C3 United States Army Criminal Investigation Command (USACIDC) Digital Forensics: A Program Overview

Patrick A. Eller, MS, USACIDC, 27130 Telegraph Road, Quantico, VA 22134; Joseph Levi White, MS*, US Army Criminal Investigation Laboratory, Digital Evidence-CFI, 4930 N 31st Street, Forest Park, GA 30297*

After attending this presentation, attendees will have gained information on the organizational structure and capabilities of the USACIDC's current digital forensics programs.

This presentation will impact the forensic science community by providing an overview of the services offered to assist criminal investigations involving Digital and Multimedia Evidence (DME) within the United States military.

As the United States Army's primary criminal investigative organization and the Department of Defense's (DoD's) premier investigative organization, the USACIDC, commonly known as CID, is responsible for conducting criminal investigations in which the United States Army is, or may be, a party of interest. The mission of the USACIDC is to investigate and deter serious crimes in which the Army has an interest. The USACIDC collects, analyzes, processes, and disseminates criminal intelligence; conducts protective service operations; provides forensic laboratory support to all DoD investigative agencies; and maintains Army criminal records. The USACIDC also provides criminal investigative support to all United States Army elements and deploys on short notice in support of contingency operations worldwide. The USACIDC Special Agents primarily investigate felony-level crime across the Army and provide investigative support to field commanders. They conduct a wide variety of investigations to include deaths, sexual assault, armed robbery, procurement fraud, computer crimes, counter-drug operations, and war crimes. The USACIDC agents also provide counter-terrorism support, criminal intelligence support, force protection, forensic laboratory investigative support, and protective services for key DoD and senior Army leadership.[1]

Within the hierarchy of the USACIDC, there are two individual organizations that share the responsibility for processing and examining DME to assist in Army criminal investigations: the USACIDC Computer Crimes Program (CCP) and the United States Army Criminal Investigation Laboratory's (USACIL) Documents and Digital Evidence (D2E) Branch.

Along with an overview of the organizational structure of the two USACIDC programs, attendees will be provided with much more information regarding each organization's capabilities, specializations, and examinations. This presentation will describe the types of examinations typically conducted in addition to an outline of the typical types of crimes investigated. This presentation will also include an overview of the anticipated future of the programs, current and anticipated evidence-processing issues, and a potential shift from reactive dead-box forensics to more proactive roles in investigations involving Internet Crimes Against Children (ICAC) and the National Center for Missing and Exploited Children (NCMEC).

The opinions or assertions contained herein are the private views of the author and are not to be construed as official or as reflecting the views of the Department of the Army or the Department of Defense. Names of commercial manufacturers or products included are incidental only, and inclusion does not imply endorsement by the authors, the Defense Forensic Science Center (DFSC), the Office of the Provost Marshal General (OPMG), the Department of the Army (DA), or the DoD.

Reference(s):

1. United States Army Criminal Investigation Command. 2017. Accessed August 09, 2017. http://www.cid.army.mil/.

Army, Military, Program Overview

*Presenting Author