Candidate No:	ELECTIVE –I (COMPUTER FORENSICS)
Culturation 110:	EEEETIVE I (COM CIERTORE)

	Demonstrate the following using Cain & Abels tool  1. APR (ARP Poison Routing)	
	2. Route Table Manager	
	3. SID Scanner	
	4. Network Enumerator	
a.	5. Remote Registry	20
		20
	Deufoure thefollowing weing Due Discover Design	
	Perform the following using ProDiscover Basic	
	<ol> <li>Capturing Physical Memory</li> <li>Add an image file to a project</li> </ol>	
	3. List detail information about image files associated with a project	
b.	4. View the contents of a disk, or image file as clusters	
	5. Viewing the Windows Event Logs	20
	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	
С	Viva	05
d	Journal	05

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

Candidate No:	ELECTIVE –I (COMPUTER FORENSICS)

	Demonstrate the following using Cain & Abels tool	
a.	<ol> <li>Network Enumerator</li> <li>Remote Registry</li> <li>Service Manager</li> </ol>	20
	4. Sniffer	
b.	5. Routing Protocol Monitors 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**

Candidate No: ELI	ECTIVE –I (COMPUTER FORENSICS)
-------------------	--------------------------------

_	Demonstrate the following using Cain & Abels tool	
a.	<ol> <li>Oracle Password Extractor via ODBC</li> <li>MySQL Password Extractor via ODBC</li> <li>Hash Calculator</li> <li>TCP/UDP Table Viewer</li> <li>Remote Console</li> <li>Remote Route Table Manager</li> <li>Remote TCP/UDP Table Viewer</li> <li>Perform the following using AccessData FTK</li> <li>Creating a Report</li> <li>Managing Bookmarks</li> </ol>	20
0.	<ol> <li>Managing Bookharks</li> <li>Managing Thumbnails</li> <li>Selecting a File Path List</li> <li>Selecting a File Properties List</li> <li>Selecting the Properties of the File Properties List</li> <li>Adding Supplementary Files and the Case Log</li> </ol>	20
С	Viva	05
d	Journal	05

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

Cana	date No: ELECTIVE -I (COMPUTER FORENS	2102
	Demonstrate the following using Cain & Abels tool	
	1. APR (ARP Poison Routing)	
	2. Route Table Manager	
	3. SID Scanner	
	4. Service Manager	
l a.	5. Sniffer	
α.	6. Routing Protocol Monitors	20
	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	
b.	4. View the contents of a disk, or image file as clusters	
0.	5. Viewing the Windows Event Logs	20
	6. View Graphic Files in Gallery	20
	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	
С	Viva	05
d	Journal	05

## UNIVERSITY OF MUMBAI

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

ELECTIVE –I (COMPUTER FORENSICS)

Candidate No: \_\_\_\_\_

Ī	0	Demonstrate the following using Cain & Abels tool	
	a.	1. Service Manager	20
		2. Sniffer	20
		3. Routing Protocol Monitors	
		4. Certificates Collector	
		5. MAC Address Scanner with OUI fingerprint	
		6. Promiscuous-mode Scanner based on ARP packets	
	1.	7. Wireless Scanner	
	b.	8. Password Crackers	20
			20
		Demonstrate hiding & retrieving text file from an image & audio file.	
Ī	С	Viva	05
l		γίνα	0.5
	d	Journal	05
1	u	o o di lidi	0.5

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

Candi	late No: ELECTIVE –I (COMPUTER FORENSIO	CS)
	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	
a.		
	Demonstrate monitoring of, network (used to connect to the internet), using	20
	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	
b.	5. Examine HTTP Traffic & Note the following details:	
	o GET request	20
	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	
С	Viva	05
d	Journal	05

#### **UNIVERSITY OF MUMBAI**

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

ELECTIVE –I (COMPUTER FORENSICS)

Candidate No: \_\_\_\_\_

a.	Demonstrate Recovering an E-mail using AccessData FTK.	
	Demonstrate hiding & retrieving a text file in a audio & image file using S-tools.	20
b.	Bemonstrate manig & retrieving a text me in a audio & image me using 5 tools.	20
		20
C	Viva	05
d	Journal	05

Candidate No:	ELECTIVE –I (COMPUTER FORENSICS)

a.	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.	20
С	Viva	05
d	Journal	05

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

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

Candidate No: ELECTIVE –I (COMPUTER FOI		CS)
a.	Process evidence provided using AccessData FTK tool . Demonstrate keyword	20
	search, emails & data carving.	
b.	Demonstrate the Forensics tool Autopsy to perform file analysis on the disk image file provided .Also generate the report in text format.	
0.		20
С	Viva	)5
d	Journal (	)5

#### **UNIVERSITY OF MUMBAI**

Candi	date No: ELECTIVE –I (COMPUTER FOREN	(SICS)
a.	Perform thefollowing using ProDiscover Basic  ☐ Capturing Physical Memory ☐ Add an image file to a project ☐ Viewing the Windows Event Logs	20
b.	<ul> <li>□ Recover a Deleted File</li> <li>□ Search for key words in image file or disk</li> <li>□ Extracting Internet History</li> <li>□ Flagging or Bookmarking Evidence of Interest</li> <li>□ Adding and Editing Comments to Evidence of Interest</li> </ul>	20
	Demonstrate hiding & retrieving a text file in a audio & image file using S-tools.	
С	Viva	05
d	Journal	05

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

Candi	idate No: ELECTIVE –I (COMPUTER FORENS	SICS)
a.	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	20
b.	<ul> <li>□ View Graphic Files in Gallery</li> <li>□ View Adding Thumbnail Images to Report for Graphic Evidence</li> <li>□ Recover a Deleted File</li> <li>□ Search for key words in image file or disk</li> <li>□ Extracting Internet History</li> </ul>	20
	Demonstrate the Forensics tool Autopsy to perform file analysis on the disk image file provided .Also generate the report in text format.	
С	Viva	05
d	Journal	05
	UNIVERSITY OF MUMBAI  I.Sc. (Part-II) INFORMATION TECHNOLOGY (Practical) SEM IV EXAMINATION JUNE- 2016  idate No: ELECTIVE –I (COMPUTER FORENS	
a.	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.	
	<ol> <li>Select a packet &amp; display the client sever conversation.</li> <li>Display the details of a packet.</li> </ol> 4 Display only HTTP traffic	20

5. Examine HTTP Traffic & Note the following details:

6. Demonstrate Use logical operators in filtering expressions

checksum caused by checksum offloading.

7. Demonstrate removing the error of a packet with "incorrect" IP header

Viva

Journal

20

05

o GET request

o User-Agent

o Accepts

o cookie

o Host

b.

 $\mathbf{C}$ 

d

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

Candidate No: ELECTIVE –I (COMPUTER FORENS)		SICS)
a.	Demonstrate working with Mobiledit Forensics.	20
	Demonstrate the Forensics tool Autopsy to perform file analysis on the disk image file provided .Also generate the report in text format.	
b.		20
С	Viva	05
d	Journal	05

## **UNIVERSITY OF MUMBAI**

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
C	Viva	05
d	Journal	05

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

Candi	date No: ELECTIVE –I (COMPUTER FORENS	SICS)
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
С	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 FORE		SICS)	
ä	a.	Demonstrate hiding & retrieving a text file in an audio & image file using S-tools.	20
ł	b.	Demonstrate the Forensics tool Autopsy to perform file analysis on the disk image file provided .Also generate the report in text format.	20
	С	Viva	05
	d	Journal	05