# PRACTICAL ASSESSMENT TABLE

| SR. NO. | PRACTICAL TITLE | PAGE NO. | | MARKS (10) | SIGN |
|---|---|---|---|---|---|
| | | FROM | TO | | |
| 1 | Setting up a DFIR lab. | | | | |
| 2 | Non-Volatile Disk imaging using FTK Imager. | | | | |
| 3 | Analyzing the Physical image using Autopsy to extract evidence. | | | | |
| 4 | Analyzing the Live running OS using Autopsy to extract evidence without Imaging. | | | | |
| 5 | Creating RAM dumps using Dump-IT and FTK. | | | | |
| 6 | Analyzing the RAM Dump using Volatility Framework to extract evidence. | | | | |
| 7 | Setup SIEM tool and upload the extracted logs from windows system. | | | | |
| 8 | Installing wire shark and creating PCAP files for analysis. Application of wire shark search filters. | | | | |
| 9 | Network malware logs analysis CTF (using Wire-shark). | | | | |
| 10 | Windows security logs analysis (using SPLUNK). | | | | |