Appendix

Automated report generated for Paypal mobile application

UNIVERSITE CATHOLIQUE DE LOUVAIN

ECOLE POLYTECHNIQUE DE LOUVAIN

Leak sources analysis

Automated report

Supervisor: Dr. Ramin SADRE

by Mattieu DETAILLE
& Mohammad Muntasib Ali SYED

1. Lack of encryption

1.1. Unencrypted word(s) extracted

Here are the word(s) we found without any encryption security:

- **mattieu**

We found the word(s) **mattieu** in the following packet(s):

- 24-05-2016 10:32:26.928204; 192.168.42.10: 68 --> 192.168.42.1: 67

...[redacted]c[redacted]sc5[redacted]7[redacted]y[redacted]
[redacted]w[redacted]9[redacted]=[redacted](z[redacted]"[redacted]3[redacted]v[redacted] [redacted]iphonede**mattieu**[redacted]...

1.2. Unencrypted file(s) extracted

No unencrypted files were extracted from your network traffic

2. Weak encryption

The security protocol SSL/TLS was used to encrypt part of your traffic, which is already a good start! 56% of your IP network traffic was encrypted using the SSL/TLS security protocol.

There are some problems regarding some hash function(s) used in your network traffic. The weak hash function(s) **MD5** was/were used!

Here are the details about the problematic packets secured using this/these weak hash function(s):

- Timestamp: 24-05-2016 10:07:25.783150; 17.110.234.27:443 --> 192.168.42.10:50083

  In this packet, the domain **mt-ingestion-service-mr22.itunes-apple.com.akadns.net**

  contacted your smart device.

  Weak hash function used: **MD5**

  Cryptographic algorithms used for encrypting this packet: RSA_WITH_RC4_128_MD5

- Timestamp: 24-05-2016 10:11:55.299035; 63.215.202.68:443 --> 192.168.42.10:50125

  In this packet, the domain **altfarm.mediaplex.com** contacted your smart device.

  Weak hash function used: **MD5**

  Cryptographic algorithms used for encrypting this packet: RSA_WITH_RC4_128_MD5

There are some problems regarding stream cipher algotihm(s) used in your network traffic. The weak stream cipher algorithm(s) **RC4** was/were used!

Here are the details about the problematic packets secured using this/these weak stream cipher algorithm(s):

- Timestamp: 24-05-2016 10:35:37.361653; 64.4.245.25:443 --> 192.168.42.10:50152

In this packet, the domain **b.stats.paypal.com** contacted your smart device.
Weak stream cipher algorithm used: **RC4**
Cryptographic algorithms used for encrypting this packet:
ECDHE_RSA_WITH_RC4_128_SHA

- Timestamp: 24-05-2016 10:35:38.112890; 64.4.245.25:443 --> 192.168.42.10:50153
  In this packet, the domain **b.stats.paypal.com** contacted your smart device.
  Weak stream cipher algorithm used: **RC4**
  Cryptographic algorithms used for encrypting this packet:
  ECDHE_RSA_WITH_RC4_128_SHA

- Timestamp: 24-05-2016 10:07:25.783150; 17.110.234.27:443 --> 192.168.42.10:50083
  In this packet, the domain **mt-ingestion-service-mr22.itunes-apple.com.akadns.net** contacted your smart device.
  Weak stream cipher algorithm used: **RC4**
  Cryptographic algorithms used for encrypting this packet: RSA_WITH_RC4_128_MD5

- Timestamp: 24-05-2016 10:07:29.546743; 64.4.245.25:443 --> 192.168.42.10:50090
  In this packet, the domain **b.stats.paypal.com** contacted your smart device.
  Weak stream cipher algorithm used: **RC4**
  Cryptographic algorithms used for encrypting this packet:
  ECDHE_RSA_WITH_RC4_128_SHA

- Timestamp: 24-05-2016 10:07:31.064256; 64.4.245.25:443 --> 192.168.42.10:50098
  In this packet, the domain **b.stats.paypal.com** contacted your smart device.
  Weak stream cipher algorithm used: **RC4**
  Cryptographic algorithms used for encrypting this packet:
  ECDHE_RSA_WITH_RC4_128_SHA

- Timestamp: 24-05-2016 10:08:15.732086; 64.4.245.25:443 --> 192.168.42.10:50100
  In this packet, the domain **b.stats.paypal.com** contacted your smart device.
  Weak stream cipher algorithm used: **RC4**
  Cryptographic algorithms used for encrypting this packet:
  ECDHE_RSA_WITH_RC4_128_SHA

- Timestamp: 24-05-2016 10:08:16.700862; 64.4.245.25:443 --> 192.168.42.10:50101

  In this packet, the domain **b.stats.paypal.com** contacted your smart device.

  Weak stream cipher algorithm used: **RC4**

  Cryptographic algorithms used for encrypting this packet:

  ECDHE_RSA_WITH_RC4_128_SHA

- Timestamp: 24-05-2016 10:09:05.452517; 64.4.245.25:443 --> 192.168.42.10:50104

  In this packet, the domain **b.stats.paypal.com** contacted your smart device.

  Weak stream cipher algorithm used: **RC4**

  Cryptographic algorithms used for encrypting this packet:

  ECDHE_RSA_WITH_RC4_128_SHA

- Timestamp: 24-05-2016 10:09:06.236268; 64.4.245.25:443 --> 192.168.42.10:50105

  In this packet, the domain **b.stats.paypal.com** contacted your smart device.

  Weak stream cipher algorithm used: **RC4**

  Cryptographic algorithms used for encrypting this packet:

  ECDHE_RSA_WITH_RC4_128_SHA

- Timestamp: 24-05-2016 10:11:55.299035; 63.215.202.68:443 --> 192.168.42.10:50125

  In this packet, the domain **altfarm.mediaplex.com** contacted your smart device.

  Weak stream cipher algorithm used: **RC4**

  Cryptographic algorithms used for encrypting this packet: RSA_WITH_RC4_128_MD5

Here are the cryptographic algorithms used for securing a part of your network traffic: AES, SHA, RC4, GCM, RSA, SHA384, ECDHE, SHA256, CBC, MD5.

3. Covert channels

3.1. Adblock

Here are all the domains blocked by the adblock module : **t.paypal.com**.

In one of the packets exchange, the following domain(s) was(were) blocked : **t.paypal.com**.
Here are some known alternative name(s) of this(these) domain(s) : **e3694.a.akamaiedge.net, t.paypal.com.edgekey.net**.
Here are the known ip adresses of this(these) domain(s) : **88.221.185.39**

3.2. DNSBL

Here are all the domains of the ips blocked by the DNSBL module :
ec2-23-23-148-99.compute-1.amazonaws.com, e.crashlytics.com, events-endpoint-455714294.us-east-1.elb.amazonaws.com, ec2-50-17-190-20.compute-1.amazonaws.com, events-endpoint-c-394794954.us-east-1.elb.amazonaws.com.

In one of the packets exchange, DNSBL's blocked the following ip(s) :

- **23.21.246.69** by the blacklist : **zen.spamhaus.org**

Here are some known domain name(s) of this(these) ip(s) :
ec2-23-23-148-99.compute-1.amazonaws.com, e.crashlytics.com, events-endpoint-455714294.us-east-1.elb.amazonaws.com.

In one of the packets exchange, DNSBL's blocked the following ip(s) :

- **50.16.238.111** by the blacklist : **zen.spamhaus.org**

Here are some known domain name(s) of this(these) ip(s) :
ec2-50-17-190-20.compute-1.amazonaws.com, events-endpoint-c-394794954.us-east-1.elb.amazonaws.com, e.crashlytics.com.

3.3. SafeBrowsing

The SafeBrowsing module didn't find any match.

3.4. SafeLookup

The SafeLookup module didn't find any match.

3.5. Potential backdoors

The open ports of the smart device were not analysed.

The following content only mention all the ports accessed by the services tested on the smart device besides ports 80(http) and 443(https). It doesn't explicitely prove the presence of backdoors, but by examining the domains and making some correlations with previous sections (like blocked domains), it may be possible to identify some suspicious access. These access may have been used to extract or inject data, which may lead to leaks.

During this session, the following ports(besides 80(http) and 443(https)) were used :

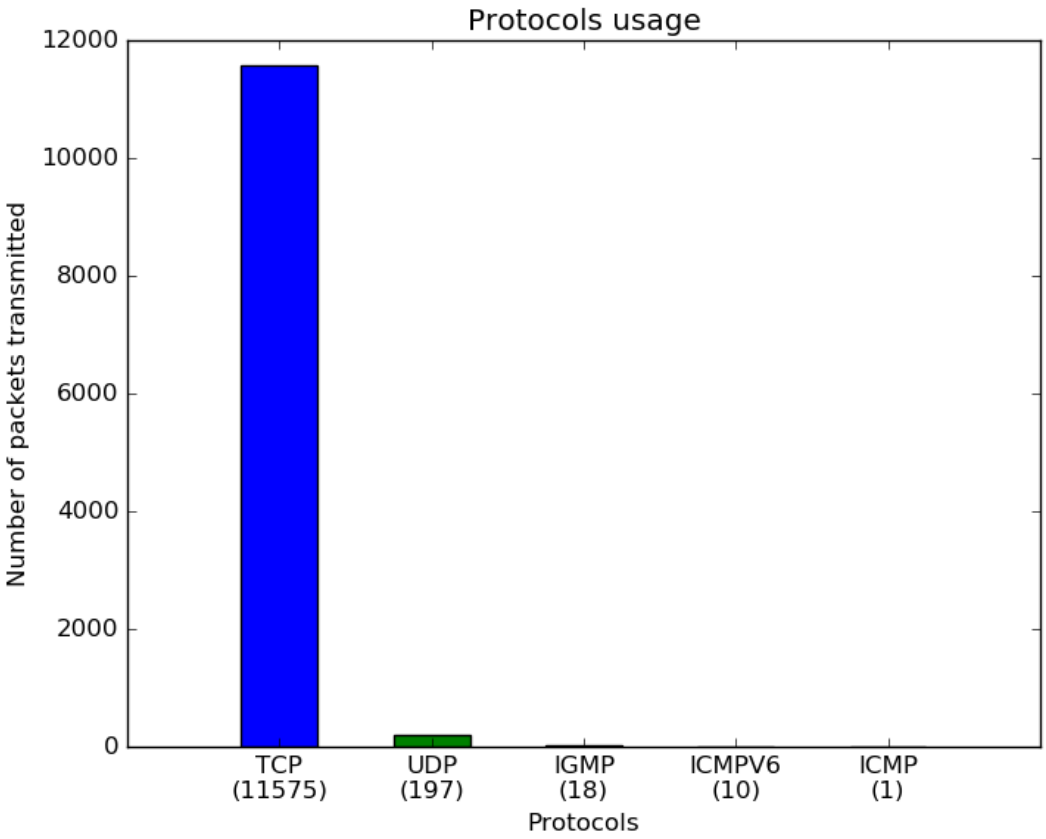
- **123** used by **ntp** service and accessed by : **time-ios.apple.com,**

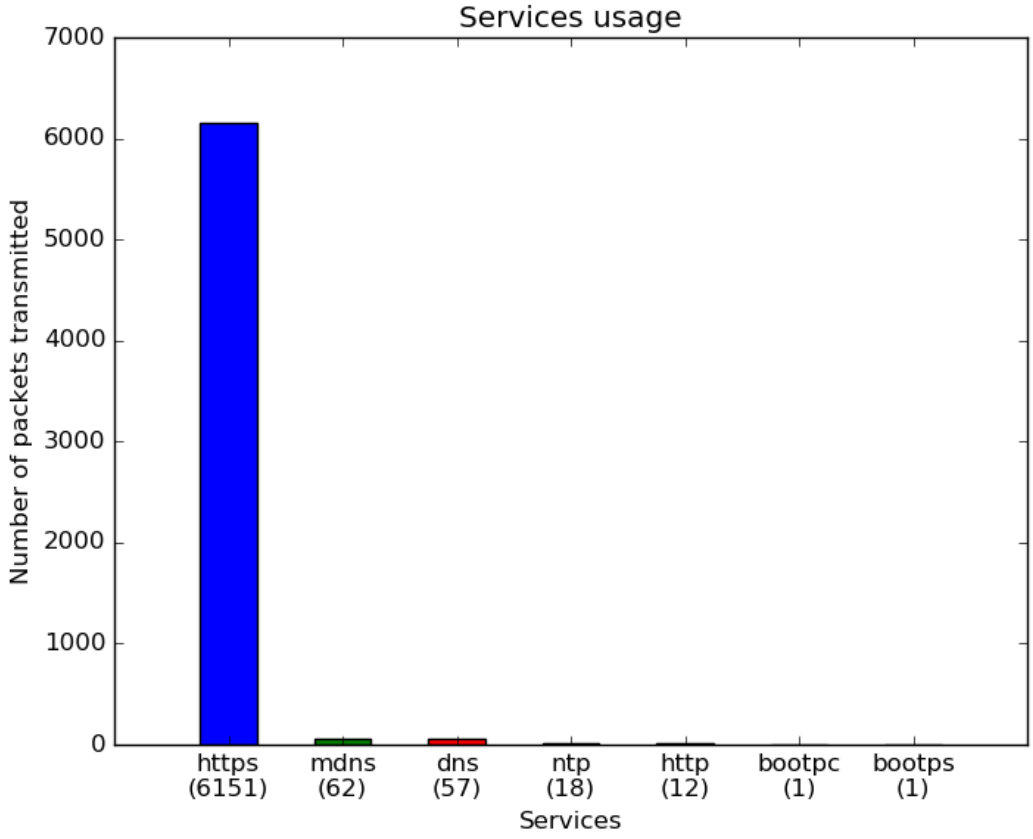
  nlams2-ntp-001.aaplimg.com, nlams2-ntp-002.aaplimg.com,

  usqas2-ntp-002.aaplimg.com, usqas2-ntp-001.aaplimg.com,

  time-ios.g.aaplimg.com

On the histograms below, you can observe a protocol and service usage overview of your network traffic. Indeed, the histograms are showing respectively the number of packets sent per protocol and the number of packets sent per service. The goal of these histograms is to give you a possibility to observe anormal protocol or service usage in order to detect some (personal) information that could be transmitted in an anormal way. For example, if you observe on the services histogram a number of dns packets higher than the https or even the http one, you could maybe conclude that dns tunneling is used to transmit some information that may be personal.


Protocols usage
Number of packets transmitted
12000
10000
8000
6000
4000
2000
0
TCP
(11575)
UDP
(197)
IGMP
(18)
ICMPV6
(10)
ICMP
(1)
Protocols


Services usage
Number of packets transmitted
7000
6000
5000
4000
3000
2000
1000
0
https
(6151)
mdns
(62)
dns
(57)
ntp
(18)
http
(12)
bootpc
(1)
bootps
(1)
Services

4. Weak authentication

4.1. Connections duration

75 connection(s) was/were **opened** or at least tried to be opened!

The **maximum TCP terminated connection duration** was **6 minute(s)**.

No terminated TCP connection lasted more than 30 minute(s).

There was/were **0 TCP connection(s) not terminated**!

No non-terminated TCP connection lasted more than 30 minute(s).

4.2. Certificate validation

We found **1** expired certificate(s).
Here are the names of the files where these certificates were saved:

- **test_00001/cert_5_0** issued by **US**, expired since **20160604010947Z**

Keep in mind that among the following self-signed certificates, some are false positives. The list of all the trusted CAs for smart devices not being available, some of the self-signed certificates given below may actually be trusted because they are root certificates issued by trusted CAs.

We found **5** self-signed certificate(s).
Here are the names of the files where these certificates were saved:

- **test_00001/cert_5_2** issued by **Apple Root CA**
- **test_00001/cert_7_3** issued by **AddTrust External CA Root**

In order to avoid overloading this report, we only reported one self-signed certificate per dinstinct issuer. You can find all the extracted certificates in the folder *RESULT/SAVE/Cert/*.

4.3. Man in the middle attack

Before reading the **warning** and the rest of this section, make sure that it was possible to connect to your service in performing the Man in the Middle attack. If it was not, you can consider that the the service you tested succeeded to pass the man in the middle attack test! This means that the service you tested is not vulnerable to this kind of attack and has thus already a resistant authentication service!

WARNING: the Man in the Middle attack was possible to perform, which is problematic! This means that the service you tested is providing a very weak authentication. Indeed, this means that the service isn't verifying whether the certificates provided are self-signed or come from a valid certificate authority. Here, **mitmproxy** (the tool we used) was considered as a valid certificate authority by the service you tested on your smart device!

Here are the words we found during the man in the middle attack: **reya**, **471604431**, **taille**, **@hotmail**, **thesisfirstname**, **analytics**, **thesisleaks2016apple@gmail.com**, **thesis**, **pass**, **taille au vivier**, **message**, **thesislastname**, **thesisl**, **detaille**, **mattieu**,

leaks, **477522662**, **email**, **5440362202229606**, **description**, **thesis2015**, **thesisf**, **thesisfi**, **mattieu.detaille@gmail.com**, **vivier**, **password**, **@gmail**, **silver**, **1993**, **tracking**, **namur**, **syed**, **token**, **male**, **thesisla**.

During the man in the middle attack, we found the word(s) **taille**, **thesisfirstname**, **thesisleaks2016apple@gmail.com**, **thesis**, **pass**, **taille au vivier**, **thesislastname**, **thesisl**, **mattieu**, **leaks**, **477522662**, **email**, **thesis2015**, **thesisf**, **thesisfi**, **vivier**, **password**, **@gmail**, **1993**, **namur**, **token**, **thesisla** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

...tent': '{"fields":[{"fieldid":"nationality","value":"be"},{"fieldid
":"legalname.firstname","value":"**thesisfirstname**"},{"fieldid":"legalna
me.lastname","value":"**thesislastname**"},{"fieldid":"credentials.**email**",
"value":"**thesisleaks2016apple@gmail.com**"},{"fieldid":"credentials.**pass
word**","value":"**thesis2015**"},{"fieldid":"dateofbirth","value":"**1993**-10-
14"},{"fieldid":"homeaddress.addressline1","value":"**taille au vivier**,
1"},{"fieldid":"homeaddress.addressline2","value":""},{"fieldid":"home
address.city","value":"**namur**"},{"fieldid":"homeaddress.zipcode","value
":"5000"},{"fieldid":"primaryphone","value":"+32**477522662**"},{"fieldid"
:"termsandconditions","value":"true"}],"intent":"buy","country":"be","
riskdata":"{\\"os... ...pclient\\",\\"touchidenrolled\\":false,\\"loca
le_lang\\":\\"fr\\",\\"comp_version\\":\\"3.5.2\\",\\"**pass**codeset\\":t
rue,\\"local_identifier\\":\\"b1b0fce3-1095-45c4-bb9f-3454671bb07d\\",
\\"sms_enabled\\":... ...79-baae-8485605d89c0\\",\\"vendor_identifier\
\":\\"d6916958-71b2-45a8-8cce-3ed63c3cbdb2\\",\\"notif_**token**\\":null,\
\"os_type\\":\\"ios\\",\\"conf_url\\":\\"https:\\\\\/\\\\\/www.paypa
lobjects.com\\\\\/w... ...:fefd:609c\\"],\\"bssid\\":\\"48:ee:c:73:43
:d0\\",\\"tz\\":3600000,\\"locale_country\\":\\"be\\",\\"**email**_configu
red\\":true,\\"tz_name\\":\\"europe\\\\\/brussels\\",\\"linker_id\\":
\\"492b5cf5-29dd-480d-... ...e\\":\\"wifi\\",\\"risk_comp_session_id\\
":\\"7e34d970-8145-42e6-86ac-7161a3a57e9a\\",\\"ssid\\":\\"**thesis**\\",\
\"location_auth_status\\":\\"unknown\\",\\"is_emulator\\":false,\\"tou
chidavailable\\":true,\\"...app_version\\":\\"6.0.1\\",\\"device_name\
\":\\"iphone de **mattieu**\\",\\"timestamp\\":1458730514691}","appinfo":"
{\\"device_app_id\\":\\"com.yourcompany.ppclient\\",\... ..."{\\"devic
e_identifier\\":\\"08df058d-b6c9-46f5-bcdb-c2241dc124d9\\",\\"device_n
ame\\":\\"iphone de **mattieu**\\",\\"device_type\\":\\"iphone de **mattieu**\
\",\\"device_key_type\\":\\"ctradioaccesstechnologylte\\",\\"device_mo
del\\":\\"iphone\\",\\"device...c2241dc124d9%22%2c%22devicenetworkcarr
ier%22%3a%22proximus%22%2c%22devicetype%22%3a%22iphone%20de%20
mattieu%
22%2c%22deviceid%22%3a%22d6916958-71b2-45a8-8cce-3ed63c3cbdb2%22%
2c%22
devicemodel%22%3a%22iphone%22...

During the man in the middle attack, we found the word(s) **taille**, **thesisfirstname**, **thesis**, **taille au vivier**, **thesislastname**, **thesisl**, **mattieu**, **5440362202229606**, **thesisf**, **thesisfi**, **vivier**, **namur**, **thesisla** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

...mat': 'relative', 'host': 'api-m.paypal.com', 'method': 'post', 'co
ntent': '{"cardholderfirstname":"**thesisfirstname**","cvv2":"[redacted]","cardnu
mber":"**5440362202229606**","expirationmonth":[redacted]"cardholderlastname":"**the
sislastname**","type":"master_card","expirationyear":[redacted],"billingaddres
s":{"schemaversion":"1.0.0","city":"**namur**","line2":"","postalcode":"50

00","fullname":"**thesisfirstname thesislastname**","countrycode":"be","li
ne1":"**taille au vivier**, 1","uniqueid":"cnb3k7bfnr4cy","state":""}}', '
headers': (('host', 'api-m.paypal.com'), ('paypal-cl...c2241dc124d9%22
%2c%22devicenetworkcarrier%22%3a%22proximus%22%2c%22devicetype%22
%3a%2
2iphone%20de%20**mattieu**%22%2c%22accountcountry%22%3a%22be%22%2c
%22devic
emodel%22%3a%22iphone%22%2c%22deviceid%22%3a%22d6916...

During the man in the middle attack, we found the word(s) **thesis**, **pass**, **thesisl**, **mattieu**, **leaks**, **email**, **thesis2015**, **password**, **token** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

...tp/1.1', 'first_line_format': 'relative', 'host': 'api-m.paypal.com
', 'method': 'post', 'content': '**password**=**thesis2015**&riskdata;=%7b%22os
_version%22%3a%229.2.1%22%2c%22c%22%3a%2230%22%2c%22device_mo
del%22%3a
%22iphone%20... ...22touchidenrolled%22%3afalse%2c%22locale_lang%22%3a
%22fr%22%2c%22comp_version%22%3a%223.5.2%22%2c%22**pass**codeset%22 %3atrue
%2c%22local_identifier%22%3a%22b1b0fce3-1095-45c4-bb9f-3454671bb07d%22
%2c%22sms_ena...
...e-8485605d89c0%22%2c%22vendor_identifier%22%3a%22d
6916958-71b2-45a8-8cce-3ed63c3cbdb2%22%2c%22notif_**token**%22%3anull%2 c%2
2os_type%22%3a%22ios%22%2c%22conf_url%22%3a%22https%3a%5c%2f%5c
%2fwww.
paypalobjects.c...
...d%22%3a%2248%3aee%3ac%3a73%3a43%3ad0%22%2c%22tz%
22%3a3600000%2c%22locale_country%22%3a%22be%22%2c%22**email**_configu red%2
2%3atrue%2c%22tz_name%22%3a%22europe%5c%2fbrussels%22%2c%22linke
r_id%2
2%3a%22492b5cf5-2... ...wifi%22%2c%22risk_comp_session_id%22%3a%22074f
c946-f2cd-4210-a382-f8ca0a93ee97%22%2c%22ssid%22%3a%22**thesis**%22%2c %22l
ocation_auth_status%22%3a%22unknown%22%2c%22is_emulator%22%3afalse
%2c%
22touchidavailable%2...2%3atrue%2c%22app_version%22%3a%226.0.1%22%2c
%2
2device_name%22%3a%22iphone%20de%20**mattieu**%22%2c%22timestamp%22 %3a1458
731018674%7d&rememberme;=false&appinfo;=%7b%22device_app_id%22%3a% 22com.
yo... ...26.0.1%22%2c%22app_category%22%3a3%7d&firstpartyclientid;=d3aa
cf450dd6aa992cfba77067560733&granttype;=**password**&deviceinfo;=%7b%22de vic
e_identifier%22%3a%2208df058d-b6c9-46f5-bcdb-c2241dc124d9%22%2c%22dev
i
ce_name...%22%3a%22iphone%20de%20**mattieu**%22%2c%22device_type%22% 3a%22i
phone%20de%20**mattieu**%22%2c%22device_key_type%22%3a%22ctradioacces stech
nologylte%22%2c%22device_model%22%3a%22iphone%22%2...
...%2c%22pp_app_
id%22%3a%22app-3p637985ef709422h%22%7d&redirecturi;=urn%3aietf%3awg %3ao
auth%3a2.0%3aoob&**email**=**thesisleaks**2016apple%40gmail.com&', 'headers':
(('host', 'api-m.paypal.com'), ('paypal-client-metadata-id', '6a... ..
.c2241dc124d9%22%2c%22devicenetworkcarrier%22%3a%22proximus%22%2c
%22de
vicetype%22%3a%22iphone%20de%20**mattieu**%22%2c%22deviceid%22%3a%2 2d69169
58-71b2-45a8-8cce-3ed63c3cbdb2%22%2c%22devicemodel%22%3a%22iphone
%22..

.%3d3916952150; tsrce=ppme')), 'timestamp_start': 1458731021.226688, '
path': '/v1/mfsauth/proxy-auth/**token**', 'timestamp_end': 1458731021.313
432, 'stickycookie': false, 'port': 443, 'is_replay': false}, 'int...

During the man in the middle attack, we found the word(s) **thesis**, **pass**, **thesisl**, **mattieu**, **leaks**, **email**, **thesis2015**, **password**, **token** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

...tp/1.1', 'first_line_format': 'relative', 'host': 'api-m.paypal.com
', 'method': 'post', 'content': '**password**=**thesis2015**&riskdata;=%7b%22os
_version%22%3a%229.2.1%22%2c%22c%22%3a%2218%22%2c%22device_mo
del%22%3a
%22iphone%20... ...22touchidenrolled%22%3afalse%2c%22locale_lang%22%3a
%22fr%22%2c%22comp_version%22%3a%223.5.2%22%2c%22**pass**codeset%22 %3atrue
%2c%22local_identifier%22%3a%22b1b0fce3-1095-45c4-bb9f-3454671bb07d%22
%2c%22sms_ena...
...e-8485605d89c0%22%2c%22vendor_identifier%22%3a%22d
6916958-71b2-45a8-8cce-3ed63c3cbdb2%22%2c%22notif_**token**%22%3anull%2 c%2
2os_type%22%3a%22ios%22%2c%22conf_url%22%3a%22https%3a%5c%2f%5c
%2fwww.
paypalobjects.c...
...d%22%3a%2248%3aee%3ac%3a73%3a43%3ad0%22%2c%22tz%
22%3a3600000%2c%22locale_country%22%3a%22be%22%2c%22**email**_configu red%2
2%3atrue%2c%22tz_name%22%3a%22europe%5c%2fbrussels%22%2c%22linke
r_id%2
2%3a%22492b5cf5-2...
...wifi%22%2c%22risk_comp_session_id%22%3a%22986c
b2e0-2973-42c3-9b71-0cac891cf3cc%22%2c%22ssid%22%3a%22**thesis**%22%2 c%22l
ocation_auth_status%22%3a%22unknown%22%2c%22is_emulator%22%3afalse
%2c%
22touchidavailable%2...2%3atrue%2c%22app_version%22%3a%226.0.1%22%2c
%2
2device_name%22%3a%22iphone%20de%20**mattieu**%22%2c%22timestamp%22 %3a1458
730750019%7d&rememberme;=false&appinfo;=%7b%22device_app_id%22%3a% 22com.
yo... ...26.0.1%22%2c%22app_category%22%3a3%7d&firstpartyclientid;=d3aa
cf450dd6aa992cfba77067560733&granttype;=**password**&deviceinfo;=%7b%22de vic
e_identifier%22%3a%2208df058d-b6c9-46f5-bcdb-c2241dc124d9%22%2c%22dev
i
ce_name...%22%3a%22iphone%20de%20**mattieu**%22%2c%22device_type%22% 3a%22i
phone%20de%20**mattieu**%22%2c%22device_key_type%22%3a%22ctradioacces stech
nologylte%22%2c%22device_model%22%3a%22iphone%22%2...
...%2c%22pp_app_
id%22%3a%22app-3p637985ef709422h%22%7d&redirecturi;=urn%3aietf%3awg %3ao
auth%3a2.0%3aoob&**email**=**thesisleaks**2016apple%40gmail.com&', 'headers':
(('host', 'api-m.paypal.com'), ('paypal-client-metadata-id', '88... ..
.c2241dc124d9%22%2c%22devicenetworkcarrier%22%3a%22proximus%22%2c
%22de
vicetype%22%3a%22iphone%20de%20**mattieu**%22%2c%22deviceid%22%3a%2 2d69169
58-71b2-45a8-8cce-3ed63c3cbdb2%22%2c%22devicemodel%22%3a%22iphone
%22..
.iserv%26time%3d4185322070')), 'timestamp_start': 1458730752.890259, '
path': '/v1/mfsauth/proxy-auth/**token**', 'timestamp_end': 1458730752.998
049, 'stickycookie': false, 'port': 443, 'is_replay': false}, 'int...

During the man in the middle attack, we found the word(s) **thesisleaks2016apple@gmail.com**, **thesis**, **thesisl**, **mattieu**, **leaks**, **email**, **@gmail** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

.../1.1', 'first_line_format': 'relative', 'host': 'api-m.paypal.com', 'method': 'post', 'content': '{"**email**id":"**thesisleaks2016apple@gmail.com**"}', 'headers': (('host', 'api-m.paypal.com'), ('paypal-client-metadata-id', '98ea18439d2c471594253c... ...c2241dc124d9%22%2c%22devicenetworkcarrier%22%3a%22proximus%22%2c%22devicetype%22%3a%22iphone%20de%20**mattieu**%22%2c%22deviceid%22%3a%22d6916958-71b2-45a8-8cce-3ed63c3cb db2%22%2c%22devicemodel%22%3a%22iphone%22...6time%3d2373317206')), 'timestamp_start': 1458730445.161184, 'path': '/v1/mfsauth/user/verification/**email**', 'timestamp_end': 1458730445.240477, 'stickycookie': false, 'port': 443, 'is_replay': false}, 'int...

During the man in the middle attack, we found the word(s) **taille**, **detaille**, **mattieu**, **email**, **description**, **mattieu.detaille@gmail.com**, **@gmail** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

...irst_line_format': 'relative', 'host': 'api-m.paypal.com', 'method': 'post', 'content': '{"payee":{"**email**":"**mattieu.detaille@gmail.com**","type":"**email**"},"amount":{"currencycode":"eur","value":1},"type":"personal"}', 'headers': (('host', 'api-m.paypal... ...5a8-8cce-3ed63c3cbdb2%22%2c%22devicelanguage%22%3a%22fr-be%22%2c%22devicetype%22%3a%22iphone%20de%20**mattieu**%22%2c%22devicenetworkcarrier%22%3a%22proximus%22 %2c%22deviceos%22%3a%22iphone%20os%22%2c%22appversi... ...ebitcard"},"amount":{"currencycode":"eur","value":2,"scale":100,"zero":false,"negative":false,"debug**description**":"moneyvalue [currencycode=eur, value=2, scale=100]","positive":true,"objecttype":"moneyvalue"},"ob... ...gmixitems":[],"fee":{"currencycode":"eur","value":1,"scale":100,"zero":false,"negative":false,"debug**description**":"moneyvalue [currencycode=eur, value=1, scale=100]","positive":true,"objecttype":"moneyvalue"},"to...talamount":{"currencycode":"eur","value":2,"scale":100,"zero":false,"negative":false,"debug**description**":"moneyvalue [currencycode=eur, value=2, scale=100]","positive":true,"objecttype":"moneyvalue"},"fu...ndingmode":{"mode":"instant","displaytext":"instant","**description**":"instant","objecttype":"sendmoneyfundingmode"},"totalrecipientamount":{"currencycode":"eur","value...":1,"scale":100,"zero":false,"negative":false,"debug**description**":"moneyvalue [currencycode=eur, value=1, scale=100]","positive":true,"objecttype":"moneyvalue"},"cu...

During the man in the middle attack, we found the word(s) **taille**, **detaille**, **mattieu**, **email**, **description**, **mattieu.detaille@gmail.com**, **@gmail** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

...5a8-8cce-3ed63c3cbdb2%22%2c%22devicelanguage%22%3a%22fr-be%22%2c%22

devicetype%22%3a%22iphone%20de%20**mattieu**%22%2c%22devicenetworkcarri
er%
22%3a%22proximus%22%2c%22deviceos%22%3a%22iphone%20os%22%2c%2
2appversi
...237223","amount":{"currencycode":"eur","value":1,"scale":100,"nega
tive":false,"positive":true,"debug**description**":"moneyvalue [currencyco
de=eur, value=1, scale=100]","zero":false,"objecttype":"moneyvalue"},"
statu...s":{"status":"canceled","displaytext":"canceled","**description**"
:"canceled","objecttype":"moneyrequeststatus"},"note":"","requestee":{
"uniqueid":"**mattieu.detaille@gmail.com**","registered":false,"**email**":"**ma
ttieu.detaille@gmail.com**","firstname":"**mattieu**","lastname":"**detaille**",
"schemaversion":"1.0.0","objecttype":"contact"},"groupmoneyrequestid":
"u-0rg681039d518574h","schem...

During the man in the middle attack, we found the word(s) **taille**, **detaille**, **mattieu**, **email**, **description**, **token** in the following packets/headers:

- Here is the content of the packet which contacted the domain

p25-mailws.icloud.com

...live'), ('accept', '*/*'), ('user-agent', 'iphone mail (13d15)'), (
'authorization', 'x-mobileme-auth**token** ndc3mdc1nzgzokfrqufbqujxs1zrefz
dujn4bhlazlnsrmzhsxldctdicxncbgdicz0='), ('accept-language', 'fr-be' .
..'id': '8ecd0074-9a2a-4059-857c-bb1b0d5b8bbd', 'type': 'http', 'respo
nse': {'content': '{"account":{"**email**id":"**mattieu**.**detaille**","fullname"
:"**mattieu detaille**","account**description**":"","**email**s":[{"address":"**matt
ieu**.**detaille**@icloud.com","cansendfrom":true}]},"aliases":[],"defaultad
dress":null}', 'headers': (('content-lengt...

During the man in the middle attack, we found the word(s) **taille**, **detaille**, **mattieu**, **email**, **mattieu.detaille@gmail.com**, **@gmail** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

..., 'content': '{"type":"services","splits":[{"amount":{"currencycode
":"eur","value":1},"requestee":{"**email**":"**mattieu.detaille@gmail.com**","
type":"**email**"}}]}', 'headers': (('host', 'api-m.paypal.com'), ('paypal
-client-metadata-id', 'a47b98efe053417a8ff...5a8-8cce-3ed63c3cbdb2%22%
2c%22devicelanguage%22%3a%22fr-be%22%2c%22devicetype%22%3a%22ipho
ne%20
de%20**mattieu**%22%2c%22devicenetworkcarrier%22%3a%22proximus%22%2c% 22dev
iceos%22%3a%22iphone%20os%22%2c%22appversi...

During the man in the middle attack, we found the word(s) **thesis**, **pass**, **message**, **mattieu**, **email**, **token** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

...22touchidenrolled%22%3afalse%2c%22locale_lang%22%3a%22fr%22%2c%22
co
mp_version%22%3a%223.5.2%22%2c%22**pass**codeset%22%3atrue%2c%22loca l_iden
tifier%22%3a%22b1b0fce3-1095-45c4-bb9f-3454671bb07d%22%2c%22sms_ena
..
.e-8485605d89c0%22%2c%22vendor_identifier%22%3a%22d6916958-71b2-45a8

-8
cce-3ed63c3cbdb2%22%2c%22notif_**token**%22%3anull%2c%22os_type%22%3a
%22io
s%22%2c%22conf_url%22%3a%22https%3a%5c%2f%5c%2fwww.paypalobjects.
c...
...d%22%3a%2248%3aee%3ac%3a73%3a43%3ad0%22%2c%22tz%22%3a3600
000%2c%22l
ocale_country%22%3a%22be%22%2c%22**email**_configured%22%3atrue%2c%22
tz_na
me%22%3a%22europe%5c%2fbrussels%22%2c%22linker_id%22%3a%22492b5
cf5-2..
. ...wifi%22%2c%22risk_comp_session_id%22%3a%22919e9734-1a9f-485a-a6ae
-6fe3d6878ea3%22%2c%22ssid%22%3a%22**thesis**%22%2c%22location_auth_st
atus
%22%3a%22unknown%22%2c%22is_emulator%22%3afalse%2c%22touchidavail
able%
2...2%3atrue%2c%22app_version%22%3a%226.0.1%22%2c%22device_name%2
2%3a%
22iphone%20de%20**mattieu**%22%2c%22timestamp%22%3a1458730787936%7d'
, 'hea
ders': (('host', 'api-m.paypal.com'), ('accept', '*/*..., '1.0.0'), ('
x-paypal-service-name', '{http://svcs.paypal.com/types/pt}accesscontro
l'), ('x-paypal-**message**-protocol', 'none'), ('x-paypal-operation-name'
, 'logriskmetadata'), ('cache-control', 'no-cache'), ...

During the man in the middle attack, we found the word(s) **thesis**, **pass**, **message**, **mattieu**, **email**, **token** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

...22touchidenrolled%22%3afalse%2c%22locale_lang%22%3a%22fr%22%2c%22
co
mp_version%22%3a%223.5.2%22%2c%22**pass**codeset%22%3atrue%2c%22loca l_iden
tifier%22%3a%22b1b0fce3-1095-45c4-bb9f-3454671bb07d%22%2c%22sms_ena
..
.e-8485605d89c0%22%2c%22vendor_identifier%22%3a%22d6916958-71b2-45a8
-8
cce-3ed63c3cbdb2%22%2c%22notif_**token**%22%3anull%2c%22os_type%22%3a %22io
s%22%2c%22conf_url%22%3a%22https%3a%5c%2f%5c%2fwww.paypalobjects.
c...
...d%22%3a%2248%3aee%3ac%3a73%3a43%3ad0%22%2c%22tz%22%3a3600
000%2c%22l
ocale_country%22%3a%22be%22%2c%22**email**_configured%22%3atrue%2c%22 tz_na
me%22%3a%22europe%5c%2fbrussels%22%2c%22linker_id%22%3a%22492b5
cf5-2..
. ...wifi%22%2c%22risk_comp_session_id%22%3a%22663207c8-b4c1-4193-8e49
-3f7d06b5f1c7%22%2c%22ssid%22%3a%22**thesis**%22%2c%22location_auth_sta tus
%22%3a%22unknown%22%2c%22is_emulator%22%3afalse%2c%22touchidavail
able%
2...2%3atrue%2c%22app_version%22%3a%226.0.1%22%2c%22device_name%2
2%3a%
22iphone%20de%20**mattieu**%22%2c%22timestamp%22%3a1458730604748%7d' , 'hea
ders': (('host', 'api-m.paypal.com'), ('accept', '*/*..., '1.0.0'), ('
x-paypal-service-name', '{http://svcs.paypal.com/types/pt}accesscontro
l'), ('x-paypal-**message**-protocol', 'none'), ('x-paypal-operation-name'
, 'logriskmetadata'), ('cache-control', 'no-cache'), ...

During the man in the middle attack, we found the word(s) **reya**, **pass**, **mattieu**, **1993**, **syed**, **male** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

...dy1zkiwzekvqgmg6fpmpsze+nlgganemdcj2s5ozcnlqizaq9neiphzj30kgqagsyxw
dfdkmgiq6mytybjtpfozisqo1imhvmmmd**reya**7whz+eav6ep4v9cgswiqax3uvfzlyy\\/
tmgxezd+skdk4fiv2azcsoilyhhmd9th2tpwl3tagriuo1ie6amduueh\\/whfgyd4z ..
.ytegtvymmpa09mbsni3vgqvssvc8fh\\/zszd6zdu2n5t2sx\\/rqqft2scfzcyyzuj7e
ha36m\\/mndelgljmqllxfknf0oa7ta**1993**dw6ye6m3uegeq82jx7crdx\\/dgxt4g2one
k+w0dy5hxehn4fv9q3dwxadmf8xnnmhoif1zhbdz2isdt9nddro7sxkpog+7pu9oj... .
..grftmzftmrftwzht2vgtmzfgsmtoncftwzed2dfdufs6d+\\/rprrfnof2dvfzpklz8h
7qj7sgvro5n7o5n6qvtfbodfm21hl0gj**syed**bahsqptovvqqutw2tswqttiyps+mvpb3ly
sersagvkgfgwffkeegrnvkvhvkwhsy9l5rbgovg9efg7dx3ylrnvw0zeueayx8ioz4...
...hyechiechsc+gtntlepbpfhq0pw05kwdamfcjhm76iokk\\/psnqoubmbaob2e5ps9y
f5hdcn0vz\\/odfc+ucmkilk39s4puorl**male**r\\/xv9p7byv62l\\/ao165+am39ef\\/
pjfwumvdlpegvkbln15l9xb\\/+qjvxnpenfy3y\\/d9ivptopi67y9otbnhhssqqsf...
...sdt6cesemr7hrgnt1k10pw+zkkfmauoefqczogumvmrybtj3qpbk6odzqat3j4qwes
miqywczsrd06hjgzpkkt4pif5lqzhymxsq**pass**9aozpcui+gvpj9snt7hcywbr5yskst4o
m06rx24serlecri4eqs7jydxt21paptb48m1c4onswnn66png0on22onq8pnawo1a0o1..
. ...gprbys9zu1y0cjkkkgnscwdwsmxvrz4jvya9rzsjppmdq+9obdhnmsyacevoqcuza
gqlneqivamlf3xreklm7bebrqrlacjif1gb**pass**zplus5frycsupbohr0ug5grps4fwgxw
iqdxqdpiierwbgqkiq1rlsq8vygaxggwkioypezqznzvts4bavtp0+alxnbekhs8im4ez.
.. ...tbjw2nrxievpg1o8kformvszxe0yp60lsy0omgfztvgkadcdjyabgxxt50yrc6bx
56ezdxbmwmtrwksrkpjsw0sywooykabvuac4**syed**gfnzy60l8z316xptozmgm669k70r wy
1xu2omo8orfhprlb5pccnhe6jeoqjvpoxswahcmzrbckk14y3w3hgugsiabglwjdbnjze5
... ...tld3kgman8jtdy3jyjqjuabyoibdbpei9cxq96vgcdmuiuq+unfcwvvtjjhobci
fncp7tlv6gtsx+\\/g7ycwxmq2skwwusmfbjs**pass**h\\/lelokgoozlr2ftph21abo4vt7
17shq5t3k1v\\/bgap3h8cbd43vely7qrdpjhq3dlyvk8vhmhkavhftcrhmmho3mskbdcz
p... ...pagbihaakcvwdtgbx1dd0pwcn4fyursqoogxmqqwoizx17przkbihwwlmf8j++
izo+ddlyfxegyk7tic2ullhmlgpdkjde352jof**reya**leov0ujawjfkv\\/fjpqphyy+fpd
pnq8scfe54e0u4ltahbbbwddar8b5n6pu3drcmx5n7s68\\/wp2f7onbpvyvqovq7+8xpy
8m... ...e193yrkjzrzsynosbhvcn8pu3te2qcdcmddlvmzl8oqzabgmadaxnv9dtgc95
yx559qta2zaaemqhhfm0xrjquipnqtksusp3qym**pass**kqwsubmskinpqxb3nmisvlrmdg e
n3xwbhjlxqd5ewkiknqdhmyqlt\\/2+h2f\\/vqxf\\/ijblyvu2fu\\/vbld379xfsf3vr
5u+...5a8-8cce-3ed63c3cbdb2%22%2c%22devicelanguage%22%3a%22fr-be%22
%2c
%22devicetype%22%3a%22iphone%20de%20**mattieu**%22%2c%22devicenetwork carri
er%22%3a%22proximus%22%2c%22deviceos%22%3a%22iphone%20os%22%2
c%22appve
rsi...

During the man in the middle attack, we found the word(s) **thesis**, **pass**, **mattieu**, **email**, **token** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

...22touchidenrolled%22%3afalse%2c%22locale_lang%22%3a%22fr%22%2c%22
co
mp_version%22%3a%223.5.2%22%2c%22**pass**codeset%22%3atrue%2c%22loca l_iden
tifier%22%3a%22b1b0fce3-1095-45c4-bb9f-3454671bb07d%22%2c%22sms_ena
..
.e-8485605d89c0%22%2c%22vendor_identifier%22%3a%22d6916958-71b2-45a8
-8
cce-3ed63c3cbdb2%22%2c%22notif_**token**%22%3anull%2c%22os_type%22%3a %22io

s%22%2c%22conf_url%22%3a%22https%3a%5c%2f%5c%2fwww.paypalobjects.
c...
...d%22%3a%2248%3aee%3ac%3a73%3a43%3ad0%22%2c%22tz%22%3a3600
000%2c%22l
ocale_country%22%3a%22be%22%2c%22**email**_configured%22%3atrue%2c%22
tz_na
me%22%3a%22europe%5c%2fbrussels%22%2c%22linker_id%22%3a%22492b5
cf5-2..
. ...wifi%22%2c%22risk_comp_session_id%22%3a%227bf85192-3c64-4d2e-87fb
-29f0d5735564%22%2c%22ssid%22%3a%22**thesis**%22%2c%22location_auth_st
atus
%22%3a%22unknown%22%2c%22is_emulator%22%3afalse%2c%22touchidavail
able%
2...2%3atrue%2c%22app_version%22%3a%226.0.1%22%2c%22device_name%2
2%3a%
22iphone%20de%20**mattieu**%22%2c%22timestamp%22%3a1458730680463%7d
&userac;
cess**token**=a103.ancp144y5snjchcorja5sjaviyvolefy2szm0z8zsncfn0ficvtgyng
v7ammclz9.vffs0ublbwsl6e7fkmufvzcio9w&u...; ...e_identifier%22%3a%2208d
f058d-b6c9-46f5-bcdb-c2241dc124d9%22%2c%22device_name%22%3a%22ipho
ne%2
0de%20**mattieu**%22%2c%22device_type%22%3a%22iphone%20de%20**mattieu**
%22%2c%
22device_key_type%22%3a%22ctradioaccesstechnologylte%22%2c%22device_m
o
del%22%3a%22iphone%22%2...c2241dc124d9%22%2c%22devicenetworkcarrier
%22
%3a%22proximus%22%2c%22devicetype%22%3a%22iphone%20de%20**mattieu**
%22%2c%
22accountcountry%22%3a%22be%22%2c%22devicemodel%22%3a%22iphone%
22%2c%2
2deviceid%22%3a%22d6916...

During the man in the middle attack, we found the word(s) **thesis**, **pass**, **mattieu**, **email**, **token** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

...22touchidenrolled%22%3afalse%2c%22locale_lang%22%3a%22fr%22%2c%22
co
mp_version%22%3a%223.5.2%22%2c%22**pass**codeset%22%3atrue%2c%22loca l_iden
tifier%22%3a%22b1b0fce3-1095-45c4-bb9f-3454671bb07d%22%2c%22sms_ena
..
.e-8485605d89c0%22%2c%22vendor_identifier%22%3a%22d6916958-71b2-45a8
-8
cce-3ed63c3cbdb2%22%2c%22notif_**token**%22%3anull%2c%22os_type%22%3a %22io
s%22%2c%22conf_url%22%3a%22https%3a%5c%2f%5c%2fwww.paypalobjects.
c...
...d%22%3a%2248%3aee%3ac%3a73%3a43%3ad0%22%2c%22tz%22%3a3600
000%2c%22l
ocale_country%22%3a%22be%22%2c%22**email**_configured%22%3atrue%2c%22 tz_na
me%22%3a%22europe%5c%2fbrussels%22%2c%22linker_id%22%3a%22492b5
cf5-2..
. ...wifi%22%2c%22risk_comp_session_id%22%3a%22b146aba6-3e9e-4771-a456
-52c8ebc6d9bc%22%2c%22ssid%22%3a%22**thesis**%22%2c%22location_auth_st atus
%22%3a%22unknown%22%2c%22is_emulator%22%3afalse%2c%22touchidavail

able%
2...2%3atrue%2c%22app_version%22%3a%226.0.1%22%2c%22device_name%22%3a%
22iphone%20de%20**mattieu**%22%2c%22timestamp%22%3a1458730979718%7d
&userac;
cess**token**=a103.jff7i9a4kqat_uvq_jvmuvavh9wqrdm4nsixmxqc4xxx9hsuyb-4y-krh8snhx0c.3rbeatjzerisruf3jrhuxlpe0d0&u...; ...e_identifier%22%3a%2208df058d-b6c9-46f5-bcdb-c2241dc124d9%22%2c%22device_name%22%3a%22iphone%20de%20**mattieu**%22%2c%22device_type%22%3a%22iphone%20de%20**mattieu**%22%2c%22device_key_type%22%3a%22ctradioaccesstechnologylte%22%2c%22device_model%22%3a%22iphone%22%2...5a8-8cce-3ed63c3cbdb2%22%2c%22devicelanguage%22%3a%22fr-be%22%2c%22devicetype%22%3a%22iphone%20de%20**mattieu**%22%2c%22devicenetworkcarrier%22%3a%22proximus%22%2c%22deviceos%22%3a%22iphone%20os%22%2c%22appversi...

During the man in the middle attack, we found the word(s) **thesis**, **message**, **mattieu**, **email**, **token** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

  ...e-8485605d89c0%22%2c%22vendor_identifier%22%3a%22d6916958-71b2-45a8
  -8cce-3ed63c3cbdb2%22%2c%22notif_**token**%22%3anull%2c%22os_type%22% 3a%22ios%22%2c%22conf_url%22%3a%22https%3a%5c%2f%5c%2fwww.paypalobjects.c .
  ..d%22%3a%2248%3aee%3ac%3a73%3a43%3ad0%22%2c%22tz%22%3a3600000%2c%22locale_country%22%3a%22be%22%2c%22**email**_configured%22%3atrue%2c%22t z_name%22%3a%22europe%5c%2fbrussels%22%2c%22linker_id%22%3a%22492b5cf5-2...
  ...nown%22%2c%22risk_comp_session_id%22%3a%226d188996-eec5-4c1b-af44-
  16df07d7475e%22%2c%22ssid%22%3a%22**thesis**%22%2c%22location_auth_sta tus%22%3a%22unknown%22%2c%22is_emulator%22%3afalse%2c%22app_version%22%3a%
  ...226.0.1%22%2c%22device_name%22%3a%22iphone%20de%20**mattieu**%22% 2c%22timestamp%22%3a1458730364631%7d', 'headers': (('host', 'api-m.paypal.com'), ('accept', '*/*..., '1.0.0'), ('x-paypal-service-name', '{http://svcs.paypal.com/types/pt}accesscontrol'), ('x-paypal-**message**-protocol', 'none'), ('x-paypal-operation-name', 'logriskmetadata'), ('cache-control', 'no-cache'), ...

During the man in the middle attack, we found the word(s) **thesis**, **message**, **mattieu**, **email**, **token** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

  ...e-8485605d89c0%22%2c%22vendor_identifier%22%3a%22d6916958-71b2-45a8
  -8cce-3ed63c3cbdb2%22%2c%22notif_**token**%22%3anull%2c%22os_type%22% 3a%22

ios%22%2c%22conf_url%22%3a%22https%3a%5c%2f%5c%2fwww.paypalobject
s.c .
..d%22%3a%2248%3aee%3ac%3a73%3a43%3ad0%22%2c%22tz%22%3a36000
00%2c%22lo
cale_country%22%3a%22be%22%2c%22**email**_configured%22%3atrue%2c%22t
z_nam
e%22%3a%22europe%5c%2fbrussels%22%2c%22linker_id%22%3a%22492b5cf
5-2...
...wifi%22%2c%22risk_comp_session_id%22%3a%2289ac918c-46c4-4a6b-82a6-
33d6758e3bbd%22%2c%22ssid%22%3a%22**thesis**%22%2c%22location_auth_st
atus%
22%3a%22unknown%22%2c%22is_emulator%22%3afalse%2c%22app_version%
22%3a%
...226.0.1%22%2c%22device_name%22%3a%22iphone%20de%20**mattieu**%22%
2c%22t
imestamp%22%3a1458730749961%7d', 'headers': (('host', 'api-m.paypal.co
m'), ('accept', '*/*..., '1.0.0'), ('x-paypal-service-name', '{http://
svcs.paypal.com/types/pt}accesscontrol'), ('x-paypal-**message**-protocol'
, 'none'), ('x-paypal-operation-name', 'logriskmetadata'), ('cache-con
trol', 'no-cache'), ...

During the man in the middle attack, we found the word(s) **taille**, **detaille**, **mattieu**, **email** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

...terid%22%3a%22f6c57980-d747-4e46-96a2-35eca7321dc8%22%2c%22hidered
u
ndanttransactions%22%3atrue%2c%22**email**id%22%3a%22**mattieu**.**detaille**%40g m
ail.com%22%2c%22limit%22%3a15%2c%22group%22%3a%22completed%22%2
c%22sta
rttime%22%3a%222013-03-23... ...terid%22%3a%22c78ae450-bd49-4c57-9558-
cc83a1da1a4b%22%2c%22hideredundanttransactions%22%3atrue%2c%22**email**i d%
22%3a%22**mattieu**.**detaille**%40gmail.com%22%2c%22limit%22%3a15%2c%22gr oup%
22%3a%22pending%22%2c%22starttime%22%3a%222013-03-23t1...

During the man in the middle attack, we found the word(s) **taille**, **detaille**, **mattieu**, **email** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

...5a8-8cce-3ed63c3cbdb2%22%2c%22devicelanguage%22%3a%22fr-be%22%2c
%22
devicetype%22%3a%22iphone%20de%20**mattieu**%22%2c%22devicenetworkcarri er%
22%3a%22proximus%22%2c%22deviceos%22%3a%22iphone%20os%22%2c%2
2appversi
...terid%22%3a%22f6c57980-d747-4e46-96a2-35eca7321dc8%22%2c%22hidered
undanttransactions%22%3atrue%2c%22**email**id%22%3a%22**mattieu**.**detaille**%40 g
mail.com%22%2c%22limit%22%3a15%2c%22group%22%3a%22completed%22
%2c%22st
arttime%22%3a%222013-03-23... ...terid%22%3a%22c78ae450-bd49-4c57-9558
-cc83a1da1a4b%22%2c%22hideredundanttransactions%22%3atrue%2c%22**emai l**id
%22%3a%22**mattieu**.**detaille**%40gmail.com%22%2c%22limit%22%3a15%2c%22 group
%22%3a%22pending%22%2c%22starttime%22%3a%222013-03-23t1...

During the man in the middle attack, we found the word(s) **@hotmail**, **mattieu**, **email**, **silver** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

...ureid":"ccb54829-2626-4a94-8753-658026693aba","profileitemdata":{"c
onfirmed":false,"primary":false,"**email**address":"the.**silver@hotmail**.fr"
},"profileitemtype":"**email**","action":"create"}]}', 'headers': (('host'
, 'api-m.paypal.com'), ('paypal-client-metadata-id', '6a...5a8-8cce-3e
d63c3cbdb2%22%2c%22devicelanguage%22%3a%22fr-be%22%2c%22devicetyp
e%22%
3a%22iphone%20de%20**mattieu**%22%2c%22devicenetworkcarrier%22%3a%22p roxim
us%22%2c%22deviceos%22%3a%22iphone%20os%22%2c%22appversi...

During the man in the middle attack, we found the word(s) **@hotmail**, **mattieu**, **email**, **silver** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

...tent': '{"profilerequests":[{"closureid":"474febb7-db12-4fe5-a3fa-d
90fd6a2c57f","profileitemdata":{"**email**address":"the.**silver@hotmail**.fr"
,"schemaversion":"1.0.0","confirmed":false,"uniqueid":"emz6ydgdx7ajq",
"primary":false},"...profileitemtype":"**email**","action":"delete"}]}', '
headers': (('host', 'api-m.paypal.com'), ('paypal-client-metadata-id',
'6a...5a8-8cce-3ed63c3cbdb2%22%2c%22devicelanguage%22%3a%22fr-be%22
%2
c%22devicetype%22%3a%22iphone%20de%20**mattieu**%22%2c%22devicenetwor kcarr
ier%22%3a%22proximus%22%2c%22deviceos%22%3a%22iphone%20os%22%2
c%22appv
ersi...

During the man in the middle attack, we found the word(s) **analytics**, **pass**, **token** in the following packets/headers:

- Here is the content of the packet which contacted the domain **www.paypal.com**

...'host': 'www.paypal.com', 'method': 'get', 'content': '', 'headers'
: (('host', 'www.paypal.com'), ('**token**', 'a103.jff7i9a4kqat_uvq_jvmuva
vh9wqrdm4nsixmxqc4xxx9hsuyb-4y-krh8snhx0c.3rbeatjzerisruf3jrhuxlpe0d .
..('x-frame-options', 'sameorigin'), ('content-security-policy', "defa
ult-src 'self' https://*.google-**analytics**.com https://*.paypal.com htt
ps://*.paypalobjects.com http://*.paypalobjects.com 'unsafe-inline' h
t... ...ervice.firstpartyapps.oaspapps.com/; script-src 'self' https:/
/nexus.ensighten.com https://*.google-**analytics**.com https://*.paypal.c
om https://*.paypalobjects.com 'unsafe-inline' 'unsafe-eval' https://a
ppsforo...23 mar 2016 11:02:29 gmt'), ('connection', 'close'), ('vary'
, 'accept-encoding'), ('set-cookie', 'by**pass**me=true; path=/'), ('set-c
ookie', 'x-pp-s=eyj0ijoimtq1odczmdk0otcymcisim0ioiiwin0; domain=.paypa
l.co...

During the man in the middle attack, we found the word(s) **message**, **mattieu** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

...5a8-8cce-3ed63c3cbdb2%22%2c%22devicelanguage%22%3a%22fr-be%22%2c%22
devicetype%22%3a%22iphone%20de%20**mattieu**%22%2c%22devicenetworkcarri er%22%3a%22proximus%22%2c%22deviceos%22%3a%22iphone%20os%22%2c%22appversi
...lt":{"code":"unknown","kind":"retrycancel","title":"la demande a \xc3\xa9t\xc3\xa9 annul\xc3\xa9e","**message**":"la personne qui vous a envoy\xc3\xa9 cette demande l\xe2\x80\x99a annul\xc3\xa9e.","retrybutton":..."r\xc3\xa9essayer","cancelbutton":"pas maintenant","debug**message**":"the money request has already been canceled","validationitems":[{"title":"la demande a \xc3\xa9t\...xc3\xa9 annul\xc3\xa9e","**message**":"la personne qui vous a envoy\xc3\xa9 cette demande l\xe2\x80\x99a annul\xc3\xa9e.","fieldpath":"d...ownstreammoneyrequestsplitout.none","isfieldmapped":false,"is**message**localized":true,"objecttype":"validationfailureitem"}],"objecttype":"validationfailure**message**"},"metadata":{"executiontimems":117,"correlationid":"1db3ae92acacf","visitorid":"08df058d-b6c9-46f5...

During the man in the middle attack, we found the word(s) **471604431, mattieu** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

...","phonetype":{"name":"mobile","shortname":"mobile"},"primary":false,"linked":false,"phonenumber":"0**471604431**"},"profileitemtype":"phone","action":"create"}]}', 'headers': (('host', 'api-m.paypal.com'), ('payp5a8-8cce-3ed63c3cbdb2%22%2c%22devicelanguage%22%3a%22fr-be%22%2c%22d
evicetype%22%3a%22iphone%20de%20**mattieu**%22%2c%22devicenetworkcarrier%22%3a%22proximus%22%2c%22deviceos%22%3a%22iphone%20os%22%2c%22appversi.
..

During the man in the middle attack, we found the word(s) **471604431, mattieu** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

...},"primary":false,"schemaversion":"1.0.0","linked":false,"uniqueid":"xj8kuswg6glqu","phonenumber":"0**471604431**"},"profileitemtype":"phone","action":"delete"}]}', 'headers': (('host', 'api-m.paypal.com'), ('payp5a8-8cce-3ed63c3cbdb2%22%2c%22devicelanguage%22%3a%22fr-be%22%2c%22d
evicetype%22%3a%22iphone%20de%20**mattieu**%22%2c%22devicenetworkcarrier%22%3a%22proximus%22%2c%22deviceos%22%3a%22iphone%20os%22%2c%22appversi.
..

During the man in the middle attack, we found the word(s) **message, token** in the following packets/headers:

- Here is the content of the packet which contacted the domain

p25-ckdatabase.icloud.com

...nts=1;device=1;presence=1;records=1;sharing=1;subscriptions=1;users
=1;mescal=1;'), ('x-cloudkit-auth**token**', 'aqaaaabwrxvi-tup7ydxgtreevzu
6ahpjqotm9y~'), ('x-cloudkit-userid', '_033d0b0e6df3c4a39144ffcf77b2-p
rotobuf; desc="https://p25-ckdatabase.icloud.com:443/static/protobuf/c
louddb/clouddbclient.desc"; **message**type=requestoperation; delimited=tr
ue'), ('accept-encoding', 'gzip'), ('x-apple-i-md-m', 'arja8ogqcb...

During the man in the middle attack, we found the word(s) **email, tracking** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

...rst_line_format': 'relative', 'host': 'api-m.paypal.com', 'method':
'post', 'content': '{"events":{"**tracking**_event":"1458730807493","acto
r":{"**tracking**_visitor_id":"08df058d-b6c9-46f5-bcdb-c2241dc124d9","**trac
king**_visit_id":"ceae60a3-dca8-47b7-812f-7b56587e982d"},"channel":"mobi
le","event_params":{"ch":"consappi...os","link":"**email**","pglk":"mobile
:consapp:profile::personalinfo:l**email**","sv":"mobile","e":"cl","device_
id":"08df058d-b6c9-46f5-bcdb-c2241dc124d9","mapv":"6.0.1","t":"1458...
727207380","g":"-60","mosv":"iphone os 9.2.1","pgln":"mobile:consapp:p
rofile:personalinfo::ios::l**email**","rsta":"fr_be","cnac":"be","wifi":"e
nabled","ua":"paypalmobile\\/platform:iphone os\\/version:6.0....0%26a
pp%3dplatformapiserv%26time%3d880276054')), 'timestamp_start': 1458730
808.956176, 'path': '/v1/**tracking**/events', 'timestamp_end': 1458730808
.976879, 'stickycookie': false, 'port': 443, 'is_replay': false...

During the man in the middle attack, we found the word(s) **1993, tracking** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

...rst_line_format': 'relative', 'host': 'api-m.paypal.com', 'method':
'post', 'content': '{"events":{"**tracking**_event":"1458730742424","acto
r":{"**tracking**_visitor_id":"08df058d-b6c9-46f5-bcdb-c2241dc124d9","**trac
king**_visit_id":"ceae60a3-dca8-47b7-812f-7b56587e982d"},"channel":"mobi
le","event_params":{"device_id":"0... ...alive'), ('x-paypal-service-v
ersion', '1.0.0')), 'timestamp_start': 1458730745.294748, 'path': '/v1
/**tracking**/events', 'timestamp_end': 1458730745.35**1993**, 'stickycookie':
false, 'port': 443, 'is_replay': false}, 'intercepted': false, 'serve
r_conn': {'ti...

During the man in the middle attack, we found the word(s) **1993, tracking** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

...rst_line_format': 'relative', 'host': 'api-m.paypal.com', 'method':
'post', 'content': '{"events":{"**tracking**_event":"145873**1993**09","acto
r":{"**tracking**_visitor_id":"08df058d-b6c9-46f5-bcdb-c2241dc124d9","**trac
king**_visit_id":"ceae60a3-dca8-47b7-812f-7b56587e982d"},"channel":"mobi
le","event_params":{"ch":"consappi...tformapiserv%26time%3d3195597398;
tsrce=ppme')), 'timestamp_start': 1458731200.552929, 'path': '/v1/**tra
cking**/events', 'timestamp_end': 1458731200.586473, 'stickycookie': fal
se, 'port': 443, 'is_replay': false...

During the man in the middle attack, we found the word(s) **message**, **tracking** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

  ...rst_line_format': 'relative', 'host': 'api-m.paypal.com', 'method': 'post', 'content': '{"events":{"**tracking**_event":"1458731186550","acto r":{"**tracking**_visitor_id":"08df058d-b6c9-46f5-bcdb-c2241dc124d9","**trac king**_visit_id":"ceae60a3-dca8-47b7-812f-7b56587e982d"},"channel":"mobi le","event_params":{"ch":"consappi... ...app:home::lerror","cust":"y5b b5gp7tlh26","page":"mobile:consapp:home:::ios::lerror","eccd":"pfclien t**message**code","mdvs":"iphone7,2","erpg":"nous ne parvenons pas \xc3\xa 0 r\xc3\xa9pondre \xc3\xa0 votre deman...tformapiserv%26time%3d2977493 590; tsrce=ppme')), 'timestamp_start': 1458731187.881521, 'path': '/v1 /**tracking**/events', 'timestamp_end': 1458731187.935366, 'stickycookie': false, 'port': 443, 'is_replay': false...

During the man in the middle attack, we found the word(s) **message**, **tracking** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

  ...rst_line_format': 'relative', 'host': 'api-m.paypal.com', 'method': 'post', 'content': '{"events":{"**tracking**_event":"1458730778065","acto r":{"**tracking**_visitor_id":"08df058d-b6c9-46f5-bcdb-c2241dc124d9","**trac king**_visit_id":"ceae60a3-dca8-47b7-812f-7b56587e982d"},"channel":"mobi le","event_params":{"ch":"consappi... ...app:home::lerror","cust":"y5b b5gp7tlh26","page":"mobile:consapp:home:::ios::lerror","eccd":"pfclien t**message**code","mdvs":"iphone7,2","erpg":"nous ne parvenons pas \xc3\xa 0 r\xc3\xa9pondre \xc3\xa0 votre deman...0%26app%3dplatformapiserv%26t ime%3d427291222')), 'timestamp_start': 1458730779.272916, 'path': '/v1 /**tracking**/events', 'timestamp_end': 1458730779.320397, 'stickycookie': false, 'port': 443, 'is_replay': false...

During the man in the middle attack, we found the word(s) **mattieu**, **token** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

  ...c2241dc124d9%22%2c%22devicenetworkcarrier%22%3a%22proximus%22%2c %22 devicetype%22%3a%22iphone%20de%20**mattieu**%22%2c%22accountcountry%2 2%3a% 22be%22%2c%22devicemodel%22%3a%22iphone%22%2c%22deviceid%22%3a %22d6916 'timestamp_start': 1458730643.812649, 'path': '/v1/mfsauth/proxy-auth /account-action/alerts?device-**token**=c418c9c23c0cbf25e410086bed99e6d239 6f6288f22644fe456c039c86ecc0a3&', 'timestamp_end': 1458730643.907...

During the man in the middle attack, we found the word(s) **mattieu**, **token** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

...c2241dc124d9%22%2c%22devicenetworkcarrier%22%3a%22proximus%22%2c%22
devicetype%22%3a%22iphone%20de%20**mattieu**%22%2c%22accountcountry%2 2%3a%22be%22%2c%22devicemodel%22%3a%22iphone%22%2c%22deviceid%22%3a%22d6916
'timestamp_start': 1458730609.523627, 'path': '/v1/mfsauth/proxy-auth/account-action/alerts?device-**token**=c418c9c23c0cbf25e410086bed99e6d2396f6288f22644fe456c039c86ecc0a3&', 'timestamp_end': 1458730609.631...

During the man in the middle attack, we found the word(s) **tracking, token** in the following packets/headers:

- Here is the content of the packet which contacted the domain **app.adjust.com**

...lative', 'host': 'app.adjust.com', 'method': 'post', 'content': 'bundle_id=com.yourcompany.ppclient&**tracking**_enabled=1&language;=fr&countr;y=be&app;_version=34&device;_name=iphone7%2c2&app;_version_short=6.0.1&i o;s ...count=2&os;_name=ios&session;_length=279&time;_spent=202&idfv;=d6916958-71b2-45a8-8cce-3ed63c3cbdb2&app;_**token**=4y6uqrurdkgf&os;_version=9.2.1&subsession;_count=5&environment;=production&created;_at=2016-03-23t11%3a...57%3a23.580z%2b0100&device;_type=iphone&event;_**token**=he59yv&idfa;=fad 3bdcc-90bc-4733-aa67-2201f9cf7b25&sent;_at=2016-03-23t11%3a57%3a23.591z %2b0100', 'hea... none, 'id': 'b63f7cdb-0cd3-4c19-b068-f0fdb878cb1f', 'type': 'http', 'response': {'content': '{"app_**token**":"4y6uqrurdkgf","adid":"dad33360cd389e2eadb46c296da8de1a"}', 'headers': (('date', 'wed, 23 mar 2016...

During the man in the middle attack, we found the word(s) **tracking, token** in the following packets/headers:

- Here is the content of the packet which contacted the domain **app.adjust.com**

...lative', 'host': 'app.adjust.com', 'method': 'post', 'content': 'bundle_id=com.yourcompany.ppclient&**tracking**_enabled=1&language;=fr&countr;y=be&app;_version=34&device;_name=iphone7%2c2&app;_version_short=6.0.1&i o;s ...count=2&os;_name=ios&session;_length=867&time;_spent=698&idfv;=d6916958-71b2-45a8-8cce-3ed63c3cbdb2&app;_**token**=4y6uqrurdkgf&os;_version=9.2.1&subsession;_count=13&environment;=production&created;_at=2016-03-23t12%3...a07%3a11.581z%2b0100&device;_type=iphone&event;_**token**=e0gtim&idfa;=fa d3bdcc-90bc-4733-aa67-2201f9cf7b25&sent;_at=2016-03-23t12%3a07%3a11.587z%2b0100', 'hea... none, 'id': 'b04c4d17-e650-4b95-8332-b2e8bce640d9', 'type': 'http', 'response': {'content': '{"app_**token**":"4y6uqrurdkgf","adid":"dad33360cd389e2eadb46c296da8de1a"}', 'headers': (('date', 'wed, 23 mar 2016...

During the man in the middle attack, we found the word(s) **tracking** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

...rst_line_format': 'relative', 'host': 'api-m.paypal.com', 'method': 'post', 'content': '{"events":{"**tracking**_event":"1458730377510","actor":{"**tracking**_visitor_id":"08df058d-b6c9-46f5-bcdb-c2241dc124d9","**tracking**_visit_id":"6955d435-48f6-4f33-a4ec-f40a962cba07"},"channel":"mobile","event_params":{"ch":"consappi...%26app%3dplatformapiserv%26time%3

d2171990614')), 'timestamp_start': 1458730381.058168, 'path': '/v1/**tra cking**/events', 'timestamp_end': 1458730381.077447, 'stickycookie': fal se, 'port': 443, 'is_replay': false...

During the man in the middle attack, we found the word(s) **tracking** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

  ...rst_line_format': 'relative', 'host': 'api-m.paypal.com', 'method': 'post', 'content': '{"events":{"**tracking**_event":"1458731224408","acto r":{"**tracking**_visitor_id":"08df058d-b6c9-46f5-bcdb-c2241dc124d9","**trac king**_visit_id":"ceae60a3-dca8-47b7-812f-7b56587e982d"},"channel":"mobi le","event_params":{"device_id":"0...tformapiserv%26time%3d3615027798; tsrce=ppme')), 'timestamp_start': 1458731226.780299, 'path': '/v1/**tra cking**/events', 'timestamp_end': 1458731226.801671, 'stickycookie': fal se, 'port': 443, 'is_replay': false...

During the man in the middle attack, we found the word(s) **email** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

  [httpflow request = request(post api-m.paypal.com:443/v1/mfsauth/us er/verification/**email**) response = response(200 ok, application/json , 249b)]...

During the man in the middle attack, we found the word(s) **token** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

  [httpflow request = request(post api-m.paypal.com:443/v1/mfsauth/pr oxy-auth/to_bind-user_for_**token**) response = response(200 ok, applic ation/json, 328b)]...

During the man in the middle attack, we found the word(s) **token** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

  [httpflow request = request(post api-m.paypal.com:443/v1/mfsauth/pr oxy-auth/**token**) response = response(200 ok, application/json, 1.71k b)]...

During the man in the middle attack, we found the word(s) **mattieu** in the following packets/headers:

- Here is the content of the packet which contacted the domain **api-m.paypal.com**

  ...5a8-8cce-3ed63c3cbdb2%22%2c%22devicelanguage%22%3a%22fr-be%22%2c %22
  devicetype%22%3a%22iphone%20de%20**mattieu**%22%2c%22devicenetworkcarri er% 22%3a%22proximus%22%2c%22deviceos%22%3a%22iphone%20os%22%2c%2

2appversi
...

Automated report generated for Airbsit mobile application

UNIVERSITE CATHOLIQUE DE LOUVAIN

ECOLE POLYTECHNIQUE DE LOUVAIN

Leak sources analysis

Automated report

Supervisor: Dr. Ramin SADRE

by Mattieu DETAILLE
& Mohammad Muntasib Ali SYED

1. Lack of encryption

1.1. Unencrypted word(s) extracted

Here are the word(s) we found without any encryption security:

- **GT-I9505**
- **password**
- **tracking**
- **namur**
- **description**
- **vivier**
- **gender**
- **taille**
- **syed**
- **analytics**
- **token**
- **october**
- **english**
- **belgium**
- **san francisco**
- **message**
- **male**
- **pass**
- **email**
- **silver**

We found the word(s) **GT-I9505**, **namur**, **vivier**, **taille**, **token**, **belgium** in the following packet(s):

- 20-05-2016 15:40:54.522674; 192.168.42.15: 37760 --> 173.194.65.95: 80

  In this packet, the domain **maps.googleapis.com** was contacted by your smart device.

  get /maps/api/js/geocodeservice.search?4s1%20chemin%20de%20la%20**taille**
  %20au%20**vivier**%2c%205000%20**namur**%2c%20**belgium**&7sus&9sen-us&key;=aizas ya
  6teyjmytlrrd3gbndg2psmmhqkltddgy&callback;=_xdc_._aw4v3b&**token**=121518 h
  ttp/1.1 host: maps.googleapis.com connection: keep-alive accept: */
  * user-agent: mozill...a/5.0 (linux; android 5.0.1; **gt-i9505** build/lr
  x22c) applewebkit/537.36 (khtml, like gecko) chrome/45.0.2454.101 cros
  swalk/16.45.421.19 mo...

We found the word(s) **description**, **gender**, **email** in the following packet(s):

- 20-05-2016 15:36:45.444051; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  file","birthday",s),this.user.sitter.about&&n.trackevent;("user","profi
  le","**description**",s),(this.user.sitter.languages||this.user.sitter.spo
  kenlanguages)&&n.trackevent;("user","profile","language",s),this.user.**g
  ender**&&n.trackevent;("user","profile","**gender**",s),this.user.sitter.lift
  &&n.trackevent;("user","profile","lift",s),this.adjustedmaxdistance&&n.;
  trac...kevent("user","profile","maxdistance",s)),"parent"===this.user.
  role&&this.user.;**email**&&n.trackevent;("user","profile","nameparent"),thi
  s.user.profilecompletion=void 0,e.updateuser(this.u...

We found the word(s) **description**, **analytics**, **token** in the following packet(s):

- 20-05-2016 15:36:44.631089; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...", "google": "aizasya6teyjmytlrrd3gbndg2psmmhqkltddgy", "googlese
  nderid": "646448084434", "google**analytics**": "ua-68859500-1", "scheme
  ": "airbsit", "mobile": true, "usesessionstore": true, "usefilestor
  ag ...agecleanlimit": 3, "localstorageprivatefields": ["deviceid
  ", "authuser", "session", "**token**", "previouslocations",
  "search", "searchquery", "storeditems"] }, "name": "app",
  ..."version": "1.0.0", "**description**": "take some air while they sit!
  " }; angular.module("gettext",[]),angular.module("gettext").constan...

We found the word(s) **description**, **message**, **pass** in the following packet(s):

- 20-05-2016 15:36:45.382513; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...tact us.":"si le probl■■me persiste, contactez-nous:","if your devi
  ce allows it, you can check your **message**s' spam folder.":"si votre app
  areil le permet, pensez ■■ v■■rifier le dossier spam de vos sms.","som
  e phone operators have trouble transmitting verification **message**s.":"c
  ertains op■■rateurs ont du mal ■■ transmettre les sms de v■■rification
  .","trouble logging in?"... ...friends":"mes amis","your start date mu
  st be in the future":"impossible d'indiquer une date dans le **pass**■■.",
  abort:"annuler","abort this sitting":"annuler ce sitting","comment:":"
  votre commentaire:",**description**:"**description**","disagree with this?":"v
  ous n'■■tes pas d'accord?","has been removed from your favorites":"n'e
  st p....","including a":"dont","price per hour":"prix ■■ l'heure","pri
  ce/h":"prix/h","proceed to payment":"**pass**er au paiement",rating:"note"
  ,"sitting summary":"r■■sum■■ du sitting",sorry:"d■■sol■■","the parent
  i...

We found the word(s) **description**, **message**, **pass** in the following packet(s):

- 20-05-2016 15:36:45.692118; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...itting afzeggen?","you can adjust the start and end time if needed"
  :"u kan de start- en eindtijd aan**pass**en wanneer nodig","you didn't add

a comment, save anyway?":"u heeft geen opmerking toegevoegd, toch ..
.eren, wifi, dromen...)","required fields are missing":"verplichte vel
den zijn niet ingevuld","enter **description**":"vul een beschrijving in",
"tell the sitters more about your family to increase your chances of f
in...initive choice":"aan het wachten op de definitieve keuze van de o
uder","about us...":"over ons...","**message** history":"berichten geschie
denis","paid":"betaald met","paid by":"betaald met","payment":"betalin
g"...

We found the word(s) **gender**, **october**, **male** in the following packet(s):

- 20-05-2016 15:36:45.443959; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...n.getstring("june"),n.getstring("july"),n.getstring("august"),n.get
  string("september"),n.getstring("**october**"),n.getstring("november"),n.g
  etstring("december")]};var o='[ion-popover-view style="width: 160px;he
  ...x;"][ion-content][div class="list" style="text-align: center;"][a
  class="item" ng-click="view.select**gender**(\'fe**male**\')"][i class="positi
  ve ion-fe**male**"][/i] [span translate]fe**male**[/span][/a][a class="item" n
  g-click="view.select**gender**(\'**male**\')"][i class="positive ion-**male**"][/i
  ] [span translate]**male**[/span][/a][/div][/ion-content][/ion-popover-vie
  w]';this.**gender**popover=i.fromtemplate(o,{scope:e});var a='[ion-popover
  -view style="width: 140px;height: 60px;"][ion...

We found the word(s) **gender**, **male**, **email** in the following packet(s):

- 20-05-2016 15:36:45.372918; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  :"modifier l'adresse","edit your profile picture and info.":"ajoutez u
  ne photo et vos infos.",**email**:"**email**","**email** address":"adresse **email**",
  end:"fin","enter a street number":"entrez un num■■ro","enter address":
  "entrez l■■■adresse","enter ...code":"code de v■■rification","enter da
  te and time":"entrez la date et l■■■heure","enter **email**":"**email**","ente
  r first name":"entrer pr■■nom","enter last name":"entrer nom","enter n
  ame (home...)":"entrer ... ...oraire ■■ 6■■■)",expiration:"expiration"
  ,"favorite sitters":"sitters favoris",february:"f■■vrier",fe**male**:"femm
  e",fe**male**:"femme","first name":"pr■■nom",fri:"ven","friends who trust
  her":"amis qui lui font d■■j■■ confianc...e","friends' sitters":"sitte
  rs d■■■amis",gallery:"galerie",**gender**:"genre","get ready!":"get ready!
  ","give a rating":"donnez une note","go to your iphone's settings, ...

We found the word(s) **gender**, **male**, **email** in the following packet(s):

- 20-05-2016 15:36:45.345375; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...address":"edit address","edit your profile picture and info.":"edit
  your profile picture and info.",**email**:"**email**","**email** address":"**email**
  address",end:"end","enter a street number":"enter a street number","en
  ter address":"enter address",..."enter code":"enter code","enter date
  and time":"enter date and time","enter **email**":"enter **email**","enter fir

st name":"enter first name","enter last name":"enter last name","enter name (home...)":"... ... hourly price)",expiration:"expiration","favo rite sitters":"favorite sitters",february:"february",fe**male**:"fe**male**",f e**male**:"fe**male**","first name":"first name",fri:"fri","friends who trust her":"friends who trust her","friends' sitt...ers":"friends' sitters", gallery:"gallery",**gender**:"**gender**","get ready!

We found the word(s) **password**, **pass**, **email** in the following packet(s):

- 20-05-2016 15:36:46.444230; 54.231.192.39: 80 --> 192.168.42.15: 37448

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...near;transition:opacity .15s ease-in,top .2s linear} input[type=sea rch],input[type=text],input[type=**password**],input[type=datetime],input[type=datetime-local],input[type=date],input[type=month],input[type=tim e],input[type=week],input[type=number],input[type=**email**],input[type=ur l],input[type=tel],input[type=color],textarea{display:block;padding-to p:2px;padding-l...

We found the word(s) **password**, **token**, **pass** in the following packet(s):

- 20-05-2016 15:36:43.642095; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...+b:c;++d[b;)a.push(d);return a})}},d.pseudos.nth=d.pseudos.eq;for(b in{radio:!0,checkbox:!0,file:!0,**password**:!0,image:!0})d.pseudos[b]=ma (b);for(b in{submit:!0,reset:!0})d.pseudos[b]=na(b);function qa(){}qa. prototype=d.filters=d.pseudos,d.setfilters=new qa,g=ga.**token**ize=functi on(a,b){var c,e,f,g,h,i,j,k=z[a+" "];if(k)return b?0:k.slice(0);h=a,i= [],j=d.prefilter;whi...

We found the word(s) **male**, **pass**, **email** in the following packet(s):

- 20-05-2016 15:36:45.751171; 54.231.192.39: 80 --> 192.168.42.15: 37448

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...re{content:"■■■"} .ion-code-working:before{content:"■■■"} .ion-coff ee:before{content:"■■■"} .ion-com**pass**:before{content:"■■■"} .ion-compo se:before{content:"■■■"} .ion-connection-bars:before{content:"■■■"} .. .ion-edit:before{content:"■■■"} .ion-egg:before{content:"■■■"} .ion-ej ect:before{content:"■■■"} .ion-**email**:before{content:"■■■"} .ion-**email**- unread:before{content:"■■■"} .ion-erlenmeyer-flask:before{content:"■■■ "} .ion-erlenmeyer-flask-bubb...before{content:"■■■"} .ion-eye:before{ content:"■■■"} .ion-eye-disabled:before{content:"■■■"} .ion-fe**male**:bef ore{content:"■■■"} .ion-filing:before{content:"■■■"} .ion-film-marker: before{content:"■■■"} .ion...

We found the word(s) **male**, **pass**, **email** in the following packet(s):

- 20-05-2016 15:36:45.745141; 54.231.192.39: 80 --> 192.168.42.15: 37448

  In this packet, the domain **app.airbsit.com** contacted your smart device.

...fore,.ion-code-download:before,.ion-code-working:before,.ion-code:b
efore,.ion-coffee:before,.ion-com**pass**:before,.ion-compose:before,.ion-
connection-bars:before,.ion-contrast:before,.ion-crop:before,.ion-c ..
.:before,.ion-earth:before,.ion-easel:before,.ion-edit:before,.ion-egg
:before,.ion-eject:before,.ion-**email**-unread:before,.ion-**email**:before,.
ion-erlenmeyer-flask-bubbles:before,.ion-erlenmeyer-flask:before,.ion-
eye-disabled:before,....ion-eye:before,.ion-fe**male**:before,.ion-filing:
before,.ion-film-marker:before,.ion-fireball:before,.ion-flag:before,.
ion-flame:...

We found the word(s) **october**, **message**, **male** in the following packet(s):

- 20-05-2016 15:36:45.372940; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...peak":"je parle ces langues:","last name":"nom","let's go?":"on y v
  a ?",logout:"d■■connexion",m:"m",**male**:"homme",**male**:"homme","manage my"
  :"g■■rer mes",march:"mars",may:"mai",**message**:"**message**",min:"min",minut
  e:"minute",minutes:"minutes",mon:"lun",month:"mois",months:"mois",mth:
  "mois",mths:"... ...:"nationalit■■","need help ?":"besoin d'aide ?",ne
  w:"nouveau","new address":"nouvelle adresse","new **message**s":"nouveaux
  messages",next:"suivant",nexts:"prochains",nice:"bien",no:"non","no fa
  vorites available!":"pas de favoris d...tant",notifications:"notificat
  ions",november:"novembre","number[br]of kids":"nombre[br]d■■■enfants",
  october:"

We found the word(s) **october**, **message**, **male** in the following packet(s):

- 20-05-2016 15:36:45.656842; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...eak":"languages i speak","last name":"last name","let's go?":"let's
  go?","logout":"logout","m":"m","**male**":"**male**","**male**":"**male**","manage my
  ":"manage my","march":"march","may":"may","**message**":"**message**","min":"m
  in","minute":"minute","minutes":"minutes","mon":"mon","month":"month",
  "months":"months","m... ..."nationality":"nationality","need help ?":"
  need help?","new":"new","new address":"new address","new **message**s":"ne
  w **message**s","next":"next","nexts":"next","nice":"nice","no":"no","no f
  avorites available!":"no favorites avai... ...yet","notifications":"no
  tifications","november":"november","number[br]of kids":"number[br]of k
  ids","**october**":"**october**","offered[br]price":"offered[br]price","ok":"o
  k","ok":"ok",

We found the word(s) **token**, **email** in the following packet(s):

- 20-05-2016 15:36:45.328967; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...d||n.get("deviceid")||o();return n.set("deviceid",t),e.usesessionst
  ore&&r;&&r.set;("deviceid",t),t}(),**token**:window.sessionstore.**token**||n.ge
  t("**token**")};return{get**token**:function(){return i.**token**},getdeviceid:fun
  ction(){return i.deviceid},isme:function(e){var n=e?e._id||e:null;retu
  rn i.user?i.u... ....user||(i.user={}),angular.extend(i.user,t),e.uses

essionstore&&r;&&r.set;("user",t),n.set("user",t),t.**token**&&(i.**token**=t.**to**
ken,n.set("**token**",t.**token**),e.usesessionstore&&r;&&r.set;("**token**",t.**token**
))},clear:function(){n.set("user",null),n.set("**token**",null),e.usesessi
onstore&&r;&&r.set;("user",null),e.usesessionstore&&r;&&r.set;("**token**",nul
l),i.user=null,i.**token**=null}}}]).factory("user",["$resource","$config"
,function(e,n){return e(n.apiurl+"/users/:id",{id:"@..._id"},{phonenum
ber:{method:"post",params:{verify:"phonenumber"}},**email**:{method:"post"
,params:{verify:"**email**"}}})}]).factory("sessionservice",["session","$r
ootscope","$loader","$confi

We found the word(s) **description**, **pass** in the following packet(s):

- 20-05-2016 15:36:45.679323; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ....","including a":"dont","price per hour":"prix ■■ l'heure","price/h
  ":"prix/h","proceed to payment":"**pass**er au paiement","rating":"note","
  sitting summary":"r■■sum■■ du sitting","sorry":"d■■sol■■","the pare ..
  .fi, r■■ves, aspirations...)","required fields are missing":"remplisse
  z les champs manquants","enter **description**":"entrez une **description**","
  tell the sitters more about your family to increase your chances of fi
  nding a sitter perfect for ...

We found the word(s) **description**, **pass** in the following packet(s):

- 20-05-2016 15:36:45.399458; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...st zijn",abort:"annuleer","abort this sitting":"annuleer deze sitti
  ng","comment:":"jouw opmerking:",**description**:"beschrijving","disagree
  with this?":"oneens met dit?","has been removed from your favorites":"
  is u ...itting afzeggen?","you can adjust the start and end time if ne
  eded":"u kan de start- en eindtijd aan**pass**en wanneer nodig","you didn'
  t add a comment, save anyway?":"u heeft geen opmerking toegevoegd, toc
  h ...eren, wifi, dromen...)","required fields are missing":"verplichte
  velden zijn niet ingevuld","enter **description**":"vul een beschrijving
  in","tell the sitters more about your family to increase your ch

We found the word(s) **message**, **pass** in the following packet(s):

- 20-05-2016 15:36:45.646439; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...rites\" style=\"font-size: 29pt;display: inline-block;vertical-alig
  n: sub\"][/i][/div][span class=\"**message**-history\" ng-class=\"{\'**messa**
  ge-history-bottom\' : view.mission.statusdisplay !== \'finished\' }\"
  ng-show=\"view.authuser.role ==...= \'parent\' && view.oneday**pass**ed()
  && view.tosee !== \'rating\'\" ng-click=\"view.showchat(view.mission.
  acceptedby, view.mission.a...cceptedby)\" translate]**message** history[/s
  pan] [span class=\"**message**-history\" ng-class=\"{\'**message**-history-bot
  tom\' : view.mission.statusdisplay !== \'finished\'}\" ng-show=\"view.
  authuser.role === ...\'sitter\' && view.oneday**pass**ed() && view.tosee !
  == \'rating\'\" ng-click=\"view.showchat(view.mission.by, view.mission

.by)\" tra...nslate]**message** history[/span] [span class=\"empty-element \"][/span][/block-loading][/ion-content][div class=\"rati...

We found the word(s) **analytics**, **message** in the following packet(s):

- 20-05-2016 15:36:45.345249; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...$on("notification",function(e,t){if(console.log("push.$on('notifica tion'",t),t.alert)i(t);else if(t.**message**)i(t);else switch(t.event){cas e"**message**":i(t)}}})}]).run(["$rootscope","sessionservice","$config"," google**analytics**","$ionicplatform",function(e,t,i,n,r){r.ready(function (){n.starttrackerwithid(i.google**analytics**),t.on("login",function(e,t){ t&&(n.trackevent("user","session","login"),n.setuserid(t._id))}),t.on("... ...g}).run(["$config","gmaps",function(e,t){t.init({libraries:"pl aces",key:e.google})}]).factory("error**message**",["$injector",function(e){return function(t){var i=e.get("gettextcatalog");if("mangopayerror"= ==t.n... either not supported or the mission you are trying to create is above the amount limit.");switch(t.**message**||t){case"connection_erro r":return i.getstring("we could not reach the server in a timely manne r. yo...

We found the word(s) **analytics**, **message** in the following packet(s):

- 20-05-2016 15:36:45.345298; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  roperly.");default:return t.**message**?i.getstring(t.**message**):i.getstring ("oops, an unknown error occured.")}}}]).factory("loadinganderrorhttpi nterceptor",["$in...jector","$q","$rootscope","$config","error**message**" ,function(e,t,i,n,r){var s=!1;return i.popupshown=!1,{requesterror:fun ction(e){return t.reject(e)},...responseerror:function(o){var a=t.defe r();if(e.invoke(["google**analytics**",function(e){e.trackevent("app","err or",o.status)}]),404==o.status||408==o.status||0==o.status||-1=... ... ").hide()}else{var c=null;if(o&&o.data;?(c=r(o.data.error),o.data.embed &&(c+="[br][br]"+o.data.embed.**message**)):c="unknown",s||i.popupshown)a. reject(o);else{s=!0,i.popupshown=!0,e.get("$loader").hide();var d=e... .get("$ionicpopup");i.popup=d.alert({template:'[div id="error-popup-**me ssage**"]'+c+"[/div]",oktype:"butto

We found the word(s) **description**, **belgium** in the following packet(s):

- 20-05-2016 15:36:56.075932; 54.231.192.39: 80 --> 192.168.42.15: 38599

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  { "name": "airbsit", "version": "0.0.24", "main": "app", "**descript ion**": "take some air while they sit!", "author": "togetair sprl", "l icense": "copyright togetair sprl **belgium**", "dependencies": ["scri pt-1462969883094.js", "style-1462969883094.css"] }

We found the word(s) **gender**, **male** in the following packet(s):

- 20-05-2016 15:36:45.393485; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...an airbsit).",expiration:"vervaldatum","favorite sitters":"favoriet
  e sitters",february:"februari",fe**male**:"vrouwelijk",fe**male**:"vrouwelijk"
  ,"first name":"voornaam",fri:"vri","friends who trust her":"vrienden d
  ie haar vertrouwe...n","friends' sitters":"sitters van vrienden",galle
  ry:"galerij",**gender**:"geslacht","get ready!":"get ready!","give a ratin
  g":"geef een cijfer","go to your iphone's setting...

We found the word(s) **gender**, **male** in the following packet(s):

- 20-05-2016 15:36:45.685831; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...rbsit).","expiration":"vervaldatum","favorite sitters":"favoriete s
  itters","february":"februari","fe**male**":"vrouwelijk","fe**male**":"vrouweli
  jk","first name":"voornaam","fri":"vri","friends who trust her":"vrien
  den die haar vertro...uwen","friends' sitters":"sitters van vrienden",
  "gallery":"galerij","**gender**":"geslacht","get ready!":"get ready!","giv
  e a rating":"geef een cijfer","go to your iphone's settin...

We found the word(s) **message**, **male** in the following packet(s):

- 20-05-2016 15:36:45.393496; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...en die ik spreek","last name":"achternaam","let's go?":"klaar om te
  gaan?",logout:"log uit",m:"mnd",**male**:"mannelijk",**male**:"mannelijk","ma
  nage my":"beheer mijn",march:"maart",may:"mei",**message**:"bericht",min:"
  min",minute:"minuut",minutes:"minuten",mon:"maa",month:"maand",months:
  "maanden",mth:...

We found the word(s) **message**, **male** in the following packet(s):

- 20-05-2016 15:36:45.672603; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...:"je parle ces langues:","last name":"nom","let's go?":"on y va ?",
  "logout":"d■■connexion","m":"m","**male**":"homme","**male**":"homme","manage
  my":"g■■rer mes","march":"mars","may":"mai","**message**":"**message**","min":
  "min","minute":"minute","minutes":"minutes","mon":"lun","month":"mois"
  ,"months":"mois","mth"... ...nationalit■■","need help ?":"besoin d'aid
  e ?","new":"nouveau","new address":"nouvelle adresse","new **message**s":"
  nouveaux **message**s","next":"suivant","nexts":"prochains","nice":"bien",
  "no":"non","no favorites available!":"pas de f...

We found the word(s) **token**, **october** in the following packet(s):

- 20-05-2016 15:36:45.340013; 54.231.192.39: 80 --> 192.168.42.15: 47540

In this packet, the domain **app.airbsit.com** contacted your smart device.

...g","$store","$injector",function(e,t,i){if(e.usesessionstore){var n
=i.get("$sessionstore"),r=t.get("**token**"),s=t.get("deviceid"),o=t.get("
user");n&&(s&&n.set;("deviceid",s),r&&n.set;("**token**",r),o&&n.set;("user",
o))}}]),___module_app.run(["$ionicplatform","$config","$globalization"
,"session...r.getstring("june"),r.getstring("july"),r.getstring("augus
t"),r.getstring("september"),r.getstring("**october**"),r.getstring("novem
ber"),r.getstring("december")]})):t.mobile&&i.getpreferredlanguage;().t
hen(funct...

We found the word(s) **password**, **pass** in the following packet(s):

- 20-05-2016 15:36:43.769526; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...{var b;return{send:function(c,d){var e,f=a.xhr(),g=++wb;if(f.open(a
  .type,a.url,a.async,a.username,a.**password**),a.xhrfields)for(e in a.xhrf
  ields)f[e]=a.xhrfields[e];a.mimetype&&f.overridemimetype;&&f.overridemi;
  m...

We found the word(s) **password**, **pass** in the following packet(s):

- 20-05-2016 15:36:43.874510; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...on(){h=!1;l()})}var k,l=function(a){k&&(f.defer.cancel(k),k=null);i
  f(!h){var e=b.val();a=a&&a.type;"**password**"===g||d.ngtrim&&"false"===d.
  ngtrim||(e=v(e));(c.$viewvalue!==e||""===e&&c.;$$hasnativevalidators)&&
  c...

We found the word(s) **description**, **message** in the following packet(s):

- 20-05-2016 15:36:45.686107; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...m aanhouden, neem dan vooral contact met ons op via:","if your devi
  ce allows it, you can check your **message**s' spam folder.":"als uw telef
  oon het toelaat, controleer dan uw berichten in de spam folder.","some
  phone operators have trouble transmitting verification **message**s.":"so
  mmige telefoon aanbieders hebben moeite met het doorsturen van verific
  atie berichten.","troub...zijn","abort":"annuleer","abort this sitting
  ":"annuleer deze sitting","comment:":"jouw opmerking:","**description**":"
  beschrijving","disagree with this?":"oneens met dit?","has been remove
  d from your favorites":"is ...

We found the word(s) **description**, **message** in the following packet(s):

- 20-05-2016 15:36:45.604475; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

...cation.fromhistory ? \'ion-bookmark\' : \'ion-ios-location\'}}\"][/
i][/div][span ng-bind=\"location.**description**\"][/span][/ion-item][/ion
-list][/ion-content][/ion-modal-view]"); $templatecache.put("mission-l
ist.resolved=\"view.missions.$resolved\"][div ng-show=\"view.visiblemi
ssions.length == 0\" class=\"info-**message**\"][span translate]nothing pl
anned yet[/span][/div][ion-list ng-if=\"view.user.

We found the word(s) **october**, **english** in the following packet(s):

- 20-05-2016 15:36:45.340024; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...r.getstring("june"),r.getstring("july"),r.getstring("august"),r.get
  string("september"),r.getstring("**october**"),r.getstring("november"),r.g
  etstring("december")]}))},function(e){console.log(e)})})}]),___module_
  app.constant("spokenlanguages",[{key:"fr",name:"fran■■ais"},{key:"en",
  name:"**english**"},{key:"nl",name:"nederlands"},{key:"ltz",name:"letzebur
  gesch"},{key:"es",name:"espa■■ol"},{key:"it...

We found the word(s) **analytics**, **october** in the following packet(s):

- 20-05-2016 15:36:45.427830; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...e.getstring("june"),e.getstring("july"),e.getstring("august"),e.get
  string("september"),e.getstring("**october**"),e.getstring("november"),e.g
  etstring("december")]))}],beforeenter:["mangopayservice","session",fun
  -dd"),i.$save({what:"bank"},function(i){e.hide(),t.next()})}])},skip:f
  unction(){this.invoke(["google**analytics**",function(e){e.trackevent("use
  r","profile","ibanskip")}]),this.next()},next:function(){this.invoke(.
  ..

We found the word(s) **analytics**, **october** in the following packet(s):

- 20-05-2016 15:36:45.432309; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  0}),this.languagepopover.hide()},onshow:["$store","$http","$config","
  watcher","session","google**analytics**","spokenlanguages","$ionicpopover"
  ,"gettextcatalog","$rootscope",function(e,t,i,n,r,s,o,a,u,c){var u.get
  string("june"),u.getstring("july"),u.getstring("august"),u.getstring("
  september"),u.getstring("**october**"),u.getstring("november"),u.getstring
  ("december")])),this.contactsshared=e.get("contactsshared"),th...

We found the word(s) **analytics**, **email** in the following packet(s):

- 20-05-2016 15:36:45.414701; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ,"menu","contact**email**"),e.share(n,"",null,"")}])}},{},e)}(dialog);dial
  og.register("favoritesdialog",favoritesdialog);var ...der","$config",
  "$timeout","$store","$ionicscrolldelegate","toast","session","gettextc

atalog","google**analytics**","$ionicpopup","$rootscope","friendservice",f
unction(e,t,i,n,r,s,o,a,u,c,d,l){var h=this;u.trackeve... ...ide()})},
600),r.scrolltop()}],share:function(){this.invoke(["socialsharing","ge
ttextcatalog","google**analytics**",function(e,t,i){var n=t.getstring("hey
, check out airbsit!");i.trackevent("user","menu","contact**email**"),e.sh
are(n,"",null,"")}])},onhide:function(){}},{},e)}(dialog);dialog.regis
ter("friendsdialog",fri...

We found the word(s) **analytics**, **email** in the following packet(s):

- 20-05-2016 15:36:45.448926; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...$traceurruntime.superconstructor(t).call(this)}return $traceurrunti
  me.createclass(t,{onshow:["google**analytics**",function(e){e.trackevent("
  user","menu","pricing")}],onhide:["$store","$rootscope",function(e,t){
  e.get("parent-pricing")||(e.set("parent-pricing",!0),t.$emit("event:cr
  eate"))}],**email**:function(){var e="mailto:support@airbsit.com";window.o
  pen(e,"_system")},facebook:function(){window....

We found the word(s) **gender**, **analytics** in the following packet(s):

- 20-05-2016 15:36:45.438333; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...$traceurruntime.superconstructor(t).call(this)}return $traceurrunti
  me.createclass(t,{onshow:["google**analytics**",function(e){e.trackevent("
  user","menu","pricing")}],onhide:["$store","$rootscope",function(e,t){
  e.superconstructor(t).call(this,e),this.user={reference:{}},this.sitte
  r_weights={wallet:25,picture:25,**gender**:5,languages:5, about:15};var r=
  new date,s=new date(r.getfullyear()-16,0,1);this.mobiscrollconfig={s..
  .

We found the word(s) **gender**, **analytics** in the following packet(s):

- 20-05-2016 15:36:45.444028; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...[i]&&(e+=this.sitter_weights[i])}this.completed=e===t},imageuploade
  d:function(){this.invoke(["google**analytics**",function(e){this.user.pict
  ureloaded=!1,this.markdirty(),"parent"===this.user.role&&e.trackevent;(
  "u ....disabled=!0,"sitter"===o.user.role&&(o.user.sitter.available=!1
  ),s.updateuser(o.user)})})})}])},show**gender**popover:function(e){this.**gen
  der**popover.show(e)},select**gender**:function(e){this.user.sitter.**gender**=e
  ,this.profileform.$dirty=!0,this.**gender**popover.hide()},showdialog:func
  tion(e){this.invoke(["mangopaycarddialog","mangopaybankdialog","toast.
  ..

We found the word(s) **october**, **email** in the following packet(s):

- 20-05-2016 15:36:45.448898; 54.231.192.39: 80 --> 192.168.42.15: 47540

In this packet, the domain **app.airbsit.com** contacted your smart device.

...i.getstring("june"),i.getstring("july"),i.getstring("august"),i.get
string("september"),i.getstring("**october**"),i.getstring("november"),i.g
etstring("december")])),e&&"sitter"===n.user.role&&-1===n.user.sitter.
...ate:function(){return"parent"===this.user.role?!(this.user.firstna
me&&this.user.lastname;&&this.user.;**email**&&this.user.language;):"sitter"=
==this.user.role?!(this.user.firstname&&this.user.lastname;&&this.user.;
...**email**&&this.user.language;&&this.user.address;&&this.user.address.add;
ress&&this.user.birthday;&&this.user.si...;

We found the word(s) **pass**, **email** in the following packet(s):

- 20-05-2016 15:36:45.393475; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...itting nu bekijken?","do you wish to edit your sitter profile now?"
  :"wilt u uw sittersprofiel nu aan**pass**en?","do you wish to receive othe
  r invitations for that time period?":"wilt u nog andere uitnodiging ..
  .ddress":"bewerk adres","edit your profile picture and info.":"bewerk
  uw profielfoto en informatie.",**email**:"e-mail","**email** address":"e-maila
  dres",end:"einde","enter a street number":"voer uw huisnummer in","ent
  er address":..."voer adres in","enter code":"voer code in","enter date
  and time":"voer datum en tijd in","enter **email**":"voer e-mailadres in"
  ,"enter first name":"voer voornaam in", "enter last name":"voer achter
  naam in...

We found the word(s) **pass**, **email** in the following packet(s):

- 20-05-2016 15:36:45.672624; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...yez qui se propose et confirmez au sitter de votre choix.","select
  country":"choisir pays","send an **email** to":"envoyez un **email** ■■","send
  invitations to the ones you'd like.":"invitez celles et ceux que vous
  pr■■f■■rez.","septe... ... nearby":"sitters pas loin","sitting":"sitt
  ing","sitting declined":"baby-sitting d■■clin■■","skip":"**pass**er","so,
  so...":"mouais■■■","something about yourself":"a propos de vous","sorr
  y":"d■■sol■■","specif...ut","start sitting":"d■■marrer","stop sitting"
  :"arr■■ter","submit code":"soumettre le code","submit **email**":"soumettr
  e e-mail","suggested sitters":"sitters sugg■■r■■s","sun":"dim","switch
  'contacts' on":"ac...

We found the word(s) **october**, **male** in the following packet(s):

- 20-05-2016 15:36:45.455203; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...slate]accepted[/span] [span translate]sorry[/span] [span translate]
  pending[/span] [span translate]fe**male**[/span] [span translate]**male**[/spa
  n] [span translate]fe**male**[/span] [span translate]**male**[/span] [span tra
  nslate]mon[/span] [span translate]tue[/span] [span translate]wed[/span
  ] [span trans...ranslate]july[/span] [span translate]august[/span] [sp

an translate]september[/span] [span translate]**october**[/span] [span tra
nslate]november[/span] [span translate]december[/span] [span translate
]next[/span] ...

We found the word(s) **october**, **message** in the following packet(s):

- 20-05-2016 15:36:45.427877; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...plate:n.getstring(o.text[a.language]),oktype:"button-light"}).then(
  function(t){u.push(o.key),i.set("**message**s",u),e.popupshown=!1})}}}})])
  }},{},e)}(service);service.register("**message**service",**message**service);v
  ar createmissiondialog=function(e){function t(e){$traceurruntime.super
  constructor(t).call(...e.getstring("june"),e.getstring("july"),e.getst
  ring("august"),e.getstring("september"),e.getstring("**october**"),e.getst
  ring("november"),e.getstring("december")]}}return t.$inject=["gettextc
  atalog"],$traceurrun...

We found the word(s) **october**, **message** in the following packet(s):

- 20-05-2016 15:36:45.393506; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  d help ?":"hulp nodig?",new:"nieuwe","new address":"nieuw adres","new
  messages":"nieuwe berichten",next:"volgende",nexts:"volgende",nice:"le
  uk",no:"nee","no favorites available! gepland",notifications:"notifica
  ties",november:"november","number[br]of kids":"aantal[br]kinderen",**oct
  ober**:"oktober","offered[br]price":"prijs",ok:"ok",ok:"ja","oops !":"oe
  ps!","oops, an unknown error occur...

We found the word(s) **message**, **email** in the following packet(s):

- 20-05-2016 15:36:46.505180; 54.231.192.39: 80 --> 192.168.42.15: 37448

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...} ion-modal-view.contact-us-dialog .container .address,ion-modal-vi
  ew.contact-us-dialog .container .**email**,ion-modal-view.contact-us-dialo
  g .container .visit{margin-top:65px} ion-view.add-contacts .image-bat;
  display:inline-block;vertical-align:bottom;margin-right:-5px} ion-view
  .add-contacts .add-contacts-**message**{text-align:center;color:#455c6c;wi
  dth:100%;height:100%;display:-webkit-flex;-webkit-justify-content...

We found the word(s) **message**, **email** in the following packet(s):

- 20-05-2016 15:36:45.650925; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...s=\"row\"][span class=\"col\" translate]some phone operators have t
  rouble transmitting verification **message**s.[/span][/div][div class=\"ro
  w\"][i class=\"col col-10 icon ion-ios-checkmark-empty positive\" styl
  ...margin-right: 5px\"][/i] [span class=\"col\" translate]if your dev
  ice allows it, you can check your **message**s\' spam folder.[/span][/div]

[div class=\"row\"][i class=\"col col-10 icon ion-ios-checkmark-empty
p...ease contact us.[/span][/div][/div][div class=\"row support\"][div
class=\"option\" ng-click=\"view.**email**()\"]support@airbsit.com[/div][
div class=\"or\" translate]or[/div][div class=\"option\" ng-click=\"v.
..

We found the word(s) **GT-I9505**, **token** in the following packet(s):

- 20-05-2016 15:37:03.624125; 192.168.42.15: 37755 --> 173.194.65.95: 80

  In this packet, the domain **maps.googleapis.com** was contacted by your smart device.

  ...sset%2fwww%2findex.html%23%2fintro&4saizasya6teyjmytlrrd3gbndg2psmm
  hqkltddgy&callback;=_xdc_._qumk5f&**token**=117073 http/1.1 host: maps.goo
  gleapis.com connection: keep-alive accept: */* user-agent: mozilla/
  5.0 (linux; android 5.0.1; **gt-i9505** build/lrx22c) applewebkit/537.36 (
  khtml, like gecko) chrome/45.0.2454.101 crosswalk/16.45.421.19 mo...

We found the word(s) **GT-I9505**, **token** in the following packet(s):

- 20-05-2016 15:40:30.586762; 192.168.42.15: 37760 --> 173.194.65.95: 80

  In this packet, the domain **maps.googleapis.com** was contacted by your smart device.

  ...d4.6138111999999865&7sus&9sen-us&key;=aizasya6teyjmytlrrd3gbndg2psmm
  hqkltddgy&callback;=_xdc_._tyvwlb&**token**=28149 http/1.1 host: maps.goog
  leapis.com connection: keep-alive accept: */* user-agent: mozilla/5
  .0 (linux; android 5.0.1; **gt-i9505** build/lrx22c) applewebkit/537.36 (k
  html, like gecko) chrome/45.0.2454.101 crosswalk/16.45.421.19 mo...

We found the word(s) **san francisco** in the following packet(s):

- 20-05-2016 15:40:57.726429; 46.137.168.242: 443 --> 192.168.42.15: 46919

  In this packet, the domain **babysit-eu-api.herokuapp.com** contacted your smart device.

  ...h assurance server ca0 ■ 140121000000z■ 170519120000z0k1 0 ■■u■■■■u
  s1■0■■■u■■■ california1■0■■■u■■■ **san francisco**1■0■■■u■ ■ heroku, inc.1
  ■0■■■u■■ ■*.herokuapp.com0■■"0 ■ *■h■■ ■■■■■■■■■■0■■
  ■■■■■■■■■@■a■!o■■
  ■4■]■■...

We found the word(s) **pass** in the following packet(s):

- 20-05-2016 15:36:45.751116; 54.231.192.39: 80 --> 192.168.42.15: 37448

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...loud-outline:before{content:"■■■"} .ion-android-color-palette:befor
  e{content:"■■■"} .ion-android-com**pass**:before{content:"■■■"} .ion-andro
  id-contact:before{content:"■■■"} .ion-android-contacts:before{conte...

We found the word(s) **pass** in the following packet(s):

- 20-05-2016 15:36:45.495749; 54.231.192.39: 80 --> 192.168.42.15: 37448

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...qmw2yge+t5rznmimgxmuaoh9a7cdic03ic12jm+2psq9y59c/fur5g+k4hgqiigonzg
  lgrikfkfgdzng58d+fpffba2erj27gozp**pass**ghb85pjzkbt2cy/p3vxbebyihruonxydr
  1nmgj/0vjtlp3gtfapjjvdunxwg6nsaet7f/gqprnfwleitots0ar9vuzdamigedhd1...

We found the word(s) **male** in the following packet(s):

- 20-05-2016 15:36:45.247510; 54.231.192.39: 80 --> 192.168.42.15: 37448

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...rmbjeciublnvkgm+gvo0zpziegw11grrb4pt5//woiswiefpiz3hhnadi2a8/zkewmo
  zqky1qkhyickqcxbewrjkgbeqqbclhkwi**male**k+k49ijij2ux0knhve7dmzb7lsskqwz+e
  xsrjy1zgq76eddepdarg+d4sgoeiyid3p1eaopaojluktqfgavscgbjuqv9w2chzcuc...

We found the word(s) **male** in the following packet(s):

- 20-05-2016 15:36:45.745216; 54.231.192.39: 80 --> 192.168.42.15: 37448

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...,.ion-locked:before,.ion-log-in:before,.ion-log-out:before,.ion-loo
  p:before,.ion-magnet:before,.ion-**male**:before,.ion-man:before,.ion-map:
  before,.ion-medkit:before,.ion-merge:before,.ion-mic-a:before,.ion-...

We found the word(s) **english** in the following packet(s):

- 20-05-2016 15:36:45.320620; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...tion(n){var t=e.findone("code",n);return t?t.name:void 0}}]).consta
  nt("languages",[{code:"en",name:"**english**"},{code:"fr",name:"fran■■ais"
  },{code:"nl",name:"nederlands"}]),___module_tchernositivex.factory("li
  ...

We found the word(s) **message** in the following packet(s):

- 20-05-2016 15:36:45.559047; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...started\'\" class=\"ongoing-sitting-sitter-img img_ongoing_sitting_
  sitter\"][/div][div class=\"stop-**message**\" ng-show=\"view.currentmissi
  on.status === \'started\' || view.currentmission.status === \'autostar
  ...

We found the word(s) **message** in the following packet(s):

- 20-05-2016 15:36:43.863284; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

... x(b)?(a=b,this):a};this.$get=["$window",function(d){function c(a){
a instanceof error&&(a.stack?a=a.**message**&&-1===a.stack.indexof(a.**messa**
ge)?"error: "+a.**message**+"\n"+a.stack:a.stack:a.sourceurl&& (a=a.**messag**
e+"\n"+a.sourceurl+":"+a.line));return a}function e(a){var b=d.console
||{},e=b[a]||b.log||c;a=!1;try{...

We found the word(s) **silver** in the following packet(s):

- 20-05-2016 15:36:46.240701; 54.231.192.39: 80 --> 192.168.42.15: 37448

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...sup{top:-.5em} sub{bottom:-.25em} fieldset{margin:0 2px;padding:.35
  em .625em .75em;border:1px solid **silver**} button,input,select,textarea{
  margin:0;outline-offset:0;outline-style:none;outline-width:0;-webkit-.
  ..

We found the word(s) **syed** in the following packet(s):

- 20-05-2016 15:36:45.953201; 54.231.192.39: 80 --> 192.168.42.15: 37448

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...//8aip54brufsaimacmaaaahaj8ddaaa//8az/54a/4etgimaemaaaahaj8cxqaa//8
  ahp/rbkwhnaimacuaaaehahmb5wfuaaka**syed**cwqrmdea//8ayf/ra80f3qimaeuaaaeha
  hmbxwaxaakasyiedwqrmdea//8ahp/rbkwhsaimacuaaaehajoa8gfyaakasyaecwqr...

We found the word(s) **syed** in the following packet(s):

- 20-05-2016 15:36:45.958581; 54.231.192.39: 80 --> 192.168.42.15: 37448

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...aacaaaehajwamqblaakasxadbaqrmdea//8anf54bi0ejqimaacaaaahaj8c7aaa//8
  af//vbasf7aimaakaaaehahmbfgamaaka**syed**cwqrmdea//8af//vbasgaaimaakaaaeha
  joaiqaqaakasyadcwqrmdea//8af//vbasf2gimaakaaaehaj0buwaqaakasx4ecwqr...

We found the word(s) **gender** in the following packet(s):

- 20-05-2016 15:36:45.638751; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ..."view.user.birthday\" placeholder=\"{{\'birthdayyy\' | translate}}\
  "][div class=\"col col-30 select-**gender**\" ng-show=\"!view.user.sitter.
  gender\" ng-click=\"view.show**gender**popover($event)\" translate]**gender**[
  /div][div class=\"col col-30 select-**gender**\" ng-show=\"view.user.sitte
  r.**gender**\" ng-click=\"view.show**gender**popover($event)\"][i class=\"posi
  tive ion-{{view.user.sitter.**gender**}}\"][/i] {{view.user.sitter.**ge**
  nder |

We found the word(s) **gender** in the following packet(s):

- 20-05-2016 15:36:46.554961; 54.231.192.39: 80 --> 192.168.42.15: 37448

In this packet, the domain **app.airbsit.com** contacted your smart device.

pe=text]{height:45px;line-height:30px} ion-view.profile-edit .user-nam
e .select-**gender**{font-size:11pt;font-weight:400;color:#afafaf} ion-vie
w.profile-edit .profile-infos .ion-location{di...

We found the word(s) **tracking** in the following packet(s):

- 20-05-2016 15:36:44.241045; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...scale=1,n.__enablescrollx=!a&&n.options.scrollingx;,n.__enablescroll
  y=!a&&n.options.scrollingy;,n.__is**tracking**=!0,n.__diddecelerationcomple
  te=!1,n.__isdragging=!a,n.__issingletouch=a,n.__positions=[]},dotouchm
  o...

We found the word(s) **tracking** in the following packet(s):

- 20-05-2016 15:36:44.207962; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...resize(),this.__fadescrollbars("out",this.options.scrollbarresizefa
  dedelay)},__issingletouch:!1,__is**tracking**:!1,__diddecelerationcomplete
  :!1,__isgesturing:!1,__isdragging:!1,__isdecelerating:!1,__isanimating
  :...

We found the word(s) **belgium** in the following packet(s):

- 20-05-2016 15:36:45.287428; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...nguages[0]]:e.name.en,{value:e.code,label:n})},!0)}}}]).constant("
  countries",[{code:"be",name:{en:"**belgium**",fr:"belgique",nl:"belg■■e",d
  e:"belgien"},prefix:"+32",currency:"eur",languages:["en","fr","nl","de
  ...

We found the word(s) **GT-I9505** in the following packet(s):

- 20-05-2016 15:40:30.723123; 192.168.42.15: 54334 --> 216.58.212.131: 80

  In this packet, the domain **csi.gstatic.com** was contacted by your smart device.

  ...n: keep-alive accept: image/webp,image/*,*/*;q=0.8 user-agent: mo
  zilla/5.0 (linux; android 5.0.1; **gt-i9505** build/lrx22c) applewebkit/53
  7.36 (khtml, like gecko) chrome/45.0.2454.101 crosswalk/16.45.421.19 m
  o...

We found the word(s) **GT-I9505** in the following packet(s):

- 20-05-2016 15:36:41.256514; 192.168.42.15: 37755 --> 173.194.65.95: 80

  In this packet, the domain **maps.googleapis.com** was contacted by your smart device.

...googleapis.com connection: keep-alive accept: */* user-agent: mo
zilla/5.0 (linux; android 5.0.1; **gt-i9505** build/lrx22c) applewebkit/53
7.36 (khtml, like gecko) chrome/45.0.2454.101 crosswalk/16.45.421.19 m
o...

We found the word(s) **email** in the following packet(s):

- 20-05-2016 15:36:45.638762; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...ired disabled=\"disabled\"][/ion-input][/div][div class=\"row\"][di
  v class=\"icon\"][i class=\"icon-**email** positive\"][/i][/div][ion-input
  class=\"item item-input col\"][input type=\"text\" ng-model=\"view.us
  er.**email**\" ng-model-options=\"{debounce: 200}\" placeholder=\"{{\'**emai
  l** address\' | translate}}\" required][/ion-input][/div][div class=\"ro
  w\" ng-click=\"view.showdialog(...

We found the word(s) **email** in the following packet(s):

- 20-05-2016 15:36:45.393528; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...rt:"start","start sitting":"start sitting","stop sitting":"stop sit
  ting","submit code":"ok","submit **email**":"voer **email** in","suggested sit
  ters":"voorgestelde sitters",sun:"zon","switch 'contacts' on":"activee
  r 'contacte...rde die u verstrekte is ongeldig. zorg ervoor dat u de g
  evraagde informatie correct invoert.","this **email** address is already u
  sed":"dit e-mail

We found the word(s) **token** in the following packet(s):

- 20-05-2016 15:36:44.659696; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...&&(t._useutc=e._useutc),t._pf=i(),t._f=e._f[r],x(t),p(t)&&(o+=t._pf
  .charsleftover,o+=10*t._pf.unused**token**s.length,t._pf.score=o,(null==a|
  |a]o)&&(a=o,n=t));f(e,n||t)}function ee(e){var t,n,i=e._i,a=rt.exec(..
  .

We found the word(s) **token** in the following packet(s):

- 20-05-2016 15:36:43.959535; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ns.length)throw ca("ueoe",this.text);return this.**token**s[0]},peek:funct
  ion(a,b,d,c){return this.peekahead(0,a,b,d,c)},peekahead:function(a,b,
  d,c,e){if(this.**token**s.length]a){a=this.**token**s[a];var f=a.text;if(f===b
  ||f===d||f===c||f===e||!(b||d||c||e))return a}return!1},expect:functio
  n(a,...b,d,c){return(a=this.peek(a,b,d,c))? (this.**token**s.shift(),a):!1
  },selfreferential:{"this":{type:s.thisexpression},$locals:{type:s.loca
  lsexpression}}}...

We found the word(s) **description** in the following packet(s):

- 20-05-2016 15:36:45.638820; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...s=\"list list-inset\" style=\"padding-bottom: 50px; margin-top: 0px
  \"][span translate class=\"title-**description**\"]**description**[/span][ion-
  input class=\"item item-input **description**\"][textarea ng-if=\"view.use
  r.role === \'sitter\'\" rows=\"5\" ng-model=\"view.user.sitter.about\"
  ...

We found the word(s) **description** in the following packet(s):

- 20-05-2016 15:36:46.548205; 54.231.192.39: 80 --> 192.168.42.15: 37448

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...2} ion-view.mission-view-sitter .event-details{font-size:12pt} ion-
  view.mission-view-sitter .status-**description**{display:-webkit-flex;-web
  k...

We found the word(s) **analytics** in the following packet(s):

- 20-05-2016 16:05:35.658453; 192.168.42.15: 41076 --> 74.125.206.97: 443

  In this packet, the domain **ssl-google-analytics.l.google.com** was contacted by your

  smart device.

  ...■ ■-■oz■■■■,l^y}?■dnj■■■x■z h■■■■■■(■+■,■/■0■■■■■ ■
  ■■■■■3■9■■■■■■■
  ■■/■5■■■■■■■■■■■ ■■■■■ssl.google-**analytics**.com■ ■■■■■■■ ■4■2■■■
  ■■■ ■
  ■■■ ■ ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■#■■■b■■■■&■=■ ■]■■■■■■mv■
  ■3...

We found the word(s) **analytics** in the following packet(s):

- 20-05-2016 15:36:45.414690; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ...config","$timeout","$store","$ionicscrolldelegate","toast","session
  service","gettextcatalog","google**analytics**","$ionicpopup","$rootscope"
  ,"friendservice",function(e,t,i,n,r,s,o,a,u,c,d,l){var h=this;u.tracke
  ve(function(e){n.user=e})})}])},share:function(){this.invoke(["socials
  haring","gettextcatalog","google**analytics**",function(e,t,i){var n=t.get
  string("hey, check out airbsit!");i.trackevent("user"

We found the word(s) **october** in the following packet(s):

- 20-05-2016 15:36:44.735742; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

...{return e.definelocale("en-au",{months:"january_february_march_apri
l_may_june_july_august_september_**october**_november_december".split("_")
,monthsshort:"jan_feb_mar_apr_may_jun_jul_aug_sep_oct_nov_dec".split("
...

We found the word(s) **october** in the following packet(s):

- 20-05-2016 15:36:44.682119; 54.231.192.39: 80 --> 192.168.42.15: 47540

  In this packet, the domain **app.airbsit.com** contacted your smart device.

  ....source+"|"+/\d{1,2}/.source)},_months:"january_february_march_apri
  l_may_june_july_august_september_**october**_november_december".split("_")
  ,months:function(e){return this._months[e.month()]},_monthsshort:"jan_
  ...

1.2. Unencrypted file(s) extracted

Some unencrypted files were extracted from your network traffic. Have a look in the *RESULS/FILES_EXTRACTED* directory!

2. Weak encryption

The security protocol SSL/TLS was used to encrypt part of your traffic, which is already a good start! 17% of your IP network traffic was encrypted using the SSL/TLS security protocol.

No problems detected for the hash functions, block cipher algorithms or stream cipher algorithms used for encrypting your network traffic!

Here are the cryptographic algorithms used for securing a part of your network traffic: CBC, AES, SHA, GCM, RSA, ECDHE, SHA256, ECDSA, POLY1305, CHACHA20.

3. Covert channels

3.1. Adblock

Here are all the domains blocked by the adblock module : **csi.gstatic.com, ssl-google-analytics.l.google.com**.

In one of the packets exchange, the following domain(s) was(were) blocked : **csi.gstatic.com**.
Here are some known alternative name(s) of this(these) domain(s) : **ams15s21-in-f131.1e100.net**.
Here are the known ip adresses of this(these) domain(s) : **216.58.212.163, 216.58.193.131, 216.58.209.99, 216.58.201.163, 216.58.212.195, 216.58.212.131, 172.217.17.227, 216.58.218.3, 172.217.1.131, 216.58.209.131, 216.58.213.3, 172.217.18.131, 216.58.213.35, 216.58.217.227, 216.58.201.195, 216.58.212.227**

In one of the packets exchange, the following domain(s) was(were) blocked : **ssl-google-analytics.l.google.com**.
Here are some known alternative name(s) of this(these) domain(s) : **wk-in-f97.1e100.net, ssl.google-analytics.com**.
Here are the known ip adresses of this(these) domain(s) : **74.125.206.97**

In one of the packets exchange, the following domain(s) was(were) blocked : **csi.gstatic.com**.
Here are some known alternative name(s) of this(these) domain(s) : **dfw25s13-in-f3.1e100.net**.
Here are the known ip adresses of this(these) domain(s) : **216.58.194.67**

In one of the packets exchange, the following domain(s) was(were) blocked : **ssl-google-analytics.l.google.com**.
Here are some known alternative name(s) of this(these) domain(s) : **wk-in-f97.1e100.net, ssl.google-analytics.com**.
Here are the known ip adresses of this(these) domain(s) : **74.125.206.97**

In one of the packets exchange, the following domain(s) was(were) blocked : **ssl-google-analytics.l.google.com**.
Here are some known alternative name(s) of this(these) domain(s) : **wk-in-f97.1e100.net, ssl.google-analytics.com**.
Here are the known ip adresses of this(these) domain(s) : **74.125.206.97**

3.2. DNSBL

The DNS blacklists module didn't find any match.

3.3. SafeBrowsing

The SafeBrowsing module didn't find any match.

3.4. SafeLookup

The SafeLookup module didn't find any match.

3.5. Potential backdoors

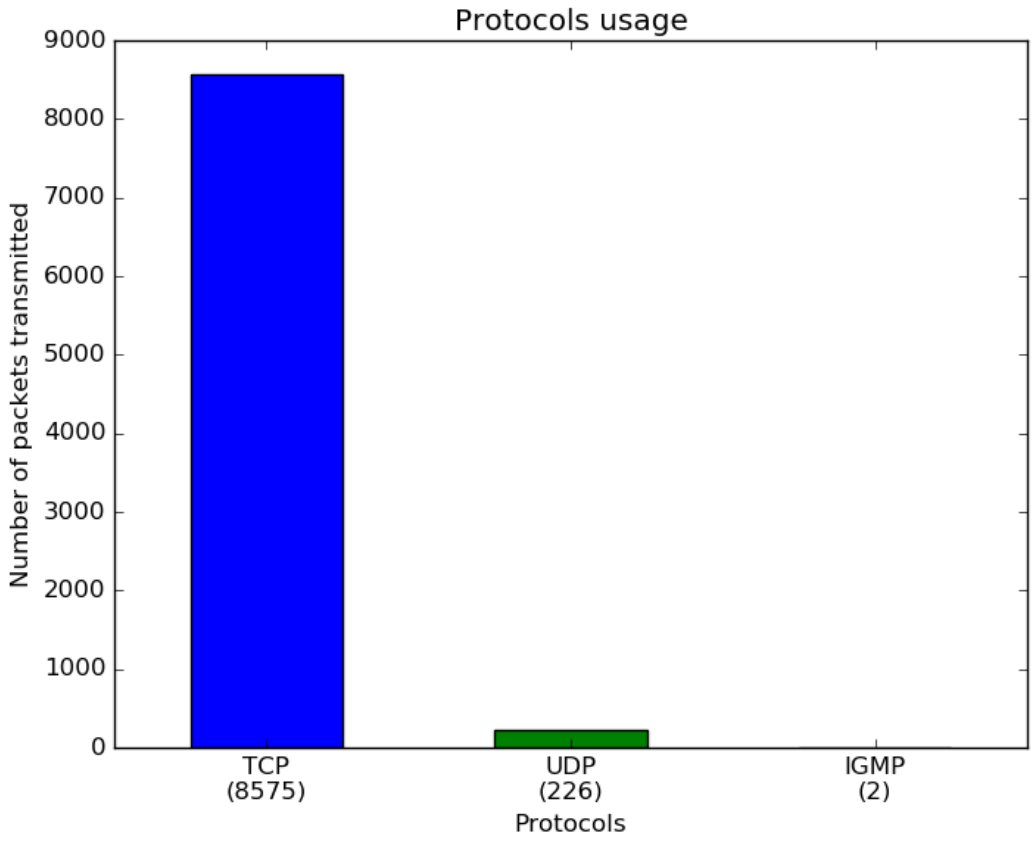
The open ports of the smart device were not analysed.

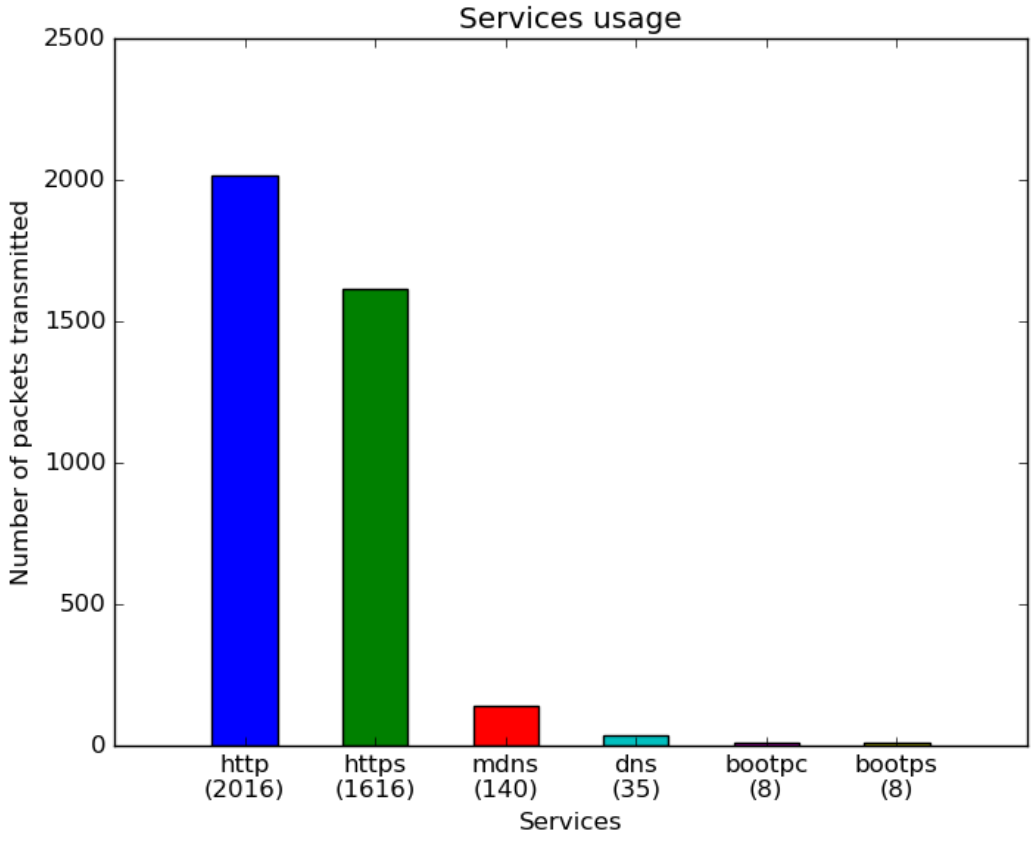
The following content only mention all the ports accessed by the services tested on the smart device besides ports 80(http) and 443(https). It doesn't explicitely prove the presence of backdoors, but by examining the domains and making some correlations with previous sections (like blocked domains), it may be possible to identify some suspicious access. These access may have been used to extract or inject data, which may lead to leaks.

During this session, the following ports(besides 80(http) and 443(https)) were used :

- **5228** used by **unknown** service and accessed by : **ee-in-f188.1e100.net**

On the histograms below, you can observe a protocol and service usage overview of your network traffic. Indeed, the histograms are showing respectively the number of packets sent per protocol and the number of packets sent per service. The goal of these histograms is to give you a possibility to observe anormal protocol or service usage in order to detect some (personal) information that could be transmitted in an anormal way. For example, if you observe on the services histogram a number of dns packets higher than the https or even the http one, you could maybe conclude that dns tunneling is used to transmit some information that may be personal.


Protocols usage
Number of packets transmitted
9000
8000
7000
6000
5000
4000
3000
2000
1000
0
TCP
(8575)
UDP
(226)
IGMP
(2)
Protocols


Services usage
Number of packets transmitted
2500
2000
1500
1000
500
0
http
(2016)
https
(1616)
mdns
(140)
dns
(35)
bootpc
(8)
bootps
(8)
Services

4. Weak authentication

4.1. Connections duration

58 connection(s) was/were **opened** or at least tried to be opened!

The **maximum TCP terminated connection duration** was **4 minute(s)**.

No terminated TCP connection lasted more than 30 minute(s).

There was/were **2 TCP connection(s) not terminated**!

The **maximum TCP non-terminated connection duration** was **1 minute(s)**.

No non-terminated TCP connection lasted more than 30 minute(s).

4.2. Certificate validation

Keep in mind that among the following self-signed certificates, some are false positives. The list of all the trusted CAs for smart devices not being available, some of the self-signed certificates given below may actually be trusted because they are root certificates issued by trusted CAs.

We found **1** self-signed certificate(s).
Here are the names of the files where these certificates were saved:

- **test_00001/cert_7_3** issued by **Go Daddy Class 2 Certification Authority**

In order to avoid overloading this report, we only reported one self-signed certificate per dinstinct issuer. You can find all the extracted certificates in the folder *RESULT/SAVE/Cert/*.

Automated report generated for MeetMe mobile application

UNIVERSITE CATHOLIQUE DE LOUVAIN

ECOLE POLYTECHNIQUE DE LOUVAIN

Leak sources analysis

Automated report

Supervisor: Dr. Ramin SADRE

by Mattieu DETAILLE
& Mohammad Muntasib Ali SYED

1. Lack of encryption

1.1. Unencrypted word(s) extracted

Here are the word(s) we found without any encryption security:

- **GT-I9505**
- **1993**
- **tracking**
- **description**
- **gender**
- **analytics**
- **token**
- **thesis message**
- **thesis**
- **san francisco**
- **message**

We found the word(s) **token**, **thesis message**, **thesis**, **message** in the following packet(s):

- 01-06-2016 15:26:19.244582; 192.168.42.15: 55435 --> 204.145.125.56: 80

  post /mobile/**message**s/new**message** http/1.1 x-auth**token**: 6a424c561f06e9
  b8fa431595f4500e70,4ac4b5b9ff5773e21040904cd1b48d8b,153396359 x-devic
  e: android,1af...2c856-f195-4373-abc6-e4f5190a163a,369:369 x-stats: {
  "methods":[{"key":"**message**thread","callback":0.002,"parse":0.023,"roun
  dtrip":0.332}],"memtotal":134217728,"memused":142840880}... ...ype: mu
  ltipart/form-data; boundary=ab155999-6e73-484a-9dd9-aa3d59e3a606 cont
  ent-length: 842 host: **message**s.meetme.com connection: keep-alive ac
  cept-encoding: gzip user-agent: okhttp/3.1.2 --ab155999-...999-6e7
  3-484a-9dd9-aa3d59e3a606 content-disposition: form-data; name="body"
  content-length: 16 **thesis message** 2 --ab155999-6e73-484a-9dd9-aa3
  d59e3a606 content-disposition: form-data; name="sourceevent" cont...

We found the word(s) **token**, **thesis message**, **thesis**, **message** in the following packet(s):

- 01-06-2016 15:26:46.677267; 192.168.42.15: 48063 --> 204.145.125.56: 80

  post /mobile/**message**s/new**message** http/1.1 x-auth**token**: 6a424c561f06e9
  b8fa431595f4500e70,4ac4b5b9ff5773e21040904cd1b48d8b,153396359 x-devic
  e: android,1af... ...ype: multipart/form-data; boundary=fae06f15-81b9-
  485f-ad47-5b56ee0e1ae8 content-length: 752 host: **message**s.meetme.com
  connection: keep-alive accept-encoding: gzip user-agent: okhttp/3.
  1.2 --fae06f15-...f15-81b9-485f-ad47-5b56ee0e1ae8 content-disposit
  ion: form-data; name="body" content-length: 16 **thesis message** 4 -
  -fae06f15-81b9-485f-ad47-5b56ee0e1ae8 content-disposition: form-data;
  name="sourceevent" cont...

We found the word(s) **gender**, **token**, **message** in the following packet(s):

- 01-06-2016 15:25:16.329003; 192.168.42.15: 43795 --> 204.145.125.42: 80

  get /mobile/search/meet/1?**gender**=&maxage;=&minage;=&includefriends;=&ison;
  line=&orderby;=&orientation;=&bodytype;=&education;=&ethnicity;=&ha; ...ude=
  50.6697268&longitude;=4.613926&pagesize;=30&locationstring;=&configuratio;
  nadslot=1 http/1.1 x-auth**token**: 6a424c561f06e9b8fa431595f4500e70,2e48
  eadbbd8327fcc7da8901cf0a2531,153396359 x-device: android,1af... x-co
  unts: 0 x-notificationtypes: boostchat,smilesent,friendaccept,newmatc
  h x-supportedfeatures: **message**stickers,stackednotifications:v4,tags,t
  wostepregistration,chatsuggestions,purchaserevamp,freetrial,r...

We found the word(s) **gender**, **token**, **message** in the following packet(s):

- 01-06-2016 15:25:19.664917; 192.168.42.15: 51501 --> 204.145.125.42: 80

  get /mobile/search/meet/2?**gender**=&maxage;=&minage;=&includefriends;=&ison;
  line=&orderby;=&orientation;=&bodytype;=&education;=&ethnicity;=&ha; ...ude=
  50.6697268&longitude;=4.613926&pagesize;=30&locationstring;=&configuratio;
  nadslot=1 http/1.1 x-auth**token**: 6a424c561f06e9b8fa431595f4500e70,2e48
  eadbbd8327fcc7da8901cf0a2531,153396359 x-device: android,1af... x-co
  unts: 0 x-notificationtypes: boostchat,smilesent,friendaccept,newmatc
  h x-supportedfeatures: **message**stickers,stackednotifications:v4,tags,t
  wostepregistration,chatsuggestions,purchaserevamp,freetrial,r...

We found the word(s) **thesis message**, **thesis**, **message** in the following packet(s):

- 01-06-2016 15:25:58.873825; 204.145.126.245: 1883 --> 192.168.42.15: 54719

  In this packet, the domain **stream.meetme.com** contacted your smart device.

  0■■■■/153396359/**message**s/new{"body":"**thesis message** 1","preview":"**thes
  is message** 1","sent_at":1464787558.7657,"received_at":1464787558.807,"
  sent_by":153394405,"header_id":"ba2c682e...

We found the word(s) **thesis message**, **thesis**, **message** in the following packet(s):

- 01-06-2016 15:26:34.687817; 204.145.126.245: 1883 --> 192.168.42.15: 54719

  In this packet, the domain **stream.meetme.com** contacted your smart device.

  0■■■■/153396359/**message**s/new{"body":"**thesis message** 3","preview":"**thes
  is message** 3","sent_at":1464787594.5706,"received_at":1464787594.621,"
  sent_by":153394405,"header_id":"b06302b7...

We found the word(s) **GT-I9505**, **tracking**, **gender** in the following packet(s):

- 01-06-2016 15:25:12.678272; 192.168.42.15: 40833 --> 37.252.170.255: 80

  In this packet, the domain **ib.adnxs.com** was contacted by your smart device.

  ...ype: application/json accept: application/json user-agent: dalvik
  /2.1.0 (linux; u; android 5.0.1; **gt-i9505** build/lrx22c) host: ib.adnx
  s.com connection: keep-alive accept-encoding: gzip content-length:
  6 ...:50}],"allow_smaller_sizes":false,"ad_types":["banner"],"prebid":
  true,"disable_psa":true}],"user":{"**gender**":0,"language":"en"},"device"
  :{"make":"samsung","model":"**gt-i9505**","useragent":"mozilla\/5.0 (linux

; android 5.0.1; **gt-i9505** build\/lrx22c; wv) applewebkit\/537.36 (khtm
l, like gecko) version\/4.0 chrome\/50.0.2661.86 mobile...":50.6697268
,"lng":4.6139261,"loc_age":217291,"loc_precision":20},"devtime":146478
7512640,"limit_ad_**tracking**":false,"device_id":{"aaid":"4f288309-8c6d-4
e81-9b75-cf9fcc79636f"},"os":"android"},"app":{"appid":"...

We found the word(s) **GT-I9505**, **tracking**, **gender** in the following packet(s):

- 01-06-2016 15:33:33.422557; 192.168.42.15: 59777 --> 37.252.171.17: 80

  In this packet, the domain **ib.adnxs.com** was contacted by your smart device.

  ...ype: application/json accept: application/json user-agent: dalvik
  /2.1.0 (linux; u; android 5.0.1; **gt-i9505** build/lrx22c) host: ib.adnx
  s.com connection: keep-alive accept-encoding: gzip content-length:
  6 ...:50}],"allow_smaller_sizes":false,"ad_types":["banner"],"prebid":
  true,"disable_psa":true}],"user":{"**gender**":0,"language":"en"},"device"
  :{"make":"samsung","model":"**gt-i9505**","useragent":"mozilla\/5.0 (linux
  ; android 5.0.1; **gt-i9505** build\/lrx22c; wv) applewebkit\/537.36 (khtm
  l, like gecko) version\/4.0 chrome\/50.0.2661.86 mobile...":50.6697268
  ,"lng":4.6139261,"loc_age":717946,"loc_precision":20},"devtime":146478
  8013295,"limit_ad_**tracking**":false,"device_id":{"aaid":"4f288309-8c6d-4
  e81-9b75-cf9fcc79636f"},"os":"android"},"app":{"appid":"...

We found the word(s) **gender**, **token** in the following packet(s):

- 01-06-2016 15:30:16.224117; 192.168.42.15: 37400 --> 204.145.125.37: 80

  In this packet, the domain **feed.meetme.com** was contacted by your smart device.

  get /mobile/chatter/0/nearme/?locationtype=country&agemin;=18&agemax;=22
  &**gender**=both&supportsfriendsuggestions;=1&includelocationoptions;=1&conf;
  igurationadslot=1 http/1.1 x-auth**token**: 6a424c561f06e9b8fa431595f4500
  e70,20c012b27a2df60ab8b3628f2de66d16,153396359 x-device: android,1af.
  ..

We found the word(s) **GT-I9505**, **analytics** in the following packet(s):

- 01-06-2016 15:30:22.020465; 192.168.42.15: 48435 --> 52.4.231.55: 80

  In this packet, the domain **s.update.openx.com** was contacted by your smart device.

  ...413654&oz;_tc=a0lyz93d4wta5ghindvvc0qkd7aljorl&oz;_url=http%3a%2f%2fs
  .update.openx.com%2f2%2f413654%2f**analytics**.js%3fsi%3d537212075%26amp%3
  bti%3d980e2b8e-31a9-4349-bd53-237e92bb66f1%26amp%3bpc%3d538075749%26am
  p% content-length: 3811 origin: http://ads.mopub.com user-agent: moz
  illa/5.0 (linux; android 5.0.1; **gt-i9505** build/lrx22c; wv) applewebkit
  /537.36 (khtml, like gecko) version/4.0 chrome/50.0.2661.86 mobile saf
  ...

We found the word(s) **GT-I9505**, **analytics** in the following packet(s):

- 01-06-2016 15:30:22.877754; 192.168.42.15: 48435 --> 52.4.231.55: 80

  In this packet, the domain **s.update.openx.com** was contacted by your smart device.

...413654&oz;_tc=a0lyz93d4wta5ghindvvc0qkd7aljorl&oz;_url=http%3a%2f%2fs
.update.openx.com%2f2%2f413654%2f**analytics**.js%3fsi%3d537212075%26amp%3
bti%3d980e2b8e-31a9-4349-bd53-237e92bb66f1%26amp%3bpc%3d538075749%26am
p%e content-length: 66 origin: http://ads.mopub.com user-agent: moz
illa/5.0 (linux; android 5.0.1; **gt-i9505** build/lrx22c; wv) applewebkit
/537.36 (khtml, like gecko) version/4.0 chrome/50.0.2661.86 mobile saf
...

We found the word(s) **GT-I9505, gender** in the following packet(s):

- 01-06-2016 15:32:05.270545; 192.44.68.5: 80 --> 192.168.42.15: 50115

  In this packet, the domain **ads.mopub.com** contacted your smart device.

  ....com/m/aclk?appid=&cid;=f45fc6477e5a45af803fe39edbc25fda&city;=&ckv;=2
  &country;_code=be&cppck;=b2383&dev;=**gt-i9505**&exclude;_adgroups=458585cc35d
  c4bce90111ab05aba5081&id;=20df0909e2aa4715aa65674ef1b8e575&is;_mraid=0&o;
  s ... x-failurl: http://ads.mopub.com/m/ad?v=6&id;=20df0909e2aa4715aa65
  674ef1b8e575&nv;=4.5.1&dn;=samsung%2c**gt-i9505**%2cjfltexx&bundle;=com.myyea
  rbook.m&q;=dev_mfr%3asamsung%2cparental_state%3anone%2cm_**gender**%3am%2c e
  ducation%3anone%2cdev_brand%3asamsung%2cdev_model%3a**gt-i9505**%2crelatio
  nship_status%3anone%2cage%3a22%2cbuild_type%3arelease%2cm_age%3a22%2cr
  eligion%3anone%2cint...erested_in%3awomen%2capp_version%3a369%2cdev_ty
  pe%3ajflte%2cethnicity%3anone%2c**gender**%3am≪=50.6697268%2c4.613926≪
  a=20&llf;=628627&z;=%2b0200&o;=p&w;=1080&h;=1920≻_a=3.0&mcc;=206&mnc;=1 0&..
  .

We found the word(s) **GT-I9505, gender** in the following packet(s):

- 01-06-2016 15:33:31.569923; 192.44.68.5: 80 --> 192.168.42.15: 41843

  In this packet, the domain **ads.mopub.com** contacted your smart device.

  ....com/m/aclk?appid=&cid;=601d7bb5c7aa4fad8335e7614ecf2e0d&city;=&ckv;=2
  &country;_code=be&cppck;=e74eb&dev;=**gt-i9505**&exclude;_adgroups=458585cc35d
  c4bce90111ab05aba5081%2c7a2b8ac273e74b398a9f87bab374372b&id;=20df0909e2
  a ... x-failurl: http://ads.mopub.com/m/ad?v=6&id;=20df0909e2aa4715aa65
  674ef1b8e575&nv;=4.5.1&dn;=samsung%2c**gt-i9505**%2cjfltexx&bundle;=com.myyea
  rbook.m&q;=dev_mfr%3asamsung%2cparental_state%3anone%2cm_**gender**%3am%2c e
  ducation%3anone%2cdev_brand%3asamsung%2cdev_model%3a**gt-i9505**%2crelatio
  nship_status%3anone%2cage%3a22%2cbuild_type%3arelease%2cm_age%3a22%2cr
  eligion%3anone%2cint...erested_in%3awomen%2capp_version%3a369%2cdev_ty
  pe%3ajflte%2cethnicity%3anone%2c**gender**%3am≪=50.6697268%2c4.613926≪
  a=20&llf;=714570&z;=%2b0200&o;=p&w;=1080&h;=1920≻_a=3.0&mcc;=206&mnc;=1 0&..
  .

We found the word(s) **GT-I9505, tracking** in the following packet(s):

- 01-06-2016 15:27:14.732553; 192.168.42.15: 48146 --> 88.198.114.198: 80

  In this packet, the domain **imp-mdsp.avazutracking.net** was contacted by your smart

  device.

  get /**tracking**/impression?bid_id=54882585513182628&ids;=hnzyxmx43nzcwox4
  2nteznzv-mtaznh4tmx4xfjf-mh4wfkjffmfuzhjvaw ...-mh4wfj&bid;_time=146478

7634&chk;=25e07dee0b5f8ee294a5bc9f29ad171c&ext;= http/1.1 host: imp-mds p.avazu**tracking**.net connection: keep-alive accept: image/webp,image/ *,*/*;q=0.8 user-agent: mozilla/5.0 (linux; ...android 5.0.1; **gt-i950 5** build/lrx22c; wv) applewebkit/537.36 (khtml, like gecko) version/4.0 chrome/50.0.2661.86 mobile saf...

We found the word(s) **token, message** in the following packet(s):

- 01-06-2016 15:27:21.527761; 192.168.42.15: 48586 --> 204.145.125.32: 80

  In this packet, the domain **api.meetme.com** was contacted by your smart device.

  get /mobile/counts http/1.1 x-auth**token**: 6a424c561f06e9b8fa431595f450 0e70,0f72a0996176ff39a218b743c8e07b86,153396359 x-device: android,1af 2c856-f195-4373-abc6-e4f5190a163a,369:369 x-stats: {"methods":[{"key" :"add**message**photo","callback":0.005,"parse":0.03,"roundtrip":1.03}],"m emtotal":134217728,"memused":165470756} x...-notificationtypes: boost chat,smilesent,friendaccept,newmatch x-supportedfeatures: **message**stic kers,stackednotifications:v4,tags,twostepregistration,chatsuggestions, purchaserevamp,freetrial,r...

We found the word(s) **token, message** in the following packet(s):

- 01-06-2016 15:24:45.109448; 192.168.42.15: 58360 --> 204.145.125.32: 80

  In this packet, the domain **api.meetme.com** was contacted by your smart device.

  get /mobile/counts http/1.1 x-auth**token**: 6a424c561f06e9b8fa431595f450 0e70,6a3d955b49f4b81773414f3e0bc9ca57,153396359 x-device: android,1af ed":90254073} x-notificationtypes: boostchat,smilesent,friendaccept,n ewmatch x-supportedfeatures: **message**stickers,stackednotifications:v4, tags,twostepregistration,chatsuggestions,purchaserevamp,freetrial,r...

We found the word(s) **message** in the following packet(s):

- 01-06-2016 15:25:40.586171; 204.145.126.245: 1883 --> 192.168.42.15: 54719

  In this packet, the domain **stream.meetme.com** contacted your smart device.

  0■■■!/153396359/**message**s/thread_status{"status":"read","set_at":146478 7540.5051,"thread_id":"00000000-0924-a487-0000-000009...

We found the word(s) **message** in the following packet(s):

- 01-06-2016 15:26:09.328351; 192.168.42.15: 54719 --> 204.145.126.245: 1883

  In this packet, the domain **stream.meetme.com** was contacted by your smart device.

  2b■+/public/153394405/153396359/**message**s/status■■{"status":"typing"}.. .

We found the word(s) **san francisco** in the following packet(s):

- 01-06-2016 15:30:33.593493; 192.44.68.6: 443 --> 192.168.42.15: 36447

In this packet, the domain **ads.mopub.com** contacted your smart device.

...sha2 high assurance server ca0 ■ 140716000000z■ 170720120000z0`1 0
■■u■■■■us1 0 ■■u■■■■ca1■0■■■u■■■ **san francisco**1■0■■■u■ ■ twitter, inc.
1■0■■■u■■ *.mopub.com0■■"0 ■ *■h■■ ■■■■■■■■■■0■■ ■■■■■■■■
■(■■*■0$■■■
m[■om■...

We found the word(s) **1993** in the following packet(s):

- 01-06-2016 15:29:59.998161; 173.241.240.143: 80 --> 192.168.42.15: 52636

  In this packet, the domain **u.openx.net** contacted your smart device.

  http/1.1 302 moved temporarily set-cookie: i=520**1993**9-5cf0-04da-9fb7-
  20bfba20de39|1464787799; version=1; expires=thu, 01-jun-2017 13:29:59
  gmt; max-age=...

We found the word(s) **GT-I9505** in the following packet(s):

- 01-06-2016 15:31:16.119788; 192.168.42.15: 33411 --> 173.241.240.220: 80

  In this packet, the domain **meetme-d.openx.net** was contacted by your smart device.

  ...n: keep-alive accept: image/webp,image/*,*/*;q=0.8 user-agent: mo
  zilla/5.0 (linux; android 5.0.1; **gt-i9505** build/lrx22c; wv) applewebki
  t/537.36 (khtml, like gecko) version/4.0 chrome/50.0.2661.86 mobile sa
  f...

We found the word(s) **GT-I9505** in the following packet(s):

- 01-06-2016 15:28:35.113049; 192.168.42.15: 34031 --> 192.44.68.5: 80

  In this packet, the domain **ads.mopub.com** was contacted by your smart device.

  ...tp/1.1 host: ads.mopub.com connection: keep-alive user-agent: mo
  zilla/5.0 (linux; android 5.0.1; **gt-i9505** build/lrx22c; wv) applewebki
  t/537.36 (khtml, like gecko) version/4.0 chrome/50.0.2661.86 mobile sa
  f...

We found the word(s) **tracking** in the following packet(s):

- 01-06-2016 15:27:14.591913; 173.241.240.220: 80 --> 192.168.42.15: 33367

  In this packet, the domain **meetme-d.openx.net** contacted your smart device.

  nge.click.php?h=5d43447cd53688c4c4ee8fc8158fc960\" target=\"_blank\"][
  img src=\"http://cdn.avazu**tracking**.net/images/201601/105/dc1d16b9a2971
  3831ac34ba27aab7ecc_320x50.gif\"/][/a] [img src=\"http://imp-mdsp.avaz
  u**tracking**.net/**tracking**/impression?bid_id=5488258513182628&ids;=hnzyxmx
  43nzcwox42nteznzv-mtaznh4tmx4xfjf-mh4wfkjffmfuzhjvaw...

We found the word(s) **tracking** in the following packet(s):

- 01-06-2016 15:27:14.649110; 192.168.42.15: 37302 --> 8.8.8.8: 53

  b ■■■■■■■■■■■imp-mdsp avazu**tracking**■net■■■■■...

We found the word(s) **token** in the following packet(s):

- 01-06-2016 15:31:22.044274; 192.168.42.15: 50171 --> 204.145.125.65: 80

  In this packet, the domain **profile.meetme.com** was contacted by your smart device.

  get /mobile/membersettings/ http/1.1 x-auth**token**: 6a424c561f06e9b8fa4 31595f4500e70,b77a5ce4bdd81619492a65243415cedc,153396359 x-device: an droid,1af...

We found the word(s) **token** in the following packet(s):

- 01-06-2016 15:31:14.055716; 192.168.42.15: 50456 --> 204.145.125.42: 80

  get /mobile/friends/v2/0/?configurationadslot=1&includeusernames;=1 htt p/1.1 x-auth**token**: 6a424c561f06e9b8fa431595f4500e70,b77a5ce4bdd816194 92a65243415cedc,153396359 x-device: android,1af...

We found the word(s) **description** in the following packet(s):

- 01-06-2016 15:28:12.708659; 93.184.221.200: 80 --> 192.168.42.15: 59119

  In this packet, the domain **cdnenestatic.ec.azureedge.net** contacted your smart device.

  ...014/01/13-19:44:00 "] [rdf:rdf xmlns:rdf="http://www.w3.org/ 1999/02/22-rdf-syntax-ns#"] [rdf:**description** rdf:about="" xmlns:xmpmm= "http://ns.adobe.com/xap/1.0/mm/" xmlns:stref="http://ns.adobe.com/xap /1.0c81a3d5910f1" stref:documentid="adobe:docid:photoshop:63c18a46-57c f-1179-8ea8-cd06cff65391"/] [/rdf:**description**] [/rdf:rdf] [/x:xmpmeta] [?xpacket end="r"?]■■■&adobe;■d■■■■■■■■■■■■ ■■5■■■■■■■■■ ■■/a■■■■■■■■■■■ ■■■■■...

We found the word(s) **description** in the following packet(s):

- 01-06-2016 15:24:52.589555; 204.145.125.81: 80 --> 192.168.42.15: 52072

  In this packet, the domain **photoserver.meetme.com** contacted your smart device.

  ...013/10/29-11:47:16 "] [rdf:rdf xmlns:rdf="http://www.w3.org/ 1999/02/22-rdf-syntax-ns#"] [rdf:**description** rdf:about="" xmlns:xmpmm= "http://ns.adobe.com/xap/1.0/mm/" xmlns:stref="http://ns.adobe.com/xap /1.0d:a9f82641-d930-42ec-9fe2-133aa1fdab8e" stref:documentid="67c548bb e53a0663a88dde92889a7152"/] [/rdf:**description**] [/rdf:rdf] [/x:xmpmeta] [?xpacket end="r"?]c ■■■■2lidatx■l■w■e■u&■;s■■■■■n■v■■ g■ ■■■■■■■4|■f &■ jo...

We found the word(s) **analytics** in the following packet(s):

- 01-06-2016 15:45:17.601894; 74.125.136.113: 443 --> 192.168.42.17: 47214

In this packet, the domain **i.ytimg.com** contacted your smart device.

...■■n■■u ■■■■e0■■a■ *.google.com■ *.android.com■■*.appengine.google.com■■*.cloud.google.com■■*.google-**analytics**.com■ *.google.ca■ *.google.cl■■*.google.co.in■■*.google.co.jp■■*.google.co.uk■■*.google.com.ar■■*.g■*.youtubeeducation.com■ *.ytimg.com■■android.clients.google.com■ android.com■■g.co■■goo.gl■■google-**analytics**.com■ google.c

We found the word(s) **analytics** in the following packet(s):

- 01-06-2016 15:35:11.645311; 192.168.42.15: 3434 --> 8.8.8.8: 53

  ~■■■■■■■■■■■ **analytics**■mopub■com■■■■■...

1.2. Unencrypted file(s) extracted

Some unencrypted files were extracted from your network traffic. Have a look in the *RESULS/FILES_EXTRACTED* directory!

2. Weak encryption

The security protocol SSL/TLS was used to encrypt part of your traffic, which is already a good start! 27% of your IP network traffic was encrypted using the SSL/TLS security protocol.

No problems detected for the hash functions, block cipher algorithms or stream cipher algorithms used for encrypting your network traffic!

Here are the cryptographic algorithms used for securing a part of your network traffic: CBC, AES, RSA, SHA, GCM, ECDHE, SHA256, ECDSA.

3. Covert channels

3.1. Adblock

Here are all the domains blocked by the adblock module : **analytics.localytics.com, beap-bc.yahoo.com, bid.g.doubleclick.net**.

In one of the packets exchange, the following domain(s) was(were) blocked : **analytics.localytics.com**.
Here are some known alternative name(s) of this(these) domain(s) : **ec2-54-225-151-203.compute-1.amazonaws.com, queuerlb-599065538.us-east-1.elb.amazonaws.com**.
Here are the known ip adresses of this(these) domain(s) : **54.225.245.143, 54.235.171.231, 23.21.253.224, 54.204.12.60, 54.235.87.112, 54.225.151.203, 54.235.189.180, 54.235.148.243**

In one of the packets exchange, the following domain(s) was(were) blocked : **beap-bc.yahoo.com**.
Here are some known alternative name(s) of this(these) domain(s) : **geoycpi-uno-deluxe.gycpi.b.yahoodns.net, r2.ycpi.vip.ams.yahoo.net**.
Here are the known ip adresses of this(these) domain(s) : **66.196.66.212, 66.196.66.213**

In one of the packets exchange, the following domain(s) was(were) blocked : **bid.g.doubleclick.net**.

Here are some known alternative name(s) of this(these) domain(s) : **ea-in-f157.1e100.net, ads-bid.l.doubleclick.net**.
Here are the known ip adresses of this(these) domain(s) : **74.125.136.157, 74.125.136.156, 74.125.136.155, 74.125.136.154**

In one of the packets exchange, the following domain(s) was(were) blocked : **bid.g.doubleclick.net**.
Here are some known alternative name(s) of this(these) domain(s) : **ea-in-f156.1e100.net, ads-bid.l.doubleclick.net**.
Here are the known ip adresses of this(these) domain(s) : **74.125.136.157, 74.125.136.156, 74.125.136.155, 74.125.136.154**

In one of the packets exchange, the following domain(s) was(were) blocked : **analytics.localytics.com**.
Here are some known alternative name(s) of this(these) domain(s) : **ec2-54-225-246-125.compute-1.amazonaws.com, queuerlb-599065538.us-east-1.elb.amazonaws.com**.
Here are the known ip adresses of this(these) domain(s) : **23.23.160.249, 54.225.246.125, 54.225.147.8, 50.17.195.105, 107.20.243.255, 23.23.102.29, 50.19.119.163, 54.243.101.215**

In one of the packets exchange, the following domain(s) was(were) blocked : **analytics.localytics.com**.
Here are some known alternative name(s) of this(these) domain(s) : **ec2-50-19-119-163.compute-1.amazonaws.com, queuerlb-599065538.us-east-1.elb.amazonaws.com**.
Here are the known ip adresses of this(these) domain(s) : **23.23.160.249, 50.19.119.163, 23.21.229.203, 50.17.195.105, 107.20.243.255, 23.23.102.29, 23.21.194.29, 54.243.101.215**

3.2. DNSBL

Here are all the domains of the ips blocked by the DNSBL module : **youtube-ui.l.google.com, www.youtube.com, 244.253-4-62.akamai.com, 96.253-4-62.akamai.com, www.google.com, ams16s21-in-f198.1e100.net, s0.2mdn.net, s0-2mdn-net.l.google.com, ams15s22-in-f14.1e100.net, ams16s22-in-f229.1e100.net, ams16s21-in-f2.1e100.net, googleads.g.doubleclick.net, pagead46.l.doubleclick.net, imp-mdsp.avazutracking.net, static.88-198-114-198.clients.your-server.de, ams16s22-in-f238.1e100.net, 224.253-4-62.akamai.com, ams15s21-in-f131.1e100.net, ams15s21-in-f2.1e100.net, android.clients.google.com, fra15s11-in-f14.1e100.net, android.l.google.com, events-endpoint-c-394794954.us-east-1.elb.amazonaws.com, e.crashlytics.com, ec2-54-243-174-126.compute-1.amazonaws.com, ams16s21-in-f194.1e100.net, ams16s21-in-f6.1e100.net, ec2-174-129-0-175.compute-1.amazonaws.com, clients3.google.com, ams16s22-in-f14.1e100.net, clients.l.google.com, pagead2.googlesyndication.com, ams16s22-in-f2.1e100.net, ams15s22-in-f174.1e100.net, ad.doubleclick.net, dart.l.doubleclick.net, ams16s22-in-f226.1e100.net, ams16s22-in-f5.1e100.net, ams15s21-in-f130.1e100.net, ams15s21-in-f3.1e100.net**.

In one of the packets exchange, DNSBL's blocked the following ip(s) :

- **62.4.253.251** by the blacklist : **dul.dnsbl.sorbs.net**
- **62.4.253.237** by the blacklist : **dul.dnsbl.sorbs.net**
- **62.4.253.244** by the blacklist : **dul.dnsbl.sorbs.net**

- **62.4.253.245** by the blacklist : **dul.dnsbl.sorbs.net**
- **62.4.253.217** by the blacklist : **dul.dnsbl.sorbs.net**
- **62.4.253.216** by the blacklist : **dul.dnsbl.sorbs.net**
- **62.4.253.210** by the blacklist : **dul.dnsbl.sorbs.net**
- **62.4.253.224** by the blacklist : **dul.dnsbl.sorbs.net**
- **62.4.253.223** by the blacklist : **dul.dnsbl.sorbs.net**
- **62.4.253.231** by the blacklist : **dul.dnsbl.sorbs.net**
- **62.4.253.230** by the blacklist : **dul.dnsbl.sorbs.net**
- **62.4.253.238** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) : **youtube-ui.l.google.com, www.youtube.com, 244.253-4-62.akamai.com**.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **62.4.253.123** by the blacklist : **dul.dnsbl.sorbs.net**
- **62.4.253.89** by the blacklist : **dul.dnsbl.sorbs.net**
- **62.4.253.109** by the blacklist : **dul.dnsbl.sorbs.net**
- **62.4.253.95** by the blacklist : **dul.dnsbl.sorbs.net**
- **62.4.253.96** by the blacklist : **dul.dnsbl.sorbs.net**
- **62.4.253.82** by the blacklist : **dul.dnsbl.sorbs.net**
- **62.4.253.116** by the blacklist : **dul.dnsbl.sorbs.net**
- **62.4.253.117** by the blacklist : **dul.dnsbl.sorbs.net**
- **62.4.253.103** by the blacklist : **dul.dnsbl.sorbs.net**
- **62.4.253.102** by the blacklist : **dul.dnsbl.sorbs.net**
- **62.4.253.110** by the blacklist : **dul.dnsbl.sorbs.net**
- **62.4.253.88** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) : **96.253-4-62.akamai.com, www.google.com**.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.198** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) : **ams16s21-in-f198.1e100.net, s0.2mdn.net, s0-2mdn-net.l.google.com**.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.174** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) : **ams15s22-in-f14.1e100.net**.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.229** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams16s22-in-f229.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.194** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams16s21-in-f2.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.194** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
googleads.g.doubleclick.net, pagead46.l.doubleclick.net, ams16s21-in-f2.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **88.198.114.198** by the blacklist : **b.barracudacentral.org**

Here are some known domain name(s) of this(these) ip(s) :
imp-mdsp.avazutracking.net, static.88-198-114-198.clients.your-server.de.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.198** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams16s21-in-f198.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.238** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams16s22-in-f238.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.174** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams15s22-in-f14.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **62.4.253.224** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
224.253-4-62.akamai.com.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.131** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams15s21-in-f131.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.130** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams15s21-in-f2.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :

- **172.217.16.174** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
android.clients.google.com, fra15s11-in-f14.1e100.net, android.l.google.com.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **23.21.118.91** by the blacklist : **zen.spamhaus.org**

Here are some known domain name(s) of this(these) ip(s) :
events-endpoint-c-394794954.us-east-1.elb.amazonaws.com, e.crashlytics.com, ec2-54-243-174-126.compute-1.amazonaws.com.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **62.4.253.244** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
244.253-4-62.akamai.com.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.198** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams16s21-in-f198.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.194** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams16s21-in-f194.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **62.4.253.96** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) : **96.253-4-62.akamai.com**.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.174** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams15s22-in-f14.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.229** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams16s22-in-f229.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.198** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams16s21-in-f6.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.194** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams16s21-in-f2.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :

- **23.21.118.91** by the blacklist : **zen.spamhaus.org**

Here are some known domain name(s) of this(these) ip(s) : **events-endpoint-c-394794954.us-east-1.elb.amazonaws.com, ec2-174-129-0-175.compute-1.amazonaws.com, e.crashlytics.com**.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.238** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) : **clients3.google.com, ams16s22-in-f14.1e100.net, clients.l.google.com**.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.226** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) : **pagead2.googlesyndication.com, ams16s22-in-f2.1e100.net, pagead46.l.doubleclick.net**.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.194** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) : **googleads.g.doubleclick.net, pagead46.l.doubleclick.net, ams16s21-in-f194.1e100.net**.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.198** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) : **ams16s21-in-f6.1e100.net**.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **172.217.16.174** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) : **fra15s11-in-f14.1e100.net**.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **88.198.114.198** by the blacklist : **b.barracudacentral.org**

Here are some known domain name(s) of this(these) ip(s) : **static.88-198-114-198.clients.your-server.de**.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.174** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) : **ams15s22-in-f174.1e100.net**.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.238** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) : **ams16s22-in-f14.1e100.net**.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.198** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams16s21-in-f198.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.194** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams16s21-in-f194.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.174** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams15s22-in-f174.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **62.4.253.96** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) : **96.253-4-62.akamai.com**.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.198** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams16s21-in-f6.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.238** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams16s22-in-f238.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.198** by the blacklist : **dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams16s21-in-f6.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.198** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams16s21-in-f6.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.198** by the blacklist : **dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) : **ad.doubleclick.net, dart.l.doubleclick.net, ams16s21-in-f6.1e100.net**.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.194** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
pagead2.googlesyndication.com, pagead46.l.doubleclick.net, ams16s21-in-f2.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.226** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams16s22-in-f226.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.198** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams16s21-in-f198.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.226** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams16s22-in-f226.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.194** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams16s21-in-f194.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.198** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams16s21-in-f198.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.198** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams16s21-in-f198.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.229** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams16s22-in-f5.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.130** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams15s21-in-f130.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **216.58.212.131** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
ams15s21-in-f3.1e100.net.

In one of the packets exchange, DNSBL's blocked the following ip(s) :
- **62.4.253.244** by the blacklist : **dul.dnsbl.sorbs.net**

Here are some known domain name(s) of this(these) ip(s) :
244.253-4-62.akamai.com.

3.3. SafeBrowsing

The SafeBrowsing module didn't find any match.

3.4. SafeLookup

The SafeLookup module didn't find any match.

3.5. Potential backdoors

The open ports of the smart device were not analysed.

The following content only mention all the ports accessed by the services tested on the smart device besides ports 80(http) and 443(https). It doesn't explicitely prove the presence of backdoors, but by examining the domains and making some correlations with previous sections (like blocked domains), it may be possible to identify some suspicious access. These access may have been used to extract or inject data, which may lead to leaks.

During this session, the following ports(besides 80(http) and 443(https)) were used :

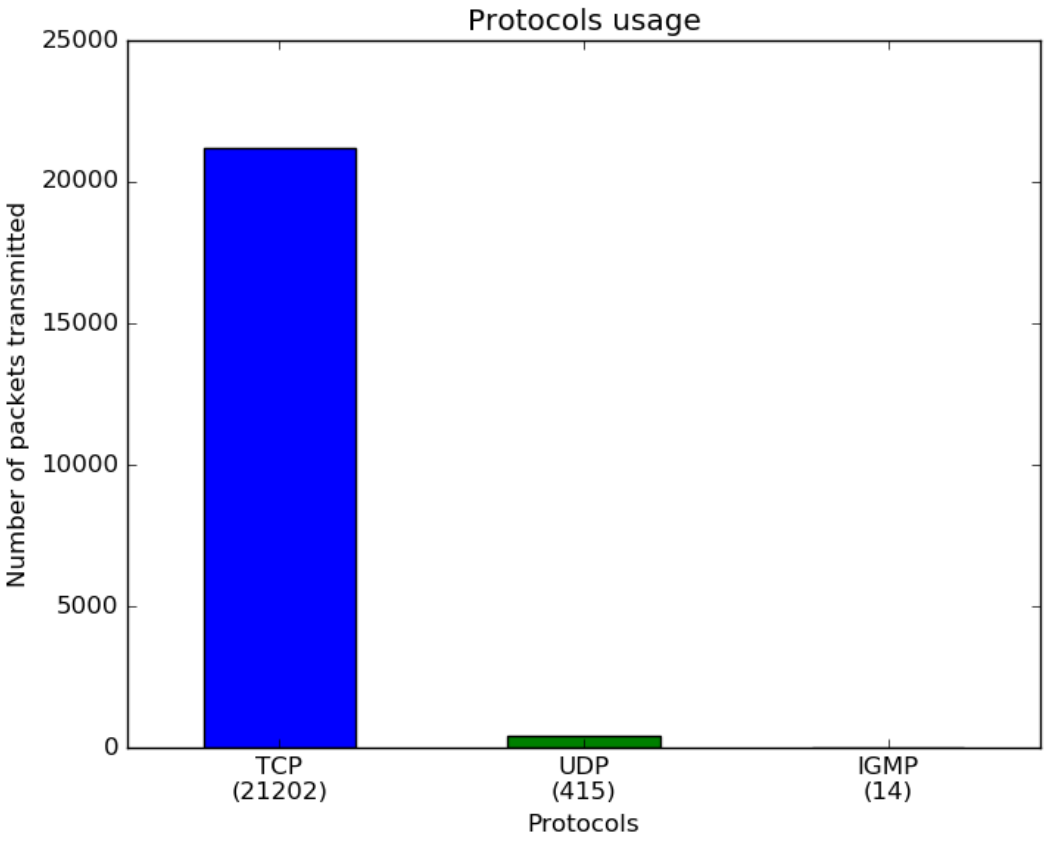
- **123** used by **ntp** service and accessed by : **2.android.pool.ntp.org,**

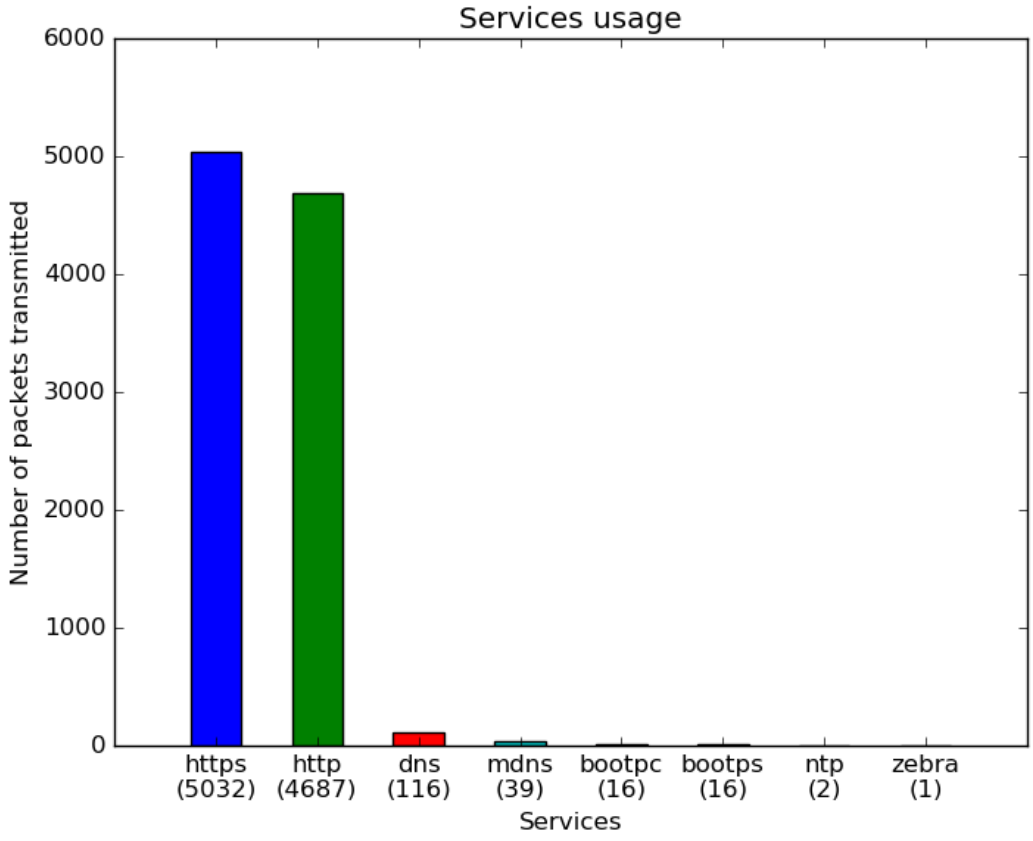
  hades.boxed-it.com

- **1883** used by **unknown** service and accessed by : **stream.meetme.com**

- **5228** used by **unknown** service and accessed by : **ea-in-f188.1e100.net**

On the histograms below, you can observe a protocol and service usage overview of your network traffic. Indeed, the histograms are showing respectively the number of packets sent per protocol and the number of packets sent per service. The goal of these histograms is to give you a possibility to observe anormal protocol or service usage in order to detect some (personal) information that could be transmitted in an anormal way. For example, if you observe on the services histogram a number of dns packets higher than the https or even the http one, you could maybe conclude that dns tunneling is used to transmit some information that may be personal.


Protocols usage
Number of packets transmitted
25000
20000
15000
10000
5000
0
TCP
(21202)
UDP
(415)
IGMP
(14)
Protocols


Services usage
Number of packets transmitted
6000
5000
4000
3000
2000
1000
0
https
(5032)
http
(4687)
dns
(116)
mdns
(39)
bootpc
(16)
bootps
(16)
ntp
(2)
zebra
(1)
Services

4. Weak authentication

4.1. Connections duration

461 connection(s) was/were **opened** or at least tried to be opened!

The **maximum TCP terminated connection duration** was **1 minute(s)**.

No terminated TCP connection lasted more than 30 minute(s).

There was/were **16 TCP connection(s) not terminated**!

The **maximum TCP non-terminated connection duration** was **37 minute(s)**.

Here are the TCP non-terminated connections that lasted more than 30 minute(s):

- The non-terminated TCP connection 69.172.216.55:80 --> 192.168.42.15:44623 lasted 31 minute(s).

  In this packet, the domain **pixel.adsafeprotected.com** contacted your smart device.

- The non-terminated TCP connection 95.172.94.45:80 --> 192.168.42.15:35002 lasted 37 minute(s).
- The non-terminated TCP connection 95.172.94.37:80 --> 192.168.42.15:36397 lasted 36 minute(s).

  In this packet, the domain **map-pb.quantserve.com.akadns.net** contacted your smart device.

- The non-terminated TCP connection 95.172.94.37:80 --> 192.168.42.15:57091 lasted 33 minute(s).

  In this packet, the domain **map-pb.quantserve.com.akadns.net** contacted your smart device.

4.2. Certificate validation

We found **4** expired certificate(s).
Here are the names of the files where these certificates were saved:

- **test_00001/cert_11_0** issued by **Symantec Class 3 Secure Server CA - G4**, expired since **20160603235959Z**
- **test_00004/cert_3_0** issued by **Symantec Class 3 Secure Server CA - G4**, expired since **20160603235959Z**
- **test_00011/cert_4_0** issued by **Symantec Class 3 Secure Server CA - G4**, expired since **20160603235959Z**

- **test_00019/cert_1_0** issued by **Symantec Class 3 Secure Server CA - G4**,

  expired since **20160603235959Z**

Keep in mind that among the following self-signed certificates, some are false positives. The list of all the trusted CAs for smart devices not being available, some of the self-signed certificates given below may actually be trusted because they are root certificates issued by trusted CAs.

We found **9** self-signed certificate(s).
Here are the names of the files where these certificates were saved:

- **test_00001/cert_0_3** issued by **AddTrust External CA Root**
- **test_00002/cert_3_2** issued by **DigiCert Global Root CA**

In order to avoid overloading this report, we only reported one self-signed certificate per dinstinct issuer. You can find all the extracted certificates in the folder *RESULT/SAVE/Cert/*.