About Us

For nearly four decades, the National White Collar Crime Center (NW3C) has worked to support state, local, tribal, and territorial law enforcement in the U.S. in efforts to prevent, investigate and prosecute economic and high-tech crime.

Through training and technical assistance in the areas of cybercrime, financial crime and intelligence analysis, NW3C has helped criminal justice personnel keep up with the ever increasing technological aspects of illegal activity. NW3C has trained over 115,000 students from over 68,000 agencies and provided thousands of hours of technical assistance to law enforcement agencies. Since the launch of NW3C's online learning platform in 2014, law enforcement personnel have completed more than 30,000 sessions, from an expanding catalog of online courses.

Instructor Bios

Tyler Wotring
Director
Cyber Forensics

As Director of Cyber Forensics, Mr. Wotring is responsible for overseeing and implementing activity that effectively support NW3C, its services, and its initiatives. Mr. Wotring oversees the planning, assigning, and directing of work; appraising complaints; provides subject matter expertise and technical assistance in the field of Cyber Forensics. Mr. Wotring manages a vast array of personnel located all across the United States.

Prior to being a Director, Mr. Wotring held supervisory and training positions within the Cyber Crimes section. Mr. Wotring provided thousands of hours of training to thousands of State, Local, and Federal law enforcement in data recovery and analysis. The topics range from basic seizing and identifying items of electronic evidence to the analysis of artifacts found in a variety of File Systems and Operating Systems in both a Windows and Mac environments, mobile environments including iOS and Android, as well as through online open source intelligence gathering. Mr. Wotring has also provided technical assistance to law enforcement personnel on cyber forensic topics on hundreds of cases.

Mr. Wotring holds a Master's in Business Administration and a Bachelor's of Science degree in Forensic and Investigative Sciences from West Virginia University.

Kurt Petro
Cyber Crime Specialist

Kurt Petro is a Cyber Crime Specialist with the National White Collar Crime Center's (NW3C) Computer Crime Section (CCS). Kurt is the Mobile/Macintosh Track Lead, Team Lead for the macOS and iOS curriculum and also teaches a number of the CCS courses; including MFA, MDFA, ICI, WinArt, IDRA, BDRA, and STOP. Prior to his tenure at NW3C, Kurt worked for two years at Hewlett Packard (HP) providing computer forensic, eDiscovery, data recovery, and incident response services to HP and outside clients. Kurt was also a non-sworn forensic examiner for McKeesport Police Department for four years. Kurt has also earned a number of certifications during his career; including GCFA, CFCE, MCSE, Network +, and A+.

Course Descriptions

1 DAY Course — Identifying and Seizing Electronic Evidence

This course introduces the information and techniques professionals need to safely and methodically collect and preserve electronic evidence in a forensically sound manner. Students learn to recognize various types of electronic media and hardware used for storing electronic data, including computers, smartphones, tablets, thumb drives, media cards, and more. Topics include the steps involved in orchestrating a digital evidence-based seizure as well as how to identify, preserve, collect, search, package, document, and transfer digital evidence.

- **Preparation.** Be ready to seize items of evidentiary value.
- **Recognition.** Identify sources of electronic evidence in a wide variety of devices.
- **Preservation.** Preserve electronic evidence at the scene so that it can be collected for later analysis.
- **Collection.** Best practices for the seizure of electronic evidence.

2 DAY Course — Social Media and Open Source Intelligence

This course covers the skills professionals need to conduct successful online investigations involving social media. Topics include internet basics such as IP addresses and domains, an overview of currently popular social media platforms, and best practices for building an online undercover profile. Instructors demonstrate both open-source and commercially-available investigative tools for social engineering, information gathering, and artifacts related to social media; as well as automated utilities to capture information and crawl websites.

- **Internet basics.** IP address assignment; resolving domains and IP addresses; networking overview.
- **Popular sites.** Facebook, Twitter, KiK Messenger, Snapchat, Instagram, tumblr, and more.
- **Tools and techniques.** Use open-source and commercial products to capture information and artifacts and crawl websites. Best practices for investigative user accounts.
- **Hands-on experience.** Use many different free open-source advanced search techniques, sites, and tools to help socially engineer and gather information. Participate in live demonstrations. (Requires Facebook, Twitter, and Instagram accounts.)

Instructors conduct live demonstrations using sites that require login credentials. Students who want to participate may bring their own laptop, and must create accounts on the following sites prior to coming to class.

- Gmail
- Facebook
- Twitter
- Instagram