This course will provide investigators with the skills, knowledge and ability to successfully utilize technology in their investigations. This course is an elective course within the POST Robert Presley Institute of Criminal Investigations (ICI).

The online format for this course will be held through in a live, interactive Zoom platform. During the live session, Government Training Agency (GTA) staff will be online with the instructor throughout the course to assist in verifying student identities and ensure student participation in course activities, which include facilitated discussions, breakout groups and the use of the chat box for questions. Students attending the course will be required to pre-register through GTA’s website and registration system. GTA staff will verify student registration in the course, prior to sending out course confirmation letters with a unique private access code for the live session. Students must be attached to an agency, using a departmental email and will be required to have a computer with a camera and microphone for their participation in the course. Prior to the start of the course, students will be held in a waiting room until student identities can be verified against the approved student roster. All student learning during the course will be verified through facilitated discussion and learning activity debriefings with the instructor. For small group work done in breakout rooms, the instructor will have the ability to move freely between the breakouts to observe group work and groups will report back in the main room on work products or discussions created in breakout rooms.

1. Course Administration & Scenario Introduction
   1. 1052(e) Specifications
      1. 1052(e) – A: Method in which trainee attendance is verified - Students will be provided an online access code to attend session prior to the session. Upon logging on to the course, they will be placed into an online “waiting room” and allowed entry into the actual course once their name has been reconciled against the approved course roster by either the instructor or staff online providing technical support.
      2. 1052(e) – A: Method in which course completion is verified – Students will be required to have their cameras on during the duration of the course and participate in both discussions in the main session as well as in breakout sessions. Instructor and GTA support staff will verify involvement and confirm students return after breaks to ensure they do not miss more than the allowable time under POST guidelines.
      3. 1052(e) – A1: Online Registration – Students will register prior to the online session and receive an unique access code for the course
      4. 1052(e) – A2: Audio or Text – Students will engage in the course via both audio (through their computer sound or microphone) and text through a chat box feature in the online platform
      5. 1052(e) – A3: Video Transmission of Trainee – Students will be live through an online platform (ex. Zoom), which allows all students to view the instructor(s) and other student participant(s) throughout the duration of the course. As such, students are required to have a camera on their computer to attend this course. No call-ins will be allowed.
      6. 1052(e) – B, Subsections 1-2: Method in which trainee interaction with the instructor for questions or exercises occurs. Students will be involved in exercises throughout the training which involve the use of audio, text and video transmission during the live online training. Students will also be able to ask or address questions using audio, text and video throughout the entire training.
      7. 1052(e) – C1: Method in which instructor evaluates trainee performance and verifies the learning took place – Students will be involved in facilitated dialogue, case studies and breakout group work throughout the training. During each opportunity, the instructor will verify learning by feedback provided from the groups and their work on the case studies.
      8. 1052(e) – C2: This course is not a tapped webinar, but will be run live in a forum that allows for real time interaction between the instructors and students. This course will not be recorded.
   2. Introductions & Overview
      1. Course Introduction & Online Platform Skills
      2. Discuss online format and expectations for participation and credit
      3. Student Introductions
      4. General course guidelines and safety
   3. Case Scenarios
2. Wireless Devices
   1. Types of Wireless Devices
      1. GPS
      2. Cellular Phones
      3. PDA
      4. Gaming Devices
      5. E-Readers
      6. Netbooks
      7. Routers
      8. Printers
      9. Bluetooth Devices
      10. Blu-Ray Devices
      11. Storage Devices
      12. Digital Cameras
   2. Criminal Applications
      1. Data Storage
      2. Case examples
3. Investigative Searches & Resources  
    A. Investigating Searches
   * 1. Locating people
     2. Tracking suspect activity
     3. Tracking monitored offenders with GPS
     4. Locating property
     5. Digital Evidence
   1. Resources
   2. Search Engines
      1. Personal Information
      2. Employers and Employment History
      3. Social Networking History
      4. Other
      5. Images
      6. Archival Data
      7. Research and Information
   3. Types of Search Engines
      1. Free  
         2. Subscription/Fee Based
   4. How Search Engines collect data
      1. Spider and Crawling
      2. Resources
   5. Advanced Internet Searches and Resources
      1. Google Features
      2. Case examples
4. Introduction to IP Tracing
   1. IP Tracing
      1. What is an IP address?
      2. Internet Service Providers
      3. URL and DNS
      4. Types of IP addresses
      5. Variants of IP addresses
      6. Internet Resources
   2. Introduction to Email structures and breakdown
      1. Locating Headers
      2. Reading Headers
   3. Case examples
   4. Practical Application
5. Cellular Telephone Technology
   1. Introduction to the cell phone
      1. Misconceptions of cellular phones
      2. Basic Components of a wireless network
   2. Cell phone evidence
   3. Cell Phone Search
      1. Information available from the Wireless Carrier
      2. Requesting information from Wireless Carrier
   4. Case examples
   5. Practical Application
      1. Cell Phone Tracking
      2. Cell Phone Mapping
      3. Meta Data
6. Social Media
   1. Introduction to Social Media
      1. Introduction to Social Networking sites
      2. What is a Social Network?
      3. Case examples
   2. Legal & Illegal purposes
   3. Investigative Tools
   4. Resources
   5. Practical Application
7. Surveillance
   1. Why use Electronic Surveillance?
   2. Overview of surveillance options
      1. Video monitoring
      2. Audio intercepts
      3. GPS tracking
      4. Other
   3. Legal Issues
      1. Requirements
      2. Court authorization
8. Search Warrants
   1. What sources of electronic information are available?
      1. Cellular telephones
      2. Computers
      3. Requesting Information
      4. Resources
   2. Who has the information?
   3. How do you request the information?
   4. Case examples
9. Electronic Takedown protocols
   1. Electronic Evidence and Seizure
      1. Recognizing Potential Electronic Evidence
      2. Sources of Evidence
      3. Preserving Digital Evidence
   2. Obtaining/Seizing Digital Evidence
      1. Legal Aspects
      2. Case examples
   3. Take-down Protocol
      1. Stand Alone (personal or non-networked) computer
      2. Networked computer
      3. Cell Phone
      4. Facsimile Machine
      5. Caller ID devices
      6. Smart Cards
      7. Other Electronic Storage Devices
      8. Legal Issues
10. Computer Crime Statutes & Legal Issues
    1. Federal Privacy Laws
       1. There are a series of federal laws that govern the collection and use of information. These laws are important for investigators, prosecutors, and IT personnel.
       2. These laws protect the privacy of electronic records and communications, limit the ability of the government to access these records, and set punishment for improper access
       3. The Electronics Privacy Act
       4. The Cable Act
       5. The Federal Education Records Protection Act
       6. HIPPA
    2. Electronic Communication Privacy Act 18 U.S.C. 2510 et seq. (ECPA)
       1. What Does ECPA Protect?
       2. Types of data under ECPA
       3. When Does ECPA Apply?
       4. Is it an Electronic Communication?
       5. Four Exceptions
       6. ECPA Analysis
    3. Types of Communications
       1. Communication in transit
       2. Communications in storage
       3. Storage Examples
       4. Interception Communications in Transit
    4. Wiretap Order
       1. A federal prosecutor can obtain a wiretap order to investigate any felony crime under 18 U.S.C. 2516(3).
       2. A CA State prosecutor can obtain a wiretap order only if the state authorizes the issuance of the order by law.
    5. Exceptions
       1. Consent Exception
       2. Provider Protection Exception
       3. Trespasser Exception
       4. Inadvertently Obtained Communications
    6. Electronic Communication Service (ECS)
       1. ECS refers to an “Electronic Communication Service” under 18 U.S.C. 2510(15)
       2. ECS or Non ECS
       3. ECS release Rules
       4. Is it stored by an RCS? RCS refers to a ‘Remote Computing Service” referenced in 18 U.S.C. 2711(2)
       5. RCS Release Rules
       6. Voluntary Disclosure
       7. Old Messages
       8. Notice Requirement
       9. Basic Subscriber Information
       10. Transactional Records
       11. Preservation letter
       12. Section 2703(d) Orders
       13. No Statutory Suppression
       14. FERPA – Family Educational Rights and Privacy Act
       15. CSPA - Cable Subscriber Privacy Act
       16. Privacy Protection Act
       17. Basic PPA Rule
       18. “Work Product”
       19. The PPA and the Internet
       20. Remedies for Violations
       21. Best Practice
       22. Other Legal Issues
       23. Marsy’s Law