SANS DFIR Stay Sharp series are 2-to-3-day courses that teach specialized topics which also follow the core concepts covered in SANS Digital Forensics and Incident Response 6-day courses. The instructional material in each Stay Sharp course has been carefully selected by SANS DFIR Curriculum authors to help students learn or sharpen a specific technical knowledge or skill in a more targeted, faster learning setting without sacrificing teaching quality or course in-depth technical content.

Here is what you can expect when you take a SANS DFIR Stay Sharp course:

- Instructor-led training taught by the world’s leading DFIR professionals.
- Quality training with less time away from work and home responsibilities.
- Targeted short courses to help you build specific skills that you can apply the same week you take your course.
- Virtual, livestream training delivered Live Online.

“The content squeezed into two days of this course is more than I could have learned on my own in six months. The resources and materials shared are going to be hugely valuable.”
— Benedict Donaldson, Dyson

First DFIR Stay Sharp Event

DFIR Stay Sharp courses are now available and are scheduled to start April 19th.

For more information or to register visit [here](#).
FOR498A: Forensic Data Acquisition (3 DAYS)

FOR498A teaches the latest tools, digital container access techniques, and enterprise methodologies to identify, access, and preserve evidence across a vast range of devices, repositories, and non-traditional storage areas. Learn how to extract actionable intelligence in 90 minutes or less. MORE

JOB ROLES: Federal Agents and Law Enforcement Personnel, First Responders, Digital Forensic Analysts, Information Security Professionals, Incident Responders, Media Exploitation Analysts, Department of Defense and Intelligence Community Professionals, and anyone interested in an understanding of the proper preservation of systems

ASSOCIATED 6-DAY COURSE: FOR498: Battlefield Forensics & Data Acquisition

FOR572A: Lethal Network Forensics (2 DAYS)

FOR572A teaches the three primary sources of network-based evidence: full packet capture, NetFlow, and logs. Whether used together or separately, or in conjunction with host-based evidence or alone, these sources can provide critical insight into the actions attackers have taken or continue to take in their victims’ environment. MORE

JOB ROLES: Incident Responders, Threat Hunters, Security Operations Center (SOC) personnel, Law Enforcement officers, Federal agents, Detectives, Network Defenders, Information Security Managers, Network engineers, IT Professionals, and anyone interested in computer network intrusions and investigations

ASSOCIATED 6-DAY COURSE: FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response

FOR585A: iOS Forensic Analysis (2 DAYS)

FOR585A teaches the proper handling and parsing skills needed to bypass locked iOS devices and correctly interpret the data. It delves into the iOS file system and discusses common areas containing files of evidentiary value. This course will prepare you to deal with the iOS device that will likely be a major component in a forensic investigation. MORE


ASSOCIATED 6-DAY COURSE: FOR585: Smartphone Forensic Analysis In-Depth

FOR610A: Introduction to Malware Analysis: Hands-on and Technical (2 DAYS)

FOR610A supercharges your incident response and forensics skills by teaching you how to use key malware analysis tools and techniques. This practical, hands-on course builds upon your existing network, system and InfoSec skills and teaches you how to turn Windows and related malware inside out. MORE

JOB ROLES: Malware Analysts, Incident Responders, Forensic Investigators, Information Security Professionals, Threat Intelligence Professionals, and Threat Hunters

ASSOCIATED 6-DAY COURSE: FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques

Have questions? Visit here.