Assignment No. 1: Write a program for Tracking Emails & Investigating Email Crimes. Write a program to analyze e–mail header

Name:	**Class:** B.E.	**Division:** A / B/C
Roll No:	**Date of Submission:**	
Marks Obtained: / 10	**Signature of subject teacher:**	

Title: Write a program for Tracking Emails & Investigating Email Crimes. i.e. Write a program to analyze e–mail header

Objectives:

1. To understand issues in cyber-crime and different attacks

Outcomes:

Analyze threats in order to protect or defend it in cyberspace from cyber-attacks.

Tools Required:

Software: MxToolbox

Theory: An email header analysis is the process of retrieving an email's sender, recipient, subject line and a few other pieces of information from the headers in an email. Cyber forensics analysts are often required to analyze emails for evidence. If this is the case for you, then you need to know how to employ email header analysis. From my experience as a cyber-forensics analyst, I have found that email headers can be crucial in analyzing emails and pulling relevant evidence from them.

An email header identifies who sent the message and where it was received. Some markers, such as "From:" — the sender's name and email address, "To:" — the recipient's name and email address, and "Date:" — the time and date the email was sent, show this information. These are all required indicators.

When a cyber-attack occurs, the email headers will be infected with malware or be marked as spam. In order to investigate the attack, you should run a header analysis on the emails that were sent during the time of the attack.

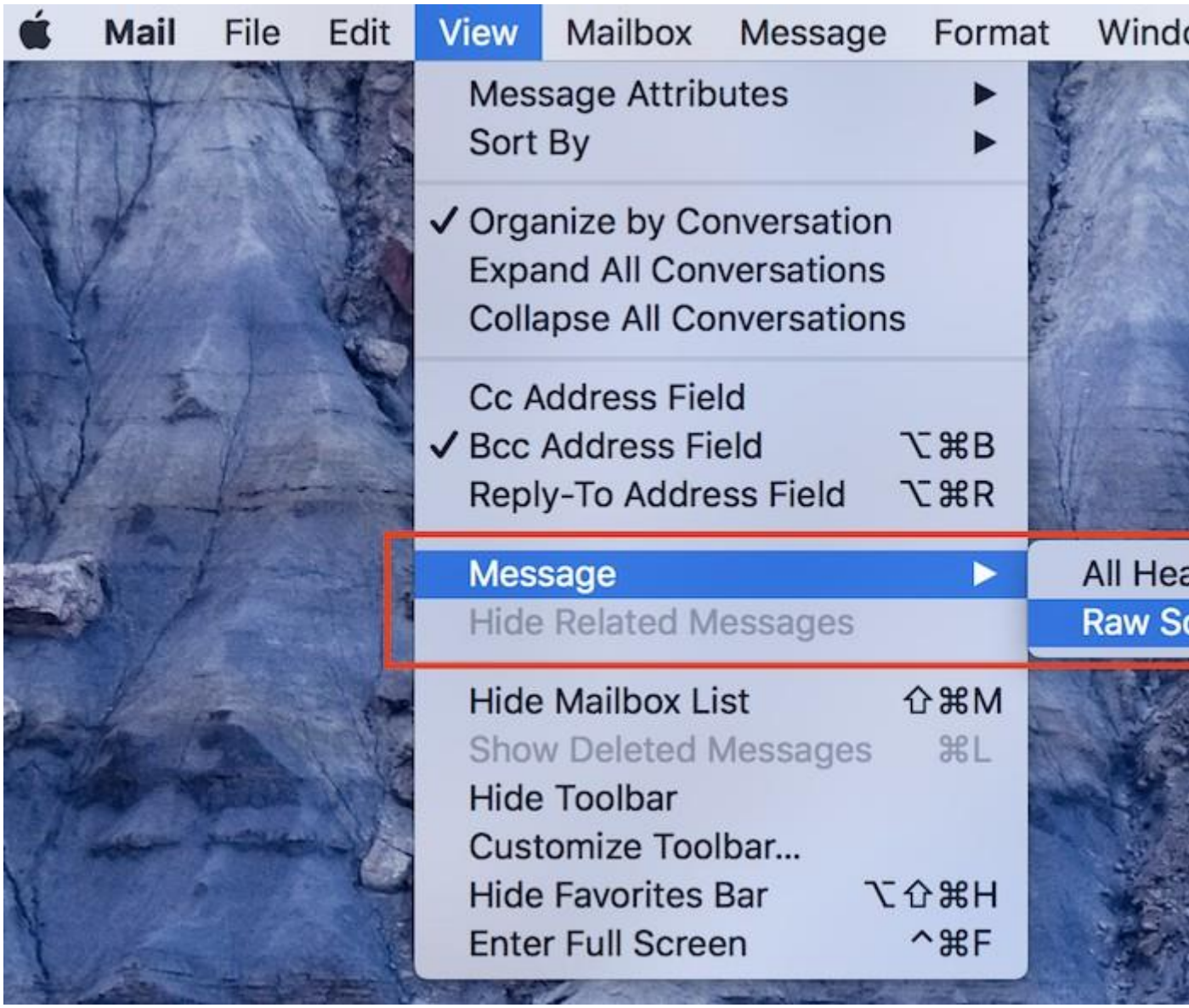
An email is divided into three parts: header, body, and attachment. The header part keeps the routing information of the email. It may contain other information like content type, from, to,

delivery date, sender origin, mail server, and the actual email address used to send/receive the email.

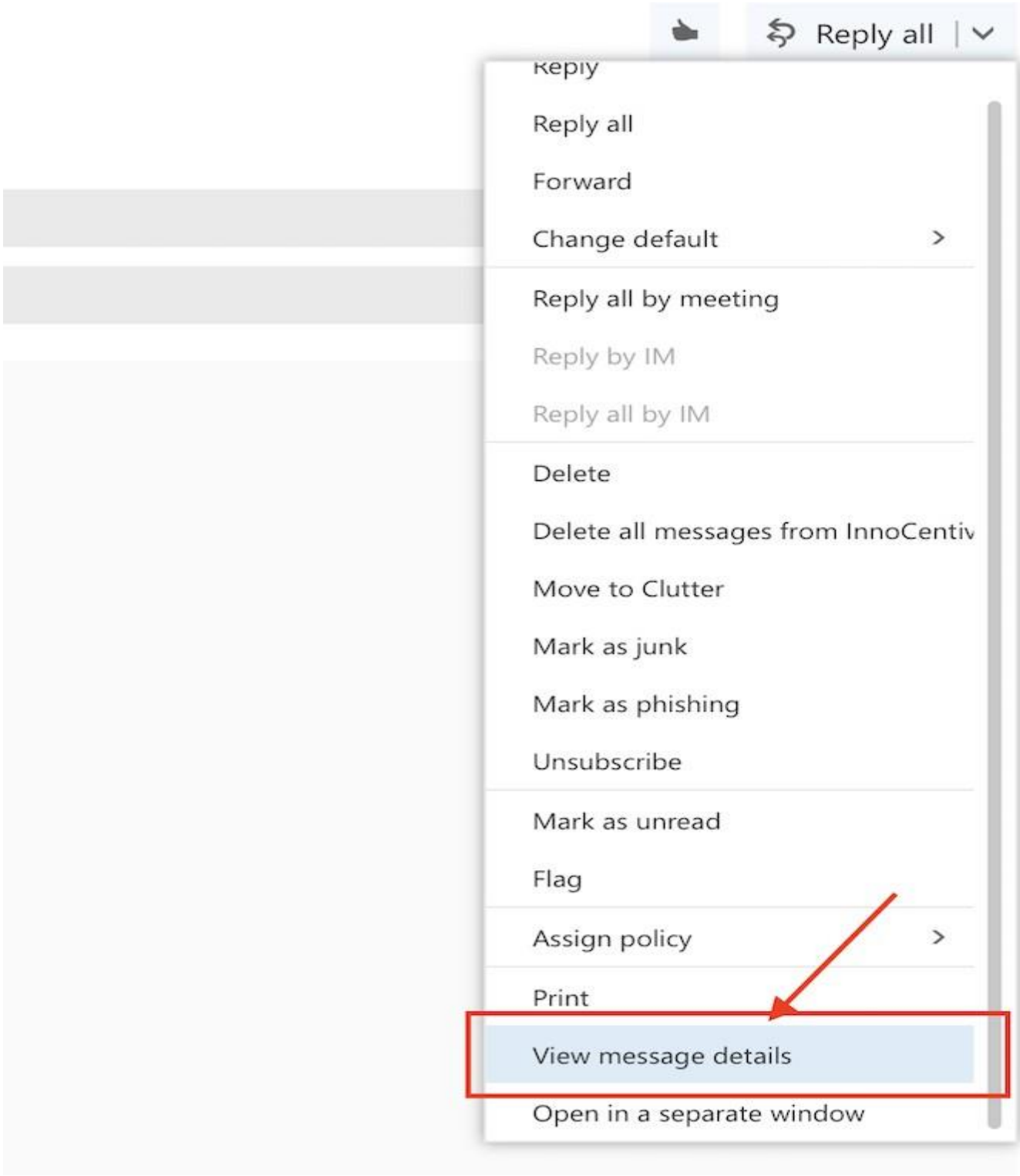
[1] Email Headers

Email Headers hold a lot of information. Much of this information is never displayed to the user. The email reader only sees a select few pieces of information like the subject, date, and the sender's email and info. The surprising part is that the information that is actually displayed to a user can be easily forged

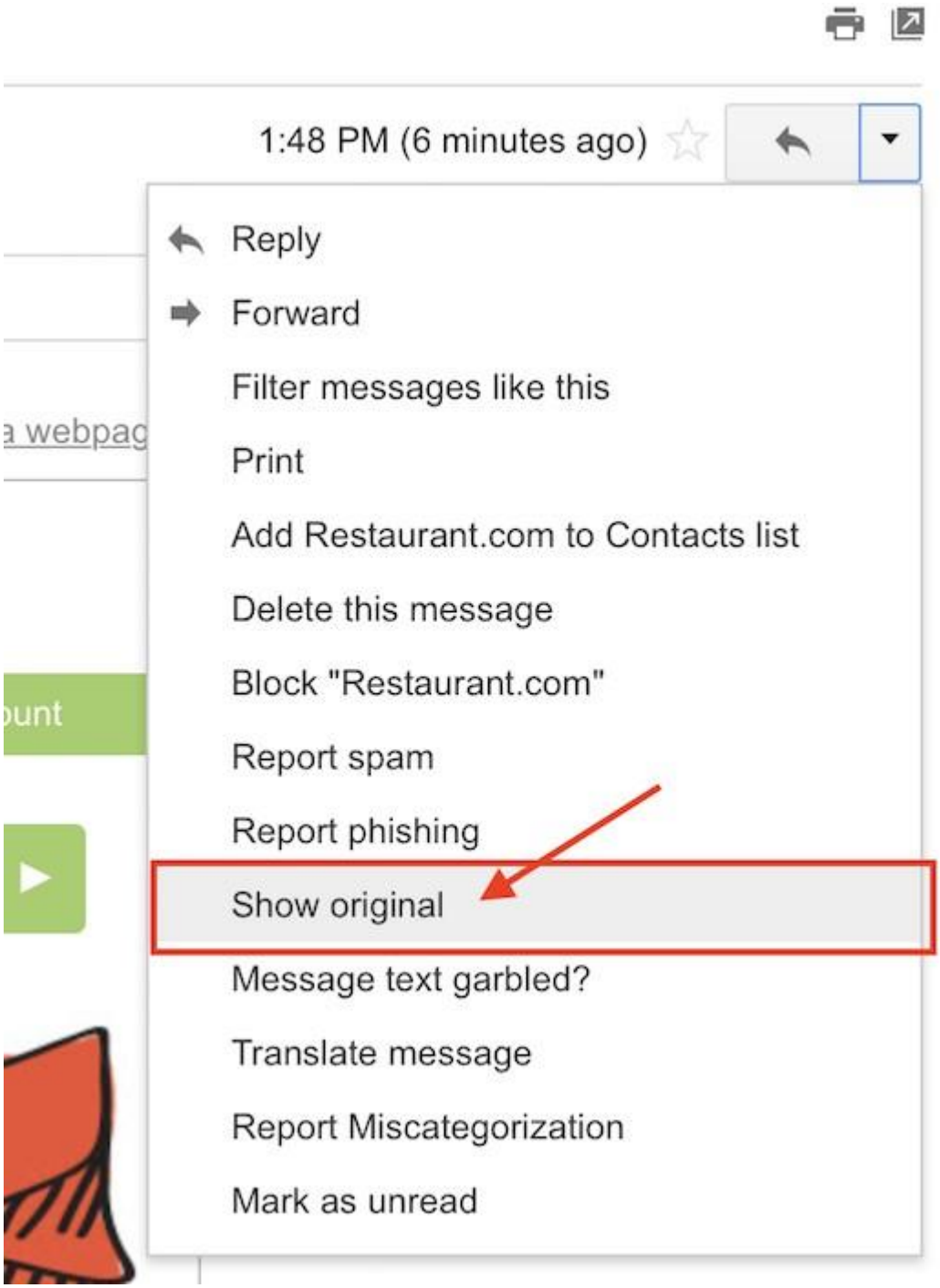
Apple Mail



[2] Outlook Web Client


Reply all
Reply
Reply all
Forward
Change default
Reply all by meeting
Reply by IM
Reply all by IM
Delete
Delete all messages from InnoCentiv
Move to Clutter
Mark as junk
Mark as phishing
Unsubscribe
Mark as unread
Flag
Assign policy
Print
View message details
Open in a separate window

[3] Gmail



STEPS TO ANALYZE EMAIL HEADER

-
-
-
-
-
-

Conclusion:

LAB EXERCISE :

1. What is the SPF Alignment & SPF Authenticated.

2. Explain DKIM Alignment