Internship Report on Network Security System

By

Izaz Mahmud

ID: 192-15-13340

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Computer Science and Engineering

Supervised by

Narayan Ranjan Chakraborty

Associate Professor

Department of Computer Science and Engineering

Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

SEPTEMBER 2025

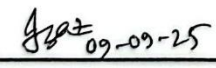
DECLARATION

We hereby declare that, the work presented in the internship report title "**Network Security System**" is done by me, Izaz Mahmud, ID: 192-15-13340 to the department of Computer Science and Engineering, Daffodil International University, under the supervision of **Narayan Ranjan Chakraborty, Assistant Professor, Department of CSE, Daffodil International University**. I am declaring this report is my original work. I also Declare that neither this Internship report nor any part of this internship report has been submitted elsewhere for award of any Degree or Diploma.

Supervised by:

Narayan Ranjan Chakraborty
Associate Professor
Department of CSE
Daffodil International University

Submitted by:



Izaz Mahmud
ID: 192-15-13340
Department of CSE
Daffodil International University

APPROVAL

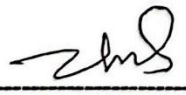
This Internship report titled **"Network Security System"**, submitted by Name: **Izaz Mahmud**, ID No: **192-15-13340** to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on **17 September, 2025**.

BOARD OF EXAMINERS

Dr. S.M Aminul Haque — **Chairman**
Professor & Associate Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Ms. Nazmun Nessa Moon — **Internal Examiner**
Associate Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Md. Abbas Ali Khan — **Internal Examiner**
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University



Dr. Md. Zulfiker Mahmud — **External Examiner**
Professor
Department of Computer Science and Engineering
Jagannath University

ACKNOWLEDGEMENT

Firstly, I would like to express my gratitude to the Almighty Supreme being for His divine blessings and for giving me the strength to successfully complete this project and internship.

I am deeply grateful and would like to extend my profound thanks to Narayan Ranjan Chakraborty, Associate Professor at Daffodil International University, Dhaka. His deep knowledge and keen interest in the field of Face Recognition work and its application design and development greatly influenced me throughout this internship. His endless patience, thorough guidance, constant encouragement, energetic supervision, constructive criticism, and valuable recommendations in reviewing several drafts helped me complete this work successfully.

I would like to express my heartfelt thanks to Professor Dr. Sheak Rashed Haider Noori, Professor and Head of the Department of Computer Science and Engineering, for his kind assistance in helping me complete my internship, and also to all the other faculty members and staff of the Computer Science and Engineering department at Daffodil International University.

I would also like to express my gratitude to all my course mates at Daffodil International University, who actively participated in discussions and assisted in completing coursework.

Finally, I would like to thank my family, especially my parents, for their continuous support and encouragement throughout the entire duration of this internship.

ABSTRACT

This internship report focuses on the practical application of network design, configuration, and security measures within the scope of tasks undertaken during the internship at Goinnovior Limited. During the project I worked with Cisco tools. I tried designing a medium office network in Packet Tracer. The plan used several subnets, a couple of routers, switches and a wireless link to make something secure. I also set up routing (RIP or maybe OSPF) and ran tests on IP addresses and subnetting to check end-to-end connectivity. Overall, the setup felt promising for later.

Additionally, one part of the job was the firewall. The intern, maybe, set up rules in the Windows Defender Firewall Wizard. He tried to block HTTP on a few ports, but kept HTTPS open. To do that, he typed the protocols, then chose block for the connections. Testing followed, looking to see if traffic stopped as planned. Therefore, the network should be a little safer, while fast enough for users. In conclusion, the setup tries to boost security without hurting access.

During the internship I got real-world practice designing, configuring and (sometimes) securing an enterprise network. It may mean I learned how traffic flows, how security protocols work, and why firewalls matter for blocking unwanted access. Those tasks, they show why hands-on skills matter for protecting today's digital systems in the modern infrastructure.

Table of Contents

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Introduction

An internship provides an excellent opportunity for students to acquire firsthand experience in their field of study and to bridge the gap between theory and practice. As a student, Bachelor of Computer Science Engineering, my objective during internship at Goinnovior Limited was to improve my hands-on skills in Cyber Security. The internship was held from 10th August 2024 to 10 December 2024 during which, I had exposure to work with industry experts and work in challenging environment where I contributed in number of Cyber Security projects like Configuration, Trouble shooting and infrastructure Reviews.

During my internship I was working to actively assist the Cyber Security team, discover and fix security vulnerabilities and optimize the security infrastructure. The experience has provided me comprehensive knowledge of Cyber Security practices, tools, and methodologies. Also, it has prepared me for the upcoming job opportunities in Cyber Security.

1.2 Motivation

I selected a Cyber Security internship as it's a rapidly emerging tech sector of the future. In the age of frequent hacking and system breaches, learning cybersecurity is a must for tech careers. As a student, I studied theories of network security, ethical hacking and data protection and I desired an opportunity to get real-world experience using this knowledge in real-life situations. Goinnovior Limited is a known brand for their dedication to solving many problems on Cyber security, so I see it as a good avenue for me to learn new things I wished to review the performance of professionals who are enthusiastic about Cyber Security and to learn through their knowledge in tackling the intricate technical problems. Also, I was looking for an opportunity to learn at least one of the latest Cyber Security tools / technologies.

1.3 Internship Objectives

The main goal of this internship was to consolidate my competencies and experiences in Cyber Security. I aimed to:

- Put cyber-security theory into real-world use.

- Build hands-on practice by installing, fixing, and keeping security tools running.
- Get problem-solving and critical thinking habits to spot weak spots and patch them.
- Boost my speaking skill by teaming up and explaining tech ideas clearly.
- With these aims I hope to pick up the needed know-how for a career in cyber-security, especially in network defense, ethical hacking, and managing security systems.

It may seem tough, but the hands-on route usually leads to confidence.

1.4 Internship Goals

Objectives for the internship included the following:

- Technical skills training may mean learning to configure firewalls, VPNs, and an intrusion detector.
- Hands-on work with these tools feel clumsy at first, yet it builds know-how.
- Problem-solving appears to happen fast when security alert blares in an office; you might sketch a script on a napkin to patch a hole.
- Solving tough security puzzles across firms also pushes you to talk with peers, which can be supportive and bit noisy.
- Knowledge growth is likely still involve reading threat feeds and new protocol updates today in practice.
- Clear communication, spoken and written, improves when you explain glitch to a non tech manager.

By doing so, I intended to further advance my professional growth and also to become skilled in tangible aspects of Cyber Security.

1.5 Introduction to the Company

Short description: Goinnovior Limited is an IT service and software maker in Dhaka, Bangladesh. It started small, but now it's may be one of the most trusted names in IT and cyber security. The firm offers end-to-end help: cyber security services, network management, and IT infrastructure support. People say the quality feels exceptional and the ideas seem fresh. That means clients can try to keep their digital stuff safe and improve security with new tools. The cyber security crew appears quite skilled and shows a strong drive to give good service. Some argue the firm pushes hype, yet many still see it as a solid place to learn about the industry.

Company Information:

- Name: Goinnovior Limited
- Location: Mirpur, Dhaka, Bangladesh.
- Industry: Cyber security, and IT solutions
- Internship Period: 10th August 2024 to 10th December 2024

Internship experience at Goinnovior Limited acquainted me with several Cyber Security projects, and a first-hand experience into the best practices of Industry.

1.6 Report Layout

This report is structured as follows:

Chapter 1 is introduction which introduces the reader to the internship; the objectives, rationale, and company. In chapter 2, organization details are given, which provides weighty penetration into GOINNOVIOR LIMITED and include SWOT analysis and organogram. The third chapter is about the TASKS, PROJECTS AND ACTIVITIES**;** describes the tasks I was assigned and provides a more detailed description of the projects and activities I initially were working on during my internship. Chapter 4 describes the Competencies and SMART Plan which focuses on the competencies achieved through the internship and provides my SMART goals. The last chapter, chapter 5, Conclusion and Future Career, provides a conclusion and how the internship was summarized as an experience as well as skills developed during this internship and career opportunities in the Cyber Security field. The appendix includes additional details, such as the internship certificate.

CHAPTER 2

ORGANIZATION

2.1 Introduction

In this chapter, I will discuss the company where I completed my internship, Goinnovior Limited. Here is a quick look at Goinnovior Limited. It is an IT service firm located in Dhaka, Bangladesh. The company seems to focus on IT consulting, managed services, digital marketing and brand promotion. Their partners include names such as Microsoft, Sophos and Google, which may help them reach a wider audience. They belong to the Bangladesh Association of Software and Information Services. The target market appears to be businesses needing tech support, though competition could be strong. A SWOT would note strong partnerships but global reach.

2.2 Internship Program Overview

During my internship at Goinnovior Limited, I was part of the Cyber Security team, where I actively contributed to various projects focused on maintaining and enhancing the company's Cyber Security infrastructure. The program spanned four months, from **10th August 2024 to 10th December 2024**, and provided me with valuable hands-on experience in managing security systems, identifying vulnerabilities, and applying solutions to improve overall security.

The internship was divided into several phases:

- Cyber security: Set firewalls, VPNs, intrusion detection systems today.
- Problem solving means spot vulnerabilities, maybe fix them quick, effectively.
- Collaboration involves cross-functional teams, sharing ideas, optimize security together continually.
- Tools and technologies demand learning security tools, protocols, methods, perhaps never-ending.

The experience helped me gain practical knowledge in the field, which was essential for my professional growth.

2.3 Target Group

Goinnovior Limited's solutions are designed for multiple businesses including small, medium and large enterprises in need of advanced IT solutions to ensure their infrastructure is secure, robust and scalable on to the digital world. The target group includes:

- Small and medium-sized enterprises (SMEs): These are businesses that are looking for cost-effective IT and security services.
- Heavy corporate companies: Need Solid Cyber Security, which will include their IT support and have access to enterprise level software services.
- E-commerce and Digital Companies: Commercial and enterprises that sell their services or products on the internet, all stand to benefit from the digital marketing solutions offered by Goinnovior to enhance their online visibility and interactions.
- Government and Public Sector Bodies: They need to implement security and IT consultancy to secure data and infrastructure.

Goinnovior partners with leading technology companies, which enables them to deliver personalized IT solutions to every business.

2.4 SWOT Analysis

SWOT analysis SWOT analysis is a technique used by companies to identify the internal strengths and weaknesses, as well as external opportunities and threats. Following is the SWOT analysis of Goinnovior Limited:

2.4.1 Strengths

- Trustworthy Name: Goinnovior is a well-known IT service provider company in the Bangladesh Market. The firm has established itself as a trusted company for diversified range of services in such as Cyber Security, managed IT services and Online marketing.
- Partnerships with Industry Leaders: Cooperation with Microsoft, Sophos, Fortinet, Kaspersky, TrendMicro, and Google contributes to the trust and craftsmanship the company delivers.
- Expert Staff: At Goinnovior, you will be attended by trained and certified staff.
- All-inclusive: Goinnovior offers many services from IT consulting to digital marketing which is why it is the hub for all IT needs.
- Membership With BASIS: Being a part of BASIS ensures Goinnovior connect with the industry standards, best practices and thus sustains credibility and trust.

2.4.2 Weaknesses

Dependence on valued partners: Goinnovior leans heavily on outside tech firms like Microsoft and Kaspersky. This reliance may mean the firm's freedom is limited. If those providers change their terms or stop service, Goinnovior could feel push-back on its own work. Some might view it as risk; others see it as a chance to learn from leaders.

Low worldwide brand awareness: The company does well inside Bangladesh but its name is hardly known abroad. In the crowded global IT and ITES market, this weak profile could slow growth. Still, a niche focus might help it stay hidden from large rivals.

High operating expenses: Delivering managed IT and cyber-security services push costs up. Small customers may not give margin.

2.4.3 Opportunities

- Cyber security services are getting bigger. Because data leaks keep happening, there's maybe a bigger push for tougher security. Goinnovior could try to grow its security menu and reach more customers. and maybe gain trust from wary clients.
- Cloud services keep spreading. More businesses want safe clouds. Goinnovior might add extra cloud options to meet that hope for reliable, protected storage. They worry about data loss, so guards help.
- International market looks open. Going abroad could help Goinnovior compete and bring new money streams. Expanding beyond borders may boost its reach.
- Working with startups that chase new tech feels useful. Partnering with firms into AI, big data, or blockchain could bring fresh ideas and services to Goinnovior.
- Government and public contracts are rising. As officials dig digital tools and security, chances appear for Goinnovior to land large public deals.

2.4.4 Threats

- The IT services market is crowded; many local firms sell alike packages. Goinnovior must stay competitive. It may mean they need to keep inventing better service offers. Some customers look for novelty, so staying ordinary could hurt.
- Tech changes fast, a headache. Goinnovior must watch new tools. They spend resources to stay current. Missing trends hurts client satisfaction. Otherwise projects could lag.
- Economic shifts create doubt. A recession or low demand can cut IT budgets. That may hurt spending on SERV On. Goinnovior must plan for drops; therefore profits shrink. They might also need to cut staff.

- Cyber threats loom. As a security firm Goinnovior appears to watch attacks. Falling behind may damage reputation. Clients could lose trust, which is vital. Staying ahead seems essential.

2.5 Organizational Structure

Goinnovior Ltd. seems built around teamwork and project handling. The Managing Director probably leads daily tasks. Below him, heads of sales, production, and finance-HR each run their own sections. Moreover, Program Managers appear for particular tech or business projects. Workers, therefore, are placed into roles that match their skills. The layout may help clear communication, though some overlap could still happen. It could need review periodically.

Organizational Hierarchy:

1. Managing Director / CEO (Kahafil Ora)
    - Head of Sales
        - Program Managers (Technical, Business)
    - Head of Production
        - Project Managers
    - Head of Finance/HR
        - Support and Operations Teams

This structure ensures smooth communication, effective management, and project delivery across various departments.

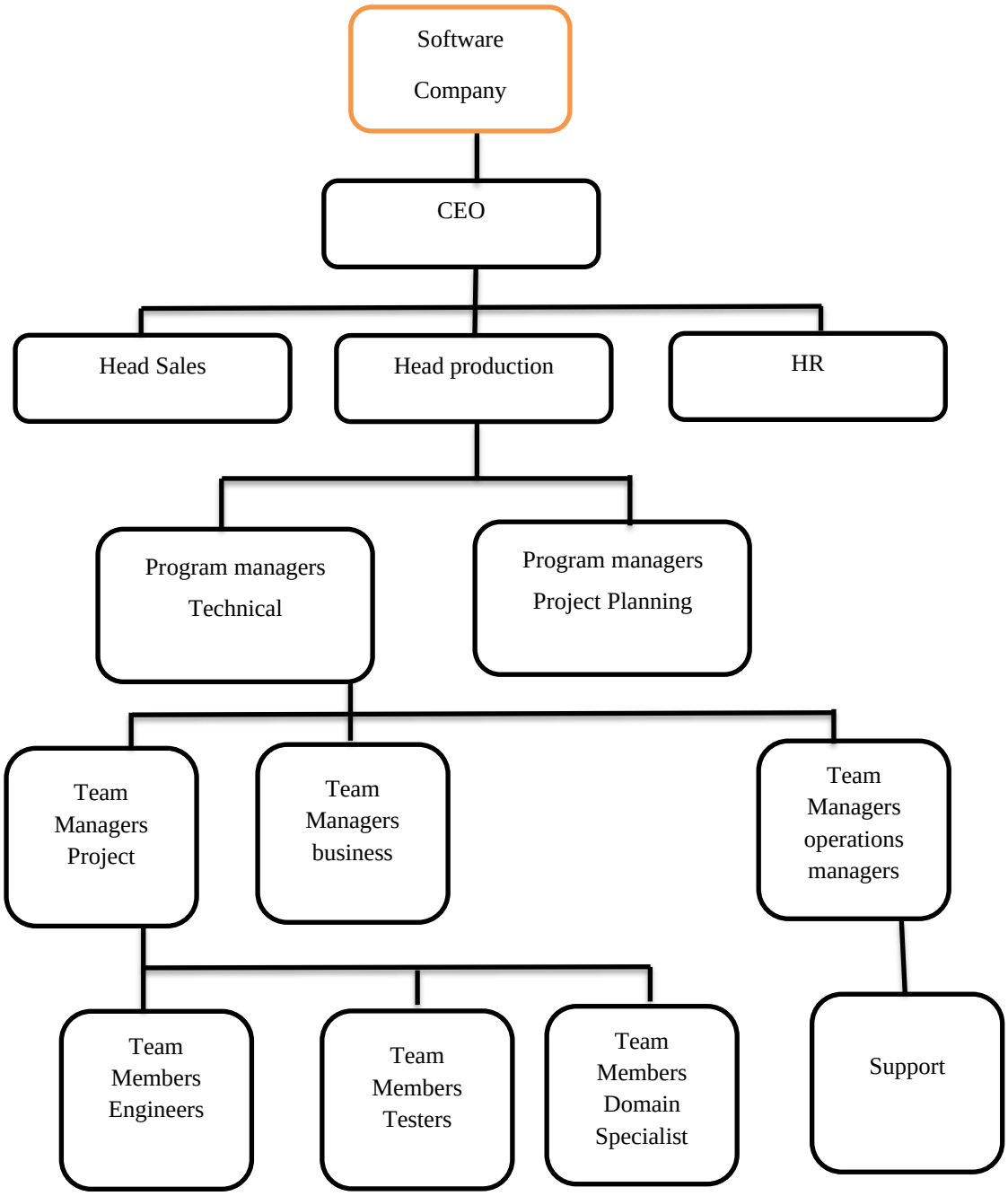


Figure2.5.1: Organizational Structure of Goinnovior Limited

CHAPTER 3

TASKS, PROJECT AND ACTIVITIES

3.1 Daily Tasks and Activities

During my internship, I was engaged in an array of daily projects-participated in creating, maintaining, and O/Ging the firm's network and Cyber Security. Here are some of the major responsibilities I performed on a daily basis:

Monitoring Network Security: Each day I check the network. I glimpse odd firewall hits, maybe someone testing it. I scan logs, catch strange alerts, and jot down any pattern that's off, it's for future reference.

Troubleshooting Network Issues: Our group maybe fixed some device connection glitches; I skimmed logs, double-checked each IP address. Some routers were mis-configured, which appears to cause drops. I also ensured cables were plugged in right, though a loose wire could be the cause. Fixes were often quick, and very, but sometimes needed more testing.

Setting Up and Configuring Firewalls: I helped with Windows Defender and other firewalls. Adding inbound rules to block ports like 80 was simple, yet it may also block needed traffic. Balancing blocking bad and allowing good seemed hard to get perfect. I documented each rule for later review.

System Configuration and Maintenance: Configuring routers, switches, and firewalls was part of my task. I kept firmware up to date and applied patches. Backups of configs were taken regularly, because loss could happen. I think the schedule could be tighter, though.

Collaborating with Team Members: We met weekly and I worked with other departments on their security needs. Sometimes goals differed, which required compromise.

Client Support and Troubleshooting: I sometimes helped support with end user questions about network security issues, walked with them on troubleshooting common connectivity and security issues.

3.2 Events and Activities

Besides the daily to-do's, I was involved in numerous events and gatherings initiated by Goinnovior Limited, which were focused on learning and team building.

3.2.1 Training and Workshops

Cyber Security Workshops:

I've attended a bunch of internal workshops in which the top-notch security professionals from the company gave sessions on the trends in Cyber Security, how to secure a network, and how to use advance tools for detecting threats.

Tool Familiarization Sessions: I participated in open-labs to further my technical knowledge in the use of Wireshark –network analysis tool, Sophos XG Firewall –advanced firewall configuration. These sessions provided me with an opportunity to use all that I had learnt in a practical setting.

Inter-Departmental Knowledge Sharing: We had round-table talks where each department somewhat outlined what they've been up to, what's tripping them up, and what's working. I ended up seeing tools from network engineers, plus tactics from digital marketers, which may be broadened my view and also shared real-world examples for everyone.

3.2.2 Security Awareness Programs

Internal Security Awareness Campaigns: We held staff meetings about maybe security risks, like phishing and password rules. I helped organize and share tips on safe web surfing and email safety for everyone.

Client Briefings on Cyber Security: I went to several client facing meeting to give drum up stone this was to briefing clients about best security practices for their business. I submitted feedback on how they could better their Cyber Security works by implementing lessons learned from my internship.

3.2.3 Networking and Teambuilding Activities

Weekly Team Meetings: These meetings were an opportunity to update the team on progress of the projects and for the team to come together to discuss issues and progress. I communicated my own progress and work with others to make deadlines.

Team Outings and Social Events:

Off-the-tech-work, we used to venture-out for team dinners and party to develop friendship and to make the bond stronger. These were informal get-togethers and an annual company party.

3.3 Project Tasks and Activities

3.3.1 Task 1: Design of the Office Network

As an intern, I had to design a network for an office into subnets with routers, switches and such. The main activities were:

Designing the Topology: I began by drawing the network topology on paper and then I switched to Cisco Packet Tracer to build the topography. Topology wise it was supposed to have different ip ranges for different departments like HR, IT and Sales.

Configuring Devices and Network Setup: I configured different internetworking devices including routers and switches in Cisco Packet Tracer. I set up DHCP server, DNS server, connected all devices for network working correctly.

Setting Up IP Addressing: I manually put a wan interface addresses on all devices and gave each subnet a unique /29 using a router as a gateway.

Routing Configuration: To accommodate inter-subnet communication, I set static routes and dynamic routing protocols (rip/ospf). I tried pinging to check the connectivity between the two servers.

Wireless Configuration: In addition, I had a wireless router elsewhere for connecting mobile devices to the network. That meant creating SSIDs, setting up WPA2 security and ensuring something that resembles "the Internet" flowed through WiFi.

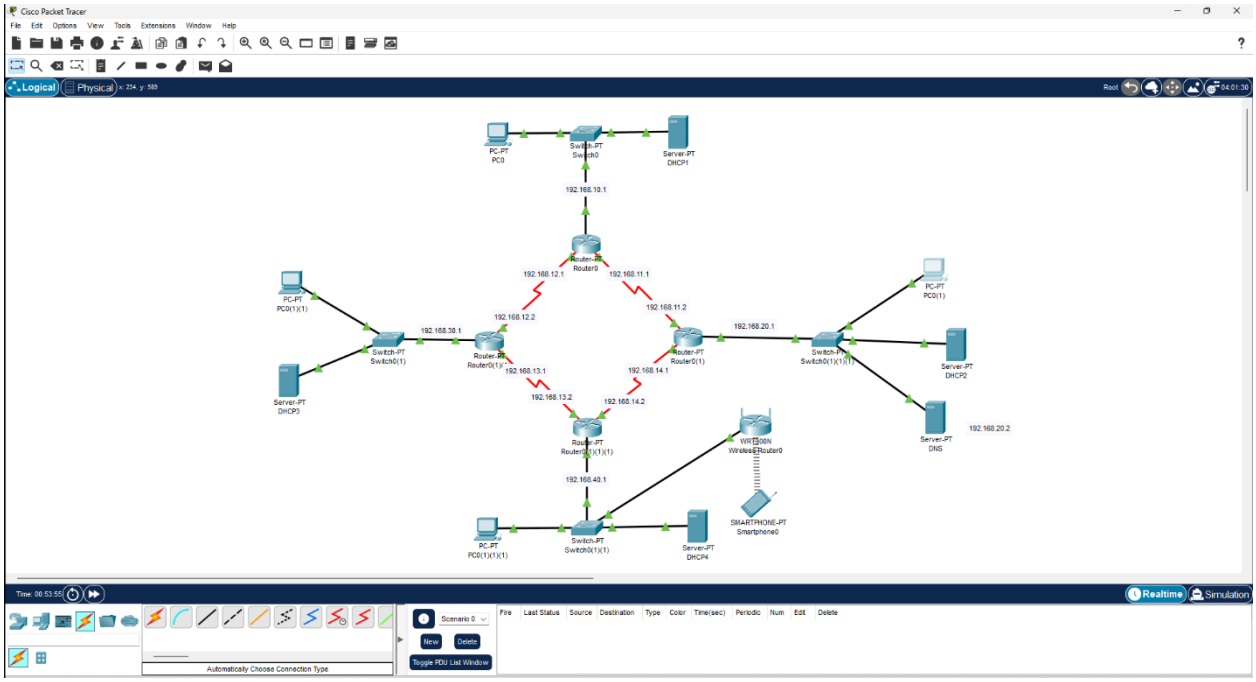


Figure 3.3.1 (a): Cisco network design

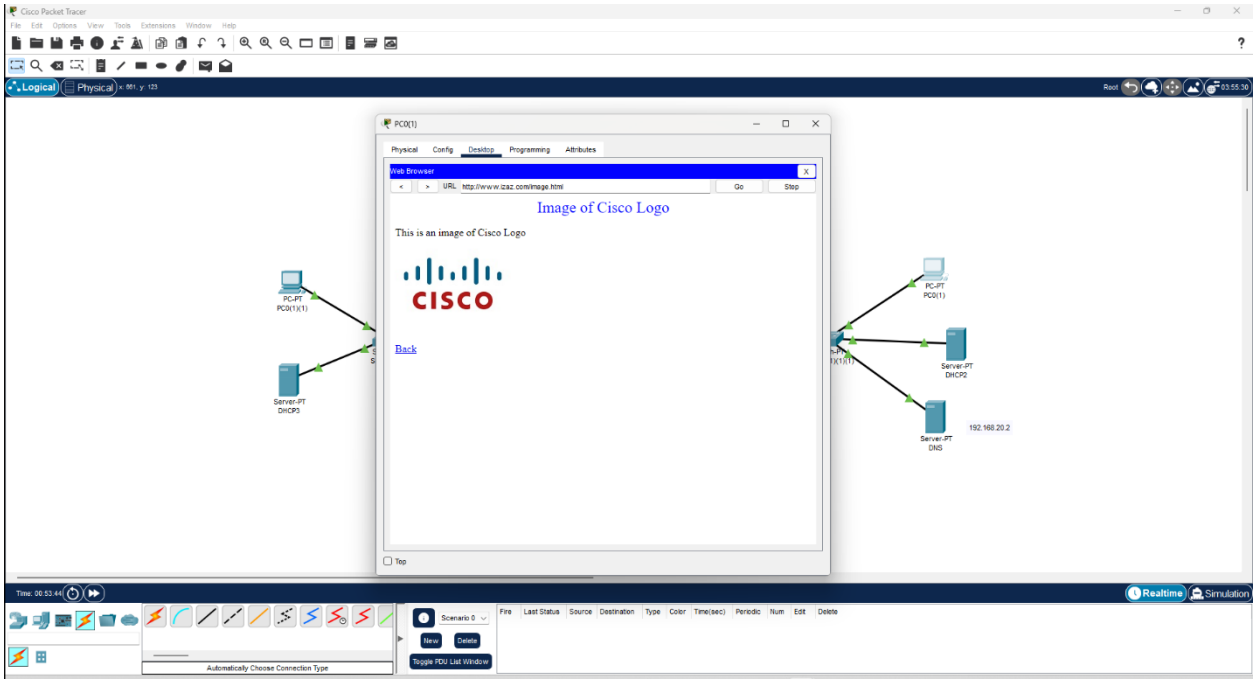


Figure 3.3.1 (b): Cisco network working

3.3.2 Task 2: Firewall Rule Design

For this project, I was responsible for creating a firewall rule to block HTTP traffic. The activities included:

1. **Configuring Firewall Rules**:
   I configured **Windows Defender Firewall** to block incoming traffic on port 80 (HTTP). This was done through the **New Rule Wizard**, where I selected the port type, specified port 80, and chose to block the connection.
2. **Testing the Rule**:
   I tested the rule by attempting to access an HTTP website, which failed to load. This confirmed that the firewall rule was working as intended. I also verified that HTTPS sites (using port 443) remained accessible.
3. **Disabling the Rule**:
   After testing, I disabled the rule to restore normal browsing functionality. I documented the process, ensuring that I understood the steps involved in creating, testing, and modifying firewall rules.
4. **Providing Documentation and Reporting**:
   I documented each step of the firewall configuration process, detailing the settings

and testing outcomes. This was included in my final report as part of the security project.

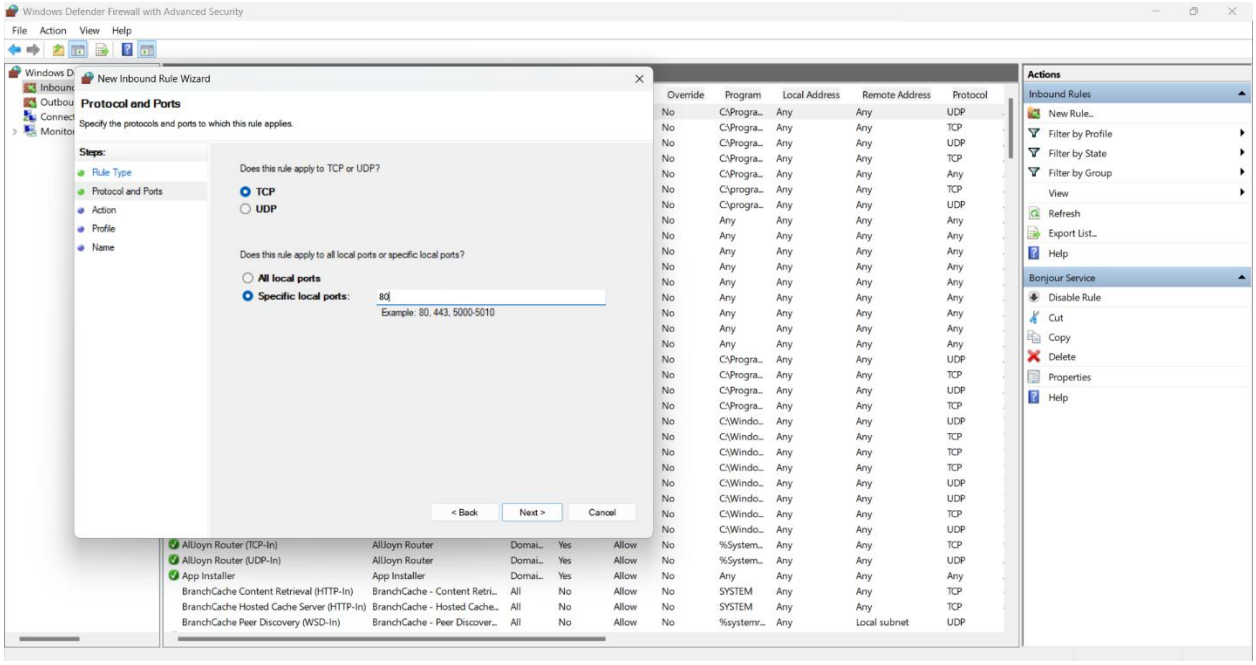


Figure 3.3.2 (a): Protocol and ports input in Firewall Rule Wizard

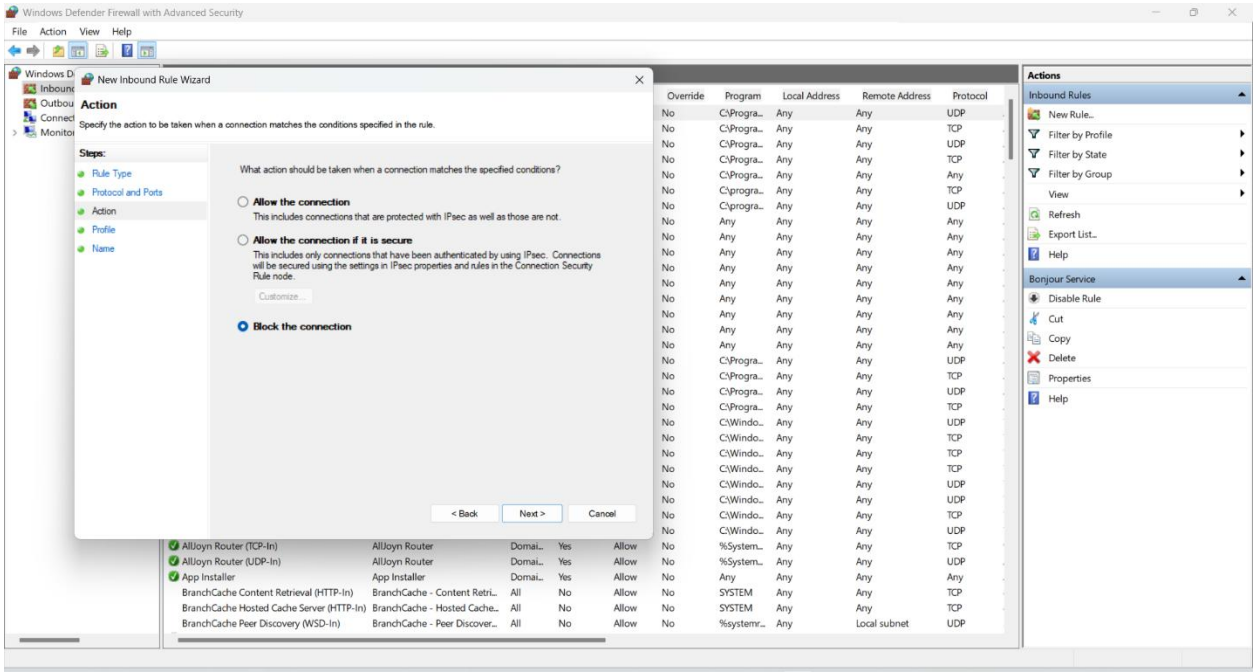


Figure 3.3.2 (b): Action connection blocking in Firewall Rule Wizard

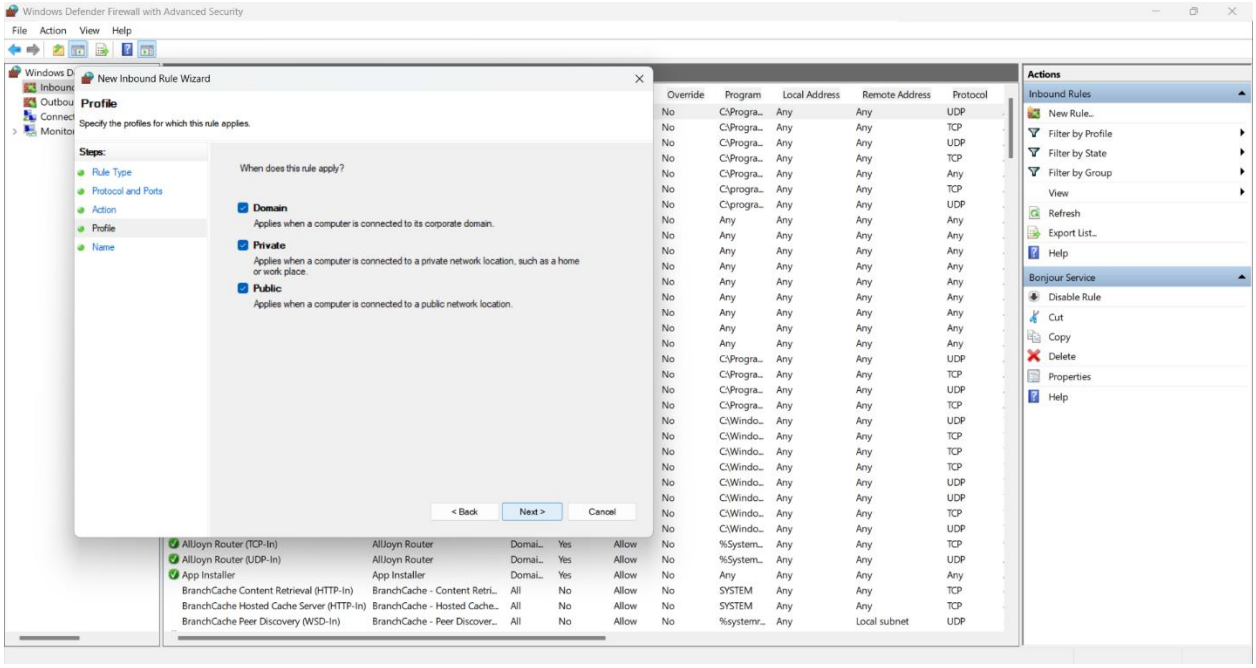


Figure 3.3.2 (c): Profile setting in Firewall Rule Wizard

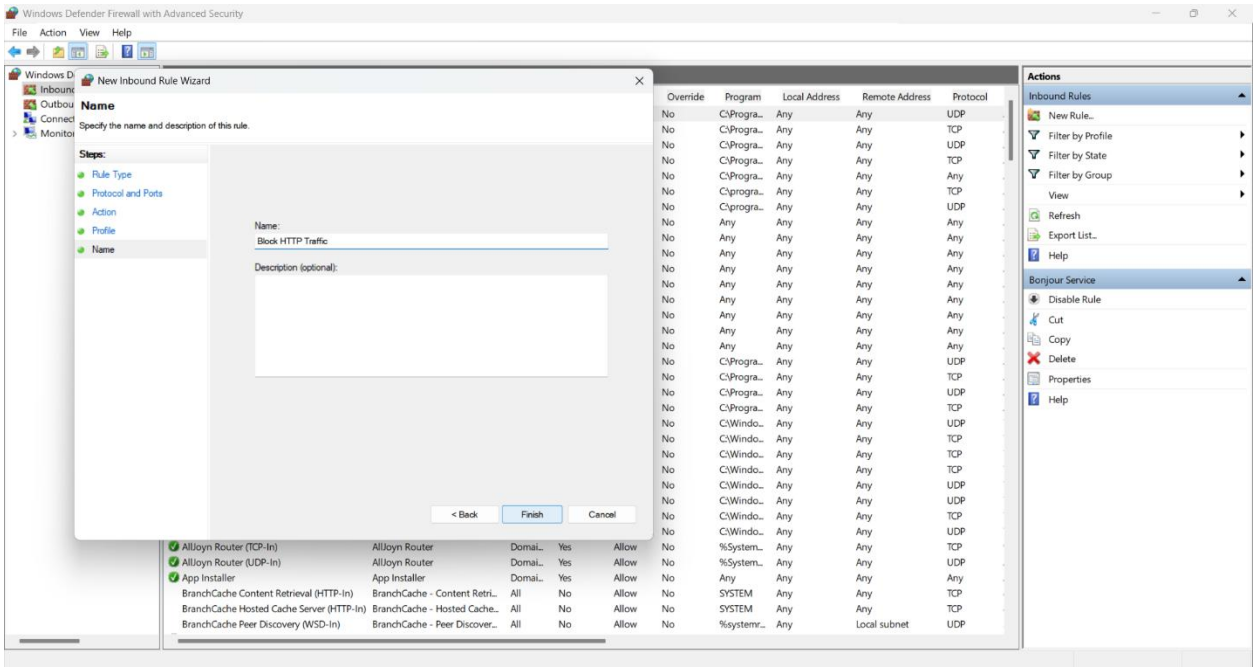


Figure 3.3.2 (d): Set new rules name in Firewall Rule Wizard

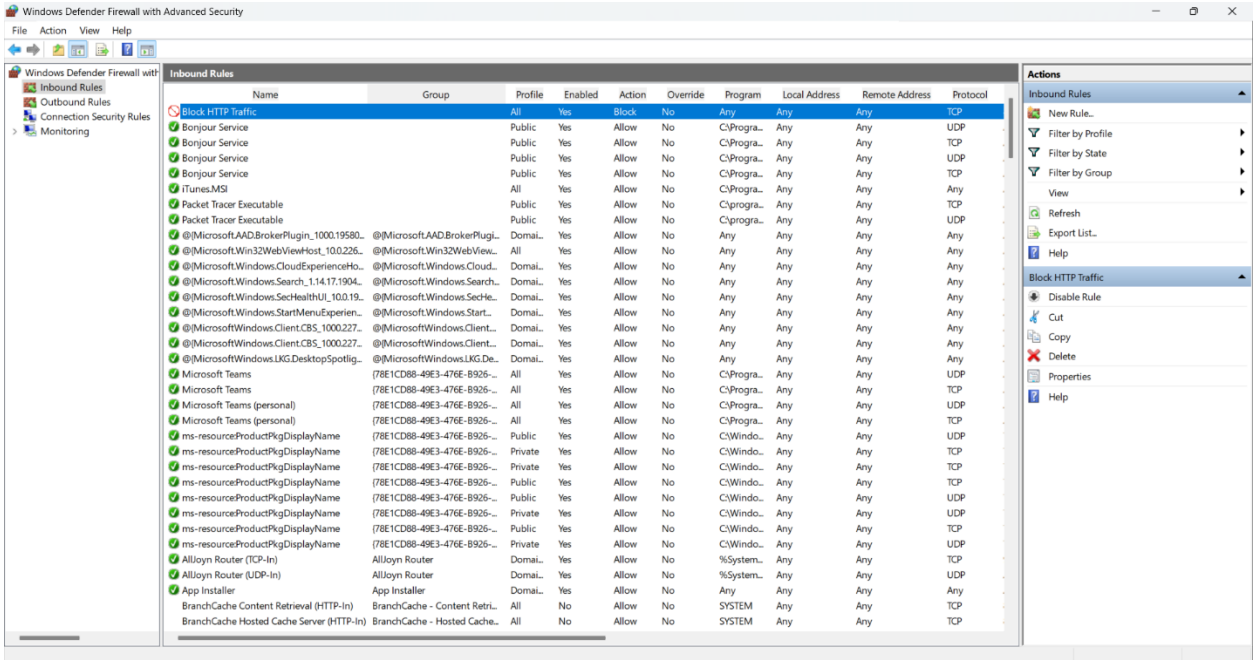


Figure 3.3.2 (e): New rules added in list in Firewall Rule Wizard

3.3.3 Task 3: Wireshark Packet Capture Analysis

1. General Network Traffic Capture

This figure shows the general network traffic capture process itself. This further demonstrates how data packets are collected and analyzed in the network.

Basically, the first capture recorded multiple types of network traffic, and the same was done within the local network. As per the observations, different protocols like UDP, TCP, MDNS, and SSDP were found. Regarding the network analysis, these protocols were seen during the study. Also, the captured packets show communication between the local client machine (192.168.0.x) and broadcast/multicast addresses, and further show communication with external IP addresses itself. We are seeing DNS queries and responses, multicast discovery, and HTTP notifications only in the observed traffic.

This figure surely shows how multiple services work together on a network at the same time. Moreover, it demonstrates how Wireshark can identify and classify these services based on their protocols and destinations.

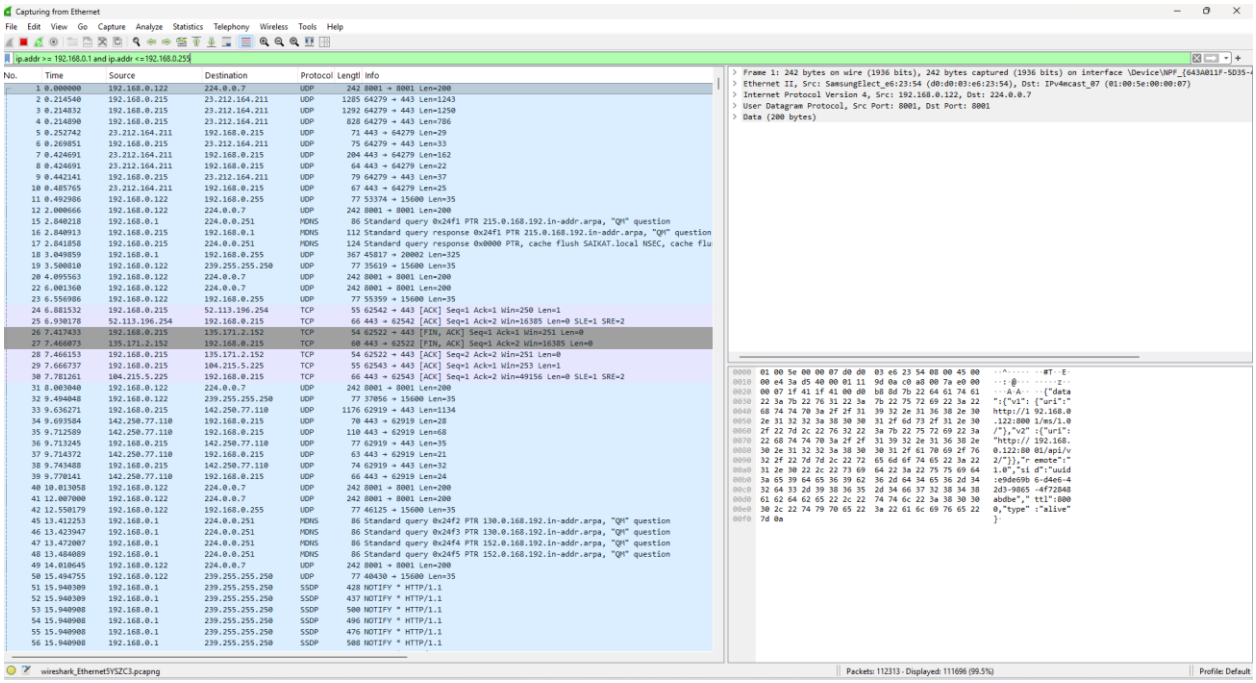


Figure 3.3.3(1): General Network Traffic Capture

2. TCP Stream – DNS Communication

This figure shows the TCP stream for DNS communication itself. This further demonstrates the network traffic patterns during domain name resolution.

The second capture actually shows a filtered TCP stream (tcp.stream eq 2) that definitely focuses on DNS communication between 192.168.0.215 (client) and 192.168.0.1 (DNS server).

As per the network analysis, the standard TCP three-way handshake process ([SYN], [SYN-ACK], [ACK]) is clearly visible. This handshake regarding connection establishment follows the expected pattern.

As per the network configuration, DNS protocol is used over TCP regarding port 53 communication. The client surely sends a DNS query to the server, and the server responds with the requested AAA record for msftncsi.com. Moreover, this exchange demonstrates the basic traffic flow in DNS communication.

This figure surely shows how DNS resolution works through TCP connections and how network analysts can examine queries and responses. Moreover, it demonstrates that Wireshark can capture the complete handshake process for detailed inspection.

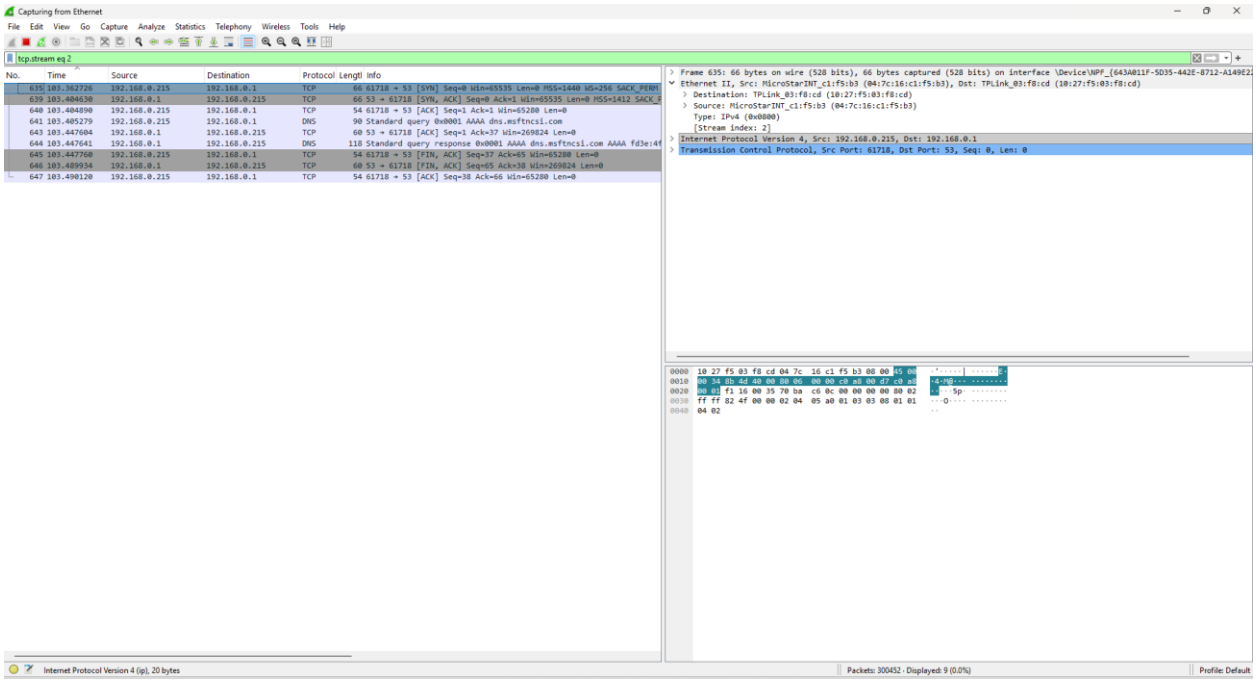


Figure 3.3.3(2): TCP Stream – DNS Communication

3. HTTP Communication

This figure surely shows the HTTP communication process between client and server. Moreover, this diagram illustrates how data packets move through the network during web requests.

The third capture shows HTTP traffic between the local client (192.168.0.215) and an external web server (103.12.74.69). This traffic itself represents the communication between these two systems for further analysis. We are seeing that the handshake means the first TCP three-way handshake is only completed. The client actually sends an HTTP GET request to get the streaming service file. This definitely starts the traffic flow for media content. The server surely sends back the requested content to the client. Moreover, a TCP RST packet is then used to close the connection completely.

We are seeing how HTTP requests and responses move through TCP connections, showing only the basic way clients send requests and servers handle responses.

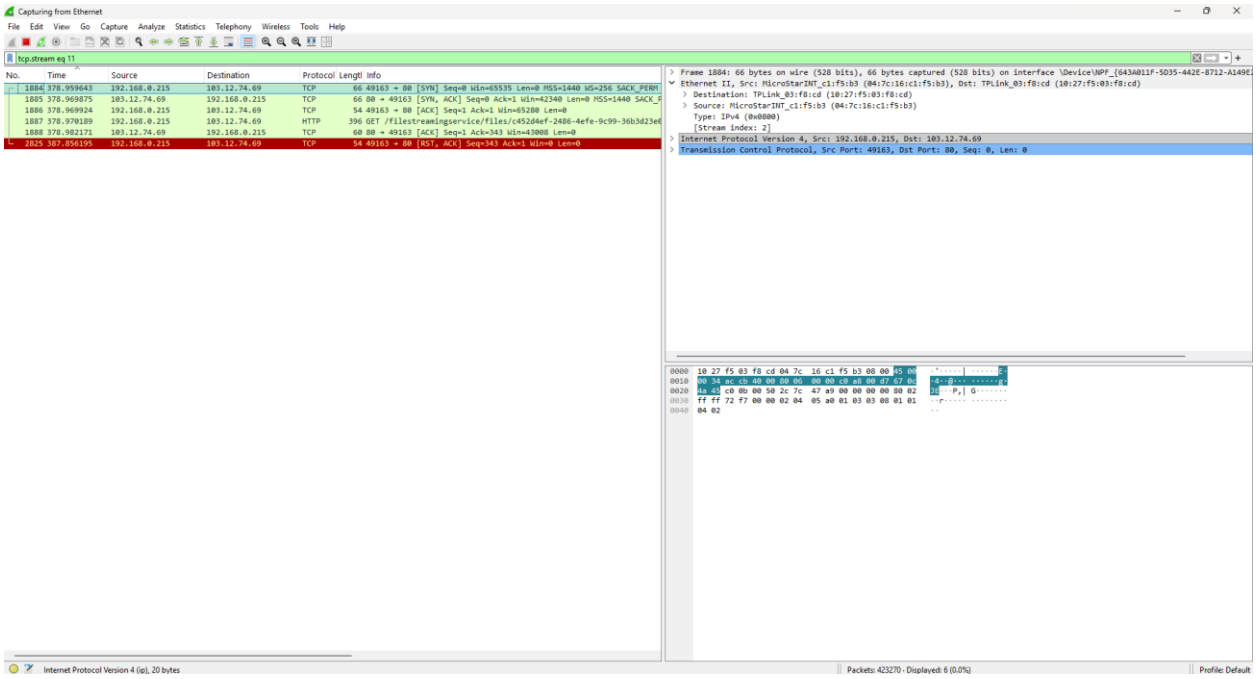


Figure 3.3.3(3): HTTP Communication

Conclusion

As per the above Wireshark analysis, it is clear that many protocols work together at the same time in a normal network. This shows regarding how different protocols operate simultaneously in typical network environments. Basically, by capturing DNS queries, multicast discovery, and HTTP communications, we can understand how data flows through the network the same way we track any information movement. During the internship, we are seeing that Wireshark was used as a practical tool for network troubleshooting only, protocol analysis, and checking communication flows.

CHAPTER 4

COMPETENCIES AND SMART PLAN

4.1 Competencies Earned

Throughout my internship, I gained transferable technological and networking skills, and improved my analytical skills. These skills are important towards my future in IT and Cyber Security. Here are the Core competences that I have developed:

1. Technical Competencies:

Networking Configuration: I developed hands-on skills in configuring network devices, routers and switches and designing various network topologies on Cisco Packet Tracer. I learned IP addressing plans, subnetting, and gateway settings which helped me gain a solid foundation in how networks work.

Configuring the Firewall: I learned how to make, manage, firewall (and use in Windows Defender Firewall and other) rules. I was taught how to allow certain traffic (eg. HTTPS (port 443)) whilst blocking others (eg. HTTP (port 80)).

Routing and Switching: I used to be configuring the routing protocols (RIP/OSPF) have been the main job and make inter-network communication or inter-network browsing work to different subnets. With this project I learned routing setting, (static, dynamic) routing and how it affects the network efficiency.

Cyber Security Practices: I deepened my knowledge of Cyber Security concepts such as vulnerabilities, patches, and intrusion detection system at all. I utilized security tools to identify and resolve threats and maintain the integrity of the network.

Setting up DNS and DHCP: I set up the DNS servers and DHCP servers for several different subnets, so I could learn how devices on a network can communicate with each other using domain names and obtain IP addresses automatically.

Setting up a Wireless Network: I learnt about configuring wireless networks, i.e., creating an SSID, enabling WPA2 security and secure access to mobile devices in the office network.

2. Soft Skills Competencies:

Communication: Working with my team and joining meetings helped me learn how to turn technical jargon into plain language for coworkers who aren't engineers. I began writing reports that explain set-up steps and security tips, trying often to keep them clear and to the point.

Team Collaboration: I got to work alongside people from both tech and non-tech backgrounds. It showed me that open talks and sharing what you know can really push a project forward. Sometimes the chat felt messy, yet the results were better.

Problem-Solving: Digging through logs let me find network or security glitches. Under pressure I had to think, come up with fixes, and test them quickly. The experience may mean I can handle real-world issues with speed.

Project Management: Juggling several tasks at once forced me to sort priorities. I learned to meet deadlines without dropping quality, though slip-ups happen.

3. Professional Competencies:

Attention to Detail: Setting up the networks and firewalls reminded me to: Pay closer attention to minor details. A little misconfiguration in the file can result in big problems in the network, so care was a big issue.

Adaptability: Needless to say, the trials and projects were constantly changing and I had to grow and learn new tools and new problems with them. I learned how to learn on the fly and make it applicable to anything I was doing.

4.2 SMART Plan

With regard to extending my career and the competences achieved in my internship, I have developed a SMART plan. This plan provides clear and realistic, related, timely objectives for my personal and professional development.

Specific Goals:

Get A Cyber Security Certification:

Obtain a CompTIA Security certification, to further explore the basics of Cyber Security and to show I know it.

Become proficient in Network Automation:

Do not rely on only network devices to do network automation, rather develop skills in network automation with tools like Ansible or Python scripts to automate your network configuration and management.

Learn Cloud Security:

Get certified in Cloud Security, for example AWS Certified Security Specialty, to learn how to secure cloud infrastructure.

Measurable Goals:

- Achieve CompTIA Security+ certificate in the next 6 months.
- Automate a minimum of three networking functions with a Python script within 3 months.
- To attend 2 Cloud Security workshop in the next 1 years in other to have more in-depth understanding on how to secure cloud service.

Achievable Goals:

- Set aside 5-6 hours each week for self-study towards certification exams.
- Join local or virtual communities and forums on network automation and cloud security to learn from peers and industry pros.
- Hands-on projects and labs: practice your automation and cloud security configuration skills.

Relevant Goals:

· As a would be Cyber Security expert, they intersect with the trajectory of my career and help me to the next level in security of both enterprise networks, systems and cloud infrastructure.

• Network automation skills will help me work faster and better with network setups and maintenance, while knowledge of cloud security will allow me to address novel security threats within cloud setups.

Time-bound Goals:

- Obtain CompTIA Security+ certificate by March 2026.
- Write Python scripts with network automation in mind by the next 3 months.
- Get Certified in Cloud Security before June 2026.

4.3 Reflection

Looking back at my working experience in Goinnovior Limited, I feel so satisfied with what I have learned, both technically and personally. My practical experience on several networking and security projects has cemented the concepts I had during the academia.

The hands-on aspect of configuring firewalls, network design, routing and switching are all skills that I can take into real world application. Being able to set up and work with networks, debug with security and be surrounded by a great mixed team was incredible. All those works made me to a technical specialist and helped me to learn also the importance of communication, team work and focus on details and openness.

I also learned that being flexible is key in IT. Technology is always advancing and my ability to learn and apply new skills will be important in my future. The internship made me understand the importance of keep learning and developing, as the technology sector is never going to stop.

It also really opened my eyes to the importance of Cyber Security in the world today. due to the threat of a cyberattack or data breach, I am incredibly motivated now to enter into this field and develop innovative solutions that will safe guard both organizations and individuals.

I can now face hard responsibilities and be a worthy member in IT and Cyber Security fields. What has my experience.... at Goinnovior Limited taught me: I am ready to achieve certifications, gain further technical knowledge and constantly develop as an IT professional in a competitive sector.

CHAPTER 5

CONCLUSION AND FUTURE CAREER

5.1 Discussion and Conclusion

I have got to let you know that, while I was undergoing my internship at the Goinnovior Limited, l as came a far a valuable check. Between real world tasks, professional development and practical exercises I now have a substantial amount of knowledge within IT and Cyber Security. Reflecting on my own journey, I have a few big takeaways:

Practical Application of Theoretical Knowledge

I knew the knowledge of books regarding on the networking and Cyber Security when I have taken these classes before my internship period. But then when I ran a real-world task like the Office Network Design and AWS NACL and SECURITY GROUP Configuration, that compelled me to fit this pattern into the real use case. These fifteen projects have given me a better understanding about network optics, security protocols in networking and also handling of network traffic.

I.E Planning the office network taught me how to put in practice IP addressing, subnetting, and routing; Configuring the firewall showed me how to block some traffic (such as HTTP) for securing the network. That meant not only getting better at the technical side of things, but also learning what kinds of problems companies are grappling with when they try to secure their most valuable technology.

Team Collaboration and Communication

The biggest lesson that I have taken away from my internship is the importance of working together with others in order to communicate efficiently. I might have had things to do, but a large part of the success of those projects had been how well I'd worked with people working on me with the respective project. Developed my ability to communicate technical ideas to both technical and non-technical staff in meetings, Q & A sessions, and resolution of issues.

The groupwork also helped me understand how to and hold my end in different ways really facilitated multicultural teams. It’s a great skill to have, the value of working with others, giving and taking knowledge and supporting one another and being part of contributing to the success of everyone else is a good lesson I can take from my time here.

Problem-Solving and Critical Thinking

Another skill I developed during my intern, was being able to recognize a problem and solve it. During the internship, I had a lot of puzzles where I really had to think and use problem solving. Whether the challenge was isolating a more or less random networking problem, or running down a hole in the firewall rule base, I needed a methodic approach to finding solutions. That's also how I was able to develop my expertise in the face of constraints and figure out creative technical solutions.

Adaptability to Evolving Technologies

Cyber Security is not static – the domain changes all the time (new tech, tools, threats). As an intern, I realized its importance of being up-to-date on those differences. The longer I pursued new security tools and techniques an IT truth started to emerge that waiting in one place is a losing proposition. This exposure is what has compelled me to keep learning all the time and be as updated as possible with the latest trends in the industry.

5.2 Scope for Future Career

Goinnovior Limited My internship at Goinnovior Limited has set me up with the foundation for a career in Cyber Security and Network Administration. The show has provided me with the next best thing and made me aware of how I want to spend the rest of my professional life. Here are a few of the places where I think there is tremendous potential to grow and career-uplift:

Cyber Security Specialist

"As a Cyber Security Specialist, my goal is to safeguard companies against digital attacks through my expertise in developing and managing security provisions. I intend to take certifications like CompTIA Security+, Certified Information Systems Security Professional (CISSP) and Certified Ethical Hacker (CEH) to enhance my competency in this area. The knowledge I acquired on firewall settings, detection of threats, network securities during my internship provides a strong basis for this career.

Network Architect

Another possible job role is to become a Network Architect. In it I'd be creating and deploying some advanced network architectures. The experience at my internship working with an office network with several subnets, routers, and security settings will give me an edge in this position. I will gain competence in network protocols, routing and network performance tuning by taking specific training and certification courses.

Cloud Security Engineer

The dependence on cloud technology is rising, and consequently so is the need for experienced Cloud Security Engineers. "I'd be responsible for securing the cloud systems and applications." As the adoption of cloud services continues to grow in enterprises, Cloud Security certifications such as AWS Certified Security Specialty and Google Cloud Professional Cloud Security Engineer will be critical to move forward in Cloud Security. My love for cloud networking and cloud security, which I have just begun experimenting during the internship, will lead at this path.

Network Automation

I think that there is a big opportunity in this area as network automation becomes a typical part of an IT workers duties. By learning to automate network configuration and management, with tools like Ansible and even Python to script elements together, I want to make processes more efficient and strive for network optimization. It will be by chiseling away at the scripting know-how I gained on my internship, applied to this new domain.

Career Development Plan

To maintain my professional development, I have got a number of career building goals:

- Short-term goal (1-2 years): Achieve certificates in CompTIA Security+ and AWS Certified Security Specialty.
- Mid-term target (3-5 years): Work in the capacity of a Cyber Security Analyst or Network Engineer, in the process learn more about cloud security and network automation.
- Longer-term goal (5+ years+): Achieve higher-level positions like Security Architect or Network Architect and continue to be in charge of teams and manage enormous IT infrastructure projects.

Staying Up-to-Date

With new technologies being developed virtually overnight I will always be learning the latest tools & techniques, and the newest areas of focus in Cyber Security & Network Design. This would mean attending conferences, workshops, webinars as well as any advance certifications in order to remain competitive in the competitive IT environment.

References

[1] W. Stallings, *Network Security Essentials: Applications and Standards*, 6th ed. Pearson, 2017.

[2] A. S. Tanenbaum and D. J. Wetherall, *Computer Networks*, 5th ed. Pearson, 2013.

[3] J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*, 8th ed. Pearson, 2021.

[4] B. A. Forouzan, *Data Communications and Networking*, 5th ed. McGraw-Hill, 2017.

[5] Cisco Systems, "Cisco Packet Tracer – Networking Simulation Tool," Cisco Networking Academy. [Online]. Available: https://www.netacad.com/courses/packet-tracer.

[6] J. Postel, "Internet Protocol," RFC 791, IETF, Sept. 1981. [Online]. Available: https://www.rfc-editor.org/rfc/rfc791.

[7] J. Moy, "OSPF Version 2," RFC 2328, IETF, Apr. 1998. [Online]. Available: https://www.rfc-editor.org/rfc/rfc2328.

[8] Microsoft, "Windows Defender Firewall with Advanced Security," Microsoft Docs. [Online]. Available: https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall.

[9] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST Special Publication 800-94, Feb. 2007.

[10] L. Chappell, *Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide*, Protocol Analysis Institute, 2017.

[11] Sophos, "Sophos XG Firewall: Technical Overview," 2024. [Online]. Available: https://www.sophos.com.

[12] Fortinet, "FortiGate Firewall Technical Documentation," 2024. [Online]. Available: https://www.fortinet.com/resources.

[13] CompTIA, "CompTIA Security+ Certification Exam Objectives," 2024. [Online]. Available: https://www.comptia.org.

[14] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 8th ed. Pearson, 2020.

[15] Wikipedia, "Software-defined networking," Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/Software-defined_networking.

APPENDIX

Introduction

Internship is to find out and perceive the real word activity, applications and implementation of the theories of the study. this can be a scope to figure for the scholars provided by the university and also the corporations before getting into the job market to grasp the real-world operating surroundings. this can be a true chance for students to correct themselves for the long run operating life.

Learning throughout spot

I have learned these things that are mentioned below throughout the spot within the Goinnovior Limited.

Discipline

From this internship I've got learned discipline that is extremely abundant vital. I've got learned the way to be disciplined within the company surroundings. however, the operating time and workplace ought to be followed and maintained I learned from spot. it's vital I did satisfy the discipline conjointly.

Team Work

Team work is extremely abundant vital for any style of work. No better service may be provided while not a higher team work. a higher synchronization it's conjointly a interest understand how to grasp team members and how to follow them for the most effective synchronization of labor.

Understanding Responsibilities

All types of job come with responsibilities which has to be happy. Face any sure scenario and manage it using ability. Senior team members created me perceive those and support me to satisfy the responsibilities of the task at scenario. I've got learned several things from my superiors.

To be skilled

Have a higher service it's required to own perfection within the work. And it's not possible to own perfection within the job while not skilled and correct operating perspective. it had been completely tutored by the senior member of the team.

CERTIFICATE

goinnovior

Mr. IZAZ MAHMUD
House-774, Road-11, Avenue-02, Mirpur
DOHS Dhaka-1216, Bangladesh

To Whom It May Concern

This is to certify that **IZAZ MAHMUD** successfully completed a 4-month internship as a **Cyber Security** at Goinnovior Limited from **10th August 2024 to 10th December 2024**.

During the course of the internship, **IZAZ MAHMUD** displayed a high level of dedication, enthusiasm, and commitment to his role. He actively contributed to the Cyber Security team by assisting in the configuration, troubleshooting, and maintenance of the company's Cyber Security infrastructure. Their responsibilitiesincluded identifying Cyber Security issues, implementing solutions, and collaborating with team members to optimize Cyber performance.

IZAZ MAHMUD demonstrated a solid understanding of Cyber Security concepts and protocols, and they effectively applied their knowledge to resolve various technical challenges. They exhibited excellent problem-solving skills, tackling complex issues with a systematic and analytical approach. His ability to work both independently and as part of a team was commendable.

Throughout the internship, **IZAZ MAHMUD** exhibited strong communication skills when interacting with colleagues and supervisors. He was able to conveytechnical information clearly and concisely, facilitating effective collaboration and knowledge sharing within the team.

We wish **IZAZ MAHMUD** all the best in their future endeavors and have no doubtthat he will continue to excel in their career in the field of Cyber Security.

Sincerely,

GOINNOVIOR DHAKA, BANGLADESH

Kahafil Ora
Managing Director,
Goinnovior Limited

+8801844-185480
+8801844-185485
www.goinnovior.com
info@goinnovior.com
House-774, Road-11, Avenue-02
Mirpur DOHS, Dhaka - 1216, BD

CERTIFICATE
OF COMPLETION

Certificate No: SJ/CS-20240100021

Registration No: 240100021

CERTIFICATE IN

Cyber Security

is Awarded to

IZAZ MAHMUD

Son/Daughter of

Mr. G M Hasan Mahmud & Ms. Khorsheda Akter

for having achieved the following units of competency through Virtual training program 4 month's held from 10/08/2024 to 10/12/2024 at skill jobs.

Trainer

CEO, Skill Jobs

Issue Date: January 18, 2025

Match Groups

- 57 Not Cited or Quoted 17%
  Matches with neither in-text citation nor quotation marks
- 0 Missing Quotations 0%
  Matches that are still very similar to source material
- 0 Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- 0 Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

15% Internet sources
5% Publications
12% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Internet dspace.daffodilvarsity.edu.bd:8080	10%
2	Internet 123dok.com	<1%
3	Submitted works Daffodil International University on 2019-05-22	<1%
4	Submitted works Polytechnic Institute Australia on 2025-09-14	<1%
5	Submitted works Daffodil International University on 2019-05-22	<1%
6	Submitted works University of Central Lancashire on 2024-04-11	<1%
7	Publication Yuxin Meng, Lam-for Kwok, "A Generic Scheme for the Construction of Contextua...	<1%
8	Submitted works Middle East College on 2025-06-23	<1%
9	Submitted works University of East London on 2025-01-13	<1%
10	Submitted works RMIT University on 2025-09-20	<1%

23% detected as AI

The percentage indicates the combined amount of likely AI-generated text as well as likely AI-generated text that was also likely AI-paraphrased.

Caution: Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Detection Groups

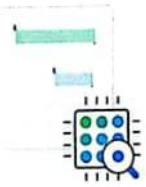
35 AI-generated only 23%
Likely AI-generated text from a large-language model.

0 AI-generated text that was AI-paraphrased 0%
Likely AI-generated text that was likely revised using an AI-paraphrase tool or word spinner.

Disclaimer
Our AI writing assessment is designed to help educators identify text that might be prepared by a generative AI tool. Our AI writing assessment may not always be accurate (it may misidentify writing that is likely AI generated as AI generated and AI paraphrased or likely AI generated and AI paraphrased writing as only AI generated) so it should not be used as the sole basis for adverse actions against a student. It takes further scrutiny and human judgment in conjunction with an organization's application of its specific academic policies to determine whether any academic misconduct has occurred.

Frequently Asked Questions

How should I interpret Turnitin's AI writing percentage and false positives?
The percentage shown in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was either likely AI-generated text from a large-language model or likely AI-generated text that was likely revised using an AI paraphrase tool or word spinner.



False positives (incorrectly flagging human-written text as AI-generated) are a possibility in AI models.

AI detection scores under 20%, which we do not surface in new reports, have a higher likelihood of false positives. To reduce the likelihood of misinterpretation, no score or highlights are attributed and are indicated with an asterisk in the report (*%).

The AI writing percentage should not be the sole basis to determine whether misconduct has occurred. The reviewer/instructor should use the percentage as a means to start a formative conversation with their student and/or use it to examine the submitted assignment in accordance with their school's policies.

What does 'qualifying text' mean?
Our model only processes qualifying text in the form of long-form writing. Long-form writing means individual sentences contained in paragraphs that make up a longer piece of written work, such as an essay, a dissertation, or an article, etc. Qualifying text that has been determined to be likely AI-generated will be highlighted in cyan in the submission, and likely AI-generated and then likely AI-paraphrased will be highlighted purple.

Non-qualifying text, such as bullet points, annotated bibliographies, etc., will not be processed and can create disparity between the submission highlights and the percentage shown.