**COMPUTER NETWORKS LAB**

**INDUSTRY PROBLEM – MALWARE TRAFFIC ANALYSIS USING WIRESHARK**

**REPORT**

**Team Member Names and SRNs:-**

**1. Vinti Agrawal PES2UG20CS385**

**2. Vishwa Mehul Mehta PES2UG20CS389**

**3. Vismaya R PES2UG20CS391**

**The following questions have been answered after analyzing the wireshark capture when a web page with files that may contain malware were downloaded.**

**We extracted the files that were downloaded in the capture and then they were uploaded to a hash generator. This hash was then searched in the VirusTotal website to find out if the file was infected. The website shows the degree of malware content in the file with that hash.**

**Now if the file was malware free it was safe to assume that the website and the file is safe to use and load.**

**If on the other hand if the file is infected then we find the host name and host url of the website from which the file was extracted and also the source and destination IP Addresses along with the MAC Address of the host machine.**

**This method is used to analyse the traffic that may contain malware and prevent us from downloading these files to protect our systems from threats.**















