

Nombre: Carlos Alberto Valladares Guerra

Proyecto 1: Uso de un Protocolo Existente (MCP)

1. Especificación de los servidores MCP desarrollados

Durante el proyecto se implementaron e integraron cuatro servidores MCP distintos:

- **Servidor Local (HTTP):**
 - Desarrollado en Python con Flask + SQLAlchemy.
 - Funcionalidad: gestión de tareas (crear, listar, completar, posponer).
 - Endpoints principales: /initialize, /describe, /run.
 - Parámetros: puerto 6000, namespace 'local_'.
- **Servidor Remoto (HTTP en Google Cloud Run):**
 - Implementado como microservicio en la nube.
 - Funcionalidad: operaciones financieras (consultar saldos, registrar pagos).
 - Endpoints: /initialize, /describe, /run.
 - Parámetros: URL pública asignada por Cloud Run, namespace 'remoto_'.
- **Filesystem MCP (Oficial):**
 - Ejecutado vía: `npx -y @modelcontextprotocol/server-filesystem <directorio_root>`.
 - Funcionalidad: lectura, escritura y listado de archivos dentro del directorio workspace.
 - Se comunicó vía STDIO, con herramientas como `read_file`, `write_file`, `list_directory`.
 - Namespace: 'fs_'.
- **Git MCP (Oficial):**
 - Ejecutado con: `python -m mcp_server_git --repository ./repo_git`.
 - Funcionalidad: control de versiones (`git status`, `git add`, `git commit`, `git log`).
 - Comunicación STDIO, exponiendo herramientas equivalentes a comandos de Git.
 - Namespace: 'git_'.

2. Análisis de comunicación en red

Se utilizó Wireshark y los logs de ejecución para analizar la comunicación del protocolo MCP:

Local:

- **Capa de Enlace (OSI 2):** transmisión de tramas Ethernet/Wi-Fi entre cliente y servidor en la red local.

Capturando desde Adapter for loopback traffic capture

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplicar un filtro de visualización... <Ctrl>F

No.	Time	Source	Destination	Protocol	Length	Info	Seq	Ack	BytesInFlight	Len
313	19:53:39.746242	127.0.0.1	127.0.0.1	TCP	88	32479 → 50100 [PSH, ACK] Seq=389 Ack=385 Win=214 Len=44	389	385	44	
314	19:53:39.746270	127.0.0.1	127.0.0.1	TCP	44	50100 → 32479 [ACK] Seq=385 Ack=433 Win=190 Len=0	385	433		
315	19:53:39.761241	127.0.0.1	127.0.0.1	TCP	48	50100 → 32479 [PSH, ACK] Seq=385 Ack=433 Win=190 Len=4	385	433	4	
316	19:53:39.761270	127.0.0.1	127.0.0.1	TCP	44	32479 → 50100 [ACK] Seq=433 Ack=389 Win=214 Len=0	433	389		
317	19:53:39.761322	127.0.0.1	127.0.0.1	TCP	88	50100 → 32479 [PSH, ACK] Seq=389 Ack=433 Win=190 Len=44	389	433	44	
318	19:53:39.761337	127.0.0.1	127.0.0.1	TCP	44	32479 → 50100 [ACK] Seq=433 Ack=389 Win=214 Len=0	433	389		
319	19:53:41.104237	127.0.0.1	127.0.0.1	TCP	347	49676 → 18242 [PSH, ACK] Seq=8276 Ack=188 Win=241 Len=303	8276	188	303	
320	19:53:41.104272	127.0.0.1	127.0.0.1	TCP	44	18242 → 49676 [ACK] Seq=188 Ack=8579 Win=145 Len=0	188	8579		
321	19:53:44.019482	127.0.0.1	127.0.0.1	TCP	50	32619 → 1042 [PSH, ACK] Seq=97 Ack=33 Win=253 Len=6	97	33	6	
322	19:53:44.019509	127.0.0.1	127.0.0.1	TCP	44	1042 → 32619 [ACK] Seq=33 Ack=103 Win=250 Len=0	33	103		
323	19:53:44.019794	127.0.0.1	127.0.0.1	TCP	46	1042 → 32619 [PSH, ACK] Seq=33 Ack=103 Win=250 Len=2	33	103	2	
324	19:53:44.019816	127.0.0.1	127.0.0.1	TCP	44	32619 → 1042 [ACK] Seq=103 Ack=35 Win=253 Len=0	103	35		
325	19:53:44.711592	192.168.0.6	224.0.0.252	IGMPv2	36	Membership Report group 224.0.0.252				
326	19:53:47.189724	127.0.0.1	127.0.0.1	TCP	57	49676 → 18242 [PSH, ACK] Seq=8579 Ack=188 Win=241 Len=13	8579	188	13	
327	19:53:47.189744	127.0.0.1	127.0.0.1	TCP	44	18242 → 49676 [ACK] Seq=188 Ack=8592 Win=144 Len=0	188	8592		
328	19:53:47.204451	192.168.0.6	224.0.0.251	IGMPv2	36	Membership Report group 224.0.0.251				
329	19:53:47.587202	127.0.0.1	127.0.0.1	TCP	61	18242 → 49676 [PSH, ACK] Seq=188 Ack=8592 Win=144 Len=17	188	8592	17	
330	19:53:47.587226	127.0.0.1	127.0.0.1	TCP	44	49676 → 18242 [ACK] Seq=8592 Ack=205 Win=241 Len=0	8592	205		
331	19:53:49.180700	127.0.0.1	127.0.0.1	TCP	325	49676 → 18242 [PSH, ACK] Seq=8592 Ack=205 Win=241 Len=281	8592	205	281	
332	19:53:49.180739	127.0.0.1	127.0.0.1	TCP	44	18242 → 49676 [ACK] Seq=205 Ack=8873 Win=143 Len=0	205	8873		

Frame 1: 57 bytes on wire (456 bits), 57 bytes captured (456 bits) on interface \Device\NPF_{...}_id 0

Null/Loopback

Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

Transmission Control Protocol, Src Port: 49676, Dst Port: 18242, Seq: 1, Ack: 1, Len: 13

Data (13 bytes)

0000 02 00 00 00 45 00 00 35 4a fe 40 00 00 06 00 00 ... E 5 2 @ ...

0010 7f 00 00 01 7f 00 00 01 c2 0c 47 42 0e f7 bc d3 ... GB ...

0020 eb 52 a5 dc 50 18 00 f2 f1 bd 00 00 81 0b 7b 22 ... R P ...

0030 74 79 70 65 22 3a 36 7d 1e ... type'16)

Adapter for loopback traffic capture: live capture in progress

Paquetes: 332

Perif: CarlosValledares

19°C

Mayorm. nublado

19:53

11/09/2023

• Capa de Red (OSI 3): direccionamiento IP; en local 127.0.0.1 para servidores locales, y direcciones externas para el servidor remoto en Google Cloud Run.

Capturando desde Adapter for loopback traffic capture

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplicar un filtro de visualización... <Ctrl>F

tcp.port == 6000

No.	Time	Source	Destination	Protocol	Length	Info	Seq	Ack	BytesInFlight	Len
467	19:54:59.114826	127.0.0.1	127.0.0.1	X11	209	Event: <Unknown eventcode 72>, <Unknown eventcode 103>, <Unknown eventcode 4...	1	143	165	
468	19:54:59.114849	127.0.0.1	127.0.0.1	TCP	44	12684 → 6000 [ACK] Seq=143 Ack=166 Win=65280 Len=0	143	166		
469	19:54:59.114872	127.0.0.1	127.0.0.1	X11	63	Event: <Unknown eventcode 123>	166	143	19	
470	19:54:59.114881	127.0.0.1	127.0.0.1	TCP	44	12684 → 6000 [ACK] Seq=143 Ack=185 Win=65280 Len=0	143	185		
471	19:54:59.115466	127.0.0.1	127.0.0.1	TCP	44	12684 → 6000 [FIN, ACK] Seq=143 Ack=185 Win=65280 Len=0	143	185		
472	19:54:59.115552	127.0.0.1	127.0.0.1	TCP	44	6000 → 12684 [ACK] Seq=185 Ack=144 Win=65280 Len=0	185	144		
473	19:54:59.140200	127.0.0.1	127.0.0.1	TCP	44	6000 → 12684 [FIN, ACK] Seq=185 Ack=144 Win=65280 Len=0	185	144		
474	19:54:59.140367	127.0.0.1	127.0.0.1	TCP	44	12684 → 6000 [ACK] Seq=144 Ack=186 Win=65280 Len=0	144	186		
601	19:55:50.025467	127.0.0.1	127.0.0.1	TCP	56	8240 → 6000 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM	0	0		
602	19:55:50.025512	127.0.0.1	127.0.0.1	TCP	56	6000 → 8240 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM	0	1		
603	19:55:50.025540	127.0.0.1	127.0.0.1	TCP	44	8240 → 6000 [ACK] Seq=1 Ack=1 Win=65280 Len=0	1	1		
604	19:55:50.025727	127.0.0.1	127.0.0.1	X11	186	Requests: CopyColormapAndFree	1	1	142	
605	19:55:50.025741	127.0.0.1	127.0.0.1	TCP	44	6000 → 8240 [ACK] Seq=1 Ack=141 Win=65280 Len=0	1	141		
606	19:55:50.026998	127.0.0.1	127.0.0.1	TCP	209	Event: <Unknown eventcode 72>, <Unknown eventcode 103>, <Unknown eventcode 4...	1	143	165	
607	19:55:50.026997	127.0.0.1	127.0.0.1	TCP	44	8240 → 6000 [ACK] Seq=143 Ack=166 Win=65280 Len=0	143	166		
608	19:55:50.026999	127.0.0.1	127.0.0.1	X11	63	Event: <Unknown eventcode 123>	166	143	19	
609	19:55:50.027000	127.0.0.1	127.0.0.1	TCP	44	8240 → 6000 [ACK] Seq=143 Ack=185 Win=65280 Len=0	143	185		
610	19:55:50.027368	127.0.0.1	127.0.0.1	TCP	44	8240 → 6000 [FIN, ACK] Seq=143 Ack=185 Win=65280 Len=0	143	185		
611	19:55:50.027402	127.0.0.1	127.0.0.1	TCP	44	6000 → 8240 [ACK] Seq=185 Ack=144 Win=65280 Len=0	185	144		
612	19:55:50.031179	127.0.0.1	127.0.0.1	TCP	44	6000 → 8240 [FIN, ACK] Seq=185 Ack=144 Win=65280 Len=0	185	144		

Frame 462: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF_{...}_id 0

Null/Loopback

Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

Transmission Control Protocol, Src Port: 12684, Dst Port: 6000, Seq: 0, Len: 0

0000 02 00 00 00 45 00 00 34 4c 92 40 00 00 06 00 00 ... E 4 L @ ...

0010 7f 00 00 01 7f 00 00 01 31 8c 17 70 d9 ea f0 da ... 1 p ...

0020 00 00 00 00 00 02 ff ff 63 28 00 00 02 04 ff d7 ... c(...

0030 01 03 03 00 01 01 04 02 ...

wireshark_Adapter for loopback traffic capture\TSC3.pcapng

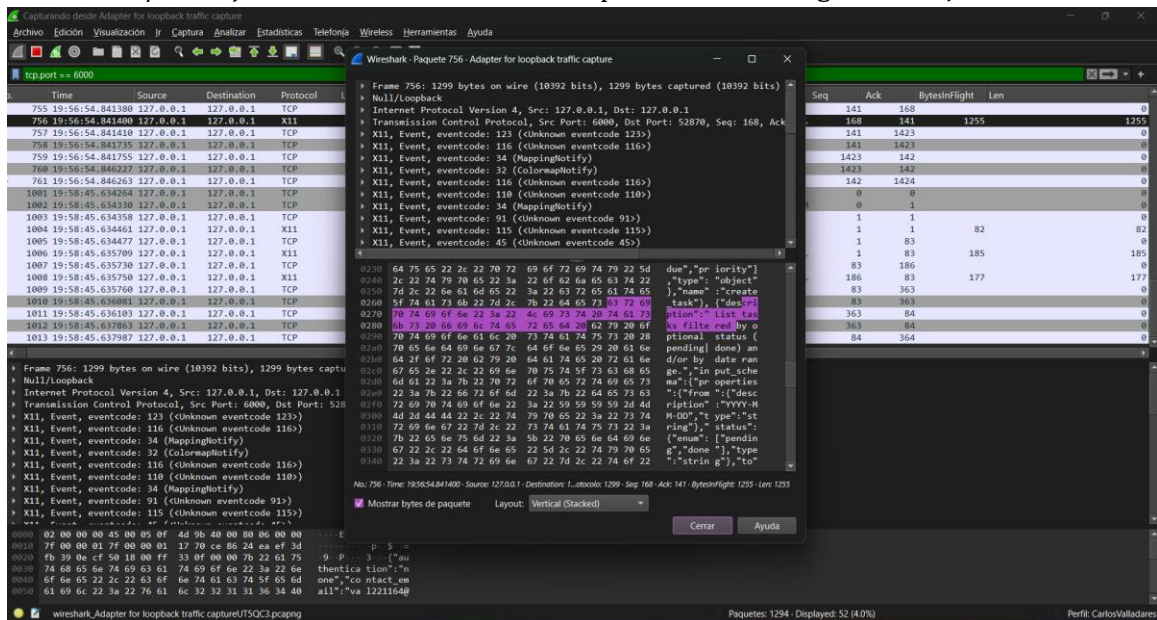
Paquetes: 646 - Displayed: 26 (4.0%)

Perif: CarlosValledares

• Capa de Transporte (OSI 4): uso de TCP como protocolo confiable para la entrega de mensajes.

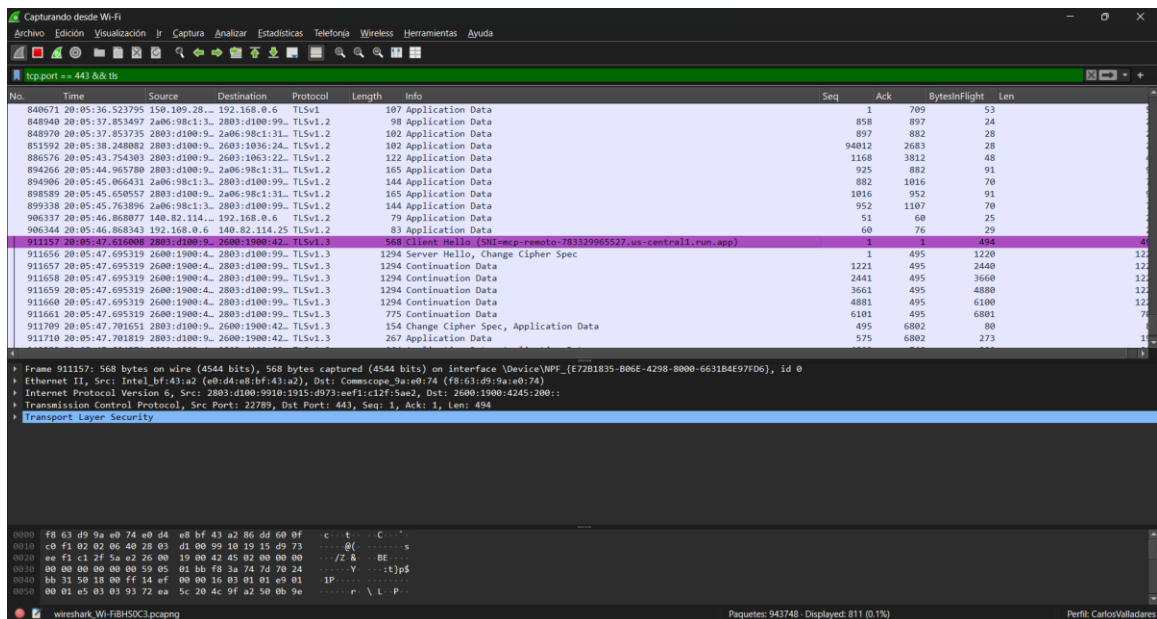
No.	Time	Source	Destination	Protocol	Length	Info	Seq	Ack	BytesInFlight	Len
607	19:55:50.026979	127.0.0.1	127.0.0.1	TCP	44	8240 → 6000 [ACK] Seq=143 Ack=166 Win=65280 Len=0	143	166		
608	19:55:50.026999	127.0.0.1	127.0.0.1	X11	63	Event: <Unknown eventcode 123>	166	143	19	
609	19:55:50.027009	127.0.0.1	127.0.0.1	TCP	44	8240 → 6000 [ACK] Seq=143 Ack=185 Win=65280 Len=0	143	185		
610	19:55:50.027368	127.0.0.1	127.0.0.1	TCP	44	8240 → 6000 [FIN, ACK] Seq=143 Ack=185 Win=65280 Len=0	143	185		
611	19:55:50.027402	127.0.0.1	127.0.0.1	TCP	44	6000 → 8240 [ACK] Seq=185 Ack=144 Win=65280 Len=0	185	144		
612	19:55:50.031179	127.0.0.1	127.0.0.1	TCP	44	6000 → 8240 [FIN, ACK] Seq=185 Ack=144 Win=65280 Len=0	185	144		
613	19:55:50.031222	127.0.0.1	127.0.0.1	TCP	44	8240 → 6000 [ACK] Seq=144 Ack=186 Win=65280 Len=0	144	186		
749	19:56:54.840128	127.0.0.1	127.0.0.1	TCP	56	52870 → 6000 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM	0	0		
750	19:56:54.840131	127.0.0.1	127.0.0.1	TCP	56	6000 → 52870 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM	0	1		
751	19:56:54.840220	127.0.0.1	127.0.0.1	TCP	44	52870 → 6000 [ACK] Seq=1 Ack=1 Win=65280 Len=0	1	1		
752	19:56:54.840364	127.0.0.1	127.0.0.1	X11	184	Requests: CopyColormapAndFree	1	1	140	
753	19:56:54.840378	127.0.0.1	127.0.0.1	TCP	44	6000 → 52870 [ACK] Seq=1 Ack=141 Win=65280 Len=0	1	141		
754	19:56:54.841368	127.0.0.1	127.0.0.1	X11	211	Event: <Unknown eventcode 72>, <Unknown eventcode 103>, <Unknown eventcode 4...	1	141	167	
755	19:56:54.841380	127.0.0.1	127.0.0.1	TCP	44	52870 → 6000 [ACK] Seq=141 Ack=168 Win=65280 Len=0	141	168		
756	19:56:54.841400	127.0.0.1	127.0.0.1	X11	1299	Event: <Unknown eventcode 123>, <Unknown eventcode 116>, MappingNotify, Colo...	168	141	1255	
757	19:56:54.841410	127.0.0.1	127.0.0.1	TCP	44	52870 → 6000 [ACK] Seq=141 Ack=123 Win=64000 Len=0	141	123		
758	19:56:54.841735	127.0.0.1	127.0.0.1	TCP	44	6000 → 52870 [FIN, ACK] Seq=0 Ack=141 Win=65280 Len=0	141	142		
759	19:56:54.841755	127.0.0.1	127.0.0.1	TCP	44	6000 → 52870 [ACK] Seq=142 Ack=142 Win=65280 Len=0	142	142		
760	19:56:54.846227	127.0.0.1	127.0.0.1	TCP	44	6000 → 52870 [FIN, ACK] Seq=142 Ack=142 Win=65280 Len=0	142	142		
761	19:56:54.846263	127.0.0.1	127.0.0.1	TCP	44	52870 → 6000 [ACK] Seq=142 Ack=142 Win=64000 Len=0	142	142		

- Capa de Aplicación (OSI 7): intercambio de mensajes JSON-RPC con estructura definida:
 - initialize: negociación inicial, devuelve protocolVersion, capabilities y serverInfo.
 - describe/list_tools: descubrimiento de herramientas expuestas.
 - call_tool/run: ejecución de la herramienta especificada, con argumentos JSON.



Remoto:

- Capa de Enlace (OSI 2): transmisión de tramas Ethernet/Wi-Fi entre cliente y servidor en la red.



- Capa de Red (OSI 3): direccionamiento IP; en local 127.0.0.1 para servidores locales, y direcciones externas para el servidor remoto en Google Cloud Run.

tcp.port == 443 && !ts

No.	Time	Source	Destination	Protocol	Length	Info	Seq	Ack	BytesInFlight	Len
894266	20:05:44.965780	2803:d100:9::2a06:98c1:31::	2803:d100:99::	TLSv1.2	165	Application Data	925	882	91	
894906	20:05:45.066431	2a06:98c1:3::2803:d100:99::	TLSv1.2	144	Application Data	882	1016	70		
895859	20:05:45.050557	2803:d100:9::2a06:98c1:31::	TLSv1.2	165	Application Data	1016	952	91		
899338	20:05:45.763896	2a06:98c1:3::2803:d100:99::	TLSv1.2	144	Application Data	952	1107	70		
906337	20:05:46.868077	140.82.114...192.168.0.6	TLSv1.2	79	Application Data	51	60	25		
906344	20:05:46.868343	192.168.0.6	140.82.114.25	TLSv1.2	83	Application Data	60	76	29	
111557	20:05:47.616008	2803:d100:9::2600:1900:42::	TLSv1.3	568	Client Hello (SNI=mcg-remoto-703329965527.us-central1.run.app)	1	1	494		
911656	20:05:47.695319	2600:1900:4::2803:d100:99::	TLSv1.3	1294	Server Hello, Change Cipher Spec	1	495	1220		
911657	20:05:47.695319	2600:1900:4::2803:d100:99::	TLSv1.3	1294	Continuation Data	1221	495	2440		
911658	20:05:47.695319	2600:1900:4::2803:d100:99::	TLSv1.3	1294	Continuation Data	2441	495	3660		
911659	20:05:47.695319	2600:1900:4::2803:d100:99::	TLSv1.3	1294	Continuation Data	3661	495	4880		
911660	20:05:47.695319	2600:1900:4::2803:d100:99::	TLSv1.3	1294	Continuation Data	4881	495	6100		
911661	20:05:47.695319	2600:1900:4::2803:d100:99::	TLSv1.3	775	Continuation Data	6101	495	6801		
911709	20:05:47.701651	2803:d100:9::2600:1900:42::	TLSv1.3	154	Change Cipher Spec, Application Data	495	6802	80		
911710	20:05:47.701819	2803:d100:9::2600:1900:42::	TLSv1.3	267	Application Data	575	6802	273		
912352	20:05:47.804871	2600:1900:4::2803:d100:99::	TLSv1.3	964	Application Data, Application Data	6802	768	890		
912362	20:05:47.806097	2803:d100:9::2600:1900:42::	TLSv1.3	98	Application Data	768	7692	24		
925412	20:05:49.859013	2803:d100:9::2600:1901:1::	TLSv1.2	117	Application Data	173	161	43		
925874	20:05:49.931552	2600:1901:1::2803:d100:99::	TLSv1.2	114	Application Data	161	216	40		
927638	20:05:50.211695	2603:1063:2::2803:d100:99::	TLSv1.2	118	Application Data	3812	1216	44		

111557

568 bytes on wire (4544 bits), 568 bytes captured (4544 bits) on interface \Device\NPF_{E7201835-B06E-4298-8000-66318497FD6}, id 0
 Ethernet II, Src: Intel_Bf43:a2 (08d4:a8bf43:a2), Dst: Comscape_9a:e0:74 (f8:63:d9:9a:e0:74)
 Internet Protocol Version 6, Src: 2803:d100:9910:1915:d973:efc1:c2f:5a0, Dst: 2600:1900:4245:2001:
 0110 = Version: 6
 P 0000 0000 = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
 1111 1100 0000 1111 0001 = Flow Label: 0xc0f1
 Payload Length: 534
 Next Header: TCP (6)
 Hop Limit: 64
 Source Address: 2600:1900:4245:2001:1915:d973:efc1:c2f:5a0
 Destination Address: 2600:1900:4245:2001:
 [Stream index: 33]
 Transmission Control Protocol, Src Port: 22789, Dst Port: 443, Seq: 1, Ack: 1, Len: 494

0000 f8 63 d9 9a e0 74 e0 d4 e8 bf 43 a2 86 dd 60 0f c 2 t C
 0010 c0 f1 02 02 06 40 28 03 d1 00 99 10 19 15 d9 73ZL...
 0020 e0 f1 c2 f5 a2 e2 26 00 19 00 42 45 02 00 00 00 ..ZL...
 0030 00 00 00 00 00 00 59 05 01 bb f8 3a 74 7d 70 24 ..IP...tjs
 0040 bb 31 50 18 00 ff 14 ef 00 00 16 03 01 01 e9 01
 0050 01 e5 03 03 93 92 ea 5c 20 4c 9f a2 50 0b 0eL...

wireshark-Wi-FiH8SC03.pcapng

Paquetes: 157260 - Displayed: 1546 (0.1%)

Perfil: Carlos Valladares

- Capa de Transporte (OSI 4): uso de TCP como protocolo confiable para la entrega de mensajes.

Capturando desde Wi-Fi

Archivo

Edición

Visualización

Tr

Captura

Análisis

Herramientas

Telefonía

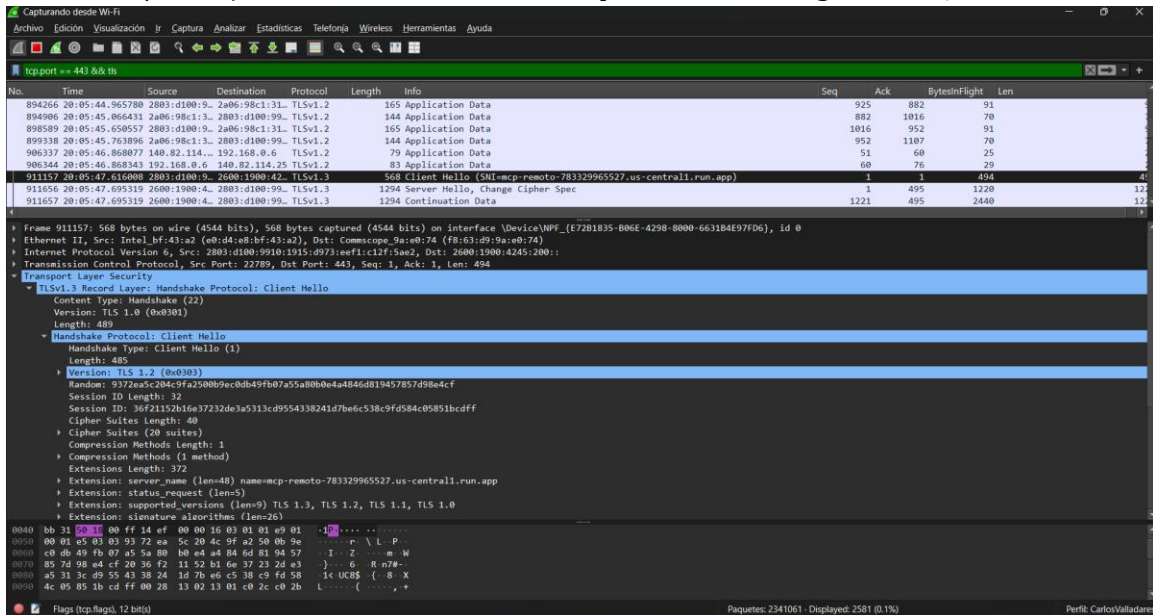
Configuración

Ayuda

</

- Capa de Aplicación (OSI 7): intercambio de mensajes JSON-RPC con estructura definida:
 - initialize: negociación inicial, devuelve protocolVersion, capabilities y serverInfo.
 - describe/list_tools: descubrimiento de herramientas expuestas.

- call_tool/run: ejecución de la herramienta especificada, con argumentos JSON.



3. Conclusiones y comentarios

El proyecto permitió comprobar la utilidad del protocolo MCP como mecanismo de integración entre un chatbot y múltiples servidores especializados. Se logró unificar la gestión de tareas, operaciones financieras, manejo de archivos y control de versiones en un mismo asistente conversacional.

Comentarios principales:

- MCP facilita la interoperabilidad, pero no es plug & play: requiere inicialización y manejo de sesiones.
- Los servidores oficiales (Filesystem, Git) validan que el estándar puede aplicarse a casos reales.
- Las principales dificultades fueron compatibilidad en Windows y validación de nombres de herramientas, resueltas con configuración y sanitización.
- El uso de logs permitió mantener trazabilidad de todas las operaciones.

En conclusión, el proyecto cumplió con los objetivos académicos, integrando teoría de protocolos de red con práctica en sistemas distribuidos.