Total No. of Pages *Roll No. .....*

FIFTH SEMESTER (Supplementary) **B.Tech. (I.T.)**

END SEMESTER EXAMINATION (FEBRUARY-2019)

IT-321 MALWARE ANALYSIS

Time: 3 Hour *Max. Marks: 50*

Note: Attempt any **five** questions. Assume suitable missing data, if any.

Q1. What is static analysis. Explain different type of techniques to perform static analysis(atleast three). [10]

Q2. How to use OllyDbg tool effectively for dynamic analysis. Explain its unique features and powerful capabilities to analyse. [10]

Q3. (i) What is windows API. Explain the types and core components of windows API with example.
(ii) Explain the difference between windows registry and windows API [5+5]

Q4. What are packet sniffers used for. Explain how **wireshark** tool does packet sniffing including its advantages and disadvantages. [10]

Q5. What is android malware. Explain plankton malware with its special characterstics. [10]

Q6. What is the purpose of virtual snapshot manager in malware analysis . How can one connect a virtual machine to internet using VMware. [10]

Q7. Explain the following:
i. downloaders and launchers
ii. rootkits
iii. kernel vs user mode
iv. packing and unpacking [2.5*4]