UNSW CANBERRA | Cyber

Digital Forensics

Location	UNSW Canberra
Duration	5 days
Standard Price	$4,550.00
Defence Price	$4,095.00

Description

This course will introduce participants to digital forensic analysis and investigation first principles. Students will be introduced to theoretical concepts including the digital forensic method, intent and its application. The course will also cover introductory Microsoft Windows centric technical topics such as file system, memory and operating system artefact analysis using contemporary open source tools, techniques and procedures. Students will be expected to demonstrate both their theoretical and technical understanding through the completion of practical exercises in a simulated operational environment.

This is an introductory course covering:

- Basic forensic theory and practical exercises targeting the Microsoft Windows Operating platform
- Disk forensic theory and practical exercises targeting the NTFS filesystem
- Configuration forensic theory and practical exercises targeting the Microsoft Windows Registry
- Memory forensic theory and practical exercises targeting (mostly) the Microsoft Windows operating platform
- Basic network forensic theory and practical exercises

Learning Outcomes

On completion of this course, participants should be able to:

- Understand basic digital forensic theory, including purpose and intent
- Understand how to professionally approach a digital forensic investigation, determining both its scope and duration
- Demonstrate they can utilise contemporary open source tools, techniques and procedures to conduct analysis
- Demonstrate they can achieve an acceptable level of intelligence outcomes within a defined period of time
- Perform a basic forensic examination, producing an actionable intelligence product

Who Should Attend

The intended audience for this course are students that have no previous experience or exposure to the field of digital forensics. As a result, students should expect the course material to be introductory and all inclusive, with no digital forensic pre-reading required.

NICE Framework mapping

This course maps to the highlighted work categories:

Securely Provision
Oversee & Govern
Analyse
Investigate
Operate & Maintain
Protect & Defend
Collect & Operate

To find out more about the NICE Framework go to: niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework

Course Day Breakdown

Day 1

Disk Forensics

Day 1 gives an overview of the history of disk forensics. Basics such as file structures, metadata, file systems concepts, windows file systems and disk partitioning are covered leading to a practical investigative scenario.

Topics

File system features, FAT, exFAT, NTFS, File slack, Volume shadow copies, Master boot record partition table, GUID partition table, Partition slack.

Day 2

Registry Forensics

This session will focus on the analysis of low level configuration settings located within the Microsoft Windows registry. You will gain a better understanding of the Windows registry as a hierarchical database which will culminate in a practical exercise of detecting malware within the registry utilising Python.

Topics

Configuration analysis, Registry keys & values, Registry root keys, Hives, Deleted registry keys.

Day 3

Network Forensics

Day 3 will look at how network investigations deal with volatile and dynamic information, focusing on the analysis and monitoring of computer network traffic for the purposes of information gathering, legal evidence and intrusion detection.

Topics

The internet protocol, Packet structures, Addressing methods, Application layer protocols, Netflow.

Day 4

Memory Forensics

The first part of the day will cover the history of memory forensics and modern computer architecture. We will then cover several memory management techniques and look at how these can be leveraged in forensic processes.

Topics

Process concept, Memory layout, Process management, Windows environment block, Thread concept, Thread management, Virtual memory, Page concept, Memory protections, Virtual Address Descriptor (VAD), Kernel interface, Hibernation.

Day 5

The Forensic Method

Day 5 will cover various digital forensic analysis techniques from multiple viewpoints in order to derive meaning and intelligence from gathered evidence. We will look at what it is like to be in an offensive position and how this can provide analysts with a significant tactical advantage.

Topics

Locard's Exchange Principle, Offensive Operations, Forensic Investigation Requirements, Digital Forensic Life Cycle.

> *"The narrative-based labs encouraged students to think laterally and were balanced well with the theoretical concepts."*
>
> Course participant

CRICOS No. 00098G • 337361580

UNSW Canberra Cyber

UNSW Canberra Cyber is a unique, cutting-edge, interdisciplinary research and teaching centre, working to develop the next generation of cyber security experts and leaders. The centre is based in Canberra at the Australian Defence Force Academy and provides professional, undergraduate and post graduate education in cyber security. Our air-gapped, state of the art cyber range offers a secure environment where we deliver a number of technical and highly specialised learning opportunities. Our courses are designed to give the next generation of cyber security professionals the skill sets needed to thrive in the industry. We can also create bespoke professional education programs tailored to your organisation's needs. Contact us at cyber@adfa.edu.au to discuss how.

Find out more

✉ cyber@adfa.edu.au

🌐 unsw.adfa.edu.au/cyber