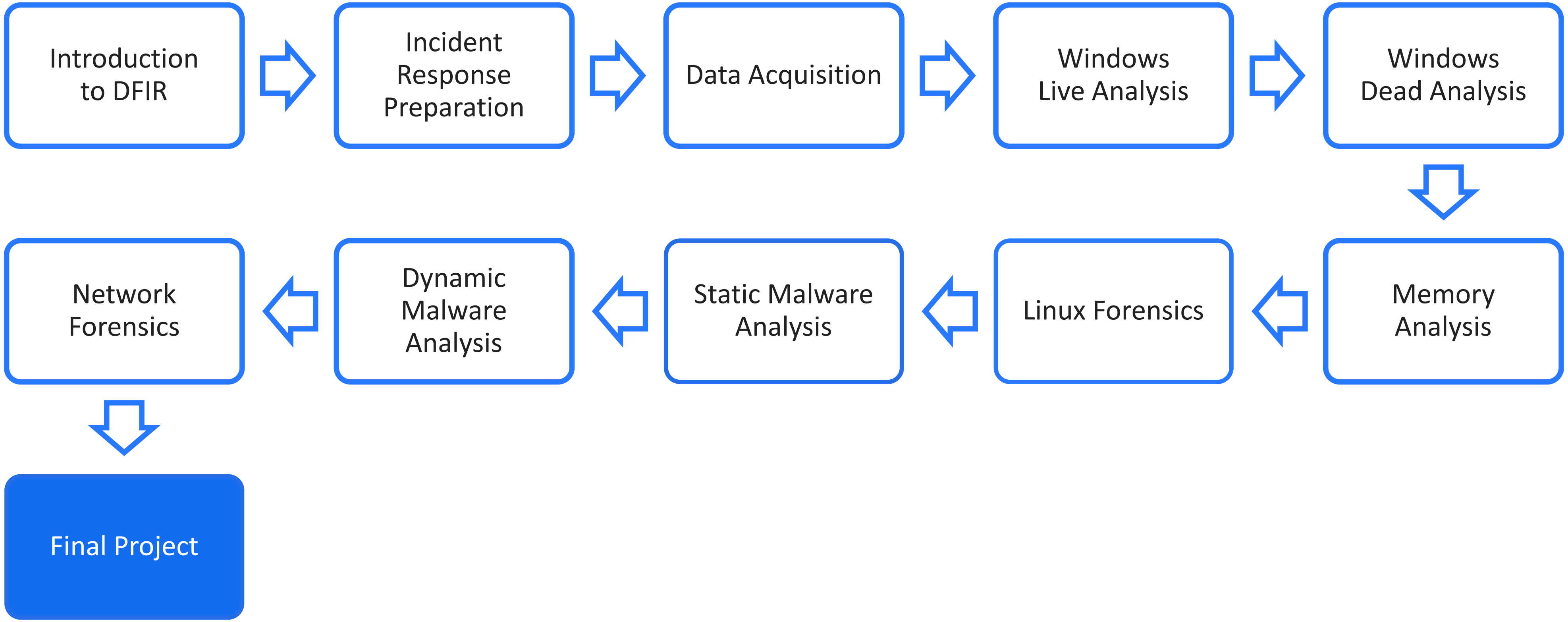
Cyber Security Professional Program

# Final Project

Digital Forensics & Incident Response

Digital Forensics & Incident Response

# Course Path



Introduction to DFIR

Incident Response Preparation

Data Acquisition

Windows Live Analysis

Windows Dead Analysis

Memory Analysis

Linux Forensics

Static Malware Analysis

Dynamic Malware Analysis

Network Forensics

Final Project

DFIR Final Project

# Objectives

This is a presentation for the final project of the course.

The project focuses on using multiple forensics techniques to solve the challenge of investigating malware and its activity.

- Project Requirements
- Project Steps

Final Project

# Project Requirements

Project Requirements

# Before You Start

- Download all the necessary files (3).
- Make sure your investigation environment is set up and ready.

> Virtual machines in the environment should have snapshots of all the major stages.

Project Requirements

# The Story

The challenge includes three stages:

- Identify the beginning of the attack.
- Identify malicious activity in the VM.
- Unlock the final file.

> Each stage in the challenge must be solved before moving on to the next stage.

Final Project

# Project Steps

Project Steps

# Pcap Investigation

Investigate the pcap file.

Did you find anything suspicious?

Project Steps

# Extracting Logs

Use Zeek to extract valuable information from the pcap file.

Project Steps

# Locate the Malware

Locate the malicious file in the captured data.

Project Steps

# Identify the Malware

Study and identify the nature of the malicious file.

Project Steps

# Discover how the Attack Began

Find evidence of malicious activity in the pcap file, and find the first packet of the attack.

Project Steps

# Investigate the VM

Start investigating the infected machine (192.168.23.130) in VMWare Player (download and install the free version).

The sequence of the first malicious packet is the password.

Project Steps

# Identify Backdoors

Identify any backdoors the attacker may have left.

Project Steps

# Identify the Malware 2

Investigate the second malware.

Project Steps

# Follow the Hint

Follow the hint in the executable.

Project Steps

# Finish Part 2

Finish the investigation of the second part.

Project Steps

# Complete the Challenge

Use the information obtained from the investigation to unlock the last piece of the challenge (investigate_me3.bin).

Thank You

# Questions?