2019

Rethinking digital forensics

Andrew Jones
Edith Cowan University

Stilianos Vidalis

10.33166/AETiC.2019.02.005
Jones, A., & Vidalis, S. (2019). Rethinking digital forensics. *Annals of Emerging Technologies in Computing (AETiC), 3*(2), 41-53. https://doi.org/10.33166/AETiC.2019.02.005

Annals of Emerging Technologies in Computing (AETiC)
Vol. 3, No. 2, 2019

Review Article

Rethinking Digital Forensics

Andrew Jones[1,2,*] and Stilianos Vidalis[1]

[1]University of Hertfordshire, United Kingdom.
andy1.jones@btinternet.com, s.vidalis@herts.ac.uk
[2]Security Research Institute, Edith Cowan University, Australia
*Correspondence: andy1.jones@btinternet.com

Received: 1st February 2019; Accepted: 25th February 2019; Published: 1st April 2019

Abstract: In the modern socially-driven, knowledge-based virtual computing environment in which organisations are operating, the current digital forensics tools and practices can no longer meet the need for scientific rigour. There has been an exponential increase in the complexity of the networks with the rise of the Internet of Things, cloud technologies and fog computing altering business operations and models. Adding to the problem are the increased capacity of storage devices and the increased diversity of devices that are attached to networks, operating autonomously. We argue that the laws and standards that have been written, the processes, procedures and tools that are in common use are increasingly not capable of ensuring the requirement for scientific integrity. This paper looks at a number of issues with current practice and discusses measures that can be taken to improve the potential of achieving scientific rigour for digital forensics in the current and developing landscape.

Keywords: ***Digital forensics; scientific rigour; standards; procedures; tools***

---

1. Introduction

Due to the modern socially-driven, knowledge-based virtual computing environment that organisations are operating in, we argue that the processes, procedures and tools that have been accepted and are commonly used in digital forensics can no longer meet the need for scientific rigour. The U.S. Department of Defense (DOD), in its publication Information Operations[1], has defined the Information Environment (IE) as "the aggregate of individuals, organizations and systems (resources) that collect, process, disseminate, or act on information." The document concludes that "the information environment is where humans and automated systems observe, orient, decide, and act upon information, and is therefore the principle environment for decision making".

The main attributes of the modern IE are:

- the physical and virtual size of it (large);
- the rapid evolution as a result of the introduction of new technologies;
- the great irregularity between physical and virtual boundaries of different stakeholders and legal entities;
- the transparent access to and control of assets;
- the speed of information and knowledge exchange involving users across boundaries;

Andrew Jones and Stilianos Vidalis, "Rethinking Digital Forensics", *Annals of Emerging Technologies in Computing (AETiC)*, Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 41-53, Vol. 3, No. 2, 1st April 2019, Published by International Association of Educators and Researchers (IAER), DOI: 10.33166/AETiC.2019.02.005, Available: http://aetic.theiaer.org/archive/v3/v3n2/p5.html.

- the stealth and limited attribution because of technologies and legislation, the rapid concentration of capability allowing for rapid generation and escalation of events;
- the non-serial and distributed nature that allows the parallel execution of events against multiple targets creating non-linear events.

2. Literature Review

The underlying principles that are applied to the digital forensic process were developed in the 1990s, but follow the general standard for the acceptability of evidence in a court of law that were provided as a result of the 1923 Frye v. United States case. In this case, the admissibility of a systolic blood pressure deception test as evidence was discussed. The Court in the Frye case held that expert testimony must be based on scientific methods that are sufficiently established and accepted.

Later, in 1993, in the Daubert v. Merrell Dow Pharmaceuticals, Inc. United States Supreme Court case (Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579, 584-587.), the standards for admitting expert testimony in U.S. federal courts were determined and the Court in this case held that the enactment of the Federal Rules of Evidence implicitly overturned the Frye standard. The standard that the Court articulated is referred to as the Daubert standard. This was given as:

• **'Judge is gatekeeper':** Under Rule 702 (Testimony by Expert Witnesses), the task of "gatekeeping", or assuring that scientific expert testimony truly proceeds from "scientific knowledge", rests on the trial judge.

• **Relevance and reliability:** This requires the trial judge to ensure that the expert's testimony is "relevant to the task at hand" and that it rests "on a reliable foundation". Concerns about expert testimony cannot be simply referred to the jury as a question of weight. Furthermore, the admissibility of expert testimony is governed by Rule 104(a), not Rule 104(b); thus, the Judge must find it more likely than not that the expert's methods are reliable and reliably applied to the facts at hand.

• **Scientific knowledge = scientific method/methodology:** A conclusion will qualify as scientific knowledge if the proponent can demonstrate that it is the product of sound "scientific methodology" derived from the scientific method.

• **Illustrative Factors:** The Court defined "scientific methodology" as the process of formulating hypotheses and then conducting experiments to prove or falsify the hypothesis, and provided a set of illustrative factors (i.e., not a "test") in determining whether these criteria are met:

1. Whether the theory or technique employed by the expert is generally accepted in the scientific community;
2. Whether it has been subjected to peer review and publication;
3. Whether it can be and has been tested;
4. Whether the known or potential rate of error is acceptable; and
5. Whether the research was conducted independent of the particular litigation or dependent on an intention to provide the proposed testimony.'

After a number of other, relevant rulings, Rule 702 was amended in 2000 in an attempt to codify and structure elements embodied in the "Daubert trilogy." The rule then read as follows:

• **Rule 702. Testimony by Experts:** If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified

as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if:

1. the testimony is based upon sufficient facts or data,
2. the testimony is the product of reliable principles and methods, and
3. the witness has applied the principles and methods reliably to the facts of the case.

Then, again, in 2011, Rule 702 was amended to make the language clearer. The rule now reads:

• **Rule 702. Testimony by Expert Witnesses:** A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:

a. The expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
b. The testimony is based on sufficient facts or data;
c. The testimony is the product of reliable principles and methods; and
d. The expert has reliably applied the principles and methods to the facts of the case.

While these are all US based cases, current best practice for digital forensics around the world, for the most part, attempts to satisfy this standard. In the UK this is expressed in the Association of Police Officers (ACPO) good practice guide Principles of Digital Evidence[2][1].

In the USA, the Scientific Working Group on Digital Evidence (SWDGE) produced the SWGDE Best Practices for Digital Evidence Collection[3] and the SWGDE Best Practices for Computer Forensic Examination[4] (latest versions -2018) to give advice for the collection and processing of digital evidence.

3. The 'Scientific rigour of process' paradox

The Daubert standard requires general acceptance of the theory and technique used in the digital forensic process to be generally accepted by the scientific community and have been peer reviewed. Considerable research has been undertaken into the theory that underpins the processes in use but, unfortunately, for the most part it is dated and has not addressed the current technologies and where it has, it has not been adopted in practice. The majority of the techniques that are used in the digital forensic process have not satisfied the criteria of known error rates. Most of the main tools that are in use are proprietary commercial products and there is no published data available on error rates. Of more concern is that on the occasions when these tools have been tested, they have been found to produce, in some cases, significantly different results[5-7]. The paradox is that due to lack of a better solution, experts have shifted their risk homeostasis levels of what is acceptable for the notions of 'scientific', 'rigour' and of 'process'.

In the USA, the National Institute for Standards and Technology (NIST) currently has 3 projects running: the National Software Reference Library (NSRL), the Computer Forensic Tool Testing (CFTT) and the Computer Forensic Reference Data Sets (CFReDS). They have also created a digital forensic tool catalogue and state that "The primary goal of the Tool Catalog is to provide an easily

[1] The Daubert Trilogy refers to the three key cases that established precedence for how judges determine the admissibility of expert testimony. The three cases that make up the trilogy are: Daubert v Merrell Dow Pharmaceuticals, Inc., 590 U.S. 579 (1993), General Electric Co. v Joiner, 522 U.S. 136 (1997) and Kumho Tire Co., Ltd. v Carmichael, 526 U.S. 137 (1999).

searchable catalog of forensic tools. This enables practitioners to find tools that meet their specific technical needs." However they caveat this with a cautionary note that "tool information is provided by the vendor".

- The NSRL provides file profiles computed from this software (such as MD5 and SHA-1 hashes) as a Reference Data Set (RDS) of information. The RDS can be used in the forensic examination of file systems, for example, to speed the process of identifying unknown or suspicious files.
- The CFTT provides a methodology consisting of tool requirements specifications, test procedures, test criteria, test sets, and test hardware.
- The CFReDS provide to an investigator a documented sets of simulated digital evidence items for examination.

In 2018, NIST published a document by the Organization of Scientific Area Committees for Forensic Science (OSAC) entitled "A Framework for Harmonizing Forensic Science Practices and Digital/Multimedia Evidence"[8] which states that "Like many other specializations within forensic science, the digital/multimedia discipline has been challenged with respect to demonstrating that the processes, activities, and techniques used are sufficiently scientific" The document then goes on to detail the work carried out by the OSAC Task Group (TG).

There is now a considerable level of expertise and experience in the imaging of computer hard disks. While the volume of data that they might contain continues to grow, the underlying technologies (electromechanical and solid state) have not seen significant disruption for a number of years and disks that will work in one computer can normally be expected to work in another; although there are exceptions. When dealing with mobile phones, tablet computers and other devices, there is an increasing number of issues that include the range of operating systems and the versions of them, and the number of manufacturers that do not apply common standards and, indeed, seek to differentiate themselves.

There are now also an increasing range of products on the market that contain computer processors and memory that may contain potential evidence and these can be classed as Internet of Things (IoT) devices. Many of these have limited processing power and digital storage but may contribute valuable evidence to an investigation or have been used in the commission of a crime. An example of this is was reported in 2016[9], when more than 1.5 million CCTV cameras were hijacked and used to carry a denial of service attack on a security website.

4. The Challenges of the Paradox

Some of the challenges we are now facing as a result of the characteristics of the modern information environment are:

1. Completeness. Given the increasing volume of data storage on all forms of media, with computer hard disks now at 10 plus TB, USB storage devices at more than two Tb and micro SD cards at 512 GB together with the issues created by cloud storage, the concept of collecting a 'complete' set of the data is becoming increasingly problematic due to the size of the storage media and the volume of data. There is now an issue of the time to capture and process the volumes of data and issues of privacy when the data is being collected from a server that holds the data of more than one person or organisation as a result of the disparity between the physical and virtual boundaries of the stakeholders

and the increasing transparency of access to and control of the assets. If the 'complete' dataset is not collected there is the potential for an accusation of selective collection of only the data that supports a case and the exclusion of exculpatory evidence. The question, if we adopt an approach of selective collection, is how do we guarantee that all relevant data has been collected and how do we ensure that the process is repeatable? More of the point, because of the developing technological environment, the speed of information exchange across logical boundaries and the non-serial and distributed nature of processing that may create non-linear events will have greatly changed after the initial collection of data, rendering our process non-applicable and outdated.

2. Live forensics. This is when the artefacts are being discovered and captured on a live running system from volatile memory. The main purpose is to acquire volatile data that would otherwise get lost if the computer system was turned off or would be overwritten if the computer system were to remain turned on for a longer period. As the size of RAM in computer devices increases, so does the potential volume of data that may be of value as evidence that it may contain. The very action of capturing the data stored in RAM is likely to result in changes to elements of the data and as a result, a second attempt to image the logical device will be on the changed data and as a result, will generate a different MD5 or SHA hash value. While the reality of this has been accepted in practice, it falls short of the requirement for a scientific methodology. More of the point, paging, caching and true distribution of processing and storage, combined especially with the potential for the rapid concentration of capability and non-serial and distributed processing, challenge the underlying principles and foundations of live forensics and the quality of data that can be collected.
3. Volatility. Associated with the ongoing development of existing technologies, the introduction of new technologies and the speed of data exchange, increasingly across international boundaries, together with the increased use of devices that contain an ever-increasing capacity of volatile memory and an increasing number of devices with limited volatile storage and processing capability (mostly IoT devices), the potential volume and life of potential evidence is moving, at the same time, to two extremes. For devices with an increasing size of volatile memory, there is not only the potential for evidence, but also that it will exist for longer before the storage space is overwritten. For the IoT devices, with limited storage, potential evidence may be transitory and only exist for a very short period of time but again, once the data is captured, it may not be possible to repeat the process and get the same result.
4. Logical versus physical acquisition. With the increasing storage capacity of mobile devices (tablets, mobile phones, drones, fitbits, etc.) there is the potential for significant volumes of data and potential evidence. However, for many of these devices, it is not possible to extract an image of the physical device that would include all of the device settings and we are often limited to obtaining an image of the logical device which will normally only give the user data. One of the issues here is that capturing the logical image of this type of device will normally result in the process not being repeatable as a number of the files that are contained are constantly changing and, similar to live forensics, a second attempt to create an image of the logical device will result in a different MD5 or

SHA hash value. While the reality of this has been accepted in practice, it falls short of the requirement for a scientific methodology.

5. The increasing diversity of devices and the range of operating systems is directly linked to the speed of evolution that is taking place, the introduction of new technologies and the increasing transparency of access to and control of assets. Prior to the introduction of the Android operating system in 2007, the forensic investigator was most likely to encounter either the Windows, Linux or the Apple Operating systems for most computers and the Windows, Apple and Blackberry OS for most mobile phones. In the period, since then, with the introduction of a wide range of IoT devices, another 8 operating systems[10] have come into use. Each of these adds a level of complexity and the requirement of knowledge and experience in how to deal with the capture of data and subsequent analysis.
6. The Cloud. Cloud computing has been a significant advance in the information technology (IT) services that are available today. One of the issues with the Cloud is that the Cloud Service Providers (CSPs) have not been open and allowed their customers see how the Cloud environment that they are offering works. This lack of transparency is an issue in digital investigations. In addition, jurisdiction, data duplication and multi-tenancy in the cloud platforms will add to the challenge of locating, identifying and separating the data relating to suspect activity or the targets of attacks for digital forensic investigations. At the present time, the approaches that are taken to evidence collection and recovery of evidence in a traditional non-cloud environment do not map well into a Cloud environment as they rely on physical and unrestricted access to the relevant system and user data. This is not possible in the cloud environment due its decentralized data processing and storage.

It is increasingly clear that the concepts of traditional digital forensics cannot be directly used in cloud systems. In particular, the distributed processing and multi-tenancy nature of cloud computing, as well as its highly virtualized and dynamic environment, make the identification of digital evidence and its preservation and collection difficult. In agreement with Biggs and Vidalis[11], the development of the Cloud environment was not undertaken with digital forensics and evidence integrity in mind, and as a result it is a challenging technically, logistically and legally.

In cloud computing the forensic process needs to be carried out in three distinct areas; Client system forensics, Cloud forensics and Network forensics. The Client system forensic process is well understood and practiced and is the 'traditional' forensics.

Cloud server forensics, although not a new concept, greatly adds to our paradox with the issues of multi-tenancy, physical inaccessibility and unknown location of the artefacts to be collected and this can lead to jurisdictional issues. The artefacts may include user data, system logs, application logs, user authentication and access information, database logs etc. In a highly decentralized and virtualized cloud environment it is quite common for data to be located in multiple data centres located in different geographic locations[12]. Traditional approach to seizing the system is not practical in the cloud environment, even if the location is known, as the effect would be disproportionate and could bring down whole data centre, affecting a large number of other users due to multi-tenancy. A number of research papers have discussed this issue and some possible solutions[12-16]. The problem of governance is another significant issue in cloud forensics as

discussed in the European Network and Information Security Agency (ENISA) cloud computing risk assessment report, which highlights the 'loss of governance' as one of the top risks of cloud computing, especially in Infrastructures as a Service (IaaS)[17]. In IaaS, users have more control and relatively unfettered access to the system logs and data, whereas in the Platform as a Service (PaaS) model their access is limited to the application logs and any pre-defined APIs provided, and in the Software as a Service (SaaS) model the customers have little or no access to such data. As the customers increasingly rely on the CSPs to provide the functionality and services they, of necessity, give more control of their information assets to the CSPs. As the customers relinquishes control, they inevitably lose access to important data and as a result it is not available for identification and collection for any subsequent forensic needs[12]. As the degree of control decreases, there will be less data of forensic value available for investigations and as a result there is a greater dependency on the CSPs in order to gain access to such data. This will also be dependent on the Service Level Agreement (SLA) that the customer has with the CSP are what they are capable of and willing to provide. In a traditional server based environment, where the physical locations of the systems are known, the investigators can have full control over the forensic processes. In a cloud environment, there is a high likelihood of evidence being overwritten or modified at any given time, since the cloud platforms are subject to constant and rapid changes. This highlights the importance of preserving the evidence as soon as it is identified, using appropriate and acceptable preservation techniques.

Traditional network forensics deal with the analysis of network traffic and the logs that systems produce for tracing events that have occurred. Network forensics is theoretically also possible in cloud environments. The TCP/IP protocol layers can, potentially, provide information on communications between Virtual Machine (VM) instances within cloud and also with instances outside the cloud. CSPs do not normally provide the network traces or communication logs generated by the customer instances or applications despite the fact that such logs may be critical element of data for a forensic investigation[13]. In addition, the Virtual Machine (VM) instances may be subject to movement within a data centre, outside one data centre to a different data centre in the same jurisdiction or to a data centre located in a separate jurisdiction, based upon many factors such as load balancing, business continuity etc. Such moves, carried out by the CSPs, are completely outside the control of the client. This also adds additional challenges to the cloud server-side forensics.

It is not only the digital evidence itself that needs to be acceptable to any court of law, but also the processes followed in the conduct of an investigation. In the last two decades, academic researchers and forensic practitioners have proposed a significant number of digital forensic frameworks and previously published processes and frameworks have been refined, resulting in a variety of digital forensic process models and terminology. While this can be seen as a natural development to meet the changes in technology and the law, it results in a lack of standardisation in the processes and procedures adopted. At the same time the volume and diversity of devices that have digital processing and storage have continued to expand rapidly with the result that there has not been adequate research carried out on these devices to establish scientifically sound methods for the extraction of evidence.

4. The Tools and Their Provenance

Throughout the digital forensics landscape, there are a number of tools that have been widely used and accepted for use in digital forensic imaging and analysis. The National Institute of Justice,

in the USA, in conjunction with another of other agencies, including NIST, has carried out some excellent work on tests on a significant number of commercial data acquisition and imaging tools and publicised reports on their operation. For the analysis and reporting phases of an investigation, the main tools in use are also, for the most part, commercially developed, and while there is de-facto acceptance of their capabilities, there is increasing concern with regard to their veracity. In a number of recent research publications, significant differences have been noted in the output of these tools, both from version to version of the tool and in comparison to the output of other tools. As these tools are commercially developed and have been well marketed and accepted as de-facto standard tools in the community, there has not been the any level of independent testing of their functionality. The practitioners have no visibility of whether it has been subjected to peer review, whether it can be and has been tested and whether there is a known or potential rate of error that would be acceptable. For the open source tools, some of the same issues are also true, although, potentially, the access to the source code would allow for experimentation and testing and the ability to determine error rates.

The accepted practice to validate the evidence that is to be presented is to use the dual tool approach, where two separate tools are used to confirm that the evidence is accurate. Unfortunately, this approach has a number of issues. Without knowing the algorithms that have been used in the tools that are being used, there is no way to ascertain that they are not using the same algorithm and are, in effect, self-validating. The other, more pragmatic issue is that of resources. To use two tools for each task would double the cost and also the workload of practitioners who already cannot deal with the workloads caused by the other issues detailed above.

According to Statista.com, 364.59 million Hard Disk Drives (HDDs) shipped globally in the first three quarters of 2015, and a figure of 416.7 million HDDs and 153.8 million Solid State Drives (SSDs) was projected for the whole of 2015. The average size of the Seagate HDDs is now over one terabyte. Based on these statistics, we can assume that a typical case would require Law Enforcement Agency (LEA) Officers to collect, on average, more than 1TB of data (including CDs, DVDs, internal and external HDDs/SSDs) for each case. The automated procedures that can be used to assist in the processing of this data, such as file signature analysis and hash analysis, are employed. Apropos, a large amount of data has to be manually analysed. Even before the analysis stage, there is a lot of work to be undertaken. Forensically wiping one Samsung HD105SI 1TB drive, using a tableau TD2u, was achieving an average of a 6.6GB/min transfer rate and a projected turnaround time of 2h 30 minutes. Furthermore, in a recent disk study the authors performed, a large number of hard disks were acquired and forensically analysed. The average acquisition transfer rate that was achieved was 2.76GB/min. This translates on an average time investigators would need to spend in the acquisition phase of at least 6 hours per disk.

After the acquisition of the devices, a forensic analyst will get to the analysis phase, where, depending on the case, they will perform any/all of the following activities:

- Disk geometry analysis (number, size and type of partitions (deleted or not))
- Time-zone analysis
- Operating System analysis
- Hash analysis
- File signature analysis
- Registry analysis
- Compound file analysis

- Log file analysis
- Internet artefacts analysis
- Email analysis

Following the above, more specific analytical steps will have to be performed (the list is not meant to be comprehensive):

- Deleted files recovery
- Identification of USB devices that were ever connected and when they were connected
- Identification of files and folders that have been exfiltrated
- CD/DVDS that may have been burned
- Websites visited and by which user account
- Lists of recently used programs, the files they have accessed, and when they have done so
- Programs that have been installed and uninstalled
- Attempts at data destruction/hiding
- Program settings that can deduce knowledge of an act or technology
- What programs start when the computer starts and any related DLLs, cross-examining findings for the identification of malware footprints
- How many times a program has ever been run and by which user account
- Wi-Fi connection points that have been accessed and when
- Hidden email and other internet accounts
- Identify and analyse photos and deduce the geographic location of where photos were taken
- What particular user performed a task (related to the above activities or to case specific activities)

Nowadays, most of the above analytical tasks have been automated. Still, depending on the datasets used, the analysis phase will take an average of two days per disk to complete. This translates in two days per disk before the forensic analyst will be able to start the manual analytical activities, the file indexing and any case-specific raw searches. It also translates in two days that physical computing resources will have to be locked down and assigned to the execution of the aforementioned tasks.

5. Potential solutions

The constant introduction and development of new technologies and their adoption in all environments means that frameworks, procedures and tools need to be constantly reviewed and developed to meet the environment in which they are required to work.

Currently, ISO 17025:2017 (General requirements for the competence of testing and calibration laboratories) is being widely used to standardise the policies, processes and procedures within digital forensic laboratories. In reality, while there is logic in the use of this standard, it is not fit for purpose. As the title suggests it is for testing and calibration laboratories and was not developed with the digital forensic environment in mind. Consideration should be given to developing a specific standard to meet the current and developing environment of digital forensics.

While it is recognised that the testing of analysis and reporting tools, particularly in a rapidly changing technological environment where new versions of tools are being developed on a regular basis is both expensive and time consuming, an international effort should be undertaken to fulfil this requirement. The work that the NIJ and NIST has undertaken in the area of digital forensics is of huge value, but does not currently go far enough. One current initiative that may address some of the issues is the Cyber-investigation Analysis Standard Expression (CASE). This is a community-developed evolving standard, which is aimed at serving the needs of the widest possible range of cyber-investigation domains, including digital forensic science, incident response, counter-terrorism, criminal justice, forensic intelligence and situational awareness. The underlying motivation for this initiative is that of interoperability in the exchange of cyber-investigation information between tools and organizations. CASE aligns with and extends the Unified Cyber Ontology (UCO) which is intended to support information integration and cyber situational awareness in cybersecurity systems.

The development of ISO/IEC 27037:2012 —Guidelines for identification, collection, acquisition and preservation of digital evidence, addresses the need for a stand for these phases of an investigation, but does not address the issues with the tools that are used and later phases of an investigation.

In support of CASE and UCO, we need to manage the paradox discussed in the previous section and the risks that it introduces. As with any risks, we can accept, we can mitigate, we can insure against or we can avoid completely. High frequency and high impact risks must be avoided. Low frequency low impact risks may be accepted. Low frequency high impact risks and high frequency low impact risks should be mitigated by procedural and technical solutions underlined by intelligence operations principles.

Paraphrasing Clausewitz, by intelligence we mean any sort of information about the potential suspects and their operational environment (linked to actus-reus and mens-rea).

Today, investigators need to have forensic intelligence[18-19], even for the simplest and most trivial computer-related crime, that can lead to forensic evidence which, when combined, can lead to a strong supporting case for a prosecution. Such intelligence can be used either in a pro-active or in a re-active manner. As a concept, this is not new. It was first introduced and discussed a number of decades ago[20-21]. For example, in the UK, ENDORSE (National Crime Agency 2015) is a nation-wide forensic and law enforcement initiative to collect and analyse information from drug seizures made in the UK. Apropos, the use case for ENDORSE is limited to a specific problem and a specific crime type within one national jurisdiction. Furthermore, computer-related criminal activities can be seen as a very complex problem, combining different types of traditional criminal activities with different and innovative technologies for transcending jurisdictional boundaries.

The procedural requirements for a modern digital forensic framework aligned with CASE and UCO, addressing the discussed paradox and the issues introduced by the modern information environment are:

- The Officer In Charge (OIC) must be enabled to identify physical and logical boundaries (internal and external) that are within the scope of the investigation;
- The OIC must be enabled to identify assets within the scope of the investigation;
- The OIC must be enabled to identify, specify and direct the collection of specific types of information;

- The investigative team (including relevant representatives from the environment under investigation) must be enabled to clearly communicate the requirements (priorities and essential elements of information);
- The OIC must be enabled to identify systems and processes that will be used in the collection phase as these may be organisation or technology specific;
- The OIC must be enabled to develop an operational collection plan with specific disciplines (HUMINT, SIGINT, OSINT) and methods for the intelligence based collection of the evidence.

Additionally, any solution must not be disruptive to business and must be seen as a catalyst in ensuring business continuity. Only then businesses may fully engage and allow for a truly integrated and complete approach in the collection and analysis of data. The solution must also be modular, portable, extensible and scalable. It must be complementary to SIEM strategies and make use of NOC and SOC technologies. More importantly, a viable solution must be integrated into Risk Operations Centres (ROC). Due to the intelligence-based nature of the solution (see requirements above) it is not feasible for Law Enforcement Agencies (LEAs) to be in charge of the operational part of the collection activities. Instead we argue that LEAs should only be responsible for the processing and analysis phases (see following figure).

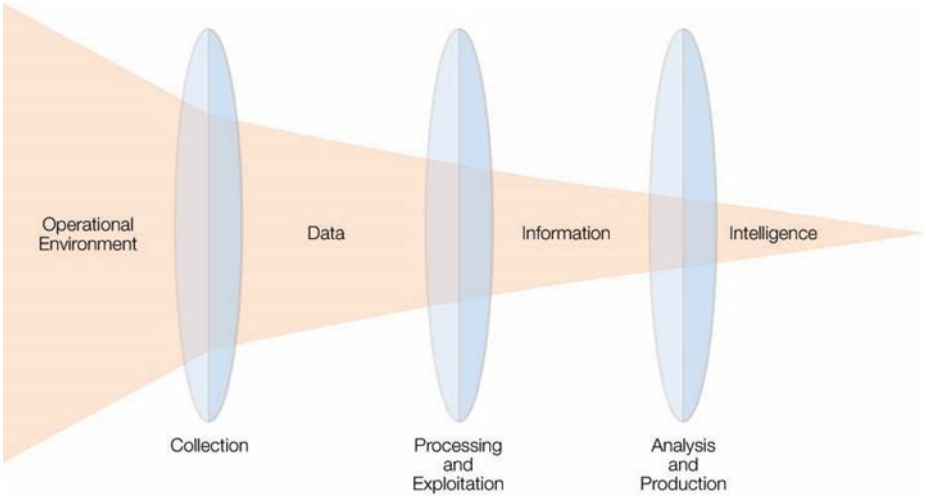

Figure 1. Relationship of data, information and intelligence [22]

5. Conclusions

While academic research is very good at developing frameworks and methodologies for digital forensic processes, it does not have the resources (or the remit) to test tools. There are more than 20 frameworks and methodologies that have been proposed over the last two decades to try and address the developing issues but, while essential, they can cause confusion as they add to the uncertainty and do not present a standardised approach. There is a need for a purpose developed digital forensic standard that will address current issues and is designed to meet the future challenges that the changes in technology will bring to enable scientific rigour to be applied to the processes.

There is a need to develop processes and procedures that will facilitate the integration of law enforcement and corporate resources at an operational level to support investigations. The reality is that LEAs will increasingly have to rely on other organisations to capture data from large data stores which may be outside of their jurisdiction and which may be using operating systems and

applications that are outside their knowledge area and expertise, but need to be able to guide these resources to achieve the highest levels of scientific rigour in the collection phase.

There is a need for education and additional training of the management of digital forensics resources to ensure that they have the overview of the issues and potential resources and can manage an intelligence led approach.

Given the characteristics of the modern information environment and the shortfalls of the current digital forensic methodologies, we should establish new procedural boundaries (supported by relevant legislation) spanning across the corporate and policing sectors. We should also fully integrate the use of intelligence into digital forensics and make use of new and emerging technologies throughout the TCP/IP stack.

References

[1] US DoD, "Joint Publication 3-13", Information Operations, 2012, Available: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.

[2] ACPO, "Good Practice Guide for Digital Evidence", Version 5, March 2012, Available: http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf.

[3] SWGDE, "SWGDE Best Practices for Digital Evidence Collection", Version 1, 2018, Available: https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Digital%20Evidence%20Collection

[4] SWGDE, "SWGDE Best Practices for Computer Forensic Examination", Version 1, 2018, Available: https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Computer%20Forensic%20Examination.

[5] Marberry and Craiger, "Factors affecting one way hashing of CD-R Media", Chapter 10, *Advances in Digital Forensics III*, IFIP International Conference on Digital Forensics, 2007.

[6] Newsham et al., "Breaking Forensics Software: Weaknesses in Critical Evidence Collection", 2007, Available: https://www.nccgroup.trust/globalassets/our-research/us/whitepapers/isec-breaking_forensics_software-paper.v1_1.bh2007.pdf.

[7] Dimpe P. M. and Kogeda O.P., "Impact of Using Unreliable Digital Forensic Tools", *Proceedings of the World Congress on Engineering and Computer Science*, Vol. I, 2017, Available: http://www.iaeng.org/publication/WCECS2017/*WCECS2017*_pp118-125.pdf.

[8] NIST, "A Framework for Harmonizing Forensic Science Practices and Digital/Multimedia Evidence", 2018, Available: https://www.nist.gov/news-events/news/2018/01/framework-harmonizing-forensic-science-practices-and-digitalmultimedia.

[9] Bannister A., "Hijack of nearly 1.5m surveillance cameras a wake-up call for security industry", *Ifsecglobal*, 2018, Available: https://www.ifsecglobal.com/installer-zone/hijack-surveillance-cameras-wake-up-call-security-industry/.

[10] Froehlich, A., "8 IoT Operating Systems Powering The Future", Information Week, Available: https://www.informationweek.com/iot/8-iot-operating-systems-powering-the-future/d/d-id/1324464.

[11] Biggs, S. and Vidalis, S., "Cloud Computing: The impact on digital forensic investigations", *Proceedings of the International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 1-6, 2009.

[12] Hay et al., "Storm Clouds Rising: Security Challenges for IaaS Cloud Computing", 2011, Available: http://nob.cs.ucdavis.edu/bishop/papers/2011-hicss-1/iaas.pdf.

[13] Birk and Wegener, "Technical Issues of Forensic Investigations in Cloud Computing Environments", 2011, Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6159124.

[14] Guo et al., "Forensic investigations in cloud environments", *Proceedings of the 2012 International Conference on Computer Science and Information Processing (CSIP)*, pp. 248-251, 2012.

[15] Reilly et al., "Cloud computing: pros and cons for computer forensic investigations", *International Journal of Multimedia Image Process (IJMIP)*, 1 (2011), pp. 26-34.

[16] Wolthusen, S.D., "Overcast: Forensic Discovery in Cloud Environments", 2009, Available: https://ieeexplore.ieee.org/abstract/document/5277835.

[17] Catteddu and Hogben, "Cloud Computing Risk Assessment", ENISA, 2009, Available: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment.

[18] Ribaux O., Girod A., Walsh S. J., Margot P., Mizrahi S. and Clivaz V, "Forensic intelligence and crime analysis", *Law, Probability and Risk*, Volume 2, issue 1, pp. 47-60, 2003.

[19] Legrand, T., and Vogel, L., "Forensic Intelligence", 2012, Available: https://www.academia.edu/1519407/Forensic_Intelligence.

[20] Birkett, J. (1989) "Scientific scene linking", *Journal of the Forensic Science Society*, volume 29, Issue 4, pp 271-284.

[21] Ribaux O. and Margot P., "Inference structures for crime analysis and intelligence: The example of burglary using forensic science data", *Forensic Science International*, 100(3), pp. 193-210, 1999, Available: https://www.sciencedirect.com/science/article/pii/S0379073898002138?via%3Dihub.

[22] US DOD, "Joint Publication 2-0: Joint Intelligence", *Information Operations*, 2013, Available: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf.