

COLLEGE OF COMPUTER STUDIES AND MULTIMEDIA ARTS

**IT0203**

**(Digital Forensic Essentials)**

**EXERCISE**

**8**

**Email and Malware Forensics**

*"Dissecting Phishing Emails and Malware Artifacts"*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Student Name / Group Name:** | Raniel John Britos | |  | |
| **Members (if Group):** |  | **Name** | **Role** |  |
|  |  |
|  |  |
|  |  |
| **Section:** | TC23 | |  | |
| **Professor:** | Juan Paulo Magcuyao | |  | |

# Objective:

By the end of this lab, students will:

To analyze email headers and identify signs of phishing or malware delivery, and to examine basic malware behavior using a static analysis approach.

# Requirements:

# Sample phishing emails (in .eml or .txt format) with fake metadata and headers.

# Sample malware file (non-executable or obfuscated for safety, such as .txt version of a .exe or screenshots of code).

# Access to online tools:

# Email header analyzer (e.g., MXToolbox)

# VirusTotal (for checking file hashes)

**III. Overview and Orientation**

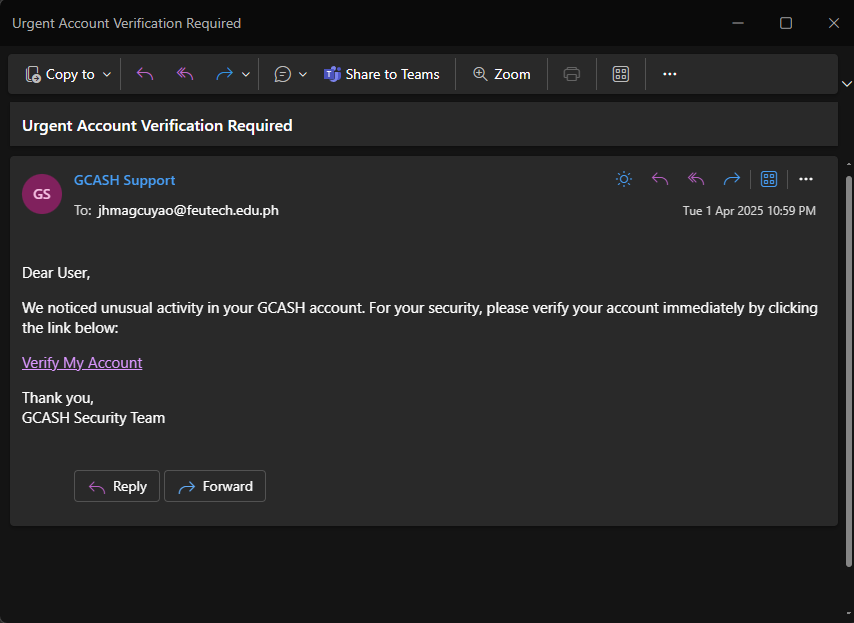
* **Email Forensics:** Analyzing email headers to trace origin, detect spoofing, or identify phishing attempts.
* **Malware Forensics:** Examining files or indicators of compromise to understand how malware behaves or is delivered.

**IV. Hands-On Activity**

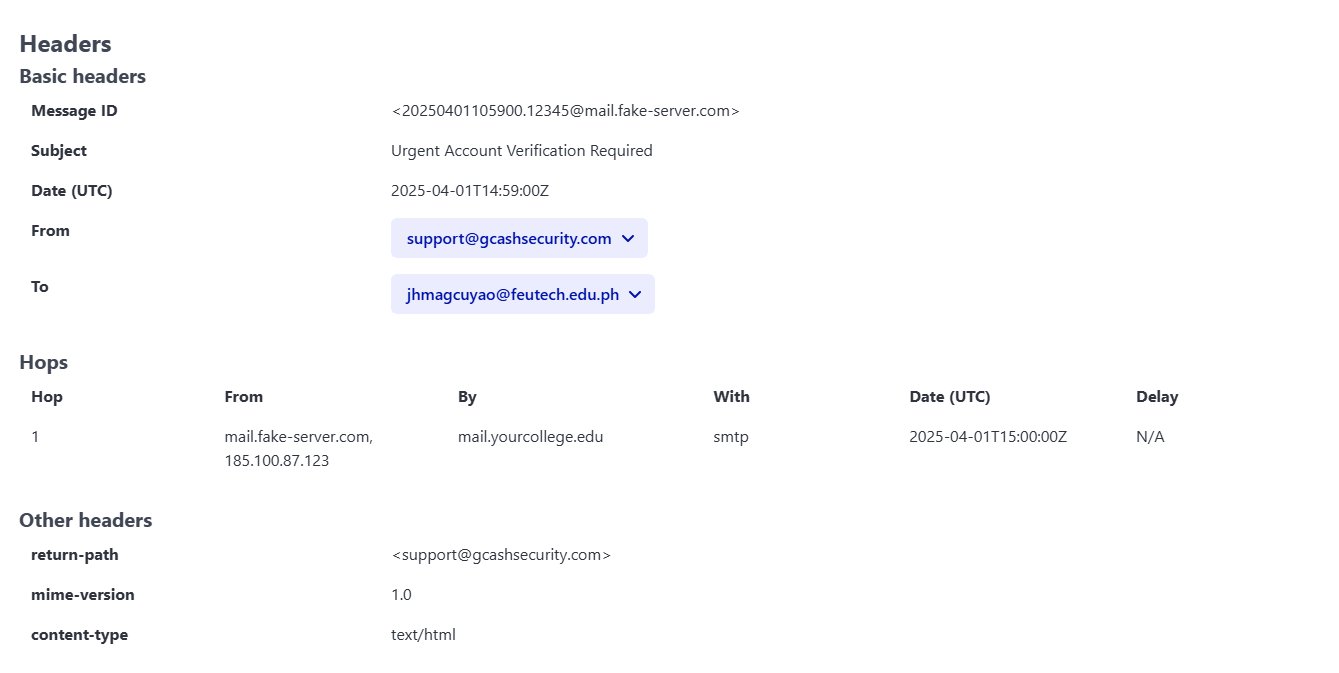
**Part 1: Email Header Analysis**

Instructions:

1. **Open the sample email file provided.**

****

1. **Use an email header analyzer tool to parse the raw header.**

****

1. **Identify:**
   * Sender’s real IP address

**Ans:** 185.100.87.123

* + Email source domain

**Ans:** mail.fake-server.com

* + SPF/DKIM/DMARC results (if available)
  + Any signs of spoofing or anomalies

**Ans:** Comes from a suspicious domain and no author signature

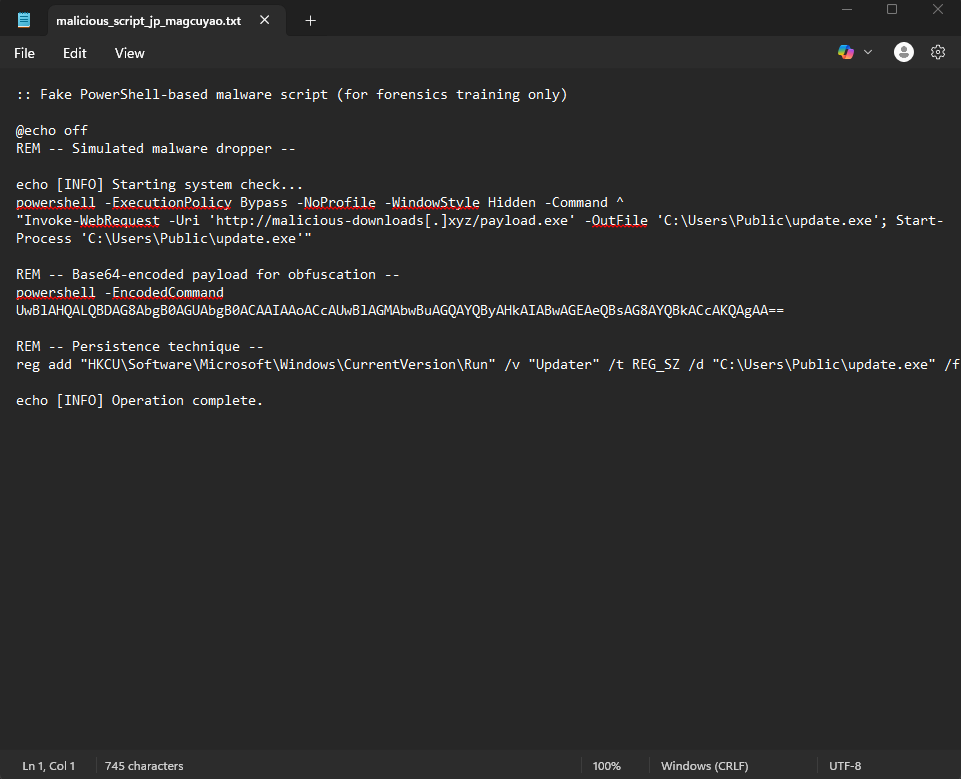
**Task:**  
Fill out the following fields in the worksheet:

* Sender's IP Address:
* Actual Sending Server:
* Spoofing Indicators (Yes/No and Why):
* Verdict: Is this email suspicious or safe?

**Part 2: Static Malware Artifact Analysis (10 minutes)**

**Instructions:**

1. **Open the sample malware artifact (a safe, obfuscated version or a code snippet). *(malicious\_script\_jp\_magcuyao.txt)***



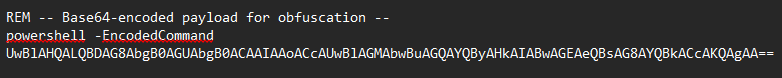
1. **Look for clues such as:**
   * Suspicious file names or extensions (e.g., .scr, .bat)

**Ans:** No suspicious file extensions out .exe files

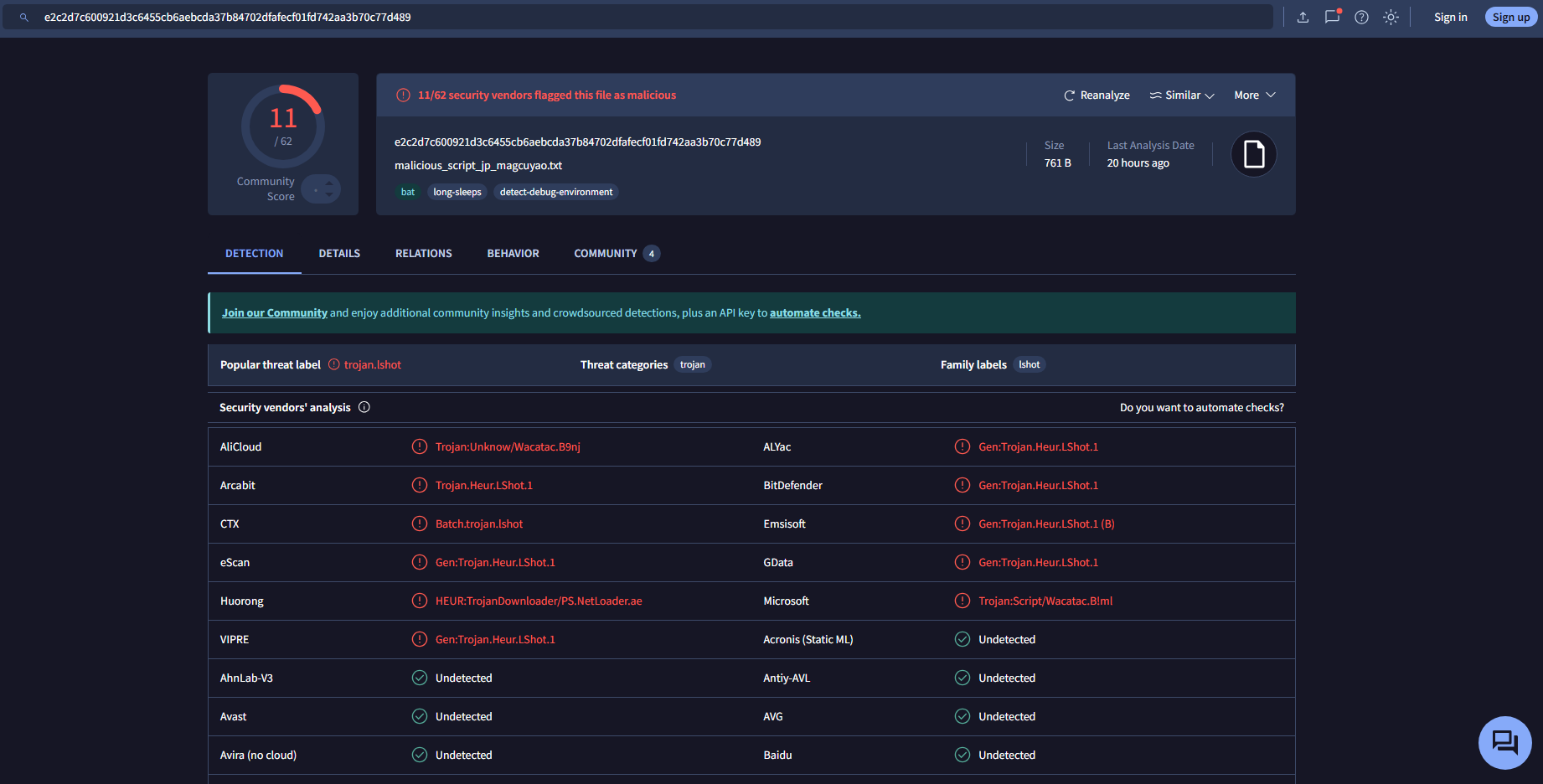
* + Embedded URLs or IP addresses



* + Use of PowerShell or Base64-encoded strings



**Optional:** Use a hash provided to search for the file on [VirusTotal.com].



**Task:**

* File name and type: malicious\_script\_jp\_magcuyao.txt
* One suspicious behavior or indicator: Base64-ecoded strings and embedded URL
* Does this file look malicious? Why? Yes, because it is replacing itself with the legit updater.exe built into windows and posing as it when run. This is evident with the file name and extension as well as registry editor line essentially adding itself as a legitimate program in the system

**3. Reporting Findings (5 minutes)**

Students will summarize both email and malware findings and give a short final verdict on what was discovered.

For the phishing email, a suspicious ip address and domain was found as well as a suspicious link attached to the message. Malware findings involved embedding itself to the system using windows registry editor as well as having embedded urls and base64-encoded strings.

**Worksheet Template**

**A. Email Forensics**

* Sender IP: 185.100.87.23
* Return Path Domain: support@gcashsecurity.com
* SPF/DKIM/DMARC Status: Not seen or available
* Suspicious? Why? Unknown domains and ip address and a suspicious link within the message

**B. Malware Forensics**

* File Name: malicious\_script\_jp\_magcuyao.txt
* Suspicious Code Snippet or Behavior: Base64-encoded strings, embedded URL, Registry Editor code
* VirusTotal Detection (if used): 11/62 vendors flagged as malicious
* Verdict: Harmless or Malicious? Malicious

Briefly explain how both the email and the malware could be linked in a real attack scenario.

**Key Red Flags in This Email:**

* **Fake domain** (gcashsecurity.com) pretending to be GCASH.
* **Received from suspicious IP**: 185.100.87.123 (commonly used by anonymizers).
* **Phishing link**: http://secure-gcash-login.com/verify — not a real GCASH domain.
* **Generic greeting**: “Dear User” (common in phishing emails).
* **Urgent tone** to trick the user into quick action.

# IV. QUESTION AND ANSWER

# (Minimum of 3 sentences each question)

1. Explain how digital forensic investigators analyze email headers and malware artifacts to trace the origin and intent of a cyberattack. In your response, describe key elements in an email header that may reveal phishing or spoofing attempts, and outline the basic techniques used in malware analysis (both static and dynamic).

**Ans:** To determine the origin and purpose of a cyberattack, digital forensic investigators examine malware artifacts and email headers. To identify indications of phishing or spoofing, they search email headers for important information such as the sender's IP address, the "From" and "Received" fields, and authentication results (SPF, DKIM, DMARC). They utilize dynamic analysis to run the malware in a secure environment and watch what it does, and static analysis to look at the code without running it, searching for unusual file or string behaviors. When combined, these actions aid in identifying the attack's origin, tactics, and objectives.

1. Discuss the role of email forensics in identifying phishing campaigns. What specific artifacts should a forensic examiner look for when analyzing suspicious emails, and how can these artifacts help link the email to a larger cybercrime operation?

**Ans:** By locating hints concealed in dubious emails, email forensics is essential in detecting phishing attempts. Fake sender addresses, odd URLs, deceptive topic lines, and unsuccessful SPF, DKIM, or DMARC tests are among the artifacts that a forensic examiner searches for. Additionally, they look for traceable routing paths and secret sender IPs in the email header. By exposing patterns such as shared servers, repurposed domains, or comparable email formats, these artifacts can link the email to a more extensive, well-planned cybercrime scheme.

1. Malware is often used as a delivery tool in email-based attacks. Explain how forensic investigators can safely examine suspicious files attached to emails. Include a comparison between static and dynamic analysis and discuss when each method is most appropriate.

**Ans:** To prevent the spread of possible virus, forensic investigators use secure, regulated environments to investigate dubious email attachments. Static analysis, which is helpful for brief, secure overviews or when execution is too risky, entails looking at the file without running it to look for code patterns, file structure, or embedded strings. When static approaches are insufficient, dynamic analysis is the best option. It entails executing the file in a secure environment to observe its actual behavior, such as file modifications or network activities. Both techniques reduce the chance of infection while assisting investigators in understanding the intent, source, and possible effects of the virus.

**VIII. REFERENCES**

**EC-Council. (n.d.). *Digital Forensics Essentials (DFE) courseware*. EC-Council.** [**https://www.eccouncil.org**](https://www.eccouncil.org)