THIRD-YEAR OF BACHELOR OF COMPUTER SCIENCE REVISED SYLLABUS ACCORDING TO CBCS

COURSE TITLE: CYBER FORENSICS

SEMESTER-V, W.E.F. 2021-2022

Recommended by the Board of Studies in Computer Science
And
Approved by the Academic Council

Devrukh Shikshan Prasarak Mandal's
Nya. Tatyasaheb Athalye Arts, Ved. S. R. Sapre Commerce, and Vid. Dadasaheb Pitre Science College (Autonomous), Devrukh.
Tal. Sangameshwar, Dist. Ratnagiri-415804, Maharashtra, India

Academic Council Item No: _____

Name of the Implementing Institute	:	Nya. Tatyasaheb Athalye Arts, Ved. S. R. Sapre Commerce, and Vid. Dadasaheb Pitre Science College (Autonomous), Devrukh. Tal. Sangameshwar, Dist. Ratnagiri-415804,
Name of the Parent University	:	University of Mumbai
Name of the Programme	:	Bachelor of Science
Name of the Department	:	Computer Science
Name of the Class	:	Third Year
Semester	:	Six
No. of Credits	:	03
Title of the Course	:	Cyber Forensics
Course Code	:	USCST63
Name of the Vertical	:	Elective I
Eligibility for Admission	:	Any 12^{th} Pass seeking Admission to Degree Programme in adherence to Rules and Regulations of the University of Mumbai and Government of Maharashtra
Passing Marks	:	40%
Mode of Assessment	:	Formative and Summative
Level	:	UG
Pattern of Marks Distribution for TE and CIA	:	70:30
Status	:	CBCS
To be implemented from Academic Year	:	2021-2022
Ordinances /Regulations (if any)		

Syllabus for Third Year of Bachelor of Science in Computer Science

(With effect from the academic year 2021-2022)

SEMESTER-VI **Paper No.– 3**

Course Title: Cyber Forensics **No. of Credits - 03**

Type of Vertical: Elective I **COURSE CODE: USCST63**

Learning Outcomes Based on BLOOM's Taxonomy:

After completing the course, the learner will be able to…		
Course Learning Outcome No.	Blooms Taxonomy	Course Learning Outcome
CO-01	Understand	The student will be able to plan and prepare for all stages of an investigation - detection, initial response and management interaction, investigate various media to collect evidence, report them in a way that would be acceptable in the court of law

Syllabus for Third Year of Bachelor of Science in Computer Science

(With effect from the academic year 2021-2022)

SEMESTER-VI **Paper No.–3**

Course Title: Cyber Forensics **No. of Credits - 03**

Type of Vertical: Elective I **COURSE CODE: USCST63**

COURSE CONTENT			
Unit No.	**Content**	**Credits**	**No. of Lectures**
I	Computer Forensics : Introduction to Computer Forensics and standard procedure, Incident Verification and System Identification ,Recovery of Erased and damaged data, Disk Imaging and Preservation, Data Encryption and Compression, Automated Search Techniques, Forensics Software Network Forensic : Introduction to Network Forensics and tracking network traffic, Reviewing Network Logs, Network Forensics Tools, Performing Live Acquisitions, Order of Volatility, Standard Procedure Cell Phone and Mobile Device Forensics: Overview, Acquisition Procedures for Cell Phones and Mobile Devices	**01**	**15**
II	Internet Forensic : Introduction to Internet Forensics, World Wide Web Threats, Hacking and Illegal access, Obscene and Incident transmission, Domain Name Ownership Investigation, Reconstructing past internet activities and events E-mail Forensics : e-mail analysis, e-mail headers and spoofing, Laws against e-mail Crime, Messenger Forensics: Yahoo Messenger Social Media Forensics: Social Media Investigations	**01**	**15**

	Browser Forensics: Cookie Storage and Analysis, Analyzing Cache and temporary internet files, Web browsing activity reconstruction		
III	Investigation, Evidence presentation and Legal aspects of Digital Forensics: Authorization to collect the evidence , Acquisition of Evidence, Authentication of the evidence, Analysis of the evidence, Reporting on the findings, Testimony Introduction to Legal aspects of Digital Forensics: Laws & regulations, Information Technology Act, Giving Evidence in court, Case Study – Cyber Crime cases, Case Study – Cyber Crime cases	**01**	**15**
	Total	03	45

Required Previous Knowledge

Students should know basic concepts related to computer and computer handling

Access to the Course

The course is available for all the students admitted for Bachelor of Science (Computer Science).

Forms of Assessment

The assessment of the course will be of Diagnostic, Formative and Summative type. At the beginning of the course diagnostic assessment will be carried out. The formative assessment will be used for the Continuous Internal Evaluation whereas the summative assessment will be conducted at the end of the term. The weightage for formative and summative assessment will be 60:40. The detailed pattern is as given below.

Semester End Evaluation (70 Marks)
Question Paper Pattern
Time: 2:30 hours

Question No.	Unit/s	Question Pattern	Marks
Q.1	I ,II &III	MCQ/Fill in the blanks/One line sentence	10
Q.2	I	Descriptive Questions	20
Q.3	II	Descriptive Questions	20
Q4.	III	Descriptive Questions	20
	Total		**70**

Internal evaluation (30 Marks)

Sr. No.	Description	Marks
1	Classroom Tests	10
2	Project/ Viva/ Presentations/ Assignments	10
3	Attendance	10
	Total	**30**

Grading Scale

10 points grading scale will be used. The grading scale used is O to F. Grade O is the highest passing grade on the grading scale, and grade F is a fail. The Board of Examinations of the college reserves the right to change the grading scale.

Reference book:

- Guide to computer forensics and investigations, Bill Nelson, Amelia Philips and Christopher Steuart, course technology,5th Edition,2015

Text book:

- Techmax publication book

Additional References:

- Incident Response and computer forensics, Kevin Mandia, Chris Prosise, Tata McGrawHill,2nd Edition,200

Course: USCSP68	Practical of USCST63 (Credits : 1, Lectures/Week: 3)
USCSP68	1. Creating a Forensic Image using FTK Imager/Encase Imager : - Creating Forensic Image - Check Integrity of Data - Analyze Forensic Image 2. Data Acquisition: - Perform data acquisition using: - USB Write Blocker + Encase Imager - SATA Write Blocker + Encase Imager - Falcon Imaging Device 3. Forensics Case Study: - Solve the Case study (image file) provide in lab using Encase Investigator or Autopsy 4. Capturing and analyzing network packets using Wireshark (Fundamentals) : - Identification the live network - Capture Packets - Analyze the captured packets 5. Analyze the packets provided in lab and solve the questions using Wireshark : - What web server software is used by www.snopes.com? - About what cell phone problem is the client concerned? - According to Zillow, what instrument will Ryan learn to play? - How many web servers are running Apache? - What hosts (IP addresses) think that jokes are more entertaining when they are explained? 6. Using Sysinternals tools for Network Tracking and Process Monitoring : - Check Sysinternals tools - Monitor Live Processes - Capture RAM - Capture TCP/UDP packets - Monitor Hard Disk

	- Monitor Virtual Memory - Monitor Cache Memory 7. Recovering and Inspecting deleted files - Check for Deleted Files - Recover the Deleted Files - Analyzing and Inspecting the recovered files Perform this using recovery option in ENCASE and also Perform manually through command line 8. Acquisition of Cell phones and Mobile devices 9. Email Forensics - Mail Service Providers - Email protocols - Recovering emails - Analyzing email header 10. Web Browser Forensics - Web Browser working - Forensics activities on browser - Cache / Cookies analysis - Last Internet activity