MAR 2021 | VOL II ISSUE 1

FORENSIC NEWSLETTER

Alliance IFA Sdn. Bhd.
Email Newsletter

Unlike traditional accounting firms, Alliance IFA works purely in forensic space!

Our Services:

- **Investigative and Forensic Accounting**
- **Damage Quantification**
- **Fraud Risk Management**
- **Cyber Crime Investigation**
- **Digital Forensics**
- **Digital Analytics**

To know more about us,
visit https://www.allianceifa.com.my
Call us at +603 7710 9946

CYBERCRIME INVESTIGATION – LEGAL AND ETHICAL OBLIGATION [PART II]

by Akash Rosen & Prabhat Kumar

In our last edition issued during January 2021, we discussed about two phases of any cyber crime or computer forensic investigation either by a private investigator or by an appropriate authority.

Let us understand 3 more stages i.e. Acquisition, Preservation, Analysis & Reporting. In the final part, we will discuss about admissibility of digital evidence and its assessment.

iii) Acquisition:

As we know, digital evidence is highly fragile and can get altered by not following the right procedure while reviewing and analyzing. Hence it must be obtained for review as a copy of the original, without compromising the integrity of the original stored data. Obtaining data without altering is possible by creating a duplicate copy of the data from the device where it is stored by using an imaging technique.

Once imaged and original is preserved the imaged copy can be used for various analytical purposes. One can easily access various files stored.

To copy the data through imaging the original data is possible because the computer forensic technician uses a device called write blocker. Write blocker prevents the alteration of data during copying process and as a result the hash value of the entire data which have been imaged from the device , remains the same. Through this technique one can be assured about the content which has been imaged for duplication is the same as the original. Therefore, it is paramount that the person who is processing the data for imaging is competent enough to carry such exercise and when necessary can be requested to give evidence in Court with proper explanations of the entire procedure.

To confirm, whether the duplicate is an exact copy of the original, a hash value is calculated using mathematical computations. For this, a cryptographic hash function is used to produce a hash value. If the hash value for the original and copy match, then the contents of the duplicate are the exact same as the original. However, there are certain circumstances where a person finds it necessary to access original data [i.e., during live acquisitions]. In such a situation, the person [accessing this data] must be competent (Trained/ qualified and experienced Computer forensic expert) to do so and be able to give evidence explaining the relevance and the implications of his/her actions.

Once the device is properly acquired, examination process begins with the help of appropriate digital forensic tools and set methods to uncover digital data. As mentioned above, there are number of tools available and an examiner can use any of them depending on the type of device which is to be examined such as Encase, FTK, and X-Ways Forensics etc.

iv) Preservation:

During the process of data acquisition for evidentiary purposes, it is vital to maintain the chain of custody from the time of acquisition of the physical digital evidence till it is submitted as evidence in the Court. The process through which the chain of custody is maintained must have verifiable records to reflect as who collected the evidence, where and how the evidence was collected, which individuals took possession of the evidence, and when they took possession of it. Meticulous documentation at each stage of the digital forensics process is essential to ensuring that evidence is admissible in court.

One must keep in mind that there is no universally accepted and adopted digital forensics process. Every country has its own investigations and forensics protocols. However, there are international standards and good practices. These practices can be adopted by countries while dealing with cybercrime investigations and digital forensics.

v) Analysis:

The purpose of the analysis is to confirm the significance and probative value of evidence. The basic objective of analysis is to correlate evidence if possible to reach to a conclusion. During the examination, the investigator try to confirm whether the evidence under examination has the tendency to confirm the existence of certain fact/s which is the center of allegation/ dispute. During this process generally examiner develops various hypothesis in the given set of situation and try to examine the relevance of such evidence which has been collected through imaging. For example, copy of the email or memo exchanged between two persons, copy of a letter in draft form etc.

vi) Reporting:

It is one of the most important aspects of the whole process through which it is explained by the expert through a detailed description about the steps taken by him/ her throughout the digital forensics process. It does contain the digital evidence uncovered, number of files extracted and filtered, list of key word used to search the file and the conclusions reached based on the results of the digital forensics process and the evidence revealed.

vii) Conclusion:

Computer forensics is a vast subject and one can master over various aspects only after getting involved in the acquisition and preservation process again and again. We have explained only few of the very fundamental aspects for some basic understanding to deal with the situations. Some of these standards and best practices described above are to understand the validity and reliability of digital forensics results.

The digital forensics results are considered reliable when, same results are obtained on different occasions using the same data, tools, and techniques. Further results are considered reproducible when the same digital forensics results are obtained using the same test items, but different equipment, laboratories, and operators.

****