This 5-day training course is designed to give you the skills you need for tweaking, customizing, or outright developing your own tools. We put you on the path of creating your own tools, empowering you to better automate the daily routine of today's information security professional and to achieve more value in less time. Again, and again, organizations serious about security emphasize their need for skilled tool builders. There is a huge demand for people who can understand a problem and then rapidly develop prototype code to attack or defend against it.

**Students will learn to:**

* Leverage Python to perform routine tasks quickly and efficiently
* Automate log analysis and packet analysis with file operations, regular expressions, and analysis modules to discover malicious activity
* Develop forensics tools to carve binary data and extract new artifacts
* Read data from databases and the Windows Registry
* Interact with websites to collect intelligence
* Develop UDP and TCP client and server applications
* Automate system processes and process their output

**Course Outline:**

Day 1:

* Introduction/Assessment of Skills/Review
  + Syntax
  + Variables
  + Math Operators
  + Strings
  + Functions
  + Modules
  + Control Statements
  + Introspection
  + Lists
  + Loops
  + Tuples
  + Dictionaries
  + The Python Debugger
  + Coding Tips
  + Tricks and Shortcuts
  + System Arguments
  + ArgParser Module

Day 2:

* File Operations
* The STRUCT module
* Python Sets
* Regular Expressions
* Data Analysis Tools and Techniques
  + iPython/Jupyter
  + numpy
  + Pandas
  + Matplotlib
* SQL Queries
* HTTP Communications with Python Built in Libraries
* Web Communications with the Requests Module

Day 3:

* Log Parsing
* Network Socket Operations
* Exception Handling
* Process Execution
* Blocking and Non-blocking Sockets
* Using the Select Module for Asynchronous Operations
* Python Objects

Day 4:

* Argument Packing and Unpacking
* Raw Network Sockets and Protocols
* Packet Analysis
* Packet Reassembly
* Payload Extraction
* Acquiring Images from Disk

Day 5:

* Image Forensics and PIL
* Memory and the Network
* File Carving
* Long-Tail/Short-Tail Analysis
* Geolocation Acquisition
* Blacklists and Whitelists