UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

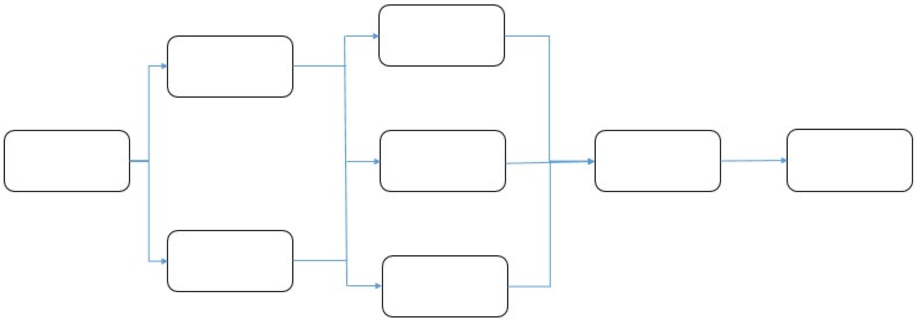
End Semester Examination, April/May 2018

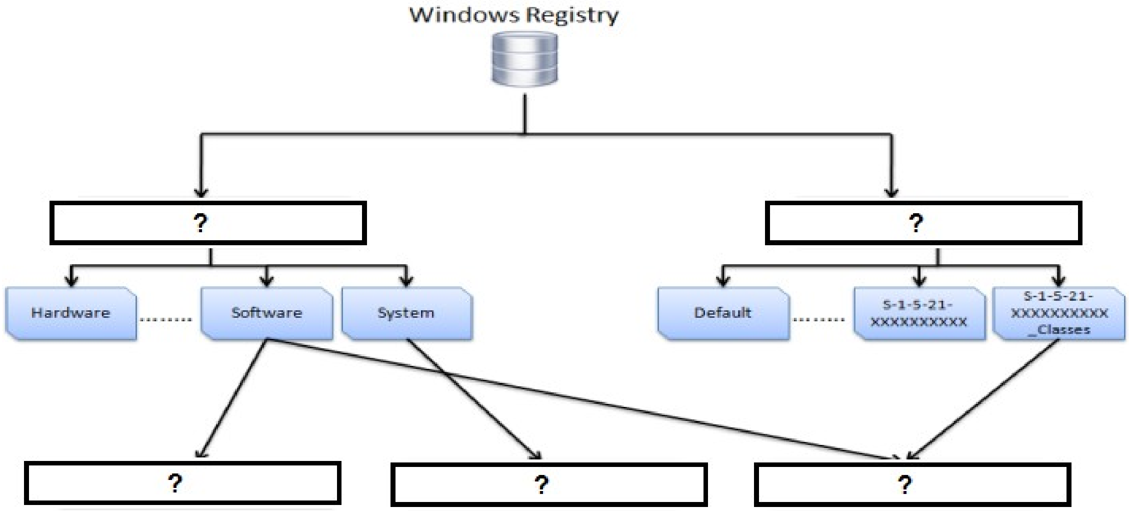
Course: Digital Forensics 1 (CSIB 363) **Semester: VI**
Program: B.Tech CSE + CSF
Time: 03 hrs. **Max. Marks: 100**

Instructions:

1. Be specific while answering the questions.
2. For cipher based question, consider ABCDEFGHIJKLMNOPQRSTUVWXYZ as your dataset and avoid spaces which encoding/decoding.
3. Indexing of dataset is 0 to 25.
4. There is an internal choice in question 11.

SECTION A

S. No.		Marks	CO
1	Consider following as the phases in forensics investigation process: ***Review, Production, Analysis, Identification, Collection, Preservation Processing, Presentation*** Arrange the processes in the flow given below: 	**4**	**CO1**
2	Map the stages and their steps which are given in jumbled order: **<u>Stages:</u>** Investigation Preparation, Analysis of Evidence, Evidence Acquisition, Results dissemination **<u>Steps:</u>** identify resources required, preserve digital evidence, process data, interpret analysis results, present findings, report findings, identify source of digital evidence, identify the purpose of investigation, and identify tools and techniques to be used. ***Note***: Each stage may have multiple steps; your answer should have stages and steps in correct order.	**4**	**CO1**
3	Draw a block diagram to demonstrate working of one complete process of Digital Signature (from Signer to Receiver).	**4**	**CO2**
4	Identify the email clients for the extensions given below: 1. .pab 2. .pst 3. .wab	**4**	**CO3**

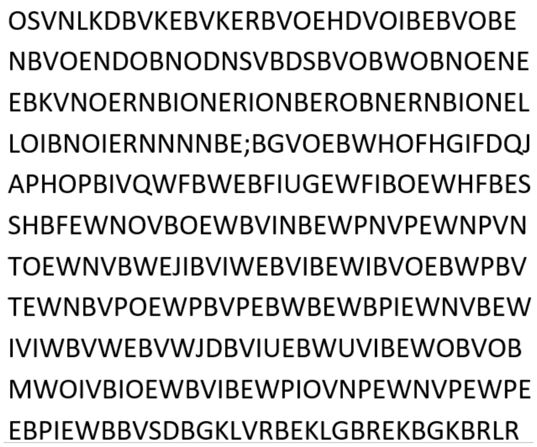
	4. .msf		
5	Identify the missing words: 1. In Linux each file or directory is uniquely identified by its name, the directory in which it resides, and a unique identifier, typically called a/an ________________ 2. __________ does not have journaling system. 3. ____________ registry hive contains information about the current hardware profile of the local computer system. 4. The main benefit of _________is that it allows journaling but don't have option to keep it off.	**4**	**CO1**
	SECTION B		
6	There are five logical root keys in the Windows Registry which are: 1. HKEY_CLASSES_ROOT. 2. HKEY_CURRENT_USER. 3. HKEY_LOCAL_MACHINE. 4. HKEY_USERS. 5. HKEY_CURRENT_CONFIG. Fit them in the blank boxes to show relationship between windows registry root keys.  Windows Registry ? ? Hardware .... Software System Default .... S-1-5-21-XXXXXXXXXX S-1-5-21-XXXXXXXXXX_Classes ? ? ?	**10**	**CO1**
7	Write the windows power shell commands for following: 1. list all children of C drive 2. List the children of the current working directory 3. Parse system and user hives 4. list all the active processes 5. lists all the established TCP connections in our system	**10**	**CO1**
8	During investigating an email, you came across an email header, which is suspected as "spoofed mail". With the help of header provided below answer the following questions: 1. What is the sender's email id?	**10**	**CO3**

2. Is it a spoofed mail based on given information?
3. Justify your answer by extracting evidences from the header below.

```
Delivered-To: jatin.sethi09@gmail.com
Received: by 10.200.113.22 with SMTP id z22csp277956qto;
        Tue, 10 Apr 2018 22:38:49 -0700 (PDT)
X-Google-Smtp-Source:
AIpwx4+ph5Ra9l5/0S3xtpSEDU+wQqZ4ikhP53Agh57b6dJ48fj7Pr+xlD8m1pMgG53+GO
iN3ZxW
X-Received: by 10.98.236.220 with SMTP id
e89mr2768588pfm.173.1523425129137;
        Tue, 10 Apr 2018 22:38:49 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1523425129; cv=none;
        d=google.com; s=arc-20160816;

b=gQTQMT8pj+HdqUppSqg9psmtZ4zZm93xpef65aRTyWEFIn2GusSsKVyZMDjFgxvrPH

a3XQSzQgZWRPYNMQ9DHrfJEHJfxwDarSjniL3LSBRlJJgETkirR6SNYQNL/cZ5BVamEz

PCtvi2vG1HmKfNm+ol762PWqpKLAorRwxRcaeauA4qLfV9yojGo9I6MU6wRvKQahocWc

cJ0sjNu928SrJXKT1MHVMY/O8ug1p6r5vvuguAkX7TsO5HhXlbqxx2zKTh7rMgtmzCgx

06XquD9C+SmXeO4h5k3RG0wB/9tCgCcWed8PNaqgf/wa9ixy5YxQRQwCSrBAyWPh/c58
         V5qA==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed;
d=google.com; s=arc-20160816;
        h=mime-version:spamdiagnosticmetadata:spamdiagnosticoutput
         :content-language:accept-language:message-id:date:thread-
index
         :thread-topic:subject:to:from:dkim-signature
         :arc-authentication-results;
        bh=9O2+tcG8+j3R55CGvptLa8HD8fUftNrVeXqhrV6QPwE=;
        b=WQB8ji8wu1Vdz/byuoagLlQIDqFn+upq8qUAEt9JLAIgr8ihwRu4C8ZY9xJ/
v1ECza

yESCFnpsM+RdC++QeB8BB/Xg8VyCRxGbWZjkN2F1m7R5TrE4vjXaYYWJswdxzBnN8jy0

k2Dej5blFzHvf2aYkESQhqxnfKzurGpMV2lwvAfHFyNjnjBrFCowSdgh3e9/NcAwFaS0

1RRDQPxf9CLBL44SNbkhnsWyHwg9fD3mkeCw1qYansKYJJyAuXSrllCocejvC6nIfU4k

AusAdAdevDZ7BOnFAry6S879486IPuwy5Hdu+PPcbBvBUMNWA1mIquOVEPLZTMWNHChm
         A5RA==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@laureateapac.onmicrosoft.com
header.s=selector1-ddn-upes-ac-in header.b=W+ucgz8H;
       spf=pass (google.com: domain of jsethi@ddn.upes.ac.in
designates 104.47.125.53 as permitted sender)
smtp.mailfrom=jsethi@ddn.upes.ac.in
Return-Path: <jsethi@ddn.upes.ac.in>
Received: from APC01-SG2-obe.outbound.protection.outlook.com (mail-
sg2apc01on0053.outbound.protection.outlook.com. [104.47.125.53])
        by mx.google.com with ESMTPS id
d17si257259pgv.576.2018.04.10.22.38.48
        for <jatin.sethi09@gmail.com>
```

```
         (version=TLS1_2 cipher=ECDHE-RSA-AES128-SHA bits=128/128);
        Tue, 10 Apr 2018 22:38:49 -0700 (PDT)
Received-SPF: pass (google.com: domain of jsethi@ddn.upes.ac.in
designates 104.47.125.53 as permitted sender) client-ip=104.47.125.53;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@laureateapac.onmicrosoft.com
header.s=selector1-ddn-upes-ac-in header.b=W+ucgz8H;
       spf=pass (google.com: domain of jsethi@ddn.upes.ac.in
designates 104.47.125.53 as permitted sender)
smtp.mailfrom=jsethi@ddn.upes.ac.in
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=laureateapac.onmicrosoft.com; s=selector1-ddn-upes-ac-in;
h=From:Date:Subject:Message-ID:Content-Type:MIME-Version;
bh=9O2+tcG8+j3R55CGvptLa8HD8fUftNrVeXqhrV6QPwE=;
b=W+ucgz8H7uVC+EzVHKglrFmGQQ7lvXsKaIJjMrLk/l0Kulj9XoFMgMYLLCT13F4L3Ct4
l40auJSG24eub+AikAFA/97wdyRrcnUNffVMSQk6+EqVnicme/
b5rDj3Y0Vby0M3VKjxw5/Czj9gB7Alch/eCkRe8k4qvYLk7qCNMi0=
Received: from PS1PR0201MB2234.apcprd02.prod.outlook.com
(10.170.181.7) by PS1PR0201MB2074.apcprd02.prod.outlook.com
(10.170.178.11) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256) id 15.20.653.12;
Wed, 11 Apr 2018 05:38:46 +0000
Received: from PS1PR0201MB2234.apcprd02.prod.outlook.com
([fe80::11fb:a503:5773:fa8d]) by
PS1PR0201MB2234.apcprd02.prod.outlook.com ([fe80::11fb:a503:5773:fa8d
%13]) with mapi id 15.20.0653.018; Wed, 11 Apr 2018 05:38:46 +0000
```

9	Explain(in 1 or 2 sentences) what following commands will do: 1. **p0f –h** 2. **p0f –L** 3. **p0f –i eth0 –p -o /root/Desktop/testdata.log**	**10**	**CO2**
	SECTION-C		
10	A 12th class reserved kind of boy who is good in mathematics is annoyed from his parents, but not telling them the reason. The parents told you that they are not able to figure out the reason but they know that their son writes everything in his daily diary in his computer. Therefore, you acquire the diary and tried to open it but it needs a **key** for which some hint is given, say **Evidence 1**. Once you are able to crack the key you find out that this boy is fond of cryptography and mathematics so he encodes what he write. Now from encoded **Evidence 2,** which uses key that was found in Evidence 1, you need to figure out the reason. **Evidence 1:**	**20**	**CO2**

	 OSVNLKDBVKEBVKERBVOEHDVOIBEBVOBE NBVOENDOBNODNSVBDSBVOBWOBNOENE EBKVNOERNBIONERIONBEROBNERNBIONEL LOIBNOIERNNNNBE;BGVOEBWHOFHGIFDQJ APHOPBIVQWFBWEBFIUGEWFIBOEWHFBES SHBFEWNOVBOEWBVINBEWPNVPEWNPVN TOEWNVBWEJIBVIWEBVIBEWIBVOEBWPBV TEWNBVPOEWPBVPEBWBEWBPIEWNVBEW IVIWBVWEBVWJDBVIUEBWUVIBEWOBVOB MWOIVBIOEWBVIBEWPIOVNPEWNVPEWPE EBPIEWBBVSDBGKLVRBEKLGBREKBGKBRLR *Hint → When nothing is going right, go left* **Evidence 2:** **W JEYT LH ZW GTSF FPCSNLM OWT ESNKK MAMDI** *Hint: French pronunciation:* ***[viʒnɛːʁ]***		
11	Choose **any 2** sections of IT Act and perform the following tasks: 1. Create a crime scenario which will later fall under sections chosen by you (maximum 8 points) 2. Identify the possible evidences. List them. 3. Identify and classify the tools which will be used for: a. Acquisition b. Examination c. Analysis 4. Write a 2-3 line summary stating the possible punishment/penalty for the case mapping with the IT Acts sections chosen by you	**20**	**CO4**

Name: **Enrolment No:**	

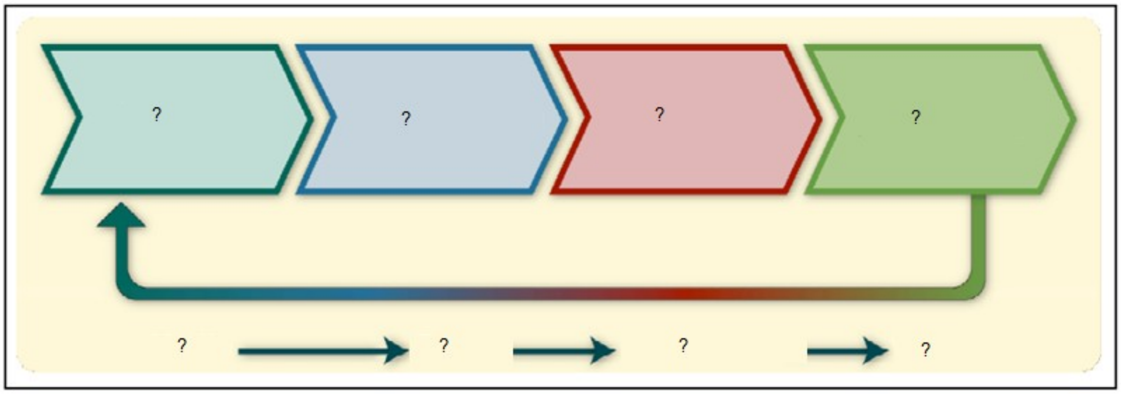
UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, April/May 2018

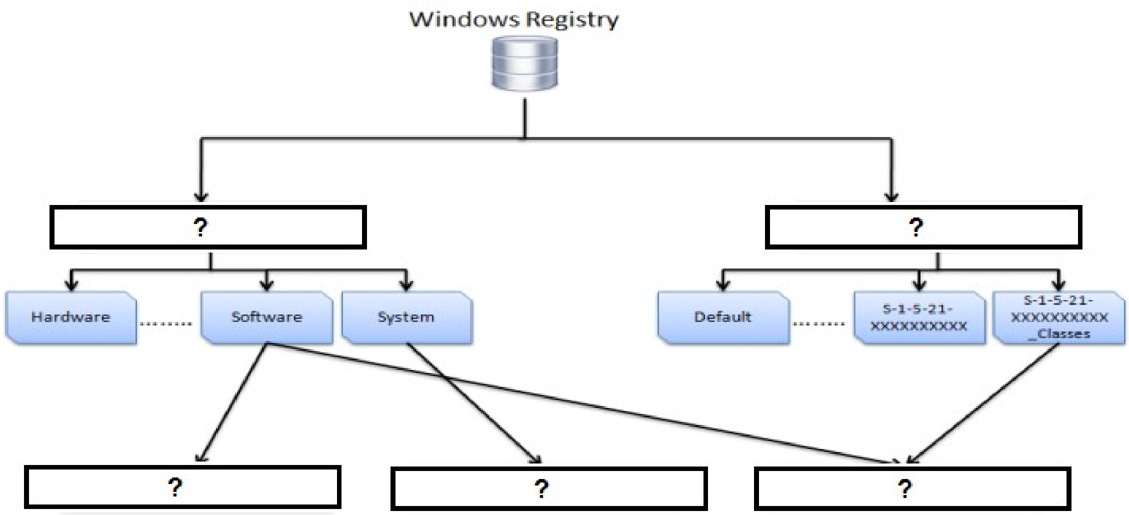
Course: Digital Forensics 1 (CSIB 363) **Semester: VI**
Program: B.Tech CSE + CSF
Time: 03 hrs. **Max. Marks: 100**

Instructions:

1. Be specific while answering the questions.
5. For cipher based question, consider ABCDEFGHIJKLMNOPQRSTUVWXYZ as your dataset and avoid spaces which encoding/decoding.
2. Indexing of dataset is 0 to 25.
3. There is an internal choice in question 11.

SECTION A

S. No.		**Marks**	**CO**
1	Map the stages and their steps which are given in jumbled order: **Stages:** Investigation Preparation, Analysis of Evidence, Evidence Acquisition, Results dissemination **Steps:** identify resources required, preserve digital evidence, process data, interpret analysis results, present findings, report findings, identify source of digital evidence, identify the purpose of investigation, and identify tools and techniques to be used. Note: Each stage may have multiple steps, your answer should have stages and steps in correct order.	**4**	**CO1**
2	Complete the diagram as per NIST 800-86: 	**4**	**CO1**
3	Draw a block diagram to demonstrate working of one complete process of Asymmetric Key Algorithm (from Sender to Receiver).	**4**	**CO2**
4	Identify the email clients for the extensions given below: 1. .mbx 2. .pst	**4**	**CO3**

	3. .eml 4. .msf		
5	Identify the missing words: 1. In Linux each file or directory is uniquely identified by its name, the directory in which it resides, and a unique identifier, typically called a/an _______________ 2. _________ is a supervisor directory commands, configuration files, disk configuration files, valid user lists, groups, ethernet, hosts, where to send critical messages. 3. ___________ registry hive contains information about the current hardware profile of the local computer system. 4. The main benefit of ________is that it allows journaling and have option to keep it off.	**4**	**CO1**
SECTION B			
6	There are five logical root keys in the Windows Registry, which are 1. HKEY_CLASSES_ROOT. 2. HKEY_CURRENT_USER. 3. HKEY_LOCAL_MACHINE. 4. HKEY_USERS. 5. HKEY_CURRENT_CONFIG. Fit them in the blank boxes to show relationship between windows registry root keys.  Windows Registry ? ? Hardware Software System Default S-1-5-21-XXXXXXXXXX S-1-5-21-XXXXXXXXXX_Classes ? ? ?	**10**	**CO1**
7	Write the windows power shell commands for following: 1. get a list of all the available event logs 2. list the Security, Application and System event logs 3. lists all the established TCP connections in our system 4. list all the active processes 5. list all children of C drive	**10**	**CO1**
8	During investigating an email, you came across an email header which is suspected as "spoofed mail". With the help of header provided below answer the following	**10**	**CO3**

questions:

1. What is the sender's email id?
2. Is it a spoofed mail based on given information?
3. Justify your answer by extracting evidences from the header below.

```
Delivered-To: jatin.sethi09@gmail.com
Received: by 10.200.113.22 with SMTP id z22csp283435qto;
        Tue, 10 Apr 2018 22:47:38 -0700 (PDT)
X-Google-Smtp-Source:
AIpwx48+WGC8Kfh2kgprhe7Ft0PxiZfBwP4zhC5NjkT/Q7JtEZ9FwUO/DGAnPV5TJM9Qhc
CAk4tY
X-Received: by 2002:a25:4e83:: with SMTP id c125-
v6mr1604155ybb.17.1523425658195;
        Tue, 10 Apr 2018 22:47:38 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1523425658; cv=none;
        d=google.com; s=arc-20160816;

b=EIk2b8qb/FFzOIfcf24iRScYUJSriPQQmevHh+WREq06iXcFGUmz0hEL/nLy5CvqKw

LYfN1Ba+czNCIeT6pSdFd91bXO2mbm/4Yq3Wr9cxATW/D1qOJqTGm8ZeE+AymZeS+smM

42pSR8HwWkCQSJ5E5Fg1tksTUuJRXk1/3/s8HyFDg46TGtqFsjCvp1E/IsBhCQhnZoxW

06OLnl7tnv2StX1g+hN8lLQrpmzdWXHLe6dMk08Ecs7ntMrQXd6xj12a+F15EokIR2GM

h+kL/GUPpdyvU778UfcgvZqFaN9jDt47eG2Mnfpoia6am7kdDt1AMl7d2YF/HVZlk5eH
         2QQg==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed;
d=google.com; s=arc-20160816;
        h=x_awex_uid:date:message-id:from:mime-version:subject:to
         :arc-authentication-results;
        bh=jYJmgH0mn5PeUOZ34Iz/UP94df2RussqT2tLRAlbx60=;

b=SP5wxO6eQG1/AeSqBzTjnd0xsRAHdUZeLIfWcbYEEQoZPa+T5KuUi9HdcC/e5LCJOf

9Rk59GKzg60Zxj2dqqugteECSdT/e07Au1jjQmcXjmCuNGtkp5+eHkc494ftbduSC5oB

uqN9FT428RgDvy/LAq0G6PSaBFU4Z9TrjrlNxMyXU6Y0Cz/9PeT+kMh+bOkuqDGR/gk7

3f4d/wzzyJTvFBAjOrd/RWWBVspxvXh1GWGSswUjFBoIaC4R6SYW0tw92wuwrXpZ+Epl

PL9ugIWH0/16JXP9AZI477BYZSyPKxUOL+i7I6GGqYugsqVtIe3xqABAZYRpypFv0e3L
         upYQ==
ARC-Authentication-Results: i=1; mx.google.com;
       spf=pass (google.com: best guess record for domain of
5370554@us-imm-node6c.000webhost.io designates 153.92.0.72 as
permitted sender) smtp.mailfrom=5370554@us-imm-node6c.000webhost.io
Return-Path: <5370554@us-imm-node6c.000webhost.io>
Received: from us-imm-postlady1.000webhost.io (us-imm-
postlady1.000webhost.io. [153.92.0.72])
        by mx.google.com with ESMTPS id
a189si80298ywf.522.2018.04.10.22.47.38
        for <jatin.sethi09@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256
bits=128/128);
        Tue, 10 Apr 2018 22:47:38 -0700 (PDT)
Received-SPF: pass (google.com: best guess record for domain of
5370554@us-imm-node6c.000webhost.io designates 153.92.0.72 as
permitted sender) client-ip=153.92.0.72;
Authentication-Results: mx.google.com;
       spf=pass (google.com: best guess record for domain of
5370554@us-imm-node6c.000webhost.io designates 153.92.0.72 as
permitted sender) smtp.mailfrom=5370554@us-imm-node6c.000webhost.io
Received: from [127.0.0.1] (localhost [127.0.0.1]); Wed, 11 Apr 2018
05:47:37 +0000 (UTC)
To: jatin.sethi09@gmail.com
Subject: Test 2
X-PHP-Originating-Script: 5370554:external_email_send.php
MIME-Version: 1.0
Content-type: text/html;charset=UTF-8
```

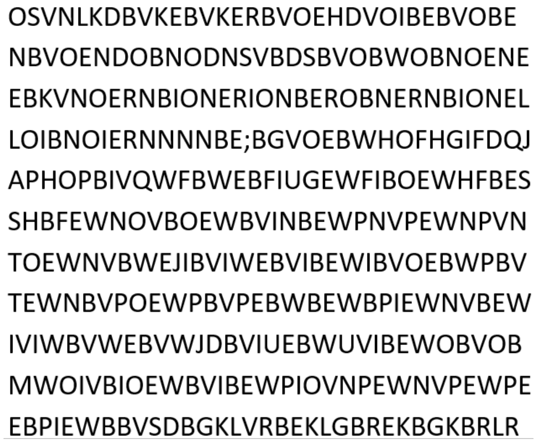
9 Explain(in 1 or 2 sentences) what following commands will do: **10** **CO2**

1. **$ hashdeep <filename>**
2. **$ hashdeep -r <directory>**
3. **$ hashdeep -e <directory/file>**

SECTION-C

10 A 12th class reserved kind of boy who is good in mathematics is annoyed from his parents, but not telling them the reason. The parents told you that they are not able to figure out the reason but they know that their son writes everything in his daily diary in his computer. Therefore, you acquire the diary and tried to open it but it needs a **key** for which some hint is given, say **Evidence 1**. Once you are able to crack the key you find out that this boy is fond of cryptography and mathematics so he encodes what he write. Now from encoded **Evidence 2,** which uses key that was found in Evidence 1, you need to figure out the reason. **20** **CO2**

Evidence 1:



OSVNLKDBVKEBVKERBVOEHDVOIBEBVOBE
NBVOENDOBNODNSVBDSBVOBWOBNOENE
EBKVNOERNBIONERIONBEROBNERNBIONEL
LOIBNOIERNNNNBE;BGVOEBWHOFHGIFDQJ
APHOPBIVQWFBWEBFIUGEWFIBOEWHFBES
SHBFEWNOVBOEWBVINBEWPNVPEWNPVN
TOEWNVBWEJIBVIWEBVIBEWIBVOEBWPBV
TEWNBVPOEWPBVPEBWBEWBPIEWNVBEW
IVIWBVWEBVWJDBVIUEBWUVIBEWOBVOB
MWOIVBIOEWBVIBEWPIOVNPEWNVPEWPE
EBPIEWBBVSDBGKLVRBEKLGBREKBGKBRLR

Hint → When nothing is going right, go left

Evidence 2:

	W JEYT LH ZW GTSF FPCSNLM OWT ESNKK MAMDI *Hint: French pronunciation:* ***[viʒnɛːʁ]***		
11	Choose **any 2** sections of IT Act and perform the following tasks: 1. Create a crime scenario which will later fall under sections chosen by you (maximum 8 points) 2. Identify the possible evidences. List them. 3. Identify and classify the tools which will be used for: a. Acquisition b. Examination c. Analysis 4. Write a 2-3 line summary stating the possible punishment/penalty for the case mapping with the IT Acts sections chosen by you	**20**	**CO4s**