# Sixth Semester

## Information Technology / Computer Science & Engineering

## Scheme OCBC 2022

## NETWORK FORENSICS

***Time : Three Hours*** ***Maximum Marks : 70***

**Note :** i) Attempt total ***six*** questions. Question No. **1** (Objective type) is compulsory. From the remaining questions attempt any ***five***.

कुल **छः** प्रश्न हल कीजिए। प्रश्न क्रमांक **1** (वस्तुनिष्ठ प्रकार का) अनिवार्य है। शेष प्रश्नों में से किन्हीं **पाँच** को हल कीजिए।

ii) In case of any doubt or dispute, the English version question should be treated as final.

किसी भी प्रकार के संदेह अथवा विवाद की स्थिति में अंग्रेजी भाषा के प्रश्न को अंतिम माना जायेगा।

1. Choose the correct answer. 2 each

सही उत्तर का चयन कीजिए।

i) Which one of the following is not a function of network layer?

(a) Congestion control (b) Error control

(c) Routing (d) Inter-networking

इनमें से कौन-सी नेटवर्क लेयर का फंक्शन नही हैं

(अ) कंजेशन कंट्रोल (ब) ऐरर कंट्रोल

(स) रूटींग (द) इंटर-नेटवर्किंग

ii) Which of this is not a network edge device?

(a) Switch (b) PC

(c) Smartphones (d) Servers

इनमें से कौन-सी नेटवर्क ऐज डिवाईस नहीं है?

(अ) स्विच (ब) PC

(स) स्मार्टफोन्स (द) सर्वर

iii) Which of the following is an example of Bluetooth?

(a) Wide area network (b) Virtual private network

(c) Local area network (d) Personal area network

इनमें से कौन–सा ब्लूटूथ का उदाहरण है

(अ) वाइड एरिया नेटवर्क (ब) वर्चुअल प्राइवेट नेटवर्क

(स) लोकल एरिया नेटवर्क (द) पर्सनल एरिया नेटवर्क

iv) Network layer at source is responsible for creating a packet from data coming from another _____.

(a) Station (b) Link

(c) Node (d) Protocol

नेटवर्क लेयर दूसरी तरफ से आने वाले डाटा के द्वारा क्रिएट किये गये पैकेट के रिस्पांसिबल होती है _____

(अ) स्टेशन (ब) लिंक

(स) नोड (द) प्रोटाकॉल

v) Identify the protocol primarily used of browsing data.

ब्राउजिंग डाटा के लिये शुरूआत में उपयोग होने वाले प्रोटोकॉल को पहचानिए।

(a) FTP (b) TCP

(c) TFTP (d) HTTP

2. a) Explain networking concepts and protocol. 7

नेटवर्किंग कान्सेप्ट्स और प्रोटोकाल्स को समझाइए।

b) Define various aspects of network forensics in detail. 5

नेटवर्क फारेंसिक्स के वेरियस आस्पेक्ट्स को विस्तार से परिभाषित कीजिए।

3. a) What do you mean by wire shark and TCP dump? Explain it. 8

वायर शार्क और TCP डम्प से आपका क्या अर्थ है? समझाइए।

b) Explain network port mirroring, snooping and scanning tools in detail. 4

नेटवर्क पोर्ट मिररींग, स्नूपिंग और स्केनिंग टूल्स को विस्तार से समझाइए।

4. a) Explain ethernet switch logs and MAC table in detail. 6

इथरनेट स्विच लॉग्स और मेक टेबलस् को विस्तार से समझाइए।

b) Define data link layer and physical layer with suitable diagram. 6

डाटा लिंक लेयर और फिजिकल लेयर उपयुक्त चित्र की सहायता से परिभाषित कीजिए।

5. a) What do you mean by router logs and Wi-Fi device logs? Explain it. 4

रूटर लाग्स और वाई-फाय डिवाईस लाग्स से आपका क्या अर्थ है? समझाइए।

b) Explain firewall logs with suitable diagram. 8

फायरवाल लाग्स को उपयुक्त चित्र के द्वारा समझाइए।

6. a) Describe enabling and examining server logs in detail. 7

सर्वर लाग्स इनेबलिंग और एग्जामिनिंग को विस्तार से वर्णित कीजिए।

b) Explain browser history analysis and proxy server logs with one example. 5

ब्राउजर हिस्टरी एनालिसिस और प्राक्सी सर्वर लाग्स को एक उदाहरण देकर समझाइए।

7. a) Write limitations and challenges of network forensics due to encryption. 6

एन्क्रीप्शन के कारण फारेंसिक नेटवर्क की सीमाएँ एंव चैलेंजेस को लिखिए।

b) Define spoofing, mobility and storage limitations in detail. 6

स्पूफिंग, मोबाइलिटी और स्टोरेज लिमिटेशन को विस्तार से परिभाषित कीजिए।