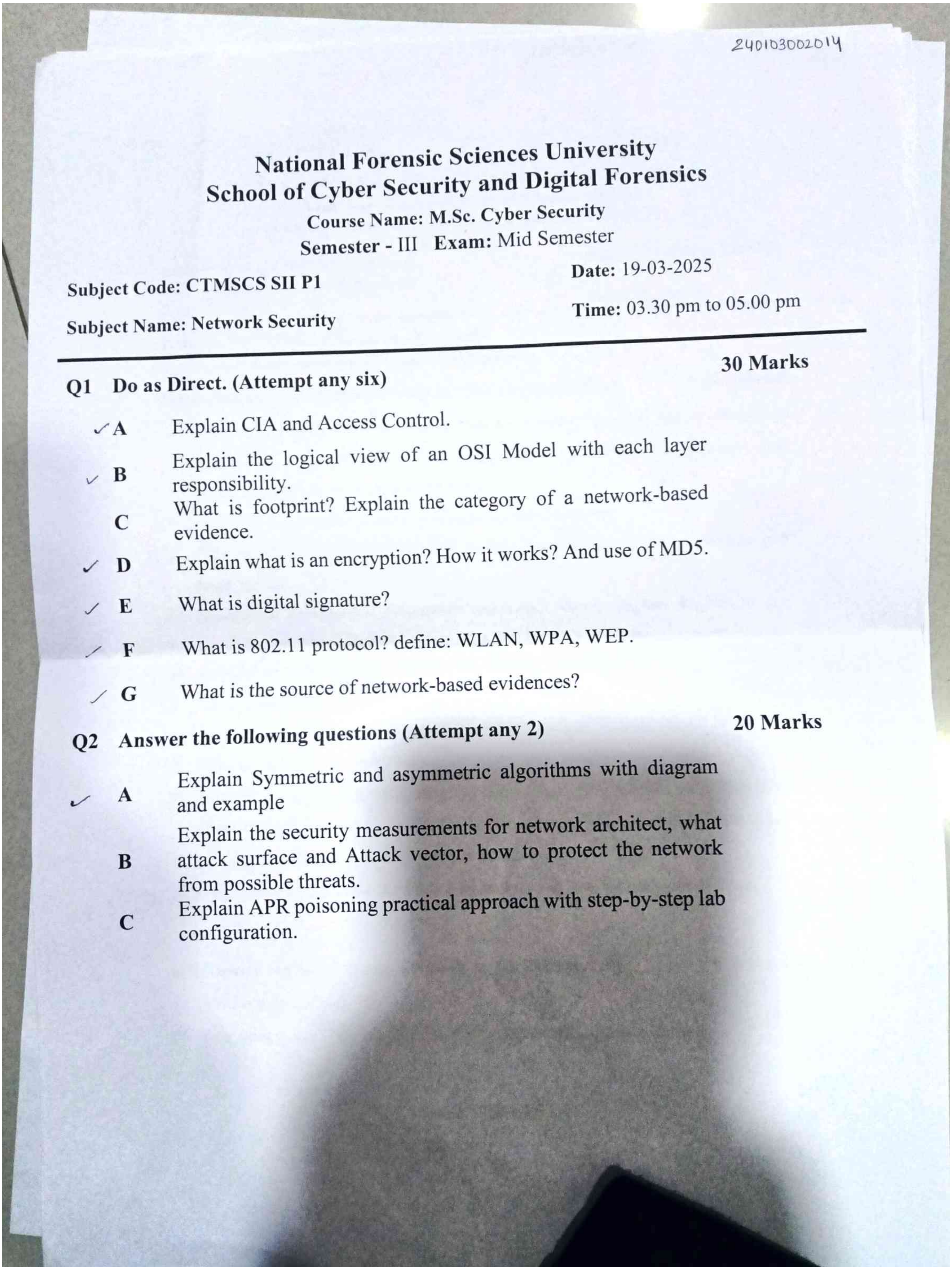


240103002014

National Forensic Sciences University
School of Cyber Security and Digital Forensics

Course Name: M.Sc. Cyber Security

Semester - III **Exam:** Mid Semester

Subject Code: CTMSCS SII P1

Date: 19-03-2025

Subject Name: Network Security

Time: 03.30 pm to 05.00 pm

Q1 Do as Direct. (Attempt any six) **30 Marks**

✓ **A** Explain CIA and Access Control.

✓ **B** Explain the logical view of an OSI Model with each layer responsibility.

C What is footprint? Explain the category of a network-based evidence.

✓ **D** Explain what is an encryption? How it works? And use of MD5.

✓ **E** What is digital signature?

✓ **F** What is 802.11 protocol? define: WLAN, WPA, WEP.

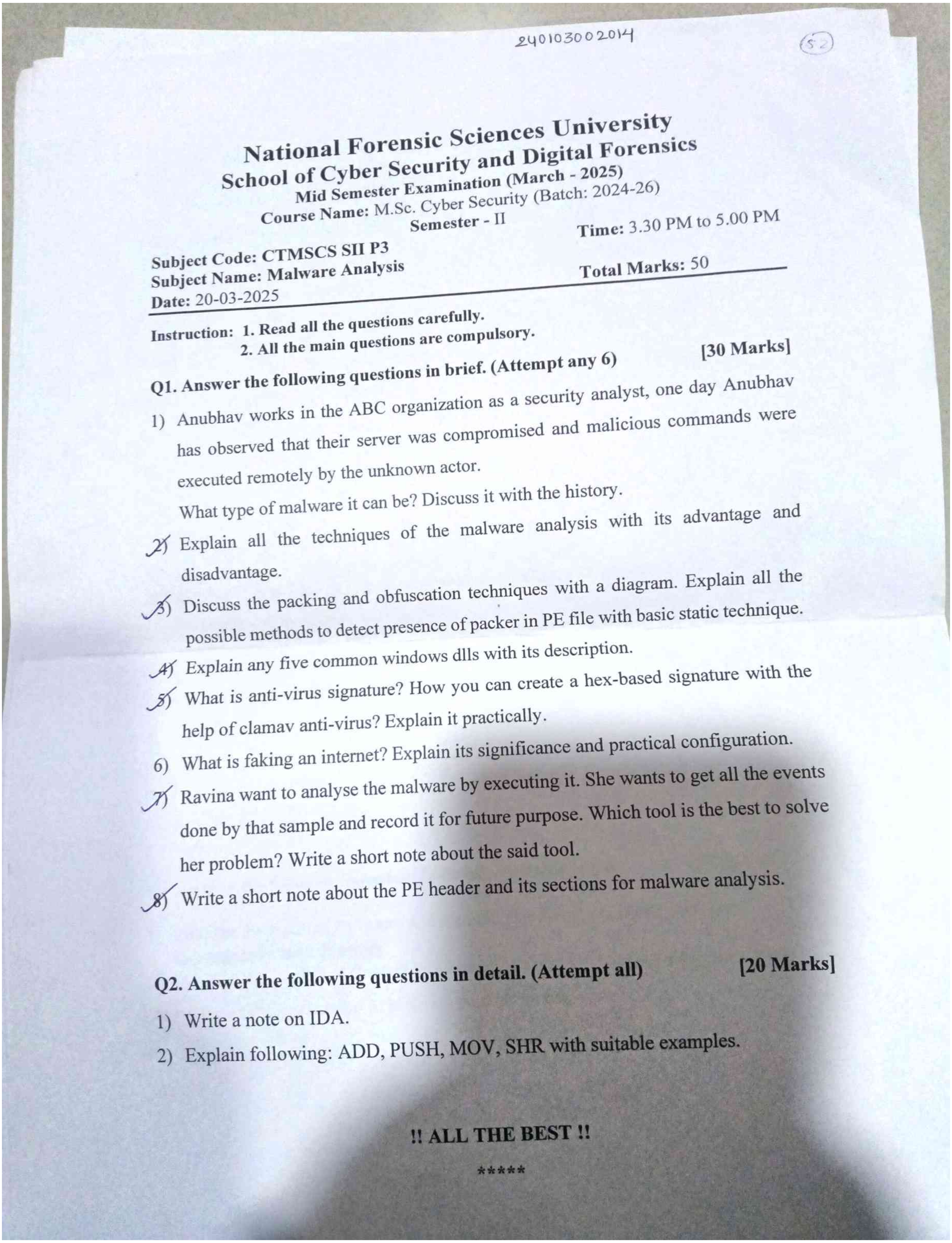
✓ **G** What is the source of network-based evidences?

Q2 Answer the following questions (Attempt any 2) **20 Marks**

✓ **A** Explain Symmetric and asymmetric algorithms with diagram and example

B Explain the security measurements for network architect, what attack surface and Attack vector, how to protect the network from possible threats.

C Explain APR poisoning practical approach with step-by-step lab configuration.



240103002014

52

National Forensic Sciences University

School of Cyber Security and Digital Forensics

Mid Semester Examination (March - 2025)

Course Name: M.Sc. Cyber Security (Batch: 2024-26)

Semester - II

Subject Code: CTMSCS SII P3 **Time:** 3.30 PM to 5.00 PM

Subject Name: Malware Analysis **Total Marks:** 50

Date: 20-03-2025

Instruction: 1. Read all the questions carefully.
2. All the main questions are compulsory.

Q1. Answer the following questions in brief. (Attempt any 6) **[30 Marks]**

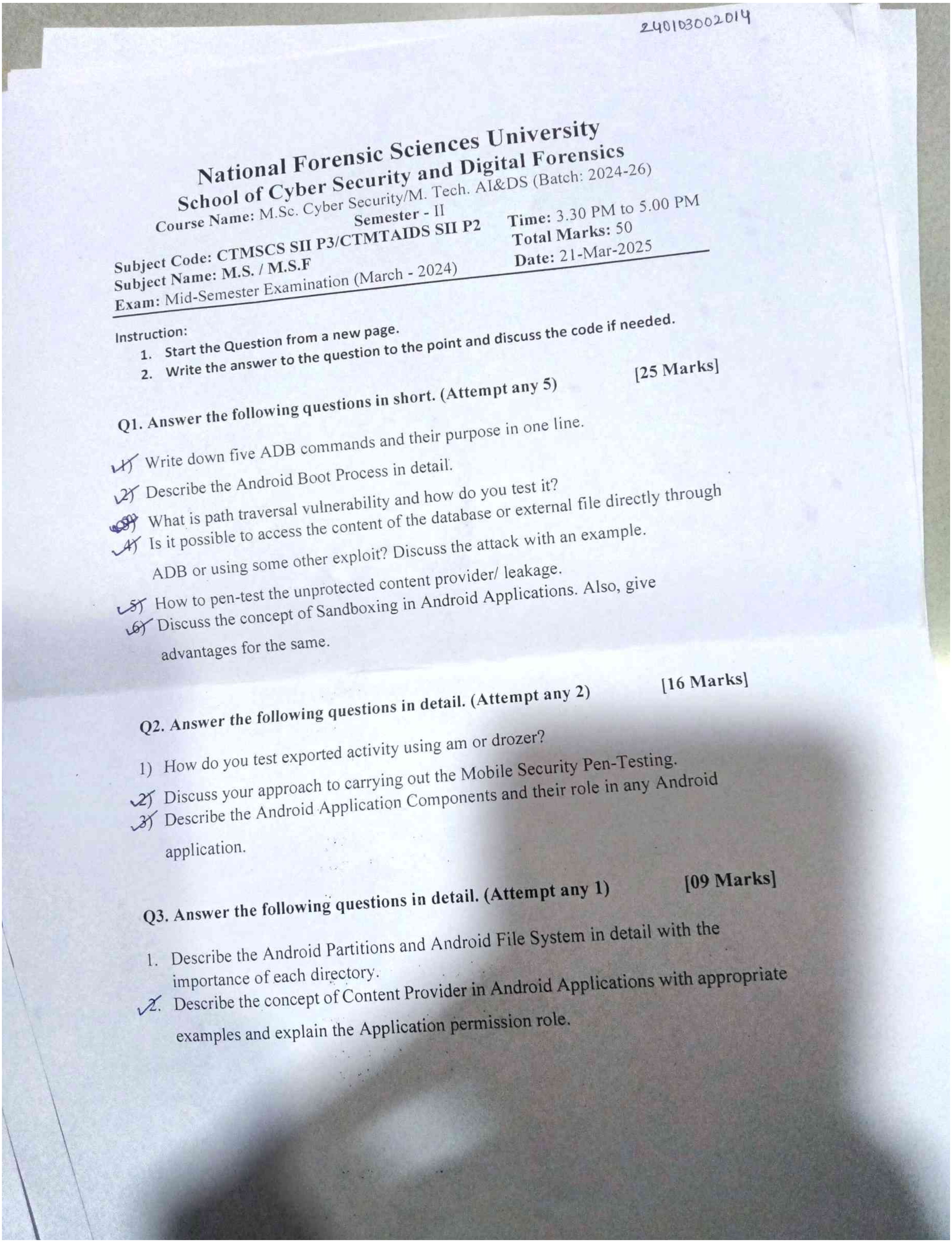
1) Anubhav works in the ABC organization as a security analyst, one day Anubhav has observed that their server was compromised and malicious commands were executed remotely by the unknown actor.
   What type of malware it can be? Discuss it with the history.
2) Explain all the techniques of the malware analysis with its advantage and disadvantage.
3) Discuss the packing and obfuscation techniques with a diagram. Explain all the possible methods to detect presence of packer in PE file with basic static technique.
4) Explain any five common windows dlls with its description.
5) What is anti-virus signature? How you can create a hex-based signature with the help of clamav anti-virus? Explain it practically.
6) What is faking an internet? Explain its significance and practical configuration.
7) Ravina want to analyse the malware by executing it. She wants to get all the events done by that sample and record it for future purpose. Which tool is the best to solve her problem? Write a short note about the said tool.
8) Write a short note about the PE header and its sections for malware analysis.

Q2. Answer the following questions in detail. (Attempt all) **[20 Marks]**

1) Write a note on IDA.
2) Explain following: ADD, PUSH, MOV, SHR with suitable examples.

!! ALL THE BEST !!

****



240103002014

National Forensic Sciences University

School of Cyber Security and Digital Forensics

Course Name: M.Sc. Cyber Security/M. Tech. AI&DS (Batch: 2024-26)

Semester - II

Subject Code: CTMSCS SII P3/CTMTAIDS SII P2 **Time:** 3.30 PM to 5.00 PM

Subject Name: M.S. / M.S.F **Total Marks:** 50

Exam: Mid-Semester Examination (March - 2024) **Date:** 21-Mar-2025

Instruction:

1. **Start the Question from a new page.**
2. **Write the answer to the question to the point and discuss the code if needed.**

Q1. Answer the following questions in short. (Attempt any 5) **[25 Marks]**

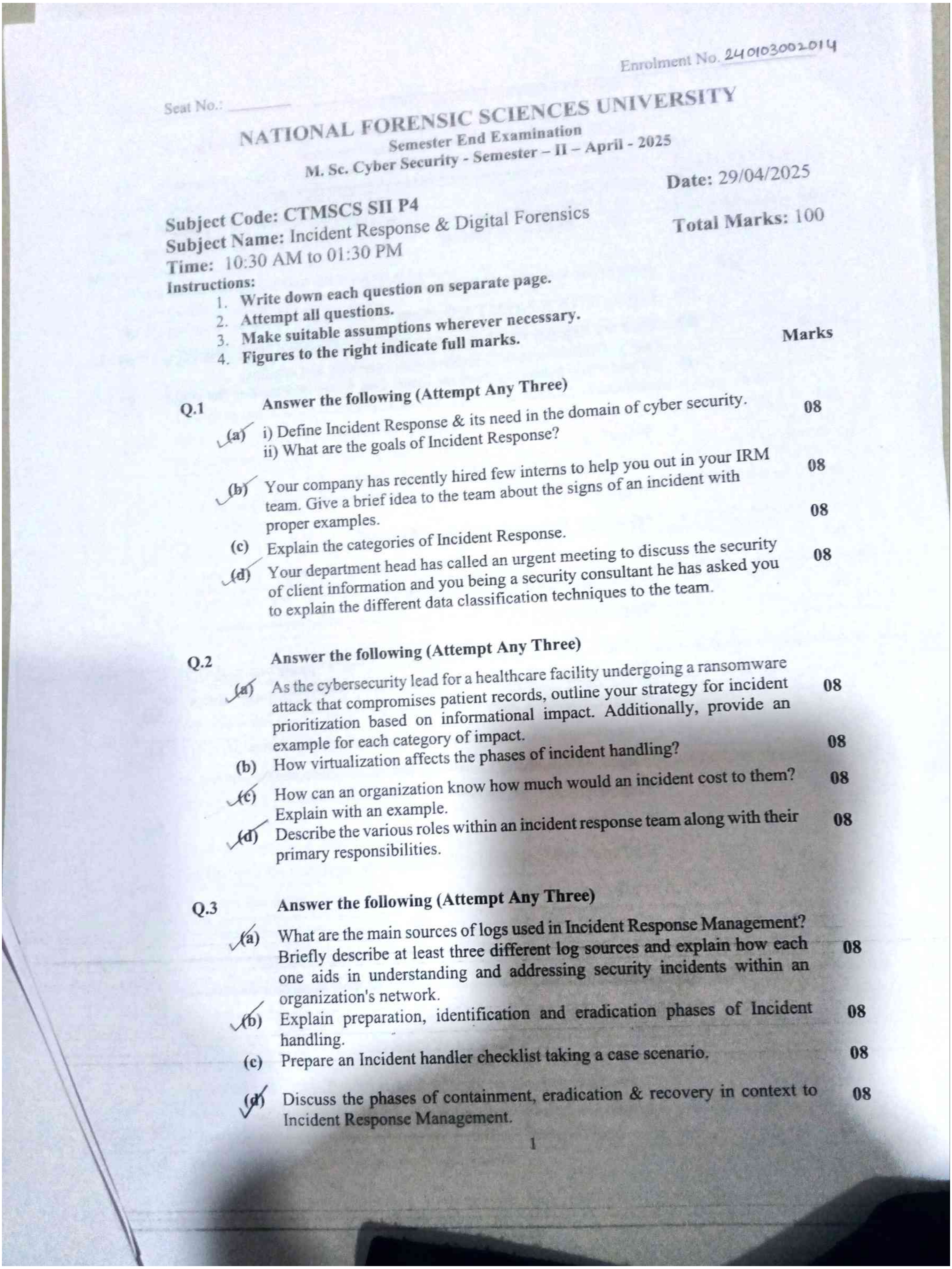
1) Write down five ADB commands and their purpose in one line.
2) Describe the Android Boot Process in detail.
3) What is path traversal vulnerability and how do you test it?
4) Is it possible to access the content of the database or external file directly through ADB or using some other exploit? Discuss the attack with an example.
5) How to pen-test the unprotected content provider/ leakage.
6) Discuss the concept of Sandboxing in Android Applications. Also, give advantages for the same.

Q2. Answer the following questions in detail. (Attempt any 2) **[16 Marks]**

1) How do you test exported activity using am or drozer?
2) Discuss your approach to carrying out the Mobile Security Pen-Testing.
3) Describe the Android Application Components and their role in any Android application.

Q3. Answer the following questions in detail. (Attempt any 1) **[09 Marks]**

1. Describe the Android Partitions and Android File System in detail with the importance of each directory.
2. Describe the concept of Content Provider in Android Applications with appropriate examples and explain the Application permission role.



Enrolment No. 240103002014

Seat No.: ________

NATIONAL FORENSIC SCIENCES UNIVERSITY

Semester End Examination

M. Sc. Cyber Security - Semester – II – April - 2025

Date: 29/04/2025

Subject Code: CTMSCS SII P4
Subject Name: Incident Response & Digital Forensics
Time: 10:30 AM to 01:30 PM

Total Marks: 100

Instructions:

1. **Write down each question on separate page.**
2. **Attempt all questions.**
3. **Make suitable assumptions wherever necessary.**
4. **Figures to the right indicate full marks.**

Marks

Q.1 **Answer the following (Attempt Any Three)**

[✓ **(a)**] i) Define Incident Response & its need in the domain of cyber security. ii) What are the goals of Incident Response? **08**

[✓ **(b)**] Your company has recently hired few interns to help you out in your IRM team. Give a brief idea to the team about the signs of an incident with proper examples. **08**

(c) Explain the categories of Incident Response. **08**

[✓ **(d)**] Your department head has called an urgent meeting to discuss the security of client information and you being a security consultant he has asked you to explain the different data classification techniques to the team. **08**

Q.2 **Answer the following (Attempt Any Three)**

[✓ **(a)**] As the cybersecurity lead for a healthcare facility undergoing a ransomware attack that compromises patient records, outline your strategy for incident prioritization based on informational impact. Additionally, provide an example for each category of impact. **08**

(b) How virtualization affects the phases of incident handling? **08**

[✓ **(c)**] How can an organization know how much would an incident cost to them? Explain with an example. **08**

[✓ **(d)**] Describe the various roles within an incident response team along with their primary responsibilities. **08**

Q.3 **Answer the following (Attempt Any Three)**

[✓ **(a)**] What are the main sources of logs used in Incident Response Management? Briefly describe at least three different log sources and explain how each one aids in understanding and addressing security incidents within an organization's network. **08**

[✓ **(b)**] Explain preparation, identification and eradication phases of Incident handling. **08**

(c) Prepare an Incident handler checklist taking a case scenario. **08**

[✓ **(d)**] Discuss the phases of containment, eradication & recovery in context to Incident Response Management. **08**

1

Q.4 **Answer the following (Attempt Any Two)**

(a) Explain Digital Forensics and its branches. Also state the importance of Locard's Principle of Exchange in Digital Forensics. **07**

(b) What is Chain of Custody and explain its necessity in Digital Forensics? Also state how is integrity maintained in Digital Forensics. **07**

(c) Answer the following : **07**
   i) Write Blockers
   ii) Imaging v/s Cloning

Q.5 **Answer the following (Attempt Any Two)**

(a) Explain NTFS & FAT32 File Systems. **07**

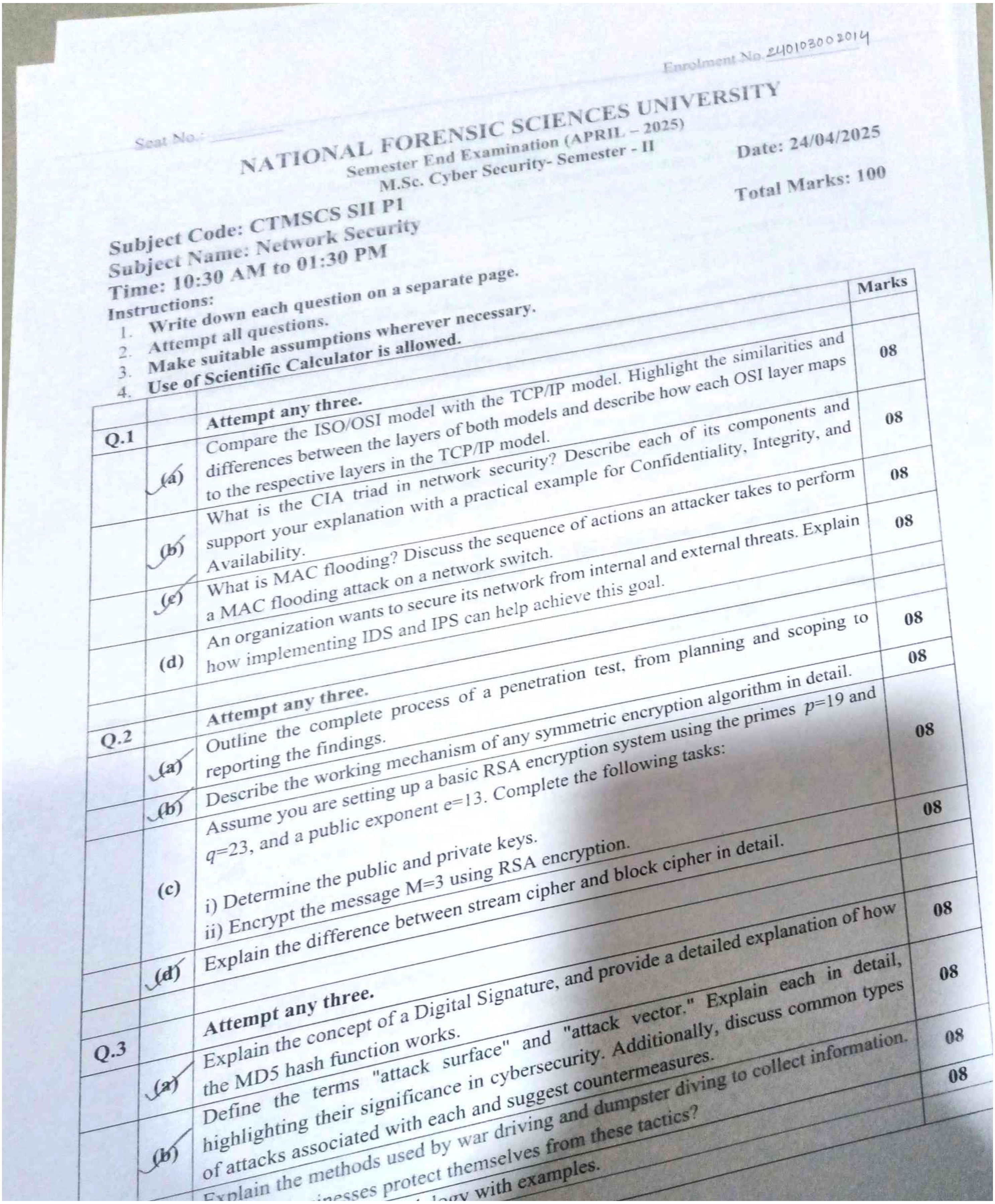
(b) What are Registry Artefacts and how are they important in establishing a case in Digital Forensics? Explain with examples and artefacts. **07**

(c) Consider the following Sysmon Event Log Entry and answer the asked question: **07**

```
{
 "Event": {
  "Timestamp": "2023-05-20T13:45:55.000Z",
  "EventID": 1,
  "Provider": "Microsoft-Windows-Sysmon",
  "Channel": "Microsoft-Windows-Sysmon/Operational",
  "Computer": "SERVER-EXAMPLE",
  "EventData": {
   "Image": "C:\\Windows\\System32\\rundll32.exe",
   "ParentImage": "C:\\Windows\\System32\\svchost.exe",
   "ParentCommandLine": "svchost.exe -k netsvcs",
   "TargetImage": "C:\\ProgramData\\Malicious\\malware.exe",
   "TargetCommandLine": "malware.exe -start -mode stealth",
   "GrantedAccess": "0x1410",
   "LogonId": "0x3e7",
   "UtcTime": "2023-05-20 13:45:54.500"
  }
 }
}
```

Explain the following event log parameters & their significance and also Identify the potential threat through the provided event log.

--- End of Paper---



Enrolment No. 240103002014

Seat No.: ________

NATIONAL FORENSIC SCIENCES UNIVERSITY

Semester End Examination (APRIL – 2025)

M.Sc. Cyber Security- Semester - II

Subject Code: CTMSCS SII P1 **Date: 24/04/2025**

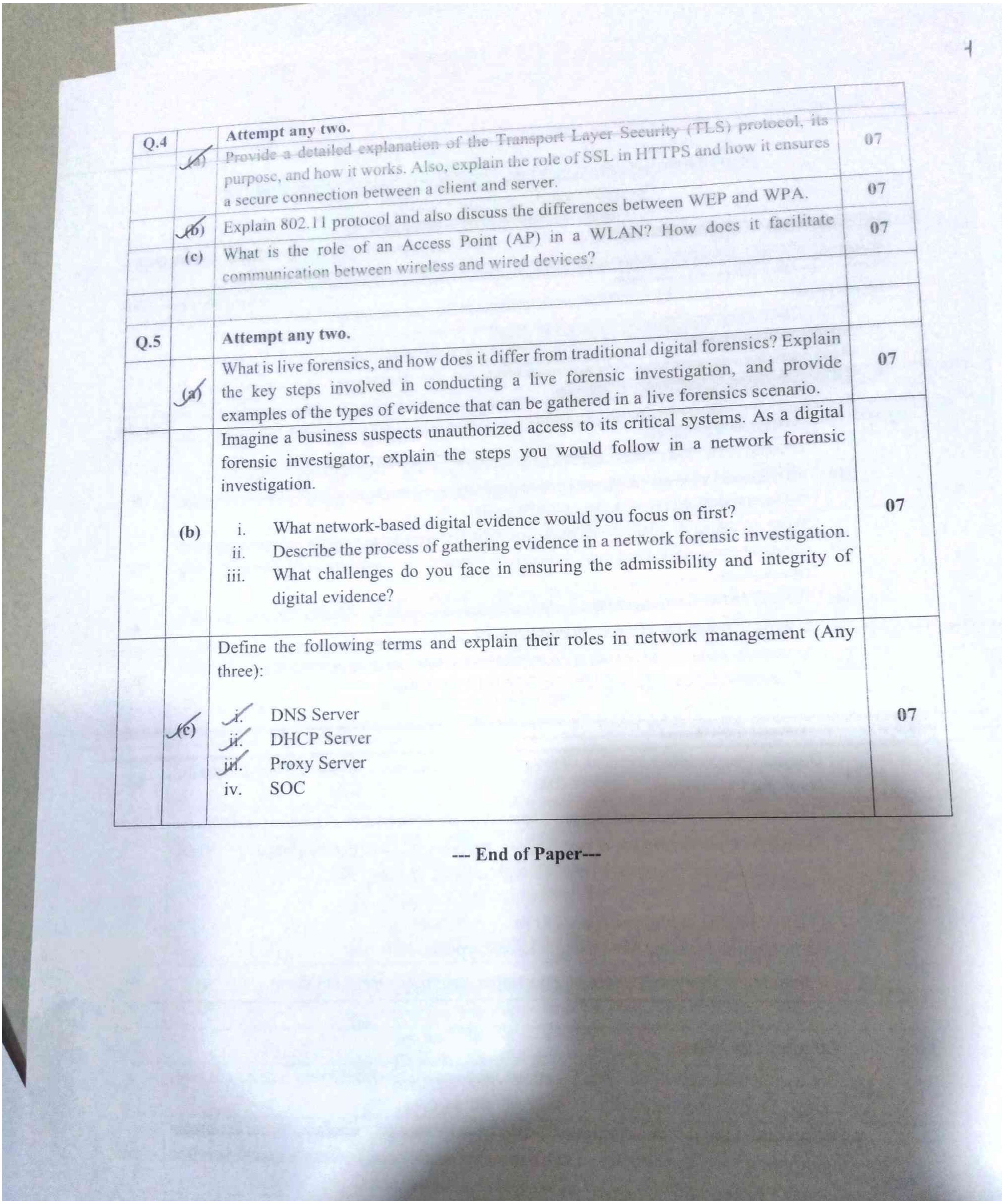
Subject Name: Network Security

Time: 10:30 AM to 01:30 PM **Total Marks: 100**

Instructions:

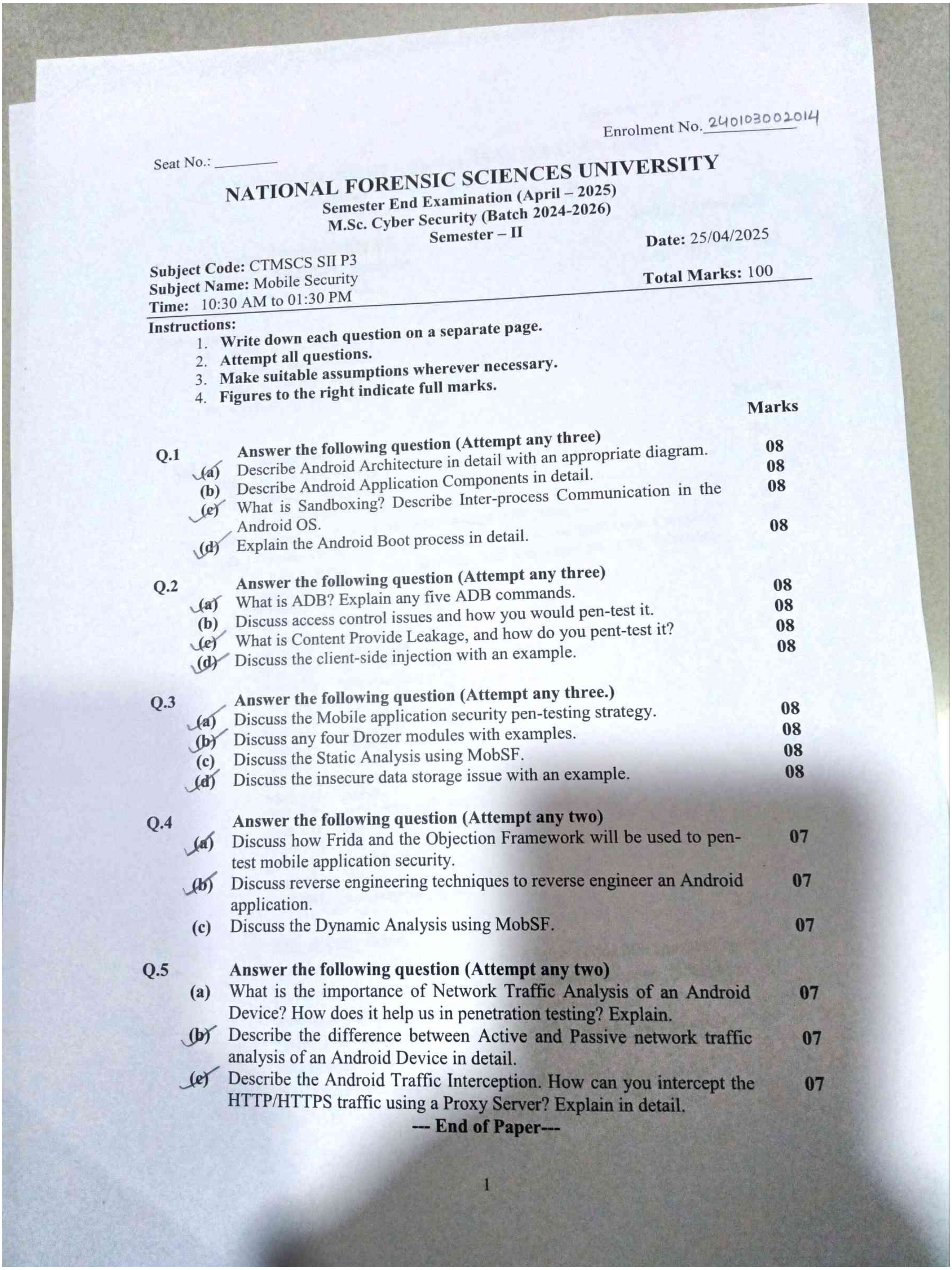
1. **Write down each question on a separate page.**
2. **Attempt all questions.**
3. **Make suitable assumptions wherever necessary.**
4. **Use of Scientific Calculator is allowed.**

			Marks
Q.1		**Attempt any three.**	
	(a)	Compare the ISO/OSI model with the TCP/IP model. Highlight the similarities and differences between the layers of both models and describe how each OSI layer maps to the respective layers in the TCP/IP model.	**08**
	(b)	What is the CIA triad in network security? Describe each of its components and support your explanation with a practical example for Confidentiality, Integrity, and Availability.	**08**
	(c)	What is MAC flooding? Discuss the sequence of actions an attacker takes to perform a MAC flooding attack on a network switch.	**08**
	(d)	An organization wants to secure its network from internal and external threats. Explain how implementing IDS and IPS can help achieve this goal.	**08**
Q.2		**Attempt any three.**	
	(a)	Outline the complete process of a penetration test, from planning and scoping to reporting the findings.	**08**
	(b)	Describe the working mechanism of any symmetric encryption algorithm in detail.	**08**
	(c)	Assume you are setting up a basic RSA encryption system using the primes p=19 and q=23, and a public exponent e=13. Complete the following tasks: i) Determine the public and private keys. ii) Encrypt the message M=3 using RSA encryption.	**08**
	(d)	Explain the difference between stream cipher and block cipher in detail.	**08**
Q.3		**Attempt any three.**	
	(a)	Explain the concept of a Digital Signature, and provide a detailed explanation of how the MD5 hash function works.	**08**
	(b)	Define the terms "attack surface" and "attack vector." Explain each in detail, highlighting their significance in cybersecurity. Additionally, discuss common types of attacks associated with each and suggest countermeasures.	**08**
		Explain the methods used by war driving and dumpster diving to collect information. inesses protect themselves from these tactics?	**08**
		logy with examples.	



Q.4		**Attempt any two.**	
	(a)	Provide a detailed explanation of the Transport Layer Security (TLS) protocol, its purpose, and how it works. Also, explain the role of SSL in HTTPS and how it ensures a secure connection between a client and server.	**07**
	(b)	Explain 802.11 protocol and also discuss the differences between WEP and WPA.	**07**
	(c)	What is the role of an Access Point (AP) in a WLAN? How does it facilitate communication between wireless and wired devices?	**07**
Q.5		**Attempt any two.**	
	(a)	What is live forensics, and how does it differ from traditional digital forensics? Explain the key steps involved in conducting a live forensic investigation, and provide examples of the types of evidence that can be gathered in a live forensics scenario.	**07**
	(b)	Imagine a business suspects unauthorized access to its critical systems. As a digital forensic investigator, explain the steps you would follow in a network forensic investigation. i. What network-based digital evidence would you focus on first? ii. Describe the process of gathering evidence in a network forensic investigation. iii. What challenges do you face in ensuring the admissibility and integrity of digital evidence?	**07**
	(c)	Define the following terms and explain their roles in network management (Any three): i. DNS Server ii. DHCP Server iii. Proxy Server iv. SOC	**07**

--- End of Paper---



Enrolment No. 240103002014

Seat No.: ________

NATIONAL FORENSIC SCIENCES UNIVERSITY

Semester End Examination (April – 2025)

M.Sc. Cyber Security (Batch 2024-2026)

Semester – II

Date: 25/04/2025

Subject Code: CTMSCS SII P3

Subject Name: Mobile Security

Time: 10:30 AM to 01:30 PM

Total Marks: 100

Instructions:

1. **Write down each question on a separate page.**
2. **Attempt all questions.**
3. **Make suitable assumptions wherever necessary.**
4. **Figures to the right indicate full marks.**

Marks

Q.1 Answer the following question (Attempt any three)

[✓ **(a)**] Describe Android Architecture in detail with an appropriate diagram. **08**

(b) Describe Android Application Components in detail. **08**

[✓ **(c)**] What is Sandboxing? Describe Inter-process Communication in the Android OS. **08**

[✓ **(d)**] Explain the Android Boot process in detail. **08**

Q.2 Answer the following question (Attempt any three)

[✓ **(a)**] What is ADB? Explain any five ADB commands. **08**

(b) Discuss access control issues and how you would pen-test it. **08**

[✓ **(c)**] What is Content Provide Leakage, and how do you pent-test it? **08**

[✓ **(d)**] Discuss the client-side injection with an example. **08**

Q.3 Answer the following question (Attempt any three.)

[✓ **(a)**] Discuss the Mobile application security pen-testing strategy. **08**

[✓ **(b)**] Discuss any four Drozer modules with examples. **08**

(c) Discuss the Static Analysis using MobSF. **08**

[✓ **(d)**] Discuss the insecure data storage issue with an example. **08**

Q.4 Answer the following question (Attempt any two)

[✓ **(a)**] Discuss how Frida and the Objection Framework will be used to pen-test mobile application security. **07**

[✓ **(b)**] Discuss reverse engineering techniques to reverse engineer an Android application. **07**

(c) Discuss the Dynamic Analysis using MobSF. **07**

Q.5 Answer the following question (Attempt any two)

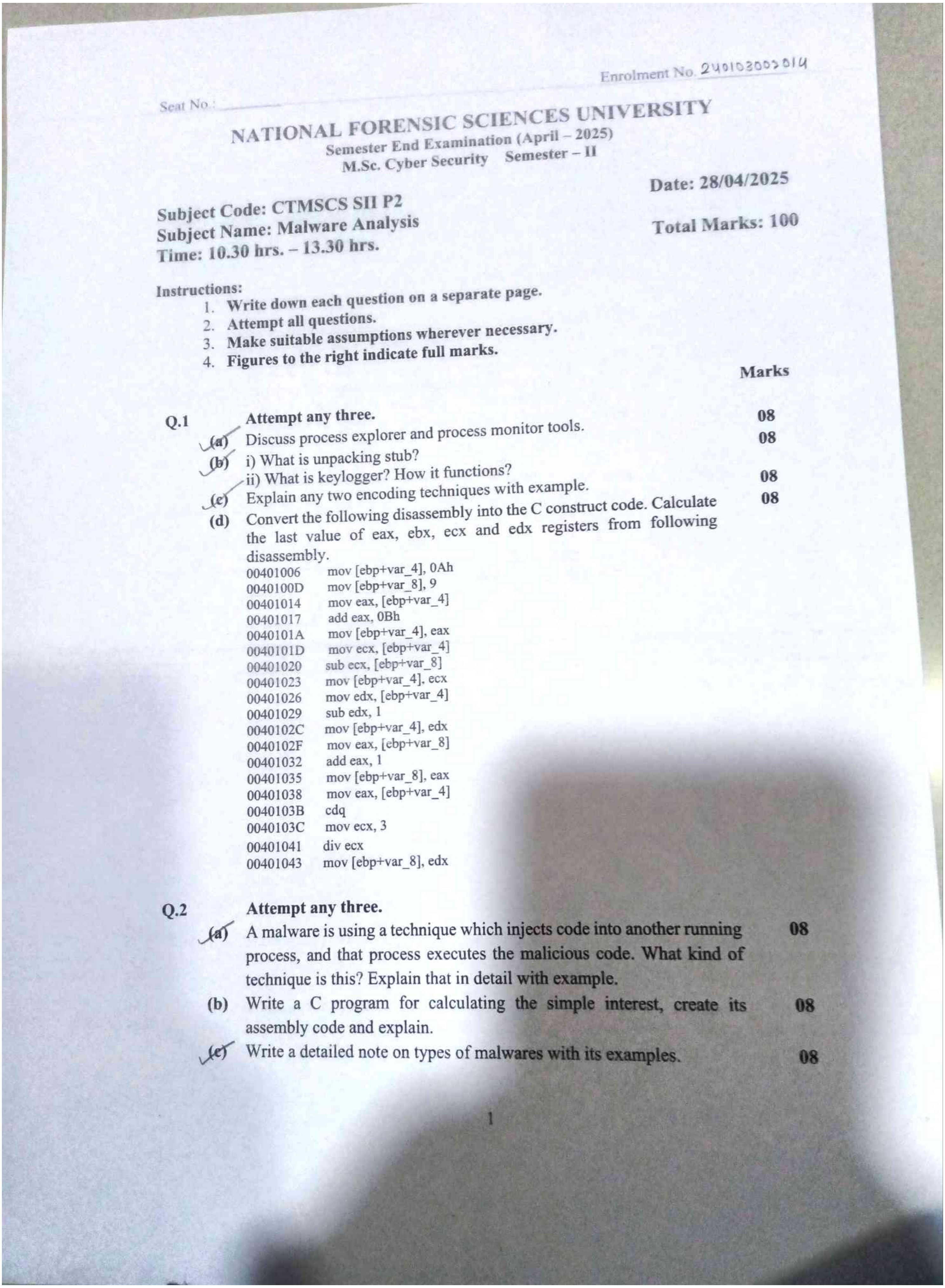
(a) What is the importance of Network Traffic Analysis of an Android Device? How does it help us in penetration testing? Explain. **07**

[✓ **(b)**] Describe the difference between Active and Passive network traffic analysis of an Android Device in detail. **07**

[✓ **(c)**] Describe the Android Traffic Interception. How can you intercept the HTTP/HTTPS traffic using a Proxy Server? Explain in detail. **07**

--- End of Paper---

1



Enrolment No. 240103003014

Seat No.: ________

NATIONAL FORENSIC SCIENCES UNIVERSITY

Semester End Examination (April – 2025)

M.Sc. Cyber Security   Semester – II

Date: 28/04/2025

Subject Code: CTMSCS SII P2

Subject Name: Malware Analysis

Total Marks: 100

Time: 10.30 hrs. – 13.30 hrs.

Instructions:

1. **Write down each question on a separate page.**
2. **Attempt all questions.**
3. **Make suitable assumptions wherever necessary.**
4. **Figures to the right indicate full marks.**

Marks

Q.1 **Attempt any three.**

(a) Discuss process explorer and process monitor tools. **08**

(b) i) What is unpacking stub? **08**
ii) What is keylogger? How it functions?

(c) Explain any two encoding techniques with example. **08**

(d) Convert the following disassembly into the C construct code. Calculate the last value of eax, ebx, ecx and edx registers from following disassembly. **08**

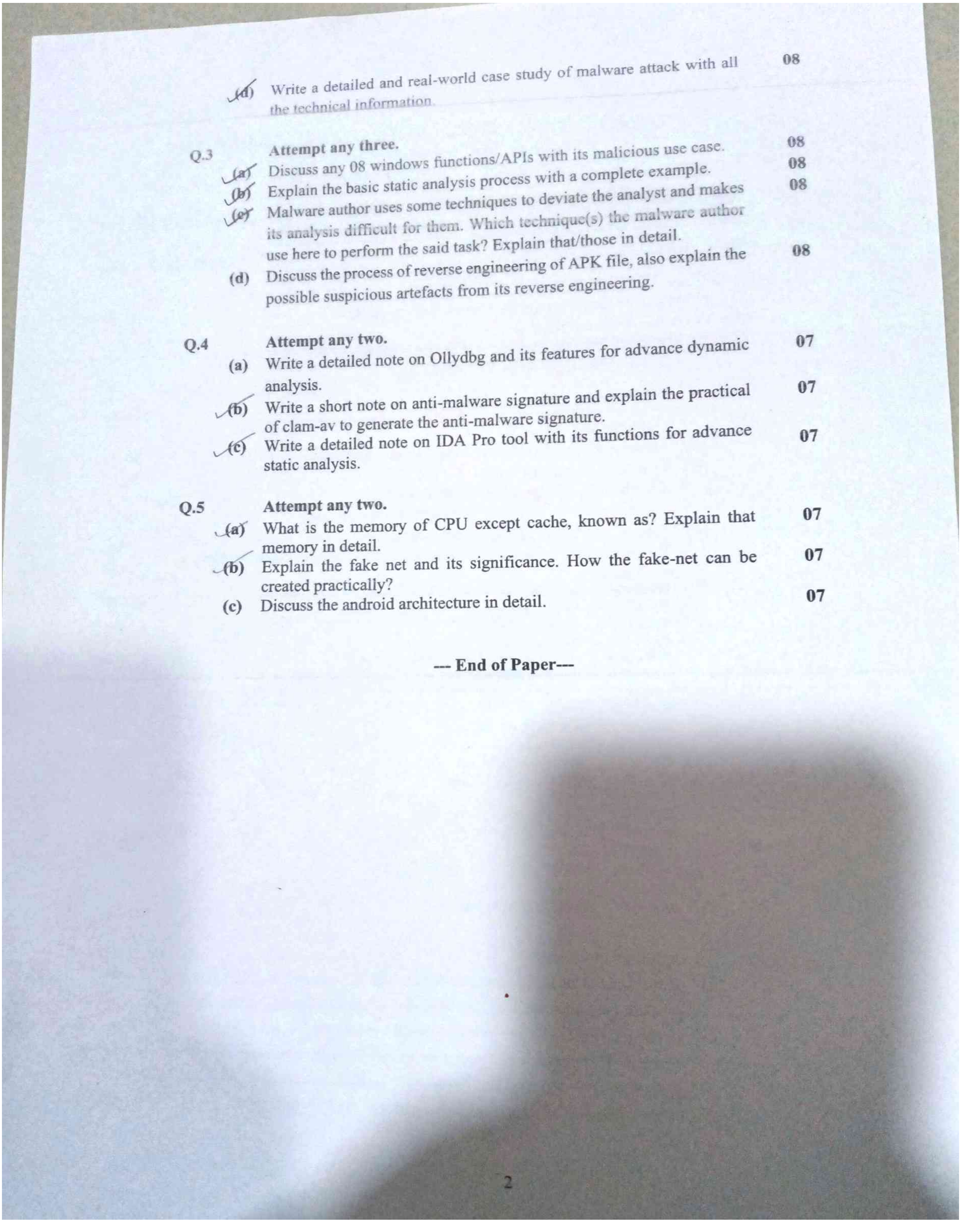
```
00401006    mov [ebp+var_4], 0Ah
0040100D    mov [ebp+var_8], 9
00401014    mov eax, [ebp+var_4]
00401017    add eax, 0Bh
0040101A    mov [ebp+var_4], eax
0040101D    mov ecx, [ebp+var_4]
00401020    sub ecx, [ebp+var_8]
00401023    mov [ebp+var_4], ecx
00401026    mov edx, [ebp+var_4]
00401029    sub edx, 1
0040102C    mov [ebp+var_4], edx
0040102F    mov eax, [ebp+var_8]
00401032    add eax, 1
00401035    mov [ebp+var_8], eax
00401038    mov eax, [ebp+var_4]
0040103B    cdq
0040103C    mov ecx, 3
00401041    div ecx
00401043    mov [ebp+var_8], edx
```

Q.2 **Attempt any three.**

(a) A malware is using a technique which injects code into another running process, and that process executes the malicious code. What kind of technique is this? Explain that in detail with example. **08**

(b) Write a C program for calculating the simple interest, create its assembly code and explain. **08**

(c) Write a detailed note on types of malwares with its examples. **08**



[✓ (d)] Write a detailed and real-world case study of malware attack with all the technical information. **08**

Q.3 **Attempt any three.**

[✓ (a)] Discuss any 08 windows functions/APIs with its malicious use case. **08**

[✓ (b)] Explain the basic static analysis process with a complete example. **08**

[✓ (c)] Malware author uses some techniques to deviate the analyst and makes its analysis difficult for them. Which technique(s) the malware author use here to perform the said task? Explain that/those in detail. **08**

(d) Discuss the process of reverse engineering of APK file, also explain the possible suspicious artefacts from its reverse engineering. **08**

Q.4 **Attempt any two.**

(a) Write a detailed note on Ollydbg and its features for advance dynamic analysis. **07**

[✓ (b)] Write a short note on anti-malware signature and explain the practical of clam-av to generate the anti-malware signature. **07**

[✓ (c)] Write a detailed note on IDA Pro tool with its functions for advance static analysis. **07**

Q.5 **Attempt any two.**

[✓ (a)] What is the memory of CPU except cache, known as? Explain that memory in detail. **07**

[✓ (b)] Explain the fake net and its significance. How the fake-net can be created practically? **07**

(c) Discuss the android architecture in detail. **07**

--- End of Paper---