

Анализ качества передачи данных в облачном сервисе OneDrive с использованием Wireshark

Ёлгин Роман Николаевич

Приамурский государственный университет имени Шолом-Алейхема

Студент

Аннотация

В статье рассматривается процесс анализа качества передачи данных при взаимодействии с облачным сервисом OneDrive от компании Microsoft. С помощью sniffерной программы Wireshark был произведен перехват сетевого трафика во время загрузки и скачивания файлов. На основе полученных данных проведена оценка характеристик канала связи в прямом и обратном направлениях, определены ключевые параметры качества передачи данных.

Ключевые слова: OneDrive, Wireshark, перехват трафика.

Data transmission quality analysis in OneDrive cloud service using Wireshark

Yolgin Roman Nikolaevich

Sholom-Aleichem Priamursky State University

Student

Abstract

The article discusses the process of analyzing the quality of data transmission when interacting with the OneDrive cloud service from Microsoft. The Wireshark sniffer program was used to intercept network traffic during file uploads and downloads. Based on the data obtained, the characteristics of the communication channel in the forward and reverse directions were evaluated, and key parameters of data transmission quality were determined.

Keywords: OneDrive, Wireshark, traffic interception.

1 Введение

1.1 Актуальность

Облачные сервисы, такие как OneDrive, активно используются для хранения и обмена данными, что делает важным вопрос качества их работы. Анализ сетевого трафика помогает понять, насколько эффективно происходит передача информации между клиентом и сервером, а также выявить возможные узкие места в канале связи. Исследование актуально для ИТ-специалистов, сетевых администраторов и пользователей, заинтересованных в повышении производительности облачных технологий.

1.2 Обзор исследований

И.Д. Ширяев и Л.Е. Попок в своей работе рассматривают облачное хранилище OneDrive, анализируя его роль в цифровизации экономики и ключевые функциональные возможности [1]. О.А. Абрамкина исследует методики анализа сетевого трафика с помощью Wireshark, уделяя особое внимание TCP-сеансам и извлечению передаваемых данных [2]. А.П. Киреев, Д.В. Колмыков и др. изучают применение Wireshark для мониторинга корпоративных сетей, демонстрируя его эффективность в выявлении аномалий трафика [3]. Е.В. Мешкова рассматривает практические аспекты перехвата и анализа сетевых данных с использованием Wireshark, подчеркивая его значение в диагностике сетевых соединений [4]. Ж.М. Кубалиев и В.А.Ружников исследуют возможности Wireshark в перехвате пакетов специализированных протоколов, таких как X11, что подтверждает универсальность данного инструмента [5].

1.3 Цель исследования

Цель исследования – оценить качество передачи данных при работе с облачным сервисом OneDrive, проанализировав сетевой трафик с помощью Wireshark. Определить, в каком направлении (загрузка или скачивание) канал связи обладает лучшими характеристиками.

2 Материалы и методы

Исследование проводилось с использованием сетевого анализатора Wireshark для перехвата и анализа трафика при работе с OneDrive. Методика включала тестовые передачи файлов с последующей оценкой скорости, задержек и потерь пакетов в обоих направлениях. Это позволило объективно сравнить качество канала при загрузке и скачивании данных.

3 Результаты и обсуждения

Прежде всего нужно установить и настроить необходимые программы (рис. 1).

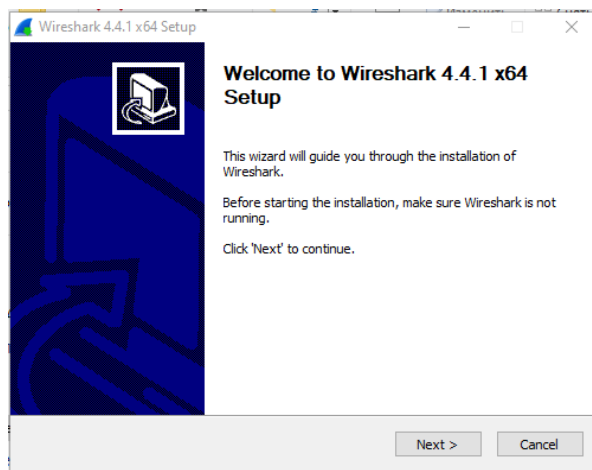


Рисунок 1. Установка WinPcap и Wireshark

Выполняем команду «ping www.onedrive.com» в cmd (рис. 2).

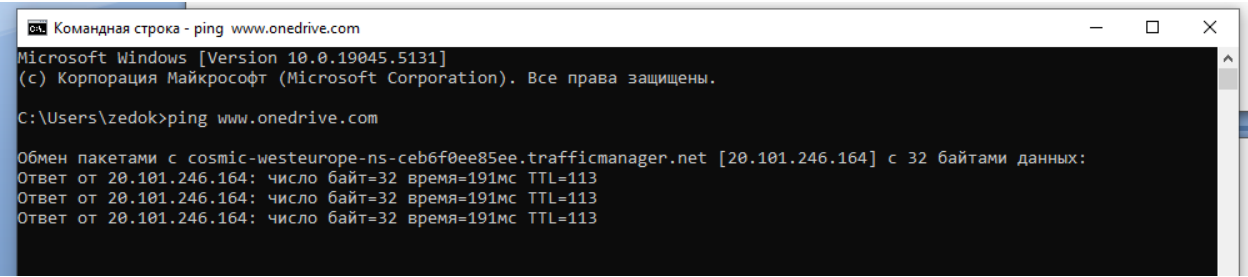


Рисунок 2. Команда ping

Проходим аутентификацию в Облачном сервисе OneDrive (рис. 3).

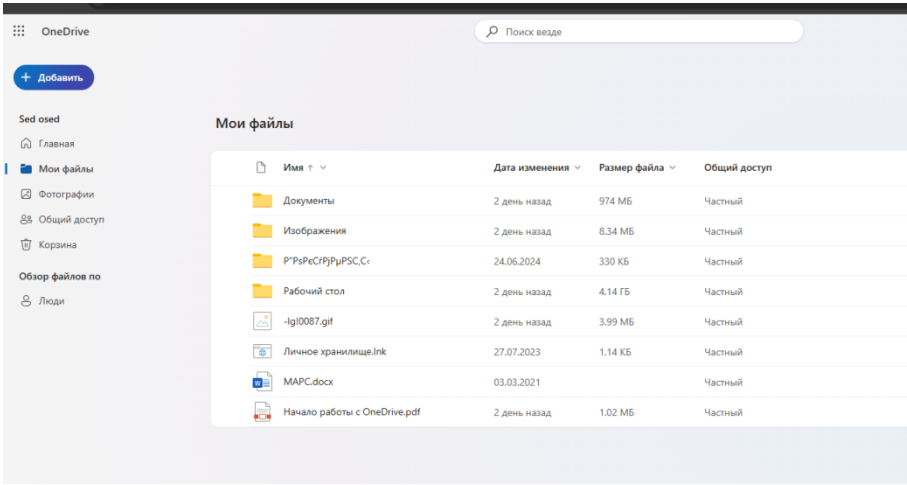


Рисунок 3. Рабочий стол OneDrive

Осуществим перехват трафика сети Internet с помощью программы Wireshark. Ниже показаны пакеты максимальной и минимальной длины пакета в реальном трафике, которые будут идти только после ClientHello и только в формате TCP (рис. 4).

No.	Time	Source	Destination	Protocol	Length	Info
21	2.692801	192.168.1.35	142.250.217.174	TCP	54	65174 → 443 [ACK] Seq=2911 Ack=598 Win=510 Len=0
22	2.693833	142.250.217.174	192.168.1.35	TLSv1.2	309	Application Data
23	2.694035	192.168.1.35	142.250.217.174	TLSv1.2	89	Application Data
24	2.694883	142.250.217.174	192.168.1.35	TLSv1.2	85	Application Data
25	2.694978	142.250.217.174	192.168.1.35	TLSv1.2	93	Application Data
26	2.695054	192.168.1.35	142.250.217.174	TCP	54	65174 → 443 [ACK] Seq=2946 Ack=923 Win=509 Len=0
27	2.695288	192.168.1.35	142.250.217.174	TLSv1.2	93	Application Data
28	2.814627	192.168.1.35	52.182.143.210	TCP	54	65131 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1020 Len=0
29	2.815192	192.168.1.35	52.182.143.210	TCP	66	65193 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
30	2.822360	93.158.134.119	192.168.1.35	TCP	60	443 → 64166 [RST, ACK] Seq=1 Ack=1 Win=166 Len=0
31	2.936370	142.250.217.174	192.168.1.35	TCP	60	443 → 65174 [ACK] Seq=923 Ack=2985 Win=1024 Len=0
32	3.023291	52.182.143.210	192.168.1.35	TCP	60	443 → 65131 [FIN, ACK] Seq=1 Ack=2 Win=16389 Len=0
33	3.023519	192.168.1.35	52.182.143.210	TCP	54	65131 → 443 [ACK] Seq=2 Ack=2 Win=1020 Len=0
34	3.023845	52.182.143.210	192.168.1.35	TCP	66	443 → 65193 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
35	3.024079	192.168.1.35	52.182.143.210	TCP	54	65193 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
36	3.024359	192.168.1.35	52.182.143.210	TLSv1.2	283	Client Hello (SNI=self.events.data.microsoft.com)
37	3.251827	52.182.143.210	192.168.1.35	TCP	1414	443 → 65193 [ACK] Seq=1 Ack=230 Win=4195328 Len=1360 [TCP PDU reassembled in 44]
38	3.251953	52.182.143.210	192.168.1.35	TCP	1414	443 → 65193 [ACK] Seq=1361 Ack=230 Win=4195328 Len=1360 [TCP PDU reassembled in 44]
39	3.252019	192.168.1.35	52.182.143.210	TCP	54	65193 → 443 [ACK] Seq=230 Ack=1361 Win=262144 Len=0
40	3.252039	52.182.143.210	192.168.1.35	TCP	1414	443 → 65193 [ACK] Seq=2721 Ack=230 Win=4195328 Len=1360 [TCP PDU reassembled in 44]
41	3.252088	192.168.1.35	52.182.143.210	TCP	54	65193 → 443 [ACK] Seq=230 Ack=2721 Win=262144 Len=0
42	3.252135	192.168.1.35	52.182.143.210	TCP	54	65193 → 443 [ACK] Seq=230 Ack=4081 Win=262144 Len=0
43	3.252155	52.182.143.210	192.168.1.35	TCP	1414	443 → 65193 [ACK] Seq=4081 Ack=230 Win=4195328 Len=1360 [TCP PDU reassembled in 44]
44	3.252228	52.182.143.210	192.168.1.35	TLSv1.2	922	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
45	3.252274	192.168.1.35	52.182.143.210	TCP	54	65193 → 443 [ACK] Seq=230 Ack=5441 Win=262144 Len=0

Рисунок 4. Перехват трафика в Wireshark

На начальном этапе исследования, при отсутствии активной передачи

данных, был зафиксирован минимальный размер сетевых кадров – порядка 90 байт. Данные кадры соответствуют служебному трафику (управляющие пакеты TCP, ARP-запросы и другие фоновые сетевые взаимодействия) (рис.5).

11	2.414278	192.168.1.35	142.250.217.174	TLSv1.2	978 Application Data
12	2.534574	162.244.34.43	192.168.1.35	TCP	66 8886 → 57953 [ACK] Seq=1 Ack=2 Win=4 Len=0 SLE=1 SRE=2
13	2.574387	149.154.167.99	192.168.1.35	TLSv1.2	167 Application Data
14	2.621317	192.168.1.35	149.154.167.99	TCP	54 64548 → 443 [ACK] Seq=333 Ack=227 Win=2060 Len=0
15	2.655574	142.250.217.174	192.168.1.35	TCP	60 443 → 65174 [ACK] Seq=1 Ack=1361 Win=1029 Len=0
16	2.655696	142.250.217.174	192.168.1.35	TCP	60 443 → 65174 [ACK] Seq=1 Ack=1948 Win=1027 Len=0
17	2.655720	142.250.217.174	192.168.1.35	TCP	60 443 → 65174 [ACK] Seq=1 Ack=1987 Win=1027 Len=0
18	2.655750	142.250.217.174	192.168.1.35	TCP	60 443 → 65174 [ACK] Seq=1 Ack=2911 Win=1024 Len=0
19	2.657120	142.250.217.174	192.168.1.35	TLSv1.2	93 Application Data
20	2.692648	142.250.217.174	192.168.1.35	TLSv1.2	612 Application Data
21	2.692881	192.168.1.35	142.250.217.174	TCP	54 65174 → 443 [ACK] Seq=2911 Ack=598 Win=510 Len=0
22	2.693833	142.250.217.174	192.168.1.35	TLSv1.2	309 Application Data
23	2.694035	192.168.1.35	142.250.217.174	TLSv1.2	89 Application Data
24	2.694883	142.250.217.174	192.168.1.35	TLSv1.2	85 Application Data
25	2.694978	142.250.217.174	192.168.1.35	TLSv1.2	93 Application Data
26	2.695054	192.168.1.35	142.250.217.174	TCP	54 65174 → 443 [ACK] Seq=2946 Ack=923 Win=509 Len=0
27	2.695288	192.168.1.35	142.250.217.174	TLSv1.2	93 Application Data
28	2.814627	192.168.1.35	52.182.143.210	TCP	54 65131 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1020 Len=0
29	2.815192	192.168.1.35	52.182.143.210	TCP	66 65193 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
30	2.822360	93.158.134.119	192.168.1.35	TCP	60 443 → 64166 [RST, ACK] Seq=1 Ack=1 Win=166 Len=0
31	2.936370	142.250.217.174	192.168.1.35	TCP	60 443 → 65174 [ACK] Seq=923 Ack=2985 Win=1024 Len=0
32	3.023291	52.182.143.210	192.168.1.35	TCP	60 443 → 65131 [FIN, ACK] Seq=1 Ack=2 Win=16389 Len=0
33	3.023519	192.168.1.35	52.182.143.210	TCP	54 65131 → 443 [ACK] Seq=2 Ack=2 Win=1020 Len=0
34	3.023845	52.182.143.210	192.168.1.35	TCP	66 443 → 65193 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
35	3.024079	192.168.1.35	52.182.143.210	TCP	54 65193 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0

Рисунок 5. Анализ сетевого трафика до передачи файла

В процессе загрузки/скачивания файла в облачное хранилище OneDrive наблюдалось увеличение длины кадров до максимального значения (1414 байт), что соответствует предельно допустимому размеру Ethernet-фрейма (MTU 1500 байт с учетом заголовков). Это свидетельствует об активной передаче полезных данных с максимальной эффективностью использования канала связи (рис.6).

51	3.465018	192.168.1.35	52.182.143.210	TCP	1414 65193 → 443 [ACK] Seq=1247 Ack=6360 Win=261120 Len=1360 [TCP PDU reassembled in 66]
52	3.465081	192.168.1.35	52.182.143.210	TCP	1414 65193 → 443 [ACK] Seq=2607 Ack=6360 Win=261120 Len=1360 [TCP PDU reassembled in 66]
53	3.465142	192.168.1.35	52.182.143.210	TCP	1414 65193 → 443 [ACK] Seq=3967 Ack=6360 Win=261120 Len=1360 [TCP PDU reassembled in 66]
54	3.465207	192.168.1.35	52.182.143.210	TCP	1414 65193 → 443 [ACK] Seq=5327 Ack=6360 Win=261120 Len=1360 [TCP PDU reassembled in 66]
55	3.465272	192.168.1.35	52.182.143.210	TCP	1414 65193 → 443 [ACK] Seq=6687 Ack=6360 Win=261120 Len=1360 [TCP PDU reassembled in 66]
56	3.465339	192.168.1.35	52.182.143.210	TCP	1414 65193 → 443 [ACK] Seq=8047 Ack=6360 Win=261120 Len=1360 [TCP PDU reassembled in 66]
57	3.465409	192.168.1.35	52.182.143.210	TCP	1414 65193 → 443 [ACK] Seq=9407 Ack=6360 Win=261120 Len=1360 [TCP PDU reassembled in 66]
58	3.465475	192.168.1.35	52.182.143.210	TCP	1414 65193 → 443 [ACK] Seq=10767 Ack=6360 Win=261120 Len=1360 [TCP PDU reassembled in 66]
59	3.465538	192.168.1.35	52.182.143.210	TCP	1414 65193 → 443 [ACK] Seq=12127 Ack=6360 Win=261120 Len=1360 [TCP PDU reassembled in 66]
60	3.673247	52.182.143.210	192.168.1.35	TCP	60 443 → 65193 [ACK] Seq=6360 Ack=2607 Win=4195584 Len=0
61	3.673398	52.182.143.210	192.168.1.35	TCP	60 443 → 65193 [ACK] Seq=6360 Ack=5327 Win=4195584 Len=0
62	3.673464	192.168.1.35	52.182.143.210	TCP	1414 65193 → 443 [ACK] Seq=13487 Ack=6360 Win=261120 Len=1360 [TCP PDU reassembled in 66]
63	3.673565	192.168.1.35	52.182.143.210	TCP	1414 65193 → 443 [ACK] Seq=14847 Ack=6360 Win=261120 Len=1360 [TCP PDU reassembled in 66]
64	3.673631	52.182.143.210	192.168.1.35	TCP	60 443 → 65193 [ACK] Seq=6360 Ack=8047 Win=4195584 Len=0
65	3.673635	192.168.1.35	52.182.143.210	TCP	1414 65193 → 443 [ACK] Seq=16207 Ack=6360 Win=261120 Len=1360 [TCP PDU reassembled in 66]
66	3.673704	192.168.1.35	52.182.143.210	TLSv1.2	1300 Application Data
67	3.673776	192.168.1.35	52.182.143.210	TCP	1414 65193 → 443 [ACK] Seq=18813 Ack=6360 Win=261120 Len=1360 [TCP PDU reassembled in 75]
68	3.673832	192.168.1.35	52.182.143.210	TCP	1414 65193 → 443 [ACK] Seq=20173 Ack=6360 Win=261120 Len=1360 [TCP PDU reassembled in 75]
69	3.673930	192.168.1.35	52.182.143.210	TCP	1414 65193 → 443 [ACK] Seq=21533 Ack=6360 Win=261120 Len=1360 [TCP PDU reassembled in 75]
70	3.673980	192.168.1.35	52.182.143.210	TCP	1414 65193 → 443 [ACK] Seq=22893 Ack=6360 Win=261120 Len=1360 [TCP PDU reassembled in 75]
71	3.673977	192.168.1.35	52.182.143.210	TCP	1414 65193 → 443 [ACK] Seq=24253 Ack=6360 Win=261120 Len=1360 [TCP PDU reassembled in 75]
72	3.674025	192.168.1.35	52.182.143.210	TCP	1414 65193 → 443 [ACK] Seq=25613 Ack=6360 Win=261120 Len=1360 [TCP PDU reassembled in 75]
73	3.674058	52.182.143.210	192.168.1.35	TCP	60 443 → 65193 [ACK] Seq=6360 Ack=10767 Win=4195584 Len=0
74	3.674095	52.182.143.210	192.168.1.35	TCP	60 443 → 65193 [ACK] Seq=6360 Ack=13487 Win=4195584 Len=0
75	3.674117	192.168.1.35	52.182.143.210	TLSv1.2	112 Application Data

Рисунок 6. Мониторинг трафика во время передачи файла

По окончании загрузки/скачивания файла размер кадров возвращался к исходным значениям (в диапазоне 54-253 байт), что соответствует служебным пакетам (подтверждениям передачи, управляющим сообщениям TCP и другим завершающим сетевым взаимодействиям) (рис.7).

No.	Time	Source	Destination	Protocol	Length	Info
171	10.650598	185.162.130.8	192.168.1.35	TCP	60	8886 → 57950 [PSH, ACK] Seq=1 Ack=1 Win=4 Len=3
172	10.650753	192.168.1.35	185.162.130.8	TCP	57	57950 → 8886 [PSH, ACK] Seq=1 Ack=4 Win=510 Len=3
173	10.658800	192.168.1.35	149.154.167.99	TCP	54	64548 → 443 [ACK] Seq=1379 Ack=1194 Win=2056 Len=0
174	10.793671	185.162.130.8	192.168.1.35	TCP	60	8886 → 57950 [ACK] Seq=4 Ack=4 Win=4 Len=0
175	11.489793	162.244.34.4	192.168.1.35	TCP	60	8886 → 57960 [PSH, ACK] Seq=1 Ack=1 Win=8 Len=3
176	11.489952	192.168.1.35	162.244.34.4	TCP	57	57960 → 8886 [PSH, ACK] Seq=1 Ack=4 Win=510 Len=3
177	11.759057	162.244.34.4	192.168.1.35	TCP	60	8886 → 57960 [ACK] Seq=4 Ack=4 Win=8 Len=0
178	11.792164	192.168.1.35	185.223.94.42	TCP	55	63748 → 8886 [ACK] Seq=1 Ack=1 Win=511 Len=1
179	11.908229	185.223.94.42	192.168.1.35	TCP	60	8886 → 63748 [ACK] Seq=0 Ack=2 Win=8 Len=0
180	11.908268	192.168.1.35	185.223.94.42	TCP	54	[TCP Dup ACK 178#1] [TCP ACKED unseen segment] 63748 → 8886 [ACK] Seq=
181	11.934242	185.223.94.42	192.168.1.35	TCP	66	[TCP Previous segment not captured] 8886 → 63748 [ACK] Seq=1 Ack=2 Win=
182	11.970684	185.162.130.26	192.168.1.35	TCP	60	8886 → 57966 [PSH, ACK] Seq=1 Ack=1 Win=8 Len=3
183	11.970961	192.168.1.35	185.162.130.26	TCP	57	57966 → 8886 [PSH, ACK] Seq=1 Ack=4 Win=511 Len=3
184	12.121766	185.162.130.26	192.168.1.35	TCP	60	8886 → 57966 [ACK] Seq=4 Ack=4 Win=8 Len=0
185	12.443176	192.168.1.35	149.154.167.99	TLSv1.2	253	Application Data
186	12.621048	149.154.167.99	192.168.1.35	TLSv1.2	167	Application Data
187	12.625299	162.244.34.42	192.168.1.35	TCP	60	8886 → 57959 [PSH, ACK] Seq=1 Ack=1 Win=4 Len=3
188	12.625496	192.168.1.35	162.244.34.42	TCP	57	57959 → 8886 [PSH, ACK] Seq=1 Ack=4 Win=511 Len=3
189	12.674598	192.168.1.35	149.154.167.99	TCP	54	64548 → 443 [ACK] Seq=1578 Ack=1307 Win=2056 Len=0
190	12.807988	192.168.1.35	142.250.217.174	TCP	55	65175 → 443 [ACK] Seq=1 Ack=1 Win=515 Len=1
191	12.896890	162.244.34.42	192.168.1.35	TCP	60	8886 → 57959 [ACK] Seq=4 Ack=4 Win=4 Len=0
192	13.189374	185.162.128.91	192.168.1.35	TCP	60	8886 → 57961 [PSH, ACK] Seq=1 Ack=1 Win=8 Len=3
193	13.189539	192.168.1.35	185.162.128.91	TCP	57	57961 → 8886 [PSH, ACK] Seq=1 Ack=4 Win=511 Len=3
194	13.241319	192.168.1.35	142.250.217.174	TCP	54	65175 → 443 [RST, ACK] Seq=1362 Ack=1 Win=0 Len=0
195	13.339576	185.162.128.91	192.168.1.35	TCP	60	8886 → 57961 [ACK] Seq=4 Ack=4 Win=8 Len=0

Рисунок 7. Оценка трафика после завершения передачи

Полученные данные импортируем в Excel для дальнейшего анализа (рис.8).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.35	87.250.251.119	TCP	55	64172 > 443 [ACK] Seq=1 Ack=1 Win=508 Len=1
2	0.109642	87.250.251.119	192.168.1.35	TCP	66	443 > 64172 [ACK] Seq=1 Ack=2 Win=166 Len=0 SLE=1 SRE=2
3	0.407516	192.168.1.35	149.154.167.99	TLSv1.2	187	Application Data
4	0.565388	149.154.167.99	192.168.1.35	TLSv1.2	167	Application Data
5	0.609408	192.168.1.35	149.154.167.99	TCP	54	64548 > 443 [ACK] Seq=134 Ack=114 Win=2060 Len=0
7	2.263810	192.168.1.35	162.244.34.43	TCP	55	57953 > 8886 [ACK] Seq=1 Ack=1 Win=511 Len=1
8	2.409616	192.168.1.35	149.154.167.99	TLSv1.2	253	Application Data
9	2.414113	192.168.1.35	142.250.217.174	TCP	1414	65174 > 443 [ACK] Seq=1 Ack=1 Win=513 Len=1360 [TCP PDU reassembled in 9]
10	2.414183	192.168.1.35	142.250.217.174	TLSv1.2	641	Application Data
11	2.414231	192.168.1.35	142.250.217.174	TLSv1.2	93	Application Data
12	2.414278	192.168.1.35	142.250.217.174	TLSv1.2	978	Application Data
13	2.534574	162.244.34.43	192.168.1.35	TCP	66	8886 > 57953 [ACK] Seq=1 Ack=2 Win=4 Len=0 SLE=1 SRE=2
14	2.574387	149.154.167.99	192.168.1.35	TLSv1.2	167	Application Data
15	2.621317	192.168.1.35	149.154.167.99	TCP	54	64548 > 443 [ACK] Seq=333 Ack=227 Win=2060 Len=0
16	2.655574	142.250.217.174	192.168.1.35	TCP	60	443 > 65174 [ACK] Seq=1 Ack=1361 Win=1029 Len=0
17	2.655696	142.250.217.174	192.168.1.35	TCP	60	443 > 65174 [ACK] Seq=1 Ack=1948 Win=1027 Len=0
18	2.655720	142.250.217.174	192.168.1.35	TCP	60	443 > 65174 [ACK] Seq=1 Ack=1987 Win=1027 Len=0
19	2.655750	142.250.217.174	192.168.1.35	TCP	60	443 > 65174 [ACK] Seq=1 Ack=2911 Win=1024 Len=0
20	2.657120	142.250.217.174	192.168.1.35	TLSv1.2	93	Application Data
21	2.692648	142.250.217.174	192.168.1.35	TLSv1.2	612	Application Data
22	2.692801	192.168.1.35	142.250.217.174	TCP	54	65174 > 443 [ACK] Seq=2911 Ack=598 Win=510 Len=0
23	2.693833	142.250.217.174	192.168.1.35	TLSv1.2	309	Application Data
24	2.694035	192.168.1.35	142.250.217.174	TLSv1.2	89	Application Data
25	2.694883	142.250.217.174	192.168.1.35	TLSv1.2	85	Application Data
26	2.694978	142.250.217.174	192.168.1.35	TLSv1.2	93	Application Data
27	2.695054	192.168.1.35	142.250.217.174	TCP	54	65174 > 443 [ACK] Seq=2946 Ack=923 Win=509 Len=0
28	2.695288	192.168.1.35	142.250.217.174	TLSv1.2	93	Application Data
29	2.814627	192.168.1.35	52.182.143.210	TCP	54	65131 > 443 [FIN, ACK] Seq=1 Ack=1 Win=1020 Len=0
30	2.815192	192.168.1.35	52.182.143.210	TCP	66	65193 > 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
31	3.022260	93.158.134.119	192.168.1.35	TCP	60	443 > 64166 [RST, ACK] Seq=1 Ack=1 Win=166 Len=0
32	2.936370	142.250.217.174	192.168.1.35	TCP	60	443 > 65174 [ACK] Seq=923 Ack=2985 Win=1024 Len=0
33	3.023291	52.182.143.210	192.168.1.35	TCP	60	443 > 65131 [FIN, ACK] Seq=1 Ack=2 Win=16389 Len=0
34	3.023519	192.168.1.35	52.182.143.210	TCP	54	65131 > 443 [ACK] Seq=2 Ack=2 Win=1020 Len=0
35	3.023845	52.182.143.210	192.168.1.35	TCP	66	443 > 65193 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
36	3.024079	192.168.1.35	52.182.143.210	TCP	54	65193 > 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
37	3.024359	192.168.1.35	52.182.143.210	TLSv1.2	283	Client Hello (SN=self.events.data.microsoft.com)
38	3.251827	52.182.143.210	192.168.1.35	TCP	1414	443 > 65193 [ACK] Seq=1 Ack=230 Win=4195328 Len=1360 [TCP PDU reassembled in 44]
39	3.251953	52.182.143.210	192.168.1.35	TCP	1414	443 > 65193 [ACK] Seq=1361 Ack=230 Win=4195328 Len=1360 [TCP PDU reassembled in 44]

Рисунок 8. Таблица в Excel

Вычислим задержку передачи в excel, для этого воспользуемся распределением информации по колонкам (рис. 9).

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	No.	Time	Source	Destination	Protocol	Length	Info							
2	1	0.000000	192.168.1.87	250.251	TCP	55	64172 > 443 [ACK] Seq=1 Ack=1 Win=508 Len=1							
3	2	0.109642	87.250.251	192.168.1.	TCP	66	443 > 64172 [ACK] Seq=1 Ack=2 Win=166 Len=0 SLE=1 SRE=2							
4	3	0.407516	192.168.1.	149.154.16	TLSv1.2	187	Application Data							
5	4	0.565388	149.154.16	192.168.1.	TLSv1.2	167	Application Data							
6	5	0.609408	192.168.1.	149.154.16	TCP	54	64548 > 443 [ACK] Seq=134 Ack=114 Win=2060 Len=0							
7	6	2.263810	192.168.1.	162.244.34	TCP	55	57953 > 8886 [ACK] Seq=1 Ack=1 Win=511 Len=1							
8	7	2.409616	192.168.1.	149.154.16	TLSv1.2	253	Application Data							
9	8	2.414113	192.168.1.	142.250.21	TCP	1414	65174 > 443 [ACK] Seq=1 Ack=1 Win=513 Len=1360 [TCP PDU reassembled in 9]							
10	9	2.414183	192.168.1.	142.250.21	TLSv1.2	641	Application Data							
11	10	2.414231	192.168.1.	142.250.21	TLSv1.2	93	Application Data							
12	11	2.414278	192.168.1.	142.250.21	TLSv1.2	978	Application Data							
13	12	2.534574	162.244.34	192.168.1.	TCP	66	8886 > 57953 [ACK] Seq=1 Ack=2 Win=4 Len=0 SLE=1 SRE=2							
14	13	2.574387	149.154.16	192.168.1.	TLSv1.2	167	Application Data							
15	14	2.621317	192.168.1.	149.154.16	TCP	54	64548 > 443 [ACK] Seq=333 Ack=227 Win=2060 Len=0							
16	15	2.655574	142.250.21	192.168.1.	TCP	60	443 > 65174 [ACK] Seq=1 Ack=1361 Win=1029 Len=0							
17	16	2.655696	142.250.21	192.168.1.	TCP	60	443 > 65174 [ACK] Seq=1 Ack=1948 Win=1027 Len=0							
18	17	2.655720	142.250.21	192.168.1.	TCP	60	443 > 65174 [ACK] Seq=1 Ack=1987 Win=1027 Len=0							
19	18	2.655750	142.250.21	192.168.1.	TCP	60	443 > 65174 [ACK] Seq=1 Ack=2911 Win=1024 Len=0							
20	19	2.657120	142.250.21	192.168.1.	TLSv1.2	93	Application Data							
21	20	2.692648	142.250.21	192.168.1.	TLSv1.2	612	Application Data							
22	21	2.692801	192.168.1.	142.250.21	TCP	54	65174 > 443 [ACK] Seq=2911 Ack=598 Win=510 Len=0							
23	22	2.693833	142.250.21	192.168.1.	TLSv1.2	309	Application Data							
24	23	2.694035	192.168.1.	142.250.21	TLSv1.2	89	Application Data							
25	24	2.694883	142.250.21	192.168.1.	TLSv1.2	85	Application Data							
26	25	2.694978	142.250.21	192.168.1.	TLSv1.2	93	Application Data							
27	26	2.695054	192.168.1.	142.250.21	TCP	54	65174 > 443 [ACK] Seq=2946 Ack=923 Win=509 Len=0							
28	27	2.695288	192.168.1.	142.250.21	TLSv1.2	93	Application Data							
29	28	2.814627	192.168.1.	52.182.14	TCP	54	65131 > 443 [FIN, ACK] Seq=1 Ack=1 Win=1020 Len=0							
30	29	2.815192	192.168.1.	52.182.14	TCP	66	65193 > 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM							
31	30	2.822360	93.158.134	192.168.1.	TCP	60	443 > 64166 [RST, ACK] Seq=1 Ack=1 Win=166 Len=0							
32	31	2.936370	142.250.21	192.168.1.	TCP	60	443 > 65174 [ACK] Seq=923 Ack=2985 Win=1024 Len=0							
33	32	3.023291	52.182.14	192.168.1.	TCP	60	443 > 65131 [FIN, ACK] Seq=1 Ack=2 Win=16389 Len=0							
34	33	3.023519	192.168.1.	52.182.14	TCP	54	65131 > 443 [ACK] Seq=2 Ack=2 Win=1020 Len=0							
35	34	3.023845	52.182.14	192.168.1.	TCP	66	443 > 65193 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM							
36	35	3.024079	192.168.1.	52.182.14	TCP	54	65193 > 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0							
37	36	3.024359	192.168.1.	52.182.14	TLSv1.2	283	Client Hello (SNI=self.events.data.microsoft.com)							
38	37	3.251827	52.182.14	192.168.1.	TCP	1414	443 > 65193 [ACK] Seq=1 Ack=230 Win=4195328 Len=1360 [TCP PDU reassembled in 44]							
39	38	3.251953	52.182.14	192.168.1.	TCP	1414	443 > 65193 [ACK] Seq=1361 Ack=230 Win=4195328 Len=1360 [TCP PDU reassembled in 44]							

Рисунок 9. Распределённая таблица в Excel

Произведём вычисления, реакция сервера высчитывается по формуле:

Реакция сервера = ответ сервера – запрос = 3.024-0 = 3.024 сек.

Рассчитаем полезную пропускную способность сети для кадров максимального и минимального размера в теории и на практике.

Максимальный размер кадра Ethernet со служебной информацией составляет 1526 байт (12208 бит), минимальный – 72 байт (576 бит), межкадровый интервал – 96 бит.

Рассчитаем период следования кадров, время передачи кадра при скорости 100Мбит/с, и затем определим частоту следования кадров, проходящих по сети за 1 секунду для кадра минимальной длины.

Значит, кадр минимальной длины в 576 бит требует время прохождения в 576 bt. Учтем так же межкадровый интервал: 576+96=672 bt.

Минимальная длина пакета (теоретическая) – 72 байта Максимальная длина пакета (теоретическая) – 1526 байта Минимальная длина пакета (по реальному трафику) – 54 байта; Максимальная длина пакета (по реальному трафику) – 1414 байт.

Межкадровый интервал = 96 bt

54*8=432 bt - размер кадра минимальной длины на практике

T=528/100=5,28 мкс – время прохождения кадра минимальной длины на практике

1414*8=11 312 bt - размер кадра максимальной длины на практике

T= 11 408 /100=114,08 мкс – время прохождения кадра максимальной длины на практике

Частота следования кадра:

$F_{\text{мин. теор.}} = 1/\text{след.кадров} = 148809 \text{ кадр/с}$

$F_{\text{макс. теор.}} = 1/\text{след.кадров} = 8127 \text{ кадр/с}$

$F_{\text{мин. реал.}} = 1/\text{след.кадров} = 189393 \text{ кадр/с}$

$F_{\text{макс. реал.}} = 1/\text{след.кадров} = 8765 \text{ кадр/с}$

Ппол в Мбит/с по полученным данным для трафика сети Интернет с применением Облачного Сервиса OneDrive.

$P_{\text{пол мин.теор.}} = 8 * V_{\text{пол}} * F = 8 * 72 * 148809 = 85,71 \text{ Мбит/с}$

$P_{\text{пол макс.теор.}} = 8 * V_{\text{пол}} * F = 8 * 1526 * 8127 = 99,21 \text{ Мбит/с}$

$P_{\text{пол мин.реал.}} = 8 * V_{\text{пол}} * F = 8 * 54 * 189393 = 81,81 \text{ Мбит/с}$

$P_{\text{пол макс.реал.}} = 8 * V_{\text{пол}} * F = 8 * 1414 * 8765 = 99,14 \text{ Мбит/с}$

4 Выводы

В ходе исследования были получены данные о качестве передачи информации между клиентом и сервером OneDrive. Выявлены возможные факторы, влияющие на производительность (например, задержки, потери пакетов). Результаты могут быть использованы для оптимизации работы с облачными сервисами и улучшения пользовательского опыта. Исследование демонстрирует эффективность использования Wireshark для анализа облачных сервисов и может быть полезно для дальнейших изысканий в области сетевых технологий.

Библиографический список

1. Ширяев И.Д., Попок Л.Е. Облачное хранилище OneDrive // Цифровизация экономики: направления, методы, инструменты. Краснодар, 2023. С. 332-334.
2. Абрамкина О.А. Анализ сетевого трафика с помощью программы "Wireshark": ТСП-сеансы, извлечение информации // Научный взгляд на современное общество. - Уфа: Общество с ограниченной ответственностью "ОМЕГА САЙНС", 2015. С. 10-13.
3. Киреев А.П., Колмыков Д.В., Михайлов С.Ю., Пепеляев А.В. Анализ сетевого трафика корпоративной сети посредством программного обеспечения Wireshark // ФРАКТАЛ. 2019. №3. С. 11-15.
4. Мешкова Е.В. Перехват и анализ сетевого трафика с помощью "Wireshark" // КОНТЕНТУС. 2016. №8 (49). С. 158-162.
5. Кубалиев Ж.М., Ружников В.А. Перехват пакетов протокола X11 с использованием Wireshark // Научные труды SWORLD. 2015. №4 (41). С. 71-75.