

NahamCon CTF 2025



Welcome to [NahamCon CTF 2025](#)


Main CTF:

May 23rd, 12:00 PM PST - May 25th, 12:00 PM PST

48-Hour Competition

OSINT

▼ Taken to School

 **Taken to School**
481 points - OSINT - 4 Solved - easy

Author: @Jstith


"I was reading the news this week, and I saw that a student tried to hack a school's computer system!" a worried professor remarked to an IT employee during lunch. "I'm glad we've got people like you keeping our network safe." While Bob the IT admin appreciated the warm comment, his stomach dropped. "Dang it.. I haven't checked that firewall since we set it up months ago!".


IT has pulled a log file of potentially anomalous events detected by the new (albeit poorly tuned) network security software for your school. Based on open-sourced intelligence (OSINT), identify the anomalous entry in the file.

Each log entry contains a single line, including an MD5 hash titled `eventHash`.

The challenge flag is `flag{MD5HASH}` containing the `eventHash` of the anomalous entry.

Download the file(s) below.

Attachments:  `network-log.cel`

 `flag{not_really_tho}` Submit

<https://www.bleepingcomputer.com/news/security/powerschool-hack-exposes-student-teacher-data-from-k-12-districts/>

- Ta được cung cấp 1 file chứa ghi log của palo alto log hoặc gì đó .
- Nó sẽ như vậy ghi mở vscode .

```
network-log.cef X
1 2024-12-22T14:19:23 CEF:0|Gigamon|GigaVUE|9.7|80231|Remote Desktop Logon|8|src=170.170.164.131 dst=192.168.117.111 spt=13678 dpt=3389 proto=
2 2024-12-22T15:51:37 CEF:0|PaloAltoNetworks|PAN-OS|8.1|47617|Suspicious File Download|7|src=12.57.27.150 dst=192.168.112.50 spt=26318 dpt=44
3 2024-12-22T05:49:31 CEF:0|Gigamon|GigaVUE|10.3|84032|Remote Desktop Logon|7|src=199.150.118.18 dst=192.168.117.33 spt=22345 dpt=3389 proto=
4 2024-12-22T08:43:22 CEF:0|Gigamon|GigaVUE|8.2|70636|Network Logon Attempt|4|src=162.72.14.215 dst=192.168.113.242 spt=54601 dpt=445 proto=S
5 2024-12-22T10:59:50 CEF:0|Gigamon|GigaVUE|9.4|85093|Remote Desktop Logon|4|src=205.20.162.94 dst=192.168.114.152 spt=45049 dpt=3389 proto=T
6 2024-12-22T09:27:23 CEF:0|PaloAltoNetworks|PAN-OS|10.4|56863|Trojan Signature Match|8|src=81.9.177.20 dst=192.168.110.1 spt=27655 dpt=443 p
7 2024-12-22T21:54:48 CEF:0|Gigamon|GigaVUE|10.5|75344|Network Logon Attempt|4|src=96.242.29.168 dst=192.168.110.87 spt=11655 dpt=445 proto=S
8 2024-12-22T21:59:52 CEF:0|Gigamon|GigaVUE|9.3|95757|Network Logon Attempt|7|src=131.161.110.244 dst=192.168.111.95 spt=1308 dpt=445 proto=S
9 2024-12-22T11:45:27 CEF:0|Gigamon|GigaVUE|10.8|35149|Network Logon Attempt|4|src=145.116.31.166 dst=192.168.119.50 spt=62728 dpt=445 proto=
10 2024-12-22T02:23:49 CEF:0|PaloAltoNetworks|PAN-OS|8.1|29769|Trojan Signature Match|9|src=184.132.209.115 dst=192.168.114.108 spt=25180 dpt=
11 2024-12-22T02:40:56 CEF:0|PaloAltoNetworks|PAN-OS|9.8|69417|Suspicious File Download|9|src=151.91.215.126 dst=192.168.119.26 spt=44444 dpt=
12 2024-12-22T13:53:19 CEF:0|Gigamon|GigaVUE|8.4|61353|Network Logon Attempt|9|src=97.25.142.133 dst=192.168.114.117 spt=28685 dpt=445 proto=S
13 2024-12-22T03:01:01 CEF:0|PaloAltoNetworks|PAN-OS|9.5|89847|Suspicious File Download|9|src=164.172.84.139 dst=192.168.116.40 spt=1120 dpt=4
14 2024-12-22T05:44:08 CEF:0|Gigamon|GigaVUE|8.9|31370|Remote Desktop Logon|10|src=168.21.191.32 dst=192.168.117.46 spt=9498 dpt=3389 proto=TC
15 2024-12-22T08:25:39 CEF:0|PaloAltoNetworks|PAN-OS|9.4|88867|Trojan Signature Match|6|src=84.94.136.217 dst=192.168.116.170 spt=18126 dpt=44
16 2024-12-22T17:13:22 CEF:0|PaloAltoNetworks|PAN-OS|8.8|98547|Suspicious File Download|9|src=145.12.98.138 dst=192.168.116.251 spt=54718 dpt=
```

- Với gợi ý là chỉ mới gần đây ,khoảng 1 tuần ,
- Và tôi tìm được link bài viết này tại :

<https://www.bleepingcomputer.com/news/security/powerschool-hack-exposed>

PowerSchool hack exposes student, teacher data from K-12 districts

By **Lawrence Abrams**

January 7, 2025 11:26 PM 8



- Xem trong bài viết , thì có một IP đáng ngờ , là **"91.218.50.11"**

This guide and other reports indicate that data was first stolen on December 22, 2024, from IP address **91.218.50.11**. This IP address belongs to a website and virtual hosting company in Ukraine.

```
[Web Handler 215209] 2024-12-22 15:00:50.386 UID=200A0 IP=91.218.50.11 XFF=  
URL=/ws/md/v1/massdata/executeExport/Students_export.csv KV= P=request_locale V=POST  
EX=13e55609d89d40fe87238b301b18f82e
```

```
[Web Handler 476966] 2024-12-23 06:09:47.301 UID=200A0 IP=91.218.50.11 XFF=  
URL=/ws/md/v1/massdata/executeExport/Teachers_export.csv KV= P=request_locale V=POST  
EX=812dc0f05b094ebf8466739b204dda5a
```

Logs showing data exfiltration by the attacker at the 91.218.50.11 ip address


Source: Romy Backus

- Ctrl F trong file log thì chỉ thấy 1 log chứa IP này, kéo qua để xem hash

```
930|Network Logon Attempt|7|src=142.110.94.180 dst=91.218.50.11 spt=26428 dpt=443 proto=HTTPS  
904|Remote Desktop Logon|7|src=120.189.218.22 dst=91.218.50.11 spt=50252 dpt=445 proto=SMB act=detecte  
S|9.9|26429|Trojan Signature Match|6|src=70.198.205.85 dst=192.168.114.155 spt=32412 dpt=3389 proto=TCP act=detec  
410|Network Logon Attempt|4|src=65.213.111.118 dst=192.168.118.87 spt=50252 dpt=445 proto=SMB act=detecte  
9151|Remote Desktop Logon|7|src=86.213.165.226 dst=192.168.116.121 spt=32412 dpt=3389 proto=TCP act=detec  
S|10.2|17915|Spam Rule Matched|7|src=83.66.104.38 dst=192.168.111.215 spt=37722 dpt=443 proto=HTTPS act=d  
S|10.5|35535|Trojan Signature Match|5|src=143.76.180.184 dst=192.168.117.75 spt=17345 dpt=443 proto=HTTPS  
S|10.2|65282|Ransomware Signature Match|4|src=216.76.238.34 dst=192.168.115.221 spt=31880 dpt=443 proto=H  
S|9.7|58324|Trojan Signature Match|9|src=19.199.86.219 dst=192.168.115.119 spt=33751 dpt=443 proto=HTTPS  
S|8.3|44985|Trojan Signature Match|9|src=91.218.50.11 dst=192.168.113.2 spt=27660 dpt=443 proto=HTTPS act  
445|Network Logon Attempt|5|src=130.142.140.231 dst=192.168.114.78 spt=64970 dpt=445 proto=SMB act=quaran  
961|Network Logon Attempt|9|src=109.56.138.63 dst=192.168.118.79 spt=47125 dpt=445 proto=SMB act=allowed
```

eventHash=5b16c7044a22ed3845a0ff408da8afa9

▼ /Sending Mixed Signals

 **Sending Mixed Signals**
480 points · OSINT · 66 Solves · medium

Expires in: 00:18:19 + Extend Reset Stop

Author: @Jstith

Turns out the Houthi PC Small Group was only the tip of the iceberg...

REMINDER: Brute force guessing is NOT permitted.
Press the **Start** button begin this challenge.

Connect with:

- <http://challenge.nahamcon.com:30344>

Submit

- Trong chall này thì không chỉ tìm 1 flag mà ta phải tìm 3 thông tin sau để có được flag chính thức .

Sending Mixed Signals

United States Official Mike Waltz made global headlines in March when he accidentally added an editor of *The Atlantic* to a private Signal group chat with several high-ranking U.S. officials discussing military plans in Yemen ([link](#)). Recently, he made headlines again as a picture of his phone revealed him using a mock-version of the Signal messaging app with glaring cybersecurity vulnerabilities.

Fill in all three answers below:

Part 1:
Find the hard-coded credential in the application used to encrypt log files. (format `JUSTHEDATA`, no quotes)

Part 2:
Find the email address of the developer who added the hard-coded credential from question one to the code base (format `name@email.site`)

Part 3:
Find the first published version of the application that contained the hard-coded credential from question one (case sensitive, format `Word_#.#.#.#####`).

Đề bài nhắc đến “mock-version of the Signal messaging app with glaring cybersecurity vulnerabilities”. Nghĩa là đây không phải bản chính thức của Signal mà một bản “nhái” do bên thứ ba nào đó dựng lên

- Ta thực hiện search trên google để tìm các thứ liên quan đến dữ kiện, ở đây ta dùng **AI perplexity để tìm kiếm trên google nhanh hơn** ,
- Và sau khi tổng hợp nhiều nguồn liên quan, thì tôi phát hiện 1 trang nghi ngờ nhất và tiến hành OSINT trên đó .

link : <https://nvd.nist.gov/vuln/detail/CVE-2025-47730>

CVE-2025-47730 Detail

Exclusively Hosted Service

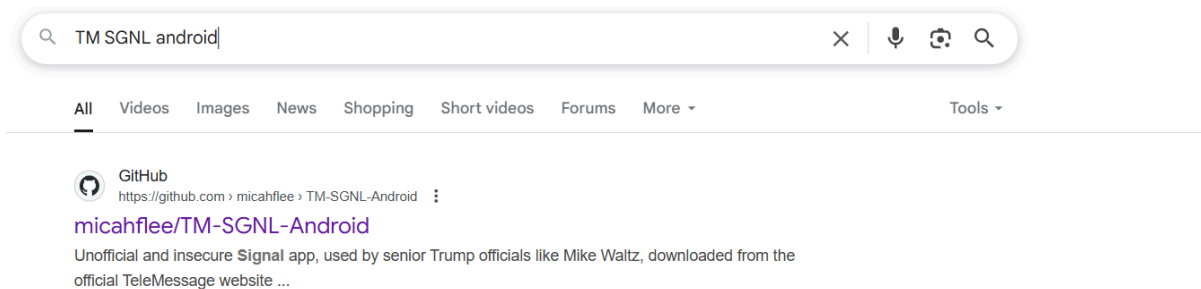
AWAITING ANALYSIS

This CVE record has been marked for NVD enrichment efforts.

Description

The TeleMessage archiving backend through 2025-05-05 accepts API calls (to request an authentication token) from the [TM SGNL \(aka Archive Signal\)](#) app with the credentials of logfile for the user and `enRR8UVVywXYbFkqU#QDPRkO` for the password.

- Trên CVE này, ta có thể thấy rằng có 1 strings nghi ngờ trên này và thông tin còn đang trở về TM SGNL. Search thử nó coi ra cái gì.



- Xuất hiện 1 trang github (TeleMessage – TM)

Đề bài có nhắc rõ

"hard-coded credential in the application used to encrypt log files" → tức là một chuỗi hằng số cố định được nhúng trực tiếp trong mã nguồn.

Định dạng gợi ý (format jUStHEdATA) cho thấy chuỗi này là một biến string hỗn hợp chữ hoa/chữ thường, có ký tự đặc biệt.

▼ Part 1 :

Part 1:

Find the hard-coded credential in the application used to encrypt log files. (format `JUSTHEDATA`, no quotes)

Answer for part 1

enRR8UVVywXYbFkqU#QDPRkO

- Vậy với 2 thông tin trên, thì nhìn vào CVE cũng có mô tả 1 đoạn string tương tự như vậy , nó chính là flag của part 1 này .

gaining system-level permissions.

Fill in all three answers below:

Part 1:

Find the hard-coded credential in the application used to encrypt log files. (format `JUSTHEDATA`, no quotes)

Answer for part 1

Part 2:

Find the email address of the developer who added the hard-coded credential from question one to the code base (format `name@email.site`)

Answer for part 2

Part 3:

Find the first published version of the application that contained the hard-coded credential from question one (case sensitive, format `Word_#.#.#.#####`).

Answer for part 3

Submit

Results:

Part 1: **correct**

Part 2: **incorrect**

Part 3: **incorrect**

▼ Part 2 :

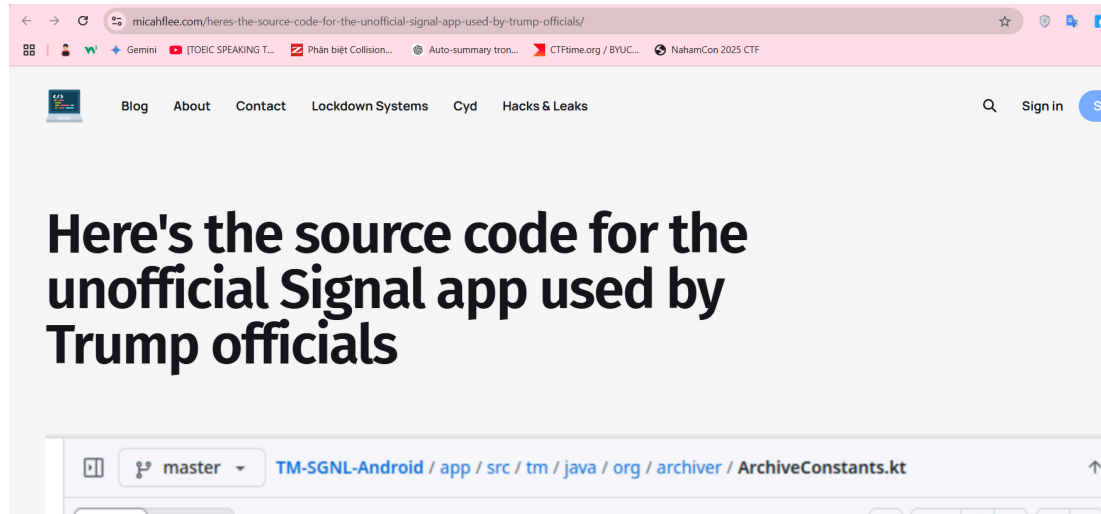
Part 2:

Find the email address of the developer who added the hard-coded credential from question one to the code base (format `name@email.site`)

Answer for part 2

- Tôi có tìm thêm trang liên quan đến repo trên git, 1 bài viết trên ["https://micahflee.com/"](https://micahflee.com/)

<https://micahflee.com/heres-the-source-code-for-the-unofficial-signa>



- Nó có chỉ ra đoạn strings trên part 1 bằng hình ảnh luôn, và còn 1 thông tin quan trọng sau đây :

The Android source code includes a full `.git` folder, with a complete Git history and multiple branches and tags, all of which I have pushed to GitHub. We can see exactly [who contributed what code](#). And while it's not easily viewable from the GitHub interface, if you clone the repo you can see their email addresses – `moti@telemesssage.com`, `shilo@telemesssage.com`, `davidt@telemesssage.com`, etc.

- Thấy rằng 3 thông tin về email đúng với format câu 2 , và 3 email nào cũng được biết đến là người cập nhật repos luôn, ta có thể xem commit trên git xem ai là người đầu tiên, nhưng nó ko giới hạn lượt submit thử nên paste cả 3 vào luôn sẽ **lòi** ra 1 email đúng .

`moti@telemesssage.com`

Part 2:

Find the email address of the developer who added the hard-coded credential from question one to the code base (format `name@email.site`)

Answer for part 2

Part 3:

Find the first published version of the application that contained the hard-coded credential from question one (case sensitive, format `Word_#.#.#.`).

Answer for part 3

Submit

Results:

Part 1: **incorrect**

Part 2: **correct**

▼ **Part 3 :**

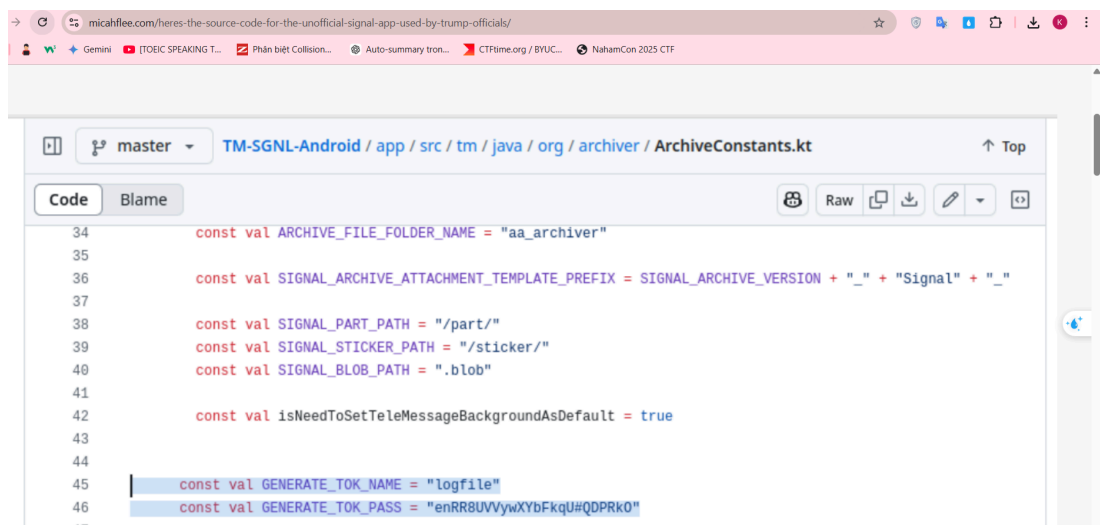
Part 3:

Find the first published version of the application that contained the hard-coded credential from question one (case sensitive, format `Word_#.#.#.`).

Answer for part 3

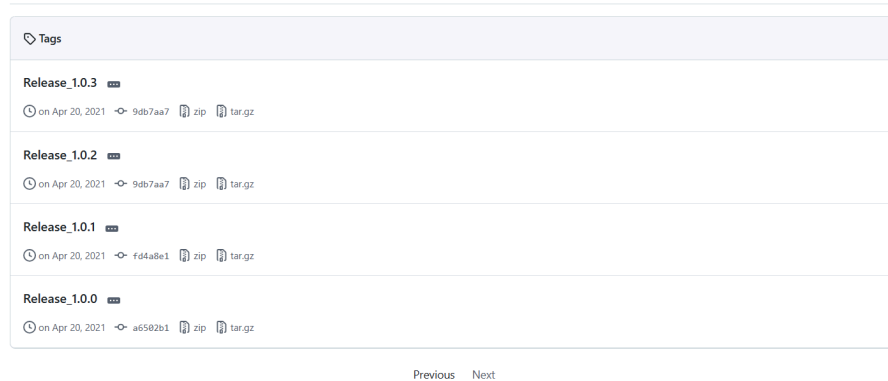
Submit

- Trong **/tag** trong **github** sẽ chứa các **version** và **commit** sau mỗi lần chỉnh sửa trong file code .
- Với đề bài là tìm version nào mà chứa đoạn strings như ở Part 1, thì cách tôi thực hiện là xem commit cũ nhất đến mới nhất, xem cái nào có chứa nội dung đó thì chính là đáp án cho Part 3 .
-

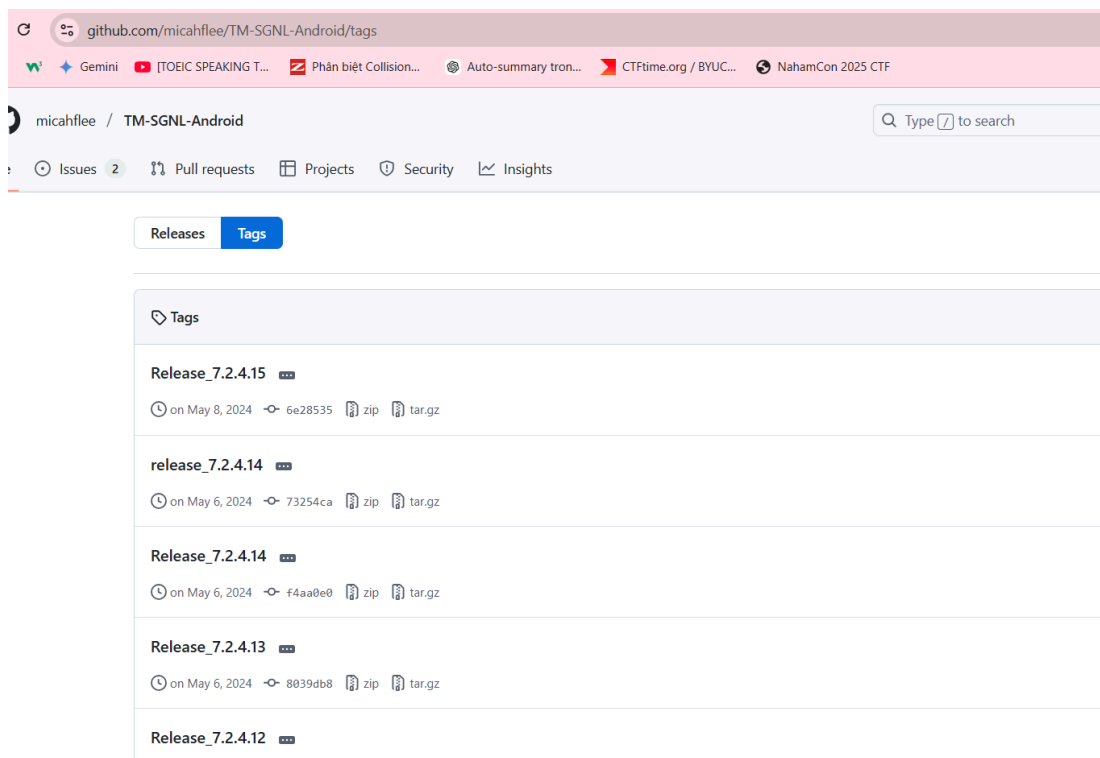


```
34     const val ARCHIVE_FILE_FOLDER_NAME = "aa_archiver"
35
36     const val SIGNAL_ARCHIVE_ATTACHMENT_TEMPLATE_PREFIX = SIGNAL_ARCHIVE_VERSION + "_" + "Signal" + "_"
37
38     const val SIGNAL_PART_PATH = "/part/"
39     const val SIGNAL_STICKER_PATH = "/sticker/"
40     const val SIGNAL_BLOB_PATH = ".blob"
41
42     const val isNeedToSetTeleMessageBackgroundAsDefault = true
43
44
45     const val GENERATE_TOK_NAME = "logfile"
46     const val GENERATE_TOK_PASS = "enRR8UVVywXYbFkqU#QDPRk0"
47
```


- Commit cũ nhất có version là 1.0.0 luôn, vào xem xem có đoạn chỉnh sửa liên quan tới strings không,



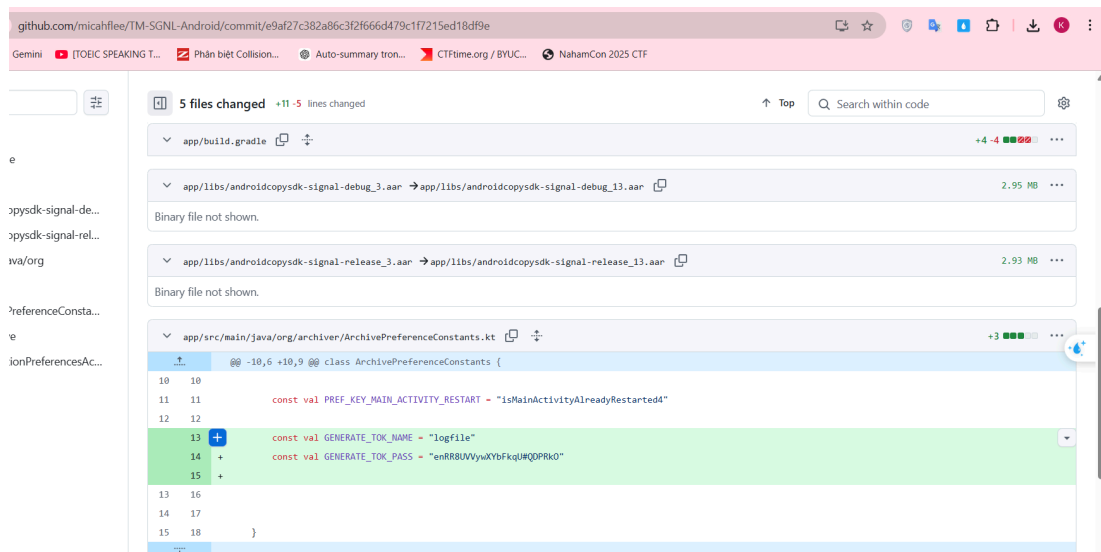
- Vào **commit a6502b1** để check thì ko thấy gì liên quan cả,
- Tôi lần lượt tới các bản cao hơn , cho tới khi bắt gặp bản **Release_5.4.11.20** và mở nó lên xem .



Release_5.4.11.20

on Jun 11, 2021 e9af27c zip tar.gz

- Vào e9af27c và thấy được là có thêm strings part 1 tại đây , chính là version đầu tiên chứ không phải bản 1.0.0 kia .



```
@@ -10,6 +10,9 @@ class ArchivePreferenceConstants {  
10 10  
11 11     const val PREF_KEY_MAIN_ACTIVITY_RESTART = "isMainActivityAlreadyRestarted"  
12 12  
13 13     const val GENERATE_TOK_NAME = "logfile"  
14 14     const val GENERATE_TOK_PASS = "enRR8UVVyuXybFkqUWQOPRk0"  
15 15  
13 16  
14 17  
15 18 }
```

Release_5.4.11.20

Part 3:

Find the first published version of the application that contained the hard-coded credential from question one (case sensitive, format `Word_#.#.#.`).

Answer for part 3

Submit

Results:

Part 1: **incorrect**

Part 2: **incorrect**

Part 3: **correct**

- Tổng hợp và submit đúng cùng lúc 3 flag thì sẽ có được flag.

Results:

Part 1: **correct**

Part 2: **correct**

Part 3: **correct**

Congrats! Here's the flag: `flag{96143e18131e48f4c937719992b742d7}`



Sending Mixed Signals

469 points - OSINT - 81 Solves - **medium**

Start