**Student id: 20625630**

**Name: Viraj Punjani**

**Assignment-1 CFN**

Digital Forensic Investigation Report: Suspected Corporate Espionage at XYZ Technologies

1. **Case Assessments:**

Our digital forensic team launched an investigation into John Miller, a senior software engineer at XYZ Technologies, in response to a rumoured case of corporate espionage. The lawsuit centres around the alleged theft of confidential business information and IP from Miller's Windows-based work PC. Three days ago, the event was reported.

2. **Legal Obligations:**

We accept the legal requirements governing the collecting of digital forensic data before moving along with our enquiry. To maintain the admissibility of the evidence in court, we must secure its preservation and chain of custody in compliance with the applicable laws and regulations. Furthermore, we must abide by XYZ Technologies' privacy rules and respect the undercover subject's right to privacy.

3**. Crime Scene Search:**

To find any evidence connected to the alleged theft, our digital forensics team thoroughly searched John Miller's work on a computer. This investigation includes looking through files, system logs, email, and any odd applications or actions on the machine. Several suspicious files and network activity logs were discovered throughout the analysis, necessitating further research.

4. **Evidence Collection**:

**File Analysis:** We located and gathered files that included confidential business information and intellectual property. The fact that these files were encrypted and tucked away in ambiguous directories suggests possible data-hiding strategies.

**Network Activity Logs:** Extensive network activity logs were recovered, demonstrating unauthorised access to XYZ Technologies' servers outside of business hours, adding credence to the idea that corporate espionage was taking place.

**System Logs:** A review of the system logs revealed indications of unusual login attempts and the unauthorised installation of third-party software.

**Email Correspondence:** We found and saved emails that suggested John Miller had discussions with other parties about transferring sensitive material.

**Forensic image:** To preserve the integrity of the evidence, a forensic picture of the complete hard disc was made. To confirm the accuracy of the gathered data, hash values were created.

5. **Documentation and Report:**

Each item of evidence was identified, documented, and safely kept to establish a clear chain of custody. We generated comprehensive documentation of our results, including file names, timestamps, and pertinent information. We created a thorough digital forensic report outlining our findings and actions.

**Conclusion:**

The results of our research into the alleged corporate espionage case involving John Miller point to data theft and unauthorised access as key factors. The gathered data—hidden files, network activity logs, system logs, and email correspondence—strongly supports Miller's denials of the accusations. The admissibility of the evidence in possible legal proceedings was ensured by our activities, which were carried out in accordance with legal requirements and privacy regulations.

# References

Carrier, B. (2005). *File System Forensic Analysis.* Addison-Wesley Professiona. Avalaible at: <<https://books.google.com.au/books/about/File_System_Forensic_Analysis.html?id=Zpm9CgAAQBAJ&redir_esc=y>>

Davidoff, S. (2012). *Network Forensics: Tracking Hackers Through Cyberspace.* Prentice Hall. Avalaible at:<<https://books.google.com.au/books/about/Network_Forensics.html?id=bDX3FBwBvf8C&redir_esc=y>>

Dudley, A. (2011). *Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices.* Information Science Reference Information Science Reference . Available at: <<https://www.researchgate.net/publication/215705616_Investigating_Cyber_Law_and_Cyber_Ethics_Issues_Impacts_and_Practices>>

Luttgens, J. T. (2014). *Incident Response & Computer Forensics, Third Edition.* McGraw Hill Professional. Available at: <<https://books.google.com.au/books/about/Incident_Response_Computer_Forensics_Thi.html?id=JKNQAwAAQBAJ&redir_esc=y>>

Volonino, L. (2007). *Computer Forensics: Principles and Practices. Avalaible at:<* <https://books.google.com.au/books/about/Computer_forensics.html?id=EWVGAAAAYAAJ&redir_esc=y>*>*