Privacy Detective

Sniffing Out Your Data Leaks for Android

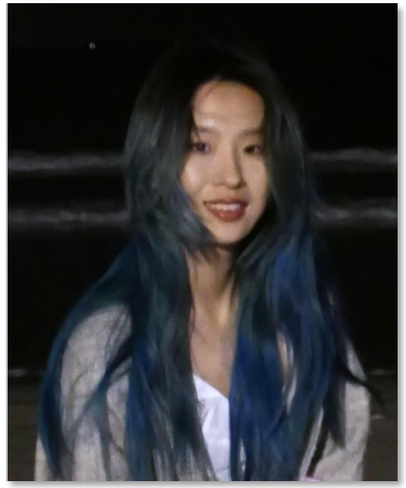
—— Abbie & Meggie

About us

Abbie Zhou,

A security researcher and engineer, specializes in reverse, development of security features and security tools.

He **led the development of Privacy Detective**. And he has a long-standing interest in mobile security and mobile privacy related issues.



Meggie He,

A security researcher at OPPO, specializes in security certification, security feature research, and security tool development.

She leads in certification projects, leads the writing of OPPO's IoT security specifications, and development of this tool.

Background

Companies Challenges

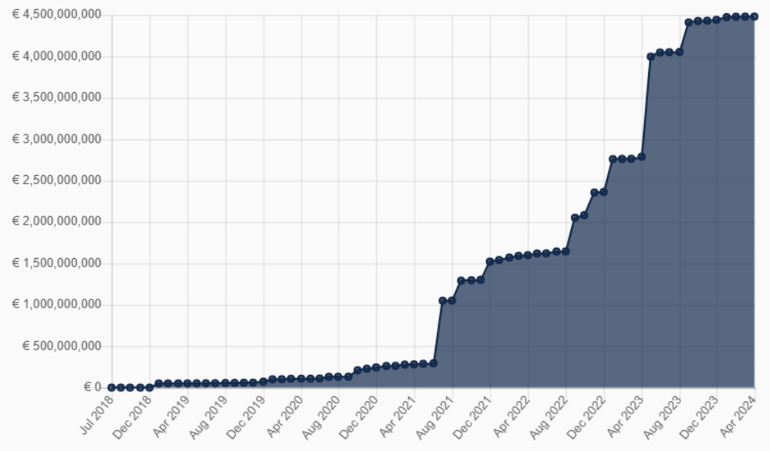
Europe

United States

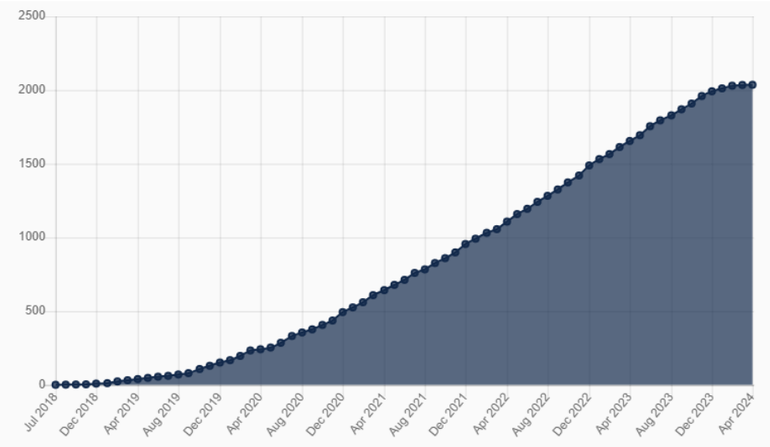
Source: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4426146

Companies Challenges

- Course of overall sum of fines (cumulative):



- Course of overall number of fines (cumulative):



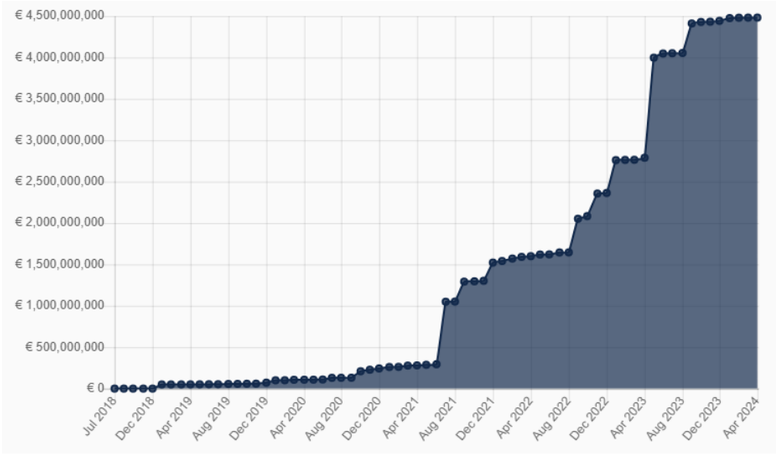
- The maximum fine for a GDPR violation is €20 million, or 4% of a company's global annual revenue, whichever is higher.

- The sum of fines has been growing dramatically, while the number is stably increased.

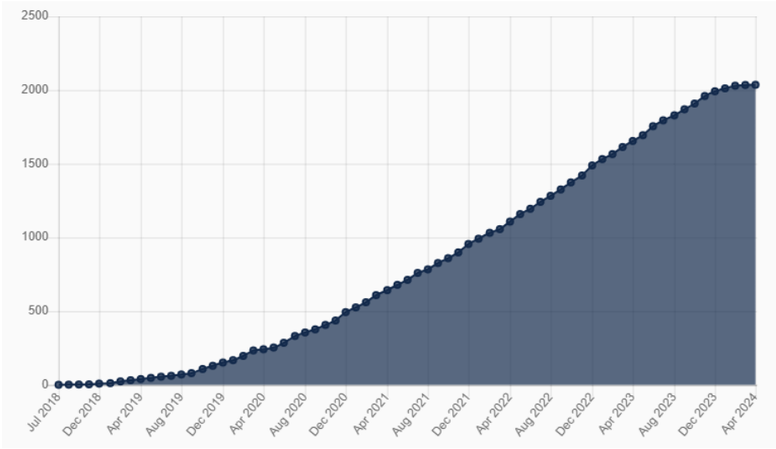
Source： https://www.enforcementtracker.com/?insights

Companies Challenges

- Course of overall sum of fines (cumulative):

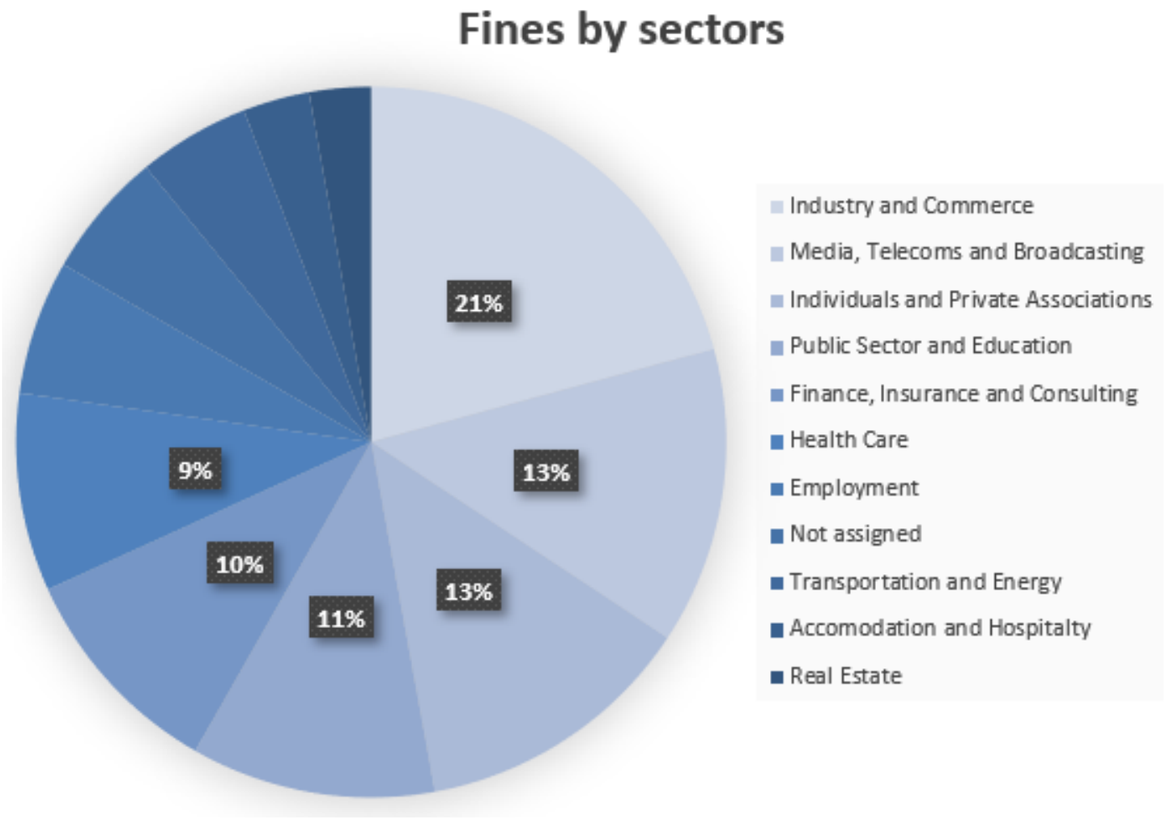


- Course of overall number of fines (cumulative):



Source： https://www.enforcementtracker.com/?insights

-



- All-area companies are under legislative’s inspection.

Specific External Requirements (from GDPR)

- The device should only use secure and non deprecated (TLSv1.2) channels for communication (HTTPS).
- The source code reveals hardcoded URLs.
- Only certificates signed by a trusted CA are accepted.
- Pre installed application should only communicate with servers in EU.
- Encryption is the best way to protect data during transfer and one way to secure stored personal data.

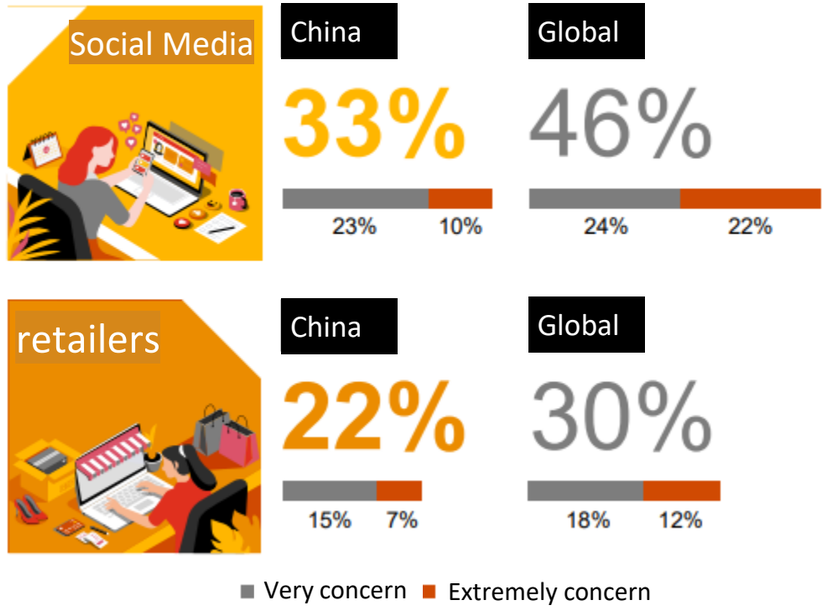




Consumer Concerns

Some **third-party** E-commerce apps are like mind-reader. …

Consumers level of Privacy concern



Source: https://www.pwc.com/gx/en/industries/consumer-markets/consumer-insights-survey-feb-2023.html

Motivations:

- European area’s increasing regulation requirements;
- Reduce the risk of increasingly strict inspections for the company.
- Curious about convenient apps are achieved.

Objectives:

- Find non-compliance transmission behaviors and prepared for further analysis

Preparations

We have already integrated a novice-friendly auto-deployment script in the tool，while you still need the following preparations:

1. Win 10 or higher
2. Python 3.10 or higher
3. An emotional stable security researcher :)

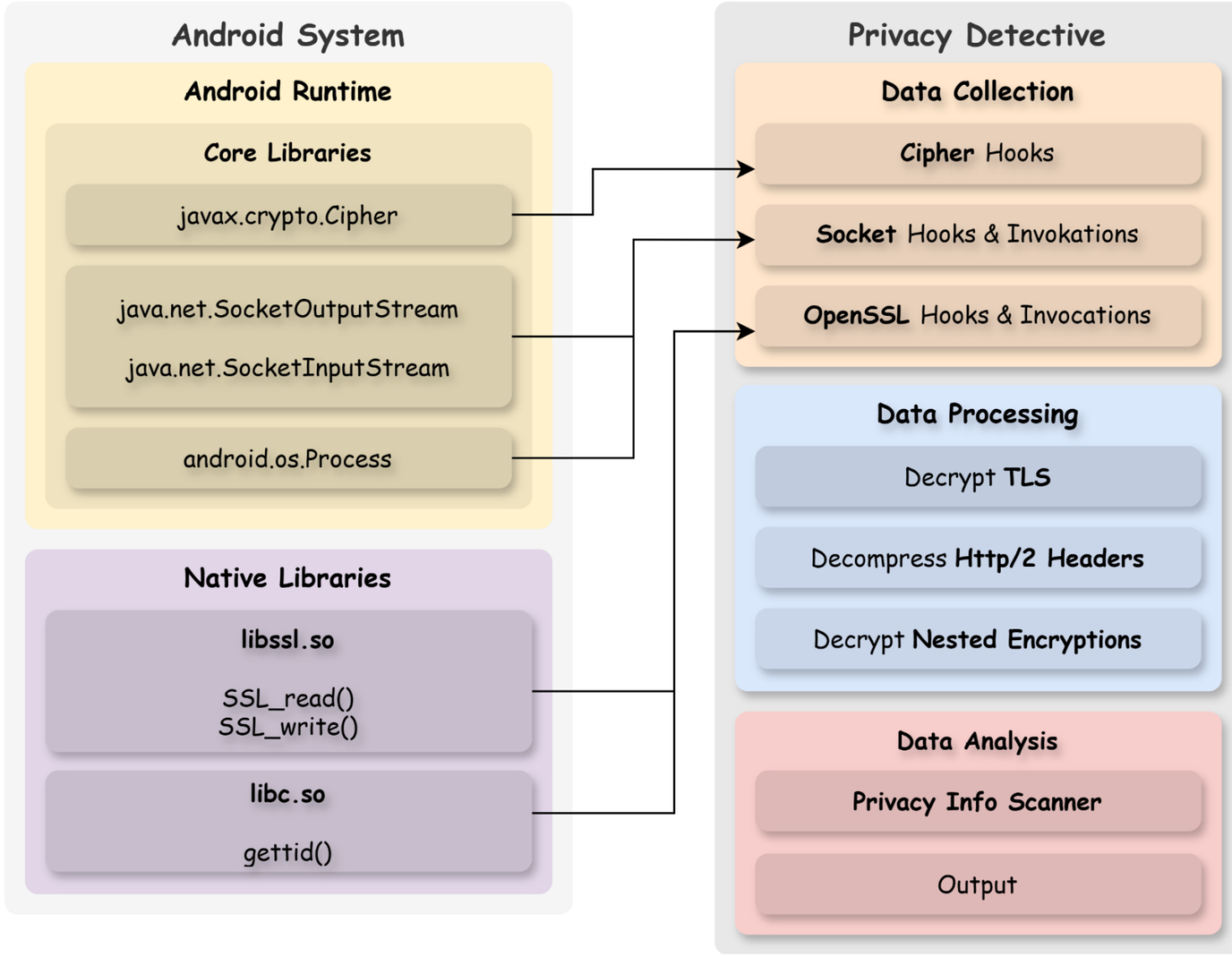
Our Research

- Overview
- Data collection
- Data processing
- Data analysis

Overview

Supported functions:

- Network & cipher capture
- TLS decryption
- Decryption of nested encryption
- H2 header decoder
- Sensitive data scanner



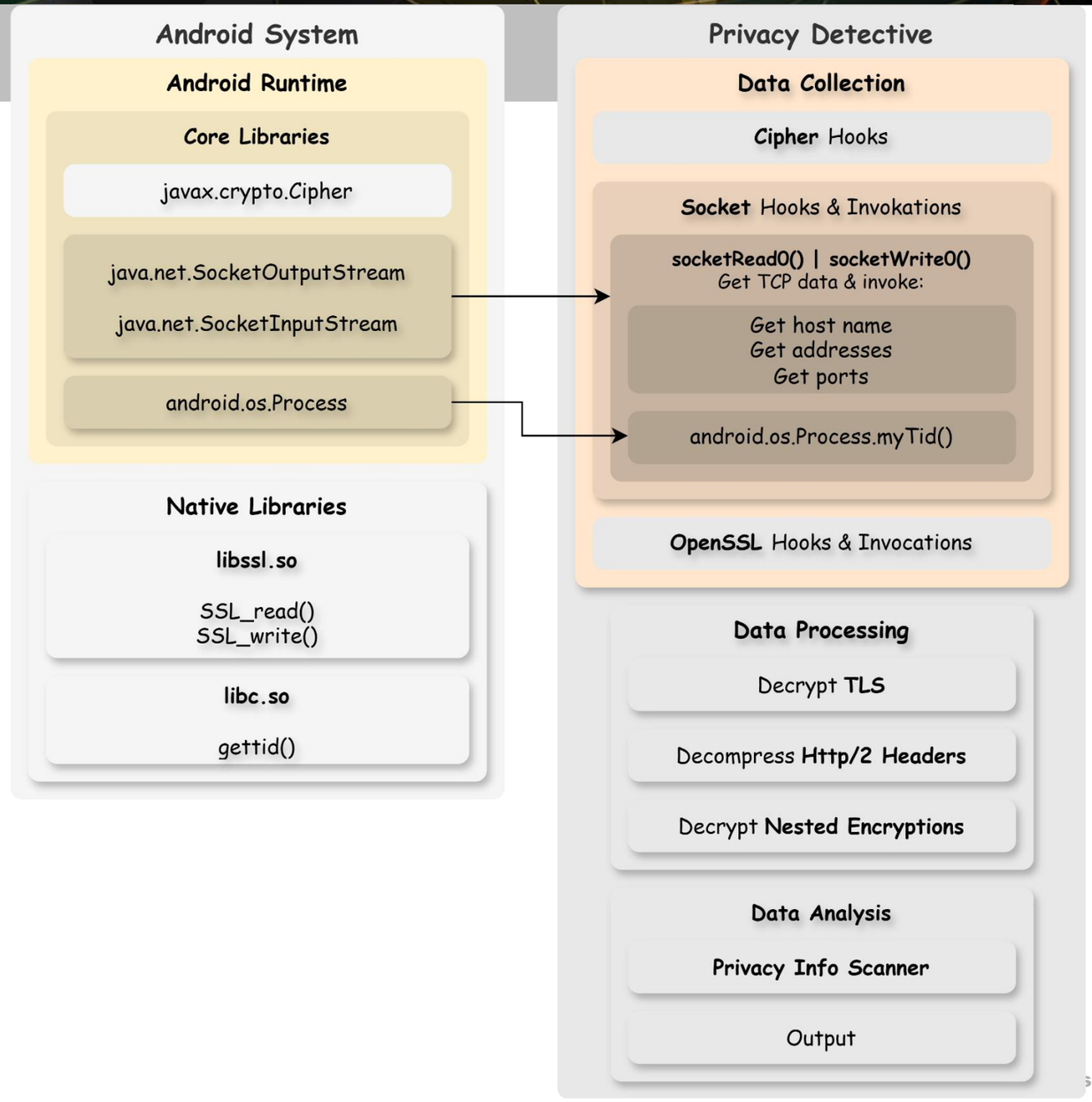
Data Collection

TCP&TLS Capture

TCP Socket Hook(Runtime):

- **Hook**
- **TCP data**: “java.net.SocketOutput(Input)Stream”

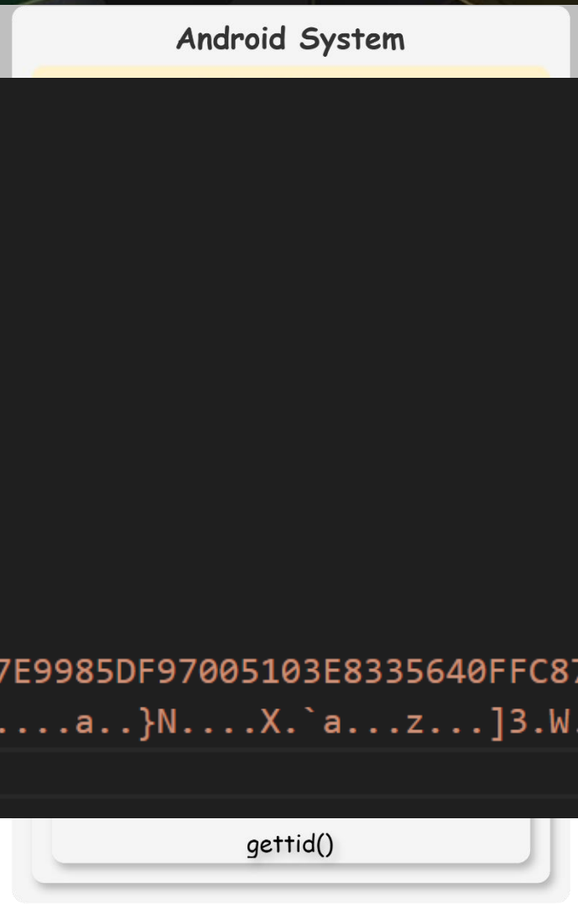
- **Invoke**
- **Server name:** “getHostString()”
- **Ips:** “getLocal(Remote)SocketAddress()”
- **Ports:** “getPort()”
- **Thread id:** “myTid()”

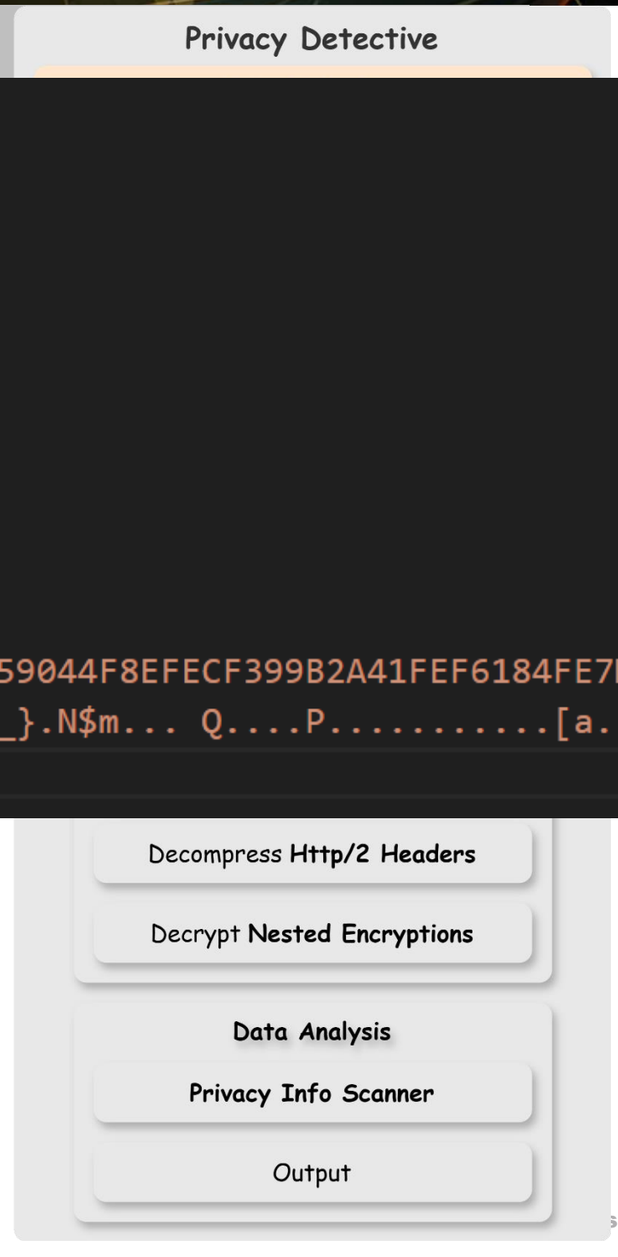


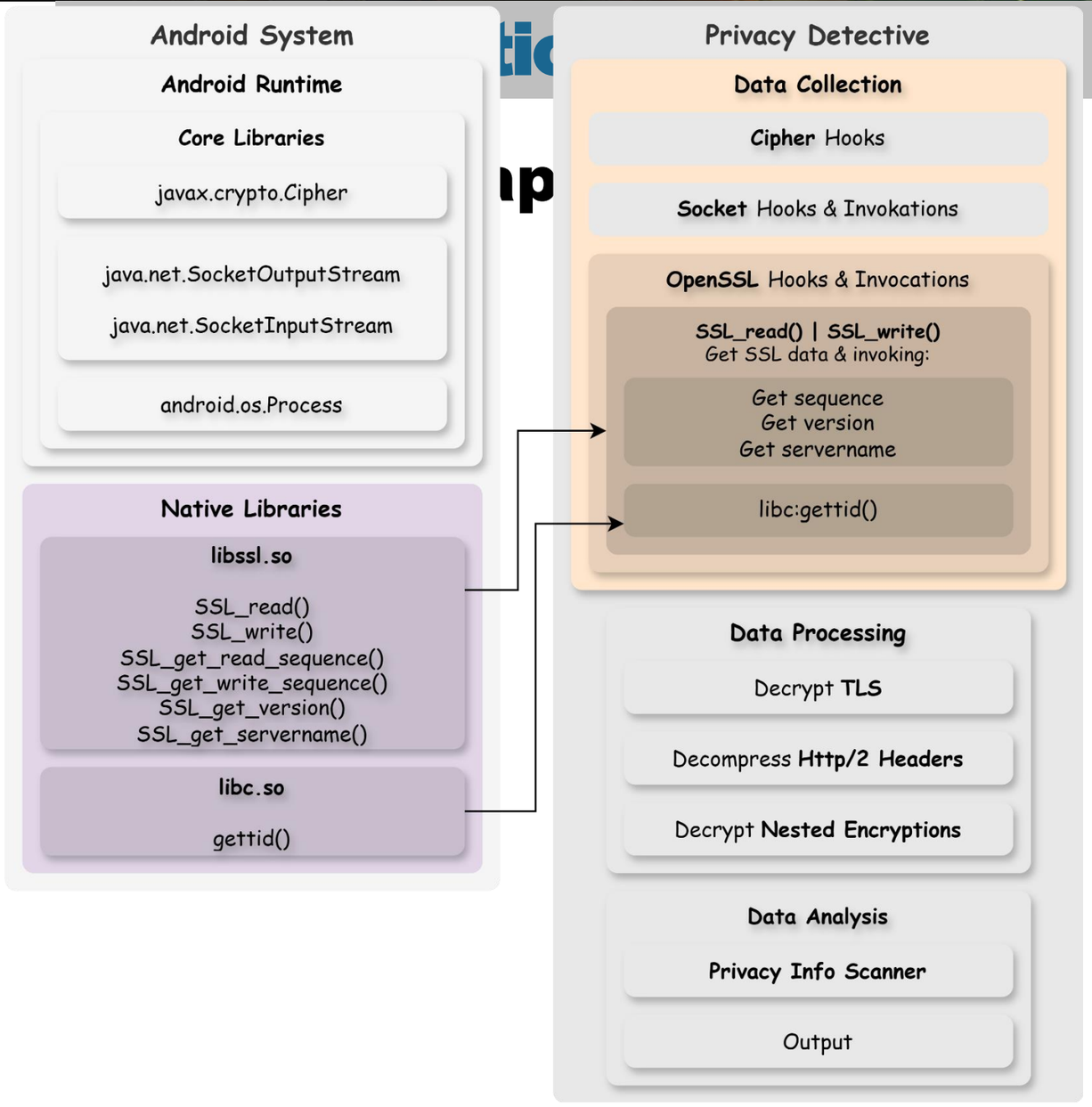
Data Collection


```
{
    "src-ip": "2[redacted].5",
    "src-port": 443,
    "dst-ip": "10.[redacted].178",
    "dst-port": 42618,
    "timestamp": "2024-01-19 11:05:23:452859",
    "sequence": null,
    "thread_id": 24340,
    "tls": null,
    "hostname": "mapi[redacted].com",
    "funcname": "TCP_recv",
    "hex": "17030302453A6BA55F5FC83672880A81E8A6B81463D707E9985DF97005103E8335640FFC87E59044F8EFECF399B2A41FEF6184FE7D
    "str": "....E:k.__.6r.......c....].p..>.5d.....D.........a..}N....X.`a...z...]3.W.[_}.N$m... Q....P...........[a..
},
```


- **Ips:** “getLocal(Remote)SocketAddress()”
- **Ports:** “getPort()”
- **Thread id:** “myTid()”





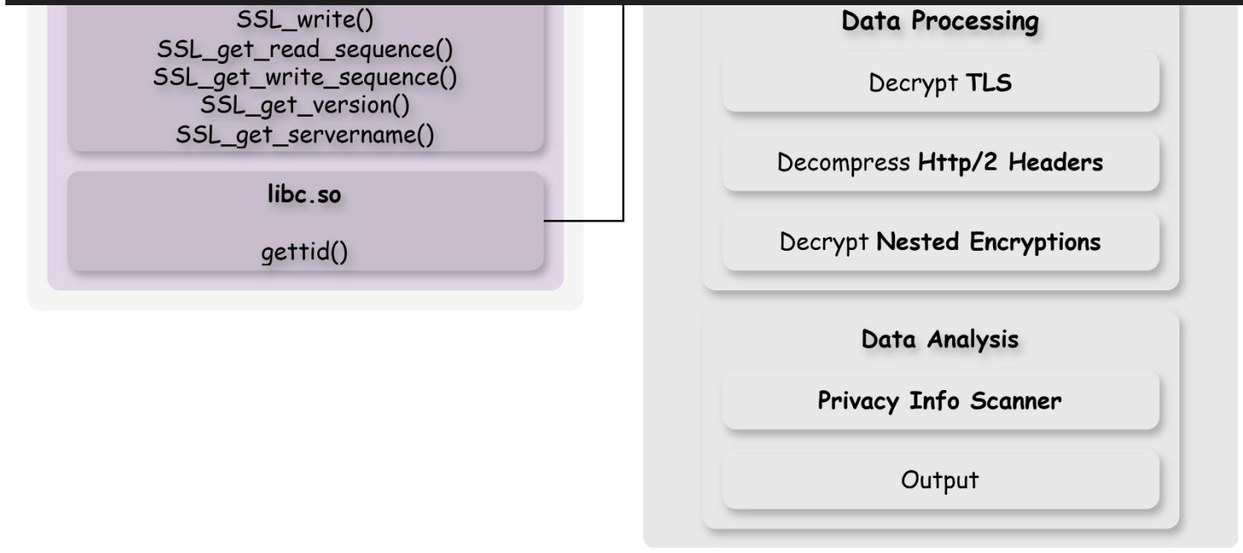


SSL Hook(Native):

- **Hook**
- **SSL data:** “libssl: SSL_read(write)”

- **Invoke**
- **SSL seq. no.:** “SSL_get_read(write)_sequence()”
- **SSL version:** “SSL_get_version()”
- **Server name:** “SSL_get_servername()”
- **Thread id:** “gettid()”

```
{
    "src-ip": null,
    "src-port": 0,
    "dst-ip": null,
    "dst-port": 0,
    "timestamp": "2024-01-19 11:05:23:853486",
    "sequence": 1,
    "thread_id": 24340,
    "tls": "TLSv1.2",
    "hostname": "mapi.[redacted].com",
    "funcname": "SSL_read",
    "hex": "485454502F312E3120323030204F4B0D0A446174653A204672692C203139204A616E20323032342030333A30343A303220474D540D0A436F6E74656E74
    "str": "HTTP/1.1 200 OK..Date: Fri, 19 Jan 2024 03:04:02 GMT..Content-Type: application/binary;charset=UTF-8..Content-Length: 240.
},
```

- **Invoke**
  - **SSL seq. no.:** “SSL_get_read(write)_sequence()”
  - **SSL version:** “SSL_get_version()”
  - **Server name:** “SSL_get_servername()”
  - **Thread id:** “gettid()”

Data Collection

Cipher Capture(JVM hook):

Cipher Hook(Runtime):

- **Hook (**“javax.crypto.Cipher”**)**
- **Cipher blocks:** “update()”, “doFinal()”
- **Parameters:** “chooseProvider()”

- One small tip.

Data Collection

Cipher Capture(JVM hook):

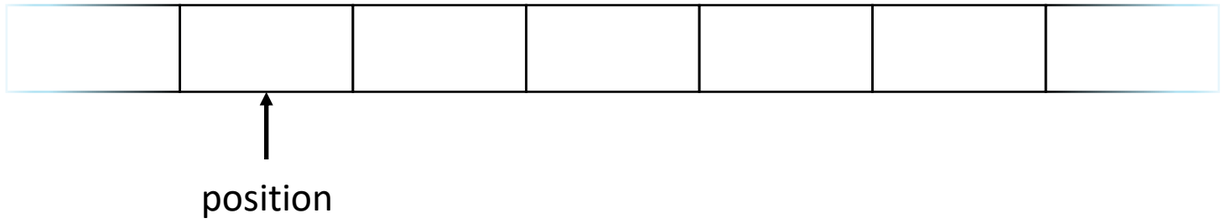
Bytebuffer

Cipher Hook(Runtime):

- **Hook (**“javax.crypto.Cipher”**)**
- **Cipher blocks:** “update()”, “doFinal()”
- **Parameters:** “chooseProvider()”

- One small tip.

Original workflow：



Data Collection

Cipher Capture(JVM hook):

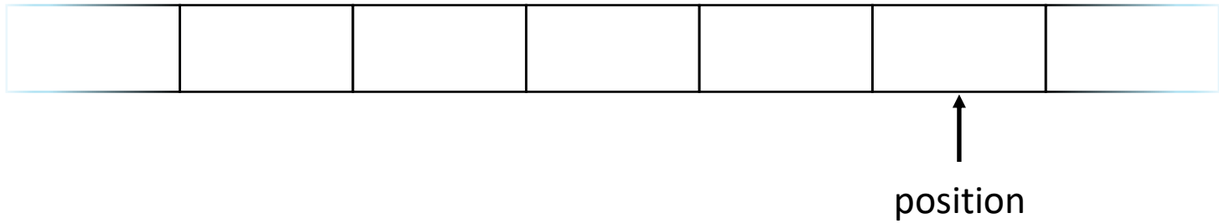
Bytebuffer

Cipher Hook(Runtime):

- **Hook (**“javax.crypto.Cipher”**)**
- **Cipher blocks:** “update()”, “doFinal()”
- **Parameters:** “chooseProvider()”

- One small tip.

Original workflow：



Data Collection

Cipher Capture(JVM hook):

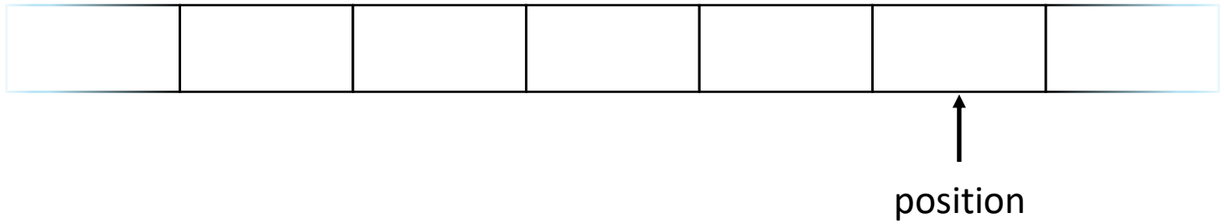
Bytebuffer

Cipher Hook(Runtime):

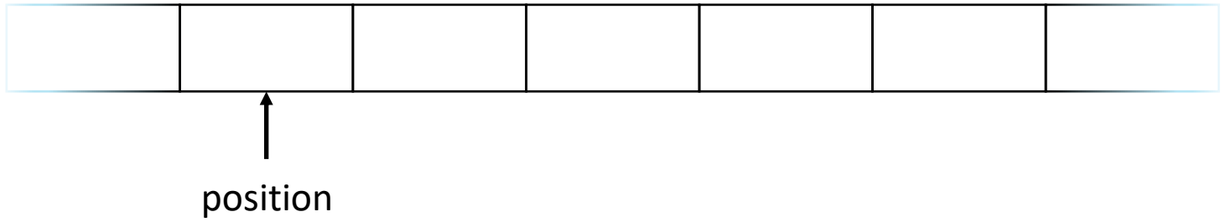
- **Hook (**“javax.crypto.Cipher”**)**
- **Cipher blocks:** “update()”, “doFinal()”
- **Parameters:** “chooseProvider()”

- One small tip.

Original workflow：



Hooked workflow：



Data Collection

Cipher Capture(JVM hook):

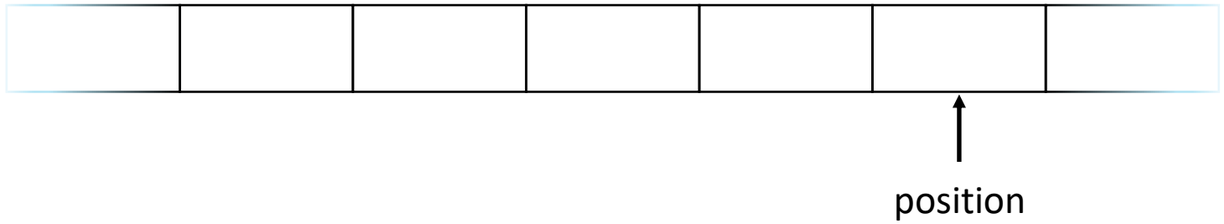
Bytebuffer

Cipher Hook(Runtime):

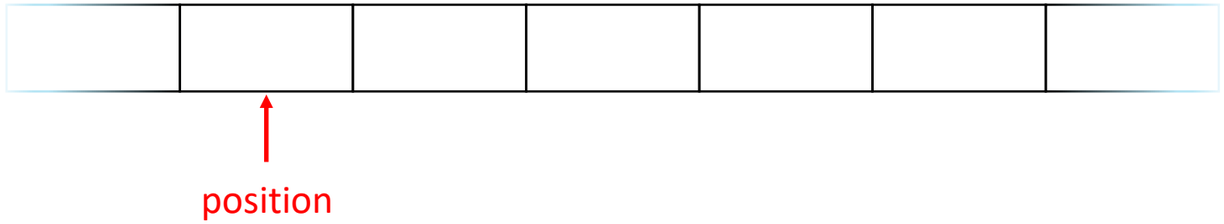
- **Hook (**“javax.crypto.Cipher”**)**
- **Cipher blocks:** “update()”, “doFinal()”
- **Parameters:** “chooseProvider()”

- One small tip.

Original workflow：



Hooked workflow：



Data Collection

Cipher Capture(JVM hook):

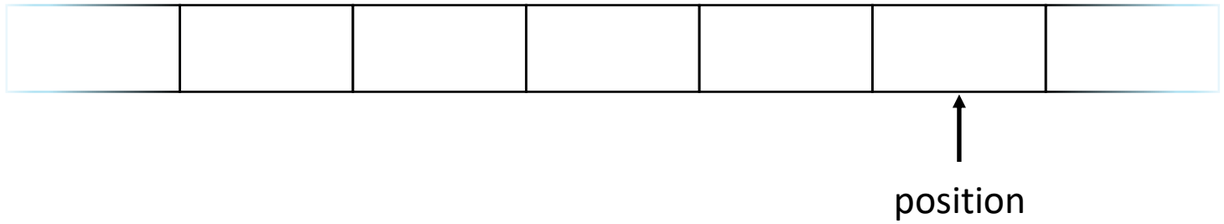
Bytebuffer

Cipher Hook(Runtime):

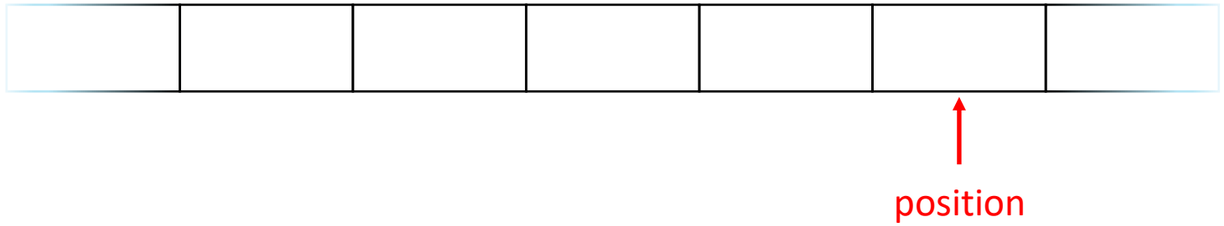
- **Hook (**“javax.crypto.Cipher”**)**
- **Cipher blocks:** “update()”, “doFinal()”
- **Parameters:** “chooseProvider()”

- One small tip.

Original workflow：



Hooked workflow：



Data Collection

Cipher Capture(JVM hook):

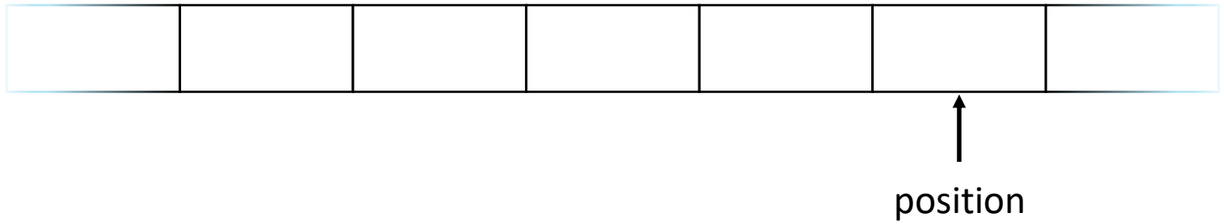
Bytebuffer

Cipher Hook(Runtime):

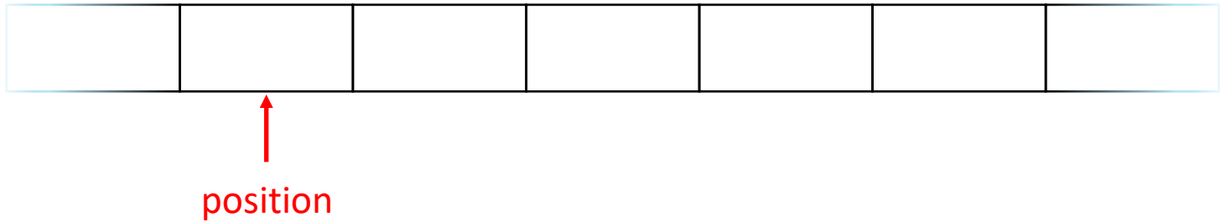
- **Hook (**“javax.crypto.Cipher”**)**
- **Cipher blocks:** “update()”, “doFinal()”
- **Parameters:** “chooseProvider()”

- One small tip.

Original workflow：



Hooked workflow：



Data Collection

Cipher Capture(JVM hook):

Cipher Hook(Runtime):

- **Hook (**“javax.crypto.Cipher”**)**
- **Cipher blocks:** “update()”, “doFinal()”
- **Parameters:** “chooseProvider()”

- Get encryption key and parameters in chooseProvider
- Splice the blocks and return the cipher text with plain text.

Data Collection

Cipher Ca

Cipher Hook(R

- **Hook (**“javax.c
- **Cipher blocks:**
- **Parameters:**

- Get encryption ke
- Splice the blocks a


```
{
    "transformation": "AES/GCM/NoPadding",
    "block_size": 16,
    "opmode": 1,
    "plain":
    "7B22776561746865722D6C6F636174696F6E2D7365727669636522 3A226A69757A6A7
    75A6C4B3535314D344F4D36537A74724970574536 2B46746C72594D335A764F56634A7
    057343D227D",
    "plain_string": "
    {\"weather-location-service\":\"jiuzjwZlK551M4OM6SztrIpWE6
    +FtlrYM3ZvOVcJpW4=\"}",
    "crypto":
    "C3B40663C389C286C2BFC2ADC28FC2A443042371C3B6C2BE51C39F17C39F58C2A06A0
    B45C3BF5F2FC381C3A3C3ADC288C2A76EC39347C2A13DC28BC3B0C2AC394DC28D3D1C4
    A5CC3B87877222AC3BEC28144C2B437C381C396C3A4C390C39C33C3A567495CC3B0C29
    9C3B5C382C3A2C293C299C3B900C38EC2997F5A7C594161576F48C3BA48C385C29A",
    "password": "",
    "IV": "67 0F 64 39 60 50 86 0F BC D0 04 41 "
},
```

Data Collection

Cipher Ca

Cipher Hook(R

- **Hook (**“javax.c
- **Cipher blocks:**
- **Parameters:**

- Get encryption ke
- Splice the blocks a


```
{
    "transformation": "AES/GCM/NoPadding",
    "block_size": 16,
    "opmode": 1,
    "plain":
    "7B22776561746865722D6C6F636174696F6E2D7365727669636522 3A226A69757A6A7
    75A6C4B3535314D344F4D36537A74724970574536 2B46746C72594D335A764F56634A7
    057343D227D",
    "plain_string": "
    {\"weather-location-service\":\"jiuzjwZlK551M4OM6SztrIpWE6
    +FtlrYM3ZvOVcJpW4=\"}",
    "crypto":
    "C3B40663C389C286C2BFC2ADC28FC2A443042371C3B6C2BE51C39F17C39F58C2A06A0
    B45C3BF5F2FC381C3A3C3ADC288C2A76EC39347C2A13DC28BC3B0C2AC394DC28D3D1C4
    A5CC3B87877222AC3BEC28144C2B437C381C396C3A4C390C39C33C3A567495CC3B0C29
    9C3B5C382C3A2C293C299C3B900C38EC2997F5A7C594161576F48C3BA48C385C29A",
    "password": "",
    "IV": "67 0F 64 39 60 50 86 0F BC D0 04 41 "
},
```

Data Processing

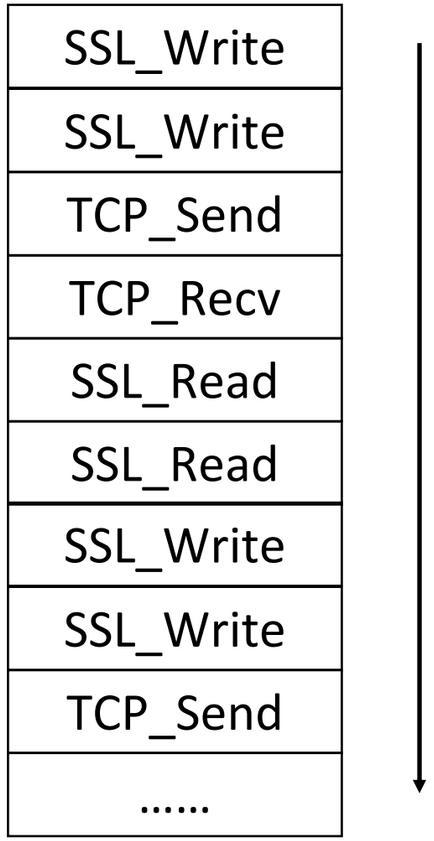
Can we decrypt TLS?

What we get in one connection?

- Time-based TLS and TCP data sequence.

How do TCP and TLS relate?

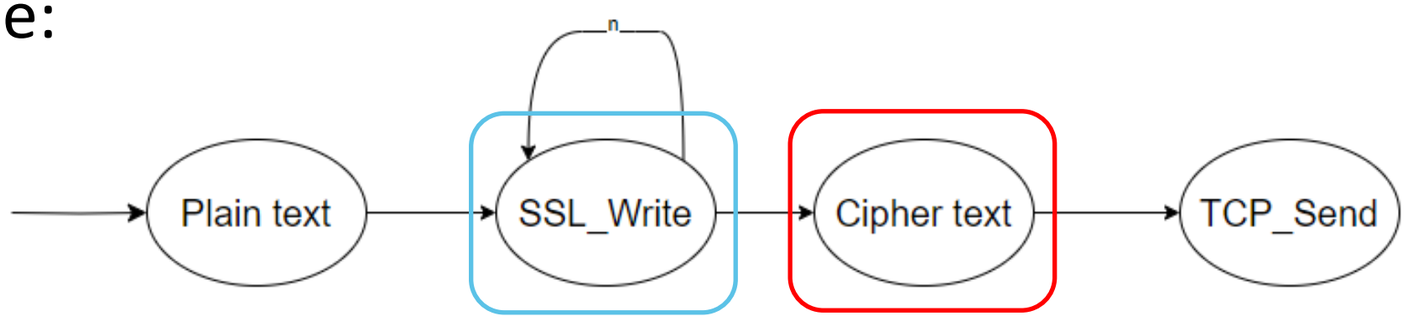
Let’s dive into TCP/TLS workflow.



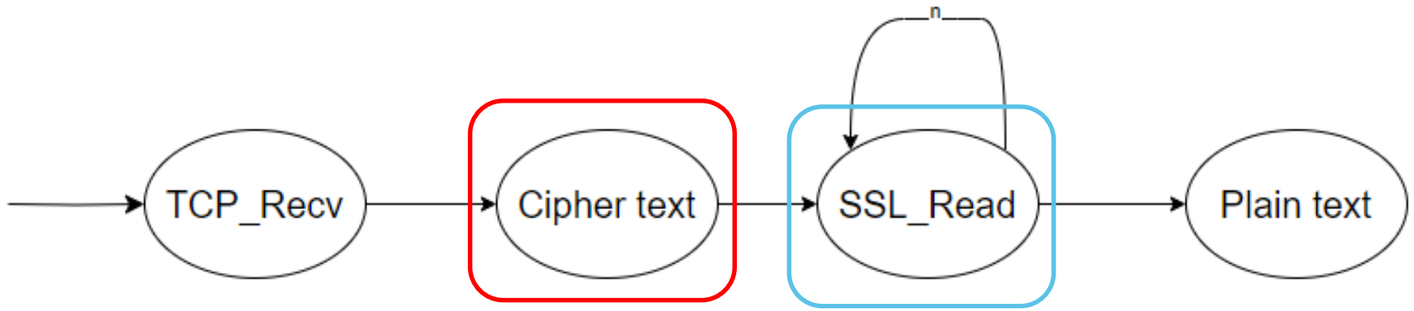
Data Processing

How do TCP and TLS relate?

Send Routine:



Receive Routine:

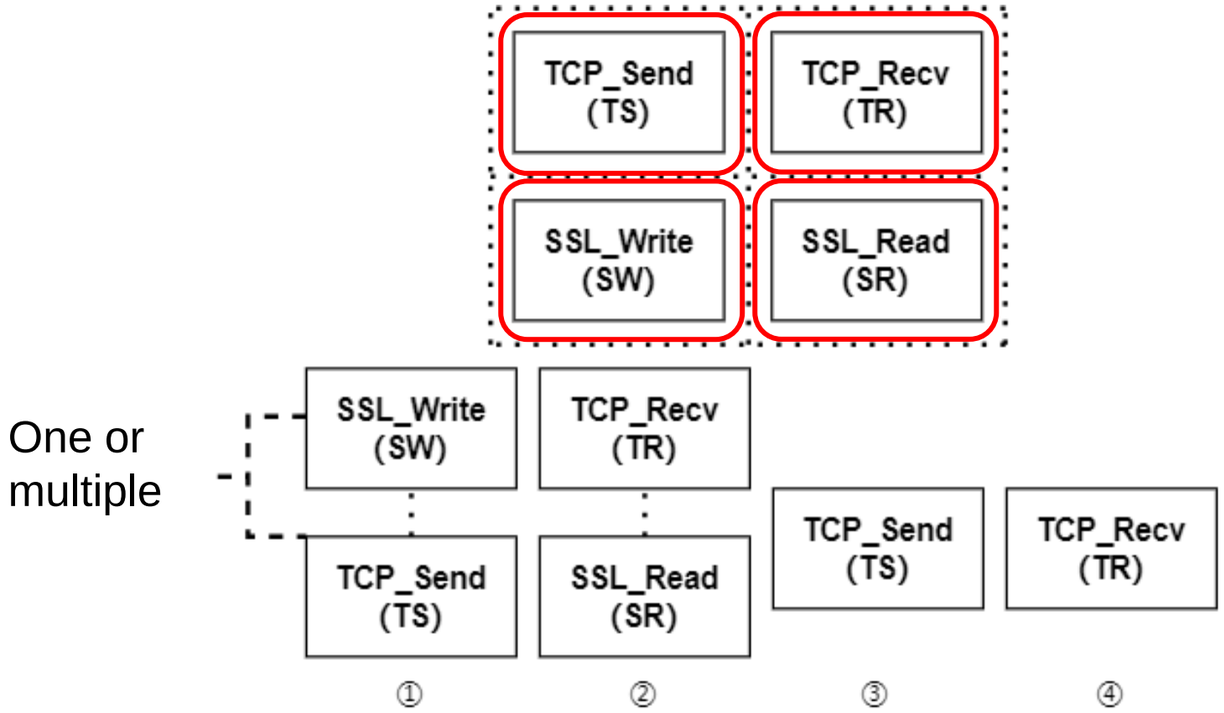


Data Processing

Can we decrypt TLS?

What we get in one connection?

- 4 different data



Data Processing

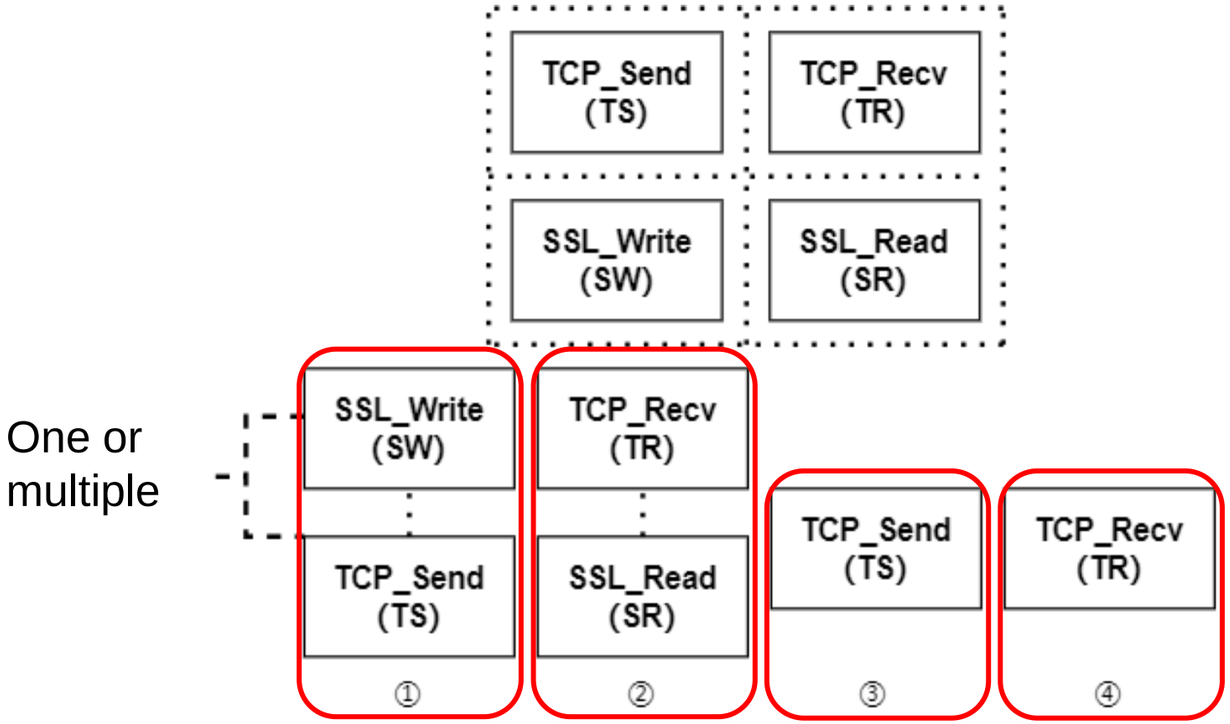
Can we decrypt TLS?

What we get in one connection?

- 4 different data

What is in the context of TLS?

- **TCP_Recv** follows:
  one or multiple SSL_Read
- **one or multiple SSL_Write** follows:
  TCP_Send



Data Processing

Can we decrypt TLS?

What we get in one connection?

- 4 different data

What is in the context of TLS?

- **TCP_Recv** follows:
  one or multiple SSL_Read
- **one or multiple SSL_Write** follows:
  TCP_Send

SSL_Write
SSL_Write
TCP_Send
TCP_Recv
SSL_Read
SSL_Read
TCP_Send
TCP_Recv
SSL_Read
……

Data Processing

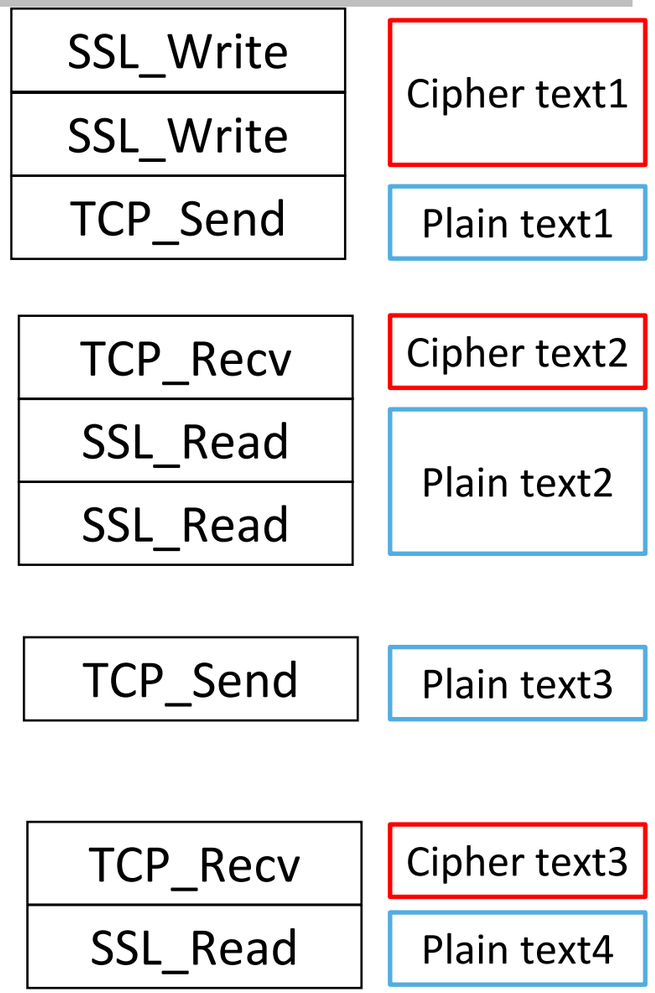
Can we decrypt TLS?

What we get in one connection?

- 4 different data

What is in the context of TLS?

- **TCP_Recv** follows:
  one or multiple SSL_Read
- **one or multiple SSL_Write** follows:
  TCP_Send



Data Processing

Can we decrypt TLS?

YES,

SSL_Write	Plain text1
SSL_Write	Cipher text1
TCP_Send	
TCP_Recv	Cipher text2
SSL_Read	Plain text2
SSL_Read	
TCP_Send	Plain text3
TCP_Recv	Cipher text3
SSL_Read	Plain text4
……	

BUT

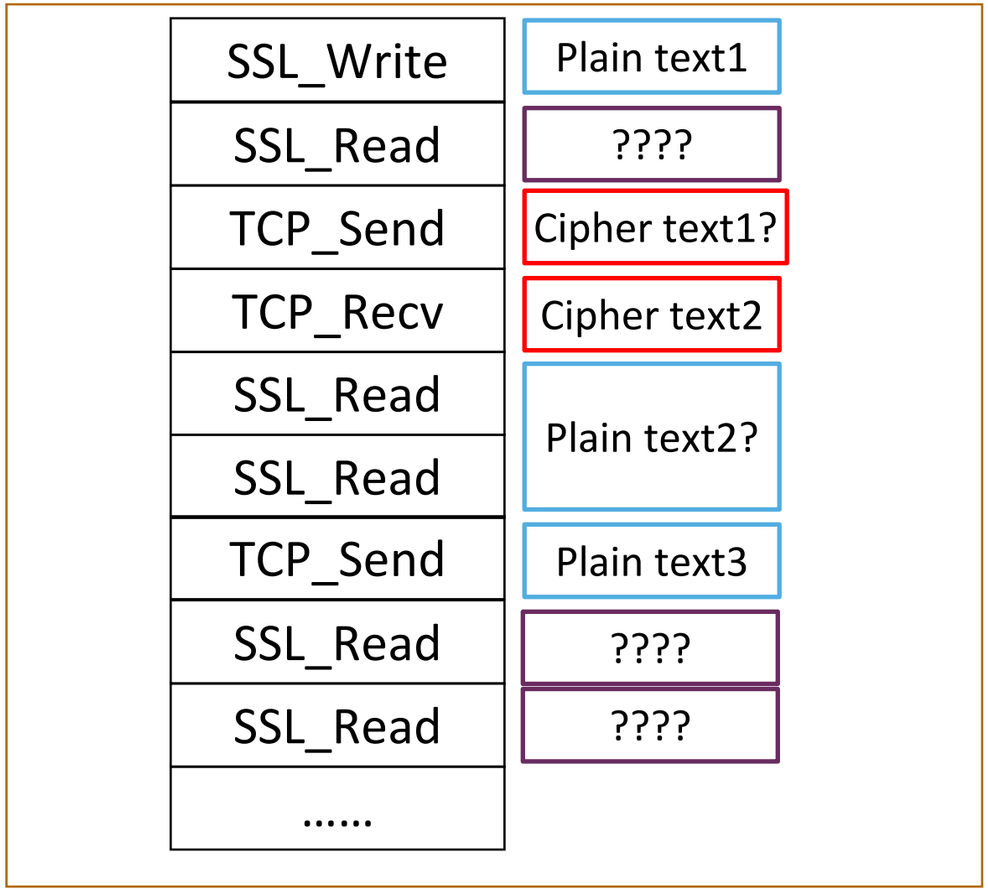
SSL_Write	Plain text1
SSL_Read	????
TCP_Send	Cipher text1?
TCP_Recv	Cipher text2
SSL_Read	Plain text2?
SSL_Read	
TCP_Send	Plain text3
SSL_Read	????
SSL_Read	????
……	

Data Processing

Can we decrypt TLS?

In one app or service,
there may be multiple TCP connections.

BUT

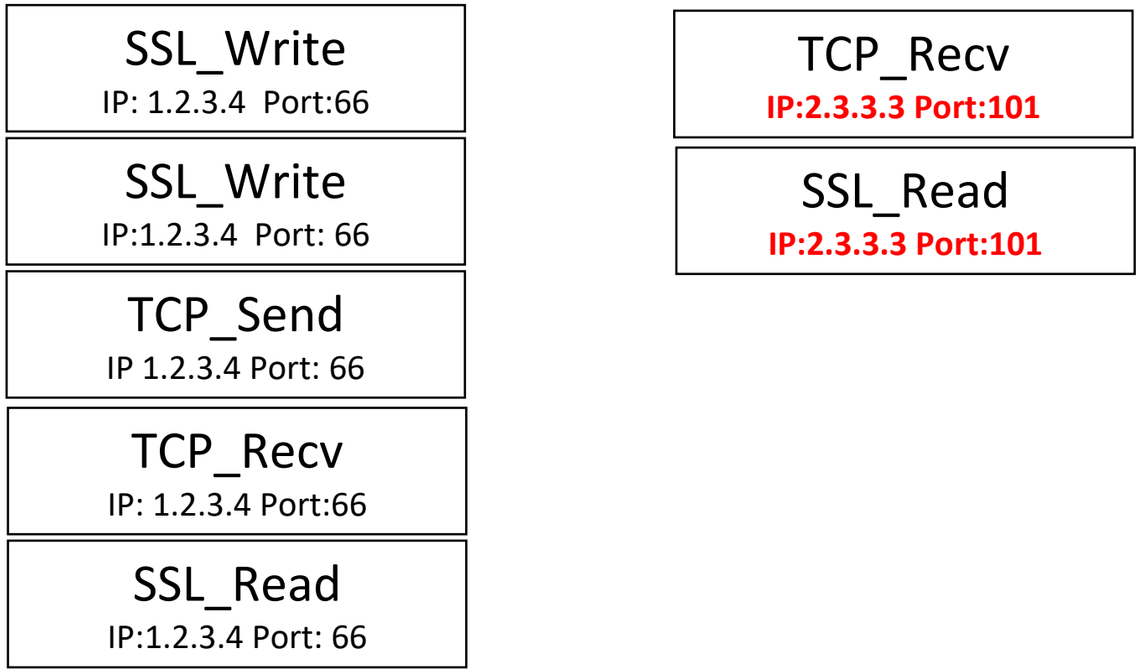


Data Processing

Can we decrypt TLS?

How to find one TCP connection?

- Match the ip and port in TLS & TCP.

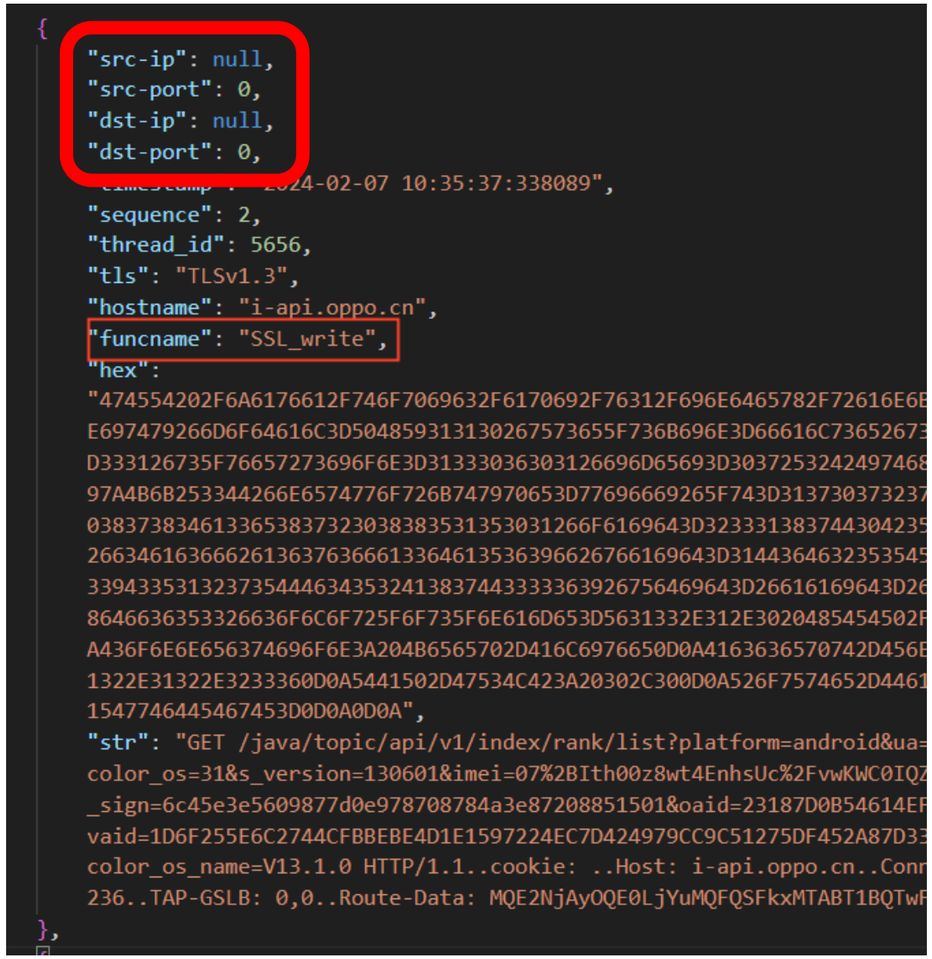


Data Processing

Can we decrypt TLS?

How to find one connection?

- Theoretically, we can match the ip and port in TLS & TCP.
- Practically, we cannot obtained the ip and port in TLS. T^T



Data Processing

Can we decrypt TLS?

How to find one connection?

- Theoretically, we can match the ip and port in TLS & TCP.
- Practically, we cannot obtained the ip and port in TLS.

- **So, we move to thread id**


```
{
    "src-ip": "2[redacted].15",
    "src-port": 443,
    "dst-ip": "10[redacted]52",
    "dst-port": 42362,
    "timestamp": "2024-03-25 19:11:16:036542",
    "sequence": null,
    "thread_id": 26814,
    "tls": null,
    "hostname": "catdot[redacted].com",
    "funcname": "TCP_recv",
    "hex": "17030300C5A989859BF947EB78DBE641347C3894AEE069020083F15B27813D
    "str": "..........G.x..A4|8...i....['.=\\).z.VMQ.3z..h.%..P...$..J.AZ
},
{
    "src-ip": null,
    "src-port": 0,
    "dst-ip": null,
    "dst-port": 0,
    "timestamp": "2024-03-25 19:11:16:037539",
    "sequence": 14,
    "thread_id": 26814,
    "tls": "TLSv1.2",
    "hostname": "catdot[redacted].com",
    "funcname": "SSL_read",
    "hex": "485454502F312E3120323030204F4B0D0A5365727665723A206F70656E7265
    "str": "HTTP/1.1 200 OK..Server: openresty..Date: Mon, 25 Mar 2024 11:
},
```

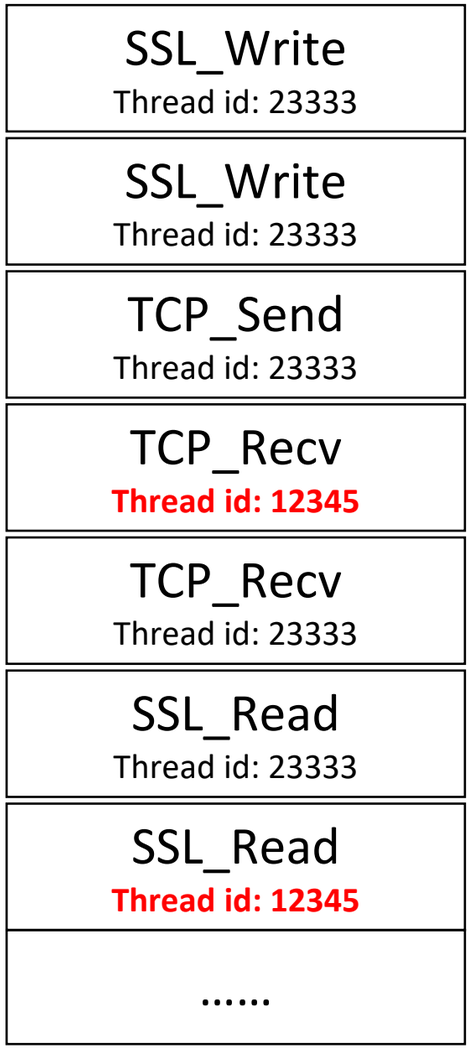
Data Processing

Can we decrypt TLS?

How to find one connection?

- Theoretically, we can match the ip and port in TLS & TCP.
- Practically, we cannot obtained the ip and port in TLS.

- **So, we move to thread id**



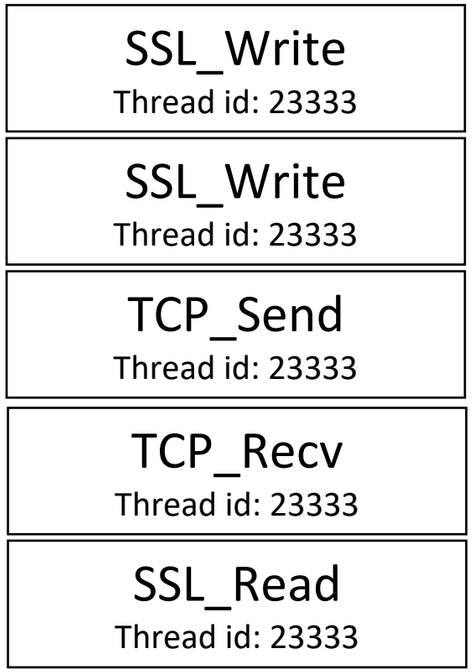
Data Processing

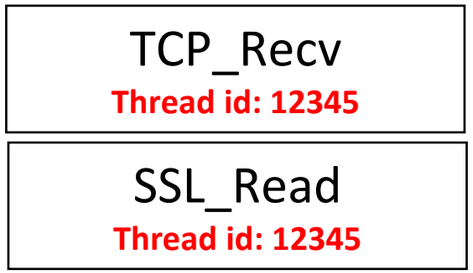
Can we decrypt TLS?

How to find one connection?

- Theoretically, we can match the ip and port in TLS & TCP.
- Practically, we cannot obtained the ip and port in TLS.

- **So, we move to thread id**



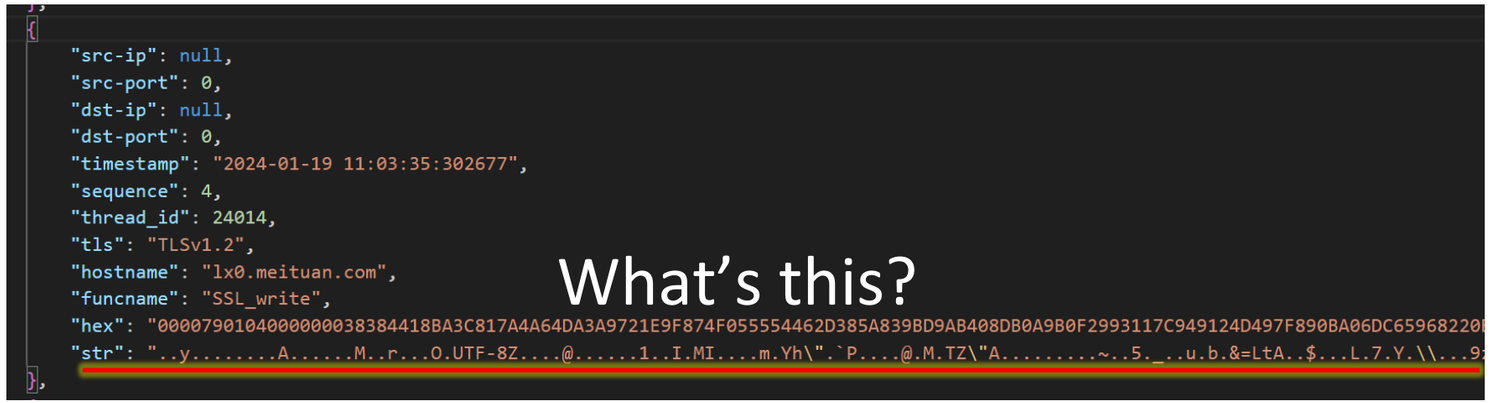


Data Processing

New encryption?

What are captured?

- Sequenced TLS and TCP data stream
- Sorted data stream by thread id.
- Matched TCP and TLS.



What We Get?

- Plain TCP data!
- But everything done?!

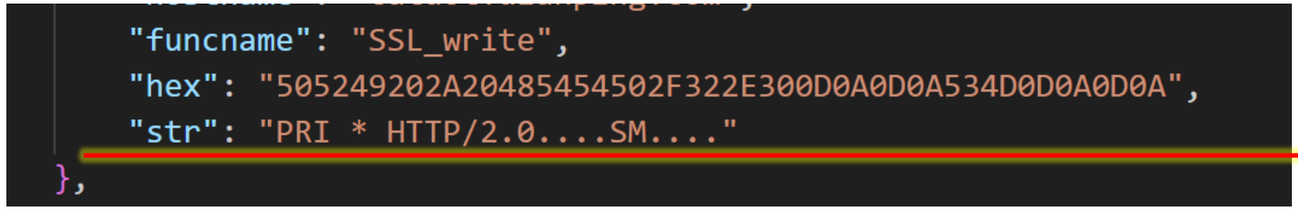
Data Processing

New encryption?

What are captured?

- Sequenced TLS and TCP data stream
- Sorted data stream by thread id.
- Matched TCP and TLS.

H2 head compress



What We Get?

- Plain TCP data!
- But everything done?!

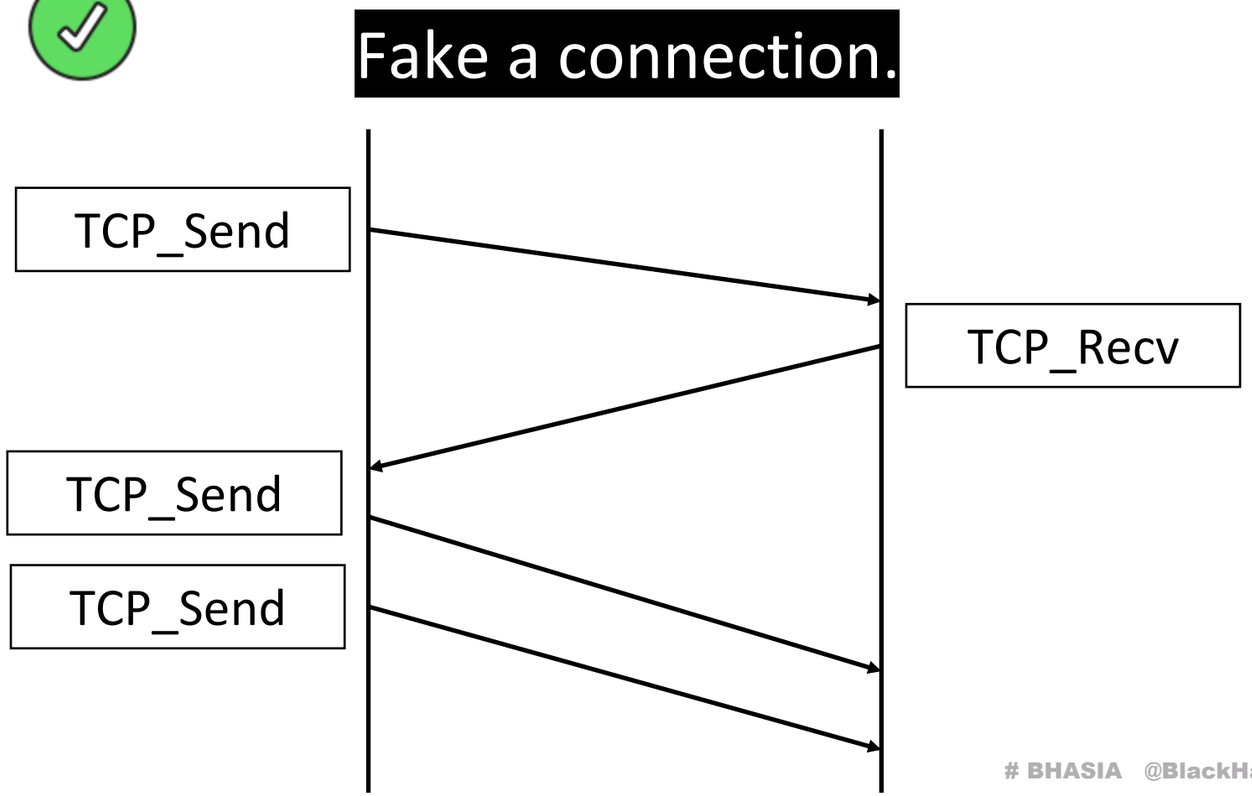
Data Processing

How to decompress HTTP/2.0 header completely?

1. Implement the algorithm to reverse the h2 encode algorithm.

2. Use the existing libraries.

3. What we get?



Data Processing


```
{
    "src-ip": "[redacted]",
    "src-port": 49246,
    "dst-ip": "[redacted]",
    "dst-port": 443,
    "timestamp": "2024-03-25 19:11:08:993762",
    "thread_id": 28071,
    "tls": "TLSv1.2",
    "hostname": "cat[redacted]com",
    "funcname": "TCP_send",
    "hex": "000115 ..... 0000",
    "str": "HTTP/2.0 [<RequestReceived stream_id:3, headers:[(':method', 'POST'), (':path',
    p=1&unionId=b[redacted]'), (':authorit
    ('content-type', 'application/x-www-form-urlencoded'), ('user-agent', 'Dalvik/2.1.0 (Lir
    ('accept-encoding', 'gzip'), ('content-length', '257')]>, <DataReceived stream_id:3, flo
```

Data Analysis

Privacy info scanner:

We used a self-developed regex-based script to scan the plaintext.

We highly recommend researchers have their own scan rules, or use open-source libs.

```
patterns = {"private_ssh_key": "-----BEGIN PRIVATE KEY-----[a-zA-Z0-9\\S]{100,}-----END PRIVATE KEY-----",
            "private_rsa_key": "-----BEGIN RSA PRIVATE KEY-----[a-zA-Z0-9\\S]{100,}-----END RSA PRIVATE KEY-----",
            "pgp_private_key_block": "-----BEGIN PGP PRIVATE KEY BLOCK-----",
            "generic_api_key": "[a|A][p|P][i|I][_]?[k|K][e|E][y|Y].*['|\"][0-9a-zA-Z]{32,45}['|\"]",
            "generic_secret": "[s|S][e|E][c|C][r|R][e|E][t|T].*['|\"][0-9a-zA-Z]{32,45}['|\"]",
            "ip_address": r"(?:(?:1\d\d|2[0-5][0-5]|2[0-4]\d|0?[1-9]\d|0?0?\d)\.){3}(?:1\d\d|2[0-5][0-5]|2[0-4]\d|0?[1-9]\d|0?0?\d)",
            "link_finder": "((?:https?://|www\d{0,3}[.])[a-zA-Z0-9_-]+(?:\.[a-zA-Z0-9_-]+)+[\w().=/;,#:@?&~*+!$%{}-]*)",
            "password_in_url": "[a-zA-Z]{3,10}://[^/\\s:@]{3,20}:[^/\\s:@]{3,20}@.{1,100}[\"'\\s]" }
```

Data Analysis

Our findings:


```
{
    "transformation": "DES/CBC/PKCS5Padding",
    "block_size": 8,
    "opmode": 1,
    "plain": "7B2241 ..... 5D7D",
    "plain_string": "{\"data\":[\"biz.bokhorst.xprivacy\",\"de.robv.android.xposed.in
    \"com.soft.apk008v\",\"net.digitalfeed.pdroidalternative\",\"net.anylocation\",\"
    tools\",\"com.dobe.sandbox\",\"com.xiaobai.gaiji\",\"com.sigma_rt.totalcontrol\",\
    qgwapp.shadowside\",\"com.qyqd\",\"top.a1024bytes.mockloc.ca.propushservice\",\"co
    daniu\",\"com.soft.aok008v\",\"zpp.wjy.xxsq\",\"com.wan1.you\",\"com.eagle.mdz\",\
    dimonvideo.luckypatcher\",\"com.speedsoftware.rootexplorer\",\"com.rinzz.avatar\",\"com.
    example.my.zjabc\",\"com.safe.dz\"]}",
    "crypto": "778D5 ..... DFDC2",
    "password": "6B ..... 49                                ",
    "IV": "6B ..... 49                              "
}
```


- Xprivacy
- Virtualdroid
- Godinsec
- Daniu
- ……

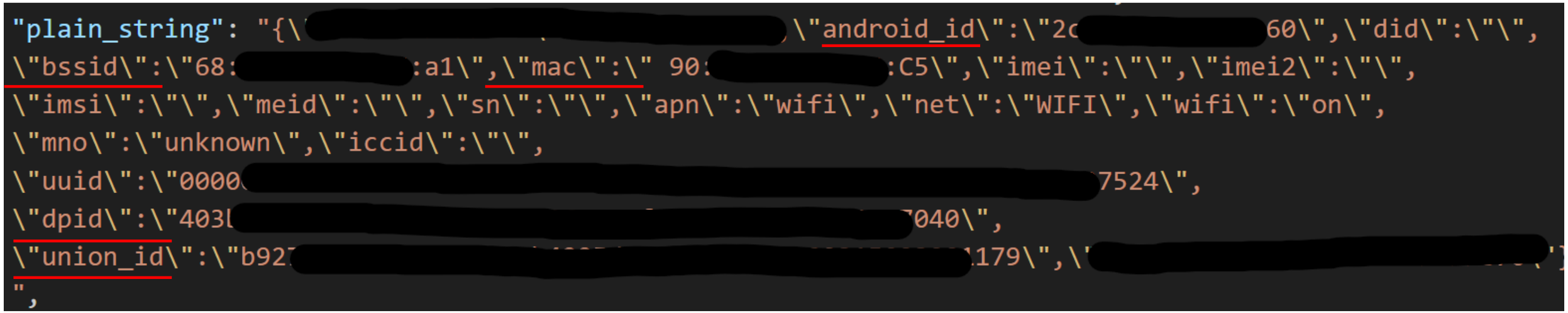
Data Analysis

Our findings:


```
{
    "transformation": "DES/CBC/PKCS5Padding",
    "block_size": 8,
    "opmode": 2,
    "plain": "53454C45435420434F554E542830292046524F4D206576656E74207768657265206C6576656C3C3D3F",
    "plain_string": "SELECT COUNT(0) FROM event where level<=?",
    "crypto": "0F3436FF35CCB8376C6AC43D385069E381E5B2E19B54E7874DDEC5337A5FDCF649F6DD8723D80B63FE00C5DA7D580622",
    "password": "[redacted]",
    "IV": "[redacted]"
},
```

Data Analysis

Our findings:



Data Analysis

Our findings:


```
{
    "src-ip": "192.168.137.177",
    "src-port": 51230,
    "dst-ip": "13.36.124.147",
    "dst-port": 443,
    "timestamp": "2024-03-12 12:00:31:767377",
    "thread_id": 28541,
    "tls": "TLSv1.2",
    "hostname": "weather                .com",
    "funcname": "TCP_send",
    "hex": "......",
    "str": "HTTP/2.0 [<RequestReceived stream_id:11, headers:[(':method', 'POST'), (':path', '/weather/location,
                                ), (':authority', 'weather                .com'), (':scheme', 'https'),
    ('cipherinfo', '{\"crypto-cipher-service\":{\"tmpPublicKey\":\"MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEOfA4U2\\\\/
    MlgHjt+yh2eh01i6R0QaBfnpP\\\\/4DqowwI2JuD5wLMQhnjgR\\\\/2noJndJB5Ilv4QN5q8BxA0u4DCXcRAA==\",
    \"salt\":\"Y6W8M1FiPvH84DsYL88rnTIXmfBr62b1GvufSY2R76U=\",\"info\":\"d2VhdGhlci1sb2NhdGlvbi1zZXJ2aWNl\"}}'),
    ('wrapperkey', '{\"cipher\":\"389cN4NAPOmX3Samiac58gb0eZmJ2s49RhVwXuPGnfPudUwatJIR19\\\\/205Pz62g\\\\/0MEvf\\\\/
    CFpNdOf1xofsBOBnX3eNECb53db+n\\\\/Zzo+zZeIiBvJFh6\\\\/l+s=\",\"iv\":\"RRWwGTbEi4WYaPSP\"}'), ('encryptflag',
    '3'), ('content-type', 'application/json; charset=utf-8'), ('content-length', '380'), ('accept-encoding',
    'gzip'), ('user-agent', 'okhttp/4.9.0')]>, <DataReceived stream_id:11, flow_controlled_length:380,
    data:7b22616374697661746f6e54696d657374616d>, <StreamEnded stream_id:11>]  Data:
    {\"bssid\":\"86:          :04\",\"latitude\":\"KUCVO5YF\",\"ssid\":\"\\\"              \\\"\",
    \"todayLocateCnt\":\"10\",\"longitude\":\"KkOIIJ0JWQ==\",\"ts\":\"2024-03-12 12:00:30 GMT+08:00\"}",
    "num": 37,
    "identity": {
        "MAC": [
            "86:          :04"
        ]
    }
```

Data Analysis

Our findings:

Deployment

Deployment

Automation:

- Install.bat :

  Install or upgrade dependency;

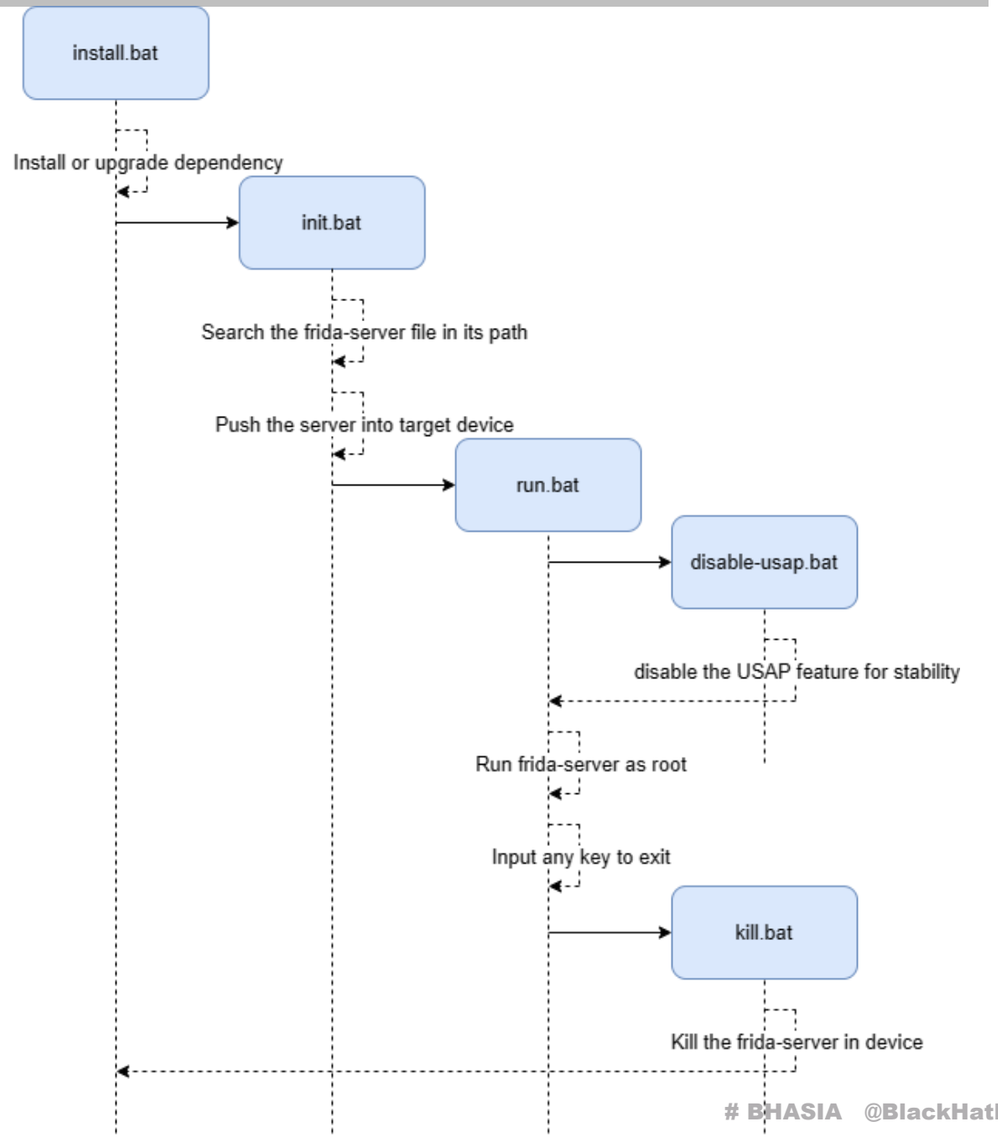
- Init.bat :

  Push Frida-server into device;

- run.bat :

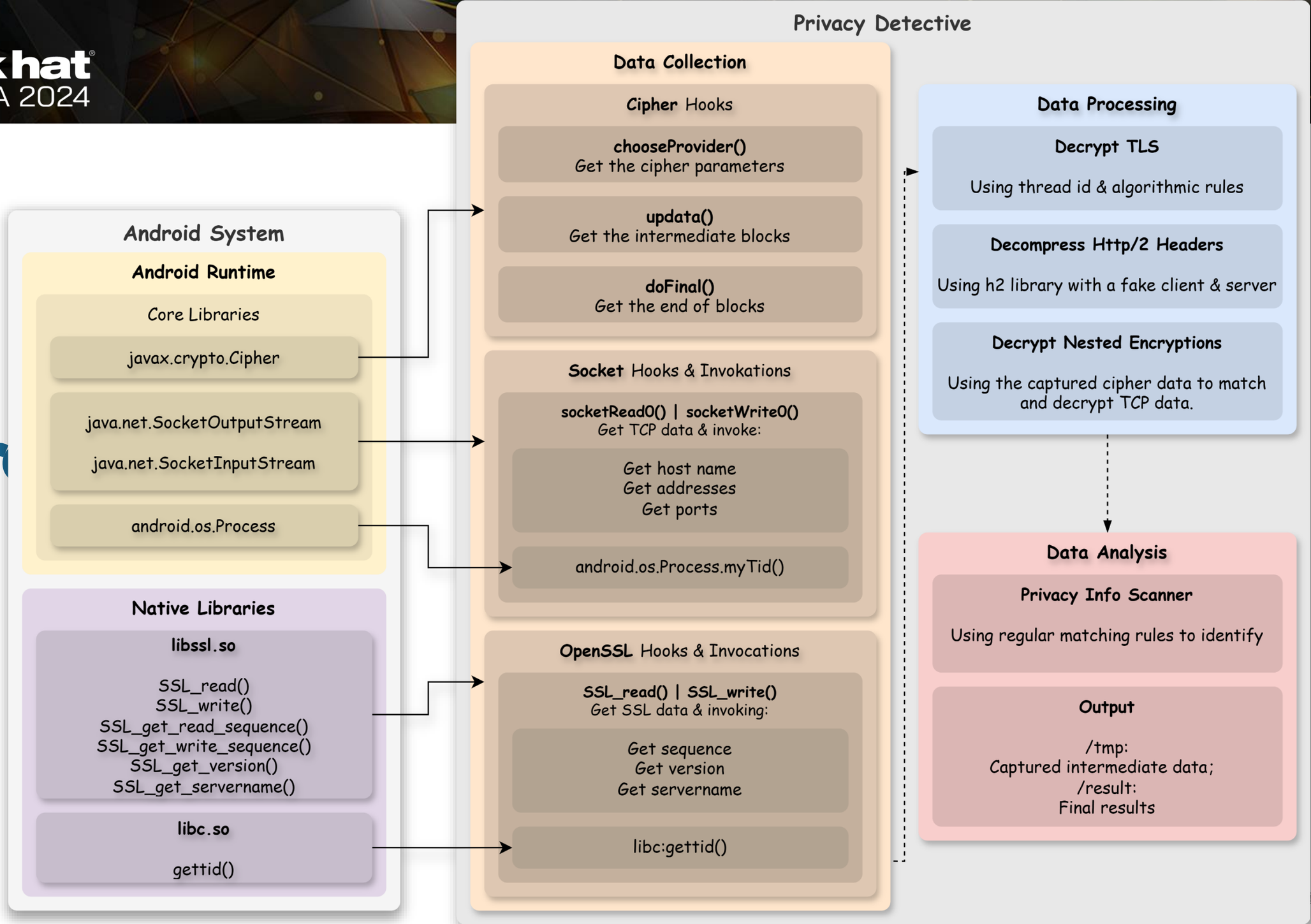
  Run Frida & Invoke disable-usap.bat;

  Waiting kill command.



Prospects

- Add UDP support
- Add Chrome & Firefox core support
- Add pcap output
- Rewrite a Xposed version


Privacy Detective
Data Collection
Cipher Hooks
chooseProvider()
Get the cipher parameters
updata()
Get the intermediate blocks
doFinal()
Get the end of blocks
Socket Hooks & Invokations
socketRead0() | socketWrite0()
Get TCP data & invoke:
Get host name
Get addresses
Get ports
android.os.Process.myTid()
OpenSSL Hooks & Invocations
SSL_read() | SSL_write()
Get SSL data & invoking:
Get sequence
Get version
Get servername
libc:gettid()
Android System
Android Runtime
Core Libraries
javax.crypto.Cipher
java.net.SocketOutputStream
java.net.SocketInputStream
android.os.Process
Native Libraries
libssl.so
SSL_read()
SSL_write()
SSL_get_read_sequence()
SSL_get_write_sequence()
SSL_get_version()
SSL_get_servername()
libc.so
gettid()
Data Processing
Decrypt TLS
Using thread id & algorithmic rules
Decompress Http/2 Headers
Using h2 library with a fake client & server
Decrypt Nested Encryptions
Using the captured cipher data to match and decrypt TCP data.
Data Analysis
Privacy Info Scanner
Using regular matching rules to identify
Output
/tmp:
Captured intermediate data;
/result:
Final results

Takeaways

- How to decrypt TLS in TCP traffic without IP info.
- ➢ By using Linux thread ID as the feature, and through analysis of the packet sequences, we decrypt TLS traffic on Android without IP, port or certificate information.

- How to decrypt nested encrypted TCP data.
- ➢ We hooked most implementations of “Cipher” class to get all the encryption and decryption data, then restored the double-encrypted content in TCP. But please be careful with Byte Buffer.

- How can we protect our privacy from tracking.
- ➢ As we showed on “Our findings” slides. For a Android user, we highly suggest you to use the latest version to obtain the newest security & privacy strategy, practice the principle of least privilege.

Q&A

The End