**UNIVERSIDADE ESTÁCIO – CAMPUS FAP**

LEONARDO AFONSO DA SILVA SOARES - 202009262988

**RELATÓRIO DE LOGS DE REDES**

Belém – PA

2020

**Objetivo**

Coletar o log do tráfego de pacotes de rede capturados ao longo de um intervalo de tempo a critério dos alunos (em torno de 20 a 30 minutos), mais de 85.000 pacotes monitorados.Além de escrever um relatório explicando detalhes de uma amostragem do tráfego coletado, contendo:

* Protocolos utilizados
* Portas e IPs de origem e destino
* Detalhes dos pacotes como se o pacote for um ACK TCP
* Tamanho de janela
* Versão do protocolo IP utilizado
* Endereço MAC da placa de rede da interface utilizada para coletar os dados
* Tamanho do protocolo

**Procedimento Teórico**

Foi analisado um total de 1201 segundos, equivalente a 20 minutos de análise de tráfego, os protocolos que foram coletados e imagens serão exibidos abaixo.

**Protocolo Coletados:**

**ARP (Address Resolution Protocol)** é um protocolo que permite obter o MAC Address de uma interface a partir de seu endereço IP.

**DCP (Discovery and Configuration Protocol)** é uma definição de protocolo dentro do contexto PROFINET. É um protocolo baseado em camada de link para configurar nomes de estações e endereços IP. É restrito a uma sub-rede e usado principalmente em aplicativos pequenos e médios sem um servidor DHCP instalado.

**DHCP (Dynamic Host Configuration Protocol)** é um protocolo de camada de aplicação responsável por permitir que um dispositivo obtenha automaticamente um endereço IP (e endereços de outros recursos importantes de rede, como servidores DNS e roteadores).

**DNS (Domain Name System)** é um dos protocolos mais importantes da internet, pois é uma espécie de cola que une tudo. O DNS associa nomes de domínio, como www.google.com, a endereços IP, como 74.125.159.99.

## HTTP (Hypertext Transfer Protocol) é um protocolo de comunicação (na camada de aplicação segundo o Modelo OSI) utilizado para sistemas de informação de hipermídia, distribuídos e colaborativos. Ele é a base para a comunicação de dados da World Wide Web.

## ICMPv6 foi definido na RFC 4443 de modo a oferecer suporte para o conjunto de recursos necessários ao IPv6, juntamente com melhorias adicionais. Não discutiremos o ICMPv6 separadamente neste livro, pois ele usa a mesma estrutura de pacote dos pacotes ICMP. Pacotes ICMPv6 são, de modo geral, classificados como mensagens de erro ou mensagens informativas.

## 

## IGMPv2 é um protocolo que permite que um host anuncie sua associação de grupo de multicast a switches e roteadores vizinhos. O IGMP é um protocolo padrão usado pelo pacote de protocolos TCP/IP para obter uma multicast dinâmica. O IGMPv2 também adiciona a capacidade de roteadores para eleger o consultor IGMP, sem depender do protocolo multicast para executar esta tarefa. Para obter mais informações, consulte RFC 2236.

## IGMPv3 hospeda a assinatura do sinal para roteadores do último salto de grupos multicast. Os hosts podem sinalizar a associação de grupo com capacidades de filtragem em relação às fontes. Um host pode indicar que deseja receber o tráfego de todas as fontes enviadas para um grupo, exceto para algumas fontes específicas (chamado de modo de exclusão), ou que deseja receber o tráfego somente de algumas fontes específicas enviadas para o grupo (chamado de modo de inclusão).

## LLMNR (Link-Local Multicast Name Resolution) determina os nomes dos computadores da rede, se a mesma não possuir um servidor DNS (Domain Name System). A função LLMNR Responder trabalha em ambos os ambientes IPv4 ou IPv6 ao utilizar um computador que possui a função LLMNR Sender como o Windows Vista®.

## 

## MDNS é o protocolo DNS Multicast . A " multicast " encaminha a mesma mensagem para vários pontos de extremidade em uma rede. mDNS é um método de descoberta de rede de vizinhança.

## NBNS é um protocolo de nível de apresentação que usa a porta UDP /TCP 137. Raramente usa TCP, mas, teoricamente, ele pode. É parte das NetBIOS sobre TCP /IP pacote (NBT), que é um antecedente análogo de DNS.

## NTP (Network Time Protocol) é um protocolo para sincronização dos relógios dos computadores baseado no protocolo UDP sob a porta 123. É utilizado para sincronização do relógio de um conjunto de computadores e dispositivos em redes de dados com latência variável.

## QUIC é um protocolo de transporte experimental de baixa latência da internet do Google sobre o UDP, um protocolo que é usado frequentemente por jogos, streaming de mídia e serviços VoIP. ... Com o QUIC o Google visa combinar algumas das melhores características do TCP e UDP com ferramentas de segurança modernas.

## SSDP (Simple Service Discovery Protocol) é um protocolo de rede baseado no conjunto de protocolos da Internet para propaganda e descoberta de serviços de rede e informações de presença.

## SSLv2 é um protocolo para fazer a troca criptografada de mensagens entre servidores e clientes. Isso faz com que o usuário acredite que ao utilizar um site com suporte https está seguro em relação a privacidade dos dados que trafegam na rede e, nem sempre, isso é verdade.

## 

## TCP (Transmission Control Protocol) está definido na RFC 793, cuida do sequenciamento de dados e da recuperação de erros e, em última análise, garante que os dados cheguem até o ponto em que devem chegar. O TCP é considerado um protocolo orientado à conexão (connection-oriented protocol), pois estabelece uma conexão formal antes de transmitir dados, monitora a entrega de pacotes e geralmente tenta encerrar formalmente os canais de comunicação quando a transmissão é concluída.

**TLSv1.2 TLSv1.3** é um protocolo de criptografia destinado a manter os dados seguros quando são transferidos em uma rede. Estes artigos descrevem as etapas necessárias para garantir que a comunicação segura do *Configuration Manager* use o protocolo TLS 1.2. Estes artigos também descrevem os requisitos de atualização para os componentes usados com frequência e a solução de problemas comuns.

**UDP (User Datagram Protocol)** é um protocolo simples da camada de transporte. Ele é descrito na RFC 768 e permite que a aplicação envie um datagrama encapsulado num pacote IPv4 ou IPv6 a um destino, porém sem qualquer tipo de garantia que o pacote chegue corretamente. O protocolo UDP não é confiável como o TCP.

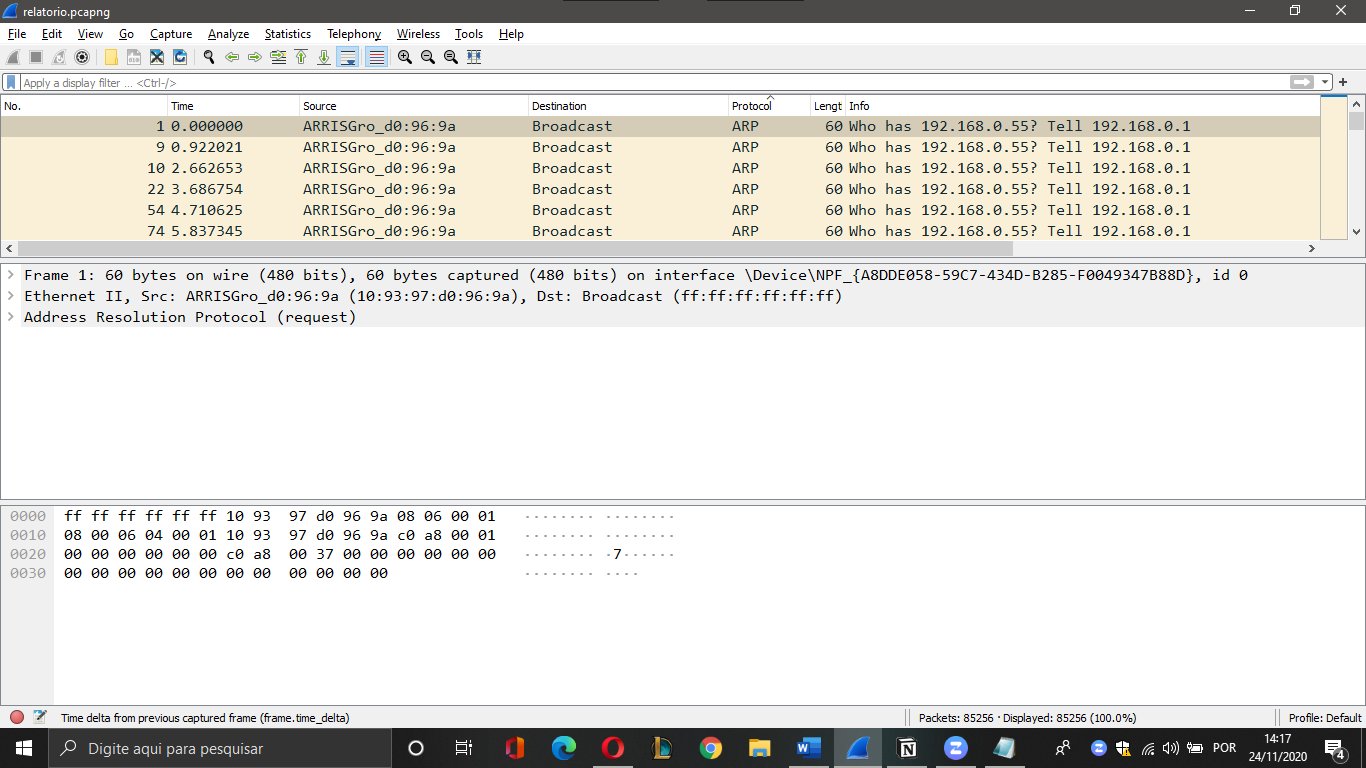
**Análises de alguns dos protocolos coletados**

Devido ao grande número de pacotes, será analisado apenas os pacotes de proto- colos mais conhecidos bem como outras características.

Começando pelo ARP (Address Resolution Protocol) no qual possui o endereço IP de origem ARRISGro\_d0:96:9a e o destino Broadcast, é responsável pela transmissão de qualquer tipo de mídia. Pode ser via ondas de rádio, satélite, cabos, fibras ópticas, linhas telefônicas etc. Na internet, fazer broadcast é geralmente fazer transmissão de vídeos e músicas.No caso eu estava com Sportify e o YouTube abertos no navegador Opera.

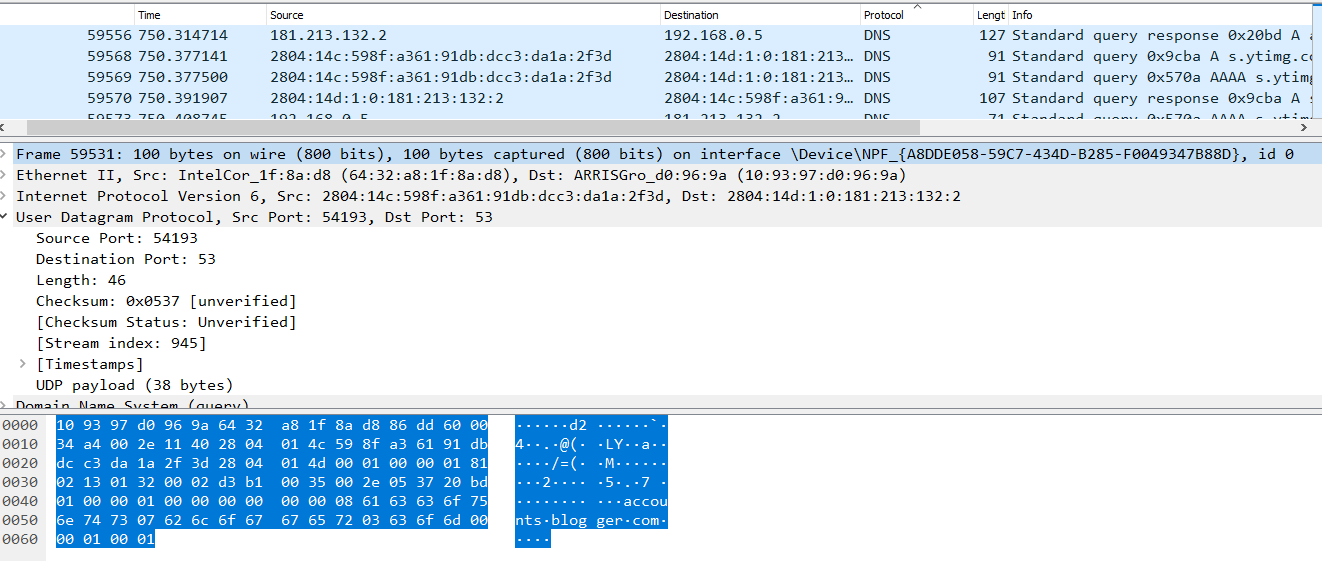
Já esse pacote não é um ACK devido não ser um protocolo TCP.O número de sequência analisado foi o 1 e utilizou-se ARP (Address Resolution Protocol) no qual foi o seu projeto é genérico, podendo ser usado em outros tipos de tecnologias de rede tais como Token-Ring e FDDI.O endereço MAC utilizado foi A8DDE058-59C7-434D-B285-F0049347B88D, tendo capturado 60 bytes (480 bits).Veja a imagem abaixo do protocolo analisado.

Figura 1: Detalhes do pacote utilizando o Wireshark



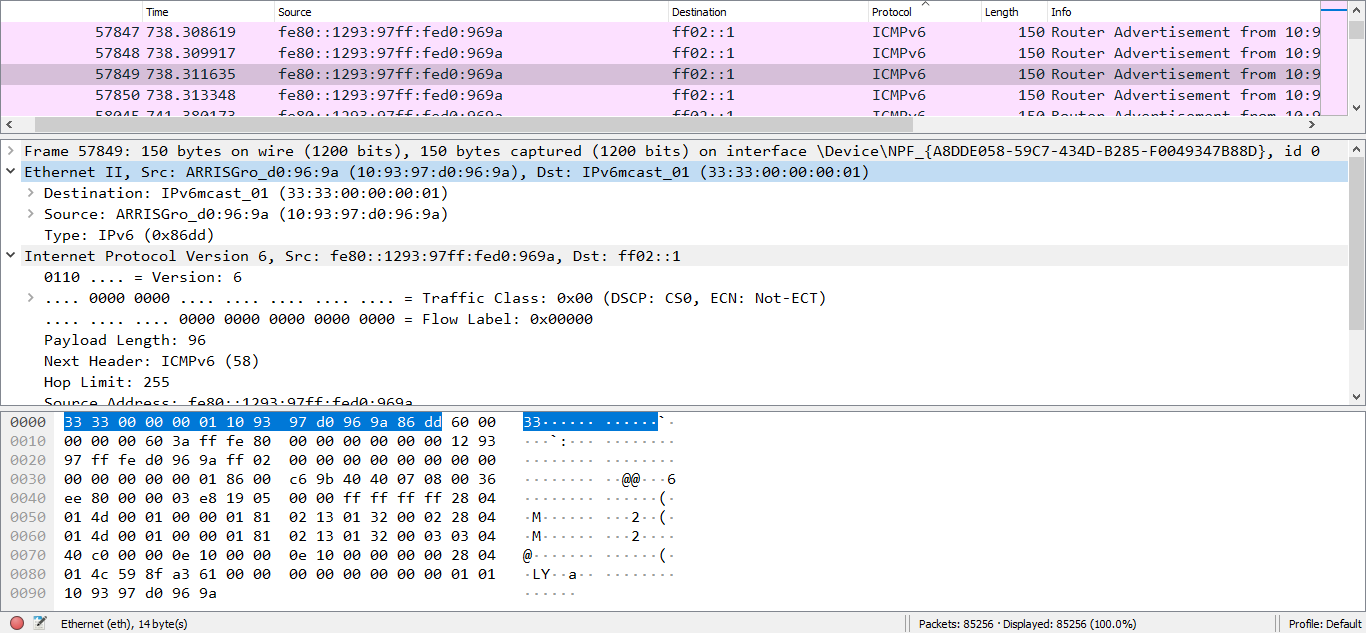
Agora o DNS (Domain Name System) no pacote o endereço de origem era 2804:14c:598f:a361:91db:dcc3:da1a:2f3d e o destino era 2804:14d:1:0:181:213:132:2 e o tamanho de 100 bytes (800 bits) e o número de sequência 59531.E o endereço MAC é A8DDE058-59C7-434D-B285-F0049347B88D, e a versão IP (versão 6) é um novo pacote de protocolos padrão para a camada de rede da Internet. O IPv6 foi projetado para resolver muitos dos problemas da versão atual do pacote de protocolos IP (conhecido como IPv4) relacionados ao o esgotamento de endereços, a segurança, a configuração automática, a necessidade de extensibilidade e outros.Houve a utilização do protocolo UDP para transferir arquivos e a porta de origem foi 54193 e a porta de destino foi 53.Abaixo tem a imagem com mais detalhes do protocolos. Tal ação pode ter acontecido devido o YouTube está sendo utilizado no navegador Opera.

Figura 2: Detalhes do pacote utilizando o Wireshark



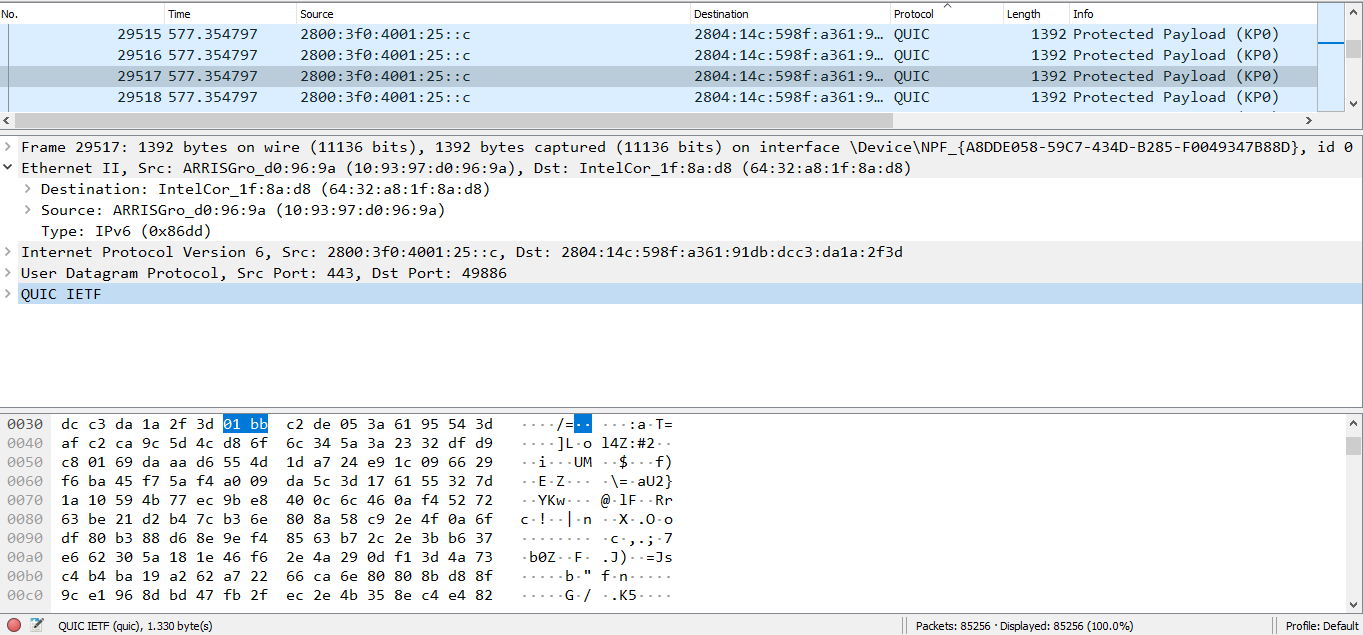
Agora com o pacote ICMPv6 o endereço de origem foi fe80::1293:97ff:fed0:969ª e o endereço de destino ff02::1 na qual possui tamanho de 150 bytes (1200 bits) na qual possui endereço MAC A8DDE058-59C7-434D-B285-F0049347B88D.Na camada ethernet a origem é ARRISGro\_d0:96:9a e o destino foi 10:93:97:d0:96:9a, a versão do protocolo IP é 6 com endereço MAC: ARRISGro\_d0:96:9a (10:93:97:d0:96:9a).Abaixo temos a imagem com detalhes do pacote.

Figura 3: Detalhes do pacote utilizando o Wireshark



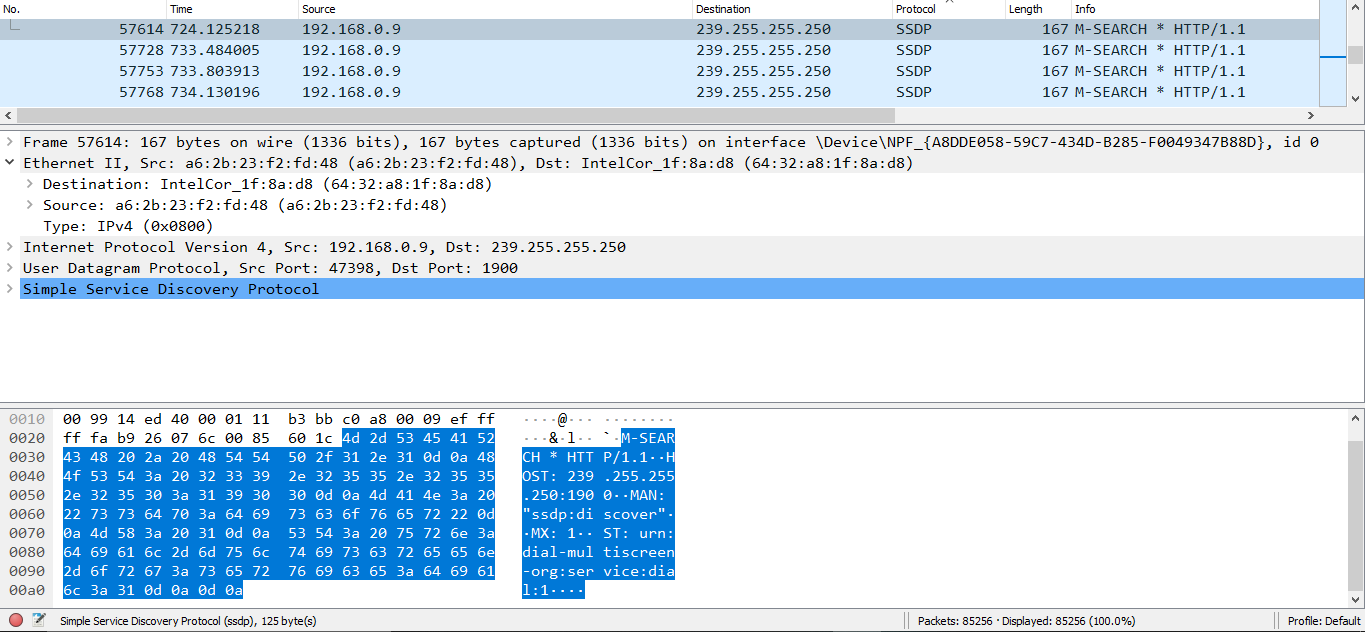
O próximo protocolo a ser analisado será um pacote utilizando QUIC  o novo protocolo desenvolvido pela Google tem a intenção de combinar os recursos do HTTP/2, TCP, UDP e TLS (criptografia), entre outras.A origem foi 2800:3f0:4001:25::c e o destino dos dados eram 2804:14c:598f:a361:91db:dcc3:da1a:2f3d com um tamanho de 1392 bytes (11.136 bits), com um endereço MAC A8DDE058-59C7-434D-B285-F0049347B88D e na Enthenet possuindo o endereço de origem ARRISGro\_d0:96:9a (10:93:97:d0:96:9a) e destino IntelCor\_1f:8a:d8 (64:32:a8:1f:8a:d8), possuindo protocolo IP versão 6 (com origem 2800:3f0:4001:25::c e destino 2804:14c:598f:a361:91 db:dcc3:da1a:2f3d).Devido estar utilizando o YouTube usa-se o protocolo UDP com a porta de origem 443 e a porta de destino 49886.A imagem abaixo é exibido os detalhes do pacote analisado.

Figura 4: Detalhes do pacote utilizando o Wireshark



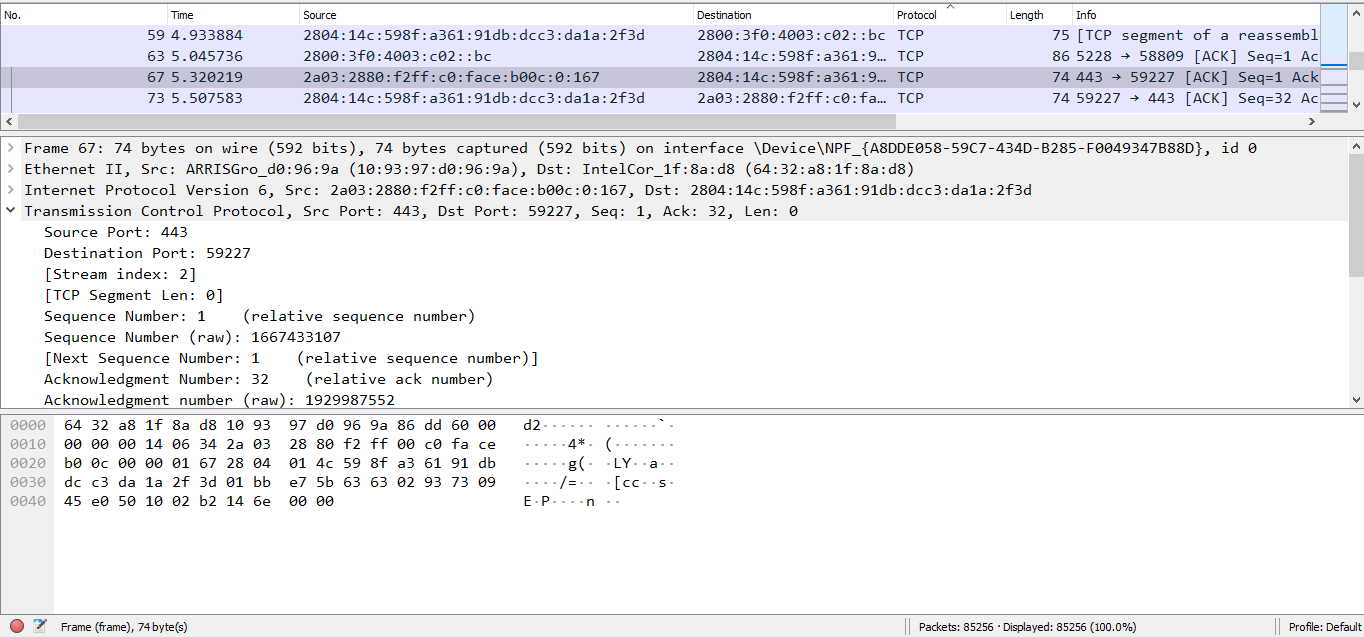
O número de sequência 57514 com origem 192.168.0.9 e destino de 239.255.255 .250 e com protocolo SSDP, possuindo o tamanho de pacote de 167 bytes (1336 bits), possuindo o endereço MAC A8DDE058-59C7-434D-B285-F0049347B88D.Os detalhes do pacote na camada de Enlace com a origem a6:2b:23:f2:fd:48 (a6:2b:23:f2:fd:48) e destino IntelCor\_1f:8a:d8 (64:32:a8:1f:8a:d8) do tipo IPv4.Com IP na versão 4 (com origem 192.168.0.9 e destino 239.255.255.250).Com UDP utilizando a porta 47398 e destino a porta 1900.Abaixo tem imagem com mais detalhes do pacote.

Figura 5: Detalhes do pacote utilizando o Wireshark



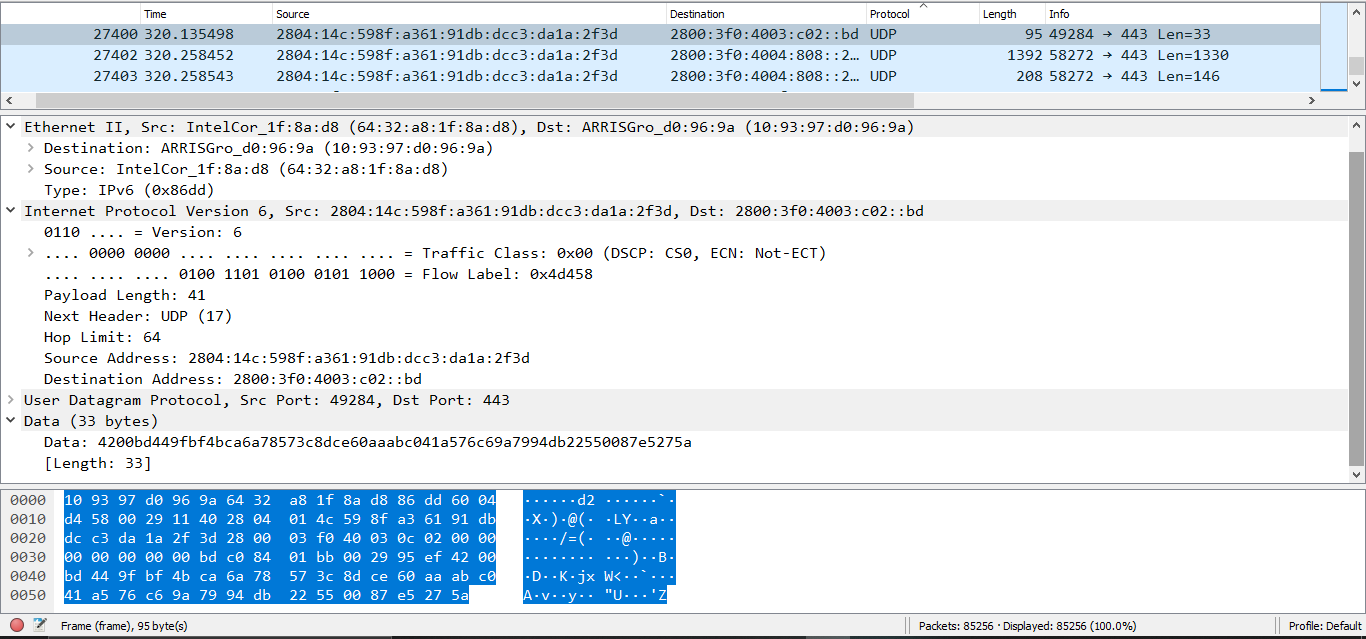
O número de sequência 67 com o endereço de origem 2a03:2880:f2ff:c0:face: b00c:0:167 e com destino 2804:14c:598f:a361:91db:dcc3:da1a:2f3d e utilizando o protocolo TCP com um tamanho de 74 bytes (592 bits) e utilizando a porta 443 e a porta de destino 59227 possuindo o endereço MAC A8DDE058-59C7-434D-B285-F0049 347B88D.Possuindo ACK sendo um número do próximo byte esperado do outro lado no qual foi comunicado, com sequência 1 e Ack 32 com Win 690.Na camada OSI a origem ARRISGro\_d0:96:9a (10:93:97:d0:96:9a) e o destino IntelCor\_1f:8a:d8 (64:32:a8:1f:8a: d8).Já a versão do IP é a 6 com origem 2a03:2880:f2ff:c0:face:b00c:0 :167 e destino 2804:14c:598f:a361:91db:dcc3:da1a:2f3d.Abaixo temos a figura com os detalhes do número de sequência.

Figura 6: Detalhes do pacote utilizando o Wireshark



O último pacote a ser analisado é o de sequência 27.400 com o endereço de origem 2804:14c:598f:a361:91db :dcc3:da1a:2f3d e de destino 2800:3f0:4003:c02::bd.Tal pacote utiliza o UDP com um tamanho de 95 bytes (760 bits) e utilizando-se do endereço MAC: A8DDE058-59C7-434D-B285-F0049347B88D.No quesito Ethernet tem como origem o IntelCor\_1f:8a:d8 (64:32:a8:1f:8a:d8) e destino o ARRISGro\_d0:96:9a (10:93:97:d0:96:9a) na qual fez-se uso do protocolo IPv6 (versão 6 do protocolo IP) com origem 2804:14c:598f:a361:91db:dcc3:da1a:2f3d e destino 2800:3f0:4003:c02::bd, as portas utilizadas pelo protocolo UDP foram 49284 como origem e 443 como destino.Abaixo tem-se uma imagem com mais detalhes.

Figura 7: Detalhes do pacote utilizando o Wireshark



**Conclusão**

O relatório foi finalizado com uma análise de aproximadamente 20 minutos e adicionado conteúdos da internet (artigos, livro, trabalhos acadêmicos e etc).Tal conteúdo foi adicionado para complementar e também devido a dificuldade na realização da análises, conceitos relacionados aos protocolos (conceito e funcionalidade), além de dificuldade em utilizar o software (Wireshark) e conhecer suas funcionalidades para a analises dos pacotes.Apesar de tais impasses muitas dúvidas foram solucionadas com referências biográficas e aulas gravadas pela plataforma Teams.

**Referências Bibliográficas**

SANDERS, Chris. **ANÁLISE DE PACOTES NA PRÁTICA**: Usando Wireshark Para Solucionar Problemas de Rede do Mundo Real. 1. ed. São Paulo: Novatec Editora Ltda, 2017. 463 p. v. 1. ISBN 978-85-7522-585-1.

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO (Espírito Santo). Laboratório de Pesquisa em Redes Multimídia. O Protocolo ARP. **O Protocolo ARP**, Espírito Santo, p. 9 – 30.

MICROSOFT. Protocolo IP versão 6. *In*: **Protocolo IP versão 6**: Protocolo IP versão 6. 1. 1. ed. [*S. l.*], 2017. Disponível em: https://docs.microsoft.com/pt-br/dotnet/framewor k/network-programming/internet-protocol-version-6#references. Acesso em: 24 nov. 2020.

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO (Espírito Santo). Laboratório de Pesquisa em Redes Multimídia. O Protocolo TCP. **O Protocolo TCP**, Espírito Santo, p. 2 - 10, 15 nov. 2010. Disponível em: http://www.inf.ufes.br/~zegonc/material/ Redes\_de\_Computadores/O%20Protocolo%20TCP.pdf. Acesso em: 24 nov. 2020.

PEREIRA , Diego. Aplicações de Redes de Computadores: Aula 10 - Camada de Transporte TCP (Transmission Control Protocol) Parte 2. **Aula 10 - Camada de Transporte TCP (Transmission Control Protocol) Parte 2**, Rio Grande do Norte, p. 1 - 22, 15 nov. 2010. Disponível em: https://docente.ifrn.edu.br/diegopereir a/disciplinas/2012/aplicacoes-de-redes-de-computadores/aula-10-camada-de-transporte-tcp-parte-2. Acesso em: 24 nov. 2020.