**RASHTRIYA RAKSHA UNIVERSITY**

**Proposed Training Program under ITEC scheme, MEA**

**Name of the School:** SITAICS

**Nameof the Program:** Memory Forensics

**Training Mode:** Virtual / Online – face to face

**Duration of the program:** 3-5 days

**Teaching Lectures total :** 20

**Teaching Lectures per day :** 4

**Hours per Lecture:** 1 Hour

**Eligibility Criteria:** Working knowledge of computers

**Target Audience:** Police Officials, Government Officials , Law Enforcement officials , Forensic Lab Officials **,** Investigating officers

**Intake :** Minimum 10 & Maximum 30 Officials

**Language of Instruction:** English

**Modules / Topics:**

1. Introduction to types of memory, Memory management, contiguous memory allocation, non-contiguous memory allocation, paging, multilevel paging, Kernel, Basics of virtualization based security, Linux Memory structure
2. Acquisition procedure of live system, tools to acquire physical memory from windows operating system, Hibernation and page file memory extraction and conversion, virtual machine memory acquisition, acquisition process of Linux Physical Memory using
3. Analysis of memory image using different tools – volatility, rekall, redline. Identifying rouge processes and DLLs, review network activity, look for evidences of code injection, rootkit hunting in memory, windows registry examination, extracting prefetch and shimcache from memory, analysis of compromise using windows baseline

**Learning Outcome** :

1. In-depth knowledge and hands-on training in the field of memory forensics
2. Sharpen the skills of professionals who are already working in this field
3. Exposure of the live scenario of memory forensic in simulated environment

**Evaluation / Assessment :** Based on Exam

**Name of the Faculty :** Mr. Akash Thakar