Digital Forensics: 2020 (Seeds are Sown)

– Lt Col Santosh Khadsare
Scientist E, Cyber Forensics Lab, CERT-In Ministry of Electronics and IT
@santkhad2 santoshkhadsare@gmail.com

Article History
Paper Nomenclature:
Argument Based Credentials (ABC)
Paper Code: CYBNMV1N7DEC2019ABC3
Submission Online: 14-Dec-2019
Manuscript Acknowledged: 15-Dec-2019
Originality Check: 17-Dec-2019
Originality Test Ratio: 19%
Peer Reviewers Comment: 20-Dec-2019
Blind Reviewers Remarks : 21-Dec-2019
Author Revert: 28-Dec-2019
Camera-Ready-Copy: 29-Dec-2019
Editorial Board Citation: 30-Dec-2019
Published Online First: 11-Feb-2020

Digital Forensics is a scientifically derived and proved method of Identification, Collection , Analysis, Preservation and Presentation of evidence derived from digital exhibits such as Computers. Storage Media, Mobiles, Network, Cloud, etc. The Investigation Officer on the basis on the analysis report should be able to reconstruct the sequence of events that took place in the digital domain.

Keywords : Digital Forensics | Cyber | BRICS | Organization | Governance

Introduction

Mark my words... The year 2020 is for 'Digital Forensics'. You will see a lot of young aspirants trying to get in this field, lot of money will be spent on research, development of tools, and establishment of labs all across the country. Don't forget even our Prime Minister during the BRICS summit in Nov 2019 has said that India will conduct a workshop on Digital Forensics.

But are we prepared to take a leap from were we are at present. I conduct a lot of lectures for academia, industry and specially for the Law Enforcement Agencies (LEAs) and have a lot of say but in this piece I will touch few issues, maybe not related to each other but off course related of Digital Forensics.

Back to Basics

Firstly, what I observed after interacting with the attendees during my talks is that we still lack the basics. Firstly we need to teach concerned the seizing procedures (digital artifacts) and make available the infrastructure and training for the same.

Digital Forensics is not a one man's arena. It has to be a team of different skills and qualifications.

source:https://drivesaversdatarecovery.com/blog/digital-forensic-process-preservation-collections/

We need people who can do the seizure, who can do imaging, who can do analysis, who can do report writing, who can do research and some more tasks.... And training has to be given to them in that manner or we will be 'JACK OF ALL and MASTER OF NONE'

Deposing as an Expert Witness in a Court of Law'

It is seen that most forensicators shy away or try to avoid it. But, if you get an opportunity...Grab it..As it rarely comes unless you are in a law enforcement agency or part of some notified forensic laboratory

Let's be frank deposing in the court as an expert witness is a very unpleasant experience. It is not only professional grilling by the defense lawyer but also personal most of the time. No one will spare you, not even the judge, you feel like you are surrounded by a pack of wolves.

But let me be truthful, nothing can teach you more than standing in the court, being bombarded with all sort of questions and answering them. You get to know what defense and judge think about your analysis. Many aspects which you may not have dwelled upon, different approaches other than yours

which are available. It makes you a much better analyst than just reading about it. You are a more enlightened person when you walk out.

After deposing on numerous occasions, every time I am summoned I think it as an opportunity to learn something more. Sometimes the defense walks up and praises my report in person (of course not in the court) and an equal number of times thrashes it.

Cyber Forensic Analyst for government/LEA (A) vs. Private company/ Independent (B)

- 'A' gets to investigate a lot of cases of varied nature while 'B' has limited cases.
- 'A' has access to numerous commercial licensed tools while 'B' mostly works on open source tools and frameworks.
- 'A' has more opportunities for training as it is paid by the employer while 'B' has a disadvantage as the training is very expensive.
- 'A' gets an opportunity to depose as an Expert Witness in a court of Law while 'B' rarely gets this chance.
- 'A' has a good knowledge of Admissibility of Electronic Evidence in court why 'B' may lack the same.
- 'A' mostly works on commercial licensed tools and is used to results on a click of a button. They have to work on open source tools and frameworks to excel in their analysis. And the most important is also having a bit of coding skills. When they go for a job in private this becomes a big issue for most of the forensic analysts.
- But still 'A' has an upper hand when it comes to overall development and career path profile.

I have just penned my thoughts which may be very generic but are important.

Be ready for more failures than success when you are at work (be practical). You should have technical and legal knowledge but above all you should be logical. Lastly as a Digital Forensic Analyst (Fornicator) as I always say if do not have Passion and Patience is the right time to change your profession

References

- https://en.m.wikipedia.org/wiki/Cibermen
- https://www.buzzfeed.com/franciswhittaker/dozens-of-people-are-reported-to-have-died-in-a-huge-attack
- https://www.fimfiction.net/story/165043/6/chapter-6-run-like-hell
- https://www.facebook.com/bbcworldservice/videos/as-more-people-shift-towards-cashless-payment-are-wepreparede
- https://csc301csudhfall2016.weebly.com/uploads/2/2/7/6/22764976/how_to_become_a_computer_forensics_investigator__career_and_salary_information.pdf
- https://www.emaze.com/@ATLQRTRR/intro-to-digital-forensics#!

Investigations begin now.....

Frequently asked Question (FAQ) vis-à-vis Digital forensics

Computer forensics, or digital forensics, is a reasonably new-fangled field. Computer forensics investigators, also known as computer forensics specialists, computer forensics examiners, or computer forensics analysts, are charged with recognition and recitation the information contained on, or the state or survival of, a digital artifact. Digital artifacts include computer systems, hard drives, CDs, and other storage devices, as well as electronic documents and files like emails and JPEG images. The fast-growing field of computer forensics includes several branches related to firewalls, networks, databases, and mobile devices. Digital forensics technicians can locate employment with many types of organizations: government (local, state, and federal), accounting firms, law firms, banks, and software development companies. Fundamentally, any type of organization that has a computer system may have a need for a digital forensics specialist. Some digital forensics specialists decide on to establish their own businesses, giving them an occasion to work with a range of client. **There are certain FAQ which would be helpful for the technocrats and learners to excel their career in Digital Forensic**

What is digital forensics used for?

Digital forensics is the procedure of discovery and interprets electronic data. The goal of the process is to conserve any substantiation in its most original form while performing a structured investigation by collecting, identifying and validating the **digital** information for the purpose of reconstructing past events.

What is the difference between digital forensics and cyber security?

Cyber security is the method of protecting and defending information systems from threats such as the mistreat of systems, attackers, data theft, malware outbreaks, and system outages. While **cyber forensics** is the compilation, preservation, acquirement, and analysis of **digital** artifacts for use in legal proceedings

What degree do you need for digital forensics?

Career Requirements

Aspiring **forensic computer** analysts characteristically **require** a bachelor's **degree** in a field such as **digital forensics**, **computer forensics**, or **computer** security.

Do forensic scientists get paid well?

Forensic science technicians **make** a median yearly salary of $70,000 as of 2020, and the bottom half of them can expect to **earn** less **pay** and the top half more **pay**. This works out to about $40 an hour, which is more than the median hourly wage of $20 for all occupations

How do I get into digital forensics?

There are certain Steps for Becoming a Computer Forensics Analyst

- Attend a degree program and/or gain experience in a related field.*
- Become certified as a GIAC Certified Forensic Analyst (GCFA). **
- Apply for an open position as a computer forensics investigator.
- Complete an interview.
- Get hired as a computer forensics investigator.

Santosh Khadsare is an Information security professional who specializes in Digital Forensics. He is a Scientist 'E' in CERT-In (Cyber Forensics), Ministry of Electronics and Information Technology (MeitY), (Government of India) and heading the Cyber Forensics Lab at CERT-In. The author is B.E (Electronics And Telecommunications) and possesses additional qualifications such as CHFI, CEH, RHCSA, Advance Cyber Forensic Course (CDAC), Cyber Crime Investigator, and Access Data Certified Professional. Santosh has 19+ years plus of rich experience in the field of Information Security, Digital Forensics, Cyber Audit, Cyber Laws and Incident Response. Speaker in various international conferences such as CII Conference on Cyber Security, CSI Conference, It-sa Conference on Cyber Security, International Conference on Cyber Law, Cybercrime & Cyber Security, C0C0N, HAKON, National Cyber Defense Summit and GovInfoSec Summit Asia. Authored various articles on information security and Digital Forensics in national and international publications won the COMMUNITY STAR award at NULLCON International Cyber Security Conference 2017.

@santkhad2 santoshkhadsare@gmail.com
https://www.linkedin.com/in/santosh-khadsare-3539a818

Annexure I

Submission Date	Submission Id	Word Count	Character Count
17-Dec-2019	D62942702 (urkund)	1789	10130

Urkund Analysis Result

Analysed Document: ABC-4 Digital Forensics Santosh.docx (D62942702)
Submitted: 17/12/2019 3:13:00 PM
Submitted By: scholastic.seed@gmail.com
Significance: 19 %

Sources included in the report:

week12-version2.docx (D51449462)
https://selectbioindia.com/conference/biographies.php?speaker=228&conf=FRA19
https://cert.eccouncil.org/chfi-scheme-committee.html
https://www.guru99.com/digital-forensics.html

Instances where selected sources appear: 9

Note: Cybernomics runs an Urkund plagiarism tool for the originality check of an article before publication. Urkund is developed by Prio Infocenter AB based in Stockholm, Sweden.

Reviewers Comment

Review 1: The author has covered all the facts on digital forensic in the current scenario. The instance as we leave traces of ourselves in this physical world, similarly we do leave traces when we work on the digital network. The Data recovering here plays a major role in digital forensic.

Review 2: The forthcoming digital forensic is tend to change from Data centric examination to Conduct centric analysis which contains Multi source evidence acquisition, association analysis, Intuitive analysis and Involuntary analysis based on the profile.

Review 3: In my opinion; Artificial Intelligence has completed their way into digital forensics but they are not available in the market. The urbane algorithm can be used in document review and cybercrime detection.

Editorial Excerpt

The above named "**Digital Forensics: 2020 (Seeds are Sown)** "has 19% plagiarism. The Digital Forensic is the procedure of improving, examining and interpreting electronic data. The aim of the procedure is to sanctuary any evidence in its most original form while carrying out a thorough investigation of collecting and authorizing the digital data. These can be obtainable as indication to the court or any other judicial system. The main aspect of the forensic team is to identify, preserve, recover, examine and present. After Editorial board decision it is decided to categorise this article under **"Argument Based Credentials (ABC)".**

Acknowledgement

Author is highly indebted to Scholastic Seed Inc & editorial team of Cybernomics, For making the write-up in the shape of an article.

Disclaimer

The article published in a magazine Cybernomics is an excerpt of my researchs and are necessary to quote as and when required.

Citation

Santosh Khadsare
"Digital Forensics: 2020 (Seeds are Sown)"
Volume-1, Issue-7, Dec 2019. (www.cybernomics.in)

Frequency: Monthly, Published: 2019
Conflict of Interest: Author of a Paper had no conflict neither financially nor academically.

Scholastic Seed Inc.
www.scholasticseed.in