List of Practicals -MSC Cyber Security (SEM-II)

Sr. No	Particulars	Reference
1.	Analyze and monitor system logs using the event viewer	https://www.windowscentral.com/how-use-event-viewer-windows-10
2.	Install and demonstrate system internal tools (process explorer). Classify data with process ID and company name.	https://www.howtogeek.com/school/sysinternals-pro/lesson2/
3.	With the help of disk monitoring identify the read and write process having length>5.	https://www.golinuxcloud.com/monitor-disk-io-performance-statistics-linux/ https://www.thewindowsclub.com/use-resource-monitor-windows-10
4.	Installation and demonstration of sawmill on windows OS. Generate a custom report.	https://www.youtube.com/watch?v=gKOMAahUpsM&ab_channel=CyberTrainings https://www.youtube.com/watch?v=BqTRkvlnyeU&ab_channel=SawmillAnalytics
5.	Install and configure snort for network security and protection against cyber threats.	https://zaeemjaved10.medium.com/installing-configuring-snort-2-9-17-on-windows-10-26f73e342780 https://techofide.com/blogs/snort-intrusion-detection-system-prevention-system-installation-use-in-windows/
6.	Install and demonstrate Splunk for log analysis	https://www.splunk.com/en_us/resources/videos/installing-splunk-on-windows.html https://www.educba.com/install-splunk/
7.	Use Autopsy to recover file from the given data source. Present your details accordingly	https://www.section.io/engineering-education/how-to-recover-data-from-digital-storage-media-using-autopsy/ https://www.cybervie.com/blog/introduction-to-autopsy-an-open-source-digital-forensics-tool/ https://www.autopsy.com/
8.	Install cyber triage and collect the given system report.	https://docs.cybertriage.com/en/latest/index.html

	Analyse your data accordingly	
9.	Perform digital forensics to analyze RAM timeline using CAINE tool	https://www.caine-live.net/page5/page5.html
10.	Install Wireshark to analyse captured packet. Discuss your results obtained from the tool.	https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it https://www.lifewire.com/wireshark-tutorial-4143298
11.	Examine files, folders on local hard disk and network drive using FTK Imager	https://www.golinuxcloud.com/create-forensic-image-ftk-imager/ https://laptrinhx.com/step-by-step-tutorial-of-ftk-imager-beginners-guide-466694096/
12.	Install Tally software and create a company. Add sufficient data. After modifications, analyze the windows registry to identify evidence related to the company.	https://tallysolutions.com/download/
13.	Install fedora workstation using virtual environment to demonstrate working of open source-based platform	https://www.fedoraproject.org/ https://itsfoss.com/install-fedora-in-virtualbox/
14.	Use USB drive as data source and Belkasoft X to demonstrate data / file carving	https://belkasoft.com/carving-and-its-implementations
15.	Use PhotoRec to recover lost files, audio or video content from the HDD/USB Drive using file carving	https://resources.infosecinstitute.com/topic/file-carving/