ထိုမြင်ကွင်းအတွင်းမှ High Performance ကိုအမှတ်တပ်လိုက်ပါ။



၇။ Softwares To Speed Up Windows 7 ကိုလေ့လာခြင်း

စာဖတ်သူအနေဖြင့် ဘယ် Windows ပဲသုံးသုံး ကွန်ပျူတာရဲ့လုပ်ဆောင်ချက်တွေကို မြင့်မားစွာသုံးနိုင်ရန် အောက်ပါ Software တစ်မျိုးမျိုးကိုသုံးစွဲသင့်ပါတယ်။

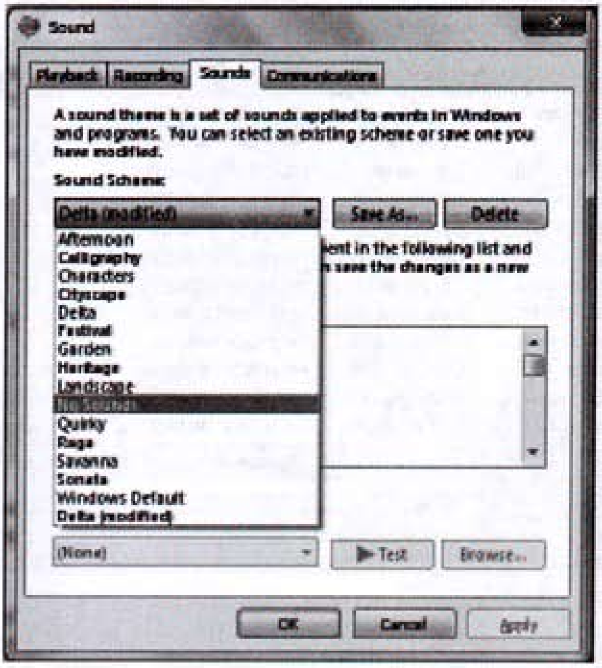
* Wise Registry Cleaner
* CCleaner (စီဒီထဲတွင်ထည့်သွင်းပေးထားပါတယ်)
* TCP Optimizer
* TeraCopy
* Startup Delayer

၈။ Disable Unwanted System Sounds in Windows 7 ကိုလေ့လာခြင်း

၁- Windows Key နှင့် R ကိုပေါင်းနှိပ်ပြီး Run Box ကိုဖွင့်ပါ။

၂- ထိုအထဲတွင် mmsys.cpl ကိုထည့်သွင်းပြီး Enter ခေါက်ပါ။

၃- ထိုမြင်ကွင်းအတွင်းမှ Sounds Tab ကိုရွေးပါ။ Sound Scheme Choose Box နေရာတွင် No Sounds ကိုရွေးချယ်လိုက်ပါ။ ထပ်မံရွေးချယ်ဖို့ပြောလျှင် Cancel လို့ပြောလိုက်ပါ။



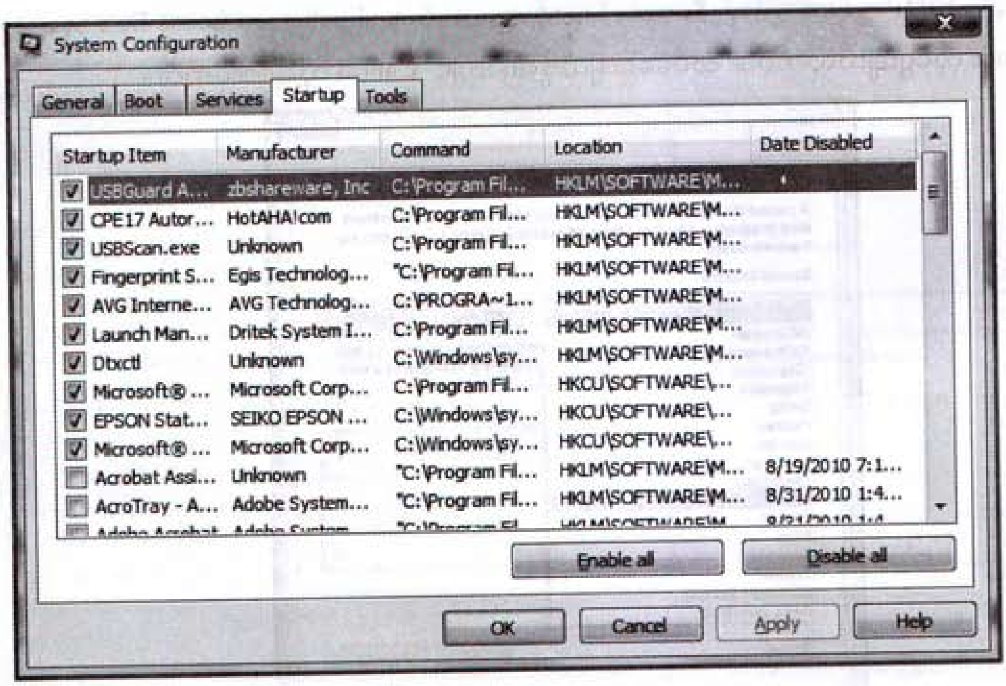
၉။ Disable Unwanted Start Up Items and Speed Up ကိုအသုံးပြုခြင်း

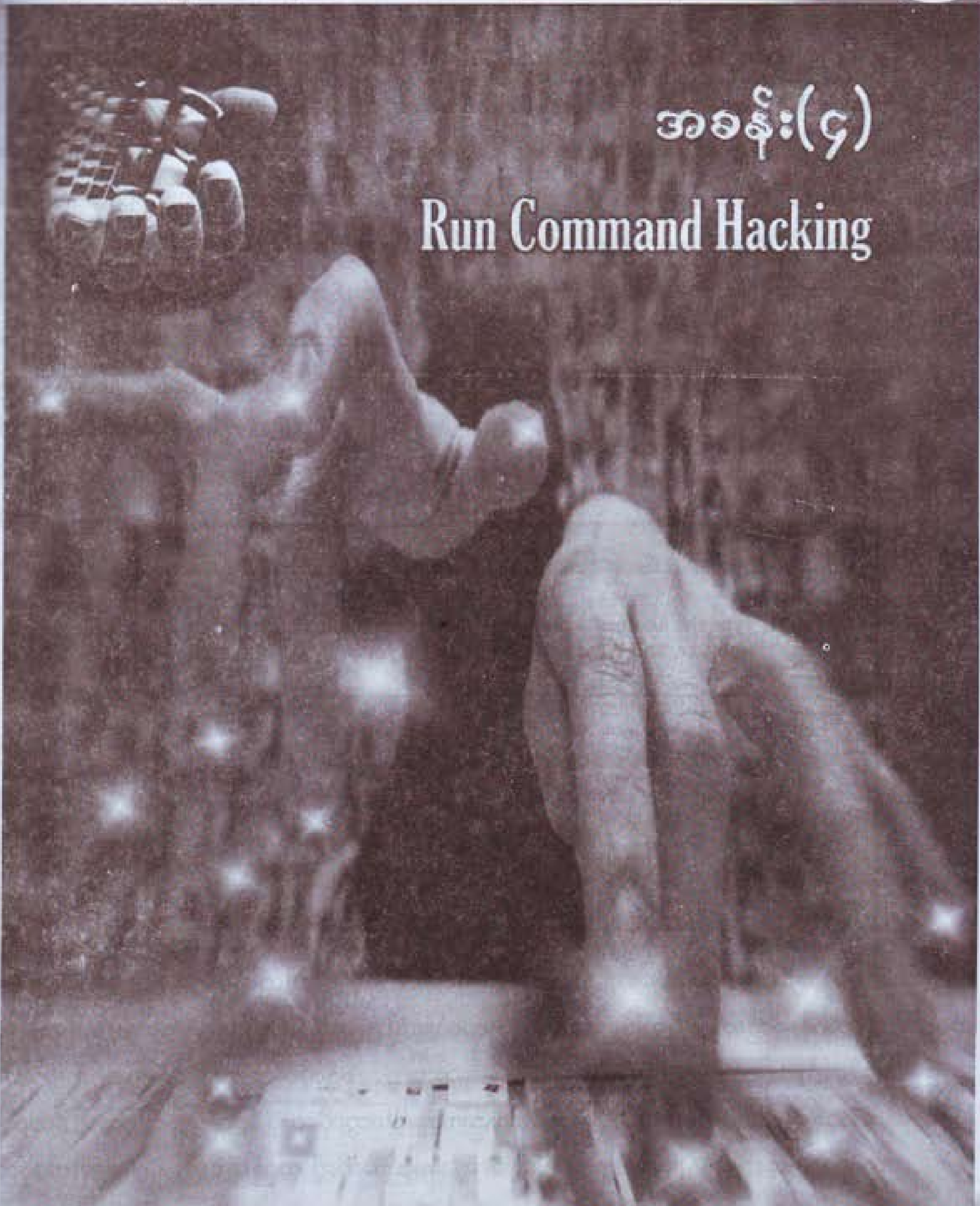
စက်စတင်တင်ခြင်း ဖွင့်လှစ်ရမယ့် Program စာရင်းတွေရှိတဲ့နေရာကိုသွားရောက်ပြီး စာဖတ်သူကိုယ်တိုင် Install လုပ်ထားတဲ့ Program အချို့မှ စတင်လျှင်တင်ခြင်း မလိုအပ်သည့် Program တွေကိုဖြုတ်လိုက်လျှင် အတော်ပင်မြန်ဆန်လာပါတယ်။

၁- Windows Key နှင့် R ကိုပေါင်းနှိပ်ပြီး Run Box ကိုဖွင့်ပါ။

၂- ထိုအထဲတွင် msconfig ကိုထည့်သွင်းပြီး Enter ခေါက်ပါ။

၃- ထိုမြင်ကွင်းအတွင်းမှ Startup Tab ကိုရွေးပါ။ အတွင်းတွင် အသုံးချ Application Program များကိုတွေ့ရပါလိမ့်မယ်။ Anti-Virus Program တွေကလွဲလျှင်အမှတ်ဖြုတ်လိုက်ပါ။ Restart ချဖို့လိုပါတယ်။ အကယ်၍ စာဖတ်သူအတွက်အမှန်တကယ်လိုအပ်သည်ကို ပိတ်ထားမိလျှင် အထက်ပါအတိုင်းပြန်လည်ဝင်ရောက်ပြီးအမှတ်ပြန်တပ်လိုက်ပါ။





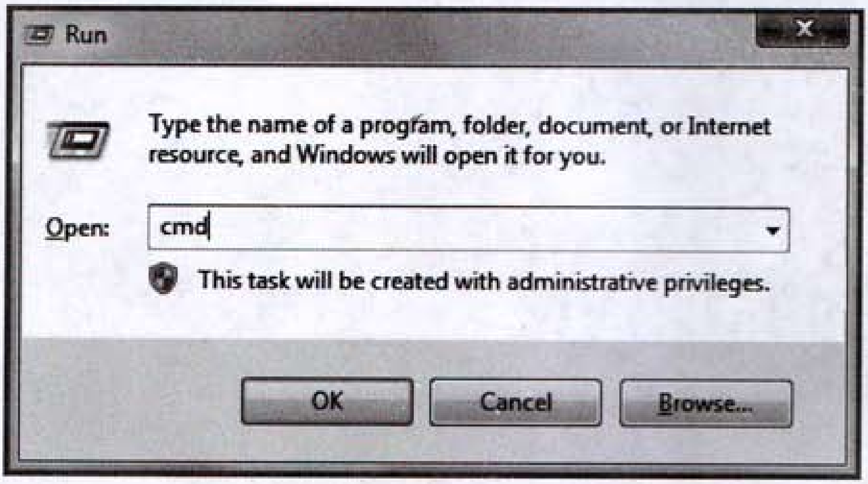
အခန်း(၄)
Run Command Hacking
goldenshadetech@gmail.com
http://thanhtikegs.weebly.com

Run Box မှတိုက်ရိုက်ဖွင့်နိုင်သော Command Key များကိုလေ့လာခြင်း

Honest Hacker တွေဟာ System Controller တွေကိုအမြန်ဆုံးဖွင့်တတ်သုံးတတ်ရပါမယ်။ ဥပမာ–ဂဏန်းပေါင်းစက် (Calculator)ကိုသုံးနိုင်ရန် Start => All Programs => Accessories => Calculator မှအဆင့်လိုက် ဝင်ရောက်ဖွင့်ရပါတယ်။ ဒီ့ထက်မကသော အသုံးဝင် Application Programs လေးတွေကို Run Box မှတစ်ဆင့်တိုက်ရိုက်ဖွင့်သုံးနိုင်ပါတယ်။

စာဖတ်သူတွေ့မြင်ဖူးမှာပါ။ ကွန်ပျူတာကျွမ်းကျင်သူတွေ၊ Service Technician တွေဟာ အဆိုပါ Run Command တွေကိုကျွမ်းကျင်စွာကိုင်တွယ်နေတာကိုပါ။ စာဖတ်သူလည်းကျက်ထားလိုက်ပေါ့နော်။

Run Box ကိုဖွင့်တဲ့ Shortcut ကိုတော့ဖော်ပြခဲ့ပြီးပြီနော်။ မှတ်မိသေးရဲ့လား။ Windows Key + R ဖြစ်ပါတယ်။



စာဖတ်သူသတိပြုရမှာကတော့ Shortcut Name တွေကိုမှန်ဖို့လိုပါတယ်။ မှားနေလျှင်မပွင့်လာပါ။ အမည်ရှည်တွေကိုလည်းတိုက်ရိုက်ဖြည့်သွင်းနိုင်ပါတယ်။ ဒါပေမယ့် စာလုံးပေါင်းတော့မှန်ပါစေ။

တစ်ဖက်စာမျက်နှာမှာRun Command တွေကိုအက္ခရာစဉ်လိုက်အကန့်ခွဲဖော်ပြထားပါတယ်။ မြန်မာလိုသီးသန့်မရှင်းပြတော့ပါ။ အသုံးများ Run Command တွေကိုတော့ စာလုံးနဲနဲထူပြထားပါတယ်။

စာဖတ်သူဖွင့်လိုတဲ့ Application Programs ရဲ့ အမည်အတိုကို ထည့်သွင်းပြီး Enter ခေါက်လိုက်တာနဲ့ အဆိုပါ Programs ပွင့်လာပါလိမ့်မယ်။

	Program/Utility	Run Command
1	Accessibility Controls	access.cpl
2	**Add Hardware Wizard**	**hdwwiz.cpl**
3	**Add/Remove Programs**	**appwiz.cpl**
4	Administrative Tools	control admintools
5	Authorization Manager	azman.msc
6	Automatic Updates	wuaucpl.cpl
7	Bluetooth Transfer Wizard	fsquirt
8	**Calculator**	**calc**
9	Certificate Manager	certmgr.msc
10	**Character Map**	**charmap**
11	**Check Disk Utility**	**chkdsk**
12	Clipboard Viewer	clipbrd
13	**Command Prompt**	**cmd**
14	Component Services	dcomcnfg
15	Computer Management	compmgmt.msc (or) CompMgmtLauncher
16	**Control Panel**	**control**
17	**Date and Time Properties**	**timedate.cpl**
18	**Device Manager**	**devmgmt.msc**
19	Direct X Control Panel (If Installed)	directx.cpl
20	Direct X Troubleshooter	dxdiag
21	**Disk Cleanup Utility**	**cleanmgr**
22	**Disk Defragment**	**dfrg.msc**
23	Defragment User Interface	dfrgui
24	**Disk Management**	**diskmgmt.msc**
25	**Disk Partition Manager**	**diskpart**

26	Display Properties	control desktop
27	Display Properties	desk.cpl
28	Display Properties (w/Appearance Tab Preselected)	control color
29	Ditilizer Calibration Tool	tabcal
30	Downloads	Downloads
31	DPI Scaling	dpiscaling
32	Driver Package Installer	dpinst
33	Dr. Watson System Troubleshooting Utility	drwtsn32
34	Driver Verifier Utility	verifier (or) reset
35	DVD Player	dvdplay
35	Encryption File System	rekeywiz
37	Event Viewer	eventvwr.msc
38	Fax Cover Sheet Editor	fxscover
39	File Signature Verification Tool	sigverif
40	Findfast	findfast.cpl
41	Folders Properties	control folders
42	**Fonts (Control Panel)**	**control fonts**
43	Fonts Folder	fonts
44	Free Cell Card Game	freecell
45	Game Controllers	joy.cpl
46	Group Policy Editor	gpedit.msc
47	Iexpress Wizard	iexpress

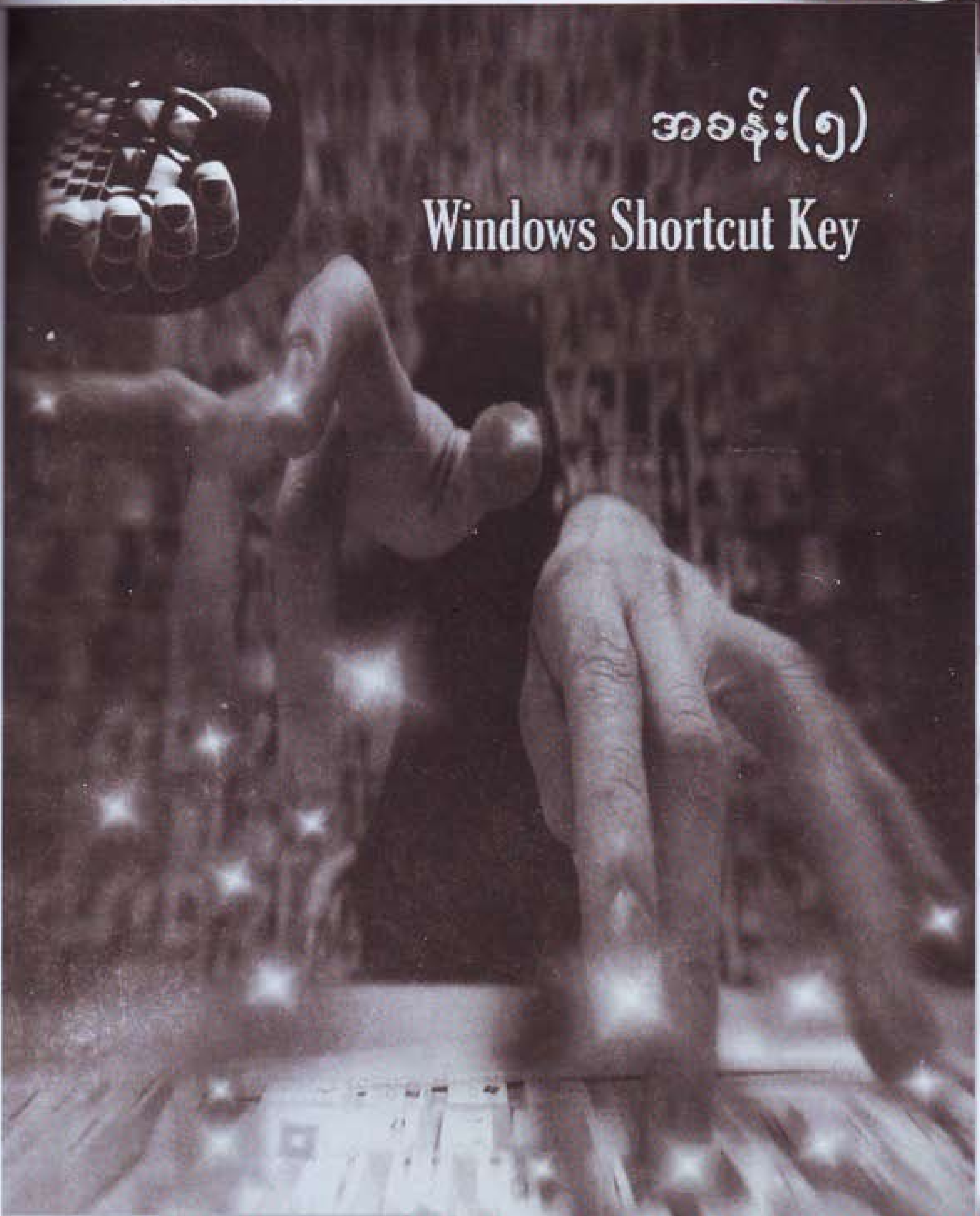
48	Indexing Service	ciadv.msc
49	Internet Properties	inetcpl.cpl
50	Internet Explorer	iexplore
51	**IP Configuration (Display Connection Configuration)**	**ipconfig /all**
52	IP Configuration (Display DNS Cache Contents)	ipconfig /displaydns
53	IP Configuration (Delete DNS Cache Contents)	ipconfig /flushdns
54	IP Configuration (Release All Connections)	ipconfig /release
55	IP Configuration (Renew All Connections)	ipconfig /renew
56	IP Configuration (Refreshes DHCP & Re-Registers DNS)	ipconfig /registerdns
57	IP Configuration (Display DHCP Class ID)	ipconfig /showclassid
58	IP Configuration (Modifies DHCP Class ID)	ipconfig /setclassid
59	iSCSI Initiator	iscsicpl
60	Java Control Panel (If Installed)	jpicpl32.cpl
61	Java Control Panel (If Installed)	javaws
62	Keyboard Properties	control keyboard
63	Libraries (Explorer)	explorer or Windows key + E
64	Local Security Settings	secpol.msc
65	Local Users and Groups	lusrmgr.msc

66	Log Out Of Windows	logoff
67	Microsoft Chat	winchat
68	Microsoft Support Diagnostic Tool	msdt
69	Microsoft Paint	mspaint
70	Mouse Properties	control mouse
71	**Mouse Properties**	**main.cpl**
72	Network Connections	control netconnections
73	Network Connections	ncpa.cpl
74	Network Setup Wizard	netsetup.cpl
75	**Notepad**	**notepad**
76	Object Packager	packager
77	On Screen Keyboard	osk
78	Optional Features Manager	optionalfeatures
79	Paint	mspaint
80	Password Properties	password.cpl
81	Performance Monitor	perfmon.msc
82	Performance Monitor	perfmon
83	Phone and Modem Options	telephon.cpl
84	Power Configuration	powercfg.cpl
85	Printers and Faxes	control printers
86	Printers Folder	printers
87	Printer Migration	PrintBrmUi
88	Private Character Editor	eudcedit
89	Regional Settings	intl.cpl

90	**Registry Editor**	**regedit**
91	Registry Editor	regedit32
92	Remote Assistance	msra
93	Remote Desktop	mstsc
94	Removable Storage	ntmsmgr.msc
95	Removable Storage Operator Requests	ntmsoprq.msc
96	Resultant Set of Policy	rsop.msc
97	**Run Command Line Box**	**run**
98	Scanners and Cameras	sticpl.cpl
99	Scheduled Tasks	control schedtasks
100	Security Center	wscui.cpl
101	Services	services.msc
102	Shared Folders	fsmgmt.msc
103	Shuts Down Windows	shutdown
104	Snipping Tool	snippingtool
105	Sounds and Audio	mmsys.cpl
106	Sound Recorder	soundrecorder
107	**Sound Volume**	**sndvol**
108	Spider Solitare Card Game	spider
109	SQL Client Configuration	cliconfg
110	Sticky Note	StikyNot
111	Stored User Names and Passwords	credwiz
112	**System Configuration Editor**	**sysedit**
113	System Configuration Utility	msconfig

114	**System File Checker Utility**	**sfc**
115	System File Checker Utility (Scan Immediately)	sfc /scannow
116	**System File Checker Utility (Scan Once At Next Boot)**	**sfc /scanonce**
117	System File Checker Utility (Scan On Every Boot)	sfc /scanboot
118	System File Checker Utility (Return to Default Setting)	sfc /revert
119	System File Checker Utility (Purge File Cache)	sfc /purgecache
120	System File Checker Utility (Set Cache Size to size x)	sfc /cachesize=x
121	System Information	msinfo32
122	System Properties	sysdm.cpl (or) Windows key + Pause/Break
123	**Task Manager**	**taskmgr**
124	Trusted Platform Module	TpmInit
125	User Account Management	nusrmgr.cpl
126	Utility Manager	utilman
127	Windows Firewall	firewall.cpl
128	Windows Magnifier	magnify
129	Windows Management Infrastructure	wmimgmt.msc
130	Windows System Security Tool	syskey
131	Windows Update Launches	wupdmgr
132	**Wordpad**	**write**

အခန်း(၅)
Windows Shortcut Key



goldenshadetech@gmail.com
http://thanhtikegs.weebly.com

Windows Keys နှင့်တွဲသုံးရသော Shortcut များကိုလေ့လာခြင်း

Windows 7 မှာသုံးနိုင်မယ့် အမြန်သုံး Shortcut Key တွေကိုဖော်ပြလိုက်ပါတယ်။ စာဖတ်သူအနေဖြင့် ကွန်ပျူတာကိုအကျွမ်းကျင်ဆုံးနှင့် အမြန်ဆုံးသုံးနိုင်ဖို့အထောက်အကူပြုပါတယ်။ သိရှိပြီးသားကျွမ်းကျင်သူတွေကတော့ ကျော်ဖတ်သွားလိုက်ပါ။

အထက်ပါ Key ကို ကွန်ပျူတာအသုံးပြုသူတိုင်းတွေ့မြင်ဖူးမှာပါ။ Windows Key လို့ခေါ်ပါတယ်။ အဆိုပါ Windows Key ကိုဖိလိုက်ပြီးလွှတ်လိုက်လျှင် Start Button ကိုနှိပ်လိုက်သည်နှင့်တူညီပါတယ်။ ဒါ့ကြောင့် အခြား Key တစ်ခုခုနှင့်တွဲသုံးလိုလျှင် Windows Key ကိုဦးစွာဖိထားပြီးမှ အခြား Key ကိုနှိပ်ရပါမယ်။

Windows Key + D

ပထမဦးစွာ စာဖတ်သူဟာ အသုံးချဆော့ဖ်ဝဲလေးငါးခုမကဖွင့်သုံးနေပါတယ်။ ထိုအချိန်မှာ Desktop Screen မျက်နှာစာကိုသွားရောက်ဖို့လိုတဲ့အခါ ဖွင့်ထားသမျှကို လိုက်လုပ်ရပါလိမ့်မယ်။ ထိုအခါ Windows Key နှင့် D ကိုတွဲနှိပ်လျှင် ဖွင့်ထားသမျှဆော့ဖ်ဝဲအားလုံး Minimize ဖြစ်သွားပါလိမ့်မယ်။

Windows Key + E

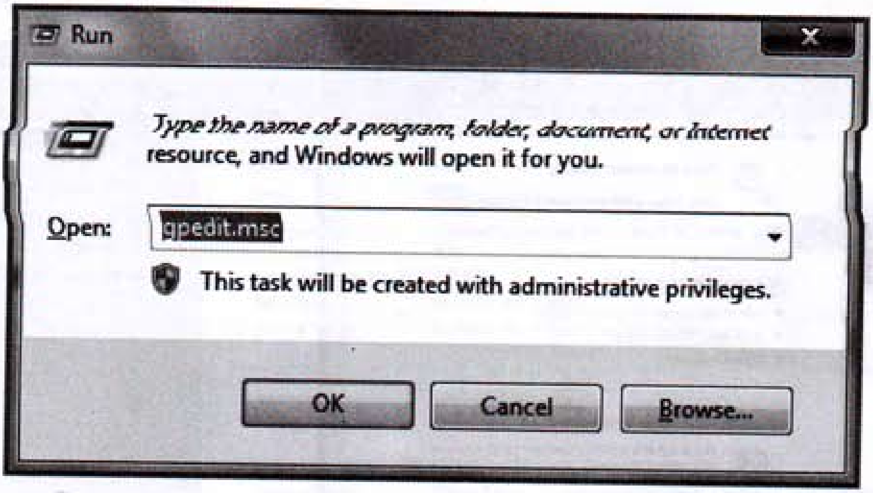
အဆိုပါ Shortcut Key ကိုတော့ Windows Explorer ကိုဖွင့်ရန်သုံးပါတယ်။

Windows Key + F

အဆိုပါ Shortcut Key မှာ File, Folder တွေကိုရှာဖွေသော Search ကိုဖွင့်ရန်သုံးပါတယ်။

Wndows Key + R

အဆိုပါ Shortcut Key ကို Run Command Box ကိုဖွင့်ရန်သုံးပါတယ်။



Wndows Key + M

အဆိုပါ Shortcut Key မှာ All Open Program Minimize လုပ်သော Wndows Key + D နှင့် တူညီပါတယ်။

Wndows Key + L

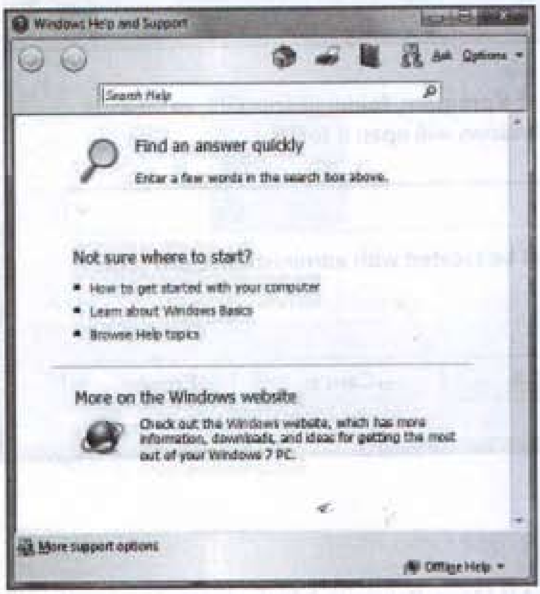
အဆိုပါ Shortcut Key ကိုတော့ စာဖတ်သူဟာကွန်ပျူတာသုံးနေစဉ် အကြောင်းတစ်ခုခုကြောင့် တစ်နေရာရာသို့သွားရလျှင် လက်ရှိသုံးလက်စကွန်ပျူတာကို အခြားသူများဆက်လက်မသုံးစေရန်၊ မကိုင်စေရန် Lock လုပ်ဖို့သုံးပါတယ်။ ပြန်ရောက်လျှင် Log On Password ကိုပြန်ဖွင့်လိုက်တာနဲ့ ဆက်လက်သုံးနိုင်တာပေါ့။

Wndows Key + U

အဆိုပါ Shortcut Key ကိုတော့ Utilites Manager ကိုဖွင့်ဖို့သုံးပါတယ်။

Wndows Key + F1

အဆိုပါ Shortcut Key ကတော့ Windows Help and Support ကိုဖွင့်ဖို့သုံးပါတယ်။

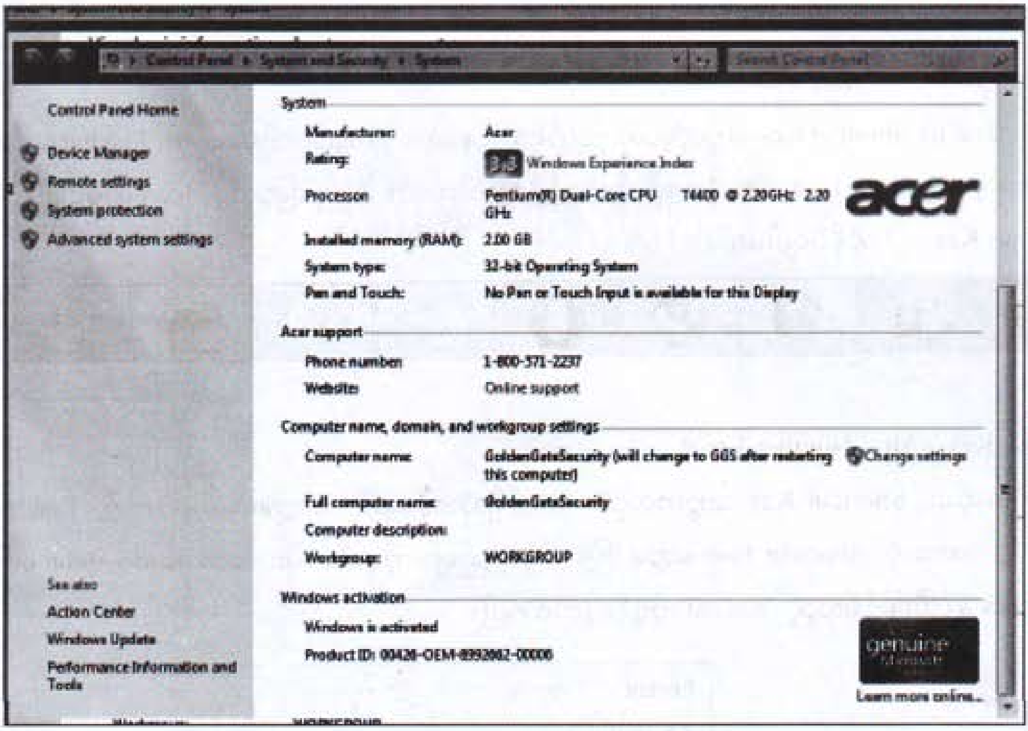


Wndows Key + Tab

အဆိုပါ Shortcut Key ကတော့ဖွင့်ထားသမျှ Program, File တွေကိုစာအုပ်အားဘေးမှမြင်သလို အားလုံးကိုမြင်စေရန်ပြုလုပ်ပါတယ်။

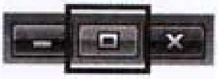
Wndows Key + Pause Break

အဆိုပါ Shortcut Key ကတော့ကွန်ပျူတာမှာတပ်ဆင်ထားတဲ့ Processor , RAM, Windows System, Activated တွေကိုစစ်ဆေးလေ့လာနိုင်ပါတယ်။



Wndows Key + Down Arrow

အဆိုပါ Shortcut Key အား လက်ရှိသုံးနေသော Program ၏မျက်နှာစာကို အလတ်စားချုံ့သော(Restore Down)ပြုလုပ်ရန်ဖြစ်ပါတယ်။

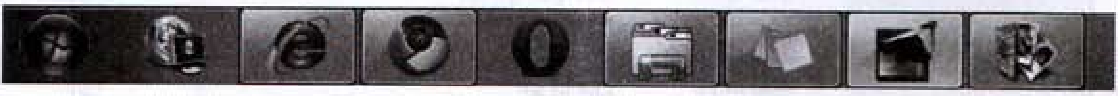


Wndows Key + Up Arrow

Program ၏မျက်နှာစာကို အလတ်စားချုံ့(Restore Down)လုပ်ထားရာမှ အကျယ်အပြည့် ပြန်ချဲ့သော Maximize ပြုလုပ်ရန်ဖြစ်ပါတယ်။

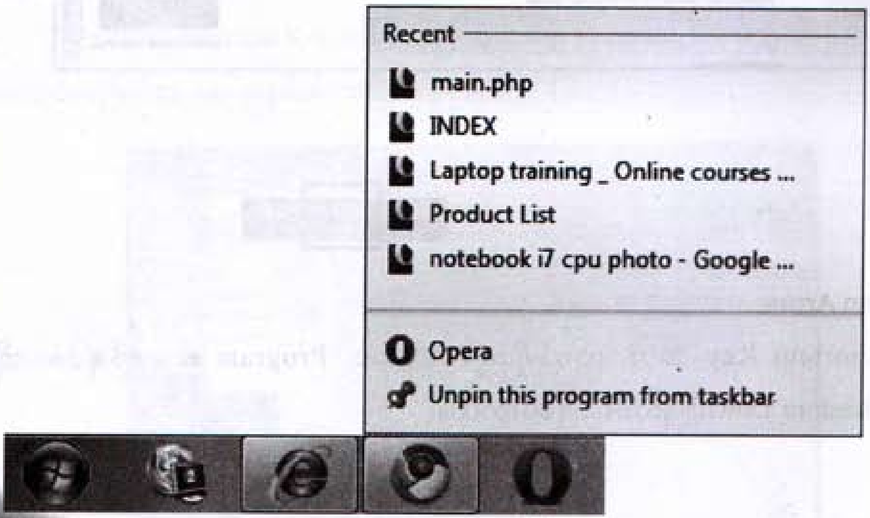
Wndows Key + Number 1 to 9

အဆိုပါ Shortcut Key တွေကိုတော့ လက်ရှိသုံးနေသော Program ဒါမှမဟုတ် Taskbar ပေါ်မှာ တင်ထားတဲ့ Shortcut Icon တွေကိုအစဉ်လိုက်ဖွင့်ဖို့သုံးပါတယ်။ သုံးခုမြောက်မှ Icon ကိုဖွင့်လိုလျှင် Windows Key + 3 ကိုနှိပ်ရပါမယ်။



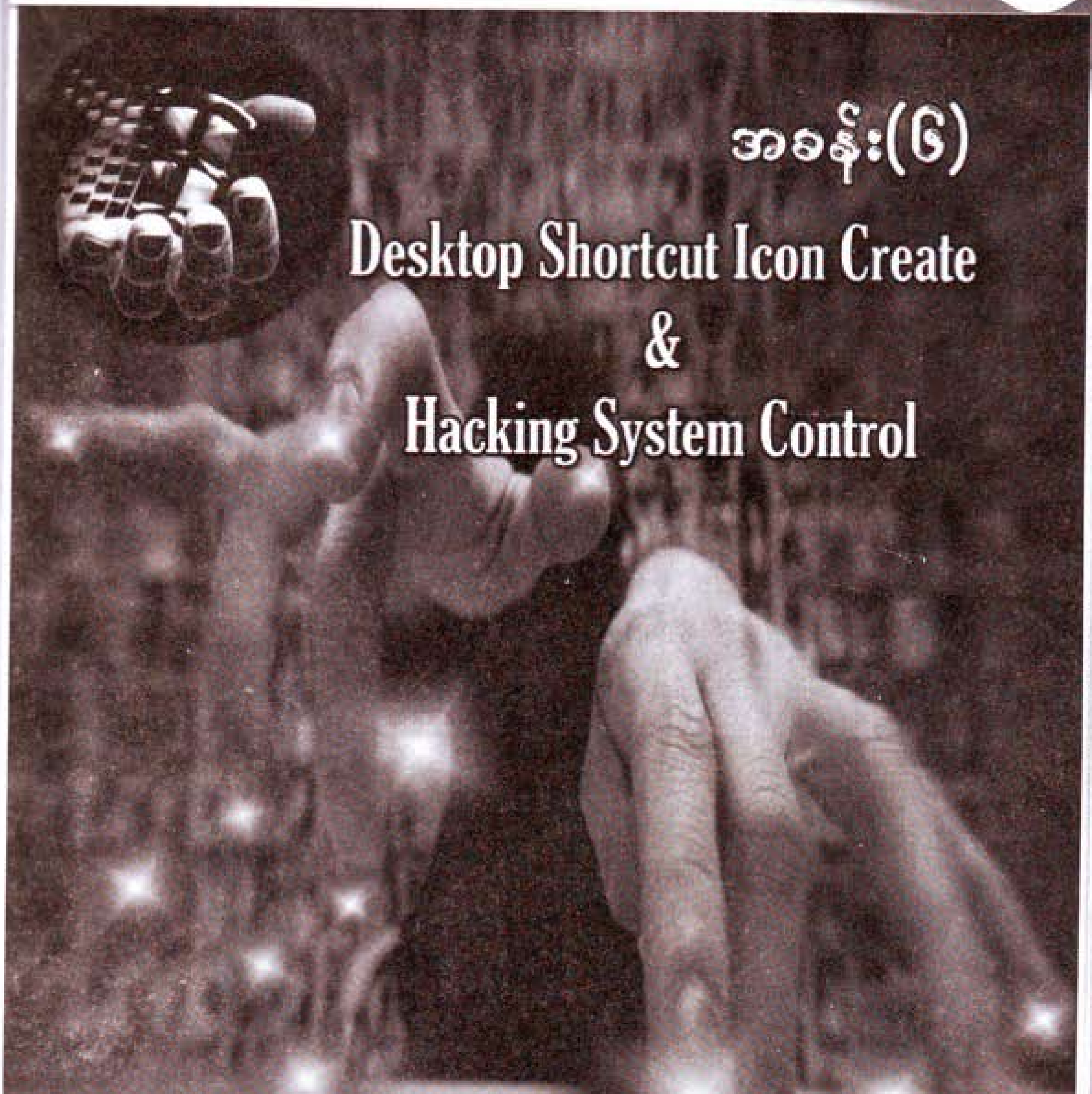
Wndows Key +Alt + Number 1 to 9

အဆိုပါ Shortcut Key တွေကလည်း လက်ရှိသုံးနေသော Program ဒါမှမဟုတ် Taskbar ပေါ်မှာ တင်ထားတဲ့ Shortcut Icon တွေမှ ပြုလုပ်ခဲ့သည်များကိုမှတ်တမ်းတင်ထားသော Icon ပေါ် RightClick နှိပ်ပြီးမြင်ရသည့် Recent ကိုဖွင့်လိုက်တာပါ။



အခန်း(၆)

Desktop Shortcut Icon Create & Hacking System Control

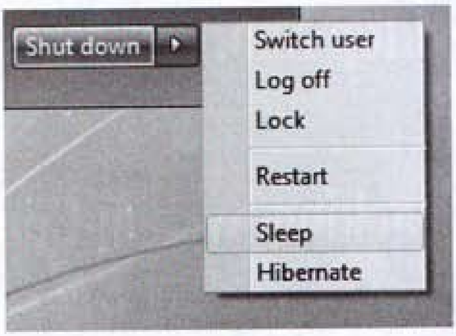


goldenshadetech@gmail.com

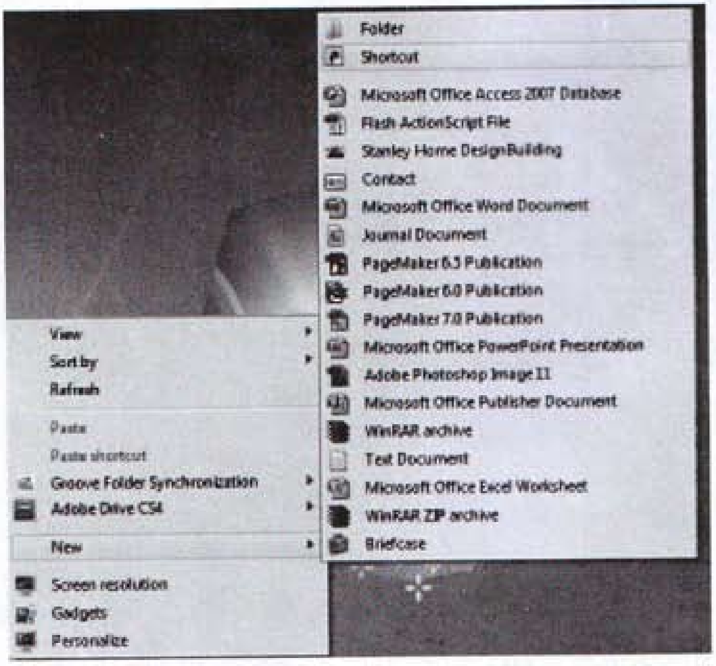
http://thanhtikegs.weebly.com

Desktop ပေါ်တွင် Sleep Command Shortcut Key ကိုဖန်တီးခြင်း

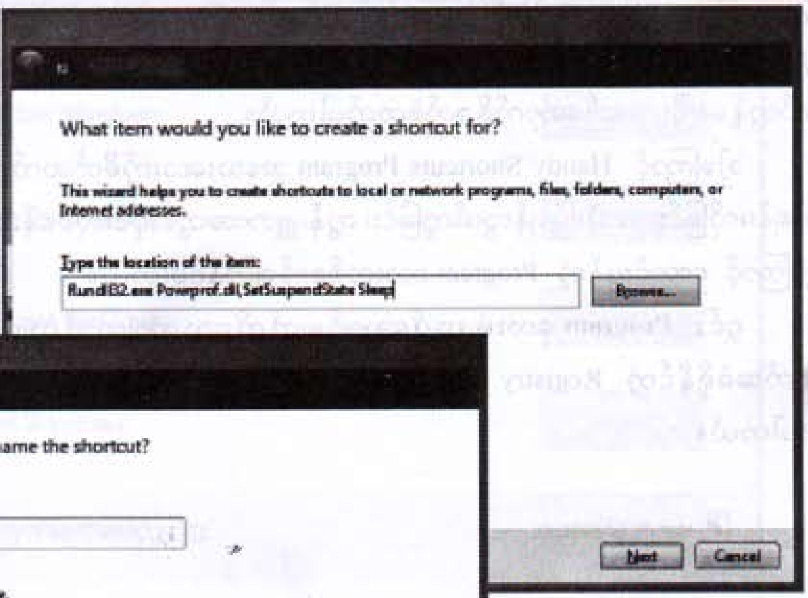
ကွန်ပျူတာကိုသုံးနေစဉ်ခဏရပ်ထားလိုတဲ့အခါမျိုးတွေကို Sleep ချထားဖို့လိုပါတယ်။ ပုံမှန်အားဖြင့် Sleep ချထားဖို့ Start => Shut Down ဘေးမှမြားကိုဖွင့်ပြီး Sleep ကိုရွေးရပါမယ်။

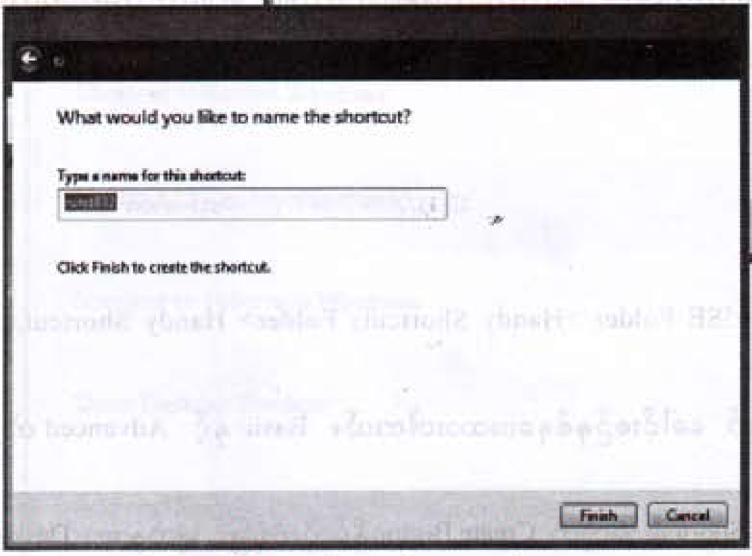


ဒါကြောင့် အလွယ်တကူ Sleep ချနိုင်ရန်အောက်ပါအတိုင်း Shortcut Key တစ်ခုဖန်တီးပါမယ်။ ပထမဦးစွာ Desktop ပေါ်တွင် RightClick နှိပ်ပြီး New=> Shortcutကိုရွေးချယ်ပါ။



အောက်ပါအတိုင်း Box တွေ့မြင်ရလျှင် Type the Location ---- နေရာတွင် **Rundll32.exe Powrprof.dll,SetSuspendState Sleep** ကိုရိုက်ထည့်ပြီး Next Button ကိုရွေးရပါမယ်။





အထက်ပါအတိုင်းအမည်ပေးရန် Box တွင် Type a name ----နေရာတွင် **Rundll32** သာထားပြီး Finish Button ကိုနှိပ်ရပါမယ်။ အဆိုပါနေရာမှာအခြားအမည်မပြောင်းပါနှင့်။

မျက်နှာစာပေါ်မှာ စာဖတ်သူပြုလုပ်ထားတဲ့ **Rundll32** Icon ပေါ် RightClick နှိပ်ပြီး Rename ကိုပြောပါ။ Sleep Win လို့စာရေးသူကတော့ အမည်ပေးလိုက်ပါတယ်။ စာဖတ်သူစိတ်ကြိုက် အမည်တစ်ခုလည်းပေးနိုင်ပါတယ်။

Sleep ချတယ်ဆိုတာ ကွန်ပျူတာတစ်ခုလုံးကိုပိတ်လိုက်တာပါ။ ဒါပေမယ့် အသုံးပြုလက်စ လုပ်ငန်းတွေ မပိတ်သွားပါဘူး။ ပါဝါပြန်ဖွင့်တာနှင့် ဆက်လက်သုံးနိုင်ပါတယ်။

Desktop ပေါ်တွင် Shortcut Icon များကိုတည်ဆောက်ခြင်း

ကွန်ပျူတာကိုနေ့စဉ်ထိတွေ့သုံးစွဲနေရသူတွေအတွက်ကတော့ အလွယ်သုံး Shortcut Icon တွေဟာ လုပ်ငန်းကိုမြန်စေလို့ နှစ်ခြိုက်သဘောကျကြပါတယ်။ ကျွမ်းကျင်သူတွေအနေနှင့် အလွယ်တကူ တည်ဆောက်နိုင်သော်လည်း၊ သာမန်ကွန်ပျူတာသုံးစွဲသူတွေအတွက်ကတော့ နည်းလမ်းသိလည်း လက်တွန့်နေပြီး တည်ဆောက်ဖို့ခက်ခဲတတ်ပါတယ်။

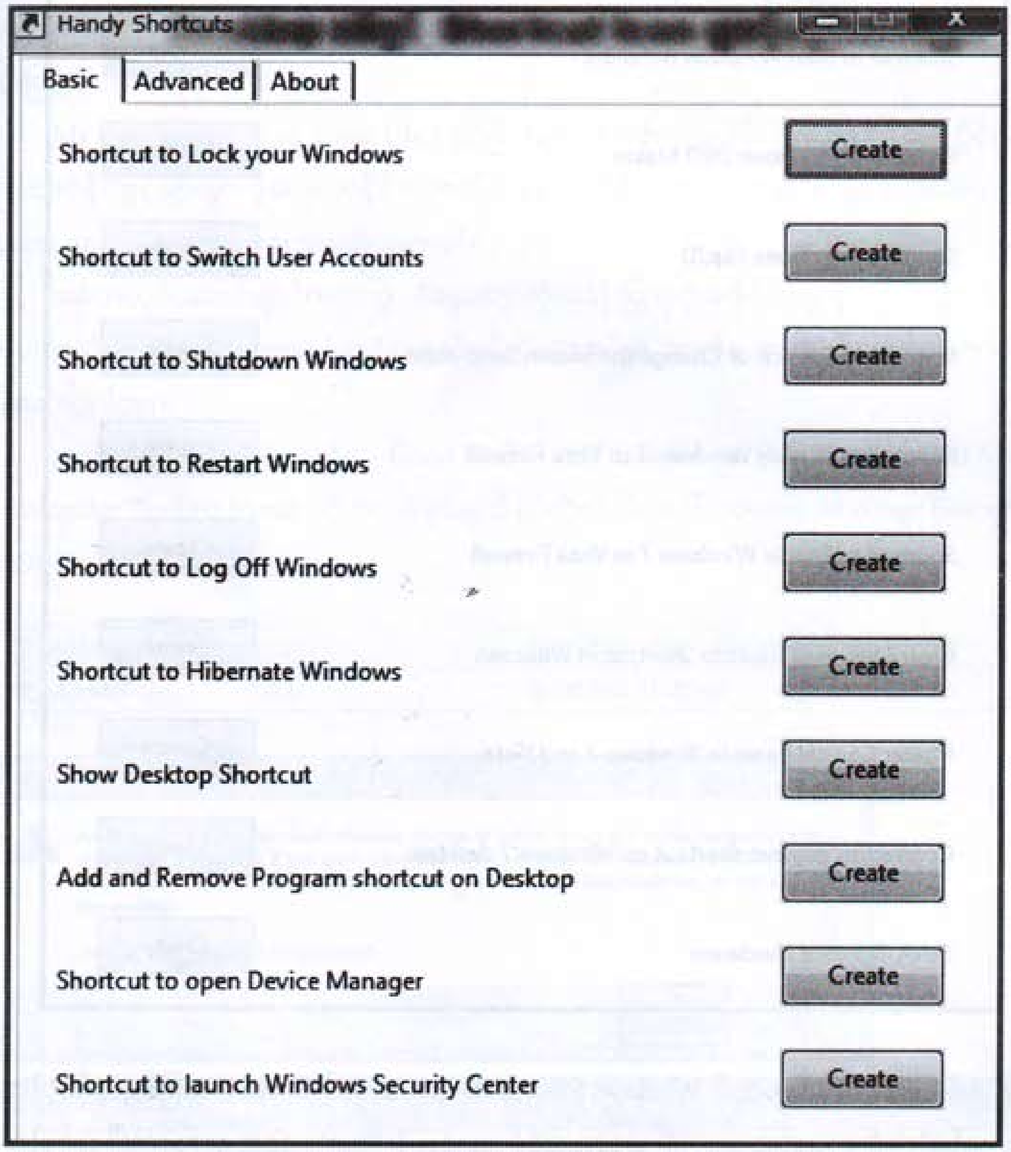
ဒါ့ကြောင့် Handy Shortcuts Program အသေးလေးကိုမိတ်ဆက်ပေးလိုက်ပါတယ်။ Install လုပ်ရန်မလိုခြင်း၊ အသုံးပြုရန်လွယ်ကူခြင်း၊ ကွန်ပျူတာအတွင်းပိုင်းလုပ်ငန်းစဉ်တွင်နေရာမယူထားခြင်း တို့ကြောင့် ကောင်းမွန်တဲ့ Program လေးတစ်ခုလို့ပြောနိုင်ပါတယ်။

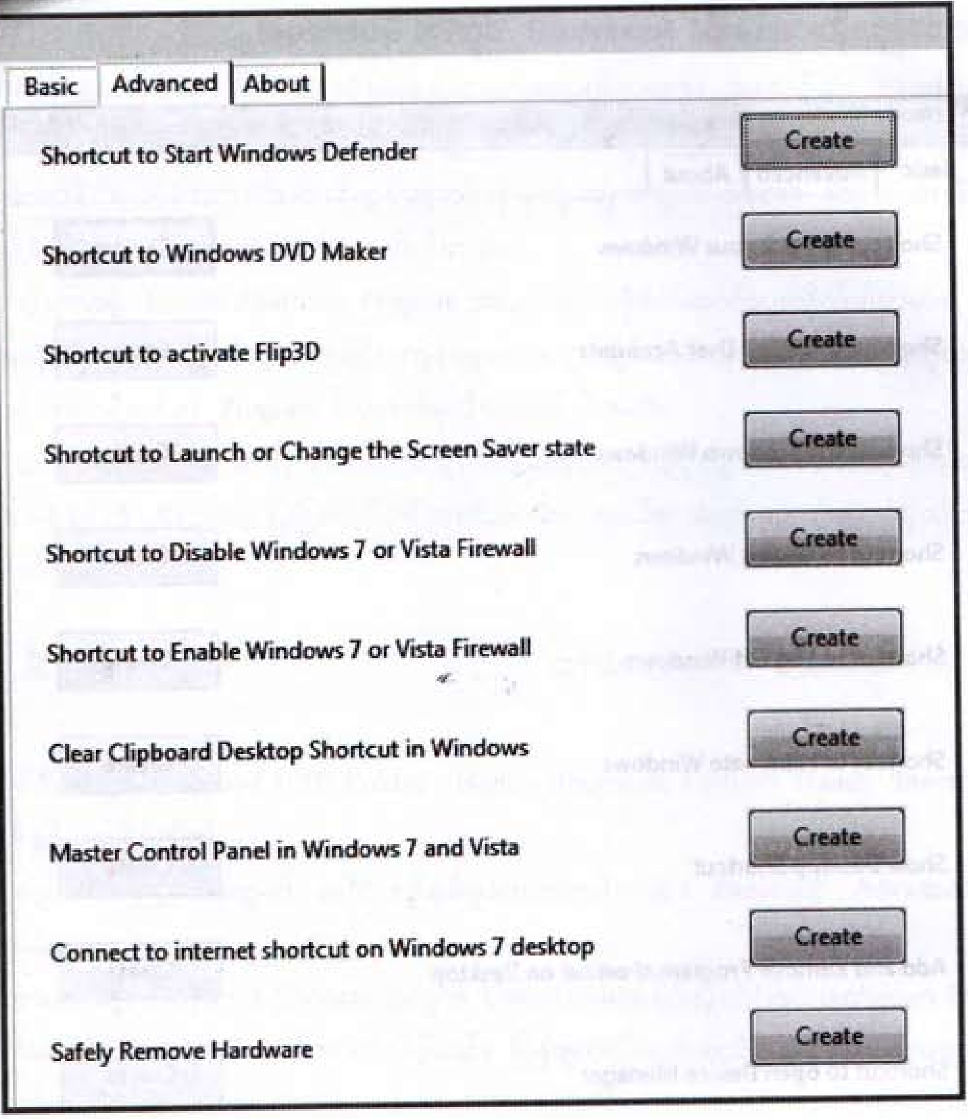
၄င်း Program လေးရဲ့လုပ်ဆောင်ချက်ကိုလေ့လာကြည့်လျှင် စာဖတ်သူများအတွက် အခက်အခဲရှိနိုင်တဲ့ Registry ပြုပြင်ခြင်းကိုသက်သာစေပါတယ်။ Registry ကိုတိုက်ရိုက်ပြင်ဆင် ပေးပါတယ်။

စီဒီအတွင်းမှ Good USE Folder >Handy Shortcuts Folder> Handy Shortcut.exe ကိုကလစ်နှစ်ချက်နှိပ်လိုက်ပါ။

လုပ်ဆောင်ချက်အတွက် ခေါင်းစဉ်နှစ်ခုပေးထားပါတယ်။ Basic နှင့် Advanced တို့ပဲ ဖြစ်ပါတယ်။

စာဖတ်သူရယူလိုသော Shortcut အတွက် Create Button နှိပ်လိုက်ရုံဖြင့် မျက်နှာစာ Desktop ပေါ်သို့ အဆိုပါ Shortcut ရောက်လာပါလိမ့်မယ်။ ပြန်ဖျက်လိုလျှင်လည်း Delete ဖြင့်အလွယ်သာ ပြန်ဖျက်လိုက်ပါ။


Handy Shortcuts
Basic
Advanced
About
Shortcut to Lock your Windows
Create
Shortcut to Switch User Accounts
Create
Shortcut to Shutdown Windows
Create
Shortcut to Restart Windows
Create
Shortcut to Log Off Windows
Create
Shortcut to Hibernate Windows
Create
Show Desktop Shortcut
Create
Add and Remove Program shortcut on Desktop
Create
Shortcut to open Device Manager
Create
Shortcut to launch Windows Security Center
Create



Advanced အပိုင်းအတွင် Windows Systems Button တွေကို Shortcut အဖြစ်ရယူနိုင်ပါတယ်။ ယခုလောက်ဆိုလျှင် စာဖတ်သူအတွက် အသုံးတည့်ဖို့ အသုံးဝင် Shortcut တွေရလောက်ပြီထင်ပါတယ်။

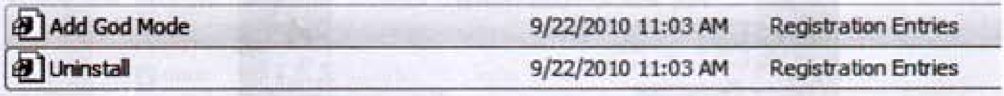
Honest Hacker အသုံး System Process Control

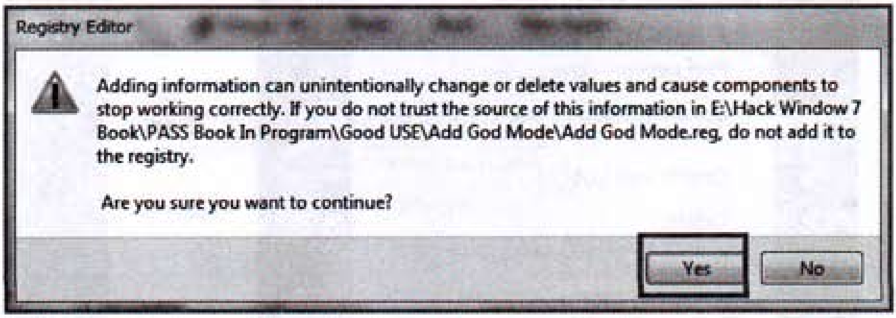
ကွန်ပျူတာအတွင်းပိုင်းမှ system ပိုင်းဆိုင်ရာတွေကို ပြောင်းလဲပြင်ဆင်လေ့လာလိုတဲ့အခါ သွားရောက်ဖွင့်ဖို့က အခက်အခဲရှိပါလိမ့်မယ်။ အောက်ပါအတိုင်း Script Registry Program ကိုသုံးကြည့်ပါ။

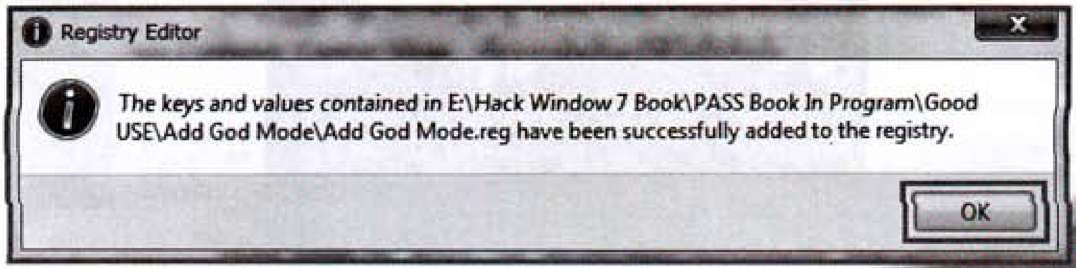
My Computer Icon ကို Right Click နှိပ်ပြီး Good Mode ကိုဖွင့်ပြီး System Process ပိုင်းဆိုင်ရာ လုပ်ဆောင်နိုင်ခွင့်များစွာကိုလေ့လာနိုင်ပါတယ်။ နောက်ပိုင်းကဏ္ဍများတွင်ဖော်ပြထားသော Script Program ရေးနည်းအတိုင်းရေးသားထားတာပါ။

အဓိကလုပ်ဆောင်ချက်ကတော့ Registry ကိုအသုံးပြုရတဲ့အပိုင်းတွေကို တိုက်ရိုက်သုံးစွဲခွင့် ရလာပါတယ်။ System Control Load တွေကိုဖွင့်လိုတဲ့အခါမှာ ဘယ်နားသွားဖွင့်ရမယ်ဆိုတာမျိုးတွေ မကြုံရတော့ပါဘူး။

အသုံးပြုနိုင်ရန် စီဒီအတွင်းမှ Good USE > Add GoodMode Folder >Add God Mode in My Computer Context Menu ကိုကလစ်နှစ်ချက်နှိပ်လိုက်ပါ။ ပေါ်လာသော Massage Box များတွင် Yes/ Ok Button နှိပ်သွားပါ။



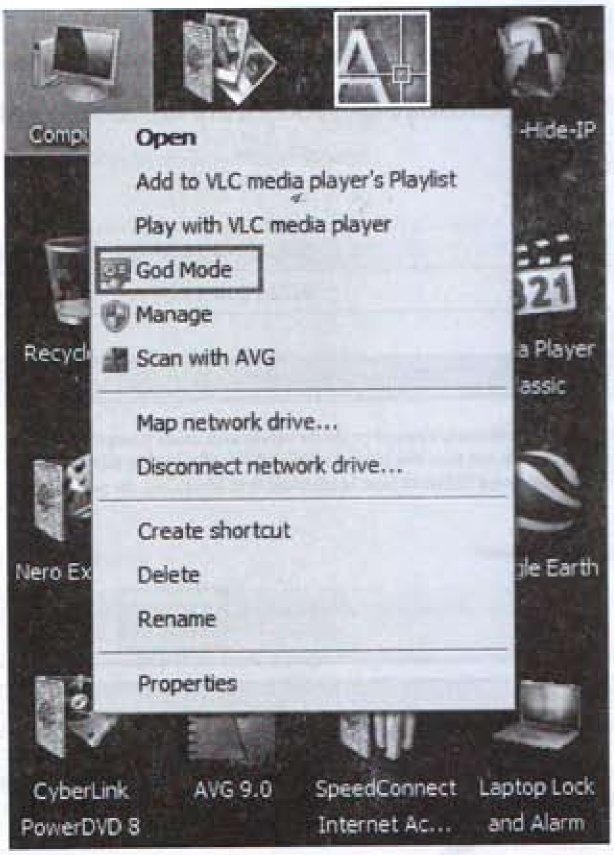




Desktop/ Start Menu မှ My Computer Icon ပေါ်တွင် Right Click နှိပ်ပြီး ထွက်ပေါ်လာသော Menu တွင် Good Mode ကိုရွေးနှိပ်လိုက်ပါ။

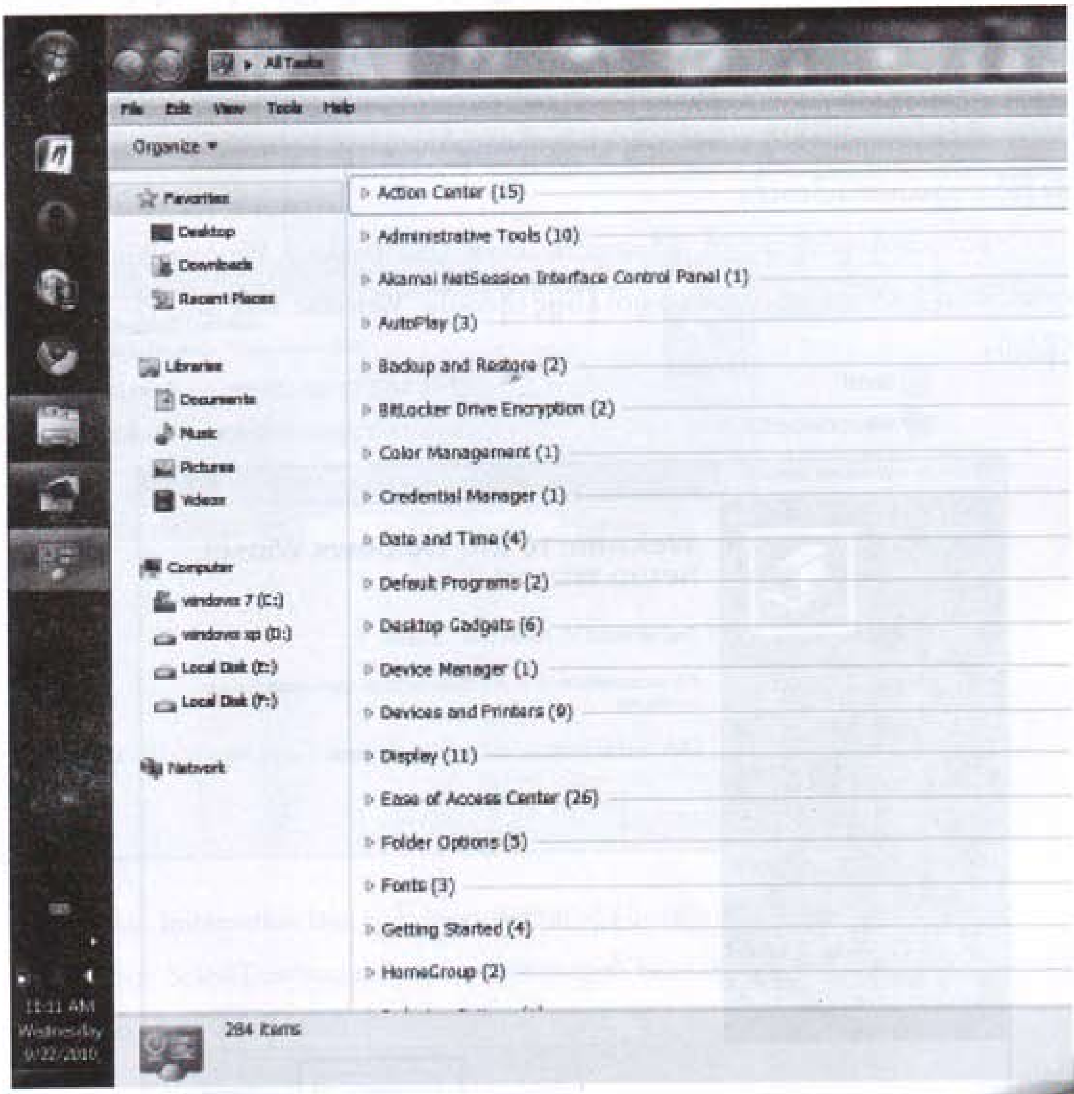
Good Mode ကို အပိုင်း ၄၇ ပိုင်းဖြင့်ခွဲခြားထားပါတယ်။ ကွန်ပျူတာတစ်ခုလုံးမှ System Process ပိုင်းဆိုင်ရာအားလုံးပါရှိပါတယ်။ တစ်ခုခြင်းရှင်းပြမနေတော့ပါ။ စာဖတ်သူကိုယ်တိုင် အလွယ်တကူလေ့လာနိုင်ပါတယ်။

အသုံးမလိုတော့သဖြင့် ပြန်လည်ဖြုတ်လိုတဲ့အခါမှာလည်း စီဒီအတွင်းမှ ကူးယူထည့်သွင်းခဲ့သည့်နေရာ ပြန်သွားကာ Uninstall ကိုကလစ်နှစ်ချက်နှိပ်လိုက်ရုံပင်။



Good Mode တွင်ပါဝင်သောအပိုင်းများမှ ခေါင်းစဉ်များကိုတွေ့မြင်ရတာဖြစ်ပါတယ်။ စာဖတ်သူအနေဖြင့် ပထမဆုံးတစ်ခေါက်ကိုတော့ စေ့စေ့စပ်စပ်လေ့လာထားသင့်ပါတယ်။

အရေးလိုလို့ ဖွင့်ချင်မှ ဘာကိုဘယ်နားသွားရှာရမယ်မှန်းမသိဖြစ်နေပါလိမ့်မယ်။ တစ်ခုခြင်း ဖွင့်ကြည့်လိုက်၊ ပြန်ပိတ်လိုက်ဖြင့် လေ့လာသွားပါ။ အဓိကကတော့ System ပိုင်းဆိုင်ရာထိန်းချုပ်မှုများကို ဝင်ရောက်ပြင်ဆင်ရန်/ ပြောင်းလဲရန်သင့်တော်ပါတယ်။



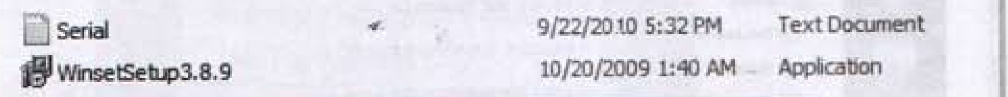
အသုံးဝင်သော Windows Winset Program ကိုလေ့လာခြင်း

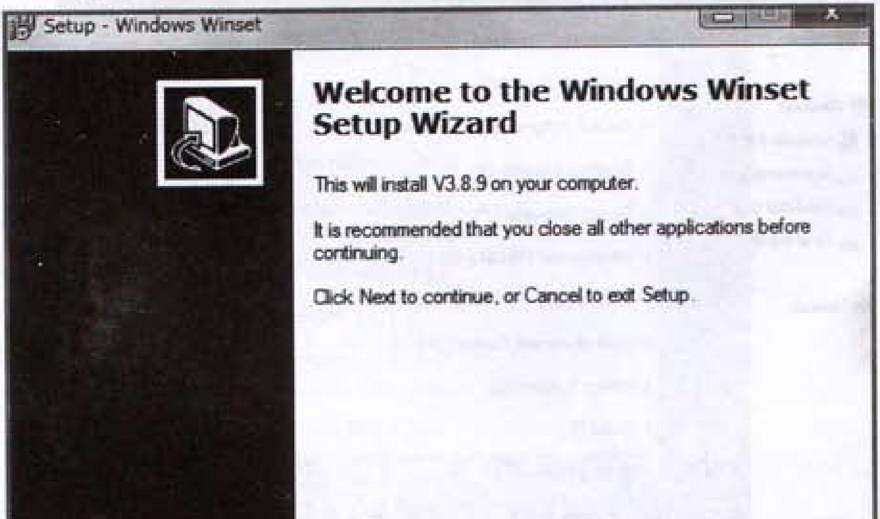
Honest Hacker တွေရဲ့အလုပ်ထဲမှာ System Program တွေကိုအသုံးချတတ်တာလည်း ပါဝင်ပါတယ်။ အဖျက် Hacker တွေကလည်း ယခုကဲ့သို့သော System Program မျိုးတွေကို သုံးနေရပါသေးတယ်။ အကြောင်းကတော့ ကွန်ပျူတာတစ်လုံးကို အကောင်းဆုံးထိန်းထားနိုင်သလို အဆင့်မြင့်လုပ်ဆောင်ချက်တွေအထိခိုင်းစေနိုင်လို့ပါ။

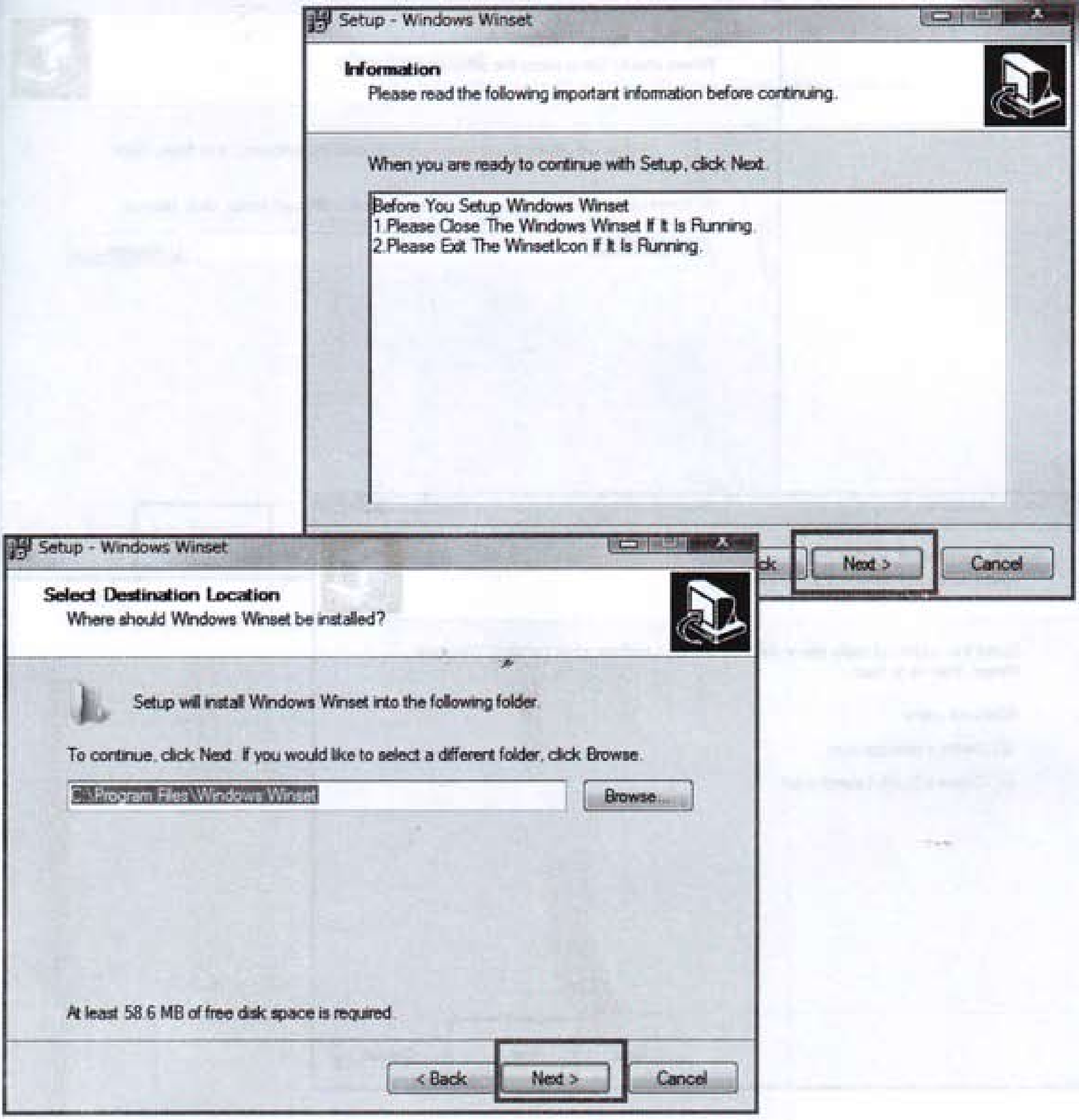
ကွန်ပျူတာကို စစ်ဆေးခြင်း၊ အဆင့်မြှင့်တင်ခြင်းနှင့် ကာကွယ်ခြင်းအပိုင်းတွေကို အလွယ်တကူ တိုက်ရိုက်ညွှန်ကြားထိန်းချုပ်နိုင်ပါတယ်။ စာဖတ်သူဟာ မိမိကွန်ပျူတာကိုအကောင်းဆုံးစီမံထားချင်လျှင် အသုံးဝင်စေဖို့ထည့်သွင်းပေးလိုက်ရတာပါ။ အသုံးမလိုတော့လည်းဘေးဖယ်ထားလိုက်ပေါ့။

လိုင်စင်ဗားရှင်းဖြစ်လို့ စာဖတ်သူများအတွက်ရေရှည်သုံးနိုင်ရန် Serial Number တွေကို Serial.txt File ဖြင့်ထည့်ပေးထားပါတယ်။

စတင်ထည့်သွင်းဖို့အတွက် စီဒီအတွင်းမှ Good USE Folder > Window Winset Folder > WinsetSetup 3.8.9.exe ကိုကလစ်နှစ်ချက်နှိပ်ဖွင့်လိုက်ပါ။ Welcome Box အတွက် Next Button ကိုနှိပ်ပါ။

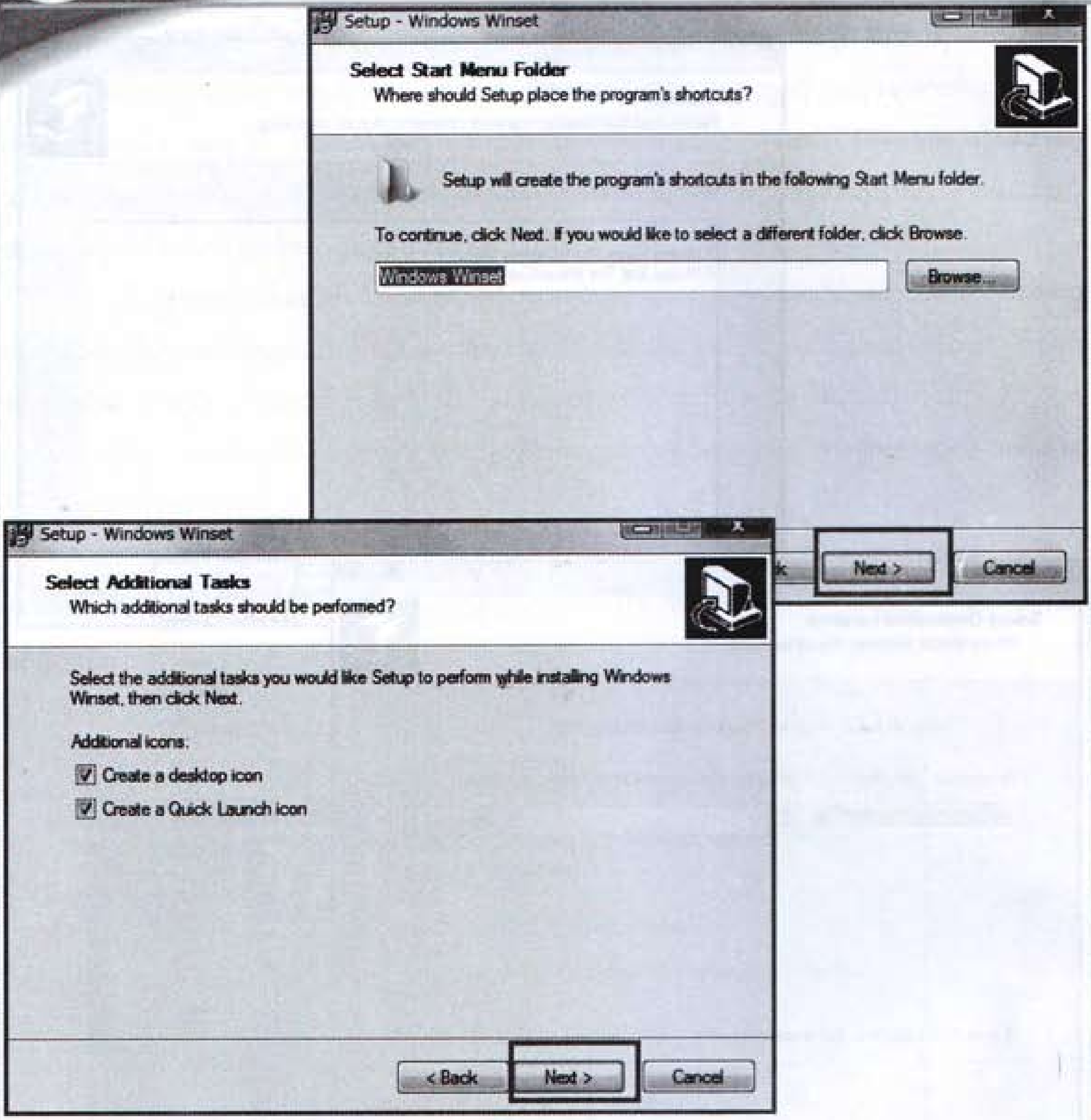






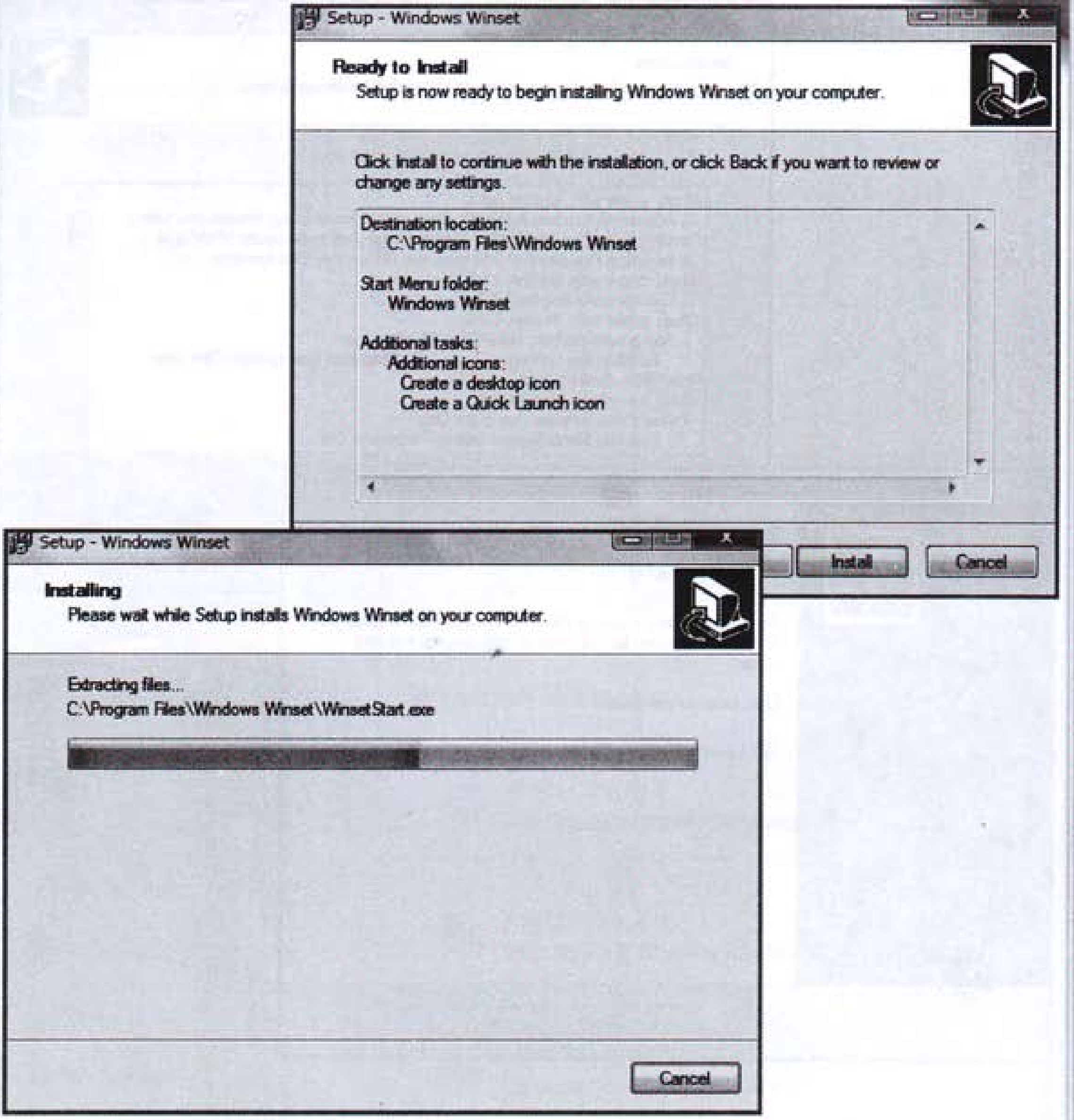
ပထမ Information Box တွင် Next Button ကိုနှိပ်ပါ။

ဒုတိယ Select Destination Location Box အတွက် File Location ကိုပေးသည့်အတိုင်းထားကာ Next Button ကိုသာနှိပ်လိုက်ပါ။

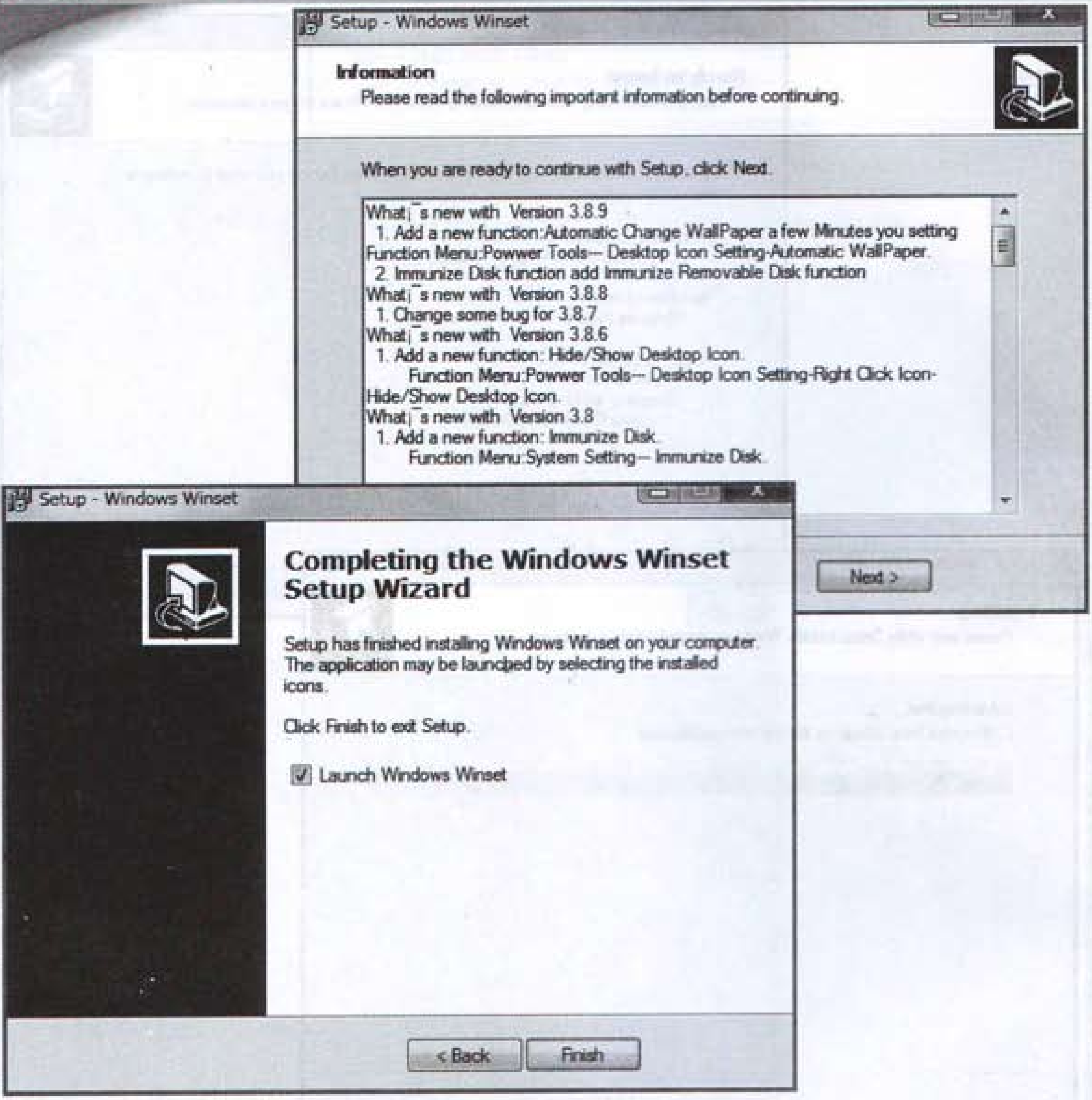


ပထမ Select Start Menu Folder Box တွင် ပေးသည်ကိုသာယူပြီး Next Button ကိုနှိပ်ပါ။

ဒုတိယ Select Additional Tasks Box အတွက် Desktop Icon ထားမလားမေးသည်ဖြစ်၍ နှစ်ခုစလုံးအမှတ်တပ်ကာ Next Button ကိုသာနှိပ်လိုက်ပါ။



ပထမပုံအတွက် Install လုပ်ရန်အသင့်ဖြစ်ပြီလားလို့ မေးသည်ဖြစ်၍ Install Button ကိုနှိပ်ပါ။ ဒုတိယပုံကတော့ Install လုပ်နေသည်ကိုတွေ့ရတာပါ။ ခဏသာစောင့်ရပါမယ်။



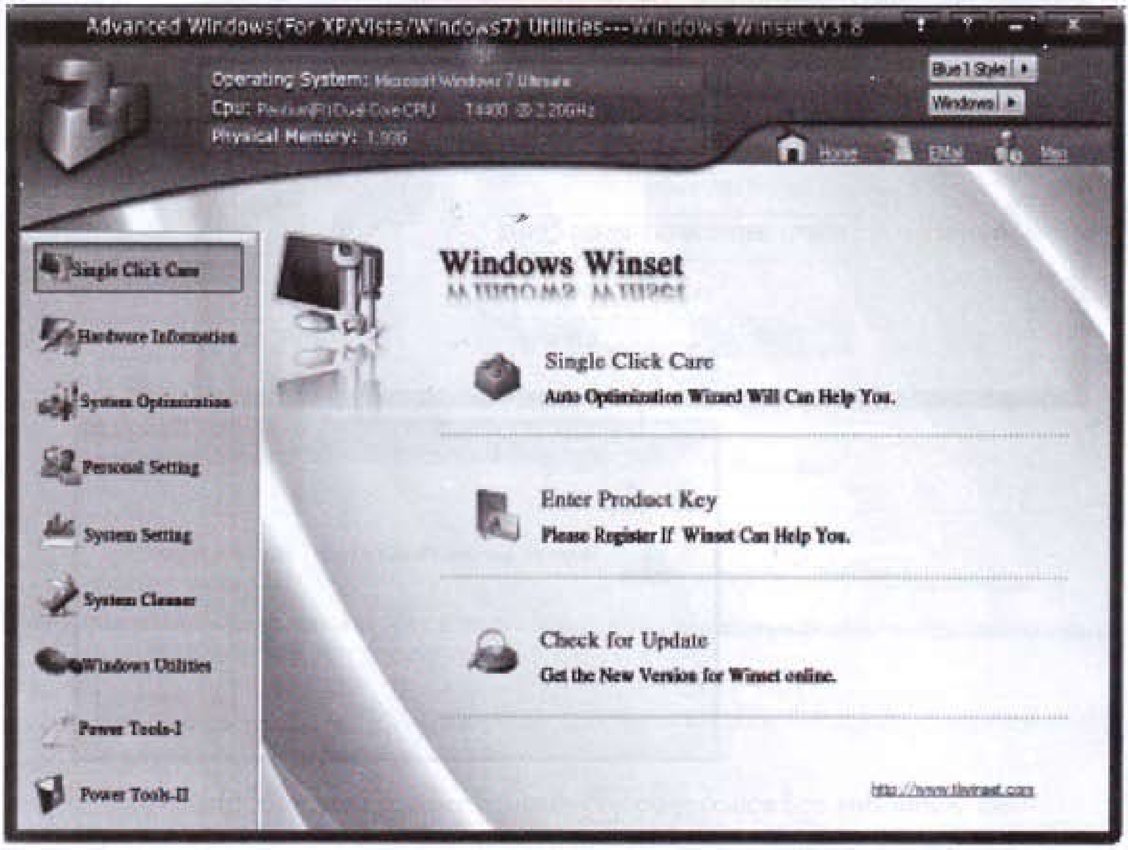
ပထမပုံအတွက်Next Button ကိုသာနှိပ်ပါ။

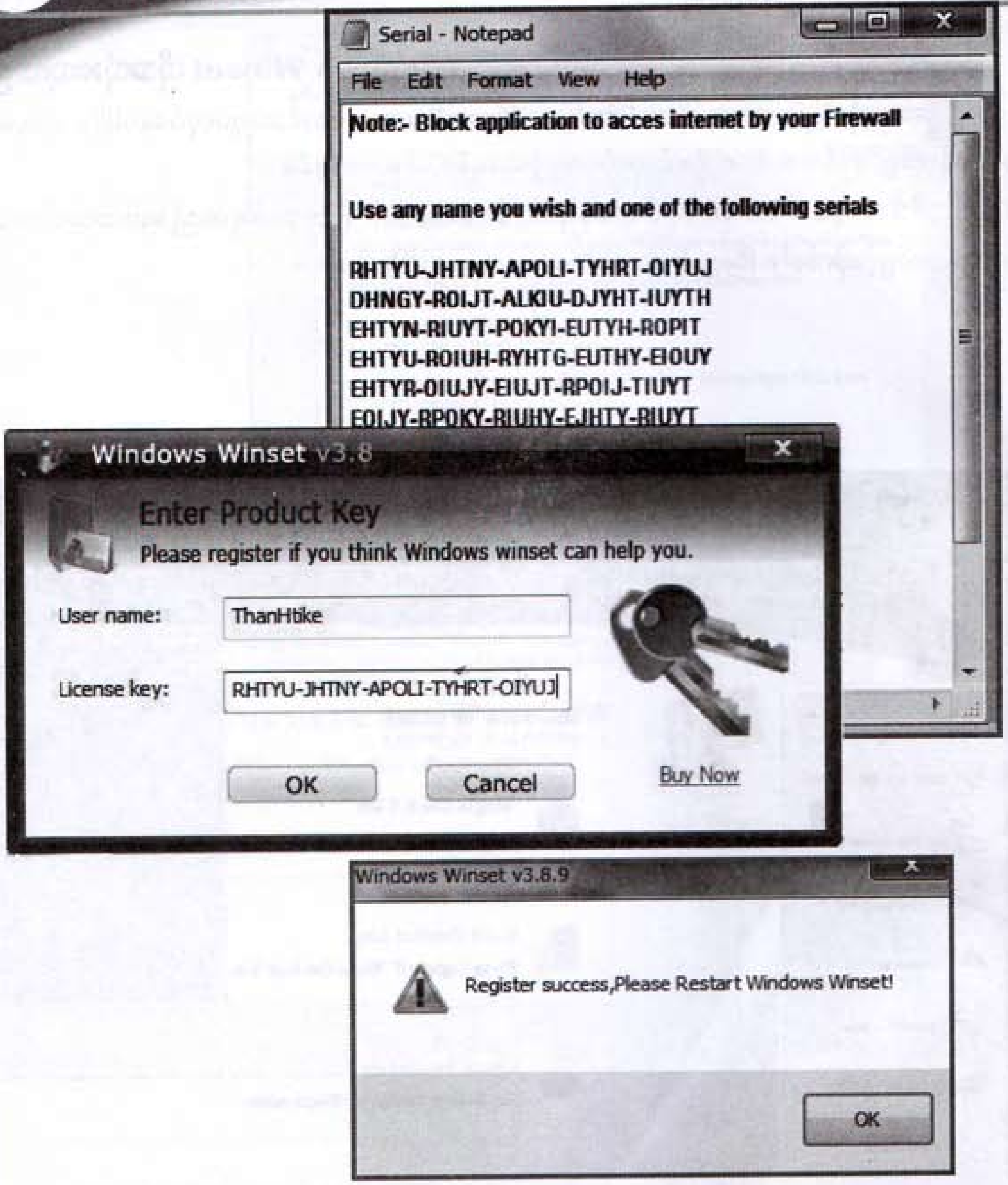
ဒုတိယပုံတွင် Launch Windows Winset Box အားအမှတ်တပ်ပြီး Finish Button ကိုသာ နှိပ်လိုက်ပါ။ အားလုံးထည့်သွင်းပြီးဖြစ်လို့ တစ်ဖက်စာမျက်နှာမှအတိုင်းစတင်တွေ့မြင်ရပါပြီ။

Windows Winset ကိုအသုံးလေ့လာခြင်း

အောက်ပါမြင်ကွင်းအတိုင်း Windows Winset Program စတင်အလုပ်လုပ်နေပါပြီ။ ဒါပေမယ့် လိုင်စင်ဗားရှင်းဖြစ်အောင် လိုင်စင်ကုတ် ထည့်ပေးရန်လိုပါသေးတယ်။

စီဒီအတွင်း Install လုပ်ရာနေရာတွင် Serial.txt File တစ်ခုထည့်ပေးထားပါတယ်။ သွားရောက်ဖွင့်လိုက်ပါ။ ပြီးလျှင် Enter Product Key ကိုနှိပ်လိုက်ပါ။



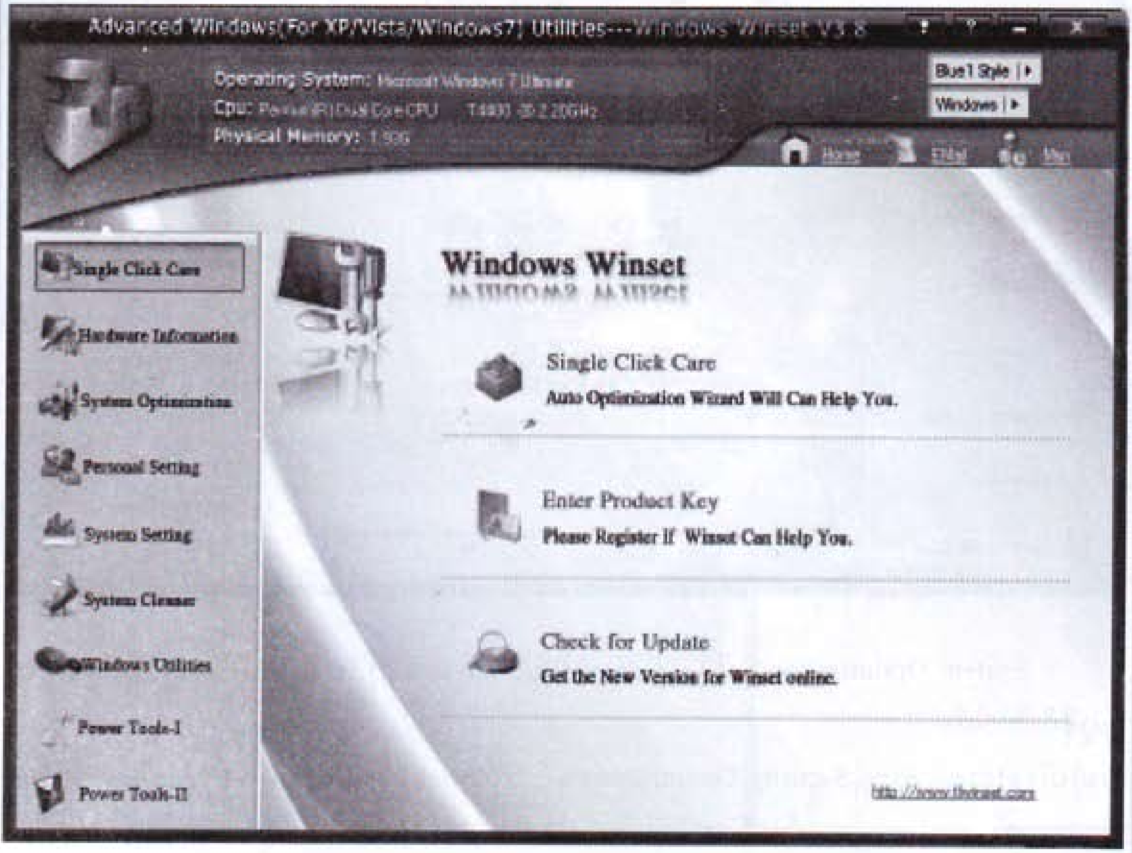


User Name Box တွင်စာဖတ်သူစိတ်ကြိုက်အမည်တစ်ခုထည့်ပေးလိုက်ပါ။

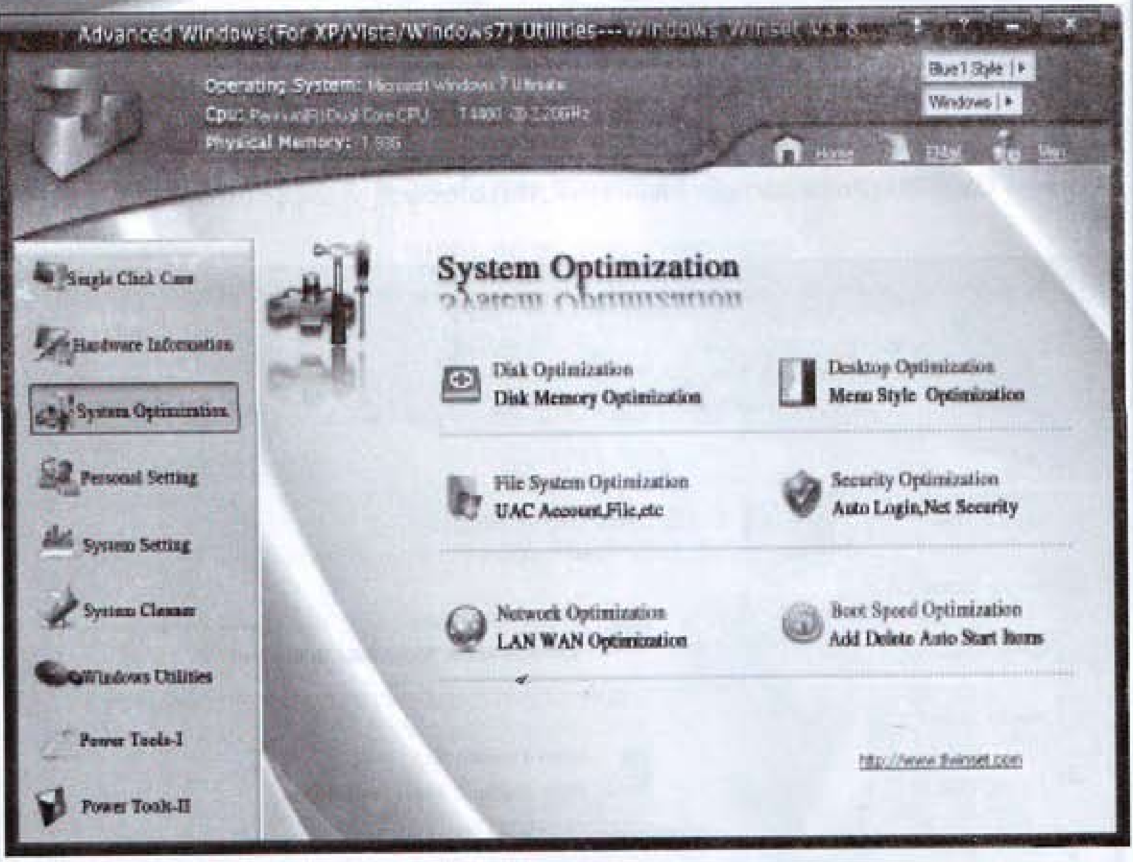
လိုင်စင်နံပတ်ကို Notepad ထဲမှကြိုက်ရာတစ်ကြောင်းအားကူးယူကာ License Key box တွင်ဖြည့်သွင်းပြီး Ok Button ကိုနှိပ်လိုက်ပါ။ အောက်ဆုံးမှ Command Box ကိုလည်း OK ကိုသာနှိပ်ပါ။

Windows Winset Program ကိုဖွင့်သုံးရန် မျက်နှာစာပေါ်မှအဆိုပါ Icon ကိုကလစ်နှစ်ချက်နှိပ်လိုက်ပါ။ Program ပွင့်လာသောအခါ စတင်လေ့လာမည်ကတော့ အသုံးဝင် ခေါင်းစဉ်များဖြစ်ပါတယ်။

ထိပ်ပိုင်းနားတွင် လက်ရှိသုံးနေသော ကွန်ပျူတာ၏ သတင်းအချက်အလက်များပေးထားပါတယ်။ Windows OS, CPU (Processor) နှင့် Memory (RAM) ပါဝင်မှုတို့ကိုသိရှိနိုင်ပါတယ်။



Program ဘယ်ဘက်အခြမ်းတွင်အသုံးချလုပ်ငန်းစဉ်အတွက်ခေါင်းစဉ်တွေပေးထားပါတယ်။ အများစုကိုစာဖတ်သူကိုယ်တိုင်လေ့လာကြည့်နိုင်ပါတယ်။

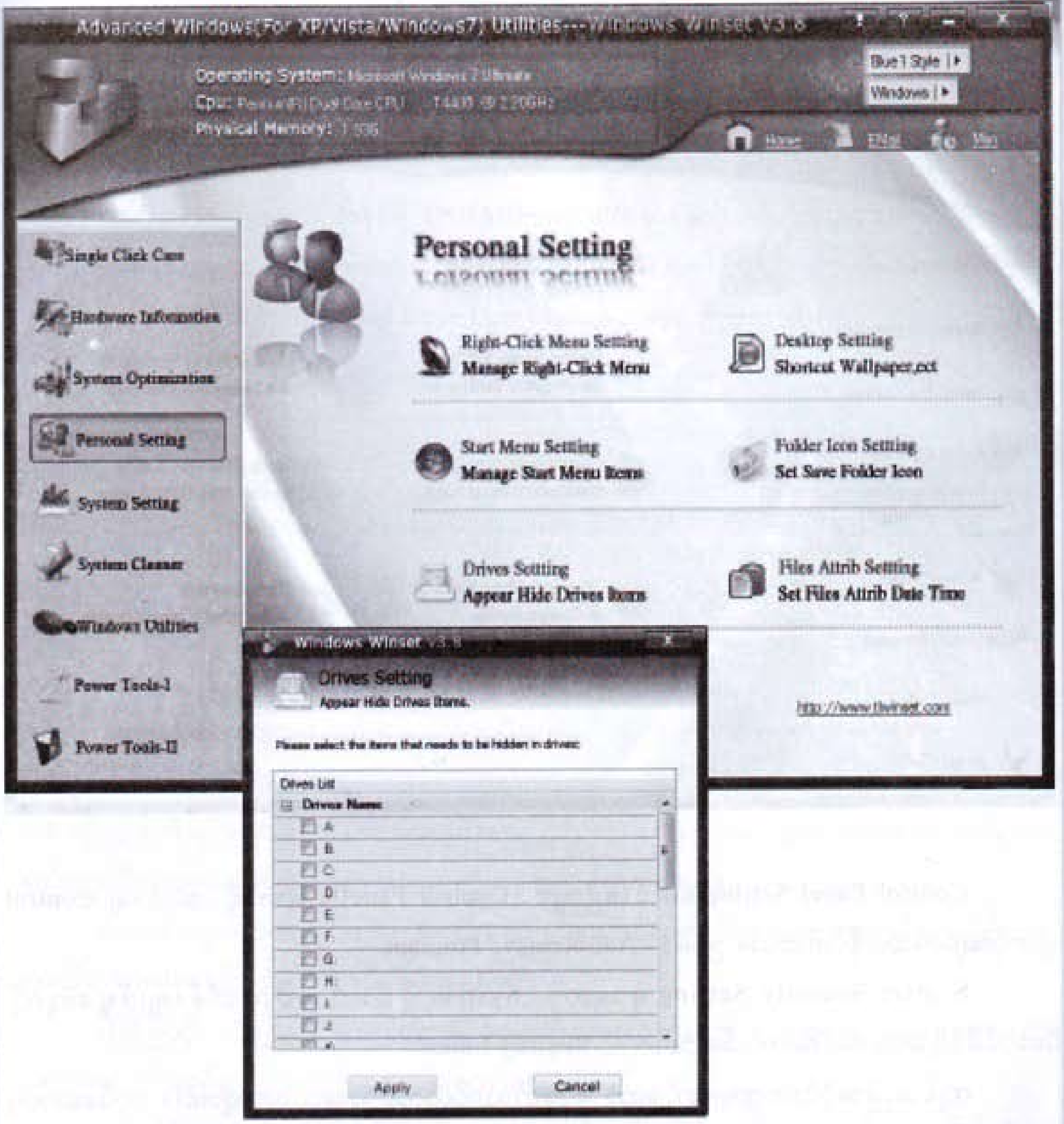


System Optimization ခေါင်းစဉ်အောက်တွင် System ပိုင်းဆိုင်ရာထိန်းချုပ်နိုင်မှုတွေကို ရယူနိုင်ပါတယ်။

အဆိုပါခေါင်းစဉ်ထဲတွင် Security Optimization နှင့် Network Optimization တို့ကတော့ Hacker တွေအတွက် အသုံးတည့်လက်နက်တွေပါရှိပါတယ်။

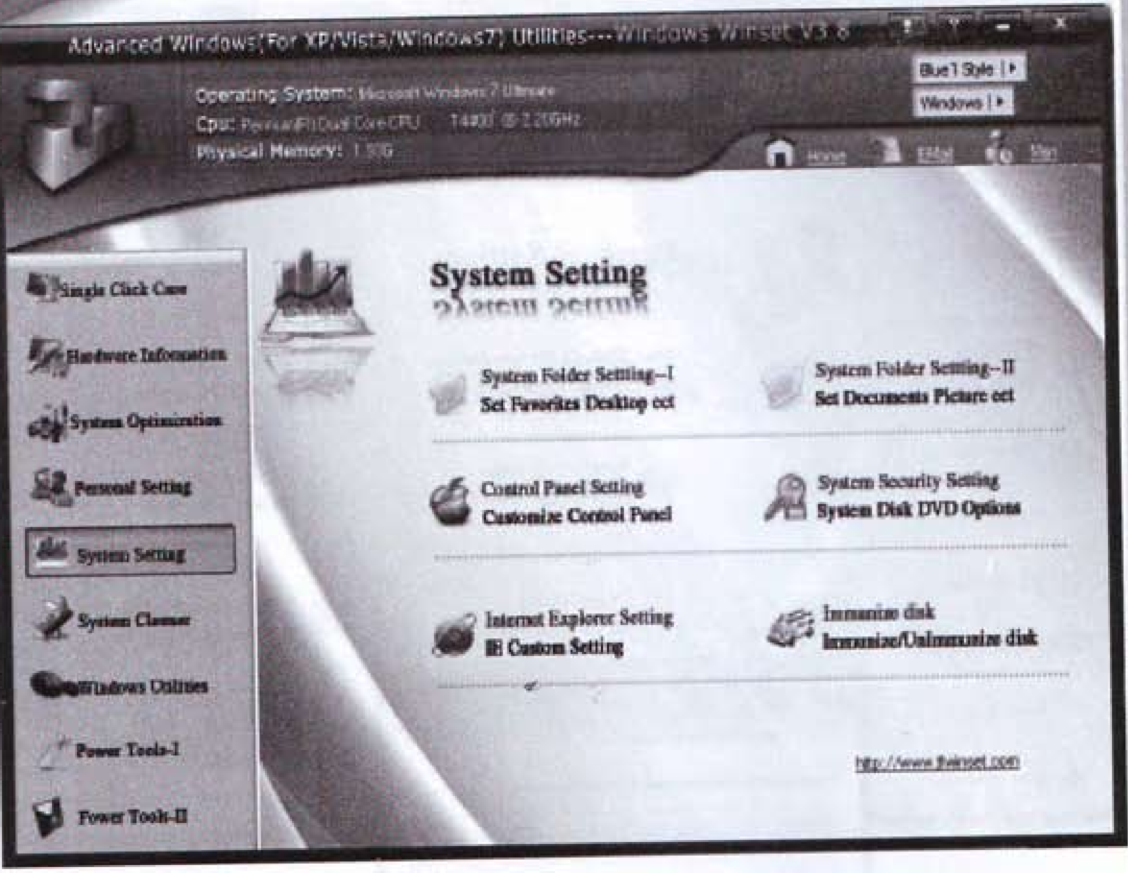
Boot Speed Optimization တွင် Boot လုပ်ငန်းစဉ်ကိုမြှင့်တင်ပေးသော လုပ်ဆောင်ချက်တွေ ပါရှိပါတယ်။ စာဖတ်သူကိုယ်တိုင်သာလေ့လာကြည့်လိုက်ပါ။

အမှတ်တပ်ပြီး ရွေးချယ်ရတာမျိုးဖြစ်လို့ မကြိုက်လျှင်၊ အသုံးမဝင်လျှင် ပြန်လည်ပြင်ဆင်ရတာ အလွယ်တကူရှိပါတယ်။



Personal Optimization ခေါင်းစဉ်၌ Desktop Setting တွင် Icon များကိုဖျောက်ထားခြင်း၊ Start Menu Setting တွင်လည်း အသုံးပြုခွင့်မပေးလိုသော Icon များကိုဖျောက်ထားနိုင်ပါတယ်။

Drives Settig တွင် Harddisk Partion Drive Letter များနှင့် DVD, VCD Drive ကိုအလွယ်တကူဖွက်ထားနိုင်ပါတယ်။



Control Panel Setting ခေါင်းစဉ်တွင် Control Panel အောက်ရှိ အသုံးချ Control များကိုဖျောက်ထားနိုင်ပါတယ်။ ဥပမာ– Add/Remove Program

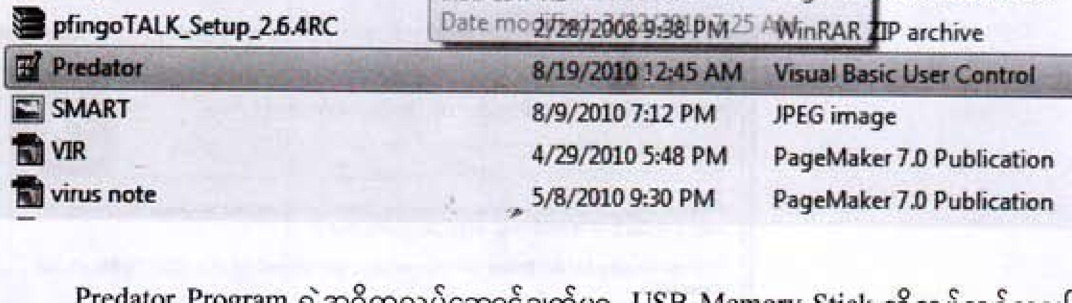
System Security Setting မှာတော့ System ပိုင်းကို အဓိကထိန်းချုပ်မှုတွေကို ပိတ်ပင်နိုင်ဖို့အတွက်ပါရှိပါတယ်။ ဥပမာ – Registry Editor

ကျန်သည့်အပိုင်းကဏ္ဍများကိုတော့ စာဖတ်သူကိုယ်တိုင်သာလေ့လာသွားပါ။ လုပ်ဆောင်ရလွယ်ကူပြီး နားလည်ရလည်းလွယ်ကူသော စကားပြေဖြစ်တာကြောင့် အသေးစိတ် ဝင်ရောက်မရှင်းပြတော့ပါ။

လုံခြုံရေးစနစ်ဖန်တီးပေးသော Predator Program ကိုလေ့လာခြင်း

ကွန်ပျူတာအသုံးပြုသူတွေဟာ တစ်ခါတရံလုပ်လက်စအလုပ်ကိုဒီတိုင်းထားပြီး စက်ရှေ့မှ ထသွားတဲ့အခါ Security ပိုင်းမှာသုံးနိုင်ဖို့ ယခု Predator Program ကိုလေ့လာတင်ပြလိုက်ပါတယ်။

Predator Program ကိုသုံးနိုင်ဖို့ USB Memory Stick တစ်ခုလိုအပ်ပါတယ်။ Data ဆိုဒ်ကတော့ ဘာပဲဖြစ်ဖြစ်ရပါတယ်။ ယခု Predator Program ကို Visual Basic Language ဖြင့်ရေးသားထားပြီး USB Memory Stick အတွင်း Visual Basic User Control File တစ်ခုထည့်သုံးမှာပါ။



Predator Program ရဲ့အဓိကလုပ်ဆောင်ချက်မှာ USB Memory Stick ကိုတပ်ဆင်ထားပြီး Predator Program ကို Run ထားရပါမယ်။ ကိစ္စတစ်ခုခုကြောင့်စက်ရှေ့မှထရတဲ့အခါ USB Memory Stick ကိုဆွဲဖြုတ်သွားတာနဲ့ သိပ်မကြာခင် စက္ကန့်ပိုင်းလောက်မှာ ကွန်ပျူတာမျက်နှာစာတစ်ခုလုံး မဲနက်သွားပြီး လုပ်ဆောင်ချက်တွေအားလုံးကိုတားမြစ်လိုက်ပါတယ်။

အားနည်းချက်ကတော့ အစမှ Restart ချပြီးပြန်ဖွင့်လိုက်လျှင်ပုံမှန်အသုံးအတိုင်းပြန်ဖြစ်သွားပါတယ်။ Windows ပြန်လည်စတင်ပါလိမ့်မယ်။

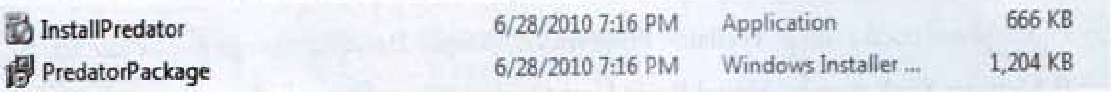
ဒါ့ကြောင့် လုံခြုံရေးပိုင်းမှာတော့ အားသိပ်မထားသင့်ပါဘူး။ ထူးထူးခြားခြားသုံးလိုတဲ့သူတွေအတွက် ရည်ရွယ်ပြီးထည့်သွင်းရှင်းပြထားတာပါ။

USB Memory Stick မလိုပဲ ပုံမှန်အတိုင်းသုံးလိုလျှင်လည်း မျက်နှာစာပေါ်မှ အဆိုပါ Icon ကိုကလစ်နှစ်ချက်နှိပ်လိုက်တာနဲ့ မျက်နှာစာတစ်ခုလုံးကို ကာကွယ်ထားလိုက်ပါတယ်။

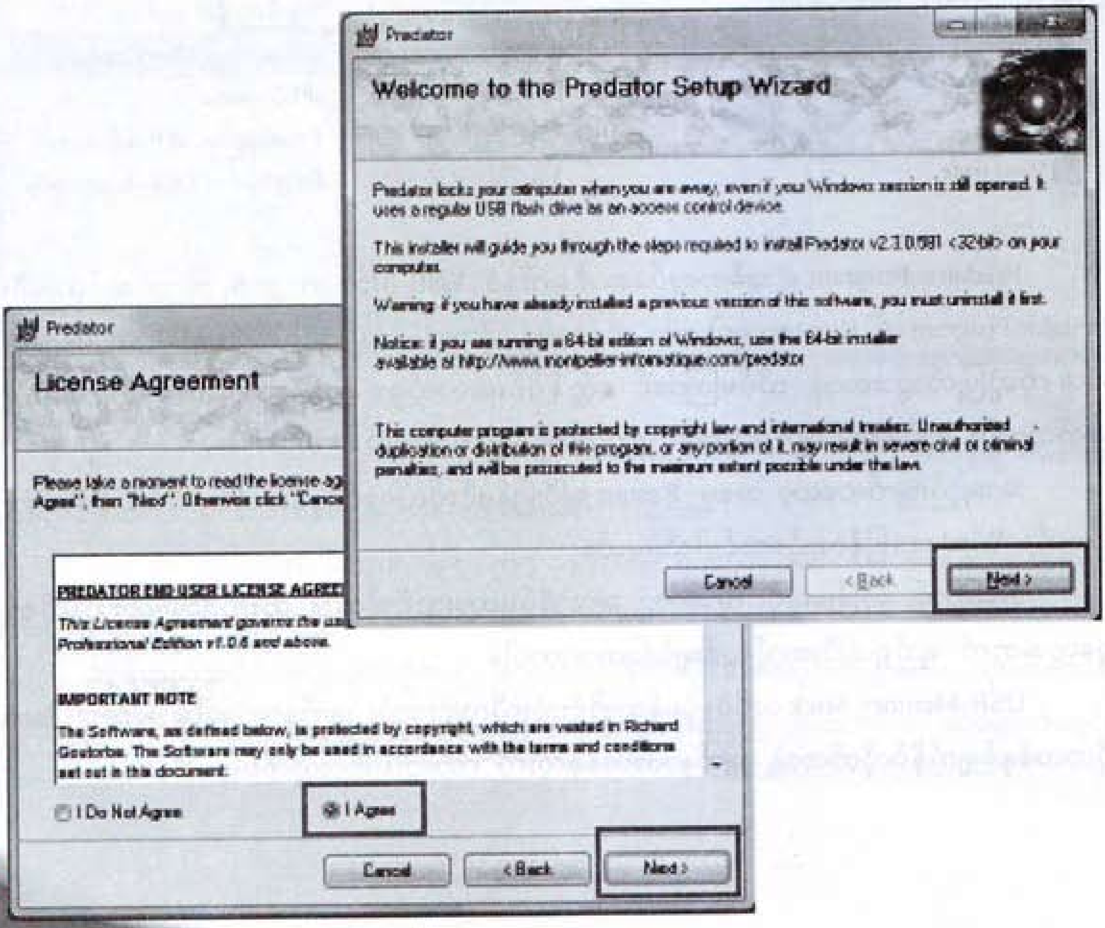
Predator Program Installation

Predator Program ကိုအောက်ပါအတိုင်းအဆင့်လိုက်ထည့်သွင်းရပါမယ်။

ပထမဦးစွာ စာအုပ်နှင့်တွဲပါသော DVD ထဲမှ PROGRAM => Predator Folder ကိုဖွင့်လိုက်ပါ။ အောက်ပါဖိုင်နှစ်ခုတွေ့ရပါမယ်။ PredatorPackage ကိုကလစ်နှစ်ချက်နှိပ်လိုက်ပါ။

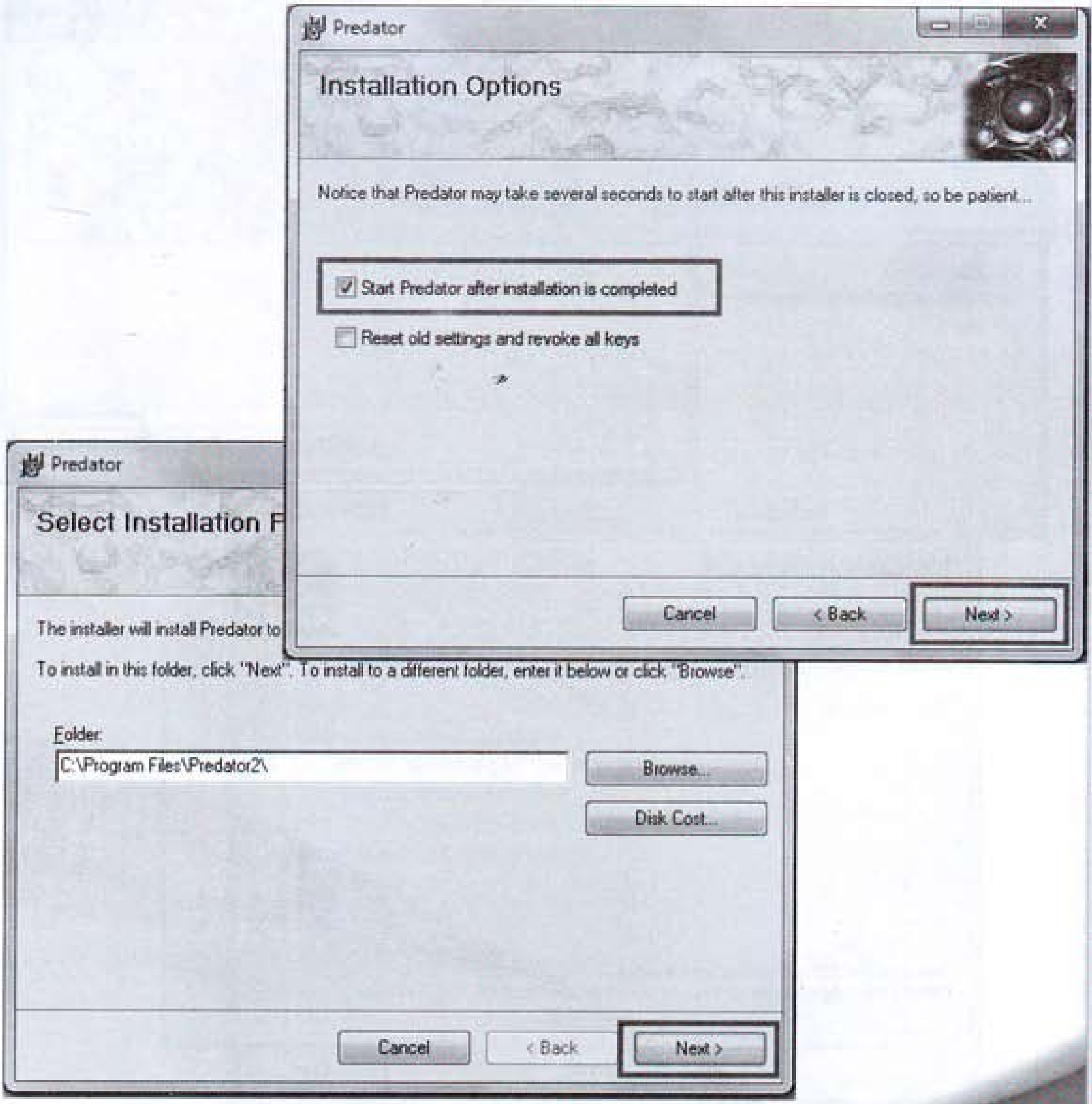


Welcome Box တက်လာလျှင် Next Button ကိုနှိပ်ရမှာဖြစ်ပြီး၊ License Agreement Box အတွက်ကတော့ I Agree ကိုရွေးကာ Next Button ကိုသာနှိပ်ရပါမယ်။



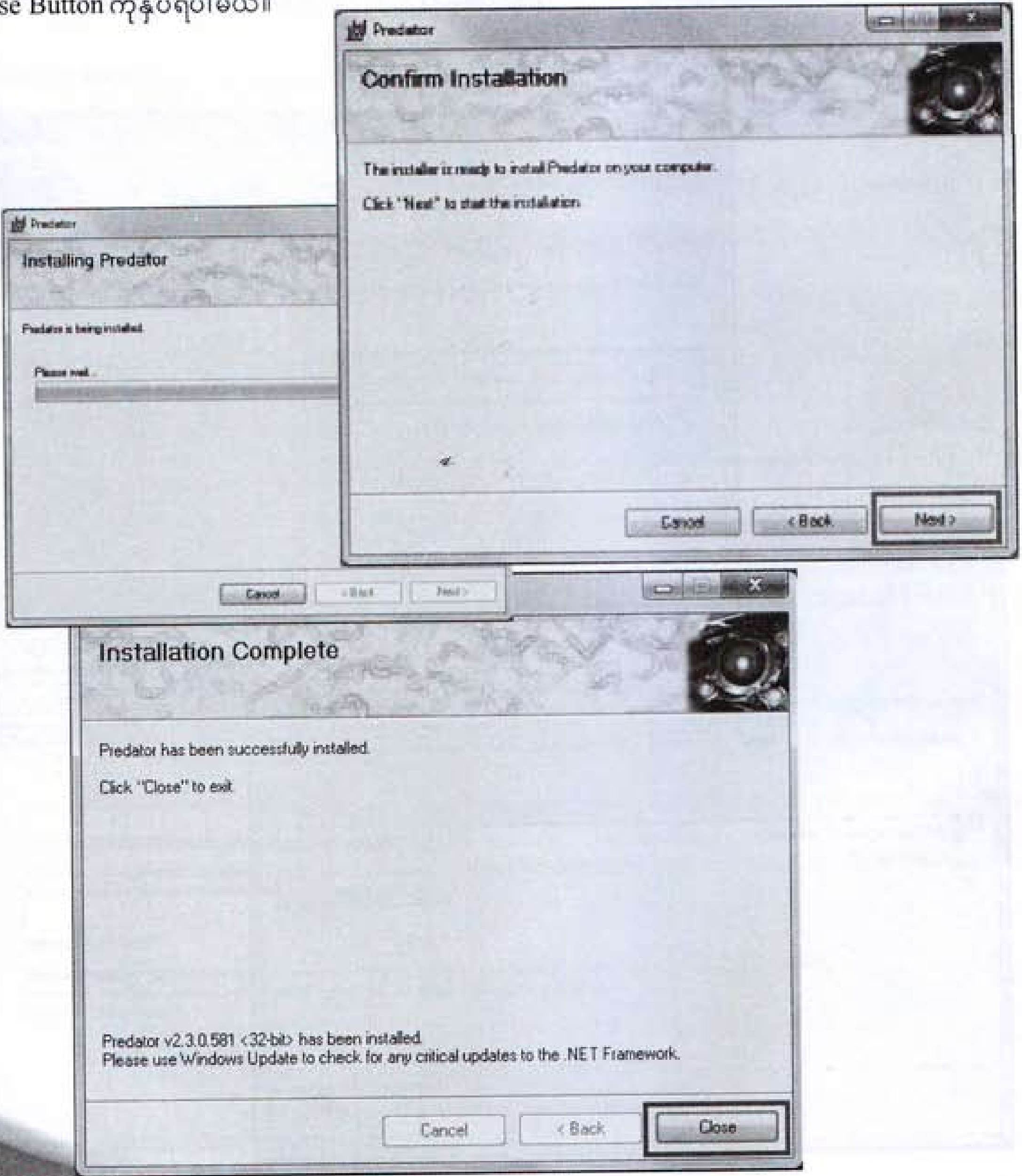
Installation Options Box မှာတော့ Start Predator after----- ကိုရွေးချယ်အမှတ်တပ်ပြီး Next Button ကိုနှိပ်ရပါ။

Select Installation Folder Box အတွက်ကတော့ File Location ကိုပေးသည့်အတိုင်းထားကာ Next Button ကိုသာနှိပ်ရပါမယ်။

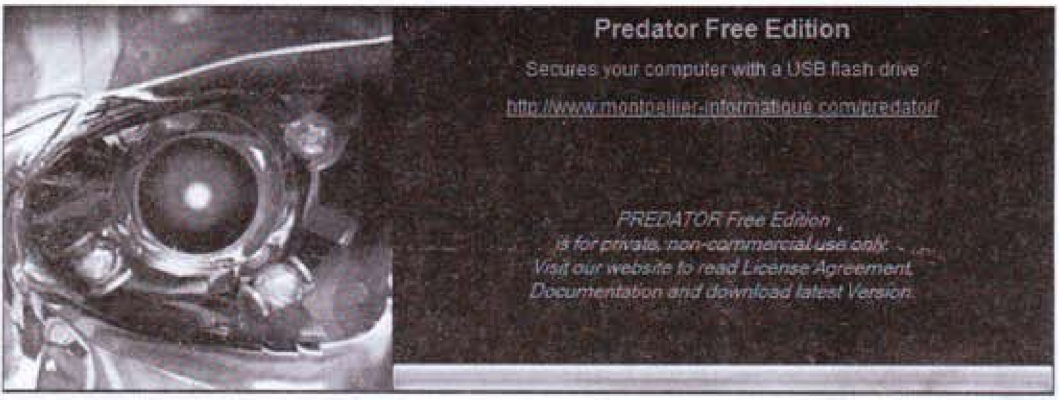


Confirm Installation Box မှာတော့ Next Button ကိုသာနှိပ်ရပါမယ်။ Installation လုပ်နေတာကို ဒုတိယပုံအတိုင်းခဏစောင့်ဆိုင်းရပါမယ်။

အောက်ဆုံးမှပုံ Installation Complete Box ကတော့ File တွေအားလုံးထည့်သွင်းပြီးသွားတာပါ။ Close Button ကိုနှိပ်ရပါမယ်။

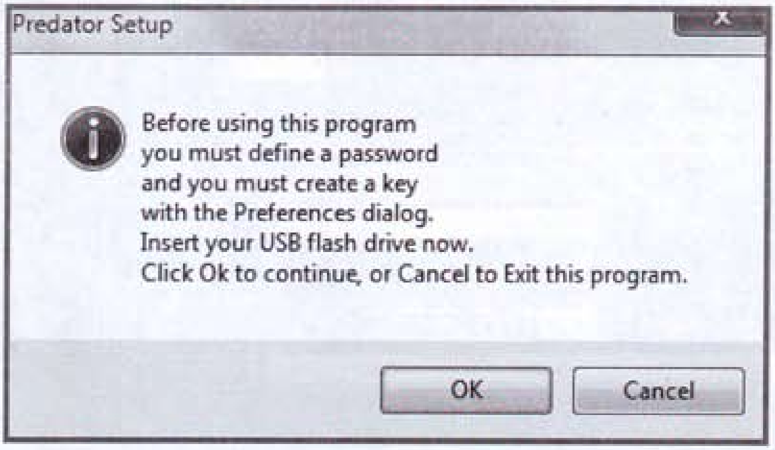


အသုံးပြုရန်အဆင်သင့်ဖြစ်နေပြီဖြစ်လို့အောက်ပါအတိုင်း Predator Program စတင်မောင်းနှင်နေသည်ကိုတွေ့မြင်ရပါမယ်။



အောက်ပါအတိုင်း Predator မှတောင်းဆိုမှုအဖြစ် USB Flash Drive တပ်ဆင်ပြီးလျှင်အသုံးပြုရန် OK Button ကိုနှိပ်ဖို့လိုပါတယ်။ Cancel Button ကတော့ အလုပ်မလုပ်ပဲထွက်မယ်ဆိုလျှင်ရွေးရပါမယ်။

ဒါကြောင့် စာဖတ်သူရဲ့ USB Flash Drive ကို USB Port မှာတပ်ဆင်ကာ OK Button ကိုနှိပ်လိုက်ပါ။



အောက်ပါအတိုင်း Predator စတင်လုပ်ဆောင်နေသည့်အတွက် Main Options ကိုတွေ့နေရပါပြီ။ ရှင်းလင်းပြေပြစ်တဲ့ စကားလုံးတွေနဲ့ စနစ်တွေကိုလုပ်ဆောင်ထားပါတယ်။

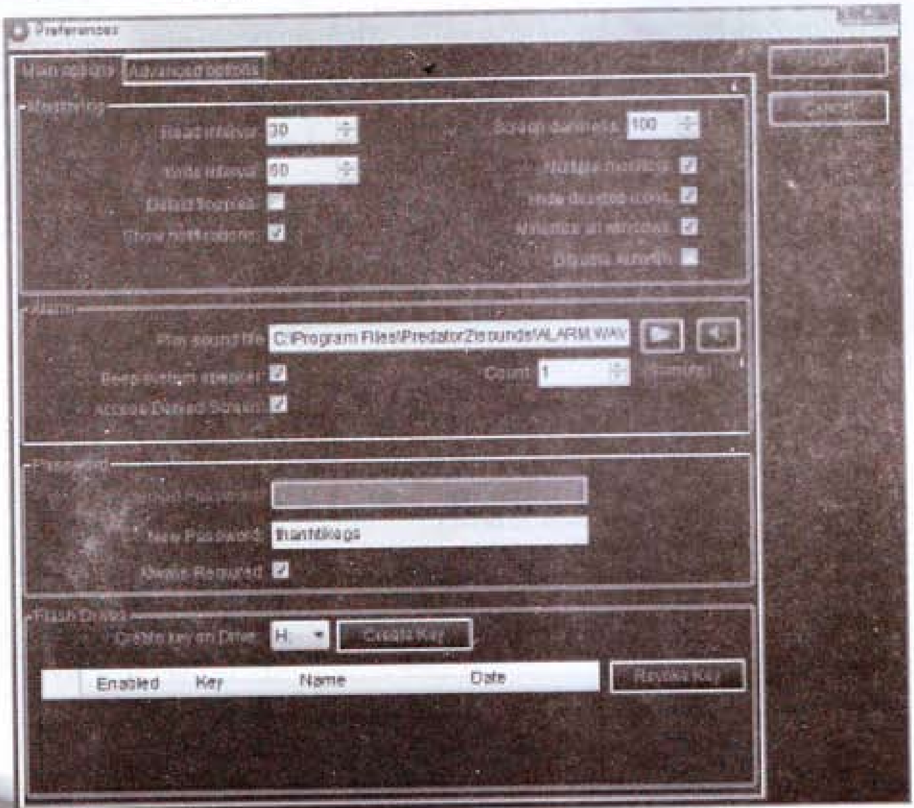
Monitoring အုပ်စုမှာဆိုလျှင် Lock ကျသွားတဲ့အခါ တွေ့မြင်ရမယ့်ပုံစံတွေကို ပြင်ဆင်ယူဖို့အတွက်ဖွဲ့စည်းထားပါတယ်။

Alarm အုပ်စုမှာတော့ အသံဖြင့်သတိပေးဖို့အတွက် Program နှင့်အတူပါလာသော Sound File ကိုညွှန်ပြထည့်သွင်းထားပါတယ်။ အကြိမ်ကြိမ်အသံပြုလိုလျှင် Count ကိုတိုးထားနိုင်ပါတယ်။

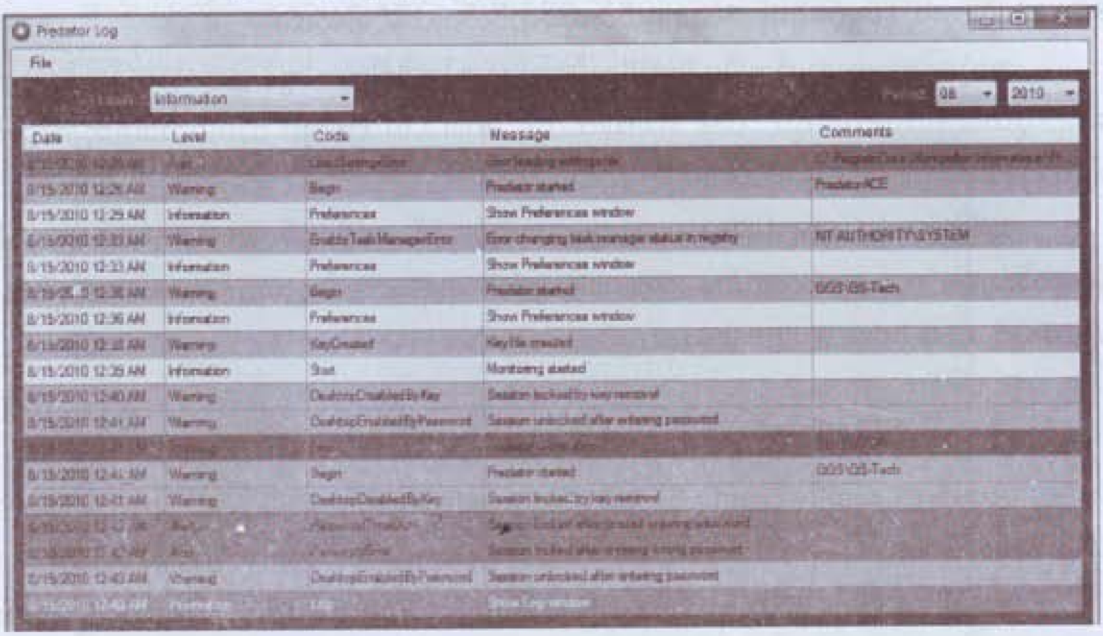
Password တွင် ပထမဆုံးအကြိမ်ဖြစ်တဲ့အတွက် New Password ကိုသာထည့်သွင်းပေးရပါမယ်။

USB Flsh Drive ကိုတော့ အလိုအလျောက်ရွေးချယ်ပေးပါလိမ့်မယ်။ နှစ်ခုလောက်တပ်ထားလျှင် အသုံးပြုမယ့် USB Flsh Drive ကိုရွေးပေးရပါမယ်။

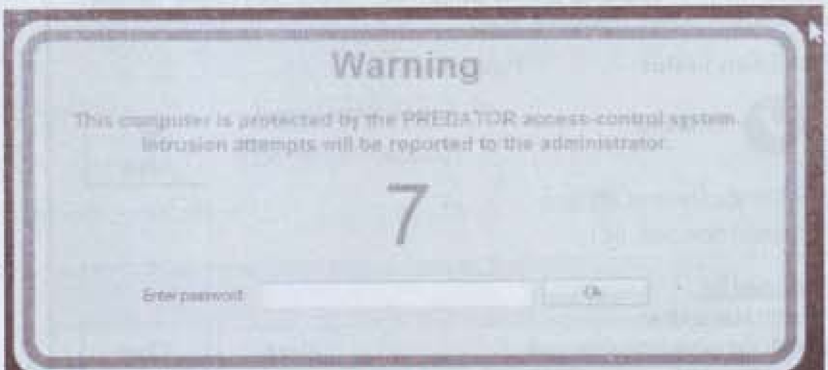
အားလုံးပြင်ဆင်ပြီးလျှင် Create Key Button ကိုသာနှိပ်လိုက်ပါ။ USB Flsh Drive အတွင်းသို့ အလိုအလျောက် အစီအစဉ်ချသွားပါလိမ့်မယ်။



အောက်တွင်တွေ့မြင်နေရတဲ့ပုံစံကတော့ Predator ကိုအသုံးပြုထားတဲ့ Information List တွေဖြစ်ပါတယ်။ ကိုယ့်အပြင်အခြားသုံးသူတွေကိုသိနိုင်ပါတယ်။



အောက်တွင်တွေ့မြင်နေရတဲ့ပုံစံကတော့ Predator ကိုအသုံးပြုထားပြီး Lock ချလိုက်လျှင်တွေ့မြင်ရမည့် မျက်နှာစာမှ Warning Box ဖြစ်ပါတယ်။ စက္ကန့်၂၀အတွင်း Password ကိုထည့်ပေးရပါမယ်။ မထည့်နိုင်လျှင်/မှားနေလျှင် Alarm မည်ပြီးလုပ်ဆောင်ခွင့်များ ပိတ်သွားပါလိမ့်မယ်။

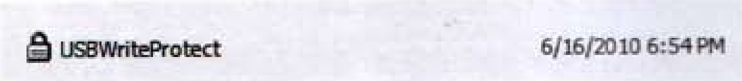


USB Memory Stick and USB Drive ဖြင့်ကူးယူခြင်းအားထိန်းချုပ်ခြင်း

ကွန်ပျူတာအတွင်းမှ စာရေးသူ၏အချက်အလက်များကို မသက်ဆိုင်သူများမှ USB Memory Stick သုံးပြီးကူးယူနိုင်ခွင့်မရှိရန် Security ပိုင်းဆိုင်ရာပိတ်ထားနိုင်ပါတယ်။

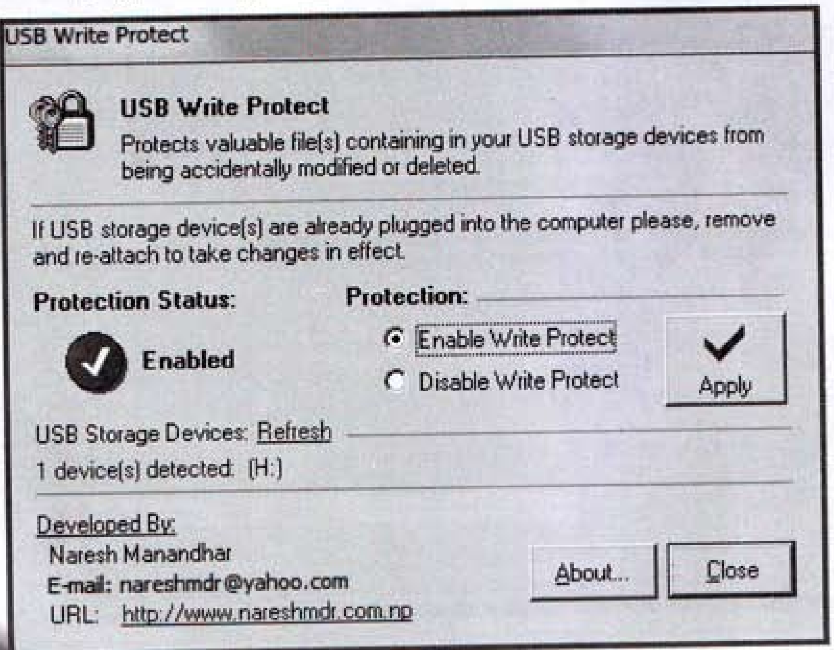
အသုံးပြုရအထူးလွယ်ကူပြီး၊ Install လုပ်ရခြင်းလည်းမရှိပါဘူး။ ကွန်ပျူတာအတွင်းဝင်ရောက်နေရာယူထားခြင်းလည်းမရှိပဲ Task Manager တွင် Run List Process ကိုပါမထားရှိတဲ့အတွက် ခြေရာပြန်ကောက်ဖို့တောင်မလွယ်ကူပါ။

ထူးခြားသည်ကတော့ USB Memory Stick အတွင်းမှဖိုင်များကို ကွန်ပျူတာအတွင်းသို့ကူးယူရရှိနိုင်သော်လည်း၊ ကွန်ပျူတာအတွင်းမှ Data File များကို တစိုးတစိပင်ကူးယူခွင့်မပေးပါ။ အရှင်းဆုံးပြောရလျှင် USB Drive Write Protected လုပ်ထားတာပါ။



ပထမဦးစွာ စာအုပ်နှင့်တွဲပါသော CD ထဲမှ Security Folder > USB Write Protect Folder > USB Write Protect.exe ကိုကလစ်နှစ်ချက်နှိပ်လိုက်ပါ။ အောက်ပါပုံအတိုင်းတွေ့ရပါလိမ့်မယ်။

Install လုပ်ရန်၊ Copy ကူးထည့်ထားရန် မလိုအပ်ပါ။ တိုက်ရိုက်အကျိုးသက်ရောက်စေပါတယ်။



Enable Write Protect ကိုရွေးထားပြီး Apply Button ကိုနှိပ်လိုက်ပါ။ Protection Status နေရာတွင် အမှန်ခြစ်အစိမ်းလေး ပေါ်လာပါလိမ့်မယ်။ Close ဖြင့်ထွက်နိုင်ပါပြီ။ USB Drive ကိုကာကွယ်ပြီးပါပြီ။

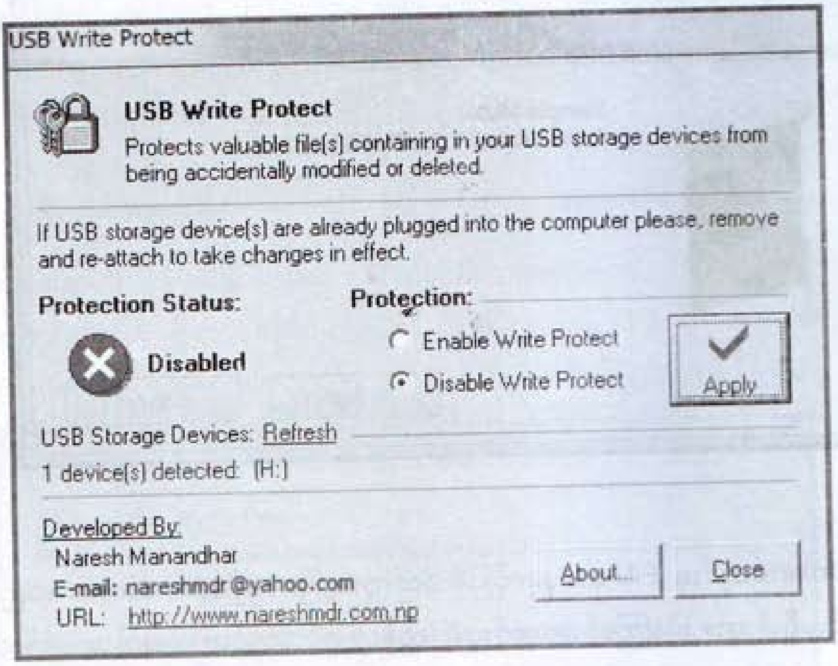
အဆိုပါအတိုင်းကာကွယ်ပြီးလျှင် ဖိုင်တစ်ခုခုကို နည်းတစ်မျိုးမျိုးဖြင့် USB Drive အတွင်း ကူးထည့်ကြည့်ပါ။ အောက်ပါ Error Box တက်လာပါလိမ့်မယ်။

USB Drive အတွင်းမှ File တစ်ခုခုကိုပြန်လည်ကူးယူပြီး ကွန်ပျူတာအတွင်း ထည့်ကြည့်ပါ။ တားမြစ်ထားခြင်းမရှိပါဘူး။ ဒါ့ကြောင့် စာဖတ်သူရဲ့ ကွန်ပျူတာအတွင်းမှ အချက်အလက်တွေအတွက် အခြားသူများမကူးယူနိုင်တော့လို့စိတ်ချသွားလို့မရသေးပါ။ ဤဆော့ဖ်ဝဲရှိနေသူတစ်ယောက်ယောက်က ပြန်လည်ဖွင့်သွားနိုင်ပါတယ်။

ရှင်းရှင်းပြောရလျှင် မူပိုင် Admin တစ်ဦးသုံးဖြစ်မနေပါ။ ဆော့ဖ်ဝဲရှိနေသူတိုင်းပြန်လည်ဖွင့်သုံးနိုင်ပါတယ်။ ဒါ့ကြောင့် ဘာပဲဖြစ်ဖြစ် အလွန်ကိုအရေးကြီးတဲ့ အချက်အလက်များကို ရယူသွားလျှင်တောင် ပြန်လည်မဖတ်နိုင်အောင် Encryped လုပ်ထားသင့်ပါတယ်။

Write Protect ကိုပြန်ဖြုတ်ဖို့ကတော့ CD အတွင်းမှ USB Write Protect.exe ကို ကလစ်နှစ်ချက်နှိပ်လိုက်ပါ။ ထွက်ပေါ်လာသော အောက်ပါပုံတွင် Disable Write Protect ကိုရွေးပြီး Apply Button နှိပ်လိုက်ကာ Close ဖြင့်ပိတ်လိုက်ပါ။

USB Drive ကိုပြန်သုံးနိုင်ပါပြီ။ ယခုနှစ်ပိုင်းတွင် ထွက်ပေါ်နေသော Laptop အချို့တွင် Write Protect System ကိုသုံးထားပါတယ်။ ဒါပေမယ့် ယခုဆော့ဖ်ဝဲမဟုတ်ပါ။ သို့သော်လည်း ယခုဆော့ဖ်ဝဲဖြင့် ဝင်ရောက်ပြီး Disable Write Protect ထားကာအသုံးပြုကြည့်ပါဦး။

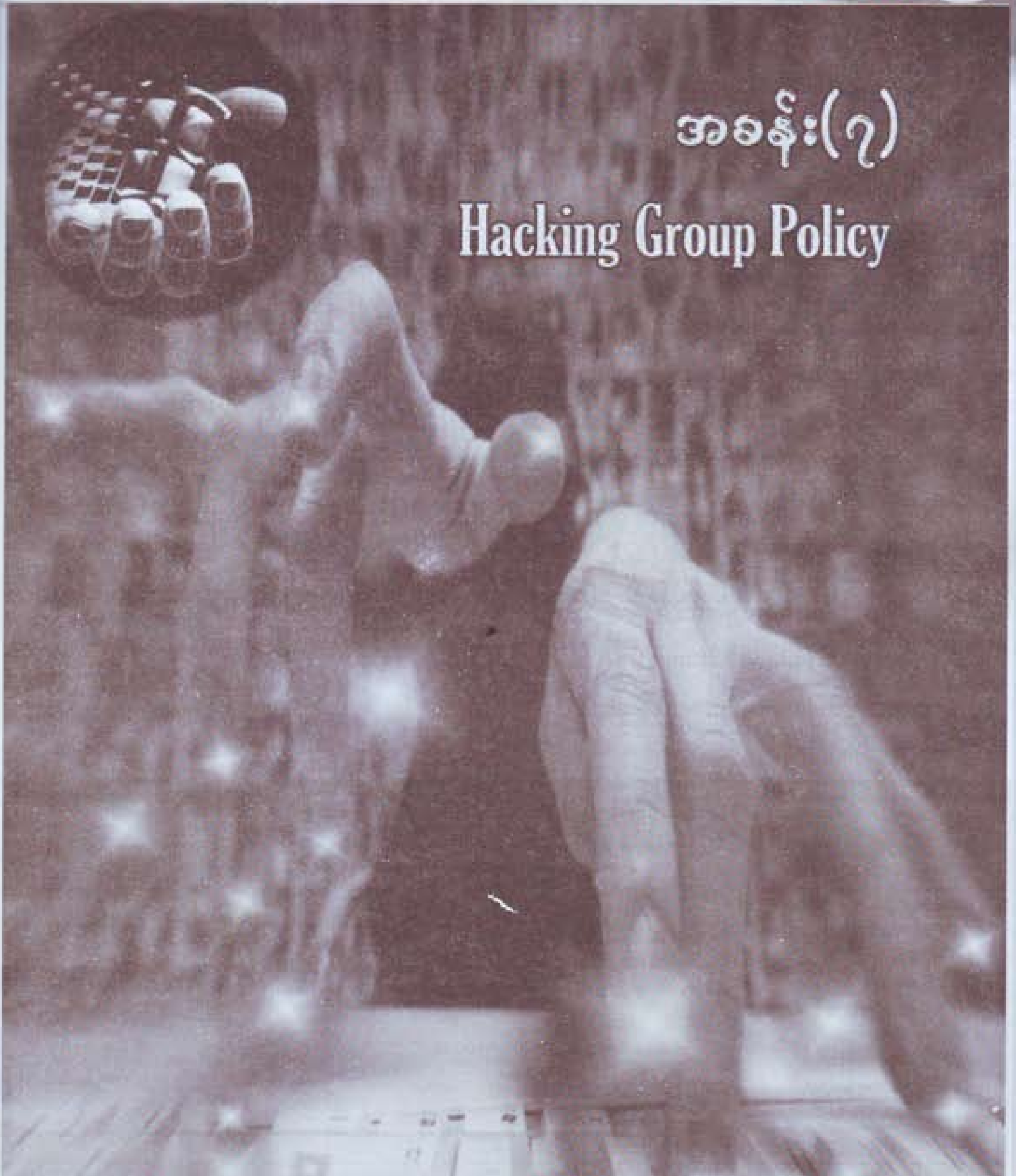


စာဖတ်သူဟာ ကွန်ပျူတာနည်းပညာများကိုအတွင်းကျကျလေ့လာနေသူဖြစ်ခဲ့လျှင် ယခုဆော့ဖ်ဝဲလေးကိုဆောင်ထားလိုက်ပါ။ အသုံးတည့်ဖို့ရှိလာမှာပါ။ Honest Hacker တွေအတွက်အသုံးဝင်မှာပါ။

ယခုဆော့ဖ်ဝဲလေးဟာ ပေါ့ပေါ့ပါးပါးရှိသလို နောက်ကြောင်းပြန်မကောက်နိုင်တာကတော့ System Registry အတွင်းဝင်ပြင်ပြီး ပြန်ထွက်သွားလို့ဖြစ်ပါတယ်။

အခန်း(၇)

Hacking Group Policy



Group Policy ကိုလေ့လာခြင်း

ကွန်ပျူတာအသုံးပြုအများစုဟာ Registry ကိုသိသူ/ သုံးသူများကြပေမယ့် Group Policy ကိုသိပ်မသိကြပါဘူး။ Hacker တွေအတွက်ကတော့ Registry နှင့်တန်းတူအရေးပါအရာရောက်ပါတယ်။ ကွန်ပျူတာစက်ပြင်သမားတွေအတွက်ကလည်း အရေးပါပါတယ်။

Group Policy ဆိုတာ ကွန်ပျူတာအတွင်းမှ System ဆိုင်ရာညွှန်ကြားချက်တွေကို ပြန်လည်ထိန်းချုပ်ထားတဲ့ နေရာတစ်ခုဖြစ်ပါတယ်။ Group Policy တစ်ခုကိုကိုယ်တိုင်ပြန်လည်တည်ဆောက်နိုင်ပါတယ်။ သို့သော် ပြန်လည်တည်ဆောက်ပုံတွေမှာ ပြဿနာဖြစ်ပေါ်လာနိုင်တာကြောင့် စာရေးသူအနေဖြင့် ချန်လှပ်ထားတဲ့ရပါတယ်။

Group Policy ကိုအဓိကအားဖြင့် အပိုင်းနှစ်ပိုင်းခွဲခြားထားပါတယ်။

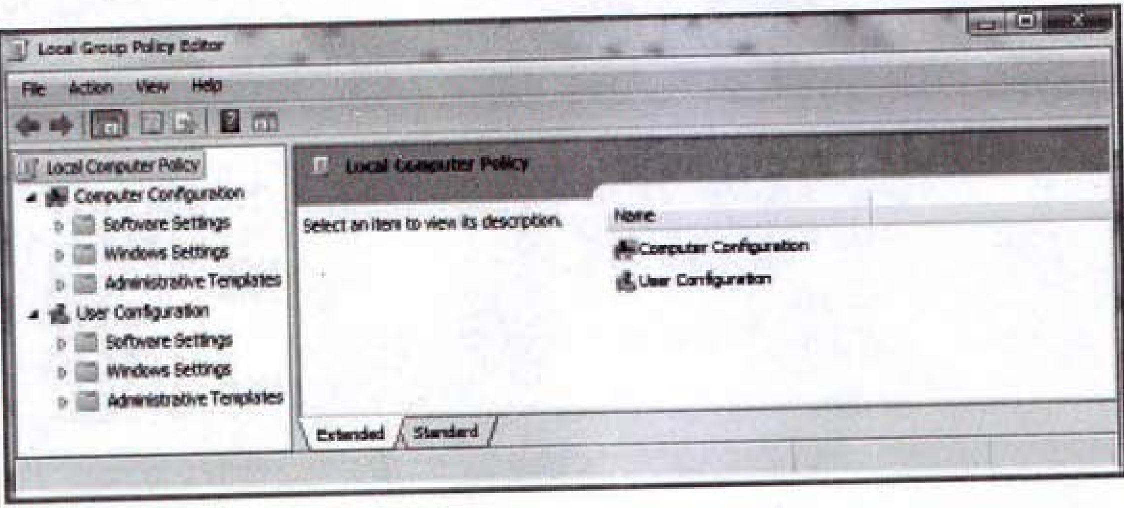
၁။ Computer Configuration

၂။ User Configuration တို့ဖြစ်ကြပါတယ်။ အဆိုပါ နှစ်ပိုင်းလုံးအောက်တွင် ခေါင်းစဉ်သတ်မှတ်ချက်တူညီပြီး အတွင်းပိုင်းလုပ်ငန်းစဉ်မတူညီသော စနစ်ဆိုင်ရာအုပ်စု သုံးခုရှိပါတယ်။

၁– Software Settings

၂– Windows Settings

၃– Administrative Templates

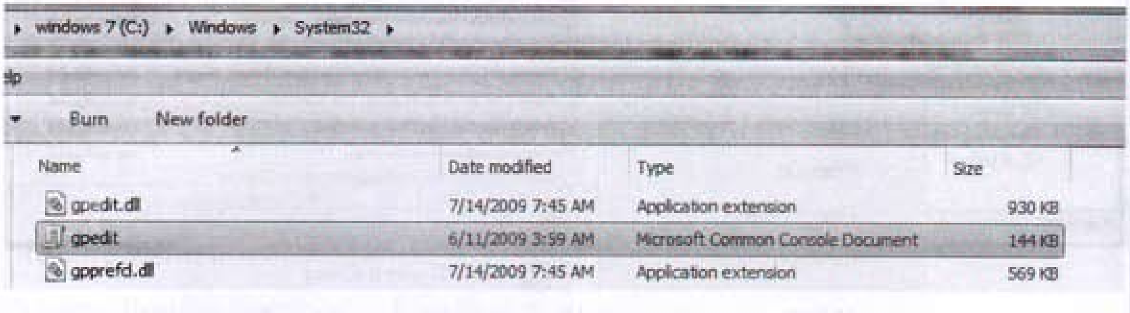


Registry Editor, Command Prompt အပါအဝင် System ပိုင်းဆိုင်ရာများစွာကို ထိန်းချုပ်နိုင်ပါတယ်။ စာဖတ်သူတွေရဲ့ထိန်းချုပ်နိုင်စွမ်းမှာ Registry Editor နှင့်မတူညီတာကတော့ တိုက်ရိုက်အကျိုးသက်ရောက်ပါတယ်။ Restart ချဖို့မလိုအပ်ပါဘူး။ ထို့အပြင် ဝင်ရောက်ပြင်ဆင်ရတာလည်း အလွန်လွယ်ကူပါတယ်။

ယခုကဏ္ဍကို စာဖတ်သူများနားလည်စေရန် သာရည်ရွယ်တာကြောင့် အစဉ်လိုက်ရှင်းပြမနေတော့ပဲ အစဉ်သင့်သလိုရှင်းပြသွားပါမယ်။ ပထမဦးစွာ Start Menu ပိုင်းထိန်းချုပ်နိုင်တာတွေကို ရှင်းပြပါ့မယ်။

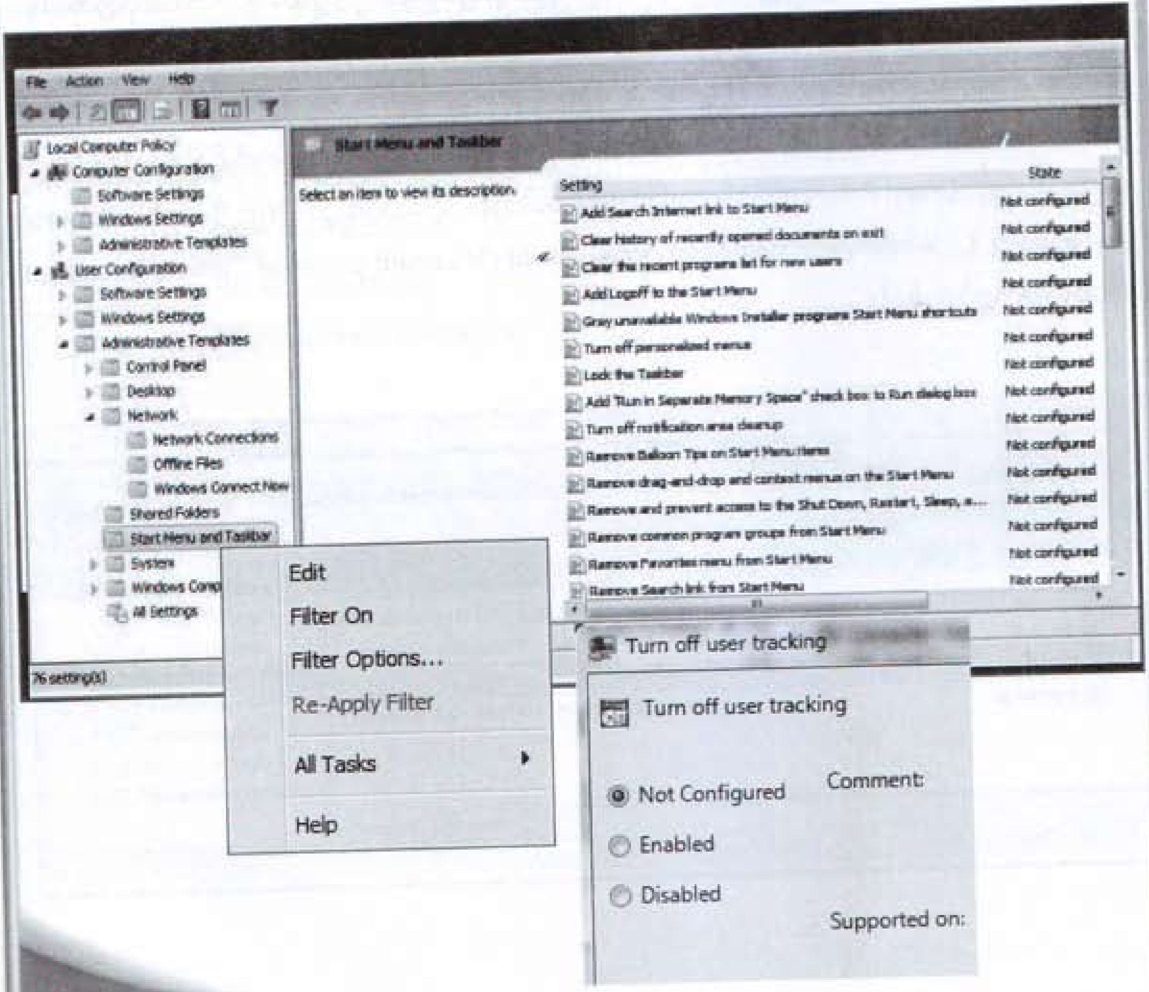
Start Menu မှာပါဝင်သမျှ System ပိုင်းဆိုင်ရာထိန်းချုပ်မှုများကို ကွယ်ပျောက်ထားလိုတဲ့အခါမှာ အသုံးဝင်ပါတယ်။ ဘယ်လောက်တောင်အသုံးဝင်တယ်ဆိုတာကတော့အောက်ဖက်မှာလက်တွေ့သာ လုပ်ဆောင်ကြည့်လိုက်ပါ။

Group Policy ကိုဖွင့်ဖို့အတွက် Run Box ကိုသုံးလိုလျှင် gpedit.msc လို့ရိုက်ထည့်ရပါမယ်။ အများအားဖြင့် Group Policy ကိုပိတ်ထားခြင်းမရှိကြပါဘူး။ သို့သော်လည်း Run Box ကိုပိတ်ထားတဲ့အခါမှာတော့ C:\Windows\System32 အောက်မှ "gpedit (Microsoft Common Console Document) ကိုဝင်ရောက်ဖွင့်လှစ်ပါ။



Group Policy ကိုမပြင်ဆင်ခင် စာဖတ်သူသိထားရမည်ကတော့ Group Policy မှာ ညွှန်းထားတဲ့ ညွှန်ကြားချက်တွေဟာ 'ဖျက်လိုက်မည်'၊ 'ပိတ်ထားမည်' စသဖြင့် လုပ်ပြီးသားတွေကိုသာညွှန်းပါတယ်။ ဒါကြောင့် မသုံးလိုလို့ ပိတ်ထားဖို့၊ ဖျက်လိုက်ဖို့ညွှန်းလျှင် Enable ကိုသုံးရပါမယ်။ မူလအတိုင်းပြန်လည်ရှိစေလိုလျှင်တော့ Disable ကိုသုံးပါမယ်။ ဒါမှမဟုတ်မူရင်းထားရှိသည့် Not Configured ကိုလည်းရွေးချယ်နိုင်ပါတယ်။

ပြောင်းလိုသည့် ညွှန်ကြားချက်လိုင်းပေါ် Right Click နှိပ်ပြီး Edit ကိုရွေးပါ။ ပေါ်လာသော Property Box တွင် ပိတ်ထား/ဖျက်ထားလိုပါက Enable ကိုရွေးပေးလိုက်ပြီး Ok/ Apply Button ကိုနှိပ်လျှင်ရပါပြီ။



Group Policy ဖြင့် Start Menu ကိုထိန်းချုပ်ခြင်း

User Configuration > Administrative Templates > Start Menu and Taskbar

Group Policy မှ Start Menu အတွက် ထိန်းချုပ်နိုင်သော ညွှန်ကြားချက်များမှာ အောက်ပါတို့ဖြစ်ပါတယ်။ ဒီ့ထက်မကသော ညွှန်ကြားနိုင်မှုများကျန်ရှိနေပါသေးတယ်။ စာဖတ်သူကိုယ်တိုင် လေ့လာသွားပါ။ ကွန်ပျူတာအသုံးပြုနေသူများဖြစ်လို့ တစ်ခုချင်းကို ဘာသာမပြန်ပြတော့ပါ။ နားမလည်လျှင် Enable ပေးကြည့်ပြီး Start Menu ကိုဖွင့်ကြည့်ပါ။ မပြုလုပ်လိုလျှင် Not Configured ပြန်ထားလိုက်ပါ။

- Add Search Internet link to Start menu
- Clear history of recently opened documents on exit
- Clear the recent programs list for new users
- Add Logoff to the Start menu
- Gray unavailable Windows Installer programs Start menu shortcuts
- Turn off personalized menus
- Lock the taskbar
- Add "Run in Separate Memory Space" check box to Run dialog box
- Turn off notification area cleanup
- Remove Balloon Tips on Start menu items
- Remove drag-and-drop and context menus on the Start menu
- Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands
- Remove common program groups from Start menu
- Remove Favorites menu from Start menu
- Remove Search link from Start menu
- Remove frequent programs list from Start menu
- Remove Games link from Start menu
- Remove Help menu from Start menu
- Turn off user tracking
- Remove All Programs list from Start menu

Group Policy ဖြင့် System ပိုင်းကိုထိန်းချုပ်ခြင်း

User Configuration > Administrative Templates > System > Ctrl+Alt+Del Options

Group Policy မှ System ဆိုင်ရာလုပ်ဆောင်ချက်တွေကိုထိန်းချုပ်နိုင်ပါတယ်။ စာရေးသူနှင့်အတူ လက်တွေ့လေ့လာကြည့်ရအောင်။

ကွန်ပျူတာအသုံးပြုနေသူအတော်များများသိကြတဲ့ Ctrl+Alt+Del Key သုံးလုံးပေါင်းနှိပ်တဲ့ စနစ်ကိုပြင်ဆင်ကြပါ့မယ်။ ထိုစနစ်အတွင်းမှာ ပါဝင်တဲ့

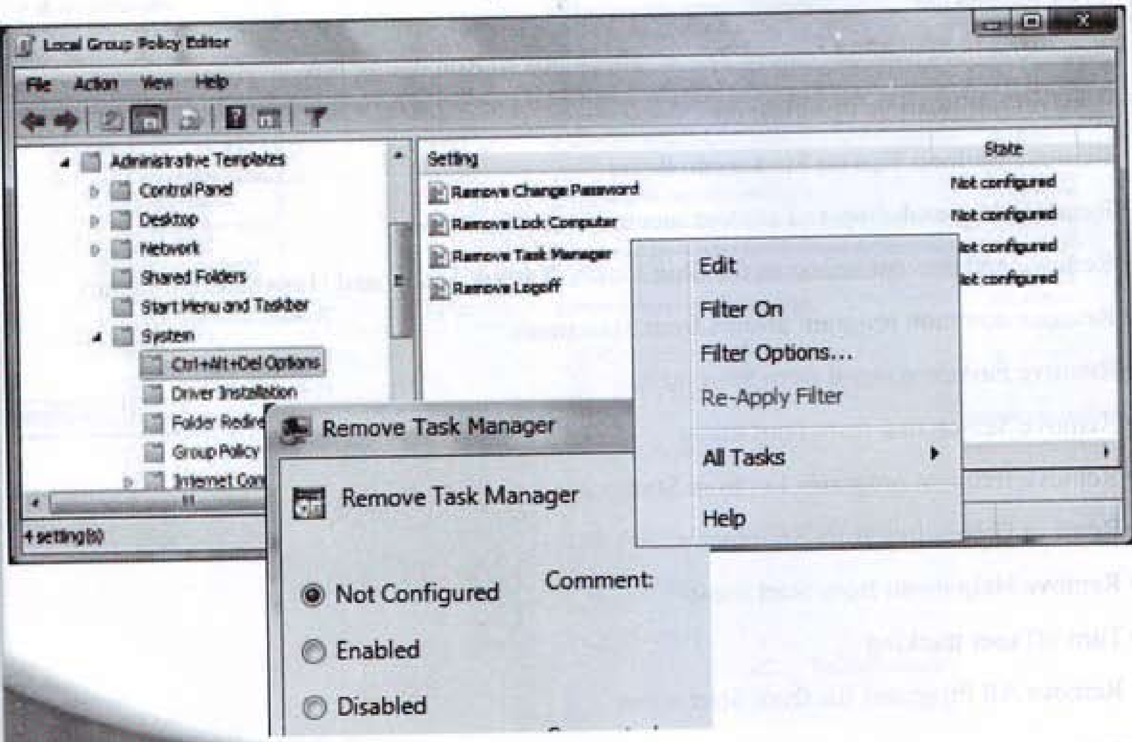
Remove Change Password

Remove Lock Computer

Remove Task Manager

Remove Logoff တွေကိုအသုံးပြုခွင့်ပိတ်ထားနိုင်ပါတယ်။

ပုံးစံအတိုင်း Property မှာ Enable ကိုထားပြီး၊ Ctrl+Alt+Del Key ဖြင့်ဝင်ကြည့်လိုက်ပါ။ ဥပမာ Task Manager ကိုပိတ်ထားလျှင် Task Manager မတွေ့ရတော့ပါဘူး။

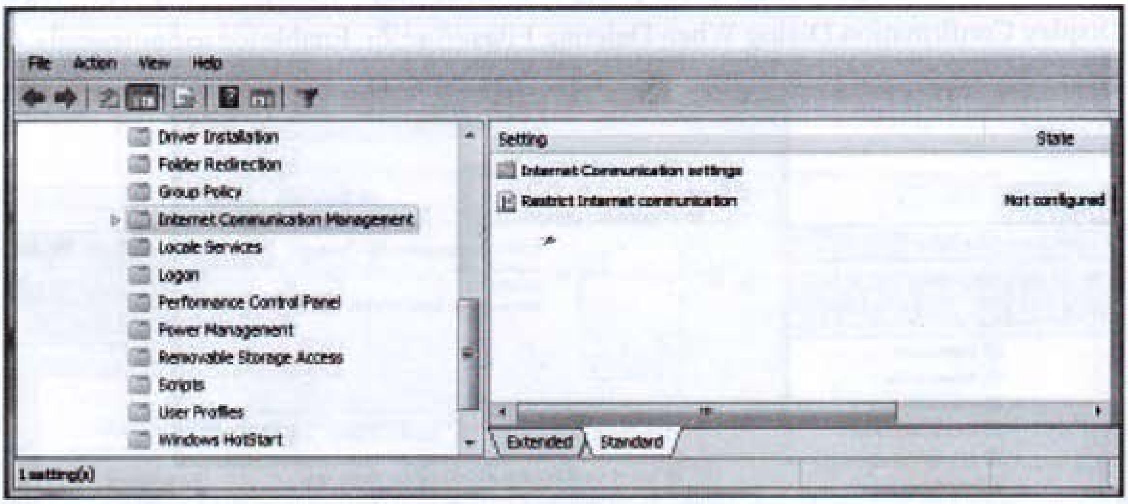


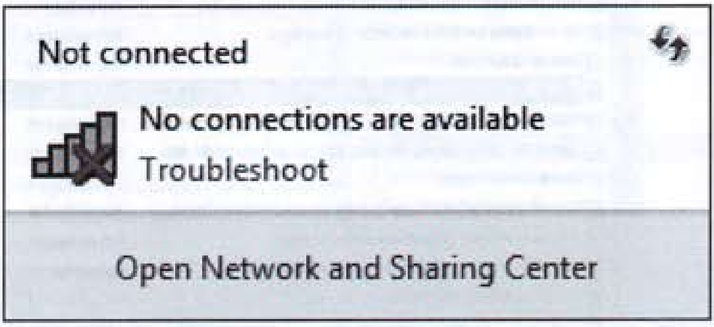
Group Policy ဖြင့် Internet Connection ပိုင်းကိုထိန်းချုပ်ခြင်း

User Configuration > Administrative Templates > System > Internet Communication Management

ဒီတစ်ခါတော့ Internet ချိတ်ဆက်မှုကိုတားမြစ်ထားပါမယ်။ Company နှင့် Office များတွင် အင်တာနက်လိုင်းချိတ်ဆက်ထားပြီးအသုံးမပြုစေလိုတဲ့အခါမှာ၊ ဒါမှမဟုတ် မိမိကိုင်ကွယ်ရမယ့်ကွန်ပျူတာမှာ Internet Line ကိုပိတ်ထားတဲ့အတွက် Hacking လုပ်ရမယ့်အခါအသုံးဝင်ပါတယ်။

အထက်ပါအတိုင်းအဆင့်ဆင့်ဝင်ရောက်ပြီး Internet Communication Management ၏ ညာဘက်မှ Option တွင် Restrict Internet Communication ကိုဖွင့်ပြီးပြင်ဆင်ရမှာပါ။





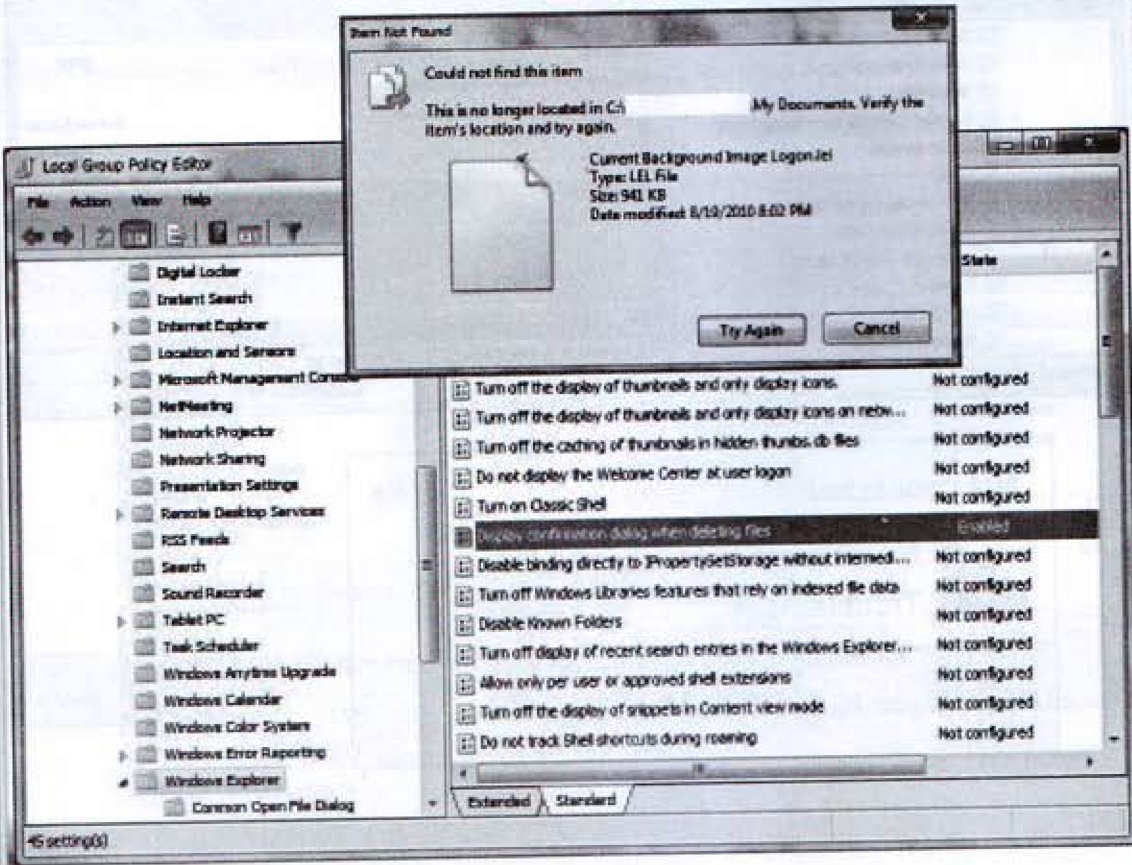
Group Policy ဖြင့် File Delete မပြုလုပ်ရန်ထိန်းချုပ်ခြင်း

User Configuration > Administrative Templates > Windows Components > Windows Explorer > Display Confirmation Dialog When Deleting Files

ဒီတစ်ခါတော့ My Documents > Documents အတွင်းမှမည်သည့်ဖိုင်ကိုမှ မဖျက်နိုင်စေရန် ပိတ်ပင်ထားမြစ် ထားပါမယ်။ ဒီလိုပြုလုပ်ထားခြင်းဖြင့် မိမိကွန်ပျူတာအတွင်းမှ ဖိုင်များ၊ အချက်အလက်များကို အခြားသူတစ်ဦးမှ ဝင်ရောက်ဖျက်သွားခြင်းမပြုနိုင်တော့ပါဘူး။

သို့သော် အခြားနေရာမှ ဖိုင်တွေကိုတော့ ဝင်ဖျက်နိုင်ပါတယ်။ တစ်ခုကိုသာကာကွယ်ပေးတာပါ။

အထက်ပါအတိုင်းအဆင့်ဆင့်ဝင်ရောက်ပြီး Windows Explorer ၏ညာဘက်မှ Option တွင် Display Confirmation Dialog When Deleting Files ကိုဖွင့်ပြီး Enable ပြင်ဆင်ပေးရမှာပါ။



Group Policy ဖြင့် Registry Editor and Command Prompt ကိုထိန်းချုပ်ခြင်း

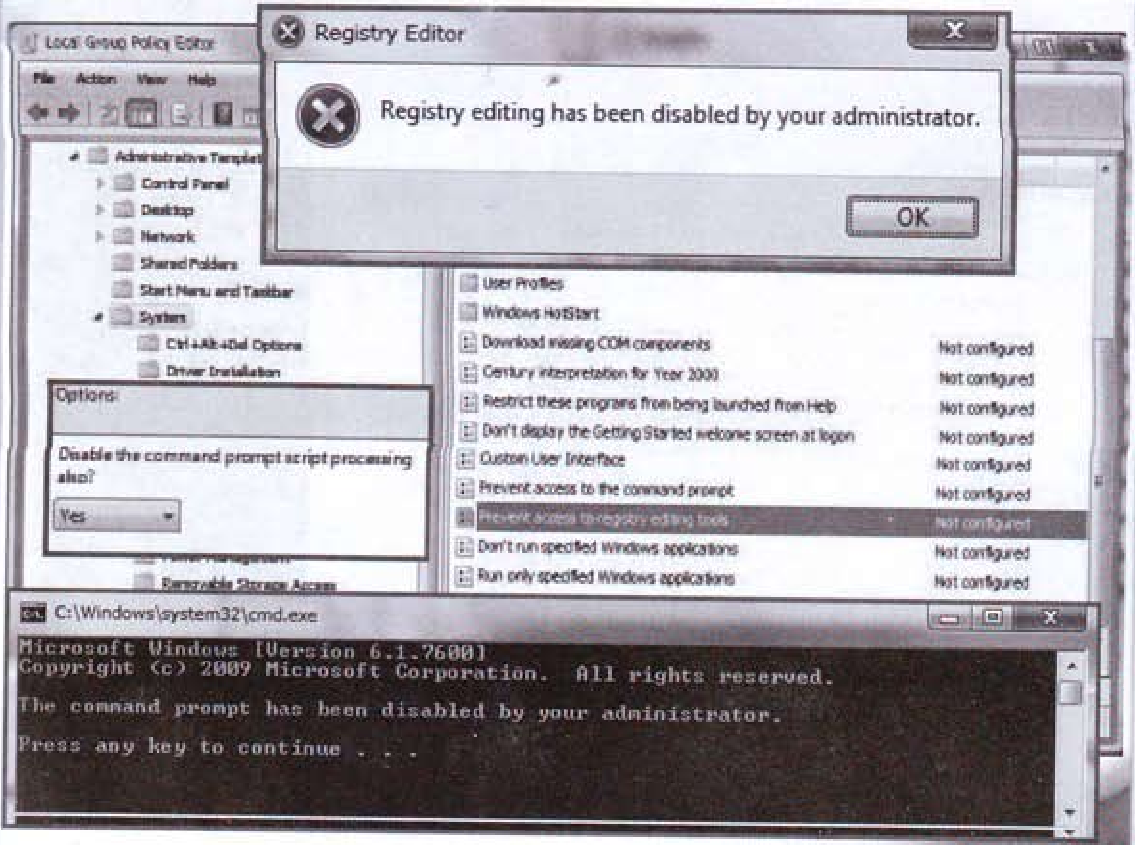
User Configuration > Administrative Templates > System

ဒီတစ်ခါတော့ System Command တွေပေးရတဲ့အခါ အရေးကြီးဆုံးဖြစ်တဲ့ Registry Editor နှင့် Command Prompt ကိုပိတ်ထားပါမယ်။

အများသုံးကွန်ပျူတာတွေမှာ ဒီလိုပိတ်ထားတဲ့အခါ ပြုပြင်စရာနည်းလမ်းကတော့ Group Policy မှဝင်ပြင်ယူခြင်းနှင့် Script Program ဖြင့်ပြင်ဆင်ခြင်းတို့ပဲရှိပါတော့တယ်။

အထက်ပါအတိုင်းအဆင့်ဆင့်ဝင်ရောက်ပြီး System ၏ညာဘက်ရှိ Option အောက်တွင် Prevent Access To Registry Editing Tools

Prevent Access To The Command Prompt တို့ရှိနေပါတယ်။ ပြောင်းလဲလိုသောအပေါ် ကလစ်နှစ်ချက်နှိပ်ဖွင့်ကာ Enable ကိုရွေးပါ။ Option အောက်တွင် Yes ကိုထပ်ရွေးပေးပါ။



Group Policy ဖြင့် Control Panel ကိုဖျောက်ထားခြင်း

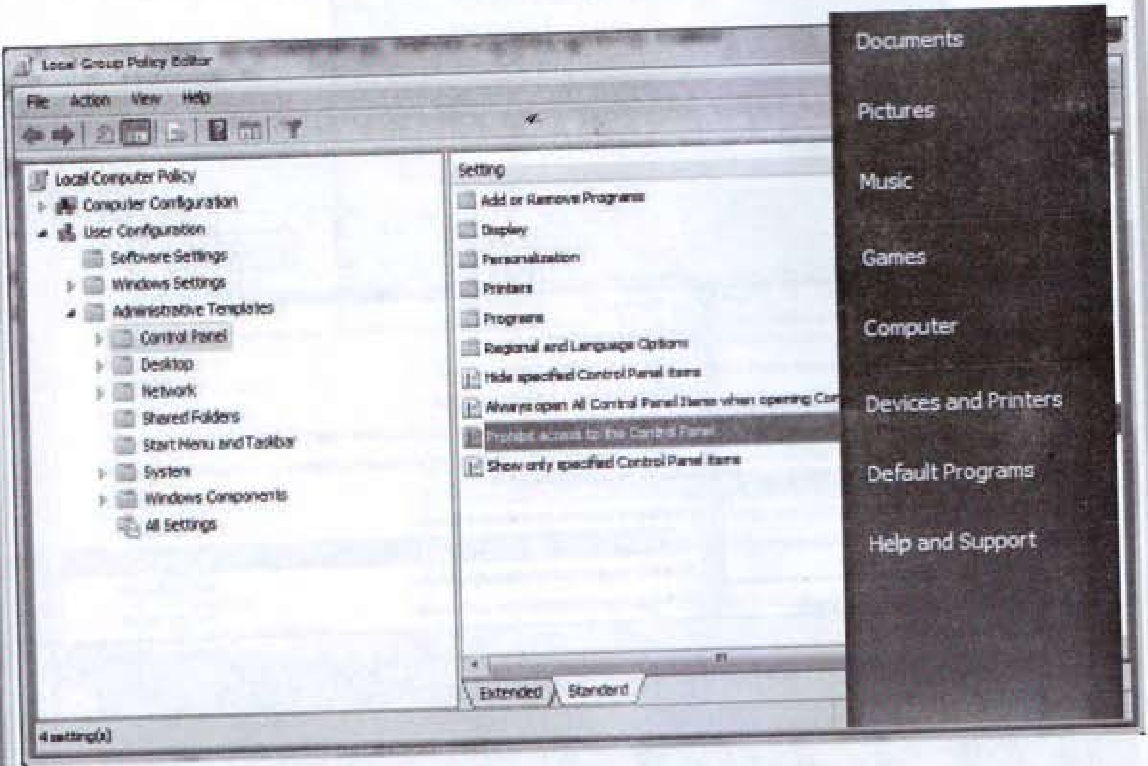
User Configuration > Administrative Templates > Control Panel >

ဒီတစ်ခါတော့ System ဆိုင်ရာHardware နှင့် Software တွေကိုထိန်းချုပ်ထားတဲ့ Control Panel ကိုအသုံးပြုခွင့်ပိတ်ထားပါ့မယ်။

အများသုံးကွန်ပျူတာတွေမှာ Control Panel ကိုသူတစ်ပါးဝင်သုံးခွင့်အား ပိတ်ထားကြပါတယ်။ အလွယ်တကူ စက်ချို့ယွင်းလွယ်တဲ့အတွက်ကြောင့်ပါ။

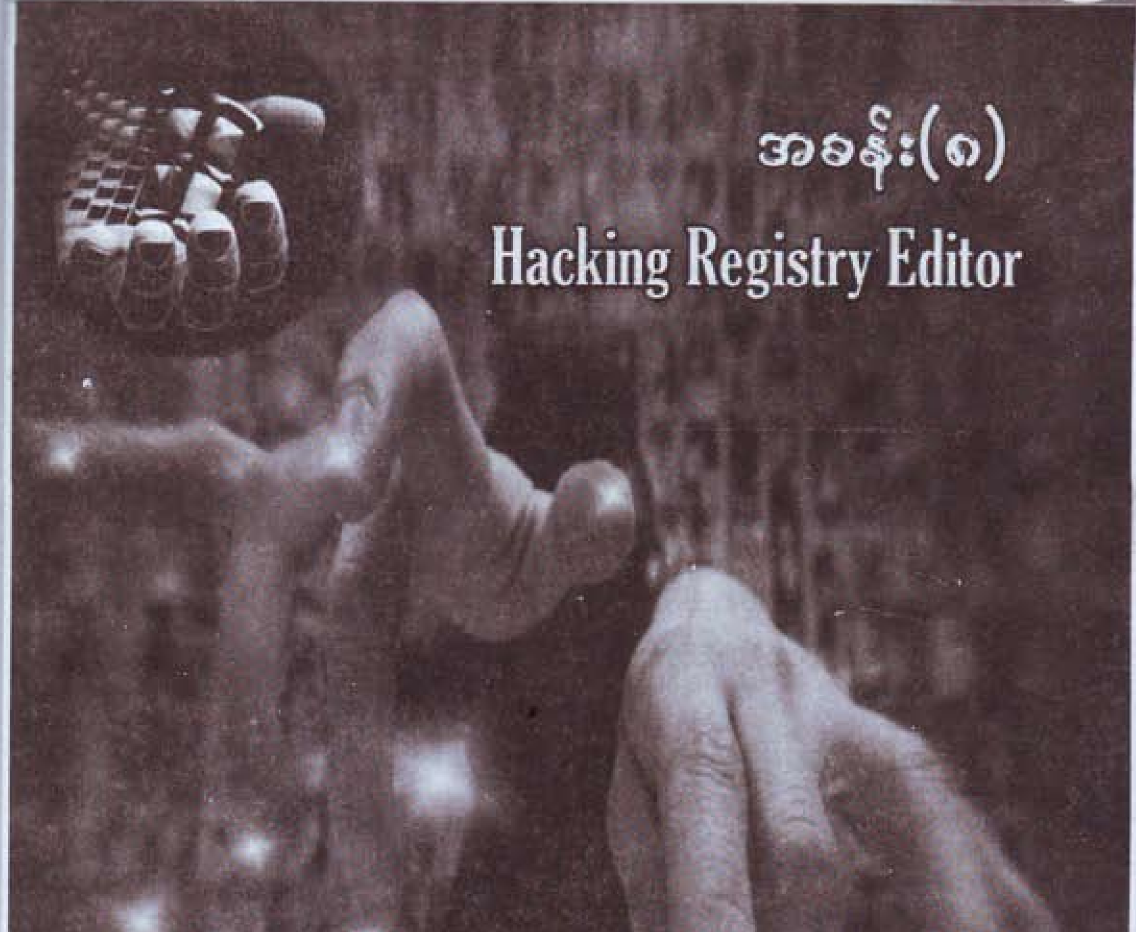
အထက်ပါအတိုင်းအဆင့်ဆင့်ဝင်ရောက်ပြီး Control Panel ၏ညာဘက်ရှိ Option အောက်တွင် Prohibit access to the Control Panel ကိုကလစ်နှစ်ချက်နှိပ်ပြီးEnable ကိုရွေးပါ။

Start Menu တွင် Control Panel Icon ကိုမတွေ့ရတော့ပါဘူး။ ပြန်ဖွင့်စေလိုလျှင် အထက်ပါအတိုင်းဝင်ရောက်ပြီး Not Configured ကိုပြန်နှိပ်လိုက်လျှင်ရပါပြီ။



အခန်း(၈)

Hacking Registry Editor



goldenshadetech@gmail.com

http://thanhtikegs.weebly.com

Hacker လက်သုံး Registry အကြောင်းကိုအတွင်းကျကျလေ့လာခြင်း

မကောင်းမှုပြုသော Hacker ဖြစ်ဖြစ်၊ ကောင်းတာပြုသော Hacker ဖြစ်ဖြစ် Registry များ အကြောင်းကိုအတွင်းကျကျသိထား၊ တတ်ထားရပါမယ်။ မဖြစ်မနေကို သိသင့်တတ်သင့်ပါတယ်။

ကွန်ပျူတာပညာရပ်ဆိုင်ရာများကို ပညာရှင်တစ်ဦးကဲ့သို့ကျွမ်းကျင်ရန် ကြိုးစားနေသော မည်သူမဆို Registry အသုံးပြုထိန်းချုပ်ပုံတွေကို သိထားမှသာ မိမိဆန္ဒအလျှောက်ထိန်းကြောင်း၊ ထိန်းချုပ်နိုင်မှာပါ။

ဥပမာဆိုရသော် မိမိကွန်ပျူတာကို၊ ဒါမှမဟုတ် မိမိတာဝန်ယူထားရသောကွန်ပျူတာကို လုံခြုံရေးစနစ်ပြည့်ဝစေရန် အတားအဆီးများ၊ အပိတ်အဆို့များပြုထားလိုတဲ့အခါအသုံးတည့်သလို၊ မိမိလက်ဝယ် ပြင်ဆင်ရန်ရောက်လာတဲ့ကွန်ပျူတာရဲ့ ပိတ်ဆို့တားဆီးမှုတွေကို ထိုးဖောက်နိုင်ဖို့အတွက် Registry ဟာအဓိကကျနေပါတယ်။

Windows System ရဲ့ စနစ်ပိုင်းဆိုင်ရာရပ်တည်မှုတွေဟာ Registry ပေါ်မှာမူတည်နေပါတယ်။ စနစ်ပိုင်းဆိုင်ရာ Software, Hardware တွေရဲ့ပြောင်းလဲမှုတိုင်းကို မှတ်တမ်းတင်ထားရှိတာ Registry ပဲဖြစ်ပါတယ်။

ဒါ့အပြင် System File တွေကိုလည်း အကျိုးသက်ရောက်ထိန်းချုပ်ထားပါတယ်။ ဥပမာ– Windows စတင်ရန်အရေးပါ ဖိုင်တစ်ခုဖြစ်တဲ့ NTLDR ဟာ Registry နဲ့အပြန်အလှန်အကျိုးသက်ရောက်စေပါတယ်။

အင်တာနက်ဆိုင်များ၊ သင်တန်းများနှင့် အများကိုပေးသုံးထားသော ကွန်ပျူတာများဆိုလျှင် အများအားဖြင့် Run Box, Control Panel, Shoutdown Button, Restart Button , Registry, Task Manager များကိုပိတ်ထားဖို့လိုအပ်တာကြောင့် အများစုက ပိတ်ထားကြပါတယ်။ အကြောင်းသင့်လို့ ပြန်ဖွင့်လိုတဲ့အခါမှာ ယခင်ပိတ်ထားသူမရှိတော့လို့ စာဖတ်သူလက်ထဲရောက်လာခဲ့လျှင် Honest Hacker တစ်ယောက်အတွက်အသုံးဝင်ဖို့ နည်းလမ်းတွေဖြစ်လာမှာပါ။

အရေးကြီးဆုံးကတော့ Registry ကို Backup ဦးစွာပြုလုပ်ထားပါ။ အကြောင်းပေါင်းမသင့်လျှင် စာဖတ်သူရဲ့လက်ချက်ကြောင့် Windows ပြန်တက်မလာသည်အထိဖြစ်လာနိုင်ပါတယ်။

ဒါ့အပြင်စာဖတ်သူလက်တည့်စမ်းသမျှကို မှတ်စုတစ်အုပ်မဖြစ်မနေထားရှိပါ။ Hacker တွေရဲ့အသက်ဟာ မှတ်စုဖြစ်နေတယ်ဆိုတာ တစ်ချိန်ချိန်မှာသိလာပါလိမ့်မယ်။

Registry Backup ဦးစွာပြုလုပ်ထားခြင်း(ပထမနည်းလမ်း)

အောက်ပါအဆင့်တွေအတိုင်း Registry ကို Backup လုပ်ထားပါ။ သို့သော်လည်း Registry လုပ်ဆောင်ခွင့်ပိတ်ထားတဲ့အခါမှာတော့ Registry ကိုဦးစွာပြန်ဖွင့်ဖို့လိုပါတယ်။ Registry ကိုပြန်ဖွင့်မယ့် Group Policy ကိုပါပိတ်ထားခဲ့လျှင်သုံးနိုင်ဖို့ Script Program တစ်ပုဒ်ကိုပါ နောက်ပိုင်းမှာအသေးစိတ်ဖော်ပြထားပါတယ်။

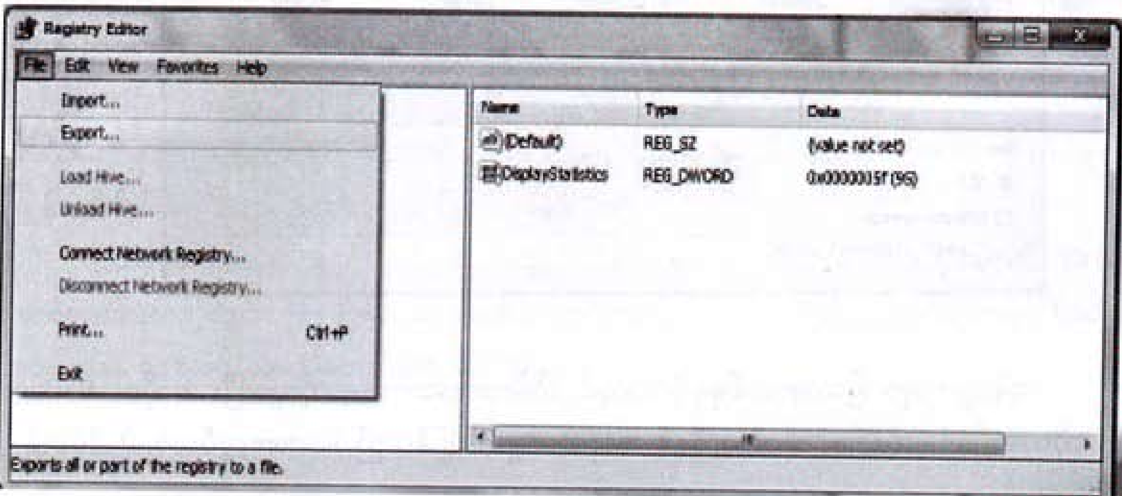
ဟုတ်ပါပြီ။ Registry ကိုဖွင့်သုံးနိုင်သည့်အခြေအနေကိုရောက်ရှိနေပြီလို့မှတ်ထားပြီး အောက်ပါအဆင့်တွေကို ပြုလုပ်ပါ။ နည်းလမ်းနှစ်မျိုးရှိလို့ နှစ်မျိုးလုံးကိုဖော်ပြပေးလိုက်ပါတယ်။ ဆန္ဒရှိလျှင် နှစ်မျိုးလုံးပြုလုပ်ထားနိုင်ပါတယ်။

တစ်ချိန်ချိန်မှာ Registry ကြောင့် Windows တက်မလာတဲ့အခါ ပြန်လည် Registry Restore လုပ်နိုင်ပါတယ်။ Registry Restore ပြန်လည်ပြုလုပ်ခြင်း ကိုနောက်ပိုင်းမှာ ဆက်လက်ရှင်းပြထားပါတယ်။

တစ်ခုသတိထားရမှာကတော့ Registry Backup File ကို Windows မသွင်းထားသော Harddisk Drive တစ်ခုခုမှာသိမ်းသင့်ပါတယ်။ ဥပမာ Drive D:\, E:\, F:\ မှာပေါ့။

၁- Registry ကိုဝင်ရန် Run Box ကိုဖွင့်ပြီး Regedit လို့ရိုက်ပါ။ Enter ကိုနှိပ်ပါ။ အောက်ပါပုံအတိုင်း Registry Editor ပွင့်လာပါလိမ့်မယ်။

၂- File Menu ကိုဝင်ပြီး Export ရွေးချယ်နှိပ်လိုက်ပါ။

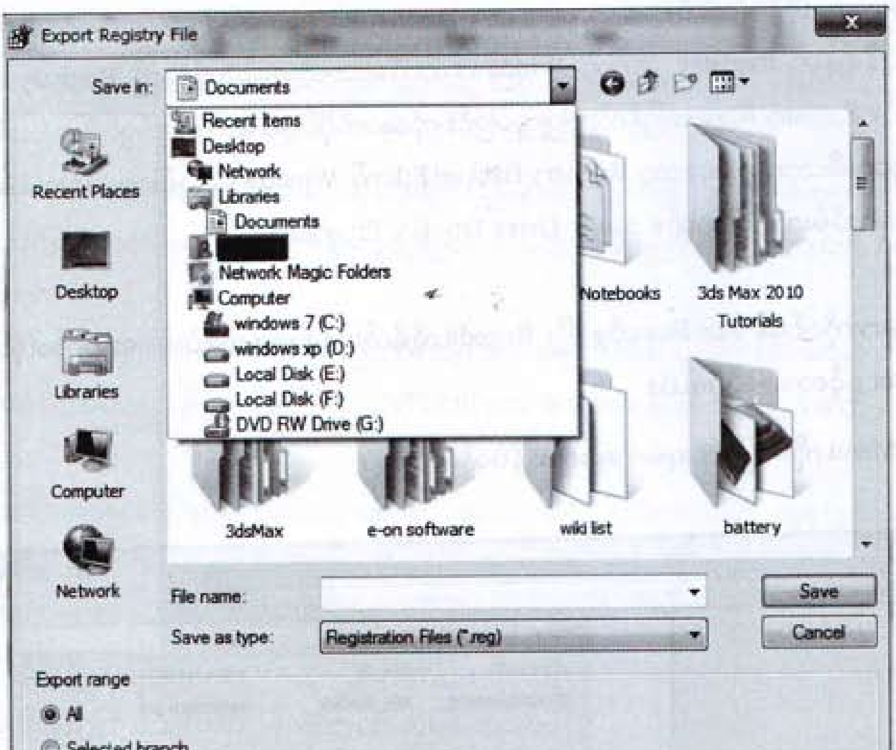


၃- Save In Choose Box မှတစ်ဆင့် သိမ်းထားလိုသောနေရာကိုသွားရောက်ပါ။

၄- File Name Box မှာ စိတ်ကြိုက်အမည်တစ်ခုပေးပါ။ Save As Type Box မှာ Registration File (*.reg) ကိုရွေးရပါမယ်။ အများအားဖြင့် အလိုအလျောက်ပေးထားတတ်ပါတယ်။

၅- အောက်ဖက်နားရှိ Export range မှာတော့ All ကိုသာရွေးပေးလိုက်ပါ။ (တစ်ခါတရံ Error တက်နိုင်ပါတယ်။ ထိုအခါ နောက်တစ်နည်းကိုသုံးပါ)

၆- Save Button ကိုနှိပ်လိုက်ပါ။ Backup အသင့်ပြုလုပ်သွားပါလိမ့်မယ်။



ကွန်ပျူတာမှာ ပြဿနာတစ်ခုခုရှိလာလျှင် သိမ်းထားသောနေရာကိုသွားပြီး အဆိုပါ Backup File ကိုကလစ်နှစ်ချက်နှိပ်ဖွင့်လိုက်သည်နှင့် အလိုအလျောက် ပြန်လည် Restore လုပ်သွားပါလိမ့်မယ်။

Registry Backup ပြုလုပ်ခြင်း(ဒုတိယနည်းလမ်း)

ယခုနည်းလမ်းကို လူသိပိုများပြီး အသုံးပိုဝင်ပါတယ်။ စာရေးသူရဲ့ သင်တန်းတွေမှာ အမြဲသင်ပေးနေတဲ့ နည်းလမ်းဖြစ်ပါတယ်။ Windows မတက်နိုင် ဖြစ်နေတဲ့အခါတွေမှာ အခြားကွန်ပျူတာတစ်လုံးကို အကူအညီယူပြီး ပြန်လည် Restore လုပ်နိုင်တဲ့ နည်းလမ်းဖြစ်ပါတယ်။

ဤနည်းလမ်းကိုအသုံးပြုနိုင်ဖို့ စာဖတ်သူဟာ ကွန်ပျူတာစက်ပြင်အခြေခံရှိနေလျှင် ပိုသင့်တော်ပါတယ်။ ဘာ့ကြောင့်လဲဆိုတော့ အခြားကွန်ပျူတာတစ်လုံးမှာ Harddisk ကို တပ်ဆင်တဲ့အခါမှာ ဒုတိယအဆင့် Extended (Slave) အဖြစ်သာတပ်နိုင်ပါတယ်။ Windows OS ရှိနေရမည့် ပထမမူရင်း Harddisk ဟာ Primary (Master) ဖြစ်နေတဲ့အတွက်ကြောင့်ဖြစ်ပါတယ်။

IDE Harddisk ရဲ့နောက်ဖက်မှာ အဆိုပါပြုလုပ်ချက်အတွက် Jumper လို့ခေါ်သော ပြောင်းလဲနိုင်တဲ့နေရာရှိပါတယ်။ ဒါပေမယ့် ယခုနောက်ပိုင်းထွက် SATA Harddisk တွေမှာတော့ အထက်ပါပြဿနာဖြစ်စရာမလိုတော့ပါ။ အလိုအလျောက်သိတဲ့စနစ်ပါရှိထားပါတယ်။

လက်ရှိကွန်ပျူတာမှ Drive Name တွေရဲ့နောက်မှာဆက်လက်ပြီးအမည်သစ်နဲ့ရှိလာပါလိမ့်မယ်။ ဥပမာ– Drive Name C, D, E ရှိပြီးသားဖြစ်လျှင် F(Windows OS), G, H လို့တက်လာပါလိမ့်မယ်။ ထိုအခါ ရှိနေတဲ့ ကိုဖွင့်ပြီးအောက်ဖော်ပြပါနည်းလမ်းတွေအတိုင်းအလွယ်တကူပြုလုပ်လိုက်လျှင် စနစ်ပြန်ကောင်းပါလိမ့်မယ်။

စာဖတ်သူသတိထားရမည်ကတော့ ဖော်ပြပါအတိုင်းပြန်လည်ကယ်ဆယ်ပေမယ့်လည်း Windows တက်မလာလျှင် အခြားဖြစ်နိုင်ခြေနည်းလမ်းများကိုရှာဖွေစဉ်းစားပါ။ လိုအပ်လျှင် တတ်ကျွမ်းသူ ပညာရှင်များထံမှာ အကူအညီတောင်းယူပါ။

ယခုနောက်ပိုင်းထုတ် Virus တွေဟာ System File တွေကိုဖျက်ထုတ်လိုက်တာကြောင့် Registry နှင့်မသက်ဆိုင်ပါ။ ထိုအခါမှာတော့ နောက်ဆုံးနည်းလမ်းအဖြစ် Windows တစ်ခုလုံး ပြန်သွင်းခြင်းသည်သာ အကောင်းဆုံးဖြစ်ပါလိမ့်မယ်။

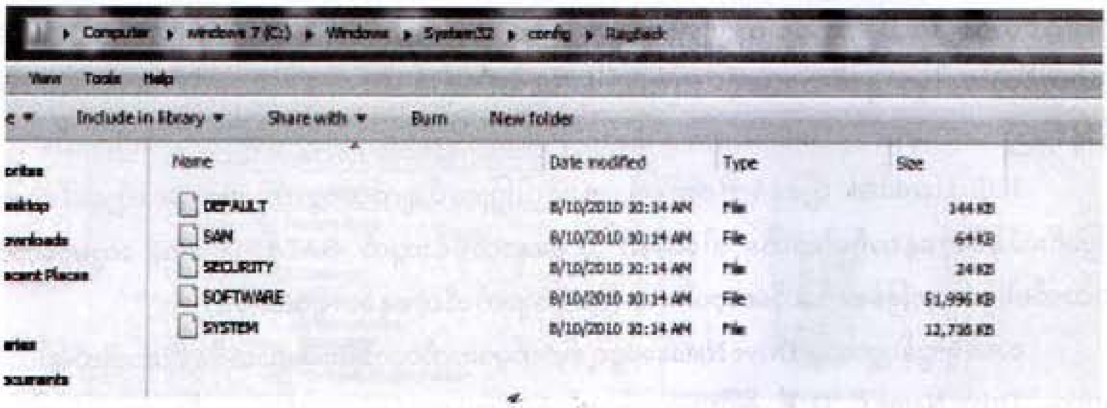
ယခုဖော်ပြမည့် နည်းလမ်းကိုသုံးလျှင် Software Install တစ်ခု၊ ဒါမှမဟုတ် Driver တစ်ခုထပ်မံထည့်သွင်းတိုင်း ပြန်လည် Backup လုပ်ပေးရပါမယ်။ အသုံးပြုရလွယ်ကူစေရန် Backup လုပ်သော နေ့စွဲဖြင့် အမည်ပေးသိမ်းသင့်ပါတယ်။

၁- Registry Control File ရှိတဲ့နေရာကိုသွားရပါမယ်။

Windows XP- C:\Windows\System32\Repair\Config Folder

Windows Vista & 7 - C:\Windows\System32\Config\Regback Folder

၂- အဆိုပါ Folder အတွင်းတွင် အောက်ပါ ဖိုင်၅ဖိုင်ကိုရှာဖွေရပါမယ်။ အများအားဖြင့် အဆိုပါ ဖိုင်၅ဖိုင်သာရှိနေတတ်ပါတယ်။



၃- အဆိုပါ File ၅ခုစလုံးကို Copy ကူးယူပါ။ အခြားသင့်လျော်ရာနေရာတစ်ခုမှာ လက်ရှိနေ့စွဲ တပ်ပြီး Folder ဖွဲ့ကာထည့်သွင်းထားပါ။

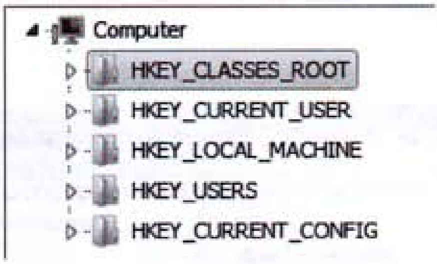
စာရေးသူ ရှေ့တွင်ပြောခဲ့သလိုပါပဲ လိုအပ်လာတဲ့အချိန်ကြလျှင် အဆိုပါ Backup လုပ်ထားတဲ့ ဖိုင်၅ဖိုင်ကို အထက်ပါနေရာများအတိုင်းပြန်လည်ထည့်သွင်းလိုက်ပါ။

ထည့်သွင်းတဲ့အခါမှာလည်း မူလမကောင်းတော့တဲ့ ဖိုင်၅ဖိုင်ကိုဖျက်ပြီးမှထည့်လျှင် ပိုကောင်းပါတယ်။ Replace ဖြင့်ထည့်လျှင်လည်းရပါတယ်။

Registry ဆိုတာ ကွန်ပျူတာရဲ့အသက်ပါပဲ။ အမြဲတောင့်တင်းသန်မာနေဖို့ လိုအပ်ပါတယ်။ ဒါ့ကြောင့် သန့်ရှင်းရေးပုံမှန်ပြုလုပ်ပေးသင့်ပါတယ်။ နောက်ပိုင်းတွင် Registry ကိုကျန်းမာ ကြံ့ခိုင်အောင်ပြုလုပ်ပေးသော Registry Easy Program ကိုထည့်သွင်းနည်း၊ အသုံးပြုနည်းတွေကိုပါ ထည့်ပေးလိုက်ပါတယ်။

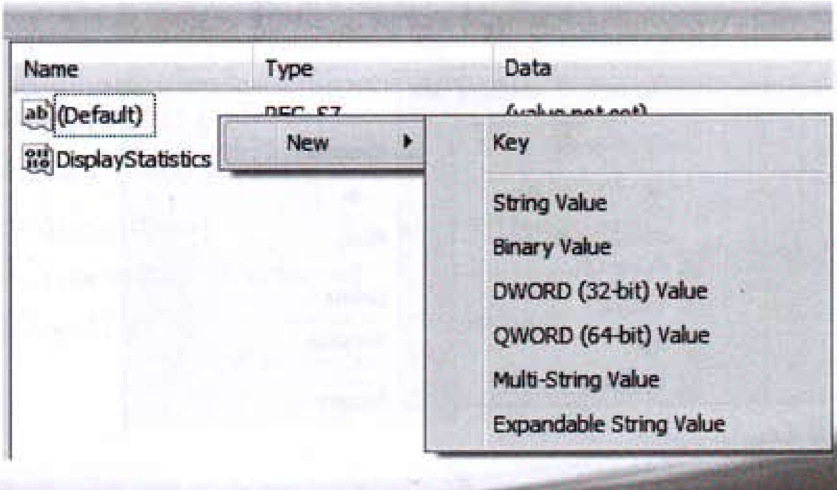
Registry Editor အတွင်းပိုင်းတည်ဆောက်ပုံကိုလေ့လာခြင်း

Registry Editor ကိုလုပ်ငန်းစဥ်ငါးရပ်ခွဲပြီးဖွဲ့စည်းထားပါတယ်။ လုပ်ငန်းစဥ်တိုင်းတွင် အဆင့်မြင့်လုပ်ဆောင်ချက်များပါရှိပါတယ်။ အဓိကကတော့ သိမ်းထားရမည့် System ဆိုင်ရာမှတ်တမ်းများပါရှိပါတယ်။



လုပ်ဆောင်ချက်များအတွက်မှားယွင်းမှုကိုလက်မခံပါ။ Registry ကိုအသေးစိတ်ပြင်ဆင်ရန်လိုအပ်သလို သက်ဆိုင်ရာလမ်းကြောင်းတွေမှာပဲ အကျိုးသက်ရောက်စေပါတယ်။ အဓိကထိန်းချုပ်စနစ်ကို **0 or 1** ဖြင့်ခိုင်းစေထားပါတယ်။ **0** ဟာပုံမှန်အသုံးဖြစ်ပြီး၊ **1** ကိုတော့ပြင်ဆင်ပြောင်းလဲမှုအတွက်သုံးပါတယ်။ ဒီထက်ရှင်းအောင်ပြောရလျှင် **0** ကို **Yes, Enable, Default, Show** အဖြစ်သုံးပြီး၊ **1** ကို **No, Disable, Change(Remove), Hide** အဖြစ်သတ်မှတ်ပါတယ်။ Registry ကတော့ Value အဖြစ်နားလည်ထားပါတယ်။ သုံးစွဲသည့်ခိုင်းစေချက်ပေါ်မူတည်ပြီးပြောင်းလဲနိုင်ပါတယ်။

စာဖတ်သူများအနေဖြင့်နောက်တစ်ချက်သိထားသင့်သည်ကတော့ ထည့်သွင်းအချက်အလက်တွေကို ထိန်းချုပ်ပေးတဲ့ Data Type ပဲဖြစ်ပါတယ်။ အောက်မှပုံစံကတော့ Windows 7 ရဲ့ Data Type တွေပဲဖြစ်ပါတယ်။ လက်တွေ့အသုံးများကိုတော့ နောက်ပိုင်းမှာဆက်လက်လေ့လာသွားပါ။

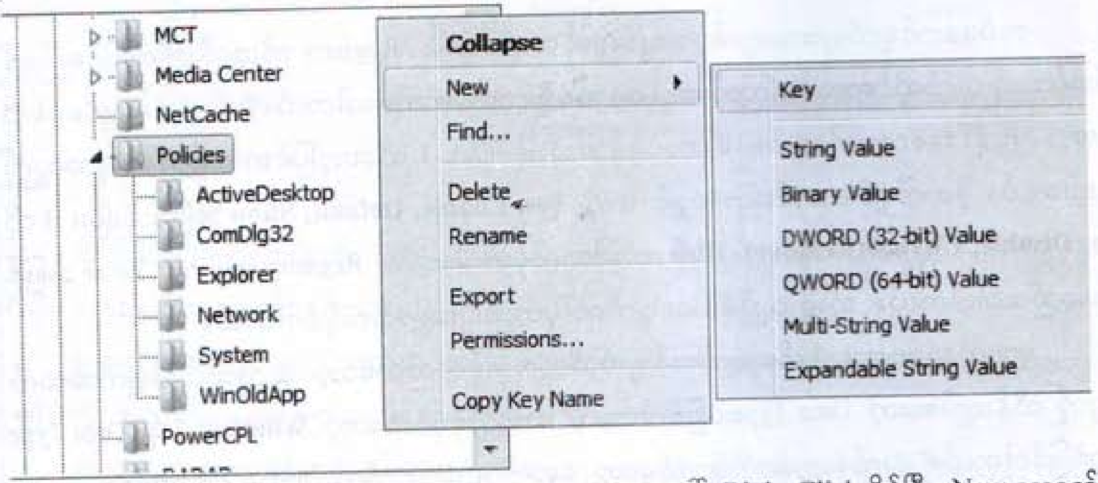


Registry Editor အသုံးပြုနည်း

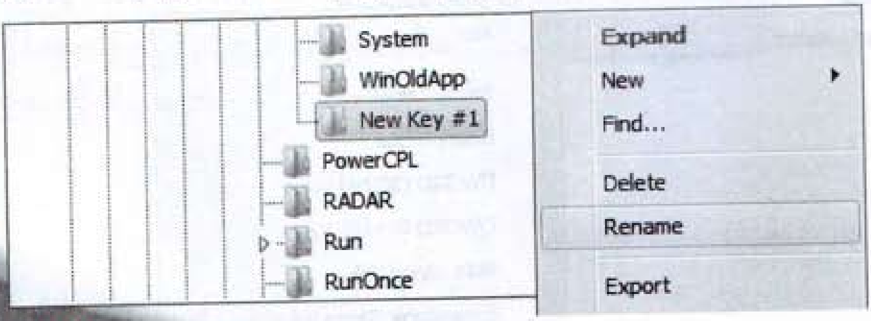
Registry Editor ကိုအသုံးပြုတဲ့အခါ ညွှန်ကြားချက်အတိုင်းလုပ်ဆောင်ရာတွင် အသုံးပြုဖိုင်အမည်နှင့် အချက်အလက်များရှိနေလျှင်အကြောင်းမဟုတ်သော်လည်း မရှိခဲ့သော်ဖြည့်သွင်းတတ်ဖို့လိုပါတယ်။

SubKey အသစ်ထည့်သွင်းရန်

ညွှန်ကြားချက်အတိုင်းအဆင့်လိုက်ဝင်ရောက်သွားသော်လည်း တစ်ခါတရံမှာတော့ အသင့်မပါရှိတဲ့အတွက် ကိုယ်တိုင်တည်ဆောက်ပေးရတတ်ပါတယ်။ အောက်ပါအတိုင်းတည်ဆောက်ရပါမယ်။

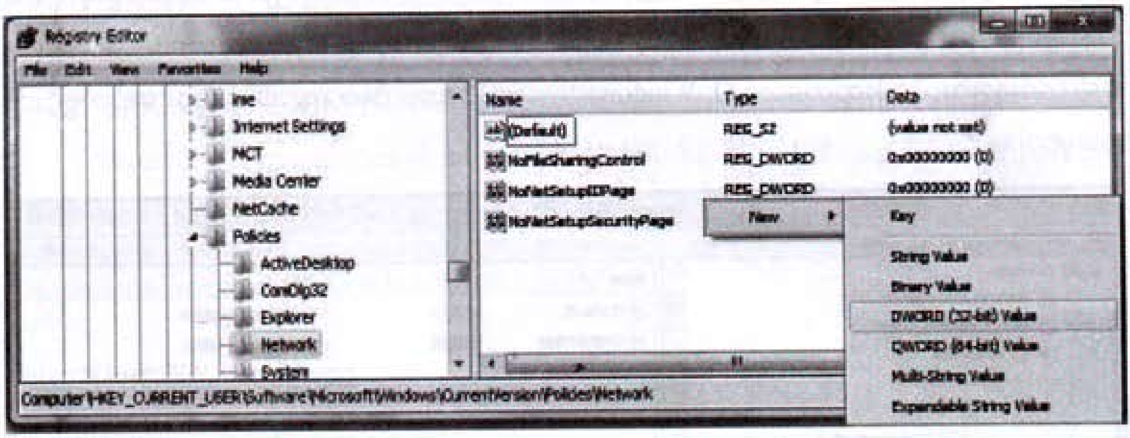


ထည့်သွင်းလိုသော Master SubKey(eg; Policies) ပေါ် Right Click နှိပ်ပြီး New အောက်မှ Key ကိုရွေးနှိပ်လိုက်ပါ။ အောက်ပါအတိုင်း New Key #1 အမည်ဖြင့် SubKey အသစ်ရောက်လာပါပြီ။ Right Click နှိပ်ပြီး Rename ကိုရွေးကာ ညွှန်ကြားချက်အတိုင်းအမည်တစ်ခုပေးရပါမယ်။



ValueName အသစ်ထည့်သွင်းရန်

ValueName ကတော့ ကိုယ်တိုင်တည်ဆောက်ပေးရတာများပါတယ်။ Registry Editor ရဲ့ ညာဘက်ခြမ်းမှာတည်ဆောက်ရမှာပါ။ ညွှန်ကြားချက်သည် ValueName အမည်များကိုစနစ်တကျ သတ်မှတ်ချက်အတိုင်း ပေးထားတာဖြစ်ပါတယ်။ စာလုံးအကြီးအသေးကအစ၊ Space မခြားထားတာတွေကိုပါဂရုပြုပါ။



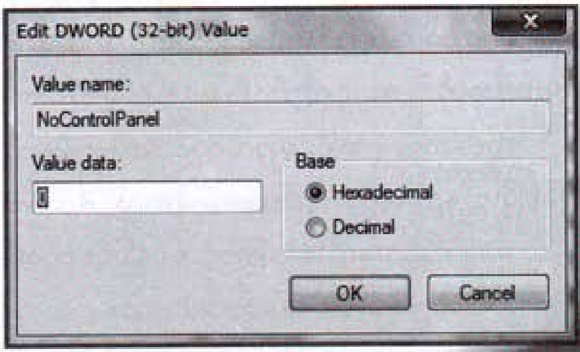
အများဆုံးသုံးတာကတော့ DWORD Value(REG_DWORD) နှင့် String Value(REG_SZ) တို့ပဲဖြစ်ပါတယ်။ တစ်ခါတရံ Binary Value(REG_BINARY)ကိုသုံးတာလည်းရှိပါတယ်။

ညာဘက်မျက်နှာစာပေါ် Right Click နှိပ်ပြီး New အတွင်းမှညွှန်ကြားချက်အတိုင်း Value အသစ်တစ်ခုထည့်သွင်းပေးပါ။ အသစ်ရလာတဲ့ Value Name ကို ညွှန်ကြားထားတဲ့အမည် ပြောင်းပေးလိုက်ပါ။

ValueData ဖြည့်သွင်းရန်

ValueData ကိုတော့အများအားဖြင့် 0 or 1 သာအသုံးများပါတယ်။

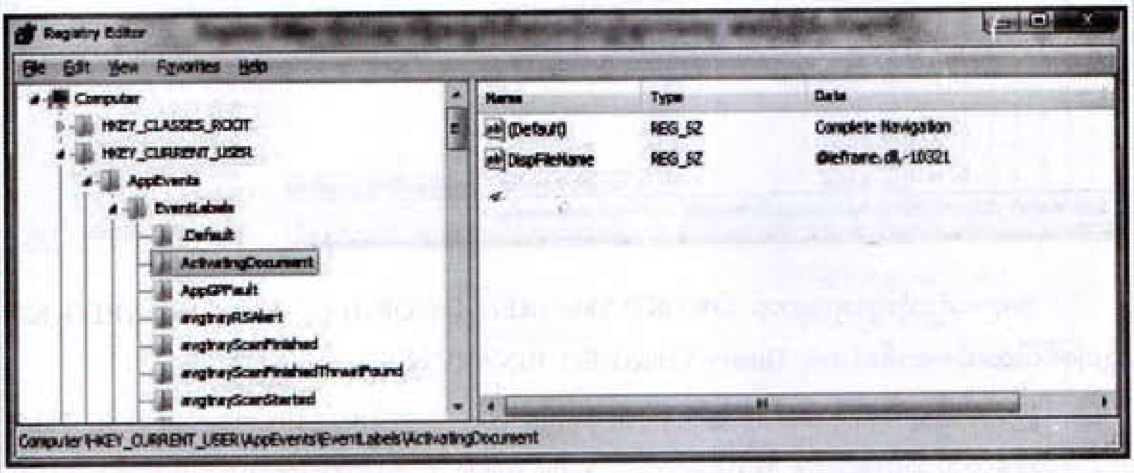
Base Type မှာတော့ Hexadecimal ကိုသာရွေးရပါတယ်။



Registry Editor ဝင်ရောက်ဖို့ရာ

Registry Editor ကိုဝင်ရောက်ဖို့အတွက်သိထားသင့်သည်များကတော့ အဆင့်လိုက်ဝင်ရောက်ခြင်းနှင့် ထည့်သွင်းညွှန်ကြားချက်မှန်ကန်ခြင်းပဲဖြစ်ပါတယ်။ Registry Editor ကိုဖွင့်ဖို့ နည်းလမ်းနှစ်ခုကတော့ Run Box မှ regedit ထည့်သွင်းဖွင့်ခြင်းနှင့် C:\Windows\System32\ regedt32 ကိုသွားရောက်ဖွင့်ခြင်းတို့ ဖြစ်ပါတယ်။

အချို့ကွန်ပျူတာတွေဟာ Run Box ကိုပိတ်ထားတတ်ပါတယ်။ ဒါဆိုလျှင် သာမန်သုံးစွဲသူတို့ဟာ ထိန်းချုပ်ခြင်းပြုလုပ်နိုင်တဲ့ Run Box မရှိတဲ့အတွက် Registry ကိုသုံးနိုင်မှာမဟုတ်ပေမယ့် System အကြောင်းနားလည်သူတွေကတော့ C:\Windows\System32 အောက်မှာ regedt32 ကိုဝင်ရောက်ဖွင့်သုံးသွားမှာပါ။



အထက်မှပုံကိုကြည့်ကြည့်ပါ။ HKEY_CURRENT_USER အောက်ကိုအဆင့်လိုက်ဝင်ရောက်သွားပုံကိုပြထားတာပါ။ ညာဘက်အခြမ်းမှာတော့ မျက်နှာစာပေါ် Right Click နှိပ်ပြီး စာဖတ်သူအနေဖြင့် ညွှန်ကြားချက်အတိုင်း ပြင်ဆင်ထည့်သွင်းနိုင်ပါတယ်။ နောက်ပိုင်းကဏ္ဍများကို လုပ်ဆောင်တဲ့အခါမှာ အထက်ပါအတိုင်းအဆင့်လိုက်ဝင်ရောက်နိုင်ဖို့လိုပါတယ်။

လုပ်ဆောင်ချက်ပြီးမြောက်လျှင် Restart ချဖို့လိုအပ်ပါတယ်။ Windows ပြန်တက် မလာခဲ့လျှင် ဖော်ပြခဲ့ပြီးတဲ့နည်းတွေအတိုင်းသာ ပြန်လည် Recovery ပြုလုပ်လိုက်ပါတော့။

စာမျက်နှာအခက်အခဲကြောင့်တစ်ခုခြင်း ဝင်ရောက်ပုံတွေကို မဖော်ပြတော့ပါ။ ဝင်ရောက်ရမယ့် လမ်းကြောင်းတွေကိုသာဖော်ပြလိုက်ပါတယ်။

Control Panel အသုံးပြုခွင့်ပိတ်ထားခြင်း

စာဖတ်သူအနေဖြင့် ကွန်ပျူတာရဲ့လုံခြုံရေးကောင်းမွန်စေရန် Control Panel ကိုအသုံးပြုခွင့်ပိတ်ထားလိုတဲ့အခါ အောက်ပါနည်းလမ်းများကိုပြုလုပ်ပါ။ User အပိုင်းနှင့် System အပိုင်းနှစ်နေရာမှာပြုလုပ်ရမှာဖြစ်ပါတယ်။

User Key:

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

SystemKey:

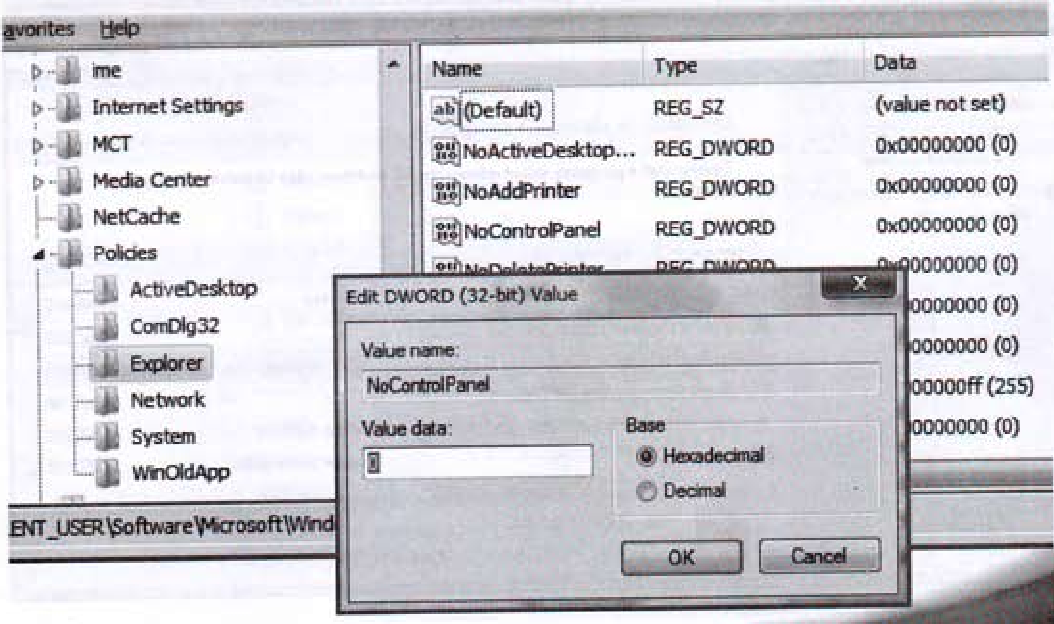
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

အမည်သတ်မှတ်ချက်ထားရန်အတွက် Explorer ကိုနှိပ်ပြီး၊ မြင်ရသောညာဘက်ခြမ်းတွင် NoControlPanel အမည်ပေးပြီးရှိလျှင် ၎င်းပေါ် Right Clic နှိပ်ကာ Modify ---ကိုရွေးပြီး တိုက်ရိုက်ပြင်ဆင်နိုင်ပါတယ်။ ပြန်သုံးလိုလျှင် အဆိုပါအတိုင်းဝင်ရောက်ပြီး Value = 0 ပြန်ပေးလျှင် ရပါပြီ။

Value Name: NoControlPanel

Data Type: REG_DWORD (DWORD Value)

Value Data: (0 = disable restriction, 1 = enable restriction)



Control Panel အတွင်းမှ Add Remove Program အသုံးပြုခွင့်ပိတ်ထားခြင်း

ယခုလုပ်ဆောင်ချက်ကတော့ Control Panel တစ်ခုလုံးကိုမပိတ်ထားလိုပဲ အခြားအသုံးပြုသူများမှ မိမိစက်အတွင်းမှ Program တွေကိုဖျက်ထုတ်ခြင်းမပြုနိုင်စေဖို့ Add Remove Program Setting ကိုပိတ်ထားနိုင်ပါတယ်။

User Key:

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Uninstall]

SystemKey:

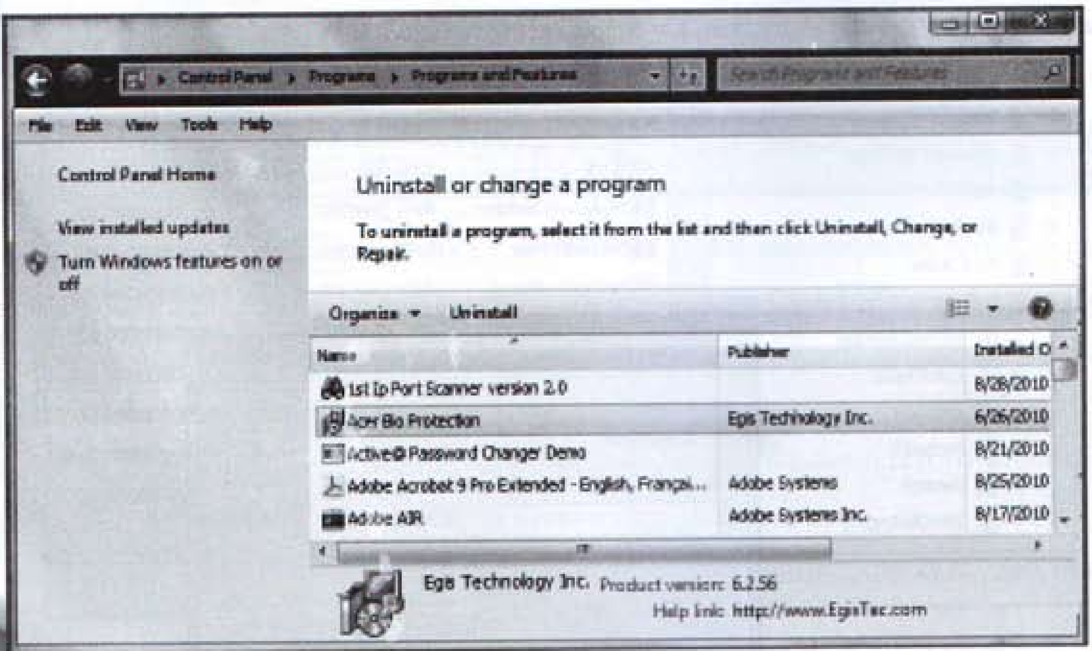
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Uninstall]

Policies အောက်မှာ SubKey Uninstall မရှိလျှင်အသစ်တည်ဆောက်ပါ။ Uninstall ကိုရွေးချယ်ထားစဉ် ညာဘက်တွင် Value ကိုထည့်သွင်းရမှာပါ။

Value Name: NoAddRemovePrograms

Data Type: REG_DWORD (DWORD Value)

Value Data: (0 = Default restriction, 1 = Lock restriction)



MyComputer Icon မြင်ကွင်းမှပျောက်ထားခြင်း

စာဖတ်သူဟာ ကွန်ပျူတာရဲ့မျက်နှာစာ Desktop ကိုပြင်ဆင်အသုံးပြုခွင့် ပိတ်ထားလိုတဲ့အခါ အောက်ပါနည်းလမ်းများကိုပြုလုပ်ပါ။ User အပိုင်းနှင့် System အပိုင်းနှစ်နေရာမှာပြုလုပ်ရမှာဖြစ်ပါတယ်။

User Key:

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\NonEnum]

SystemKey:

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\NonEnum]

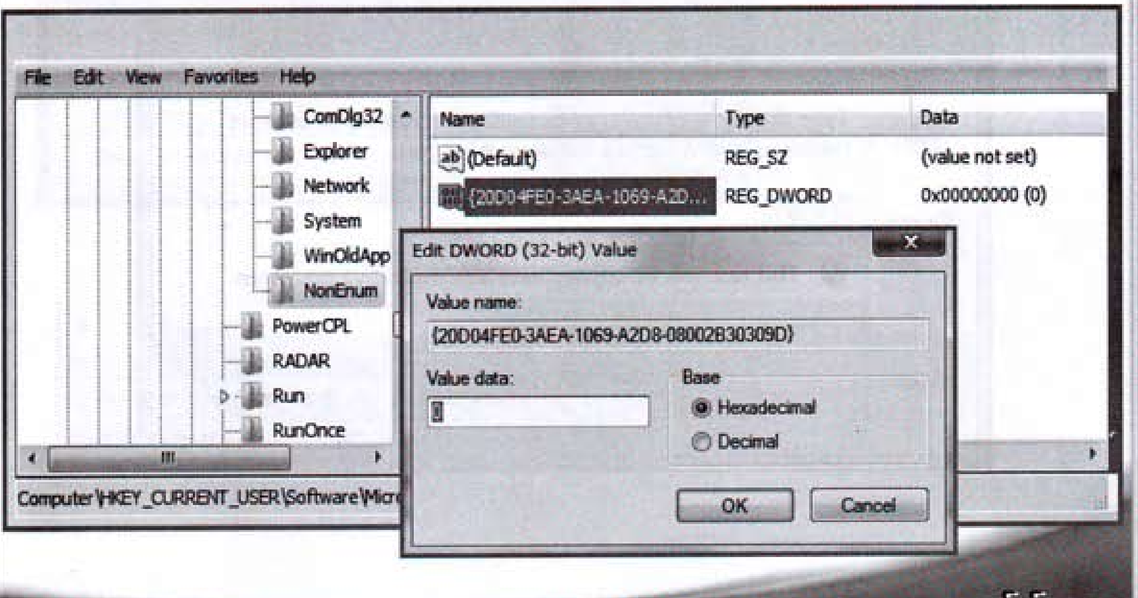
အထက်ပါနှစ်နေရာစလုံး Policies အောက်တွင် NonEnum ကိုမိမိဘာသာတည်ဆောက်ပေးရပါမယ်။ System ပိုင်းမှာတော့ အများအားဖြင့်တည်ဆောက်ပြီးအသင့်ရှိတတ်ပါတယ်။

ထည့်သွင်းရမယ့် Value Name ကိုအထူးဂရုစိုက်ဖြည့်သွင်းပါ။ System Key များဖြစ်နေလို့ပါ။ အခြားသတိထားရမှာကတော့ကဏန်း Zero (0) များသာပါရှိပါတယ်။ အက္ခရာအို (O) မပါပါဘူး။ ဒီ့အပြင် { } ကိုလည်းထည့်သွင်းရိုက်ရမှာဖြစ်ပါတယ်။

Value Name: {20D04FE0-3AEA-1069-A2D8-08002B30309D}

Data Type: REG_DWORD (DWORD Value)

Value Data: (0 = Show restriction, 1 = Hide restriction)



Run Box အသုံးပြုခွင့်ပိတ်ထားခြင်း

အန္တရာယ်သိပ်များတဲ့လုပ်ဆောင်ချက်ဖြစ်ပါတယ်။ Run Box ကိုပိတ်လိုက်တဲ့အတွက် Registry Editor ကို ရှေ့တွင်ဖော်ပြခဲ့သလို System32 အောက်မှသွားရောက်ဖွင့်လှစ်ပြင်ဆင်ရပါတော့မယ်။ Run Box ကိုပါပိတ်ထားလိုက်လျှင် ပြင်ဆင်ရဖို့အတွက် ဝင်ပေါက်မရှိတော့ပါဘူး။ ယခုစာအုပ်နှင့်တွဲပါရှိတဲ့ စီဒီထဲမှ Golden Gate Security Program ကိုစမ်းသပ်ပြီးမှသုံးစွဲသင့်ပါတယ်။

User Key:

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

SystemKey:

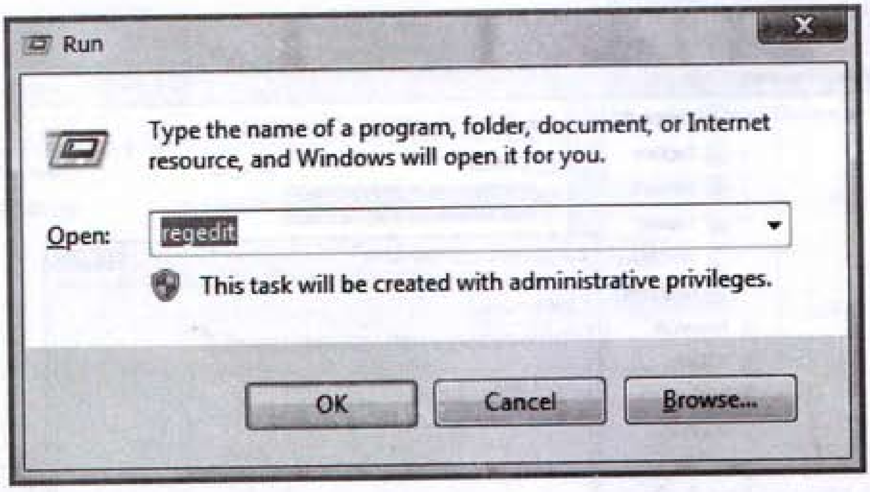
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Explorer အောက်မှာ Value Name = NoRun မရှိလျှင်အသစ်တည်ဆောက်ပါ။ Value Data တွင် 1 ထည့်လိုက်လျှင် Run Box ကိုပိတ်လိုက်ပါပြီ။ ပြန်ဖွင့်လိုလျှင် ထိုနေရာတွင် 0 ပြန်ထည့်ပြီး Restart ချလိုက်ပါ။

Value Name: NoRun

Data Type: REG_DWORD (DWORD Value)

Value Data: (0 = disable restriction, 1 = enable restriction)



ShutDown,Restart အသုံးပြုခွင့်ပိတ်ထားခြင်း

ယခုလုပ်ဆောင်ချက်ကတော့ Windows သုံးနေစဉ် Start ပေါ်ကနေ ကွန်ပျူတာကို ShutDown, Restart များပြုလုပ်ခွင့်မပြုစေချင်လျှင်သုံးတာပါ။ တစ်ခုတော့ရှိပါတယ်။ System Unit မှ Power Button, Restart Button တွေကိုတော့မသုံးနိုင်အောင်လုပ်ထားပေါ့နော်။

User Key:

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

SystemKey:

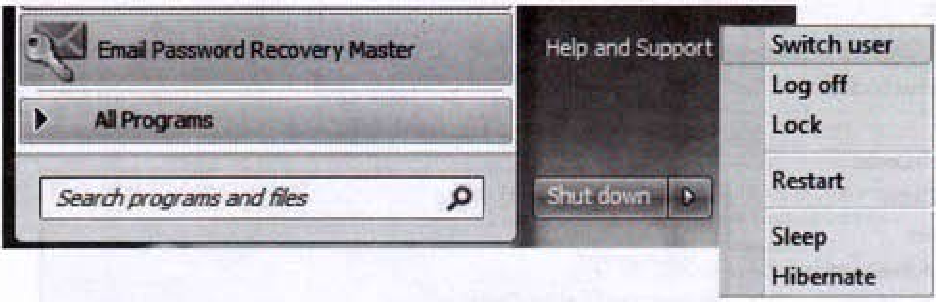
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Explorer အောက်မှာ Value Name = NoRun မရှိလျှင်အသစ်တည်ဆောက်ပါ။ Windows 7 တွင် System Key အတွက် Policies အောက်မှာ Explorer မရှိတဲ့အတွက် SubKey အသစ် ထည့်ပေးရပါမယ်။ အောက်ဖက်ဆုံးမှပုံကိုကြည့်ပါ။ Log Off, Swith user နှင့် Lock သာကျန်ပါတော့တယ်။

Value Name: NoClose

Data Type: REG_DWORD (DWORD Value)

Value Data: (0 = Default restriction, 1 = Hide restriction)



Desktop အသုံးပြုခွင့်ပိတ်ထားခြင်း

စာဖတ်သူဟာ ကွန်ပျူတာရဲ့မျက်နှာစာ Desktop ကိုပြင်ဆင်အသုံးပြုခွင့် ပိတ်ထားလိုတဲ့အခါ အောက်ပါနည်းလမ်းများကိုပြုလုပ်ပါ။ User အပိုင်းနှင့် System အပိုင်းနှစ်နေရာမှာပြုလုပ်ရမှာဖြစ်ပါတယ်။

User Key:

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

SystemKey:

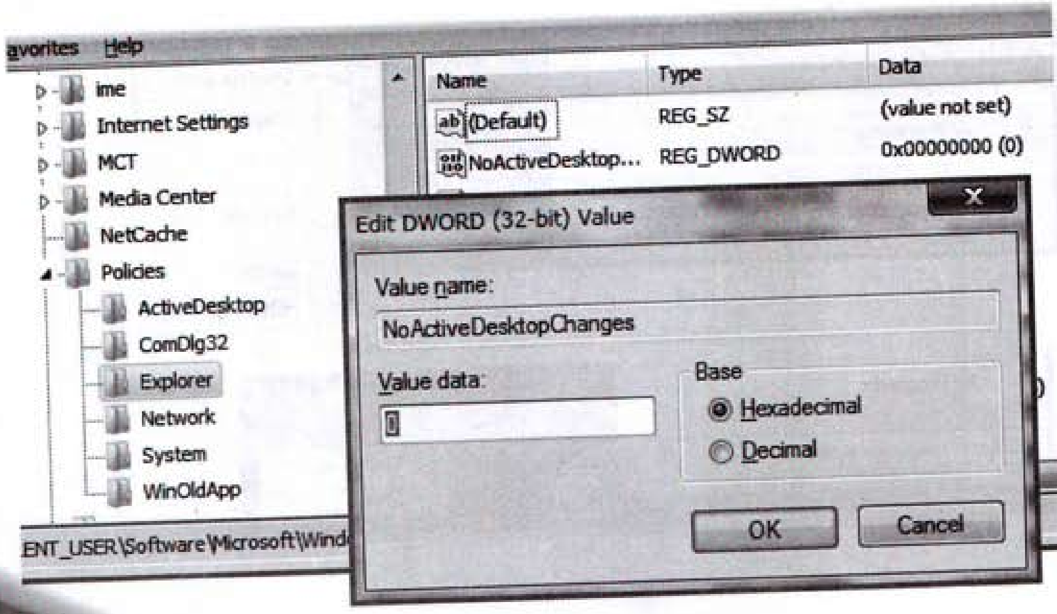
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

အမည်သတ်မှတ်ချက်ထားရန်အတွက် Explorer ကိုနှိပ်ပြီး၊ မြင်ရသောညာဘက်ခြမ်းတွင် NoActiveDesktopChanges လို့အမည်ပေးပြီးရှိလျှင် ၄င်းပေါ် Right Clic နှိပ်ကာ Modify ---ကိုရွေးပြီး Value Data 1 ထည့်ရပါမယ်။ System ပိုင်းမှာတော့ အမည်အသစ်ထည့်ဖို့လိုပါတယ်။ ပြန်သုံးလိုလျှင် အဆိုပါအတိုင်းဝင်ရောက်ပြီး Value = 0 ပြန်ပေးလျှင် ရပါပြီ။

Value Name: NoActiveDesktopChanges

Data Type: REG_DWORD (DWORD Value)

Value Data: (0 = disable restriction, 1 = enable restriction)



Processor(CPU) အမျိုးအစားကိုပြောင်းလဲတော်ပြခြင်း

စာဖတ်သူအနေဖြင့် ကွန်ပျူတာမှာတပ်ဆင်ထားတဲ့ Processor(CPU)ကိုကြည့်ရှုရန် My Computer-Right Click >Property မှကြည့်ကြပါတယ်။ အတွင်းတွင်ဖော်ပြထားတဲ့ Processor နေရာမှာ စာဖတ်သူစိတ်ကြိုက်ခပ်မြင့်မြင့်ကို စိတ်ရှုးပေါက်သလိုထည့်ထားနိုင်ပါတယ်။ အများအမြင်လန့်သွားသည်အထိ မဖြစ်နိုင်တာသာထည့်လိုက်ပေါ့။

SystemKey:

[HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTON\System\CentralProcessor\0]

ဒီတစ်ခါတော့ရှိပြီးသား Data တွေကိုပြန်ပြင်ရုံပါပဲ။ CentralProcessor အောက်မှာ 0 , 1 နှစ်ခုရှိပြီး နှစ်ခုစလုံးရဲ့ညာဘက်ခြမ်း ဖော်ပြချက်တွေဟာလည်း အများဆုံးတူညီနေပါတယ်။
စာဖတ်သူပြုပြင်ရမှာကတော့ ညာဘက်ခြမ်းမှ ProcessorNameString မှာဖြစ်ပါတယ်။ ကြိုက်တာသာထည့်လိုက်ပါ။

ဥပမာဆိုရလျှင် –GoldenShade[R]Nuclear[R] 6 CPU @ 9.99GHz

မူရင်းအတိုင်းပြန်လိုချင်တဲ့အခါ ပြန်သွင်းနိုင်အောင် မူရင်းစာတန်းကို တစ်နေရာရာမှာ ကူးရေးထားသင့်ပါတယ်။

Registry Editor အသုံးပြုခွင့်ပိတ်ထားခြင်း

စာဖတ်သူအနေဖြင့်ယခုအပိုင်းကို အရမ်းလိုအပ်မှသာပြုလုပ်သင့်ပါတယ်။ Registry Editor ကိုပိတ်ထားလျှင် ကွန်ပျူတာအတွက် အလုံခြုံဆုံးဖြစ်ပေမယ့် တစ်ချိန်ချိန်မှာ ပြင်ဆင်ရန်လိုအပ်လာလျှင် စာဖတ်သူကိုယ်တိုင်အသုံးပြုခွင့်ဆုံးရှုံးရပါမယ်။

ဒါ့ကြောင့် နောက်ကဏ္ဍမှာ Script Program အသေးလေးများရေးနိုင်းဖို့ ရှင်းပြထားပါတယ်။ စာဖတ်သူသတိထားရမှာကတော့ အလားတူ Script Program ရေးသားနိုင်သူတိုင်း ပြန်ဖွင့်နိုင်တယ်ဆိုတာကိုပါ။ ဟက်ကာတစ်ယောက်ဟာ ဘယ်လိုကာကွယ်ထားပါစေ ဘာကိုမဆို ထိုးဖောက်နိုင်ဖို့လိုပါတယ်။

User Key:

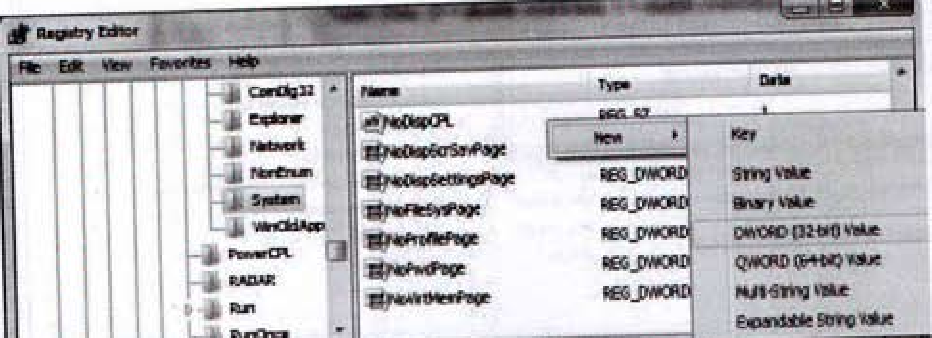
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]

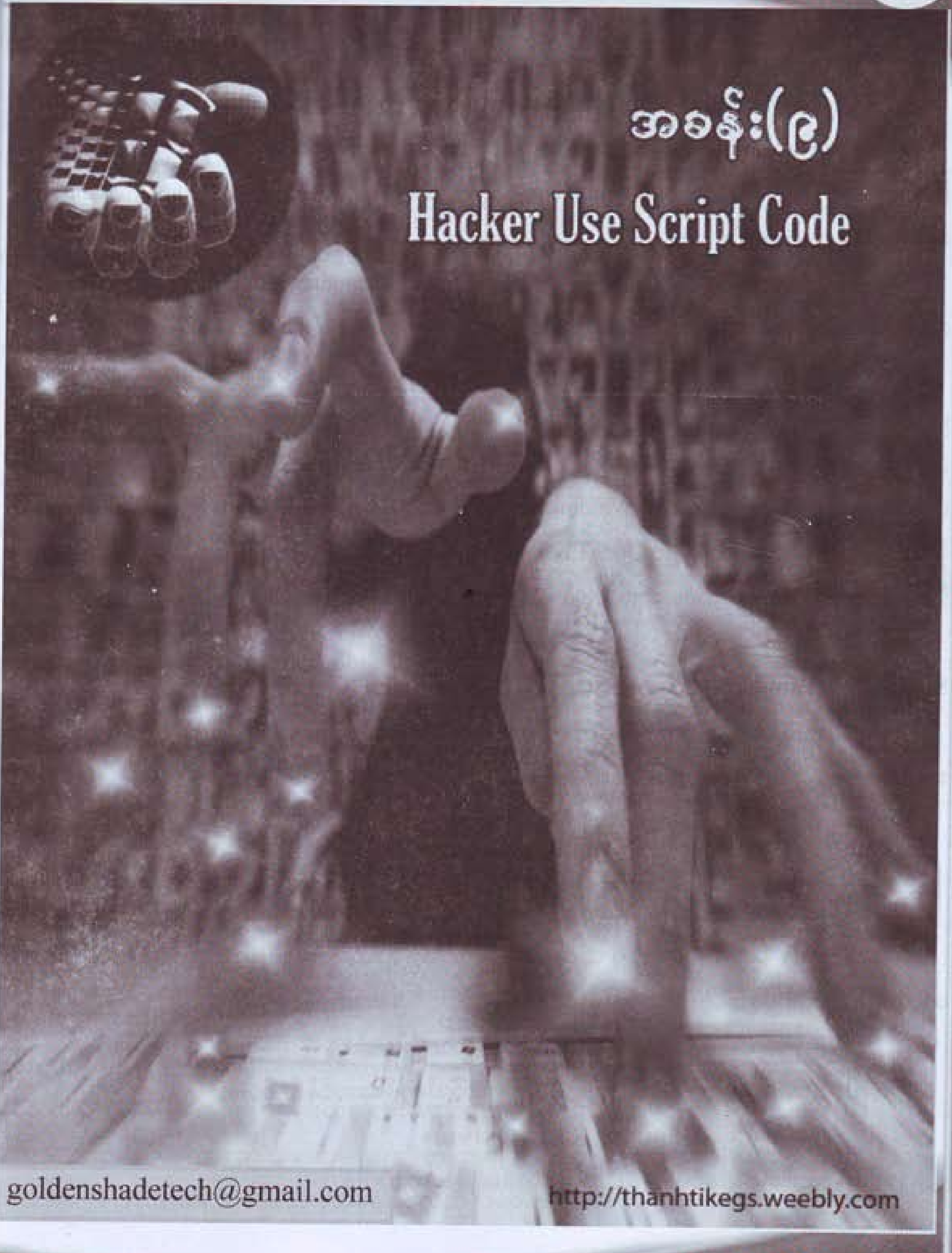
System အောက်မှာ Value ကို DisableRegistryTools အဖြစ်အသစ်ထပ်မံထည့်သွင်းရပါမယ်။ Value Data ကို 1 အဖြစ်ထည့်သွင်းပြီး Restart ပြန်လုပ်သည်နှင့် Registry Editor ကိုခေါ်ခွင့်မရတော့ပါဘူး။ ပြန်ခေါ်လိုလျှင် NotePad မှာ Script Program အဖြစ်ရေးပြီးပြန်ခေါ်ရပါမယ်။

Value Name: DisableRegistryTools

Data Type: REG_DWORD (DWORD Value)

Value Data: (0 = disable restriction, 1 = enable restriction)





အခန်း(၉)

Hacker Use Script Code

goldenshadetech@gmail.com

http://thanhtikegs.weebly.com

Script Program ဆိုသည်မှာ

(ကွန်ပျူတာရောဂါများနှင့် ကာကွယ်ဆေးစာအုပ်မှထုတ်နုတ်ချက်)

Script Program အသေးလေးတွေကို ကွန်ပျူတာအခြေခံသိရှိထားသူမည်သူမဆိုရေးသားအသုံးပြုနိုင်ပါတယ်။ Computer System Command တွေကို ကိုယ်တိုင်ရေးထားတဲ့ Script Program တွေနဲ့ ထိန်းချုပ်နိုင်ပါလိမ့်မယ်။

နည်းပညာလေ့လာနေသူများအတွက် Programming Language အခြေခံရစေပါတယ်။ အဓိက နောက်ခံထိန်းကျောင်းပေးထားတာကတော့ Command Prompt ပဲဖြစ်ပါတယ်။

Script ရေးသားနိုင်တဲ့ အသုံးချလမ်းကြောင်းနှစ်ခုရှိပါတယ်။ ပထမတစ်ခုကတော့ Notepad မှာရေးပြီး Command Prompt ကိုခိုင်းစေတာပါ။ ပုံမှန်ကွန်ပျူတာလုပ်ဆောင်ချက်ရှိနေစဉ်မှာ အသုံးပြုနိုင်ပါတယ်။ တစ်ခါတရံတော့ Windows ကြောင့်ပဲဖြစ်ဖြစ်၊ Virus ကိုက်လို့ပဲဖြစ်ဖြစ် Windows မတက်နိုင်တော့ပဲ Second Windows သေးသေးလေးဖြစ်တဲ့ Safe Mode ကနေခိုင်းစေရတာမျိုးရှိပါလိမ့်မယ်။ ဒါမှမဟုတ် Safe Mode Command Prompt ကနေခိုင်းရတာမျိုးလည်းရှိလာနိုင်ပါတယ်။ ဒီအခါလည်း Script Program ရေးလိုလျှင် DOS Code - "edit" Command ဖြင့်သုံးနိုင်ပါတယ်။

Script Program ရေးဖို့သိထားရမည့်လုပ်ငန်းစဉ်များ

သိထားဖို့လိုတာထက် သိမှကိုစာဖတ်သူကိုယ်တိုင်စီစဉ်ရေးဆွဲနိုင်မှာပါ။ သိထားသင့်တဲ့ အချက်တွေကို အသေးစိတ်ရှင်းပြလိုက်ပါတယ်။

၁။ မိမိခိုင်းစေလိုတဲ့ အချက်ကိုတိတိကျကျသိရပါမယ်။

၂။ တိကျတဲ့လမ်းညွှန်စေခိုင်းချက်ရှိရပါမယ်။

၃။ Registry ကိုပြင်ဆင်ဖို့ဆိုလျှင် တိကျတဲ့လမ်းကြောင်းဖော်ပြရပါမယ်။

Registry တွေကိုပြင်ဆင်ဖို့ဆိုတာအလွန်ပင်အန္တရာယ်များလှပါတယ်။ ပြုလုပ်လိုသည်ကို တိတိကျကျ ညွှန်ပြဖို့အထူးလိုအပ်ပါတယ်။

၄။ အသုံးပြုမယ့် Script Code ကိုသိထားရပါမယ်။

ဒါမှသာမိမိညွှန်ကြားမှုကို အပြည့်အဝနားလည်လုပ်ဆောင်နိုင်မှာပါ။

၅။ သိမ်းရမယ့်ဖိုင်ပုံစံကို သိထားရပါမယ်။

ပြန်လည်မောင်းနှင်တဲ့အခါ အခက်အခဲမရှိဖို့အတွက်ပါ။

Script Program အခြေခံ Code (Key Word) များ

Script တွေကိုလက်ခံရေးသားတဲ့ Program တွေဟာ တိုက်ရိုက်သုံး Programming Language Program တွေမဟုတ်တဲ့အတွက် Key Word တွေလည်းများများစားစား မရှိပါဘူး။

Script Program စခြင်းကို **@echo off** ဖြင့်စရပါတယ်။ ဒီလိုစတင်မှသာ Program ကို အသုံးပြုဖို့ ဖွင့်လိုက်လျှင် ရှင်းလင်းသောမြင်ကွင်းနဲ့စတင်လာမှာပါ။ သို့မဟုတ်လျှင် Command Prompt ပေါ်မှမြင်ကွင်းအတွင်း စာတွေရှုပ်နေအောင်မြင်ရတတ်ပါတယ်။

echo ကတော့ အခြား Programming Language တွေမှာသုံးသလို show, output နှင့်ဆင်တူပါတယ်။ ၄င်း **echo** နောက်မှာထည့်ထားတဲ့စာသားတွေကို အသုံးပြုသူအား မြင်တွေ့စေဖို့ သုံးရပါတယ်။ ဥပမာ– **echo** Choose the Shutdown?

echo. ကိုတော့ စာကြောင်းခြားလိုတဲ့အခါသုံးရတဲ့ Key Word ဖြစ်ပါတယ်။ နှစ်ကြောင်းခြား လိုလျှင် နှစ်ကြောင်းထည့်ပေးရပါတယ်။ ခြားလိုသလောက်ထည့်ပေးနိုင်ပါတယ်။ တစ်ခုတော့သတိ ထားပါ။ **echo** နောက်မှာ Full stop (.) ထည့်ဖို့လုံးဝမမေ့ပါနဲ့။ မပါခဲ့လျှင် ECHO is off လို့စာတန်း ထိုးလိုက်ပါလိမ့်မယ်။

: (Full Column) ကိုအထူးအသုံးပြုရမှာပါ။ စာဖတ်သူညွှန်းဆိုလုပ်ဆောင်ချက်ကို ၄င်းနောက်မှ ထည့်သွင်းပေးရပါမယ်။ ၄င်း Full Column မပါလျှင် ညွှန်းဆိုမရပါ။

if ကိုလည်းအရေးပါ Key Word အဖြစ်သိထားရပါမယ်။ အသုံးပြုသူအား မေးလိုသောမေးခွန်းကို အဖြေပြန်ပေးလျှင် သိစေရန်ညွှန်းဆိုသောလုပ်ဆောင်ချက်ဖြစ်ပါတယ်။ ပြန်ဖြေသောအဖြေပေါ်မူတည်ပြီး အထက်ပါ **: (Full Column)** နောက်မှလုပ်ဆောင်ချက်ကိုခိုင်းစေကြပါတယ်။

if /I ကတော့ Input Key ဟာစာလုံးအကြီးအသေးမခွဲခြားစေဖို့အတွက်ပါ။

% ---% ကတော့ **if** နှင့်တွဲသုံးရပါတယ်။ ၄င်းတစ်ခုတည်းသီးသန့်မသုံးနိုင်ပါ။ ၄င်း နှစ်ခုကြားထဲမှာလုပ်ဆောင်ချက်ကိုမူတည်တန်ဖိုးပေးထားရပါမယ်။ စကားလုံး ကိုစိတ်ကြိုက်သုံးနိုင် သော်လည်း ညွှန်းဆိုချက်မူတည်တန်ဖိုးနှင့်တူညီရပါမယ်။

goto ကိုလည်း အထက်ပါ **if , %** တို့နှင့်တွဲသုံးဖို့ပါ။ ညွှန်းဆိုလိုက်တဲ့ နေရာကိုသွားခိုင်းတာပါ။ ရှင်းရှင်းပြောရလျှင် **: (Full Column)** နောက်မှညွှန်းချက်ကိုသွားခိုင်းတာပါ။ **goto** ကိုအသုံးချပြီး မိမိသွားလိုတဲ့ နေရာတစ်ခု၊ ဒါမှမဟုတ်လုပ်ဆောင်ချက်တစ်ခုကိုသွားဖို့ညွှန်ကြားနိုင်ပါတယ်။

goto:main ကတော့ အစဆုံးမှာထားခဲ့တဲ့ :main ကိုပြန်လည်သွားခိုင်းတာပါ။ အစကိုပြန်ရောက် စေတာပေါ့။ Program တစ်ခုလုံးကိုအစမှပြန်လည်လုပ်ဆောင်ဖို့ခိုင်းလိုက်တာပါ။

call ကလည်း ညွှန်းဆိုထားတဲ့ အခြား Program File တစ်ခုကိုခေါ်ယူအသုံးပြုစေတာပါ။ Calculator ကိုဖွင့်စေလိုလျှင် **call calc** လို့သုံးတာမျိုးပါ။

exit ဆိုတာကတော့ လက်ရှိသုံးနေတာကိုရပ်လိုက်ပါတော့မယ်။ ပိတ်လိုက်ပါဆိုပြီးသုံးပါတယ်။ ပုံမှန်အားဖြင့်တော့ စာဖတ်သူမှထွက်ခွင့်ကိုခိုင်းစေရပါတယ်။

cls ကလည်း DOS Command တွေမှာအသုံးများခဲ့တဲ့ Key တစ်ခုပါပဲ။ သိသူများပါတယ်။ လက်ရှိမျက်နှာစာကိုရှင်းလင်းလိုက်တာပါ။

pause ကတော့ ညွှန်းချက်တစ်ခုပြီးသွားတဲ့အခါ ခဏရပ်နေပါ့မယ်လို့ခိုင်းစေတာမှာသုံးပါတယ်။ ဆက်လက်အသုံးပြုလိုလျှင် Key တစ်ခုခုကိုနှိပ်ဖို့ခိုင်းတတ်ပါတယ်။

set ကိုတော့ အသုံးပြုသူကထည့်လိုက်တဲ့ ညွှန်းချက်တစ်ခုကိုနားလည်စေဖို့သုံးပါတယ်။

set /p ကတော့ အသုံးပြုသူထည့်ရမယ့် ညွှန်းချက်ကို စာသားဖြင့် ဖော်ပြထားဖို့သုံးပါတယ်။ **/p** ကို သုံးရတာကတော့ ညွှန်းချက်ပါသတ်မှတ်ချက်မဟုတ်လျှင် အလုပ်မလုပ်စေဖို့ထားရှိတာပါ။

color ကို အရောင်ထည့်သွင်းပြောင်းလဲရန်သုံးပါတယ်။ ပုံမှန်အားဖြင့် Command Prompt က နောက်ခံအမဲရောင်ပေါ် အဖြူစာလုံးသုံးပါတယ်။ ဒါကိုစိတ်ကြိုက်ပြောင်းဖို့သုံးပါတယ်။ color command ကိုနောက်ခံရော စာလုံးကိုပါတွဲပြီးတစ်ခါတည်းထည့်သုံးနိုင်ပါတယ်။ ဥပမာ – **color 1A** ဆိုသည်မှာ ရှေ့ **1** ကနောက်ခံ အရောင်၊ နောက် **A** ကတော့စာလုံးအရောင်ဖြစ်ပါတယ်။

အရောင်စာရင်းမှာ–

0 = Black	8 = Gray
1 = Blue	9 = Light Blue
2 = Green	A = Light Green
3 = Aqua	B = Light Aqua
4 = Red	C = Light Red
5 = Purple	D = Light Purple
6 = Yellow	E = Light Yellow
7 = White	F = Bright White

တို့ဖြစ်ပါတယ်။

စာဖတ်သူအနေနဲ့သုံးနေရင်း မေ့သွားလို့ သိချင်ခဲ့လျှင် Command Prompt မှာ **color /?** လို့ခေါ်ယူကြည့်နိုင်ပါတယ်။ အထက်ပါ အရောင်စာရင်းပေါ်လာပါလိမ့်မယ်။

အရောင်တွေကိုစမ်းထည့်ကြည့်လို့အဆင်မပြေလျှင် ထည့်ပြီးမှပြန်ပြင်နိုင်ပါသေးတယ်။

Registry တွေကိုပြင်ဖို့အတွက် Registry Key word တွေကိုသီးသန့်သိရှိထားရပါမယ်။ Registry ကိုပြင်ဆင်ရတာမလွယ်ကူပါဘူး။ တစ်ခါတလေ ပြုလုပ်မရတာတွေလည်းရှိတတ်ပါတယ်။ သီးသန့် Parameter တွေ ထားရှိပါတယ်။ အသုံးများတာတွေကိုသာဖော်ပြလိုက်ပါတယ်။

reg add ကတော့ Registry ကိုပြုပြင်ထည့်သွင်းဖို့သုံးရမယ့် Key Word ဖြစ်ပါတယ်။ Registry အတွက် သီးသန့်သာသုံးနိုင်ပါတယ်။

reg delete ကတော့ Registry အတွင်းမှတစ်ခုခုကိုဖျက်ရန်သုံးရမယ့် Key Word ဖြစ်ပါတယ်။

/v ကို Value ကိုနာမည်ပေးဖို့အတွက်သုံးရပါတယ်။ ကိုယ်တိုင်စိတ်ကြိုက်သုံးဖို့အတွက် ဖြစ်ပါတယ်။

/ve ကို Value Name အားကွန်ပျူတာသတ်မှတ်ချက်အတိုင်းပေးဖို့သုံးပါတယ်။

/t ကိုတော့ Value ရဲ့ Data Type ကိုညွှန်းဆိုဖို့သုံးပါတယ်။

/d ကိုတော့ Data ကိုညွှန်းဆိုဖို့သုံးပါတယ်။

/f မှာလုပ်ဆောင်ချက်တစ်ခုခုအတွက် လုပ်/မလုပ် ပြန်လည်မေးခွန်းထုတ်သည်ကို မထုတ်ပါနဲ့လို့ ခိုင်းစေတာမျိုးမှာသုံးပါတယ်။

ယခုလောက်ဆိုလျှင် Script အကြောင်းတီးမိခေါက်မိပြီထင်ပါတယ်။ လုံးဝမခက်ခဲပါဘူး။ အကြောင်းမသိလို့သာ ခက်ခဲမယ်ထင်ပါတယ်။ Program ရေးဖို့စိတ်ဝင်စားသူတွေဆိုလျှင် Script တစ်ပုဒ်လောက်ရေးပြီးပြီဆိုတာနဲ့ ဆက်ဆက်ပြီးရေးချင်လာပါတယ်။

စာဖတ်သူကွန်ပျူတာထဲမှာရှိနေတဲ့ ထိန်းကျောင်းမှုစနစ်တွေကို ယခုရှင်းပြမယ့် Script တွေနဲ့ ညွှန်ကြားနိုင်ပါတယ်။ ဖျက်မရတဲ့ Virus Files တွေကိုလည်း အလွယ်တကူဖျက်ဖို့ညွှန်ကြားနိုင်ပါတယ်။ ကိုယ်တိုင်ရေးထားတဲ့ Program တစ်ပုဒ်ကိုသုံးပြီး ကိုယ့်ကွန်ပျူတာကိုကိုယ်တိုင်ထိန်းကျောင်းနိုင်တော့ စိတ်ထဲမှပျော်ရွှင်လာမှာပါ။

စာဖတ်သူသတိပြုရမှာကတော့ အသုံးပြု Program က Notepad ဖြစ်နေပေမယ့် သိမ်းဆည်းရမယ့် ဖိုင်ပုံစံကတော့ .cmd နှင့် .bat ပဲဖြစ်ပါတယ်။ စာဖတ်သူပြုလုပ်ထားတဲ့ Program File ပေါ် Right Click နှိပ်ပြီး Edit ဖြင့်ပြန်လည်ပြင်ဆင်နိုင်ခွင့်ရှိပါတယ်။

နောက်ကဏ္ဍများမှာအရှင်းဆုံး လက်တွေ့အသုံးချ Script များရေးသားပုံကိုရှင်းပြထားသလို စာအုပ်နှင့်တွဲပါ စီဒီချပ်ထဲမှာလည်း Control Script Folder၌တစ်ခါတည်းထည့်သွင်းပေးထားပါတယ်။ ကလစ်နှစ်ချက်နှိပ်ပြီး တိုက်ရိုက်သုံးနိုင်ပါတယ်။

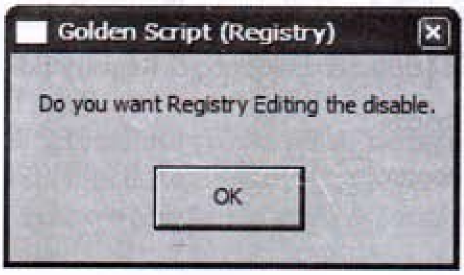
Registry Control Script Program ကိုရေးသားလေ့လာခြင်း

ယခု Program ကတော့ Virus File တွေဖန်တီးတတ်တဲ့ .vbs File စနစ်ကိုသုံးပြီး အကျိုးပြု Registry Control Script prgram တစ်ခုဖန်တီးထားတာပါ။ အရှင်းဆုံး Program Code တွေကို အသုံးပြုထားပါတယ်။ ယခု Program လေးကို Script Code တွေမသုံးထားပါဘူး။ Programming Language အများစုမှာသုံးနေကြတဲ့ Program Code တွေကိုသာသုံးပြီး .vbs Script တစ်ခုဖန်တီးပြလိုက်တာပါ။

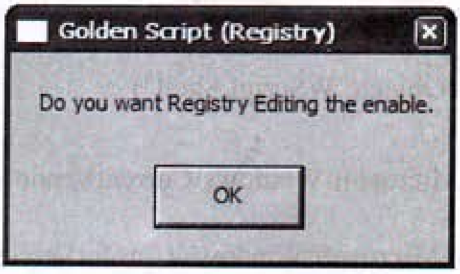
```
Option Explicit

Dim WSHShell, rr, rr2, MyBox, val, val2, ttl, toggle
Dim golden, itemtype
On Error Resume Next
Set WSHShell = WScript.CreateObject("WScript.Shell")
val = "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\ Disable-
RegistryTools"
val2 = "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\ Dis-
able-RegistryTools"
itemtype = "REG_DWORD"
golden = "Registry Editing Tools are now "
ttl = "Golden Script (Registry)"
'reads the registry key value.
rr = WSHShell.RegRead (val)
rr2 = WSHShell.RegRead (val2)
toggle=1
If (rr=1 or rr2=1) Then toggle=0
If toggle = 1 Then
WSHShell.RegWrite val, 1, itemtype
WSHShell.RegWrite val2, 1, itemtype
Mybox = MsgBox(golden & "disabled.", 4096, ttl)
Else
WSHShell.RegDelete val
WSHShell.RegDelete val2
Mybox = MsgBox(golden & "enabled.", 4096, ttl)
End If
```

တစ်ဖက်စာမျက်နှာမှာဖော်ပြထားတဲ့ Script Code တွေကို Notepad မှာရေးသားပြီး Regcontrol.vbs ဖြင့်သိမ်းဆည်းရပါမယ်။ ဒီတစ်ခါတော့ ကြိုက်ရာနေရာမှသိမ်းထားနိုင်ပါတယ်။ File Location သတ်မှတ်ထားတာမရှိပါဘူး။ ကြိုက်တဲ့နေရာမှာထားပြီးကလစ်နှစ်ချက်နှိပ်ဖွင့်လိုက်တာနဲ့ အောက်ဖက်မှာပြထားသလို Command Box တစ်ခုပေါ်လာပါလိမ့်မယ်။

ပထမတစ်ခါလုပ်ဆောင်ချက်မှာ Registry ကို Disable လုပ်လိုက်ခြင်းပါ။ Restart ပြန်ချစရာမလိုပါဘူး။ တိုက်ရိုက်အကျိုးသက်ရောက်ပါတယ်။ Disable လုပ်ထားတဲ့အတွက်ခေါ်ယူလျှင် ဘေးမှပုံစံ Error Box တက်လာပါတယ်။



Registry ကို Enable ပြန်လည်ပြုလုပ်ကာအသုံးပြုလိုလျှင် ၄င်း Regcontrol.vbs ပေါ်မှာ ကလစ်နှစ်ချက်နှိပ်ပြီးဖွင့်လိုက်တာနဲ့ အောက်ပါပုံ Command Box တက်လာပြီး Registry Enable ဖြစ်သွားပါလိမ့်မယ်။



Registry ကို Enable/ Disable ပြုလုပ်အသုံးချရန်မှာ– မိမိကွန်ပျူတာကိုတပါးသူမှ ပြင်ဆင်ခြင်း မလုပ်ရန်နှင့် Virus ကြောင့် Disable ဖြစ်နေတဲ့အခါပြန်ဖွင့်ရန်အတွက်သုံးနိုင်ပါတယ်။ တခါတည်း Registry ကို Disable လုပ်ထားလျှင် Virus ကြောင့် Registry ပိတ်ဆို့ထားခြင်းကို ကာကွယ်နိုင်ပါတယ်။

Golden Script (Registry) Program လေးဟာရိုးသာဟက်ကာတွေရဲ့လက်စွဲဖြစ်လာမှာပါ။

.vbs Script ကိုထိုးထွင်းလေ့လာဖန်ခြင်း

စာရေးသူရှေ့ပိုင်းမှာဆိုခဲ့သလို Hacker တွေဟာ Programming တွေကိုလည်းကျွမ်းကျင်ရပါမယ်။ အသုံးချ Programming Language တွေများစွာရှိတဲ့အထဲမှ ယခု .vbs စနစ်နှင့် သာမန် Script စနစ်တို့ကိုရေးသားနိုင်ခြင်းဟာ ပညာရှင်ဆန်ဆန်လက်နက်တစ်ခုပါပဲ။ အလွယ်တကူရေးသားနိုင်ပြီး လက်ခံဆော့ဖ်ဝဲလ်မလိုပဲ ပင်တိုင်ရပ်တည်နိုင်ပါတယ်။ ရေးသားရန်အတွက်လည်း ဖန်တီးရှင်ဆော့ဖ်ဝဲလ်လည်း မလိုအပ်ပါဘူး။

ဟုတ်ပါပြီခင်ဗျာ-- စာရေးသူရှေ့ကဏ္ဍမှာ Registry ကိုပြင်ဆင်ဖို့ Registry Editor အတွင်းမှ Value တွေ၊ Data တွေကိုပြင်ဆင်ပြသွားပါတယ်။ အဆိုပါလမ်းကြောင်းတွေကို ယခုရေးပြီးသား Golden Script (Registry) Program ထဲမှာ ပြင်ဆင်ပြီးအလွယ်လုပ်ကိုင်နိုင်ပါတယ်။ ပြောရလျှင် Registry Editor ကိုတောင်မလိုအပ်တော့ပါဘူး။ ပိတ်ထားလည်းသုံးနိုင်ပါတယ်။

ရှေ့မှ Golden Script (Registry) Program ကိုခွဲခြားလေ့လာကြည့်ပါမယ်။

Option Explicit

Dim WSHShell, rr, rr2, MyBox, val, val2, ttl, toggle
Dim golden, itemtype

Dim ကသုံးစွဲခွင့်တောင်းယူလိုက်တာပါ။

On Error Resume Next

Error ဖြစ်ခဲ့လျှင် ပြန်စခိုင်းတာပါ။

Set WSHShell = WScript.CreateObject("WScript.Shell")

တူညီမှုတစ်ခုသတ်မှတ်လိုက်တာပါ။

*** val = "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\Disable-RegistryTools"

*** val2 = "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\Disable-RegistryTools"

အထက်ပါ val နှင့် val2 ကတော့ Registry အတွင်းမှလမ်းကြောင်းတွေပဲဖြစ်ပါတယ်။ စာဖတ်သူအနေဖြင့်အခြား လုပ်ဆောင်ချက်များအတွက် ယခုနေရာမှာအစားထိုးရပါမယ်။ HKCU က HKEY_CURRENT_USER ရဲ့အတိုကောက်ဖြစ်ပြီး၊ HKLM ကတော့ HKEY_LOCAL_MACHINE ရဲ့အတိုသုံးဖြစ်ပါတယ်။ Script Code တွေမှာ အထက်ပါအတိုင်းအတိုစာလုံးပြောင်းသုံးရပါတယ်။

```
*** itemtype = "REG_DWORD"
```
ကတော့ DWORD Value ကိုပြောလိုက်တာပါ။
```
golden = "Registry Editing Tools are now "
ttl = "Golden Script (Registry)"
```
Massage Box အတွက်ဖြစ်ပါတယ်။
```
'reads the registry key value.
rr = WSHShell.RegRead (val)
rr2 = WSHShell.RegRead (val2)
toggle=1
```
Value Data တန်ဖိုးပေးလိုက်တာပါ။
```
If (rr=1 or rr2=1) Then toggle=0
If toggle = 1 Then
WSHShell.RegWrite val, 1, itemtype
WSHShell.RegWrite val2, 1, itemtype
Mybox = MsgBox(golden & "disabled.", 4096, ttl)
Else
WSHShell.RegDelete val
WSHShell.RegDelete val2
Mybox = MsgBox(golden & "enabled.", 4096, ttl)
End If
```
If တွေနဲ့စပြီးညွှန်ကြားနေတာကတော့ Value Data တွေကိုပြောင်းလဲထည့်ဖို့ညွှန်နေတာပါ။ လုပ်ဆောင်ချက်တစ်ခုနှင့်ကိုက်ညီပြီးလုပ်ဆောင်လိုက်တိုင်း Massage Box တွေကိုပါတွေ့မြင်ဖို့ ခိုင်းစေနေတာပါ။

ယခုလောက်ဆို စာဖတ်သူနားလည်လောက်ပြီထင်ပါတယ်။ အဓိကအချက်ကိုကောက်နုတ်ရလျှင် ***ပြထားသော Registry ဆိုင်ရာ Value တွေ၊ Data တွေကိုပြင်ဆင်ပြောင်းလဲရမှာပါ။ အခြားတွေကိုပြင်ဆင်ဖို့မလိုအပ်ပါဘူး။

စာဖတ်သူကိုယ်တိုင် Run Box ကိုဖျောက်ခြင်း၊ ပေါ်ခြင်းအတွက် အထက်ပါနေရာများတွင်ပြင်ဆင်ပြီးဖန်တီးကြည့်လိုက်ပါ။ ဟင်းစားရောကွန်ချက်ပါပြလိုက်တာပါ။ အသင့်ရေးပြီးသားများကို http://thanhtikegs.weebly.com မှာ Download လုပ်ယူနိုင်ပါတယ်။

Control System Enable Script Program ကိုရေးသားခြင်း

ယခု Program ကတော့ Control System Effect တွေကိုသုံးမရအောင်ဖျောက်ထားတဲ့အခါ သုံးဖို့အတွက် ရေးသားထားတာပါ။ Registry Editor, Task Manager, Run Program, Show Folder Option တွေကိုပြန်လည်ရယူသုံးနိုင်ရန် ပြန်ခေါ်ယူတဲ့ Script Program တစ်ပုဒ်ဖြစ်ပါတယ်။

ပြန်ခေါ်ယူတာသီးသန့်ဖြစ်ပါတယ်။ ပြန်လုပ်တာပေါ့နော်။

ယခု Program လေးကို Script Code တွေ Notepad မှာရေးပြီးပါက Control System.bat ဖြင့်သိမ်းထားရပါမယ်။ ကွန်ပျူတာမရွေးအလွယ်တကူပြန်သုံးနိုင်ပါတယ်။

```
@ECHO OFF
prompt $p$g
title GOLDEN GATE SECURITY (Control System Effect)
COLOR E1

:-CONTROL
CLS
ECHO.
ECHO.
ECHO                GOLDEN GATE SECURITY
ECHO                Control System Effect
ECHO.
ECHO.
ECHO         The Scirpt Program are System Control Service.
ECHO.
ECHO.
ECHO         1. Registry Editor to Enable.
ECHO.
ECHO         2. Task Manager(Ctrl+Alt+Del) to Enabel.
ECHO.
ECHO         3. Run Program to Enable.
ECHO.
ECHO         4. Show Folder Option (Control Panel).
ECHO.
ECHO         Q. EXIT
ECHO.
ECHO.
ECHO.
```

```
SET/P val =       Your Choose and Type one Key Number :
IF "%val%" == "1" GOTO -1
IF  "%val%" == "2" GOTO -2
IF "%val%" == "3" GOTO -3
IF "%val%" == "4" GOTO -4
IF/I "%val%" == "Q" GOTO -Q
GOTO :-CONTROL


:-1
ECHO.
REG DELETE HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\
POLICIES\EXPLORER /V DisableRegistryTools /f
ECHO.
pause
GOTO :-CONTROL

:-2
ECHO.
REG DELETE HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\
POLICIES\SYSTEM /V DisableTaskMgr /f
ECHO.
pause
GOTO :-ONTROL

:-3
ECHO.
REG DELETE HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\
POLICIES\EXPLORER /V NoRun /f
pause
GOTO :-CONTROL

:-4
ECHO.
REG DELETE HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\
POLICIES\EXPLORER /V NoFolderOptions /f
ECHO.
pause
GOTO :-CONTROL
```

```
:-Q
ECHO.
ECHO  You want to Exit, Thank You.
ECHO.
PAUSE
EXIT
```

ပြန်သုံးသပ်ခြင်း

ယခုရေးသားထားသော Script Program ကိုပြန်လည်သုံးသပ်ရလျှင် System Controller တွေကိုပြန်လည်ခေါ်ယူခြင်းသာအသုံးပြုနိုင်ပါတယ်။

အဓိကညွှန်ကြားချက်ပေးတဲ့ Script Codeကတော့ REG DELETE ပဲဖြစ်ပါတယ်။ ညွှန်ကြားမှုကိုလုပ်ဆောင်တာကတော့ Registry အတွင်းမှ ရေးသွင်းပြီးသား Value & Data တွေကိုဖျက်လိုက်တာပါ။ ဥပမာအနေဖြင့် အောက်ပါ Code Line ကိုလေ့လာကြည့်ပါ။

REG DELETE HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\EXPLORER /V DisableRegistryTools /f

နောက်ဆုံးမှ f ကတော့ ဖျက်ဖို့ခိုင်းစေတဲ့အခါ ကွန်ပျူတာကနေ Yes or No အတည်ပြုချက်တောင်းတာကို တိုက်ရိုက်အတည်ပြုပေးလိုက်တာပါ။

.vbs File System ရေးနည်းကပိုမိုနက်နဲပါတယ်။ ယခုလို .bat File System ရေးနည်းကတော့ အလွယ်ဆုံးဖြစ်ပါတယ်။

ဖော်ပြချက်များအတိုင်းအဆင်သင့်ရေးသားပြီးလျှင် Control System.bat ဆိုပြီးသိမ်းပါ။ အဆိုပါဖိုင်ကိုကလစ်နှစ်ချက် နှိပ်ဖွင့်လိုက်လျှင်အောက်ပါအတိုင်း လုပ်ဆောင်ချက် လေးခုတောင်းဆိုသော Command Prompt မြင်ကွင်းကို တွေ့ရပါလိမ့်မယ်။

စာဖတ်သူပြန်လည်ရယူလိုသော ညွှန်းဆိုချက်ကို ၁၊ ၂၊ ၃၊ ၄ အစီအစဉ်အရရိုက်ထည့်ပြီး Enter ခေါက်လိုက်သည်နှင့်အလိုအလျောက်ပြုပြင်သွားပါလိမ့်မယ်။ Registry ပြုပြင်မှုဖြစ်တာကြောင့် Restart ပြန်ချပေးဖို့လိုပါတယ်။

```
GOLDEN GATE SECURITY (Control System Effect)

              GOLDEN GATE SECURITY
              Control System Effect

      The Scirpt Program are System Control Service.

      1. Registry Editor to Enable.

      2. Task Manager<Ctrl+Alt+Del> to Enabel.

      3. Run Program to Enable.

      4. Show Folder Option <Control Panel>.

      Q. EXIT

      Your Choose and Type one Key Number :
```

Control System Disable Script Program အတွက်ပြင်ဆင်ရေးသားခြင်း

ယခု Program ကတော့ Control System Effect တွေကိုသုံးမရအောင်ဖျောက်ထားတဲ့အခါ သုံးဖို့အတွက် ရေးသားထားတာပါ။ Registry Editor, Task Manager, Run Program, Show Folder Option တွေကိုပြန်လည်ရယူသုံးနိုင်ရန် ပြန်ခေါ်ယူတဲ့ Script Program တစ်ပုဒ်ဖြစ်ပါတယ်။

ပြန်ခေါ်ယူတာသီးသန့်ဖြစ်ပါတယ်။ Disable ပြန်လုပ်တာပေါ့နော်။

```
@ECHO OFF
prompt $p$g
title GOLDEN GATE SECURITY (Control System LOCK Effect)
COLOR E1

:-CONTROL
CLS
ECHO.
ECHO.
ECHO                    GOLDEN GATE SECURITY
ECHO                    Control System LOCK Effect
ECHO.
ECHO.
ECHO            The Scirpt Program are System Control Service.
ECHO.
ECHO.
ECHO            1. Registry Editor to Disable.
ECHO.
ECHO            2. Task Manager(Ctrl+Alt+Del) to Disable.
```

```
ECHO.
ECHO        3. Run Program to Disable.
ECHO.
ECHO        4. Hide Folder Option (Control Panel).
ECHO.
ECHO        Q. EXIT
ECHO.
ECHO.
ECHO.

SET/P val =     Your Choose and Type one Key Number :
IF "%val%" == "1" GOTO -1
IF  "%val%" == "2" GOTO -2
IF "%val%" == "3" GOTO -3
IF "%val%" == "4" GOTO -4
IF/I "%val%" == "Q" GOTO -Q
GOTO :-CONTROL


:-1
ECHO.
REG ADD HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\
EXPLORER /V DisableRegistryTools /t reg_dword /d 1 /f
ECHO.
PAUSE
GOTO :-CONTROL
```

```
:-2
ECHO.
REG ADD HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\
SYSTEM /V DisableTaskMgr /t reg_dword /d 1 /f
ECHO.
pause
GOTO :-ONTROL

:-3
ECHO.
REG ADD HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\
EXPLORER /V NoRun /t reg_dword /d 1 /f
pause
GOTO :-CONTROL

:-4
ECHO.
REG ADD HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\
EXPLORER /V NoFolderOptions /t reg_dword /d 1 /f
ECHO.
pause
GOTO :-CONTROL
```

-Q

CLS

ECHO.

ECHO You want to Exit, Thank You.

ECHO.

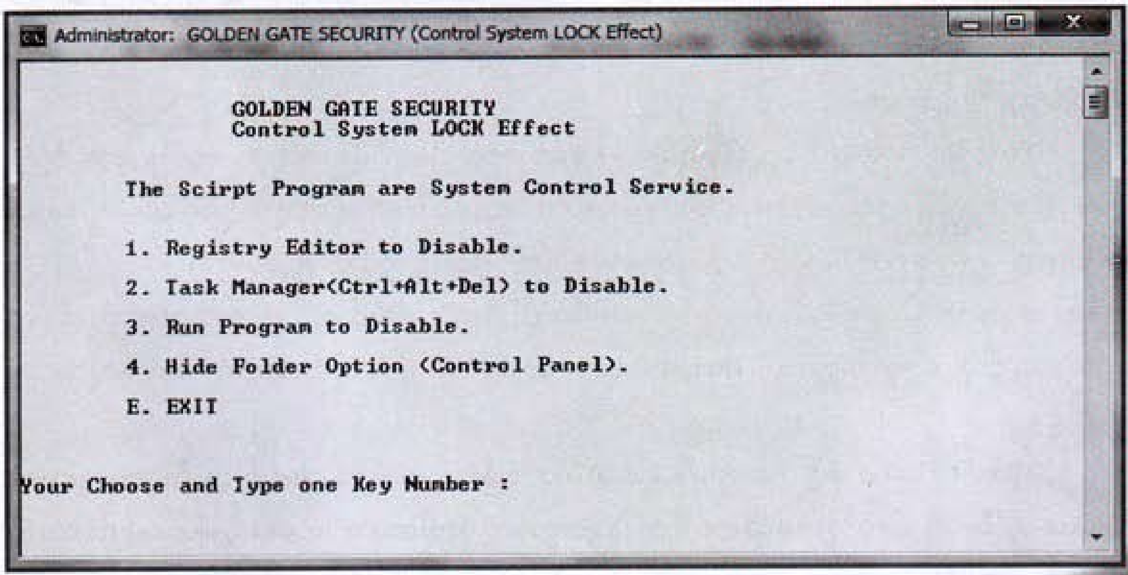
PAUSE

EXIT

အဆင်သင့်ရေးသားပြီးလျှင် Control System Disable.bat ဆိုပြီးသိမ်းပါ။ အဆိုပါဖိုင်ကို ကလစ်နှစ်ချက် နှိပ်ဖွင့်လိုက်လျှင်အောက်ပါအတိုင်း လုပ်ဆောင်ချက် လေးခုတောင်းဆိုသော Command Prompt မြင်ကွင်းကို တွေ့ရပါလိမ့်မယ်။

စာဖတ်သူအသုံးပြုလိုသော ညွှန်းဆိုချက်ကို ၁၊ ၂၊ ၃၊ ၄ အစီအစဉ်အရကြိုက်တာ ရိုက်ထည့်ပြီး Enter ခေါက်လိုက်သည်နှင့်အလိုအလျောက်ပြုပြင်သွားပါလိမ့်မယ်။ Registry ပြုပြင်မှုဖြစ်တာကြောင့် Restart ပြန်ချပေးဖို့လိုပါတယ်။

တစ်ပြိုင်တည်း လေးခုစလုံးညွှန်ကြားနိုင်ပါတယ်။ အစဉ်လိုက်တစ်ခုပြီးတစ်ခုပြုလုပ်သွားပါ။



စာဖတ်သူများအနေဖြင့် Script Program တွေကို ရေးဆွဲတဲ့အခါ တွေ့ကြုံရမယ့် ပြဿနာ အနည်းငယ်ရှိတတ်ပါတယ်။ Script တွေကို အမျိုးအစားအမျိုးမျိုးတွေ့ရပြီး အသုံးချ Code Line တွေဟာလည်း မတူညီကြပါဘူး။ အသုံးအများဆုံးကတော့ Command Script တွေဖြစ်ပြီး။ Vb Script, Java Script နှင့် PHP Script တွေကိုလည်း သိထားတတ်ထားသင့်ပါတယ်။

Script တွေမှာအဓိကတွေ့ကြုံရတဲ့ ပြဿနာကတော့ Running လုပ်ဆောင်ချက်မရရှိခြင်းပါ။ အဆိုပါပြဿနာမျိုးတွေဖြစ်လာလျှင် သေချာစွာပြန်စစ်ဆေးကြည့်ပါ။ မလိုအပ်ပဲ အစက်တစ်စက်ပိုနေလျှင် အလုပ်မလုပ်တာမျိုးတွေရှိတတ်ပါတယ်။

အများဆုံးဖြစ်တတ်တဲ့ နောက်ပြဿနာတစ်ခုကတော့ စာလုံးပေါင်းမှားနေခြင်းပါပဲ။ စာလုံးပေါင်းမှားယွင်းမှုဟာ Script တွေအတွက်အကြီးမားဆုံးပြဿနာဖြစ်လာစေပါတယ်။ Script တွေဟာ ရေးသွင်းထားတဲ့ စာလုံးတွေပေါ်မှာမှီခိုလုပ်ဆောင်ရတာကြောင့် မည်သို့သောမှားယွင်းမှုကိုမှလက်မခံပါ။

နောက်တစ်ချက်ကတော့ ခိုင်းစေချက်လမ်းကြောင်း File Location မှားယွင်းနေတာပါ။ ဒါကိုလဲ Script Program တွေဟာနားလည်မပေးပါဘူး။ စာဖတ်သူသေချာစွာသုံးသပ်ကြည့်ပါ။ စာဖတ်သူခိုင်းစေလိုက်သော လုပ်ဆောင်ချက်အတွက် ပြုလုပ်ရန် သွားရောက်ရှာဖွေသောအခါ အဆိုပါညွှန်းထားသော File Location တွင် ခိုင်းစေချက်မရှိပါက ဘာကိုလုပ်ဆောင်မည်နည်း။

Network Hacker တွေဟာ Programming ပညာရပ်ကို အများဆုံးကျွမ်းကျင်ကြပါတယ်။ Website ရေးဆွဲခြင်းဆိုင်ရာ ပညာရပ်တွေကိုလည်း ထိုးထိုးဝင်ဝင် ဆိုင်ရာပညာတွေမှာလည်းမခေသလို၊ သိကျွမ်းနေကြပါတယ်။

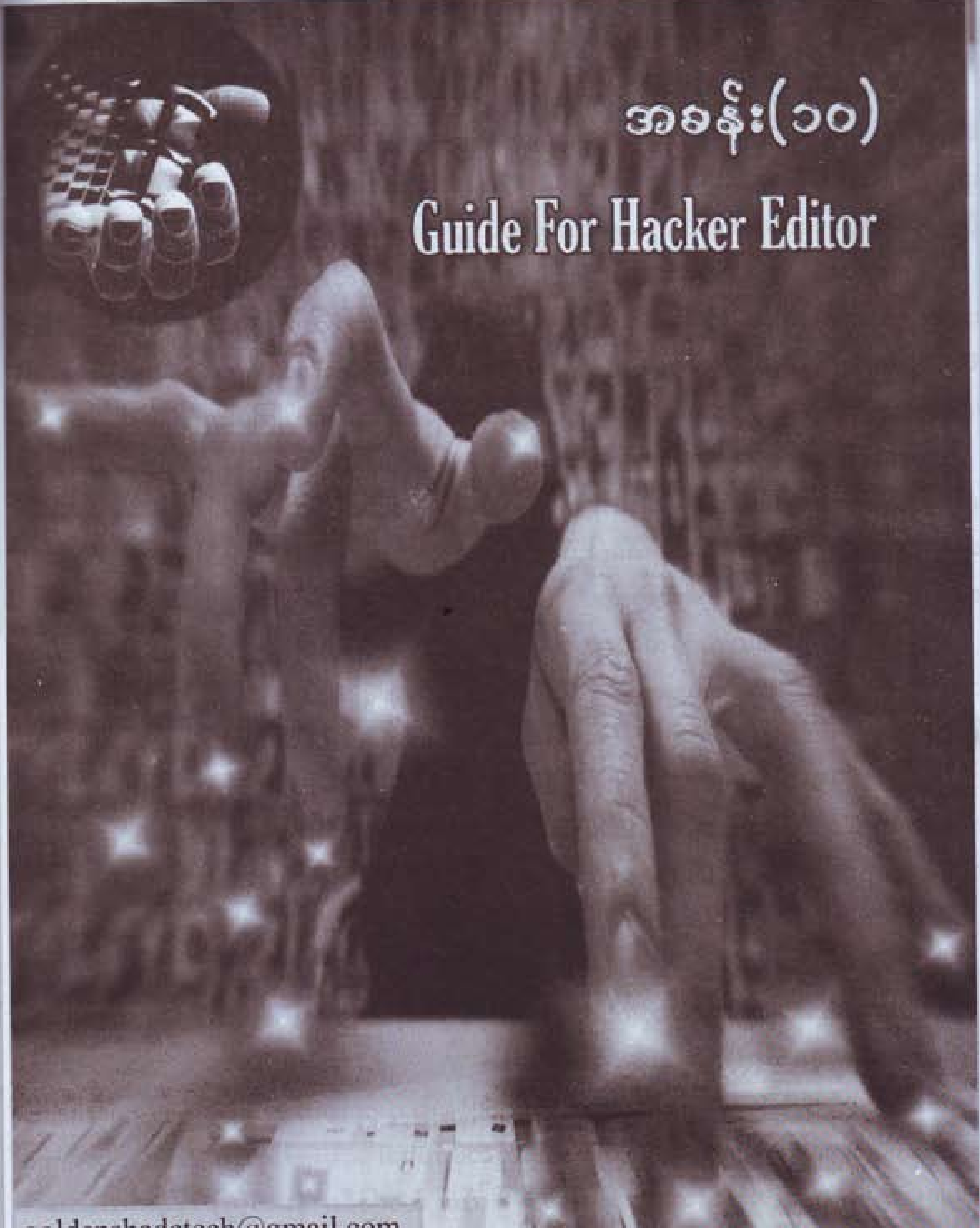
Program, Software တွေကိုလည်း နှံ့နှံ့စပ်စပ်တတ်မြောက်ဖို့လည်းလိုပါတယ်။ အဆင့်မြင့် Hacker တွေဆိုလျှင် ကိုယ်ပိုင် Operation System ကိုပင် ကိုယ်တိုင်ရေးဆွဲအသုံးပြုကြပါတယ်။ Hacker အများစုဟာ Windows OS ထက် Open Source OS ကိုပိုမိုသုံးစွဲကြတာတွေ့ရပါတယ်။

စိတ်ဓာတ်မြင့်မားပြီး၊ ကောင်းမွန်သောလမ်းကြောင်းပေါ်မှာ ရပ်တည်နေကာ နည်းပညာဆိုင်ရာ ပြဿနာတွေကို ဖြေရှင်းပေးမယ့် Honest Hacker တွေဆိုတာ နိုင်ငံတိုင်းအတွက် အလွန်လိုအပ်နေပါတယ်။

Honest Hacker နှင့် Black Hacker ဆိုတာ မျဉ်းလေးတစ်ခုသာခြားပါတယ်။ စာရေးသူထံ Hacker ဆိုပြီး ကိုယ့်ကိုကိုယ်မိတ်ဆက်လာသူများစွာတွေ့ဖူးပါတယ်။ စာရေးသူပြောနေကြစကားရှိပါတယ်။ "ဟုတ်ကဲ့ တွေ့ရတာတော့ဝမ်းသာပါတယ်၊ ဒါပေမယ့်ကြောက်တယ်ဗျ"

အခန်း(၁၀)

Guide For Hacker Editor



goldenshadetech@gmail.com

Guide For Hacker Editor

Hacker တွေဟာ ကွန်ပျူတာတစ်လုံးကိုကိုင်တွယ်အသုံးပြုဖို့လိုအပ်နေတဲ့အချိန်မှာ Registry Editor နဲ့ Run Box ကိုပိတ်ထားတယ်ဆိုလျှင် အမြန်ဆုံးနည်းလမ်းရှာကာ Command Prompt ကိုဖွင့်ဖို့ကြိုးစားကြပါတယ်။ Command Prompt ဟာ Hacker တွေရဲ့အသက်ပဲဆိုလျှင်မမှားပါဘူး။ ဒီ့ထက်အဆင့်မြင့်စွာပိတ်ထားတဲ့ကွန်ပျူတာတွေမှာတော့ Command Prompt ကိုပင်ဖွင့်လို့မရကြပါဘူး။

ဒီလိုအချိန်ဟာ Hacker တွေအတွက်နောက်ဆုံးကြိုးစားဖို့လိုလာတဲ့အချိန်ပါပဲ။ ရေကုန်ရေခန်းထိုးဖောက်နိုင်ဖို့ နည်းလမ်းတစ်ခုသာကျန်ပါတော့တယ်။ ဒါကိုတော့ ဘယ်လိုမှပိတ်လို့မရတော့ပါဘူး။ USB Disk တစ်ခုခုကနေလည်းထည့်သွင်းအသုံးပြုနိုင်တဲ့ NotePad, WordPad ပဲဖြစ်ပါတယ်။ အများစုကတော့ NotePad, WordPad တွေကိုပိတ်ထားရကောင်းမှန်းမသိကြပါဘူး။

ဘာပဲဖြစ်ဖြစ် Script Program တစ်ခုအား နေရာတစ်ခုခုကနေအလွယ်ရေးနိုင်ပါတယ်။ စာဖတ်သူသိထားရမှာကတော့ Script Program မှာသုံးတဲ့ Code Line ပုံစံတွေကိုပါပဲ။ NotePad ပေါ်မှာရေးမယ်။ .bat ဒါမှမဟုတ် .cmd နဲ့သိမ်းမယ် ပြီးလျှင်ကလစ်နှစ်ချက်နှိပ် Run မယ်။ ဒါလောက်ဆိုလျှင် စာဖတ်သူသဘောပေါက်ပြီထင်ပါတယ်။

ဥပမာတစ်ခုအနေထက်လက်တွေ့လုပ်ဆောင်ချက်တစ်ခုအဖြစ်ရှင်းပြပါ့မယ်။ စာဖတ်သူလက်ထဲကိုရောက်လာတဲ့ ကွန်ပျူတာဟာ BIOS ကနေ Power ဖွင့်ဖွင့်ချင်း ကွန်ပျူတာကို Password ဖြင့်ပိတ်ထားပါ့မယ်။ ဒါကို **Power On Password ပိတ်ထားခြင်း၊ နံပတ်(၁)** လို့မှတ်ထားပါ။

ဒီလို Power ဖွင့်ဖွင့်ချင်း ကွန်ပျူတာကို Password ဖြင့်ပိတ်မထားနိုင်ဖို့ BIOS ထဲကိုဝင်ပြင်ရပါမယ်။ ဒီအခါလည်း Admin တစ်ယောက်သာပြင်ဆင်ခွင့်အတွက် Password ဖြင့်ပိတ်ထားပါဦးမယ်။ **BIOS Password ပိတ်ထားခြင်း၊ နံပတ်(၂)**လို့မှတ်ထားပါ။

Windows OS စနစ်ကိုစတင်ဝင်ရောက်တာနဲ့ User Logon ဆိုပြီး Password တစ်ခုထပ်ရှိပါလိမ့်မယ်။ ဒါ့အပြင်မျက်နှာပြင်ဖတ်လုံခြုံရေးစနစ်(Face Recognition)နှင့် လက်ဗွေရာလုံခြုံရေးစနစ် (Finger Bio Protection) တွေနဲ့တိုးပါပြီ။ ဟုတ်ကဲ့ပါ–ဒီအုပ်စုတစ်ခုလုံးကို **Logon Passoword ပိတ်ထားခြင်း၊ နံပတ်(၃)** လို့ မှတ်ထားလိုက်ပါ။

ဒီလိုနဲ့ပဲ Windows OS အတွင်းရောက်လာပါပြီ။ အသုံးဝင်လက်နက်တွေဖြစ်တဲ့ Run, Registry Editor, Group Prolicy, Task Manager တွေတစ်ခုမှခေါ်ခွင့်မရပါဘူး။ ရှင်းရှင်းပြောရလျှင် သုံးခွင့်ပြုတယ်ဆိုယုံပဲ ရှိနေပါတယ်။ ဒါကိုတော့ **ပိတ်ဆို့ထားခြင်း၊ နံပတ်(၄)** လို့မှတ်ထားပါ။

ယခုလောက်ဆိုလျှင်စာဖတ်သူလည်း ပိတ်ဆို့ထားခြင်းလေးမျိုးကိုနားလည်လောက်ပါပြီ။ အဆိုပါလေးမျိုးကိုအဆင့်လောက်ဝင်ရောက်ဖြေရှင်းပြပါ့မယ်။ ပြုလုပ်နိုင်မယ့် Windows OS တွေကတော့ Windows XP(all), Windows Vista, Windows 7 တွေပဲဖြစ်ပါတယ်။ ရှေ့ပိုင်းတွေကိုတော့ အသုံးအရမ်းနည်းသွားလို့ မရှင်းပြတော့ပါဘူး။

ယခုကဏ္ဍဟာ ဒီစာအုပ်တစ်ခုလုံးရဲ့အနှစ်ချုပ်ပါပဲ။ **ရိုးသားစွာထိုးထွင်းလေ့လာခြင်း** ဟုဆိုထားတဲ့အတွက် စက်ပြင်ပညာရှင်တွေအတွက်တော့ တကယ့်လက်သုံးဖြစ်မှာပါ။

နံပတ်(၁)

PowerOn Password ပိတ်ထားခြင်း

ယခုအပိုင်းအတွက်ကတော့ BIOS ကိုဖွင့်နိုင်လျှင်ရပါပြီ။ အတွင်းမှဝင်ရောက်ပြောထားတာပါ။ ဒါ့ကြောင့် နံပတ်(၂) အပိုင်းနှင့်တွဲဖက်ရှင်းပြသွားပါ့မယ်။

နံပတ်(၂)

BIOS Password ပိတ်ထားခြင်း

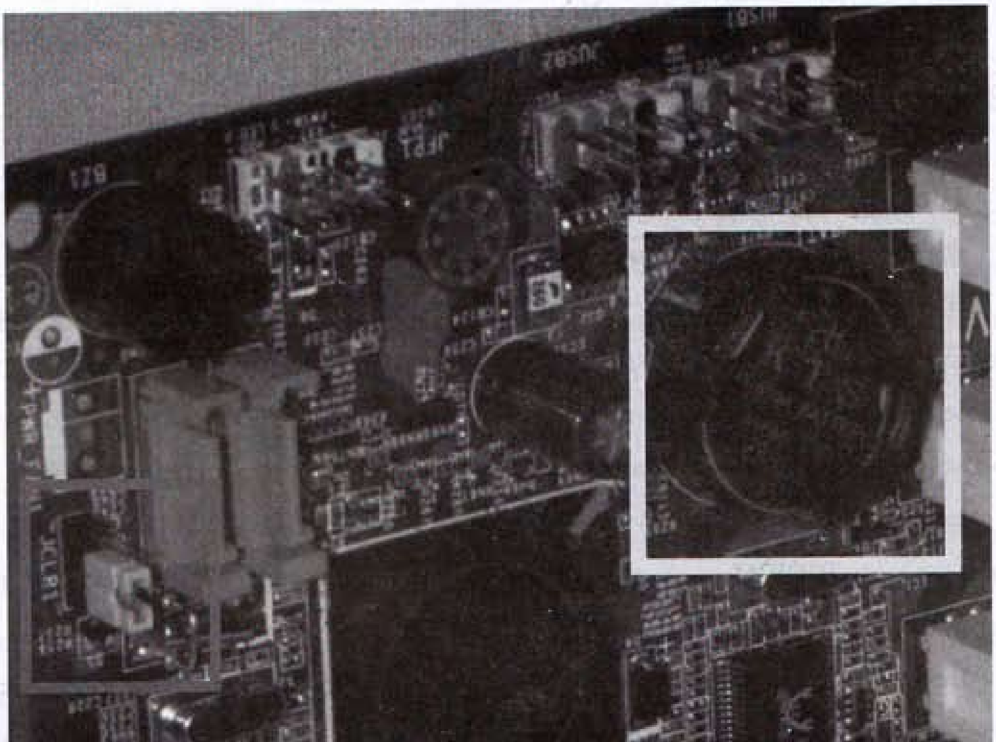
BIOS ဆိုတာ Basic Input/ Output System ရဲ့အတိုကောက်ဖြစ်ပါတယ်။ ကွန်ပျူတာတစ်ခုလုံးရဲ့ တပ်ဆင်ထားသမျှ Hardware တွေကိုစာရင်းပြုစုထားတာပါ။ Windows စတင်နိုင်ဖို့ Start RUN File For OS ထားရှိရာလိပ်စာကိုပြောင်းလဲနိုင်ပါတယ်။ အများသိထားတဲ့ Boot လုပ်တယ်ဆိုတာကိုပြောတာပါ။ အသေးစိတ်ကိုတော့ စက်ပြင်စာအုပ်တွေမှာလေ့လာကြည့်ပါ။

အဆိုပါ BIOS Password တွေကိုဖြုတ်ဖို့အတွက်နည်းလမ်းသုံးလမ်းရှိပါတယ်။ ပထမနည်းလမ်းက BIOS Memory ကိုရှော့ရိုက်လိုက်တာပါ။ အများသိထားသည်ကတော့ Jumper ချိုးလိုက်တယ်လို့ပြောကြပါတယ်။

Desktop PC တွေအနေနဲ့အခက်အခဲမရှိသော်လည်း Laptop တွေအတွက်ကတော့ ကျွမ်းကျင်မှုအတော်လိုအပ်နေပါတယ်။ ဘာကြောင့်လဲဆိုတော့ Laptop အတွင်းပိုင်းထဲကိုဝင်ရောက်ပြီး Jumper ကိုသွားပြောင်းရမှာဖြစ်လို့ပါ။(စာရေးသူရဲ့- " Laptop ကွန်ပျူတာပြုပြင်နည်းနှင့်သိသင့်စရာများ" စာအုပ်ကိုဦးစွာလေ့လာပါ။)

အောက်ဖက်တွင် PC MotherBoard ပေါ်တွင်တွေ့မြင်ရမည့် BIOS ကိုထိန်းချုပ်ထားသော Jumper နှင့် Battery ကိုပြထားတာပါ။ Battery ကမြင်လွယ်သော်လည်း Jumper က ရှာရခက်နေတတ်ပါတယ်။ စာရေးထားလျှင် အများအားဖြင့် JCLR လို့ရေးထားတက်ပါတယ်။

အဆိုပါ Jumper ကိုအောက်မှပုံအတိုင်း ခြေသုံးချောင်းတွင် နှစ်ချောင်းအစွပ်တပ်ပြီးသားဖြစ်နေပါလိမ့်မယ်။ ဒါကိုပုံမှန်လို့ခေါ်ပြီး၊ အဆိုပါအစွပ်ကိုချွတ်ကာ ဒုတိယပုံအတိုင်း ကျန်အဖျားဘက်ကိုပြောင်းစွပ်လိုက်၍ ၁မှ ၁၀ ထိရေတွက်ကာ မူလအတိုင်းပြန်ထားသည်နှင့် BIOS အတွင်းမှ Password, Control Data များပြုတ်သွားပါလိမ့်မယ်။

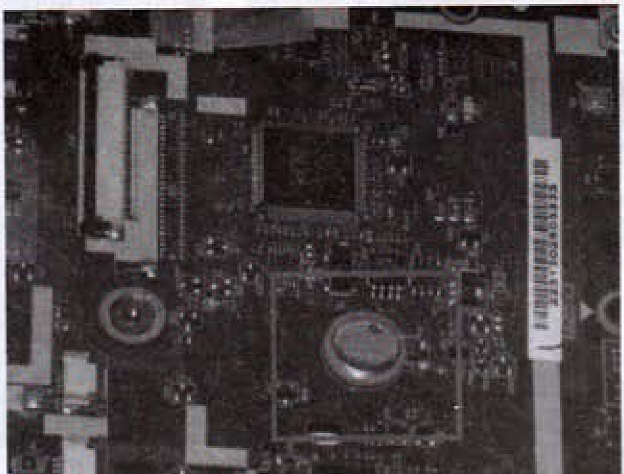


ကနဦး PC MotherBoard များတွင် SATA Drive များသုံးထားပါက Disable ပြောင်းသွားတတ်ပါတယ်။ ထိုအခါ SATA Drive Setting ကိုဝင်ရောက်ရှာဖွေပြီး Enable ပြောင်းမှသာ SATA Drive (Harddisk, DVD Drive) တွေကိုသိပါလိမ့်မယ်။

ဒုတိယနည်းကတော့ BIOS/CMOS ကို လျှပ်စစ်ပေးထားတဲ့ Battery ကိုခဏဖြုတ်ထားလိုက်တာပါ။ ယခုနည်းကို ပိုမိုအသုံးများပါတယ်။ လုပ်ဆောင်ရလွယ်ကူသလို၊ ပြဿနာလည်းနည်းပါတယ်။ လုပ်ဆောင်ရမှာကတော့ အဆိုပါ Battery ကိုဖြုတ်လိုက်ပြီး အမှတ်စဉ် ၁ မှ ၁၀ ထိမှန်မှန်ရေတွက်ကာ ပြန်တပ်လိုက်လျှင်ရပါပြီ။

Laptop တွေမှာလည်းအထက်ပါအတိုင်းပြုလုပ်ရမှာပဲဖြစ်ပါတယ်။ ဖြုတ်တပ်ဖို့ခက်ခဲတာကတော့ Laptop တွေရဲ့ထုံးစံပါ။ အောက်ဖက်မှပုံတွေကတော့ Laptop မှ BIOS/CMOS Battery တွေရဲ့ပုံတွေပဲဖြစ်ပါတယ်။

တတိယနည်းဖြစ်တဲ့ Software ကိုသုံးပြီးဖြေရှင်းတာကတော့ အသက်သာဆုံးနည်းဖြစ်ပေမယ့် Password Clear Software ဟာရှားပါးပါတယ်။ စာရေးသူသုံးတဲ့ Software မှာတော့ BIOS/CMOS Password ကိုဖော်ပြပေးတဲ့ အမျိုးအစားဖြစ်ပါတယ်။ နောက်ပိုင်းတွင်အသေးစိတ်ရှင်းပြထားပါတယ်။



နံပတ်(၃)

LogIn Password ပိတ်ထားခြင်း

Windows OS အတွင်းအဆင့်ဆင့်ဝင်ရောက်ပြီးသွားတဲ့အခါမှာတော့ Windows စတင်သုံးနိုင်ရန် သတ်မှတ် User တွေသာသုံးခွင့်ရှိဖို့ LogIn Password ကိုပိတ်ထားပြန်ပါတယ်။ ဟာ အတွင်းဝင်ရောက်ဖို့ နောက်ဆုံးတံခါးပေါက်ဖြစ်ပါတယ်။ Security Sytem ကိုသုံးမျိုးသုံးစား အသုံးပြုကြပါတယ်။

Desktop PC တွေမှာတော့သာမန်သုံး Key Type Password ကိုသာပေးထားပါတယ်။ ယခုနှစ်အတွင်း ထွက်ပေါ်လာတဲ့နောက်ဆုံးပေါ် Laptop တွေမှာတော့ Finger Print နဲ့ Face Recognition ကိုသုံးလာကြပါတယ်။ အဆိုပါ Security နည်းတွေနဲ့ LogIn ကိုကာကွယ်ထားကြပါတယ်။

စာရေးသူသုံးသပ်ထားသည်ကိုလေ့လာကြည့်ပါဦး။ အဆိုပါ တွေအကြောင်းစာရေးသူမွှေနှောက်လေ့လာခဲ့ပါတယ်။ ယခုဆိုလိုချက်တွေဟာ စာရေးသူရဲ့အာဘော်သာဖြစ်ပါတယ်။

Finger Print နဲ့ Face Recognition တွေတည်ဆောက်ထားပုံကိုဦးစွာတင်ပြပါ့မယ်။ Finger Print ကတော့ အသုံးပြုသူထည့်သွင်းထားတဲ့လက်ဗွေရာတွေကိုမှတ်ထားပြီး ထပ်တူညီတဲ့လက်ဗွေရာတွေ့ရှိမှသာစက်ကို ပေးသုံးပါ့မယ်။

Face Recognition ကလည်းအဆိုပါအတိုင်းပါပဲ။ မျက်လုံး၊ မျက်ခုံး၊ နှာခေါင်းထိပ်နှင့် အပေါ်နှုတ်ခမ်းအလယ်အကွေးထိပ်များကိုမှတ်ထားပြီး ထပ်တူညီမှုရှိမှသာ သုံးခွင့်ပြုပါတယ်။

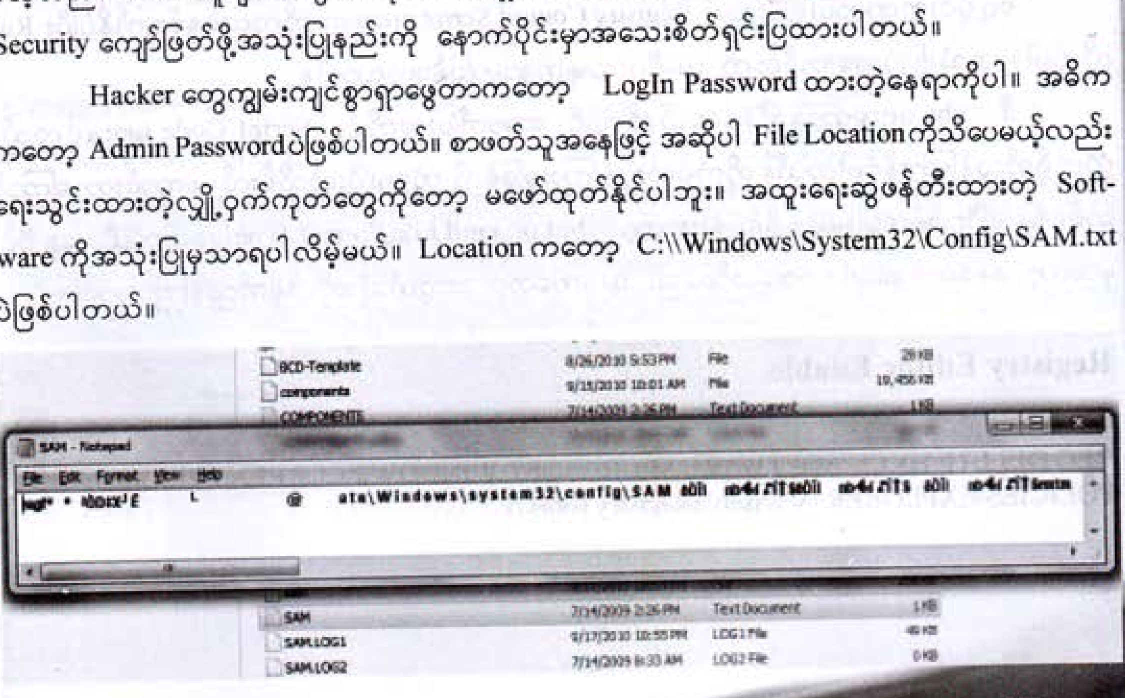
စာဖတ်သူအနေဖြင့် အလုံခြုံဆုံးရှိသွားပြီလို့ ယူဆနေပြီထင်ပါတယ်။ မယူဆပါနဲ့ဦး။ အားနည်းချက်ရှိနေတာကိုလေ့လာကြည့်ပါဦး။ အဆိုပါ Bio Security နစ်ခုကိုထည့်သွင်းသတ်မှတ်တဲ့အခါမှာ ကိုယ်ပိုင်ရပ်တည်မှုဖြင့်သီးသန့်သတ်မှတ်ကာ အသုံးမပြုပဲ Windows OS ရဲ့ LogIn ရပ်တည်နေမှုကိုမှီခိုထားပါတယ်။

ရှင်းရှင်းပြောရလျှင် LogIn Password နှင့်ထပ်တူစတင်စေပြီး Password Keys များကိုမနှိပ်လိုတဲ့အခါမှာ Finger Scanner ပေါ် လက်ဗွေရာပေးခြင်း၊ ဒါမှမဟုတ် အသင့်ပါ WebCam ဖြင့်မျက်နှာကို ဖတ်စေပြီးဝင်ရောက်စေတာပါ။ တစ်ခုတည်းသီးသန့်လုံခြုံရေးစနစ်မထားရှိပါဘူး။

ဒီလိုအားနည်းချက်ကြောင့် LogIn Password ကို Hack Software သုံးပြီးကျော်ဖြတ်လိုက်တာနဲ့ Windows အတွင်းအလွယ်ဝင်ရောက်နိုင်ပါပြီ။ ပစ္စည်းရောင်းကောင်းအောင် ထည့်ထားတဲ့အဆင့်သာရှိနေတာကို စာဖတ်သူများနားလည်လောက်ပါပြီ။ ဘာပဲပြောပြော လူကြားထဲမှာ မိမိလျှို့ဝှက်နံပတ်ကိုရိုက်နေစရာမလိုတာကတော့ လူရိုန်တာပေါ့။

LogIn Security ကိုကျော်ဖြတ်နိုင်တဲ့ Software တွေများစွာရှိနေသော်လည်း စာရေးသူလက်တွေ့စမ်းသပ်ချက်အရ Hiren's Boot CD ကိုသဘောအကျဆုံးဖြစ်ပါတယ်။ လိုင်စင်ဖြင့်သုံးရတာဖြစ်ပေမယ့်လည်း စာဖတ်သူများအတွက် လိုင်စင်ဗားရှင်း Hiren Boot CD ကိုထည့်ပေးထားပါတယ်။ LogIn Security ကျော်ဖြတ်ဖို့အသုံးပြုနည်းကို နောက်ပိုင်းမှာအသေးစိတ်ရှင်းပြထားပါတယ်။

Hacker တွေကျွမ်းကျင်စွာရှာဖွေတာကတော့ LogIn Password ထားတဲ့နေရာကိုပါ။ အဓိကကတော့ Admin Password ပဲဖြစ်ပါတယ်။ စာဖတ်သူအနေဖြင့် အဆိုပါ File Location ကိုသိပေမယ့်လည်း ရေးသွင်းထားတဲ့လျှို့ဝှက်ကုတ်တွေကိုတော့ မဖော်ထုတ်နိုင်ပါဘူး။ အထူးရေးဆွဲဖန်တီးထားတဲ့ Software ကိုအသုံးပြုမှသာရပါလိမ့်မယ်။ Location ကတော့ C:\\Windows\System32\Config\SAM.txt ပဲဖြစ်ပါတယ်။



နံပတ်(၄)

ပိတ်ဆို့ထားခြင်း

Windows OS အတွင်းအဆင့်ဆင့်ဝင်ရောက်ခဲ့သော်လည်း System Control လက်နက်တွေဖြစ်တဲ့ Registry Editor, Task Manager, Run Box, Commad Prompt တွေသုံးခွင့်မရတဲ့အတွက် နောက်ဆုံးရောက်မှ လက်လျှော့လိုက်မှာလား။

စာဖတ်အနေဖြင့်ရှေ့ပိုင်းကဏ္ဍတွေကို ဖတ်ရှုခဲ့တာနားလည်တယ်ဆိုခဲ့လျှင် ဘာလို့ပြန်မဖွင့်နိုင်ရမှာလဲ။ ဒီလိုဆိုလျှင် ပြန်မေးမယ်ထင်တယ်နော်။ Registry Editor ကိုပြန်ဖွင့်ဖို့ Gruop Policy လည်းသုံးခွင့်မရ။ တစ်ခုခုထဲဝင်ဖို့သုံးရမယ့် Run Box လည်းမရှိ။ Commad Prompt ကလည်းဖွင့်လို့မရ။ ဘာနဲ့ထိန်းချုပ်ပြီးညွှန်ကြားချက်ပေးရမှာလဲပေါ့။

တည်ရှိရာ Location အတွင်းထဲကိုဝင်ရောက်ဖွင့်ကြည့်ပါ။ မရလျှင်တော့ မရလို့ပေါ့နော်။

ယခုကဲ့သို့လမ်းဆုံးနောက်နေလျှင် ကျန်ရှိသောနည်းလမ်းကတော့ NotePad မှာ Script Program တစ်ပုဒ်ရေးပြီး Run လိုက်ယုံပေါ့။ အကောင်းဆုံးအတွက် သိမ်းဆည်းပေးရမယ့်ဖိုင်ပုံစံကတော့ .vbs ပဲဖြစ်ပါတယ်။ မကြာခဏယခုလိုအသုံးပြုနေရသူတွေကတော့ အောက်ပါ Script Program လေးကို USB Stick ထဲသိမ်းထားသင့်ပါတယ်။

ရှေ့ပိုင်းကဏ္ဍမှာပါရှိပြီးသား Registry Control Script program ကိုကလစ်နှစ်ချက်နှိပ်ပြီး Run လိုက်ပါ။ အသုံးပြုပုံအသေးစိတ်ကို အဆိုပါစာမျက်နှာမှာပြန်လေ့လာပါ။

ဒီ .vbs ရေးရတာခက်နေတယ်ဆိုလျှင် အောက်ပါအတိုင်း Script Code များနှင့်လည်း တိုက်ရိုက်ညွှန်ကြားနိုင်ပါတယ်။ တိုက်ရိုက်ညွှန်ကြားမှုဖြစ်လို့ တွဲရေးပြီးတွဲသိမ်းလို့မကောင်းတာကြောင့် တစ်ခုစီရေးပြီးသိမ်းရပါမယ်။ ဖိုင်ပုံစံကတော့ **.bat or .cmd** File Format Type ဖြစ်ပါတယ်။ ရှေ့ပိုင်းမှာတော့ စနစ်တကျရေးပြထားသော်လည်း ယခုကတော့ အလွယ်သုံးတိုက်ရိုက်ညွှန်ကြားမှာပါ။

Registry Editor Enable

```
@echo off
REG DELETE HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\
POLICIES\EXPLORER /V DisableRegistryTools /f
```

Run Box Enable

@echo off
REG DELETE HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\EXPLORER /V NoRun /f

Task Manager Enable

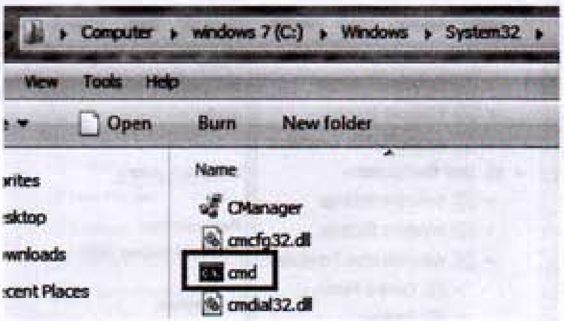
@echo off
REG DELETE HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM /V DisableTaskMgr /f

Task Manager Enable

@echo off
REG DELETE HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM /V DisableTaskMgr /f

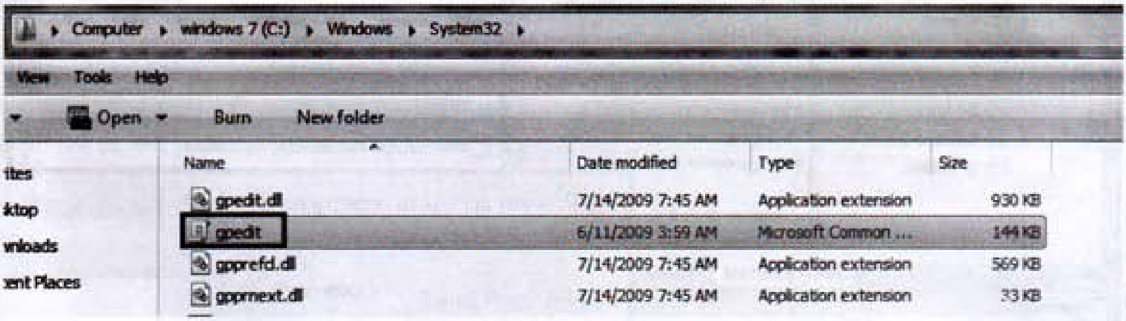
Command Prompt Open

C:\Windows\System32\cmd.exe



Group Policy Open

C:\Windows\System32\gpedit.msc

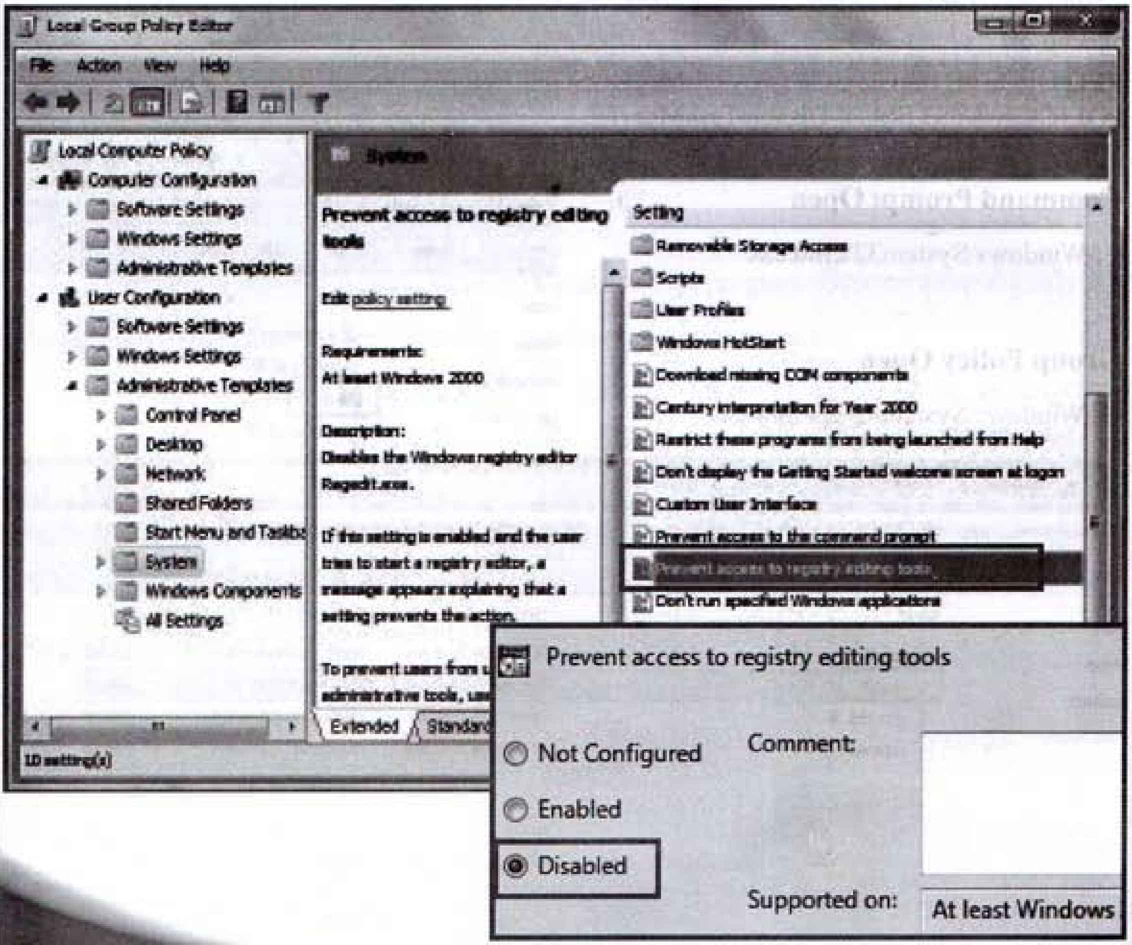


Registry Editor ကို Group Policy မှဝင်ဖွင့်ခြင်း

စာဖတ်သူအနေဖြင့် Registry Editor ဖွင့်နိုင်ဖို့နောက်တစ်နည်းစမ်းကြည့်သင့်ပါသေးတယ်။ C:\Windows\System32\gpedit.msc ကိုဝင်ရောက်ပြီးရှာဖွေကာ ကလစ်နှစ်ချက်ဆင့်နှိပ်ပြီးဖွင့်ကြည့်ပါ။ သာမန်အားဖြင့် မပိတ်ထားတတ်ကြပါဘူး။ ပွင့်လာခဲ့လျှင် Registry Editor ကိုဖွင့်နိုင်ပါပြီ။

အတွင်းသို့ဝင်ရောက်ရမယ့်လမ်းကြောင်းကတော့ ဘယ်အခြမ်းတွင် User Cofiguration > Administrative Templates>System ထိရောက်အောင်သွားနှိပ်ပါ။

အဆိုပါ System ၏ညာဘက်ခြမ်းတွင် Prevent access to registry editing tools ကိုရှာဖွေပြီး ကလစ်နှစ်ချက်နှိပ်လိုက်ပါ။ ပေါ်လာသော Box တွင် Disabled ကိုရွေးပြီး OK Button နှိပ်ထွက်လိုက်ပါ။ Registry Editor ပိတ်ထားလိုလျှင် Enabled ကိုရွေးပြီး ယခုနေရာမှပိတ်ထားနိုင်ပါတယ်။



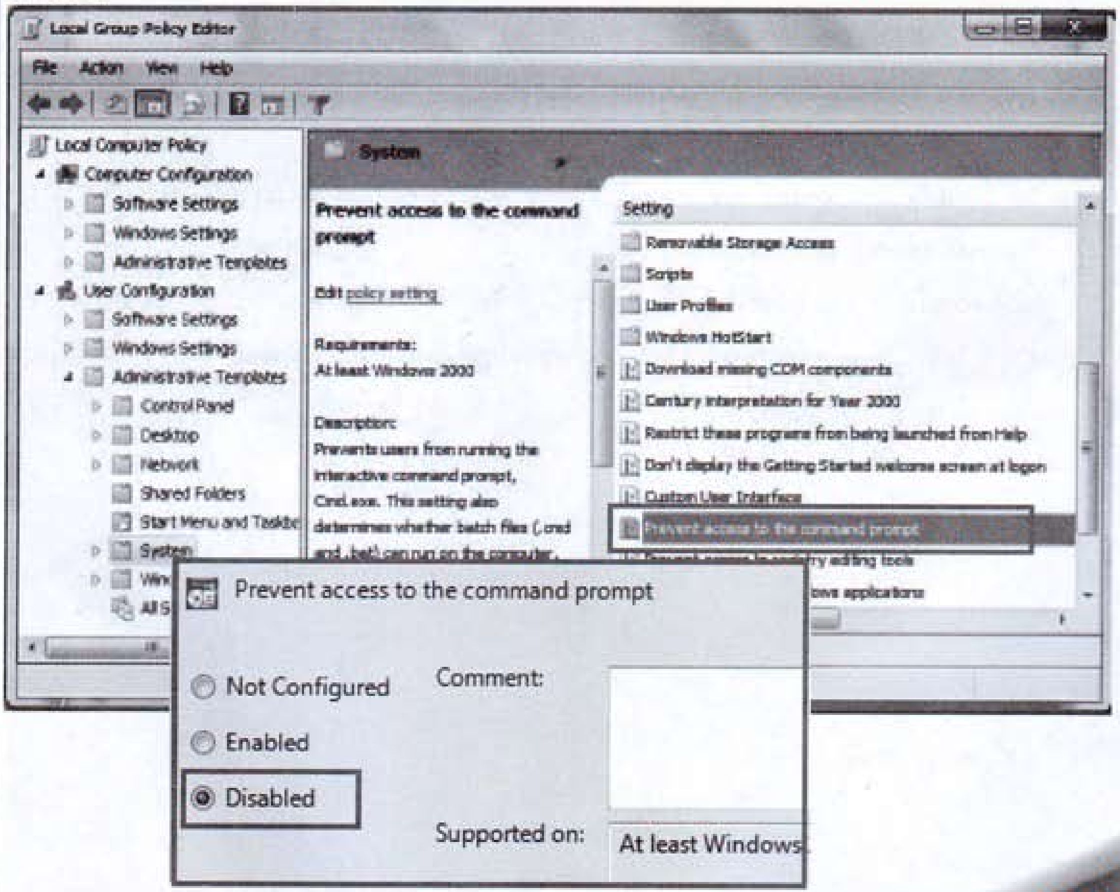
Command Prompt ကို Group Policy မှဝင်ဖွင့်ခြင်း

စာဖတ်သူအနေဖြင့် Command Prompt ဖွင့်သုံးနိုင်ဖို့ Group Policy မှာပင်ပြုလုပ်နိုင်ပါတယ်။ C:\Windows\System32\cmd.exe ကိုဝင်ရောက်ပြီးရှာဖွေကာ ကလစ်နှစ်ချက်ဆင့်နှိပ်ပြီးဖွင့်ကြည့်ပါဦး။ ပုံမှန်အားဖြင့် မပိတ်ထားတတ်ကြပါဘူး။

အတွင်းသို့ဝင်ရောက်ရမယ့်လမ်းကြောင်းကတော့ ဘယ်အခြမ်းတွင် User Cofiguration > Administrative Templates>System ထိရောက်အောင်သွားနိုပ်ပါ။

အဆိုပါ System ၏ညာဘက်ခြမ်းတွင် Prevent access to the command Prompt ကိုရှာဖွေပြီး ကလစ်နှစ်ချက်နှိပ်လိုက်ပါ။ ပေါ်လာသော Box တွင် Disabled ကိုရွေးပြီး OK Button နှိပ်ထွက်လိုက်ပါ။

Command Prompt ကိုအသုံးမပြုစေလိုတဲ့အခါမှာလည်း Enabled ကိုရွေးထားပြီး ပိတ်ထားနိုင်ပါတယ်။



Honest Hacker တစ်ယောက်အနေဖြင့် စွယ်စုံ၊ ဘက်စုံတတ်ကျွမ်းထားရန်လိုအပ်ပါတယ်။ အဓိကအကျဆုံးတတ်ကျွမ်းထားရမယ့်နည်းပညာတွေကတော့

၁။ Windows Operating System Logic

၂။ Operating System Controller

၃။ Pascal, C, C++, C# Programming

၄။ Script, Java Script, VB Script, HTML Script Programming

၅။ Computer Service (A+)

၆။ Network System Technology

၇။ PHP, HTML, SQL Server, ASP Server (Database)

၈။ DOS Command

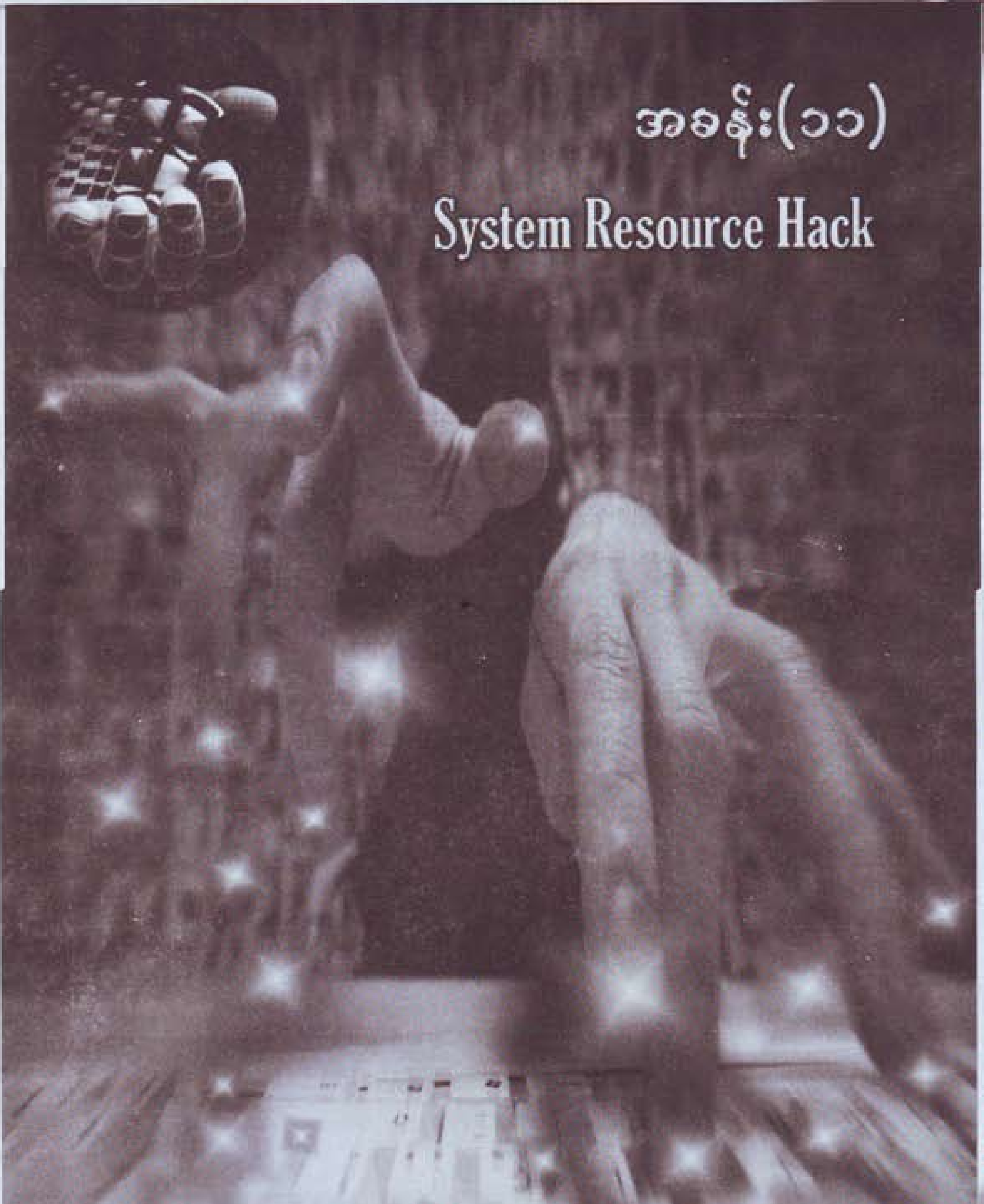
၉။ SpyWare, BackDoor, Trojan Process

အထက်ပါနည်းပညာများကိုလေ့လာဖို့အတွက် မလွယ်ကူဟုထင်ရသော်လည်း ဇွဲနပဲကြီးကြီး လေ့လာလျှင်ရနိုင်ပါတယ်။

ယခုစာအုပ်ကတော့ မိမိကိုင်ကွယ်ရမယ့်ကွန်ပျူတာတစ်လုံးအတွက်တော့ အသုံးချစရာတွေကို အသုံးတည့်ဖို့ဦးတည်ပြုစုထားတဲ့အတွက် Honest Hacker တစ်ယောက်အတွက်တော့ လက်သုံးစာအုပ်လေးဖြစ်လာမှာပါ။

အခန်း(၁၁)

System Resource Hack



goldenshadetech@gmail.com
http://thanhtikegs.weebly.com

System Resource ကို Hacking လုပ်လေ့လာခြင်း

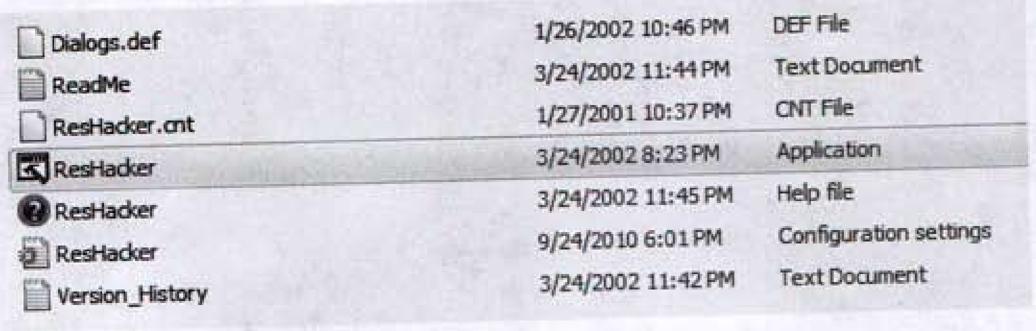
Honest Hacker တွေအတွက် Resource ဆိုတဲ့ System Controller File တွေရဲ့အရင်းအမြစ်တွေကို ထိုးဖောက်လေ့လာနိုင်ဖို့လိုအပ်ပါတယ်။ တည်ဆောက်မှုတစ်ခုရဲ့ အခြေအမြစ်တွေကိုလေ့လာနိုင်တဲ့ ပညာရှင်တွေကိုပြပါဆိုလျှင် Honest Hacker တွေကိုပြရပါမယ်။ စာရေးသူယခုတင်ပြမယ့်ကဏ္ဍကို ကွန်ပျူတာပညာရပ်အားအထူးပြုလေ့လာနေသူများအတွက် အလွန်အဖိုးတန်ပါတယ်။

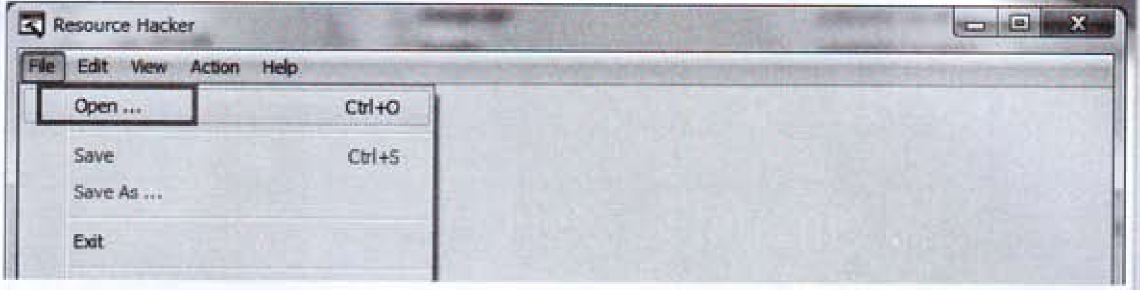
စာရေးသူအနေဖြင့် အပြည့်စုံဆုံးဖြစ်အောင်တင်ပြချင်ပေမယ့် အကြောင်းအမျိုးမျိုးကြောင့် တင်ပြခွင့်မရခဲ့ပါဘူး။ ဒါ့ကြောင့် http://thanhtikegs.weebly.com မှတစ်ဆင့် ဆွေးနွေးလိုသည်များရှိလျှင် ဆွေးနွေးနိုင်ပါတယ်။

ယခုအခန်းကဏ္ဍကိုလေ့လာနိုင်ရန် လိုအပ်သော Resource Hacker Program ကိုလည်း စီဒီနှင့်အတူထည့်ပေးထားပါတယ်။ Install လုပ်ရန်မလိုအပ်ပဲ တိုက်ရိုက်ကလစ်နှစ်ချက်နှိပ် အသုံးပြုနိုင်တဲ့ အတွက် အိပ်ဆောင် Program လေးဖြစ်လာမှာပါ။

စာဖတ်သူထိုးဖောက်လေ့လာနိုင်တဲ့ System File Type တွေကတော့ .exe, .dll, .cpl, .scr, .res နှင့် အခြားပုံစံတို့ဖြစ်ပြီး၊ ၎င်းတို့ရဲ့တည်ဆောက်ပုံတွေကိုအသေးစိတ်လေ့လာနိုင်ပါတယ်။

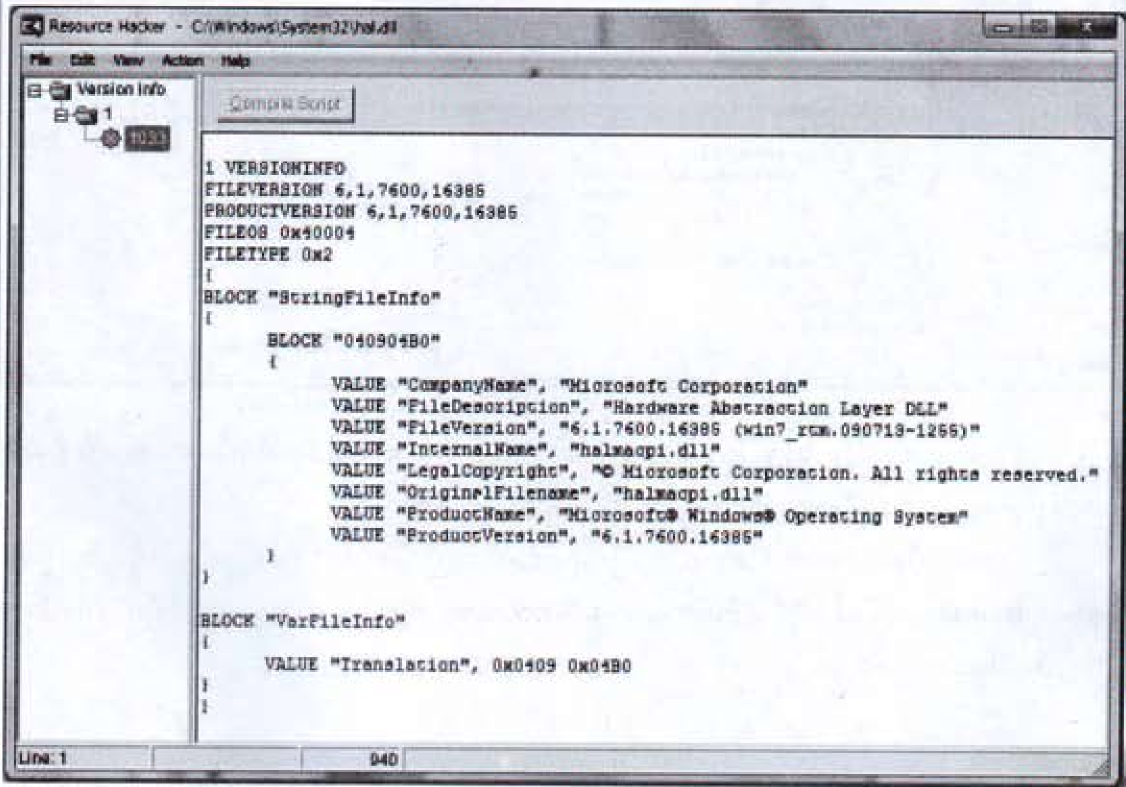
ပထမဦးစွာ hal.dll ဆိုတဲ့ System File ကိုထိုးဖောက်လေ့လာပါ့မယ်။ hal.dll က Windows စတင်လည်ပတ်ရန် မရှိမဖြစ် System File ဖြစ်ပါတယ်။ ဒါ့ကြောင့် Resource Hacker Program ကိုဖွင့်ဖို့အတွက် စီဒီအတွင်းမှ Hacking Program Folder > ResHack Folder > ResHacker.exe ကိုကလစ်နှစ်ချက်နှိပ်ဖွင့်လိုက်ပါ။



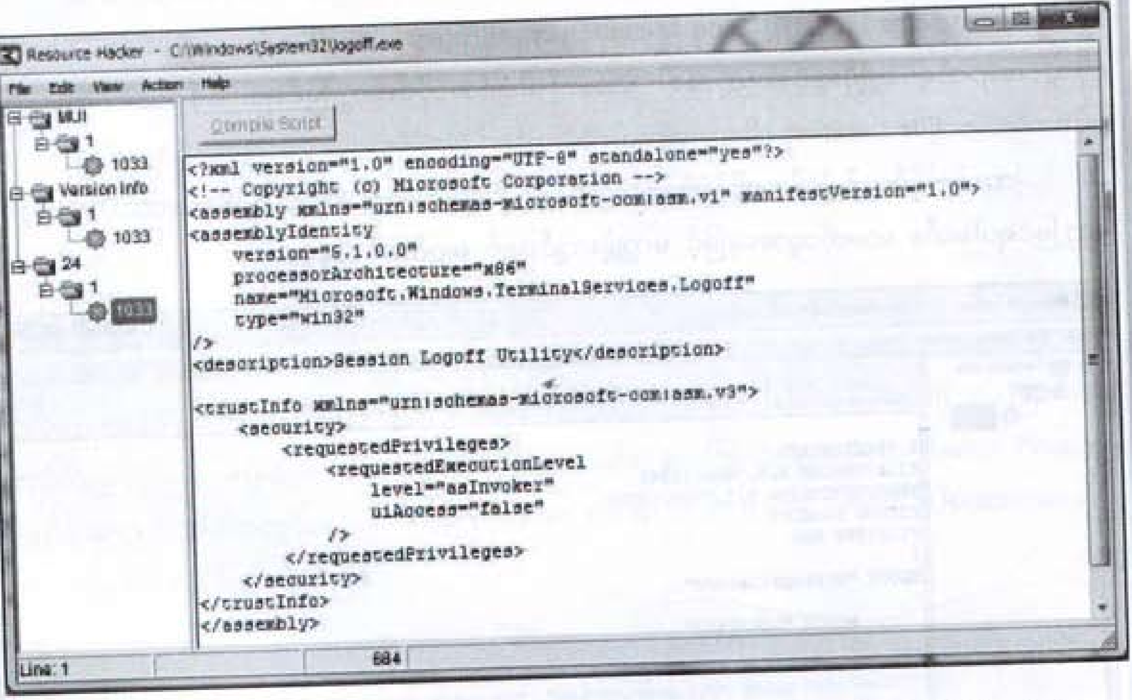


အသစ်စတင်သည်မို့ File Menu>Open ကိုဖွင့်ကာ C:\Windows\ System32\hal.dll ကိုသွားရောက်ရှာဖွေပြီးဖွင့်ပေးတဲ့အခါ အောက်ပါပုံစံအတိုင်းတွေ့မြင်ရပါလိမ့်မယ်။ Title တွင် ဖွင့်ထားသော File Location ကိုတွေ့နေရပါလိမ့်မယ်။

ဘယ်ဘက်တွင် ပုံပါအတိုင်းအဆင့်လိုက်ဝင်ဖွင့်သွားတဲ့အခါ hal.dll ရဲ့ Resource Data တွေကို တွေ့မြင်ရပါမယ်။ စာဖတ်သူအနေဖြင့် မကျွမ်းကျင်လျှင် မပြင်ဆင်ပါနှင့်။

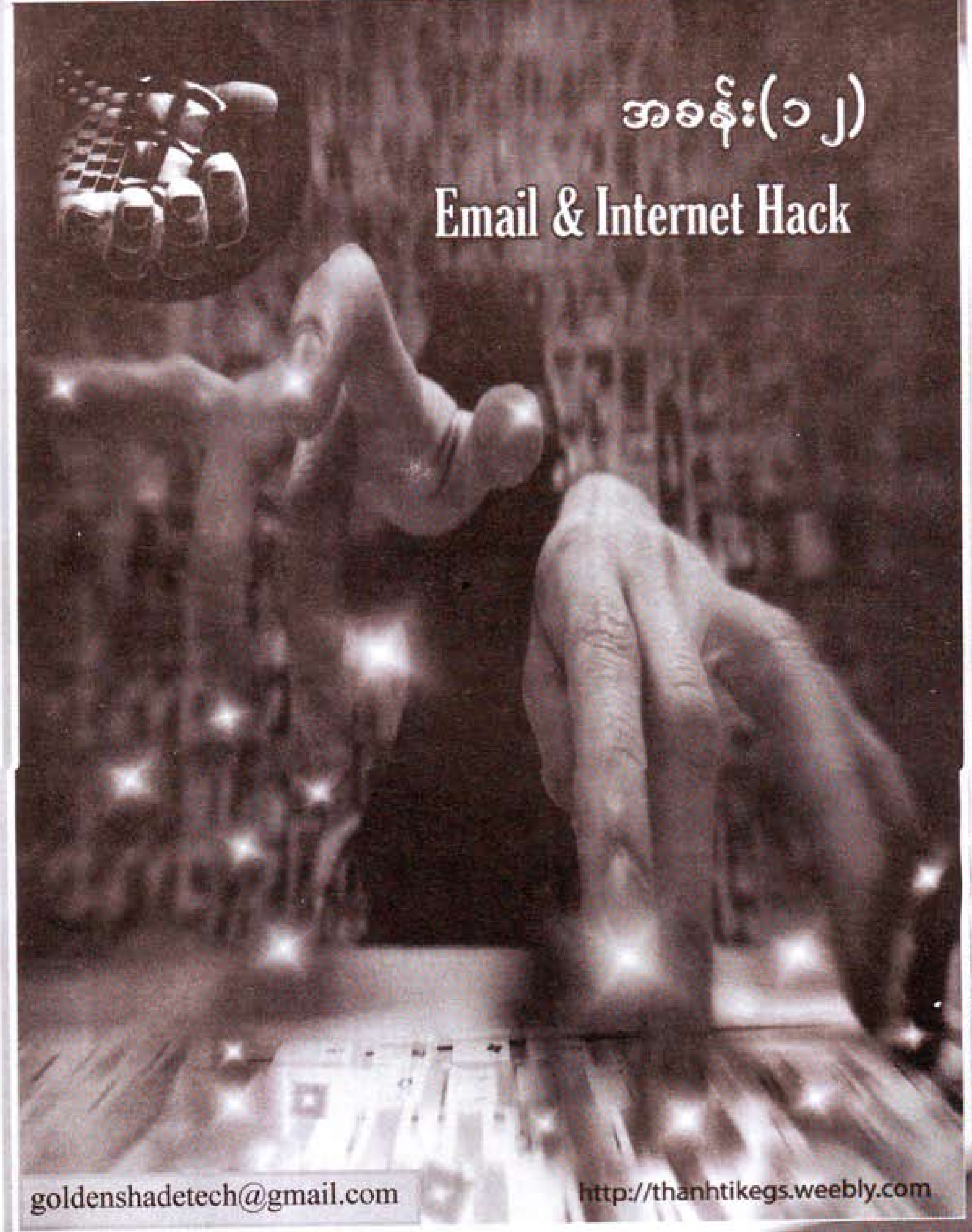


Logoff ဆိုတာလက်ရှိသုံးနေသော စနစ်အတွင်းမှခေတ္တပြန်ထွက်ပြီး User Account ကိုပြန်ဝင်တဲ့အခါမှာသုံးတဲ့စနစ်တစ်ခုဖြစ်ပါတယ်။ Program သမားတွေအတွက်ကတော့ ယခုကဲ့သို့ ထိုးဝင်လေ့လာနိုင်ခြင်းဟာ တကယ့်အဖိုးတန်တွေပါ။ သာမန်သုံးသူတို့ကတော့ လေ့လာတယ်ဆိုယုံပဲ ရှိပါလိမ့်မယ်။ စာရေးသူအနေဖြင့်လည်း မတူညီတဲ့စာဖတ်သူတွေကြားထဲ အန္တရာယ်ရှိလာမည်ကိုဆိုး၍ အသေးစိတ်မရှင်းပြရတာပါ။



သာမန်စာဖတ်သူအနေနှင့် ဘာတွေလုပ်နိုင်သလဲဆိုတာတော့အနည်းသိချင်ပါလိမ့်မယ်။ ရှိသမျှ ဆော့ဖ်ဝဲများမှ Icon, Cursor, Bitmap တွေကိုပြောင်းလဲနိုင်ပါတယ်။

Menu အုပ်စုရှိ Action Menu ကိုဖွင့်ပြီး ပြောင်းလိုသည်ကိုနှိပ်ကာ မိမိပြောင်းလဲလိုသော Icon, Cursor, Bitmap တစ်ခုခုနှင့်ချိန်းနိုင်ပါတယ်။ အဓိကကတော့ File အရွယ်အစားတူညီပြီး၊ File Type ပါတူညီရပါမယ်။


အခန်း(၁၂)
Email & Internet Hack
goldenshadetech@gmail.com
http://thanhtikegs.weebly.com

Email များဖောက်ထွင်းမှုမှကာကွယ်ရန်

Email ဆိုတဲ့ အင်တာနက်သုံးစာပို့စနစ်မှာ လိုင်စင်ဖြင့် အခကြေးငွေပေးကာဝယ်ယူခြင်းနှင့် အခမဲ့ Web Mail တွေကိုရယူခြင်းတို့ရှိကြပါတယ်။ လိုင်စင်ဖြင့်ဝယ်ယူလျှင် စိတ်ချရမှုရှိသော်လည်း လူငယ်တွေကြားမှာတော့ Web Mail တွေကိုသာပိုသုံးကြပါတယ်။

Email တွေထဲမှာ နာမည်ရှိဆုံးကတော့ Google Mail ဖြစ်ပြီး၊ မြန်မာနှင့်အာရှမှာအအောင်မြင်ဆုံး ဖြစ်ပါတယ်။ Yahoo Mail ကိုလည်းအသုံးများကြပါတယ်။ စာရေးသူထံမကြာခဏမေးမြန်နေကြ တာကတော့ Gmail -GTalk ကိုထိုးဖောက်လို့ရသလား၊ ထိုးဖောက်မခံရဖို့ ဘယ်လိုကာကွယ်ကြမလဲ စတာတွေအမေးများကြပါတယ်။

ပထမဦးစွာ Gmail -GTalk ကိုဘယ်လိုထိုးဖောက်နိုင်တယ်ဆိုတာရှင်းပြပါ့မယ်။ Gmail Account တွေဟာ Web Mail ဖြစ်လို့ Google Web Server ထဲမှာအလွယ်ရှိနေပါတယ်။ ဒီလိုပြောလို့ အလွယ်ဝင်ယူလို့ရတယ်မထင်ပါနဲ့နော်။ အတော်ပင်လုံခြုံအောင်စီမံထားပါတယ်။ အဓိကပြဿနာ ကတော့ တန်ကြေးပေးဝယ်သုံးရတဲ့ License Mail တွေကဲ့သို့ လုံခြုံရေးစနစ်မတင်းကျပ်တာပါပဲ။

ဥပမာတွေဖြင့်ရှင်းပြရလျှင်– စာဖတ်သူရဲ့ Mail Account အတွက်လုံခြုံရေးနံပတ်ကိုအခြားသူ တစ်ယောက်ယောက်ကလိုချင်လျှင် နည်းလမ်း ၆ မျိုးနဲ့ရယူပါလိမ့်မယ်။

၁။ အယောင်ဆောင် Website မှတစ်ဆင့် ရယူခြင်း

အင်တာနက်ဆိုတာ ပင်လယ်မကျ၊ သမုဒ္ဒရာကြီးမက ကျယ်ပြန့်လှသလို ၄င်းပေါ်မှာလည်း အယောင်ဆောင် Spy Website တွေများစွာရှိနေပါတယ်။ အဆိုပါ Spy Website တစ်ခုခုကို ဝင်ရောက်တဲ့ အခါမှာ စာဖတ်သူအကြိုက် တစ်ခုခုကိုဖန်းပြပြီး Mail Account နှင့် Mail Password ကို တောင်းဆိုပါ လိမ့်မယ်။ ဖောင်ထွင်းခံရဖို့ အစပြုပါပြီ။

၂။ အများသုံး Cyber Cafe နေရာတွင်သုံးခဲ့ခြင်း

စာဖတ်သူအနေဖြင့် Cyber Cafe တွေမှာသုံးပြီး Gmail, GTalk တွေကို အစအဆုံး ပိတ်ပြီးထပြန် ခဲ့ပါတယ်။ ဒါပေမယ့် စက်ကတော့ပွင့်နေခဲ့မယ်လေ။ စာဖတ်သူကြားဖူးလား Cookies ဆိုတာ။ အမှန်ပေါ့ဗျာ။ အဆိုပါ Cookies ကိုဘာသာပြန်ဆိုနိုင်ခဲ့လျှင် စာဖတ်သူရဲ့ LogIn Password ကို ရသွားပါပြီ။

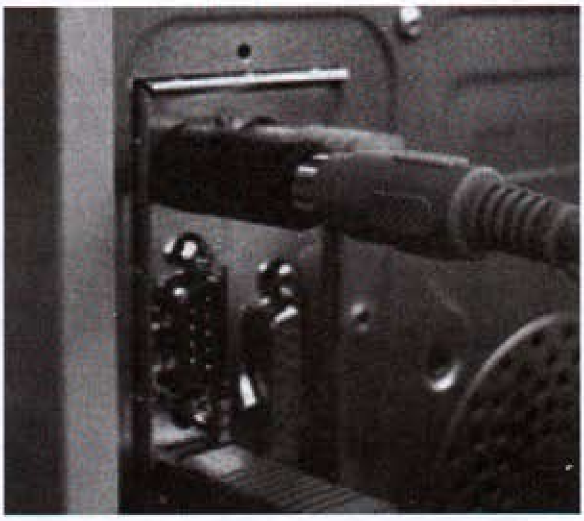
၃။ KeyLogger Software ကိုထည့်ထားပြီးရယူခြင်း

စာဖတ်သူကြားဖူးလား KeyLogger Software တွေကိုပေါ့။ တကယ်ရှိတာပါ။ အလွယ်လည်းရနိုင်သလို အခကြေးငွေပေးပြီးလည်းဝယ်ယူနိုင်ပါတယ်။ စာဖတ်သူကွန်ပျူတာအတွင်း KeyLogger Software တစ်ခုခုရှိနေခဲ့လျှင် စာဖတ်သူ Keyboard ကိုသုံးပြီး ရိုက်လိုက်သမျှစာလုံးတွေကိုမှတ်သားထားလိုက်ပါတယ်။ ထည့်သွင်းသူ Admin ကအလွယ်ပြန်ဖွင့်ကြည့်ပြီးစစ်ဆေးလိုက်သည်နှင့် စာဖတ်သူရိုက်ခဲ့သမျှ Key တွေကိုသိသွားပါပြီ။

၄။ KeyLogger Hardware ကိုထည့်ထားပြီးရယူခြင်း

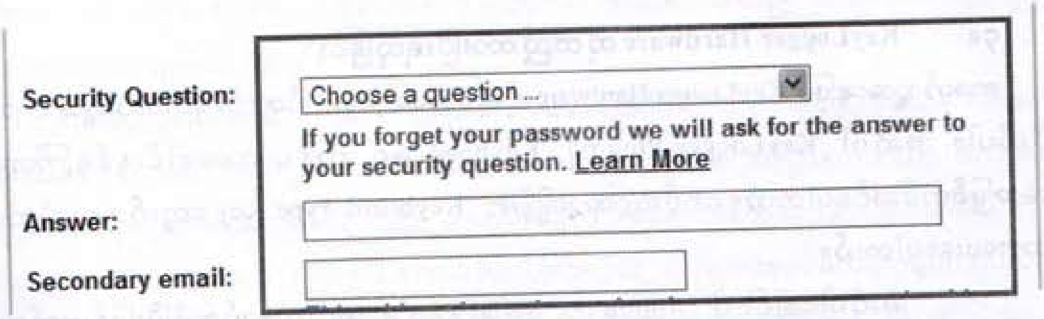
စာဖတ်သူအနေဖြင့် KeyLogger Hardware ဆိုလိုမယုံတော့ဘူးထင်တယ်။ ရှိပါတယ်ဗျာ။ ရဲရဲသာယုံလိုက်ပါ။ အဆိုပါ KeyLogger Plug ကို Keyboard နှင့် ကွန်ပျူတာခေါင်းနှစ်ခုကြားမှာကြားခံအဖြစ်တပ်ဆင်ရပါတယ်။ တပ်ဆင်ထားချိန်မှာ Keyboard Type Key တွေကိုအလွယ်တကူမှတ်သားပေးနေပါတယ်။

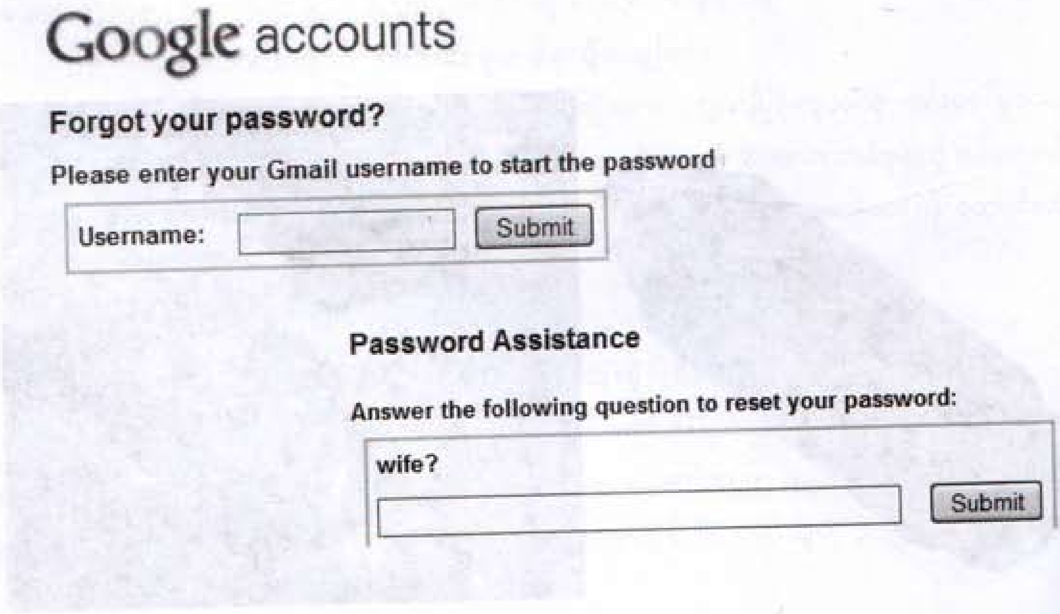
အဆိုပါခေါင်းကို Admin က Serial Port မှာအလွယ်တပ်ဆင်ပြီးပြန်လည်ရယူနိုင်ပါတယ်။



၅။ Password မေ့သွားလို့ပါဆိုပြီး Hack သွားခြင်း

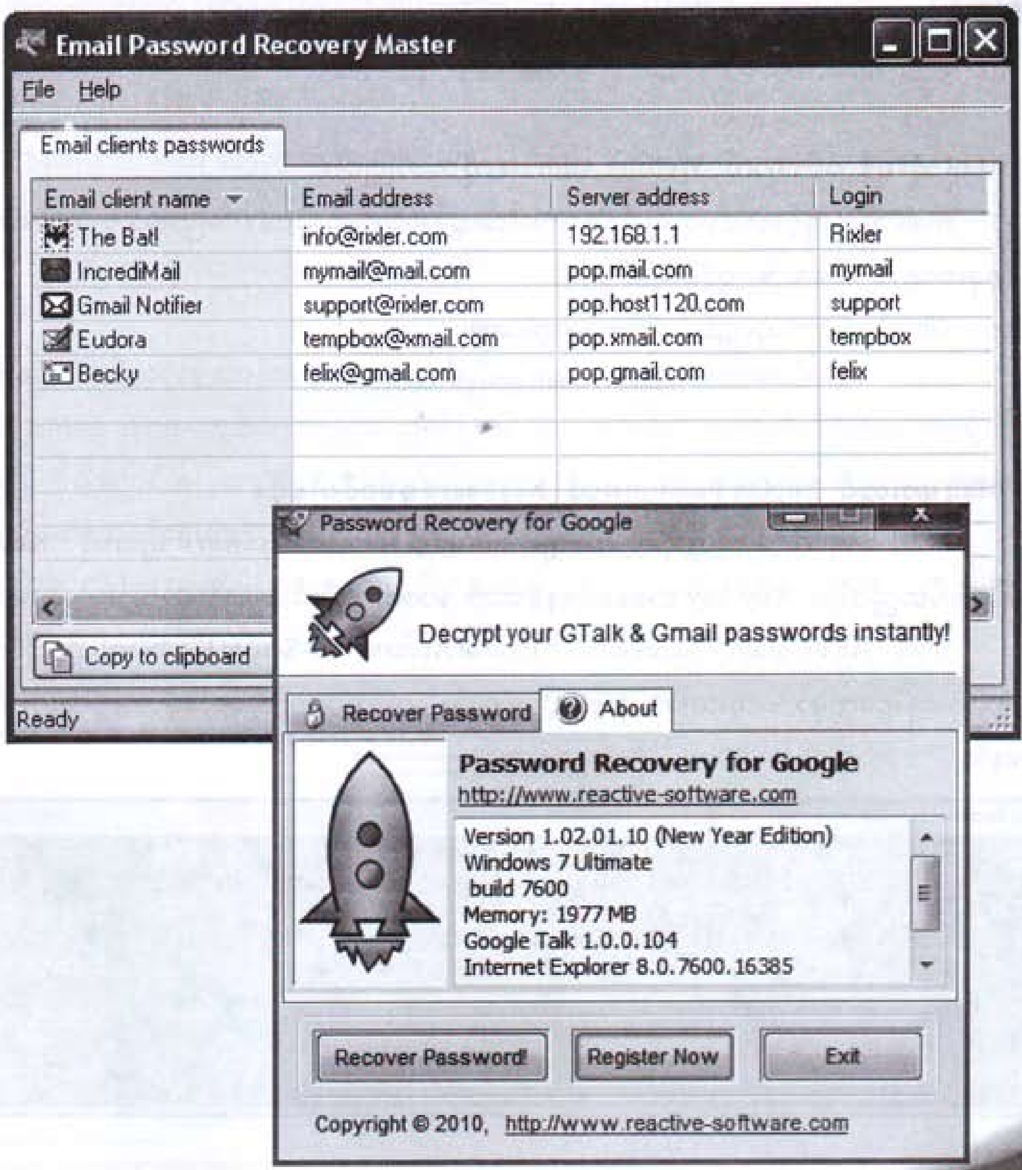
စာဖတ်သူရဲ့ Mail Password မေ့သွားတဲ့အခါ၊ Forget My Password ကိုနှိပ်ပြီး KeyLogger Password ကိုပြန်လည်တောင်းခံနိုင်ပါတယ်။ တစ်ခုတော့ရှိတယ်။ Server Admin ကမေးတဲ့ မေးခွန်းတွေကိုမှန်ကန်ဖို့တော့လိုပါတယ်။ Gmail မှာ မေးခွန်းတစ်ခုကို ပြန်လည်ကယ်ဆယ်နိုင်ရန် စတင်တည်ဆောက်စဉ်ကပင် မေးထားပါတယ်။ အဆိုပါမေးခွန်းရဲ့အဖြေကိုခန့်မှန်းဖြေဆိုပြီးရသွားသူတွေ များစွာရှိနေပါတယ်။





၆။ Software များသုံးပြီး Hack သွားခြင်း

အင်တာနက်အတွင်း Mail Password Recovery Software တွေကိုပလူပျံလောက်အောင် တွေ့နေရပါတယ်။ အလကားပေးတာရှိသလို၊ လိုင်စင်ဖြင့် အခပေးဝယ်ယူရတာတွေရှိပါတယ်။ စာရေးသူလည်း အလကားရတာလေးတွေရယူပြီးစမ်းသပ်ကြည့်သော်လည်း မပြောပုဆိုးပါပဲ။



Mail လုံခြုံရေးပြဿနာဖြေရှင်းနည်းလမ်းများ

ပထမဦးဆုံး Mail တွေကိုဘယ်လိုလုံခြုံအောင်လုပ်ရမယ်ဆိုတာကိုရှင်းပြပါ့မယ်။ အကောင်းဆုံး လုပ်ဆောင်စရာတွေကိုသာ နည်းလမ်းတကျရှင်းပြလိုက်ပါတယ်။ စာဖတ်သူအနေဖြင့် ကိုယ်ပိုင်ကွန်ပျူတာ သုံးသလို၊ အများသုံးကွန်ပျူတာတွေသုံးရတာလည်းရှိမှာပါ။ အောက်ပါနည်းလမ်းများကတော့ ဘယ်အချိန် ဘယ်ကွန်ပျူတာပဲသုံးသုံး ပြုလုပ်သင့်တာတွေပါ။ ဥပမာပြအနေဖြင့် အများသုံးသော GMail ကို ဦးတည်ရှင်းပြထားပေမယ့် အခြား Mail များတွင်လည်းသုံးစွဲနိုင်ပါတယ်။

၁။ Mail သုံးရန် ဝင်ရောက် Website Address ကိုသတိပြုပါ။

Mail ကိုသုံးခွင့်ပေးသော မိခင် Website အတွင်းမှသာဖွင့်သုံးပါ။ အခြားသော Website, Link တစ်ခုခုကနေ ဘယ်တော့မှ ဖွင့်မသုံးပါနှင့်။

ဥပမာ– Gmail အတွက်ဆိုလျှင်– www.google.com

https://mail.google.com

၂။ Mail များတွင် LogOn Password ကို Keyboard မှမဝင်ပါနှင့်။

Mail တွေကို သုံးဖို့ဖွင့်လိုက်လျှင် LogIn Name, Password များကို Keyboard သုံးပြီးရိုက်ထည့်ပါက Key Spy တစ်ခုခုရှိနေခဲ့သော် စာဖတ်သူရိုက်သမျှကိုမှတ်သွားပါလိမ့်မယ်။

Start > All Program > Accessories > Ease of Access > On-Screen Keyboard ကိုဖွင့်ပြီးသုံးပါ။ အများသုံးနေရာတွေမှာ အထူးသဖြင့်သုံးစွဲသင့်ပါတယ်။ ဘေးကနေကြည့်မှတ်နေတာကိုလည်း ဂရုစိုက်ဦးနော်။

၃။ Password ကိုမကြာခဏပြောင်းပေးပါ။

လျှို့ဝှက်နံပတ်ကိုအလုံခြုံဆုံးပေးလိုလျှင် အမည်တစ်ခုကို စာလုံးဘာသာပုံစံဖြင့်ပေးသင့်ပါတယ်။ ဥပမာ– စာဖတ်သူပေးလိုသောအမည်က ကျော်စွာ၂၀၁၀ ဆိုလျှင် 20ausmfpGm10 လို့ပေးလိုက်ပါ။

၄။ အရေးပါစာများကို ဖတ်ပြီး/ကူးယူပြီး တစ်ခါတည်းဖျက်ပစ်ပါ။

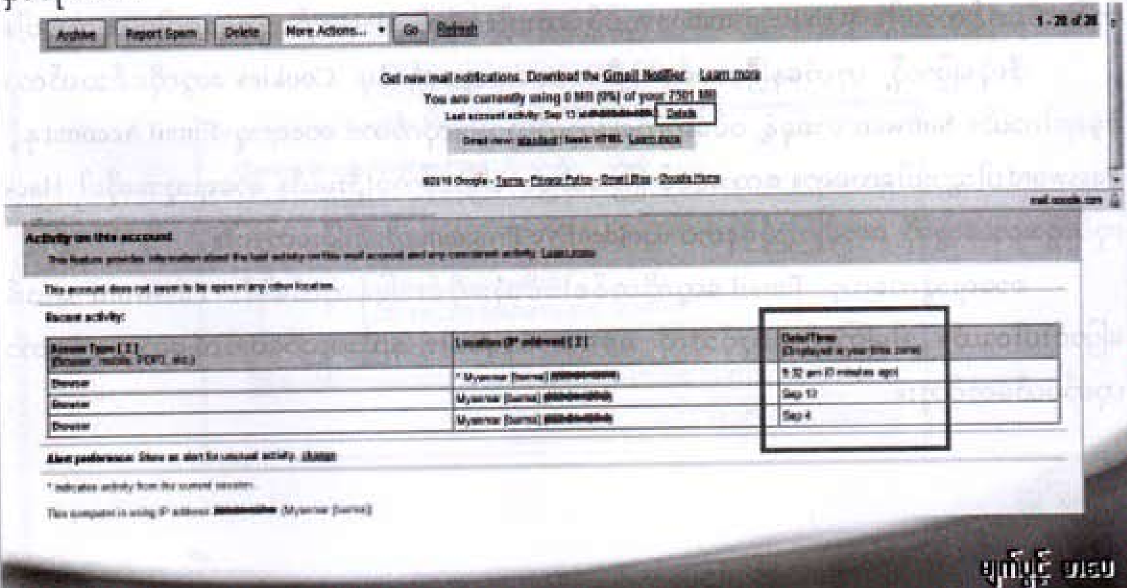
၅။ Password Recovery လုပ်နိုင်သော Recovery Quaction ၏အဖြေကို အခက်ခဲဆုံးဖြစ်ပါစေ။

Mail Password တွေကိုမေ့သွားတဲ့အခါ ပြန်လည် Recovery လုပ်ရာမှာထည့်သွင်းပေးရတဲ့အဖြေကို သိလွယ်၊ စဉ်းစားလွယ်သော အဖြေများမပေးထားသင့်ပါ။ ဥပမာ– ငယ်အမည်ကိုမေးခွန်းထားပြီး ငယ်အမည်ကိုသာအဖြေပေးထားလျှင် မိမိငယ်သူငယ်ချင်းများ သိနိုင်ပါတယ်။

၆။ မိမိနောက်ဆုံးသုံးခဲ့သောအချိန်၊ နေ့ရက်တို့ကိုမှတ်ထားပြီးစစ်ဆေးပါ။

GMail သုံးသူတွေအတွက်ဖြစ်ပါတယ်။ မိမိသုံးခဲ့တဲ့အချိန်၊ နေ့ရက်တွေကိုပြန်ကြည့်လိုက်သည်နှင့် မိမိအပြင်အခြားတစ်ယောက်ဝင်သုံးထားသလားဆိုတာသိရှိနိုင်ပါတယ်။ Google မှစေတနာလက်ဆောင်ပေးထားတာပါ။

မိမိ GMail ကိုဖွင့်သုံးထားစဉ် မျက်နှာစာအောက်ဆုံးထိရောက်အောင်သွားပါ။ Datails ကိုနှိပ်လိုက်ပါ။



၇။ Website တွေကိုအလည်အပတ်လျှော့ပါ။

Website တွေကိုအလည်အပတ်လျှော့ပါလို့ပြောလျှင် စာရေးသူဆိုစိတ်ဆိုးမိမယ်ထင်တယ်။ စာရေးသူကို မသွားပါနှင့်ဆိုတဲ့ခရီးသိပ်သွားချင်တာပါ။ တစ်ယောက်ယောက်က အဲ့ဒီဆိုက်ဝင်မကြည့်နဲ့နော် ထောင်ချောက်ကွ လို့ပြောရင် တစ်ခါလောက်တော့စမ်းဝင်ကြည့်ပါတယ်။

အမှန်ပါပဲ။ စာရေးသူကိုယ်တိုင်ခံလိုက်ရတာပါ။ ဒါပေမယ့်လဲ စာရေးသူက အင်တာနက်သုံးဖို့အတွက် Windows 7 ကို Harddisk Partition တစ်ခုမှာသီးသန့်ထားပါတယ်။ အခြား Partition တွေဟာ အဆိုပါ Windows 7 သုံးနေစဉ်ပိတ်ဆို့ထားလိုက်ပါတယ်။ ကဲဘယ်နှယ့်ရှိစ ဘာမှကိုလုပ်မရတော့ဘူး။ သူလုပ်သွားတာတွေကိုပဲ ထိုင်ကြည့်နေလိုက်တယ်။

အဆိုပါကဲ့သို့ Traps Website တွေဟာ ဝင်ကြည့်ယုံနဲ့ မိမိကွန်ပျူတာကိုထိန်းချုပ်ခွင့်ရယူနိုင်ပါတယ်။ ဒါပေမယ့်တစ်ခုတော့ရှိတယ်။ လိုင်စင် Windows ဖြစ်ပြီး၊ FireWall ချထားရင်လုံးဝ ဝင်လို့မရပါဘူး။

၈။ Website တွေမှာ Registration လုပ်ဖို့လိုလျှင်

Website တော်တော်များများဟာ သူတို့ထဲဝင်ကြည့်တာထက် တစ်ခုခုရယူလိုလျှင် စာဖတ်သူ Email, Password တွေကိုပေးရတတ်ပါတယ်။ စာဖတ်သူအရမ်းစိတ်ဝင်စားတဲ့အရာတွေမြင်နေရလျှင် Email, Password တွေကိုပေးကြတော့တာပါပဲ။ ပြီးမှ ကယ်ပါ၊ ကူပါဦးလို့အော်နေတော့တာပါပဲ။

ဒီလိုမျိုးအင်တာနက်ပေါ်မှာ မွှေနှောက်ဝင်ရောက်ရတာအားပါတယ်ဆိုလျှင် Email Account တစ်ခုသီးသန့်ထားပါ။ Web Registration လုပ်ဖို့ပဲသုံးပါ။ သူတို့ Hack ရင်လဲဘာမှမပါတော့ဘူးပေါ့။

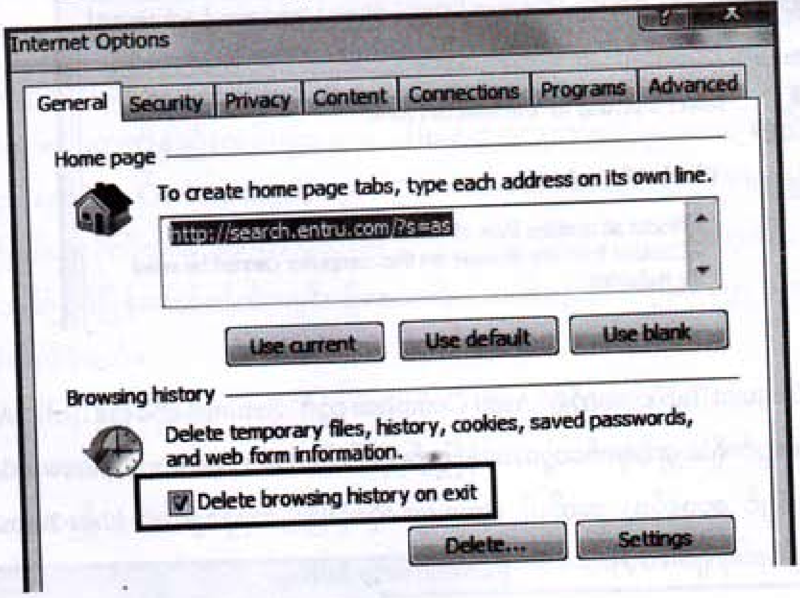
ဒီလိုပြောလို့ ဟုတ်နေပြီမထင်ပါနဲ့ဦး။ စာရေးသူစက်ထဲမှ Cookies တွေကိုဝင်သယ်တာခံခဲ့ရပါတယ်။ Software တစ်ခုနဲ့ ဝင်ရောက်ဖြေထုတ်ယူသွားလိုက်တာ စာရေးသူ Email Account နှင့် Password ပါသွားပါလေရော။ စကားမစပ် ကြားထဲဖြတ်ပြောလိုက်ပါဦးမယ်။ စာရေးသူအဆိုပါ Hack လုပ်သွားတာတွေကို စောင့်ကြည့်နေတာ GoldenEye Program ကိုသုံးပြီးတော့ပါ။

စာရေးသူကတော့ Email တွေကိုတစ်ခါဝင်သုံးတိုင်း ပြန်ထွက်ခါနီး Password အသစ်ပြောင်းပါတယ်။ ဒါကြောင့်လဲလုပ်သလို မခံရတာနေမှာပါ။ နည်းပညာတော်လို့တော့ မခံရတာ ဟုတ်မယ်မထင်ဘူး။

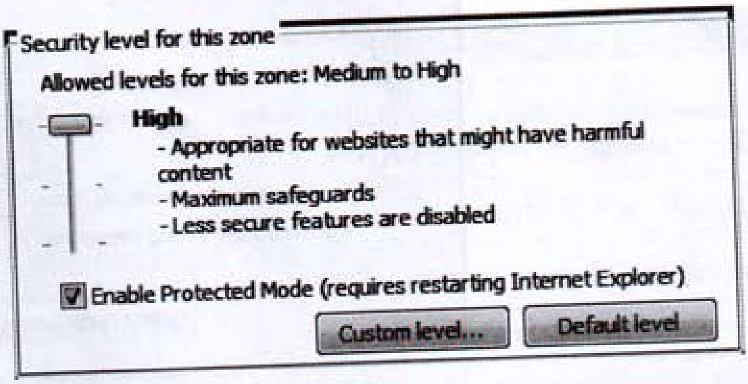
Internet Explorer သုံးသူများနှင့်ပြဿနာ

IE Browser သုံးသူတွေအတွက်အရေးပါသိသင့်တာလေးတွေရှိပါတယ်။ အများသုံး Cyber Cafe တွေမှာစက်သုံးသူများသိထားသင့်ပါတယ်။ Tool Menu အတွင်းမှ Internet Options ကိုဖွင့်ပါ။

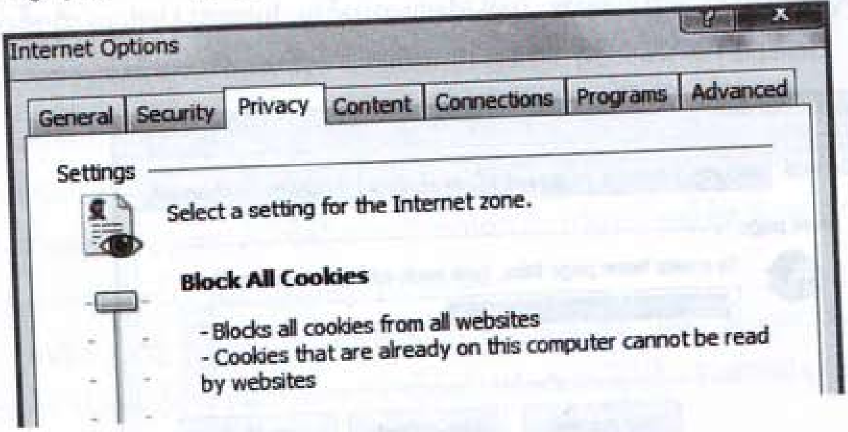
၁။ General Tab အောက်ရှိ Delete Browing --- တွင်အမှတ်တပ်ပါ။



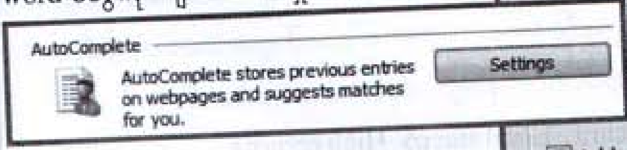
၂။ Security Tab အောက်ရှိ Security Level Bar ကို High ထားပါ။

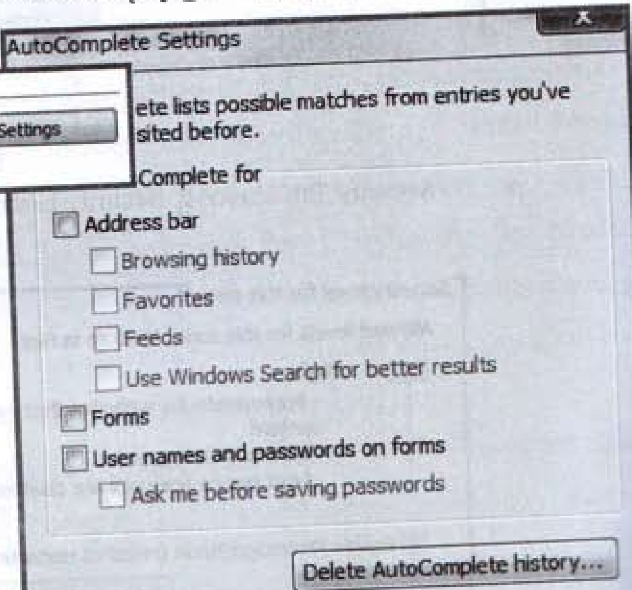


၃။ Privacy Tab အောက်ရှိ Cookies Setting Bar ကိုအမြင့်ဆုံး Block All Cookies ထားပါ။ Cookies တွေကိုယူဆောင်သွားခြင်းအား လုံးဝမခွင့်မပြုတော့ပါ။



၄။ Content Tab အောက်ရှိ Auto Complete တွင် Settings ကိုရွေးနှိပ်ပါ။ Auto Complete Settings Box တွင် ရှိသမျှအမှတ်တွေအကုန်ဖြုတ်လိုက်ပါ။ User Name and passwords on forms ကိုအမှတ်တပ်ထားလျှင် စာဖတ်သူ အဆိုပါ Browser ကိုသုံးပြီး ထည့်သွင်းတဲ့ User Name နဲ့ password တွေကိုမဖျက်ပဲထားရှိပါလိမ့်မယ်။





Cookies တွေအစားခံရတဲ့အခါ

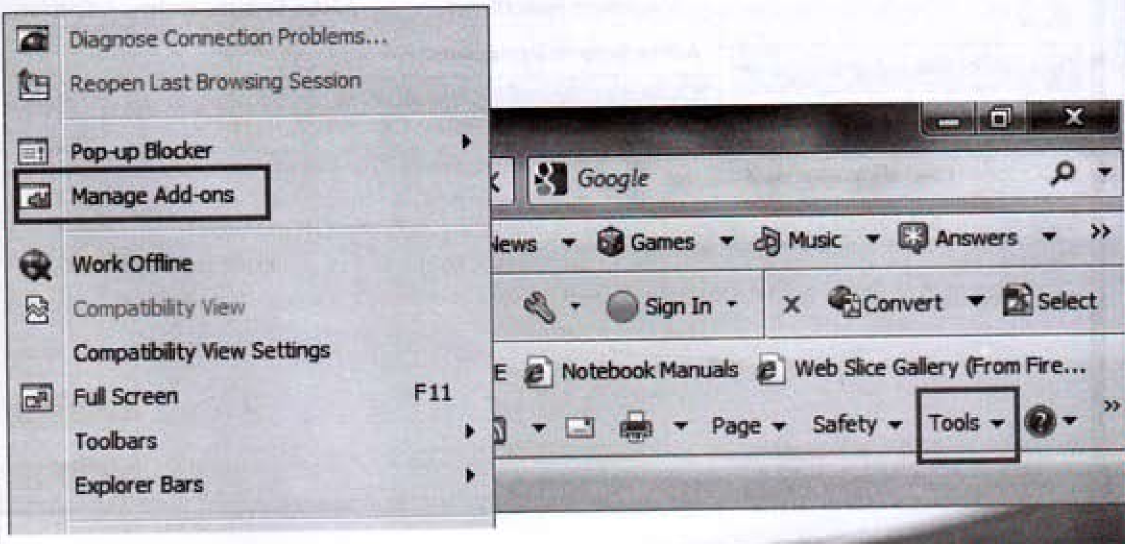
တရုတ်နိုင်ငံမှထုတ်တဲ့ တရုတ်တံဆိပ်နဲ့ Cookies ကိုစာရေးသူသိပ်ကြိုက်ပါတယ်။ ဒီတစ်ခါ ပြောပြမယ့် Cookies ဆိုတာ စာဖတ်သူသုံးစွဲနေမှုများကို လက်တလောသိမ်းထားတဲ့ မှတ်တမ်း စနစ်တစ်ခုပါ။ ကွန်ပျူတာအတွင်းရှိနေတဲ့ Hacker ကြိုက်တဲ့ Cookies တွေကို C:\Users\ CurrentUser Name\AppData\Roaming\Microsoft\Windows\Cookies မှာတွေ့ရပါတယ်။ တစ်ခါတရံ Cookies Foler ကိုရှာဖွေမတွေ့ပဲရှိနေတတ်ပါတယ်။ ပြဿနာမဟုတ်ပါ။

Cookies တွေကိုနည်းလမ်းများစွာနဲ့ Hacker တွေဟာရဖို့ကြိုးစားကြပါတယ်။ ရသွားပြီ ထားပါတော့။ ရလာတဲ့ Cookies တွေကို၊ ၎င်းရဲ့ Cookies ထားရာနေရာမှာ Upload ဖြင့်ထည့်လိုက်ပြီး Browser ကိုဖွင့်သုံးလိုက်တာနဲ့ စာဖတ်သူသုံးနေသည့်အတိုင်း ၎င်းလည်းသုံးနေရပါပြီ။ Cookies တွေဟာ ကွန်ပျူတာတစ်ကြိမ်ပြန်မပိတ်လိုက်မချင်း ရှိနေတတ်ပါတယ်။ ပြန်ပိတ်ပြီးပြန်ဖွင့်လိုက်လျှင် ID, Name တော့ကျန်ခဲ့ပါလိမ့်မယ်။

စာဖတ်သူဟာ Hacker တွေတည်ထားတဲ့ Traps Website ကိုဝင်ကြည့်မိသွားတယ်။ သူတို့ ဆွဲဆောင်မှုကိုလက်ခံပြီး တစ်ခုခု Download ရယူလိုက်ပါတယ်။ အဲ့ဒီအခါ စာဖတ်သူကွန်ပျူတာဟာ Spyware တွေထည့်သွင်းခံလိုက်ရပါပြီ။

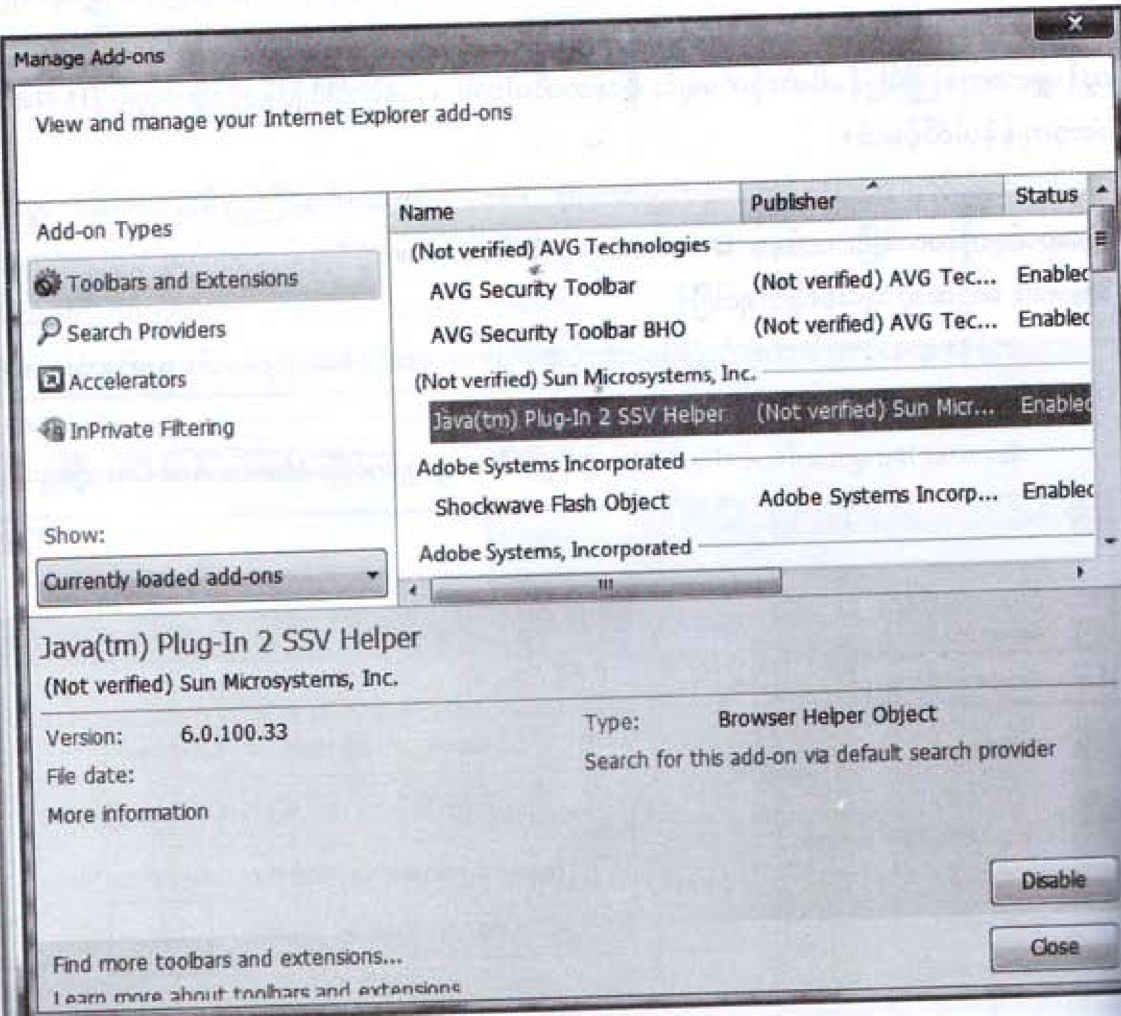
တစ်နေရာရာမှာအင်တာနက်သုံးဖို့စတင်တဲ့အခါ Browser ကိုစစ်ဆေးရပါမယ်။ ယခုအသုံးများတဲ့ IE Browser ကိုစတင်ရှင်းပြပါ့မယ်။

Browser Bar များပေါ်တွင် Tools Menu ကိုရှာပါ။ တွေ့လျှင်ဖွင့်ပြီး Manage Add-Ons ကိုရွေးပါ။



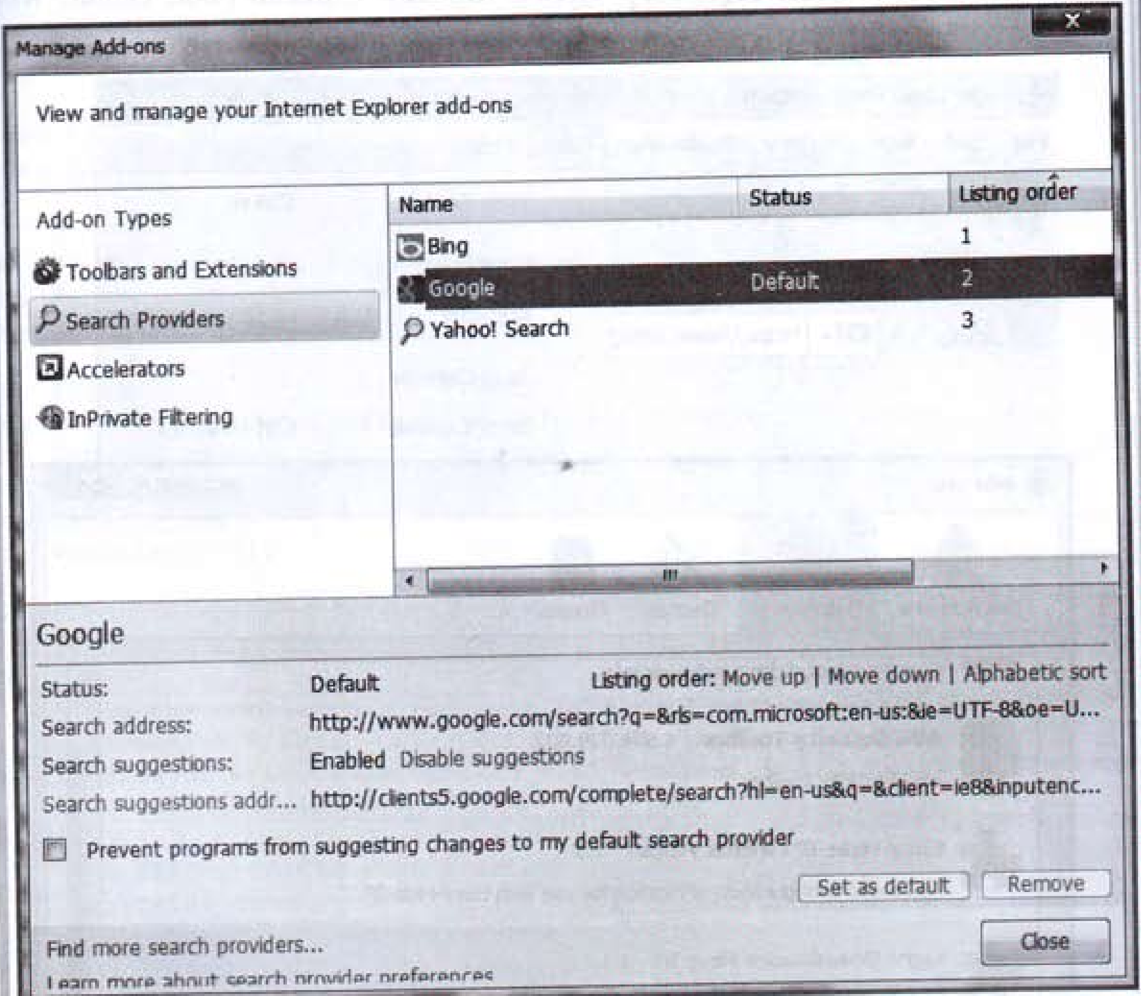
အောက်ပါအတိုင်း Manage Add-Ons Box တွင် ဘယ်ဘက်မှ Toolbars and Extensions ကိုရွေးပါ။ ညာဘက်တွင် တစ်ခုခြင်းစစ်ဆေးသွားပါ။ စာဖတ်မသိသောအမည်များ၊ တိရစ္ဆာန်အမည်များ ဖြစ်နေလျှင် ရွေးချယ်ပြီး အောက်ဖက်နားမှ Disable ကိုနှိပ်ပါ။

Browser Add-On တွင်နာမည်ကြီးသော BackDoor Hack Program များမှာ– Grease Monkey, Chicken Foot, Donut, Win များဖြစ်ပါတယ်။ တွေ့လျှင်၊ မသင်္ကာလျှင် Disable သာလုပ်လိုက်ပါ။



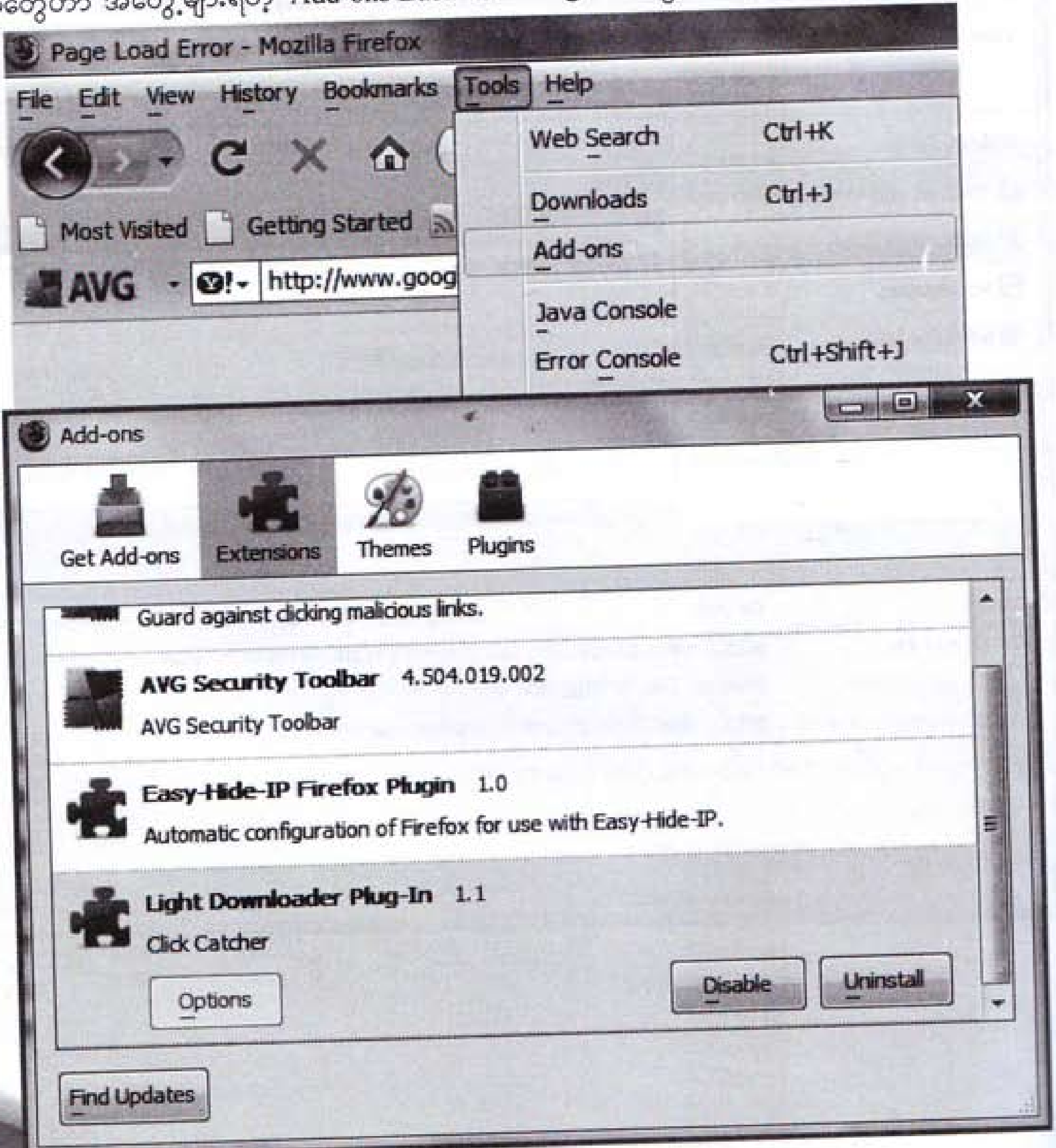
Manage Add-Ons Box တွင် ဘယ်ဘက်မှ Search Providers ကိုရွေးပြီး။ ဖော်ပြပုံပါသုံးမျိုးအပြင် ဖြစ်တတ်သူမကြားဖူးသော Search Engine တစ်ခုတွေ့လျှင် Remove လုပ်ပစ်ပါ။

Accelerators တွင်လည်း မသင်္ကာစရာများပါရှိနေလျှင် Remove, Disable လုပ်လိုက်ပါ။



Mozilla Firefox တွင် Tools > Add-Ons ကိုရွေးလိုက်ပါ။ Add-ons Box တွင်စာဖတ်သူ ထည့်သွင်းထားသော Software များသာရှိပါလိမ့်မယ်။ ရှေ့တွင်ပြောခဲ့သလို မသင်္ကာစရာ အမည်များ၊ တိရစ္ဆာန်အမည်များတွေ့လျှင် Uninstall လုပ်ပစ်ပါ။

BackDoor Program တွေကတော့ Grease Monkey, Chicken Foot, Donut, Win စတာတွေဟာ အတွေ့များရတဲ့ Add-ons BackDoor Program တွေပါ။



Cookies Crack Program Code

စာဖတ်သူဟာ Programming Language လေ့လာနေသူဖြစ်လျှင် အသုံးဝင်စေဖို့ Program Code အချို့ကိုဖော်ပြပေးလိုက်ပါတယ်။ သာမန်စာဖတ်သူများကတော့ ကျော်သာဖတ်သွားလိုက်ပါ။ Honest Hacker တွေအတွက်ရည်ရွယ်ဖော်ပြရတာပါ။ ဒါကြောင့်အသေးစိတ်မရှင်းပြတော့ပါ။

```
#!/usr/local/bin/perl -w

use CGI qw/:standard/;
use CGI::Cookie;


# use CGI module to retrieve command
my $query = new CGI;
my $command =$query->param('cookie_command');

my $cookie_cli = "favorite_flavor"; # this one's set by the client
my $cookie_svr = "calories"; # this one's set on the server (here)
my $status_code = 1; # code to send back to client; 1 = success, -1 =
failure
my $status_msg = ""; # status string to send back to the client
my @cookies = ();

# If cookie command is set a cookie
if ($command eq "set")
{
  # dig the cookie that was sent by the client (VoiceXML browser)
  my %cookies = fetch CGI::Cookie;
  my $flavor = $cookies{$cookie_cli}->value;
  if (!defined($flavor))
  {
    # ERROR. Cookie wasn't set or sent
    $status_code = -1;
    $status_msg = "No flavor was specified"
  }
  else
  {
    # given the user's flavor choice, get the calorie count,
    # and return the value in a cookie
    # Note that this data could be returned via the namelist of
    # the return element
    my $cals = GetCalories($flavor);
```

```
    my $cookie = new CGI::Cookie(
        -name   => $cookie_svr,
        -value  => $cals,
        -expires =>'+1h', # or less if session/call ends
        #-domain =>'.tellme.com',
        #-path   =>'/'
        );

    $status_code = 1;
    $status_msg = "set calorie cookie";
    push @cookies, $cookie;
  }
}
elsif ($command eq "delete")
{
   # delete the server/calorie cookie
   my $c1 = new CGI::Cookie(
     -name      => $cookie_svr,
     -value => 0,
     -expires => 'Tue, 1 Jan 1980 08:00:00 UTC' #'-1d', #
yesterday...
   #  -domain =>'.tellme.com',
   #  -path   =>'/'
     );

   push @cookies, $c1;

   # delete the client/flavor cookie
   my $c2 = new CGI::Cookie(
     -name     => $cookie_cli,
     -value => 0,
     -expires => 'Tue, 1 Jan 1980 08:00:00 UTC' # '-1d', #
yesterday...
     #-domain =>'.tellme.com',
     #-path   =>'/'
     );

   push @cookies, $c2;

   $status_code = 1;
   $status_msg = "deleted cookies";
}
```

```
else
{
   $status_code = -1;
   if (defined($command))
   {
      $status_msg = "unexpected CGI param";
   }
   else
   {
      $status_msg = "expected CGI param set or delete";
   }
}

WriteSubdialog(\@cookies, $status_code, $status_msg);

# write some VoiceXML to the client
sub WriteSubdialog
{
   my ($raCookies, $code, $msg) = @_;

   # write http headers (including cookies)
   foreach $cookie (@$raCookies)
   {
      print "Set-Cookie: $cookie\n";
   }
   print "Content-Type: text/xml\n\n";

   # write http msg body
   print <<EOF;
<vxml version="2.0">
   <var name="code" expr="$code"/>
   <var name="msg" expr="'$msg'"/>

   <form>
   <block>
      <log> @$raCookies </log>
      <return namelist="code msg"/>
   </block>
   </form>
</vxml>
EOF
}

# given the cookie flavor, return the number of calories per serving
```

```
# a "real" implementation would retrieve this information from a
"nutrition data server",
# undoubtedly a "Web Service" of the not-too-distant future
# If the flavor can't be found in our simple hash table, return 0 (no
calories)
sub GetCalories
{
   my($flavor) = @_;

   my $lcFlav = lc($flavor); # convert to lowercase

   my %flav2cal = (
          'chocolate chip' => 150,
          'oreo' => 175,
          'graham cracker' => 75,
          'vanilla wafer' => 60);

   return (exists($flav2cal{$lcFlav}) ? $flav2cal{$lcFlav} : 0);
}
```

စာရေးသူထံကို စာတွေပို့ပို့ပြီးမေးလာကြပါတယ်။ အဆိုပါဖော်ပြထားတဲ့ Program Code Line တွေကို နားလည်ချင်လို့ရှင်းပြပါတဲ့။ စာဖတ်သူတွေကိုသိပ်ရှင်းပြချင်တာပေါ့။ Program တစ်ပုဒ်ရဲ့ အသက်သွေးကြောတွေဖြစ်တဲ့ Code Line တွေကိုရှင်းပြဖို့ဆိုတာ စာရေးသူအတွက်လွယ်ချင်လွယ်မယ်၊ သာမန်စာဖတ်သူအတွက် နားလည်သွားဖို့ဆိုတာ လုံးဝမလွယ်ကူတဲ့ကိစ္စဖြစ်နေလေရဲ့။

စာအုပ်တစ်အုပ်ကို စာရေးသူဖန်တီးတည်ဆောက်တဲ့အခါတိုင်း ဒွိဟဖြစ်နေရတာ အဲ့ဒီ့ကိစ္စပါ။ စာအုပ်ဆိုတာ အဆင့်အတန်းပေါင်းစုံအတွက်ဖြစ်လျှင် အကောင်းဆုံးပါ။ ဒါ့ကြောင့် အမြင့်စား စကားလုံး အသုံးအနှုန်းတွေ၊ သဘောတရားခပ်မြင့်မြင့်တွေကိုရှောင်ရှားပြီး အပြေပြစ်ဆုံး စကားပြောစကားပြေနဲ့သာ ရေးခဲ့တာပါ။ စာဖတ်သူစီစဉ်နေပါတယ်။ Program တစ်ပုဒ်ကိုလက်တွေ့အစမှအဆုံးရှင်းပြပြီး စာအုပ်ထုတ်ဖို့ပါ။ လက်တွေ့တိုက်ရိုက်ရေးဆွဲနိုင်တဲ့စာအုပ်မျိုးပေါ့။

ယခုစာအုပ်ပါ Program Code တွေဟာအနည်းငယ်နက်ရှိုင်းပါတယ်။ ဒါ့ကြောင့်နားလည်လွယ်တာတွေကိုအသေးစိတ်ရှင်းပြပေးပြီး၊ နားလည်ဖို့ခက်ခဲတာတွေ တစ်ချိန်မှာပြန်သုံးနိုင်အောင် မှတ်တမ်းတင်ပေးလိုက်ရတာပါ။

Gmail-GTalk ဆိုင်ရာအသုံးချလုပ်ဆောင်မှု

Gmail-GTalk Hack ဆိုတာနဲ့ Password တွေကိုခိုးယူပြီးမတရားဝင်ရောက်မယ့်နည်းလမ်းတွေလို့ မယူဆပါနှင့်။ ရှိတော့ရှိပါတယ်။ စာရေးသူလည်းမတတ်လို့မပြောပြနိုင်ပါဘူး။

ယခုဖော်ပြမယ့်အကြောင်းအရာတွေကတော့ သုံးသူတွေအတွက် အသုံးချနည်းလမ်းများ ဖြစ်ပါတယ်။ မြန်မာနိုင်ငံအပါအဝင် အင်တာနက်အသုံးပြုသူအများစုဟာ Google နှင့်မကင်းနိုင်ကြပါဘူး။ ဒါ့ကြောင့်ယခုဖော်ပြပါနည်းလမ်းများဟာ စာဖတ်သူများအတွက်အသုံးဝင်စေမှာပါ။

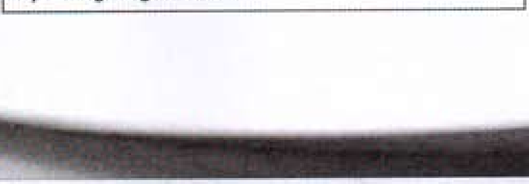
၁။ မိမိကို စကားမပြောချင်တော့ဘူးလား ----

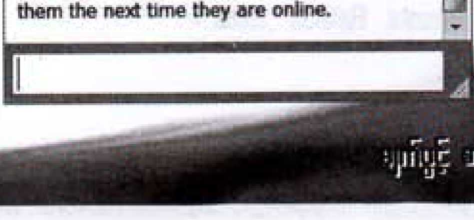
စာဖတ်သူရဲ့ Account ကိုတစ်ဖက်အသုံးပြုသူမှ ပိတ်ထား(Block) လားလို့ သိချင်ကြမှာပါ။ ဘယ်လိုကြည့်ရပါသလဲဆိုတဲ့မေးခွန်းတွေ စာရေးသူထံမကြာခဏရောက်ရောက်လာပါတယ်။ စာဖတ်သူနဲ့ သဟဇာတမဖြစ်လို့ စကားမပြောချင်တော့ဘူးဆိုလျှင် Account Name ပေါ်မှာ Right Click နှိပ်ပြီး Block လို့ပြောလိုက်လျှင် အဆိုပါ ပိုင်ရှင်ရှိစာရင်းတွင် မိမိ Account Name မှာအမြဲ Offline ဖြစ်သွားပါလိမ့်မယ်။

ဒီလိုပါပဲ။ စာဖတ်သူကို ချစ်သူက၊ ဒါမှမဟုတ် သူငယ်ချင်းက စကားမပြောချင်လို့ လုပ်ထားသလားဆိုတာ သိချင်တဲ့အခါအောက်ပါအတိုင်းစမ်းသပ်ကြည့်ရှုနိုင်ပါတယ်။

အဆိုပါသိလိုတဲ့ Account Name ကိုရွေးချယ်ပြီး Send VoiceMail နှိပ်လိုက်ပါ။ Call ပြုလုပ်နေတာဖြစ်လို့ ခဏအကြာမှာ ပုံမှန်အားဖြင့်ဆိုလျှင် မိန်းခလေးတစ်ဦးမှ Massage Speak ပေးနေသံကြားရလျှင် လုပ်မထားပါဘူး။ အမှန်တကယ် အသုံးမပြုပဲရှိနေတာပါ။

ဒါမှမဟုတ်ပဲ Call ခေါ်လိုက် လိုင်းကျသွားလိုက်ဖြစ်နေလျှင်တော့ ကြိမ်းသေ Block လုပ်ထားပါတယ်။ ဒါဆိုလျှင် စာဖတ်သူအနေဖြင့် Email မှာရေးလိုတာတွေ ရေးသာပြောလိုက်ပါတော့။





Gmail ပို့ထားတာတွေပြန်ဖျက်ဖို့

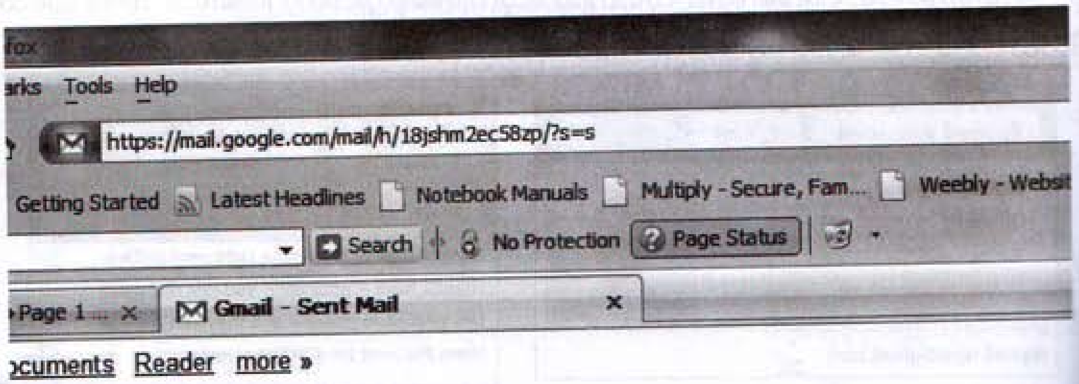
Gmailကိုအသုံးပြုပြီး Mailတွေအပြန်အလှန်ပေးပို့ကြပါတယ်။ တစ်ခါတရံမှာ ပို့ပြီးသား Mail တွေကိုပြန်ဖျက်လိုတာမျိုး ကိစ္စတွေရှိလာမှာပါ။ အထူးသဖြင့် သမီးရည်းစားကိစ္စတွေမှာ စာရေးသူထံ မကြာခဏအကူအညီတောင်းသူတွေရှိပါတယ်။ သူမပို့ထားတဲ့ Gmail ကိုအသုံးပြုပြီး သူမနှင့်ပြဿနာ ရှိလာသောအခါ သူမအား အကျပ်ကိုင်နေပါသဖြင့် ကူညီပေးဖို့ပေါ့။

ထိုအခါ အဆိုပါပို့ထားမိတဲ့စာကိုပြန်ဖျက်ဖို့လိုအပ်လာပါပြီ။ အခ်ိကကတော့ ပို့ထားတဲ့စာရင်းကို ဖျက်ပစ်ဖို့ပါ။ တကယ်တော့လုံးဝမလွယ်ကူပါဘူး။ သို့သော်လည်း စာဖတ်သူအတွက် Googleက ၂၀၀၈ အကုန်မှာ လက်ဆောင်တစ်ခုဖြည့်သွင်းပေးခဲ့ပါတယ်။ ဒါကတော့ Undo Setting တစ်ခုဖြစ်ပါတယ်။ စမ်းသပ်ကြည့်ရအောင်။ စာရေးသူလက်တွေ့ပြုလုပ်ကြည့်သည်မှာ ၁၅ ရက်နောက်ပိုင်းစာများမရတော့ပါ။ ထို့အပြင် Starredရွေးထားလိုက်လျှင်လည်းမရတော့ပါ။ ဒါကြောင့်စာပို့စဉ်ကပင်ဂရုစိုက်သင့်ပါတယ်။

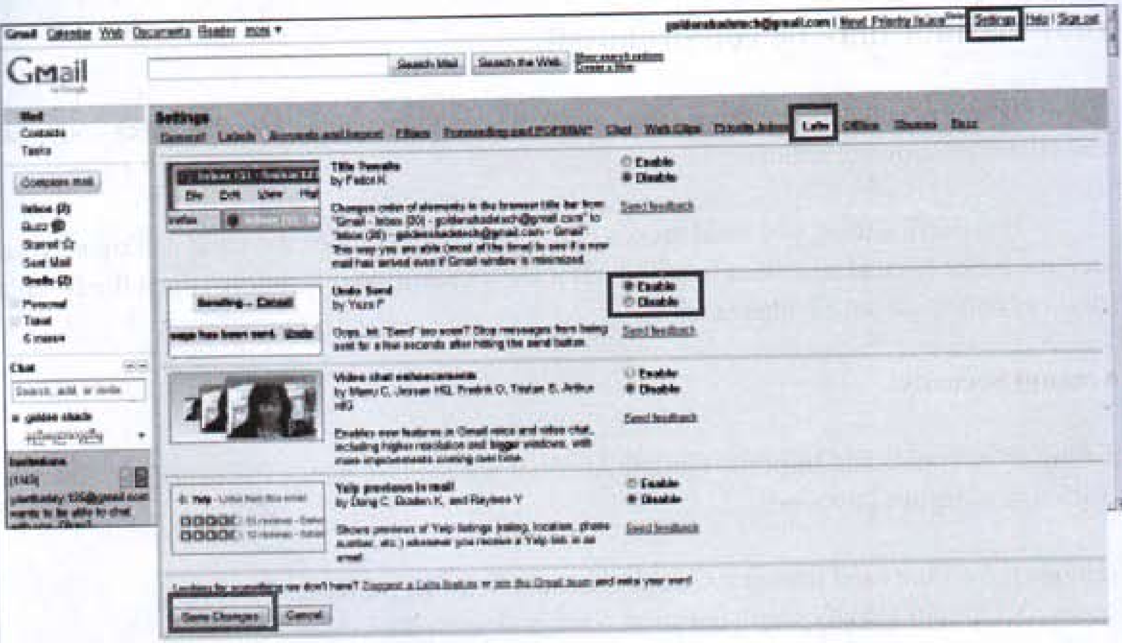
စာဖတ်သူရဲ့ Gmail Accountကိုဖွင့်ပါ။ အပေါ်ညာဘက်နားကိုကြည့်ပါ။ အောက်ပါအတိုင်းNew Prioity Inboxတွေ့ရှိမှသာ ပြင်ဆင်နိုင်မှာပါ။ ယခုမှစသုံးလျှင် ရှေ့ပိုင်းစာများ Undo လုပ်မရပါ။

ပထမဦးစွာ Gmail Updateလုပ်ရပါမယ်။ Address Boxတွင် mail/ အထိထားပြီးနောက်မှစာများ ဖျက်လိုက်ပါ။ mail/ နောက်တွင် /?labs=0. ထပ်ဖြည့်ပြီး Enter ခေါက်လိုက်ပါ။

https://mail.google.com/mail/?labs=0.



အောက်ပါပုံစံရလာတဲ့အခါ Setting Menu ကိုဖွင့်ပြီး Labs ကိုရွေးပါ။ ထို့နောက် Undo Send အောက်ရှိ Enable ကိုရွေးချယ်လိုက်ပါ။ အသစ်လုပ်ဆောင်ချက် အဖြစ် Save Changes Button ကိုနှိပ်ကာ ပြောင်းလဲသိမ်းဆည်းလိုက်ပါ။



အထက်ပါလုပ်ဆောင်ချက်လုပ်ပြီးသွားသည့်နောက်ပိုင်း ပေးပို့လိုက်သမျှ Mail တွေကိုပြန်ဖျက်လိုလျှင် ချက်ခြင်းပို့ထားသောစာဖြစ်နေပါက Sending --- Cancel နှိပ်လိုက်ပါ။ ရက်ပိုင်းကြာပြီးသောစာဆိုလျှင် Undo ကိုရွေးချယ်လိုက်ပါ။

စမ်းသပ်အဆင့်သာရှိနေသေးလို့ ယုံကြည်ချက်အပြည့်အဝဖြင့်မသုံးပါနှင့်။ ဒီ့ထက်ကောင်းအောင်ပြုလုပ်လာသလို၊ အခက်အခဲများလည်းရှိလာမှာပါ။

စာလက်ခံသူဟာ

Gmail သုံးသူတိုင်းလုပ်ဆောင်ဖို့ရာ

Gmail ကိုပိုင်ဆိုင်ထားသူတိုင်း အလွယ်တကူတိုက်ခိုက်ခံရခြင်းမှကာကွယ်ရန် အောက်ပါလုပ်ဆောင်စရာများကို လုပ်ဆောင်ရန်လိုအပ်ပါတယ်။ မူရင်းဆောင်းပါးအတိုင်းဖော်ပြလိုက်ပါတယ်။ စာဖတ်သူကိုယ်တိုင် ကြိုးစားဘာသာပြန်ဆိုကာ ဖော်ပြပါအတိုင်းအဆင့်လိုက်လုပ်ဆောင်သွားပါ။

Your account may be compromised.

If your account has been compromised/ hacked/stolen you will need to check and fix at least all of the following settings.

Bus the first thing you need to do is check the buttom of the Inbox and make sure your account is not open at any other locations. If it shows additional locations, open the Details windows and "Sign out all other sessions".

Account Security:

Settings > Accounts and Import > Google Account Settings > Change Password
[Pick a new secure Password]

Settings > Accounts and Import > Google Account Settings > Change Password
Recovery Options [Verify secret question, SMS and recovery E-mail address]

Potential Spam:

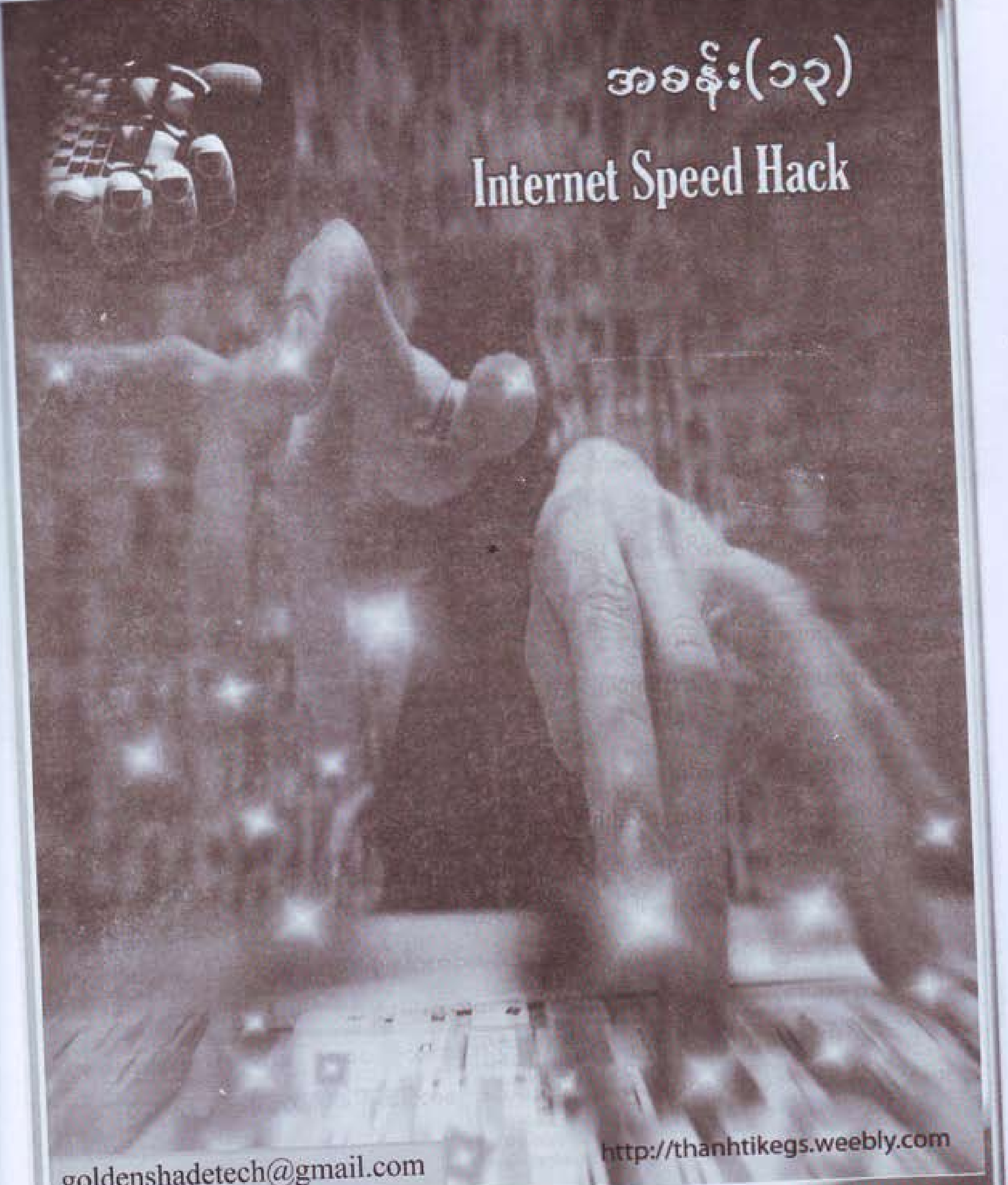
Settings > General > Signature [Make sure nothing as been added]
Settings > General > Vacation Responder [Make sure it's disable and empty]

E-Mail Theft;

Settings > Accounts and Import > Send Mial As [Make sure it is using your correct e-mail address]
Settings > Filters [No filters that forward or delete e-mail]
Settings > Forwarding and POP/IMAP > Forwarding [Disabled or correct address]
Settings > Forwarding and POP/IMAP > POP Dwonload [Disable]
Settings > Forwarding and POP/IMAP > IMAP Access [Disable]

အခန်း(၁၃)

Internet Speed Hack



Internet Connection Speed Hack

ယခုကဏ္ဍကတော့ ကမ္ဘာတစ်ခုလုံးမှာ Popular အဖြစ်ဆုံးကိစ္စဖြစ်ပါတယ်။ အသုံးပြုနေတဲ့ လက်ရှိ Connection ကိုတစ်ဦးတစ်ယောက်အားထိခိုက်မှုမရှိစေပဲ Speed Up လုပ်ဆောင်ဖို့စီစဉ်တာပါ။ ဘယ်နေရာတွေမှာအသုံးလိုသလဲဆိုတော့ အင်တာနက်ပေါ်မှ Program များကို Download လုပ်ယူတဲ့အခါ၊ လိုင်းအားနိမ့်နေလို့ Gtalk, VZO ပြောမရတဲ့အခါတွေမှာအသုံးဝင်ပါတယ်။

ခေါင်းစဉ်ကိုဖတ်ပြီး နားလည်မှုလွဲမသွားပါနဲ့။ စာရေးသူကြားဖူးပါတယ်။ လက်ရှိနိုင်ငံမှာ သုံးနေပြီး အခြားနိုင်ငံတစ်ခုရဲ့လိုင်းကိုဆွဲယူတယ်ဆိုတာမျိုးပါ။ စာရေးသူတော့မလုပ်တတ်ပါဘူး။ လုပ်တတ်လျှင်လည်း ချမ်းသာနေလောက်ပါပြီ။ Server ထောင်ပြီး လိုင်းအားကောင်းကောင်းတွေ ရောင်းစားမှာပေါ့။ ဟာသပြောတာပါဗျာ။ ယုံတမ်းစကားလို့သာမှတ်ထားပါ။

ပထမဦးစွာ လက်ရှိလိုင်းဆွဲအားကို အနည်းငယ် ၂၀% လောက်တိုးမြှင့်ကြည့်ရအောင်။ တကယ်တန်းကြတော့ ၅ % လောက်သာတိုးလာတယ်ဆိုတာစမ်းသပ်မိပါတယ်။ ဘာပဲပြောပြော နည်းနည်းရလဲ အရှုံးမရှိပါဘူး။

Group Policy ထဲကိုဝင်ရန် Run Box ကိုဖွင့်ပါ။ gpedit.msc ကိုရိုက်ထည့်ပြီး Enter Key နှိပ်ပါ။

Computer Configuration

Administrative Templates

Network

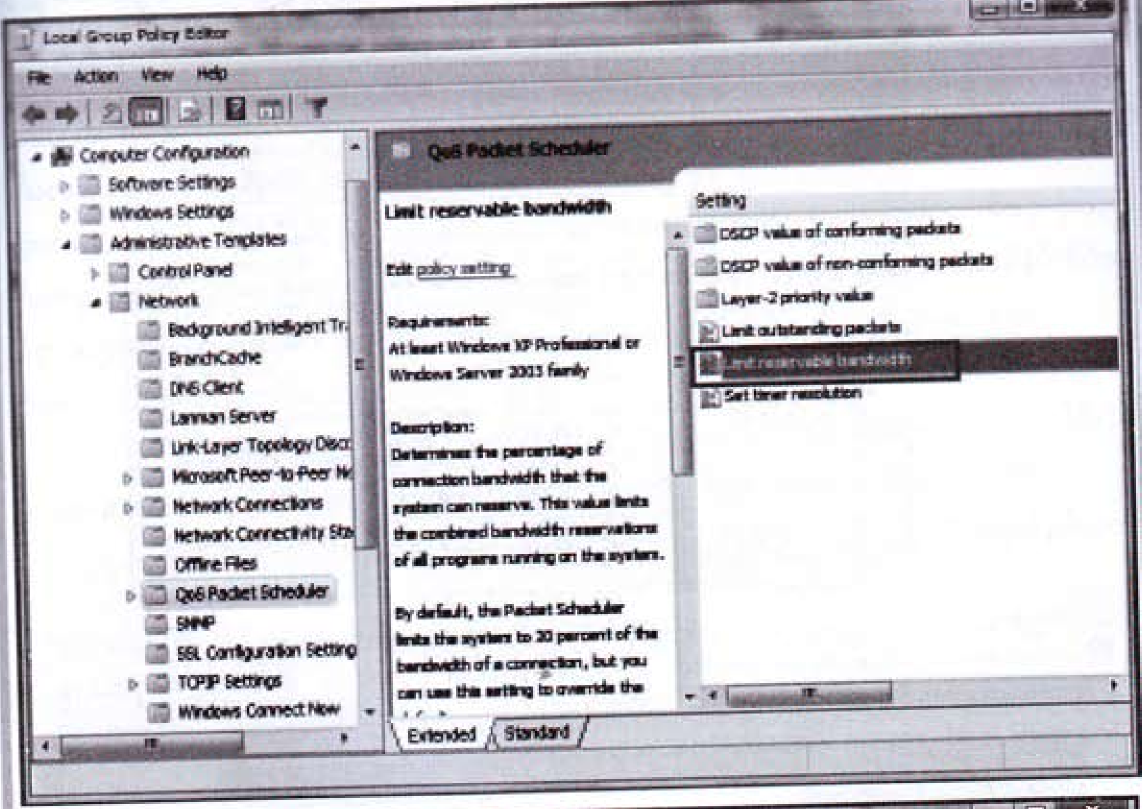
QoS Packet Scheduler ရဲ့ညာဘက်ခြမ်းရှိ

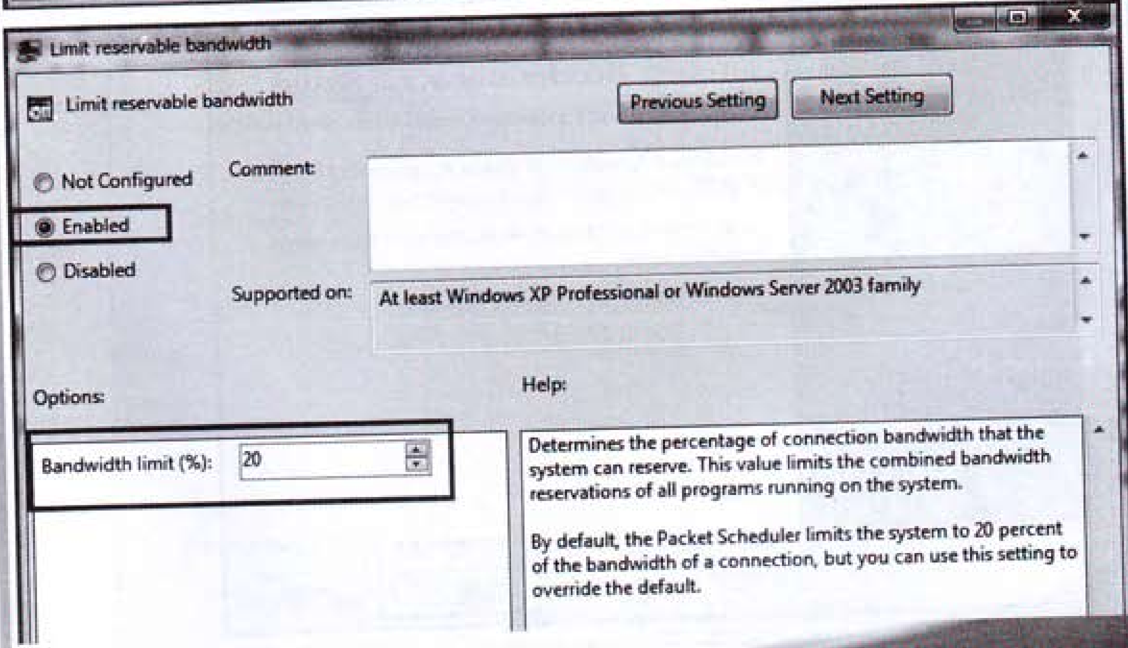
Limit reservable bandwidth ကိုကလစ်နှစ်ချက်နှိပ်လိုက်ပါ။

Enabled ကိုရွေးချယ်ပြီး Options အောက်ရှိ Bandwidth Limit Box အတွင်း 20 ထည့်လိုက်ပါ။ ပုံများကို တစ်ဖက်စာမျက်နှာမှာဖော်ပြပေးထားပါတယ်။

ဒီ့ထက်ပိုထည့်လို့ရပါသလားလို့ မေးချင်မယ်ထင်တယ်။ ၄င်းရဲ့ညာဘက်အခြမ်းမှာဖော်ပြပေးပြီး ဖြစ်ပါတယ်။ မရပါဘူး။ အမြင့်ဆုံး ၂၀ % လို့သာပေးထားပါတယ်။

အရမ်းကိုဆန္ဒပြင်းပြနေလျှင်တော့ စိတ်ကြိုက်သာ ၁၀၀၀ လောက်ထည့်ကြည့်ပေါ့။ သွားမလုပ်ပါနဲ့ဦး။ စာရေးသူတရားခံဖြစ်နေပါဦးမယ်။ စကားအရ ပြောတာပါဗျာ။


Local Group Policy Editor
File Action View Help
Computer Configuration
Software Settings
Windows Settings
Administrative Templates
Control Panel
Network
Background Intelligent Tr
BranchCache
DNS Client
Lanman Server
Link-Layer Topology Disco
Microsoft Peer-to-Peer Ne
Network Connections
Network Connectivity Sta
Offline Files
QoS Packet Scheduler
SNMP
SSL Configuration Setting
TCPIP Settings
Windows Connect Now
QoS Packet Scheduler
Limit reservable bandwidth
Edit policy setting
Requirements:
At least Windows XP Professional or Windows Server 2003 family
Description:
Determines the percentage of connection bandwidth that the system can reserve. This value limits the combined bandwidth reservations of all programs running on the system.
By default, the Packet Scheduler limits the system to 20 percent of the bandwidth of a connection, but you can use this setting to override the
Setting
DSCP value of conforming packets
DSCP value of non-conforming packets
Layer-2 priority value
Limit outstanding packets
Limit reservable bandwidth
Set timer resolution
Extended
Standard

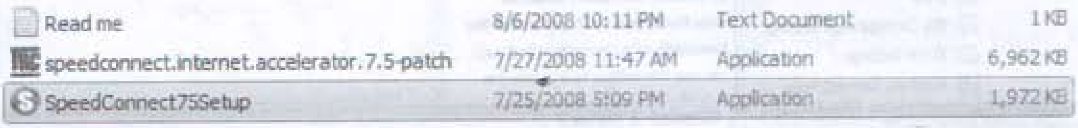

Limit reservable bandwidth
Limit reservable bandwidth
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows XP Professional or Windows Server 2003 family
Options:
Help:
Bandwidth limit (%):
20
Determines the percentage of connection bandwidth that the system can reserve. This value limits the combined bandwidth reservations of all programs running on the system.
By default, the Packet Scheduler limits the system to 20 percent of the bandwidth of a connection, but you can use this setting to override the default.

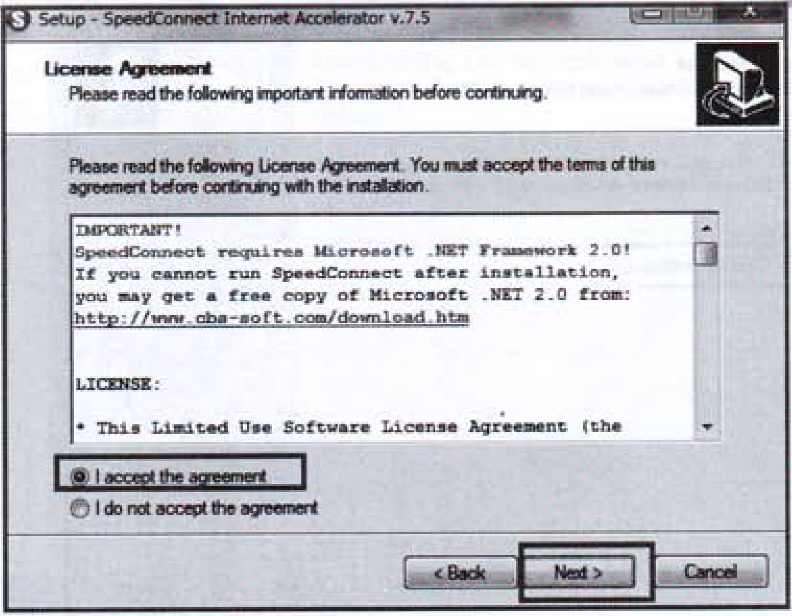
Speed Connect Program ကိုလေ့လာခြင်း

စာရေးသူလက်ရှိအသုံးပြုနေတဲ့ Speed Up Program ဖြစ်ပါတယ်။ နေရာစားမှုသက်သာပြီး Connection ကို ၂၀% မကလုပ်ဆောင်ပေးပါတယ်။ Internet Connection ထိုးကျနေချိန် အများသုံးသူတွေတောင် Gmail, GTalk ဖွင့်မရဖြစ်နေချိန်မှာ ၄င်း Program ကသုံးလို့ရအောင်ရပ်တည်ပေးနေပါတယ်။ စာရေးသူစမ်းသပ်ခဲ့ပါတယ်။ မိမိရဲ့လုပ်ဆောင်ချက်ဟာ တစ်ပါးသူကိုထိခိုက်ပါသလား။ ဟုတ်ကဲ့။ မထိခိုက်နိုင်တာတွေကိုသာ စာဖတ်သူများအတွက် နည်းပညာအဆင့်မြင့်မားစေဖို့ ရေးသားပြုစုပေးတာပါ။

ယခု Program ကိုစမ်းသုံးကြည့်ပါ။ စာဖတ်သူနှစ်ခြိုက်မှာပါ။ ပထမဦးစွာ ကွန်ပျူတာအတွင်း ထည့်သွင်းပါ့မယ်။ ထည့်သွင်းပုံအဆင့်လိုက်ကို ပုံများနှင့်တကွရှင်းပြထားပါတယ်။ လိုင်စင်ဖားရှင်း သုံးနိုင်ရန်လည်း Register စနစ်ပါရှိပါတယ်။

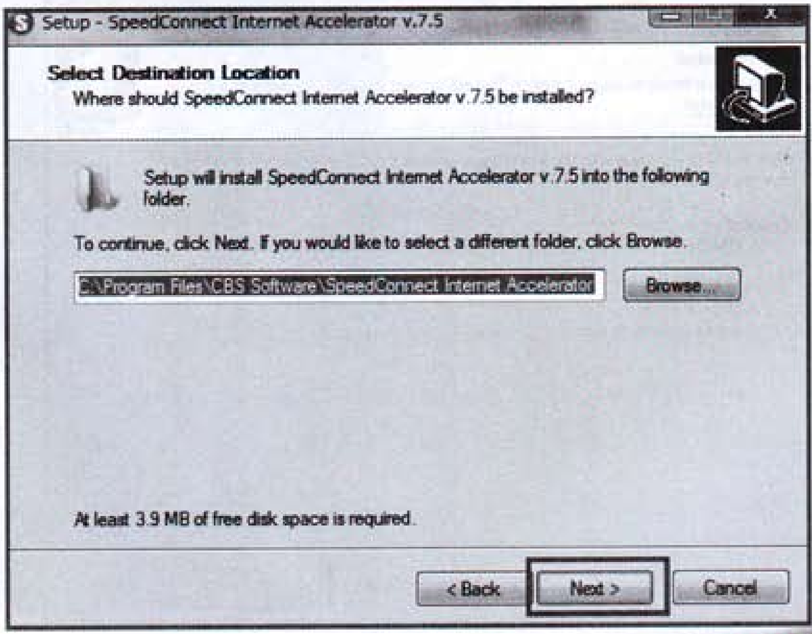
စီဒီအတွင်းမှ Program Folder > SpeedConnect7.5 Folder > SpeedConnect75Setup.exe ကို ကလစ်နှစ်ချက် နှိပ်ဖွင့်လိုက်ပါ။ Welcome Box အတွက် Next Button ကိုနှိပ်ပြီးစတင်လိုက်ပါ။

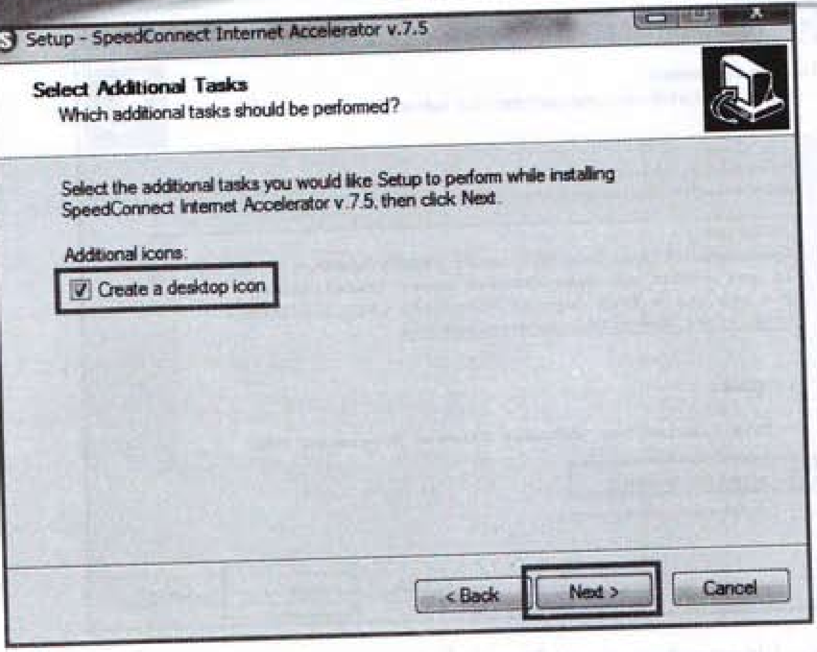




အပေါ်ပုံ License Agreement Box တွင် I accept the --- ကိုရွေးချယ်ပြီး Next Button ကို နှိပ်လိုက်ပါ။

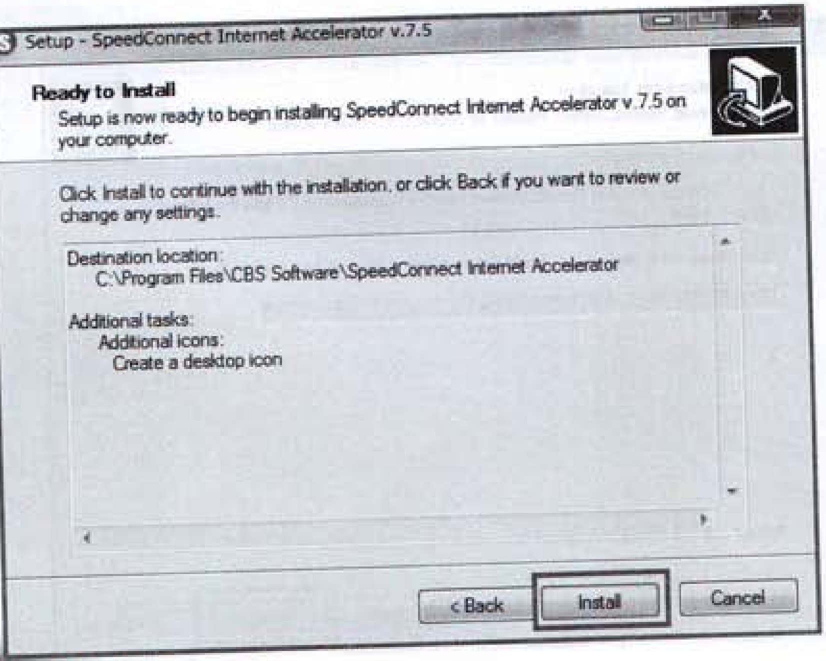
အောက်ပုံကတော့ Install Location အတွက်ဖြစ်လို့ပေးသည့်အတိုင်းယူကာ Next Button ကို နှိပ်ပါ။

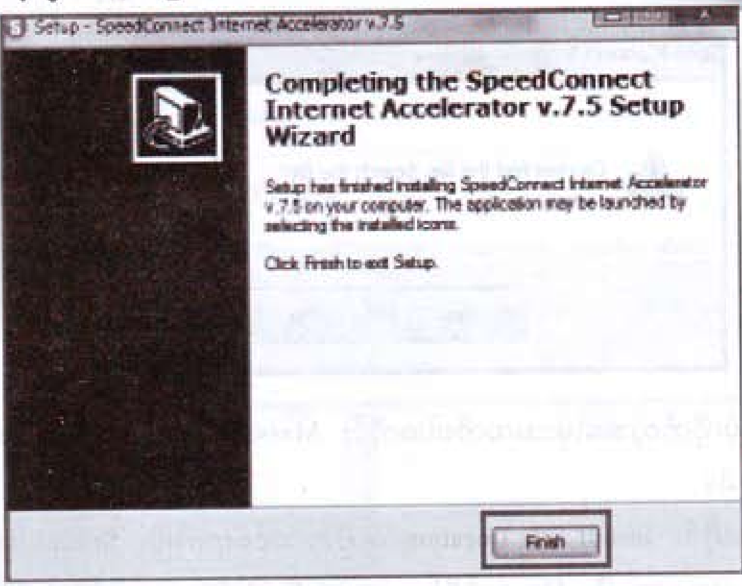


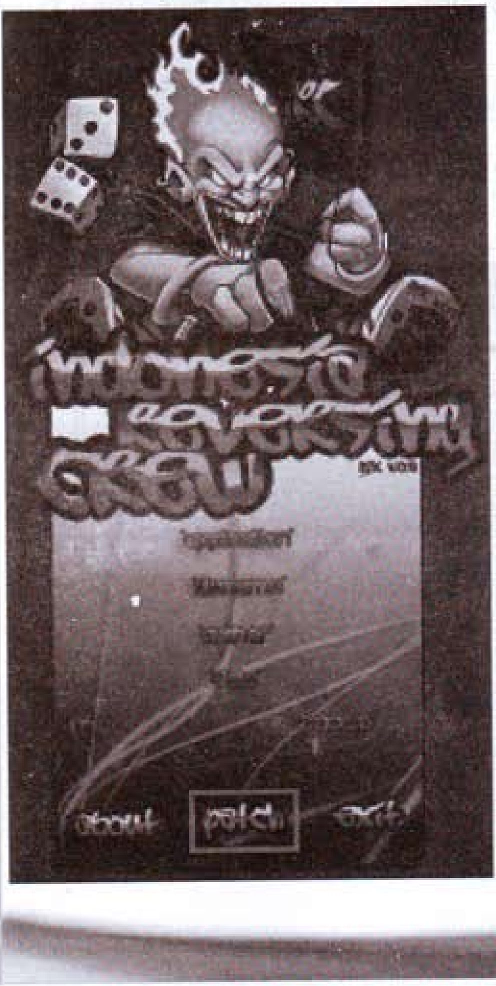


အပေါ်ပုံတွင် Create a desktop icon ကိုအမှတ်ခြစ်ရွေးချယ်ကာ Next Button ကို နှိပ်လိုက်ပါ။

အောက်ပုံမှာ Ready To Install ဖြစ်ပြီးလားမေးလို့ Install Button ကိုသာနှိပ်လိုက်ပါ။







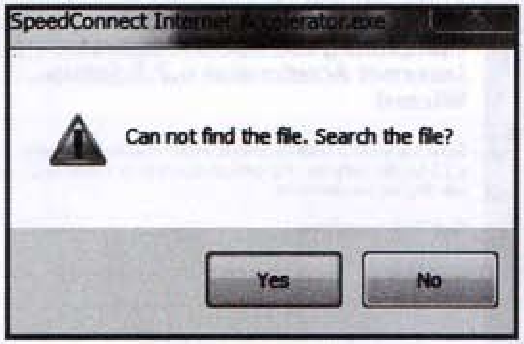
အပေါ်ပုံတွင် Installပြုလုပ်တာပြီးသွားပြီဖြစ်လို့ Finish Button ကို နှိပ်လိုက်ပါ။

ယခုဆော့ဖ်ဝဲကိုလိုင်စင်ဗားရှင်း သုံးနိုင်ရန်အတွက် NotePadဖြင့်လိုင်စင်နံပတ်ထည့်ပေးထားပေမယ့် အလွယ်တကူ Patch စနစ်ဖြင့်သာလိုင်စင်ရယူရအောင်။

၄င်း Folder အတွင်းရှိ SpeedConnect.internet .accelerator 7.5-patch.exeကိုနှိပ်လိုက်ပါ။ ဘယ်ဘက်ပုံအတိုင်းတွေ့မြင်ရပါမယ်။

Patch ကိုနှိပ်လိုက်ပါ။ သတိထားရမှာကတော့ အချို့ Anti-Virus Programတွေက Patch, KeyGun Software တွေကို Trojen Virus အဖြစ်ပြတတ်ပါတယ်။

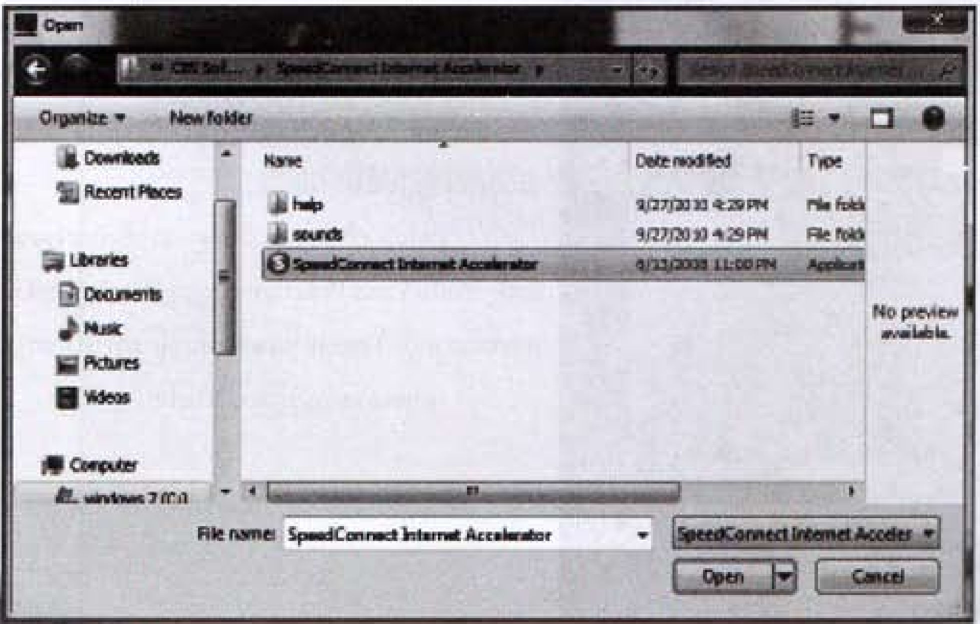
Ignore ဖြင့်ခွင့်ပြုလိုက်ပါ။

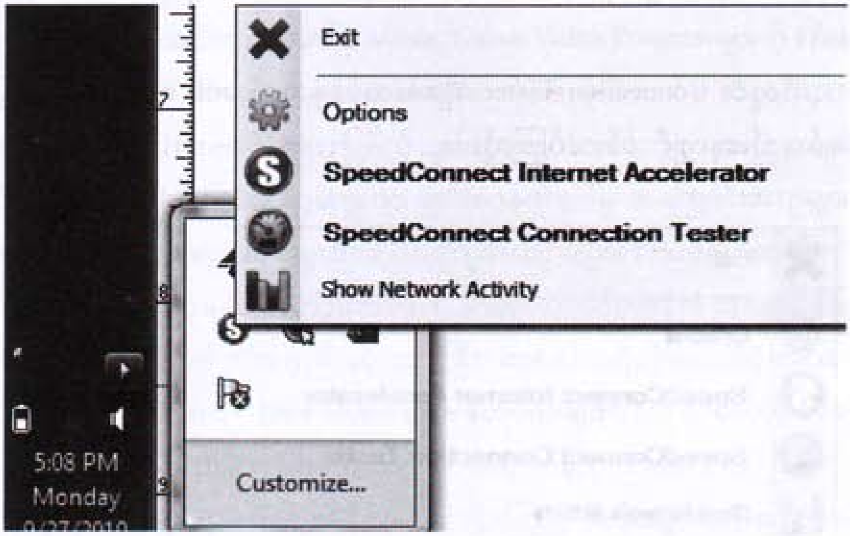


Patch ကိုနှိပ်လိုက်တဲ့အခါမှာအထက်ပါအတိုင်း Massage Box တက်လာပါလိမ့်မယ်။ Yes Button ကိုနှိပ်လိုက်ပါ။

အောက်ပုံအတိုင်း Install File Location အတိုင်း ဝင်ရောက်ပြီး SpeedConnect Internet Accelerator.exe ကိုသွားရှာပေးပြီး Open ကိုနှိပ်ရပါမယ်။ Patch Box အောက်နားတွင် Patch Done ဟုစာထိုးသွားလျှင် လိုင်စင်ဗားရှင်းသုံးခွင့်ရပါပြီ။

ပုံမှန်အားဖြင့် C:\Program File\CBS Software\ SpeedConnect Internet Accelerator Folder\ အောက်မှာရှိနေပါတယ်။ C:\ Drive Latter ကတော့လက်ရှိ Windows ရဲ့ Drive Latter ဖြစ်ပါတယ်။



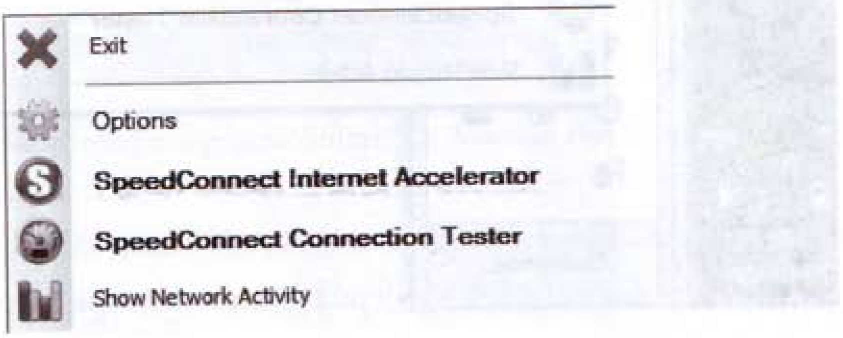


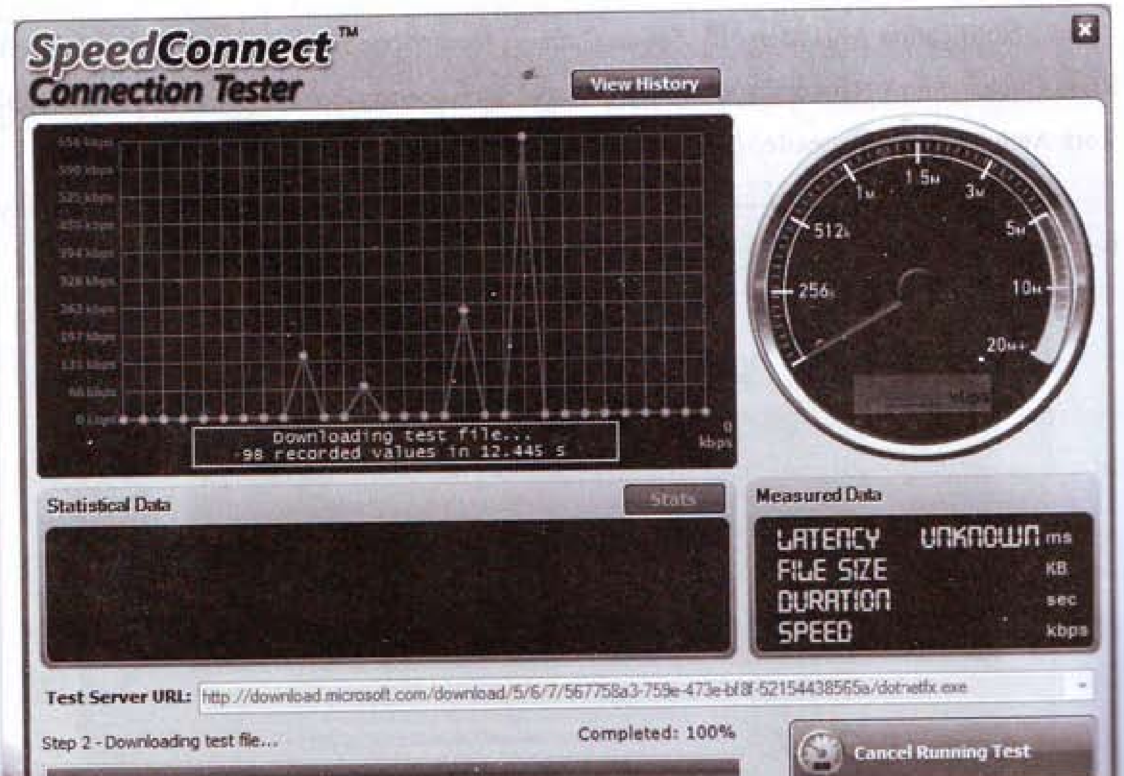
Notification Area အတွင်းရှိ Speed Connect Icon ကိုကလစ်နှစ်ချက်နှိပ်လျှင်၊ ဒါမှမဟုတ် Right Click မှ Show Network Activity နှိပ်လိုက်လျှင် မျက်နှာစာအောက်ခြေ ညာဘက်နားတွင် Network Atcivity Box ပေါ်လာပါလိမ့်မယ်။

အဆိုပါ Box တွင် လိုင်းအလျားများဖြင့် ကြိမ်နှုန်းကိုလှုပ်ရှားပြနေပါလိမ့်မယ်။ ထို Activity Box ကိုမမြင်စေလိုလျှင် ညာဘက်အပေါ်ထောင့်ရှိ Hide ကိုနှိပ်လိုက်ပါ။

အဆိုပါ Right Click အတွင်းမှ SpeedConnect Connection Tester နှိပ်ပြီး အင်တာနက်လိုင်းကို စမ်းသပ်နိုင်ပါတယ်။

အောက်ဘက်တွင် Connection Tester ကိုစမ်းသပ်နေသည်အား တွေ့ရတဲ့ပုံဖြစ်ပါတယ်။ လိုင်းဝင်အား အရမ်းနည်းနေလျှင် စမ်းသပ်ကြည့်ပါ။





Light Downloader Program အသုံးချလေ့လာခြင်း

စာဖတ်သူဟာ အင်တာနက်ပေါ်မှ Music, Game, Video, Program များကို Download မကြာခဏ ချရသူဖြစ်နေလျှင် ယခု Program လေးကအလွန်အသုံးတည့်ပါတယ်။ စာရေးသူလက်ရှိသုံးနေသော Program လေးဖြစ်လို့ Honest Hacker ဖြစ်လိုသူတွေအတွက်လက်တို့ရတာပါ။ ဘာဆိုင်လို့လဲလို့တော့ မထင်လိုက်ပါနဲ့။ Hacker ဖြစ်ချင်သူတွေဟာ အင်တာနက်ပေါ်မှ အကြောင်းအရာများစွာကို ရယူကူးချ လေ့လာနေရပါတယ်။ Program တွေကိုလည်း ဒုက္ခအတွေ့ခံပြီးစမ်းသပ်ရပါတယ်။

စာဖတ်သူများယုံမလားတော့မသိဘူး။ စာရေးသူအင်တာနက်သုံးနေချိန်မြင်ချင်စမ်းပါဘိ။ ကွန်ပျူတာနှစ်လုံးလောက်ကိုအနည်းဆုံးထားပြီး တစ်ခါတရံသုံးလေးလုံးအထိ တစ်ယောက်ထဲ ကိုင်ပါတယ်။ တစ်လုံးကို Download နှစ်ခုလောက်ချရိုင်းလိုက်တယ်။ နောက်တစ်လုံးကို နာမည်ကျော်ကြားနေတဲ့ Black Website တွေကိုဝင်ရောက်လေ့လာပါတယ်။

ဒုက္ခကိုသိလာမှ သုခကိုပြောပြနိုင်မှာပါ။ ဒါ့ကြောင့် ဒီလိုတွေဝင်သုံးလေ့လာပြီး ဖြေရှင်းရမယ့် နည်းလမ်းတွေကိုရှာဖွေကာ ပြန်လည်ဝေငှရပါတယ်။

စကားတွေလဲဘေးရောက်ကုန်ပါပြီ။ ပြန်ဆက်ရအောင်။ Light Download Program ဟာ Download လုပ်ချိန်အလွန်ကြာကြာရယူရတဲ့အခါမျိုးတွေမှာ အသုံးဝင်ပါလိမ့်မယ်။ ဒါပေမယ့် ဆိုင်တွေမှာ သုံးသူတွေအတွက်ကတော့ အပေါ့စား Download တွေကိုသာလုပ်သင့်ပါတယ်။

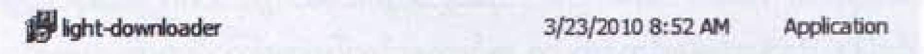
အများသုံးနေရာတွေမှာ အဆိုပါကဲ့သို့ Download Program တွေကိုတပ်ဆင်ထားခဲပါတယ်။ အများအားဖြင့် Download Manager လောက်သာထည့်သွင်းထားကြပါတယ်။ ဒါတောင်အချို့ဆိုင်တွေမှာ License Out of Date ဖြစ်နေလို့ လိုင်စင်နံပတ်ထည့်ပေးပါဆိုပြီး မကြာခဏ Error Massage Box တွေ တတ်တတ်လာလို့ ပိတ်နေရတာတွေတောင်ရှိပါတယ်။

ယခု ဆော့ဖ်ဝဲလ်ကတော့ မီးပျက်လို့ပဲဖြစ်ဖြစ်၊ အချိန်မရတော့လို့ပဲဖြစ်ဖြစ်၊ လိုင်းကျသွားလို့ပဲ ဖြစ်ဖြစ် ရပ်သွားတဲ့အခါ၊ ပြန်စသည်နှင့် ပြန်လည်မောင်းနှင်နိုင်ပါတယ်။ ရောက်လေရာနေရာက ဆက်လက် Download လုပ်ပေးပါတယ်။

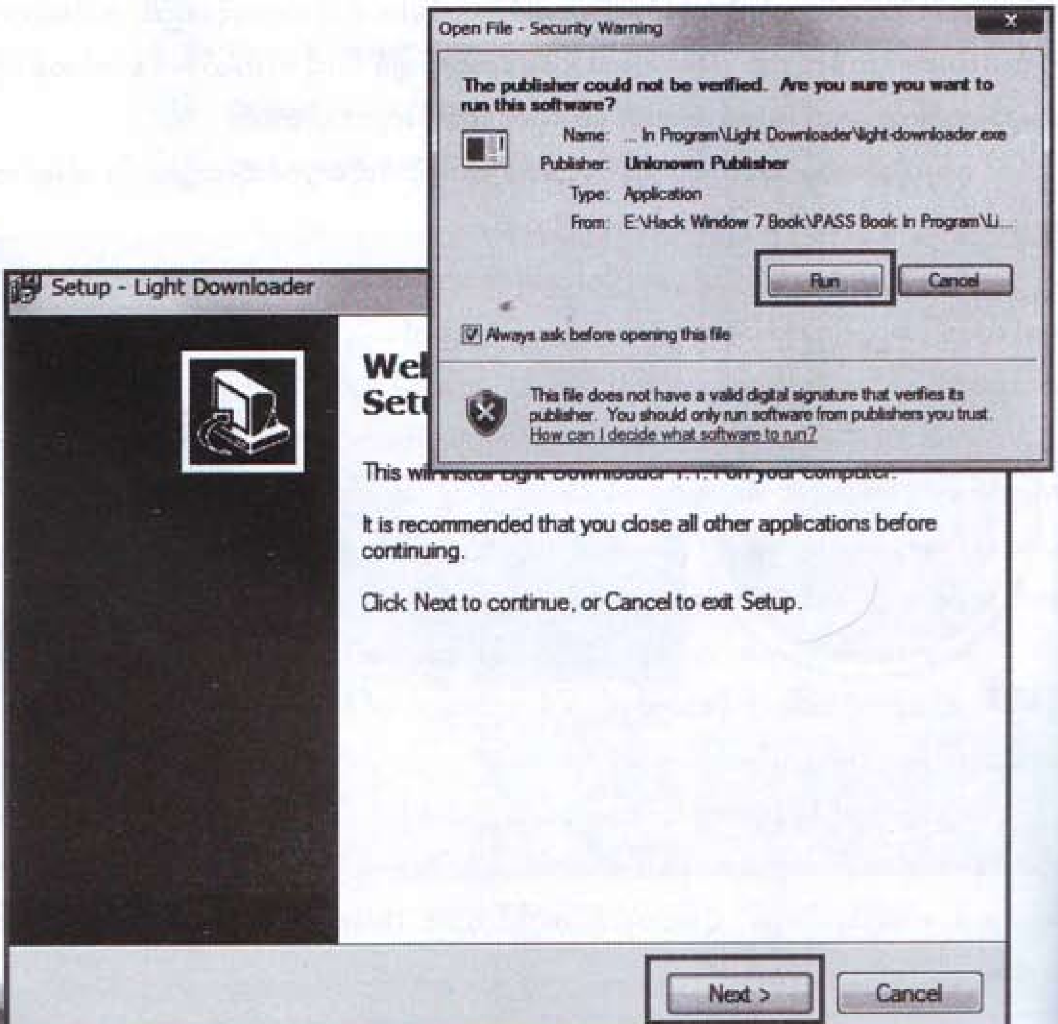
ကူးယူတဲ့အရှိန်နှုန်းကလည်း အတော်အသင့်မြန်ဆန်ပါတယ်။ လက်ရှိသုံးနေတဲ့ Connection ကိုမထိခိုက်စေပဲ နောက်ကွယ်ကနေသာ Download လုပ်နေတာဖြစ်လို့ လိုင်းကျပ်ပြီးလေးသွားခြင်းမျိုး မရှိပါဘူး။ စာရေးသူဆိုလျှင် သုံးလေးခုထိ တပြိုင်တည်း Download လုပ်တတ်ပါတယ်။ သုံးနေတဲ့ Website လိုင်းကတော့ ပုံမှန်ပါပဲ။

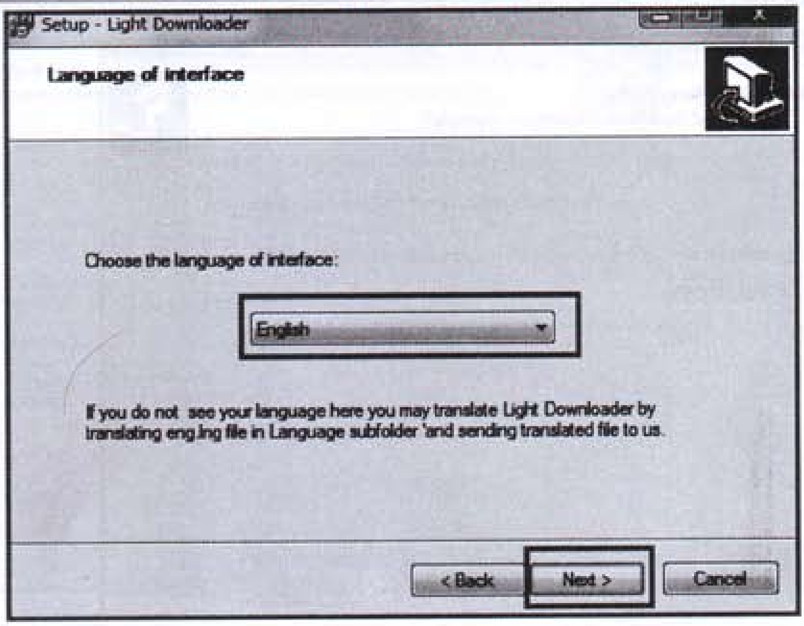
Light Downloader Program Installation

Light Download Program ကိုစတင် Install ပြုလုပ်ရန် စာအုပ်ပါစီဒီအတွင်းမှ Program Folder> Light Downloader Folder ကိုဖွင့်ပြီး Light Downloader.exe ကိုကလစ်နှစ်ချက်နှိပ်လိုက်ပါ။

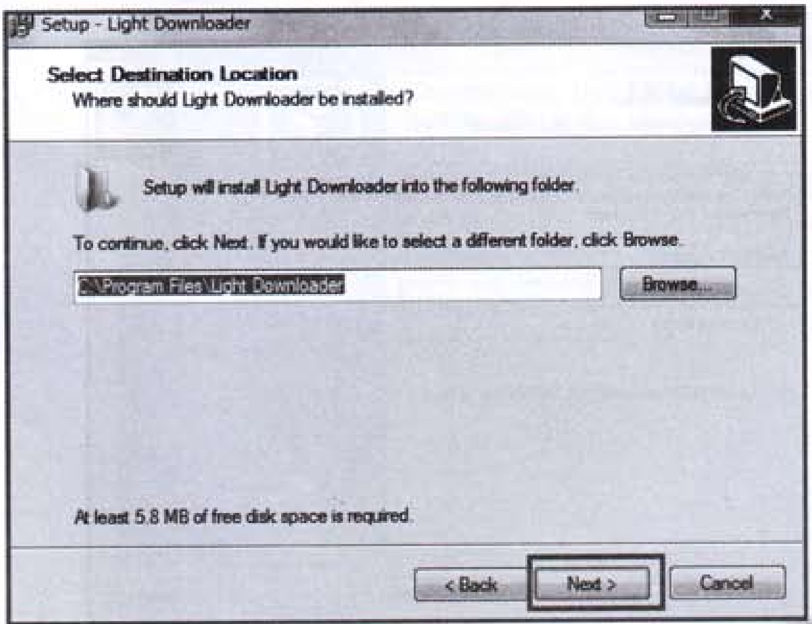


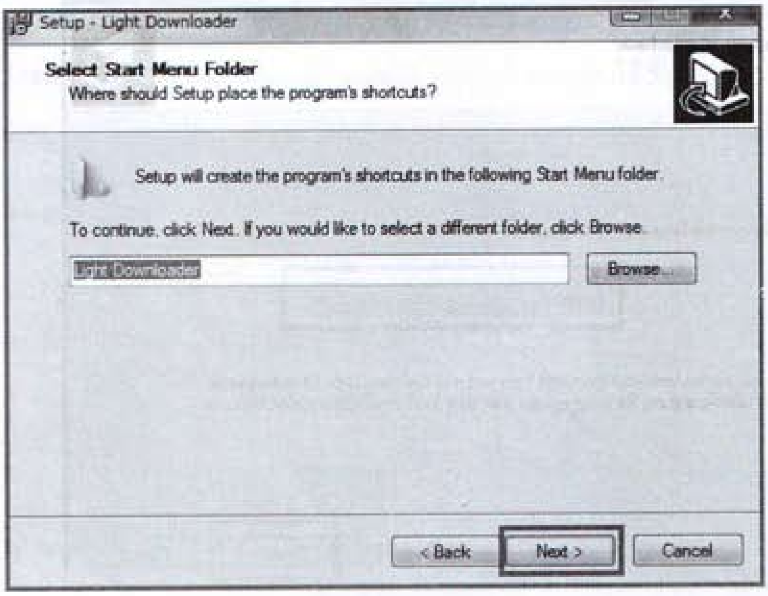
အောက်ပါပုံအတိုင်း Security Warning ပေါ်လာတဲ့အခါ Run ကိုနှိပ်လိုက်ပါ။ Welcome Box ပေါ်လာပါလိမ့်မယ်။ Next Button ကိုနှိပ်လိုက်ပါ။



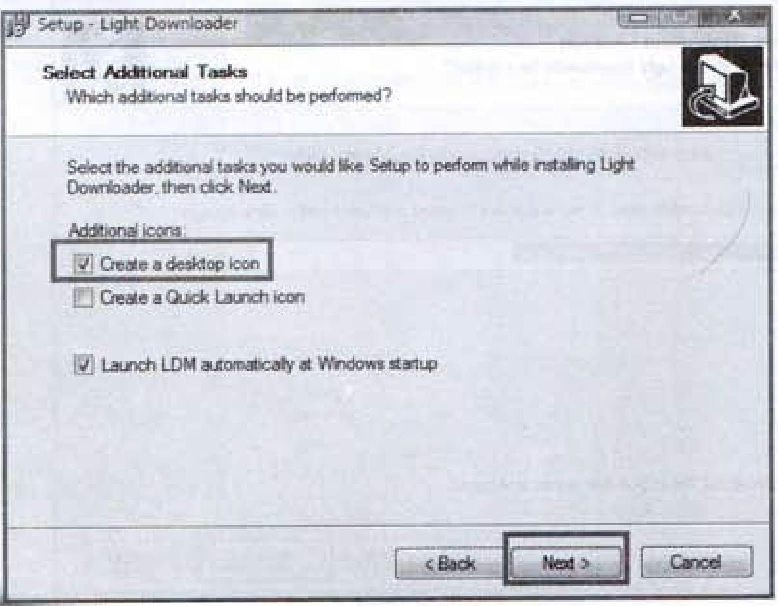


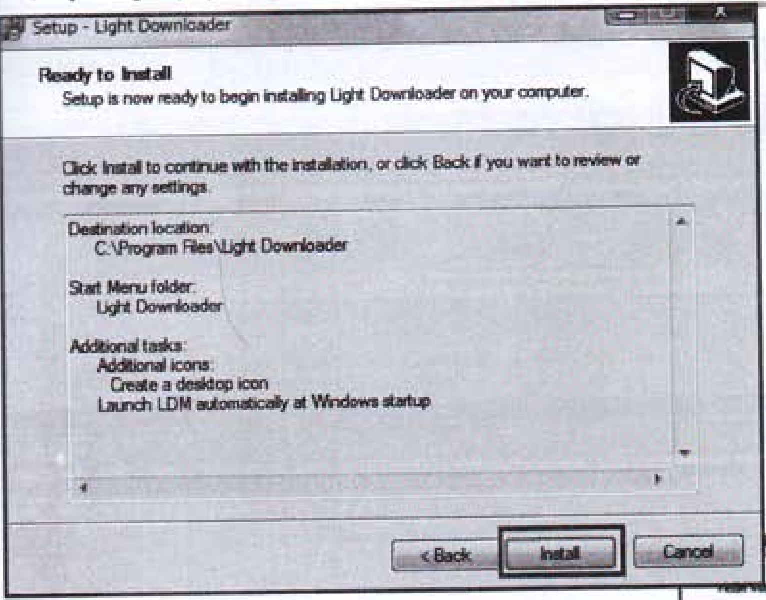
အထက်ပုံတွင် Language အတွက်ဖြစ်၍ English ကိုသာရွေးကာ Next Button နှိပ်လိုက်ပါ။ အောက်ပုံတွင် Install File Location အတွက်ပေးသည်ကိုသာယူပြီး Next Button ကိုနှိပ်လိုက်ပါ။

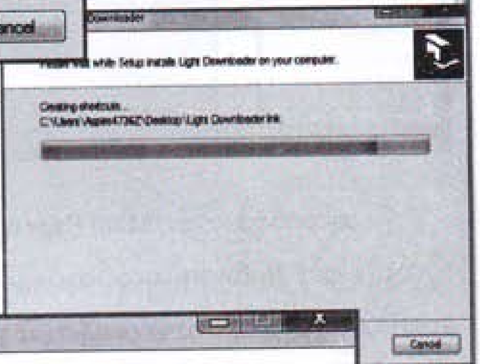




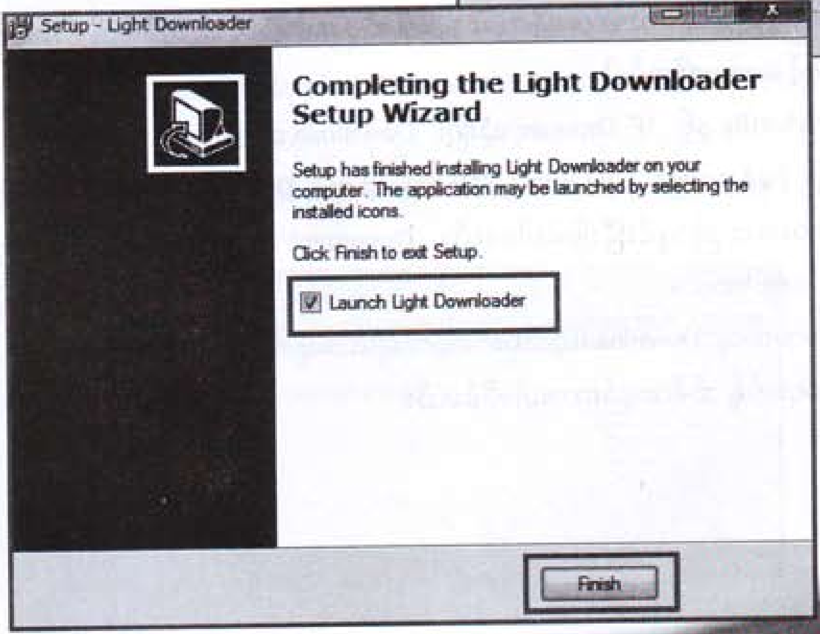
အထက်ပုံတွင် Start Menu အတွက်အမည်ပေးရန်ဖြစ်၍ ပေးသည့်အတိုင်းထားကာ Next Button နှိပ်လိုက်ပါ။ အောက်ပုံတွင် Create a desktop icon တွင်အမှတ်တတ်ပြီး Next Button ကိုနှိပ်လိုက်ပါ။

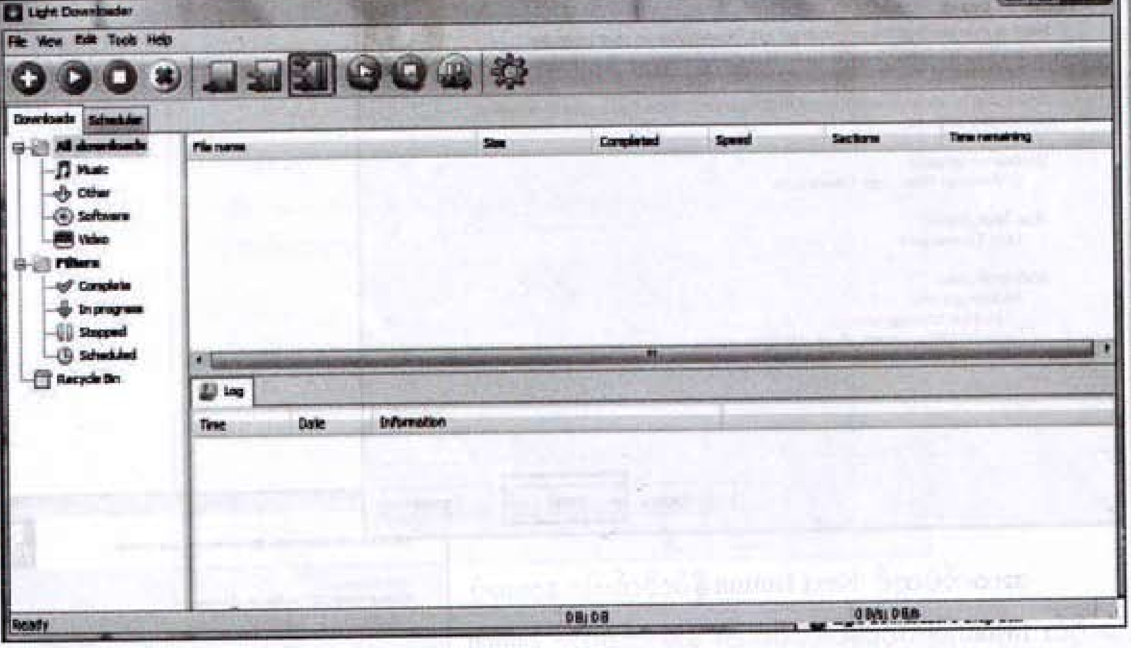






အထက်ပုံတွင် Next Button နှိပ်လိုက်ပါ။ အောက်ပုံအတိုင်း Install ပြုလုပ်နေပါလိမ့်မယ်။ အောက်ပုံတွင် Lunch Light Downloader ကိုအမှတ်တတ်ပြီး Finish Button ကိုနှိပ်လိုက်ပါ။ Install လုပ်ခြင်းပြီးဆုံးသွားပါပြီ။



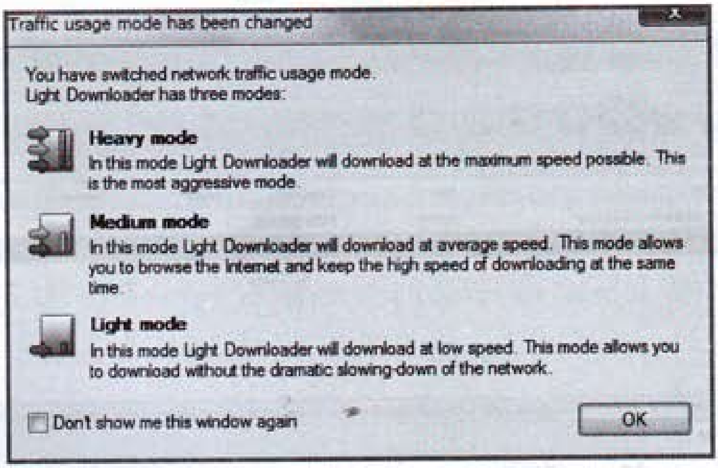


အထက်ပုံအတိုင်း Main Page ကိုတွေ့ရပါပြီ။ အခမဲ့ဗားရှင်းဖြစ်လို့ လိုင်စင်ကီးတွေ မေ့ထားလိုက်ပါ။ ၄င်း Software အလုပ်လုပ်နေလျှင် စာမျက်နှာ ညာဘက်ထောင့်အောက်နားတွင် Icon လေးပေါ်နေပါလိမ့်မယ်။ အလိုအလျောက် ထိန်းကျောင်းစနစ်ဖြစ်လို့ အင်တာနက်သုံးနေစဉ် သီးသန့်ဖွင့်ပေးဖို့မလိုအပ်ပါ။

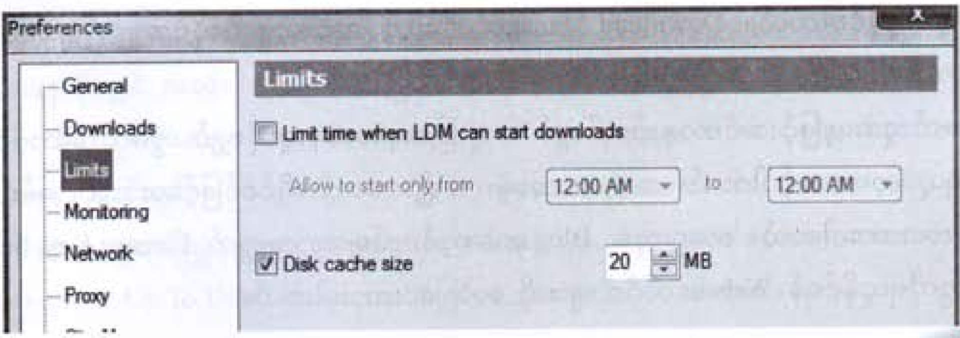
Mozilla နှင့် IE Browser သုံးပြီး Download ဆွဲတဲ့အခါ အလိုအလျောက်မောင်းနှင်ပေးပါလိမ့်မယ်။ ပုံမှန်အားဖြင့် C:\ Drive Latter အောက်တွင် Download Folder တစ်ခုကို Software Install လုပ်စဉ်ကပင်ထည့်သွင်းပြီးဖြစ်ပါတယ်။ Document > Download Folder တွင်လည်း Folder တစ်ခုရှိတတ်ပါတယ်။

စာဖတ်သူ Download လုပ်လိုက်သောပုံများ၊ အချက်အလက်များဟာ အဆိုပါ Download Folder များတွင်ရောက်ရှိ သိမ်းဆည်းထားပါလိမ့်မယ်။

Download လျှင်မြန်မှုနှုန်းကိုချိန်ယူပေးထားရပါမယ်။ စာရေးသူစမ်းသပ်ထားသည်မှာ နှစ်နည်းရှိပါတယ်။ ပထမနည်းကတော့ Standard Bar မှ Mode Setting သုံးမျိုးတွင် Heavy Mode ကိုရွေးပေးထားပါ။

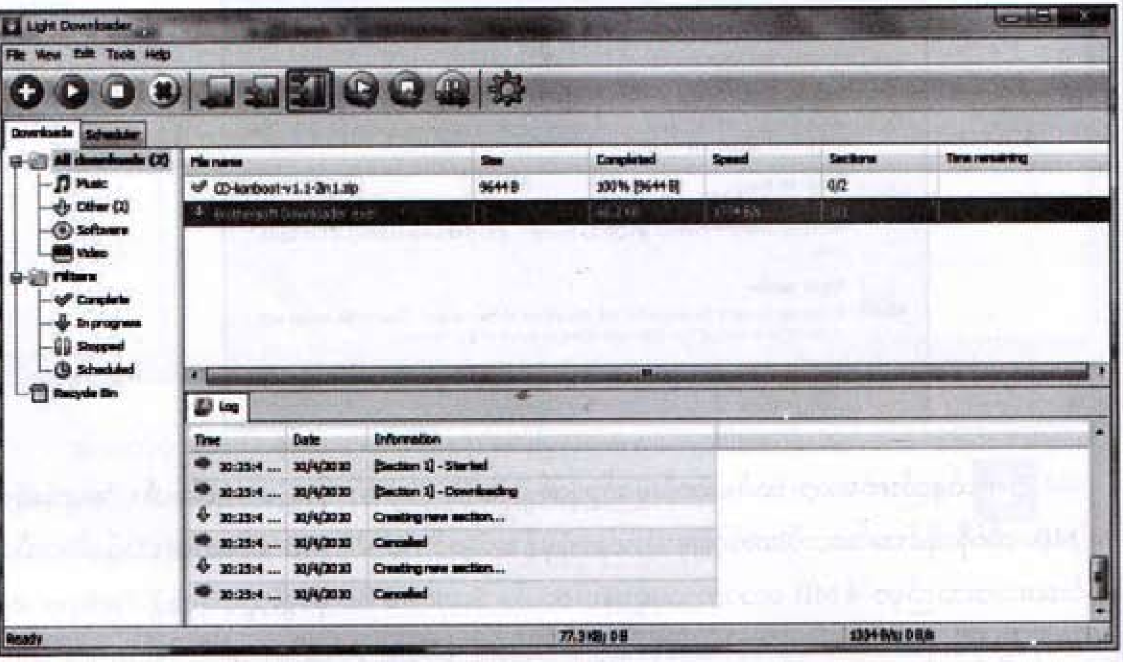


ဒုတိယနည်းကတော့ ထပ်ဆောင်းမှတ်ဉာဏ် Cache Size ကိုတိုးချဲ့ပေးရပါမယ်။ အများဆုံး 30 MB ထိကိုလိုင်းအားတော်တော်ကျမှသုံးပါ။ ပုံမှန်အားဖြင့် 15-20 MB ထိသာသုံးသင့်ပါတယ်။ မူရင်းပေးထားသည်မှာ 4 MB လောက်သာရှိနေပါတယ်။ Standard Bar မှခွေးသွားစိတ်ပုံ Preferences Icon ကိုရွေးနှိပ်လိုက်ပါ။ အောက်ပါအတိုင်းတွေ့မြင်ရလျှင် Limits Tab ကိုရွေးချယ်ပါ။ Disk Cache Size ကိုအမှတ်တတ်ပြီး 20 MB ကိုထည့်လိုက်ပါ။ အလျဉ်းသင့်သလို အလျှော့အတင်းလုပ်သွားပါ။



အောက်ပါပုံကတော့ Download လုပ်ငန်းခွင်မှမြင်ကွင်းပဲဖြစ်ပါတယ်။ အမှန်ခြစ်လေးတွေပေါ်နေတာကတော့ အဆင်ပြေစွာ Download ပြီးဆုံးသွားတဲ့သင်္ကေတဖြစ်ပါတယ်။

ခေတ္တရပ်ထားလိုလျှင် ဒါမှမဟုတ် လိုင်းကျသွားလျှင် Pause Icon ဒီလိုသင်္ကေတလေးပေါ်လာပါတယ်။ ပြန်လည်စတင်လိုတဲ့အခါ အဆိုပါဖိုင်ကိုရွေးချယ်ပြီး Play Icon ကိုနှိပ်လိုက်ပါ။



Hight Speed Download လုပ်နိုင်သော Software များစွာရှိပါတယ်။ အင်တာနက်ပေါ်မှာ အလွယ်တကူရယူနိုင်ပါတယ်။ Download Manager ကိုတော့ အင်တာနက်ဆိုင်အတော်များများက အသုံးပြုပါတယ်။

စာဖတ်သူအနေဖြင့် အင်တာနက်ပေါ်တွင် အထူးပြုလေ့လာနေသူဆိုလျှင် တွဲဖက် ဆော့ဖ်ဝဲလ်များစွာကို ရယူလေ့လာသင့်ပါတယ်။ အချို့က အခမဲ့၊ အချို့ကတော့ လိုင်စင်ဖြင့်ပေးသလို၊ စမ်းသပ်အဆင့်လည်းပေးထားပါတယ်။ စာရေးသူရဲ့ Blog မှာဆော့ဖ်ဝဲလ်များစွာအတွက် License Key, Serial Number တွေကိုရယူနိုင်ရန် Website လိပ်စာများကို ဖော်ပြပေးထားပါတယ်။

Honest Hacker တို့အတွက် Proxy ဆိုသည်မှာ

ယခုတလော မြန်မာအပါအဝင် နိုင်ငံတကာ Internet သုံးသူများအကြား ရေပန်းအစားဆုံး
စကားလုံးဖြစ်နေပါတယ်။ Proxy Server ဆိုတာကတော့ အသုံးချဒေသအတွင်းမှ အင်တာနက်
ခေါ်ဆိုမှုကိုထိန်းချုပ်ထားတဲ့ စနစ်တစ်ခုဖြစ်ပါတယ်။ Network တွေရဲ့ Proxy setting ကိုမည်သူမဆို
ပြင်ဆင်ရယူနိုင်ပါတယ်။

Proxy ကိုနှစ်မျိုးတွေ့နိုင်ပါတယ်။ Internal Proxy နှင့် External Proxy တို့ဖြစ်ပါတယ်။
သက်ဆိုင်ရာဒေသအတွက် ISP မှ Proxy Port တွေကိုချပေးထားပါတယ်။ အဆိုပါ Proxy ကို ISP
Internal Proxy လို့ခေါ်ဆိုပါတယ်။ Internal Proxy တွေကိုပြင်ဆင်ခွင့်ဟာ Admin ဖြစ်တဲ့ ISP
နှင့်သာသက်ဆိုင်ပါတယ်။

External Proxy တွေကို လွတ်လပ်စွာသုံးစွဲခွင့်အား အင်တာနက်သုံးစွဲသူ User တိုင်းရရှိနိုင်
ပါတယ်။ မည်သူမဆို လွတ်လပ်စွာ ပြောင်းလဲသုံးစွဲနိုင်ပါတယ်။ အဆိုပါ External Proxy တွေကို
အသုံးမပြုစေဖို့ ပိတ်ပင်လို့မရနိုင်ပါဘူး။ ပိတ်ပင်ချင်လျှင် အင်တာနက်သုံးခွင့်တစ်ခုလုံးအား
ပိတ်ပင်ရပါမယ်။

စာဖတ်သူဟာ အခြားနိုင်ငံတစ်ခုမှ External Proxy Code တစ်ခုခုကို အကြောင်းတစ်ခုခုကြောင့်
ရလာလျှင် မည်သည့်နိုင်ငံတွင်သုံးစွဲနေပါစေ ထည့်သွင်းသုံးစွဲနိုင်ပါတယ်။ နိုင်ငံတကာ အင်တာနက်
ဆိုင်ရာဥပဒေကြောင်းအရပါ ခွင့်ပြုထားပါတယ်။ Browser တွေတွင်အလွယ်တကူထည့်သွင်းသုံးစွဲခွင့်
ရှိသည်ကို ကြည့်ခြင်းအားဖြင့် နည်းဥပဒေအရပါခွင့်ပြုထားကြောင်းတွေ့ရပါတယ်။

သို့သော်လည်း မကောင်းသောအချက်များကိုထောက်ပြဖို့လိုပါသေးတယ်။ အချို့သော
ပညာရှင်တို့သည် အင်တာနက်ကွန်ရက်ပေါ်တွင် လေ့လာမှုများပြုလုပ်သောအခါ နိုင်ငံတကာမှ Ex-
ternal Proxy Code တွေသိလျှင် ပေါ့ပါးသွက်လက်စွာ လိုင်းပေါ်တွင်သုံးစွဲနိုင်ကြသော်လည်း၊ Exter-
nal Proxy Code ဟာမကြာခဏပြောင်းလဲနေတာကြောင့် အခက်အခဲတွေ တွေ့နေရပါတယ်။
စာရေးသူဆိုလျှင် အဆိုပါကဲ့သို့သော ပြဿနာကိုမကြာခဏတွေ့ကြုံနေရပါတယ်။

ဒီအတွက် Auto Proxy Program တွေ၊ Proxy Support Website တွေကိုလေ့လာခဲ့ပါတယ်။
အင်တာနက်ပေါ်တွင် မည်သူမဆိုအလွယ်တကူလေ့လာရယူနိုင်ပါတယ်။ အကောင်းဆုံး Proxy Sup-
port Website များကိုညွှန်းရလျှင် www.proxy4free.com, www.publicproxyservers.com တို့သည်
နိုင်ငံတကာမှ Up To Date ဖြစ်နေသော Proxy Code တွေကိုပေးပါတယ်။

Proxy အကြောင်းထပ်မံရှင်းပြရလျှင် Network Protocol တွေကိုဦးစွာသိထားရပါမယ်။ အင်တာနက်ပေါ်ပေါက်လာရခြင်းဟာ Protocol System ကိုဖန်တီးနိုင်ခဲ့လို့ပါ။ Protocol System ဆိုတာကတော့ ကွန်ရက်အတွင်းမှအနည်းဆုံး Unit နှစ်ခုကိုချိတ်ဆက်ပေးပြီး အချက်အလက်ကူးပြောင်းမှုပြုစေသောစနစ်ဖြစ်ပါတယ်။

Proxy Code တွေဟာအဆိုပါစနစ်တွေကိုရှင်သန်စေတဲ့အရာတစ်ခုလို့ဆိုနိုင်ပါတယ်။ စာဖတ်သူကိုယ်တိုင် ထည့်သွင်းပြင်ဆင်နိုင်သော Proxy Type တွေကိုရှင်းပြပါ့မယ်။

၁။ HTTP Proxy (Hyper Text Transfer Protocol)

ဒီ Proxy ကတော့ အသုံးအများဆုံး၊ Popular အဖြစ်ဆုံး Proxy တစ်ခုဖြစ်ပါတယ်။ ပုံမှန်သုံး Proxy လို့လဲခေါ်ဆိုနိုင်ပါတယ်။ စာဖတ်သူများအဓိကထားပြုပြင်ယူရမယ့် Proxy လည်းဖြစ်ပါတယ်။

၂။ SSL Proxy (Secure Sockets Layer)

အင်တာနက်ပေါ်မှ လျှို့ဝှက်သောလုပ်ဆောင်ချက်များအတွက်ဖန်တီးပေးထားသော Protocol စနစ်တစ်ခုဖြစ်ပါတယ်။

၃။ FTP Proxy (File Transfer Protocol)

အင်တာနက်ပေါ်ကိုအသုံးပြုပြီး အချက်အလက်လွှဲပြောင်းရာတွင် အသုံးများစနစ်ဖြစ်ပါတယ်။ Website များမှ Download ရယူခြင်း၊ ပေးအပ်ခြင်းအတွက် ၄င်းစနစ်ဟာအသုံးများပါတယ်။

၄။ Gopher Proxy (Search Protocol)

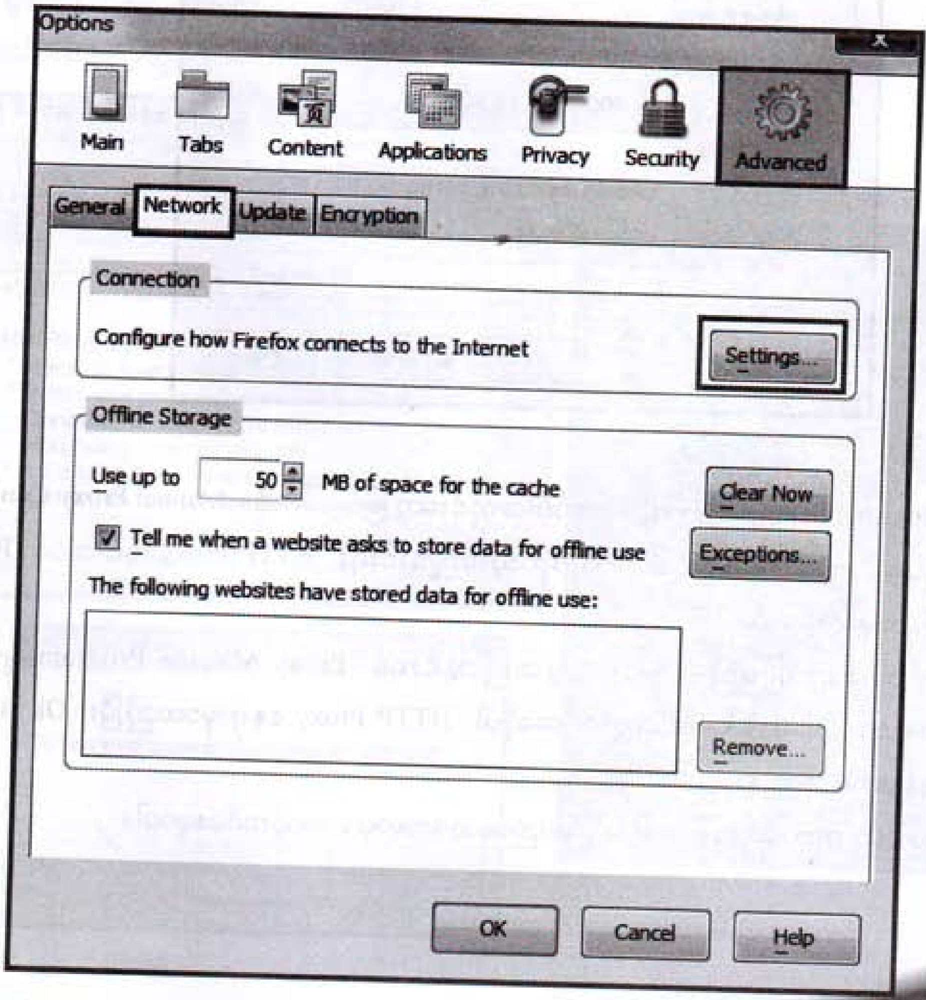
အချက်အလက်များရှာဖွေဖို့အတွက် အသုံးဝင်ပါတယ်။ Web Technology နှင့်အလုပ်တူမှုကွဲစနစ်ဖြစ်နေလို့ ယနေ့ အချိန်မှာတော့ လူသိနည်းလာခဲ့ပါတယ်။

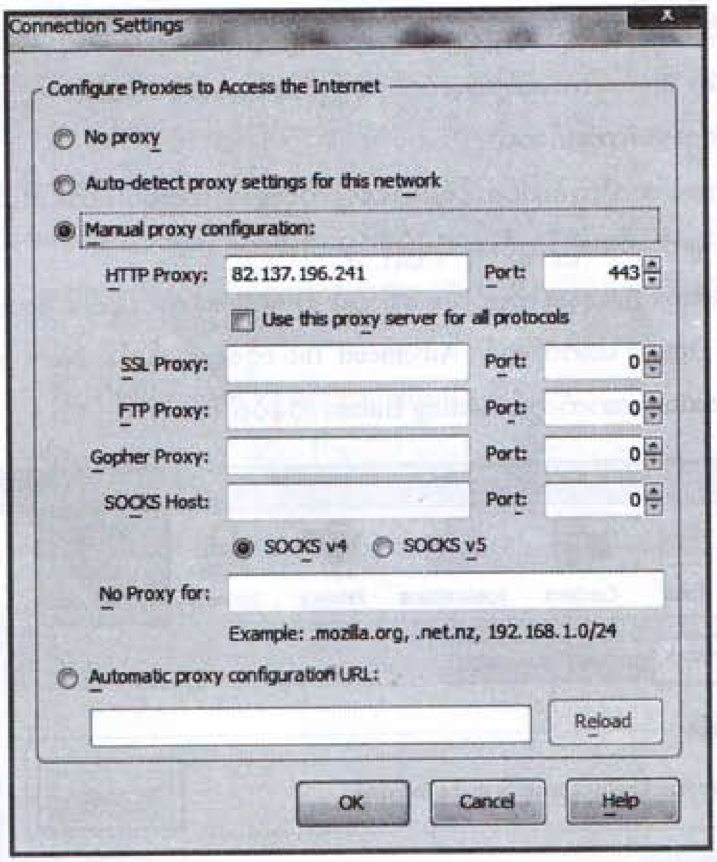
အထက်ပါ Proxy လေးမျိုးအနက်စာဖတ်သူသိထားရမယ့် အသုံးဝင် Proxy ကတော့ HTTP Proxy ပဲဖြစ်ပြီး နောက်ပိုင်းကဏ္ဍအသုံးချ Proxy Code တွေထည့်သွင်းပေးရမယ့်နေရာလည်းဖြစ်ပါတယ်။

စာရေးသူဆိုခဲ့သလို Proxy တွေကိုပြင်ဆင်ပြီး အမြန်နှုန်းတစ်ခုကို အတိုင်းအတာတစ်ခုထိရယူနိုင်ဖို့ Mozilla Firefox Browser ကတော့အကောင်းဆုံးဖြစ်နေပါတယ်။ အလွယ်တကူပြင်ဆင်ထည့်သွင်းနိုင်အောင်တည်ဆောက်ပေးထားပါတယ်။

External Proxy ထည့်သွင်းပြင်ဆင်ရမယ့်နေရာကိုဦးစွာသိထားရပါမယ်။ ဒါမှသာ Proxy Code တစ်ခုသိလာတာနဲ့ ချက်ခြင်းထည့်သွင်းအသုံးပြုနိုင်မှာပါ။

Mozilla Firefox Browser ကိုဖွင့်ပါ။ မရှိလျှင် Download လုပ်ယူပါ။ Tool Menu အတွင်းမှ Option ကိုနှိပ်ပါ။ Option အောက်တွင် Advanced Tab ကိုရွေးချယ်ပါ။ Network Tab ကိုထပ်မံရွေးချယ်ပါ။ Connection အောက်တွင် Setting Button ကိုနှိပ်လိုက်ပါ။





Connection Settings Box ကိုအထက်ပါအတိုင်းတွေ့မြင်ရပါမယ်။ Manual Proxy Configuration ကိုရွေးချယ်ပေးလိုက်ပါ။ ထိုအခါ စာဖတ်သူထည့်သွင်းရန် HTTP Proxy အပါအဝင် Proxy နေရာတွေပွင့်လာပါလိမ့်မယ်။

ဆက်လက်ဖော်ပြမယ့် Proxy ရယူထည့်သွင်းရန် Proxy Manage Program များကို အသုံးပြုပြီးရလာတဲ့ Proxy Code တွေကို အဆိုပါ HTTP Proxy နေရာမှာထည့်ပြီး Ok Button နှိပ်လိုက်တာနဲ့စတင်သုံးဆွဲနိုင်ပါပြီ။

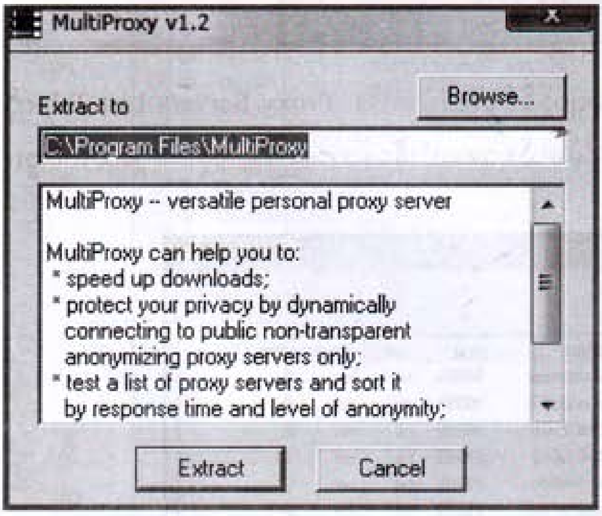
ရိုးသားဟက်ကာတွေဖြစ်လာဖို့ နည်းပညာလေ့လာရာမှာ အသုံးဝင်စေမှာပါ။

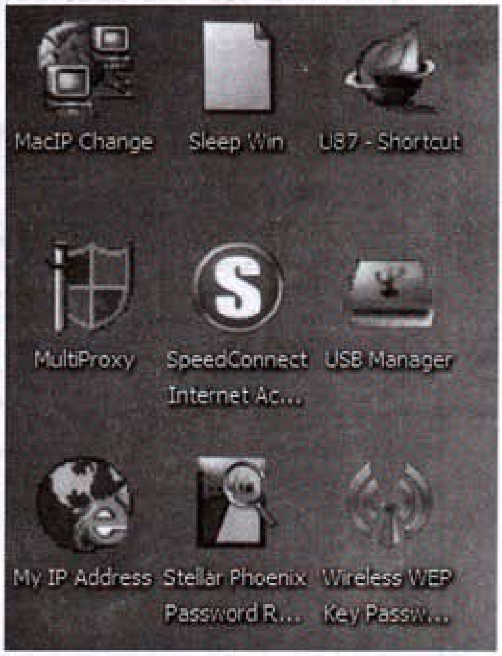
Multi Proxy Program ကိုလေ့လာခြင်း

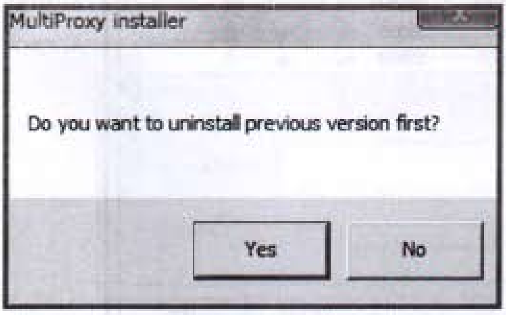
ယခု Program ကတော့ Proxy တွေကိုအလွယ်တကူရှာဖွေပေးမယ့် Multi Proxy Program တစ်ပုဒ်ဖြစ်ပါတယ်။ အသုံးပြုရလွယ်ကူသလို လုပ်ဆောင်မှုစနစ်လည်း ပေါ့ပါးပါတယ်။ အခမဲ့ဗားရှင်းဖြစ်လို့ ရေရှည်လည်းအသုံးပြုနိုင်ပါတယ်။

စတင် Install ပြုလုပ်ရန် စီဒီအတွင်းမှ Program Folder > Multi Proxy Foler ကိုဖွင့်ပြီး အတွင်းရှိ mproxy12.exe ကိုကလစ်နှစ်ချက်နှိပ်လိုက်ပါ။ ချုံ့ထားတဲ့ဖိုင်စနစ်ဖြစ်နေလို့ Extract ကိုနှိပ်ပေးရပါမယ်။ အပေါ်နားတွင် Install File Location ကိုပြထားပါသေးတယ်။

Massage Box ကိုပေးလာလျှင် Yes Button ကိုသာနှိပ်ပေးပါ။ ဘာပြဿနာမှမရှိပါဘူး။ အလွန်မြန်ဆန်စွာထည့်သွင်းသွားလို့ စာဖတ်သူသတိတောင်ထားမိမယ်မထင်ပါ။ အခြား Install တွေလိုမေးခွန်းတွေမများပါ။ Desktop ပေါ်မှာ Multi Proxy Icon လေးရောက်ရှိနေပါပြီ။

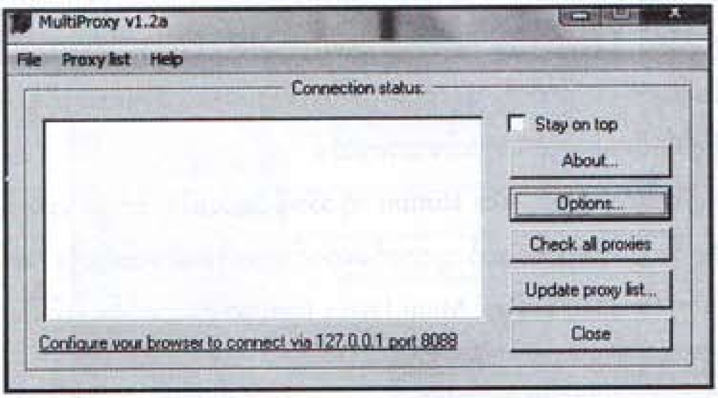




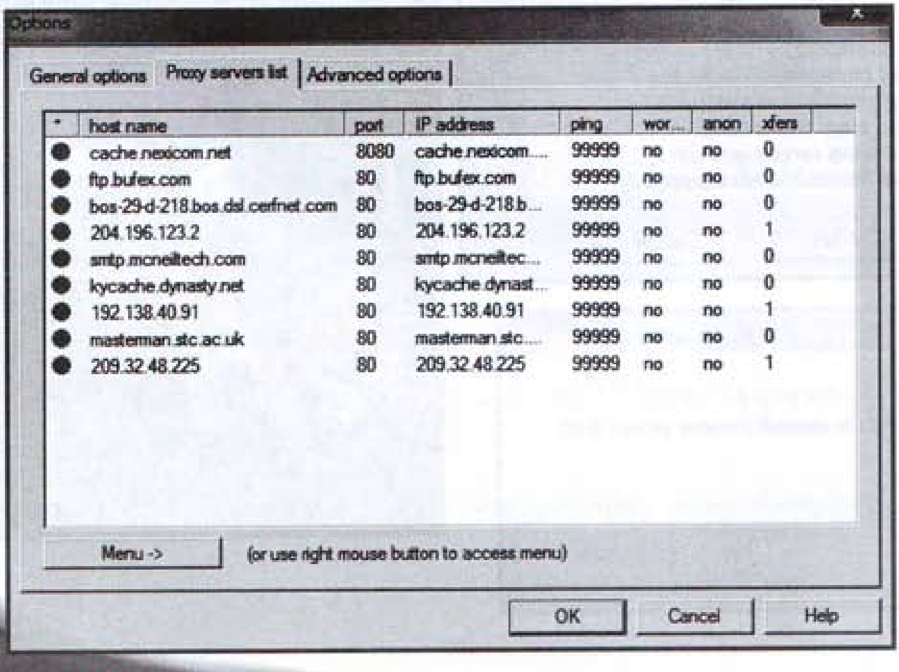


Internet Connection Line ရနေပြီဆိုလျှင် မျက်နှာစာပေါ်မှ MultiProxy Icon ကို ကလစ်နှစ်ချက်နှိပ်လိုက်ပါ။ အောက်ပါအတိုင်းတွေ့ရပါလိမ့်မယ်။

စတင်ရန် Options Button ကိုနှိပ်လိုက်ပါ။



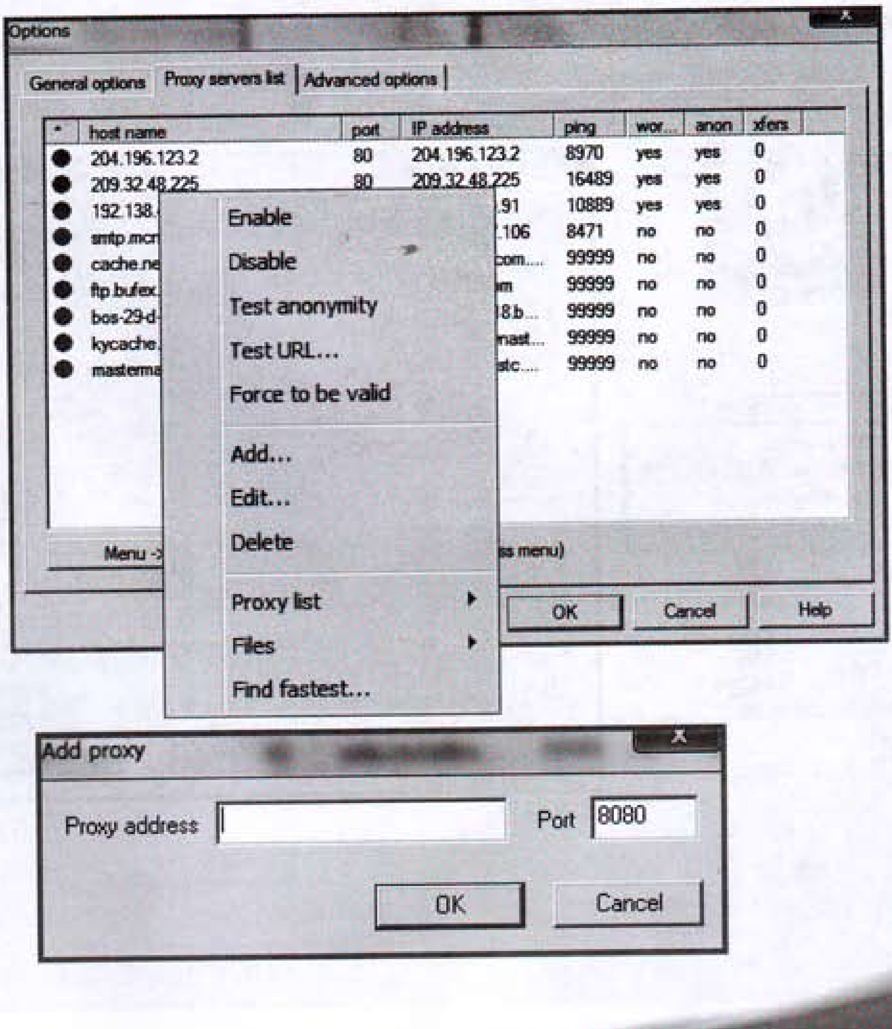
Option Box တွင်ခေါင်းစဉ်သုံးခုရွေးချယ်နိုင်ပါလိမ့်မယ်။ Proxy Servers List Tab ကို ကလစ်နှိပ်လိုက်ပါ။ အောက်ပါအတိုင်းတွေ့ရပါလိမ့်မယ်။ အားလုံးနီနေတာကြောင့် လိုင်းမရှိသေးပါဘူး။



Proxy Code များရရှိရန် လက်ရှိအသုံးပြုနေရာရဲ့ IP Port ကိုပေးရပါလိမ့်မယ်။ အလွယ်ဆုံး လက်ရှိသုံးနေသာ IP Address ကို သိလိုလျှင် အသေးစား ဆိုတာလေးသုံးနိုင်ပါတယ်။ နောက်တစ်မျက်နှာကိုကျော်ဖတ်လိုက်ပါ။

အဆိုပါ ISP Internal Proxy ကိုမှတ်သားပြီး Option Box အောက်နားရှိ Menu Button ကိုဖွင့်ကာ Add ကိုရွေးပေးရပါမယ်။ မှတ်သားထားသည်ကို ထည့်သွင်းပြီး နှိပ်လိုက်သည်နှင့် အောက်ပါပုံအတိုင်း အစိမ်းရောင်လေးတွေရလာပါပြီ။

အဆိုပါ အစိမ်းရောင်လိုင်းတွေကို ရှေ့တွင်ဆိုခဲ့သလို Mozilla Browser တွင်ထည့်သုံးနိုင်ပါပြီ။



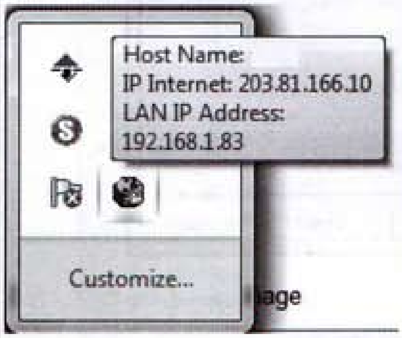
My IP Address Program အသုံးပြု၍ ဆီ IP Address ကိုလေ့လာခြင်း

စာဖတ်သူဟာလက်ရှိသုံးနေတဲ့ IP Address ကိုသိဖို့လိုလာတာမျိုးတွေရှိပါလိမ့်မယ်။ ယခု Program လေးက ပေါ့ပေါ့ပါးပါးဖြင့် စာဖတ်သူလက်ရှိသုံးနေတဲ့ IP Internet Address နှင့် LAN IP Address ကိုဖော်ပြပေးပါတယ်။

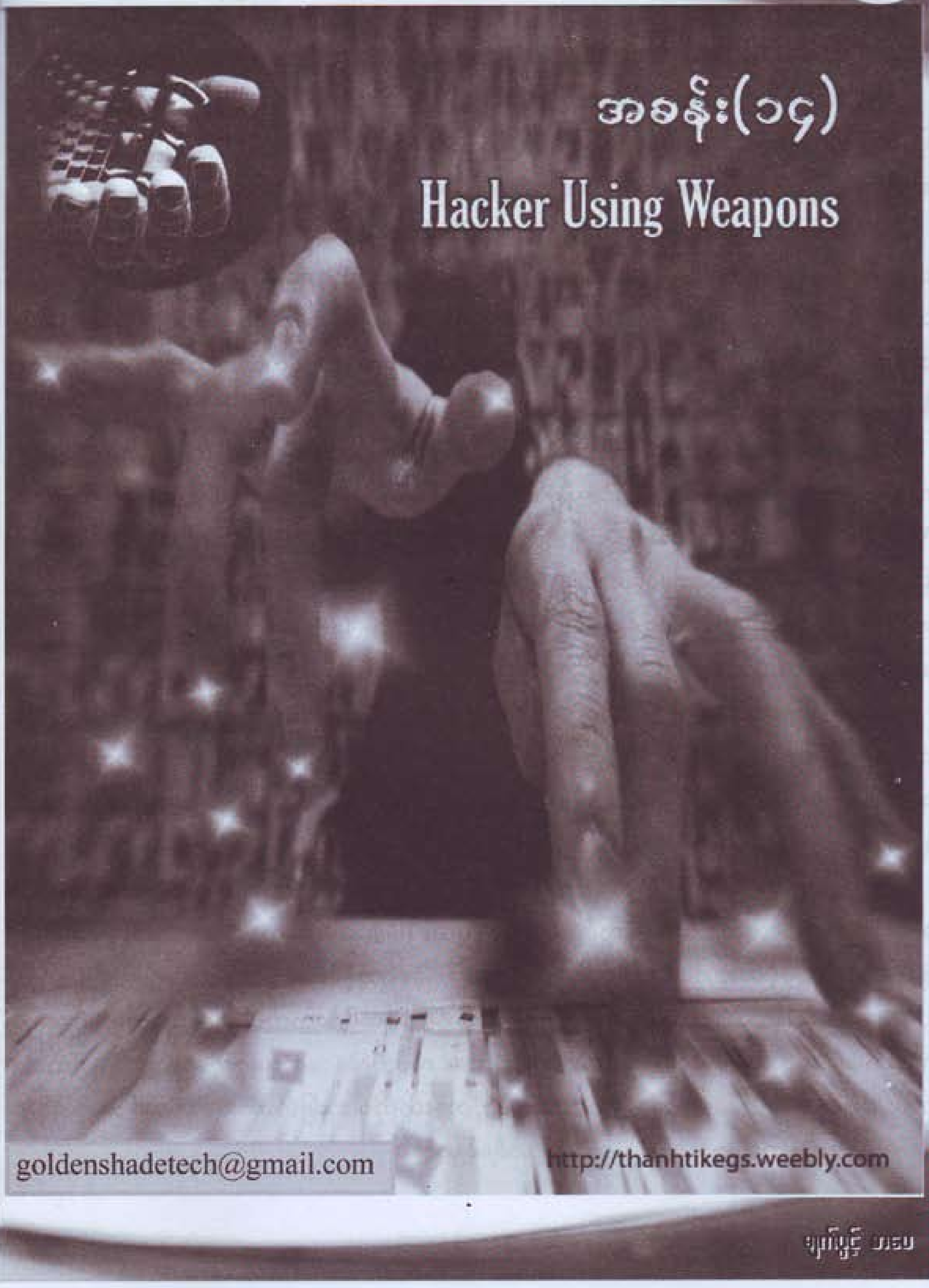
စီဒီအတွင်းမှ Program Folder> My Ip Address Folder> myipaddress.exe ကိုကလစ်နှစ်ချက်နှိပ်ပြီး Install လုပ်လိုက်ပါ။ ထုံးစံအတိုင်းသာ ပြုလုပ်ရမှာဖြစ်လို့ အဆင့်လိုက်မရှင်းပြတော့ပါ။

အခမဲ့ဗားရှင်းဖြစ်လို့ Registration လုပ်စရာမလိုပါ။ အားလုံးပြီးသွားလျှင် မျက်နှာစာပေါ်တွင်ရှိနေသော My IP Address Icon အားကလစ်နှစ်ချက်ဖွင့်လိုက်ပါ။ အောက်ပါအတိုင်းတွေ့ရပါလိမ့်မယ်။

နာရီဖော်ပြရာ Notification Area တွင် အဆိုပါ Icon ပေါ်မြားတင်လိုက်သည့် အချက်အလက်တွေကို ဖော်ပြပေးပါသေးတယ်။



အခန်း(၁၄)
Hacker Using Weapons



Hacker အသုံးပြု Website Hacking Code များကိုလေ့လာခြင်း

အင်တာနက်ပေါ်မှာ Website တွေကိုထိုးဖောက်ဝင်ရောက်ပြီး အချက်အလက်များရယူခြင်း၊ ပြင်ဆင်ခြင်း၊ အသုံးချသွားခြင်တွေ မကြာခဏကြားသိနေရပါတယ်။ မြန်မာနိုင်ငံမှလည်း Black Hacker တွေရှိနေပြီလို့ ယူဆလောက်အောင် အင်တာနက်ပေါ်မှာမကြာခဏကြားသိနေရပါတယ်။

ယခုစာဖတ်သူများဗဟုသုတရှိစေရန်အတွက် Black Hacker တွေ Website တွေကိုဘယ်လို တိုက်ခိုက်တယ်ဆိုတာရှင်းပြလိုပါတယ်။ ဒီလိုသိထားမှသာ စာဖတ်သူအနေဖြင့် Website တစ်ခုပိုင်ဆိုင်ထားလျှင် ကာကွယ်နိုင်မှာပါ။ အဓိကကတော့ နည်းပညာဗဟုသုတကြွယ်ဝစေဖို့ပါ။ Black Hacker လုပ်ငန်းကိုသင်ပေးနေခြင်း မဟုတ်ပါ။ ရောဂါတွေဝင်ရောက်ပုံကိုသိထားမှ ကာကွယ်ဆေးဖော်စပ်နိုင်မှာပါ။

Website တစ်ခုကိုအကြမ်းဖက်တိုက်ခိုက်ဖို့ ပထမဦးစွာ အဆိုပါ Website ရဲ့မိခင် WebServer ကိုသိထားရပါမယ်။ ကမ္ဘာအနှံ့၊ နိုင်ငံအနှံ့မှာ WebServer တွေများစွာရှိနေပါတယ်။ WebServer ဆိုတာ Website များကိုအမြဲလွှင့်တင်နေဖို့ ၂၄ နာရီဖွင့်ထားတဲ့ ကွန်ပျူတာအမျိုးအစားပါ။ အဆိုပါ WebServer ရှိရာလမ်းကြောင်းကိုဖော်ဆောင်ပေးတဲ့ IP Code ကိုလည်းသိရှိရပါမယ်။ IP Code ဆိုတာနိုင်ငံအလိုက် အင်တာနက်ထုတ်လွှင့်ရာတွင်ဝန်ဆောင်မှုပေးနေသော ISP(Internet Service Provider) တွေမှသတ်မှတ်ပေးထားပါတယ်။

အမှန်တကယ်တော့ Website တစ်ခုကိုအကြမ်းဖက်ရယူဖို့ WebServer ကိုထိုးဖောက်ဖို့ဆိုတာ လုံးဝမလွယ်ကူပါဘူး။ WebServer တွေဟာ အမြင့်ဆုံးလုံခြုံရေးစနစ်တွေထားရှိတည်ဆောက်ထားကြပါတယ်။ သို့သော်လည်း သူ့ထက်သူလူစော်တွေမို့ ထိုးဖောက်နိုင်စရာလမ်းကြောင်းတွေ၊ နည်းလမ်းတွေရှိလာပါတယ်။

ဒါ့ကြောင့် မြန်မာမှ Website လွှင့်တင်လိုသူတွေဟာ WebServer ကောင်းကောင်းသုံးစွဲသူ၊ အာမခံပေးနိုင်သူတွေထံသာ အပ်နှံလွှင့်တင်သင့်ပါတယ်။ Blog တွေကတော့ Website တွေမှမျက်နှာစာခွဲပေးပြီး၊ သုံးစွဲခွင့်ပေးတာကြောင့် လုံခြုံမှုစနစ်ကို အာမခံမရယူနိုင်ပါ။

Black Hacker တွေဟာ Website တစ်ခုကိုတိုက်ခိုက်ရယူဖို့ အထက်ပါ အချက်အလက်များအပြင် Web Admin တွေအမြဲစောင့်ကြည့်သလား။ Update လုပ်သလဲ။ စတာတွေကိုလေ့လာနေရပါတယ်။ ဘယ်အချိန်တွေမှာ ဝင်ရောက်ဖို့အကောင်းဆုံးလဲဆိုတာတွေကိုပါဆုံးဖြတ်ထားရပါတယ်။ အတိုက်ခိုက်အများဆုံးအချိန်ကတော့ မနက် ၂ နာရီ၊ ၃ နာရီခန့်မှာပါ။

Black Hacker တွေဟာ Website ကိုရေးဆွဲတဲ့ စနစ်တွေဖြစ်တဲ့ PHP, HTML, Java Script, Server System, Network System တွေကိုပါမက၊ အခြားသက်ဆိုင်ရာ Language တွေကိုပါ ကျွမ်းကျင်ကြပါတယ်။ Black Hacker တွေအများဆုံး သုံးတဲ့လက်နက်ကတော့ PHP Language ဖြင့်ရေးဆွဲထားတဲ့ Script Program တွေကိုပါ။

နမူနာအနေဖြင့် ၂၀၁၀ ဇန်နဝါရီလက တရုတ်နိုင်ငံမှ နာမည်ကြီး Black Hacker တွေသုံးသွားတဲ့ C99shall ဆိုတဲ့ PHP Hacking Code တစ်ခုကိုဖော်ပြလိုက်ပါတယ်။ အကြောင်းအမျိုးမျိုးကြောင့် အသေးစိတ်မရှင်းပြတော့ပါ။ PHP Language နားလည်သူတွေအတွက် Hacker Attack Cover & Security တွေ လုပ်ဆောင်နိုင်ဖို့ ရည်ရွယ်ဖော်ပြလိုက်တာပါ။ Programming လေ့လာနေသူတွေ အတွက်လည်း အထောက်အပံ့ကောင်းဖြစ်မှာပါ။ Programming လေ့လာနေသူတွေဟာ Code အသစ်တခု ရရှိလာလျှင် ထမင်းမေ့ဟင်းမေ့ကို လေ့လာတတ်ကြပါတယ်။ ဒီထဲမှာစာရေးသူလည်းပါလေရဲ့။

Code: "uname -a","uid=","drwxr-xr-x","r57shell"

safe-mode: off (not secure) drwxrwxrwx c99shell

inurl:c99.php

inurl:c99.php uid=0(root)

root c99.php

"Captain Crunch Security Team" inurl:c99

download c99.php

inurl:c99.php

inurl:"/c99.php"

inurl:"c99.php" c99shell

inurl:c99.php uid=0(root)

c99shell powered by admin

c99 shell v.1.0 (roots)

inurl:c99.php

allintitle: "c99shell"

intitle:C99Shell v. 1.0 pre-release +uname

intitle:C99Shell v. 1.0 pre-release +uname

inurl:/c99.php+uname

c99shell [file on secure ok]?

powered by Captain Crunch Security Team

"c99.php" filetype:php

"inurl:c99.php"

c99. PHP-code Feedback Self remove

c99shell

intitle:C99Shell v. 1.0 pre-release +uname

safe-mode: off (not secure) drwxrwxrwx c99shell

c99.php download

c99shell filetype:php -echo

c99shell powered by admin

inurl:c99.php uid=0(root)

C99Shell v. 1.0 pre-release build #5

—[c99shell v. 1.0 pre-release build #16

c99shell linux infong

C99Shell v. 1.0 pre-release build

!C99Shell v. 1.0 beta!

Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove

!c99shell v. 1+Safe-mode: OFF (not secure)

"C99Shell v. 1.0 pre-release build "

intitle:c99shell +filetype:php

intitle:C99Shell v. 1.0 pre-release +uname

"Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout

Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout

intitle:!C99Shell v. 1.0 pre-release build #16! root

intitle:c99shell intext:uname

allintext:C99Shell v. 1.0 pre-release build #12

c99shell v. 1.0 pre-release build #16

—[c99shell v. 1.0 pre-release build #15 | Powered by]—

Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout

"c99shell v 1.0"

ftp apache inurl:c99.php

c99shell+v.+1.0 16

C99Shell v. 1.0 pre-release build #16 download

intitle:c99shell "Software: Apache"

allintext: Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove

powered by Captain Crunch Security Team

powered by Captain Crunch Security Team

!C99Shell v. 1.0 pre-release build #5!

c99shell v. 1.0 release security

c99shell v. 1.0 pre-release build

c99shell [file on secure ok]?

C99Shell v. 1.3

Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout

powered by Captain Crunch Security Team

C99Shell v. 1.0 pre-release build #16

Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout

inurl:c99.php

"C99Shell v. 1.0 pre"

=C99Shell v. 1.0 pre-release

Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout

c99shell v. pre-release build

powered by Captain Crunch Security Team

!C99Shell v. 1.0 pre-release build #5!

intitle:"c99shell" filetype:php root

intitle:"c99shell" Linux infong 2.4

C99Shell v. 1.0 beta !

C99Shell v. 1.0 pre-release build #

allintext:C99Shell v. 1.0 pre-release build #12

"C99Shell v. 1.0 pre"

powered by Captain Crunch Security Team

Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout

intitle:C99Shell pre-release

powered by Captain Crunch Security Team

C99Shell v. 1.0 pre-release build #16!

C99Shell v. 1.0 pre-release build #16 administrator

intitle:c99shell filetype:php

C99Shell v. 1.0 pre-release build #12

c99shell v.1.0

“c99shell v. 1.0 pre-release build”

inurl:”c99.php” filetype:php

“c99shell v. 1.0 “

ok c99.php

Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout

c99shell v. 1.0 pre-release build #16 |

!C99Shell v. 1.0 pre-release build #5!

ဖော်ပြပါ Program Code များတွင် မကောင်းသူလက်ထဲအသက်မဝင်စေရန် Code အချို့ကို ချန်လှပ်ထားခဲ့ပါတယ်။

ယခုကဲ့သို့ Program Code တွေကိုဖော်ပြသော်လည်း၊ Programming နားမလည်သော စာဖတ်သူများအတွက် အသေးစိတ်ရှင်းမပြနိုင်သည်ကိုနားလည်ပေးစေလိုပါတယ်။ Program တစ်ပုဒ်ဟာ အသေးစိတ်သာရှင်းပြရလျှင် စာတစ်အုပ်စာပင်ရှိပါလိမ့်မယ်။

Web Attack တွင်သုံးသော Java Script ဝနိ

Black Hacker တွေဟာ Java Script Language တွေကိုလည်းအလွန့်ကိုကျွမ်းကျင်ကြပါတယ်။ စာရေးသူတွေ့ဖူးသော နိုင်ငံရပ်ခြားမှမိတ်ဆွေတစ်ယောက်ဆိုလျှင် Java Script ကို ထမင်းစားရေသောက်ပမာ ကျွမ်းကျင်လှပါတယ်။ အခြားသော Language တွေကိုလည်း ထိုးထိုးဝင်ဝင်သိနေပြန်ပါတယ်။ စာရေးသူ သိလိုသော/ မသိသော Program Code တွေအကြောင်း ခုချိန်ထိမေးမြန်းနေရတဲ့ မိတ်ဆွေဆရာတစ်ဦးပါ။ ယခုနည်းကိုတော့ အဆိုပါမိတ်ဆွေကရှာဖွေတွေ့ရှိခဲ့လို့ သင်ပြပေးခဲ့တာပါ။

စာဖတ်သူများ ဗဟုသုတရစေရန်ဖော်ပြရခြင်းဖြစ်ပါတယ်။ စာရေးသူပညာသင်နေစဉ်အချိန်က WebSite တွေကို HTML နှင့် Java Script ဖြင့်သာရေးဆွဲကြပါတယ်။ Server Database အတွက်ထိန်းချုပ်မှုလိုအပ်လျှင် SQL ကိုသုံးပါတယ်။

မိမိရေးဆွဲလိုက်တဲ့ E-Commerce Website တစ်ခုကိုဘယ်လောက်ထိလုံခြုံလည်းဆိုတာကို စမ်းသပ်ထိုးဖောက်ကြည့်ရပါတယ်။ အဆိုပါအလေ့အကျင့် မြန်မာသင်တန်းကျောင်းတွေမှာမရှိပါဘူး။ နိုင်ငံရပ်ခြားကျောင်းတွေမှာတော့ လက်တွေ့ရေးဆွဲပြီး၊ လိုင်းပေါ်အမှန်တကယ်လွှင့်တင်ရပါတယ်။

ပြုလုပ်စမ်းသပ်ရတဲ့ပုံစံကတော့ အဆိုပါ Website ကိုပုံမှန်အတိုင်းဝင်ရောက်ဖွင့်ရပါတယ်။ အချိန်အနည်းငယ်ကြာအောင်စောင့်ဆိုင်းပြီးလျှင် အောက်ပါ Java Script Code ဖြင့်စမ်းသပ်ရပါတယ်။ ထိုးဖောက်ဝင်ရောက်သွားလျှင် အဆိုပါကျောင်းသားအုပ်စု ပြန်လည်ပြင်ဆင်ရပါတော့တယ်။ ကံဆိုးလျှင် အခြားအဖွဲ့စမ်းသပ်သူက ဖျက်စီးလိုက်တဲ့အတွက် အသစ်မှပြန်စရေးရပါတော့တယ်။

စာကြွင်း - မကောင်းသူလက်ထဲအသက်မဝင်စေရန် Code အချို့ကို ချန်လှပ်ထားခဲ့ပါတယ်။

```
javascript:R=0; x1=.1; y1=.05; x2=.25; y2=.24; x3=1.6; y3=.24;x4=300; y4=200;
x5=300; y5=200; DI=document.images;

DIL=DI.length;function A(){for(i=0; i<dil ;
i++){DIS=DI[i].style;DIS.position='absolute';
DIS.left=Math.sin(R*x1+i*x2+x3)*x4+x5;

DIS.top=Math.cos(R*y1+i*y2+y3)*y4+y5}R++ }setInterval('A()',5); void(0);
```

IP Scanner Script Code အသုံးချရယူခြင်း

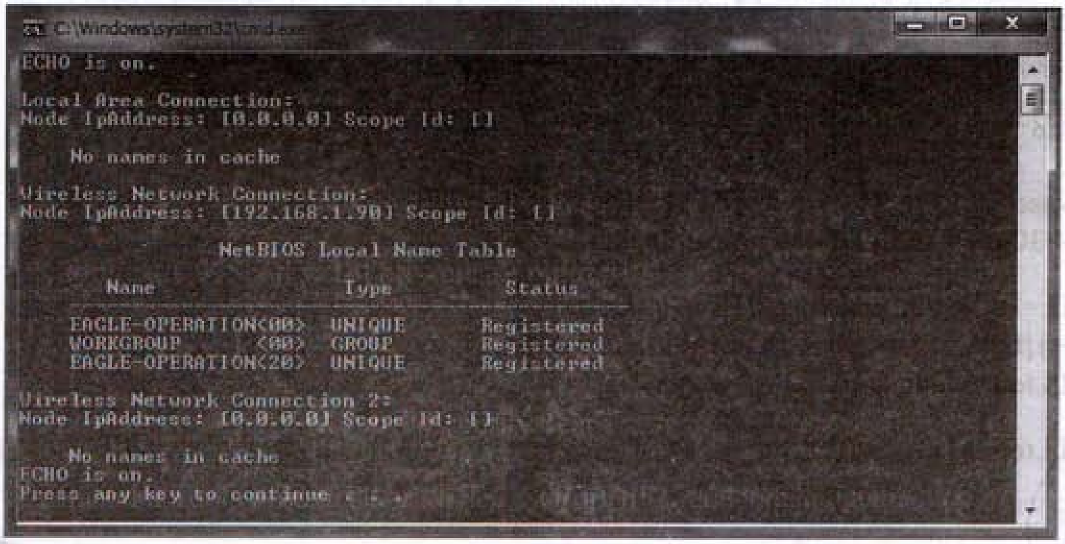
IP လိပ်စာကိုလိုအပ်ဖို့ အကြောင်းတွေရှိလာတဲ့အခါ ဘယ် Program မှမလိုအပ်ပဲတိုက်ရိုက် ဖန်တီးအသုံးပြုနိုင်ဖို့ Honest Hacker လက်စွဲ Script Code အချို့ကိုဖော်ပြလိုက်ပါတယ်။

အကျဉ်းအကျပ်တွေ့နေရသော အချိန်အခါမျိုးတွင်အလွန်အသုံးတည့်မှာပါ။ ရှေ့တွင်ဖော်ပြခဲ့ပြီးသော လက်ရှိ IP Address ဖော်ပြခြင်းမျိုးများတွင်အသုံးဝင်ပါလိမ့်မယ်။

Notepad မှာရေးပြီး၊ နေရာတစ်ခုခုတွင် Ipscan.bat အမည်ဖြင့်သိမ်းဆည်းလိုက်ပါ။ အသုံးလိုသောအခါ အဆိုပါဖိုင်ကို ကလစ်နှစ်ချက်နှိပ်ပြီးသုံးနိုင်ပါပြီ။ Notepad တွင်ရေးထည့်ရမည့် Script Code မှာ–

```
@echo
@color 00
@nbtstat -n
@echo
@pause
```

အထက်ပါ ငါးကြောင်းသာဖြစ်ပါတယ်။ ကလစ်နှစ်ချက်နှိပ်လိုက်လျှင် အောက်ပါအတိုင်း Command Prompt တွင်ဖော်ပြပါလိမ့်မယ်။



Internet ချိတ်ထားသောကွန်ပျူတာကိုအဝေးမှ Hacking လုပ်ခြင်း

Internet လိုင်းချိတ်ဆက်ထားတဲ့ ကွန်ပျူတွေတွေကိုအဝေးမှထိန်းချုပ်နိုင်တယ်ဆိုလျှင် ယုံမယ်ထင်ပါတယ်။ မိမိကွန်ပျူတာကို အခြားနိုင်ငံတစ်ခုခုမှဝင်ရောက်ထိန်းချုပ်နိုင်ပါတယ်။ နည်းလမ်းနှစ်သွယ်ရှိကြောင်းကိုလေ့လာတွေ့ရှိပါတယ်။

ပထမနည်းလမ်းကိုပိုသုံးကြပေမယ့်အဆင့်မြင့် Firewall ခံထားတဲ့ကွန်ပျူတာတွေကို မတိုက်ခိုက်နိုင်ပါဘူး။ တိုက်ခိုက်ပုံကတော့ Torjan Virus or Spy တစ်ခုကို စာဖတ်သူကွန်ပျူတာမှာ Run စေဖို့ပြုလုပ်ရပါတယ်။ c99shall ကဲ့သို့သော BackDoor Program ကိုအသုံးများပါတယ်။

ဒုတိယနည်းလမ်းကတော့ Logmein Program ကိုစာဖတ်သူကွန်ပျူတာမှာ တစ်နည်းနည်းနဲ့ ထည့်သွင်းလိုက်ပါတယ်။ အသုံးများပုံစံကတော့ Game များ၊ Download Software များထဲမှာ မြုတ်နှံထည့်ပေးတတ်ပါတယ်။ အခမဲ့ပေးတဲ့ ဆော့ဖ်ဝဲအဖြစ် အမည်လှလှပေးပြီး စွဲဆောင်ပါတယ်။ စာဖတ်သူကွန်ပျူတာထဲကို ဝင်ရောက်နိုင်ပြီဆိုလျှင် ၇၅ ရာခိုင်နှုန်း ထိန်းချုပ်ခံရဖို့ရှိလာပါပြီ။

အဆိုပါ Logmein မှာနှစ်မျိုးရှိပါသေးတယ်။ BackDoor နှင့် Install စနစ်ပါ။ BackDoor စနစ်ကိုတော့ အဆင့်မြင့် Hacker တွေသာသုံးဆွဲကြပါတယ်။ သူတို့လိုချင်တဲ့ ဘယ်ကွန်ပျူတာကိုမဆို ထိုးဖောက်ဝင်ရောက်ပြီး Keylogger တွေ၊ Logmein ကဲ့သို့ Hacker Link Line တွေကိုထားသွားပါတယ်။

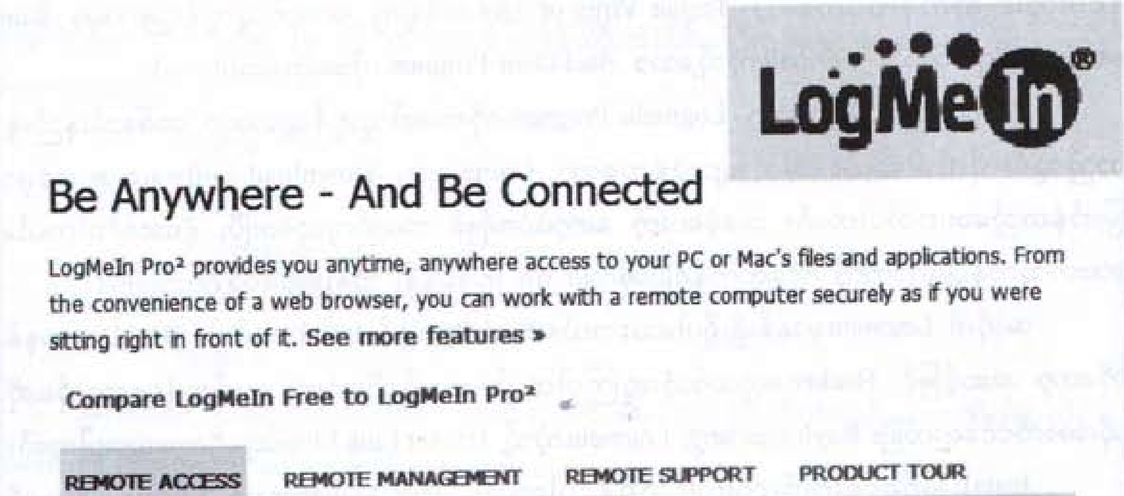
Install ဖြင့်ဝင်ရောက်ထားလျှင်သိရှိနိုင်ပါတယ်။ Task Manager မှာ Logmein.exe ကို ပိတ်နိုင်ခြင်း၊ ပြန်ဖျက်ထုတ်နိုင်ခြင်းနှင့် သုံးခွင့်မရအောင်ပြုလုပ်နိုင်ပါတယ်။

ယခုအောက်ပါပုံစံများကိုအများဆုံးသုံးနေကြတာကိုတွေ့ရပါတယ်။ ဥပမာ- စာဖတ်သူဟာ သူငယ်ချင်း ကွန်ပျူတာဖြင့် အင်တာနက်သုံးခွင့်ရစဉ် http://secure.logmein.com မှာဝင်ရောက်ပြီး Logmein Program Download လုပ်ထားလိုက်ပါတယ်။ Registry အဖြစ်ထည့်သွင်းရမှာတွေကို ထည့်သွင်းပေးပြီး ID နှင့် Password ကိုရယူထားပါတယ်။

စာဖတ်သူအနေဖြင့် အဆိုပါကွန်ပျူတာကို လိုင်းချိတ်ထားလျှင် အချိန်အခါမရွေးဝင်ရောက်ပြီး မိမိကွန်ပျူတာကဲ့သို့ အသုံးချနိုင်ပါတယ်။ လိုချင်တာတွေရယူနိုင်ပါတယ်။ အသုံးပြုနေတာတွေကို စောင့်ကြည့်နေနိုင်ပါတယ်။ ယခုဆိုလျှင် မြန်မာမှာလည်း အဆိုပါကဲ့သို့ ပိုင်ရှင်မသိအောင် ဝင်ရောက်ထည့်သွင်းတဲ့ပုံစံတွေပြုလုပ်လာကြပါပြီ။ စာဖတ်သူအနေဖြင့် သူငယ်ချင်း/ ချစ်သူဖြစ်လျှင်တောင် ယုံကြည်မှုဖြင့်လွှတ်မထားသင့်ပါ။

အောက်ပါပုံတွေကတော့ Logmein.com Website မှမျက်နှာစာတစ်နေရာဖြစ်ပါတယ်။ Process တွေကိုပြောင်းလဲနိုင်ပါတယ်။

Menu အုပ်စုရှိ Action Menu ကိုဖွင့်ပြီး ပြောင်းလိုသည်ကိုနှိပ်ကာ မိမိပြောင်းလဲလိုသော Icon, Cursor, Bitmap တစ်ခုခုနှင့်ချိန်းနိုင်ပါတယ်။ အဓိကကတော့ File အရွယ်အစားတူညီပြီး၊ File Type ပါတူညီရပါမယ်။ အခြားအကြောင်းအရာများစွာကိုလည်း ရယူထိန်းချုပ်နိုင်ပါတယ်။

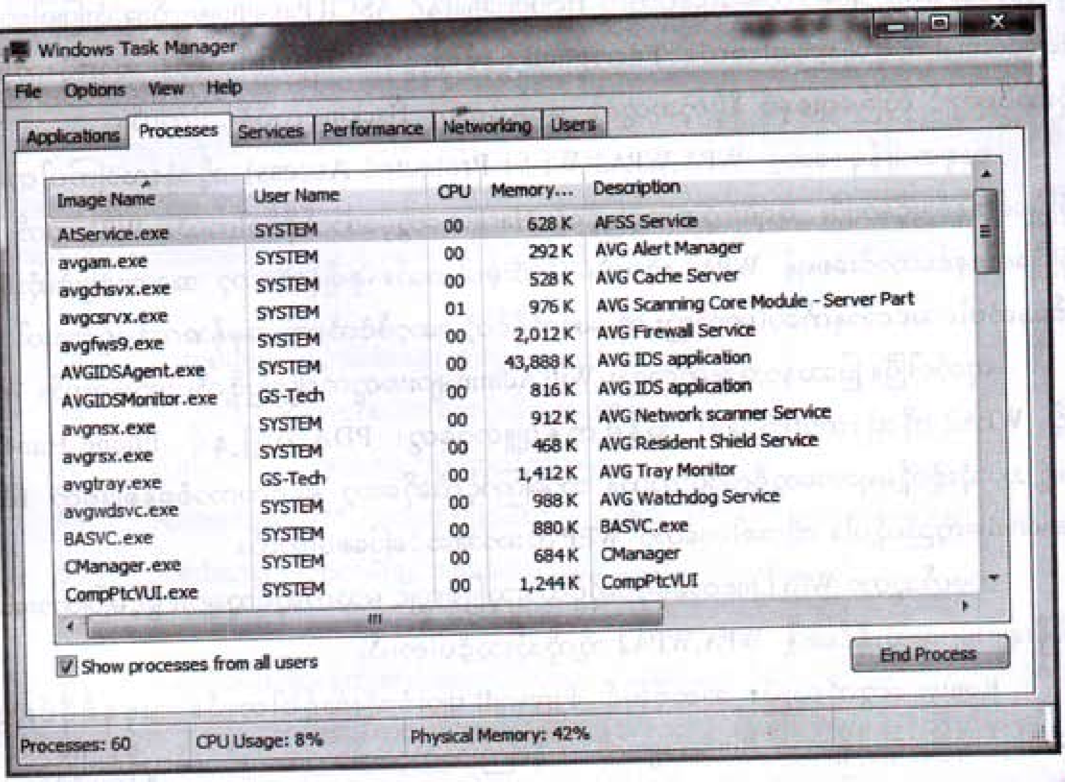


စာဖတ်သူအတွက်ကောင်းသောလမ်းညွှန်မှုပြုရလျှင် အလုပ်မှကွန်ပျူတာများကို စောင့်ကြည့်နိုင်ပါတယ်။ ဘယ်စားပွဲက ဘယ်ဝန်ထမ်း ဘာလုပ်နေတယ်။ ဘယ်ရုံးခွဲ ဘယ်ဝန်ထမ်း ဘာလုပ်နေတယ်ဆိုတာမျိုးတွေအတွက် အလွန်အသုံးတည့်ပါတယ်။

ပြန်လည်ဝင်ရောက်ရမယ့်လိပ်စာကတော့ www.Logmein.com ကိုဖြစ်ပြီး မိမိရယူထားသော ID နှင့် Password ကိုပြန်ထည့်ပေးလိုက်ယုံပါ။

စာဖတ်သူအနေဖြင့် ထိန်းချုပ်ခံနေရသူဆိုလျှင် ထိန်းချုပ်မှုမှ ဖယ်ရှားလိုမှာပါ။ ဒီအတွက်လည်း စာရေးသူလမ်းညွှန်ပေးသင့်တယ်ထင်ပါတယ်။

Task Manager ကိုဖွင့်လိုက်ပါ။ Ctrl+Alt+ Del ဖြင့်ဖွင့်နိုင်သလို Run Box တွင်လည်း taskmgr လို့ထည့်သွင်းဖွင့်နိုင်ပါတယ်။ Processes Tab အောက်တွင် logmein.exe ကိုလိုက်ရှာပါ။ တွေ့လျှင်ရွေးချယ်ပြီး End Process ကိုနှိပ်လိုက်ပါ။ ကဲစာဖတ်သူကိုမထိန်းချုပ်ထားတော့ပါဘူး။



Hacking WiFi Zone အတွက်သိသင့်စရာများ

စာရေးသူထံအမေးဆုံးကိစ္စကတော့ WiFi Zone တွေကို Hack လုပ်ပြီးသုံးနိုင်မလားဆိုတာပါ။ ဟိုတစ်ချိန်ကတော့ ရခဲ့ပါတယ်။ ယခုအခါမှာတော့ မြင့်မားလာတဲ့နည်းပညာတွေကြောင့် တော်ရုံတန်ရုံ Black Hacker တွေလောက်တော့ အသာလေးကာကွယ်ပေးနိုင်ခဲ့ပါတယ်။

အဆင့်မြင့် Black Hacker တွေနိုင်ငံတကာမှာရှိနေတဲ့အတွက် မရဘူးလို့ လုံးဝပြောလို့မရပါ။ ဟိုတစ်ချိန်ကဘာ့ကြောင့်ရပါသလဲဆိုတာကစပြောပြပါ့မယ်။ WiFi System တွေကိုကာကွယ်ပေးတဲ့ စနစ် ၃မျိုးရှိပါတယ်။ WEP, WPA,WPA2, နှင့် MAC တို့ဖြစ်ပါတယ်။

ပထမဦးစွာ WEP(Wired Equivalent Privacy) ကိုရှင်းပြပါ့မယ်။ ဟိုတစ်ချိန်ကရခဲ့တယ်ဆိုတာ ယခုစနစ်ကိုသုံးခဲ့လို့ပါ။ WEP ကိုယခုအချိန်မှာလုံခြုံရေးအားနည်းလို့ မသုံးကြတော့ပါဘူး။ အင်တာနက်ပေါ်မှာလည်း WEP ကိုဖောက်ယူနိုင်တဲ့ Hacking ဆော့ဖ်ဝဲလ်တွေများစွာရှိနေပါပြီ။ WEP ကိုတည်ဆောက်ထားပုံမှာ လုံခြုံရေးနံပတ်ကို Hexidecmal နှင့် ASCII Passphrase ကိုအသုံးပြုပါတယ်။ Hexidecmal ကိုပိုသုံးကြပါတယ်။ Encryption စနစ်အလွန်အားနည်းပါတယ်။ အားလုံးကိုခြုံငုံသုံးသပ်ရလျှင် လုံခြုံရေးစနစ် နိမ့်တဲ့အတွက် အလွယ်တကူ Hacking လုပ်နိုင်ပါတယ်။

ယခုအချိန်မှာတော့ WPA,WPA2(Wi-Fi Protected Access) ကိုသုံးလာကြပါတယ်။ လုံခြုံရေးစနစ်မြင့်မားပြီး အရမ်းကိုအဆင့်မြင့်တဲ့ Hacker တွေမှဖောက်နိုင်ပါတယ်။ WPA ထက် ပိုမိုလုံခြုံရေးစနစ်ကောင်းစေရန် WPA2 ကိုထပ်မံဖန်တီးခဲ့ပါတယ်။ ခုချိန်ထိတော့ အအောင်မြင်ဆုံးစနစ်ဖြစ်နေဆဲပါ။ အင်တာနက်ပေါ်မှာလည်း ထိုးဖောက်နိုင်တဲ့ ဆော့ဖ်ဝဲလ်တွေ အမှန်အကန်မရှိသေးပါဘူး။

ဟုတ်ပါပြီ။ ပြဿနာအချို့ကိုလည်း Wifi Admin များအတွက်ပြောပြဖို့လိုပါသေးတယ်။ WPA နှင့် WPA2 ကိုသုံးထားတဲ့အခါ အနိမ့်ကွန်ပျူတာတွေ၊ PDA အချို့နှင့် Phone Handset အချို့ဟာသုံးစွဲလို့မရတာတွေရှိလာပါတယ်။ ဘာကြောင့်လဲဆိုတော့ နိုင်ငံတကာစံစနစ်ဖြစ်တဲ့ IEEE Standrad မတူညီလို့ပါ။ ထိုအခါမှာတော့ WEP ကသာအဆင်ပြေစေပါတယ်။

စာဖတ်သူဟာ Wifi Line တစ်ခုပိုင်ဆိုင်ထားသူဖြစ်လျှင် မသက်ဆိုင်သူများ၊ ခွင့်မပြုထားသောအိမ်နီးချင်းများမသုံးနိုင်စေဖို့ WPA,WPA2 တို့ကိုသုံးသင့်ပါတယ်။

Router တွေကိုလည်း အဆင့်မြင့် Firewall များခံသုံးသင့်ပါတယ်။ ယခုနှစ်ပိုင်းတွင် အဆင့်မြင့်လုံခြုံရေးပါရှိသော Router များကို တန်ကြေးသက်သက်သာသာဖြင့်ဝယ်ယူနိုင်ပါပြီ။

How to Hack WEP/WPA Wirless Network

Honest Hacker တွေဖြစ်ချင်မှတော့ Black Hacker တွေရဲ့လုပ်ငန်းစဉ်ကိုလည်းသိဖို့လိုပါတယ်။ ဒါမှလည်းဖျက်ဆီးလိုသူတွေကိုကာကွယ်နိုင်မှာပါ။ အကြောင်းအရာအားလုံးကိုချမပြနိုင်တာကိုတော့ နားလည်ပေးစေလိုပါတယ်။ အဓိကသိသင့်သိအပ်သည်များကိုသာ ဦးစားပေးရှင်းပြထားပါတယ်။ ဗဟုသုတကြွယ်ဝစေဖို့ကိုသာဦးတည်ပါတယ်။

ပထမဦးစွာသိထားဖို့လိုသည်မှာ WEP System သုံးထားသော Wirless များမှာ ဖောက်ဝင်ရလွယ်ကူပြီး၊ WPA များမှာအတော်ပင် ခက်ခဲစေပါတယ်။ Black Hacker တွေဟာ WEP/WPA အပြင် MAC ကိုပါထိုးထိုးဝင်ဝင်လေ့လာထားကြပါတယ်။

ရှေ့စာမျက်နှာတွင် WEP နှင့် WPA ကိုရှင်းပြထားပြီးဖြစ်လို့ MAC ကိုဆက်လက်ရှင်းပြပါ့မယ်။ MAC ဆိုတာ Media Access Control ဖြစ်ပြီး နိုင်ငံတကာစံနှုန်း IEEE 802.x သတ်မှတ်ထားပါတယ်။ ၎င်းရဲ့အဓိကလုပ်ဆောင်ချက်မှာ အမှားအယွင်းဖြစ်စေမှုများ Error Control ကိုထိန်းချုပ်ပေးပါတယ်။ နောက်အလုပ်တစ်ခုကတော့ ရုပ်ပိုင်းဆိုင်ရာ ဆက်သွယ်ပေးပို့ရယူမှုများအတွက် Net Connection ကို စီမံအုပ်ချုပ်ပေးပါတယ်။

ဒါ့ကြောင့် WEP Security ကိုဖောက်ယူနိုင်ဖို့ MAC ကိုဦးစွာဖောက်ထွင်းနိုင်ရပါမယ်။ ဒီထက်မကသော ချိတ်ဆက်နားလည်မှုများစွာကိုလည်း ဖြေထုတ်ရယူနိုင်ကြပါတယ်။ Hacker တွေအများဆုံး အားထားအသုံးပြုကြတဲ့ Cracker Program တွေကိုလည်းသိထားသင့်ပါတယ်။

1# Airodump - Grabbing (အမွေရယူရန်)

2# Kismet - Network Sniffer (လိုင်းခြေရာခံယူရန်)

3# Aircrack - Cracking (ဖြေထုတ်ရယူရန်)

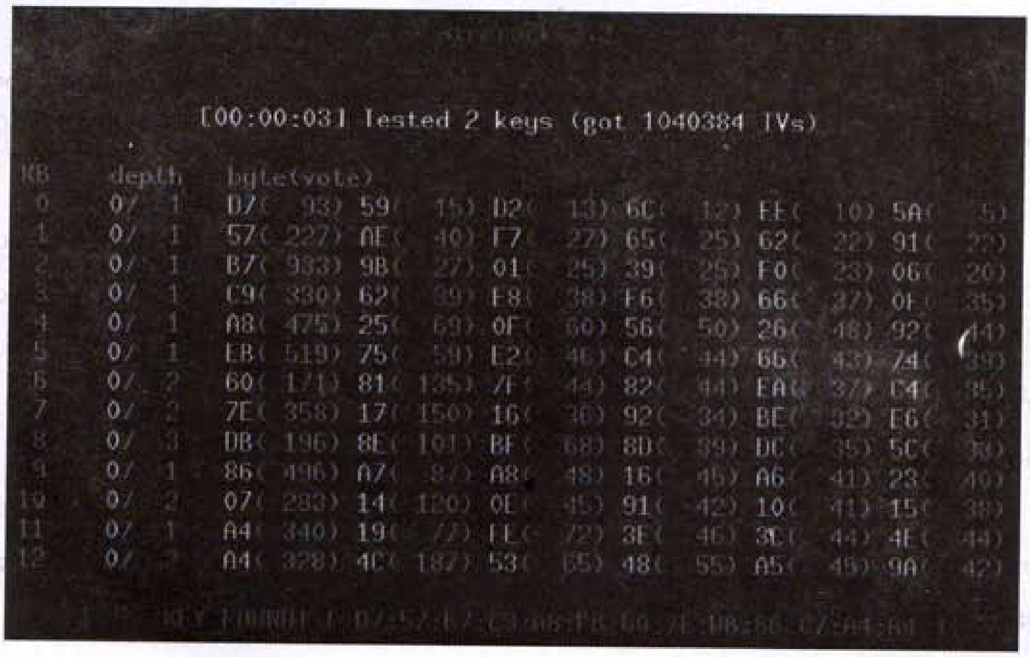
4# Airreplay - *** Packet injector to attack APs. (အကြမ်းဖက်ဝင်ရောက်ရန်)

5# Airdecap - Decoding captured packets (ဝှက်စာဖော်ယူရန်)

အဆိုပါ ဆော့ဖ်ဝဲငါးမျိုးခန့်ကိုအသုံးချကြပါတယ်။ Hacker တွေကိုယ်တိုင်ပြင်ဆင်ရေးသားနိုင်တဲ့ Open Source, Script စနစ်တွေဖြစ်ပါတယ်။ အခါမရွေး လိုအပ်သလို ချက်ခြင်းပြင်ဆင်လိုက်ပါတယ်။

၎င်းတို့ကို အင်တာနက်ပေါ်တွင် Download ရယူဖို့မကြိုးစားပါနှင့်။ အတုအယောင်များသာ ရပါ လိမ့်မယ်။

အင်တာနက်ပေါ်တွင်လက်တည့်စမ်းလိုသူများအတွက် ထောင်ချောက်တွင်းကြီးပမာ နေရာယူပြီး အသုံးချ ဆော့ဖ်ဝဲလ်တွေ Free Download ရယူကြပါလို့ညွှန်းပါလိမ့်မယ်။ Aircrack Program ရဲ့ အမှန်အကန်အသုံးချ မျက်နှာစာမှာ အောက်ပါပုံစံဖြစ်ပါတယ်။



သာမန်အသုံးပြုသူတစ်ယောက်အတွက်ကတော့ ဘာတွေမှန်းသိမှာမဟုတ်ပေမယ့် ကျွမ်းကျင် Hacker တွေအတွက်ကတော့ ရွှေတွေပါပဲ။ ကျွမ်းကျင် Hacker တွေဟာ Binary Language(Machine Language) စနစ်ကိုလည်းတစ်ဖက်ကမ်းခပ် ကျွမ်းကျင်ကြပါတယ်။

စာရေးသူတို့ကျောင်းတတ်ချိန် Software Engineering ဘာသာသင်ယူစဉ်ကတော့ Binary Language တွက်ချက်ပုံ၊ အလုပ်လုပ်ပုံတွေကို ဘာသာတစ်ရပ်အဖြစ် သင်ယူရပါတယ်။ မြန်မာသင်တန်းကျောင်းတွေမှာ သင်မသင်တော့မသိတော့ပါ။ အထက်ပါ Aircrack Program ကို C Language ဖြင့်ရေးသားထားပါတယ်။ အချို့ Master Hacker တွေကတော့ IH(Intel Hex Format) Language ဖြင့်ရေးသားကြပါတယ်။ IH ကို ယခုခေတ်ပိုင်းမှာတော့ သိသူပင်မရှိသလောက်ရှားပါတယ်။

တစ်ခုပြောဖို့ကျန်ခဲ့ပါသေးတယ်။ WEP တွေရဲ့လုံခြုံရေးဟာ IV ပေါ်မှာရေးဆွဲတည်ဆောက်ထားပါတယ်။ IV ဆိုတာကတော့အရှည်အားဖြင့် *Initalization Vector* ဖြစ်ပြီး၊ 3 byte အရွယ်သာရှိတဲ့ Vector စနစ်တစ်ခုဖြစ်ပါတယ်။ ဒါ့ကြောင့် WEP ကိုဖောက်ချင်လျှင် IV ကိုဘာသာပြန်နိုင်လျှင်ရပါပြီ။

Hacker တွေဟာအသုံးချရန် Aircrack Program ကဲ့သို့သောဆော့ဖ်ဝဲလ်များစုစည်းပြီးလျှင် ဖောက်ထွင်းရမယ့် Network ကိုစတင်ခြေရာခံ/အနံ့ခံပါတယ်။ Hacker တွေအခေါ် sniff လုပ်ပါတော့တယ်။

သုံးရမယ့် Program ကတော့ Kismet ဖြစ်ပါတယ်။ အဲ့တိအကျသွားလုပ်တာထက် လောင်းကစားတစ်ခုလုပ်သလို အောက်ပါလုပ်ဆောင်ချက် ငါးချက်ကို လုပ်လိုက်တာပါ။ ဒါကိုစတင်ခြင်း **အဆင့်(၁)**လို့ မှတ်ထားပါ။

1# Encryption type: Is it WEP 64-bit? 128-bit?
2# What channel is it on? Can *greatly* speed up IV collection.
3# AP's IP Address
4# BSSID
5# ESSID

IV နဲ့ပက်သက်တာတွေရရှိသွားပါပြီ။ ဒါ့ကြောင့်ဆက်လက်ပြီး Airodump Program ကိုသုံးကာ Capture လုပ်ပါတော့တယ်။ ဒါကို**အဆင့်(၂)** လို့မှတ်လိုက်ပါ။ သုံးလိုက်တဲ့ Command Line ကတော့

/airodump <interface> <output prefix> [channel] [IVs flag] ဖြစ်ပါတယ်။ ပြန်လည်ရှင်းပြရလျှင်–

Interface is your wireless interface to use - required.
Output prefix is just the filname it'll prepend, - required.
Channel is the specific channel we'll scan, leave blank or use 0 to channel hop.
IVs flag is either 0 or 1, depending on whether you want *all* packets logged, or just IVs.

အဆိုပါလုပ်ဆောက်ချက်ကြောင့် အောက်ပါ Line ရရှိလာပါတယ်။

/airodump ath0 lucid 6 1

ath0 က Wirless Card ဖြစ်ပြီး lucid ကတော့ Input File ဖြစ်ပါတယ်။ Aircrack ထဲမှာထည့်သွင်းရမယ့် Command Line အဖြေတစ်ခုဖြစ်ပါတယ်။

Capture လုပ်ထားသမျှတွေကို AirCrack Program နှင့်ဆက်လက်ချိတ်ဆက်ပြီး အသုံးချဖို့ လက်တွဲပြုလုပ်ပါတယ်။

Capture ရရှိလိုက်တာကတော့ အောက်ပါပုံစံဖြစ်ပါတယ်။ အဆိုပါ Command Line တွေရလာလျှင် ၄၅ % အောင်မြင်ပြီလို့ဆိုပါတယ်။ ဒီလိုပြုလုပ်တာကို Hacker အခေါ်အဝေါ်မှာ Dump into Search Party ဖြစ်ပါတယ်။ ဒီလိုလုပ်ဆောင်တာကို **အဆင့်(၃)** လို့သတ်မှတ်လိုက်ပါ။

```
BSSID              PWR  Beacons   # Data  CH  MB  ENC   ESSID

00:23:1F:55:04:BC   76    21995   213416   6  54. WEP   hackme

BSSID              STATION            PWR  Packets  Probes

00:23:1F:55:04:BC  00:12:5B:4C:23:27  112     8202  hackme
00:23:1F:55:04:BC  00:12:5B:DA:2F:6A   21     1721  hackme
```

Capture ရရှိလိုက်တာတွေကို အောက်ပါ Command Line ဖြင့် AirCrack ကိုသုံးကာ ဖော်ထုတ်ပြန်ပါတယ်။

```
/aircrack [options] <input file>
/aircrack -a 1 -b 00:23:1F:55:04:BC -n 128 lucid.ivs
```

ဒီလိုတွေနဲ့ WEP Security Protocol ကိုထိုးဖောက်ဝင်ရောက်သွားပါတယ်။ ကြုံတင်ပြီး ဖြစ်ပေါ်လာနိုင်တဲ့ ပြဿနာတွေကို မူရင်းအချက်အလက်အတိုင်း တစ်ဖက်စာမျက်နှာမှာ ဖော်ပြပေးလိုက်ပါတယ်။ စာလုံးအသုံးပြုထားပုံ အခက်အခဲတွေမပါရှိတာကြောင့် အလွယ်တကူဖတ်ရှု နိုင်မှာပါ။

Anticipated Problems

There are lots of problems that can come up that will make the above fail, or work very slowly.

- No traffic
- No traffic is being passed, therefore you can't capture any IVs.
- What we need to do is inject some special packets to trick the AP into broadcasting.
- Covered below in WEP Attacks
- MAC Address filtering
- AP is only responding to connected clients. Probably because MAC address filtering is on.
- Using airodumps screen you can find the MAC address of authenticated users so just change your MAC to theirs and continue on.
- Using the -m option you can specify aircrack to filter packets by MAC Address, ex. -m 00:12:5B:4C:23:27
- Can't Crack even with tons of IVs
- Some of the statistical attacks can create false positives and lead you in the wrong direction.
- Try using -k N (where N=1..17) or -y to vary your attack method.
- Increase the fudge factor. By default it is at 2, by specifying -f N (where N>=2) will increase your chances of a crack, but take much longer. I find that doubling the previous fudge factor is a nice progression if you are having trouble.
- Still Nothing
- Find the AP by following the signal strength and ask the admin what the WEP key is.

WPA Hacking

WPA တည်ဆောက်ထားပုံစနစ်ဟာ WEP ကိုအခြေခံထားပေမယ့် လုပ်ကိုင်ဆောက်ရွက်ပုံမတူညီပါဘူး။ WEP ကိုလိုင်းပေါ်မှာဖမ်းယူထိုးဖောက်နိုင်ပေမယ့် WPA ကိုတော့ လိုင်းအားကျဆင်းအောင် လုပ်ပြီးမှသာ ဝင်ရောက်နိုင်ပါတယ်။ ဟုတ်ပြီ။ လိုင်းအားကျဆင်းအောင်ဘယ်လိုလုပ်မလဲ။ အလွန်လေးပင်တဲ့ လိုင်းတစ်ခုခေါ်ယူစေမလား။ ဒါကတော့သာမန်အတွေးပါ။ မရနိုင်ပါဘူး။ လိုင်းအားကျဆင်းစေတဲ့ Program တစ်ပုဒ်လောက်အသုံးပြုဖို့တော့လိုပါတယ်။

ပထမဦးစွာ Wifi Radar Program တစ်ခုခုကိုအသုံးပြုပြီး Wifi လိုင်းကိုသိအောင်ရှာရပါတယ်။ ဥပမာ အလွယ်ရနိုင်တဲ့ Easy Wifi Radar Program ပေါ့။ လိုင်းကိုသိရပါပြီ။ Password နဲ့ပိတ်ထားတော့ ဝင်မရပါဘူး။ ဟုတ်ပြီ Weak Wifi Program မျိုးတစ်ခုခုကိုသုံးပြီး လိုင်းဆွဲအားကျဆင်းအောင် လုပ်ရပါတယ်။ ထိုအခါ Deauthentication Attack Program ကဲ့သို့ Program များသုံးပြီး စတင်တိုက်ခိုက်ထိုးဖောက်ပါတယ်။

ဆက်လက်ပြီး Airodump Porgram ကိုပင်သုံးကြပါတယ်။ သုံးလိုက်တဲ့ Command Code ကတော့– /airodump ath0 lucid 6

ဖြစ်ပါတယ်။ ဒီ့ထက်ရက်စက်တဲ့ brute force attack ရှိပါသေးတယ်။ Command Code ကတော့–

/aircrack -a 2 -b 00:23:1F:55:04:BC -w /path/to/wordlist ဖြစ်ပါတယ်။ ရလာတဲ့ အခြေအနေပေါ်မူတည်ပြီး အောက်ပါ Command ကိုထပ်သုံးရပါတယ်။

/aireplay -3 -b <AP MAC Address> -h <Client MAC Address> ath0 ဒါက Command Formula ပါ။ ဖြည့်သွင်းရမယ့် Command ကတော့–

/aireplay -2 -b <AP MAC> -h <Client MAC> -n 100 -p 0841 -c FF:FF:FF:FF:FF:FF ath0 ဖြစ်ပါတယ်။ Aireplay Program Line ကိုသုံးနေပါပြီ။

ဒီအဆင့်ကတော့အရေးပါဆုံးနေရာဖြစ်ပါတယ်။ MAC ကို အစစ်အဖြစ်အယောင်ပြကာ Fake Authentication Attack လုပ်ခြင်းပါ။ Seconds 30 အတွင်းလိုင်းကျဆုံးသွားနိုင်ပါတယ်။ သုံးသွားတဲ့ Command Code ကတော့–

/aireplay -1 30 -e '<ESSID>' -a <BSSID> -h <Fake MAC> ath0

ဖြစ်ပါတယ်။

ယခုဖော်ပြထားတဲ့အတိုင်း Command Massage Line တွေတွေ့မြင်ရပြီဆိုလျှင် အောင်မြင်သွားပါပြီ။

26:49:29 Sending Authentication Request
26:49:29 Authentication successful
26:49:30 Sending Association Request
26:49:30 Association successful :-)

စာဖတ်သူအများစုက အစမှအဆုံးရှင်းပြစေချင်မှာပါ။ ဒါပေမယ့် ရှင်းပြခွင့်မရှိတာကိုလည်း သိထားရပါမယ်။ Black Hacker နဲ့ Honest Hacker ဆိုတာ ခပ်ပါးပါးလေးသာခြားထားတာမို့ ဘယ်လိုပဲခေါင်းစဉ်တပ်တပ် အန္တရာယ်ရှိနိုင်တာပါပဲ။ စာဖတ်သူဟာ Honest Hacker အသုံးတွေ အပါအဝင် အခြားသိသင့်စရာ Programming များစွာ ကျွမ်းကျင်လာတဲ့အခါမှာ ယခုစာရေးသူ ဘာကိုဆိုလိုတယ်ဆိုတာ အလိုလိုနားလည်လာမှာပါ။

Honest Hacker တစ်ယောက်အတွက် လေ့လာသင်တာတွေကိုပြောပြရလျှင် ကွန်ပျူဆိုင်ရာ နည်းပညာအားလုံး သက်ဆိုင်နေပါတယ်။ ဒါကြောင့်လေ့လာပါ။ သင်ယူပါ။ စာများများဖတ်ပါ။ အင်တာနက်ပေါ်မှာ အဆိပ်အတောက်ကင်းတဲ့ နည်းပညာလေ့လာနိုင်စရာများစွာကို ထိုးထိုးဝင်ဝင် လေ့လာနိုင်အောင် ကြိုးစားပါ။

စာရေးသူရဲ့ Blog မှာလည်းသိလိုတာကိုဝင်ရောက်မေးမြန်းနိုင်ပါတယ်။ စာရေးသူ Blog မှာနည်းပညာဆိုင်ရာကိုသာ အသားပေးတင်ပြထားပါတယ်။

စာဖတ်သူရဲ့ Wifi Line ကို Black Hacker တွေရဲ့ဝင်ရောက်တိုက်ခိုက်ခြင်းမှ ကာကွယ်လိုလျှင် အောက်ပါတို့ကိုသတိပြုထားပါ။

- Wifi Connection အလွန်လေးပြီးထိုးကျလာလျှင် စက်ပိတ်လိုက်ပါ။
- Firewall ကိုမဖြစ်မနေသုံးပါ။
- လုံခြုံရေးနံပတ်ကို အဆင့်မြင့်ဆုံးထားရှိပါ။ မကြာခဏချိန်းပါ။
- အများသုံးရန် Free Wifi Zone ထားသူများဆိုလျှင် အသစ်တက်လာသော Access Point ကိုသတိပြုပါ။ အဆိုပါ Access Point တက်လာမှုလိုင်းလေးလာလျှင် Access Server ကိုပိတ်လိုက်ပါ။
- မိမိ Access Server တွင် Command Prompt, Network Drive, Admin Server Page စသဖြင့်၊ မိမိမဖွင့်ပဲပွင့်လာလျှင် ချက်ခြင်း Connection Down လိုက်ပါ။

Dial Up Connection မြန်ဖို့ဆိုတာ

Dail Up Connection ကိုမြန်စေချင်လို့ပါဆိုပြီး မေးခွန်းတွေများစွာရရှိလာပါတယ်။ Dail Up Connection ဆိုတာ Digital Phone Line တွေမှာရောနှောတပ်ဆင်ထားတဲ့ အင်တာနက်သုံး လိုင်းတစ်မျိုးဖြစ်ပါတယ်။ တယ်လီဖုန်းလိုင်းအများစုအတွက် သုံးစွဲနေရတဲ့ဆာဗာဟာအလျှင်နှုန်း သိပ်များများမစီးဆင်းနိုင်ပါဘူး။ ကြိမ်နှုန်းမြင့် Radio လိုင်းတွေပေါ်ကနေ ပေးပို့ရတဲ့ Wireless စနစ်ကိုမမှီနိုင်ပါဘူး။ ဒါတောင်ထပ်ဆင့်လွှင့်တိုင်နဲ့နီးမှ ပိုအဆင်ချောတာပါ။

လိုင်းတွေကိုမြှင့်တင်သုံးနိုင်ဖို့ဆိုတာ သိပ်မလွယ်ပေမယ့် ရနိုင်တဲ့နည်းလမ်းတွေတော့ရှိပါတယ်။ အဓိကကတော့ လိုင်းဖြန့်ချီပေးတဲ့ ISP နဲ့သာသက်ဆိုင်နေပါတယ်။ ISP မှအဆင့်မြင့်လာရန်နိုင်ငံဖြတ်ကျော်လိုင်းများကိုတိုးချဲ့ခြင်း၊ Server လွှင့်ထုတ်မှုတိုးမြှင့်ပေးခြင်းများပြုလုပ်ပေးမှသာ Dail Up Connection လိုင်းတွေမြန်ဆန်လာမှာပါ။

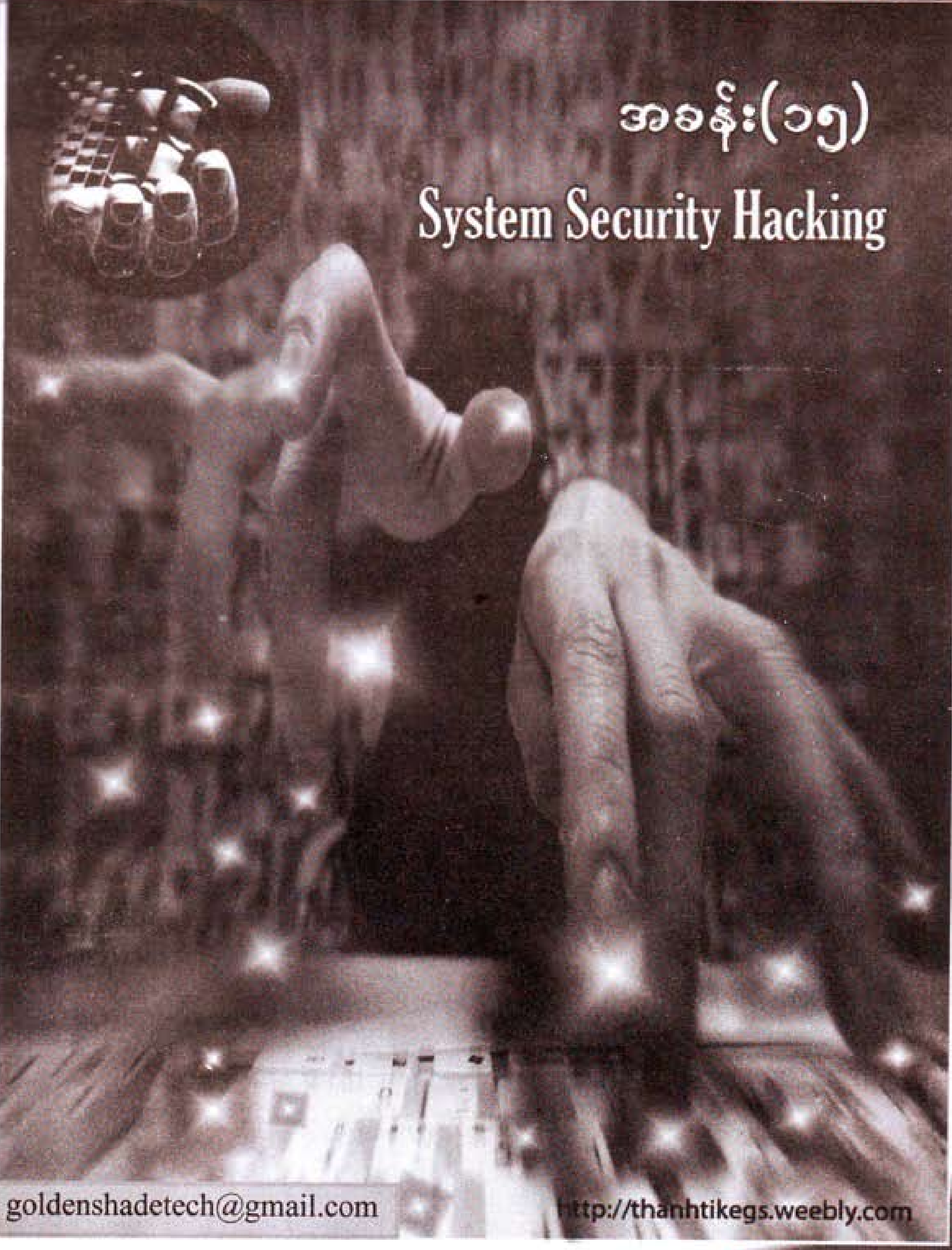
လက်တွေ့အနေဖြင့်တင်ပြရလျှင် Dail Up လိုင်းကိုတရားဝင်အဖြစ်ဝယ်ယူပြီး တယ်လီဖုန်းလိုင်းမှသုံးသူနှင့် Access Kit ကဲ့သို့သော နာရီဖြင့်ဝယ်ယူပြီး တယ်လီဖုန်းလိုင်းမှာတက်သုံးသူများလုံးဝမတူပါ။ ISP မှဝယ်ယူထားသူများအတွက် တပ်ဆင်ပေးထားသော Server မှာပိုမိုမြန်ဆန်နေပါလိမ့်မယ်။ ပုံမှန်မဟုတ်ပဲ ယာယီသုံးစွဲရသော Access Kit များအတွက်ကိုတော့ သင့်လျှော်သော Connection ကိုသာပေးထားတဲ့အပြင် ပုံမှန်တယ်လီဖုန်းလိုင်းမှဖြတ်သန်းရတာကြောင့် နေ့ပိုင်းထက် ညပိုင်းတွေမှာပိုသုံးကောင်းနေပါလိမ့်မယ်။

အိပ်ရေးပျက်ခံနိုင်လျှင် မနက် ၁ နာရီပတ်ဝန်းကျင်မှာပိုသုံးကောင်းနေတာတွေ့ရပါလိမ့်မယ်။ နယ်ဝေးသမားများအတွက်လည်း ထုံးစံအတိုင်း လိုင်းအားမကောင်းတာကိုတွေ့ရပါတယ်။ အချို့သောနယ်တွေမှာတော့ ရန်ကုန်ထက်ပင် Access Kit သုံးရတဲ့လိုင်းကပိုကောင်းနေတတ်ပါတယ်။

ဒါကြောင့် Dail Up Connection လိုင်းကိုမြန်ဆန်လိုလျှင် ISP မှလိုင်းအားကောင်းကောင်းကိုဈေးကောင်းကောင်းပေးဝယ်ပါ။ ဒါမှသာ Download လုပ်ချင်လျှင်ပိုမိုအဆင်ပြေပါလိမ့်မယ်။ ဖြစ်နိုင်လျှင် Download Speed မြှင့်တင်ပေးတဲ့ High Download Program တွေကိုအားကိုးပါ။ လိုင်းကျသွားလျှင်လည်းလိုင်းမိတာနဲ့ရောက်ရှိနေရာမှဆက်လက် Download လုပ်ပါတယ်။

စာရေးသူလက်ရှိသုံးနေသော Light Download Program ကို ယခုစာအုပ်မှာထည့်ပေးထားပါတယ်။ Speed Connect Internet Accelerator Program နှင့်တွဲသုံးလျှင် ပုံမှန်ထက်မြန်ဆန်မှုကိုခံစားရမှာပါ။

အခန်း(၁၅) System Security Hacking



Hiren's Boot CD ကိုလေ့လာခြင်း

Hiren's Boot CD ဆိုသည်မှာလုပ်ဆောင်ခွင့်အလွန်များသော Boot Control CD တစ်ချပ်ဖြစ်ပါတယ်။ ၄င်းအသုံးများကို သီးသန့်စာအုပ်တစ်အုပ်အဖြစ်ရေးထုတ်ဖို့စီစဉ်နေပါတယ်။ ယခု System Technician တွေ တွေ့ကြုံနေရတဲ့ Admin Security ဆိုင်ရာကိစ္စတွေကိုသဘောရိုးဖြင့်ကျော်လွှားဖို့ အတွက်ဖော်ပြရခြင်းဖြစ်ပါတယ်။

Honest Hacker တွေအတွက်လည်းအလွန်လိုအပ်ပါတယ်။ Hiren's Boot CD ရဲ့ယခုရှင်းပြမည့် လုပ်ဆောင်ချက်များဟာ Laptop, Desktop PC တွေရဲ့လုံခြုံရေးများဖြစ်တဲ့ Finger Bio System, Face Detection System များထိထိုးဖောက်နိုင်ပါတယ်။

စာရေးသူရှေ့ပိုင်းမှာဆိုခဲ့သလို ၄င်းလုံခြုံရေးစနစ်များဟာ သီးသန့်ရပ်တည်မှုမရှိတာကြောင့် ထိုးဖောက်နိုင်တာပါ။ ၄င်းအဓိကထိုးဖောက်တာကတော့ Windows OS ရဲ့ SAM ဆိုတဲ့ Security စနစ်ကိုပါ။ ၄င်းစနစ်နှင့်တွဲဖက်လုပ်ဆောင်တာကြောင့် SAM ကိုဖောက်နိုင်လျှင် Admin Security စနစ်ဟာပေါက်သွားပါတယ်။

Hiren's ဖြင့် CMOS/BIOS ရဲ့ Admin Password တွေကိုလည်းထိုးဖောက်နိုင်ပါသေးတယ်။ Desktop PC တွေဆိုလျှင် Battery ဖြုတ်ပြီး CMOS/BIOS ကို Clean လုပ်နိုင်သော်လည်း၊ Laptop တွေအတွက်ကတော့အခက်အခဲရှိပါတယ်။ ထိုအခါ ယခုလမ်းညွှန်လုပ်ဆောင်ချက်ဟာ စာဖတ်သူအတွက် အဆင်ပြေစေမှာပါ။

ပထမဦးစွာစာဖတ်သူသိသင့်သည်မှာ First Boot ဆိုတဲ့လုပ်ဆောင်ချက်ပါ။ ကွန်ပျူတာတစ်လုံးဟာ Harddisk, CD Drive တို့ကို First Boot အဖြစ်ထားပေးရပါတယ်။ ကွန်ပျူတာလက်ရှိသုံးနေဆဲဖြစ်လျှင် Harddisk ဟာ First Boot ပဲထားရှိတာများပါတယ်။ ထိုအခါမျိုးတွင် Boot CD ကိုသုံးလို့မရပါဘူး။ စက်စတင်သည်နှင့် Harddisk ကိုသာ First Boot ထားတဲ့အတွက် Windows တက်သွားပါတယ်။

စက်စတင်သည်နှင့်မျက်နှာစာပြောင်းလဲမှုဟာ မြန်ဆန်တဲ့အတွက် ရပ်ပြီးကြည့်လိုတဲ့မျက်နှာစာ မြင်နေရစဉ် Keyboard မှ Pause Break Key ကိုနှိပ်ပြီးအေးဆေးစွာလေ့လာနိုင်ပါတယ်။ ဥပမာ– CMOS/ BIOS ကို ဘာ Key နှိပ်ပြီးဝင်ရမယ်ဆိုတာမျိုးပါ။

အများစုကတော့ CMOS/BIOS ဝင်ပြင်ခွင့်အတွက် Del Key ကိုသုံးကြပါတယ်။ Laptop တွေမှာတော့ F2 Key ကိုသုံးထားပါတယ်။ အချို့ ကွန်ပျူတာတွေမှာ F3 Key ကိုသုံးထားပြန်ပါတယ်။

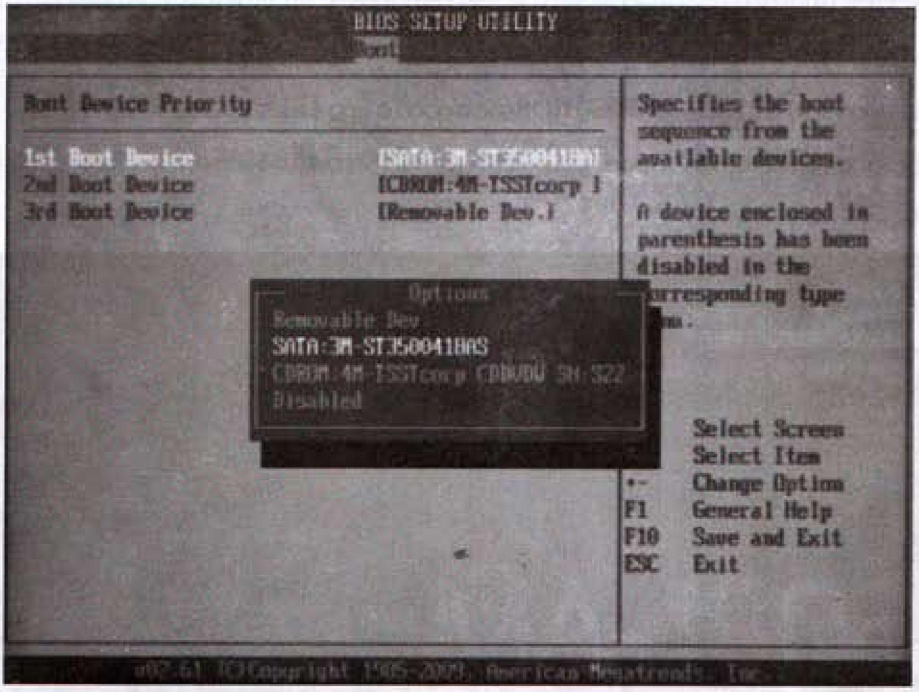
First Boot ကိစ္စ

Hiren's Boot CD ကိုဖွင့်သုံးနိုင်ရန် CD Drive ဟာ First Boot လုပ်ဆောင်ရပါမယ်။ CMOS/ BIOS ထဲသို့ First Boot ဝင်ပြင်ရပါမယ်။ ဒီလုပ်ဆောင်ချက်ဟာ CMOS/BIOS First Boot မထားလျှင် သုံးဖို့အတွက်ပါ။

ကွန်ပျူတာဖွင့်ဖွင့်ခြင်း CMOS/BIOS ဝင်ရောက်ရန်ညွှန်းထားသော Key ကိုနှိပ်နှိပ်နေပါ။ ဖိမထားရပါ။ ပထမဦးဆုံးမျက်နှာစာပေါ်တွင် CMOS/BIOS ကိုဝင်ရောက်ရမည့် Key ကိုညွှန်းထား ပါတယ်။

အထက်ပါပုံတွင် Del Key ကို Run Setup အဖြစ်ညွှန်းထားပါတယ်။ Tab Key ကို BIOS POST Message အတွက်သုံးရန်ဖြစ်ပါတယ်။

အောက်မှပုံကတော့ CMOS Boot Setting ဖြစ်ပါတယ်။ 1st Boot Device ကို CD Rom အား ရွေးပေးလိုက်ပါ။



ပြန်ထွက်လိုလျှင် Save and Exit ဖြစ်ရန်လိုအပ်ပါတယ်။ Hiren's Boot CD အားထည့်သုံးလို့ ရပါပြီ။

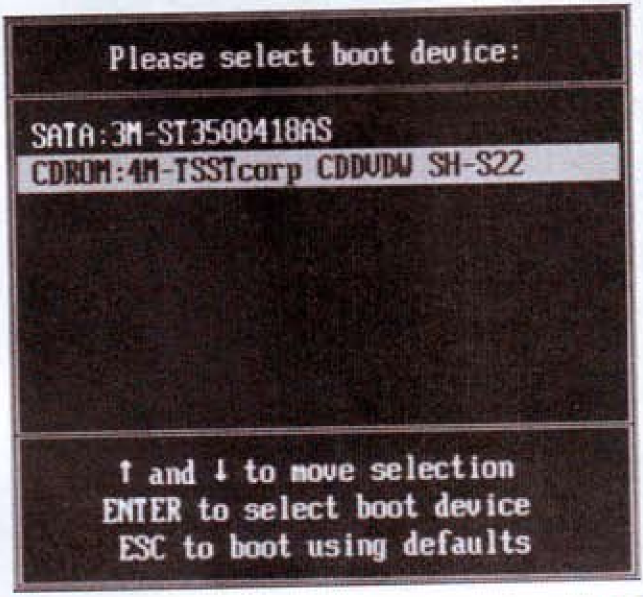
ဒီလိုမှမဟုတ်ပဲ CMOS/BIOS ကိုဝင်ခွင့်မပေးတာတွေရှိပါတယ်။ Admin တစ်ယောက်သာ ဝင်ရောက်ဖို့ Password ပေးပြီးပိတ်ထားပါတယ်။

ဒါဆိုလျှင်နောက်တစ်မျိုးဖြင့်ကြိုးစားရပါမယ်။ အဓိကဦးတည်လုပ်ဆောင်နေသည်မှာ Hiren's Boot CD ကို First Boot အဖြစ်လုပ်ဆောင်ဖို့ဖြစ်ပါတယ်။

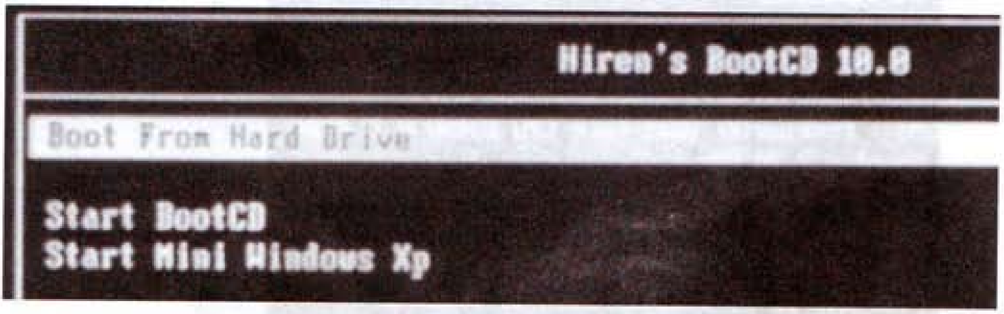
ကွန်ပျူတာစဖွင့်တဲ့မျက်နှာစာမှာညွှန်းထားတဲ့ BIOS POST Message ကိုဝင်ရောက်ရန် Key ကိုနှိပ်လိုက်ပါ။ အများအားဖြင့် Tab Key ကိုသုံးကြပါတယ်။ Pause Break လုစ်ခနဲသာပြတတ်လို့ Pause Break ဖြင့်စမ်းကြည့်ရပါမယ်။

BIOS POST Message ရဲ့မြင်ကွင်းဖြစ်ပါတယ်။ DEL ကို Run Setup သုံးရန်ဖြစ်ပြီး၊ F8 ကို BBS POPUT အတွက်သုံးဖို့ညွှန်းထားပါတယ်။ ဒါဆိုလျှင် စာဖတ်သူ First Boot ကိုချိန်းရန် F8 Key ကိုသုံးရပါမယ်။

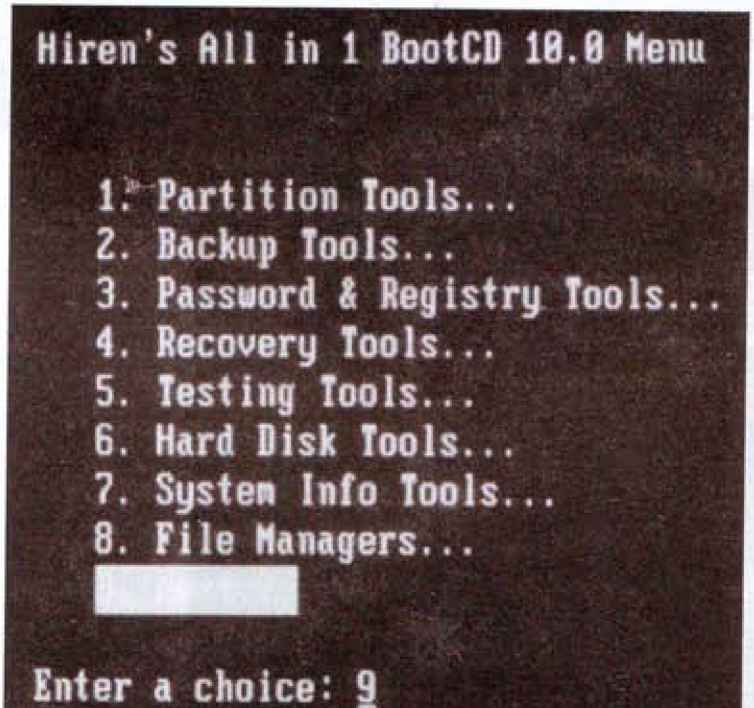
ကွန်ပျူတာကိုအစမှပြန်ဖွင့်လိုက်ပါ။ F8 Key ကိုမပျက်နှိပ်နှိပ်နေပါ။ အောက်ပါအတိုင်းတွေ့မြင်ရလျှင် CD Rom ကိုရွေးပေးလိုက်ယုံပင်ဖြစ်ပါတယ်။ Enter ခေါက်ပြီးထွက်လိုက်ပါ။

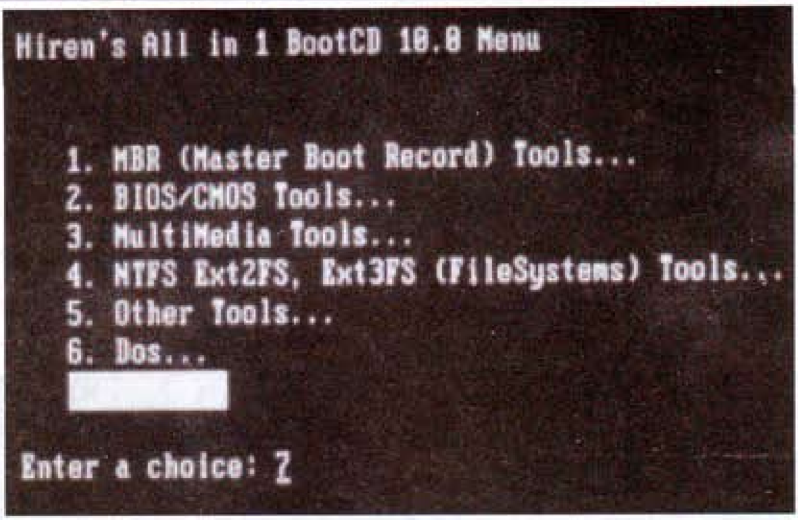


အောက်ပါအတိုင်း Hiren's Boot CD စတင်လုပ်ဆောင်နေသည်ကိုတွေ့ရပါမယ်။ Start BootCD ကိုရွေးပြီး Enter ခေါက်လိုက်ပါ။



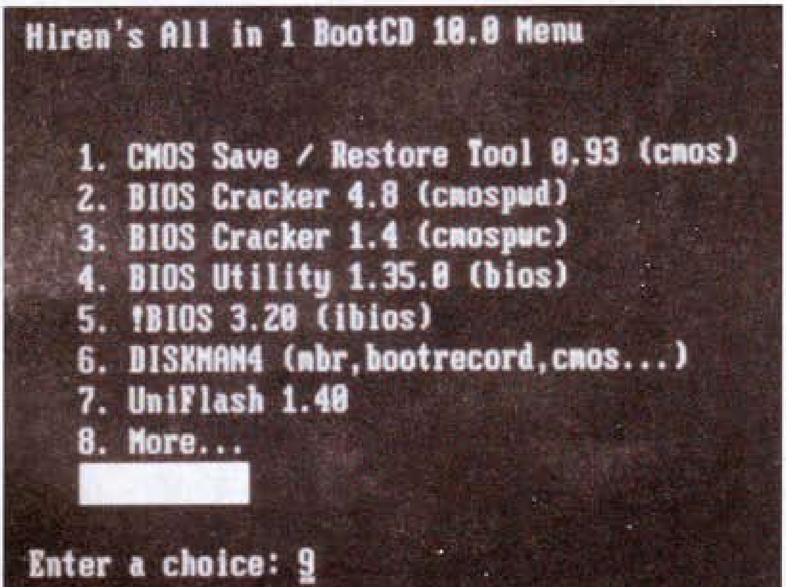
ယခုပြုလုပ်မှာကတော့ Hiren's Boot CD ကိုသုံးပြီး BIOS/CMOS ရဲ့ Admin Password ကိုရှာဖွေပါမယ်။ BIOS/CMOS တစ်ခုလုံးကိုဖျက်လိုက်ပြီး အစမှပြန်စနိုင်တာတွေရှိပေမယ့်၊ အခန့်မသင့်လျှင် လုံးဝသုံးမရတာတွေရှိတာကြောင့် Admin Password ကိုသာရှာဖွေတဲ့ ယခုစနစ်ကို သုံးပါ့မယ်။ အောက်မှမျက်နှာစာတွင် အဆိုပါစနစ်မပါသေးလို့ Next ကိုရွေးပြီး Enter ခေါက်ပါ။





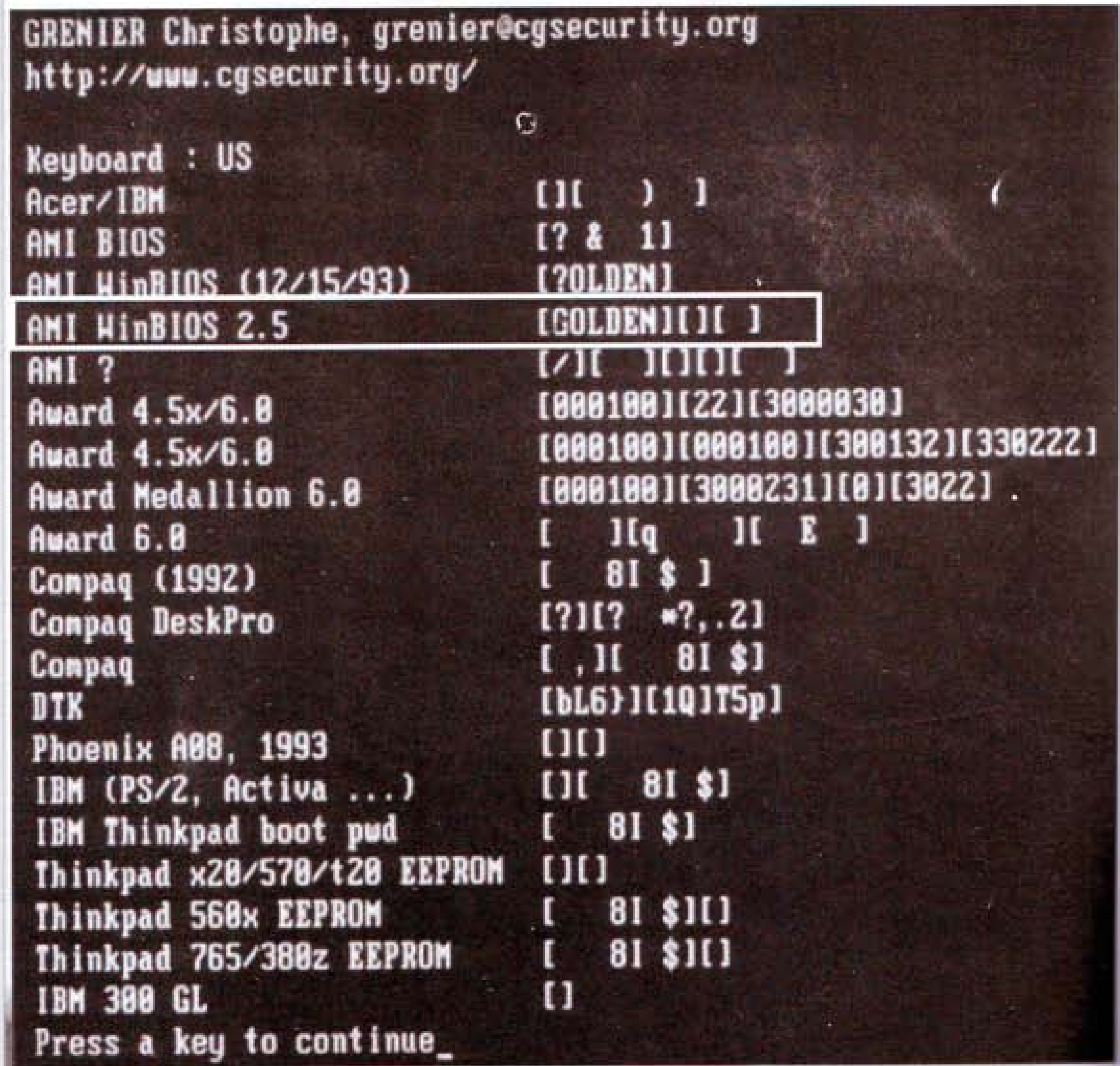
အထက်စာမျက်နှာအတိုင်း ဒုတိယမျက်နှာစာကိုတွေ့ရပါမယ်။ BIOS/CMOS Tools ကိုရွေးပြီး Enter ခေါက်ပါ။

အောက်ပါအတိုင်း BIOS/CMOS Tools အောက်ရှိလုပ်ဆောင်ချက်များကိုတွေ့ရပါလိမ့်မယ်။ စာဖတ်သူအတွက် ရှာဖွေရန်သာသုံးပြမှာဖြစ်လို့ 2. BIOS Cracker 4.8 (cmospwd) ကိုရွေးပြီး Enter ခေါက်လိုက်ပါ။



အောက်မှပုံအတိုင်း BIOS Cracker 4.8 ရဲ့လုပ်ဆောင်ချက်ကိုတွေ့ရပါလိမ့်မယ်။ BIOS/CMOS Password ကို AMI WinBIOS 2.5 ဘေးတွင်တွေ့ရပါမယ်။ စာရေးသူစမ်းသပ်ထားတဲ့စက်မှ Password က GOLDEN ဖြစ်ပါတယ်။ နောက်ဘက်မှကွင်းနှစ်ကွင်းကတော့ အလွတ်သာပေးထားပါတယ်။ စာလုံးအကြီး (Capital) တွေ့နဲ့သာဖော်ပြထားပေမယ့် စာလုံးသေး (Small Latter) ဖြစ်နိုင်ပါတယ်။

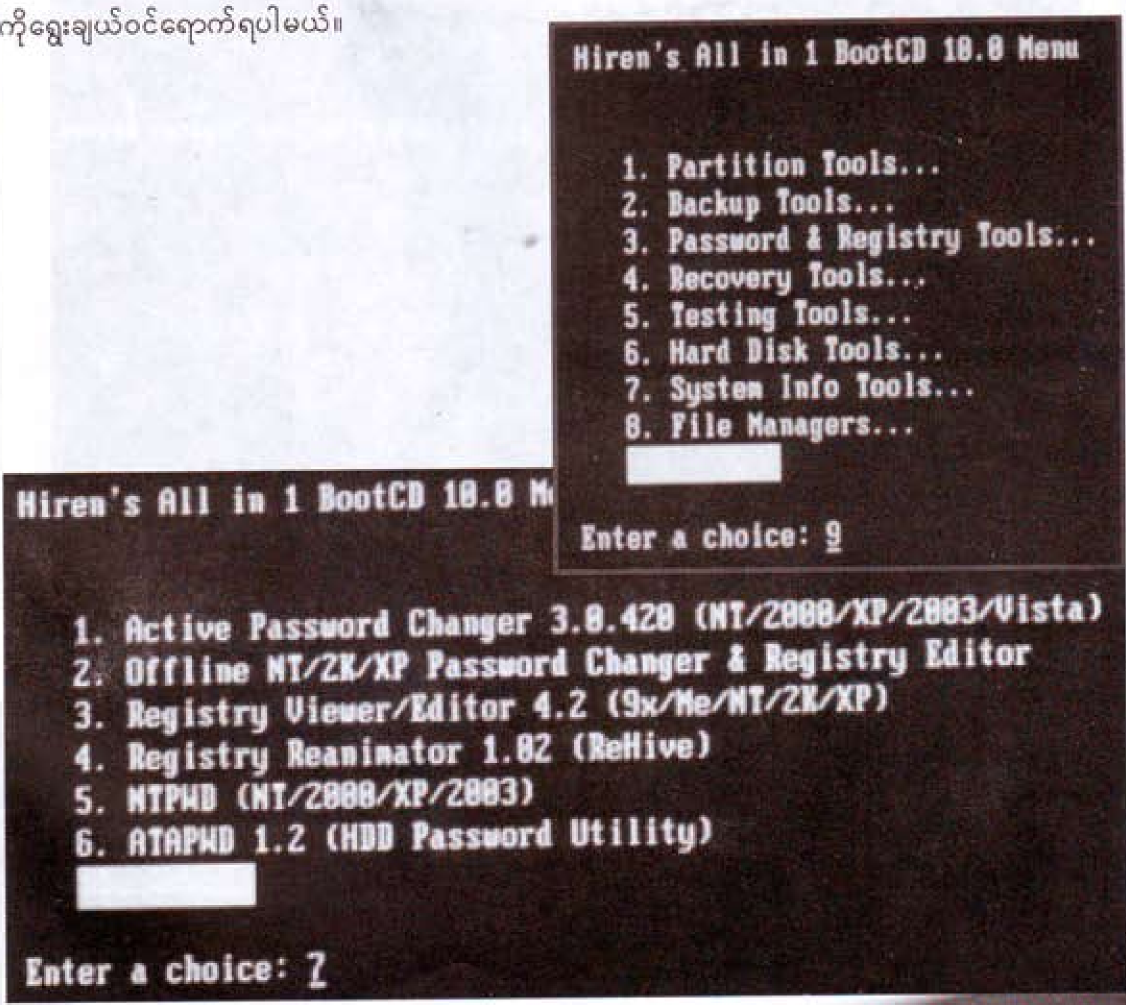
အဆိုပါ Password ကိုမှတ်ထားပြီး BIOS/CMOS အတွင်းသို့အစမှပြန်ဝင်ပြီး၊ အကြီးအသေး နှစ်မျိုးစမ်းသုံးကြည့်ပါ။



Admin Security ကိုထိုးဖောက်ခြင်း

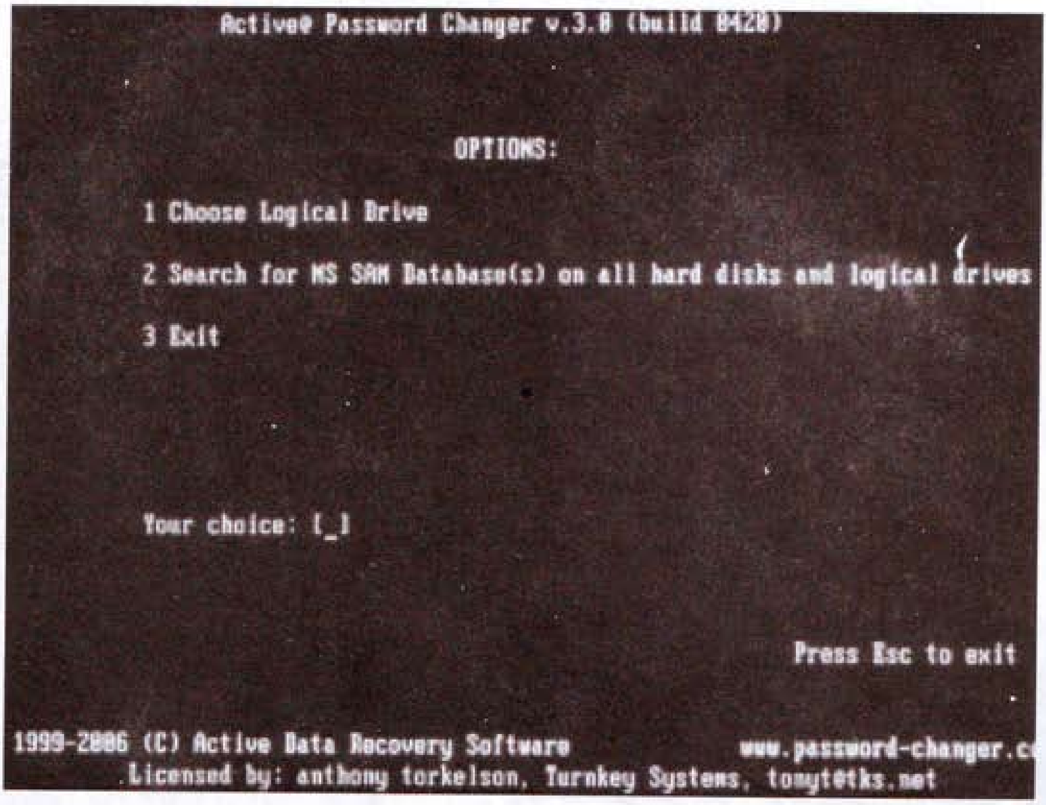
ကွန်ပျူတာကို Admin တစ်ယောက်သာသုံးခွင့်ရရန် LogOn Password ပေးထားကြပါတယ်။ စာဖတ်သူဟာ ကွန်ပျူတာစက်ပြင်ဆင်သူဆိုလျှင် အဆိုပါပြဿနာမျိုးတွေ မကြာခဏတွေ့ရပါလိမ့်မယ်။ ကိုယ်ပေးထားတဲ့ Admin LogOn Password ကိုကိုယ်ပြန်မဖွင့်နိုင်လို့ ဆိုင်ရောက်လာကြတာတွေ အများသားပါ။

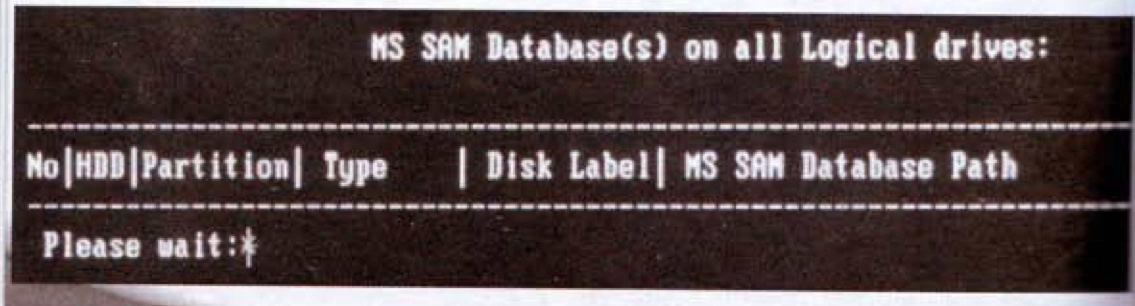
Hiren's BootCD ကိုထည့်ပြီးဖော်ပြခဲ့ပြီးသောနည်းအတိုင်း First Boot ဖြင့်ဝင်ရောက်လိုက်ပါ။ Start Boot CD ထဲသို့ဝင်ပါ။ အောက်ပါအတိုင်း ပထမမျက်နှာစာမှ 3. Password & Registry Tools ကို ရွေးချယ်ဝင်ရောက်ပါ။ အောက်ဆုံးမှပုံအတွက် 1. Active Password Changer 3.02 ---- ကိုရွေးချယ်ဝင်ရောက်ရပါမယ်။



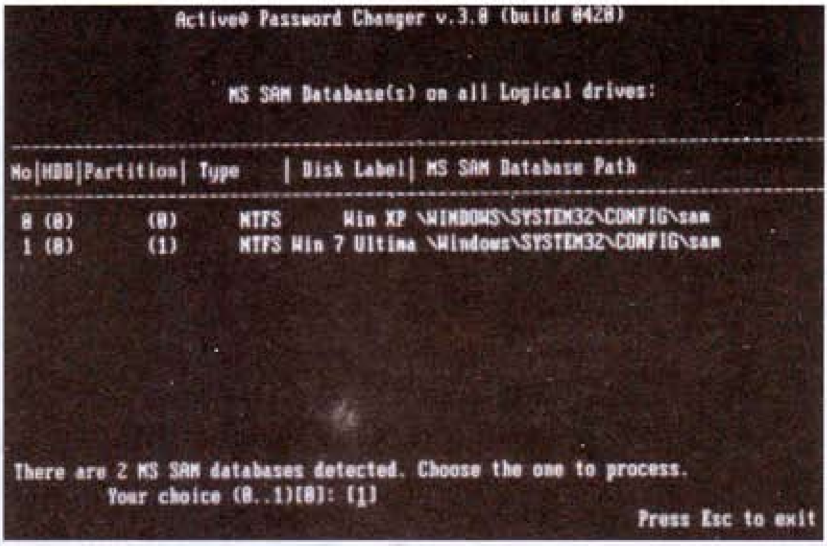
Active Password Changer ကိုအောက်ပါအတိုင်းတွေ့မြင်ရပါမယ်။ Password များထားရှိရာ SAM Database ကို Harddisk အပိုင်းအားလုံးမှာရှာရန်ဖြစ်လို့ 2.Search For MS SAM ---ကိုရွေးပေးရပါမယ်။ ဒီတစ်ခါတော့ ခေါင်းစဉ်အညွှန်းရှေ့ပိုင်းမှ နံပတ်ကိုသုံးရပါမယ်။

ဒါကြောင့် 2 ကိုရိုက်သောအခါ Your Choice ( ) အကွက်တွင်ပေါ်နေပါလိမ့်မယ်။ ရိုက်ပြီး Enter ခေါက်ပါ။ အောက်ဆုံးမှပုံအတိုင်း Please Wait ; # စာတန်းထိုးကာ ခေတ္တစောင့်ရပါလိမ့်မယ်။

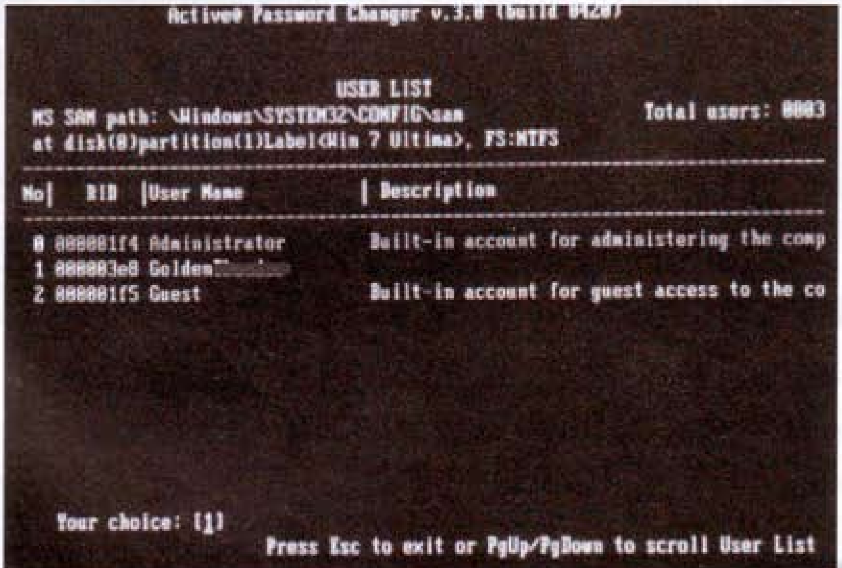




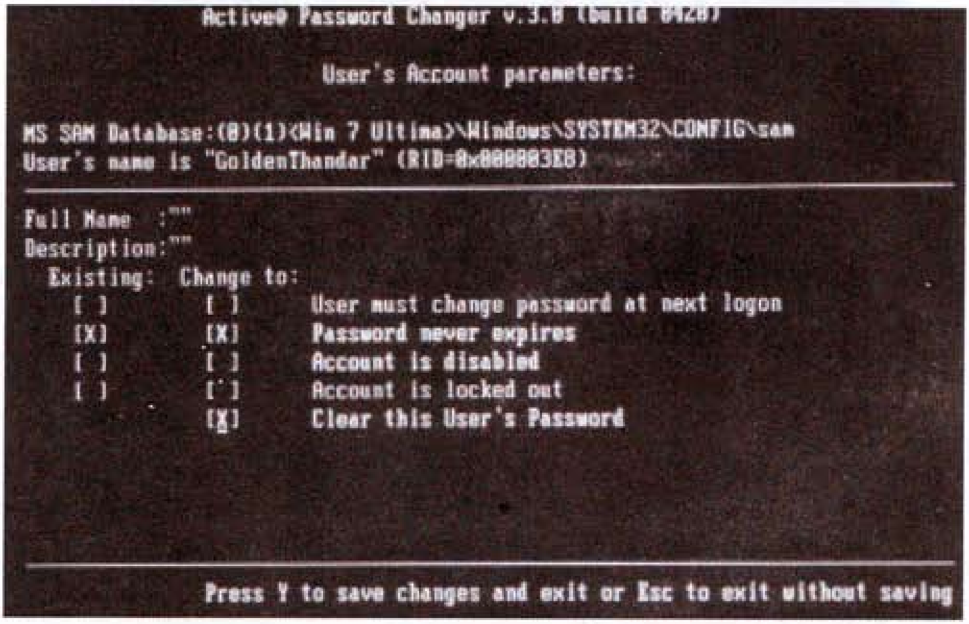
စာရေးသူစက်တွင် Windows OS ၂မျိုးထားရှိလို့ အောက်ပါအတိုင်းတွေ့ရပါလိမ့်မယ်။ ယခု Windows 7 LogOn Password ကိုထိုးဖောက်မှာဖြစ်လို့ ခေါင်းစဉ်နံပတ် 1 ကိုရွေးရန် 1 ရိုက်ထည့်ပါ။

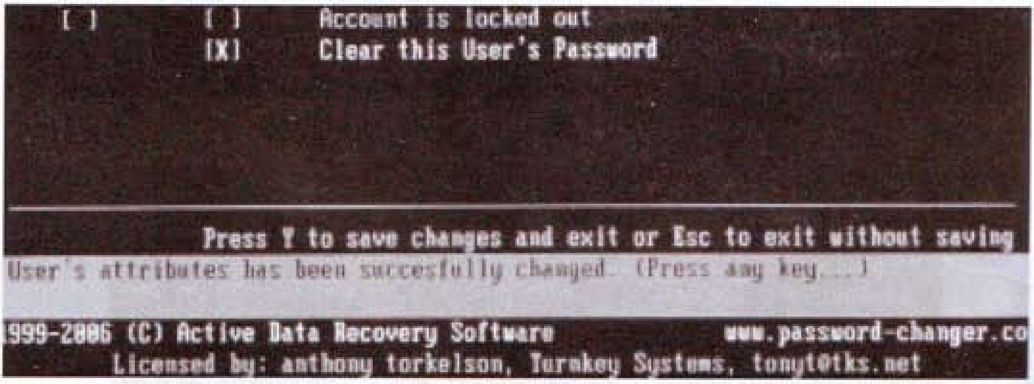


စာရေးသူ၏ Windows 7 မှာထားရှိသော LogOn Account မှာ ခေါင်းစဉ်နံပတ် 1 ရှိ Golden ဖြစ်ပါတယ်။ ဒါကြောင့် နံပတ် 1 ကိုရိုက်ထည့်ရွေးချယ်ပါ။



အောက်ပါအတိုင်း Account Password Clear မျက်နှာစာကိုတွေ့မြင်ရလျှင် y key ကိုနှိပ်လိုက်ပါ။ အောက်ဆုံးမှပုံကိုတွေ့ရပြီး Pass Any Key လို့တောင်းဆိုနေတာကြောင့် Space Bar ဖြစ်ဖြစ်နှိပ်ပေးလိုက်ပါ။





အားလုံးပြီးဆုံးသွားပြီဖြစ်လို့ Ctrl + Alt + Del ကိုနှိပ်ပြီး Restart ချလိုက်ပါ။ တစ်မှပြန်စပွင့်လာသောအခါ Security လုပ်ဆောင်ချက်များမရှိတော့ပြီဖြစ်လို့ စာဖတ်သူစိတ်ကြိုက် ဝင်ရောက်အသုံးပြုနိုင်ပါပြီ။ ယခုလုပ်ဆောင်ချက်မှာ Windows 7 အတွက်ဖြစ်လို့ Windows 7 အတွင်းဝင်ရောက်သွားလျှင် ယခင်ကလို LogOn Password မရှိတော့ပါ။ တိုက်ရိုက်ဝင်ရောက်သွားပါတယ်။

Deep Freeze နှင့်ပြဿနာအဖြာဖြာ

ကွန်ပျူတာအသုံးပြုသူအများစုနှင့် အင်တာနက်ဆိုင်အများစုသည် Deep Freeze ကို Security ပိုင်းအရသုံးဆွဲကြပါတယ်။ Deep Freeze Program ကိုနေရာပေါင်းစုံမှ ပုံစံမျိုးစုံရလာကြပါတယ်။ ပြဿနာကထိုမှစတင်တွေ့လာရပါပြီ။

စာရေးသူလည်းယခင်က စမ်းသုံးခဲ့စဉ် Password အသေဖြင့်ပေးထားသော Deep Freeze Program ကိုသုံးခဲ့ရပါတယ်။ Password ကအသေဖြစ်နေပြီး ဖော်ပြမထားတဲ့အတွက် ပြန်ပြင်လို့မရတော့ပါဘူး။ အကြောင်းရှိလို့ Program ထပ်ထည့်လိုတဲ့အခါတွေမှာ Password မသိတော့ Deep Freeze ကိုပိတ်လို့မရဖြစ်ခဲ့ပါတယ်။

ဒါ့ကြောင့် နိုင်ငံရပ်ခြားရှိ မိတ်ဆွေတစ်ဦးထံသို့ စာပို့အကူအညီတောင်းခံခဲ့ပါတယ်။ အလွန်လွယ်ကူပြီး ပေါ့ပေါ့ပါးပါးရှိလှသော Remove Program လေးကိုပေးပို့ခဲ့ပါတယ်။ စာရေးသူလည်း အင်တာနက်ပေါ်တွင် အများအတွက်ဖြန့်ဝေပေးခဲ့ပါတယ်။ အဆိုပါမိတ်ဆွေကတော့ သိပ်သဘောမတူချင်ပါဘူး။

ယခုကဲ့သို့သော ကိစ္စတွေဟာ စာရေးသူတစ်ယောက်တည်းကြုံနေရတာမဟုတ်ပါဘူး။ အများသူငှာတွေလည်းတွေ့ကြုံနေရပါတယ်။ Deep Freeze ဟာ Uninstall မရှိပါဘူး။ ပြန်ဖြုတ်လိုလျှင် Install လုပ်စဉ်ကလိုပြန်လုပ်မှသာ Uninstall လုပ်ခွင့်ရှိပါတယ်။ အဓိကကတော့ Password သိဖို့လိုပါသေးတယ်။

အင်တာနက်ဆိုင်တွေဆိုလျှင် Server စနစ်သုံးထားလို့ ပိုဒုက္ခရောက်ရပါတယ်။ Deep Freeze ဖြုတ်ချင်လျှင် Windows အသစ်ပြန်တင်မှသာရတော့မယ့်အနေအထားပါ။

သတိပြုရမှာကတော့ အင်တာနက်ဆိုင်များတွင် ယခု Program ဖြင့် Deep Freeze ကိုဝင်ဖြုတ်ပြီး ဖျက်စီးမှုတွေပြုလုပ်တတ်ပါတယ်။ Server ကိုင်သူမှ စက်တစ်လုံး Restart ကျသွားလျှင် အနီးကပ်သွားကြည့်ပါ။ နာရီထားရှိရာဘေးတွင် ဝက်ဝံပုံအမှတ်အသားဖြင့် ကြက်ခြေခတ်ပြထားလျှင် အဆိုပါ User ကိုစက်ပြောင်းပေးလိုက်ပါ။ Deep Freeze ပြုတ်ကျသွားပါပြီ။ ပြန်ဖွင့်ဖို့လိုအပ်ပါတယ်။

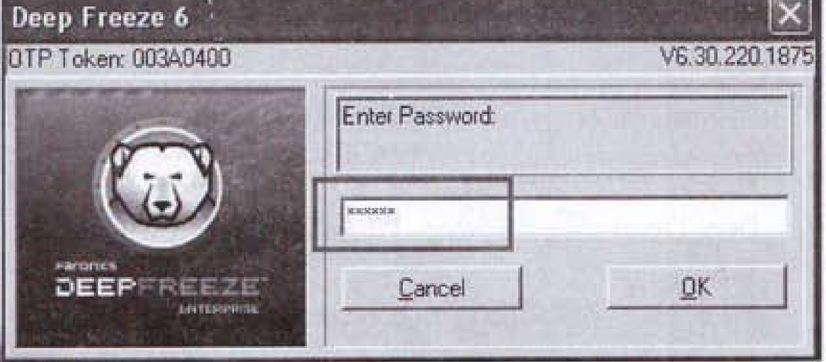
Deep Freeze ဟာ ဖြုတ်ခြင်း၊ တပ်ခြင်း၊ ပိတ်ခြင်းများကို ပြောင်းလဲတိုင်းစက်ကို Restart ပြန်ချမှရပါတယ်။ ဒါကြောင့် Server Admin မှ User များကိုအလွတ်မပေးထားသင့်ပါ။ ယခုအခါ အင်တာနက်ပေါ်တွင် Deep Freeze ကိုဖြုတ်နိုင်သော Program များစွာအလွယ်ရနေပါပြီ။

စာရေးသူစီဒီအတွင်းမှ Faronics Folder > Deep Freeze Password Remover Folder> df_Pass_Remover.exe ကို ကလစ်နှစ်ချက်နှိပ်ပြီးစတင်လိုက်ပါ။

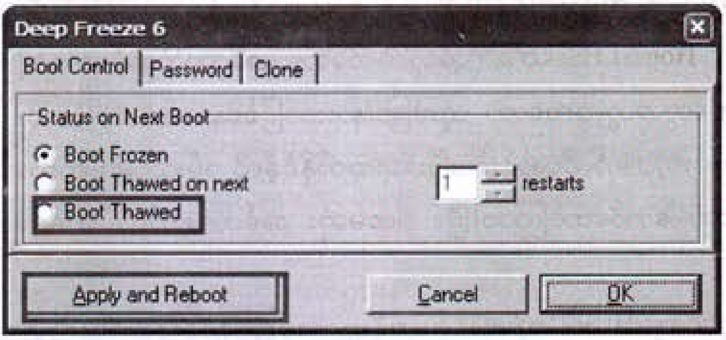
df_pass_remover 11/16/2009 2:59 PM Application

အောက်ပုံစံတွေ့မြင်ရလျှင် ပထမ cHANGE 1T Button ကိုနှိပ်ပါ။ ဒုတိယ OK Button ကိုနှိပ်ပါ။ တတိယ အပေါ်ညာထောင့်မှ X close ဖြင့်ပိတ်ပါ။ Deep Freeze ရဲ့ Password ကိုဖျက်လိုက်ပါပြီ။ တစ်ခါသုံးဖြစ်လို့ တစ်ကြိမ်သာအဝင်အထွက်ရရှိတယ်ဆိုတာမမေ့ပါနှင့်။

Deep Freeze ကိုဖွင့်ရန်အတွက် Ctrl + Alt + Shift + F6 လေးလုံးတွဲနှိပ်ပြီးဝင်နိုင်သလို၊ နာရီဘေးရှိ ဝက်ဝံပုံ Icon ကို Shift + Mouse Click ဖြင့်နှိပ်ပြီးလည်းဝင်ရောက်နိုင်ပါတယ်။ အောက်ပါအတိုင်း Password ကျလာတဲ့အခါ ဘာမှမထည့်ပဲ OK Button ကိုနှိပ်လိုက်ပါ။

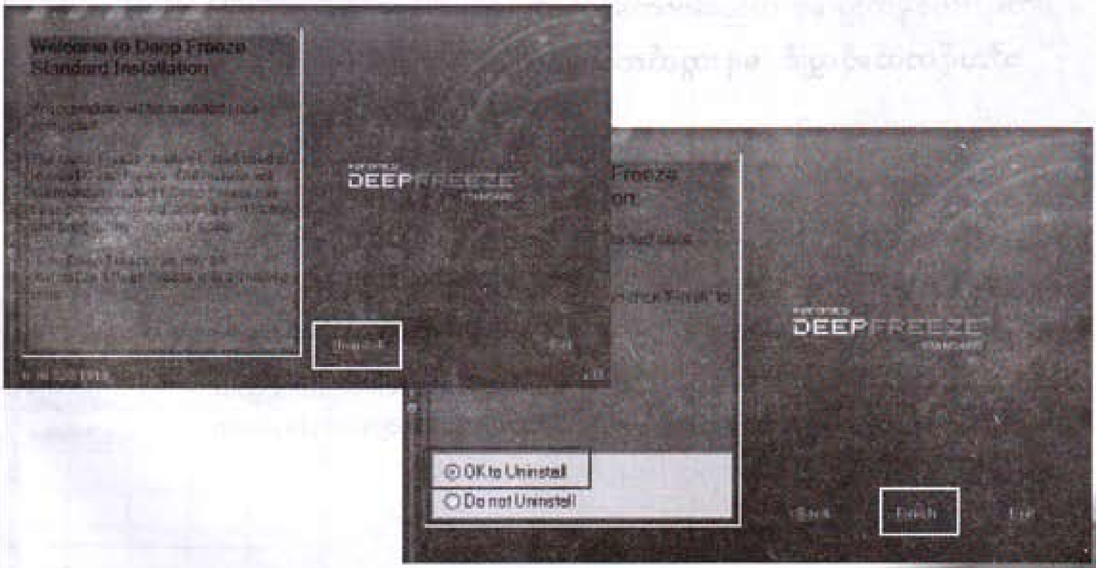


အောက်အတိုင်းတွေ့မြင်ရသောအခါ Boot Control Tab အောက်ရှိ Boot Thawed ကိုရွေးချယ်ပြီး Apply and Reboot Button ကိုနှိပ်လိုက်ပါ။ စက်ပြန်လည်စတင်သောအခါ Deep Freeze အလုပ်မလုပ်တော့ကြောင်းကို နာရီဘေးရှိ ဝက်ဝံပုံတွင် အနီရောင်အမြှောက်ရှိနေပါလိမ့်မယ်။



Deep Freeze Program Uninstall

Deep Freeze ကိုမည်သည့်ပုံမှန်နည်းနှင့်မှ ပြန်ဖျက်မရနိုင်ပါ။ သာမန်သူတို့ဝင်ရောက်မဖျက်နိုင်ရန် Safety မြင့်မြင့် လုပ်ထားတာပါ။ Uninstall လုပ်လိုလျှင် Install လုပ်စဉ်အတိုင်းပြန်လုပ်ရပါမယ်။ Install လုပ်ပြီးသားဖြစ်လို့ အောက်ပါ Uninstall Box များတက်လာပါမယ်။ Uninstall ကိုနှိပ်လိုက်ပါ။ ဒုတိယပုံစံတွင် Ok to Uninstall ကိုရွေးချယ်ပြီး Finish ကိုနှိပ်ပါ။ အလိုအလျှောက်ပြန်လည်ဖျက်သွားပါလိမ့်မယ်။



နှုတ်ဆက်စကား ...

Honest Hacker ဖြစ်လိုသူဆိုတာ ရှင်းရှင်းပြောရလျှင် အလွန်ရှားပါတယ်။ အများအားဖြင့် သူတစ်ပါးကို ဒုက္ခပေးလိုသူကပိုများနေပါတယ်။ ဒါကြောင့် ဒီစာအုပ်လေးကို ရင်တမမနဲ့ပဲ ရေးထုတ်လိုက်ပါတယ်။ Honest Hacker တွေအတွက်ကတော့ အထောက်အပံ့ကောင်းဖြစ်စေမှာပါ။

Black Hacker တွေအတွက်ကတော့ ထူးမခြားနားသာဖြစ်နေမယ်ထင်ပါတယ်။ ဘာပဲဖြစ်ဖြစ် စာရေးသူအနေဖြင့် ကောင်းတဲ့ဘက်ကိုဖေးပေးပြီးရေးထုတ်နိုင်ခဲ့လို့ ဝမ်းသာမိပါတယ်။ ယခုစာအုပ်ကို စတင်ရေးဖို့ကြိုးစားခဲ့တာ တော်တော်ကြာပါပြီ။ ပထမဆုံး အင်တာနက်လိပ်စာများ စာအုပ်ကပင် ကြော်ငြာခဲ့တာပါ။

အဓိကကတော့ ကျောင်းသား/သူများနှင့် ကွန်ပျူတာပညာရပ်လေ့လာနေသူများ၊ ကွန်ပျူတာ စက်ပြင်ဝါသနာရှင်များနှင့် ရပ်ဝေး–နယ်ဝေး၊ နိုင်ငံရပ်ခြားမှ ကိုယ်ပိုင်ပညာရှာနေသူများအတွက် ရည်ရွယ်ရေးသားပါတယ်။ အခြားသိလိုသည်များကိုလည်း စာရေးသူရဲ့ Blog မှတဆင့်ဝင်ရောက်မေးမြန်း လေ့လာနိုင်ပါတယ်။

သင်တန်းကျောင်းများတွင် မသင်ကြားတဲ့ သင်ခန်းစာများနှင့် ဗဟုသုတရရှိနိုင်သလို လက်တွေ့အသုံးဝင်လုပ်ဆောင်ချက်များစွာကို ရှင်းရှင်းလင်းလင်းရှင်းပြထားတဲ့အပြင် လိုအပ်တဲ့ဆော့ဖ်ဝဲလ် တွေကိုလည်းထောက်ပံ့ပေးထားပါတယ်။

စိတ်ရင်းတစ်ခုတည်းနှင့် တည်ဆောက်ခဲ့တဲ့ရည်ရွယ်ချက်က –

" သိသင့်တယ်ဆိုလျှင် မဖုံးကွယ်ထားချင်လို့ပါ "

ကျေးဇူးတင်လျက်

သန်းထိုက်(ရွှေရိပ်)

goldenshadetech@gmail.com
http://thanhtikegs.weebly.com

HACKING ဆိုတာအတွင်းကျကျသိရှိခြင်းပါ။

Windows ကိုအတွင်းကျကျလေ့လာနိုင်ဖို့ဦးတည်ပြုစုထားတဲ့စာအုပ်တစ်အုပ် ....

Honest Hacking လုပ်ဆောင်အဖြစ်ဦးတည်စေတာကတော့ ရိုးသားတဲ့စိတ်တစ်ခုပေါ်မှူတည်ပြီး သဘောရိုးဖြင့် အတွင်းကျကျလေ့လာနိုင်ဖို့အတွက်ဖြစ်ပါတယ် ....

Windows
Registry
Group Policy
BIOS Security Hack
System Security Hack
Windows Speed Hack
Internet Speed Hack
Gmail, Gtalk Hack
Study To Hakcing Software
SpeedUp Software
DeepFreeze Remove and Hack
Using the Hiren Boot System

သန်းထိုက် (ရွှေရိပ်)
goldenshadetech@gmail.com
http://thanhtikegs.weebly.com