DIGITAL FORENSICS TRENDS 2020

Digital forensics process involves collection, preservation, analysis and presentation of evidence from digital sources. With the rise of challenges in the field of forensic investigations, problems that are more interesting are looming on the horizon for both victims and investigators. As computers become smaller, faster and cheaper, computers are increasingly being embedded inside other larger systems which allow information to be created, stored, processed, analyzed and communicated in ways that are unpredicted. Once we gathered digital evidence from monolithic, stand-alone mainframes whereas today we have PCs, supercomputers, distributed client-server networks, laptops and smart phones, and LANs and WANs to convey information across the world, each of which is a potential source of digital evidence. Evidences stored in a computer is not unique with regard to relevancy and materiality, but because it can be easily duplicated and modified, often without leaving any traces and is readily available to a miscreant using another computer half a world away and hence, should be constrained by evolving legal standards and constraints to defend privacy issues.

In general, privacy means allowing or disallowing access to information. The code of ethics requires the forensics professionals to maintain the privacy of the client. In the event of proper investigation of cases, depending on the sensitivity of the issue and the requirement of the result, the privacy of the client may need to be compromised.

But it is also possible the victim organization might lose out the trust over forensics team. Moreover, there are organizations where in any slight leakage of the issue may attract huge media attention resulting in endangering the reputation and finally the business of organization. In such situations, privacy rights and law enforcement's need to search and seize digital evidence during digital forensic belong together. It may also be possible that the forensics expert may not share the information with any third party but takes the advantage of the confidential information of the client himself, which is also a case of violation of right to privacy.

That is why, it is the policy maker's responsibility to see the impact of forensics in the broader context of business goals and make the hard decisions that trade off forensics capabilities with issues of privacy and, correspondingly, morale. Key strategies for digital forensics in order to

protect privacy are selective revelation, strong audit and rule processing technologies.

In the present situation, how to monitor digital forensics while keeping search information secret? How do we keep private information from being improperly disclosed in the name of forensics?

Law enforcement faced numerous significant challenges in developing and mastering the skills, tools and techniques of digital forensics. It is not easy in finding qualified forensics personnel, either in the private sector or government sector. This is due to the limitations placed to the civilian access on training programs. In law enforcement, difficulties arise due to structural and cultural factors in certain communities. Even though some cases were well trained, there are still limitations in achieving successful prosecution. It includes the lack of suitable equipment and facilities to process digital evidence and unfamiliarity of prosecutor with the issues surrounding the seizure and processing the evidence. Even with these skills, there is no guarantee that the investigator will able to find enough evidence.

CURRENT TRENDS IN DIGITAL FORENSIC

DATA BREACH INCIDENTS ARE INCREASING

More events, more forensics needed.

LACK OF PREPARATION FOR WHEN THINGS GO BAD

Rather than relying on technology, we need more skilled professionals.

LOSS OF FORENSIC EXPERTISE

Corporate-based forensic experts tend to flee to higher paying jobs with technology vendors and service providers.

CIVIL CASES INCREASING IN SOPHISTICATION

As lawyers learn more, cases become more complex. Lee talked about the burgeoning focus on meta data in legal cases.

TOO MUCH DATA

It's like LogRhythm, Log Logic, ArcSight, Nitro, and Q1 Labs present a ton of data to evaluate. The real challenge is host-based data, not network data.

MOBILE DATA FORENSICS

We need the ability to understand what's happening on iPhones, Droids, and Blackberries, not just Windows PCs.

VOLATILE DATA COLLECTION AND ANALYSIS

This is all about the collection of data residing in memory, which could make or break a case.

FUTURE OF DIGITAL FORENSICS

FACES SECURITY CHALLENGES IN FIGHTING BORDERLESS CYBER CRIME & DARK WEB TOOLS

Cybercrime has now become so extensive, underground suppliers are cropping up on the dark web offering easy access to the tools, programming frameworks, and services required to carry out cyberattacks.

Cybercriminals wreak havoc in a multitude of ways—identity theft, cyberbullying, data leakage, distributed denials of service, and malware attacks on medical devices and smart vehicles. They stand ready to bring businesses and governments to their knees.

Cyberattacks can have a significant socioeconomic impact on both global enterprises and individuals. Therefore, cybercriminals should be promptly identified, and high-quality evidences of the attacks should be made available in the courtroom.

CHALLENGES FOR DIGITAL FORENSICS

EXPLOTION OF COMPLEXIVITY

Evidence is no longer confined within a single host but, rather, is scattered among different physical or virtual locations, such as online social networks, cloud resources, and personal network–attached storage units. For this reason, more expertise, tools, and time are needed to completely and correctly reconstruct evidence. Partially automating some tasks has been highly criticized by the digital investigation community, because it could quickly deteriorate the quality of the investigation.

DEVELOPMENT OF STANDARDS

They add that investigations of cutting-edge cybercrimes might require processing information in a collaborative manner or using outsourced storage and computation. Therefore, a core step for the digital forensics community will be the development of proper standard formats and abstractions.

PRIVACY PRESERVING INVESTIGATIONS

Nowadays, people bring into cyberspace many aspects of their lives, primarily through online social networks or social media sites. Unfortunately, collecting information to reconstruct and locate an attack can severely violate users' privacy and is linked to other hurdles when cloud computing is involved.

LEGITIMICY

Modern infrastructures are becoming complex and virtualized, often shifting their complexity at the border or delegating some duties to third parties.

"An important challenge for modern digital forensics will be executing investigations legally, for instance, without violating laws in borderless scenarios."

RISE OF ANTIFORENSICS TECHNIQUES

Defensive measures encompass encryption, obfuscation, and cloaking techniques, including information hiding.

Cooperation among international jurisdictions notwithstanding, investigating cybercrime and collecting evidence is essential in building airtight cases for law enforcement. For that, security experts need the best tools to investigate.

"Digital forensics is fundamental to investigations performed in a reality that's often tightly coupled with its cyber extension. Modern digital societies are subject to cybercriminal activities and fraud leading to economic losses or hazards for individuals. Therefore, the new wave of forensics tools should be engineered to support heterogeneous investigations, preserve privacy, and offer scalability