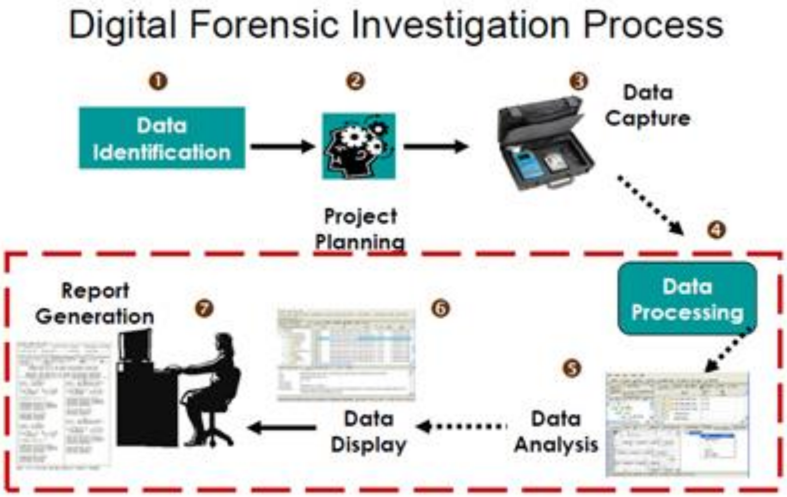
Digital Forensics အကြောင်း သိကောင်းစရာ

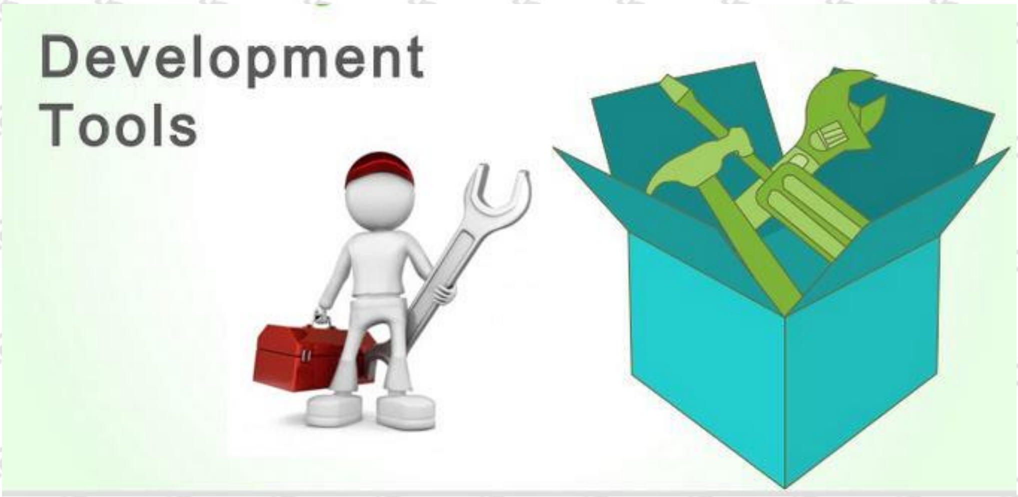
Digital Forensics ဆိုသည်မှာ Digital Device များအား စုံစမ်းရှာဖွေခြင်းနှင့် ပြန်လည်ရယူခြင်း စသည့် သိပ္ပံနည်းကျ စုံစမ်းလေ့လာခြင်း၏ အမျိုးအစားတစ်ခုဖြစ်ပြီး ကွန်ပျူတာဆိုင်ရာ ရာဇဝတ်မှုဖြင့်လည်း သက်ဆိုင်သော စုံစမ်းလေ့လာခြင်းဖြစ်ပါသည်။ Digital Forensics ကို အစောပိုင်းတွင် Computer Forensic ဟူ၍ အသုံးပြုကြပြီး Digital Data များကို သိုလှောင်ထားသော Device များအားလုံး၏ စုံစမ်းရှာဖွေခြင်းသည်ပို၍ ကျယ်ပြန့်လာပါသည်။



Development of Forensic Tools

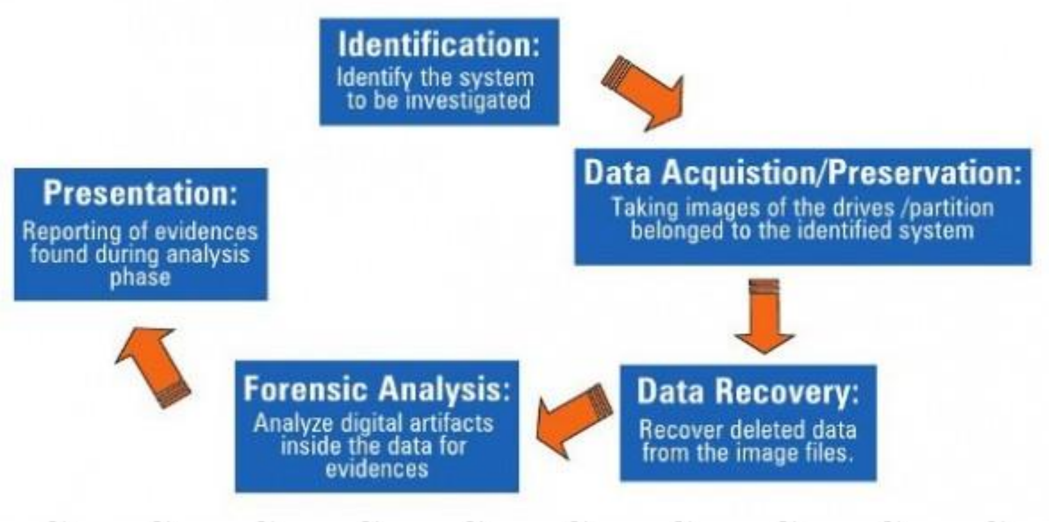
လွန်ခဲ့သော ၁၉၈၀ ဝန်းကျင်တွင် Digital Forensic Tools များအနည်းငယ်သာရှိခဲ့သည်။ သို့ဖြစ်သောကြောင့် စုံစမ်းရှာဖွေသူများသည် မကြာခဏ Media ပေါ်မှ Analysis လုပ်ခြင်းကို live အနေဖြင့်လုပ်ဆောင်ခြင်း၊ operating system များကို Sysadmin Tools အသုံးပြု၍ Evidence များကို ဖော်ပြပေးရန် ကွန်ပျူတာတွင်စစ်ဆေးခြင်းတို့ကိုသာ အသုံးပြုခဲ့ပါသည်။ အဆိုပါ Practice များဖြင့် ၁၉၉၀ တွင် Digital Forensic Tools များစွာကို တီထွင်နိုင်ခဲ့ကြပါသည်။

Copyright © 2015, Myanmar Computer Emergency Response Team, mmCERT/cc



Forensic Process

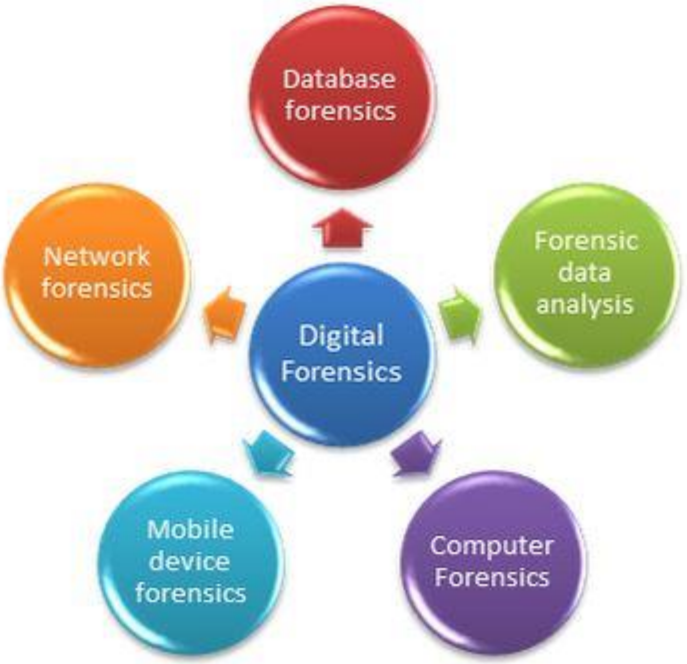
Digital Forensic ပိုင်းဆိုင်ရာ စုံစမ်းရှာဖွေခြင်းကို လုပ်ဆောင်ရာတွင် အများအားဖြင့် Acquisition၊ Analysis၊ Reporting အပိုင်း ၃ ပိုင်းပါဝင်ပါသည်။ Acquisition တွင် ကွန်ပျူတာ RAM များ၏ ပုံရိပ်ကိုဖမ်းယူခြင်း၊ လူထုဆက်သွယ်ရေးလမ်းကြောင်း၏ တိကျသော Sector Level နစ်ခုဖန်တီးခြင်း၊ Device များကို မူလပုံစံအတိုင်း ပြုပြင်ပြောင်းလည်းမှု မရှိနိုင်အောင်ကာကွယ်ခြင်း စသည်တို့ ပါဝင်သည်။ Analysis လုပ်နေစဉ်တွင် Investigator အနေဖြင့် အမျိုးမျိုးသော နည်းစနစ်များ Tools များကိုအသုံးပြု၍ Evidence Material များကို ပြန်လည်ရယူခြင်း၊ Registry အချက်အလက်များနှင့် ဖျက်ထားသော File များကို ပြန်လည်ရယူခြင်း စသည်တို့ကို လုပ်ဆောင်ရပါမည်။ ထိုသို့ Investigation ပြုလုပ်၍ Data များကို ပြန်လည်ရရှိသောအခါတွင် ပုံမှန်အားဖြင့် ၄င်းနှင့် ပတ်သက်သော အကြောင်းအရာများကို Report ရေးသင့်ပါသည်။



Copyright © 2015, Myanmar Computer Emergency Response Team, mmCERT/cc

Branches

စုံစမ်းရှာဖွေခြင်းကို နည်းပညာအားဖြင့် Digital Device များဖြင့် ဆက်နွယ်၍ ကွန်ပျူတာဆိုင်ရာ စုံစမ်းလေ့လာခြင်း၊ ကွန်ယက်ပိုင်းဆိုင်ရာ စုံစမ်းလေ့လာခြင်း ၊ Malware များအား စုံစမ်းလေ့လာခြင်း၊ အင်တာနက်နှင့်ပတ်သက်သည်များကို စုံစမ်းလေ့လာခြင်း နှင့် Mobile Device များအား စုံစမ်းလေ့လာခြင်း စသည်ဖြင့် အမျိုးမျိုးခွဲခြားနိုင်သည်။



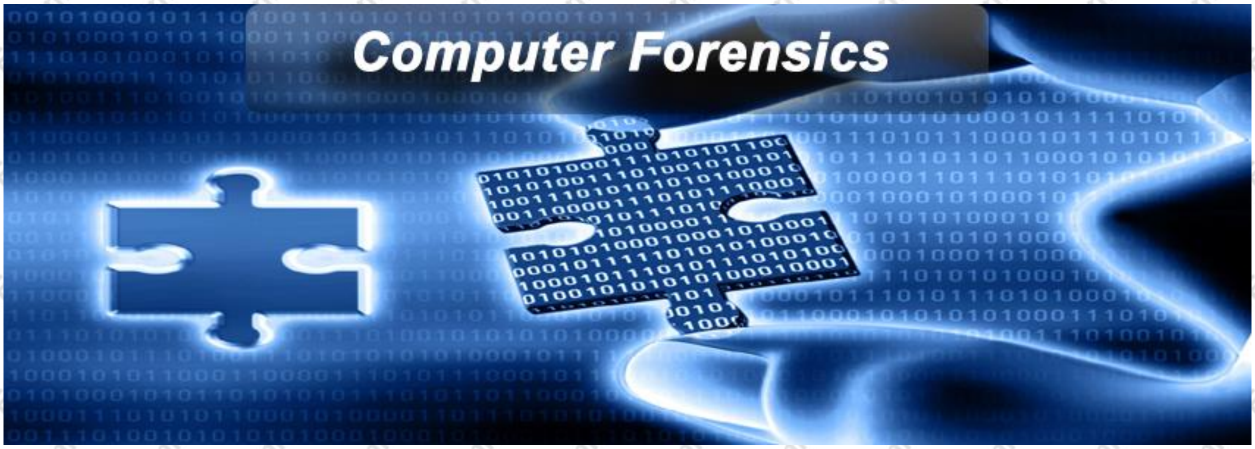
Computer Forensics

Computer Forensics သည် Computer science ၏ အလွန်အရေးကြီးသော အပိုင်းတစ်ခုဖြစ်ပြီး ကွန်ပျူတာ၊ အင်တာနက် ရာဇဝတ်မှုများနှင့်လည်း ဆက်နွယ်ပါသည်။ Computer Forensics ၏ ရည်ရွယ်ချက်မှာ Digital Data များမှ Crime နှင့် ပတ်သက်သော အသေးစိတ်ကို Investigation လုပ်ဆောင်ရန်၊ Digital ပိုင်းဆိုင်ရာ ပစ္စည်းတစ်ခုခု၏ ရွေ့လျားနေသော အနေအထားကို ဖော်ပြရန် ဥပမာ ကွန်ပျူတာ System၊ Storage Medium နှင့် Electronic Document တို့ဖြစ်သည်။ Computer Forensics ၏ စည်းကမ်းဥပဒေ တွင် ကွန်ပျူတာ၏ USB pen drives ကဲ့သို့ Static Memory ပစ္စည်းနှင့် မူလအခြေခံဖြစ်သော Power၊ Onboard Memory အစရှိသည့် Digital Devices များကို Cover လုပ်ရန်ဖြစ်ပါသည်။

Copyright © 2015, Myanmar Computer Emergency Response Team, mmCERT/cc

ထိုသို့ စုံစမ်းလေ့လာရန်အတွက် Developers များမှ Computer Forensics Tools များစွာကို ဖန်တီးထုတ်လုပ်ခဲ့ပါသည်။ Computer Forensics Tools များကို အောက်ပါအတိုင်း အမျိုးမျိုး ခွဲခြားနိုင်ပါသည်။

- Disk and data capture tools
- File viewers
- File analysis tools
- Registry analysis tools
- Internet analysis tools
- Email analysis tools
- Mobile devices analysis tools
- Mac OS analysis tools
- Network forensics tools
- Database forensics tools



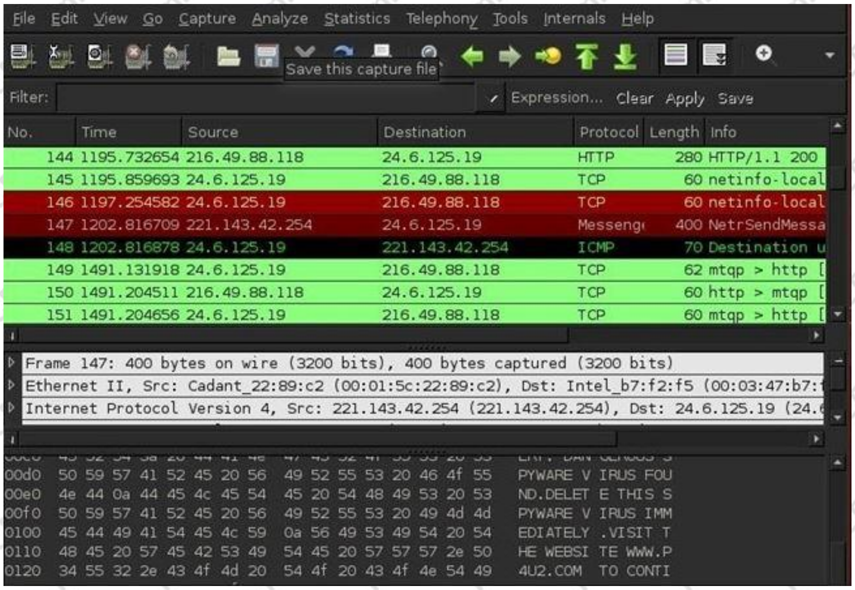
Mobile Device Forensics

Mobile Device Forensics သည် Mobile Device မှ Data သို့မဟုတ် Digital Evidence များကို ပြန်လည် Recover လုပ်ရန် ဆက်နွယ်နေသော Digital Forensic ၏ အစိတ်အပိုင်းတစ်ခု ဖြစ်ပါသည်။ Mobile Forensic သည် ဆက်သွယ်ရေးစနစ် ယန္တရားများ(GSM)၊ ဖုန်း Call Data များနှင့် SMS/Email Data များကို ပြန်လည် Restore ပြန်လုပ်ခြင်း စသည်တို့ကို Forensics လုပ်ဆောင်သဖြင့် Computer Forensic နှင့် ကွဲပြားခြားနားပါသည်။

Copyright © 2015, Myanmar Computer Emergency Response Team, mmCERT/cc

Network Forensics

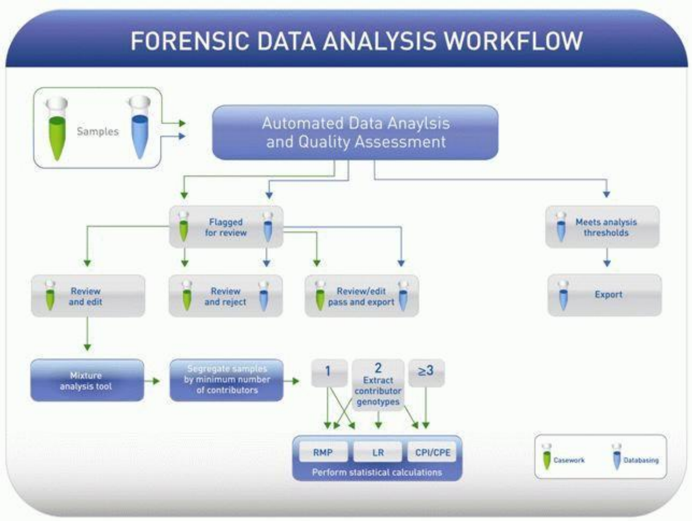
Network forensics သည် ကွန်ပျူတာကွန်ယက်လမ်းကြောင်း LAN နှင့် WAN များကို Morning ပြုလုပ်ခြင်း၊ Analysis ပြုလုပ်ခြင်း၊ Information Gathering ပြုလုပ်ခြင်း၊ Evidence များကို စုဆောင်းခြင်း၊ Intrusion Detection ပြုလုပ်ခြင်း စသည်တို့နှင့် သက်ဆိုင်ပါသည်။



Copyright © 2015, Myanmar Computer Emergency Response Team, mmCERT/cc

Forensic Data Analysis

Forensic Data Analysis သည် Digital Forensics ၏ အစိတ်အပိုင်းတစ်ခုဖြစ်ပြီး ငွေရေးကြေးရေးပိုင်းဆိုင်ရာ ရာဇဝတ်မှု၏ အကျိုးဆက်ဖြစ်ပေါ်နေသော လုပ်ရှားမှုများကို စုံစမ်းစစ်ဆေးရန် ရည်ရွယ်ပါသည်။



Database Forensics

Forensic Data Analysis သည် Digital Forensics ၏ အစိတ်အပိုင်းတစ်ခုဖြစ်ပြီး DataBase များနှင့် ၄င်းတို့၏ Metadata များကို စုံစမ်းလေ့လာခြင်းနှင့် သက်ဆိုင်ပါသည်။ ၄င်းတွင် Log File များ၊ RAM Data များနှင့် ဆက်စပ်ပတ်သက်နေသော DataBase Contents များကို ပြန်လည် စုံစမ်းစစ်ဆေးရန် နှင့် Recover ပြန်လည်လုပ်ဆောင်ရန်ဖြစ်သည်။

Copyright © 2015, Myanmar Computer Emergency Response Team, mmCERT/cc

Reference:

https://en.wikipedia.org/wiki/Digital_forensics

Copyright © 2015, Myanmar Computer Emergency Response Team, mmCERT/cc