Contribution ID: **89** Type: **Oral**

RegTrace: USB-Based Windows Registry Forensic Tool

Abstract:
The Windows Registry is a critical source of evidence in digital forensics,containing extensive traces of user activity,system configurations and application behavior.Despite its value,obtaining Registry hives from live systems without altering data remains a major challenge for investigators.To address this,developed "RegTrace",a portable USB-based tool that automates both the acquisition and interpretation of Registry artifacts.Using Microsoft's Volume Shadow Copy Service (VSS),the tool acquires protected hives in a read-only manner, thereby maintaining forensic integrity.The acquired hives are then parsed to extract details on user actions,device history,software execution and network connections,while anomaly detection highlights irregular patterns such as time manipulation or missing entries..By combining evidence collection and automated reporting in a single workflow,RegTrace reduces examiner workload and enables rapid,reliable on-site analysis.Its design makes it particularly useful in incident response scenarios as well as traditional forensic casework.

Keywords: Windows Registry,Digital Forensics,Volume Shadow Copy Service,Artifact Acquisition, Timeline Analysis, Forensic Integrity.

Author: Mr BHAT, Aditya (JAIN (Deemed-to-be University))

Co-author: Mr VENKATESH, N VISHNU (JAIN (Deemed-to-be University))

Presenter: Mr BHAT, Aditya (JAIN (Deemed-to-be University))

Track Classification: Physical Sciences