ELECTIVE-III

DIGITAL FORENSICS AND INCIDENT RESPONSES

MINI-PROJECT REPORT

Project Title: Email Analysis

By

Navya Peram PES1UG21CS924

Namita Patil PES1UG21CS357

Navaneetha N PES1UG21CS365

Contents

○ Abstract:

Our project focuses on developing an advanced email analysis tool to enhance email security. The tool offers features such as header analysis for detecting phishing attempts, content analysis for identifying suspicious content, and attachment analysis for detecting potentially malicious files. It also integrates sender reputation analysis and threat intelligence feeds to provide real-time updates on emerging threats. With a user-friendly interface, our tool aims to empower users to make informed decisions and mitigate the risks associated with email-based threats.

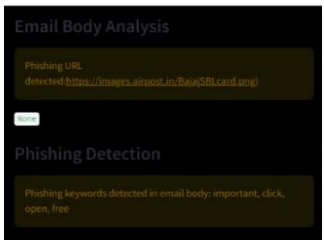
○ Problem Description:

Email communication is a cornerstone of modern communication, yet it is increasingly targeted by malicious actors through techniques like phishing and malware distribution. Existing email security measures often fall short in detecting sophisticated threats, leaving users vulnerable to data breaches and financial losses. Moreover, users may lack the tools and knowledge to assess the legitimacy of incoming emails effectively. Thus, there is a pressing need for an advanced email analysis tool that can comprehensively evaluate email headers, content, and attachments to identify potential threats and provide users with real-time updates on emerging cybersecurity risks. By empowering users to make informed decisions and mitigate email-based threats, such a tool can significantly enhance overall email security posture and protect against cyber-attacks.

○ Implementation:

1. Header Analysis: Extraction and analysis of email headers to identify suspicious patterns, inconsistencies, and potential indicators of phishing or spoofing attempts.

2. Content Analysis: Examination of the email body for phishing keywords, suspicious URLs, and other indicators of malicious intent. Utilization of machine learning-based summarization techniques to provide users with concise summaries of email content.



3. Attachment Analysis: Detection and analysis of email attachments to identify potentially malicious files using advanced threat intelligence feeds.

4. Sender Reputation Analysis: Evaluation of sender reputation by querying external threat intelligence sources and analyzing sender IP addresses extracted from email headers.

5. Threat Intelligence Integration: Integration with external threat intelligence feeds to provide users with real-time updates on emerging threats and trends in the cybersecurity landscape.

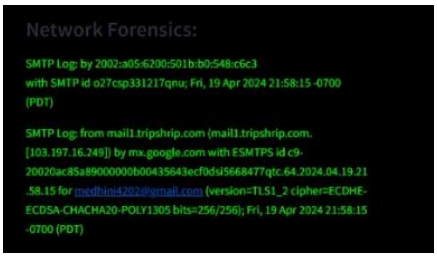
6. User-Friendly Interface: Implementation of an intuitive and user-friendly interface for seamless navigation and interaction with the email analysis tool.

7. Compliance Checks: Implement checks for compliance with email security standards such as DMARC, DKIM, and SPF to verify email authenticity and reduce the likelihood of spoofed emails.

8. Network Forensics:

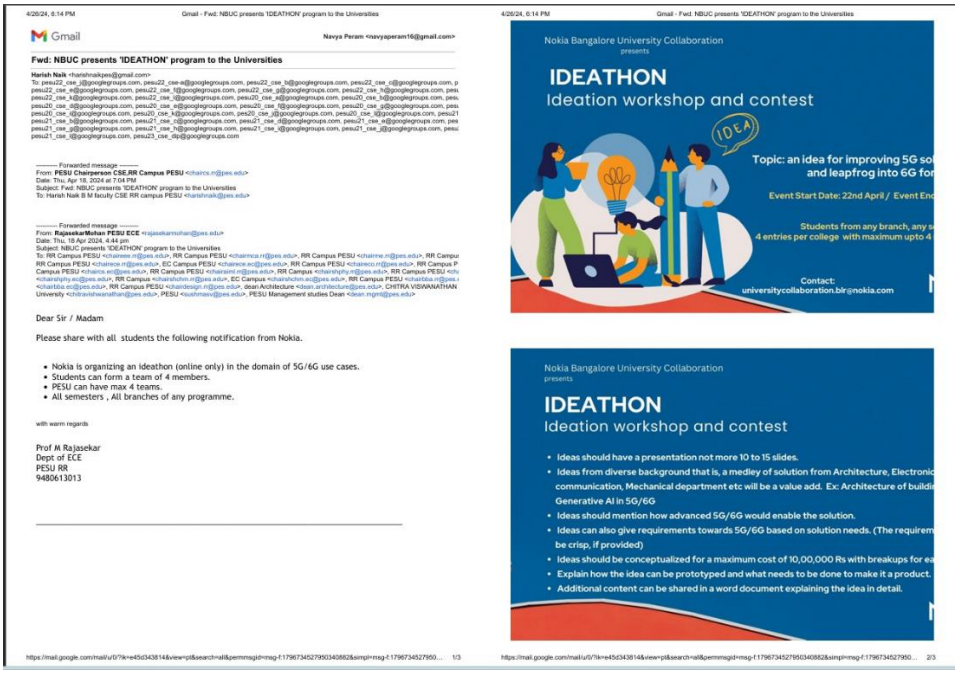
   - Analyze network traffic associated with the email transmission, including SMTP (Simple Mail Transfer Protocol) logs, email server logs, and firewall logs.

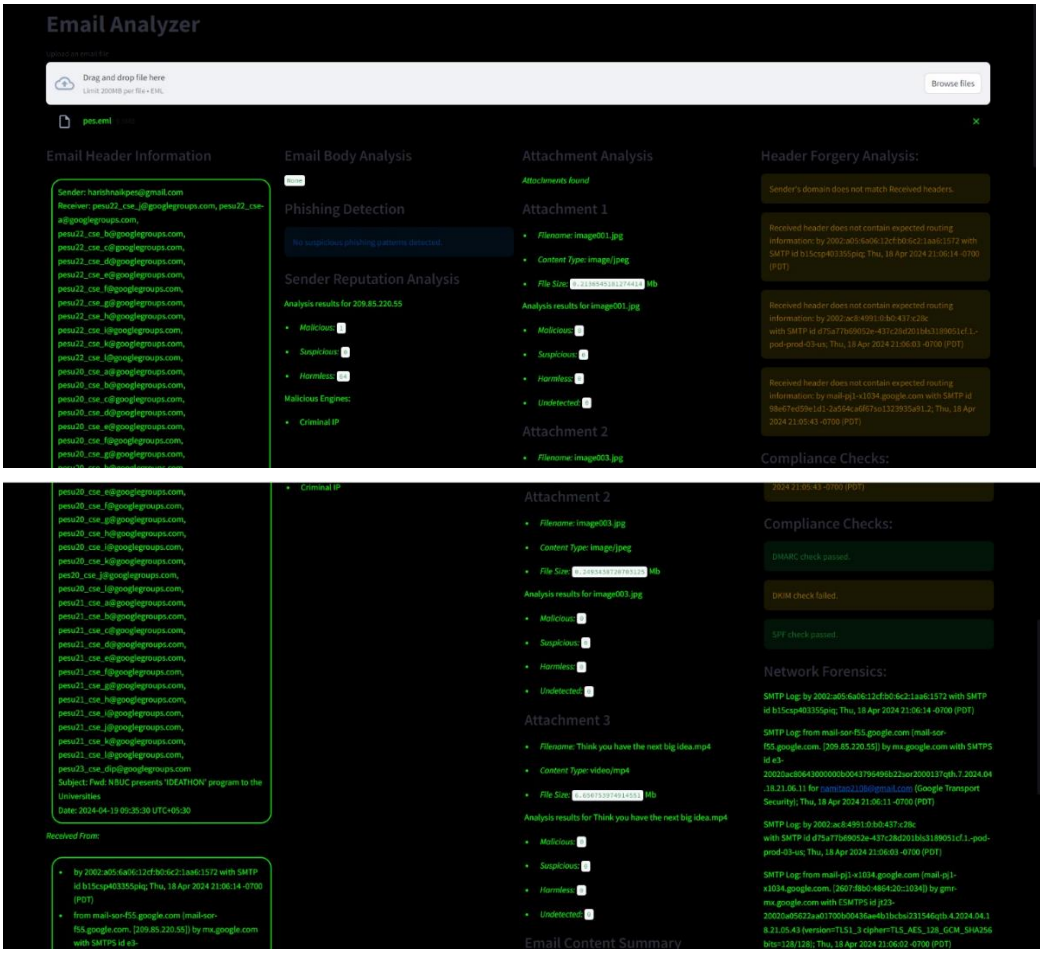
   - Look for suspicious patterns or anomalies in the network traffic that may indicate malicious activities, such as unusual email attachment sizes, multiple failed delivery attempts, or connections to known command-and-control servers.

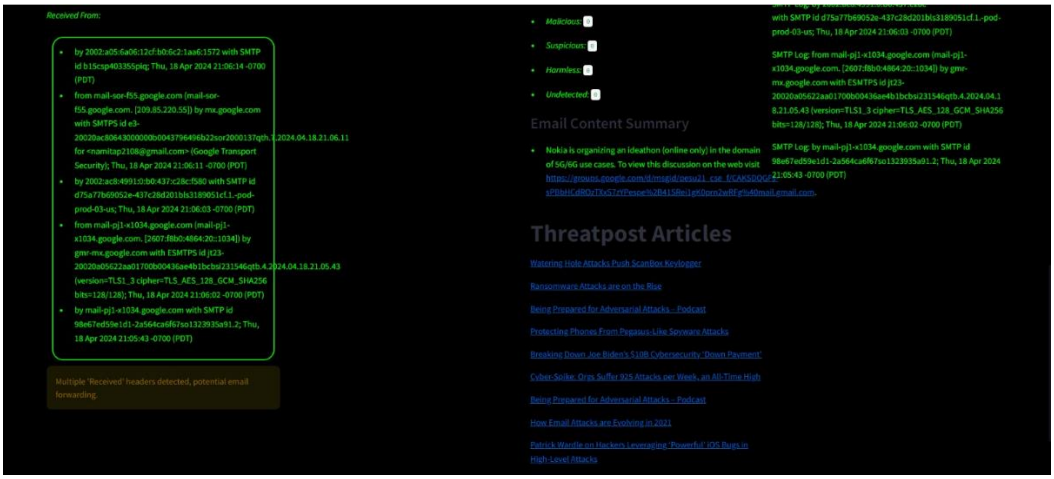


○ Results:

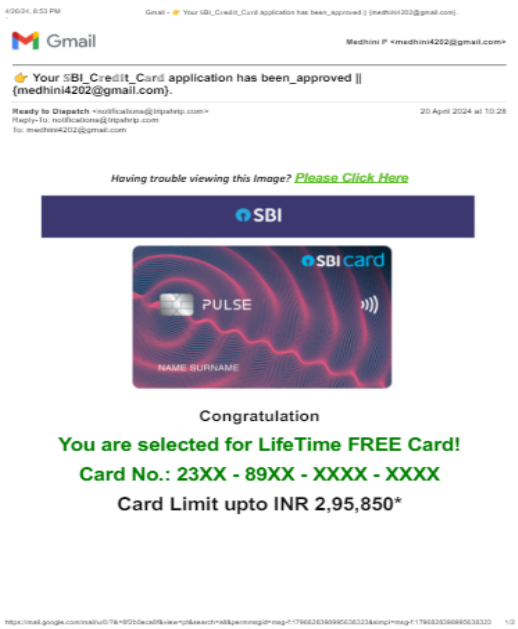
1. No suspicious content

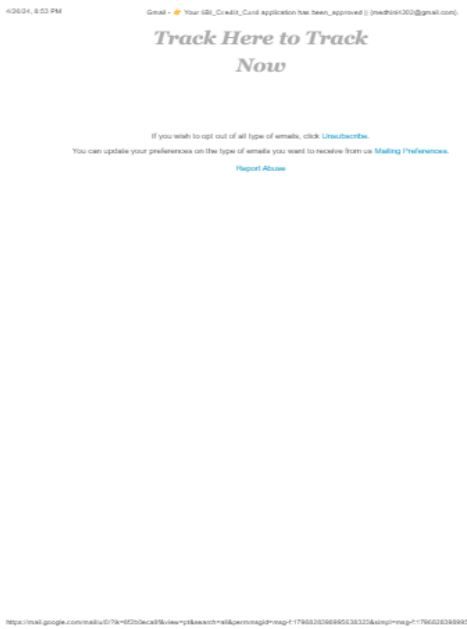


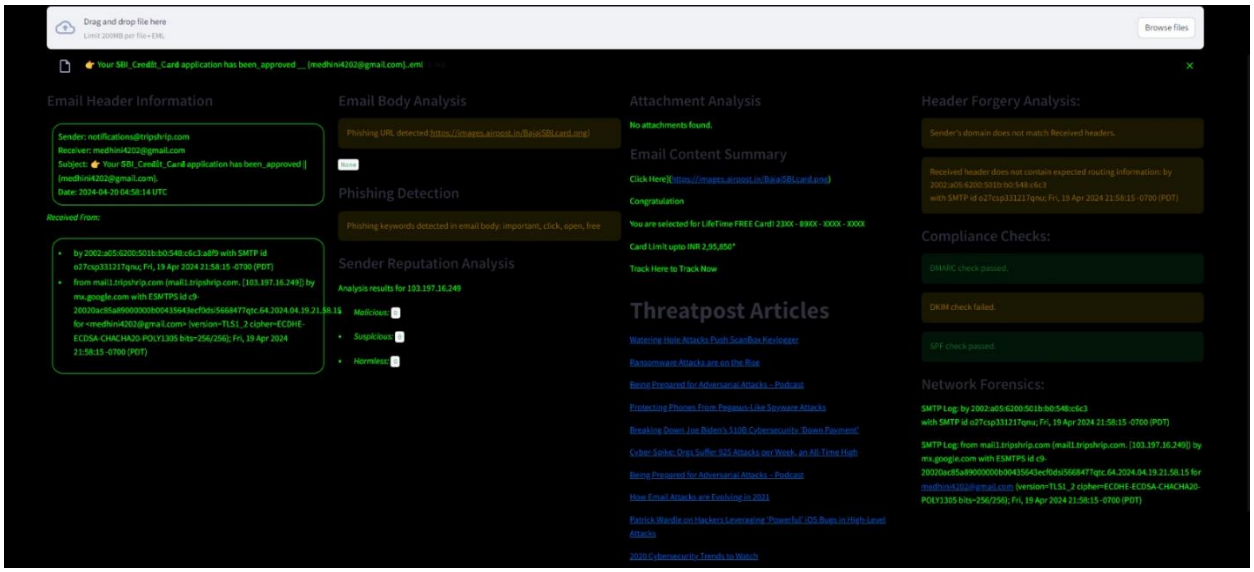


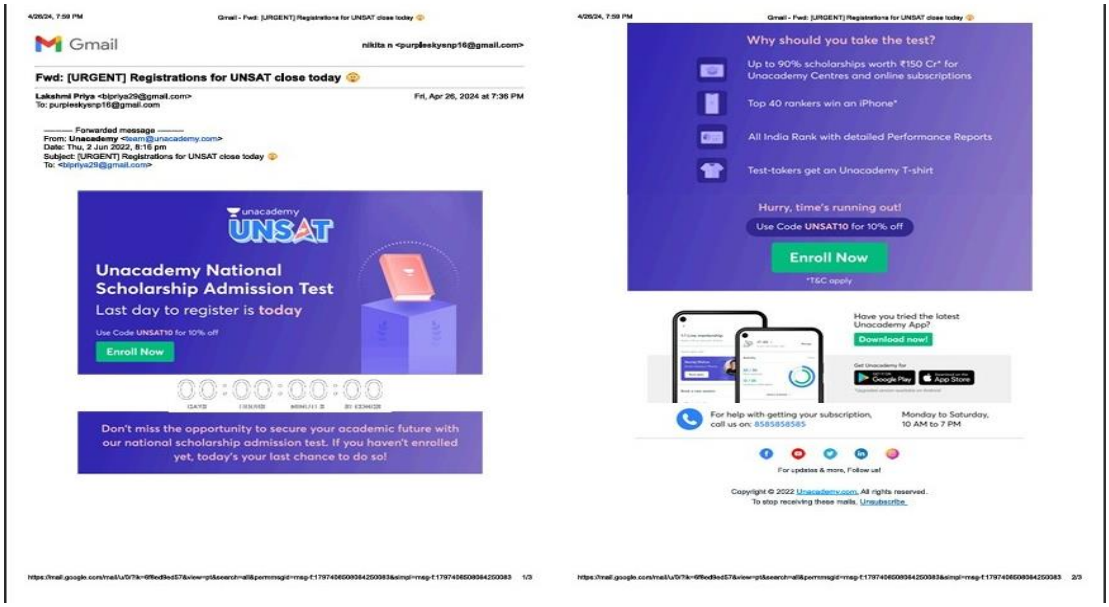


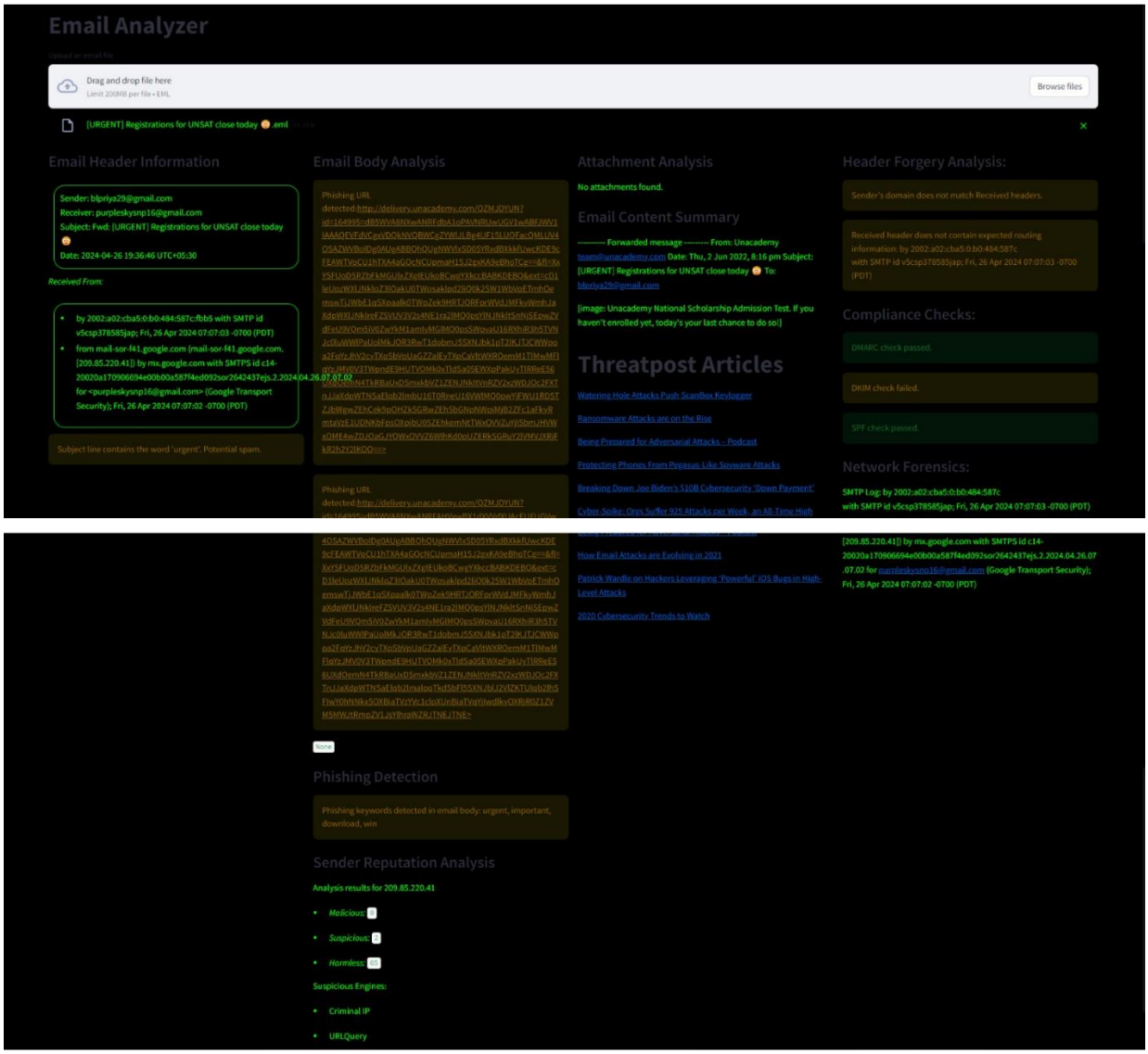
2. Detected phishing content








Gmail
Fwd: [URGENT] Registrations for UNSAT close today
Unacademy National Scholarship Admission Test
Last day to register is today
Enroll Now
Why should you take the test?
Up to 90% scholarships worth ₹150 Cr* for Unacademy Centres and online subscriptions
Top 40 rankers win an iPhone*
All India Rank with detailed Performance Reports
Test-takers get an Unacademy T-shirt
Hurry, time's running out!
Use Code UNSAT10 for 10% off
Enroll Now
*T&C apply


Email Analyzer
Drag and drop file here
Browse files
[URGENT] Registrations for UNSAT close today .eml
Email Header Information
Email Body Analysis
Attachment Analysis
Header Forgery Analysis:
Email Content Summary
Threatpost Articles
Compliance Checks:
Network Forensics:
Phishing Detection
Sender Reputation Analysis

○ Conclusion:

The experiment conducted with our email analysis tool yielded promising results, showcasing its efficacy in enhancing email security and mitigating the risks associated with email-based threats. By analyzing email headers, content, and attachments, the tool successfully identified phishing attempts, malicious content, and suspicious sender behavior. Additionally, integration with real-time threat intelligence feeds provided users with timely updates on emerging cybersecurity risks, enabling proactive defense against potential threats. Overall, the experiment underscores the value of our email analysis tool in empowering users to make informed decisions and bolstering email security posture.

Recommendations for Future Use/Development/Behavior:
Looking ahead, it is imperative to continue refining and advancing the capabilities of the email analysis tool to address evolving email security challenges effectively. This entails further optimization of threat detection algorithms, expansion of threat intelligence integration, and enhancement of user interface and usability aspects. We can enable continuous monitoring and analysis of email traffic for detecting and responding to security threats or anomalies in real-time. To achieve this, enhancing authentication mechanisms such as IMAP (Internet Message Access Protocol) or OAuth (Open Authorization) authentication could be crucial. IMAP authentication could be improved to provide better integration with real-time monitoring systems, allowing for seamless access to email data streams for analysis purposes. Similarly, leveraging OAuth authentication, which provides secure, token-based access to email accounts, could enhance the security and reliability of real-time monitoring systems by ensuring proper authorization and access control.
Moreover, ongoing user education and training initiatives are essential to ensure widespread adoption and effective utilization of the tool across various user demographics. By prioritizing continuous improvement and user engagement, our email analysis tool can serve as a crucial asset in safeguarding against email-based threats and promoting a secure email communication environment.

○ Appendix:

Sample Email Files: Gmail

External Libraries and APIs: VirusTotal, Streamlit, BeautifulSoup, Bert, Email, Summarizer, Requests, Html

Contribution:

1. Namita Patil – Email header information, Attachment analysis, Sender reputation analysis
2. Navya Peram – Email body analysis, Phishing detection, Email content summary, Threatpost articles
3. Navaneetha N- Header forgery analysis, Compliance checks, Network forensics

References: https://docs.streamlit.io/, https://docs.python.org/3/library/email.html, https://www.crummy.com/software/BeautifulSoup/bs4/doc/, https://docs.python-requests.org/en/latest/, https://docs.python.org/3/library/html.html, https://developers.virustotal.com/v3.0/reference.