Intro to Cyber Forensics Lab Grading Sheet

Project: Lab 5 – E-mail Forensics
Member Name: Alejandro Marin Arellano Member
Name: Christopher Bowen Member
Name: Terrence Scott Member
Name: Saehwan Park Member
Name: George Hendrick

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

Contents

1 Executive Summary **3**

2 Apparatus **4**

3 Laboratory Procedures **5**

3.1 Time-line / Log 5

3.2 Procedure 6

4 Problem Solving and Troubleshooting **17**

5 Conclusion and Recommendations **18**

6 References **19**

Appendices **19**

1 Executive Summary

The objective of this lab was to find evidence of AI Lagniappe's involvement using email files recovered for analysis. This process involved finding the incoming and outgoing correspondence related to the suspected crime. To do the email analysis, we used an online email analyzer called PhishTool. Analysis was done both automatically and manually.

Investigators began by opening each email in PhishTool and utilizing automatic analysis to find any warnings the program may find. The .eml file named: "Collaboration - Check This Out.eml" was the only file to automatically trigger warnings when analyzed.

On this file, SPF received a soft fail, as the IP address was detected to probably not be permitted to send emails on behavior of the lsu.edu domain, indicating the email is non-legitimate. DMARC tests also failed on this file. The authentication mechanisms weren't passed with an authenticated identifier in sufficient alignment from lsu.edu, further indicating the illegitimacy of this email being from the lsu.edu domain.

Investigators also found various signatures missing, most likely due to wiping. This is found in the .eml file "Collaboration - Check This Out" lacking a DKIM signature, and the .eml file "Hello + Collaboration (1).eml" lacking a SPF, DKIM, and a DMARC signature.

2 Apparatus

Table 1 lists the hardware and software used in this lab.

Table 1: apparatus of tools used in the image capture process

ITEM/PART	**MODEL NUMBER**	**VERSION**	**USAGE**
MSI Vector	GP66	Windows 11 PRO	Analyze evidence
PhishTool	n/a	n/a	Analyze Emails

3 Laboratory Procedures

3.1 Time-line / Log

Table 2: The log of all actions taken in the investigation

#	DATE	TIME (24hr)	ACTION TAKEN / INVESTIGATIVE LEAD
1.	03/09/2023	12:13	Downloaded email files to VM
2.	03/09/2023	12:14	Downloaded PhishTool and created account
3.	03/09/2023	12:18	Uploaded email files in PhishTool
4.	03/09/2023	12:19	Opened "Hello + Collaboration", gathered relevant information
5.	03/09/2023	12:20	Opened "Re: Hello + Collaboration", gathered relevant information
6.	03/09/2023	12:22	Opened "RE: Hello + Collaboration", gathered relevant information
7.	03/09/2023	12:24	Opened "Collaboration - Check This Out", gathered relevant information
8.	03/09/2023	12:26	Opened suspicious link in secure browser received in "Collaboration - Check This Out"
9.	03/09/2023	12:27	Used https://whatismyipaddress.com/ to locate the suspicious IP address found in "Collaboration - Check This Out"
10.	03/09/2023	12:30	IP found to be in Czechia

3.2 Procedure

Investigators began the investigation by downloading a copy of the emails collected from the crime scene. The investigators then used the online tool PhishTool to automatically analyze the four emails collected. The email chain began with Ibrahim Baggili(ibaggili@lsu.edu) emailing Super Rick(superrickml@gmail.com) at 4:51 pm, Mar 8th, 2023 (Figure 1). This email was confirmed to be sent by Ibrahim Baggili's account by the security checks of Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) (Figure 2). The email's content was asking for collaboration between the two. The follow-up email from superrickml@gmail.com, at 04:52 pm, Mar 8th, 2023, could not be confirmed if it was from Super Rick (Figure 3). The fields of SPF, DKIM, and DMARC were not supplied in the response (Figure 4). The content of the second email was accepting the ask for collaboration and setting up a meeting. The third email sent was from Ibrahim Baggili(ibaggili@lsu.edu) at 04:52 pm, Mar 8th 2023, confirming the collaboration and stating that Dr.Baggili would follow up (Figure 5). This email was confirmed to be sent by Ibrahim Baggili(ibaggili@lsu.edu) with SPF, DKIM, and DMARC (Figure 6). The fourth and final email was sent from ibaggili@lsu.edu to superrickML@gmail.com and was determined to be spoofed (Figure 7, 8). This final email sent at 04:55 pm, Mar 8th, 2023, had failed SPF and DMARC (Figure 9, 10). The email also did not have DKIM. After further investigation, Investigators found that the sender's ip of 89.187.129.27 originated from Czechia (Figure 11). The investigators noticed that in the spoofed email, there was a link to a malicious cite. The investigators used a secure browser to view the site and in figures 13-18, the site can be seen performing a malicious attack. The timeline of these events is shown in Figure 12. After automatic analysis of the emails, Investigators turned to viewing the source code for each associated email. Investigators were able to view the source of each of the emails using PhishTool's source tab. After manual inspection, investigators determined that the cause for the spoofed email not having DKIM was due to potential scrubbing.

Analysis / Hello + Collaboration

Hello + Collaboration

Headers | Received lines | X-headers | Security | Attachments | Message URLs

From	ibaggili@lsu.edu
Display name	Ibrahim Baggili
To	superrickML@gmail.com
CC	*None*
Timestamp	04:51 pm, Mar 8th 2023
Reply-To	*None*
Return-Path	ibaggili@lsu.edu
Originating IP	2a01:111:f400:7ea9::708 (Received-SPF)
rDNS	mail-sn1nam02on20708.outbound.protection.outlook.com

Figure 1: Header information of "Hello + Collaboration" email

Analysis / Hello + Collaboration

Hello + Collaboration

Headers | Received lines | X-headers | Security | Attachments | Message URLs

SPF

Result	PASS
Originating IP	2a01:111:f400:7ea9::708 (Received-SPF)
rDNS	mail-sn1nam02on20708.outbound.protection.outlook.com
Return-Path domain	lsu.edu
SPF record	v=spf1 ip4:130.39.6.0/24 ip4:130.39.4.0/24 ip4:96.125.27.69 include:spf.protection.outlook.com ~all

DKIM

Result	PASS
Verification(s)	1 Signature - 1 PASS
Selector	selector2._domainkey.lsu.edu (Signature 1 of 1)
Signing domain	lsu.edu
Algorithm	rsa-sha256
Verification	PASS

DMARC

Result	PASS
From domain	lsu.edu
DMARC record	v=DMARC1; p=none; pct=100; rua=mailto:re+sxs2k5mren9@dmarc.postmarkapp.com, mailto:secnotify@lsu.edu; sp=none; aspf=r;

Figure 2: Security information of "Hello + Collaboration" email

Analysis / Re: Hello + Collaboration

Re: Hello + Collaboration

Headers | Received lines | X-headers | Security | Attachments | Message URLs

From	superrickml@gmail.com
Display name	Super Rick
To	ibaggili@lsu.edu
CC	*None*
Timestamp	04:52 pm, Mar 8th 2023
Reply-To	*None*
Return-Path	*None*
Originating IP	*None*
rDNS	*None*

Figure 3: Header information of "Re: Hello + Collaboration" email

Analysis / Re: Hello + Collaboration

Re: Hello + Collaboration

Headers | Received lines | X-headers | Security | Attachments | Message URLs

SPF

Result	*None*
Originating IP	*None*
rDNS	*None*
Return-Path domain	*None*
SPF record	*None*

DKIM

Result	*None*
Verification(s)	0 Signatures
Selector	*None*
Signing domain	*None*
Algorithm	*None*
Verification	*None*

DMARC

Result	*None*
From domain	*None*
DMARC record	*None*

Figure 4: Security information of "Re: Hello + Collaboration" email

Analysis / RE: Hello + Collaboration

RE: Hello + Collaboration

Headers | Received lines | X-headers | Security | Attachments | Message URLs

From	ibaggili@lsu.edu
Display name	Ibrahim Baggili
To	superrickml@gmail.com
CC	*None*
Timestamp	04:52 pm, Mar 8th 2023
Reply-To	*None*
Return-Path	ibaggili@lsu.edu
Originating IP	2a01:111:f400:7eaa::729 (Received-SPF)
rDNS	mail-dm6nam11on20729.outbound.protection.outlook.com

Figure 5: Header information of "RE: Hello + Collaboration" email

Analysis / RE: Hello + Collaboration

RE: Hello + Collaboration

Headers | Received lines | X-headers | Security | Attachments | Message URLs

SPF

Result	PASS
Originating IP	2a01:111:f400:7eaa::729 (Received-SPF)
rDNS	mail-dm6nam11on20729.outbound.protection.outlook.com
Return-Path domain	lsu.edu
SPF record	v=spf1 ip4:130.39.6.0/24 ip4:130.39.4.0/24 ip4:96.125.27.69 include:spf.protection.outlook.com ~all

DKIM

Result	PASS
Verification(s)	1 Signature - 1 PASS
Selector	selector2._domainkey.lsu.edu (Signature 1 of 1)
Signing domain	lsu.edu
Algorithm	rsa-sha256
Verification	PASS

DMARC

Result	PASS
From domain	lsu.edu
DMARC record	v=DMARC1; p=none; pct=100; rua=mailto:re+sxs2k5mren9@dmarc.postmarkapp.com, mailto:secnotify@lsu.edu; sp=none; aspf=r;

Figure 6: Security information of "RE: Hello + Collaboration" email

Analysis / Collaboration - Check This Out

Collaboration - Check This Out

Headers | Received lines | X-headers | Security | Attachments | Message URLs

From	ibaggili@lsu.edu
Display name	Ibrahim Baggili
To	superrickML@gmail.com
CC	*None*
Timestamp	04:55 pm, Mar 8th 2023
Reply-To	ibaggili@lsu.edu
Return-Path	ibaggili@lsu.edu
Originating IP	89.187.129.27 (Received-SPF)
rDNS	emkei.cz

Figure 7: Header information of "Collaboration - Check This Out" email

Analysis / Collaboration - Check This Out

Collaboration - Check This Out

Headers | Received lines | X-headers | Security | Attachments | Message URLs

SPF

Result	SOFTFAIL
Originating IP	89.187.129.27 (Received-SPF)
rDNS	emkei.cz
Return-Path domain	lsu.edu
SPF record	v=spf1 ip4:130.39.6.0/24 ip4:130.39.4.0/24 ip4:96.125.27.69 include:spf.protection.outlook.com ~all

DKIM

Result	*None*
Verification(s)	0 Signatures
Selector	*None*
Signing domain	*None*
Algorithm	*None*
Verification	*None*

DMARC

Result	FAIL
From domain	lsu.edu
DMARC record	v=DMARC1; p=none; pct=100; rua=mailto:re+sxs2k5mren9@dmarc.postmarkapp.com, mailto:secnotify@lsu.edu; sp=none; aspf=r;

Figure 8: Security information of "Collaboration - Check This Out" email

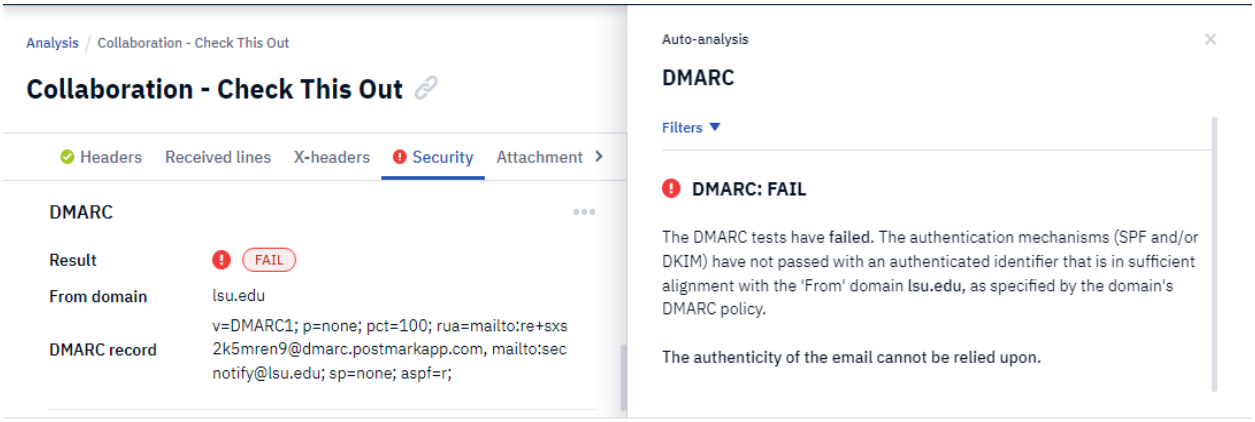

Figure 9: List of software used during the analysis

Figure 10: List of found data artifacts on suspect's VM

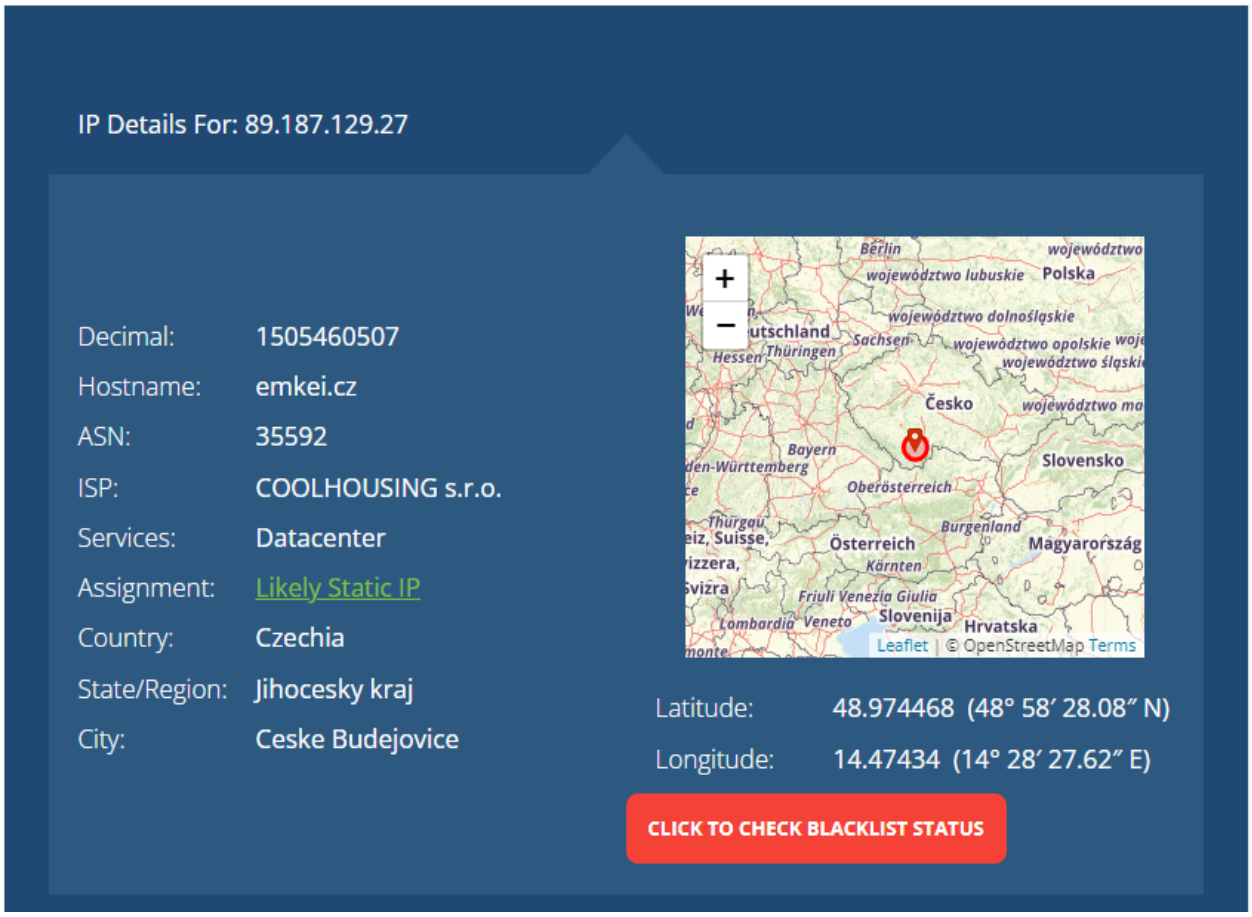

Figure 11: Location of the IP address that sent the spoofed email.

Figure 12: Timeline of emails.

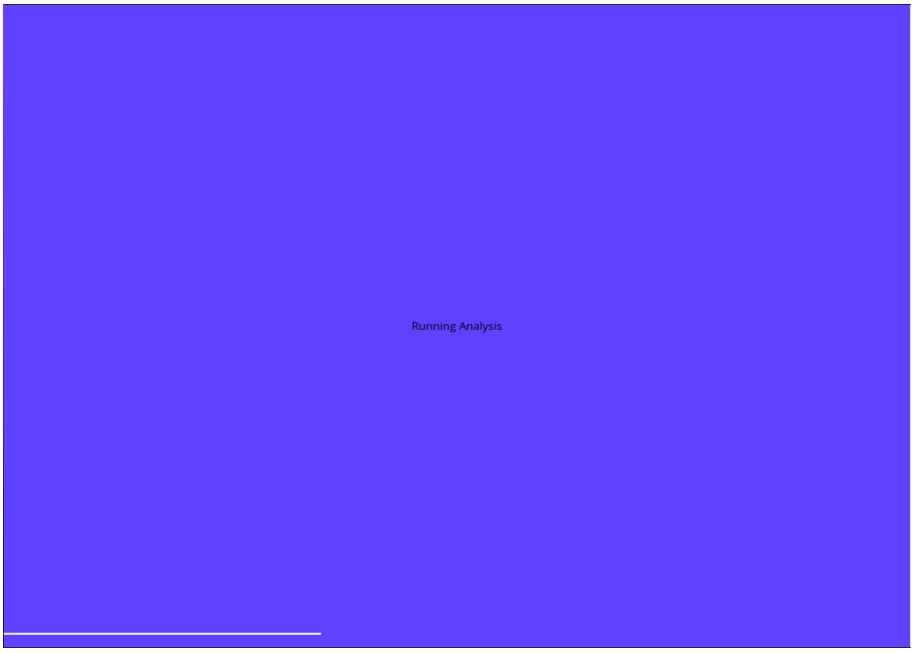

Figure 13: Image from the malicious website.

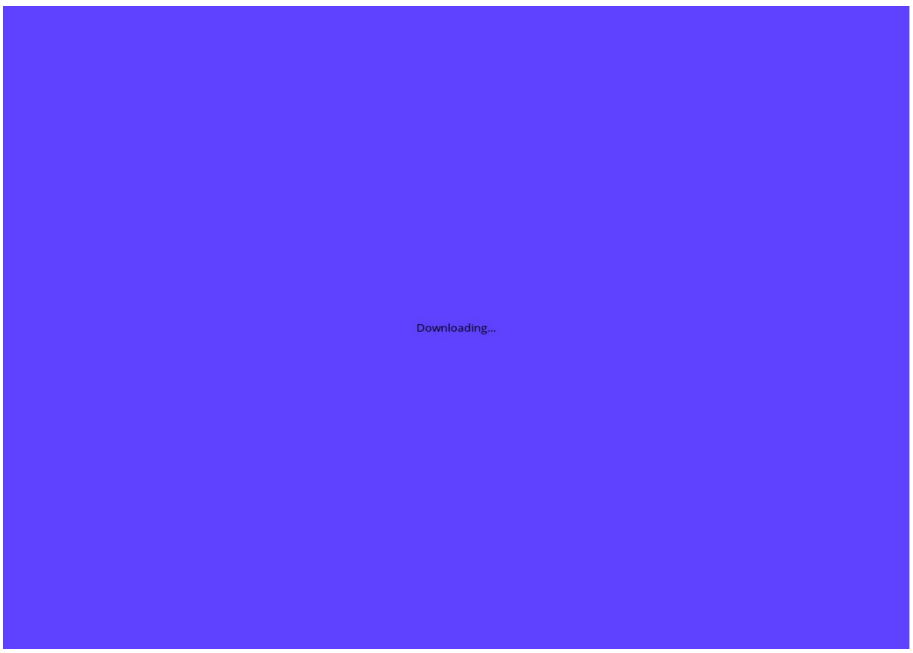

Figure 14: Image from the malicious website.

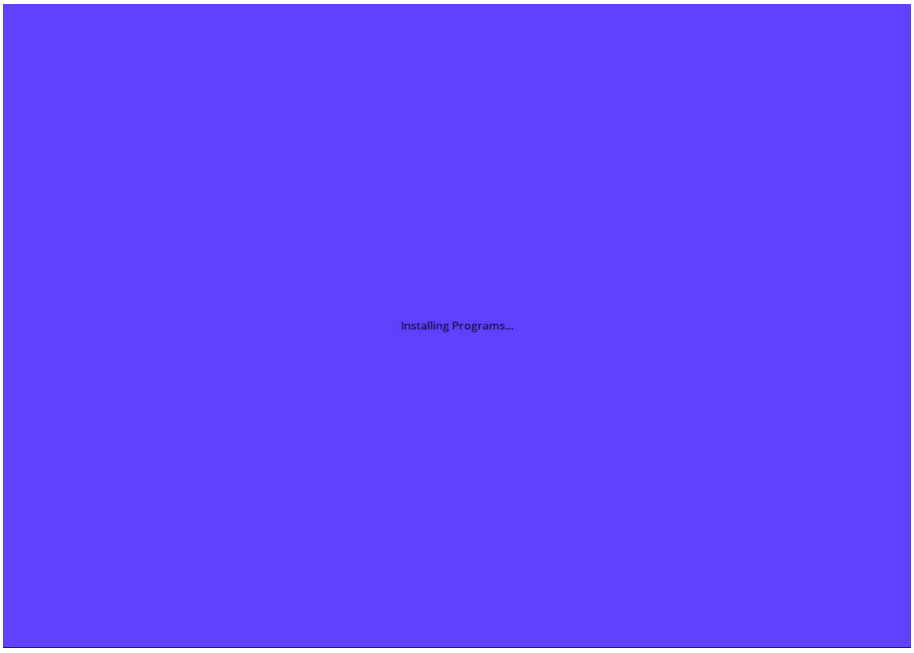

Figure 15: Image from the malicious website.

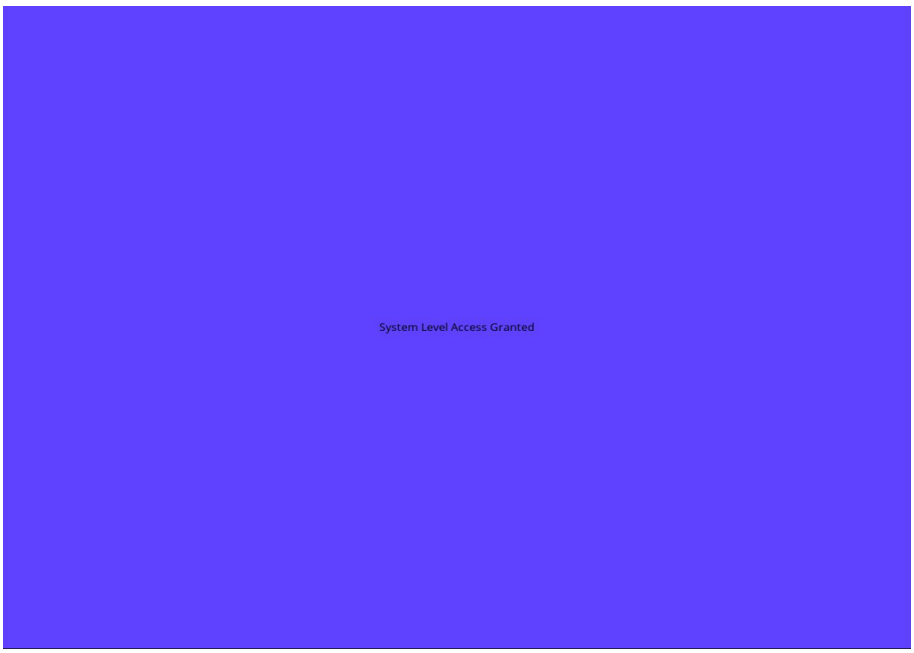

Figure 16: Image from the malicious website.

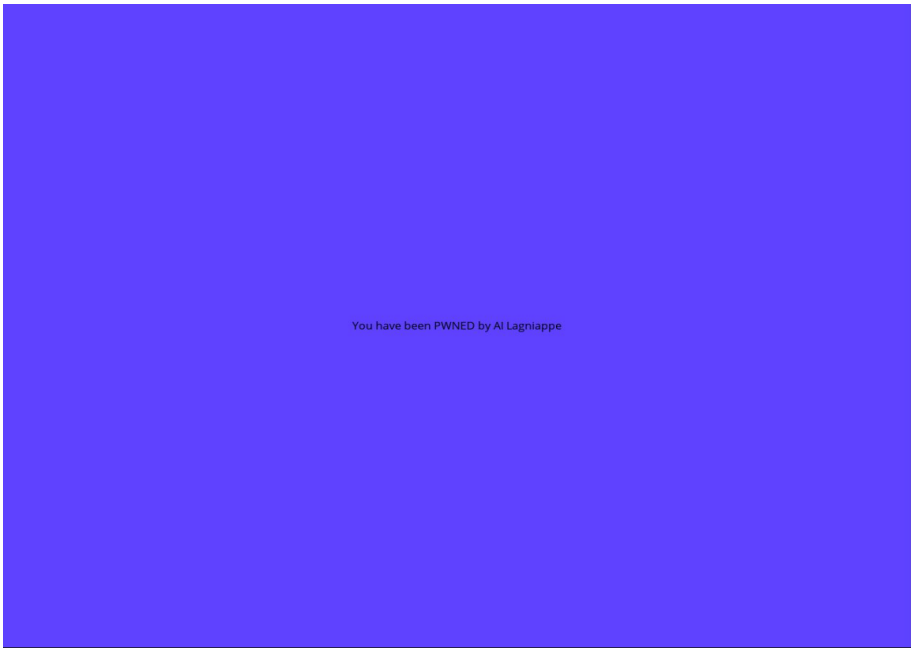

Figure 17: Image from the malicious website.

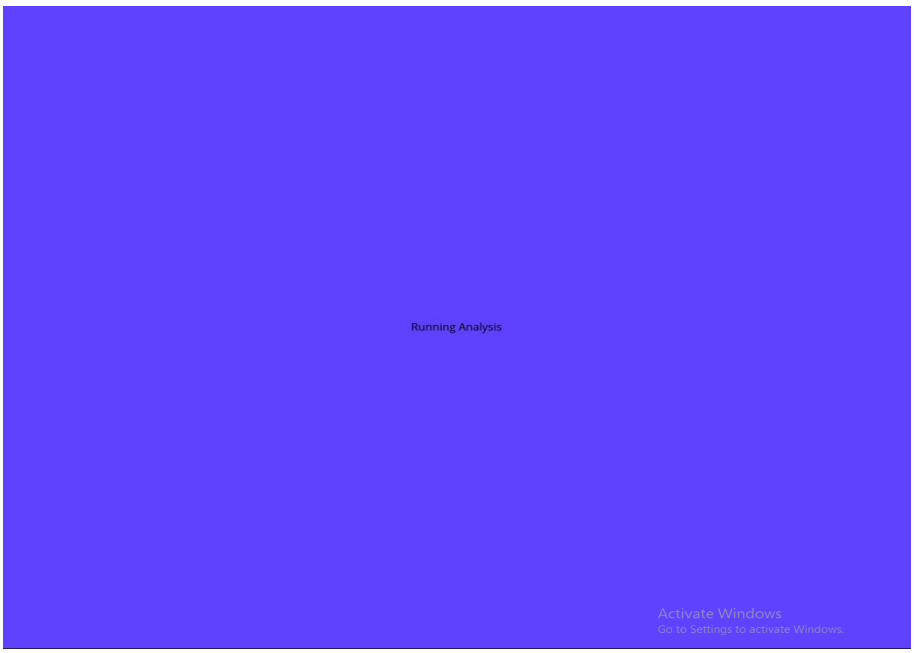

Figure 18: Image from the malicious website.

4 Problem Solving and Troubleshooting

Problem 1: The originating IP address of "Collaboration - Check This Out" was not identifiable.
Solution 1: Check if the IP address matched the originating addresses of the other emails.
Final Solution: Investigators used an IP locator to find where the email was spoofed from.

5 Conclusion and Recommendations

Investigators found that a malicious email was sent to Super Rick. The email was sent from a likely spoofed email source and a likely false IP address, as seen in Figures 9, 10, and 11, and had a malicious web page linked within. When investigators viewed this link using a secure browser, they saw there were images with text implying an attempt at attacking the computer the link was opened on, and downloading and installing files to the system, as seen in Figures 13-18. This exercise thus teaches not only to always investigates every part of an email for legitimate sourcing and identification, but also to safely investigate any links within potentially incriminatory emails.

As usual, standard procedures and safety precautions should always be followed during an investigation, as any suspicious link can cause severe issues in the investigation process. Improper handling of email evidence, especially from a likely illegitimate email, could damage a system, and improper searching could cause investigators to not find important evidence.

6 References

References

Appendices