UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA - CIn
RESIDÊNCIA EM ROBÓTICA E INTELIGÊNCIA ARTIFICIAL - SOFTEX

ALINE ASSAKA TANI

CAPTURA DE PACOTES UTILIZANDO A FERRAMENTA WIRESHARK

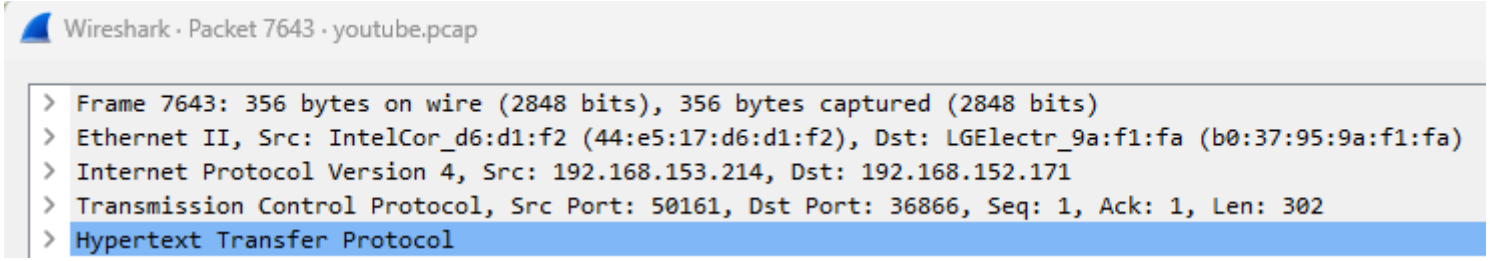
Recife,
2023

O presente trabalho teve como objetivo analisar o tráfego de rede ao se acessar o site www.youtube.com utilizando a ferramenta WireShark. Abaixo é apresentado o fluxo ocorrido para acesso ao site mencionado anteriormente:

No.	Time	Source	Destination	Protocol	Length	Info
7637	20.897479	192.168.153.214	192.168.152.171	TCP	66	50161 → 36866 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7641	20.899101	192.168.152.171	192.168.153.214	TCP	66	36866 → 50161 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
7642	20.899210	192.168.153.214	192.168.152.171	TCP	54	50161 → 36866 [ACK] Seq=1 Ack=1 Win=131328 Len=0
7643	20.899444	192.168.153.214	192.168.152.171	HTTP	356	GET /apps/YouTube HTTP/1.1
7646	20.901240	192.168.152.171	192.168.153.214	TCP	54	36866 → 50161 [ACK] Seq=1 Ack=303 Win=30336 Len=0
7659	20.938788	192.168.152.171	192.168.153.214	HTTP/X…	509	HTTP/1.1 200 OK

As linhas 7637, 7641 e 7642 apresentam a conexão TCP sendo criada entre a origem (192.168.153.214 - meu computador) e o destino (192.168.152.171 - site do youtube), seguindo o protocolo SYN -> SYN ACK -> ACK (aperto de mão de três vias)

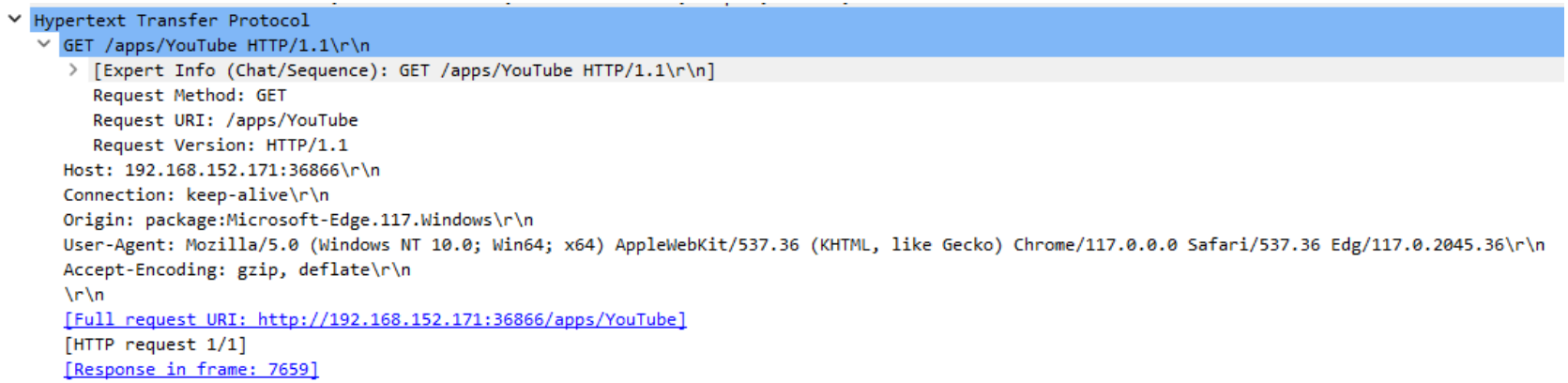
A linha 7643 apresenta o pedido do meu computador ao servidor web uma solicitação HTTP do tipo GET:



Foi solicitado que fossem explicados os campos dos cabeçalhos dos protocolos para todas as camadas (Enlace, Rede, Transporte e Aplicação) e o objetivo de cada protocolo no contexto da captura HTTP:

1. Camada de Aplicação:

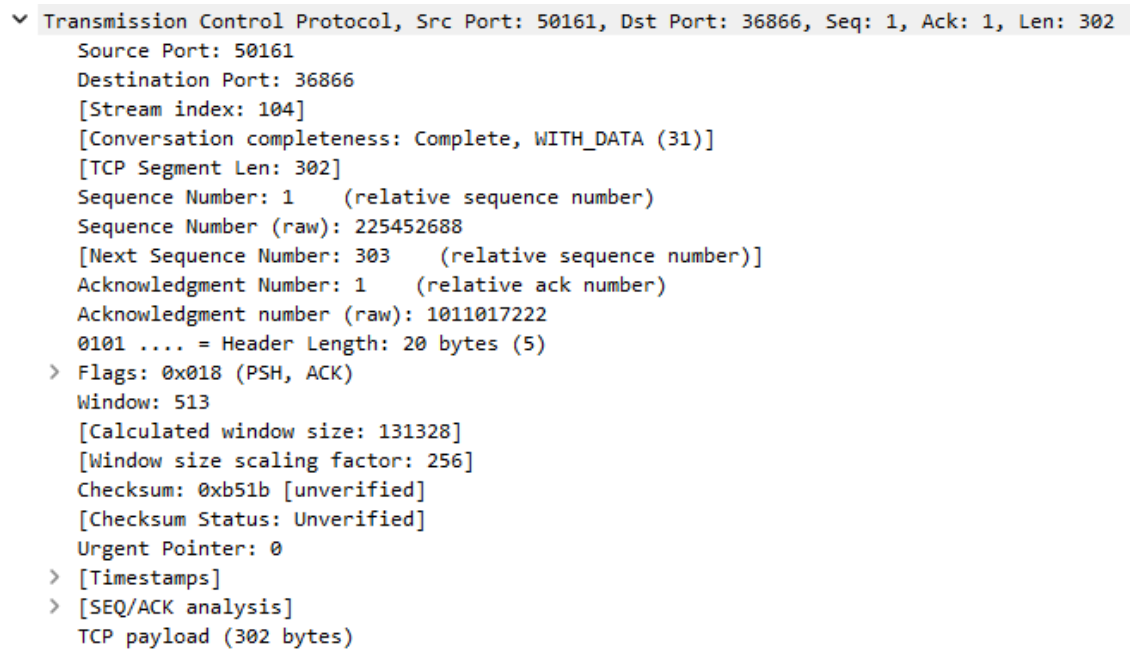
   O Hypertext Transfer Protocol (HTTP) é o protocolo usado na camada de aplicação que especifica como deverá se dar a comunicação entre o navegador do cliente e o servidor web, com o objetivo de permitir a troca de informações entre si. É mostrado abaixo o cabeçalho da solicitação HTTP:



1.1. **Request Method: GET:** método de requisição, neste caso é o GET, que é utilizado para obter recursos do servidor;
1.2. **Request URI: /apps/YouTube:** caminho e identificador do site solicitado pelo cliente
1.3. **Request Version: HTTP/1.1:** versão do HTTP
1.4. **Host: 192.168.152.171:36866:** IP do servidor web em que o cliente está solicitando um GET
1.5. **Connection: keep-alive:** tipo de conexão keep-alive, que significa que a conexão vai se manter, não sendo interrompida ao receber a resposta da requisição GET
1.6. **Origin: package:Microsoft-Edge.117.Windows:** Navegador do cliente
1.7. **User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36 Edg/117.0.2045.36\r\n:** informações acerca dos navegadores existentes
1.8. **[Full request URI: http://192.168.152.171:36866/apps/YouTube]:** o URL completo

2. Camada de Transporte:

O TCP é o protocolo de controle e transmissão utilizado na camada de transporte e define como os dados serão transmitidos entre as duas partes do processo de maneira a garantir uma comunicação confiável e orientada à conexão. O TCP ainda é responsável por detectar possíveis erros ocasionados durante a transmissão de dados, gerencia a segmentação e remontagem de dados e pela retransmissão de dados. É mostrado abaixo o cabeçalho da solicitação TCP:



2.1. **[Conversation completeness: Complete, WITH_DATA (31)]:** mostra que a conversa está completa após 31 pacotes de dados

2.2. **[TCP Segment Len: 302]:** tamanho do segmento TCP

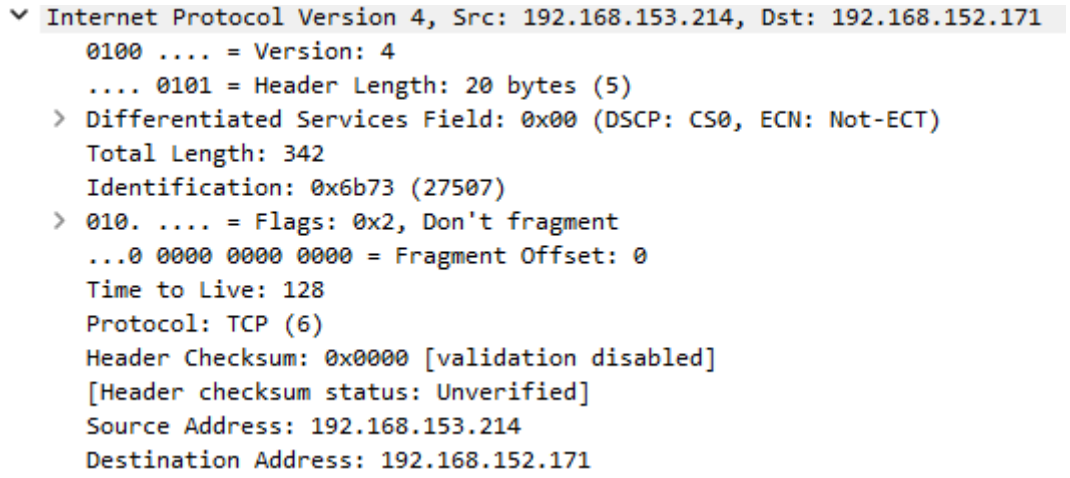
2.3. **Sequence Number: 1 (relative sequence number):** número do primeiro pacote (utilizado para organizar os pacotes recebidos e montá-los em ordem)

2.4. **[Next Sequence Number: 303 (relative sequence number)]:** o próximo número da sequência

2.5. **0101 .... = Header Length: 20 bytes (5):** comprimento do cabeçalho TCP (20 bytes)

3. Camada de Rede:

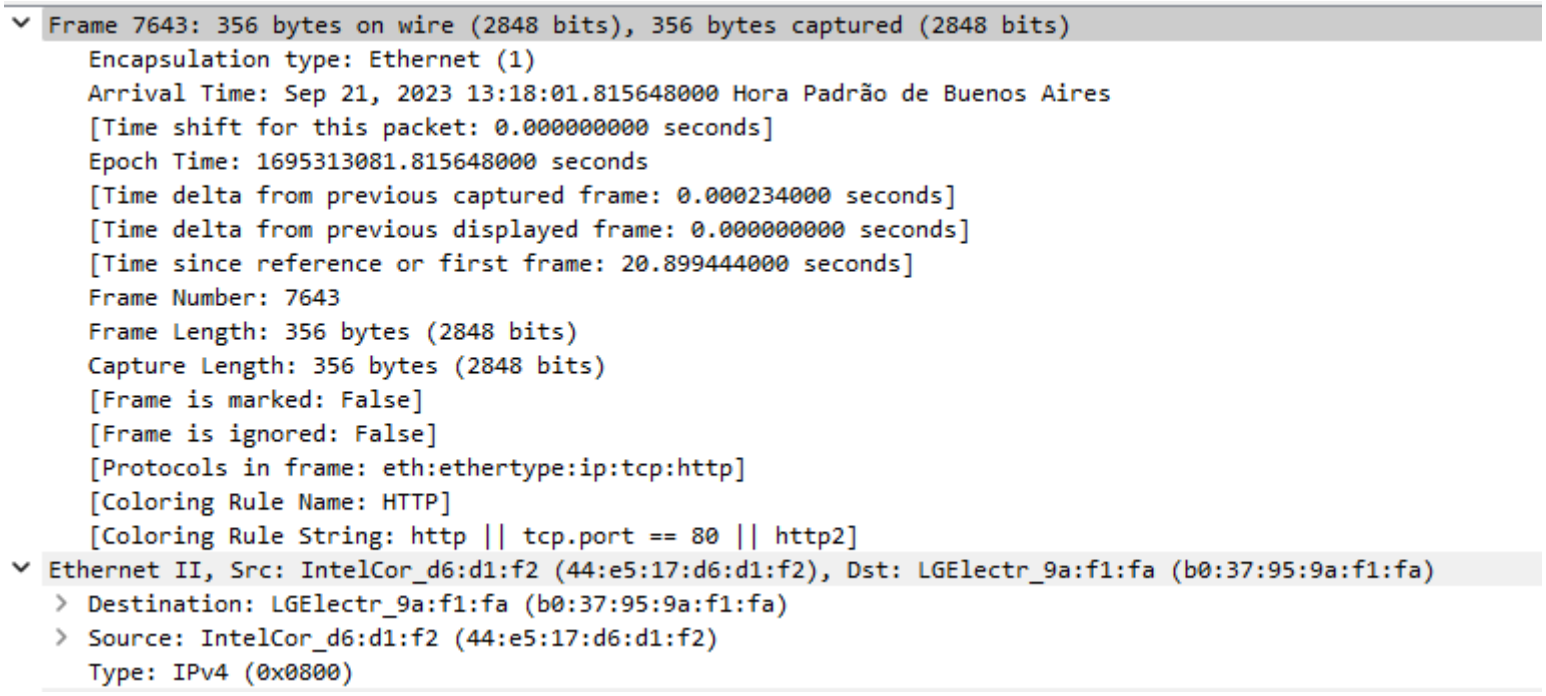
O IPV4 é um protocolo da camada de rede que tem como objetivo reger como os outros protocolos e tecnologias de redes interagem em uma rede, tem como função identificar e endereçar dispositivos em redes IP. É mostrado abaixo o cabeçalho da solicitação IPV4:



3.1. **0100 .... = Version: 4:** Versão do IPV4
3.2. **.... 0101 = Header Length: 20 bytes (5):** comprimento do cabeçalho IPv4 (20 bytes)
3.3. **Total Length: 342:** comprimento total do pacote IPv4 (342 bytes)
3.4. **Identification: 0x6b73 (27507):** número de identificação do pacote
3.5. **010. .... = Flags: 0x2, Don't fragment:** atributo que rege a não fragmentação do pacote durante o trânsito
3.6. **...0 0000 0000 0000 = Fragment Offset: 0:** não há threshold para fragmentação
3.7. **Time to Live: 128:** número máximo de saltos
3.8. **Protocol: TCP (6):** protocolo de transporte usado
3.9. **Source Address: 192.168.153.214:** IP de origem
3.10. **Destination Address: 192.168.152.171:** IP de destino

4. Camada de Enlace:

Na camada de Enlace o frame Ethernet se refere a uma unidade básica de transmissão de dados em uma rede Ethernet e tem como objetivo transmitir dados em uma rede. É mostrado abaixo o cabeçalho do quadro Ethernet:



Ethernet II: quadro formato Ethernet II

4.1. **Destination: LGElectr_9a:f1:fa (b0:37:95:9a:f1:fa):** Endereço MAC de destino

4.2. **Source: IntelCor_d6:d1:f2 (44:e5:17:d6:d1:f2):** Endereço MAC de origem

4.3. **Type: IPv4 (0x0800):** tipo de protocolo encapsulado

4.4. **Internet Protocol Version 4, Src: 192.168.153.214, Dst: 192.168.152.171:** IP de origem e destino, respectivamente, para a camada de rede

4.5. **Transmission Control Protocol, Src Port: 50161, Dst Port: 36866, Seq: 1, Ack: 1, Len: 302:** Portas de origem e destino para a camada de transporte
4.6. **Hypertext Transfer Protocol:** tipo de protocolo para a camada de aplicação

Frame 7643: número do quadro capturado

4.7. **Encapsulation type: Ethernet (1):** encapsulamento do quadro é do tipo Ethernet
4.8. **[Time delta from previous captured frame: 0.000234000 seconds]:** tempo decorrido entre a captura do quadro anterior até a captura do quadro atual
4.9. **[Time delta from previous displayed frame: 0.000000000 seconds]:** tempo decorrido entre a exibição do quadro anterior até a captura do quadro atual
4.10. **[Time since reference or first frame: 20.899444000 seconds]: te**mpo decorrido entre a captura do primeiro quadro até a captura do quadro atual
4.11. **Frame Length: 356 bytes (2848 bits):** tamanho total do quadro em bytes (356 bytes)
4.12. **Capture Length: 356 bytes (2848 bits):** tamanho do quadro capturado