

New M2Bridge

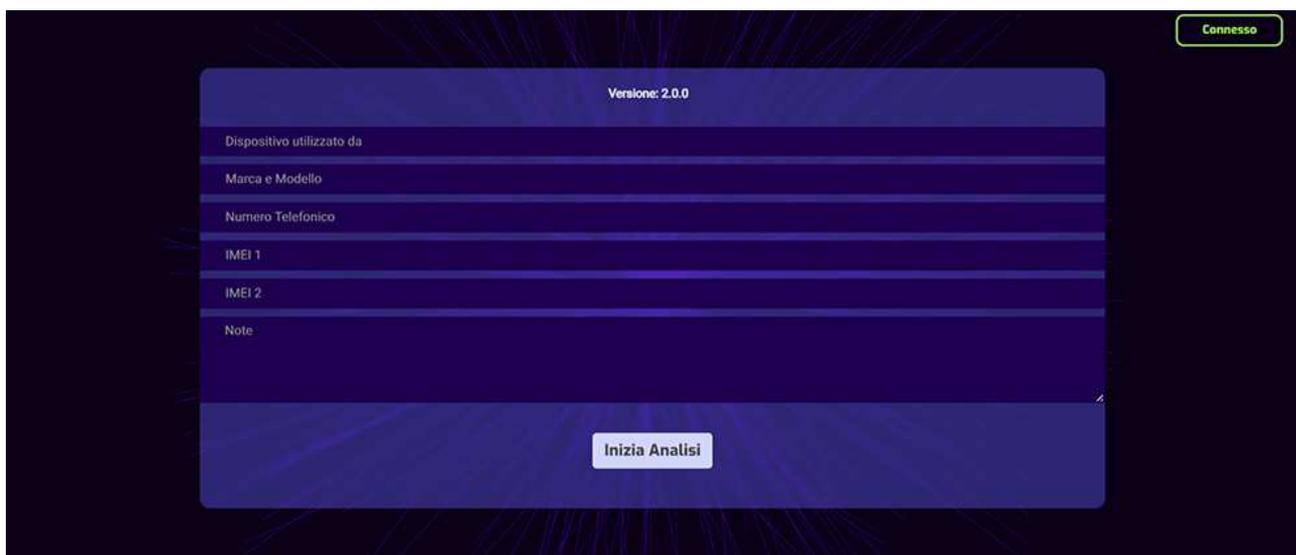
Bonifiche su Smartphone e Tablet



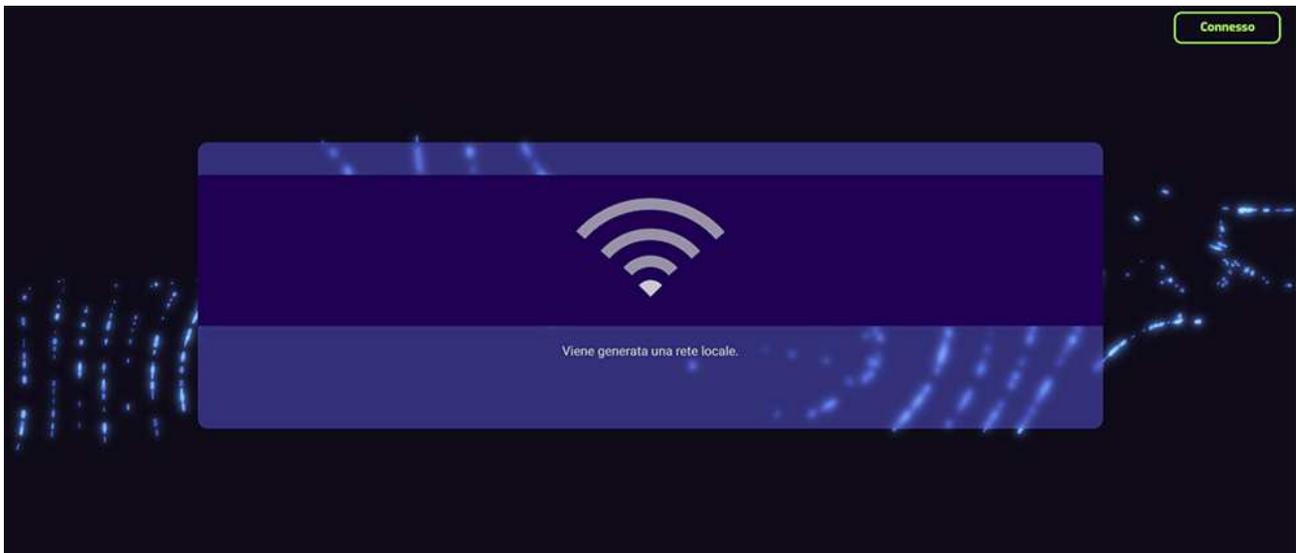
Con l'apparato M2 Bridge New possiamo analizzare il traffico rete di qualsiasi Cellulare o Tablet e comprendere se vi è un Trojan-Software Spy al suo interno.

- Il Cellulare o Tablet da analizzare non viene neppure “toccato dall'operatore”.
- M2 Bridge New è un dispositivo che utilizza la tecnologia di Sniffing – “Man in the Middle” passivo.
- E' sufficiente che il proprietario del cellulare da analizzare si agganci alla rete Wi-Fi locale che M2 Bridge New andrà a generare e segue le indicazioni dell'operatore.
- In automatico verrà generato un **Report** (pdf in italiano) il quale produce documentazione certificata ammissibile ed utilizzabile in corso di procedimento legale + un file *capture.pcap* per utilizzo forense.
- E' possibile analizzare qualsiasi dispositivo con qualunque sistema operativo.
- Analisi estremamente veloce e automatizzata.
- **Nessun collegamento a server esterni.**
- **Nessun analisi da REMOTO tramite tunnel VPN.**
- Aggiornamenti sempre disponibili.
- Valigia Antiurto, dimensioni: 36x26x14,5 cm – peso: 4 kg.
- Connessione Wi Fi per utilizzo PC o Tablet esterni ad M2 Bridge New.
- Batteria interna ad alta capacità, autonomia oltre 10 ore. Ricarica circa 4 ore.
- Monitor Apple iPad.
- Connettore USB direttamente nel pannello per scaricare il Report.
- Possibilità di inviare il Report con Airdrop o E-mail oppure caricarlo su un Cloud.
- Connettore SIM direttamente nel pannello.
- Connettore esterno RJ45 per connessione senza SIM.
- Due ventole esterne più una interna.

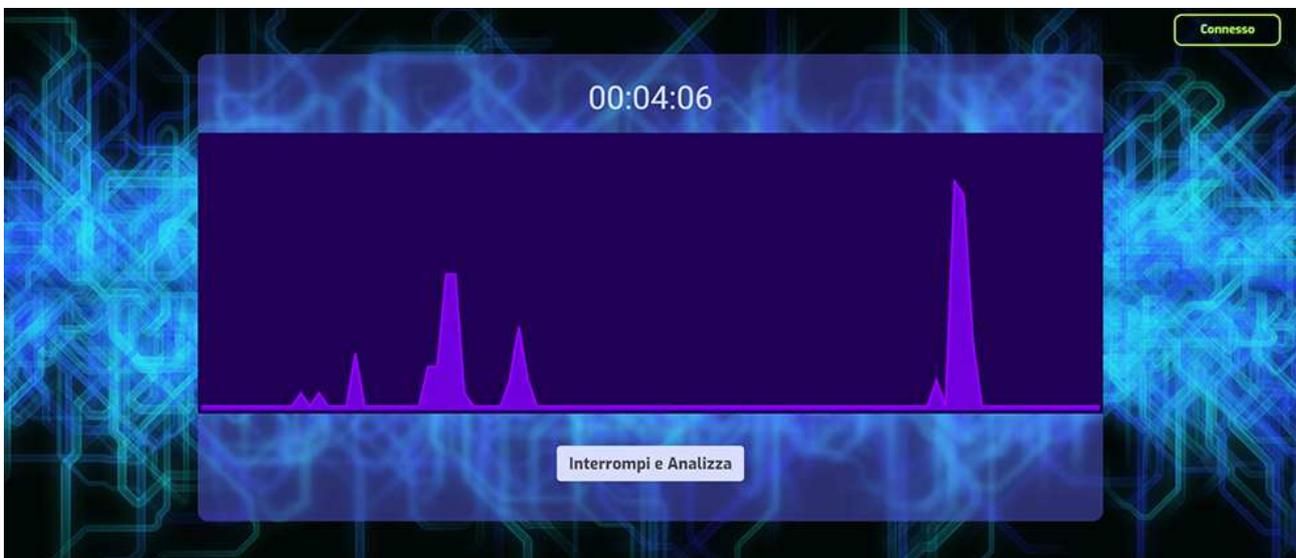
Alcuni screenshot di M2 Bridge New



- Possibilità di inserire del testo manualmente, le informazioni immesse verranno automaticamente incluse nel Report in PDF.
- Controllo sempre attivo di verifica della connessione.



- Possibilità di generare una rete Wi-Fi temporanea per l'analisi del dispositivo.
- SSID e Password sempre differenti per ogni analisi.



- Analisi del dispositivo connesso.
- Sniffing (Man in the Middle passivo).



- Primo responso.

Analisi Effettuata

Comunicazioni che necessitano approfondimenti

INDICE DI COMPROMISSIONE: ALTO DMTRO

È stata effettuata una richiesta DNS a **mobile-tracker-data.com** con contrassegno Trojan Software Spy.

Il nome di dominio **mobile-tracker-data.com** visualizzato nell'acquisizione è stato esplicitamente contrassegnato come dannoso. Questo comportamento è palesemente indicativo. Sicuramente il dispositivo è compromesso da un Trojan Software Spy.

Indirizzo IP	Protocollo	Porta	2 Dominio	Certificato
51.158.154.183	TLS	443	mobile-tracker-data.com	SNI: mobile-tracker-data.com; SNI: undefined

3 ⇌ Controllo IP
Controllo URL ⇌ 4

INDICE DI COMPROMISSIONE: BASSO HCHST

Il server 1.1.1.1 non è stato risolto da nessuna query DNS durante la sessione

Questo indica che il server 1.1.1.1 probabilmente non è stato risolto da nessun nome di dominio o che la risoluzione è già

- Relazione completa.
- 1 collegamento al Whois Domain Tools.
- 2 collegamento al Dominio.
- 3 collegamento a ipTRACKERonline.
- 4 collegamento a SECURI.

Nel Report in PDF, generato automaticamente, avremo:

- Dispositivo utilizzato da; Marca e Modello; Numero Telefonico; IMEI 1; IMEI 2; Note; queste informazioni saranno presenti solo se precedentemente inserite.

In automatico:

- Rapporto generato in data e ora.
 - La durata dell'acquisizione in secondi.
 - Inizio dell'acquisizione.
 - Termine dell'acquisizione.
 - Il numero dei pacchetti.
 - Il BLAKE2s di acquisizione.
 - Indirizzo MAC del dispositivo.
-
- Inoltre avremo le descrizioni date dagli Indicatori di Compromissione.
 - Il posizionamento delle Comunicazioni e di tutte le trasmissioni intercettate:
 - L'indirizzo IP di destinazione - il numero della Porta di destinazione - il Protocollo - il Dominio (se disponibile) – il Certificato.

Esempio di Report in PDF
(si genera automaticamente)

Rapporto di Acquisizione	
Dispositivo utilizzato da: Mario Rossi	Marca e modello: Samsung Galaxy S10
Numero telefonico: 33826985412	Rapporto generato in data e ora: 02/07/2024 - 15:12:13
Durata acquisizione: 113,277351391 secondi	Indirizzo MAC dispositivo: 7a:18:da:77:a7:29
Inizio acquisizione: 2024/07/02 - 15:10:06	IMEI 1: 355962378921453
Termine acquisizione: 2024/07/02 - 15:11:59	IMEI 2: 352661578921841
Numero di pacchetti: 11007	BLAKE2s acquisizione: 98116a7eb405886164ad978112350ac8 38a47e6d1cb391d333737720a54fe76c
Note: Analisi effettuata dal tecnico Ing. Paolo Brambilla presso la sede del cliente.	

Il dispositivo è compromesso da Trojan Software Spy poiché sono presenti uno avvisi con priorità elevata.

INDICE DI COMPROMISSIONE
ALTO

ANALISI
DMTRO

È stata effettuata una richiesta DNS a mobile-tracker-data.com con contrassegno Trojan Software Spy.

Il nome di dominio **mobile-tracker-data.com** visualizzato nell'acquisizione è stato esplicitamente contrassegnato come dannoso. Questo comportamento è palesemente indicativo. Sicuramente il dispositivo è compromesso da un Trojan Software Spy.

INDICE DI COMPROMISSIONE
MODERATO

ANALISI
INPRD

UDP comunicazione in uscita dalla rete locale a 157.240.203.14.

Il protocollo **UDP** è comunemente utilizzato nelle reti interne. Verificare se l'host **157.240.203.14** ha sfruttato altri avvisi, fattore che potrebbe indicare un possibile comportamento dannoso.

INDICE DI COMPROMISSIONE
BASSO

ANALISI
NCHST

Il server 149.154.167.151 non è stato risolto da nessuna query DNS durante la sessione

Questo indica che il server **149.154.167.151** probabilmente non è stato risolto da nessun nome di dominio o che la risoluzione è già stata memorizzata nella cache dal dispositivo. Se l'host viene visualizzato in altri avvisi, controllarlo.

INDICE DI COMPROMISSIONE
BASSO

ANALISI
HTPBG

Sono state generate comunicazioni HTTP dirette all'host www.semanticscholar.org

Il dispositivo ha effettuato uno scambio con l'host **www.semanticscholar.org** utilizzando HTTP, un protocollo non criptato. Anche se questo comportamento non è dannoso in sé, è raro rilevare comunicazioni HTTP generate da applicazioni per smartphone in esecuzione in background. Controllare la reputazione dell'host effettuando una ricerca in Internet.

connessione a 149.154.167.50 tramite una porta superiore o uguale a 1024.

Sono state rilevate connessioni a **149.154.167.50** tramite la porta **5222**. L'utilizzo di una porta non standard a volte può essere associato ad attività dannose. È consigliabile verificare se questo host ha una buona reputazione esaminando altri avvisi ed effettuando una ricerca in Internet.

Comunicazioni che necessitano approfondimenti

IP	Porta	Protocollo	Dominio	Certificato
di destinazione				
51.158.154.183	443	TLS	mobile-tracker-data.com	mobile-tracker-data.com
18.66.218.126	80, 80	HTTP, TCP	www.semanticscholar.org	
149.154.167.151	443	TCP		
157.240.203.14	443	UDP		

Comunicazioni non categorizzate

IP	Porta	Protocollo	Dominio	Certificato
di destinazione				
52.84.150.50	443	TLS	venmo.com	venmo.com
--	53	DNS	GOOGLE.COM	
--	53	DNS	google.com.onion	

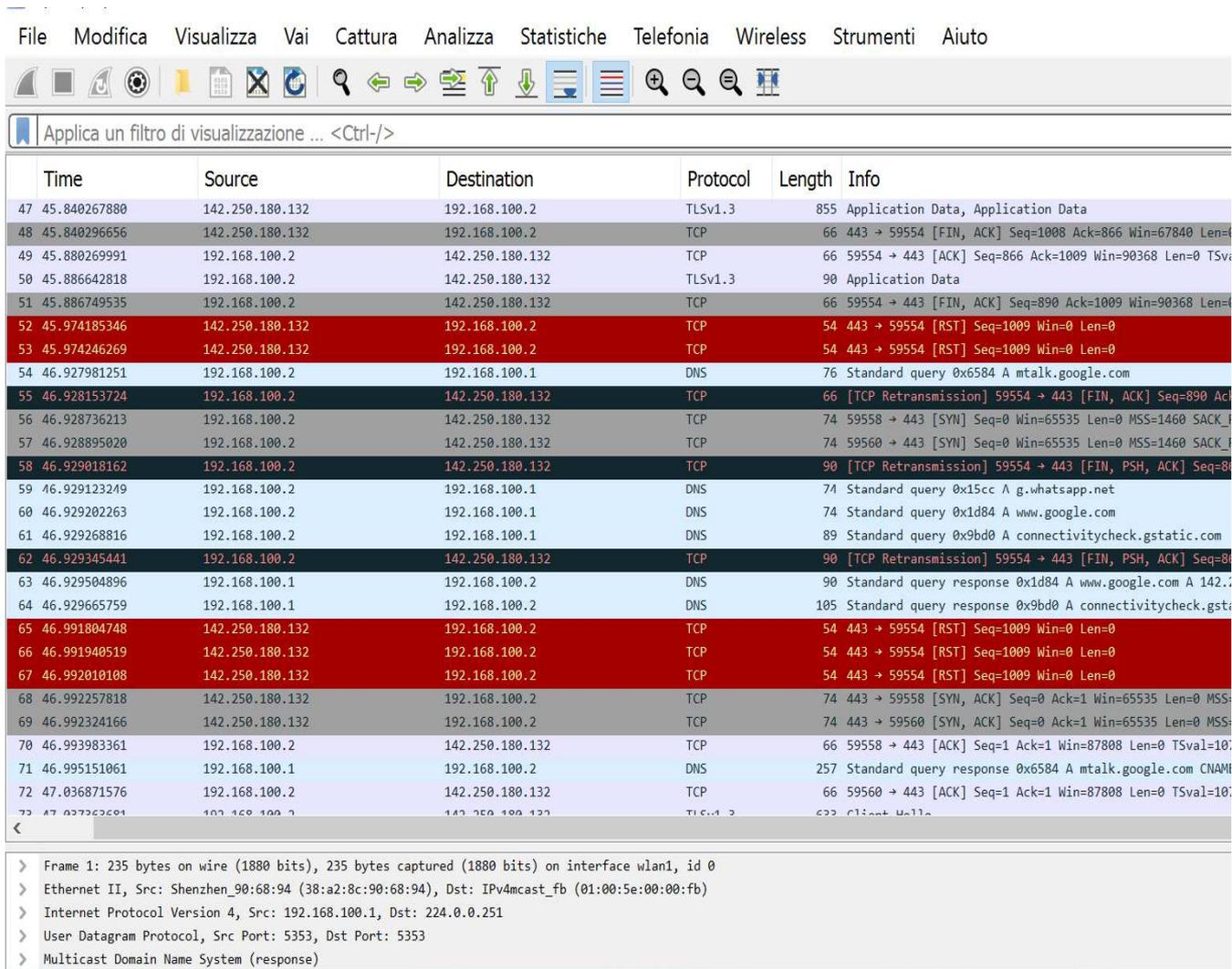
Comunicazioni inserite nella whitelist

IP	Porta	Protocollo	Dominio	Certificato
di destinazione				
10.42.0.68	68, --	DHCP, ICMP		
ff02:0000:0000:0000:0000:0000:0000:0002	--	IPV6-ICMP		

IP	Porta	Protocollo	Dominio	Certificato
di destinazione				
ff02:0000:0000:0000:0000:0000:0000:00fb	5353	UDP		
224.0.0.251	5353	UDP		
ff02:0000:0000:0000:0000:0000:0000:0016	--	IPV6-ICMP		
142.251.209.3	80	HTTP	connectivitycheck.gstatic.com	
ff02:0000:0000:0000:0000:0001:ff77:a729	--	IPV6-ICMP		
104.18.35.70	443	TLS	cdn.zimperium.com	cdn.zimperium.com, cdn.zimperium.com, cdn.zimperium.com, cdn.zimperium.com
54.73.148.110	443	TLS	netflix.com	netflix.com
151.101.66.167	443	TLS	twitch.tv	twitch.tv
104.91.22.142	443	TLS	www.disneyplus.com	www.disneyplus.com
216.58.204.132	443	TLS	www.google.com	www.google.com
157.240.203.61	5222, 443	TCP, TCP	g.whatsapp.net	
31.13.86.8	443	TLS		web.facebook.com
157.240.203.17	443	TLS	edge-mqtt.facebook.com	edge-mqtt.facebook.com
157.240.203.14	443, 443	TLS, UDP	graph.facebook.com, api.facebook.com, web.facebook.com	api.facebook.com, graph.facebook.com
157.240.203.13	443	TLS	gateway.facebook.com	gateway.facebook.com
151.101.67.42	443	TLS	open.spotify.com	open.spotify.com
108.157.188.43	443	TLS	mtddemo-cdn.zimperium.com	mtddemo-cdn.zimperium.com, mtddemo-cdn.zimperium.com
184.87.212.59	80, 80	HTTP, TCP	www.samsung.com	
18.66.196.108	80, 80	HTTP, TCP	www.tizen.org	
108.177.119.188	5228	TLS	mtalk.google.com	mtalk.google.com

Oltre al Report verrà generato, sempre automaticamente, un file *capture.pcap* per utilizzo forense.

Esempio di file *capture.pcap* (si genera automaticamente)



File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto

Applica un filtro di visualizzazione ... <Ctrl-/>

	Time	Source	Destination	Protocol	Length	Info
47	45.840267880	142.250.180.132	192.168.100.2	TLSv1.3	855	Application Data, Application Data
48	45.840296656	142.250.180.132	192.168.100.2	TCP	66	443 → 59554 [FIN, ACK] Seq=1008 Ack=866 Win=67840 Len=0
49	45.880269991	192.168.100.2	142.250.180.132	TCP	66	59554 → 443 [ACK] Seq=866 Ack=1009 Win=90368 Len=0 TSv
50	45.886642818	192.168.100.2	142.250.180.132	TLSv1.3	90	Application Data
51	45.886749535	192.168.100.2	142.250.180.132	TCP	66	59554 → 443 [FIN, ACK] Seq=890 Ack=1009 Win=90368 Len=0
52	45.974185346	142.250.180.132	192.168.100.2	TCP	54	443 → 59554 [RST] Seq=1009 Win=0 Len=0
53	45.974246269	142.250.180.132	192.168.100.2	TCP	54	443 → 59554 [RST] Seq=1009 Win=0 Len=0
54	46.927981251	192.168.100.2	192.168.100.1	DNS	76	Standard query 0x6584 A mtalk.google.com
55	46.928153724	192.168.100.2	142.250.180.132	TCP	66	[TCP Retransmission] 59554 → 443 [FIN, ACK] Seq=890 Ac
56	46.928736213	192.168.100.2	142.250.180.132	TCP	74	59558 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_I
57	46.928895020	192.168.100.2	142.250.180.132	TCP	74	59560 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_I
58	46.929018162	192.168.100.2	142.250.180.132	TCP	90	[TCP Retransmission] 59554 → 443 [FIN, PSH, ACK] Seq=8
59	46.929123249	192.168.100.2	192.168.100.1	DNS	74	Standard query 0x15cc A g.whatsapp.net
60	46.929202263	192.168.100.2	192.168.100.1	DNS	74	Standard query 0x1d84 A www.google.com
61	46.929268816	192.168.100.2	192.168.100.1	DNS	89	Standard query 0x9bd0 A connectivitycheck.gstatic.com
62	46.929345441	192.168.100.2	142.250.180.132	TCP	90	[TCP Retransmission] 59554 → 443 [FIN, PSH, ACK] Seq=8
63	46.929504896	192.168.100.1	192.168.100.2	DNS	90	Standard query response 0x1d84 A www.google.com A 142.7
64	46.929665759	192.168.100.1	192.168.100.2	DNS	105	Standard query response 0x9bd0 A connectivitycheck.gsti
65	46.991804748	142.250.180.132	192.168.100.2	TCP	54	443 → 59554 [RST] Seq=1009 Win=0 Len=0
66	46.991940519	142.250.180.132	192.168.100.2	TCP	54	443 → 59554 [RST] Seq=1009 Win=0 Len=0
67	46.992010108	142.250.180.132	192.168.100.2	TCP	54	443 → 59554 [RST] Seq=1009 Win=0 Len=0
68	46.992257818	142.250.180.132	192.168.100.2	TCP	74	443 → 59558 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=
69	46.992324166	142.250.180.132	192.168.100.2	TCP	74	443 → 59560 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=
70	46.993983361	192.168.100.2	142.250.180.132	TCP	66	59558 → 443 [ACK] Seq=1 Ack=1 Win=87808 Len=0 TSval=10:
71	46.995151061	192.168.100.1	192.168.100.2	DNS	257	Standard query response 0x6584 A mtalk.google.com CNAMI
72	47.036871576	192.168.100.2	142.250.180.132	TCP	66	59560 → 443 [ACK] Seq=1 Ack=1 Win=87808 Len=0 TSval=10:
73	47.037223201	192.168.100.2	142.250.180.132	TLSv1.3	622	Client Hello

> Frame 1: 235 bytes on wire (1880 bits), 235 bytes captured (1880 bits) on interface wlan1, id 0
> Ethernet II, Src: Shenzhen_90:68:94 (38:a2:8c:90:68:94), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
> Internet Protocol Version 4, Src: 192.168.100.1, Dst: 224.0.0.251
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
> Multicast Domain Name System (response)