F401 Triage and Analysis

Duration 5 days Beginner, Intermediate and Advanced

The first step of any investigation is the collection of evidence, as in digital forensics. The evidence used in forensics consists of data and data can appear in many different forms and places. First, we need to be able to identify the data we may need, determine where that data is located, and create a plan and procedure for collecting it. In forensics, we usually only have one chance to collect evidence. Failure to properly collect the data not only harms the investigation but can also result in the destruction of data that could be used as evidence. Unfortunately, there is no single standardized method of collecting evidence for all of today's various storage technologies as investigators unable to reach a conclusion by simply examining the image of a single hard drive. In addition, with the increasing use of cloud storage and applications belonging to various service providers, it is becoming increasingly difficult to properly collect data from all these areas. This training was created to develop the skills necessary for first responders and forensic examiners to identify, collect and protect evidence within a wide range of data storage devices. With the practical applications in the training, data acquisition and analysis processes will be worked on in many different scenarios from hard drives to portable drives, from mobile phones to network storage units.

MODULE 1 Data, file systems, evidence files, quick data collection, crime scene management	MODULE 4 Unorthodox Image Acquisition Methods, Cloud Data, Remote Image Acquisition, Multi-Drive Storage Devices, and Network Image Acquisition
MODULE 2 Acquiring and Collecting Evidence	MODULE 5 IoT, Apple Device Image, Online Identification
MODULE 3 Mounting Evidence, Triage, RAM and Live Data Collection	MODULE 6 Data Carving and Rebuilding, Data Recovery