مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

# پکیج فارنزیک سنز | SANS Forensics Pack

رهگیری جرم سایبری (دوره FOR۵۷۲ & FOR۵۰۰)

## مروری بر دوره

این دوره ذهن شما را در زمینه تجزیه، تحلیل و بررسی دقیق اطلاعات آماده می کند و ذهن فعالی در حوزه رهگیری جرم خواهید داشت. این دوره به گونه ای طراحی شده که از مفاهیم پایه مرحله به مرحله آموزش داده می شود، دانشجویان در این دوره دانش عمیق و جامعی از رهگیری جرم سایبری در سیستم عامل ویندوز و شبکه ارتباطی به دست آورده و خواهند آموخت که روش های رهگیری جرم سایبری را در موارد مختلف و موقعیت های متفاوت به کار گیرند و به آن ها این امکان را می دهد در دنیای واقعی روش مناسب را برای دستیابی به بهترین نتیجه انتخاب کنند.

## سرفصل ها

FOR۵۰۰: Windows Forensic Analysis

- Digital Forensics and Advanced Data Triage
- Registry Analysis, Application Execution, and Cloud Storage Forensics
- Shell Items and Removable Device Profiling
- Email Analysis, Windows Timeline, SRUM, and Event Logs
- Web Browser Forensics

FOR۵۷۲: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response

- Off the Disk and Onto the Wire
- Core Protocols & Log Aggregation/Analysis
- NetFlow and File Access Protocols

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

- Commercial Tools, Wireless, and Full-Packet Hunting
- Encryption, Protocol Reversing, OPSEC, and Intel

## پیش نیاز ها

- گذراندن دوره نتورک پلاس و یا بهره مندی از دانشی در سطح آن