UNIVERSITY OF MUMBAI

M.Sc. (Part-II) INFORMATION TECHNOLOGY (Practical) SEM IV EXAMINATION
JUNE- 2016

Candidate No: _____ ELECTIVE –I (COMPUTER FORENSICS)

a.	Demonstrate the following using Cain & Abels tool 1. APR (ARP Poison Routing) 2. Route Table Manager 3. SID Scanner 4. Network Enumerator 5. Remote Registry	20
b.	Perform thefollowing using ProDiscover Basic 1. Capturing Physical Memory 2. Add an image file to a project 3. List detail information about image files associated with a project 4. View the contents of a disk, or image file as clusters 5. Viewing the Windows Event Logs 6. View Graphic Files in Gallery 7. View Adding Thumbnail Images to Report for Graphic Evidence 8. Recover a Deleted File 9. Search for key words in image file or disk 10. Extracting Internet History	20
C	Viva	05
d	Journal	05

UNIVERSITY OF MUMBAI

M.Sc. (Part-II) INFORMATION TECHNOLOGY (Practical) SEM IV EXAMINATION

JUNE- 2016

Candidate No: _____ ELECTIVE –I (COMPUTER FORENSICS)

a.	Demonstrate the following using Cain & Abels tool 1. Network Enumerator 2. Remote Registry 3. Service Manager 4. Sniffer 5. Routing Protocol Monitors	20
b.	Perform the following using AccessData FTK 1. Creating a Report 2. Managing Bookmarks 3. Managing Thumbnails 4. Selecting a File Path List 5. Selecting a File Properties List 6. Selecting the Properties of the File Properties List 7. Adding Supplementary Files and the Case Log	20
C	Viva	05
d	Journal	05

UNIVERSITY OF MUMBAI

M.Sc. (Part-II) INFORMATION TECHNOLOGY (Practical) SEM IV EXAMINATION

JUNE- 2016

Candidate No: _____ ELECTIVE –I (COMPUTER FORENSICS)

a.	Demonstrate the following using Cain & Abels tool 1. Oracle Password Extractor via ODBC 2. MySQL Password Extractor via ODBC 3. Hash Calculator 4. TCP/UDP Table Viewer 5. Remote Console 6. Remote Route Table Manager 7. Remote TCP/UDP Table Viewer	20
b.	Perform the following using AccessData FTK 1. Creating a Report 2. Managing Bookmarks 3. Managing Thumbnails 4. Selecting a File Path List 5. Selecting a File Properties List 6. Selecting the Properties of the File Properties List 7. Adding Supplementary Files and the Case Log	20
C	Viva	05
d	Journal	05

UNIVERSITY OF MUMBAI

M.Sc. (Part-II) INFORMATION TECHNOLOGY (Practical) SEM IV EXAMINATION

JUNE- 2016

Candidate No: _____ ELECTIVE –I (COMPUTER FORENSICS)

a.	Demonstrate the following using Cain & Abels tool 1. APR (ARP Poison Routing) 2. Route Table Manager 3. SID Scanner 4. Service Manager 5. Sniffer 6. Routing Protocol Monitors	20
b.	Perform thefollowing using ProDiscover Basic 1. Capturing Physical Memory 2. Add an image file to a project 3. List detail information about image files associated with a project 4. View the contents of a disk, or image file as clusters 5. Viewing the Windows Event Logs 6. View Graphic Files in Gallery 7. View Adding Thumbnail Images to Report for Graphic Evidence 8. Recover a Deleted File 9. Search for key words in image file or disk 10. Extracting Internet History	20
C	Viva	05
d	Journal	05

UNIVERSITY OF MUMBAI

M.Sc. (Part-II) INFORMATION TECHNOLOGY (Practical) SEM IV EXAMINATION

JUNE- 2016

Candidate No: _____ ELECTIVE –I (COMPUTER FORENSICS)

a.	Demonstrate the following using Cain & Abels tool 1. Service Manager 2. Sniffer 3. Routing Protocol Monitors 4. Certificates Collector 5. MAC Address Scanner with OUI fingerprint 6. Promiscuous-mode Scanner based on ARP packets 7. Wireless Scanner	20
b.	8. Password Crackers Demonstrate hiding & retrieving text file from an image & audio file.	20
C	Viva	05
d	Journal	05

UNIVERSITY OF MUMBAI

M.Sc. (Part-II) INFORMATION TECHNOLOGY (Practical) SEM IV EXAMINATION
JUNE- 2016

Candidate No: _____ ELECTIVE –I (COMPUTER FORENSICS)

a. b.	Perform the following using AccessData FTK 1. Creating a Report 2. Managing Bookmarks 3. Managing Thumbnails 4. Selecting a File Path List 5. Selecting a File Properties List 6. Selecting the Properties of the File Properties List 7. Adding Supplementary Files and the Case Log Demonstrate monitoring of, network (used to connect to the internet), using wireshark and perform the following: 1. Capture dns packets. 2. Select a packet & display the client sever conversation. 3. Display the details of a packet. 4. Display only HTTP traffic 5. Examine HTTP Traffic & Note the following details: o GET request o Host o User-Agent o Accepts o cookie 6. Filter to find the request corresponding to the form was submitted using the POST method: 7. Filter for URLs containing the substring “simple” 8. Building filter for HTTP response corresponding to attempt to visit an inexistent page	20 20
C	Viva	05
d	Journal	05

UNIVERSITY OF MUMBAI

M.Sc. (Part-II) INFORMATION TECHNOLOGY (Practical) SEM IV EXAMINATION
JUNE- 2016

Candidate No: _____ ELECTIVE –I (COMPUTER FORENSICS)

a. b.	Demonstrate Recovering an E-mail using AccessData FTK. Demonstrate hiding & retrieving a text file in a audio & image file using S-tools.	20 20
C	Viva	05
d	Journal	05

UNIVERSITY OF MUMBAI

M.Sc. (Part-II) INFORMATION TECHNOLOGY (Practical) SEM IV EXAMINATION
JUNE- 2016

Candidate No: ________ ELECTIVE –I (COMPUTER FORENSICS)

a. b.	Demonstrate monitoring of, network (used to connect to the internet), using wireshark and perform the following: 1. Capture dns packets. 2. Select a packet & display the client sever conversation. 3. Display the details of a packet. 4. Examine HTTP Traffic & Note the following details: o GET request o Host o User-Agent o Accepts o cookie 5. filter the traffic so that only request packets are shown. 6. Filter to find the request corresponding to the form was submitted using the POST method: 7. Demonstrate Use logical operators in filtering expressions 8. Demonstrate removing the error of a packet with “incorrect” IP header checksum caused by checksum offloading. Demonstrate the Forensics tool Autopsy to perform file analysis on the disk image file provided .Also generate the report in text format.	20 20
C	Viva	05
d	Journal	05

UNIVERSITY OF MUMBAI

M.Sc. (Part-II) INFORMATION TECHNOLOGY (Practical) SEM IV EXAMINATION

JUNE- 2016

Candidate No: _____ ELECTIVE –I (COMPUTER FORENSICS)

a.	Demonstrate the Forensics tool Autopsy to perform file analysis on the disk image file provided .Also generate the report in text format.	
b.	Demonstrate monitoring of, network (used to connect to the internet), using wireshark and perform the following: 1. Capture dns packets. 2. Select a packet & display the client sever conversation. 3. Display the details of a packet. 4. Display only HTTP traffic 5. Examine HTTP Traffic & Note the following details: o GET request o Host o User-Agent o Accepts o cookie 6. Filter for URLs containing the substring “simple” 7. Demonstrate Use logical operators in filtering expressions 8. Demonstrate removing the error of a packet with “incorrect” IP header checksum caused by checksum offloading.	20 20
C	Viva	05
d	Journal	05

UNIVERSITY OF MUMBAI

M.Sc. (Part-II) INFORMATION TECHNOLOGY (Practical) SEM IV EXAMINATION
JUNE- 2016

Candidate No: _____ ELECTIVE –I (COMPUTER FORENSICS)

a. b.	Process evidence provided using AccessData FTK tool . Demonstrate keyword search, emails & data carving. Demonstrate the Forensics tool Autopsy to perform file analysis on the disk image file provided .Also generate the report in text format.	20 20
C	Viva	05
d	Journal	05

UNIVERSITY OF MUMBAI

M.Sc. (Part-II) INFORMATION TECHNOLOGY (Practical) SEM IV EXAMINATION
JUNE- 2016

Candidate No: _____ ELECTIVE –I (COMPUTER FORENSICS)

a. b.	Perform thefollowing using ProDiscover Basic □ Capturing Physical Memory □ Add an image file to a project □ Viewing the Windows Event Logs □ Recover a Deleted File □ Search for key words in image file or disk □ Extracting Internet History □ Flagging or Bookmarking Evidence of Interest □ Adding and Editing Comments to Evidence of Interest Demonstrate hiding & retrieving a text file in a audio & image file using S-tools.	20 20
C	Viva	05
d	Journal	05

UNIVERSITY OF MUMBAI

M.Sc. (Part-II) INFORMATION TECHNOLOGY (Practical) SEM IV EXAMINATION
JUNE- 2016

Candidate No: _____ ELECTIVE –I (COMPUTER FORENSICS)

a. b.	Perform thefollowing using ProDiscover Basic • Capturing Physical Memory • Add an image file to a project • List detail information about image files associated with a project • View the contents of a disk, or image file as clusters • Viewing the Windows Event Logs • View Graphic Files in Gallery • View Adding Thumbnail Images to Report for Graphic Evidence • Recover a Deleted File • Search for key words in image file or disk • Extracting Internet History Demonstrate the Forensics tool Autopsy to perform file analysis on the disk image file provided .Also generate the report in text format.	20 20
C	Viva	05
d	Journal	05

UNIVERSITY OF MUMBAI

M.Sc. (Part-II) INFORMATION TECHNOLOGY (Practical) SEM IV EXAMINATION
JUNE- 2016

Candidate No: _____ ELECTIVE –I (COMPUTER FORENSICS)

a. b.	Demonstrate hiding & retrieving a text file in a audio & image file using S-tools. Demonstrate monitoring of, network (used to connect to the internet), using wireshark and perform the following: 1. Capture dns packets. 2. Select a packet & display the client sever conversation. 3. Display the details of a packet. 4. Display only HTTP traffic 5. Examine HTTP Traffic & Note the following details: o GET request o Host o User-Agent o Accepts o cookie 6. Demonstrate Use logical operators in filtering expressions 7. Demonstrate removing the error of a packet with “incorrect” IP header checksum caused by checksum offloading.	20 20
C	Viva	05
d	Journal	05

UNIVERSITY OF MUMBAI

M.Sc. (Part-II) INFORMATION TECHNOLOGY (Practical) SEM IV EXAMINATION
JUNE- 2016

Candidate No: _____ ELECTIVE –I (COMPUTER FORENSICS)

a. b.	Demonstrate working with Mobiledit Forensics. Demonstrate the Forensics tool Autopsy to perform file analysis on the disk image file provided .Also generate the report in text format.	20 20
C	Viva	05
d	Journal	05

UNIVERSITY OF MUMBAI

M.Sc. (Part-II) INFORMATION TECHNOLOGY (Practical) SEM IV EXAMINATION
JUNE- 2016

Candidate No: _____ ELECTIVE –I (COMPUTER FORENSICS)

a. b.	Demonstrate monitoring of, network (used to connect to the internet), using wireshark and perform the following: 1. Capture dns packets. 2. Select a packet & display the client sever conversation. 3. Display the details of a packet. 4. Display only HTTP traffic 5. Examine HTTP Traffic & Note the following details: o GET request o Host o User-Agent o Accepts o cookie 6. Building filter for HTTP response corresponding to attempt to visit an inexistent page Demonstrate the Forensics tool Autopsy to perform file analysis on the disk image file provided .Also generate the report in text format.	20 20
C	Viva	05
d	Journal	05

UNIVERSITY OF MUMBAI

M.Sc. (Part-II) INFORMATION TECHNOLOGY (Practical) SEM IV EXAMINATION

JUNE- 2016

Candidate No: _____ ELECTIVE –I (COMPUTER FORENSICS)

a. b.	Demonstrate hiding & retrieving a text file in a audio & image file using S-tools. Perform the following using AccessData FTK 1. Creating a Report 2. Managing Bookmarks 3. Managing Thumbnails 4. Selecting a File Path List 5. Selecting a File Properties List 6. Selecting the Properties of the File Properties List 7. Adding Supplementary Files and the Case Log	20 20
C	Viva	05
d	Journal	05

UNIVERSITY OF MUMBAI

M.Sc. (Part-II) INFORMATION TECHNOLOGY (Practical) SEM IV EXAMINATION

JUNE- 2016

Candidate No: _____ ELECTIVE –I (COMPUTER FORENSICS)

a. b.	Demonstrate hiding & retrieving a text file in an audio & image file using S-tools. Demonstrate the Forensics tool Autopsy to perform file analysis on the disk image file provided .Also generate the report in text format.	20 20
C	Viva	05
d	Journal	05