Diana Blankinship

4/12/2025

Introduction

A Digital Forensic Analyst is a great example of a career in the cybersecurity field that relies heavily on social science research and knowledge. They often employ social science research when analyzing information from digital sources. For both computer crimes and non-computer crimes, Digital Forensic Analyst will work hand in hand with criminology and political science (law). Undoubtedly, as humans are the weakest link in cybersecurity, psychological concepts will be used on a regular basis. Due to costs of technology and training, economic limitations must be battled. Their role is also of vital importance to marginalized groups who are often victims of cybercrime.

Research Methods

Due to the need for valid and reliable forensic data, Digital Forensics Analysts use social

science research methods to investigate the tools and processes they use to find digital

evidence. Archival research is one common method of research seen in digital forensics

as there has been an explosion of research in recent years with the growth of technology. A

digital forensic analyst recovers data from archives found on social media websites such

as YouTube, Twitter, and Facebook. If they work in research, they may also review research

articles. In one article reviewed, analysts in defense collected, stored, and analyzed data

from multiple social media sites to analyze extremist behavior It is also crucial for the

data to be reliable fo corporate and criminal investigations therefore the Digital

Forensic Analyst must be up to date on rapidly advancing technology to ensure

data is obtained objectively. (Berzinji, Muhammed, and Muhammed).

Political Science

When Digital Forensics Analyst investigate cybercrimes, they will need to follow the most up to date policies and laws in cybersecurity. If they are investigating a data breach, the investigation must also be completed timely for notification laws. There are also privacy laws that must be taken into consideration when extracting data from technology such as smart phones and laptops. Currently, there is a vital need to develop standardized rules and procedures for managing digital evidence which will require Digital Forensic Analysts to combine their knowledge and expertise with the legal profession. (Rakha)

Criminology

The expertise of a Digital Forensic Analyst is often needed by law enforcement to investigate criminals by searching their computers and cell phones for evidence that could tie them to a crime. When analyzing data to investigate a crime, analysts may use the Neutralization Theory to understand the mind of the criminal. If they identify digital evidence shows a hacker justifying a financial hack by stating that nobody got hurt, the analyst is using the Denial of Injury Neutralization Theory. (Keeling, Losavio)

Psychology

As humans are the most important link in cybersecurity, it is not surprising to find that psychology is also very important in the work of a Digital Forensic Analyst. When analyzing digital information, the analyst needs to understand the user. When digital information from a social media site such as Twitter is analyzed, the analyst uses Cognitive theory when looking for words that help identify the thought processes and possible behavior of the user. Cognitive theories see a person’s thoughts and beliefs as the source of their emotions. An analyst may use this theory when investigating a potential suspect in a crime by looking for specific emotions such as anger and anxiety in the digital evidence. (Adkins, Al Bataneih, Khalaf).

Marginalized Groups

Women are highly underrepresented in cybersecurity and they are also frequent victims of cybercrime, therefore, Digital Forensic Analysts must focus on this marginalized group. In India, an online Cybercrime reporting portal was established to help prevent cybercrime against women (Bali). Analysts can focus on this group by including this demographic in their research and also by researching ways to prevent technology from victimizing women.

In India, they are investigating ways to remove certain technologies that offend women (Bali). More women in this profession will also help to bring more diversity and ideas to help this marginalized group.

Conclusion

Social sciences provide valuable theories for Digital Forensic Analysts to analyze data. Laws against cybercrime are considered daily as cybercrime continues to grow. Criminology theories are helpful are used by Digital Forensic Analysts when analyzing digital data of potential crime suspects. Psychology is a huge science to know as Digital Forensic Analysts use Natural Language Processing to identify hackers and criminals.

Women are a marginalized group for Digital Forensic Analysts to consider in their research.

References

Berzinji, A., Muhammed, R., Muhammed, D. (2021). Development of an Intelligence Gathering Framework for Analysing Cyber Extremism on Social Media Networks. International Journal of Cyber Criminology, Volume 18, Issue 1. January – June 2024.

<https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view>

Adkins, J., Al Bataineh, A., Khalaf, M. (2024). Identifying Persons of Interest in Digital Forensics Using NLP-Based AI. Future Interent, Volume 16, Number 11. November 2024.

[Identifying Persons of Interest in Digital Forensics Using NLP-Based AI – DOAJ](https://doaj.org/article/a98569cd8b1e437a981abfbd54469639)

Bali, S. (2023). Cybercrimes against Women in India: How Can the Law and the Technology Help the Victims? CRC Press

[e-Reader | Cybercrimes against Women in India: How Can the Law and the](https://www-taylorfrancis-com.proxy.lib.odu.edu/reader/download/ed67ef4c-5a5e-491d-81f2-506b54503553/chapter/pdf?context=ubx)

Keeling, D., Losavia, M. (2017)Public Security and Digital Forensics in the United States: The Continued Need for Expanded Digital Systems for Security. Journal of Digital Foresnsics, Security and Law. Volume 12, Article 6. (2017)