

CIFR Class Schedule

Day	Week 1	Week 2
Monday	<p>Lecture:</p> <ul style="list-style-type: none"> ➤ Network theory ➤ Microsoft network architecture <p>Labs:</p> <ul style="list-style-type: none"> ➤ Remote Desktop ➤ Join an AD domain ➤ Use of net.exe commands ➤ Create group policies (GPOs) 	<p>Lecture:</p> <ul style="list-style-type: none"> ➤ Windows event logs ➤ Windows image analysis focusing on malware and intrusion artifacts <p>Labs:</p> <ul style="list-style-type: none"> ➤ Event log analysis with Event Log Explorer ➤ Event log analysis with Log Parser and Log Parser Studio ➤ Windows artifacts extraction and analysis
Tuesday	<p>Lecture:</p> <ul style="list-style-type: none"> ➤ Log types, locations and contents ➤ Wireshark <p>Labs:</p> <ul style="list-style-type: none"> ➤ Use of Wireshark ➤ Wireshark scenario 	<p>Lecture:</p> <ul style="list-style-type: none"> ➤ Linux fundamentals ➤ Linux analysis <p>Labs:</p> <ul style="list-style-type: none"> ➤ Analysis of compromised Linux image
Wednesday	<p>Lecture:</p> <ul style="list-style-type: none"> ➤ Linux commands for log analysis <p>Labs:</p> <ul style="list-style-type: none"> ➤ Use Linux commands for log analysis of multiple log types 	<p>Lecture:</p> <ul style="list-style-type: none"> ➤ RAM capture and analysis <p>Labs:</p> <ul style="list-style-type: none"> ➤ RAM capture with multiple tools ➤ RAM analysis with Volatility 3 and other tools
Thursday	<p>Lecture:</p> <ul style="list-style-type: none"> ➤ Remote analysis ➤ Remote imaging ➤ Use of Velociraptor for analysis at scale <p>Labs:</p> <ul style="list-style-type: none"> ➤ Capture Windows image across the network using FTK Image CLI and netcat ➤ Capture Linux image across the network using dd and netcat 	<p>Lecture:</p> <ul style="list-style-type: none"> ➤ Static and dynamic malware analysis <p>Labs:</p> <ul style="list-style-type: none"> ➤ Static and dynamic malware analysis of Office documents, PDFs, and Windows executables <p>Capstone Exercise:</p> <ul style="list-style-type: none"> ➤ Walkthrough of PowerShell Empire ➤ Walkthrough of mimikatz

	<ul style="list-style-type: none"> ➤ Capture Linux image across the network using dd and ssh ➤ Remote analysis with Forensic Explorer ➤ Remote analysis with Velociraptor 	<ul style="list-style-type: none"> ➤ Walkthrough of scripted deployment of ransomware ➤ Capture RAM across the network ➤ Capture drive image across the network
Friday	<p>Lecture:</p> <ul style="list-style-type: none"> ➤ Log2Timeline / Plaso <p>Labs:</p> <ul style="list-style-type: none"> ➤ Log2Timeline / Plaso timeline generation and analysis ➤ ssh attack log analysis ➤ Web server attack log analysis 	<p>Lecture:</p> <ul style="list-style-type: none"> ➤ Guided analysis processes for capstone evidence <p>Labs:</p> <ul style="list-style-type: none"> ➤ Analyze capstone evidence