National Forensics Sciences University, Goa Campus
Mid- semester Examination

Programme– M.Sc Cyber Security / M.Sc DFIS **Sem – 2** **Date- 27/03/2024**

Subject Name: Malware Analysis / Malware Forensic

Subject Code- CTMSCS SII P2 / CTMSDFIS SII P1

Time- 1.5 Hours **Max. Marks- 50**

Instructions - 1) Answer all questions. 2) Assume suitable data.

Q.1	**Solve any four**	**20 marks**
	a. Explain following terms. a. cmp eax,5 b. mov ecx, [x] c. xor eax, 2 d. shl al, 2 e. mov [ebx],eax	5 marks
	b. Explain all Conditional instruction for X86 processor.	5 marks
	c. List difference between PEId vs PEView.	5 marks
	d. Explain bit, word, d-word in details.	5 marks
	e. Explain PEStudio tool function and feature in static analysis.	5 marks
Q.2	**Attempt all** Any 2	**15 marks**
	a. Recall the benefits of sandbox and list various sandbox tool.	5 marks
	b. Explain ESP, EBP, EIP, DF Flag, Push operation with example.	5 marks
	c. Explain function and feature of IDA Pro in dynamic malware analysis.	5 marks
Q. 3	**Attempt all**	**20 marks**
	a. Explain different types of data transfer instruction with assembly program example.	10 Marks
	b. Explain different types of arithmetic operation instruction with assembly program example.	10 Marks

*** All the best***