# Risk Mitigation and Quality Assurance in Digital Forensic Investigations

**Niladri Sarkar**
Digital Investigation and forensic computing, University college Dublin
Email: niladri.sarkar@ucdconnect.ie

DOI: 10.29322/IJSRP.9.06.2019.p9022
http://dx.doi.org/10.29322/IJSRP.9.06.2019.p9022

***Abstract***: Digital forensics involves the application of tried and tested methodologies for the Acquisition, preservation, validation, identification, analysis, documentation, interpretation, and presentation of evidences from sources in digital form, which can later be used to replicate the events found to be illegal[1]. Acquisition, Preservation, Analysis are few of the most critical processes. The risk involved in these processes, the impact of the risk and standardisation followed to minimise risk are discussed in detail in this paper.

***Index Terms:*** Risk Mitigation, Digital forensics, Digital investigation

## INTRODUCTION

**Digital forensics** as defined by First Digital Forensic Research Workshop (DFRWS) in the paper 'A Road Map for Digital Forensic Research' is "The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal…."[2].

**Acquisition** can also be termed as Preparation or Extraction of data from suspicious digital devices obtained from the site related to the act. Forensic experts can receive a dick image of the data or the real copy, they ensure the integrity of the data is maintained and converts the requests made to them to sensible questions and decides on the tools to be used to answer these questions. **Preservation** of digital evidence involves efficient protocols to be involved to ensure that the integrity of the evidence is maintained throughout and the same can be proved whenever necessary. As defined by Landwehr, integrity is "assuring that digital information is not modified (either intentionally or accidentally) without proper authorization"[3]. The digital evidences has evolved from traditional ones and in the process it has maintained all the complexities it earlier had in traditional form and also has added additional ones of its own.[4] As digital evidences are rich and volatile it is necessary to protect or seal the original image in such a way that challenges due to volatility of the digital evidences are answered. Previous work in this field has shown how this can be achieved by following a theoretical model of the umbrella principle.[5] **Analysis** phase for the forensic expert is to connect the dots in order to identify and reconstruct the occurred scenario in such a way that it can answer all the queries expected form the client. The examiners are also expected to define the procedure followed to achieve the output and from where it was documented. As a result of which examiners make sure they record the findings in a suitable manner in support of their findings.
Organisation bring in Quality Management and Information Security Management System standardisations to make sure they minimise risk related to the investigation phases and improve quality of work. Well know Quality management standardisation is ISO 9004:2018, which guides to achieve sustainable success it also follows the quality management principles mentioned in ISO 9000:2015[6]. Along with this ISO/IEC 27000 family is also followed which assures to keep an organisation's information assets safe and secure. There are multiple standardisations in this family among which ISO/IEC 27001 is well known to satisfy the need of an Information Security Management System. [7]

[1] Collective work of all DFRWS attendees, 'A Road Map for Digital Forensic Research', < dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf > accessed on 28th Feb 2019
2 Collective work of all DFRWS attendees, 'A Road Map for Digital Forensic Research', < dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf > accessed on 28th Feb 2019
[3] Landwehr CE. Computer security. Int J Inf Secur. 2001;1(1):3–13.

[4] Shahzad Saleem, Oliver Popov, Ibrahim Bagilli, 'Extended Abstract Digital Forensics Model with Preservation and Protection as Umbrella Principles' 2014, Procedia Computer Science Vol. 35, page 812-821.
[5] Shahzad Saleem, Oliver Popov, Ibrahim Bagilli, Preserving the integrity of digital evidence as an umbrella activity ,'Extended Abstract Digital Forensics Model with Preservation and Protection as Umbrella Principles' 2014, Procedia Computer Science Vol. 35, page 812-821.
[6] ISO 9004:2018, ISO <https://www.iso.org/standard/70397.html> accessed on 28th Feb 2019
[7] ISO/IEC 27000 family - Information security management systems, ISO,<https://www.iso.org/isoiec-27001-information-security.html> accessed on 28th Fed 2019

Digital Evidences

Data from a digital device, an internal or WAN network, wireless platforms and from different types of storage devices should be collected in a manner that it can be admissible as an evidence in a court.

Common types of **Digital Evidences** are

a. **Persistent:** This form of evidences are stored in local or remote hard drives and are saved and stored even when the digital device is in powered off state.
b. **Volatile:** They are information in volatile memory of a system for example in RAM of a device, which has potential risk to get lost when the system is powered off or can get replaced if the evidence is not collected on the correct time.
c. **Network:** These data are collected from gateway devices or network devices like a firewall or router or proxy by running debug commands and usually saved in .pcap format for further analysis. Most of the devices automatically saves system logs and network traffic to a syslog server or on some similar platforms so that it can later be used if in case required.

Risks involved and recommendations

If a digital investigation is performed badly without following the standards the evidence has a chance to stand inadmissible in front of the court of law. Hence, it is very important to perform risk analysis at an initial stage and proceed further.
The risks that are involved for the Acquisition and Preservation phase can be broadly divided into two groups:

a. Integrity risks.
b. Legal risks.

**Integrity risks:** It can be defined as loss of a portion of an evidence or the entire evidence in the process of collection of data from the device by the application of different technology on the evidence. The challenges that can result in integrity risk and recommendations to avoid them are mentioned below.

1. There is always a risk of altering the evidence on the disk while investigating on it by application of different tools by an investigator.
   *Recommendation*: A copy of the disk image should be used for investigation in order to make sure the original image is not tampered during the process. It is also necessary to maintain hash values of the image to ensure integrity of the image.
2. While doing a live data collection, we tend to run user and Kernel based tools in the end system, which results in creating at least one new process in the target machine, which may result in losing an interesting evidence in volatile form. Also, by creating a new process the OS allocates memory to the new process which may also overwrite the data in SWAP file system.
   *Recommendation:* It is advised to make a copy of the RAM or volatile memory first and then proceed with the live data collection on the system.[8] One can also make a note of the services and processes running on the system before and after running the forensic tool.
3. Often signs of intuition plays an important role during live data collection, there could be signs that the part of the data on the memory are created by the used acquisition tool resulting in untrusted data.
   *Recommendation:* It is very useful to keep a note of such instances, further in later phases it may come handy. An investigator may then decide whether to use the data to yield an output of follow a different approach.
4. The tolls or scripts used to capture the network traffic are not always successful to retrain all the packets that are captured by the Kernel. There is no question of retransmission even in case of a TCP communication as the network sniffers never participate in the communication. Well known tools used for this process are tcpdump, NetWitness and Snort, they usually read the traffic from buffered memory by libpcap.
   *Recommendation:* Before dumping the unread packets by the sniffers libpcap keeps a record to the percentage of the packets that are not read by the tool. Although recovering the data is not possible, it is essential for an investigator to check the percentage of the data that was not captured during the process, this gives the accuracy of the data.
5. Network monitoring tools or programs has the feature of enabling filters, in doing so they capture only interesting traffic with respect to the filter applied. If the filters are not correct we tend to capture incorrect data.
   *Recommendation:* An investigator should have a look at the filters applied in the first place and document the same. If the traffic is not bulky, it is recommended to capture the entire traffic and later analyse the same using log analyser tools.

**Legal risks :** The organisations or individuals who fail to comply with the regulatory standards risk themselves in loosing reputation and business in future. They may be liable to pay a heavy penalty or sometimes face legal actions depending on the case scenario. Examples with recommendations given below:

[8] SANS Digital Forensics and Incident Response Blog,SANS DFIR <https://digital-forensics.sans.org/blog/2009/09/12/best-practices-in-digital-evidence-collection/> accessed on 1 March 2019

1. Before intercepting an employ's email, an investigator must get the company's policy checked which allows him to do a surveillance of the employ's emails, else it may result in privacy breach.
2. Violation of any of the company's statues during investigation may be a punishable offence leading to penalty or imprisonment, it is recommended to consult a legal counsel if in case any doubt arises.
3. It can be taken as an example when HP tried to probe into CNET's journalist to find out the source of her information. They in this case used a web bug. This has to be kept in mind that the use of such technologies are not always legal and has to be confirmed by a legal counsel first.[9][10]

[9] Dean Takahashi,HP scandal sheds light on electronic tracking technologies <https://www.seattletimes.com/business/hp-scandal-sheds-light-on-electronic-tracking-technologies/> accessed on 1st March 2019
[10] Risk Analysis for Evidence Collection <https://www.cs.nmt.edu/~df/StudentPapers/Thakore%20Risk%20Analysis%20for%20Evidence%20Collection.pdf> accessed on 1st March 2019