

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.

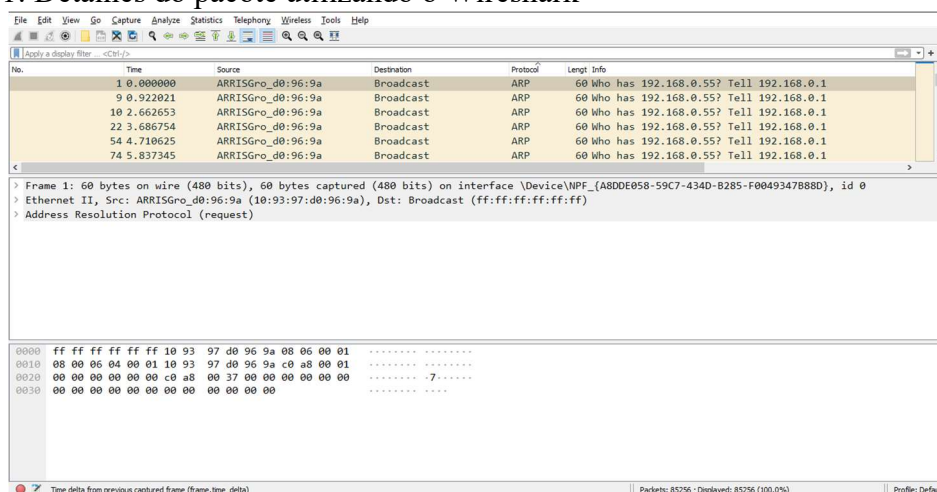
Análises de alguns dos protocolos coletados

Devido ao grande número de pacotes, será analisado apenas os pacotes de protocolos 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 Spotify 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:ccc3: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 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 protocolo. Tal ação pode ter acontecido devido o YouTube está sendo utilizado no navegador Opera.

Figura 2: Detalhes do pacote utilizando o Wireshark

Time	Source	Destination	Protocol	Length	Info
59556 750.314714	181.213.132.2	192.168.0.5	DNS	127	Standard query response 0x20bd A
59568 750.377141	2804:14c:598f:a361:91db:ccc3:da1a:2f3d	2804:14d:1:0:181:213...	DNS	91	Standard query 0x9cba A s.ytimg.co
59569 750.377500	2804:14c:598f:a361:91db:ccc3:da1a:2f3d	2804:14d:1:0:181:213...	DNS	91	Standard query 0x570a AAAA s.ytimg.co
59570 750.391907	2804:14d:1:0:181:213:132:2	2804:14c:598f:a361:9...	DNS	107	Standard query response 0x9cba A
59573 750.409745	181.213.132.2	192.168.0.5	DNS	74	Standard query 0x570a AAAA s.ytimg.co

> Frame 59531: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface \Device\NPF_{A8DDE058-59C7-434D-B285-F0049347B88D}, id 0	
> Ethernet II, Src: IntelCor_1f:8a:d8 (64:32:a8:1f:8a:d8), Dst: ARRISGro_d0:96:9a (10:93:97:d0:96:9a)	
> Internet Protocol Version 6, Src: 2804:14c:598f:a361:91db:ccc3:da1a:2f3d, Dst: 2804:14d:1:0:181:213:132:2	
> User Datagram Protocol, Src Port: 54193, Dst Port: 53	
Source Port: 54193 Destination Port: 53 Length: 46 Checksum: 0xa0537 [unverified] [Checksum Status: Unverified] [Stream index: 945] > [Timestamps] UDP payload (38 bytes)	
> Domain Name System (query)	
0000	10 93 97 d0 96 9a 64 32 a8 1f 8a d8 86 dd 60 00
0010	34 a4 00 2e 11 40 28 04 01 4c 59 8f a3 61 91 db
0020	dc c3 da 1a 2f 3d 28 04 01 4d 00 01 00 00 01 81
0030	02 13 01 32 00 02 d3 b1 00 35 00 2e 05 37 20 bd
0040	01 00 00 01 00 00 00 00 00 00 08 61 63 63 6f 75
0050	6e 74 73 07 62 6c 6f 67 67 65 72 03 63 6f 6d 00
0060	00 01 00 01

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

The image shows a Wireshark packet capture of an ICMPv6 Router Advertisement. The packet list at the top shows several ICMPv6 packets. The selected packet (No. 57847) is expanded in the packet details pane, showing the Ethernet II header, Internet Protocol Version 6 header, and the ICMPv6 payload. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
57847	738.308619	fe80::1293:97ff:fed0:969a	ff02::1	ICMPv6	150	Router Advertisement from 10:9
57848	738.309917	fe80::1293:97ff:fed0:969a	ff02::1	ICMPv6	150	Router Advertisement from 10:9
57849	738.311635	fe80::1293:97ff:fed0:969a	ff02::1	ICMPv6	150	Router Advertisement from 10:9
57850	738.313348	fe80::1293:97ff:fed0:969a	ff02::1	ICMPv6	150	Router Advertisement from 10:9

Packet Details:

- Ethernet II, Src: ARRISGro_d0:96:9a (10:93:97:d0:96:9a), Dst: IPv6mcast_01 (33:33:00:00:00:01)
- Destination: IPv6mcast_01 (33:33:00:00:00:01)
- Source: ARRISGro_d0:96:9a (10:93:97:d0:96:9a)
- Type: IPv6 (0x86dd)
- Internet Protocol Version 6, Src: fe80::1293:97ff:fed0:969a, Dst: ff02::1
- 0110 = Version: 6
- 0000 0000 = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
- 0000 0000 0000 0000 = Flow Label: 0x000000
- Payload Length: 96
- Next Header: ICMPv6 (58)
- Hop Limit: 255
- Source Address: fe80::1293:97ff:fed0:969a

Packet Bytes:

```

0000 33 33 00 00 00 01 10 93 97 d0 96 9a 86 dd 60 00 33 .....
0010 00 00 00 60 3a ff fe 80 00 00 00 00 00 12 93 .....
0020 97 ff fe d0 96 9a ff 02 00 00 00 00 00 00 00 .....
0030 00 00 00 00 01 86 00 c6 9b 40 40 07 08 00 36 .....
0040 ee 00 00 00 03 e8 19 05 00 00 ff ff ff 28 04 .....
0050 01 4d 00 01 00 01 81 02 13 01 32 00 03 04 .....
0060 01 4d 00 01 00 01 81 02 13 01 32 00 03 04 .....
0070 40 c0 00 00 0a 10 00 00 0a 10 00 00 00 28 04 .....
0080 01 4c 59 8f a3 61 00 00 00 00 00 00 01 01 .....
0090 10 93 97 d0 96 9a .....
  
```

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:ccc3: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:a361:91db:ccc3: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

The image shows a Wireshark packet capture of a QUIC packet. The packet list at the top shows several QUIC packets. The selected packet (No. 29517) is expanded in the packet details pane, showing the Ethernet II header, Internet Protocol Version 6 header, User Datagram Protocol header, and the QUIC payload. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
29515	577.354797	2800:3f0:4001:25::c	2804:14c:598f:a361:9...	QUIC	1392	Protected Payload (KP0)
29516	577.354797	2800:3f0:4001:25::c	2804:14c:598f:a361:9...	QUIC	1392	Protected Payload (KP0)
29517	577.354797	2800:3f0:4001:25::c	2804:14c:598f:a361:9...	QUIC	1392	Protected Payload (KP0)
29518	577.354797	2800:3f0:4001:25::c	2804:14c:598f:a361:9...	QUIC	1392	Protected Payload (KP0)

Packet Details:

- Ethernet II, Src: ARRISGro_d0:96:9a (10:93:97:d0:96:9a), Dst: IntelCor_1f:8a:d8 (64:32:a8:1f:8a:d8)
- Destination: IntelCor_1f:8a:d8 (64:32:a8:1f:8a:d8)
- Source: ARRISGro_d0:96:9a (10:93:97:d0:96:9a)
- Type: IPv6 (0x86dd)
- Internet Protocol Version 6, Src: 2800:3f0:4001:25::c, Dst: 2804:14c:598f:a361:91db:ccc3:da1a:2f3d
- User Datagram Protocol, Src Port: 443, Dst Port: 49886
- QUIC IETF

Packet Bytes:

```

0030 dc c3 da 1a 2f 3d 01 bb c2 de 05 3a 61 95 54 3d .....
0040 af c2 ca 9c 5d 4c d8 6f 6c 34 5a 3a 23 32 df d9 .....
0050 c8 01 69 da aa d6 55 4d 1d a7 24 e9 1c 09 66 29 .....
0060 f6 ba 45 f7 5a f4 a0 09 da 5c 3d 17 61 55 32 7d .....
0070 1a 10 59 4b 77 ec 9b e8 40 0c 6c 4e 0a f4 52 72 .....
0080 63 be 21 d2 b4 7c b3 6e 80 8a 58 c9 2e 4f 0a 6f .....
0090 df 80 b3 88 d6 8e 9e f4 85 63 b7 2c 2e 3b b6 37 .....
00a0 e6 62 30 5a 18 1e 46 f6 2e 4a 29 0d f1 3d 4a 73 .....
00b0 c4 b4 ba 19 a2 62 a7 22 66 ca 6e 80 80 8b d8 8f .....
00c0 9c e1 96 8d bd 47 fb 2f ec 2e 4b 35 8e c4 e4 82 .....
  
```

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

The image shows a Wireshark capture of an SSDP M-SEARCH packet. The packet list at the top shows four packets of type SSDP, all with source 192.168.0.9 and destination 239.255.255.250. The packet details pane shows the following structure:

- Frame 57614: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits) on interface \Device\NPF_{A8DDE058-59C7-434D-B285-F0049347B88D}, id 0
- Ethernet II, Src: a6:2b:23:f2:fd:48 (a6:2b:23:f2:fd:48), Dst: IntelCor_1f:8a:d8 (64:32:a8:1f:8a:d8)
 - Destination: IntelCor_1f:8a:d8 (64:32:a8:1f:8a:d8)
 - Source: a6:2b:23:f2:fd:48 (a6:2b:23:f2:fd:48)
 - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.0.9, Dst: 239.255.255.250
- User Datagram Protocol, Src Port: 47398, Dst Port: 1900
- Simple Service Discovery Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII. The ASCII column shows the SSDP message: "M-SEARCH * HTTP/1.1\r\nST: 239.255.255.250:1900\r\nMAN: \"ssdp:discover\"\r\nMX: 1\r\nST: urn:schemas-upnp-org:service:discovery:1\r\n\r\n".

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:ccc3: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-F0049347B88D.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:ccc3:da1a:2f3d.Abaixo temos a figura com os detalhes do número de sequência.

Figura 6: Detalhes do pacote utilizando o Wireshark

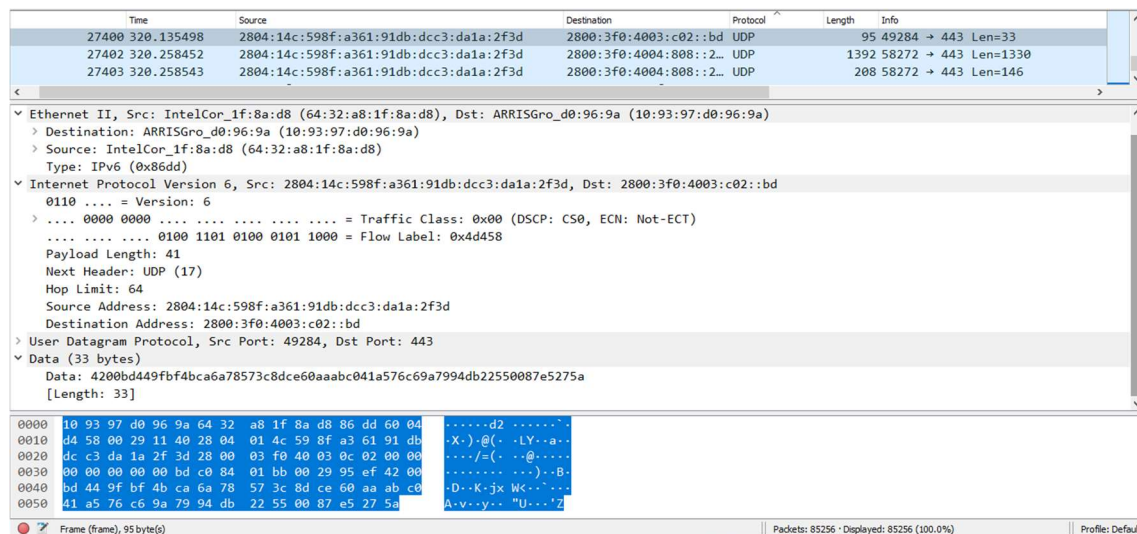
The image shows a Wireshark capture of a TCP segment. The packet list at the top shows four packets of type TCP, all with source 2a03:2880:f2ff:c0:face:b00c:0:167 and destination 2804:14c:598f:a361:91db:ccc3:da1a:2f3d. The packet details pane shows the following structure:

- Frame 67: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{A8DDE058-59C7-434D-B285-F0049347B88D}, id 0
- Ethernet II, Src: ARRISGro_d0:96:9a (10:93:97:d0:96:9a), Dst: IntelCor_1f:8a:d8 (64:32:a8:1f:8a:d8)
- Internet Protocol Version 6, Src: 2a03:2880:f2ff:c0:face:b00c:0:167, Dst: 2804:14c:598f:a361:91db:ccc3:da1a:2f3d
- Transmission Control Protocol, Src Port: 443, Dst Port: 59227, Seq: 1, Ack: 32, Len: 0
 - Source Port: 443
 - Destination Port: 59227
 - [Stream index: 2]
 - [TCP Segment Len: 0]
 - Sequence Number: 1 (relative sequence number)
 - Sequence Number (raw): 1667433107
 - [Next Sequence Number: 1 (relative sequence number)]
 - Acknowledgment Number: 32 (relative ack number)
 - Acknowledgment number (raw): 1929987552

The packet bytes pane shows the raw data in hexadecimal and ASCII. The ASCII column shows the TCP segment: "4* (LY... [cc... P...".

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 análises 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/framework/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/diegopereira/disciplinas/2012/aplicacoes-de-redes-de-computadores/aula-10-camada-de-transporte-tcp-parte-2>. Acesso em: 24 nov. 2020.