VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science and Engineering

CSE4004 – Digital Forensics Laboratory
Final Assessment Test – Fall 2019-20

Slot: L25+26 **Duration: 1 hr 30 Min**

Date: 06/11/2020 **Time: 8:00 – 9:30 AM**

SET 1: Registered Numbers

17BCE0085	17BCE0235	17BCE0471	17BCE0861
17BCE0972	17BCE2243	18BCE0154	18BCE0542
18BCE0646	18BCE0703	18BCE0929	18BCE2258
18BCE2314	18BCE2473		

SET 2: Registered Numbers

16BCE0448	17BCE0167	17BCE0246	17BCE0600
17BCE0880	17BCE0988	17BCE2321	18BCE0169
18BCE0559	18BCE0662	18BCE0711	18BCE0949
18BCE2287	18BCE2318	18BCE2486	

SET 3: Registered Numbers

17BCB0109	17BCE0196	17BCE0328	17BCE0770
17BCE0945	17BCE0996	17BEC0708	18BCE0505
18BCE0582	18BCE0675	18BCE0714	18BCE0959
18BCE2288	18BCE2438	18BEE0040	

SET 4: Registered Numbers

17BCB0110	17BCE0210	17BCE0410	17BCE0778
17BCE0946	17BCE2078	18BCE0004	18BCE0516
18BCE0583	18BCE0699	18BCE0787	18BCE0974
18BCE2290	18BCE2462		

SET 5: Registered Numbers

17BCE0053	17BCE0223	17BCE0447	17BCE0831
17BCE0959	17BCE2191	18BCE0074	18BCE0533
18BCE0586	18BCE0700	18BCE0850	18BCE2231
18BCE2292	18BCE2470		

Examination Guidelines

- All the students are requested to login to MS teams without by 7:50 AM.
- Commencement of the exam, 8:00 AM.
- Write your Reg. No | Name | Qn. Set No.| Date of Examination.
- Check out the google drive link: ***https://tinyurl.com/yyxms3v3***
- Download the respective files (E01 & PCAP) from the corresponding numbered folder.
- Execute and analyse the dataset.
- Write the answers to the respective questions.
- Prepare a single document with two subtitles, Autopsy and Wireshark.
- Convert the file to pdf format.
- Upload the respective pdf file.

- ***Part- A: Autopsy (25 Marks)***
    a. Find the hash of the image and all the files that are extracted.
    b. Note the path of the files that are extracted.
    c. Check if there are any emails, office documents and multimedia content.
    d. Analyse them thoroughly and Arrive at a conclusion of what has happened.
    e. Include all the respective snapshots and the corresponding explanations / interpretations.
    f. Generate the overall report and provide proper interpretation to the report.
- ***Part- B: Wireshark (25 Marks)***
    a. Find the host name, IP address, MAC address for the sender and receiver.
    b. Check the emails, attachment, chats, ports and provide its explanation / interpretation.
    c. Establish a timeline and explain what is happening in the pcap file.
    d. Include all the respective snapshots and the corresponding explanations / interpretations.