

**POST GRADUATE DIPLOMA IN
INFORMATION SECURITY (PGDIS)**

Term-End Practical Examination

December, 2017

MSEI-027 (P) : DIGITAL FORENSICS

Time : 3 hours

Maximum Marks : 100

*Note : (i) Attempt 2 out of 3 questions. Each question carries
40 marks.*

(ii) Viva-voce carries 20 Marks.

1. Select an image, find Artifacts of the image, apply steganography on the image and generate the new image. By using any reverse engineering or forensics tools, find the hidden file details from the steganographic image. **40**

2. Identify Networks Forensics details as given below using any Sniffer like Wireshark etc. **40**
 - (a) Shows all TCP Packets that contain the word "Facebook".
 - (b) Displays all HTTP responses that were sent more than 2 seconds after the request.
 - (c) Sets a filter for any packet with X.X.X.X as the source or dest IP.
 - (d) List of the protocols like ICMP, ARP, SMTP and DNS Packets only.

3. Take a Removable External drive or pen drive. Find all Artifacts from the removable drive, delete some files and then try to recover those files and calculate its MD5 and SHA1 Hash Values. 40
-