EFF'S SURVEILLANCE SELF-DEFENSE

Linux ကွန်ပျူတာစနစ်အသုံးပြုသူများအတွက် အချက်အလက်များ လုံခြုံစွာဖျက်နည်းလမ်းညွှန်

https://ssd.eff.org/en/about-surveillance-self-defense

LOCALIZATION LAB

Linux ကွန်ပျူတာစနစ်အသုံးပြုသူများအတွက် အချက်အလက်များ လုံခြုံစွာဖျက်နည်းလမ်းညွှန်

ကူးဆွဲရန်နေရာ - https://www.bleachbit.org/download/linux

လိုအပ်သောကွန်ပျူတာစနစ် - အဓိက Linux စနစ်အားလုံးအတွက်ဖြစ်သည်။ ဤလမ်းညွှန်တွင် Ubuntu ၁၈.၀၄ ကို ရည်ညွှန်းထားပါသည်။

ဤလမ်းညွှန်တွင်အသုံးပြုထားသော Version ပုံစံများ - BleachBit 2.0

လိုင်စင်- GPLv3

အဆင့်- အခြေခံ

ကြာချိန်- ၁၀ မိနှစ်မှ နာရီအနည်းငယ်အထိ (ဖျက်မည့် ဖိုင်နှင့် disk အရွယ်အစား ပေါ်မူတည်သည်)

နောက်ဆုံးစိစစ်ထားသည့်ရက်စွဲ - ၂၀၂၁ ခုနှစ် ဧပြီ ၂၉ ရက်

> ဒီလမ်းညွှန်မှာပါတဲ့ နည်းလမ်းတွေကို spinning drives အသုံးပြုတဲ့ကွန်ပျူတာတွေပေါ် သိမ်းဆည်းထားတဲ့ အချက်အလက်များ ဖျက်ပစ်ရန်အတွက်သာ အသုံးပြုသင့်ပါတယ်။ Spinning drive အစား Solid State Drives (SSDs) အသုံးပြုတဲ့ ခေတ်မီကွန်ပျူတာများ၊ USB သော့များ/ USB thumb drive များ၊ SD ကဒ်များ/ flash memory ကဒ်များအတွက် အသုံးမဝင်ပါ။ USB flash drive များ၊ SD ကဒ်များကဲ့သို့ SSD သုံးတဲ့စနစ်များတွေမှာ ဟောင်းနွမ်းပျက်စီးမှုဖြန့်ကျက်ခြင်း (wear leveling) နည်းပညာကို အသုံးပြုတဲ့အတွက် အချက်အလက်တွေကို လုံလုံခြုံခြုံဖျက်ပစ်ဖို့ ခဲယဉ်းပါတယ်။ ဒီစနစ်ပေါ် သိမ်းဆည်းထားတဲ့ bit တွေကို အလွယ်တကူဝင်ရောက်ဖျက်ဆီးခြင်း မပြုနိုင်ပါဘူး။ (SSD ပေါ်က အချက်အလက်တွေကို ဘာကြောင့် လုံလုံခြုံခြုံ ဖျက်ပစ်ဖို့ခဲယဉ်းကြောင်း ဒီနေရာ မှာ အသေးစိတ်ဆက်လက်ဖတ်ရှုနိုင်ပါတယ်)။ တစ်ကယ်လို့ မိမိဟာ SSD ကွန်ပျူတာ သို့မဟုတ် USB flash drive အသုံးပြုနေတယ်ဆိုပါက ဤအပိုင်းသို့ကျော်ပြီး ဖတ်ရှုပါ။

ဖိုင်တစ်ခုကိုဖျက်မယ်ဆိုပါစို့။ ဖျက်ချင်တဲ့ဖိုင်ကို စွန့်ပစ်ဖိုင်တွဲ (trash folder) ထဲရွှေ့လိုက်မယ်။ ဖိုင်တွဲကို ရှင်းလင်းဖို့ empty နှိပ်လိုက်မယ်။ ဒါဆို ဖိုင်လုံးဝပျက်သွားပြီးလား။ မပျက်သွားပါဘူး။

ကွန်ပျူတာပေါ်မှာရှိ နေတဲ့ ဖိုင်တွေကို “ဖျက်” လို့မရပါဘူး။ ဖိုင်ဖျက်တယ်ဆိုတာ ဖိုင်ကိုကွန်ပျူတာပေါ်မှာမမြင်ရအောင် ခဏ ဖျောက်ပေးလိုက်ရုံသာဖြစ်တယ်။ နောက်ထပ်ဖိုင်တစ်ခုထပ်သိမ်းလိုတဲ့အချိန်မှသာ ပထမဖိုင်နေရာမှာ ဒုတိယ ဖိုင်နဲ့ ထပ်ရေးပြီး (overwrite) သိမ်းဆည်းပေးပါတယ်။ ဒါကြောင့် နောက်ဖိုင်တစ်ခု ထပ်မရေးခင် အချိန်အထိ “ဖျက်လိုက်တဲ့” ဖိုင်ဟာ disk ပေါ်မှာ ဆက်ရှိနေပါလိမ့်မယ်။ ဒါပေမယ့် နောက်ထပ်ဖိုင်တစ်ခု ထပ်ရေးဖို့ ရက်သတ္တပတ်၊ လ၊ နှစ်နှင့်ချီပြီး ကြာနိုင်ပါတယ်။ ထပ်မရေးနိုင်မီ အချိန်စပ်ကြားမှာ ဖျက်လိုက်တဲ့ဖိုင်ဟာ မျက်စိနဲ့မမြင်နိုင်ပေမယ့် ကွန်ပျူတာပေါ် ဆက်ရှိနေမှာ ဖြစ်တယ်။ ဒါကြောင့် နည်းပညာအနည်းငယ် အသုံးချရုံနဲ့ (ဥပမာ “ဖျက်ပစ်ထားသောဖိုင်ကို ပြန်ခေါ်ရန်” ဆော့ဖ်ဝဲ သို့မဟုတ် သဲလွန်စခွဲခြမ်းခြေရာခံသည့် နည်းလမ်းများ သုံးပြီး) ယင်းဖိုင်ကို ပြန်လည်ခေါ်ယူနိုင်ပါလိမ့်မယ်။

ဒါဆို ဖိုင်တစ်ခုကို အပြီးသတ်ဖျက်ဆီးဖို့ ဘယ်လိုလုပ်ဆောင်ရမလဲ။ ဖျက်လိုက်တဲ့ ဖိုင်နေရာမှာ နောက်ထပ်ဖိုင် တစ်ခုနဲ့ ချက်ချင်းအစားထိုးဖို့ လုပ်ဆောင်နိုင်ပါတယ်။ ချက်ချင်းထပ်ရေးလိုက်မှသာ နဂိုဖိုင်ဟာ ကွန်ပျူတာပေါ် ဆက်ရှိမနေတော့ဘဲ ဆော့ဖ်ဝဲသုံးပြီး ပြန်ခေါ်ဖို့ ခက်ခဲပါလိမ့်မယ်။ ဒီလို နောက်ထပ်ဖိုင်တစ်ခု ချက်ချင်းထပ်ရေး ပေးနိုင်တဲ့ ဆော့ဖ်ဝဲက ကွန်ပျူတာလည်ပတ်ရေးစနစ်မှာ ပါရှိပြီးသားလည်း ဖြစ်နိုင်ပါတယ်။ ဒီဆော့ဖ်ဝဲသုံးပြီး ကွန်ပျူတာပေါ်မှာရှိတဲ့ “နေရာလွတ်” မှန်သမျှမှာ ထပ်ရေးဖို့ ဖိုင်အသစ်များဖန်တီးနိုင်တယ်။ အရင်ဖျက်ထားတဲ့ ဖိုင်တွေ အားလုံးရဲ့နေရာမှာ အသစ်ဖန်တီးထားတဲ့ဖိုင်များနဲ့ ထပ်ရေးလိုက်မယ်ဆိုရင် အချက်အလက်များ ထာဝရ ပျက်စီးသွားပါလိမ့်မယ်။

Linux စနစ်မှာတော့ ဒီလိုလုပ်ဖို့ BleachBit သုံးဖို့ အကြံပြုလိုပါတယ်။ BleachBit ဟာ Linux နဲ့ Windows စနစ်သုံး ကွန်ပျူတာတွေမှာ ရှိတဲ့အချက်အလက်တွေကို လုံလုံခြုံခြုံဖျက်ပစ်ဖို့ တီထွင်ထားတဲ့ အများသုံး (open-source) နည်းပညာ ဖြစ်ပါတယ်။ ဒီနည်းပညာဟာ ကွန်ပျူတာမှာ အလိုအလျောက်ပါလာတဲ့ “ဆုတ်ဖြဲခြင်း” (shred) နည်းလမ်းထက် ပိုအဆင့်မြင့်ပါတယ်။ ကိုယ်ဖျက်လိုတဲ့ဖိုင်တစ်ခုချင်းစီကို လုံလုံခြုံခြုံ ဖျက်ပစ်ဖို့အပြင် အချက်အလက်တွေကို ပုံမှန်ရှင်းလင်းဖို့အတွက်လည်း လွယ်လွယ်ကူကူ မြန်မြန်ဆန်ဆန် လုပ်ဆောင်နိုင်တယ်။ ဖိုင်ဖျက်ဖို့အစီအစဉ်များကို မိမိဘာသာသီးသန့်ရေးသားညွှန်ကြားခြင်းလည်း လုပ်ဆောင် နိုင်ပါတယ်။ ဒီနေရာမှာ ပိုပြီးပြည့်ပြည့်စုံစုံဖတ်နိုင်ပါတယ်။

ကွန်ပျူတာမှာ BleachBit တပ်ဆင်ခြင်း

Ubuntu ဆော့ဖ်ဝဲသုံး၍ တပ်ဆင်ခြင်း

Ubuntu Software application ကိုသုံးပြီး Ubuntu ကနေ BleachBit ကို ရယူနိုင်ပါတယ်။ စိတ်ကြိုက် အက်ပလီကေးရှင်းများ (favorite applications) ထဲရောက်နေပါက ကွန်ပျူတာမျက်နှာပြင်ရဲ့ ဘယ်ဘက်အခြမ်း မှာရှိတဲ့ Favorites ဖိုင်ပေါ် ကလစ်နှိပ်ပြီး ရယူနိုင်ပါတယ်။

သို့မဟုတ်ပါက ကွန်ပျူတာမျက်နှာပြင်ရဲ့ ဘယ်ဘက်အောက်မှာရှိတဲ့ application ခလုတ်ကို နှိပ်ပြီး search field သုံးပြီးရှာဖွေပါ။

Search field မှာ “software” လို့ရိုက်ထည့်ပြီး Ubuntu Software ပုံပေါ်လာရင် ယင်းပုံကို နှိပ်ပါ။

စာရင်းထဲမှာ BleachBit အလိုအလျောက်ပါလာမှာမဟုတ်ပါ။ BleachBit ဖိုင်ရှာတွေ့ရန် community-maintained packages ကိုအရင်ဖွင့်ရပါမယ်။ Community-maintained packages ဖွင့်ဖို့ ထိပ်ဆုံး menu ပေါ်မှာ “Ubuntu Software” ကိုနှိပ်ပြီး “Software & Updates” ကိုဆက်နှိပ်ပါ။

အသစ်ပေါ်လာတဲ့ ပြတင်းပေါက်မှာ “Community-maintained free and open-source software (universe)” စာသားဘေး အမှန်ခြစ်ပါ။ ပြီးလျှင် “Close” နှင့် “Reload” ကိုနှိပ်ပါ။ အမှန်ခြစ်ပြီးသား ဖြစ်နေရင် “Close” တစ်ခုတည်းနှိပ်လို့ရပါတယ်။

ဒါဆို Ubuntu Software ထဲမှာ BleachBit ကိုရှာနိုင်ပါပြီ။ ပိုပြီးမြန်မြန်ရှာတွေ့အောင် search field သုံးဖို့ ပြတင်းပေါက်ရဲ့ အပေါ်ညာဘက်ထောင့်မှာရှိတဲ့ မှန်ဘီလူးပုံကိုနှိပ်ပါ။

Search field ပေါ်လာရင် “BleachBit” လို့ရိုက်ထည့်ပါ။

BleachBit ပေါ်လာရင် ဖိုင်ကိုနှိပ်ပါ။ တပ်ဆင်ဖို့ Install ခလုတ်ကိုဆက်နှိပ်ပါ။

တပ်ဆင်ခွင့်ရဖို့ Ubuntu Software က မိမိရဲ့စကားဝှက် password ကို တောင်းပါလိမ့်မယ်။ စကားဝှက် ရိုက်ထည့်ပြီး Authenticate ခလုတ်ကို နှိပ်ပါ။

Ubuntu Software Center က BleachBit ကို ကွန်ပျူတာပေါ်မှာတပ်ဆင်ပေးပြီး မည်မျှတပ်ဆင်ပြီးစီးကြောင်း ဘားပုံစံဖြင့် ပြပါလိမ့်မယ်။ တပ်ဆင်ခြင်း ပြီးစီးသွားရင် “Launch” နှင့် “Remove” ခလုတ်များ ပေါ်လာ ပါလိမ့်မယ်။

Terminal မှ တပ်ဆင်ခြင်း

Terminal ကိုသုံးပြီးလည်း Ubuntu ပေါ်မှ BleachBit ကို ရယူနိုင်ပါတယ်။ ကွန်ပျူတာမျက်နှာပြင် ဘယ်ဘက် အောက်ခြေမှာရှိတဲ့ application ခလုတ်ကို နှိပ်ပြီး search field သုံးပြီးရှာဖွေပါ။

Search field ပေါ်လာရင် “terminal” လို့ရိုက်ထည့်ပြီး ပေါ်လာတဲ့ Terminal ပုံကို နှိပ်ပါ။

ပြီးရင် “sudo apt-get install bleachbit” လို့ရိုက်ထည့်ပြီး Enter ခေါက်ပါ။

BleachBit ကို တပ်ဆင်ဖို့ စကားဝှက်တောင်းပါလိမ့်မယ်။ မိမိရဲ့စကားဝှက်ကိုရိုက်ထည့်ပြီး Enter ခေါက်ပါ။

BleachBit ကို တပ်ဆင်နေတဲ့အချိန်မှာ ဘယ်လောက်တပ်ဆင်မှုပြီးစီးပြီဆိုတာကို မြင်ရပါလိမ့်မယ်။ တပ်ဆင်မှု ပြီးစီးတဲ့အခါ အစက အမိန့်ပေးလမ်းကြောင်းကို ပြန်ရောက်သွားပါလိမ့်မယ်။

Sidebar မှာ BleachBit ပေါင်းထည့်ခြင်း

ကွန်ပြူတာမျက်နှာပြင် ဘယ်ဘက်အောက်မှာရှိတဲ့ application ခလုတ်ကို နှိပ်ပါ။ ပြီးရင် search field ကိုသုံးပါ။

Search field မှာ “bleach” လို့ရိုက်လိုက်ရင် ရွေးချယ်စရာနှစ်ခုပေါ်လာပါလိမ့်မယ်။ BleachBit နှင့် BleachBit (as root) လို့ တွေ့ရပါလိမ့်မယ်။

> BleachBit (as root) ကို သေသေချာချာ အသုံးပြုတတ်မှသာ ရွေးချယ်သင့်ပါတယ်။ မဟုတ်ရင် BleachBit (as root) သုံးပြီး ကွန်ပျူတာလည်ပတ်မှုစနစ်အတွက်လိုတဲ့ ဖိုင်တွေ မှားဖျက်မိရင် ပြန်ပြင်မရအောင် ပျက်စီးသွား နိုင်လို့ပါ။

BleachBit ပေါ် ညာကလစ် နှိပ်ပြီး “Add to Favorites” ကိုရွေးချယ်ပါ။

BleachBit ကိုအသုံးပြုခြင်း

ကွန်ပျူတာမျက်နှာပြင်ဘယ်ဘက်ခြမ်းမှာရှိတဲ့ Favorites ကနေ BleachBit ပုံကို နှိပ်ပါ။

BleachBit ရဲ့ ပင်မပြတင်းပေါက် ပွင့်လာပြီး ရွေးချယ်ရန် preferences များကို ပြသပါလိမ့်မယ်။ ဖျက်လိုက်တဲ့ ဖိုင်များကို ပြန်လည်ရယူခြင်းမပြုနိုင်စေဖို့ ဖိုင်ပါအကြောင်းအရာများအပေါ် ထပ်ရေးခိုင်းရပါမယ်။ ဒါ့ကြောင့် “Overwrite contents of files to prevent recovery” ကိုရွေးပြီး အမှန်ခြစ်ထားပါလို့ အကြံပြုပါတယ်။

ဆက်လက်ပြီး “Close” ခလုတ်ကိုနှိပ်ပါ။

BleachBit က ကွန်ပျူတာမှာ အများအားဖြင့် တပ်ဆင်အသုံးပြုလေ့ရှိတဲ့ ပရိုဂရမ်တွေကို ရှာဖွေဖော်ပြပါလိမ့်မယ်။ ပရိုဂရမ်တစ်ခုချင်းစီအတွက် ဘာလုပ်ချင်သလဲ ရွေးချယ်စရာများလည်း တွေ့ရပါလိမ့်မယ်။

Presets များအသုံးပြုခြင်း

ဆော့ဖ်ဝဲတစ်ချို့က အသုံးပြုပြီးရင် ဘယ်အချိန် ဘယ်လိုအသုံးပြုခဲ့တယ်ဆိုတဲ့ မှတ်တမ်းကို ကွန်ပျူတာပေါ်ချန်ထားတတ်ကြတယ်။ ဒီပြဿနာကို ကျယ်ကျယ်ပြန့်ပြန့်ကြံတွေ့ရနိုင်ပြီး အရေးကြီးဥပမာအနေနဲ့ မကြာသေးမီကသုံးပြုခဲ့သော စာရွက်စာတမ်းများ “Recent Documents” နဲ့ web browser မှတ်တမ်း

တို့ကို ကြည့်ပါ။ အချို့ဆော့ဖ်ဝဲတွေဟာ မကြာသေးမီက အသုံးပြုပြင်ဆင်ခဲ့တဲ့ စာရွက်စာတမ်းတွေကို လိုက်လံမှတ် သားထားတတ်တယ်။ ဒါ့ကြောင့် မကြာသေးခင်က အသုံးပြုထားတဲ့ဖိုင်တွေရဲ့နာမည်တွေဟာ အဲဒီဖိုင်တွေ ဖျက်လိုက်ပြီးချိန်မှာတောင် ကွန်ပျူတာပေါ်မှတ်တမ်းကျန်နေပါလိမ့်မယ်။ Web browser တွေဟာလည်း လတ်တလော ဝင်ကြည့်ခဲ့တဲ့ ဝက်ဘ်ဆိုဒ်စာရင်းကို အသေးစိတ်မှတ်ထားကြပါတယ်။ ဒါ့အပြင် နောက်တစ်ကြိမ် ထပ်ဝင်ကြည့်တဲ့အခါ မြန်မြန်ပေါ်လာစေဖို့ ဝင်ကြည့်ခဲ့တဲ့ဝက်ဘ်ဆိုဒ်က စာမျက်နှာများ၊ ပုံများကိုပါ ပုံတူပွား သိမ်းဆည်းထားလေ့ရှိပါတယ်။

BleachBit မှာ အဲဒီ မှတ်တမ်းတွေကို ဖျက်ပစ်ဖို့ “preset” များပါပါတယ်။ ဒီ preset တွေကို BleachBit ဆော့ဖ်ဝဲရေးသားသူများက ကွန်ပျူတာပေါ်မှာရှိတဲ့ ဘယ်နေရာမှာရှိတဲ့ မှတ်တမ်းတွေက မိမိလုပ်ဆောင်မှုများ အကြောင်း ဖော်ထုတ်ပြသနိုင်သလဲဆိုတာကို လေ့လာဆန်းစစ်ပြီး ဖန်တီးထားတာပါ။ ဒီလမ်းညွှန်မှာ ဥပမာအနေ နဲ့ preset နှစ်ခုအကြောင်း တင်ပြပါမယ်။

System ဘေးရှိ လေးထောင့်ကွက်မှာ အမှန်ခြစ်ပါ။ System အောက်ရှိ အကွက်အားလုံးမှာပါ အမှန်ခြစ်ပြီးသား ဖြစ်သွားပါလိမ့်မယ်။ System အကွက်မှ အမှန်ခြစ်ကို ပြန်ဖြုတ်ပြီး Recent document list နဲ့ Trash ဘေးမှ အကွက်များကို အမှန်ခြစ်ပါ။ ပြီးရင် “Clean” ခလုတ်ကို နှိပ်ပါ။

BleachBit က တကယ်ဖျက်ချင်ကြောင်း အတည်ပြုခိုင်းပါလိမ့်မယ်။ ဖျက်ရန် Delete ခလုတ်ကို နှိပ်ပါ။

BleachBit ကဖိုင်အချို့ကို ရှင်းလင်းပြီး ဘယ်လောက်ရှင်းလင်းပြီးကြောင်း ပြပါလိမ့်မယ်။

ဖိုင်တွဲတစ်ခုကို လုံလုံခြုံခြုံဖျက်နည်း

ပြတင်းပေါက်အပေါ်ဆုံးက Menu ဘားမှာ File ကိုနှိပ်ပါ။ ဖိုင်တွဲဖျက်ဆီးဖို့ Shred Folders ကိုနှိပ်ပါ။

ပြတင်းပေါက်အသေးလေး ထပ်ပွင့်လာပါလိမ့်မယ်။ ကိုယ်ဖျက်လိုတဲ့ ဖိုင်တွဲကိုရွေးချယ်ပါ။

မိမိရွေးချယ်ထားတဲ့ဖိုင်များကို ‘အပြီးသတ်ဖျက်ပစ်လိုကြောင်း သေချာသလား’ လို့မေးပါလိမ့်မယ်။ Delete ခလုတ်ကိုနှိပ်ပြီး အပြီးသတ်ဖျက်လိုက်ပါ။

ဆက်လက်ပြီး ဖျက်လိုက်တဲ့ ဖိုင်နာမည်တွေ ပေါ်လာပါလိမ့်မယ်။ BleachBit က ဖိုင်တွဲထဲမှာ သိမ်းဆည်းထားတဲ့ ဖိုင်တစ်ခုချင်းစီကို အရင်လုံခြုံစွာဖျက်ပြီး နောက်ဆုံးမှာ ဖိုင်တွဲတစ်ခုလုံးကို ဖျက်ပစ်မှာဖြစ်ပါတယ်။

ဖိုင်တစ်ခုချင်းစီကို လုံလုံခြုံခြုံဖျက်နည်း

ပြတင်းပေါက်အပေါ်ဆုံးက Menu ဘားမှာ File ကိုနှိပ်ပါ။ ဖိုင်တစ်ခုချင်းစီကိုဖျက်ရန် Shred Files ကိုရွေးချယ် ပါ။

ပြတင်းပေါက်အသစ်မှာ ဖိုင်စာရင်း ပေါ်လာပါလိမ့်မယ်။ ကိုယ်ဖျက်လိုတဲ့ ဖိုင်ကိုရွေးချယ်ပါ။

မိမိရွေးချယ်ထားတဲ့ဖိုင်များကို 'အပြီးသတ်ဖျက်ပစ်လိုကြောင်း သေချာသလား' လို့မေးပါလိမ့်မယ်။ Delete ခလုတ်ကိုနှိပ်ပြီး အပြီးသတ်ဖျက်လိုက်ပါ။

BleachBit သုံးပြီး တစ်ခြားကိစ္စတွေလည်း လုပ်ဆောင်နိုင်ပါတယ်။ ဥပမာ ကွန်ပျူတာပေါ်မှာရှိတဲ့ နေရာလွတ် တွေကို ရှင်းလင်းပေးဖို့ သုံးနိုင်ပါတယ်။ နေရာလွတ်တွေရှင်းလင်းလိုက်မှသာ ဖျက်လိုက်တဲ့ဖိုင်တွေရဲ့ အစအန အားလုံးကို လက်စဖျောက်နိုင်မှာဖြစ်ပါတယ်။ တစ်ခါတစ်ရံ Linux စနစ်သုံး ကွန်ပျူတာတွေမှာ နေရာလွတ် ကျန်နေရင် ဖျက်လိုက်တဲ့ဖိုင်တွေရဲ့ တစ်စိတ်တစ်ပိုင်းကိုဖြစ်စေ၊ အားလုံးကိုဖြစ်စေ အဲဒီနေရာလွတ်တွေမှာ ဆက်သိမ်းထားတာမျိုး ကြုံတွေ့ရနိုင်တယ်။ ဒါကြောင့် နေရာလွတ်ဆိုပြီး ဒီအတိုင်းမထားဘဲ ရှင်းလင်းသင့် ပါတယ်။ တမင်ဖန်တီးထားတဲ့ အချက်အလက်တွေနဲ့ ယင်းနေရာလွတ်တွေပေါ်ထပ်ရေးလိုက်မယ်ဆိုရင် ယခင် ဖျက်ထားတဲ့အချက်အလက်တွေ ကျန်ခဲ့စရာအကြောင်းမရှိတော့ပါဘူး။ ဒါပေမယ့် drive ပေါ်မှာနေရာလွတ် အများကြီးရှိနေမယ်ဆိုရင် နေရာလွတ်ရှင်းလင်းတာ အချိန်အရမ်းကုန်နိုင်ပါတယ်။

လုံခြုံသောအချက်အလက်ဖျက်နည်းပညာများ၏ ကန့်သတ်ချက်များ

အခုဖော်ပြခဲ့တဲ့ လမ်းညွှန်ချက်တွေကို မိမိအသုံးပြုနေတဲ့ကွန်ပျူတာရဲ့ disk ပေါ်မှာသိမ်းထားတဲ့ အချက်အလက် တွေ ဖျက်ပစ်ဖို့သာ သုံးနိုင်တယ်ဆိုတာကို သတိပြုပါ။ ကွန်ပျူတာရဲ့ disk မဟုတ်ဘဲအခြားတစ်နေရာမှာဖြစ်စေ၊ အခြား disk သို့မဟုတ် USB drive ပေါ်မှာဖြစ်စေ၊ "Time Machine"၊ အီးမေးလ် ဆာဗာ၊ cloud ပေါ်မှာ တင်ထားသည်ဖြစ်စေ၊ မိမိ၏အဆက်အသွယ်များကို ပေးပို့ပြီးဖြစ်စေ အရန်သိမ်းဆည်းထားတဲ့ အချက်အလက် တွေကို မဖျက်ပေးနိုင်ပါ။ ဖိုင်တစ်ခုကို လုံလုံခြုံခြုံဖျက်ဖို့ဆိုရင် သိမ်းထားသမျှ၊ ပေးပို့ခဲ့သမျှ မိတ္တူဖိုင် အားလုံး ကို လက်စဖျောက် ဖျက်ပစ်ဖို့ လိုပါတယ်။ ဒါပေမယ့် cloud ဝန်ဆောင်မှုတွေ (ဥပမာ Dropbox သို့မဟုတ် အခြားဖိုင်မျှဝေခြင်း ဝန်ဆောင်မှုများ) ပေါ်မှာ ဖိုင်များ သိမ်းဆည်းထားတယ်ဆိုရင်တော့ ပြန်လည်ရယူခြင်း မပြုနိုင်အောင် အပြီးသတ်ဖျက်ဆီးလို့ ရ၊ မရ အာမမခံနိုင်ပါ။

လုံခြုံတဲ့အချက်အလက်ဖျက်နည်းပညာတွေမှာ နောက်ထပ်အားနည်းချက်တစ်ခုလည်းရှိပါသေးတယ်။ ရှေ့မှာ ဖော်ပြခဲ့တဲ့ လမ်းညွှန်ချက်အားလုံးကို လိုက်နာပြီး ရှိသမျှဖိုင်မိတ္တူအားလုံးကို ဖျက်နိုင်ခဲ့သည်ဆိုပါစို့။ ဖျက်လိုက် တဲ့ဖိုင်ရဲ့ ခြေရာအချို့ ကွန်ပျူတာပေါ်မှာ ဆက်ကျန်နေနိုင်ပါသေးတယ်။ ဖိုင်တစ်ခုလုံးပျက်သွားတယ် ဆိုပေမယ့် ကွန်ပျူတာလည်ပတ်မှုစနစ် ရဲ့အချို့အစိတ်အပိုင်းများနဲ့ ပရိုဂရမ်အချို့ မှာ ဖိုင်သိမ်းဆည်းခဲ့ဖူးကြောင်း မှတ်တမ်း ကျန်ရစ်နေနိုင်ပါတယ်။

ဘာကြောင့်ဒီလိုဖြစ်ရသလဲဆိုတဲ့ အကြောင်းရင်းများစွာရှိပေမယ့် ဥပမာနှစ်ခု ပေးလိုပါတယ်။ Windows သို့မဟုတ် macOS သုံးကွန်ပျူတာတွေမှာ Microsoft Office သုံးရင် ဖျက်လိုက်တဲ့ဖိုင်ရဲ့ နာမည်က

‘မကြာသေး မီကဖွင့်ခဲ့သောစာရွက်စာတမ်းများ’ (“Recent Documents”) menu မှာ ဆက်ပေါ်နေနိုင်ပါတယ် (တစ်ခါတစ် လေ ဖျက်လိုက်တဲ့ဖိုင်ထဲက အကြောင်းအရာတွေကို Microsoft Office က ယာယီဖိုင်တစ်ခုအနေနဲ့ ထပ်သိမ်း ထားတာမျိုး ကြုံရနိုင်ပါတယ်)။ အလားတူ LibreOffice ပရိုဂရမ်ကလည်း Microsoft Office လိုပဲ မှတ်တမ်းမှတ်ရာတွေ ချန်ထားနိုင်ပါတယ်။ ဒါ့အပြင် ဖိုင်ကိုလုံခြုံစွာဖျက်လိုက်ပေမယ့် ဖိုင်နာမည်ပါနေတဲ့ ကုဒ်တွေကို သုံးစွဲသူမှတ်တမ်းဖိုင်မှာ ဆက်သိမ်းထားတာမျိုးလည်း တွေ့ရပါတယ်။ Microsoft Office နဲ့ LibreOffice အပြင် တစ်ခြား ပရိုဂရမ်တွေလည်း ဒီလိုဘဲ မှတ်တမ်းချန်တာမျိုး လုပ်ဆောင်နိုင်ပါတယ်။

ဒီလိုပြဿနာတွေကို ဖြေရှင်းဖို့ ခက်ခဲနိုင်တယ်။ ဒါကြောင့် ဖိုင်တစ်ခုကို ကွန်ပျူတာပေါ်ကနေ လုံခြုံတဲ့ နည်းလမ်း နဲ့ ဖျက်လိုက်တယ်ဆိုပေမယ့် အဲဒီဖိုင်ရဲ့အမည်ကို ကွန်ပျူတာပေါ်မှာ အချိန်တစ်ခုကြာ ဆက်တွေ့နေနိုင်တယ်လို့ မှတ်ယူပါ။ ဖိုင်နာမည်ပါ ရာနှုန်းပြည့်ပျက်သွားစေဖို့ဆိုရင် disk တစ်ခုလုံးကို ထပ်ရေးဖို့နည်းလမ်းသာရှိပါတယ်။ “ဖျက်လိုက်တဲ့ဖိုင်တစ်ခုရဲ့ မိတ္တူ ကွန်ပျူတာပေါ်မှာ ကျန်နေသေးသလားဆိုတာကို disk မှာရှိတဲ့ အချက်အလက် တွေကနေတစ်ဆင့်အတည်ပြုနိုင်လား” လို့မေးနိုင်ပါတယ်။ တစ်ချို့တစ်ဝက်ပဲ အတည်ပြုနိုင်ပါတယ်။ Disk တစ်ခုလုံးကို ရှာရင် အချက်အလက်တွေ plaintext အနေနဲ့ ကျန်၊ မကျန် အတည်ပြုနိုင်ပါတယ်။ ဒါပေမယ့် ချုံထားတဲ့ပုံစံ၊ ကုဒ်ဖြင့်ပြောင်းထားတဲ့ ပုံစံများနဲ့ ကျန်၊ မကျန် မပြောနိုင်ပါ။ ဖိုင်ပါအကြောင်းအရာများ ကွန်ပျူတာပေါ်မှာ ဆက်လက်ကျန်နိုင်ခြေ ရာခိုင်နှုန်းနည်းသော်လည်း ရာနှုန်းပြည့် မသေချာနိုင်ပါ။ ဒါကြောင့် ဖိုင်မှတ်တမ်းအားလုံး ၁၀၀ ရာခိုင်နှုန်း ပျက်စီးစေဖို့ဆိုရင် disk တစ်ခုလုံးကို ထပ်ရေးပြီး ကွန်ပျူတာလည်ပတ်မှု စနစ်အသစ်တစ်ခု တပ်ဆင်ခြင်းနည်းလမ်းသာ ရှိပါတယ်။

စက်ပစ္စည်း Hardware အဟောင်း စွန့်ပစ်ချိန်တွင် လုံလုံခြုံခြုံ အချက်အလက်ဖျက်နည်း

မသုံးတော့တဲ့ စက်ပစ္စည်းတစ်ခုကို လွှတ်ပစ်မယ်၊ ဒါမှမဟုတ် eBay လို အင်တာနက်ဝက်ဘ်ဆိုဒ်တွေကတစ်ဆင့် ပြန်ရောင်းမယ်ဆိုပါစို့။ ကွန်ပျူတာပေါ် သိမ်းထားတဲ့ အချက်အလက်တွေ တစ်ခြားသူလက်ထဲ မရောက်သွားနိုင် အောင် အချက်အလက်တွေကို အရင်ဆုံးလုံလုံခြုံခြုံဖျက်ဆီးရပါမယ်။ လေ့လာတွေ့ရှိချက်တွေအရကတော့ ကွန်ပျူတာပိုင်ရှင်အများစုက သူတို့ရဲ့စက်ပစ္စည်းတွေပြန်မရောင်းခင်မှာ အရေးကြီးအချက်အလက်တွေကို hard drive ပေါ်ကနေ လုံလုံခြုံခြုံ ဖျက်ထားတာမျိုး မရှိတတ်ဘူး။ ဒါဟာအန္တရာယ်များတဲ့အတွက် ကွန်ပျူတာ အဟောင်းတွေကို မစွန့်ပစ်ခင်၊ ပြန်လည်မရောင်းချခင်၊ recycle မလုပ်ခင် အချက်အလက်သိမ်းဆည်းထားတဲ့ နေရာတွေအပေါ်မှာ အခြားအသုံးမဝင်တဲ့အချက်အလက်တွေနဲ့ ထပ်ရေးပါ။ ကွန်ပျူတာအဟောင်းတွေကို ချက်ချင်းမစွန့်ပစ်ဘဲ အိမ်မှာဘဲသိမ်းဆည်းထားမယ်ဆိုရင်တောင်မှ hard drive တစ်ခုလုံးကို

အရင်ဖျက်ပစ်ဖို့ (ထပ်ရေးဖို့) အကြံပြုလိုပါတယ်။ ဒီလိုလုပ်ဖို့ Darik's Boot and Nuke နည်းပညာကို သုံးနိုင်ပြီး အသုံးပြုနည်း ကို အင်တာ နက်ပေါ်မှာ ရှာဖွေဖတ်ရှုနိုင်ပါတယ်။ ဒီနေရာ မှာလည်း ကြည့်ရှုနိုင်ပါတယ်။

အပြည့်အဝ ကုဒ်ဖြင့်ပြောင်းလဲသည့် ဆော့ဖ်ဝဲတစ်ချို့မှာ စကားဝှက်သော့ကြီးကို ဖျက်ပစ်နိုင်စွမ်း ရှိတတ်ပါတယ်။ စကားဝှက်သော့ကြီးကို ဖျက်လိုက်မယ်ဆိုရင် hard drive ပေါ်မှာ ကုဒ်ဖြင့်ပြောင်း၍သိမ်းဆည်းထားတဲ့ အချက်အလက်အားလုံးကို ဘယ်တော့မှ ပြန်ဖြည်ပြီးဖတ်နိုင်တော့မှာမဟုတ်ပါဘူး။ ဒါဆိုအချက်အလက်တွေ ပေါက်ကြားစရာအကြောင်းမရှိတော့ပါဘူး။ စကားဝှက်သော့က အရွယ်အစားသေးတဲ့အတွက် ချက်ချင်းဖျက် ပစ်နိုင်ပါတယ်။ ဒါ့ကြောင့် Darik's Boot ၊ Nuke လို ဆော့ဖ်ဝဲတွေသုံးပြီး drive တစ်ခုလုံးကို ထပ်ရေးတာထက် အချိန်မြန်မြန်ပြီးစီးနိုင်ပါတယ်။ ဒါပေမယ့် ဒီနည်းလမ်းက ကုဒ်ဖြင့်ပြောင်းလဲထားတဲ့ hard drive တွေအတွက်ဘဲ အသုံးဝင်ပါတယ်။ အပြည်အဝကုဒ်ဖြင့်ပြောင်းလဲသည့်စနစ်ကို နဂိုကတည်းက မသုံးထားဘူးဆိုရင် drive တစ်ခုလုံးကိုထပ်ရေးခြင်းမှတစ်ပါး အခြားနည်းလမ်းမရှိပေ။

CD- သို့မဟုတ် DVD-ROMs များကို စွန့်ပစ်ခြင်း

CD- သို့မဟုတ် DVD-ROMs တွေကို စွန့်ပစ်တဲ့အခါ အရေးကြီးစာရွက်စာတမ်းများ စွန့်ပစ်သလို အရင်ဆုတ်ဖြဲ ဖျက်စီးပြီးမှ စွန့်ပစ်သင့်ပါတယ်။ ဆုတ်ဖြဲဖျက်စီးတဲ့ shredder စက်တွေကို ဈေးနည်းနည်းနဲ့ ဝယ်ယူနိုင်ပါတယ်။ အခြားသူတွေမသိသင့်တဲ့ အချက်အလက်တွေပါတဲ့ CD- သို့မဟုတ် DVD-ROMs တွေကို ဘယ်တော့မှ အရင်မဖျက်ဆီးဘဲ မစွန့်ပစ်ပါနဲ့။

Solid-state Disks (SSDs) ၊ USB Flash Drives နှင့် SD ကဒ်များပေါ်ရှိ အချက်အလက်များကို လုံခြုံစွာဖျက်ပစ်ခြင်း

SSDs ၊ USB Flash Drives နှင့် SD ကဒ်များပေါ်မှာ သိမ်းဆည်းထားတဲ့ ဖိုင်တစ်ခုချင်းစီနှင့် နေရာလွတ်တွေကို လုံလုံခြုံခြုံဖျက်ပစ်ဖို့ မဖြစ်နိုင်ပါ။ ဒါ့ကြောင့် ဒီလိုအချက်အလက်တွေကို ကာကွယ်ဖို့ အကောင်းဆုံးနည်းလမ်း ကတော့ ကုဒ်ဖြင့်ပြောင်းလဲခြင်း စနစ်ဖြစ်ပါတယ်။ ကုဒ်ဖြင့်ပြောင်းလဲလိုက်တဲ့အတွက် disk ပေါ်မှာရှိတဲ့ ဖိုင်တွေကို ကုဒ်ပြန်မဖြည် နိုင်သရွေ့ အခြားသူတွေ နားလည်နိုင်မှာမဟုတ်ပါ။ SSD ပေါ်က အချက်အလက် တွေကို အပြီးသတ်ဖယ်ရှားဖို့ နည်းလမ်းကောင်း ယနေ့ထက်တိုင်မရှိသေးပါ။ ဒီကိစ္စကို ပိုမိုနားလည်လိုရင် အောက်မှာ ဆက်ဖတ်ပါ။

ရှေ့မှာပြောခဲ့တဲ့အတိုင်း SSD နဲ့ USB flash drive တွေမှာ ဟောင်းနွမ်းပျက်စီးမှုဖြန့်ကျက်ခြင်း (wear leveling) နည်းပညာကို အသုံးပြုထားပါတယ်။ ဒီစနစ်သုံးတဲ့ disk ပေါ်မှာ နေရာလွတ်တွေကို အကန့်တစ်ကန့်စီ အနေနဲ့ခွဲထားပါတယ်။ ဥပမာ စာအုပ်တစ်အုပ်မှာ စာမျက်နှာတစ်ရွက်စီခွဲထားသလိုမျိုးပေါ့။ ဒီ disk ပေါ်မှာ ဖိုင်တစ်ခု ရေးလိုက်တယ် ဆိုပါစို့။

ရေးလိုက်တဲ့ဖိုင်ကို သတ်မှတ်ထားတဲ့ အကန့်တစ်ခု သို့မဟုတ် အကန့်တစ်ချို့ (စာမျက်နှာတစ်ခုစီ) မှာ သွားသိမ်းထားလိုက်မှာ ဖြစ်ပါတယ်။ ဒီဖိုင်ကို နောက်ဖိုင်တစ်ခုနဲ့ ထပ်ရေးဖို့ဆိုရင် ပထမ ဖိုင် သိမ်းဆည်းထားတဲ့အကန့်ပေါ်မှာ ကွက်တိထပ်ရေးရမှာဖြစ်ပါတယ်။ ဒါပေမယ့် အကန့်တစ်ခုတည်းကို ခဏ ခဏ ဖျက်လိုက်၊ ရေးလိုက်လုပ်တာက SSD နဲ့ USB flash drive တွေကို မြန်မြန်ပျက်စီးစေပါတယ်။ ဖျက်လိုက်၊ ရေးလိုက်လုပ်တာ အကြိမ်အရေအတွက်တစ်ခုပြည့်သွားရင် အဲဒီအကန့်က အလုပ်မလုပ်တော့ပါဘူး (စာရွက်ပေါ်မှာ ခဲတံနဲ့ ဖျက်လိုက်ရေးလိုက် အကြိမ်ကြိမ်လုပ်ရင် စာရွက်ပေါက်ပြီး ဆက်ရေးမရတော့သလိုမျိုး)။ ဒါကြောင့် drive တစ်ခုလုံး ကြာကြာခံစေဖို့ SSD နဲ့ USB flash drive တွေမှာ အကန့်တစ်ခုတည်းကို အကြိမ် ကြိမ်ထပ်မရေးဘဲ အကန့်အားလုံးမျှအောင် လုပ်ထားပါတယ် (ဒါ့ကြောင့် ဒီနည်းလမ်းကို ဟောင်းနွမ်း ပျက်စီးမှုဖြန့်ကျက်ခြင်းနည်းလမ်းလို့ ခေါ်တာပါ)။ ဒါပေမယ့် ဒီလိုလုပ်တဲ့အတွက် ဖျက်လိုက်တဲ့ဖိုင်နေရာမှာ တစ်ခြားဖိုင်တစ်ခုနဲ့ ထပ်ရေးဖို့ဆိုရင် နဂိုသိမ်းဆည်းထားတဲ့အကန့်ပေါ် ကွက်တိထပ်မရေးဘဲ တစ်ခြားအကန့်မှာသွားရေးတာမျိုး လုပ်နိုင်ပါတယ်။ စာအုပ်ဥပမာနဲ့ပြောရရင် ပြင်ရေးချင်တဲ့စာမျက်နှာပေါ်မှာ မရေးဘဲ တစ်ခြား စာမျက်နှာပေါ် သွားရေးခြင်းနဲ့ ဆင်တူပါတယ်။ ထပ်ရေးလိုက်တဲ့အကြောင်းအရာက မာတိကာမှာကြည့်ရင် စာမျက်နှာ အသစ်မှာပေါ်နေမှာဖြစ်တယ်။ ဒီဖြစ်စဉ်တွေဟာ disk ရဲ့ အလွန်အဆင့်နိမ့်တဲ့ အီလက်ထရော နစ်များမှာ ဖြစ်ပေါ်ပါတယ်။ ဒါ့ကြောင့် ကွန်ပျူတာလည်ပတ်မှုစနစ်က ဒီဖြစ်စဉ် ဖြစ်ပွားခဲ့မှန်း သိလိုက်မှာ မဟုတ်ပါဘူး။ ဖိုင်တစ်ခုကို ထပ်ရေးလိုက်ရင် ထပ်ရေးလိုက်တဲ့ဖိုင်က ဖျက်ချင်တဲ့ဖိုင်နေရာမှာ ကွက်တိဝင်သွား အောင် လုပ်ဖို့နည်းလမ်းမရှိပါဘူး။ ဒါ့ကြောင့် SSD မှာ အချက်အလက်တွေကို လုံလုံခြုံခြုံဖျက်ပစ်ဖို့ ခဲယဉ်းခြင်း ဖြစ်ပါတယ်။