ارژنگ
مؤسسه آموزش عالی آزاد

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

# دوره **SANS Forensics Pack** | سطح ۳

سطح پیشرفته - کد دوره های: FOR۵۰۰-FOR۵۲۶-FOR۵۸۵-FOR۶۱۰

## مروری بر دوره

شرکتSANS یکی از بزرگترین شرکت های آموزشی در دنیا می باشد که هدف آن آموزش شرکت ها و سازمان ها در حوزه های تست نفوذ و فارنزیک و Cyber Defense براساس دوره های SANS Forensics Pack Level ۳ می باشد دوره فارنزیک شرکتSANS طراحی شده است و هدف این پکیج آموزشی فارنزیک یا جرم شناسی در حوزه های سیستم عامل ویندوز و Threat Hunting و شبکه می باشد دانشجویان در این دوره آموزشی می توانند به عنوان یک متخصص جرم های سایبری که در سطح شبکه و یا سیستم عامل ویندوز اتفاق افتاده است را شناسایی کنند این دوره جز دوره های خاص امنیت بحساب می آید و متخصصین کمی را در دنیا شامل می شود و نیاز سازمان ها و شرکت ها به این افراد بسیار زیاد می باشد لذا بازار خوبی را برای متخصصین این حوزه ایجاد کرده است.

## آنچه در این دوره خواهید آموخت

- آشنایی با روش ها و تکنیک های جرم شناسی برروی سیستم عامل ویندوز
- آشنایی با روش ها و تکنیک های پیشرفته برای آنالیز RAM برای فرآیند جرم شناسی
- آشنایی و آنالیز Malware با استفاده از روش های Static و Dynamic و Reverse Engineering
- PWK و یا CEH یا SANS Pack Level ۱

## سرفصل ها

## FOR500.1: Digital Forensics and Advanced Data

# Triage

- Windows Operating System Components
  - Key Differences in Modern Windows Operating Systems
- Core Forensic Principles
  - Analysis Focus
  - Determining Your Scope
  - Creating and Investigative Plan
- Live Response and Triage-Based Acquisition Techniques
  - RAM Acquisition and Following the Order of Volatility
  - Triage-Based Forensics and Fast Forensic Acquisition
  - Encryption Detection
  - Registry and Locked File Extraction
  - Leveraging the Volume Shadow Service
  - KAPE Triage Collection

- Windows Image Mounting and Examination
- NTFS File System Overview
- Document and File Metadata
- File and Stream Carving
    - Principles of Data Carving
    - Recovering File System Metadata
    - File and Stream Carving Tools
    - Custom Carving Signatures
- Memory, Pagefile, and Unallocated Space Analysis
    - Artifact Recovery and Examination
    - Chat Application Analysis
    - Internet Explorer, Edge, Firefox, Chrome, and InPrivate Browser Recovery
    - Email and Webmail, including Yahoo, Outlook.com, and Gmail

## FOR500.2: Registry Analysis, Application

## Execution, and Cloud Storage Forensics

- Registry Forensics In-Depth
- Registry Core
  - Hives, Keys, and Values
  - Registry Last Write Time
  - MRU Lists
  - Deleted Registry Key Recovery
  - Identify Dirty Registry Hives and Recover Missing Data
  - Rapidly Search and Timeline Multiple Hives
- Profile Users and Groups
  - Discover Usernames and Relevant Security Identifiers
  - Last Login
  - Last Failed Login
  - Login Count
  - Password Policy
- Core System Information

  - Identify the Current Control Set
  - System Name and Version
  - Document the System Timezone
  - Wireless, Wired, VPN, and Broadband Network Auditing
  - Perform Device Geolocation via Network Profiling
  - Identify System Updates and Last Shutdown Time
  - Registry-Based Malware Persistence Mechanisms
- User Forensic Data
  - Evidence of File Downloads
  - Office and Microsoft 365 File History Analysis
  - Windows 7, Windows 8/8.1, Windows 10 Search History
  - Typed Paths and Directories
  - Recent Documents (RecentDocs)
  - Open Save/Run Dialog Boxes Evidence
  - Application Execution History via UserAssist,

Prefetch, Windows 10 Timeline, System Resource Usage Monitor (SRUM), and BAM/DAM

- Cloud Storage Forensics
  - Microsoft OneDrive
  - OneDrive Files on Demand
  - Microsoft OneDrive for Business
  - OneDrive Unified Audit Logs
  - Google Drive
  - Google Workspace (G Suite) File Stream
  - Google Workspace (G Suite) Logging
  - Dropbox
  - Dropbox Decryption
  - Dropbox Logging
  - Box Drive
  - Box Backup and Sync
  - Synchronization and Timestamps
  - Forensic Acquisition Challenges
  - User Activity Enumeration

# FOR500.3: Shell Items and Removable Device Profiling

- Shell Item Forensics
  - Shortcut Files (.lnk) - Evidence of File Opening
  - Windows 7-10 Jumplists - Evidence of File Opening and Program Execution
  - Shellbag Analysis - Evidence of Folder Access
- USB and BYOD Forensic Examinations
  - Vendor/Make/Version
  - Unique Serial Number
  - Last Drive Letter
  - MountPoints2 Last Drive Mapping Per User (Including Mapped Shares)
  - Volume Name and Serial Number
  - Username that Used the USB Device
  - Time of First USB Device Connection
  - Time of Last USB Device Connection

  - Time of Last USB Device Removal
  - Auditing BYOD Devices at Scale

## FOR500.4: Email Analysis, Windows Timeline, SRUM, and Event Logs

- Email Forensics
  - Evidence of User Communication
  - How Email Works
  - Email Header Examination
  - Email Authenticity
  - Determining a Sender's Geographic Location
  - Extended MAPI Headers
  - Host-Based Email Forensics
  - Exchange Recoverable Items
  - Exchange Evidence Acquisition and Mail Export
  - Exchange Compliance Search and eDiscovery
  - Unified Audit Logs in Office 365

  - Google Workspace (G Suite) Logging
  - Recovering Data from the Google Workspace (G Suite)
  - Web and Cloud-Based Email
  - Webmail Acquisition
  - Email Searching and Examination
  - Mobile Email Remnants
  - Business Email Compromise
- Forensicating Additional Windows OS Artifacts
  - Windows Search Index Forensics
  - Extensible Storage Engine (ESE) Database Recovery and Repair
  - Thumbs.db and Thumbcache Files
  - Windows Recycle Bin Analysis (XP, Windows 7-10)
  - Windows 10 Timeline Activities Database
  - System Resource Usage Monitor (SRUM)
    - Connected Networks, Duration, and Bandwidth Usage

        - Applications Run and Bytes Sent/Received Per Application
        - Application Push Notifications
        - Energy Usage
- Windows Event Log Analysis
    - Event Logs that Matter to a Digital Forensic Investigator
    - EVTX and EVT Log Files
        - Track Account Usage, including RDP, Brute Force Password Attacks, and Rogue Local Account Usage
        - Audit and Analyze File and Folder Access
        - Prove System Time Manipulation
        - Track BYOD and External Devices
        - Microsoft Office Alert Logging
        - Geo-locate a Device via Event Logs

## FOR500.5: Web Browser Forensics

- Browser Forensics
    - History
    - Cache
    - Searches
    - Downloads
    - Understanding Browser Timestamps
    - Chrome
        - Chrome File Locations
        - Correlating URLs and Visits Tables for Historical Context
        - History and Page Transition Types
        - Chrome Preferences File
        - Web Data, Shortcuts, and Network Action Predictor Databases
        - Chrome Timestamps
        - Cache Examinations
        - Download History
        - Web Storage, IndexDB, and the HTML5 File

        System
    - Chrome Session Recovery
    - Chrome Profiles Feature
    - Identifying Cross-Device Chrome Synchronization
- Edge
    - Chromium Edge vs. Google Chrome
    - History, Cache, Cookies, Download History, and Session Recovery
    - Microsoft Edge Collections
    - Edge Internet Explorer Mode
    - Chrome and Edge Extensions
    - Edge Artifact Synchronization and Tracking Multiple Profiles
    - Edge HTML and the Spartan.edb Database
    - Reading List, WebNotes, Top Sites, and SweptTabs
- Internet Explorer
    - IE Forensic File Locations

    - History Files: Index.dat and WebCache.dat
    - Cache Recovery and Timestamps
    - Microsoft Universal Application Artifacts
    - IE Download History
    - Gaining Access to Credentials Stored in the Windows Vault
    - Internet Explorer Tab Recovery Analysis
    - Cross-Device Synchronization, Including Tabs, History, Favorites, and Passwords
  - Firefox
    - Firefox Artifact Locations
    - SQLite Files and Firefox Quantum Updates
    - Download History
    - Firefox Cache2 Examinations
    - Detailed Visit Type Data
    - Form History
    - Session Recovery
    - Firefox Extensions

        - Firefox Cross-Device Synchronization
    - Private Browsing and Browser Artifact Recovery
        - IE and EdgeHTML InPrivate Browsing
        - Chrome, Edge, and Firefox Private Browsing
        - Investigating the Tor Browser
        - Identifying Selective Database Deletion
    - SQLite and ESE Database Carving and Examination of Additional Browser Artifacts
        - DOM and Web Storage Objects
        - Rebuilding Cached Web Pages
        - Browser Ancestry

## FOR508.1: Advanced Incident Response & Threat Hunting

### Real Incident Response Tactics

- Preparation: Key tools, techniques, and procedures that an incident response team needs to respond properly to intrusions

- Identification/Scoping: Proper scoping of an incident and detecting all compromised systems in the enterprise
- Containment/Intelligence Development: Restricting access, monitoring, and learning about the adversary in order to develop threat intelligence
- Eradication/Remediation: Determining and executing key steps that must be taken to help stop the current incident and the move to real-time remediation
- Recovery: Recording of the threat intelligence to be used in the event of a similar adversary returning to the enterprise
- Avoiding "Whack-A-Mole" Incident Response: Going beyond immediate eradication without proper incident scoping/containment

## Threat Hunting

- Hunting versus Reactive Response

- Intelligence-Driven Incident Response
- Building a Continuous Incident Response/Threat Hunting Capability
- Forensic Analysis versus Threat Hunting Across Endpoints
- Threat Hunt Team Roles
- ATT&CK - MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK(TM))

## Threat Hunting in the Enterprise

- Identification of Compromised Systems
- Finding Active and Dormant Malware
- Digitally Signed Malware
- Malware Characteristics
- Common Hiding Mechanisms
- Finding Evil by Understanding Normal

## Incident Response and Hunting across Endpoints

- WMIC & PowerShell

- PowerShell Remoting Scalability
- PowerShell Remoting Credential Safeguards
- Kansa PowerShell Remoting IR Framework

## Malware Defense Evasion and Identification

- Service Hijacking/Replacement
- Frequent Compilation
- Binary Padding
- Packing/Armoring
- Dormant Malware
- Signing Code with Valid Certificates
- Anti-Forensics/Timestomping

## Malware Persistence Identification

- AutoStart Locations, RunKeys
- Service Creation/Replacement
- Service Failure Recovery
- Scheduled Tasks

- DLL Hijacking
- WMI Event Consumers

### Investigating WMI-Based Attacks

- WMI Overview
- WMI Attacks Across the Kill Chain
- Auditing the WMI Repository
- WMI File System and Registry Residue
- Command-Line Analysis and WMI Logs
- WMI Process Anomalies

## FOR508.2: Intrusion Analysis

### Stealing and Utilization of Legitimate Credentials

- Pass the Hash
- Single Sign On (SSO) Dumping using Mimikatz
- Token Stealing

- Cached Credentials
- LSA Secrets
- Kerberos Attacks
- NTDS.DIT theft

## Advanced Evidence of Execution Detection

- Attacker Tactics, Techniques, and Procedures (TTPs) Observed Via Process Execution
- Prefetch Analysis
- Application Compatibility Cache (ShimCache)
- Amcache Registry Examination
- Scaling ShimCache and Amcache Investigations

## Lateral Movement Adversary Tactics, Techniques, and Procedures (TTPs)

- Compromising Credentials Techniques
- Remote Desktop Services Misuse
- Windows Admin Share Abuse
- PsExec and Cobalt Strike Beacon PsExec Activity

- Windows Remote Management Tool Techniques
- PowerShell Remoting/WMIC Hacking
- Vulnerability Exploitation

## Log Analysis for Incident Responders and Hunters

- Profiling Account Usage and Logons
- Tracking and Hunting Lateral Movement
- Identifying Suspicious Services
- Detecting Rogue Application Installation
- Finding Malware Execution and Process Tracking
- Capturing Command Lines and Scripts
- PowerShell Transcript and ScriptBlock Logging
- Discovering Cobalt Strike beacon PowerShell Import Activity
- PowerShell Script Obfuscation
- WMI Activity Logging
- Anti-Forensics and Event Log Clearing

# FOR508.3: Memory Forensics in Incident Response & Threat Hunting

## Remote and Enterprise Incident Response

- Remote Endpoint Access in the Enterprise
- Remote Endpoint Host-based Analysis
- Scalable Host-based Analysis (one analyst examining 1,000 systems) and Data Stacking
- Remote Memory Analysis

## Triage and Endpoint Detection and Response (EDR)

- Endpoint Triage Collection
- EDR Capabilities and Challenges
- EDR and Memory Forensics

## Memory Acquisition

- Acquisition of System Memory from both Windows 32/64-bit Systems

- Hibernation and Pagefile Memory Extraction and Conversion
- Virtual Machine Memory Acquisition
- Memory changes in Windows 10
- Windows 10 Virtual Secure Mode

## Memory Forensics Analysis Process for Response and Hunting

- Understanding Common Windows Services and Processes
- Identify Rogue Processes
- Analyze Process DLLs and Handles
- Review Network Artifacts
- Look for Evidence of Code Injection
- Check for Signs of a Rootkit
- Acquire Suspicious Processes and Drivers

## Memory Forensics Examinations

- Live Memory Forensics

- Advanced Memory Analysis with Volatility
- Webshell Detection Via Process Tree Analysis
- Code Injection, Malware, and Rootkit Hunting in Memory
- WMI and PowerShell Processes
- Extract Memory-Resident Adversary Command Lines
- Investigate Windows Services
- Hunting Malware Using Comparison Baseline Systems
- Find and Dump Cached Files from RAM

### Memory Analysis Tools

- Volatility
- F-Response
- Velociraptor
- Comae Windows Memory Toolkit

## FOR508.4: Timeline Analysis

## Malware Defense Evasion and Detection

- Indicators of Compromise - YARA
- Entropy and Packing Analysis
- Executable Anomalies
- Digital Signature Analysis

## Timeline Analysis Overview

- Timeline Benefits
- Prerequisite Knowledge
- Finding the Pivot Point
- Timeline Context Clues
- Timeline Analysis Process

## Filesystem Timeline Creation and Analysis

- MACB Meaning by Filesystem
- Windows Time Rules (File Copy versus File Move)
- Filesystem Timeline Creation Using Sleuthkit and fls
- Bodyfile Analysis and Filtering Using the mactime

Tool

### Super Timeline Creation and Analysis

- Super Timeline Artifact Rules
- Program Execution, File Knowledge, File Opening, File Deletion
- Timeline Creation with log2timeline/Plaso
- log2timeline/ Plaso Components
- Filtering the Super Timeline Using psort
- Targeted Super Timeline Creation
- Super Timeline Analysis Techniques
- Scaling Super Timeline Analysis

## FOR508.5: Incident Response & Hunting Across the Enterprise | Advanced Adversary & Anti-Forensics Detection

### Volume Shadow Copy Analysis

- Volume Shadow Copy Service
- Options for Accessing Historical Data in Volume Snapshots
- Accessing Shadow Copies with vshadowmount
- Volume Shadow Copy Timelining

## Advanced NTFS Filesystem Tactics

- NTFS Filesystem Analysis
- Master File Table (MFT) Critical Areas
- NTFS System Files
- NTFS Metadata Attributes
- Rules of Windows Timestamps for $StdInfo and $Filename
- Detecting Timestamp Manipulation
- Resident versus Nonresident Files
- Alternate Data Streams
- NTFS Directory Attributes
- B-Tree Index Overview and Balancing

- Finding Wiped/Deleted Files using the $I30 indexes
- Filesystem Flight Recorders: $Logfile and $UsnJrnl
- Common Activity Patterns in the Journals
- Useful Filters and Searches in the Journals
- What Happens When Data Is Deleted from an NTFS Filesystem?

### Advanced Evidence Recovery

Markers of Common WIpers and Privacy Cleaners

Deleted Registry Keys

Detecting "Fileless" Malware in the Registry

File Carving

Volume Shadow Carving

Carving for NTFS and Event Log Records

Effective String Searching

NTFS Configuration Changes to Combat Anti-Forensics

### مخاطبان دوره

- کارشناسان شبکه
- کارشناسان امنیت
- علاقمندان به حوزه فارنزیک

## پیش نیاز ها

- PWK و یا CEH یا SANS Pack Level 1

## دوره های مرتبط

دوره Network+ کامپتیا | CompTIA Network+

دوره تست نفوذ SANS Security Pack | سطح ۱