This course provides the technical and legal information prosecutors need to see cases involving digital evidence through the entire criminal justice process, from seizure and extraction to admissibility to verdict. Topics include digital evidence commonly seized during the execution of a search warrant, digital evidence stored remotely by third-party service providers, and the processes investigators use to obtain this evidence (such as the interrogation of digital devices). There is a strong focus on case law and other legal issues surrounding the collection and custody of digital evidence, as well as its use at trial. The course also examines new legislation like the CLOUD Act, which is reforming the digital evidence landscape just as rapidly as the ever-changing case law.

**Evidence stored on devices.** Digital devices and the data they hold.

**Evidence held by third parties.** Cellular service providers, social media platforms, and cloud storage. The implications of *Carpenter* and other recent cases.

**The digital forensics process.** Hashing, validation, imaging, examination, and reporting.

**Case law.** State-specific case law on the seizure, examination, and admissibility of digital evidence. Issues that may arise during motions and/or at trial.

**Building your case.** Effective courtroom presentation of digital evidence. Direct examination of a digital forensic examiner.

To register, visit our training site at:

[www.nw3c.org](http://www.nw3c.org)

Questions? Call 877-628-7674