Course Description

DF310 ADFA-Win	Advanced Digital Forensic Analysis: Windows
Digital Forensics	This course covers the identification and extraction of artifacts associated with the Microsoft Windows operating system. Topics include the Change Journal, BitLocker, and a detailed examination of the various artifacts found in each of the Registry hive files. Students also examine Event Logs, Volume Shadow Copies, link files, and thumbnails. This course uses a mixture of lecture, discussion, demonstration, and hands-on exercises.
Classroom course	
4 days	
Prerequisite: None	

To register, visit our training site at:

www.nw3c.org

Questions? Call 877-628-7674

Version 4.0, updated November 2018

"This project was supported by Grant No. 2018-MU-BX-K001 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Department of Justice's Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the SMART Office. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice."