 **[Hacking and Crime](https://edge.apus.edu/portal/site/424869/tool/cf659c17-3e9c-4fff-9b08-6bf9318f8371/discussionForum/message/dfViewThread" \o " Hacking and Crime )**

**Gabrielle Nesburg(Mar 18, 2020 10:51 PM)**- Read by: 3

[[https://edge.apus.edu/messageforums-tool/images/trans.gif?sakai.tool.placement.id=cf659c17-3e9c-4fff-9b08-6bf9318f8371](javascript:void(0);)Mark as Read](javascript:void(0);)[[Reply to This Message](https://edge.apus.edu/portal/site/424869/tool/cf659c17-3e9c-4fff-9b08-6bf9318f8371/discussionForum/message/dfViewThread) Reply](https://edge.apus.edu/portal/site/424869/tool/cf659c17-3e9c-4fff-9b08-6bf9318f8371/discussionForum/message/dfViewThread)

*1. Why do many in the computer community oppose the use of "hacker" to describe cybercriminals? Can a meaningful distinction be drawn between hacking and cracking? What kind of hacking can be justified on either legal or ethical grounds?*

The technical definition of hacking does not include any malintent at all, rather it is simply discovering an alternative use of computer hardware or software in order to find a faster or simpler solution to a problem (Hall & Watson 2016, 8). The word has several origins, but is most commonly thought to have originated in the 1950s as a term for a shortcut or technique used to bypass the original operation of a system (Hall & Watson 2016, 9). It was not until the late 1980s when the term took on a malicious meaning as individuals began to bypass security protocols for personal gain (Hall & Watson 2016, 10). Hacking can now be defined as the, “unauthorized use of computer and network resources” (Negi 2011, 1).

Cracking can actually be aligned directly with software. The term cracking stems from the idea that one will “crack” software in order to make it free, distribute it, and use it for personal gain (Negi 2011, 1). Often times, a person will remove or disable features such as copy protection, trial/demo version, serial number, hardware key, date checks, or CD checks (Negi 2011, 1).

There are two types of hacking that can be justified on ethical grounds. The first type is White Hat hacking (Hall & Watson 2016, 11). These individuals only hack systems in order to discover vulnerabilities (Hall & Watson 2016, 11). One discovered, they push to close those exploitable gaps by releasing updates and patches to the public (Hall & Watson 2016, 11). Though less ethical, Grey Hat hacks can also fall into ethical hacking (Hall & Watson 2016, 11). They may actually use illegal means to exploit a system vulnerability, but they will share their findings with the company or individual in order to improve the end user’s security posture (Hall & Watson 2016, 11).

*2. What implications does the conviction of the four cofounders of the Pirate Bay Web site in 2009 have for international attempts to prosecute intellectual property crimes globally? Should the four men also have been required to stand trial in all of the countries in which copyrighted material had been downloaded from their Web site? Will the outcome of the Pirate Bay trial likely deter entrepreneurs, worldwide, from setting up future P2P sites that allow the illicit file sharing of copyrighted material?  What is your opinion of the case?*

The interesting piece regarding The Pirate Bay (TPB) case is that TPB was only prosecuted in Swedish court, despite the fact that 17 different music and media corporations were involved in the suit (Kiss 2009, 1). The prosecutors won their case against TPB individuals, however no follow on suits were prosecuted against the individuals. This seemingly indicates that where the base of operations resides for a site such as TPB is the one and only place that a suit will take place. With the way the Internet of Things (IoT) is now, from a personal opinion standpoint, it makes sense to me that they might only stand trial where the base of operations is at. As long as all parties, such as the corporations, that are affected are part of the suit, then it makes sense to prosecute one, rather than multiple times with multiple different sets of laws. However, this can work against a rightful verdict as some laws might be stricter than others. It is unlikely that we will see a decrease in Point to Point (P2P) sharing websites. Ultimately, large scale corporations do not have the infrastructure necessary to monitor and prosecute all individuals that participate in P2P activities. End users and providers understand that if they fly under the radar, and take minimum precautionary measures to somewhat lock down their sites, then it is unlikely that they will face legal consequences. Ultimately, once you begin sharing out on P2P sites with multiple individuals, you deserve to be prosecuted for illegal actions.

Resources:

Hall, Gary, and Erin Watson. Hacking: Computer *Hacking, Security Testing, Penetration Testing and Basic Security*. CreateSpace Independent Publishing Platform, 2016.

Kiss, Jemima. “The Pirate Bay Trial: Guilty Verdict.” *The Guardian*, Guardian News and Media, 17 Apr. 2009, www.theguardian.com/technology/2009/apr/17/the-pirate-bay-trial-guilty-verdict.

“Pragmatic Overview of Hacking & Its Counter Measures.” 2011, pp. 1–23.

Response 2

Carrillo

Nowadays the practice of using automated software has served law enforcement and courts very well because seasoned officers and prosecutors have been able to use their well-developed policing expertise to reveal sound physical proof, and augment that proof with sound digital evidence from investigative software. But for the digital evidence to be admissible in court the investigative software should meet what many experts call “trier of fact” of requirements and expectations. This means the process used to reveal the digital evidence, and chain of custody to maintain its integrity, must be repeatable and able to yield the same results (Hayes, 2015). Ultimately, the software should be capable of, and have the veracity to, determine the facts amongst the body of digital evidence in order to accurately and reliably reveal when something existed or some event occurred. Experts like Guo, Slay, and Beckett (2009) explain that forensic tools should include a verifiable validation and verification framework that can be tested. These experts’ opinions are in line with Hayes (2015), who explains that, when the evidence is tested, the results should be able to be recreated. For this reason, it is critical the reliability of the investigation software is tested with a set of reputable standards and approved by organizations with authority.

The Computer Forensic Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST) provides such reputable standards, in particular a methodology for evaluating investigative software methods by establishing general tool requirements, research protocols, test parameters, test sets and hardware testing. Their approach is based on well-known international methodologies for conformity research and quality testing. The results reveal the necessary information for toolmakers to improve investigative software, for users to choose the most appropriate investigative software, and for interested parties to understand the investigative software capabilities (NIST, 2019). The latter, understanding capabilities, is of high importance because it determines whether the investigative software can consistently recreate accurate and reliable test results; in line with the recommendations from experts like Hayes, Guo, Slay, and Becket. There are other organizations that utilize reputable standards and are accepted by authoritative entities such as the Federal Bureau of Investigations (FBI) civil society organizations, and agencies and entities of the United Nations and Inter-American systems. These include the Scientific Working Group on Digital Evidence (SWGDE), the International Organization on Digital Evidence (IOCE) (OAS, n.d.), and the American Society of Crime Laboratory Directors (ASCLD) (FBI, 2000). These organizations agree that investigative software should include key capabilities such as revealing direct evidence on the machine, associating a machine with data, providing investigative leads, revealing evidence that corroborates or refutes allegations or alibis, and revealing behavioral evidence (OAS, n.d.).

Three tools that follow these well-established standards and includes the internationally agree-upon set of capabilities are EnCase, The Forensic Toolkit, or FTK, and X Ways Forensics (XWF) (InfoSec, n.d.). EnCase is designed for forensics, digital security, security investigation, and e-discovery primarily from recouped or seized hard drives (InfoSec Institute, n.d.). But it’s very expensive, going over $3,500 for a single license (ITClick, 2020). FTK is an investigation package great for hard drive scans and string searches, as well as taking images of the hard disk. But it can’t multitask, doesn’t display a progress bar to estimate the time remaining, and doesn’t have a timeline view (making hard to conduct temporal analysis) (InfoSec, n.d.). Like EnCase, FTK is also pricey (about $4,000), but unlike EnCase, the price buys a perpetual license. XWF is considered powerful since its portable and conducts deep and granular investigations of commercial computers. However, although the price of a perpetual license about $1,000 cheaper than FTK and EnCase, updates will only be included for two years (XWays, n.d.), it’s very complex, and would not work without the required dongle (InfoSec, n.d.).

References:

Guo, Y., Slay, J., & Beckett, J. (2009). Validation and verification of computer forensic software tools—Searching Function. digital investigation, 6, S12-S22. Accessed on March 16, 2020. Retrieved from https://edge.apus.edu/access/content/group/science-and-technology-common/ISSC/ISSC621/Supplemental%20Readings/3\_Validation%20of%20Computer%20Forensics%20Tools.pdf

Hayes, D. R. (2015). A Practical Guide to Computer Forensics Investigations. New York: Pearson Education, Inc.

National Institute of Standards and Technology (NIST) Computer Forensics Tool Testing Program (CFTT). (2019, November 15). NIST. Accessed on March 18, 2020. Retrieved from https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt

International Organization on Digital Evidence (IOCE). (n.d.). Office of Legal Cooperation. OAS - Organization of American States: Democracy for peace, security, and development. Accessed on March 18, 2020. Retrieved from https://www.oas.org/juridico/english/cyber\_links\_ioce.htm

Organization of American States (OAS). (n.d.). Computer Forensic Capabilities. OAS. Accessed on March 18, 2020. Retrieved from http://www.oas.org/juridico/english/cyb\_mex\_forensic.pdf

InfoSec Institute. (n.d.). Tool Comparison. Infosec Resources. Accessed on March 18, 2020. Retrieved from https://resources.infosecinstitute.com/category/computerforensics/introduction/commercial-computer-forensics-tools/tool-comparison/#gref

ITQlick. (2020, February 18). EnCase Forensic Pricing. Accessed on March 18, 2020. Retrieved from https://www.itqlick.com/encase-forensic/pricing

X Ways -Place Orders, Request Quotes for New Licenses. (n.d.). Software for Computer Forensics, Data Recovery, and IT Security. Accessed on March 18, 2020. Retrieved from https://www.x-ways.net/order.html