M2 Bridge New

Smartphone and tablet forensics

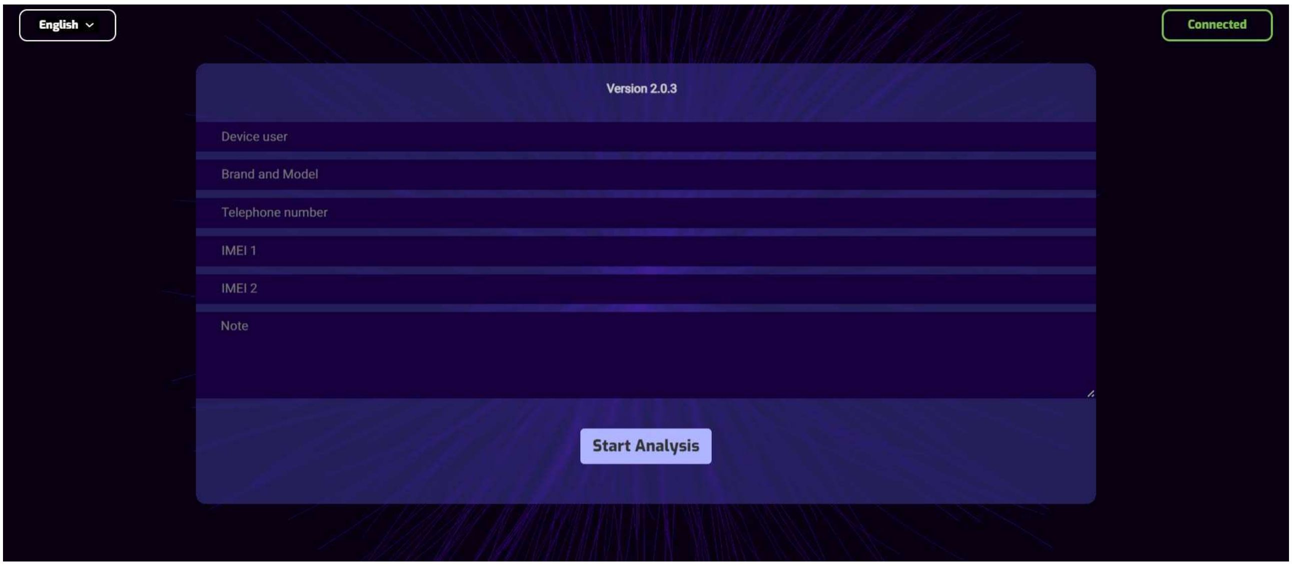
MADE IN ITALY

CE

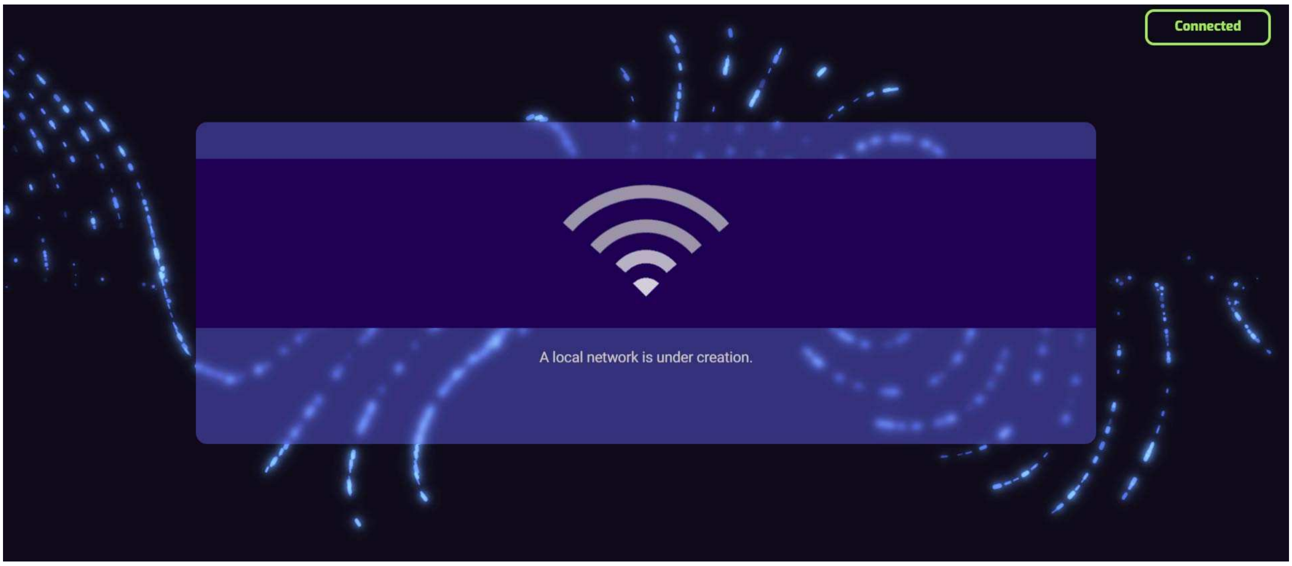
With the M2 Bridge New device, we can analyze the network traffic of any mobile phone or tablet and determine if there is a *Trojan Software Spy* inside.

- The mobile phone or tablet to be analyzed is not even "touched by the operator".
- M2 Bridge New is a device that uses Sniffing “Man in the Middle passive” technology .
- It ‘s sufficient for the owner of the mobile phone to be analyzed to connect to the local Wi-Fi network that M2 Bridge New will generate and follow the operator's instructions.
- A **Report** will be automatically generated which produces certified documentation that is admissible and usable during legal proceedings + a capture.pcap file for forensic use.
- It is possible to analyze any device with any operating system.
- Extremely fast and automated analysis.
- **No connection to external servers.**
- **No remote analysis.**
- Updates always available.
- Shockproof Suitcase, dimensions: 36x26x14,5 cm – weight: 4 kg.
- Wi-Fi connection for using PCs or Tablets external to M2 Bridge New.
- High capacity internal battery, autonomy over 10 hours. Charging approximately 4 hours.
- Apple iPad Monitors.
- USB connector directly into the panel to download the Report.
- Ability to send the Report via Airdrop or Email or upload it to a Cloud.
- SIM connector directly in the panel.
- External RJ45 connector for connection without SIM.
- Two external fans plus one internal one.

Some screenshots of M2 Bridge New

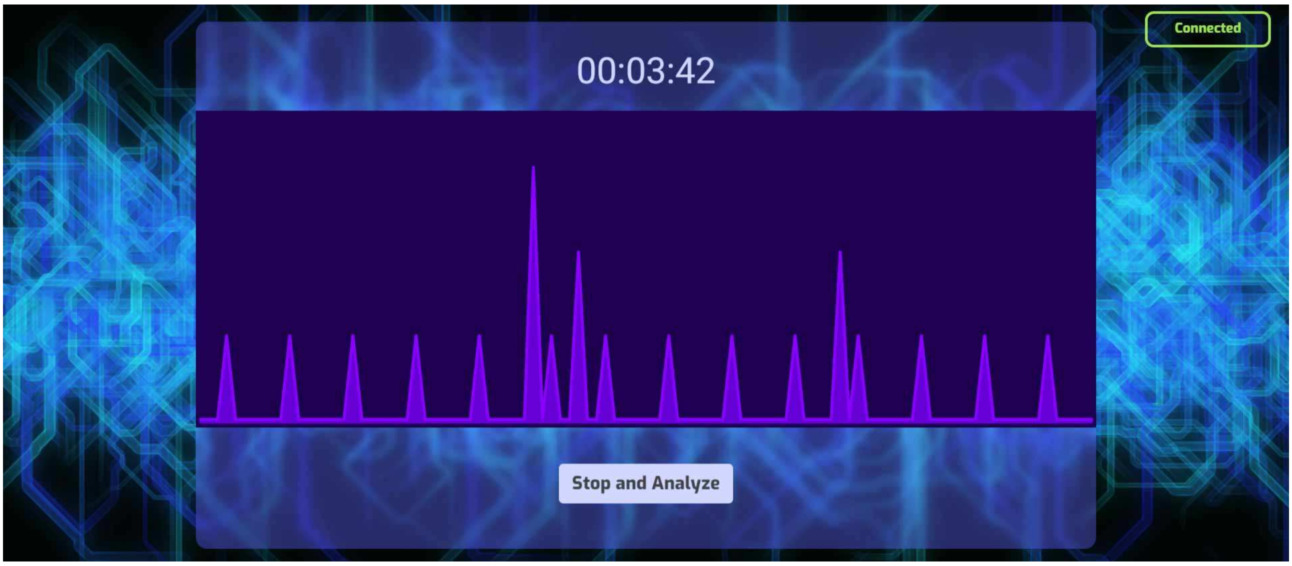


- Ability to enter text manually, the information entered will be automatically included in the PDF Report.
- Always-on connection verification check.

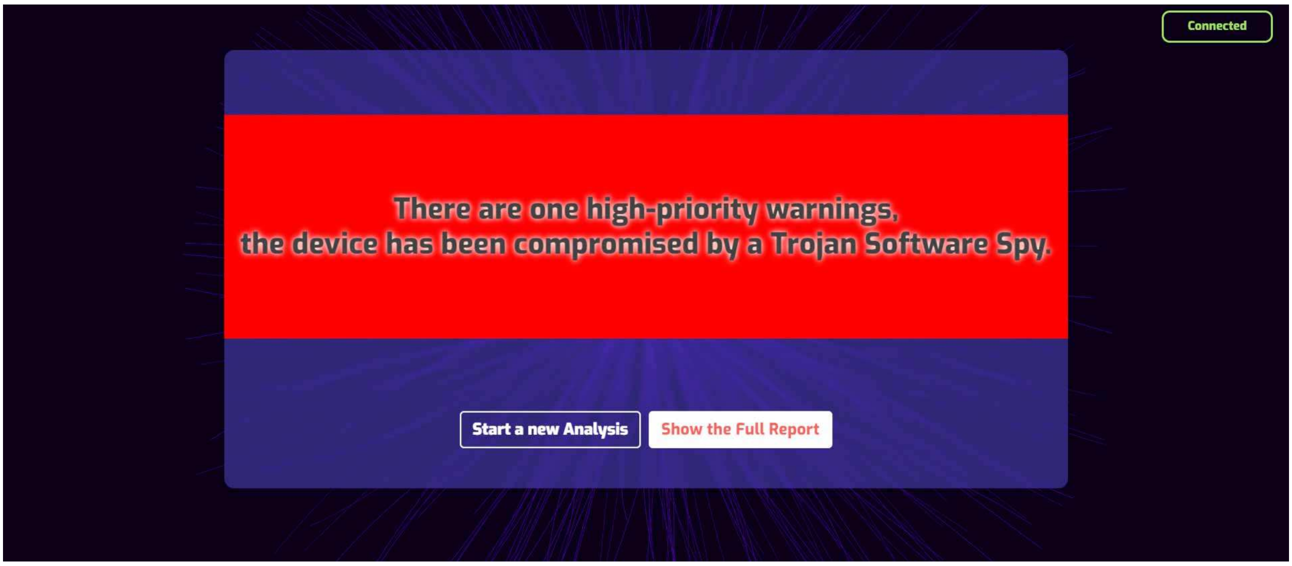


A local network is under creation.

- Ability to generate a temporary Wi-Fi network for device analysis.
- SSID and Password always different for each analysis.

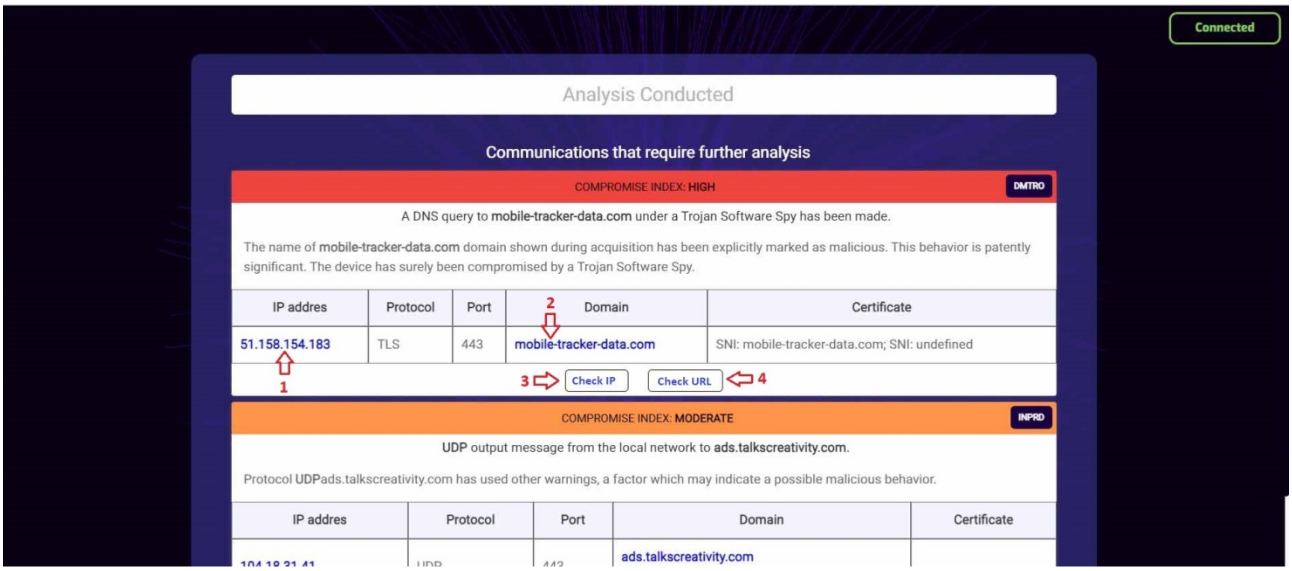


- Connected device analysis.
- Sniffing (Man in the Middle passive).



There are one high-priority warnings,
the device has been compromised by a Trojan Software Spy.

- First response.



Analysis Conducted

Communications that require further analysis

COMPROMISE INDEX: **HIGH**

A DNS query to **mobile-tracker-data.com** under a Trojan Software Spy has been made.

The name of **mobile-tracker-data.com** domain shown during acquisition has been explicitly marked as malicious. This behavior is patently significant. The device has surely been compromised by a Trojan Software Spy.

IP addres	Protocol	Port	Domain	Certificate
51.158.154.183	TLS	443	mobile-tracker-data.com	SNI: mobile-tracker-data.com; SNI: undefined

COMPROMISE INDEX: **MODERATE**

UDP output message from the local network to **ads.talkscreativity.com**.

Protocol **UDP**ads.talkscreativity.com has used other warnings, a factor which may indicate a possible malicious behavior.

IP addres	Protocol	Port	Domain	Certificate
104.18.31.41	UDP	443	ads.talkscreativity.com	

- Full report.
- 1 link to Whois Domain Tools.
- 2 link to Domain
- 3 link to ipTRACKERonline.
- 4 link to SECURI.

In the automatically generated PDF report, we will have:

- Device user; Brand and Model; Telephone number; IMEI 1; IMEI 2; Notes; this information will only be present if previously entered.

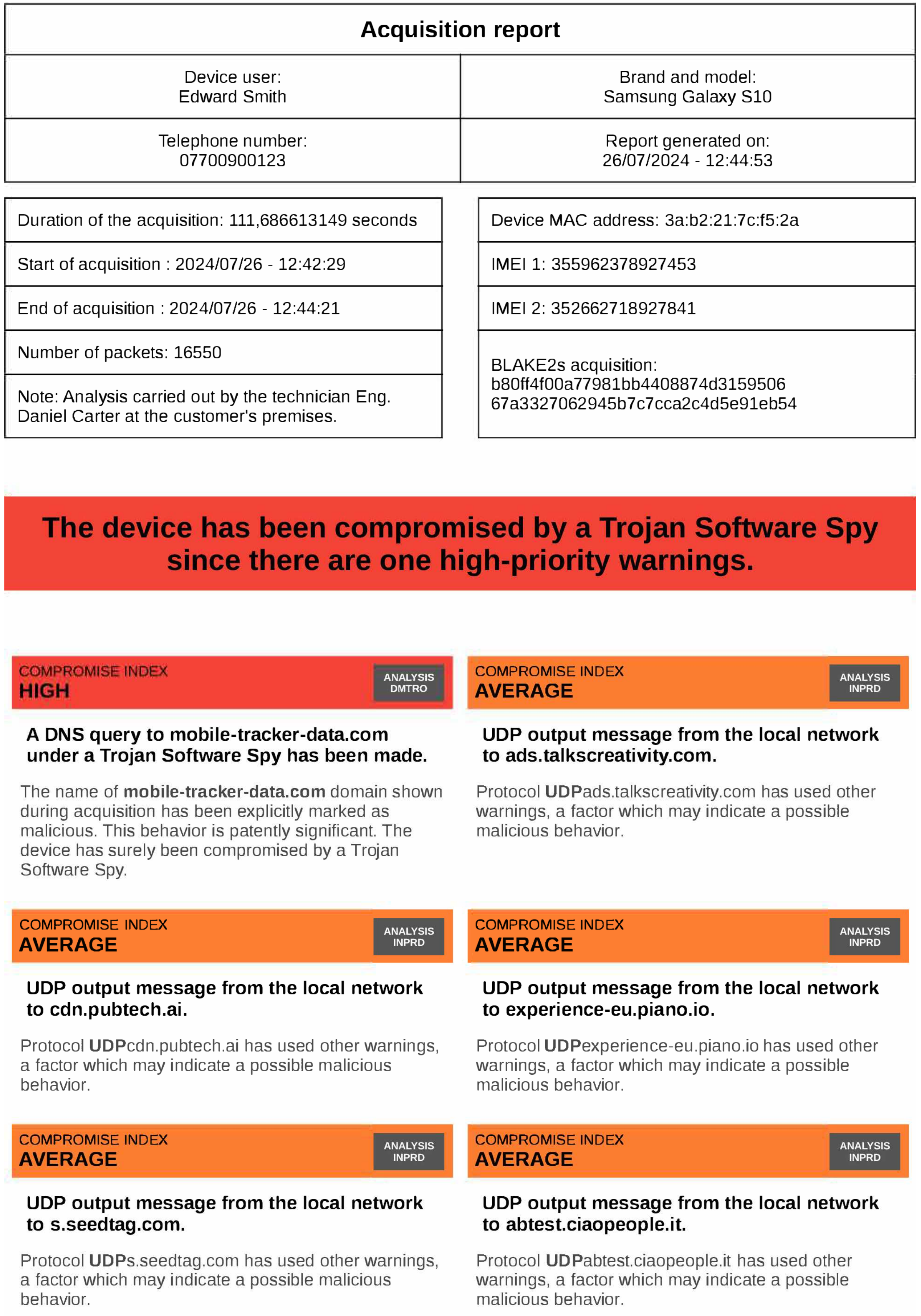
Automatically:

- Report generated on.
- Duration of the aquisition in seconds.
- Start of acquisition.
- End of acquisition.
- Number of packets.
- BLAKE2s of acquisition.
- Device MAC address.

- We will also have the descriptions given by the Indicators of Compromise.
- The positioning of Communications and all intercepted transmissions:
- The destination IP address - the destination Port number - the Protocol the Domain (if available) - the Certificate (if available).

PDF Report Example

(It generates automatically)



Acquisition report	
Device user: Edward Smith	Brand and model: Samsung Galaxy S10
Telephone number: 07700900123	Report generated on: 26/07/2024 - 12:44:53

Duration of the acquisition: 111,686613149 seconds	Device MAC address: 3a:b2:21:7c:f5:2a
Start of acquisition : 2024/07/26 - 12:42:29	IMEI 1: 355962378927453
End of acquisition : 2024/07/26 - 12:44:21	IMEI 2: 352662718927841
Number of packets: 16550	BLAKE2s acquisition: b80ff4f00a77981bb4408874d3159506 67a3327062945b7c7cca2c4d5e91eb54
Note: Analysis carried out by the technician Eng. Daniel Carter at the customer's premises.	

The device has been compromised by a Trojan Software Spy since there are one high-priority warnings.

COMPROMISE INDEX
HIGH
ANALYSIS DMTRO

A DNS query to mobile-tracker-data.com under a Trojan Software Spy has been made.

The name of **mobile-tracker-data.com** domain shown during acquisition has been explicitly marked as malicious. This behavior is patently significant. The device has surely been compromised by a Trojan Software Spy.

COMPROMISE INDEX
AVERAGE
ANALYSIS INPRD

UDP output message from the local network to ads.talkscreativity.com.

Protocol **UDP**ads.talkscreativity.com has used other warnings, a factor which may indicate a possible malicious behavior.

COMPROMISE INDEX
AVERAGE
ANALYSIS INPRD

UDP output message from the local network to cdn.pubtech.ai.

Protocol **UDP**cdn.pubtech.ai has used other warnings, a factor which may indicate a possible malicious behavior.

COMPROMISE INDEX
AVERAGE
ANALYSIS INPRD

UDP output message from the local network to experience-eu.piano.io.

Protocol **UDP**experience-eu.piano.io has used other warnings, a factor which may indicate a possible malicious behavior.

COMPROMISE INDEX
AVERAGE
ANALYSIS INPRD

UDP output message from the local network to s.seedtag.com.

Protocol **UDP**s.seedtag.com has used other warnings, a factor which may indicate a possible malicious behavior.

COMPROMISE INDEX
AVERAGE
ANALYSIS INPRD

UDP output message from the local network to abtest.ciaopeople.it.

Protocol **UDP**abtest.ciaopeople.it has used other warnings, a factor which may indicate a possible malicious behavior.

COMPROMISE INDEX
AVERAGE

ANALYSIS INPRD

UDP output message from the local network to cdn.pubtech.ai.

Protocol **UDP**cdn.pubtech.ai has used other warnings, a factor which may indicate a possible malicious behavior.

COMPROMISE INDEX
AVERAGE

ANALYSIS INPRD

UDP output message from the local network to t.seedtag.com.

Protocol **UDP**t.seedtag.com has used other warnings, a factor which may indicate a possible malicious behavior.

COMPROMISE INDEX
AVERAGE

ANALYSIS FRCRT

An SSL connection to ms-cookie-sync.presage.io is using a free certificate.

Free certificates such as Let's Encrypt are widely used by command and control servers linked to malicious implants or phishing websites. It is recommendable you check the host linked to this certificate. Pay attention to the name of the domain and to the date of creation or check its reputation on the Internet.

COMPROMISE INDEX
LOW

ANALYSIS NCHST

Server 149.154.167.50 has not been fixed by any DNS query during the session

This suggests that server **149.154.167.50** has not been fixed by any domain name or that the fixing has already been stored in the cache by the device. If the host is shown in other warnings, check it.

COMPROMISE INDEX
LOW

ANALYSIS NCHST

Server 149.154.166.120 has not been fixed by any DNS query during the session

This suggests that server **149.154.166.120** has not been fixed by any domain name or that the fixing has already been stored in the cache by the device. If the host is shown in other warnings, check it.

COMPROMISE INDEX
LOW

ANALYSIS NCHST

Server 149.154.175.60 has not been fixed by any DNS query during the session

This suggests that server **149.154.175.60** has not been fixed by any domain name or that the fixing has already been stored in the cache by the device. If the host is shown in other warnings, check it.

Communications that require further analysis

IP	Port	Protocol	Domain	Certificate
of destination				
149.154.167.50	443	TCP		
149.154.166.120	443	TCP		
52.19.50.187	443	TLS	ms-cookie-sync.presage.io	ms-cookie-sync.presage.io
34.149.50.64	443, 443, 443	TLS, UDP, TCP	s.seedtag.com	s.seedtag.com
108.157.188.84	443, 443	TLS, UDP	abtest.ciaopeople.it	abtest.ciaopeople.it
104.16.144.111	443, 443	TLS, UDP	experience-eu.piano.io, code.piano.io, id-eu.piano.io, c2-eu.piano.io, buy-eu.piano.io	buy-eu.piano.io
51.158.154.183	443	TLS	mobile-tracker-data.com	mobile-tracker-data.com

IP	Port	Protocol	Domain	Certificate
of destination				
			js.omg.neodatagroup.com, trz.neodatagroup.com, tracker.neodatagroup.com	
2.16.22.231	443	TCP	sync-jp.im-apps.net	
--	53	DNS	pxl.connexity.net	
--	53	DNS	id.geistm.com	

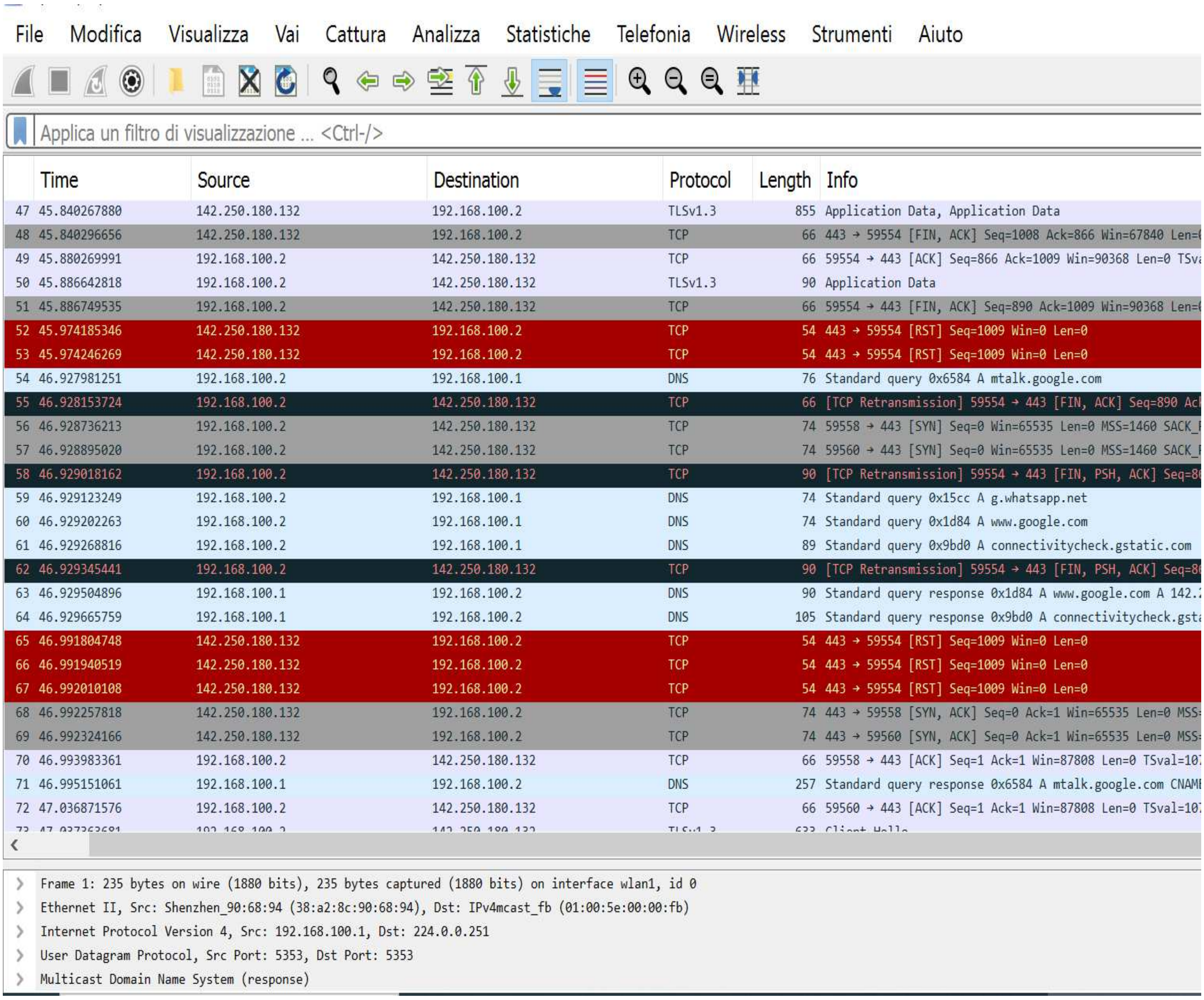
Whitelisted communications

IP	Port	Protocol	Domain	Certificate
of destination				
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		
ff02:0000:0000:0000:0000:0001:ff26:c974	--	IPV6-ICMP		
108.139.243.28	443	TLS	config.aps.amazon-adsystem.com	config.aps.amazon-adsystem.com
34.192.193.130	443	TLS	jadserve.postrelease.com	jadserve.postrelease.com
37.157.6.243	443	TLS	c1.adform.net, dmp.adform.net	dmp.adform.net
178.250.7.13	443	TLS	gum.criteo.com	gum.criteo.com
108.157.198.129	443	TLS	dayjlzv1ljqs2.cloudfront.net	dayjlzv1ljqs2.cloudfront.net
184.87.213.205	443, 443	TLS, TCP	images.outbrainimg.com	images.outbrainimg.com
2.20.157.131	443	TLS	a.teads.tv	a.teads.tv
216.239.34.181	443, 443	TLS, UDP	analytics.google.com	analytics.google.com
34.250.83.82	443	TLS	secure-it.imrworldwide.com	secure-it.imrworldwide.com
108.138.190.150	443	TLS	c.amazon-adsystem.com	c.amazon-adsystem.com

In addition to the Report, a *capture.pcap* file will be automatically generated for forensic use.

Example of capture.pcap file

(It generates automatically)



	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=
49	45.880269991	192.168.100.2	142.250.180.132	TCP	66	59554 → 443 [ACK] Seq=866 Ack=1009 Win=90368 Len=0 TSva
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=
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_
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_
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.
64	46.929665759	192.168.100.1	192.168.100.2	DNS	105	Standard query response 0x9bd0 A connectivitycheck.gst
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 CNAM
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	47.037363681	192.168.100.2	142.250.180.132	TLSv1.3	633	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)
```