JAN 2021 | VOL 1 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

by Akash Rosen & Prabhat Kumar

The Cybercrime investigation and digital forensics professionals are required to investigate cyber crime cases legally and ethically. They interpret digital evidence to identify whether the investigation is proactive or reactive. It is proactive when the investigation is in response to intelligence and reactive when the investigation takes place in response to the identification or reporting of cyber crime.

The legal obligations are prescribed by national and international law whereas ethical obligations are self-imposed and/or prescribed by respective government agencies and professional organizations. The code of ethics, which often includes digital forensics professionals and cybercrime investigations, provides a guide to as what individuals should always do and what they should never do under any circumstances. For example, the International Society of Forensic Computer Examiners has a Code of Ethics for its members to abide by to ensure that the standards are being met to make the process accurate and trustworthy.

As a result, the members are required to follow legal orders and conduct a comprehensive examination of the evidence according to the existing laws of that country, standards, procedures, and guidelines. They must prohibit themselves from certain acts such as withholding evidence, engaging in biased analysis or biased reporting of evidence and misrepresenting qualifications. Important phases in any cybercrime or computer forensic investigation either by a private investigator or by the appropriate authority may be mentioned as follows:

i) Identification
ii) Collection
iii) Acquisition
iv) Preservation
v) Analysis & reporting
vi) Admissibility and
vii) Evidence assessment/consideration

i) Identification:

This is the first phase. Based on preliminary information obtained about who was involved, when the crime occurred, location and the way it was committed. Investigators identify the gadget and the system. Having answers to these questions will provide guidance on how to proceed with the case to a cybercrime investigator.

ii) Collection:

it is important to mention that the crime scene is not limited to the physical location of the digital device but may include devices that potentially hold digital evidence including systems and servers. It is important for the first responder and or investigator to identify and protect the crime scene from contamination and preserve it by isolating the users of all digital devices found at the crime scene. If possible, hold them in an isolated room. Before the evidence is collected, the crime scene is documented as it is required throughout the entire investigation process. This documentation should include detailed information about the digital devices along with the operational state of device and physical characteristics such as the make, model, serial number, connections, etc. The actual collection of the evidence involves the preservation of volatile evidence and the powering down of digital devices. The collection procedure is dictated depending on the state of operation of the digital devices that have been encountered by the investigator. For example, if a device is a computer and it is on, it is volatile evidence (e.g., temporary files, register, cache, and network status and connections, to name a few) and is preserved before the power is down and then collect it. If the device is off, then it remains off and is collected.

………to be continued in Volume II in our next issue.