Training course outline

ITU and Naif Arab University for Security Sciences (NAUSS)

Title	**Windows Forensic Analysis**
Modality	Online Instructor led
Dates	30-31 March 2022
Duration	2 days
Registration deadline	23 March 2022
Training fees	0 USD (Free)
Description	This training provides insights to Microsoft Windows operating System forensics, with practical exercises on forensic imaging, and recovery of forensic artifacts from the windows OS.
Code	22OI28033ARB-E

1. LEARNING OBJECTIVES

To perform in-depth forensic analysis of Windows 10 operating system to identify and report potential forensic artifacts.

2. LEARNING OUTCOMES

- Understand the best practices in dealing with computer forensics.
- Apply the skills to perform forensic disk image analysis and reporting.
- Identify ways to extract potential artifacts from web browsers.
- Examine windows registry to uncover forensic evidence.
- Analyze Windows event logs to answer critical questions.

3. TARGET POPULATION

The course targets security professionals, engineers, technical staff, telecom operators, administrators from government organizations, industry companies and academia, as well as individuals who are interested in computer forensics.

4. ENTRY REQUIREMENTS

There is not mandatory prerequisite course to attend this course, but the following knowledge and skills preferred:

- Have a background of computer science and IT related experience.
- Basic knowledge about windows operating system

5. TUTORS/INSTRUCTORS

Name of tutor(s)/instructor(s)	Contact details
Sundaresan Ramachandran	sramachandran@nauss.edu.sa

6. TRAINING COURSE CONTENTS

Topic	Description
Forensic Fundamentals	This topic covers the best practices in dealing with computer forensics
Introduction to NTFS File system and Master File Table (MFT)	The fundamentals of NTFS filesystem and Master file table (MFT) attributes
Windows Registry	This topic discusses about the basic directory structure of the windows registry and five important Hives
Browser Artifacts Analysis	This topic covers use of browser forensic tools to uncover browser history and search terms.
Windows Event log analysis	This topic discusses about how to audit system and user performed events in the computer.

7. TRAINING COURSE SCHEDULE (Riyadh Time)

Day / Session	Time	Topic	Exercises and interactions
Day 1: 30 March	9:00 to 13:00	Forensic Fundamentals Introduction to NTFS File system and Master File Table (MFT) Windows Registry	Hashing and Imaging Registry Analysis USB forensics exercise
Day 2: 31 March	9:00 to 13:00	Browser Artifacts Windows Event log analysis	Forensic disk image analysis and reporting Event log analysis **Final Exam**

8. METHODOLOGY (Didactic approach)

The course will include Instructor-led presentations, case studies, group exercises and assignments.

9. EVALUATION AND GRADING

The training will be concluded with the final test with passing score of 70 percent.

10. TRAINING COURSE COORDINATION

Training Coordinator:	**ITU Coordinator:**
Dr. Abdulrazaq Al-Morjan Director of Centre of Excellence in Cyber Crimes and Digital Forensics, at NAUSS Mobile: +966 54 470 05 53 Email: t-aalmargan@nauss.edu.sa	**Mr. Ahmed El Raghy** Senior Advisor ITU Arab Regional Office Tel: +202 3537 1777 Mobile: +201005281908 Fax: +202 3537 1888 Email: ahmed.elraghy@itu.int