





#### IV. CONCLUSION

Technology is a boon or bane? Well, that has been a topic of debate for decades now. While several tools and technologies have enabled us to incorporate security in our systems, many malicious activists also use these technologies to perform various cyber-attacks. They try to perform these malicious activities in such a way that these actions go untraceable. They do so using different tools. In this paper, we discussed about Anti-Forensics and its techniques. We specifically talked about anti forensic techniques for network layer. We explained a few techniques for network anti-forensics and corresponding tools and made a comparison which may help our readers in understanding these techniques.

#### REFERENCES

- [1] Chandran, R., & Yan, W. Q. (2013). A Comprehensive Survey of Antiforensics for Network Security. *Managing Trust in Cyberspace*, 419.
- [2] Kessler, Gary C. "Anti-forensics and the digital investigator." In *Australian Digital Forensics Conference*, p. 1. 2007.
- [3] Chandran, R., & Yan, W. Q. (2014). Attack Graph Analysis for Network Anti-Forensics. *International Journal of Digital Crime and Forensics (IJDCF)*, 6(1), 28-50.
- [4] Garfinkel, S. (2007, March). Anti-forensics: Techniques, detection and countermeasures. In *2nd International Conference on i-Warfare and Security* (p. 77).
- [5] SecTools.Org: Top 125 Network Security Tools [8<sup>th</sup> Dec, 2015]
- [6] Wang, Meijuan, et al. "Countering anti-forensics to wavelet-based compression." *Image Processing (ICIP), 2014 IEEE International Conference on*. IEEE, 2014.
- [7] Spoofing Attack: IP, DNS & ARP. [8<sup>th</sup> Dec, 2015]
- [8] Harris, R. (2006). Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. *digital investigation*, 3, 44-49.
- [9] Lubacz, Józef, Wojciech Mazurczyk, and Krzysztof Szczypiorski. "Principles and overview of network steganography." *arXiv preprint arXiv:1207.0917* (2012).
- [10] Chen, W., & Yeung, D. Y. (2006, April). Defending against TCP SYN flooding attacks under different types of IP spoofing. In *Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, 2006. ICN/ICONS/MCL 2006. International Conference on* (pp. 38-38). IEEE.
- [11] Lomas, M. (1993, December). Encrypting network traffic. In *Fast Software Encryption* (pp. 64-70). Springer Berlin Heidelberg.