INFORMATION SECURITY AND DIGITAL FORENSICS
A panacea tools for combating cyber-crime and terrorism

[1]Asere Gbenga Femi, [2]Makoshi Bonat Joshua, [3]Iseyemi Oluwole Samuel
Department of Computer Science, Federal School of Statistics, Manchok, Kaduna State, Nigeria[1], Federal School of Statistics, Manchok, Kaduna State, Nigeria[2], Department of Statistics Federal School of Statistics, Manchok, Kaduna State, Nigeria[3]
aseregbenga@gmail.com[1], bonatj@yahoo.com[2]

ABSTRACT
With the headway in digital region, continuous utilization of web and advances prompts digital assaults. Computerized measurable is settled on procuring electronic data and examination of pernicious proof found in framework or on network in such a way that makes it acceptable in court. It is additionally used to recuperate lost data in a framework. The recuperated data is utilized to arraign a lawbreaker. Number of wrongdoings perpetrated against a web and malware assaults over the computerized gadgets have expanded. Memory investigation has turned into a basic capacity in computerized legal sciences since it gives knowledge into the framework express that ought not to be addressed by customary media examination. In this paper, we concentrate on the subtleties of digital legal sciences and furthermore give the essential data in regards to unmistakable apparatuses work in advanced legal cycle. It incorporates legal examination of scrambled drives, circle investigation, examination tool compartment, unstable memory examination, catches and investigates parcels on network and concluded that information security and digital forensics is a panacea tools for combating cyber-crime and terrorism.

KEY Words: Cyber-Crime, Forensics, Digital, Information Security

INTRODUCTION
Nowadays, digital hoodlums appear to be all over. They hide in the haziest corners of the web, duping individuals, hacking, taking, and stowing away from specialists with virtual obscurity. As per Wired, digital crooks are unleashing devastation by releasing ransomware assaults, taking information, in any event, upsetting everyday government tasks. This issue is just getting greater as indicated by a report distributed by Accenture, the quantity of digital protection breaks expanded by 11% from 2017 to 2018. The expense of such breaks is galactic - about $600 billion around the world, as indicated by the Economic Impact of Cybercrime report.

Digital forensics is the general study of recuperation and examination of material found on a wide range of computerized gadgets. PC crime scene investigation is a part of computerized criminology that spotlights on proof found on PCs and advanced stockpiling media like hard drives or USB drives. Ordinarily, these branches are utilized during examinations that include cybercrime or standard wrongdoings that have proof put away on some kind of gadget. With the expanded fame of workstations, cell phones, installed frameworks and other web of things gadgets, practically all wrongdoing includes some kind of PC framework. Hence, having the option to separate proof from PCs while following every one of the expected strategies that makes that proof allowable in court is an extremely extraordinary and significant range of abilities for regulation requirement, military and private examinations.

Types of Digital Forensics

I. **Disk Forensics:** This area centers around removing information from capacity media, for example, a hard drive via looking for dynamic, changed or erased records. For instance, this would recuperate erased documents that could be utilized as proof or demonstrate that a record was made and adjusted at a specific time.

II. **Network Forensics:** This is connected with checking and dissecting traffic between various PCs on an organization. You can consider it snooping on a discussion, the objective is to gather the data being sent and use it as proof.

III. **Memory Forensics:** This specialty centers around recuperating information from framework memory (framework registers, RAM or reserve). This is significant in light of the fact that multiple occasions information or malware is just found in memory and never saved to the hard drive (circle), so it's essential to have the option to separate this data straightforwardly from memory.

IV. **Mobile Device Forensics:** As the name recommends this region centers around looking at, separating and dissecting proof found on cell phones, for example, cell phones, iPads and so forth Some of things that experts separate are telephone contacts, call logs, sound and video.

V. **Automotive Forensics:** This branch centers around the recuperation of advanced proof or information put away in auto modules, organizations and messages shipped off auto frameworks. This can incorporate things like gps areas, matched gadgets, client addresses and so forth as vehicles become further developed, incorporate with more gadgets like individuals' cell phones and become more independent, this region could turn out to be substantially more famous.

VI. **Database forensics:** This branch studies and analyses data sets and their connected metadata. This would include attempting to demonstrate when records were made, who got to the data and when.

VII. **Drone Forensics (UAV Forensics):** Drone forensics centers around the handling and criminology investigation of automated air vehicles. This is especially valuable for military use as robot's can contain a great deal of helpful data like flight way information, geo-area of significant regions (send off and landing destinations), metadata, wifi information and bluetooth/combined gadgets.

1) Where is Digital forensics used?

- Nowadays, any individual who utilizes the web benefits from advanced legal sciences in network protection. That is on the grounds that any organization that gathers information from web clients utilizes individuals who battle and examine cybercrime.
- Offices and associations must be hyper-careful with the information they gather and safeguard, so they are continually trying their frameworks, searching for weaknesses and forcefully seeking after individuals who hack into networks to carry out wrongdoings.
- Facebook, Twitter, Instagram, Homeland Security, the FBI, Target Corp., the military, nearby and state regulation requirement, and practically every bank involves advanced crime scene investigation in network safety to safeguard individuals utilizing the web.
- Initially, it is utilized in criminal examinations. So assuming a wrongdoing has been perpetrated commonly individuals might have video, instant messages or records put away on their cell phones and PCs that contain important proof. At times individuals will attempt to stow away or erase that data prior to getting captured. This is the place where computerized legal sciences become an integral factor in assisting with getting that data off the gadget, demonstrate its legitimacy and assist the police with getting a conviction.

- Besides, it tends to be utilized in corporate/private examinations. This can be examining representative unfortunate behaviour. For instance, assuming a representative is associated with taking protected innovation from the organization, advanced legal sciences might be utilized to check whether that worker got to the record, downloaded it, messaged it or set it on a USB drive.
- Lastly, it is utilized after a cyberattack. At the point when an organization is hacked, computerized criminology is vital to reveal precisely the way in which the hack occurred, how the programmer treated the frameworks and affirming that the programmer's entrance has been eliminated once all of the security work has been finished.

Digital Forensics in Cyber Security

Individuals who work with advanced crime scene investigation in network safety are on the bleeding edges in the battle against cybercrime. They're individuals who gather, cycle, save, and examine PC related proof.

They assist with distinguishing network weaknesses and afterward foster ways of alleviating them. They dive deep inside organizations, PCs, and cell phones looking for proof of crime. Furthermore, they run counterintelligence against programmers, lawbreakers, and others with accursed intensions.

Furthermore, they utilize logical investigatory procedures to make it happen.

What Skills Are Needed for Digital Forensics in Cyber Security

As you can envision, not only anybody with a PC and web access can be a computerized criminology proficient. It takes a ton of information and a lot of abilities, including:

- a profound comprehension of PCs, innovation across a wide range, and online protection standards and practices,
- a functioning information on PCs, organizations, and coding,
- top to bottom analytical capacities,
- decisive reasoning abilities and insightful ability
- the capacity to successfully convey and work with a wide scope of individuals

Makes the occupation so fascinating that occasionally the proof is effectively open, however different times it's secret profound inside the PC or organization. Frequently, it's been erased by the suspect. It's the occupation of the experts to utilize their insight and abilities to track down the proof, any place it very well might stow away.

Also now and again it comes down to observing the information that has been concealed with a solitary keystroke.

How Digital Forensics in Cyber Security Makes a Difference

The field of computerized legal sciences in digital protection is invigorating on the grounds that it has a substantial effect in the existences of individuals the nation over and all over the planet.

The experts who work in the business have assisted catch with peopling managing in unlawful porn. They have dealt with executioners. They've followed fear based oppressors, found missing individuals, and observed in any case customary representatives who were taking great many dollars.

Truth be told, the field is critical to such an extent that it really produced its own personal network show. Back in 2015 and 2016, CBS delivered CSI: Cyber, which aided shed light on how the business tackles violations.

LITERATURE REVIEW

Cyber Forensics becoming as a wellspring of examination since human master observers are significant since courts won't perceive programming devices like Encase, Pasco, Ethereal as a specialist witness [Meyers and

Rogers, 2004]. Digital legal sciences are valuable for some, experts like military, private area and industry, the scholarly world, and regulation. These regions have many requirements including information security, information obtaining, imaging, extraction, cross examination, standardization, investigation, and detailing. It is significant for all experts working in the arising field of digital crime scene investigation to have a working and working dictionary of terms like bookmarks, treats, webhit and so forth, that are consistently applied all through the calling and industry. Albert and Robert [2008] centered the digital criminology global rules, related key terms, and instruments in their field manual. The goal of Cyber criminology is to recognize advanced proof for an examination with logical strategy to reach inferences. Instances of examinations that utilization digital crime scene investigation incorporate unlawful utilization of PCs, kid sexual entertainment, and digital illegal intimidation.

The area of digital criminology has become conspicuous field of examination since: (1) Forensics frameworks permit manager to analyse blunders (2) Intrusion location frameworks are fundamental in staying away from digital violations (3) Change discovery can be conceivable with proactive legal sciences Cyber-crime scene investigation can be utilized for two advantages [Whitman, Mattord, 2010]: (1) To explore claims of computerized impropriety (2) To perform underlying driver examination.

Digital legal sciences have four particular stages: occurrence distinguishing proof, securing of proof, investigation of proof, and revealing with capacity of proof [Cole, 2010]. The distinguishing proof stage predominantly manages episode ID, proof assortment and checking of the proof. The securing stage saves the condition of a PC framework that can be additionally examined. The examination stage gathers the obtained information and looks at it to track down the bits of confirmations. The detailing stage includes documentation and proof maintenance. When proof gathered, it is important to represent its whereabouts. Agents would require nitty gritty legal sciences to lay out a chain of authority, the documentation of the ownership of proof. Chain of care is an indispensable piece of PC legal sciences and the general set of laws [McQuade and Samuel, 2006] and objective is to safeguard the honesty of proof, so proof ought to be actually gotten in a protected spot alongside a point by point log.

According to regulation requirement local area, there are three kinds of usually acknowledged crime scene investigation procurement: identical representation, criminology duplication and live securing. A Mirror picture, bit-for-bit duplicate, includes the reinforcements of whole hard circle. Making of identical representation is straightforward in principle, however its precision should satisfy proof guidelines. The reason for having perfect representation is proof accessible on account of unique framework should be restarted for additional examination. A legal copy, area by-area, is a high level technique that makes a duplicate of each piece with zero trace of the proof. The resultant might be single huge record and should be an accurate portrayal of the first drive at bitstream level. This technique is most normal kind of obtaining in light of the fact that it makes a measurable picture of the e-proof and it additionally contains document slack. If there should arise an occurrence of little record overwrites a bigger document, surplus bytes are accessible in the record slack. The scientific duplication interaction should be possible with the assistance of instruments like Forensic Tool Kit (FTK) imager, UNIX dd order, or Encase. Access Data's FTK is one of the more integral assets accessible and one of the promising highlights is the capacity to recognize steganography, practice of disguising information on display. It is regularly attractive to catch unpredictable data, which is put away in RAM; it can't be gathered after the framework has been shut down. This data may not be recorded in a document framework or picture reinforcements and it might hold signs connected with aggressor. All as of now running cycles, open

attachments, as of now logged clients, ongoing associations and so forth, are accessible in unpredictable data. For the most part, gatecrasher finds a way ways to keep away from discovery. Trojans, keyloggers, worms and so on, are introduced in unpretentious spots. One of such things to be considered in the obtaining system is rootkits, computerized bundles that make indirect accesses. Interlopers/programmers use rootkits to eliminate log documents and other data to conceal the presence of gatecrasher. Cell phones are become one of the instruments for digital wrongdoings, cell phone proof obtaining testing process are talked about in [Baggili et al, 2007]. 3. Investigation Phase Forensic examination is the method involved with comprehension, re-making, and dissecting inconsistent occasions that have assembled from computerized sources [Caloyannides, 2001]. The examination stage gathers the obtained information and analyzes it to track down the bits of confirmations. This stage additionally distinguish that the framework was altered or not to keep away from recognizable proof. Examination stage analyzes all the proof gathered during assortment and procurement stages. There are three kinds of assessments can be applied for the crime scene investigation examination; restricted, incomplete or full assessment. Restricted assessment covers the information regions that are indicated by authoritative records or in light of meetings. This assessment interaction is least tedious and most normal sort. Incomplete assessment manages noticeable regions. Key regions like log records, vault, treats, E-mail envelopes and client catalogues and so on, are inspected for this situation of incomplete assessment. This fractional assessment depends on broad inquiry standards which are created by legal specialists. Most tedious and less successive assessment process is full assessment. This requires the inspector to look every single imaginable piece of information to observe the underlying drivers of the episode. Record slack assessment is done in this assessment. Some of instruments utilized in the examination stage are Coroner, Encase, FTK. The Coroner tool compartment run under UNIX and EnCase is a tool stash that runs under Windows. [Marcella, Albert, 2008]. EnCase can handle bigger sums and permit the client to utilize predefined contents to pull data from the information being handled. FTK contains an assortment of isolated devices (text ordering, NAT recuperation, information extraction, record separating, E-mail recuperation and so on,) to aid the assessment.

The announcing stage includes documentation and proof maintenance. The logical technique is utilized in this stage to reach determinations in light of the assembled proof. This stage is chiefly founded on the Cyber regulations and presents the ends for comparing proof from examination. There is a need of good approach for how lengthy proof from an episode ought to be maintenance. Elements to be considered in this interaction are arraignment, information maintenance and cost [Karen et al, 2008]. To meet the maintenance prerequisites there is a need of keeping up with log authentic [Tomar et al, 2010]. The filed logs should be safeguarded to keep up with classification and uprightness of logs.

The International Association of Computer Investigative Specialists (IACIS) has fostered a criminological philosophy which can be summed up as follows: • Protect the Crime Scene, power closure for the PC and report the equipment setup and transport the PC framework to a solid area • Bit Stream reinforcement of computerized media, use hash calculations to validate information on all capacity gadgets and record the framework date and time • Search watchwords and check document space the executives (trade document, document slack assessment, unallocated space) • Evaluate program usefulness, archive discoveries/results and hold Copies of programming III. Digital Forensics Tools The primary goal of digital legal sciences apparatuses is to remove computerized proof which can be acceptable in official courtroom. Electronic proof (e-proof, for short) is assuming fundamental part in digital wrongdoings. PC legal sciences apparatuses used to track down skeletons in computerized media. To decrease the impact of against legal sciences instruments the Investigator is probably

going to have the devices and information expected to counter the utilization of anti-forensics methods [Willassen, 2008]. Some of the time assortment of advanced proof is clear since interlopers post data about themselves from Facebook, Orkut, Twitter, MySpace and visit about their criminal operations.

A summon, rather than exceptional crime scene investigation apparatuses, required get this data; these messages or visits from interpersonal organizations can be acceptable as proof. Jansen, Ayers [2006] gave a depiction of the cutting edge of legal programming instruments for mobiles. Baggili et al [2007] had shown the interaction model for cell apparatus testing. [Marcella, Albert, 2008] depicted different digital criminology apparatuses and their portrayal, some of them are: (1) The Coroner's Toolkit (TCT), is an opensource set of criminological devices intended to lead examination UNIX frameworks. (2) The Forensic Toolkit (FTK) is extremely integral asset however not easy to utilize. (3) I2Analyst is an alternate sort of examination device from those data security experts are utilized to. (4) LogLogic's LX 2000 is strong and circulated log investigation instrument. (5) NetWitness, security insight, is an organization traffic security analyzer instrument (6) ProDiscover Incident Response (IR) is a finished IT legal Reserved apparatus that can get to PCs over the organization to concentrate on the organization conduct (7) The Sleuth Kit is one of organization forensic stools used to observe record cases in a NTFS document.

MATERIALS AND METHODS

A. MATERIALS

ProDiscover Forensic

ProDiscover Forensic is a PC security application that permits you to find every one of the information on a PC circle. It can safeguard proof and make quality reports for the utilization of lawful techniques. This device permits you to separate EXIF (Exchangeable Image File Format) data from JPEG records.

Highlights:

- This item upholds Windows, Mac, and Linux document frameworks.
- You can see and look for dubious records rapidly.
- This Digital criminology programming makes a duplicate of the whole speculated circle to guard the first proof.
- This apparatus assists you with seeing web history.
- You can import or product .dd design pictures.
- It empowers you to add remarks to proof of your advantage.
- ProDiscover Forensic backings VMware to run a caught picture.

Link: https://www.prodiscover.com

2) Sleuth Kit (+Autopsy)

Sleuth Kit (+Autopsy) is a Windows based utility instrument that makes legal investigation of PC frameworks simpler. This apparatus permits you to inspect your hard drive and cell phone.

Highlights:

- You can recognize movement utilizing a graphical point of interaction actually.
- This application gives investigation to messages.
- You can bunch records by their sort to track down all reports or pictures.
- It shows a thumbnail of pictures to speedy view pictures.
- You can label documents with the erratic label names.
- The Sleuth Kit empowers you to remove information from call logs, SMS, contacts, and so on
- It assists you with hailing records and organizers in light of way and name.

Connect: https://www.sleuthkit.org

3) CAINE

CAINE is an Ubuntu-based application that offers a total criminological climate that gives a graphical point of interaction. This apparatus can be coordinated into existing programming devices as a module. It consequently removes a timetable from RAM.

Highlights:

- It upholds the advanced agent during the four periods of the computerized examination.
- It offers an easy to use interface.
- You can modify elements of CAINE.
- This product offers various easy to understand instruments.

Interface: https://www.caine-live.net

4) PDF to Excel Convertor

Acrobat PDF to Excel Convertor moves PDF information and content directly into an Excel accounting page. This changed over record demonstrates accommodating for finding cybercriminals from anyplace on the planet. This PC measurable instrument upholds both halfway and clump change.

Highlights:

- Permits you to work from anyplace
- Super-quick with great result
- It holds the first design and arranging

5) Google Takeout Convertor

Google Takeout Convertor changes over filed email messages from Google Takeout alongside all connections. This product examines officials to concentrate, process, and decipher the genuine proof.

Highlights:

- Cluster different commodity documents from the Google Takeout record immediately to save time and exertion.
- This PC measurable application likewise offers a clump mode highlight that assists you with saving time and exertion.
- Upholds changing over Google Takeout documents to the most famous cloud-based email administration.
- Offers double mode work for stacking and changing over Google Takeout documents/organizers.
- Upheld stage: Windows

2) 6) PALADIN

PALADIN is Ubuntu based device that empowers you to improve on a scope of legal undertakings. This Digital criminology programming gives in excess of 100 valuable instruments for researching any malevolent material. This instrument assists you with improving on your legal undertaking rapidly and actually.

Highlights:

- It gives both 64-cycle and 32-bit renditions.
- This apparatus is accessible on a USB thumb drive.
- This tool stash has open-source instruments that assist you with looking for the expected data easily.
- This apparatus has in excess of 33 classes that help you in achieving a digital measurable errand.

Connect: **https://sumuri.com/programming/paladin/**

7) EnCase

Encase is an application that assists you with recuperating proof from hard drives. It permits you to direct a top to bottom examination of records to gather evidence like archives, pictures, and so forth

Highlights:

- You can procure information from various gadgets, including cell phones, tablets, and so on
- It is one of the most incredible versatile scientific devices that empowers you to deliver total reports for keeping up with proof respectability.
- You can rapidly look, distinguish, as well as focus on proof.
- Encase-scientific assists you with opening scrambled proof.
- It is one of the most incredible advanced legal sciences instruments that computerizes the arrangement of proof.
- You can perform profound and emergency (seriousness and need of imperfections) investigation.

Connect: https://www.guidancesoftware.com/encase-criminological

8) SIFT Workstation

Filter Workstation is a PC legal sciences conveyance in light of Ubuntu. It is one of the most mind-blowing PC scientific apparatuses that gives a computerized measurable and occurrence reaction assessment office.

Highlights:

- It can chip away at a 64-digit working framework.
- This instrument assists clients with using memory in a superior manner.
- It consequently refreshes the DFIR (Digital Forensics and Incident Response) bundle.
- You can introduce it by means of SIFT-CLI (Command-Line Interface) installer.
- This instrument contains various most recent measurable devices and procedures.

Interface: https://www.sans.org/apparatuses/filter workstation/

9) FTK Imager

FTK Imager is a scientific tool stash I created by Access Data that can be utilized to get proof. It can make duplicates of information without making changes to the first proof. This device permits you to indicate models, similar to document size, pixel size, and information type, to decrease how much insignificant information.

Highlights:

- It gives a wizard-driven way to deal with identify cybercrime.
- This program offers better perception of information utilizing a diagram.
- You can recuperate passwords from in excess of 100 applications.
- It has a high level and robotized information investigation office.
- FTK Imager assists you with overseeing reusable profiles for various examination prerequisites.
- It upholds pre and post-handling refinement.

Interface: https://accessdata.com/itemsadministrations/criminologicaltoolbox

10) Magnet RAM catch

Magnet RAM catch records the memory of a presumed PC. It permits specialists to recuperate and break down important things which are found in memory.

Highlights:

- You can run this application while limiting overwritten information in memory.
- It empowers you to trade caught memory information and transfer it into investigation apparatuses like magnet AXIOM and magnet IEF.
- This application upholds an immense scope of Windows working frameworks.
- Magnet RAM catch upholds RAM obtaining.

Interface: https://www.magnetforensics.com/assets/magnet-smash catch/

11) X-Ways Forensics

X-Ways is programming that gives a workplace to PC measurable analysts. This program is upholding circle cloning and imaging. It empowers you to work together with others who have this instrument.

Highlights:

- It has capacity to understand apportioning and record framework structures inside .dd picture documents.
- You can get to circles, RAIDs (Redundant exhibit of autonomous plate), from there, the sky is the limit.
- It naturally recognizes lost or erased allotments.
- This apparatus can without much of a stretch distinguish NTFS (New Technology File System) and ADS (Alternate Data Streams).

- X-Ways Forensics upholds bookmarks or explanations.
- It can investigate distant PCs.
- You can see and alter double information by utilizing formats.
- It gives compose assurance to keeping up with information legitimacy.

Interface: http://www.x-ways.net/crime scene investigation/

12) Wireshark

Wireshark is a device that examines an organization parcel. It tends to be utilized to for network testing and investigating. This instrument assists you with checking different traffic going through your PC framework.

Highlights:

- It gives rich VoIP (Voice over Internet Protocol) investigation.
- Catch documents compacted with gzip can be de-pressurized without any problem.
- Result can be sent out to XML (Extensible Mark-up Language), CSV (Comma Separated Values) document, or plain message.
- Live information can be perused from the organization, blue-tooth, ATM, USB, and so on
- Decoding support for a very long time that incorporate IPsec (Internet Protocol Security), SSL (Secure Sockets Layer), and WEP (Wired Equivalent Privacy).
- You can apply natural investigation, shading rules to the parcel.
- Permits you to peruse or compose document in any configuration.

Interface: https://www.wireshark.org

13) Registry Recon

Library Recon is a PC crime scene investigation instrument used to separate, recuperate, and examine vault information from Windows OS. This program can be utilized to productively decide outer gadgets that have been associated with any PC.

Highlights:

- It upholds Windows XP, Vista, 7, 8, 10, and other working frameworks.
- This instrument naturally recuperates important NTFS information.
- You can coordinate it with the Microsoft Disk Manager utility apparatus.
- Right away mount all VSCs (Volume Shadow Copies) VSCs inside a plate.
- This program reconstructs the dynamic library information base.

Interface: https://arsenalrecon.com/items/

14) Volatility Framework

Unpredictability Framework is programming for memory investigation and legal sciences. It is one of the most amazing Forensic imaging instruments that assists you with testing the runtime condition of a framework utilizing the information found in RAM. This application permits you to work together with your colleagues.

Highlights:

- It has API that permits you to queries of PTE (Page Table Entry) signals rapidly.
- Instability Framework upholds KASLR (Kernel Address Space Layout Randomization).
- This instrument gives various modules to checking Mac record activity.
- It naturally runs Failure order when an assistance neglects to begin on different occasions.

Interface: https://www.volatilityfoundation.org

15) Xplico

Xplico is an open-source criminological examination application. It upholds HTTP (Hypertext Transfer Protocol), IMAP (Internet Message Access Protocol), and then some.

Highlights:

- You can get your result information in the SQLite data set or MySQL data set.
- This instrument gives you constant coordinated effort.
- No size limit on information section or the quantity of records.
- You can without much of a stretch make any sort of dispatcher to coordinate the extricated information in a helpful manner.
- It is one of the most incredible open source legal apparatuses that help both IPv4 and IPv6.
- You can perform save DNS query from DNS bundles having input documents.
- Xplico gives PIPI (Port Independent Protocol Identification) element to help advanced measurable.

Interface: https://www.xplico.org

16) e-fense

E-fense is an apparatus that assists you with meeting your PC crime scene investigation and network safety needs. It permits you to find documents from any gadget in one easy to utilize interface.

Highlights:

- It gives assurance from pernicious conduct, hacking, and strategy infringement.
- You can gain web history, memory, and screen catch from a framework onto a USB thumb drive.
- This device has an easy to utilize interface that empowers you to accomplish your examination objective.
- E-fense upholds multithreading, that implies you can execute more than one string at the same time.

Interface: http://www.e-fense.com/products.php

17) Crowdstrike

Crowdstrike is computerized legal programming that gives danger insight, endpoint security, and so forth It can rapidly distinguish and recuperate from online protection occurrences. You can involve this apparatus to find and obstruct assailants progressively.

Highlights:

- It is one of the most amazing digital crime scene investigation instruments that assist you with overseeing framework weaknesses.
- It can consequently dissect malware.
- You can get your virtual, physical, and cloud-based server farm.

B. METHODS

Process of information security are as follows:

- Keep software up-to-date
- Avoid Phishing scams - beware of suspicious emails and phone calls
- Practice good password management
- Be careful what you click
- Never leave devices unattended
- Safeguard Protected Data
- Use mobile devices safely
- Install antivirus/anti-malware protection
- Back up your data

Process of Digital forensics includes

- Identification,
- Preservation,
- Analysis,
- Documentation and,
- Presentation.

RESULT DISCUSSION

Digital Forensics is a sizzling subject of the latest things. Numerous specialists began doing concentrated exploration in this current region. New bearings in this field incorporates creation investigation, advanced proof assortment and legal sciences examination process, proactive legal sciences, interruption recognition

frameworks with the assistance of honeypots, building proof diagrams, distinguishing utilization of cell phones in digital violations and hash work for saving honesty of proof.

Turnbull and Slay [2007] recorded the benefits and detriments of blocking remote organization traffic for the purpose of finding potential proof sources during proof seizure. Likewise, in similar work the benefits and weaknesses of debilitating interchanges to or from 802.11-based remote organizations during measurable seizure were examined. Fast bitwise scan model for enormous scope computerized legal examinations utilizing design matching board to look for string and complex normal articulations talked about in [Hyungkeun et al, 2007].

Willassen [2008] in his postulation proposed different techniques on how the evidential worth of computerized timestamps can be upgraded by adopting a speculation based strategy to the examination of computerized timestamp. Examination of Instant Messaging as far as PC criminology and interruption location is neglected as of not long ago. Creation arrangement utilized for criminology investigation or disguise discovery [A. Orebaugh and J. Allnutt, 2009]. Baggili [2010]

proposed the formation of versatile programming that sudden spikes in demand for a portable gadget and objective is to help crime location work force in the assortment of computerized gadgets throughout an examination.

CONCLUSION

Information security and Digital forensics is an arising field in the latest thing. An overview of the field of information security and digital forensics and how it can serve as a panacea tools for combating cyber-crimes and terrorism is given in this paper. When dissecting digital criminology, the most common way of doing as such is unique than the customary legal sciences. In this study paper we depicted different PC criminology related definitions and periods of digital criminology and legal sciences strategy. The different periods of Cyber criminology have been talked about and each stage investigated with their separate apparatuses. It actually advances and will stay an interesting issue as lengthy as there are ways of undermining information security.

REFERENCES

[1] Orebaugh and J. Allnutt, 2009, Angela Orebaugh and JeremyAllnutt, “Classification of Instant Messaging Communications for Forensics Analysis”, The International Journal of Forensics Computer Science, 2009 (1), pp. 22- 28.

[2] Arfid Ahmed, 2005, “Have You Been Hacked”? A Primer to Cyber Security and Cyber Forensics, the Chartered Accountant, Dec 2005.

[3] Ashley et.al.,2006 Ashley Brinson, Abigail Robinson, Marcus Rogers, “A Cyber Forensics Ontology: Creating a New Approach to Studying Cyber Forensics”, Digital Instigation, Elsevier, 2006.

[4] Baggili and Rogers, 2009. Ibrahim Baggili, Marcus Rogers, “Self-Reported Cyber Crime: An Analysis on the Effects of Anonymity and Pre-Employment Integrity”, International Journal of Cyber Criminology, Vol 2, Issue 2, July-Dec 2009.

[5] Baggili et al, 2007 Ibrahim M. Baggili, Richard Mislan, Marcus Rogers, “Mobile Phone Forensics Tool Testing: A Database Driven Approach”, International Journal of Digital Evidence Fall 2007, Vol. 6, Issue 2.

[6] Baggili, 2010 Ibrahim Baggili, “Generating System Requirements for a Mobile Digital Device Collection System”, European and Mediterranean Conference on Information Systems 2010, Abudhabi, UAE.

[7] Caloyannides, 2001 Caloyannides, Michael A, "Computer Forensics and Privacy". Artech House, Inc. 2001.

[8] Cole, 2010 Eric Cole, Ronald Krutz, James W. Conley, "Network Security: Bible", 2nd Edition, (2010), p.p 730 Wiley India Pvt. Ltd.

[9] Garber, 2001 Garber, L. 2001, "Computer Forensics: HighTech Law Enforcement", IEEE Computer Society's Computer Magazine, 34 (1). pp. 22-27.

[10] Hougton, 2000 Houghton Miffin Company – The American Heritage Dictionary, 4th Edition, 2000.

[11] Hyungkeun et al, 2007 Hyungkeun Jee, Jooyoung Lee,and DowonHong, "High Speed Bitwise Search for Digital Forensic System", Proceedings of World Academy of Science Engineering and Technology, Vol. 26, 2007.

[12] Jansen, Ayers, 2006 Wayne Jansen, Rick Ayers, "Forensic Software Tools for Cell Phone Subscriber Identity Modules", Conference on Digital Forensics, Security and Law, 2006

[13] Karen et al, 2008 Karen Scarfone, Tim Grance, Kelly Masone, "Computer Security Incident Handling Guide", NIST SpecialPublication pp. 800-61, (2008).

[14] Kruse and Heiser, 2002 Kruse W.G, and Heiser J.G, "Computer Forensics Incident Response Essentials", 2002, Addison Wesley Pearson Education, Boston

[15] Marcella, Albert, 2008 Marcella Jr., Albert J., "Cyber Forensics: A Field Manual for Collecting, Examining and Preserving Evidence of Computer Crimes". 2008. Taylor & Francis Group, LLC. Auerbach Publications. pp. 27-48 pp.77-85 pp.87.

[16] McQuade and Samuel, 2006 McQuade, Samuel C. "Understanding and Managing Cybercrime", (2006). Pearson Education, Inc. pp. 373-374.

[17] Meyers and Rogers, 2004 Meyers M, Rogers M, "Computer Forensics: The Need for Stand Ardization and Certification", International Journal of Digital Evidence, 2004.

[18] Oliver et al, 2009 Oliver De Vel, Alison Anderson, Mal Corney, George Mohay, "E-Mail Authorship Attribution for Computer Forensics", Applications of Data Mining in Computer Security, Springer (2009), pp. 230.

[19] Rogers, 2006 Rogers, M. (2006), "DCSA: A Practical Approach to Digital Crime Scene Analysis". West Lafayette, Purdue University.

[20] Tomar et al, 2010, Deepak Singh Tomar, Nikhil Kumar Singh, Bhopal Nath Roy, "An Approach to Understand the End user Behavior Through Log Analysis", International

[21] Journal of Computer Applications pp. 0975-8887) Vol. 5 No. 11, August 2010.