



Fast CyberForensic Triage (FCT)

This 3-day course will introduce investigators and first responders to the process known as Fast CyberForensic Triage. Fast forensics is defined as “those investigative processes that are conducted within the first few hours of an investigation, that provides information used during the suspect interview phase. Due to the need for information to be obtained in a relatively short time frame, fast forensics usually involves an on site/field analysis of the computer system in question.”

The course will utilize both presentation and hands-on training. The course content is based on practical, applied investigative processes and stresses both knowledge of the concepts and application of the knowledge to “real world” case scenarios. Students will learn to quickly prioritize and recover time-sensitive digital evidence, while observing forensically sound practices. Class participation and networking with colleagues are strongly emphasized. Upon completion of the course, participants will receive a certificate of completion.

To enroll in the course, students must have successfully completed NW3C's BDRA course(or equivalent training from another agency), and have at least one year of experience examining digital evidence.

Topics will include:

Day 1:

- Pretest
- Context & Overview
- The Triage Model
- Communicating with the case agent
- Steganography and data hiding

Day 2:

- User profiles
- Chronology & Timelines
- Internet Artifacts
- Small scale digital devices

Day 3:

- Review
- Final Examination