

GUJARAT TECHNOLOGICAL UNIVERSITY**M. E. - SEMESTER – III • EXAMINATION – WINTER • 2013****Subject code: 732303****Date: 28-11-2013****Subject Name: Software Forensics****Time: 10.30 am – 01.00 pm****Total Marks: 70****Instructions:**

1. Attempt all questions.
2. Make suitable assumptions wherever necessary.
3. Figures to the right indicate full marks.

- Q.1** (a) Explain the software forensic technologies and practices. **07**
(b) Define software and network forensics. What are the objectives and objects of software forensics? **07**
- Q.2** (a) Discuss types of blackhats and its general characteristics. **07**
(b) Explain analytical tools. **07**
- OR**
- (b) Discuss Cogger, SCRUPLE and tool for finding duplicate code. **07**
- Q.3** (a) Describe in brief detection techniques. **07**
(b) What is plagiarism? Explain the use of YAP and JPlag. **07**
- OR**
- Q.3** (a) Discuss decompilation and its various tools. **07**
(b) Explain programming process. **07**
- Q.4** (a) Explain the structure of virus and trojan. **07**
(b) Discuss stealth and anti-detection measures. **07**
- OR**
- Q.4** (a) Explain rules of evidence. **07**
(b) Discuss the legal systems and types of evidence. **07**
- Q.5** (a) Write a short note on plagiarism detection versus authorship analysis. **07**
(b) What are indicators? Briefly explain indicators of programming style. **07**
- OR**
- Q.5** (a) What is Cusum? Discuss programmer skill and objective with reference to programming style. **07**
(b) Which are the 3 standard forms of authenticity? Write a short note on non content metrics as evidence of authorship. **07**
