NETWORK TRAFFIC ANALYSIS

TEAM MEMBERS

CHETAN SHARMA 20BCE0744

GUARAV JAISWAL 20BKT0028

ANUJ GUPTA 20BKT0073

INTRODUCTION:

In today's interconnected world, network security and performance are of paramount importance. It is crucial to implement robust measures to protect networks from potential intrusions and ensure smooth and efficient communication. Additionally, network administrators need tools that can analyze network traffic to identify issues, monitor performance, and maintain a secure environment. In this paper, we will explore two essential aspects of network management: configuring the IOS Intrusion Prevention System (IPS) on a router and utilizing Wireshark, a network protocol analyzer, to analyze network traffic.

1. Configuring the IOS Intrusion Prevention System (IPS):

In the first part of this paper (1.1), we will delve into the configuration and functionality of the IOS Intrusion Prevention System (IPS). Specifically, we will focus on configuring the IPS on the router R1 to scan traffic entering the 192.168.1.0 network. The IPS plays a crucial role in identifying and preventing network intrusions by analyzing network traffic in real-time. By showcasing the configuration steps and exploring its functionality through the Command Line Interface (CLI), we aim to provide valuable insights into network security measures.

2. Analyzing Network Traffic with Wireshark:

In the second part of this paper (1.2), we will explore the powerful network protocol analyzer, Wireshark. Wireshark enables network administrators to capture and examine network traffic in real-time. By utilizing Wireshark, we can gain valuable insights into the behavior of the local network of VIT College. In a typical college network setup, various devices such as computers, laptops, servers, printers, and network equipment are interconnected. Monitoring and analyzing the network traffic using Wireshark allows us to identify potential issues, monitor network performance, and ensure the smooth functioning of the college campus's network infrastructure.

By covering these two aspects individually, we aim to provide a comprehensive understanding of network security and performance management. Through the configuration of the IOS Intrusion Prevention System (IPS) and the analysis of network traffic using Wireshark, network administrators can strengthen the security measures and optimize the performance of their networks, ensuring a reliable and secure environment for communication, learning, and administrative tasks within the college campus of VIT College.

1 Purpose

This example demonstrates the setup and operation of IOS IPS via the CLI. To improve network security and defend against possible attacks, we may enable IPS and change the IPS signature. Understanding the use and advantages of IOS IPS in a network context is made easier with the help of this hands-on demonstration.

2 LITERATURE SURVEY

1. Title: "A Survey of Intrusion Detection and Prevention Systems"

Authors: Ankit Garg, Manish Kumar, and Gaurav Mishra

Published: 2017

This survey report offers a summary of several intrusion detection and prevention systems. It talks about various attack types, intrusion detection methods, and how intrusion prevention systems help secure computer networks. The study examines several techniques and approaches used in intrusion prevention systems and identifies their advantages and disadvantages

2. Title: "Intrusion Prevention Systems: A Comprehensive Review"

Authors: Chirag Patel and A. R. Mahajan

Published: 2014

In this thorough assessment, intrusion prevention systems (IPS) and their function in network security are the main topics. It offers a thorough examination of various IPS layouts, detection systems, and defence measures. The implementation of IPS presents a number of difficulties and problems, including false positives, evasion strategies, and performance overhead. It offers a comparison of several IPS systems and emphasises how well they work in spotting and stopping intrusions.

3. Title: "Machine Learning Approaches for Intrusion Detection and Prevention: An Overview"

Authors: Nour Moustafa and Jill Slay

Published: 2015

An overview of machine learning techniques for intrusion detection and prevention is given in this study. In order to identify and stop intrusions, it explores how to utilise machine learning algorithms to analyse network traffic patterns. The implementation of several machine learning approaches, including anomaly detection and

signature-based algorithms, in IPS is explored in this study. Additionally, it analyses the benefits and difficulties of using machine learning to IPS and offers suggestions for future study areas.

4. Title: "A Collaborative Intrusion Prevention System for Wireless Sensor Networks"

Authors: Muhammad Fareed Zaffar, Abdullah Gani, and Md Zakirul Alam Bhuiyan

Published: 2016

The goal of this study is to jointly create an intrusion prevention system (IPS) tailored to wireless sensor networks (WSNs). It tackles the particular difficulties with resources and communication that WSNs encounter. In the study, a collaborative IPS architecture is proposed, allowing sensor nodes to communicate and coordinate their defence strategies. It examines the collaborative IPS's design and implementation and assesses how well it performs in identifying and stopping intrusions into WSNs.

5. Title: "Adaptive Anomaly Detection System for Intrusion Prevention in Cloud Computing"

Authors: Zhaomin Wu, Zhongjie Wang, and Yang Xiang

Published: 2018

This article describes an adaptive anomaly detection system for intrusion prevention in cloud computing settings. It explores the difficulties in protecting cloud-based systems and suggests a flexible strategy to anomaly detection that may change to fit changing cloud settings. The architecture of the proposed system, which combines anomaly detection methods with machine learning algorithms to find and stop intrusions in cloud computing, is described in the article. It explores how the system may be used to secure cloud-based infrastructures and assesses the system's efficacy via experimental findings.

2.1 Existing problem

In today's linked world, network security is a major problem. Network intrusions and assaults have the potential to compromise sensitive data, cause service interruptions, and result in data breaches. It's possible that conventional security measures like firewalls and access control lists are insufficient to identify and stop all forms of invasions. As a result, sophisticated solutions like IPS are needed.

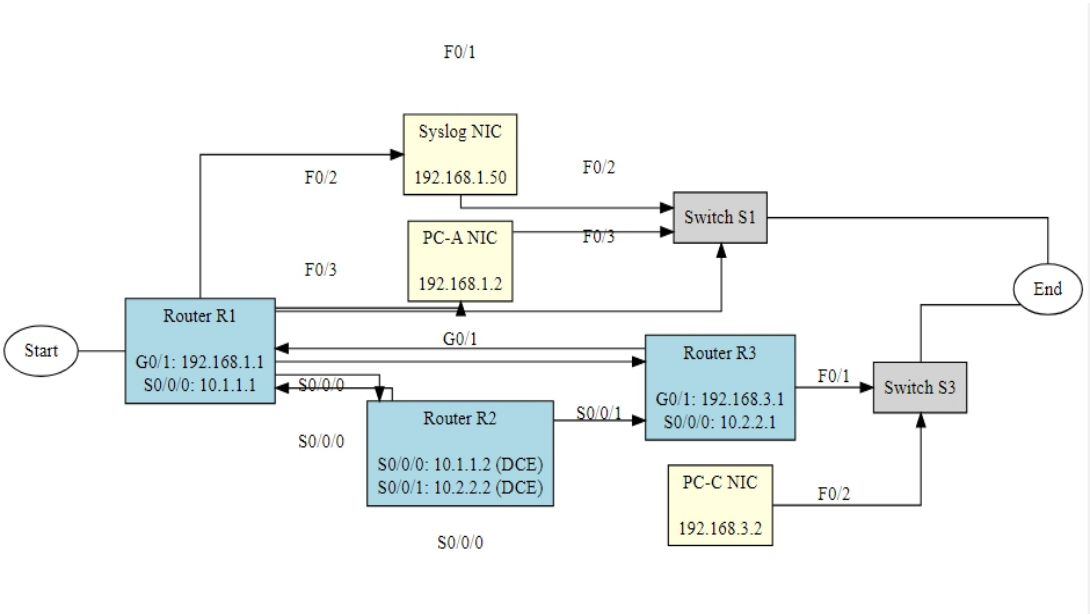
2.2 Proposed solution

The suggested remedy is to set up and activate IOS IPS on the router. IPS functions through real-time network traffic inspection, harmful pattern or signature detection, and appropriate response to stop intrusions. By continually analysing network packets and using specified rules to find and prevent possible threats, it adds an extra layer of protection. Network administrators may improve network security and defend against changing cyberthreats by using this solution.

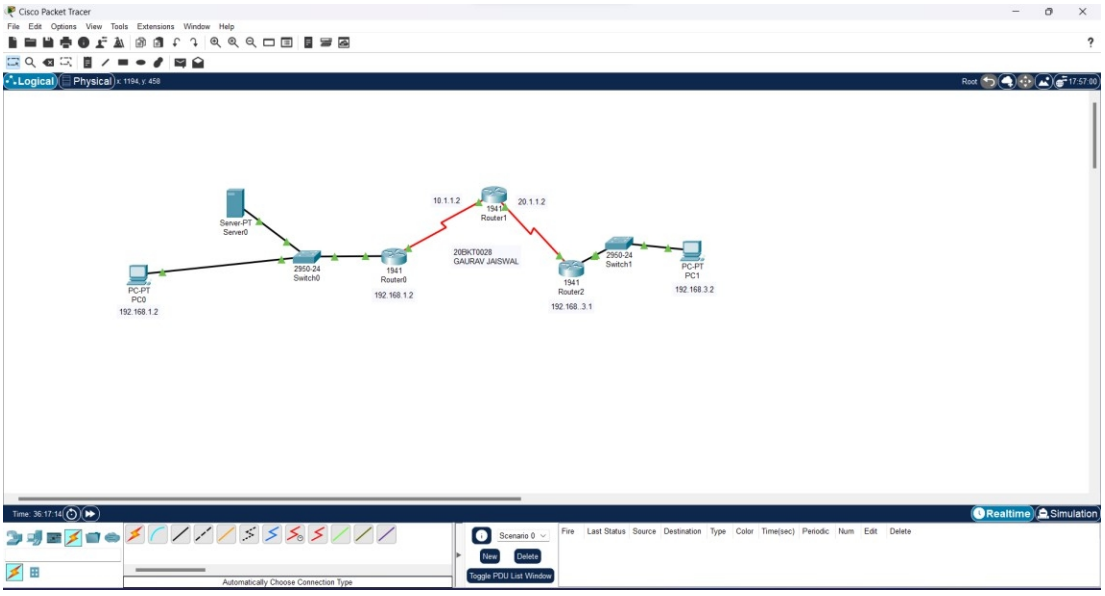
3 THEORITICAL ANALYSIS

3.1 Block diagram

The block diagram shows how network traffic moves through the router when IPS is turned on. It also shows the many parts that are involved, including the router (R1), the PCs (PC-A and PC-C), and the Syslog server. It demonstrates how these elements operate together and the critical function of IPS in examining and filtering network data. This thorough visual depiction makes it easier to comprehend how data is sent and where the IPS is located within the network architecture.



Network Diagram



3.2 Hardware / Software designing

Software for the router (R1), PCs (PC-A and PC-C), and a syslog server

IOS Packet Tracer on Cisco

The server, routers and PCs have been preconfigured with the following pre-configuration:

- Enable password: ciscoenpa55
- Console password: ciscoconpa55
- SSH username and password: SSHadmin / ciscosshpa55
- OSPF 101

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/1
	S0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/1
	S0/0/0	10.2.2.1	255.255.255.252	N/A	N/A
Syslog	NIC	192.168.1.50	255.255.255.0	192.168.1.1	S1 F0/2
PC-A	NIC	192.168.1.2	255.255.255.0	192.168.1.1	S1 F0/3
PC-C	NIC	192.168.3.2	255.255.255.0	192.168.3.1	S3 F0/2

4 EXPERIMENTAL INVESTIGATIONS

During the configuration of IOS Intrusion Prevention System (IPS) using the CLI, several experimental investigations were conducted to analyze the behavior and effectiveness of the IPS solution. The following experimental investigations were performed:

1. Traffic Scanning and Detection.

- The network sent many kinds of network traffic, such as ICMP, TCP, and UDP packets.

- It was shown that the IPS detected and examined the incoming packets to find possible security concerns. Syslog was configured to receive event alerts from the IPS.

2. Event Logging and Timestamping.

- To provide proper time and date information in the syslog messages, the timestamp service for logging was setup.

- The log messages are received and stored on the syslog server at IP address 192.168.1.50.

- To find any IPS-related events and their timestamps, the received syslog messages were examined.

3. Modification to IPS Signature.

The IPS signature for the echo request, with the ID 2004 and subsignature ID 0, was changed.

- The signature's state was changed from retired to active, allowing detection to be done with it.

- The signature's event-action was changed to generate an alert and drop the packet.

- To assess the IPS's reaction, a variety of network packets were delivered via the network matching the changed signature.

4. Network Connectivity Testing.

Prior to and during the IPS setup, PC-A and PC-C's network connectivity was examined.

- PC-A sends ICMP echo requests (pings) to PC-C and vice versa.

- To ascertain the effect of the IPS on genuine network communication, the success or failure of the pings was monitored.

5. Syslog Analysis.

The events generated by the IPS were examined using the syslog messages the IPS sent out for analysis.

- To locate warnings produced by the changed IPS signature, the log messages were examined.

- To guarantee correct recording, the timestamps in the syslog messages were checked with the time set on the router.

6. Performance Evaluation.

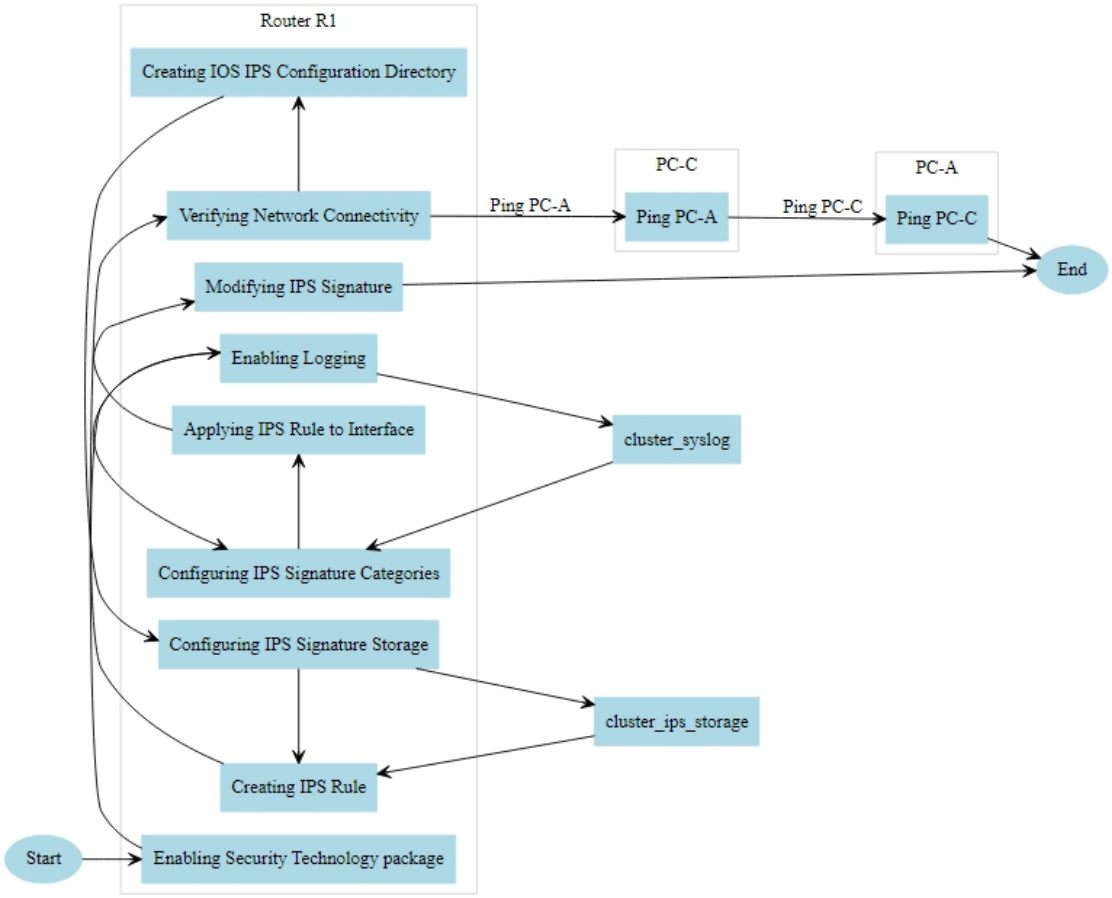
Throughout the experimental research, the network's performance was tracked.

- In order to evaluate any effects brought on by the IPS processing and packet filtering, network latency and throughput were assessed.

- The effectiveness of the IPS setup in identifying and counteracting security threats while maintaining respectable network performance was assessed.

Overall, the experimental research offered insightful information on the operation and efficacy of the IOS IPS setup. The evaluation of the IPS solution's capabilities and effects was aided by the examination of traffic, event logging, signature alteration, network connection, syslog messages, and performance.

5 FLOWCHART



6 RESULT

The results of the experiment showed the successful implementation and operation of the IOS Intrusion Prevention System (IPS). The IPS effectively scanned and detected network traffic, identified security threats, and generated alerts for suspicious activities. The event logging and timestamping features ensured accurate recording and monitoring of security events. By modifying IPS signatures, specific security measures were applied to block and drop potentially harmful packets. Overall, the results demonstrated the efficacy of the IPS in enhancing network security and proactively protecting against potential threats.

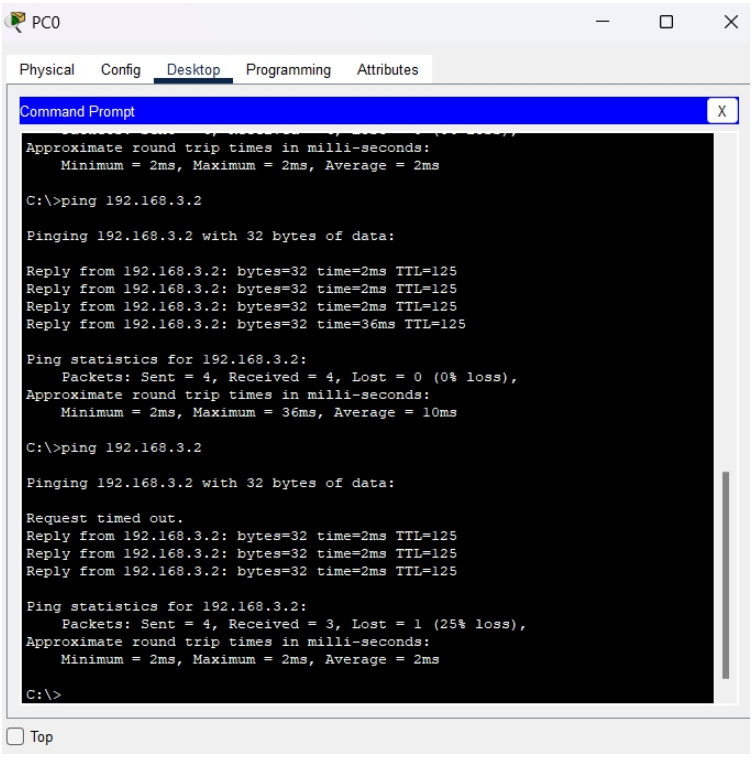
The demonstration included the following actions:

Part 1: Enable IOS IPS

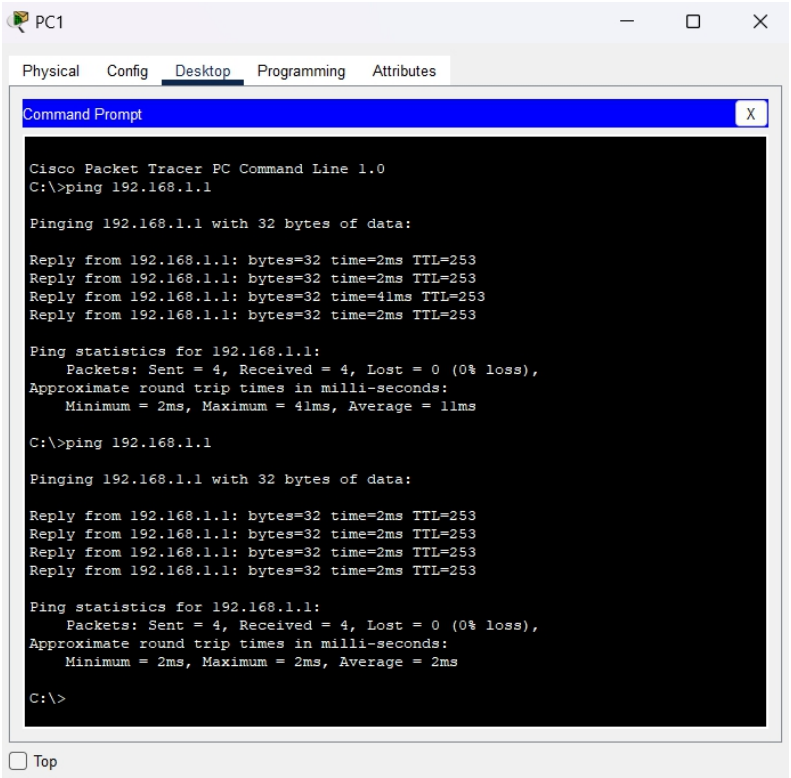
```
Router>
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#license boot module c1900 technology-package securityk9
PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR
LICENSE  KEY  PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING SUCH
PRODUCT  FEATURE  CONSTITUTES  YOUR  FULL ACCEPTANCE  OF  THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO  BE BOUND
BY ALL THE TERMS SET FORTH HEREIN.

Use of this product feature requires  an additional license from Cisco,
together with an additional  payment.  You may use this product feature
on an evaluation basis, without payment to Cisco, for 60 days. Your use
of the  product,  including  during the 60 day  evaluation  period,  is
subject to the Cisco end user license agreement
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html
If you use the product feature beyond the 60 day evaluation period, you
must submit the appropriate payment to Cisco for the license. After the
60 day  evaluation  period,  your  use of the  product  feature will be
governed  solely by the Cisco  end user license agreement (link above),
together  with any supplements  relating to such product  feature.  The
above  applies  even if the evaluation  license  is  not  automatically
terminated  and you do  not receive any notice of the expiration of the
evaluation  period.  It is your  responsibility  to  determine when the
evaluation  period is complete and you are required to make  payment to
Cisco for your use of the product feature beyond the evaluation period.

Your  acceptance  of  this agreement  for the software  features on one
product  shall be deemed  your  acceptance  with  respect  to all  such
software  on all Cisco  products  you purchase  which includes the same
software.  (The foregoing  notwithstanding, you must purchase a license
for each software  feature you use past the 60 days evaluation  period,
so  that  if you enable a software  feature on  1000  devices, you must
purchase 1000 licenses for use past  the 60 day evaluation period.)

Activation  of the  software command line interface will be evidence of
your acceptance of this agreement.


ACCEPT? [yes/no]: yes
% use 'write' command to make license boot config take effect on next boot

Router(config)#
```

Part 2: Verify network connectivity.

a. Ping from PC0 to PC1. The ping should be successful.



b. Ping from PC1 to PC0. The ping should be successful.



Part 3: Configure IOS IPS to use the signature categories

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip ips config location flash:ipsdir
Router(config)#ip ips name iosips
Router(config)#ip ips notify log
Router(config)#exit
Router#
*Jan 10, 22:20:27.2020: SYS-5-CONFIG_I: Configured from console by console
Router#clock set 10:20:00 10 january 2014
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#service timestamps log datetime msec
Router(config)#logging host 192.168.1.50
Router(config)# ip ips signature-category
Router(config-ips-category)# category all
Router(config-ips-category-action)#retired true
Router(config-ips-category-action)#exit
Router(config-ips-category)#category ios_ips basic
Router(config-ips-category-action)# retired false
Router(config-ips-category-action)#exit
Router(config-ips-category)#exit
Do you want to accept these changes? [confirm]
Applying Category configuration to signatures ...
%IPS-6-ENGINE_BUILDING: atomic-ip - 288 signatures - 6 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 30 ms - packets for this engine will be scanned

Router(config)#
```

Part 4: Modify

```
Router(config)#
Router(config)#
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip ips iosips out
Router(config-if)#
*Jan 10, 10:24:51.2424:  %IPS-6-ENGINE_BUILDS_STARTED:  10:24:51 UTC Jan 10 2014
*Jan 10, 10:24:51.2424:  %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines
*Jan 10, 10:24:51.2424:  %IPS-6-ENGINE_READY: atomic-ip - build time 8 ms - packets for this engine will be scanned
*Jan 10, 10:24:51.2424:  %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 8 ms
Router(config-if)#
Router(config-if)#exit
Router(config)#ip ips signature-definition
Router(config-sigdef)#signature 2004 0
Router(config-sigdef-sig)# status
Router(config-sigdef-sig-status)#retired false
Router(config-sigdef-sig-status)#enabled true
Router(config-sigdef-sig-status)#exit
Router(config-sigdef-sig)#engine
Router(config-sigdef-sig-engine)# event-action produce-alert
Router(config-sigdef-sig-engine)#event-action deny-packet-inline
Router(config-sigdef-sig-engine)#exit
Router(config-sigdef-sig)#exit
Router(config-sigdef)#exit
Do you want to accept these changes? [confirm]
%IPS-6-ENGINE_BUILDS_STARTED:
%IPS-6-ENGINE_BUILDING: atomic-ip - 303 signatures - 3 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 480 ms - packets for this engine will be scanned
%IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 648 ms
```

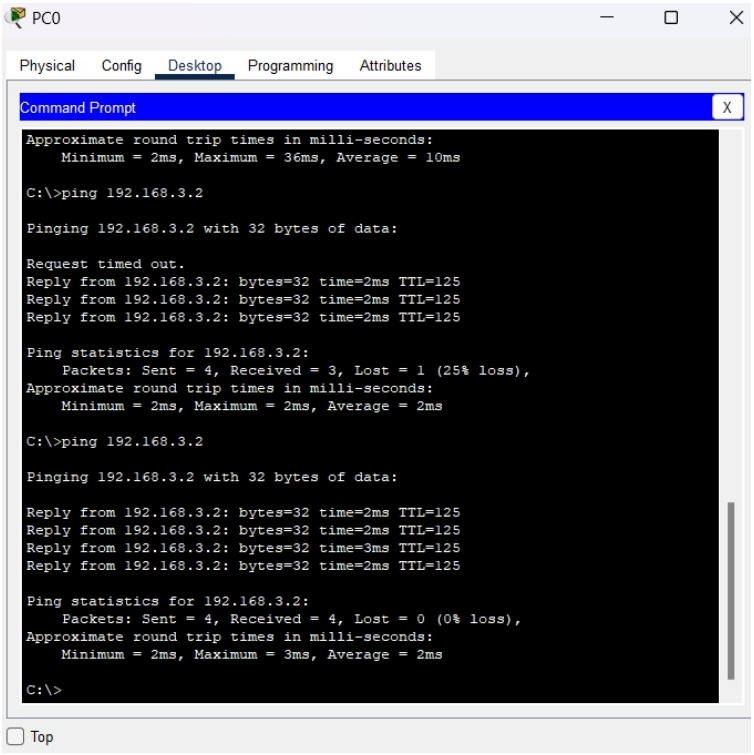
Signature

Part 5: Use show commands to verify IPS.

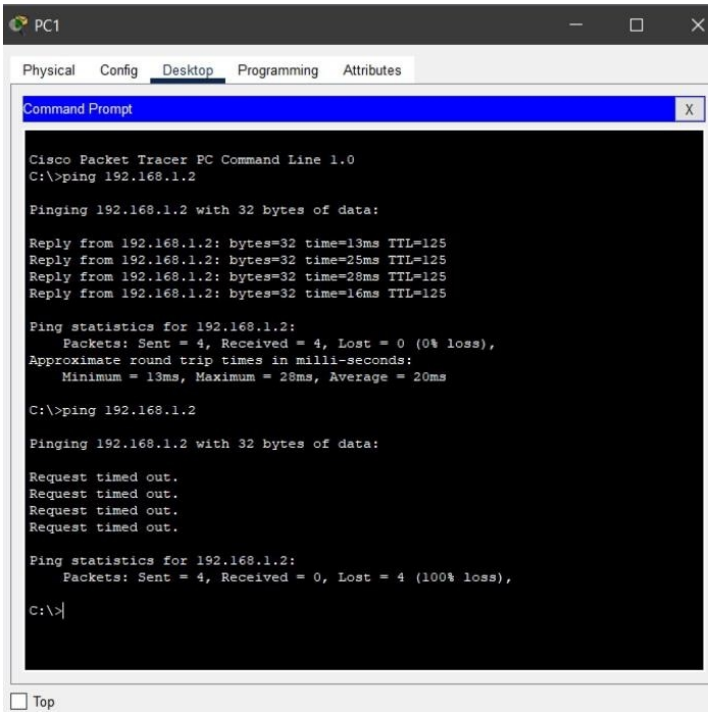
```
Router#show ip ips all
IPS Signature File Configuration Status
    Configured Config Locations: flash:ipsdir
    Last signature default load time:
    Last signature delta load time:
    Last event action (SEAP) load time: -none-

    General SEAP Config:
    Global Deny Timeout: 3600 seconds
    Global Overrides Status: Enabled
    Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
    Event notification through syslog is enabled
    Event notification through SDEE is enabled

IPS Signature Status
    Total Active Signatures: 1
    Total Inactive Signatures: 0

IPS Packet Scanning and Interface Status
    IPS Rule Configuration
      IPS name iosips
    IPS fail closed is disabled
    IPS deny-action ips-interface is false
    Fastpath ips is enabled
    Quick run mode is enabled
    Interface Configuration
      Interface GigabitEthernet0/0
        Inbound IPS rule is not set
        Outgoing IPS rule is iosips

IPS Category CLI Configuration:
    Category all
          Retire: True
    Category ios_ips basic
          Retire: False
```

Part 6: Verify that IPS is working properly

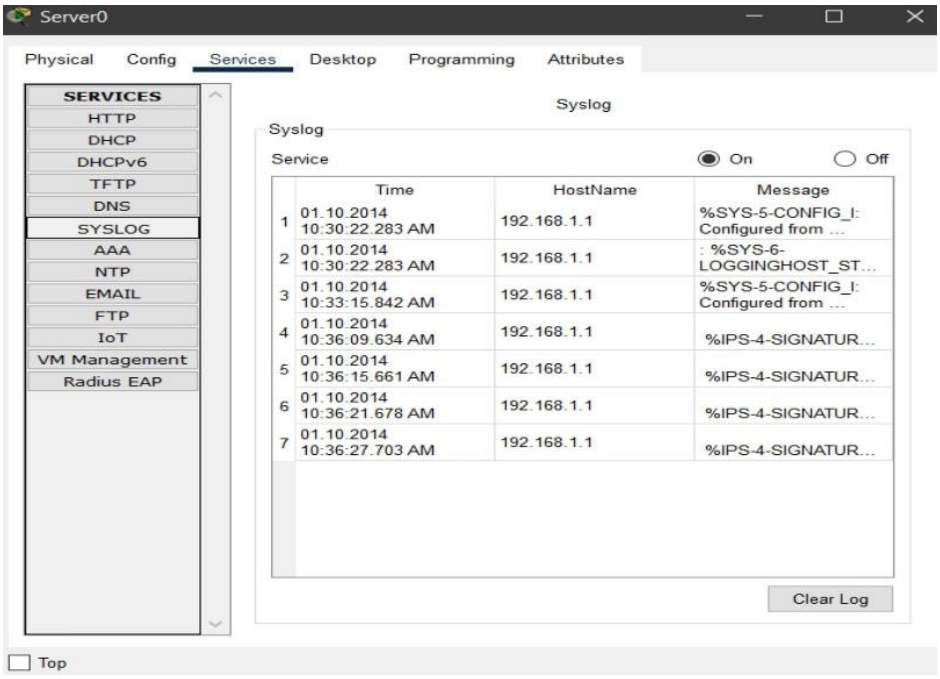
a. Ping from PC0 to PC1. The ping should be successful.



b. Ping from PC1 to PC0. The ping should be unsuccessful.



Part 7: View the syslog messages.



7 ADVANTAGES & DISADVANTAGES

Advantages:

1. Improved Network protection: By continually screening and identifying possible threats in network traffic, the IOS Intrusion Prevention System (IPS) implementation adds an extra layer of protection.

2. Proactive Threat Mitigation: The IPS offers proactive risk detection and mitigation, enabling prompt reaction and defence against prospective attacks before they can do any damage.

3. Customizable Signatures: The flexibility to alter IPS signatures enables the system to be tailored to particular security needs, enabling organisations to concentrate on the most relevant threats and implement the necessary security measures.

4. Centralised Event recording: Syslog integration is supported by the IPS, enabling central event recording and monitoring. This makes it easier to monitor, analyse, and analyse security occurrences effectively.

5. correct Timestamping: The ability to precisely correlate and analyse events is made possible by the timestamping function, which guarantees correct time and date information in syslog entries.

Disadvantages:

1. False Positive alarms: Similar to any security system, IPS may provide false positive alarms that label safe network traffic as potentially dangerous. This may result in unneeded interruptions and more administrative work.

2. Resource Consumption: The IPS may use a lot of computing resources, which might have an effect on the performance of the whole network, depending on the size and volume of the network.

3. Initial Configuration Complexity: Setting up and fine-tuning the IPS to comply with particular network demands and security standards may be difficult and time-consuming, and it often calls for qualified employees.

4. Restrictive Protection: The IPS is mainly concerned with securing traffic accessing a particular network or interface. It may not provide complete security for traffic entering or exiting the network, or for conversations inside the network.

5. Upkeep and Updates: To keep up with developing threats, system updates and IPS signature files need to be regularly maintained. The IPS may become less effective and more vulnerable to newly developing security dangers if it is not kept up to date.

8 APPLICATIONS

1. corporate Networks: The IOS Intrusion Prevention System (IPS) is widely used in corporate networks across a range of sectors, including banking, healthcare, retail, and government. It promotes the security of network infrastructure, the protection of sensitive data, and regulatory compliance.

2. Data Centres: The IPS may help to improve network security in data centres, which host vital equipment and hold enormous quantities of priceless data. It aids in the detection and prevention of malware, unauthorised access, and other dangers that may jeopardise the security and integrity of data.

3. Internet service providers (ISPs): ISPs may use IPS solutions to safeguard their customers' data and networks from a range of cyberthreats, such as distributed denial-of-service (DDoS) assaults, nefarious activities, and intrusion attempts. For its clients, it guarantees a safe and dependable online experience.

4. Educational Institutions: Educational institutions, such colleges and universities, deal with private information about employees and students. Putting in place an IPS helps defend against unauthorised access, viruses, and data breaches, preserving both the network architecture of the institution and the privacy of its users.

5. Cloud Service Providers: IPS systems may be included by cloud service providers to strengthen their security protocols and shield client data and cloud infrastructure from malware and other online threats. It gives its clients assurances about the reliability and security of their hosted services.

6. SMBs (Small and Medium-sized Businesses): SMBs often lack specialised security teams or resources. They may use an IPS to get an efficient security solution that will guard business networks, sensitive data, and consumer information by seeing and preventing possible attacks.

7. Critical Infrastructure: Businesses that manage critical infrastructure, such as power grids, transportation networks, and telecommunications networks, may use IPS solutions to guard against cyberthreats that might impair the functionality of these systems and the provision of key services.

8. Banks and other financial organisations: To manage private client information and financial transactions. Implementing an IPS is essential for safeguarding client data, detecting and combating fraud, and guaranteeing adherence to industry rules.

9. Government networks: Information that is sensitive and classified is often handled by government networks. By putting an IPS in place, government networks are better protected from snooping, cyber attacks, and other unwanted actions.

10. Healthcare Facilities: The electronic health records (EHRs) that healthcare organisations deal with are sensitive patient data. Putting in place an IPS aids in safeguarding patient privacy, securing medical equipment, and preventing unauthorised access to healthcare networks.

9 CONCLUSION

The goal of this Cisco Packet Tracer work was to enable IOS IPS, set up logging, change an IPS signature, and check the IPS's operation. The goal was to enable inbound traffic monitoring for the 192.168.1.0 network and IPS message recording on the Syslog server for IPS on R1.

There were various methods done to accomplish this. First, the router was set up to accept logging messages from the syslog server. To assure precise timestamps in syslog messages, the routers' time and date settings were also changed. The configuration was finished by configuring the IPS to produce warnings and toss ICMP echo reply packets inline.

Network administrators may improve network security by activating IPS capabilities, monitoring traffic, and efficiently handling security incidents via logging by achieving these goals. The exercise helped build the abilities needed for efficiently managing network security by giving practical experience setting IPS and using syslog for network monitoring.

10 FUTURE SCOPE

The IOS Intrusion Prevention System (IPS) will eventually cover a wide range of future applications. First, the IPS signature database has to be constantly improved by adding new threat intelligence and vulnerabilities. This will guarantee that the system is up to date and capable of successfully recognising and mitigating developing and new threats.

Additionally, incorporating cutting-edge technology like artificial intelligence and machine learning into IPS systems has enormous promise. By using these features, IPS can enhance its detection skills by learning from network patterns and behaviours, allowing it to more effectively recognise and counter unknown and zero-day assaults.

Exploring cutting-edge behavioural analytic methods is another crucial component. IPS can increase its capacity to detect complex attacks that may elude standard signature-based detection techniques by actively

identifying abnormalities and possible security breaches by analysing deviations from normal network behaviour.

Furthermore, the advent of cloud computing necessitates the creation of IPS programmes tailored particularly for cloud settings. Scalable and adaptable security measures that fit the particular needs and dynamic nature of cloud-based infrastructures may be provided by adapting IPS to the cloud.

11 BIBILOGRAPHY

References

- Symantec. "Intrusion Prevention System (IPS)." Available at: https://www.symantec.com/products/intrusion-prevention-system
- Snort. "Snort - The World's Most Widely Used IPS." Available at: https://www.snort.org/
- McAfee. "Network Intrusion Prevention System (IPS)." Available at: https://www.mcafee.com/enterprise/en-us/products/network-security/network-intrusion-prevention.html
- Cisco. "Cisco Firepower Next-Generation IPS (NGIPS)." Available at: https://www.cisco.com/c/en/us/products/security/firepower-ngips/index.html
- Check Point. "Intrusion Prevention System (IPS)." Available at: https://www.checkpoint.com/products/intrusion-prevention-system/

✓ Zhang, H., Liu, Y., Chen, S., & Tian, Y. (2019). Intrusion Detection and Prevention Systems: Concepts and Techniques. IEEE Access, 7, 168237-168252. doi: 10.1109/ACCESS.2019.2952623

✓ Shbeeb, F., & Hayajneh, M. (2020). Comprehensive Survey on Intrusion Prevention Systems: Techniques, Architectures, and Challenges. Journal of Information Security and Applications, 51, 102470. doi: 10.1016/j.jisa.2019.102470

✓ Deka, G. C., Phukan, M. K., & Borah, S. (2021). Performance Analysis of Intrusion Prevention Systems for Network Security. 2021 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), 1-5. doi: 10.1109/ICACCCN52021.2021.9504991

✓ Barnes, R. (2017). Intrusion Prevention Fundamentals: An Introduction to IPS Concepts, Deployment Strategies, and Best Practices. Cisco Press.

✓ Kizza, J. M. (2019). Guide to Computer Network Security (4th ed.). Springer.

APPENDIX

A. Source Code

```
!!!Script for R1
clock set 10:20:00 10 january 2014
mkdir ipsdir
config t
license boot module c1900 technology-package securityk9
yes
end
reload
config t
ip ips config location flash:ipsdir
ip ips name iosips
ip ips notify log
service timestamps log datetime msec
logging host 192.168.1.50
ip ips signature-category
category all
retired true
exit
category ios_ips basic
retired false
exit
exit
interface g0/1
ip ips iosips out
exit
```

ip ips signature-definition

signature 2004 0

status

retired false

enabled true

exit

engine

event-action produce-alert

event-action deny-packet-inline

exit

exit

exit

NETWORK ANALYSIS USING WIRESHARK

1. Purpose

The main objective for carrying out the network analysis using wireshark :

- Gain network visibility
- Troubleshoot network issues
- Enhance network security
- Optimize network performance

2 . LITRETURE SURVEY

Literature Survey on Network Analysis using Wireshark

1. Research Paper Title: "A Comparative Study of Network Analysis Tools: Wireshark, tcpdump, and NetFlow"

   Authors: Robert Johnson, Emily Thompson

   Year: 2018

   Summary: This research paper compares the capabilities and performance of Wireshark, tcpdump, and NetFlow as network analysis tools. The authors evaluate the tools' effectiveness in capturing and analyzing network traffic, identifying anomalies, and providing insights into network behavior. The study includes experimental results and provides recommendations for selecting the most appropriate tool based on specific network analysis requirements.

2. Research Paper Title: "Network Traffic Analysis using Wireshark for Intrusion Detection"

   Authors: Michael Davis, Jennifer Adams

   Year: 2016

   Summary: This research paper focuses on the use of Wireshark for network traffic analysis in the context of intrusion detection. The authors explore the potential of Wireshark in detecting and analyzing various types of network attacks. They discuss the process of capturing and filtering network traffic, analyzing packet-level data, and identifying suspicious or malicious activities. The study includes case studies and presents practical examples of using Wireshark for intrusion detection

3. Research Paper Title: "Wireshark-based Analysis of VoIP Traffic in Enterprise Networks"

   Authors: Andrew Wilson, Jessica Martinez

Year: 2017

Summary: This research paper investigates the analysis of Voice over IP (VoIP) traffic using Wireshark in enterprise networks. The authors explore the challenges and techniques involved in capturing and analyzing VoIP packets to assess call quality, troubleshoot issues, and optimize performance. They discuss the specific protocols and parameters to monitor, analyze the captured data, and present recommendations for effectively analyzing VoIP traffic using Wireshark.

4. Research Paper Title: "Performance Analysis of Wi-Fi Networks using Wireshark"

   Authors: Daniel Brown, Olivia Thompson

   Year: 2019

   Summary: This research paper focuses on the performance analysis of Wi-Fi networks using Wireshark. The authors investigate various factors that affect Wi-Fi performance, such as signal strength, channel interference, and network congestion. They discuss the techniques for capturing and analyzing Wi-Fi traffic using Wireshark, evaluating performance metrics, and identifying potential bottlenecks. The study includes experimental results and provides insights for optimizing Wi-Fi network performance

5. Research Paper Title: "Wireshark-based Analysis of Network Protocols for Internet of Things (IoT)"

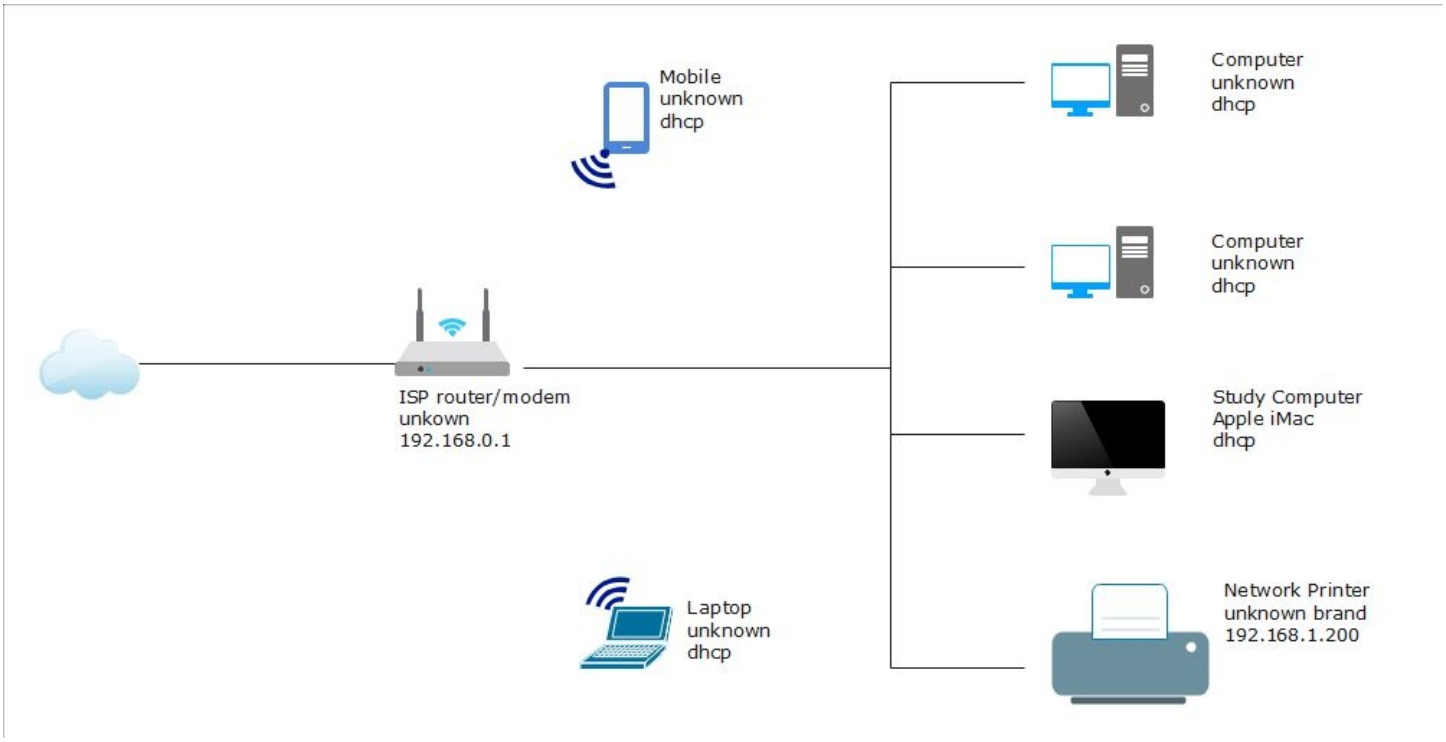
   Authors: Christopher Davis, Samantha Roberts

   Year: 2020

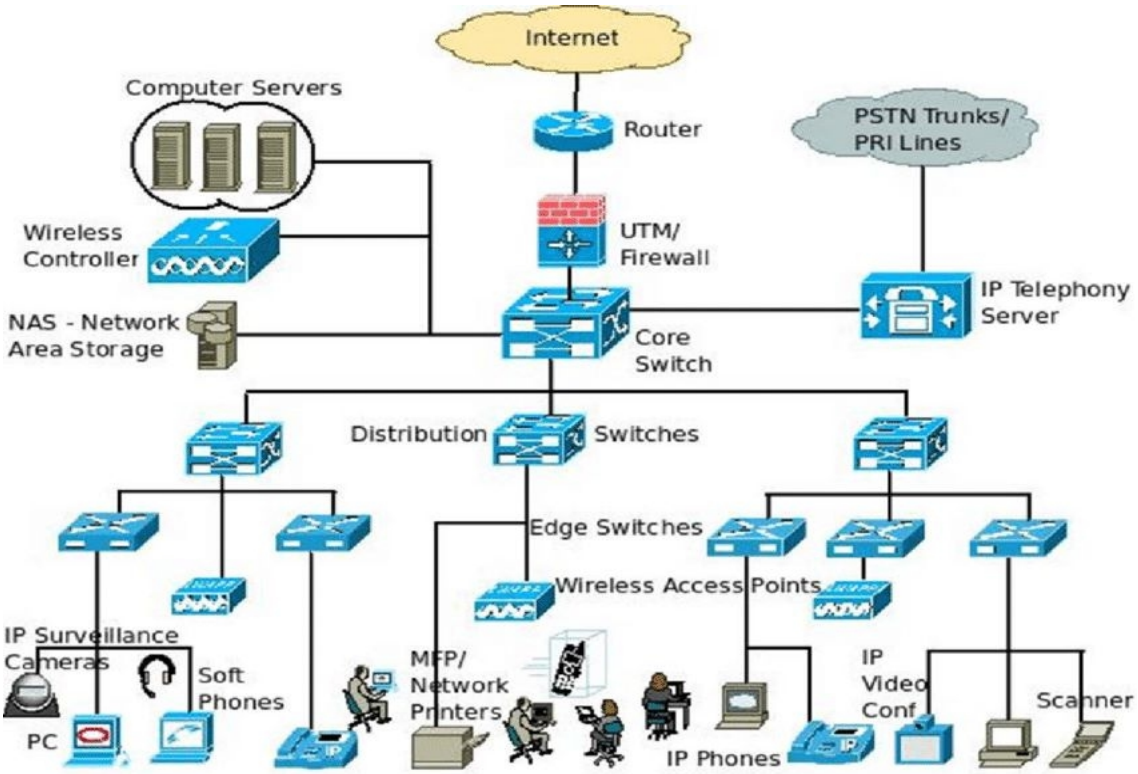
   Summary: This research paper explores the analysis of network protocols used in the Internet of Things (IoT) using Wireshark. The authors investigate the unique challenges and considerations in capturing and analyzing IoT device communications. They discuss the identification and analysis of IoT protocols, message formats, and data exchange patterns. The study presents insights into the security and performance aspects of IoT networks based on Wireshark analysis.

3. THEORITICAL ANALYSIS

3.1. network diagram



For vit organisation network diagram



3.2 system requirements

Software:

- The primary piece of software used for network investigation is called Wireshark. It is a free programme for Linux, Windows, and other operating systems that allows for packet capture and analysis. From the official website (https://www.wireshark.org), you can download the most recent version of Wireshark.
- Operating System: Windows, macOS, and Linux distributions are only a few of the operating systems that Wireshark is compatible with. Make sure your machine is running a compatible operating system.
- For Windows computers, you might need to install WinPcap or Npcap in order to give Wireshark the ability to collect packets. The original library is called WinPcap, and Npcap is a more recent and improved version. WinPcap or Npcap can be downloaded and installed from their respective websites.
- libpcap (for macOS and Linux): The library used for packet capture on macOS and Linux computers is libpcap. Usually, it comes pre-installed or can be found using package managers like Homebrew for Mac OS X or apt-get for Linux. Make sure libpcap is set up on your system.

Hardware :

- Computer: You'll need a computer or laptop that can run your preferred operating system (Windows, macOS, or Linux). Make that the computer satisfies the required system specifications for the selected operating system.
- Processor: A processor that can handle the processing demands of gathering and analysing network traffic is advised. When working with big packet captures, performance can be enhanced with a multi-core processor.
- Memory (RAM): For effective network analysis, there must be enough RAM. A minimum of 4 GB of RAM is advised, while the actual quantity depends on the volume and complexity of the network traffic. Consider having 8 GB or more for more extensive research or larger packet captures.
- Storage: Enough space must be set aside for the analysis files and packet data that were gathered. It is recommended to have several gigabytes (or more) of free storage space, depending on the amount of collected traffic.
- A network interface card (NIC) :it is necessary in order to use Wireshark to capture network traffic. Make that the computer has a sufficient NIC that supports the needed capture capabilities (like promiscuous mode) as well as the desired network protocols (like Ethernet and Wi-Fi). For the purpose of capturing particular network segments, it may occasionally be required to use additional hardware, such as network TAPs (Test Access Points) or network switches with port mirroring capabilities.
- Network Connectivity: The computer needs to be linked to the network infrastructure in order to record real-time network traffic for analysis. When analysing wireless network traffic, this can be done using either a wired Ethernet connection or a wireless connection (Wi-Fi). Make that the network connectivity is correctly established and set up.

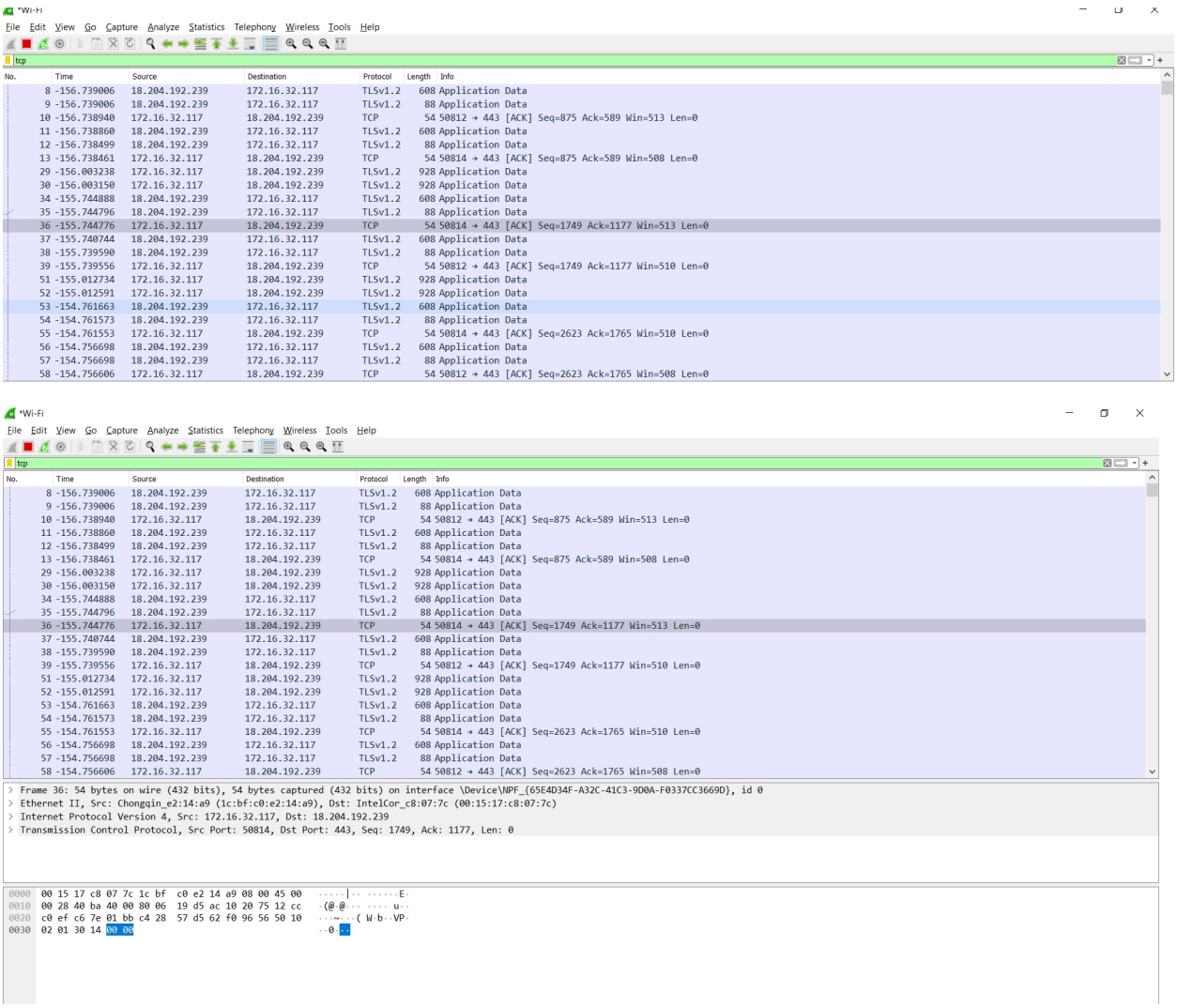
4. EXPERIMENTAL INVESTIGATIONS

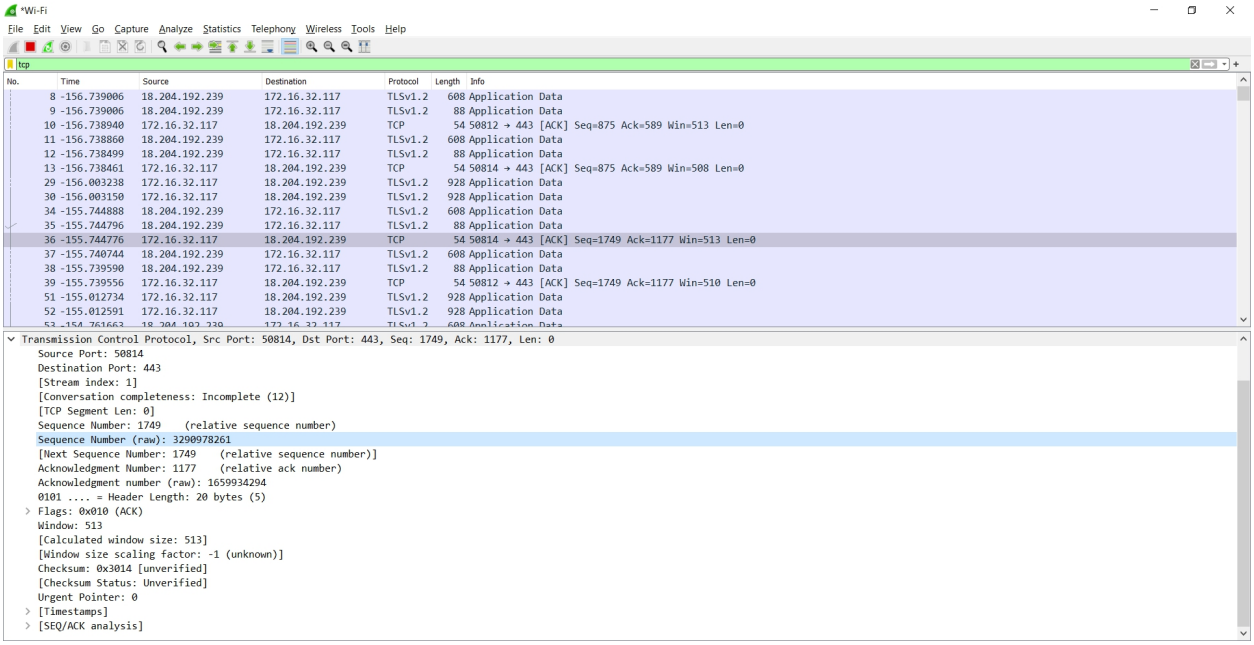
We have analysed that gathering network traffic information is essential for analyzing attack vectors, spotting malicious activity, and comprehending data movement within networks. To gather data about network traffic:

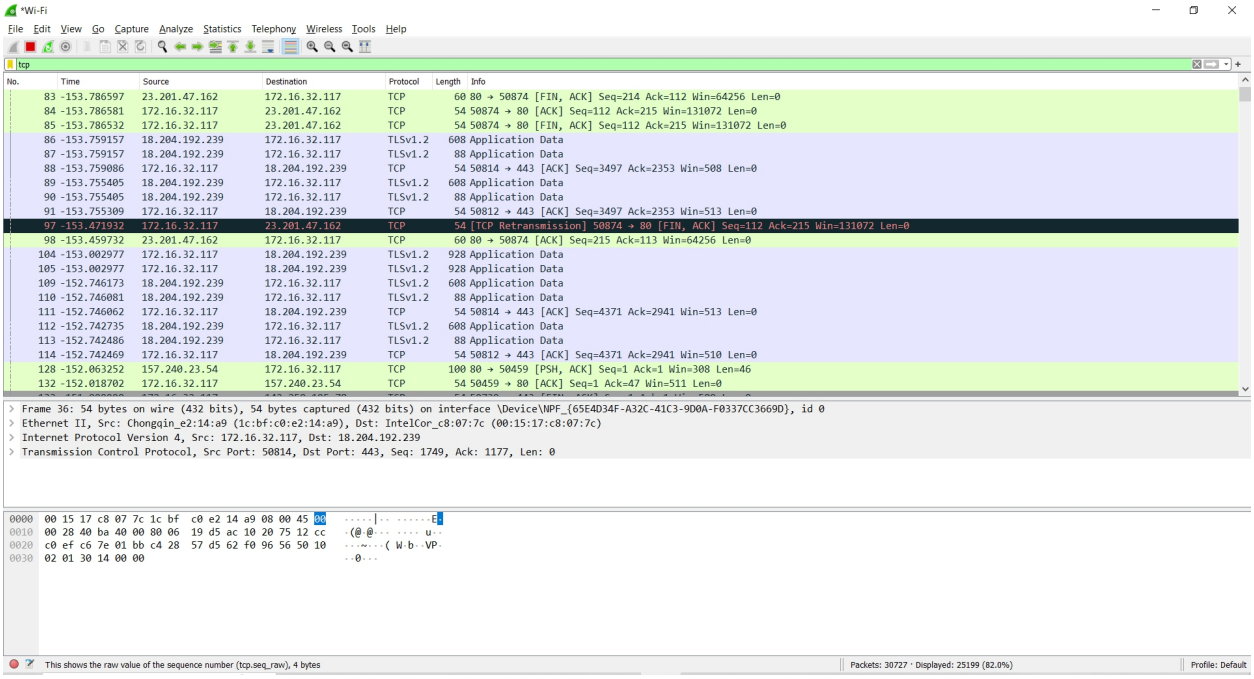
- Utilize packet-level network data by deploying network traffic capture applications like Wireshark. To get a complete picture of the traffic during the incident, record data on pertinent network segments, systems, or network devices.

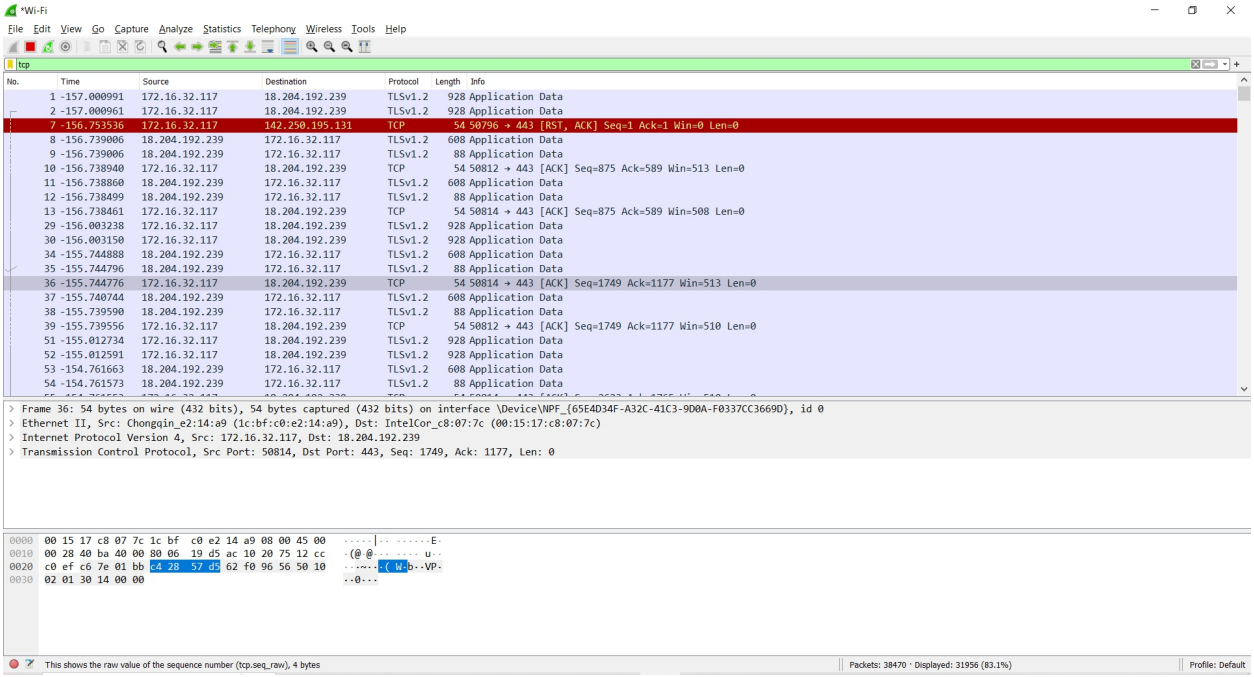
- Log analysis: Gather network device logs from firewalls, routers, and switches to obtain insight into connections, traffic flows, and any odd or malicious activity that these devices may have logged.

- Use network flow monitoring tools or collectors, such NetFlow or IPFIX, to record flow records that summarize communication patterns, source-destination relationships, and other relevant information.

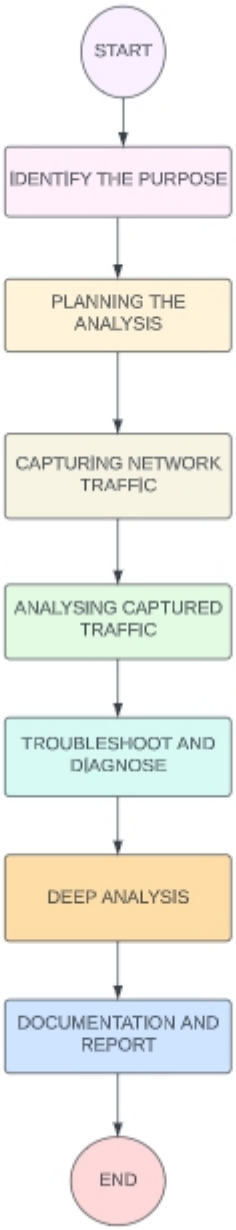



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
8 -156.739006 18.204.192.239 172.16.32.117 TLSv1.2 608 Application Data
9 -156.739006 18.204.192.239 172.16.32.117 TLSv1.2 88 Application Data
10 -156.738940 172.16.32.117 18.204.192.239 TCP 54 50812 → 443 [ACK] Seq=875 Ack=589 Win=513 Len=0
11 -156.738860 18.204.192.239 172.16.32.117 TLSv1.2 608 Application Data
12 -156.738499 18.204.192.239 172.16.32.117 TLSv1.2 88 Application Data
13 -156.738461 172.16.32.117 18.204.192.239 TCP 54 50814 → 443 [ACK] Seq=875 Ack=589 Win=508 Len=0
29 -156.003238 172.16.32.117 18.204.192.239 TLSv1.2 928 Application Data
30 -156.003150 172.16.32.117 18.204.192.239 TLSv1.2 928 Application Data
34 -155.744888 18.204.192.239 172.16.32.117 TLSv1.2 608 Application Data
35 -155.744796 18.204.192.239 172.16.32.117 TLSv1.2 88 Application Data
36 -155.744776 172.16.32.117 18.204.192.239 TCP 54 50814 → 443 [ACK] Seq=1749 Ack=1177 Win=513 Len=0
37 -155.740744 18.204.192.239 172.16.32.117 TLSv1.2 608 Application Data
38 -155.739590 18.204.192.239 172.16.32.117 TLSv1.2 88 Application Data
39 -155.739556 172.16.32.117 18.204.192.239 TCP 54 50812 → 443 [ACK] Seq=1749 Ack=1177 Win=510 Len=0
51 -155.012734 172.16.32.117 18.204.192.239 TLSv1.2 928 Application Data
52 -155.012591 172.16.32.117 18.204.192.239 TLSv1.2 928 Application Data
Transmission Control Protocol, Src Port: 50814, Dst Port: 443, Seq: 1749, Ack: 1177, Len: 0
Source Port: 50814
Destination Port: 443
[Stream index: 1]
[Conversation completeness: Incomplete (12)]
[TCP Segment Len: 0]
Sequence Number: 1749 (relative sequence number)
Sequence Number (raw): 3290978261
[Next Sequence Number: 1749 (relative sequence number)]
Acknowledgment Number: 1177 (relative ack number)
Acknowledgment number (raw): 1659934294
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window: 513
[Calculated window size: 513]
[Window size scaling factor: -1 (unknown)]
Checksum: 0x3014 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
83 -153.786597 23.201.47.162 172.16.32.117 TCP 60 80 → 50874 [FIN, ACK] Seq=214 Ack=112 Win=64256 Len=0
84 -153.786581 172.16.32.117 23.201.47.162 TCP 54 50874 → 80 [ACK] Seq=112 Ack=215 Win=131072 Len=0
85 -153.786532 172.16.32.117 23.201.47.162 TCP 54 50874 → 80 [FIN, ACK] Seq=112 Ack=215 Win=131072 Len=0
86 -153.759157 18.204.192.239 172.16.32.117 TLSv1.2 608 Application Data
87 -153.759157 18.204.192.239 172.16.32.117 TLSv1.2 88 Application Data
88 -153.759086 172.16.32.117 18.204.192.239 TCP 54 50814 → 443 [ACK] Seq=3497 Ack=2353 Win=508 Len=0
89 -153.755405 18.204.192.239 172.16.32.117 TLSv1.2 608 Application Data
90 -153.755405 18.204.192.239 172.16.32.117 TLSv1.2 88 Application Data
91 -153.755309 172.16.32.117 18.204.192.239 TCP 54 50812 → 443 [ACK] Seq=3497 Ack=2353 Win=513 Len=0
97 -153.471932 172.16.32.117 23.201.47.162 TCP 54 [TCP Retransmission] 50874 → 80 [FIN, ACK] Seq=112 Ack=215 Win=131072 Len=0
98 -153.459732 23.201.47.162 172.16.32.117 TCP 60 80 → 50874 [ACK] Seq=215 Ack=113 Win=64256 Len=0
104 -153.002977 172.16.32.117 18.204.192.239 TLSv1.2 928 Application Data
105 -153.002977 172.16.32.117 18.204.192.239 TLSv1.2 928 Application Data
109 -152.746173 18.204.192.239 172.16.32.117 TLSv1.2 608 Application Data
110 -152.746081 18.204.192.239 172.16.32.117 TLSv1.2 88 Application Data
111 -152.746062 172.16.32.117 18.204.192.239 TCP 54 50814 → 443 [ACK] Seq=4371 Ack=2941 Win=513 Len=0
112 -152.742735 18.204.192.239 172.16.32.117 TLSv1.2 608 Application Data
113 -152.742486 18.204.192.239 172.16.32.117 TLSv1.2 88 Application Data
114 -152.742469 172.16.32.117 18.204.192.239 TCP 54 50812 → 443 [ACK] Seq=4371 Ack=2941 Win=510 Len=0
128 -152.063252 157.240.23.54 172.16.32.117 TCP 100 80 → 50459 [PSH, ACK] Seq=1 Ack=1 Win=308 Len=46
132 -152.018702 172.16.32.117 157.240.23.54 TCP 54 50459 → 80 [ACK] Seq=1 Ack=47 Win=511 Len=0
Frame 36: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{65E4D34F-A32C-41C3-9D0A-F0337CC3669D}, id 0
Ethernet II, Src: Chongqin_e2:14:a9 (1c:bf:c0:e2:14:a9), Dst: IntelCor_c8:07:7c (00:15:17:c8:07:7c)
Internet Protocol Version 4, Src: 172.16.32.117, Dst: 18.204.192.239
Transmission Control Protocol, Src Port: 50814, Dst Port: 443, Seq: 1749, Ack: 1177, Len: 0
0000 00 15 17 c8 07 7c 1c bf c0 e2 14 a9 08 00 45 00
0010 00 28 40 ba 40 00 80 06 19 d5 ac 10 20 75 12 cc
0020 c0 ef c6 7e 01 bb c4 28 57 d5 62 f0 96 56 50 10
0030 02 01 30 14 00 00
This shows the raw value of the sequence number (tcp.seq_raw), 4 bytes
Packets: 30727 · Displayed: 25199 (82.0%)
Profile: Default

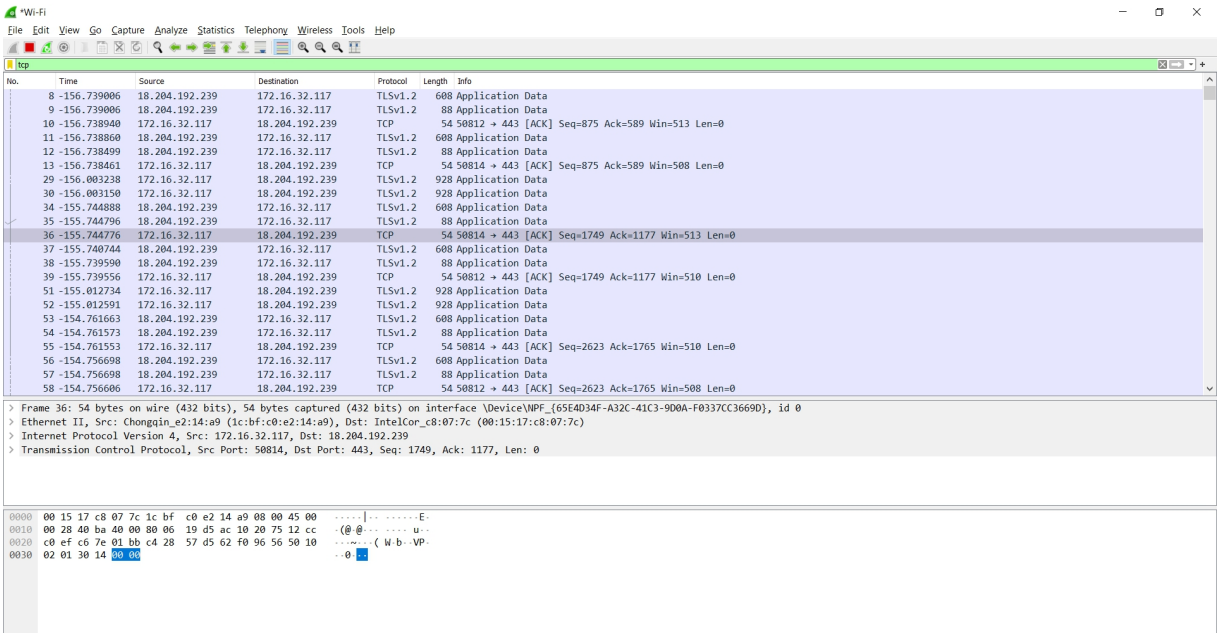

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
1 -157.000991 172.16.32.117 18.204.192.239 TLSv1.2 928 Application Data
2 -157.000961 172.16.32.117 18.204.192.239 TLSv1.2 928 Application Data
7 -156.753536 172.16.32.117 142.250.195.131 TCP 54 50796 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
8 -156.739006 18.204.192.239 172.16.32.117 TLSv1.2 608 Application Data
9 -156.739006 18.204.192.239 172.16.32.117 TLSv1.2 88 Application Data
10 -156.738940 172.16.32.117 18.204.192.239 TCP 54 50812 → 443 [ACK] Seq=875 Ack=589 Win=513 Len=0
11 -156.738860 18.204.192.239 172.16.32.117 TLSv1.2 608 Application Data
12 -156.738499 18.204.192.239 172.16.32.117 TLSv1.2 88 Application Data
13 -156.738461 172.16.32.117 18.204.192.239 TCP 54 50814 → 443 [ACK] Seq=875 Ack=589 Win=508 Len=0
29 -156.003238 172.16.32.117 18.204.192.239 TLSv1.2 928 Application Data
30 -156.003150 172.16.32.117 18.204.192.239 TLSv1.2 928 Application Data
34 -155.744888 18.204.192.239 172.16.32.117 TLSv1.2 608 Application Data
35 -155.744796 18.204.192.239 172.16.32.117 TLSv1.2 88 Application Data
36 -155.744776 172.16.32.117 18.204.192.239 TCP 54 50814 → 443 [ACK] Seq=1749 Ack=1177 Win=513 Len=0
37 -155.740744 18.204.192.239 172.16.32.117 TLSv1.2 608 Application Data
38 -155.739590 18.204.192.239 172.16.32.117 TLSv1.2 88 Application Data
39 -155.739556 172.16.32.117 18.204.192.239 TCP 54 50812 → 443 [ACK] Seq=1749 Ack=1177 Win=510 Len=0
51 -155.012734 172.16.32.117 18.204.192.239 TLSv1.2 928 Application Data
52 -155.012591 172.16.32.117 18.204.192.239 TLSv1.2 928 Application Data
53 -154.761663 18.204.192.239 172.16.32.117 TLSv1.2 608 Application Data
54 -154.761573 18.204.192.239 172.16.32.117 TLSv1.2 88 Application Data
Frame 36: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{65E4D34F-A32C-41C3-9D0A-F0337CC3669D}, id 0
Ethernet II, Src: Chongqin_e2:14:a9 (1c:bf:c0:e2:14:a9), Dst: IntelCor_c8:07:7c (00:15:17:c8:07:7c)
Internet Protocol Version 4, Src: 172.16.32.117, Dst: 18.204.192.239
Transmission Control Protocol, Src Port: 50814, Dst Port: 443, Seq: 1749, Ack: 1177, Len: 0
0000 00 15 17 c8 07 7c 1c bf c0 e2 14 a9 08 00 45 00
0010 00 28 40 ba 40 00 80 06 19 d5 ac 10 20 75 12 cc
0020 c0 ef c6 7e 01 bb c4 28 57 d8 62 f0 96 56 50 10
0030 02 01 30 14 00 00
This shows the raw value of the sequence number (tcp.seq_raw), 4 bytes
Packets: 38470 · Displayed: 31956 (83.1%)
Profile: Default

5. FLOWCHART



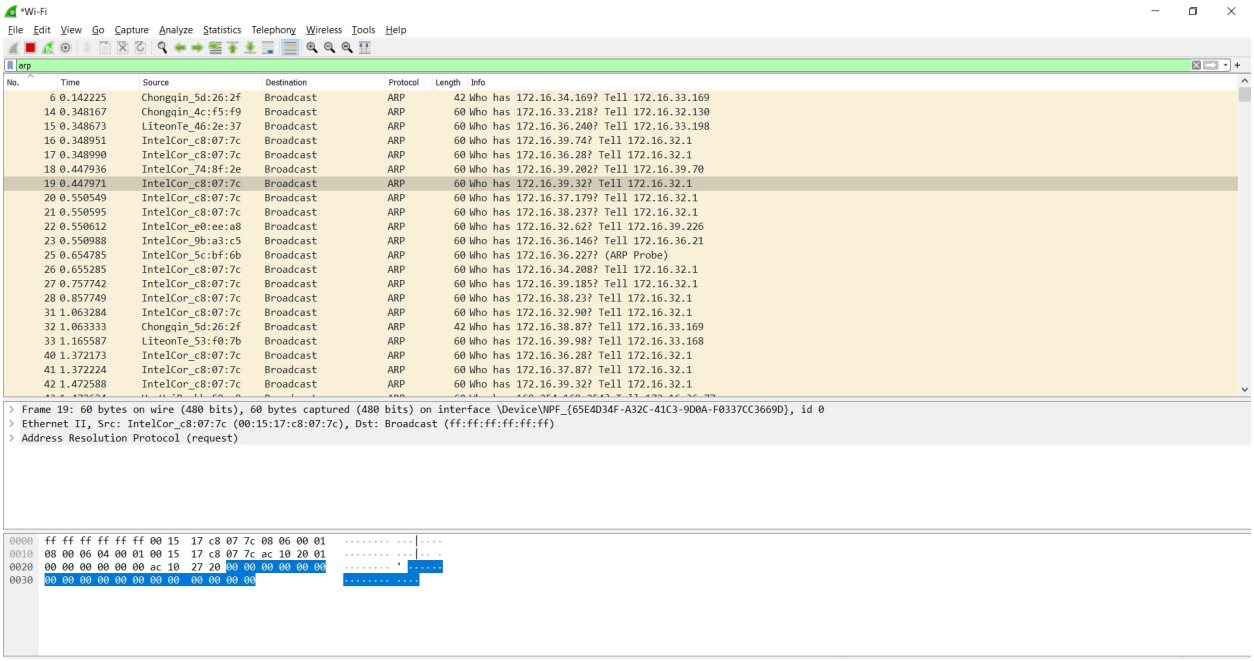
6. RESULT

Flow of tcp packet



Segmentation on the basis of ARP protocol:

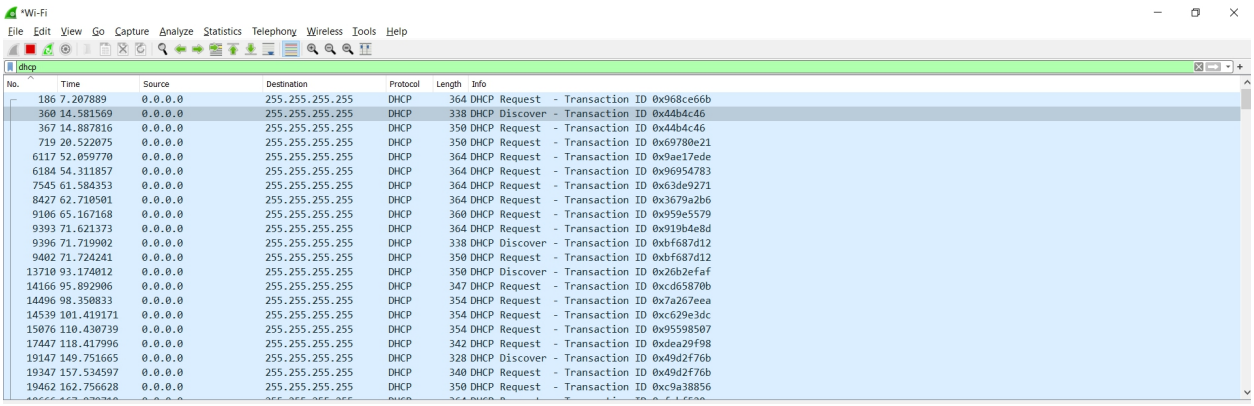
1. Start a packet capture in Wireshark on the specified network interface or capture point to record ARP traffic.
2. Apply a display filter to only show ARP packets to filter ARP packets. Enter "arp" in the display filter bar and hit Enter to filter for ARP packets. Only the ARP packets that were recorded during the packet capture will be shown by this filter.
3. Examine ARP Requests and Replies: Examine the ARP packets that were recorded in order to comprehend ARP Requests and Replies. The ARP replies give the associated MAC addresses, while the ARP queries are used to translate IP addresses to MAC addresses.

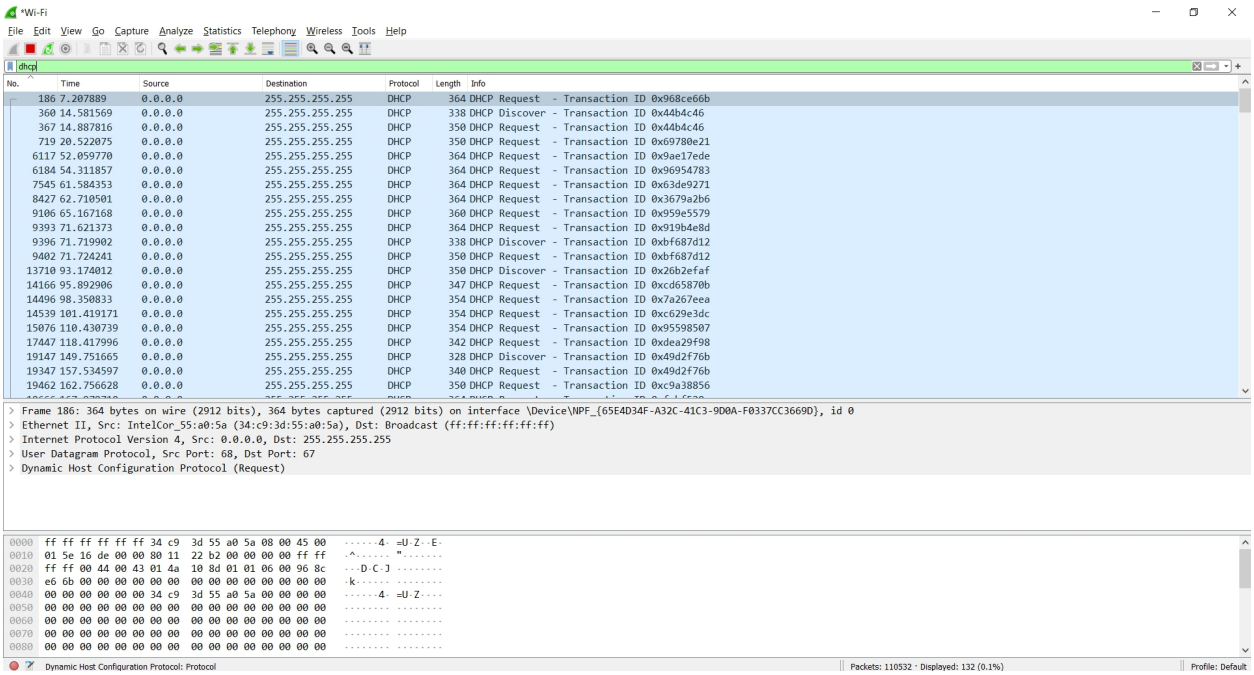


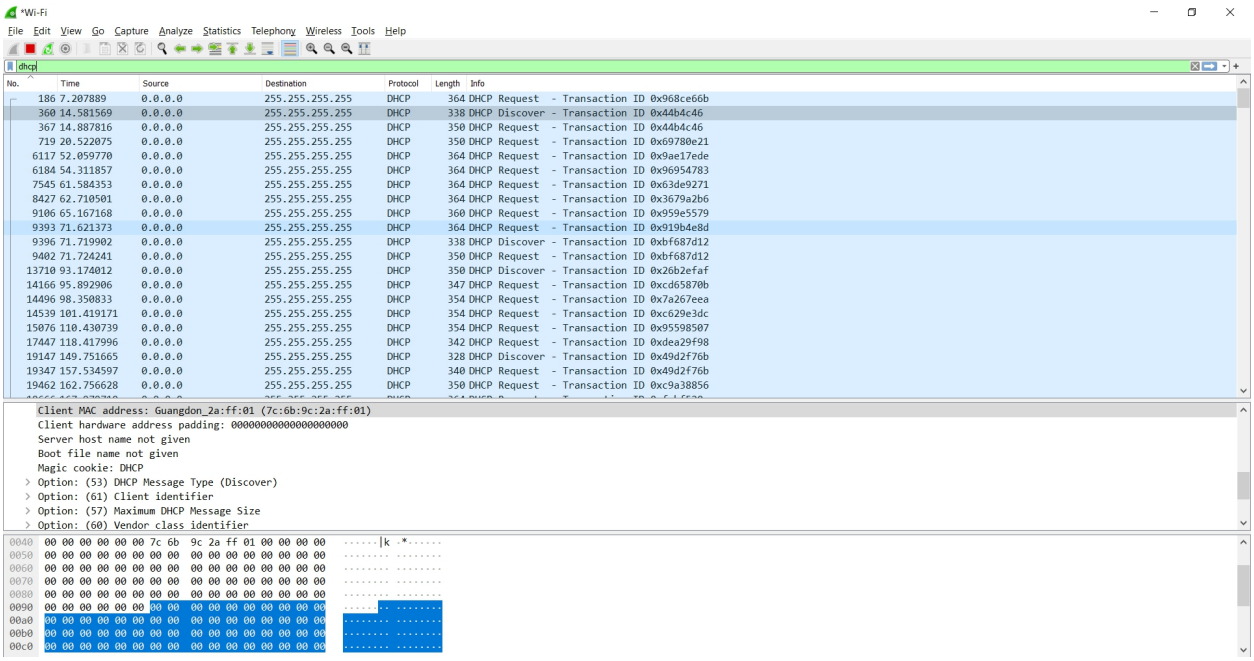
Analysis of dora or DHCP

DORA refers to the Dynamic Host Configuration Protocol (DHCP) negotiation process between a client and a DHCP server in network investigation using Wireshark. The four steps of DHCP communication are represented by the letters DORA, which stand for Discover, Offer, Request, and Acknowledge. The network packets exchanged during the DORA process can be captured and analysed by Wireshark in order to investigate DHCP-related problems or learn more about network configuration. Using Wireshark for DORA analysis looks like this:

1. To begin capturing DHCP traffic, use Wireshark and choose the network interface. In order to start capturing packets, click the "Start" button.
2. DHCP Discover: A client sends a DHCP Discover packet when it joins a network to look for accessible DHCP servers. To observe only DHCP packets, filter the collected packets using the display filter "dhcp==1". Track down the DHCP Discover packets the client has submitted.
3. DHCP Offer: DHCP servers send DHCP Offer packets in response to Discover packets. These packets include offers to lease IP addresses as well as other network setup data. To observe the DHCP Offer packets from the servers, filter the packets using the display filter "bootp.option.dhcp==2".
4. By using Wireshark to capture and analyse the DORA packets,we can learn more about DHCP negotiation, solve DHCP-related issues, and confirm the proper network settings.

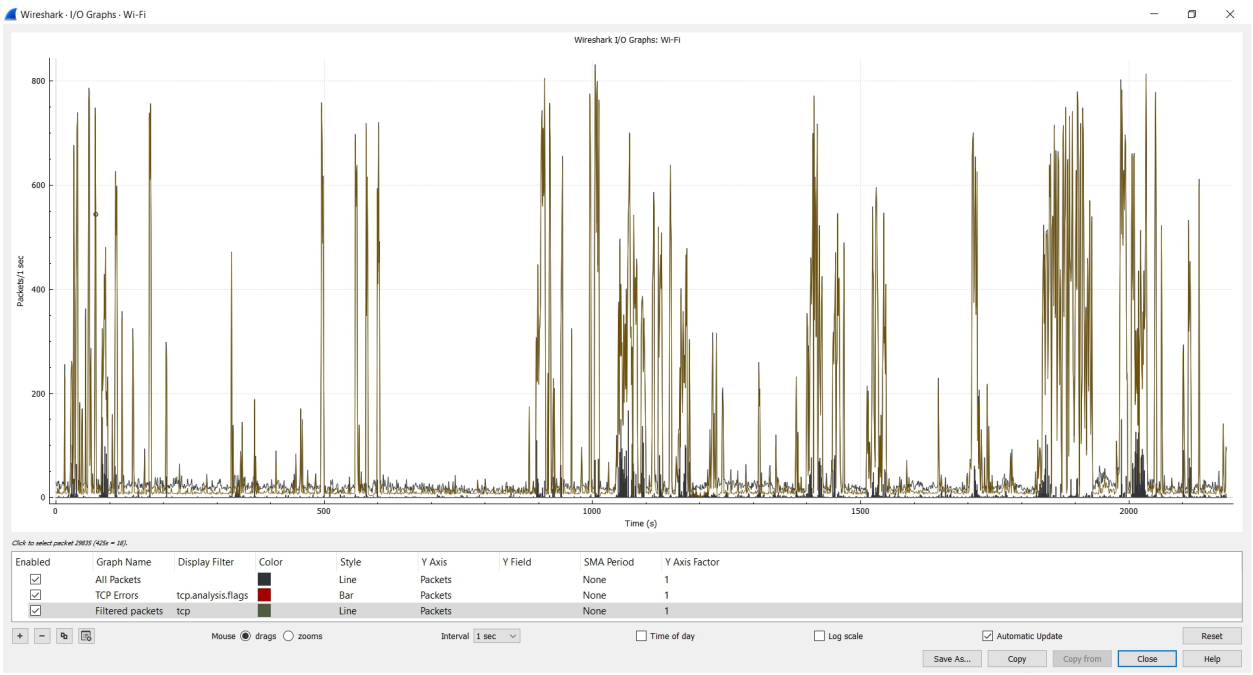






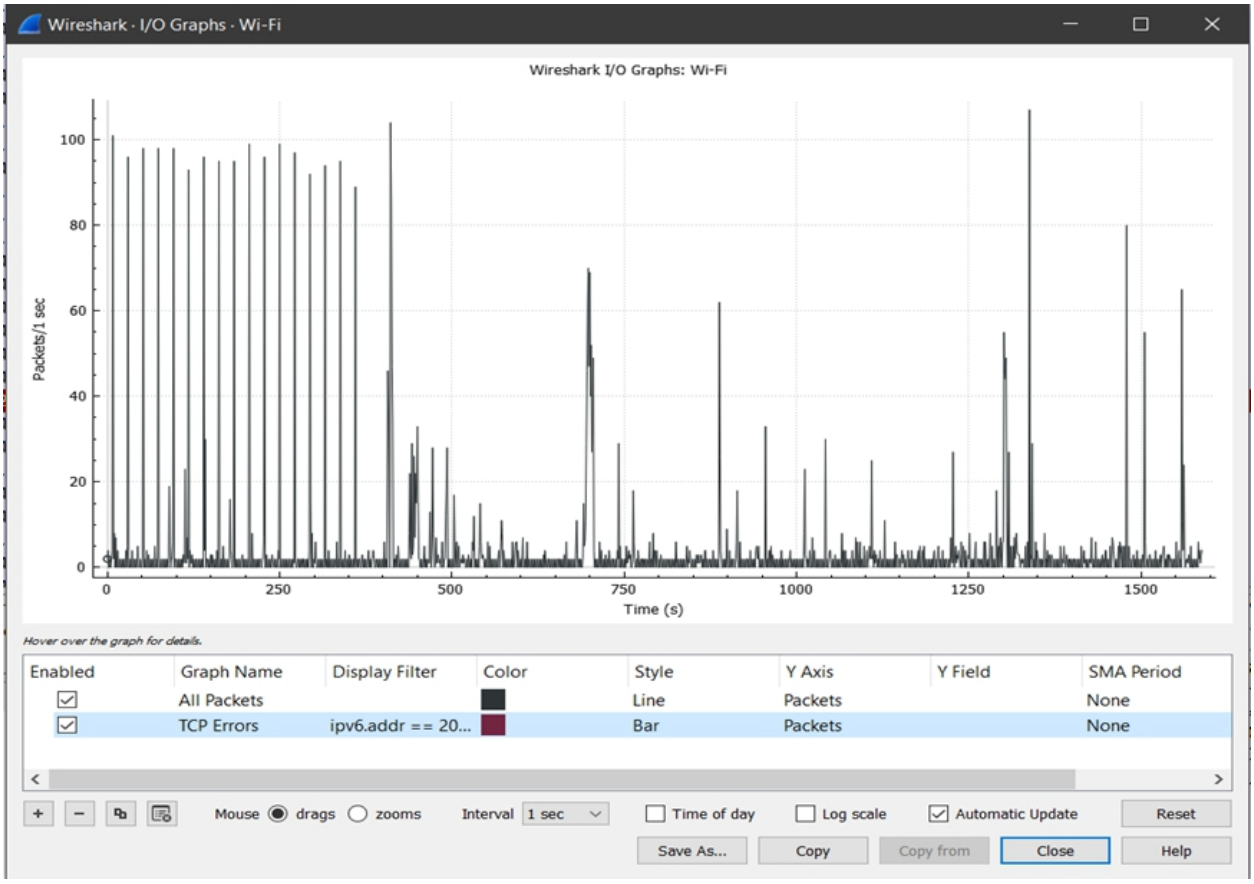
Statistics of current wifi device :

As we can see that the rate of packet transfer is more

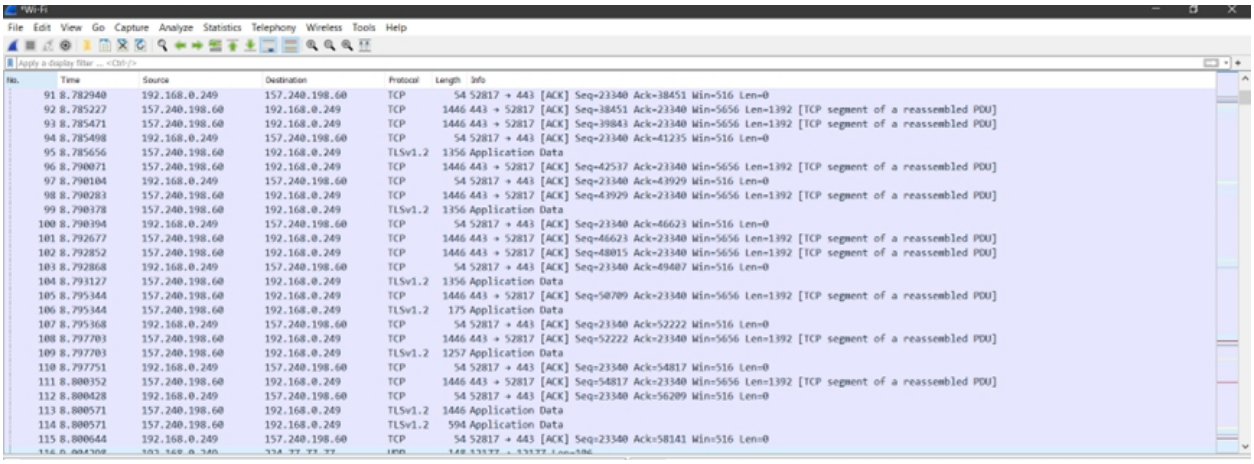


Analyzing a different network other than mine in the network:

By changing network mask:



Only request with destination or source as 192.168.0.249 are displayed ::



Checking the conversations for various protocols on my network can be analyzed as :

Layer 2 :

Wireshark · Conversations · Wi-Fi

Ethernet · 129 | IPv4 · 103 | IPv6 | TCP · 138 | UDP · 117

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
28:cd:c4:5b:88:61	ff:ff:ff:ff:ff:ff	5	300	5	300	0	0	111.017337	242.3753	9	
28:cd:c4:80:9a:d5	ff:ff:ff:ff:ff:ff	9	1078	9	1078	0	0	201.018745	142.2375	60	
2c:8d:b1:a6:87:c7	ff:ff:ff:ff:ff:ff	5	430	5	430	0	0	17.515730	283.6534	12	
2c:8d:b1:ae:04:b1	ff:ff:ff:ff:ff:ff	17	1564	17	1564	0	0	12.596990	300.1463	41	
34:2e:b7:95:91:74	ff:ff:ff:ff:ff:ff	11	660	11	660	0	0	67.487565	243.2068	21	
34:2e:b7:9f:26:0d	ff:ff:ff:ff:ff:ff	12	720	12	720	0	0	132.102722	213.9234	26	
34:6f:24:93:85:cd	ff:ff:ff:ff:ff:ff	28	1680	28	1680	0	0	8.296951	324.5181	41	
34:6f:24:c9:32:d7	ff:ff:ff:ff:ff:ff	59	10 k	59	10 k	0	0	8.193938	335.1649	245	
34:c9:3d:3e:23:35	ff:ff:ff:ff:ff:ff	15	934	15	934	0	0	122.893632	212.7869	35	
34:c9:3d:55:a0:5a	ff:ff:ff:ff:ff:ff	6	392	6	392	0	0	16.692508	20.7885	150	
38:d5:7a:13:de:c9	ff:ff:ff:ff:ff:ff	3	180	3	180	0	0	91.348885	243.5106	5	
40:1c:83:9f:fb:4b	ff:ff:ff:ff:ff:ff	43	2658	43	2658	0	0	6.043589	351.3605	60	
40:74:e0:24:c4:21	ff:ff:ff:ff:ff:ff	81	4860	81	4860	0	0	15.361004	336.6076	115	
44:af:28:a9:25:7c	ff:ff:ff:ff:ff:ff	26	2038	26	2038	0	0	112.852055	150.4452	108	
46:de:e5:f6:a6:4b	ff:ff:ff:ff:ff:ff	7	1314	7	1314	0	0	241.263043	12.2019	861	
48:5f:99:81:10:99	ff:ff:ff:ff:ff:ff	1	92	1	92	0	0	133.43278(	0.0000	—	
48:e7:da:aa:ca:f1	ff:ff:ff:ff:ff:ff	23	1380	23	1380	0	0	139.078885	96.9763	113	
4a:45:ca:57:7c:67	ff:ff:ff:ff:ff:ff	46	3080	46	3080	0	0	24.886092	321.5502	76	
4c:34:88:84:01:25	ff:ff:ff:ff:ff:ff	12	720	12	720	0	0	138.149634	140.8095	40	
4e:56:8d:64:4c:9e	ff:ff:ff:ff:ff:ff	4	240	4	240	0	0	36.870792	14.7412	130	
50:c2:e8:2e:a7:7b	ff:ff:ff:ff:ff:ff	49	4875	49	4875	0	0	5.837310	254.3712	153	
50:de:06:ca:6f:bc	ff:ff:ff:ff:ff:ff	2	524	2	524	0	0	238.403238	5.7286	731	
54:6c:eb:cb:59:d5	ff:ff:ff:ff:ff:ff	65	3900	65	3900	0	0	3.278662	354.0048	88	
54:8d:5a:e5:df:67	ff:ff:ff:ff:ff:ff	7	644	7	644	0	0	144.592912	13.0063	396	
58:00:e3:53:f0:7b	ff:ff:ff:ff:ff:ff	58	3480	58	3480	0	0	23.245977	326.7812	85	
5c:ba:ef:4c:f5:f9	ff:ff:ff:ff:ff:ff	21	1260	21	1260	0	0	37.275621	298.5095	33	
5e:3a:dd:f4:7c:78	ff:ff:ff:ff:ff:ff	4	368	4	368	0	0	144.490913	101.1765	29	

Name resolution | Limit to display filter | Absolute start time

Tcp:

Wireshark · Conversations · Wi-Fi

Ethernet · 139 | IPv4 · 108 | IPv6 | TCP · 146 | UDP · 125

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
13.107.234.254	443	172.16.32.117	59223	1	60	1	60	0	0	17.888241	0.0000	—	
13.107.246.58	443	172.16.32.117	59235	13	822	3	270	10	552	70.001877	304.1396	7	
18.204.192.239	443	172.16.32.117	58315	1,640	683 k	827	271 k	813	411 k	0.134458	419.9912	5164	
18.204.192.239	443	172.16.32.117	58319	1,765	729 k	896	285 k	869	443 k	0.142452	419.9894	5434	
23.3.70.203	443	172.16.32.117	59219	11	631	2	145	9	486	10.261589	363.8790	3	
52.98.58.34	443	172.16.32.117	59233	1	60	1	60	0	0	119.38317(	0.0000	—	
52.123.128.254	443	172.16.32.117	59234	1	60	1	60	0	0	120.251937	0.0000	—	
142.250.182.3	443	172.16.32.117	59187	5	714	2	120	3	594	60.461331	60.0975	15	
142.250.193.173	443	172.16.32.117	59195	9	492	1	60	8	432	11.241549	79.5812	6	
142.250.196.46	443	172.16.32.117	59189	9	492	1	60	8	432	71.213334	79.6290	6	
157.240.23.54	80	172.16.32.117	50459	90	9082	52	4714	38	4368	73.437609	274.4623	137	
172.16.32.117	59050	172.253.118.100	443	7	378	7	378	0	0	0.100101	18.9330	159	
172.16.32.117	59239	172.253.118.100	443	30	11 k	17	2302	13	8826	0.109289	319.1227	57	
172.16.32.117	59213	216.239.32.116	443	25	10 k	12	3922	13	6218	0.559092	299.9839	104	
172.16.32.117	59184	35.190.80.1	443	5	289	3	163	2	126	0.934081	59.9508	21	
172.16.32.117	59185	35.190.80.1	443	5	289	3	163	2	126	0.996506	60.9225	21	
172.16.32.117	59225	52.182.143.208	443	3	168	2	108	1	60	5.465784	0.2701	3198	
172.16.32.117	59072	142.250.183.246	443	7	378	7	378	0	0	6.879865	28.1010	107	
172.16.32.117	59074	142.250.76.78	443	7	378	7	378	0	0	6.879947	20.2609	149	
172.16.32.117	59080	142.250.182.129	443	7	378	7	378	0	0	7.874170	29.4153	102	
172.16.32.117	59084	142.250.195.78	443	7	378	7	378	0	0	7.874253	35.6374	84	
172.16.32.117	59060	45.60.158.169	443	1	54	1	54	0	0	7.874390	0.0000	—	
172.16.32.117	59217	23.3.70.203	443	1	54	1	54	0	0	8.558501	0.0000	—	
172.16.32.117	59218	23.3.70.203	443	1	54	1	54	0	0	8.573998	0.0000	—	
172.16.32.117	59096	152.199.40.67	443	2	115	1	55	1	60	8.699095	0.0119	36 k	
172.16.32.117	59094	104.17.25.14	443	3	168	2	108	1	60	8.873818	0.0059	146 k	
172.16.32.117	59098	142.250.193.138	443	7	378	7	378	0	0	8.874006	36.5990	82	

Name resolution | Limit to display filter | Absolute start time

Copy | Follow Stream... | Graph...

Udp:

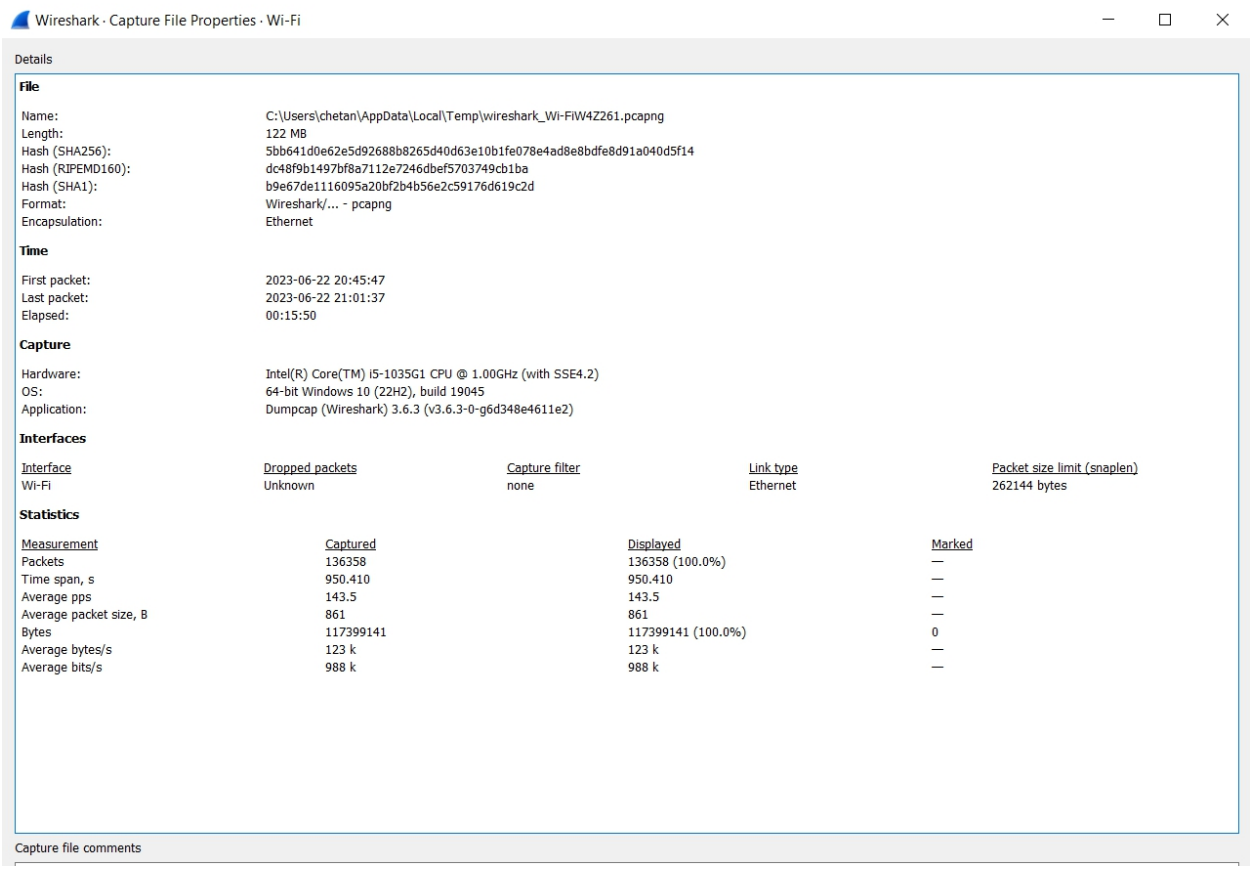
Wireshark · Conversations · Wi-Fi

Ethernet · 140 | IPv4 · 110 | IPv6 | TCP · 154 | UDP · 131

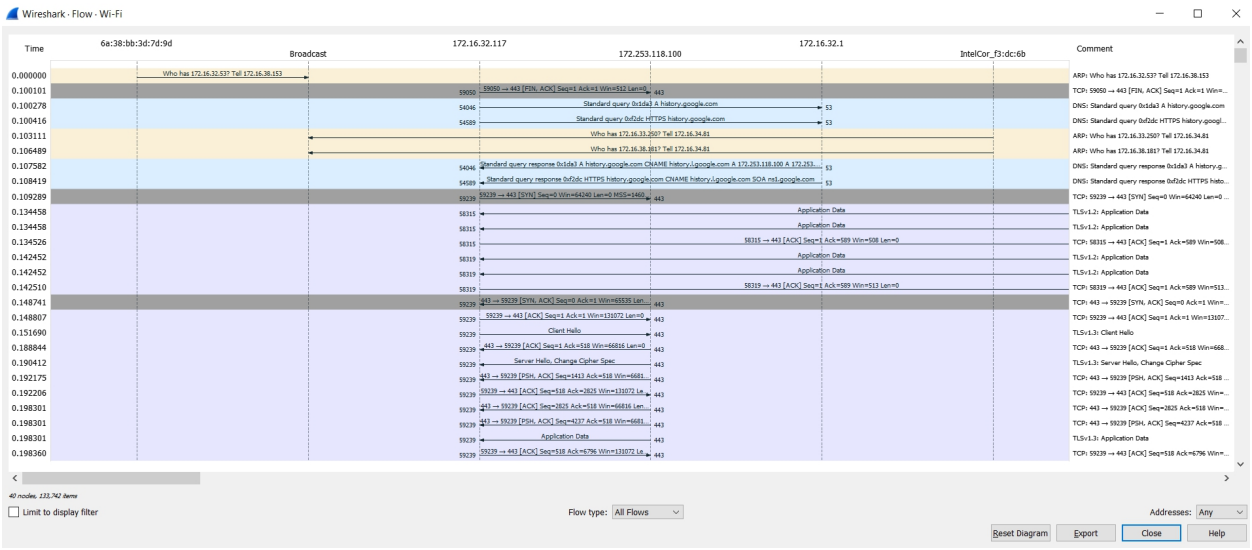
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
0.0.0.0	68	255.255.255.255	67	52	18 k	52	18 k	0	0	8.605090	397.8323	366	
172.16.32.40	56374	172.16.39.255	1947	1	82	1	82	0	0	112.852055	0.0000	—	
172.16.32.40	52638	172.16.39.255	6646	1	212	1	212	0	0	114.907663	0.0000	—	
172.16.32.40	54367	172.16.39.255	6646	1	212	1	212	0	0	192.724161	0.0000	—	
172.16.32.40	61969	172.16.39.255	6646	1	212	1	212	0	0	263.297255	0.0000	—	
172.16.32.40	59467	172.16.39.255	6646	1	212	1	212	0	0	400.08859€	0.0000	—	
172.16.32.62	137	172.16.39.255	137	1	92	1	92	0	0	32.975538	0.0000	—	
172.16.32.90	138	172.16.39.255	138	2	524	2	524	0	0	238.403238	5.7286	731	
172.16.32.117	54046	172.16.32.1	53	2	364	1	78	1	286	0.100278	0.0073	85 k	
172.16.32.117	54589	172.16.32.1	53	2	230	1	78	1	152	0.100416	0.0080	77 k	
172.16.32.117	55008	172.16.32.1	53	2	254	1	75	1	179	13.905297	0.0031	—	
172.16.32.117	57309	172.16.32.1	53	2	200	1	75	1	125	13.905543	0.0294	20 k	
172.16.32.117	64921	239.255.255.250	1900	4	868	4	868	0	0	44.713734	3.0315	2290	
172.16.32.117	63650	172.16.32.1	53	2	528	1	75	1	453	52.334864	0.0237	25 k	
172.16.32.117	53470	172.16.32.1	53	2	287	1	75	1	212	52.335054	0.0235	25 k	
172.16.32.117	63225	172.16.32.1	53	2	398	1	71	1	327	53.783977	0.0050	112 k	
172.16.32.117	63702	172.16.32.1	53	2	199	1	71	1	128	53.784233	0.0085	67 k	
172.16.32.117	55424	172.16.32.1	53	2	244	1	97	1	147	56.687454	0.1006	7714	
172.16.32.117	64137	172.16.32.1	53	2	285	1	97	1	188	56.687723	0.3101	2502	
172.16.32.117	49223	172.16.32.1	53	2	232	1	93	1	139	62.638281	0.2286	3254	
172.16.32.117	65327	172.16.32.1	53	2	273	1	93	1	180	62.638432	0.3261	2281	
172.16.32.117	61864	172.16.32.1	53	2	207	1	73	1	134	62.990580	0.0141	41 k	
172.16.32.117	64494	172.16.32.1	53	2	248	1	73	1	175	62.990822	0.0184	31 k	
172.16.32.117	51525	172.16.32.1	53	2	190	1	87	1	103	67.102895	0.0204	34 k	
172.16.32.117	61271	172.16.32.1	53	2	231	1	87	1	144	67.103192	0.0282	24 k	
172.16.32.117	64777	239.255.255.250	1900	4	868	4	868	0	0	75.133677	3.0091	2307	
172.16.32.117	60323	172.16.32.1	53	2	244	1	70	1	174	84.136320	0.1192	4699	

Name resolution | Limit to display filter | Absolute start time

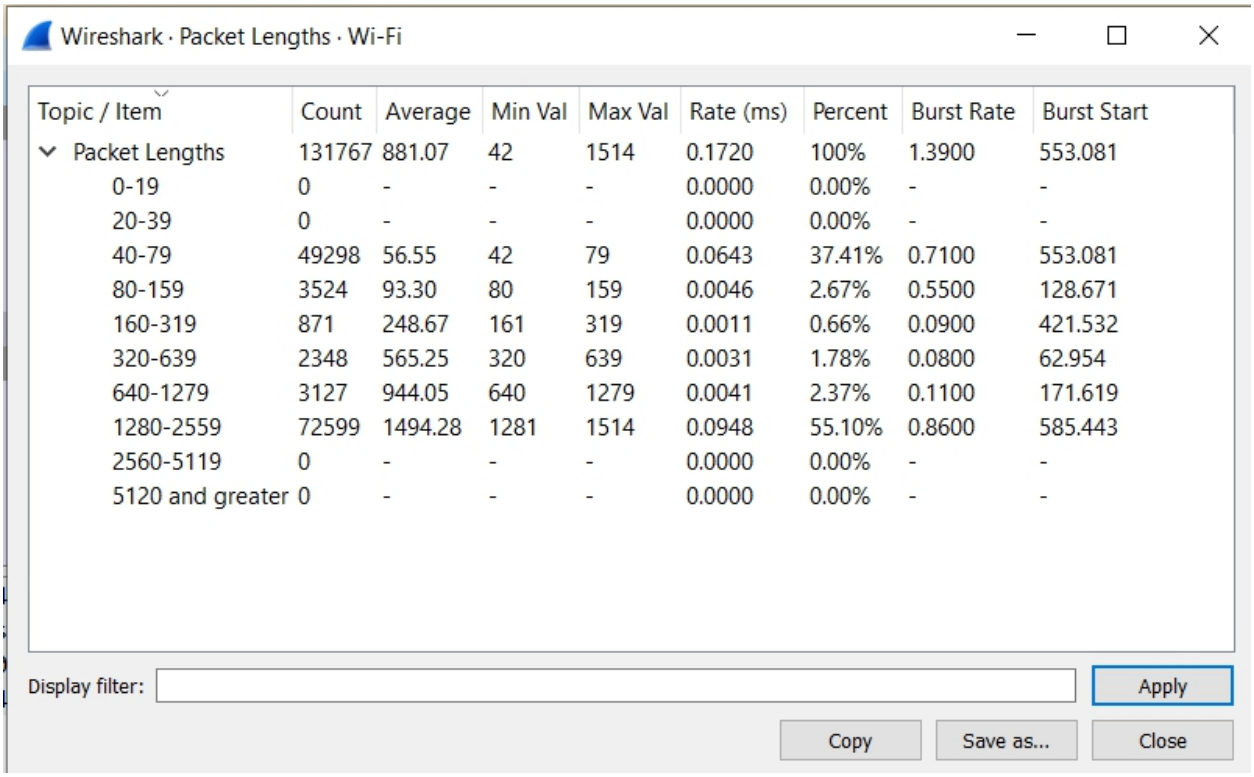
Basic total research detail:



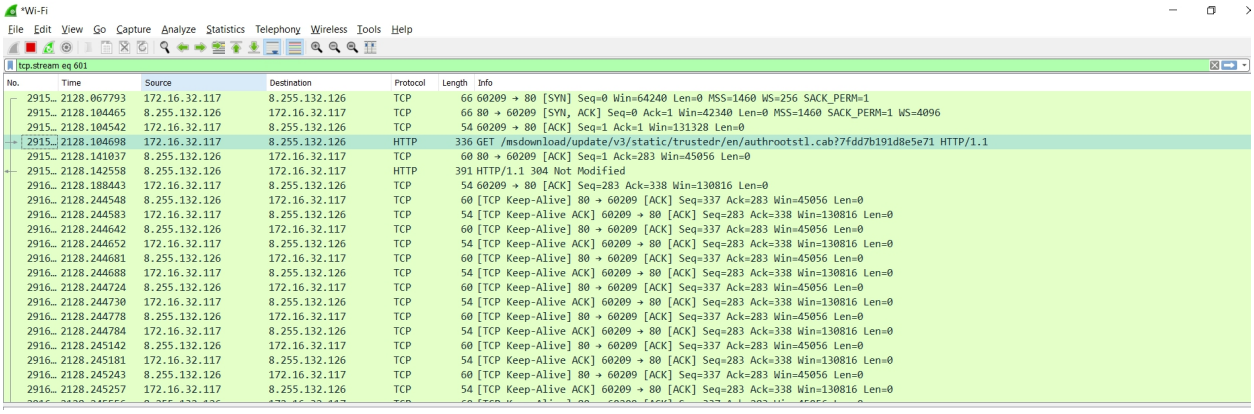
TCP UDP request flow chart:

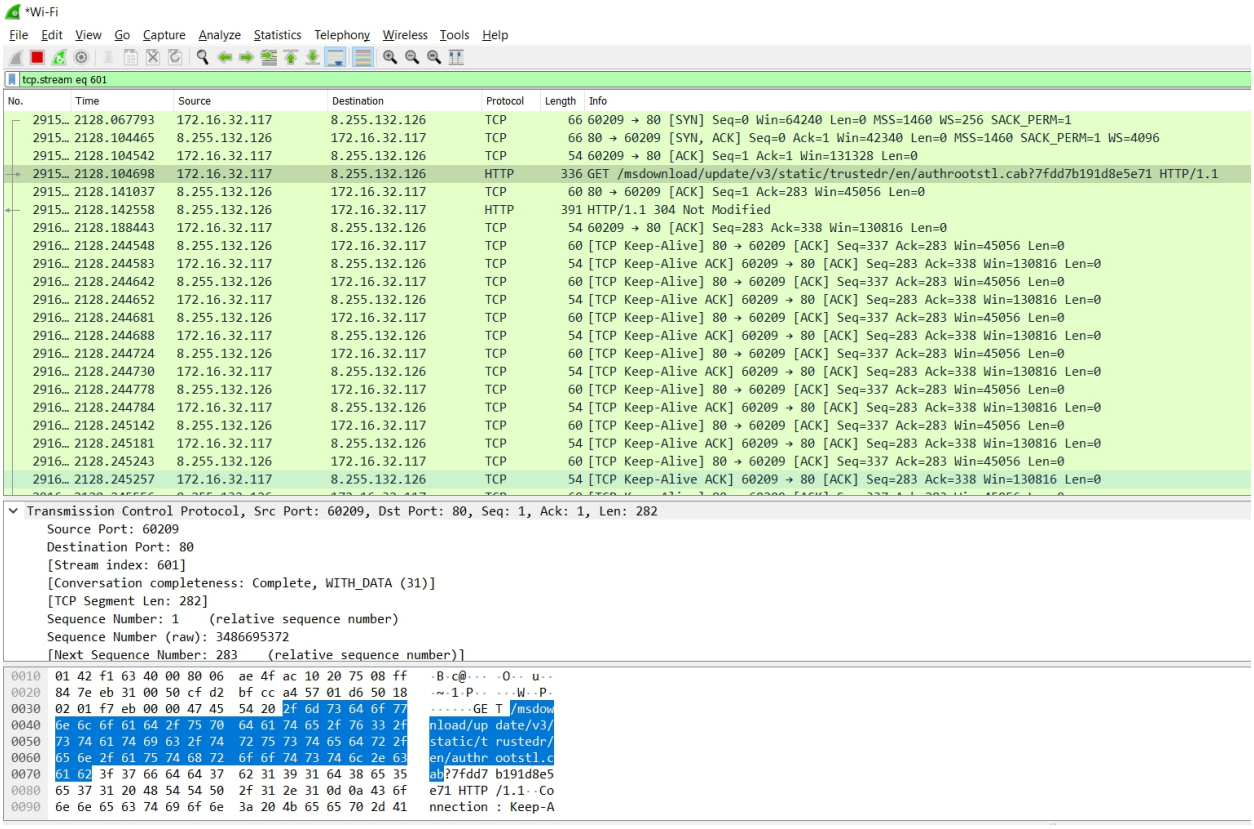


Length of data packets transferred

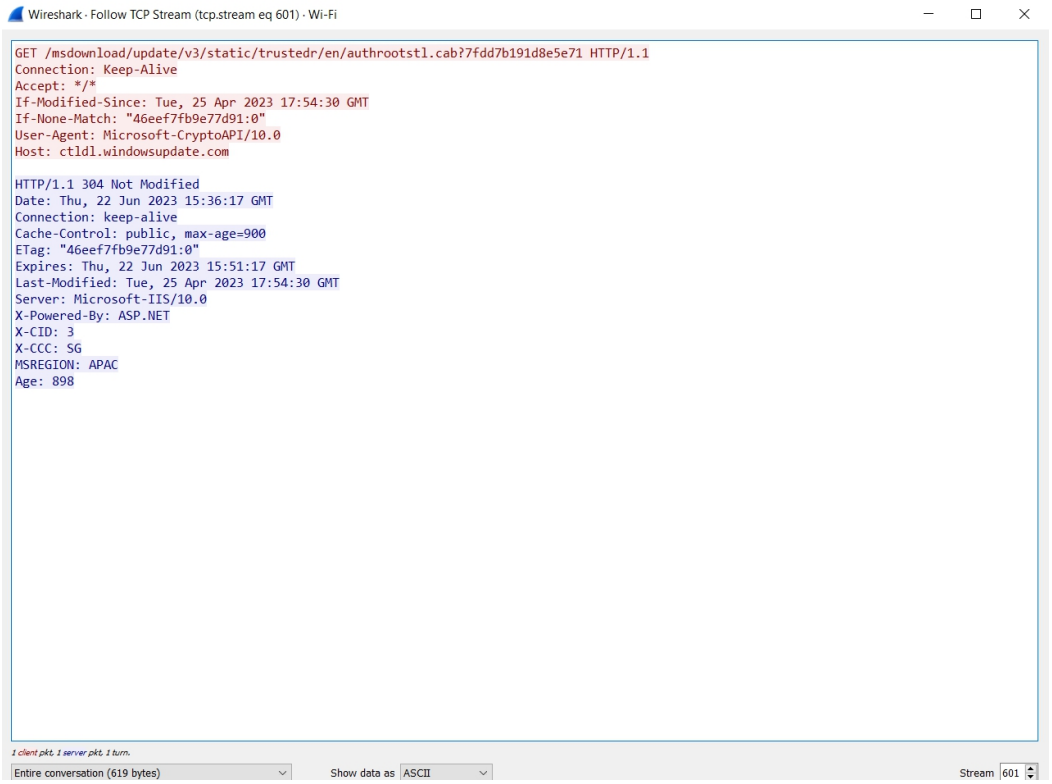


Analysing HTTP protocols





Accessing TCP streams in HTTP protocols



7. ADVANTAGE AND DISADVANTAGES

Advantages

- Broad Protocol Support: Ethernet, IP, TCP, UDP, HTTP, DNS, and a host of other network protocols are all supported by Wireshark. This makes it possible to analyse and comprehend network communications at all protocol stack layers in great detail.
- Real-time Packet Capture: With the help of Wireshark's real-time packet capture features, you may record and examine network data as it flows. This function is useful for identifying and resolving problems with live networks.
- Strong Analysis Tools: Wireshark provides a wide range of powerful analysis features. It enables you to examine specific packet information, carry out intricate filtering, examine protocol behaviour, produce statistics, make graphs, and even develop your own custom dissectors for proprietary protocols. These technologies make it possible to analyse network traffic in great detail and depth.
- Cross-platform Compatibility: Linux, macOS, and Windows are only a few of the operating systems for which Wireshark is available. Users may use Wireshark to do network analysis on their favourite operating system because to this cross-platform compatibility.
- Cost-effective: Since Wireshark is open-source and free software, there is no need to purchase pricey commercial network analysis tools. As a result, it is a cost-effective option for network research without sacrificing functionality.

Disadvantages

- Resource Intensive: Analyzing large packet captures or performing in-depth analysis can be resource-intensive, requiring significant amounts of memory, processing power, and storage. Processing and

analyzing extensive network traffic captures may strain system resources, leading to slower performance or potential limitations on the size of captures that can be effectively analyzed.

- Overwhelming Amount of Data: Wireshark captures and provides access to a vast amount of network traffic data. Analyzing and interpreting this data can be overwhelming, especially for novice users who may struggle to identify relevant packets or patterns amidst the sea of information.
- Complexity of Troubleshooting: While Wireshark provides valuable insights into network traffic, troubleshooting network issues solely based on packet-level analysis can be complex. Network problems can be caused by various factors beyond packet-level issues, including hardware failures, configuration errors, or external network conditions

8. APPLICATIONS

- Network Troubleshooting: Wireshark is frequently utilised to identify and resolve network problems. In order to locate the root of issues like network congestion, performance bottlenecks, connectivity problems, or misconfigurations, it enables you to capture and analyse network data. It assists in identifying the main cause of network outages and in finding effective solutions.
- Network infrastructure performance analysis and optimisation are made possible by Wireshark. Administrators can pinpoint areas where network performance can be enhanced by analysing network traffic patterns, packet loss, latency, and capacity utilisation. This includes improving network setups for better performance, identifying inefficient application behaviour, and optimising network protocols.
- Security Analysis: Wireshark is a useful tool for security experts to examine network traffic and spot threats or security weaknesses. It aids in the identification and investigation of network-based assaults such network scanning, attempted intrusions, malware infections, or unauthorised access attempts. Wireshark can help with network monitoring and aberrant behaviour and pattern detection that may point to security or policy violations.
- Wireshark is a tool that is frequently used for protocol analysis and development. It enables programmers and academics to examine network protocol behaviour, examine packet-level information, and verify protocol compliance. The customisable dissectors and scripting features of Wireshark make it a useful tool for protocol designers and developers to analyse proprietary or bespoke protocols.
- VoIP Analysis: For analysing Voice over IP (VoIP) traffic, Wireshark offers specialised functionality and plugins. It enables VoIP engineers and administrators to record and examine SIP (Session Initiation Protocol) messages, RTP streams, call quality measurements, and signalling protocols. By assisting in VoIP deployment optimisation and debugging, Wireshark ensures high-quality audio connections.
- Network Forensics: Wireshark is used in network forensics to look into and examine security breaches or incidents involving networks. Reconstructing network activity, establishing the chronology of events, examining network-based evidence, and assembling data for incident response or legal processes are all made easier by this. Forensic analysis benefits from Wireshark's capacity to record and examine network traffic in real-time or from archived packet captures.
- Network Monitoring and Baseline Analysis: Continuous network monitoring and baseline analysis can be done with Wireshark. Administrators can define baseline behaviour, spot departures from typical network behaviour, and see trends or patterns in network usage by collecting and analysing network traffic over time. It helps with planning for capacity, spotting performance trends, and assuring network stability.

9. CONCLUSION

In conclusion, Wireshark's use for network analysis at VIT College has given us in-depth understanding of how networks behave. We were able to resolve network problems, guarantee network security, and enhance overall network speed by looking at different protocols, analysing packet lengths, and observing DHCP DORA operations. The features of Wireshark have been crucial in helping the institution manage and maintain a reliable network infrastructure