

# CounterTack Training

## Advanced Malware Analysis Using Responder® PRO

This, virtual, hands-on course provides a challenging and deep level of understanding of Malware Analysis and Reverse Engineering using Responder PRO. Discover methods used by malware authors to inject code into running processes, detect and reverse-engineer backdoor implants, reverse-engineer drivers and Botnets, and assess the capabilities of virtual machine-based obfuscation techniques. The course enhances the skills and techniques taught during the Basic Malware Analysis class.

<b>Duration:</b>	12 Hours (CPE Credits: 12 Units)
<b>Prerequisites:</b>	A computer investigations background is helpful. Basic computer and memory architecture as well as Windows OS architecture required. Assembly language preferred.
<b>Who Should Attend:</b>	Anyone who is trying to further their knowledge in the latest memory analysis techniques. This includes Tier 1 professionals and up. <ul style="list-style-type: none"><li>• Forensic Investigators</li><li>• IT Security Professionals</li><li>• Security Analysts</li><li>• Incident Responders</li></ul>
<b>Course Objectives:</b>	By the end of the course, students will be able to: <ul style="list-style-type: none"><li>• Understand the component of Windows memory</li><li>• Properly acquire a memory image using FastDumpPro</li><li>• Quickly determine the most malicious code using Responder PRO</li><li>• Identify common malware types</li><li>• Decipher the common malware types in Responder PRO</li><li>• Record and analyze malware using REcon in Responder PRO</li></ul>
<b>Materials:</b>	Each student is provided the following: <ul style="list-style-type: none"><li>• Student lab exercise guide</li><li>• Student lab solution guide</li><li>• Certificate of completion</li></ul>
<b>Real Life Scenarios:</b>	In each class, you will analyze real memory malware using Responder PRO to strengthen your analysis skills. Common malware will be used to replicate everyday situations.
<b>Delivery Format:</b>	Online Virtual lab & training center. 6 hours a day, 2 consecutive days
<b>Related Courses:</b>	See also 4-hour Online Training: Introduction to Using Responder PRO.
<b>More Info:</b>	See <a href="http://www.countertack.com/training">www.countertack.com/training</a> or email <a href="mailto:info@countertack.com">info@countertack.com</a> .