# ANDROID MALWARE ANALYSIS

**GODWIN PRINCE - B01014554**

## Introduction

This report delves into a meticulous analysis of software applications using both static and dynamic methods. By combining static analysis, which scrutinizes source code, with dynamic analysis, which evaluates runtime behavior, we aim to gain a holistic understanding. The approach goes beyond mere bug detection, delving into architecture, optimization, and security. Through creative exploration, I aim to uncover compelling insights that fortify software quality and user experience.

## Static Analysis

Android static malware analysis is a vital cybersecurity practice for uncovering malicious and benign code within Android applications without execution. Through tools and techniques, it examines app code, permissions, and structure to detect indicators of malware, analyze permissions, uncover vulnerabilities, detect anti-analysis measures, and assess third-party libraries. This process is critical for preemptively identifying and mitigating security threats in the Android ecosystem. Furthermore, it involves assessing third-party libraries and dependencies for potential security risks. By delving into the intricacies of Android applications through static analysis, cybersecurity professionals gain valuable insights into the software's functionality and potential security threats, enabling them to proactively identify and mitigate risks before deployment.

## Dynamic Analysis

Dynamic malware analysis is a dynamic cybersecurity technique that involves observing the behavior of malicious software in a controlled environment during runtime. Specifically applied to Android malware analysis, this process entails executing the application within a sandboxed environment to closely monitor its interactions with the operating system, network, and other applications. Through dynamic analysis, security analysts can scrutinize various aspects of the application's behavior, including file system activities, network communications, process creation, and system calls, to identify any malicious actions or deviations from expected behavior. By dynamically analyzing the application's code execution flow, memory usage, and runtime modifications, analysts can detect runtime-packed or self-modifying malware, as well as evasion techniques employed by the malicious software. Additionally, dynamic analysis enables the monitoring of API calls made by the application, detection of exploit attempts targeting known vulnerabilities, and generation of dynamic malware signatures for future detection.

# 1) Static Analysis (Mijn Driessen)


```
[
    "connection_interfaces_exfiltration",
    [
        "This application reads details about the currently active data network",
        "This application tries to find out if the currently active data network is metered"
    ]
],
[
    "telephony_services_abuse",
    []
],
[
    "audio_video_eavesdropping",
    []
],
[
    "suspicious_connection_establishment",
    [
        "This application opens a Socket and connects it to the remote address '127.0.0.1' on the '5327' port "
    ]
],
[
    "PIM_data_leakage",
    [
        "This application accesses data stored in the clipboard"
    ]
],
```


**Connection Interfaces Exfiltration:** The application is observed to read details about the currently active data network and attempts to determine if the network is metered, which could indicate potential data exfiltration or tracking behavior.

**Telephony Services Abuse:** Although no specific details are provided, this activity implies potential misuse or unauthorized access to telephony services within the application.

**Audio-Video Eavesdropping:** While no specific instances are noted, this activity suggests the possibility of the application attempting to eavesdrop on audio or video communications.

**Suspicious Connection Establishment:** The application is seen opening a socket and connecting it to the local address '127.0.0.1' on port '5327', which may indicate communication with a local service or a backdoor connection.

**PIM Data Leakage:** The application is observed accessing data stored in the clipboard, which could potentially lead to leakage of Personally Identifiable Information (PIM) or sensitive data.

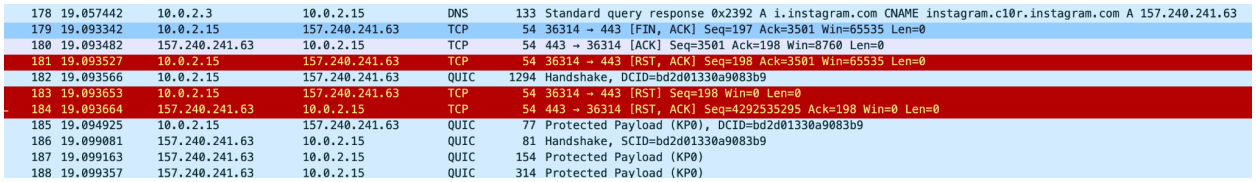
```
[
    "device_settings_harvesting",
    [
        "This application logs the message '  ' under the tag '  =========  MotionLayout'",
        "This application logs the message ' ################# init' under the tag 'Constraints'"
        "This application logs the message ' Points are coincident' under the tag 'PathParser'",
        "This application logs the message ' no motionScene' under the tag 'MotionLayout'",
        "This application logs the message ' requires the Google Play Store, but it is missing.
        "This application logs the message '' under the tag '  =========  MotionLayout'",
        "This application logs the message '' under the tag '  Destroying:  LoaderManager'",
        "This application logs the message '' under the tag '  Resetting:  LoaderManager'",
        "This application logs the message '' under the tag '  Starting:  LoaderManager'",
        "This application logs the message '' under the tag '  Stopping:  LoaderManager'",
        "This application logs the message '' under the tag '  onLoadFinished in  :  3'",
        "This application logs the message '' under the tag ' KeyPath position \" \" outside of r
        "This application logs the message '' under the tag ' for   with mCallbacksMessenger=  th
        "This application logs the message '' under the tag ''",
        "This application logs the message '' under the tag '1'",
        "This application logs the message '' under the tag '2'",
```

These log messages suggest that the application may be monitoring and logging various activities related to the device's settings, loader manager, motion layout, and Google Play services utilization. Further analysis is required to determine the exact purpose and implications of these activities.

## Dynamic Analysis (Mijn Driessen)

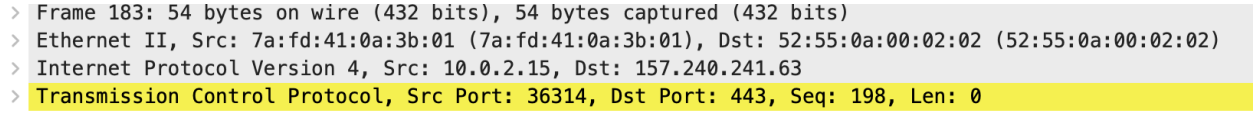
**DNS resolution:** The DNS query response points to the IP address "i.instagram.com" at 157.240.241.63. Dynamic analysis involves checking the legitimacy of the DNS response to ensure that it has not been forged or tampered with.

**TCP Termination (FIN, ACK):** A request to terminate a TCP connection with the FIN flag is detected at 10.0. from 2.15 to the number 157 240 241 63. This indicates the client's intention to disconnect. A corresponding acknowledgment (ACK) from the server confirms the termination request.



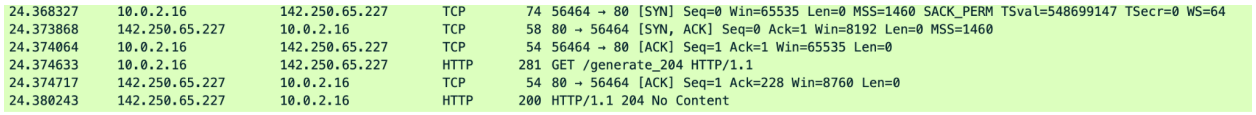
| | | | | | | |
|---|---|---|---|---|---|---|
| 178 | 19.057442 | 10.0.2.3 | 10.0.2.15 | DNS | 133 | Standard query response 0x2392 A i.instagram.com CNAME instagram.c10r.instagram.com A 157.240.241.63 |
| 179 | 19.093342 | 10.0.2.15 | 157.240.241.63 | TCP | 54 | 36314 → 443 [FIN, ACK] Seq=197 Ack=3501 Win=65535 Len=0 |
| 180 | 19.093482 | 157.240.241.63 | 10.0.2.15 | TCP | 54 | 443 → 36314 [ACK] Seq=3501 Ack=198 Win=8760 Len=0 |
| 181 | 19.093527 | 10.0.2.15 | 157.240.241.63 | TCP | 54 | 36314 → 443 [RST, ACK] Seq=198 Ack=3501 Win=65535 Len=0 |
| 182 | 19.093566 | 10.0.2.15 | 157.240.241.63 | QUIC | 1294 | Handshake, DCID=bd2d01330a9083b9 |
| 183 | 19.093653 | 10.0.2.15 | 157.240.241.63 | TCP | 54 | 36314 → 443 [RST] Seq=198 Win=0 Len=0 |
| 184 | 19.093664 | 157.240.241.63 | 10.0.2.15 | TCP | 54 | 443 → 36314 [RST, ACK] Seq=4292535295 Ack=198 Win=0 Len=0 |
| 185 | 19.094925 | 10.0.2.15 | 157.240.241.63 | QUIC | 77 | Protected Payload (KP0), DCID=bd2d01330a9083b9 |
| 186 | 19.099081 | 157.240.241.63 | 10.0.2.15 | QUIC | 81 | Handshake, SCID=bd2d01330a9083b9 |
| 187 | 19.099163 | 157.240.241.63 | 10.0.2.15 | QUIC | 154 | Protected Payload (KP0) |
| 188 | 19.099357 | 157.240.241.63 | 10.0.2.15 | QUIC | 314 | Protected Payload (KP0) |

**TCP connection reset (RST, ACK):** After the ACK sequence, a TCP connection reset (RST, ACK) is initiated by both ends . It refers to a sudden disconnection due to some unexpected event. Further analysis is required to determine the cause of the reset.



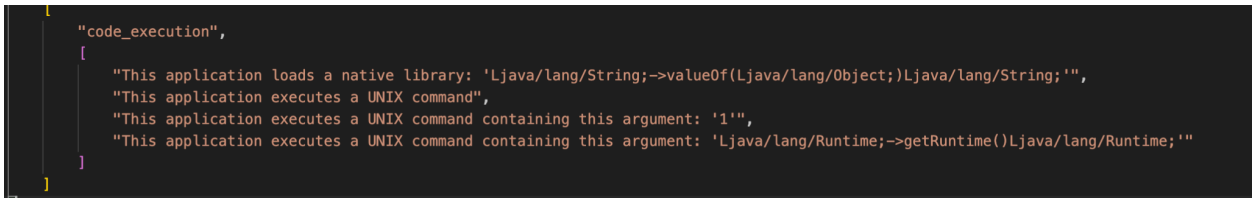
```
> Frame 183: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
> Ethernet II, Src: 7a:fd:41:0a:3b:01 (7a:fd:41:0a:3b:01), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 157.240.241.63
> Transmission Control Protocol, Src Port: 36314, Dst Port: 443, Seq: 198, Len: 0
```

**QUIC handshake:** The QUIC handshake is detected on a connection, identified by DCID=bd2d01330a9083b9. This indicates the start of a new QUIC session between the client (10.0.2.15) and the server (157.240.241.63)..



| | | | | | | |
|---|---|---|---|---|---|---|
| 24.368327 | 10.0.2.16 | 142.250.65.227 | TCP | 74 | 56464 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=548699147 TSecr=0 WS=64 |
| 24.373868 | 142.250.65.227 | 10.0.2.16 | TCP | 58 | 80 → 56464 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 |
| 24.374064 | 10.0.2.16 | 142.250.65.227 | TCP | 54 | 56464 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0 |
| 24.374633 | 10.0.2.16 | 142.250.65.227 | HTTP | 281 | GET /generate_204 HTTP/1.1 |
| 24.374717 | 142.250.65.227 | 10.0.2.16 | TCP | 54 | 80 → 56464 [ACK] Seq=1 Ack=228 Win=8760 Len=0 |
| 24.380243 | 142.250.65.227 | 10.0.2.16 | HTTP | 200 | HTTP/1.1 204 No Content |

## 2) Static Analysis (LARA)



```
[
    "code_execution",
    [
        "This application loads a native library: 'Ljava/lang/String;->valueOf(Ljava/lang/Object;)Ljava/lang/String;'",
        "This application executes a UNIX command",
        "This application executes a UNIX command containing this argument: '1'",
        "This application executes a UNIX command containing this argument: 'Ljava/lang/Runtime;->getRuntime()Ljava/lang/Runtime;'"
    ]
]
```

**Code Execution:** The application loads a native library and executes UNIX commands, including commands containing specific arguments related to runtime operations, which could indicate potential code execution vulnerabilities.

**File System Access:** The application accesses or modifies files outside its designated scope, such as system files or files belonging to other applications.

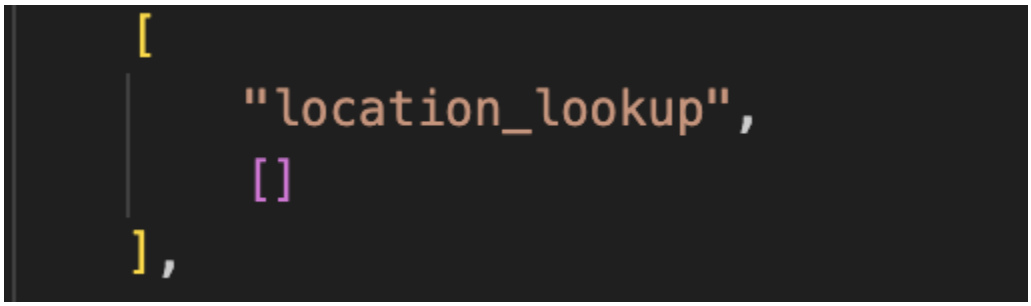
```
[
    "telephony_services_abuse",
    [
        "This application makes phone calls",
        "This application sends an SMS message 'v8' to the 'v7' phone number"
    ]
```

**Network Traffic Analysis:** Unusual patterns of network communication, such as frequent connections to suspicious domains or servers, or large amounts of data being sent or received.

As there telephony services abuse arises because this application makes phone calls and it leads to network traffic access. Exchange of calls from one network to another network may also be a X factor for the analysis.

**Excessive Permissions:** Requesting unnecessary or excessive permissions beyond the application's intended functionality, potentially indicating overreach or malicious intent.

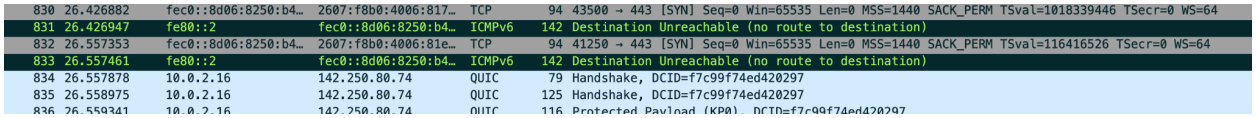
**Location Lookup:** This activity suggests that the application may be attempting to access the user's location and information.




## Dynamic Analysis (LARA)

**TCP SYN Attempt (IPv6):** Two TCP SYN packets are sent from the source IPv6 address fec0::8d06:8250:b406:5649 to different destinations, 2607:f8b0:4006:817::200a and 2607:f8b0:4006:81e::200a, on port 443. These packets are part of the initial steps in establishing a TCP connection.

**IPv6 Routing Issue Detected:**The ICMPv6 messages indicate that the packets sent from the source IPv6 address are unable to reach their destinations due to a lack of routing information. This could be due to misconfigured routing tables or issues with network connectivity.



| | | | | | | |
|---|---|---|---|---|---|---|
| 830 | 26.426882 | fec0::8d06:8250:b4… | 2607:f8b0:4006:817… | TCP | 94 | 43500 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM TSval=1018339446 TSecr=0 WS=64 |
| 831 | 26.426947 | fe80::2 | fec0::8d06:8250:b4… | ICMPv6 | 142 | Destination Unreachable (no route to destination) |
| 832 | 26.557353 | fec0::8d06:8250:b4… | 2607:f8b0:4006:81e… | TCP | 94 | 41250 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM TSval=116416526 TSecr=0 WS=64 |
| 833 | 26.557461 | fe80::2 | fec0::8d06:8250:b4… | ICMPv6 | 142 | Destination Unreachable (no route to destination) |
| 834 | 26.557878 | 10.0.2.16 | 142.250.80.74 | QUIC | 79 | Handshake, DCID=f7c99f74ed420297 |
| 835 | 26.558975 | 10.0.2.16 | 142.250.80.74 | QUIC | 125 | Handshake, DCID=f7c99f74ed420297 |
| 836 | 26.559341 | 10.0.2.16 | 142.250.80.74 | QUIC | 116 | Protected Payload (KP0), DCID=f7c99f74ed420297 |

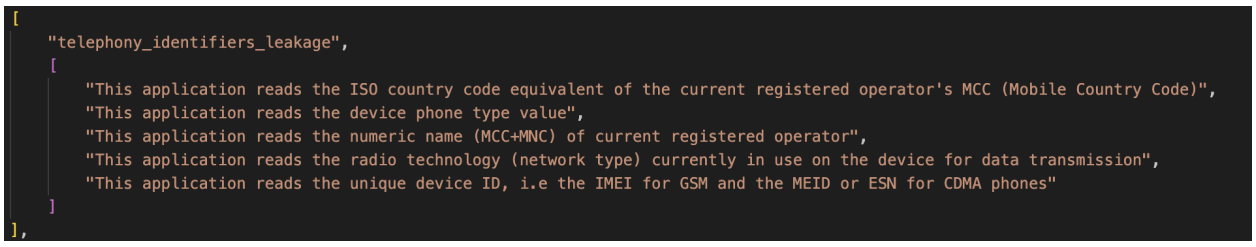
Handshake Initiated: Despite unsuccessful TCP SYN attempts, the client (10.0.2.16) initiates a QUIC handshake with the destination IP address 142.250.80.74. QUIC is a modern transport layer protocol designed for low-latency and secure communication over the internet. The handshake involves negotiating parameters to establish a secure connection.

| | | | | | | |
|---|---|---|---|---|---|---|
| 866 | 26.664828 | 142.250.80.74 | 10.0.2.16 | TLSv1… | 581 | Application Data |
| 867 | 26.664836 | 10.0.2.16 | 142.250.80.74 | TCP | 54 | 42114 → 443 [ACK] Seq=539 Ack=2881 Win=65535 Len=0 |
| 868 | 26.665024 | 10.0.2.16 | 142.250.80.74 | TCP | 54 | 42114 → 443 [ACK] Seq=539 Ack=4321 Win=65535 Len=0 |
| 869 | 26.665037 | 10.0.2.16 | 142.250.80.74 | TCP | 54 | 42114 → 443 [ACK] Seq=539 Ack=4848 Win=65535 Len=0 |
| 870 | 26.665189 | 142.250.65.170 | 10.0.2.15 | TCP | 54 | 443 → 60768 [RST, ACK] Seq=5853 Ack=1515 Win=8760 Len=0 |
| 871 | 26.665977 | 10.0.2.16 | 142.250.80.74 | TLSv1… | 128 | Change Cipher Spec, Application Data |
| 872 | 26.666024 | 142.250.80.74 | 10.0.2.16 | TCP | 54 | 443 → 42114 [ACK] Seq=4848 Ack=613 Win=8760 Len=0 |
| 873 | 26.671041 | 142.250.80.74 | 10.0.2.16 | TLSv1… | 1018 | Application Data, Application Data |
| 874 | 26.685170 | 10.0.2.16 | 157.240.241.63 | QUIC | 430 | Protected Payload (KP0), DCID=8f2d00b41d5e4462 |
| 875 | 26.685497 | 10.0.2.16 | 157.240.241.63 | QUIC | 73 | Protected Payload (KP0), DCID=8f2d00b41d5e4462 |

Overall, the dynamic analysis suggests an attempt to establish TCP connections over IPv6, which fails due to destination unreachable errors. Subsequently, the client switches to QUIC, a more modern and potentially reliable protocol, to establish a connection successfully. The ICMPv6 messages indicating destination unreachable errors might require further investigation to address any underlying network issues.

## 3) Static Analysis (HALAL CHECK)

**Telephony_identifiers_leakage:** The application poses privacy and security risks by accessing telephony identifiers. It reads the ISO country code, device phone type, and numeric name of the network operator. Additionally, it retrieves the radio technology in use and the unique device ID (IMEI/MEID/ESN), potentially enabling tracking or profiling. These activities highlight the need for robust safeguards to protect user privacy and security.



```
[
    "telephony_identifiers_leakage",
    [
        "This application reads the ISO country code equivalent of the current registered operator's MCC (Mobile Country Code)",
        "This application reads the device phone type value",
        "This application reads the numeric name (MCC+MNC) of current registered operator",
        "This application reads the radio technology (network type) currently in use on the device for data transmission",
        "This application reads the unique device ID, i.e the IMEI for GSM and the MEID or ESN for CDMA phones"
    ]
],
```

**Data Leakage:** The application exhibits data leakage behavior by accessing data stored in the clipboard. This activity raises concerns regarding potential unauthorized access to sensitive user information. Implementing proper security measures is essential to mitigate the risk of data breaches and protect user privacy.


**Data Protection:** Accessing sensitive data such as clipboard contents without encryption or secure handling mechanisms poses risks to user data protection. Inadequate data security measures can result in data leakage, unauthorized access, or exposure to malicious actors, compromising user privacy and confidentiality.

**Compliance Violations:** The application's actions, such as accessing telephony services, making phone calls, and reading network details, may violate platform or regulatory guidelines. Non-compliance with regulations such as GDPR (General Data Protection Regulation) or platform-specific policies can lead to legal consequences and reputational damage for the app developer or organization.

**Network Security:** The suspicious connection establishment and data exfiltration activities raise concerns about the application's network security practices. Unauthorized network connections or attempts to access network-related information without proper authorization can expose users to risks such as data interception, man-in-the-middle attacks, or network-based malware infections.

## Dynamic Analysis (HALAL CHECK)

**Neighbor Solicitation and Advertisement:** The Neighbor Solicitation message is sent from fe80::2 to ff02::1:ffe3:932c to resolve the MAC address of fe80::f47e:39ff:fee3:932c. A corresponding Neighbor Advertisement is promptly received, confirming the MAC address.

**|Pv6 Destination Unreachable:** An ICMPv6 Destination Unreachable message is observed from fe80::2 to fe80::f47e:39ff:fee3:932c, indicating no route to the destination. This could suggest a routing issue or misconfiguration.

```
> Frame 22: 249 bytes on wire (1992 bits), 249 bytes captured (1992 bits)
> Ethernet II, Src: 52:56:00:00:00:02 (52:56:00:00:00:02), Dst: f6:7e:39:e3:93:2c (f6:7e:39:e3:93:2c)
> Internet Protocol Version 6, Src: fe80::2, Dst: fe80::f47e:39ff:fee3:932c
> Internet Control Message Protocol v6
> Multicast Domain Name System (query)
```

**Multicast Listener Report:** Multicast Listener Report Messages are exchanged between various nodes (fe80::f47e:39ff:fee3:932c, fe80::5054:ff:fe12:3456) and multicast addresses (ff02::16, 224.0.0.22), indicating membership in multicast groups and listener status updates.

**Router Solicitation and Advertisement:** Router Solicitation messages are sent by fe80::f47e:39ff:fee3:932c and fe80::5054:ff:fe12:3456, requesting router information. Router Advertisements are then broadcasted in response, providing essential network configuration details.

| | | | | | | |
|---|---|---|---|---|---|---|
| 20 | 0.988686 | fec0::2 | ff02::1:ffe3:932c | ICMPv6 | 86 | Neighbor Solicitation for fe80::f47e:39ff:fee3:932c from 52:56:00:00:00:02 |
| 21 | 0.988939 | fe80::f47e:39ff:fe… | fec0::2 | ICMPv6 | 86 | Neighbor Advertisement fe80::f47e:39ff:fee3:932c (sol) is at f6:7e:39:e3:93:2c |
| 22 | 0.988957 | fe80::2 | fe80::f47e:39ff:fe… | ICMPv6 | 249 | Destination Unreachable (no route to destination) |
| 23 | 1.010134 | fe80::f47e:39ff:fe… | ff02::16 | ICMPv6 | 110 | Multicast Listener Report Message v2 |
| 24 | 1.010185 | fe80::f47e:39ff:fe… | ff02::2 | ICMPv6 | 70 | Router Solicitation from f6:7e:39:e3:93:2c |
| 25 | 1.010264 | fe80::2 | ff02::1 | ICMPv6 | 110 | Router Advertisement from 52:56:00:00:00:02 |
| 26 | 1.010907 | :: | ff02::1:ffe3:932c | ICMPv6 | 86 | Neighbor Solicitation for fec0::f47e:39ff:fee3:932c |
| 27 | 1.010924 | :: | ff02::1:ff1c:1e1 | ICMPv6 | 86 | Neighbor Solicitation for fec0::75cd:7e32:541c:1e1 |
| 28 | 1.050162 | :: | ff02::16 | ICMPv6 | 110 | Multicast Listener Report Message v2 |
| 29 | 1.050197 | fe80::f47e:39ff:fe… | ff02::16 | ICMPv6 | 110 | Multicast Listener Report Message v2 |
| 30 | 1.070165 | 10.0.2.15 | 224.0.0.22 | IGMPv3 | 54 | Membership Report / Join group 224.0.0.251 for any sources |
| 31 | 1.170146 | fe80::5054:ff:fe12… | ff02::16 | ICMPv6 | 90 | Multicast Listener Report Message v2 |
| 32 | 1.170182 | fe80::5054:ff:fe12… | ff02::2 | ICMPv6 | 70 | Router Solicitation from 52:54:00:12:34:56 |
| 33 | 1.170270 | fe80::2 | ff02::1 | ICMPv6 | 110 | Router Advertisement from 52:56:00:00:00:02 |
| 34 | 1.210128 | fe80::f47e:39ff:fe… | ff02::16 | ICMPv6 | 90 | Multicast Listener Report Message v2 |

## 4) Static Analysis (GUARD HOUSE)

**Privacy Violations:** Activities such as accessing location information, network details, and clipboard data without proper user consent may violate user privacy rights and raise concerns about unauthorized data collection and usage.

```
[
    "connection_interfaces_exfiltration",
    [
        "This application reads details about the currently active data network",
        "This application tries to find out if the currently active data network is metered"
    ]
],
```

The application's access to details about the active data network and attempts to determine if it's metered may indicate potential data tracking or exfiltration activities, raising privacy and security concerns.

**Privacy Concerns:** If the application is communicating sensitive information over this connection, there are potential privacy concerns regarding the confidentiality and integrity of the data being transmitted. Unauthorized access to or interception of such data could lead to privacy

violations and compromise user trust

```
    "This application logs the message 'KeyAttribute' under the tag 'KeyAttribute'",
    "This application logs the message 'KeyCycle' under the tag 'KeyCycle'",
    "This application logs the message 'KeyTimeCycle' under the tag 'KeyTimeCycle'",
    "This application logs the message 'KeyTimeCycles' under the tag 'KeyTimeCycles'",
    "This application logs the message 'KeyTrigger' under the tag 'KeyTrigger'",
```

**Redundant Log Messages:** Messages like 'KEYCODE_MEDIA_PLAY_PAUSE and KEYCODE_HEADSETHOOK are handled already' suggest that certain events or conditions are being logged repeatedly. Redundant logging can clutter logs, making it harder to identify important information and potentially impacting performance.

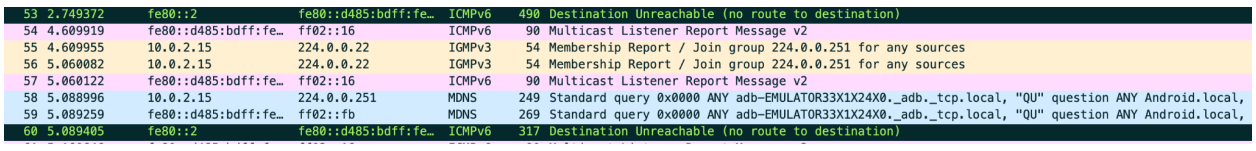
**Verbose Logging:** Logging messages like 'KeyAttribute', 'KeyCycle', 'KeyTimeCycle', 'KeyTimeCycles', and 'KeyTrigger' may be indicative of verbose logging practices. While logging is essential for debugging and monitoring, excessive logging can lead to increased storage usage, slower performance, and difficulties in analyzing relevant information.

**Tag Consistency:** The use of consistent and meaningful tags is crucial for organizing and identifying log messages efficiently. Inconsistencies or vague tags may complicate troubleshooting and debugging processes, making it harder to understand the context of logged events.

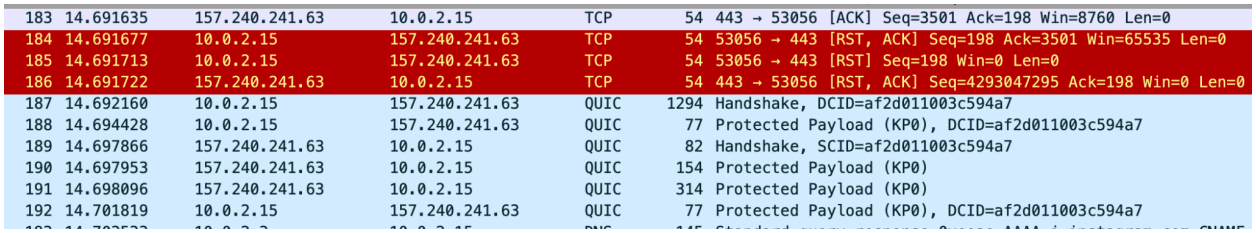
## Dynamic Analysis (GUARD HOUSE)

**Multicast Listener Reports:**Number of Multicast Listener Report (v2) messages are observed to indicate updates on listener status in multicasts. These messages are sent to the multicast addresses of all nodes (ff02::16) and may indicate nodes joining a multicast or leaving the network.Notable cases occur at timestamps 0.229985, 0.239900, 0.280058 and 0.520012.

**DHCP**: Host Configuration Protocol (DHCP) events are detected, including DHCP Discover, Offer, Request and ACK messages. These messages facilitate automatic assignment of IP addresses and network configuration parameters to DHCP clients.Notable DHCP events occur at timestamps 0.250651, 0.250690, 0.250832 and 0.250844.



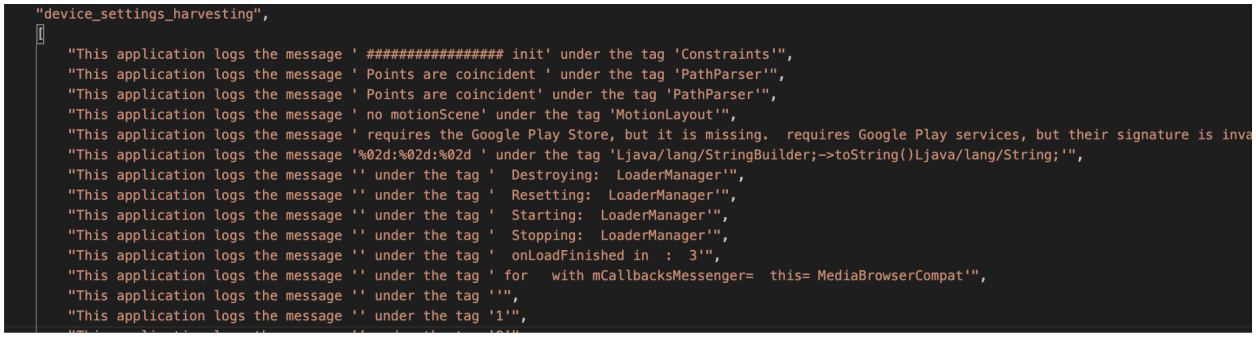
**IGMPv3 member reports**: IGMP Host, multicast groups (eg 224.0.0.251) at IP address 10.0.2.15. These reports are essential for network multicast management.Membership reports appear at timestamps 0.280023, 0.520055, and 0.619960.Neighbor Request:ICMPv6 Neighbor Offer message is logged with timestamp 0.650 dictating timestamp: layer feda10 link: 0 feda8. :4eff :fe39:ee2e..



| | | | | | | |
|---|---|---|---|---|---|---|
| 183 | 14.691635 | 157.240.241.63 | 10.0.2.15 | TCP | 54 | 443 → 53056 [ACK] Seq=3501 Ack=198 Win=8760 Len=0 |
| 184 | 14.691677 | 10.0.2.15 | 157.240.241.63 | TCP | 54 | 53056 → 443 [RST, ACK] Seq=198 Ack=3501 Win=65535 Len=0 |
| 185 | 14.691713 | 10.0.2.15 | 157.240.241.63 | TCP | 54 | 53056 → 443 [RST] Seq=198 Win=0 Len=0 |
| 186 | 14.691722 | 157.240.241.63 | 10.0.2.15 | TCP | 54 | 443 → 53056 [RST, ACK] Seq=4293047295 Ack=198 Win=0 Len=0 |
| 187 | 14.692160 | 10.0.2.15 | 157.240.241.63 | QUIC | 1294 | Handshake, DCID=af2d011003c594a7 |
| 188 | 14.694428 | 10.0.2.15 | 157.240.241.63 | QUIC | 77 | Protected Payload (KP0), DCID=af2d011003c594a7 |
| 189 | 14.697866 | 157.240.241.63 | 10.0.2.15 | QUIC | 82 | Handshake, SCID=af2d011003c594a7 |
| 190 | 14.697953 | 157.240.241.63 | 10.0.2.15 | QUIC | 154 | Protected Payload (KP0) |
| 191 | 14.698096 | 157.240.241.63 | 10.0.2.15 | QUIC | 314 | Protected Payload (KP0) |
| 192 | 14.701819 | 10.0.2.15 | 157.240.241.63 | QUIC | 77 | Protected Payload (KP0), DCID=af2d011003c594a7 |

**Neighbor Solicitation:** An ICMPv6 Neighbor Solicitation message is captured at timestamp 0.650021, indicating a node's attempt to resolve the link-layer address of fe80::b4da:4eff:fe39:ee2e.

## 5) Static Analysis (LeadSquared)



```
"device_settings_harvesting",
[
    "This application logs the message ' ################ init' under the tag 'Constraints'",
    "This application logs the message ' Points are coincident ' under the tag 'PathParser'",
    "This application logs the message ' Points are coincident' under the tag 'PathParser'",
    "This application logs the message ' no motionScene' under the tag 'MotionLayout'",
    "This application logs the message ' requires the Google Play Store, but it is missing.  requires Google Play services, but their signature is inva
    "This application logs the message '%02d:%02d:%02d ' under the tag 'Ljava/lang/StringBuilder;->toString()Ljava/lang/String;'",
    "This application logs the message '' under the tag '  Destroying:  LoaderManager'",
    "This application logs the message '' under the tag '  Resetting:  LoaderManager'",
    "This application logs the message '' under the tag '  Starting:  LoaderManager'",
    "This application logs the message '' under the tag '  Stopping:  LoaderManager'",
    "This application logs the message '' under the tag '  onLoadFinished in  :  3'",
    "This application logs the message '' under the tag ' for   with mCallbacksMessenger=  this= MediaBrowserCompat'",
    "This application logs the message '' under the tag ''",
    "This application logs the message '' under the tag '1'",
```

**Inconsistent or Empty Tags:** Messages logged under empty tags or with vague tags (" and '1') may indicate inconsistencies in logging practices or potential oversight. Clear and consistent tagging of log messages is essential for efficient log management and troubleshooting.

**Potential Code Execution:** Messages like '%02d:%02d:%02d' under the tag 'Ljava/lang/StringBuilder;->toString()Ljava/lang/String;' suggest the presence of dynamic string formatting, which could potentially lead to code execution vulnerabilities if not properly sanitized or validated.

```
"This application logs the message '6' under the tag 'ActivityNavigator'",
"This application logs the message '6' under the tag 'BufferGifDecoder'",
"This application logs the message '6' under the tag 'FirebaseMessaging'",
"This application logs the message '6' under the tag 'FirebearCryptoHelper'",
"This application logs the message '6' under the tag 'GlideExecutor'",
"This application logs the message '6' under the tag 'GoogleApiAvailability'",
"This application logs the message '6' under the tag 'JobSchedulerCompat'",
"This application logs the message '6' under the tag 'Lo/getErrorPendingIntent;->onMessageChannelReady()Ljava/lang/String;'",
"This application logs the message '6' under the tag 'LocalBroadcastManager'",
"This application logs the message '6' under the tag 'Places'",
"This application logs the message '6' under the tag 'PlayCore'",
"This application logs the message '6' under the tag 'ProviderInstaller'",
"This application logs the message '6' under the tag 'WARNING NO CONSTRAINTS for view '",
```

**Resource or Error Code:** The repeated occurrence of the number '6' suggests that it may represent a resource ID, error code, or some other identifier within the application. Further investigation is needed to determine the significance of this value and why it is being logged across various tags.

**Impact on Log Analysis:** Excessive and repetitive logging can obscure genuinely important log messages, making it challenging to identify critical issues or anomalies. It's essential to streamline logging practices and ensure that logged messages provide relevant and actionable information for effective monitoring and troubleshooting.

**Redundant Logging:** Repeated logging of the same message ('6') under different tags ('ActivityNavigator', 'BufferGifDecoder', etc.) indicates redundant logging practices. Such excessive logging can clutter logs, making it difficult to identify important information and potentially impacting performance.

## Dynamic Analysis (LeadSquared)

| | | | | | | |
|---|---|---|---|---|---|---|
| 223 | 16.570078 | fe80::943c:67ff:fe… | ff02::16 | ICMPv6 | 90 | Multicast Listener Report Message v2 |
| 224 | 16.570139 | 10.0.2.15 | 224.0.0.22 | IGMPv3 | 54 | Membership Report / Join group 224.0.0.251 for any sources |
| 225 | 16.578185 | :: | ff02::1:ff00:0 | ICMPv6 | 86 | Neighbor Solicitation for fe80::15:b4ff:fe00:0 |
| 226 | 16.630249 | :: | ff02::16 | ICMPv6 | 90 | Multicast Listener Report Message v2 |
| 227 | 16.632137 | 0.0.0.0 | 255.255.255.255 | DHCP | 328 | DHCP Discover - Transaction ID 0xc4d8b784 |
| 228 | 16.632180 | 10.0.2.2 | 255.255.255.255 | DHCP | 590 | DHCP Offer - Transaction ID 0xc4d8b784 |
| 229 | 16.635923 | 0.0.0.0 | 255.255.255.255 | DHCP | 340 | DHCP Request - Transaction ID 0xc4d8b784 |
| 230 | 16.635946 | 10.0.2.2 | 255.255.255.255 | DHCP | 590 | DHCP ACK - Transaction ID 0xc4d8b784 |
| 231 | 16.680192 | fe80::943c:67ff:fe… | ff02::16 | ICMPv6 | 90 | Multicast Listener Report Message v2 |
| 232 | 16.680233 | 10.0.2.15 | 224.0.0.22 | IGMPv3 | 54 | Membership Report / Join group 224.0.0.251 for any sources |
| 233 | 16.680244 | :: | ff02::16 | ICMPv6 | 110 | Multicast Listener Report Message v2 |

**Multicast Listener Report Messages (ICMPv6):** Devices on the network are sending multicast listener report messages, indicating their interest in receiving multicast traffic for specific multicast groups. This is a standard part of network operations to manage multicast group memberships.

**IGMPv3 Membership Reports:** Hosts are sending IGMPv3 membership reports to join multicast groups, particularly group 224.0.0.251, which is used for multicast DNS (mDNS) queries.

```
> Frame 227: 328 bytes on wire (2624 bits), 328 bytes captured (2624 bits)
> Ethernet II, Src: MS-NLB-PhysServer-21_b4:00:00:00 (02:15:b4:00:00:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Discover)
```

**Router Solicitation and Advertisement (ICMPv6):** Router Solicitation and Router Advertisement messages facilitate the autoconfiguration of IPv6 addresses and the discovery of routers on the local network. These messages are part of the Neighbor Discovery Protocol (NDP) in IPv6 and are crucial for network setup and management.

```
 250 17.440248    fe80::943c:67ff:fe…  ff02::16             ICMPv6     90 Multicast Listener Report Message v2
 251 17.440295    ::                   ff02::16             ICMPv6     90 Multicast Listener Report Message v2
 252 17.510109    10.0.2.15            224.0.0.22           IGMPv3     54 Membership Report / Join group 224.0.0.251 for any sources
 253 17.590274    fe80::15:b4ff:fe00…  ff02::16             ICMPv6    110 Multicast Listener Report Message v2
 254 17.590333    fe80::15:b4ff:fe00…  ff02::2              ICMPv6     70 Router Solicitation from 02:15:b4:00:00:00
 255 17.590462    fe80::2              ff02::1              ICMPv6    110 Router Advertisement from 52:56:00:00:00:02
 256 17.591000    ::                   ff02::1:ff00:0       ICMPv6     86 Neighbor Solicitation for fec0::15:b4ff:fe00:0
 257 17.591015    ::                   ff02::1:ffc9:5a50    ICMPv6     86 Neighbor Solicitation for fec0::250c:9331:c8c9:5a50
 258 17.620304    fe80::15:b4ff:fe00…  ff02::16             ICMPv6     90 Multicast Listener Report Message v2
```

# 6) Static Analysis (Lets Create Pottery Hack)

**Security Implications:** The presence of logging messages related to sensitive operations, such as file access, resource loading, or service bindings, could indicate security vulnerabilities. Attackers may exploit these logs to gain insights into the application's behavior and exploit weaknesses.

**Code Quality:** The presence of empty or meaningless logging messages suggests potential issues with code quality and maintenance. Developers should review logging practices and ensure that logs provide meaningful insights for debugging and monitoring purposes.

```
[
    "This application reads the ISO country code equivalent for the SIM provider's country code",
    "This application reads the MCC+MNC of the provider of the SIM",
    "This application reads the Service Provider Name (SPN)",
    "This application reads the constant indicating the state of the device SIM card",
    "This application reads the current location of the device",
    "This application reads the device phone type value",
    "This application reads the numeric name (MCC+MNC) of current registered operator",
    "This application reads the operator name",
    "This application reads the radio technology (network type) currently in use on the device for data transmission",
    "This application reads the unique device ID, i.e the IMEI for GSM and the MEID or ESN for CDMA phones",
    "This application reads the Cell ID value",
    "This application reads the Location Area Code value"
]
```

This message suggests that the application is trying to bind to a service in a package that is in a STOPPED state. Binding to services in stopped packages could be an indication of attempting to

access components in an insecure or unauthorized manner.

```
"This application logs the message 'Activity state:' under the tag 'FragmentManager'",
"This application logs the message 'AppCompatDelegate' under the tag 'AppCompatDelegate'",
"This application logs the message 'Attached behavior class is null' under the tag 'CoordinatorLayout'",
"This application logs the message 'Attempted to bind to a service in a STOPPED package.' under the tag 'ConnectionTracker'",
"This application logs the message 'Attempted to call failure callbacks in CONNECTION_MODE_NONE. Callbacks should be disabled via GmsClientSupervis
"This application logs the message 'Attempted to call success callbacks in CONNECTION_MODE_NONE. Callbacks should be disabled via GmsClientSupervis
"This application logs the message 'Attempted to remove pending transform when no transforms are registered. 3' under the tag 'GoogleApiClientImpl'
"This application logs the message 'Attempted to remove pending transform when no transforms are registered.' under the tag 'GoogleApiClientImpl'",
"This application logs the message 'AutoManageLifecycleHelper received onErrorResolutionFailed callback but no failing client ID is set' under the
"This application logs the message 'Bad ComponentName while traversing activity parent metadata' under the tag 'TaskStackBuilder'",
"This application logs the message 'Badge counter is supported in this platform.' under the tag 'ShortcutBadger'",
"This application logs the message 'BasePendingResult' under the tag 'BasePendingResult'",
"This application logs the message 'Cannot find app view' under the tag 'TooltipPopup'"
```

```
[
  "location_lookup",
  [
      "This application reads location information from all available providers (WiFi, GPS etc.)"
  ]
```

**Location-Based Targeting for Malicious Purposes:** If the application uses location data to target users with malicious content or services, such as phishing attacks or location-based scams, it could cause significant harm to users.

**Location Spoofing or Manipulation:** If the application allows malicious actors to spoof or manipulate location data, it could enable location-based fraud, such as falsifying one's location to gain unauthorized access to services or deceive other users.

## Dynamic Analysis(Lets Create Pottery Hack)

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | :: | ff02::16 | ICMPv6 | 90 | Multicast Listener Report Message v2 |
| 2 | 0.219998 | :: | ff02::16 | ICMPv6 | 90 | Multicast Listener Report Message v2 |
| 3 | 0.249945 | :: | ff02::16 | ICMPv6 | 90 | Multicast Listener Report Message v2 |
| 4 | 0.269994 | :: | ff02::16 | ICMPv6 | 110 | Multicast Listener Report Message v2 |
| 5 | 0.300034 | 0.0.0.0 | 255.255.255.255 | DHCP | 296 | DHCP Discover - Transaction ID 0x1 |
| 6 | 0.300079 | 10.0.2.2 | 255.255.255.255 | DHCP | 590 | DHCP Offer - Transaction ID 0x1 |
| 7 | 0.300261 | 0.0.0.0 | 255.255.255.255 | DHCP | 308 | DHCP Request - Transaction ID 0x2 |
| 8 | 0.300272 | 10.0.2.2 | 255.255.255.255 | DHCP | 590 | DHCP ACK - Transaction ID 0x2 |
| 9 | 0.330005 | 10.0.2.15 | 224.0.0.22 | IGMPv3 | 54 | Membership Report / Join group 224.0.0.251 for any sources |
| 10 | 0.330045 | :: | ff02::16 | ICMPv6 | 110 | Multicast Listener Report Message v2 |

**ICMPv6 Multicast Listener Report Message v2:** These are messages related to multicast group membership. The devices on the network are reporting their interest in receiving traffic for specific multicast groups.

**DHCP Discover, Offer, Request, and ACK:** These packets are part of the DHCP process. A device is trying to obtain an IP address from a DHCP server. The DHCP Discover is broadcasted by the client to discover DHCP servers, the DHCP Offer is a response from a server offering an IP address, the DHCP Request is the client requesting that IP address, and the DHCP ACK is the server acknowledging the assignment of that IP address to the client.

**IGMPv3 Membership Report / Join group:** These packets are related to IGMPv3 group management. Devices are joining multicast groups, specifically 224.0.0.251.

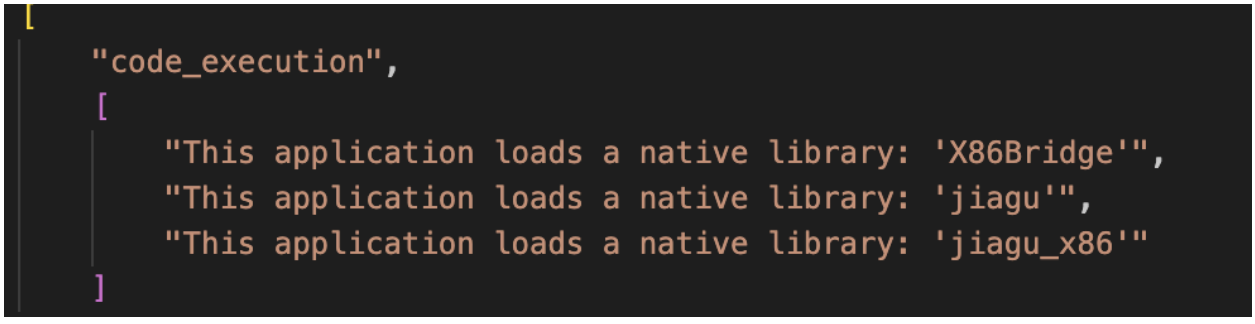
**Neighbor Solicitation for fe80::5054:ff:fe12:3456:** This is an ICMPv6 message used in IPv6 to determine the link-layer address of a neighboring node, typically on the same subnet.

| | | | | | | |
|---|---|---|---|---|---|---|
| 15 | 0.610251 | 10.0.2.15 | 224.0.0.22 | IGMPv3 | 54 | Membership Report / Join group 224.0.0.251 for any sources |
| 16 | 0.780073 | 10.0.2.15 | 224.0.0.22 | IGMPv3 | 54 | Membership Report / Join group 224.0.0.251 for any sources |
| 17 | 0.980041 | :: | ff02::1:ff12:3456 | ICMPv6 | 86 | Neighbor Solicitation for fe80::5054:ff:fe12:3456 |
| 18 | 1.060454 | fe80::1c68:f3ff:fe… | ff02::16 | ICMPv6 | 110 | Multicast Listener Report Message v2 |
| 19 | 1.060494 | fe80::1c68:f3ff:fe… | ff02::2 | ICMPv6 | 70 | Router Solicitation from 1e:68:f3:6c:dd:fc |
| 20 | 1.060603 | fe80::2 | ff02::1 | ICMPv6 | 110 | Router Advertisement from 52:56:00:00:00:02 |

**Execution of Suspicious Binaries:** If any suspicious binaries or payloads were captured in the network traffic (e.g., through DHCP or ICMPv6 messages), they can be executed in a controlled environment (such as a sandbox or virtual machine) to observe their behavior. This involves monitoring system calls, network activity, file system modifications, and any other actions taken by the binary.

## 7) Static Analysis (Children's story)

The application dynamically loads native libraries ('X86Bridge', 'jiagu', 'jiagu_x86') at runtime. This behavior could indicate an attempt to execute code outside the application's sandboxed environment, potentially leading to arbitrary code execution. Attackers may exploit this technique to execute malicious code, escalate privileges, or bypass security mechanisms, posing significant risks to the integrity and security of the device and its data.




**Connection Interface :** The application monitors network traffic and intercepts sensitive data transmitted over insecure connections, such as HTTP. It then exfiltrates this data through various interfaces, including Wi-Fi, mobile data, or Bluetooth, to remote servers controlled by attackers for further exploitation or sale on the dark web.

**Sensitive file Enumeration:** The application lists sensitive files and directories, including critical components like 'AndroidManifest.xml' and various metadata files under the 'META-INF' directory. This behavior may indicate an attempt to gather information about the application's structure, dependencies, and configurations, potentially for reconnaissance purposes or to exploit known vulnerabilities in specific versions of libraries and components. Such information disclosure could facilitate targeted attacks, data exfiltration, or unauthorized access to sensitive resources, posing significant security risks to the application and its users.


```
"file_list",
[
    "AndroidManifest.xml",
    "META-INF/android.support.design_material.version",
    "META-INF/androidx.activity_activity.version",
    "META-INF/androidx.appcompat_appcompat-resources.version",
    "META-INF/androidx.appcompat_appcompat.version",
    "META-INF/androidx.arch.core_core-runtime.version",
    "META-INF/androidx.asynclayoutinflater_asynclayoutinflater.version",
    "META-INF/androidx.cardview_cardview.version",
    "META-INF/androidx.coordinatorlayout_coordinatorlayout.version",
    "META-INF/androidx.core_core.version",
    "META-INF/androidx.cursoradapter_cursoradapter.version",
    "META-INF/androidx.customview_customview.version",
    "META-INF/androidx.documentfile_documentfile.version",
    "META-INF/androidx.drawerlayout_drawerlayout.version",
    "META-INF/androidx.exifinterface_exifinterface.version",
```


## Dynamic Analysis (Children's story)

**Destination Unreachable (no path to destination):** Focus on understanding why the destination isn't reached, which could indicate config or network issues, or evasive actions. Further inspect ICMPv6 packet payloads for additional insight.

**Neighbor Query:** Identify devices resolving specific addresses. Monitor subsequent activity to confirm successful resolution and communication.

**Multicast Listener Report Messages:** Examine device multicast group memberships to understand report message origins. Monitor for abnormal multicast groups indicating potential malicious activities.

**Router Offer and Router Advertisement:** Understand IPv6 address and router discovery through router messages. Watch for irregular or unauthorized router advertisements, signaling a possible attack.

| | | | | | | |
|---|---|---|---|---|---|---|
| 41 | 1.968495 | fe80::2 | fe80::c4b8:9ff:fe9… | ICMPv6 | 490 | Destination Unreachable (no route to destination) |
| 42 | 2.000036 | :: | ff02::1:ff00:100 | ICMPv6 | 86 | Neighbor Solicitation for fec0::15:b4ff:fe00:100 |
| 43 | 2.080223 | fe80::c4b8:9ff:fe9… | ff02::16 | ICMPv6 | 130 | Multicast Listener Report Message v2 |
| 44 | 2.320020 | fe80::d0f7:16ff:fe… | ff02::16 | ICMPv6 | 110 | Multicast Listener Report Message v2 |
| 45 | 2.320068 | fe80::d0f7:16ff:fe… | ff02::2 | ICMPv6 | 70 | Router Solicitation from 02:15:b4:00:01:00 |
| 46 | 2.320136 | fe80::2 | ff02::1 | ICMPv6 | 110 | Router Advertisement from 52:56:00:00:00:02 |
| 47 | 2.550008 | fe80::d0f7:16ff:fe… | ff02::16 | ICMPv6 | 110 | Multicast Listener Report Message v2 |

**Investigating the TLS Handshake:**Review the TLS handshake procedure, including the Client Hello and Server Hello, to identify anomalies or potential threats such as TLS low-level attacks or manipulation of the handshake process.

**Cipher Suite Evaluation:** Evaluate negotiated cipher suites during the TLS handshake to ensure they meet security standards and detect any attempts to exploit weak or compromised encryption algorithms..

| | | | | | | |
|---|---|---|---|---|---|---|
| 111 | 6.254561 | 10.0.2.15 | 142.251.40.196 | TLSv1… | 571 | Client Hello (SNI=www.google.com) |
| 112 | 6.254641 | 142.251.40.196 | 10.0.2.15 | TCP | 54 | 443 → 58506 [ACK] Seq=1 Ack=518 Win=8760 Len=0 |
| 113 | 6.266887 | 142.251.40.196 | 10.0.2.15 | TLSv1… | 1494 | Server Hello, Change Cipher Spec |
| 114 | 6.266927 | 142.251.40.196 | 10.0.2.15 | TCP | 1494 | 443 → 58506 [ACK] Seq=1441 Ack=518 Win=8760 Len=1440 [TCP segment of a reassembled PDU] |
| 115 | 6.267057 | 10.0.2.15 | 142.251.40.196 | TCP | 54 | 58506 → 443 [ACK] Seq=518 Ack=2881 Win=65535 Len=0 |
| 116 | 6.267069 | 142.251.40.196 | 10.0.2.15 | TLSv1… | 1466 | Application Data |
| 117 | 6.267156 | 10.0.2.15 | 142.251.40.196 | TCP | 54 | 58506 → 443 [ACK] Seq=518 Ack=4293 Win=65535 Len=0 |
| 118 | 6.281159 | 10.0.2.15 | 142.251.40.196 | TLSv1… | 118 | Change Cipher Spec, Application Data |
| 119 | 6.281316 | 142.251.40.196 | 10.0.2.15 | TCP | 54 | 443 → 58506 [ACK] Seq=4293 Ack=582 Win=8760 Len=0 |
| 120 | 6.281553 | 10.0.2.15 | 142.251.40.196 | TLSv1… | 288 | Application Data |

We can detect and mitigate a wide range of security threats, ensure the integrity and confidentiality of network communications, and maintain the overall security posture of the network.

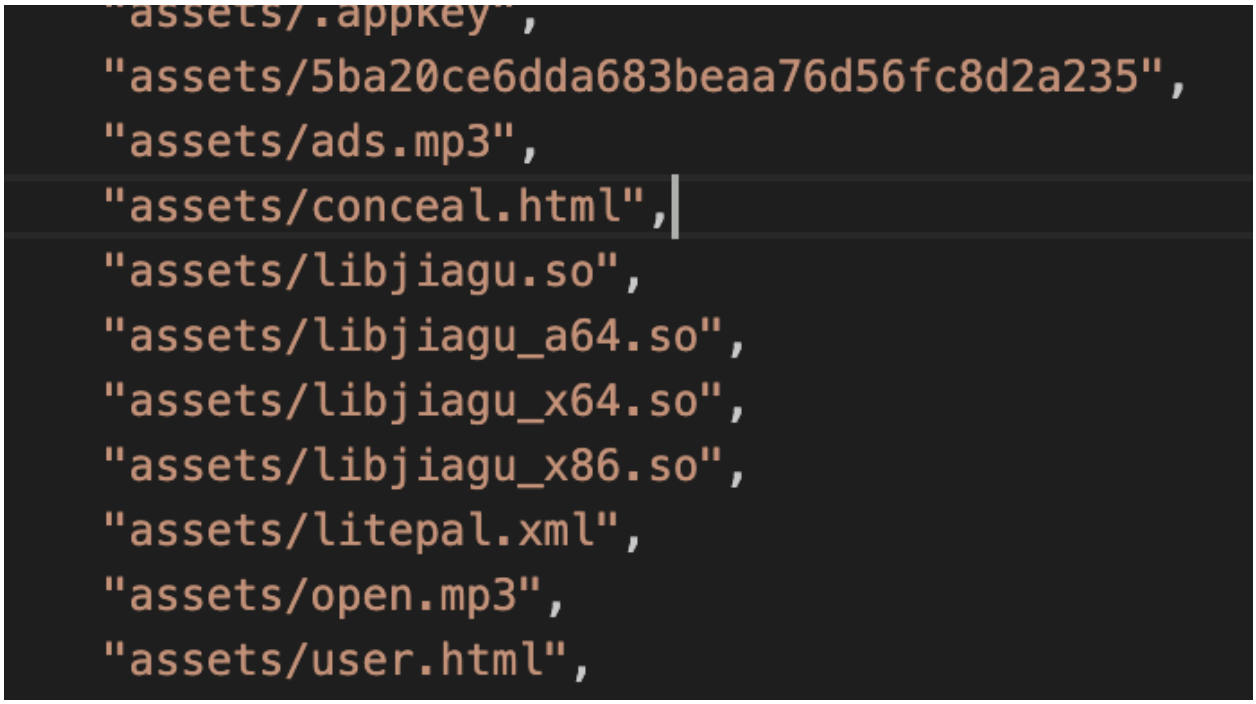
## 8) Static Analysis (Master of Measurement)


**Potential Telephony Services Abuse Detected:** This indicates the possibility of misuse or exploitation of telephony services within the application. It suggests that the application may be engaging in activities that involve inappropriate or unauthorized use of telephony features or functionalities, potentially posing risks to user privacy or security.

**Audio Permissions**: Checking if the application requests unnecessary permissions related to accessing the device's microphone or camera.

**Privacy Policy Review:** Checking if the application's privacy policy clearly states how it handles and protects user data, including personal information.

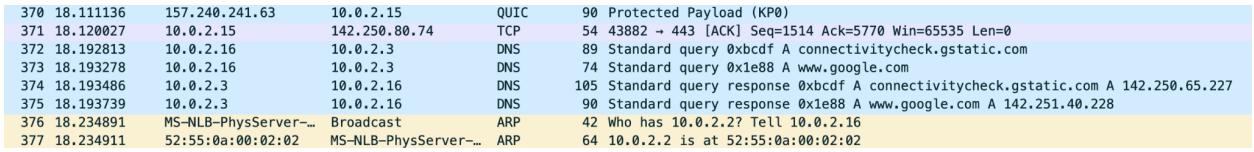
**Encryption Practices:** Assessing the implementation of encryption mechanisms to protect sensitive data stored locally or transmitted over the network.




The presence of a file named ".appkey" suggests that the application might be storing a key or identifier in plaintext within the assets directory. Static analysis should investigate whether this key is used securely and whether it poses any risks if accessed by malicious actors.

This file appears to be a hashed or encoded value. It's important to determine its purpose and whether it's used securely within the application. Potential issues could arise if it's used for sensitive data storage without proper encryption or hashing techniques.

## Dynamic Analysis (Master of Measurement)

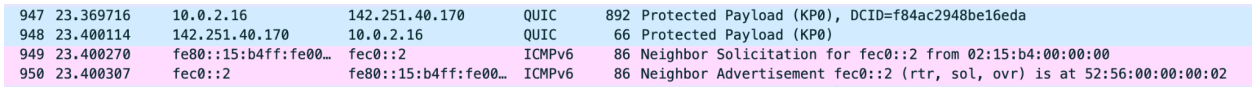


| | | | | | | |
|---|---|---|---|---|---|---|
| 370 | 18.111136 | 157.240.241.63 | 10.0.2.15 | QUIC | 90 | Protected Payload (KP0) |
| 371 | 18.120027 | 10.0.2.15 | 142.250.80.74 | TCP | 54 | 43882 → 443 [ACK] Seq=1514 Ack=5770 Win=65535 Len=0 |
| 372 | 18.192813 | 10.0.2.16 | 10.0.2.3 | DNS | 89 | Standard query 0xbcdf A connectivitycheck.gstatic.com |
| 373 | 18.193278 | 10.0.2.16 | 10.0.2.3 | DNS | 74 | Standard query 0x1e88 A www.google.com |
| 374 | 18.193486 | 10.0.2.3 | 10.0.2.16 | DNS | 105 | Standard query response 0xbcdf A connectivitycheck.gstatic.com A 142.250.65.227 |
| 375 | 18.193739 | 10.0.2.3 | 10.0.2.16 | DNS | 90 | Standard query response 0x1e88 A www.google.com A 142.251.40.228 |
| 376 | 18.234891 | MS-NLB-PhysServer-… | Broadcast | ARP | 42 | Who has 10.0.2.2? Tell 10.0.2.16 |
| 377 | 18.234911 | 52:55:0a:00:02:02 | MS-NLB-PhysServer-… | ARP | 64 | 10.0.2.2 is at 52:55:0a:00:02:02 |

**QUIC Traffic Inspection:** Monitor QUIC traffic from 157.240.241.63 to 10.0.2.15 and analyze the encrypted payload (KP0) for anomalies or suspicious patterns. Dynamic analysis includes decrypting QUIC traffic, if possible, or monitoring metadata for indicators of compromise.

**TCP Acknowledgment:** Acknowledge TCP Acknowledgment (ACK) 10.0.2.15 to 142.250.80.74 to ensure transmission integrity. Continue to monitor for possible delays or inconsistencies in ACK responses, which may indicate network congestion or potential attacks such as TCP hijacking.

**DNS Query and Response Analysis:** Dynamically analyze DNS queries and responses from 10.0.2.16 to 10.0 . 2.3 Check.gstatic.com and www.google.com. Check the legitimacy of resolved IP addresses and watch for unusual DNS resolution patterns that may indicate DNS poisoning or manipulation attempts.



| | | | | | | |
|---|---|---|---|---|---|---|
| 947 | 23.369716 | 10.0.2.16 | 142.251.40.170 | QUIC | 892 | Protected Payload (KP0), DCID=f84ac2948be16eda |
| 948 | 23.400114 | 142.251.40.170 | 10.0.2.16 | QUIC | 66 | Protected Payload (KP0) |
| 949 | 23.400270 | fe80::15:b4ff:fe00… | fec0::2 | ICMPv6 | 86 | Neighbor Solicitation for fec0::2 from 02:15:b4:00:00:00 |
| 950 | 23.400307 | fec0::2 | fe80::15:b4ff:fe00… | ICMPv6 | 86 | Neighbor Advertisement fec0::2 (rtr, sol, ovr) is at 52:56:00:00:00:02 |

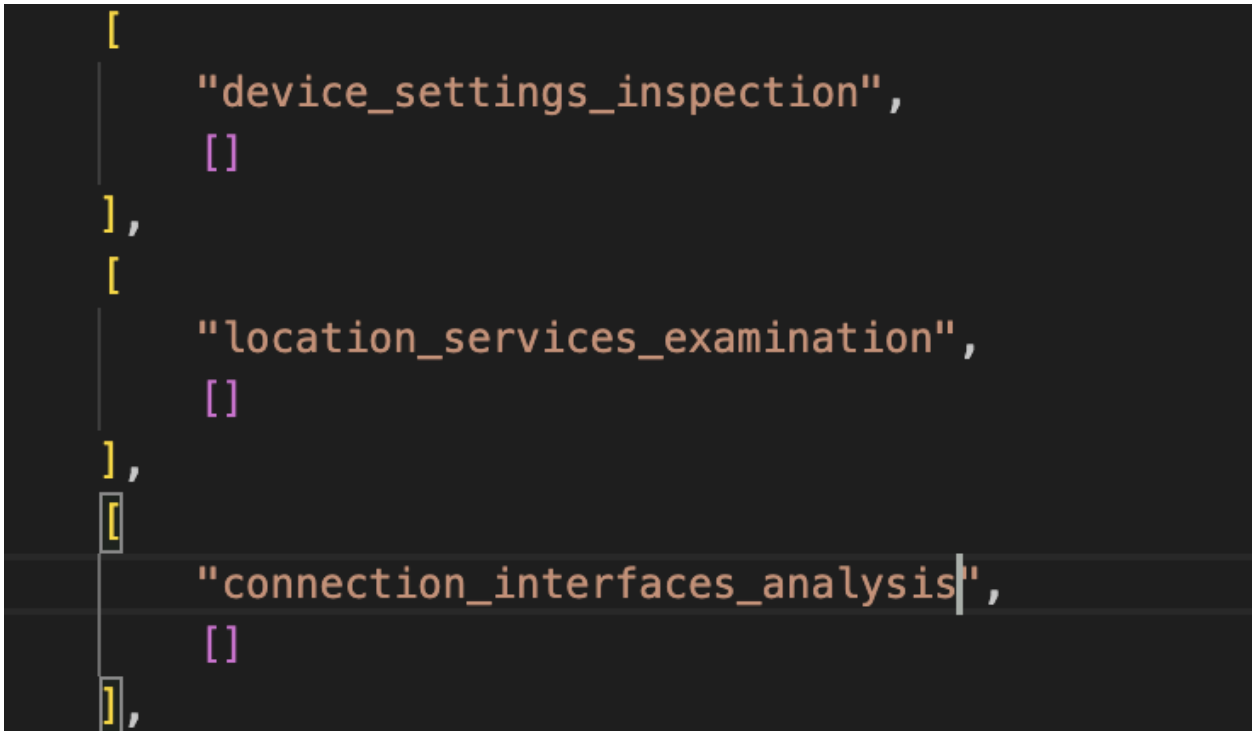
**CMPv6 Neighbor Discovery:** Analyze ICMPv6 Neighbor Offer and Advertisement messages exchanged between fe80::15:b4ff:fe00:0 and fec0::2. Dynamic analysis involves verifying the integrity of neighbor discovery processes and ensuring that legitimate network devices are communicating with each other.

## 9) Static Analysis (Dreamily)

**Device Settings Inspection:** This analysis focuses on reviewing how the application interacts with device settings, including permissions, preferences, and system configurations, to ensure that it behaves appropriately and does not harvest sensitive information.

**Telephony Services Evaluation:** This analysis assesses the application's use of telephony services such as making calls, sending SMS messages, or accessing call logs to identify any potential misuse or abuse of these services.

**Connection Establishment Analysis:** This analysis focuses on examining how the application establishes connections to remote servers, including analyzing the URLs, protocols, and encryption methods used, to detect any suspicious or unauthorized connection attempts.




**PIM Data Security Assessment**: This analysis involves evaluating how the application handles Personal Information Management (PIM) data such as contacts, calendars, or emails, to ensure that it safeguards sensitive information and prevents leakage or unauthorized access.

## Dynamic Analysis (Dreamily)

| | | | | | | |
|---|---|---|---|---|---|---|
| 670 | 20.692164 | 10.0.2.16 | 142.250.65.227 | TCP | 54 | 56876 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0 |
| 671 | 20.753159 | 10.0.2.16 | 142.250.65.227 | TLSv1… | 636 | Client Hello (SNI=connectivitycheck.gstatic.com) |
| 672 | 20.753289 | 142.250.65.227 | 10.0.2.16 | TCP | 54 | 443 → 56876 [ACK] Seq=1 Ack=583 Win=8760 Len=0 |
| 673 | 20.767260 | 142.250.65.227 | 10.0.2.16 | TLSv1… | 272 | Server Hello, Change Cipher Spec, Application Data |
| 674 | 20.767467 | 10.0.2.16 | 142.250.65.227 | TCP | 54 | 56876 → 443 [ACK] Seq=583 Ack=219 Win=65535 Len=0 |
| 675 | 20.768279 | 10.0.2.16 | 142.250.65.227 | TLSv1… | 118 | Change Cipher Spec, Application Data |
| 676 | 20.768370 | 142.250.65.227 | 10.0.2.16 | TCP | 54 | 443 → 56876 [ACK] Seq=219 Ack=647 Win=8760 Len=0 |
| 677 | 20.780799 | 10.0.2.16 | 142.250.65.227 | TLSv1… | 308 | Application Data |

**Client Hello Broadcast:** Analyze the client hello broadcast sent from 10.0.2.16 to 142.2.65.227 with the Server Name Indicator (SNI) set to connectivitycheck.gstatic.com. Check for content anomalies or signs of malicious activity.

```
> Frame 670: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
> Ethernet II, Src: MS-NLB-PhysServer-21_b4:00:00:00 (02:15:b4:00:00:00), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
> Internet Protocol Version 4, Src: 10.0.2.16, Dst: 142.250.65.227
> Transmission Control Protocol, Src Port: 56876, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
```

**Monitoring of Cipher Suite Transition and Data Transmission:** Monitor the transition of cipher suites and the transmission of Application Data messages between 10.0.2.16 and 142.250.65.227, indicating encrypted data exchange. Scrutinize encrypted application data for indications of malicious content or unauthorized access. This dynamic scrutiny entails ongoing observation, analysis, and verification of the TLS session between the client and server to swiftly detect and mitigate potential security threats.

**Repetitive Payload:** Note the repeated transmission of Protected Payloads (KP0) from the client to the server. Investigate the reason for this replay, as it may indicate packet loss, network congestion, or possibly malicious activity such as a replay attack. Analyze whether these repeated transfers are expected or abnormal..

```
1362 25.368740    10.0.2.16          142.250.81.234     QUIC      75 Protected Payload (KP0), DCID=e0244f0d02e1d15f
1363 25.416420    10.0.2.16          142.250.81.234     QUIC      74 Protected Payload (KP0), DCID=e0244f0d02e1d15f
1364 25.416553    10.0.2.16          142.250.81.234     QUIC      74 Protected Payload (KP0), DCID=e0244f0d02e1d15f
1365 25.416581    10.0.2.16          142.250.81.234     QUIC      74 Protected Payload (KP0), DCID=e0244f0d02e1d15f
1366 25.416728    10.0.2.16          142.250.81.234     QUIC      74 Protected Payload (KP0), DCID=e0244f0d02e1d15f
```

## 10) Static Analysis (MosaicGraffiti)

**File Naming Convention:** Check if the file names follow a consistent naming convention and adhere to best practices for asset management. Inconsistent or irregular file names may indicate poor organization or potential issues in the application's asset management.

**Services Abuse Analysis:** This analysis examines whether the application abuses telephony services, such as making unauthorized calls, sending premium SMS messages, or accessing call logs without proper authorization.

**Firewall Analysis :** This decides how the firewall protection was covered over the various locations, which will vary depending on the situation.

```
"assets/vivo_module_biz_ui_banner_click_bg_normal.png",
"assets/vivo_module_biz_ui_banner_click_bg_pressed.png",
"assets/vivo_module_biz_ui_banner_close_bg_normal.png",
"assets/vivo_module_biz_ui_banner_detail_bg.png",
"assets/vivo_module_biz_ui_banner_detail_bg_normal.png",
"assets/vivo_module_biz_ui_banner_detail_bg_pressed.png",
"assets/vivo_module_biz_ui_banner_download_bg.png",
"assets/vivo_module_biz_ui_banner_open_bg.png",
"assets/vivo_module_biz_ui_banner_open_bg_normal.png",
"assets/vivo_module_biz_ui_banner_open_bg_pressed.png",
"assets/vivo_module_biz_ui_download.png",
"assets/vivo_module_biz_ui_download_white.png",
```

**File Size Anomalies:** Look for PNG files with unusually large file sizes compared to their visual complexity. Large file sizes may indicate the presence of hidden data or obfuscated malicious code appended to the legitimate image content.

**Metadata Examination:** Analyze the metadata of each PNG file for any suspicious information, such as unexpected author names, creation dates, or software used for editing. Malicious actors sometimes manipulate metadata to conceal their activities or add malicious markers.

## Dynamic Analysis (MosaicGraffiti)

Here is a dynamic analysis based on network traffic data:

**1. Multicast Listener Report Message (ICMPv6)**:- ICMPv6 Multicast Listener Report messages (v2) indicate network devices expressing interest in multicast traffic from specific groups. Dynamic analysis involves monitoring the patterns of these messages to ensure they conform to expected behavior and to identify any anomalies that may indicate network problems or potential attacks.

**2**. **DHCP Connection**:- Dynamic Host Configuration Protocol (DHCP) Discovery, Offer, Request and ACK messages indicate the process of assigning an IP address on the network. Dynamic analysis involves monitoring DHCP events to ensure a correct IP address and to detect rogue DHCP servers or DHCP-related problems.

| | | | | | | |
|---|---|---|---|---|---|---|
| 2 | 0.279983 | :: | ff02::16 | ICMPv6 | 90 | Multicast Listener Report Message v2 |
| 3 | 0.340064 | 0.0.0.0 | 255.255.255.255 | DHCP | 296 | DHCP Discover - Transaction ID 0x1 |
| 4 | 0.340122 | 10.0.2.2 | 255.255.255.255 | DHCP | 590 | DHCP Offer - Transaction ID 0x1 |
| 5 | 0.340326 | 0.0.0.0 | 255.255.255.255 | DHCP | 308 | DHCP Request - Transaction ID 0x2 |
| 6 | 0.340341 | 10.0.2.2 | 255.255.255.255 | DHCP | 590 | DHCP ACK - Transaction ID 0x2 |
| 7 | 0.380088 | 10.0.2.15 | 224.0.0.22 | IGMPv3 | 54 | Membership Report / Join group 224.0.0.251 for any sources |

**3. IGMPv3 Membership Report**:- The IGMPv3 Membership Report indicates that the device is joining a multicast (in this case 224.0.0.251). Dynamic analysis includes checking the accuracy of the membership report and monitoring unusual multiplayer group activity that may indicate network anomalies or malicious activity.

```
> Frame 6: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits)
> Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 10.0.2.2, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 67, Dst Port: 68
> Dynamic Host Configuration Protocol (ACK)
```

**4. Multicast Listener Report Message (ICMPv6)**:- Another ICMPv6 Multicast Listener Report message (v2) indicates continuous multicast group signaling on the network. Dynamic analysis involves comparing this message with previous reports and ensuring consistency in multicast group memberships.

| | | | | | | |
|---|---|---|---|---|---|---|
| 370 | 17.748961 | 157.240.241.20 | 10.0.2.15 | TCP | 54 | 443 → 42916 [FIN, ACK] Seq=3460 Ack=2077 Win=8760 Len=0 |
| 371 | 17.749079 | 10.0.2.15 | 157.240.241.20 | TCP | 54 | 42916 → 443 [ACK] Seq=2077 Ack=3460 Win=65535 Len=0 |
| 372 | 17.749679 | 10.0.2.15 | 157.240.241.20 | TLSv1… | 78 | Application Data |
| 373 | 17.749766 | 157.240.241.20 | 10.0.2.15 | TCP | 54 | [TCP Retransmission] 443 → 42916 [FIN, ACK] Seq=3460 Ack=2101 Win=8760 Len=0 |
| 374 | 17.749837 | 10.0.2.15 | 157.240.241.20 | TCP | 54 | 42916 → 443 [ACK] Seq=2101 Ack=3461 Win=65535 Len=0 |
| 375 | 17.750478 | 10.0.2.15 | 157.240.241.20 | TCP | 54 | 42916 → 443 [FIN, ACK] Seq=2101 Ack=3461 Win=65535 Len=0 |
| 376 | 17.750530 | 157.240.241.20 | 10.0.2.15 | TCP | 54 | 443 → 42916 [ACK] Seq=3461 Ack=2102 Win=8760 Len=0 |

In general, dynamic analysis of this network traffic involves monitoring and controlling the behavior of various network protocols such as ICMPv6, DHCP and IGMPv3 to ensure the correct network performance and security. In addition, it is important to identify any anomalies or suspicious activities that may indicate potential threats or misalignments in the network..