Criminal Profile

[Name of the Writer]

[Name of the Institution]

Criminal Profile

**Introduction**

Cybercrime is a serious offense committed by a particular under the law sanction that is held in the constitution as it invades personal privacy. Moreover, it can also be used to commit data theft through a series of hacking processes made by a particular person. When dealing with cybercrime, it is essential to trace the source from where the crime is being committed. Criminals used to cybercrime often have certain ways of being hidden from the outside world, thus following certain steps may lead to a fruitful investigation. When investigating a criminal offense, it is important to understand the motive behind the crime. This paper would summarize all the important answers to the questions which are frequently asked during a cybercrime investigation. It would analyze Joe’s role in committing a ransomware attack on a celebrity model by accessing some of her data through a malware that was initially impossible to break through (Thomas, 2018).

**Discussion**

As a law enforcement officer that has been assigned to this case, the first step towards this initial investigation would be to identify or gather any possible evidence which can be used against Joe. As an FBI agent, I have the knowledge and experience in catching criminals who commit cybercrime or data theft. That is the reason why it makes me the correct person for this particular case. FBI's jurisdictional authority lies within all states of the US. The laws applicable to the crime and the criminal who committed it, in this case, are cybersquatting, cybersex, identity theft, illegal access to data, child pornography, malware breach, terrorism, etc.

The effectiveness of a partnership working in crime has many positive outcomes. These can be identified as relationship building through common understanding or common grounds between organizations. Moreover, obliging or providing work apprehended on the case to help solve the crime. While working on the case, it is important for me to locate and identify the evidence, which can be done through a series of steps. Being able to evaluate sources of evidence through accumulating certain strategies and techniques, and then filtering results. After finding the evidence on joe, the search and seizure procedure that was followed was through searching the personal property and confiscating any relevant evidence found.

A chain of custody tracking keeps the evidence safe at hands, which is why it is crucial for me to analyze the best chain of custody tracking through keeping Joe's essential files, DNA, photographs, or through disproving defendant's argument for the jury to make a confident decision. As for authenticating the confiscated evidence for a trial, it is vital first to satisfy all the requirements of authentication. Based on testimony on the witness, non-expert opinion, comparison between the trier of fact, and distinctive characteristics. After going through the whole process, I would finally be able to catch Joe for the crime he committed (Ben-Asher, & Gonzalez, 2015).

**Conclusion**

After Joe is caught for his crime, he is prosecuted, and the evidence that is heard from the witnesses are the call logs that are made to Ms. Rebecca Beale and the encrypted files that were encrypted through some special malware. The bitcoin exchange is yet another admissible evidence which the court would be reluctant to hear as this money exchange is illegal. Admissibility and exclusion of evidence can be brought upon by the state law. It negates the rules of evidence which would be used, such as the witness testimony, written statements, audio recordings, digital evidence, photographs, etc. This project was considerably helpful and practical as it helped to understand the topic of criminal justice and law from a broader perspective. Mostly because it helped solve the case.

**References**

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, *48*, 51-61.

Thomas, J. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks.