Student Name

Professor Name

Course

Date

Current Challenges of Digital Forensic

New possibilities in digital forensic occur every day because the development of forensic science and technology progresses rapidly. However, these opportunities often present a way for malicious individuals to compromise the public order and certain individuals' and organizations' ability to perform their duties. This is mostly done to gain personal benefits such as valuable information or money. Nevertheless, digital forensic units and researchers are always searching for solutions and ways to prevent and solve computer-related crimes. In this paper, the current challenges of digital forensic – such as evidence detection and processing – will be analyzed. The second part of the paper describes the most recent researches performed in the field of digital forensic, their goals and results.

**Current Challenges**

Currently, digital forensic is facing some problematic issues that have a potential of changing the course of the current digital forensic science's development. Lillis et al. suggest five problems: complexity, diversity, consistency and correlation, volume, and unified time lining (2). The first challenge arises because of the necessity to reduce acquired data before analyzing it correctly. The issue of diversity – inability to properly analyze multiple evidence sources – is a direct result of the fact that the data collected from various devices grows in volumes every day. This occurs because of the expansion of devices' ability to store information, which is essentially the volume problem. The third problem occurs

because there is no automatized way to analyze evidence gathered from multiple sources that contain a lot of excessive information. Finally, the unified time lining is rather self-explanatory: there are different time zones, and various devices may include different references to them. This also includes timestamp interpretation possibilities and other time-related problems.

Dezfoli et al. notice that the current trend in technology development creates lots of diversity when it comes to collecting evidence (48). While early investigations required gathering the evidence from just one PC, now it takes to "dig" into mobile phones, laptops, networks, and so on. Moreover, the evidence stored in personal computers may not even be created on one particular PC. The problem, then, is to advocate for privacy issues properly. In addition, there are researches that tend to aim at some very particular topics. For example, Tahar et al. focus on “forensic challenges in the mobile cloud computing" (4). Cloud storages as a new type of data gathering sources provide both challenges and possibilities for forensic units.

Thus, a significant number of problems are presented to the investigators working in digital forensic units. Aside from the ones mentioned above, there are lots of problematic issues related to the need to collect high-quality evidence and methods of its collection. As it becomes apparent, this need is of utmost importance in the modern era, when evidence is easily duplicated – often without leaving any trace – and criminals are making this possible without even directly working with the device, on which the evidence is found.

Another important discussion is the nature of researches undertaken on the subject of digital forensic. Lately, a significant diversity in opinions has established. Some researchers believe that it is better to approach digital forensic from a practical standpoint, while others tend to suggest a more theoretical approach. This is

stipulated by the fact that providing digital security is often closely related to the organizations' or individuals' personal needs and mindset. More importantly, the leadership of some companies tends to perceive digital security as irrelevant, therefore creating some obstacles that would otherwise not prevent digital forensic units from carrying out their duties.

Thus, there is a great coverage on the nature of digital forensic investigations. Which crimes are to be considered computer-related? What individuals are identified as digital criminals? What malware and technology do they use? All of these questions trouble researchers that undertake theory-based researches. The practice-oriented studies describe means of protection, specifications of malware used by criminals and ways of eliminating possible threats and negating the damage done.

**Recent Researches**

More recent researches tend to focus mostly on practical sides of the question. For instance, Raut and Paikrao dedicate their research to investigate the current trends of visual cryptography and steganography (126). During their research, the authors came to a conclusion that these techniques are a valuable asset, when it comes to data reception. With the implementation of encryption, the inappropriate usage of sensitive data may be completely avoided.

Some researchers prefer to focus on the narrowest topics. These researches, however, provide valuable information on particular types of devices and how they must be interacted with to collect evidence. An example of that would be the research by Alyahya and Kausar, where authors provide guidelines to discover digital forensic artifacts on smartphones that are using Android OS (1036). The authors conclude that, although most of the data that remained on the device is lost most of the time, about 10% of images and videos may be recovered and the

percentage of other data is progressively bigger (1040). This may provide forensic units with crucial evidence to solve computer-related crimes.

Finally, Cheng et al. provide coverage of "a lightweight live memory forensic approach based on hardware virtualization" (1). The authors develop a tool that may be used in active forensic investigations. The challenge that arises with creation of this tool is essentially the need to implement it in the investigations. Although impossible for now, the tool will most likely be incorporated in digital investigations later.

**Conclusion**

Thus, digital forensic has a lot of current challenges and some of the most recent researches undertaken in this field of criminology prove that these challenges are slowly resolved. The researchers that are studying this problem are coming closer to solving each of the problematic issues. However, it is most likely that the problems will continue to appear as criminals will always try to find new ways of bypassing security and avoiding detection.

Works Cited

Alyahya, Tadani, and Firdous Kausar. “Snapchat Analysis to Discover Digital Forensic Artifacts on Android Smartphone.” *Procedia Computer Science*, vol. 109, no. 1, 2017, pp. 1035-1040.

Cheng, Yinxin, et al. “A Lightweight Live Memory Forensic Approach Based on Hardware Virtualization.” *Information Sciences*, vol. 379, no. 1, 2017, pp. 23-41.

Dezfoli, Farhood, et al. “Digital Forensic Trends and Future.” *International Journal of Cyber-Security and Digital Forensics*, vol. 2, no. 2, 2013, pp. 48-76.

Tahar, Kechadi, et al. “The State of the Art Forensic Techniques in Mobile Cloud Environment: A Survey, Challenges and Current Trends.” *International Journal of Digital Crime and Forensics*, vol. 7, no. 2, 2015, pp. 1-19.

Lillis, David, et al. “Current Challenges and Future Research Areas for Digital Forensic Investigation.” *The 11th ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016)*, edited by Marc Rogers et al., Daytona Beach, 2016, pp. 1-11. www.researchgate.net/publication/292996779_Current_Challenges_and_Future_Research_Areas_for_Digital_Forensic_Investigation. Accessed 7 Jul. 2017.

Raut, Radhika, and Prashant L Paikrao. “A Review on Visual Cryptography and Steganography.” *International Journal of Advanced Electronics and Communication Systems*, vol. 6, no. 2, 2017, pp. 125-129.