CLARITAS

Digital Media Exploitation

The Digital Media Exploitation courses unfold the intricate world of digital forensics to its participants, bridging the gap between theoretical knowledge and practical skill application in the analysis of contemporary mobile and computing devices.

Justification and Overview

In an era where information is as valuable as currency, this course positions itself at the forefront of intelligence gathering, equipping learners to adeptly navigate the digital terrain of devices powered by iOS, Android, and Windows platforms.

As the digital ecosystem evolves, so do the means of exploitation. This course takes participants on an exploratory journey through the latest advancements in the field. They will be immersed in real-time scenarios that mimic the complexity of current digital environments. From extracting sensitive information across personal and professional networks to unveiling the secrets behind user patterns and behaviors, this course imparts crucial analytical techniques.

The curriculum is carefully structured to guide students through the myriad aspects of digital forensics, teaching them how to uncover and exploit network susceptibilities, extract and interpret life patterns data, and penetrate communication vaults to access directories, messages, and emails. As cloud storage becomes the norm, students will also learn sophisticated approaches to infiltrate cloud systems, with a specialized focus on popular services like iCloud and Google Cloud.

The practical component is underscored by rigorous training in reverse engineering and the discreet use of applications to gain and maintain access to devices, all while avoiding detection. In the contemporary context, the course also integrates the increasingly significant field of drone forensics – addressing the challenges of extracting and deciphering data from unmanned aerial devices, which are becoming more prevalent in both civilian and security applications.

In response to the growing interconnectedness of digital and physical security, the course content is designed not just for individual proficiency but for its strategic value in broader operations. It acts as a complementary piece in a larger puzzle, fitting into our Targeted Equipment Interference Programme and enriching capabilities in infosec, internet operations, network reconnaissance, and Wi-Fi exploitation.

Through a blend of rigorous academic study, hands-on practical exercises, and real-world case studies, this course is structured to cultivate a comprehensive understanding of the landscape of digital forensics.

Graduates will emerge with an arsenal of skills, ready to apply their newfound expertise to the **diverse challenges posed by the intersection of technology, security, and investigation in a hyper-connected world.**

Digital Media Exploitation

Indicative Course Content

Setup of environment

- Setting Up a Forensics Lab
- Data Exfil
- Bagging Tagging and Photos

Wi-Fi Overview

- What is Wi-Fi?
- What makes Wi-Fi special are vulnerabilities and access methods
- Wi-Fi 6 and 7 issues and vulnerabilities
- Legal considerations

Identifying the target

- War Driving, identifying networks
- Building a data set
- Multiple location tracking
- Adding GPS data to a scan
- OSINT enhancement of reconnaissance findings
- Identifying Targets with MAC randomisation

Attacking Wi-Fi

- Jamming
- Targeted de-authentication
- Fake Access points
- Small form factor Wi-Fi Devices
- Man in the Middle Attacks
- Wi-Fi Intercept
- Password Cracking

Lab and Real-world scenarios

- Identify
- Attack
- Practice
- COTS Wi-Fi adaptation

COURSE AIMS

This course educates students on how to capitalise on the vulnerabilities present within Wi-Fi networks, enabling them to intercept data, deny or disrupt capabilities, and/or facilitate undetected access to premises and assets.

CONDITIONS OF ENTRY

Students are not required to have any specific experience before participating in this course. A strong technical aptitude and the completion of other courses CCA series are strongly recommended or equivalent training, will lay a robust groundwork for this course.

To learn more, speak to our team today:

info@claritasinsight.com