



Cyber Investigation 101 - STOP

This 2-day course is intended for probation/parole, detectives, and officers conducting “knock and talk” interviews, spot checks or consent searches. This class utilizes TUX4N6™, a Linux-based bootable CD to preview a suspect computer system for potential evidence in a forensically sound manner. TUX4N6™ has the advantage of being able to “read” other computer systems’ files without writing to or altering the data on those systems.

Location of Training:

AZ Peace Officer Standards and Training (AZ POST)
2643 East University Drive
Phoenix, AZ 85034

This is Free Training for Law Enforcement Agencies

Training Agenda

INTRODUCTION TO COMPUTER FORENSICS

Learn the various steps of a computer forensic investigation, as well as how digital evidence relates to crimes.

HARDWARE RECOGNITION

Understand and identify the wide range of computer hardware that can hold digital evidence.

COMPUTER ACCESS

Learn how to access the Basic Input/Output System (BIOS) in a computer system to ensure the machine will boot to the TUX4N6™ CD. Learn how to handle a computer system on-scene when the system is powered on or turned off.

USING TUX4N6™

Learn how to use NW3C’s TUX4N6™ to quickly and forensically preview/triage digital evidence found on scene.

KNOCK & TALK

Learn how to do a successful consent search (also referred to as a “knock & talk”) to generate admissible evidence, as well as many considerations for going on-scene when digital evidence is expected.