MITHIBAI COLLEGE AUTONOMOUS

Computer Science Department

Subject:-Cyber forensics -2 Lab **Lab Assignment No:-9** **Course**: TYBSc (CS)

Assignment Date:-12/02/2025 **Submission Date**: - 04/03/2025

Network Tracking and Process Monitoring using Sysinternal and Ram capture tools

Write-up

- **Sysinternal tool and commands**
- **RAM capture tool and commands**

❖ Using Sysinternals tools for Network Tracking and Process Monitoring :
- Check Sysinternals tools

Monitor Live Processes
- Capture RAM
- Capture TCP/UDP packets
- Monitor Hard Disk
- Monitor Virtual Memory
- Monitor Cache Memory

https://docs.microsoft.com/en-us/sysinternals/downloads/procmon