सायबर फॉरेन्सिक तपास

-मार्गदर्शक पुस्तिका

FORnSEC SOLUTIONS

SACHIN SATHE

Copyright-FORnSEC Solutions

सायबर फॉरेन्सिक तपास

-मार्गदर्शक पुस्तिका

लेखक

सचिन साठे

संपादक
आरान्शा बडगे

द्वारा प्रकाशित

कॉपीराइट
2020

Copyright-FORnSEC Solutions

लेखक प्रोफाइल

श्री.सचिन साठे (PGDC, CHFI)

ते सायबर फॉरेन्सिक तज्ज्ञ असून, त्यांनी FORnSEC Solutions मध्ये एक जबाबदार अधिकृत स्थान व्यापले आहे.

त्यांनी विविध कायद्याची अंमलबजावणी करणार्या संस्थांसाठी नागपूरमध्ये आणि बाहेर सायबर फॉरेन्सिक तपास प्रकरणे हाताळली आहे. ते सायबर वक्तृत्वकला, युनायटेडस्टेट्स आणि EC-परिषद प्रमाणित सायबर फॉरेन्सिक तपासनीस नागपूर पदव्युत्तर आहे . त्यांनी सायबर फॉरेन्सिक तपास क्षेत्रात ८ वर्षांहून अधिक अनुभव घेतला आहे. तसेच 3000 पेक्षा जास्त LEA प्रकरणांची तपासणी केली आहे आणि 1000 खाजगी प्रकरणांची तपासणी केली आहे. काही बाबतींमध्ये ते देखील LEA च्या पुढील प्रक्रियेसाठी वैयक्तिकरित्या न्यायालयात उपस्थित झाले आहेत.

गेल्या काही वर्षांपासून त्यांनी नागपूर ग्रामीण सायबर सेल, नागपूर शहरातील सायबर सेल आणि अन्य स्थानिक पोलिस स्टेशनसाठी सायबर फॉरेन्सिक कन्सल्टंसींग तसेच खाजगी महाविद्यालये व संस्थाही पुरविल्या आहेत. ते विविध पोलिस विभाग आणि महाविद्यालयांना प्रशिक्षण आणि अतिथी व्याख्यानही देतात.

copyright-FORnSEC Solutions

साहित्य

पाठ १: परिचय......5

पाठ २: सायबरगुन्हे......7

२.१: वर्गीकरण

२.२: प्रकार

२.३: तंत्रज्ञान

पाठ ३: डिजिटलपुरावा......13

३.१: 'पंचनामा' करतांना मुद्दांचा विचार करणे गरजेचे

पाठ ४: डिजिटल फॉरेन्सिक......19

४.१: डिजिटल फॉरेन्सिक प्रकार

पाठ ५: प्राथमिक तपास पाऊल......22

पाठ ६: प्रथम प्रतिसादकर्ता टूलकिट......24

६.१: फॉरेन्सिक इमेजर सॉफ्टवेअर

- फॉरेन्सिक प्रतिकृती

Copyright-FORnSEC Solutions

६.२: हॅशकॅल्क्युलेटर

- हॅशकॅल्क्युलेटर आणि अहवाल निर्मिती (रिपोर्ट जनरेशन)

६.३: USB गार्ड

-राईट ब्लॉकर टूल

६.४: सिम कार्ड रीडर

६.४.१: सिम कार्ड डेटा विश्लेषण सॉफ्टवेअर

६.५: सिग्नल बॅग अवरोधित

- फॅरेडेबॅग

६.६: मोबाइल डेटा पुनर्प्राप्ती (recovery) सॉफ्टवेअर

- डॉ. फोन वंडरशेर

६.७: पुरावा संकलन बॅग

- अँटी स्टॅटिक बॅग

६.८: मेमरी कार्ड रीडर

पाठ ७: कायदा २००८...33

पाठ ८: घटनेचा अभ्यास...37

Copyright FORnSEC Solutions

पाठ १

परिचय

या पुस्तकाचा हेतू सायबर गुन्हेगाराविषयी जागरुकता निर्माण करणे आणि कायद्याची अंमलबजावणी करणार्या एजन्सीची योग्य तंत्र आणि प्राथमिक स्तरावरील सायबर फॉरेन्सिक तपासणी करणे हे आहे.

तंत्रज्ञान इतके जलद गतीने वाढले आहे की आता गोष्टी इलेक्ट्रॉनिक, तांत्रिक आणि संगणक-आधारित बनल्या आहेत. संगणक गुन्ह्यांचा वाढते दर; सायबर गुन्हेगार जसे की हॅकर्स, फसवणूक करणारे आणि अन्य सायबर गुन्हेगार पूर्वीपेक्षा अधिक शक्तिशाली होतात आणि वृत्तपत्र आणि मिडियाच्या इतर स्वरूपातील मध्यस्थ आणि बुलेटिन व्यापत आहेत.तर, सायबर हल्ल्यांच्या वारंवारता आणि सुसंस्कृतपणासह; आता संगणक (कंप्यूटर) फॉरेन्सिक आणि त्याच्याशी निगडित विविध मार्ग माहित असणे आता खूप आवश्यक बनले आहे. हे पुस्तक प्रामुख्याने प्रथम प्रतिसाद टूलकिट

बद्दल आहे ज्यामध्ये डिजिटल फॉरेन्सिक साधने आणि हार्डवेअर असतात ज्यात उत्पादक संगणक तपासणी करण्यात मदत होते. मूलभूत कॉरपोरेट फॉरेन्सिक साधनांच्या समर्थनासह डिजिटल डेटा प्राप्त करताना योग्य प्रोटोकॉल आणि कार्यपद्धती अंमलात आणून हे पुस्तक आपल्याला अपराध दृश्यात डिजिटल पुराव्यासह हाताळण्यास मदत करेल. डिजिटल पुराव्यांवर कब्जा करताना आणि डिजिटल पुराव्याच्या चेकसमची निर्मिती करताना न्यायालयीन स्थितीत कायदेशीररित्या धरून ठेवता यावे, यासाठी हे पुस्तक गुन्हाच्या घटनेवर ' पंचनामा ' भरण्याविषयी माहिती देतात. डिजिटल पुराव्याला सुरक्षितपणे हाताळणं आणि

Copyright-FORnSEC Solutions

सुरक्षित माहिती साठवून ठेवणं आवश्यक आहे जेणेकरुन महत्वाच्या माहितीची माहिती नष्ट होऊ नये. हे डिजिटल पुराव्याच्या तपासणीदरम्यान सर्वात सामान्य परिस्थिती आणि अडचणींमधून मार्गदर्शन करेल.

पुस्तकाच्या शेवटी, घटनेचा अभ्यासाचे उदाहरण व्यावहारिक दृष्टीकोन आणि अनुभवांसाठी सादर केले आहेत. बुकलेटमध्ये दिलेली साधने आणि पद्धती आपल्याला सर्वात प्रभावी पध्दतीने सायबर गुन्हेगारीची तपासणी करण्यास मदत करतील.

Copyright-FORnSEC Solutions

पाठ २

सायबर

सायबर गुन्हे हे असे गुन्हे आहेत जे डिजिटल पुरावे जसे संगणक, मोबाईल आणि इंटरनेट यांचा समावेश करतात. काही प्रकरणांमध्ये संगणक हे गुन्हा करण्यासाठी वापरले गेले असावे आणि इतर बाबतीत संगणक हे गुन्हा लक्ष्य म्हणून वापरले गेले असावे.

सोप्या शब्दात, सायबर गुन्हे हे संगणक, मोबाईल आणि इंटरनेटचा वापर करणारी गुन्हेगारी कृती आहे जे कायद्याच्या विरोधात आहे.

२.१: सायबर गुन्हे वर्गीकरण

सायबर गुन्हे सामान्यपणे खालील तीन श्रेणींमध्ये वर्गीकृत केले जाऊ शकतात -

व्यक्तीविरुद्ध सायबर गुन्हे - व्यक्तीविरुद्ध सायबर गुन्हेगारीमध्ये सायबर छळवणूक, DOS हल्ला, सायबर स्टॉकिंग, बाल पोर्नोग्राफी, ईमेल गुन्हा अशा विविध गुन्ह्यांचा समावेश आहे. या गुन्ह्यांना लोभी व्यक्तीपासून वैयक्तिक बदलासाठी विविध कारणांसाठी निर्देशित केले जातात. सायबर गुन्ह्यांचा हा प्रकार हा यंगस्टर्ससाठी धोकादायक धोका आहे आणि जर त्यांच्यावर नियंत्रण ठेवले नाही तर त्यांच्यावर अवांछित आघात उरला असेल.

Copyright-FORnSEC Solutions

मालमत्ता विरुद्ध सायबर गुन्हे - अशा प्रकारचा सायबर गुन्हा सर्व प्रकारच्या संपत्तीवर आधारित आहे आणि यात संगणक चोरी देखील समाविष्ट आहे. ही वाढती समस्या आहे आणि तंत्रज्ञानाच्या प्रवेशासह वाढीसह बहुविध वाढ झाली आहे. या संदर्भात 'संपत्ती' म्हणजे केवळ संगणकास किंवा त्यातील घटकच नव्हे तर सॉफ्टवेअर, कॉपराइट्स, ट्रेडमार्क आणि कॉम्प्यूटर सोर्स कोडचाही संदर्भ असतो. या प्रकारच्या गुन्ह्यांना सामान्यपणे विविध हेतूसाठी संस्थेच्या विरोधात लक्ष्य केले जाते.

सरकार आणि समाज विरुद्ध सायबर गुन्हे - इंटरनेटच्या वाढीमुळे सरकार आणि समाजांवर हल्ला होऊ शकला आहे. सरकार आणि सैन्याच्या संवेदनशील वेबसाइट्स हॅक झाल्या आहेत. या संस्था सरकारी वेबसाइट्स आणि बँकांवर हल्ला करण्यासाठी त्यांची युक्ती आणि पद्धत बदलत असतात.

Copyright-FORnSEC Solutions

२.२. सायबर गुन्हेगारीचे प्रकार

सायबर गुन्हे अनेक प्रकारचे आहेत आणि सर्वात सामान्य प्रकार खाली स्पष्ट केले आहे:

आर्थिक गुन्हे - आर्थिक गुन्हे, नावाप्रमाणेच, आर्थिक लाभ मिळविण्यासाठी बांधील आहेत. सर्व अपराधांमागे पैसा हा सामान्य उद्देश आहे. सायबर गुन्हे प्रामुख्याने मजेशीर किंवा सूड किंवा आव्हानापेक्षा आर्थिक फायद्यासाठी बांधील आहेत. फसवणूक करणार्या लोकांसाठी दर मिनिटाला अनेक नवीन तंत्र तयार केले जातात. आर्थिक गुन्हे हे क्रेडिट कार्डची फसवणूक, बँक सर्व्हर आणि आर्थिक घोटाळे मध्ये हॅकिंगपर्यंत मर्यादित नाहीत.

माहिती चोरी -कोणत्याही संस्थेसाठी,माहिती ही कंपनीची प्रमुख मालमत्ता आहे. माहितीची चोरी ही औद्योगिक घुसखोरीसाठी असू शकते. गेल्या काही वर्षांपासून अशी चोरी प्रचंड प्रमाणात वाढत आहे. बहुतांश घटनांमध्ये, आतील बाजू घुसखोरांची माहिती चोरीची जबाबदार असते. माहितीचे रक्षण करण्यासाठी अधिक सुरक्षा उपाय विकसित केले जातात, माहिती चोरीसाठी संवेदनशीलतेचे नवीन भाग उघडण्यात आले आहेत.

सायबर खंडणी -सायबर खंडणी असा गुन्हा आहे ज्यामध्ये एखाद्या एंटरप्राइझवरील हल्ल्याचा किंवा दहशतवादी हल्ल्याचा निषेध करणारा सर्वसाधारणपणे डेनियल ऑफ सर्व्हिस आक्रमण (डीओएस) किंवा इतर प्रकारच्या हल्ल्यांचा वापर करून पैसे रोखण्यासाठी मागणी केली जाते. DoS हल्ला तेव्हा होतो जेव्हा संगणक अधिक विनंत्यांसह भरला जातो जे ते हाताळू शकते. हा हल्ला त्याच्या अधिकृत वापरकर्त्यांना सेवा नाकारतो. कधीकधी, सायबर ह्या प्रमाणीकरणात अत्याधुनिक पैशाचा समावेश असू शकतो जेणेकरून आक्रमण थांबविण्याची हमी दिली जाऊ नये. हे हल्ले दुर्गम ठिकाणे किंवा देशांच्या बनावटी नमुने वापरून नियंत्रित आहेत जेणेकरून गुन्हेगारांना शोधणे कठिण होऊ शकते.

छळ - आभासी छळ मोठ्या प्रमाणात वाढला आहे. हजारो सामाजिक नेटवर्किंग छळाच्या प्रकरणांची नोंदणी दररोज केली जाते. उत्पीड़ना सामान्यतः स्त्रियांना केले जाते परंतु विशिष्ट गटात जसे वंश किंवा धर्म यांचा समावेश केला जाऊ शकतो. उत्पीड़न ईमेलद्वारे किंवा फेसबुक पोस्टद्वारे किंवा सोशल नेटवर्किंग ॲप्लिकेशन्स वर अश्लील आणि आक्षेपार्ह सामग्रीचे प्रेषण केले जाते. हे खोटे आणि त्रासदायक संदेश सामान्यतः खोटे ईमेल खात्याद्वारे पीडितांना पाठवले जातात.

Copyright-FORnSEC Solutions

सायबर पाठलाग -सायबर गुंडगिरीचा अर्थ एका व्यक्तीच्या इंटरनेटवरील हालचालींचा पाठपुरावा करणे आणि ईमेल संदेश पोस्ट करणे, चॅट रूम्स, सोशल मीडिया आणि इतर कोणत्याही ऑनलाईन माध्यमाने ती त्याला भेट देत असलेल्या साइट्सवर त्यांच्यावर गोळीबार करणे. व्यक्तीबद्दल पुरेशी वैयक्तिक माहिती गोळा करून, ते त्रास देण्याची योजना करतात.

बौद्धिक मालमत्ता चोरी - याचा अर्थ सॉफ्टवेअर, कॉपीराइट, ट्रेडमार्क आणि अशा इतर अमूर्त मालमत्तेशी संबंधित अधिकारांची मालकी. जेव्हा मालकांचे हे अधिकार संपूर्णपणे किंवा आंशिकपणे वंचित असतात, तेव्हा ते बौद्धिक संपत्ती अधिकार (आयपीआर) म्हटले जाते. ते विनामूल्य डाउनलोड किंवा अपलोड केलेल्या प्रोग्रामच्या बदल्यात सॉफ्टवेअर उपलब्ध करतात.

संगणक विध्वंस- हे कोणत्याही भौतिक संगणक हानीकडे किंवा त्याच्या भागांना संगणकीय विध्वंस म्हणून ओळखले जाते. यात संगणकाची चोरी, त्याचे भाग किंवा उपकरणे किंवा कोणत्याही प्रकारचे नुकसान किंवा त्यांना झालेल्या कोणत्याही प्रकारच्या हानीचा समावेश होऊ शकतो.

संगणक बर्फाळ एक कार्यक्रम आहे जो दुर्भावनापूर्ण कार्य करतो जसे की वापरकर्त्यांचे संकेतशब्द किंवा इतर डेटा काढणे किंवा हार्ड डिस्क मिटविणे.

Copyright-FORnSEC Solutions

२.३ सायबर तंत्र

संगणक व्हायरस आणि वर्म्स -व्हायरस एक दुर्भावनापूर्ण प्रोग्राम आहे जो संगणकास हानी होऊ शकतो. हे स्वत: ची प्रतिकृती कार्यक्रम आहे जे स्वत: च्या इतर कॉपी करण्यायोग्य कोडमध्ये संलग्न करुन स्वतःचे कोड तयार करते. व्हायरस डेटा भ्रष्ट किंवा हटवू शकतो.

फिशिंग / स्पूफिंग -_हा हल्ला वेगवान वाढणारा ऑनलाइन घोटाळा आहे. या प्रकारच्या हल्ल्यात, सायबर गुन्हेगारी बनावट वेबसाइट तयार करते जे वास्तविक दिसते आणि सहसा ईमेल आणि मुखवटे विश्वासू संस्थेच्या रूपात पाठवले जाते. या तंत्राला फिशिंग म्हणतात. सायबर गुन्हेगारी आपल्याला लॉटरी ईमेल देखील पाठवू शकतात आणि आपल्या तपशीलांसाठी जसे क्रेडिट कार्ड तपशील, बँक खाते तपशील आणि इतर अशी माहिती देऊ शकतात.

DoS हल्ला - हा हल्ला एक अशी तंत्र आहे जो वेबसाइट किंवा सेवा अनुपलब्ध करते. विशेषत: साइट किंवा नेटवर्कच्या खाली विनंत्या करणार्या विनंत्यांद्वारे अनेक संगणक वापरुन हे प्राप्त केले जाते अशा प्रकारचा आक्रमण कदाचित तुमची वेबसाइट तात्पुरती किंवा कायमस्वरूपी कामकाजापासून रोखू शकते आणि परिणामी डेटा व आर्थिक नुकसान होऊ शकते.

Copyright-FORnSEC Solutions

सामाजिक अभियांत्रिकी - हे एक पद्धत आहे जेथे सायबर गुन्हेगार ईमेल किंवा फोन कॉलचा वापर करतात. ते आपला आत्मविश्वास वाढवण्याचा प्रयत्न करतात आणि प्रत्यक्ष ओळख म्हणून ठाम करतात आणि त्यांना आवश्यक माहिती मिळवितात. ही माहिती आपल्या बँक खात्याचे तपशील, पैसे, आपली कंपनी किंवा सायबर गुन्हेगारांसाठी उपयोगी असू शकते अशी कोणतीही गोष्ट असू शकते.

ओळख चोरी -ओळख चोरी हा सायबर क्राइममधील सर्वात सामान्य प्रकारांपैकी एक आहे. टर्म आयडेंटिटी चोरीचा उपयोग केला जातो, जेव्हा एखादी व्यक्ती आर्थिक लाभांकरिता फसवे करण्यासाठी काही इतर व्यक्तीची इच्छा असते. इतरांची ओळख माहिती चोरणारे सर्वसाधारण स्त्रोत म्हणजे खाजगी, सरकारी किंवा फेडरल वेबसाइटच्या डेटाच्या उल्लंघनांपासून ज्यात आर्थिक तपशील समाविष्ट आहे.

Copyright-FORnSEC Solutions

पाठ ३

डिजिटल पुरावा

डिजिटल पुरावे किंवा इलेक्ट्रॉनिक पुरावे हे डिजिटल स्वरूपात संग्रहित किंवा संक्रमित केलेली कोणतीही संभाव्य माहिती आहे जी न्यायालयीन प्रकरणाचा पक्ष चाचणीस वापरली जाऊ शकते

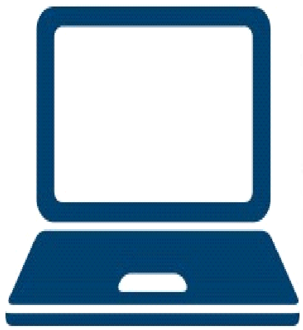
दुस-या शब्दात, एका इलेक्ट्रॉनिक साधनाद्वारे संग्रहित, प्राप्त किंवा प्रेषित केलेल्या एखाद्या अन्वेषणानुसार माहिती आणि डेटा मूल्य म्हणून डिजिटल पुरावे परिभाषित केले जातात.

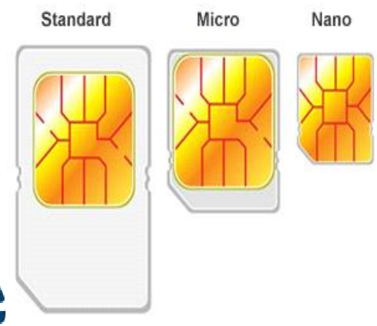
आजच्या युगात, डिजिटल गॅझेट्सचा वापर सर्व लोकांपर्यंत आणि सर्व ठिकाणी केला जातो. जेव्हा संगणक, मोबाइल फोन, लॅपटॉप्स, टॅब्लेट आणि इतर इलेक्ट्रॉनिक्स डिव्हाइसेसच्या रूपात डिजिटल गॅझेट्स् वापरुन सायबर गुन्ह्यांचा वापर केला जातो तेव्हा डिजिटल पुरावा नाटकामध्ये येतो. हे सायबर आक्रमणसाठी एक माध्यम म्हणून वापरले जातात प्रत्येक वेळी, जेव्हा सायबर गुन्ह्यांमुळे डिजिटल प्रिंटचे ट्रेस सोडले जाते तेव्हा हे सायबर गुन्हेगारांना शोधण्यात मदत करते. योग्य छापण्याच्या साधनांसह गुन्हेगारीवर सापडलेल्या डिजिटल उपकरणांची तपासणी आणि तपासणीनंतर हे छापे मिळवता येतात. डिजिटल पुरावे इ-मेल, सोशल नेटवर्किंग साईट्स, एटीएम लॉग आणि बर्याच गोष्टींमधून मिळू शकतात.

येथे, गुन्हेगारीच्या घटनेबद्दल अन्वेषण करण्यासाठी आपल्याला प्रथम प्रतिसादकर्त्याची आवश्यकता आहे. त्याच्या जबाबदार्या म्हणजे डिजिटल पुरावे ओळखणे, एकत्रित करणे आणि वाहतूक करणे जेणेकरुन पुरावे सुरक्षित करण्यावर

Copyright FORnSEC Solutions

कोणतीही प्रतिकूल प्रभाव पडत नाही जसे त्यांना अत्याधिक तापमान, आर्द्रता आणि स्थिर वीज यांसारखे नुकसान होऊ नये.





डिजिटल पुराव्याचे अनेक स्त्रोत आहेत आणि सर्वात सामान्य आहेत -

१.इंटरनेट.

२.संगणक.

३.मोबाइलफोन.

विविधप्रक्रिया, तंत्र, आणि फॉरेन्सिक साधने पुरावा घेणे सराव केला जातो.

१. इंटरनेट-

गुन्हा करण्याची सर्वात आवश्यक आणि आवश्यक माध्यम म्हणजे 'इंटरनेट'. इंटरनेटमध्ये प्रत्येक डेटा आवश्यक आहे. इंटरनेटच्या मदतीने, माहितीचा वैश्विक प्रवेश गुन्हा दराने अतिशय उच्च वाढला आहे. सायबर गुन्हेगारांनी मुख्यतः सरकारी वेबसाईट किंवा पोर्टल, बँक, नेटवर्क आणि अन्य प्रणालींना पैसे, ओळख, बँक खाते तपशील, वैयक्तिक तपशील आणि इतर मौल्यवान डेटा चोरण्यासाठी लक्ष्य केले आहे. जेव्हा एखादा गुन्हा इंटरनेटवर बांधील असतो तेव्हा बहुतेक वेळा तपासणीस मदत करते तसेच पुराव्याचा एक पुरावा देते ज्यायोगे गुन्हेगारीचा शोध घेणे सोपे होते.

<u>उदाहरणार्थ -</u>आयपी पत्ता बॅकट्रेकिंगद्वारे ईमेल फेटाळला जाऊ शकतो. यात स्थान आणि मालकाची माहिती ज्याला आयपी पत्ता वाटप करण्यात आला त्याबद्दलचे तपशील आणि अशा प्रकारे, गुन्हेगार सापडले जाऊ शकतात.

२. संगणक-

गुन्हा घडवून आणण्यासाठी एक माध्यम माध्यमांचा एक आवश्यक मुख्य स्त्रोत आहे. व्याख्या म्हणते की, इंटरनेट आणि कॉम्प्यूटर हे दोन महत्वाचे साधन आहेत. त्याचवेळी, जेव्हा एखादा संगणक गुन्हा करतो, तेव्हा डिजिटल पुराव्याचे मापन संगणकाच्या हार्ड ड्राइव्हवर होते. गुन्हेगारीच्या घटनेची तपासणी करण्यासाठी, हार्ड ड्राइव्हचा ताबा घेणे डिजिटल पुरावे गोळा करण्याचा एक महत्वाचा स्त्रोत आहे आणि इतर परिधीय साधने जसे पेनड्रीव, बाह्य हार्ड डिस्क, सीडी-रॉम डिस्क आणि इतर डिजिटल मीडिया. हे आवश्यक पुरावे डिजिटल फॉरेन्सिक साधनांच्या सहाय्याने एका यशस्वी तपासणीसाठी विविध प्रक्रिया आणि तंत्रज्ञानासह विश्लेषित करा.

Copyright-FORnSEC Solutions

उदाहरणार्थ -अलीकडे, एक गुन्हेगार एक मंत्री एक धमकी संदेश पाठविले की एक केस आली. संगणकावरून संदेशाचा मागोवा घेण्यासाठी आम्ही हार्डडिस्कचे फॉरेन्सिक साधनासह विश्लेषण केले आणि आम्ही यशस्वीरित्या संदेश पुनर्प्राप्त केला आणि गुन्हेगारांना न्यायालयात दोषी ठरवण्यात आले.

३. मोबाइल फोन्स-

आजकाल, मोबाईल फोन आता कुशलतेने कार्य करणार्या संगणकाचे स्थान घेत आहेत. सेल फोनमध्ये सर्व आवश्यक माहिती जसे की स्थान, व्यक्तिगत दस्तऐवज, संपर्क, संदेश, कॉल इतिहास, डिजिटल फोटो, क्रेडिट कार्ड तपशील आणि बरेच सामान्यतः, सायबर गुन्हेगार या तपशीलांमध्ये प्रवेश करण्यासाठी नेटवर्कद्वारे व्हायरस किंवा मालवेयर इंजेक्शनची पद्धत वापरतात. मोबाईल फोरेन्सिक साधनांचा वापर करून मोबाइल फोनमध्ये पुरावा गोळा केला जाऊ शकतो.

उदाहरणार्थ - सोशल नेटवर्किंगवर जसे की फेसबुकवर पोस्ट केलेली माहिती त्यात स्थान किंवा त्या स्थानापासून ते स्थानावरील तपशील असू शकतात. योग्य तपास करून डिजीटल ॲडव्हान्समुळे मौल्यवान माहिती मिळू शकते आणि न्यायालयामध्ये कायदेशीररित्या सिद्ध केले जाऊ शकते.

Copyright-FORnSEC Solutions

३.१ 'पंचनामा' करत असताना विचारात घेण्याचे मुद्दे

1. उघडती आणि बंद वेळ

प्रथम, प्रारंभ वेळचा उल्लेख करा नंतर गुन्हा देखावाचे विश्लेषण करा आणि नंतर हॅश मूल्य निर्माण करा. मग, हॅश चेकसम निर्मिती केल्या नंतर पुर्णचिन्ह बंद करा.

टीप - पंचनामाला बंद करण्यापूर्वी डिजीटल उपकरणांचे हॅश मूल्य निर्माण केले पाहिजे. जर पंचनामा बंद केल्यानंतर हॅश व्हॅल्यूची निर्मिती होत असेल तर, डिजिटल पुराव्यामध्ये वैधता नसेल.

2. पंचनामा करत असताना, सर्व प्राथमिक डिजिटल उपकरण, सहयोगी वस्तू, सर्व हार्डवेअर उपकरणे, जप्त करण्यात आलेल्या उपकरणांविषयीची माहिती आणि सविस्तर माहिती पूर्ण माहिती गोळा करणे यासारख्या संरक्षणाची एक श्रृंखला कायम ठेवावी.

3. पंचनामा पुर्ण झाल्यावर, write blocker tool वापरल्याशिवाय मूळ पुरावे उघडू नका.

4. पंचगणिच्या वेळी 2 साक्षीदारांची उपस्थित असणे अनिवार्य आहे.

5. उदाहरण- केस माहिती Punchnama मध्ये ठेवणे आवश्यक

Copyright-FORnSEC Solutions

CASE INFORMATION	
Investigator Name:	Agency Name: Station
Investigator Number:	Place of Seizure:
Case Name:	Date of Seizure:
Case Number:	Time of Seizure:
Evidence Number: Hard Disk WD Blue 500gb	Witness Name 1:
Seizure Memo #:	Witness Name 2:
Suspect Name:	

Copyright-FORnSEC SO

पाठ ४:

डिजिटल फॉरेन्सिक

डिजिटल फोरेन्सिक्स (कधीकधी डिजिटल फॉरेन्सिक सायन्स म्हणून ओळखले जाते) फॉरेन्सिक विज्ञान शाखेत असते जे डिजिटल उपकरणांमध्ये सापडलेल्या साहित्याच्या पुनर्प्राप्ती आणि तपासणीस असतात, सहसा संगणक गुन्हाच्या संबंधात.

दुसऱ्या शब्दांत, डिजिटल फोरेन्सिक्स संगणकाचा, मोबाईल फोन, आणि इतर मेमोरी स्टोरेज डिव्हाइसेसच्या संपादन, विश्लेषण, पुनर्प्राप्ती आणि इलेक्ट्रॉनिक्स उपकरणांच्या अहवालासह मदत करतात.

डिजिटल पुराव्या प्राप्त करण्याची प्रक्रिया अशा पद्धतीने केली पाहिजे की ती त्याच्या पुराव्याचे मूल्य जतन करणे आणि कायदेशीर कार्यवाहीमध्ये त्याची स्वीकारार्हता सुनिश्चित करणे आवश्यक आहे.

डिजिटल फॉरेन्सिक प्रक्रियेमध्ये सामान्यत: 3 टप्पे असतात -

1. संपादन / इमेजिंग - त्यात इलेक्ट्रॉनिक उपकरणांची हॅशिंग आणि कॅप्चर करणे आणि मिडियाचा अचूक डुप्लिकेट तयार करणे, सहसा मूळ ब्लॉकचे पुरावे बदलणे किंवा नष्ट करणे टाळण्यासाठी प्रायोजक बनविणे.

2. विश्लेषण - विश्लेषण मूलतः मूळ डिव्हाइसवरुन कॅप्चर केलेल्या प्रतिमेवर केले जाते कारण मूळ डिव्हाइसला संरक्षित करणे आवश्यक होते जेणेकरून ते न्यायालयामध्ये कायम ठेवू शकेल. हे विश्लेषण डिजिटल फॉरेन्सिक साधनाद्वारे योग्य पद्धतीने घेतले जाते.

Copyright-FORnSEC Solutions

प्रत्येक विश्लेषणात, प्रक्रिया वेगवेगळी असते परंतु सामान्य पध्दती असते जसे की फाइल्स, हटविणे किंवा पुनर्प्राप्ती डेटामधील कीवर्ड शोधणे.

3. अहवाल - विश्लेषण तपास केल्यानंतर निष्कर्ष एक स्पष्ट, संक्षिप्त आणि संरचित अहवालात सादर केला जातो. अधिग्रहित आणि मूळ प्रतिमा दोन्ही हॅश करण्यात आली आहेत आणि सत्यापित करा की तुलना केलेल्या कॉपी हॅश अल्गोरिदम सारखी SHA-1 किंवा MD5 वापरून अचूक आहे फॉरेन्सिक तपासणीमध्ये हॅश व्हॅल्यूची गणना करण्याची गरज म्हणजे डिजिटल डेटाची अचूकता सिद्ध करणे आणि इतर कोणतेही बदल करणे शक्य नाही.

४.१ डिजिटल फॉरेन्सिक्सचे प्रकार

डिजिटल फोरेन्सिक्समध्ये उप-शाखांशी संबंधित अनेक उपकरणे समाविष्ट आहेत.

1. कॉम्प्युटर फॉरेन्सिक:

संगणक फोरेन्सिकमध्ये, लक्ष्य म्हणजे हार्ड डिस्क किंवा इतर काढण्यायोग्य साधनांसारख्या स्टोरेज डिव्हाइसेसचे विश्लेषण करणे. ते छायाचित्रे, व्हिडीओज, कागदपत्रे आणि इतर डिस्कवरील माहिती काढून टाकते.

2. मोबाइल फॉरेन्सिक:

मोबाइल फोरेन्सिक मोबाइल फोन किंवा टॅब्लेट वरून पुनर्प्राप्त करण्याशी संबंधित आहे. हे सिमकार्ड डेटाचे विश्लेषण आणि संपर्क पुनर्प्राप्ती, आयएमएसआय, संदेश आणि इतर अनेक आवश्यक माहिती हाताळते. शिवाय, व्हाट्सएप आणि इतर सोशल नेटवर्किंग ऍप्लिकेशन्सची तपासणी केली जाते.

FORnSEC Solutions

3. नेटवर्क फॉरेन्सिक्स:

नेटवर्क फॉरेन्सिक्स माहिती गोळा करणे, पुरावे संकलन किंवा घुसखोरी शोधण्याच्या उद्द्देशाने संगणक नेटवर्क रहदारीचे परीक्षण आणि विश्लेषणाशी संबंधित आहे.

Copyright-FORnSEC Solutions

पाठ ५:

प्राथमिक तपास पायऱ्या

1. संगणक गुन्हा ओळखा.

 - गुन्हेगारीच्या पठडीवर पोहोचल्यानंतर, कोणत्या प्रकारचा सायबर गुन्हा तयार झाला आणि त्यानुसार तपासणी केली.

2. प्राथमिक पुरावा गोळा करणे.

 - गुन्हा देखावा पोहोचण्याआधी प्राथमिक पुरावा गोळा करणे.

3. जप्तीसाठी न्यायालय / उच्च प्राधिकार परवानगी प्राप्त करणे (आवश्यक असल्यास).

 - खासगी छापय़ासाठी आपल्याला परवानगीची पत्रे घ्यावी लागतील.

4. प्रथम प्रतिसादकर्ता टूल सुरू करा.

 - जर संगणक चालू अवस्ते ' मध्ये असेल तर इंटरनेट वापरलेली माहिती, कुकीज इत्यादि गोळा करण्यासाठी प्रथम प्रतिसाद साधनाचा वापर करा आणि त्यानंतर योग्यरित्या संगणक बंद करा आणि हार्डडिस्क काढून टाका 'ऑफ मोड' च्या बाबतीत, कॉम्प्यूटरच्या हार्डडिस्क काढून टाका.

5. गुन्हा साक्ष जप्त करा.

-हार्डडिस्क संगणकावरून व्यवस्थित काढून टाका आणि त्यानंतर पुराव्यांच्या हॅश व्हॅल्यूची निर्मिती करा आणि नंतर स्टिक बॅगमध्ये पुरावे पॅक करा. मोबाईलच्या बाबतीत, मोबाईलचा मोबाईल जप्त करा.

Copyright-FORnSEC Solutions

6. न्यायालयीन प्रयोग शाळेत पुरावा देणे.

- विश्लेषण उद्देशासाठी पुरावा पोहचवा.

7. पुराव्याच्या दोन-बिट प्रवाह प्रती तयार करा

- एक वापरकर्त्यासाठी आणि दुसरी विश्लेषणसाठी.

8. प्रतिमावर SHA1 चेकसम व्युत्पन्न करा

- एकाग्रतेसाठी हॅश मूल्य व्युत्पन्न करा

9. ताब्यात ठेवणे

गुन्हा अन्वेषण करण्यासाठी योग्य पद्धत अवलंबुन प्रकरणांची माहिती पद्धतशीरपणे नोंदवा.

10. एखाद्या सुरक्षित ठिकाणामध्ये मूळ पुरावे संचयित करा.

पुराव्यामध्ये मुक्त ओलावा आणि धातूच्या जागेत साठवून ठेवा जेणेकरून त्यावर परिणाम होऊ नये.

11. पुराव्यासाठी प्रतिमेचे विश्लेषण करा.

- डिजिटल ब्लॉकर उपकरण वापरून डिजीटल पुरावा मिळण्यासाठी डुप्लिकेट कॉपीचे विश्लेषण / पुनर्प्राप्त.

12. फॉरेन्सिक अहवाल तयार करा.

- डिजिटल पुराव्याच्या फॉरेन्सिक अहवाल व्युत्पन्न करा आणि आरोपपत्रांसह जोडा.

13. आवश्यक असल्यास, न्यायालयात उपस्थित रहा आणि तज्ञ म्हणून साक्ष द्या.

Copyright-FORnSEC Solutions

पाठ ६:

प्रथम प्रतिसादकर्ता टूलकिट

६.१: फॉरन्सिक इमेजर सॉफ्टवेअर - फॉरन्सिक रेप्लिकेटर

६.२: हॅश कॅल्क्युलेटर - हॅश कॅल्क्युलेटर आणि रिपोर्ट जनरेशन

६.३: USB संरक्षित - ब्लॉक करा उपकरण टाइप करा

६.४: सिम कार्ड रीडर

६. ४.१: सिम कार्ड डेटा विश्लेषण सॉफ्टवेअर - सिम कार्ड जप्ती

६.५: सिग्नल ब्लॉकिंग - फॅरडे बॅग

६.६: मोबाईल डेटा पुनर्प्राप्ती सॉफ्टवेअर - डॉ.फोन वंडर्सशेअर

६.७: पुरावा संग्रह बॅग - अँटी स्टॅटिक बॅग

६.८: मेमरी कार्ड रीडर

Copyright-FORnSEC Solutions

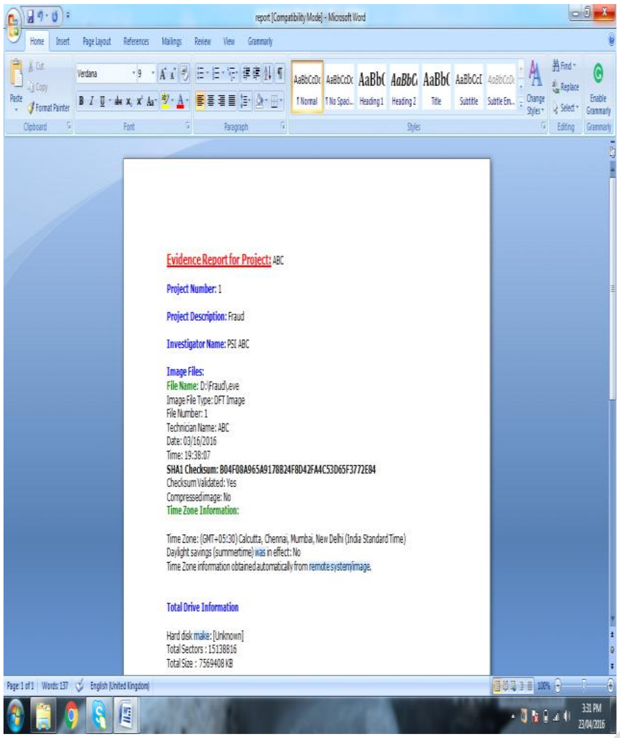
६.१: फॉरन्सिक इमेजर सॉफ्टवेअर - फॉरन्सिक रेप्लिकेटर

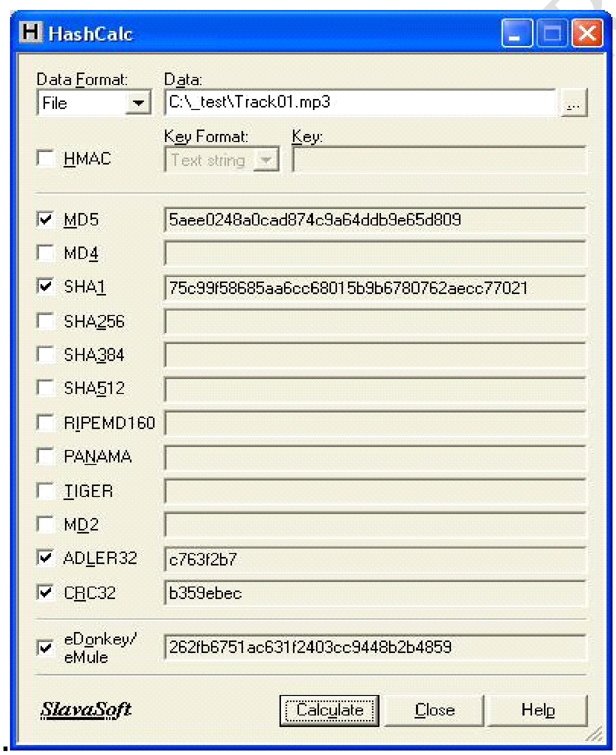
फॉरेन्सिक रेप्लिकेटर एक बिट-स्ट्रीम फोरेन्सिक प्रतिमा निर्मिती साधन आहे. फॉरेन्सिक रेप्लिकेटर विंडोज आधारित साधन आहे जो हार्ड ड्राइव्हस आणि संबंधित मीडियाच्या बिट-बाय-बिट कच्च्या DD प्रतिमा तयार करतो. आपण प्रतिमा एन्क्रिप्ट करण्यासाठी PFR स्वरूपात देखील प्रतिमा तयार करू शकता, ती संक्षिप्त करू शकता, किंवा लहान तुकडे तो तोडून फॉरेन्सिक रेप्लिकेटर आपल्याला फॉरेन्सिक इमेजिंग साधनामध्ये अपेक्षित असलेले सर्व काही देतो. आपण बिट-बाय-बिट फॉरेन्सिक प्रतिमा तयार करू शकता, हॅश कॅलक्युलेशनसह आपली प्रतिमा एकाग्रता सत्यापित करू शकता, आपल्या अहवालात लेखन ब्लॉकरचा दस्तऐवज वापर, प्रतिमाच्या सामग्री पाहू शकता आणि बरेच काही फौजदारी रेप्लिकेटर आपल्या पुराव्याचे जतन करण्यासाठी मोठ्या प्रमाणात कार्य करतो. सॉफ्टवेअर-आधारित लेखन संरचनेत तयार केल्याने आपल्याला आपल्या पुराव्यांबद्दल लिहणार नाही हे सुनिश्चित करण्यात मदत होते. हॅश सत्यापन आणि तपशीलवार अहवाल आपल्या डेटाची सत्यता टिकवून ठेवण्यासाठी देखील मदत करतात.

६.२: हॅश कॅल्क्युलेटर - हॅश कॅल्क्युलेटर आणि रिपोर्ट जनरेशन

ही प्राथमिक तपासणीची शेवटची प्रक्रिया आहे. हॅशने गणना केली आहे की फॉरेन्सिक साधने वापरून गुन्हा देखावातून जप्त केलेले पुरावे खरा आहे आणि कोणतेही बदल किंवा बदल केले गेले नाहीत. हे पुराव्यावर चेकसमची गणना करते आणि अहवालासह मूल्य तयार करते.

Copyright-FORnSEC Solutions


Evidence Report for Project: ABC
Project Number: 1
Project Description: Fraud
Investigator Name: PSI ABC
Image Files:
File Name: D:\Fraud\.eve
Image File Type: DFT Image
File Number: 1
Technician Name: ABC
Date: 03/16/2016
Time: 19:38:07
SHA1 Checksum: B04F08A965A9178B24F8D42FA4C53D65F3772E84
Checksum Validated: Yes
Compressedimage: No
Time Zone Information:
Time Zone: (GMT+05:30) Calcutta, Chennai, Mumbai, New Delhi (India Standard Time)
Daylight savings (summertime) was in effect: No
Time Zone information obtained automatically from remote system/image.
Total Drive Information
Hard disk make: [Unknown]
Total Sectors : 15138816
Total Size : 7569408 KB


HashCalc
Data Format:
File
Data:
C:_test\Track01.mp3
HMAC
Key Format:
Text string
Key:
MD5
5aee0248a0cad874c9a64ddb9e65d809
MD4
SHA1
75c99f58685aa6cc68015b9b6780762aecc77021
SHA256
SHA384
SHA512
RIPEMD160
PANAMA
TIGER
MD2
ADLER32
c763f2b7
CRC32
b359ebec
eDonkey/ eMule
262fb6751ac631f2403cc9448b2b4859
SlavaSoft
Calculate
Close
Help

६.३: यूएसबी संरक्षित - ब्लॉक करा उपकरण टाइप करा

हार्डवेअर किंवा सॉफ्टवेअर स्वरूपात संरक्षण साधन लिहा. डाटा स्टोरेज डिव्हाइसेसची एकाग्रता टिकवून ठेवण्यासाठी संगणक फोरेन्सिकमध्ये एक तंत्र वापरले आहे. डिव्हाइसवर सर्व लेखन ऑपरेशन टाळण्याद्वारे, उदा. एक हार्ड ड्राइव्ह, हे डिव्हाइस डेटा पुनर्प्राप्ती पद्धती द्वारे अबाधित राहते याची खात्री केली जाऊ शकते.

६.४: सिम कार्ड रीडर

एक सिम कार्ड विश्लेषणासाठी , एक सिम कार्ड वाचक आवश्यकआहे.

ight-FC nSEC Solutions

६.४.१: सिम कार्ड डेटा विश्लेषण सॉफ्टवेअर - सिम कार्ड जप्ती

हे फोरेन्सिक साधन सिम कार्ड विश्लेषण आणि डेटा प्राप्त करण्यासाठी वापरला जातो. पाराबेन सिम कार्ड जप्ती एक व्यापक फोरेन्सिक्स साधन आहे जे आपल्याला त्याच्या एकाग्रतेवर परिणाम न करता सिम कार्डवरील डेटामध्ये प्रवेश करू देते. हे फोन नंबर, पत्ते, तारखा, वेळा इत्यादी सारख्या डेटा पुनर्प्राप्त करण्यासाठी डिझाइन केले आहे आणि डेटामध्ये बुकमार्क शोधणे आणि जोडण्याचे मार्ग प्रदान करते. सिम कार्ड जप्ती ही माहिती प्राप्त करण्यासाठी व त्याचे परीक्षण करण्यासाठी अतिशय उपयुक्त साधन आहे, आणि आपल्या तपास मध्ये अत्यंत मौल्यवान असेल हटविले एसएमएस / मजकूर संदेश पुनर्प्राप्त आणि सिम कार्ड डेटा एक व्यापक विश्लेषण सुरू सिम कार्ड जप्ती पॅराबेनच्या उपकरण जप्तीपासून सिम कार्ड संपादन आणि विश्लेषण घटक घेते आणि ते एका विशिष्ट सिम कार्ड फोरेन्सिक ॲक्विजिशन आणि विश्लेषण टूलमध्ये ठेवतात. सिम कार्ड जप्तीमध्ये सॉफ्टवेअर तसेच फॉरेन्सिक सिम कार्ड रीडर समाविष्ट आहे. जर तुमच्याकडे आधीच उपकरण जप्ती आणि उपकरण जप्ती टूलबॉक्स असेल तर सिम कार्ड जप्ती मिळण्याकरिता आपल्याला काही आवश्यकता नाही कारण त्यामध्ये फॉरेन्सिक सिम कार्ड संपादन आणि विश्लेषण करण्यासाठी घटक असतात. हे साधन अन्वेषकांसाठी आहे जे फक्त सिम कार्ड खरेदी करू इच्छित आहे आणि सर्व सेल फोन डेटा फोरेन्सिक परीक्षा करू इच्छित नाही.

yright-FORnSEC Solutions

६.५: सिग्नल ब्लॉकिंग - फॅराडे बॅग

फॅराडे बॅग म्हणजे काय?

एक फॅराडे बॅग (रेडिओ फ्रीक्वेन्सी) फोम पॅड केलेले नायलॉन बाह्य स्तरापासून बनविलेले बॅगचे संरक्षण केले जाते आणि विशेषत: डिझाइन केलेले RF शील्डिंग सामग्रीचे दोन स्तर असतात जे इलेक्ट्रोमॅग्नेटिक सिग्नल ब्लॉक करते, ज्यामध्ये बाहेरच्या सिग्नलपासून बचाव करण्यासाठी सेल फोन सारख्या उपकरणांचा वापर होतो.

<u>गरज -</u>

सेल फोन म्हणजे असे उपकरण जे वायरलेस सिग्नलद्वारे दूरसंचार नेटवर्कशी जोडतात. काही सेल फोन्स ब्ल्यूटूथ डिव्हाइस किंवा वायरलेस नेटवर्कशी देखील कनेक्ट करू शकतात. सेल फोनवर सुरक्षा वैशिष्ट्ये सक्षम नसल्यास, फोनशी कनेक्ट करणे आणि फोनवर डिजिटल पुरावे जोडणे, हटवणे किंवा जोडणे शक्य होऊ शकते. हे एखाद्या सेल फोनवर लक्ष ठेवत नाही. हे अतिशय महत्त्वाचे आहे की डिजिटल पुरावे जप्तीच्या वेळेपर्यंत संरक्षित केले जातात जोपर्यंत न्यायालयात पुरावे म्हणून सादर केले जात नाही. जर पुराव्यामध्ये

Copyright FORnSEC Solutions

छेडछाड केल्याचा संशय आहे, तर न्यायालयामध्ये प्रवेश नाकारता येण्यासारखा आहे. म्हणून, Faraday वापरून आणि पुराव्याच्या पुराव्यावरून त्याचा वापर लक्षात घेऊन डिजिटल पुराव्याचे जतन करणे महत्त्वाचे आहे.

६.६:मोबाईल डेटा पुनर्प्राप्ती सॉफ्टवेअर - Dr.Fone Wondershare

Dr. Fone Wondershare हे अँड्रॉइड फोन आणि टॅब्लेटमधील हटविलेल्या डेटा पुनर्प्राप्त करण्याकरिता एक शक्तिशाली टूलकिट आहे ज्यामध्ये अंतर्गत मेमरी कार्ड आणि बाह्य मेमरी कार्ड्स गमावलेल्या डेटा, तुटलेली Android डिव्हाइसेसवरील बचाव डेटा आणि अँड्रॉइड लॉक स्क्रीन काढून टाकली जाते. आपण ओएस क्रॅश किंवा रॉम फ्लॅशिंगमुळे अचानक अपघातात किंवा गमावले असल्यास मजकूर संदेश, फोटो, संपर्क, कॉल इतिहास, व्हिडिओ, व्हाट्सएप संदेश, ऑडिओ फायली आणि बरेच काही पुनर्प्राप्त करण्यात सक्षम आहे. अँड्रॉइड फाईल पुनर्प्राप्ती -अँड्रॉइड साठी Dr.Fone Wondershare, अँड्रॉइड डिव्हाइसेसवरील हटविलेल्या फायली पुनर्प्राप्त करण्यासाठी खूप चांगले कार्य करते. तथापि, आपण आपल्या पुनर्प्राप्तीबरोबर चांगले व्यवहार करत नसल्यास आपल्या अँड्रॉइड डिव्हाइसवरून सर्व फायली हटविल्या जाऊ शकत नाहीत.

मजकूर संदेश, फोटो, संपर्क, व्हाट्सएप संदेश, व्हिडीओज, कॉल लॉग आणि ऑडिओ फाइल्स पुनर्प्राप्त करण्याशिवाय डॉ. फोऑन वंडर्सशेअर- मायक्रोसॉफ्ट वर्ड डॉक्युमेंट्स, एक्सेल वर्कशीट्स, पॉवरपॉईंट सादरीकरण फाइल्स, PDF दस्तऐवज आणि अधिक डेटा पुनर्प्राप्त करतो.

Copyright FORnSEC Solutions

६.७: पुरावा संग्रह बॅग - विरोधी स्टॅटिक बॅग

इलेक्ट्रिक स्टोरेज डिव्हाइसेस आणि इलेक्ट्रॉस्टॅटिक डिस्चार्जमुळे होणार्या नुकसानास बळी पडलेल्या घटकांवरील संचयित करण्यासाठी अँटी स्टॅटिक बॅगचा वापर केला जातो.

या पिशव्या सहसा प्लास्टिक पॉलीथिलीन टेरेफाथलेट (पीईटी) असतात आणि एक विशिष्ट रंग असतो. यांत्रिक नुकसान आणि इलेक्ट्रोस्टॅटिक नुकसान दोन्हीपासून संरक्षणासाठी अनेक स्तर वापरले जातात. हे महत्त्वाचे आहे की पिशव्या केवळ स्थिर-मुक्त वर्कस्टेशन्सवर उघडता येतील.

ht-FORnSEC Solutions

६.८: मेमरी कार्ड रीडर

मेमरी कार्ड रीडर म्हणजे मेमरी कार्ड जसे की कॉम्पॅक्ट फ्लॅश (सीएफ), सिक्योर डिजिटल (एसडी) किंवा मल्टीमीडिया कार्ड (एमएमसी) वर डेटा ऍक्सेस करण्यासाठीचे साधन आहे. बहुतेक कार्ड वाचक लेखन क्षमता देखील देतात आणि कार्डसह एकत्र करतात, हे पेन ड्राइव्ह म्हणून कार्य करू शकतात.

Copyright-FORnSEC Solutions

पाठ ७:

आयटी अधिनियम: 2008

माहिती तंत्रज्ञान कायदा, 2008, 27 ऑक्टोबर 2009 रोजी लागू झाला आहे.

महत्वाची विभाग-

कलम 43 - संगणक प्रणालीला किंवा संगणकाला हानी पोहचविणे.

दंड - त्यामुळे प्रभावित व्यक्तीस एक कोटी रुपयांपेक्षा जास्त नुकसान भरपाई नाही.

कलम 43 ए - डेटा संरक्षण देण्यात अपयश आल्यास सहकार्य करा.

दंड - त्यामुळे प्रभावित व्यक्तीस पाच कोटी रुपयांपेक्षा अधिक नुकसान भरपाई नाही.

कलम 65 - संगणक स्त्रोत दस्तऐवजांसह छेदन.

दंड - तीन वर्षापर्यंत कारावासाची शिक्षा, किंवा दोन लाख रुपयांपर्यंतचा दंड, किंवा दोघांनाही

कलम 66 - संगणक-संबंधित अपराध

दंड - तीन वर्षांपर्यंतच्या कारावासाची शिक्षा किंवा दंड किंवा पाच लाख रुपयांपर्यंतच्या दंड

कलम 66 ए - दळणवळण संदेश पाठविण्याचे दंड, इ.

दंड - तीन वर्षांपर्यंतच्या आणि जबरदस्त कालावधीसाठी तुरुंगवास.

Copyright FORnSEC Solutions

कलम 66 ब - अप्रामाणिकपणे चोरलेल्या संगणक संसाधन किंवा दळणवळण साधनासाठी शिक्षा.

दंड - तीन वर्षांपर्यंतच्या मुदतीसाठी कारावासाची शिक्षा किंवा जबरदस्तीने एक लाख रूपये किंवा दोनशेने दंड होऊ शकतो.

कलम 66 सी - ओळख चोरीसाठी शिक्षा.

दंड - तीन वर्षापर्यंतच्या मुदतीसाठी तुरुंगवास आणि एक लाख रुपयांपर्यंत दंड होऊ शकतो.

कलम 66 डी - संगणक संसाधनांचा वापर करुन फसवून फसवणूक केल्याबद्दल शिक्षा

दंड - तीन वर्षापर्यंतच्या मुदतीसाठी तुरुंगवास आणि एक लाख रुपयांपर्यंत दंड होऊ शकतो.

कलम 66 ई - गोपनीयतेचे उल्लंघन केल्याबद्दल शिक्षा

दंड - कारावासाची शिक्षा जी तीन वर्षांपर्यंत किंवा दोन लाख रुपयांपेक्षा अधिक असू शकते किंवा दोन्ही शिक्षा लागू.

कलम 66 एफ - सायबर दहशतवादासाठी शिक्षा.

दंड - जीवन कारावास वाढू शकते असे कारावास.

Copyright-FORnSEC Solutions

कलम 67 - इलेक्ट्रॉनिक स्वरूपात अश्लील साहित्य प्रकाशित किंवा प्रसार करण्यासाठी शिक्षा.

दंड - तीन वर्षांपर्यंतच्या मुदतीसाठी तुरुंगवास आणि पाच लाख रुपयांपर्यंत दंडाची तरतूद आणि दुस-या किंवा त्यानंतरच्या निर्णयामुळे तुरुंगवासाची शिक्षा पाच वर्षापर्यंत कारावास आणि दंड जे दहा लाख रुपयांपर्यंत वाढू शकते.

कलम 67 अ - इलेक्ट्रॉनिक स्वरूपात लैंगिक स्वरूपातील सुस्पष्ट कृतीसह सामग्री प्रकाशित किंवा प्रसारित करण्याची शिक्षा.

दंड - पाच वर्षांपर्यंतची कारावासाची शिक्षा आणि दहा लाख रुपयांपर्यंत दंड होऊ शकतो आणि दुस-या किंवा त्यानंतरच्या निर्णयामध्ये कारावासाची शिक्षा सात वर्षापर्यंत आणि दंडसहित होऊ शकते. दहा लाख रुपयांपर्यंत वाढू शकते.

कलम 67 ब - लैंगिकरित्या सुस्पष्ट कारवाईतील मुलांचे वाटप करणार्या साहित्याचे प्रकाशन किंवा प्रसार करण्यासाठी शिक्षा इ.

दंड - पाच वर्षांपर्यंतच्या कारावासाची शिक्षा आणि दहा लाख रुपयांपर्यंत दंडाची शिक्षा आणि दुस-या किंवा त्यानंतरच्या निर्णयामध्ये तुरुंगवास किंवा सात वर्षापर्यंतचे कारावास आणि दंड जे दहा लाख रुपयांपर्यंत वाढू शकते.

कलम 67 सी - मध्यस्थांद्वारे माहितीचे संरक्षण व धारण करणे.

दंड - तीन वर्षांपर्यंतच्या मुदतीसाठी तुरुंगवास आणि दंड होऊ शकतो.

Copyright-FORnSEC Solutions

कलम 70 - संरक्षित प्रणालीसाठी अनधिकृत प्रवेश.

<u>दंड</u> - दहा वर्षांपर्यंतच्या मुदतीसाठी तुरुंगवास आणि दंड होऊ शकतो.

कलम 72 - गोपनीयतेचे उल्लंघन आणि गोपनीयता

<u>दंड</u> - दोन वर्षांपर्यंतच्या मुदतीसाठी कारावासाची शिक्षा, किंवा एक लाख रुपयांपर्यंत दंड किंवा दोन्ही शिक्षा होऊ शकतात.

कलम 72 अ - कराराच्या उल्लंघनातील माहितीचे प्रकटीकरण

<u>दंड</u> - तीन वर्षांपर्यंतच्या मुदतीसाठी कारावासाची शिक्षा, किंवा पाच लाख रुपयांपर्यंत दंड होऊ शकतो किंवा दोन्ही शिक्षा होऊ शकतात.

Copyright-FORnSEC Solutions

पाठ ८:

घटनेचा अभ्यास

केस 1 - फेसबुक

समस्या - आजचे विद्यार्थी तंत्रज्ञानाच्या वापराशी परिचित आहेत आणि जवळजवळ प्रत्येक सोशल नेटवर्किंग साइटवर आहेत; एका महाविद्यालयीन विद्यार्थ्याने आपल्या वैयक्तिक चॅटमध्ये शाळेच्या प्राचार्यवर अश्लील प्रतिमा आणि अवैध संदेश पाठविले.

उपाय - प्राचार्य ने तिच्या जवळच्या पोलिस स्टेशनवरील व्यक्तीविरूद्ध तक्रार दाखल केली आणि पोलिस अधिकार्यांसह तिच्या समस्येविषयी चर्चा केली. पोलिसाने त्या महिलेच्या खात्याचे तपशील विचारले आणि तरुणांनी पाठविलेला संदेश बघितला. सायबर क्राइम तज्ज्ञ कडून प्रकरणाची पडताळणी करण्यासाठी पोलीस कर्मचारी येथे पोलिसांनी मला फोन केला. पोलिस अधिकार्याने स्त्रीच्या बाबतीत माझ्याशी चर्चा केली आणि मी छायाचित्रांवर आणि संदेशांवर एक नजर टाकली. या प्रकरणाचा तपास करण्यासाठी, मी अपराधीचा मोबाईल फोन जप्त केला आणि इलेक्ट्रॉनिक गॅझेटच्या अधोरेखित विश्लेषण केले. काही वेळाने, मी त्यांना त्या प्रतिमा आणि संदेश मोबाईल फोनवर पाठवले. मी प्राचार्यांच्या फेसबुक अकाऊंटच्या अनेक संगणक स्क्रीनशॉट देखील घेतल्या ज्यात त्या संदेशांना एक पुरावा आहे आणि वैयक्तिक प्रतिमाच्या SHA-1 हॅश व्हॅल्यूची निर्मिती केली. त्याचबरोबर, मी इलेक्ट्रॉनिक्स रेकॉर्ड पुरावे कायद्याची ६5 (ब) पात्रता प्रदान केली. जेणेकरून केस कोर्टात धरता येईल आणि गुन्हेगाराने त्याच्या चुकीच्या गोष्टी मान्य केल्या पाहिजेत. या घटनेची कलम ६7 ए नुसार नोंद झाली.

Copyright-FORnSEC Solutions

केस 2 - ईमेल आणि फेसबुक

समस्या - नुकत्याच झालेल्या एका प्रकरणात, एक तरूण एका मुलीला ईमेल द्‍वारे धमकी आणि त्रास देत होता. तो तिच्यावर दबाव टाकत असे आणि तिच्या कुटुंबाबद्‍दल तिला धमकवत असे. त्यांनी आपल्या मित्राच्या वर्तुळातील मुलीबद्‍दल फसवणुकीचा ईमेलस् पाठवले. एवढेच नव्हे तर त्यांनी तिच्या कुटुंबियांना आणि इतर नातेवाईकांना फेसबुकवर संदेश फेटाळून लावले आणि तिच्या हालचालींचा मागोवा ठेवला.

उपाय- या मुलीने माझ्या ऑफिसमध्ये तक्रार नोंदवली आणि ही पुर्ण घटना सांगितली. तिचे ऐकले नंतर, मी त्या मुलीच्या ईमेलवर एक नजर टाकण्यासाठी तिला ईमेल खात्याचे तपशील देण्यास विनंती केली. गुन्हेगार आणि त्याचे स्थान शोधण्यासाठी, मी IP पत्ता आणि ईमेल शीर्षलेखाचा शोध लावला की जेणेकरून मला काही सुचना मिळू शकतील. कालांतराने मला आढळले की सायबर क्राइमसाठी त्याने खासगी IP पत्ता वापरला आहे आणि Google खासगी IP पत्ता मुखवटा करतो. नंतर, माहितीचा स्रोत मिळवण्यासाठी आणि इतर माहिती शोधण्यासाठी, मी कायदे अंमलबजावणी एजन्सीकडे गेलो आणि गुगल मुख्यालये, US वर तपशिलांची विनंती केली. केस ६7 अन्वये कायद्‍याअंतर्गत गुन्हा दाखल करण्यात आला.

केस 3 - खून

समस्या - 15 मार्च 201६ रोजी नागपूरमध्ये दोन लोकांनी चाकूने एका व्यक्तीची हत्या केली. रात्रीच्या वेळी घटना घडली.

उपाय - ही घटना ताबडतोब नोंदवली गेली आणि पोलीस अधिकाऱ्यांनी मला क्राईम सीनकडे बोलवले. क्राईम सीनवर पोहोचल्या नंतर मी त्या ठिकाणाचे विश्लेषण केले आणि जवळच्या ठिकाणी सीसीटीव्ही फुटेज गोळा करण्याच्या समाधानासाठी बाहेर आलो. ही घटना त्यांच्या

Copyright FORnSEC Solutions

सीसीटीव्ही पाळत ठेवण्यात आली होती आणि खून फुटेजही उपस्थित होते. मी तीन वेगवेगळ्या ठिकाणी असलेल्या व्हिडिओंची तपासणी करण्यासाठी तीन वेगवेगळे कोन सोडले. त्या व्हिडीओज वेगवेगळ्या पेन ड्राईव्हमध्ये गोळा केल्या होत्या आणि पेन ड्राईव्हची एकाग्रता कायम ठेवण्यासाठी आम्ही सीसीटीव्ही फूटेजच्या हॅश व्हॅल्यूची गणना केली आणि सेक्शन 65-बी खाली एसएचए -1 रिपोर्ट तयार केला. प्रकरण 134,177 च्या कलमांतर्गत गुन्हा दाखल करण्यात आला.

केस 4 - व्हिडिओ कन्फेशन

समस्या - एका गूढ खून प्रकरणात एका व्यक्तीने त्याच्या मित्राचा खून केला होता, दोन्हीही मद्यधुंद होते. त्या व्यक्तीने आपल्या सोबत्याला काही नागरी दंडासंबंधात दगड फेकून मारला. कोर्टात संशयितांना पकडण्यासाठी कोणताही पुरावा नव्हता. एकही सीसीटीव्ही कॅमेरे किंवा कोणतीही डोळ्यांची साक्षीदार नव्हती.

उपाय - या प्रकरणात कोणताही पुरावा नव्हता तसेच साक्षीदारांची तपासणी करणे ही कठीण झाले. दरम्यान, ज्याने आपल्या सोबत्याला जिवे मारण्याचा प्रयत्न केला तो गुन्हा कबूल करतो. त्यांच्या विरोधात कोणतेही पुरावे नसल्यास एखाद्या व्यक्तीचे विधान कायदेशीर राहणार नाही. मग मी पोलिस स्टेशन मध्ये वेबकॅमवरून खून गुन्हाचे व्यक्तिमत्व कबुलीजबाब घेतली. मी व्हिडिओला मेमरी कार्डमध्ये संचयित केले आणि मेमरी कार्डचे SHA-1 हॅश मूल्य निर्माण केले जेणेकरून छेडछाड केल्यापासून मूळ पुरावे कायम ठेवता येतील. न्यायालयात खरे पुरावे देण्यात आले. या प्रकरणी कलम 302, 34 नुसार नोंदणी करण्यात आली.

Reference

Copyright-FORnSEC Solutions

1) https://www.google.com/search?biw=13६६&bih=६६2&tbm=isch&sa=1&ei=_lwfW-T8O5C2rQHNx43gAw&q=sandisk+1६gb&oq=sandisk+1&gs_l=img.1.1.0l10.3६0300.3६2011.0.3६3511.2.2.0.0.0.0.170.332.0j2.2.0....0...1c.1.६4.img..0.2.330...0i६7k1.0.aKxL3KCu5uk#imgrc=ubfhBT2dvNzY8M:
2) https://www.google.com/search?biw=13६६&bih=६६2&tbm=isch&sa=1&ei=iF4fW६SuCdKy9QOSiaWYAg&q=forensic+replicator&oq=Forensic+Repl&gs_l=img.3.0.0i24k1.87285.91282.0.93255.14.14.0.0.0.0.279.2094.0j६j4.10.0....0...1c.1.६4.img..4.10.2091.0..0j35i39k1.0.GpasKkQrmWY#imgrc=_
3) https://www.google.com/search?biw=13६६&bih=६६2&tbm=isch&sa=1&ei=7F4fW--7OM-w9QOQwZmICQ&q=hash+calculator&oq=hash+calculator&gs_l=img.3...237049.241877.0.2421६0.1६.11.0.0.0.0.0.0..0.0....0...1c.1.६4.img..1६.0.0.0...0.IghVSlbTh2s#imgrc=BJlVLyAJBzF3jM:
4) https://www.google.com/search?biw=13६६&bih=६13&tbm=isch&sa=1&ei=5l8fW-TjB5j_9QONgLOwDg&q=sim+card+seizure&oq=sim+card+seizure&gs_l=img.3..0i30k1j0i24k1l3.14६3594.1471534.0.1472803.17.11.0.६.६.0.2६4.2215.2-10.10.0....0...1c.1.६4.img..1.1६.2259.0..0j0i६7k1j0i10k1j0i5i30k1.0.tSSVO98TlTU#imgrc=3qMI52i37LFTQM:
5) https://www.google.com/search?biw=13६६&bih=६13&tbm=isch&sa=1&ei=pWcfW877E4HO0gTH9a2wDg&q=dr.phone+wondershare&oq=Dr.phone+won&gs_l=img.3.0.0i24k1.8331.15753.0.185६4.13.13.0.0.0.0.522.2058.2-

Copyright-FORnSEC Solutions

5j0j1j1.7.0....0...1c.1.६4.img..६.7.205६.0..0j35i39k1j0i६7k1j0i30k1.0.bdPTr_H2rRs

6) https://www.google.com/search?biw=13६६&bih=६13&tbm=isch&sa=1&ei=umcfW_TUJcLJ0gTK5YawCw&q=evidence+collection+bag+and+faraday+bag&oq=evidence+collection+bag+and+faraday+bag&gs_l=img.3...29527.58230.0.585६2.53.43.4.4.4.0.424.5270.0j2j18j1j1.22.0....0...1c.1.६4.img..23.23.34६5.0..0j35i39k1j0i६7k1j0i10i24k1j0i30k1.0.l9r7TKtUMDs

7) https://www.google.com/search?q=sim+card+reader&source=lnms&tbm=isch&sa=X&ved=0ahUKEwin95KzjM7bAhXFp48KHcGsC६wQ_AUICigB&biw=13६६&bih=६13

Copyright-FORnSEC Solutions