



# STARK STATE COLLEGE

## GENERAL SYLLABUS

### Course Information

**Course Name:** File Systems Analysis  
**Course Number:** CFS257

### Required Materials

**Textbook(s):**

1. Windows Forensic Analysis Toolkit: *4E*, Carvey, Syngress 2014, ISBN-978-0-12-417157-2
2. (Optional) File System Forensic Analysis, Carrier, 2005, Addison Wesley. ISBN 0-321-26817-2

**Required Readings:** None

**Additional Materials:**

1. Personal computer running **Windows 10 Professional** (Not Home Edition), a virtual machine running Windows 10 Professional or an external hard drive with a Windows to Go installation running Windows 10 Professional.
2. Additional material furnished by the instructor or available online

### Course Outline/Calendar

The date of coverage and order of coverage may be modified based on the faculty member and events beyond the control of faculty members that interfere with class times and teaching.

Week	Chapter/Topic/Lab
Week 1	<b>Introduction, Windows Forensics, Ethics &amp; Professionalism</b> <ul style="list-style-type: none"> <li>• Academic Honesty Prerequisite</li> <li>• Chapter 1 Analysis Concepts</li> <li>• Ethics Lab</li> </ul>
Week 2	<b>Incident Preparation &amp; Training, System Information</b> <ul style="list-style-type: none"> <li>• <b>Chapter 2 Incident Preparation</b></li> <li>• <b>System Information Lab</b></li> </ul>
Week 3	<b>Volume Shadow Copy, Host Protected Area</b> <ul style="list-style-type: none"> <li>• Chapter 3 Volume Shadow Copy</li> <li>• Volume Shadow Copy Lab</li> </ul>
Week 4	<b>Master File Table, NTFS File System, Event Logs, Recycle Bin</b> <ul style="list-style-type: none"> <li>• Chapter 4 File Analysis</li> <li>• MFT Lab</li> </ul>
Week 5	<b>Prefetch Files, Scheduled Tasks, Jump Lists &amp; Hibernation Files</b> <ul style="list-style-type: none"> <li>• Exam 1, Chapter 4 continued</li> <li>• Prefetch &amp; Jump List Lab</li> </ul>
Week 6	<b>Application Files, Memory &amp; Hibernation Analysis, GREP</b>

Week	Chapter/Topic/Lab
	<ul style="list-style-type: none"> <li>• Chapter 4 concluded</li> <li>• Memory Analysis Lab</li> </ul>
Week 7	<b>Advanced Registry Analysis, Shellbags</b> <ul style="list-style-type: none"> <li>• Chapter 5 Registry Analysis</li> <li>• Manual Registry Lab</li> </ul>
Week 8	<b>Malware, Alternate Data Streams,</b> <ul style="list-style-type: none"> <li>• Chapter 6 Malware Detection</li> <li>• ADS Lab</li> </ul>
Week 9	<ul style="list-style-type: none"> <li>• Live Response, Power Shell</li> <li>• PS Tools Lab, Power Shell Lab</li> </ul>
Week 10	<b>Windows Log Files, Timelines</b> <ul style="list-style-type: none"> <li>• SRUM</li> <li>• Exam 2, Chapter 7 Timeline Analysis</li> <li>• SRUM Lab</li> </ul>
Week 11	<ul style="list-style-type: none"> <li>• E-Mail Artifacts</li> <li>• E-Mail Lab</li> </ul>
Week 12	<b>Tying Artifacts Together Shimcache &amp; Shellbag Artifacts</b> <ul style="list-style-type: none"> <li>• Chapter 8 Correlating Artifacts</li> <li>• Artifacts Lab</li> </ul>
Week 13	<b>Password Recovery, Ohio Cyber Range</b> <ul style="list-style-type: none"> <li>• Chapter 9 Reporting</li> <li>• Password Cracking Labs, Ohio Cyber Range Lab</li> </ul>
Week 14	Browser Artifacts Internet Browser Artifacts Lab
Week 15	Browser Artifacts continued
Week 16	Final Practical Exam