



Don Bosco Institute of Technology, Mumbai – 400070
Report on Digital Forensics: Practical Methodology and Tools

Title : Workshop on Digital Forensics: Practical Methodology and Tools

Date : 04th October, 2019

Time : 2pm to 4pm

Venue : Comp Lab - 3

Participants : B.E. Computer

Resource Person : Ms. Mayura Gavhane

Organizing Department / Committee / Authority : Computer Department

Objective : To understand and explore techniques used in digital forensics

Outcomes :

1. Understand fundamentals of digital forensics
2. Understand methodologies for acquiring volatile data from windows and unix platforms
3. Understand and apply forensic duplication techniques for retrieving and backing up data from hdd and other storage media
4. Applying various tools for forensic image analysis

Excerpt : Workshop on Digital Forensics: Practical Methodology and Tools

Report :

A workshop on Digital Forensic was conducted on 4th October 2019 at 2pm in Computer Lab – 3, DBIT with Professor Mayura Ghavane as the speaker.

The workshop focused on the term “digital forensics” meaning the methodologically examining computer media (basically computer keeping a record of all activities which can later be used as evidence in case of cybercrime) and the main three things under methodology

- Acquire (acquire evidence without damage/alter in original)
- Authenticate (to check if same as original)

- Analyze (if evidence useful or not)

Topics like computer incident (unlawful behavior performed through the computer or computer network), CSIRT (Computer Security Incident Response Team) for handling incident, Stages of CSIR (Pre-Incident Preparation, Detection of Incident, Initial Response, Formulating Response strategy, investigating incident, Data collect/analysis, Report) were covered.

Data Collection of the system data (volatile) and by creating a duplicate copy of the victim's system and work on the duplicate copy on another system was explained in the workshop. Data collection and Data analyzing part was demonstrated showing full investigation of a live system.

Data Collection: Hands-on on who logged a system, date, recording file modification access, open ports and apps associated with the ports, running processes, MD5 or SHA512 for storing cryptographic hash of files and recording checksum was shown.

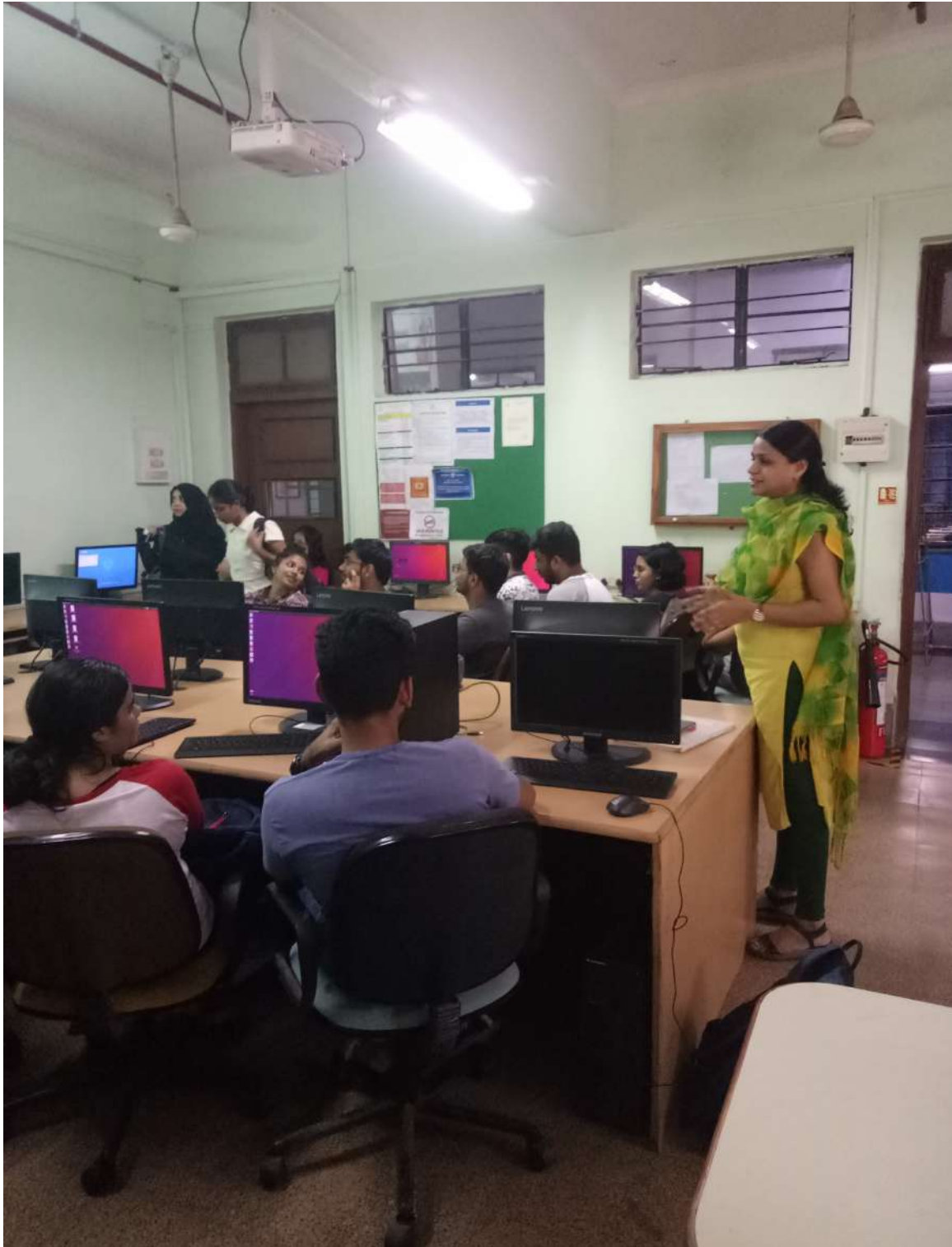
Data Duplication and Analyze: Tools were installed

- DD (data duplicator)
- DCFL DD (DD for forensic analysis designed by US Department of Defense)
- Sleuth-Kit - Autopsy (for performing analysis of the data)

Fdisk command was used to check the sectors in disk, pen drive data was used to copy the data for data duplication. Hash algorithms were used for checksums and related lock files. The output duplicate file with a .dd extension was given to Autopsy tool running in the browser for data analysis and analyzed the data using keyword search. Thus, the digital forensic tools were demonstrated and understood.

Report Prepared By : Sherin Shaji

Pictures:





DON BOSCO INSTITUTE OF TECHNOLOGY
Department of Computer Engineering

Workshop on "Digital Forensics: Practical Methodology and Tools"

Speaker: Ms. Mayura Gavhane

Faculty Coordinator: Ms. Shafaque Syed

Date: 4th October, 2019

Time: 2pm to 4pm

Roll No.	Name	Signature
1	Abreo Russel Oswald Mohini	
2	Adhikari Afi Irfan Nujat	
3	Alphonso Elana Savita Leelamma	
5	Banka Sourab Nilkantha Lalita	
6	Bharambe Dipesh Sanjay Ranjana	
7	Caunder Rosy Selvanathan Annamall	
8	Chanchal Sagar Vijaykumar Gayatri	
9	Chitre Mihir Milind Rupa	
10	Christy Lyona Joseph Vijayan Ponrani	
12	Crasto Calvin Oswin Carol	
15	Desai Tanmay Prasad Pradnya	
16	Deshmukh Atharva Sanjay Anita	
19	Dsouza Briclad Brian Clara	
22	Dsouza Diana Manuel Eremita	
25	Fernandes Shalomi Francis Saira	
27	Gounder Jacklin Lawrence Irudayamary	
28	Jadhav Aishwarya Balasaheb Sunita	
29	Jadhav Vaidehi Ravindranath Rupali	
31	Kale Pranav Pramod Swati	
32	Khan Tooba Rizwan Azra	
34	Lobo Desmond Sebastian Pauline	

DON BOSCO INSTITUTE OF TECHNOLOGY

Department of Computer Engineering

Workshop on "Digital Forensics: Practical Methodology and Tools"

Speaker: Ms. Mayura Gavhane

Faculty Coordinator: Ms. Shafaque Syed

Date: 4th October, 2019

Time: 2pm to 4pm

	35	Maner Shifa Muhtaque	Smant
38		Menezes Joyce Jerald Precilla	Joyce.
41		Nimbekar Rohini Anand Rekha	Rohini
42		Palamattam Sherin Shaji Anita	Sherin
45		Patil Harshada Shivnarayan Asha	Harshada
46		Patil Yogesh Sanjay Sunita	Yogesh
47		Pawar Aditya Anil Anjali	Aditya
51		Puliyani Akhil Thomas	— AB —
52		Puranik Priyanka Santosh Smita	Priyanka
56		Rebello Sneden Ivor Romilla	Rebello
59		Sanil Bryan John Stella	Bryan
60		Sapkal Shubham Sampat Sunita	Shubham
64		Syed Saqib Shakir Nigar	Saqib
65		Varghese David Mathew Sarah	David
67		Vignesh Sundaram Sundaram Laxmi	Vignesh
70		Yadav Sagarika Ramsevak Manju	— AB —
72		Nare Vinit Ramesh Revati	Vinit