ဒစ်ဂျစ်တယ် Forensics Lab အတွက် စံလုပ်ထုံးလုပ်နည်းများ

မိတ်ဆက်

၁။ စံလုပ်ထုံးလုပ်နည်းများသည် အရည်အသွေးတိုးတက်စေရန်နှင့် ဒစ်ဂျစ်တယ် Forensics ဆိုင်ရာ လုပ်ငန်းများကို တိကျမှန်ကန်သောနည်းဖြင့် တသမတ်တည်း လုပ်ဆောင်နိုင်မည့် လုပ်ငန်းစဉ်များကို အကောင်အထည်ဖော်ရာတွင် မရှိမဖြစ် အရေးပါပေသည်။

ရည်ရွယ်ချက်

၂။ ဤစံလုပ်ထုံးလုပ်နည်း၏ရည်ရွယ်ချက်မှာ ဒစ်ဂျစ်တယ်ပစ္စည်များနှင့် ၎င်းတို့၏ ဆက်စပ်သိုလှောင်ပစ္စည်းများတွင် Forensics ဆိုင်ရာ လုပ်ငန်းဆောင်တာများကို ဆောင်ရွက်ရာ၌ လိုက်နာရမည့် လုပ်ငန်းစဉ်များနှင့် လုပ်ထုံးလုပ်နည်းများကို ဖော်ပြရန်အတွက် ဖြစ်သည်။

ဒစ်ဂျစ်တယ် Forensics

၃။ ဒစ်ဂျစ်တယ် Forensics သည် ကွန်ပျူတာ၊ ဒစ်ဂျစ်တယ်ပစ္စည်းများနှင့် အခြား ဒစ်ဂျစ်တယ် သိုလှောင်ပစ္စည်းများတွင် သိမ်းဆည်းထားသည့် အချက်အလက်များကို ခွဲခြား သတ်မှတ်ခြင်း၊ ရယူခြင်း၊ လေ့လာဆန်းစစ်ခြင်း၊ ရလဒ်များကိုတင်ပြခြင်း စသည်တို့ကို အထူးပြု လုပ်ဆောင်သည့် မှုခင်းသိပ္ပံဆိုင်ရာ ပညာရပ်တစ်ခုဖြစ်သည်။

၄။ စုံစမ်းထောက်လှမ်းရာတွင် အရေးပါသည့် တန်ဖိုးရှိအချက်အလက်များကို သိမ်းဆည်း သိုလှောင်ထားသည့် ကွန်ပျူတာ၊ ဒစ်ဂျစ်တယ်ပစ္စည်းများနှင့် အခြား ဒစ်ဂျစ်တယ် သိုလှောင်စနစ်များသည် ဒစ်ဂျစ်တယ် သက်သေအထောက်အထားများပင် ဖြစ်သည်။ ဥပမာပြရလျှင် လက်တော့ပ်၊ စမတ်ဖုန်း၊ ဆာဗာ၊ ဒစ်ဂျစ်တယ်ဗွီဒီယို Recorder၊ စီစီတီဗွီစနစ်၊ ဒရုန်းနှင့် GPS စနစ် စသည်တို့ပင်ဖြစ်သည်။

ဒစ်ဂျစ်တယ်သက်သေ အထောက်အထားအတွက် စည်းမျဉ်းများ

၅။ ဒစ်ဂျစ်တယ်သက်သေ အထောက်အထားကို ကိုင်တွယ်ရာတွင် အောက်ပါစည်းမျဉ်းများကို လိုက်နာရမည် -

(က) ဒစ်ဂျစ်တယ်သက်သေအထောက်အထားကို တရားဝင်နည်းလမ်းဖြင့် ရယူရမည်။

(ခ) ဒစ်ဂျစ်တယ် သက်သေအထောက်အထားသည် တရားရုံးမှလက်ခံနိုင်သော သက်သေအထောက်အထား ဖြစ်ရမည်။

(ဂ) ဒစ်ဂျစ်တယ် သက်သေအထောက်အထားသည်စစ်ဆေးနေသောအမှုနှင့်ပတ်သက်ဆက်နွယ်မှုရှိရမည်။

(ဃ) ဒစ်ဂျစ်တယ် သက်သေအထောက်အထားသည် ပြီးပြည့်စုံမှုရှိရမည်။ အစိတ်အပိုင်းတစ်စုံတစ်ရာပျောက်ဆုံးနေခြင်းမျိုး မရှိစေရ။

(င) သက်ဆိုင်ရာဝန်ထမ်းများသည် ဒစ်ဂျစ်တယ် သက်သေအထောက်အထားကို ကိုင်တွယ်ဖြေရှင်းခြင်းမပြုမီ သင့်လျော်သော သင်တန်းတစ်ခုခုကို တတ်မြောက်ပြီးဆုံးပြီးဖြစ်ရမည်။ အသိအမှတ်ပြုလက်မှတ် ရရှိထားရမည်။

(စ) ဒစ်ဂျစ်တယ် သက်သေအထောက်အထားပေါ်တွင် လုပ်ဆောင်သည့် မည်သည့်လုပ်ရပ်မဆို ၎င်းအထောက်အထား၏ အချက်အလက်များ ပြောင်းလဲမှု မရှိစေရ။ အကယ်၍ မဖြစ်မနေ မူရင်းအချက်အလက်များကို ရယူရခြင်း (သို့) System Setting ပြောင်းလဲခြင်းများ ပြုလုပ်ရပါက အရည်အချင်းပြည့်ဝသည့် ကျွမ်းကျင်ဝန်ထမ်းကသာ လုပ်ဆောင်ရမည်။

(ဆ) မူရင်းအချက်အလက်ကို ရယူရမည့် (သို့) ပြောင်းလဲရမည့် မည်သည့်လုပ်ရပ်မဆို မှတ်တမ်းတင် ထားရှိရမည်ဖြစ်ပြီး ဖြစ်နိုင်လျှင် မျက်မြင်သက်သေအဖြစ် အခြားလုပ်ဖော်ကိုင်ဘက်တစ်ဦး ထားရှိဆောင်ရွက်ရမည်။

(ဇ) ဒစ်ဂျစ်တယ် သက်သေအထောက်အထားကို ကိုင်တွယ်ဖြေရှင်းရာတွင် လုပ်ဆောင်ခဲ့သမျှကို မှတ်တမ်းထားသည့် မှတ်တမ်းတစ်ခု ထားရှိရမည်ဖြစ်ပြီး ပြန်လည်အစစ်ဆေးခံနိုင်ရန်အတွက် ထိန်းသိမ်းထားရှိရမည်ဖြစ်သည်။ အခြားလွတ်လပ်သည့် တတိယအဖွဲ့အစည်းတစ်ခုခုမှ ပြန်လည်စစ်ဆေးခဲ့သော် တူညီသောရလဒ်သာ ထွက်ပေါ်စေရမည်။

ဒစ်ဂျစ်တယ်သက်သေအထောက်အထားကို ကိုင်တွယ်ဖြေရှင်းခြင်း

၆။ ဒစ်ဂျစ်တယ် သက်သေအထောက်အထားကို ကိုင်တွယ်ဖြေရှင်းရာတွင် အောက်ပါအချက်များကို လိုက်နာရမည်-

(က) ဒစ်ဂျစ်တယ်သက်သေအထောက်အထားကို သင့်လျော်ရာအထုတ် (သို့) ဘူးတွင် ထည့်သွင်းပြီး Seal ကပ်ကာ ထုပ်ပိုးထားရမည်။

(ခ) Seal ပေါ်တွင် တာဝန်ယူလက်ခံသူ၏ လက်မှတ်နှင့်လက်ခံသည့်နေ့စွဲပါရှိရမည်။

(ဂ) ဒစ်ဂျစ်တယ် Forensics Lab သို့ ရောက်ရှိလာသော သက်သေအထောက်အထားများကို Label ကပ်ပေးရမည်။ အကယ်၍ သက်သေအထောက်အထားပေါ်တွင် Label ကပ်ရန်ခက်ခဲပါက ၎င်းကို ထုပ်ပိုးထားသည့် အထုတ် (သို့) ဘူး၏ Seal ပေါ်တွင် Label ကပ်ရမည်။

(ဃ) ၎င်း Label သည် ဒစ်ဂျစ်တယ် Forensics Lab တွင် သက်သေအထောက်အထား ရှိနေသမျှ ကာလပတ်လုံး တည်မြဲနေရမည်။

(င) သက်သေအထောက်အထားကို ထုတ်ယူပြီးသည့်အချိန်တိုင်း ပြန်လည် Seal ကပ်ရမည်ဖြစ်ပြီး တာဝန်ယူဆောင်ရွက်သူ၏ လက်မှတ်နှင့် ရက်စွဲပါရှိရမည်။

(စ) Label များသည် ၎င်းတို့၏ ဆက်စပ်အမျိုးအစားများကို ဖော်ပြနိုင်စွမ်းရှိရမည်။ ဥပမာ- မိုဘိုင်းဖုန်း တစ်လုံးကို DFL-MP01 ဟု Label ကပ်ထားပါက ၎င်းတွင် ပါဝင်သော SIM ကတ်ကို DFL-MP01-SIM01 ဟု Label ကပ်ပေးရမည်။

(ဆ) သက်သေ အထောက်အထားအတွက် ပြည့်စုံသည့်မှတ်တမ်းတစ်ခုကို ဖန်တီးထားရှိရမည်။ မှတ်တမ်းတွင် ပါဝင်ရမည့်အချက်များမှာ သက်သေအထောက်အထားအမျိုးအစား၊ Serial Number၊ ထုတ်လုပ်သူ၊ ချို့ယွင်းချက်များနှင့် Label နံပါတ်များ စသည်တို့ ဖြစ်သည်။

(ဇ) သက်သေအထောက်အထား ထိန်းသိမ်းထားမှုမှတ်တမ်း (Chain of Custody Record) ကို သက်သေအထောက်အထား တစ်ခုချင်းစီအတွက် ဖန်တီးထားရှိရမည်။

Acquisition အတွက် ပြင်ဆင်ခြင်း

၇။ Acquisition အတွက် ပြင်ဆင်ရာတွင် အောက်ပါအချက်များကို လိုက်နာရမည် -

(က) Acquisition ပြုလုပ်မည့်သူနှင့် စစ်ဆေးမည့်သူတို့သည် တစ်ဦးစီဖြစ်ရမည်။ Acquisition ပြုလုပ်မည့်သူသည် ဒစ်ဂျစ်တယ်ပစ္စည်းများမှ ဒစ်ဂျစ်တယ် သက်သေအထောက်အထားများကို ထုတ်နှုတ်ရယူမည့် နည်းလမ်းတစ်ခုချင်းစီ၏ ကန့်သတ်ချက်များကို သိရှိနားလည်ထားရမည်ဖြစ်ပြီး ၎င်းကန့်သတ်ချက်များကို လျှော့ချနိုင်သည့်နည်းလမ်းများကို သင့်တော်သလို ထည့်သွင်းစဉ်းစားထားရမည်။

(ခ) Acquisition ပြုလုပ်မည့်သူသည် ၎င်းရွေးချယ်လိုက်သည့် ထုတ်နှုတ်ယူမည့် နည်းလမ်းက အရင်းခံဒစ်ဂျစ်တယ်ပစ္စည်းပေါ်သို့ အကျိုးသက်ရောက်မှု ရှိသွား

နိုင်သည်ကို သဘောပေါက်နားလည်ထားရမည်ဖြစ်ပြီး ဆိုးကျိုးများကို တတ်နိုင်သမျှ လျော့နည်းအောင် လုပ်ဆောင်ရမည်။

(ဂ) Acquisition ပြုလုပ်မည့်သူသည် ဒစ်ဂျစ်တယ် သက်သေအထောက်အထားကို ထုတ်နှုတ်ရယူရာတွင် သုံးစွဲမည့်သင့်လျော်ရာ Hardware နှင့် Software Tool များကို ကြိုတင်သတ်မှတ်ထားရမည်ဖြစ်ပြီး ၎င်း Tool များ၏ ကန့်သတ်ချက်အသီးသီးကိုလည်း သေချာနားလည်သဘောပေါက်ထားရမည်။

(ဃ) Acquisition ပြုလုပ်မည့်သူသည် ၎င်း Tool များတွင်ဖြစ်ပေါ်တတ်သည့် ပြဿနာများကိုလည်း သိရှိနားလည်ထားရမည်ဖြစ်ပြီး ၎င်းပြဿနာများကို လျော့ချနိုင်မည့် နည်းလမ်းများကိုလည်း စီမံဆောင်ရွက်ထားရမည်။

(င) Acquisition ပြုလုပ်မည့်သူသည် သက်သေအထောက်အထားကို ထုတ်နှုတ်ရယူခြင်းမတိုင်မီ လိုအပ်ပါက ကူးယူသိမ်းဆည်းမည့် မီဒီယာတစ်ခုကို ပြင်ဆင်ထားရမည်။

(စ) Acquisition ပြုလုပ်မည့်သူသည် ဥပဒေရေးရာနှင့်ပတ်သက်ပြီး ရှင်းလင်းချက်လိုအပ်ပါက သင့်လျော်သော ဥပဒေရေးရာအကြံပေးနှင့် ဆွေးနွေးတိုင်ပင်ရမည်။

သက်သေအထောက်အထားထုတ်နှုတ်ရယူခြင်း

၈။ ဒစ်ဂျစ်တယ်သက်သေအထောက်အထားသည် ပျက်စီးလွယ်ပြီး မသင့်လျော်စွာ ကိုင်တွယ်ဖြေရှင်းစစ်ဆေးခြင်းအားဖြင့် အလွယ်တကူ ပြောင်းလဲနိုင်၊ ပျက်စီးနိုင်၊ ဖျက်ဆီးနိုင်ပါသည်။ သို့ဖြစ်ပါ၍ သက်သေအထောက်အထားကို ထိန်းသိမ်းရန်အတွက် အထူးကြိုတင်ကာကွယ်မှုများအား အောက်ပါအတိုင်း ဆောင်ရွက်ထားရန် လိုအပ်ပါသည်။

(က) မူရင်းအချက်အလက်၏ ပြောင်းလဲမှုကို ဖြစ်ပေါ်စေခြင်းမရှိဘဲ ဒစ်ဂျစ်တယ် သက်သေအထောက်အထားကို ရယူရမည်။ သို့ရာတွင် မိုဘိုင်း Forensics ကဲ့သို့သော အချို့ကိစ္စရပ်များတွင် ခွင်းချက်ရှိနိုင်သည်။

(ခ) မူရင်း ဒစ်ဂျစ်တယ်သက်သေအထောက်အထား၏ စစ်မှန်မှုကို ထိန်းသိမ်းနိုင်ရန် သက်သေအထောက်အထားကို ကော်ပီတစ်စုံထက်မက ကူးယူထားရမည်။

(ဂ) မူရင်းသက်သေ အထောက်အထားနှင့် ၎င်းကိုကူးယူထားသည့် ဖိုင်တို့၏ Hash တန်ဖိုးများ တူညီရမည်။ သို့ရာတွင် မိုဘိုင်း Forensics ကဲ့သို့သော အချို့ကိစ္စရပ်များတွင် ခွင်းချက်ရှိနိုင်ပါသည်။

သက်သေအထောက်အထားကို စစ်ဆေးခြင်း

၉။ သက်သေအထောက်အထားကို စစ်ဆေးရာတွင် စစ်ဆေးသူအနေဖြင့် အောက်ပါအချက်များအား အထူးဂရုပြု လိုက်နာဆောင်ရွက်ရမည်-

(က) မူရင်းသက်သေအထောက်အထားကို အသုံးပြုစစ်ဆေးခြင်းအား တတ်နိုင်သမျှ ရှောင်ကြဉ်ရမည်။

(ခ) မူရင်းအထောက်အထား၏ ပထမကော်ပီကို စစ်ဆေးခြင်းမပြုပဲ ပွားယူထားသည့် ဒုတိယကော်ပီကိုသာ စစ်ဆေးရမည်။

(ဂ) ရှောင်လွဲ၍မရသောအခြေအနေတွင် မူရင်းအထောက်အထားကို Write Blocker အသုံးပြုပြီး ရယူစစ်ဆေးရမည်။

(ဃ) စစ်ဆေးရန် တောင်းဆိုထားသူ၏ တောင်းဆိုချက်တွင်ပါရှိသော အချက်များကိုသာ စစ်ဆေးရမည်။ ဥပမာပြရလျှင် ဗွီဒီယိုဖိုင်များကိုသာ စစ်ဆေးပေးရန် တောင်းဆိုပါက ဖုန်းအဝင်အထွက်ခေါ်ဆိုမှုများနှင့်အခြားသော မသက်ဆိုင်သော ဖိုင်များကို စစ်ဆေးခြင်းမပြုလုပ်ရ။

(င) စစ်ဆေးသူ မအားလပ်၍ သက်သေအထောက်အထားကို စစ်ဆေးရန် ရပ်နားထားပါက သက်သေအထောက်အထားကို လုံခြုံစွာ သိမ်းဆည်းထားရမည်။

အစီရင်ခံတင်ပြခြင်း

၁၀။ စစ်ဆေးတွေ့ရှိချက်များကို ရှင်းရှင်းလင်းလင်းနှင့် နားလည်လွယ်အောင် ရေးသားရမည်။ စစ်ဆေးမှုရလဒ်ကို စနစ်တကျဖြင့် အတိုချုံးဖော်ပြရမည်ဖြစ်ပြီး စစ်ဆေးရန်တောင်းဆိုသူ၏ တောင်းဆိုချက်ကို ထိထိမိမိနှင့် ရှင်းလင်းပြည့်စုံအောင် ဖော်ပြရမည်။ စစ်ဆေးသူသည် သက်သေအထောက်အထားအပေါ် လေ့လာဆန်းစစ်ချက်ရလဒ်များနှင့် တွေ့ရှိချက်များကို တိကျမှန်ကန်ပြည့်စုံစွာ အစီရင်ခံရန်တာဝန်ရှိသည်။ အစီရင်ခံတင်ပြချက်တွင် အောက်ပါအချက်တို့ ပါဝင်ရမည်-

(က) အစီရင်ခံရမည့် ဌာန (သို့) အဖွဲ့အစည်း၊

(ခ) စစ်ဆေးမှုပြုလုပ်သည့် နေရာဌာန၊

(ဂ) သက်သေအထောက်အထားအတွက် တင်ပြပေးပို့မှုနံပါတ်၊

(ဃ) စစ်ဆေးရန်တောင်းဆိုသူ၏ ရာထူး၊ အဆင့်နှင့် ဆက်သွယ်ရန် အချက်အလက်၊

(င) လက်ခံရရှိသည့်နေ့စွဲ၊

(စ) အစီရင်ခံတင်ပြချက် ပေးပို့သည့်နေ့စွဲ၊

(ဆ) စစ်ဆေးရန်အတွက် ပေးပို့လာသည့် ပစ္စည်းအသီးသီး၏ Model နံပါတ်၊ Serial နံပါတ်များ စသည်တို့ပါဝင်သည့် ဖော်ပြချက်စာရင်း၊

(ဇ) စစ်ဆေးစဉ်အတွင်း ဖျက်ထားသည့်ဖိုင်များကို ပြန်လည်ရယူခြင်းနှင့် Log၊ String စသည်များကို ရှာဖွေခြင်းကဲ့သို့သော စစ်ဆေးစဉ်အတွင်း ပြုလုပ်ခဲ့သည့် နည်းလမ်းနှင့် လုပ်ငန်းစဉ်များကို အကျဉ်းချုပ်ဖော်ပြချက်၊

(ဈ) ရလဒ်နှင့် နိဂုံးချုပ်သုံးသပ်ချက်၊

(ည) စစ်ဆေးသူ၏ရာထူး၊ အဆင့်နှင့် လက်မှတ်၊

၁၁။ အစီရင်ခံတင်ပြချက်နှင့်အတူပါဝင်မည့်အထောက်အကူပြုပစ္စည်းများဖြစ်သည့် သက်သေအထောက်အထားအချို့၏ Printout များ၊ သက်သေအထောက်အထားများ၏ ဒစ်ဂျစ်တယ် ကော်ပီများ၊ သက်သေအထောက်အထား ထိန်းသိမ်းထားမှု မှတ်တမ်းမှတ်ရာ (Chain of Custody Documentation) စသည်တို့ကိုလည်း စာရင်းပြုစုထားရမည်။

သက်သေအထောက်အထားသိမ်းဆည်းမှု

၁၂။ သက်သေအထောက်အထားများကို သိမ်းဆည်းရာတွင် အောက်ပါအတိုင်း လိုက်နာဆောင်ရွက်ရမည်-

(က) ဒစ်ဂျစ်တယ် သက်သေအထောက်အထားများကို လုံခြုံသည့်နေရာတွင် ရယူခွင့်အကန့်အသတ်ဖြင့် သိမ်းဆည်းရမည်။

(ခ) သက်သေအထောက်အထားသိုလှောင်ခန်းမှ သက်သေအထောက်အထား အသွင်းအထုတ် မှတ်တမ်းကို ထားရှိဆောင်ရွက်ရမည်။

(ဂ) သက်သေ အထောက်အထားများကို ရေ၊ အပူ၊ စိုထိုင်းဆနှင့် လျှပ်စစ်သံလိုက်စက်ကွင်း စသည်တို့၏ ဘေးအန္တရာယ်မှ ကင်းလွတ်အောင် အထူးဂရုပြု သိမ်းဆည်းရမည်။

(ဃ) သက်သေအထောက်အထား ထိန်းသိမ်းထားမှု အချိန်ကာလကို အထက်ဌာန၏ မူဝါဒအရ လိုက်နာဆောင်ရွက်ရမည်။

ကိုးကားစာရင်း

1. Global Guidelines for Digital Forensics Laboratories, Interpol
2. Forensics Examination of Digital Evidence: A Guide for Law Enforcement, U.S. Department of Justice
3. SWGDE Best Practices for Computer Forensic Acquisitions, Scientific Working Group on Digital Evidence
4. SWGDE Model Standard Operation Procedures for Computer Forensics, Scientific Working Group on Digital Evidence