

Análise da Captura do Tráfego de Redes via Wireshark e TCPDump: Um comparativo do consumo de dados na plataforma Discord

Fernanda Maria de Souza

Nikolas Jensen

Matias Giuliano Gutierrez Benitez

Vinicius Takeo Friedrich Kuwaki



UDESC
UNIVERSIDADE
DO ESTADO DE
SANTA CATARINA

Seções

Introdução

Ferramentas

Discord

Skype

Wireshark

TCPDump

Casos de Estudo

Trabalho Referenciado

Objetivo

Coleta de Dados

Análise

Análise

Conclusões

Caso de estudo

Objetivo

Coleta de Dados

Análise

Conclusões

Introdução

- Implicações do COVID-19;
- Mudança de hábitos;
- Comunicações humanas;
- Utilização de ferramentas:
 - Skype;
 - Discord;



Figura 1: Discord e Skype.

Introdução

- Objetivo do trabalho:
 - Comparativo;
 - Discord x Skype;
 - Com base em (KASSIM et al., 2017);
- Ferramentas utilizadas:
 - Wireshark;
 - TCPDump;
- Captura de pacotes;

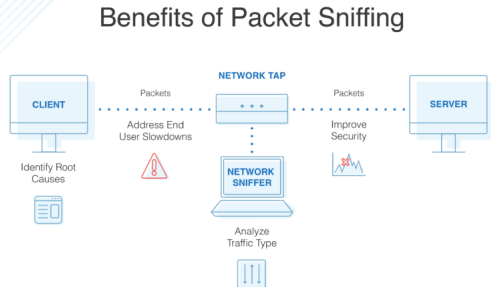


Figura 2: Estrutura dos *Sniffers* de Rede.

Seções

Introdução

Ferramentas

Discord

Skype

Wireshark

TCPDump

Casos de Estudo

Trabalho Referenciado

Objetivo

Coleta de Dados

Análise

Análise

Conclusões

Caso de estudo

Objetivo

Coleta de Dados

Análise

Conclusões

Considerações Finais

- Ferramentas de comunicação:
 - Discord;
 - Skype;
- Ferramentas de *Sniffing*:
 - Wireshark;
 - TCPDump;

Discord

- Criado por Jason Citron e Stan Vishnevskiy;
- Utilização em jogos online;
- Disponibilizada ao mundo em 2015;
- Atualmente:
 - 100 milhões de usuários ativos por mês;
 - + de 4 horas diárias;

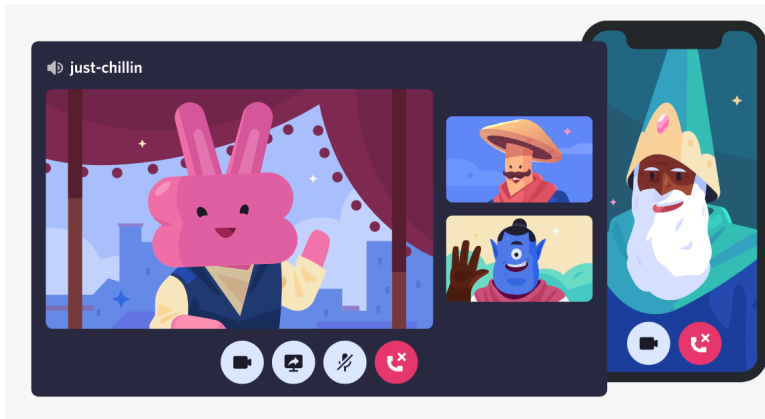


Figura 3: Representação gráfica da interface do Discord.

Skype

- Lançado em 2003;
- Criado por Janus Friis e Niklas Zennstrom;
- Atualmente pertence a Microsoft;



Figura 4: Apresentação do Skype no site da Microsoft.

- Analisador de tráfego de rede;
- Multiplataforma;
- Código aberto;
- Apresenta os pacotes capturados;
- Organizando-os por protocolos;

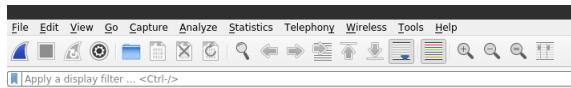


Figura 5: Interface do Wireshark.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.0.13	224.0.0.251	MDNS	136	Standard query 0x0006 PTR %9E5E7C8F47989526C98CD95024084F6F0...
2	2.561240744	192.168.0.17	34.73.232.153	TCP	66	47296 → 443 [ACK] Seq=1 Ack=1 Win=3967 Len=0 TSval=286791584...
3	2.696569680	34.73.232.153	192.168.0.17	TCP	66	[TCP ACKed unseen segment] 443 → 47296 [ACK] Seq=1 Ack=2 Win=...
4	4.525270467	192.168.0.17	107.167.110.216	TCP	66	58946 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=2591488412...
5	5.762596399	192.168.0.17	205.185.194.197	TLSv1.2	129	Application Data
6	5.830256725	205.185.194.197	192.168.0.17	TCP	66	443 → 46713 [ACK] Seq=1 Ack=64 Win=1025 Len=0 TSval=179170007...
7	5.889785220	34.73.232.153	192.168.0.17	TLSv1.2	100	Application Data
8	5.890282459	192.168.0.17	34.73.232.153	TLSv1.2	104	Application Data
9	6.026331014	34.73.232.153	192.168.0.17	TCP	66	443 → 47338 [ACK] Seq=35 Ack=39 Win=1331 Len=0 TSval=25444026...
10	6.577209927	192.168.0.17	34.107.195.226	TCP	66	40874 → 443 [ACK] Seq=1 Ack=1 Win=16844 Len=0 TSval=296615936...
11	6.593233008	2804:14c:f287:9804::...	2800:3f0:4003:c01::...	TCP	86	52350 → 5228 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=1646960558...
12	6.598216888	34.107.195.226	192.168.0.17	TCP	66	[TCP ACKed unseen segment] 443 → 40874 [ACK] Seq=1 Ack=2 Win=...
13	6.659011850	2800:3f0:4003:c01::...	2804:14c:f287:9804::...	TCP	86	[TCP ACKed unseen segment] 5228 → 52350 [ACK] Seq=1 Ack=2 Win=...

Figura 6: Captura de pacotes no Wireshark.

- Desenvolvido pelo grupo *Network Research Group*;
- Baseado em linha de comando;
- Possui uma versão para Windows;

```
root@TakeoPC: /home/takeofriedrich
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda
root@TakeoPC:/home/takeofriedrich# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
20:47:02.912248 IP 192.168.0.14.38966 > 192.168.0.255.65001: UDP, length 20
20:47:02.912801 IP6 TakeoPC.39887 > 2804:14d:1:0:181:213:132:3.domain: 58938+ [1
au] PTR? 255.0.168.192.in-addr.arpa. (55)
20:47:02.920822 IP6 2804:14d:1:0:181:213:132:3.domain > TakeoPC.39887: 58938 NXD
omain* 0/1/1 (141)
20:47:02.920953 IP6 TakeoPC.39887 > 2804:14d:1:0:181:213:132:3.domain: 58938+ PT
R? 255.0.168.192.in-addr.arpa. (44)
20:47:02.928729 IP6 2804:14d:1:0:181:213:132:3.domain > TakeoPC.39887: 58938 NXD
omain* 0/1/0 (130)
20:47:02.929319 IP6 TakeoPC.45997 > 2804:14d:1:0:181:213:132:3.domain: 37636+ [1
au] PTR? 14.0.168.192.in-addr.arpa. (54)
20:47:02.938185 IP6 2804:14d:1:0:181:213:132:3.domain > TakeoPC.45997: 37636 NXD
omain* 0/1/1 (140)
20:47:02.938324 IP6 TakeoPC.45997 > 2804:14d:1:0:181:213:132:3.domain: 37636+ PT
R? 14.0.168.192.in-addr.arpa. (43)
20:47:02.946560 IP6 2804:14d:1:0:181:213:132:3.domain > TakeoPC.45997: 37636 NXD
omain* 0/1/0 (129)
20:47:02.947204 IP6 TakeoPC.59151 > 2804:14d:1:0:181:213:132:3.domain: 7899+ [1a
u] PTR? 3.0.0.0.2.3.1.0.3.1.2.0.1.8.1.0.0.0.0.0.1.0.0.0.d.4.1.0.4.0.8.2.ip6.arpa
. (101)
20:47:02.954764 IP6 2804:14d:1:0:181:213:132:3.domain > TakeoPC.59151: 7899 NXDo
```

Figura 7: Uso do TCPDump.

Seções

Introdução

Ferramentas

Discord

Skype

Wireshark

TCPDump

Casos de Estudo

Trabalho Referenciado

Objetivo

Coleta de Dados

Análise

Análise

Conclusões

Caso de estudo

Objetivo

Coleta de Dados

Análise

Conclusões

Casos de Estudo

- Uso crescente da Internet: aprimoramento da capacidade de transmissão de dados.
- Ferramentas multimídia: Discord e Skype, respectivamente, 100 e 40 milhões de usuários ativos por mês.
- Pandemia COVID-19: mudanças na quantidade de acessos a diversas plataformas.

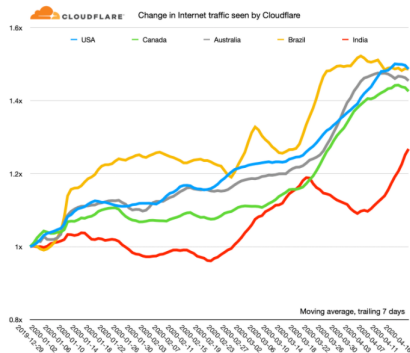


Figura 8: Mudanças no tráfego na Internet analisadas pela Cloudflare durante o período de pandemia. Fonte: (GRAHAM-CUMMING, 2020)

Casos de Estudo

- Aumento gradual do número de usuários nessas plataformas: necessidade de quantizar as informações sobre consumo de dados.
- Determinar consequências do uso de determinados softwares da categoria VoIP para rede.
- Comparação entre Skype e Discord com relação ao consumo de dados.

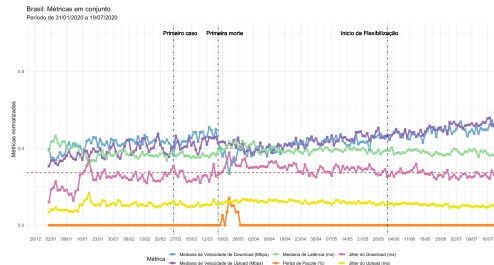


Figura 9: Impactos na qualidade da internet no Brasil durante a pandemia de COVID-19, análise realizada entre 31/01/2020 e 19/07/2020. Fonte: (BR, 2020)

Trabalho Referenciado

- Análise do software multimídia Skype foi feita por (KASSIM et al., 2017).

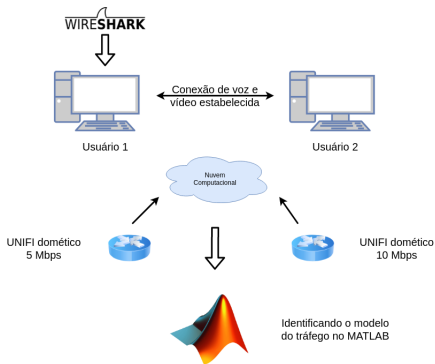


Figura 10: Arquitetura do Experimento. Adaptado de: (KASSIM et al., 2017)

Objetivo

- Análise baseada em chamadas de vídeo e voz, do tráfego de rede da aplicação Skype em uma Rede UniFi doméstica.

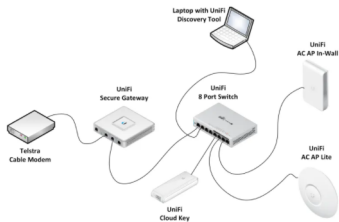


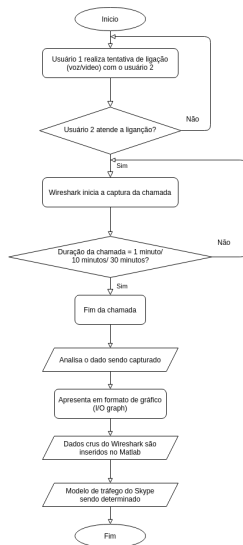
Figura 11: Rede UniFi. Adaptado de: (KASSIM et al., 2017)



Figura 12: Exemplo Rede UniFi. Adaptado de: (KASSIM et al., 2017)

Objetivo

- Determinar a quantidade de uso da largura de banda oferecida por uma rede doméstica UniFi.
- Métricas utilizadas:
 - Cálculo do uso da largura de banda;
 - RTT (Round Trip Time) - Latência;
 - Número de pacotes perdidos;
 - Análise do protocolo do Skype.
- Capturas feitas pelo Wireshark.
- Dados analisados usando o software MATLAB.



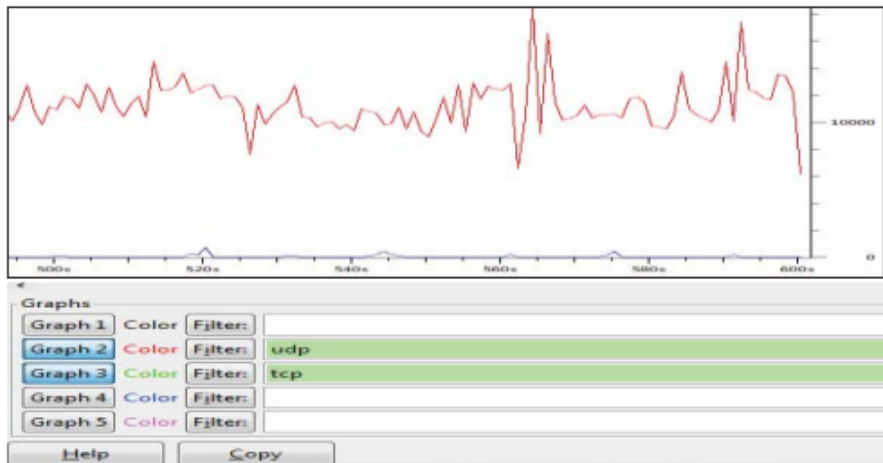


Figura 14: Gráfico I/O no *Wireshark*. Fonte: (KASSIM et al., 2017).

Minutos	Mesma Rede		Rede Diferente	
	Hora com Pico	Hora Sem-Pico	Hora com Pico	Hora Sem-Pico
1 m Voz	965.963	768.204	955.091	3.651.753
10 m Voz	5.152.728	8.345.655	9.619.294	11.486.743
30 m Voz	6.554.357	54.309.322	26.333.824	13.547.012
1 m Vídeo	8.725.198	4.208.836	8.313.583	653.401
10 m Vídeo	91.323.711	29.867.780	66.189.705	58.269.214
30 m Vídeo	199.000.000	863.000.000	181.000.000	201.000.000

Tabela 1: Largura de Banda Total para chamadas de voz e vídeo no Skype. Fonte: Adaptado de: (KASSIM et al., 2017).

Tipo de	Duração em	Mesma Rede		Rede Diferente	
		Hora com Pico	Hora Sem-Pico	Hora com Pico	Hora Sem-Pico
Aplicação Vídeo	1 minuto	0	0	3	0
	10	0	0	18	0
	30	3	125	0	0
Voz	1	0	0	2	2
	10	0	0	28	1
	30	16	743	75	0

Tabela 2: Quantidade de pacotes perdidos durante chamadas de voz e vídeo no Skype. Fonte: Adaptado de: (KASSIM et al., 2017).

Tipo de	Duração em	Mesma Rede		Rede Diferente	
		Hora com Pico	Hora Sem-Pico	Hora com Pico	Hora Sem-Pico
Aplicação Vídeo	Minutos	0,038	-	-	-
	10	0,264	0,011	0,216	0,395
	30	0,199	0,003	0,098	0,007
Voz	1	0,038	-	-	0,231
	10	0,0436	0,018	0,204	0,913
	30	0,005	0,003	0,041	0,045

Tabela 3: Tráfego em RTT. Fonte: (KASSIM et al., 2017).

Conclusões

- Skype usa mais protocolos UDP do que TCP.
- Utiliza cerca de 10% da largura de banda oferecida (considerado pouco).

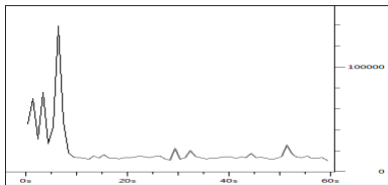


Figura 15: Duração do tráfego para chamadas de voz. Adaptado de: (KASSIM et al., 2017)

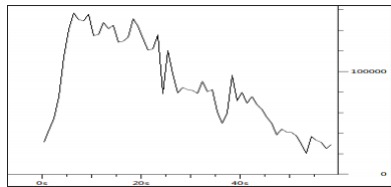


Figura 16: Duração do tráfego para chamadas de vídeo. Adaptado de: (KASSIM et al., 2017)

Caso de estudo

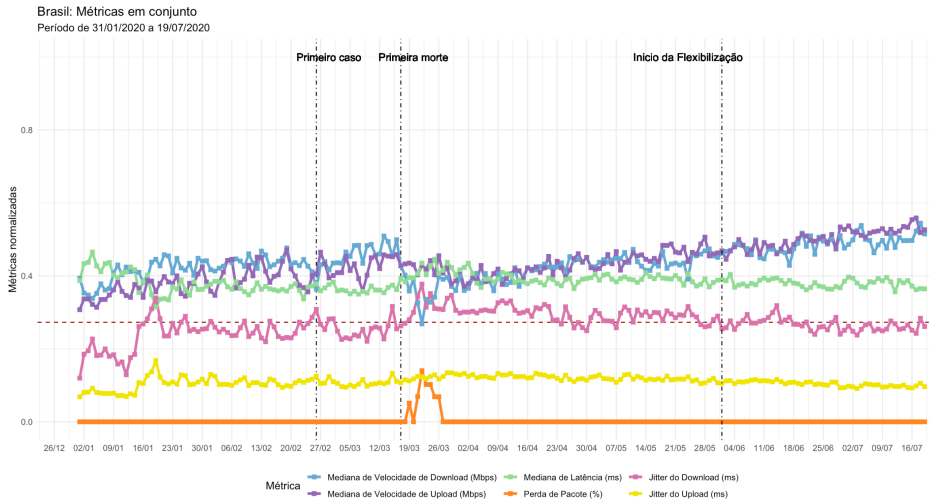


Figura 17: Impactos na qualidade da internet no Brasil durante a pandemia de COVID-19, análise realizada entre 31/01/2020 e 19/07/2020. Fonte: (BR, 2020).

Objetivo

- Captura de pacotes transmitidos durante uma sessão de vídeo chamada na plataforma Discord em diferentes dispositivos.
- Comparação dos resultados com o artigo do (KASSIM et al., 2017), levando em consideração:
 - Duração da vídeo chamada.
 - Banda-larga de cada usuário.
 - Resultados obtidos nas ferramentas Wireshark e TCPDump.

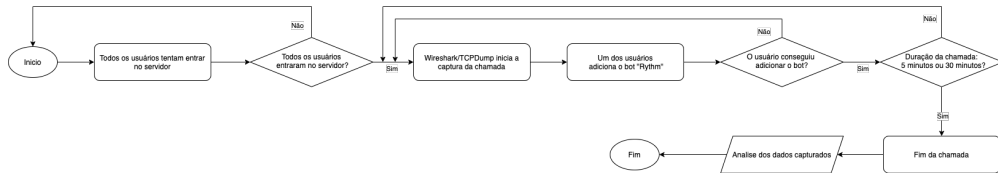


Figura 18: Fluxograma de uma captura do experimento. Próprios autores.

Configurações dos Dispositivos

	Localização	Sistema Operacional	Processador	Placa de Rede	Taxa de Download	Taxa de Upload
Dispositivo 1	Joinville, SC - Brasil	Linux Mint 20	Intel i3 9100F 3.6 GHz	Realtek RTL8111/8168/8411	14 Mbps	1.3 Mbps
Dispositivo 2	Assunção, Paraguai	MacOS Catalina 10.15.5	Intel i7 7700HQ 2.8 GHz	AirPort Extreme (0x14E4, 0x173)	10 Mbps	34 Mbps
Dispositivo 3	Florianópolis, SC - Brasil	Windows 10 Home 1909	Intel i7 7700HQ 2.8 GHz	Intel(R) Dual Band Wireless-AC 8265.	135 Mbps	15.63 Mbps

Tabela 4: Tabela com as especificações dos dispositivos utilizados pelos autores. Fonte: Próprios Autores.

- *Bytes in flight*

		Bytes in Flight (% do total da captura e número de pacotes)		
Duração em minutos	Versão da Captura	Dispositivo 1	Dispositivo 2	Dispositivo 3
5	Captura 1	0.2 % - 257	0.7% -773	0.3 % - 486
	Captura 2	0.2% - 190	0.5% - 614	0.2 % - 306
30	Captura 1	0.3% - 1547	0.5% - 3300	0.4% - 3029

Tabela 5: Bytes in Flight. Fonte: Próprios Autores.

- Retransmissão

		Retransmissão (% do total da captura e número de pacotes)		
Duração em minutos	Versão da Captura	Dispositivo 1	Dispositivo 2	Dispositivo 3
5	Captura 1	0 % - 9	0% -31	0% - 14
	Captura 2	0% - 6	0% - 15	0% - 5
30	Captura 1	0% - 59	0% - 172	0% - 5

Tabela 6: Retransmissão. Fonte: Próprios Autores.

- Perda de pacotes

Duração em minutos	Versão da Captura	Perda de pacotes (% do total da captura e número de pacotes)		
		Dispositivo 1	Dispositivo 2	Dispositivo 3
5	Captura 1	0% - 12	0% - 14	0% - 0
	Captura 2	0% - 3	0% - 1	0% - 1
30	Captura 1	0% - 16	0% - 11	0% - 7

Tabela 7: Perda de Pacotes. Fonte: Próprios Autores.

- Tamanho dos pacotes

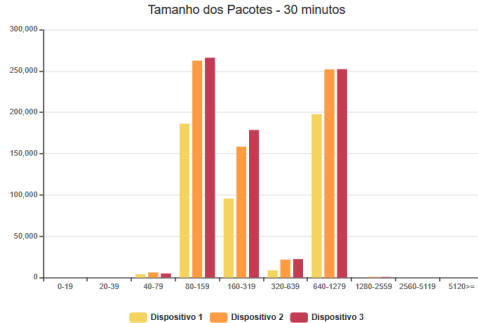


Figura 19: Gráfico de Barras para o tamanho dos pacotes em 30 minutos.
Fonte: Próprios Autores

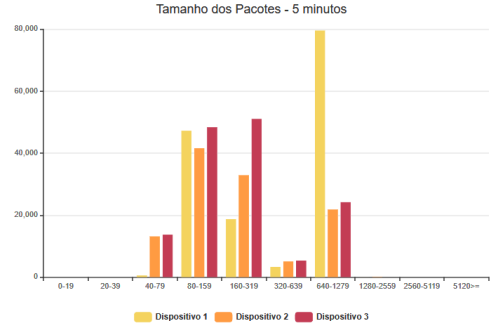


Figura 20: Gráfico de Barras para o tamanho dos pacotes em 5 minutos
Fonte: Próprios Autores.

- Latência *Round-trip time*

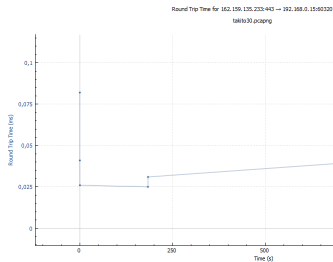


Figura 21: Gráficos RTT - Dispositivo 1. Fonte: Próprios autores.

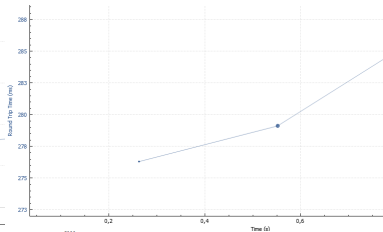


Figura 22: Gráficos RTT - Dispositivo 2. Fonte: Próprios autores.

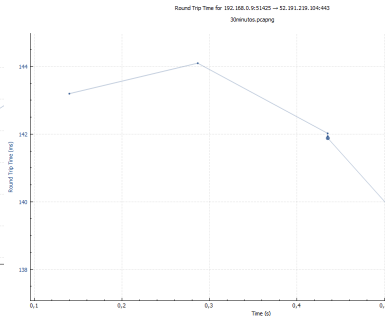


Figura 23: Gráficos RTT - Dispositivo 3. Fonte: Próprios autores.

- Gráficos I/O

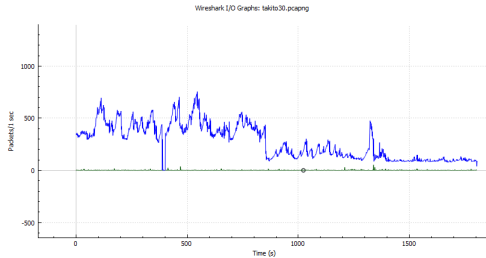


Figura 24: Gráfico I/O - Dispositivo 1 para capturas de 30 minutos. Fonte: Próprios Autores.

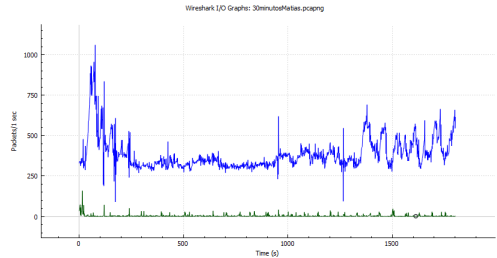


Figura 25: Gráfico I/O - Dispositivo 2 para capturas de 30 minutos. Fonte: Próprios Autores.

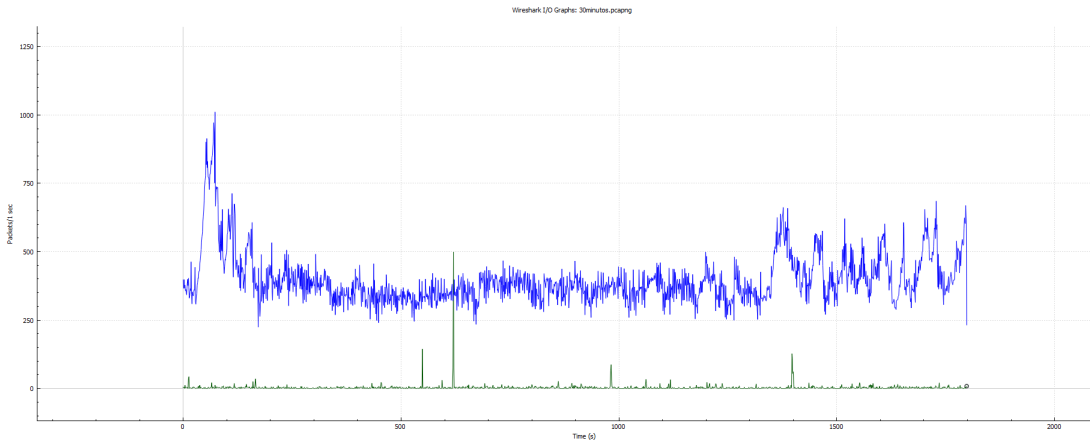


Figura 26: Gráfico I/O - Dispositivo 3 para capturas de 30 minutos. Fonte: Próprios Autores.

- Gráficos I/O

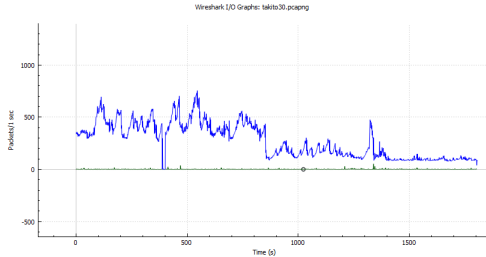


Figura 27: Gráfico I/O - Dispositivo 1 para capturas de 30 minutos. Fonte: Próprios Autores.

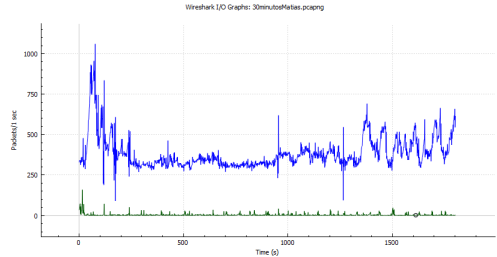


Figura 28: Gráfico I/O - Dispositivo 2 para capturas de 30 minutos. Fonte: Próprios Autores.

- *Throughput*

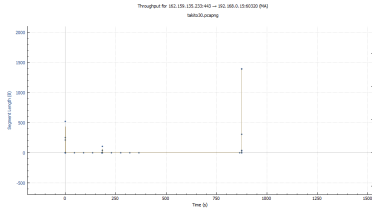


Figura 29: Gráficos
Throughput - Dispositivo 1.

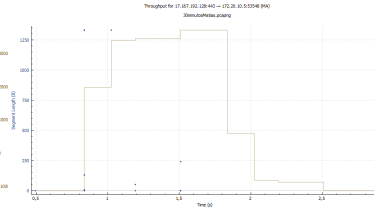


Figura 30: Gráficos
Throughput - Dispositivo 2.

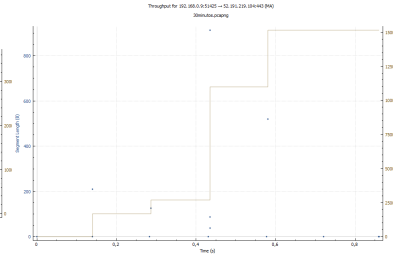


Figura 31: Gráficos
Throughput - Dispositivo 3.

Duração em minutos	Largura de Banda (% do total da captura e número de pacotes)		
	Dispositivo 1	Dispositivo 2	Dispositivo 3
30	268978981	343480813	350480017

Tabela 8: Largura de Banda. Fonte: Próprios autores.

Conclusões

- Achemos uma diferença notável entre as capturas do Wireshark e TCPDump.
- A rede 4G teve mais dificuldade em relação à transmissão de pacotes.
- Diferença do dispositivo 1 ao resto em questão de Bytes in flight.
- Perda de pacotes do Discord ≈ 0 .

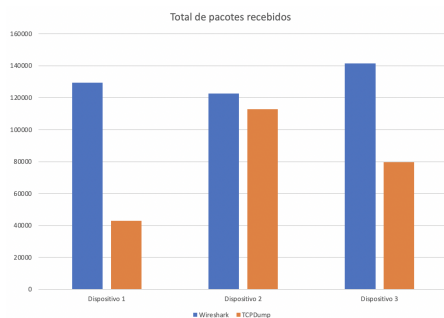


Figura 32: Comparação Wireshark vs TCPDump em 5 minutos. Próprios autores.

Seções

Introdução

Ferramentas

Discord

Skype

Wireshark

TCPDump

Casos de Estudo

Trabalho Referenciado

Objetivo

Coleta de Dados

Análise

Análise

Conclusões

Caso de estudo

Objetivo

Coleta de Dados

Análise

Conclusões

Considerações Finais

- Eficiência do *Discord* quando comparado ao *Skype*.
- Diferença entre as ferramentas de captura.
- Desempenho da aplicação.


Considerações Finais

Comparação Skype x Discord					
Plataforma	Tabela	Duração em minutos	Dispositivo 1	Dispositivo 2	Dispositivo 3
Discord	Largura de Banda (Bytes)	30	268978981	343480813	350480017
Skype			201000000		
Discord	RTT(ms)	30	158	300	5
Skype			7		
Discord	Perda de pacotes(Total)	30	16	11	7
Skype			0		

Tabela 9: Comparação Skype x Discord. Fonte: Próprios autores.


 In: . [S.l.]: Disponível em:

<<https://www.deviantart.com/dykletiu/journal/Official-Chat-Servers-Discord-And-Skype-621842802>>. Acesso em: 30 set. 2020.


 In: . [S.l.]: Disponível em: <<https://discord.com>>. Acesso em: 30 set. 2020.


 In: . [S.l.]: Disponível em: <<https://www.skype.com/pt-br/>>. Acesso em: 30 set. 2020.


 ASRODIA, P.; PATEL, H. **Network Traffic Analysis Using Packet Sniffer.**


 ASRODIA, P.; PATEL, H. Analysis of various packet sniffing tools for network monitoring and analysis. **International Journal of Electrical, Electronics and Computer Engineering**, Citeseer, v. 1, n. 1, p. 55–58, 2012.


 BEST 10 Packet Sniffer and Capture Tools in 2020. In: . [S.l.]: Disponível em: <<https://www.dnsstuff.com/packet-sniffers>>. Acesso em: 30 set. 2020.


 BR, N. de Informação e Coordenação do P. **COVID-19 IMPACTOS NA QUALIDADE DA INTERNET NO BRASIL**. 2020. Disponível em: <<https://www.ceptro.br/assets/publicacoes/pdf/2020.07.13-relatorio-semanal.pdf>>.


 CALLSTATS. **What is Round-trip Time and How Does it Relate to Network Latency?** 2018. Disponível em: <<https://www.callstats.io/blog/what-is-round-trip-time-and-how-does-it-relate-to-network-latency>>.


 Chandran, P.; Lingam, C. Performance evaluation of voice transmission in wi-fi networks using r-factor. In: **2015 International Conference on Information Processing (ICIP)**. [S.l.: s.n.], 2015. p. 481–484.


 CHAPPELL, L. **Wireshark Network Analysis (Second Edition): The Official Wireshark Certified Network Analyst Study Guide**. Chapell University, 2012. (Wireshark Solutions). ISBN 9781893939943. Disponível em: <https://books.google.com.br/books/about/Wireshark_Network_Analysis.html?id=x4iaLgEACAAJ&redir_esc=y>.


 CHAPPELL, L.; COMBS, G. **Wireshark 101: Essential Skills for Network Analysis**. Protocol Analysis Institute, Chapell University, 2013. (Wireshark Solutions). ISBN 9781893939721. Disponível em: <<https://books.google.com.br/books?id=FQEZmAEACAAJ>>.


 FAVALE, T. et al. Campus traffic and e-learning during covid-19 pandemic. **Computer Networks**, v. 176, p. 107290, 2020. ISSN 1389-1286. Disponível em: <<http://www.sciencedirect.com/science/article/pii/S1389128620306046>>.

 GITE, V. **TCPDump: Capture and Record Specific Protocols / Port**. 2008. Disponível em: <<https://www.cyberciti.biz/faq/tcpdump-capture-record-protocols-port/>>.


 GOMES, P. C. T. **ENTENDA O QUE É O PROTOCOLO SNMP E SUA IMPORTÂNCIA NO MONITORAMENTO**. 2017. Disponível em: <<https://www.opservices.com.br/snmp/>>.


 GRAHAM-CUMMING, J. **Internet performance during the COVID-19 emergency**. 2020. Disponível em: <<https://blog.cloudflare.com/recent-trends-in-internet-traffic/>>.


 KASSIM, M. et al. Skype multimedia application traffic analysis on home unifi network. In: . [S.l.: s.n.], 2017. p. 184–189.


 Korhonen, J.; Wang, Y. Effect of packet size on loss rate and delay in wireless links. In: **IEEE Wireless Communications and Networking Conference, 2005**. [S.l.: s.n.], 2005. v. 3, p. 1608–1613 Vol. 3.


 LYON, G. **Top 125 Network Security Tools**. 2019. Disponível em: <<https://sectools.org/>>.


 MALLET, Q. **What is the difference between Tcpdump and Wireshark?** 2017. Disponível em: <<https://www.quora.com/What-is-the-difference-between-Tcpdump-and-Wireshark>>.







 NELLY. **Discord Transparency Report: Jan — June 2020**. 2020. Disponível em: <<https://blog.discord.com/discord-transparency-report-jan-june-2020-2ef4a3ee346d/>>.

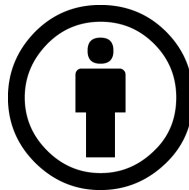
 NICOLETTI, M.; BERNASCHI, M. Forensic analysis of microsoft skype for business. **Digital Investigation**, Elsevier, v. 29, p. 159–179, 2019.

 OLUDELE, A. et al. Packet sniffer – a comparative characteristic evaluation study. In: . [S.l.: s.n.], 2015. p. 091–100.

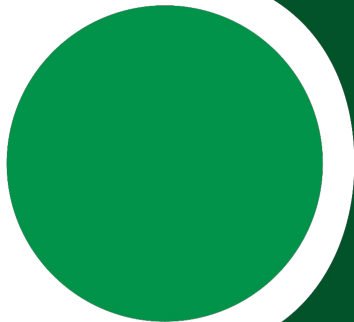
 SANDERS, C. **Analise de pacotes na prática: Usando Wireshark para solucionar problemas de rede do mundo real**. Novatec Editora, 2017. ISBN 9788575225851. Disponível em: <https://books.google.com.br/books?id=N_ooDwAAQBAJ>.

 SHARPE, R.; WARNICKE, E.; LAMPING, U. **Wireshark User's Guide: Version 3.3.0**. [S.l.: s.n.], 2011.

-  SURI, S.; BATRA, V. Comparative study of network monitoring tools. **International Journal of Innovative Technology and Exploring Engineering (IJITEE)**, Citeseer, v. 1, n. 3, p. 63–65, 2010.
-  TCPDUMP and Libpcap. 2020. Disponível em: <<https://www.tcpdump.org>>.
-  WARRAG, T. **Why is Wireshark useful?** 2016. Disponível em: <<https://www.quora.com/Why-is-Wireshark-useful>>.
-  WIRESHARK. 2020. Disponível em: <<https://1.as.dl.wireshark.org/docs/user-guide.pdf>>.
-  WIRESHARK. **Awards and Accolades.** 2020. Disponível em: <<https://www.wireshark.org/about.html#authors>>.
-  WIRESHARK FAQ. Disponível em: <<https://ask.wireshark.org/questions/>>.



Attribution 4.0 International (CC BY 4.0)



Duvidas:

Fernanda Maria de Souza

Nikolas Jensen

Matias Giuliano Gutierrez Benitez

Vinicius Takeo Friedrich Kuwaki

vtkwki@gmail.com

github.com/takeofriedrich