tnc25 THE COMMUNITY HUB

Innovation Programme Spotlight

MANANA
(Mobile App Network trAffic Nutrition fActs)

Giuseppe Aceto

Università di Napoli Federico II

Project start funded by

GÉANT Innovation Programme 2024

Two halves: the research...

- **mobile app traffic** constitutes **about 1/3 of all Internet traffic***
- mobile apps **communication patterns** can depend on multiple aspects, all **dynamic** in nature, and **hard to observe/control/model**
  - user actions
  - third-party components
    - services (advertising, payment gateways, map, social login)
    - scripts (progressive apps)
  - network conditions

Network traffic observation is necessary to many endeavours, but is **limited by privacy issues**: only app **developers**, service **providers**, network **operators**, and **third-party** service providers have different degrees of visibility (notably, **not the user**), and can't/won't share them.

* According to [sandvine2024gipr], on the average total rate worldwide (~33 EB/day)

Two halves: … and the user

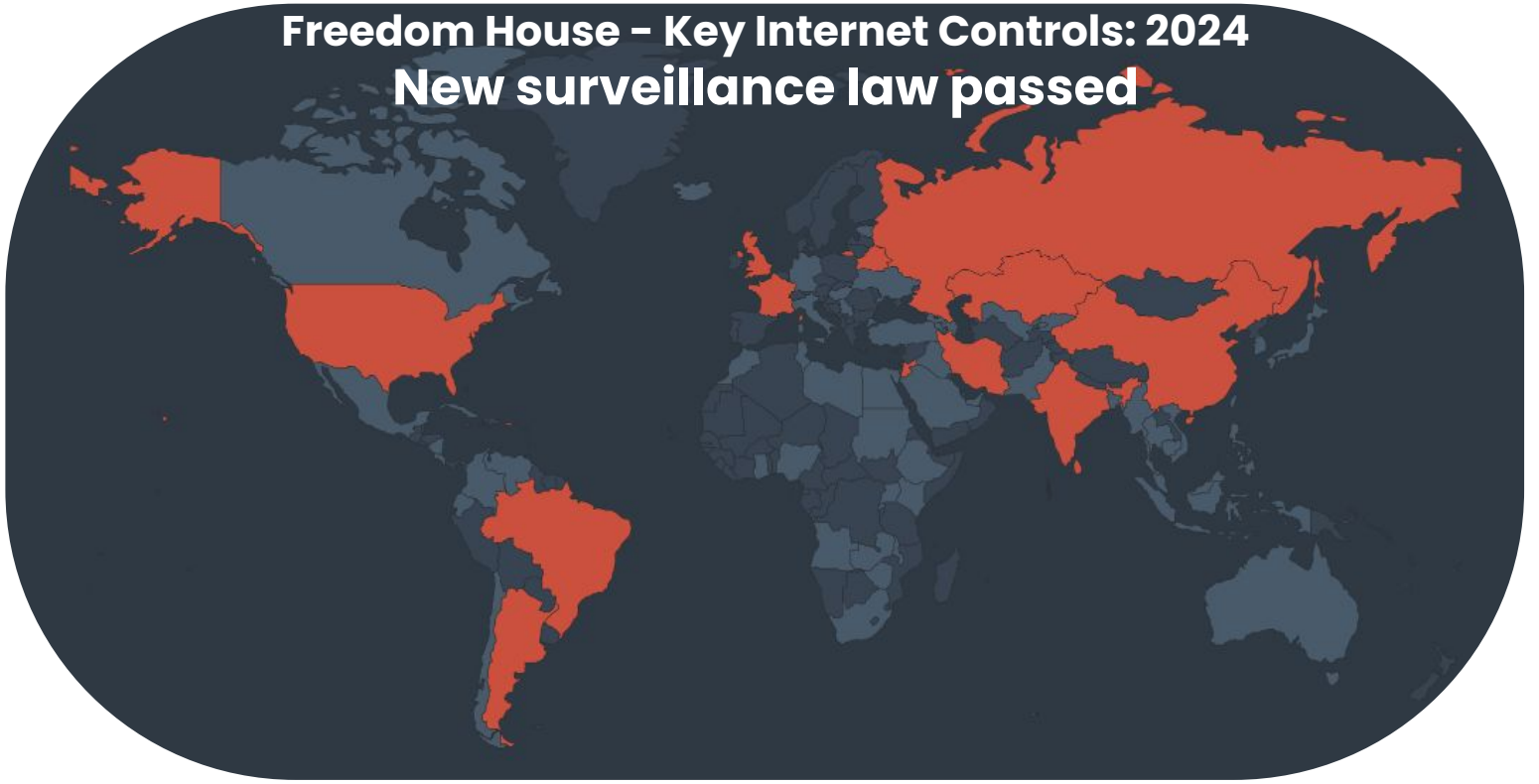
To reach a significant number of users, for a non-negligible duration of time, the monitoring service must continually **provide value to the user**

MANANA provides the user with the answer to a number of questions

- ***which country*** *my mobile apps are communicating with*, in their everyday functioning? and ***how much***?
- do these communications happen in **clear** or **encrypted**?
- which **countries** are **traversed** by my traffic?
- which countries the **managers of the network** infrastructure are accountable to?
- is this **behavior** the same for **different apps** that provide the **same kind of service**?
- is this **behavior** the same for **different mobile operators**?

Why should the user care: regulation exposure

- **national governments** have been **regulating mobile apps usage** and enforcing *Internet censorship* by different means, including disrupting Internet connectivity, throttling, or imposing service geo-blocking [freedomhouse]
- **digital sovereignty** is increasingly invoked in all kinds of political regimes, no more in authoritarian ones only [deGregorio2022digital]



Why should the user care: not just her country

The **physical and overlay Internet topology** are closer to a *hub-and-spoke* than to a *mesh*

- *a few gateways* can observe (and tamper with) significant fractions of a country's traffic.
- routing (limited by logical and physical connectivity) for most countries implies **strong dependence** on a few other countries for Internet connectivity

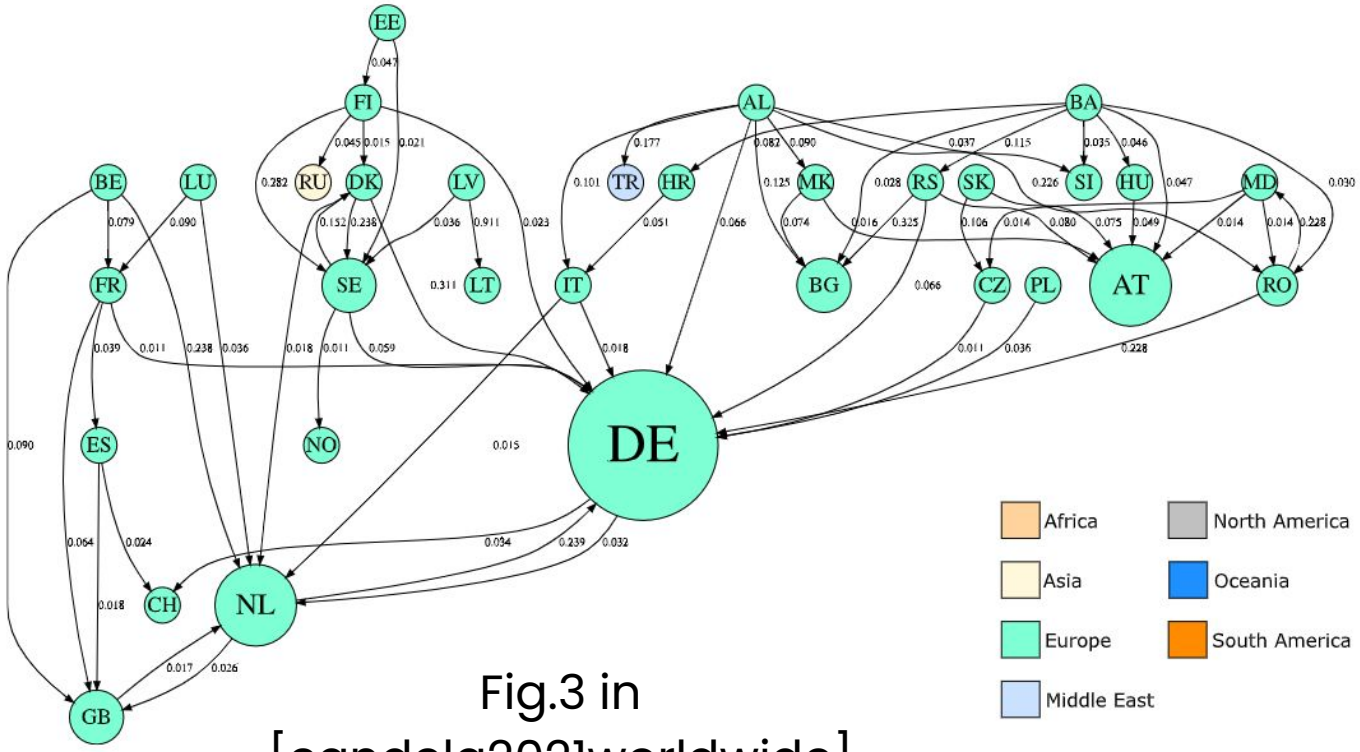


Fig.3 in [candela2021worldwide]

Why should the user care: a possible choice

- **functionally-similar apps** can have a significantly **different impact (and dependence)** on the communication infrastructure
  - the user could **choose less risky apps**, or know if an alternative is worth exploring/adopting, and why (e.g. moving from TikTok to RedNote?)
- **different mobile operator** may have different **connectivity** and different implementation of **compliance**

BUT

with no way of observing the (geopolitic) network footprint, **the user cannot enact informed choices**, nor **participate in the political debate** about information access and regulation

MANANA: design goals and principles

- ease of use (**laymen oriented**)
  - *easy-to-read* characterization of network traffic (**nutrition labels** - style)
  - a summarizing index of **"information freedom risk"** associated with the **country**, weighted according to the fraction of **traffic** of the app reaching or traversing the country
  - **no rooting** of the device is required
- user **privacy** must be guaranteed
- must be **useful** to the user
  - at least, providing **awareness** of the communication infrastructure
- must be useful to the **research community**
  - help collect datasets that are useful for scientific research

MANANA: use

(1) launch MANANA

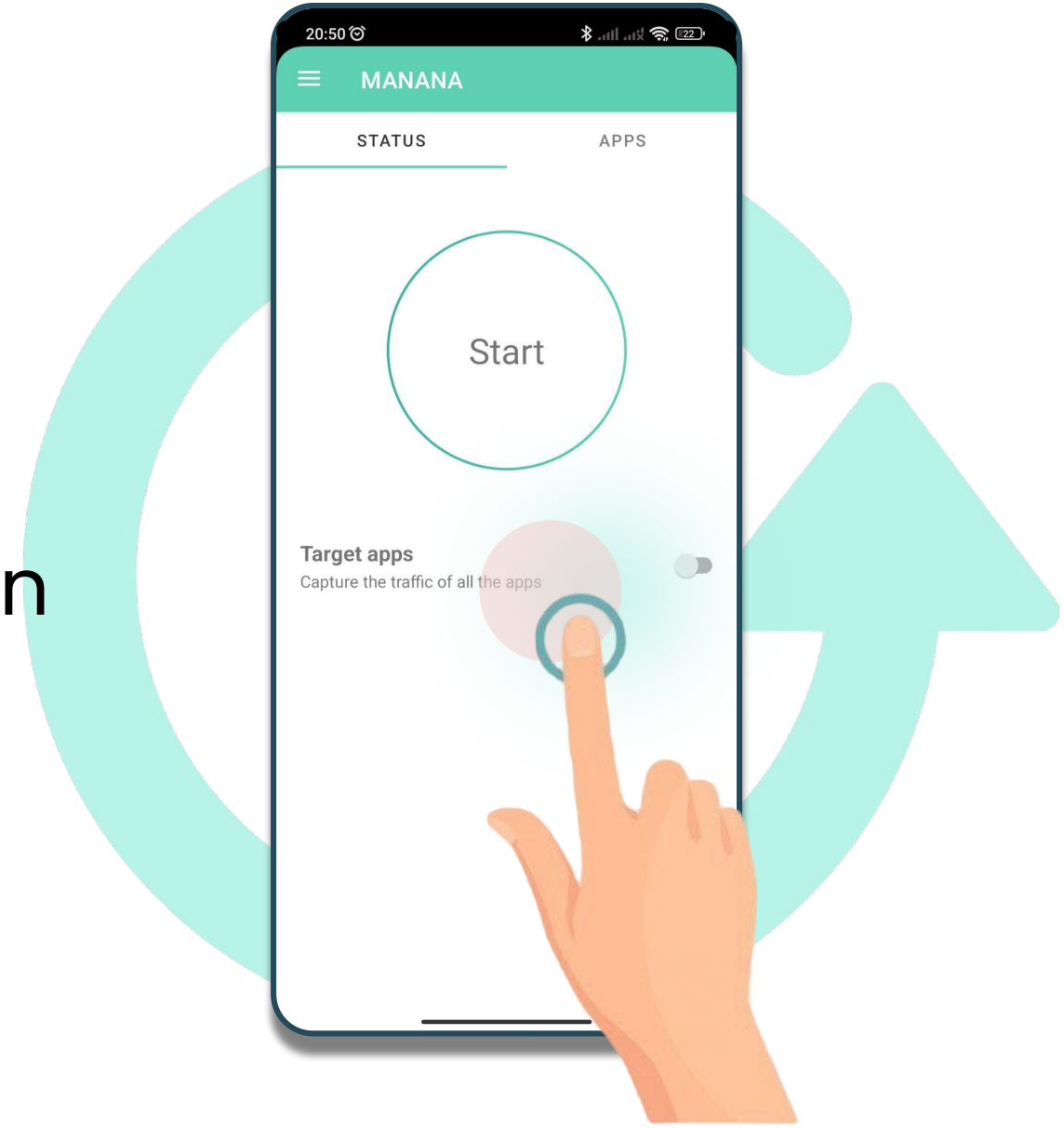
(2) select the **target apps**
   - the selection is kept over restarts

(3) **start** the traffic observation

(4) **inspect** the results

(5) **share** the results with the community

(6) REPEAT!



Overall information safety report

(1) launch MANANA

(2) select the target apps
   - the selection is kept over restarts

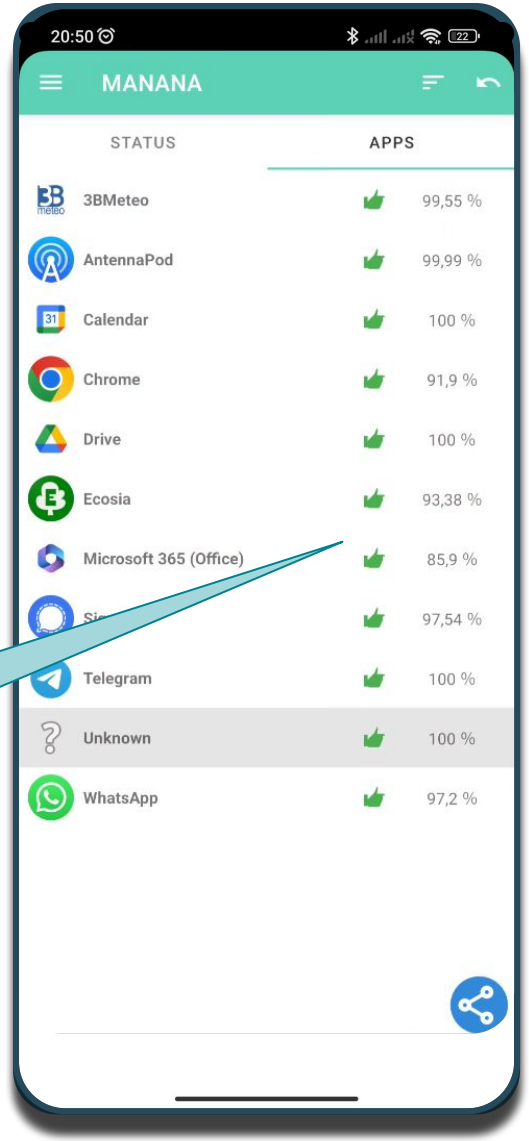
(3) start the traffic observation

(4) **inspect the results**

(5) share the results with the community

(6) REPEAT!

a single summarizing value (**information safety index***) is provided for each app



* more details later

MANANA: information safety labels

(1) launch MANANA

(2) select the target apps
   - the selection is kept over restarts

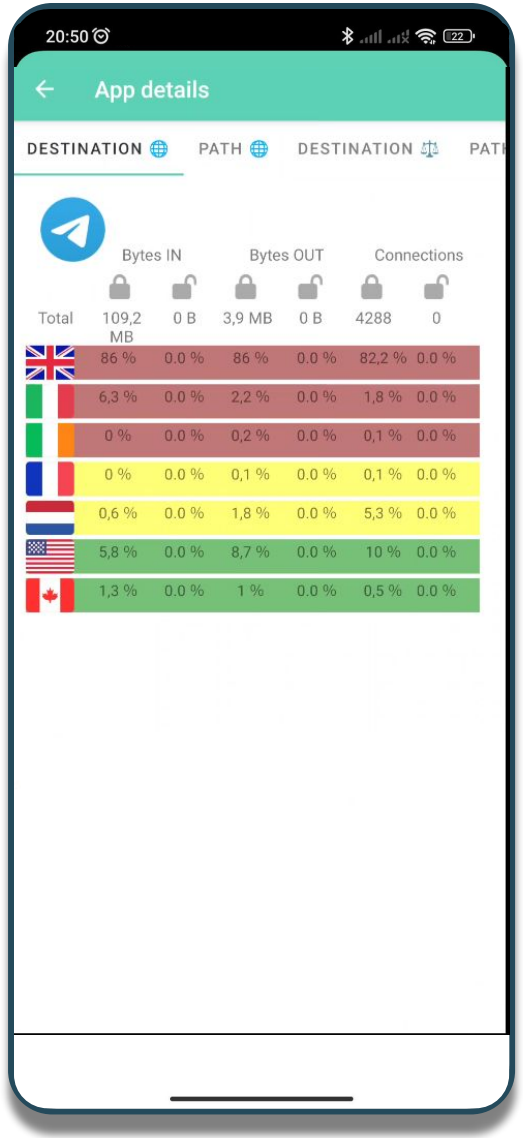
(3) start the traffic observation

(4) **inspect the results**

(5) share the results with the community

(6) REPEAT!

for **each app**, a traffic profile is reported, in the form of **"nutrition labels"**



DESTINATION GEOGRAPHIC COMPOSITION

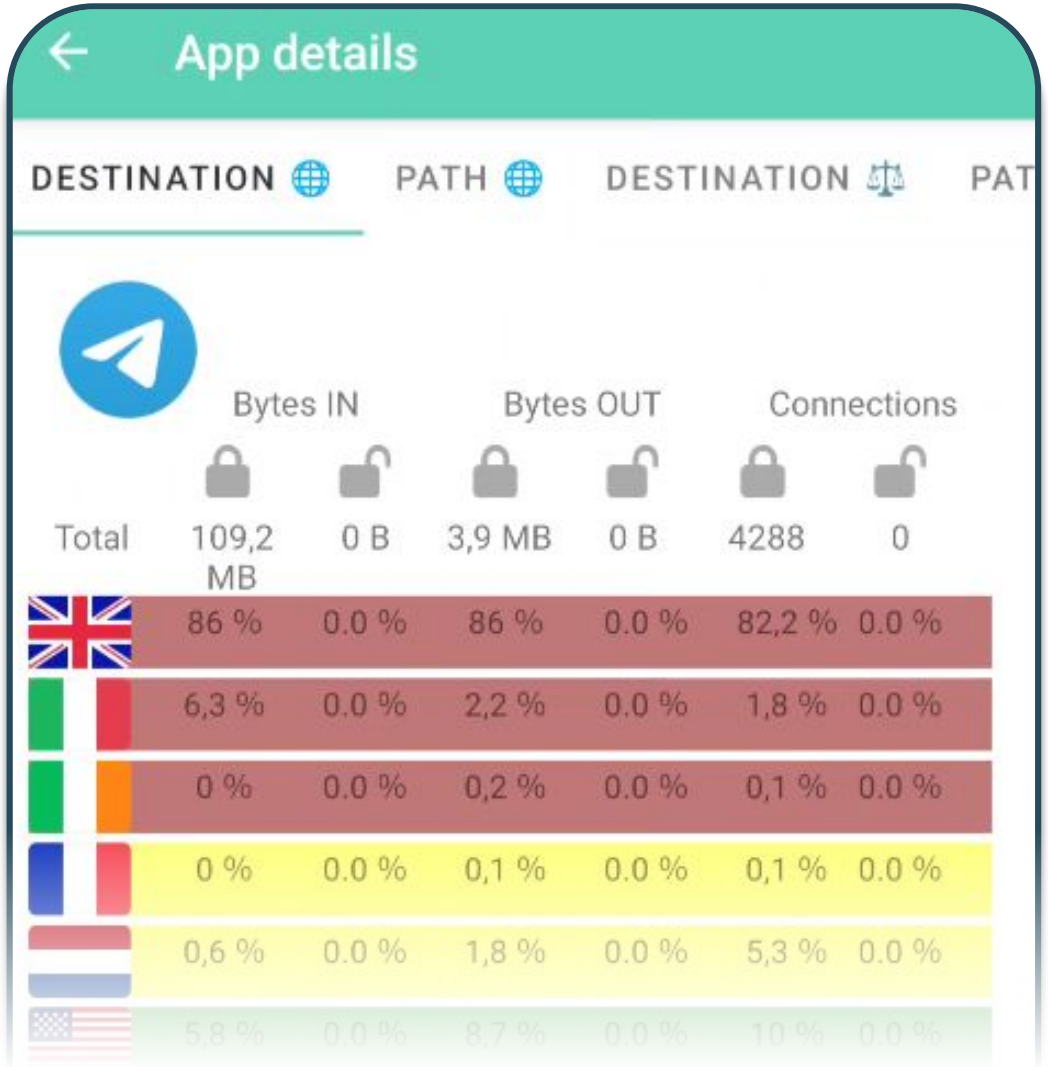
on columns get the breakdown of traffic

Bytes IN/OUT, connections

further divided in
- encrypted
- not encrypted

in total for the app, and by **server country** (**destination IP**, geodb)

this represents physical dependence/exposition



DESTINATION GEOGRAPHIC COMPOSITION

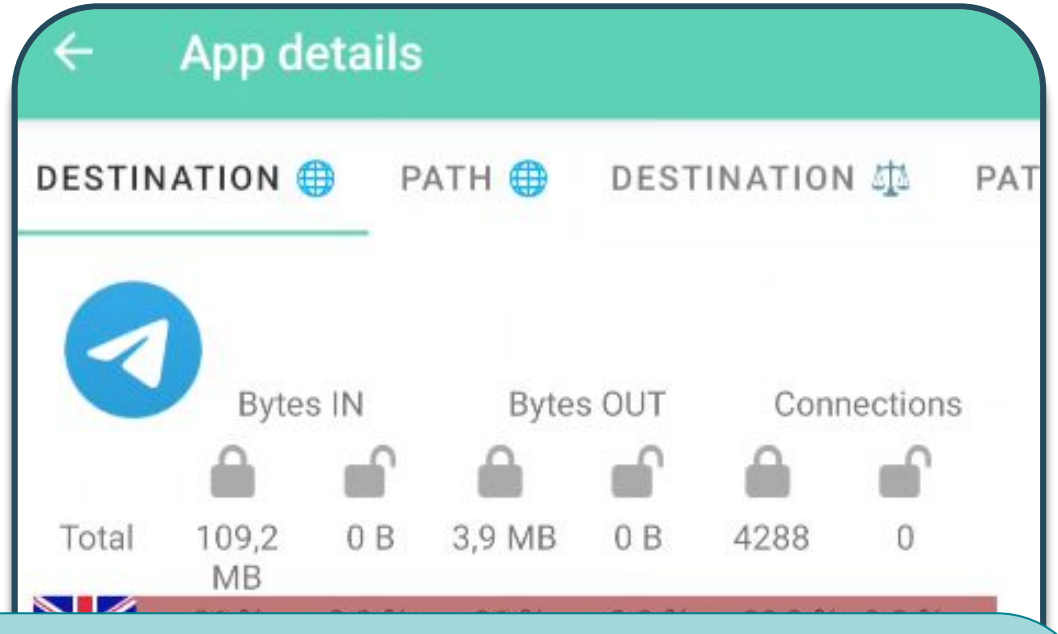
on columns get the breakdown of traffic

Bytes IN/OUT, connections

further divided in
- 🔒 encrypted
- 🔓 not encrypted

in total for the app, and by **server country** (**destination IP**, geodb)

this represents physical dependence/exposition



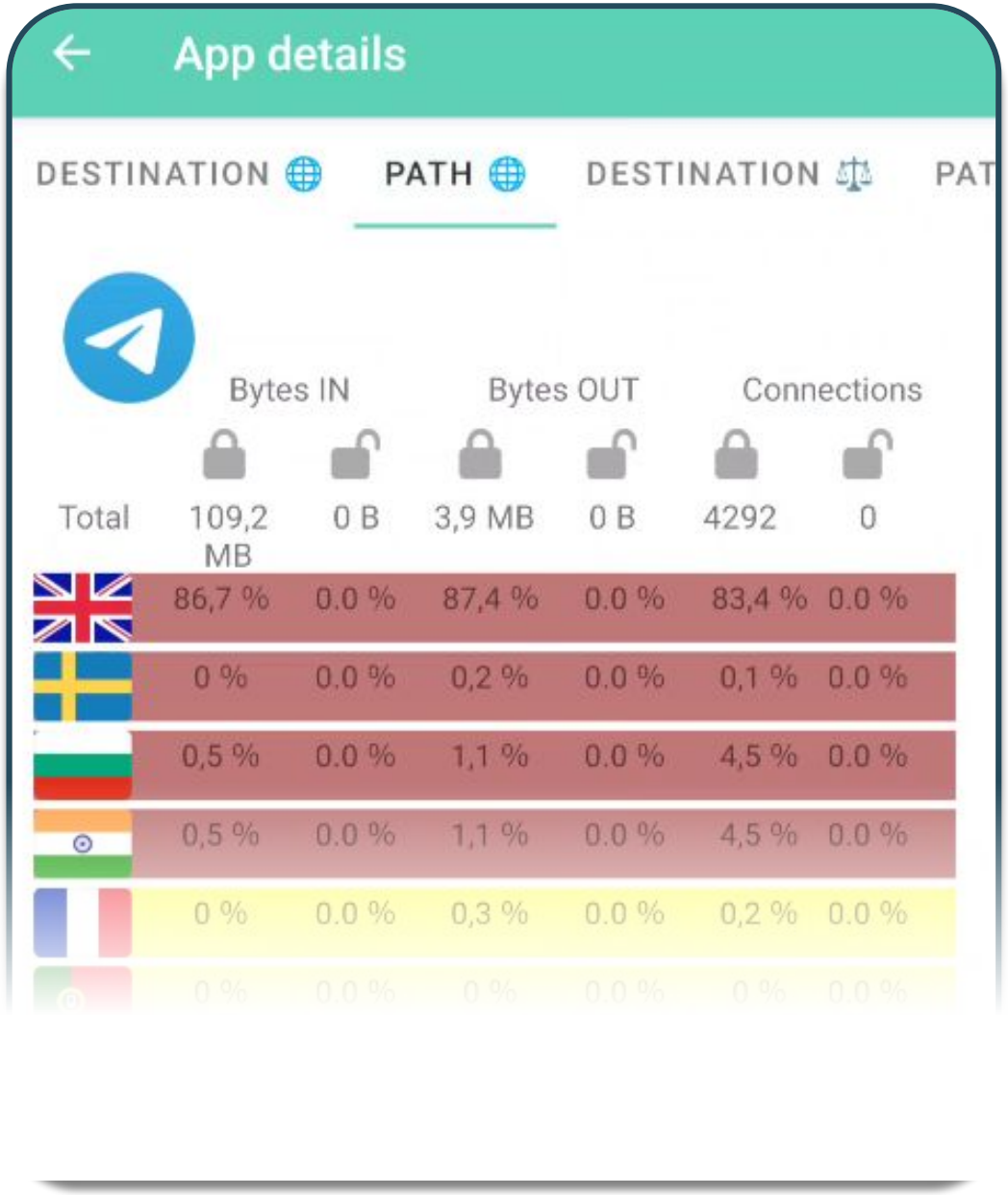
the **[not-]encrypted** classification leverages **`ndpi` heuristics**, in turn derived by reverse-engineering the Great Firewall of China filtering behavior [wu2023how]

PATH
GEOGRAPHIC COMPOSITION

Same kind of information, for **traversed countries** (**intermediate traceroute IPs**, geodb).

In this case the percentage shows **which share passed through a given country**.

Only “passing through” countries are considered: neither the source (100%), nor the destination (shown in previous tab).

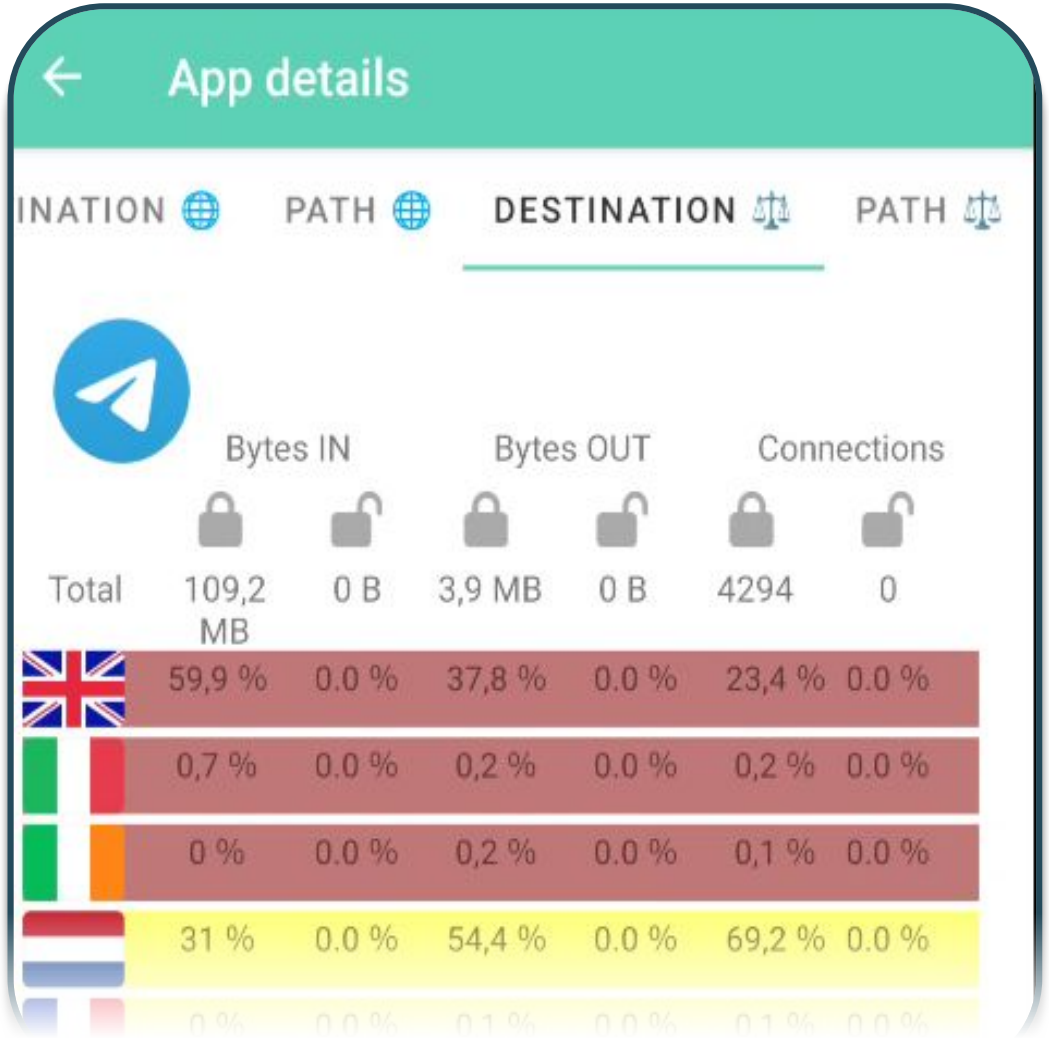


DESTINATION ADMINISTRATIVE COMPOSITION

Same kind of information, for **administrative destinations** (**destination IPs**, WHOIS).

In this case the percentage shows which share is sent to **hosting servers** whose **manager is legally located** in a given country

(exposed to lawful interception, or different degrees of censorship)

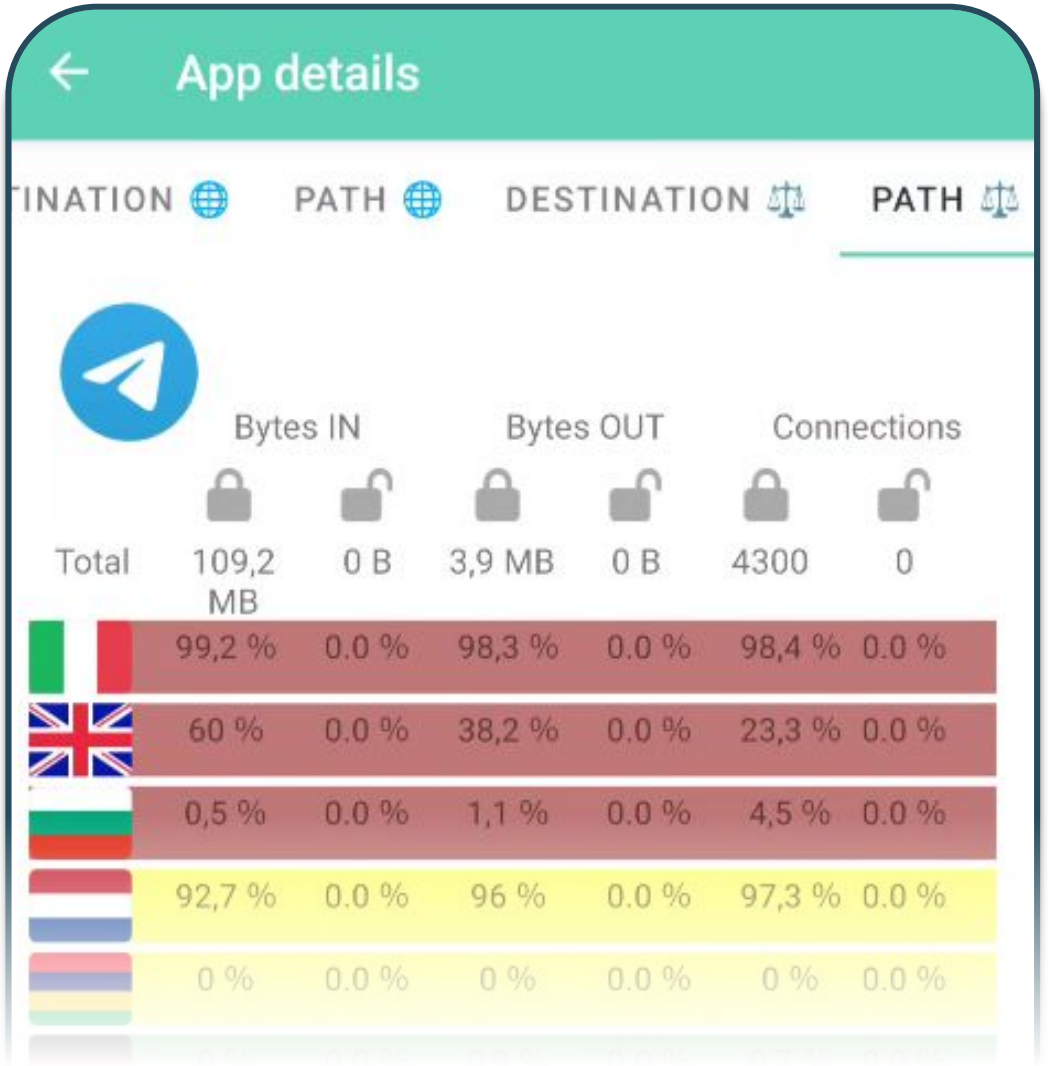


PATH ⚖️ ADMINISTRATIVE COMPOSITION

Same kind of information, for **administrative destinations** (**intermediate traceroute IPs**, WHOIS).

In this case the percentage shows which share passed **through a network device** whose **manager is legally located** in a given country.

(exposed to lawful interception, or different degrees of censorship)



COUNTRY DETAIL AND CLASSIFICATION

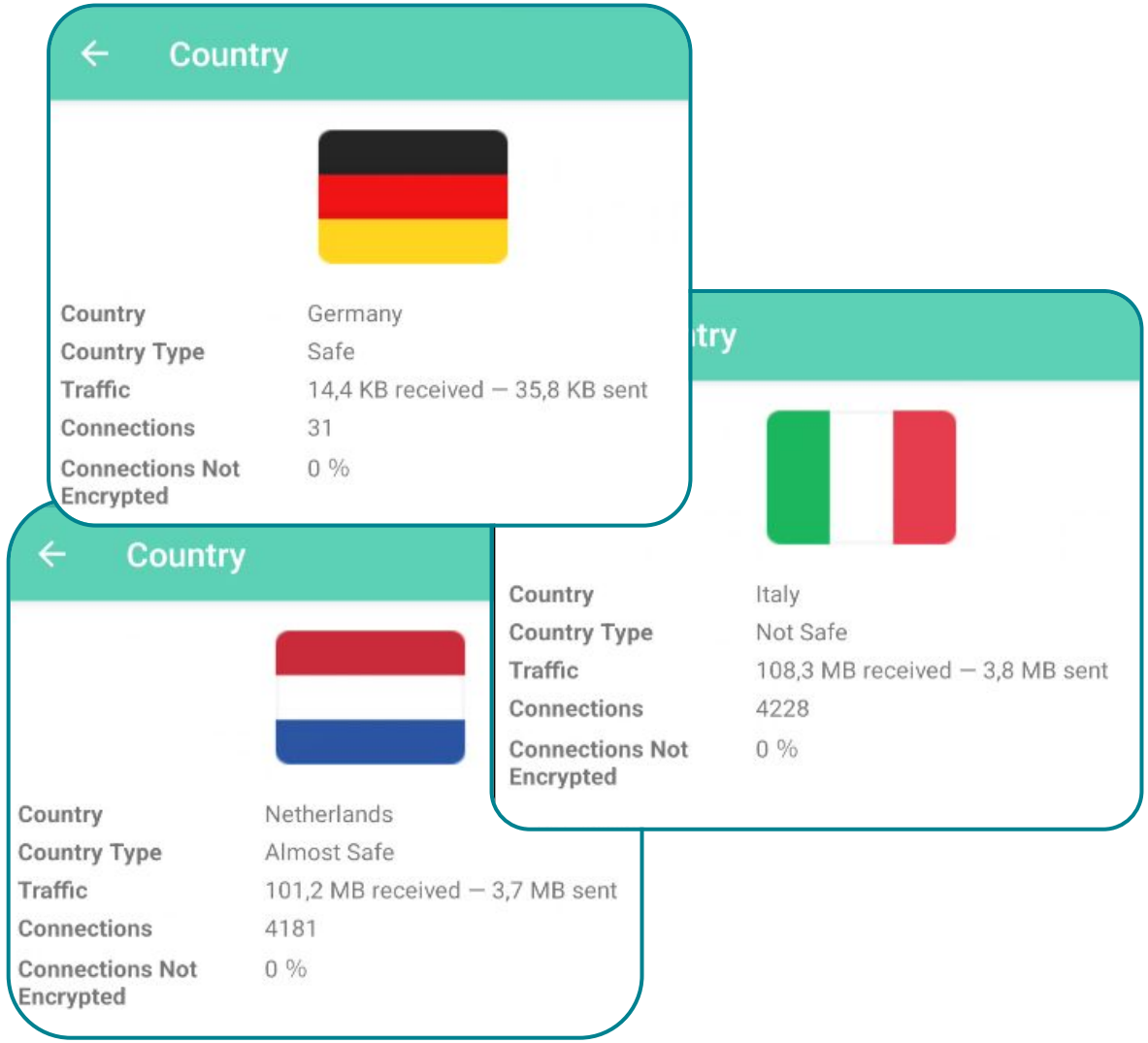
Each country shows sent/received counters, and the **country type**.

This is derived from **V-DEM** project* dataset, specifically values about

- Internet censorship effort
- Governm. Internet filtering in practice
- Governm. Internet shut down capacity
- Governm. Internet shut down in practice
- Privacy protection by law content

the **minimum** (worst) value among the listed fields is mapped as follows**

A.	>=3	*Safe*
B.	in]1,3[	*Almost Safe*
C.	<=1	*Not Safe*



** this is arbitrarily chosen as a *first working hypothesis*, to be refined.

* by V-Dem Institute, Dept. of Political Science, University of Gothenburg, Sweden. https://www.v-dem.net/

Uploaded files: connections report

This file contains data regarding the various observed connections.
Source IP is not logged. Each connection (5-tuple) reports the following values:

- **IPProto**: Protocol field of the IP Packet
- **SrcIP**: Source IP (**private: local VPN**)
- **SrcPort**: Source port number
- **DstIp**: Destination IP
- **DstPort**: Destination Port
- **UID**: App identificator
- **App**: App Name
- **Country**: Destination IP geolocation
- **ASN**: Destination IP related ASN
- **ClassificationValue**: Country information-safety Classification
- **Proto**: Application Level Protocol (from **ndpi** classification library)
- **Status**: Connection Status
- **Info**: domain (from observed DNS queries)
- **BytesSent**, **BytesRcvd**
- **PktsSent**, **PktsRcvd**
- **FirstSeen**: Timestamp* First Seen
- **LastSeen**: Timestamp* Last Seen

* **timestamps are anonymized** with **Random Shifts** (anticipated up to 2h) - see Sec.4.3 RFC6235.
A different offset is drawn for each observation session.

Uploaded files: connections report

This file contains data regarding the various observed connections.
Source IP is not logged. Each connection (5-tuple) reports the following values:

- **IPProto**: Protocol field of the IP Packet
- **SrcIP**: Source IP (**private: local VPN**)
- **SrcPort**: Source port number
- **DstIp**: Destination IP
- **DstPort**: Destination Port
- **UID**: App identificator
- **App**: App Name
- **Country**: Destination IP geolocation
- **ASN**: Destination IP related ASN

- **ClassificationValue**: Country information-safety Classification
- **Proto**: Application Level Protocol (from **ndpi** classification library)
- **Status**: Connection Status
- **Info**: domain (from observed DNS queries)
- **BytesSent**, **BytesRcvd**
- **PktsSent**, **PktsRcvd**
- **FirstSeen**: Timestamp* First Seen
- **LastSeen**: Timestamp* Last Seen

* **timestamps are anonymized** with **Random Shifts** (anticipated up to 2h) - see Sec.4.3 RFC6235.
A different offset is drawn for each observation session.

Manana Server: statistics example - Gmail

Search App

Gmail

Statistics of: Gmail

Stats by Destination Autonomous System Number

ASN Name	Entry Count	Entry [%]	Bytes ↑ [%]	Bytes ↓ [%]	Packets ↑ [%]	Packets ↓ [%]
AS8075 - Microsoft Corporation	1381	58.59%	52.40%	43.88%	52.86%	44.81%
AS396982 - Google LLC	945	40.09%	44.35%	54.84%	45.53%	53.85%
AS15169 - Google LLC	26	1.10%	3.22%	1.27%	1.59%	1.32%
Unknown ASN	5	0.21%	0.02%	0.01%	0.02%	0.02%

Stats by Source Autonomous System Number

ASN Name	Entry Count	Entry [%]	Bytes ↑ [%]	Bytes ↓ [%]	Packets ↑ [%]	Packets ↓ [%]
AS32934 - Facebook, Inc.	1009	42.81%	42.18%	44.03%	41.73%	41.54%
AS6762 - TELECOM ITALIA SPARKLE S.p.A.	798	33.86%	32.47%	29.29%	34.95%	33.98%
AS30722 - Vodafone Italia S.p.A.	15	0.64%	0.71%	0.58%	0.70%	0.72%

Early numbers

Analysis span: **November 30, 2024 to Jun 05, 2025**

- **737** reports (uncompressed 59.3 MB)
- **216** different **mobile applications** analyzed
- **>554k connections** observed
- **17.5 GB** total **traffic** observed, average **23.7 MB** per report

Footprint of the MANANA app:

- **16.2MB** app size
- **2%** additional network traffic
  - (traceroute probes, WHOIS requests)
- **596KB** average compressed report size

Early stage development

the prototype proved feasibility, not ready for common public yet (you can have a run and participate in the experimentation - stay tuned for updates)

- ONGOING DEVELOPMENT
  - extensive **testing**
  - manage **issue** ticketing
  - process **feedback** about usability and privacy requirements
  - **documentation** in app, and on website
  - more advanced **probing optimization** (beyond local caching)

Improvement plan

Once the main functionalities have been extensively tested

we plan to

- publish on **F-Droid**
  (for independent vetting and auto-update of new versions)
- explore **multiple different** criteria for country **information-safety classification** (to maximize user's utility and thus adoption)
- find **anomalies** (traceroute/geoIP/ WHOIS artifacts), **improve accuracy**

also, would be nice-to-have

- provide a **direct comparison** *personal-vs-crowdsourced* statistics
  (to allow the user to compare her results with others / other not-installed apps)
- allow the user to set her **custom *country safety evaluation***
- integrate MANANA with **other mobile analysis tools/projects** [exodus]
- implement **other network measurements** (useful for the both the user and research) like latency [weichao2027towards]

Manana Server running instance

http://143.225.229.154

MANANA latest-beta APK

HAVE A TASTE!

https://www.traffic.comics.unina.it/software/manana/latest

Contacts: **giuseppe.aceto@unina.it**
Follow the project on codeberg:
https://codeberg.org/MANANA_project-UniNA.rss
Project page: https://www.traffic.comics.unina.it/manana/

ACKNOWLEDGEMENTS (1/2)

MANANA is a project by the **Traffic research group**,
Department of Electrical Engineering and Information Technology (**DIETI**)
University of Napoli Federico II.
https://www.traffic.comics.unina.it/manana
(with special thanks to *Angelo Tuorto, B.Sc.* and *Raffaele Carillo, M.Sc.*)

The project started with a **grant** from **GÉANT Innovation Programme 2024**.
https://community.geant.org/innovationprogramme

Source code of the app and the server can be found here:
https://codeberg.org/MANANA_project-UniNA

The **information-safety** classification criteria (ab)use the **dataset** published as **[coppedge2024vdem]** *Coppedge, Michael, et al. 2024. "V-Dem Country-Year Dataset v14", Varieties of Democracy (V-Dem) Project. https://doi.org/10.23696/mcwt-fr58*

The **IP geolocation** dataset is "IP to Country Lite" by DB-IP https://db-ip.com
licensed under a Creative Commons Attribution 4.0 International License

ACKNOWLEDGEMENTS (2/2)

The **mobile app code** is based on **PCAPdroid** (traffic capture and analysis) by Emanuele Faranda https://github.com/emanuele-f/PCAPdroid licensed under GPL3.0 which in turn is composed of many open-source components, including

- nDPI: deep packet inspection library, provides the connections metadata
- mitmproxy: a local proxy for the TLS decryption
- zdtun: minimal TCP/IP stack for the non-root capture

In addition to these, MANANA app includes

the **traceroute code** from the **Mobiperf** project by Google https://github.com/Mobiperf licensed under Apache License 2.0

The MANANA collection and analysis server include

the **ftp server**: **vsftpd** https://security.appspot.com/vsftpd.html (GPL lincense)

the **statistics web server**: implemented in the **Django** framework https://www.djangoproject.com (BSD license)

REFERENCES (1/2)

[bashar2024understanding] Bhaskar, Abhishek, and Paul Pearce. "Understanding Routing-Induced Censorship Changes Globally." Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security. 2024. https://dl.acm.org/doi/pdf/10.1145/3658644.3670336

[candela2021worldwide] Candela, Massimo, et al. "A worldwide study on the geographic locality of Internet routes." Computer Networks 201 (2021): 108555. https://doi.org/10.1016/j.comnet.2021.108555

[deGregorio2022digital] De Gregorio, Giovanni, and Roxana Radu. "Digital constitutionalism in the new era of Internet governance." International Journal of Law and Information Technology 30.1 (2022): 68-87. https://doi.org/10.1093/ijlit/eaac004

[exodus] The εxodus project - privacy audit for Android apps https://reports.exodus-privacy.eu.org/en/

[freedomhouse] Freedom House - *Freedom of the Net 2024: The Struggle for Trust Online* https://freedomhouse.org/report/freedom-net/2024/struggle-trust-online

[li2017toward] Li, Weichao, et al. "Toward accurate network delay measurement on android phones." *IEEE Transactions on Mobile Computing* 17.3 (2017): 717-732. https://doi.org/10.1109/TMC.2017.2737990

REFERENCES (2/2)

[liu2023inferring] Liu, Yan, et al. "Inferring router ownership based on the classification of intra-and inter-domain links." Scientific Reports 13.1 (2023): 5090.

[marder2018pushing] Marder, Alexander, et al. "Pushing the boundaries with bdrmapit: Mapping router ownership at internet scale." Proceedings of the Internet Measurement Conference 2018. 2018. https://dl.acm.org/doi/pdf/10.1145/3278532.3278538

[sandvine2024gipr]Sandvine's 2024 Global Internet Phenomena Report - https://www.sandvine.com/global-internet-phenomena-report-2024

[wu2023how] Wu, Mingshi, et al. "How the Great Firewall of China detects and blocks fully encrypted traffic." 32nd USENIX Security Symposium (USENIX Security 23). 2023. https://www.usenix.org/conference/usenixsecurity23/presentation/wu-mingshi

[wu2024enhancing] Wu, Weili, et al. "Poster: Enhancing Internet Disruption Investigation via Path Monitoring." *Proceedings of the 2024 ACM on Internet Measurement Conference*. 2024. https://dl.acm.org/doi/pdf/10.1145/3646547.3689675

Backup slides

Path-tracing limitations in MANANA

- reverse-path uncertainties
  - *Internet routing may be **asymmetric***
    - *traceroute inherent limitation, we have to live with this*
- path stability assumptions
  - *the path towards each destination is sampled **once per observation session***
  - *no big issue in our application scenario: no impact on AS- and country-paths inferred*
    - *Internet routes are expected to change at a lower frequency*
    - *ECMP is expected to be employed* within an AS
- ICMP vs TCP/UDP data probes
  - crafting probes of the same type of data packet would ensure to follow the very same path
  - in MANANA app, we are limited to **ICMP** to avoid rooting of the smartphone (not general audience)
- third-party IP addresses
  - the RFC1812 states that the source address of an ICMP error packet should correspond to the outgoing interface of the ICMP reply, rather than the interface on which the packet triggering the error was received
  - this behavior can cause a traceroute IP path to include addresses associated to interfaces not included in the path actually traversed
  - this may cause the inference of **inaccurate AS paths**
    - path-data cleaning (e.g., checking for AS paths shorter that 3 hops during post-processing?) can mitigate such issue
- AS-border identification
  - may impact length of the portion of the path within an AS, and thus proportions and stats
  - not a major issue in our case
  - https://dl.acm.org/doi/abs/10.1145/3278532.3278538
- IP Geofeeds
  - https://hal.science/hal-04663776/document
  - RFC 8805 (2021), draft 2013. info included in WHOIS data (inetnum objects)

report .csv example

… plus first/last packet timestamps

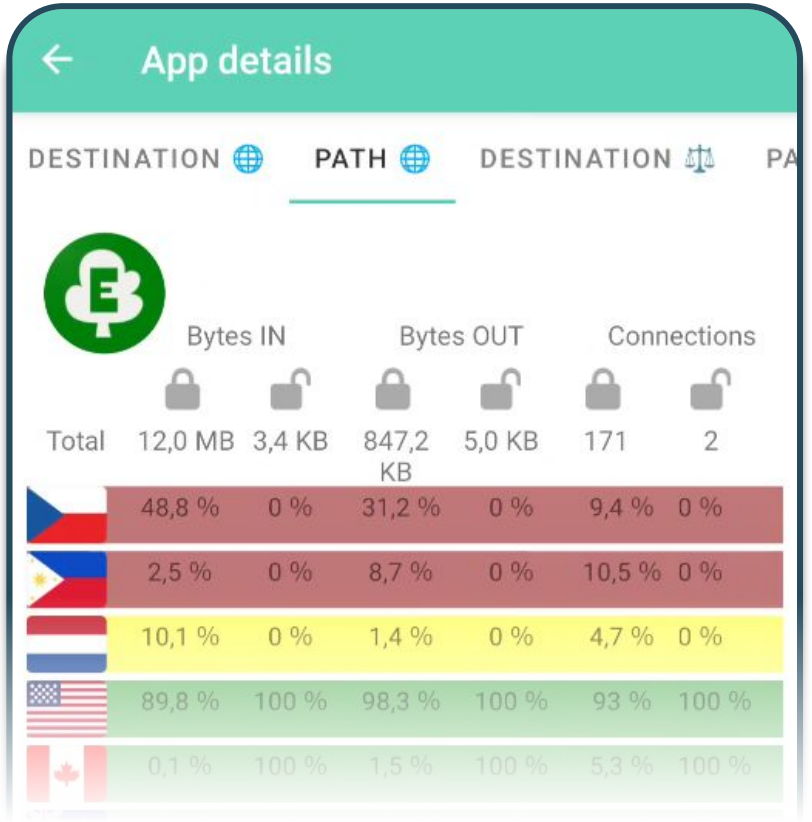
IPProto	SrcIP	SrcPort	DstIp	DstPort	UID	App	Country	ASN	fication	Proto	Status	Info	BytesSent	BytesRcvd	PktsSent	PktsRcvd
17	10.215.173.1	27736	10.215.173.2	53	0	Root	No Info	Unknown ASN	-1	DNS	Closed	mdm2.asus.com	59	59	1	1
17	10.215.173.1	16359	10.215.173.2	53	0	Root	No Info	Unknown ASN	-1	DNS	Closed	mdm2.asus.com	59	59	1	1
17	10.215.173.1	20869	10.215.173.2	53	0	Root	No Info	Unknown ASN	-1	DNS	Closed	portal.fb.com	59	118	1	1
6	10.215.173.1	60834	157.240.231.15	80	10071	Facebook	Italy	AS32934 - Facebook, Inc.	1	HTTP	Active	portal.fb.com	357	284	4	3
6	10.215.173.1	60834	157.240.231.15	80	10071	Facebook	Italy	AS32934 - Facebook, Inc.	1	HTTP	Active	portal.fb.com	0	0	4	3
17	10.215.173.1	20658	10.215.173.2	53	0	Root	No Info	Unknown ASN	-1	DNS	Closed	whois.lacnic.net	62	78	1	1
17	10.215.173.1	32361	10.215.173.2	53	0	Root	No Info	Unknown ASN	-1	DNS	Closed	clients3.google.com	65	115	1	1
17	10.215.173.1	14543	10.215.173.2	53	0	Root	No Info	Unknown ASN	-1	DNS	Closed	static.whatsapp.net	65	118	1	1
6	10.215.173.1	35442	157.240.231.60	443	10140	WhatsApp	Italy	AS32934 - Facebook, Inc.	1	HTTPS	Active	static.whatsapp.net	912	3698	9	8
6	10.215.173.1	35442	157.240.231.60	443	10140	WhatsApp	Italy	AS32934 - Facebook, Inc.	1	HTTPS	Active	static.whatsapp.net	0	0	9	8
6	10.215.173.1	59725	216.58.204.142	80	10140	WhatsApp	d Kingdom	AS15169 - Google LLC	1	HTTP	Active	clients3.google.com	359	255	4	3
6	10.215.173.1	59725	216.58.204.142	80	10140	WhatsApp	d Kingdom	AS15169 - Google LLC	1	HTTP	Active	clients3.google.com	0	0	4	3
17	10.215.173.1	8624	10.215.173.2	53	0	Root	No Info	Unknown ASN	-1	DNS	Closed	asia.pool.ntp.org	63	127	1	1
17	10.215.173.1	53746	162.159.200.1	123	10140	WhatsApp	Canada	AS13335 - Cloudflare, Inc.	3	NTP	Active	asia.pool.ntp.org	76	76	1	1
17	10.215.173.1	53746	162.159.200.1	123	10140	WhatsApp	Canada	AS13335 - Cloudflare, Inc.	3	NTP	Active	asia.pool.ntp.org	0	0	1	1
17	10.215.173.1	19303	10.215.173.2	53	0	Root	No Info	Unknown ASN	-1	DNS	Closed	whois.ripe.net	60	76	1	1
17	10.215.173.1	5242	10.215.173.2	53	0	Root	No Info	Unknown ASN	-1	DNS	Closed	whois.arin.net	60	108	1	1
17	10.215.173.1	24242	10.215.173.2	53	0	Root	No Info	Unknown ASN	-1	DNS	Closed	whois.apnic.net	61	77	1	1
17	10.215.173.1	26689	10.215.173.2	53	0	Root	No Info	Unknown ASN	-1	DNS	Closed	whois.nic.or.kr	61	77	1	1
17	10.215.173.1	10349	10.215.173.2	53	0	Root	No Info	Unknown ASN	-1	DNS	Closed	mtalk.google.com	62	117	1	1
6	10.215.173.1	47527	108.177.96.188	5228	10029	ıp Transport	ited States	AS15169 - Google LLC	3	TLS	Active	mtalk.google.com	1286	1184	8	8
6	10.215.173.1	47527	108.177.96.188	5228	10029	ıp Transport	ited States	AS15169 - Google LLC	3	TLS	Active	mtalk.google.com	0	0	8	8
17	10.215.173.1	19143	10.215.173.2	53	0	Root	No Info	Unknown ASN	-1	DNS	Active	android.apis.google.com	69	0	1	0
17	10.215.173.1	19143	10.215.173.2	53	0	Root	No Info	Unknown ASN	-1	DNS	Active	android.apis.google.com	0	119	1	0
6	10.215.173.1	54438	142.251.209.14	443	10029	ıp Transport	Italy	AS15169 - Google LLC	1	HTTPS	Active	android.apis.google.com	1492	1683	7	6
6	10.215.173.1	54438	142.251.209.14	443	10029	ıp Transport	Italy	AS15169 - Google LLC	1	HTTPS	Active	android.apis.google.com	0	0	7	6

Uploaded files: traceroute report .json (1/2)

This file reports on the traceroute result (for every connection **DstIP**)…

Every app is characterised by (1):

- **AppName**
- a list of **IPs**, associated to the app, each with following data
  - the **result** of the Traceroute towards that IP
  - **timeStamp** at the end of the Traceroute
  - **orderedListCountry,** the countries associated to the IPs found from the Traceroute and geolocated
  - **sentBytesEnc**, encrypted, **sentBytesNotEnc**, unencrypted
  - **rcvdBytesEnc**, **rcvdBytesNotEnc**
  - **numConnsEnc**, **numConnsNotEnc.**



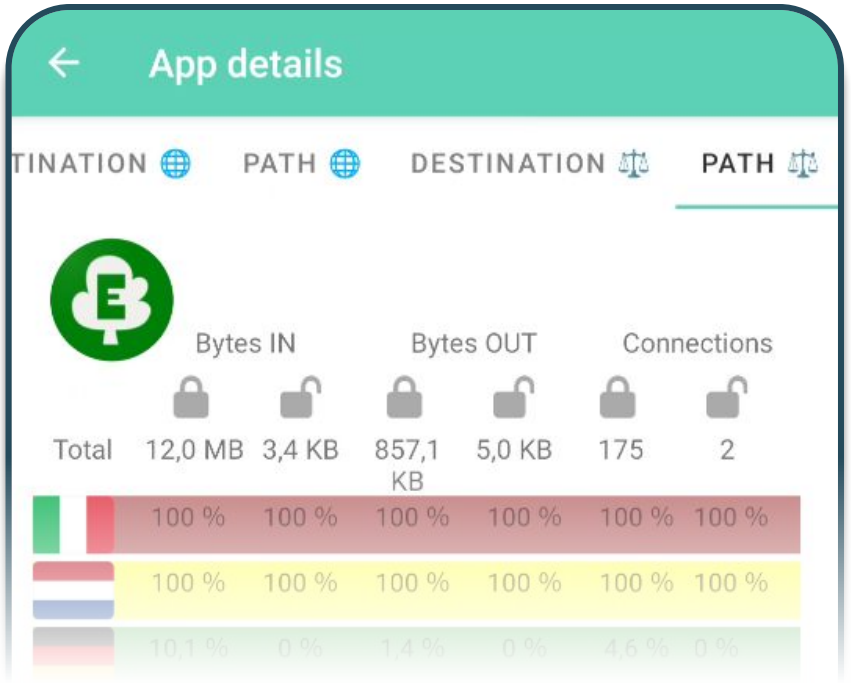
Uploaded files: traceroute report .json (2/2)

This file reports also on Whois query
(for every connection **DstIP and IPs of the trace**).

Every app is characterised also by (2):

- **WhoisTraceCountries,** same format as traceCountries but the **orderedListCountry** from whois queries

- **WhoisDestinationCoutries,** a list of countries, each with:
  - **IpList:** the IPs associated to that country and the Timestamp associated to the Whois query
  - **classificationValue** associated to the country
  - **rcvdBytesEnc**, **rcvdBytesNotEnc**
  - **sentBytesEnc**, **sentBytesNotEnc**
  - **numConnsEnc**, **numConnsNotEnc**



Path analysis via Traceroute

- Traceroute implementation by **MobiPerf**
  - Current traceroute implementation sends out **3 ICMP probes** per TTL
  - One ping every 0.2s is the lower bound before some platforms require root to run ping.
  - reduced timeout w.r.t. MobiPerf default

Manana Server

Collects the reports provided by the users

- Each report is received by an **ftps server** (running in its own virtual machine) and then moved to an archive outside the VM
- Periodically (30 min.) the **reports are aggregated** and newly updated statistics are generated using all the reports
- The newly generated stats are saved to a relational **database**
- The updated statistics are published by the **web server**

Manana Server: statistics

- For **each app** the computed statistics include:
  - For **each destination AS** and **destination country**
    - The total count of the **entries** in all the reports and the relative overall **share**
    - The share of **data** sent/received
    - The share of **packets** sent/received
  - For each **destination country**, a **safety rating** is shown (with same criteria adopted for the mobile app, based on V-Dem dataset)
  - Similarly, the entry count, share and safety rating of each **country traversed** according to the traceroute reports

traceroute: report.json example


```
[
  {
    "AppName": "Root",
    "WhoisDestinationCoutries": [
      {
        "IpList": [
          {
            "8.8.8.8":
"2024-10-29T16:33:18.645+01:00"
          }
        ],
        "classificationValue": 3,
        "name": "US",
        "numConnsEnc": 0,
        "numConnsNotEnc": 2,
        "rcvdBytesEnc": 0,
        "rcvdBytesNotEnc": 196,
        "sentBytesEnc": 0,
        "sentBytesNotEnc": 135
      }
    ],
```

```
"WhoisTraceCountries": {
      "8.8.8.8": {
        "numConnsEnc": 0,
        "numConnsNotEnc": 2,
        "orderedListCountry": [
          "NL",
          "US",
          "US"
        ],
        "rcvdBytesEnc": 0,
        "rcvdBytesNotEnc": 196,
        "result": [],
        "sentBytesEnc": 0,
        "sentBytesNotEnc": 135,
        "timeStamp":
     "2024-10-29T16:38:20.207+01:00"
      }
    },
```

```
"traceCountries": {
      "8.8.8.8": {
        "numConnsEnc": 0,
        "numConnsNotEnc": 2,
        "orderedListCountry": [
          "IT",
          "US",
          "US"
        ],
        "rcvdBytesEnc": 0,
        "rcvdBytesNotEnc": 196,
        "result": [
          {
            "hosts": [
              "192.168.0.1:"
            ],
            "rtt": 13.666666666666666
          },
        "sentBytesEnc": 0,
        "sentBytesNotEnc": 135,
        "timeStamp":
"2024-10-29T16:33:36.893+01:00"
```

Updating Data

The data updates from a new connection are:

- **AppStats,** this class is associated to an app, its values are updated depending on the value of the UID in the connection. If the data are unencrypted it will updated its **sentBytesNotEnc**, **rcvdBytesNotEnc numConnsNotEnc** otherwise its **sentBytesEnc rcvdBytesEnc**, **numConnsEnc.**
- **Destination Countries,** a list of countries in AppStats made by DstIP geolocation of every connection generated by the app. It updates data for every country in the same way.
- **traceCountries,** a list of IPs and its relative Traceroute data in AppStats. The data are updated before the Traceroute execution in the same way mentioned above.
- **countriesAD** and **traceCountriesAD** (respectively **WhoisDestinationCoutries** and **WhoisTraceCountries** from the previous slide), also present in Appstats and update the data in the same way.

Manana Server: statistics example - Telegram

Statistics of: Telegram

Stats by Destination Autonomous System Number

ASN Name	Entry Count	Entry [%]	Bytes ↑ [%]	Bytes ↓ [%]	Packets ↑ [%]	Packets ↓ [%]
AS62041 - Telegram Messenger Inc	115	95.04%	89.21%	98.31%	93.04%	92.65%
AS62014 - Telegram Messenger Inc	6	4.96%	10.79%	1.69%	6.96%	7.35%

Stats by Source Autonomous System Number

ASN Name	Entry Count	Entry [%]	Bytes ↑ [%]	Bytes ↓ [%]	Packets ↑ [%]	Packets ↓ [%]
AS32934 - Facebook, Inc.	43	35.54%	40.78%	90.64%	42.97%	47.67%
Unknown ASN	43	35.54%	22.80%	3.02%	24.42%	20.97%
AS30722 - Vodafone Italia S.p.A.	2	1.65%	1.53%	0.53%	1.85%	1.79%
AS6762 - TELECOM ITALIA SPARKLE S.p.A.	33	27.27%	34.89%	5.82%	30.76%	29.57%

Stats by Destination Country

Country Name	Entry Count	Entry [%]	Bytes ↑ [%]	Bytes ↓ [%]	Packets ↑ [%]	Packets ↓ [%]	Safety
United Kingdom	115	95.04%	89.21%	98.31%	93.04%	92.65%	DANGEROUS
Netherlands	6	4.96%	10.79%	1.69%	6.96%	7.35%	NON-SECURE

Stats by Traversed Countries

Country Name	Entry Count	Percentage	Safety
Italy	12	28.57%	DANGEROUS
United Kingdom	22	52.38%	DANGEROUS
United States	6	14.29%	SECURE
Netherlands	2	4.76%	NON-SECURE