စိတ်ကူးချိုချိုအနုပညာ

သင့်ကွန်ပျူတာအတွက် မရှိမဖြစ် ဆော့ဖ်ဝဲများ

ESSENTIAL SOFTWARES FOR YOUR COMPUTER

ဂျူလိုင်စိုး

ဒို့အာဇာနည်အရေးသုံးပါး

ပြည်ထောင်စု မပြိုကွဲရေး	ဒို့အရေး
တိုင်းရင်းသားစည်းလုံးညီညွတ်မှု မပြိုကွဲရေး	ဒို့အရေး
အချုပ်အခြာအာဏာတည်တံ့ခိုင်မြဲရေး	ဒို့အရေး

ပြည်သူ့သဘောထား

* ပြည်ပအားကိုး ပုဆိန်ရိုး အဆိုးမြင်ဝါဒီများအား ဆန့်ကျင်ကြ။
* နိုင်ငံတော် တည်ငြိမ်အေးချမ်းရေးနှင့် နိုင်ငံတော်တိုးတက်ရေးကို နှောင့်ယှက်ဖျက်ဆီးသူများအား ဆန့်ကျင်ကြ။
* နိုင်ငံတော်၏ ပြည်တွင်းရေးကို ဝင်ရောက်စွက်ဖက်နှောင့်ယှက်သော ပြည်ပနိုင်ငံများအား ဆန့်ကျင်ကြ။
* ပြည်တွင်းပြည်ပ အဖျက်သမားများအား ဘုံရန်သူအဖြစ် သတ်မှတ်ချေမှုန်းကြ။

နိုင်ငံရေးဦးတည်ချက် (၄) ရပ်

* နိုင်ငံတော်တည်ငြိမ်ရေး၊ ရပ်ရွာအေးချမ်းသာယာရေးနှင့် တရားဥပဒေ စိုးမိုးရေး၊
* အမျိုးသားစည်းလုံးညီညွတ်မှုခိုင်မာရေး၊
* စည်းကမ်းပြည့်ဝသောဒီမိုကရေစီစနစ်ရှင်သန်ခိုင်မာအောင်တည်ဆောက်ရေး၊
* ဖွဲ့စည်းပုံအခြေခံဥပဒေနှင့်အညီ ခေတ်မီဖွံ့ဖြိုး တိုးတက်သော နိုင်ငံတော်သစ် တည်ဆောက်ရေး၊

စီးပွားရေးဦးတည်ချက် (၄) ရပ်

* စိုက်ပျိုးရေးကို ပိုမိုဖွံ့ဖြိုးတိုးတက်အောင် ဆောင်ရွက်ပြီး ခေတ်မီစက်မှုနိုင်ငံထူထောင်ရေး နှင့် အခြားစီးပွားရေးကဏ္ဍများကိုလည်း ဘက်စုံဖွံ့ဖြိုးတိုးတက်အောင်တည်ဆောက်ရေး၊
* ဈေးကွက်စီးပွားရေးစနစ် ပီပြင်စွာဖြစ်ပေါ်လာရေး၊
* ပြည်တွင်းပြည်ပမှ အတတ်ပညာနှင့်အရင်းအနှီးများဖိတ်ခေါ်၍ စီးပွားရေး ဖွံ့ဖြိုးတိုးတက်အောင် တည်ဆောက်ရေး၊
* နိုင်ငံတော်စီးပွားရေးတစ်ရပ်လုံးကို ဖန်တီးနိုင်မှုစွမ်းအားသည် နိုင်ငံတော် နှင့် တိုင်းရင်းသားပြည်သူတို့၏ လက်ဝယ်တွင်ရှိရေး၊

လူမှုရေးဦးတည်ချက် (၄) ရပ်

* တစ်မျိုးသားလုံး၏စိတ်ဓာတ်နှင့် အကျင့်စာရိတ္တမြင့်မားရေး၊
* အမျိုးဂုဏ်၊ ဇာတိဂုဏ်မြင့်မားရေးနှင့် ယဉ်ကျေးမှုအမွေအနှစ်များ အမျိုးသားရေးလက္ခဏာများ မပျောက်ပျက်အောင် ထိန်းသိမ်းစောင့်ရှောက်ရေး၊
* စစ်မှန်သော မျိုးချစ်စိတ်ဓာတ်ဖြစ်သည့် ပြည်ထောင်စုစိတ်ဓာတ်ရှင်သန်ထက်မြက်ရေး၊
* တစ်မျိုးသားလုံးကျန်းမာကြံ့ခိုင်ရေးနှင့် ပညာရည်မြင့်မားရေး၊

စိတ်ကူးချိုချိုစာအုပ်

သင့်ကွန်ပျူတာအတွက် မရှိမဖြစ် ဆော့ဖ်ဝဲများ

ဂျူလိုင်စိုး

ပထမအကြိမ်

သင့်ကွန်ပျူတာအတွက်မရှိမဖြစ်သောဆော့ဖ်ဝဲများ
ဂျူလိုင်စိုး

ပုံနှိပ်မှတ်တမ်း

စာမူခွင့်ပြုချက်အမှတ်	-	အုပ်စု - ၁၊ နည်းပညာ
ထုတ်ဝေသူ	-	ဦးစန်းဦး
ပုံနှိပ်သူ	-	ဒေါ်ဝင်းမာ
မျက်နှာဖုံးဒီဇိုင်း	-	အမ်အက်စ်အို
ကွန်ပျူတာဖလင်	-	အီးဂဲလ်
လက်ခွဲဖလင်	-	အေဇက်
စာအုပ်ချုပ်	-	ကိုတင်အေး(လှိုင်)

ဝဝ၆
ဂျူလိုင်စိုး
သင့်ကွန်ပျူတာအတွက်မရှိမဖြစ်သောဆော့ဖ်ဝဲများ /
ဂျူလိုင်စိုး -ရန်ကုန်၊
စိတ်ကူးချိုချိုစာပေ၊ ၂၀၁၂၊ စာမျက်နှာ ၂၀၅ မျက်နှာ၊
၁၄.၅ စင်တီ× ၂၃ စင်တီ
(၁)သင့်ကွန်ပျူတာအတွက်မရှိမဖြစ်သောဆော့ဖ်ဝဲများ

၂၀၁၂၊ ဖေဖော်ဝါရီလ၊ အုပ်ရေ ၅၀၀
ရောင်းဈေး

မာတိကာ

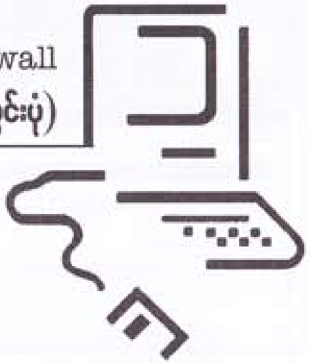
- အမှာ ၁

၁။ COMODO Fire wall
(Windows လုံခြုံရေးစနစ် ထည့်သွင်းပုံ) ၃
၂။ KeePass software ကို Install လုပ်ပုံနှင့် အသုံးပြုပုံ ၂၆
၃။ True Crypt အား Install ပြုလုပ်ပုံနှင့် Standard Volumes များ ဖန်တီးပုံ ၅၁
၄။ Recuva ပျက်စီးသွားသော ဖိုင်များကို ပြန်လည်ရယူခြင်း ၈၅
၅။ CCleaner တိကျသောဖိုင်ဖျက်သိမ်းမှုနှင့် အလုပ်လုပ်သည့်ကဏ္ဍ၌ သုတ်သင်ရှင်းလင်းခြင်းအပိုင်း ၁၁၀
၆။ RiseUp - လုံခြုံသော အီးမေးလ်ဝန်ဆောင်မှု ၁၃၄
၇။ Thunderbird - လုံခြုံစိတ်ချရသော အီးမေးလ်သုံးစွဲမှုစနစ် ၁၅၆

အမှာ

ကွန်ပျူတာတစ်လုံး သင့် အိမ်မှာရှိတယ်ဆိုရင်၊ နောက်ပြီး အဲဒီ ကွန်ပျူတာကလဲ အင်တာနက်ချိတ်ထားတယ်ဆိုရင် ဒီစာအုပ်ထဲမှာပါတဲ့ ဆော့ဖ်ဝဲတွေဟာ သင့်အတွက် တကယ် အသုံးတည့်မှာပါ။ ဒီ ဆော့ဖ်ဝဲအားလုံးဟာ သင့်ရဲ့ ကွန်ပျူတာမှာ အခြေခံအားဖြင့် မရှိမဖြစ် လိုအပ်တဲ့ ဆော့ဖ်ဝဲတွေ ဖြစ်ပါတယ်။ ကွန်ပျူတာအတွက် အသင့်တော်ဆုံးနဲ့ အသုံးတည့်ဆုံးဖြစ်မယ့် ဆော့ဖ်ဝဲတွေကို စုစည်းဖော်ပြပေးထားပါတယ်။ ဒီဆော့ဖ်ဝဲတွေကို အင်တာနက်ပေါ်က အခမဲ့ download ရယူနိုင်သလို ကွန်ပျူတာဆော့ဖ်ဝဲ ရောင်းချတဲ့ဆိုင်တွေမှာလည်း အလွယ်တကူ ဝယ်ယူလို့ ရပါတယ်။ ဒီစာအုပ်မှာ အခန်းကဏ္ဍအလိုက် ဆော့ဖ်ဝဲကို စတင် installation လုပ်တဲ့အချိန်ကနေ အသုံးချပုံ အသုံးချနည်းအထိ အဆင့်ဆင့် ဖော်ပြပေးထားပါတယ်။ အမေးအဖြေ ပုံစံမျိုးနဲ့လည်း ရှင်းလင်းထားပါတယ်။ လုံခြုံစိတ်ချရတဲ့ ကွန်ပျူတာတစ်လုံးကို ပိုင်ဆိုင်နိုင်ဖို့ ဒီစာအုပ်လေး လက်ကိုင်ထားမယ်ဆိုရင် သင့်တော်ပါလိမ့်မယ်။

COMODO Fire wall (Windows လုံခြုံရေးစနစ် ထည့်သွင်းပုံ)



ဤအခန်းတွင်ပါဝင်သည့်အပိုင်းများမှာ

(2.0)- COMODO Firewall ထည့်သွင်းခြင်း လုပ်ငန်းစဉ်များ
(2.1)- Windows တွင်ပါရှိသည့် Firewall (လုံခြုံရေးစနစ်)အား ဖယ်ရှားပုံ
(2.2)- COMODO Firewall အား Windows ၌ ထည့်သွင်းပုံ

2.0 COMODO Firewall ထည့်သွင်းခြင်း လုပ်ငန်းစဉ်များ

COMODO Firewall ကို ထည့်သွင်းရာ၌ အဆင့်နှစ်ဆင့် ခွဲခြား၍ လွယ်ကူလျင်မြန်စွာ ဆောင်ရွက်နိုင်သည်။ ပထမအဆင့်မှာ Windows ရှိ Firewall ၏ လုပ်ဆောင်ချက်များကို ရပ်ပစ်ရန်နှင့် ဒုတိယအဆင့်မှာ COMODO Firewall ကို ထည့်သွင်းရန်ဖြစ်သည်။

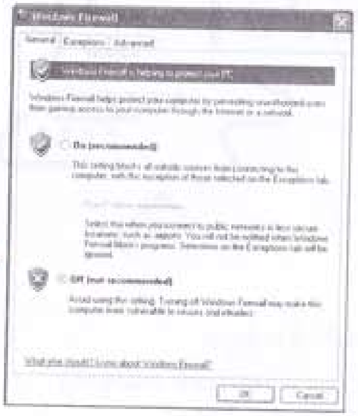
အကြံပေးလိုသည်မှာ မည်သည့်အချိန်တွင်မဆို သင်၏ ကွန်ပျူတာတွင် Windows လုံခြုံရေးစနစ်ကို program တစ်မျိုးသာလျှင် အသုံးပြုသင့်သည်။ COMODO Firewall ကို သင်၏ ကွန်ပျူတာ System သို့ မထည့်သွင်းမီ သင်၏ ကွန်ပျူတာတွင်ယခု အသုံးပြုနေသော Firewall ကို ရှုပ်ထွေးမှု မဖြစ်စေရန် အရင်ထုတ်ပစ်ရမည်။

2.1 Windows Firewall အား ဖယ်ရှားပုံ

Windows Firewall program အား ဖယ်ရှားရန် အောက်ပါ အစီအစဉ်များ ဆောင်ရွက်ရမည်။

အဆင့် 1: Start menu ရှိ Control Panel ကို သွားပါ။ Control Panel ၌ Windows Firewall Program ကို ဖွင့်ပါ။

အဆင့် 2: အောက်ဖော်ပြပါ ပုံ (1) အတိုင်း Windows Firewall အား ဖယ်ရှားရန် Off option အား စစ်ဆေးပါ။



ပုံ 1: Windows Firewall ရှိ Off option အား တွေ့ရပုံ

အဆင့် 3: Windows Firewall အား ပိတ်ရန် Off option ကို Enable နှိပ်ပါ။

2.2 COMODO Firewall ကို ထည့်သွင်းပုံ

မှတ်ချက်။ အကယ်၍ သင်၏ ကွန်ပျူတာတွင် COMODO Firewall program ရှိနေနှင့်ပြီးပါက ယခုနောက်ဆုံး ထည့်သွင်းမည့် versions သည် မူလ versions အား အလိုအလျောက်ဖယ်ရှားမည် မဟုတ်ဘဲ ၎င်း၏ အညွှန်းပုံစံအတိုင်း လိုက်ပါဆောင်ရွက်ခြင်းအားဖြင့် ဖယ်ရှားပေးလိမ့်မည်။

COMODO Firewall အား ထည့်သွင်းရန် အောက်ပါအဆင့်များကို ဆောင်ရွက်ရမည်။

အဆင့် 1: COMODO Firewall Software ကို နှစ်ကြိမ်နှိပ် (Double Click)ပါ။

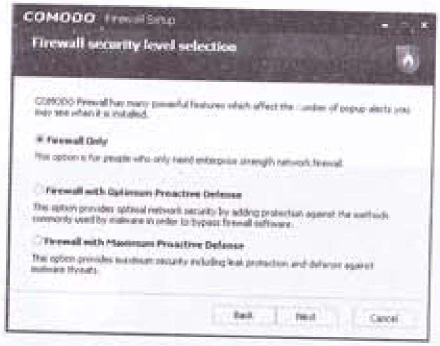
လုံခြုံရေး အချက်ပေးသည့် dialog box ပေါ်လာက Yes ကိုနှိပ်ပါ။ အောက်တွင်ပါရှိသည့်ပုံအတိုင်း အတည်ပြုချက်ပေးမည့် Dialog box ပေါ်လာလိမ့်မည်။

ပုံ 2 : ဘာသာစကားသုံးစွဲမှုကို အတည်ပြုချက်ပေးမည့် dialog box ပုံ

အဆင့် 2: Yes ကို နှိပ်ပါ။ သုံးစွဲသူ (User) ၏ သဘောတူညီချက် ရယူမည့် screen ပေါ်လာလိမ့်မည်။ ကျန်အဆင့်များကိုဆက်လက် မဆောင်ရွက်ခင် ၎င်း dialog box ပါ စာ (End User License Agreement) ကို အရင်ဖတ်ပါ။ ထို့နောက် အခမဲ့ မှတ်ပုံတင်ခြင်း (Free Registration) screen ပေါ်လာရန် Yes ကို နှိပ်ပါ။

အဆင့် 3: သင်၏ email လိပ်စာကို email လိပ်စာထည့်ရန် ပေးထားသော ကွက်လပ်၌ ဖြည့်ရန်မလိုပါ။ Soft ware တွင် ပါရှိသည့် အချက်အလက်များကို ရယူရန်သာ click လုပ်ပါ။
အချက်အလက်ရယူခြင်း လုပ်ငန်းပြီးဆုံးပါက သင်၏ Firewall Setupကို ထည့် ရမည့် Folder ရွေးချယ်ရန် ပေါ်လာလိမ့်မည်။

အဆင့် 4: ရွေးချယ်သည့် လမ်းကြောင်းရယူပြီးပါက Firewall လုံခြုံရေးအဆင့် ရွေးချယ်ခြင်း screen ပေါ်လာရန် click လုပ်ပါ။ ထို့နောက် ပုံပါအတိုင်း Firewall Only option ကို စစ်ဆေးပါ။



ပုံ 3: Firewall လုံခြုံရေးအဆင့် ရွေးချယ်ခြင်း screen ပုံ

Firewall လုံခြုံရေးအဆင့် ရွေးချယ်ခြင်း၏ အဓိပ္ပာယ်ဖွင့်ဆိုချက်

Firewall လုံခြုံရေး အဆင့်တစ်ခုစီတိုင်းသည် အသုံးပြုသူ (user) များကို အဆင့်အလိုက် အဆင်ပြေစေရန် စီမံဖြည့်စွမ်းပေးသည်။ Option တစ်ခုစီသည် သင် လက်ခံရရှိမည့် Security အချက်ပေးမှုများနှင့်တကွ အသုံးပြုရာ၌ ရှုပ်ထွေးမှုရှိသော အကာအကွယ် ပေးခြင်းများကို ညီမျှအောင် ဆောင်ရွက်ပေးသည်။ လုံခြုံရေး အဆင့် တစ်ခုစီ၏ အတိုချုပ် ဖော်ပြချက်ကို အောက်တွင် တွေ့ရှိရမည်။

Firewall သာ အသုံးပြုခြင်း

ဤရွေးချယ်မှုတွင် သင့်အား COMODO Firewall ကို ခုခံမှုအဆင့် တိုးမြှင့်ခြင်း (Defense⁺) မပါဘဲ အလုပ် လုပ်ပေးလိမ့်မည်။ ၎င်းသည် ကွန်ရက်ရှာဖွေမှုများ၊ (Web browsers) နှင့် Email အသုံးပြုသူများ၊ (Email Clients) ကဲ့သို့သော လုံခြုံမှု ရှိသည့် Applications များကို အဆင်သင့် ခွဲခြားပေးပြီး သင်လက်ခံရရှိမည့် လုံခြုံရေး အချက်ပေးမှုများ (Security Alerts) များကို လျှော့ချပေးသည်။ လုံခြုံရေး အချက်ပေး မှုများ ပေါ်ပေါက်ရသည့် အကြောင်းရင်းများကိုလည်း ရှင်းပြပေးသည်။ ခြုံငုံ၍ ကြည့်ပါက ဤအဆင့်တွင် ဆောင်ရွက်ရမည့် ကိစ္စများကို ရိုးရှင်းစွာ ပြုလုပ်သည်။

ပိုမိုမြင့်မားသော ခုခံမှုစွမ်းအားနှင့် Firewall အား အသုံးပြုခြင်း

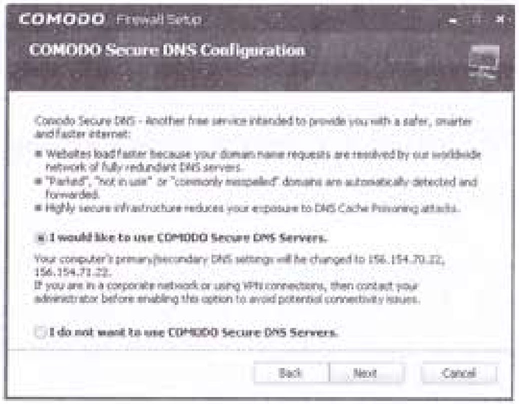
ဤအဆင့်သည် Firewall သာမက ခုခံမှုအဆင့် တိုးမြှင့်ခြင်း (Defense⁺) ကိုပါ ပေါင်းစပ်ထားသော ကာကွယ်မှု အပြည့်ပေးသည့် အဆင့်ဖြစ်သည်။ ခုခံမှုအဆင့်

တိုးမြှင့်ခြင်း (Defense⁺) သည် Firewall အသီးသီးအား ပိုင်းရုံတိုက်ခိုက်ရန် ဒီဇိုင်း ဆွဲထားသည့် malware များကို ကာကွယ်ပေးသည်။ COMODO Firewall အချက်ပေး မှုများ (Alerts) သည် application တစ်ခု သို့မဟုတ် request တစ်ခုတို့အား အဘယ် ကြောင့် ပိတ်ဆို့ရသည်ဆိုသည်ကိုလည်း ပို၍ တိကျလေးနက်သော ဖြေရှင်းချက်များ ပေးသည်။ ထို့အပြင် သံသယဖြစ်ဖွယ်ရှိသော File (သို့) Program တို့ကို 'sandboxing' လုပ်ခြင်းသော်လည်းကောင်း၊ သီးခြားဖယ်ရှားထားခြင်းသော် လည်းကောင်း ပြုလုပ်နိုင် သည်။

အမြင့်ဆုံး ခုခံစွမ်းအားနှင့် Firewall အား အသုံးပြုခြင်း

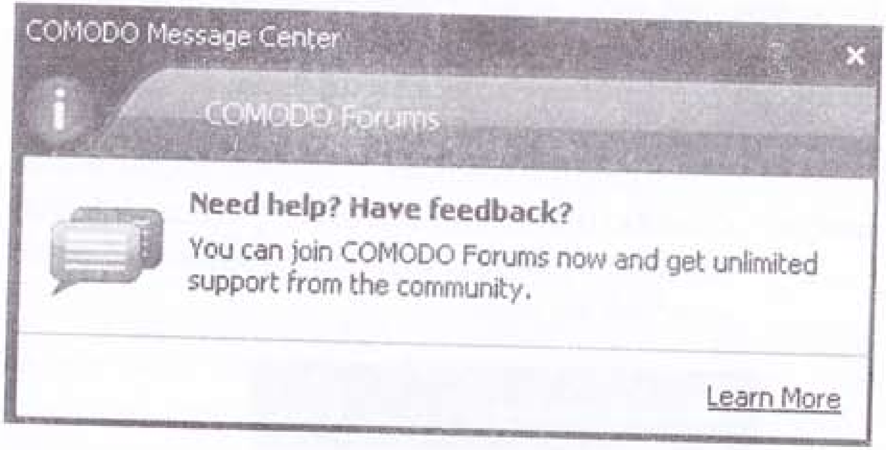
ဤအဆင့်တွင် အင်တာနက်ပေါ်သို့ စေလွှတ်ထားသော သင်၏ကွန်ပျူတာရှိ ports များ၏ အသေးစိတ် အချက်အလက်များကို နှောင့်ယှက်ခြင်းကဲ့သို့သော လုံခြုံရေး ခြိမ်းခြောက်မှု အများအပြား ဝင်ရောက်လာခြင်းကို ကာကွယ်ပေးသည်။ 'sandbox' သည် အလိုအလျောက်စနစ်ဖြင့် ဆောင်ရွက်ပြီးဖြစ်သည်။

အဆင့် 6: COMODO DNS Configuration screen ကို လုပ်ဆောင်ရန် နှိပ်ပါ။ DNS server ကို အသုံးပြုပါမည့်အကြောင်း Option ကို ဖွင့်ထားပုံကို အောက်တွင် တွေ့ရမည်။



ပုံ 4: COMODO secure DNS Cnfiguration screen ပုံ

DNS server အများစုသည် လုံခြုံမှု အပြည့်အဝရှိသည် မဆိုနိုင်သော်လည်း COMODO secure DNS server ကို အသုံးပြုခြင်းဖြင့် အကျိုးကျေးဇူးကို ပိုမိုရရှိနိုင်ပါသည်။ ၎င်းသည် သင်၏ ကွန်ပျူတာအား အန္တရာယ်ရှိသော site များသို့ အပိုင်းစီး (hijack) ပို့ဆောင်ခြင်းများအား ထပ်မံကာကွယ်ပေးသည်။ ထို့ပြင် COMODO နှင့် မှတ်ပုံတင်ထားသော websites များတွင် လုံခြုံလွယ်ကူသော လုပ်ဆောင်မှုပေးခြင်း။ Installiation လုပ်ငန်းစဉ်အတွင်း၌ လွယ်ကူစွာ ဆောင်ရွက်ပြီးစီးနိုင်ရန် အစိုးရ၏ ဝင်ရောက်စွက်ဖက်မှုများမှလည်း ကာကွယ်ပေးသည်။ ဥပမာအားဖြင့် URL လိပ်စာ တစ်ခုကို မတော်တဆ မှားယွင်းရိုက်မိပါက COMODO Secure DNS server များမှ message တစ်ခုကို ဖော်ပြလိမ့်မည်။



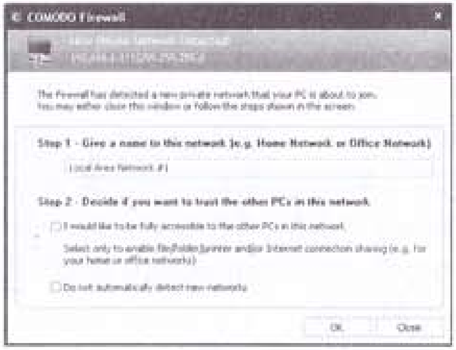
ပုံ 5: COMODO Secure DNS server သတိပေးချက်တစ်ခုပုံ

အဆင့် 7: COMODO Firewall အား Install လုပ်ရန် အသင့်အနေအထားရှိသော screen ဖွင့်ရန် နှိပ်ပါ။ COMODO Firewall အား Install လုပ်ပါ။ Installation လုပ်ငန်းစဉ် ပြီးစီးပါက COMODO Firewall Setup ပြီးစီးကြောင်း screen ပေါ်လာလိမ့်မည်။

အဆင့် 8: Done ကို နှိပ်ပါ။ အောက်ပါ dialog box ကို တွေ့ရမည်။

ပုံ 6: Firewall Installer ၏ အတည်ပြုသည့် dialog box ပုံ

အဆင့် 9: သင်၏ ကွန်ပျူတာကို restart လုပ်ပါ။ COMODO Firewall ထည့်သွင်း ခြင်း လုပ်ငန်းစဉ် ပြီးစီးပါပြီ။ သင်၏ ကွန်ပျူတာ restart လုပ်ပြီးပါက 'ကိုယ်ပိုင် ကွန်ရက်တစ်ခုကို ရှာဖွေတွေ့ရှိကြောင်း' screen ပေါ်လာ လိမ့်မည်။



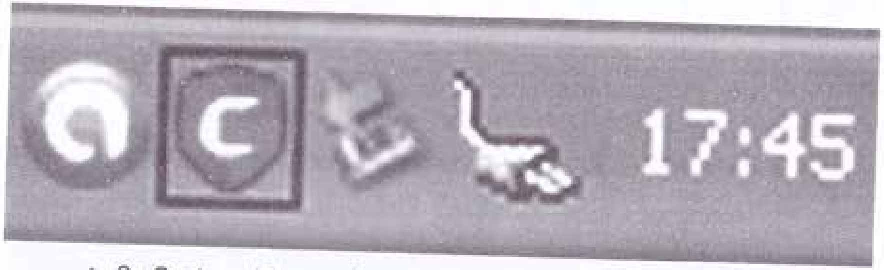
ပုံ 7: COMODO Firewall ကိုယ်ပိုင်ကွန်ရက် ရှာဖွေတွေ့ရှိမှု screen ပုံ

မှတ်ချက် ။ ။ သင်သည် အသေးစား network ဆက်သွယ်မှု ပတ်ဝန်းကျင်တွင် အလုပ်လုပ်နေပါက ၎င်း network ပေါ်ရှိ ကွန်ပျူတာများနှင့် မည်သည့် File, Folder နှင့် printer များကိုမဆို မျှဝေသုံးစွဲပိုင်ခွင့် အပြည့်အဝရရှိနိုင်အောင် အသေအချာ စစ်ဆေးရမည်။

အဆင့် 10: Network အမည် ရိုက်ရန်ကွက်လပ်တွင် သင်ရိုက်လိုသည့် အမည် ရိုက်နိုင်သကဲ့ ပုံ 7 တွင် ဖော်ပြထားသည့် default name ကိုလည်း ရယူနိုင်သည်။ အဆင့် ၂ တွင် ပါရှိသည့် Options များကို ချန်ခဲ့ပါ။ ဤ network ပေါ်ရှိ အခြားကွန်ပျူတာများကို ယုံကြည်မှု ရှိမရှိ 'un

checked' လုပ်ရန် ဆုံးဖြတ်ပါ။ Installation ကို အဆုံးသတ်ပါ။

COMODO Firewall ၏ desktop icon နှင့် connectivity icon နှစ်ခုတို့ ပုံ 7 နှင့် တစ်ပြိုင်တည်း desktop ပေါ်တွင် ပေါ်လာလိမ့်မည်။ Internet နှင့် သင် မဆက်သွယ်မီ 'connectivity' သည် System Tray ထဲတွင် ပေါ်လာလိမ့်မည်။



ပုံ 8: System Tray ထဲရှိ COMODO Firewall connectivity iconကို အမည်းရောင်မျဉ်းကြောင်းဖြင့် ဖော်ပြထားပုံ

Online တက်ခြင်း(သို့) Online နှင့် ဆက်စပ်နေသော Program များ အသုံးပြုခြင်း (ဥပမာ– ကွန်ရက်ရှာဖွေစက်များ) ဖြင့် သင်သည် desktop ပေါ်တွင် လိမ္မော်ရောင် (သို့) အစိမ်းရောင် မြားခေါင်းပုံသဏ္ဌာန် မီးလုံးများသည် အထက်မှအောက်၊ အောက်မှ အထက် လင်းချီ မှိတ်ချီ သွားလာနေသည်ကို တွေ့ရမည်ဖြစ်ပြီး ၎င်းသည် အဝင်နှင့် အထွက် connection requests များကို ပြသနေသည်ကို အောက်ဖော်ပြပါ ပုံတွင် တွေ့နိုင်သည်။

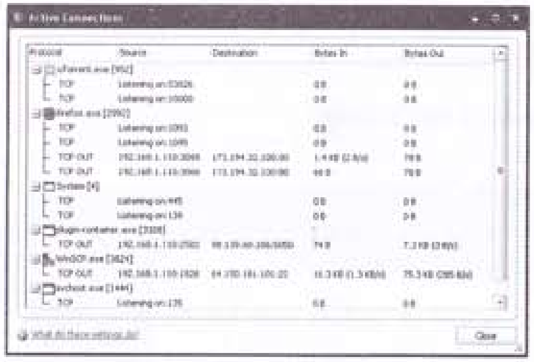
ပုံ 9: Connetivity icon အသက်ဝင်လှုပ်ရှားနေပုံ

COMODO Firewall ကိုအချိန်ခဏကြာ run ပြီးပါက COMODO သတင်းအချက်အလက်စင်တာမှ သတိပေးချက်တစ်ခု တက်လာလိမ့်မည်။

ပုံ 10: COMODO သတင်းအချက်အလက်စင်တာပုံ

မှတ်ချက် ။ ။ COMODO အဖွဲ့အစည်းထံသို့ ညွှန်ပြရန် ပို၍ များပြားသော Site များအကြောင်း သင်ယူမည့်အကြောင်း နိုင်ပါ။

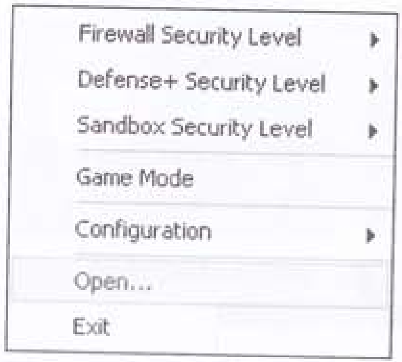
သတိပြုရန် ။ ။ System Tray ထဲရှိ 'connectivity icon' ကို ထောက်၍ Right-click လုပ်ပါ။ အောက်ဖော်ပြ pop - up menu များနှင့် ၎င်း၏ sub-menu များကို တွေ့ရမည်။



ပုံ 11: 'connectivity icon ' ကို ၎င်း၏ menu, sub-menu များနှင့် တွေ့ရပုံ

Connectivity icon ရှိ menu များသည် သင်အသုံးပြုနေသော COMODO Firewall ၏ ထုတ်ကုန်များကို ပြောင်းလဲခွင့်ပေးသည်။ Configuration item တစ်ခုကို ရွေးချယ်ခြင်းဖြင့် သင်၏ Configuration sub-menu များကိုပါ ရွေးချယ်သည့် လုပ်ဆောင်မှု ကိုပေးသည်။ Sub- menu များမှတစ်ဆင့် COMODO လုံခြုံရေးအဆင့်မြင့်မားသော level (သို့) 'sand boxing' အသုံးပြုနိုင်သော အင်တာနက်လုံခြုံရေးအဆင့်တို့ကို ရွေးချယ် နိုင်သည်။

အချုပ်အားဖြင့် product တစ်ခုစီတိုင်းကို 'connetivity' ရှိ 'pop-up' များမှ တစ်ဆင့် လုံခြုံရေးအဆင့်ကို ညှိနိုင်းဆောင် ရွက်ပေးနိုင်သည်။ ဤလုံခြုံရေးအဆင့်များနှင့် ပတ်သက်သော အသေးစိတ် အချက်အလက်များကို section 4.1 ၌ Firewall ၏ ပြုမူဆောင်ရွက်ပုံ window နှင့် section 4.2 ၌ ခုခံမှုအဆင့်မြှင့်ခြင်း (Defense') window တို့၌ ဆွေးနွေးတင်ပြထားသည်။



ပုံ 12: Connectivity icon ရှိ Firewall ၏ လုံခြုံရေးအဆင့် sub-menu ပုံ

COMODO Firewall အား အသုံးပြုပုံ

ဤစာမျက်နှာရှိ အပိုင်းကဏ္ဍများမှာ

3.0 - COMODO Firewall ကို အသုံးပြု၍ access များကို ခွင့်ပြုခြင်း၊ တားဆီးခြင်း တို့ ဆောင်ရွက်ပုံ

3.1 - COMODO Firewall ၏ အဓိက user interface ကို ဖွင့်ပုံ

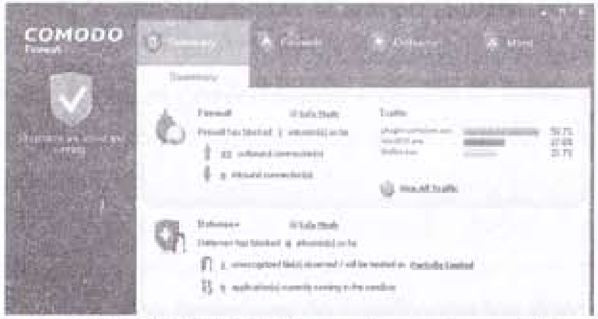
3.2 - COMODO Firewall ၏ user interface အား အထွေထွေ သုံးသပ်ချက်

3.0-COMODO Firewall ကို အသုံးပြု၍ access များကို ခွင့်ပြုခြင်း၊ တားဆီးခြင်းတို့ဆောင်ရွက်ပုံ

Firewall ဆိုသည်မှာ သင်၏ကွန်ပျူတာကို ထိခိုက်ပျက်စီးစေလိုသော ရည်ရွယ်ချက်ဖြင့် ချဉ်းကပ်လာသော hackers များနှင့် malware များကို ကာကွယ်ရန် စီစဉ်ဖန်တီးထားသည့် program တစ်ခုဖြစ်သည်။ ၎င်း hacker နှင့် malware နှစ်မျိုးစလုံးသည် သင်၏ ကွန်ပျူတာကို တိုက်ရိုက် access လုပ်ရန် ကြိုးပမ်းခြင်း (သို့)

သင်၏ ကွန်ပျူတာပေါ်ရှိ သတင်းအချက်အလက်များကို အခြားသော ထုတ်လုပ်သူ (third party) ဆီသို့ ပို့ဆောင်ခြင်းတို့ကို လုပ်ဆောင်သည်။ COMODO Firewall သည် သင်၏ system ကို လုံခြုံစိတ်ချမှု မရှိသော software နှင့် ဆိုးရွားသည့် process များမှ တောင်းဆိုချက် (request) များကို ပိတ်ပင်ပေးပြီး မည်သည့် တောင်းဆိုချက်သည် လုံခြုံမှုရှိပြီး အသုံးပြုရန် ခွင့်ပြုချက်ပေးသင့်ကြောင်းကို မှတ်သားထားရန်လည်း အတည်ပြုချက်ပေးရမည်။ မည်သည့် တောင်းဆိုချက်က တရားဝင်ဖြစ်ပြီး မည်သည်က ခြိမ်းခြောက်မှုများ ဖြစ်သည်ဆိုသည်မှာ အချိန်အနည်းငယ်ယူကာ ရရှိသည့် အတွေ့အကြုံမှ ဆုံးဖြတ်ပေးလိမ့်မည်။

COMODO Firewall သည် တောင်းဆိုချက်တစ်ခုကို ရရှိသည့်အကြိမ်တိုင်း သင်၏ system အား အင်တာနက်နှင့် access လုပ်သင့် မလုပ်သင့်ကို Firewall အချက်ပေးစနစ် pop-up မှ ချက်ချင်းအဖြေပေးလိမ့်မည်။ Firefox ကဲ့သို့သော လုံခြုံစိတ်ချရသည့် program များ ပါဝင်နေသည့် လေ့ကျင့်မှုများသည် Firewall အချက်ပေးစနစ်နှင့် ပို၍ ရင်းနှီးမှုရှိစေရန် ကူညီပေးပြီး အသုံးချပုံကိုလည်း သိရှိစေနိုင်သည်။ တစ်ခါတစ်ရံ အများသုံးအဖြစ် လက်ခံထားသော browser နှင့် email program များမှ တောင်းဆိုချက်များကို ခွင့်ချက်ထားသော်လည်း ဆက်သွယ်မှုတောင်းဆိုချက် တစ်ကြိမ်ပြုလုပ်တိုင်း Firewall အချက်ပေးစနစ်သည် အောက်ပါအတိုင်း ထွက်ပေါ်လာလိမ့်မည်။



ပုံ 1: COMODO Firewall အချက်ပေးစနစ် ဥပမာပြပုံ

Firewall ဆိုသည်မှာ သင်၏ system မှ အတွင်းအပြင် သွားလာဆက်သွယ်မှုများကို စောင့်ကြည့်ရန် ရိုးရှင်းစွာ ချမှတ်ထားသော စည်းကမ်းချက်တစ်ခု ဖြစ်သည်။ Network မှ ဆက်သွယ်မှုတစ်ခုကို သင်ပြုလုပ်တိုင်း ၎င်း process (သို့) program တို့အတွက် စည်းမျဉ်းတစ်ခုကို COMODO Firewall က ချမှတ်ပေးသည်။ COMO-

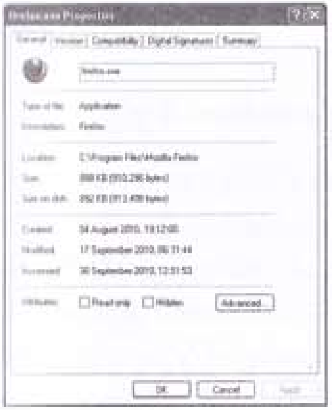
DO Firewall သည် ၎င်း မှတ်သားထားခြင်းမရှိသော (သို့) အသစ်ဖြစ်သော process (သို့) program တို့အတွက်လည်းကောင်း။ Defense+– Tasks> Computer Security Policy window အတွင်းရှိ ယုံကြည်စိတ်ချရသော software ရောင်းချသူ များ၏ စာရင်းပြုစုချက်များကိုလည်းကောင်း အထက်ပါအတိုင်း စည်းကမ်း သတ်မှတ် ချက်များ ပြုလုပ်သည်။

Remember my answer option ကို COMODO Firewall မှ program တစ်ခုအား access လုပ်ရာတွင် သင့်အနေဖြင့် ခွင့်ပြုမှု (သို့) ပိတ်ဆို့မှု ပြုလုပ်ထားသည်ကို မှတ်သားထားရန် အသုံးပြုသည်။ COMODO Firewall သည် သင်၏ ယခု ရွေးချယ်မှုကို အခြေခံ၍ နောက်တစ်ကြိမ် ၎င်း program သင်၏ ကွန်ပျူတာနှင့် ဆက်သွယ်မှုရှိလာပါက ခွင့်ပြုမှု (သို့) ပိတ်ဆို့မှုတို့ကို အလိုအလျောက် ပြုလုပ်ပေးလိမ့်မည်။

သတိပေးချက် ။ ။ သင်သည် COMODO Firewall အား စတင်အသုံးပြုချိန်တွင် 'Remember my answer' option အား မပိတ်မိစေရန် တင်းကျပ်စွာ သတိ ပေးအပ်ပါသည်။ မတူညီသော ဆက်သွယ်မှု တောင်းဆိုချက်များကို ခွင့်ပြုမည် (သို့) ပိတ်ဆို့မည်ကို ဆုံးဖြတ်ပါ။ ထို့နောက် ဆုံးဖြတ်ချက်သည် သင်၏ system လုပ်ဆောင်မှုအပေါ်၌ မည်သို့မည်ပုံအကျိုးသက်ရောက်မှုရှိသည်ကို လေ့လာပါ။ သင်၏ ဆုံးဖြတ်ချက် လုံးဝ သေချာပြီဆိုမှသာ 'Remember my answer' option ကို ဖွင့်ပါ။

မှတ်ချက် ။ ။ သင်၏ system အား access လုပ်ရာ၌ ကန့်သတ်ချက်ကို တင်းကြပ်စွာ ချမှတ်ထားခြင်းသည် သင်၏ ကွန်ပျူတာလုံခြုံရေးအတွက် အကောင်းဆုံး ချဉ်းကပ်မှု ဖြစ်သည်။ သံသယဖြစ်ဖွယ်ရှိသော၊ သက်သေအထောက်အထား မခိုင်လုံသော တောင်းဆိုချက်များအား ပိတ်ဆို့ရန် ဝန်မလေးပါနှင့်။ ၎င်းသည် သာမာန် program တစ်ခုအား မှန်မှန်ကန်ကန် အလုပ်လုပ်ခြင်းမှ ရပ်ဆိုင်းစေပါက နောက်တစ်ကြိမ် Firewall အချက်ပေးချက်ကို သင်ရရှိသည့်အခါ ထို process ကို လုပ်ဆောင်ရန် ခွင့်ပေးနိုင်သည်။

အဆင့် 1: program နှင့် process များမှ တောင်းဆိုချက်များအကြောင်းကို ပိုမိုလေ့လာရန် Firefox ၏ properties ကို Click လုပ်ပါ။



ပုံ 2: Firefox . exe ၏ properties ပုံ

အဆင့် 2: Properties screen ကို ပိတ်ပါ။

အဆင့် 3: Properties screen တွင် ဖော်ပြထားသော အချက်အလက်ပေါ်တွင် အခြေခံ၍ တောင်းဆိုချက်တစ်ခုသည် သေချာမှု (သို့) လုံခြုံမှုမရှိဟု သင်ယူဆပါက သင်၏ system ပေါ်တွင် access မလုပ်နိုင်ရန် COMODO Firewall မှ တစ်ဆင့် ငြင်းဆိုပါ။ သို့မဟုတ် program သည် တရားဝင်ပြီး အန္တရာယ် မပေးနိုင်သော တောင်းဆိုချက်ဖြစ်ပါက system နှင့် access လုပ်ရန် ခွင့်ပြုပါ။

အဆင့် 4: COMODO Firewall မှ တစ်ဆင့် Firefox ကို access လုပ်ရန် Click လုပ်ပါ။

အဆင့် 5: Firefox သည် လုံခြုံမှုရှိသော program ဖြစ်သောကြောင့် COMODO Firewall က ၎င်း program နောက်တစ်ကြိမ် သင်၏ system နှင့် access လုပ်သည့်အခါတွင် အလိုအလျောက်လုပ်ရန် ခွင့်ပြုချက် ပေး မပေးကို စစ်ဆေးပါ။

မှတ်ချက် ။ ။ ခွင့်ပြုပေးမည့် ခလုတ်သည် process (သို့) program တစ်ခုအား access လုပ်ရာ၌ အဆင့်တစ်ဆင့်ချင်းစီ လမ်းညွှန် လုပ်ဆောင်ခွင့်ပြုသည်။

မှတ်သားရန် ။ ။ COMODO Firewall ၏ help files ကို Online မှ တစ်ဆင့် access လုပ်ရန် Click ပါ။

COMODO Firewall ကို အသုံးပြု၍ ရရှိသော အတွေ့အကြုံနှင့် ယုံကြည်စိတ်ချမှုတို့က ခွင့်ပြုခြင်း (သို့) ပိတ်ဆို့ခြင်း ရွေးချယ်မှုတို့ကို မှန်မှန်ကန်ကန် လုပ်ဆောင်နိုင်သည့် စွမ်းရည်ကို တိုးတက်စေသည်။

3.1- COMODO Firewall ၏ အဓိက User interface ကို ဖွင့်ပုံ

သင်၏ ကွန်ပျူတာတွင် ထည့်သွင်းထားသော COMODO Firewall သည် system ကို Restart လုပ်ပြီးနောက် အလိုအလျောက် စတင်အလုပ်လုပ်သည်။ ၎င်းတွင် Control Panel အပိုတစ်ခုပါပြီး များစွာသော ဖွဲ့စည်းပုံနှင့် အသုံးချပုံများ ပါဝင်သည်။ စတင်အသုံးပြုသူ (Beginner level) များသည် COMODO Firewall လုံခြုံရေးစနစ်ကို မည်သို့ အသုံးချရမည်ကို လျင်မြန်စွာ သင်ယူနိုင်သည်။ အတွေ့အကြုံရှိသူ (Experienced) နှင့် အဆင့်မြင့် (Advance) user များမှာ Firewall ၏ ပိုမိုရှုပ်ထွေးသော စီစဉ်ဆောင်ရွက်မှုများကို လေ့လာသင်ယူရမည်။

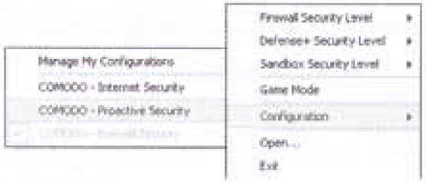
မှတ်ချက် ။ ။ ယခုဖော်ပြထားသည့် ဥပမာများအားလုံးသည် COMODO Firwall ရှိ Optimum Defense mode ကို အခြေခံထားသည်။ ဆိုလိုသည်မှာ ကျူးကျော်မှုများမှ ခုခံကာကွယ်ပေးသော Defense+ system အား အလိုအလျောက် ဖွင့်ထားပြီး ဖြစ်သည်။ အကယ်၍ သင်သည် COMODO Firewall ထည့်သွင်းရာ၌ Firewall only option ကို ရွေးချယ်ခဲ့ပါက Defense+ အား ဖွင့်ထားနိုင်မည် မဟုတ်ပေ။

COMODO Firewall ၏ အဓိက User Interface ကို ဖွင့်ရန် အောက်ပါအဆင့်များကို ဆောင်ရွက်ရမည်။

အဆင့် 1: Start> Programs> Comodo> Firewall> Comodo Firewall ကို ရွေးပါ။

သတိပြုရန် ။ ။ နောက်တစ်မျိုးအနေဖြင့် သင်သည် desktop ပေါ်ရှိ COMODO Firewall icon ကိုသော်လည်းကောင်း၊ System Tray အတွင်းရှိ icon ကိုသော်လည်းကောင်း၊ Double click လုပ်ခြင်းဖြင့် user interfaceကို ဖွင့်နိုင်သည်။ ထပ်မံ၍ COMODO Firewall icon ကို right- click လုပ်ခြင်းဖြင့် ၎င်း၏ pop-up menu ကို တွေ့နိုင်သည်။ ထို့နောက် အောက်ပါအတိုင်း Open ကိုရွေးပါ။

ပုံ 3: COMODO Firewall connectivity pop-up menu ပြပုံ



ပုံ 4:COMODO Firewall ၏ user interface ကို အကျဉ်းချုံးထားပုံ

3.2- COMODO Firewall ၏ အဓိက user interface အား အထွေထွေ သုံးသပ်ချက်

COMODO Firewall သည် ၎င်းထံသို့ ချဉ်းကပ်လာသော processes နှင့် programs တို့၏ အတွင်းအပြင် တောင်းဆိုချက်များ၏ အသေးစိတ် အချက်အလက်များကို ရှင်းလင်း ပြည့်စုံစွာ ဖော်ပြပေးသည်။ အတွင်းဘက်ထက် အပြင်ဘက်မှ တောင်းဆိုချက်က ပိုများသည့် သဘောရှိသည်။ Safe mode ကို default လုပ်ထားပြီး အခြားသော operating modes များကိုလည်း ဤအပိုင်းတွင် ဖော်ပြသွားမည်။ အတွင်းအပြင် သွားလာဆက်သွယ်မှုများက အမျိုးမျိုးသော process နှင့် program တို့၏ ဆောင်ရွက်ချက်များကို ပြသပေးသည်။ တောင်းဆိုမှုများ၏ အရေအတွက်ကိုလည်း ရာခိုင်နှုန်းဖြင့် ပြသည်။

အချိန်ခဏတာအတွင်း အပြင်ဘက်မှ တောင်းဆိုမှု (outbond requests) များ၏ သက်ဆိုင်ရာ အသေးစိတ် အချက်များကို ကြည့်ရန် Click လုပ်ပါ။

ပုံ 5: **အင်တာနက် ဆယ်သွယ်လှုပ်ရှားသွားလာမှုများ၏ အသေးစိတ်အချက်အလက်များကို ပြသနေသော သက်ဝင်လှုပ်ရှား** (Active Connection) **တစ်ခုပုံ**

Active Connections window ကို အဝင်ဘက် တောင်းဆိုချက် (inbound requests) များအတွက် ဆောင်ရွက်ရန် Click လုပ်ပါ။

သတိပြုရန်အချက် ။ ။ အကယ်၍ သင်သည် သံသယရှိသော ဖျက်ဆီးရေး process (သို့) program တစ်ခုခုတို့မှ ၎င်းတို့ကိုယ်တိုင် operation ၌ download လုပ်ခြင်း၊ သင်၏ အင်တာနက် ဝန်ဆောင်မှုသည် ရုတ်တရက်ကျသွားခြင်းတို့ ဖြစ်ပါက အတွင်းအပြင် တောင်းဆိုချက် အားလုံးကိုရပ်ရန် Click လုပ်ပါ။ ထိုသို့ ရုတ်တရက် ရပ်လိုက်ခြင်းသည် Firewall mode မှ Safe mode ကို ပြောင်းပေးသည်။ ပြဿနာ၏ ဖြစ်နိုင်ခြေရှိသော အရင်းအမြစ်ကို ခွဲခြားရန် Active Connections window ရှိ အသေးစိတ် အချက်အလက်များ၌ ပြန်ကြည့်ပါ။ သင်သည် ဤပြဿနာကို အောင်မြင်စွာ ဖြေရှင်းပြီးကြောင်း သေချာပါက အတွင်းအပြင် တောင်းဆိုချက်များ လုပ်ငန်းစဉ်ကို ပြန်စရန် Click လုပ်ပါ။ COMODO Firewall ၏ မူလအခြေအနေသို့ ပြန်၍သွားပါ။

3.2.1 COMODO Firewall ၏ အခြေအနေပြ icon ပုံ

COMODO Firewall နှင့် Defense+ တို့သည် အတူတကွ အလုပ်လုပ်ကြသည်။ ထိုသို့ နှစ်ခုစလုံး အလုပ်လုပ်နေချိန်၌ အဓိက user interface ၏ ဘယ်ဘက်၌ရှိသော ညွှန်ပြချက် အောက်ပါအတိုင်း ပေါ်လာလိမ့်မည်။

ပုံ 6: အစိမ်းရောင် COMODO Firewall အခြေအနေပြ icon ပုံ

အကယ်၍ ၎င်း program နှစ်ခုလုံးကို ပိတ်ထား (disabled) ပါက အခြေအနေပြ icon သည် မည်သည့် Firewall နှင့် ကာကွယ်မှုပေးသည့် အစိတ်အပိုင်းကိုမဆို ပိတ်ထားကြောင်း ဖော်ပြလိမ့်မည်။

ပုံ 7: COMODO Firewall ကို ပိတ်ထားသည့် အခြေအနေပြ အဝါရောင် icon ပုံ

programs နှစ်ခုစလုံးကို disabled လုပ်ထားသော်လည်း အခြေအနေပြ iconကို အောက်ပါအတိုင်း တွေ့ရမည်။

ပုံ 8: COMODO Firewall ၏ စွယ်စုံကာကွယ်မှုကို ပိတ်ထားသည့် အခြေအနေပြအဝါရောင် icon

သက်ဆိုင်ရာ ခုခံကာကွယ်မှုများကို ရရှိရန် program နှစ်ခုလုံးအား enabled ပြန်လုပ်ပါ။

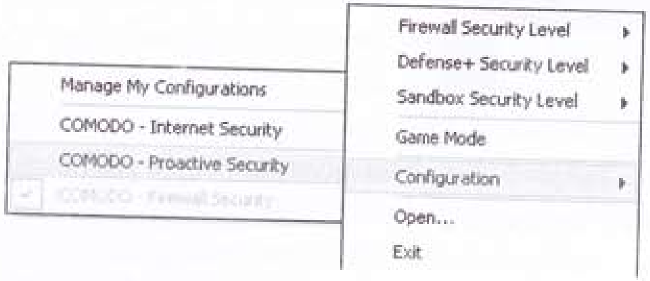
အဆင့်မြင့်ပုံဖော်ခြင်း (configurations) နှင့် ပြင်ဆင်ခြင်း (settings) များ

ဤစာမျက်နှာရှိ အပိုင်းကဏ္ဍများမှာ

- 4.0 Firewall နှင့် Defense+ တို့အား Access လုပ်ပုံ
- 4.1 Firewall ၏ ဆောင်ရွက်ချက်ပြ Settings များ
- 4.2 Defense+ ၏ Settings များ

4.0 Firewall နှင့် Defense⁺ တို့အား Access လုပ်ပုံ

COMODO Firewall ၏ အဓိက User Interface ကို Firewall နှင့် Defense⁺ ဟူ၍ နှစ်လွှာခွဲထားသည်။



ပုံ 1: Firewall နှင့် Defense⁺ နှစ်လွှာစလုံးကို ဖော်ပြထားသော COMODO Firewall ၏ အဓိက User Inter-face

Firewall နှင့် Defense⁺ တို့၏ Settings များတွင် တွဲဖက်ပါဝင်သည့် windows နှင့် ခလုတ်များ (Tabs) ကို အသုံးပြုနိုင်ရန် ၎င်း Settings နှစ်ခုအား Click လုပ်ခြင်းဖြင့် Access လုပ်နိုင်သည်။

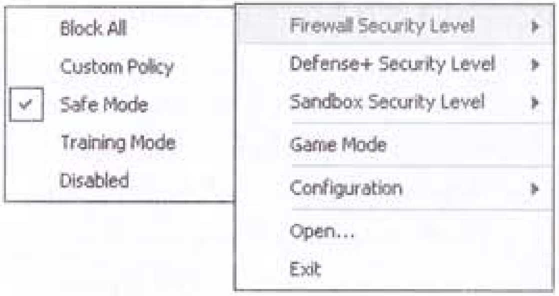
အောက်ဖော်ပြပါ အဆင့်များကို ဆောင်ရွက်ခြင်းဖြင့် သင်သည် အဆိုပါ Settings နှစ်ခုစလုံးကို တစ်လှည့်စီ Access လုပ်နိုင်သည်။

အဆင့် 1: COMODO Firewall ၏ အဓိက User Interface ကို ဖွင့်ပါ။

အဆင့် 2: Firewall (သို့) Defense⁺ ၏ Tasks panes များကို လုပ်ဆောင်ရန် Click လုပ်ပါ။

အဆင့် 3: Firewall (သို့မဟုတ်) Defense⁺ တို့၏ Settings Tab များကို ဖွင့်ရန် Click လုပ်ပါ။

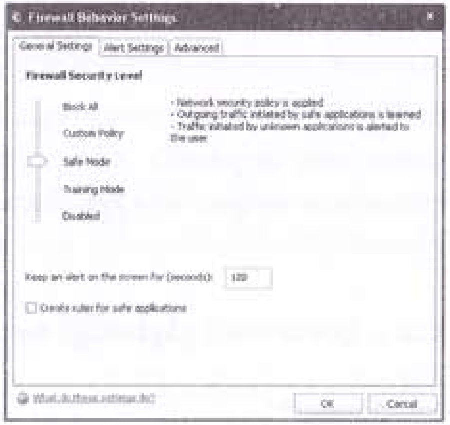
သတိပြုရန် ။ ။ System Tray ထဲတွင်ရှိသော connectivity icon ကို အသုံးပြု၍ အောက်တွင်ဖော်ပြထားသော အပိုင်းအသီးသီးရှိ Firewall လုံခြုံရေးအဆင့်၊ ခုခံမှုအဆင့်တိုးမြှင့်ခြင်း လုံခြုံရေးအဆင့်နှင့် Sandbox လုံခြုံရေးအဆင့်တို့ကို လွယ်ကူအကျိုးရှိစွာ အသုံးချနိုင်သည်။ အောက်ပါအတိုင်း pop-up menu နှင့် sub-menu များကို အလုပ်လုပ်ဆောင်ရန် 'connectivity icon' ကို Right click လုပ်ပါ။



ပုံ 2: Connectivity icon ၏ pop-up menu နှင့် Firewall လုံခြုံရေးအဆင့်၏ sub-menu ပြပုံ

4.1 Firewall ၏ ဆောင်ရွက်ချက်ပြ Settings များ

Firewall ၏ ဆောင်ရွက်ချက်ပြ Settings များသည် Firewall လုံခြုံရေးအဆင့်တစ်ခုလုံးကို ၎င်းတွင်ပါဝင်သော ပုံစံနှင့် အသုံးချနည်းလမ်းများဖြင့် ခွဲခြမ်းစိတ်ဖြာဆောင်ရွက်နိုင်သည်။ Firewall settings များတွင် Firewall လုံခြုံရေးအဆင့်၊ လက်ခံရရှိသော လုံခြုံရေး အချက်ပေးမှုများ (security alerts) ၏ အမျိုးအစားနှင့် အရေအတွက်၊ အချက်အလက်များ ပါဝင်သော packet များကို ကြည့်ရှုစစ်ဆေးခြင်းတို့လည်း ပါဝင်သည်။



ပုံ 3: Firewall ၏ ဆောင်ရွက်ချက်ပြ Settings မှ အထွေထွေလုပ်ဆောင်မှုခလုတ် (General Settings tab)

General Settings tab သည် COMODO Firewall အတွက် မည်သည့်

လုံခြုံရေးအဆင့်က သင့်လျော်သည်ကို သင့်အား ခွဲခြားဆုံးဖြတ်စေသည်။ Sliderသည် အောက်ပါ option များအကြား လုံခြုံရေး level များကို ရွှေ့လျားညှိနှိုင်းပေးသည်။

အလုံးစုံ ပိတ်ဆို့ခြင်း (Block All) : ဤ အဆင့်သည် အင်တာနက်နှင့် ဆက်သွယ်သော သွားလာမှု (Traffic) ကိုရပ်တန့်စေပြီး သင်ခွဲခြားစိစစ်ထားသော မည်သည့် Firewall ၏ ခန့်မှန်းချက်နှင့် စည်းကမ်းချက်များကိုမဆို တားဆီးသည်။ ထို့အပြင် ၎င်းသည် အလုပ်လုပ်ဆောင်သည့် applications များအတွက် အသွားအလာ စည်းမျဉ်း (Traffic Rules) ကိုလည်း ထုတ်မပေးတော့ဘဲ ၎င်း applications တို့၏ ပြုမူဆောင်ရွက် ပုံများကို ကူးယူခြင်း၊ လေ့လာခြင်းလည်း မရှိတော့ပေ။

ကုန်ပစ္စည်းဆိုင်ရာ မူဝါဒ (Custom Policy) : ဤ အဆင့်တွင် သင် မူလ ရွေးချယ်ထားသော Firewall Tasks အတွင်းရှိ Network လုံခြုံရေးမူဝါဒနှင့် Defense⁺ Tasks အတွင်းရှိ ကွန်ပျူတာ လုံခြုံရေးမူဝါဒများကိုသာ သုံးစွဲသူ ရွေးချယ်မှု (User - defined) ဖြစ်သော COMODO Firewall လုံခြုံရေးမူဝါဒနှင့် ကွန်ရက်သွားလာမှုမူဝါဒ (network traffic policy) များအဖြစ် အသုံးချသည်။

Saft mode : Safe mode သည် Optimum Proactive Defense နှင့် Maximum Proactive Defense တို့၏ ထည့်သွင်းခြင်း (installations) များပါဝင်သော COMODO Firewall ၏ default setting ဖြစ်သည်။

အသုံးချအချက်အလက် ။ ။ COMODO Firewall သည် pop-up အချက်ပေးချက်များမရရှိဘဲ လုံခြုံစိတ်ချရသည်ဟု ခွဲခြားထားသည့် အသုံးပြုနေကျ app-lications နှင့် files များ၏ အတွင်းဘက် အစီအစဉ်များကို ပြုပြင်ပေးသည်။

သတိပြုရန် ။ ။ (Training mode) နှင့် (Disabled mode) တို့သည် သင့် system အား အဖျက်အစီး ဝင်ရောက်ခြင်းမှ ကာကွယ်မပေးဘဲ COMODO Firewallအား အကျိုးဆက်များ ဖြစ်ပေါ်စေသဖြင့် ၎င်း mode နှစ်ခုစလုံးကို ရွေးချယ်ရန် မထောက်ခံပါ။

4.2 : (Defense⁺) ခုခံမှုအဆင့်မြင့် Settings များ

မှတ်ချက် ။ ။ ဤအပိုင်းတွင်ပါဝင်သောပုံစံနှင့် အသုံးချနည်းလမ်းများ လုပ်ဆောင်ရန် Firewall နှင့် ၎င်း၏ လုံခြုံရေးလုပ်ထုံးများကို ကြိုတင်နားလည်ရန် လိုအပ်သည်။ ဤအပိုင်းကို အဆင့်မြင့် အသုံးပြုသူများ (Advanced users) အတွက် ကျယ်ပြန့်စွာ စီစဉ် ဖန်တီးထားသည်။

အရေးကြီး ။ ။ COMODO Firewall အား install လုပ်သည့်အချိန်တွင် Optimum proactive Defense နှင့် Maximum Proactive Defense options များကို စစ်ဆေး ကြည့်ပါက ကျူးကျော်ဝင်ရောက်မှုများကို ကာကွယ်ပေးသည့် Defense⁺ ၏ system သည် အလိုအလျောက် ဖွင့်ထား (enabled) ပြီး ဖြစ်လိမ့်မည်။ သို့သော်လည်း သင်သည် Firewall Only option ကို စစ်ဆေးကြည့်ပါက Defense⁺ system ကို လမ်းညွှန်နည်းလမ်းအတိုင်း ဖွင့်ပေးသည်ကို တွေ့ရမည်။ Defense⁺ option ကို အလုပ်လုပ်ရန် စုစည်းထားသော သတင်းအချက်အလက်များစွာအတွက် enabled လုပ်ပေးရမည်။

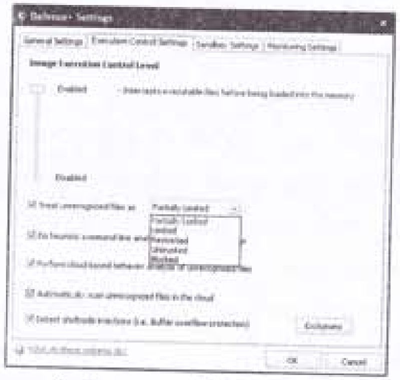
COMODO Firewall Defense⁺ သည် ကျူးကျော်ဝင်ရောက်မှုများကို ကာကွယ်ပေးသည့် system တစ်ခုဖြစ်သည်။ Network တစ်ခုနှင့် ဆက်သွယ်ထားသော မည်သည့် ကွန်ပျူတာမဆို နည်းပညာအားဖြင့် စကားပြောသည် (သို့) သက်ဝင်လှုပ်ရှားသည်ဟု ဆိုနိုင်သည်။ Defense⁺ system သည် သင်၏ ကွန်ပျူတာပေါ်သို့ ရောက်ရှိနေသော ဆောင်ရွက်ရန် အသင့်ရှိသည့် files များ၏ လုပ်ဆောင်မှုများကို မျက်ခြေမပြတ် ကြည့်ရှုစစ်ဆေးရမည်။ ဆောင်ရွက်ရန် အသင့်ရှိသည့် files ဆိုသည်မှာ သီးခြားစီမဟုတ်ဘဲ ၎င်းတို့၏ ဝိသေသ လက္ခဏာများ ဥပမာ– (.bat, .exe, .dll, .sys....etc) စသည်ဖြင့် file extension များတွဲလျက် ဖော်ပြထားသော application (သို့) program (သို့) ၎င်းတို့၏ တစ်စိတ်တစ်ပိုင်း ဖြစ်သည်။

အမျိုးအမည်မသိသော File တစ်ခု အလုပ်လုပ်ရန် ရောက်ရှိလာတိုင်း Defense⁺ မှ အချက်ပေး pop-up ထွက်ပေါ်လာလိမ့်မည်။ ထို pop-up မှ သင့်အား အလုပ်လုပ်ခြင်းကို ပိတ်ပင်သင့်၊ မပိတ်ပင်သင့်ကို တိုက်တွန်းလိမ့်မည်။ သင်၏ ခွင့်ပြုချက်(သို့) သိရှိခြင်းမရှိဘဲ သင်၏ ကွန်ပျူတာကို အပိုင်စီး၍ malware နှင့် spam များ ပြန့်ပွားစေခြင်း၊ သင်၏ hard disk ကို format ပြန်လုပ်ခြင်း၊ သင်၏ ကိုယ်ရေးကိုယ်တာ သတင်းအချက်အလက်များ ခိုးယူခြင်း၊ malware များအား applications (သို့) programs များ ပျက်စီးစေရန် ဝင်ရောက်စေခြင်းကဲ့သို့ အရေးကြီး အခြေအနေများကိုလည်း ပြသပေးသည်။

4.2.1 ခုခံမှုအဆင့်မြင့် (Defense⁺) Settings များ - အထွေထွေလုပ်ဆောင်မှု ခလုတ် (General Settings tab)

Defense⁺ system နှင့် Defense⁺ settings တို့ကို enable လုပ်ရန် အောက်ပါ အဆင့်များကို ဆောင်ရွက်ရမည်။

အဆင့် 1: COMODO Firewall ၏ အဓိက User Interface ရှိ Defense⁺ ကို Click လုပ်ပါ။ ထို့နောက် အောက်ပါ screen ကို အလုပ်လုပ်ရန် Click လုပ်ပါ။



ပုံ 6: General Settings tab အား ဖော်ပြထားသော Defense⁺ window ပုံ

အဆင့် 2: အထက်ပါ ပုံ 6 တွင် ဖော်ပြထားသည့်အတိုင်း Slider ကို အပေါ်သို့ ရွှေ၍ Saft mode သို့ ပြောင်းပါ။ Defense⁺ system ကို enable လုပ်ပါ။

Defense⁺ Security level နှင့် Firewall Behavior Security level တွင် ပါဝင်သည့် အသုံးချ options များမှာ အတူတူပင်ဖြစ်ကြပြီး သင်၏system အတွက် ကျူးကျော်မှုများကာကွယ်မည့် ပိုမိုမြင့်မားသောအဆင့် (level) ကို ရွေးချယ်ရန် slider ကို အသုံးပြုခွင့်ပေးသည်။

Paranoid Mode : ဤ အဆင့်သည် အမြင့်ဆုံးလုံခြုံရေးစနစ်ကို ပေးနိုင်သည့် level ဖြစ်ပြီး စိတ်ချယုံကြည်ရသော Software ကုန်ပစ္စည်းများစာရင်း (Trusted Software Vendor List) တွင် ပါဝင်သော File များမှတစ်ပါး မည်သည့် အမျိုးအမည် မသိ File ကိုမဆို ကြည့်ရှုစစ်ဆေးသည်။ ၎င်းသည် လုံခြုံရေးအချက်ပေးမှု အများဆုံး ထုတ်ပေးပြီး System ၏ လုပ်ငန်းဆောင်ရွက်မှုကိုလည်း Configuration Settings

မှတစ်ဆင့် စိစစ်ဖြတ်သန်းစေသည်။

Safe Mode : ဤ အဆင့်တွင် အမျိုးအမည်မသိ application တို့၏ အလုပ်လုပ်ဆောင်ပုံကို အလိုအလျောက် လေ့လာကာ System ၏ လုပ်ဆောင်ချက် အမှားများကို ရှာဖွေကြည့်ရှုသည်။ သေချာရေရာခြင်း မရှိသည့် Application များ အလုပ်လုပ်သည့် အခါတိုင်း လုံခြုံရေးအချက်ပေးမှုပေါ်ထွက်လာသည်။ ဤအဆင့်ကို Users အများစု အသုံးချရန် လမ်းညွှန်ထားသည်။

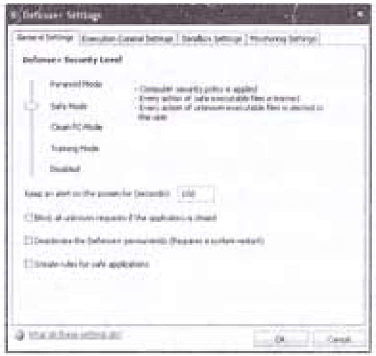
သင်၏ ကွန်ပျူတာ လုံခြုံရေးမူဝါဒနှင့် မကိုက်ညီသော အမည်မသိ applications နှင့် programs များ၏ တောင်းဆိုချက်များအားလုံးကို အလိုအလျောက် ပိတ်ပေးသည်။

Defense⁺ ၏ လုပ်ဆောင်မှုကို တရားဝင်ရပ်စဲခြင်း (Deactivate the Defense⁺) option သည် ကျူးကျော်ဝင်ရောက်မှု ကာကွယ်ရေး Defense⁺ systemကို လမ်းညွှန်ချက်အတိုင်း လုပ်ဆောင်၍ ရပ်စဲရန် ခွင့်ပေးသည်။ System ကို restart လုပ်ရန် လိုအပ်သည်။ သို့သော် ဤ option ကို မသုံးရန် တားမြစ်ထားသည်။

4.2.2 ခုခံမှုအဆင့်မြင့် (Defense⁺ Settings) - ထိန်းချုပ်မှု စီမံဆောင်ရွက်ခြင်းခလုတ် (Execution Control Settings tab)

Execution Control Settings tab သည် သံသယဖြစ်ဖွယ်ရှိသော (သို့) အမည်မသိသော file တစ်ခုက သင်၏ system အရင်းအမြစ်များကို ကိုယ်တိုင်ဝင်ရောက် access လုပ်ကာ ချဲ့ထွင်ခြင်းကို ကန့်သတ်ထားသည်။ ထို့နောက် ၎င်း file များကို ခွဲခြမ်းစိတ်ဖြာရန် တင်ပြပေးသည်။

ပုံ 7: Defense+ Execution Control Settings tab ပုံ



သတိပြုရန် ။ ။ အဆင့်မြင့် Users များသည် ကန့်သတ်အလွှာ (Exclusions pane) ကို click လုပ်ခြင်းဖြင့်လည်းကောင်း၊ ရှေ့တွင် ဖော်ပြထားသော တာဝန်များကို သီးခြားကန့်သတ်မှု ပြုလုပ်နိုင်သည်။ အမျိုးမျိုးသော processes (သို့) programs များကို ရှာဖွေရွေးချယ် ၍သော်လည်းကောင်း။

မှတ်ချက် ။ ။ အတွေ့အကြုံရှိ အဆင့်မြင့် Users များသည် Momtoring Settings tabs, Sandbox Settings နှင့် Execution Control Settings များနှင့် သက်ဆိုင်သော online အကူအညီ (Help) ကို COMODO မှ ရယူ access လုပ်ရန် တိုက်တွန်းအားပေးထားသည်။ Http://help.comodo.com/ topic -72-1-155-1074-Introduction-to-Comodo-Internet-Security.html လိပ်စာကိုသွား၍ online မှတစ်ဆင့် အကူအညီပေးနိုင်သည့် ခေါင်းစဉ်များစာရင်းမှ ရွေးချယ်နိုင်သည်။

F AQ and Review (မကြာခဏမေးလေ့ရှိသော မေးခွန်းများနှင့် သုံးသပ်ချက်)

5.0 မူဟာင်းနှင့် ဆယ်လီမတို့ နှစ်ဦးစလုံးသည် COMODO Firewall ၏ အလုပ်လုပ်ပုံ အဆင်ပြေချောမွေ့ခြင်းနှင့် အသုံးပြုရ လွယ်ကူခြင်းတို့ကြောင့် အထူးပင် ကျေနပ်သဘောကျကြသည်။ သို့သော်လည်း ၎င်းတို့တွင် မေးစရာမေးခွန်းများ ကျန်ရှိနေသေးသည်။

မေး ။ ။အကယ်၍ ကျွန်တော်သာ Firewall တစ်ခုကို အသုံးမပြုလျှင် ဘယ်လိုအန္တရာယ်ရှိတဲ့ threats မျိုးကို ရရှိနိုင်ပါသလဲ။ ကျွန်တော့်ရဲ့ ကွန်ပျူတာထဲကို ဝင်ရောက်ပြီး အန္တရာယ်ပြုနိုင်တဲ့ program အမျိုးအစား ဘယ်နှစ်မျိုးလောက်ရှိလဲ။ ပြီးတော့ ဘယ်လိုအန္တရာယ်မျိုးတွေ ပေးနိုင်သလဲ။

ဖြေ ။ ။တကယ်လို့ သင်သာ သင်ရဲ့ ကွန်ပျူတာကို Firewall မပါဘဲ အလုပ်လုပ်မယ်ဆိုရင် ထောင်ပေါင်းများစွာသော programs တို့ဟာ သင်ရဲ့ ကွန်ပျူတာထဲကို အင်တာနက်မှတစ်ဆင့် ဝင်ရောက်လာနိုင်တယ်လို့ ပြောရပါမယ်။ ဥပမာအားဖြင့် Firewall မရှိတဲ့ ကွန်ပျူတာများကို ရှာဖွေဝင်ရောက် ဒီဇိုင်းဆွဲထားတဲ့ Web crawlers (သို့) 'spider' ကဲ့သို့ Software များသည် သင်၏ ကွန်ပျူတာထဲသို့ ဝင်ရောက်လာပြီး ၎င်းတို့၏ လိပ်စာများကို စီးပွားရေးနှင့် ပတ်သက်သော၊ အန္တရာယ်ပြုနိုင်သော အဖွဲ့ အစည်းများသို့ ပို့ဆောင်ပေးသည်။ ထို့ပြင် တချို့သော program များသည် သင်၏ system ကို အပိုင်စီးပြီး သင်ကိုယ်တိုင် ခွင့်ပြုသိရှိသည့်အနေဖြင့် spam များ ပို့လွှတ်ခြင်း၊

မမှန်ကန်သော လုပ်ငန်းဆိုင်ရာ အရောင်းအဝယ်များ (သို့) ပို့ဆောင်လမ်းပြခြင်းတို့ကို လုပ်ဆောင်သည်။ နောက်ဆုံးတွင် သင်ကိုယ်တိုင် မကျူးလွန်သော ဥပဒေနှင့် မလွတ်ကင်းသည့် လုပ်ဆောင်မှုများကို လုပ်ဖြစ်အောင် ပုံသွင်းခြင်း ခံရနိုင်သည်။

မေး ။ ။ COMODO Firewall သာ ဒီ program အားလုံးကို ထိန်းထားနိုင်မယ်ဆိုရင် တခြား anti-virus program တွေ၊ anti-spyware program တွေကို ဘာကြောင့် လိုအပ်မှာလဲ။

ဖြေ ။ ။ Firewall သည် Internet မှ အပြန်အလှန် အသွားအလာရှိသည့် program တို့၏ access လုပ်ခြင်းကို စီစစ်တားမြစ်ပေးသည်။ ၎င်းသည် program တစ်ခု (သို့) ကွန်ပျူတာ ကျွမ်းကျင်သူ (hacker) တို့ သင်၏ system သို့ ဝင်ရောက်ခြင်းကိုသာ ကာကွယ်ပေးနိုင်ပြီး download လုပ်ယူထားသော email web page နှင့် ပြင်ပရှိ disks drive များမှ malware များပါဝင်လာမှုကို အကာအကွယ်မပေးနိုင်ပါ။ သင်၏ system ၌ အလုပ်လုပ်ရန် သင် ခွင့်ပြုထားသော အမျိုးအမည်မသိ file များကို ကြည့်ရှုရန်အတွက် ကျူးကျော်ဝင်ရောက်မှုများကို ခုခံပေးသည့် ကာကွယ်ရေး system တစ်ခုဖြစ်သော Defense⁺ သည် COMODO Firewall တွင် ပါဝင်သည်။ Anti-virus နှင့် anti- spyware program များသည် Firewall နှင့် မသက်ဆိုင်သော အခြားကူးစက်ဝင်ရောက်ခြင်းများကို ဖြည့်စွက် ကာကွယ်ပေးသည်။ ၎င်း program များသည် သင်၏ ကွန်ပျူတာတွင် ရှိနှင့်နေပြီးသော malware များကို အမှန်တကယ် ဖယ်ရှားပေးသည်။

မေး ။ ။ Windows programs (သို့) users နှင့် ရင်းနှီးကျွမ်းဝင်ပြီးသား program များနှင့် အလားသဏ္ဍာန်တူ သတိထားသင့်သည့် malware အမျိုးအစားများ ရှိပါသလား။ malware ဆိုတာ ဘာကိုခေါ်ပါသလဲ။

ဖြေ ။ ။ အဲဒီလိုမျိုး program တွေ ရှိပါတယ်။ သင့်အနေနဲ့ download (သို့) install လုပ်ယူထားတဲ့ software ရဲ့ မူလအရင်းအမြစ်ကို အထူးဂရုစိုက်သင့်ပါတယ်။ အကြံပေးချင်တာက သင့်ရဲ့ အလုပ်များ လုံးဝ မလိုအပ်၊ မဆီလျော်တဲ့ software မျိုး အထူးသဖြင့် သင့်ရဲ့ ကွန်ပျူတာပေါ်မှာ ထိခိုက်လွယ်တဲ့ data အများအပြား ရှိမယ်ဆိုပါက ၎င်း software မျိုးကို install မလုပ်သင့်ပါ။ ယခု COMODO ၏ Defense⁺ က Trusted Software Vendors list ထဲမှာ မပါဘဲ သင် လောလောဆယ် install

လုပ်ထားတဲ့ applications များမှ အမျိုးအမည်မသိ file များကို နှိုင်းယှဉ် ခွဲခြားပြခြင်းဖြင့် ၎င်း၏ အသုံးဝင်မှုကို ပြသနိုင်သည်။ ဖြစ်နိုင်ချေရှိသော အန္တရာယ်ရှိ software များကို စစ်ဆေးရန် အလိုအလျောက် ဖော်ပြပေးသည်။ သင့် Internet ၏ လွတ်လပ်မှု၊ လုံခြုံမှုတို့ကိုလည်း တိုးပွားစေသည်။

မေး ။ ။ COMODO Firewall က hackers တွေကို ဘယ်လို ဖယ်ရှားပေးသလဲ။
ဖြေ ။ ။ COMODO Firewall က သင်၏ window platform ကို over access လုပ်ခြင်းများမှ အပြည့်အဝ ထိန်းချုပ်မှုပေးသည်။ Firewall သည် ၎င်း၏ ဖွဲ့စည်းပုံအလိုက် စွမ်းဆောင်နိုင်စွမ်းရှိသည်။ အစပိုင်း၌ စိန်ခေါ်မှုများရှိစေကာမူ သင့်အနေဖြင့် အလျော့မပေးဘဲ ဆက်လက် သုံးစွဲသင့်သည်။ ထို့ကြောင့် COMODO Firewall အကြောင်းကို သင်ယူပါ။ သင့်၌ အတွေ့အကြုံ များလာလေ ၎င်း၏ ကျယ်ပြန့်သော ခုခံကာကွယ်ရေးစနစ်မှ ရရှိသော အကျိုးကျေးဇူးကို ပို၍ ခံစားရလေ ဖြစ်လိမ့်မည်။

5.1 မေးခွန်းများ သုံးသပ်ချက်

တစ်ကြိမ်မှာ Firewall တစ်ခုထက်ပို၍ သုံးစွဲနိုင်သလား။

သင့်အနေနဲ့ ရင်းနှီးကျွမ်းဝင်မှု မရှိတဲ့ program တစ်ခုကို သင့်ကွန်ပျူတာပေါ်မှာ ခွင့်ပြုဖို့ လုံခြုံမှု ရှိ၊မရှိ ဘယ်လို စစ်ဆေးမလဲ။

Firewall က ဘယ်လိုအလုပ် လုပ်သလဲ။

Firewall နဲ့ ကျူးကျော်မှု အန္တရာယ်ကာကွယ်ရေး system ဘယ်လို ကွာခြားသလဲ။

Firewall ကို install လုပ်ဖို့ ဘာတွေ လိုအပ်သလဲ။

KeePass software ကို Install လုပ်ပုံနှင့် အသုံးပြုပုံ

ဤစာမျက်နှာရှိ ပါဝင်သောအပိုင်းကဏ္ဍများမှာ

*20 Keepass ကို install လုပ်ပုံ

*21 လျှို့ဝှက်စကားလုံး (password) များထည့်သွင်း စုဆောင်းမည့် database အသစ်တစ်ခု ဖန်တီးပုံ

*22 Entry တစ်ခု ထည့်သွင်းပုံ

*23 Entry တစ်ခုကို တည်းဖြတ်ပုံ

*24 အလှည့်သင့်ရာ passwords များကို ထုတ်လုပ်ပုံ

*25 KeePass မှထွက်ခြင်း (Exit)၊ အသေးချုံ့ခြင်း (Minimize)၊ ပြန်လည်သိမ်းဆည်းခြင်း (Restore) တို့ ပြုလုပ်ပုံ

*26 Password database file ကို ကူးယူခြင်း (backup) ပြုလုပ်ပုံ

*27 သင်၏ မူပိုင် (master) password ကို တစ်ကျော့ပြန်လုပ်ခြင်း (reset) လုပ်ပုံ

2.0 KeePass ကို install လုပ်ပုံ

အဆင့် 1: File ဖွင့်ရန် double click လုပ်ပါ။ လုံခြုံရေးအချက်ပေး dialog box ပေါ်လာလိမ့်မည်။

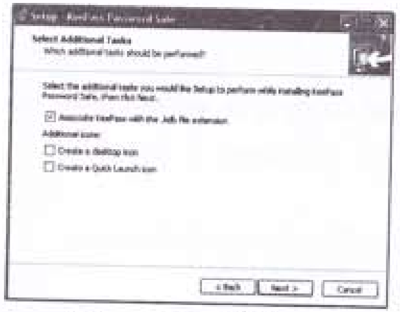
အဆင့် 2: Setup ကို လုပ်ဆောင်ရန် click လုပ်ပါ။ KeePass password safe setup ကို တွေ့ရမည်။

အဆင့် 3: User ခွင့်ပြုမှုရယူမည့် screen ကို ckick လုပ်ပါ။ ကျန်သည့် installation အပိုင်းများကို ဆက်မလုပ်မီ User သဘောတူညီချက်ပါ အချက်အလက်များကို ဖတ်ပါ။

အဆင့် 4: သဘောတူညီချက် ရယူပြီးနောက် Next ကို နှိပ်ပါ။ ဤ program အားသိမ်းမည့် destination တည်နေရာပြ screen ကိုရောက်ရန် click လုပ်ပါ။

အဆင့် 5: ကွန်ပျူတာက အလိုအလျောက် ရွေးချယ်ပေးသည့် installation path ကို လက်ခံပါ။ Start Menu Folder screen ကို သွားပါ။ ရွေးချယ်ပေးသည့် Folder ကို လက်ခံရန် click လုပ်ပါ။

အဆင့် 6: အောက်ပါ screen ကို သွားရန် click လုပ်ပါ။



ပုံ 1: တွဲလျက်ပါဝင်သော တာဝန်များအား ရွေးချယ်ခြင်း (Select Additional Tasks) screen ပုံ

အဆင့် 7: ပုံ 2 တွင် ပြသထားသော options များကို စစ်ဆေးပါ။

မှတ်ချက် ။ ။ ' Don't create a Start Menu ' folder option ကို ပိတ်ခဲ့ပါက KeePass Password Safe installation သည် Start menu ထဲ၌ KeePass Quick Launch icon တစ်ခုကို အလိုအလျောက် ထည့်သွင်းပေးလိမ့်မည်။

အဆင့် 8: ' Ready to Install ' screen ကို စတင်ရန် click လုပ်ပါ။ ထို့နောက် ၎င်း၏ လုပ်ငန်းစဉ် အခြေအနေပြဘား ပါဝင်သော install လုပ်မည့် screen သို့ click လုပ်ပါ။ စက္ကန့်အနည်းငယ်ကြာပြီးနောက် ' KeePass Password Safe Setup ' ပြီးပြည့်စုံစွာ ဆောင်ရွက်ပြီးကြောင်း screen ပေါ်လာလိမ့်မည်။

အဆင့် 9: KeePass ဖွင့်ရန် ' Launch KeePass ' option ကို နှိပ်ပါ။ သင့်၌ Internet ချိတ်ဆက်မှု ရှိပါက ' KeePass Plugins and Extensions web site ' သို့ ဆက်သွယ်ပေးလိမ့်မည်။

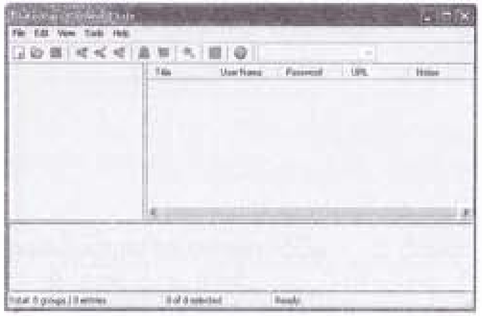
2.1 လျှို့ဝှက်စကားလုံး (password) များ ထည့်သွင်းစုဆောင်းမည့် database အသစ်တစ်ခု ဖန်တီးပုံ

အောက်ဖော်ပြပါ အပိုင်းတွင် သင်၏ မူပိုင် password တစ်ခုကို ဖန်တီးခြင်း။ အသစ်ပြုလုပ်ထားသော database (အချက် အလက်စုဆောင်းရာနေရာ) ကို သိမ်းဆည်းခြင်း။ သီးခြား program တစ်ခုစီအတွက် အလှည့်သင့်ရာ password များ ထုတ်ပေးခြင်း။ database ၏ backup ကို ကူးယူထားခြင်း။ လိုအပ်ပါက password များကို KeePass မှ ထုတ်ယူခြင်း နည်းလမ်းများကို လေ့လာသင်ယူနိုင်သည်။

KeePass ကို ဖွင့်ရန် အောက်ပါ အဆင့်များကို ဆောင်ရွက်ရမည်။

အဆင့် 1- Start>programs>KeePass Password Safe> KeePass ကို သွားပါ။ (သို့မဟုတ်) ပုံပါအတိုင်း KeePass ၏ အဓိက screen ကိုဖွင့်ရန် desktop ပေါ်ရှိ KeePass icon ကို နှိပ်ပါ။

ပုံ 2: KeePass Password Safe ထိန်းချုပ်မှုစားပွဲ (console) ပုံ



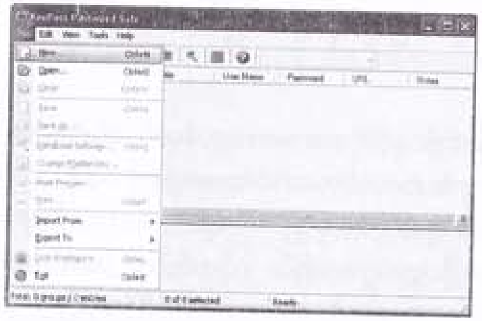
2.1.1 Password Database အသစ်တစ်ခု ဖန်တီးပုံ

Password Database အသစ်ပြုလုပ်ရာတွင် အဆင့် 2 ဆင့်ပါဝင်သည်။

သင်၏ passwords များ စုစည်းရာ database ကို lock ချရန်(သို့) ဖွင့်ရန်တို့အတွက် တစ်ခုတည်းသော ကျစ်လျစ်သိပ်သည်းမှုရှိသည့် password ကို ရွေးချယ်ရမည်။ ထို့နောက် ၎င်း password database ကို save လုပ်ရမည်။

Password Database ဖန်တီးရန် အောက်ပါအဆင့်များကို ဆောင်ရွက်ပါ။

အဆင့် 1: File အသစ် ရွေးချယ်ပါ။ (select File> New)ပုံ



ပုံ 3: File အသစ်ရွေးချယ်ထားသော Kee-Pass screen ပုံ။

အောက်ပါပုံကို ထပ်တွေ့ရမည်။

ပုံ 4: Password Database အသစ်ဖန်တီးထားသော KeePass screen ပုံ

အဆင့် 2: မူပိုင် password ထည့်ရန်နေရာ၌ သင် ရွေးချယ်ထားပြီးသော password ကို ရိုက်ထည့်ပါ။

ပုံ 5: Password ရိုက်ထည့်ထားသော 'Kee-Pass Set Composite Master Key'ပုံ

Password ထည့်သည့်နေရာ၏ အောက်ဘက်တွင် အစိမ်းရောင်၊ လိမ္မော်ရောင် အလုပ် လုပ်ဆောင်မှုပြဘားတစ်ခုကို တွေ့ရမည်။ သင်အသုံးပြုသော စာလုံး အရေအတွက်ပေါ် မူတည်၍ သင်၏ password ကြံ့ခိုင်မှုနှင့်ရှုပ်ထွေးမှုတို့ ပိုများလာပါက အဆိုပါဘားပေါ်ရှိ အစိမ်းရောင်အရေအတွက် ပို၍ မြင့်မားလာလိမ့်မည်။

သတိပြုရန် ။ ။ သင်၏ password ကို ရိုက်နှိပ်ပြီးချိန်၌ ၎င်းဘားပေါ်ရှိသော အစိမ်းရောင်အမှတ်အသားသည် အနည်းဆုံး ထိုဘား၏ တစ်ဝက်ရောက်သည့်အထိ ပြည့်နေရမည်။

အဆင့် 3: သင်ရိုက်နှိပ်ထားသော password ကို သေချာမှုရှိစေရန် 'Repeat Master Password ' screen ကို သွားပါ။

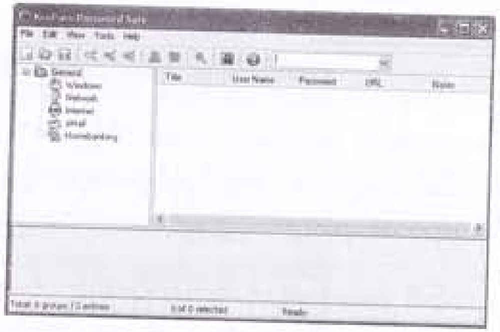
ပုံ 6: KeePass Repeat Master Password screen ပုံ

အဆင့် 4: မူလရိုက်ထားသော password ကို ပြန်ရိုက်ထည့်ပါ။ click လုပ်ပါ။

အဆင့် 5: သင်ရိုက်လိုက်သော password မှန်ကန်မှု ရှိ၊ မရှိ စစ်ဆေးရန် click လုပ်ပါ။

သတိပေးချက် ။ ။ အကယ်၍ တစ်စုံတစ်ယောက် သင်၏ နောက်ကျောဘက်၌ ရှိနေမည်ဆိုပါက ဤကဲ့သို့ password ထည့်သွင်းရာ၌ သတိထားရန်လိုအပ်သည်။

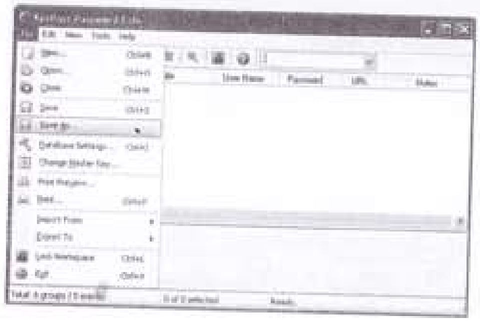
သင်၏ မူပိုင် password ကို အောင်မြင်စွာ ထည့်သွင်းပြီးပါက၊ KeePass console က အောက်ပါအတိုင်း ဆောင်ရွက်လိမ့်မည်။



ပုံ 7: **အလုပ်လုပ်ရန် အသင့်ရှိနေသော** ' KeePass Password Safe ' screen ပုံ

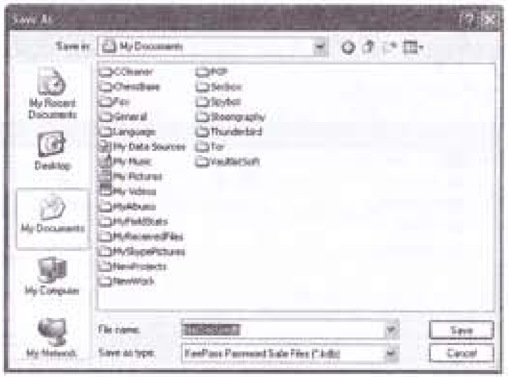
Password database ကို ဖန်တီးပြီးပါက ၎င်းကို save လုပ်ရမည်။ Password database ကို save လုပ်ရန် အောက်ပါအဆင့်များ ဆောင်ရွက်ရမည်။

အဆင့် 1: File အတွင်းရှိ Save As ကို ရွေးပါ။



ပုံ 8: ' KeePass Password Safe screen' ပုံ

' Save as ' screen ကို တွေ့ရမည်။



ပုံ 10: ' Save As ' screen ပုံ

အဆင့် 2: သင်၏ password database file အသစ်အတွက် အမည်တစ်ခု ရိုက်ထည့်ပါ။

အဆင့် 3: database ကို save လုပ်ပါ။

သတိပြုရန် ။ ။ သင့် Database ၏ တည်နေရာနှင့် File အမည်တို့ကို မှတ်သားထားပါ။ သင့် database ၏ backup ကူးယူသည့်အခါတွင် အလွယ်တကူ ရှာဖွေ အသုံးပြုနိုင်သည်။

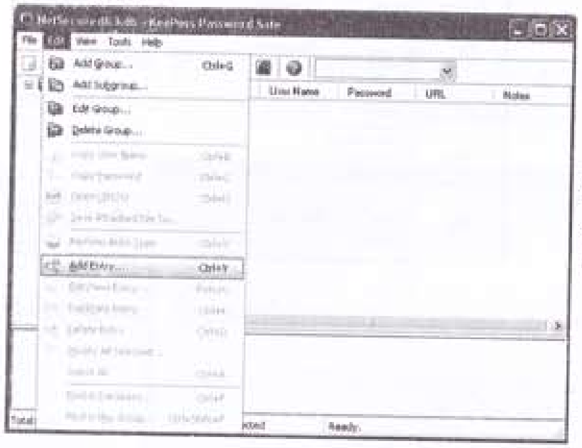
သင်၏ လုံခြုံစိတ်ချရသော password database တစ်ခုကို အောင်မြင်စွာ ဖန်တီးတည်ဆောက်ပြီးပါပြီ။ ယခုအချိန်မှစ၍ သင် အသုံးပြုနေဆဲ၊ အသုံးပြုမည် ဖြစ်သော မည်သည့် passwords ကိုမဆို password database ထဲသို့ ထည့်သွင်းနိုင် ပါသည်။

2.2 Entry တစ်ခု ထည့်သွင်းပုံ

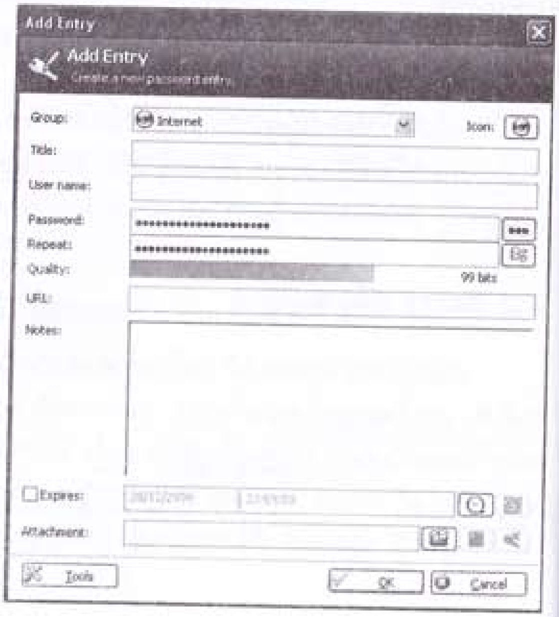
Add Entry screen က သင်အသစ်ဖန်တီးလိုက်သော Database အတွင်းသို့ သင်၏ စာရင်းအချက်အလက်များ၊ passwords များနှင့် အခြားအရေးကြီးသည့် အချက်အလက်များကို ထည့်သွင်းခွင့်ပေးသည်။ အောက်တွင်ဖော်ပြထားသော ဥပမာအရ web sites နှင့် email accounts အမျိုးမျိုးတို့အတွက် အသုံးပြုသူ အမည်နှင့် passwords များကို သိုလှောင်သိမ်းဆည်းရန် Entry များ ပေါင်းထည့်ပေးလိမ့်မည်။

အဆင့် 1: Edit ကို နှိပ်ပါ။ ' KeePass Password Safe ' screen ရှိ ' Add Entry ' ကိုနှိပ်ပါ။ ' Add Entry ' screen ပေါ်လာလိမ့်မည်။

မှတ်ချက် ။ ။ ' Add Entry ' screen တွင် ဖြည့်စွက်ရန် နေရာတချို့ကို သင်တွေ့ရမည်။



ပုံ 10: Add Entry ကို ရွေးချယ်ထားသော ' KeePass Password Safe ' screen ပုံ



ပုံ 11: ' KeePass Add Entry ' screen ပုံ

ဤနေရာရှိကွက်လပ်များကို မလိုအပ်ဘဲ ဖြည့်စွက်နိုင်ခြင်းမဟုတ်ဘဲ သင်ဖြည့်စွက်သည့် အချက်အလက်များက သင်၏ အဆင်ပြေမှုကို အထောက်အကူပြုသည်။ တိကျသော Entry မျိုးကို ရှာဖွေသည့် အခြေအနေမျိုးတွင် ၎င်းက များစွာ အကျိုးရှိစေသည်။

၎င်းကွက်လပ် (Text boxes) များအကြောင်း အသေးစိတ် ရှင်းလင်းချက်ကို အောက်တွင် ဖော်ပြထားသည်။

✻ **Group (အုပ်စု)** : KeePass က သင်၏ passwords များကို ကြိုတင်မှခြားအမည်ပေးထားသော Groups များအတွင်းသို့ စီစဉ်ထည့်သွင်းပေးသည်။ ဥပမာ ' Internet ' ဟု အမည်ပေးထားသော Group အတွင်းသို့ website accounts များနှင့် ပတ်သက်သော passwords များ ထည့်သွင်းပေးခြင်းမျိုး ဖြစ်သည်။

✻ **Title (ခေါင်းစဉ်)** : တိကျသော password entry ကို ဖော်ပြရန် အမည်။ ဥပမာ (Gmail password)

User name (သုံးစွဲသူ၏ အမည်) : သုံးစွဲသူ၏ အမည်သည် password entry နှင့် တစ်ဆက်တည်းရှိပါသည်။ ဥပမာ - (securitybox @ gmail.com)

✻ **URL (အင်တာနက် လိပ်စာ)** : Internet site သည် password entry နှင့် တစ်ဆက်တည်း ဖြစ်သည်။ ဥပမာ- (http://mail.google.com)

✻ **Password (လျှို့ဝှက်စကားလုံး)** : ' Add Entry ' screen ကို ရောက်သည်နှင့် အလှည့်သင့်ရာ password ကို အလိုအလျောက် ထုတ်ပေးလိမ့်မည်။ Email account အသစ်တစ်ခုကို သင် မှတ်ပုံတင်မည်ဆိုပါက ဤကွက်လပ်၌ ပေးထားသော password ကိုပင် အသုံးပြုနိုင်သည်။ ရှိပြီးသား password အား အသုံးမပြုဘဲ KeePass မှ ထုတ်ပေးသည့် passwords နှင့်လည်း လဲလှယ်အသုံးပြုနိုင်သည်။ KeePass က အမြဲတစေ မှတ်သားထားသည့်အတွက် password ကို ကြည့်ရန်ပင် မလိုအပ်ပေ။ အလှည့်သင့်ရာ ထုတ်ပေးသော password က ကျူးကျော်ဖျက်ဆီးသူများအား မှန်းဆရန်ခက်ခဲစေပြီး ဝင်ရောက်ချိုးဖောက်ရန်လည်း မလွယ်ကူပါ။ အလှည့်သင့်ရာ password များ ထုတ်လုပ်မှုကို တောင်းဆိုခြင်းအား အောက်တွင် ဆက်လက်ဖော်ပြထားလိမ့်မည်။ ရှိပြီးသား password နေရာ၌ သင့်ကိုယ်ပိုင် password တစ်ခုကို အမှန်တကယ် အစားထိုးထည့်နိုင်သည်။ ဥပမာအားဖြင့် သင်သည် မူလရှိပြီးသား account အတွက် Entry တစ်ခု ဖန်တီးမည်ဆိုပါက ဤကွက်လပ်တွင် မှန်ကန်မှုရှိသည့် password ဖြင့် ဝင်ရောက်ရမည်။

✻ Repeat Password (password ကို နောက်တစ်ကြိမ်ထည့်ခြင်း) : သင် ရိုက်နှိပ်ထားသော password မှန်၊ မမှန် စစ်ဆေးခြင်း။

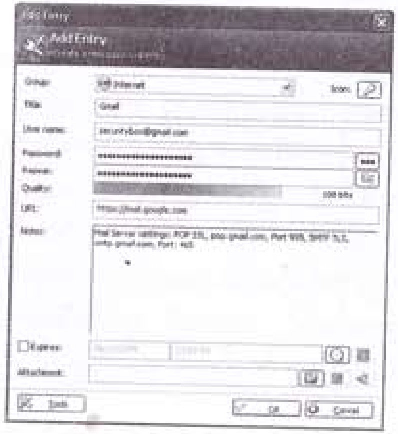
✻ Quality (အရည်အသွေး) : တိုးတက်မှုပြဘား (progress bar) က password ၏ အရှည်နှင့် ရောက်ရှိလာသည့် အနေအထားကို ကြည့်၍ မည်မျှ ကြံ့ခိုင်မှု ရှိသည်ကို တိုင်းတာသည်။ ဘားအပေါ်တွင် အစိမ်းရောင်များလေလေ သင် ရွေးချယ်သည့် password ပို၍ ကြံ့ခိုင်လေလေ ဖြစ်သသည်။

✻ Notes (မှတ်ချက်) : ဤကွက်လပ်၌ သင်ရွေးချယ်ထားသော account (သို့) site တို့၏ အထွေထွေ သတင်းအချက်အလက် ဖော်ပြချက်များကို ရိုက်ထည့်ရန် ဖြစ်သည်။

ဥပမာ - (Mail server settings : POP3 SSL, pop.gamil.com, Port: 995; SMTP TLS, smtp.gmail.com,Port:465)

မှတ်ချက် ။ ။ password entry များကို ဖန်တီးခြင်း၊ ပြုပြင်ခြင်းတို့ကြောင့် Kee-Pass က သင်၏ password အစစ်အမှန်ကို မပြောင်းလဲနိုင်ပါ။ KeePassကို သင်၏ password များအတွက် စိတ်ချယုံကြည်ရသော electronic address book တစ်ခုအဖြစ် မှတ်ထားပါ။ ၎င်းက သင်ရေးသည့် အကြောင်းအရာကျော်လွန်၍ မည်သည့်အရာကိုမှ သိမ်းဆည်းပေးမည် မဟုတ်ပါ။

အုပ်စုရွေးချယ်ရာတွင် 'Internet' ကို စာရင်းထဲမှရွေးချယ်မည်ဆိုပါစို့။ သင်၏ password entry က အောက်ပါအတိုင်း ပြန်ပေါ်လာလိမ့်မည်။



ပုံ 12: လုပ်ဆောင်ချက်ပြီး (compled) Kee Pass Add Entry screen ပုံ

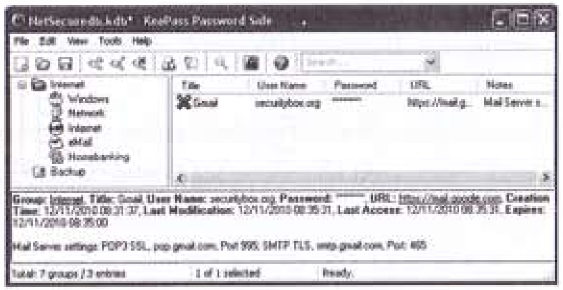
အဆင့် 2: Add Entry screen ၌ သင်၏ အပြောင်းအလဲများကို save လုပ်ရန် click နှိပ်ပါ။ ယခု သင်၏ password entry ကို Internet group ထဲ၌ တွေ့ရမည်။

ပုံ 13: KeePass Password Safe screen ပုံ

မှတ်ချက် ။ ။ window အောက်ခြေရှိ ဇယားကွက်သည် ရွေးချယ်ထားသော Entry ၏အချက်အလက်များကို ဖော်ပြပေးသည်။ သင့်အနေဖြင့် Entry ထဲတွင် မှတ်သားထားသော မှတ်စုများ၊ ကန့်သတ်ချက်ကုန်ဆုံးချိန်၊ တည်းဖြတ်ခြင်းနှင့်ဖန်တီး ပြုလုပ်ခြင်းများလည်း ၎င်း၌ ပါဝင်သည်။ ၎င်းက password ကို ထုတ်ဖော်မပေးပါ။

✻ Expires (ကန့်သတ်ချိန် ကုန်ဆုံးခြင်း) : Text boxes အတွင်းရှိ ကန့်သတ်ချိန် ကုန်ဆုံးပြီးသော ရက်စွဲများကို ခွဲခြားရန် ဤအချက်ကို စစ်ဆေးပါ။ တိကျသော အချိန်တစ်ခု (ဥပမာ- 3 လတစ်ကြိမ်)၌ password ကို ပြောင်းလဲရန် သင့်အတွက် သတိပေးချက်တစ်ခု ထည့်ပေးထားနိုင်သည်။ နောက်တွင် အနီရောင် ကြက်ခြေခတ် ပေါ်လာလိမ့်မည်။ အောက်တွင် ဥပမာ ပြထားသည်။

ပုံ 14: NetSecure Db.kdb screen ရှိ expired key ပုံ



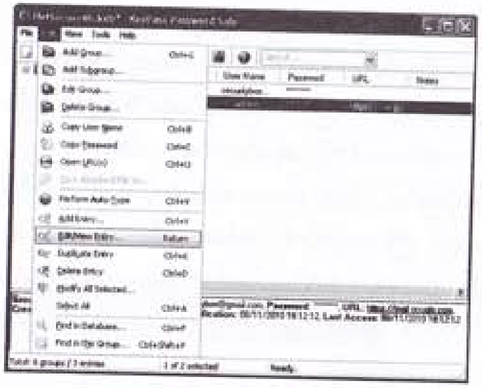
2.3 Entry တစ်ခုကို တည်းဖြတ်ပုံ

KeePass အတွင်းရှိ မူလရှိပြီးသား Entry တစ်ခုကို အချိန်မရွေး သင် တည်းဖြတ်နိုင်သည်။ သင်၏ password ကို ပြောင်းလဲနိုင်သည်။ (ယေဘုယျအားဖြင့် 3 လမှ 6 လ တစ်ကြိမ် password ကို ပြောင်းလဲပေးခြင်းသည် လုံခြုံရေးအတွက် ကောင်းသောအလေ့အကျင့်ဖြစ်သည်ဟု ယူဆသည်)။ သို့မဟုတ် password entry အတွင်း သိမ်းဆည်းထားသော အခြား အသေးစိတ်အချက်အလက်များကို ပြုပြင်နိုင်သည်။

Entry တစ်ခုကို တည်းဖြတ်ရန် အောက်ပါအဆင့်များကို ဆောင်ရွက်ရမည်။

အဆင့် 1: ဘယ်ဘက်ခြမ်းရှိ Entry များ တွဲလျက် ပါဝင်သော Group ကို မှန်မှန် ကန်ကန် ရွေးချယ်ပါ။

အဆင့် 2: ဆီလျော်သော Entry ကိုရွေးပါ။ အောက်ဖော်ပြပါ window ကို လုပ် ဆောင်ရန် ရွေးချယ်ထားသော Entry ပေါ်သို့ right click လုပ်ပါ။



ပုံ 15: Edit menu ကို ဖော်ပြထားသော KeePass Password Safe screen ပုံ

အဆင့် 3: Password အပါအဝင် လိုအပ်သော အပြောင်းအလဲ ဟူသမျှကို save လုပ်ပါ။

သင်အစပိုင်းက ပြုလုပ်ထားသော Password နှင့် KeePass က ပေးထားသည့် password ကို လဲလှယ်ရန် အောက်ပါအပိုင်းကို ဖတ်ပါ။

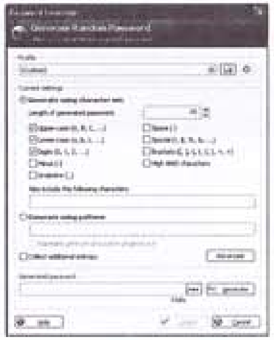
2.4 အလှည့်သင့်ရာ password များကို ထုတ်လုပ်ပုံ

လုံခြုံရေးလောကဌ် ရှည်လျားပြီး ပုံမှန်မဟုတ်ဘဲ အလှည့်သင့်သလို ထွက်ပေါ်လာသော password များကို ကြံ့ခိုင်မှု ရှိသည်ဟု ယူဆသည်။ ဤသို့ အလှည့်သင့်သလို ပျောက်လာနိုင်ရန် သချာစည်းမျဉ်းများကို အခြေခံပြုလုပ်ထားပြီး သင်၏ accountsများကို ဝင်ရောက်ချိုးဖောက်ရန် ကြိုးစားသူ မည်သူကမျှ မှန်းဆရန် မလွယ်ကူပါ။ ဤလုပ်ငန်းရပ်များဆောင်ရွက်နိုင်ရန် KeePass က ' Password Generator ' တစ်ခုကို ပေးထားသည်။ အထက်တွင် သင်မြင်ခဲ့ရသည့်အတိုင်း Entry အသစ်တစ်ခု ပေါင်းထည့်သောအခါ အလှည့်သင့်ရာ password ကို အလိုအလျောက် ထုတ်ပေးသည်။ ဤအပိုင်းတွင် သင်ကိုယ်တိုင် password တစ်ခုကို မည်သို့မည်ပုံ ထုတ်ယူရမည်ကို ဖော်ပြထားသည်။

မှတ်ချက် ။ ။ ' Password Generator ' ကို Add Entry နှင့် Edit/View Entry screens များမှတစ်ဆင့် ထုတ်ယူ လုပ်ဆောင်နိုင်သည်။ ၎င်းတို့ အတွင်းရှိ Tools မှ တစ်ဆင့် ' Password Generator ' ကို အဆင်ပြေသလို ဆွဲယူလုပ်ဆောင်နိုင်သည်။

အဆင့် 1: Password Generator ' screen ကို လုပ်ဆောင်ရန် Add Entry or Edit/View Entry တို့မှတစ်ဆင့် click လုပ်ပါ။

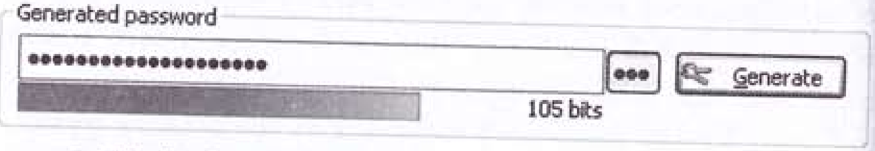
ပုံ 16: KeePass Password Generator screenပုံ



' Password Generator ' screen က password တစ်ခု ထုတ်ယူရာ၌ ရွေးချယ်ခွင့်များစွာပေးထားသည်။ ပြုလုပ်ထားသော password ၏ စကားလုံး အရေအတွက်ကိုလည်းကောင်း၊ အလိုရှိသော password ၏ အရှည်ကိုလည်းကောင်း၊ အခြား အမျိုးအပြားကိုပါ ခွဲခြားစိတ်ဖြာနိုင်သည်။ ကျွန်ုပ်တို့ အလိုရှိရာကို ပြုပြင်နိုင်ရန်

ပေးထားသော options များကို အသုံးပြုနိုင်သည်။ ဆိုလိုသည်မှာ ထုတ်လုပ်ပေးသော passwordသည် စာလုံးရေ 20 ရှည်လျားပြီး စကားလုံး အကြီးအသေးများ၊ ဂဏန်းများ ပါဝင်သည်။

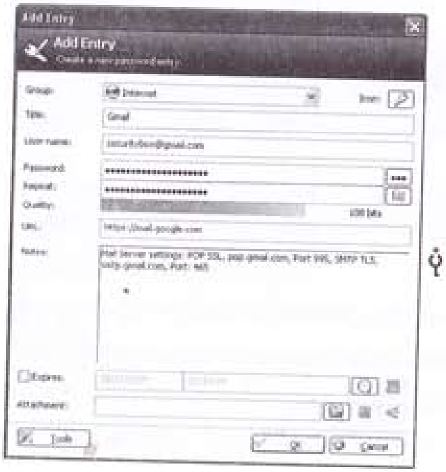
အဆင့် 2: လုပ်ငန်းစဉ်ကိုစတင်ရန် click လုပ်ပါ။ လုပ်ငန်းစဉ်ပြီးဆုံးပါက KeePass က သင့်ကို password တစ်ခု ထုတ်ပေးလိမ့်မည်။



ပုံ 17: KeePass ၏ Passward ထုတ်ပေးသော အပိုင်းကဏ္ဍပုံ

မှတ်ချက် ။ ။ ထုတ်ပေးသော password ကို click လုပ်၍ ကြည့်နိုင်သည်။ သို့သော် ကျွန်ုပ်တို့ အထက်တွင် ဆွေးနွေးခဲ့ သည့်အတိုင်း ၎င်းက လုံခြုံရေးကို အနှောင့်အယှက် ဖြစ်စေသည်။ လက်တွေ့တွင် သင့်အနေဖြင့် password ကို လုံးဝ ကြည့်ရန် မလိုအပ်ပါ။ အခန်း ' 3.0 KeePass Password များကို အသုံးပြုခြင်း' တွင် ကျွန်ုပ်တို့ ထပ်မံ ရှင်းလင်းတင်ပြပါမည်။

အဆင့် 3- Password ကို လက်ခံရန် click လုပ်ပါ။ ပြီးနောက် Add Entry screen သို့ အောက်ပါအတိုင်း ပြန်သွားပါ။



ပုံ 18: KeePass Add Entry screen ပုံ

အဆင့် 4: Entry ကို save လုပ်ရန် click ပါ။

အဆင့် 5: File ကို ရွေးချယ်ပါ။ သင်၏ နောက်ဆုံး ပြုပြင်မွမ်းမံထားသော(updated) password database ကို save လုပ်ပါ။

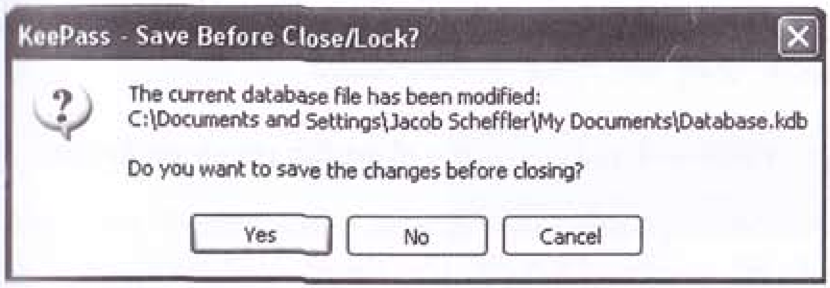
2.5 KeePass မှ ထွက်ခြင်း (Exit)၊ အသေးချုံခြင်း (Minimize) ၊ ပြန်လည်ပြီးသည်းခြင်း (Restore) တို့ ပြုလုပ်ပုံ

သင်သည် KeePass program ကို အချိန်မရွေး minimize လုပ်ခြင်း၊ exit လုပ်ခြင်းတို့ ပြုလုပ်နိုင်သည်။သင်သည် ၎င်း Program ကို open လုပ်ခြင်း၊ restore လုပ်ခြင်းတို့ပြုလုပ်ပါက သင်၏ မူပိုင် Master Password ဖြင့် ဝင်ရောက်ရန် လိုအပ်သည်။

KeePass သည် system tray ထဲ၌ screen ၏ အောက်ခြေ ညာဘက်ထောင့်တွင် minimize လုပ်ထားပုံကို အောက်ပါအတိုင်း တွေ့ရမည်။

အောက်ပါအဆင့်များကို ဆောင်ရွက်ခြင်းဖြင့် KeePass က programကို lock ချရန် ခွင့်ပြုသည်။

အဆင့် 1: File ကို ရွေးချယ်ပါ။ အောက်ပါ screen ကို လုပ်ဆောင်ရန် Workspace ကို lock လုပ်ပါ။



ပုံ 19: KeePass - Safe Before Close/Lock prompt screen ပုံ

အဆင့် 2: သင်၏ သတင်းအချက်အလက်များကို save လုပ်ရန် click ပါ။

KeePass console ကို disable လုပ်ပါ။ ပုံ 20 တွင် ပါရှိသည့်အတိုင်း မော်ပြပါ icon သည် System Tray ထဲ၌ ပေါ်လာလိမ့်မည်။

computer dummy.ps: Plate 12

အဆင့် 1: KeePass ကို ပုံမှန်အရွယ်အစားသို့ ပြန်သွားရန် 'double click 'လုပ်ပါ။ အောက်ပါ screen ကို လုပ်ဆောင်ပါ။

ပုံ 20: KeePass Open Database-NetSecure Db.kdb screen ပုံ

အဆင့် 3: KeePass ကို ဖွင့်ရန် Master Password ရိုက်ထည့်ပါ။ KeePass ကို ပိတ်ရန် အောက်ပါအတိုင်း ဆောင်ရွက်ပါ။

အဆင့် 1: File မှတစ်ဆင့် KeePass program ကို Exit လုပ်၍ ပိတ်နိုင်ပါသည်။

Database ထဲ၌ save မလုပ်ရသေးသော အကြောင်းအရာများရှိပါက KeePass က ၎င်းကို save လုပ်ရန် သတိပေးလိမ့်မည်။

2.6: Password Database file ကို ကူးယူခြင်း (Backup) ပြုလုပ်ပုံ

သင်၏ ကွန်ပျူတာပေါ်တွင် KeePass database File ကို file extension (.kdb) ဖြင့် အမှတ်အသားပြုသည်။ ၎င်း File ကို USB memory stick ထဲသို့ ကူးယူနိုင်သည်။ မည်သူ တစ်ဦးတစ်ယောက်ကမှ master password မပါဘဲ ဤ database file ကို မဖွင့်နိုင်ပါ။

အဆင့် 1: File မှတစ်ဆင့် Save as ကို သွားပါ။ ပင်မ screen ပေါ်ရှိ database ကို ကူးယူ၍ အခြားတစ်နေရာ၌ save လုပ်ပါ။

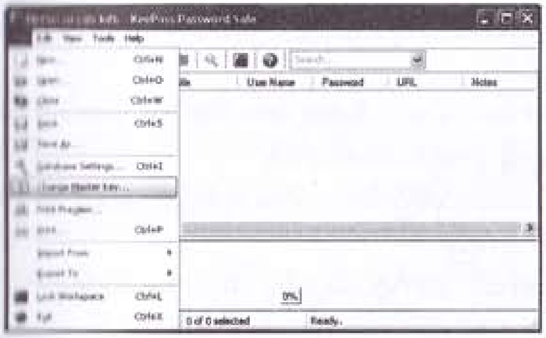
KeePass program တစ်ခုလုံးကို USB Memory Stick မှတစ်ဆင့် သင်၏

ကွန်ပျူတာပေါ်၌ အလုပ်လုပ်နိုင်သည်။ အိတ်ဆောင် KeePass အသုံးချ စာမျက်နှာကို ကြိုးစားပါ။

2.7 သင်၏ မူပိုင် (master) password ကို တစ်ကျော့ပြန်လုပ်ခြင်း (reset) လုပ်ပုံ

သင်သည် master password ကို အချိန်မရွေး ပြောင်းလဲနိုင်သည်။ သင် password database ကို တစ်ကြိမ်ဖွင့်တိုင်း ယခု လုပ်ငန်းစဉ်ကို လုပ်ဆောင်နိုင်သည်။

အဆင့် 1: File မှတစ်ဆင့် Change Master Key ကို ရွေးပါ။



ပုံ 21: KeePass Change Master Key screen ပုံ

အဆင့် 2: Master password အသစ်ကို ညွှန်ကြားထားသည့်အတိုင်း နှစ်ကြိမ် ရိုက်ထည့်ပါ။

ပုံ 22: Master Key ပြောင်းလဲသော KeePass screen ပုံ

KeePass- လုံခြုံမှုရှိသော Password များကို သိုလှောင်ထားခြင်း

KeePass သည် password များကို စီစဉ်ဆောင်ရွက်ရာ၌ အသုံးပြုရန် လွယ်ကူပြီး လုံခြုံမှုရှိသည့် အသုံးချ program တစ်ခုဖြစ်သည်။

KeePass ကို download လုပ်ယူခြင်း

* လက်စွဲလမ်းညွှန်ပါ 'မိတ်ဆက်' (Introduction) ကို ဖတ်ပါ။

* www. keepass.info/download.html ကို ဖွင့်ရန် KeePass icon ကို click လုပ်ပါ။

* webpage ပေါ်ရှိ " Classic Edition " အပိုင်းမှ " KeePass 1.xx (Installer EXE for Windows) " ကို click လုပ်ပါ။

* Installer ဖြစ်သည့် KeePass - 1.xx - Setup -exe file ကို save လုပ်ပါ။ ထို့နောက် ၎င်းတည်နေရာကို ရှာ၍ double click လုပ်ပါ။

* KeePass ကို အောင်မြင်စွာ install လုပ်ပြီးပါက သင်၏ ကွန်ပျူတာပေါ်ရှိ installation program ကို ဖျက်ပစ်နိုင်ပါသည်။

အောက်ပါဖော်ပြချက်များသည် လက်စွဲလမ်းညွှန်မှ KeePass အကြောင်း ' Introduction ' ဖြစ်သည်။

* KeePass ၏ Homepage မှာ www.keepass. info ဖြစ်သည်။

* Computer နှင့် ပတ်သက်သော လိုအပ်ချက်မှာ မည်သည့် windows versions ကိုမဆို အသုံးပြုနိုင်သည်။

* ဤ လမ်းညွှန်တွင် သုံးစွဲထားသည့် versions မှာ 1.18 ဖြစ်သည်။

* License မှာ Free ဖြစ်ပြီး Open-Source software တစ်ခုဖြစ်သည်။

* ဖတ်ရန်လိုအပ်သည့် အကြောင်းအရာမှာ Chapter 3 ရှိ ကောင်းမွန်သော passwords များ ဖန်တီးခြင်းနှင့် ပြုပြင်ခြင်း အကြောင်းဖြစ်သည်။

* Level အဆင့်များမှာ 1: Beginner , 2: Average , 3: Intermediate , 4: Experienced , 5: Advanced

* ဤ programm ကို စတင်အသုံးချရန် လိုအပ်ချိန်မှာ 15 မိနစ်ဖြစ်သည်။

* သင်ရမည့် အကျိုးတရားများကတော့ သင်၏ passwords များအားလုံးကို အဆင့်မြင့် လုံခြုံမှုရှိသည့် Database တစ်ခုထဲတွင် သိမ်းဆည်းနိုင်ခြင်း၊ မှတ်သားထားရန် မလိုအပ်ဘဲ

ခိုင်မှုရှိသည့် passwords များကို ဖန်တီး သိုလှောင်ထားနိုင်ခြင်းတို့ ဖြစ်သည်။

* KeePass ကို GNU Linux နှင့် Mac OS များအတွက် KeePass X version ပုံစံဖြင့် ရရှိနိုင်သည်။ i Phone, BlackBerry, Android, Pocket PC စသည့် platforms များအတွက်လည်း KeePass versions များ ရှာဖွေနိုင်သည်။ အကယ်၍ KeePass ကဲ့သို့ အခြားသော programs များကို စမ်းကြည့်ချင်ပါက ကျွန်ုပ်တို့ ညွှန်းလိုသည်မှာ Microsoft Windows များနှင့် GNU Linux တို့အတွက်' Password Safe ' program, Mac OS, Microsoft Windows, iPhone နှင့် iPad တို့အတွက် ' I Password ' program တို့ ဖြစ်ကြသည်။

1.1 ဤ program ကို စတင်မလုပ်ဆောင်မီ သိသင့်သည့် အချက်များ

KeePass သည် အသုံးပြုရန် လွယ်ကူ၍ အစွမ်းထက်သော tool တစ်ခုဖြစ်ပြီး သင်၏ passwords များအားလုံးကို အဆင့်မြင့် လုံခြုံမှုရှိသည့် database တစ်ခုထဲတွင် သိမ်းဆည်းစီစဉ်ဆောင်ရွက်ရန် ကူညီသည်။ ၎င်း database နှင့် KeePass program နှစ်ခုလုံးကို USB memory stick ၌ထည့်၍ သွားလေရာ သယ်ဆောင်နိုင်သည်။ Database ကို သင်ဖန်တီးထားသော 'Master Password' နှင့် ကာကွယ်ပေးထားသည်။ ၎င်း password ကို database တွင် ပါဝင်သည့် အကြောင်းအရာ အချက်အလက် များအားလုံး အသွင်ပြောင်း (encrypt) လုပ်ရာတွင်လည်း အသုံးပြုသည်။ KeePass တွင် သင်၏ မူလ passwords များကို သိမ်းနိုင်ပြီး ၎င်းမှလည်း passwords များ ထုတ်ယူနိုင်သည်။ KeePass တွင် installation အတွက် လမ်းညွှန်ကြားချက် များ နှင့် ကြိုတင်ပြင်ဆင်ထားသောပုံစံများ မလိုအပ်ဘဲ သင်အသုံးပြုလိုသည့်အခါ အဆင်သင့် လွယ်ကူစွာ အသုံးပြုနိုင်သည်။

* KeePass ကို Install လုပ်ခြင်းနှင့် အသုံးပြုခြင်း

* KeePass Passwords များကို အသုံးချခြင်း

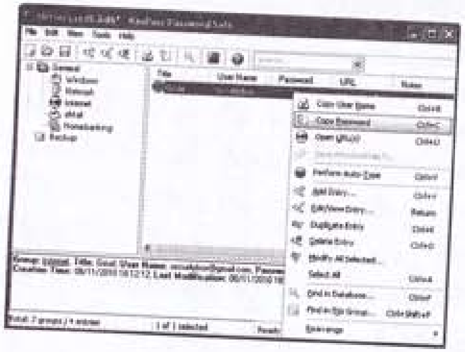
* မေးလေ့ရှိသော မေးခွန်းများနှင့် သုံးသပ်ချက်

3.0 KeePass Passwords များကို အသုံးပြုခြင်း

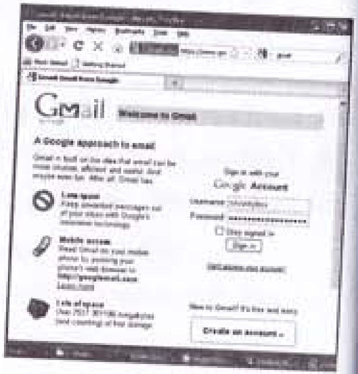
လုံခြုံစိတ်ချရသော password တစ်ခုကို မှတ်သားရန် မလွယ်ကူကြောင်း သိရသည့်အတိုင်း KeePass က ၎င်းကို database မှ ကူးယူ၍လိုအပ်သော websites (သို့) accounts များပေါ်၌ ပြန်ထည့်ပေးသည်။ ပိုမိုလုံခြုံမှုရှိစေရန်အတွက် ကူးယူထားသော password သည် ၎င်း clipboard ပေါ်၌ 10 စက္ကန့်ခန့်သာ တည်ရှိနေနိုင်သည်။ထို့ကြောင့် လိုအပ်သောနေရာတွင် သင့်တော်သော password ကို ထည့်သွင်းရန်အတွက် အသင့်ဖွင့်ထားပြီးသော သင်၏ account (သို့) website ကို ရှာဖွေရန် အချိန်ကုန် သက်သာသည်။

အဆင့် 1: Password entry ကို right click လုပ်ပါ။ ကျလာသော စာရင်းမှ လိုအပ်သော password ကို ရွေးချယ်ပါ။

အဆင့် 2: အောက်ပါအတိုင်း ' Copy Password ' ကို ရွေးပါ။



ပုံ 1: KeePass Password Safe screen ပုံ



အဆင့် 3: · သက်ဆိုင်ရာ account (သို့) website ကိုသွား၍ ၎င်းနှင့် ဆီလျော်သောကွက်လပ်တွင် password ကို ထည့်သွင်းထားသော Gmail Account တစ်ခုပုံ

အကြံပြုရန် ။ ။ ကူးယူခြင်း(copying)၊ ထည့်သွင်းခြင်း (pasting) နှင့် windows အမှုဒ်အဝိတ်လုပ်ခြင်းများကို လွယ်ကူလျင်မြန်စေရန် keyboard မှ အတိုကောက် shortcuts များကို အသုံးပြုပါ။ password တစ်ခုကို copy လုပ်ရန် Ctrl key နှင့် C တို့ကို တစ်ပြိုင်နက် နှိပ်ပါ။ ၎င်း password ကို paste လုပ်ရန် Ctrl key နှင့် V တို့ကို တစ်ပြိုင်နက် နှိပ်ပါ။ ဖွင့်ထားသော programs များနှင့် windows တို့အကြား အမှုဒ်အဝိတ်များ လုပ်ဆောင်ရန် Alt နှင့် tab key ကို တစ်ပြိုင်နက် နှိပ်ပါ။

မှတ်ချက် ။ ။ KeePass ကို တစ်ချိန်လုံး အသုံးပြုခြင်းဖြင့် သင်၏ password ကို သိရှိရန် ၊ ကြည့်ရှုရန် လုံးဝ မလိုအပ်ပါ။ Copy /paste လုပ်ဆောင်မှုများက passwords များကို database မှ လိုအပ်သော window သို့ ရွှေ့ပြောင်းရာတွင် ကူညီပေးသည်။ အကယ်၍ သင်သည် အလုည့်သင့်ရာ ထုတ်ပေးသည့် 'Random Generator' ကို အသုံးပြုမည် ဆိုပါစို့။ Email account အသစ်တစ်ခု မှတ်ပုံတင်သည့် လုပ်ငန်းစဉ်တွင် password ကို ' Generator ' မှ တစ်ဆင့်လွှဲပြောင်းရာတွင် သင်တစ်ကြိမ်တစ်ခါမျှ မှန်းဆ မြင်ယောင်ကြည့်၍ပင် မရနိုင်သော passwords မျိုးကို သင်အသုံးပြုရလိမ့်မည်။ ၎င်းသည်လည်း အလုပ်ဖြစ်ဆဲ ဖြစ်သည်။

FAQ and Review (မကြာခဏ မေးလေ့ရှိသော မေးခွန်းများနှင့် သုံးသပ်ချက်)

4.0 : KeePass သည် နီကိုလိုင်နှင့်အယ်လီနာတို့အတွက် အသုံးပြုရ လွယ်ကူသည့် program တစ်ခု ဖြစ်ပုံရသည်။ သူတို့အတွက် အနည်းငယ် ရှုပ်ထွေးသည်ဟု ထင်ရသောအပိုင်းမှာ passwords အသစ်များကို ဖန်တီးသည့် အလေ့အကျင့်ပင် ဖြစ်သည်။ Password တစ်ခုအား တစ်ကြိမ်တစ်ခါမျှ မြင်ခွင့်မရခြင်းကို သမားရိုးကျ ဖြစ်စေရန် အယ်လီနာအား ခက်ခဲစေသည်။ သို့သော် ဤသည်က ၎င်းတို့ကို မှတ်သားရခြင်းထက် ပို၍လွယ်ကူပါသည်။

မေး ။ ။ နီကိုလိုင်၊ KeePass ရဲ့ အသုံးပြုရ လွယ်ကူမှုကိုတော့ ကျွန်မ ကျေနပ်ပါတယ်။ ဒါပေမဲ့ ကျွန်မရဲ့ master password ကို မေ့သွားတဲ့အခါမျိုးမှာ ကျွန်မရဲ့ password databases တွေကို ရယူဖို့ KeePass ကို access လုပ်ရမယ့် အခြားနည်းလမ်း မရှိတော့ဘူးလား။

ဖြေ ။ ။ အော်...ဒါ လွယ်လွယ်လေးပါ။ အဲ မဟုတ်ပါဘူး။ ဆောရီးပဲ အယ်လီနာ။

ဒီလိုကိစ္စမျိုးမှာ မင်း ဘာမှ လုပ်လို့မရဘူး။ အကောင်းဘက်က ကြည့်မယ်ဆိုရင်တော့ အနည်းဆုံး မင်းရဲ့ password database ကို တခြားဘယ်သူမှ access လုပ်လို့ မရတော့ဘူးပေါ့။ ဒီလိုမဖြစ်အောင် လမ်းညွှန်စာအုပ် အခန်း 3 "ကောင်းမွန်သော passwords များကို ဖန်တီးခြင်းနှင့် ပြုပြင်မွမ်းမံခြင်း" အခန်းမှာ ဖော်ပြထားတဲ့ password တစ်ခုကို မှတ်သားရန် နည်းလမ်းများထဲမှ တချို့ကို အသုံးပြုနိုင်ပါတယ်။

မေး ။ ။ ပြီးတော့ တကယ်လို့ KeePass ကို ကျွန်မ 'uninstall' လုပ်ရင် ကျွန်မရဲ့ passwords တွေ ဘာဖြစ်သွားနိုင်လဲ။

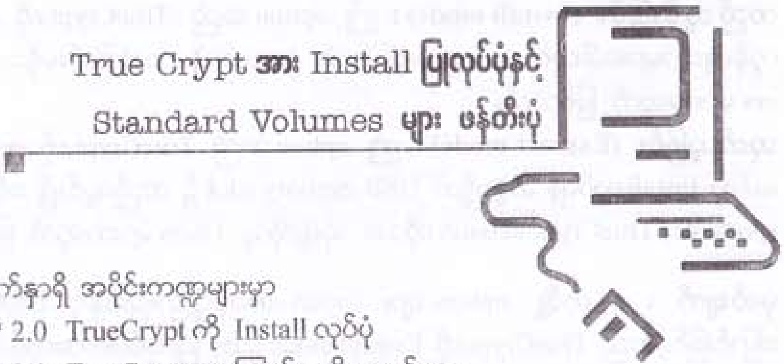
ဖြေ ။ ။ မင်းရဲ့ ကွန်ပျူတာပေါ်မှာရှိတဲ့ program ကို ဖျက်ပစ်လိုက်ပေမဲ့ (.kdb) extension နဲ့ သိမ်းထားတဲ့ file ကတော့ ကွန်ပျူတာပေါ်မှာ ကျန်ခဲ့လိမ့်မယ်။ နောက်တစ်ကြိမ် မင်း KeePass ကို 'install' လုပ်ပြီးတဲ့အခါ အဲဒီ file ကို အချိန်မရွေး ဖွင့်ကြည့်လို့ရတယ်။

မေး ။ ။ ကျွန်မ database file ကို အမှတ်မထင် ဖျက်လိုက်မိတယ်လို့ ထင်တယ်။

ဖြေ ။ ။ မင်းစောစောက Backup တစ်ခု လုပ်ခဲ့လိမ့်မယ်လို့ မျှော်လင့်ရတာပဲ။ နောက်ပြီး အဲဒီ Backup file ကို ဘယ်နေရာမှာ သိမ်းထားတယ်ဆိုတာလဲ မမေ့အောင် သေသေချာချာ ဂရုစိုက်ပါ။ မင်းရဲ့ ကွန်ပျူတာမှာ (.kdb) extension ပါတဲ့ file ကိုပါ ဖျက်မိတယ်ဆိုရင်တော့ လက်စွဲစာအုပ်မှာပါတဲ့ Recuva ကို ကြည့်ပါ။ file ကို ပြန်ရဖို့ မင်းကို ကူညီပါလိမ့်မယ်။

4.1 မေးခွန်းများ သုံးသပ်ချက်

✱ ကြံ့ခိုင်မှုရှိတဲ့ password ဖြစ်အောင် ဘယ်လိုလုပ်သလဲ။
✱ ရှိနှင့်ပြီးသား password entry တစ်ခုကို KeePass မှာ ဘယ်လိုပြုပြင်မလဲ။
✱ KeePass မှာ စာလုံးရေ 30 ရှိတဲ့ password ကို ဘယ်လို ထုတ်ယူမလဲ။



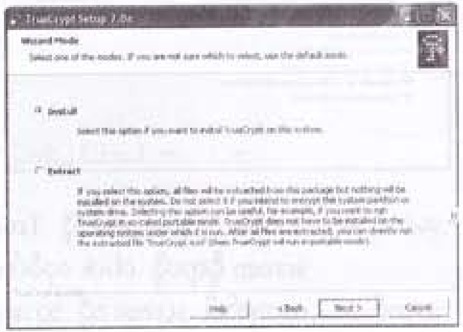
True Crypt အား Install ပြုလုပ်ပုံနှင့် Standard Volumes များ ဖန်တီးပုံ

ဤစာမျက်နှာရှိ အပိုင်းကဏ္ဍများမှာ

* 2.0 TrueCrypt ကို Install လုပ်ပုံ
* 2.1 TrueCrypt အကြောင်း သိကောင်းစရာ
* 2.2 Standard Volume တစ်ခုကို ဖန်တီးခြင်း
* 2.3 USB Memory stick ပေါ်၌ Standard Volume တစ်ခု ဖန်တီးခြင်း
* 2.4 Standard Volume တစ်ခုကို ဖန်တီးခြင်း (အဆက်)

2.0 TrueCrypt ကို Install လုပ်ပုံ

အဆင့် 1: File ဖွင့်ရန် Double click လုပ်ပါ။ လုံခြုံရေး အချက်ပေး ဖယားကွက် (dialog box) ပေါ်လာလိမ့်မည်။ TrueCrypt license screen သို့ သွားရန် click လုပ်ပါ။



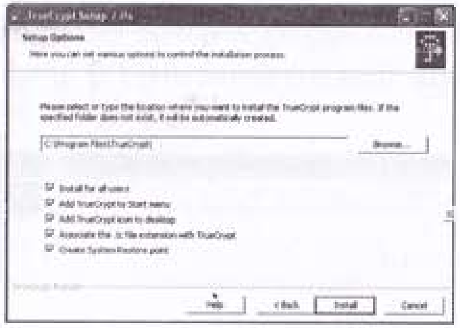
ပုံ 1: Default Install mode အတွင်းရှိ Wizard mode

အဆင့် 2: 'Accept button ကို နှိပ်ရန် License option က ကန့်သတ်ထားသော သဘောတူညီချက်များကို စစ်ဆေးပါ။
အောက်ပါ screen သို့ ရောက်ရန် click လုပ်ပါ။

ထည့်သွင်းခြင်း (Install mode) ၊ ဤ option သည် TrueCrypt ကို ၎င်းတို့၏ ကွန်ပျူတာများပေါ်တွင် တင်ယူသုံးစွဲခြင်းကို ဖုံးကွယ်ရန် အကြောင်းမရှိသည့် Users များအတွက် ဖြစ်သည်။
ထုတ်ယူခြင်း (Extract mode) ၊ ဤ option သည် TrueCrypt ကို ကွန်ပျူတာပေါ်သို့ Install လုပ်ရန် ဆန္ဒမရှိဘဲ USB memory stick ၌ ထည့်သွင်း၍ ခရီးဆောင် (portable) TrueCrypt version ကိုသာ သုံးစွဲလိုသူ Users များအတွက် ဖြစ်သည်။

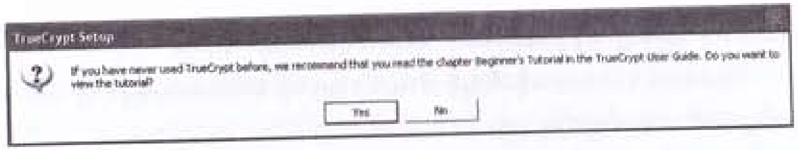
မှတ်ချက် ။ ။ တချို့ option များ (ဥပမာ-အခန်းခွဲခြားခြင်းနှင့် Disk အသွင်ပြောင်းခြင်း)သည် TrueCrypt ကို Extract mode ၌သာ ပြုလုပ်ပါကအလုပ် မလုပ်ပါ။

မှတ်ချက် ။ ။Default Install mode ကို အသုံးပြုရန် ထောက်ခံထားသော်လည်း TrueCrypt ကို Portable mode ၌လည်း အသုံးပြုနိုင်သည်။ TrueCrypt Traveller mode အကြောင်းကို လေ့လာရန် Portable TrueCrypt စာမျက်နှာ၌ ရှာကြည့်ပါ။
အဆင့် 3: အောက်ပါ screen သို့ သွားရန် click လုပ်ပါ။



ပုံ 2: Setup Options window ပုံ

အဆင့် 4: သင်၏ System ပေါ်သို့ TrueCrypt ကို Install လုပ်ရန် Installing screen ရှိရာသို့ click လုပ်ပါ။
အဆင့် 5: အောက်ပါ screen သို့ သွားရန် click လုပ်ပါ။



ပုံ 3: TrueCrypt Setup ကို ပြုလုပ်ရန် သေချာမှုရှိ၊ မရှိ မေးသည့် dialog box

အဆင့် 6: TrueCrypt website ကို ဖွင့်ရန် click လုပ်ပါ။ Installing လုပ်ငန်းစဉ်ကို ပြီးဆုံးအောင် လုပ်ပါ။ ထို့နောက် click လုပ်ပါ။
မှတ်ချက် ။ ။ ဤအဆင့်များ ဆောင်ရွက်ပြီးစီးပါက TrueCrypt ၌ ရရှိနိုင်သော Help files များ၌ အသေးအချာ မေးမြန်းလေ့လာသင်ယူရန် Users အားလုံးကို တိုက်တွန်းပါသည်။

2.1 TrueCrypt အကြောင်း သိကောင်းစရာ

TrueCrypt သည် သင်၏ files များကို password မှန်ကန်မှု မရှိဘဲ ဝင်ရောက် access လုပ်မည့်သူများကို ကာကွယ်ပေးသည့် လုံခြုံရေး program တစ်ခုဖြစ်သည်။ ၎င်းသည် electronic safe တစ်ခုကဲ့သို့ လုပ်ဆောင်သည်။ သင်၏ files များကို lock ချထားပြီး မှန်ကန်မှုရှိသော password နှင့် ဝင်ရောက်မှသာ ရရှိနိုင်မည်။ TrueCrypt က files များကို လုံခြုံစိတ်ချစွာ သိမ်းဆည်းနိုင်ရန် သင်၏ ကွန်ပျူတာပေါ်တွင် အပိုင်းများ (sections) နှင့် volumes များ တည်ဆောက်ခွင့် ပေးသည်။ သင့်အနေနှင့် Data များကို ၎င်းတို့အတွင်း၌ ပြုလုပ်သည်ဖြစ်စေ၊ ပြင်မှ ရွှေ့ပြောင်းယူသည်ဖြစ်စေ TrueCrypt က အချက်အလက်များကို အလိုအလျောက် အသွင်ပြောင်းပေးသည်။ အကယ်၍ ၎င်း file များကို ထုတ်ယူသုံးစွဲမည်ဆိုပါက TrueCrypt ကပင် အလိုအလျောက် မူလပုံစံ ပြန်ပြောင်းပေးသည်။ ၎င်း လုပ်ငန်းစဉ်ကို အမြန်အလုန် အသွင်ပြောင်းခြင်း (on-the-fly encryption) ဟု ခေါ်သည်။

2.2 Standard Volume တစ်ခု ဖန်တီးပုံ

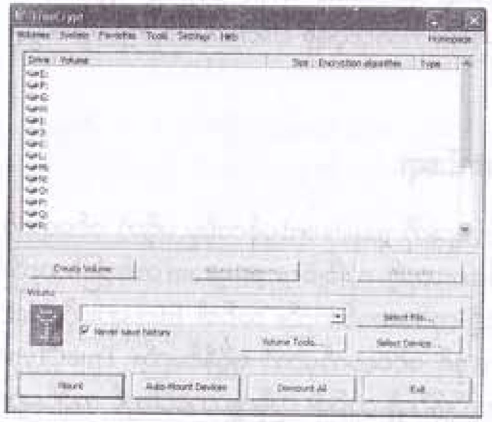
TrueCrypt က သင့်အား Volume အမျိုးအစားနှစ်မျိုးကို ဖန်တီးရန် ခွင့်ပြုသည်။ ၎င်းတို့မှာ ဖုံးကွယ်ထားသော (Hidden) Volume နှင့် Standard Volume တို့ ဖြစ်ကြသည်။ ဤအပိုင်းတွင် သင်၏ files များကို သိမ်းဆည်းရန် Standard

Volume ကို မည်သို့ ဖန်တီးရမည်ကို လေ့လာသင်ယူနိုင်သည်။

Standard Volume ဖန်တီးရန် TrueCrypt ကို စတင်အသုံးပြုရာ၌ အောက်ပါအဆင့်များကို ဆောင်ရွက်ရမည်။

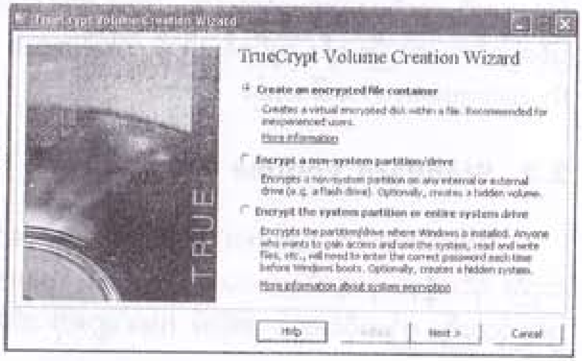
အဆင့် 1: TrueCrypt ကို Double click နှိပ်ခြင်းဖြင့်သော်လည်းကောင်း Start menu မှ Programs>True Crypt>TrueCrypt ကိုသွား၍ ဝင်ရောက်နိုင်သည်။

အဆင့် 2: TrueCrypt pane ၌ ဖော်ပြထားသော စာရင်းရှိ drive တစ်ခုကို ရွေးပါ။



ပုံ 4: TrueCrypt Console ပုံ

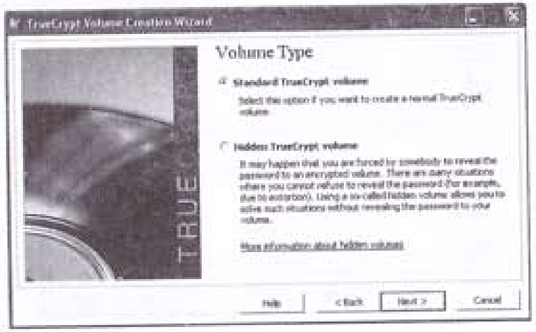
အဆင့် 3: TrueCrypt Volume Creation Wizard ကို အောက်ပါအတိုင်း click လုပ်၍ သွားပါ။



ပုံ 5: TrueCrypt Volume Creation Wizard ပုံ

ပုံ 5 ရှိ TrueCrypt Standard Volume တစ်ခုကို အသွင်ပြောင်း (Encryption)ရာတွင် options သုံးခုရှိသည်။ ဤအခန်းတွင် အသွင်ပြောင်းထားသော file ထည့်သွင်းရန် container ပြုလုပ်ခြင်း option ကို အသုံးပြုကြမည်။ အခြား option နှစ်ခုအတွက် ဖော်ပြချက်များကို TrueCrypt အကြောင်း မှတ်တမ်းမှတ်ရာများ၌ ရှာဖွေကြည့်ရှုနိုင်သည်။

အဆင့် 4: အောက်ပါ screen သို့သွားရန် click လုပ်ပါ။



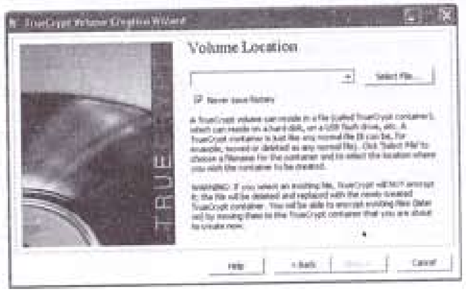
ပုံ 6: Volume Type Window ပုံ

TrueCrypt Volume Creation Wizard ရှိ Volume အမျိုးအစား (Type) window က သင့်အား Standard နှင့် Hidden volume များ ဖန်တီးရန် ရွေးချယ်ခွင့်ပေးသည်။

အရေးကြီး ။ ။ Hidden Volume တစ်ခုကို ဖန်တီးပုံအကြောင်း ထပ်မံသိရှိလိုပါက Hidden Volumes page ၌ ကြည့်ပါ။

အဆင့် 5: Standard TrueCrypt Volume option ကို စစ်ဆေးပါ။

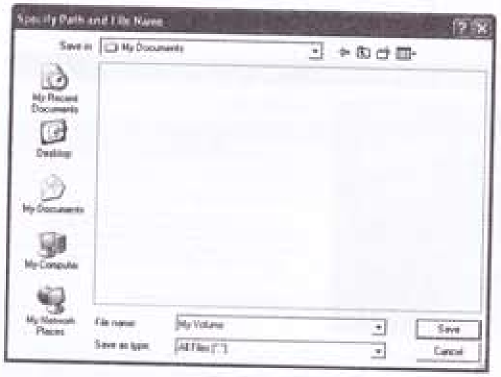
အဆင့် 6: အောက်ပါ screen သို့သွားရန် click လုပ်ပါ။



ပုံ 7: Volume Creation Wizard ရှိ Volume တည်နေရာအလွှာ (location pane) ပုံ

Volume Creation Wizard ရှိ Volume location screen တွင် Standard Volume ကို မည်သည့်နေရာ၌ သိမ်းဆည်းထားမည်ဆိုသည်ကို ခွဲခြားသတ်မှတ်နိုင်သည်။ ဤ file ကို အခြား file များကဲ့သို့ပင် သိမ်းဆည်းနိုင်သည်။

အဆင့် 7: File အမည်ကို text field ထဲသို့ ရိုက်ထည့်ပါ (သို့) အောက်ပါ screen သို့သွားရန် click လုပ်ပါ။

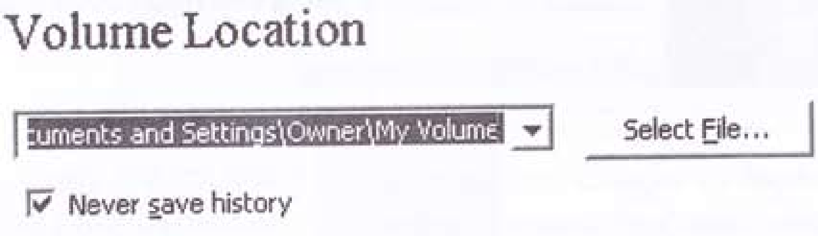


ပုံ 8: သတ်မှတ်ထားသော တည်နေရာနှင့် file အမည်ပြ window ပုံ

မှတ်ချက် ။ ။ TrueCrypt Volume သည် သာမန် file အမျိုးအစား၌ ပါဝင်သည်။ ဆိုလိုသည်မှာ ၎င်း file ကို ရွှေ့ပြောင်းနိုင်သည်။ ကူးယူနိုင်သည်။ ဖျက်ပစ်နိုင်သည်။ File ၏ တည်နေရာနှင့် အမည်တို့ကို မှတ်သားထားရန် လိုအပ်သည်။ သို့သော်လည်း သင် ဖန်တီးထားသည့် volume အတွက် file အမည်သစ်ကို ရွေးချယ်ရမည်။ (အခန်း 2.3 ရှိ USB Memory stick ပေါ်၌ Standard Volume တစ်ခုကို ဖန်တီးခြင်းကိုလည်း ကြည့်ပါ။)။ ဤအခန်းတွင် My Documents Folder ထဲ၌ Standard Volume ကို ဖန်တီးမည်ဖြစ်ပြီး အထက်ပါ ပုံ 8 တွင် ဖော်ပြထားသည့်အတိုင်း File ကို My Volume ဟု အမည်ပေးလိုက်သည်။

သတိပြုရန် ။ ။ သင်သည် မည်သည့် file အမည်နှင့် extensions အမည်ကိုမဆို အသုံးပြုနိုင်သည်။ ဥပမာအားဖြင့် သင်၏ Standard Volume အမည်ကို recipes.doc ဟူ၍လည်းကောင်း (Word document တစ်ခုအဖြစ် ထင်မှတ်စေရန်)၊ holidays.mpg ဟူ၍လည်းကောင်း (movie file တစ်ခုအဖြစ် မှတ်ယူရန်) အသုံးပြုနိုင်သည်။ ၎င်းက သင်၏ Standard Volume တည်ရှိနေခြင်းကို ဖုံးကွယ်ပေးထားနိုင်သည့် နည်းလမ်းတစ်ခုဖြစ်သည်။

အဆင့် 8: အောက်တွင် ဖော်ပြထားသည့်အတိုင်း Volume Creation Wizard window သို့ ပြန်သွားရန် သတ်မှတ်ထားသော တည်နေရာနှင့် file အမည်ပြ window ကို click လုပ်၍ ပိတ်ပါ။



ပုံ 9: Volume တည်နေရာပြအကွက်ကို ပြသထားသော TrueCrypt Volume Creation Wizard ပုံ

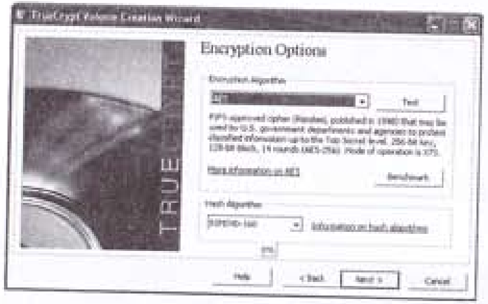
အဆင့် 9: ပုံ 10 သို့သွားရန် click လုပ်ပါ။

2.3 USB Memory stick တစ်ခုပေါ်၌ Standard Volume တစ်ခု ဖန်တီးပုံ

USB Memory stick တစ်ခုပေါ်၌ TrueCrypt Standard Volume တစ်ခု ဖန်တီးရန် အခန်း 2.2 ရှိ Standard Volume ဖန်တီးခြင်း အဆင့် 1 မှ 3 အထိ ပြန်၍ လုပ်ဆောင်ပါ။ File တည်နေရာ ရွေးချယ်ရာတွင် My Documents ကို မရွေးဘဲ USB Memory stick ကို ညွှန်ပြ၍ ရွေးချယ်ပါ။ ထို့နောက် File အမည် တစ်ခုဖြင့် ဝင်ရောက်၍ Standard Volume တစ်ခုကို တည်ဆောက်ပါ။

2.4 Standard Volume တစ်ခု ဖန်တီးပုံ (အဆက်)

ဤအဆင့်တွင် သင်သည် screen ပေါ်၌ ညွှန်းဆိုထားသော တိကျသည့် အသွင်ပြောင်းခြင်း method (သို့) algorithm (ဖြေရှင်းရန်နည်းလမ်း) တစ်ခုကို ရွေးချယ်ရမည်။ ၎င်းက သင်၏ Standard Volume ရှိ data များကို ပြောင်းလဲ (encode) လုပ်ပေးသည်။



ပုံ 10: Volume Creation Wizard ၌ Encryption Options များပုံ

မှတ်ချက် ။ ။ ယခုပေါ်နေသော default options ကို အသုံးမပြုဘဲ ထားခဲ့နိုင်သည်။ Options နှစ်ခုလုံးတွင် ပေးထားသောနည်းလမ်း (algorithms) အားလုံးကို ယုံကြည်စိတ်ချရသည်ဟု မှတ်ယူနိုင်သည်။

အဆင့် 10: အောက်ပါ TrueCrypt Volume Creation Wizard screen သို့သွားရန် click လုပ်ပါ။

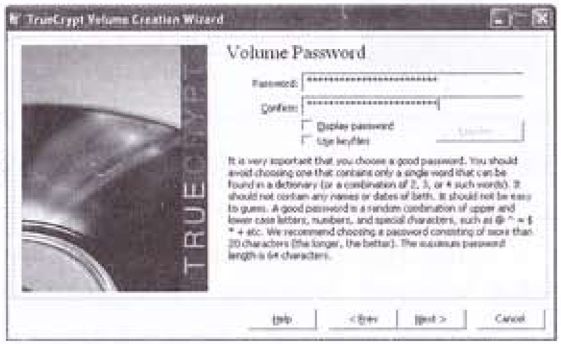
ပုံ : Volume အရွယ်အစား (size) ကို ပြသနေသော Volume Creation Wizard ပုံ

Volume Size က သင့်အား Standard Volume ၏ အရွယ်အစားကို သတ်မှတ်ခွင့်ပေးသည်။ ဤဥပမာတွင် Volume size ကို 10 megabytes ဟု သတ်မှတ်ထားသော်လည်း သင့်အနေဖြင့် အခြား အရွယ်အစား အမျိုးမျိုးတို့ဖြင့် သတ်မှတ်နိုင်သည်။ သင် သိမ်းဆည်းလိုသော documents နှင့် files အမျိုးအစားများ၏ size ကို စဉ်းစားပါ။ ထို့နောက် ၎င်းတို့အတွက် သင့်တော်သော volume size ကို ရွေးချယ်သတ်မှတ်ပါ။

သတိပြုရန် ။ ။ အကယ်၍ သင်၏ Standard Volume ကို CD ပေါ်သို့ Backup

လုပ်မည်ဆိုပါက ၎င်း၏ size ကို 700MB (သို့) ၎င်း အရွယ်အစားထက် လျော့၍ သတ်မှတ်ရမည်။

အဆင့် 11: Text field ထဲသို့ သင်၏ သတ်မှတ်ထားသော volume size ကို ရိုက်ထည့်ပါ။ အောက်ပါ screen သို့သွားရန် click လုပ်ပါ။



ပုံ 12: Volume Password pane ကို ပြသထားသည့် True-Crypt Volume Creation Wizard

အရေးကြီး ။ ။ Standard Volume တစ်ခုကို တည်ဆောက်ရာတွင် မှန်ကန်ပြီး ကြံ့ခိုင်မှုရှိသည့် password တစ်ခုကို ရွေးချယ်ခြင်းက သင်ဆောင်ရွက်ရမည့် အရေးကြီးဆုံး တာဝန်တစ်ရပ် ဖြစ်သည်။ ကောင်းမွန်သော password တစ်ခုသည် သင်၏ အသွင်ပြောင်း (encrypted) volume ကို ကာကွယ်ပေးပြီး ပိုမိုကြံ့ခိုင်မှုရှိသော password ကို ရွေးချယ်ပါက ပိုကောင်းသည်။ KeePass ကဲ့သို့ password ထုတ်ပေးသည့် program တစ်ခုကို သုံးစွဲပါက passwords များကို သင်ကိုယ်တိုင် ဖန်တီးစရာလည်းမလို၊ ၎င်းတို့ကို မှတ်သားစရာလည်း မလိုတော့ပေ။ Password ဖန်တီးခြင်းနှင့် သိမ်းဆည်းခြင်းတို့ အကြောင်းကို လေ့လာရန် KeePass ကို ကိုးကား ကြည့်ရှုပါ။

အဆင့် 12: သင်၏ password ကို ရိုက်ထည့်ပါ။ Confirm text field ထဲ၌လည်း နောက်တစ်ကြိမ် ပြန်ရိုက်ပါ။

အရေးကြီး ။ ။ Text fields နှစ်ခုစလုံးရှိ password များမတူခြင်း 'Next' button သည် disabled ဖြစ်နေလိမ့်မည်။ အကယ်၍ သင်၏ password မှာ လုံခြုံ စိတ်ချရမှု မရှိပါက သင့်အား အကြံပြုသည့် သတိပေးချက်တစ်ခုကို တွေ့ရမည်။
Password ကို ပြန်ပြောင်းရန် စဉ်းစားပါ။ အဘယ်ကြောင့်ဆိုသော် TrueCrypt က သင်ရွေးချယ်ပေးသည့် မည်သည့် password နှင့်မဆို လုပ်ဆောင်နိုင်သော်လည်း

ပုံ 13: Volume Format pane ကို ဖော်ပြထားသော TrueCrypt Volume Creation Wizard

သင်၏ data များမှာ လုံခြုံမှု မရှိသောကြောင့် ဖြစ်သည်။

အဆင့် 13: အောက်ပါ screen သို့ရောက်ရန် click လုပ်ပါ။

TrueCrypt သည် Standard Volume ကို ဖန်တီးရန် အဆင်သင့် ဖြစ်နေပါပြီ။ သင်၏ Mouse ကို TrueCrypt Volume Creation Wizard window ထဲ၌ စက္ကန့် အနည်းငယ်ကြာ အလိုက်သင့် လှုပ်ရှားပေးပါ။ Mouse ကို ကြာကြာရွှေ့လေ encryption key ၏ အရည်အသွေး ပိုကောင်းလေဖြစ်သည်။

အဆင့် 14: Standard Volume ကို စတင်ဖန်တီးရန် click လုပ်ပါ။

အစောပိုင်းက ဖော်ပြခဲ့သည့်အတိုင်း TrueCrypt က My Volume အမည်ရှိ file ကို My Documents folder ထဲ၌ တည်ဆောက်လိမ့်မည်။ ၎င်း file ၌ TrueCrypt Volume ပါဝင်လိမ့်မည်။ ၎င်း Volume သည် အရွယ်အစား 10 MB ရှိပြီး သင်၏ files များကို လုံခြုံစိတ်ချစွာ သိုလှောင်သိမ်းဆည်းနိုင်သည်။

Standard Volume ကို အောင်မြင်စွာ တည်ဆောက်ပြီးပါက အောက်ပါ dialog box ကို တွေ့ရမည်။

ပုံ 14: Message screen ကို အောင်မြင်စွာ ဖန်တီးထားသော TrueCrypt volume ပုံ

အဆင့် 15: Standard Volume တည်ဆောက်ခြင်း ပြီးပြည့်စုံအောင် click လုပ်ပါ။ ထို့နောက် TrueCrypt console သို့ ပြန်ပါ။

အဆင့် 16: TrueCrypt Volume Creation Wizard ကို ပိတ်ရန် click လုပ်ပါ။

TrueCrypt – လုံခြုံစိတ်ချရသော ဖိုင်သိမ်းဆည်းမှု

TrueCrypt က မှန်ကန်သည့် password မပါဘဲ ဝင်ရောက်မှုများကို ကာကွယ်ထားခြင်းဖြင့် သင်၏ ဖိုင်များကို လုံခြုံမှုရရှိ စေသည်။ ၎င်းက သင်လုံခြုံစွာ သိမ်းဆည်းထားသော ဖိုင်များကို အသုံးပြုနိုင်ရန် လျှပ်စစ်စွမ်းအားသုံး လုံခြုံရေးစနစ်တစ်ခုကဲ့သို့ လုပ်ဆောင်ပေးသည်။

TrueCrypt ကို download လုပ်ယူခြင်း

* လက်စွဲလမ်းညွှန်ပါ မိတ်ဆက်နိဒါန်းကို ဖတ်ပါ။
* www.truecrypt.org/downloads ကို ဖွင့်ရန် အောက်ခြေရှိ TrueCrypt iconကို click လုပ်ပါ။
* နောက်ဆုံးတည်ငြိမ်မှုရှိပြီးသော ပုံသဏ္ဍာန် (Latest Stable Version) အောက်ခြေရှိ windows section မှ Download ခလုတ်ကို click လုပ်ပါ။
* သင်၏ ကွန်ပျူတာတွင် ထည့်သွင်းရန် software ကို သိမ်း (save) ပါ။ ၎င်းအား ရှာဖွေပြီး double click လုပ်ပါ။
* လုပ်ဆောင်မှုမစခင် အောက်ရှိ ညွှန်ကြားချက်များကို ဖတ်ပါ။
* သင်၏ ကွန်ပျူတာတွင် TrueCrypt ကို ပြီးပြည့်စုံအောင် ထည့်သွင်းပြီးပါက ၎င်း၏ထည့်သွင်းခြင်း (Installation) program ကို ဖျက်လိုက်ပါ။ TrueCrypt အသုံးပြုရန် လမ်းညွှန်ပါအချက်အလက်များမှာ အောက်ပါအတိုင်း ဖြစ်သည်။
* မူရင်းစာမျက်နှာ (Homepage) မှာ www.truecrypt.org ဖြစ်သည်။
* ကွန်ပျူတာ လိုအပ်ချက်များမှာ Windows 2000/XP/2003/Vista/7 ထည့်သွင်း ခြင်းဖြင့် (installation) သို့မဟုတ် volumes ဖန်တီးခြင်းအတွက် စီမံကွပ်ကဲသူ (administrator) ခွင့်ပြုမှုလိုအပ်ပြီး တည်ရှိပြီးသော volumes များကို access မလုပ်ရပါ။

* ဤလမ်းညွှန်တွင် အသုံးပြုထားသော Versions အမျိုးအစားများမှာ 7.0a ဖြစ်သည်။
* License သဘောတူညီချက်မှာ ရှင်းလင်းပြီး အခမဲ့ဖြစ်သော Sofrware အမျိုးအစားဖြစ်သည်။
* ဖတ်ထားသင့်သော အကြောင်းအရာမှာ အခန်း 4 ရှိ 'သင်၏ ကွန်ပျူတာရှိ ထိခိုက်လွယ်သော ဖိုင်များကို ကာကွယ်ပုံ' ဖြစ်သည်။
* အဆင့် သတ်မှတ်ချက်မှာ (Standard Volumes) အတွက်
  1: Beginner, 2: Average, 3: Intermediate, 4: Experienced, 5: Advanced ဖြစ်ကြပြီး (Hidden Volumes) အတွက် 1: Beginner, 2: Average, 3: Intermediate, 4: Experienced, 5: Advanced တို့ ဖြစ်ကြသည်။
* စတင် အသုံးပြုရန် ကြာသောအချိန်မှာ Standard Volumes အတွက် 30 မိနစ်၊ Hidden Volumes အတွက် 30 မိနစ် ဖြစ်သည်။
* သင်ရရှိမည့် အကျိုးကျေးဇူးများမှာ သင်၏ ဖိုင်များကို ဖျက်ဆီးသူများ(သို့) ခွင့်ပြုချက်မရဘဲ access လုပ်မှုများအတွက် အကျိုးရှိရှိ ကာကွယ်နိုင်သည့် စွမ်းရည်၊ သင်၏အရေးပါသော file များ၏ မူပွား (copies) များကို လွယ်ကူ လုံခြုံစွာ သိမ်းဆည်းနိုင်သည့် စွမ်းရည်တို့ ဖြစ်ကြသည်။

GNU Linux, Mac OS နှင့် Microsoft မှ ထုတ်လုပ်သော windows programs များ

မှတ်ချက် ။ ။ GNU Linux နှင့် Mac OS များတွင် TrueCrypt ကို အသုံးပြုကြရန် အထူးတလည် လမ်းညွှန်ပါသည်။

GNU Linux ထုတ်ဝေမှုများ (ဥပမာ– Ubuntu) သည် disk တစ်ခုလုံးကို အပြန်အလှန် encryption နှင့် decryption ပြုလုပ်ရန်အတွက် standard feature တစ်ခု ထုတ်ပေးထားသည်။ သင့်အနေဖြင့် System တစ်ခုလုံးကို ကွန်ပျူတာပေါ်သို့ ထည့်သွင်းချိန်တွင် ၎င်းကို အသုံးပြု မပြုကို ဆုံးဖြတ်နိုင်သည်။ dm-crypt၊ cryptsetup နှင့် LUKS တို့ကို ပေါင်းစပ်ပြီး integrate ပြုလုပ်ထားသည်ကို အသုံးပြုခြင်းဖြင့် encryption လုပ်ငန်းစဉ်များကို သင်၏ Linux system သို့ ပေါင်းထည့်နိုင်သည်။ အခြားနည်းလမ်းတစ်ခုမှာ ရှင်းလင်းပြီး အခမဲ့ဖြစ်သော အပြန်အလှန် encryption နှင့် decryption ပြုလုပ်ပေးသည့် program ဖြစ်သည့် Linux SD4L အတွက် Scram Disk ကို အသုံးပြုရန် ဖြစ်သည်။

Mac OS system အတွက် File Vault ကို အသုံးပြုနိုင်သည်။ ၎င်းသည် operating system ၏ အစိတ်အပိုင်းတစ်ခုဖြစ်ပြီး သင်၏ home folder နှင့် ၎င်းနှင့်တွဲလျက် folder အားလုံး၏ file များကို encryption နှင့် decryption ပြုလုပ်ပေးနိုင်သည်။ အခြားသော free program တစ်ခုဖြစ်သည့် 'Encrypt This' program သည်လည်း အသုံးဝင်ကြောင်း တွေ့ရမည်။ သင်၏ ရွေးချယ်ထားသော file များကို ၎င်းက .DMG ပုံရိပ် (disk image) အဖြစ် အသွင်ပြောင်းပေးသည်။

Microsoft မှ ထုတ်လုပ်သော windows (os) များအတွက် အသုံးပြုရန် Encryption program များစွာရှိသည်။ တစ်ချို့ ကို အောက်တွင် လမ်းညွှန်ပေးထားသည်။

* 'Free CompuSec' သည် အခမဲ့ program ဖြစ်ပြီး encryption နှင့် decryption နှစ်မျိုးလုံး လုပ်ဆောင်ပေးသည့် အသုံးပြုရန် သင့်လျော်သော program ဖြစ်သည်။ ၎င်းသည် CD (သို့) USB drives (သို့) computer disk တစ်ခုလုံးကို လည်းကောင်း၊ အစိတ်အပိုင်းငယ်တစ်ခုစာသာလည်းကောင်း အသွင်ပြောင်း (encrypt) လုပ်နိုင်သည်။ 'CompuSec' ရှိ 'DataCrypt' အပိုင်းမှလည်း file တစ်ခုချင်းစီကို encrypt လုပ်နိုင်သည်။
* 'CryptoExpert 2009 Lite' software သည် အခမဲ့ဖြစ်ပြီး encryption နှင့် decryption နှစ်မျိုးစလုံး ဆောင်ရွက်နိုင်သည်။ ၎င်းက 'TrueCrypt' ကဲ့သို့ file များကို encryption ပြုလုပ်ပြီး သိုလှောင်ရန် နေရာတစ်ခု ဖန်တီးပေးသည်။
* 'AxCrypt' သည်လည်း အခမဲ့ software ဖြစ်ပြီး သီးခြားဖြစ်နေသော files များကို encrypt လုပ်ပေးသည်။
* 'Steganos LockNote' သည် အခမဲ့ program ဖြစ်ပြီး အက္ခရာစာလုံးများ (text) ကို encrypt (သို့) decrypt ပြုလုပ်နိုင်သည်။ ၎င်း 'text' ကို 'LockNote' ၏ application တွင် သိမ်းဆည်းနိုင်သည်။ 'note' တစ်ခုကို encrypt (သို့) decrypt လုပ်ရန် အသုံးပြုသည့် လုပ်ငန်းစဉ်မှာလည်း ၎င်း 'LockNote' ၏ အစိတ်အပိုင်း ဖြစ်သည်။ 'LockNote' သည် အသုံးပြုရ လွယ်ကူသည့် အိတ်ဆောင်အမျိုးအစားဖြစ်ပြီး installation ပြုလုပ်ရန် မလိုအပ်ပါ။

1.1 အသုံးမပြုခင် သိသင့်သောအကြောင်းအရာများ

TrueCrypt က သင်ဖန်တီးထားသော password အကူအညီဖြင့် သင်၏ data များကို access လုပ်ခြင်းကို သော့ပိတ်ထားခြင်း (locking) အားဖြင့် အကာအကွယ်ပေးသည်။ သင် password ကို မေ့သွားပါက သင်၏ data များကို access လုပ်ခွင့် ဆုံးရှုံးလိမ့်မည်။ TrueCrypt က သင်၏ files များကို ကာကွယ်ရန် 'encryption' ဟူသည့် လုပ်ငန်းစဉ်တစ်ရပ်ကို အသုံးပြုသည်။ အချို့သော နိုင်ငံများတွင် 'encryption' ကို အသုံးပြုခြင်းသည် တရားဝင်သောနည်းလမ်း မဟုတ်သည်ကို စိတ်တွင် မှတ်သားထားပါ။ Files တစ်ခုချင်းစီကို encrypt လုပ်ခြင်းထက် TrueCrypt က သင်၏ ကွန်ပျူတာပေါ်တွင် volume ဟုခေါ်သည့် အကာအကွယ်ပေးမည့်နေရာတစ်ခုကို ပြုလုပ် ပေးသည်။ သင်၏ files များကို ဤ အသွင်ပြောင်း (encrypted) volume အတွင်း၌ လုံခြုံစွာ သိမ်းဆည်းနိုင်သည်။

TrueCrypt က ဖုံးကွယ်ထားသော (hidden) volume နှင့် စံချိန်စံညွှန်းမီ အသွင်ပြောင်း (encrypted) volume တို့ကို ဖန်တီးရန် အခွင့်အရေးပေးသည်။ နှစ်ခုစလုံးက သင်၏ files များအတွက် ယုံကြည်မှုရှိစေသော်လည်း Hidden Volumeသည် သင်၏ TrueCrypt volume ကို အများသိသာအောင် ထုတ်ဖော်ခြင်းခံရလျှင်တောင်မှ သင်၏ ထိခိုက်လွယ်သော data များကို ကာကွယ်ရန် အရေးကြီးသော သတင်းအချက်အလက်များကို ဖုံးကွယ်ပေးသည်။ အောက်ပါ လမ်းညွှန်ချက်က ၎င်း volume နှစ်ခုစလုံး၏ အသေးစိတ်အကြောင်းအရာများကို ရှင်းပြထားသည်။

* TrueCrypt အား Install ပြုလုပ်ပုံနှင့် Standard Volumes များ ဖန်တီးပုံ
* Standard Volume ကို အစီအစဉ်တကျဖြစ်အောင် ဆောင်ရွက်ပုံ
* သင်၏ Volume ကို မှပွား (back up) ပြုလုပ်ပုံ
* ဖုံးကွယ်ထားသော (Hidden) volumes များ
* မကြာခဏမေးလေ့ရှိသော မေးခွန်းများနှင့် သုံးသပ်ချက်

Standard Volume ကို အစီအစဉ်ကျအောင် ပြုလုပ်ပုံ

ဤစာမျက်နှာရှိ အပိုင်းကဏ္ဍများမှာ

* 3.0 Standard Volume ကို အစီအစဉ်ကျအောင် ပြုလုပ်ပုံ
* 3.1 Standard Volume ၏ ပုံစံ အစီအစဉ်ကို ဖျက်သိမ်းပုံ

3.0 Standard Volume ကို အစီအစဉ်ကျအောင် ပြုလုပ်ပုံ

TrueCrypt တွင် Standard Volume တစ်ခုကို အစီအစဉ်ကျအောင် ပြုလုပ်ခြင်းဆိုသည်မှာ ၎င်း standard volume ကို အသုံးပြုရန် အဆင်သင့် အနေအထား ရရှိအောင် ဆောင်ရွက်ခြင်းဖြစ်သည်။ ဤအပိုင်းတွင် သင် အသစ်ဖန်တီးထားသော Standard Volume ကို အစီအစဉ်ကျအောင် မည်သို့မည်ပုံ ပြုလုပ်ရမည်ဆိုသည်ကို လေ့လာနိုင်သည်။

သင်၏ standard volume ကို စီစဉ်ခြင်း (mount) လုပ်ရန် အောက်ပါ အဆင့်များကို လုပ်ဆောင်ပါ။

အဆင့် 1: TrueCrypt ကိုဖွင့်ရန် double click (သို့မဟုတ်) Start> programs>TrueCrypt>TrueCrypt ကို ရွေးပါ။

အဆင့် 2: ဖော်ပြထားသည့် စာရင်းမှ Drive တစ်ခုခုကို ရွေးချယ်ပါ။

ပုံ 1: TrueCrypt Console ပုံ

ဤဥပမာတွင် Standard Volume ကို M:drive အဖြစ် သတ်မှတ်လုပ်ဆောင်မည်။

မှတ်ချက် ။ ။ ပုံ 1 တွင် M:drive ကို Standard Volume အား Mount လုပ်ရန် ရွေးချယ်ထားသော်လည်း သင်နှစ်သက်ရာ drive တစ်ခုခုကိုလည်း ပြောင်းလဲ ရွေးချယ်နိုင်သည်။

အဆင့် 3: Click လုပ်ပါ။

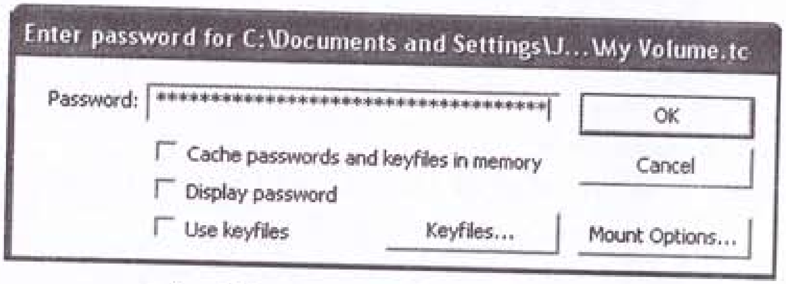
အောက်ပါအတိုင်း TrueCrypt Volume ရွေးချယ်ရန် screen တစ်ခု ပေါ်လာလိမ့်မည်။

ပုံ 2: 'Select a TrueCrypt Volume' screen ပုံ

အဆင့် 4: သင်ပြုလုပ်ထားသော standard volume ဖိုင်ကို ရွေးပါ။ ပုံ 2: ကိုပိတ်ပြီး TrueCrypt သို့ ပြန်သွားပါ။

အဆင့် 5: Password ရိုက်ရန် သတိပေးသည့် screen သို့ သွားရန် click လုပ်ပါ။

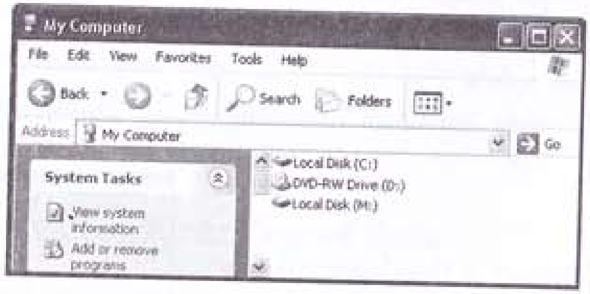
အဆင့် 6: Password ရိုက်ရန်နေရာတွင် password ကို ရိုက်ထည့်ပါ။



ပုံ 3: 'Enter password prompt' screen ပုံ

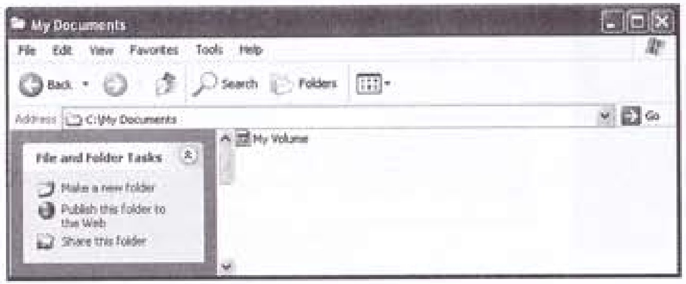
အဆင့် 7: Standard Volume ကို အစီအစဉ်ချခြင်း (mounting) စတင်ရန် click လုပ်ပါ။

မှတ်ချက် ။ ။ သင်ရိုက်ထည့်သော password သည် မှားနေပါက TrueCrypt က password ကို ပြန်ရိုက်ရန် သတိပေးလိမ့်မည်။ ထို့နောက် click လုပ်ပါ။ Password မှန်ကန်မှုရှိပါက Standard Volume ကို အောက်ပါအတိုင်း အစီအစဉ် ကျအောင် ဆောင်ရွက်ပေးသည်။



ပုံ 4: Standard Volume ကို အစီအစဉ်တကျဖြစ်အောင် စတင် ဆောင်ရွက်နေခြင်းကို ပြသသော TrueCrypt console ပုံ

အဆင့် 8: TrueCrypt အတွင်းရှိ အမှတ်အသား (high light) လုပ်ထားသော entry နေရာတွင် double click လုပ်ပါ (သို့မဟုတ်) 'My Computer' screen တွင် သက်ဆိုင်ရာ drive ၏ စာလုံးအမည်ကို click လုပ်ပါ။ ၎င်းက သင်၏ ကွန်ပျူတာပေါ်ရှိ drive : M ပေါ်တွင် mounted လုပ်ထားသော Standard Volume ကို access လုပ်ရန်ဖြစ်သည်။

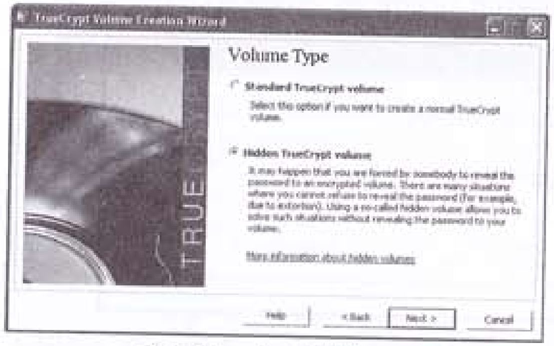


ပုံ 5: 'My Computer' screen မှ Standard Volume ကို access လုပ်ခြင်းပုံ

မှတ်ချက် ။ ။ ကျွန်ုပ်တို့သည် My Volume ရှိ standard volume ကို အမှန်တကယ် ရှိသည်ဟု ထင်ရအောင် ပြုလုပ်ထားသော virtual disk : M အပေါ်တွင် အစီအစဉ်တကျ ဖြစ်အောင် လုပ်ဆောင်ပြီး ဖြစ်သည်။ ၎င်း virtual disk သည် အစစ်အမှန် disk တစ်ခုကဲ့သို့ ပြုမူဆောင်ရွက်ပြီး ၎င်း disk တစ်ခုလုံးကို encryption လုပ်ထားသည်။

မည်သည့် file ကိုမဆို ၎င်း virtual disk ပေါ် သို့ ကူးယူခြင်း၊ ရွှေ့ပြောင်းခြင်း၊ သိမ်းဆည်းခြင်းတို့ ပြုလုပ်ပါက အဆိုပါ file များကို အလိုအလျောက် encrypt လုပ်ပေးသည်။ ၎င်းမှာ on-the-fly encryption လုပ်ငန်းစဉ် ဖြစ်သည်။ သင်သည် Standard Volume ရှိ files များကို အခြားသော ပုံမှန် disk များမှာကဲ့သို့ ကူးယူခြင်း၊ ၎င်းဆီသို့ ရွှေ့ပြောင်းခြင်းများကို ပြုလုပ်နိုင်သည်။ (ဥပမာ-drag-drop file) Standard Volume မှ file တစ်ခုကို သင်ထုတ်ယူသည်နှင့် တစ်ပြိုင်နက် ၎င်း file ကို မူလပုံစံ အသွင်ပြောင်း (decrypt) ပြုလုပ်ပြီးဖြစ်သည်။ ထို့အတူ Standard Volume ပေါ်သို့ file တစ်ခုကို ရွှေ့ပြောင်းပါက TrueCrypt က ၎င်း file ကို အလိုအလျောက် အသွင်ပြောင်း (encrypt) လုပ်ပေးသည်။ သင်၏ ကွန်ပျူတာ ရုတ်တရက် ချို့ယွင်းခြင်း၊ မီးပျက်ခြင်းတို့ ကြုံရပါက TrueCrypt က Standard Volume ကို ချက်ချင်း ပိတ်ပေးသည်။

အရေးကြီး ။ ။ TrueCrypt volume သို့ files များကို ရွှေ့ပြောင်းရာတွင် ၎င်းတို့ မူလတည်ရှိရာနေရာ (ဥပမာ– ကွန်ပျူတာနှင့် USB memory stick)များတွင် ၎င်း file များ၏ သက်သေအမှတ်အသားများ ကျန်ရစ်ခဲ့ခြင်း မရှိစေရန် သတိပြုပါ။ အခန်း 6 ရှိ ထိခိုက်လွယ်သော သတင်းအချက်အလက်များ ဖျက်ဆီးပုံကို ကြည့်ပါ။

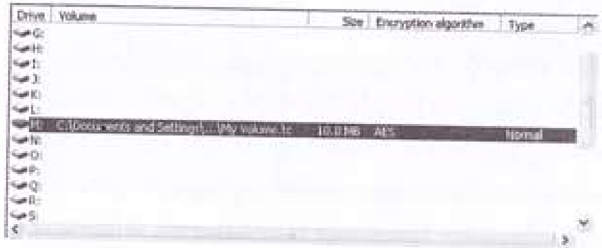


3.1 Standard Volume ၏ ပုံစံအစီအစဉ်ကို ဖျက်သိမ်းပုံ

TrueCrypt တွင် Standard Volume ၏ ပုံစံအစီအစဉ်ကို ဖျက်သိမ်းခြင်း ဆိုသည်မှာ volume တစ်ခုကို အသုံးပြုရန် အနေအထားမရှိအောင် ပြုလုပ်ခြင်းပင် ဖြစ်သည်။

Standard Volume ကို ပိတ်ရန် (သို့) password လက်ဝယ်ရှိသူ တစ်စုံတစ်ယောက်ကိုသာ ၎င်း၏ ဖိုင်များကို access လုပ်ခွင့်ပေးရန် အောက်ပါ အဆင့်အတိုင်း ဆောင်ရွက်ရမည်။

အဆင့် 1: ပင်မ TrueCrypt window ရှိ mounted volumes များမှ volume တစ်ခုကို ရွေးပါ။



ပုံ17: Standard Volume က dk dismount လုပ်ရန် ရွေးချယ်ထားပုံ

အဆင့် 2: သင်၏ TrueCrypt standard volume ကို ပိတ်ပါ။ သို့မဟုတ် dis-mount လုပ်ရန် click လုပ်ပါ။

အရေးကြီး ။ ။ TrueCrypt ကို dismount မလုပ်မီ ၎င်းကို အသင့်အနေအထား (standby) (သို့) (Hibernate) modes များတွင် မထားရှိကြောင်း သေချာအောင်လုပ်ပါ။ ပို၍ကောင်းသည်မှာ သင်၏ ကွန်ပျူတာကို အလုပ်မလုပ်သည့်အချိန်များတွင် သင် တစ်နေရာရာသို့ သွားမည်ဆိုပါက အမြဲတမ်း ပိတ်ထားသင့်သည်။

၎င်းက သင်၏ volume password ကို တစ်စုံတစ်ယောက်က ရယူခြင်းမှ ကာကွယ်ပေးသည်။

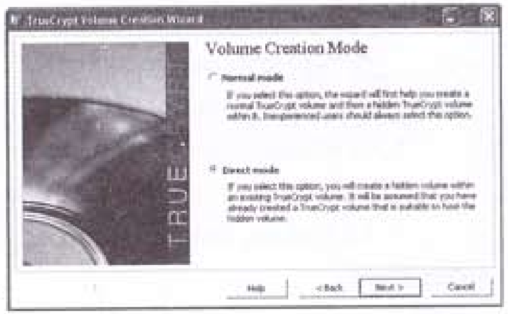
သင် dismount လုပ်ထားသော volume အတွင်းရှိ file ကို ပြန်လည်ရယူလိုပါက volume ကို mount ပြန်လုပ်ရမည်။

သင်၏ Volume ကို Back up ပြုလုပ်ပုံ

သင်၏ မှတ်တမ်းများ (documents) ဖိုင်များနှင့် folders များကို အခြေခံ နည်းစနစ်ပေါ်တွင် မူပွား ပြုလုပ်ခြင်းသည် ချို့ယွင်းချက်များ ရှိသည်။ TrueCrypt volume ကို မူပွားပြုလုပ်ခြင်းသည် မဖြစ်မနေ ပြုလုပ်သင့်ပြီး ကံအားလျော်စွာ လုပ်ဆောင်ရန်လည်း လွယ်ကူပါသည်။ Back up မလုပ်မီတွင် သင်၏ volume ကို dismount လုပ်ရန် မမေ့ပါနှင့်။

အဆင့် 1- Standard Volume ဖိုင်ဆီသို့ သွားပါ။ (ပုံ 1 တွင် My Documents အတွင်းရှိ standard volume တည်ရှိသည်)

ပုံ 1: My Volume file ကို ဖော်ပြထားသော My Documents window ပုံ



အဆင့် 2: File ကို CD၊ DVD (သို့) USB memory stick ကဲ့သို့ ပြင်ပ သိမ်းဆည်းသည့် ကိရိယာထဲသို့ သိမ်း (save) ပါ။

သတိပြုရန် ။ ။ သင်၌ ရေရှည်ထိန်းသိမ်းရန် အသွင်ပြောင်းခြင်း၊ ကူးယူခြင်းတို့ ပြုလုပ်လိုသော data များစွာရှိပါက CD (သို့) DVD တို့၏ အရွယ်အစား (size) ရှိသော Standard Volume အသစ်တစ်ခုကို ဖန်တီးသင့်သည်။ ၎င်းသည် လုံခြုံမှုရှိသော သိုလှောင်သိမ်းဆည်းမှု နည်းစနစ်ဖြစ်သည်။ Standard Volume ကို ရွှေ့ပြောင်း တပ်ဆင်နိုင်သော device တစ်ခုသို့ back up မလုပ်မီ ၎င်း device၏ အရွယ်အစား သည် သင့် volume ၏ အရွယ်အစားနှင့် ဆီလျော်မှု ရှိ၊ မရှိ သေချာအောင် ပြုလုပ်ပါ။
ဖုံးကွယ်ထားသော Volumes များ

Back up ပြုလုပ်မည့် ကြားခံ ပစ္စည်း	ရှိသင့်သော TrueCrypt volume အရွယ်အစား
CD	700 mb
DVD	3900 mb
USB memory stick	စုစုပေါင်း ဝင်ဆံ့သည့် ပမာဏ၏ 25 ရာခိုင်နှုန်း (ဥပမာ 128 MB ရှိသော USB stick တစ်ခုတွင် သင်၏ Standard Volume အရွယ်အစားသည် 3 0 M B ရှိသင့်သည်။)

ဤစာမျက်နှာရှိ ခေါင်းစဉ်များမှာ

* 5.0 ဖုံးကွယ်ထားသော (Hidden) Volumes များအကြောင်း
* 5.1 Hidden Volume တစ်ခု ဖန်တီးပုံ
* 5.2 Hidden Volume ကို အစီအစဉ်တကျ (mount) ရှိအောင် ပြုလုပ်ပုံ
* 5.3 Hidden disk ရှိ လုပ်ဆောင်မှုများကို လုံခြုံစိတ်ချစွာ အသုံးပြုရန် နည်းလမ်းများ

5.0 Hidden Volumes များအကြောင်း

TrueCrypt တွင် Hidden Volume ကို သင်၏ အသွင်ပြောင်းထားသော Standard volume အတွင်း၌ သိမ်းဆည်းထားသော်လည်း ၎င်းတည်ရှိနေပုံကို ဖုံးကွယ်ထားသည်။ သင်၏ standard volume ကို mount လုပ်လျှင်သော်မှ ၎င်း Hidden Volume တည်ရှိနေခြင်းကို သက်သေပြခြင်း (သို့) ၎င်းကို ရှာဖွေခြင်းငှာ မဖြစ်နိုင်ပါ။ သင်၏ Standard volume တည်နေရာနှင့် ၎င်းအတွင်းရှိ အချက်အလက်များ၊ ၎င်း၏ password တို့ကို အကြောင်းတစ်စုံတစ်ရာကြောင့် ဖော်ထုတ်လိုက်ရသော်လည်း Hidden volume ကိုမူ မဖော်ထုတ်နိုင်ပါ။

လျှို့ဝှက်အတွင်းအိတ်များ ပါဝင်သော လက်ဆွဲအိတ်တစ်လုံးကို မြင်ယောင်ကြည့်ပါ။ သင့်အနေဖြင့် အရေးမကြီးဟု ယူဆရသော၊ ပျောက်ဆုံးသော်လည်း ပြဿနာမရှိနိုင်သော ဖိုင်များကို သာမန်နေရာ၌သာ သင်သိမ်းမည်ဖြစ်သည်။ အရေးကြီး၍ ကိုယ်ရေးကိုယ်တာ အကြောင်းအရာများ ပါဝင်သော ဖိုင်များကိုမူ လျှို့ဝှက်အကန့်တွင် သင် သိမ်းလိမ့်မည်။ လျှို့ဝှက်အကန့် (အထူးစီမံပြုလုပ်ထားသော) ဆိုသည်မှာ ၎င်းရှိနေသည့်အကြောင်းကို ၎င်းကို အသုံးပြုသူမှတစ်ပါး အခြားမည်သူမျှ မသိရှိစေနိုင်ပါ။ ထို့အတူ ၎င်းတွင် သိမ်းဆည်းထားသည့် အကြောင်းအရာများကိုလည်း ရှာမတွေ့စေနိုင်ပါ။

5.1 Hidden Volume တစ်ခု ဖန်တီးပုံ

TrueCrypt hidden volume ပြုလုပ်ပုံနှင့် standard volume ပြုလုပ်ပုံမှာ အတူတူပင်ဖြစ်သည်။ တချို့သော window အသွင်အပြင် ပုံစံများမှာလည်း အတူတူ ဖြစ်သည်။

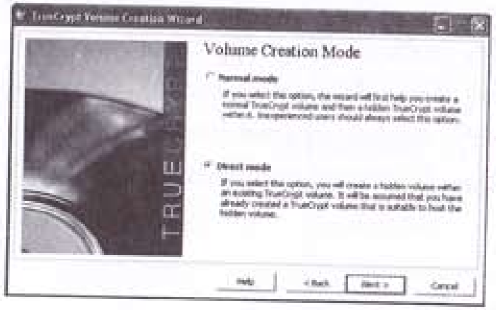
အဆင့် 1: TrueCrypt ကို ဖွင့်ပါ။
အဆင့် 2: 'TrueCrypt Volume Creation Wizard' ကို သွားရန် click လုပ်ပါ။
အဆင့် 3: ပေးထားသော အသွင်ပြောင်းဖိုင်ပါဝင်သည့်နေရာကို ဖန်တီးရန် option ကို လက်ခံပါ။
အဆင့် 4: Hidden TrueCrypt volume ၏ option များကို စစ်ဆေးပါ။

Hidden Volume

The volume cluster bitmap has been scanned and the maximum possible size of the hidden volume has been determined. In the next steps you will set the options, the size, and the password for the hidden volume.

ပုံ 1: Hidden volume option လုပ်ဆောင်ရန် အသင့်ရှိပုံကို ပြသထားသော TrueCrypt Volume Creation Wizard

အဆင့် 5: အောက်ပါ screen ကို လုပ်ဆောင်ရန် click လုပ်ပါ။



ပုံ 2: TrueCrypt Volume Creation Wizard-Mode window ပုံ

* Direct mode : ရှိပြီးသား Standard Volume အတွင်း၌ Hidden Volume တစ်ခု တည်ဆောက်ခွင့် ပေးသည်။
* Normal mode : Hidden Volume ကို သိမ်းထားရန် ပြီးပြည့်စုံသော Standard Volume အသစ်တစ်ခု တည်ဆောက်ခွင့် ပေးသည်။

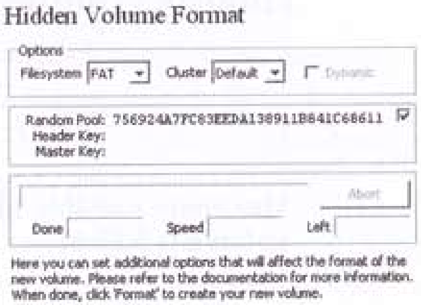
ယခု ဥပမာတွင် Direct mode ကို အသုံးပြု၍ ပြသမည်။

မှတ်ချက် ။ ။ Standard Volume ကို အသစ်ပြုလုပ်ခြင်းဖြင့် စတင်လိုပါက အပိုင်း 2.2 ရှိ Standard Volume ဖန်တီးပုံ လုပ်ငန်းစဉ်ကို ပြန်သွား၍ လုပ်ဆောင်ပါ။

အဆင့် 6: Direct mode ကို စစ်ဆေးပြီး TrueCrypt volume ဖန်တီးခြင်း (creation)- Volume တည်နေရာ (Location) window ကို သွားပါ။

မှတ်ချက် ။ ။ Standard Volume ကို မရွေးမီ ၎င်းအား အစီအစဉ်မချရသေးကြောင်း (unmounted) စစ်ဆေးပါ။

အဆင့် 7: အောက်ပါ screen သို့ သွားရန် click လုပ်ပါ။



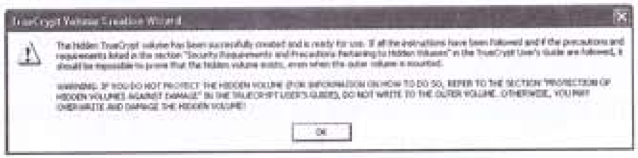
ပုံ 3: TrueCrypt Volume Creation Wizard-Selected a TrueCrypt Volume window ၏ ပုံ

အဆင့် 8: ပုံ 3 တွင် ပြထားသည့်အတိုင်း 'Select a TrueCrypt Volume' window ကို အသုံးပြု၍ volume ဖိုင်ကို တည်နေရာချပါ။

အဆင့် 9: 'TrueCrypt Volume Creation Wizard' သို့ ပြန်သွားပါ။

အဆင့် 10: 'Enter Password' screen သို့ သွားရန် click လုပ်ပါ။

အဆင့် 11: အောက်ပါ screen သို့ သွားရန် password ရိုက်ရန်နေရာတွင် Standard Volume ဖန်တီးစဉ်က သင် အသုံးပြုထားသော password ကို ရိုက်ထည့် ပါ။

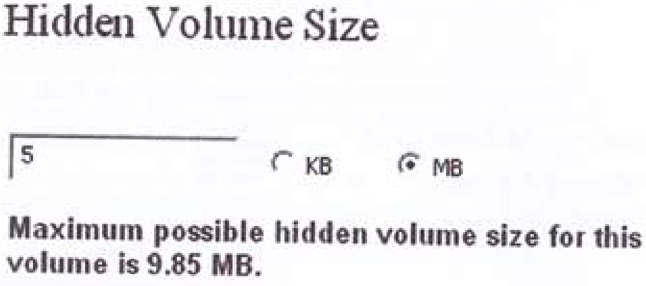


ပုံ 4 : TrueCrypt Volume Creation Wizard - Hidden Volume သတိပေးချက် Message ပုံ

အဆင့် 12: Hidden Volume Encryptions Options ကို သွားရန် message ဖတ်ပြီးလျှင် click လုပ်ပါ။

မှတ်ချက် ။ ။ Hidden Volume အတွက် ပေးထားသောပုံစံ (settings) ဖြစ်သည့် Encryption Algorithm နှင့် Hash Algorithm များကို ချန်ခဲ့ပါ။

အဆင့် 13: အောက်ပါ screen သို့ သွားရန် click လုပ်ပါ။



ပုံ 5: TrueCrypt Volume Creation Wizard- Hidden Volume အရွယ်အစား (size) ပြ (window) ပုံ

Hidden Volume ၏ အရွယ်အစားကို ဖော်ပြရန် သင့်ကို သတိပေးလိမ့်မည်။

မှတ်ချက် ။ ။ မှတ်တမ်းမှတ်ရာ အမျိုးအစား၊ အရေအတွက်နှင့် အရွယ်ပမာဏကို ထည့်တွက်ပါ။ Standard Volume အတွက် နေရာချန်ပါ။ Hidden Volume အတွက် ရရှိနိုင်သော အကြီးဆုံး အရွယ်ပမာဏကို ရွေးချယ်မိပါက သင်သည် မူရင်း Standard Volume အတွင်း၌ ဖိုင်အသစ်များ ထပ်ထည့်ရန် မဖြစ်နိုင်ပါ။

သင်၏ Standard Volume သည် 10 MB အရွယ်ပမာဏရှိပြီး Hidden Volume ၏ အရွယ်အစားကို ပုံ 6 တွင် မြင်ရသည့်အတိုင်း 5 MB ဟု ရွေးချယ်ပါက သင့်တွင် 5 MB အရွယ်အစား အသီးသီးရှိကြသော volume နှစ်ခု (Hidden volume နှင့် Standard volume) ရရှိမည် ဖြစ်သည်။

ထို့ကြောင့် Standard Volume တွင် သင် သိမ်းဆည်းမည့် အချက်အလက်များ၏ အရွယ်အစားသည် သင် သတ်မှတ်ပေးထားသော 5 MB ထက် မကျော်လွန်ရန် သေချာအောင်လုပ်ပါ။ အကြောင်းမှာ TrueCrypt program သည် Hidden Volume ကို အလိုအလျောက် မသိရှိနိုင်သည့်အပြင် မတော်တဆလည်း ၎င်းအား ဖျက်ဆီးမိနိုင်သည်။ ထို့ကြောင့် သင် မူလ သတ်မှတ်ထားသော size ထက် ကျော်လွန်၍ ဖိုင်များကို သိုလှောင်မိပါက Hidden volume ရှိ သိမ်းဆည်းထားသော ဖိုင်များကိုပါ ဆုံးရှုံးနိုင်သည်။

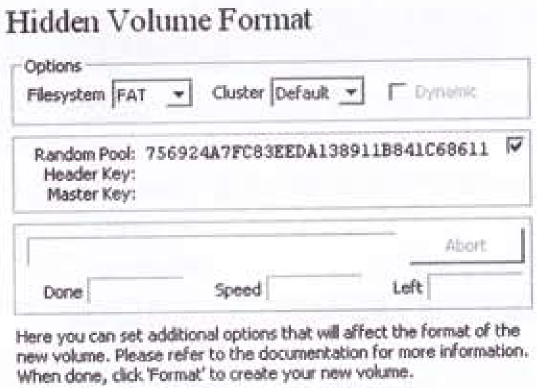
အဆင့် 14: ပုံ 6 တွင် ပြထားသည့်အတိုင်း သက်ဆိုင်ရာနေရာတွင် အလိုရှိသော Hidden Volume ၏ အရွယ်ပမာဏကို ရိုက်ထည့်ပါ။

အဆင့် 15: Hidden Volume Format window သို့ သွားပါ။

သင်၏ Standard Volume ကို ကာကွယ်ရန် အသုံးပြုသော passwordနှင့် မတူညီသော password တစ်ခုကို Hidden Volume အတွက် ပြုလုပ်ပါ။ တစ်ဖန် ကြံ့ခိုင်မှုရှိသော password ကို ရွေးချယ်ရန် သတိရပါ။ ကြံ့ခိုင်သော passwordsများ ပြုလုပ်ခြင်းအကြောင်းကို KeePass အခန်းတွင် ကြည့်ပါ။

သတိပြုရန် ။ ။ သင်၏ TrueCrypt Volumes များကို ဖော်ထုတ်ပေးရမည့် အခြေအနေမျိုး ရှိသည်ဟု ယူဆပါက Standard Volume အတွက် password ကို KeePass တွင် သိမ်းပြီး Hidden Volume အတွက်သာ သင်မှတ်မိနိုင်မည့် တစ်ခုတည်းသော ကြံ့ခိုင်မှုရှိသည့် password ကို ရွေးချယ်ပါ။ ၎င်းက သင် Hidden Volume တည်ရှိခြင်း အကြောင်း မည်သည့် သဲလွန်စမှ မပေးခဲ့သဖြင့် Hidden Volume ကို ဖုံးကွယ်ပေးသည်။

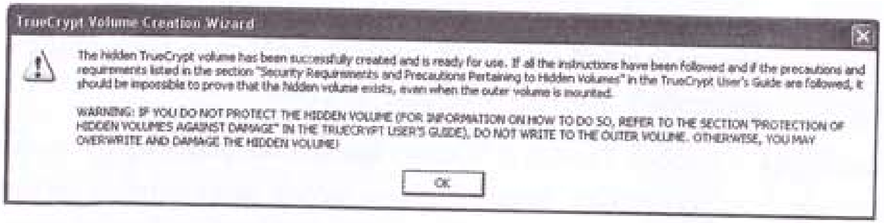
အဆင့် 16: Password တစ်ခုပြုလုပ်ပြီး နှစ်ကြိမ်ရိုက်ထည့်ပါ။ အောက်ပါ screen သို့ သွားပါ။



ပုံ 6: TrueCrypt Volume Creation Wizard - Hidden Volume Format မြင်ကွင်းပုံ

ပေးထားသော ဖိုင် system နှင့် Cluster option များကို သူ့အတိုင်းထားပါ။

အဆင့် 17: Encryption ၏ လျှို့ဝှက်ကုတ်ရေးသားခြင်း စွမ်းရည်မြင့်မားစေရန် mouse ၏ cursor ကို screen ပေါ်တွင် လှုပ်ရှားပေးပါ။ ထို့နောက် Hidden Volume ကို လုပ်ရန် click လုပ်ပါ။ Hidden Volume ကို format လုပ်ပြီးသောအခါ အောက်ပါ screen ပေါ်ထွက်လာသည်။



ပုံ 7: TrueCrypt Volume Creation Wizard သတင်းပေးချက် screen ၏ ပုံ

မှတ်ချက် ။ ။ ပုံ 7 တွင် သင်၏ Hidden Volume တစ်ခုကို အောင်မြင်စွာ တည်ဆောက်ပြီးစီးကြောင်းနှင့် standard volume ထဲသို့ ဖိုင်များ သိမ်းဆည်းချိန်တွင် hidden volume ရှိ ဖိုင်များ ပျက်ဆီးခြင်း အန္တရာယ်ကိုလည်း သတိပေးသည်။

အဆင့် 18: Hidden Volume တည်ဆောက်ပြီးစီးခြင်း window ကို click လုပ်ပြီး သွားပါ။ ထို့နောက် TrueCrypt console သို့ ပြန်ပါ။

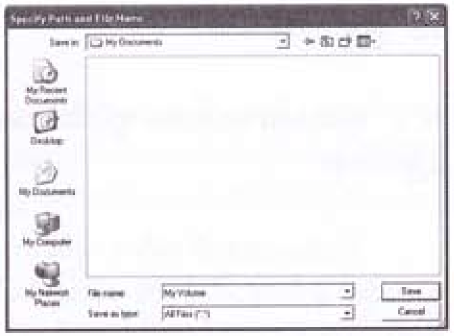
Hidden volume ကို standard volume အတွင်း၌ တည်ဆောက်ပြီး ဖြစ်သည်။ သင်သည် ယခု Hidden volume ထဲတွင် မှတ်တမ်းမှတ်ရာနေရာများကို သိမ်းဆည်းနိုင်ပြီ ဖြစ်သည်။ ၎င်းကို Standard Volume အားဖွင့်ရန် password ရရှိထားသူသော်မှ မြင်နိုင်ရန် မဖြစ်နိုင်ပါ။

5.2 Hidden Volume ကို အစီအစဉ်တကျ (mount) ပြုလုပ်ပုံ

Hidden Volume ကို အသုံးပြုနိုင်အောင် mount လုပ်သည့် နည်းလမ်းမှာ Standard Volume မှာကဲ့သို့ပင် ဖြစ်သည်။ တစ်ခုတည်းသော ကွာခြားချက်မှာ Hidden Volume အတွက် သင် ပြုလုပ်ထားသော password ကိုသာ အသုံးပြုရမည်။

Hidden Volume ကို mount လုပ်ရန် အောက်ပါအတိုင်း ဆောင်ရွက်ပါ။

အဆင့် 1: Drive တစ်ခုကို ရွေးချယ်ပါ။ (ဤ ဥပမာတွင် drive K ဖြစ်သည်)



ပုံ 8: TrueCrypt Volume screenရှိ ရွေးချယ်ထားသောmount လုပ်မည့် drive ၏ ပုံ

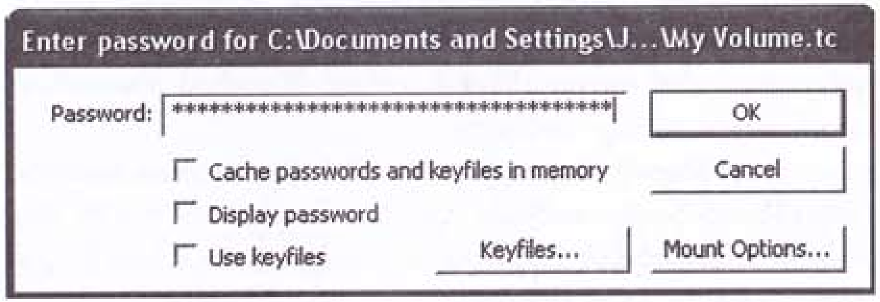
အဆင့် 2: 'Select a TrueCrypt Volume' window ကို click လုပ်ပြီး သွားပါ။

အဆင့် 3: TrueCrypt Volume ဖိုင်ကို လမ်းညွှန်ပြီး ရွေးပါ။ (Standard volume မှာကဲ့သို့ တူညီသောဖိုင်)

အဆင့် 4: TrueCrypt console သို့ click လုပ်ပြီး ပြန်ပါ။

အဆင့် 5: သတိပေးချက်အဖြစ်လာမည့် 'Enter Password' screen သို့ click လုပ်ပြီး သွားပါ။

အဆင့် 6: Hidden Volume အတွက် သင် ပြုလုပ်ထားသော password ကို ရိုက်ထည့်ပြီး click လုပ်ပါ။



ပုံ 10: အသစ်ဖွင့်ထားသော Hidden Volume ကို ပြထားသည့် TrueCrypt ပင်မ screen ၏ ပုံ

သင်၏ Hidden Volume ကို ဖွင့်ပြီး (mounted) တွေ့ရမည်။

အဆင့် 7: အထက်ပါ (Entry) ဝင်ရောက်ခွင့်ကို double click နှိပ်ပါ (သို့) My Computer window မှတဆင့် access လုပ်ပါ။

5.3 Hidden Volume တွင် ပါဝင်သော လုပ်ဆောင်ချက်များကို လုံခြုံစိတ်ချစွာ အသုံးပြုပုံ နည်းလမ်းများ

Hidden disk ၏ အဓိက လုပ်ဆောင်မှုမှာ သင်၏ အထိခိုက် အလွယ်ဆုံးသော သတင်းအချက်အလက်များကို ဖော်ထုတ်ရန် အမှန်တကယ် အားပေးခြင်းမရှိဘဲ သင့်ထက် ဩဇာရှိသူ တစ်စုံတစ်ယောက်က သင်၏ encrypted ဖိုင်များကို ကြည့်ရှုလိုသော ဆန္ဒကြောင့် ၎င်းတို့ကို လွှဲပြောင်းရယူရန် ဖြစ်ပေါ်လာသည့် အန္တရာယ်ရှိသော အခြေအနေမျိုးမှ လွတ်မြောက်အောင် ဆောင်ရွက်ရန် ဖြစ်သည်။ ၎င်းသည် သင်နှင့် သင်၏ တွဲဖက်လုပ်ကိုင်သူ (partners) များ၏ လုံခြုံမှုကိုလည်း ကာကွယ်ပေးသည်။ ၎င်းနည်းစနစ်ကို အကျိုးရှိရှိ အသုံးချရန်မှာ သင်၏ ဖိုင်များကို ကြည့်ရှုစစ်ဆေးမည့်သူကို ပြသမည့် ဖိုင်များသည် ၎င်းတို့အား ကြည့်ရှုပြီးသည်နှင့် ဆက်လက်စုံစမ်းလိုသော ဆန္ဒမျိုး မပေါ်ပေါက်ဘဲ သင်တို့အား ဘေးအန္တရာယ်ကင်းကင်း ဆက်လက်လုပ်ဆောင်ခွင့်ပေးမည့် အခြေအနေမျိုးဖြစ်အောင် ဖန်တီးရမည်။

ထိုသို့ ပြုလုပ်ရန် အောက်ပါ အကြံပြုချက်အချို့ကို ဖြည့်စွက် လုပ်ဆောင်ရမည်။

သင့်အနေဖြင့် အထူးတလည် လျှို့ဝှက်ထားရန် မလိုအပ်သော မှတ်တမ်းမှတ်ရာအချို့ကို Standard Volume အတွင်းသို့ထည့်ပါ။ သို့သော်လည်း ၎င်းမှတ်တမ်းမှတ်ရာများမှာ သင်၏ encrypted ဖိုင်အဖြစ် သတ်မှတ်သိမ်းဆည်းရန် လုံလောက်သော သတင်းအချက်အလက်မျိုး ပါဝင်ရမည်။

သင်၏ ဖိုင်များကို စစ်ဆေးမည့်သူသည် သင်၏ Hidden Volume အကြောင်းကို သိရှိနေနိုင်သည်ကိုလည်း သတိပြုပါ။ သို့သော် သင်သည် TrueCrypt ကို မှန်မှန်ကန်ကန် အသုံးချမည်ဆိုပါက စစ်ဆေးသူသည် သင့်၌ Hidden Volume ရှိသည်ကို သက်သေမပြနိုင်ဘဲ သင်၏ ငြင်းဆိုချက်ကိုလည်း ပိုရှုယုံကြည်ဖွယ်ရာရှိသည်။

Standard Volume အတွင်းရှိ ဖိုင်များကို တစ်ပတ်တစ်ခါ update လုပ်ပါ။ ဤသို့ပြုလုပ်ခြင်းက သင်သည် ၎င်းဖိုင်များနှင့်အမှန်တကယ် အလုပ်လုပ်ဆောင်မှုရှိသည့် အနေအထားကို ဖြစ်စေသည်။

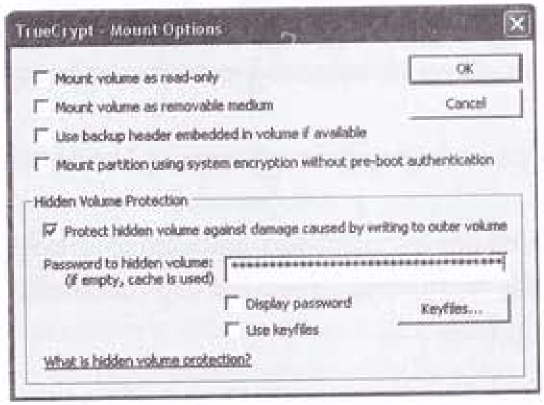
TrueCrypt Volume ကို သင် အစီအစဉ်ချသည့်အခါ အပြင်ဘက်ရှိ Volume တွင် ဖြစ်ပေါ်တတ်သော ထိခိုက်ပျက်စီးမှုများမှ ကာကွယ်ရန် 'Protect hidden volume' ကို enable လုပ်ထားသင့်သည်။ ၎င်းသည် အလွန်အရေးကြီးသော လုပ်ဆောင်

ချက် (feature) ဖြစ်ပြီး Hidden Volume ရှိ encrypted ဖိုင်များကို မတော်တဆ ဖျက်ဆီးမိခြင်းနှင့် overwriting ဖြစ်မည့် အန္တရာယ်မရှိဘဲ သင်၏ standard volume အတွင်းသို့ သင်ကဟန်ဆောင်အသုံးချပြမည့် ဖိုင်အသစ်များကို ပေါင်းထည့်ရန် ခွင့်ပြုသည်။

အစောပိုင်းတွင် အသိပေးခဲ့သည့်အတိုင်း standard volume အတွင်းရှိ သိမ်းဆည်းသည့် ပမာဏကို ချဲ့ထွင်ခြင်းသည် သင်၏ ဖုံးကွယ်ထားသော ဖိုင်များကို ပျက်စီးနိုင်သည်။ TrueCrypt volume ကို mount လုပ်သည့်အခါ 'Protect hidden volume' ကို enable မလုပ်ပါနှင့်။ ထိုသို့ ပြုလုပ်ခြင်းသည် သင်၏ hidden volume ထဲသို့ လျှို့ဝှက် password ဖြင့် ဝင်ရောက်ရန် လိုအပ်ပြီး ၎င်း volume တည်ရှိနေမှုကို ရှင်းရှင်းလင်းလင်း ဖော်ထုတ်ပြီးဖြစ်လိမ့်မည်။ သင်၏ဟန်ဆောင်အသုံးချမည့် ဖိုင်များကို update လုပ်သည့်အခါတွင်သာ ဤ option ကို enable လုပ်သင့်သည်။

'Protect hidden volume' လုပ်ဆောင်ချက်ကို အသုံးပြုရန် အောက်ပါ အဆင့်များကို ဆောင်ရွက်ပါ။

အဆင့် 1: ပုံ 10 တွင် ပြထားသည့် 'Enter Password' သတိပေးချက်ကို click လုပ်ပါ။ ၎င်းက Mount option ရှိရာ window ကို ခေါ်သွားလိမ့်မည်။



ပုံ 11: Mount Options window ၏ ပုံ

အဆင့် 2: အပြင်ဘက်ရှိ volume တွင် အလုပ်လုပ်ရာမှ ဖြစ်ပေါ်လာ သော ထိခိုက်ပျက်စီးမှု ရှိ၊ မရှိ 'Protect hidden volume' ကို check လုပ်ပါ။

အဆင့် 3: Hidden Volume အတွက် password ရိုက်ပြီး click လုပ်ပါ။

အဆင့် 4: Standard volume ကို mount လုပ်ရန် click လုပ်ပါ။ အောင်မြင်စွာ လုပ်ဆောင်ပြီးပါက ဟန်ဆောင်အသုံးချမည့် ဖိုင်များကို hidden volume အား မထိခိုက်စေဘဲ ထည့်သွင်းနိုင်ပါပြီ။

အဆင့် 5: Dismount ကို click လုပ်ပါ။ (သို့မဟုတ်) ၎င်း၏ ဖိုင်များကို ပြုပြင်မွမ်းမံပြီးပါက standard volume ကို အသုံးမပြုနိုင်အောင် ပြုလုပ်ထားပါ။

သတိရရန်မှာ ဤ အစီအစဉ်ကို သင်၏ standard volume ရှိ ဖိုင်များ update လုပ်ရာတွင်သာ ပြုလုပ်ရန် လိုအပ်သည်။ တစ်စုံတစ်ယောက်ကို သင်၏ standard volume အား ပြသရန်ရှိပါက ၎င်း 'Protect hidden volume' လုပ်ဆောင်ချက်ကို အသုံးမပြုသင့်ပါ။

မကြာခဏမေးလေ့ရှိသော မေးခွန်းများနှင့် သုံးသပ်ချက် (FAQ & Review)
6.0 FAQ and Review

ကလောဒီယာနှင့် ပါဗလိုတို့သည် TrueCrypt ၏ လုပ်ဆောင်မှုကို ကျေနပ်ကြသည်။ အထူးသဖြင့် ပရိုဂရမ်သည် install လုပ်ရလွယ်ကူပြီး သူ့အလိုအလျောက် အလုပ် လုပ်သောကြောင့် ဖြစ်သည်။ သို့သော်လည်း ဤ ပရိုဂရမ်ကို အသုံးပြုဖို့ ဆုံးဖြတ်ချက် မကျခင် ၎င်းတို့၌ TrueCrypt နှင့် ပတ်သက်၍ မေးစရာ မေးခွန်းအချို့ ရှိနေကြသည်။

မေး ။ ။ TrueCrypt ထဲကို password တွေ ရိုက်ထည့်နေရတာနဲ့ပဲ အချိန်ကုန်နေမှာလား။

ဖြေ ။ ။ Standard Volume ကို မင်း ဖွင့်တဲ့အချိန်မှာ password ကို တစ်ကြိမ်သာ ရိုက်ထည့်ဖို့ လိုအပ်ပါတယ်။ အဲဒါပြီးတာနဲ့ password တွေ ထပ်ခါထပ်ခါ ရိုက်စရာမလိုပဲ ဖွင့်လိုတဲ့ ဖိုင်ကို ဖွင့်နိုင်ပါတယ်။

မေး ။ ။ တကယ်လို့ TrueCrypt ကိုပါ မလိုအပ်တော့ဘူးဆိုရင် အလွယ်တကူ uninstall လုပ်လို့ရပါ့မလား။ အဲဒီလို လုပ်ရင်ရော ငါ့ရဲ့ ဖိုင်တွေဟာ encrypted ဖြစ်ပါ့ဦးမလား။

ဖြေ ။ ။ TrueCrypt ကို Start>Programs>TrueCrypt>Uninstall TrueCrypt

ကိုသွားပြီး ရွေးချယ်ရုံနဲ့ အလွယ်တကူ ဖယ်ရှားနိုင်ပါတယ်။ ၎င်းပရိုဂရမ်ကို မဖယ်ခင်မှာ volume အတွင်းမှာရှိတဲ့ သင့်ရဲ့ ဖိုင်တွေကို နေရာပြန်ချဖို့ သတိပြုပါ။ သို့မဟုတ်ပါက သင့်အနေဖြင့် ၎င်းတို့ကို access လုပ်ရန် မဖြစ်နိုင်ပါ။ တခြား ကွန်ပျူတာတစ်လုံးမှာ volume ကို ရွှေ့ပြောင်းထည့်မည်ဆိုလျှင်လည်း access လုပ်ဖို့ကတော့ သင့်ရဲ့ password နဲ့ TrueCrypt ပရိုဂရမ်တို့ကို လိုအပ်နေဦးမှာပါပဲ။

မေး ။ ။ တကယ်လို့ TrueCrypt နဲ့ ပတ်သက်ပြီးတော့ ပြဿနာတစ်ခုခုရှိမယ်ဆိုရင် အကူအညီတောင်းစရာ website လိပ်စာ (သို့) အီးမေးလ်လိပ်စာများ ရှိပါသလား။

ဖြေ ။ ။ အကူအညီ အထောက်အပံ့အတွက် TrueCrypt ရဲ့ မှတ်တမ်းမှတ်ရာကို ကြည့်ရှုရန် လိပ်စာတွေကတော့ http://www. TrueCrypt.org/docs/ (သို့) http://forums.truecrypt.org// (သို့) !http://security.ngoinabox.org/en/truecrypt- main တို့ ဖြစ်ကြပါတယ်။ ဒါပေမဲ့ မေ့သွားတဲ့ volume password ကိုတော့ ပြန်ရအောင် ဘယ်သူမှ ကူညီရှာဖွေနိုင်မှာ မဟုတ်ပါဘူး။

မေး ။ ။ Version မတူတဲ့ Windows တွေမှာ TrueCrypt ကို အသုံးပြုရင် မတူညီတဲ့ ပြင်ကွင်းတွေနဲ့ အသုံးချရမှာလား။

ဖြေ ။ ။ သူတို့ရဲ့ ပုံသဏ္ဍာန်ဟာ အနည်းငယ်မျှ ကွာခြားနိုင်ပေမဲ့ အထဲမှာပါဝင်တဲ့ လုပ်ဆောင်ချက်ကတော့ အတူတူပါပဲ။

မေး ။ ။ 'Encryption' လုပ်ရန်အတွက် ဘယ်လိုအချက်အလက်တွေ လိုအပ်သလဲ။

ဖြေ ။ ။ ကိုယ်ရေးကိုယ်တာနဲ့ သက်ဆိုင်ပြီး ထိခိုက်လွယ်တဲ့ သတင်း အချက်အလက်တွေပါဝင်တဲ့ ဖိုင်တွေနဲ့ သင့်ရဲ့ မှတ်တမ်းမှတ်ရာနဲ့ ရုပ်ပုံတွေအားလုံးကို encrypt လုပ်သင့်ပါတယ်။ သင်၏ ကွန်ပျူတာကို ဆုံးရှုံးသွားတာမျိုး ဒါမှမဟုတ် တစ်စုံတစ်ယောက်က သိမ်းတာကိုခံရတာမျိုးဆိုလျှင်လည်း TrueCrypt volume ထဲမှာရှိတဲ့ သတင်းအချက်အလက်တွေဟာ လုံခြုံမှုရှိနေဦးမှာ ဖြစ်ပါတယ်။

မေး ။ ။ ကျွန်တော်တို့ ဖိုင်တွေဟာ ဘယ်လို လုံခြုံမှု ရှိပါသလဲ။

ဖြေ ။ ။ TrueCrypt ဟာ ၎င်းကိုတောင်းဆိုတဲ့ လုပ်ဆောင်ချက်တွေကို ဆောင်ရွက်မှု ရှိ၊ မရှိ ဘယ်လောက်ထိကောင်းအောင် ဆောင်ရွက်တယ်ဆိုတာကို အထူး

ကျွမ်းကျင်သူများက အသေအချာ စစ်ဆေးဝေဖန်ထားပါတယ်။ ရလဒ်မှန်သမျှမှာ TrueCrypt ဟာ အဆင့်အတန်းမြင့်တဲ့ ကာကွယ်မှုတစ်ခု ဖြစ်တယ်ဆိုတာကိုလည်း ပြသနေပါတယ်။ သင့် volume ရဲ့ လုံခြုံရေးအတွက် ကြံ့ခိုင်မှုရှိတဲ့ password ကို မဖြစ်မနေ ရွေးချယ်ဖို့ လိုအပ်ပါတယ်။

TrueCrypt ရဲ့ hidden disk လုပ်ဆောင်ချက်ဟာ ကွန်ပျူတာပေါ်မှာ သိမ်းဆည်းထားတဲ့ သတင်းအချက်အလက်တွေအတွက် ညီညွတ်မှုရှိတဲ့ လုံခြုံရေးအဆင့်ကို ပေးပါတယ်။ အသုံးပြုသူက ပရိုဂရမ်နဲ့ ၎င်းရဲ့ အခြေခံလုပ်ဆောင်ချက်တွေကို မိမိရရ ဆုပ်ကိုင်ဖို့ လိုအပ်ပြီး ကိုယ့်ရဲ့ လုံခြုံရေး အခြေအနေကိုလည်း ကျွမ်းကျွမ်းကျင်ကျင် access လုပ်နိုင်မှ hidden disk ကို အကျိုးရှိအောင် အသုံးချနိုင်မှာ ဖြစ်ပါတယ်။

မေး ။ ။ Hidden volume မပါဘဲ ငါ့ရဲ့ မူရင်း standard volume ကို ဘယ်လို mount လုပ်ရမယ်ဆိုတာ ပြန်ပြောပြပါဦး။

ဖြေ ။ ။ ဒါတွေအားလုံးဟာ password ရိုက်ရမယ့်နေရာမှာ သင် ဘယ်လို password ရိုက်ထည့်ခဲ့သလဲဆိုတာ အပေါ်မှာ မူတည်တယ်။ Standard Volume ရဲ့ password ကို ရိုက်မယ်ဆိုရင် TrueCrypt က Standard Volume ကိုပဲ mount လုပ်ပေးပြီး Hidden Volume ရဲ့ password ရိုက်ခဲ့ရင်တော့ TrueCrypt က Hidden Volume ကိုပဲ mount လုပ်ရမှာ ဖြစ်ပါတယ်။ ဒါကြောင့် သင့်ရဲ့ TrueCrypt ထဲမှာရှိတဲ့ သတင်း အချက်အလက်တွေကို ကြည့်ရှု စစ်ဆေးချင်တဲ့သူကို Standard volume ကို ဖွင့်ပြရုံပါပဲ။ ဒါက သင့်ကို ငါးမျှားချိတ်က လွတ်စေပြီး ဒုက္ခမရောက်အောင် လုံလောက်တဲ့ အခြေအနေတစ်ရပ် ဖြစ်လိမ့်မယ်လို့ မျှော်လင့်ရပါတယ်။

မေး ။ ။ သင့်ရဲ့ Hidden Volume ဟာ အမှတ်မထင် ပျက်စီးတာတို့ ဖျက်သိမ်းခံရတာတို့ရော ဖြစ်နိုင်ရဲ့လား။

ဖြေ ။ ။ ဖြစ်နိုင်ပါတယ်။ Hidden disk အတွက် နေရာမရှိနိုင်လောက်အောင် Standard Volume ထဲမှာ ဖိုင်တွေ ထပ်ထည့်နေရမယ်ဆိုလျှင် သင့်ရဲ့ Hidden disk ဟာ အလိုအလျောက် overwrite ဖြစ်ပြီး ပျက်စီးသွားမှာဖြစ်ပါတယ်။ Hidden disk ကို overwrite ဖြစ်မယ့်အရေးက ကာကွယ်ပေးတဲ့ option တစ်ခုဟာ TrueCrypt ရဲ့ volume ထဲမှာ ရှိပါတယ်။ ဒါပေမဲ့ ၎င်း option ကို ဖွင့်ထားခြင်းဟာ သင် Standard Volume ကို အသုံးပြုတဲ့အချိန်မှာ Hidden disk လည်း တည်ရှိနေတယ်ဆိုတဲ့ အကြောင်းကို သင့်ရဲ့ ပြိုင်ဘက်သိအောင် ဖွင့်ဆိုပြသလို ဖြစ်နေပါလိမ့်မည်။

မေး ။ ။ Hidden disk တည်ဆောက်ပြီးတဲ့ အချိန်မှာ ၎င်းရဲ့ အရွယ်အစားကို ပြန်ပြောင်းလို့ ရပါသလား။

ဖြေ ။ ။ မရပါဘူး။ သင်ဟာ Hidden disk အသစ်တစ်ခုကို တည်ဆောက်ရမှာ ဖြစ်ပြီး သင့်ရဲ့ ဖိုင်တွေကိုလည်း အစီအစဉ်တကျ ရွှေ့ပြောင်းရမှာ ဖြစ်ပါတယ်။

မေး ။ ။ TrueCrypt မှာရှိတဲ့ mount လုပ်ထားတဲ့ ဖိုင်တွေကို disk စစ်ဆေးခြင်း (check dist) disk ကို နေရာအစီအစဉ်ကျနအောင် ပြုလုပ်ခြင်း (disk defragmenter) စတာတွေ ပြုလုပ်လို့ ရ၊ မရ သိချင်ပါတယ်။

ဖြေ ။ ။ TrueCrypt ဟာ တကယ့် disk drive တစ်ခုကဲ့သို့ ပြုမူဆောင်ရွက်ပြီး ၎င်းရဲ့အထဲမှာ mount လုပ်ထားတဲ့ ဖိုင်တွေကို စစ်ဆေးခြင်း၊ အစီအစဉ်ကျနအောင် ပြုလုပ်ခြင်းစတဲ့ မည်သည့်ဖိုင် system ကိုမဆို အသုံးပြုဖို့ ဖြစ်နိုင်ပါတယ်။

မေး ။ ။ Hidden Volume ရဲ့ password ကို ပြောင်းလဲဖို့ ဖြစ်နိုင်ပါသလား။

ဖြေ ။ ။ ဖြစ်နိုင်ပါတယ်။ 'Password ပြောင်းလဲခြင်း လုပ်ဆောင်ချက်(feature) က Standard နဲ့ Hidden volume နှစ်ခုစလုံးကို လုပ်ဆောင်ခွင့်ပြုပါတယ်။ 'Current Password' ဆိုတဲ့ အကွက်ထဲမှာ hidden volume ရဲ့ password ကို ရိုက်ထည့်ရုံပါပဲ။ ၎င်းကို 'Volume Password Change' သတိပေးချက်မှာ တွေ့နိုင်ပါတယ်။

မေး ။ ။ Hidden disk ရဲ့ feature ကို ဘယ်အချိန်မှာ လုပ်ဆောင်သင့်ပါသလဲ။

ဖြေ ။ ။ သင့် ကွန်ပျူတာပေါ်မှာရှိတဲ့ တိကျသေချာတဲ့ သတင်း အချက်အလက်တွေ ရှိနေတာကို ဖုံးကွယ်ထားဖို့ လိုအပ်တဲ့အခါ TrueCrypt ရဲ့ hidden disk ကို အသုံးပြုပါ။ မှတ်သားထားဖို့က ဒါဟာ အချက်အလက်တွေကို ကာကွယ်မှုပေးတဲ့ access ပြုလုပ်တဲ့ Standard Volume ကို အသုံးပြုခြင်းနဲ့တော့ ကွဲပြားခြားနားတယ်ဆိုတာပါပဲ။

TrueCrypt ရဲ့ မေးခွန်း အသေးစိတ်တွေကို လေ့လာမယ်ဆိုလျှင် http://www.TrueCrypt.org/fag.php ကို ကြည့်ရှုပါ။

6.1 Standard Volume အတွက် မေးခွန်း သုံးသပ်ချက်များ

* 'Encryption' ဆိုတာ ဘာလဲ။
* 'Standard Volume' ဆိုတာ ဘာလဲ။
* USB memory stick တစ်ခုအပေါ်မှာ Standard Volume တစ်ခု ဘယ်လို တည်ဆောက်မလဲ။
* Standard Volume ကို dismount လုပ်ဖို့ နည်းလမ်းတွေက ဘာတွေလဲ။
* သင့်ရဲ့ Standard Volume အတွက် ကောင်းမွန်တဲ့ password တစ်ခုကို ဘယ်လိုရွေးချယ်ပြီး ပြင်ဆင်မှု ဘယ်လိုလုပ်မှာလဲ။
* သင့် Standard Volume ရဲ့ မူပွား (back up) တစ်ခုကို ပြုလုပ်ဖို့ ဖြစ်နိုင်ချေတွေက ဘာလဲ။
* ကွန်ပျူတာပေါ်မှာ သင့်ရဲ့ Standard Volume ကို ကွယ်ဖျောက်ထားဖို့ နည်းလမ်းတွေက ဘာတွေလဲ။

6.2 Hidden Volume အတွက် မေးခွန်းသုံးသပ်ချက်များ

* Standard Volume နှင့် Hidden Volume နှစ်ခုကြား အဓိက ကွာခြားချက်က ဘာလဲ။
* သင့်မှာ Hidden Volume လည်း ရှိမယ်ဆိုရင် Standard Volume ထဲကို ဘယ်လို ဖိုင်အမျိုးအစားတွေ ထည့်သွင်းသလဲ။
* Hidden Volume က ဘယ်နေရာမှာ ရှိတာလဲ။
* Hidden Volume ရဲ့ ရှိသင့်တဲ့ အရွယ်အစားက ဘာလဲ။
* သင့်ရဲ့ Hidden Volume ကို မတော်တဆ ထိခိုက်ပျက်စီးမှုများက ကာကွယ်ခြင်းရဲ့ ကောင်းကျိုးနဲ့ ဆိုးကျိုးက ဘာတွေလဲ။

Recuva ပျက်စီးသွားသော ဖိုင်များကို ပြန်လည်ရယူခြင်း

Recuva သည် အသုံးပြုရလွယ်ကူသော ပျက်စီးသွားသည့် ဖိုင်များကို ပြန်လည်ရယူသည့် tool တစ်ခုဖြစ်သည်။ ၎င်းက သင့်အား ပျက်စီးဆုံးရှုံးသွားသော မှတ်တမ်းမှတ်ရာများ၊ ဖိုင်များ၊ folders များနှင့် အီးမေးလ်၊ ရုပ်ပုံများ၊ ဗီဒီယို Formats များ ပါဝင်သော သတင်း အချက်အလက်များကို စစ်ဆေးပြီး ပြန်လည် ရယူခွင့်ပေးသည်။ Recuva က အရေးကြီးပြီး ကိုယ်ရေးကိုယ်တာနှင့် သက်ဆိုင်သော(သို့) ထိခိုက်လွယ်သော သတင်းအချက်အလက်များကို ပယ်ဖျက်ရန် လုံခြုံမှုရှိသော ဖျက်ဆီးခြင်းစနစ်ကို အသုံးပြုပေးသည်။

Recuva ကို install ပြုလုပ်ခြင်း

* လမ်းညွှန်ချက် အသေးစိတ်ကို ဖတ်ပါ။
* အောက်တွင်ရှိသော 'Recuva icon' ကို နှိပ်ပြီး www.piriform.com/recuva/builds download စာမျက်နှာကို သွားပါ။
* 'Recuva-Slim' ခေါင်းစဉ်အောက်ရှိ 'Download' ကို နှိပ်ပါ။
* 'resetup-slim.exe' ဖိုင်ကို သင့်ကွန်ပျူတာမှာ သိမ်းပါ။ ၎င်းဖိုင်ကို ရှာပြီး double click လုပ်၍ installation ပရိုဂရမ်ကို စတင်ပါ။
* သင်ဆက်လက် မလုပ်ဆောင်မီ နောက်အခန်းတွင် ပါဝင်သော 'Installation လမ်းညွှန်ချက်များ' ကို ဖတ်ပါ။

Recuva ပရိုဂရမ်ကို ကွန်ပျူတာပေါ်တွင်အောင်မြင်စွာ တင်ပြီးပါက ၎င်း၏ installation ပရိုဂရမ်ကို ဖျက်ပစ်နိုင်ပါသည်။

အောက်ပါတို့မှာ Recuva နှင့် ပတ်သက်သောအချက်အလက်များ ဖြစ်ကြသည်။

* မူရင်းစာမျက်နှာ (Home Page) မှာ www.piriform.com/recuva ဖြစ်သည်။
* ကွန်ပျူတာလိုအပ်ချက်မှာ Windows Versions အကုန်လုံးအတွက် ဖြစ်သည်။ (ချက် ။ ။ Window 98 အတွက် အထောက်အကူ မပြုတော့ပါ။)
* ဤလမ်းညွှန်တွင် အသုံးပြုထားသော Window Version မှာ 1.3 ဖြစ်သည်။
* ဖတ်ရှု မှတ်သားသင့်သည်မှာ အခန်း 5 ရှိ 'ဆုံးရှုံးသွားသော သတင်းအချက်အလက်များအား ပြန်လည်ရယူခြင်း' ကို ဖြစ်သည်။
* ပါဝင်သော level အဆင့်များမှာ 1: Beginner, 2: Average, 3: Intermediate, 4: Experienced, 5: Advanced တို့ ဖြစ်ကြသည်။
* ဤပရိုဂရမ်ကို စတင်အသုံးပြုရန် လိုအပ်သည့်အချိန်မှာ မိနစ် 20 ဖြစ်သည်။
* သင်ရရှိမည့် အကျိုးကျေးဇူးများမှာ ရှာဖွေစစ်ဆေးခြင်း (scanning) နည်းစနစ်အမျိုးမျိုးတို့ကို ဆောင်ရွက်နိုင်ခြင်း ဖြစ်သည်။ ထို့ပြင် သင်၏ ကွန်ပျူတာပေါ်ရှိ ဖျက်ပြီးသား ဖိုင်များကို ပြန်လည်ရရှိခြင်း။ ကိုယ်ရေးကိုယ်တာ သတင်းအချက်အလက်များကို လုံခြုံစွာဖျက်ဆီးနိုင်ခြင်းတို့လည်း ရရှိနိုင်သည်။
* GNU linux, Mac Os နှင့် Microsoft Windows များနှင့် တွဲဖက် ဆောင်ရွက်နိုင်သော ပရိုဂရမ်များ . . . .

GNU linux အသုံးပြုသူများအတွက် Microsoft Window နှင့် သာမက GNU linux နှင့်ပါ အဆင်ပြေသည့် 'Test Disk and PhotoRec' ကို သင့်လျော်မည် ထင်ပါသည်။ Recuva အပြင် Microsoft Windows နှင့် အဆင်ပြေနိုင်မည့် file recovery ပရိုဂရမ်များမှာ . . . .

* NTFS Undelete
* Disk Digger
* PCInspector File Recovery
* FileRestorePlus တို့ ဖြစ်ကြပါသည်။

1.1 သင်အသုံးမပြုခင် သိထားသင့်သော အကြောင်းအရာများ

သင့်ရဲ့ ကိုယ်ရေးကိုယ်တာ ဖိုင်တွေ (သို့မဟုတ်) ထိခိုက်ပျက်စီးလွယ်တဲ့

ဖိုင်တွေကို မှားယွင်းပြီး ဖျက်ပစ် (delete) လိုက်တဲ့ အခြေအနေမျိုးမှာ Recuva က ၎င်းဖိုင်တွေကို ရှာဖွေပြီး ပြန်လည်ရယူပေးနိုင်ဖို့ ကူညီဆောင်ရွက်ပါတယ်။ အခန်း 6 မှာ ပါဝင်တဲ့ 'ထိခိုက်လွယ်သော သတင်း အချက်အလက်များကို ဖျက်ဆီးပုံ' မှာ ပြောခဲ့သလိုပါပဲ။ Windows ရဲ့ OS မှာပါဝင်တဲ့ 'Delect' function မှ ဖျက်ထုတ်လိုက်တဲ့ ဖိုင်တွေဟာ အမှိုက်ခြင်း (recycle bin) ထဲကိုရောက်ရှိပြီး ၎င်း recycle bin ကို ဗလာခါလျှင်တောင်မှ ၎င်းဖိုင်ဟာ သင့်ရဲ့ ကွန်ပျူတာပေါ်မှာ ရှိနေနိုင်ပါတယ်။

ဒါပေမဲ့ သင့်ရဲ့ ဖိုင်တွေကို ပြန်လည်ရယူဖို့ Recuva အနေနဲ့ မတတ်နိုင်တဲ့ အခြေအနေမျိုးလဲ ရှိပါတယ်။ တကယ်လို့ သင်ဟာ CCleaner ရဲ့ 'Secure file deletion (Slower)' option ကိုသာ enable လုပ်ပြီး ယာယီအသုံးပြုနေတဲ့ ဖိုင်တွေကို ရှင်းပစ်တာပဲဖြစ်ဖြစ်၊ မူလဖိုင်တွေကို ဖျက်ပစ်တာပဲဖြစ်ဖြစ် ၎င်းဖိုင်တွေကို ပြန်မရနိုင်တော့ပါဘူး။ Recuva က 'CClear' (သို့) 'Eraser' စတဲ့ ပရိုဂရမ်တွေ အသုံးပြုပြီး disk နေရာကို အလွတ်ဖြစ်အောင် ရှင်းလင်းထားတာမျိုးကို ပြန်ပြီး ရယူမပေးနိုင်ပါဘူး။ Window ကိုယ်တိုင်က ဖိုင်တစ်ဖိုင် တည်ရှိပြီးသားနေရာပေါ်မှာ overwrite ဖြစ်သွားတာမျိုးကိုလည်း ကူညီပြီး မယူပေးနိုင်ပါဘူး။ နောက်ပြီး ပျက်စီးနေပြီးသား မှတ်တမ်းမှတ်ရာနဲ့ ဖိုင်တွေကို Recuva က ပြန်ပြီး မယူပေးနိုင်ပါဘူး။

Recuva ကို သင့်ရဲ့ ကိုယ်ရေးကိုယ်တာ၊ ထိခိုက်လွယ်တဲ့ data တွေကို လုံခြုံစွာဖျက်စီးရာမှာလည်း အသုံးပြုနိုင်ပါတယ်။

* Recuva ကို install ပြုလုပ်ပုံ
* Recuva ကို အသုံးပြုပြီး ရှာဖွေစစ်ဆေးခြင်း အမျိုးမျိုး ဆောင်ရွက်ပုံ
* Recuva ကို အသုံးပြုပြီး ဖိုင်တွေ ပြန်လည်ရယူပုံနှင့် ဖိုင်တွေကို လုံခြုံစွာ ဖျက်ဆီးပုံ
* မကြာခဏ မေးလေ့ရှိသော မေးခွန်းများနှင့် သုံးသပ်ချက်

Recuva ကို Install ပြုလုပ်ပုံ

2.0 Recuva ကို Install ပြုလုပ်ပုံ

Recuva ကို Install ပြုလုပ်ခြင်းဟာ လွယ်ကူလျှင်မြန်တဲ့ လုပ်ငန်းစဉ် ဖြစ်ပါတယ်။ Recuva ကို Install စတင်ပြုလုပ်ရန် အောက်ပါအဆင့်များကို ဆောင်ရွက်ပါ။

အဆင့် 1: 'Open File' ကို double click နှိပ်ပါ။ လုံခြုံရေး အချက်ပေး dialog

box ပေါ်လာပါလိမ့်မယ်။ အောက်ပါ dialog box ကို သွားဖို့ click ဆက်လုပ်ပါ။

အဆင့် 2: 'Welcome to the Recuva Setup Wizard' screen ကို သွားရန် click

ပုံ 1: Installer ၏ ဘာသာစကား ရွေးချယ်မှုပြ dialog box ၏ ပုံ

လုပ်ပါ။

အဆင့် 3: အသုံးပြုသူ၏ သဘောတူညီချက်ကို လက်ခံမည့် license Agreement screen ကို သွားရန် click လုပ်ပါ။ License Agreement ပါ အကြောင်း အရာများကို ကျန်သည့် Installation လုပ်ငန်းစဉ်များ မပြုလုပ်ခင် သေသေချာချာ ဖတ်ပါ။

အဆင့် 4: တည်နေရာ ရွေးချယ်ရန် 'Choose Location' screenကို click လုပ်ပြီး သွားပါ။

အဆင့် 5: 'Install Options' screen ကို ရွေးချယ်ပြီး click လုပ်ပါ။

မှတ်ချက် ။ ။ 'Install Options' သည် 'Install optional Yahoo!tool bar' option ကို enable လုပ်လျက် ပူးတွဲပေါ်လာလိမ့်မည်။ 'Yahoo! toolbar' ကို install မလုပ်ပါနှင့်။ ၎င်းက သင့် အင်တာနက်၏ ပုဂ္ဂိုလ်ရေးနှင့် လုံခြုံရေးဆိုင်ရာတို့ကို ချတ်ယွင်းချက်များ ဖြစ်စေသည်။

အဆင့် 6: အောက်ပါပုံ 2 တွင် ပြထားသကဲ့သို့ 'Install optional Yahoo! toolbar' ၏ check box ၌ disable လုပ်ပါ။

ပုံ 2: Optional Yahoo! toolbar ကို disable လုပ်ထားသော 'Install Options' screen ၏ ပုံ

အဆင့် 7: Recuva ကို install လုပ်ရန် click လုပ်ပါ။ ၎င်းက installation အခြေအနေကို ပြသနေသော bar တစ်ခုကို screen ပေါ်တွင် တွေ့ရစေပြီး လုပ်ငန်းစဉ် ပြီးဆုံးပြီး မိနစ်အနည်းငယ်အကြာတွင် အလိုအလျောက် ပျောက်ကွယ်သွားလိမ့်မည်။

အဆင့် 8: Recuva ကို install လုပ်ခြင်း ပြီးဆုံးပါက click လုပ်ပါ။

ယခု သင်သည် Recuva ကို အောင်မြင်စွာ install ပြုလုပ်ပြီးပါပြီ။ သင်သည် ဖိုင်များ ပြန်လည်ရယူခြင်း၊ ကိုယ်ရေးကိုယ်တာနှင့် ထိခိုက်လွယ်သော ဖိုင်အမျိုးအစားများကို စိတ်ချစွာ ဖျက်ဆီးနိုင်ခြင်းတို့ကိုလည်း ဆောင်ရွက်နိုင်ပါပြီ။ အခန်း 3.0 ရှိ 'Recuva ကို အသုံးပြုပြီး ရှာဖွေစစ်ဆေးခြင်း နည်းလမ်းအမျိုးမျိုးဆောင်ရွက်ပုံ' ကို ဆက်လက် လေ့လာပါဦး။

Recuva ကို အသုံးပြုပြီး ရှာဖွေစစ်ဆေးခြင်း နည်းလမ်းအမျိုးမျိုး ဆောင်ရွက်ပုံ

ဤစာမျက်နှာရှိ အပိုင်းကဏ္ဍများမှာ–

* 3.0 သင်စတင် အသုံးမပြုခင်
* 3.1 Recuva Wizard ကို အသုံးပြုပြီး ရှာဖွေစစ်ဆေးမှုတစ်ခု ဆောင်ရွက်ပုံ
* 3.2 Recuva Wizard ကို အသုံးမပြုဘဲ ရှာဖွေစစ်ဆေးမှုတစ်ခု ဆောင်ရွက်ပုံ
* 3.3 Recuva ကို အသုံးပြုပြီး စေ့စေ့စပ်စပ် ရှာဖွေစစ်ဆေးပုံ
* 3.4 'Options' screen အတွက် မိတ်ဆက်

3.0 သင်စတင် အသုံးမပြုခင်

ဤအပိုင်းတွင် သင်သည် ရှာဖွေစစ်ဆေးခြင်းနည်းလမ်းအမျိုးမျိုးတို့ ဆောင်ရွက်ပုံကို လေ့လာရန်နှင့် 'Options' screen ရှိ အထွေထွေ (General) နှင့် လုပ်ရှားမှု (Actions) tabs များကို ထိတွေ့သင်ယူရမည်။

မှတ်ချက် ။ ။ ရှာဖွေစစ်ဆေးခြင်းတစ်ခုသည် အမှန်တကယ် ပြန်လည်ရရှိနိုင်သော ဖိုင်များကို ပြသပေးပြီး ၎င်းတို့ကို ပြန်ယူပေးသည်။ ပြန်လည်ရယူမှု အစီအစဉ်များကို အခန်း (4) 'Recuva ကို အသုံးပြုပြီး ဖိုင်များ ပြန်လည်ရယူပုံနှင့် ဖိုင်များကို လုံခြုံစွာ ဖျက်ဆီးပုံ'တွင် ဆွေးနွေးတင်ပြထားပါသည်။

3.1 Recuva Wizard ကို အသုံးပြုပြီး ရှာဖွေစစ်ဆေးမှုတစ်ခု ဆောင်ရွက်ပုံ

Recuva Wizard ကို သင် ရှာဖွေရယူလိုသောဖိုင်၏ အမည်အပြည့်အစုံ (သို့မဟုတ်) တစ်စိတ်တစ်ပိုင်းကို သိရသည့် အနေအထားတွင် အသုံးပြုရန် လိုအပ်သည်။ သင်သည် Recuva ကို ပထမဆုံးအကြိမ် သုံးစွဲခြင်းဖြစ်ပါကလည်း ၎င်းကို သုံးကြည့်သင့်သည်။ Recuva Wizard က ဖိုင်၏ အမျိုးအစား။ ၎င်းဖိုင်ကို ဖျက်သိမ်းခဲ့သည့်နေရာစသည်ဖြင့် သင့်အား သိရှိခွဲခြားစေပြီး စစ်ဆေးခြင်း တန်ဖိုးသတ်မှတ်ချက်များ ပြုလုပ်စေသည်။

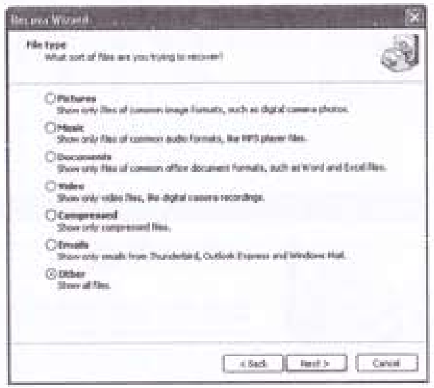
ဖျက်ထားသည့် ဖိုင်များကို ရှာဖွေစစ်ဆေးခြင်း စတင်ရန် အောက်ပါအဆင့်များကို ဆောင်ရွက်ပါ။

အဆင့် 1: Recuva ကို click လုပ်ပါ။ သို့မဟုတ် Start> Programs> Recuva> Recuva ကို ရွေးပြီး ပရိုဂရမ်ကို စတင်ပါ။ အောက်ပါ screen ပေါ်လာလိမ့်မည်။

ပုံ 1: 'Welcome to the Recuva Wizard' screen ပုံ

သတိပြုရန် ။ ။ သင် ရှာဖွေရယူလိုသော ဖိုင်၏ နာမည်အပြည့်အစုံ (သို့) တစ်ပိုင်း တစ်စကို သိပါက 'Piriform Recuva' ၏ ပင်မမျက်နှာစာ (main user interface)သို့ သွားရောက်ပြီး အခန်း '3.2 Recuva Wizard ကို အသုံးမပြုဘဲ ရှာဖွေစစ်ဆေးခြင်းတစ်ခု ဆောင်ရွက်ပုံ' ပါ အဆင့်များကို ဆောင်ရွက်ပါ။

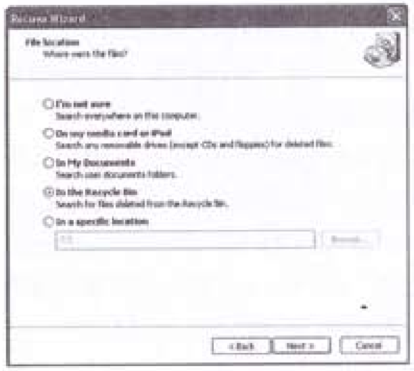
အဆင့် 2: အောက်ပါ screen သို့သွားရန် click လုပ်ပါ။



ပုံ 2: Recuva Wizard ဖိုင်အမျိုးအစားပြ screen ပုံ

Recuva Wizard ဖိုင်အမျိုးအစားပြ screen က ဖိုင်အမျိုးမျိုးတို့ကို ပြသထားပြီး option တစ်ခုစီကို enable လုပ်သည်နှင့် မည်သည့်ဖိုင်ကို ပြန်လည် ရယူနိုင်သည်ကို ဖော်ပြသည်။

အဆင့် 3: ပုံ 2 ရှိ အခြား Option များကို (check) စစ်ဆေးပြီး အောက်ပါ screen သို့ click လုပ်ပြီး သွားပါ။



ပုံ 3: Recuva Wizard ဖိုင်တည်နေရာပြ screen ပုံ

မှတ်ချက် ။ ။ Recuva Wizard ဖိုင်တည်နေရာပြ screen တွင် default setting မှာ " I'm not sure" ဖြစ်သည်။ ၎င်းက ကွန်ပျူတာရှိ drive များသာမက ပြင်ပမှ တပ်ဆင်ထားသော drive များ (CDs နှင့် DVDs မှလွဲ၍) ကိုပါ ရှာဖွေစစ်ဆေးခြင်း ပြုလုပ်သည်။ ထို့ကြောင့် ရလဒ်ကိုသိရန် အချိန်ယူရမည်။

ဖိုင်အများအပြားကို အဓိက ဖျက်သိမ်းသူမှာ Windows OS ရှိ အမှိုက်ခြင်း (Recycle bin)မှ ဖြစ်ပြီး ၎င်းက သင်၏ ကိုယ်ရေးကိုယ်တာနှင့် ထိခိုက်လွယ်သော ဖိုင်များကို မတော်တဆ ဖျက်မိပါက ပြန်လည်ရယူရန် အခွင့်အရေး နည်းပါးစေသည်။

အဆင့် 4: အထက်ပါ ပုံ 3 တွင် ဖော်ပြထားသော အမှိုက်ခြင်း (Recycle bin) option ကို စစ်ဆေးပြီး အောက်ပါ screen ကို သွားရန် click လုပ်ပါ။

ပုံ 4: **ကျေးဇူးတင်ပါသည်။ Recuva က သင်၏ ဖိုင်များကို ရှာဖွေရန် အဆင်သင့်ဖြစ်ပါပြီ။**

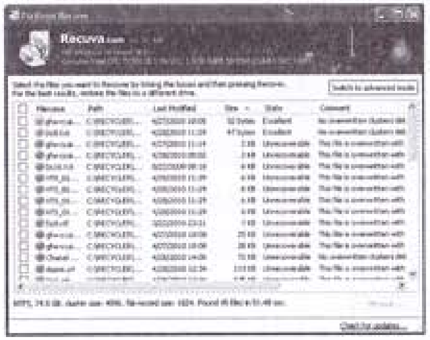
မှတ်ချက် ။ ။ ဤလေ့လာမှုအတွက် 'Deep Scan' option ကို enable မလုပ်ပါနှင့်။ ၎င်း စစ်ဆေးခြင်းနည်းလမ်းကို အခန်း 3.3 'Recuva ကို အသုံးပြုပြီး စေ့စေ့စပ်စပ် ရှာဖွေစစ်ဆေးပုံ' ကဏ္ဍတွင် ဆက်လက်ဆွေးနွေးပါမည်။

အဆင့် 5: သင်၏ ဖျက်သိမ်းထားသော ဖိုင်များကို ပြန်လည်ရယူရန် click လုပ်ပါ။

ဖိုင်ကို ပြန်လည်ရယူခြင်း လုပ်ငန်းစဉ်တွင် အခြေအနေပြ bar နှစ်ခုသည် လျှင်မြန်သော တိုးတက်မှု ပုံသဏ္ဍာန်ဖြင့် ပေါ်လာလိမ့် မည်။ Drive ပေါ်ရှိ ဖျက်ထားသော ဖိုင်များကို ရှာဖွေခြင်း အခြေအနေကို ပြသည့် box က ဖျက်ပြီးသော ဖိုင်များကို စာရင်းပြုစုသည်။ ဖိုင်တွင် ပါဝင်သော အကြောင်းအရာ၊ အခြေအနေကို စစ်ဆေးသည့်

bar က ၎င်းဖိုင်များ၏ အမျိုးအစားနှင့် ပြန်လည်ရရှိနိုင်သည့် အခြေအနေတို့ကို အုပ်စုများ ခွဲခြားစီစဉ်ပေးသည်။ ရှာဖွေခြင်းနှင့် စစ်ဆေးခြင်း လုပ်ငန်းစဉ်၏ ကြာမြင့်ချိန် ကိုလည်း ပြသပေးသည်။ သင်၏ 'Piriform Recuva' အဓိက မျက်နှာစာ၌ အောက်ပါပုံ ပေါ်လာလိမ့်မည်။

ပုံ 5: **ဖျက်ပြီးသား ဖိုင်များနှင့်** 'Piriform Recuva' **၏ အဓိကမျက်နှာစာပုံ**



'Piriform Recuva' ၏ ပင်မမျက်နှာစာ၌ ဖျက်ပြီးသား ဖိုင်များ၏ အချက်အလက်များကို စာရင်းပြုပြီး ကော်လံ 6 ခုခွဲ၍ ဖော်ပြထားသည်။ ကော်လံများကို အောက်ပါ ပုံစံအတိုင်း ဖော်ပြထားသည်။

ဖိုင်အမည် (File name) : ဖိုင်အမည်နှင့် ၎င်း၏ extensions များကို ဖော်ပြသည်။ ဖျက်ပြီးဖိုင်များကို အက္ခရာစဉ်အတိုင်း စီရန် 'File name' ကို click လုပ်ပါ။

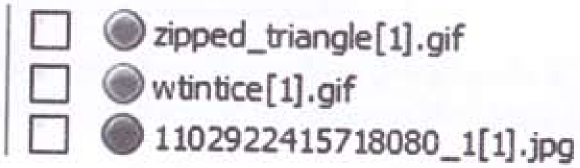
နေရာ (Path) : ဖျက်ပြီးသားဖိုင်ကို မည်သည့်နေရာတွင် တွေ့ရှိရသည်ကို ဖော်ပြသည်။ ဤဥပမာတွင် 'In the Recycle Bin' option ကို enable လုပ်ထားသည်ဟု ယူဆပါ။ ထိုအခါ ဖျက်ပြီးသား ဖိုင်များ၏ လမ်းကြောင်းနေရာမှာ C:RECYCLER ဖြစ်သည်။ သီးခြားလမ်းညွှန် (သို့) ဖိုင်တည်နေရာကို စာရင်းပြုထားသော ဖိုင်အားလုံးကို ကြည့်ရှုချင်ပါက 'Path' ကို click လုပ်ပါ။

နောက်ဆုံးပြုပြင်ချိန် (Last Modified) : ဖိုင်ကို မဖျက်ခင် ပြုပြင်မွမ်းမံခဲ့သည့် နောက်ဆုံးအချိန်ကို ဖော်ပြသည်။ သင် ရှာဖွေရယူလို သည့်ဖိုင်ကို ခွဲခြားပြရန်လည်း အကူအညီရသည်။ အဟောင်းဆုံးဖိုင်များနှင့် ယခုလက်ရှိ တည်ရှိခဲ့သော deleted ဖိုင်များကို စီစဉ်ရန် 'Last Modified' ကို click လုပ်ပါ။

အရွယ်အစား (size) : ဖိုင်၏ အရွယ်အစားကို ပြသည်။ ဖျက်ပြီးသားဖိုင်များကို အသေးဆုံး (သို့) အကြီးဆုံးမှ စတင်စာရင်းပြုစုပြရန် 'size' ကို နှိပ်ပါ။

အခြေအနေ (Status) : ၎င်းက ပြန်လည်ရယူနိုင်သော ဖိုင်၏ အလျားကို ပြသသည်။ အောက်ပါပုံ 6 တွင် ဆွေးနွေးထားသော ဖိုင် အခြေအနေပြ icon နှင့်လည်း ဆက်စပ်နေသည်။ ဖျက်ပြီးသားဖိုင်များကို အခြေခံအမျိုးအစား 3 မျိုး ခွဲခြားပြီး 'Excellent'မှနေ၍ 'Unrecoverable' အထိ စီစဉ်ရန် 'Status' ကို နှိပ်ပါ။
မှတ်ချက် (Comment) : ၎င်းကပေးထားသော ဖိုင်သည် မည်သည့်အကြောင်းကြောင့် ပြန်လည်ရယူနိုင် မရယူနိုင်ကို ပြသသည်။ 'Windows Master File Table'၌ ဖျက်ဆီးခဲ့ပြီးသော ဖိုင်များ၏ အလျားကိုလည်း ပြသသည်။ ဖိုင်တစ်ဖိုင် (သို့) ဖိုင်အစုအဝေးတစ်စုတို့ overwrite ပြုလုပ်ပြီးသော အလျားကို ကြည့်ရန် 'Comment' ကို နှိပ်ပါ။

ဖိုင်တစ်ဖိုင်စီတွင် ၎င်းဖိုင်ကို မည်မျှအထိ အောင်အောင်မြင်မြင် ပြန်လည်ရယူနိုင်မည်ဆိုသည်ကို ညွှန်ပြသော အရောင်ခြယ်ပြ (status icon) များ တွဲလျက်ပါသည်။



ပုံ 6: File အခြေအနေပြ (status icon)

အောက်ပါတို့မှာ status icon တစ်ခုစီကို ဖော်ပြထားသည်။
* အစိမ်းရောင် : အပြည့်အဝ ပြန်လည်ရယူရန် အခွင့်အရေး အလွန်ကောင်းသည်။
* လိမ္မော်ရောင် : ပြန်လည်ရယူရန် အခွင့်အရေးမှာ လက်ခံနိုင်သည့် အဆင့်ဖြစ်သည်။
* အနီရောင် : ပြန်လည်ရယူရန် အခွင့်အရေး မရှိလှပါ။

3.2 Recuva Wizard ကို အသုံးမပြုဘဲ စစ်ဆေးခြင်းတစ်ခု ပြုလုပ်ပုံ

Recuva Wizard ကို အသုံးမပြုဘဲ Recuva ၏ ပင်မမျက်နှာစာ (User Interface) ကို access လုပ်ရန် အောက်ပါအတိုင်း ဆောင်ရွက်ပါ။

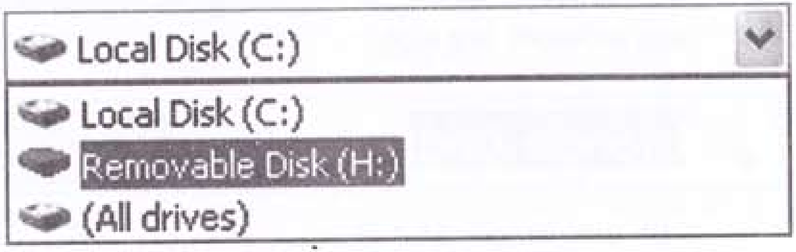
အဆင့် 1: Start>Programs>Recuva>Recuva ကို ရွေးချယ်ပါ (သို့) click လုပ်ပြီး ပုံ 1 ပါအတိုင်း ဆောင်ရွက်ပါ။

အဆင့် 2: 'Do not show this Wizard on statup' option ကို check လုပ်ပါ။ အောက်ပါပုံကို သွားရန် click လုပ်ပါ။

ပုံ 7: Recuva ၏ ပင်မမျက်နှာစာ (Main User Interface) ၏ ပုံ

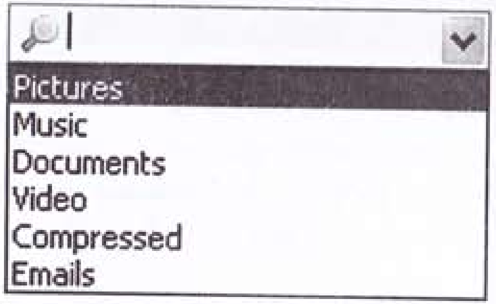
'Piriform Recuva' ၏ ပင်မမျက်နှာစာကို ဘယ်ဘက်ခြမ်းတွင် ရရှိသည့် ရလဒ်ပုံစံကို သုံးသပ်ချက် (Preview) ၊အချက်အလက် (Info) နှင့် ခေါင်းစဉ် (Header) ဟူ၍ tabs များ ခွဲခြားပြီး ၎င်းတို့က ဖျက်ပြီးသော ဖိုင်တစ်ခုချင်းစီ၏ သတင်းအချက်အလက်များကို အစီအစဉ်ကျအောင် ပြုလုပ်ထားသည်။ 'Piriform Recuva' သည် 'Recuva Wizard' မှာကဲ့သို့ပင် တိကျသော ရှာဖွေစစ်ဆေးမှု options များ သတ်မှတ်ခွင့်ပေးထားသည်။

အဆင့် 3: အပေါ်မှ ဆွဲချသည့် စာရင်း (drop-down list) ကို click လုပ်ပြီး ဆွဲယူပါ။ scan ပြုလုပ်စစ်ဆေးမည့် drive ကိုရွေးပါ။ 'Local Disk(c)' ကို default ပေးထားပြီး ဤဥပမာတွင် အသုံးပြုထားသည်။



ပုံ 8: Drop-down list yg Hard drives များ၏ ပုံ

ဖိုင်အမည်နှင့် တည်နေရာကိုပြသော drop-down list က သင် ရှာဖွေနေသော ဖိုင်အမျိုးအစားကို ခွဲခြားပြသပေးသည်။ ပုံ 2 တွင် ဖော်ပြထားသော Recuva Wizar ၏ 'File type' screen နှင့် အလားသဏ္ဍာန်တူသည်။



ပုံ 9: ဖိုင်အမည်နှင့် တည်နေရာပြ drop-down list ၏ ပုံ

ဖိုင်အမည်နှင့် တည်နေရာပြ လုပ်ဆောင်ချက်သည် drop-down list နှင့် စာရိုက်ထားသည့်အကွက် (text box) တို့ ပေါင်းစပ်ထားခြင်း ဖြစ်သည်။ ၎င်းတွင် အဓိက အသုံးချစရာ နှစ်မျိုးရှိသည်။ တိကျသော ဖိုင်တစ်ခုကို တိုက်ရိုက်ရှာဖွေခွင့်ပေးခြင်း၊ ဖိုင်အမျိုး အစားပေါ်မူတည်ပြီး ဖျက်ပြီးသား ဖိုင်စာရင်းကို စီစဥ်ပေးခြင်းတို့ဖြစ်သည်။

ဖိုင်အမည်နှင့် တည်နေရာပြ လုပ်ဆောင်ချက်သည် ဖိုင်အမျိုးအစား အတိအကျ ရှာဖွေခြင်းနှင့် ရလဒ်ပုံစံတွင် ပြထားသော ဖျက်ပြီး ဖိုင်များ၏ အထွေထွေစာရင်းကို စီစဥ်ပေးခြင်းတို့ ပြုလုပ်ပေးသည်။

အမည်အပြည့်အစုံ (သို့) တစ်စိတ်တစ်ပိုင်းကို သိထားသော ဖိုင်ကို စစ်ဆေးခြင်း ပြုလုပ်ရန် အောက်ပါအဆင့်အတိုင်း ဆောင်ရွက်ပါ။

အဆင့် 1: သင် ရယူလိုသောဖိုင်၏ အမည်အပြည့်အစုံ (သို့) တစ်ပိုင်းတစ်စကို အောက်ပါအတိုင်း ရိုက်ထည့်ပါ။ (ဤဥပမာတွင် ဖိုင် triangle.png ကို scan ဖတ်နေပုံကို တွေ့ရမည်။)

ပုံ 10: triangle. png ဖိုင်ကို ပြထားသော ဖိုင်အမည်နှင့် တည်နေရာ drop-drown list ၏ ပုံ

သတိပြုရန် ။ ။ ဖိုင်အမည်နှင့် တည်နေရာကို reset ပြန်လုပ်ပါ။ (မီးခိုးရောင် ပုံသဏ္ဍာန်ဖြင့် ပေါ်လာသည်။)

အဆင့် 2: သင်၏ ဖျက်ပြီးသား ဖိုင်များကို scan ဆက်လုပ်ရန် click ပါ။ ခဏ အကြာတွင် အောက်ပါအတိုင်း screen တစ်ခု ပေါ်လာလိမ့်မည်။

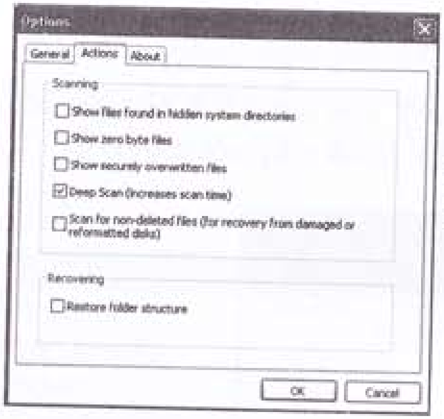
ပုံ 11: သုံးသပ်ချက် (Preview tab) အတွင်း၌ တွေ့ရသော triangle.png ဖိုင်ကို ပြထားသည့် Recuva user interface ၏ ပုံ

3.3 Recuva ကို အသုံးပြုပြီး စေ့စေ့စပ်စပ်ရှာဖွေစစ်ဆေးခြင်းတစ်ရပ် ဆောင်ရွက်ပုံ

စေ့စေ့စပ်စပ် ရှာဖွေစစ်ဆေးခြင်း (Deep Scan) option ကို enable လုပ်ခြင်းသည် scan ဖတ်ရာတွင် ပို၍ နှံ့နှံ့စပ်စပ် ရှာဖွေ စစ်ဆေးပေးသည်။ သင့် ကွန်ပျူတာ၏ အမြန်နှုန်းနှင့် သင့်၌ ရှိသောဖိုင်အရေအတွက်ကို မူတည်၍ အချိန်လည်း ပိုကြာနိုင်သည်။ သင်မူလ ရှာဖွေသောဖိုင်ကို scan က မပြသည့်အခါ ဤ option က အသုံးဝင်ကြောင်း ပြလိမ့်မည်။ Deep scan ပြုလုပ်ခြင်းသည် သင်၏ ကွန်ပျူတာ၌ သိုလှောင်ထားသော အချက်အလက် (data) ပမာဏပေါ်မူတည်ပြီး နာရီ အနည်းငယ် ကြာနိုင်သော်လည်း သင် လိုအပ်သော ဖိုင်များကို ပြန်လည်ရယူရန် အခွင့်အရေး ပိုမိုရရှိသည်။

Recuva Wizard အတွင်းရှိ 'Enable Deep Scan' option ကို check လုပ်ခြင်းဖြင့် ၎င်းကို အသုံးပြုနိုင်သည်။ (ပုံ 4 တွင် ကြည့်ပါ။)

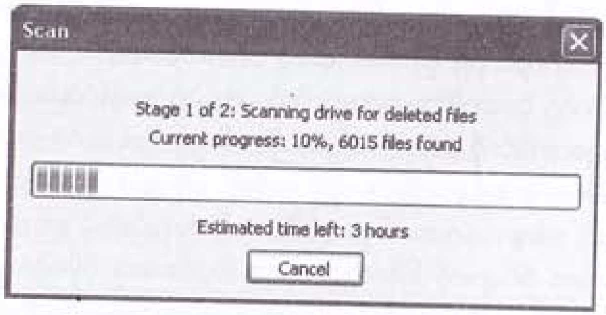
အဆင့် 1: 'Options' screen သို့ click လုပ်ပြီးသွားပါ။ 'Actions' tab ကို click လုပ်ပါ။



ပုံ 12: 'Actions' tab အပါအဝင် 'Options' screen၏ ပုံ

အဆင့် 2: 'Deep Scan' option ကို check လုပ်ပါ။ (scan ဖတ်ချိန်ကို တိုးထားပါ) ထို့နောက် click လုပ်ပါ။

အဆင့် 3: 'Deep Scan' option ကို အသုံးပြုပြီး ဖျက်ပြီးသားဖိုင်များကို စစ်ဆေးခြင်း စတင်ရန် click လုပ်ပါ။ အစဦးက ပြောခဲ့သည့်အတိုင်း 'Deep Scan' သည် သင့် ကွန်ပျူတာ၏ မြန်နှုန်းနှင့် Hard disk တို့၏ အရွယ်အစား ပေါ်မူတည်ပြီး နာရီအနည်းငယ် ကြာနိုင်သည်။



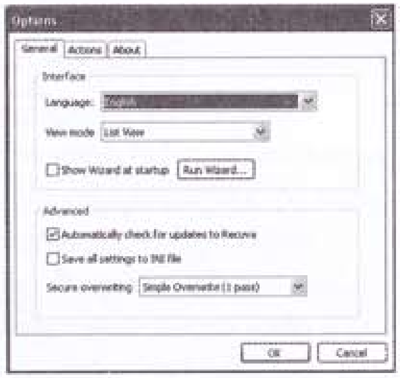
ပုံ 13: 'Deep Scan' အတွက် လိုအပ်သောခန့်မှန်းခြေကြာမည့်နာရီကို ပြသထားသည့် စစ်ဆေးခြင်းတစ်ခုပုံ

3.4 'Options' screen အတွက် မိတ်ဆက်ခြင်း

ဤအပိုင်းတွင် 'Options' screen မှတစ်ဆင့် သင်၏ ကိုယ်ရေးကိုယ်တာနှင့် ထိခိုက်လွယ်သော သတင်း အချက်အလက်များကို အောင်မြင်စွာ ရှာဖွေရယူခြင်းနှင့် ဖျက်ဆီးခြင်းများပြုလုပ်ရန် အသုံးချပုံအမျိုးမျိုးတို့ကို လေ့လာနိုင်သည်။ ၎င်း အသုံးချနည်းများ (settings) ပြုလုပ်ရန် အောက်ပါအတိုင်း ဆောင်ရွက်ပါ။

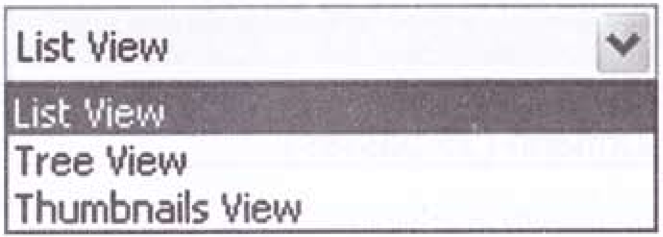
အဆင့် 1: အောက်ပါ screen သို့ click လုပ်ပြီး သွားပါ။

ပုံ 14: Default mode ဖြင့် ပေးထားသော 'General' tab ကို 'Options' screenနှင့် တွေ့ရပုံ



'Options' screen ကို အထွေထွေ(General)၊ ပြုမူပုံ (Actions) နှင့် အကြောင်းအရာ (About) ဟူ၍ tabs များ ခွဲခြားထားသည်။

'General' tab တွင် အရေးကြီးသော အသုံးချပုံအချို့ကို ပြုလုပ်ခွင့်ပြုသည်။ ၎င်းတို့မှာ language (Recuva သည် ဘာသာစကားပေါင်း 37 မျိုးကို အသုံးပြုနိုင်သည်) View mode နှင့် Recuva Wizard ကို enable (သို့)disable ပြုလုပ်ခြင်းပင် ဖြစ်သည်။



ပုံ 15: View mode ၏ drop-down list ပုံ

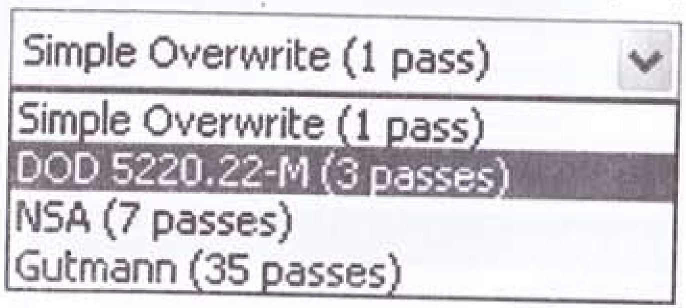
View mode သည် သင် ကြည့်ရှုလိုသော deleted ဖိုင်များကို ရွေးချယ်ခွင့်ပေးသည်။ 'Piriform Recuva' ရှိ ဖိုင်တစ်ဖိုင်ကို right click လုပ်သည်နှင့် ၎င်း view mode ကို enable လုပ်ပြီး ဖြစ်သည်။

* List: ဤ option က ပုံ 5 တွင် ပြထားသည့်အတိုင်း ဖျက်ပြီးသား ဖိုင်များ၏ စာရင်းကို ကြည့်နိုင်သည်။
* Tree: ဤ option က ဖျက်ပြီးဖိုင်များ၏ တည်နေရာ လမ်းကြောင်းများကို သစ်ပင်ပုံသဏ္ဍာန် အကိုင်းအခက်များ ခွဲခြားပြသပေးသည်။
* Thumbnails: ဤ option က ဖျက်ပြီးသား ဖိုင်များကို ဖြစ်နိုင်ပါက ဂရပ်ဖစ်နှင့် ရုပ်ပုံသဏ္ဍာန်များဖြင့် ပြသသည်။

'General' tab ၏ အဆင့်မြင့်အပိုင်းတွင် သင့်အား ရန်လိုသော(သို့) ပြိုင်ဘက်အဖွဲ့အစည်းများမှ သင်၏ data များကို ရယူခြင်းမှ ကာကွယ်ရန် ၎င်းတို့ကို overwrite ဖြစ်စေမည့် အကြိမ်အရေအတွက်ကို သတ်မှတ်ထားနိုင်သည်။

လုံခြုံစိတ်ချရသော overwriting drop-down list က သင်၏ ကိုယ်ရေးကိုယ်တာ အချက်အလက်များကို overwrite လုပ်ရန်အတွက် option လေးခု ပြထားသည်။ ၎င်း၏ default mode သည် Simple Overwrite (1pass) ဖြစ်ပြီး ပုံ 14 တွင် ဖော်ပြထားသည်။ 'Pass' တစ်ခုသည် သင်၏ မှတ်တမ်းမှတ်ရာများ၊ ဖိုင် (သို့) folder တို့ကို အလှည့်သင့်ရာ data များဖြင့် လုံးဝ ဖတ်ရှု၍ မရနိုင်အောင် overwrite လုပ်မည့် အကြိမ်အရေအတွက်ကို ရည်ညွှန်းသည်။

အဆင့် 2: DOD 5220.22-M(3 passes) option ကို အောက်ပါအတိုင်း ရွေးချယ်ပါ။

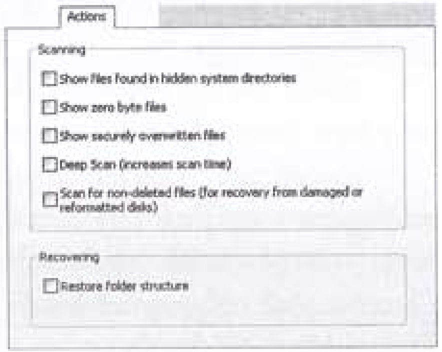


ပုံ 16: DOD 5220.22-M(3 passes) ကို ရွေးချယ်ထားသော လုံခြုံစိတ်ချရသည့် overwriting drop-down list ၏ ပုံ

ပေးထားသော မှတ်တမ်း၊ ဖိုင်နှင့် folder တို့ကို overwrite လုပ်ခြင်းတွင် 'pass' တစ်ခုသည် အတော်အတန် အကျိုးသက်ရောက်မှုရှိပါသည်။ သို့သော် ပေါ့ပါးလုံခြုံမှုရှိသော overwrite တစ်ခုကို ပြန်လည်ရယူရန် ကျွမ်းကျင်မှုနှင့် အရင်းအမြစ်များပါရှိသော အဖွဲ့အစည်းများစွာလည်း ရှိပါသည်။ '3 passes' တွင်မူ လုံခြုံမှုရှိသော overwrite ဆောင်ရွက်ရန် အချိန်နှင့်မှတ်တမ်း၊ ဖိုင်နှင့် folder များ ပြန်လည်ရယူရန် စွမ်းရည်နှစ်ခုကြားတွင် ခိုင်မာသော ဟန်ချက်ညီမှု (balance) ရှိသည်။

အဆင့် 3: 'General' tab ၏ ဆောင်ရွက်မှု options ကို save လုပ်ပါ။

ပုံ 17: 'Actions' tab ပါဝင်သော 'Options' screen ၏ ပုံ



Hidden system ၏ လမ်းညွှန်ချက်များတွင် တွေ့ရသော ဖိုင်များကို ပြပါ (Show files found in hidden system directories) : ဤ option သည် hidden system လမ်းညွှန်ချက်များမှ ဖိုင်များကို ပြသခွင့်ပေးသည်။

Zero-byte ဖိုင်များပြပါ (Show Zero-byte files) : ဤ option သည် ဖိုင်အတွင်း၌ မည်သည့် အချက်အလက်မှ မပါရှိသော၊ အခြေခံအားဖြင့် ပြန်လည်ရယူရန် မဖြစ်နိုင်သောဖိုင်များကို ပြထားပေးသည်။

လုံခြုံစွာဖျက်ဆီးပြီးသော ဖိုင်များကိုပြပါ (Show securely delected files): ဤ option သည် ရလဒ်ပြသည့်နေရာ၌ လုံခြုံစွာဖျက်ဆီးပြီးသော ဖိုင်များကို ပြသပေးသည်။

မှတ်ချက် ။ ။ CCleaner (သို့) ၎င်းနှင့် ပုံစံတူ ပရိုဂရမ်တစ်ခုကို သင် အသုံးပြုပြီးဖြစ်ပါက လုံခြုံရေး အကြောင်းအချက်ကြောင့် ဖျက်ဆီးပြီးသော ဖိုင်တစ်ခု၏ အမည်ကို ZZZZZZZ.ZZZ သို့ ပြောင်းလဲပေးသည်။

Deep Scan : ဤ option သည် ဖျက်ပြီးသော မှတ်တမ်း (သို့) ဖိုင်ကို ရှာဖွေရန် drive တစ်ခုလုံးကို scan လုပ်သည်။ အရင်ပြုလုပ်ဖူးသော scan တွင် သင့်ဖိုင်၏ တည်နေရာကို အကျိုးရှိရှိ မရှာဖွေနိုင်ပါက ယခု Deep Scan က အသုံးဝင်ကြောင်း တွေ့ရပါလိမ့်မည်။ သို့သော် အချိန်များများ လိုပါသည်။ အခန်း 3.3 'Recuva ကို အသုံးပြုပြီး စေ့စေ့စပ်စပ် ရှာဖွေစစ်ဆေးခြင်း ဆောင်ရွက်ပုံ' တွင် လေ့လာပါ။

Scan for non-deleted files (ပျက်စီးနေသော (သို့) format ပြန်ချထားသော disk များမှ ရယူရန်) : ဤ option သည် disk များ၏ ပြင်ပပုံသဏ္ဍာန်ပျက်စီးမှု (သို့) Sofrware နှင့် ပတ်သက်သော ပျက်စီးမှုကြောင့် ပျောက်သွားသော ဖိုင်များကို ပြန်လည်ရယူပေးသည်။

'About' tab က Piriform web site နှင့် ၎င်း၏ သက်ဆိုင်ရာ အဆက်အသွယ်များ (links) နှင့် 'version' အချက်အလက်များကို ပြသပေးသည်။

ယခုသင်သည် 'Options' screen ပေါ်ရှိ 'General', 'Action' tab များ၏ အသုံးချမှုများ၊ scan လုပ်ရန် နည်းလမ်းအမျိုးမျိုးတို့ကို ပိုမိုထိတွေ့မှု ရှိလာပါပြီ။ ထို့အတူ အခန်း 4.0 တွင် သင်၏ ကိုယ်ရေးကိုယ်တာနှင့် ထိခိုက်လွယ်သော ဖိုင်များကို ပြန်လည်ရယူပုံနှင့် လုံခြုံစွာဖျက်ဆီးပုံအကြောင်းများကို သင်ယူလေ့လာရန် အဆင်သင့်ဖြစ်လောက်ပြီဟု ထင်ပါသည်။

Recuva ကို အသုံးပြုပြီး ဖိုင်များပြန်လည်ရယူပုံနှင့် ဖိုင်များလုံခြုံစွာဖျက်ဆီးပုံ

- 4.0 သင် စတင်အသုံးမပြုခင်
- 4.1 ဖျက်ပြီးသားဖိုင်ကို ပြန်လည်ရယူပုံ
- 4.2 Pop-up menu အသုံးပြုပုံ
- 4.3 ဖျက်ပြီးသားဖိုင်ကို လုံခြုံစိတ်ချစွာ ဖျက်ဆီးပုံ

4.0 သင်စတင် အသုံးမပြုခင်

ဤအပိုင်းတွင် ဖျက်ပြီးသားဖိုင်ကို မည်သို့ ပြန်လည်ရယူရမည်ကိုလည်းကောင်း၊ သင်၏ ကိုယ်ရေးကိုယ်တာနှင့် ထိခိုက်လွယ်သော သတင်း အချက်အလက်များကို မည်သို့ လုံခြုံစိတ်ချစွာ ဖျက်ဆီးမည်ကိုလည်းကောင်း လေ့လာနိုင်သည်။

Recuva က သင် ပြန်လည်ရယူထားသော ဖိုင်များသိမ်းရန် folder အသစ်

တစ်ခုကို တည်ဆောက်ခွင့်ပေးသည်။ Recuva က ရှိပြီးသား folder များကို အသုံးပြုခွင့်ပေးသော်လည်း လုံခြုံရေးအတွက် သင် ပြန်လည်ရယူထားသော ဖိုင်များကို backup drive (သို့) USB memory stick ကဲ့သို့ ရွှေ့ပြောင်းနိုင်သောကိရိယာများတွင် ကူးယူထည့်သွင်းထားပါ။

အရေးကြီး ။ ။ Recuva သည် လုံခြုံစွာဖျက်ဆီးခြင်းအတွက် ကောင်းမွန်သော လုပ်ဆောင်မှုရှိသော်လည်း ဖိုင်များတည်ရှိမှုကို မှတ်သားရန် file marker တစ်ခု ထားရှိသည်။ ၎င်းက သင်၏ ကိုယ်ရေးကိုယ်တာနှင့် လုံခြုံရေးကို ကာကွယ်ရန် အရေးကြီးပြီး ထိခိုက်လွယ်သော သတင်း အချက်အလက်များကို မူလတည်နေရာတွင် မဟုတ်ဘဲ ရွှေ့ပြောင်းနိုင်သော ကိရိယာတစ်ခုသို့ ကူးယူသိမ်းထားရန် အာရုံခံပေးသည်။

4.1 ဖျက်ပြီးသားဖိုင်ကို ပြန်လည်ရယူပုံ

ဖျက်ပြီးသားဖိုင်ကို ပြန်လည်ရယူရန် အောက်ပါ အဆင့်များ ဆောင်ရွက်ပါ။

အဆင့် 1: သင်၏ ကွန်ပျူတာတွင် ရွှေ့ပြောင်းတပ်ဆင်နိုင်သော disk (သို့) USB memory stick ကို ဆက်သွယ်ထားပါ။

အဆင့် 2: 'Recuva' ကို enable လုပ်ရန် သင်ရယူလိုသော ဖိုင်၏ အနောက်တွင် ရှိသော 'check box' တွင် check လုပ်ပါ။ သို့မဟုတ် ၎င်းဖိုင်အား double click နှိပ်ခြင်းဖြင့် check လုပ်ပြီး မှတ်သားထားပါ။

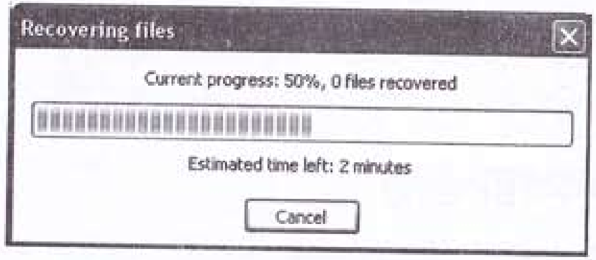
အဆင့် 3: 'Browse For Folder' screen ကို click လုပ်ပြီး သွားပါ။

အဆင့် 4: အောက်ပါပုံ 1 တွင် ပြထားသည့်အတိုင်း သင်၏ 'recovery folder'ကို တည်ဆောက်ရန် နေရာရွေး၍ click လုပ်ပါ။

ပုံ 1: ရွှေ့ပြောင်းတပ်ဆင်နိုင်သော ကိရိယာပေါ်ရှိ အသစ်ပြုလုပ်ထားသော folder ကို ပြသထားသော 'Browse For Fol-der' dialog box' ၏ ပုံ

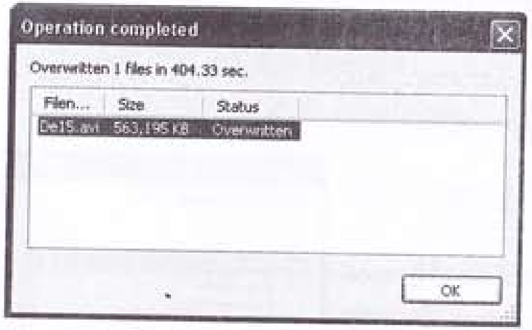
မှတ်ချက် ။ ။ ဤဥပမာတွင် သင် ပြန်လည်ရယူထားသောမှတ်တမ်းများနှင့် ဖိုင်များကို သိုလှောင်ရန် တည်ဆောက်ထားသော folder ကို သိသာထင်ရှားသော နာမည်အညွှန်း ပေးရမည်။ သို့သော် သင်၏ folder ကို အမည်ပေးရာတွင် သင်၏ ပုဂ္ဂိုလ်ရေးနှင့် လုံခြုံရေးကို တွေးတောဆင်ခြင်၍ ပိုမိုဂရုစိုက်သင့်သည်။

အဆင့် 5: ဖိုင်ရယူမှုလုပ်ငန်းစဉ် စတင်ရန် click လုပ်ပါ။ လုပ်ငန်းစဉ် အခြေအနေပြ screen အောက်ပါအတိုင်း ပေါ်လာလိမ့်မည်။



ပုံ 2: ဖိုင်ပြန်လည်ရယူခြင်း လုပ်ငန်းစဉ်အခြေအနေပြ screen ပုံ

ဖိုင်များ ပြန်လည်ရယူပြီးနောက် အတည်ပြုချက်ယူမည့် screen အောက်ပါ အတိုင်း ထွက်ပေါ်လာလိမ့်မည်။



ပုံ 3: အလုပ်ပြီးမြောက်ခြင်းပြသည့် screen ၏ ပုံ

မှတ်ချက် ။ ။ Recuva က ဖိုင်ပြန်လည်ရယူမှု နည်းလမ်းအမျိုးမျိုးကို အထောက်အကူ ပြုသည်။ သင် ပြန်လည်ရယူလိုသော ဖိုင်၏ 'check box' ကို 'check ပေးပြီး အဆင့် 3 မှ 5 အထိ ဆောင်ရွက်ပါ။

ယခုသင်သည် ယခင်ဖျက်ပြီးသားဖိုင်များ ပြန်လည်ရယူခြင်းကို အဆင်ပြေအောင် ဆောင်ရွက်နိုင်ပြီဖြစ်ရာ pop-up menu ရှိ ဖိုင်ရယူနည်းအမျိုးမျိုးနှင့် ဖိုင်များကို လုံခြုံမှုရှိရှိ ဖျက်သိမ်းခြင်းများ ပြုနိုင်ရန် လေ့လာသင်ယူနိုင်ပါပြီ။

4.2 Pop-up Menu ကို အသုံးပြုပုံ

Recuva က သင်ဖျက်ချင်သော (သို့) ဖျက်ဆီးချင်သော မှတ်တမ်း၊ ဖိုင်နှင့် folder များကို ရွေးချယ်ရန် 'options' အမျိုးမျိုး ပေးထားသည်။

* စစ်ဆေးခြင်း (Checking) ကို ပြန်လည်ရယူရန် (သို့) ဖျက်ဆီးရန် အကွဲကွဲ အပြားပြားဖြစ်နေသော ဖိုင်များကို မြန်မြန်ဆန်ဆန် ရွေးချယ်ရာတွင် အသုံးပြုသည်။
* သီးခြားမှတ်သားခြင်း (Highlighting) ကို ပြန်လည်ရယူရန် (သို့) ဖျက်ဆီးရန် အစုအဝေးတစ်ခုအနေဖြင့် ဆက်စပ်နေသော ဖိုင်အမျိုးမျိုးတို့ကို မြန်မြန်ဆန်ဆန် ရွေးချယ်ရာတွင် အသုံးပြုသည်။

pop-up တစ်ခုကို ဆောင်ရွက်ရန် Recuva ရှိ ဖျက်ပြီးသား ဖိုင်တစ်ခုကို right click နှိပ်ပါ။

Recover Highlighted : သင် သီးခြားမှတ်သားထားသော ဖျက်ပြီးသား ဖိုင်များကို ပြန်လည်ရယူပေးသည်။

Recover Checked : 'Check' လုပ်ထားသော ဖျက်ပြီးဖိုင်ကို ပြန်လည် ရယူပေးသည်။

Check Highlighted : သင် သီးခြားရွေးထားသော ဖျက်ပြီးဖိုင်ကို 'Check' လုပ်ပေးသည်။

Uncheck Highlighted : သင် သီးခြားရွေးထားသော ဖျက်ပြီးဖိုင်ကို 'Uncheck' လုပ်သည်။

သင် သိထားသကဲ့သို့ပင် 'options' screen ရှိ 'General' tab ၌လည်း View Mode ကို ထားရှိနိုင်သည်။ ၎င်းက ဖျက်ပြီးဖိုင်များကို သင်ကြည့်လိုသည့် ပုံစံ အတိုင်း ရွေးချယ်ခွင့်ပေးသည်။

* List : ဤoption သည် ပုံ 4 တွင် ပြထားသည့်အတိုင်း ဖျက်ပြီး ဖိုင်များကို စာရင်းတစ်ခုအဖြစ် ကြည့်ရှုခွင့်ပြုသည်။

* Tree : ဖျက်ပြီးဖိုင်များ၏ လမ်းကြောင်းတည်နေရာကို သစ်ပင်တစ်ပင်၏ အကိုင်းအခက်များ ပုံသဏ္ဍာန် ပြုလုပ်ပြသပေးသည်။
* Thumbnails : ဤ option က ဖြစ်နိုင်ပါက ဖျက်ပြီးဖိုင်များကို ဂရပ်ဖစ်(သို့) ရုပ်ပုံပုံစံများဖြင့် ပြသပေးသည်။

Highlight Folder : ဤ option က လမ်းကြောင်းတည်နေရာအရ ဖျက်ပြီးသားဖိုင်အမျိုးမျိုးကို ရွေးချယ်ခွင့်ပေးသည်။ ၎င်းတို့၏ pop-up menu တွင် ပါရှိသော ဆောင်ရွက်မှုများကိုလည်း ပြုလုပ်ခွင့်ပေးသည်။

Secure Overwrite Highlighted : ဤ option က သီးခြားမှတ်သားထားသော ဖျက်ပြီး ဖိုင်ကို ဖျက်ဆီးခွင့်ပြုသည်။

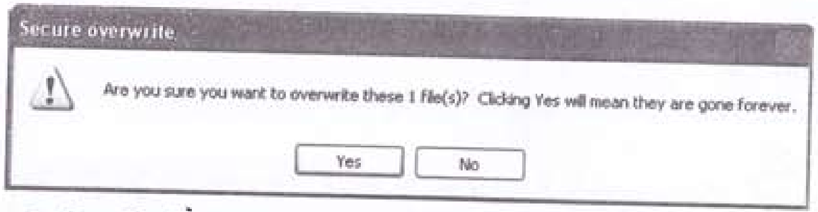
Secure Overwrite Checked: ဤoption က 'check' လုပ်ထားသော ဖျက်ပြီးဖိုင်ကို ၎င်း၏ status icon အား အနီရောင်သို့ ပြောင်းလဲစေပြီး လုံခြုံစွာ ဖျက်ဆီးခွင့်ပြုသည်။

4.3 ဖျက်ပြီးသားဖိုင်ကို လုံခြုံစိတ်ချစွာ ဖျက်ဆီးပုံ

ဖျက်ပြီးဖိုင်ကို လုံခြုံစွာ ဖျက်ဆီးရန် အောက်ပါအဆင့်များကို ဆောင်ရွက်ပါ။

အဆင့် 1: သင်လုံခြုံစွာ ဖျက်ဆီးလိုသော ဖိုင်တစ်ဖိုင် ရွေးပါ။ 'check box' ကို right click နှိပ်ပြီး pop-up menu ကို သွားပါ။

အဆင့် 2: အောက်ပါ အတည်ပြုချက်ယူမည့် dialog box ကို လုပ်ဆောင်ရန် ရွေးချယ်ပါ။



ပုံ 4: လုံခြုံမှုရှိသောဖျက်ဆီးခြင်းအတွက် အတည်ပြုချက်ရယူမည့် dialog box ပုံ

အဆင့် 3: overwrite လုပ်ငန်းစဉ် စတင်ရန် click လုပ်ပါ။ ဖိုင်၏ အရွယ်အစားနှင့် အခြေအနေကိုမူတည်၍လည်းကောင်း။ 'Options' screen ရှိ 'General'

tab မှ သင်ရွေးချယ်သော overwrite option ကြောင့်လည်းကောင်း အချိန်အနည်းငယ် ကြာနိုင်သည်။ Overwriting ပြီးစီးပါက အောက်ပါ screen ပေါ်လာလိမ့်မည်။

ပုံ 5: လုပ်ငန်းစဉ် ပြီးပြည့်စုံကြောင်းပြသည့် screen

မူလက ဖျက်ထားသော ဖိုင်များကို Recuva အား အသုံးပြု၍ ပြန်လည်ရယူခြင်းနှင့် လုံခြုံစွာဖျက်ဆီးခြင်းကို သင် အောင်မြင်စွာ လုပ်ဆောင်နိုင်ပါပြီ။ Recuvaနှင့် ပတ်သက်သော သင်၏ပဟုသုတတို့ကို သုံးသပ်ဝေဖန်ရန် 'မေးလေ့ရှိသော မေးခွန်းများနှင့် သုံးသပ်ချက်' အခန်းသို့ ဆက်ကြပါဦးစို့။

5.0 မကြာခဏ မေးလေ့ရှိသော မေးခွန်းများနှင့် သုံးသပ်ချက်

အယ်လီနာနှင့် နီကိုလိုင်တို့သည် Recuva ၏ လွယ်ကူအကျိုးရှိသော အလုပ်လုပ်ဆောင်ပုံကို များစွာကျေနပ်အားရလျက်ရှိသည်။ သို့သော်လည်း သူတို့ နှစ်ယောက်စလုံး၌ ဤ software ၏ အဆင့်မြင့် options များနှင့် အချို့အကြောင်းအရာများကို မေးရန် မေးခွန်းတချို့ ရှိနေကြသည်။

မေး ။ ။ Recuva က ပြန်လည်ရယူဖို့မတတ်နိုင်တဲ့ ဖိုင်အမျိုးအစားများ ရှိပါသလား။

ဖြေ ။ ။ မရှိပါဘူး။ Recuva က ဖိုင်အားလုံးကို ရယူပေးနိုင်ပါတယ်။

မေး ။ ။ လုံခြုံစွာ ဖျက်ဆီးပြီးတဲ့ ဖိုင်ကို ပြန်လည်ရယူနိုင်ပါသလား။

ဖြေ ။ ။ တစ်ခါဖျက်ဆီးပြီးသွားရင် ဘယ်တော့မှ ပြန်မရနိုင်တော့ပါဘူး။

မေး ॥ ॥ ကျွန်တော် တစ်ခါတလေ သတိထားမိတာက ဖိုင်တစ်ဖိုင်ကို လုံးဝ ဖျက်ဆီးပြီးသည့်တိုင် အဲဒီဖိုင်ကို ပြန်လည်ရယူနိုင်ဖို့ မှတ်သားထားသည့်ပုံမျိုးတွေ့ရတာ ဖြစ်နိုင်ပါ့မလား။

ဖြေ ॥ ॥ မင်းဟာ မူရင်းဖိုင်တစ်ဖိုင် တည်ရှိတဲ့နေရာကို ညွှန်ပြတဲ့ 'file maker' တစ်ခုကိုတွေ့တာ ဖြစ်နိုင်ပါတယ်။ ဒါပေမဲ့ မင်း အဲဒီဖိုင်ကို ရယူပြီး ဖွင့်ကြည့်တဲ့အခါ အထဲမှာပါတဲ့ အချက်အလက်တွေကို ဖတ်လို့ရမှာ မဟုတ်ပါဘူး။

မေး ॥ ॥ ကျွန်တော် ကျန်ခဲ့တဲ့ 5 မိနစ်လောက်ကမှ ဖန်တီးထားတဲ့ ဖိုင်တစ်ခုကို မတော်တဆ ဖျက်လိုက်မိပါတယ်။ အဲဒါကို လွယ်လွယ်နဲ့ ပြန်လည်ရယူနိုင်မယ်လို့ ထင်ခဲ့တယ်။ ဘာဖြစ်လို့များ Recuva က ပြန်မရှာပေးနိုင်တာလဲ။

ဖြေ ॥ ॥ ရယ်စရာကောင်းတာက သင့် ကွန်ပျူတာပေါ်မှာ မိနစ် အနည်းငယ် လောက်က ပြုလုပ်ထားတဲ့ ဖိုင်ကိုရှိပြီး temporary file တွေက overwrite လုပ်တဲ့ ဖြစ်နိုင်ချေက အချိန်အတော်ကြာကတည်းက ကွန်ပျူတာပေါ်မှာရှိခဲ့တဲ့ ဖိုင်တွေကို overwrite လုပ်ခြင်းထက် ပိုများတယ် ဆိုတာပါပဲ။ Recuva က ဖန်တီးထားတာ မကြာသေးတဲ့ဖိုင်တွေကို ချက်ချင်းဖျက်ဆီးပစ်လိုက်တာမျိုးကို ပြန်လည်ရယူဖို့ မလွယ် ပါဘူး။

မေး ॥ ॥ ကျွန်တော့် ကွန်ပျူတာ system ကို CCleaner နဲ့ ရှင်းလင်းပြီးတဲ့အခါမှာ data တွေကို ပြန်လည်ရယူနိုင်ပါ့မလား။

ဖြေ ॥ ॥ ပြန်လည်ရှာဖွေရယူမှု ပြုလုပ်တဲ့ လူရဲ့ ကျွမ်းကျင်မှုနဲ့ ရရှိနိုင်တဲ့ အရင်း အမြစ်တွေပေါ် မူတည်ပြီး ဖြစ်နိုင်ချေရှိပါတယ်။ CCleaner မှာ Windows ရဲ့ မှတ်ပုံတင်စာနှင့် ယာယီဖိုင်တွေကိုရှင်းတဲ့အခါ သင် အသုံးပြုတဲ့ ဖျက်သိမ်းခြင်း စနစ်များ သေချာမှု ရှိ မရှိပေါ်မှာ မူတည်ပါတယ်။ သင့်ရဲ့ ကိုယ်ရေးကိုယ်တာနဲ့ ထိခိုက် ပျက်စီးလွယ်တဲ့ အချက်အလက်တွေကို အခြားသူများအတွက်လုပ်ဖို့ အခွင့်အလမ်း မရှိအောင်လုပ်မယ်ဆိုရင် CCleaner မှာ 'Secure Deletion' option ကို enable လုပ်ပါ။ Recuva မှာလည်း data တွေကို လုံခြုံစွာ overwrite လုပ်ဖို့ 'Passes' တွေကို အသုံးပြုခဲ့သလိုမျိုးပေါ့။ ဒါဟာ မေးခွန်းကောင်းတစ်ခုပါပဲ။ ဘာဖြစ်လို့လဲဆိုတော့ သင့်ရဲ့ ပုဂ္ဂိုလ်ရေး၊ လုံခြုံရေးဆိုင်ရာတွေကို ကာကွယ်မှုပြုဖို့ ကြိုးစားရာမှာ tools တွေဟာ တစ်ခုနဲ့တစ်ခု ဘယ်လိုဆက်စပ်ပြီး အလုပ်လုပ်တယ်ဆိုတာကို ပြသနိုင်လို့ပါပဲ။

5.1 မေးခွန်း သုံးသပ်ချက်

* ကွန်ပျူတာကို ပိတ်ခြင်းက သင်ဖျက်ထားတဲ့ မှတ်တမ်း၊ ဖိုင်နဲ့ folder တွေကို Recuva ကနေ အကျိုးရှိရှိ ပြန်လည်ရယူနိုင်စွမ်း လျော့ကျစေပါသလား။
* ဖိုင် (သို့) မှတ်တမ်းတစ်ခုကို overwrite လုပ်ရာမှာ 'Pass' အရေအတွက်ကို တိုးပေးခြင်းက ဘာအကျိုးသက်ရောက်မှု ဖြစ်စေသလဲ။
* Recuva တွင် ဖျက်ပြီး ဖိုင် (သို့) မှတ်တမ်းတစ်ခုကို အောင်မြင်စွာ ပြန်လည် ရယူရန် အကျိုးရှိသည့် အခြေအနေ နှစ်ရပ်ကို ဖော်ပြပါ။
* Recuva တွင် 'Deep Scan' ကို enable လုပ်ရန် နည်းလမ်း နှစ်မျိုးရှိသည်။ ၎င်းတို့ကို ဖော်ပြပါ။
* ဖျက်ပြီးဖိုင်တွေကို ရှာဖွေစစ်ဆေးရာမှာ ဘယ်လို အခြေအနေမျိုးဆိုရင် Recuva Wizard ကို သင် အသုံးပြုသင့်သလဲ။

CCleaner တိကျသော ဖိုင်ဖျက်သိမ်းမှုနှင့် အလုပ်လုပ်သည်ကဏ္ဍ၌ သုတ်သင်ရှင်းလင်းခြင်း အပိုင်း

CClearner သည် သင်၏ ပုဂ္ဂိုလ်ရေးနှင့် လုံခြုံရေးဆိုင်ရာ ကာကွယ်ရေး အတွက် မရှိမဖြစ်လိုအပ်သော လွယ်ကူအကျိုးရှိသည့် အသုံးချ ပရိုဂရမ်တစ်ခု ဖြစ်သည်။ သင် အလုပ်လုပ်ရာတွင် သင်၏ ကွန်ရက်ရှာဖွေစက် (browser) မှ ဖန်တီးထားသည့် web site တစ်ခုကို ကြည့်ရှုရာမှ ကျန်ရှိသော အစိတ်အပိုင်းများဖြစ်သည့် history၊ cookies နှင့် temporary files များကို အမြဲတစေ ဖျက်သိမ်းပေးပြီး disk ပေါ်တွင် နေရာလွတ်များ ရရှိစေသည်။ ထို့ပြင် အခြား ရန်လိုသော ပြိုင်ဘက်အဖွဲ့အစည်းများမှ သင်၏ လုပ်ကိုင်ပုံ အလေ့အထများကို ချောင်းမြောင်းကြည့်ရှု၍ သင်၏ system ကို ဝင်ရောက်ဖျက်ဆီးခြင်းကိုလည်း ကန့်သတ်ချက်များ ပြုလုပ်ထားသည်။

CCleaner အား Install ပြုလုပ်ခြင်းတွင် အောက်ပါ အကြောင်းအရာများကို သိရှိရန် လိုအပ်သည်။

* လမ်းညွှန်ချက် အသေးစိတ်ကို ဖတ်ပါ။
* www. piriform.com/ccleaner/builds စာမျက်နှာကို သွားရန် CCleaner icon ကို click လုပ်ပြီး ဖွင့်ပါ။
* 'CCleaner- Slim' တွင် 'Download' ကို နှိပ်ပါ။ ပရိုဂရမ်ကို install လုပ်ရန် download file ကိုရှာပြီး double click လုပ်ပါ။
* Install ဆက်မလုပ်ခင် လမ်းညွှန်ချက်များကို နောက်တစ်ပိုင်းတွင် ဖတ်ပါ။

* CCleaner ကို အောင်မြင်စွာ install ပြုလုပ်ပြီးစီးပြီဆိုပါက installation ပရိုဂရမ်ကို သင်၏ ကွန်ပျူတာမှ ဖျက်ပစ်လိုက်ပါ။
* CCleaner ၏ မူလစာမျက်နှာ (Home page) မှာ www. ccleaner.com ဖြစ်သည်။
* ကွန်ပျူတာ လိုအပ်ချက်များမှာ Windows versions အားလုံးကို အထောက် အကူပြုသည်။
* ဤလမ်းညွှန်တွင် အသုံးပြုသော window version မှာ 2.33 ဖြစ်သည်။
* License ခွင့်ပြုချက်မှာ အခမဲ့ပင် ဖြစ်သည်။
* ဖတ်ထားသင့်သည့် အကြောင်းအရာမှာ အခန်း 6 'ထိခိုက်ပျက်စီးလွယ်သော သတင်း အချက်အလက်များ ဖျက်ဆီးပုံ' အကြောင်း ဖြစ်သည်။
* စတင် အသုံးပြုရန် လိုအပ်သော အချိန်မှာ 15 မိနစ် ဖြစ်ပါသည်။
* သင် ပြန်လည်ရရှိမည့် အကျိုးတရားများမှာ
* သင်၏ ကွန်ပျူတာနှင့် ဆက်သွယ်မှုရှိသော disks များတွင် နေရာလွတ်များ ရရှိအောင် ရှင်းလင်းနိုင်ခြင်း
* Windows Registry ကို ရှင်းလင်းနိုင်ခြင်း
* သင်၏ ကွန်ပျူတာကို စတင်ချိန်တွင် အလုပ်လုပ်နေသော ပရိုဂရမ်များကို ထိန်းချုပ်နိုင်စွမ်းရှိခြင်းတို့ ဖြစ်ကြပါသည်။

GNU Linux ၊ Mac OS နှင့် အခြား Microsoft Windows တို့နှင့် တွဲဖက် ဆောင်ရွက်နိုင်သော ပရိုဂရမ်များ

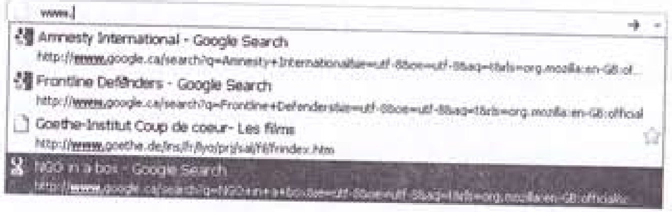
GNU Linux ၊ Microsoft Windows တို့နှင့် တွဲဖက်ဆောင်ရွက်နိုင်သော ကောင်းမွန်သည့် ဖိုင် ဖယ်ရှားခြင်း tool တစ်ခုမှာ 'BleachBit' ဖြစ်သည်။ 'BleachBit' သည် လူသိများထင်ရှားသော applications ပေါင်း 70 ရှိသည့်အနက်မှ OS ၏ temporary files များကို ရှင်းလင်းပေးပြီး hard disk ကို နေရာလွတ်များ ရှင်းလင်းပေးသည်။ လွတ်လပ်သော ရင်းမြစ်ဖြစ်ပြီး လွယ်ကူစွာ အသုံးချနိုင်သည့် 'BleachBit' ပရိုဂရမ်ကို ဘာသာစကားပေါင်း 32 မျိုးဖြင့် အသုံးပြုနိုင်သည်။ သင်၏ system ရှင်းလင်းရေးအတွက် Ubuntu Linux users များအနေဖြင့် မလိုအပ်သော ဖိုင်အပျက် အစီးများကို ရှင်းလင်းခြင်း လမ်းညွှန်ကို ကြည့်ရှုသင့်သည်။

Mac OS users များအတွက် Titanium's Software မှ 'OnyX and Maintenance' က သင့်အလုပ်ကဏ္ဍမှ ဖြစ်ပေါ်လာသော သဲလွန်စများကို ဖျက်ပစ်ရန် အကူအညီပေးသော အခမဲ့ tools များ ဖြစ်ကြသည်။ သင်၏ အမှိုက်များ (Trash) ကို လုံခြုံစွာ ရှင်းပစ်ရန် 'Finder' application သို့သွား၍ menu တွင် Finder>Secure Empty Trash ဟူ၍ ရွေးချယ်ပါ။ သင်၏ အမှိုက်များ (Trash) များကို ရှင်းလင်းရန် Finder ၏ ရွေးချယ်မှုဖြစ်သော Advance tab ကိုလည်း အသုံးချနိုင်သည်။ 'Empty Trash' ကို check လုပ်ထားနိုင်သည်။ Disk ပေါ်တွင် နေရာလွတ်များ ပြုလုပ်ရန် system application တစ်ခုဖြစ်သော 'Disk Utility' ကိုသွားပါ။ 'disk partation' ကို ရွေးပါ။ ၎င်းမှ 'Erase' tab ကို ရွေးပါ။ 'Erase Free Space' ခလုတ်ကို နှိပ်ပါ။

1.1 ဤပရိုဂရမ်ကို စတင်အသုံးမပြုခင် သိသင့်သောအချက်များ

သင့်ကွန်ပျူတာ system ပေါ်မှာရှိတဲ့ ပေးထားတဲ့ settings တွေနဲ့ အင်တာနက် browser ကနေ စုစည်းတည်ဆောက်ထားတဲ့ အချက်အလက်တွေကို ကျွမ်းကျင်တဲ့ ပြိုင်ဘက်အဖွဲ့အစည်းများက ခြေရာကောက်နိုင်ပါတယ်။ (မုဆိုးနဲ့ သားကောင်လို့တော့လဲ မဟုတ်ဘူးပေါ့) ပရိုဂရမ်တစ်ခု (သို့) word processor (သို့) အင်တာနက် browser တစ်ခုကို သင်သုံးစွဲသည့်အခါတိုင်း ယာယီ data တွေနဲ့ ဖိုင်တွေဟာ သင့် ကွန်ပျူတာ system ပေါ်မှာ ထွက်ပေါ်လာပြီး သိမ်းဆည်းထားတတ်ပါတယ်။

မကြာသေးမီကမှကြည့်ထားတဲ့ မှတ်တမ်းတွေနဲ့ web စာမျက်နှာတွေ အကြောင်းကိုလည်း သင့် system မှာ တွေ့နိုင်ပါတယ်။ ဥပမာအားဖြင့် အင်တာနက် browser တစ်ခုမှာ web site လိပ်စာတစ်ခုကို ရိုက်ထည့်သည့်အခါ သင်ရိုက်လိုက်တဲ့ လိပ်စာရဲ့ အစအက္ခရာစာလုံး ပါဝင်ပတ်သက်တဲ့ (သို့) ၎င်းနှင့် ဆက်နွယ်နေတဲ့ web site လိပ်စာများ ပေါ်ထွက်လာမှာ ဖြစ်ပါတယ်။



ပုံ 1: URL အမျိုးမျိုးကိုဖော်ပြနေသော အင်တာနက် browser ၏ လိပ်စာ barပုံ

Browser ၏ history များဟာ အဆင်ပြေကောင်းပြေနိုင်ပေမဲ့ သင် သွားရောက်ခဲ့တဲ့ web sites လိပ်စာများကိုတော့ တစ်စုံတစ်ယောက်က ရှာဖွေတွေ့ရှိအောင် ခွင့်ပြုသလို ဖြစ်နေပါတယ်။ ထို့အပြင် အင်တာနက်ရဲ့ ပုံစံနဲ့ ရိုက်ထားတဲ့ သတင်းအချက်အလက်တွေ၊ အီးမေးလ် messages တွေအပါအဝင် web sites တွေကနေ ရယူထားတဲ့ ရုပ်ပုံတွေပါဝင်တဲ့ data တွေဟာ သင့်ရဲ့ လောလောဆယ် လုပ်ဆောင်မှုတွေကို အထင်းသား ဖြစ်စေပါတယ်။

ပရိုဂရမ်တစ်ခုကို သင်အသုံးပြုတဲ့ အကြိမ်တိုင်းမှာ ယာယီရောက်ရှိလာတဲ့ data တွေကို ဖယ်ရှားဖို့ပရိုဂရမ်တစ်ခုစီတိုင်းရဲ့ directory ကိုဖွင့်ပြီး အဲဒီမှာရှိတဲ့ ယာယီပရိုဂရမ်တွေကို ခွဲခြားဖျက်သိမ်းရမှာ ဖြစ်ပါတယ်။ CCleaner က ပရိုဂရမ်တွေရဲ့ စာရင်းတစ်ခုကို ပြသထားပြီး ဖျက်ပစ်သင့်တဲ့ ယာယီဖိုင်တွေအားလုံးကို ၎င်းပရိုဂရမ်များမှ ရွေးချယ်ပေးပါတယ်။

အရေးကြီး ။ ။ CCleaner က သင့် ကွန်ပျူတာပေါ်မှာ သိမ်းထားတဲ့မှတ်တမ်းအစစ်အမှန်တွေကို ဖျက်ပစ်တာမဟုတ်ဘဲ ယာယီဖိုင်များကိုသာ ဖျက်ခြင်းဖြစ်သော်လည်း သင့်ရဲ့ မှတ်တမ်းတွေကို အချိန်နှင့်အမျှတစ်ပြေးညီ အဆင့်မီအောင် back up ပြုလုပ်ထားသင့်ပါတယ်။ ဒါတွေကို လေ့လာဖို့အခန်း 5 မှာရှိတဲ့ 'ဆုံးရှုံးသွားတဲ့ သတင်းအချက်အလက်များ ပြန်လည်ရယူပုံ' နဲ့ 'မူပွားတစ်ခုကို ပြုလုပ်ပုံ' ခေါင်းစဉ်များမှာ ကြည့်ရှုနိုင်ပါတယ်။

CCleaner ကို အသုံးပြုလိုက်တဲ့အခါ သင့်ရဲ့ browser နဲ့ လောလောဆယ် အသုံးပြုထားတဲ့ မှတ်တမ်းမှတ်ရာတွေရဲ့ နောက်ကြောင်းတွေ၊ save လုပ်ထားတဲ့ pass words တွေကို ဆုံးရှုံးနိုင်ပါတယ်။ ဒါပေမဲ့ ဒီပရိုဂရမ်ရဲ့ အဓိကအချက်က သင့်ရဲ့ ကွန်ပျူတာ system ကို ချောင်းမြောင်းကြည့်ရှုခြင်းနဲ့ အဖျက်အဆီး ဝင်ရောက် ခြင်းတို့ ပျောက်ကွယ်သွားဖို့ပဲ ဖြစ်ပါတယ်။

* CCleaner ကို Install ပြုလုပ်ပုံနှင့် လုပ်ဆောင်ပုံ
* CCleaner ၌ ယာယီဖိုင်များကို ဖျက်သိမ်းပုံ
* CCleaner ၌ Windows Registry ကို ရှင်းလင်းပုံ
* အဆင့်မြင့် Options များ၊ မကြာခဏမေးလေ့ရှိသော မေးခွန်းများနှင့် သုံးသပ်ချက်

CCleaner ကို Install ပြုလုပ်ပုံနှင့် ပြင်ဆင်ပုံ

ဤစာမျက်နှာရှိ အပိုင်းကဏ္ဍများမှာ

* 2.0 CCleaner ကို Install ပြုလုပ်ပုံ
*2.1 CCleaner ကို လုပ်ဆောင်မှု မပြုလုပ်ခင် သိသင့်သည်များ
* 2.2 Malware နှင့် Viruses များ ရှာဖွေစစ်ဆေးပုံတို့ ဖြစ်ကြသည်။

2.0 CCleaner ကို Install ပြုလုပ်ပုံ

CCleaner ကို Install ပြုလုပ်ခြင်းသည် လွယ်ကူလျှင်မြန်သော လုပ်ငန်းစဉ်တစ်ရပ်ဖြစ်သည်။ CCleaner ကို install စတင်ပြုလုပ်ရန် အောက်ပါအဆင့်များကို ဆောင်ရွက်ပါ။

အဆင့် 1: Installation လုပ်ငန်းစဉ်စတင်ရန် double click နှိပ်ပါ။ ဖိုင်ကို ဖွင့်ပါ။ လုံခြုံရေးအချက်ပေး dialog box ပေါ်လာလိမ့်မည်။ အောက်ပါ screen ကို click လုပ်ပြီးသွားပါ။

ပုံ 1: Installer ၏ ဘာသာစကား ရွေးချယ်မှုပြု dialog box ပုံ

အဆင့် 2: 'Welcome to the CCleaner v 2.33 Setup Wizard' screen ကို click လုပ်ပြီး သွားပါ။

အဆင့် 3: ထို့နောက် အသုံးပြုသူ၏ သဘောတူညီချက်ရယူသော 'CCleaner License Agreement' screen သို့ သွားပါ။ Installation လုပ်ငန်းစဉ်ကို ဆက်လက်မလုပ်ဆောင်ခင် သဘောတူညီချက်ပါ အကြောင်းအရာကို ဖတ်ပါ။

အဆင့် 4: တည်နေရာ ရွေးရန် 'Choose Install Location' screen သို့ click

လုပ်ပြီးသွားပါ။

အဆင့် 5: 'Install Options' screen သို့ click လုပ်ပါ။

မှတ်ချက် ။ ။ 'Install Option ' screen သည် 'Add CCleaner Yahoo! toolbar' နှင့် တွဲလျက်ပေါ်လာပြီး 'use CCleaner from your browser' option ကို enable လုပ်ပါ။ Yahoo! toolbar ကို install မလုပ်ပါနှင့်။ ၎င်းက သင်၏ အင်တာနက် လုံခြုံရေးကို ညှိနှိုင်းပေးသည်။

အဆင့် 6: 'Add CCleaner Yahoo! toolbar' ကို နှိပ်ပါ။ ပုံ 2 မှာ ပြထားသည့်အတိုင်း 'use CCleaner from your browser' option ကို disable လုပ်ပါ။

ပုံ 2: Yahoo! toolbar ကို disable လုပ်ထားသော 'Install Options' ၏ ပုံ

အဆင့် 7: Install လုပ်ပါ။ လုပ်ငန်းစဉ် အခြေအနေပြ bar ကို ပြသထားသော screen ကို တွေ့ရမည်။

အဆင့် 8: CCleaner ကို install လုပ်ခြင်း ပြီးစီးအောင် click လုပ်ပါ။ Piriform CCleaner ၏ ပင်မမျက်နှာစာ (user interface) ကို သွားပါ။

ပုံ 3: Piriform CCleaner ၏ ပင်မ မျက်နှာစာပုံ

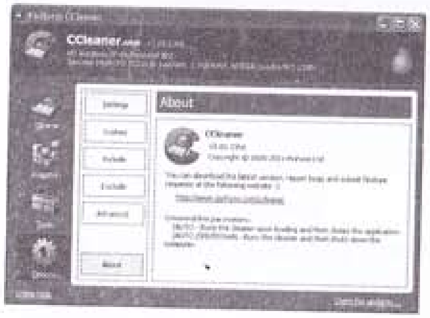
2.1 CCleaner ကို လုပ်ဆောင်ခြင်း မပြုမီ သိသင့်သည်များ

အခန်း 6 ရှိ 'ထိခိုက်ပျက်စီးလွယ်သော သတင်းအချက်အလက်များကို ဖျက်ဆီးပုံ' ခေါင်းစဉ်တွင် အသေးစိတ် ဖော်ပြထားသကဲ့သို့ပင် Microsoft Windows ၏ ဖိုင်များကို ဖျက်သိမ်းခြင်းနည်းလမ်းများမှာ recycle bin ကို သင် ဗလာခါသည့် အချိန်၌ပင် မူလ data အစစ်အမှန်ကို disk ပေါ်မှ မဖျက်နိုင်ပါ။ ယာယီဖိုင်များတွင်လည်း ထို့အတူပင် ဖြစ်သည်။ ၎င်းတို့ကို hard disk ပေါ်မှ အသေအချာ ဖျက်ဆီးရန်မှာ ဖိုင်များကို အဆင်ပြေသလို ရရှိထားသော data များဖြင့် overwrite ပြုလုပ်ရမည်။ CCleaner ကို default mode ဖြင့် မလုပ်ဆောင်သောကြောင့် ၎င်းဖျက်သည့် ဖိုင်များကို overwrite ပြုလုပ်ရန် ပြင်ဆင်ထားသည်။ ထို့ကြောင့် ၎င်းက ဖိုင်များကို အသေအချာ ဖျက်ပစ်သည်။ CCleaner က disk ပေါ်တွင် နေရာလွတ်များ ရှင်းလင်းပေးခြင်းဖြင့်လည်း အချက်အလက်ဟောင်းများကို ဖျက်ပေးသည်။ အပိုင်း 5.3 ရှိ 'CCleaner ကို အသုံးပြု၍ disk နေရာအလွတ်များ ရှင်းလင်းပုံ' တွင် ကြည့်ပါ။

CCleaner ကို အသုံးမပြုခင် ယာယီဖိုင်အားလုံးကို လုံခြုံစွာ ဖျက်ပစ်ရန် ပြင်ဆင်သင့်သည်။

အဆင့် 1: Piriform CCleaner ၏ ပင်မမျက်နှာစာ (main user interface) ကို သွားရန် Start>Programs> CCleaner ကို ရွေးချယ်ပါ (သို့) click လုပ်ပါ။

အဆင့် 2: အောက်ပါပုံသို့ သွားရန် click လုပ်ပါ။



ပုံ 4: Default About pane ပုံ

အဆင့် 3: 'Settings' pane သို့ click လုပ်ပြီးသွားပါ။ ၎င်းက သင်နှင့်အဆင်အပြေဆုံး ဖြစ်စေမည့်ဘာသာစကားကို ရွေးချယ်ခွင့်ပေးပြီး CCleaner ကို အသုံးပြု၍

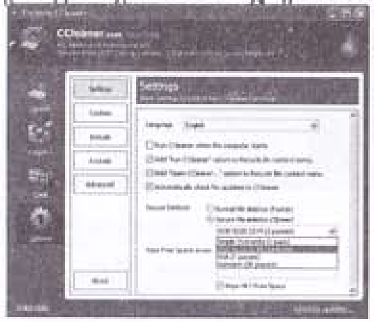
ယာယီဖိုင်နှင့် drives များကို မည်သို့ ရှင်းလင်းဖျက်ဆီးမည်ကို ဆုံးဖြတ် နိုင်သည်။

မှတ်ချက် ။ ။ 'Normal file deletion' option ကို enable လုပ်ထားသော တိကျသေချာသောဖိုင် ဖျက်သိမ်းခြင်း အပိုင်းကဏ္ဍ ပေါ်လာလိမ့်မည်။

အဆင့် 4: 'Secure file deletion (Slower)' option ကို နှိပ်ပါ။

အဆင့် 5: Drop-down list ကို ချဲ့ယူပြီး DOD 5220.22 M ကို 'Secure file deletion (Slower)' option မှ ရွေးပါ။ အောက်ပါ screen ပေါ်လာလိမ့်မည်။

ဤ option ကို သင် ရွေးချယ်ပြီးပါက ဖျက်ရန်အတွက် သင် ရွေးချယ်ထား



ပုံ 5: 'Secure Deletion' options များပြထားသော 'Settings' pane

သော ဖိုင်နှင့် folder များကို CCleaner အလှည့်သင့်ရာ အချက်အလက် (random data) များဖြင့် overwrite လုပ်၍ သင်၏ hard disk ပေါ်မှ အကျိုးရှိစွာ ရှင်းလင်းပေးလိမ့်မည်။ Secure deletion ၏ drop-down list ရှိ 'pass' များမှာ သင်၏ data ကို random data ဖြင့် overwrite လုပ်မည့် အကြိမ် အရေအတွက် ဖြစ်သည်။ 'Pass' အရေအတွက် များလေလေ၊ သင်၏ မှတ်တမ်း၊ ဖိုင်နှင့် folder ကို random data ဖြင့် overwrite လုပ်မည့် အကြိမ်အရေအတွက် များလာလေပင် ဖြစ်သည်။ ၎င်းက မှတ်တမ်း၊ ဖိုင်နှင့် folder တို့ကို ပြန်လည်ရယူနိုင်စွမ်း လျော့နည်း စေပြီး ရှင်းလင်းခြင်း (wiping) လုပ်ငန်းစဉ်ကို အချိန်ပိုကြာစေသည်။

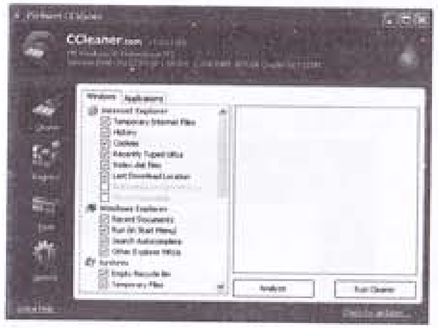
CCleaner ၌ ယာယီဖိုင်များကို ဖျက်သိမ်းပုံ

ဤအပိုင်းတွင် သင်၏ ကွန်ပျူတာပေါ်တွင် အများဆုံးအသုံးပြုသော ap

plications များနှင့် Microsoft Windows တို့မှ ပြုလုပ်ထားသော ယာယီဖိုင်များ အားလုံးကို ဖျက်သိမ်းပုံကို လေ့လာကြရမည်။

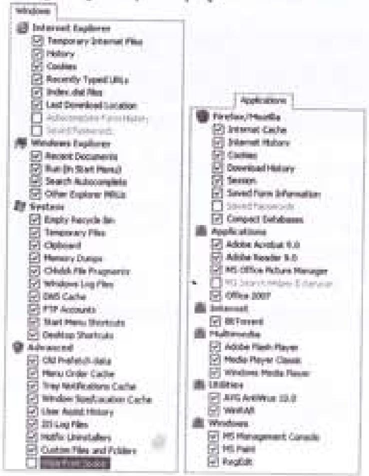
အဆင့် 1: Start>Programs>CCleaner ကို ရွေးချယ်ပါ (သို့) click လုပ်ပြီး CCleaner ၏ ပင်မမျက်နှာစာသို့ သွားပါ။

အဆင့် 2: အောက်ပါ screen ကို သွားရန် click လုပ်ပါ။



ပုံ : CCleaner Pane ကို ဖော်ပြထားသော CCleaner ပင်မမျက်နှာစာ

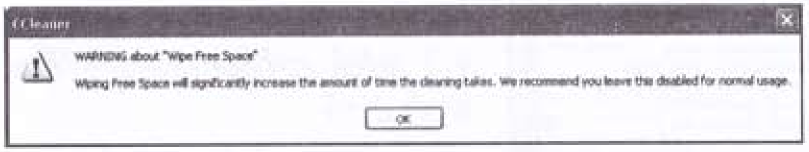
CCleaner window ကို နှစ်ခြမ်းခွဲနိုင်သည်။ ဘယ်ဘက်ခြမ်းတွင် Windows နှင့် Applications တို့၏ tabs များကို ဖော်ပြထားပြီး ညာဘက်ခြမ်းတွင် ရှင်းလင်းခြင်းလုပ်ငန်းစဉ်မှ ရရှိသောရလဒ်နှင့် သတင်းအချက်အလက်များကို ဖော်ပြရန် နေရာလွတ်ရှိသည်။ စစ်ဆေးခြင်း (Analyze) နှင့် လုပ်ဆောင်ခြင်း (Run) Cleaner ခလုတ်မှာ ၎င်းနေရာ၏ အောက်ဘက်တွင် ရှိသည်။



ပုံ 2: Options အားလုံးကို checked လုပ်ထားသော Windows နှင့် Applications tabs များပုံ

မှတ်ချက် ။ ။ ဖော်ပြပါအဆင့်များကို ပြုလုပ်ခြင်းဖြင့် Windows နှင့် Applications tabs များတွင် သင် checked လုပ်ခဲ့သောအရာများ (item) အတွက် ယာယီဖိုင် အားလုံးကို ဖျက်ပစ်လိမ့်မည်။ အသုံးပြုသူ အသီးသီးတို့သည် ၎င်းတို့၏ ကွန်ပျူတာပေါ်တွင် ပရိုဂရမ်အမျိုးမျိုးတို့ကို install ပြုလုပ်ကြသည်ဖြစ်ရာ သင်၏ Applications စာရင်းကို ပုံ : 2 မှာကဲ့သို့ အနည်းငယ် ပြောင်းလဲစေလိမ့်မည်။

အဆင့် 3: Windows နှင့် Applications tabs ကို ဆွဲချပြီး အဆင့်မြင့် အပိုင်း (Advanced Section) တွင် ပါဝင်သော options အားလုံးကို check လုပ်ပါ။ အချို့ option များကို check လုပ်ရာတွင် သတိပေးချက် dialog box ပေါ်လာပြီး ၎င်း option တို့၏ အကျိုးသက်ရောက်မှုကို ရှင်းပြပေးလိမ့်မည်။

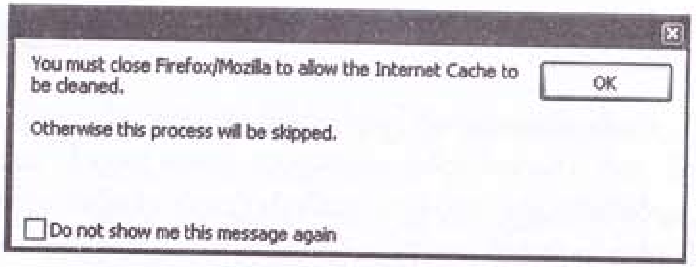


ပုံ 3: သတိပေးချက် dialog box ပုံစံပြဥပမာတစ်ခု

မှတ်ချက် ။ ။ ယာယီဖိုင်များ အားလုံးကို နှံ့နှံ့စပ်စပ် ပြည့်ပြည့်စုံစုံ ရှင်းလင်းနိုင်ရန် Windows နှင့် Applications tabs ရှိ options အားလုံးကို check လုပ်ပါ။ သို့သော် သင်ဖျက်သိမ်းသည့် တည်ဆောက်ခြင်း (Configurations) နှင့် သတ်မှတ်ခြင်း (Settings) များကို သိရှိနားလည်ရန် လိုအပ်သည်။

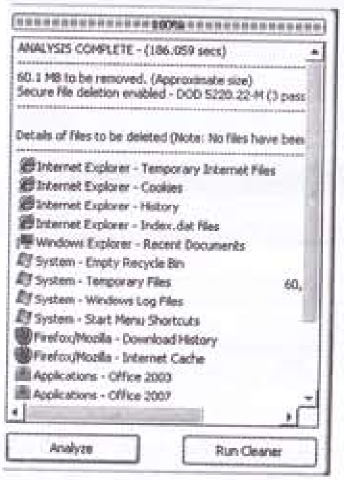
အဆင့် 4: ဖျက်သိမ်းရန် ရရှိနိုင်သော ယာယီဖိုင်များစာရင်းကို ထုတ်ယူကြည့်ရှုရန် click လုပ်ပါ။

သတိပြုရန် ။ ။ ရှင်းလင်းမည့် လုပ်ငန်းစဉ်မစမီ အခြားပရိုဂရမ်အားလုံးကို ပိတ်ထားပါ။ အကယ်၍ ဖွင့်ထားမိပါက ၎င်းပရိုဂရမ်များနှင့် သက်ဆိုင်သော ယာယီဖိုင်များကို ဖယ်ရှားမည်မဟုတ်ဘဲ ပုံ : 4 တွင် ဖော်ပြထားသည့် သတိပေးချက် pop-up တစ်ခု ပေါ်လာလိမ့်မည်။



ပုံ 4: Firefox (သို့) Mozilla ကို ပိတ်ရန် သတိပေးသည့် ဥပမာတစ်ခုပုံ

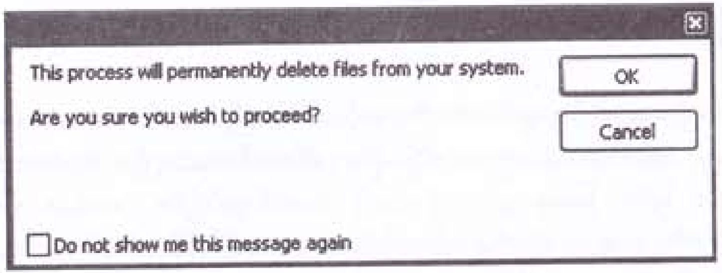
အဆင့် 5: ဖျက်ရန်အတွက် ဖိုင်များကို စာရင်းပြုပါ။



ပုံ 5: ဖျက်ရန် စာရင်းပြုထားသော ယာယီဖိုင်များကို ပြသည့် ဥပမာပုံ

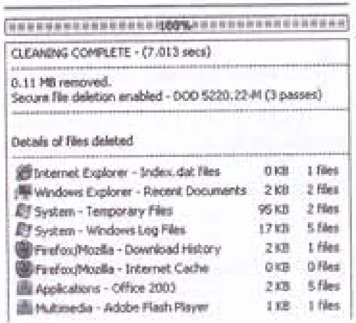
မှတ်ချက် ။ ။ CCleaner က သင်အသုံးပြုသော application မှ ထုတ်လုပ် ထားသော ယာယီဖိုင်များကိုသာ ဖျက်ပေးသည်။ ၎င်း Application တစ်ခုလုံးကိုတော့ ဖျက်မပေးနိုင်ပါ။ ဥပမာတစ်ခုအနေဖြင့် ပုံ 5: တွင် ကြည့်ပါ။ Office 2003 ပရိုဂရမ်သည် ၎င်း ၏ ယာယီဖိုင်များအားလုံးကို ဖျက်ဆီးပြီးသော်လည်း မူလ install လုပ်ထားသော ပရိုဂရမ်သည် ကွန်ပျူတာပေါ်မှာ ကျန်ရှိနေသည်။ CCleaner ကို အသုံးပြုပြီး ပရိုဂရမ် တစ်ခုကို uninstall လုပ်မည်ဆိုပါက အဆင့်မြင့် (Advanced) Options များ။ မကြာခဏ မေးလေ့ရှိသော မေးခွန်းများနှင့် သုံးသပ်ချက်မှ အခန်း 5.1 'CCleaner ကို အသုံးပြုပြီး ပရိုဂရမ်များ uninstall ပြုလုပ်ပုံ' ၌ ကြည့်ပါ။

အဆင့် 6: ယာယီဖိုင်များကို ဖျက်သိမ်းရန် click လုပ်ပြီး အောက်ပါ screen သို့ သွားပါ။



ပုံ 6: အတည်ပြုချက်ယူသည့် dialog box ပုံ

အဆင့် 7: အောက်ပါအတိုင်း ယာယီဖိုင်များကို ဖျက်ရန် click လုပ်ပါ။ ဖျက်သိမ်းခြင်း ပြီးစီးပါက အောက်ရှိပုံတွင် ဖော်ပြထားသည့်အတိုင်း ရလဒ်များ ဖော်ပြထားသည်။



ပုံ 7: ဖိုင်ဖျက်သိမ်းခြင်း ရလဒ်များ

ယခုသင်သည် CCleaner ကို အသုံးပြု၍ Applications tabs များမှ ယာယီဖိုင်များကို အောင်မြင်စွာ ဖျက်သိမ်းပြီးစီးပါပြီ။

CCleaner ၌ Windows Registry ကို ရှင်းလင်းပုံ

ဤစာမျက်နှာရှိ အပိုင်းကဏ္ဍများမှာ

* 4.0 သင် စတင်အသုံးမပြုခင် သိသင့်သည်များ
* 4.1 CCleaner ကို အသုံးပြု၍ သင်၏ Windows Registry ကို ရှင်းလင်းပုံ
* 4.2 သင်၏ Registry မူပွားဖိုင်ကို ပြန်လည်ရယူပုံ

4.0 သင် စတင် အသုံးမပြုခင် သိသင့်သည်များ

CCleaner က သင်၏ ကွန်ပျူတာပေါ်ရှိ hardware နှင့် software settings

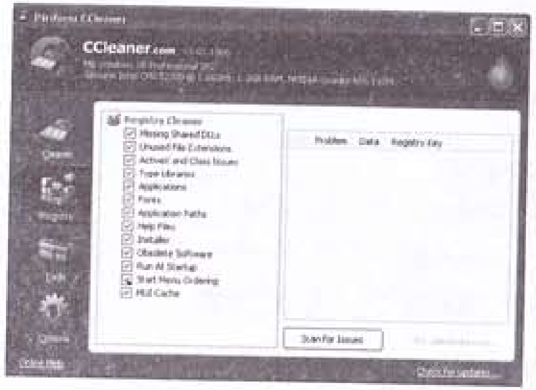
များနှင့် တည်ဆောက်ပုံအချက်အလက်များကို သိမ်းဆည်းထားသော database တစ်ခုဖြစ်သည့် Windows Registry ကိုလည်း ရှင်းလင်းပေးသည်။ Software များ ထည့်သွင်း ခြင်း၊ ပြုနေကျတာဝန်များကို ဆောင်ရွက်ခြင်း၊ အခြေခံ system တည်ဆောက်ပုံ အချက်အလက်များကို ပြောင်းလဲသည့်အချိန်တိုင်း ၎င်းပြောင်းလဲမှုများကို Windows Registry က သိမ်းထားပေးသည်။

ထို့ကြောင့် အချိန်ကြာသောအခါ ခေတ်မမီတော့သော ပရိုဂရမ်များ၏ သဲလွန်စများ အပါအဝင် outdated ဖြစ်နေသည့် တည်ဆောက်ပုံ အချက်အလက်နှင့် အသုံးချနည်းစနစ်များသည် Windows Registry တွင် စုဆောင်းမိလာသည်။ CCleaner Registry option က ထိုသို့ အချက်အလက်များကို ရှာဖွေစစ်ဆေးပြီး ဖယ်ရှားခြင်းဖြင့် သင့် system ၏ ဆောင်ရွက်ချက်များနှင့် အမြန်နှုန်းကို တိုးတက်စေသည်။ သင်၏ ပုဂ္ဂိုလ်ရေးရာများနှင့် လုံခြုံရေးအတွက်လည်း ကာကွယ်ပေးသည်။

သတိပြုရန် ။ ။ Windows Registry ကို scan ဖတ်ခြင်းအား လစဉ် ပုံမှန်ပြုလုပ်သင့်သည်။

4.1 CCleaner ကို အသုံးပြုပြီး သင်၏ Windows Registry ကို ရှင်းလင်းပုံ

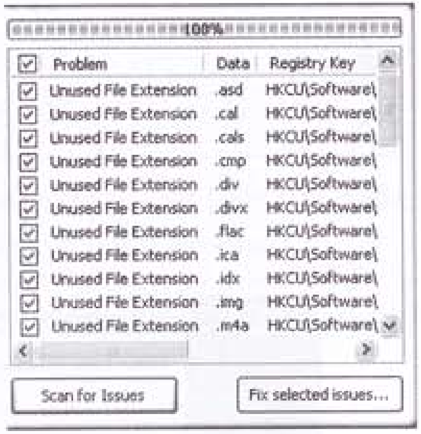
အဆင့် 1: အောက်ပါ screen သို့ သွားရန် click လုပ်ပါ။



ပုံ 1: Registry mode ၌ တွေ့ရသော CCleaner ၏ ပင်မမျက်နှာစာ

CCleaner ၏ Registry window ကို ပေါင်းစည်း Registry စာရင်းနှင့် ပြဿနာရှာဖွေပြီးသောအချက်အလက်များကို ပြထားသည့်စာမျက်နှာတစ်ခုဟူ၍ ပိုင်းခြားထားသည်။

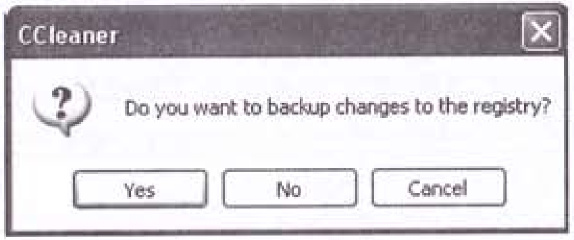
အဆင့် 2: ပေါင်းစည်း Registry စာရင်းရှိ item အားလုံးကို check လုပ်ပြီး registry နှင့် ပတ်သက်သော ပြဿနာများကို ရှာဖွေပြင်ဆင်ရန် click လုပ်ပါ။ အချိန်ခဏအကြာတွင် သင်၏ ရလဒ်များကို အောက်ပါအတိုင်း တွေ့ရ မည်။



ပုံ 2: ပြင်ဆင်ရန် လိုအပ်သော ပြဿနာအချို့ကို ပြထားသောရလဒ် စာမျက်နှာပုံ

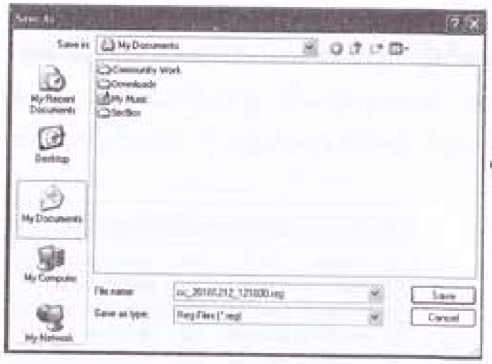
Windows Registry ကို ပြင်ဆင်ခြင်းမပြုမီ ကြိုတင်ကာကွယ်မှုအနေဖြင့် သင်၏ registry ကို back up ပြုလုပ်ထားရန် သတိပေးချက် ပေါ်လာလိမ့်မည်။ Windows Registry ကို ရှင်းလင်းပြီးနောက် တစ်စုံတစ်ရာ ပြဿနာတွေ့ရှိပါက ၎င်း back up ဖိုင်ကို အသုံးပြု၍ Windows Registry ၏ မူလအခြေအနေကို ပြန်ထားနိုင်ပါသည်။

အဆင့် 3: အောက်ပါအတည်ပြုချက်ယူမည့် dialog box ကို click လုပ်ပြီး သွားပါ။



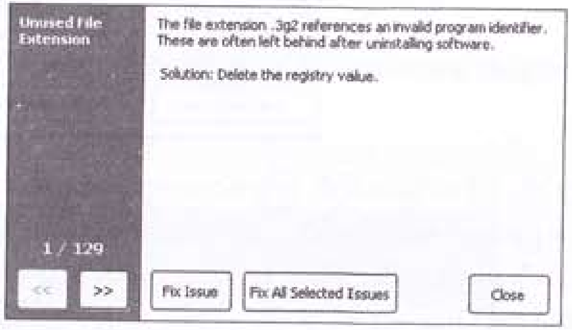
ပုံ 3: အတည်ပြုချက်မေးသည့် dialog box ပုံ

မှတ်ချက် ။ ။ သင်၏ back up registry ဖိုင်ကို မည်သည့်နေရာ၌ သိမ်းဆည်းမိသည်ကို မေ့သွားပါက .reg ဖိုင် extension ကို search လုပ်ပါ။



ပုံ 4: တည်နေရာ ရွေးချယ်သော Save As location browser ပုံ

အဆင့် 5: သင်၏ back up ဖိုင်အတွက် တည်နေရာရွေးချယ်ပြီးပါက click လုပ်ပါ။ အောက်ပါ dialog box ကို တွေ့ရမည်။



ပုံ 5: Fix Issue/Fix All Selected Issues dialog box ပုံ

ကျွမ်းကျင်သော အဆင့်မြင့် အသုံးပြုသူများသည် ၎င်းတို့၏ လိုအပ်ချက်ပေါ်မူတည်၍ ဖိုင်အားလုံးကို မပြင်ဆင်ဘဲ အချို့ကိုသာ ပြင်ဆင်နိုင်သည့် စွမ်းရည်ကို သဘောကျကြသည်။ သာမန်နှင့်စတင်အသုံးပြုသူများမှာမူ ရွေးချယ်ထားသော issues များအားလုံးကို ပြင်ဆင်ရန် လမ်းညွှန်ပါသည်။

အဆင့် 6: ပြဿနာတစ်ရပ်စီကို ကြည့်ရှုရန် click လုပ်ပါ။ ထို့နောက် သင် ပြင်ဆင်လိုသော ပြဿနာကို ရွေးချယ်ရန် click လုပ်ပါ။

အဆင့် 7: ရွေးချယ်ထားသော အကြောင်းအရာများ (issues) အားလုံးကို ပြင်ရန် click လုပ်ပါ။

Windows Registry ကို အောင်မြင်စွာ ရှင်းလင်းပြီးပါပြီ။

သတိပြုရန် ။ ။ ဖြေရှင်းရန် ပြဿနာ တစ်စုံတစ်ရာမရှိသည့် အချိန်အထိ အဆင့် 3 မှ 6 အထိ ထပ်ပြန်တလဲလဲ လုပ်ဆောင်ပါ။

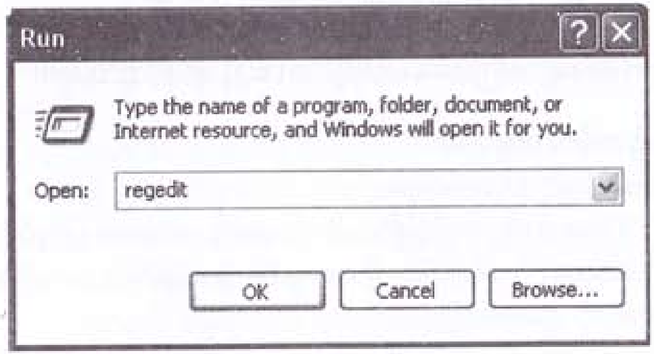
4.2 သင်၏ Registry မူပွားဖိုင်ကို ပြန်လည်ရယူပုံ

Windows Registry ကို ရှင်းလင်းခြင်းက သင် system ၏ ဆောင်ရွက်မှုကို အနှောင့်အယှက်ဖြစ်စေသည်ဟု သင်သံသယ ရှိပါက အခန်း 4.1 တွင် အဆင့် 3 မှ 5 အထိ သင် ပြုလုပ်ခဲ့သော Registry မူပွားဖိုင်ကို အသုံးပြု၍ မူရင်း registry ကို သိမ်းဆည်းထားနိုင်ပြီး သင်၏ system ကို ဝင်ရောက်နှောင့်ယှက်ခြင်းများမှ လျော့ချပေးသည်။

မူရင်း Registry ကို သိမ်းထားရန် အောက်ပါအဆင့်များ ဆောင်ရွက်ပါ။

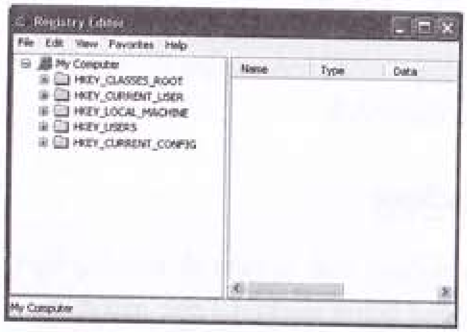
အဆင့် 1: Start>Run ကို select လုပ်ပါ။ Run confirmation box ပေါ်လာလိမ့်မည်။ 'regedit' ကို ရိုက်ထည့်ပါ။

အဆင့် 2: အောက်ပါ screen သို့ သွားရန် click လုပ်ပါ။



ပုံ 6: Run confirmation dialog box ပုံ

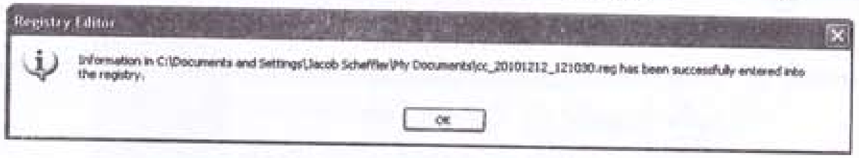
အဆင့် 3: Menu bar မှ File>Import ကို select လုပ်ပြီး Import Registry File screen ကို သွားပါ။



ပုံ 7: Registry စီစဉ်တည်းဖြတ်သူ (Editor)

အဆင့် 4: အောက်ပါ အတည်ပြုချက်ပေးမည့် dialog box ကို click လုပ်ပြီးသွားပါ။

အဆင့် 5: Registry မူပွားဖိုင်ကို သိမ်းဆည်းခြင်း ပြီးပြည့်စုံရန် click လုပ်ပါ။



ပုံ 8: Registry မူပွားဖိုင်ကို သိမ်းဆည်းပြီးကြောင်း အတည်ပြုပေးသည့် အခြား Registry Editor dialog box ၏ ပုံ

အဆင့်မြင့် Options များ၊ မကြာခဏမေးလေ့ရှိသော မေးခွန်းများနှင့် သုံးသပ်ချက်

ဤစာမျက်နှာရှိ အပိုင်းကဏ္ဍများမှာ

* 5.0 အဆင့်မြင့် Options များ
* 5.1 CCleaner ကို အသုံးပြုပြီး ပရိုဂရမ်များကို uninstall ပြုလုပ်ပုံ
* 5.2 CCleaner ၌ ပရိုဂရမ်အလိုအလျောက် စတင်ခြင်း (Auto-Start Programs) ကို disable ပြုလုပ်ပုံ
* 5.3 CCleaner ကို အသုံးပြုပြီး disk နေရာလွတ်ဖြစ်အောင် ရှင်းလင်းပုံ
* 5.4 မကြာခဏမေးလေ့ရှိသော မေးခွန်းများနှင့် သုံးသပ်ချက်
* 5.5 မေးခွန်း သုံးသပ်ချက်များ

5.0 Options အဆင့်မြင့်များ

CCleaner ၏လုပ်ဆောင်ချက်နှစ်ခုဖြစ်သော Uninstall နှင့် Startup လုပ်ဆောင်ချက်များသည် အောက်ပါအပိုင်းကဏ္ဍများတွင် ဖော်ပြပါရှိသည့်အတိုင်း သင့်ကွန်ပျူတာ system တစ်ခုလုံး၏ အကျိုးသက်ရောက်မှုကို တိုးတက်စေသည်။ သီးခြား drive တစ်ခုပေါ်တွင် နေရာလွတ်ရရန် ဖျက်သိမ်းရှင်းလင်းပေးသည်။

5.1 CCleaner ကို အသုံးပြုပြီး ပရိုဂရမ်များကို uninstall ပြုလုပ်ပုံ

အရေးကြီး ။ ။ သင်စတင် မပြုလုပ်မီ ဖျက်သိမ်းမည့် (သို့) uninstall ပြုလုပ်မည့် ပရိုဂရမ်သည် သင့်ကွန်ပျူတာ၏ လတ်တလောလုပ်ဆောင်မှုအတွက် မရှိမဖြစ် လိုအပ်သော ပရိုဂရမ်မျိုးမဖြစ်ရန် သေချာအောင်လုပ်ပါ။

CCleaner အား အသုံးမပြုခင် ယခင်က install လုပ်ထားသော အသုံးမပြုလိုသည့် (သို့) မလိုအပ်သည့် software များကို ဖျက်ရာတွင် ၎င်းတို့၏ ယာယီဖိုင်နှင့် folder များကိုပါ ဖယ်ရှားပစ်ရမည်။ ဤသို့ပြုလုပ်ခြင်းဖြင့် ဖျက်သိမ်းရမည့် ဖိုင်နှင့် folder အရေအတွက်များကို လျော့နည်းစေပြီး ရှင်းလင်းရေးလုပ်ဆောင်ချက်ကို ပြုလုပ်ရာတွင် အချိန်ကုန်သက်သာသည်။

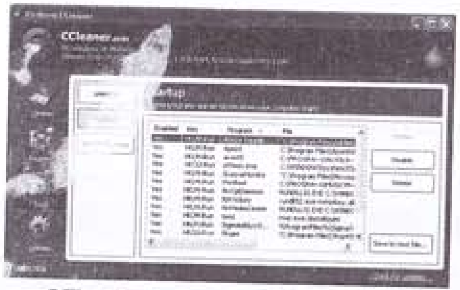
CCleaner ၏ uninstall လုပ်ဆောင်ချက်သည် Microsoft Windows ၏ 'Add or Remove Programs' လုပ်ဆောင်ချက်နှင့် အတူတူပင်ဖြစ်သည်။ 'Uninstall' လုပ်ဆောင်ချက်က ပရိုဂရမ်များကို ပို၍ ရှင်းလင်းလျှင်မြန်စွာ ဖော်ပြနိုင်သည်။

ခေတ်မမီတော့သော ပရိုဂရမ်များကို uninstall ပြုလုပ်ရန် အောက်ပါတို့ကို ဆောင်ရွက်ပါ။

အဆင့် 1: Start>Programs>CCleaner ကို ရွေးချယ်ပြီး Piriform CCleaner ၏ ပင်မမျက်နှာစာ (main user interface) ကို သွားပါ။

အဆင့် 2: အောက်ပါ screen သို့ click လုပ်ပြီး သွားပါ။

အဆင့် 3: ဖယ်ရှားရန် ပရိုဂရမ်များစာရင်း (Program to remove list) မှ ပရိုဂရမ်တစ်ခုကို ရွေးချယ်ပါ။ ၎င်းကို unistall လုပ်ရန် click ပါ။



ပုံ 1: Uninstall pane ကို ပြထားသော 'Tools' option ပုံ

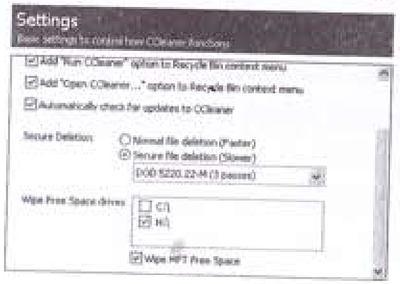
သတိပြုရန် ။ ။ အဆင့်မြင့် (Advanced) နှင့် အတွေ့အကြုံရှိ (Experienced) အသုံးပြုသူများအတွက် 'Rename Entry' နှင့် 'Delete Entry' တို့သည် private software တစ်ခုကိုထားရှိခြင်း၌ အသုံးဝင်သည်။ ထိုလုပ်ဆောင်ချက်နှစ်ခုစလုံးက Microsoft Windows ၏ 'Add/Remove Programs' (သို့) CCleaner ကို အသုံးပြု၍ ၎င်း software ကို ဝင်ရောက်ကြည့်ရှုလိုကြသော ပြိုင်ဘက်အဖွဲ့အစည်းများ၏ အန္တရာယ် ကို ကာကွယ်ပေးပြီး ၎င်းပရိုဂရမ်တည်ရှိမှုကို သင်တစ်ယောက်တည်းကိုသာ သိထားစေ သည်။

ပရိုဂရမ်ကို အမည်ပြန်ပေးရန် click လုပ်ပါ။ (သို့) ပရိုဂရမ်ကို ဖျက်သိမ်းရန် click လုပ်ပါ။ ၎င်းသည် အမှန်တကယ် uninstall လုပ်ခြင်းကား မဟုတ်ပါ။

5.2 CCleaner ၌ ပရိုဂရမ် အလိုအလျောက်စတင်ခြင်း (Auto-Start Programs) ကို disable ပြုလုပ်ပုံ

'Auto-Start Program' ဆိုသည်မှာ သင်၏ ကွန်ပျူတာကို ဖွင့်သည့်အခါတိုင်းတွင် ၎င်း ပရိုဂရမ်ကိုယ်တိုင် အလိုအလျောက် စတင်အောင် ပြုလုပ်ထားခြင်းကို ဆိုလိုသည်။ 'Auto-Start Program' သည် ကန့်သတ်ချက်ရှိသော system အရင်းအမြစ်များမှ တောင်းဆိုမှုများ ပြုလုပ်ပြီး သင်၏ ကွန်ပျူတာ စတင်ချိန် (start-up time) ကို အရှိန်လျော့ကျစေသည်။

အဆင့် 2: အောက်ပါ screen သို့ click လုပ်ပြီးသွားပါ။



ပုံ 12: 'Start up' pane ကို ဖော်ပြထားသော 'Tools' option ၏ ပုံ

အဆင့် 3: 'Start up' pane ရှိ ပရိုဂရမ်များစာရင်းမှ တစ်ခုကို ရွေးချယ်ပြီး သင်၏ ကွန်ပျူတာကို စတင်ဖွင့်ချိန်၌ အလိုအလျောက်စတင်ခြင်း မပြုနိုင်အောင် ၎င်း ပရိုဂရမ်ကို disable လုပ်ပါ။

5.3 CCleaner ကို အသုံးပြုပြီး disk နေရာအလွတ်ရှိအောင် ရှင်းလင်းပုံ

Windows ၏ OS တွင် ဖိုင်တစ်ဖိုင်ကို ဖျက်သိမ်းခြင်းသည် ၎င်းဖိုင်၏ အပေါ်ယံတည်ရှိမှုကိုသာ ဖယ်ရှားခြင်းဖြစ်ပြီး ၎င်း၏ data များကိုမူ မဖယ်သေးပါ။ Drive တစ်ခု၏ နေရာများပေါ်တွင် ဖိုင်အသစ်သစ်တို့သည် အကြိမ်ကြိမ်အခါခါ overwrite ဖြစ်၍ တည်ရှိနိုင်သော်လည်း ကျွမ်းကျင်မှုရှိသော တစ်စုံတစ်ယောက်ကသာ ၎င်း မူလဖိုင်၏ တစ်စိတ်တစ်ပိုင်း (သို့) အားလုံးကို ပြန်လည်တည်ဆောက်ပေးနိုင်သည်။ ဤသို့မဖြစ်အောင် ကာကွယ်ရန်မှာ သင်၏ hard disk ပေါ်ရှိနေရာများ အလွတ်ဖြစ် အောင် ရှင်းလင်းခြင်း ဖြစ်သည်။ CCleaner က မူလဖိုင်ဇယား (Master File Table) ကိုလည်း ရှင်းပေးသည်။

Master File Table (MFT) သည် ဖိုင်အားလုံး၏ အမည်၊ တည်နေရာနှင့် အချက်အလက်များကို ဖော်ပြထားသော ဇယားဖြစ်သည်။ ဖိုင်တစ်ဖိုင်ကို Microsoft Windows က ဖျက်သည့်အခါတွင် ၎င်းက အဆိုပါ ဖိုင်ကို ပိုမိုကောင်းမွန်စေရန် ဖျက်သိမ်းသည်ဟု အကြောင်းပြ၍ ၎င်း၏အညွှန်း entry ကို မှတ်သားထားသည်။ ထိုဖိုင်အတွက် MFT entry နှင့် ၎င်းတွင် ပါဝင်သည့်အချက်အလက်များမှ hard disk ပေါ်တွင် ဆက်လက်ကျန်ရှိနေသည်။

မှတ်ချက် ။ ။ Hard disk နှင့် Master File Table တို့ကို ရှင်းလင်းရန် အချိန်များစွာ လိုအပ်သည်။ ၎င်းအချိန်မှာ သင် သတ်မှတ်ထားသော 'Pass' အရေအတွက်ပေါ်တွင် မူတည်သည်။

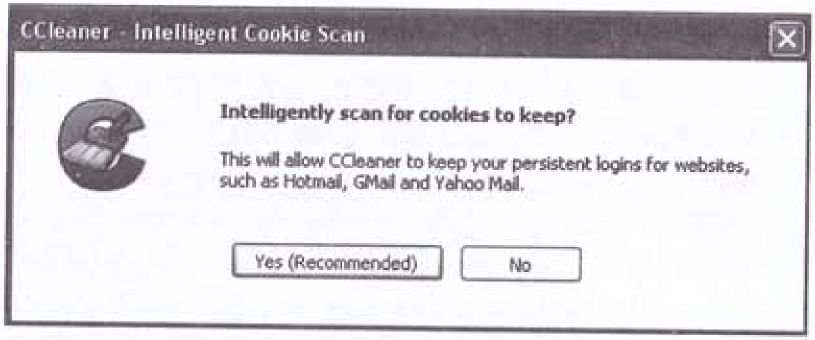
သင်၏ hard disk ပေါ်ရှိ နေရာလွတ်များနှင့် Master File Table ကို စတင်ရှင်းလင်းရန် Options>Settings နှင့် Cleaner panes နှစ်ခုစလုံးတွင် တိကျသော options များ သတ်မှတ်ပေးရမည်။

သင် ရှင်းလင်းလိုသော drive ကို ရွေးချယ်သတ်မှတ်ရန် အောက်ပါအဆင့်များကို ဆောင်ရွက်ပါ။

အဆင့် 1: 'Secure Deletion' နှင့် 'Secure file deletion (Slower)' options

နှစ်ခုကို စစ်ဆေးရန် စာရင်းကို လျှောချ (Scroll down) လုပ်ပြီး ကြည့်ပါ။ သင် မရွေးရသေးပါက ရွေးပါ။

အဆင့် 2: 'Settings' pane ကို click လုပ်ပြီး သွားပါ။



ပုံ 3: ရှင်းလင်းရန် options နှစ်ခုစလုံးကို check လုပ်ထားသော 'Settings' pane ပုံ

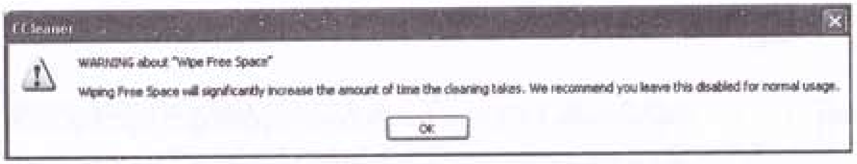
အဆင့် 3: အောက်တွင် ဖော်ပြထားသည့်အတိုင်း ရှင်းလင်းခြင်းပြုလုပ်ရန် 'Wipe Free Space drives' နှင့် 'Wipe Free Space' options နှစ်ခုကို check လုပ်ပြီး ရွေးပါ။

အဆင့် 4: Piriform CCleaner ၏ ပင်မမျက်နှာစာ (main user interface) ကို click လုပ်ပြီး သွားပါ။

မှတ်ချက် ။ ။ သင်၏ ယာယီဖိုင်များကို နေ့စဉ်ရှင်းလင်းချိန်တွင် ဤအပိုင်းကို enable လုပ်ထားပြီးဖြစ်ပါက နောက်တစ်ဆင့်တွင် သင်စိတ်ကြိုက် ရွေးချယ်ပြီး ပြုလုပ်ပါ။

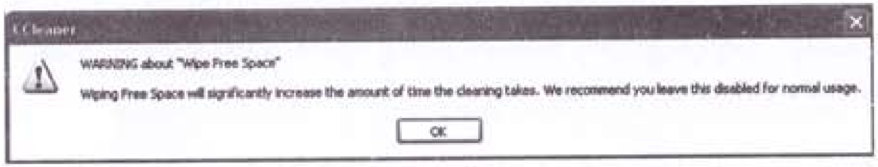
သတိပြုရန် ။ ။ရှင်းလင်းရေး လုပ်ငန်းစဉ် မစတင်မီ အခြားပရိုဂရမ်အားလုံးကို ပိတ်ထားရန် သတိပြုပါ။ အကယ်၍ ဖွင့်ထားမိပါက CCleaner က ၎င်းပရိုဂရမ်နှင့် ဆက်စပ်နေသော ဖိုင်များကို ဖယ်ရှားပေးနိုင်မည် မဟုတ်ပါ။

အဆင့် 5: Windows tab ကိုဆွဲချပြီး အဆင့်မြင့် (Advanced) section ကို သွားပါ။ ထို့နောက် 'Wipe Free Space' option ကို check လုပ်၍ရွေးပါ။ အောက်ပါ သတိပေးချက် တွေ့ရမည်။



ပုံ 4: သတိပေး အတည်ပြုမည့် dialog box ၏ ပုံ

အဆင့် 6: အောက်ပါ screen သို့ click လုပ်ပြီးသွားပါ။



ပုံ 5: အတည်ပြုချက်ယူမည့် dialog box ၏ ပုံ

အဆင့် 7: သင်၏ Hard disk နှင့် Master File Table ရှိ နေရာလွတ်များ ရှင်းရန် click လုပ်ပါ။

5.4 မကြာခဏ မေးလေ့ရှိသော မေးခွန်းများနှင့် သုံးသပ်ချက်

အယ်လီနာနှင့် နီကိုလိုင်တို့သည် CCleaner ၏ အသုံးပြုရလွယ်ကူမှုကို သိရှိပြီး တချို့ အသုံးပြုပုံ အသုံးပြုနည်းနှင့် ပတ်သက်၍မေးရန် မေးခွန်းများ ရှိကြသည်။

မေး ။ ။ CCleaner ကို uninstall လုပ်လျှင် မူလဖျက်ထားတဲ့ အရာတွေဟာ အဲဒီအတိုင်း ကျန်ရှိနေမှာလား။

ဖြေ ။ ။ ဟုတ်ပါတယ်။ CCleaner ကို မှန်မှန်ကန်ကန် အသုံးပြုထားမယ်ဆိုလျှင် ဖျက်ပြီးသားဖိုင်ဟာ အမြဲတမ်း ဖျက်ပြီး ဖြစ်နေမှာပါ။

မေး ။ ။ USB memory stick တစ်ခုမှာ CCleaner ကို ကူးထားတဲ့အခါ ၎င်းကို ကျွန်တော် အင်တာနက်ကဖေးမှာ ထိုင်တဲ့အချိန် ကွန်ပျူတာမှာ အသုံးပြုပြီး ကျန်ခဲ့တဲ့ သဲလွန်စတွေကို ဖျောက်ဖျက်ဖို့ သုံးနိုင်ပါသလား။ မသုံးနိုင်ဘူးဆိုရင်ရော ဘာအကြောင်းကြောင့်ပါလဲ။

ဖြေ ။ ။ သုံးနိုင်ပါတယ်။ CCleaner မှာ အိတ်ဆောင်ပုံစံအတွက် ထုတ်လုပ်ထားတဲ့ version ရှိပါတယ်။ (www.piriform.com/ ccleaner/builds စာမျက်နှာမှာ CCleaner-Portable section တွင်ကြည့်ပါ။ သင်ထိုင်ပြီး အလုပ်လုပ်ခဲ့တဲ့ အင်တာနက်ကဖေးမှာ USB memory stick ကနေ ပရိုဂရမ်တွေ အသုံးပြုဖို့ ခွင့်ပြုရင် ဖြစ်နိုင်ပါတယ်။ သင် လုပ်ဆောင်ခဲ့တဲ့ လုပ်ရပ်တွေရဲ့ သဲလွန်စတွေကို CCleaner ရဲ့ အိတ်ဆောင်ပုံစံ version ကိုအသုံးပြုပြီး ဖယ်ရှားနိုင်ပါတယ်။ ဒါပေမဲ့ သင်မှတ်ထားရမှာက အင်တာနက်ကဖေးမှာဆိုလျှင် သင့်ကိုစောင့်ကြည့်မယ့်သူ ရှိနိုင်တယ်ဆိုတာပါပဲ။ ဒါ့အပြင် အင်တာနက်ကဖေးမှာ သင့်ကွန်ပျူတာကို memory stick နဲ့ တွဲဖက် အသုံးပြုခြင်းဟာ အနှောင့်အယှက် အဖျက်အစီးများလည်း ဝင်ရောက်စေနိုင်ပါတယ်။

မေး ။ ။ CCleaner ကို 'Pass' တစ်ခုပဲ သုံးမယ်ဆိုလျှင် တစ်စုံတစ်ယောက်က ကျွန်တော့် data တွေကို ရယူဖို့ရာ ဖြစ်နိုင်ပါ့မလား။ တကယ်လို့ 'Pass' ကို 7 ခု အထိ သုံးမယ်ဆိုရင် ဘာဖြစ်မလဲ။
ဖြေ ။ ။ အလွန်ကောင်းတဲ့ မေးခွန်းပါပဲ။ Data ကို ရှင်းဖို့ 'Pass' ကို များများ သုံးလေ အဲဒီ data ကို တစ်စုံတစ်ယောက်က ပြန်လည်ရယူဖို့ အခွင့်အလမ်းနည်းလေ ပါပဲ။ ဒါပေမဲ့ data တွေ ရှင်းလင်းရာမှာ 'Pass' ကို များများသုံးလေ ရှင်းလင်းမယ့် လုပ်ငန်းစဉ်ရဲ့ အချိန်ကြာလေ ဖြစ်ပါလိမ့်မယ်။

မေး ။ ။ ကျွန်တော့် ကွန်ပျူတာပေါ်မှာ ယာယီထည့်သွင်း အသုံးပြုထားတဲ့ ပရိုဂရမ်တွေရဲ့ ထင်ရှားတဲ့ သင်္ကေတ အမှတ်အသားတွေကို ဖယ်ရှားခြင်းအတွက် Windows Registry ကို ရှင်းလင်းခြင်းက သင့်တော်ပါသလား။
ဖြေ ။ ။ သင့်တော်ပါတယ်။ သင့်ရဲ့ ယာယီဖိုင်များ အားလုံးကို ဖျက်သိမ်းသင့်ပြီး သင် အသုံးပြုတဲ့ software ရဲ့ လုပ်ဆောင်ချက်နဲ့ သဲလွန်စတွေ အားလုံးကို ဖယ်ရှားပစ်ဖို့ Windows Registry ကို ရှင်းလင်းရပါမယ်။ တကယ်လို့ အချိန်ကန့်သတ်ချက် ရှိထားမယ်ဆိုလျှင် Windows Registry ကို အရင်ဆုံး စရှင်းတာ အကောင်းဆုံးပါ။

5.5 မေးခွန်းသုံးသပ်ချက်များ

* ဘယ်လိုအချက်အလက်တွေကို CCleaner က သင့်ရဲ့ ကွန်ပျူတာမှ ဖယ်ရှားပေးတာလဲ။
* အဲဒါက ဘယ်လို လုပ်ဆောင်တာလဲ။
* သင့် data ကို စိတ်ချစွာ overwrite လုပ်နိုင်ဖို့ သင်ရွေးချယ်တဲ့ 'Pass' အရေအတွက်က ဘာတွေလုပ်ဆောင်သလဲ။
* Windows Registry ဆိုတာ ဘာလဲ။ အဲဒါကို ဘာကြောင့် ရှင်းလင်းပေးသင့်သလဲ။
* Windows Registry ကို ရှင်းလင်းရေး မစမီ သင် ဘာလုပ်သင့်သလဲ။

RiseUp- လုံခြုံသော အီးမေးလ်ဝန်ဆောင်မှု

RiseUp သည် နိုင်ငံရေးနှင့် လူမှုရေးဆိုင်ရာ တရားဥပဒေကို တာဝန်ယူထားသော လူတစ်ဦးချင်း (သို့) အဖွဲ့အစည်းများအား လုံခြုံမှုရှိသည့် အီးမေးလ်နှင့် ဆက်သွယ်ရေး ဝန်ဆောင်မှုများ ထုတ်ပေးရန် သတ်မှတ်ထားသော အဖွဲ့အစည်းတစ်ခု ဖြစ်သည်။

* RiseUp ၏ home page မှာ https://riseup.net/ ဖြစ်သည်။
* ကွန်ပျူတာလိုအပ်ချက်များမှာ ကွန်ရက်ဆက်သွယ်မှု (internet connection) ရှိရမည်။ RiseUp ကို Firefox ၏ ကွန်ရက်ရှာဖွေစက် (web browser) နှင့် တွဲဖက်လုပ်ဆောင်ရန် အကောင်းဆုံး ဖြစ်သည်။
* License မှာ အခမဲ့ (freeware) ဖြစ်သည်။
* ဖတ်သင့်သော အကြောင်းအရာမှာ အခန်း 7: 'သင်၏ အင်တာနက်ဆက်သွယ်မှုကို သီးသန့်ထားရှိခြင်း' ခေါင်းစဉ်ဖြစ်သည်။
* အဆင့်သတ်မှတ်ချက်မှာ Level 1: Beginner, 2: Average, 3: Inter-mediate, 4: Experienced, 5: Advanced တို့ဖြစ်ကြသည်။
* ဤပရိုဂရမ်ကို စတင်အသုံးပြုရန် ကြာသောအချိန်မှာ မိနစ် 20 ဖြစ်သည်။
* သင်ရရှိမည့် အကျိုးကျေးဇူးများမှာ
* ထိန်းချုပ်မှုရှိသော လူမှုအဖွဲ့အစည်းတစ်ခုနှင့် စီးပွားရေးကြော်ငြာများမှ ကင်းလွတ်သော အီးမေးလ် account တစ်ခု၊

* အသွင်ပြောင်း ဆက်သွယ်ချက်တစ်ခုပေါ်မှ သီးသန့် အီးမေးလ် ဆက်သွယ်ဆောင်ရွက်မှုနှင့် သင်၏ အီးမေးလ်ကို အင်တာနက် (သို့) အီးမေးလ် ပရိုဂရမ် တစ်ခုနှင့် access လုပ်နိုင်ခွင့်၊
* သင်၏ အီးမေးလ်လိပ်စာကို ပြောင်းလဲခွင့်၊ အီးမေးလ် box အရွယ်အစားကို သတ်မှတ်ခြင်းနှင့် အခြားသူများအား RiseUp နှင့် ပူးပေါင်းဆောင်ရွက်ရန် ဖိတ်ခေါ်နိုင်ခြင်းတို့ ဖြစ်ကြသည်။

ရွေးချယ်စရာ အီးမေးလ် ဝန်ဆောင်မှုများ

Rise Up သည် အင်တာနက်ဆိုင်ရာ လုံခြုံမှုနှင့် မူပိုင်ဖြစ်မှုတို့ကို ယုံကြည်ရသော ထောက်ခံသူများကစီစဉ်ထားသည့် စိတ်ချရသော အီးမေးလ် ဝန်ဆောင်မှုဖြစ်သော်လည်း တစ်မူထူးခြားသော အီးမေးလ်ဝန်ဆောင်မှုတစ်ခုက အာမခံချက်မရှိဘဲ ဝင်ရောက်ဆွဲဆောင်မှုများ ရှိတတ်သည်။ ၎င်းက သင့်၏ တိုင်းပြည်တွင်းမှာရှိသော လူသိများထင်ရှားသည့် အီးမေးလ်ဝန်ဆောင်မှုလုပ်ငန်းနှင့်တွဲဖက်အသုံးပြုသော အခြေအနေမျိုးတွင် ပို၍ အဓိပ္ပာယ် ရှိစေပါသည်။ ရည်ရွယ်ချက်မှာ သင်၏ လုံခြုံရေးဆိုင်ရာ လိုအပ်ချက်အနိမ့်ဆုံးကို ညှိနှိုင်းခြင်းမရှိဘဲ ဆုံးဖြတ်ချက်ပြုလုပ်ရန် ဖြစ်သည်။ အီးမေးလ်ဝန်ဆောင်မှုတစ်ခုကို ရွေးချယ်ရာတွင် ထည့်သွင်းစဉ်းစား သင့်သည့်အချက်များကို အောက်တွင် ပေးထားသည်။

အဆင့် 1: သတင်းအချက်အလက်များ အားလုံး ရွှေ့ပြောင်းခြင်း (login-in အချက်အလက်များနှင့် သင်၏ အီးမေးလ်များ အပါအဝင်) အတွက် အသွင်ပြောင်း channels များ (https နှင့် IMAPs, POP3s, SMTPs ကဲ့သို့ SSL အသွင်ပြောင်းခြင်းနှင့် ဆက်နွယ်သော ပြဿနာ ရှိ၊ မရှိ (ဥပမာ encryption certificates များနှင့် ပတ်သက်သော ပြဿနာများ)။

အဆင့် 2: အီးမေးလ် servers တွေကို လုံခြုံတဲ့ နည်းလမ်းနဲ့ စီစဉ်ထားခြင်း ရှိပါသလား။ သင့်ရဲ့ သတင်းအချက်အလက်တွေကို ကာကွယ်ဖို့ အကောင်းဆုံး လေ့ကျင့်မှုတွေ ပြုလုပ်ထားတဲ့ ကျွမ်းကျင်သူ professionals တွေက အီးမေးလ် ဝန်ဆောင်မှုကို လုပ်ဆောင်ပါသလား။ ၎င်းတို့က တခြား ပြိုင်ဘက် အဖွဲ့အစည်းတွေဆီကို အကြောင်းအမျိုးမျိုးကြောင့် (စီးပွားရေး၊ လူမှုရေး၊ ဘာသာရေး စသဖြင့်) သင့်ရဲ့ သတင်းအချက်အလက်တွေ

ကို access လုပ်ခွင့် ထုတ်ပေး။ မပေးကို ယုံကြည်လို့ရပါ့မလား။

အဆင့် 3: သင့် servers တွေရဲ့ နယ်မြေဆိုင်ရာ မူပိုင်ခွင့် ပြုလုပ်ထားတဲ့ နေရာသို့မဟုတ် ၎င်း company မှတ်ပုံတင်ခြင်း ပြုလုပ်ရာနေရာကို သိပါသလား။ ဒီသတင်းအချက်အလက်တွေဟာ သင့်ရဲ့ အီးမေးလ် လုပ်ဆောင်မှုနှင့် သတင်းအချက်အလက်တွေရဲ့ လုံခြုံမှုနဲ့ မူပိုင်ခွင့်အတွက် ဆက်သွယ်မှု ဘယ်လိုရှိတယ်ဆိုတာကို သိပါသလား။

ကမ္ဘာကြီးရဲ့ အချို့နေရာတွေမှာ Google Mail နဲ့ Rise Up တို့ကို ပေါင်းစပ်အသုံးပြုမှုဟာ အလွန်အသုံးဝင်တဲ့ ပေါင်းစည်းခြင်း ဖြစ်တယ်ဆိုတာကို ပြသနေပါတယ်။ ၎င်းရဲ့ စီးပွားရေးဆိုင်ရာ သဘောသဘာဝအရ လုံခြုံရေးကိုလည်း ညှိနှိုင်းမှုများ မပြုလုပ်ပါဘူး။

1.1 ဤပရိုဂရမ်ကို သင်မစတင်မီမှာ သိထားသင့်သော အကြောင်းအရာများ

Rise Up သည် နိုင်ငံရေးနှင့် လူမှုရေးဆိုင်ရာ တရားဥပဒေကို တာဝန်ယူထားသော လူတစ်ဦးချင်း (သို့) အဖွဲ့အစည်းများအား လုံခြုံမှုရှိသော ဆယ်သွယ်ရေးဝန်ဆောင်မှု၊ စာရင်းပြုစုခြင်းနှင့် မေးလ်ဝန်ဆောင်မှုတို့ ထုတ်လုပ်ပေးရန် ရည်ရွယ်ထားသော အဖွဲ့အစည်းတစ်ခု ဖြစ်သည်။ ၎င်းတို့၏ ဝန်ဆောင်မှုမှာ အခမဲ့ဖြစ်သောကြောင့် သင်၏ အီးမေးလ် account သည် အခြား လုံခြုံမှုမရှိသော၊ စီးပွားရေးကြော်ငြာဦးစားပေး ထုတ်လုပ်သူများ၏ account များထက် ပို၍ သေးငယ်နိုင်သည်။ ကျွန်ုပ်တို့၏ Digital Security Project တွင် ပါဝင်သူများ (သို့) မူလရှိထားသော အဖွဲ့ဝင်များမှ ဖိတ်ခေါ်သော code နံပါတ်ကို ရရှိလူသာလျှင် account အသစ်တစ်ခုကို မှတ်ပုံတင်ခြင်း ပြုလုပ်နိုင်သည်။

Rise Up သည် အင်တာနက်ပေါ်မှတစ်ဆင့် လျှို့ဝှက်သင်္ကေတ သွင်းရန်ပေးပို့ရာတွင် အသုံးပြုသော Secure Sockets Layer (SSL) မှတစ်ဆင့် သီးခြားအလုပ်လုပ်သည်။ ၎င်း SSL သည် သင်၏ ကွန်ပျူတာနှင့် ၎င်းတို့၏ servers များ အကြား လုံခြုံသော ဆက်သွယ် မှုကို ထုတ်လုပ်ပေးသည်။ ဤ လုံခြုံမှုကို စိတ်ချရသော POP, IMAP နှင့် SMTP ဆက်သွယ်မှုများ (သင်၏ အီးမေးလ်ကို မေးလ်ပရိုဂရမ်တစ်ခုမှ download ရယူရန် အသုံးပြုသော အထူး protocols များကို ရည်ညွှန်းသည်)မှတစ်ဆင့် client program ၌ သင်၏ အီးမေးလ်ကို ဖတ်ရှုသည့်အခါတွင်

ပြင်ဆင်ပေးသည်။ RiseUP ကို Mozilla Thunderbird နှင့်လည်း ပူးတွဲ အသုံးပြုနိုင်သည်။ သင်၏ Rise Up အီးမေးလ် account ကို access လုပ်ရန် Mozilla Thunderbird အား မည်ကဲ့သို့ တပ်ဆင်ရမည်ကို Thunderbird အခန်းအရောက်တွင် ကြည့် ပါ။

* RiseUp Account တစ်ခု ဖန်တီးပုံ
* သင်၏ RiseUp Account သို့ ဝင်ရောက်ပုံ
* သင်၏ Account အသုံးချပုံ (settings) များကို ပြုပြင်ပုံ
* မကြာခဏ မေးလေ့ရှိသော မေးခွန်းများနှင့် သုံးသပ်ချက်

RiseUp Account တစ်ခုဖန်တီးပုံ

ဤစာမျက်နှာရှိ အပိုင်းကဏ္ဍများမှာ

* 2.0 RiseUp Account တစ်ခုကို မှတ်ပုံတင်ခြင်းအတွက် နည်းလမ်းအမျိုးမျိုး
* 2.1 Account သတင်းအချက်အလက် ပုံစံ (form)
* 2.2 Password ပုံစံ (form)
* 2.3 အပြန်အလှန် ကူညီထောက်ပံ့မှု ပုံစံ (form)
* 2.4 လုပ်ဆောင်မှု ပုံစံ (form)

2.0 RiseUp Account တစ်ခုကို မှတ်ပုံတင်ခြင်းအတွက် နည်းလမ်းအမျိုးမျိုး

RiseUp က အီးမေးလ် account တစ်ခုကို မှတ်ပုံတင်ရန် သင့်အား နည်းလမ်း 3 မျိုး ပေးထားသည်။ နည်းလမ်း 1 မျိုးစီတွင် အချိန်နှင့် အားထုတ်မှုအမျိုးမျိုးတို့ ရင်းနှီးမြှုပ်နှံရန် လိုအပ်သည်။

1: RiseUp Account ရှိပြီးသော အဖွဲ့ဝင်နှစ်ဦးမှ ပုဂ္ဂိုလ်တစ်ဦးချင်း (သို့) အဖွဲ့အစည်းများကို ၎င်းတို့နှင့် ဆက်သွယ်ရန် ဖိတ်ကြားခြင်း။
ဤနည်းလမ်းကို လုပ်ဆောင်နိုင်ရန်မှာ ၎င်းတို့မှ သင့်အား ဖိတ်ကြားသည့် code နံပါတ်ကို လိုအပ်သည်။ မည်ကဲ့သို့ codes များ ထုတ်ပေးသည်ကို သိချင်ပါက အခန်း 4.3 ရှိ 'ဖိတ်ကြားခြင်း စာမျက်နှာ (Invites Page)'တွင် ကြည့် ပါ။

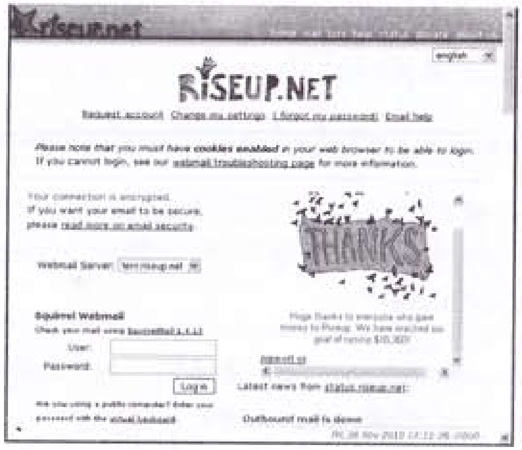
Black

2: RiseUp အဖွဲ့ထံမှ မိမိကိုယ်တိုင် account တစ်ခုကို တိုက်ရိုက်တောင်းဆိုခြင်း။ RiseUp သည် ယေဘုယျအားဖြင့် စေတနာ့ဝန်ထမ်း ကူညီသူများ၏ စေတနာ၊ ဝါသနာနှင့် လှူဒါန်းကူညီမှုများကို အခြေပြု၍ တည်ဆောက်ထားသည်ကို သင့်စိတ်ထဲမှာ မှတ်ထားပါ။ ထို့ကြောင့် ဤနည်းလမ်းအတွက် စိတ်ရှည်သည်းခံပြီး စောင့်ဆိုင်းရန် လိုအပ်သည်။

3: ကျွန်ုပ်တို့၏ လေ့ကျင့်ရေးအပိုင်းကဏ္ဍတွင် ပါဝင်ထားကြသော ပူးပေါင်း ဆောင်ရွက်သူများသည် တစ်ဦးချင်းစီ ဖိတ်ကြားသည့် codes နံပါတ်များကို ရရှိမည်ဖြစ်ပြီး ၎င်း၏ Security Edition ကို hard copy (ဥပမာ CD, DVD) တစ်ခုအနေဖြင့် ထုတ်ဝေပေးထားသည်။

သင့်အား ဖိတ်ကြားထားသည့် code နံပါတ်ကို ရရှိပြီးပါက သင်၏ RiseUp account ကို အခမဲ့မှတ်ပုံတင်ရန် အောက်ပါအဆင့်များ ဆောင်ရွက်ပါ။

အဆင့် 1: သင်၏ web browser မှ တစ်ဆင့် https://mail.riseup.net ကို ရိုက်ထည့်ပါ။ အောက်ပါ RiseUp site ကို တွေ့ရမည်။



ပုံ 1: https://mail.riseup.net/ page ပုံ

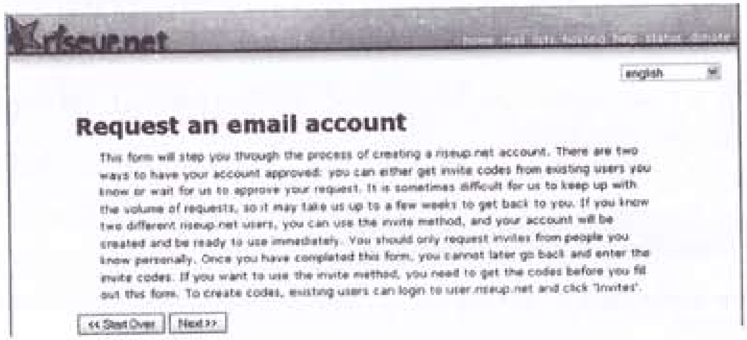
မှတ်ချက် ။ ။ https:// တွင်ပါဝင်သော 's' စာလုံးမှာ သင်သည် ယခု Secure Socket Layer (SSL) မှတစ်ဆင့် ဆက်သွယ်မှုများ ပြုလုပ်နေကြောင်းကို ပြသနေသည်။

၎င်း အသိပေးသည့် message သည် login ဝင်ရောက်မည့် ကွက်လပ်၏ အပေါ်ဘက်တွင် ပေါ်လာလိမ့်မည်။

ဤအကြောင်းကို ပိုမို သိရှိလိုပါက အခန်း 7 ရှိ 'သင်၏ အင်တာနက် ဆက်သွယ်မှုကို သီးသန့်ထားရှိခြင်း' ခေါင်းစဉ် (သို့) https://help.riseup.net security တွင် ကြည့်ပါ။

အဆင့် 2: account တောင်းဆိုမှုပြု 'Request Account' page ကို click လုပ်ပြီးသွားပါ။

အဆင့် 3: RiseUp Request မှ အီးမေးလ် account တစ်ခု ကျွန်ုပ်တို့၏ အီးမေးလ်ဝန်ဆောင်မှု page ကို click လုပ်ပြီး သွားပါ။



ပုံ 2: **အီးမေးလ်** account **တစ်ခုကို တောင်းဆိုသော** RiseUp Request page **၏** ပုံ

အရေးကြီး ။ ။ သင်၏ RiseUp Account ဖန်တီးခြင်းတွင် ဆက်လက်လုပ်ဆောင်ရန် အောက်ပါ options များကို enable လုပ်ထားရမည်။

အဆင့် 4: RiseUp ၏ မူဝါဒအသီးသီးကို သင်ဖတ်ရှုပြီးပါက check boxes များ၌ အောက်ပါ options များကို enable လုပ်ရန် click နှိပ်ပါ။

- I accept riseup.net's privacy policy -option (riseup.net ၏ မူပိုင်ရေးရာ ဝါဒကို လက်ခံကြောင်း)
- I accept riseup.net's terms of service-option (riseup.net ၏ ဝန်ဆောင်မှု ပုံစံများကို လက်ခံကြောင်း)

အဆင့် 5: အောက်ပါအွန်လိုင်း forms များကို ဖြည့်စွက်၍ သင်၏ Rise Up

account ကို ဖန်တီးရန် click လုပ်ပါ။
၎င်းတို့မှာ account အချက်အလက်၊ password ၊အပြန်အလှန် ကူညီထောက်ပံ့မှု၊ လုပ်ဆောင်မှု ပုံစံများ (forms) ဖြစ်ကြသည်။

2.1 Account သတင်းအချက်အလက်ပုံစံ

အဆင့် 6: သင်၏ account အတွက် အလိုရှိရာ အသုံးပြုသူအမည်ဖြင့် ဝင်ရောက်ပါ။ ၎င်းက သင်၏ ဝင်ရောက်ခွင့် (login) နှင့် သင်၏ အီးမေးလ်လိပ်စာ ဖြစ်လာလိမ့်မည်။ (ဤ လက်တွေ့သင်ခန်းစာတွင် ssayyed @ riseup.net ဟူသော အီးမေးလ် account ကို ထုတ်ပေးရန် 'ssayyed' ဟူသော အမည်ကို ဥပမာပြု ထားသည်)

အရေးကြီး ။ ။ အသုံးပြုသူ အမည်ထည့်ရာတွင် ကော်မာ(comma), full stops (.) နှင့် spaces များ မသုံးပါနှင့်။

ပုံ 3: ပြည့်စုံသော account သတင်းအချက်အလက်ပုံစံပြ ဥပမာတစ်ခု

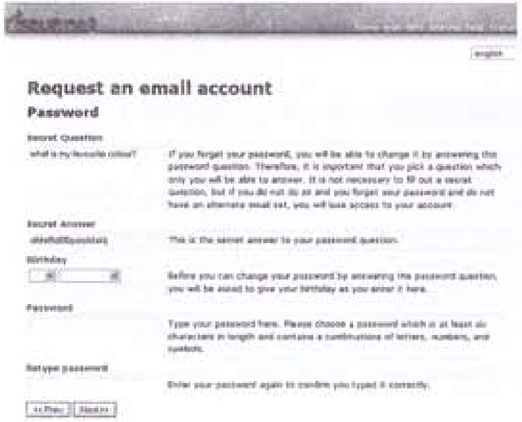
အဆင့် 7: ညီညွတ်မှု (Unique) ဖြစ်သော အသုံးပြုသူအမည်ကို ရွေးချယ်ပြီးပါက 'Password ပုံစံ' သို့သွားရန် click လုပ်ပါ။

မှတ်ချက် ။ ။ အသုံးပြုသူ အမည်တူရှိပါက သင့်အား အမည်အသစ်ရွေးရန် သတိပေးချက် ပေါ်လာလိမ့်မည်။

2.2 Password ပုံစံ

Password ပုံစံတွင် သင်သည် လုံခြုံရေးဆိုင်ရာ မေးခွန်းများနှင့် အဖြေများ၊ ကြံ့ခိုင်မှုရှိသော password တို့ကို ပြုလုပ်ပေးရမည်။ သို့မဟုတ်ပါက account ဖန်တီးခြင်းလုပ်ငန်းစဉ်ကို ဆက်လက်လုပ်ဆောင်ရန် ခွင့်ပြုချက်ရမည် မဟုတ်ပါ။သင်၏ password ကို မေ့သွားသည့်အခါမျိုး ဖြစ်ပေါ်လာပါက ယခု လုပ်ဆောင်ချက် များ၏ ကူညီမှုကို ရရှိရန် RiseUp က တိုက်တွန်းထားသည်။ သို့သော် ဤကဲ့သို့ ရည်ရွယ်ချက်ကောင်းကောင်းဖြင့် ပြုလုပ်ထားသော်လည်း ကံအကြောင်းမလှပါက ၎င်းတို့ကပင် လုံခြုံရေးအန္တရာယ်ကို ဖြစ်ပေါ်စေနိုင်သည်။

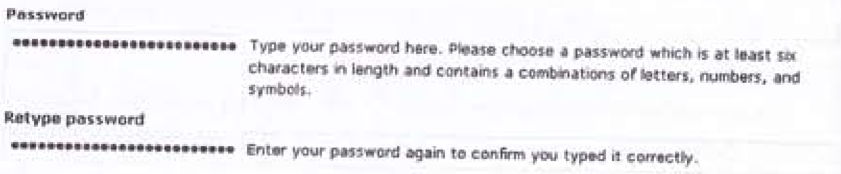
ဥပမာ သင်၏တစ်ဖက်ရန်သူမှ အဖြေကို မှန်ကန်စွာမှန်းဆနိုင်ခြင်း (သို့မဟုတ်) သင့်ထံသို့ ပို့လိုက်သော password ကို ကြားဖြတ်ဖမ်းယူခြင်းတို့ ဖြစ်ကြသည်။သင်၏ လျှို့ဝှက်မေးခွန်းမှ အဖြေကိုမှန်းဆရယူမည့် ခြိမ်းခြောက်သူများကို ဖယ်ရှားရန် မေးခွန်းကို ဖြေထားသောအဖြေကို ဖျက်ဆီးပစ်ရန် သတိပေးပါသည်။ ၎င်းကို အောက်ပါ ဥပမာတွင် ပြထားသကဲ့သို့ ကွက်လပ်နှစ်နေရာအား ဖျက်ဆီးခြင်းဖြင့် လုပ်ဆောင်နိုင် ပါသည်။



ပုံ 4: မေးခွန်းပုံစံ ဥပမာတစ်ခုနှင့် password form ထဲရှိ ဖျက်ဆီးပြီး အခြေအနေပြပုံ

သတိပေးချက် ။ ။ ဤသို့ပြုလုပ်ခြင်းသည် သင်၏ password အား အလိုအလျောက် အားဖြင့် reset ပြုလုပ်ရန် မဖြစ်နိုင်ပါ။ သင်သည် သင်၏ password ကို မှတ်သား ထားရမည် (Remember your Password!) ၎င်းသည် အဆင်အပြေဆုံး မဟုတ်သော်လည်း လုံခြုံမှုအရှိဆုံး option ဖြစ်သည်။

သင့် RiseUp account တွင်ရှိသော password သည် သင်၏ account လုံခြုံရေးတွင် အရေးအပါဆုံး အခြေခံအကြောင်း အရာ ဖြစ်သည်။ ကြံ့ခိုင်မှုရှိသော password တစ်ခုကို ဖန်တီးနိုင်ရန် KeePass ၏ လမ်းညွှန်ချက်များရှိ အခန်း 3 တွင်ပါဝင်သော 'ကောင်းမွန်သည့် passwords များကို ဖန်တီးပုံနှင့် ပြုပြင်ပုံ' ခေါင်းစဉ်၌ ကြည့် ပါ။



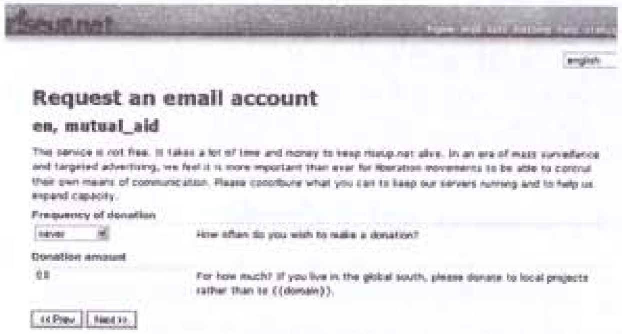
ပုံ 5: Password ပုံစံရှိ ပြီးပြည့်စုံသော password ထည့်သွင်းမှု အပိုင်းပုံ

အဆင့် 8: 'အပြန်အလှန် ထောက်ပံ့ကူညီမှု ပုံစံ'ကို လုပ်ဆောင်ရန် click လုပ်ပါ။

2.3 အပြန်အလှန် ထောက်ပံ့ကူညီမှု ပုံစံ

RiseUp သည် လှူဒါန်းသူများနှင့် စေတနာ့ဝန်ထမ်းကူညီသူများ၏ ကြင်နာခြင်း။ ရက်ရောခြင်းတို့အပေါ်တွင် လုံးဝ မှီခိုအားထားနေရသည်။ ဘဏ္ဍာရေးဆိုင်ရာ ထောက်ပံ့မှုများအတွက် ၎င်းတို့၏ တောင်းဆိုချက်များမှာ တရားဝင်ဖြစ်ပြီး မဖြစ်မနေ လိုအပ်သော်လည်း RiseUp က အသုံးပြုသူတို့၏ ပြည်တွင်းရှိ လူမှုရေးဆိုင်ရာ တရားမျှတရေး ဆောင်ရွက်မှုလုပ်ငန်းများတွင်လည်း ၎င်းတို့၏ပိုက်ဆံများကို ထည့်သွင်းကြပါရန် တိုက်တွန်းထားသည်။ RiseUp တွင် လှူဒါန်းခြင်း ပြု၊ မပြုကို ဆုံးဖြတ်ရန်မှာ သင် (သို့) သင်၏ အဖွဲ့အစည်းအပေါ်တွင် မူတည်ပါသည်။

မှတ်ချက် ။ ။ သင်၏ ဆုံးဖြတ်ချက်က သင်၏ account ဖန်တီးခြင်း လုပ်ဆောင်ချက် အပေါ်တွင် မည်သို့မျှ သက်ရောက်မှု မရှိပါ။ သင်၏ အခမဲ့ RiseUp account ကို ဆက်လက် လုပ်ဆောင်နိုင်ပါသည်။



ပုံ 6: အပြန်အလှန် ကူညီထောက်ပံ့မှု ပုံစံ

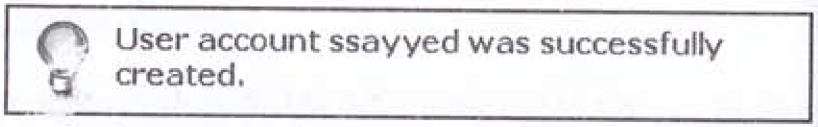
အဆင့် 9: 'လုပ်ဆောင်ချက် ပုံစံ' သို့သွားရန် click လုပ်ပါ။

2.4 လုပ်ဆောင်ချက် ပုံစံ

လုပ်ဆောင်ချက်ပုံစံတွင် သင့်ကို ဖိတ်ကြားထားသော codes နံပါတ်ဖြင့် ဝင်ရောက်ရန် လိုအပ်သည်။

အဆင့် 10: သက်ဆိုင်ရာ ကွက်လပ်တွင် ဖိတ်ကြားသည့် codes နံပါတ်ကို ရိုက်ထည့်ပါ။

ပုံ 7: ပြီးပြည့်စုံသော 'လုပ်ဆောင်ချက် ပုံစံ'ပြ ဥပမာတစ်ခုပုံ



ပုံ 8 : Account တစ်ခုကို အောင်မြင်စွာဖန်တီးပြုလုပ်ထားသော ဥပမာတစ်ခု

အဆင့် 11: သင်၏ RiseUp account ပြုလုပ်ခြင်း အဆုံးသတ်ရန် click လုပ်ပါ။

အဆင့် 12: ပုံ 2: သို့ ပြန်သွားရန် click ပါ။

'ဂုဏ်ယူပါတယ်'၊ ယခု သင်၏ RiseUp အီးမေးလ် account ကို အောင်မြင်စွာ ဖန်တီးပြုလုပ်ပြီးပါပြီ။ အထက်ရှိ ပုံ :2 သို့ ပြန်၍ သွားပါ။

သင်၏ RiseUp Account အတွင်းသို့ ဝင်ရောက်ပုံ

ဤစာမျက်နှာရှိ အပိုင်းကဏ္ဍများမှာ

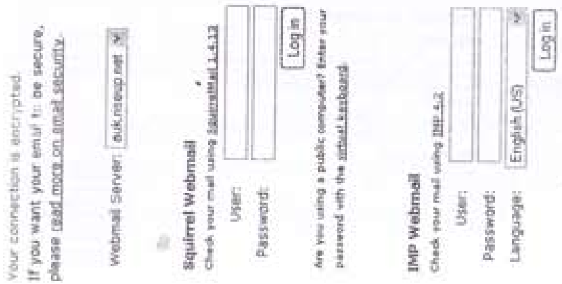
* 3.0 သင်၏ RiseUp Account အတွင်းသို့ ဝင်ရောက်ပုံ
* 3.1 Virtual Keyboard (အစစ်အမှန် မဟုတ်သော လက်ကွက်ခုံ)ကို အသုံးပြုပုံ

3.0 သင်၏ RiseUp Account အတွင်းသို့ ဝင်ရောက်ပုံ

သင်၏ RiseUp Account သို့ ဝင်ရောက်ရန် အောက်ပါအဆင့်များ ဆောင်ရွက်ပါ။

အဆင့် 1: https://mail.riseup.net/ မှတစ်ဆင့် SSL mode ဖြင့် RiseUp ၏ home page ကို ဖွင့်ပါ။

RiseUp ၏ မေးလ်စာမျက်နှာတွင် ဝင်ရောက်ခြင်းပြု log in အပိုင်းကို ဘယ်ဘက်တွင်လည်းကောင်း၊ News (သတင်း)ကို ညာဘက်တွင်လည်းကောင်း ခွဲခြားထားသည်။

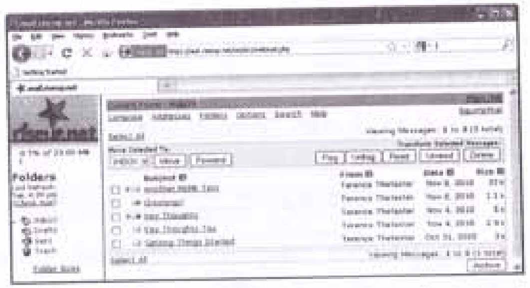


ပုံ 1: RiseUp ၏ မေးလ် ဝင်ရောက်မှုပြု စာမျက်နှာ

မှတ်ချက် ။ ။ ပေးထားသော web mail system နှစ်မျိုးလုံးကို အသုံးပြုနိုင် ပါသည်။ IMP Webmail က အင်္ဂလိပ်ဘာသာစကား အသုံးမပြုသော interfaces များ အတွက် ပို၍ သင့်လျော်ပါသည်။

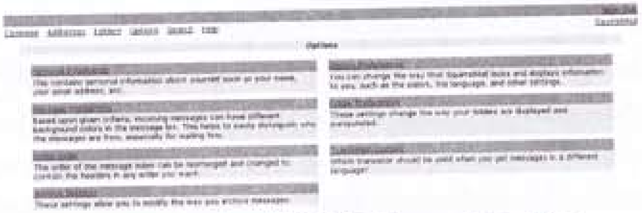
အဆင့် 2: Squirrel Webmail (သို့) IMP Webmail အပိုင်းများတွင် သက်ဆိုင်ရာ text fields ၌ အမည်နှင့် password များ ထည့်သွင်းပါ။ အမည်ကွက်လပ်တွင် '@ riseup.net အပိုင်းကို ထည့်သွင်းရန် မလိုပါ။ ဤအဆင့်ကို သင့် ဆန္ဒအရ လိုအပ်လျှင် လုပ်ဆောင်ပါ။ IMP Webmail ၏ drop-down list မှတစ်ဆင့် သင်အသုံးပြုလိုသော ဘာသာစကားကို ရွေးချယ်ပါ။

အဆင့် 3: သင်၏ account ကို ဖော်ပြရန် click လုပ်ပါ။



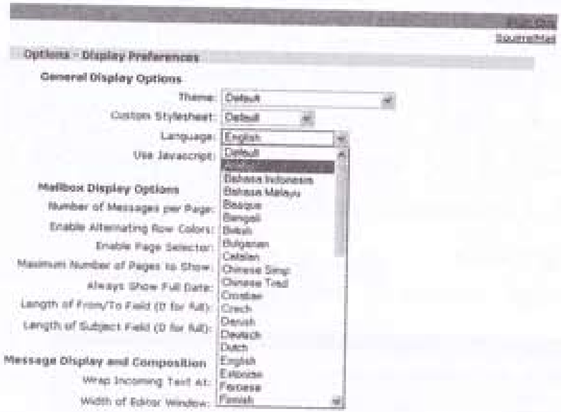
ပုံ 2: RiseUp Squirrel Webmail Account တစ်ခု၏ ဥပမာပြပုံ

သင့်စိတ်ကြိုက် ရွေးချယ်ပြုလုပ်နိုင်သောအဆင့် : သင်သည် လက်တင်စကားလုံး သတ်မှတ်ထားခြင်းမရှိသော အီးမေးလ်တစ်ခုကို ရေးသားခြင်းနှင့် လက်ခံရရှိခြင်းတို့ ဖြစ်ပါက Webmail account အတွက် ၎င်းကို ခွဲခြားပေးရမည်။ Squirrel Webmail ၏ opotions window သည် အောက်ပါအတိုင်း ပေါ်လာလိမ့်မည်။



ပုံ 3: Squirrel Mail Options pane ၏ ပုံ

အဆင့် 4: Options ကို လုပ်ဆောင်ရန် ရွေးပါ။ နှစ်သက်ရာ ရွေးချယ်နိုင်သော Display Preferences pane ကို အောက်ပါအတိုင်း တွေ့ရမည်။



ပုံ 4: Squirrel Mail Options - Display Preference pane ပုံ

အဆင့် 5: ဘာသာစကားရွေးချယ်မည့် drop-down menu ကို ပုံ 4: တွင် ဖော်ပြထားသည့်အတိုင်း နေရာချပါ။ ထို့နောက် သင်၏ အီးမေးလ် သတင်းပေးပို့မှုအတွက် သင့်လျော်သော character set ကို ရွေးချယ်ပါ။

ဤ option က သင်ပေးပို့သော (သို့) လက်ခံရရှိသော အီးမေးလ် သတင်းများကို မှန်ကန်သော encoding ဖြစ်အောင် ဆုံးဖြတ်ရာတွင် ကူညီပေးသည်။

3.1 Virtual Keyboard (အစစ်အမှန် မဟုတ်သော လက်ကွက်ခုံ)ကို အသုံးပြုပုံ

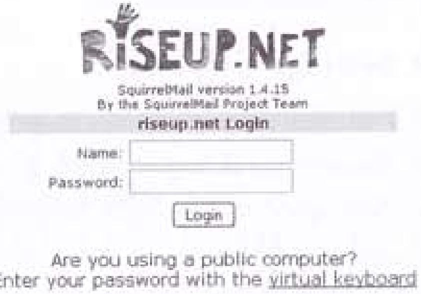
သင်၏ ကွန်ပျူတာကို လူထုအတွက် သတ်မှတ်ထားသော အနေအထားမျိုးမှာ အသုံးပြုနေပါက (ဥပမာ–အင်တာနက်ကဖေး၊ ဆက်သွယ်ရေးစင်တာ၊ စာကြည့်တိုက် စသဖြင့်) သင်၏ password ဝင်ရောက်ရာတွင် virtual keyboard ကို အသုံးပြုနိုင်ပါသည်။ ၎င်းက ပြင်ပမှ ဝင်ရောက်နိုင်သည့် key-logger programs များမှ သင်၏ system ကို ကာကွယ်ပေးမည့်အလွှာတစ်ခုကို လုပ်ဆောင်ပေးသည်။ Key-logger ပရိုဂရမ်ဆိုသည်မှာ အသုံးပြုသူက Keyboard ၏ ခလုတ်များမှတစ်ဆင့်

ရိုက်ထည့်လိုက်သော အမည်၊ password နှင့် အရေးကြီးသော အချက်အလက်များကို ၎င်း key ခလုတ်မှ မှန်းဆကြည့်ရှုရန် စီစဉ်ဖန်တီးထားသည့် ပရိုဂရမ် ဖြစ်သည်။ Virtual Keyboard က ဤလုံခြုံရေးဆိုင်ရာ အားနည်းချက်မှ ကာကွယ်ရန် အသုံးပြုသူများကို mouse မှတစ်ဆင့် ၎င်းတို့၏ password ဝင်ရောက်စေခြင်းဖြင့် ခွင့်ပြုထားသည်။

RiseUp Virtual Keyboard ကို အသုံးပြုရန် အောက်ပါအဆင့်များ ဆောင်ရွက်ပါ။

အဆင့် 1: https://mail.riseup.net/ မှတစ်ဆင့် SSL mode ဖြင့် RiseUp ၏ Home page ကို ဖွင့်ပါ။

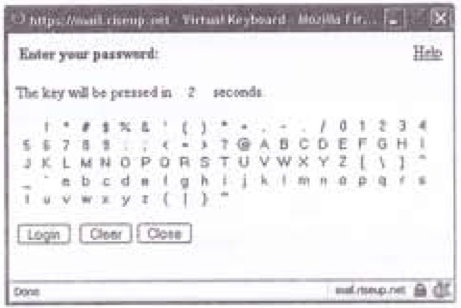
အဆင့် 2: အောက်ပါအတိုင်း RiseUp သို့ ဝင်ရောက်ရန် login စာမျက်နှာကို click လုပ်ပြီး သွားပါ။



ပုံ 5: RiseUp log in စာမျက်နှာ ပုံ

အဆင့် 3: Virtual Keyboard ကို ဆောင်ရွက်ရန် click လုပ်ပါ။

ပုံ 6: Virtual Keyboard ၏ ပုံ



အဆင့် 4: သင်၏ password ပြုလုပ်ရန် ပေးထားသော character ပေါ်မှ mouse pointer ကို 2 စက္ကန့်လောက် ထောက်ထားပါ။ (သို့) အလိုရှိရာ password ကို key ခလုတ်များပေါ်တွင် mouse ဖြင့် ထောက်၍ ထည့်သွင်းပါ။

အဆင့် 5: သင်၏ RiseUp account ကို access လုပ်ရန် click ပါ။

သင်၏ Account Settings ကို ပြောင်းလဲပုံ

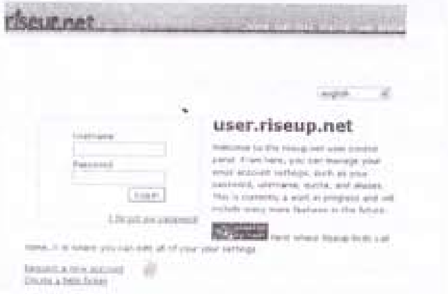
ဤစာမျက်နှာရှိ အပိုင်းကဏ္ဍများမှာ

* 4.0 သင်၏ Account Settings ကို ပြောင်းလဲပုံ
* 4.1 My Settings စာမျက်နှာ
* 4.2 Email Settings စာမျက်နှာ
* 4.3 ဖိတ်ကြားသည့် Invites စာမျက်နှာ

4.0 သင်၏ Account Settings ကို ပြောင်းလဲပုံ

RiseUp က သင်၏ account အတွက် settings အမျိုးမျိုးတို့ကို လုပ်ဆောင်ပေးသည်။ သင်သည် သင့် အီးမေးလ် box ၏ အရွယ်အစားကို ခွဲခြားသတ်မှတ်နိုင်သည်။ သင်၏ account အမည်၊ လိပ်စာများကို ပြောင်းလဲခြင်း၊ အမည်ပြောင်းများ (aliases) ထည့်သွင်းခြင်း စသဖြင့် လုပ်ဆောင်နိုင်သည်။ သင်၏ မိတ်ဆွေများ၊ အပေါင်းအဖော်များထံသို့ ၎င်းတို့၏ RiseUp ကိုယ်ပိုင် account များ ဖွင့်နိုင်ရန် codes များ ပေးပို့ ဖိတ်ကြားနိုင်သည်။

အဆင့် 1: https://user.riseup.net/ မှတစ်ဆင့် သင်၏ RiseUp Account Settings စာမျက်နှာသို့ သွားပါ။



ပုံ 1: user. riseup. net စာမျက်နှာ

အဆင့် 2: သက်ဆိုင်ရာ ကွက်လပ်အသီးသီး၌ သင်၏ အသုံးပြုသူအမည်နှင့် password တို့ကို ရိုက်ထည့်ပါ။

အဆင့် 3: အောက်ပါ screen သို့ click လုပ်ပြီး သွားပါ။

ပုံ 2: riseup.net ထိန်းချုပ်မှု ပေးနိုင်သည့် user control စာမျက်နှာ

4.1 My Settings စာမျက်နှာ

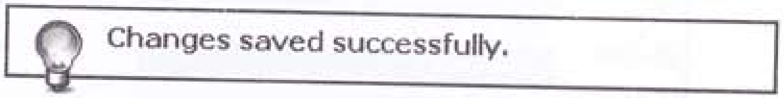
My Settings စာမျက်နှာတွင် သင်မူလ ဝင်ရောက်ခဲ့သည့် အခန်း 2.1 မှ 'account အချက်အလက်ပုံစံ' ရှိ သတင်းအချက်အလက်များ အားလုံးကို ဖော်ပြထားသည်။

အဆင့် 1: အောက်ပါ screen သို့ သွားရန် click လုပ်ပါ။

ပုံ 3: Settings စာမျက်နှာ

ဤ screen တွင် သင်၏ အသုံးပြုသူအမည်ကို ပြောင်းလဲနိုင်သည်။ ၎င်းက သင်၏ အီးမေးလ်လိပ်စာကိုပါ ပြောင်းပေးလိမ့် မည်။ အမည်သစ်သည်လည်း ညီညွတ်မှု (unique) ရှိရမည်။ ဤနေရာတွင် သင်၏ alternative အီးမေးလ်၊ password စသည့် account ၏ အသေးစိတ်အချက်များကိုလည်း ပြောင်းလဲနိုင်သည်။

အဆင့် 1: သင်၏ သတင်းအချက်အလက် အသစ်ကို ရိုက်ထည့်ပြီး ဤ အသ–ိပေး ချက်ကို ဖော်ပြရန် click လုပ်ပါ။



ပုံ 4: သင်၏ ပြောင်းလဲမှုများကို အောင်မြင်စွာ update လုပ်ပြီး ပုံ

4.2 အီးမေးလ် settings စာမျက်နှာ

အီးမေးလ် settings စာမျက်နှာက အီးမေးလ် သိုလှောင်မှုနှင့် ပတ်သက်သော သတင်းအချက်အလက်များကို ကြည့်ရန် (သို့) ပြင်ဆင်ရန် ခွင့်ပြုသည်။ RiseUp server တစ်ခုပေါ်ရှိ သင်၏ အီးမေးလ် account အတွက် သီးသန့်ထားရှိသော နေရာပမာဏ (သို့) သင်၏ ခွဲတမ်း (quota) ကိုလည်း သတ်မှတ်နိုင်သည်။

အဆင့် 1: အောက်ပါ screen ကို လုပ်ဆောင်ရန် click လုပ်ပါ။

ပုံ 5: အီးမေးလ် settings စာမျက်နှာ

အဆင့် 2: Quota (ခွဲတမ်း) ကွက်လပ်ထဲသို့ သင့်တော်သော အရေအတွက် ဂဏန်းကို ရိုက်ထည့်ပါ။

မှတ်ချက် ။ ။ သင်၏ account အရွယ်အစားကို 47 MB အထိသာ အများဆုံး

သတ်မှတ်ထားသည်။ ၎င်းသည် အရေးကြီးသော အီးမေးလ် ဆက်သွယ်မှုအတွက် လုံလောက်သော ပမာဏဖြစ်သည်ဟု ယူဆသည်။ သို့သော် သင်သည် အီးမေးလ်များကို များစွာသော ဂရပ်ဖစ်ရုပ်ပုံများ တွဲဖက်ပို့ဆောင်ခြင်း (သို့) လက်ခံရယူခြင်းတို့ ပုံမှန်ပြုလုပ်လိုပါက RiseUp သည် အကောင်းဆုံး ရွေးချယ်မှု မဖြစ်နိုင်ပါ။

ဤစာမျက်နှာတွင် သင်၏ အမည်ပြောင် (aliases) များကိုလည်း ဖန်တီးနိုင်သည်။ Alias ဆိုသည်မှာ သင်၏ account အတွက် nickname (အမည်ပြောင်) နှင့် အလားသဏ္ဍာန်တူသည်။

သင်၏ ပင်မ account သည် ယခင်ကကဲ့သို့ ဆက်လက်ရှိနေပါက သင်၏ အမည်ပြောင်ပေးထားသော လိပ်စာသို့လည်း အီးမေးလ် ပို့လွှတ်နိုင်သည်။

ပုံ 6: အီးမေးလ် Settings စာမျက်နှာရှိ အမည်ပြောင်ပေးခြင်း အပိုင်း

ဥပမာ ။ ။ ssayyed @ riseup.net account တွင် အမည်ပြောင် နှစ်ခုရှိသည်။ ၎င်း အမည်ပြောင်ဖြစ်သော safeandsecure @ riseup.net နှင့် salsaytest @ riseup.net လိပ်စာသို့ ပေးပို့သော အီးမေးလ်ကို သင်၏ ပင်မ account သို့ ထပ်မံပို့ပေးလိမ့်မည်။ ၎င်းသည် သင်၏ account လိပ်စာကို သီးခြားဖြစ်စေရန် အသုံးဝင်သော လုပ်ဆောင်မှု ဖြစ်စေသည်။

အဆင့် 4: သင်၏ အမည်ပြောင်အသစ်များကို click လုပ်ပြီး သိမ်း (save) ပါ။

4.3 ဖိတ်ကြားသည့် Invites စာမျက်နှာ

Invites စာမျက်နှာသည် RiseUp သို့ ဆက်သွယ်ရန် သင်၏ မိတ်ဆွေ အပေါင်းအဖော်များသို့ ဖိတ်ကြားရာတွင်အသုံးပြုသော codes နံပါတ်များ ထုတ်ပေးသည်။

အရေးကြီး ။ ။ Account အသစ်တစ်ခုစီတွင် အသုံးပြုသူနှစ်ဦးမှ ပို့လွှတ်သော invite code တစ်ခုစီ လိုအပ်သည်။ သင် အလိုရှိသလောက် invite code များများ ထုတ်ယူနိုင်သည်။

အဆင့် 1: အောက်ပါ screen သို့ click လုပ်ပြီး သွားပါ။

အဆင့် 2: ဖိတ်ကြားသည့် codes နံပါတ်ထုတ်ယူရန် click လုပ်ပါ။

ပုံ 7: ဖိတ်ကြားသည့် Invites **စာမျက်နှာ**

မှတ်ချက် ။ ။ code တစ်ခုကို တစ်လသာ အသုံးပြုရန် ခွင့်ပြုသည်။

Code	Expires on
ocozuwel	Dec 31 2010
leimeila	Dec 31 2010

Print invites | Create a new invite code

ပုံ 8: **ထုတ်ပေးထားသော ဖိတ်ကြားသည့်** codes **နံပါတ်များပြဥပမာတစ်ခု**

အဆင့် 3: ဖိတ်ကြားသည့် invite codes များကို print ထုတ်ပြီး RiseUp အီးမေးလ် account တစ်ခု ပြုလုပ်လိုသောသူထံသို့ ပေးပါ။

5.0 မကြာခဏ မေးလေ့ရှိသော မေးခွန်းများနှင့် အဖြေများ

မှုဟင်ဒိုနှင့် ဆယ်လီမတို့သည် RiseUp ၏ လွယ်ကူစွာ အသုံးပြုနိုင်ပုံကို များစွာကျေနပ်ကြပြီး ၎င်း၏ တိုးတက်သော လူမှုရေးဆိုင်ရာ တန်ဖိုးများအတွက် ကတိကဝတ်ပြုမှုများကို များစွာအထင်ကြီးကြသည်။ သို့သော် နောက်ဆက်တွဲ မေးရန် မေးခွန်းအချို့ ကျန်ရှိနေသေးသည်။ ကံကောင်းသည့်မှာ ၎င်းတို့၏ ဖခင် အာဆင်နီမှ ၎င်းတို့ သိလိုသောအဖြေများကို ဖြေကြားပေးနိုင်သည်။

မေး ။ ။ ဘယ်လို အခြေအနေမျိုးမှာ Squirrelmail အစား IMP webmail ကို အသုံးပြုသင့်သလဲ။

ဖြေ ။ ။ ဒါ မေးခွန်းကောင်း တစ်ခုပါပဲ။ အခြေခံအားဖြင့်တော့ ခြားနားချက် ဘာမှ မရှိပါဘူး။ အကြောင်းအရာ အချို့ကတော့ အီးမေးလ် ဝန်ဆောင်မှုတစ်ခု down သွားတာမျိုး၊ ပုံမှန် ပြုလုပ်နေကြ ပြင်ဆင်ခြင်း ပြုလုပ်တဲ့အခါမျိုးမှာ တစ်ခြား တစ်ခုကို အနှောက်အယှက်မရှိဘဲ ဆက်လက် လုပ်ဆောင်နိုင်ပါတယ်။ IMP webmail ဝန်ဆောင်မှုကတော့ အင်္ဂလိပ်စာမဟုတ်ဘဲ အခြား ဘာသာစကားများ လုပ်ဆောင်ရာမှာ ပိုပြီး အထောက်အကူ ရပါတယ်။

မေး ။ ။ ကျွန်တော်ရဲ့ account ကို ဖန်တီးနေတဲ့ အချိန်မှာ ကျွန်တော် စဉ်းစားမိတာက တကယ်တမ်း ကျွန်တော်ရဲ့ သတင်းအချက်အလက်တွေကို ထုတ်ပေးဖို့ မလိုအပ်ဘူးလို့ ထင်တာပါပဲ။

ဖြေ ။ ။ အမှန်တကယ်လည်း မင်း အဲဒီလို လုပ်စရာမလိုပါဘူး။ မင်းရဲ့ password ကိုသာ 3 လ (သို့) 6 လ တစ်ခါလောက် ပြောင်းပေးဖို့ မမေ့ပါနဲ့။

မေး ။ ။ မှုဟင်ဒိုနှင့် ကျွန်မမှာ RiseUp account တစ်ခုစီ ရှိပါတယ်။ အာဆင်နီရှင့်အတွက် တစ်ခုကို ကျွန်မတို့ ဘယ်လို မှတ်ပုံတင်ပေးရမှာလဲ။

ဖြေ ။ ။ မင်းတို့ နှစ်ယောက်စလုံးက invite code တစ်ခုစီ ထုတ်ပေးပြီး ငါ့ဆီကို ပို့ပေးပါ။ ငါ့ရဲ့ RiseUp account ကို ပြုလုပ်ပြီး မှတ်ပုံတင်တဲ့အခါမှာ မင်းတို့ရဲ့ invite codes တွေကို အသုံးပြုရမှာ ဖြစ်ပါတယ်။

မှတ်ချက် ။ ။ RiseUp ကို စေတနာ့ဝန်ထမ်းကူညီသူများရဲ့ ကြိုးစားလုပ်ဆောင်မှု၊

စေတနာထက်သန်မှုနဲ့ အလှူငွေများအပေါ် မှီခိုပြီး တည်ထောင်ထားသည့်အတွက်ကြောင့် စီးပွားရေးဆိုင်ရာ အီးမေးလ်ဝန်ဆောင်မှု ပြုသူများနဲ့ ယှဉ်ပြိုင်ခြင်းဟာ စိန်ခေါ်ချက်တစ်ရပ်ပဲ ဖြစ်ပါတယ်။ ဒါပေမဲ့ အခု RiseUp ကို Facebook ပေါ်မှာ 'Crabgrass' အမည်နဲ့ လွတ်လပ်ပြီးပွင့်လင်းတဲ့ အရင်းအမြစ်တစ်ခုအဖြစ် အသုံးချနိုင်အောင် တင်ထားပါတယ်။ ၎င်းက အဆင့်မြှင့်ထားတဲ့ မှုပိုင်နှင့် လုံခြုံရေးဆိုင်ရာကဏ္ဍများကို ဝေမျှပေးပါတယ်။ ရည်ရွယ်ချက်ကတော့ လူမှုရေးဆိုင်ရာ ဝန်ဆောင်မှုပေးတဲ့ အဖွဲ့အစည်းများ၊ အစိုးရမဟုတ်သော အဖွဲ့အစည်းများနဲ့ ပတ်ဝန်းကျင် စိမ်းလန်းရေး ဆောင်ရွက်တဲ့ အဖွဲ့အစည်းများမှ အသုံးချနိုင်ဖို့ပါပဲ။ ရည်ရွယ်ချက်ရှိရှိ၊ တာဝန်သိသိ၊ စွမ်းအင်ရှိရှိဖြင့် RiseUp က အောက်ပါ ယှဉ်ပြိုင်ရွေးချယ်စရာများကို ထုတ်လုပ်ပေးလိုက်ပြီး မဝေးတဲ့ အနာဂတ်မှာလည်း RiseUp ကို တော်လှန်တဲ့ အီးမေးလ်ဝန်ဆောင်မှုအသွင်နဲ့ တွေ့ရမှာပါ။

* Collaborative Document Editing (etherpad): ဤဝန်ဆောင်မှုက အသုံးပြုသူ အများစုကို တစ်ချိန်တည်းမှာ မှတ်တမ်းတစ်ခု (document)ကို တည်းဖြတ်ဖို့ ခွင့်ပြုပါတယ်။
* Encrypted Internet Proxy (openvpn): ဤဝန်ဆောင်မှုက သင်၏ အင်တာနက်ကို ဆွဲယူကြည့်ရှုရန် အသွင်ပြောင်းထားသော ကွန်ရက်နှင့် အင်တာနက်အကြား ဆက်သွယ်ပေးသော server (Internet proxy server) ကို အသုံးပြုခွင့်ပေးသည်။ ၎င်းသည် 'Tor' နှင့် အလားသဏ္ဌာန်တူသည်။
* Real-Time Chat (XMPP): ဤဝန်ဆောင်မှုက သင့်အား အချိန်နှင့်အညီ chatting လုပ်ရန် ခွင့်ပြုပြီး ၎င်းမှာ Gmail chat နှင့် Microsoft Instant Messaging နှင့် အတူတူပင်ဖြစ်သည်။

5.1 မေးခွန်းသုံးသပ်ချက်များ

* သင်၏ အီးမေးလ်ကို webmail ကတစ်ဆင့် ဖတ်တာနဲ့ အီးမေးလ် ပရိုဂရမ်တစ်ခုကနေ ဖတ်တာ ဘာကွာခြားပါသလဲ။
* Secure Socket Layer (SSL) ဆိုတာ ဘာလဲ။ အဲဒါက ဘယ်လို အလုပ်လုပ်တာလဲ။
* Virtual keyboard ဆိုတာ ဘာလဲ။ အဲဒါက ဘယ်လို အလုပ်လုပ်တာလဲ။

* သင့်ရဲ့ အီးမေးလ် account မှာ အမည်ပြောင်(alias) ကို ဘယ်လို ထည့်ရမလဲ။
* အသစ်ပြုလုပ်လိုက်တဲ့ ဖိတ်ကြားတဲ့ invite code ဟာ အချိန် ဘယ်လောက်ကြာကြာခံမှာလဲ။

Thunderbird - လုံခြုံစိတ်ချရသော အီးမေးလ်သုံးစွဲမှုစနစ်

Mozilla Thunder bird သည် အီးမေးလ်များ ပို့ဆောင်ခြင်း၊ လက်ခံခြင်းနှင့် သိမ်းဆည်းခြင်းများအတွက် အခမဲ့ဖြစ်ပြီး လွတ်လပ်ပွင့်လင်းသော အသုံးချ ပရိုဂရမ် တစ်ခုဖြစ်သည်။ ပရိုဂရမ်တစ်ခုမှ အီးမေးလ် account များစွာကို သင် ဖန်တီးနိုင်သည်။ သင့် အီးမေးလ် ဆက်သွယ်ချက်များ၏ မူပိုင်ခွင့်နှင့် လုံခြုံရေးတို့ကို သေချာမှုရှိစေရန် Enigmail နှင့် GnuPG တို့မှ authentication (User ၏ log in information ကို စစ်ဆေးပေးသော လုပ်ငန်းစဉ်)၊ digital signing (electronic နည်း ပညာအရ ပေးပို့သောသတင်း (သို့) စာတမ်းတစ်ခုကို ပေးပို့သူမည်သူမည်ဝါဖြစ်ကြောင်း ဖော်ပြသည့် ဖြစ်စဉ်) နှင့် encryption (ဝှက်စာအသွင်ပြောင်းခြင်း) တို့ကို access လုပ်ရန် သင့်အား ခွင့်ပြုသည်။

Thunderbird, Enigmail နှင့် GnuPG တို့အား download လုပ်ပုံ

* လက်စွဲလမ်းညွှန်ပါ မိတ်ဆက်အချက်အလက်များကို ဖတ်ပါ။
* www.mozilla.com/thunderbird web စာမျက်နှာကို ဖွင့်ရန် အောက်ရှိ Thunderbird icon ကို နှိပ်ပါ။
* အခမဲ့ download ရယူမည့် link ဆက်သွယ်ချက်ကို click လုပ်ပြီး install လုပ်မည့်ဖိုင်ကို သိမ်း (save) ပါ။ ၎င်းအား နေရာချပါ။ ထို့နောက် download click နှိပ်ပါ။

* www.enigmail.mozdev.org/download ကို ဖွင့်ရန် အောက်ရှိ Enigmail icon ကို click လုပ်ပါ။
* Thunderbird 3.1 link အတွက် v 1.1.2 ကို ရယူရန် download ခလုတ်ကို rightclick နှိပ်ပါ။ ၎င်း၏ add-on software ကို သင်၏ desktop ပေါ်မှာ သိမ်း (save) ပါ။
* www.gnupg.org/download စာမျက်နှာကို ဖွင့်ရန် အောက်ရှိ GnuPG icon ကို click လုပ်ပါ။
* Mouse နှင့် ဆွဲချပြီး Binaries section ကို သွားပါ။ Microsoft Windows FTP အတွက် စုစည်းထားတဲ့ GnuPG 1.4 ကို click လုပ်ပါ။ Install ပြုလုပ်မယ့် ဖိုင်ကို သိမ်း (save) ပါ။
* Thunderbird အတွက် လမ်းညွှန်မှာပါတဲ့ အခန်း 4.1 ကို Enigmail နှင့် GnuPG တို့ install လုပ်ဖို့အတွက် ဆက်သွားပါ။

  သင့်ရဲ့ installation လုပ်ငန်းစဉ် ပြီးဆုံးချိန်မှာ သင့်ကွန်ပျူတာမှာ သင် သိမ်းခဲ့တဲ့ installers တွေနဲ့ add-ons software တွေကို ဖျက်ပစ်နိုင်ပါတယ်။

* Thunderbird၊ Enigmail နဲ့ GnuPG တို့အတွက် home page များကတော့ www.mozilla.com/thunderbird ၊ www.enigmail. mozdev.org နဲ့ www.gnupg.org တို့ပဲ ဖြစ်ကြပါတယ်။

ကွန်ပျူတာ လိုအပ်ချက်တွေကတော့ Windows Version အားလုံးနဲ့ တွဲပြီး သုံးနိုင်ပါတယ်။

ဒီလမ်းညွှန်မှာသုံးထားတဲ့ version တွေကတော့

* Thunderbird 3.1.5
* Enigmail 1.1.2
* GNU Privacy Guard (Gnu PG) 2.0.4 တို့ ဖြစ်ကြပါတယ်။

အဆင့် 1: လိုင်စင်ခွင့်ပြုမှုက အခမဲ့ဖြစ်ပြီး ပွင့်လင်းတဲ့ အရင်းအမြစ် အခြေခံတဲ့ ဆော့ဖ်ဝဲဖြစ်ပါတယ်။

အဆင့် 2: ဖတ်ရမယ့် အကြောင်းအရာကတော့ အခန်း 7 မှာပါတဲ့ 'သင့်ရဲ့ အင်တာနက် ဆက်သွယ်မှုကို သီးခြားထားရှိခြင်း' ခေါင်းစဉ်ပဲ ဖြစ်ပါတယ်။

အဆင့် 3: အဆင့်သတ်မှတ်ချက်များကတော့ Level: 1: Beginner, 2: Average, 3: Inter mediate, 4: Experienced, 5: Advanced တို့ ဖြစ်ကြပါတယ်။
အဆင့် 4: ဒီပရိုဂရမ်ကို စတင်အသုံးပြုဖို့ ကြာတဲ့အချိန်ကတော့ မိနစ် 40 ဖြစ်ပါတယ်။

သင်ရရှိမယ့် အကျိုးကျေးဇူးတွေကတော့ . . . .

* ပရိုဂရမ်တစ်ခုထဲကနေပြီး အီးမေးလ် account အမျိုးမျိုးတို့ကို စီစဉ်ဆောင်ရွက်နိုင်ခြင်း
* အင်တာနက်မှ ဆက်သွယ်မှု ရပ်စဲပြီးနောက် သတင်းပေးပို့ချက်တွေကို ဖတ်ရှုခြင်း၊ ရေးသားခြင်းတို့ ဆောင်ရွက်နိုင်ခြင်း
* သင့်ရဲ့ အီးမေးလ်ကို သီးခြားလျှို့ဝှက်ထားဖို့ အများဆိုင်လုံခြုံရေး key များကိုသုံး၍ encryption ပြုလုပ်ခြင်းတွေပဲ ဖြစ်ပါတယ်။

GNU Linux, Mac OS နဲ့ အခြား Microsoft Windows တို့အတွက် တွဲဖက်လုပ်ဆောင်နိုင်တဲ့ ပရိုဂရမ်များ

GNU Linux၊ Mac OS၊ Microsoft Windows နဲ့ တစ်ခြား OS များ အတွက် Mozilla ရဲ့ 'Thunderbird- အီးမေးလ်သုံးစွဲမှု'ကို ရရှိနိုင်ပါတယ်။ အီးမေးလ်အကောင့်များစွာကို စီစဉ်ဆောင်ရွက်ခြင်းဟာ ဒစ်ဂျစ်တယ် လုံခြုံရေး အမြင်အရကြည့်ရင် အင်မတန် ရှုပ်ထွေးတဲ့ တာဝန်တစ်ရပ်ပါ။ ဒါကြောင့် ဒီရည်ရွယ်ချက်နဲ့ သုံးမယ်ဆိုရင် Mozilla ရဲ့ Thunderbird ကို အသုံးပြုဖို့ ကျွန်ုပ်တို့က လမ်းညွှန်လိုပါတယ်။ အခြေခံနည်းပညာရပ်တွေနဲ့ ပြုလုပ်ထားပြီး အခမဲ့နဲ့ ပွင့်လင်းတဲ့ ရင်းမြစ်များရှိတဲ့ ပရိုဂရမ်ဖြစ်တဲ့ Thunderbird မှာ ရရှိနိုင်တဲ့ လုံခြုံရေးဆိုင်ရာ အကျိုးတရားများဟာ Microsoft Outlook ကဲ့သို့ စီးပွားရေးဆိုင်ရာ ညီမျှချက်တွေရှိတဲ့ ပရိုဂရမ်တွေနဲ့ နှိုင်းယှဉ်ကြည့်ရင် ပိုပြီး အရေးကြီးပါတယ်။

ဒါပေမဲ့ သင့်အနေနဲ့ Mozilla Thunderbird မဟုတ်တဲ့ တခြား ပရိုဂရမ် တစ်ခုခုကို အသုံးပြုချင်တယ်ဆိုရင်တော့ အောက်မှာပါရှိတဲ့ အခမဲ့နဲ့ ပွင့်လင်းတဲ့ ရင်းမြစ်တွေ ရရှိနိုင်တဲ့ ရွေးချယ်စရာပရိုဂရမ်များကို ညွှန်းလိုပါတယ်။

* GNU Linux နဲ့ Microsoft Windows တို့အတွက် Claws Mail၊
* GNU Linux၊ Mac OS နဲ့ Microsoft Windows များအတွက် Sylpheed

* နောက်ထပ် GNU Linux၊ Mac OS နဲ့ Microsoft Windows တို့အတွက် Alpine တို့ဖြစ်ကြပါတယ်။

1.1 ဤပရိုဂရမ်ကို သင်စတင် အသုံးမပြုမီ သိသင့်သောအရာများ

Mozilla Thunderbird ကို အထောက်အကူပြု နည်းပညာအခြေခံ ပြုလုပ်ထားပြီး အခမဲ့နဲ့ ပွင့်လင်းတဲ့ ရင်းမြစ်များ ရရှိနိုင်တဲ့ အီးမေးလ်သုံးစွဲမှုစနစ် ဖြစ်ပါတယ်။ ၎င်းက အီးမေးလ် ပို့လွှတ်ခြင်း၊ လက်ခံခြင်းနဲ့ သိမ်းဆည်းခြင်းများ လုပ်ဆောင်ပေးပါတယ်။ အီးမေးလ် သုံးစွဲမှုစနစ်ဆိုတာဟာ ကွန်ပျူတာရဲ့ application တစ်ခုဖြစ်ပြီး ၎င်းက အင်တာနက် ကွန်ရက်ရှာဖွေစက် (web browser) မပါဘဲ သင့်ရဲ့ အီးမေးလ် သတင်းပေးပို့ချက်တွေကို စီစဉ်ဆောင်ရွက်ခွင့်နဲ့ download လုပ်ယူခွင့်တို့ ပေးပါတယ်။ ပရိုဂရမ်တစ်ခုတည်းကိုပဲ အသုံးပြုပြီး အီးမေးလ်အကောင့်များစွာကို စီမံဆောင်ရွက်နိုင်ပါတယ်။ Thunderbird ကို အသုံးမပြုခင် သင့်မှာ အီးမေးလ်အကောင့်တစ်ခု ရှိပြီးသားဖြစ်ရပါမယ်။ သင်ဆန္ဒရှိရင် Gmail (သို့) RiseUp အီးမေးလ်အကောင့်များ ကိုလည်း ဖွင့်ထားနိုင်ပါတယ်။

Enigmail ဟာ Thunderbird မှာ ထပ်ပေါင်း ဖြည့်စွက်ထားတဲ့ ပရိုဂရမ်ဖြစ်ပါတယ်။ ၎င်းက GNU Privacy Guard (GnuPG) က ထုတ်ပေးတဲ့ လက္ခဏာနှစ်ရပ်ဖြစ်တဲ့ authentication (အစစ်အမှန် ဟုတ်၊ မဟုတ် စစ်ဆေးခြင်း)နဲ့ encryption (ဝှက်စာ အသွင်ပြောင်းခြင်း)တို့ကို access လုပ်ရန် အသုံးပြုသူများကို ခွင့်ပြုပါတယ်။

GnuPG ဟာ အများဆိုင် key များကို ဝှက်စာအသွင်ပြောင်းပေးတဲ့ ပရိုဂရမ်တစ်ခုဖြစ်ပြီး သင့်ရဲ့ အီးမေးလ်ဆက်သွယ်ချက်တွေ သီးသန့်လုံခြုံမှုရရှိစေဖို့နဲ့ သတင်းပေးပို့ချက်တွေကို ဝှက်စာအသွင်ပြောင်းခြင်း (encryption) နဲ့ ဝှက်စာဖြည်ခြင်း (decryption) တို့မှာ အသုံးပြုနိုင်တဲ့ key အစုံများကို ထုတ်လုပ်စီစဉ်ပေးပါတယ်။ Enigmail အလုပ်လုပ်ဖို့ GnuPG ကို install လုပ်ထားရပါမယ်။ ဒီအကြောင်းကို ယခုအခန်းရဲ့ နောက်ပိုင်းမှာ ဖော်ပြထားပါတယ်။

* Thunderbird ကို install ပြုလုပ်ပုံ
* Thunderbird ၌ လုံခြုံရေးဆိုင်ရာ Settings များကို ပြင်ဆင်ဆောင်ရွက်ပုံ
* Thunderbird ၌ GnuPG ကို Enigmail နှင့် တွဲဖက်အသုံးပြုပုံ
* မကြာခဏ မေးလေ့ရှိသော မေးခွန်းများနှင့် သုံးသပ်ချက်

Thunderbird ကို install ပြုလုပ်ပုံ

ဤစာမျက်နှာရှိ အပိုင်းကဏ္ဍများမှာ

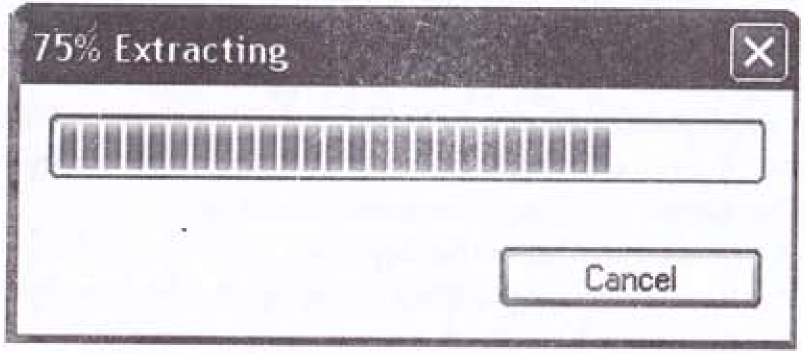
* 2.0 Thunderbird ကို install ပြုလုပ်ပုံ
* 2.1 ကမ္ဘာလုံးဆိုင်ရာရှာဖွေမှု (Global Search) နှင့် အညွှန်းပြသူ (Indexer) option များကို Thunderbird ၌ disable ပြုလုပ်ပုံ
* 2.2 Thunderbird ၌ အီးမေးလ်အကောင့် တစ်ခုကို မှတ်ပုံတင်ခြင်းပြုလုပ်ပုံ
* 2.3 Thunderbird ၌ Blogs၊ News Feeds နှင့် Newsgroup အကောင့်များကို မှတ်ပုံတင်ခြင်း ပြုလုပ်ပုံ

2.0 Thunderbird ကို install ပြုလုပ်ပုံ

Thunderbird ကို install ပြုလုပ်ခြင်းသည် မြန်ဆန်ပြီး တစ်ဆက်တည်း လုပ်ဆောင်နိုင်သည့် လုပ်ငန်းစဉ်ဖြစ်သည်။ Thunderbird ကို စတင် install လုပ်ရန် အောက်ပါအဆင့်များကို ဆောင်ရွက်ပါ။

အဆင့် 1: Double click လုပ်ပြီး ဖိုင်ကိုဖွင့်ပါ။ လုံခြုံရေးအချက်ပေး dialog box ပေါ်လာလိမ့်မည်။ အောက်ပါ screen သို့ click လုပ်ပြီး သွားပါ။

Thunderbird ဖိုင်များအားလုံး ဖြည်ပြီးသောအခါ 'Welcome to the Mozilla Thunderbird Setup Wizard' window ပေါ်လာလိမ့်မည်။



ပုံ 1: Install ဖိုင်ကို ဖြည်ချ (extract) သည့် အခြေအနေပြ bar ပုံ

အဆင့် 2: Mozilla Thunderbird ၏ setup အမျိုးအစားပြ Setup type window ကို click လုပ်ပြီး ဆောင်ရွက်ပါ။

အဆင့် 3: ပေးထားသော default settings ကိုလက်ခံပြီး အောက်ပါ screen သို့ သွားရန် click လုပ်ပါ။

ပုံ 2: Mozilla Thunderbird - Summary screen ပုံ

အဆင့် 4: Installation လုပ်ငန်းစဉ် စတင်ရန် click လုပ်ပါ။ Install လုပ်နေသည့် အခြေအနေပြသည့် Windows ပေါ်လာလိမ့်မည်။ Installation လုပ်ငန်းစဉ် ပြီးဆုံးပါက အောက်ပါ screen ပေါ်လာလိမ့်မည်။

ပုံ 3: 'Mozilla Thunderbird Setup Wizard' ပြီးဆုံးကြောင်းပြသည့် screen

အဆင့် 5: Installation လုပ်ငန်းစဉ် အဆုံးသတ်ရန် click လုပ်ပါ။

သတိပြုရန် ။ ။ 'Launch Mozilla Thunderbird now' check box ကို check လုပ်ခဲ့မည်ဆိုပါက Thunderbird သည် အလိုအလျောက် စတင်လုပ်ဆောင်လိမ့်မည်။ ၎င်းကို ပုံ 3 မှာ ပြထားသည်။ နောက်ပိုင်းတွင် ၎င်းပရိုဂရမ်ကို ဖွင့်လိုပါက desk-top ပေါ်ရှိ Thunderbird icon ကို double click လုပ်ပါ။ (သို့) Start>Programs>

Mozilla Thunderbird> Mozilla Thunderbird ကို ရွေးပါ။

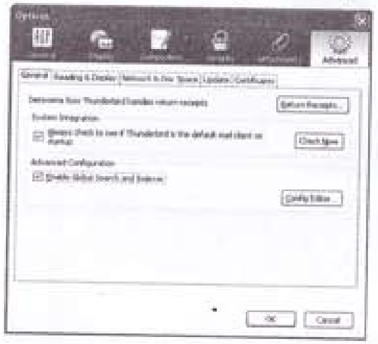
2.1 ကမ္ဘာလုံးဆိုင်ရာရှာဖွေမှု (Global Search) နှင့် (Indexer) အညွှန်းပြုသူ option များကို Thunderbir ၌ disable ပြုလုပ်ပုံ

သတိပေးချက် ။ ။ Thunderbird ရှိ Global Search နှင့် Indexer လက္ခဏာရပ်နှစ်ခုကို ပိုမိုကောင်းမွန်သော လုပ်ဆောင်မှု ရရှိစေရန် ပိတ်ထားရမည်။ သင့် အီးမေးလ်များ၏ အရွယ်အစားနှင့် အရေအတွက် ပေါ်မူတည်ပြီး သင့် system ၏ အမြန်နှုန်းကို လျော့ကျစေသည်။ ၎င်းတို့က သင်၏ hard drive ပေါ်၌ သတင်းအချက်အလက်များကို မလိုအပ်ဘဲ အဆက်မပြတ် over-write လုပ်ခြင်း ဖြစ်ပွားစေသည်။ သင်၏ hard drive ပို၍ ပြည့်လာသောအခါ အခြားမသက်ဆိုင်သော system ၏ လုပ်ဆောင်ချက်များကိုပါ အရှိန်လျော့နည်းစေသည်။

Global Search နှင့် Indexer option များကို ပိတ်ရန် အောက်ပါအဆင့်များ ဆောင်ရွက်ပါ။

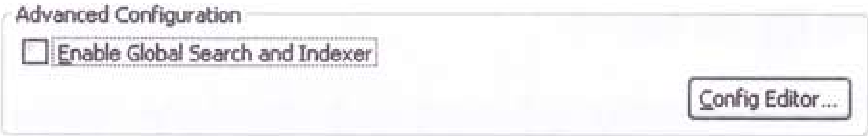
အဆင့် 1: Options window ကို လုပ်ဆောင်ရန် Thunderbird console ရှိ Tools မှတစ်ဆင့် Options ကို ရွေးပါ။

အဆင့် 2: အောက်ပါအတိုင်း ၎င်းနှင့် တွဲလျက်ပါရှိသော ခလုတ် (tab) ကို လုပ်ဆောင်ရန် click နှိပ်ပါ။



ပုံ 4: Advanced tab ကို ပြထားသော Options window ပုံ

အဆင့် 3: 'Enable Global Search and Indexer' စာတန်းပါ check box ကို click နှိပ်ခြင်းဖြင့် ၎င်း option ကို disable လုပ်ပါ။ အောက်ပါအတိုင်း တွေ့ရမည်။



ပုံ 5: Advanced Configuration section ပုံ

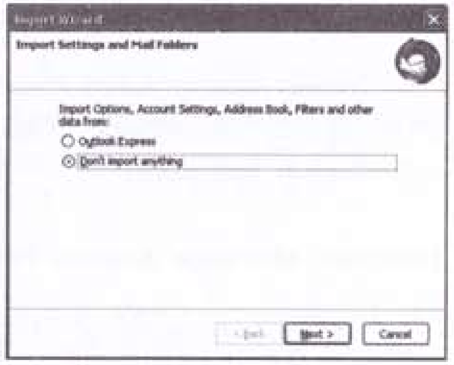
ယခုသင်သည် ဤ option ကို အောင်မြင်စွာ ပိတ်ပြီးပါပြီ။ Thunderbird၌ အီးမေးလ်အကောင့်တစ်ခုကို မှတ်ပုံတင်ခြင်း ပြုလုပ်ရန် အဆင်သင့် ဖြစ်ပါပြီ။

2.2 Thunderbird ၌ အီးမေးလ်အကောင့် တစ်ခုကို မှတ်ပုံတင်ခြင်း ပြုလုပ်ပုံ

Import Wizard- Settings နှင့် Mail Folders များကို Import လုပ်ရန်ပြသည့် Window သည် ပထမအကြိမ် သင် Thunderbird ကို install လုပ်သည့်အခါ၌သာ ပေါ်လာလိမ့်မည်။

အဆင့် 1: 'Don't import anything' option ကို check မလုပ်ပါနှင့်။ ထိုမှသာ အောက်ပါ screen ပေါ်လာလိမ့်မည်။

ပုံ 6: Import Wizard- Import Settings and Mail Folders

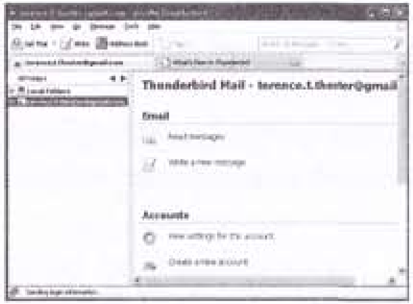


အဆင့် 2: အောက်ပါ screen သို့ click လုပ်ပြီး သွားပါ။

ပုံ 7: မေးလ်အကောင့်ပြုလုပ်ခြင်းပြ window

အဆင့် 3: သက်ဆိုင်ရာ ကွက်လပ်များ၌ အမည်၊ အီးမေးလ်လိပ်စာ၊ password များ ရိုက်ထည့်ပါ။ 'Remember my password' option ကို ဝိတ်ရန် check box ကို click လုပ်ပါ။ အထက်ပါ ပုံ 7 အတိုင်း တွေ့ရမည်။

အဆင့် 4: အောက်ပါ screen ကို လုပ်ဆောင်ရန် click လုပ်ပါ။



ပုံ 8: 'Access Folders and messages from multiple computer' option ကို ဖွင့်ထားသော IMAP နှင့်အတူ တွေ့ရသော မေးလ်အကောင့်ပြုလုပ်ခြင်းပြ windowပုံ

IMAP နှင့် POP : ရှင်းလင်းချက်များနှင့် အသုံးပြုပုံ

Internet Message Access Protocol (IMAP) နှင့် Post Office Protocol (POP) တို့သည် အီးမေးလ်များ သိမ်းဆည်းရန်နှင့် လက်ခံရန် အသုံးပြုသော နည်းလမ်းနှစ်မျိုး ဖြစ်ကြသည်။

Internet Message Access Protocol (IMAP)

IMAP ကို အသုံးပြုချိန်တွင် သင်၏ folder အားလုံး (Inbox၊ Drafts၊ Templates၊ Sent၊ Trash နှင့် အခြား folder များ အပါအဝင်)ကို အီးမေးလ်ဆာဗာပေါ်၌ တင်ထားသည်။ ထို့ကြောင့် ဤ folder များကို အခြား ကွန်ပျူတာတစ်လုံးမှ သင် access လုပ်နိုင်သည်။ အစပိုင်းတွင် သတင်းပေးပို့ချက်များ (messages) အားလုံးကို ဆာဗာပေါ်၌ထားပြီး အီးမေးလ်သတင်းများ၏ ခေါင်းစဉ်များသာ (အချိန်၊ ရက်စွဲ၊ အကြောင်းအရာ၊ ပို့သူအမည် စသည်တို့ ပါဝင်သည်) သင်၏ ကွန်ပျူတာ၌ ပြသရန် download လုပ်ယူထားသည်။ သတင်းအပြည့်အစုံကို သင်ဖွင့်ကြည့်မှသာ download လုပ်ယူသည်။ အင်တာနက် ဆက်သွယ်ချက်မရှိဘဲ ၎င်းတို့နှင့်အတူ အလုပ်လုပ် ဆောင်ရန် သင့်ကွန်ပျူတာရှိ folder အားလုံး (သို့) အချို့တို့မှ သတင်းပေးပို့သော

စာတိုများကို ကူးယူသိမ်းဆည်းရန် Tunderbird ကို ပြင်ဆင်ထားနိုင်သည်။ IMAP သင်သည် အီးမေးလ် (သို့) folder များကို ဖျက်သည့်အခါ သင်၏ ကွန်ပျူတာနှင့် ဆာဗာနှစ်ခုစလုံးပေါ်၌ ၎င်းကို လုပ်ဆောင်ရမည်။

Post Office Protocol (POP)

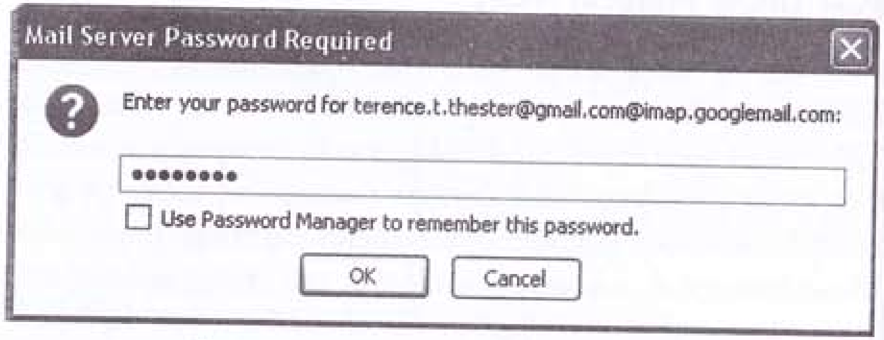
POP ကို အသုံးပြုရာတွင် Inbox folder ကိုသာ (အသစ်ရောက်လာသော သတင်းပေးပို့ချက်များ ဝင်ရောက်သည့် folder တစ်ခု) ဆာဗာ၌ တင်ထားသည်။ အခြား folder များအားလုံးကို သင်၏ ကွန်ပျူတာပေါ်၌ ထားရှိသည်။ ဆာဗာပေါ်ရှိ Inbox folder မှ ကျန်ရှိသော သတင်းပို့ချက်များ (messages) ကို သင်၏ ကွန်ပျူတာပေါ်သို့ download ရယူရွေးချယ်နိုင်သလို ဆာဗာပေါ်မှာပင်ဖျက်ပစ်နိုင်ပါသည်။ သင်၏ အီးမေးလ်အကောင့်ကို အခြားကွန်ပျူတာတစ်လုံးမှ သင် access လုပ်သည့်အခါ Inbox folder အတွင်းရှိ သတင်းပို့ချက်များ (သတင်းအသစ်များ၊ သင် မဖျက်ရသေးသော သတင်းအဟောင်းများ)ကိုသာ ကြည့်ရှုနိုင်မည်ဖြစ်သည်။

အဆင့် 5: သင်၏ အကောင့်ကို ပြုလုပ်ပါ။ ဖော်ပြပါပုံအတိုင်း ဘယ်ဘက်ခြမ်းရှိ 'All Folders' sidebar တွင် ပြထားသော အီးမေးလ်အကောင့်နှင့် Thunderbird console ကို လုပ်ဆောင်ပါ။

ပုံ 9: အသင့်ပြုလုပ်ထားသော ဂျီမေးလ်အကောင့်ကို ဖော်ပြထားသည့် Mozilla Thunderbird ၏ ပင်မမျက်နှာစာ

မှတ်ချက် ။ ။ အခြား အီးမေးလ်အကောင့်တစ်ခု ထပ်ထည့်ရန် ဤအခန်းရှိ ပုံ 7 တွင် ပြထားသကဲ့သို့ File>New>Mail Account ကို ရွေးချယ်ပြီး အဆင့် 3 မှ အဆင့် 5 ကို ပြန်လည်လုပ်ဆောင်ပါ။

Thunderbird ၌ သင်၏ အီးမေးလ်အကောင့်ကို အောင်မြင်စွာ မှတ်ပုံတင်ပြီးစီးပါက နောက်တစ်ကြိမ် ပင်မမျက်နှာစာကို သင်ဖွင့်သည့်အခါ သင်၏ အကောင့်တစ်ခုစီ အတွက် password ဝင်ရောက်ရန် သတိပေးချက်သည် အောက်ပါအတိုင်း ပေါ်လာ လိမ့်မည်။



ပုံ 10: Password လိုအပ်ကြောင်းပြသည့် Mail Server Password Required window ပုံ

မှတ်ချက် ။ ။ ယေဘုယျအားဖြင့် အင်တာနက်ဆိုင်ရာ မူပိုင်ခွင့်နှင့် လုံခြုံရေးအရ ကြည့်မည်ဆိုလျှင် password အား မှတ်သားထားခြင်း လုပ်ငန်းစဉ် ('remembering' feature) ကို လုပ်ဆောင်ရန် မသင့်သော်လည်း Thunderbird မှ 'Master Password' feature တစ်ခုကို အထောက်အကူ ပေးထားသည်။ ၎င်းက သင်၏ setup လုပ်ဆောင်စဉ်က အကောင့်အသီးသီး၌ ဝင်ရောက်ခဲ့သော passwords များကို ကာကွယ်ရန် တစ်ခုတည်းသော password ကို အသုံးပြုခွင့်ပေးသည်။ ဤအကြောင်းအရာနှင့် ပတ်သက်၍ ပိုမို သိရှိလိုပါက အခန်း 3.3 ရှိ 'Thunderbird ၌ လုံခြုံရေးဆိုင်ရာ tabs (Password tab) များကို စီမံဆောင်ရွက်ပုံ' ခေါင်းစဉ်၌ ကြည့်ပါ။

2.3 Blogs ၊ News Feeds နှင့် Newsgroup အကောင့်များကို မှတ်ပုံတင်ခြင်း ပြုလုပ်ပုံ

Blogs ၊ News Feeds နှင့် Newsgroup များအတွက် အကောင့်တစ်ခု

တည်ဆောက်ရန် အောက်ပါအဆင့်အတိုင်း ဆောင်ရွက်ပါ။

အဆင့် 1: File>New>Other Accounts ကို ရွေးပါ။ ၎င်းက Account Wizard ရှိ 'New Account Setup' window သို့ ရောက်သွားလိမ့်မည်။

အဆင့် 2: Blogs ၊ News Feeds (သို့) Newsgroup တစ်ခုခု၏ အကောင့် option ကို check လုပ်ပါ။ အောက်ပါ screen သို့ click လုပ်ပြီး သွားပါ။

ပုံ 11: Account Wizard ရှိ အကောင့်အမည်ပြ window

အဆင့် 3: အောက်ပါ screen ကို လုပ်ဆောင်ရန် click လုပ်ပါ။

ပုံ 12: Account Wizard ရှိ Congratulations window

အဆင့် 4: Account setup လုပ်ငန်းစဉ် ပြီးဆုံးရန် click လုပ်ပြီး Thunderbird console ကို ပြန်သွားပါ။

ယခုသင်သည် Thunderbird ကို ပိုမိုကောင်းမွန်စွာ အသုံးပြုနိုင်အောင် ပြင်ဆင်ပြီးပါပြီ။ ထို့နောက် 'Thunderbird ၌ လုံခြုံရေး settings များကို ပြင်ဆင်ဆောင်ရွက်ပုံ' အခန်းကို ဆက်လက်လုပ်ဆောင်ပါ။

Thunderbird ၌ လုံခြုံရေးဆိုင်ရာ Settings များကို ပြင်ဆင်ဆောင်ရွက်ပုံ

ဤစာမျက်နှာရှိ အပိုင်းကဏ္ဍများမှာ

* 3.0 Thunderbird ရှိ လုံခြုံရေး options များအကြောင်း
* 3.1 Thunderbird ၌ Preview Pane ကို disable ပြုလုပ်ပုံ
* 3.2 Thunderbird ၌ HTML လုပ်ဆောင်ချက်ကို disable ပြုလုပ်ပုံ
* 3.3 Thunderbird ၌ လုံခြုံရေးခလုတ်များ (tabs) ကို ပြင်ဆင်ဆောင်ရွက်ပုံ
* 3.4 Account Settings ရှိ Junk Mail Filter (အသုံးမလိုသော စာများကို စစ်ယူသောနေရာ)ကို enable ပြုလုပ်ပုံ

3.0 Thunderbird ရှိ လုံခြုံရေး options များအကြောင်း

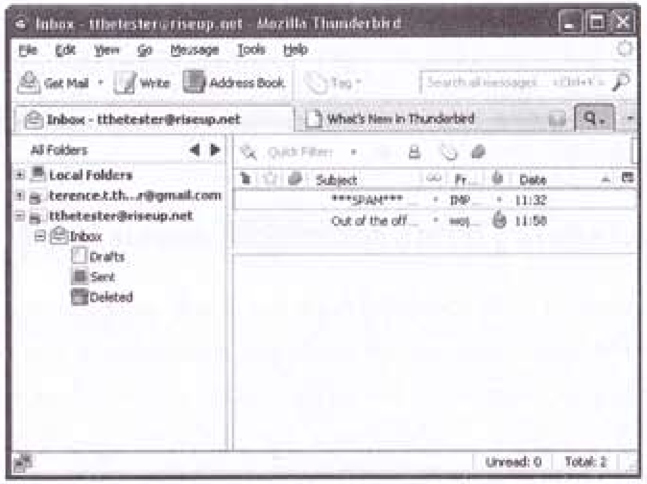
Mozilla Thunderbird တွင် ယေဘုယျအားဖြင့် လုံခြုံရေး (security) ဟူသော စကားရပ်သည် သင်၏ ကွန်ပျူတာကို အန္တရာယ်ရှိသော အီးမေးလ် သတင်းပို့ချက်များ၏အနှောင့်အယှက်မှ ကာကွယ်ပေးခြင်းကို ဆိုလိုသည်။ ၎င်းအီးမေးလ်တချို့တွင် spam များသာပါဝင်ပြီး တချို့တွင်လည်း spyware နှင့် viruses များပါ ပါဝင်နိုင်သည်။ Mozilla Thunderbird တွင် သင်၏အီးမေးလ်မှတစ်ဆင့် သင်၏ system ကို ဝင်ရောက်တိုက်ခိုက်မှုများအား ခုခံကာကွယ်နိုင်စွမ်းကို မြှင့်တင်ရန် ပြင်ဆင်ဆောင်ရွက်ရမည့် settings များစွာရှိသည်။ ၎င်းအပြင် သင့်၌ malware ခုခံကာကွယ်သော ဆော့ဖ်ဝဲနှင့် firewall ကဲ့သို့ ဆော့ဖ်ဝဲများလည်း မရှိမဖြစ် လိုအပ်သည်။

၎င်း အန္တရာယ်ရှိသော ဝင်ရောက်တိုက်ခိုက်မှုများမှ ကာကွယ်ရန် အကြောင်းကို လမ်းညွှန်စာအုပ်ပါ အခန်း 1 'သင်၏ ကွန်ပျူတာကို Viruses၊ Malware နှင့် Hackers များ အန္တရာယ်မှ ကာကွယ်ခြင်း' တွင် ကြည့်ရှု၍ Avast၊ Comodo Firewall နှင့် Spybot တို့ကဲ့သို့ လုံခြုံရေး ဆော့ဖ်ဝဲများအကြောင်းကို လေ့လာနိုင်သည်။

3.1 Thunderbird ၌ Preview Pane ကို disable ပြုလုပ်ပုံ

Thunderbird ၏ console ကို အပိုင်းသုံးပိုင်း ခွဲခြားထားသည်။ ဘယ်ဘက်ရှိ sidebar သည် သင့် အီးမေးလ်အကောင့်အတွက် folders များ ပြထားပြီး ညာဘက်ခြမ်းတွင် သတင်းပို့ချက်စာရင်းတစ်ခု ပြသထားသည်။ အောက်ခြေရှိအပိုင်းတွင် ရွေးချယ်ထားသော အီးမေးလ်သတင်းပို့ချက်ကို ပြထားသည်။ ၎င်းသည် preview pane ဖြစ်သည်။ ၎င်းသတင်းပို့ချက်ကို ရွေးချယ်ပြီးသည်နှင့် တစ်ပြိုင်နက် အောက်ခြေရှိ အပိုင်းတွင် အလိုအလျောက် တွေ့မြင်နိုင်သည်။

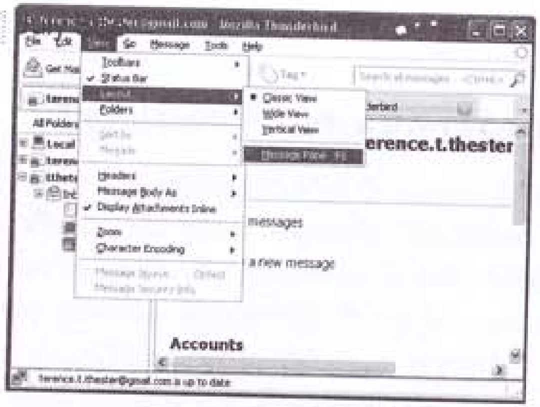
မှတ်ချက် ။ ။ အီးမေးလ်တစ်ခုတွင် အန္တရာယ်ရှိသော code များလည်း ပါရှိနိုင်သဖြင့် ၎င်း သတင်းပို့ချက်ကို ဖော်ပြသည့်အပိုင်းကို disable ပြုလုပ်ထားရန် ပို၍ သင့်လျော်ပါသည်။



ပုံ 1: Thunderbird ၏ ပင်မမျက်နှာစာ

Preview pane ကို disable ပြုလုပ်ရန် အောက်ပါအဆင့်များ ဆောင်ရွက်ပါ။

အဆင့် 1: View>Layout submenu ကို ရွေးပါ။ 'Message Pane' option ကို disable လုပ်ရန် ရွေးချယ်ပါ။



ပုံ 2: Layout submenu ကို ပြထားသော view menu နှင့် ရွေးချယ်ထားသော 'Message Pane' option ပုံ

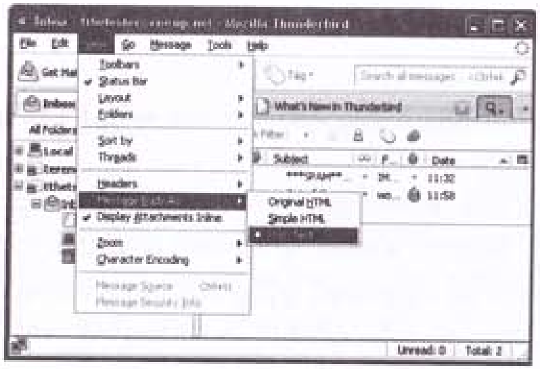
'Message Pane' ပေါ်လာလိမ့်မည်။ အီးမေးလ်သတင်းပို့ချက်တစ်ခုကို ဖတ်ရန် 'double click' နှိပ်ပါ။ အီးမေးလ်သတင်းတစ်ခုသည် သံသယဖြစ်ဖွယ်ရှိပါက (ဥပမာ- ပေးပို့သူ အမည်မပါသည့်အခါ (သို့) အဆီအငေါ်မတည့် ခေါင်းစဉ်မျိုး ပေးထားသည့်အခါ) ၎င်း၌ မည်သည့်အကြောင်းအရာပါသည်ကို ကြည့်ရှုရန် မလိုဘဲ ဖျက်ရန် ရွေးချယ်နိုင် ပါသည်။

3.2 Thunderbird ၌ HTML လုပ်ဆောင်ချက်ကို disable ပြုလုပ်ပုံ

Thunderbird သည် သတင်းပို့ချက်များ ရေးသားရန်၊ ဖတ်ရှုရန်အတွက် HTML (Hyper Text Markup Language) ကို အသုံးပြုခွင့် ပေးထားသည်။ ၎င်းက အရောင်၊ စာလုံးပုံစံ၊ ရုပ်ပုံများနှင့် အခြားသော format ပြုလုပ်သော လုပ်ဆောင်မှုများ ပါဝင်သည့် သတင်းများကို ပေးပို့ခြင်း၊ လက်ခံခြင်းများ ပြုလုပ်ခွင့်ပေးသည်။ သို့သော် လည်း HTML သည် ကွန်ရက်စာမျက်နှာများအတွက် အသုံးပြုသော ဘာသာစကားပင် ဖြစ်သောကြောင့် သတင်းပို့ချက်များကို HTML format ဖြင့် ကြည့်ရှုခြင်းသည် ကွန်ရက်စာမျက်နှာများမှ ထုတ်လွှတ်သော ပိုးမွှားများ ခြိမ်းခြောက်မှုမျိုးဖြင့် သင့်ထံသို့ အန္တရာယ်ရှိသော အီးမေးလ်များအနေဖြင့် ဝင်ရောက်လာနိုင်သည်။

HTML formatting လုပ်ဆောင်ချက်ကို disable ပြုလုပ်ရန် အောက်ပါအတိုင်း ဆောင်ရွက်ပါ။

အဆင့် 1: View>Message Body As> Plain Text ကို ရွေးပါ။



ပုံ 3: Message Body submenu ကို ပြထားသော View menu နှင့် ရွေးချယ်ထားသော Plain Text option ပုံ

3.3 လုံခြုံရေးဆိုင်ရာ Options များကို ပြင်ဆင်ဆောင်ရွက်ပုံ

Thunderbird တွင် သင့်ထံသို့ ဝင်ရောက်လာသော မည်သည့်သတင်းပို့ချက်က spam ဖြစ်သည်ကို ဆုံးဖြတ်ပေးသော၊ အသုံးမလိုသည့်စာများကို စစ်ယူပေးသောနေရာ (junk mail filter) နှစ်ခုပါရှိသည်။ မူလအနေအထားအရ ၎င်းတို့ကို disable လုပ်ထားပြီး အသုံးပြုလိုပါက enable လုပ်ပေးရမည်။ ၎င်းတို့ကို enable လုပ်ပြီးသော်လည်း junk mail များကို ဆက်လက် ရရှိနေနိုင်သည်။ သို့သော် Thunderbird က ၎င်း junk mail များကို အလိုအလျောက် စီစဉ်ပြီး Junk folder ထဲသို့ ထည့်ပေးသည်။

အီးမေးလ်လှည့်စားခြင်း : ၎င်းက သင့်အား အီးမေးလ်အတွင်း၌ မြှုပ်နှံထားသော link တစ်ခုကို နှိပ်မိစေပြီး သင့်ကွန်ပျူတာ၏ browser မှတစ်ဆင့် ကွန်ရက်စာမျက်နှာတစ်ခုသို့ လမ်းညွှန်ပေးပြီး ၎င်းကွန်ရက်စာမျက်နှာမှတစ်ဆင့် ပိုးရပ်စ် ဝင်ရောက်လာနိုင်သည်။ အခြားတစ်နည်းမှာ ၎င်း link မှတစ်ဆင့် တရားဝင်ပြီး မှန်ကန်မှုရှိသည်ဟု ထင်ရသော ကွန်ရက်စာမျက်နှာတစ်ခုသို့ ဝင်ရောက်သွားပြီး ၎င်းထံ၌ သင့်အားအမည်နှင့် password များ တင်ပြရန် ဖြားယောင်းလိမ့်မည်။ ထို့နောက်တွင် ၎င်း အချက်အလက်များကို စီးပွားရေးအရသော်လည်းကောင်း၊ မကောင်းသော ရည်ရွယ်ချက် ဖြင့်သော်လည်းကောင်း ပြန်လည်ရောင်းချခံရလိမ့်မည်။

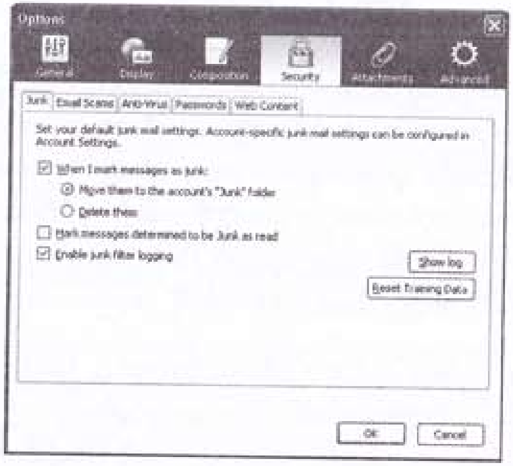
Thunderbird က ထိုကဲ့သို့ အီးမေးလ်များအကြောင်းကို သင့်အား ခွဲခြား ရှာဖွေပြီး သတိပေးနိုင်သည်။ ၎င်းအန္တရာယ်ရှိသော ကွန်ရက်စာမျက်နှာများမှ ကူးစက် ဝင်ရောက်ခြင်းကို ကာကွယ်နိုင်သည့် ထပ်မံဖြည့်စွက်ထားသော လုပ်ဆောင်ချက်များကို

'Firefox' အခန်းရှိ 'Mozilla ၏ အခြားအသုံးဝင်သော ဖြည့်စွက်ပရိုဂရမ်များ' ခေါင်းစဉ်တွင် ဖော်ပြထားသည်။

Junk mail များ စုပေါင်းထားသည့် ပထမဆုံး အစုအစည်းနှင့် လုံခြုံရေး ထိန်းချုပ်မှုများကို Security window ရှိ Options မှ access လုပ်နိုင်သည်။ ၎င်း Security window သည် လုံခြုံရေးနှင့် မူပိုင်ခွင့်ဆိုင်ရာ options များကို ဆောင်ရွက်နိုင်သော အဓိကနေရာဖြစ်သည်။ ၎င်းတို့ကို access လုပ်ရန် အောက်ပါအဆင့်များ လုပ်ဆောင်ပါ။

အဆင့် 1: Options window သို့သွားရန် Tools>Options ကိုရွေးပါ။

အဆင့် 2: အောက်ပါ screen သို့ click လုပ်ပြီးသွားပါ။



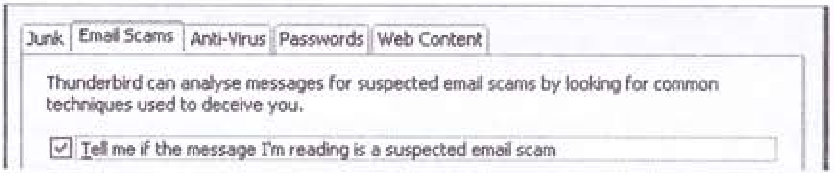
ပုံ 4: တွဲလျက်ပါဝင်သော ခလုတ်များ (tabs) ကို ပြထားသော Security window ပုံ

The Junk tab

အဆင့် 1: သင်က junk mail ဟုယူဆရသော အီးမေးလ်ကိုဖျက်ရန် Thunderbird ကို enable ပြုလုပ်ရန်အတွက် အထက်ပါပုံ 4 တွင် ဖော်ပြထားသည့် အတိုင်း Junk tab ရှိ သက်ဆိုင်ရာ option ကို check လုပ်ပါ။ သက်ဆိုင်ရာ Junk Mail Settings များကို နောက်ပိုင်းတွင် ဤအပိုင်း၌ ဖော်ပြထားသည်။

The Email Scams tab

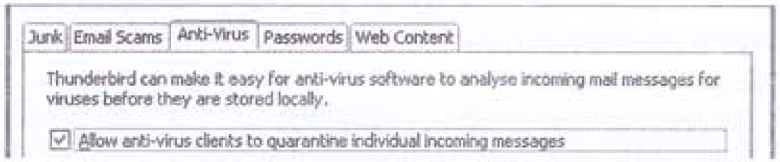
အဆင့် 1: အောက်ပါအတိုင်း အီးမေးလ်လှည့်စားမှုများ (email scams) အတွက် သတင်းပေးပို့ချက်များကို ခွဲခြားကြည့်ရှုရန် Thunderbird ကို enable လုပ်ဖို့ရာ 'Tell me if the message I'm reading is a suspected email scam' option ကို check လုပ်ပါ။



ပုံ 5: Email Scams tab ပုံ

The Anti-Virus tab

အဆင့် 1: အောက်ပါ screen ကို လုပ်ဆောင်ရန် Anti-Virus tab ကို click လုပ်ပါ။



ပုံ 6: Anti-Virus tab ပုံ

ဤ option က ရောက်ရှိလာသော သတင်းတစ်ခုချင်းကို သင်၏ ဗိုင်းရပ်စ်ကာကွယ်သည့် ဆော့ဖ်ဝဲမှ တစ်ဆင့် စစ်ဆေးပြီး သီးသန့်ထားရှိသည်။ ၎င်း setting ကို enable မလုပ်ထားပါက အကယ်၍ သင်သည် ကူးစက်မှုခံထားရသော သတင်းကို လက်ခံရရှိသောအခါ သင့် 'Inbox folder' တစ်ခုလုံးကို ကူးစက်ခြင်း မခံရစေအောင် သီးသန့်ထားရှိခြင်းမျိုး ဖြစ်ပွားနိုင်သည်။

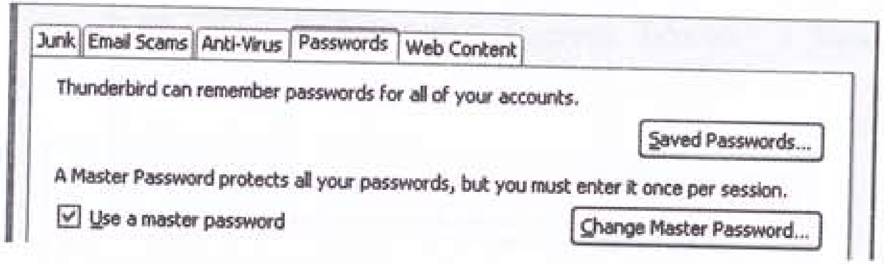
မှတ်ချက် ။ ။ သင့်၌ ဗိုင်းရပ်စ်ကာကွယ်သည့် ဆော့ဖ်ဝဲတစ်ခုကို install ပြုလုပ်ထားသင့်သည်။ 'ဗိုင်းရပ်စ်ကာကွယ်သည့် ဆော့ဖ်ဝဲကို install ပြုလုပ်ပုံနှင့် စီမံဆောင်ရွက်ပုံ' ကို 'Avasst' မှာကြည့်ပါ။

The Passwords tab

အရေးကြီး ။ ။ သင်၏ passwords များကို လျှို့ဝှက်ပြီး လုံခြုံမှုရှိစေရန် ရည်ရွယ်ချက်ရှိရှိ တိကျစွာ ထုတ်လုပ်ထားသော ဆော့ဖ်ဝဲမျိုးကို ရွေးချယ်ရန် အကြံပြုပါသည်။ 'Kee Pass' တွင် အချက်အလက်များ ရှာပါ။

မှတ်ချက် ။ ။ သင်၏ 'Password tab' ရှိ option သည် Thunderbird ၌ သင်၏ အီးမေးလ်အကောင့်များ မှတ်ပုံတင်ခြင်း ပြု လုပ်သောအခါ ပထမဆုံး 'မေးလ်အကောင့်ပြုလုပ်ခြင်း' screen တွင် 'Remember password' option အား check လုပ်ခဲ့မှသာလျှင် အလုပ်လုပ်နိုင်ပါလိမ့်မည်။

အဆင့် 1: အောက်ပါ screen ကို လုပ်ဆောင်ရန် click လုပ်ပါ။

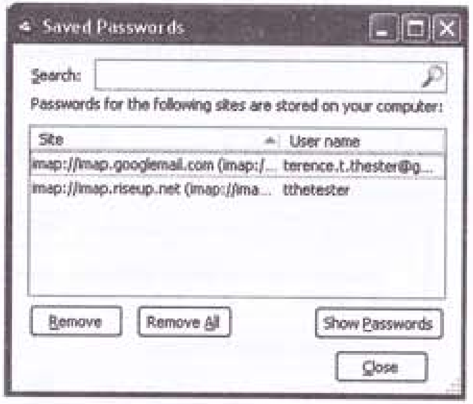


ပုံ 8: Saved Passwords window ပုံ

Saved Passwords window က သင်၏ အကောင့်တစ်ခုစီအတွက် သက်ဆိုင်ရာ passwords များ အားလုံးကို ကြည့်ရှုရန် (သို့) ဖယ်ရှားရန်ခွင့်ပြုသည်။ သို့သော် သင်၏ လုံခြုံရေးနှင့်မူပိုင်ခွင့်ကို ပိုမိုအကျိုးရှိစေရန် 'Thunderbird password' options များနှင့် အကျွမ်းတဝင်ရှိသူမှတစ်ပါး အခြားသူများက သင်၏ password အကောင့်များကို access လုပ်ခြင်းမပြုနိုင်ရန် 'Master Password' တစ်ခု သတ်မှတ်ထားနိုင်သည်။

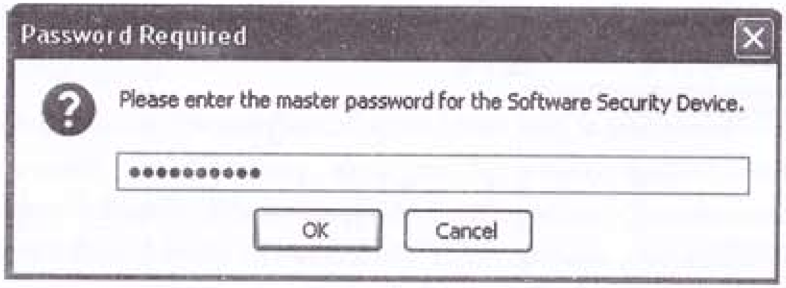
အဆင့် 3: 'Change Master password' ခလုတ်ကို enable လုပ်ရန် ပုံ 7: ပါ အတိုင်း 'Use a master password option ကို check အရင်လုပ်ပါ။

အဆင့် 4: အောက်ပါ screen သို့ click လုပ်ပြီးသွားပါ။



ပုံ 9: Change Master Password window ပုံ

အဆင့် 5: သင်တစ်ဦးတည်း မှတ်မိနိုင်သော ခက်ခဲသည့် password တစ်ခု ရိုက်ထည့်ပါ။ ၎င်းကို သင်၏ Master password အဖြစ် အတည်ပြုရန် click နှိပ်ပါ။ နောက်တစ်ကြိမ် သင် click လုပ်သည့်အခါ သင်၏ master password ကို ဝင်ရောက်ရန် သတိပေးချက်ပြသော screenကို တွေ့ရမည်။

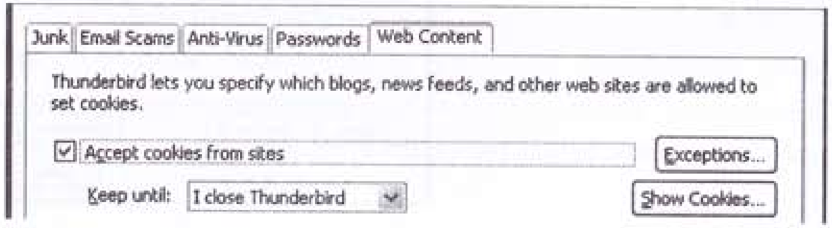


ပုံ 10: Password Required screen ပုံ

The Web Content tab

'Cookie' ဆိုသည်မှာ ကွန်ရက်စာမျက်နှာတစ်ခုကို ခွဲခြမ်းစစ်ဆေးရာတွင် အသုံးပြုသော သင်၏ကွန်ရက်ရှာဖွေစက် (web browser) ရှိ သေးငယ်သောစာဖိုင်(သို့) စာကြောင်းတစ်ကြောင်းသာ ဖြစ်သည်။ 'Web Content tab' က မည်သည့် blog, newsfeed နှင့် newsgroup cookies များသည် ယုံကြည်စိတ်ချရသည်ကို ခွဲခြားပေးသည်။

အဆင့် 1: အောက်ပါ screen သို့သွားရန် Web Content tab ကို click လုပ်ပါ။



ပုံ 11: Web Content tab ပုံ

အဆင့် 2: လုံခြုံရေးအခြေအနေအရ Thunderbird အသုံးပြုမှုကို သင်ပိတ်သည့်အခါ 'cookies' များကို ဖျက်ရန်အတွက် 'I close Thunderbird item in the Keep until' option ကို ရွေးပါ။

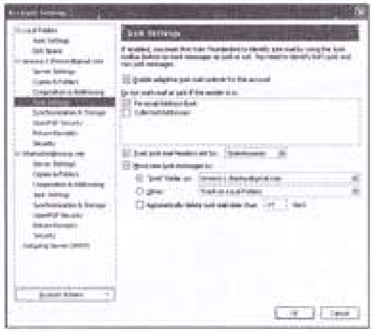
3.4 Account Settings ရှိ Junk Mail Filter (အသုံးမဝင်သော စာများကို စစ်ယူသောနေရာ) ကို enable ပြုလုပ်ပုံ

Thunderbird ၏ junk mail filter ဒုတိယအမျိုးအစားကို Account Settings ရှိ Junks Settings window တွင် တွေ့ရမည်။ မူလအားဖြင့် ၎င်း filters များကို disable လုပ်ထားပြီး အသုံးပြုလိုသော ဆန္ဒရှိမှသာ enable လုပ်ရမည်။ အသုံးမဝင်သော အီးမေးလ်များ ရောက်ရှိလာတိုင်း Thunderbird က ၎င်းတို့ကို အလိုအလျောက် စိစစ်ပြီး အကောင့်အသီးသီးနှင့် ဆက်စပ်နေသော Junk folders များအတွင်းသို့ ထည့်ပေးသည်။

အဆင့် 1: Account Settings window ကို လုပ်ဆောင်ရန် Tools> Account Settings ကို ရွေးပါ။

အဆင့် 2: Sidebar တွင် Gmail (သို့) Riseup အကောင့်တစ်ခုခု ပါဝင်သော Junk Settings option ကို ရွေးပါ။

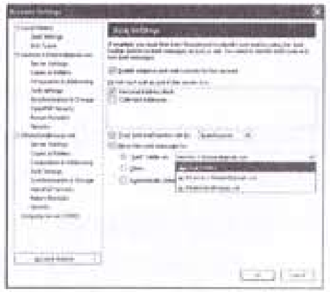
အဆင့် 3: ၎င်း Junk Settings option ကို enable လုပ်ခြင်းဖြင့် သင်၏ ကိုယ်ပိုင် Account Settings- Junk Settings screen ကို အောက်ပါအတိုင်း တွေ့ရမည်။



ပုံ 12: Account Settings- Junk Settings window ပုံ

အဆင့် 4: Account Settings window ပြင်ဆင်ဆောင်ရွက်ခြင်း ပြီးဆုံးအောင် click လုပ်ပါ။

မှတ်ချက် ။ ။ အကောင့်တစ်ခုစီအတွက် Junk Settings option ကို သီးခြားစီ ဆောင်ရွက်ရမည်။ Gmail (သို့) Riseup အကောင့်တစ်ခုအတွက် Junk mail ကို ၎င်းနှင့် သက်ဆိုင်သော Deleted folder ၌ ထည့်ထားရမည်။ နောက်တစ်မျိုးမှာ သင်၏ အကောင့်အားလုံးမှ junk mail များကို လက်ခံရန် Local folder တစ်ခု ဆောက်ပေးရမည်။



ပုံ 13: ဗဟို junk folder အတွက် settings များ ပါဝင်သော Account Settings မှ Junk Settings ပုံ

အဆင့် 1: Sidebar အတွင်းရှိ Local Folder အောက်မှ Junk Settings option ကို ရွေးပါ။

အဆင့် 2: ပုံ 13: တွင် ပြထားသော drop-down list ရှိ "Junk" folder မှ Local Folders ကို ရွေးပါ။

အဆင့် 3: Account Settings window ပြင်ဆင်ခြင်း ပြီးဆုံးရန် click လုပ်ပါ။

ယခု သင်သည် Thunderbird ရှိ လုံခြုံရေး options နှင့် junk mail settings များအားလုံးကို အောင်မြင်စွာ ပြင်ဆင်ဆောင်ရွက်နိုင်ပါပြီ။
'Enigmail နှင့် GnuPG တို့ကို Thunderbird ၌ အသုံးချပုံ' အခန်းကို ဆက်ကြပါဦးစို့။

Thunderbird ၌ Enigmail နှင့် GnuPG တို့ကို အသုံးချပုံ

ဤစာမျက်နှာရှိ အပိုင်းကဏ္ဍများမှာ

* 4.0 Enigmail ၊ GnuPG နှင့် လျှို့ဝှက်အများဆိုင် Key အသွင်ပြောင်းခြင်း အကြောင်း
* 4.1 Enigmail နှင့် GnuPG တို့ကို install ပြုလုပ်ပုံ
* 4.2 Key အစုံများ ထုတ်ယူပုံနှင့် သင်၏ အီးမေးလ်အကောင့်နှင့် လုပ်ဆောင်ရန် Enigmail ကို စီစဉ်ဆောင်ရွက်ပုံ
* 4.3 အများဆိုင် Keys များ လဲလှယ်ပုံ
* 4.4 Key တစ်စုံကို တရားဝင်အောင် ပြုလုပ်ပုံနှင့် အမှတ်အသားပြုပုံ
* 4.5 သတင်းတစ်ခုကို အသွင်ပြောင်း ဝှက်စာပြုလုပ်ခြင်းနှင့် ဝှက်စာဖြည်ခြင်း ပြုလုပ်ပုံ

4.0 Enigmail ၊ GnuPG နှင့် လျှို့ဝှက်အများဆိုင် Key အသွင်ပြောင်းခြင်းအကြောင်း

Enigmail သည် Mozilla Thunderbird ၏ ဖြည့်စွက်ပရိုဂရမ်ဖြစ်ပြီး သင့်အီးမေးလ်ဆက်သွယ်ချက်များ၏ မူပိုင်ခွင့်ကို ကာကွယ်ပေးသည်။ Enigmail သည် Thunderbird အတွင်းရှိ GnuPG ဝှက်စာအသွင်ပြောင်းခြင်း ပရိုဂရမ်ကို သင့်အား အသုံးပြုခွင့်ပေးသော စာမျက်နှာ (interface) ဖြစ်သည်။ Thunderbird ၏ console too bare တွင် Enigmail ကို OpenPGP အဖြစ် တွေ့ရသည်။

Enigmail ကို အများဆိုင် Key များကို ဝှက်စာစကားလုံးများ (သို့)

ပဟေဠိစကားလုံးများ ပြုလုပ်ခြင်းဆိုင်ရာ နည်းပညာဖြင့် အခြေခံထားသည်။ ဤနည်းလမ်းတွင် ပုဂ္ဂိုလ်တစ်ဦးချင်းစီ၌ ၎င်း၏ ကိုယ်ပိုင် Key အစုံကို ထုတ်ပေးထားရမည်။ ပထမ key သည် လျှို့ဝှက် key ဖြစ်သည်။ ၎င်းကို password (သို့) passphrase တစ်ခုဖြင့် ကာကွယ်ထားပြီး အခြားမည်သူနှင့်မှ မျှဝေခြင်းမရှိစေရန် စောင့်ရှောက် ထားသည်။

ဒုတိယ key ကို အများဆိုင် key အဖြစ် သတ်မှတ်သည်။ ဤ key ကို သင်နှင့် အဆက်အသွယ်ရှိသူ မည်သူနှင့်မဆို မျှဝေသုံးစွဲနိုင်သည်။ သင့်၌ သင်နှင့် အဆက်အသွယ်ရှိသူ၏ အများဆိုင် key ကို ရရှိပါက ၎င်းထံသို့ ဝှက်စာ အသွင်ပြောင်းထားသော အီးမေးလ်များ စတင်ပေးပို့နိုင်သည်။ ၎င်းကသာလျှင် သင်၏ အီးမေးလ်ကို ဝှက်စာဖြည်၍ ဖတ်ရှုခြင်း ပြုနိုင်သည်။ အဘယ်ကြောင့်ဆိုသော် ထိုသူသာလျှင် တူညီသော လျှို့ဝှက် key ဖြင့် access လုပ်နိုင်သောကြောင့်ဖြစ်သည်။

အလားတူပင် သင့်အများဆိုင် key ၏ မူပွားကို သင်နှင့် အီးမေးလ်ဆက်သွယ်သူထံသို့ပေးပို့ပြီး တူညီသောလျှို့ဝှက် key ကို လျှို့ဝှက်ထားလျှင် ထိုသူထံမှ သတင်းများကို ဖြည်၍ဖတ်ရှုရန် သင်တစ်ဦးသာ တတ်နိုင်သည်။

Enigmail က သင်၏ သတင်းပို့ချက်များနှင့် ပေးပို့သူ မည်သူမည်ဝါ ဖြစ်ကြောင်းကို အာမခံချက်ပေးသော digital signature နှင့် တွဲဖက်ပေးသည်။ သင်၏ စစ်မှန်သော အများဆိုင် key မူပွားကို ရရှိထားသည့် သင့်ထံမှ သတင်းကို လက်ခံမည့် သူသည် ၎င်း အီးမေးလ်မှာ သင့်ထံမှလာခြင်းဖြစ်ကြောင်း ခွဲခြားနိုင်ပြီး လမ်းခရီး တစ်လျှောက်တွင် ခြေရာလက်ရာပျက်ခြင်း ရှိ မရှိကိုလည်း သိရှိနိုင်သည်။ ထို့အတူ သင့်၌ ဆက်သွယ်သူ၏ အများဆိုင် key ရှိပါကလည်း ၎င်း၏ သတင်းပေးပို့ချက်များပေါ်မှ digital signatures ကို ခွဲခြားနိုင်သည်။

4.1 Enigmail နှင့် GnuPGG တို့ကို install ပြုလုပ်ပုံ

လမ်းညွှန်ချက်ရှိ download အပိုင်းတွင် 'Enigmail နှင့် GnuPG တို့ကို download လုပ်ယူပုံ' ကို ကြည့်ပါ။

4.1. GnuPG ကို install ပြုလုပ်ပုံ

GnuPG ကို install ပြုလုပ်ခြင်းမှာ တစ်ဆက်တည်း ပြုလုပ်နိုင်ပြီး သင်

ပြုလုပ်ဖူးသော ဆော့ဖ်ဝဲ installations များနှင့် အတူတူပင် ဖြစ်သည်။

GnuPG ကို install စတင်ပြုလုပ်ရန် အောက်ပါအဆင့်များ ဆောင်ရွက်ပါ။

အဆင့် 1: Installation လုပ်ငန်းစဉ် စတင်ရန် double click နှိပ်ပါ။ ဖိုင်ကို ဖွင့်လျှင် လုံခြုံရေးအချက်ပေး dialog box ပေါ်လာလိမ့်မည်။ ထိုသို့ဖြစ်ပွားပါက အောက်ပါ screen သို့ click လုပ်ပြီး သွားပါ။

ပုံ 1: GNU Privacy Guard Setup Wizard

အဆင့် 2: GNU Privacy Guard Setup မှတစ်ဆင့် User သဘောတူညီချက် ရယူမည့် License Agreement window ကို သွားပါ။ ပါဝင်သော အကြောင်းအရာများ ဖတ်ပြီးသောအခါ GNU Privacy Guard Setup ရှိ Choose Components window ကို သွားပါ။

အဆင့် 3: ပေးထားသော settings ကို လက်ခံပါ။ Install Options ရှိ ဘာသာစကားရွေးရန် Language Selection window သို့ သွားပါ။

အဆင့် 4: en-English ကို အလိုရှိသော ဘာသာစကားအဖြစ် လက်ခံပါ။ တည်နေရာရွေးရန် Choose Install Location window သို့ သွားပါ။

အဆင့် 5: ပေးထားသော installation လမ်းကြောင်းကိုပဲ ရွေးချယ်ပါ။ Choose Start Menu Folder screen သို့ သွားပါ။

အဆင့် 6: GnuPG တွင် ပါဝင်သော packages အမျိုးမျိုးတို့ကို ပြည့်ချပြီး install လုပ်ရန် click နှိပ်ပါ။ လုပ်ငန်းစဉ် အလိုအလျောက် လုပ်ဆောင်ပြီးပါက Installation Complete screen ကို တွေ့ရမည်။

အဆင့် 7- GnuPG ပရိုဂရမ် install လုပ်ခြင်း ပြီးစီးကြောင်း click လုပ်ပါ။

4.1.2 ဖြည့်စွက်ပရိုဂရမ် Enigmail ကို install ပြုလုပ်ပုံ

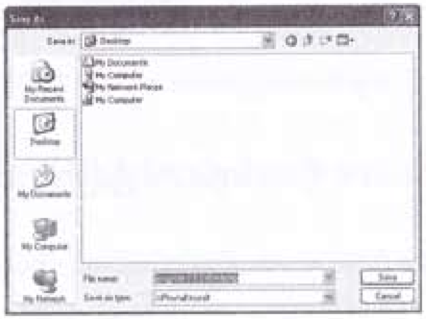
ပုံ 2: Extensions pane ကို ပြသထား သော Add-ons window ပုံ

GnuPG ဆော့ဖ်ဝဲကို အောင်မြင်စွာ install ပြုလုပ်ပြီးလျှင် ဖြည့်စွက်ပရိုဂရမ် Enigmail ကို install လုပ်ရန် အဆင်သင့် ဖြစ်ပါပြီ။

Enigmail ကို install လုပ်ရန် အောက်ပါအဆင့်များ ဆောင်ရွက်ပါ။

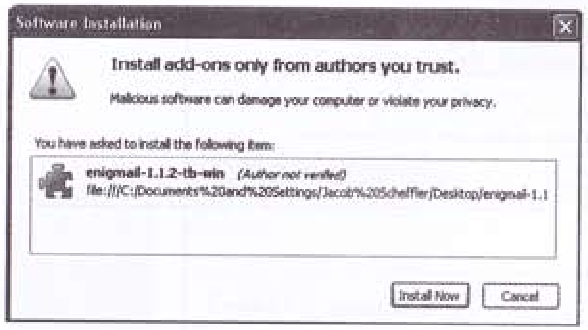
အဆင့် 1: Thunderbird ကို ဖွင့်ပါ။ Tools>Add-ons ကို ရွေးပြီး Add-ons window ကို သွားပါ။ Add-ons window သည် Get Add-ons pane ကို enabled လုပ်လျက် ပေါ်လာလိမ့်မည်။

အဆင့် 2: အောက်ပါ screen ကို လုပ်ဆောင်ရန် click လုပ်ပါ။



ပုံ 3: Install လုပ်ရန် extenstion ရွေးချယ်မှုပြပုံ

အဆင့် 3: Enigmail ကို သင် save လုပ်ခဲ့သော folder သို့ သွားပါ။ အောက်ပါ screen ကို လုပ်ဆောင်ရန် click နှိပ်ပါ။



ပုံ 4: Software Installation window ပုံ

အရေးကြီး ။ ။ ဤအဆင့်ကို သင်မဆောင်ရွက်မီ သင်၏ online နှင့် ပတ်သက်သော အလုပ်ဟူသမျှကို save လုပ်ထားရန် လိုအပ်သည်။

အဆင့် 7: ပုံ 4:သို့ ပြန်သွားပါ။ Enigmail ဖြည့်စွက်ပရိုဂရမ် install လုပ်ငန်းစဉ် ပြီးဆုံးရန် click လုပ်ပါ။

သင်၏ Enigmail install လုပ်ငန်းစဉ်အောင်မြင်မှု ရှိ မရှိ ခွဲခြားရန် Thunderbird ၏ ပင်မမျက်နှာစာ (main user interface) သို့ သွားပါ။ Thunderbird tool bar ၌ 'Open OGP' ပေါ် မပေါ် စစ်ဆေးပါ။

ပုံ 5: Open PGP ကို အမှတ်အသားပြုထားသော Thunderbird toolbar

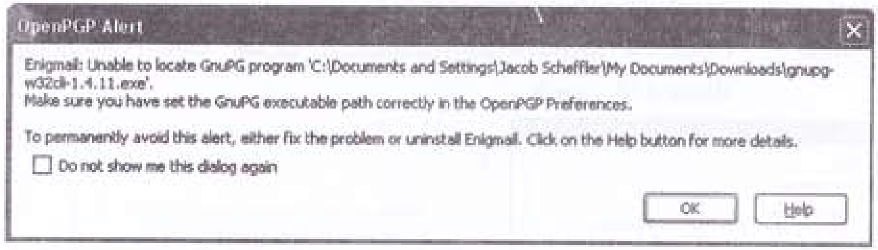
4.1.3 Enigmail နှင့် GnuPG တို့ အလုပ်လုပ်ဆောင်မှုရှိကြောင်း အတည်ပြုပုံ

သင်၏ အီးမေးလ်များကို ဝှက်စာအသွင်ပြောင်းခြင်းနှင့် အမှန်စစ်ဆေးခြင်းများ ပြုလုပ်ရန် Enigmail နှင့် GnuPG တို့ကို အသုံးမပြုခင် ၎င်းတို့ နှစ်ခုစလုံးသည် တစ်ခုနှင့်တစ်ခု ဆက်သွယ်ချက်ရှိကြောင်း သေချာအောင် ပြုလုပ်ပါ။

အဆင့် 1: Open PGP Preferences screen ကို ပြသရန် Open PGP> Preferences ကို ရွေးပါ။

ပုံ 6: Open PGP Preferences screen ပုံ

GnuPG ကို အောင်မြင်စွာ install ပြုလုပ်ပြီးပါက ၎င်းကို ဖိုင် (Files) နှင့် အညွှန်းပြဆိုချက်များ (directories) အပိုင်းတွင် တွေ့မြင်နိုင်သည်။ သို့မဟုတ်ပါက pop-up အချက်ပေးချက်တစ်ခု အောက်ပါအတိုင်း ပေါ်လာလိမ့်မည်။



ပုံ 7: OpenPGP Alert pop-up message ပုံ

သတိပြုရန် ။ ။ ၎င်း သတိပေးချက်ကို ရရှိပါက ၎င်းကသင်သည် ဖိုင်ကို နေရာမှား၍ ထားရှိကြောင်း ပြသခြင်းဖြစ်သည်။ Browse ခလုတ်ကို enable လုပ်ရန် Override with option ကို check လုပ်ပါ။ GnuPG ကို နေရာချမည့် 'Locate GnuPG' ပရိုဂရမ်ကို လုပ်ဆောင်ရန် click လုပ်ပါ။ သင်၏ ကွန်ပျူတာရှိ gpg.exe ဖိုင်ကို ညွှန်ပြလိမ့်မည်။

အဆင့် 2: Thunderbird console သို့ ပြန်သွားရန် click လုပ်ပါ။

4.2 Key အစုံများ ထုတ်ယူပုံနှင့် Enigmail ကို သင့် အီးမေးလ်အကောင့်များနှင့် တွဲ၍ အလုပ်လုပ်ရန် စီမံဆောင်ရွက်ပုံ

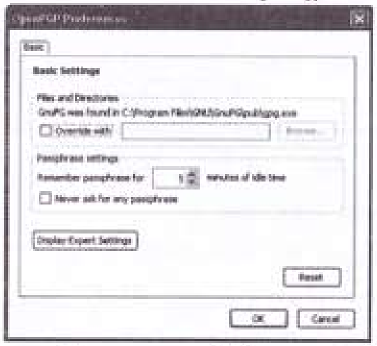
Enigmail နှင့် GnuPG တို့သည် ကောင်းစွာအလုပ်လုပ်ကြောင်း အတည်ပြုပြီးသောအခါ တစ်ခု(သို့) တစ်ခုထက်ပိုသော အီးမေးလ်အကောင့်များကို အသုံးပြု၍ Enigmail မှတစ်ဆင့် တစ်ခု (သို့) တစ်ခုထက်ပိုသော လျို့ဝှက်/အများဆိုင် keyအစုံများကို ထုတ်ယူနိုင်သည်။

4.2.1 Key အစုံတစ်ခုကို ထုတ်ယူရန် OpenPGP Wizard ကို အသုံးပြုပုံ

Enigmail မှ လျို့ဝှက်(သို့) အများဆိုင် Key အစုံ ထုတ်ယူရန် နည်းလမ်းနှစ်မျိုးရှိသည်။ ပထမတစ်မျိုးမှာ OpenPGP Wizard ကို အသုံးပြုပြီး ဒုတိယတစ်မျိုးမှာ Key များ စီမံကွပ်ကဲမှု (Key Management) screen ကို အသုံးပြုသည်။

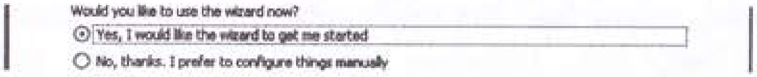
OpenPGP Wizard ကို ပထမအကြိမ် စတင်အသုံးပြုရာတွင် key အစုံထုတ်ယူရန် အောက်ပါအဆင့်များ ဆောင်ရွက်ပါ။

အဆင့် 1: OpenPGP Setup Wizard screen ကို ဖွင့်ရန် OpenPGP>Setup Wizard ကို ရွေးပါ။



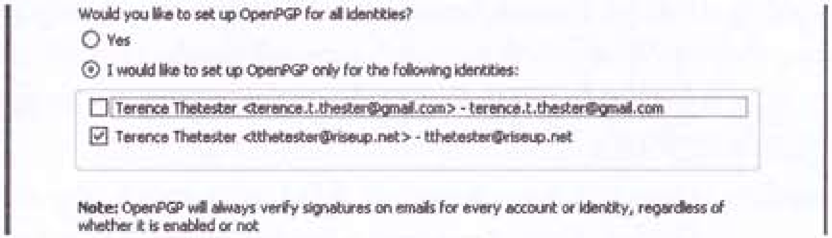
ပုံ 8: Welcome to the OpenPGP Setup Wizard screen ပုံ

အဆင့် 2: အောက်ပါ screen သို့ click လုပ်ပြီးသွားပါ။



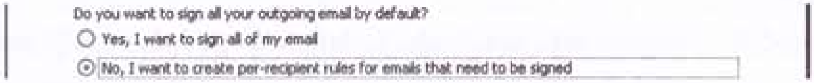
ပုံ 9: အမှတ်အသား ရွေးချယ်ခြင်းပြ Select Identities screen ပုံ

အဆင့် 3: အောက်ပါ screen သို့ သွားရန် click လုပ်ပါ။



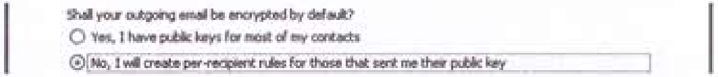
ပုံ 10: အမှတ်အသားပြုခြင်း- သင်၏ အပြင်သို့ စေလွှတ်မည့် အီးမေးလ်များကို ဒီဂျစ်တယ်နည်းအရ အမှတ်အသားပြုလုပ်ခြင်း screen ပုံ

အဆင့် 4: အောက်ပါ screen ကို လုပ်ဆောင်ရန် click လုပ်ပါ။



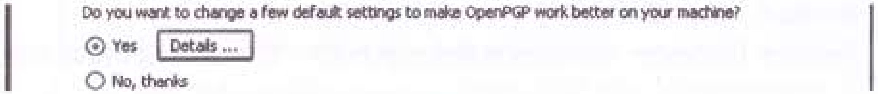
ပုံ 11: ဝှက်စာအသွင်ပြောင်းခြင်း- သင်၏ အပြင်သို့စေလွှတ်မည့်အီးမေးလ်များကို ဝှက်စာအသွင်ပြောင်းခြင်းပြ screen ပုံ

အဆင့် 5: အောက်ပါ screen ကို လုပ်ဆောင်ရန် click လုပ်ပါ။



ပုံ 12: ရွေးချယ်ခြင်း- OpenPGP ကိုပို၍ လွယ်ကူစွာ အသုံးချနိုင်ရန် သင်၏ အီးမေးလ် Settings များ ပြောင်းလဲခြင်းပြပုံ

အဆင့် 6: အောက်ပါ screen သို့ click လုပ်ပြီးသွားပါ။



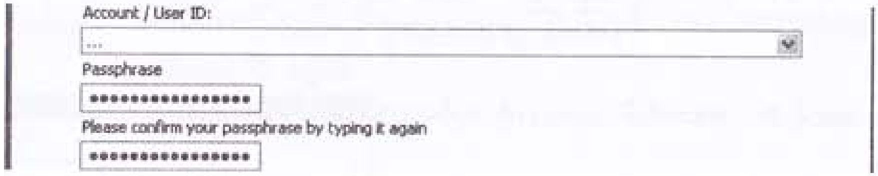
ပုံ 13: ရွေးချယ်ခြင်းပြ screen ပုံ

မှတ်ချက် ။ ။ အပိုင်း 3.3 ရှိ 'Thunderbird ၌ HTML လုပ်ဆောင်ချက်ကို disable ပြုလုပ်ပုံ' ၌ HTML ဖြင့် format လုပ်ထားသော သတင်းများတွင် ဗိုင်းရပ်စ် အမျိုးမျိုးတို့ ဝင်ရောက်တိုက်ခိုက်နိုင်ကြောင်းကို အသေးစိတ် ဆွေးနွေးခဲ့ကြသည်။ သတင်းကို plain text ဖြင့် ကြည့်ရှုခြင်းနှင့် HTML format ဖြင့် သတင်းများ ရေးသားအသုံးမပြုရန် အကြောင်းများဖြစ်သည်။

အဆင့် 7: Open PGP Setup Wizard သို့ ပြန်ရန် click လုပ်ပါ။ Key တစ်ခု ပြုလုပ်ရန် 'Create Key-Create A Key To Sign and Encrypt Email' window သို့ သွားရန် click လုပ်ပါ။

မှတ်ချက် ။ ။ အီးမေးလ်အကောင့်တစ်ခုအတွက် ပထမအကြိမ် Key တစ်ခု ပြုလုပ်ရာတွင် သင့် drop-down list ၌ သင်၏ အီးမေးလ်အကောင့်များကို တွေ့ရမည် မဟုတ်ပါ။

အဆင့် 8: အက္ခရာဂဏန်း အနည်းဆုံး 8 လုံးရှိသည့် passphrase (သို့) password ကို ရိုက်ပါ။



ပုံ 14: Create Key- Create A Key To Sign and Encrypt Email window ပုံ

အဆင့် 9: ၎င်း Settings များကို အတည်ပြုရန် click လုပ်ပါ။ ထို့နောက် Key ပြုလုပ်သည့် screen သို့ ပြန်သွားပါ။ သင့်၏ ပထမ အီးမေးလ်အကောင့် အမည်ကို အောက်ပါအတိုင်း တွေ့ရမည်။

Account / User ID:
Terence Thetester <tthetester@riseup.net> - tthetester@riseup.net

ပုံ 15: အသစ်ပြုလုပ်ထားသော အကောင့်၊ အသုံးပြုသူ၏ ID

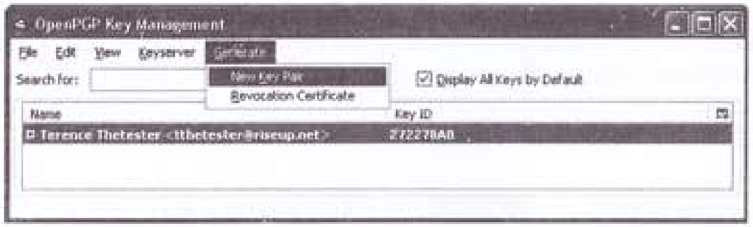
အဆင့် 10: Summary screen သို့ click လုပ်ပြီးသွားပါ။ ၎င်းက Key အစုံများ ထုတ်နေချိန်တွင် အသုံးပြုသော Settings များကို အခြေခံကျကျ ပြသပေးသည်။

မှတ်ချက် ။ ။ OpenPGP Setup Wizard ကို အသုံးပြု၍ ထုတ်ယူသော key အစုံများသည် 2048-bit ပုံစံကို အခြေခံထားသည်။ သက်တမ်းအားဖြင့် 5 နှစ်ခန့် ကြာရှည်သည်။ ဤနည်းလမ်းကို အသုံးပြု၍ ထုတ်ယူသော မည်သည့် key အစုံ လိုက်၌မဆို ဤလက္ခဏာရပ်နှစ်ခုစလုံး မပြောင်းလဲနိုင်ပါ။

4.2.2 Key အစုံများ ထပ်မံထုတ်ယူပုံနှင့် အခြားအီးမေးအကောင့်အတွက် တရားဝင် သတ်မှတ်ချက်အား ပယ်ဖျက်ခြင်း

အီးမေးလ်အကောင့် တစ်ခုစီအတွက် Key တစ်စုံစီ ရရှိရန်မှာ စံသတ်မှတ်ချက် ဖြစ်သည်။ သင်၏ အခြား အီးမေးလ်အကောင့်များအတွက် Key အစုံများ ထပ်မံထုတ်ယူရန် အောက်ပါအတိုင်း လိုက်၍ ဆောင်ရွက်ပါ။ Key တစ်စုံထုတ်ယူခြင်းတွင် ၎င်း Key အစုံနှင့်အတူ တရားဝင် သတ်မှတ်ချက်အား ပယ်ဖျက်ခြင်း (revocation certificate) တစ်ခု ပါရှိသည်။ ၎င်း certificate ကို သင်နှင့် ဆက်သွယ်သူထံသို့ ပို့၍ အကယ်၍ ၎င်း Key ကို access မလုပ်နိုင်သည့်အခါ (သို့) သင်၏ လျှို့ဝှက် Key ချို့ယွင်းသွားသည့်အခါ သင်၏ အများဆိုင် Key အသုံးပြုမှုကို disable ပြုလုပ်နိုင်းပါ။

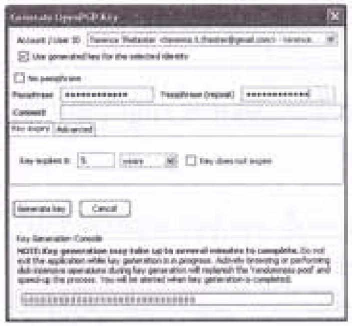
အဆင့် 1: အောက်ပါ screen ကို လုပ်ဆောင်ရန် Open PGP>Key Management ကို ရွေးပါ။



ပုံ 16: Key အစုံ အသစ်ရွေးထားသော Open PGP Key Management Generate Menu ပုံ

မှတ်ချက် ။ ။ 'Display All Keys by Default' option ကို check လုပ်ပါ။ ၎င်း၌ ပုံ 16: တွင် ဖော်ပြထားခဲ့သည့်အတိုင်း သင်၏ ပထမ အီးမေးလ်အကောင့်အတွက် OpenPGP Setup Wizard ကို အသုံးပြု၍ ထုတ်ပေးထားသော Key အစုံကို ကြည့်နိုင်သည်။

အဆင့် 2: ပုံ 16: တွင် ဖော်ပြထားသည့်အတိုင်း key အစုံသစ် ထုတ်ယူရန် Key Management မှ Generate>New Key Pair ကို ရွေးပါ။

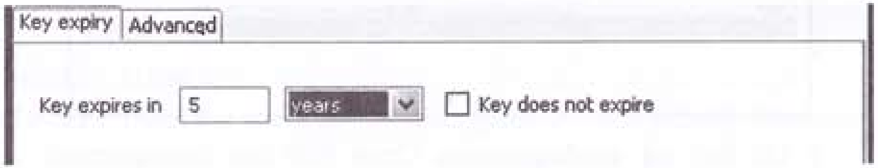


ပုံ 17: Generate OpenPGP Key screen ပုံ

အဆင့် 3: အကောင့် (သို့) အသုံးပြုသူ ID ၏ drop-down list မှ အီးမေးလ် အကောင့်တစ်ခုရွေးပါ။ 'Use generated key for the selected identity' option ကို check လုပ်ပါ။ သင်၏ လျှို့ဝှက် key ကို ကာကွယ်ရန် passphrase တစ်ခု ဖန်တီးပါ။

မှတ်ချက် ။ ။ 'passphrase' ဆိုသည်မှာ password အရှည်တစ်ခုကို သွယ်ဝိုက်သော နည်းဖြင့် ခေါ်ဆိုခြင်း ဖြစ်သည်။ Enigmail က သင့်အား သာမန်ထက်ပို၍ လုံခြုံမှုရှိပြီး ရှည်လျားသော password ကို ထည့်သွင်းရန် သတိပေးထားသည်။

အရေးကြီး ။ ။ Key အစုံများကို passphrase ရှိမှသာ ထုတ်ယူနိုင်သည်။ ထို့ကြောင့် 'no passphrase' option ကို .enable လုံးဝ မလုပ်ပါနှင့်။

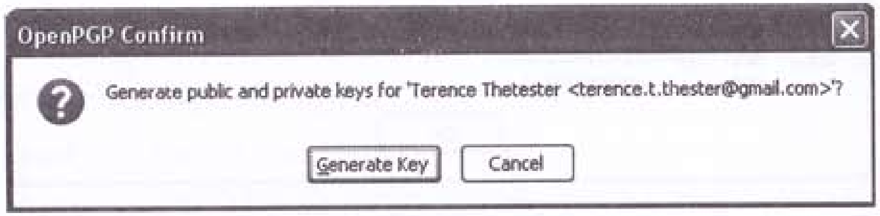


ပုံ 18: Key Expiry tab ကို ပြထားသော OpenPGP Key

မှတ်ချက် ။ ။ Key တစ်စုံသည် မည်မျှအချိန်ကြာကြာ ရေရှည်ခံသည်ကို ကြည့်ရန်မှာ သင်၏ မူပိုင်ခွင့်နှင့် လုံခြုံရေးလိုအပ်ချက်များပေါ်တွင် လုံးဝ မှီခိုနေသည်။ သင်၏ Key အစုံကို မကြာခဏ ပြောင်းလေလေ ၎င်း Key အသစ်ကို လိုက်လျောညီထွေဖြစ်အောင် လုပ်ရန် ခက်ခဲလေလေဖြစ်သည်။ သို့သော် သင်၏ Key အစုံကို အသစ်ပြောင်းသည့်အခါတိုင်း သင်နှင့်စာပေးစာယူဆက်သွယ်သူများထံသို့ ၎င်း Key အစုံကို ပို့ပြီး တစ်ခုစီကိုလည်း ခွဲခြားပေးရမည်။

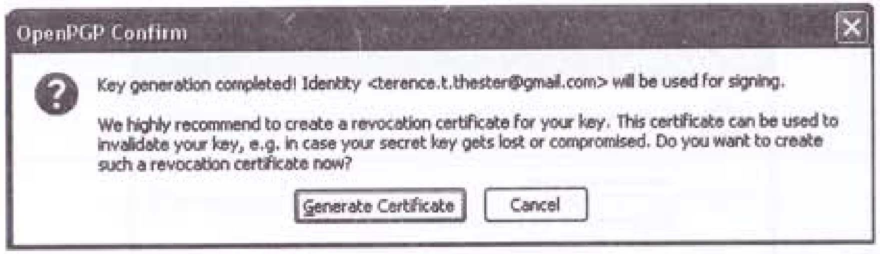
အဆင့် 5: ဆီလျော်သော နံပါတ် ရိုက်ပါ။ ထို့နောက် Key အစုံ တရားဝင်ရှိရမည့် အလိုရှိသော အချိန်ကာလ (ရက်၊ လ၊ နှစ် စသည်) ကိုရွေးပါ။

အဆင့် 6: အောက်ပါ screen သို့ clcik လုပ်ပြီးသွားပါ။



ပုံ 19: OpenPGP Confirm dialog box ပုံ

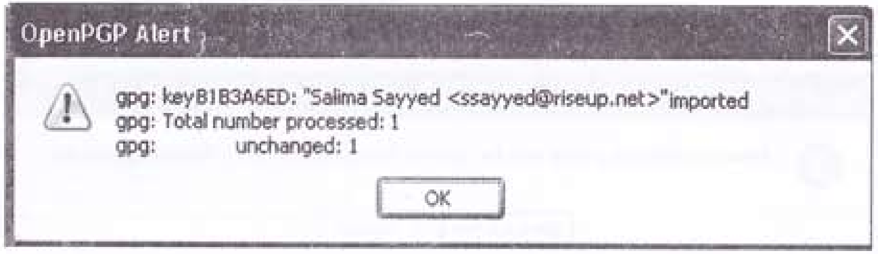
အဆင့် 7: အောက်ပါ screen သို့ click လုပ်ပြီးသွားပါ။



ပုံ 20: OpenPGP Prompt confirmation dialog box ပုံ

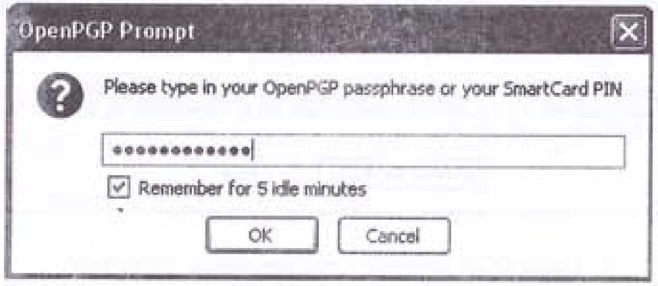
အဆင့် 8: 'Create & Save Revocation Certificate' navigation window ကို click လုပ်ပြီးသွားပါ။

မှတ်ချက် ။ ။ အကယ်၍ ရန်သူ (သို့) အတိုက်အခံအဖွဲ့အစည်းမှ ခွင့်ပြုချက်မရဘဲ access လုပ်မှုကြောင့် သင်၏အများဆိုင် Key (သို့) ၎င်း Key ကို access လုပ်ရန် ဆုံးရှုံးခြင်းများကို သင်သိရပါက သင်နှင့် ဆက်သွယ်သူများထံသို့ တရားဝင် သတ်မှတ်ခြင်းအား ပယ်ဖျက်ခြင်းပုံစံ (revocation certificate) ကို ပို့လွှတ်ပြီး သင့် အများဆိုင် Key ကို အသုံးမပြုတော့ရန် အသိပေးသင့်သည်။ သင်၏ ကွန်ပျူတာ ပျောက်ဆုံးခြင်း၊ အခိုးခံရခြင်းနှင့် ပျက်စီးခြင်းများ ဖြစ်ပွားမှသာ ဤသို့ ပြုလုပ်ရန်လည်း မှတ်သားထားပါ။ သင်၏ revocation certificate ကို ကာကွယ်ပေးရန်နှင့် မူပွားတစ်ခု ပြုလုပ်ထားရန်လည်း အကြံပေးပါသည်။



ပုံ 21: OpenPGP Alert confirmation screen ပုံ

အဆင့် 9: အောက်ပါ screen ကို လုပ်ဆောင်ရန် click လုပ်ပါ။ ဤအကြောင်းနှင့် တွဲဖက်လျက်ပါရှိသော သင်၏ passphrase ကို ရိုက်ထည့်ပါ။



ပုံ 22: Key အစုံ ထုတ်ယူခြင်း လုပ်ဆောင်ရာ၌ 'Please Type In Your Open PGP passphrase' option ကို တွေ့ရပုံ

အဆင့် 10: Key အစုံနှင့် revocation certificate ထုတ်ယူခြင်း လုပ်ငန်းစဉ်ပြီးဆုံးရန် click လုပ်ပါ။ အောက်ပါ screen သို့ ပြန်သွားပါ။

မှတ်ချက် ။ ။ သင့်ပတ်ဝန်းကျင် အခြေအနေသည် လုံးဝ လုံခြုံစိတ်ချရသည်ဟု ဆိုပါက 'Display All Keys by Default' option ကို check လုပ်၍ Key အစုံအားလုံးနှင့် ၎င်းတို့၏ အကြောင်းများကို ကြည့်ရှုနိုင်သည်။

သင်၏ Key အစုံနှင့် revocation certificate များကို အောင်မြင်စွာ ထုတ်ယူပြီးပါက အများဆိုင် key များကို ယုံကြည်စိတ် ချရသော ဆက်သွယ်သူနှင့် လဲလှယ်ယူရန် အဆင်သင့်ဖြစ်ပြီဟု ထင်ပါသည်။

4.2.3 သင်၏ အီးမေးလ်အကောင့်နှင့်အတူ အသုံးပြုရန်အတွက် Enigmail ကို စီမံဆောင်ရွက်ပုံ

သီးခြားအီးမေးလ်အကောင့်တစ်ခုနှင့် Enigmail ကို တွဲဖက်အသုံးပြုရန် အောက်ပါအဆင့်များ ဆောင်ရွက်ပါ။

အဆင့် 1: Tools>Account Settings ကို ရွေးပါ။

အဆင့် 2: အောက်ပါအတိုင်း sidebar အတွင်းရှိ OpenPGP Security menu ကို ရွေးပါ။

ပုံ 23: Account Settings-OpenPGP Security screen

အဆင့် 3: 'Enable OpenPGP supoort' option ကို check လုပ်ပါ။ ပုံ 11 တွင် ပြထားသည့်အတိုင်း OpenPGP key ကို ခွဲခြားရန် 'Use email address of this identity to identify OpenPGP Key' option ကို ရွေးပါ။

အဆင့် 4: Thunderbird console သို့ ပြန်သွားရန် click လုပ်ပါ။

4.3 အများဆိုင် Key များလဲလှယ်ပုံ

သင်တို့ တစ်ဦးနှင့်တစ်ဦး ဝှက်စာအသွင်ပြောင်း အီးမေးလ်သတင်းများ ပေးပို့ခြင်း မပြုခင် သင်နှင့် သင်၏ ဆက်သွယ်သူသည် အများဆိုင် key များကို လဲလှယ်ကြရမည်။ သင်လက်ခံရရှိသော key များသည် ၎င်းအားပေးပို့သူ အမှန်တကယ် ပိုင်ဆိုင်သော key များဖြစ်ပြီး ၎င်းတို့၏ သက်တမ်းကိုလည်း သေချာအောင် ပြုလုပ်ထားရမည်။

4.3.1 Enigmail ကို အသုံးပြု၍ အများဆိုင် key ပို့လွှတ်ပုံ

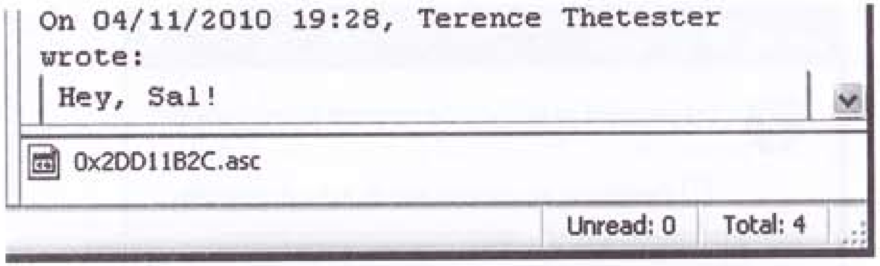
Enigmail/OpenPGP ကို အသုံးပြု၍ အများဆိုင် key ပို့လွှတ်ရန် သင်နှင့် သင်ဆက်သွယ်မည့်သူ နှစ်ဦးစလုံးသည် အောက်ပါအတိုင်း ဆောင်ရွက်ရမည်။

အဆင့် 1: Thunderbird ကို ဖွင့်ပြီး သတင်းပို့ချက် (message) အသစ်တစ်ခုရေးရန် click လုပ်ပါ။

အဆင့် 2: Attach File(s) window ကို လုပ်ဆောင်ရန် File>Attach>File(s) ကို click (သို့) ရွေးပါ။ သင်၏ အများဆိုင် key ထံသို့သွားပြီး ၎င်းကို တွဲယူရန် click လုပ်ပါ။ အောက်ပါ screen ကို တွေ့ရမည်။

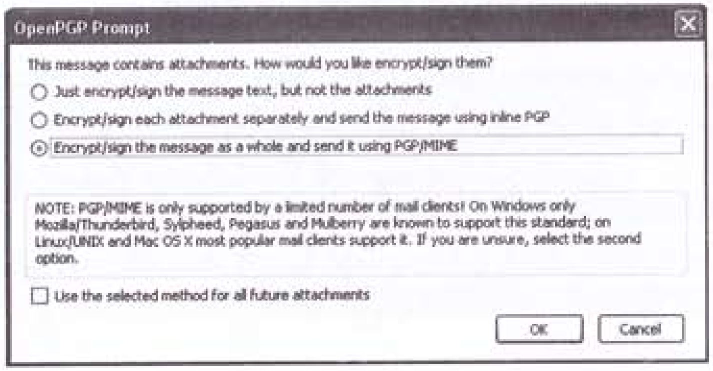
ပုံ 24: Attachments pane၌ တွဲယူထားသော အများဆိုင် keyကို ပြထားသောသတင်းရေးရန် နေရာပြပုံ

မှတ်ချက် ။ ။ သင်၏ အများဆိုင် key ကို OpenPGP>Attach My Public Key အား ရွေးချယ်၍လည်း တွဲယူနိုင်သည်။ သို့သော် ဤနည်းလမ်းမှာ Attachments pane ၌ ဖော်ပြခြင်းမရှိဘဲ သင်နှင့် ဆက်သွယ်သူ၏ message pane အောက်ခြေတွင် အောက်ပါအတိုင်း ပေါ်လာလိမ့်မည်။



ပုံ 25: OpenPGP ရှိ 'Attach my Public Key' item ကို အသုံးပြု၍ တွဲယူထားသော အများဆိုင် Key တစ်ခု၏ဥပမာပြပုံ

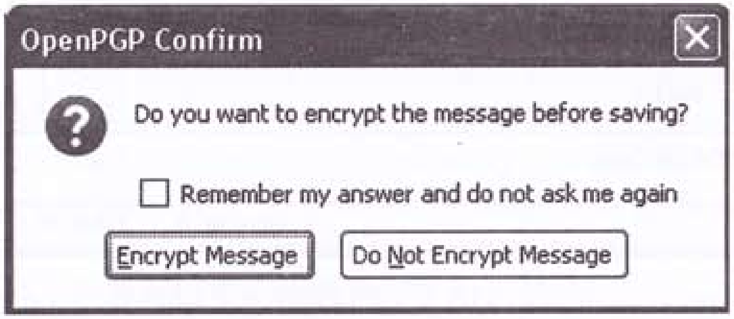
အဆင့် 3: အောက်ပါ screen ကို လုပ်ဆောင်ရန် အများဆိုင် key တွဲယူထားသော သင်၏ အီးမေးလ်ကို ပို့လွှတ်ရန် click လုပ်ပါ။



ပုံ 26: ဝှက်စာအသွင်ပြောင်းခြင်း (encryption) နှင့် အမှတ်အသားပြုခြင်း (signing) mode ကို ပြင်ဆင်ခြင်းအတွက်ဖော်ပြသော OpenPGP Prompt screen

အဆင့် 4: Encrypt/Sign message ကို option တစ်ခုလုံး check လုပ်ပါ။ ပုံ 23: ကို လုပ်ဆောင်ရန် click လုပ်ပါ။

အဆင့် 5: သင်၏ passphrase ဝင်ရောက်ပါ။ အောက်ပါ screen သို့သွားရန် click လုပ်ပါ။



ပုံ 27: OpenPGP prompt- သတင်းပို့ချက်ကို သိမ်းဆည်းခြင်းမပြုမီ ဝှက်စာ အသွင်ပြောင်းလို၊ မပြောင်းလို မေးမြန်းသည့် screen

အဆင့် 6: ဝှက်စာပြောင်းခြင်း၊ အမှတ်အသားပြုခြင်းနှင့် သတင်းပို့ရန် click လုပ်ပါ။

4.3.2 Enigmail ကို အသုံးပြု၍ အများဆိုင် key ကို တင်ပို့ပုံ

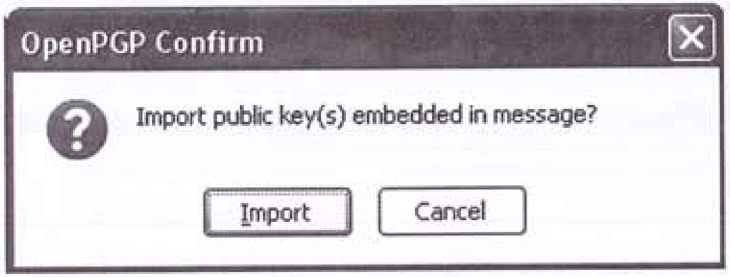
သင်နှင့် စာပေးစာယူ ဆက်သွယ်မည့်သူနှင့် သင်တို့ နှစ်ဦးစလုံးသည် အများဆိုင် key များ တင်ပို့သည့်အခါ တူညီသောအဆင့်များ ဆောင်ရွက်ရမည်။

အဆင့် 1: သင့်ဆက်သွယ်သူ၏ အများဆိုင် key ပါဝင်သော အီးမေးလ်ကို ရွေးချယ်ပြီး ဖွင့်ပါ။

သင်ဆက်သွယ်မည့်သူ၏ အများဆိုင် key ကို အီးမေးလ်ထဲတွင် မြှုပ်ထားပါက 'Decrypt' ခလုတ်ကို enable လုပ်ရမည်။ သင်၏ 'message pane' ၌ အောက်ပါအတိုင်း ပေါ်လာလိမ့်မည်။

ပုံ 28: messgaeအတွင်း၌ အများဆိုင် key ထည့်သွင်းရန် 'Decrypt' ခလုတ်ကို နှိပ်ပါ။

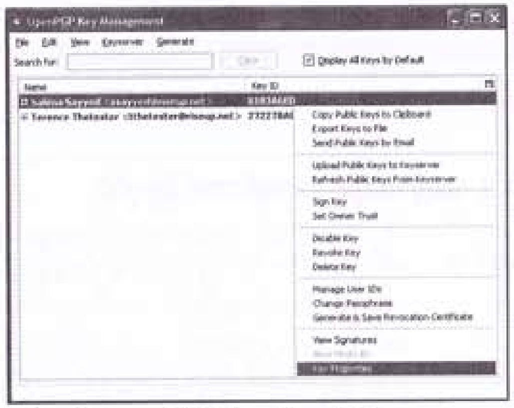
အဆင့် 2: ဝှက်စာအသွင်ပြောင်း data များအတွက် လက်ခံရရှိသော သတင်းပို့ချက်တွင် ပါဝင်သည့် အကြောင်းအရာများကို အလိုအလျောက် scan ဖတ်ရှုနိုင်ရန် click လုပ်ပါ။ Enigmail/OpenPGP မှ အများဆိုင် key ပါဝင်သော message ကို ရှာတွေ့ပြီးပါက သင့်အား key များ တင်ပို့ရန် သတိပေးချက် အောက်ပါအတိုင်း ပေါ်လာလိမ့်မည်။



ပုံ 29: Message အတွင်း၌ public key မြှုပ်နှံထားခြင်း ရှိ၊ မရှိ အတည်ပြုပေးသည့် OpenPGP

အဆင့် 3: သင်ဆက်သွယ်မည့်သူ၏ အများဆိုင် key ကိုတင်သွင်းရန် click လုပ်ပါ။

အများဆိုင် key ကို အောင်မြင်စွာ တင်သွင်းပြီးပါက အောက်ပါ သတင်းပို့ချက် တစ်ခုပေါ်လာလိမ့်မည်။



ပုံ 30: သင့်ဆက်သွယ်သူ၏ အများဆိုင် key ကို ဖော်ပြထားသော OpenPGP အချက်ပေး screen ပုံ

သင်ဆက်သွယ်မည့်သူ၏ အများဆိုင် key ကို လက်ခံရရှိပြီးကြောင်း အတည်ပြုချက်ယူရန် အောက်ပါအဆင့်များ ဆောင်ရွက်ပါ။

အဆင့် 1: OpenPGP ၏ key စီမံမှုဆိုင်ရာ screen ကို ဖော်ပြရန် OpenPGP> Key Management ကို ရွေးပါ။

ပုံ 31: လတ်တလော တင်ပို့ထားသော အများဆိုင် key အား ပြသထားသည့် OpenPGP ၏ Key Management screen

4.4 Key တစ်စုံကို တရားဝင်အောင် ပြုလုပ်ပုံနှင့် အမှတ်အသားပြုလုပ်ပုံ

နောက်ဆုံးတွင် တင်ပို့လိုက်သော key တို့သည် ၎င်းအား အတိအကျ ပေးပို့လိုက်သော ပုဂ္ဂိုလ်မှ အသေအချာပိုင်ဆိုင်ကြောင်းကို သင်က ခွဲခြားပေးရမည်။ ထို့နောက် ၎င်း key ၏ အရည်အသွေး စစ်မှန်မှုကို စစ်ဆေးရမည်။ ဤအဆင့်တွင် သင်နှင့်တကွ သင်၏ အီးမေးလ်ဆက်သွယ်သူများသည် လက်ခံရရှိသော အများဆိုင် key တစ်ခုစီကို စစ်ဆေးရမည်ဖြစ်သောကြောင့် အရေးကြီးသောအဆင့် ဖြစ်သည်။

4.4.1 Key တစ်စုံကို တရားဝင်အောင် ပြုလုပ်ပုံ

အဆင့် 1: သင်နှင့် စာပေးစာယူဆက်သွယ်မည့်သူထံသို့ အီးမေးလ်ဖြင့် မဟုတ်ဘဲ အခြားတစ်နည်းနည်းဖြင့် ဆက်သွယ်ပါ။ တယ်လီဖုန်း၊ စာတိုပေးပို့ခြင်း၊ အင်တာနက်မှတစ်ဆင့် စကားပြောဆက်သွယ်ခြင်း (VoIP) သို့မဟုတ် အခြားနည်းလမ်းများ အသုံးပြုပါ။ သင်စကားပြောဆိုမည့်သူသည် သင်တွေ့လိုသောသူဖြစ်ကြောင်း သေချာရမည်။ သင်နှင့် တွေ့ဆုံမည့် သူဘက်မှ အဆင်ပြေပြီး ပတ်ဝန်းကျင်ကိုလည်း လုံခြုံစိတ်ချရအောင် စီစဉ်နိုင်မည်ဆိုပါက ဖုန်းဖြင့်စကားပြောခြင်း၊ မျက်နှာစုံညီ တွေ့ဆုံဆွေးနွေးခြင်းတို့မှာ အကောင်းဆုံးဖြစ်သည်။

အဆင့် 2: သင်နှင့် သင်စာပေးစာယူ ပြုလုပ်မည့်သူ နှစ်ဦးစလုံးသည် သင်တို့ချင်း လဲလှယ်ထားသော အများဆိုင် key များ၏ သက်သေအမှတ်အသား 'fingerprints' ကို ခွဲခြားစစ်ဆေးရမည်။ "Finger print" ဆိုသည်မှာ key တစ်ခုစီကို ခွဲခြားသတ်မှတ်ရန် ပြုလုပ်ထားသည့် ညီညွတ်သော ကိန်းဂဏန်းနှင့် အက္ခရာအစုအဝေး တစ်ခုဖြစ်သည်၊ သင် တင်ပို့လိုက်သော အများဆိုင်ရာ Key နှင့် သင် ဖန်တီးထားသော Key အစုံများ၏ 'finger-print' ကို ကြည့်ရှုရန် 'OpenPGP Key Management' screenကို အသုံးပြုနိုင်သည်။

Key အစုံတစ်ခု၏ 'finger print' ကို ကြည့်ရှုရန် အောက်ပါအဆင့်များ ဆောင်ရွက်ပါ။

အဆင့် 1: OpenPGP >Key Management ကို ရွေးပါ။ Key တစ်ခုပေါ်၌ right-click နှိပ်ပါ။ pop-up menu တစ်ခု ပေါ်ထွက်လာလိမ့်မည်။

ပုံ 32: Key Properties ကို ရွေးချယ်ပြသထားသော OpenPGP Key Management menu ပုံ

အဆင့် 2: အောက်ပါ screen ကို လုပ်ဆောင်ရန် Key Properties ကို ရွေးပါ။ သင်နှင့် ဆက်သွယ်မည့်သူသည်လည်း ဤအဆင့်များကို လုပ်ဆောင်ရမည်။

ပုံ 33: Key Properties screen ပုံ

သင်တို့ နှစ်ဦးအလဲအလှယ်ပြုလုပ်ထားသော key များ၏ 'fingerprint' သည် ပေးပို့သူ၏ မူလ 'fingerprint' နှင့် ကိုက်ညီမှု ရှိ၊ မရှိ စစ်ဆေးပါ။ အကယ်၍ ကိုက်ညီမှုမရှိပါက သင်တို့၏ အများဆိုင် key များကို ထပ်မံလဲလှယ်ပြီး တရားဝင်ဖြစ်အောင် ပြုလုပ်ခြင်း။ လုပ်ငန်းစဉ်ကို ပြန်လည်လုပ်ဆောင်ပါ။

မှတ်ချက် ။ ။ 'finger print' ကို လျှို့ဝှက်ချက်တစ်ခုအဖြစ် သတ်မှတ်ထားခြင်းမရှိဘဲ နောက်ပိုင်း ခွဲခြားစစ်ဆေးမှုများတွင် သင် အဆင်ပြေမှုရှိအောင် record လုပ် ထားနိုင်သည်။

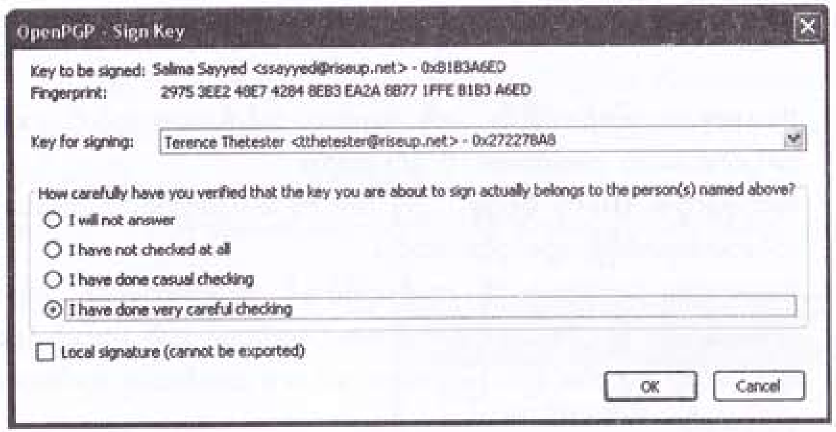
4.4.2 တရားဝင် အများဆိုင် Key တစ်ခုကို အမှတ်အသားပြုလုပ်ပုံ

သင်ဆက်သွယ်သည့်သူမှ ပေးပို့လိုက်သော Key သည် သေချာသော ကိုက်ညီမှု ရှိကြောင်း သင်ယူဆပါက ၎င်းကို အမှတ်အသားပြု (sign) ရမည်။ ထိုမှသာ ဤ key ကို တရားဝင်သည်ဟု သတ်မှတ်သည်။

တရားဝင် အများဆိုင် Key တစ်ခုကို အမှတ်အသားပြုရန် အောက်ပါအဆင့်များ ဆောင်ရွက်ပါ။

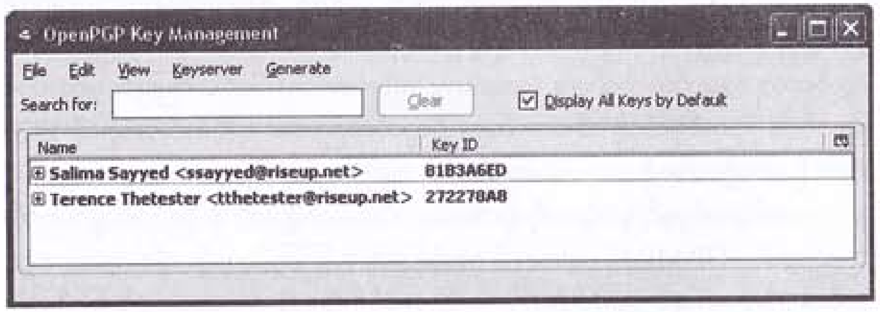
အဆင့် 1: Key Management screen သို့ ပြန်သွားရန် click လုပ်ပါ။

အဆင့် 2: သင်ဆက်သွယ်ထားသူ ပေးပို့လိုက်သော အများဆိုင် Key ကို right click နှိပ်ပါ။ menu ရှိ Sign Key ကို ရွေးပါ။



ပုံ 34: OpenPGP-Sign Key screen ပုံ

အဆင့် 3: 'I have done very careful checking' option ကို check လုပ်ပါ။ သင် ဆက်သွယ်သူ၏ Key ကို အမှတ်အသားပြုခြင်း ပြီးစီးရန် click လုပ်ပါ။ တရားဝင်ဖြစ်အောင် ဆောင်ရွက်ခြင်း လုပ်ငန်းစဉ် ပြီးဆုံးအောင် ဆောင်ရွက်ပါ။ OpenPGP Key Management window ကို ပြန်သွားပါ။



ပုံ 35: တရားဝင်သတ်မှတ်ပြီးသော Key အစုကို ပြထားသည့် OpenPGP Key Management screen

4.4.3 သင်၏ Key အစုကို စီမံဆောင်ရွက်ပုံ

OpenPGP Key Management window ကို Key အစုံများ ထုတ်ယူရန်၊ တရားဝင်ဖြစ်အောင် ပြုလုပ်ရန်နှင့် အမှတ်အသားပြုရန် အသုံးပြုသည်။ သို့သော် Key Management နှင့် ဆက်နွယ်သောအခြားလုပ်ဆောင်မှုများကို ဆောင်ရွက်ရဦးမည်။

* **Passphrase ပြောင်းလဲခြင်း** : ဤ item က သင်၏ Key အစုံကို အကာအကွယ်ပေးသော passphrase ကို ခွင့်ပြုသည်။
* **အသုံးပြုသူ၏ IDs ကို စီစဉ်မှု** : ဤ item က key အစုံတစ်ခုသို့ အီးမေးလ်လိပ်စာတစ်ခုထပ်ပို၍ တွဲစပ်ခွင့်ပေးသည်။
* **Revocation Certificate ကို ထုတ်ယူခြင်းနှင့် သိမ်းဆည်းခြင်း** : ၎င်းက သင်အစောပိုင်း ပြုလုပ်ခဲ့သော Revocation Certificate သည် မှားယွင်းနေရာချမိခြင်း (သို့) ပျောက်ဆုံးခြင်း ဖြစ်ပွားပါက သင့်အား အသစ်တစ်ခု ထုတ်ပေးရန် ခွင့်ပြုသည်။

4.5 အီးမေးလ်သတင်းပို့ချက်ကို ဝှက်စာအသွင်ပြောင်းခြင်း၊ ဝှက်စာဖြည်ခြင်းများ ပြုလုပ်ပုံ

အရေးကြီး ။ ။ အီးမေးလ် သတင်းပို့ချက် တစ်ခု၏ခေါင်းစဉ် (၎င်းတွင် အကြောင်းအရာနှင့် ပေးပို့လိုသော သူ၏ အမည်ပါဝင်ပြီး အချက်အလက်များပါဝင်သော To၊ CC နှင့် BCC fields များလည်း ပါရှိသည်) ကို ဝှက်စာအသွင်ပြောင်းခြင်း မပြုနိုင်ဘဲ open text တစ်ခုအဖြစ်သာ ပို့လွှတ်နိုင်သည်။ သင်၏ အီးမေးလ်ပို့ဆောင်မှုများ၏ မူပိုင်ခွင့်နှင့် လုံခြုံရေးအတွက် သေချာမှုရှိစေရန် သင့်အီးမေးလ်၏ ခေါင်းစဉ်၌ ထိခိုက်လွယ်သော အချက်အလက်များ (sensitive information) ပါဝင်ဖော်ပြခြင်း မရှိအောင် ပြုလုပ်ပါ။ လူတစ်စုထံသို့ အီးမေးလ်များ ပို့လွှတ်သည့်အခါ လိပ်စာအားလုံးကို BCC field ၌ ထည့်ထားရန် လေးလေးနက်နက် အကြံပြုပါသည်။

တစ်စုံတစ်ခုနှင့် ပူးတွဲပေးပို့လိုက်သော အီးမေးလ်များကို ဝှက်စာ အသွင်ပြောင်းသည့်အခါ PGP/MIME option ကို အသုံးပြုရန် အကြံပြုပါသည်။ ၎င်း optionသည် သင်၏ အီးမေးလ်နှင့် ပူးတွဲပါရှိသော မည်သည့်ဖိုင်ကိုမဆို ဝှက်စာအသွင်ပြောင်းခြင်း လုပ်ပေးသည်။

4.5.1 သတင်းတစ်ခုကို ဝှက်စာအသွင်ပြောင်းပုံ

သင်နှင့် သင်ဆက်သွယ်သူနှစ်ဦးစလုံးတို့သည် တစ်ဦးစီ၏ အများဆိုင် key များကို တရားဝင်အောင် ပြုလုပ်ခြင်း၊ အမှတ်အသားပြုခြင်းနှင့် တင်ပို့ခြင်းများ ပြုလုပ်ပြီးပါက ဝှက်စာအသွင်ပြောင်း သတင်းများပေးပို့ခြင်း၊ ဝှက်စာဖြည်ပြီးသော သတင်းများ လက်ခံခြင်းတို့ကို စတင်ဆောင်ရွက်နိုင်ပါပြီ။

သင်နှင့် သင်ဆက်သွယ်မည့်သူထံသို့ ပေးပို့မည့် သင်၏ အီးမေးလ်သတင်း၌ ပါဝင်သော အကြောင်းအရာများကို ဝှက်စာအသွင်ပြောင်းရန် အောက်ပါအဆင့်များ ဆောင်ရွက်ပါ။

အဆင့် 1: သင်၏ အီးမေးလ်အကောင့်ကို ဖွင့်ပြီး အီးမေးလ်တစ်စောင်ရေးရန် click လုပ်ပါ။

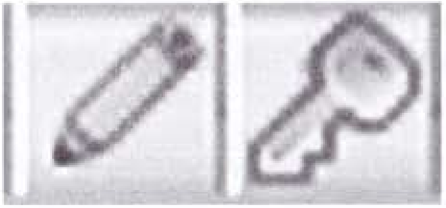
ပုံ 36: OpenPGP Encryption pop-up window ပုံ

အဆင့် 2: အောက်ပါ screen ကို လုပ်ဆောင်ရန် click လုပ်ပါ။

မှတ်ချက် ။ ။ Encrypt/ Sign option တစ်ခုလုံးကို check လုပ်ထားပါက PGP/MIME အသုံးပြု၍ ပုံ 28: ပါအတိုင်း စာပို့ပါ။ ပုံ 35 ပါအဆင့်ကို တွေ့ရမည် မဟုတ်ပါ။

အဆင့် 3: ပုံ 32: တွင် ဖော်ပြထားသည့်အတိုင်း Sign Message နှင့် Encrypt Message option များကို check လုပ်ပါ။ ထို့နောက် သင့် အီးမေးလ်အတွက် ဝှက်စာအသွင်ပြောင်းခြင်းနှင့် အမှတ်အသားပြုလုပ်ခြင်း လုပ်ငန်းစဉ် ပြီးစီးအောင် click လုပ်ပါ။

မှတ်ချက် ။ ။ သင်၏ သတင်းပို့ချက်သည် အမှတ်အသားပြုခြင်းနှင့် အသွင်ပြောင်းခြင်းနှစ်ခုစလုံး ပြုလုပ်ပြီး၊ မပြီး ခွဲခြားစစ်ဆေးပါ။ Message pane ၏ အောက်ခြေညာဘက်ထောင့်တွင် ၎င်း icon နှစ်ခု ပေါ်လာမလာကို ကြည့်ပါ။

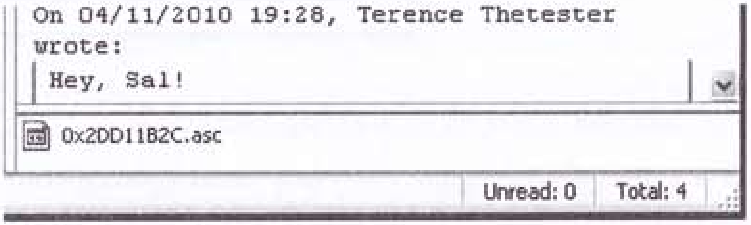


ပုံ 37: Message Signing and Encry-ption Confirmation icons များ ပုံ

အဆင့် 4: သတင်းပို့ချက်ကို စေလွှတ်ရန် click လုပ်ပါ။ ၎င်းသတင်းကို အမှတ်အသားပြုရန် သင်၏ လျှို့ဝှက် key ကို အသုံးပြုဖို့ရာ password တောင်းသည့် သတိပေးချက်ပေါ်လာလိမ့်မည်။

4.5.2 သတင်းပို့ချက်တစ်ခုကို ဝှက်စာဖြည်ခြင်း ပြုလုပ်ပုံ

ဝှက်စာအသွင်ပြောင်းထားသော သတင်းတစ်ခုကို သင်လက်ခံရရှိပြီး ဖွင့်ကြည့်သောအခါ Enigmail/ OpenPGP က ၎င်းသတင်းကို အလိုအလျောက်ဝင်ရောက်၍ ဝှက်စာဖြည်ပေးလိမ့်မည်။ ၎င်းကို အောက်ပါ screen တွင် တွေ့ရမည်။



ပုံ 38: သင်၏ Smart Card PIN နံပါတ် (သို့) သင်၏ OpenPGP passphrase ရိုက်ထည့်ရန် တောင်းဆိုသော OpenPGP Prompt

အဆင့် 1: ပုံ 38: တွင် ပြထားသည့်အတိုင်း သင်၏ 'passphrase' ကို ရိုက်ထည့်ပါ။

သင့်လျှို့ဝှက် Key ၏ passphrase ကို ရိုက်ထည့်ပြီးပါက သင်၏ သတင်းကို ဝှက်စာဖြည်၍ ဖော်ပြသည်။

သင်သည် ဤသတင်းပို့ချက်ကို အောင်မြင်စွာ ဝှက်စာဖြည်ပြီးပါပြီ။ သင်နှင့်ဆက်သွယ်မည့်သူတို့ သတင်းပို့ချက်များ အပြန်အလှန်ပြုလုပ်တိုင်း အပိုင်း 4.5 တွင်

ဖော်ပြထားသော အဆင့်များကို ပြန်လည်ဆောင်ရွက်ခြင်းဖြင့် သင်၏ အီးမေးလ်ပို့ဆောင်မှုများကို တစ်စုံတစ်ယောက်မှ ချောင်းမြောင်းကြည့်ရှုမည်ကို မစိုးရိမ်ရဘဲ လျှို့ဝှက်၍ စစ်မှန်သော ဆက်သွယ်ရေးလမ်းကြောင်းတစ်ခုကို ရရှိနိုင်ပါသည်။

5.0 မကြာခဏမေးလေ့ရှိသော မေးခွန်းများနှင့်အဖြေများ

ကလော်ဒီယာနှင့် ပါဘလိုတို့သည် ၎င်းတို့၏ RiseUp အကောင့်မှတစ်ဆင့် အီးမေးလ်ပို့ခြင်း၊ လက်ခံခြင်း ပြုလုပ်ရန် Mozilla Thunderbird ကို စီမံဆောင်ရွက်ထားကြသည်။ ၎င်းတို့၏ အီးမေးလ်ကို စစ်ဆေးပြီးနောက် အင်တာနက် ဆက်သွယ်မှုမရှိသော်လည်း သတင်းပို့ချက်ကို ဆက်လက်ဖတ်ရှုနိုင်ခြင်းကို များစွာသဘောကျကြသည်။

များမကြာမီပင် ကလော်ဒီယာနှင့် ပါဘလိုတို့သည် GnuPG နှင့် Enigmail တို့ကို install လုပ်၍ သက်ဆိုင်ရာ Key အစုံများ ပြုလုပ်ခြင်း၊ အများဆိုင် key များ လဲလှယ်ခြင်းနှင့် 'fingerprints' များ နှိုင်းယှဉ်၍ key တစ်ခုစီကို တရားဝင်ဖြစ်အောင် ပြုလုပ်ခြင်းများ လုပ်ကြသည်။

အများဆိုင် key များကို စာအသွင်ပြောင်းခြင်းအတွက် ရှုပ်ထွေးမှုများကို နားလည်ရန် အချိန်ယူရသော်လည်း ၎င်းတို့နှစ်ဦးသည် အသွင်ပြောင်းနိုင်သော လုံခြုံစိတ်ချရသည့် ဆက်သွယ်ရေးလမ်းကြောင်းတစ်ခု ရရှိခြင်း၏ အကျိုးကျေးဇူးကို ကျေနပ်အားရလျက်ရှိသည်။ ဆော့ဖ်ဝဲအသစ်များတွင် ကြုံလေ့ရှိသည့်အတိုင်း ၎င်းတို့တွင် မေးရန်မေးခွန်းများ ရှိနေကြသည်။

မေး ။ ။ GnuPG မပါဘဲ Enigmail ကိုပဲ install လုပ်လျှင် ဘာဖြစ်မလဲ။

ဖြေ ။ ။ ရိုးရိုးလေးပါပဲ။ Enigmail က လုံးဝ အလုပ်မလုပ်နိုင်ပါဘူး။ တကယ်တော့ Enigmail အသုံးပြုတဲ့ ဝှက်စာအသွင်ပြောင်းစက်ဟာ GnuPG ဆော့ဖ်ဝဲက ထုတ်ပေးထား တာပါ။

မေး ။ ။ Thunderbird မှာ အီးမေးလ်အကောင့် ဘယ်နှစ်ခုလောက် တပ်ဆင်အသုံးပြုနိုင်သလဲ။

ဖြေ ။ ။ သင်အလိုရှိသလောက် ဖြစ်နိုင်ပါတယ်။ Thunderbird ဟာ အီးမေးလ်များ စီမံဆောင်ရွက်သူ (manager) ဖြစ်ပြီး 20 (သို့) 20 ထက်ပိုတဲ့ အရေအတွက်ရှိတဲ့ အီးမေးလ်များကို ထိန်းသိမ်းထားနိုင်ပါတယ်။

မေး ။ ။ ကျွန်တော့်သူငယ်ချင်းမှာ Gmail အကောင့်တစ်ခုရှိပါတယ်။ သူ့ကို Thunderbird, Enigmail နဲ့ GnuPG များ install လုပ်ဖို့ တိုက်တွန်းသင့်ပါသလား။

ဖြေ ။ ။ ဒါဖြစ်နိုင်ပါတယ်။ သေချာအောင် လုပ်ရမှာတစ်ခုက သူ့ရဲ့ လုံခြုံရေးဆိုင်ရာ Settings တွေကို သင်လုပ်သလို တိတိကျကျ စီစဉ် ဆောင်ရွက်ထားနိုင်ဖို့ပါပဲ။ ဒါဆို သင်တို့ နှစ်ယောက်စလုံးရဲ့ မူပိုင်ခွင့်နဲ့ လုံခြုံရေးအတွက် အင်မတန် အကျိုးရှိတဲ့ ဆက်သွယ်ရေးနည်းလမ်းကို ရရှိမှာပါ။

မေး ။ ။ အီးမေးသတင်းရဲ့ ဘယ်အပိုင်းကို Enigmail က ဝှက်စာ အသွင်ပြောင်းတယ်ဆိုတာ နောက်တစ်ခေါက်လောက် ကျွန်တော့်ကို ပြောပြပါဦး။

ဖြေ ။ ။ Enigmail က သတင်းမှာပါတဲ့ အကြောင်းအရာကို ဝှက်စာ အသွင်ပြောင်းပါတယ်။ သတင်းရဲ့ ခေါင်းစဉ်ပိုင်းကိုတော့ အသွင်ပြောင်း မပေးပါဘူး။ သင့်ရဲ့ အီးမေးလ်လိပ်စာ ဒါမှမဟုတ် အီးမေးလ်အကောင့်နဲ့ တွဲဖို့ ရွေးထားတဲ့ အမည်စတာတွေပေါ့။ ဒါကြောင့် အတွင်းရေး ကိစ္စများပါဝင်တဲ့ သတင်းမျိုးပေးပို့မယ်ဆိုရင် ခေါင်းစဉ်ပိုင်းမှာ ပေါက်ကြားခြင်းမရှိအောင် ဂရုစိုက်ရပါမယ်။ အကယ်၍ သင့်အကြောင်းကို လူသိမခံချင်ဘူးဆိုပါက သင့်ရဲ့ အီးမေးလ်အကောင့်မှာ သင့်ရဲ့ အမည် အစစ်အမှန်ကို တောင်မှ မသုံးမပြုပါနဲ့။

မေး ။ ။ ကျွန်တော်ရဲ့ သတင်းပေးပို့ချက်များကို ဒီဂျစ်တယ်နည်းအရ အသိအမှတ်ပြု မှတ်သားရတဲ့ ရည်ရွယ်ချက်ကို အခုထိ နားမလည်သေးဘူး။

ဖြေ ။ ။ ဒီဂျစ်တယ်နည်းအရ ပြုလုပ်ထားတဲ့ အမှတ်အသားဆိုတာ သင်ဟာ သတင်းပို့ချက်တစ်ခုရဲ့ ပေးပို့သူ အစစ်အမှန်ဖြစ်ကြောင်းကို သက်သေပြပေးပြီး အဲဒီ သတင်းဟာ သင်ပို့လိုတဲ့ သူ့ဆီကို အရောက်ခင်လမ်းခရီးမှာ နှောင့်ယှက်ခြင်း မခံရကြောင်း ကိုလည်း ပြပါတယ်။ အရေးကြီးတဲ့ စာတစ်စောင်ပါဝင်တဲ့ စာအိတ်တစ်အိတ်ကို ဖယောင်းကပ်ပြီး ချိတ်ပိတ်တဲ့ ပုံစံမျိုးနဲ့ ခပ်ဆင်ဆင်တူပါတယ်။

5.1 မေးခွန်းသုံးသပ်ချက်

* သင့်ရဲ့ မိတ်ဆွေ တစ်ယောက်ဆီကို ဝှက်စာအသွင်ပြောင်းထားတဲ့ သတင်းမပို့ခင် ဘယ်ဆော့ဖ်ဝဲကို install လုပ်ပြီး ဘယ်လိုစီစဉ်ဆောင် ရွက်မလဲ။

* Thunderbird ကို အသုံးပြုပြီး သင့်ရဲ့ အီးမေးလ်ကို လုံလုံခြုံခြုံ access ဘယ်လိုလုပ်မလဲ။
* Thunderbird မှာ သင့်ရဲ့ အီးမေးလ်အကောင့် password ကို လုံခြုံအောင် ဘယ်လိုသိမ်းမလဲ။
* အန္တရာယ်ရှိတဲ့ အကြောင်းအရာများပါဝင်တဲ့ အီးမေးလ်များမှ သင့်ကိုယ်သင် ဘယ်လို ကာကွယ်မလဲ။
* သင့်ရဲ့ အီးမေးလ်ကို access လုပ်ရာမှာ အင်တာနက် ကွန်ရက်ရှာဖွေစက်ကို သုံးတာနဲ့ Thunderbird ပရိုဂရမ်ကို သုံးတာနှစ်ခုကြားမှာ ဘာကွာခြားချက် ရှိပါသလဲ။

ESSENTIAL SOFTWARES FOR YOUR COMPUTER

သင့် ကွန်ပျူတာ အတွက် မရှိမဖြစ် ဆော့ဖ်ဝဲများ