Name:

Enrolment No:

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination QP, May 2021

Course: Digital Forensics I	**Semester: IV**
Program: B.Tech CSE-CSF	**Time : 03 hrs.**
Course Code: CSSF 3003	**Max. Marks: 100**

Instructions: *All questions are compulsory in Section A and Section C. There is an internal choice in Section B.*

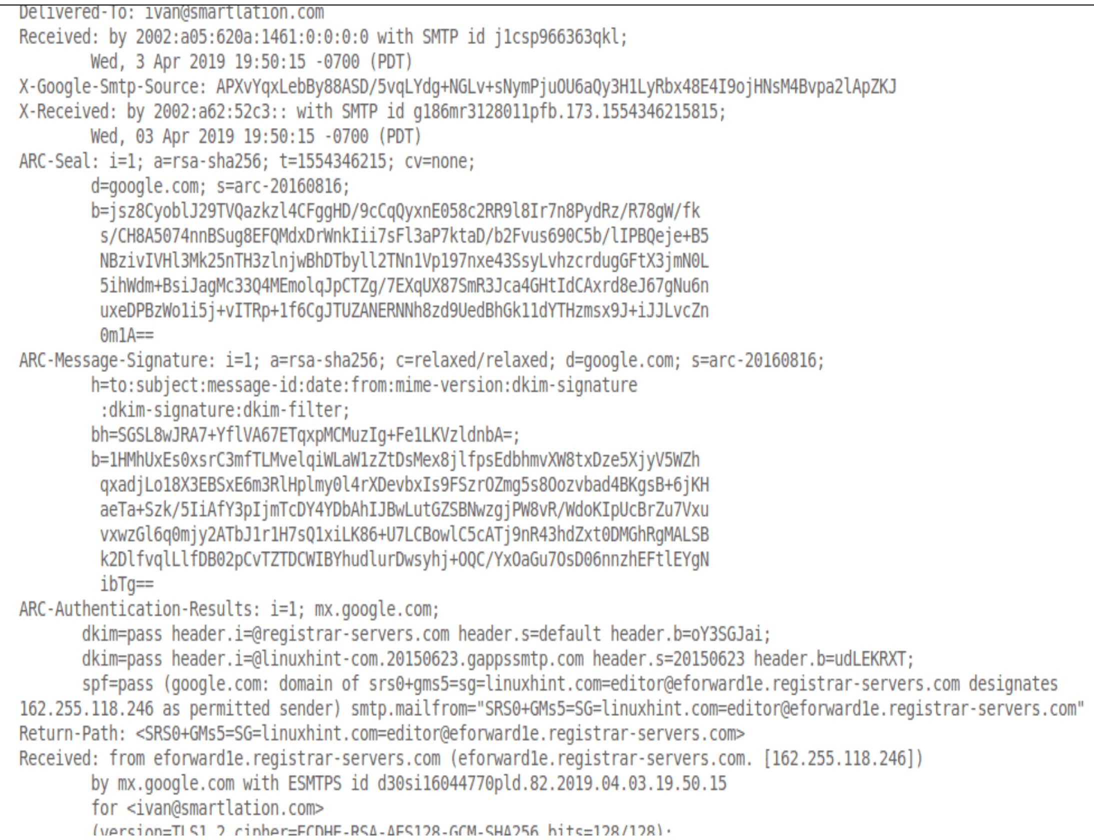
SECTION A (30 Marks)

1. **Each Question will carry 5 Marks**
2. **Instruction: This section contains FB, T/F, multiple choice, and multiple answer questions.**

S. No.		Marks	CO
Q 1	What is an incident and what are the goals of incident response?	**5**	**CO1**
Q 2	**Write the "full" volatility commands: -** i. To see the information related to the image. ii. To list the processes those were running iii. To identify the processes which could be rootkit or malware. iv. To list the dll files v. To list the connections made on network	**5**	**CO2**
Q 3	**Choose the correct answer: -** i. Which of the following is NOT a service level for the cloud? a) Platform as a service b) Infrastructure as a service c) Virtualization as a service d) Software as a service ii. With cloud systems running in a virtual environment, ________________ can give you valuable information before, during, and after an incident. a) Carving b) live acquisition c) RAM d) snapshot iii. Specially trained system and network administrators are often a CSP's first responders. (True/False)? iv. The law requires search warrants to contain specific descriptions of what's to be seized. For cloud environments, the property to be seized usually describes physical hardware rather than data, unless the CSP is a suspect. (True/False)? v. Forensics tools can directly mount VMs as external drives. (True/False)?	**5**	**CO3**
Q 4	**Choose the correct answer: -** i. The sale of sensitive or confidential company information to a competitor is known as ________. a) Industrial sabotage	**5**	**CO4**

	b) industrial espionage c) industrial collusion d) industrial betrayal ii. The acquisition format in ProDiscover Basic is the _______________. a) Raw format b) Proprietary format c) Advanced Forensic Format d) Advanced capture image iii. ________ does not recover data in free or slack space. a) Raw format acquisition b) Live acquisition c) Static acquisition d) Sparse acquisition iv. Which one of the following is not a Hashing technique? a) CRC-32 b) MD5 c) SHA 1 d) Triple DES v. When using a target drive that is FAT32 formatted, what is the maximum size limitation for split files? a) 512 MB b) 2 GB c) 1 TB d) 1 PB		
Q 5	**Identify the type of cyber-crime for each of the following situations:** a) Hacking into a web server and defacing legitimate Web pages. b) Introducing viruses, worms, and other malicious code into a network or computer. c) Unauthorized copying of copyrighted software, music, movies, arts, books. d) Internet gambling and trafficking. e) Seema is browsing the internet but while visiting one website, she repeatedly receives pop-up messages advertising pornographic content.	**5**	**CO5**
Q 6	With respect to digital evidence, state five differences between primary evidence and secondary evidence.	**5**	**CO5**

<table>
<tr><td colspan="4"><b>SECTION B (50 Marks)</b>
<b>1. Each question will carry 10 marks</b>
<b>2. Instruction: Write short / brief notes</b></td></tr>
<tr><td>Q 7</td><td>Why is it important for an investigator to capture volatile information first during an investigation? What kinds of volatile information can an investigator get from a system?</td><td><b>10</b></td><td><b>CO2</b></td></tr>
<tr><td>Q 8</td><td>A man has been arrested by the Cyber Crime Branch of the Mumbai Police for installing a secret camera in a hotel room where Samira was staying, secretly watching her activities and even records the video of this incident. With respect to this incident, answer the following questions: -
a. In what category does this type of cyber-crime fall? [1]
b. Which section/(s) of the IT Act 2000 will be applicable in this scenario? [3]
c. Explain Modus Operandi. [3]
d. What proactive measures Samira would have taken to save herself from such scam? [3]
<b>OR</b>
Suresh has been arrested by the Cyber Crime Branch of the Mumbai Police for creating a fake Facebook profile of Rani using her name and photograph, and posting sexually explicit content on it. With respect to this incident, answer the following questions: -
a. In what category does this type of cyber-crime fall? [1]
b. Which section/(s) of the IT Act 2000 will be applicable in this scenario? [3]
c. Explain Modus Operandi. [3]
d. What proactive measures Samira would have taken to save herself from such scam? [3]</td><td><b>10</b></td><td><b>CO5</b></td></tr>
<tr><td>Q 9</td><td>Explain the Standard Operating Procedure (SOP) of seizing digital evidence when the system is in POWER ON condition at the place of crime scene.</td><td><b>10</b></td><td><b>CO4</b></td></tr>
<tr><td>Q 10</td><td>Explain Incident handling and response process in detail with the help of appropriate flowchart.</td><td><b>10</b></td><td><b>CO1</b></td></tr>
<tr><td>Q 11</td><td>Explain the steps involved in email forensic investigation with reference to the below image:-</td><td><b>10</b></td><td><b>CO3</b></td></tr>
</table>



```
Delivered-To: ivan@smartlation.com
Received: by 2002:a05:620a:1461:0:0:0:0 with SMTP id j1csp966363qkl;
        Wed, 3 Apr 2019 19:50:15 -0700 (PDT)
X-Google-Smtp-Source: APXvYqxLebBy88ASD/5vqLYdg+NGLv+sNymPjuOU6aQy3H1LyRbx48E4I9ojHNsM4Bvpa2lApZKJ
X-Received: by 2002:a62:52c3:: with SMTP id g186mr3128011pfb.173.1554346215815;
        Wed, 03 Apr 2019 19:50:15 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1554346215; cv=none;
        d=google.com; s=arc-20160816;
        b=jsz8CyoblJ29TVQazkzl4CFggHD/9cCqQyxnE058c2RR9l8Ir7n8PydRz/R78gW/fk
         s/CH8A5074nnBSug8EFQMdxDrWnkIii7sFl3aP7ktaD/b2Fvus690C5b/lIPBQeje+B5
         NBzivIVHl3Mk25nTH3zlnjwBhDTbyll2TNn1Vp197nxe43SsyLvhzcrdugGFtX3jmN0L
         5ihWdm+BsiJagMc33Q4MEmolqJpCTZg/7EXqUX87SmR3Jca4GHtIdCAxrd8eJ67gNu6n
         uxeDPBzWo1i5j+vITRp+1f6CgJTUZANERNNh8zd9UedBhGk11dYTHzmsx9J+iJJLvcZn
         0m1A==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=to:subject:message-id:date:from:mime-version:dkim-signature
         :dkim-signature:dkim-filter;
        bh=SGSL8wJRA7+YflVA67ETqxpMCMuzIg+Fe1LKVzldnbA=;
        b=1HMhUxEs0xsrC3mfTLMvelqiWLaW1zZtDsMex8jlfpsEdbhmvXW8txDze5XjyV5WZh
         qxadjLo18X3EBSxE6m3RlHplmy0l4rXDevbxIs9FSzrOZmg5s8Oozvbad4BKgsB+6jKH
         aeTa+Szk/5IiAfY3pIjmTcDY4YDbAhIJBwLutGZSBNwzgjPW8vR/WdoKIpUcBrZu7Vxu
         vxwzGl6q0mjy2ATbJ1r1H7sQ1xiLK86+U7LCBowlC5cATj9nR43hdZxt0DMGhRgMALSB
         k2DlfvqlLlfDB02pCvTZTDCWIBYhudlurDwsyhj+OQC/YxOaGu7OsD06nnzhEFtlEYgN
         ibTg==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@registrar-servers.com header.s=default header.b=oY3SGJai;
       dkim=pass header.i=@linuxhint-com.20150623.gappssmtp.com header.s=20150623 header.b=udLEKRXT;
       spf=pass (google.com: domain of srs0+gms5=sg=linuxhint.com=editor@eforward1e.registrar-servers.com designates
162.255.118.246 as permitted sender) smtp.mailfrom="SRS0+GMs5=SG=linuxhint.com=editor@eforward1e.registrar-servers.com"
Return-Path: <SRS0+GMs5=SG=linuxhint.com=editor@eforward1e.registrar-servers.com>
Received: from eforward1e.registrar-servers.com (eforward1e.registrar-servers.com. [162.255.118.246])
        by mx.google.com with ESMTPS id d30si16044770pld.82.2019.04.03.19.50.15
        for <ivan@smartlation.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
```

SECTION-C (20 marks)

1. **Question carries 20 Marks.**
2. **Instruction: Write long answer.**

Q 12	With reference to Windows Forensics, answer the following questions: - a) Explain Windows (XP/7/8/10) boot process. [4] b) What kinds of volatile information can an investigator get from a Windows OS? [3] c) What kinds of non-volatile information can an investigator get from a Windows OS? [3] d) What is the purpose of Windows registry? How do malwares take advantage of registry? [4] e) How many types of registry root keys are there? Name List the function of each root key. [5] f) Name at least one tool to view and edit registry. [1]	**20**	**CO2**