Digital Forensics – As we know it today…

Dr K Rama Subramaniam
CEO, Valiant Technologies Pvt Ltd
rama@valiant-technologies.com

'Digital Forensics' is better understood by the common connotation of the words rather than through a formally approved definition. It may not be far from reality to state that 'Digital Forensics' begs an academically rigorous definition though there are quite a few good working definitions. A briefing note (1) on Digital Forensics prepared for the British Parliament states that "There is no standard definition, but the UK Forensic Science Regulator (2) defines digital forensics as the process by which information is extracted from data storage media (e.g. devices, systems associated with computing, …), rendered into a useable form, processed and interpreted for the purpose of obtaining intelligence for use in investigations, or evidence for use in criminal proceedings." Ken Zatyko (3) former Director of the US Defense Computer Forensics Laboratory prefers a more process oriented definition when he suggests that digital forensics can be defined as "the application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation." As we wade through these approaches to defining digital evidence, a very different view point is found in SWGDE (Scientific Working Group on Digital Evidence) glossary (4) where computer forensics is defined as a "sub-discipline of Digital & Multimedia Evidence, which involves the scientific examination, analysis, and/or evaluation of digital evidence in legal matters." Interestingly this definition found in SWGDE glossary positions forensics as a subset of evidence while the common understanding is that evidence is sub-set of the forensic process. This paper is no place for an elaborate debate on whether forensics is a subset of evidence or *vice-versa*.

Digital Forensics and Traditional Forensics

As opined by Donn Parker, in a paper-based environment, the legal system assumes a set of processes that is fully understood and observed by all parties. However, when we apply these processes to digital evidence, we encounter a set of problems that requires a legally defensible solution for digital forensics to have served its purpose (5). While most of the work on the development of digital forensics can be credited to law enforcement and criminal justice systems of different countries, there is a sprinkling of contribution by private enterprises as well; mostly by vendors of products used in the digital forensics process. The largest users of digital forensics services are the prosecution and judiciary while private enterprises are slowly but surely understanding the importance of this discipline as significant value adders for their internal investigations on cyber infractions.

Digital forensics started getting some attention when the specialized laws that were enacted to curb cyber-crimes had to be dovetailed into the country's generic legal system and stakeholders asked a poignant question – "how will evidence look like in a digital environment?" Crime management and jurisprudence depended on evidence of probative value to determine whether a crime had in fact been committed and if so, to identify the perpetrators beyond reasonable doubt. A key question that is still being asked is if such identification of perpetrators is possible at all, given that anonymity is the hallmark of the Internet. This process of ensuring dependence on reliable evidence of probative value can be seen supporting some of the well- known principles of jurisprudence including the one propounded by Sir William Blackstone way back in 1765 when he said that "Better that ten guilty persons escape than that one innocent suffer." (6) Can digital evidence ever be so water tight or will application of these principles to poorly structured digital forensic processes result in poor rates of prosecution and sentencing.

Given the importance of evidence in criminal justice dispensation, it is important to understand the ways in which evidence is identified, gathered, analyzed and interpreted and finally presented in a court of law in line with the procedural requirements laid down locally. Matters relating to evidence in conventional forms of crimes (*eg*., murder, armed robbery, etc.) have been well established for a long time and all the parties handling such evidence *viz*., the law enforcement, prosecuting and defense attorneys and the judges know quite clearly the ways in which evidence will be handled, analyzed and interpreted. It is widely believed that the legal interpretation of autopsy was recorded in a Chinese work (7) dating back to the 13th century while 16th century saw the European interest in forensics with the French, Italian and German surgeons propounding the concept of police medicine and took forward the Chinese work on autopsy to more logical conclusions. (8) We later had ballistics, toxicology, anthropometry and finally the now famous finger prints. Digital forensics is struggling to reach the same level of maturity in less than forty years, what took traditional forensics close to four hundred years to reach.

Ubiquity of Digital Forensics

The Association of Chief Police Officers (ACPO) bring out the ubiquity of digital evidence quite clearly when they state that "it must be present in almost every crime." (9) This ubiquity can be understood when we realize that we have gone past the era when digital forensics mostly looked at PCs and laptops. Now, material to support digital forensic investigation can be found a wide variety of devices including PDAs, smart phones, GPS devices, asset access controllers, CCTV, game

consoles, fitness wrist-wraps and in third party devices like those operated and controlled by ISPs. There is also a growing tendency to capture data or evidence in transit as data moves between network devices and voice call intercepts, with lawful authority to do so. As we keep pace with the proliferation of devices that are potential repositories of evidence for digital forensic analysis, an interesting trend is the skewed distribution of devices used to collect digital evidence. Smart phones continue to remain the most analyzed device for collection of digital evidence while investigating cyber-crimes. The UK Metropolitan Police reports that mobile phones constitute three-quarters of the plethora of evidence holding devices that they examine annually (10).

Digital Forensics process – is it a scientific method?

Even as we decide on the relevance, applicability and uniformity of what has come to be called a scientific process of forensic analysis involving evidence collection and interpretation, there are questions being raised about digital forensics being a scientific discipline. Simon A Cole (11) points to the efforts by forensic communities to fit themselves into a template called "scientific method" constructed around hypothesis testing. However, he also points to the fact that "scientific method" is more of an honorific rather than a description of what society generally calls "science." This reflects the contemporary American thought that digital forensics cannot be any more scientific than the general forensic science can be. The British thought on this subject is more focused on processes, unlike the Americans who have considered the perspectives. The Forensic Science Regulator in the UK admits that risk of errors occurring in digital forensics is significant (12) and strongly recommends that digital forensic processes must be carried out in institutions accredited to ISO17025 standards. So, we are now facing the prospect of collecting, analyzing and interpreting digital evidence in frameworks that does not seem to fit a conventional "scientific method" template and can remain error-prone. It is important to understand this caveat since users of digital forensic processes should not be carried away by the belief that the results are conclusive and beyond an iota of doubt, though in many cases the results can pass the legal test of being beyond 'reasonable' doubt.

Digital Forensic Processes - Evolution

The digital forensic process is often seen to adopt a life-cycle approach since it has a clear start, end and a defined flow. Most of what we have as digital forensics process framework today can be traced back to the pioneering work that nurtured at the various Digital Forensics Research Workshops (DFRWS). As an example, Palmer's Roadmap for Digital Forensics Research (13) presented in the first DFRWS paved way for two adaptations. Firstly, it formed the basis for development of 'Systematic Digital Forensic Investigation Model' by Agarwal *et al (14)* in 2011. Palmer can also be credited with laying the foundation for developing a framework for comparative study of digital forensic models, spearheaded by Reith *et al (15)* Carrier and Spafford (16) pioneered the concept of event centric digital forensic investigation, which appears to have influenced the Enhanced Digital Investigation Process by Baryamureeba and Tushabe. (17) I have personally heard some information security professionals claim that digital forensics is another *avatar* of incident response process and have embedded evidence collection as a component of the the incident response process.

Most models discussed above and a few more that are actively used (including that proposed by Perumal,(18) Perumal *et al (19)* and Kohn (20)) substantially adopt the waterfall model and expect that all steps are followed in the right sequence and covers all evidence that can be collected at a crime scene and related locations. However, in the case of emergencies involving digital forensic analysis, investigators have done well to learn from the medical emergency processes and apply the concept of triage. In the medical world, triage is the assignment of degrees of urgency to wounds or illnesses to decide the order of treatment of a large number of patients or casualties. In a digital crime scene, the concept of triage has been built in the decision process to determine acquisition, quick assessment of the relevance of what has been acquired and decide on the course of action, particularly when threatened with device overload or data deluges. This becomes important in situations where speed of decision to act on evidence collected becomes important; as could be in cases where digital forensic process points to clues related to kidnapping; ransom demands, etc. While not many have questioned the relevance of triage in the digital forensics context, a key concern appears to be that investigating officers using triage could be in conflict with the requirement of independence expected at every stage of digital forensic process. This arises because in a triage, by definition, the investigating officer will pass instant judgement on the relevance, accuracy and admissibility of evidence on hand. Among the mitigating measures to address this risk of lack of independence, one that is gaining ground is that the prosecuting officers do not interpret the triage results but stop with using them as factual evidence and take a call. It is not hard to understand the difficulty in adopting such a dichotomous attitude when confronted with large volumes of evidence and principles of triage is to be adopted.

With a view to addressing some of the limitations of using forensic investigation tools and methods in criminal justice dispensation, Crown prosecutors in the UK often follow a process leading to the creation of Streamlined Forensic Reporting (SFR). This has helped in reducing court time and efforts by facilitating an early mutual acceptance of the forensic issues by the prosecution and defense and also agreeing on what will be contested. SFR or its equivalent is slowly gaining ground in different jurisdictions with the Crown Prosecution in the UK formally endorsing its relevance to digital forensics investigation. (21)

Challenges to Digital Forensics processes

In addition to the conceptual challenges and issues that plague the evolution of a robust and globally applicable digital forensic process framework as discussed above, there are other challenges that often confront a digital forensic investigator. The most common problem relates to the way in which data is stored securely. Encryption is recognized as the cornerstone on which many data security solutions have been built. When a digital forensic investigator encounters encrypted data, nothing much can be done unless the forensically relevant data is decrypted. Laws in many countries, including India, have provisions that enable a law enforcement officer of a certain rank to warrant the disclosure of the decryption key enabling access to the data in plain text format. The United States tried what is commonly known as the LEAF – Law Enforcement Access Field as a means of being able to decrypt messages in encrypted format when the Government wanted access, in national interest and in counter-terrorism activities. Though this is no longer in use, there is suspicion that some legacy systems may still carry this. The process centered around the 'Clipper Chip' developed by the US National Security Agency and was meant to encrypt voice and data messages. The Clipper Chip used a crypto algorithm called 'Skipjack' that was also developed by US National Security Agency and at the core of this development was the concept of key-escrow which enabled US Government agencies, after demonstrating their authority to do so, to decrypt and access plain text data or voice communication. Amid strong protests from Electronic Privacy Information Center and the Electronic Frontier Foundation as well as other privacy protagonists, LEAF was discontinued but the law enforcement still holds the right to compel decryption under certain conditions. Notwithstanding all that has been said about the power available with law enforcement to compel decryption or sharing of crypto-keys, such process is time consuming and situations requiring quick access to OoFI (Objects of Forensic Importance) will still throw up challenges.

Increased reliance on the Cloud for storage of information poses a second set of challenge for the digital forensic investigator. In a cloud environment that permit multiple access paths to data storage with collaborative computing, there can be challenges arising from even minor issues like one user over-writing on a location where logically deleted data was originally stored. This will result in permanently losing the deleted data which could contain OoFI. Most cloud access is subject to strong access control protocols that is bound to delay forensic analysis of information held in the cloud. Further, cloud service provider and the servers on which data is stored may be in jurisdictions other than where the investigation is happening. Though investigators may seek support under Mutual Legal Assistance Treaties to access information in different jurisdictions, such processes will be painfully slow.

A third and perhaps technologically the most exciting challenge is anti-forensics. Cyber-crime perpetrators often have full knowledge of the various methods and processes adopted by digital forensic investigators. To derail the digital forensic investigation process and to mislead investigators, anti-forensic processes are adopted. Some of the more common anti-forensic practices include changes to calendar and time stamps; overwrite file content so that it is permanently unavailable to the investigators; using multiple passwords to access different parts of the storage where different parts of the data is stored, etc. The last process ensures that even when one password is disclosed under duress or using due process of law, it will point to only one part of the information which does not to contain anything incriminating. It is highly unlikely that the digital forensic investigator will always suspect that what is available is incomplete unless the anti-forensic process has been flawed.

Digital Forensics as a Service (DFaaS)

Though we have identified the proliferation of cloud computing as an impediment to quick digital forensic analysis, a section of digital forensic professionals are looking at the option of harnessing the power, architecture and ubiquitous reach of the cloud to develop a Digital Forensics as a Service (DFaaS) model. Building on the findings of Lee and Un (22) that efficiency of cloud systems significantly improves during indexed searches, Wen *et al (23)* proposed a cloud-based service harnessing the potential of parallel computing to overcome the problem of data magnitude that threatened digital forensic processes with unacceptable levels of delay. This service, in the words of Wen *et al* (cited supra) "deals with a large volume of forensic data, sharing interoperable forensic software, and providing tools for forensic investigators to create and customize forensic data processing workflows." They further report that based on testing a number of scenarios, the workflow solution proposed can save upto 87% of analysis time in the tested scenarios. When will DFaaS come of age is too early to guess though one successful use case was reported by van Baar *et a (24)* when they tried implementing DFaaS in the Netherlands Forensic Institute with success.

What direction will the actual implementation of digital forensics services take in the future is unclear but what remains clear is that digital forensics is here to stay. The more mature, repeatable, reliable and objective digital forensic processes become, the more will its acceptability be in the pursuit of evidence of probative value.

References

1. Parliamentary office of Science and Technology, *Digital Forensics and Crime,* Post Note 520 (March 2016)
2. UK Forensic Science Regulator *Newsletter* No. 26 (2015)

3. Ken Zatyko, Commentary*: Defining Digital Forensics*, Forensics Magazine on-line version (January 2007) < https://www.forensicmag.com/article/2007/01/commentary-defining-digital-forensics> accessed on 30 May 2018
4. Scientific Working Group on Digital Evidence, *SWGDE Multimedia and Digital Evidence glossary*, Ver 3.0 (June 2016) p.6 < https://swgde.org/documents/Current%20Documents/SWGDE%20Digital%20and%20Multimedia%20Evidence%20Glossary> accessed on 30 May 2018
5. Donn B. Parker, Computer Crime: Criminal Justice Resource Manual (National Institute of Justice, Washington DC, 1989).
6. There are dissenting views as well on this principle. Bismarck is said to have opined that he would rather let ten innocent persons suffer than let one guilty person escape.
7. Ascribed to work on autopsy and court handling of evidence from autopsy by Song Ci (1248)
8. Work by French scientists Ambroise Pare and Francois Immanuele Fodéré; Italian surgeons Fortunato Fidelis and Paolo Zacchia and German physician Johann Peter Frank laid the foundation of modern day medical forensics
9. Association of Chief Police Officers (ACPO), *Good Practice Guide for Digital Evidence*, 2012
10. Metropolitan Police Service (UK), Digital Cyber and communications Forensics – Information for prospective Bidders (2015)
11. Simon A Cole, *Who will Regulate American Forensic Science?* Seton Law Review Vol 48 - 563
12. Forensic Science Regulator, UK, *Annual Report, 2015*
13. Palmer, G., A Road Map for Digital Forensic Research. *First Digital Forensic Research Workshop*, 2001, Utica, New York. pp. 27–30
14. Agarwal, A., Gupta, M., Gupta, S., Gupta, S.C., Systematic Digital Forensic Investigation Model. *International Journal of* Computer *Science and Security* (2011), 5(1), pp. 118–131.
15. *Reith*, M., Carr, C. and Gunsch, G., An Examination of Digital Forensic Models. *International Journal of Digital Evidence*, 2002, 1(3), pp. 1–12
16. Carrier, B. and Spafford, E.H., An Event-Based Digital Forensic Investigation Framework. In *Proceedings of Digital Forensic Research Workshop* (2004) pp. 11–13.
17. Baryamureeba, V. and Tushabe, F., The Enhanced Digital Investigation Process Model. In *Proceedings of the Fourth Digital Forensic Research Workshop* (2004) pp. 1–9.
18. Perumal, S., Digital Forensic Model Based on Malaysian Investigation Process. *International Journal of* Computer *Science and Network Security*, (2009) 9, pp. 38–44.
19. Perumal, S., Norwawi, N.M. and Raman, V., Internet of Things (IoT) Digital Forensic Investigation Model: Top-Down Forensic Approach Methodology. In *Fifth International Conference on Digital Information Processing and Communications (2015)*, IEEE, pp. 19–23.
20. Kohn, M.D., Eloff, M.M. and Eloff, J.H.P., Integrated Digital Forensic Process Model. *Computers & Security* (2013) 38, pp. 103–115.
21. Crown Prosecution Service, UK, National Streamlined Forensic Reporting Guidance (2015) Sec. 2
22. Lee, J. and Un, S., 2012. Digital Forensics as a Service: A Case Study of Forensic Indexed Search. In *International Conference on ICT Convergence (2012)*, pp. 499–503
23. Wen, Y., Man, X., Le, K. and Shi, W., Forensics-as-a-Service (FaaS): Computer Forensic Workflow Management and Processing using Cloud. In *The Fifth International Conferences on Pervasive Patterns and Applications (2013)* pp. 1–7
24. van Baar, R.B., van Beek, H.M.A. & van Eijk, E.J., Digital Forensics as a Service: A Game Changer. *Digital Investigation* (2014) 11, pp. S54–S62

About the author

Dr K Rama Subramaniam is CEO of Valiant Technologies Pvt Ltd, a consulting organization providing services in the areas of information security, GRC, privacy, digital forensics and cyber criminology. He served as Adjunct Professor at the University of Madras (India) and Copperstone University (Zambia) and taught a masters course at the University of Dubai. He is the current Global Chair of International Institute of Certified Forensics Information Professionals, Inc. and Vice Chair of Cyber Security and Digital Forensics Research Foundation. He served earlier as Global Chair of the E&A Group of GAISP and Chair of Accreditation Committee of OISSG. He is an IBM GIO Alumni and served three terms as India's country representative at IFIP-TC11. He has an MBA (with Distinction) from the University of Lincoln and a multi-disciplinary doctorate in the area of cyber criminology. He has CISSP, CISA, CISM credentials and FCA, FCFIP and FISC fellowships. He was recipient of the ISC-Prof S S Srivastava prize for excellence in social sciences research.

Robert Baptiste, a French security expert and ethical hacker, today tweeted that "an anonymous source" has full access to database of PM Narendra Modi's website. Baptiste added that he would start a security audit after PM Modi contacts him in private. He later claimed that 'narendramodi.in' team got in touch with him and they will take appropriate measures.