Digital Forensics Trends of 2020 and Beyond

The sector of Digital Forensics continues to grow along with the ever growing market at a compound annual growth rate of 14%. It is expected to grow from 4 billion USD in 2018 to 9 billion USD in revenues by 2022. The demand for cybersecurity and digital forensics is driven by stringent government norms and a booming IT market. Moreover, the rising use of the Internet of Things (IoT) devices expects an even higher requirement for digital forensics.

As the market continues to evolve and grow, the field of digital forensics is severely challenged by the growing demand for digital devices and various software and operating systems. Also, there is a rise in cyber-attacks and has challenged organizations and their business models by implementing Crime as a Service (CaaS).

The following are the key challenges in the field of digital forensics.

- High speed and volumes
- Explosion of complexity
- Development of standards
- Privacy-preserving investigations
- Legitimacy
- Rise of anti-forensics techniques

A multidisciplinary approach has to be implemented to anticipate the future of Digital Forensics for 2020 and beyond.

Cyber Forensics for Governments:

Cybersecurity and Forensics at the government level will be very challenging and intricate. Countries with intellectual and technological ownership will boast an advantage while other countries will be forced to work on open-source software and develop their cyber forensic tools. Need for sophisticated national security organizations will increase and governments will tend to use them for hunting cybercriminals and wage cyber warfare and propaganda. These organizations will have the responsibility to develop anti-forensics tools and methods to keep their data and assets safe.

Cybercrime Forensics for Corporates:

Information security standards such as ISO27001 and ITIL will be implemented in all organizations ranging from large to enterprise levels. It will be necessary for firms to have proper cybercrime investigation procedures and tools. Some of these companies will even own their cyber forensics wing for internal organizational operations. To date, some companies have controlled the forensics sector and are pioneers for new technology and innovation in this field. These companies supply tools to government agencies and train their officials. Due to strict laws and security clearances, most of the forensics companies will operate in their own country.

Cybercrime Forensics in Universities:

The slow and traditional approach of academic institutions compared to a faster speed of development and implementation of the market creates a huge void in students. Hence students prefer to get professional certifications more than traditional university education. This happens as the programs in the universities are not aligned with those of the fast-developing market needs. The education sector needs to bridge the gap between students and the IT sector by imparting better knowledge and hands-on training to students who grow and become better professionals in the industry.

Cybercrime forensics in Media:

Magazines, websites, blogs specializing in cybersecurity will be a driving force of the industry with the power to criticize, vote and promote products, solutions, and education. Companies with a higher budget for media and marketing will sell better than their competitors in this industry. A product or service campaign backed by a strong marketing and media relations team will guarantee a larger chunk of the market share. Independent websites and magazines will find it difficult to sustain is such cut-throat competition.

In the upcoming future, everything will be linked to cyberspace and IT, this move will force governments and companies to try new methods of data collection like data mining to preserve their interests. Privacy norms will be revised and suspicious activity will be detected at the carrier stage itself. Data mining will be used to identify suspicious people. All user information like contacts, social media, financial logs, user activity will be combined into massive databases and will be used to monitor suspicious behavior and frauds. This in turn will start a new chapter in the history of mankind.

An Executive Summary by
Saket Thombre