



**Instructor-Led Training (ILT)**

**OSForensics Certification Course**

*<Description>*The 2.5 day *OSForensics Certification Course* is the official product training course offered and developed by PassMark® Software, makers of OSForensics. This interactive course is intended to provide new users of OSForensics with the skills and knowledge necessary to effectively utilize OSForensics as a complete digital forensics and triage solution. The course will prepare students to successfully pass both the OSFTC (OSForensics Triage Certification) and the OSFCE (OSForensics Certified Examiner) certifications which will be administered (optionally) at the end of the course.

*<Prerequisites>*The primary focus of this course will be on the operation of the software and learning to use its many features; NOT on teaching students the foundations of digital forensics. Although not required, it is recommended that students:

* Have a basic knowledge of computer forensic investigations, procedures and terms
* Are comfortable working with the Microsoft Windows Operating System
* Understand material presented in the English language

*<Hardware Prerequisites>*Students are required to provide their own laptop for use during the hands-on exercises and testing. Laptops should meet the following minimum specifications:

* CPU: Intel-based / Core 2 Duo or better
* RAM: Minimum 8GB’s
* Operating System: Windows 7 - 10

*<Schedule>*

* *Day 1 – 8:00 am to 5:00 pm (Lunch on your own 11:50-1:00)*
* *Day 2 – 8:00 am to 5:00 pm (Lunch on your own 11:50-1:00)*
* *Day 3 – 8:00 am to 12:00 pm*

 *<DAY 1>…………………………………………………………………………………………….*

**1. Introductions & Housekeeping (8:00AM – 8:50AM)** 1.1 – Company Intro
 1.2 – Course Objectives
 1.2.1 – Review Course Schedule
 1.3 – Instructor Intro
 1.4 – Student Intros
 1.5 – System Requirements
 1.6 – OSF Licensing & Options
 1.7 – OSF EULA
 1.8 – *Copy Training Files to Student Computers*

**2. Intro to Computer Forensics (9:00AM – 9:10AM)**
 2.1 – Best Practices
 2.2 – Legal Issues

**3. Getting Started (9:10AM – 9:50AM)**
 3.1 – Installing OSForensics
 3.1.1 – Directory Structure
 3.2 – Installing to USB
 3.2.1 – *Create an OSF USB* 3.2.2 – *Create a Bootable OSF USB* 3.3 - Creating a Case
 3.4 - Case Log Options
 3.5 - Adding Devices
 3.6 - Editing a Case
 3.7 - Case Report & Narrative Options
 3.8 - Offloading & Loading a Case
 3.9 – *Practical Exercise*

**4. OSForensics Workflow (10:00AM – 10:15AM)**
 4.1 – Developing Your Workflow for Live Analysis
 4.2 – Developing Your Workflow for Offline Analysis
 4.3 – *Practical Exercise*

**5. Features & Modules (10:15AM – 5:00PM)
 5.1 - System Information (10:15AM – 10:30AM)** 5.1.1 - Creating Custom Presets
 5.1.2 - 3rd Party Compatibility
 5.1.3 – Creating a System Information Report/Adding Artifacts to your Case
 5.1.4 – *Practical Exercise*

 **5.2 – Memory Viewer (10:30AM – 10:50AM)** 5.2.1 – Live Memory Analysis
 5.2.2 – Capturing RAM
 5.2.3 – Static Memory Analysis
 5.2.4 – Volatility Workbench
 5.2.5 – *Practical Exercise*

 **5.3 – Recent Activity (11:00AM – 11:50AM)** 5.3.1 – Overview of Artifacts Extracted
 5.3.2 – Sorting
 5.3.3 – Creating a Timeline Report/Adding Artifacts to Your Case
 5.3.4 – *Practical Exercise*
 *(LUNCH BREAK 11:50AM – 1:00PM))*

 **5.4 – Passwords (1:00PM – 1:50PM)** 5.4.1 – Overview of Passwords Extracted
 5.4.2 – Decrypting Windows User Passwords
 5.4.3 – File Decryption
 5.4.4 – Creating a Passwords Report/Adding Artifacts to Your Case
 5.4.5 – *Practical Exercise*

 **5.5 – File Name Search (2:00PM – 2:30PM)** 5.5.1 – Navigating the Presets
 5.5.2 – Utilizing the Search Box
 5.5.3 – Creating Custom Presets
 5.5.4 – Sorting Options (by Color)
 5.5.5 – Reviewing Compound (Compressed) Files
 5.5.6 – Creating a FNS Report/Adding Artifacts to Your Case
 5.5.7 – *Practical Exercise*

 **5.6 – Deleted File Search (2:30PM – 2:50PM)** 5.6.1 – Default File Recovery with Search Presets
 5.6.2 – Data Carving Options
 5.6.3 – Advanced Carving Options
 5.6.4 – Creating a Deleted File Report/Adding Artifacts to Your Case
 5.6.5 – *Practical Exercise*

 **5.7 – Mismatch File Search (3:00PM – 3:15PM)** 5.7.1 – How it works
 5.7.2 – Understanding the Filters
 5.7.3 – Creating a Mismatch File Search Report/Adding Artifacts to Your Case

 **5.8 – Create Index (3:15PM – 3:50PM)** 5.8.1 – Creating a Basic Index
 5.8.2 – Creating Custom Indexing Templates
 5.8.3 – Understanding the Options (Extensions, Skip Lists, Languages & Stemming)
 5.8.4 – *Practical Exercise*

 **5.9 – Search Index (4:00 – 4:50PM)** 5.9.1 – Choosing an Index
 5.9.2 – Using Word Lists
 5.9.3 – Creating a Word List
 5.9.4 – Reviewing Results
 5.9.5 – *Practical Exercise*

 *<DAY 2>…………………………………………………………………………………………….*

 **5.10 – Prefetch Viewer (8:00AM – 8:15AM)** 5.10.1 – Understanding the Windows Prefetch
 5.10.2 – Application Names, Run Counts, Mapped Files & More
 5.10.3 *–* Creating a Prefetch Report/Adding Artifacts to Your Case5.10.4 – *Practical Exercise*

 **5.11 – Registry Viewer (8:15 – 8:50AM)** 5.11.1 – Identifying Hives of Interest
 5.11.2 – Analyzing a Windows User Account in the SAM Hive (Hex to ASCII)
 5.11.3 – Locating USB devices in the SYSTEM Hive
 5.11.4 – Analyzing the NTUSER.DAT
 5.11.5 – Examining Hives that haven’t been Added to the Case
 5.11.6 – Adding keys of interest to the Case
 5.11.7 – *Practical Exercise*

 **5.12 – File System Browser / File Viewer / String Extraction (9:00AM – 9:40AM)** 5.12.1 – Exploring File Systems (Windows, Mac, Linux)
 5.12.2 – Available Options (Show Hidden Files)
 5.12.3 – Right-Click Options (Add to Logical Image)
 5.12.4 – Viewing Files with OSF’s File Viewer (Image, Video, Word Doc, Pagefile,
 Executable)
 5.12.5 – String Extraction
 5.12.6 – *Short Practical Exercise*

 **5.13 – SQLite DB Browser (9:40AM – 9:50AM)** 5.13.1 – Examining a SQLite DB with OSF
 5.13.2 – Adding Artifacts of Value to Your Case

 **5.14 – Web Browser (10:00AM – 10:15AM)** 5.14.1 – Screen Capturing
 5.14.2 – Saving Webpages
 5.14.3 – *Practical Exercise*

 **5.15 – Raw Disk Viewer (10:15AM – 10:30AM)** 5.15.1 – Viewer & Options
 5.15.2 – Manual File Carving
 5.15.3 – Using Regular Expressions
 5.15.4 – *Practical Exercise*

 **5.16 – Verify / Create Hash (10:30AM – 10:50AM)** 5.16.1 – Hashing a File
 5.16.2 – Hashing a Disk Image
 5.16.3 – *Practical Exercise*

 **5.17 – Hash Sets (11:00AM – 11:30AM)** 5.17.1 – Installing Hash Sets
 5.17.2 – Searching for Known Files
 5.17.3 – *Practical Exercise*

 **5.18 – Create & Compare Signatures (11:30AM – 11:50AM)** 5.18.1 – Uses for Feature
 5.18.2 – Creating a Signature
 5.18.3 – Compare a Signature
 5.18.4 – Identifying Deleted, Modified and Duplicate Files
 5.18.5 – Creating a File List
 5.18.6 – *Practical Exercise*

*<Lunch Break – 11:50AM – 1:00PM)*

 **5.19 – Advanced / Other Features (1:15PM – 1:50PM)** 5.19.1 – USN Journal Viewer
 5.19.2 – PLIST Viewer
 5.19.3 – ESE Database Viewer
 5.19.4 – Email Viewer
 5.19.5 – Thumbcache Viewer
 5.19.6 – Volume Shadow Copy Analysis
 5.19.7 – *Practical Exercises*

 **5.21 – Imaging / Housekeeping (2:00PM – 2:15PM)** 5.21.1 – Drive Preparation
 5.21.2 – Disk Imaging
 5.21.2.1 – Disk Imaging
 5.21.2.2 – Restoring an Image to Disk
 5.21.2.3 – HPA/Detection
 5.21.2.4 – RAID Rebuilding
 5.21.2.5 – Custom Logical Imaging
 5.21.3 – *Practical Exercise*
 5.21.4 – Debug Logs

 **5.22 – Generating Your Case Report (2:15PM – 2:40PM)** 5.22.1 – Narrative
 5.22.2 – Report Templates
 5.22.3 – Report Options
 5.22.4 – Adding External Reports
 5.22.5 – *Practical Exercise*

**6. Free Tools from PassMark Software (2:40PM – 2:50PM)** 6.1 – OSFMount
 6.2 – OSFClone
 6.3 – ImageUSB
 6.4 – Volatility Workbench
 6.5 – Other Free Tools from PassMark Software

**7. Practical Exercise (3:00PM – 5:00PM)** 7.1 – *Work Entire Case from Start to Finish (Graded)*

*<Day 3…>*

**8. OSForensics Triage Certification (OSFTC) - (8:00AM – 10:00AM)** 8.1 – Register for an Account at PassMark.com (8:00AM – 8:20AM)
 8.2 – OSFTC Review (OSForensics Triage Certification) (8:20AM – 8:50AM)
 8.3 – OSFTC Test (9:00AM – 9:50AM)

**9. OSForensics Certified Examiner (OSFCE) -** **(10:00AM – 12:00PM)**
 9.1 – OSFCE Review (10:00AM – 10:40AM)
 9.2 – Q&A session (10:40AM – 10:50AM)
 9.3 – OSFCE Test (11:00AM – 12:00PM)

<…CLASS DISMISSED AT 12:00PM…>