

## Windows Live Memory Forensics and Malware Analysis using Responder™ Field Edition Computer-based Training (CBT)

The accurate reconstruction of events is important to all investigations, and this is no less important in digital investigations when attempting to understand root cause, or attribute a course of conduct to user activity. In most modern investigations, a computer forms part of the evidence trail, and in turn, the collection and analysis of memory (RAM) needs to be considered. This course uses hands-on application training and scenarios to ensure users gain a rapid and practical exposure to the various concepts taught.

This self-contained computer-based training consists of six self-paced modules, spanning approximately 3 hours. However, the course is designed to be consumed on an opportunistic, asynchronous basis, so it will take much longer for the typical beginner to successfully complete the course and the quizzes (approx. 8 hours).

**CPE Credits:** 16

**Level:** Introductory

**Prerequisites:** Basic computer skills

### Course Objectives:

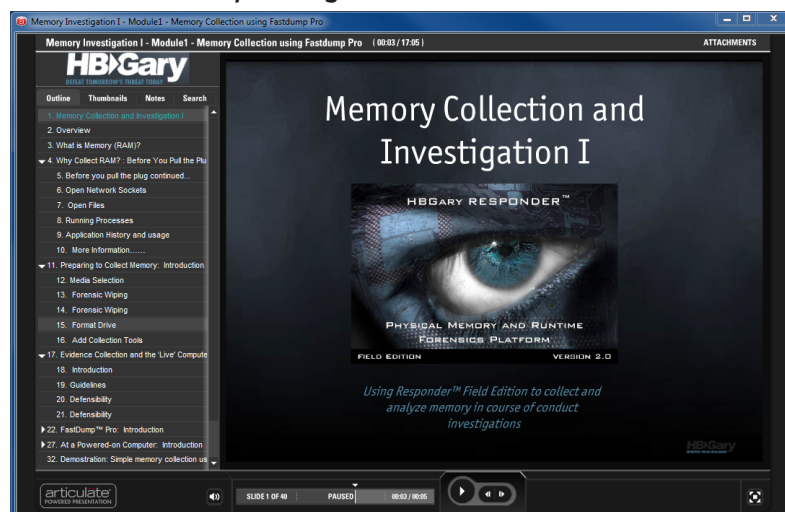
- Collect a copy of RAM from a running computer
- Identify data structures in memory
- Search and analyze artifacts left in memory by commonly used applications
- Reconstruct files mapped in memory
- Report findings and processes

**Audience:** This course is aimed at those new to digital investigations, and experienced examiners familiar with digital investigations, who are seeking to understand how memory is used to complement their existing collection and analysis process.

### Course Outline:

#### I. Collecting Memory using FastDump Pro™ (17:00 + 20 question quiz)

- What is RAM?
- Why collect RAM?
- Forensic processes: forensically sound versus minimally invasive
- Collecting memory using FastDump Pro
- Running tools from a command line
- Managing the integrity of collected evidence
- Collection from a powered-on machine with physical and administrative access
- Collection from a powered-on remote machine with administrative access
- Collection types: .hpk and .bin when to use



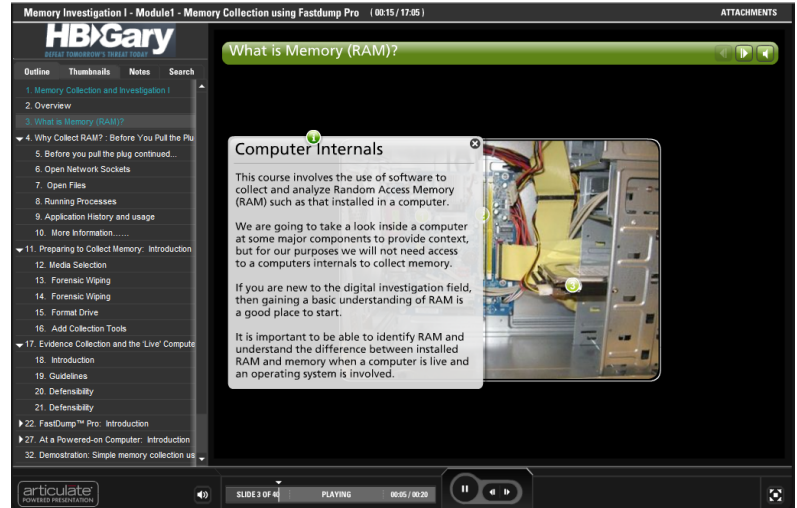
# Responder™ Field Edition

## II. Using Responder Field Edition to Analyze a Memory Image (43:01 + 30 minute hands-on lab + 10 question quiz)

- Starting a new project in Responder Field Edition
- Navigating the Responder Field Edition interface
- Reviewing artifacts parsed by Responder Field Edition
- Searching for patterns in a memory image
- Reviewing search results and annotation

## III. Introduction to Data Structures in Memory (16:38 + 11 question quiz)

- How RAM works
- Windows Memory model
- Physical Memory vs. Virtual Memory
- Paging to disk
- Virtual Memory allocation
- Virtual Address descriptors
- Memory mapping
- Using the probe feature in FastDump Pro



## IV. Associating Data with Applications in Memory (25:01 + 30 minute hands-on lab + 11 question quiz)

- What is file data?
- Identifying files by header and creating patterns for searching
- Conducting searches using patterns in Responder Field Edition
- File fragmentation in memory
- Recovering file data from memory
- Associating file data with processes

## V. Internet History, Webmail and Chat Artifacts in Memory (20:13 + 30 minute hands-on lab + 8 question quiz)

- Investigation Preparation
- Building case specific keywords and patterns
- String and Hex searches
- Identifying Applications
- Processes associated with applications
- Data created by applications i.e. chat logs, internet browsing history
- Analyzing applications
- Researching common applications and exploring functions
- Reviewing a processes Memory Map object
- Understanding the Internet History object in Responder Field Edition
- Understanding the Keys and Passwords object in Responder Field Edition

## VI. Introduction to Malware Analysis (27:33 + 30 minute hands-on lab + 11 question quiz)

- Malware and remote access Trojans
- Functionality
- Identifying suspicious ports and processes
- Using and editing Baserules in Responder Field Edition
- Using the Summary and Technical Details reports
- Disassembling an executable using Responder Field Edition
- Searching for and reviewing Assembly Code
- Understanding and reviewing the Interrupt Descriptor Table
- Understanding and reviewing the System Service Descriptor Tables
- Exporting a package as .livebin file