



Model Question Paper (Blank) is on next page

Name:		
Enrolment No:		
UNIVERSITY OF PETROLEUM AND ENERGY STUDIES End Semester Examination, May 2020		
Course: Cyber Forensics & Cyber Security Program: LL.M. Course Code: CLLT7001		Semester: II Time: 03 hrs. Max. Marks: 100
Instructions: Attempt all questions. Marks are mentioned against each questions.		
SECTION A		(30-50 Words for each answer)
S. No.	Write short notes on the following:	Marks
Q 1	Network Forensics	5
Q 2	Documentary Evidence	5
Q 3	Mobile Phone Forensics	5
Q 4	Scanner Forensics	5
Q 5	Electronic record	5
Q 6	Steganography	5
SECTION B		(100-150 Words for each answer)
Q 7	Define computer forensic. Explain at least two techniques for computer forensic investigation	10
Q 8	Explain the difference between copying and imaging of a hard disk.	10
Q 9	Differentiate between Public Key Cryptography and Private Key Cryptography.	10
Q 10	Define Computer Forensic Toolkit. What standard features should be built in a toolkit? How are these useful in computer forensic analysis of digital evidence?	10
Q 11	What is spoofing? Explain Caller ID spoofing, Email Spoofing, Web Spoofing in brief.	10
SECTION-C		(300-500 Words)
Q 10	<p>The Supreme Court has reiterated in a number of cases that any electronic record in the form of secondary evidence cannot be admitted in evidence unless a certificate under Section 65B (4) of the Evidence Act is produced. One of the important judgment states that “an electronic record by way of secondary evidence shall not be admitted in evidence unless the requirements under Section 65B are satisfied. Thus, in the case of CD, VCD, chip, etc., the same shall be accompanied by the certificate in terms of the concerned Section.”</p> <p><i>On the basis of above stated problem, answer the following questions. Yes/No is not acceptable. Justify your answer with relevant case laws. All questions carry equal marks. (10 X 2)</i></p> <p>1. Explain the need, importance, and contents of the above mentioned certificate.</p>	20

	2. Is certification required for production of electronic evidence? Explain with recent case law.	
Name:		
Enrolment No:		
UNIVERSITY OF PETROLEUM AND ENERGY STUDIES End Semester Examination, May 2020		
Course: Cyber Forensics & Cyber Security	Semester: II	
Program: LL.M.	Time: 03 hrs.	
Course Code: CLLT7001	Max. Marks: 100	
Instructions: Attempt all questions. Marks are mentioned against each questions.		
SECTION A		(30-50 Words for each answer)
S. No.	Write short notes on the following:	Marks
Q 1	Denial of Service attack	5
Q 2	Data acquisition	5
Q 3	VoIP based services	5
Q 4	Email bombing	5
Q 5	Electronic record	5
Q 6	Steganography	5
SECTION B		(100-150 Words for each answer)
Q 7	What is spoofing? Explain Caller ID spoofing, Email Spoofing, Web Spoofing in brief.	10
Q 8	What is volatile data? How it is useful in computer forensic investigation? Explain the method and tools for capturing volatile data.	10
Q 9	Explain the difference between copying and imaging of a hard disk.	10
Q 10	Elucidate the steps of Cyber Forensic Investigation Process.	10
Q 11	Differentiate between Public Key Cryptography and Private Key Cryptography.	10
SECTION-C		(300-500 Words)
Q 12	<p>. Data breaches resulting from web application hacking are almost always accomplished through the exploitation of application vulnerabilities like SQL injection (web hacking technique) or cross-site scripting. If cyber security is not improved at a larger scale, the industry will continue to be plagued with security incidents that result in data breaches or other consequences that are even more disastrous. Changing the attitude toward cyber security, however, would require a culture shift, a shift that places importance on proactive risk management rather than immediate return on investment. This shift won't happen overnight. In the meantime, cyber security professionals should follow these recommendations to implement a few immediate measures to effect positive changes:</p> <ul style="list-style-type: none"> • Demand software quality and security from suppliers. 	20

- Perform stringent acceptance tests for third-party code.
- Disable default accounts from applications.
- Establish a secure operational environment for applications.
- Implement effective bug-reporting and handling.

As the buyer side starts to demand secure cyber software, the power balance will start to shift toward more strategic approaches to managing cyber-level risks. Cyber security professionals can encourage this change by engaging in these longer-term initiatives:

- Work toward an industry certification program for secure development practices.
- Implement a cyber-security program.
- Continue to drive awareness of the changing cyber threat landscape.

So, in order to improve cyber security, companies and cyber security professionals should work in a concerted fashion to cultivate a culture that values and promotes cyber security. To help usher in such a culture, cyber security professionals should:

- Do their part to promote a cyber-security ecosystem.
- Use mobile proliferation as a catalyst for cyber security.

Cybercriminals from China have spent more than six years cautiously working to obtain data from more than 70 government agencies, corporations and non-profit groups. The campaign, named Operation Shady RAT (remote access tool) was discovered by the security firm McAfee. The loss of this data represents a massive economic cyber threat not just to individual companies and industries, but to entire countries that face the prospect of decreased economic growth in a suddenly more competitive landscape; the loss of jobs in industries that lose out to unscrupulous competitors in another part of the world; not to mention, the national security impact of the loss of sensitive intelligence or defense information.

On the basis of above stated problem, answer the following questions. Yes/No is not acceptable. Justify your answer with relevant case laws. All questions carry equal marks. (10 X 2)

1. In order to implement a few immediate measures to effect positive changes, what recommendations should cyber security professionals follow?
2. Cyber security professionals can encourage change by engaging in which longer-term initiatives?