Bibliography details

Name of the Serial/Publication: Veritas

Volume No.: 1

Issue No.: 1

Month & Year of publication: August 2021

Page numbers: Feature Articles (67-69)

Title of Article: Facts that you should know about Digital Forensics

Contributor (s)

1. Ms. Elizabeth Deepika Ponnuraj

FACTS THAT YOU SHOULD KNOW ABOUT DIGITAL FORENSICS

Ms. Elizabeth Deepika Ponnuraj

Digital forensics investigation is one of the emerging disciplines developed from the branch of Forensic Science. However, despite the remarkable development in the digital world and the increase in cybersecurity attacks through digital tools and techniques, most forensic scientists lack the appropriate knowledge to perform investigations under digital forensics but it is necessary that every organization with a working computer system needs the services of a qualified digital forensics analyst.

Moreover, owing to the increment of cybercrimes nowadays, digital forensics is also applied by law enforcement agencies and other corporate organizations like MNCs across the globe.

The Concept of Digital Forensics:

Digital forensics covers the recovery and investigation of materials detected in digital devices which are usually concerning computer crimes. In simple terms, it is the process of identifying, extracting, preserving and documenting digital evidence through digital tools which can be used in the court of law.

Similarly, it also provides forensic experts with the greatest strategies and technologies to deal with complicated computer-based crimes. It also has several applications in its field but the most widespread use is to disprove or prove a fact in the court of law.

It is also applied in the corporate sector for computer hacking investigations and internal corporate investigations. Here, the digital forensics analysts investigate the environment and degree of an unlaw-

ful network intrusion or system hack. The rapidly expanding field of digital forensics includes numerous branches related to databases, malware, firewalls, mobile devices, cloud and network forensics.

Use of Digital Forensics in an Investigation:

For your digital evidence to be admissible in the court of law, it is necessary that the materials gathered are handled in a certain manner so that the evidence may not be tampered with. Most people think that the scope of digital forensics and incident response are only applicable for organizations that function in the most security-conscious fields.

However, it is not true because awareness about the digital world and of the best cybersecurity practices is always beneficial. Regardless of the type or size of your organization, it is always important that your IT security team or those responsible for handling your security always follow an informed, structured, and effective process when a security incident happens.

The general steps that are involved in an investigation of digital forensics are:

1. Planning -

The first phase of any successful endeavour is planning. In the digital world, where events occur quickly, you need to plan your approach. Pinpoint and prioritize your targets so you can obtain relevant and useful evidence. Make plans to follow every relevant and regulatory policy. To gather your evidence on time, you may miss out on some legal requirements which will render your evidence to be dismissible in the court of law. So always keep it legal.

2. Identification and Preservation -

The next step is to identify the evidence. Ensure that all the data gathered have not been tampered with. Don't work on the original copies, make duplicates so that the integrity of the original data is preserved. To be on the safer side, isolate and preserve the original copy. This involves stopping people from manipulating the evidence.

3. Analysis -

The next step is to analyse all the evidence, based on the timeframe of their occurrence. Since you are going to get your data from several sources, their timestamps may be different. By gathering your data based on their timeframes, you can build a comprehensive picture of events and pinpoint a fact supporting your evidence. You need to be systematic about your analysis. Make a hypothesis and run tests to support all your findings.

4. Documentation -

The next step is to generate a report on all the data that you have gathered to reconstruct the scene of crime. This report must be detailed, understandable, factual and must include only defensible data. Make sure that everything you captured is recorded just as they are, dated, and signed. Ensure that your report does not contain too much technical linguistics. This way, even non-technical people can understand your report.

5. Presentation -

The final step of any investigation is to present a report of your findings in the court of law. Your findings must be presented without any bias or partiality.

While your report summarizes your findings, you still need to ensure that you answer all the doubts addressed in the court of law diligently. In a more critical case, other certified forensic scientists can be called upon to verify your findings.

References:

- https://www.envistaforensics.com/experts/Daniel-Digital-Forensics-Expert-Raleigh