

# CDFS

CBIT Digital Forensics Services

# DFIR Foundations



1300 55 33 24



contact@cdfs.com.au

www.cdfs.com.au | contact@cdfs.com.au

PRESENTED BY

**Zoran Iliev**

Master of eForensics and Enterprise Security

V1 | This document is uncontrolled when printed

# DFIR is a three day course

Cyberattacks have become a common aspect of our interconnected world. In the past, a response to such incidents would be to simply kick the attacker off and rebuild any compromised computers. But with the proliferation of skilled people employing ever more complex attack vectors, there is a call to perform a deeper forensic analysis to determine the exact attack methodologies, to better harden target systems from future attempts.

This three-day course is aimed to bridge the gap between traditional Security Operations Centre incident response and digital forensics. You will learn where the two disciplines overlap, and how they can work together to create a capability that is greater than the sum of its parts.

**NOTE:** You must sign up and pay at least 30 DAYS before any class to reserve your seat! If you want a seat, make sure you do it earlier rather than later.

## Executive Summary

Students will learn the following:



Digital Forensics &  
Incident Response  
Roles



Data collection



File system artefacts



Encryption



Indicators of  
compromise



Processing and  
examining evidence



Testing and  
experimentation

T1 DFIR Foundations gives practitioners a grounding in both incident response and digital forensics so they may better understand how these disciplines can work together to solve complex problems in the cybersecurity arena. The course features both theory as well as practical case studies where students will be able to use their new skills to examine data for evidence of attack using realistic data sets and tools.

If you are an existing Tier 1 SOC team member looking to upskill, a digital forensic analyst wanting to cross-skill, or an IT professional seeking an entry into DFIR, this is a great opportunity to increase your skills and capability.



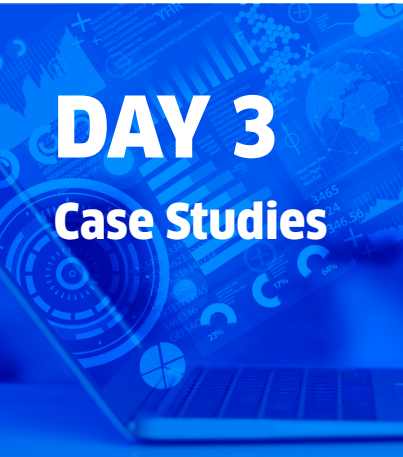
## DAY 1

- Introduction to DF & IR
- DF vs IR - how and where they overlap
- Digital Evidence
- Data collection
- Forensic Data collection at rest
- Forensic Data collection at transit
- Practical exercises



## DAY 2 Theory

- File systems forensic artefacts
- TCP / IP (v4)
- Windows OS forensic artefacts
- Application generated forensic artefacts
- Encryption and obfuscation



## DAY 3 Case Studies

- Common indicators of possible attack or compromise
- Defining a scope for data collection
- Processing and examining of the evidence
- Practical Application of Scientific methodologies  
(Testing and experimentation)

**PRICE**

**\$4500**  
ex GST

*per participant*

**OR**

**3x CDFS Training  
Vouchers**

\* Vouchers can only be used for courses delivered by CDFS at our training facility or via Virtual Instructor-Led Training.