

Universidad Cenfotec

Maestría en ciberseguridad

Documento Final Proyecto de Investigación Aplicada 2

Propuesta para determinar la viabilidad técnica del uso del protocolo QUIC UDP para las empresas en Costa Rica

Christian Araya

Agosto, 2022

DECLARACIÓN JURADA

Yo, **Araya Vargas Christian,** número de identificación: **108920187**, estudiante de la Universidad Cenfotec, de la carrera Maestría Profesional en Ciberseguridad, declaro bajo fe de juramento y consciente de las responsabilidades penales de este acto, que soy el autor intelectual del Proyecto de Investigación Aplicada 2 titulado: **"Propuesta para determinar la viabilidad técnica del uso del protocolo QUIC UDP para las empresas en Costa Rica",** por lo que libero a la Universidad Cenfotec, de cualquier responsabilidad en caso de que mi declaración sea falsa.

Firmado en San José-Costa Rica, el día 27 de agosto de 2022.



Firma estudiante

Dedicatoria

Me gustaría dedicar esta tesis a los siguientes miembros de mi familia.

A mi madre, Miriam Vargas, que desde muy temprana edad me dio el conocimiento necesario para defenderme en las áreas de ciencias y matemáticas, que me dieron la base de lo que soy el día de hoy.

A mis tres sobrinas, Kristel Duarte Araya, Julie Duarte Araya y Leilani Duarte Araya, porque he disfrutado de su compañía y han resaltado mi vida, dando ese complemento de armonía, como mis propias hijas.

A mi hermana, Hellen Araya Vargas, porque su presencia en mi vida ha sido clave para poder lograr las metas propuestas, sin su ayuda muchas cosas hubieran sido muy difíciles.

Agradecimientos

El agradecimiento principal es a mi tutor, Alonso Ramírez Jiménez, quien me apoyó para terminar esta tesis y sacó el tiempo para hacer las revisiones y correcciones necesarias y a los miembros del tribunal examinador, que me dieron el soporte para la lectura de mi documento de investigación y conseguir a las personas correctas, como Dennis Durán Céspedes, que tuvo la buena disposición y actitud para examinar mi documento de investigación. A Miguel Pérez Montero, por su coordinación en la defensa y por conseguir los recursos necesarios y el buen trato del señor Ignacio Trejos Zelaya, por su apoyo con la lectura del documento.

Universidad Cenfotec
Carrera de Postgrado
Maestría Profesional en Ciberseguridad

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría Profesional en Ciberseguridad,** requisito para optar por el título de grado de **Maestría,** para el estudiante: **Araya Vargas Christian.**

Alonso Ramírez
Digitally signed by Alonso Ramírez
Date: 2022.08.27 10:33:43 -06'00'

M. Sc. Luis A. Ramírez Jiménez
Tutor

DENNIS ALONSO DURAN CESPEDES (FIRMA)
Digitally signed by DENNIS ALONSO DURAN CESPEDES (FIRMA)
DN: SERIALNUMBER=CPF-01-1029-0075, SN=DURAN CESPEDES, G=DENNIS ALONSO, C=CR, O=PERSONA FISICA, OU=CIUDADANO, CN=DENNIS ALONSO DURAN CESPEDES (FIRMA)
Reason: I am the author of this document
Location:
Date: 2022.08.28 14:45:15-06'00'
Foxit PDF Reader Version: 12.0.0

M. Sc. Dennis Durán Céspedes
Lector 1

IGNACIO TREJOS ZELAYA (FIRMA)
Firmado digitalmente por IGNACIO TREJOS ZELAYA (FIRMA)
Fecha: 2022.08.30 21:58:58 -06'00'

M. Sc. Ignacio Trejos Zelaya
Lector 2

San José, Costa Rica, 27 de agosto de 2022

Firmada digitalmente, de conformidad con la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 8454, destacando el artículo 9°-

Tabla de contenido

Abstract 1

Capítulo 1. Introducción 8

1.1 Generalidades 8

1.2 Antecedentes del problema 9

1.3 Definición y descripción del problema 9

1.4 Justificación 10

1.5 Viabilidad 10

1.5.1 Punto de vista técnico 11

1.5.2 Punto de vista operativo 11

1.5.3 Punto de vista económico 11

1.6 Objetivos 12

1.6.1 Objetivo general 12

1.6.2 Objetivos específicos 12

1.7 Alcances y limitaciones 13

1.7.1 Alcances 13

1.7.2 Limitaciones 13

1.8 Marco de deferencia organizacional y socioeconómico 13

1.8.2 Tipo de negocio y mercado meta 15

1.8.3 Misión, visión y valores 15

1.8.4 Políticas institucionales 15

1.9 Estado de la cuestión 15

1.9.1 Fuentes de información en video 17

1.9.2 Repositorio Google Académico 18

1.9.3 Repositorio IEEE 19

1.9.4 Cadena de búsqueda scimagojr 20

1.9.5 Protocolo TCP con 1,140,101 resultados 21

1.9.6 Google Académico fuentes de información para TCP 22

1.9.7 Repositorio IETF 22

1.9.8 Repositorio IETF documentos 23

Capítulo 2. Marco conceptual 24

2.1 Comparación QUIC UDP y TCP/IP 24

2.1.2 Nube conceptual 25

2.1.3 Seguridad 26

2.1.4 Red 27

2.1.5 Multirreproducción **27**
2.1.6 Estructura **27**
2.1.7 Flujo de migración **28**
2.1.8 Baja latencia **28**
2.1.9 Concurrencia **28**
2.2.1 Protocolo QUIC **28**
2.2.2 Protocolo TCP **29**
2.2.3 Número de paquetes **29**
2.2.4 Congestión **29**
2.2.5 Comparación de la arquitectura del protocolo QUIC vs. TCP **30**
2.2.6 HTTP/1.0 ..... **30**
2.2.7 HTTP/1.1 ..... **30**
2.2.8 HTTP/2 ..... **31**
2.2.9 HTTP/3 ..... **31**
2.3 TLS/1.1 ..... **32**
2.3.1 Vector de inicialización **32**
2.3.2 Errores de relleno **32**
2.4 TLS/1.2 ..... **32**
2.4.1 Algoritmo de cifrado simétrico **33**
2.4.2 (0-RTT) **33**
2.4.3 Cifrado RSA estático y Diffie-Hellman **33**
2.4.4 Protocolos de enlace **33**
2.4.5 Funciones de derivación de clave **33**
2.4.6 Maquina de estado **34**
2.4.7 Algoritmo de curva elíptica **34**
2.4.8 Mejoras criptográficas **34**
2.5 Mecanismo de negociación **34**
2.5.1 Reanudación de la sesión **35**
2.5.2 TLS/1.3 ..... **35**
Capítulo 3. Marco metodológico 35
3.1 Tipo de investigación **35**
3.2 Alcance investigativo **36**
3.2.1 Descriptivo **36**
3.3 Enfoque **36**
3.4 Diseño **37**

3.5 Población y muestreo **38**
3.6 Instrumentos de recolección de datos **39**
3.6.1 Encuesta **42**
3.6.2 Wireshark **46**
3.7 Técnicas de análisis de información **48**
3.8 Estrategia de desarrollo de la propuesta **51**
Capítulo 4. Análisis del diagnóstico 51
4.1 Aplicación de la encuesta y aplicación con el Wireshark **51**
4.1.1 Aplicación de la encuesta **51**
4.1.2 Aplicación de la encuesta en redes sociales como WhatsApp **52**
4.1.3 Aplicación de la encuesta en redes sociales como Slack **52**
4.1.4 Uso del Wireshark **52**
4.2 Comparación de resultados **52**
4.2.1 Primer bloque de respuestas **52**
4.2.2 Segundo bloque de respuestas **55**
4.3 Comparación de resultados **58**
4.3.1 Proceso de recolección de datos **63**
4.3.2 Identificación de las fuentes de datos. **63**
4.3.3 Recopilación de contenido **67**
4.3.4 Extracción de datos **68**
4.3.4.1 Encuesta realizada con formularios de Google **68**
4.3.4.2 Resultados de las diferentes encuestas **68**
4.3.4.3 Porcentaje de la extracción de datos en la jerarquía de protocolos **70**
4.3.4.3.1 Descripción del conjunto de datos **70**
4.3.4.3.2 Descripción de variables **73**
4.3.4 Selección de variables por utilizar **81**
4.3.5 Preprocesamiento de datos y creación de variables de interés **82**
4.3.5.1 Datos y creación de variables para la encuesta **82**
4.3.5.2 Datos y creación de variables para el análisis de red **91**
Capítulo 5. Propuesta de solución 98
5.0 Introducción de la propuesta de solución **98**
5.0.1 Cómo usar el Google QUIC UDP **98**
5.0.2 Principales características técnicas **100**
5.0.3 Cómo se debe implementar **100**
5.0.4 Beneficios técnicos y económicos **101**

5.0.5 Por qué se debe implementar este protocolo QUIC UDP 101
5.0.6 Pasos para implementar el QUIC UDP 102
5.0.7 Cómo trabajan los diagramas de arquitectura 102
5.0.8 Descripción de escenarios 102
5.0.2 Introducción del escenario 1 102
5.1 Escenario 1 103
5.1.2 Situación actual 103
5.1.2.1 Usuarios finales 103
5.1.2.2 Problema de latencia 103
5.1.2.3 Desconocimiento de navegadores 103
5.1.2.4 Actualizar el centro de datos 104
5.1.3 Propuesta de solución 104
5.1.3.1 Diseño uno 104
5.1.3.1.2 Riesgos en la viabilidad del diseño uno. 104
5.1.3.2 Diseño dos 105
5.1.3.2.1 Riesgos en la viabilidad del diseño dos 106
5.1.4 Evaluación de solución 106
5.1.5 Arquitectura recomendada de solución 110
5.1.5.6 Diseño en la nube 110
5.1.6 Informe y seguimiento 111
5.1.6.1 Informe 111
5.1.6.2 Seguimiento 112
5.1.6.3 Introducción del escenario 2 112
5.2 Escenario 2 112
5.2.1 Situación actual 112
5.2.2 Propuesta de solución 113
5.2.2.2 Integración del QUIC UDP 113
5.2.3 Evaluación de la solución 115
5.2.4 Arquitectura recomendada de solución 128
5.2.4.1 Utilización de infraestructura física o virtual 128
5.2.5 Informe y seguimiento 129
5.2.5.1 Informe 129
5.2.5.2 Seguimiento 130
5.3 Esquema de evaluación 130
5.3.1 Esquema de evaluación para el escenario 1 y el escenario 2 130

Capítulo 6. Conclusiones y recomendaciones 150
6.1 Conclusiones **150**
6.1.1 Conclusiones objetivos específicos **150**
6.1.2 Conclusión objetivo n.º 1 ..... **150**
6.1.3 Conclusión objetivo n.º 2 ..... **150**
6.1.4 Conclusión objetivo n.º 3 ..... **151**
6.1.5 Conclusión objetivo n.º 4 ..... **151**
6.1.6 Conclusión objetivo n.º 5 ..... **152**
6.1.7 Conclusión objetivo n.º 6 ..... **152**
6.1.8 Conclusiones objetivo n.º 7 ..... **153**
6.1.9 Conclusión objetivo n.º 8 ..... **153**
6.1.10 Conclusión objetivo n.º 9 ..... **154**
6.1.11 Conclusión objetivo general **154**
6.2 Recomendaciones **155**
6.2.1 Recomendaciones objetivo general **155**
6.2.2 Recomendación objetivo específico **155**
Capítulo 7. Reflexiones finales 157
7.1 Reflexión final uno **157**
7.2 Reflexión final dos **158**
7.3 Reflexión final tres **158**
Capítulo 8. Trabajos para el futuro (Líneas futuras de investigación) 159
8.1 Posibles trabajos por hacer utilizando solo el QUIC UDP **159**
8.1.2 IA **159**
8.1.3 Robótica **159**
8.1.4 Redes de diferentes tecnologías **159**
8.1.5 El 5G **159**
8.1.6 El IoT, ya sea industrial o de uso doméstico **160**
8.1.7 Profundizar sobre el diseño de arquitectura del QUIC UDP **160**
8.1.7 Adaptar todos los protocolos del modelo OSI tradicional al QUIC UDP **160**
Glosario 161
Bibliografía 210
Apéndices 214

INDICE DE FIGURAS

Figura 1. Nube de palabras generado utilizando el sitio tagcrowd 25
Figura 2. Nube de palabras generado utilizando el sitio nubedepalabras 26
Figura 3. Arquitectura del Protocolo QUIC vs TCP/IP 26
Figura 4. Multiplexación del número de paquetes 29
Figura 5. Ontología del conjunto de datos 37
Figura 6. Población y muestreo para el análisis del Google QUIC y del TCP 38
Figura 7. Encuesta para reflejar el conocimiento sobre Google QUIC 41
Figura 8. Encuesta para reflejar el conocimiento sobre Google QUIC, utilizando los formularios de Google 44
Figura 9. Wireshark capturando Google Quic por medio del VirtualBox y la máquina virtual de Ubuntu 45
Figura 10. Utilizando el Ubuntu 20.04, enviamos los datos a ser requeridos por Wireshark 46
Figura 11. Comparación estadística de HTTP/2 vs HTTP3 para los diferentes sitios web y la tecnología que más se utiliza 46
Figura 12. Porcentaje de utilización de las diferentes tecnologías, el ranqueo con una muestra de 1 millón de sitios web y cómo evoluciona el Google QUIC 47
Figura 13. Tendencia histórica del uso estadístico de los diferentes protocolos que corren en los sitios web 47
Figura 14. Diagrama de flujo para la recolección de datos en la encuesta 48
Figura 15. Diagrama de flujo para la recolección de datos con pruebas de penetración Wireshark 50
Figura 16. Recolección de datos de las diferentes redes sociales conocidas, Slack, WhatsApp, Facebook 54
Figura 17. Recolección de datos de las diferentes redes sociales conocidas, Slack, WhatsApp, Facebook, Discord, Telegram 57
Figura 18. Captura correcta del protocolo HTTP que se ejecuta en Opera y Google Chrome 59
Figura 19. Alto tráfico de TCP entre cliente y servidor y protocolo TLS en dos versiones diferentes la versión 1.2 y la versión 1.3 59
Figura 20. Alto contenido o tráfico de UDP que es la base en donde QUIC procesa la información de contenido web 60
Figura 21. Comprobación de que el Google QUIC está corriendo correctamente en Opera y Chrome 61
Figura 22. Proceso de recolección de datos para crear el conjunto de datos de prueba 62
Figura 23. Primer análisis estadístico sobre la confianza de los datos que se obtienen y de sus diferentes fuentes de información 63

Figura 24. Segundo análisis estadístico sobre la confianza de los datos que se obtienen y de sus diferentes fuentes de información 64

Figura 25. Identificación de las fuentes de datos extraídas del Google Chrome y de Opera... 65

Figura 26. Captura de datos de información de Google QUIC fuente destino 66

Figura 27. Creación de la encuesta mediante los formularios de Google 67

Figura 28. Diferentes respuestas obtenidas por pregunta, para hacer un mejor análisis independiente 68

Figura 29. Jerarquía de protocolos expresado en el porcentaje de utilización en la red, el QUIC está absorbiendo el 79.3% del flujo de tráfico y el TCP solo el 21.7% 69

Figura 30. Comando que se utiliza para acceder a las banderas de configuración de Microsoft Edge 99

Figura 31. Comando que se utiliza para acceder a las banderas de configuración de Google Chrome 99

Figura 32. Comando que se utiliza para acceder a las banderas de configuración de Opera para activar o desactivar varios servicios 100

Figura 33. Diagrama de arquitectura 105

Figura 34. Diagrama de arquitectura 106

Figura 35. Diagrama de arquitectura 111

Figura 36. Diagrama de arquitectura 114

Figura 37. Diagrama de arquitectura 129

Figura 38. El QUIC UDP se desplaza en las diferentes redes y también con los DNS de Google en una razón de tiempo transcurrido en milisegundos 214

Figura 39. Mas de 300 paquetes enviados en un tiempo mayor a un segundo 215

Figura 40. Uso de protocolos TCP, UDP, QUIC UDP en una conexión de Ethernet 215

Figura 41. Filtrado de paquetes que se dan entre la herramienta web Opera y Chrome en diferentes intervalos 218

Figura 42. Diferentes intervalos en que las distintas preguntas se contestaron para la encuesta del Google QUIC UDP 218

INDICE DE TABLAS

Tabla 1: Descripción de los datos que se obtienen de las diferentes redes sociales 70
Tabla 2: Descripción de los datos que se obtiene mediante el análisis de redes 71
Tabla 3: Descripción del diseño de la encuesta con Google Forms 73
Tabla 4: Descripción de los datos que se obtienen mediante la herramienta de Wireshark .. 77
Tabla 5: Datos que se obtienen de las diferentes redes sociales 83
Tabla 6: Datos capturados y analizados por medio de pruebas de penetración 91
Tabla 7: identificación del riesgo con su probabilidad, impacto, peso del riesgo y acciones por seguir 108
Tabla 8: Identificación del riesgo con su probabilidad, impacto, peso del riesgo y acciones para seguir 116
Tabla 9: Esquema de evaluación para QUIC UDP pasos para evaluar la arquitectura del centro de datos 131
Tabla 10: Definición de acrónimos sobre conceptos importantes 161

Abstract

The following research work is to understand the evolution of the QUIC UDP protocol developed by Google, which has been improving in the last decade, and understand the technical feasibility that it may have to be implemented in the Costa Rican industry, especially in centers of data either from public or private companies for the health, financial, entertainment or communications area.

We can mention that since 2009 Google started the investigation of this new protocol to have a competitive advantage over web browsing and over the control of the internet, Google did research that web browsing protocols such as TLS had to be improved for security. HTTPS for secure or non-secure web browsing, make a great improvement with the latency problem that increases in large networks and in the same way the triple verification that TCP / IP does, therefore QUIC UDP comes to give a great contribution I have innovation at the local and also business level and at the same time we can see that there is going to be a great leap in 5G networks, AI and technological trends that are growing, important companies such as AKAMAI, APPLE and MICROSOFT have developed their versions of QUIC UDP on their computers that they offer to their clients, using programming languages such as Python, C, Swift and C#.

The aspects that QUIC UDP improves are connection identifier, flow multiplexing, reliability, security and latency for high-volume data centers and improvement at the local and home level.

The QUIC UDP was developed to improve the problems that arise in the transport of high-volume financial and health information and to have less corruption of information in a more available time.

It makes a great contribution in what are wireless and satellite communications, as a great innovation or contribution in these areas of great daily use, also in the industrial area such as SCADA systems, Industrial Internet of Things (I-IOT), and the great There is a trend with the growth of artificial intelligence (AI) and it is expected that within the evolution of the QUIC UDP architecture, the entire OSI model and its protocols can be moved to this new network design.

Now, this research presents an accessible feasibility because the subject gives access to information and can be combined with other trends that are on the rise, technically there is experienced to understand areas of networks, infrastructure, programming, operating systems, which facilitate the criteria for better support the ideas sought.

At the operational level we can say that we have local tools such as virtual machines and other types of simulators that will allow us to create the data sought and from the economic point of view the researcher will assume all the respective expenses for being an evaluative investigation and not applied where we do not need to create any hardware or work with any company.

In relation to our situation, we have many sources of information that we can obtain from reliable websites such as Cisco, the IEEE, IETF, Google Scholar and the large number of sources of information that these sites give us.

We will focus on a conceptual map, as it is an evaluative investigation, we will use a conceptual cloud, word cloud and conceptual map to understand the architecture of our QUIC UDP protocol and that it works in parallel with TCP / IP.

Our type of research is going to be evaluative and comparison between QUIC UDP and TCP/IP, therefore, the investigative scope is descriptive to understand the

different contexts analyzed and we are going to present a quantitative investigative approach to generate nomothetic type results, the most appropriate design will be quantitative due to the type of approach selected and the objectives already defined, we will use a population and sampling of two types, one based on the survey, which would be our first population, and the second population will be focused on the use of servers in the client server mode, the sampling will be a combination of probabilistic and non-probabilistic.

For our data collection we will be based on Google Forms because we can reach a large population in different places using the internet and obtain data instantly and with this to be able to prepare better responses to the desired analyzes, we will also be based on the Penetration testing tools (Wireshark) to understand the source-destination operation and capture the traffic of the desired protocols between the client and server and build our graphs with that information and have a better compression to carry out the most appropriate analysis.

In relation to our diagnosis analysis we are based on the survey and the Wireshark, to better carry out the survey we will use the available social networks such as Facebook, Slack, Discord, Telegram, WhatsApp, and for the penetration tests we will make captures with the different virtual machines available, different operating systems and different web browsers for each operating system to be used, we have as web browsers, Edge, Opera, Firefox, Chrome and as operating systems Android Tamer, Windows 10, Windows 11, Linux Ubuntu, CentOS 8.

For our solution proposal we will make an introduction to understand the understanding of the different scenarios, how to use the architecture diagrams with a guided step by step with their corresponding numbering, what are the risks present

for each scenario, how are they solved and what is proposed the QUIC UDP as an innovation towards these risks, we will be preparing a report and monitoring our different solution proposals and then we will end up creating an evaluation scheme unifying the two scenarios through a step by step that will be useful to the solution architect or data center engineer looking to migrate to Google Cloud or upgrade their data center infrastructure.

Keywords: protocols, networks, TCP, HTTP, data centers, implementation, security, artificial intelligence, infrastructure, Google, QUIC, SPDY, RTT.

Resumen

El presente trabajo de investigación se elaboró con el objetivo de entender la evolución del protocolo QUIC UDP desarrollado por Google, el cual se ha mejorado en la última década. Además, se buscó comprender la viabilidad técnica que este pueda tener para implementarse en la industria costarricense, especialmente en los centros de datos, ya sea de empresas públicas o privadas para el área de salud, financiero, entretenimiento o comunicaciones.

Asimismo, es posible mencionar que desde el año 2009 Google inició la investigación de este nuevo protocolo para tener una ventaja competitiva sobre la navegación web y sobre el control de la Internet. Google hizo investigaciones de que había que mejorar los protocolos de navegación web como el TLS para seguridad, el HTTPS para navegación web segura o no segura, hacer una gran mejora con el problema de latencia que se incrementa en redes grandes y del mismo modo la triple verificación que hace el TCP/IP.

Por lo tanto, QUIC UDP brinda aporte e innovación en el ámbito local y también empresarial y, al mismo tiempo, es posible ver que se dará un gran salto en redes

5G, IA y las tendencias tecnológicas que están en crecimiento. Empresas importantes como Akamai, Apple y Microsoft han desarrollado sus versiones de QUIC UDP en los equipos que ofrecen a sus clientes, utilizando lenguajes de programación como Python, C, Swift y C#.

Los aspectos que mejora el QUIC UDP son el identificador de conexión, multiplexación de flujos, fiabilidad, seguridad y latencia para centros de datos de alto volumen y mejoramiento en el ámbito local y de hogar.

El QUIC UDP se desarrolló para mejorar los problemas que se presentan en el transporte de información de alto volumen financiero, de salud y tener menos corrupción de información en un tiempo más disponible. Además, aporta en comunicaciones inalámbricas y satelitales, también en el área industrial como sistemas Scada, Internet de las cosas industrial (I-IoT) y la gran tendencia que hay con el crecimiento de las inteligencias artificiales (IA). Se espera que dentro de la evolución de la arquitectura de QUIC UDP se pueda mover todo el modelo OSI y sus protocolos a este nuevo diseño de redes.

Esta investigación presentó una viabilidad accesible porque el tema dio acceso a la información y se puede combinar con otras tendencias que están en auge. Técnicamente, se cuenta con experiencia para comprender áreas de redes, infraestructura, programación y sistemas operativos, que facilitan el criterio para fundamentar mejor las ideas buscadas.

A nivel operativo es posible afirmar que se contó con las herramientas locales como máquinas virtuales y otros tipos de simuladores que permiten crear los datos buscados. Desde el punto de vista económico, la persona investigadora asumió

todos los gastos por ser una investigación evaluativa y no aplicada en donde no se necesitó realizar ningún *hardware* ni trabajar con ninguna empresa.

En cuanto al estado de la cuestión, se contó con muchas fuentes de información que fue posible obtener de sitios web confiables como Cisco, la IEEE, IETF, Google Académico. Al ser una investigación evaluativa se utilizó una nube conceptual, nube de palabras y mapa conceptual para comprender la arquitectura del protocolo QUIC UDP y que trabaja en forma paralela con el TCP/IP.

El tipo de investigación fue evaluativo y de comparación entre QUIC UDP y TCP/IP, por lo tanto, el alcance fue descriptivo para entender los diferentes contextos analizados y se presentó un enfoque cuantitativo para generar resultados nomotéticos. El diseño más adecuado fue el cuantitativo por el tipo de enfoque seleccionado y los objetivos definidos.

Por otra parte, se utilizó una población y muestreo de dos tipos. Uno se basó en la encuesta que es la primera población y la segunda población se enfocó en el uso de servidores en el modo cliente servidor. El muestreo consistió en una combinación probabilístico y no probabilístico.

Para la recolección de datos se basó en Google Forms, debido a que es posible llegar a una gran población en distintos lugares utilizando la Internet y obtener datos en una forma instantánea y con esto elaborar mejores respuestas a los análisis deseados. También se basó en las herramientas de pruebas de penetración (Wireshark) para entender el funcionamiento fuente destino y capturar el tráfico de protocolos deseados entre cliente servidor y construir los gráficos con esa información para comprenderla mejor y realizar los análisis más adecuados.

El análisis del diagnóstico se fundamentó en la encuesta y el Wireshark. Para realizar mejor la encuesta se utilizaron las redes sociales disponibles como Facebook, Slack, Discord, Telegram, WhatsApp y para las pruebas de penetración se realizaron capturas con las diferentes máquinas virtuales disponibles, distintos sistemas operativos y diversos navegadores web por cada sistema operativo por utilizar. Como navegadores web están Edge, Opera, Firefox, Chrome y como sistemas operativos Android Tamer, Windows 10, Windows 11, Linux Ubuntu, CentOS 8.

Para la propuesta de solución se hizo una introducción para comprender los diferentes escenarios, como utilizar los diagramas de arquitectura con un paso a paso guiado con su numeración correspondiente, cuáles son los riesgos presentes por cada escenario, cómo se solucionan y qué es lo que propone el QUIC UDP como innovación hacia esos riesgos.

Por último, se elaboró un informe y seguimiento a las diferentes propuestas de solución y se creó un esquema de evaluación para unificar los dos escenarios mediante un paso a paso. Esto es de utilidad para el arquitecto de solución o el ingeniero del centro de datos que quiera realizar una migración al Cloud de Google o mejorar la infraestructura de su centro de datos.

Palabras clave: protocolos, redes, TCP, HTTP, centros de datos, implementación, seguridad, inteligencia artificial, infraestructura, Google, QUIC, SPDY, RTT.

Capítulo 1. Introducción

Desde el año 2013 se han desarrollado investigaciones sobre uno de los protocolos más importantes que se usan diariamente en la navegación de Internet, que es el protocolo TCP/IP y la necesidad de mejorar la navegación web mediante el protocolo HTTP/3. La empresa Google quiere desarrollar un protocolo mejor que revolucionará la forma de las comunicaciones en el uso diario, para transferir información, consultarla y varias formas de entretenimiento, como la televisión digital que utiliza la Internet para desplegar su información.

Mediante el protocolo Google QUIC se optimizan muchos problemas ya conocidos. Uno de estos problemas es la latencia en las redes y la triple verificación que hace el protocolo TCP/IP para asegurar el tráfico de la información o paquetes. Cuando las redes se hacen más grandes este problema se incrementa a niveles que no son correctos, en especial para una compañía que maneja información sensible como financiera o en el área de salud.

También se tiene una gran revolución para la Internet 5G y el área de inteligencia artificial, al diseñar redes más rápidas, seguras y una latencia extremadamente baja y todo esto para diseñarse con el Google Chrome. También empresas como Akamai y Apple desarrollan sus versiones de este protocolo que se basa en lenguajes de programación como Python, C y Swift.

1.1 Generalidades

Google, al ser una de las tres empresas más grandes del mundo, realiza investigaciones para mejorar los problemas más comunes que se presentan en las redes modernas, como la latencia, seguridad, fiabilidad, multiplexación de flujos, identificador de conexiones y muchos otros aspectos por considerar. La gran cantidad de servidores, usuarios finales, centros de datos de diferentes niveles de

calidad como nivel 3 a nivel 4, hace que estos puntos de concentración de información sean de alta sensibilidad y de cuidado para el cliente final. De esta manera, se han invertido años de investigación en el Google QUIC, para lograr que los protocolos de la capa de transporte se migren a esta versión mejorada, pero se empieza con el HTTP seguro al ser un punto de concentración masivo.

1.2 Antecedentes del problema

Los ingenieros de Google empezaron a realizar investigaciones desde el año 2009, lo que dio como resultado la primera versión experimental del Google QUIC en el 2012. Esto sirvió para resolver problemas de latencia y seguridad en empresas importantes con base en el tradicional HTTP y TLS que presentaban serios problemas en el transporte de información en países de alto volumen financiero y de salud. Lo anterior significó poner en riesgo datos sensibles y corrupción de información en servidores claves y también representaba más gastos económicos al tener que contar con más *hardware* para sustentar las necesidades empresariales y salvaguardar el activo más importante de las compañías, los datos.

1.3 Definición y descripción del problema

En este proyecto investigativo el objetivo es entender las ventajas que presenta el Google QUIC, cómo se puede comparar con el tradicional formato de comunicación que es el TCP/IP y también cómo resolver las desventajas que se puedan presentar en la implementación del Google QUIC. El problema ya se ha resuelto para varias empresas, como el mismo Google, Facebook, Apple, Akamai y otras compañías de un alto volumen de usuarios en donde se necesita la consulta de información en un tiempo demasiado corto. También cómo mejorar otros problemas de comunicación inalámbricos y satelitales en donde la arquitectura de QUIC representa una gran solución.

1.4 Justificación

Este trabajo investigativo presenta un gran aporte y una innovación hacia el futuro de las redes de comunicación en el ámbito nacional y mundial. Se ha estado trabajando con un modelo tradicional de red que es el TCP/IP, sin embargo, las redes actuales y las nuevas tecnologías ya no se pueden seguir moviendo con este modelo.

El constante crecimiento de centros de datos de más calidad y la necesidad de presentar mejor información a grandes distancias casi de forma inmediata, hace que la evolución del Google QUIC en las redes sea lo más adecuado. Incluso hay empresas de clase mundial que desarrollan su propia versión de QUIC, con lo que se reduce la latencia, problemas de seguridad, tiempo de respuesta cliente-servidor, manejo de certificados digital y claves. También fortalece las redes inalámbricas, satelitales, redes 5G, dispositivos de Internet de las cosas en el ámbito industrial (I-IoT), sistemas Scada y una gran variabilidad de inteligencias artificiales.

Otra tendencia es el uso de protocolos de red, no solo el HTTP que ha saltado a varias versiones desde la versión HTTP 1, hasta la que se mueve actualmente, la versión HTTP 3. Esto es lo que se quiere perfeccionar con el Google QUIC y que todos los demás protocolos de red como el FTP, DNS, TFTP, SMTP, POP, IMAP, IP, NAT, PAT, ICMP, OSPF, EIGRP, ARP, PPP, trabajen dentro de la arquitectura de Google QUIC, como una sola solución unificada.

1.5 Viabilidad

La viabilidad de este estudio es muy accesible. Al ser una investigación evaluativa sobre protocolos desarrollados se encuentran muchas fuentes de información que dan amplitud de criterios para desarrollar el tema expuesto y llegar a una gran variabilidad de conclusiones. A partir de esto se desarrollan otros temas

de gran innovación que se mueven en la esfera mundial como el Internet de las cosas, la inteligencia artificial, sistemas Scada, etc.

1.5.1 Punto de vista técnico

Desde el punto de vista técnico es posible afirmar que los años de trabajo, estudios universitarios anteriores y las diferentes empresas en las cuales se ha trabajado, más el conocimiento adquirido durante la carrera dan fe de que la persona investigadora tiene capacidad para comprender áreas de redes, infraestructura, programación, configuraciones complejas, servidores, diseño digital, sistemas operativos y *hardware* en general. También se ha construido el camino para comprender el área de conocimiento en redes Cisco, en lo cual se puede estabilizar la comprensión de los distintos protocolos que se utilizan en redes.

1.5.2 Punto de vista operativo

Al ser una investigación evaluativa es posible afirmar que la operabilidad de esta es muy accesible, ya que se poseen los recursos informáticos necesarios y mucha información disponible. Además, la investigación se desarrolla en forma teórica, no se construye ninguna parte práctica.

Por otra parte, se pueden hacer simulaciones utilizando el Packet Tracer, GNS3, ns3, Wireshark, VM en Ubuntu, Android Tamer, Windows 10 o Windows 11, CentOS, para crear los laboratorios necesarios y ver la viabilidad técnica de este protocolo QUIC comparado con el tradicional TCP. Además, hacer una evaluación, realizar un nuevo esquema de evaluación y llevar a cabo comparaciones de estudio que dan buenos resultados si se puede implementar en la industria tecnológica costarricense.

1.5.3 Punto de vista económico

Al ser una investigación teórica, evaluativa y comparativa, el costo es muy manejable. No se pretende fabricar ningún tipo de equipo, no se utiliza ningún *hardware*, el comportamiento de los protocolos por estudiarse quedarán expresados en forma teórica y se puede utilizar algún simulador para entender sus comportamientos en una red. Todo el tiempo y horas de investigación lo asume el mismo investigador y se cuenta con el servicio del tutor para calificar el avance de manera correcta.

1.6 Objetivos

La taxonomía cognitiva por utilizar es la de Bloom de 1956, porque es la más comprensible y posee mejores ejemplos para seguir. Se cuenta con más información para investigar sobre esa taxonomía y, gráficamente, tiene una estructura más entendida y adecuada, en donde se puede expresar mejor los objetivos necesarios, además de que se utiliza en el sistema educativo de Costa Rica.

1.6.1 Objetivo general

El objetivo general es el siguiente:

- Determinar la viabilidad técnica del uso del protocolo QUIC UDP para las empresas en Costa Rica.

1.6.2 Objetivos específicos

Los objetivos específicos de la investigación son los siguientes:

- Definir qué es el protocolo QUIC UDP.
- Describir los serios problemas de latencia que hay en las redes.
- Comprender la seguridad, establecimiento y migración de la conexión, multiplexación de Streams, control de flujo y congestión.
- Explicar las innovaciones tecnológicas que tiene este nuevo protocolo.
- Demostrar cómo QUIC es mejor que el TCP/IP.

- Analizar los beneficios de QUIC y el futuro de la Internet con el HTTP/3.
- Proponer mejores soluciones al tráfico moderno de la información en los centros de datos y su enlace con nuevas tecnologías.
- Considerar que QUIC es una solución para la criptografía moderna con relación a certificados y claves de acceso.
- Evaluar la viabilidad técnica del protocolo QUIC UDP.

1.7 Alcances y limitaciones

1.7.1 Alcances

Como parte de los alcances o entregables se tiene documentación clara y sencilla a manera de resumen que explica toda la solución en forma general. También se puede confeccionar una guía evaluativa paso a paso para entender el comportamiento del protocolo QUIC UDP *versus* el TCP/IP. Asimismo, se puede ofrecer una capacitación básica para demostrar las ventajas y desventajas de la implementación de este nuevo protocolo en una infraestructura o en un centro de datos.

1.7.2 Limitaciones

No se construye ningún *hardware* y tampoco se utiliza ningún cliente-servidor para demostrar el comportamiento del protocolo QUIC UDP, en forma práctica, todo el comportamiento quedará expreso en la documentación. El alto costo del área abordada no permite ir más allá de una propuesta teórica, solo se trabaja con la tecnología disponible en el país.

1.8 Marco de deferencia organizacional y socioeconómico

Esta investigación es evaluativa, por lo tanto, no existe relación relevante con ningún cliente. Se realiza una evaluación en forma muy teórica, con ejemplos, paso a paso y ayudas gráficas, para su mejor entendimiento.

1.8.1 Historia

De acuerdo con Morales Gómez (2019):

Desde los años 80, la capa de transporte en las redes de Internet ha sido controlada principalmente por dos protocolos: TCP (Protocolo de Control de Transmisiones) y UDP (Protocolo de Datagramas de Usuario), el primero orientado a las conexiones mientras que el segundo al envió [sic] de datagramas. Ambos protocolos presentan dificultades para adaptarse a los nuevos requerimientos de las redes actuales. Por ello, Google ha desarrollado un nuevo protocolo, QUIC (Conexiones UDP Rápidas en Internet). QUIC fue presentado en 2014 y actualmente se usa en el navegador web Google Chrome, así como en el resto de los servicios que ofrece el ecosistema de Google. Este protocolo posee la cualidad de usar UDP como protocolo de transporte, pero añade las características de control y cifrado de conexiones correspondientes a TCP y TLS (Seguridad de la Capa de Transporte) (p. 3).

Además, Estrada Corona (2004) señala:

Los protocolos IP (Protocolo de Internet) y TCP (Protocolo de Control de Transmisión) se originan a principios de 1980 y fueron adoptados por la red ARPANET en 1983, que estaba integrada por cientos de computadoras de universidad, centros de investigación militar y algunas empresas. El email (correo electrónico) fue el servicio más comúnmente utilizado entonces, mientras que el sistema operativo más empleado era UNIX, en su versión BSD UNIX, desarrollado por la Universidad de California. Fue a mediados de los ochenta cuando fue creado el protocolo TCP/IP con la finalidad de contar con un lenguaje común a todas las

computadoras conectadas a Internet, ya con la unión de las redes ARPANET, CSNET y MILNET. El protocolo TCP/IP representa, entonces las reglas que hacen posible la conexión de computadoras de marcas y tecnologías diferentes (p. 4).

1.8.2 Tipo de negocio y mercado meta

El mercado meta consiste en los centros de datos modernos que se pueden acoplar a esta nueva tecnología, los cuales pueden migrar con el Google QUIC y solo hacer algunos ajustes esenciales en su sistema operativo. También se pueden utilizar los centros de datos de Google en el ámbito mundial, empresas de la banca privada pública, centros de salud, entretenimiento, televisión 4k por Internet ofrecido por las empresas de cable y centros comerciales.

1.8.3 Misión, visión y valores

Al no tener una empresa definida y ser una investigación evaluativa con un esquema de evaluación, la misión, visión y valores se pueden definir en la calidad del trabajo realizado dentro de la evaluación y así lograr calidad en la planeación estratégica.

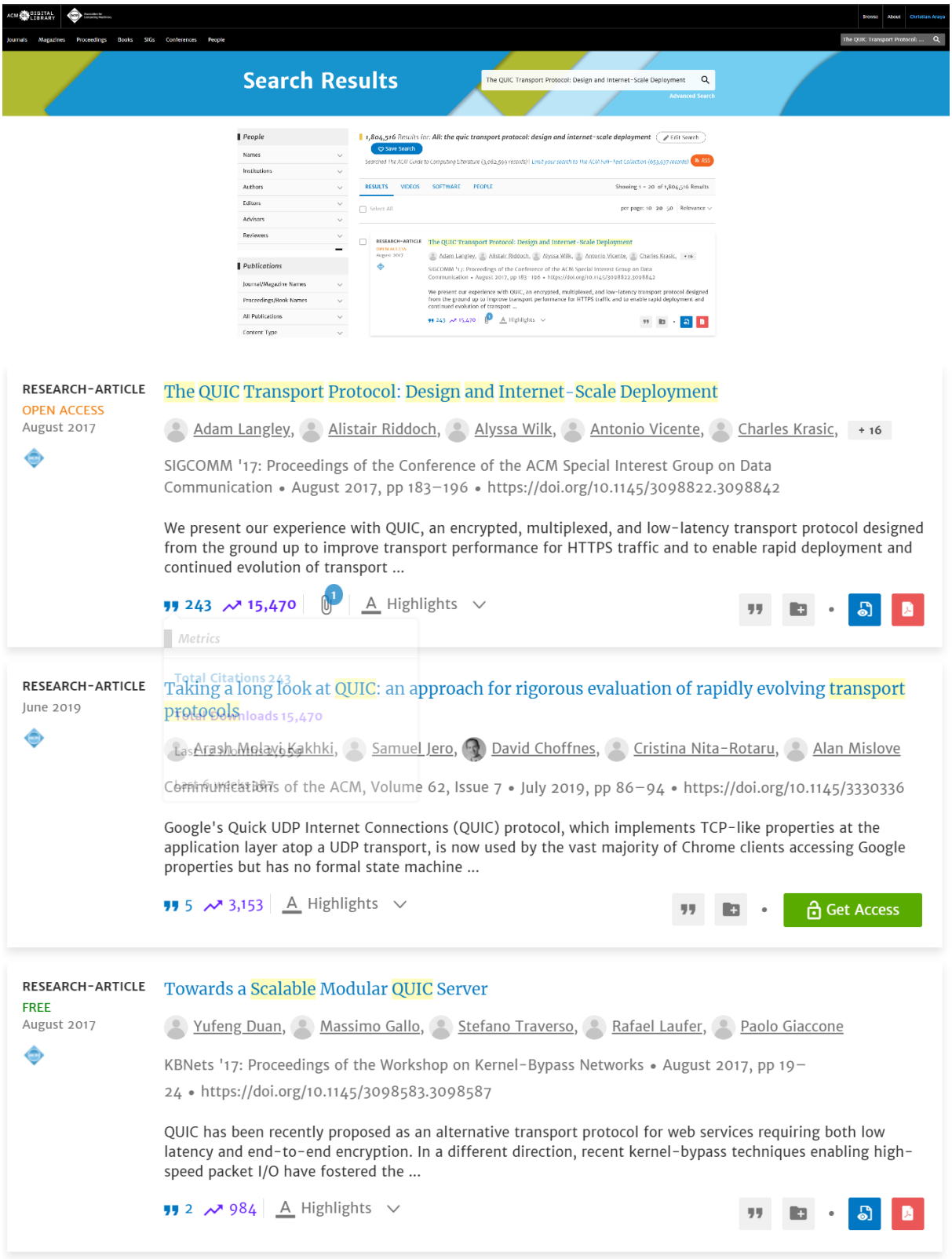
1.8.4 Políticas institucionales

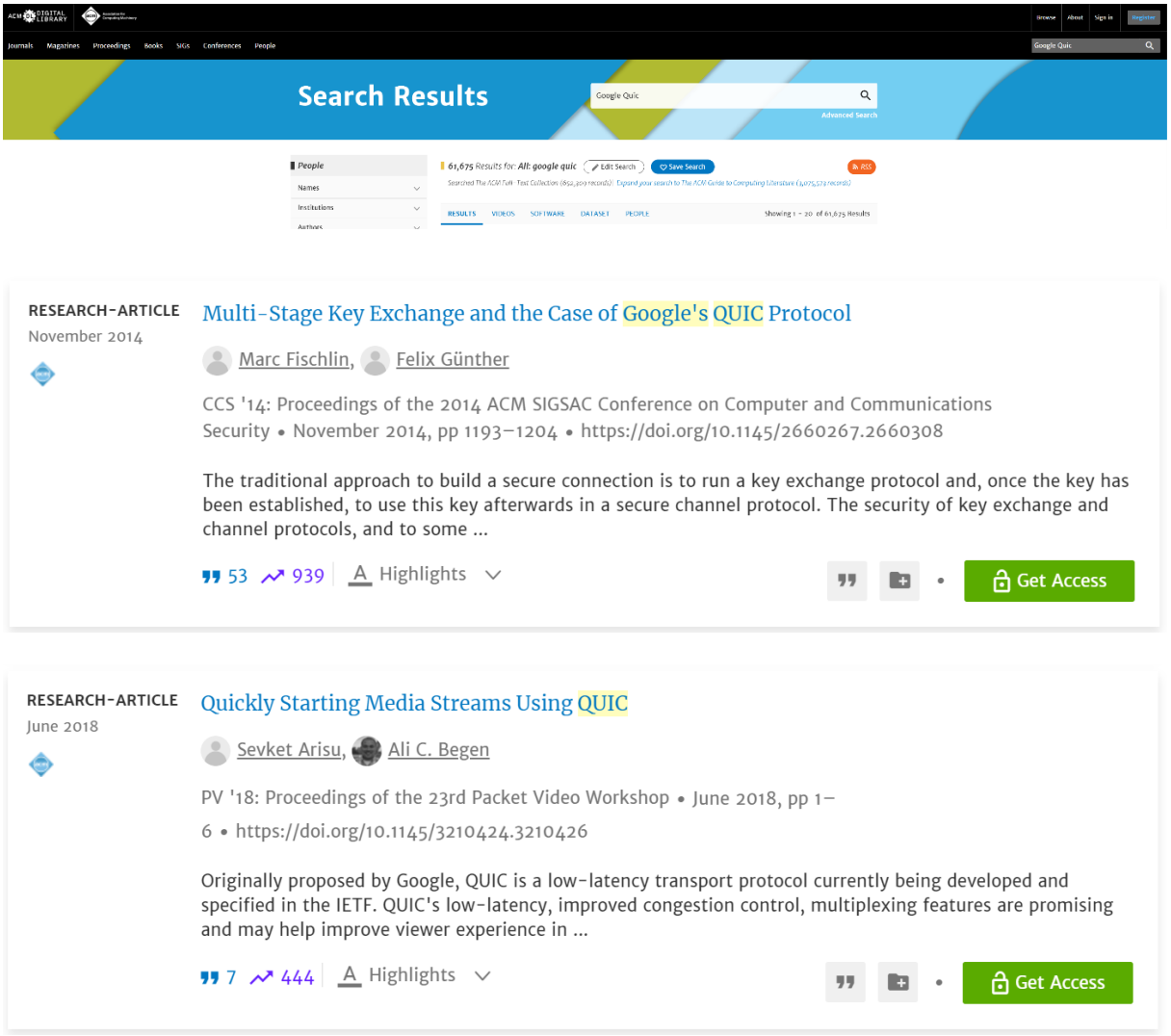
Las políticas institucionales va a crearlas el mismo investigador, debido a que la organización o la empresa no existe, sino que hará un esquema de evaluación específico en un área.

1.9 Estado de la cuestión

Para el estado de la cuestión se tienen las siguientes fuentes de información que se recopilaron de los siguientes repositorios: www.dl.acm.org/. Se encontraron 61675 fuentes de información sobre el Google QUIC y 1,804,516 fuentes de

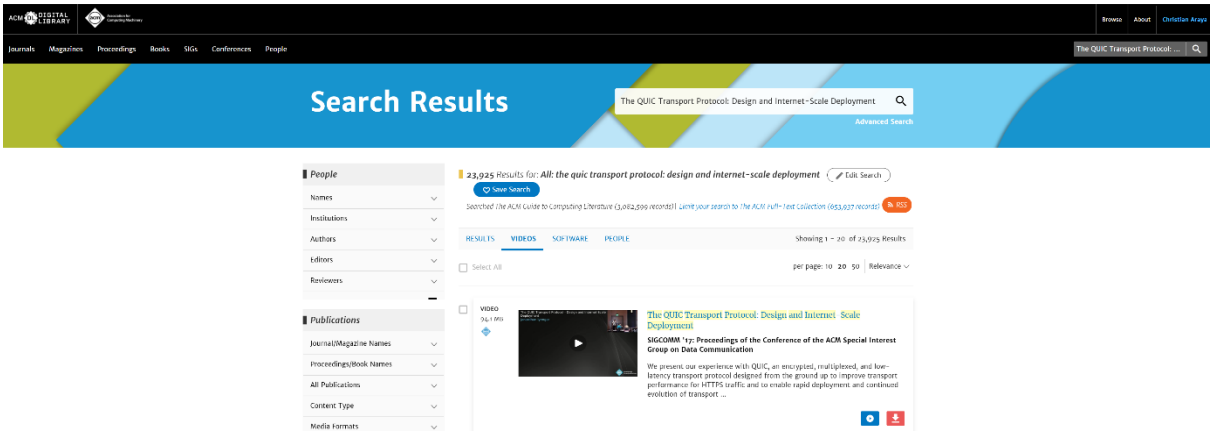
información adicionales para el despliegue escalable de Internet y su diseño con base en el protocolo de transporte QUIC.





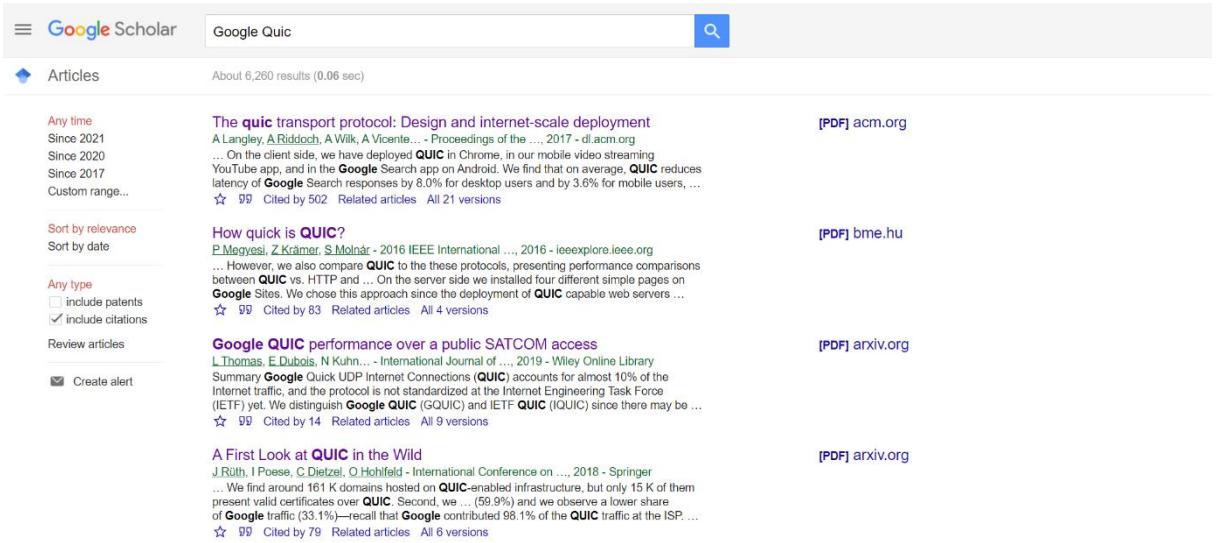
1.9.1 Fuentes de información en video

Además, es posible observar que se tienen 23,925 fuentes de información adicionales en video para entender la evolución de este protocolo QUIC.



1.9.2 Repositorio Google Académico

Otro repositorio muy importante es el Google Académico (https://scholar.google.com/) en el que se encontraron 6260 fuentes de información sobre el Google QUIC.



QUIC: Better for what and for whom? [PDF] archives-ouvertes.fr
S Cook, B Mathieu, P Truong… - 2017 IEEE International …, 2017 - ieeexplore.ieee.org
… with the one implemented in TCP [5], and they also analyze the load times of a web page when using **QUIC**, HTTP/1.1, SPDY (a now-deprecated protocol by **Google**, which has served as a basis for HTTP/2 specifications). Paper [6] also proposes a similar evaluation of …
☆ 99 Cited by 63 Related articles All 3 versions

Multipath **quic**: Design and evaluation [PDF] uclouvain.be
Q De Coninck, O Bonaventure - … of the 13th international conference on …, 2017 - dl.acm.org
… We implement Multipath **QUIC** inside the **QUIC** open-source implementation written in go [9] and compare in Section 4 its performance with MPTCP in a wide range of scenarios using … [25] identified some performance issues with the Chromium implementation of **Google QUIC**. …
☆ 99 Cited by 136 Related articles All 10 versions

A novel **QUIC** traffic classifier based on convolutional neural networks [PDF] researchgate.net
V Tong, HA Tran, S Souihi… - 2018 IEEE Global …, 2018 - ieeexplore.ieee.org
… In comparison with current methods, the proposed method can detect some kind of **QUIC**-based services such as **Google** Hangout Chat, **Google** Hangout Voice Call, YouTube, File transfer and **Google** play music. Besides, the proposed method can achieve the microaveraging …
☆ 99 Cited by 38 Related articles All 3 versions

Quickly starting media streams using **QUIC** [PDF] ozyegin.edu.tr
S Arisu, AC Begen - Proceedings of the 23rd Packet Video Workshop, 2018 - dl.acm.org
… To investigate what issues due to running HTTP over TCP can be alleviated by using HTTP over **QUIC**, we measured **QUIC**'s streaming … First, because of the lack of a Python library implementation for **QUIC**, we integrated the **QUIC** client that was provided by **Google** into the …
☆ 99 Cited by 15 Related articles All 3 versions

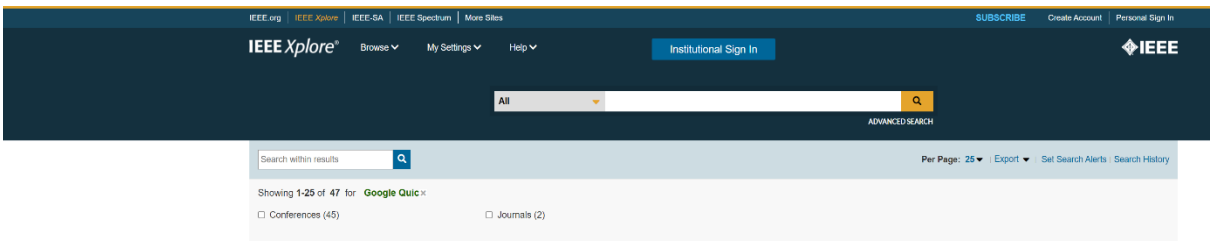
How secure and quick is **QUIC**? Provable security and performance analyses [PDF] 173.236.186.201
R Lychev, S Jero, A Boldyreva… - 2015 IEEE Symposium …, 2015 - ieeexplore.ieee.org
… While we believe **Google** may be more agreeable to tweak the protocol to make it suitable for modular analysis, until that happens, the security of **QUIC** as a whole is not known. Furthermore, the change proposed in [11] will not suffice because the way authenticated encryption …
☆ 99 Cited by 99 Related articles All 20 versions

Does **quic** make the web faster? [PDF] uh.edu
P Biswal, O Gnawali - 2016 IEEE Global Communications …, 2016 - ieeexplore.ieee.org
… Recent developments to speed up the web have resulted in two promising protocols, HTTP/2 (RFC 7540) at the application layer and **QUIC** (multiplexed stream transport over UDP). **Google** servers are using HTTP/2 and **QUIC** whereas other major sites like Facebook and …
☆ 99 Cited by 48 Related articles All 5 versions

Goooooooooogle ›
1 2 3 4 5 6 7 8 9 10 Next

1.9.3 Repositorio IEEE

Otro repositorio que complementa las fuentes de información necesarias para este estudio es la IEEE (https://ieeexplore.ieee.org/) con 47 fuentes de información sobre el Google QUIC.



Comparison of Present-day Transport Layer network Protocols and Google's QUIC
Omkar Nalawade; Amit Dhanwani; Tejashree Prabhu
2018 International Conference on Smart City and Emerging Technology (ICSCET)
Year: 2018 | Conference Paper | Publisher: IEEE
Cited by: Patents (1)

Abstract HTML

And QUIC meets IoT: performance assessment of MQTT over QUIC
Fátima Fernández; Mihail Zverev; Pablo Garrido; José R. Juárez; Josu Bilbao; Ramón Agüero
2020 16th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)
Year: 2020 | Conference Paper | Publisher: IEEE

Abstract HTML

Evaluating QUIC's Performance Against Performance Enhancing Proxy over Satellite Link
John Border; Bhavit Shah; Chi-Jiun Su; Rob Torres
2020 IFIP Networking Conference (Networking)
Year: 2020 | Conference Paper | Publisher: IEEE

Abstract HTML

CQUIC: Cross-Layer QUIC for Next Generation Mobile Networks
Gaurav Sinha; Madhan Raj Kanagarathinam; Sujith Rengan Jayaseelan; Gunjan Kumar Choudhary
2020 IEEE Wireless Communications and Networking Conference (WCNC)
Year: 2020 | Conference Paper | Publisher: IEEE
Cited by: Papers (2)

Abstract HTML

QUIC-FEC: Bringing the benefits of Forward Erasure Correction to QUIC
François Michel; Quentin De Coninck; Olivier Bonaventure
2019 IFIP Networking Conference (IFIP Networking)
Year: 2019 | Conference Paper | Publisher: IEEE

Abstract HTML

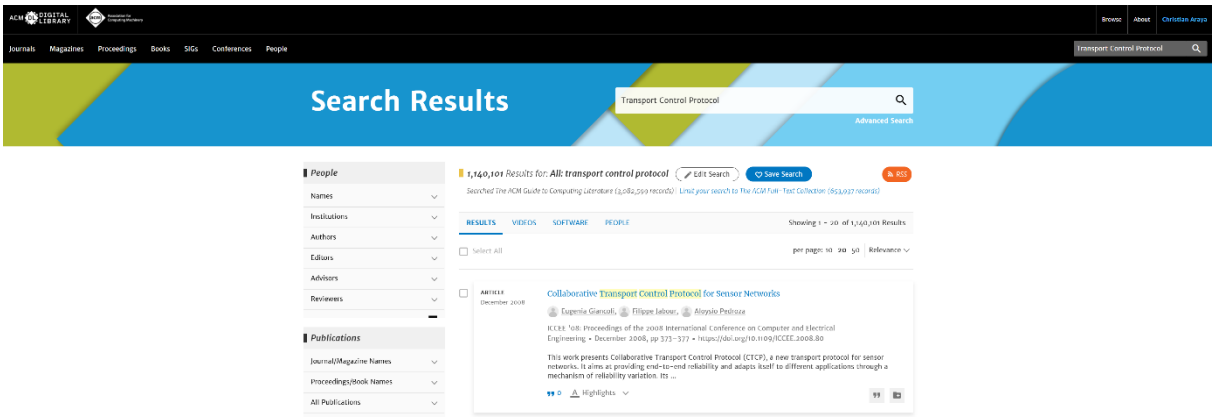
1.9.4 Cadena de búsqueda scimagojr

Asimismo, es posible verificar las cadenas de búsqueda en el sitio web:

https://www.scimagojr.com/

1.9.5 Protocolo TCP con 1,140,101 resultados

Para el estado de la cuestión que sustenta la investigación evaluativa se tiene para el protocolo TCP con 1,140,101 resultados que complementan la comparación con suficientes fuentes de información.



ARTICLE
December 2008

Collaborative Transport Control Protocol for Sensor Networks

Eugenia Giancoli, Filippe Jabour, Aloysio Pedroza

ICCEE '08: Proceedings of the 2008 International Conference on Computer and Electrical Engineering • December 2008, pp 373–377 • https://doi.org/10.1109/ICCEE.2008.80

This work presents Collaborative Transport Control Protocol (CTCP), a new transport protocol for sensor networks. It aims at providing end-to-end reliability and adapts itself to different applications through a mechanism of reliability variation. Its ...

0 | Highlights

ARTICLE
December 2009

Modified Transport Control Protocol for Cellular Network

Sonali Sankpal, P. P. Kulkarni

ICETET '09: Proceedings of the 2009 Second International Conference on Emerging Trends in Engineering & Technology • December 2009, pp 1127–1131 • https://doi.org/10.1109/ICETET.2009.153

Day by day popularity of wireless devices used to access the Internet is increasing. It indicates that in the near future TCP protocol will be frequently used over the wireless links. The wireless links characteristics are significantly different from ...

0 | Highlights

CHAPTER
January 2003

Mobility over transport control protocol/internet protocol (TCP/IP)

José Ferreira de Rezende, Michele Mara de Araújo Espíndula Lima, + 1

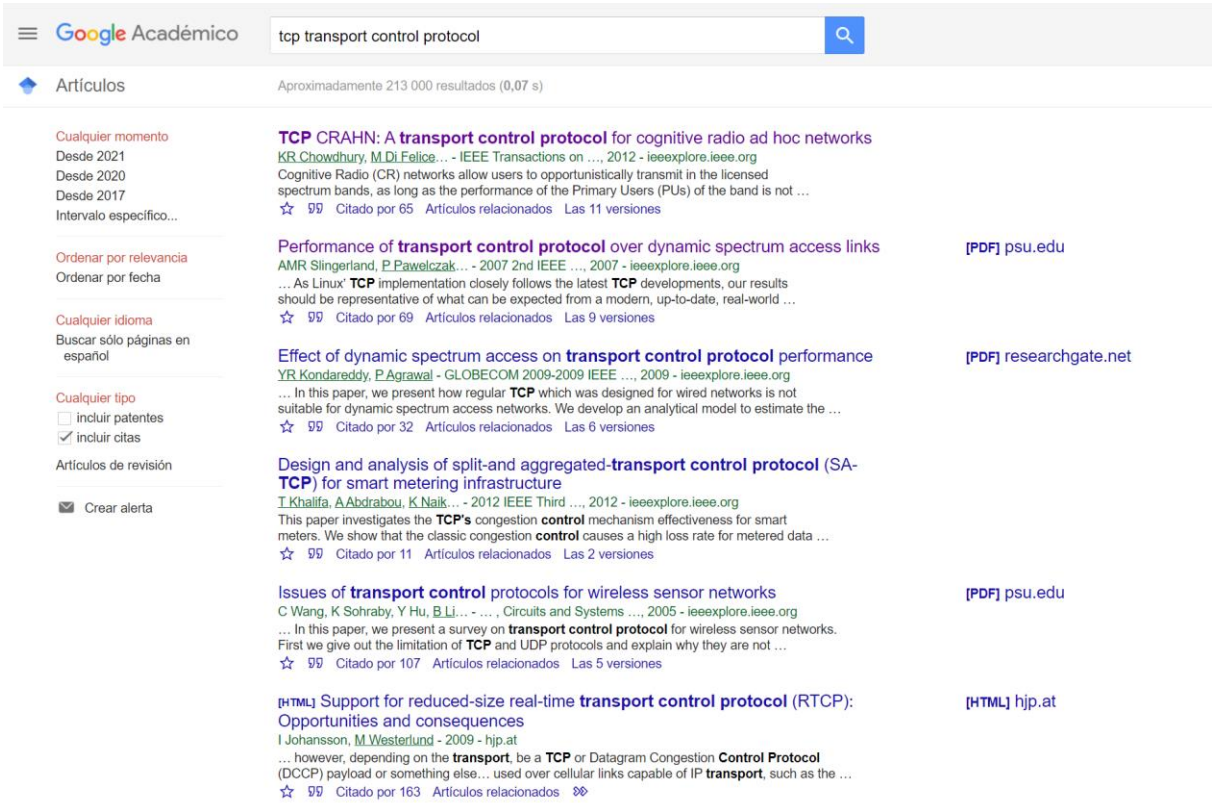
The handbook of ad hoc wireless networks • January 2003, pp 329–343

Advances in wireless communications have enabled access to the Internet for mobile users, but the Transport Control Protocol/Internet Protocol (TCP/IP) protocol stack of the Internet, designed to be independent of the link layer technology, involves ...

0 | Highlights

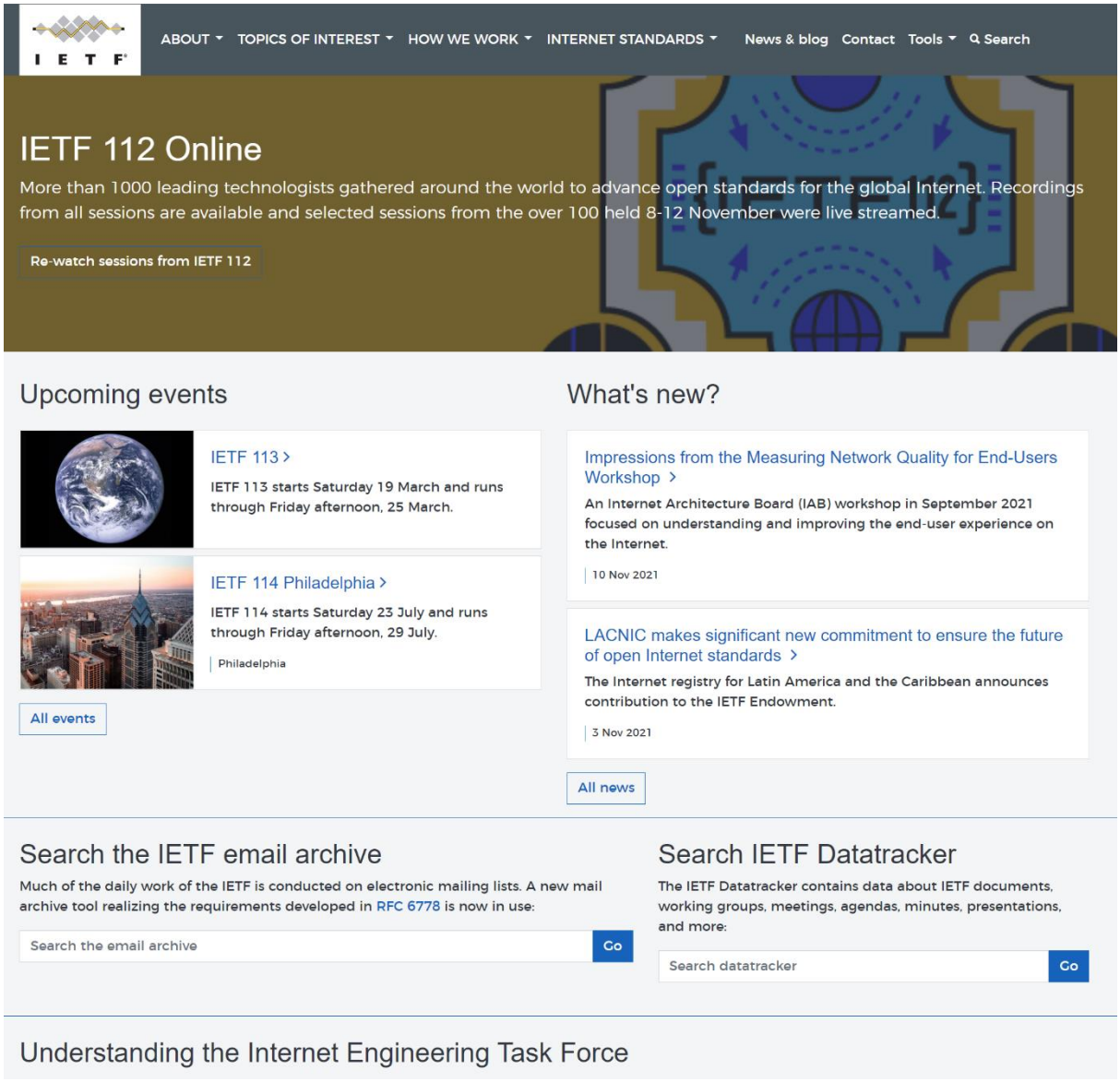
1.9.6 Google Académico fuentes de información para TCP

Si se utiliza el Google Académico para el protocolo de control de transporte TCP, se tienen 213,000 fuentes de información. A partir de esto es posible hacer una comparación entre TCP y QUIC.



1.9.7 Repositorio IETF

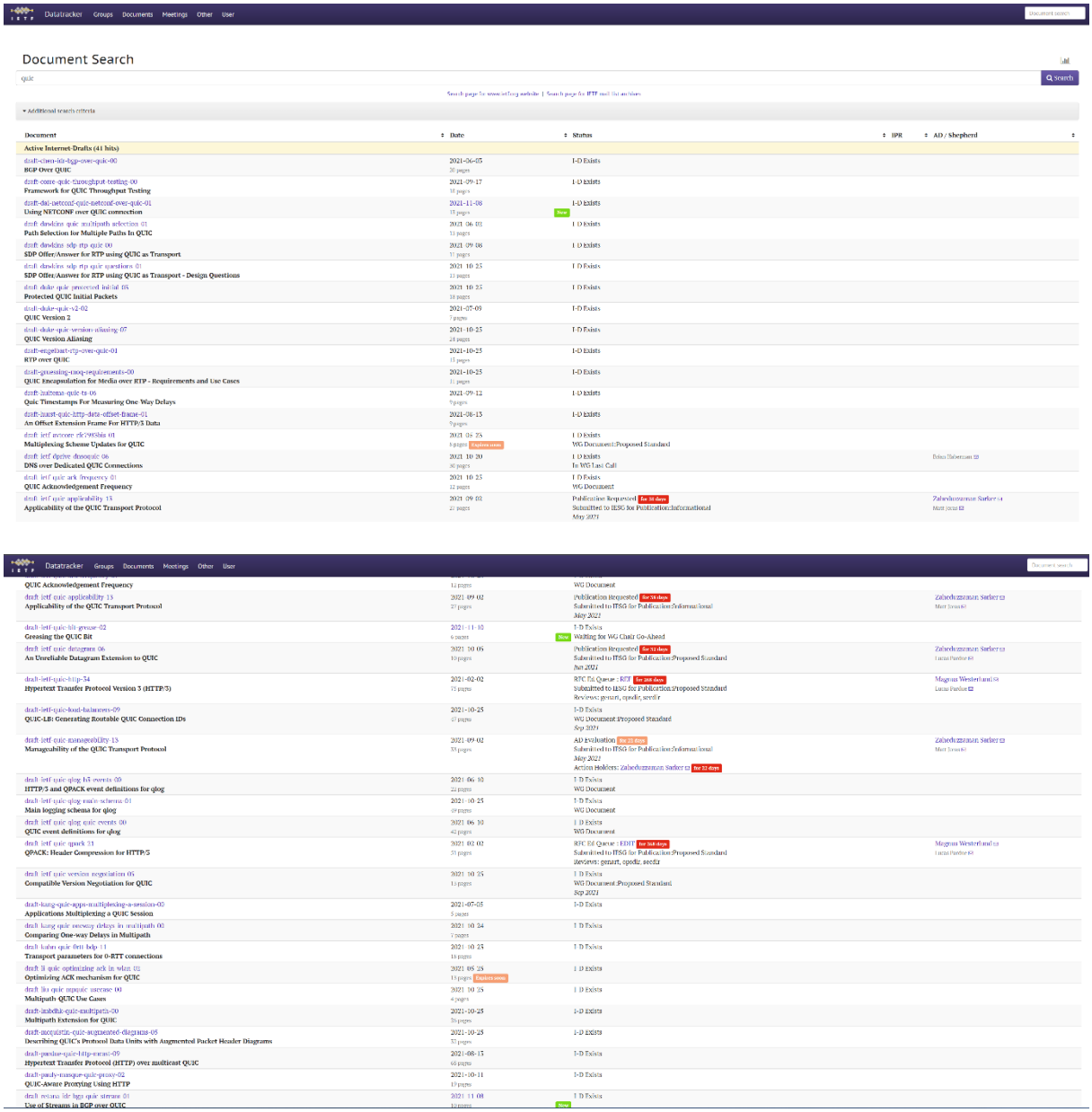
La Internet Engineering Task Force (IEFT) es otra fuente de información o repositorio. En esta trabajan con el proyecto de QUIC, lo que indica la búsqueda de información actualizada en su sitio web: https://www.ietf.org/



1.9.8 Repositorio IETF documentos

Aquí es posible observar hasta más de 50 documentos con más de 20, 40 y hasta 50 páginas para realizar investigación. Estos pueden verificarse en el siguiente enlace del IETF:

https://datatracker.ietf.org/doc/search/?name=quicyrfcs=onyactivedrafts=onyby=group



Capítulo 2. Marco conceptual

2.1 Comparación QUIC UDP y TCP/IP

En el siguiente marco conceptual se presenta una comparación entre el Google QUIC UDP y el TCP/IP. Mediante una nube conceptual, nube de palabras y un mapa conceptual se explican las principales ventajas y desventajas entre ambos protocolos y su evolución en el tiempo.

2.1.2 Nube conceptual

Como primer paso se desarrolla una nube conceptual para comprender los aspectos o términos más importantes de la investigación evaluativa y así ayudar al lector a tener un mejor acercamiento de esos términos. También se pueden observar las dos zonas de investigación entre Google QUIC y el TCP/IP que se usan por lo general en las redes actuales.

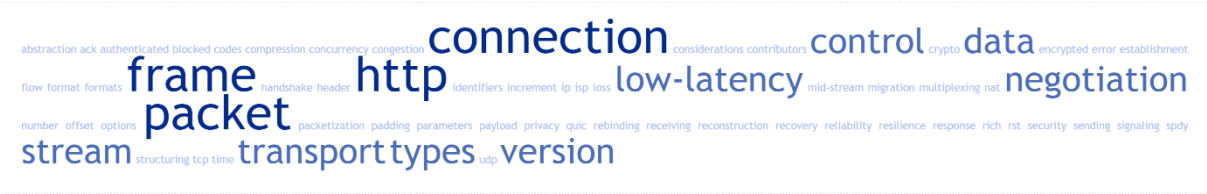


Figura 1: Nube de palabras generado utilizando el sitio tagcrowd

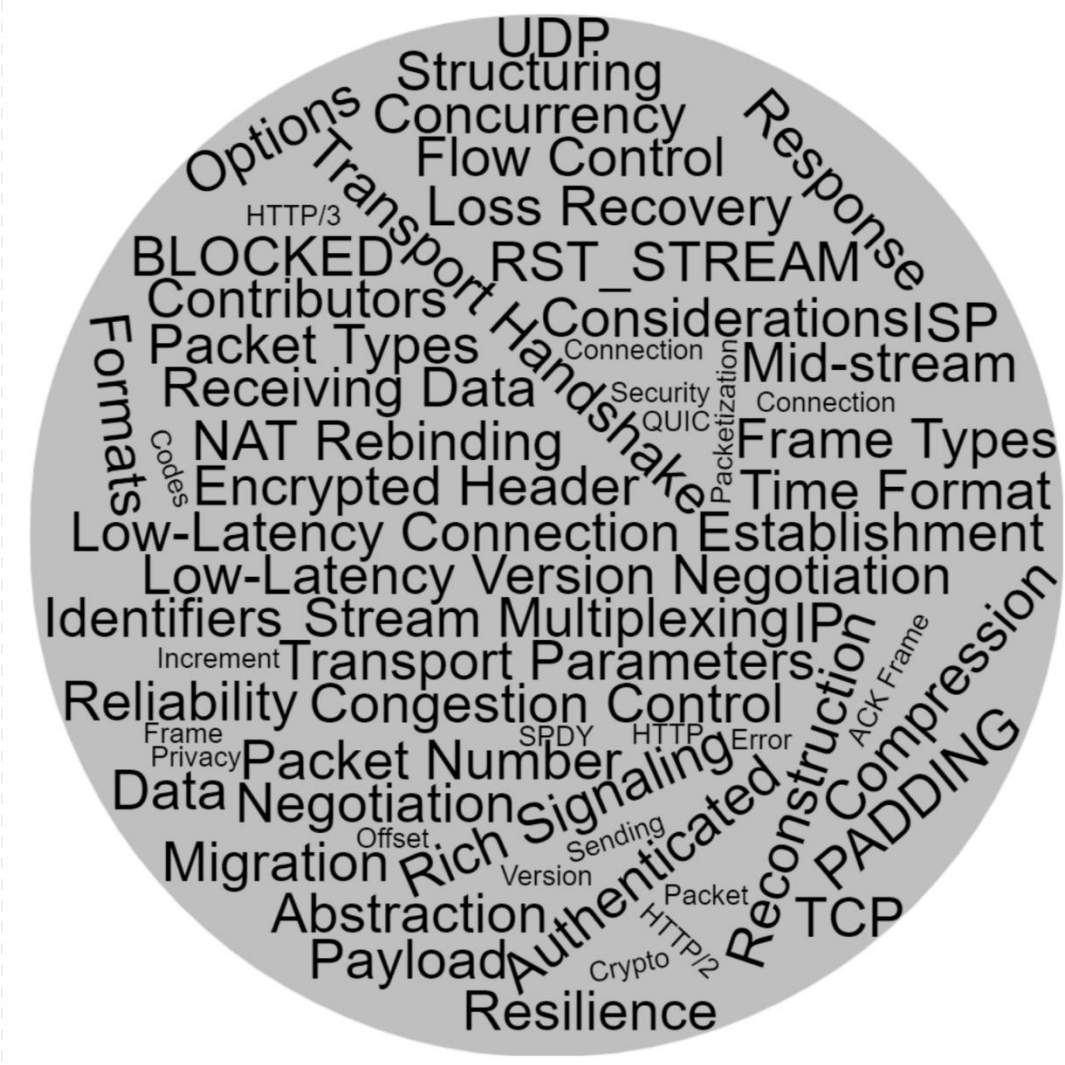


Figura 2: Nube de palabras generado utilizando el sitio nubedepalabras

Mapa conceptual.

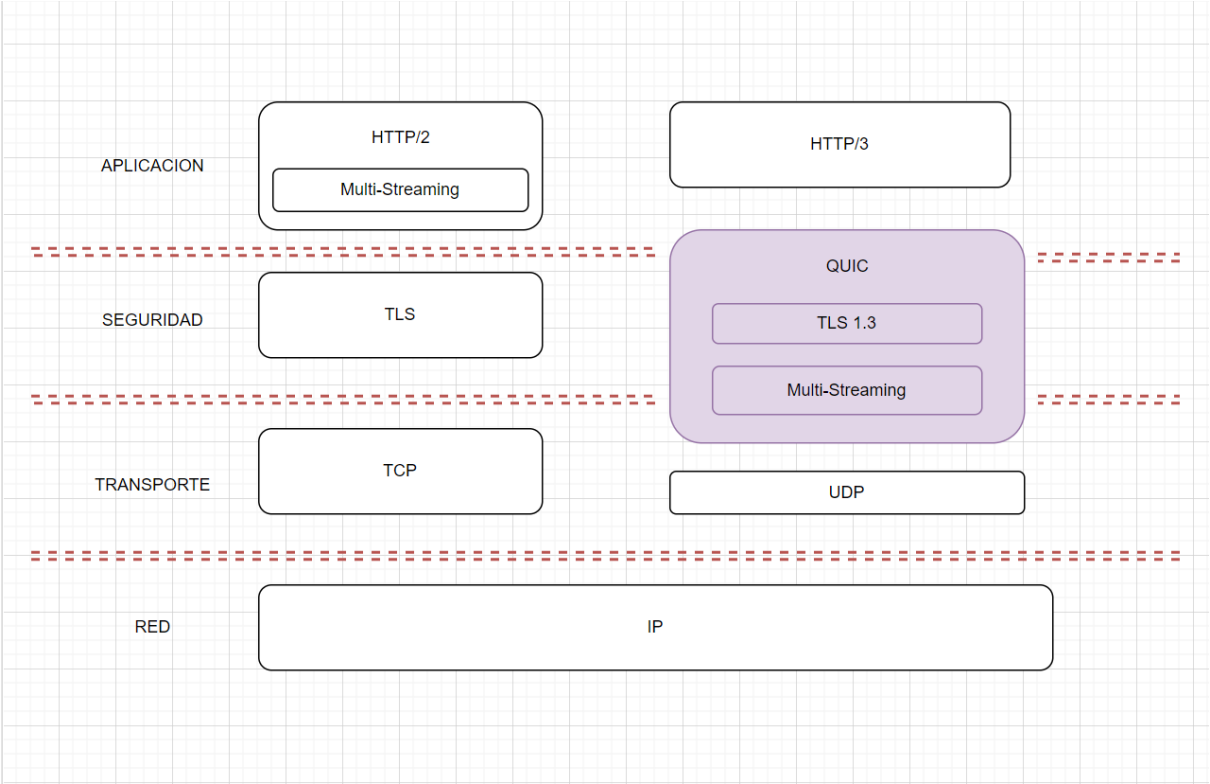


Figura 3: Arquitectura del Protocolo QUIC vs. TCP/IP

2.1.3 Seguridad

De acuerdo con Tomás Silvestre (2021):

> QUIC hace uso por defecto de la versión TLS 1.3 y por lo tanto es obligatorio con el objetivo de dificultar que dispositivos intermedios manipulen o detecten el tráfico. De este modo, no cabe la posibilidad de que haya una conexión sin cifrado. Como QUIC lleva integrado TLS, permite cifrar los mensajes sin intercambiar claves privadas entre cliente y servidor después de haber realizado el handshake de configuración inicial (p. 23).

2.1.4 Red

Según Martínez *et al*. (2005):

> Las redes en general, consisten en "*compartir recursos*", y uno de sus objetivos es hacer que todos los programas, datos y equipos estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario. Además, las diferentes topologías y los elementos que la componen. Las redes cuentan con procesos de emisión y recepción de mensajes (p. 21).

2.1.5 Multirreproducción

Cuando los mensajes de la aplicación se transportan a través de TCP pueden sufrir un bloqueo de encabezado de línea. Cuando una aplicación multiplexa muchas secuencias sobre la secuencia de prueba de un solo *byte* de TCP de abstracción, una pérdida de un segmento TCP da como resultado el bloqueo de todos los segmentos posteriores hasta que llegue una retransmisión, independientemente de los flujos de aplicaciones que se encapsulan en segmentos posteriores. QUIC asegura que los paquetes perdidos que transportan datos para un flujo individual solo impactan esa corriente específica. Los datos recibidos en otras transmisiones pueden reensamblarse y entregarse a la aplicación (Hamilton *et al*., 2016).

2.1.6 Estructura

De acuerdo con Significados.com (s. f.): "Se refiere a la disposición y distribución de las partes de un todo, cuyo orden y relación entre si permiten el funcionamiento de un determinado sistema" (s. p.).

2.1.7 Flujo de migración

El flujo se identifica generalmente por una combinación de varios factores para identificar una sola conexión. Los parámetros que intervienen en la identificación de un flujo de migración son IP de origen de dirección, dirección IP de destino, número de puerto de origen, número de puerto de destino y el protocolo (llamado 5-tupla).

2.1.8 Baja latencia

QUIC combina la negociación de versiones con el resto del establecimiento de la conexión para evitar retrasos innecesarios en los viajes de ida y vuelta. Un cliente QUIC propone una versión para usar para la conexión y codifica el resto del protocolo de enlace utilizando la versión propuesta. Si el servidor no habla la versión elegida por el cliente, fuerza la negociación de versiones y se envía un paquete de negociación de versiones al cliente, lo que provoca un retraso de ida y vuelta antes del establecimiento de la conexión (Hamilton *et al*., 2016).

2.1.9 Concurrencia

Un extremo puede limitar el número de flujos entrantes activos simultáneamente estableciendo el parámetro MSPC en los parámetros de transporte. La configuración máxima de secuencias simultáneas es específica de cada extremo y solo se aplica al par que recibe la configuración. Es decir, los clientes especifican el número máximo de secuencias simultáneas que el servidor puede iniciar y los servidores especifican el número máximo de secuencias simultáneas que el cliente puede iniciar (Hamilton *et al*., 2016).

2.2.1 Protocolo QUIC

Son conexiones rápidas a Internet UDP, un protocolo de capa de transporte que se basa en UDP.

2.2.2 Protocolo TCP

Protocolo de control de transmisión. Un protocolo de capa de transporte que se basa en el protocolo de Internet y proporciona estabilidad y fiabilidad.

2.2.3 Número de paquetes

El encabezado de cada paquete regular consta de un encabezado común seguido de campos específicos de los paquetes regulares, como se muestra a continuación:

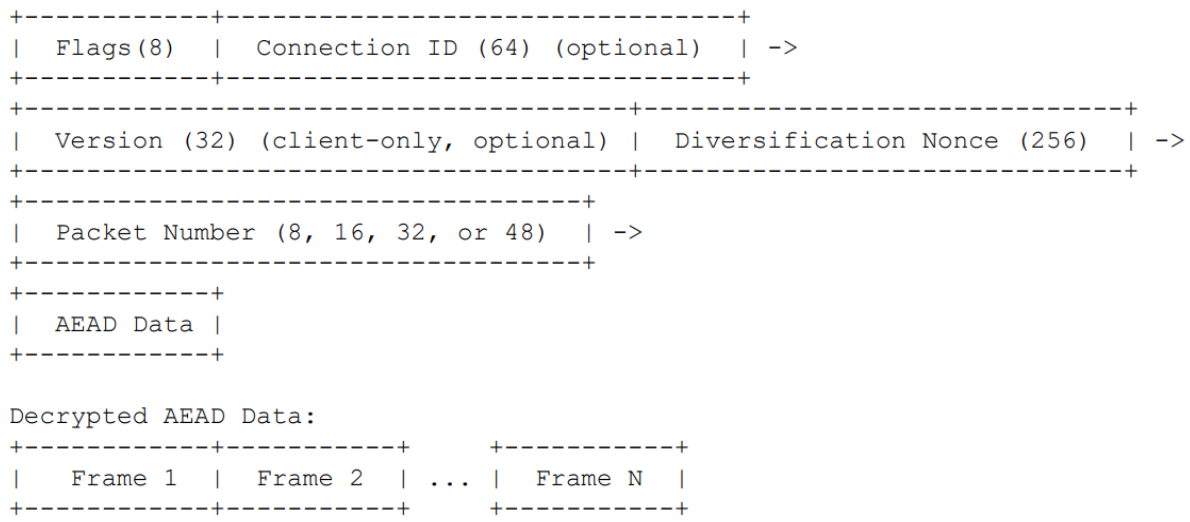


Figura 4: Multiplexación del número de paquetes

Los 8, 16, 32 o 48 *bits* inferiores del paquete número, basado en la bandera PACKET_NUMBER_SIZE, cada paquete regula, el remitente le asigna un número de paquete, el primer paquete enviado por un punto final debe tener un número de paquete de 1.

2.2.4 Congestión

El entramado y los reconocimientos de paquetes QUIC contienen información valiosa que ayuda, tanto al control de la congestión como a la recuperación de pérdidas, de manera fundamental (Hamilton *et al*., 2016).

2.2.5 Comparación de la arquitectura del protocolo QUIC vs. TCP

De acuerdo con la arquitectura del mapa conceptual Figura 3, se necesita comparar la evolución del protocolo HTTP/1.1, HTTP/2 *versus* el HTTP/3, también el TLS/1.1, TLS/1.2 *versus* el TLS/1.3. Otro aspecto importante son los multiprocesamientos y el protocolo TCP vs. QUIC.

2.2.6 HTTP/1.0

Esta versión se utilizó por casi 20 años con grandes problemas de seguridad, latencia en la red y otras vulnerabilidades a los cuales los usuarios estaban expuestos al usar Internet, hasta que en el año 1996 se dio el salto a la versión HTTP/1.1.

2.2.7 HTTP/1.1

De acuerdo con Tomás Silvestre (2021):

> Se introduce el protocolo SPDY, como un protocolo de capa de aplicación para el transporte de contenidos a través de internet, diseñado específicamente para conseguir una latencia mínima, este protocolo opera en la capa de sesión, sobre TCP, es la capa encargada de la gestión de las conexiones entre dos extremos, por lo tanto SPDY no reemplaza el protocolo HTTP, sino que lo complementa, modifica algunas funcionalidades del protocolo original y añade otras distintas que permiten mejorar las comunicaciones con la finalidad de reducir la latencia.
>
> Entre las características que incorporaba la propuesta de Google encontramos la transmisión de datos en formato binario, la introducción de flujos multiplexados, la priorización de peticiones, la compresión de las cabeceras, los

flujos iniciados por el servidor y el uso obligatorio de cifrado de datos para las comunicaciones.

Con estas nuevas funcionalidades en el protocolo SPDY, Google consiguió mejoras de hasta un 60% en los tiempos de carga de las páginas web (p. 13).

2.2.8 HTTP/2

Tomás Silvestre (2021) afirma:

Desde el año 2012 y basándose en el proyecto SPDY, el IETF (Internet Engineering Task Force) creo un equipo para el desarrollo de una nueva versión del protocolo HTTP, al que más tarde conoceríamos como HTTP/2, esta nueva versión del protocolo HTTP, se conocería luego como el HTTP/2, en donde esta nueva versión del protocolo HTTP pretendía, al igual que SPDY, mejorar las comunicaciones en Internet, logrando una reducción de latencia y mejora en la velocidad.

Entre las características que nos ofrece esta versión, nos encontramos con la transmisión binaria de los datos en lugar de la tradicional transmisión en texto plano, la compresión de la cabecera de los mensajes mediante el algoritmo "*HPACK*", la multiplexación de los datos en una sola conexión, la priorización de las solicitudes, el uso de la tecnología Server Push que permite al servidor anticiparse a las peticiones del usuario y, por último, mejoras en la seguridad con TLS (p. 14).

2.2.9 HTTP/3

La versión HTTP/3 es prácticamente la evolución de QUIC, que presenta grandes características en fiabilidad, multiplexación de flujos, identificador de conexiones,

compresión de cabecera (QPACK), priorización de flujos, servidor *push* y mayor seguridad.

2.3 TLS/1.1

El IETF hizo un esfuerzo por estandarizar el protocolo, lo que ocasionó el RFC 2246, que se publicó en enero de 1999 y se conoció como TLS 1.0. Desde entonces, el IETF ha continuado iterando en el protocolo para abordar fallas de seguridad, así como para ampliar sus capacidades: TLS 1.1 (RFC 4346) se publicó en abril de 2006, TLS 1.2 (RFC 5246) en agosto de 2008 y el trabajo está ahora en curso para definir TLS 1.3 Las principales diferencias con la versión TLS 1.0 y TLS 1.1 son:

2.3.1 Vector de inicialización

El vector de inicialización implícito (IV) se reemplaza por un IV explícito para proteger contra ataques CBC [CBCATT].

2.3.2 Errores de relleno

El manejo de errores de relleno se cambia para usar bad_record_mac alerta en lugar de la alerta decryption_failed para protegerse contra ataques CBC. Los registros de IANA se definen para parámetros de protocolo, los cierres prematuros ya no hacen que una sesión no sea reanudable y se agregaron notas informativas adicionales para varios ataques nuevos en TLS.

2.4 TLS/1.2

Principales diferencias entre el TLS 1.2 y el TLS 1.3:

2.4.1 Algoritmo de cifrado simétrico

La lista de algoritmos de cifrado simétrico compatibles se ha podado de todos los algoritmos que se consideran heredados. Los que permanecen son todos cifrados autenticados con datos asociados (AEAD) algoritmos. El concepto de conjunto de cifrado se cambió a separar los mecanismos de autenticación e intercambio de claves de los algoritmos de protección de registros (incluida la longitud de la clave secreta) y un *hash* que se utiliza con la función de derivación de claves y código de autenticación de mensajes de protocolo de enlace (MAC).

2.4.2 (0-RTT)

Se agregó un modo de tiempo de ida y vuelta cero (0-RTT). Esto ahorra un viaje de ida y vuelta al configurar la conexión para algunos datos de la aplicación, a costa de ciertas propiedades de seguridad.

2.4.3 Cifrado RSA estático y Diffie-Hellman

Se eliminaron los conjuntos de cifrado RSA estático y Diffie-Hellman. Todos los mecanismos de intercambio de claves con base en claves públicas ahora proporcionan secreto.

2.4.4 Protocolos de enlace

Todos los mensajes de protocolo de enlace posteriores al ServerHello ahora están encriptados. El mensaje EncryptedExtensions introducido recientemente permite varias extensiones enviadas en claro en el servidor Hello para que use la protección de la confidencialidad.

2.4.5 Funciones de derivación de clave

Se han rediseñado las funciones de derivación de claves. El nuevo diseño permite un análisis más fácil por parte de los criptógrafos debido a su clave, mejorada las

propiedades de separación. La clave de extracción y expansión basada en HMAC la función de derivación (HKDF) se utiliza como primitiva subyacente.

2.4.6 Maquina de estado

La máquina de estado de protocolo de enlace se ha reestructurado significativamente para ser más coherente y eliminar mensajes superfluos como ChangeCipherSpec (excepto cuando sea necesario para compatibilidad con middlebox).

2.4.7 Algoritmo de curva elíptica

Los algoritmos de curva elíptica están ahora en la especificación base y los nuevos incluyen algoritmos de firma, como EdDSA. En TLS 1.3 se eliminó la negociación del formato de puntos a favor de un formato de un solo punto para cada curva.

2.4.8 Mejoras criptográficas

Se realizaron otras mejoras criptográficas, incluido el cambio de relleno RSA para utilizar el esquema de firma probabilística RSA (RSASSA-PSS) y la eliminación de la compresión, el digital algoritmo de firma (DSA) y Diffie-Hellman efímero personalizado (DHE) de grupos.

2.5 Mecanismo de negociación

El mecanismo de negociación de la versión TLS 1.2 quedó obsoleto en favor de una lista de versiones en una extensión. Esto aumenta compatibilidad con servidores existentes que implementaron incorrectamente la negociación de versiones.

2.5.1 Reanudación de la sesión

Reanudación de la sesión con y sin estado del lado del servidor, así como los conjuntos de cifrado con base en PSK de versiones anteriores de TLS se reemplazaron por un único intercambio PSK nuevo.

2.5.2 TLS/1.3

De acuerdo con Tomás Silvestre (2021):

> TLS 1.3 es la nueva versión del protocolo y fue aprobada en 2018 por la IETF, uno de los objetivos de TLS 1.3 es reducir la latencia durante el establecimiento de la conexión. Esta versión introduce dos avances significativos en este aspecto, los modos de conexión con 1-RTT y 0-RTT, el proceso para establecer la conexión con el modo 1-RTT sigue la misma filosofía que las versiones anteriores, pero reorganiza el contenido de los mensajes para reducir el tiempo de ida y vuelta (p. 30).

Capítulo 3. Marco metodológico

3.1 Tipo de investigación

El mejor tipo de investigación que es posible utilizar es el evaluativo debido a que se hace una comparación tecnológica entre protocolos de red y cómo han evolucionado en el tiempo. Las principales comparaciones por efectuar son con protocolos como el TLS, el HTTP y entender cómo el nuevo protocolo QUIC es mejor que el TCP para la comunicación de Internet y cómo se van a mejorar los problemas de latencia cliente *versus* servidor y que, al mismo tiempo, se puede trasladar en otro tipo de redes para agilizar los paquetes de información como redes en robótica, inteligencia artificial y redes Scada.

Con todos los datos que se obtienen es posible construir mejores gráficos, tablas y hacer pruebas que ayuden a comprender mejor el tipo de investigación que se desarrolla. Con esto es posible cumplir el objetivo general y los específicos para definir si la propuesta es viable para aplicarse en las empresas costarricenses.

3.2 Alcance investigativo

De acuerdo con la investigación evaluativa, se considera el siguiente tipo de alcance investigativo.

3.2.1 Descriptivo

Se utiliza un alcance descriptivo debido a que se tienen situaciones en diferentes contextos. El que más interesa es entender cómo el protocolo QUIC se puede adaptar en las empresas costarricenses, qué tipo de características se tiene aquí con respecto al protocolo QUIC y entender en forma comparativa la arquitectura de este protocolo *versus* el protocolo tradicional más usado en las redes actuales que es el TCP.

También al analizar el perfil de las empresas es posible comprender si los otros protocolos TLS y HTTP se pueden adaptar al uso de QUIC en forma rápida y eficiente. Además, al recolectar la cantidad de datos necesarios es posible observar cómo la latencia mejora cuando muchos clientes requieren una gran cantidad de solicitudes de diferentes servicios a través de las redes y cómo el servidor o servidores de red responden a estas solicitudes.

3.3 Enfoque

El tipo de enfoque para seguir por el tipo de investigación es cuantitativo, para generar resultados nomotéticos. Lo que se pretende es realizar una deducción de datos de los protocolos QUIC y TCP, ver resultados comparativos y comprobar la

mejor opción por utilizarse. También el enfoque se puede mezclar con cualitativo y convertirse en un enfoque mixto o alternativo.

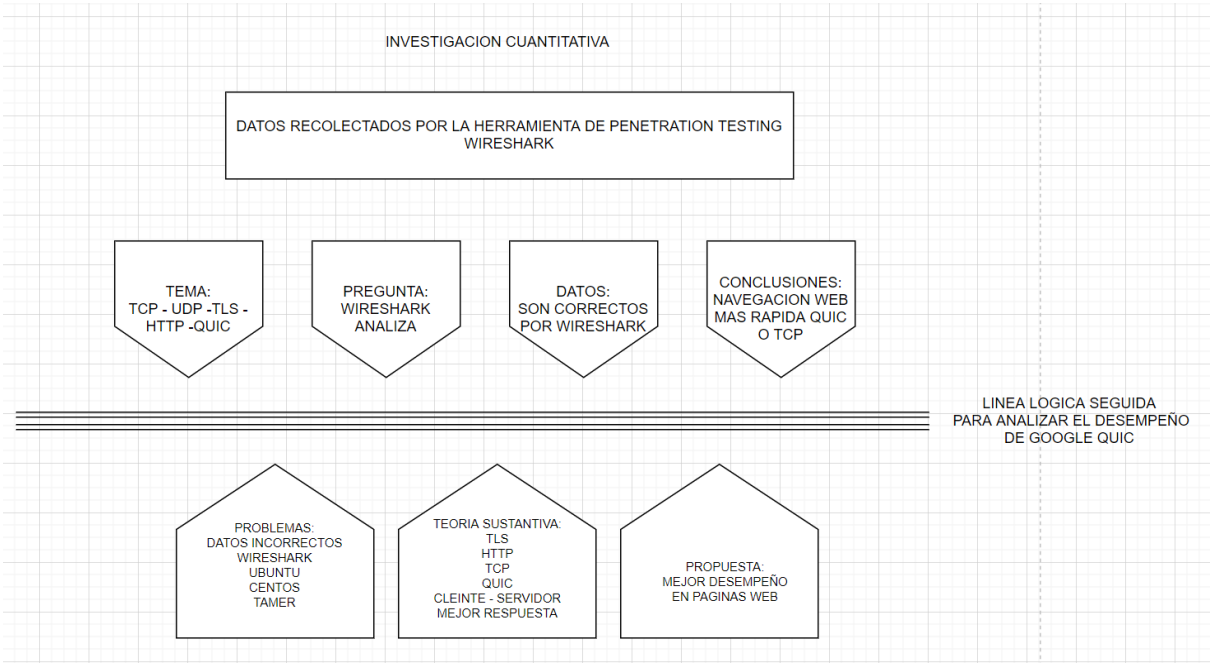


Figura 5: Ontología del conjunto de datos

3.4 Diseño

El diseño más adecuado con relación al enfoque seleccionado y los objetivos es el cuantitativo, porque se tienen muchas variables que se relacionan, las cuales están expresas en los mismos protocolos de red por compararse. Es posible entender el diseño cuantitativo mediante los siguientes pasos en relación con la arquitectura del protocolo QUIC:

- Tener claro cómo actúan las capas del modelo OSI, red, transporte, seguridad y aplicación.
- Cómo trabajan los multiprocesos en ambos protocolos QUIC y TCP.
- Cómo se ha dado la evolución de los protocolos TLS y HTTP.
- Hacer una interpretación de datos cuantitativos en relación con el alcance y el enfoque de la investigación.
- Realizar análisis final y conclusiones.

3.5 Población y muestreo

Existen dos tipos de población. La primera es la que se efectúa mediante una encuesta que permite obtener el grado de conocimiento de Google QUIC que consiste en 7 preguntas relacionadas con el entendimiento de este protocolo, qué problemas de lentitud o de latencia presenta la empresa al navegar en Internet, si se han reconocido los protocolos de comunicación en la red de la compañía y de acuerdo con los usuarios cuáles son los navegadores web preferidos durante las actividades diarias de trabajo.

Además, en relación con el grado de madurez de la empresa, determinar si esta adoptaría el Cloud de Google para la implementación correcta del Google QUIC. El tipo de muestreo hará una combinación de probabilístico y no probabilístico, debido a que se depende de respuestas de los usuarios en donde la tendencia en las respuestas está sujeta a una probabilidad de los eventos mencionados en la población anterior.

La segunda población es la que se utiliza en este caso. Esta población se concentra en servidores con una función cliente servidor, en donde se enviará información en forma de paquetes, transferidos de un equipo a otro y observando la eficiencia de transmisión de información y el tiempo en su respuesta. El tipo de muestreo hará una combinación de probabilístico y no probabilístico, debido a que es posible crear eventos en los que la comunicación de red está estable y en otras circunstancias es posible tener pérdida de información. De esta forma, se entiende mejor el comportamiento de los equipos en los centros de datos.

Se utiliza la siguiente calculadora con un tamaño de muestra de 100 servidores ubicados en un centro de datos virtual. Al determinar un margen de error

del 5 % y un nivel de confianza del 99 % es posible lograr un tamaño de muestra del 87 %.

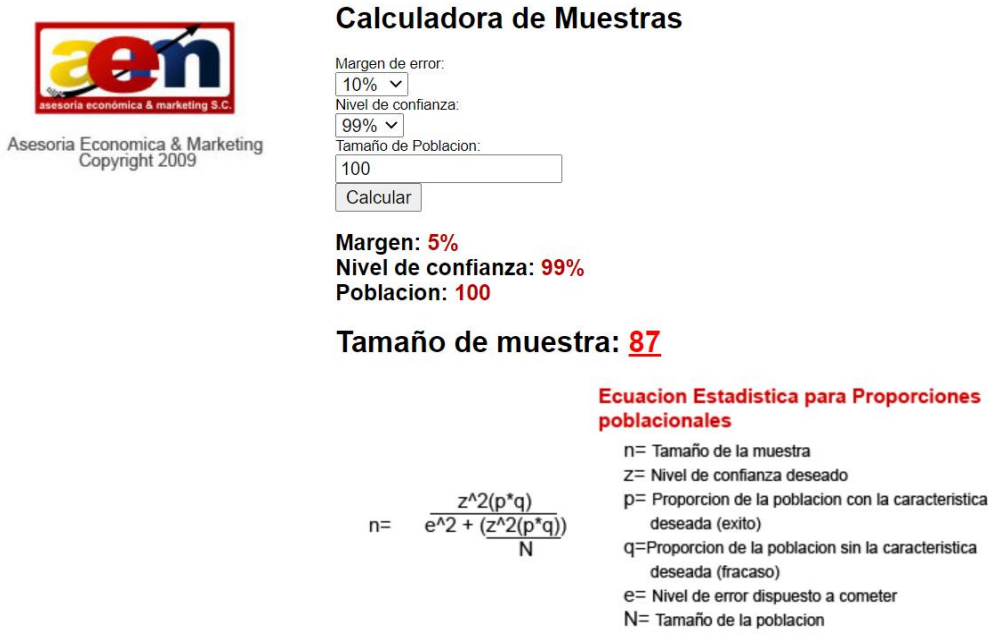


Figura 6: Población y muestreo para el análisis del Google QUIC y del TCP.

3.6 Instrumentos de recolección de datos

Para la recolección de datos se utiliza una encuesta en la que se presenta la forma básica y esencial sobre cómo opera el Google QUIC, para hacer entender al usuario final el problema de latencia en las redes y cómo la infraestructura en negocios críticos puede evolucionar, dando al cliente final un mejor servicio. También se utilizan herramientas como Wireshark, Ubuntu, CentOS y Android Tamer, Microsoft Edge, Google Chrome, Opera, para recolectar datos con los protocolos QUIC, TCP, UDP, TLS, HTTP y ver el comportamiento cliente-servidor y las respuestas en eficiencia con estos protocolos de red.

La técnica de recolección de datos se basa en el análisis documental utilizando la encuesta para lograr estos objetivos:

- Mediante las preguntas de la encuesta se tiene un panorama positivo, negativo o ambiguo sobre el conocimiento de Google QUIC.
- Diferenciar Google QUIC de TCP/IP y el problema que hay en las redes.
- Se desarrolla una buena estrategia por medio de la encuesta para crear mejores datos, hacer pruebas de mejor nivel y dar mejor entrenamiento al usuario final.

Encuesta Google Quic 2

1. ¿Conoce usted lo que es Google Quic?

    a. Usted entiende que Google Quic mejora el audio y video en las páginas web.
    b. Usted entiende que Google Quic mejora la comunicación cliente servidor en su centro de datos, en las empresas en Costa Rica.
    c. Usted comprende la autenticación de certificados y claves que se realizan en una red de infraestructura, en una empresa en Costa Rica.
    d. Le gustaría entender más la forma en que trabaja Google Quic, en centro de datos costarricense.
    e. Entiende las diferencias entre TCP/IP y Google Quic.
    f. Usaría más tecnología de Google en su centro de datos, para las empresas en Costa Rica.

2. ¿Tiene usted en su empresa problemas de lentitud en su navegación en internet?

    a. En muy lento, dependiendo de la ubicación en San Jose Costa Rica, o varía de acuerdo con la provincia, en la que usted está ubicado.
    b. El Internet se desconecta con frecuencia, la ubicación geográfica no favorece la buena conectividad de las empresas suplidoras de internet en Costa Rica.
    c. No tengo problemas, porque vino en el GAM y se me hace fácil usar servicios de mejor calidad suministrado por las compañías en Costa Rica.
    d. Los problemas de lentitud que usted observa los puede relacionar con latencia generado por un mal diseño en la red, suministrado por alguna empresa en Costa Rica de baja calidad, sabe cómo detectar eso.

3. ¿Sabe usted que protocolos de comunicación usan en la red de su empresa?

    a. TCP, es un protocolo que se mueven en las infraestructuras de las empresas en Costa Rica desde los años 70.
    b. QUIC, es un protocolo que se desarrolló por Google desde el año 2009, y aún está en evolución.
    c. UDP, es un protocolo rápido, pero no seguro, que Google Quic vino a perfeccionar.
    d. HTTP, es un protocolo de navegación web muy usado por las empresas de internet en Costa Rica y a nivel mundial para navegar en forma segura o no.
    e. TLS, es un protocolo que encripta la información de los centros de datos en Costa Rica y trabaja en conjunto con HTTP y HTTPS.

4. ¿Cuál es el navegador web que utilizan por defecto en su Empresa?

    a. Microsoft Edge, no trabaja con Google Quic como motor de búsqueda.
    b. OPERA, trabaja con Google Quic como motor de búsqueda.
    c. Google Chrome, tiene ya integrado el Google Quic como motor de búsqueda.
    d. Firefox, trabaja con Google Quic como motor de búsqueda.

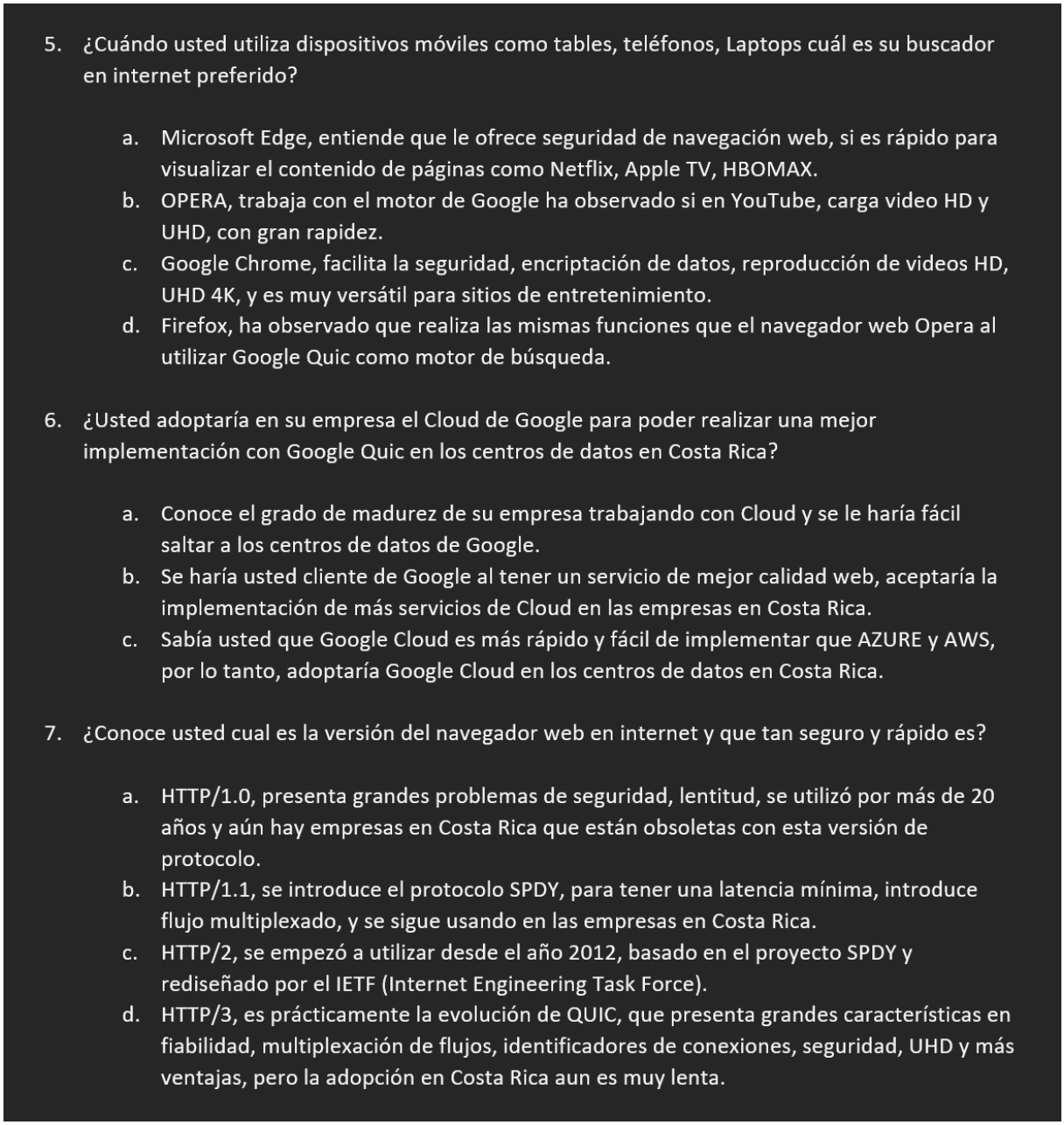
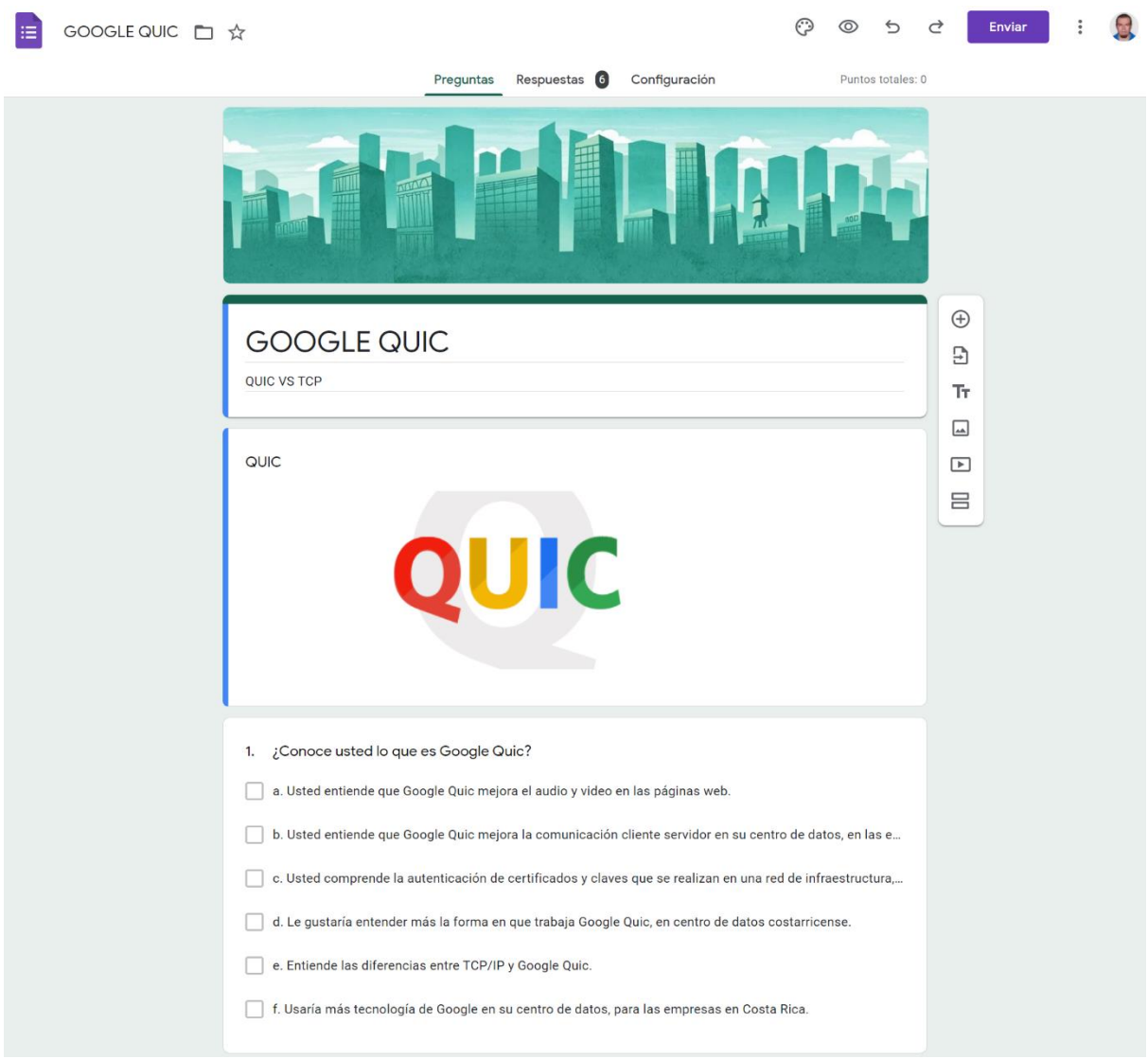


Figura 7: Encuesta para reflejar el conocimiento sobre Google QUIC.

3.6.1 Encuesta

Mediante los formularios de Google es posible crear una encuesta que se puede compartir en diferentes redes sociales y obtener respuestas más correctas y rápidas para hacer un mejor análisis de datos sobre el Google QUIC.


GOOGLE QUIC
Enviar
Preguntas
Respuestas 6
Configuración
Puntos totales: 0
GOOGLE QUIC
QUIC VS TCP
QUIC
QUIC
1. ¿Conoce usted lo que es Google Quic?
a. Usted entiende que Google Quic mejora el audio y video en las páginas web.
b. Usted entiende que Google Quic mejora la comunicación cliente servidor en su centro de datos, en las e...
c. Usted comprende la autenticación de certificados y claves que se realizan en una red de infraestructura,...
d. Le gustaría entender más la forma en que trabaja Google Quic, en centro de datos costarricense.
e. Entiende las diferencias entre TCP/IP y Google Quic.
f. Usaría más tecnología de Google en su centro de datos, para las empresas en Costa Rica.

2. ¿Tiene usted en su empresa problemas de lentitud en su navegación en internet?

- [ ] a. En muy lento, dependiendo de la ubicación en San Jose Costa Rica, o varía de acuerdo con la provincia, ...
- [ ] b. El Internet se desconecta con frecuencia, la ubicación geográfica no favorece la buena conectividad de ...
- [ ] c. No tengo problemas, porque vino en el GAM y se me hace fácil usar servicios de mejor calidad suminist...
- [ ] d. Los problemas de lentitud que usted observa los puede relacionar con latencia generado por un mal dis...

3. ¿Sabe usted que protocolos de comunicación usan en la red de su empresa?

- [ ] a. TCP, es un protocolo que se mueven en las infraestructuras de las empresas en Costa Rica desde los añ...
- [ ] b. QUIC, es un protocolo que se desarrolló por Google desde el año 2009, y aún está en evolución.
- [ ] c. UDP, es un protocolo rápido, pero no seguro, que Google Quic vino a perfeccionar.
- [ ] d. HTTP, es un protocolo de navegación web muy usado por las empresas de internet en Costa Rica y a niv...
- [ ] e. TLS, es un protocolo que encripta la información de los centros de datos en Costa Rica y trabaja en conj...

4. ¿Cuál es el navegador web que utilizan por defecto en su Empresa?

- [ ] a. Microsoft Edge, no trabaja con Google Quic como motor de búsqueda.
- [ ] b. OPERA, trabaja con Google Quic como motor de búsqueda.
- [ ] c. Google Chrome, tiene ya integrado el Google Quic como motor de búsqueda.
- [ ] d. Firefox, trabaja con Google Quic como motor de búsqueda.

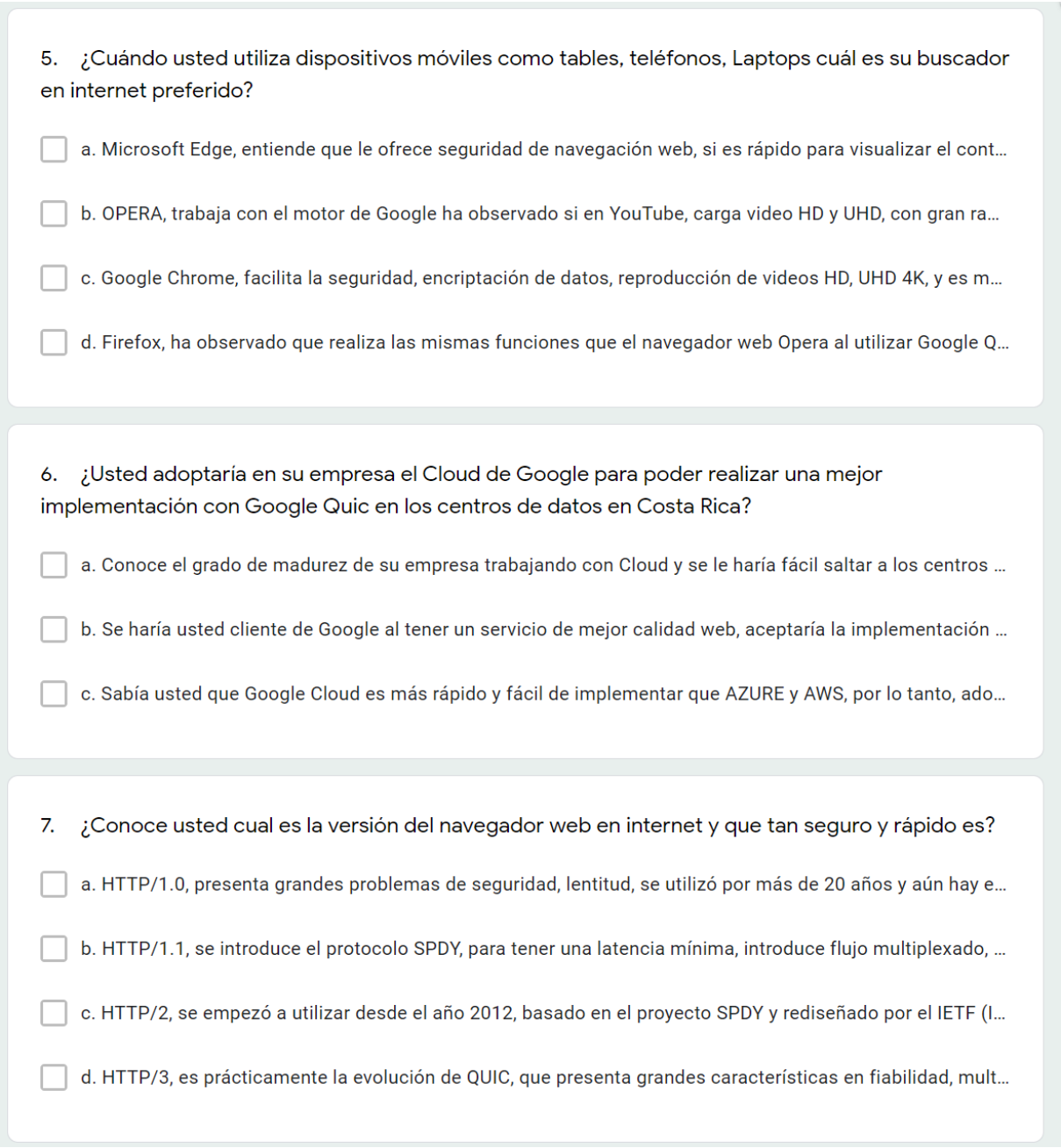


Figura 8: Encuesta para reflejar el conocimiento sobre Google QUIC, utilizando los formularios de Google

3.6.2 Wireshark

En este apartado se mencionan las herramientas de recolección de datos. Con Wireshark se captura todo el tráfico presente en la red, desde su fuente, destino, protocolo, longitud e información y el tráfico de información de Google QUIC.

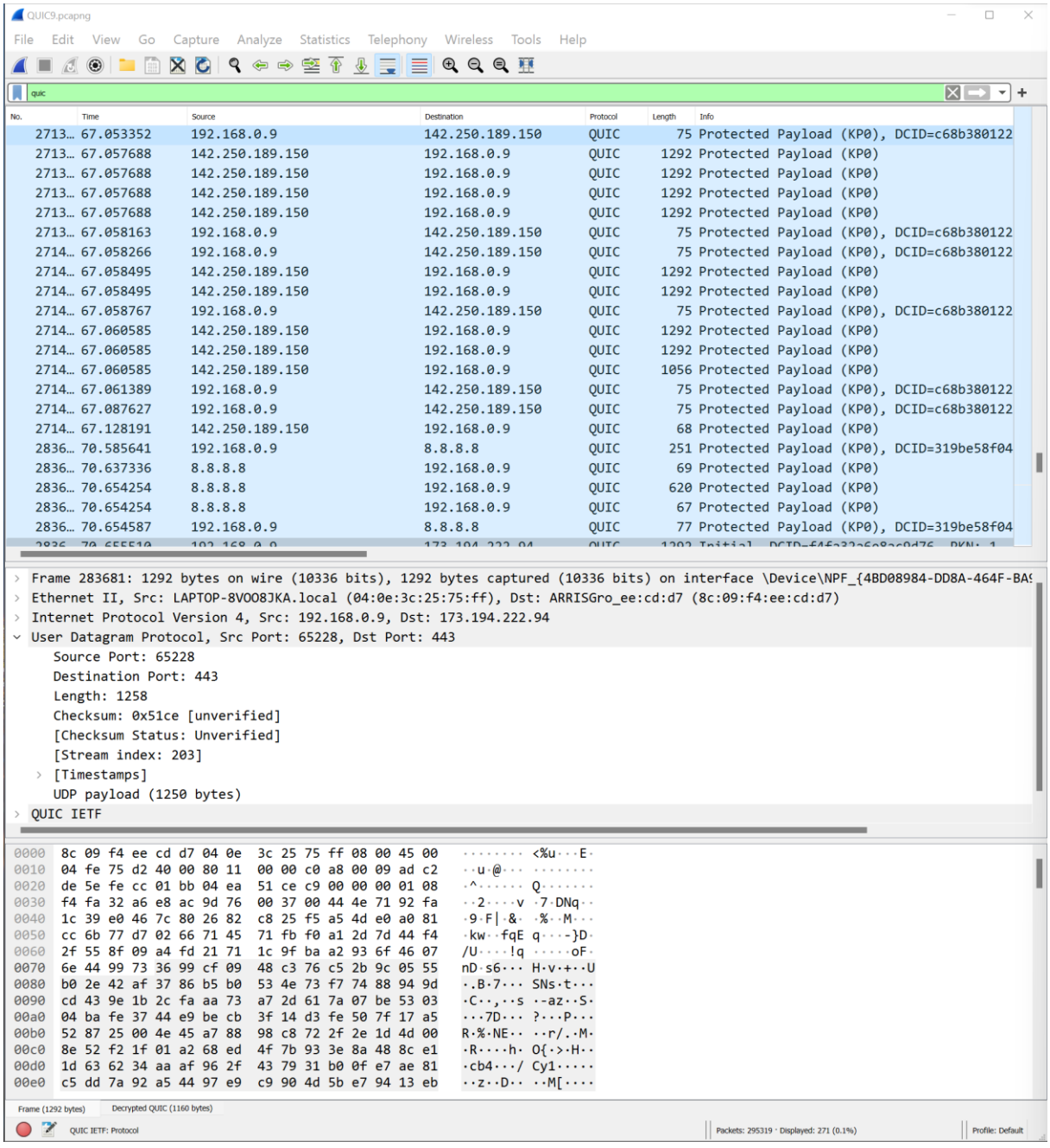


Figura 9: Wireshark capturando Google QUIC

Por medio del VirtualBox y la máquina virtual de Ubuntu es posible generar tráfico de información al utilizar Firefox, navegar en YouTube y mediante *pings* de

comunicación con la máquina virtual de CentOS 8. Lo anterior para que la herramienta de Wireshark tenga el tráfico adecuado y se puedan ver los protocolos esenciales.

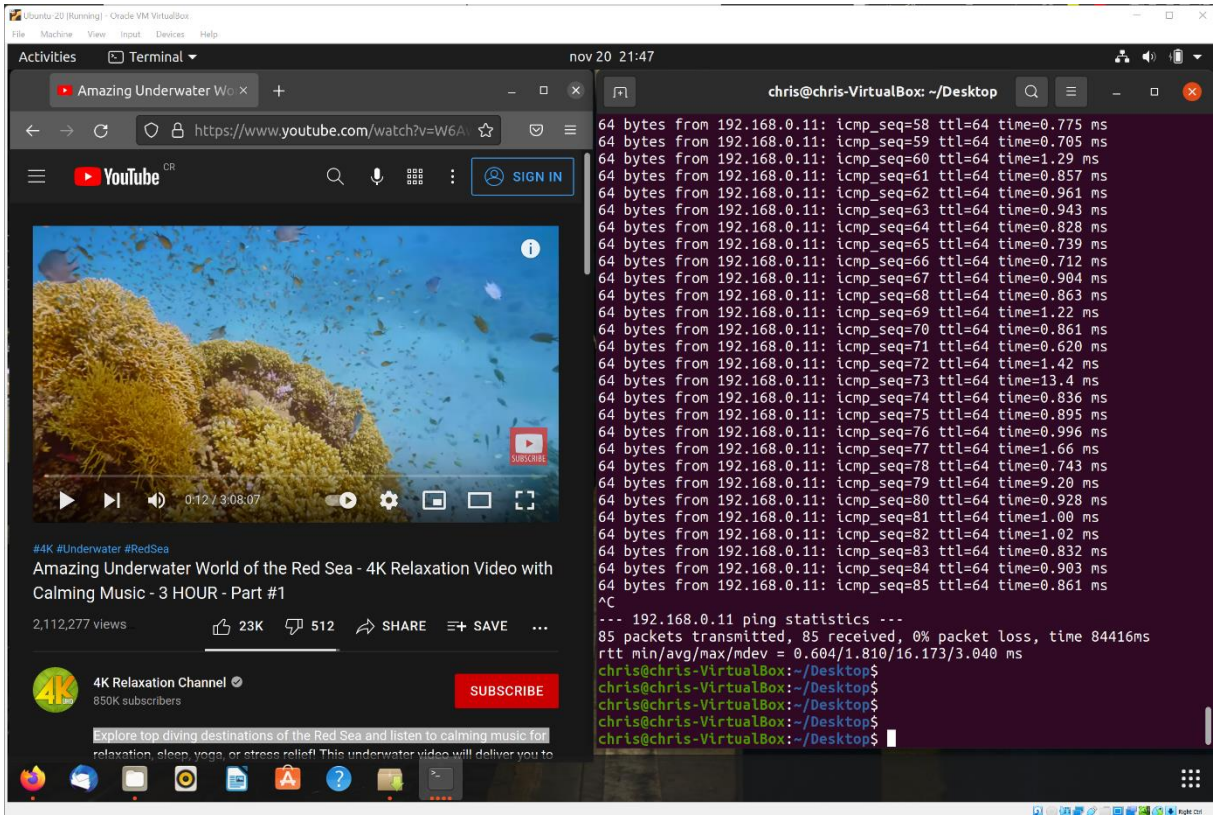


Figura 10: Utilizando el Ubuntu 20.04, enviamos los datos a ser requeridos por Wireshark

Utilizando el sitio web w3Techs es posible generar comparaciones entre protocolos de diferentes tecnologías y el uso que se le da para entender la evolución de Google QUIC en el tiempo.

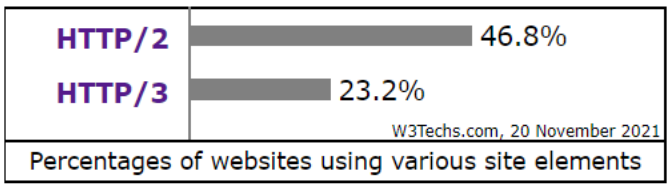


Figura 11: Comparación estadística de HTTP/2 vs. HTTP3 para los diferentes sitios web y la tecnología que más se utiliza

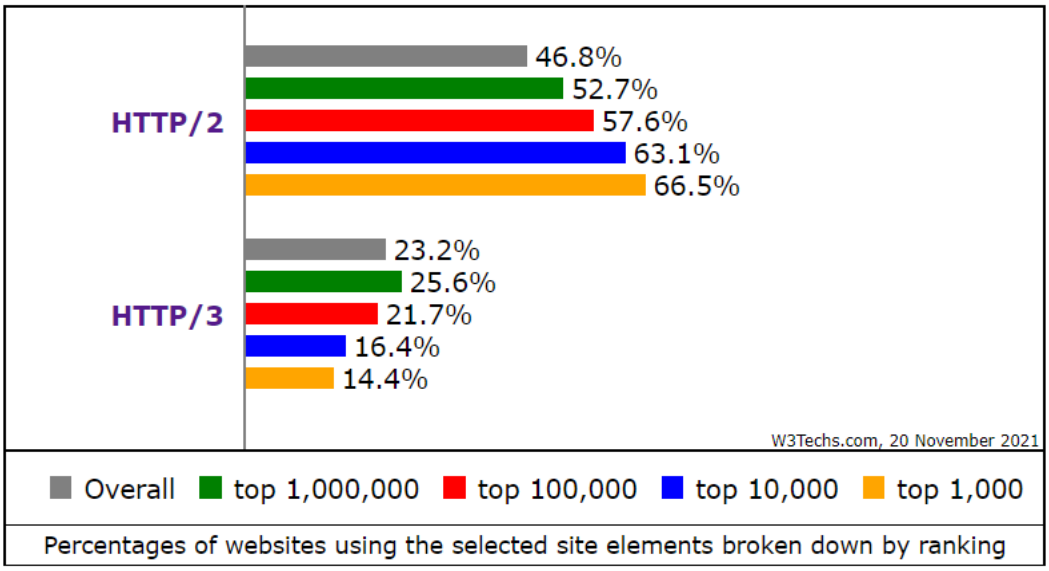


Figura 12: Porcentaje de utilización de las diferentes tecnologías, el ranqueo con una muestra de 1 millón de sitios web y cómo evoluciona el Google QUIC

	2020 1 Nov	2020 1 Dec	2021 1 Jan	2021 1 Feb	2021 1 Mar	2021 1 Apr	2021 1 May	2021 1 Jun	2021 1 Jul	2021 1 Aug	2021 1 Sep	2021 1 Oct	2021 1 Nov	2021 21 Nov
None	1.7%	1.7%	1.6%	1.6%	1.5%	1.4%	1.4%	1.4%	1.3%	1.2%	1.1%	1.1%	1.3%	1.3%
CSS	95.8%	95.9%	96.1%	96.2%	96.3%	96.3%	96.3%	96.0%	96.4%	96.4%	96.7%	96.7%	96.2%	96.3%
Compression	83.2%	82.9%	83.0%	84.2%	84.8%	85.2%	85.5%	86.0%	86.3%	86.5%	86.9%	87.1%	86.9%	87.0%
Default protocol https	66.9%	67.9%	68.8%	69.6%	70.6%	71.5%	72.2%	72.7%	73.6%	74.3%	75.1%	75.7%	76.4%	76.9%
HTTP/2	49.0%	49.4%	49.9%	50.2%	50.2%	50.6%	49.6%	45.4%	45.7%	45.9%	46.2%	46.5%	46.8%	46.8%
Default subdomain www	39.1%	39.1%	38.9%	38.8%	38.8%	38.7%	38.6%	38.5%	38.5%	38.5%	38.5%	38.3%	38.4%	38.3%
Cookies	44.5%	44.7%	44.9%	45.1%	45.4%	45.6%	46.0%	43.6%	41.7%	41.9%	42.1%	41.6%	36.9%	37.0%
HTTP/3	6.8%	3.9%	4.1%	4.2%	8.8%	14.5%	19.1%	19.5%	20.0%	20.5%	21.3%	21.9%	22.4%	23.2%
HTTP Strict Transport Security	15.6%	15.9%	16.9%	18.2%	18.6%	18.9%	19.3%	19.7%	20.2%	20.5%	20.9%	21.4%	21.9%	22.2%
IPv6	17.1%	17.2%	17.5%	17.8%	18.2%	18.4%	18.6%	18.7%	19.0%	19.2%	19.4%	19.6%	19.8%	20.2%
ETag	14.6%	14.6%	14.4%	14.5%	14.6%	14.7%	14.7%	14.7%	15.0%	15.2%	15.8%	16.0%	15.9%	16.1%
QUIC	4.9%	5.0%	5.1%	5.1%	5.0%	5.0%	5.1%	5.4%	5.6%	5.7%	5.9%	6.0%	6.1%	6.7%
Frameset	0.3%	0.3%	0.3%	0.3%	0.3%	0.3%	0.3%	0.3%	0.3%	0.3%	0.3%	0.3%	0.2%	0.2%
SPDY	0.1%	0.1%	0.1%	0.1%	0.1%	0.1%	0.1%	0.1%	0.1%	0.1%	0.1%	0.1%	0.1%	0.1%

Figura 13: Tendencia histórica del uso estadístico de los diferentes protocolos que corren en los sitios web

3.7 Técnicas de análisis de información

Para las técnicas de análisis de información se usa como primer punto de análisis los diagramas de flujo. Este tipo de algoritmo se utiliza para representar el comportamiento de las personas con respuesta a su conocimiento relacionado con Google QUIC mediante la encuesta aplicada. También se realiza otro diagrama de

flujo para las pruebas de penetración hechas con Wireshark, para comprender el desempeño en los diferentes navegadores *web* que se utilizan.

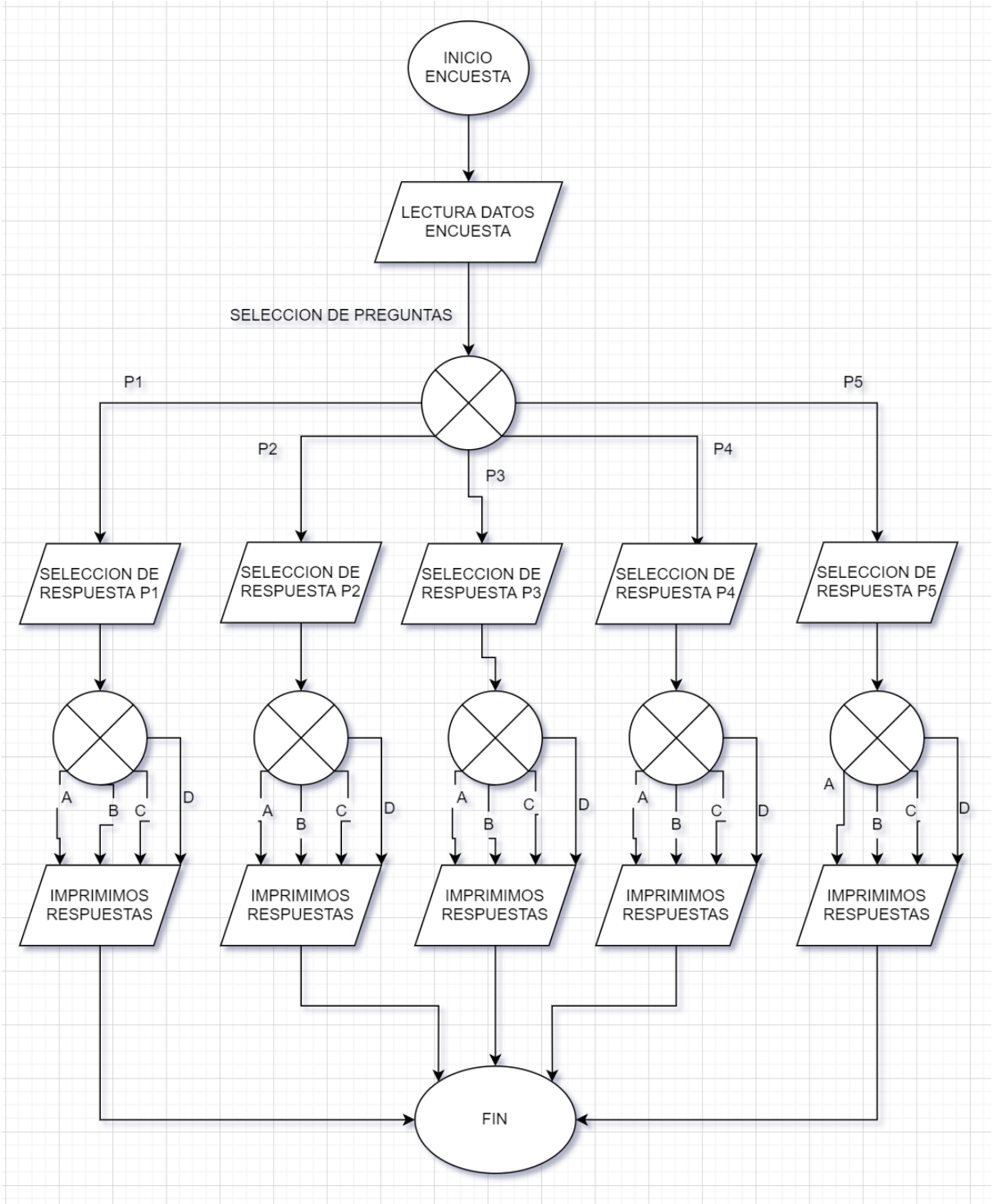


Figura 14: Diagrama de flujo para la recolección de datos en la encuesta

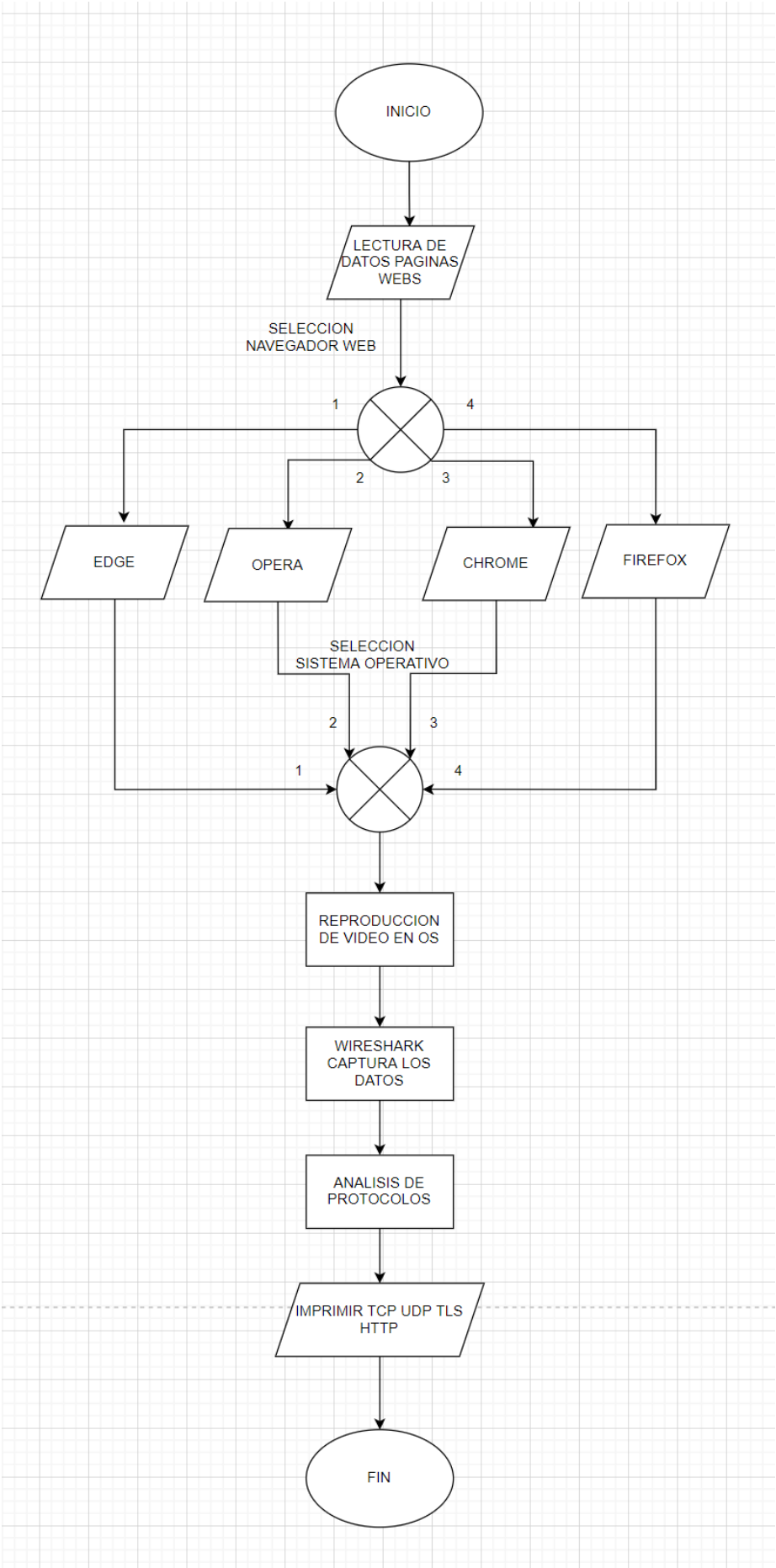

INICIO
LECTURA DE DATOS PAGINAS WEBS
SELECCION NAVEGADOR WEB
1
2
3
4
EDGE
OPERA
CHROME
FIREFOX
SELECCION SISTEMA OPERATIVO
2
3
1
4
REPRODUCCION DE VIDEO EN OS
WIRESHARK CAPTURA LOS DATOS
ANALISIS DE PROTOCOLOS
IMPRIMIR TCP UDP TLS HTTP
FIN

Figura 15: Diagrama de flujo para la recolección de datos con pruebas de penetración Wireshark

3.8 Estrategia de desarrollo de la propuesta

Para el análisis de datos se utilizan otras herramientas alternativas. Además, las herramientas opcionales son las disponibles en Kali Linux o Android Tamer.

Asimismo, se pueden utilizar más herramientas de pruebas de penetración o si no utilizar las más convenientes como recolección de datos, análisis de vulnerabilidades, análisis de aplicación web, ingeniería inversa, *sniffing* y *spoofing*, análisis forense, herramientas de reporte, herramientas de ingeniería social. Con esto se puede hacer el mejor análisis para entender el comportamiento del Google QUIC e implementar su viabilidad en las empresas en Costa Rica.

Capítulo 4. Análisis del diagnóstico

4.1 Aplicación de la encuesta y aplicación con el Wireshark

En cuanto a los datos que se recopilaron en la sección 3.6 y la sección 3.7, se tiene la información necesaria para deducir si el Google QUIC es un protocolo que pueden adoptar las empresas en Costa Rica y determinar si la implementación es realizable a un mediano plazo.

4.1.1 Aplicación de la encuesta

Aplicación de la encuesta en redes sociales como Facebook, Slack, WhatsApp, Discord, Telegram.

Utilizando el canal de comunicación de estas redes sociales es posible llegar a una gran cantidad de usuarios y obtener resultados muy interesantes y variados

sobre la implementación o viabilidad del Google QUIC en las empresas costarricenses.

4.1.2 Aplicación de la encuesta en redes sociales como WhatsApp

Mediante este otro medio de comunicación es posible crear más fuentes de información e interactuar con otros grupos universitarios u otros grupos de tecnología.

4.1.3 Aplicación de la encuesta en redes sociales como Slack

Con esta herramienta de comunicación empresarial es posible llegar a grupos de 100, 200 y hasta 600 personas que pueden dar una gran cantidad de entradas para crear un análisis más completo sobre la viabilidad del Google QUIC en las infraestructuras de centros de datos en Costa Rica.

4.1.4 Uso del Wireshark

Aplicación del uso del Wireshark en los diferentes navegadores web para comparar el flujo del Google QUIC.

4.2 Comparación de resultados

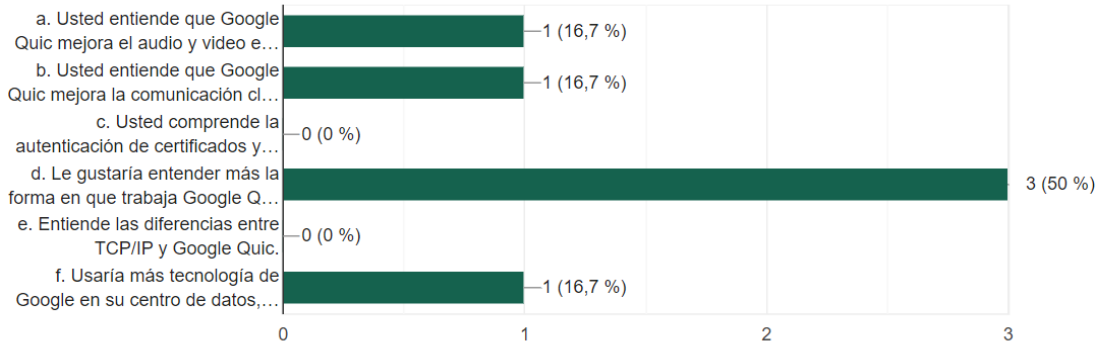
Comparación de los diferentes resultados que se encontraron en los canales de comunicación como Facebook, WhatsApp, Slack.

4.2.1 Primer bloque de respuestas

Primer bloque de respuestas de la encuesta, enviadas a las diferentes redes sociales.

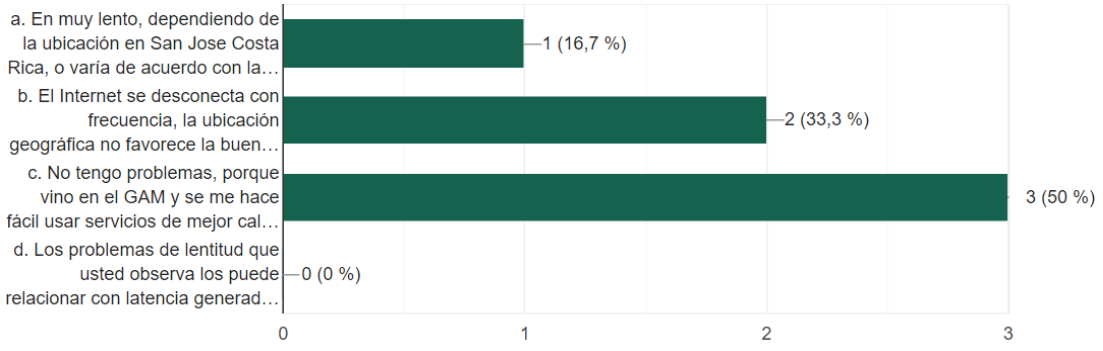
1. ¿Conoce usted lo que es Google Quic?

6 respuestas



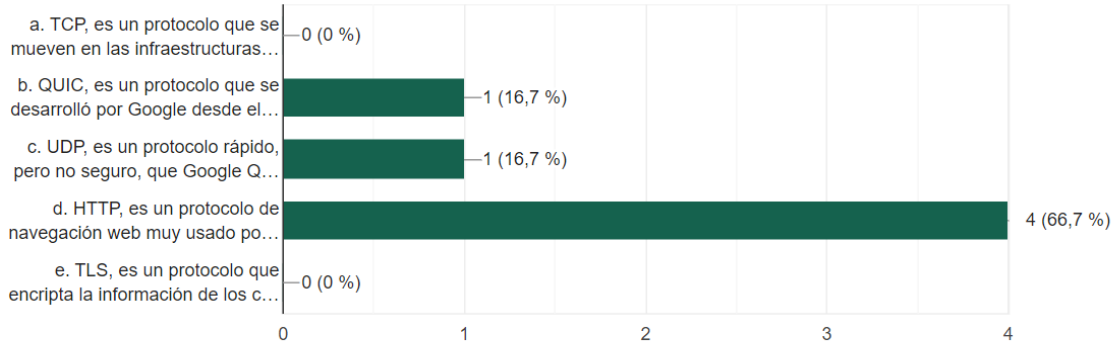
2. ¿Tiene usted en su empresa problemas de lentitud en su navegación en internet?

6 respuestas



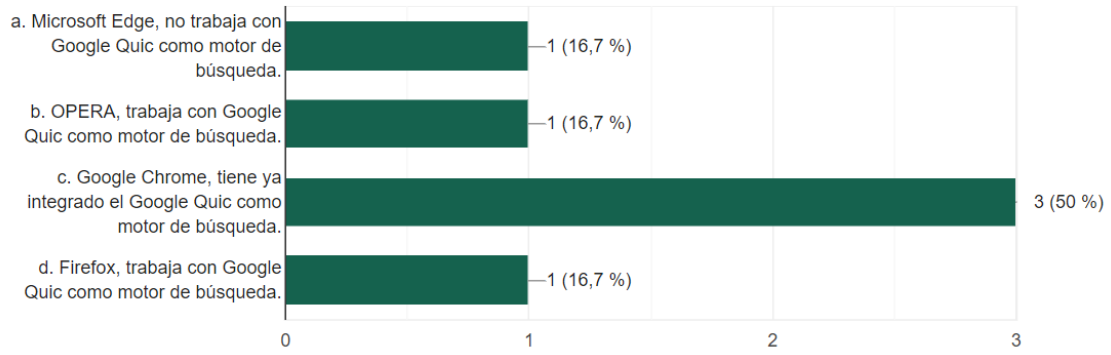
3. ¿Sabe usted que protocolos de comunicación usan en la red de su empresa?

6 respuestas



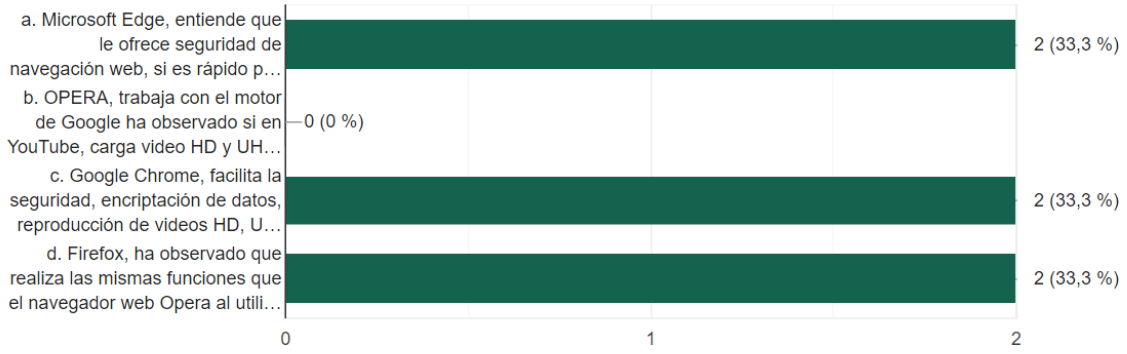
4. ¿Cuál es el navegador web que utilizan por defecto en su Empresa?

6 respuestas



5. ¿Cuándo usted utiliza dispositivos móviles como tables, teléfonos, Laptops cuál es su buscador en internet preferido?

6 respuestas



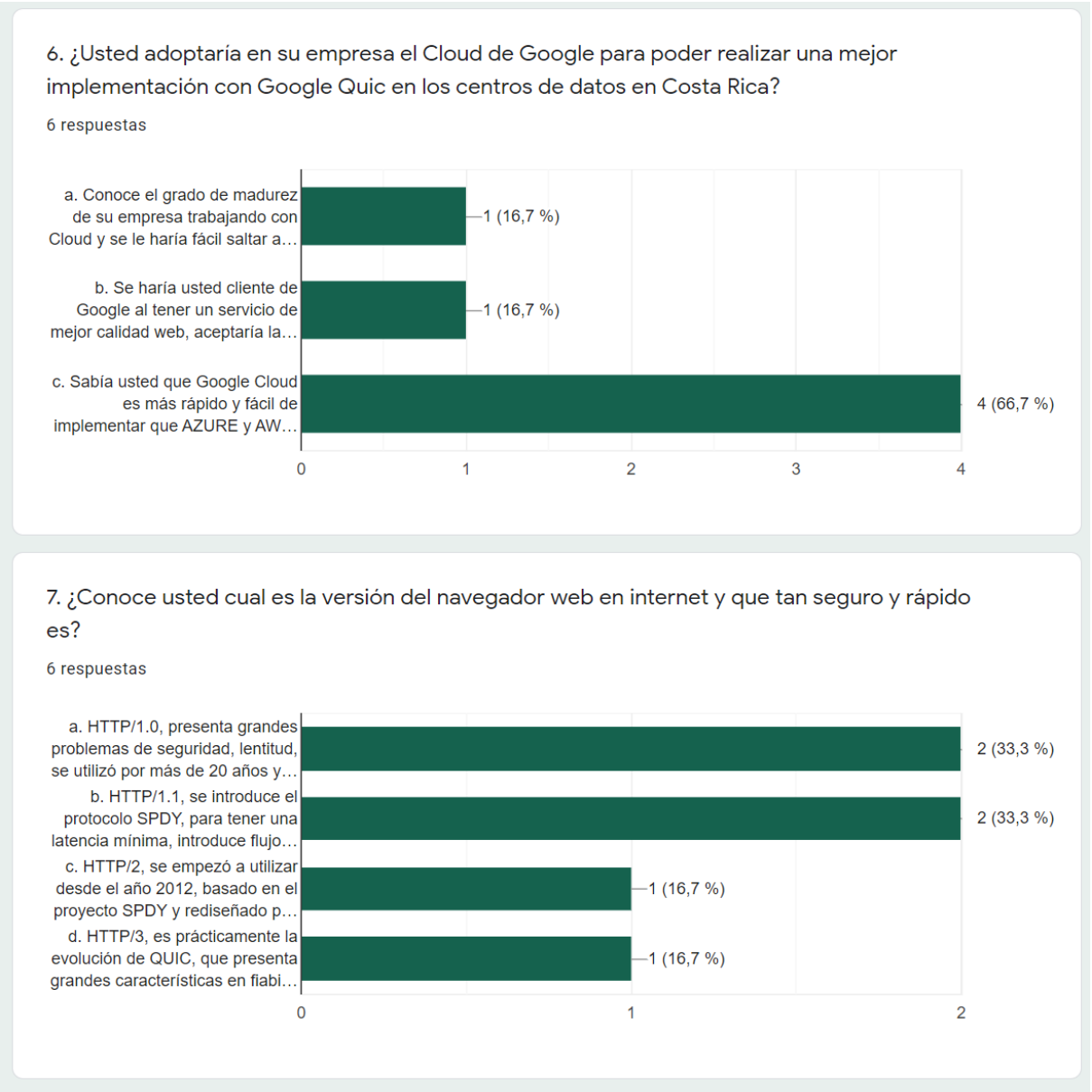


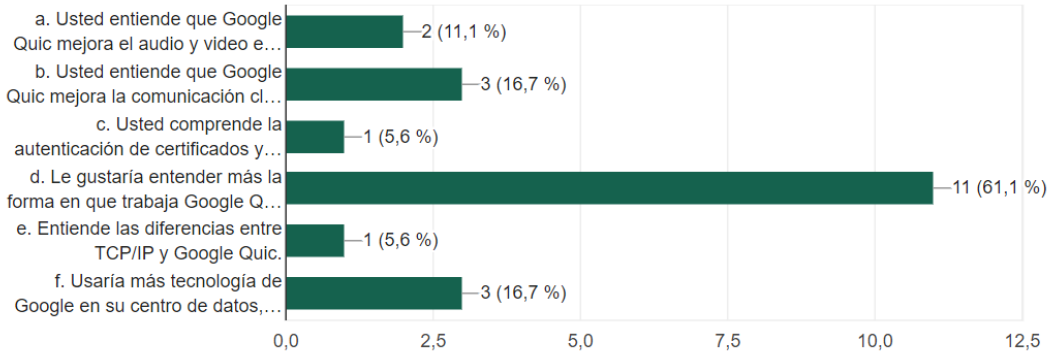
Figura 16: Recolección de datos de las diferentes redes sociales conocidas, Slack, WhatsApp, Facebook, en donde es posible entender el conocimiento de las personas con respecto a Google QUIC

4.2.2 Segundo bloque de respuestas

Segundo bloque de respuestas de la encuesta, enviadas a las diferentes redes sociales.

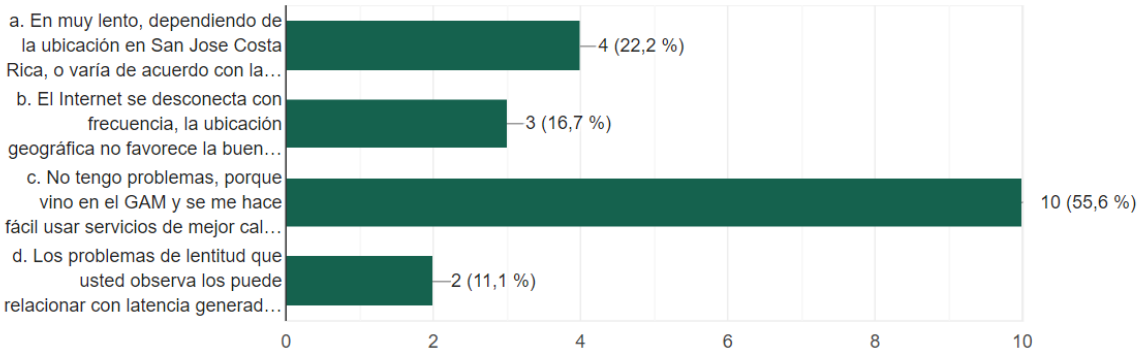
1. ¿Conoce usted lo que es Google Quic?

18 respuestas



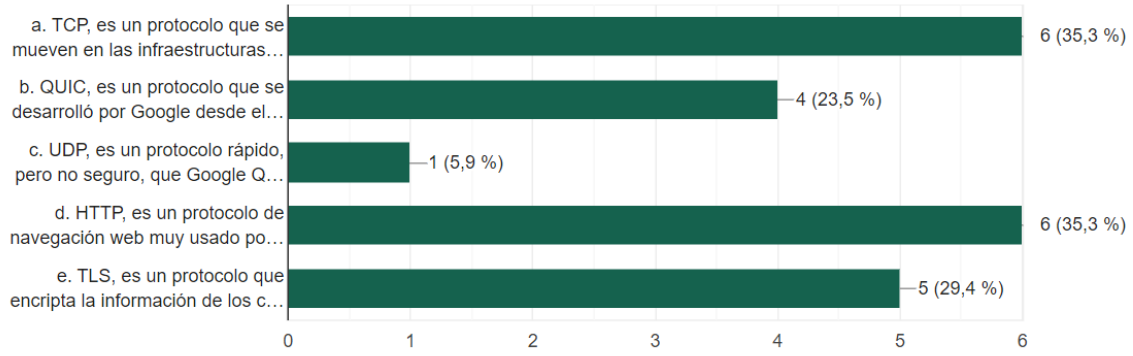
2. ¿Tiene usted en su empresa problemas de lentitud en su navegación en internet?

18 respuestas



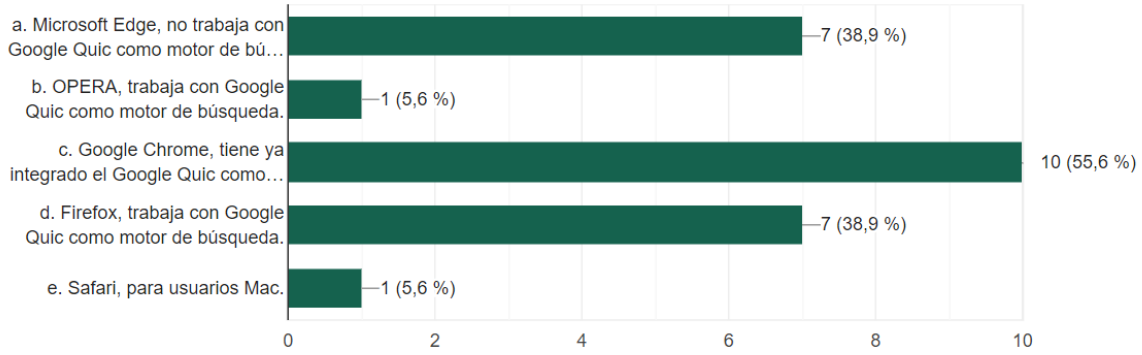
3. ¿Sabe usted que protocolos de comunicación usan en la red de su empresa?

17 respuestas



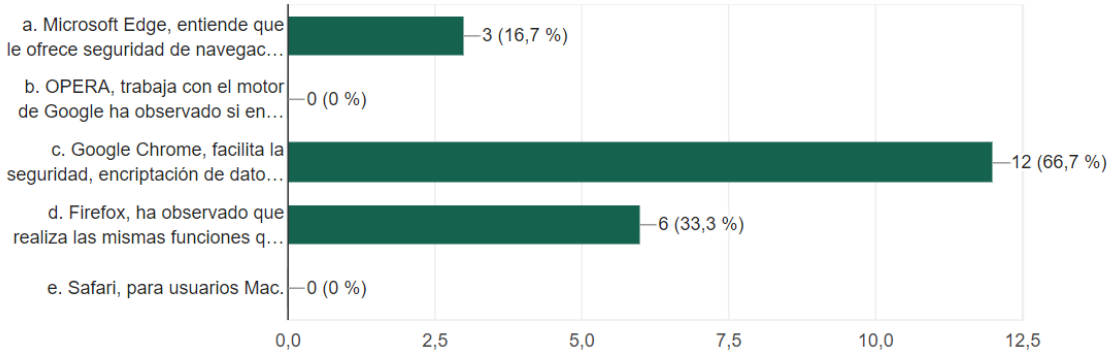
4. ¿Cuál es el navegador web que utilizan por defecto en su Empresa?

18 respuestas



5. ¿Cuándo usted utiliza dispositivos móviles como tables, teléfonos, Laptops cuál es su buscador en internet preferido?

18 respuestas



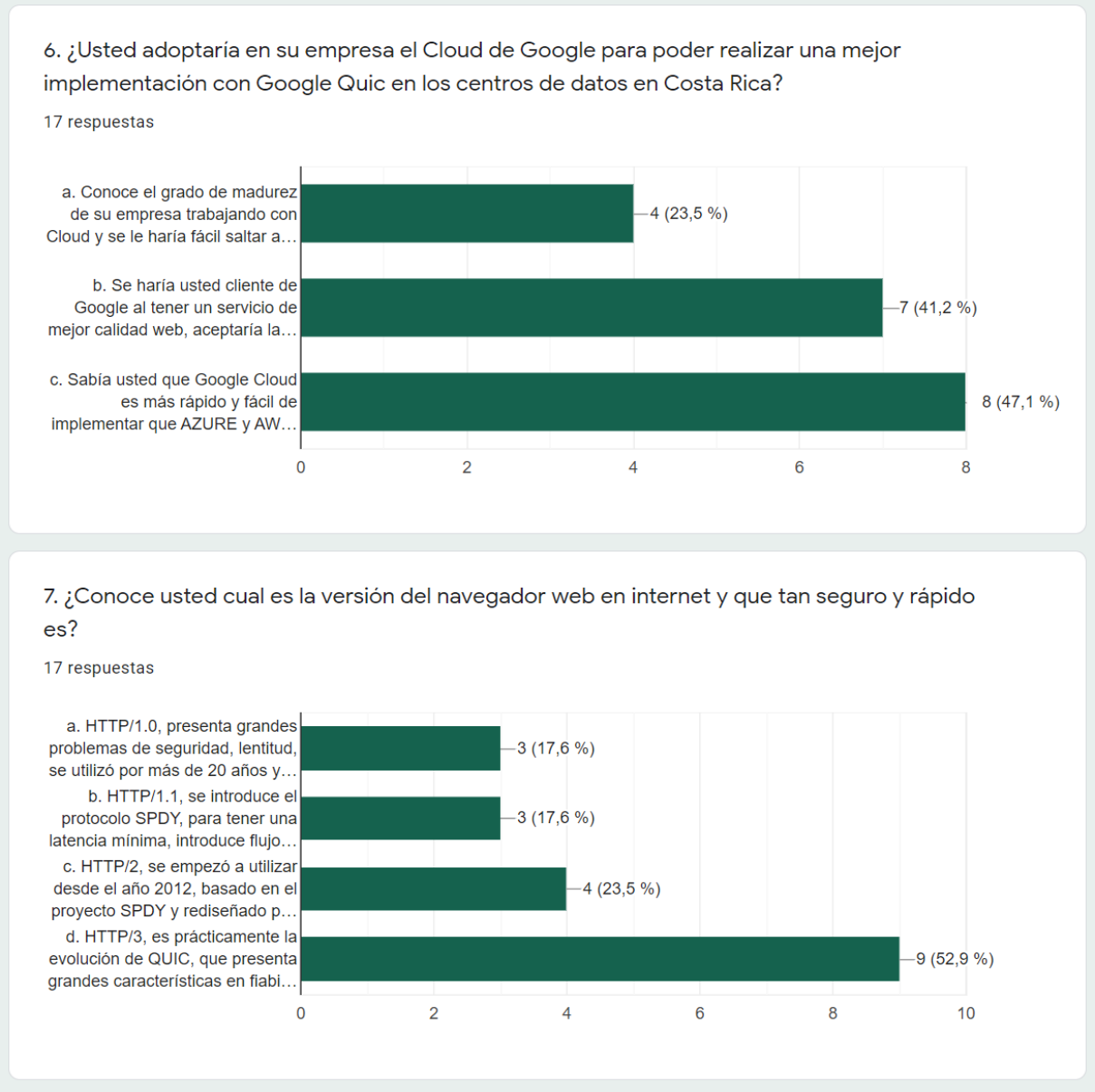


Figura 17: Recolección de datos de las diferentes redes sociales conocidas, Slack, WhatsApp, Facebook, Discord, Telegram en donde es posible entender el conocimiento de las personas con respecto a Google QUIC

4.3 Comparación de resultados

Comparación de los diferentes resultados con Wireshark, utilizando los diferentes navegadores web, para hacer un análisis de los protocolos de red que se utilizan.

Mediante diferentes capturas de tráfico de información entre fuente y destino, a través de pruebas de reproducción de video web en YouTube se ve el comportamiento de tráfico de información y se demuestra que se tienen los siguientes protocolos de red disponibles en la capa de aplicación: UDP, TCP, ICMP, TLS, HTTP y QUIC. Estos fueron capturados en forma correcta y en este caso se utiliza el navegador web Opera vs. Google Chrome, como es posible observar en la siguiente captura realizada por Wireshark.

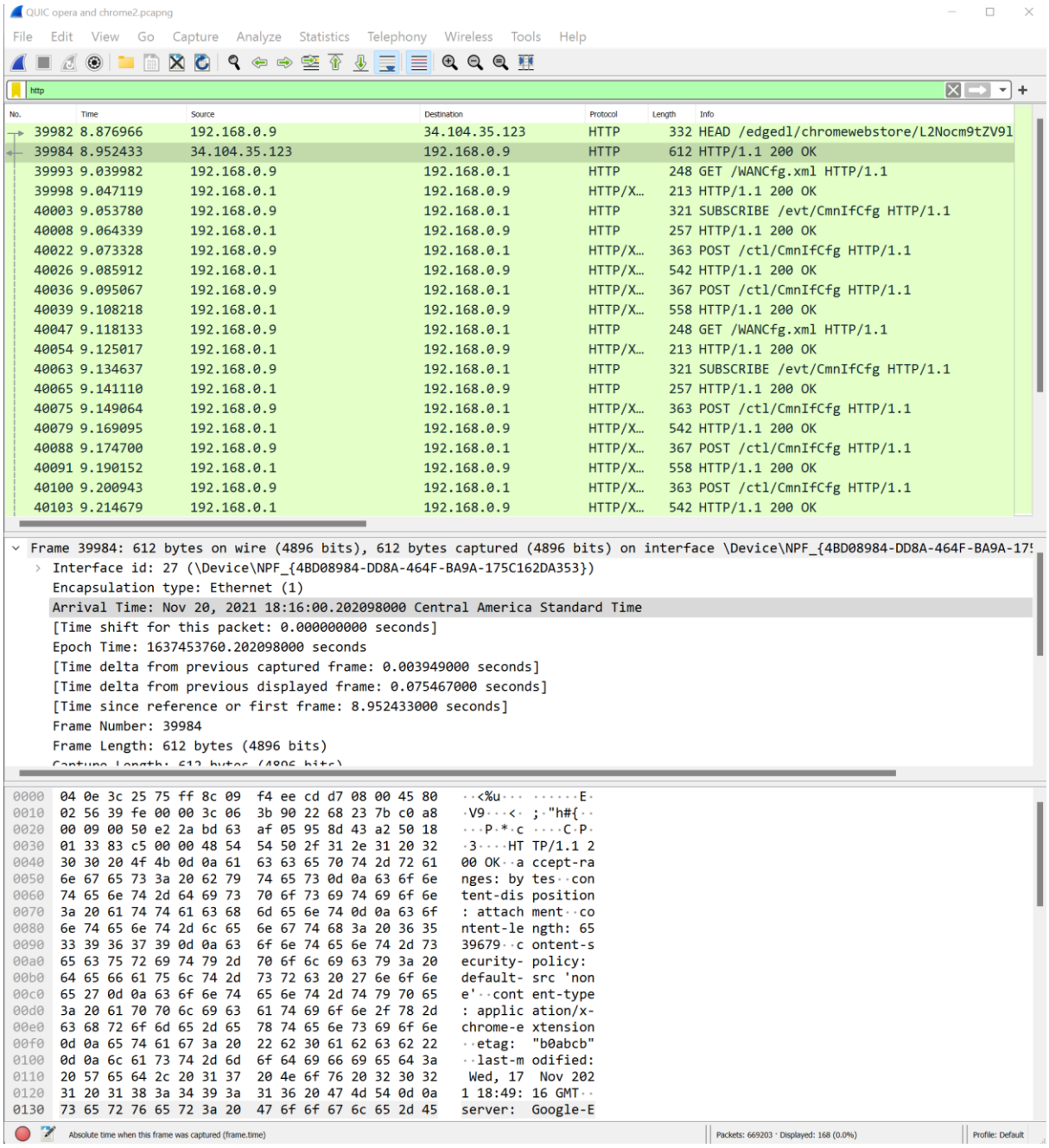


Figura 18: Captura correcta del protocolo HTTP que se ejecuta en Opera y Google Chrome

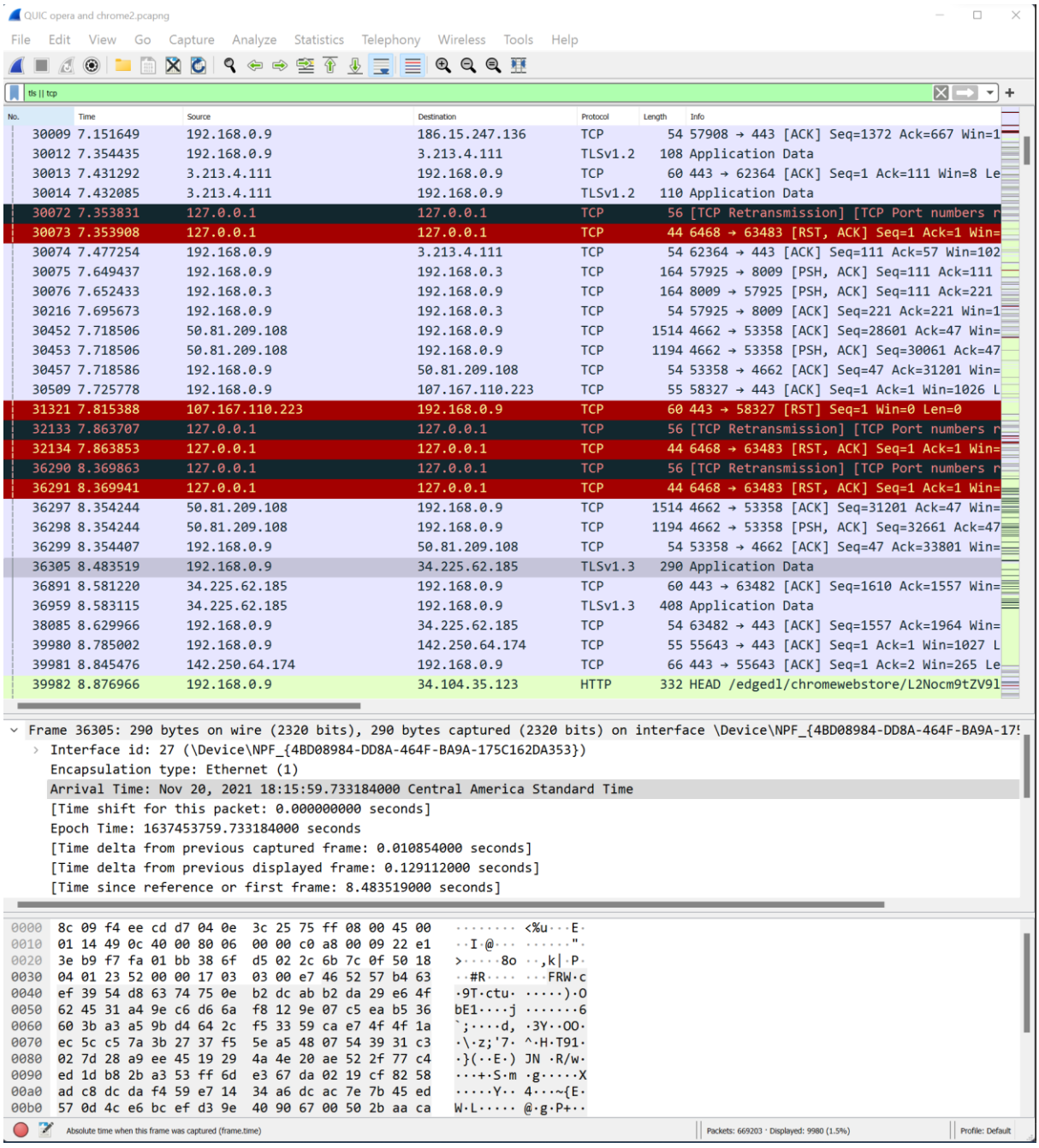


Figura 19: Alto tráfico de TCP entre cliente y servidor y protocolo TLS en dos versiones diferentes la versión 1.2 y la versión 1.3

Estas versiones son especiales para trabajar con QUIC y con el HTTP/3 ya que dan una mayor seguridad y una alta respuesta a contenido web en HD y UHD, lo que demuestra que el Google QUIC se utiliza a través de UDP.

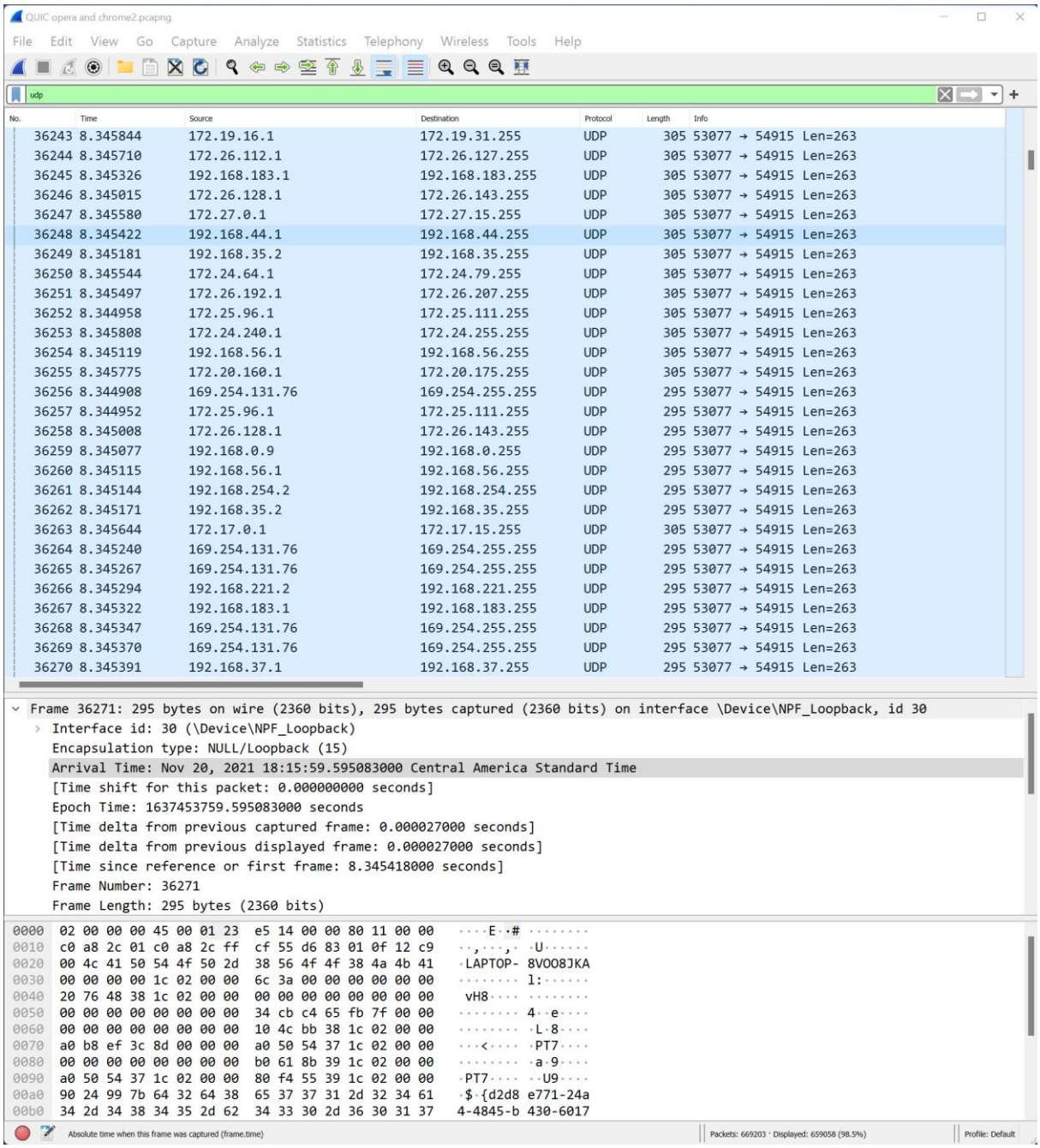


Figura 20: Alto contenido o tráfico de UDP que es la base en donde QUIC procesa la información de contenido web

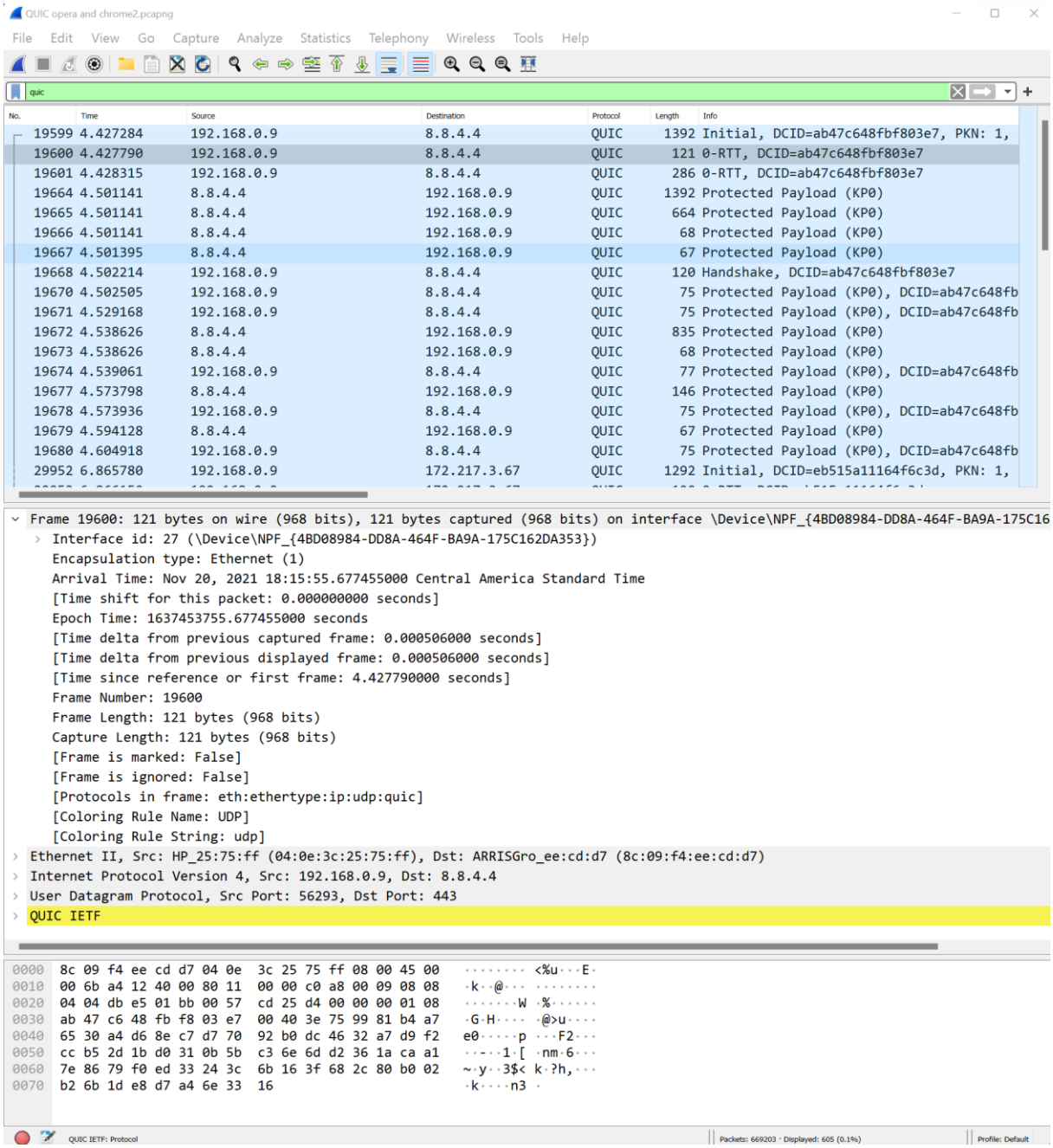


Figura 21: Comprobación de que el Google QUIC está corriendo correctamente en Opera y Chrome

Con esto se comprueba la eficacia sobre la reproducción de video y audio que se desea en contenido de alta resolución y, al mismo tiempo, se comprueba que la arquitectura en donde está implementado QUIC se cumple. Otro dato muy importante es que el Internet Engineer Task Force está llevando el Google QUIC a unas tecnologías todavía más avanzadas.

4.3.1 Proceso de recolección de datos

Proceso de recolección de datos para crear las pruebas de la encuesta y del uso de herramientas de análisis de red, en este caso el Wireshark.

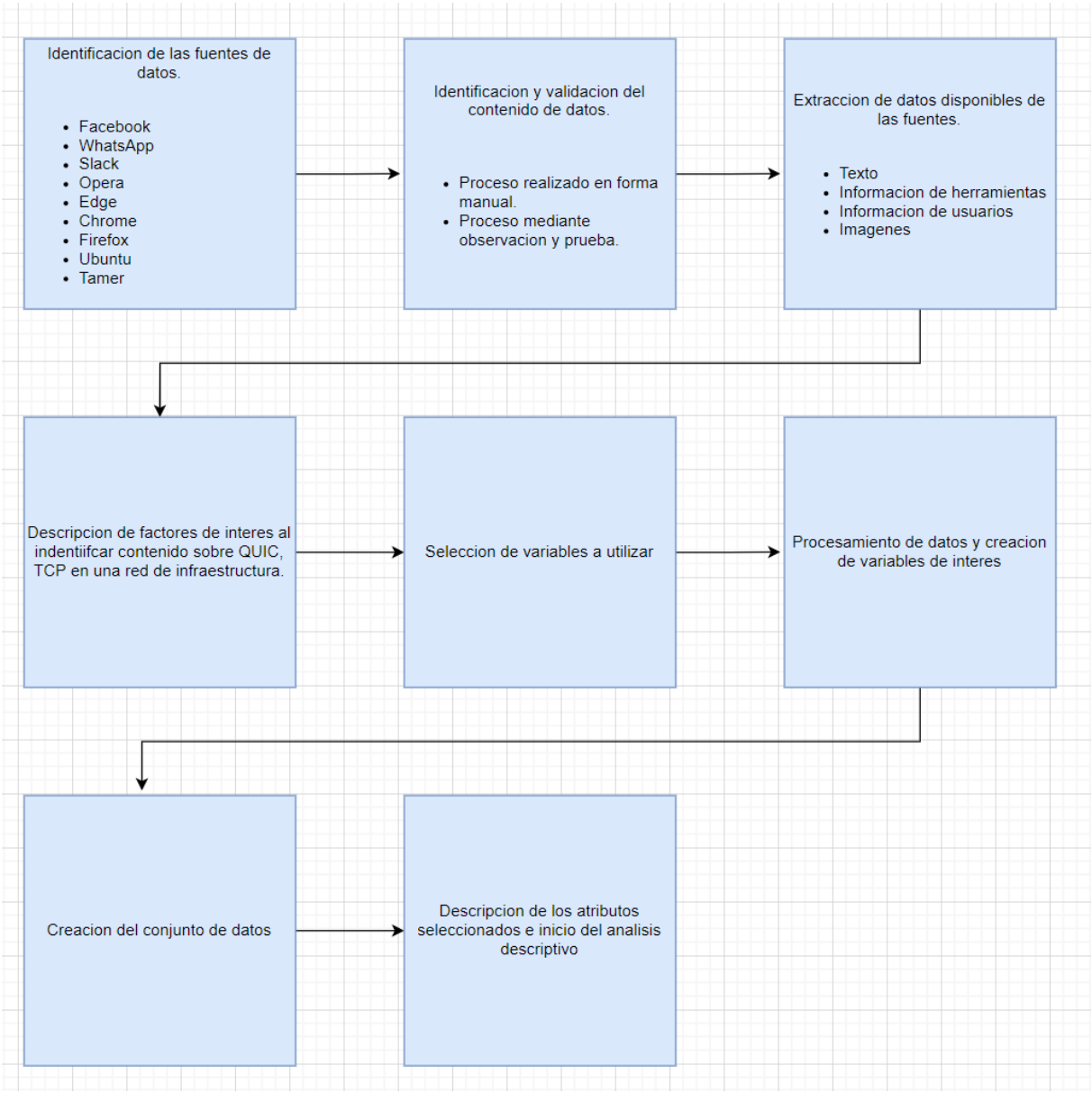


Figura 22: Proceso de recolección de datos para crear el conjunto de datos de prueba

4.3.2 Identificación de las fuentes de datos.

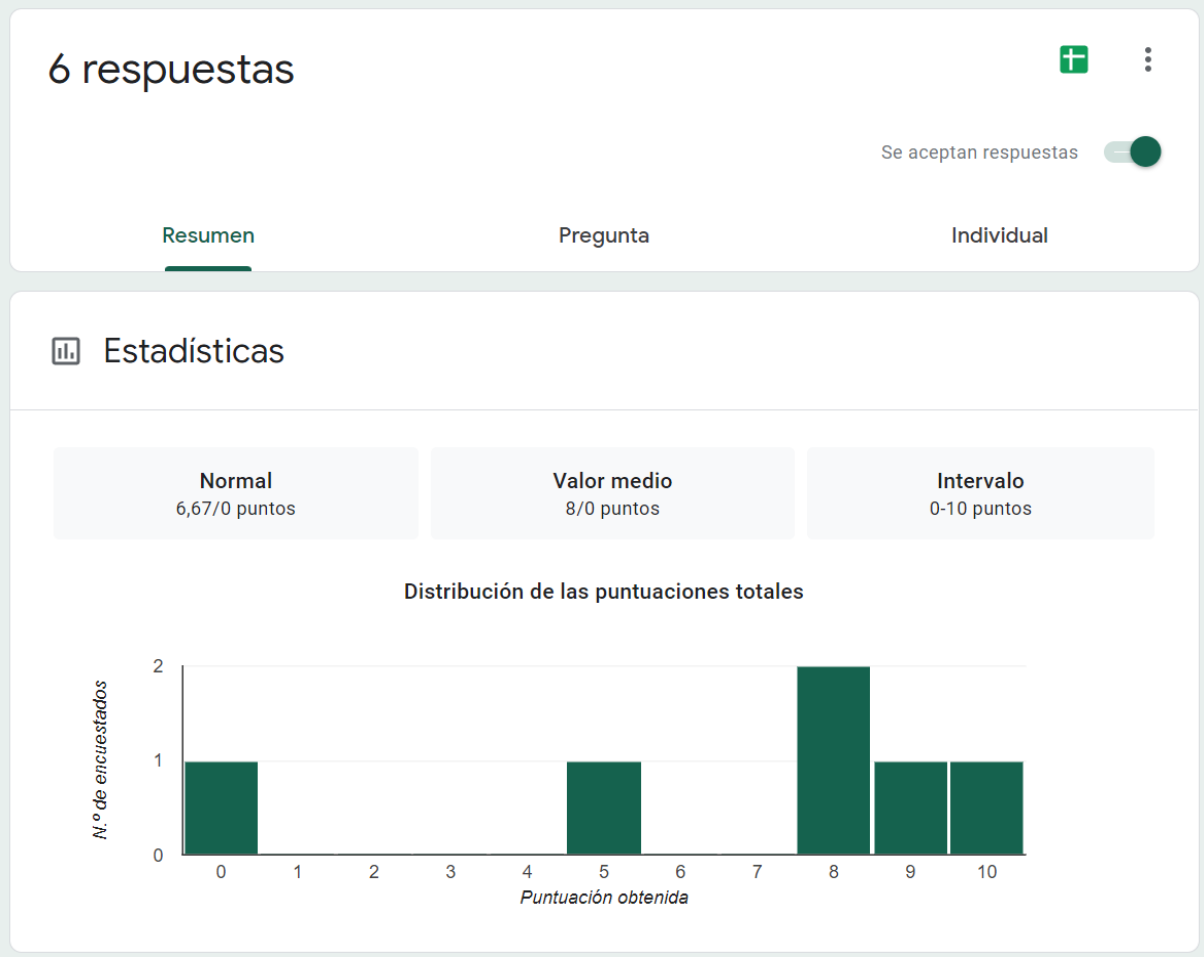


Figura 23: Primer análisis estadístico sobre la confianza de los datos que se obtienen y de sus diferentes fuentes de información



Figura 24: Segundo análisis estadístico sobre la confianza de los datos que se obtienen y de sus diferentes fuentes de información

En la Figura 25 lo que se observa es el tráfico con los datos capturados del Google QUIC en un periodo de un segundo y del TLS para los navegadores de Opera y Chrome en donde se tienen 300 paquetes de información por segundo solo de Google QUIC.



Figura 25: identificación de las fuentes de datos extraídas del Google Chrome y de Opera

En esta otra fuente de información se observa el tráfico de datos del protocolo Google QUIC entre las redes que están interactuando, comprendidas entre origen y destino con sus direcciones de IP correspondientes y cómo el tráfico de paquetes se

transfiere por segundo. También se observa el ancho de banda de la red con relación a su promedio y su uso máximo.

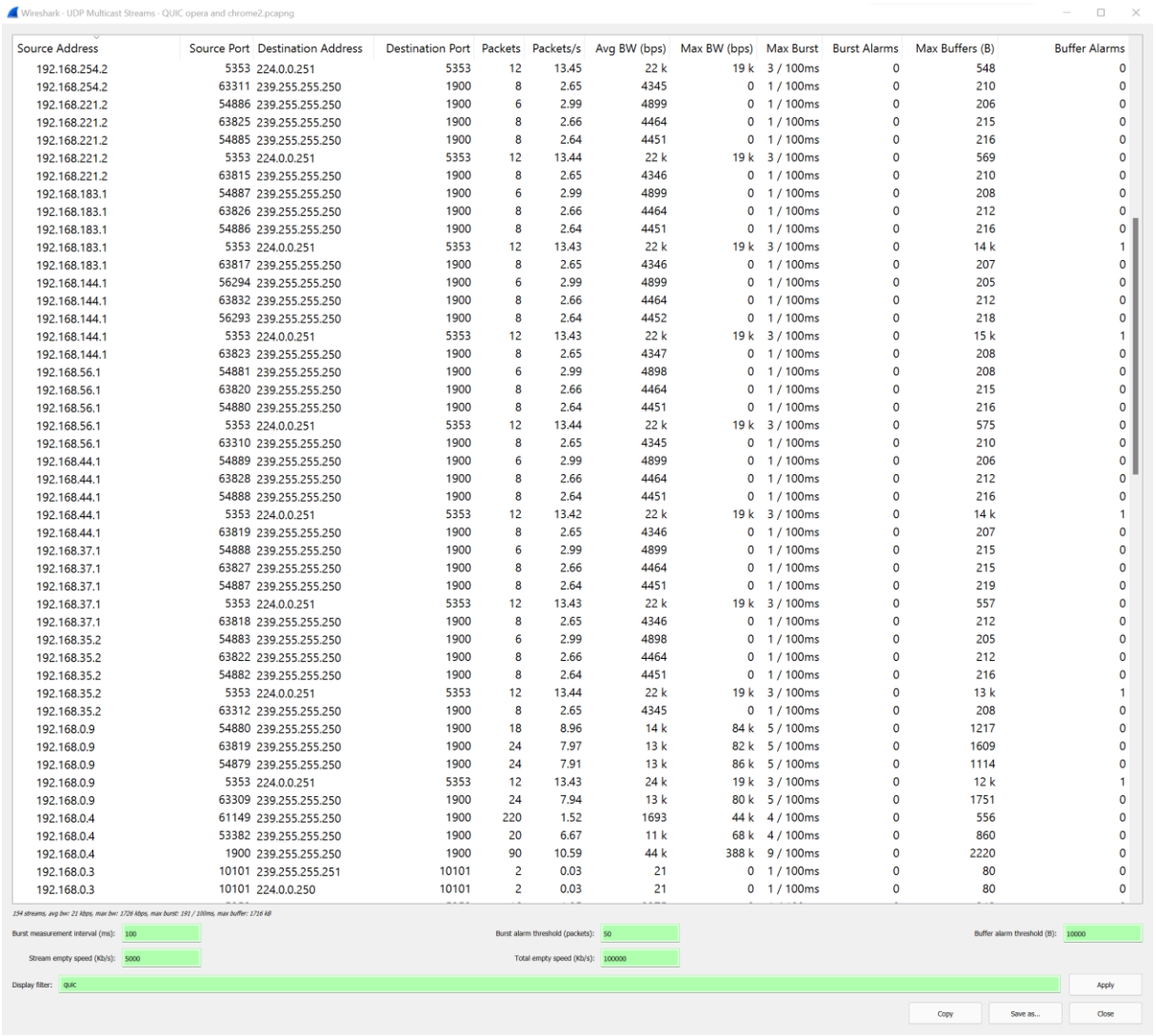


Figura 26: Captura de datos de información de Google QUIC fuente destino

4.3.3 Recopilación de contenido

Identificación de la estrategia para recopilar contenido de la encuesta y del uso de herramientas de análisis de redes (Wireshark).

- Estrategia de recolección de datos para la encuesta.
- Estrategia de la recolección de datos con el análisis de redes.

4.3.4 Extracción de datos

A continuación, se detalla.

4.3.4.1 Encuesta realizada con formularios de Google

(https://docs.google.com/forms/u/0/?tgif=d)

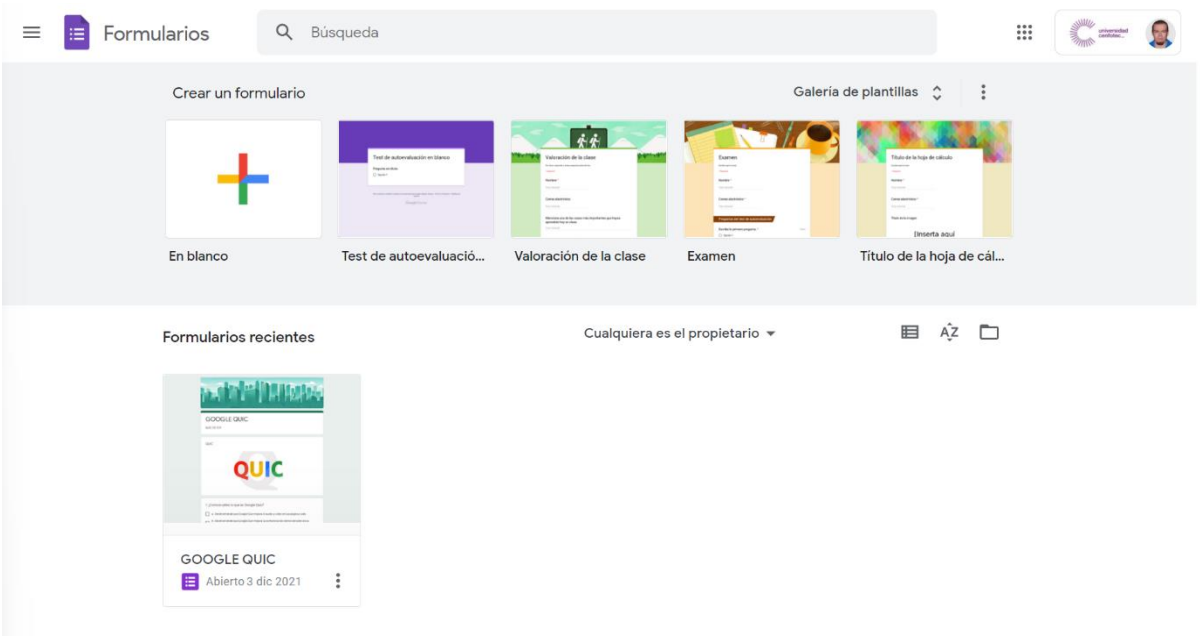


Figura 27: Creación de la encuesta mediante los formularios de Google

4.3.4.2 Resultados de las diferentes encuestas

En la Figura 28 es posible analizar las 7 preguntes de 18 respuestas y darle un porcentaje a cada respuesta según su importancia alrededor de Google QUIC.

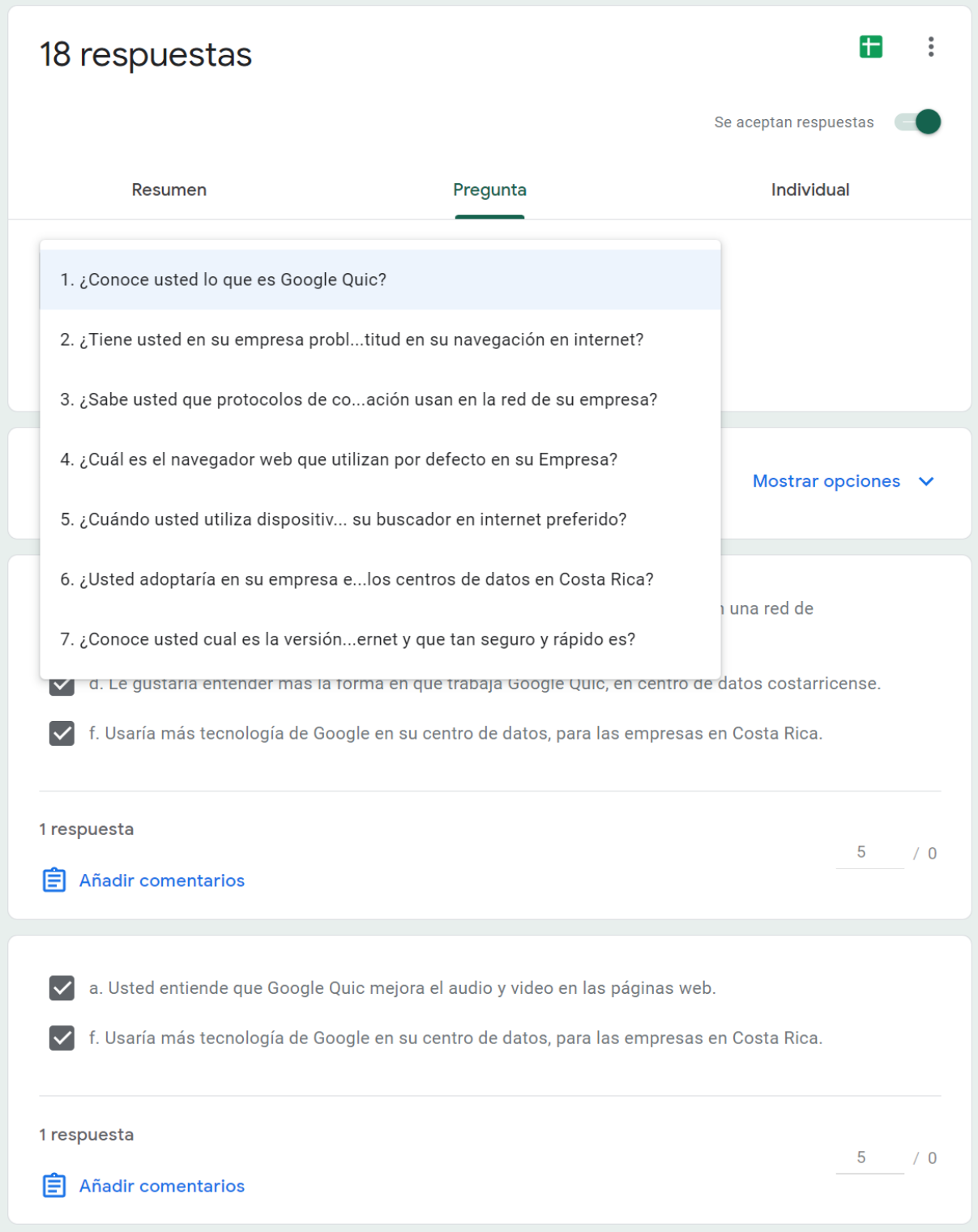
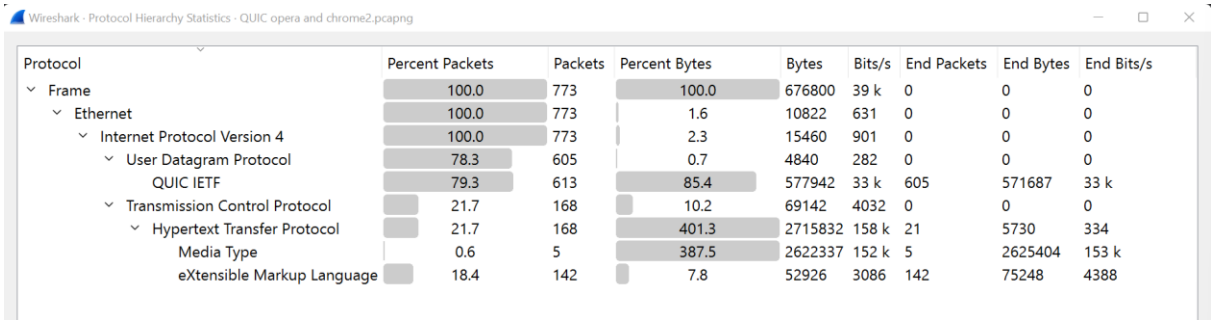


Figura 28: Diferentes respuestas obtenidas por pregunta, para hacer un mejor análisis independiente

4.3.4.3 Porcentaje de la extracción de datos en la jerarquía de protocolos



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	773	100.0	676800	39 k	0	0	0
Ethernet	100.0	773	1.6	10822	631	0	0	0
Internet Protocol Version 4	100.0	773	2.3	15460	901	0	0	0
User Datagram Protocol	78.3	605	0.7	4840	282	0	0	0
QUIC IETF	79.3	613	85.4	577942	33 k	605	571687	33 k
Transmission Control Protocol	21.7	168	10.2	69142	4032	0	0	0
Hypertext Transfer Protocol	21.7	168	401.3	2715832	158 k	21	5730	334
Media Type	0.6	5	387.5	2622337	152 k	5	2625404	153 k
eXtensible Markup Language	18.4	142	7.8	52926	3086	142	75248	4388

Figura 29: Jerarquía de protocolos expresado en el porcentaje de utilización en la red, el QUIC está absorbiendo el 79.3 % del flujo de tráfico y el TCP solo el 21.7 %

4.3.4.3.1 Descripción del conjunto de datos

La Tabla 1 describe los datos que se obtienen de las diferentes páginas web o redes sociales que se utilizan, para la interpretación del conocimiento sobre Google QUIC.

Tabla 1: Descripción de los datos que se obtienen de las diferentes redes sociales

Titulo	Conjunto de datos de las diferentes redes sociales.
Creador	Christian Araya.
Identificador	Formularios de Google.
Tema	Google QUIC.
Idioma	Español.
Fechas	Datos recopilados del 06 de diciembre de 2021 al 31 de diciembre de 2021.
Metodología	La extracción de los datos de información se llevó a cabo mediante el sitio web de documentos de Google, utilizando la herramienta o aplicación de formularios.
Procesamiento de datos	Los resultados de las diferentes encuestas se capturaron en forma automática por la misma aplicación de formularios de Google y da una forma más comprensible de los resultados. Presenta gráficos mejor acomodados para un mejor análisis de resultados y conclusiones.

Titulo	Conjunto de datos de las diferentes redes sociales.
Fuente de datos	docs.google.com/forms/
Archivo resultante	GOOGLE QUIC - Formularios de Google.pdf GOOGLE QUIC.csv
Formato del archivo	Microsoft Excel, hoja de cálculo con formato CSV o también en formato XLSX

En la Tabla 2 se describen los datos que se obtienen mediante el análisis de redes con relación a los diferentes protocolos de red utilizando herramientas de pruebas de penetración, en este caso Wireshark.

Tabla 2: Descripción de los datos que se obtienen mediante el análisis de redes

Titulo	Conjunto de datos del análisis de redes.
Creador	Christian Araya.
Identificador	Wireshark.
Tema	Google QUIC.
Idioma	Español.

Titulo	Conjunto de datos del análisis de redes.
Fechas	Datos recopilados del 20 de noviembre de 2021 al 31 de diciembre de 2021.
Metodología	La extracción de los datos de información se llevó a cabo mediante el uso de la aplicación de Wireshark.
Procesamiento de datos	Los datos se obtuvieron de máquinas físicas y virtuales como Windows 11 máquina física, Ubuntu 20.04 Linux máquina virtual, Android Tamer 4 máquina virtual y la herramienta de Wireshark versión: 3.6.0.
Fuente de datos	Windows 11, Linux, Android, Microsoft Edge, Opera, Google Chrome, Firefox.
Archivo resultante	Flow Graph QUIC.pdf Protocol Hierarchy Statistics.csv QUIC opera and chrome2.csv QUIC opera and chrome2.png QUIC opera and chrome2.pdf

Titulo	Conjunto de datos del análisis de redes.
Formato del archivo	Microsoft Excel, hoja de cálculo con formato CSV o también en formato XLSX Archivo PDF Archivo PNG

4.3.4.3.2 Descripción de variables

La Tabla 3 ayuda a entender la descripción sobre las variables que se usan mediante la aplicación de Google Forms, cuántas encuestas se realizaron, qué tipo de respuestas se tiene, qué clase de puntuación se les pueda dar y las estadísticas en forma general.

Table 3: Descripción del diseño de la encuesta con Google Forms

Variable	Descripción	Formato
URL de la encuesta	Es la dirección URL adquirida en la configuración interna de la creación de la encuesta por publicarse.	Cadena de datos

Variable	Descripción	Formato
URL del sitio web de la encuesta	Es la dirección URL de las aplicaciones de Google para utilizar la aplicación de Google Forms.	Cadena de datos
URL de la pregunta en la encuesta	Es la dirección URL independiente por pregunta.	Cadena de datos
Título de la encuesta	El título propio de la encuesta diseñado con la aplicación de formularios.	Cadena de datos
Fecha de publicación de la encuesta	Es la fecha y hora que se puede observar dentro del entorno de desarrollo interno del formulario de Google.	Fecha en formato: dd-mm-yyyy-dd'T'HH:mm:ss.SSSXXX
Autor de la encuesta	La elaboración o diseño de la encuesta es Christian Araya, quien es el autor de la encuesta.	Cadena de datos

Variable	Descripción	Formato
Texto de la encuesta	Texto elaborado dentro de la aplicación de formularios o texto completo de cada respuesta.	Cadena de datos
Cantidad de respuesta de la encuesta	Cantidad de respuesta que obtuvo la encuesta por pregunta.	Cadena de datos
Cantidad de participantes de la encuesta	Cuánta gente participó en la encuesta.	Cadena de datos
País	País de origen de la encuesta.	Cadena de datos
URL imagen principal de la encuesta	La encuesta contiene imágenes asociadas con su dirección web, las cuales se observan al abrir el enlace URL.	Cadena de datos
Puntuación de desempeño de cada pregunta	La puntuación está dentro del rango de 0 a 10 y la puntuación depende de cuántas veces se repitieron las mismas respuestas en forma aleatoria.	Cadena de datos

Variable	Descripción	Formato
Fecha de extracción de la encuesta	Es la fecha con la información al día para analizar las respuestas correspondientes.	Fecha en formato: dd-mm-yyyy-dd'T'HH:mm:ss.SSSXXX

La Tabla 4 ayuda a entender la descripción sobre las variables que se usan mediante la aplicación de Wireshark, en donde se entiende el tráfico de flujo de los protocolos de red, en relación con su fuente y destino.

Tabla 4: Descripción de los datos que se obtienen mediante la herramienta de Wireshark

Variable	Descripción	Formato
Fuente	Dirección de Internet Protocolo origen donde empieza la captura de datos.	Cadena de datos
Destino	Dirección de Internet Protocolo objetivo final o destino final en donde se cierra la captura de información.	Cadena de datos
Protocolo	Es el conjunto de reglas que se usan en las redes para procesar datos. Es el lenguaje de comunicación común que usan las computadoras en una red.	Cadena de datos
Marco	Marco o *frame,* se relaciona con el proceso de comunicación entre cliente y servidor en una red, el tipo de	Cadena de datos

Variable	Descripción	Formato
	conectividad, los protocolos de comunicación usados y más información sobre los paquetes transferidos.	
Ethernet	Es el medio de comunicación que se utiliza para que la red pueda transferir los paquetes entre fuente y destino.	Cadena de datos
IPv4	Es la versión 4 del protocolo de Internet más usado hasta el momento para comunicación entre las redes.	Cadena de datos
UDP	Protocolo de comunicación en la capa 4 del modelo OSI más rápido para entregar información, pero menos seguros.	Cadena de datos
TCP	Protocolo de comunicación en la capa 4 del modelo OSI más lento para entregar información, pero más seguro.	Cadena de datos

Variable	Descripción	Formato
QUIC IETF	El protocolo de Internet más rápido para navegación web con mejor seguridad web y con mejor respuesta para contenido de audio y video.	Cadena de datos
TLS	El protocolo de encriptación que permite proteger la información codificada entre cliente, servidor y poderla entregar al protocolo HTTP para que pueda observarla el cliente final.	Cadena de datos
HTTP	Protocolo de navegación web seguro y no seguro para observar el contenido web por la persona usuaria final	Cadena de datos
Autor del análisis de red	El uso de las herramientas involucradas lo controla Christian Araya, quien utiliza	Cadena de datos

Variable	Descripción	Formato
	la red con sus diferentes datos y aplicaciones.	
Título del análisis de red	El título propio del análisis de red varía de acuerdo con los elementos involucrados en la captura de información, pero todo va orientado al Google QUIC.	Cadena de datos
Fecha de la captura y extracción de la información	Es la fecha con la información al día para analizar las respuestas correspondientes, de las redes involucradas.	Fecha en formato: mm-dd-yyyy-dd'T'HH:mm:ss.SSSXXX

4.3.4 Selección de variables por utilizar

Después de hacer un análisis de resultados y de observar los atributos asociados con cada variable es posible destacar para la encuesta las siguientes variables por analizar:

- Título de la encuesta.
    - El título de la encuesta puede capturar rápidamente la atención del espectador y generar una influencia sobre el interés del encuestado.
- Texto de la encuesta.
    - El aspecto visual de la encuesta y su contenido despierta un interés para generar más respuestas deseadas.
- Cantidad de respuestas de la encuesta.
    - La cantidad de respuestas es fundamental para el análisis de resultados y entender el conocimiento que tienen las personas encuestadas sobre protocolos de red y sobre el mismo Google QUIC.
- Puntuación de desempeño de cada pregunta.
    - A cada pregunta se le puede asignar una puntuación de acuerdo con la profundidad o grado de dificultada de esa pregunta y también es un dato para realizar un mejor análisis sobre los resultados.

Con respecto al análisis de red con herramientas de penetración de pruebas, en este caso con el Wireshark, y después de observar los resultados y sus atributos es posible mencionar las siguientes variables por analizar:

- IP fuente.

    - Se captura la IP origen para iniciar el análisis de red.
- IP destino
    - Se captura la IP final o destino para cerrar el análisis de red.
- TLS
    - Se captura diferente tráfico de este protocolo para observar sus diferentes versiones y analizar los problemas de seguridad en la encriptación de datos.
- TCP
    - Protocolo maestro para el tráfico de paquetes entre cliente y servidor y da seguridad en la red.
- UDP
    - Protocolo maestro para el tráfico de paquetes entre cliente y servidor y da rapidez en la red.
- QUIC IETF
    - Protocolo de un alto desarrollo para la navegación web que posee una arquitectura de diseño muy profunda.
- HTTP
    - Protocolo de visualización de páginas web que interactúa con el cliente final.

4.3.5 Preprocesamiento de datos y creación de variables de interés

A continuación, se detalla.

4.3.5.1 Datos y creación de variables para la encuesta

En la Tabla 5 se encuentran las variables más significativas para entender los datos generados en la encuesta que se compartió en las redes sociales.

Tabla 5: Datos que se obtienen de las diferentes redes sociales

Variables	Datos
Título de la encuesta	• La visualización de la información. • La presentación de la página web. • Los subtítulos. • El diseño gráfico. Los datos anteriores capturan el interés del espectador.
Texto de la encuesta	• Letra legible y agradable. • Fácil de leer. • Diseño Gráfico. Los datos anteriores capturan el interés del espectador.
Cantidad de respuestas de la encuesta	Pregunta n.º 1: • R/a con 10 %

Variables	Datos
	• R/b con 15 % • R/c con 5 % • R/d con 65 % • R/e con un 5 % • R/f con 15 % La R/d es la opción en donde las personas desean obtener más conocimiento sobre cómo el Google QUIC puede trabajar en los centros de datos en Costa Rica y cómo funciona y trabaja en la infraestructura y en las redes en general.
Análisis de los resultados de la pregunta n.º 1:	De acuerdo con el 59.1 % obtenido en las respuestas, los usuarios finales necesitan conocer más de Google QUIC y cómo se implementaría en un centro de datos en Costa Rica.
Cantidad de respuestas de la encuesta	Pregunta n.º 2: • R/a con 20 % • R/b con 15 %

Variables	Datos
	• R/c con 60 % • R/d con 10 % La R/c es la opción que demuestra la gran deficiencia en el diseño de redes y cómo hay países con una muy mala implementación de Internet.
Análisis de los resultados de la pregunta n.º 2:	De acuerdo con el 54.5 % obtenido, muchos clientes finales utilizan un servicio de Internet de buena calidad si están dentro de la GAM, pero el problema se agrava a los que están fuera de esta ubicación.
Cantidad de respuestas de la encuesta	Pregunta n.º 3: • R/a con 36.8 % • R/b con 21.1 % • R/c con 10.5 % • R/d con 42.1 % • R/e con 26.3 %

Variables	Datos
	La R/d es la opción en donde las personas entienden los protocolos de navegación web y saben el HTTP.
Análisis de los resultados de la pregunta n.º 3:	De acuerdo con el 42.9 % obtenido, es posible entender que los usuarios finales tienen un conocimiento en redes y saben el protocolo TCP y el HTTP que se utilizan en las redes de su empresa.
Cantidad de respuestas de la encuesta	Pregunta n.º 4: • R/a con 35 % • R/b con 5 % • R/c con 55 % • R/d con 40 % • R/e con 5 % La R/c es la opción que demuestra que las personas utilizan más Google Chrome como motor de búsqueda y navegación web.

Variables	Datos
Análisis de los resultados de la pregunta n.º 4:	De acuerdo con el 54.5 % obtenido, los usuarios finales utilizan más el navegador web de Google, al tener el Google QUIC integrado y ser más rápido y confiable para búsquedas en Internet.
Cantidad de respuestas de la encuesta	Pregunta n.º 5: • R/a con 15 % • R/b con 0 % • R/c con 65 % • R/d con 30 % • R/e con 5 % La R/c es la opción en donde las personas usan más Google Chrome para los dispositivos móviles y confían más en la seguridad, encriptación de información y despliegue de contenido en 4 K.

Variables	Datos
Análisis de los resultados de la pregunta n.º 5:	De acuerdo con el 68.2 % obtenido, Google Chrome es la aplicación web dominante para todo lo que son dispositivos móviles en búsquedas de información de Internet.
Cantidad de respuestas de la encuesta	Pregunta n.º 6: • R/a con 21.1 % • R/b con 47.4 % • R/c con 42.1 % La R/b es la opción que demuestra que las personas se pueden cambiar a Google Cloud para obtener un servicio de más calidad
Análisis de los resultados de la pregunta n.º 6:	De acuerdo con el 42.9 % obtenido, las empresas adoptarían el Google Cloud como una mejor solución en los centros de datos en Costa Rica para tener una implementación en donde toda la tecnología sería de Google y el protocolo QUIC tendría un mejor desplazamiento entre esa infraestructura.

Variables	Datos
Cantidad de respuestas de la encuesta	Pregunta n.º 7: • R/a con 15.8 % • R/b con 15.8 % • R/c con 26.3 % • R/d con 52.6 % La R/d es la opción en donde las personas entienden que utilizan el protocolo HTTP/3 y porque aquí Google QUIC hace una gran diferencia para la multiplexación de flujos de información y la fiabilidad que debe tener una infraestructura moderna
Análisis de los resultados de la pregunta n.º 7:	De acuerdo con el 52.4 % obtenido, los usuarios están más conscientes de que pueden usar la versión del protocolo HTTP/3 como la mejor alternativa para seguridad, rapidez, fiabilidad, multiplexación de flujos, identificador de conexiones

Variables	Datos
Puntuación de desempeño de cada pregunta	Pregunta n.º 1: Obtuvo una puntuación de 115 % después de 20 respuestas o 10 encuestas.
Puntuación de desempeño de cada pregunta	Pregunta n.º 2: Obtuvo una puntuación de 105 % después de 20 respuestas o 10 encuestas.
Puntuación de desempeño de cada pregunta	Pregunta n.º 3: Obtuvo una puntuación de 136.8 % después de 20 respuestas o 10 encuestas.
Puntuación de desempeño de cada pregunta	Pregunta n.º 4: Obtuvo una puntuación de 140 % después de 20 respuestas o 10 encuestas.
Puntuación de desempeño de cada pregunta	Pregunta n.º 5: Obtuvo una puntuación de 115 % después de 20 respuestas o 10 encuestas.
Puntuación de desempeño de cada pregunta	Pregunta n.º 6: Obtuvo una puntuación de 110.6 % después de 20 respuestas o 10 encuestas.
Puntuación de desempeño de cada pregunta	Pregunta n.º 7: Obtuvo una puntuación de 110.5 % después de 20 respuestas o 10 encuestas.

4.3.5.2 Datos y creación de variables para el análisis de red

En la Tabla 6 se encuentran las variables más significativas para entender los datos generados en el análisis de red.

Tabla 6: Datos capturados y analizados por medio de pruebas de penetración

Variable	Datos	Capa de arquitectura	Funcionamiento por capa de arquitectura
IPv4 Origen cliente	Frames o marcos de información en paquetes de *bytes* o *bits*, encriptado en código hexadecimal	Red	• IP cliente: el punto final que inicia una conexión QUIC. • Punto final: el extremo cliente o servidor de una conexión. • Stream: canal lógico bidireccional de *bytes* ordenados dentro de una conexión QUIC. • Conexión: una conversación entre dos puntos finales QUIC

Variable	Datos	Capa de arquitectura	Funcionamiento por capa de arquitectura
			con un único contexto de cifrado que multiplexa los flujos dentro de este. • ID de conexión: el identificador de una conexión QUIC. • Paquete QUIC: una carga útil UDP bien formada que puede analizar un receptor QUIC, que es el tamaño de carga útil UDP.
IPv4 destino servidor	Frames o marcos de información en paquetes de *bytes* o *bits*, encriptado en código hexadecimal	Red	• IP servidor: el punto final que acepta conexiones QUIC entrantes. • Punto final: el extremo cliente o servidor de una conexión.

Variable	Datos	Capa de arquitectura	Funcionamiento por capa de arquitectura
			• Stream: canal lógico bidireccional de *bytes* ordenados dentro de una conexión QUIC. • Conexión: una conversación entre dos puntos finales QUIC con un único contexto de cifrado que multiplexa los flujos dentro de este. • ID de conexión: el identificador de una conexión QUIC. Paquete QUIC: una carga útil UDP bien formada que puede analizar un receptor QUIC, que es el tamaño de carga útil UDP.

Variable	Datos	Capa de arquitectura	Funcionamiento por capa de arquitectura
TLS	Frames o marcos de información en paquetes de *bytes* o *bits*, encriptado en código hexadecimal	Seguridad	• Mensajes de autentificación cliente y servidor (Handshake) • Validación de los parámetros 0-RTT. • Llaves 0-RTT. • Llaves cliente y servidor (Handshake) • Llaves 1-RTT. • Autentificación cliente y servidor terminada (Handshake).
TCP	Frames o marcos de información en paquetes de *bytes* o *bits*, encriptado en código hexadecimal	Transporte	

Variable	Datos	Capa de arquitectura	Funcionamiento por capa de arquitectura
UDP	Frames o marcos de información en paquetes de *bytes* o *bits*, encriptado en código hexadecimal	Transporte	
QUIC IETF	Frames o marcos de información en paquetes de *bytes* o *bits*, encriptado en código hexadecimal	Seguridad	• Negociación de versiones de baja latencia • Establecimiento de conexión de baja latencia • Multiplexación sin bloqueo de cabecera • Cabecera y carga útil autenticados y cifrados

Variable	Datos	Capa de arquitectura	Funcionamiento por capa de arquitectura
			• Señalización enriquecida para el control de la congestión y la recuperación de pérdidas • Control de flujo y conexión • Migración de conexión y resistencia a la reencuadernación de NAT
HTTP	Frames o marcos de información en paquetes de *bytes* o *bits*, encriptado en código hexadecimal	Aplicación	• Descubrimiento de los puntos finales. • Establecimiento de conexiones. • Reuso de conexiones. • Ciclo de vida de las solicitudes del HTTP. • Cierre de la conectividad.

Variable	Datos	Capa de arquitectura	Funcionamiento por capa de arquitectura
			• Mapeo de las transmisiones y uso.

Capítulo 5. Propuesta de solución

5.0 Introducción de la propuesta de solución

La propuesta de solución se enfoca en proponer dos escenarios en los que se entenderán dos propuestas de arquitectura. Cada propuesta plantea sus propios riesgos, por lo que se explica qué son y cómo se solucionan. Además, se procede a evaluar esas soluciones y definir cuál es el diseño de arquitectura recomendado.

Para que se mantenga la solución activa se debe realizar un informe y seguimiento sobre esas soluciones. Lo anterior para que se mantenga al día el desempeño de la empresa y la viabilidad de esa solución y, al mismo tiempo, mantener actualizadas a las personas con el conocimiento relacionado con tecnologías de redes y seguridad.

También se entiende cómo usar el Google QUIC UDP, cuáles son sus características técnicas, cómo se debe implementar, qué beneficios se tienen con este protocolo, técnicos y económicos, por qué se debe implementar el QUIC UDP y los pasos para implementarlo. Asimismo, se explica cómo trabajan los diagramas de arquitectura en la solución de esta arquitectura.

5.0.1 Cómo usar el Google QUIC UDP

Para usar el QUIC UDP en un navegador web, ya sea Microsoft Edge, Google Chrome u Opera se deben correr los siguientes comandos: chrome://flags, edge://flags, opera://flags. De esta forma, es posible activar las banderas de cada navegador y seleccionar el Experimental QUIC Protocol, como se ve en las siguientes capturas de pantalla.

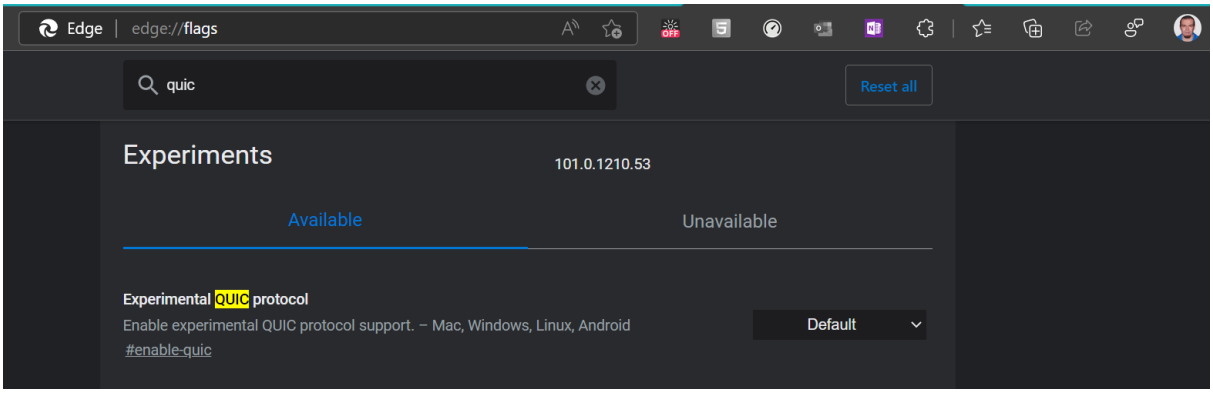


Figura 30: Comando que se utiliza para acceder a las banderas de configuración de Microsoft Edge para activar o desactivar varios servicios de navegación web, entre ellos es posible controlar el protocolo QUIC UDP

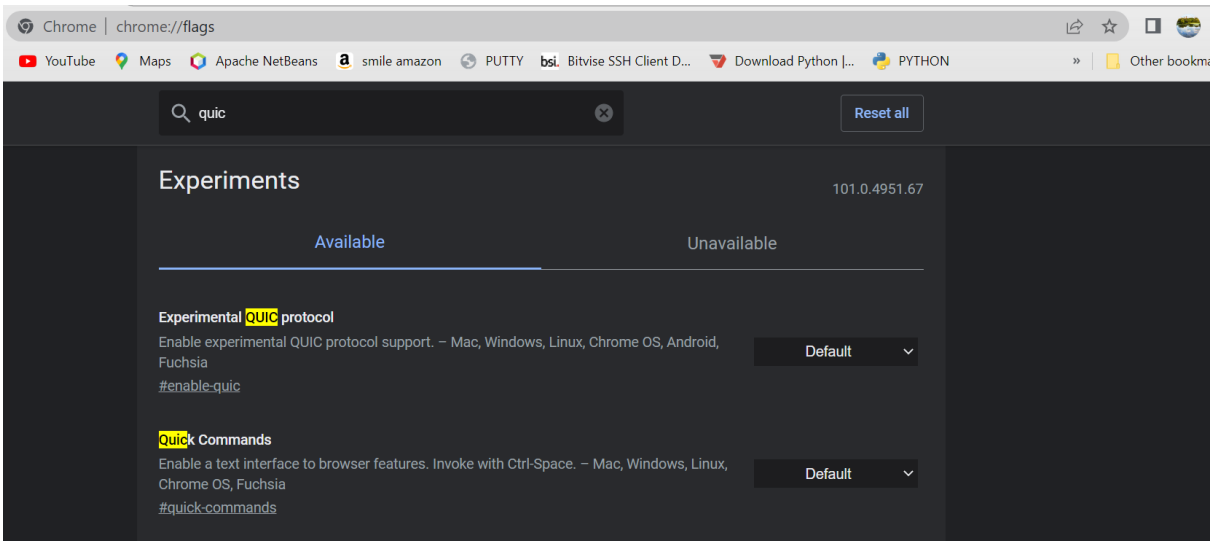


Figura 31: Comando que se utiliza para acceder a las banderas de configuración de Google Chrome para activar o desactivar varios servicios de navegación web, entre ellos es posible controlar el protocolo QUIC UDP

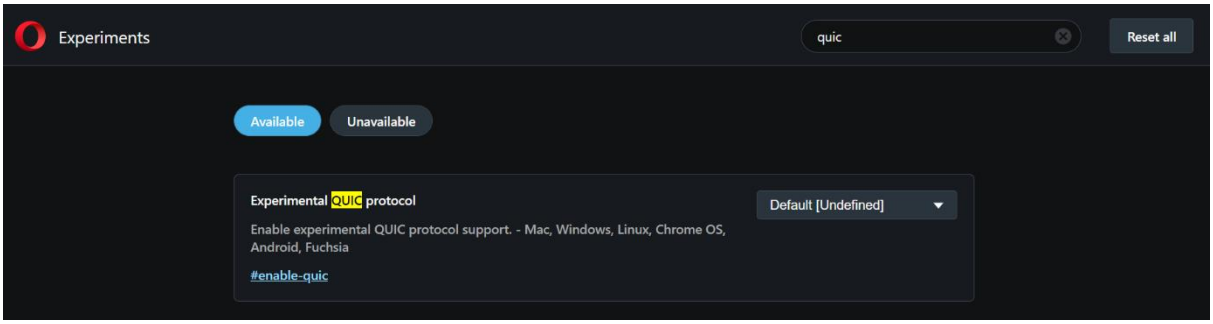


Figura 32: Comando que se utiliza para acceder a las banderas de configuración de Opera para activar o desactivar varios servicios de navegación web, entre ellos es posible controlar el protocolo QUIC UDP

La persona usuaria final tiene control sobre la navegación web desplegada en su entorno. Si la solución de la infraestructura de la empresa está orientada a los servidores de Google y al Cloud de Google por defecto utiliza los servicios de Google y sus servidores. Esto quiere decir que protocolos como HTTP, SPDY y TLS ya están activados para navegar con más eficiencia. Con esto es posible entender que la arquitectura de QUIC UDP está en uso y acoplada con el modelo tradicional TCP/IP.

5.0.2 Principales características técnicas

- Mejorar la latencia de la conexión.
- Mecanismos de control de congestión.
- Corrección de los errores de paquetes para evitar la retransmisión.

5.0.3 Cómo se debe implementar

La implementación de este protocolo es rápida y es posible afirmar que ya está servido por defecto en los navegadores web. Con un simple comando es posible acceder a activarlo y utilizando herramientas de pruebas de penetración se puede comprobar su implementación y uso adecuado de los protocolos de la red en uso.

5.0.4 Beneficios técnicos y económicos

Beneficios técnicos o ventajas:

- Rápida conectividad.
- Permite conexiones multiplexadas.
- Adjudicación de números de secuencia únicos.
- Corrección de errores hacia delante.
- Control de sobrecargas.
- Autenticación y codificación.
- Independencia del *hardware* (Digital Guide IONOS, s. f.).

Beneficios económicos:

- Ahorro en infraestructura al no tener que comprar servidores nuevos para un uso esencial.
- Ahorro en centro de datos en infraestructura física para pequeñas o medianas empresas.
- Adoptar la nube de Google como una solución de un todo en uno, en el ámbito de redes, servidores, código, bases de datos, seguridad, acceso remoto, el precio se reduce lo necesario y se agregan recursos de acuerdo con el crecimiento de la empresa.

5.0.5 Por qué se debe implementar este protocolo QUIC UDP

Este protocolo es muy visionario, los empresarios que cuentan con un buen grupo de trabajo con una visión hacia el futuro recomendarán usar este tipo de protocolo porque significa un gran aporte y mucha innovación para el futuro de las redes. Además, tiene una ventaja competitiva en los centros de datos y también en los negocios de servicios máximos a gran escala para proporcionar servicios de más calidad en audio y video.

5.0.6 Pasos para implementar el QUIC UDP

Los pasos para implementar QUIC UDP son prácticos y accesibles según la necesidad final de la empresa.

Se puede implementar en el ámbito de navegación web, como realizar una migración completa a la nube de Google.

Revisar el escenario 1 y el escenario 2 para obtener una mejor compresión de la implementación del QUIC UDP.

5.0.7 Cómo trabajan los diagramas de arquitectura

Los diagramas de arquitectura que se utilizan en esta investigación son una visión resumida de la conectividad de red. Lo anterior para que sea más fácil o agradable de leer para otros ingenieros, arquitectos o un lector general que quiera conocer del documento terminado y tener un detalle más rápido de la información de interés.

5.0.8 Descripción de escenarios

De acuerdo con lo expresado en el punto 5.0, 5.0.1, 5.0.2, 5.0.3, 5.0.4, 5.0.5, 5.0.6 y 5.0.7, es posible enfocarse en una solución que describe dos escenarios, para entender la situación actual en la viabilidad del Google QUIC UDP, en las empresas costarricenses.

5.0.2 Introducción del escenario 1

El escenario 1 plantea una situación en la cual el empresario, usuario o empleado normal de un centro de datos no tiene claro cómo trabaja el QUIC UDP, para mejorar la funcionalidad de su empresa o actualizar la seguridad de su infraestructura. En el punto 5.1.2.1, que es la situación actual, se describe la

información generada en la encuesta que se hizo en el punto 3.6.1, además, se hace una síntesis de esa información para entender mejor el escenario 1.

5.1 Escenario 1

Implementación del Google QUIC en las empresas costarricenses mediante la aplicación de los resultados en la encuesta y transferirlo a un centro de datos moderno.

5.1.2 Situación actual

5.1.2.1 Usuarios finales

La situación actual es que muchos usuarios finales no conocen sobre el Google QUIC UDP. Tampoco hay un entendimiento sobre cómo trabajan los certificados en las redes, la autentificación de claves ni cómo es la arquitectura de los protocolos en las redes para TCP, UDP y QUIC.

5.1.2.2 Problema de latencia

Se presenta un gran problema de latencia en las redes, solo un porcentaje de personas que están en la Gran Área Metropolitana tiene más opciones a servicios de más calidad, en provincias lejanas en el mismo país se complica la conectividad. No hay muchas personas que entiendan sobre protocolos de red o el conocimiento es bajo, por ende, se debe hacer un refrescamiento sobre cómo trabaja el modelo OSI en una red y cómo adaptar el protocolo QUIC en un centro de datos y forma local con los usuarios finales.

5.1.2.3 Desconocimiento de navegadores

Hay un gran desconocimiento sobre cómo trabajan los navegadores web en el ámbito empresarial y qué beneficios le dan al usuario final en su trabajo diario. La misma situación se traslada al uso de dispositivos móviles, hay un grupo de

personas que entienden cuál navegador web les da mejor rendimiento en el entorno de dispositivos móviles y cómo sacar mejor rendimiento de esas aplicaciones web que están corriendo en su sistema operativo, pero hay otras que todavía tienen dificultades y necesitan ayuda.

5.1.2.4 Actualizar el centro de datos

No muchas empresas estarían dispuestas a actualizar su centro de datos que puede estar obsoleto y con serios problemas de seguridad. Al adoptar tecnología pura de Google y mover su información con una arquitectura moderna como la que ofrece Google QUIC, se debe hacer un reforzamiento sobre protocolos de seguridad como el HTTP, el TLS, el QUIC UDP y entender sus diferentes versiones.

5.1.3 Propuesta de solución

5.1.3.1 Diseño uno

Propuesta de solución, diseño de arquitectura uno, que se basa en un centro de datos local migrado a la nube de Google.

5.1.3.1.2 Riesgos en la viabilidad del diseño uno.

Cuántos riesgos se tienen en la viabilidad de la solución que se basa en el siguiente diagrama de arquitectura.

Introducción al diagrama de arquitectura:

El siguiente diagrama es para entender cómo una empresa con diferentes pisos en el edificio y con usuarios finales conectados a la red de la compañía puede enviar todo el tráfico de navegación web, utilizando la arquitectura del Google QUIC UDP. Al final puede realizar una migración al Cloud de Google y utilizar los servicios y servidores de Google corriendo sobre QUIC UDP.

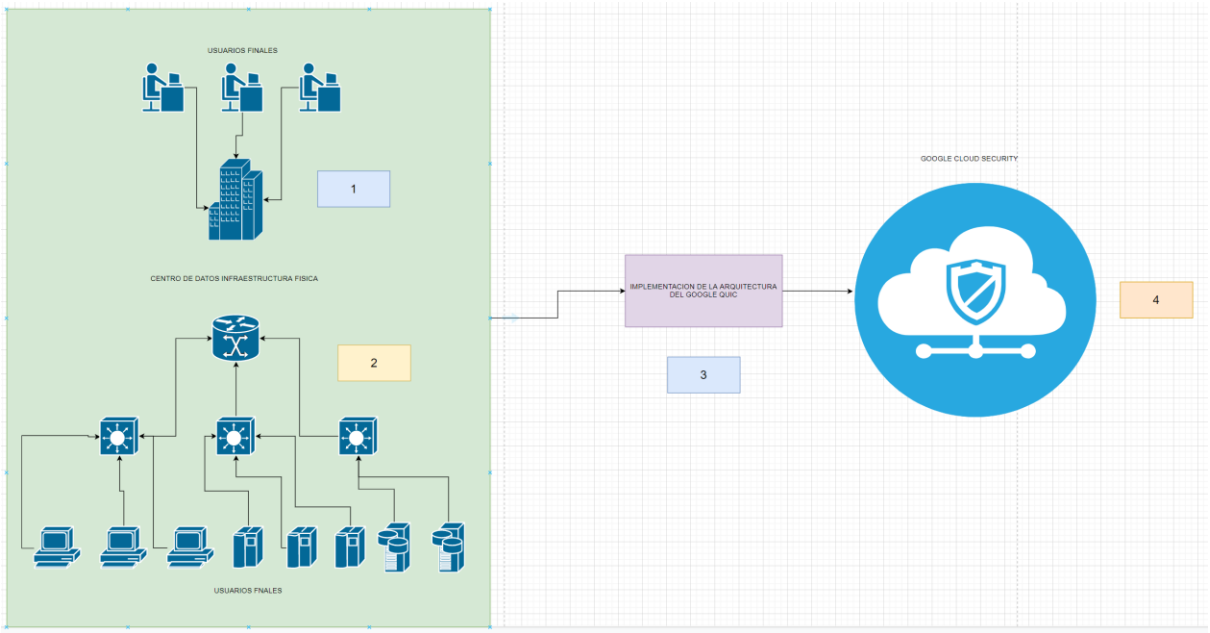


Figura 33: Diagrama de arquitectura

Este diagrama trabaja de la siguiente forma, en el punto 1 es donde están concentradas las conexiones de red distribuidas por cada nivel o piso, en donde los usuarios finales solicitarán acceso a la red. El punto 2 se enfoca en el centro de datos y cómo los dispositivos de red están interconectados y cómo cada Desktop, PC, servidor pertenece a una segmentación de red. En el punto 3 se hace una combinación del TCP/IP con el Google QUIC UDP para trabajar con las capas de red, transporte, seguridad y aplicación y enviar o solicitar información al Cloud de Google. El punto 4 es el Cloud de Google en donde se tiene toda la infraestructura virtual y se puede disponer de los servicios de Google para correr con una eficiencia mucho mejor con el protocolo QUIC UDP y hacer las migraciones necesarias con los requerimientos y solo correr dentro del Cloud de Google.

5.1.3.2 Diseño dos

Propuesta de solución, diseño de arquitectura dos, que se basa en un centro de datos de Azure migrado a la nube de Google.

5.1.3.2.1 Riesgos en la viabilidad del diseño dos

Cuántos riesgos se tienen en la viabilidad de la solución que se basa en el siguiente diagrama de arquitectura.

Introducción del diagrama de arquitectura:

El siguiente diagrama es para entender una migración del Cloud de Azure al Cloud de Google en donde todos los requerimientos de navegación web se consideran por medio del QUIC UDP.

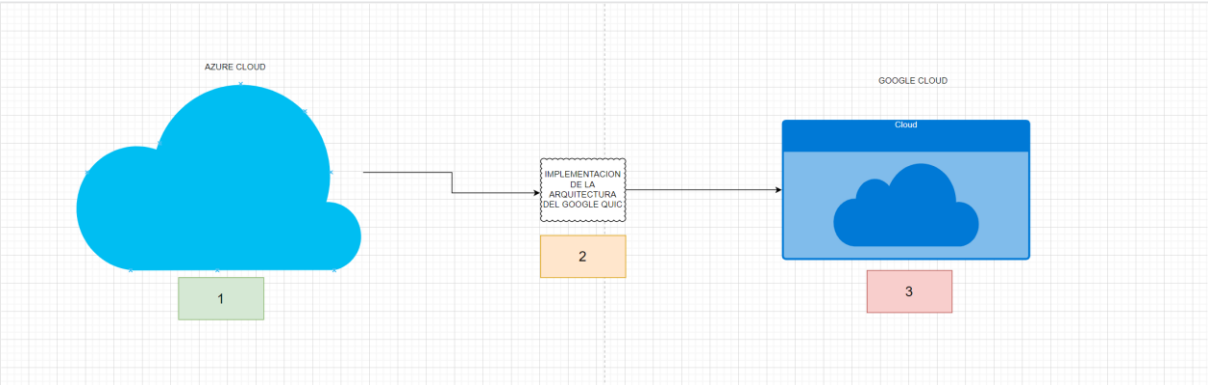


Figura 34: Diagrama de arquitectura

Este diagrama trabaja de la siguiente forma, en el punto 1 se tiene el centro de datos virtual utilizando todos los recursos de Microsoft, mediante la tecnología de Azure. En el punto 2 se tiene la combinación del modelo de redes TCP/IP y QUIC UDP en las capas de red, transporte, seguridad y aplicación y es donde se migrarán todos los requerimientos de Azure al Cloud de Google y se hace la traducción de navegación web con mejor latencia y seguridad. En el punto 3 se recibe toda la información de la migración y el cliente final trabaja solo con tecnología de Google y tiene mejores recursos en servicios y servidores. Al mismo tiempo, logra tener un ambiente de manejo con QUIC UDP, dentro la plataforma virtual de Google.

5.1.4 Evaluación de solución

Riesgos:

La Tabla 7 ayuda a entender los riesgos asociados en una red de comunicaciones que mantiene un modelo tradicional de navegación de datos mediante el protocolo TCP/IP entre dos servicios de nube, uno de ellos Azure y el otro Google, en donde se tiene de intermediario y negociador el QUIC UDP. Se describe la probabilidad de que suceda ese riesgo, así como el impacto y el peso de ese riesgo si sucede. Al mismo tiempo, se busca entender qué acción se debe tomar y cuál es el plan de acción para seguir, en donde se plantea en muchos casos implementar la arquitectura QUIC UDP, como la solución para solucionar ese riesgo.

Tabla 7: Identificación del riesgo con su probabilidad, impacto, peso del riesgo y acciones por seguir

ID -Riesgo	Probabilidad (alta, mediana y baja)	Impacto (alto, mediano y bajo)	Peso del riesgo (alto, mediano y bajo)	Acción	Plan de acción (responsable)
R001 – HTTP navegación web no segura protocolo obsoleto	Mediana	Alto	Alto	Actualizar al http/3	Implementar la arquitectura del Google QUIC UDP
R002 – TLS navegación web no segura protocolo obsoleto	Mediana	Alto	Alto	Actualizar el TLS/3	Implementar la arquitectura del Google QUIC UDP
R003 – DDOS ataque de	Alto	Alto	Alto	Utilizar DOTS-ARCH	Implementar la arquitectura del Google QUIC UDP

ID -Riesgo	Probabilidad (alta, mediana y baja)	Impacto (alto, mediano y bajo)	Peso del riesgo (alto, mediano y bajo)	Acción	Plan de acción (responsable)
navegación de servicio distribuido					para evitar los ataques de DDOS
R004 – Detección de pérdidas y control de congestión	Alto	Alto	Alto	Utilizar el diseño de transporte del QUIC UDP	Implementar la arquitectura del Google QUIC UDP
R005 – Seguridad de Infraestructura	Mediano	Alto	Alto	Configuración correcta de capa 2, MAC, ARP, VLAN, STP	Implementar la arquitectura del Google QUIC UDP

5.1.5 Arquitectura recomendada de solución

5.1.5.6 Diseño en la nube

La arquitectura recomendada es un diseño en la nube, pero que también se ajusta a la infraestructura física, adaptando la arquitectura del Google QUIC UDP en la solución de los riesgos mencionados.

Introducción del diagrama de arquitectura:

El siguiente diagrama de arquitectura es una unificación de tecnologías, las que se tienen en el Cloud como AWS, AZURE, Cisco, IBM y las que es posible tener en un centro de datos físico. Todas estas se unificarán en un punto de concentración y se canalizarán mediante el Google QUIC UDP y migrado al Cloud de Google con todos los requerimientos pertinentes.

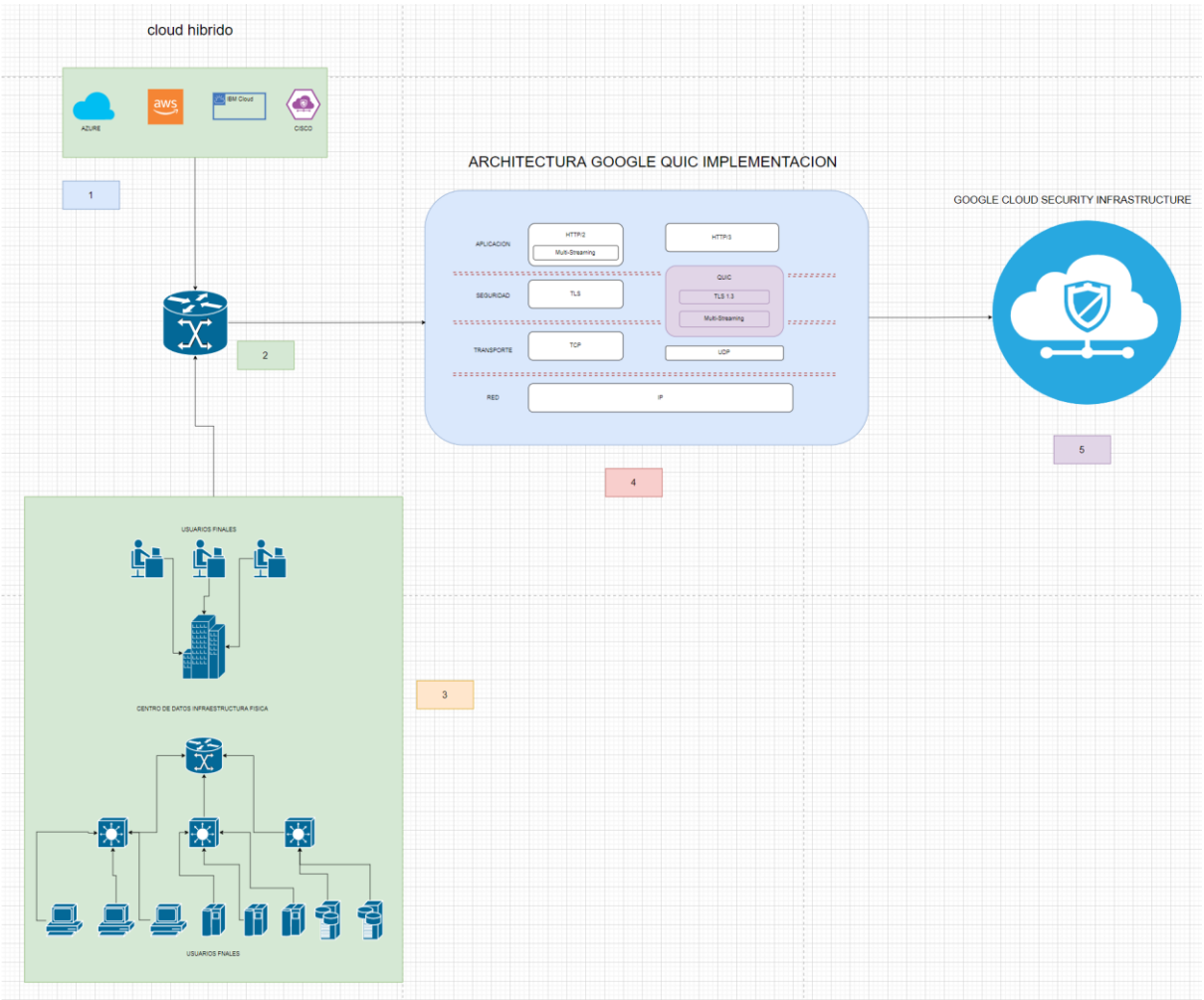


Figura 35: Diagrama de arquitectura

Este diagrama trabaja de la siguiente forma, en el punto 1 se tienen las diferentes tecnologías de Cloud más importantes del mercado. Todos estos centros de datos virtuales se interconectarán en la unificación de redes que está en el punto 2 y de esta forma se toma toda la información de la infraestructura física que está en el punto 3 y se lleva al punto 2. Después se toma la información del punto 1, el punto 3 y por medio del punto 2, se une al punto 4, en donde se tiene la arquitectura del Google QUIC UDP para las capas de red, transporte, seguridad y aplicación.

En este punto todavía se necesita la combinación del modelo tradicional de redes TCP/IP, pero trabaja en paralelo con el QUIC UDP, para dar mejor rendimiento en latencia de red y mejor seguridad en la navegación web. En el punto 5 se recibe toda la migración completa, ya sea física o virtual, pero tiene todas esas infraestructuras en un solo punto con mejores servicios de Google y utilizan servidores que son solo tecnología de Google y todos se mueven por medio de QUIC UDP.

5.1.6 Informe y seguimiento

5.1.6.1 Informe

El Departamento Técnico de Tecnología de Información debe utilizar el esquema de evaluación propuesto para realizar la auditoría correspondiente y darle al cliente final una mejor orientación del estado actual de sus equipos. Lo anterior para que la propuesta de solución se mantenga, se haga el análisis de riesgos correspondientes y que la arquitectura recomendada tenga la viabilidad para su implementación final, así los resultados son los correctos y la solución de arquitectura es la adecuada. El informe se ejecuta mediante un auditor de nivel técnico para que el criterio en las respuestas sea el más adecuado.

5.1.6.2 Seguimiento

El seguimiento que se le debe dar al esquema de evaluación es cumplir con las acciones que se recomiendan. Por ejemplo, hacer auditorías cada tres meses con un seguimiento en paralelo por mes con el equipo de ciberseguridad, para tener siempre bajo control los riesgos observados y que la implementación de arquitectura se sostenga o, en el mejor de los casos, se den recomendaciones de mejora, si estas aplican.

5.1.6.3 Introducción del escenario 2

El escenario 2 quiere plantear una situación en la cual el administrador de red en un centro de datos puede utilizar herramientas de penetración de pruebas. Lo anterior para hacer un análisis de red, estudiar los protocolos que se usan y cómo asegurará la navegación web al estar consciente que utiliza motores de búsqueda de Google para navegar con el QUIC UDP en sus navegadores web, así como crear un escudo de ciberseguridad mejor y reducir la lentitud en la red.

5.2 Escenario 2

Implementación del Google QUIC en las empresas costarricenses mediante la aplicación de herramientas analíticas de red y transferirlo a un centro de datos moderno.

5.2.1 Situación actual

Las empresas en Costa Rica no analizan o revisan cómo opera su red actual con respecto al tráfico de información, solo las compañías con un alto compromiso con el cliente final realizan verificaciones de desempeño en su centro de datos. Tampoco sacan el mejor aprovechamiento a sus navegadores web ni hay una

cultura orientada sobre los navegadores web y cuáles son mejores en los sistemas operativos.

Por lo tanto, se debe hacer una orientación sobre cómo utilizar herramientas de penetración de pruebas, que dan una gran visualización sobre el estado de los protocolos y un punto de entendimiento sobre si se corren protocolos obsoletos que deben actualizarse en el centro de datos e identificar si el QUIC IETF está corriendo correctamente en los navegadores que utilizan como motor de búsqueda. En cuanto al navegador de Google, ya sea Opera, Firefox, Safari, Edge, se debe dar un entrenamiento esencial sobre el Wireshark y una breve orientación sobre cómo migrar a los servicios de Google en la nube y adoptar esta solución para tener un mejor uso de las empresas hacia el cliente final.

5.2.2 Propuesta de solución

5.2.2.2 Integración del QUIC UDP

Propuesta de solución que se basa en la integración del Google QUIC UDP como motor de búsqueda en los navegadores web y asegurarse de los protocolos correctos.

Introducción del diagrama de arquitectura:

El siguiente diagrama de arquitectura envía información desde los diferentes equipos físicos o virtuales utilizando distintos sistemas operativos en donde se controla la navegación web. De esta forma, se envían los datos a las arquitecturas TCP/IP combinando la arquitectura del QUIC UDP, pero con énfasis en la navegación web. Después se realizan unas pruebas de penetración, para entender el estado de los protocolos de red, repitiendo el ciclo de retroalimentación en la red y estar seguros de que el QUIC UDP realiza su función correspondiente, con respecto a seguridad y latencia.

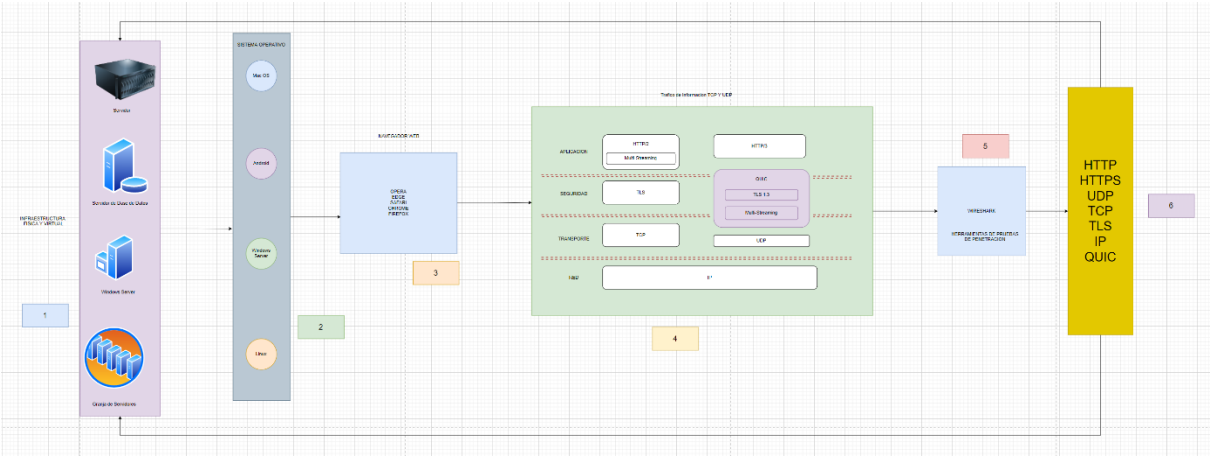


Figura 36: Diagrama de arquitectura

El siguiente diagrama trabaja de la siguiente forma, en el punto 1 lo que se tiene son los servidores, ya sean físicos o virtuales, instalados en los centros de datos y a disposición de ciertos departamentos. En el punto 2 están los sistemas operativos, ya sea Windows, Linux, Mac OS, Android, que corren en los servidores que están en el punto 1. En el punto 3 se tienen los navegadores web, que son aplicaciones que corren en los servidores del punto 1.

La información que se genera en el punto 1, 2 y 3 se envía al punto 4, que son las arquitecturas de control de transporte de TCP/IP y la combinación con QUIC UDP agregando mejor capacidad para la navegación web en seguridad y latencia. El punto 4 envía toda esta información de tráfico relacionado con el modelo OSI y se captura en el punto 5, en donde están las herramientas de pruebas de penetración por medio de la herramienta Wireshark que ayuda a entender que los protocolos de red son los correctos y tener seguridad que QUIC UDP está corriendo en la forma más adecuada. En el punto 6 se tiene esta información capturada en pantalla de acuerdo con la salida del Wireshark del punto 5.

5.2.3 Evaluación de la solución

Riesgos:

La Tabla 8 describe los riesgos asociados en una infraestructura física o virtual que está en el centro de datos, en donde se analiza con herramientas de pruebas de penetración para entender los protocolos en acción usados y presenta los riesgos asociados en esa red de comunicaciones con un modelo tradicional TCP/IP. Cada riesgo presenta una probabilidad de que suceda ese riesgo, un impacto sobre este, cuál es el peso en la red, cuál es la acción rápida por tomar y cuál es el plan de acción correcto, en donde es posible mitigar ese riesgo mediante la arquitectura QUIC UDP, que es una solución final a todos esos riesgos.

Tabla 8: Identificación del riesgo con su probabilidad, impacto, peso del riesgo y acciones para seguir

ID -Riesgo	Probabilidad (alta, mediana y baja)	Impacto (alto, mediano y bajo)	Peso del riesgo (alto, mediano y bajo)	Acción	Plan de acciones (responsable)
R001 – HTTP/2	Mediano	Alto	Alto	Actualizar al http/3	Implementar la arquitectura del Google QUIC UDP
R002 - HTTP/1	Alta	Alto	Alto	Actualizar al http/3	Implementar la arquitectura del Google QUIC UDP
R003 – TLS/1.2	Alta	Alto	Alto	Actualizar al TLS1.3	Implementar la arquitectura del Google QUIC UDP
R003 – TLS.1.1	Alta	Alto	Alto	Actualizar al TLS1.3	Implementar la arquitectura del Google QUIC UDP

ID -Riesgo	Probabilidad (alta, mediana y baja)	Impacto (alto, mediano y bajo)	Peso del riesgo (alto, mediano y bajo)	Acción	Plan de acciones (responsable)
R004 -Servidores Seguros	Alta	Alto	Alto	Remover infraestructura obsoleta	Hacer un inventario de equipos que tienen más de 5 años de uso. Las instalaciones iniciales de los servidores deben ser por las personas correctas y autorizadas y, por último, implementar la arquitectura del Google QUIC UDP, para desplazar el modelo tradicional TCP/IP

ID -Riesgo	Probabilidad (alta, mediana y baja)	Impacto (alto, mediano y bajo)	Peso del riesgo (alto, mediano y bajo)	Acción	Plan de acciones (responsable)
R005 -Filtrado de paquetes	Alta	Alto	Alto	Configuración correcta de los enrutadores de red y conmutadores	El especialista de red debe configurar correctamente los enrutadores, para descartar paquetes de dudosa procedencia y realizar supervisión constante de la red, hacer revisión de *logs* y análisis periódico de los archivos de configuración de esos enrutadores como

ID -Riesgo	Probabilidad (alta, mediana y baja)	Impacto (alto, mediano y bajo)	Peso del riesgo (alto, mediano y bajo)	Acción	Plan de acciones (responsable)
					también de los conmutadores y, por último, implementar la arquitectura de Google QUIC UDP, para desplazar el modelo viejo o tradicional de TCP/IP.
R006 -Escaneo de puertos	Alta	Alto	Alto	Revisión de capa 4 o de transporte de los protocolos TCP y UDP	El especialista en redes debe hacer un barrido constante de puertos para tener el listado de posibles debilidades en

ID -Riesgo	Probabilidad (alta, mediana y baja)	Impacto (alto, mediano y bajo)	Peso del riesgo (alto, mediano y bajo)	Acción	Plan de acciones (responsable)
					el flujo o tráfico de datos y si se detectan debilidades, hacer pruebas de penetración con herramientas como Wireshark, actualizar los protocolos web TLS y HTTP, mediante la implementación de navegadores que usen la arquitectura Google QUIC UDP.

ID -Riesgo	Probabilidad (alta, mediana y baja)	Impacto (alto, mediano y bajo)	Peso del riesgo (alto, mediano y bajo)	Acción	Plan de acciones (responsable)
R007 -Protocolos de enrutamiento	Alta	Alto	Alto	Hacer revisión de protocolos OSPF, RIP, EIGPR, BGP, etc.	El especialista de red debe hacer una revisión de todos los protocolos de enrutamiento y descartar las posibles debilidades de esos protocolos a nivel de enrutador. Muchos recomiendan quitar el protocolo RIP por otro más seguro como el OSPF o el EIGRP. Después de esta

ID -Riesgo	Probabilidad (alta, mediana y baja)	Impacto (alto, mediano y bajo)	Peso del riesgo (alto, mediano y bajo)	Acción	Plan de acciones (responsable)
					revisión implementar la arquitectura del Google QUIC UDP, para desplazar el modelo TCP/IP tradicional.
R008 -Sistemas de detección de intrusos	Alta	Alto	Alto	Sistemas diseñados con base en la nueva arquitectura de QUIC UDP	Con la implementación del Google QUIC UDP los sistemas de detección de intrusos pueden ir más allá a un nivel de avanzada superior, porque da mayor rapidez de red, o

ID -Riesgo	Probabilidad (alta, mediana y baja)	Impacto (alto, mediano y bajo)	Peso del riesgo (alto, mediano y bajo)	Acción	Plan de acciones (responsable)
					sea, mayor manejo de movimiento de datos, seguridad y manejo de carga a alto volumen, lo que da mejor empoderamiento a esos sistemas que pueden usar alguna inteligencia artificial.
R009 -Control de servicios	Mediana	Alto	Alto	Remover servicios innecesarios	El especialista de red hace un estudio, en este caso de servicios de web obsoletos, y

ID -Riesgo	Probabilidad (alta, mediana y baja)	Impacto (alto, mediano y bajo)	Peso del riesgo (alto, mediano y bajo)	Acción	Plan de acciones (responsable)
					puede proponer saltar a la actualización de la arquitectura de Google QUIC UDP para tener mejor seguridad y velocidad de navegación web, usando la última versión TLS 1.3 y HTTP/3
R010 -Deshabilitar protocolos no seguros	Alta	Alto	Alto	Actualizar el TLS, HTTP o cualquier otro protocolo que está corriendo con	Los administradores de red deben hacer un barrido de equipos capa 2 y capa 3 como

ID -Riesgo	Probabilidad (alta, mediana y baja)	Impacto (alto, mediano y bajo)	Peso del riesgo (alto, mediano y bajo)	Acción	Plan de acciones (responsable)
				aplicaciones ya obsoletas.	conmutadores y enrutadores y, al mismo tiempo, hacer un estudio de aplicaciones que corren en servidores obsoletos y solucionar problemas de seguridad asociados con esos servidores instalados en el centro de datos y remover o actualizar protocolos obsoletos.

ID -Riesgo	Probabilidad (alta, mediana y baja)	Impacto (alto, mediano y bajo)	Peso del riesgo (alto, mediano y bajo)	Acción	Plan de acciones (responsable)
R011 - No usar protocolos de control de Cisco	Mediana	Mediano	Mediano	Implementar tecnología Cisco.	Los arquitectos de redes pueden recomendar ampliar el uso de protocolos de control de Cisco para que las topologías empleadas y la estructura del modelo OSI se mantengan seguras en el ámbito de intrusiones o vulnerabilidades, así se tiene control de tráfico

ID -Riesgo	Probabilidad (alta, mediana y baja)	Impacto (alto, mediano y bajo)	Peso del riesgo (alto, mediano y bajo)	Acción	Plan de acciones (responsable)
					buena integridad de datos, para complementar todavía mejor la arquitectura del QUIC UDP.

5.2.4 Arquitectura recomendada de solución

5.2.4.1 Utilización de infraestructura física o virtual

Con infraestructura física o virtual, navegando en el sistema operativo y después haciendo un acople a la arquitectura de Google QUIC UDP, con herramientas de pruebas de penetración se asegura de que la infraestructura está navegando a nivel web sobre el QUIC UDP. Se recomienda como complemento utilizar protocolos de control de Cisco, de esta forma, se hace el acople al Cloud de Google como solución final y se completa todo el proceso de la migración a solo tecnología Google.

Introducción al diagrama de arquitectura:

El siguiente diagrama de arquitectura envía información de los servidores que están ubicados en el centro de datos físico o virtual y en cada servidor pueden correr diferentes sistemas operativos y estos con distintos navegadores web. Esta información la procesa el modelo de red TCP/IP y trabaja junto con QUIC UDP.

Después se tiene una herramienta de pruebas de penetración que ayuda a comprender los protocolos usados y visualizados en pantalla. Para tener una mejor seguridad se complementa con los protocolos de control de Cisco para tener una migración exitosa al Cloud de Google y correr con el QUIC UDP en todos los servicios que ofrece Google, instalado ya en sus servidores. Por lo tanto, se tiene mejor desempeño del QUIC UDP en un ambiente diseñado para el protocolo.

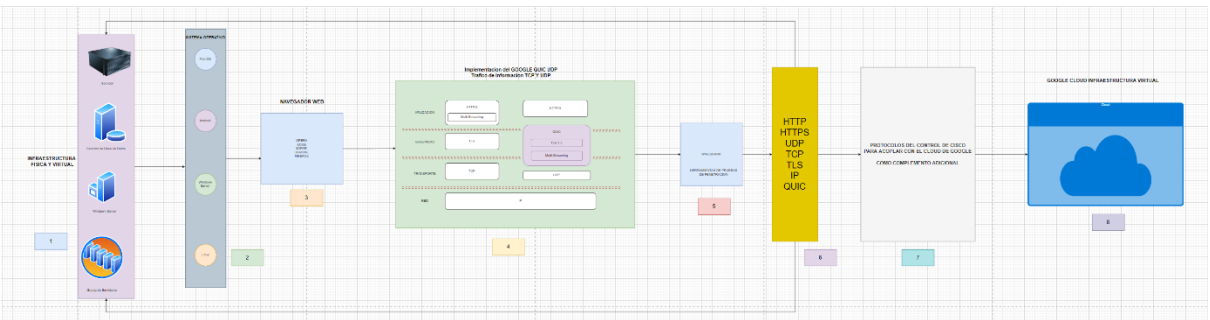


Figura 37: Diagrama de arquitectura

El siguiente diagrama trabaja de la siguiente forma, en el punto 1 se tiene la infraestructura física o virtual en donde están los servidores del centro de datos. En el punto 2 están corriendo los diferentes sistemas operativos hospedados en el punto 1 y estos permitirán utilizar las distintas aplicaciones web que están el punto 3, ya sea para Edge, Opera, Google Chrome. El punto 4 absorbe toda la información, saliente del punto 3 y da una interpretación de los protocolos de red que se utilizan para que la arquitectura TCP/IP trabaje junto con el QUIC UDP y dé mejor rendimiento en el ámbito de navegación web, lo que reduce latencia y aumenta seguridad.

En el punto 5 se utiliza el Wireshark que es la herramienta de pruebas de penetración para capturar los protocolos de red que están visualizados en el punto 6 y asegurarse de que el QUIC UDP trabaja en forma adecuada. En el punto 7 se utilizan los protocolos de control de Cisco para dar una mejora en la calidad en seguridad adicional y hacer una migración exitosa en el punto 8, que es donde está el Cloud de Google con todos los servicios y servidores para que el QUIC UDP pueda operar de forma correcta sin inconvenientes al tener toda la gobernanza de Google en su centro de datos virtual.

5.2.5 Informe y seguimiento

5.2.5.1 Informe

Este informe es prácticamente igual al que se ejecutó en el punto 5.1.6.1, pero el enfoque aquí cambia un poco al utilizar herramientas de pruebas de penetración y protocolos de control de Cisco. Los resultados son más analíticos y profundos, lo que da un criterio desde otro punto de vista al auditor final en donde

puede presentar más ideas de solución para mejorar la infraestructura que se utiliza en ese momento.

5.2.5.2 Seguimiento

El seguimiento recomendado es seguir con lo propuesto en el punto 5.1.6.2, pero se aumentan un poco más las tareas para los equipos de ciberseguridad al tener que analizar más las herramientas de pruebas de penetración y también un extraanalítico en las herramientas de protocolos de control de Cisco.

5.3 Esquema de evaluación

Propuesta de solución aplicando un esquema de evaluación, para el escenario 1 y el escenario 2, guía de orientación para el cliente final, como complemento extra o una auditoría final.

5.3.1 Esquema de evaluación para el escenario 1 y el escenario 2

La Tabla 9 explica una unificación de la solución de los dos escenarios, al aplicar un esquema de evaluación. Esta es una guía paso a paso que debe aplicar el ingeniero de redes en un centro de datos y presentar resultados finales a la dirección de arquitectura para hacer las correcciones definitivas, seguir con el mantenimiento adecuado y promover la constante actualización.

Tabla 9: Esquema de evaluación para QUIC UDP pasos para evaluar la arquitectura del centro de datos

No de Pregunta	Pregunta	Acciones por tomar	Resultado	Análisis final	Comentarios de mejoras si aplica.
1	Estado actual del inventario físico de servidores.	Hacer un barrido de qué tipo de tecnología son los servidores, Oracle, IBM, HP, Dell, Hitachi.	Cuántos hay de tecnología X86. Cuántos hay como *mainframe*. Cuántos hay de otros tipos como tipo M, tipo T, Superdome.	Con el estado actual de la infraestructura física se hace un reconocimiento o análisis de cuáles equipos ya están fuera de uso con *hardware* que pone en riesgo el centro de datos y que los parches de seguridad	1. Aislador equipos obsoletos. 2. No mezclar tecnologías. 3. No reinstalar sistemas operativos con *hardware* obsoleto. 4. Hacer un barrio de la configuración

No de Pregunta	Pregunta	Acciones por tomar	Resultado	Análisis final	Comentarios de mejoras si aplica.
				aplicados al sistema operativo ya están obsoletos. Por lo tanto, esos equipos como recomendación deben aislarse y sustituirse por otros mejores.	de red y sus VLAN para encontrar debilidades.
2	Estado actual del inventario virtual de servidores.	Hacer un barrido de cuántas máquinas virtuales están	Cuántas máquinas virtuales hay, cuáles están albergadas en tecnología X86, Oracle,	Con el estado actual del inventario virtual Se deben migrar	1. Revisar las tecnologías de *hardware* y cuántas

No de Pregunta	Pregunta	Acciones por tomar	Resultado	Análisis final	Comentarios de mejoras si aplica.
		corriendo en cada *hardware* y reconocer el *hardware* obsoleto que ya no debe albergar esas VM y cuáles deben migrarse a un mejor equipo.	Dell, HP y cuántas mezclas de equipos hay con tecnologías diferentes que no se pueden hablar correctamente.	las máquinas virtuales a una mejor tecnología más adecuada para crear virtualización y que presente una buena escalabilidad y flexibilidad para crecer en el futuro y tener todas las prevenciones de	combinaciones de VM hay. 2. Mover las VM a las tecnologías más adecuadas. 3. Instalar equipos que se pueden extender en el futuro con flexibilidad y escalabilidad.

No de Pregunta	Pregunta	Acciones por tomar	Resultado	Análisis final	Comentarios de mejoras si aplica.
				demandas tecnológicas actuales, no realizar cuellos de botella innecesarios.	
3	Conocimiento sobre navegadores web.	Revisar las aplicaciones web que están corriendo en el sistema operativo, cuáles aplicaciones web le pueden	Entendiendo el uso de las aplicaciones web como Edge, Chrome, Opera, Safari, Firefox, ver los resultados estadísticos que se pueden consultar 48+web Browser	Utilizar fuentes de información válidas para ver resultados estadísticos sobre la evolución de las aplicaciones web	Revisar el rendimiento de los navegadores web con el administrador de red.

No de Pregunta	Pregunta	Acciones por tomar	Resultado	Análisis final	Comentarios de mejoras si aplica.
		responder más rápido, qué tipo de *hardware* utiliza.	Statistics for 2022 | Interesting Browsers stats & Tips (ukwebhostreview.com) o también en web Browsers-Statistics & Facts | Statista en donde el Google Chrome es el mismo durante muchos años. Esto da una mejor orientación al usuario final de lo mejor por	para tener un mejor criterio y así utilizar con un mejor aprovechamiento	

No de Pregunta	Pregunta	Acciones por tomar	Resultado	Análisis final	Comentarios de mejoras si aplica.
			utilizar en su uso diario.		
4	Cómo migrar la infraestructura física o virtual al Cloud de Google.	Trabajar con un grupo de arquitectura de migración, ya sea local o subcontratado, que entienda los riesgos, suposiciones, problemas y dependencias, para tener una	No hay problemas de *firewall*. No hay latencia en la red. Las aplicaciones trabajan correctamente. Todas las dependencias se relacionan correctamente.	La latencia de red está dentro del rango permitido. Se puede volver a consultar datos en los servidores de la red antigua mientras se da la comunicación abierta en el *firewall*, si el	Realizar las pruebas necesarias para las aplicaciones correspondientes y estar seguro de que todo trabaja en la forma óptima.

No de Pregunta	Pregunta	Acciones por tomar	Resultado	Análisis final	Comentarios de mejoras si aplica.
		migración exitosa.	Correr en la nube da un mejor rendimiento y se puede crecer en el futuro.	cliente incluso requiere información de esa red.	
5	Cómo migrar otro servicio de nube como Azure o AWS al Cloud de Google.	De la misma forma que se trabajó con el centro de datos físico que alberga máquinas virtuales se utiliza el grupo de arquitectos de migración o	No hay problemas de puertos cerrados o *firewall*. Toda la segmentación de red está en el lugar correcto. Las aplicaciones trabajan bien con sus dependencias.	Aún se mantienen comunicaciones con las otras nubes. La red trabaja en forma óptima. Se utilizan mejores tecnologías de	El objetivo final es migrar al Cloud de Google y utilizar todos los beneficios que da el QUIC UDP debido a seguridad y latencia.

No de Pregunta	Pregunta	Acciones por tomar	Resultado	Análisis final	Comentarios de mejoras si aplica.
		subcontratando a una empresa para controlar los riegos, suposiciones, problemas y dependencias. De la misma forma esos arquitectos de migración deben especializarse en Azure, AWS y Google.	Hay mayor seguridad y escalabilidad y flexibilidad.	navegación con el QUIC UDP y todos los servicios y servidores de Google que están mejor adaptados al QUIC UDP.	

No de Pregunta	Pregunta	Acciones por tomar	Resultado	Análisis final	Comentarios de mejoras si aplica.
6	Cómo hacer pruebas de latencia en la red.	Se debe trabajar con el administrador de red para tener comprendida la ubicación fuente y destino y utilizar los comandos adecuados como ping, traceroute o tracert, según sistema operativo o dispositivo de	Respuesta rápida de todas las aplicaciones y mejor rendimiento en el uso diario de la consulta de datos. Mejor protección al estar en la segmentación adecuada. Mejor filtrado de paquetes. Por lo tanto, mejor operabilidad de los navegadores web.	El administrador de red debe hacer un estudio de la PC o servidor, ver las actualizaciones del sistema operativo, revisar configuración de la NIC, revisar la VLAN asignada, hacer una revisión del *firewall*, ubicar	El administrador de red debe recomendar usar las aplicaciones web adecuadas que se adapten mejor al QUIC UDP. La mejor tendencia de acuerdo con las estadísticas es usar el Chrome, pero todos los navegadores más importantes ya están disponibles con el QUIC UDP.

No de Pregunta	Pregunta	Acciones por tomar	Resultado	Análisis final	Comentarios de mejoras si aplica.
		red que se esté utilizando. Para tener un criterio adecuado sobre las salidas de esos comandos y tomar las acciones necesarias, como revisar la segmentación de red y analizar el diseño de la red		los equipos en el segmento de red más adecuado para navegar en la forma más eficiente.	

No de Pregunta	Pregunta	Acciones por tomar	Resultado	Análisis final	Comentarios de mejoras si aplica.
		para encontrar problemas de segmentación o *firewall* que todavía no se implementó correctamente.			
7	Saber cómo comprobar que la arquitectura del QUIC UDP opera correctamente.	Lo primero que hay que hacer es correr los comandos web recomendados en la propuesta de solución del	Los resultados son navegación web con latencia muy baja, mejor rendimiento de aplicaciones, aumento en la seguridad, mejor encriptación de datos.	De la misma forma se reduce la latencia para movilidad de datos a alto volumen y se espera que la	Si se da una adopción correcta con los servicios de Google la eficiencia empresarial es de mejor aprovechamiento

No de Pregunta	Pregunta	Acciones por tomar	Resultado	Análisis final	Comentarios de mejoras si aplica.
		Capítulo 5, para verificar que la configuración web del navegador ya está activa para el uso del QUIC UDP. Posteriormente, hacer un estudio esencial del *hardware,* lo recomendado en		seguridad sea la mejor al usar versiones mejoradas de TLS y HTTP.	porque la arquitectura QUIC UDP ya está en todos los servicios de Google.

No de Pregunta	Pregunta	Acciones por tomar	Resultado	Análisis final	Comentarios de mejoras si aplica.
		la pregunta n.º 1 y 2. Por último, con la ayuda del arquitecto de redes revisar que la arquitectura de red de QUIC UDP está disponible en los servicios de Google y que al agregar una PC o servidor la			

No de Pregunta	Pregunta	Acciones por tomar	Resultado	Análisis final	Comentarios de mejoras si aplica.
		adaptación se hará directa a la infraestructura global de Google.			
8	Después de realizar la migración utilizar los pasos correctos puede hacer pruebas adecuadas de sus aplicaciones.	Lo correcto es tener todos los equipos necesarios que soporten los procesos de pruebas y cómo hacer resolución de problemas si estos fueran	La migración se entrega en óptimas condiciones y con el mínimo de errores para que las aplicaciones trabajen adecuadamente, como fueron en los requerimientos	La red no presenta latencia, no hay problemas de seguridad y se pueden ingresar al uso de las aplicaciones de la cuenta en el sitio y en forma	Con todos los servidores virtuales en operación y todo el entorno de desarrollo sin problemas, lo que queda es seguir con el informe y seguimiento para asegurar una

No de Pregunta	Pregunta	Acciones por tomar	Resultado	Análisis final	Comentarios de mejoras si aplica.
		necesarios como Middleware, WebSphere, redes, balanceadores de carga, equipos de muros de fuego.	anteriores en la red original.	remota mediante la VPN correspondiente para los usuarios correctos.	operabilidad constante.
9	Puede comprender o analizar los riesgos involucrados en su centro de datos y qué acciones se deben seguir.	Lo mejor es revisar las dos tablas de riesgos que se utilizan en las siguientes secciones: 5.1.4 Tabla 7 y 5.2.3	Los mejores resultados se obtendrán siguiendo las acciones por tomar en las tablas de riesgos.	Las tablas de riesgos crearán el mejor camino para deducir un análisis final y proceder con el	El ingeniero de redes puede crear más ideas sobre cómo actuar de acuerdo con las acciones tomadas.

No de Pregunta	Pregunta	Acciones por tomar	Resultado	Análisis final	Comentarios de mejoras si aplica.
		Tabla 8. Con esto el ingeniero de redes tiene un panorama más amplio sobre cómo analizar los riesgos.		mejor camino de solución.	
10	Comprende cómo leer y analizar los protocolos web más esenciales del modelo OSI y mejorar la transferencia del	El ingeniero de red debe ser un profesional al menos certificado con el CCNA de Cisco o de otras tecnologías como	Los resultados son mejor diseño de redes, mejor asignación de VLAN, menos latencia, seguridad de mejor control y un enfoque de	Se harán estudios de los protocolos que se utilizan porque se debe implementar el QUIC UDP para	Al cliente final se le puede dar un mejor servicio, con mayor eficiencia.

No de Pregunta	Pregunta	Acciones por tomar	Resultado	Análisis final	Comentarios de mejoras si aplica.
	manejo de sus datos.	Palo Alto, Fortinet, etc. Así los criterios para entender el modelo OSI son más amplios y comprenden mejor la implementación del QUIC UDP y el manejo más adecuado de los datos.	utilidad en la red con mejor sustentación.	dar recomendaciones de saltar o adoptar la nube de Google.	

No de Pregunta	Pregunta	Acciones por tomar	Resultado	Análisis final	Comentarios de mejoras si aplica.
11	Entiendo la función básica de los protocolos de control de Cisco y por qué se debe usar.	Como una recomendación el ingeniero de redes debe utilizar esta solución de seguridad que cubre los diferentes niveles del modelo OSI y hacer migraciones incluso más	Hay un mejor control de tráfico y de integridad de datos y se presenta un mejor escudo a la arquitectura del QUIC UDP al disminuir las intrusiones o vulnerabilidades.	El barrido de los datos que se obtienen y sus salidas permitirán que el ingeniero de redes tome las acciones pertinentes para exponer como una buena opción. También implementar estos protocolos de control a la	Las conclusiones las tomará el CISO de la empresa junto con su equipo de seguridad.

No de Pregunta	Pregunta	Acciones por tomar	Resultado	Análisis final	Comentarios de mejoras si aplica.
		seguras a la nube de Google.		Junta Directiva de la empresa.	

Capítulo 6. Conclusiones y recomendaciones

6.1 Conclusiones

6.1.1 Conclusiones objetivos específicos

6.1.2 Conclusión objetivo n.º 1: Definir qué es el protocolo QUIC UDP. Este objetivo se alcanzó y se concluye lo siguiente:

- Las demostraciones de análisis de red demostraron la funcionalidad sobre cómo trabaja el protocolo QUIC UDP, cuál es su utilidad en las páginas web, el mejor aprovechamiento que se le puede dar según navegador y cómo es posible hacer uso eficiente de la arquitectura de este protocolo. Al mismo tiempo, la encuesta aplicada refuerza la definición del protocolo QUIC UDP al da una descripción del problema en la navegación web donde la persona usuaria final se orienta mejor y puede tomar las correcciones necesarias en el tiempo adecuado.

6.1.3 Conclusión objetivo n.º 2: Describir los serios problemas de latencia que hay en las redes. Este objetivo se alcanzó y se concluye lo siguiente:

- Las diferentes demostraciones que se hicieron con el Wireshark al analizar la red de navegación web, más la información obtenida del cuestionario, dan resultados sustentables de cuáles son las mejores opciones por seguir para mejorar los problemas de lentitud en la red y cuáles ajustes se deben hacer en los protocolos de relaciones como HTTP y TLS. Además, se demostró cómo disminuir la latencia en la red haciendo migraciones de actualización sobre los protocolos de navegación web y qué posibilidades hay para migrar a la nube de Google.

6.1.4 Conclusión objetivo n.º 3: Comprender la seguridad, establecimiento y migración de la conexión, multiplexación de Streams, control de flujo y congestión. Este objetivo se alcanzó y se concluye lo siguiente:

- La seguridad se mejora al implementar una actualización sobre dos protocolos esenciales, el TLS y HTTP, y al hacer una migración hacia la arquitectura del Google QUIC en donde controla y amplifica la multiplexación de transmisiones de audio y video desarrollando un mejor control en las capas de transporte y seguridad. Esto da un flujo de información y control sobre los paquetes transmitidos, para que la navegación web tenga una solvencia instantánea que mejore el ambiente web del usuario final. Asimismo, al tener un mejor control sobre las capas de transporte y seguridad la capa de aplicación sufre menos congestión, presentando cualquier contenido con una gran viabilidad para implementarse.

6.1.5 Conclusión objetivo n.º 4: Explicar las innovaciones tecnológicas que tiene este nuevo protocolo. Este objetivo se alcanzó y se concluye lo siguiente:

- Al trabajar con redes y tener alrededor un mundo conectado en una red mundial que es la Internet, todas las demás tecnologías como el Internet de las cosas, la inteligencia artificial, el Wifi versión 6, los dispositivos como conmutadores y enrutadores de red, más todo el desarrollo que hacen empresas como Apple, Google, Akamai, se presenta un mejor escenario futurista. En este todos los protocolos de red se acoplan o migran con la nueva arquitectura del Google QUIC y, por lo tanto, la revolución tecnológica absorberá todas las tendencias mundiales de desarrollo en dispositivos de usuario normal como *laptops*, *tablets*, celulares y toda la tecnología en el ámbito industrial.

6.1.6 Conclusión objetivo n.º 5: Demostrar como QUIC es mejor que el TCP/IP. Este objetivo se alcanzó y se concluye lo siguiente:

- El estudio que se hizo al diseño de la arquitectura del Google QUIC demuestra una mejora sustentable para el manejo de información cliente y servidor. Hay una mejora en la arquitectura sobre el modelo OSI que proyecta una gran innovación en el manejo de transmisiones múltiples que se asegura en la capa de transporte de seguridad sobre la versión mejorada del TLS 1.3. Esto impulsa la navegación web ya lista, ya que se enfoca correctamente sobre la versión 3 del HTTP, lo que ocasiona un servicio con mejor valor agregado al cliente final.

6.1.7 Conclusión objetivo n.º 6: Analizar los beneficios de QUIC y el futuro de la Internet con el HTTP/3. Este objetivo se alcanzó y se concluye lo siguiente:

- El nuevo protocolo QUIC es la puerta a una nueva dimensión del perfeccionamiento del modelo OSI tradicional. El QUIC solo se pensó para la navegación web cuando Google lo desarrolló en sus inicios, ahora se han dado cuenta de que se puede ir más allá del modelo tradicional TCP y mover todos los protocolos a la arquitectura del protocolo QUIC y quitar todos los cuellos de botella que hacen que el modelo tradicional desarrollado en los años 70 sea una arquitectura antigua que se debe renovar hacia el nuevo mundo que es el futuro de la inteligencia artificial, los nuevos modelos en la nube y todo lo que ofrece el Internet de las cosas.
- Las empresas de alta tecnología más importantes se dieron cuenta de esta innovación de Google al tener óptimos resultados. Por esta razón, Apple, Microsoft, Akamai, Google, compañías de servidores web en centros de datos de alto volumen y el mundo de los videojuegos utilizan esta nueva

versión de navegación web la HTTP/3, con óptimos resultados utilizando QUIC del IETF. Incluso con los cuellos de botella del modelo tradicional del TCP todavía queda un gran desarrollo para los siguientes años.

6.1.8 Conclusiones objetivo n.º 7: Proponer mejores soluciones al tráfico moderno de la información en los centros de datos y su enlace con nuevas tecnologías. Este objetivo se alcanzó y se concluye lo siguiente:

- El desarrollo que plantea el IETF de mover todos los protocolos del modelo tradicional OSI montado sobre TCP presenta grandes propuestas de innovación en muchas áreas que actualmente están en desarrollo. Los centros de datos tradicionales que consumen muchos recursos se migran a otros centros más modernos o migran toda su infraestructura a los servicios en la nube. Esto hace que se mejore el tráfico de información con respecto a rapidez, confiabilidad y un alto soporte en seguridad. Por lo tanto, tecnologías como robótica, con inteligencia artificial o no, el mundo de Internet de las cosas y muchas otras tendencias en el ámbito de plantas industriales de alto volumen, al estar todo esto relacionado en una gran red de interconectividad fortalece el uso sobre la innovación del protocolo QUIC y sus otros elementos asociados como TLS 1.3 y Http/3.

6.1.9 Conclusión objetivo n.º 8: Considerar que QUIC es una solución para la criptografía moderna con relación a certificados y claves de acceso. Este objetivo se alcanzó y se concluye lo siguiente:

- El protocolo Google QUIC es una verdadera solución para el uso de certificados, manejo de claves y la criptografía en general. Al estar montado sobre UDP se agiliza la rapidez y se mejora la seguridad, no se presenta una demora en la autentificación cliente-servidor, sino que la respuesta es más

inmediata. Esto con base en el nuevo diseño de arquitectura que lo que pretende es perfeccionar las deficiencias que se dan en el modelo TCP y este modelo enlace más el TLS 1.3 dentro del protocolo QUIC, haciendo que todo ocurra más en la capa de seguridad y sea desplegable con más facilidad en la capa de aplicación.

6.1.10 Conclusión objetivo n.º 9: Evaluar la viabilidad técnica del protocolo QUIC UDP. Este objetivo se alcanzó y se concluye lo siguiente:

- La viabilidad técnica de este nuevo protocolo es muy practica y sencilla. Es posible afirmar que su implementación ya está realizada, lo que queda es impulsar su perfeccionamiento y dar una buena orientación sobre cómo analizar el uso de este protocolo, cómo orientar a las personas sobre los navegadores web por utilizar, cómo utilizar herramientas analíticas como el Wireshark u otros para realizar pruebas y, al mismo tiempo, impulsar el uso de los protocolos correctos en los centros de datos y cómo entender el nuevo cambio evolutivo.

6.1.11 Conclusión objetivo general.

6.1.12 Conclusión objetivo general 1: Determinar la viabilidad técnica del uso del protocolo QUIC UDP para las empresas en Costa Rica. Este objetivo se alcanzó y se concluye lo siguiente:

- La viabilidad técnica del protocolo QUIC UDP en las empresas costarricenses es prácticamente un hecho, lo que queda es hacer una evaluación para determinar con qué infraestructura se trabaja para hacer las actualizaciones correspondientes si se requieren. También impulsar más a las compañías a que realicen las migraciones correspondientes a la nube de Google y comprender en qué grado de madurez se encuentran.

- No obstante, se debe tener en cuenta que el proceso está en evolución y la adaptabilidad se realiza en forma escalonada en los siguientes años hasta que la IETF tenga el modelo completado con relación a los protocolos de red. Por lo tanto, se debe tomar este tiempo para que las empresas en Costa Rica estén atentas a los nuevos cambios tecnológicos con sus ajustes y estar al día en sus infraestructuras para no tener deficiencias y quedarse obsoletos.

6.2 Recomendaciones

6.2.1 Recomendaciones objetivo general:

- Hacer una evaluación previa de la infraestructura en el centro de datos y conocer en qué nivel de calidad de equipos se encuentra el lugar. De esta forma, la implementación del protocolo QUIC UDP tiene una viabilidad técnica mejor aplicada.

6.2.2 Recomendación objetivo específico:

- Con un entrenamiento en herramientas de análisis de redes, como las que se enfocan en pruebas de penetración como el mismo Wireshark, se presenta un escenario analítico muy variado en el cual se puede entrenar a las personas para entender cómo se define este nuevo protocolo y la combinación de trabajo que realiza junto con los otros protocolos de red.
- Para solucionar los problemas de latencia que hay en las infraestructuras se debe crear un diseño previo de servidores, *laptops* de usuarios, cómo está la segmentación de red distribuida en los conmutadores de red y en qué forma están conectados con los enrutadores de red. Esto para regular las cargas mal distribuidas y aprovechar los recursos físicos de la manera más adecuada y con el orden cronológico en un buen diseño de red.

Al lograr lo anterior se mejora mucho la latencia en ese centro de datos y con esto se puede saltar en una mejor implementación del QUIC UDP en las redes que se quieren migrar a este servicio. Además de promover que se usen servicios en la nube que se adapten mejor al protocolo QUIC UDP y que se corra con TLS 1.3 y HTTP/3.

- Demostrarles a las personas que el modelo tradicional TCP tiene deficiencias que se heredan de los años 70, que la seguridad que se usa es buena, pero genera latencia usando el modelo tradicional de red, que las trasmisiones multiplexadas son mejores en la arquitectura del QUIC UDP y que es más inteligente en el control de flujo y congestión cliente y servidor. De esta forma, se debe entrenar o hacer una presentación sobre cómo el QUIC UDP es mejor que el TCP y por qué el futuro de muchas tecnologías se migrará a esta nueva arquitectura que sigue en desarrollo.
- Se debe hacer una presentación de todas las innovaciones tecnológicas que se mueven alrededor del QUIC UDP. Por ejemplo, el Internet de las cosas en el área industrial y no industrial, las tecnologías inalámbricas, los diferentes servicios en la nube y todas las tecnologías desarrolladas con inteligencia artificial que se van perfeccionando cada vez más.
- Al hacer demostraciones con diferentes navegadores web se pueden realizar flujos de transmisión en distintas calidades de video hasta llegar a un UHD y se le puede dar entrenamiento técnico al usuario normal sobre cómo comprender cómo QUIC UDP es mejor que el TCP, en el flujo de transferencia de información.
- Se debe lograr que la mayor cantidad de usuarios utilicen los navegadores que están corriendo con la tecnología HTTP/3 y dar recomendaciones de

cuáles son los mejores navegadores web, como Google Chrome, Safari, Edge, Opera. Además, que muchos tengan el motor de QUIC UDP para tener un mejor aprovechamiento de estos protocolos nuevos de red que están en evolución constante.

- En los centros de datos actuales se debe dar una propuesta sobre cómo tener un ambiente híbrido, tanto en la nube como en el *hardware* que se utiliza. Al mismo tiempo, migrar las tecnologías viejas a un ambiente de acuerdo con las exigencias modernas y empezar a adoptar las soluciones en la nube que ya utilizan los componentes del QUIC UDP.
- Una de las grandes innovaciones del QUIC UDP es la seguridad y la rapidez, las dos trabajan conjuntas para quitar los problemas viejos del TCP. Aquí se debe dar un resumen técnico sobre cómo se trabaja con certificados y claves para disminuir la latencia entre cliente y servidor y cómo la arquitectura del QUIC UDP se desempeña mejor para no darle lentitud a la red.
- La mejor forma de validar la viabilidad técnica del QUIC UDP es determinar el conocimiento de las personas con estas tecnologías, entender el estado de la red actual y hacer una evaluación de la infraestructura paso a paso, con la lista de revisiones correspondientes que se le brinda al equipo técnico correspondiente.

Capítulo 7. Reflexiones finales

7.1 Reflexión final uno

La encuesta presenta varios caminos que se pueden abordar cambiando el enfoque sobre el tema del protocolo QUIC UDP. Se le puede dar más profundidad técnica en forma general y también se le puede dar un enfoque específico con mayor profundidad en el análisis del modelo OSI y las capas involucradas o realizar

encuestas muy generales que sean para todo tipo de persona, cambiando los enfoques sin llegar a grandes complejidades técnicas. Lo anterior para obtener mayores resultados y crear una criticidad más abundante y obtener una ramificación de análisis más rica y profunda en la que se presenten diferentes entornos con soluciones más heterogéneas.

7.2 Reflexión final dos

No solo es suficiente el uso de una herramienta como la de pruebas de penetración para abordar el comportamiento del QUIC UDP que se mueve en las redes actuales y obtener resultados analíticos. También se pueden utilizar más laboratorios a baja escala utilizando el Kali Linux y el Android Tamer que presentan un gran número de herramientas analíticas. Con estas el punto de vista final sobre el protocolo QUIC UDP crece a un nivel en el que la recolección de datos se puede hacer mejor con más análisis de vulnerabilidades, de *sniffing* y *spoofing*. Además, hacer análisis forense de mayor profundidad creando más entornos analíticos y de propuestas de solución, pero que, al mismo tiempo, crezca el volumen de la investigación a un nivel muy alto.

7.3 Reflexión final tres

Entre todas las contribuciones teóricas que se tiene sobre el QUIC UDP se pueden desarrollar grandes temas de investigación. Debido a que este protocolo todavía está en proceso de desarrollo se necesita hacer más exploración sobre cómo todo el modelo OSI puede llegar a controlarse o adaptarse en esta nueva arquitectura y cómo crear procesos evaluativos en relación con la tecnología en uso, ya sea de Apple, Microsoft, Akamai o hacer un refinamiento del mismo Cloud de Google y hacer mejores orientaciones en el uso de la infraestructura física y virtual.

Capítulo 8. Trabajos para el futuro (Líneas futuras de investigación)

8.1 Posibles trabajos por hacer utilizando solo el QUIC UDP:

8.1.2 IA

Actualmente, cada vez más la inteligencia artificial es una realidad, ya no es más una ficción, se ha llegado a un nivel en que las AI alcanzaron el aprendizaje humano. Sin embargo, todavía se debe trabajar más en perfeccionar la empatía, la parte de las emociones, la toma de decisiones y el correcto camino para seguir, así como determinar cómo se puede acoplar mejor a sistemas robotizados y cuál es el beneficio o innovación del QUIC UDP para la AI.

8.1.3 Robótica

La robótica es un área que tiene muchos años de desarrollo, pero se potencializará más con el acople de AI y del QUIC UDP al ser todo el sistema una red unificada solo que en otro entorno de desarrollo o aplicabilidad.

8.1.4 Redes de diferentes tecnologías

Dentro del gran universo de las redes que hoy se conoce hay otros enfoques que se pueden dar, sumado al QUIC UDP, como las redes de razonamiento de máquinas, están incluidas también la máquina de aprendizaje (MR y ML), las redes ópticas y redes de radio cognitivas y Citizens Broadband Radio Service.

8.1.5 El 5G

Se quiere evolucionar en esta otra tecnología de redes, pero se está perfeccionando para que sea eficiente para transmitir entre edificios y muros. Cuando se llegue a ese perfeccionamiento se quiere sumarle la arquitectura del QUIC UDP.

8.1.6 El IoT, ya sea industrial o de uso doméstico

El Internet de las cosas está llegando a un 29 % anual de crecimiento de los dispositivos que están conectados y se puede afirmar que, en 2025, 42000 millones de dispositivos pueden estar conectados. Esto llevaría a un flujo de datos de 79 *zetta bytes*, si se logra desde ya acoplar al QUIC UDP con esta otra tecnología es un gran repunte y evolución anticipada.

8.1.7 Profundizar sobre el diseño de arquitectura del QUIC UDP

Se pueden hacer investigaciones más detalladas sobre cómo este protocolo de red se mueve en las tres últimas capas del modelo OSI, perfección del transporte, seguridad y aplicación, cómo trabaja más con la negociación de latencia, con la multiplexación, con las transmisiones de datos y control de flujo, con la autentificación de certificados, claves y la misma encriptación y cómo mantener la resiliencia para conexiones NAT. Todo esto más en profundidad en el ámbito de código de programación y cómo se acopla en las redes.

8.1.7 Adaptar todos los protocolos del modelo OSI tradicional al QUIC UDP

No solo desarrollar los protocolos TLS, HTTP, UDP y perfeccionarlos dentro de la arquitectura QUIC UDP, sino perfeccionar toda la otra gama de protocolos del modelo TCP/IP y adaptar la siguiente lista de protocolos ARP, PPP, IP, NAT, PAT, ICMP, OSPF, EIGRP, DNS, BOOTP, DHCP, SMTP, POP, IMAP, FTP, TFTP, BGP, IPv6, RARP, SCTP, NFS, SMB. Además, trabajar en las 7 capas del modelo OSI con más detalle y continuar el desarrollo en paralelo con la IETF.

Glosario

La Tabla 10 es una descripción de conceptos utilizados durante la tesis que el lector puede consultar para tener una mejor claridad de lo que se habla.

Tabla 10: Definición de acrónimos sobre conceptos importantes

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
Wireshark	Wireshark es un analizador de protocolos de red de código abierto y gratuito que permite a los usuarios navegar, de forma interactiva, por el tráfico de datos en una red informática. El	Un tipo	N/A	Alto de un 80 % hasta un 100 %

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	proyecto de desarrollo se inició con el nombre de Ethereal, pero pasó a llamarse Wireshark en 2006			
QUIC	Conexión UDP rápidas en Internet (QUIC UDP Internet Connection)	Un tipo	N/A	Alto de un 80 % hasta un 100 %
Facebook	Facebook es una red social que se creó para mantener en contacto a personas y que estas pudieran compartir información, noticias y	Un tipo	N/A	Alto de un 80 % hasta un 100 %

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	contenidos audiovisuales con sus propios amigos y familiares.			
Slack	Slack es una red social que se creó para el uso corporativo para mantener en contacto a personas y compartir información de documentos, videos, enlaces, pero también para compartir con amigos y familiares.	Un tipo	N/A	N/A

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
WhatsApp	WhatsApp es una red social para compartir información entre personas conocidas de videos, documentos, texto y enlaces.	Un tipo	N/A	Alto de un 80 % hasta un 100 %
Discord	Discord es una red social para compartir información entre personas conocidas de videos, documentos, texto y enlaces.	Un tipo	N/A	Alto de un 80 % hasta un 100 %
Telegram	Telegram es una red social para compartir	Un tipo	N/A	Alto de un 80 % hasta un 100 %

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	información entre personas conocidas de videos, documentos, texto y enlaces.			
TCP/UDP	El protocolo de control de transmisión (TCP) y el protocolo de datagramas de usuario (UDP) son protocolos de transporte que son algunos de los centrales del conjunto de protocolos de Internet. Tanto TCP	Dos tipos	IPv4: Trabaja con 32 *bits* IPv6: Trabaja con 128 *bits*	Alto de un 80 % hasta un 100 %

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	como UDP funcionan en la capa de transporte del modelo TCP/IP. TCP utiliza un protocolo de enlace de tres vías para establecer la conexión confiable, mientras que UDP no es confiable, pero es más rápido en comparación con TCP. El dispositivo de red ofrece algunos de los servicios que utilizan			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	TCP o UDP para una fácil administración del dispositivo. Los servicios se pueden habilitar o deshabilitar según el requisito.			
ICMP	ICMP es un protocolo de capa de red que forma parte del conjunto de protocolos de Internet que genera mensajes ICMP como respuesta a errores en el datagrama IP o con	Hay diferentes tipos de ICMP, especialmente para hacer ataques de DoS.	ICMP Ping Flood Attack — En un ataque ICMP Ping Flood, el ataque envía un gran número de paquetes ping al sistema de destino, generalmente mediante el uso del comando	Alto de un 80 % hasta un 100 %

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	fines de diagnóstico o enrutamiento. Los errores ICMP siempre se notifican a la dirección IP de origen original del datagrama de origen. Aunque este protocolo es muy importante para garantizar una correcta distribución de datos, pueden explotarlo usuarios malintencionados para		ping del *host*. De esta manera, el sistema atacado no puede responder al tráfico legítimo. Ataque pitufo ICMP: un ataque pitufo ICMP inunda la máquina víctima con paquetes ping falsificados. Estos son paquetes modificados que contienen una dirección IP falsificada de la	

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	realizar diferentes ataques de denegación de servicio (DoS).		víctima objetivo. Esto provoca una difusión de la información errónea a todos los *hosts* de la red local. Todos estos *hosts* responden con una respuesta al sistema de destino, que después se satura con esas respuestas. Si hay muchos *hosts* en redes usadas, la víctima será efectivamente	

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
			falsificada por una gran cantidad de tráfico.	
TLS	Capa de transporte de seguridad. Trabaja junto con el protocolo HTTP y HTTPS.			
HTTPS	HTTPS o protocolo de transferencia de hipertexto a través de Secure Sockets Layer (SSL), asegura la comunicación entre un navegador y un servidor web para los			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	usuarios de Microsoft Windows y Linux. HTTPS utiliza certificados para garantizar las identidades del servidor y para proteger la conexión del navegador. Además, usa una clave pública para cifrar los datos, incluidos el nombre de usuario y la contraseña,			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	durante el transporte a través de Internet.			
Opera	Opera es un navegador web desarrollado por la empresa noruega Opera Software.			
Google	Es una empresa de los Estados Unidos que se especializa en productos y servicios que se relacionan con Internet, *software*, dispositivos			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	electrónicos y otras tecnologías.			
Chrome	Es un navegador web de código abierto.			
Edge	Es el último navegador web desarrollado por Microsoft.			
Firefox	Es un navegador web de código libre o abierto desarrollado para distintas plataformas por la Corporación Mozilla y la Fundación Mozilla.			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
YouTube	Es un sitio web dedicado a compartir videos. Se creó en el año 2005 en USA y Google es el dueño de toda la plataforma y la compró a sus fundadores.			
Linux	Linux se desarrolló en el año 1991 por Linus Torvalds. Se creó como un sistema operativo de código abierto, pero ya se ha creado otra			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	versión con licencia para el uso empresarial.			
Ubuntu	Es una versión de Linux de código abierto que se puede instalar en PC y servidores, pero actualmente hay versiones empresariales con licencia.			
Tamer	AndroidTamer es una plataforma virtual para profesionales de la			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	seguridad de Android. Este entorno permite a las personas trabajar en una gran variedad de tareas que se relacionan con la seguridad de Android que van desde el análisis de *malware*, las pruebas de penetración y la ingeniería inversa.			
Windows	Windows es un sistema operativo que creó Microsoft. Consiste en			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	un conjunto de programas que permiten la ejecución de los recursos que tiene un ordenador.			
Paquetes	Es el conjunto de datos que se transmiten en una red entre fuente y destino. Pueden estar formados de varios *bytes*.			
QUIC IETF	Conexión UDP rápidas en Internet (QUIC UDP Internet Connection)			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	que desarrolla la Internet Engineer Task Force, para seguir con la evolución que creo Google.			
IP	Protocolo de Internet es el número asignado a la tarjeta de red que le da una ubicación a una PC o un servidor en la red para que pueda comunicarse con los otros dispositivos en la			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	misma red o redes diferentes.			
IP fuente	Es la IP de inicio de un servidor o PC que quiere enviar datos a un destino determinado.			
IP destino	Es la IP final de un servidor o PC que está listo para recibir datos enviados por la IP fuente.			
Protocolo	Los protocolos lo que hacen es realizar			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	funciones específicas en la red para cumplir con un patrón o comportamiento asociado con el tipo de protocolo. Todos los protocolos tienen un número asociado en la red que los identifica, por ejemplo, el SSH por puerto 22			
Frame	Es el marco de datos que se tiene en una captura de información			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	en la red que se hace con herramientas de pruebas de penetración, en este caso el Wireshark.			
Ethernet	Es el tipo de conexión física por cable que va conectado directo a la NIC.			
Cliente en una red	El cliente es el dispositivo que requiere de un servicio que por lo general se solicita a un servidor.			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
Servidor en una red	El servidor en una red es el que brinda los servicios solicitados por un cliente.			
Cloud	Es el nuevo concepto de brindar servicios en la nube desde seguridad, redes, inteligencia artificial, código e infraestructura.			
Modelo OSI	Es un modelo para entender las diferentes capas de interconexión			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	que se dan en una red, desde la capa física hasta llegar a la capa 7 de aplicación que interactúa con la persona. Se creó en el año 1980 por la organización internacional de normalización.			
Capas en el modelo OSI	Las capas del modelo OSI son 7: capa 1: física, capa 2: enlace de datos, capa 3 red,			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	capa 4: transporte, capa 5: sesión, capa 6: presentación, capa 7: aplicación.			
ARP	ARP (Protocolo de resolución de direcciones) se utiliza para realizar un seguimiento de todos los dispositivos que están conectados directamente al conmutador. El conmutador mantiene			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	una tabla ARP que tiene la dirección IP y la dirección MAC de cada dispositivo conectado con el conmutador. Cuando un paquete necesita enrutarse a un determinado dispositivo, el *switch* busca la dirección IP en su tabla ARP para obtener la dirección MAC del dispositivo de destino. La tabla ARP			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	proporciona información útil sobre los diferentes dispositivos conectados. En caso de que el conmutador no pueda saber si un dispositivo está conectado o no, la tabla ARP puede ayudar a determinar este problema. Además, puede agregar dispositivos			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	manualmente a la tabla ARP, lo que brinda más seguridad a la red a medida que realiza un seguimiento de cuáles dispositivos forman parte de la tabla ARP.			
VLAN	Las VLAN son un mecanismo que permite a los administradores de red crear dominios de difusión lógicos que pueden abarcar un solo conmutador o varios			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	conmutadores, independientemente de la proximidad física. Esta función es útil para reducir el tamaño de los dominios de difusión o para permitir que grupos o usuarios se agrupen lógicamente sin necesidad de estar ubicados en el mismo lugar.			
STP	Spanning-Tree Protocol (STP) evita que se			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	formen bucles cuando los conmutadores o puentes están interconectados a través de múltiples rutas. Spanning-Tree Protocol implementa el algoritmo IEEE 802.1D intercambiando mensajes BPDU con otros conmutadores para detectar bucles y, a continuación, elimina el bucle apagando las			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	interfaces de puente seleccionadas. Este algoritmo garantiza que haya una y solo una ruta activa entre dos dispositivos de red.			
Arquitectura de red	La arquitectura de red se refiere a la forma en la que los dispositivos y servicios de red están estructurados para satisfacer las necesidades de			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	conectividad de los dispositivos cliente. Los dispositivos de red suelen incluir conmutadores y enrutadores. Los tipos de servicios incluyen DHCP y DNS. Los dispositivos cliente comprenden dispositivos de usuario final, servidores y cosas inteligentes.			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
Riesgo	El riesgo es una amenaza que explota alguna vulnerabilidad que puede causar daño a un activo. El algoritmo de riesgos calcula el riesgo en función de los activos, amenazas y vulnerabilidades. Un ejemplo de un riesgo dentro de un sistema está representado por la fórmula (activo *	Riesgo crediticio Riesgo operacional Riesgo tecnológico Riesgo estratégico Riesgo legal Riesgo de mercado Riesgo de liquidez Riesgo de cumplimiento Riesgo de seguridad alimentaria Riesgo reputacional		

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	amenaza * vulnerabilidad)".			
Ciberseguridad	La ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales. Estos ataques cibernéticos generalmente tienen como objetivo acceder, cambiar o destruir información confidencial; extorsionar a los			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	usuarios o interrumpir los procesos normales de negocio. La implementación de medidas efectivas de ciberseguridad es particularmente desafiante en la actualidad, porque hay más dispositivos que personas y los atacantes se vuelven más innovadores.			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
Filtrado de red	Se puede asociar al filtrado de paquetes en la misma red, ya sea para solo enviar los paquetes requeridos y filtrar algún tipo de programa malicioso que da problemas.			
Puertos	Es un identificador asociado con un protocolo para que este se pueda mover por capa de transporte, ya sea por el TCP o por el			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	UDP. El puerto es un valor que se le asigna a un protocolo específico para que pueda viajar en la red y dar el servicio solicitado. Es posible afirmar que cada protocolo de red tiene un número de puerto asociado con este para cumplir su función específica.			
Escaneo	Revisión o lectura en este caso se puede			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	enfocar como lectura de puertos de red			
Enrutamiento	A nivel de red es posible entender que el enrutamiento es el camino que se debe trazar o construir, desde la fuente de un dispositivo hasta su destino para que sea una comunicación inmediata sin errores y no tengan problemas de latencia.			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
OSPF	Open Shortest Path First (OSPF) es un protocolo de puerta de enlace interior de estado de enlace. Los enrutadores OSPF inundan la información del estado del enlace a los enrutadores vecinos para que todos los enrutadores en un área OSPF tengan una vista completa de la topología de la red.	Existen versiones separadas de OSPF con base en la versión IP: OSPFv2 para redes IPv4 y OSPFv3 para redes IPv6. Estas versiones son independientes, es decir, OSPFv3 no es un reemplazo para OSPFv2.		

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
RIP	El protocolo de información de enrutamiento (RIP) utiliza paquetes de datos UDP de difusión para intercambiar información de enrutamiento. El *software* de Cisco envía actualizaciones de información de enrutamiento cada 30	RIP v2 IPv4 RIP v3 IPv6		

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	segundos, lo que se denomina publicidad. Si un dispositivo no recibe una actualización de otro durante 180 segundos o más, el dispositivo receptor marca las rutas servidas por el dispositivo no actualizado como inutilizables. Si todavía no hay ninguna actualización después			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	de 240 segundos, el dispositivo elimina todas las entradas de la tabla de enrutamiento para el dispositivo no actualizado.			
EIGRP	Enhanced Interior Gateway Routing Protocol (EIGRP) es una innovación única de Cisco. Muy valorado por su facilidad de implementación y rápida convergencia,	EIGRP v4 EIGRP v6		

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	EIGRP se utiliza comúnmente en muchas redes empresariales grandes. EIGRP mantiene todas las ventajas de los protocolos de vectores de distancia, al tiempo que evita las desventajas concurrentes.			
BGP	Border Gateway Protocol (BGP) es un estándar de Internet	BGP IPv4 BGP IPv6		

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	Engineering Task Force (IETF) y el más escalable de todos los protocolos de enrutamiento. BGP es el protocolo de enrutamiento de Internet global, así como para las redes privadas de proveedores de servicios. BGP ha ampliado su propósito original de llevar			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	información de accesibilidad a Internet y ahora puede transportar rutas para Multicast, IPv6, VPN y una variedad de otros datos.			
Sistema	Un sistema es un grupo de elementos que se relacionan que funcionan en conjunto.			
Detección de redes.	Es una característica de Windows o Linux que permite que los			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	dispositivos de Windows o Linux encuentren y descubran otros ordenadores y dispositivos en una red.			
Intruso en la red.	Es una PC no asociada en forma original al segmento de red que puede presentar una Mac Address de dudosa procedencia, también algún programa maligno			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	hospedado en el sistema operativo.			
Control en redes	Se puede entender como el control que se le debe dar a los dispositivos asociados en una red.			
Servicios	En las redes se tiene una gran cantidad de servidores que dan un servicio asociado con los requerimientos de esta red. Se tienen			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	servicios como DNS, DHCP, HTTP, etc.			
RTT	Round-Trip delay Time también llamado RTT. Se define como el tiempo que tarda un paquete de datos enviado desde un emisor en volver a este mismo emisor habiendo pasado por el receptor de destino.			
0-RTT	0-RTT es tecnología de protocolo de			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	vanguardia. Con este las solicitudes HTTPS cifradas se vuelven tan rápidas como las no cifradas.			
1-RTT	El tiempo de viaje con un ciclo de más.			
SPDY	SPDY es un protocolo de sesión para TCP/IP, capaz de optimizar las comunicaciones HTTP con una mejora de hasta el 64 % en carga de páginas. No			

Acrónimos	Definición	Tipos o clases	Definición por tipos o clases	% de uso.
	sustituye a HTTP, sino que, de forma transparente, lo complementa, sin que los usuarios se den cuenta. En sus inicios solo Chrome y Firefox 11 beta en adelante lo implementan.			

Bibliografía

Aboba, B.; Salgueiro, G. y Perkins, C. (2021). *Multiplexing Scheme Updates for QUIC*.

Asplund, H. y Astely, D. (2020). *Advanced Antenna Systems for 5G Network Deployments: Bridging the Gap Between Theory and Practice*.

Berners, L.; Fielding, R. y Frystyk, H. (1996). *Hypertext Transfer Protocol -- HTTP/1.0*.

Bishop, M. (2021). *Hypertext Transfer Protocol Version 3 (HTTP/3)*.

Cisco. (2018). *Configuración de los parámetros de servicio del protocolo de control de transmisión (TCP) y del protocolo de datagramas de usuario (UDP) en un switch*. https://www.cisco.com/c/es_mx/support/docs/smb/switches/cisco-250-series-smart-switches/smb2009-configure-transmission-control-protocol-tcp-and-user-datagra.html

Department of Computer Science California. (2020). *QUIC - A Quick Study-Santa Clara University*.

Digital Guide IONOS. (s. f.). *QUIC: los entresijos del protocolo experimental de Google*. https://www.ionos.es/digitalguide/hosting/cuestiones-tecnicas/quic-protocolo-de-transporte-de-internet-basado-en-udp/

Duke, M. (2021). *QUIC-LB: Generating Routable QUIC Connection IDsID*. F5 Networks, Inc - -N. Banks, Microsoft.

Estrada Corona, A. (2004). Protocolos TCP/IP de internet. *Revista Digital Universitaria, 5*(8): 1-7. http://www.revista.unam.mx/vol.5/num8/art51/sep_art51.pdf

Govers, F. (2018). *Artificial Intelligence for Robotics: Build intelligent robots that perform human tasks using AI techniques*.

Günther, F. (2017). *Modeling Advanced Security Aspects of Key Exchange and Secure Channel Protocols*.

Hamilton, R.; Iyengar, J.; Swett, I. y Wilk, A. (2016). *QUIC: A UDP-Based Multiplexed and Secure Transport*.

Hanes, D. (2017). *IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things*.

Huitema, C.; Dickinson, S. y Mankin, A. (2021). *DNS over Dedicated QUIC Connections*.

Hurst, S. (2021). *An Offset Extension Frame For HTTP/3 Data*.

Iyengar, J. y Swett, I. (2021). *QUIC Loss Detection and Congestion control*.

Krasic, C.; Bishop, M. y Frindell, A. (2021). *QPACK: Header Compression for HTTP/3*.

Kuehlewind, M. y Ericsson, B. (2021). *Manageability of the QUIC Transport Protocol*. Google Switzerland GmbH.

Lea, P. (2020). *IoT and Edge Computing for Architects: Implementing edge and IoT systems from sensors to clouds with communication systems, analytics, and security*.

Li, T.; Zheng, K.; Jadhav, R. y Kang, J. (2021). *Optimizing ACK mechanism for QUIC*.

Martínez, B.; Morales Gómez, J. C. y Ramírez Landaverde, F. (2005). *Diseño e implementación de la red interna y sistema de control de biblioteca del centro escolar Salvador Martõnez Figueroa de la ciudad de Texistepeque*, *Departamento de Santa Ana, el Salvador, Centro América. Universidad de El Salvador.* https://ri.ues.edu.sv/id/eprint/14681/1/Dise%C3%B1o%20e%20Implementaci%C3%B3n%20de%20la%20Red%20Interna%20y%20Sistema%20de%20Con_.pdf

Miralles Sole, J. (2020). *Proyectos de inteligencia artificial: Guía práctica para abordar con éxito proyectos de IA en la empresa*.

Morales Gómez, V. (2019). *Desarrollo de un disector de tráfico para el protocolo QUIC*. Universidad Autónoma de Madrid. https://repositorio.uam.es/bitstream/handle/10486/689525/morales_gomez_victor_tfg.pdf?sequence=1&isAllowed=y

Mortensen, A.; Reddy, T.; Flemming, A.; Teague, N. y Compton, R. (2020). *DDoS Open Threat Signaling (DOTS) Architecture.*

Murphy, R. (2019). *Introduction to AI Robotics, second edition (Intelligent Robotics and Autonomous Agents series)*.

Pardue, L.; Bradbury, R. y Hurst, S. (2021). *Hypertext Transfer Protocol (HTTP) over multicast QUIC*. BBC Research & Development.

Pauly, T. y Schinazi, D. (2021). *QUIC-Aware Proxying Using HTTP*.

Pola Jiménez, E. (2019). *Integración y transmisión remota de videos 3D - ING*.

Rodríguez Pérez, M. y Rodríguez Rubio, R. (2019). *Inspección pasiva de Comunicaciones TLS*.

Rodríguez, J. (2015). *Fundamentals of 5G Mobile Networks*.

Rodríguez, T. (2012). *SPDY, un protocolo para optimizar HTTP desarrollado por Google que ya no son los únicos en usar*. https://www.genbeta.com/desarrollo/spdy-un-protocolo-para-optimizar-http-desarrollado-por-google-que-ya-no-son-los-unicos-en-usarlo

Rommer, S.; Hedman, P.; Olsson, M. y Frid, L. (2019). *5G Core Networks: Powering Digitalization*.

Rouhiainen, L. (2018). *Inteligencia artificial: 101 cosas que debes saber hoy sobre nuestro futuro*.

Rueda, M. F. (2022). *Productos y servicios de Google*. https://www.coursehero.com/file/153503432/Rueda-Mar%C3%ADa-Productos-de-Google-PUBLICIDADpdf/

Sexton, D. (2020). *AI, IoT &y the Intelligent Edge: Building Your Enterprise Tech Strategy*.

Sharma, R. (2021). *IoT and IIoT: The origin, evolution, and future: ~ A primitive guide to understand the IoT, IIoT and its significance with the micro-services*.

Significados.com. (s. f.). *Significado de estructura*. https://www.significados.com/estructura/#:~:text=La%20palabra%20estructura%20se%20refiere,funcionamiento%20de%20un%20determinado%20sistema.

Sirotkin, S. (2020). *5G Radioradio Access Network Architecture: The Dark Side of 5G (IEEE Press)*.

Staple, D. (2021). *Learn Robotics Programming: Build and control AI-enabled autonomous robots using the Raspberry Pi and Python*.

Sudhakar Shetty, R. (2021). *5G Mobile Core Network: Design, Deployment, Automation, and Testing Strategies*.

Thomson, M. (2021). *Generic HTTP Binding for WebTransport using QUIC*. Mozilla.

Tomás Silvestre, E. (2021). *Estudio comparativo de las versiones más recientes de HTTP*. Universitat Politècnica de València. https://riunet.upv.es/bitstream/handle/10251/172835/Tomas%20-%20Estudio%20comparativo%20de%20las%20versiones%20mas%20recientes%20de%20HTTP.pdf?sequence=1

Unionpedia. (s. f.). *Protocolo de transferencia de hipertexto*. https://es.unionpedia.org/i/Protocolo_de_transferencia_de_hipertexto

Veneri, G. (2018). *Hands-On Industrial Internet of Things: Create a powerful Industrial IoT infrastructure using Industry 4.0*.

Villegas Saiz, N. (2021). *Comportamiento de protocolos de transporte en entornos IIoT*.

Wilkins, N. (2019a). *Inteligencia Artificial: Inteligencia artificial: Una Guía Completa sobre la IA, el aprendizaje automático, el Internet de las cosas, la Robótica, el aprendizaje profundo, el análisis y el aprendizaje reforzado*.

Wilkins, N. (2019b). *Inteligencia artificial: Lo que usted necesita saber sobre el aprendizaje automático, robótica, aprendizaje profundo, Internet de las cosas, redes neuronales, y nuestro futuro*.

Wilkins, N. (2019c). *Robótica: Lo que los principiantes deben saber sobre la automatización de procesos robóticos, robots móviles, inteligencia artificial, aprendizaje automático, drones y nuestro futuro*.

Yan, P. y Yu, N. (2020). *The QQUIC Transport Protocol: Quantum assisted UDP Internet Connections*.

Ye, Q. y Zhuang, W. (2022). *Intelligent Resource Management for Network Slicing in 5G and Beyond (Wireless Networks*.

Yong, W.; Classon, B. Mazzarese, D. (2021). *5G System Design: An End-to-End Perspective (Wireless Networks)*.

Apéndices

En este apartado se presentan los datos que se obtuvieron mediante el uso de los instrumentos diseñados en el Capítulo 3.6.



Figura 38: El QUIC UDP se desplaza en las diferentes redes y también con los DNS de Google en una razón de tiempo transcurrido en milisegundos

La Figura 38 demuestra cómo el QUIC UDP se desplaza en las diferentes redes y también con los DNS de Google en una razón de tiempo transcurrido en milisegundos. Se ven los distintos pings de comunicación en cada red y el tiempo de viaje transcurrido es de 0-RTT. Esto demuestra que la comunicación con la red 192.168.0.9 se hizo en un solo viaje por el puerto 443 debido a los paquetes enviados.

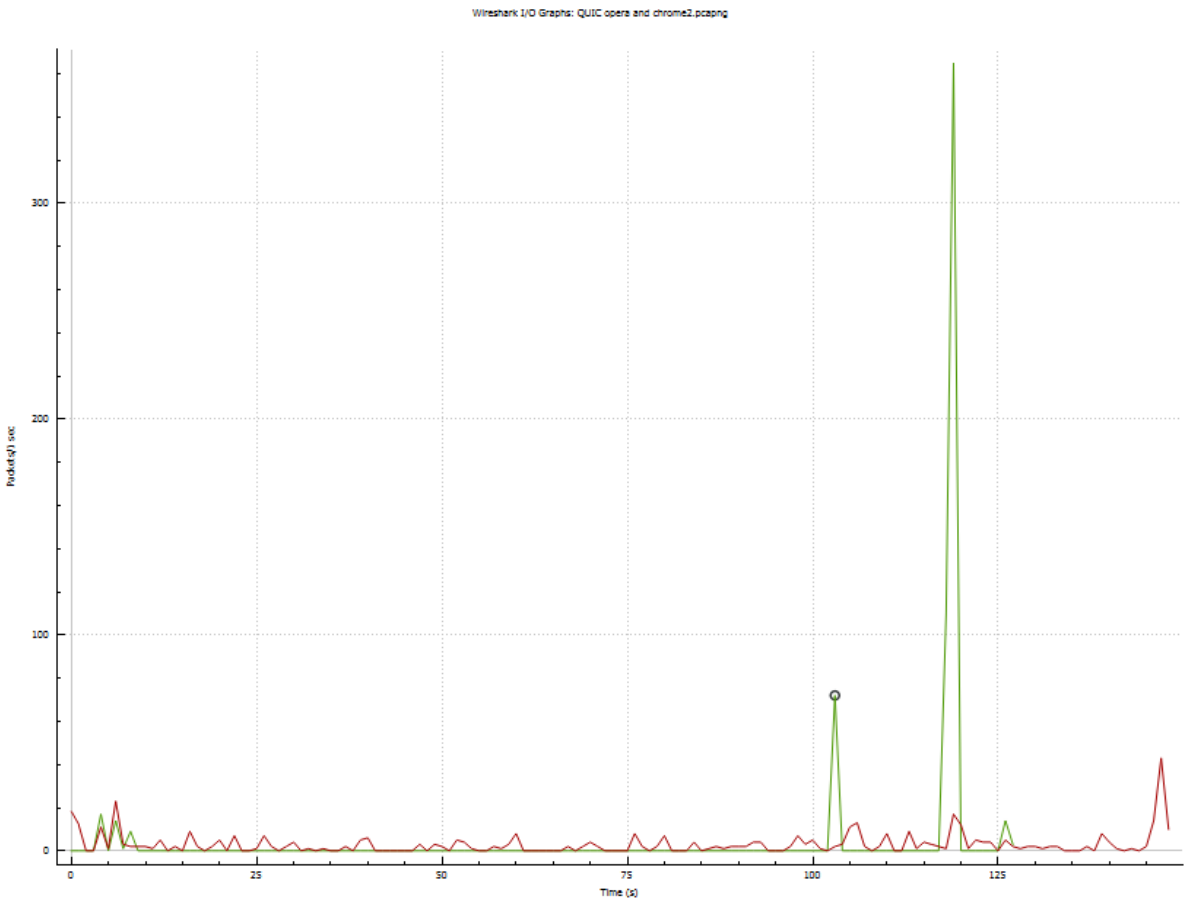


Figura 39: Más de 300 paquetes enviados en un tiempo mayor a un segundo

La Figura 39 demuestra que se enviaron más de 300 paquetes en un tiempo mayor a un segundo en donde el protocolo dominante entre Opera y Google Chrome fue el QUIC UDP. Esto demuestra la eficiencia en el transporte de información de este protocolo.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100	605	100	601946	39 k	0	0	0
Ethernet	100	605	1.4	8470	552	0	0	0
Internet Protocol Version 4	100	605	2	12100	789	0	0	0
User Datagram Protocol	100	605	0.8	4840	315	0	0	0
QUIC IETF	101.3	613	96	577942	37 k	605	571687	37 k

Protocol Hierarchy Statistics

Figura 40: Uso de protocolos TCP, UDP, QUIC UDP en una conexión de Ethernet

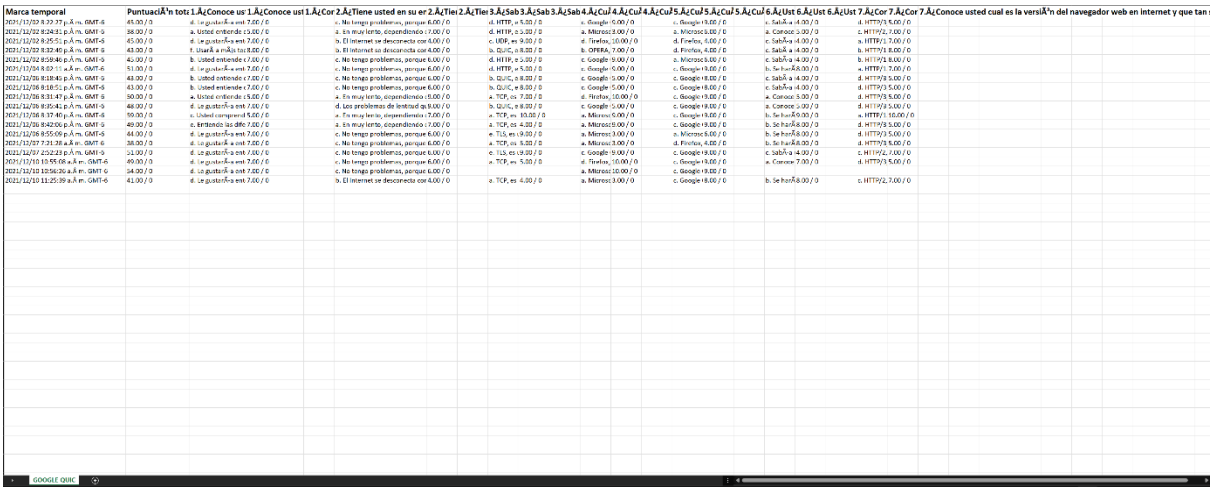
La Figura 40 lo que demuestra es el uso de protocolos TCP, UDP, QUIC UDP en una conexión de Ethernet. El protocolo dominante en el porcentaje de paquetes es el QUIC UDP, es donde se han transferido más paquetes en el porcentaje de *bytes* o *bits*.

Interval start	Filtered packets	Filtered packets
0	0	18
1	0	12
2	0	0
3	0	0
4	17	11
5	0	1
6	14	23
7	1	3
8	9	2
9	0	2
10	0	2
11	0	1
12	0	5
13	0	0
14	0	2
15	0	0
16	0	9
17	0	2
18	0	0
19	0	2
20	0	5
21	0	0
22	0	7
23	0	0
24	0	0
25	0	1
26	0	7
27	0	2
28	0	0
29	0	2
30	0	4
31	0	0
32	0	1
33	0	0
34	0	1
35	0	0
36	0	0
37	0	2
38	0	0
39	0	5
40	0	6
41	0	0
42	0	0
43	0	0
44	0	0
45	0	0
46	0	0
47	0	3
48	0	0

QUIC opera and chrome2

Figura 41: Filtrado de paquetes que se dan entre la herramienta web Opera y Chrome en diferentes intervalos

La Figura 41 demuestra el filtrado de paquetes que se da entre la herramienta web Opera y Chrome en diferentes intervalos. Con esto se demuestra el gran flujo de paquetes que se dan en los intervalos iniciales con el QUIC UDP.



Marca temporal	PuntuaciÃ³n totz 1.Â¿Conoce us 1.Â¿Conoce ust 1.Â¿Cor 2.Â¿Tiene usted en su er 2.Â¿Tier 2.Â¿Tier 3.Â¿Sab 3.Â¿Sab 3.Â¿Sab 4.Â¿Cuâ 4.Â¿Cuâ 4.Â¿Cuâ 5.Â¿Cuâ 5.Â¿Cuâ 5.Â¿Cuâ 6.Â¿Ust 6.Â¿Ust 6.Â¿Ust 7.Â¿Cor 7.Â¿Cor 7.Â¿Conoce usted cual es la versiÃ³n del navegador web en Internet y que tan
2021/11/02 8:22:27 p.Â m. GMT-6	45.00 / 0 d. Le gustarÃ-a ent 7.00 / 0 c. No tengo problemas, porque 6.00 / 0 d. HTTP, e 5.00 / 0 c. Google i 5.00 / 0 c. Google i 8.00 / 0 c. SabÃ-a 4.00 / 0 d. HTTP/1 5.00 / 0
2021/11/02 8:24:31 p.Â m. GMT-6	38.00 / 0 a. Usted entiende c 5.00 / 0 a. En muy lento, dependiendo c 7.00 / 0 d. HTTP, e 5.00 / 0 a. Microsc 3.00 / 0 a. Microsc 5.00 / 0 a. Conoce 5.00 / 0 c. HTTP/2, 7.00 / 0
2021/11/02 8:25:51 p.Â m. GMT-6	45.00 / 0 d. Le gustarÃ-a ent 7.00 / 0 b. El internet se desconecta cor 6.00 / 0 c. UDP, es 9.00 / 0 d. Firefox, i 10.00 / 0 d. Firefox, 8.00 / 0 c. SabÃ-a 4.00 / 0 a. HTTP/1 7.00 / 0
2021/11/02 8:32:40 p.Â m. GMT-6	43.00 / 0 f. UsarÃ-a mÃ¡s tar 8.00 / 0 b. El internet se desconecta cor 4.00 / 0 b. QUIC, e 8.00 / 0 b. OPERA, 7.00 / 0 d. Firefox, 4.00 / 0 c. SabÃ-a 4.00 / 0 b. HTTP/1 8.00 / 0
2021/11/02 8:59:46 p.Â m. GMT-6	45.00 / 0 b. Usted entiende c 7.00 / 0 c. No tengo problemas, porque 6.00 / 0 d. HTTP, e 5.00 / 0 c. Google i 9.00 / 0 a. Microsc 5.00 / 0 c. SabÃ-a 4.00 / 0 b. HTTP/1 8.00 / 0
2021/11/04 8:02:31 a.Â m. GMT-6	51.00 / 0 d. Le gustarÃ-a ent 7.00 / 0 c. No tengo problemas, porque 6.00 / 0 d. HTTP, e 5.00 / 0 c. Google i 5.00 / 0 c. Google i 9.00 / 0 b. Se harÃ-8.00 / 0 a. HTTP/1 7.00 / 0
2021/11/26 8:18:41 p.Â m. GMT-6	43.00 / 0 b. Usted entiende c 7.00 / 0 c. No tengo problemas, porque 6.00 / 0 b. QUIC, e 8.00 / 0 c. Google i 5.00 / 0 c. Google i 8.00 / 0 c. SabÃ-a 4.00 / 0 d. HTTP/3 5.00 / 0
2021/11/26 8:18:51 p.Â m. GMT-6	43.00 / 0 b. Usted entiende c 7.00 / 0 c. No tengo problemas, porque 6.00 / 0 b. QUIC, e 8.00 / 0 c. Google i 5.00 / 0 c. Google i 8.00 / 0 c. SabÃ-a 4.00 / 0 d. HTTP/3 5.00 / 0
2021/11/26 8:31:47 p.Â m. GMT-6	50.00 / 0 a. Usted entiende c 5.00 / 0 a. En muy lento, dependiendo c 8.00 / 0 a. TCP, es 7.00 / 0 d. Firefox, i 10.00 / 0 c. Google i 9.00 / 0 a. Conoce 5.00 / 0 d. HTTP/3 5.00 / 0
2021/11/26 8:35:41 p.Â m. GMT-6	48.00 / 0 d. Le gustarÃ-a ent 7.00 / 0 d. Los problemas de lentitud qu 9.00 / 0 b. QUIC, e 8.00 / 0 c. Google i 5.00 / 0 c. Google i 9.00 / 0 a. Conoce 5.00 / 0 d. HTTP/3 5.00 / 0
2021/11/26 8:37:40 p.Â m. GMT-6	59.00 / 0 c. Usted comprend 6.00 / 0 a. En muy lento, dependiendo c 7.00 / 0 a. TCP, es 10.00 / 0 a. Microsc 6.00 / 0 c. Google i 9.00 / 0 b. Se harÃ-9.00 / 0 a. HTTP/1 10.00 / 0
2021/11/26 8:42:06 p.Â m. GMT-6	49.00 / 0 a. Entiendo las dife 7.00 / 0 a. En muy lento, dependiendo c 7.00 / 0 a. TCP, es 4.00 / 0 a. Microsc 5.00 / 0 c. Google i 9.00 / 0 b. Se harÃ-8.00 / 0 d. HTTP/3 5.00 / 0
2021/11/26 8:55:09 p.Â m. GMT-6	44.00 / 0 d. Le gustarÃ-a ent 7.00 / 0 c. No tengo problemas, porque 6.00 / 0 e. TLS, es i 9.00 / 0 a. Microsc 3.00 / 0 a. Microsc 6.00 / 0 b. Se harÃ-8.00 / 0 d. HTTP/3 5.00 / 0
2021/11/27 7:21:28 a.Â m. GMT-6	38.00 / 0 d. Le gustarÃ-a ent 7.00 / 0 c. No tengo problemas, porque 6.00 / 0 a. TCP, es 5.00 / 0 a. Microsc 3.00 / 0 d. Firefox, 6.00 / 0 b. Se harÃ-8.00 / 0 d. HTTP/3 5.00 / 0
2021/11/27 2:52:23 p.Â m. GMT-6	51.00 / 0 d. Le gustarÃ-a ent 7.00 / 0 c. No tengo problemas, porque 6.00 / 0 c. TLS, es i 9.00 / 0 c. Google i 9.00 / 0 c. Google i 9.00 / 0 c. SabÃ-a 4.00 / 0 c. HTTP/2, 7.00 / 0
2021/11/10 10:55:08 a.Â m. GMT-6	49.00 / 0 d. Le gustarÃ-a ent 7.00 / 0 c. No tengo problemas, porque 6.00 / 0 a. TCP, es 5.00 / 0 d. Firefox, i 10.00 / 0 c. Google i 9.00 / 0 a. Conoce 7.00 / 0 d. HTTP/3 5.00 / 0
2021/11/10 10:56:20 a.Â m. GMT-6	34.00 / 0 d. Le gustarÃ-a ent 7.00 / 0 c. No tengo problemas, porque 6.00 / 0 a. Microsc 10.00 / 0 c. Google i 9.00 / 0
2021/11/10 11:25:39 a.Â m. GMT-6	41.00 / 0 d. Le gustarÃ-a ent 7.00 / 0 b. El internet se desconecta cor 4.00 / 0 a. TCP, es 4.00 / 0 a. Microsc 3.00 / 0 c. Google i 8.00 / 0 b. Se harÃ-8.00 / 0 c. HTTP/2, 7.00 / 0

Figura 42: Diferentes intervalos en que las distintas preguntas se contestaron para la encuesta del Google QUIC UDP

La Figura 42 demuestra los diferentes intervalos en que las distintas preguntas se contestaron para la encuesta del Google QUIC UDP y las personas consultadas debido a esa encuesta.