NETWARS DFIR CONTINUOUS

SANS

Master the latest skills and technologies in the industry with NetWars DFIR Continuous. All the tools needed are included with each training solution.

NetWars DFIR Continuous

Take on the role of cyber investigator and uncover key clues from the evidence. The range guides you through a series of challenges to reveal key facts within files, processes, and common programs.

Example Topics

- Windows/Endpoint incident response
- Windows forensics
- Mac forensics
- Network forensics
- Cyber threat intelligence
- Smartphone/mobile forensics
- Malware analysis

Example Tasks

Discover embedded metadata in images and documents, review and extract info from PCAP files, review social media tickets and identify suspicious accounts, find last users of applications on IOS devices, analyze a malware executable file, and more.

Suggested Tools

MemProcFS, Registry Explorer, ExifTool, FTK Imager, Arsenal Image Mounter, Wireshark, SIFT Workstation, NetFlow, iBackupBot, EvtxExplorer, and others.

Computer Requirements

- Processor: 64-bit, x86, 2.0 GHz+
- Memory: 16GB
- HD: 200GB+ Free, plus 50GB download of evidence files and virtual machines
- Interface: USB 3.0 | Type-A
- OS: Windows, Mac and Linux
- VMware (Students are expected to either provide their own forensics tools or use the local VMware VM tools that we provide.)