**Smart India Hackathon 2017** is a pan India 36 hour nonstop digital programming competition. The participating teams simultaneously compete from across 33 locations in India to offer digital yet sustainable innovative solutions to solve real time challenges faced by the nation. 29 Ministries of India had given 598 problem statements. Shortlisted from 42,000 students (7000 teams) of 2,183 engineering and management colleges and universities from across India, 1,266 teams worked nonstop for 36 hours to build products based on their ideas across 26 locations in India during the ‘Grand Finale’ of ‘Smart India Hackathon 2017’ April 1st and 2nd, 2017.

The team Technofreak from Sri Krishna College of Technology, Coimbatore, Tamil Nadu submitted their solution proposal for the problem statement on Email spoofing posted by the Ministry of External Affairs, Government of India. The problem statement was a follows.

**“Spoofed email with Swapped Email ID (and IP too) can come to any user’s inbox. Suggest a mechanism to filter the spoofed email at server side”**

The solution proposal was accepted and the team was selected as one among the 1266 teams across India who would be participating in the nation-wide hackathon which was to be conducted on 1st and 2nd of April 2017. The team had to submit the nomination for their mentors who would be guiding the team for preparation, research, planning and implementation. They had a choice to request an academician and one industry expert as their mentor. The team requested, Dr. A. Jameer Basha, Head, Department of Information Technology, Sri Krishna College of Technology, Coimbatore, Tamil Nadu to be their Academic Mentor. For the industry mentor, with the help of the faculty, the team request Arun Thundyill Saseendran, Software Development Engineer, DELL EMC, Bangalore who is an Alumni of the college to be the mentor. On acceptance from both the mentors, the final Technofreakz team with the student members as <Name of the students> and the mentors as Dr. A. Jameer Basha and Arun Thundyill Saseendran were formed.

Over the course of one month preparation, the **Technofreakz** team started the first week with deep research on the problem statement, the way the attack is being conducted, the impact of email spoofing attacks, current protocols and solutions which help in detection of email spoofing and the products that are available in the market that help mail servers detect and prevent email spoofing. As a result of the research work conducted by the team and analysis by the mentors, the team came up with the following learnings.

* SPF (Sender Policy Framework) and DKIM (Domain Keys Identified Mail) are the two protocols primarily available in the market for spoof detection.
* There exists a protocol called DMARC (Domain Message Authentication Reporting and Conformance) which in simple terms is a combination of SPF and DKIM.
* There are very less or no open source products available in the market that implements DMARC.
* There is not even one Indian product which provides immunity for email servers against email spoofing attacks.
* The available protocols such as SPF and DKIM are network and DNS (Domain Name Server) dependent. Hence when there is a mail flood there can arise a network congestion and affect the performance of the mail servers.
* There are billions of dollars lost every years even in well-established corporates and MNCs who employ the state of the art mailing servers.
* Apart from monetary lute, email spoofing was being used in a large way as a cyber warfare mechanism for retrieval of vital confidential information.

Having had a strong understanding of the problem statement and the knowledge acquired about email spoofing, the team progressed to the second week of preparation trying to study the infrastructure used by the Ministry of External Affairs for email server. By employing various white hat tricks the team understood the use of Oracle Messaging and Communications server with Covergence Web Mail being used by the National Informatics Center for email server. <Sensitive information, hence can be removed after discussion>. The team studied in detail the architecture of the email server used by the Ministry of External Affairs so as to build a product that can be easily integrated into it.

The third week of preparation was to explore and discover an open-source mail server that had a similar architecture as the proprietary mail server used by the National Informatics Center as email server. Based on the details exploration and comparative architecture study, the team identified Apache James Email server which is architecturally same as the proprietary third party mail server used by the National Informatics Center for providing email communication services to the Ministry of External Affairs.

The last week of preparation was rigorous where the team brainstormed on the various way that can be employed to detect spoofed emails. The team conducted a detailed study on the raw MIME (Multipurpose Internet Mail Extensions) – the format the email server send and receive email, and the various fields in the MIME format that can be exploited to design algorithms that can scale and is efficient in terms of memory, CPU and network usage.

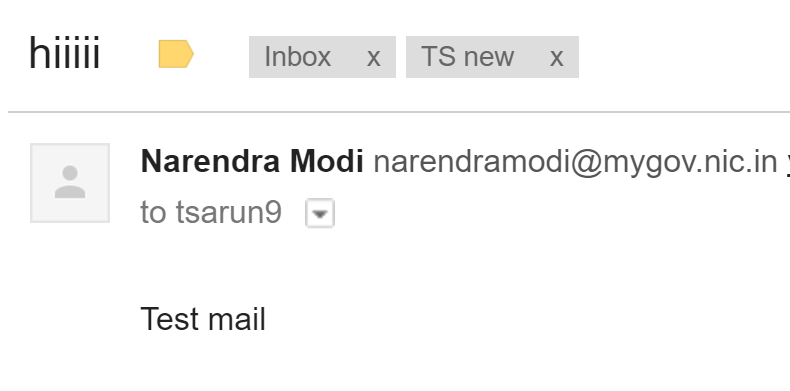
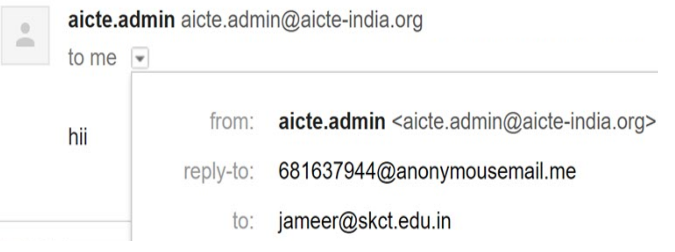


After for weeks of research and understanding, the team set out to New Delhi Institute of Management, New Delhi – the institution that was selected as the nodal center for the Smart India Hackathon 2017, for all the teams who had proposed solutions and selected for the Grand Finale by the Ministry of External Affairs.

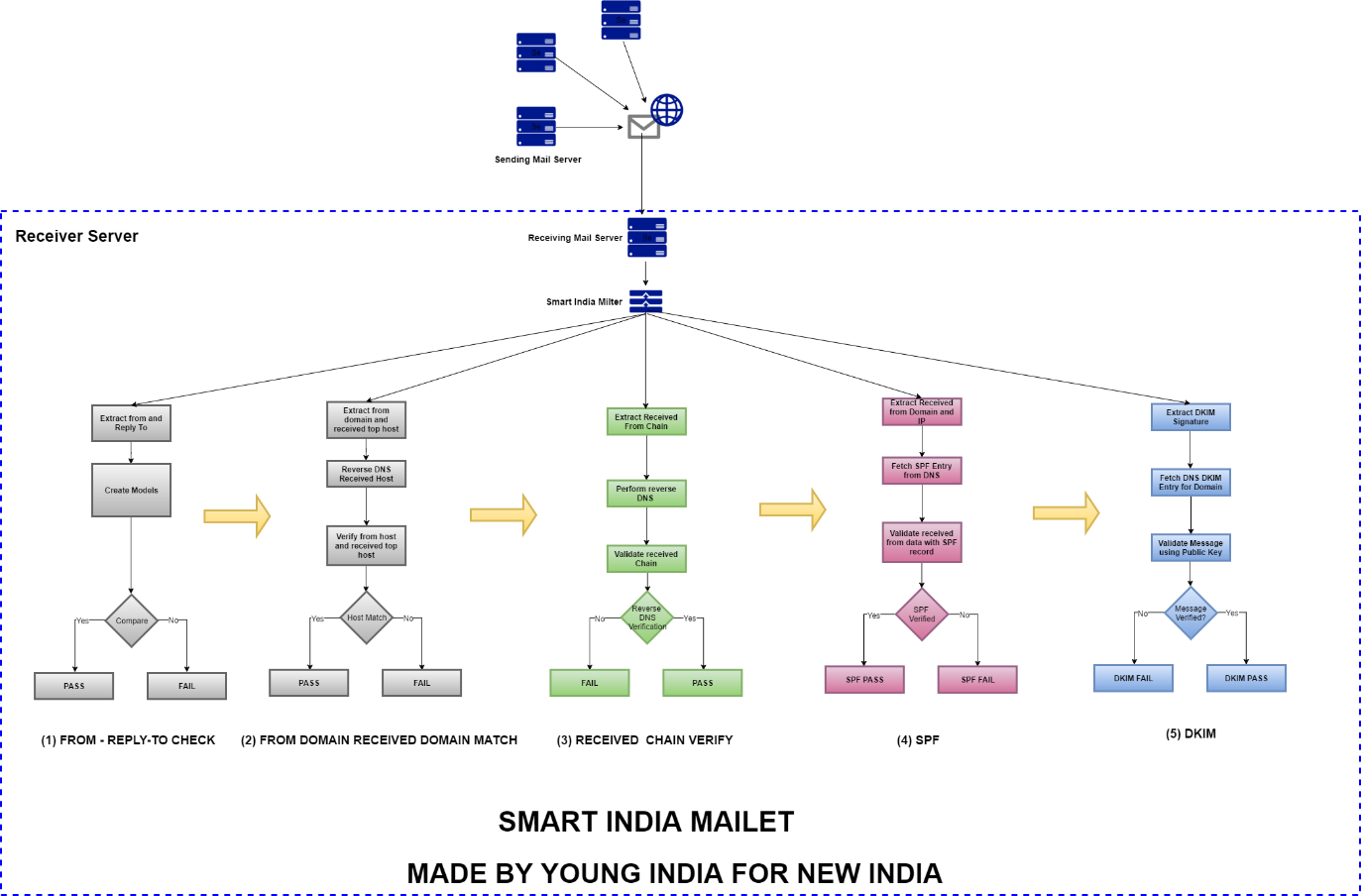
The team reach the venue of the competition on 31st Mar, 2017 and completed the registration and were allocated rooms. It was a silent day where the team kept their mind calm to liberate their complete potential.

On 1st April, 2017, 7.30 AM the team took part in the inauguration ceremony where the world witnessed it’s one of a kind event, the world’s biggest hackathon. After the inauguration ceremony, the team assembled at the places allocated for them and began the art of coding and product development with the rich knowledge of research and preparation done in the past month. The team also set up their own LAN (Local Area Network) to work collaboratively and connected all their workstations to the LAN. The event was well organized and the there were periodic short mentoring and assessment by technical experts from the Ministry of External Affairs and leading experts from Information Technology and Cyber Forensics.

The team started of the show by conducting a spoofing attack in a controlled way in which they sent mails to five nodal centers with spoofed email claiming to be the AICTE and from the email ID [aicte.admin@aicte-india.org](mailto:aicte.admin@aicte-india.org) and asking a set of five questions including one minor financial detail. The team quickly got its first kill when one of the nodal centers replied back with the required details. The team also went ahead and send a spoofed email to one of the jury members from the ministry of external affairs from the email ID [narendramodi@mygov.nic.in](mailto:narendramodi@mygov.nic.in). The email reach the inbox of the jury person’s Ministry of External Affairs Inbox and he opened the mail in front of the team and accepted that the spoofed email has reached their inbox without any trouble. The point to note here is that team did not develop a custom server for sending spoofed emails. Rather they made use of third party tools to do this. This attach demo proved that email spoofing was easy and can be done with minimal effort and if done by professional hackers, the damage caused can be catastrophic.



Having made the people understand the need for an indigenous product to detect and prevent spoofed emails from the receiving server before reaching the inbox of users, the team started the implementation of the algorithms they has planned using JAVA (JDK 1.7) with Eclipse Neon as the Integrated Development Environment. The team also took in the on the spot request of the forensic expert from the Ministry of External Affairs to implement a reporting mechanism where, when a spoofed email is detected by the product developed by the team, all the details are to extracted and send to a configurable email ID (In future, it would be the Cyber Forensics Team, to analyze the source and take appropriate action.) By the end of day on 1st April, 2017, the team has completed the implementation of the five algorithms that was planned as explained in the diagram below by splitting works among the members and working in a modular fashion, developing module with loose coupling and high cohesion.



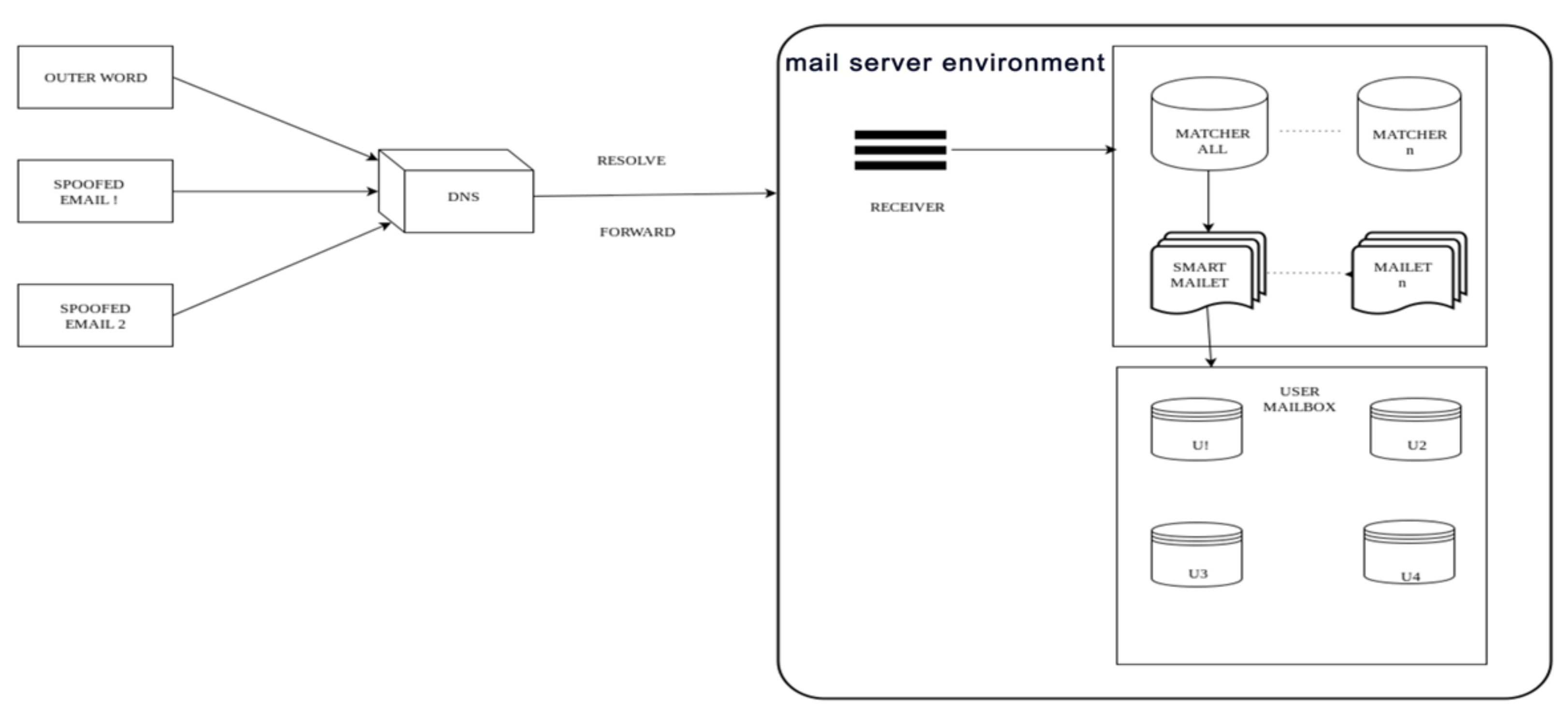
The approach taken by the team was to exploit the information available in the mail’s MIME version 1.0 format effectively before reaching the network to verify the authenticity using SPF and DKIM. The team implemented the complete protocol suit of “From-ReplyTo Check”, “From Domain - Received Domain Match”, “Received Chain Verification”, “SPF”, and “DKIM” in a fail fast design approach as discussed and suggested by the mentors so as to ensure the efficiency of the protocol suit.

The mentors put in their experience gained in Academia and Industry over the years to help the team overcome hurdles from time to time and to plan and work efficiently, actively reviewing the code base developed and suggesting improvements. At 9.00 PM, the team gathered to view the live telecast of the address by Prime Minister Narendra Modi and were further rejuvenated with the motivating session by the Prime Minister of India.

In the last evaluation on 1st April, 2017, the team showcased their algorithms and approach to the judges for which the jury members were impressed and suggested the team that implementing the solution on a live real-time environment will help showcase the effectiveness of the solution.

Well prepared for the sleepless hackthon night, the decided the following architecture and split into two groups. One group was given the responsibility of setting up the Apache James Email Server. The technology stack used was Apache James Server 3.0 Beta 5, Ubuntu OS 16.04 on Amazon Web Service Elastic Compute 2 with a configuration of 4 GB RAM, 2 Core CPU and 10 GB Elastic Block Storage.

The other team was designated the task of implement the protocol suit as a mailet (The configurable plugin feature supported by Apache James where custom developed protocols can be compiled and implemented without having the need to make any changes to the core of the mail server) and also to implement the reporting module for which the team and mentors had discussed and come up with a presentable design. The team also decided to name their product as “Smart India Mailet”, in fact the product was developed “By Young India for New India”



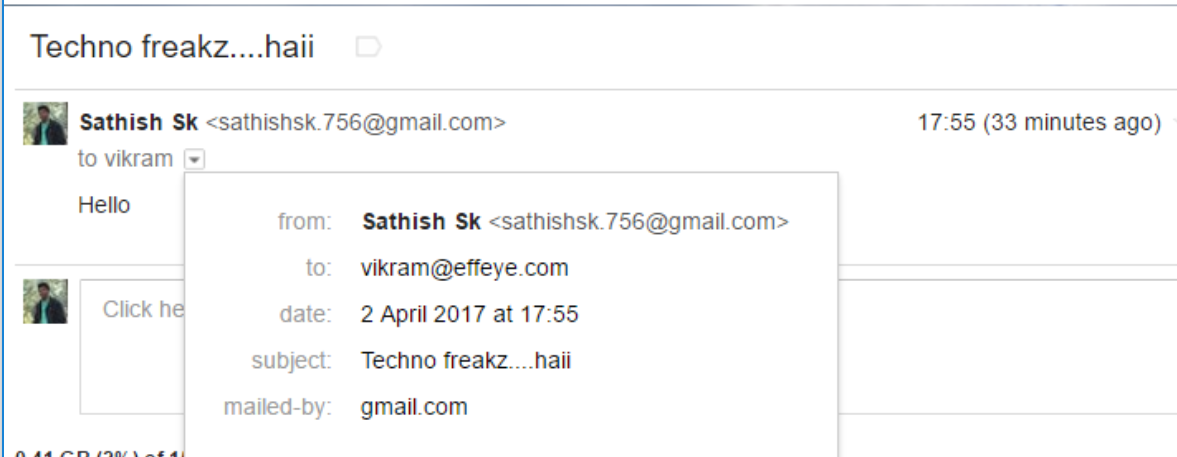
When the sun graced New Delhi on 2nd April, 2017, the pragmatic planned approach of the team has paid off. They were ready with a presentable real-time solution for email spoofing. They had setup a globally accessible mail server using Apace James on Amazon EC2 instance, deployed the Smart India Mailet which had the protocol suite implementation to detect, prevent and alert email spoofing attach on the mail server and configured it scan all email that is received by the mail server. The team was also actively testing the developed product using different test scenarios to ensure quality and fixing the identified bugs on the fly. Post breakfast, when the Director of Center of E-Governance and Information Technology, Ministry of External Affairs along with an Industry veteran came in to provide a mentoring session to the team, the team showcased their working product. The experts provided useful tips on improving the presentation and appreciated the implementation and work done. In fact, the Director of Center of E-Governance and Information Technology, Ministry of External Affairs was impressed with the solution, he invited the Mentors of the team to discuss on the enterprise grade implementation of the developed solution for the Ministry of External Affairs mail servers. The Mentors had two sessions with the director, where they explained the feasibility, the modes of implementation approaches that can be followed and also the ways the product can be further enhanced. The Director, request the team to publish the work as a journal and also exchanges contacts with the mentors for taking this ahead.

During the further rounds of evaluation, various experts from Ministry, IT Software Development, IT Security and Cyber forensics evaluated the team’s product and implementation and were impressed with the solution and gave very positive feedback. In the final power seminar, the team presented their completed work as a presentation and gave a live demo of the implemented solution to the complete jury.

The major scenarios that the team showcased are as follows.

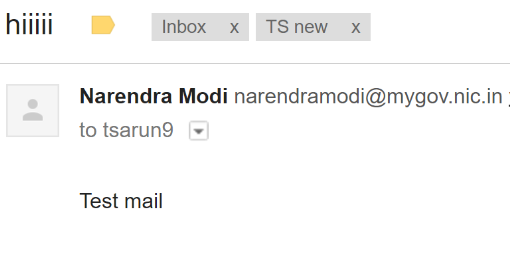
1. Receiving an email from a legitimate email server to the email server setup by students.

Result: The email server was able to receive emails without any problem.



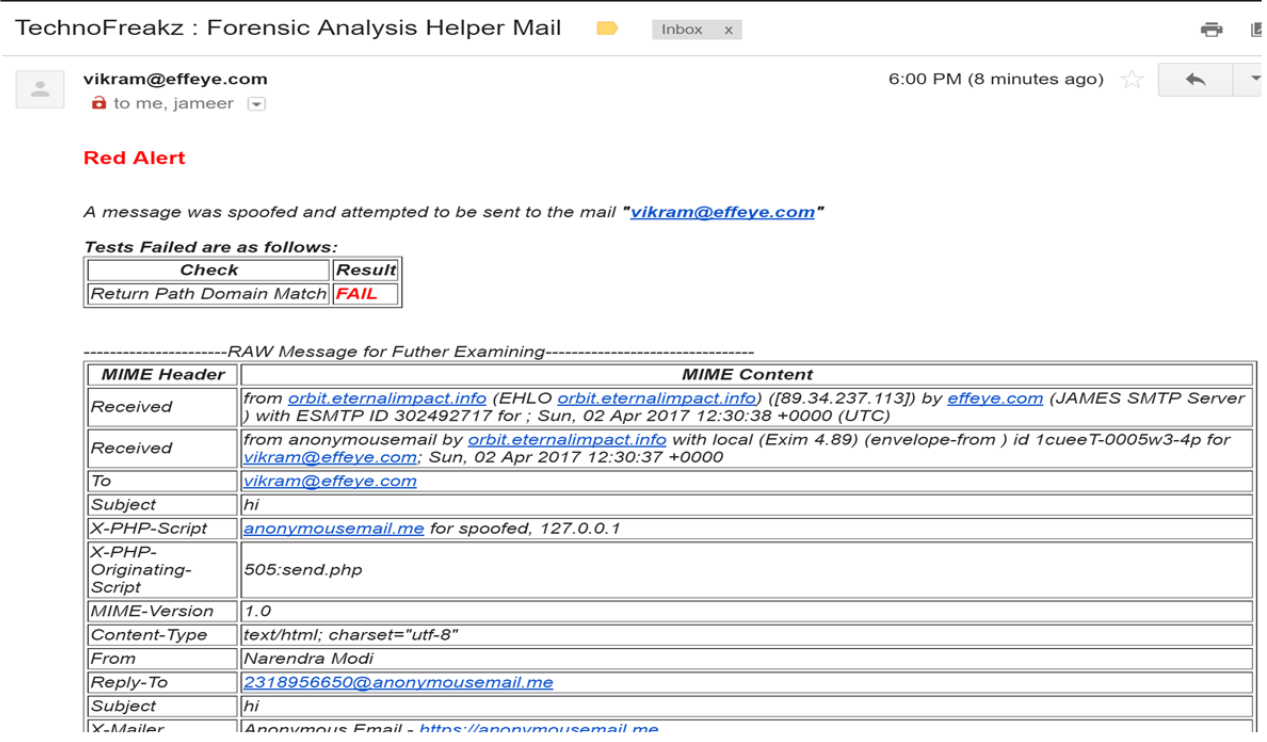
1. Sending a spoofed email to one of the popular public email service.

Result: The public email service did not detect the spoofed email, and infact allowed the mail to the inbox of the user and not even to the Spam folder.



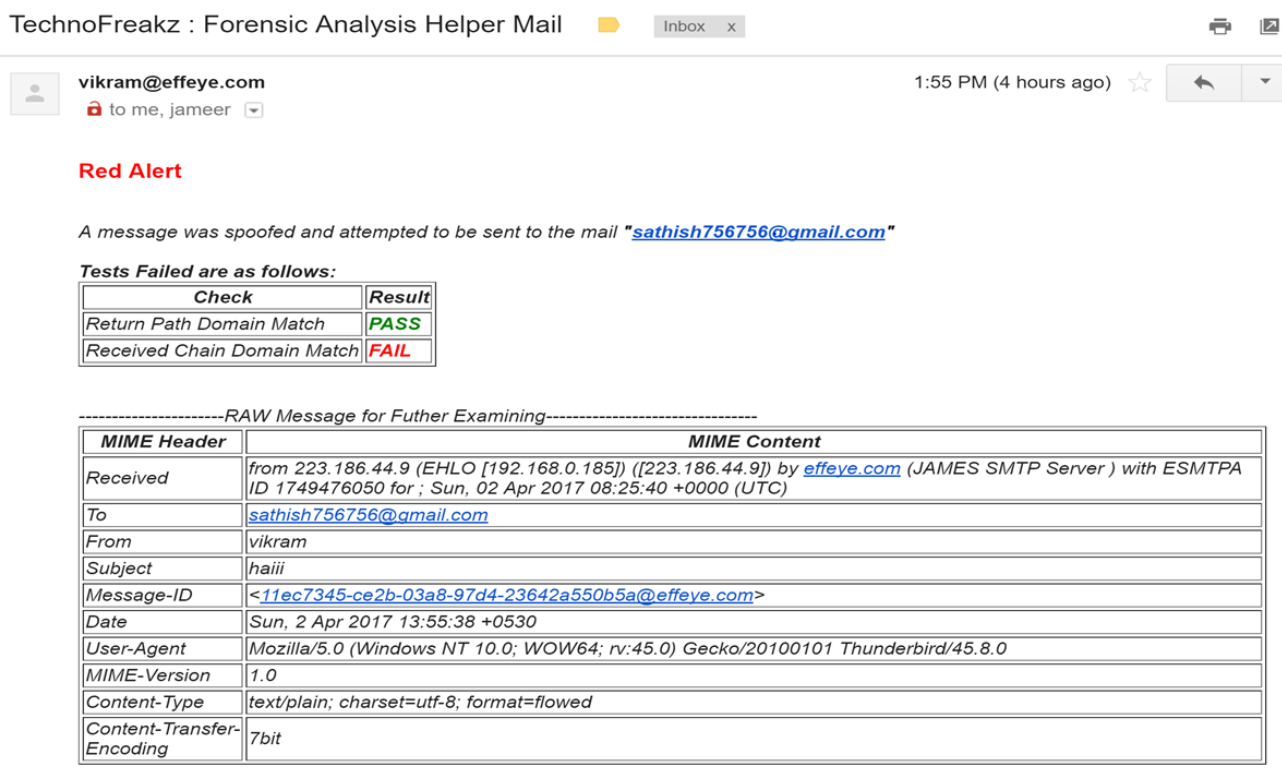
1. Sending a spoofed email with different reply-path to the mail server setup by the team with the protocol suite in action.

Result: The Smart India Mailet detected the spoofed email with the first protocol itself. Hence, stopped the mail from reaching the mailbox of the user, instead alerted the configured email address with the details. (One of the mentor’s personal email ID was set up as the alerting email address for demo. In future the alert email can be configured as the Cyber forensics email)



1. Sending a spoofed email with same reply-path to the mail server setup by the team with the protocol suite in action.

Result: The Smart India Mailet detected the spoofed email and alerted the configured alert email with the extensive reporting.



At the end of the event, the team was not aware of the results, however were very much satisfied with the work they had done in the 36 hours event. The morale and sprits of the team was high and was feeling pride with the positive feedback given by the experts throughout the event.

In the valediction ceremony, the Technofreakz team was declared nation-wide winners under the Ministry of External Affairs for the product they developed. The team was awarded with a Cash Prize of 1 Lakh INR, Medals and certificate in a ceremony where Mr. R. Chandrashekhar, President of NASSCOM was the chief guest.