ourdiu.com | Shared by MD. ABU NAYEM

Daffodil International University

Faculty of Science & Information Technology

Department of Software Engineering

Midterm Examination, Fall 2026

Course Code: CS422; Course Title: Digital Forensics

Sections & Teachers: A (AH), B &C (THZ)

Time: 1 Hour 30 Mins | Marks: 25

Answer ALL Questions

[The figures in the right margin indicate the full marks and corresponding course outcomes. All portions of each question must be answered sequentially.]

1. During an investigation into suspected data theft, a Windows computer and the suspect's personal USB drive (formatted FAT32) are seized. The USB drive appears empty, although investigators believe it previously held documents relevant to the case. The suspect may have deleted the files or used anti-forensic techniques on Windows to hide or destroy evidence. As the investigator, you must preserve the seized media, examine the USB file system and recover deleted files where possible.

a)	Define the following terms: Write Blocker, Hashing, File Carving, Metadata.	[Marks-2]	CLO1-*Level-1*
b)	Explain what happens to a FAT32 directory entry and its data clusters when a file is deleted, and why recovery of the file is often possible.	[Marks-2]	CLO1-*Level-2*
c)	Identify anti-forensic techniques the suspect is likely to have used in this case and explain how an investigator can defeat each of them on Windows.	[Marks-4]	CLO1-*Level-3*

2. The DIU Photography Club website runs on a Linux web server in the university's DMZ. One morning, students find the homepage replaced with an offensive message. The server's access log contains the following entries:

Time (UTC)	Request	Status
02:10:05	GET /robots.txt	200
02:10:12–10:40	Requests to /admin/, /backup/, /.git/ and other paths (40 requests)	404
02:11:02	GET /event?id=7'	500
02:11:05	GET /event?id=7 UNION SELECT username,password FROM users	200 (unusually large)
02:13:30	POST /admin/login (club admin account)	200
02:14:10	POST /admin/homepage/edit	200

Further investigation shows that the compromised server made an unusual outbound connection to an unknown external IP address, and firewall logs show connection attempts from it to another internal university computer. The IT volunteer proposes restoring the homepage from backup and rebooting the server immediately.

a)	From the log entries, name the web attack used to steal the credentials.	[Marks-1]	CLO2-*Level-1*
b)	As the forensic investigator, choose a suitable data acquisition method for this Linux server and state how you will maintain the chain of custody for the collected evidence.	[Marks-2]	CLO2-*Level-2*

ourdiu.com | Shared by MD. ABU NAYEM

Daffodil International University

Faculty of Science & Information Technology

Department of Software Engineering

Midterm Examination, Fall 2026

Course Code: CS422; Course Title: Digital Forensics

Sections & Teachers: A (AH), B &C (THZ)

Time: 1 Hour 30 Mins **Marks: 25**

Answer ALL Questions

[The figures in the right margin indicate the full marks and corresponding course outcomes. All portions of each question must be answered sequentially.]

1. During an investigation into suspected data theft, a Windows computer and the suspect's personal USB drive (formatted FAT32) are seized. The USB drive appears empty, although investigators believe it previously held documents relevant to the case. The suspect may have deleted the files or used anti-forensic techniques on Windows to hide or destroy evidence. As the investigator, you must preserve the seized media, examine the USB file system and recover deleted files where possible.

a)	Define the following terms: Write Blocker, Hashing, File Carving, Metadata.	**[Marks-2]**	**CLO1-** *Level-1*
b)	Explain what happens to a FAT32 directory entry and its data clusters when a file is deleted, and why recovery of the file is often possible.	**[Marks-2]**	**CLO1-** *Level-2*
c)	Identify anti-forensic techniques the suspect is likely to have used in this case and explain how an investigator can defeat each of them on Windows.	**[Marks-4]**	**CLO1-** *Level-3*

2. The DIU Photography Club website runs on a Linux web server in the university's DMZ. One morning, students find the homepage replaced with an offensive message. The server's access log contains the following entries:

Time (UTC)	Request	Status
02:10:05	GET /robots.txt	200
02:10:12–10:40	Requests to /admin/, /backup/, /.git/ and other paths (40 requests)	404
02:11:02	GET /event?id=7'	500
02:11:05	GET /event?id=7 UNION SELECT username,password FROM users	200 (unusually large)
02:13:30	POST /admin/login (club admin account)	200
02:14:10	POST /admin/homepage/edit	200

Further investigation shows that the compromised server made an unusual outbound connection to an unknown external IP address, and firewall logs show connection attempts from it to another internal university computer. The IT volunteer proposes restoring the homepage from backup and rebooting the server immediately.

a)	From the log entries, name the web attack used to steal the credentials.	**[Marks-1]**	**CLO2-** *Level-1*
b)	As the forensic investigator, choose a suitable data acquisition method for this Linux server and state how you will maintain the chain of custody for the collected evidence.	**[Marks-2]**	**CLO2-** *Level-2*

ourdiu.com | Shared by MD. ABU NAYEM

	c)	Explain your web incident investigation workflow (triage, preserve, scope, timeline, hunt, and report) by briefly explaining what you would do at each step in this case. Explain in one line why the server should not be rebooted immediately.	[Marks-5]	CLO2-*Level-4*

3. DIU Finance Department uses a cloud-hosted payment system connected to a MySQL database. A finance officer reports that payment records were altered after an email from a known supplier requested a change to its bank account details. The email looks legitimate, but the Reply-To address differs slightly from the supplier's address. The cloud provider's audit logs also show unusual activity around the same time.

Email Sample

```
From:          accounts@supplier.com
Reply-To:      accounts@supp1ier-payments.com
Return-Path:   bounce@supp1ier-payments.com
Received:      from mail.supp1ier-payments.com (203.0.113.25)
               with ESMTPS; 21 Oct 2026 09:42:10 +0600
Authentication-Results: spf=pass; dkim=pass; dmarc=pass
Subject:       Urgent: Updated Bank Account for Payment

Dear Finance Team,
Please update our bank account details before processing the
pending payment. Kindly reply to this email for confirmation.
Regards, Supplier Accounts Team
```

a)	Point out one suspicious indicator in the email sample.	[Marks-1]	CLO2-*Level-1*
b)	Name two sources of database evidence that should be collected to investigate the altered payment records.	[Marks-2]	CLO2-*Level-2*
c)	State three actions an investigator should take to preserve evidence from the cloud payment system.	[Marks-3]	CLO2-*Level-3*
d)	Analyze why the email may still be fraudulent even though SPF, DKIM and DMARC pass, and briefly show how the email headers together with database and cloud logs can rebuild the sequence of events.	[Marks-3]	CLO3-*Level-4*

ourdiu.com