

# Intro to Cyber Forensics Lab Grading Sheet

Project: Lab 5 # E- Mail Forensics  
Member Name: Yadlapalli Lakshmidhar  
Member Name: Pottolla Vinusha Goud  
Member Name: Boinapally Akshith Rao  
Member Name: Amani Ponnamm  
Member Name: Oluwatoyosi Kehinde

## Executive Summary \_\_\_\_\_ / 4 points

+ ✓ -

- ☐ ☐ ☐ Executive summary is brief and focused to the point of the project
- ☐ ☐ ☐ The summary clearly illustrates the objectives of the laboratory exercise

## Apparatus \_\_\_\_\_ / 4 points

- ☐ ☐ ☐ The apparatus are clearly illustrated and documented

## Procedures \_\_\_\_\_ / 12 points

- ☐ ☐ ☐ Adequate information provided to allow re-creation of work
- ☐ ☐ ☐ Consistent level of coverage throughout the project – nothing overly detailed or omitted

## Problem Solving \_\_\_\_\_ / 5 points

- ☐ ☐ ☐ All problems identified
- ☐ ☐ ☐ Alternative solutions identified
- ☐ ☐ ☐ Solutions attempted listed
- ☐ ☐ ☐ Final solution detailed (what fixed the problem and why?)

## Conclusions & Recommendations \_\_\_\_\_ / 5 points

- ☐ ☐ ☐ Tie back to the learning objectives identified in the executive summary - critical
- ☐ ☐ ☐ Conclusions stated in a logical fashion
- ☐ ☐ ☐ Conclusions are viable based on the procedures and results
- ☐ ☐ ☐ Recommendations practical & relevant

## Format & Grammar \_\_\_\_\_ / 5 points

- ☐ ☐ ☐ Table of Contents present
- ☐ ☐ ☐ Report written in past tense
- ☐ ☐ ☐ Proper voice (no I's, We's, Our's or The group)
- ☐ ☐ ☐ Paper easy to read (fonts, spacing, etc.)
- ☐ ☐ ☐ Proper credit given to sources in bibliography (APA style)
- ☐ ☐ ☐ Paper is cohesive and consistent in tone

\_\_\_\_\_ Spelling & grammar errors: *minus one half point for each, up to a max deduction of 5 points – at that time, paper is returned for correction and re-submission with a one letter grade penalty.*

**Final Score:** \_\_\_\_\_ / 35

## Table Of Contents

Intro to Cyber Forensics Lab Grading Sheet -----	1
1. Executive Summary -----	3
2. Apparatus -----	4
3. Laboratory Procedures -----	5
3.1 Timeline/Log -----	5
3.2 Procedure -----	5
3.2 Figures-----	8
4. Problem-Solving and Troubleshooting -----	14
5. Conclusion and Recommendations -----	15
6. References -----	16
7. Appendix A: Forms -----	17
E-mail 1 Content:-----	17
E-mail 1 Header:-----	18
E-mail 2 Content-----	19
Message 2 Source:-----	19
E-mail 3 Content-----	21
Message 3 Source:-----	22
SPAM Email content -----	27

## 1. Executive Summary

This report provides investigation data for four emails which include three emails provided to the team and one from spam box of personal email. The investigators used technologies like Mx tool box and IP void and performed both manual and automated email header examination. These tools were used for analysing e-mail headers to source where e-mails originate and look for signs of spoofing, such as mismatched sender information, domain naming deceit, or anomalies among IP addresses. The main goal was to comprehend the investigative procedures for email analysis and to showcase the observed results in detail and to identify common phishing strategies used by attackers to scam and spoof. The investigators collected information like sender details, associated IP address, email authentication mechanisms (SPF, DKIM, DMARC) and other metadata in order to determine the legitimacy of each e-mail. They had searched for typical traits in the emails that could show cybercriminal activity-like, forging the sender address, phishing links, and suspicious IP addresses.

## 2. Apparatus

**Table1: List of hardware and software used in the lab**

Items	Model Number/Version	USAGE
Mx Toolbox	<a href="https://mxtoolbox.com/">https://mxtoolbox.com/</a>	Online site to inspect emails
Ip void	<a href="https://www.ipvoid.com/">https://www.ipvoid.com/</a>	Online site to inspect Ip address

### 3. Laboratory Procedures

#### 3.1 Timeline/Log

**Table2: Timeline of steps taken during the investigation.**

DATE	TIME	ACTION TAKEN / INVESTIGATIVE LEAD
11-20-2024	06:00 PM	Acquired emails
11-20-2024	06:05 PM	Analyzed Email 1 Content and Headers
11-20-2024	06:20 PM	Analyzed Email 2 Content and Headers
11-20-2024	06:40 PM	Analyzed Email 3 Content and Headers
11-20-2024	07:10 PM	Analyzed Personal Email Content and Headers

#### 3.2 Procedure

##### 3.2.1 Email 1 Content and Headers Analysis

After investigating the content of email 1, team 3 concluded that the given email which was claimed to be from Barrister Evans Thomas appears to be a classic 419 scam. The email has been detected as fraudulent because it contains scam email indicators. Firstly, the language was unprofessional and contain lot of errors. Also, the message used a generic salutation "Dear Friend" rather than by name which indicate that it was sent to numerous of recipients. The story of a deceased individual's \$15 million inheritance and the sender's requested for personal information be forwarded to him for the monetary transaction to be completed indicate typical tactic of fraud. Additionally, the email had an urgent tone as well as promise of a large commission along with an offer to protect the recipient from law which all indicated that the email belongs to spam category.

While examining the header of the email using Mx toolbox and the Ip address associated with the email using ipvoid team found out several suspicious details. Figure 1 ,2 and 3 shows the details of email header and IP address. The email was send to baggili@gmail.com on Sunday, November 3rd, 2013 at 18:40:31. The sender was "barr\_evansthomas@yahoo.co.jp" and the IP address was 111.91.237.247 from asiaclassified.com. The SPF soft fail was an

indication that the email was from unauthorized IP 111.91.237.247, which does not match

the yahoo.co.jp domain. This therefore was a spoofed email. It also passed through asiaclassified.com-a suspicious domain-and includes a 127.0.0.1 loopback IP, which is not normal for a legitimate email to do. Moreover, the Return-Path and Reply-To addresses are inconsistent with any professional law firm, these use a yahoo address instead of a corporate domain. The outdated X-Mailer header and unusual Windows-1251 content encoding are typical of spam or phishing emails. DKIM and DMARC are not validated either, hence making it even more suspicious that this was some scam/phishing email. In addition to this, there is further data regarding another email, dispatched by the same sender, "barrevansthomas@yahoo.co.jp", on July 17, 2013, at 03:27:31. This email carried the subject line "WITH DUE RESPECT." In this instance, asiaclassified.com recorded the sender's IP Address as 203.152.117.111. Our search of the IP address on IP void indicated that it is associated with Compass Communications as the Internet Service Provider.

### **Email 2 Content and Headers Analysis**

Group 3 conducted the analysis of the email header both through automated tools and manual examination. First, in the manual examination, Group 3 checked the "From" address and domain to verify the email was from an official University of New Haven address: webmarketing1@newhaven.edu. This is consistent with the sender identified, C.J. Losapio, a Web Student Employee in the Marketing and Enrollment Communications department. The subject of the e-mail was professional and not different from a lot of the e-mails communicated within the university. He wanted to collaborate in a joint effort to develop pages for the Cyber Forensics research lab. In this regard, the "Reply-To" and "From" fields had no peculiarities, while all its' time stamps were normal. Generally speaking, it was a valid email and thus not considered as phishing or fraud.

Using MX Toolbox, which is an email header analysis tool, Group 3's investigation looked into some key areas of the header-in particular, the "Received" fields and the "X-OriginatingIP.". These are the indication of where, in fact, this email really came from. The header showed this was from a server at the University of New Haven, IP address 24.2.209.212 forwarded to Internal Exchange servers named EXCHANGE-02 and EXCHANGE-03, that part of the infrastructure within the university. This probably passed the SPF check, since the originating server matched the university's domain. No spoofing or suspicious routing was found further helping to validate the email. Figure 4 shows the email2 analysis details.

### **3.2.3 Email 3 Content and Headers Analysis**

The email seems to be a valid message sent by Matt Topor, graduate research student at the University of New Haven, about suspicious behavior during a midterm exam. The email demonstrated a level of professionalism by correctly addressing the recipient with their title and name. The content of the letter discusses noticing a pattern in that at least two of his students had similar answers, which was considered cheating. In the tone one can hear a formal and professional request for further instructions on how to proceed. Nothing in this email seems to show malicious intent, there was no alarming language or unsolicited requests. The email contains links to external websites, which may cause concerns about phishing or misleading content, but they appeared to be related to affiliations of the sender. Additionally, the email's signature was thorough, including the sender's name, some pertinent information, and an email address that matches the school's email domain.

Several important facts were revealed from the email header analysis. The "Received" fields indicate that the message was sent from the IP address 64.251.61.74, which resolves to a valid address in the University of New Haven's network and this address was from Connecticut, west haven. The domain "unh.newhaven.edu" matches the sender's email, reinforcing the fact that the email most likely come from within the university's infrastructure. There were no indicators of spoofed authentication methods, such as DKIM or DMARC failures, though DKIM showed as "none," which is unusual. The "X-MS-Exchange-Organization-AuthSource" and "X-Originating-IP" headers confirmed internal routing through the Outlook services, but there was no indication that the message had been flagged as spam or malicious. However, there was a lack of DKIM signing, which does pose a potential vulnerability to spoofing, and the presence of external links warrants caution. Figures 5,6 and 7 depicts the details of header analysis and the details of the associated IP address.

### **3.2.4 Spam email Content and Headers Analysis**

Group 3 had obtained a spam email from one of the group members' e-mail accounts. (Please find details of content and header information in Appendix A section).

The mail is suspicious because it was unsolicited, the job is supposedly enticing with compensation of \$400 per week. Even though the email has an official domain, bcom202445914@mylife.mku.ac.ke, this type of domain name can be found in many phishing or spamming attempts. Also, the message used a generic salutation "Hi there" rather than by name which is an informal and generic greeting. Moreover, the email does not specify the details of the job, like the name of the company or its physical location, which is usually done by scammers in order to avoid being caught. The tone of receiving easy money raises



suspicion that such an email might lead one to give out confidential information or be asked to click on links that could be disastrous. The header analysis indicates that the message was redirected from the address bcom202445914@mylife.mku.ac.ke, a student email address derived from Mount Kenya University. The authentication checks that the email passed included SPF, DKIM, and DMARC-all of which identified the sender's domain as legitimate. It was routed through several Microsoft Exchange servers before reaching the recipient. This was junked by the recipient's email system because it was an external email, hence, it may have been flagged as spam. Technically, the message origin was validated, but it was nonetheless recognized as coming from an untrusted source, thus, it was spam-classified. Figures 8 and 9 depicts more details of the header analysis.

## 3.2 Figures

### SPF and DKIM Information

#### Headers Found

Header Name	Header Value
Delivered-To	baggili@gmail.com Received: by 10.58.118.162 with SMTP id kn2csp90327vrb; Sun, 3 Nov 2013 18:40:31 -0800 (PST) X-Received: by 10.68.101.225 with SMTP id fj1mr15554200pb.8.1383532830983;
X-Priority	3 X-MSMail-Priority: Normal X-Mailer: Microsoft Outlook Express 6.00.2600.0000 X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000 Message-Id:

#### Received Header

```
Delivered-To: baggili@gmail.com Received: by 10.58.118.162 with SMTP id kn2csp90327vrb; Sun, 3 Nov 2013 18:40:31 -0800 (PST) X-Received: by 10.68.101.225 with SMTP id fj1mr15554200pb.8.1383532830983;
Sun, 03 Nov 2013 18:40:30 -0800 (PST) Return-Path:
<barr_evanstomas@yahoo.co.jp> Received: from asiaclassified.com (asiaclassified.com. [111.91.237.247]) by mx.google.com with ESMTSPS id ar5si9269155pbd.182.2013.11.6
Sun, 03 Nov 2013 18:40:30 -0800 (PST) Received-SPF: softfail (google.com: domain of transitioning barr_evanstomas@yahoo.co.jp does not designate 111.91.237.247 as p
client-ip=111.91.237.247; Authentication-Results: mx.google.com; spf=softfail (google.com: domain of transitioning barr_evanstomas@yahoo.co.jp does not designate 11
(UTC) Received: from User (unknown [203.152.117.111]) by asiaclassified.com (Postfix) with ESMTSP; Tue, 16 Jul 2013 15:23:53
+0000 (UTC) Reply-To: <barr_evanstomas001@yahoo.co.jp> From: "Barrister Evans Thomas"<barr_evanstomas@yahoo.co.jp> Subject: WITH DUE RESPECT Date: Wed, 17 Jul 2013
X-Priority: 3 X-MSMail-Priority: Normal X-Mailer: Microsoft Outlook Express 6.00.2600.0000 X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000 Message-Id:
<20130716152354.789A24EF1AB3@asiaclassified.com> To: undisclosed-recipients;
```

**Figure1: Header details of email 1**

<https://www.ipvoid.com/ip-blacklist-check/>


IP Reputation API

Real-time an IP address through more than 80 IP reputation and DNSBL services. This service is built with the IP Reputation API by APIVoid.

111.91.237.247

Check IP Address

IP Address Information

Analysis Date	2024-11-15 13:05:33
Elapsed Time	3 seconds
Detections Count	2/93
IP Address	111.91.237.247 <a href="#">Find Sites</a>   <a href="#">IP Whois</a>
Reverse DNS	Unknown
ASN	AS131188
ISP	Readyspace HK VPS Service
Continent	Asia
Country Code	 (HK) Hong Kong
Latitude / Longitude	<a href="#">Google Map</a>
City	Hong Kong
Region	Hong Kong

reputation/

Figure2: Details of the Ip address for email 1

203.152.117.111

Check IP Address

IP Address Information


Analysis Date	2024-11-19 18:57:02
Elapsed Time	1 seconds
Detections Count	0/93
IP Address	203.152.117.111 Find Sites   IP Whois
Reverse DNS	111.host-203-152-117.compassnet.co.nz
ASN	AS9245
ISP	Compass Communications Ltd
Continent	Oceania
Country Code	 (NZ) New Zealand
Latitude / Longitude	Google Map
City	Auckland
Region	Auckland

Figure3: Details of the Ip address for email 1

SPF and DKIM Information

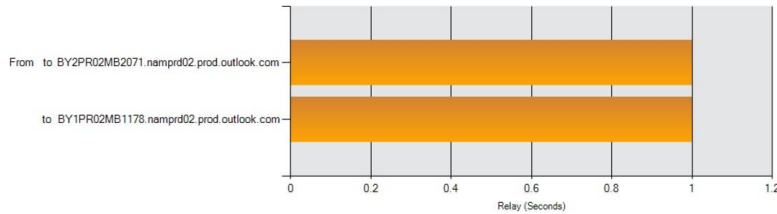
Headers Found

Header Name	Header Value
From	WSEP 1 <webmarketing1@newhaven.edu> To: "Baggili, Ibrahim" <IBaggili@newhaven.edu> Subject: Research Pages
Thread-Topic	Research Pages
Thread-Index	Ac7aRRE0n4PwO9W3TcWxmStmgH+Pqg== Date: Tue, 5 Nov 2013 11:35:41 -0500
Message-ID	
Accept-Language	en-US Content-Language: en-US X-MS-Has-Attach:
X-MS-Exchange-Organization-SCL	-1 X-MS-TNEF-Correlator:
MIME-Version	1.0
X-MS-Exchange-Organization-AuthSource	EXCHANGE-03.newhaven.local X-MS-Exchange-Organization-AuthAs: Internal
X-MS-Exchange-Organization-AuthMechanism	04
X-Originating-IP	[24.2.209.212] Content-type: multipart/alternative;

Figure4: SPF and DKIM details of email 2

## Relay Information

Received Delay: 0 seconds



Ho Del p ay	From	By	With	Time (UTC)	Blackli st
1 *	10.101.1.122	BY2PR02MB2071.namprd02.prod.outlook.com a01:111:e400:c505::23	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WIT H_AES_256_CBC_SHA384_P256)		✓
2 *	BY2PR02MB2071.namprd02.prod.outlook.com 2 a01:111:e400:58a3::27	BY1PR02MB1178.namprd02.prod.outlook.com	HTTPS	[Mon, 26 Mar 2018]	✓

Figure5: Relay Information of Email 3

## SPF and DKIM Information

### Headers Found

Header Name	Header Value
19	07:59 +0000
Authentication-Results	newhaven.edu; dkim=none (message not signed) header.d=none;newhaven.edu; dmarc=none action=none header.from=unh.newhaven.edu;
From	UNH <mtopo1@unh.newhaven.edu>
Mime-Version	1.0 (Mac OS X Mail 11.2 (3445.5.20))
Subject	Suspected Cheating Midterm
Message-Id	<C00CEFB9-F209-4608-A365-9B0E8B8AFB31@unh.newhaven.edu> Date: Mon, 26 Mar 2018 15:07:53 -0400
To	Ibrahim Baggili <ibaggili@newhaven.edu> X-Mailer: Apple Mail (2.3445.5.20)
X-MS-Exchange-Organization-Network-Message-Id	
X-MS-Exchange-Organization-AuthSource	BY2PR02MB2071.namprd02.prod.outlook.com X-MS-Exchange-Organization-AuthAs: Internal
X-MS-Exchange-Organization-AuthAs	06
X-MS-Exchange-Organization-AuthMechanism	
X-Originating-IP	[64.251.61.74]
X-ClientProxiedBy	BN6PR2001CA0038.namprd20.prod.outlook.com (2603:10b6:405:16::24) To BY2PR02MB2071.namprd02.prod.outlook.com (2a01:111:e400:c505::23)
X-MS-Exchange-Organization-MessageDirectionality	Originating Return-Path: mtopo1@unh.newhaven.edu
X-MS-PublicTrafficType	Email

X-MS-PublicTrafficType	Email
X-MS-Office365-Filtering-Correlation-Id	02067feb-7130-4ba4-1402-08d5934ca39c X-Microsoft-Antispam:
UriScan	(43345366909142);BCL:0;PCL:0;RULEID:(7020095)(4652020)(8989060)(560 0026)(4604075)(2017052603328)(7153060)(7193020);SRVR:BY2PR02MB2071;
X-Microsoft-Exchange-Diagnostics	1:BY2PR02MB2071.3:jwviqfSafZtaX3yubifAH0pp7CwczgKPolxYX+nAVLIVK 0Vn+FFVqyBOVrtMgO0mroKRDkANH72JA/RN123kwW1+Kw9oAyQpGgm5pVVA EJEUxLyGUcof77KDdH1As9Bw9RHAU4LEhZaall9ekqMGQ+L4cym8u0b00tVKIO Zr811XCMMz41b74NPc6FvX+XQk NSJ1S6DyMN+HIC6nGGjkzTtyghz9GOSicpXV 6s7uM6GyCmJu1R/c5ieNORuUAQWxSsMdEGqCE0ZvORkHAEleJk3kQWL3wzWE rHyhtqaY5Vuvd8SZCJueQ7JR1KJOsibHhT/Gjla93pgQO+qJUEyVOAVvEX TYXP3lp/HOXa+KfwXlpOncrplz8qhogkudk95L2M6I4Hmtxo8Rp1rteQFDClJtzd7Jx GW11y1sMMWkGW/TnXzUoaOMWLskgF2Qb03BWI7x8dZ7H7e6nho1zqfmxv6B+P67 E6i62arOOgCTH25se8xYHP/SgujMUB cqxW0oszEcvKOYJzP2ZdVnmQ95dyYSPUo4 C28KpP01qH5rxcK+UEz6I2R0RqQx0k0b9QglCbh+JGwGXnDg4Is15b550tohoR 92nOICRYTgpg==31 at4GpQg5IGQEnenBQMpPXqs4aXpa66FJ5rnJN0+LVS36v4J 3yVCavakE6sX05XkYulOTuPCL23lhdQPXP5+Voy3Q07ymWJ urH2JWNgTLSQ nEoRX2TYSwVEaNH6HgaW3FVGtVY9ptJDM3Jym58yNRD8ZuXFFwDKT30v9SHI 8YF5KwngZLnsIpEoOmP2D5N6ahy0FmpF+mLkQPIh66dU4xogjbc=
X-MS-TrafficTypeDiagnostic	BY2PR02MB2071:
X-MS-Exchange-AuthSource	sap=1;slp=1; X-MS-Exchange-Organization-BypassClutter: true
X-Exchange-Antispam-Report-Test	UriScan:(43345366909142); X-Exchange-Antispam-Report-CFA-Test:
BCL	0;PCL:0;RULEID:(8211001083)(910524173)(2401047)(8121501046)(823300181
X-Forefront-Antispam-Report	
SFV	SKI:SFS.DIR.INB.SFP.-SCL:-1;SRVR:BY2PR02MB2071;H[10 101.1.122];FPR:
SPF	None;LANG:en;
X-MS-Exchange-Organization-SCL	-1
SpamDiagnosticOutput	1.0
X-MS-Exchange-CrossTenant-OriginalArrivalTime	26 Mar 2018 19:07:58.5903 (UTC) X-MS-Exchange-CrossTenant-Network-Message-Id:
X-MS-Exchange-CrossTenant-FromEntityHeader	Hosted
X-MS-Exchange-CrossTenant-Id	3c71cbab-b5ed-4f3b-ac0d-95509d6c0e93 X-MS-Exchange-Transport-CrossTenantHeadersStamped: BY2PR02MB2071 X-MS-Exchange-Transport-EndToEndLatency: 00:00:00.7529108
X-MS-Exchange-Processed-By-BcfFolding	15.20.0609.000 X-Microsoft-Exchange-Diagnostics:
1:BY1PR02MB1178:9	v0Bw06ShXKGBJWtIFW4rHv40BXMKGRVaDUtU24
X-Microsoft-Antispam-Message-Info	
Content-type	multipart/alternative; boundary="B_3604921755_1415257355"

Figure6: Header analysis of email 3

64.251.61.74

Check IP Address

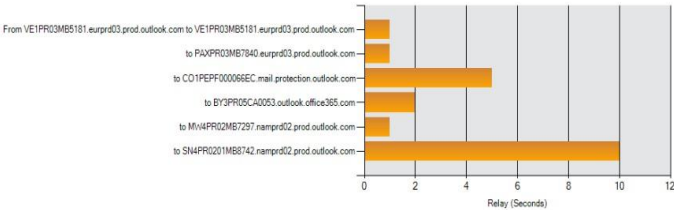
IP Address Information

Analysis Date	2024-11-21 12:19:14
Elapsed Time	4 seconds
Detections Count	0/93
IP Address	64.251.61.74 Find Sites   IP Whois
Reverse DNS	Unknown
ASN	AS22742
ISP	University of New Haven Forensics Lab
Continent	North America
Country Code	(US) United States of America
Latitude / Longitude	Google Map
City	West Haven
Region	Connecticut

Figure7: Details of Ip address associated with email 3

Relay Information

Received Delay:	14 seconds
-----------------	------------



Ho p	Delay	From	By	With	Time (UTC)	Blacklis t
1	*	VE1PR03MB5181.eurprd03.prod.outlook.com fe80:9cbf.8f67.2ed9.da82	VE1PR03MB5181.eurprd03.prod.outlook.com fe80:9cbf.8f67.2ed9.da82	mapi	9/2/2024 8:20:50 AM	
2	0 seconds	VE1PR03MB5181.eurprd03.prod.outlook.com 2603:10a6:802:a7::13	PAXPR03MB7840.eurprd03.prod.outlook.com 2603:10a6:102:20a::6	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	9/2/2024 8:20:50 AM	
3	4 seconds	AM0PR83CU005.outbound.protection.outlook.com 52.101.69.74	CO1PEPF000066EC.mail.protection.outlook.com 10.167.249.8	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	9/2/2024 8:20:54 AM	
4	1 Second	CO1PEPF000066EC.namprd05.prod.outlook.com 2603:10b6:a03:39b:cafe::6a	BY3PR05CA0053.outlook.office365.com 2603:10b6:a03:39b::28	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	9/2/2024 8:20:55 AM	
5	0 seconds	BY3PR05CA0053.namprd05.prod.outlook.com 2603:10b6:a03:39b::28	MW4PR02MB7297.namprd02.prod.outlook.com 2603:10b6:303:77::16	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	9/2/2024 8:20:55 AM	
6	9 seconds	MW4PR02MB7297.namprd02.prod.outlook.com ::1	SN4PR0201MB8742.namprd02.prod.outlook.com	HTTPS	9/2/2024 8:21:04 AM	

Figure 8: Relay information of spam email



Headers Found

Header Name	Header Value
ARC-Seal	i=2; a=rsa-sha256; s=arcselector10001; d=microsoft.com; cv=pass; b=AplZSZDKvRRQRYIFBJAuaM3fSblZ3bL.oGg+e3CHigdn9O0SszA2Tixvbc09x4FjTYEw8SzYD4JNWE6NkCCjyXOc70OBCyD6Q6XUM5OfRu5GZEK55pWL6+LA3A5Fm2POqf5ijO96NDgAgC7UxLjiJgOYcJReBRIY+XUJ31Cg95FH+uMKVnPG8wVF2cAAZn1adZVRKF9BitMBIOrwJGOoOiazQUmLeYpXOJ51uRGNZKW4pTkbgHtHbKqSZkKpDlnvnHtIGHHsLJkmxN6M4iXC0fDjOREByFOFISZSFnHLvUvVhRwkOkI51GQKXZAsPgEqNoLgTSiIV2RHnPWWX2QA==
ARC-Message-Signature	i=2; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com; s=arcselector10001; h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-AntiSpam-MessageData-ChunkCount:X-MS-Exchange-AntiSpam-MessageData-0:X-MS-Exchange-AntiSpam-MessageData-1; bh=PI57kGwNIQ/pVFPJnd3He2LiJq0Es87RwU2ITXRUS0=; b=mQ/R3NXS8Y010dMt11WuC9ePlwncDF/+WC+b6MrK9/LXM/kbnfaBpQULMKYyEEdbKCfctKDhtus6PTIvxitNvdNz7i2fhO9mLFNLO1XT9oPJt1gPFraH+OO0P6RxdhgZ2xpkZmn/aGQO6g8fMp5IS9GfEwptvdzEkGKRdwwcDKVAwgmkiywAtEj/YUEgEht6n38JHEJTJyUySSaJYwz2Zkf9NmuBc+sRHyDm1agpC02VR/bm8Prbdt8N70p/4leRX8tb/Cafi46C1thufp+QHMIe3IEzAb37Q2FSN7VhrOYFJ+KIEs3AQeTi4oNCtxvd/LpCuDPI9Xwpmn+Ww==
ARC-Authentication-Results	i=2; mx.microsoft.com 1; spf=pass (sender ip is 52.101.69.74) smtp.rcpttodomain=unh.newhaven.edu smtp.mailfrom=mylife.mku.ac.ke; dmarc=pass (p=none sp=none pct=100) action=none header.from=mylife.mku.ac.ke; dkim=pass (signature was verified) header.d=mkuac.onmicrosoft.com; arc=pass (0 oda=1 ltdi=1 spf=[1,1,smtp.mailfrom=mylife.mku.ac.ke] dkim=[1,1,header.d=mylife.mku.ac.ke] dmarc=[1,1,header.from=mylife.mku.ac.ke])
Authentication-Results	spf=pass (sender IP is 52.101.69.74) smtp.mailfrom=mylife.mku.ac.ke; dkim=pass (signature was verified) header.d=mkuac.onmicrosoft.com;dmarc=pass action=none header.from=mylife.mku.ac.ke;compauth=pass reason=100
Received-SPF	Pass (protection.outlook.com: domain of mylife.mku.ac.ke designates 52.101.69.74 as permitted sender) receiver=protection.outlook.com; client-ip=52.101.69.74; helo=AM0PR83CU005.outbound.protection.outlook.com; pr=C
DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; d=mkuac.onmicrosoft.com; s=selector2-mkuac-onmicrosoft-com; h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck; bh=PI57kGwNIQ/pVFPJnd3He2LiJq0Es87RwU2ITXRUS0=; b=MI8zcHJ5ktG7ua/KT0LpWZJVs8V95RwMly7vIE8Q06Lpw9gmfQQDRMh7TRAxpXr/F51Hykbbv7HVfypj2UloLXvdC+sw66d9ERVhiQY6Q5avndzuFEgg2owNXky6vif7wh4G4oaEYgEPloEnlXJ1sRf3jzaMA5WkVb2PR/k=
From	IAN MWANGI - BCOM202445914 <bcom202445914@mylife.mku.ac.ke>
Subject	Assistant UTH7623736
Thread-Topic	Assistant UTH7623736
Thread-Index	AQHh/RDDOWciaac2fJuaXUzKhndiRhQ==
Date	Mon, 2 Sep 2024 08:20:49 +0000
Message-ID	<VE1PR03MB5181A99DAB3000F3FD30F17083922@VE1PR03MB5181.eurprd03.prod.outlook.com>
Accept-Language	en-US
Content-Language	en-US
X-MS-Has-Attach	

X-MS-Exchange-Transport-CrossTenantHeadersStamped	PAXPR03MB7840
To	Undisclosed recipients.;
Return-Path	bcom202445914@mylife.mku.ac.ke
X-MS-Exchange-Organization-ExpirationStartTime	02 Sep 2024 08:20:55.1293 (UTC)
X-MS-Exchange-Organization-ExpirationStartTimeReason	OriginalSubmit
X-MS-Exchange-Organization-ExpirationInterval	1:00:00:00.0000000
X-MS-Exchange-Organization-ExpirationIntervalReason	OriginalSubmit
X-MS-Exchange-Organization-Network-Message-Id	1516ab63-9f5a-454b-4b4e-08dccb282a76
X-EOPAttributedMessage	0
X-EOPTenantAttributedMessage	3c71cbab-b5ed-4f3b-ac0d-95509d6c0e93:0
X-MS-Exchange-Organization-MessageDirectionality	Incoming
X-MS-Exchange-Transport-CrossTenantHeadersStripped	CO1PEPF000066EC.namprd05.prod.outlook.com
X-MS-Exchange-Transport-CrossTenantHeadersPromoted	CO1PEPF000066EC.namprd05.prod.outlook.com
X-MS-PublicTrafficType	Email
X-MS-Exchange-Organization-AuthSource	CO1PEPF000066EC.namprd05.prod.outlook.com
X-MS-Exchange-Organization-AuthAs	Anonymous

Figure9: Details of header information of spam email.

## 4. Problem-Solving and Troubleshooting

Problem 1: Difficulty in locating the appropriate tool and doing more analysis

Solution 1: We ran tests in several text editor plugins before formatting the content in Word and analyzing it in Mx Toolbox.

Problem 2: Determining Email Origin and Authenticity

Solution 2: Trace IP addresses in headers to confirm geographic location and match with the sender's claimed location.

## 5. Conclusion and Recommendations

Group 3 had performed the analysis of the given email and one from the spam folder. They had performed both manual inspection as well as header analysis using automated e-mail header analysis tools. They had concluded that the Email 1 is a scam based on several red flags present in the email. The second and third email were proven to be legitimate through the wording of the email, context of the email body, the server the mail was sent through, and the IP address supports the legitimacy of the email. And the email from the spam box was identified as suspicious from the manual inspection even though nothing suspicious was identified during the header analysis and caution should be taken before following the link provided in the email.

From this lab it was evident that they could analyze emails and obtain sufficient testing parameters from the header. They had manually analyzed the header, monitored suspicious IPs, saw the return address, and relayed information using the MX toolbox. SPF and DKIM information provided the sender server's legitimacy and digital signature in the DMARC test. Investigators who completed this lab become adept in basic to intermediate email analysis, ranging from legitimate emails to spam or phishing. Because phishing emails can sometimes evade the email server, they must be cautious before clicking any suspicious links, which may be indicated by grammatical and syntactical issues.



## 6. References

[1] [https://canvas.newhaven.edu/courses/32296/files/5518152?module\\_item\\_id=2374243](https://canvas.newhaven.edu/courses/32296/files/5518152?module_item_id=2374243)

[2] <https://www.youtube.com/watch?v=qedIyy5KesQ&feature=youtu.be>

## 7. Appendix A: Forms

### E-mail 1 Content:

EVANS THOMAS LAW FIRM  
SOLICITORS & ADVOCATES

No: 15 Allen Avenue Ikeja  
,Lagos.

Email: {barr\_evansthomas001@yahoo.co.jp}

Dear Friend

It is obvious that this proposal will come to you as a surprise. This is because we have not met before but I am inspired to sending you this email following the huge fund transfer opportunity that will be of mutual benefit to the two of us.

However, I am Barrister Evans Thomas Attorney to the late Engr. Ronald Johnson, a national of Northern American, who used to work with Shell Petroleum Development Company (SPDC) in Nigeria. On the 11th of November, 2008. My client, his wife and their three children were involved in a car accident along Sagamu/Lagos Express Road.

Unfortunately they all lost their lives in the event of the accident. Since then I have made several inquiries to several Embassies to locate any of my clients extended relatives, this has also proved unsuccessful.

After these several unsuccessful attempts, I decided to trace his relatives over the Internet to locate any member of his family but of no avail, hence I contacted you to assist in repatriating the money and property left behind by my client, I can easily convince the bank with my legal practice that you are the only surviving relation of my client.

Otherwise the Estate he left behind will be confiscated or declared unserviceable by the bank where this huge deposits were lodged. Particularly, the Bank where the deceased had an account valued at about \$15 million U.S dollars (Fifteen million U.S. America dollars).

Consequently, The bank issued me a notice to provide the next of kin or have the account confiscated within the next ten official working days. Since I have been unsuccessful in locating the relatives for over several years now. I seek your consent to present you as the next of kin to the deceased, so that the proceeds of this account valued at \$15 million U.S dollars can be paid to your account and then you and me can share the money. 55% to me and 40% to you, while 5% should be for expenses or tax as your government may require.

All I require is your honest cooperation to enable us see this deal through and also forward the following to me:

Your Full Name:

Your House Address:

Your Tele-phone And Fax No:

Your Age and Gender :

Your Nationality:

Your Occupation:

I guarantee that this will be executed under a legitimate arrangement that will protect you from any breach of the law. Please get in touch with me

VIA this my confidential email {barr\_evanstomas001@yahoo.co.jp}

Yours Faithfully,

Barr. Evans Thomas . { SAN }

## E-mail 1 Header:

Delivered-To: baggili@gmail.com Received: by 10.58.118.162 with SMTP id kn2csp90327veb; Sun, 3 Nov 2013 18:40:31 -0800 (PST) X-Received: by 10.68.101.225 with SMTP id fj1mr15554200pbb.8.1383532830983;

Sun, 03 Nov 2013 18:40:30 -0800 (PST) Return-Path:

<barr\_evanstomas@yahoo.co.jp> Received: from asiaclassified.com (asiaclassified.com. [111.91.237.247]) by mx.google.com with ESMTPS id ar5si9269155pbd.182.2013.11.03.18.39.25 for <multiple recipients> (version=TLSv1 cipher=RC4-SHA bits=128/128);

Sun, 03 Nov 2013 18:40:30 -0800 (PST) Received-SPF: softfail (google.com: domain of transitioning barr\_evanstomas@yahoo.co.jp does not designate 111.91.237.247 as permitted sender)

client-ip=111.91.237.247; Authentication-Results: mx.google.com; spf=softfail (google.com: domain of transitioning barr\_evanstomas@yahoo.co.jp does not designate 111.91.237.247 as permitted sender) smtp.mail=barr\_evanstomas@yahoo.co.jp

Received: from asiaclassified.com (unknown [127.0.0.1]) by asiaclassified.com (Postfix) with ESMTP id 789A24EF1AB3; Tue, 16 Jul 2013 15:23:53 +0000

(UTC) Received: from User (unknown [203.152.117.111]) by asiaclassified.com (Postfix) with ESMTP; Tue, 16 Jul 2013 15:23:53

+0000 (UTC) Reply-To: <barr\_evanstomas001@yahoo.co.jp> From: "Barrister Evans Thomas" <barr\_evanstomas@yahoo.co.jp> Subject: WITH DUE RESPECT Date: Wed, 17 Jul 2013 03:27:31 +1200 MIME-Version: 1.0 Content-Type: text/html; charset="Windows-1251" Content-Transfer-Encoding: 7bit

X-Priority: 3 X-MSMail-Priority: Normal X-Mailer: Microsoft Outlook Express 6.00.2600.0000 X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000 Message-Id:

<20130716152354.789A24EF1AB3@asiaclassified.com> To:  
undisclosed-recipients;;

## E-mail 2 Content

Abe,

Dr. Harichandran mentioned you're looking to make some pages for the Cyber Forensics research lab and group. Let me know if you know what you'd like and what I should start, otherwise we can find a time to meet to go over it.

Thanks,

C.J. Losapio  
Web Student Employee, Marketing and Enrollment Communications  
University of New Haven – A Leader in Experiential Education  
[webmarketing1@newhaven.edu](mailto:webmarketing1@newhaven.edu)

## Message 2 Source:

Received: from EXCHANGE-02.newhaven.local ([fe80::542b:8e94:1f9b:313e]) by  
EXCHANGE-03.newhaven.local ([fe80::a804:cf41:832f:7b97%11]) with mapi id  
14.02.0247.003; Tue, 5 Nov 2013 11:35:42 -0500  
From: WSEP 1 <webmarketing1@newhaven.edu>  
To: "Baggili, Ibrahim" <IBaggili@newhaven.edu>  
Subject: Research Pages  
Thread-Topic: Research Pages  
Thread-Index: Ac7aRRE0n4PwO9W3TcWxmStmgH+Pqg==  
Date: Tue, 5 Nov 2013 11:35:41 -0500  
Message-ID:  
<FB18C6394F8A4D4E82CF58CAC6294F9089717DCF@EXCHANGE-02.newhaven.lo  
cal>  
Accept-Language: en-US  
Content-Language: en-US  
X-MS-Has-Attach:  
X-MS-Exchange-Organization-SCL: -1  
X-MS-TNEF-Correlator:  
<FB18C6394F8A4D4E82CF58CAC6294F9089717DCF@EXCHANGE-02.newhaven.lo  
cal>  
MIME-Version: 1.0  
X-MS-Exchange-Organization-AuthSource: EXCHANGE-03.newhaven.local  
X-MS-Exchange-Organization-AuthAs: Internal  
X-MS-Exchange-Organization-AuthMechanism: 04  
X-Originating-IP: [24.2.209.212]  
Content-type: multipart/alternative;  
boundary="B\_3466603662\_1670221"

> This message is in MIME format. Since your mail reader does not understand  
this format, some or all of this message may not be legible.

--B\_3466603662\_1670221

Content-type: text/plain;  
charset="ISO-8859-1"

Content-transfer-encoding: quoted-printable

Abe,=20

Dr. Harichandran mentioned you're looking to make some pages for the Cyber Forensics research lab and group. Let me know if you know what you'd like and what I should start, otherwise we can find a time to meet to go over it=  
Thanks,

C.J. Losapio

Web Student Employee, Marketing and Enrollment Communications University  
of New Haven =AD A Leader in Experiential Education  
webmarketing1@newhaven.edu

--B\_3466603662\_1670221

Content-type: text/html;  
charset="ISO-8859-1"

Content-transfer-encoding: quoted-printable

<html dir=3D"ltr">

<head>

<meta http-equiv=3D"Content-Type" content=3D"text/html; charset=3Dutf-8">

<style type=3D"text/css" id=3D"owaParaStyle"></style>

</head>

<body fpstyle=3D"1" ocsi=3D"0">

<div style=3D"direction: ltr;font-family: Tahoma;color: #000000;font-size: 10=pt;">Abe,

<div><br>

</div>

<div>Dr. Harichandran mentioned you're looking to make some pages for the C= yber Forensics research lab and group. Let me know if you know what you'd li= ke and what I should start, otherwise we can find a time to meet to go over = it.</div>

<div><br>

</div>

<div>Thanks,<br>

<div><br>

<div style=3D"font-family:Tahoma; font-size:13px">

<div style=3D"font-size:13px"><font face=3D"Tahoma"><span lang=3D"en-US">

<div style=3D"margin:0"><font size=3D"2"><span style=3D"font-size:11pt">C.J. Losa=  
pio<br>  
</span></font></div>

<div style=3D"margin:0"><font size=3D"2"><span style=3D"font-size:11pt">Web  
Stude=

nt Employee, Marketing and Enrollment Communications</span></font></div>

<div style=3D"margin:0"><font size=3D"2"><span style=3D"font-size:11pt">Universit=  
y of New Haven =AD A Leader in Experiential Education</span></font></div>

<div style=3D"margin:0"><font size=3D"2"><span  
style=3D"font-size:11pt">webmarket=

ing1@newhaven.edu</span></font></div>

</span></font></div>

</div>

</div>

</div>

</div>

</body>

</html>

--B\_3466603662\_1670221--

## E-mail 3 Content

Hello Professor Baggili,

Several weeks ago during class, when you were away on paternity leave, we gave out the midterm exam to students to complete. I was on the lookout for any suspected cheaters as requested and I noticed suspicious behavior. I dismissed it at first.

After reviewing the exams I noticed a pattern of similar answers, and it seems that these two students shared answers as they are way to similar. I wanted to let you know this as soon as I was able to confirm. Please email back on how to proceed.

I have the names of the two students suspected, will share this information with you in person.

Regards,

Matt Topor

**Graduate Research**

**Student University of  
New Haven**  
**UNHcFREG** - <https://www.unhcfreg.com/>  
**Email:** [mtopo1@unh.newhaven.edu](mailto:mtopo1@unh.newhaven.edu)  
**Phone:** 708-668-8648  
**Website:** <https://matts.land>

**Message 3 Source:**

Received: from BY2PR02MB2071.namprd02.prod.outlook.com (2a01:111:e400:58a3::27)  
by BY1PR02MB1178.namprd02.prod.outlook.com with HTTPS via  
BY2PR0601CA0017.NAMPRD06.PROD.OUTLOOK.COM; Mon, 26 Mar 2018

19:07:59 +0000

Authentication-Results: newhaven.edu; dkim=none (message not signed)  
header.d=none;newhaven.edu; dmarc=none action=none  
header.from=unh.newhaven.edu;

Received: from [10.101.1.122] (64.251.61.74) by  
BY2PR02MB2071.namprd02.prod.outlook.com (2a01:111:e400:c505::23) with  
Microsoft SMTP Server (version=TLS1\_2,  
cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384\_P256) id 15.20.609.10;

Mon, 26

Mar 2018 19:07:58 +0000

From: UNH <[mtopo1@unh.newhaven.edu](mailto:mtopo1@unh.newhaven.edu)>

Mime-Version: 1.0 (Mac OS X Mail 11.2 \((3445.5.20)\))

Subject: Suspected Cheating Midterm

Message-Id: <C00CEFB9-F209-4608-A365-9B0E8B8AFB31@unh.newhaven.edu>

Date: Mon, 26 Mar 2018 15:07:53 -0400

To: Ibrahim Baggili <[ibaggili@newhaven.edu](mailto:ibaggili@newhaven.edu)>

X-Mailer: Apple Mail (2.3445.5.20)

X-MS-Exchange-Organization-Network-Message-Id:

02067feb-7130-4ba4-1402-08d5934ce39c

X-MS-Exchange-Organization-AuthSource:

BY2PR02MB2071.namprd02.prod.outlook.com

X-MS-Exchange-Organization-AuthAs: Internal

X-MS-Exchange-Organization-AuthMechanism: 06

X-Originating-IP: [64.251.61.74]

X-ClientProxiedBy: BN6PR2001CA0038.namprd20.prod.outlook.com

(2603:10b6:405:16::24) To BY2PR02MB2071.namprd02.prod.outlook.com

(2a01:111:e400:c505::23)

X-MS-Exchange-Organization-MessageDirectionality: Originating

Return-Path: [mtopo1@unh.newhaven.edu](mailto:mtopo1@unh.newhaven.edu)

X-MS-PublicTrafficType: Email

X-MS-Office365-Filtering-Correlation-Id: 02067feb-7130-4ba4-1402-08d5934ce39c

X-Microsoft-Antispam:

UriScan:(43345366909142);BCL:0;PCL:0;RULEID:(7020095)(4652020)(8989060)(560  
0026)(4604075)(2017052603328)(7153060)(7193020);SRVR:BY2PR02MB2071;

X-Microsoft-Exchange-Diagnostics:

1;BY2PR02MB2071;3;jwviqqFSaFztaX9wubiFA/H0pp7CwxzgKPokxYkX+nAVLIVK  
0Vn+FfVqyBOVvtMgO0mroKRDkANtH72JA/RN123kwW1+Kw9oAyQpGgm5pVVA  
EJtEUXLyGUcoF77KDdH1As9Bw9RhAU4LEhZaal09ekqMGQ+L4cym8u0b00tVKIO  
Zr811XCMvzn41itv74NPc6FvX+XQkNSjl1S6DyMN+HiC6nGGjkzTlyghz9GOSicpXV

6s7uM6GyCmJu1R/c5ieNORuUAQWxSsMdEGqCE0ZvxORkkHaEJe3kQWL3wzWE  
=;25:rHyhtqaY5VuVc8SZCUEQ7jR1KJOtSfbiHg/TGjsL9f3pqOO+qULEyvOAVvwEX  
TYXP3Ip7HOXA+kFwXfpOncrIpfz8qhokudk95L2M6l4Hmtxo8Rp1rteQFDCjUtzdt7Jx  
GWI1yIsMfWkGW/TnXzUoaOMWLskgF2Qb03jBWI7/xBdZH7e6nhoi2fqfnxv6B+P67  
E6l62arOOgCTH25se8xYHP/SgujMUBcxqW0oszEcvkO0YJzPZcIVnnQ95dyYSPUo4  
CZ8KipPO1qH5r/xCK+UEzi6l2lR0RqOx0k0tb9OgICbh/+JGwGXnDsG4Is15b550toh0R  
92nOtDCRYTg/g==;31:at4goPq5tGQEnenBQMpPXqs4a/Xrpa66FJ5rrlNJ0+LVS36vt4J  
3yVCavakEe6SxO5iXkYuiOTuPCLz3Ihd/QPXP5+VOyi3Q07yunWjurHrZjWNgTSLQ  
nEoRX2TYSwVEaN6iHg6aw3FVGitVY9ptJDM8JYm58yNRD8zuIXFHwDKT30v9Shl  
f8YF5KwgZLnsIpEoOmp2D5N6ahy0FlmrpF+mLkkQP/h66ciU4xqpjbc=

X-MS-TrafficTypeDiagnostic: BY2PR02MB2071:

X-MS-Exchange-AuthAsSourceProperties: sap=1;slp=1;

X-MS-Exchange-Organization-BypassClutter: true

X-Microsoft-Exchange-Diagnostics:

1;BY2PR02MB2071;20:r6PLXaNbrQjdt/had4yH96uIg0+7Y6QF32xy0DGzXfdtFxfhTh  
LYa45mq0CbkOkZC1h/XFMq/8autDun8KUq4zr1vBUZsdziHxrJAeUQLcn+SftGW00U  
5pDp+X7t0SdW+buQ/1Iv4tOW2nalBb+EwTpn0ybrF9SnIsY2xeR5AE2LPFjScojtdbSD  
JNijX9KTFdKKjU94c+0SSHbY4op2M7+19Wdp6ugplQEnA8/RtNF3o/8jdNEd+G2Y9  
XwZY9dC3VNMLnh4+q1jAXoHntK7WPQUiZAYs9ANiNvtLA22pNj51+Bdz0Ig8bEG  
JSVjJNjzJtrDXelkukHtQ0t9ZliHD4xbVV4Ey6bt5aDOxFqDR5z/Fpu/U86Y1nrmUkbid2  
5unD/jWp7HNDk6Eh9vJkMZONwcyiwz4fCmMJcE7hf4NvaeFRXYQ5anw1DTl4G2M  
qur2sRPolfZkugrnl7bCCDQsWlw0vpFk4b/1j27kd4MaususK2I9k1DQoEfAZuHkzLY;4:  
vInA4C9kTtr/quO1I3CBmG9FV1SIO0qgj674BHZ9OKqC8IxlDcKWUJaeEsA2ZGk5+  
C5yOTzU6lgOtk3mfJK6ZqY067ohPJy1pBY/u/kU52aL6C1IaAglA1g2LdBIkv1sTJPsZ4  
qllGDGvmK+tmM7WEu2aW2dqbQMow2UhGWqK4D+q3LYCZckl0tNkLVX2S+3BE  
Z3ZDBRaxOqh8y88Odptp5BHtKll/rtNjtt6dUQuVHhIVzgrKrDB33BNFTtB3Fv0unll87  
ykZaPLWnuNV2grkVJvOqj+Ok82Be7+lxOUDFoN4bLaX6m4NL5mxOaL1sm

X-Exchange-Antispam-Report-Test: UriScan:(43345366909142);

X-Exchange-Antispam-Report-CFA-Test:

BCL:0;PCL:0;RULEID:(8211001083)(9101524173)(2401047)(8121501046)(823300181  
(823320095)(3231221)(944501327)(52105095)(93006095)(93001095)(10201501046)(3  
002001)(201708071742011);SRVR:BY2PR02MB2071;BCL:0;PCL:0;RULEID:;SRVR:  
BY2PR02MB2071;

X-Forefront-Antispam-Report:

SFV:SKI;SFS:;DIR:INB;SFP:;SCL:-1;SRVR:BY2PR02MB2071;H:[10.101.1.122];FPR:  
;SPF:None;LANG:en;

X-MS-Exchange-Organization-SCL: -1



X-Microsoft-Exchange-Diagnostics:

1;BY2PR02MB2071;23:7eusy7oFyQ+oMG9hC5oANJL+J4cF27UT33xeHE7NIE9PSD  
M93qn+h6dm2YWBWndlh8TXG0JU+ArVZa+6fD5jcuz42KAe9vTXwBIU3gpXTRDs  
CrWr0gybcBBpDAeYVPDEuOICJd4gdQP3tMPgfPClf/sTG/dSrdwHdeGDvZYBkKk=;  
6:KBLy4/Lm4MpMJfbrTBG5TS+j/3Irrer3t2C6NzKM2T6X5eASy+h1qsRxdnlpCTAux  
WfS64GuBoULvMDzqOMhDXf2H510QMRI+grMzklEMvB008VK4UsR44js5w4654T  
5wUlhrao4t9W1PjimNpKXHNy/gxGXbIERBNrCGGBakWDdtHPJ+sJRe3jnbDjSitqWr  
58gbhDQSYT9lwVpwHN18/2AHkVQdlqIuDpxgWH4ZdOMZtE4D0/FjsuOphecn/Ms0  
YfCoUTDsA5TNzBnB+df4agMLWU0HMJsQtrQsEwKPrsP7+G/w8ZY41GJZr5s2H2G  
TT3jrBL0mJfhV9E9b8+lnyD59p7FyC6bJXdknFl5oZXhcWKXvY/v3vndNy6h8MfYiK  
Lfe5D4LVqDvg0FQSVgt5ujRC+ValLlaU1BvXq91TrB/Nr8RFay//Xp5gAYRJujewrhRJ  
2fa8hk+HaPg4uYaQ==;5:jKHPKSKu6+4VNU9lz1FEaYoNZ30wheRJY2pCTfFz2Esd7f  
sCXTa0iARY7nYCXEjfUCfLgOvYBSSyqHKCzsFjlzkk+y9JexjlvqH2Qd/sgDUqx1B+  
LfQfIO+Z4t2AfQIXGan8ikCAJ2mfCeCOofHKoNF45/VMurRHJzKi0pCZcoo=;24:7z4s  
7z1HgpeBp26r9AWP8kKDiSR647AuTmQuV+CBC8yirnRogaZVfAkdo8MAQ1k3smS  
B3mSUWqnis7PbKdQsu+9dLs96mLyVY5xhPtW/maE=

SpamDiagnosticOutput: 1:0

X-Microsoft-Exchange-Diagnostics:

1;BY2PR02MB2071;7:ntuaM5H511fxZUJqcQolAqthJgT1I4/4SqIQIdggUjFgSx3m84H  
YrmvpOGWqKmW9ftpUI000DF662UrM2y/xBvP/eCNp9wqEoPrgyGAIQLssycnCEfT  
X4t+3hAJDG3Yw9im4211aXjoX7OUIRPfWXMypRA5o1q1MXQuD5QqRG/Fj9KYlah  
o+4QFtGA15YqKR4VtqprrrxOcf4hsgIikgKbPSN0UBsbD3Y56CmSIzmhJAjhOaDPqM  
BvkM5NTKFDvm;20:wNnQw6jtuTagzn6mvNDWTXRHgvDvlGIHddz8mcarBbk40UA  
6dvCYSvo03iBlp/FYTjfVakOYPmXgUSGvE83ii0L0tA3g+nRD+ME4q5pV17eGaZckc  
W6Aw2TEmjjeZrdpamwSxMY3sYT0SsZIPW8dvWr858WOSr6x0sezdoOdkyU=

X-MS-Exchange-CrossTenant-OriginalArrivalTime: 26 Mar 2018 19:07:58.5903 (UTC)

X-MS-Exchange-CrossTenant-Network-Message-Id:

02067feb-7130-4ba4-1402-08d5934ce39c

X-MS-Exchange-CrossTenant-FromEntityHeader: Hosted

X-MS-Exchange-CrossTenant-Id: 3c71cbab-b5ed-4f3b-ac0d-95509d6c0e93

X-MS-Exchange-Transport-CrossTenantHeadersStamped: BY2PR02MB2071

X-MS-Exchange-Transport-EndToEndLatency: 00:00:00.7529108

X-MS-Exchange-Processed-By-BccFoldering: 15.20.0609.000

X-Microsoft-Exchange-Diagnostics:

1;BY1PR02MB1178;9:vGBwo6GhXfKGBJWtrlFFjvwHrVr40BXWkfGRVaDcUTU2I4  
sluXPTGmawPPIBhn9ldMQU40GvcBp/5DEF7NaXGu28V+6bRcFjhTokifPAaHKeyhl  
PcwdYg0HdmGV7+8/2

X-Microsoft-Antispam-Message-Info:

4ZdHC27o8QBNC4UD4snnyyypglWVvk3P9ADdmTi5i7Y5QIe764Lh+w0vSd7KJ+nCAx  
K2I36Q6jxeRklnVYA+ojIIjPKYfb6SPBgIn+VaCe2IKUa+c5k9Ajeu+fWOei6H7T55QZ  
KAS9Z4vU7ZdbYxPXC0polhOygh8x7tWXvWR/zBtRKE2mRiKEq3Cxc4ED4T53

X-Microsoft-Exchange-Diagnostics:

1;BY1PR02MB1178;27:s1rFCnGT7cj1inQgcZ65YEWZgC9jmhd6b6mhDZtIBkMSjkiw

Vg6DQxRIIvLqSmJXNY7Oe11WK8Er4dzhnc9EcbZcS/tajgfDreytU2XUgs9YixIaERM  
udp7oXVqsjiDg

Content-type: multipart/alternative;  
boundary="B\_3604921755\_1415257355"

> This message is in MIME format. Since your mail reader does not understand  
this format, some or all of this message may not be legible.

--B\_3604921755\_1415257355  
Content-type: text/plain;  
charset="UTF-8"  
Content-transfer-encoding: 7bit

Hello Professor Baggili,

Several weeks ago during class, when you were away on paternity leave, we gave out the  
midterm exam to students to complete. I was on the lookout for any suspected cheaters as  
requested and I noticed suspicious behavior. I dismissed it at first.

After reviewing the exams I noticed a pattern of similar answers, and it seems that these  
two students shared answers as they are way to similar. I wanted to let you know this as  
soon as I was able to confirm. Please email back on how to proceed.

I have the names of the two students suspected, will share this information with you in  
person.

Regards,

Matt Topor

Graduate Research Student

University of New Haven

UNHcFREG - <https://www.unhcfreg.com/>

Email: [mtopo1@unh.newhaven.edu](mailto:mtopo1@unh.newhaven.edu) Phone:

708-668-8648

Website: <https://matts.land>

--B\_3604921755\_1415257355

Content-type: text/html;  
charset="UTF-8"

Content-transfer-encoding: quoted-printable

<html>

<head>

<meta http-equiv=3D"Content-Type" content=3D"text/html; charset=3Dutf-8">

</head>  
<body style=3D"word-wrap: break-word; -webkit-nspace-mode: space; line-break: af= ter-white-space;" class=3D"">  
Hello Professor Baggili,  
<div class=3D""><br class=3D"">  
</div>  
<div class=3D"">Several weeks ago during class, when you were away on paterni=  
ty leave, we gave out the midterm exam to students to complete. I was on the=  
lookout for any suspected cheaters as requested and I noticed suspicious be=  
havior. I dismissed it at first.</div>  
<div class=3D""><br class=3D"">  
</div>  
<div class=3D"">After reviewing the exams I noticed a pattern of similar answe=  
rs, and it seems that these two students shared answers as they are way to =  
similar. I wanted to let you know this as soon as I was able to confirm. Ple=  
ase email back on how to proceed.</div>  
<div class=3D""><br class=3D"">  
</div>  
<div class=3D"">I have the names of the two students suspected, will share th=  
is information with you in person.</div>  
<div class=3D""><br class=3D"">  
</div>  
<div class=3D"">Regards,</div>  
<div class=3D""><br class=3D"">  
</div>  
<div class=3D"">  
<div class=3D"">  
<div style=3D"color: rgb(0, 0, 0); font-family: Helvetica; font-size: 12px; f= ont=  
style: normal; font-variant-caps: normal; font-weight: normal; letter-sp= acing:  
normal; orphans: auto; text-align: start; text-indent: 0px; text-tran= sform: none;  
white-space: normal; widows: auto; word-spacing: 0px; -webkit-t= ext-size=  
adjust: auto; -webkit-text-stroke-width: 0px;">  
Matt Topor<br class=3D"">  
<b class=3D"">Graduate Research Student</b><br class=3D"">  
<b class=3D"">University of New Haven</b><br class=3D"">  
<b class=3D"">UNHcFREG</b><span  
class=3D"Apple-converted-space">&nbsp;</span>-&=  
&nbsp;<a href=3D"https://www.unhcfreg.com/"  
class=3D"">https://www.unhcfreg.com/<=  
</a><br class=3D"">  
<b class=3D"">Email:</b>&nbsp;<a href=3D"mailto:mtopo1@unh.newhaven.edu"  
class=3D="">mtopo1@unh.newhaven.edu</a><br class=3D"">  
<b class=3D"">Phone:</b>&nbsp;<br class=3D"">  
<b class=3D"">Website:</b>&nbsp;<a href=3D"https://matts.land" class=3D"">https://=  
/matts.land</a></div>

</div>  
<br class=3D"">  
</div>  
</body>  
</html>  
--B\_3604921755\_1415257355--

## SPAM Email content

**Assistant UTH7623736 IB**  
**IAN MWANGI - BCOM202445914<bcom202445914@mylife.mku.ac.ke>**

Mon 02-09-2024 04:21

This message was identified as junk.

It's not junkShow blocked content and enable links

[EXTERNAL SENDER]

Hi there!

I hope this message finds you well. Our property management group is currently looking to hire students as virtual assistants. The position offers a weekly compensation of \$400. If you are interested or know someone who might be, please [reach out to us for more details](#).

Looking forward to hearing from you!

Best regards,  
Dr. Jean-Paul Flores

---

## Message details

Received: from MW4PR02MB7297.namprd02.prod.outlook.com (::1) by SN4PR0201MB8742.namprd02.prod.outlook.com with HTTPS; Mon, 2 Sep 2024 08:21:04 +0000 ARC-Seal: i=2; a=rsa-sha256; s=arcselector10001; d=microsoft.com; cv=pass; b=AplZSZDkvRRQRYtFBJAuaM3fSbIZ3txLoGg+e3CHigdn9O0SzA2Tixvbc09x4FjTYEw8SzYD4JNWE6NkCCjyXOc70OBCyD6Q6XUM5OfRu5GZEK55pWL6+LA3A5Frn2POqf5ijO96NDgAgC7UxLj/jgOYcJReBRIY+XUJ31Cg95FH+uMKVnPG8wVF2cAAzN1adZVRKF9BitMBIOrwJGOoOiazQUmL/eYPXOJ51uRGNZKW4pTkbqHHtbKqSZkKpDInvnH/tGHHsLJkmxN6M4iXC0fDj0REByFOFtSZSFHLvuVvhRwkOkI51GQKXZ2AsPgEqNoLgTSfIV2RHnPWWX2QA== ARC-Message-Signature: i=2; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com; s=arcselector10001; h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-AntiSpam-MessageData-ChunkCount:X-MS-Exchange-AntiSpam-MessageData-0:X-MS-Exchange-AntiSpam-MessageData-1; bh=PI57kGwNIQ/pVFPJnd3He2LiJq0Es87RwIU2ITXRUS0=; b=mQ/R3NXS8Y010dMt11WuC9ePlwncDF/+WC+b6MrK9/LXM/KbnfaBpQULMKYyEEdbKCFctKDHTus6PTlvxitNrvdNz7l2fhO9mLFNLO1XT9oPjT1gPFraH+OO0P6RxdhqfZ2xpkZmn/aGQO6g8fMp5tS9GfEwptvdzEkGKRdwxxcDkVAwgMkiywATej/YUEgEht6n38JHEJTJyUySSaJYwz2ZkfgNmuBC+sRHyDm1agpC02VR/bm8Prbdt8N70p/4leRX8tbfcAfi46C1thufp+QHM

IE3IEzAb37Q2FSN7VhrOYFJ+KIEs3AQeTli4oNCtxvd/LpJCuDPf9Xwpnb+Ww== ARC-  
Authentication-Results: i=2; mx.microsoft.com 1; spf=pass (sender ip is 52.101.69.74)  
smtp.rcpttodomain=unh.newhaven.edu smtp.mailfrom=mylife.mku.ac.ke; dmarc=pass (p=none  
sp=none pct=100) action=none header.from=mylife.mku.ac.ke; dkim=pass (signature was  
verified) header.d=mkuac.onmicrosoft.com; arc=pass (0 oda=1 ltdi=1  
spf=[1,1,smtp.mailfrom=mylife.mku.ac.ke] dkim=[1,1,header.d=mylife.mku.ac.ke]  
dmarc=[1,1,header.from=mylife.mku.ac.ke]) Received: from  
BY3PR05CA0053.namprd05.prod.outlook.com (2603:10b6:a03:39b::28) by  
MW4PR02MB7297.namprd02.prod.outlook.com (2603:10b6:303:77::16) with Microsoft SMTP  
Server (version=TLS1\_2, cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384) id  
15.20.7918.25; Mon, 2 Sep 2024 08:20:55 +0000 Received: from  
CO1PEPF000066EC.namprd05.prod.outlook.com (2603:10b6:a03:39b:cafe::6a) by  
BY3PR05CA0053.outlook.office365.com (2603:10b6:a03:39b::28) with Microsoft SMTP Server  
(version=TLS1\_2, cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384) id  
15.20.7918.24 via Frontend Transport; Mon, 2 Sep 2024 08:20:55 +0000 Authentication-Results:  
spf=pass (sender IP is 52.101.69.74) smtp.mailfrom=mylife.mku.ac.ke; dkim=pass (signature was  
verified) header.d=mkuac.onmicrosoft.com;dmarc=pass action=none  
header.from=mylife.mku.ac.ke;compauth=pass reason=100 Received-SPF: Pass  
(protection.outlook.com: domain of mylife.mku.ac.ke designates 52.101.69.74 as permitted  
sender) receiver=protection.outlook.com; client-ip=52.101.69.74;  
helo=AM0PR83CU005.outbound.protection.outlook.com; pr=C Received: from  
AM0PR83CU005.outbound.protection.outlook.com (52.101.69.74) by  
CO1PEPF000066EC.mail.protection.outlook.com (10.167.249.8) with Microsoft SMTP Server  
(version=TLS1\_2, cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384) id  
15.20.7918.13 via Frontend Transport; Mon, 2 Sep 2024 08:20:54 +0000 ARC-Seal: i=1; a=rsa-  
sha256; s=arcselector10001; d=microsoft.com; cv=none;  
b=PQ4CvSSSIIOQGMSPG6cFCnq+iEoli0JMfs+sCK517wzRlFbsGxE6gpdocKx1s2e6Si7v4Sjn0  
15mHoXWrxXcXX8UaOXOJwtoIVsS9VGNh77Cq2jai6lh32vMo3xxMVRGXEWBfyjgHoLle2O  
vKC2llvKIr7ELvX9fA3k7nhVFQp/BqPXT73g0VWZk4ZetHFzS9bpeEBPgsLxWjtwOjM77OY  
H0Krj3QnF5czqdLo59UbOzZyVqf/gd6kIJoleOHxhEuLKhBYQXpRW0o9a2yswG1CIT/v4aF  
kEw3adX7wsgFPHPD7e1eBizAkONc+jmwCWZSP3w11YAO780fZPmuQeiQ== ARC-  
Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com; s=arcselector10001;  
h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-AntiSpam-  
MessageData-ChunkCount:X-MS-Exchange-AntiSpam-MessageData-0:X-MS-Exchange-  
AntiSpam-MessageData-1; bh=PI57kGwNIQ/pVFPJnd3He2LiJq0Es87RwIU2ITXRUS0=;  
b=mX/C2aK5oqM+42eH2Ms/+OcloEbhIJyBn/zdIYKPP4AQoSJR+KKVNvFtELkHT4eeIEQF  
ZeW6K4j5G1MyYsRPGDmrBqNPHJH2arFQcmqvAZ3xGO79gB+NDUAWWicfbvsZtFlpBWr  
o4pigQZ7pMINGS8opORARPjKR6Et+2DxBLjfiCCXWgKXmWH5ajESkctsWMTE/6Bz0Ho  
MRr0cDwZkL41fYfBDLiEl0pIPjyu/hTyGIBzQ7vzmXz5YeJtpGebePLP0FJAXtdYKEDrgyJW  
FN7DkmhBF7ptkZRROVqearmVuuj2Kdln2OMCAzAkTWZIItzzWYS1MW93vIc8b95ZHeg=  
= ARC-Authentication-Results: i=1; mx.microsoft.com 1; spf=pass  
smtp.mailfrom=mylife.mku.ac.ke; dmarc=pass action=none header.from=mylife.mku.ac.ke;  
dkim=pass header.d=mylife.mku.ac.ke; arc=none DKIM-Signature: v=1; a=rsa-sha256;  
c=relaxed/relaxed; d=mkuac.onmicrosoft.com; s=selector2-mkuac-onmicrosoft-com;  
h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-  
SenderADCheck; bh=PI57kGwNIQ/pVFPJnd3He2LiJq0Es87RwIU2ITXRUS0=;

b=Ml8zcHJ5ktG7ua/KT0LpWZJV s8Vi95RwMy7vfE8iQ06Lpw9lgmfqQDRMfi7RAxpXr/F51  
Hykkbv7HVFypfj2UloLXvdC+sw66d9ERVhiQY6Q5avndzuFEqg2owNXky6vfi7wh4G4oaE  
YgEPloEnIXJ1sRf3jzaMA5WkVb2PR/k= Received: from  
VE1PR03MB5181.eurprd03.prod.outlook.com (2603:10a6:802:a7::13) by  
PAXPR03MB7840.eurprd03.prod.outlook.com (2603:10a6:102:20a::6) with Microsoft SMTP  
Server (version=TLS1\_2, cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384) id  
15.20.7918.25; Mon, 2 Sep 2024 08:20:50 +0000 Received: from  
VE1PR03MB5181.eurprd03.prod.outlook.com ([fe80::9cbf:8f67:2ed9:da82]) by  
VE1PR03MB5181.eurprd03.prod.outlook.com ([fe80::9cbf:8f67:2ed9:da82%4]) with mapi id  
15.20.7918.020; Mon, 2 Sep 2024 08:20:50 +0000 From: IAN MWANGI - BCOM202445914  
<bcom202445914@mylife.mku.ac.ke> Subject: Assistant UTH7623736 Thread-Topic: Assistant  
UTH7623736 Thread-Index: AQHa/RDdOWciaac2fUaXUzKhndiRhQ== Date: Mon, 2 Sep 2024  
08:20:49 +0000 Message-ID:  
<VE1PR03MB5181A99DAB3000F3FD30F17083922@VE1PR03MB5181.eurprd03.prod.outlo  
ok.com> Accept-Language: en-US Content-Language: en-US X-MS-Has-Attach: X-MS-TNEF-  
Correlator: msip\_labels: Authentication-Results-Original: dkim=none (message not signed)  
header.d=none;dmARC=none action=none header.from=mylife.mku.ac.ke; x-ms-  
traffictypediagnostic:  
VE1PR03MB5181:EE\_|PAXPR03MB7840:EE\_|CO1PEPF000066EC:EE\_|MW4PR02MB7297:  
EE\_|SN4PR0201MB8742:EE\_ X-MS-Office365-Filtering-Correlation-Id: 1516ab63-9f5a-454b-  
4b4e-08dccb282a76 x-ms-exchange-senderadcheck: 1 x-ms-exchange-antispam-relay: 0 X-  
Microsoft-Antispam-Untrusted:  
BCL:0;ARA:13230040|376014|7416014|1800799024|366016|41320700013|69100299015|38070  
700018; X-Microsoft-Antispam-Message-Info-Original: =?us-  
ascii?Q?7v4cRVA3YsR8ClvynIkEw9bj0BLU67Si/L8pgN2GB5nQfm6XMglgTrIb83Fk?=  
=?us-  
ascii?Q?ci5yWe/i5hIQ/kwRH9TuLT9zDvYFTQ4/kEJdYNAYOkZbWZigb1WQ9T/PLcin?=  
=?us-ascii?Q?QsJ+lfUscILu0wW6qBVKY9GL8Reqk8w9DyyV5lucQI01CzKTz3vxcjb2zztd?=  
=?us-  
ascii?Q?8qxoORCQb26ZVYSdLJ2Howhr2CxxZauSFuU2EMHLmnOxT2cBJp0q+WUqN6Fz?  
=?us-  
ascii?Q?CRDPZMxwqlhrVfjPqF73IWxwTe7Cohe6Q906Qntdmdbajdh1ZHx33g6kB5KA?=  
=?us-ascii?Q?H2q6toYWNdzqn0ONrZR8IfTsJDKELMsBmJggzI9zgLj87BthFe/0A/j27KJI?=  
=?us-ascii?Q?cCizjbEgve4Vd81bdSpPvEkk/LjvQwl2WGWwn35pA6nmnuZeBP05hxssjZK5?=  
=?us-  
ascii?Q?Pqnm2ujwCbqHk6jWbxAuzl4M8P6Vhqa5zZIHbl3s8GEhSZBkNsfdv7SQ2Sm?=  
=?us-ascii?Q?iqADBYf6Ujsju0/EwUb2XSleh0LN8x+zniwnplb6ahSyijVGN7eDICHVo6C?=  
=?us-  
ascii?Q?ZoVNUUcmK+JeyzuqZF+a7zGWpFfwzWjdlHrw7g9SZeSyqL4VcGnbIwAMmEtC?=  
=?us-  
ascii?Q?Sn/c4adsMMWrGeC09iRuRZtQYbj1Kq+Oa0EYKuvwkYgYQB1oeSGCRYqwdLvQ?  
=?us-  
ascii?Q?RC4+ZBX2NXQh8gf78sg2e7N5TH6vPz6r2JdLGGIyafRhs+0CuS3WDU1Pq0Z+?=  
=?us-  
ascii?Q?scBYxjjuYjt6K5TLLCrMnT64F/PhhZyiQWsPhjIv3bGfeaHowQWd42PHXQN0?=  
=?us-

ascii?Q?zBbBJ56B1pTHv+b9Oc9CNAHZdWmEpysvBhnJ0A6gKQUXiscGXB/qUR4pVE/d?=  
=?us-ascii?Q?896wSxv/fr1XQzJP/pF++fyoQjvKhVLUQxAftYbjWDrtBoTQh6J5ZWE9zwml?=  
=?us-  
ascii?Q?G4bBa0hBAmOZfETmzlDV14aArvspOoe0TBFbuyLF4Qxc0u2CBjHhw1vG2Axr?=  
=?us-  
ascii?Q?cgrbZ/viDPPs5u1fVhk1+o9nfgSH1olxKbLZUHBh1+NhBY0zQPbNjk+R+K0A?=  
=?us-  
ascii?Q?9nGA9Ky6Pq2CBANK186dF52Ebj2RVW/N3d73w4QGw4Q97zQyOCziJuBcXj3m?=  
=?us-  
ascii?Q?nQnYsLEmHh6kNQY7sFvcgRUd9TJkAnPch64Di5NBrmw8o9A+2rYYJ18f24Lq?=  
=?us-  
ascii?Q?dx4R0F3DFgX7myh8DldC2OEWlb7Yp0x+esBJhc1gBV20BiKNGb7vWMOy/H/e?=  
=?us-  
ascii?Q?4vPOC983FPz1rVYh8GXXKpkg4/10DbocgHTOIkmnY2LtBvVZh4Ju+C82coiDT?=  
=?us-  
ascii?Q?vP+JeiSWLLf0na57wi2WOY/Ln28wg5+tt7FFE3GL26FR26RTvOyVKzEfzePR?=  
=?us-ascii?Q?OuVCAH4voFgSzQDz8Jx8LN84ThwNldjLLdjgYq7sYrfk26licZE/h5xIqjE?=  
=?us-ascii?Q?lyOe9wc=3D?=  
X-Forefront-Antispam-Report-Untrusted:  
CIP:255.255.255.255;CTRY:;LANG:en;SCL:1;SRV:;IPV:NLI;SFV:NSPM;H:VE1PR03MB518  
1.eurprd03.prod.outlook.com;PTR:;CAT:NONE;SFS:(13230040)(376014)(7416014)(180079902  
4)(366016)(41320700013)(69100299015)(38070700018);DIR:OUT;SFP:1102; X-MS-  
Exchange-AntiSpam-MessageData-Original-ChunkCount: 1 X-MS-Exchange-AntiSpam-  
MessageData-Original-0: =?iso-8859-  
1?Q?W/iViyRgdfVIQD4Xpal0OFWqRi0/8xaPoPP1k1syam4VP3CwWGRbd3bPyP?=  
=?iso-  
8859-1?Q?QPRYJSFsecDI60qjN8ok8+An6/8X3dTbUlxS8Baf2rbQw1PZysxQDLVTz4?=  
=?iso-8859-1?Q?fWy/WGS7vp0apDI7tOhoIp8N6d5/C5IZr1V3XsK0/ZFFJLI5UHm/5efTEr?=  
=?iso-8859-  
1?Q?7WexkxSB0ll/GQCCeLZ2brfyxyVz/iC6rFymjR7QSM8UyIpYg96+knuMnG?=  
=?iso-  
8859-1?Q?oXjcqhGoJxhmux/nUZUxm2MnULdhLiE7heCijDiTBdbwfoee7WQ17wi1wy?=  
=?iso-8859-  
1?Q?fWzrWvLYF1+7qQJiXwbbhKtroURuFECQm7E63lb+rIN41ECPRrpN0li2ep?=  
=?iso-  
8859-1?Q?pfbtVykn/x/NepkCtuLdkxnXt/g8siF5WwP9T2YoPTvN9Hb00smRY5+iWy?=  
=?iso-  
8859-1?Q?Ada8k2uVfYRPtIPwUFnsf63yGU3S2y6/mtGbFZehVFUJxUPtsCND93Ak81?=  
=?iso-8859-  
1?Q?1ddNxFRJA1IQ0LAXyWz8l2DiL++dAv4Ff8dcabkOuG0vUnXijWWk+wF1Lc?=  
=?iso-  
8859-1?Q?19N0g3zqBoaAQ2EGalR2OyrwguIq/OEDK1UAKo/fFhstCT4DJ7K6F1REIY?=  
=?iso-8859-1?Q?UJnpsOYot2HsKe5EFhm3lWOlnJ8ZQJC5q5l0F0ZXEspX9vn5hL2ryYslNI?=  
=?iso-8859-1?Q?jBVLnT0olfRE3rZ/LdoM0YIcSD1jz8fsYmqValXnS65IT+5iMrZi//xeSK?=  
=?iso-8859-  
1?Q?+Z8iQ+z1qVwrbCwbYq6fRakGjfYg9F982XAVD+oA9PuWNHRWru68to8sSr?=  
=?iso-  
8859-1?Q?u7nxuiFJ6KIBYZ3y+nhyjjEg55uismwA+wfPEqz6A7Wq+jqOqvdpjkgk4?=  
=?iso-  
8859-  
1?Q?MqkpWoiUewO4I+n84sCPk+RuPNFwmqUUR6MOMZCr90iYbmUt2p4LDPgtVQ?=  
=?iso-8859-1?Q?avaAspFcNvacL6l40DADV605uKURxnNONQuz8fa/JgnltlZOxYjHkK5cb6?=  
=?iso-8859-  
1?Q?L5tBOvIOv1WOOm6fTiUS2v0CTkfdBTNKb+rC/EXAKzIFmcHwCttp4SnArO?=  
=?iso-

8859-1?Q?tEKdKQaNylOihmcQvAMaP+RSAaEMbz2yUcJAXTl6ERoCo3ncNnha6gkHS2?=  
=?iso-8859-  
1?Q?CrjJ1KEJ6KHbA1M55oZhPWgIQFBYpMYXzbbkfDcSKQjIHJh1tORfw+fQEq?=  
8859-1?Q?MQLsuQOcxrhlAdtSCH5O08cI0TAeUMI62KtbZ1TvmZ84Cyk7/CBOIKl3eb?=  
=?iso-8859-  
1?Q?b7j5W+K+uG2UHltwGBLuAZ7ObND1tje1woOLavPfk9PeymwqxxvW3js6ocz?=  
8859-1?Q?WPXAt0OXidlgxtwxJVDqU9R/EUJ6r1aGvr3P9z0zrM/mE3QZ+6Z4XVORr3?=  
=?iso-8859-1?Q?nlNbMfbqllg0JoZIRbzb4uQ8M0XGz/RQbV2o7zgONoexJCJJjQeVA9tjh?=  
=?iso-8859-1?Q?fOwi5J9LPK35/7N4Rx52IRFJZYfXrZrib2N/uSLfhIN+PHUOa6cFzPsahW?=  
=?iso-8859-  
1?Q?gXzAPkFogHwHS9kVAu/bAJUj3iwdWH7jlPl+FA6fpmkPoS0T6JqoCjUjQ?=  
8859-  
1?Q?IBSG4h1MoVk5B+10UHZuw6XWq6ygE999g6KqQHdVSDfRKQBjUP+bjLW8Wh?=  
=?iso-8859-1?Q?XZJSgkpb0QhAe1A6EftfUYJN8gHR64pdHgVz07nt/8IC3DsFtBwL80JgbG?=  
=?iso-8859-  
1?Q?drLY7uMAK0Blva8T92pmmS96TQ7xqiywr3PeVfVhAzD5XSGSoO3c3cnA?=  
8859-1?Q?=3D=3D?= Content-Type: multipart/alternative;  
boundary="\_000\_VE1PR03MB5181A99DAB3000F3FD30F17083922VE1PR03MB5181eurp\_"  
MIME-Version: 1.0 X-MS-Exchange-Transport-CrossTenantHeadersStamped:  
PAXPR03MB7840 To: Undisclosed recipients;; Return-Path:  
bcom202445914@mylife.mku.ac.ke X-MS-Exchange-Organization-ExpirationStartTime: 02 Sep  
2024 08:20:55.1293 (UTC) X-MS-Exchange-Organization-ExpirationStartTimeReason:  
OriginalSubmit X-MS-Exchange-Organization-ExpirationInterval: 1:00:00:00.0000000 X-MS-  
Exchange-Organization-ExpirationIntervalReason: OriginalSubmit X-MS-Exchange-  
Organization-Network-Message-Id: 1516ab63-9f5a-454b-4b4e-08dccb282a76 X-  
EOPAttributedMessage: 0 X-EOPTenantAttributedMessage: 3c71cbab-b5ed-4f3b-ac0d-  
95509d6c0e93:0 X-MS-Exchange-Organization-MessageDirectionality: Incoming X-MS-  
Exchange-Transport-CrossTenantHeadersStripped:  
CO1PEPF000066EC.namprd05.prod.outlook.com X-MS-Exchange-Transport-  
CrossTenantHeadersPromoted: CO1PEPF000066EC.namprd05.prod.outlook.com X-MS-  
PublicTrafficType: Email X-MS-Exchange-Organization-AuthSource:  
CO1PEPF000066EC.namprd05.prod.outlook.com X-MS-Exchange-Organization-AuthAs:  
Anonymous X-MS-Office365-Filtering-Correlation-Id-Prvs: a54b3d24-6a89-48d8-2dee-  
08dccb282759 X-LD-Processed: 3c71cbab-b5ed-4f3b-ac0d-95509d6c0e93,ExtFwd X-MS-  
Exchange-AtpMessageProperties: SA|SL X-MS-Exchange-Organization-SCL: 5  
POTENTIAL\_SPAMPHISH: This message appears to be spam. X-Forefront-Antispam-Report:  
CIP:52.101.69.74;CTRY:NL;LANG:en;SCL:5;SRV:;IPV:NLI;SFV:SPM;H:AM0PR83CU005.o  
utbound.protection.outlook.com;PTR:mail-  
westeuropeazon11020074.outbound.protection.outlook.com;CAT:SPM;SFS:(13230040)(412319  
9012)(1032899013)(69100299015)(5063199012)(5073199012)(35042699022);DIR:INB; X-  
Microsoft-Antispam:  
BCL:0;ARA:13230040|4123199012|1032899013|69100299015|5063199012|5073199012|35042  
699022; X-MS-Exchange-CrossTenant-OriginalArrivalTime: 02 Sep 2024 08:20:54.5512 (UTC)  
X-MS-Exchange-CrossTenant-Network-Message-Id: 1516ab63-9f5a-454b-4b4e-08dccb282a76  
X-MS-Exchange-CrossTenant-Id: 3c71cbab-b5ed-4f3b-ac0d-95509d6c0e93 X-MS-Exchange-  
CrossTenant-AuthSource: CO1PEPF000066EC.namprd05.prod.outlook.com X-MS-Exchange-



CrossTenant-AuthAs: Anonymous X-MS-Exchange-CrossTenant-FromEntityHeader: Internet X-MS-Exchange-Transport-CrossTenantHeadersStamped: MW4PR02MB7297 X-MS-Exchange-Transport-EndToEndLatency: 00:00:09.8687795 X-MS-Exchange-Processed-By-BccFoldering: 15.20.7918.023 X-Microsoft-Antispam-Mailbox-Delivery: ucf:0;jmr:0;auth:0;dest:J;OFR:SpamFilterAuthJ;ENG:(910001)(944506478)(944626604)(920097)(930097)(3100021)(140003);RF:JunkEmail; X-Microsoft-Antispam-Message-Info: =?us-ascii?Q?vwFKTi4MXOGNDSJSH13PRJlzYCEmSwF8eS1wHyy2OXURJQXCARlhg+VjxbeM?= =?us-ascii?Q?HCURNsl0R16h0TSXLOrVFcwaAAAtyNf3AYCIHBBgAgzTLH4dtpwJ4mWq5hVBQ?= =?us-ascii?Q?EDKKB47eerE3B5ggXMdpI7cLvNn2GgTkzx7/FpQGYNAqdmKUtnGUjwOOvpp?= =?us-ascii?Q?albycYznw/TKvMnbPbL6RH6gdi5J1Y6T1ZnQzpiwSsEosvrwciUEDCgNRagL?= =?us-ascii?Q?uSH9v0wnEeFt59e1LRnTWesVeauVnrSO7tNbnU2rXIugOCNZdbOZqCACAc4k?= =?us-ascii?Q?c7Un2+AtZ7Bqs8qiOFACySXMWrVY/R2U3Ewehf/3ZdkIvfhLXrr8bNGk0JVx?= =?us-ascii?Q?EeiNIFCaBUg+eNIhORlbUaTTBADyoQULN4msno4NjUuuWcEShBXrd/+Cw5Ui?= =?us-ascii?Q?KxbRv1JjJnzFz8kLsOiGQqW19aDXGnGh5MHNN1YuklFqmlK0V/o1hVYw/J6t?= =?us-ascii?Q?kbqeCAF3kUxccGw+hbGNECr+Xwl3SkdD1aQRNP5nIAv+clo/VdkWoD/ycd2Q?= =?us-ascii?Q?eTjFQsyUFYG2B3tgqxs09EpAQDFLLBxjkEXx4+EaIDyBOqv92kg3/wrQvpIW?= =?us-ascii?Q?4Xq4cDAi4RrAPX2xBQKt2ZtqKHNDJws4Gew+hxnyMQccXZQgO9p0Mb3qrR0y?= =?us-ascii?Q?ZzwaqeK58L/be+ubv88tslRZ/xJLy3LA62q8/jcG0M3SPfVUWgqufAyKip+2?= =?us-ascii?Q?u+8p+y+10tZOQBPJ8IrOdH+5b99NIggPES+qPEovlNJkz3T3j4bHuYwKSpG8?= =?us-ascii?Q?w3MOrCwtH4NBq6Pd9O0xSTU236CMbwzSIO1gN5PnBJaDkKie2C9z/lp/YkaX?= =?us-ascii?Q?NLVmsKY5NDGK679Cec4nhgzKsQJkOLAltbfSVqpVgMvP1JL8jMm/ghzEdVO?= =?us-ascii?Q?RnjUm1PE2VsxQF9b7yOc/axieiKY7VfdOnnUicaK1bKpaeqQpmEigT1eY+dI?= =?us-ascii?Q?tVK6df6Lvz4CTm+v60c8Kchc0ocMGzY4/K5T9xcvC8uCdtsB+p9DjQsrD+IS?= =?us-ascii?Q?EWUwXOGx9YmxQx73fhSh1JxTMdWKEkBiDdj8e4l3bevYaG1cx5XxfFrFxfkZ?= =?us-ascii?Q?QX+qijmE8Wasg5P3luWvLFUyzayaKwPKI7sGcCRn3/vb/7rB/fJvnQSxeeRJ?= =?us-ascii?Q?fwRH5I3qgCy1uPd96v2hDhNQc0i7LJmKub8SO6Z6SImbGbRoHXQy4tmogAf?= =?us-ascii?Q?iU7Ykv5czxoOUTpy/tvMJZNZo8XuDq5fBKr0fDgoeaGNB1ZNJLoQGr08QoSA?= =?us-ascii?Q?fgiFb70WtwBjJRcZgCvceYVWEiopt7P93HzzCpvTuqvCs8ILXQymrqMjas4Z?= =?us-ascii?Q?KrFKOEZQ+aF4tU8WDEDED0kualhMUAGqMzBDQCpbimwoMeIVBaKqYp4fe5cfn?= =?us-ascii?Q?YrgV+j0Cf5mkKGG1qzpk1zHtZLLK9FmeRDHdXG2gqCSOZolHGQzw3SFnkzCX?

= =?us-  
ascii?Q?x7B2go02xaJgZScwkceJu0lXqrID5gu+w9GZr2XoDoDICGUSD4z/+Zcms0z9?= =?us-  
ascii?Q?py7JKTdtxZfb7o4U1B26r8a7hy8kLXQLvumVZYzBB8R1auNC/2d8DXGfsgBE?=  
=?us-  
ascii?Q?Rg9H7njYmVqiAn6PRCJvCgf/hWKX5CqTrnZVsrQ2xWSBo6rfVZKqt9ICCdwg?=  
=?us-  
ascii?Q?Bx8+EU8qsW2tu6P32wggvIgjP0NGOI+Lo0OUsaq1t/GSo7HvdZVcGSvH5eIO?=  
=?us-  
ascii?Q?MPJTnUoK+5Df2vCK84cJG389Z4oBSwBfyI7Ef+wtE/U98TE8xJE2+Fnhkw7J?=  
=?us-  
ascii?Q?SditOWx/aeUYza37w/t+hlUvcJUyRibVBfhU48OcQD+qwQRmN6KjAefuqm4d?=  
=?us-ascii?Q?qo9esKpJmpvx2HA/v2LGhQj7zk6GXXTIFSR+32sMuSkDtxkI++OpvIG9isyt?=  
=?us-ascii?Q?BvLgtIYOBxs3cj/pcjpRUx+Hyh5R2iHKdAtWSVe3Y6U1lYkxFtlujFYTiNwJ?=  
=?us-  
ascii?Q?Y0t6SbHvcXGqD/gBZy77wmx+vJFTVjZiR+/lP9odlY9p8+hPFWWI19uF0Gkx?=  
=?us-  
ascii?Q?U1MLeZBXeudnmYxFP5PnOoOj82/Shf+LCpv5ush+KpapIY3B6YmfuWO3XaCZ?=  
=?us-  
ascii?Q?YOrH/xjhxjh9Mn1uqIfgI8/xC0zNMovsNV6TFLUMp+KqxO/mUCwCLlwhQEtn?=  
=?us-ascii?Q?sXNvHVJcInftqzgdM3+bm6FkOeyk1ikqXqp29fhpO33IJH28G/9r0hi/54HI?=  
=?us-ascii?Q?caR0Qk+S6kui8l8nuJxXp5wUqgi04LUJTj4luP1vd78nnROoJpDNA5eeAbUJ?=  
=?us-  
ascii?Q?xt8zWFaUtk941lIFk54JH/3HC2FoVje+CQu4XkYNkZuowIHQJMNfBt5pGojM?=  
=?us-ascii?Q?znM6Yo/yTw0WUtZINKnpw4A/orrYbilAqF9riQFlAKqsZ2wFA6hsVC6Un6E/?=  
=?us-  
ascii?Q?+O+aMisgfw4KtwUXFV2cXMmwR9wVFcMhVJiTpjYReSQB8CtMlrzKRe9aqgJC?=  
=?us-  
ascii?Q?tKEJXBj5+XrmWW3H90bkPHvQo347qZTmBryUNazqDQ4CBH4pwmToB59E3k9N  
=? =?us-  
ascii?Q?X86B74H7xQ2i9i5OjlrO6ZNCXgB7dJIJNxstiTZP+/wjD8wnphfgQ+NABrF3?= =?us-  
ascii?Q?NPEtFFMqXRqeXNkaVR5pdNzoN/GkCf/FbdF84MGSi8gV7+5ejZYe8V9f5f4x?=  
=?us-  
ascii?Q?QRSuYcnSWw2gq+8Ve4wX0eUeky8NqyrB6DAk8fKXWehdgtvOaDp+ApLbNTNi?=  
=?us-ascii?Q?2qvkfjefzX7ee+GZo0dj/Wa6ATKlVGwZ7ATztUL8LYfYIcL9rntsezZZhHAU?=  
=?us-ascii?Q?J3o3JSFn07AsWimmeLALYPpW+OcXluk=3D?=-