

**Building Overview:**

- Security officers are stationed at the entrance throughout the executive hallway
- There are (2) entrances to the Superintendent's office:
  - The main entrance is through the executive suite
    - The Superintendent's executive secretary's office is an anteroom and as a result anyone entering the Superintendent's office must pass through the executive secretary's office first
  - In addition, there is a side door to the Superintendent's office that is accessible through the kitchenette in the executive hallway
    - That door is not monitored or locked and could be conceivably accessed by anyone

**Technology:**

- The television in question in the Superintendent's office is a Samsung TV
  - Samsung TV Plus is the platform for the channels
  - It does not have any external sources like an Apple TV or Firestick
  - OMES and the Oklahoma County Sheriff's Office were both at OSDE yesterday and inspected all associated devices in question
  - Additionally, they have conducted multiple interviews including one with Superintendent Walters
  - After meeting with OMES yesterday, it was their belief that there is not a way that someone could stream or airplay to the Superintendent's Samsung TV
  - At no point during the day did the Superintendent log into any platform with any personal login for streaming services
  - None of the Superintendent's devices (personal or otherwise) have ever been connected to the TV
  - Samsung customer service has advised that it is not possible to recover a log of the TV's history nor is it possible to recover the television programming guide for the day of the board meeting

**Board Day:**

- On the day of the board meeting, as is standard practice, Oklahoma Highway Patrol met the Superintendent in the parking lot and walked him into the Department of Education
- Once inside, the general counsel, acting board secretary, and chief of staff met with the Superintendent in his office immediately preceding the SBE meeting, approximately 9:05am CDT
  - This meeting lasted approximately 5 minutes, at which time the parties left the office and the SBE meeting began
- The open meeting started at 9:34am CDT and lasted one hour and fifty-two minutes, at which time the regular meeting adjourned into executive session at 11:06am CDT
- The Superintendent and the board's acting secretary entered the Superintendent's office first

- The Superintendent's office secretary was already in the office setting up for lunch
- The acting board executive secretary noticed that the TV was on Fox News
- A parent who was in Executive Session for a transfer appeal stated via e-mail that there was "nothing but professionalism" (see attached)
- There were 24 members of the public who signed into the meeting
- There were 13 members of the media present
- There were 7 state troopers present
- As a result of the law enforcement questioning, the Superintendent Walters was never alone in the State Department without someone else (law enforcement, staff, fellow board members) the entire day of the board meeting



**Subject:** FW: OMES Inspection of Devices

**From:** Dan Cronin <[Dan.Cronin@omes.ok.gov](mailto:Dan.Cronin@omes.ok.gov)>  
**Sent:** Monday, July 28, 2025 1:40:30 PM  
**To:** Lexie Flanagan <[Lexie.Flanagan@sde.ok.gov](mailto:Lexie.Flanagan@sde.ok.gov)>  
**Subject:** Re: OMES Inspection of Devices

Hi Lexie,

That time works for us, thank you for the fast response.

Thank you,

**Dan Cronin | State Chief Information Officer**  
State of Oklahoma | Office of Management and Enterprise Services  
405-522-6268 |  
[oklahoma.gov](http://oklahoma.gov) | [oklahoma.gov](http://oklahoma.gov)



---

**From:** Lexie Flanagan <[Lexie.Flanagan@sde.ok.gov](mailto:Lexie.Flanagan@sde.ok.gov)>  
**Date:** Monday, July 28, 2025 at 11:28 AM  
**To:** Dan Cronin <[Dan.Cronin@omes.ok.gov](mailto:Dan.Cronin@omes.ok.gov)>  
**Subject:** FW: OMES Inspection of Devices

Hi Dan,

4 PM this afternoon works on our end for you to come by our offices and inspect the Samsung TV (with OSDE serial number **E14404**) in the main area of the Superintendent's office.

Thank you,

**Lexie Flanagan**  
Executive Assistant to the Superintendent, Ryan Walters  
Oklahoma State Department of Education  
2500 N Lincoln Blvd  
Oklahoma City, OK 73105  
Office: (405) 521-4885



**OKLAHOMA**  
Education

---

**From:** Dan Cronin <[Dan.Cronin@omes.ok.gov](mailto:Dan.Cronin@omes.ok.gov)>  
**Sent:** Monday, July 28, 2025 10:18 AM  
**To:** Ryan Walters <[Ryan.Walters@sde.ok.gov](mailto:Ryan.Walters@sde.ok.gov)>  
**Subject:** OMES Inspection of Devices

Hi Superintendent Walters,

I was asked by the OMES general counsel to get with you to inspect a few devices in your office area. Can you please let me know which devices you would like us to inspect so I can bring the appropriate IT staff to assist. We can make this our top priority to align to your schedule.

If you can provide the list of equipment and the best time to visit it would be very helpful.

Thank you,

**Dan Cronin | State Chief Information Officer**  
State of Oklahoma | Office of Management and Enterprise Services  
405-522-6268 |  
[oklahoma.gov](http://oklahoma.gov) | [oklahoma.gov/](http://oklahoma.gov/)



**OKLAHOMA**





## **Incident Investigation**

July 30, 2025

Prepared for

Dan Cronin

Office of Management and Enterprise Services

Prepared by:

**Alias Cybersecurity**

4308 Grant Blvd  
Yukon, OK 73099

(405) 261-9517

Privileged and Confidential



# Contents

|                                      |   |
|--------------------------------------|---|
| Contents .....                       | 2 |
| About Alias .....                    | 3 |
| Confidentiality Notice .....         | 3 |
| Disclaimer .....                     | 3 |
| Authorization .....                  | 3 |
| Executive Summary .....              | 4 |
| Engagement Overview .....            | 4 |
| Key Observations .....               | 4 |
| Recommended Next Steps .....         | 4 |
| Scope .....                          | 5 |
| Methodology .....                    | 5 |
| Findings .....                       | 6 |
| Detailed Findings/Observations ..... | 7 |
| Conclusion .....                     | 8 |
| Figure Documentation .....           | 9 |



## About Alias

Alias Cybersecurity (Alias Forensics, Inc.) is a privately held digital forensics firm established in 2010, specializing in the identification, preservation, analysis, and reporting of digital evidence. The Alias team brings over 30 years of combined experience in conducting forensic examinations across a wide range of digital media and platforms, including mobile devices, computers, cloud environments, and embedded systems. Examiners at Alias hold recognized industry certifications and have led or supported hundreds of forensic investigations—ranging from internal corporate matters to complex litigation support serving clients from small businesses to Fortune 500 companies and members of Forbes' list of America's Largest Private Companies. The team adheres to strict chain-of-custody protocols and uses validated forensic methodologies to ensure the integrity and admissibility of all findings.

## Confidentiality Notice

*This investigative report contains sensitive, privileged, and confidential information. Appropriate measures should be taken to protect the confidentiality and integrity of the information contained herein. Unauthorized disclosure or distribution of this report may cause reputational harm or increase the risk of further compromise. Alias Cybersecurity shall not be held liable for any special, incidental, collateral, or consequential damage arising from the use or dissemination of the information in this report.*

## Disclaimer

*This investigative report reflects the findings based on information available and accessible at the time of the investigation. It is a summary of evidence collected, and observations made during a specific point in time. The accuracy and completeness of the findings may be affected by changes made to systems, data, or personnel access during or after the investigation period. As such, this report may not capture all relevant activity or indicators that existed outside the scope or timeframe of the investigation.*

## Authorization

Alias Cybersecurity (Alias Forensics, Inc.) conducted this investigation with the full knowledge and consent of the authorized party. Permission to access, inspect, and analyze the identified electronic devices was granted by Dan Cronin, CIO, State of Oklahoma, Office of Management and Enterprise Services, who provided authorization on behalf of the investigative authority. All work was performed within the agreed scope of engagement and under the boundaries of the provided consent.



# Executive Summary

## Engagement Overview

This engagement was conducted to support an active investigation by performing a forensic examination of a smart television to assess whether it was possible to determine what content may have been displayed during a specific timeframe in the recent past, and to identify the source of that content.

Alias Cybersecurity investigators examined the physical configuration of the television, documented all connected devices—including HDMI inputs, coaxial connections, and network interfaces—and reviewed internal system settings and smart application configurations. The goal was to identify any available data related to device usage, content access, and potential sources such as streaming services, screen-mirroring features, or external input devices.

The examination was conducted in a forensically sound manner by qualified forensic analysts from Alias Cybersecurity. Findings from this analysis are intended to inform the broader investigation by establishing whether relevant viewing activity could be verified or ruled out based on available system data, peripheral connections, and usage history.

## Key Observations

During the course of the forensic examination, Alias Cybersecurity reviewed the smart television's physical configuration, connected devices, system logs, and smart application settings to identify any traces of content that may have been displayed or accessed. While the investigation confirmed the presence of various applications and devices capable of displaying streaming or stored media, no definitive artifacts were identified that could conclusively verify whether specific content was—or was not—displayed on the television.

The device's limited logging capabilities and lack of retained viewing or playback history prevented the ability to verify whether specific media had been accessed. As a result, no conclusive evidence was identified to either confirm or deny that particular content was displayed on the television during the timeframe of interest.

## Recommended Next Steps

While the forensic analysis of the smart television did not yield conclusive evidence regarding the display of specific content during the timeframe in question, the device's configuration indicated that remote casting and screen-sharing features, such as Apple AirPlay, were enabled. This suggests that content could have been transmitted to the television from an external device without leaving a persistent record on the TV itself.

To further investigate and determine what may have been displayed on the television, the following steps are recommended:



1. Interview individuals who were present in the room at the time of the alleged incident. Firsthand accounts may help establish what was observed on the screen and provide important context that cannot be recovered through technical examination.
2. Identify any computers, mobile devices, or tablets that were in the room or within wireless range of the television during the relevant timeframe. Devices in physical proximity to the television may have been used to cast or mirror content.
3. Perform a forensic examination of those identified devices. The analysis should focus on identifying application logs, casting history, AirPlay connections, or other artifacts that may indicate whether media consistent with the reported incident was transmitted to the television.
4. Conduct a forensic examination of the user account **mendy.hooks@sde.ok.gov** to identify any activity related to its use on the Samsung television or associated smart TV applications.
5. Conduct a forensic examination of relevant user accounts belonging to individuals who were present in the room or within wireless range of the television at the time of the incident.

Following these steps may help uncover additional evidence or context necessary to determine whether the television was used to display specific content relevant to the investigation.

## Scope

The investigation was performed at:

Oklahoma State Department of Education  
Oliver Hodge Building  
2500 North Lincoln Boulevard  
Oklahoma City, Oklahoma 73105

## Methodology

Alias Cybersecurity conducted a physical examination of a smart television to identify any accessible information related to content usage, device configuration, and connected peripherals. The assessment was performed on-site by two forensic investigators using a non-invasive approach.

The investigators manually navigated through all available menu items, settings, and application interfaces to evaluate system configurations and review any visible indicators of past activity. No tools were used to extract data from internal storage or system memory. The focus of this investigation was limited to direct observation and documentation of what could be visually confirmed through the television's user interface.

All investigative steps were thoroughly documented using photographs and video recordings to preserve the state of the device at the time of the examination.



#### Steps Performed

- Conducted a physical inspection of the television and noted any connected peripherals or cables.
- Manually navigated available menu items and system settings.
- Reviewed installed applications, input sources, and system information for indications of usage or content access.
- Visually documented the investigation process with photographs and video to preserve evidence and support findings.
- Maintained a non-invasive approach, with no changes made to the device configuration or settings.

## Findings

#### Examined Device Details

- Make: Samsung
- Model: UN55TU8300FXZA
- Serial Number: 0AQP3CZW902443X
- Type: 55" Class Crystal UHD TU830 (2020) (internet Lookup based on model number)
  
- Software Version: T-NKLAKUC-2700.6, BT - S
- Status code : 20401\_AD3\_Z
- Sub-micom version: T-NLINTV-1005
- E-manual Version: NIKATSCT-4.5.0
  
- Wired Mac address = C8:12:0B:78:A5:C9
- Wireless Mac Address = 68:FC:CA:B7:2D:5A
- Bluetooth Address = 68:FC:CA:B7:2D:5B
- Smart Control Bluetooth Address = 68:FC:CA:4D:05:49

#### Connected Devices at Time of Examination:

- Cox Cable Box – Connected via HDMI
- Sony DVD Player – Connected via HDMI
- VHF/UHF indoor dipole antenna (Rabbit Ears)– Connected via coaxial input



# Detailed Findings/Observations

## 1. Device Input and Operating Mode

- At the time of examination, the television's input source was set to "TV" (Figure 8), indicating it was operating in the default Samsung Smart TV Application.
- When initially powered on, the television displayed Samsung TV Plus Channel 1204 (Movie Hub Action) (Figure 7).
- Additional source inputs were reviewed, including:
  - HDMI 1 (connected to a Cox cable box)
  - HDMI 2 (connected to a Sony DVD player)
  - Remote Access features including Office 365, Remote PC, and Screen Sharing (Figures 23–26, 18).

## 2. Connected Devices and Peripherals

- The television was physically connected to three input sources (Figures 1–5):
  - Cox cable box via HDMI (confirmed powered on, Figure 4)
  - Sony DVD player via HDMI
  - Rabbit ear-style antenna via coaxial input
- When switched to HDMI 1, the Cox cable box began playing Newsmax Channel (Figure 27).
- The Cox cable box remote was not functioning reliably; a fresh set of batteries was installed to facilitate easier access to and verification of the device's configuration settings. (Figure 37)
- Cox cable box settings showed that parental controls were not enabled (Figures 28–29).
- The TV's back panel included an Ethernet port, though the device was connected via Wi-Fi at the time of examination (Figure 6).

## 3. Network Connectivity

- The television was connected to the wireless network "oklahoma\_open" (Figure 9).
- Network configuration details were captured (Figure 10), including:
  - IP Address
  - Subnet Mask
  - Default Gateway
  - DNS Server
  - DHCP Enabled
- The TV was configured to automatically obtain its network settings (DHCP).

## 4. Wireless Casting / Streaming Configuration

- Apple AirPlay was enabled on the television and required a code upon first connection (Figure 11), providing basic pairing security.
- An examination phone connected to the same Wi-Fi network (oklahoma\_open, Figure 33) attempted to cast using the "Cast to Device" button but did not detect the Samsung TV (Figure 34).
- A test PC was also connected to the network (Figure 35), and a brief network scan of a portion of the oklahoma\_open network was conducted. No visible hosts were found, due to network isolation or access controls (Figure 36).



#### 5. Device Identification and System Information

- The TV was identified as “Samsung 8 Series (55)” in the System Manager menu (Figure 12).
- The “About TV” screen provided the following information (Figure 13):
  - Model Code
  - Serial Number
  - TVkey Device ID
  - Software Version
  - Status Code
- These values were documented for forensic records.
- The AirPlay software version was also recorded (Figure 20).
- System event logs were accessed via the “About TV” settings (Figure 19).

#### 6. Application Access and User Account Activity

- Mr. Walters stated that Fox News is typically accessed through the TV’s default apps screen (Figure 14).
- Selecting “The Will Cain Show” triggered launch of the YouTube TV app (Figure 15), where the user “Mendy” was actively signed in.
- The home screen and settings menus confirmed the signed-in user account: mendy.hooks@sde.ok.gov (Figures 16, 21).

#### 7. System Configuration and Content Controls

- Parental control settings for the Samsung TV were turned off, allowing unrestricted content (Figure 22).
- The search function offered predictive text suggestions but contained no usable search history (Figures 30–31).
- The Samsung TV app “Guide” was accessed and showed the available live channels and programming schedule (Figure 32).

## Conclusion

Due to the device’s limited logging functionality and the absence of any retained viewing or playback history, it was not possible to determine whether specific media content had been accessed or displayed. This lack of historical data significantly constrained the scope of the forensic analysis. Consequently, no definitive evidence could be established to either confirm or refute the viewing of particular content on the television during the timeframe in question. Without corroborating logs or playback records, the investigation remains inconclusive regarding media activity on the device.



## Figure Documentation

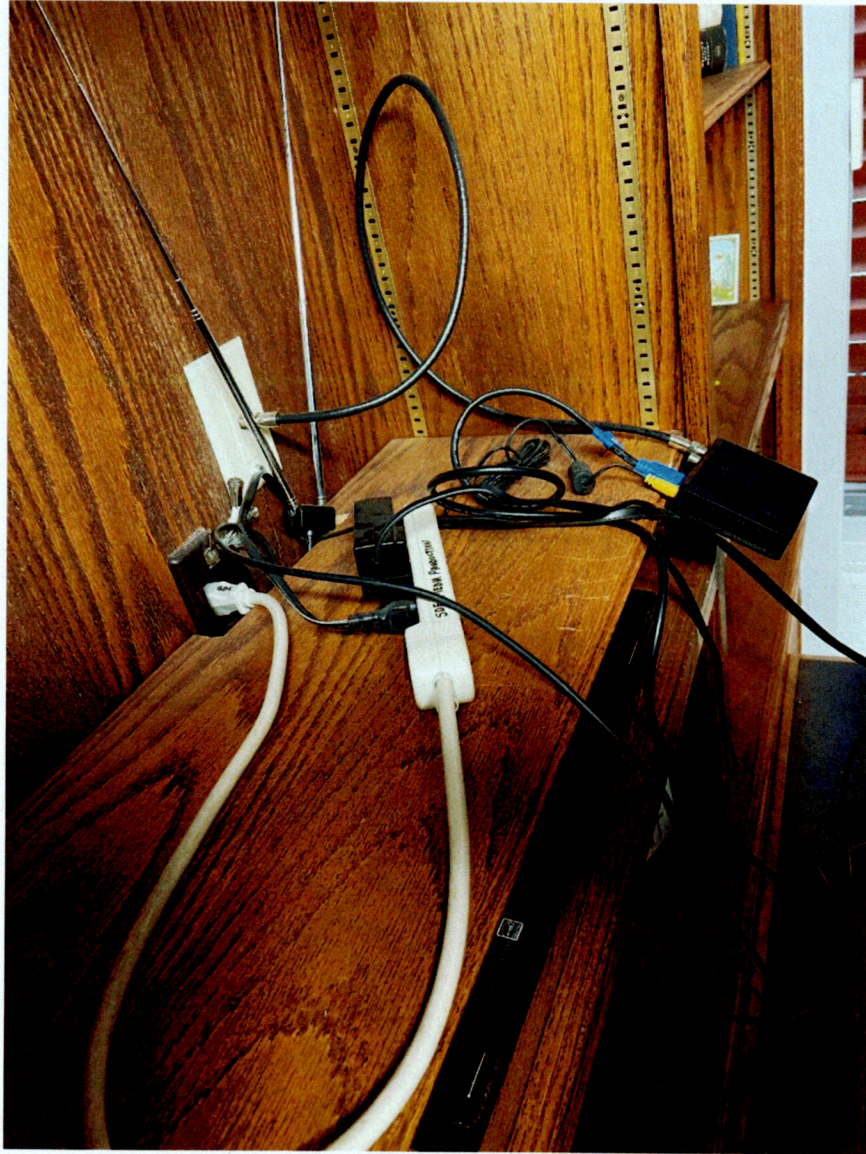


Figure 1: DVD Player, Cox Cable Box, and Rabbit Ear Antenna connected to the TV.



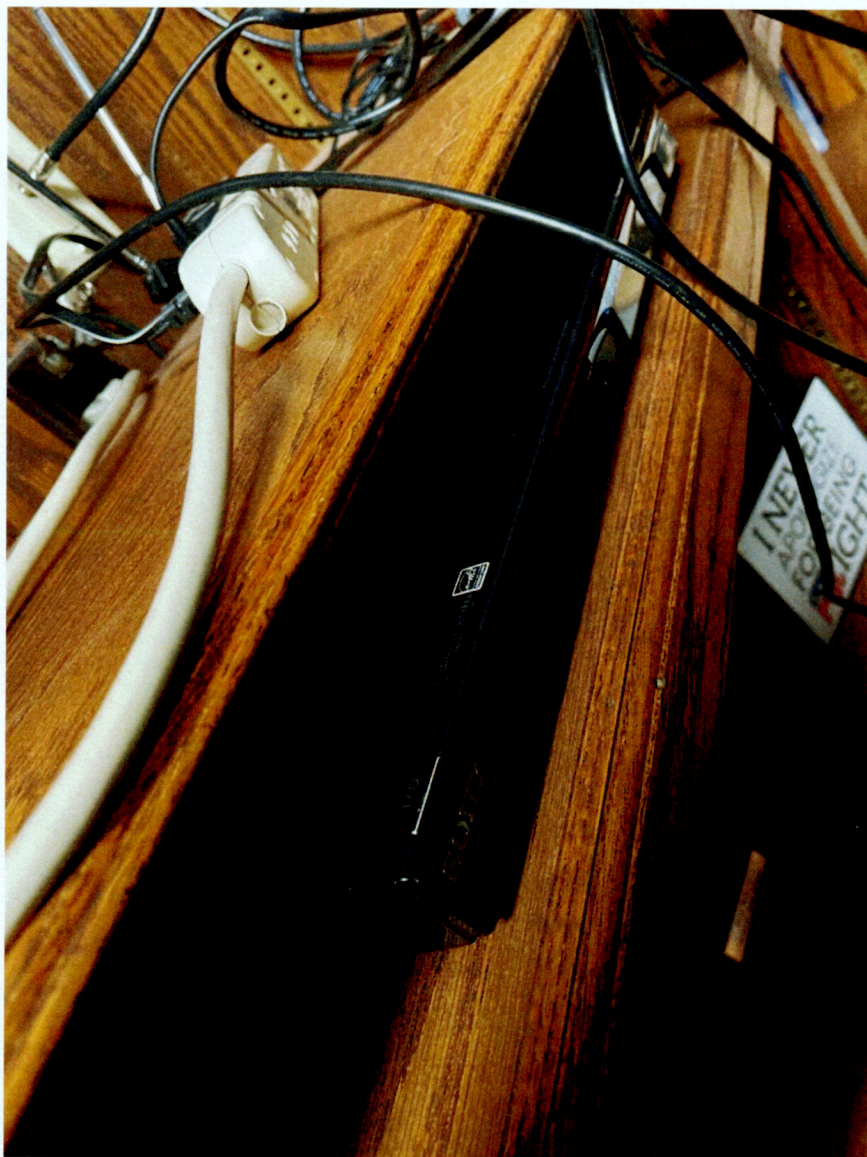


Figure 2: Sony DVD Player Connected to TV via HDMI





*Figure 3: Cox Cable Box Connected to the TV via HDMI*





Figure 4: Cox Cable Box Displaying Green Light





*Figure 5: 2 Cables from the Sony DVD Player, Cox Cables Box, and Rabbit Ears Connected to the Back of the TV*





*Figure 6: Cables Connected to TV with Ethernet port visible*



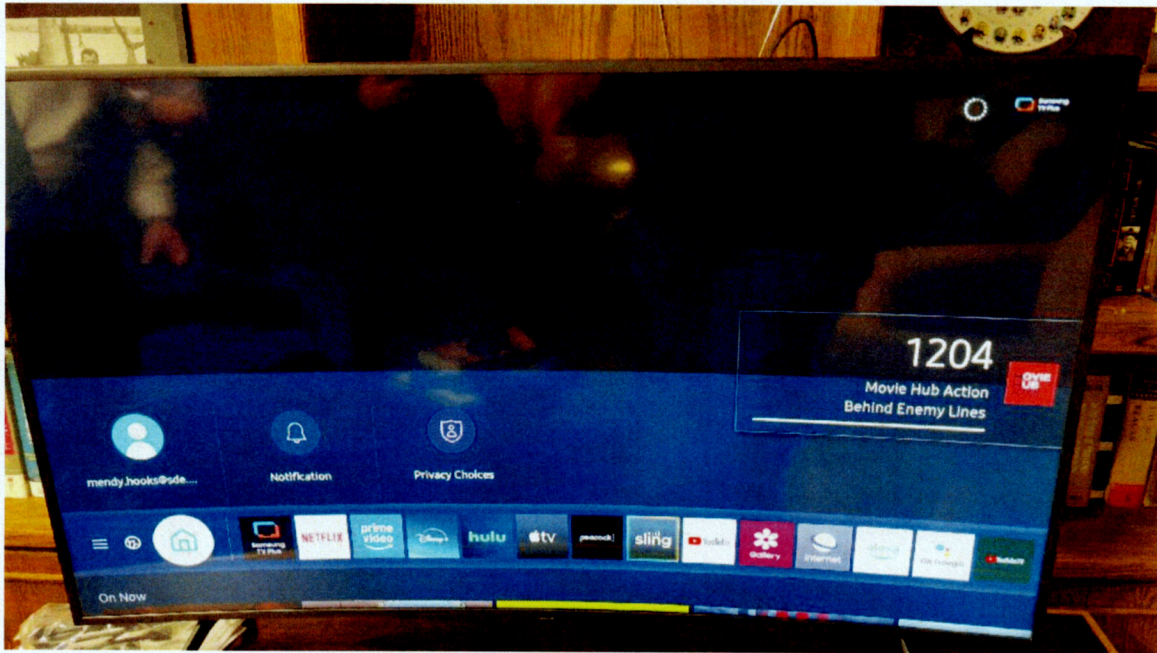


Figure 7: TV Display upon Initial Investigation Power-On Showing Channel 1204 (Movie Hub Action) on Samsung TV app.



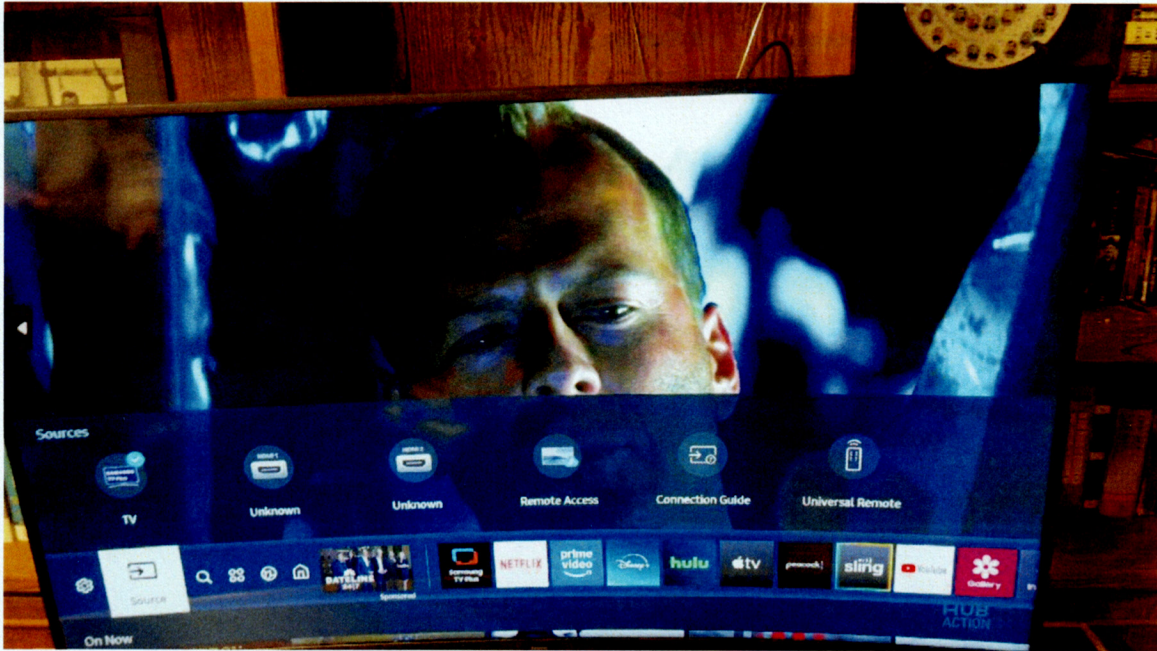


Figure 8: "Source" Setting set to "TV"

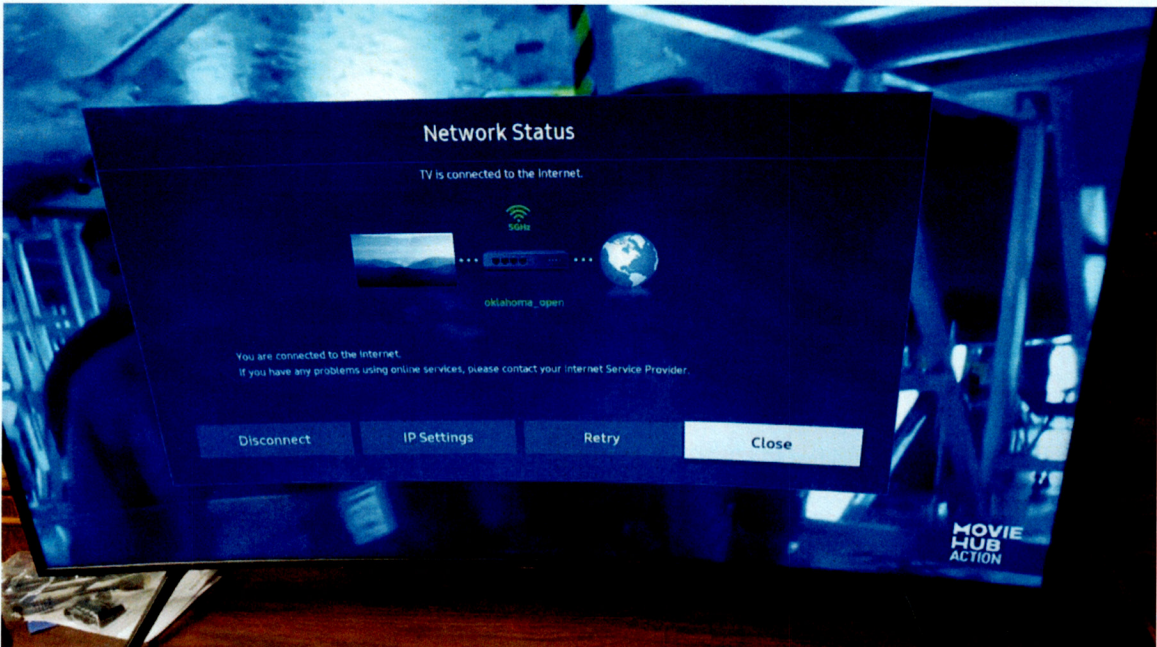


Figure 9: Network Status Showing Connection to "oklahoma\_open" WiFi SSID



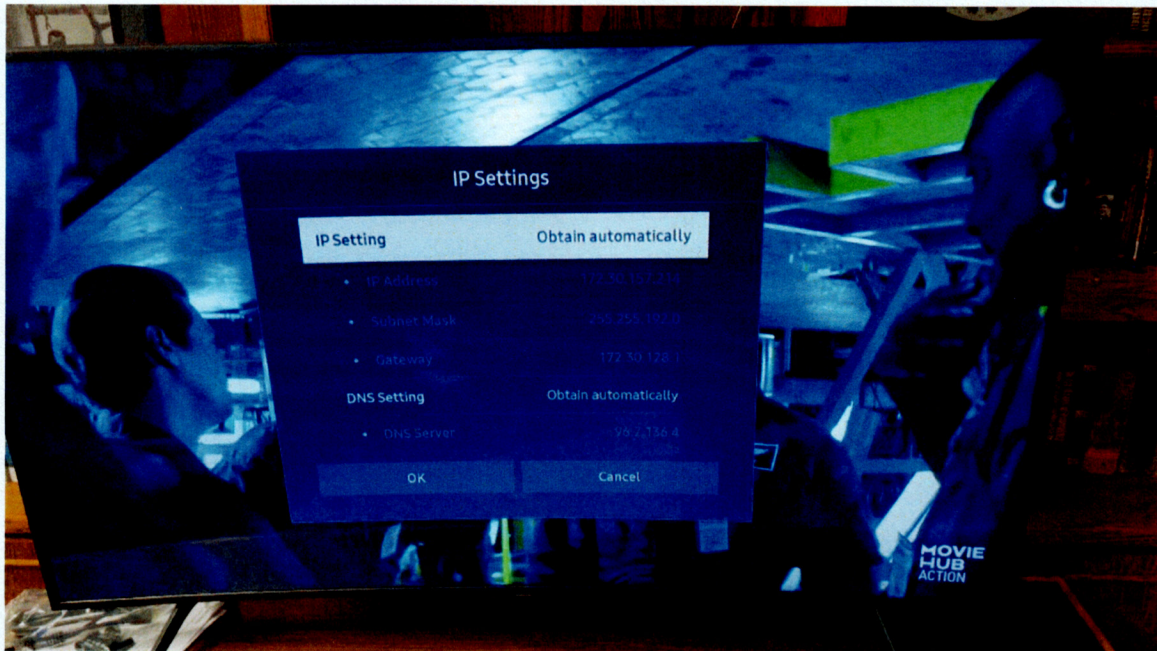


Figure 10: IP Settings Showing IP Address, Subnet Mask, Gateway, DHCP Configuration, and DNS Server

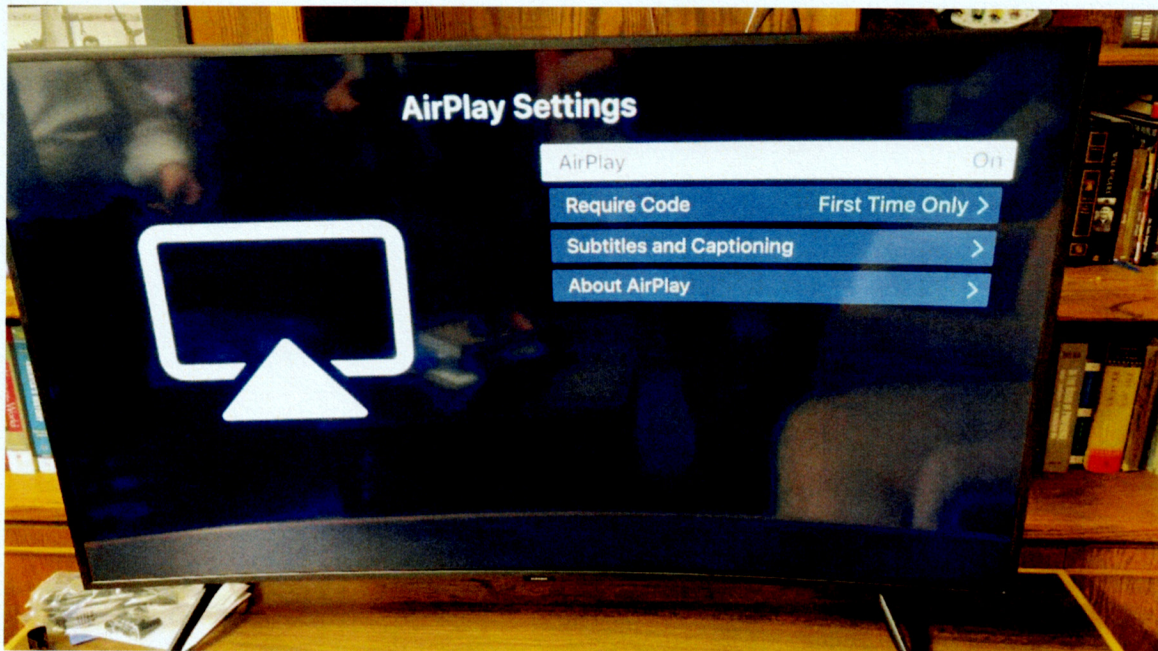


Figure 11: Apple AirPlay is set to "On" but Requires Code upon First Connection



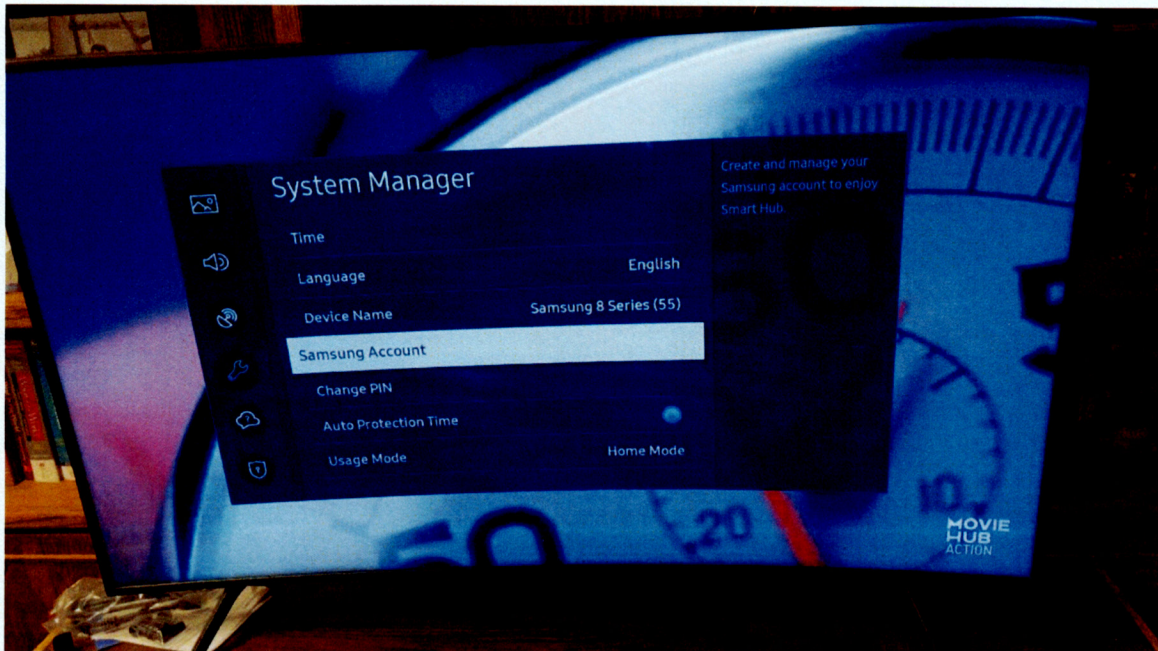


Figure 12: "System Manager" Settings, Showing the TV Name was set to "Samsung 8 Series (55)"

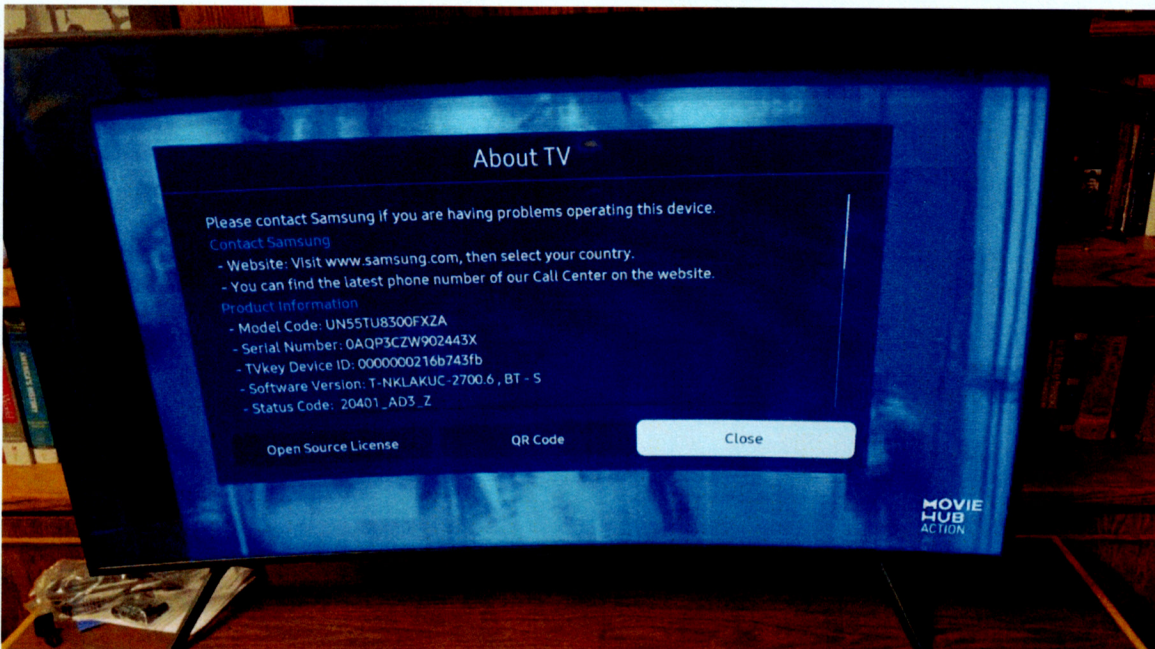


Figure 13: "About TV" Settings Menu Showing Model Code, Serial Number, TVkey Device ID, Software Version, and Status Code.





Figure 14: Mr. Walters Stated he Normally Access Fox News Through the Default Apps Screen of the TV

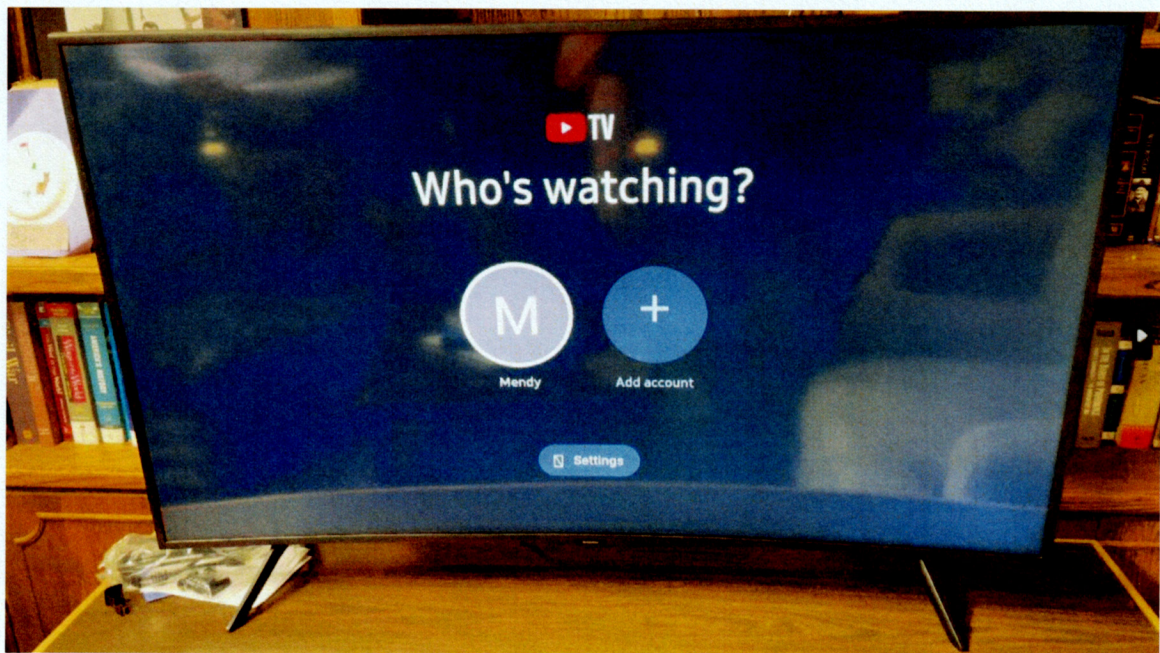


Figure 15: Upon Clicking on "The Will Cain Show" (fig. 14) the YouTube TV app Opens on the TV. The Account "Mendy" is Currently Signed In to YouTube app.



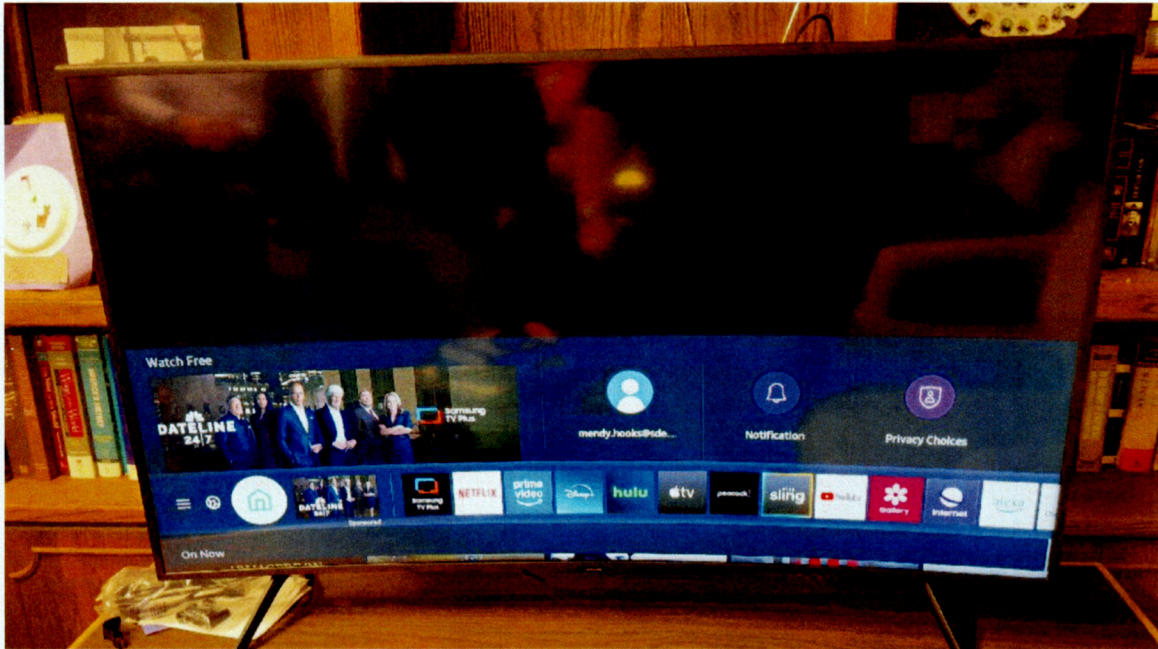


Figure 16: Home Menu Shows Signed In Account [mendi.hooks@sde.ok.gov](mailto:mendi.hooks@sde.ok.gov)



Figure 17: "Remote Access" in Source Menu



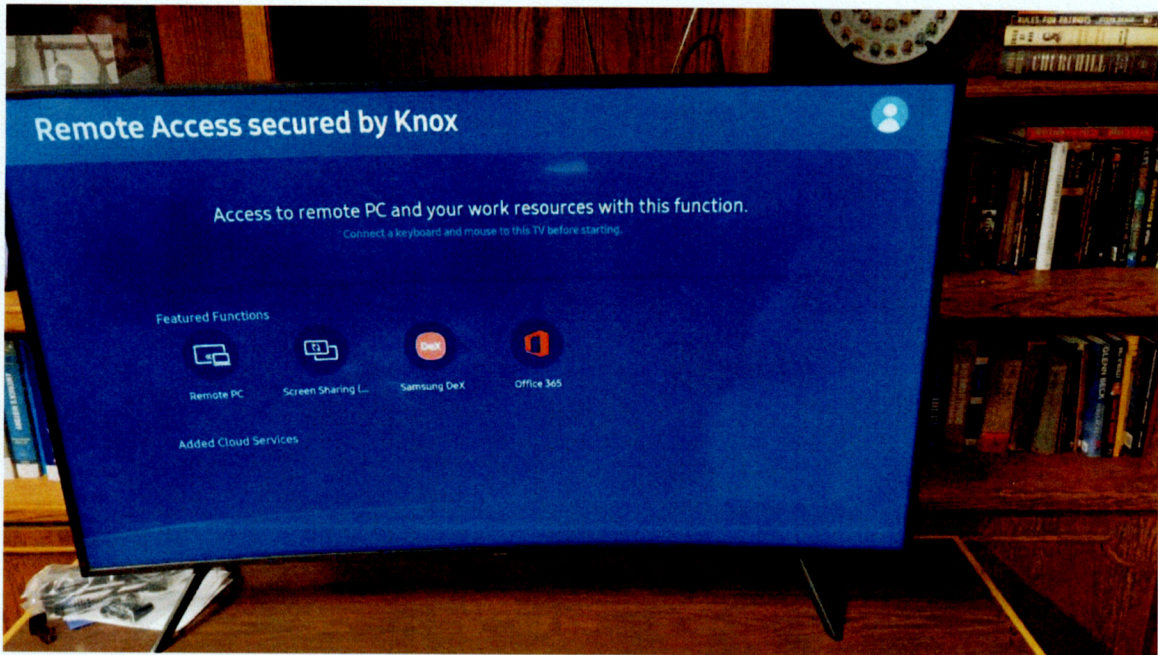


Figure 18: "Remote Access" Menu of the TV. Shows "Featured Functions" Including Remote PC, Screen Sharing, Samsung Dex, and Office 365



Figure 19: "About TV" Settings Menu Showing Event Logs.



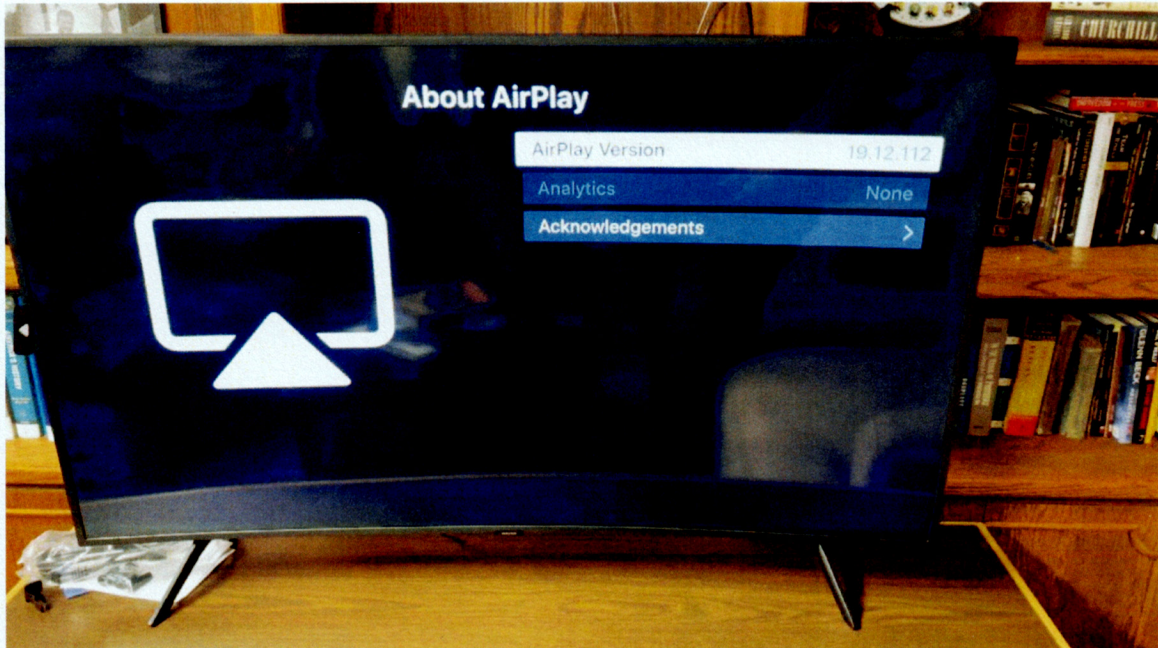


Figure 20: Apple AirPlay Software Version

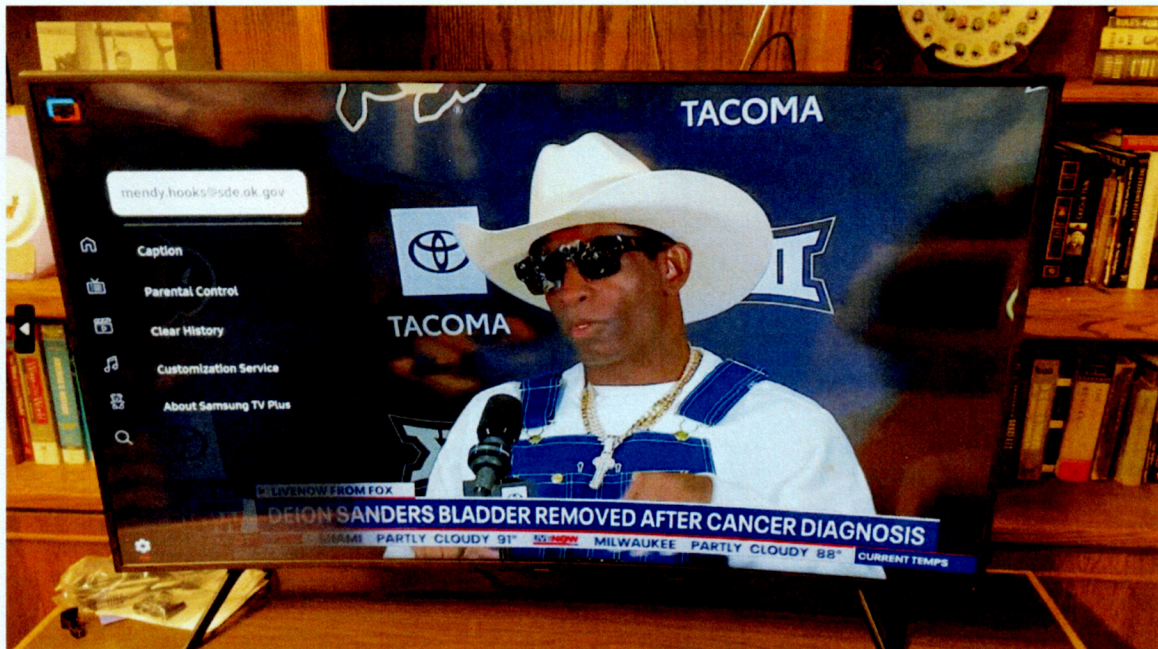


Figure 21: Account "mendy.hooks@sde.ok.gov" is Signed Into the TV



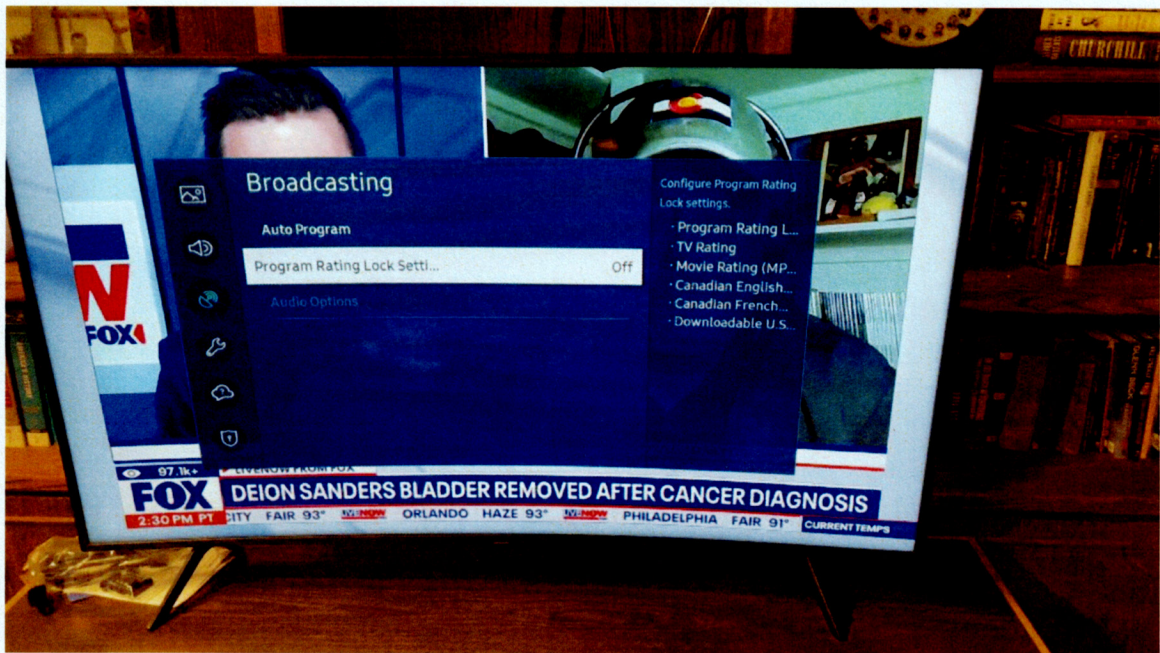


Figure 22: Parental Control "Program Rating Lock Setting" is Turned Off.



Figure 23: Display when "Source" is changed to "HDMI 2"





Figure 24: Display of the TV when Source is set to Remote Access > Office 365

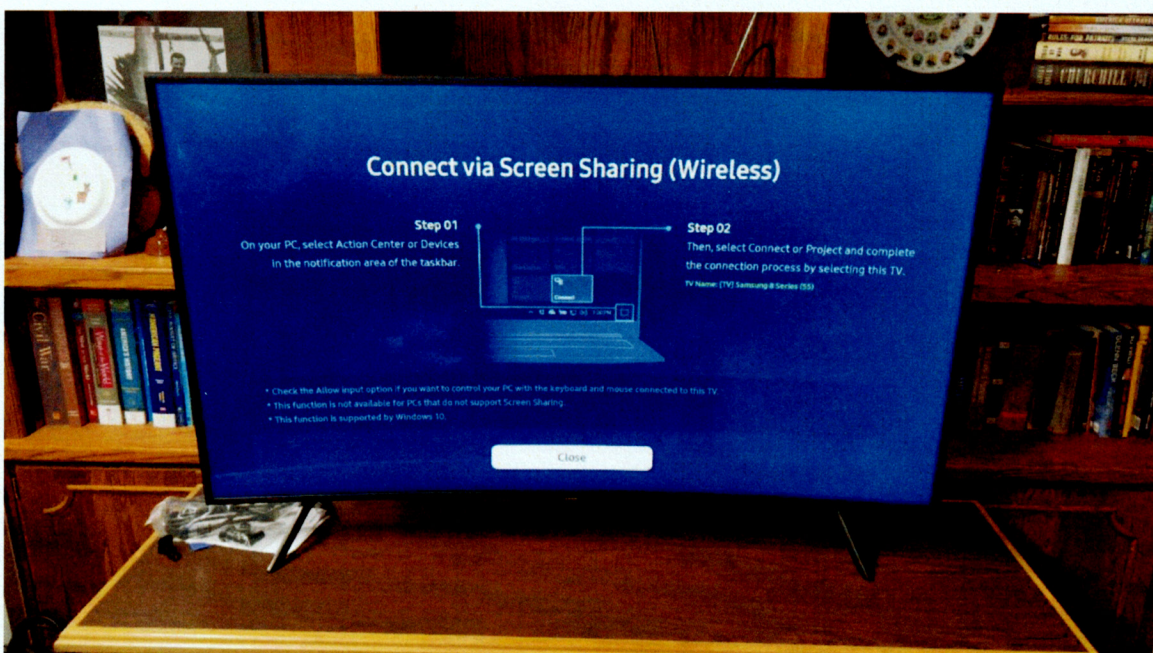


Figure 25: Display of the TV when Source is set to Remote Access > Screen Sharing



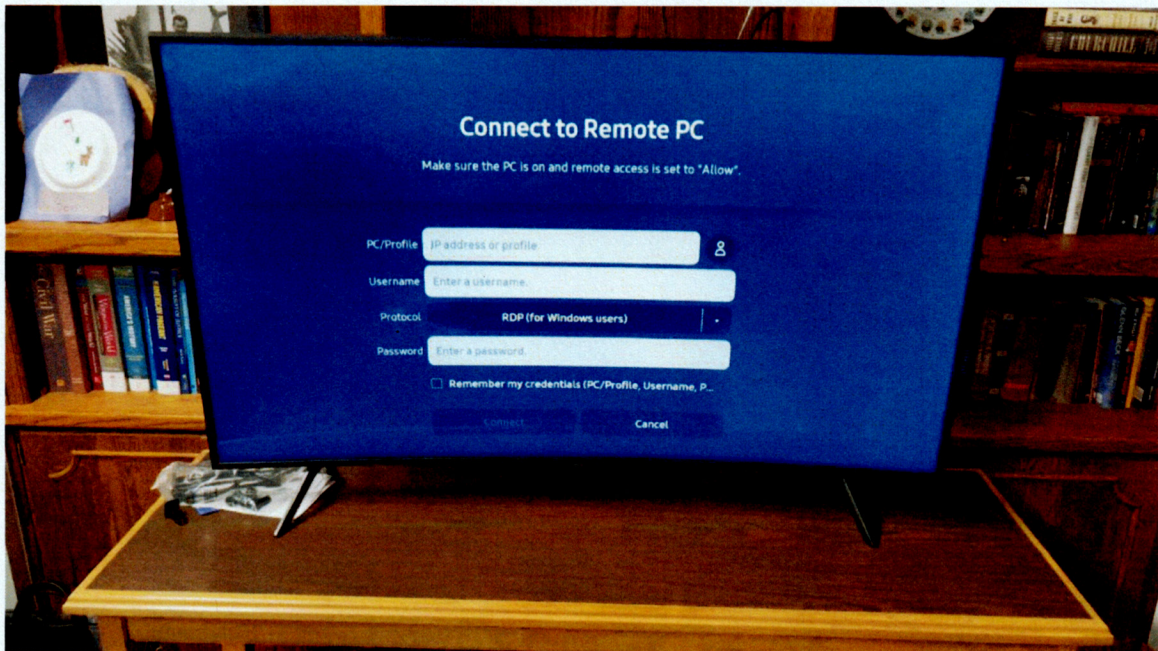


Figure 26: Display of the TV when Source is set to *Remote Access > Remote PC*

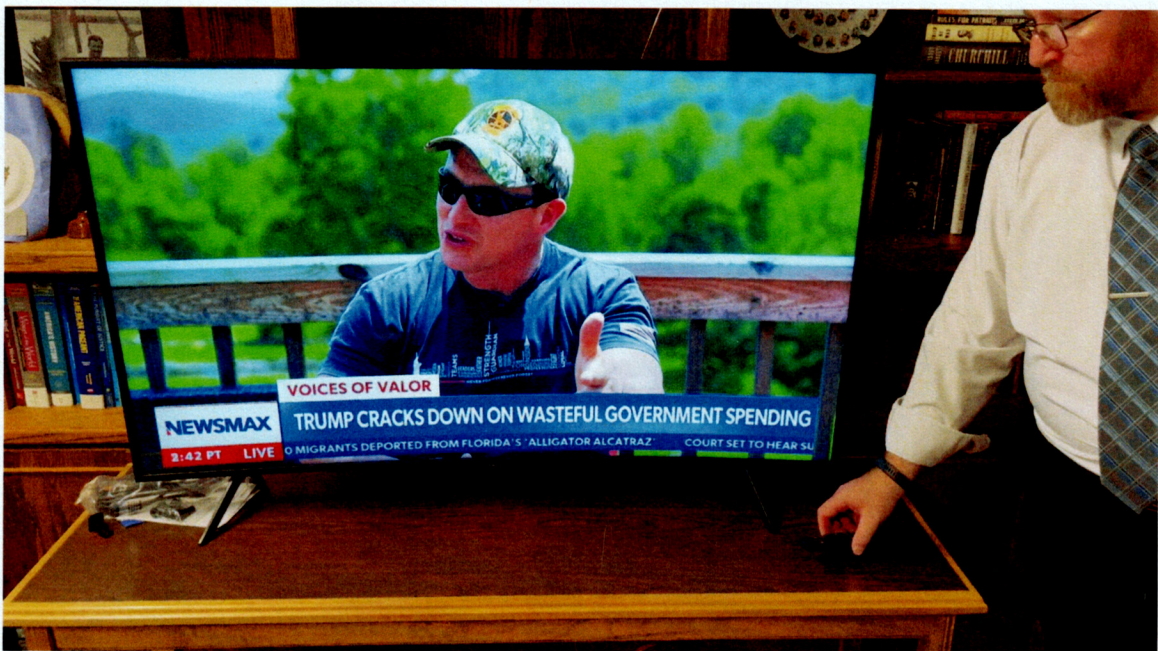


Figure 27: Source "HDMI 1" Connects to Cox Cable Box and Begins Playing Newsmax Channel



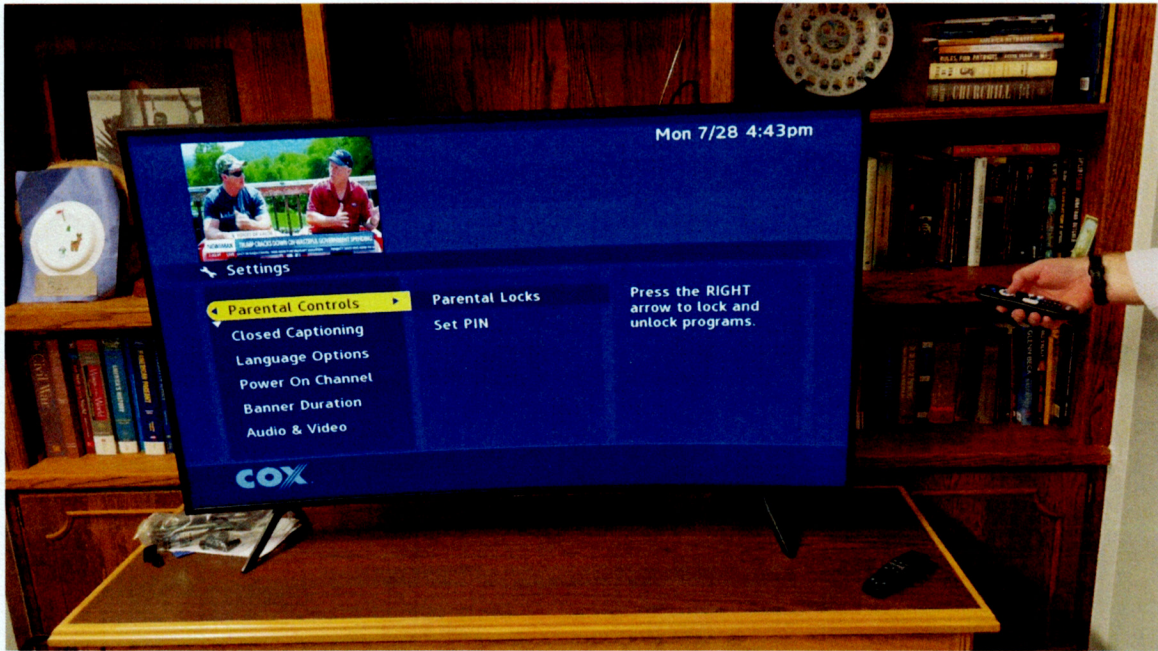


Figure 28: Cox Cable Box Settings

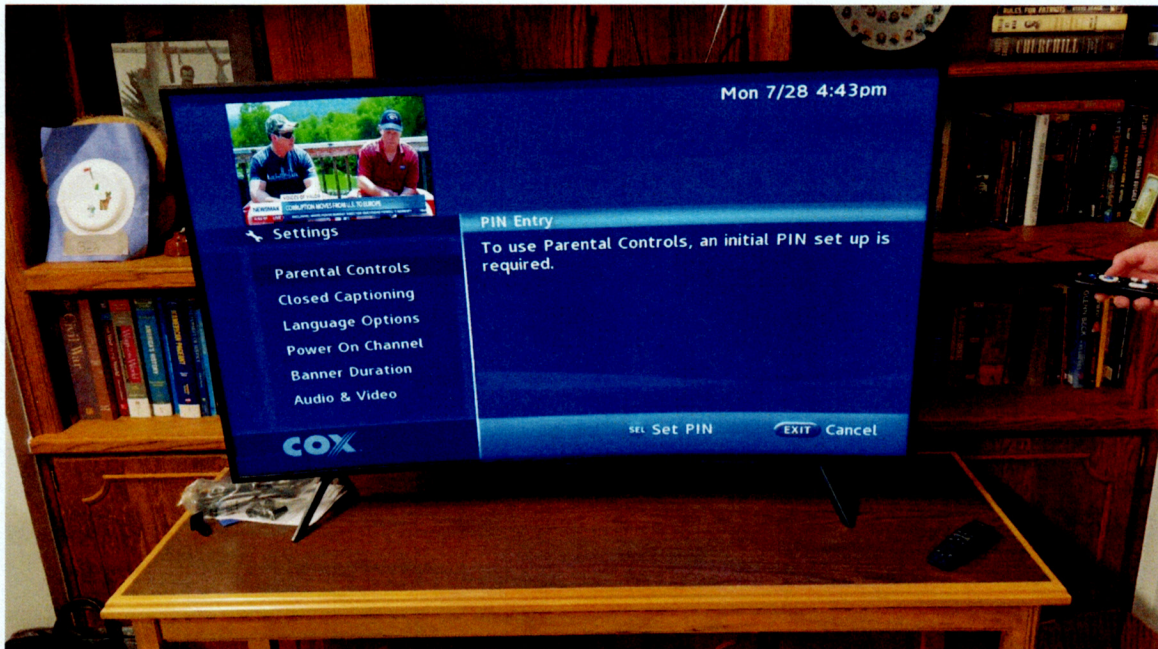


Figure 29: Parental Controls on Cox Cable Box are not Enabled.



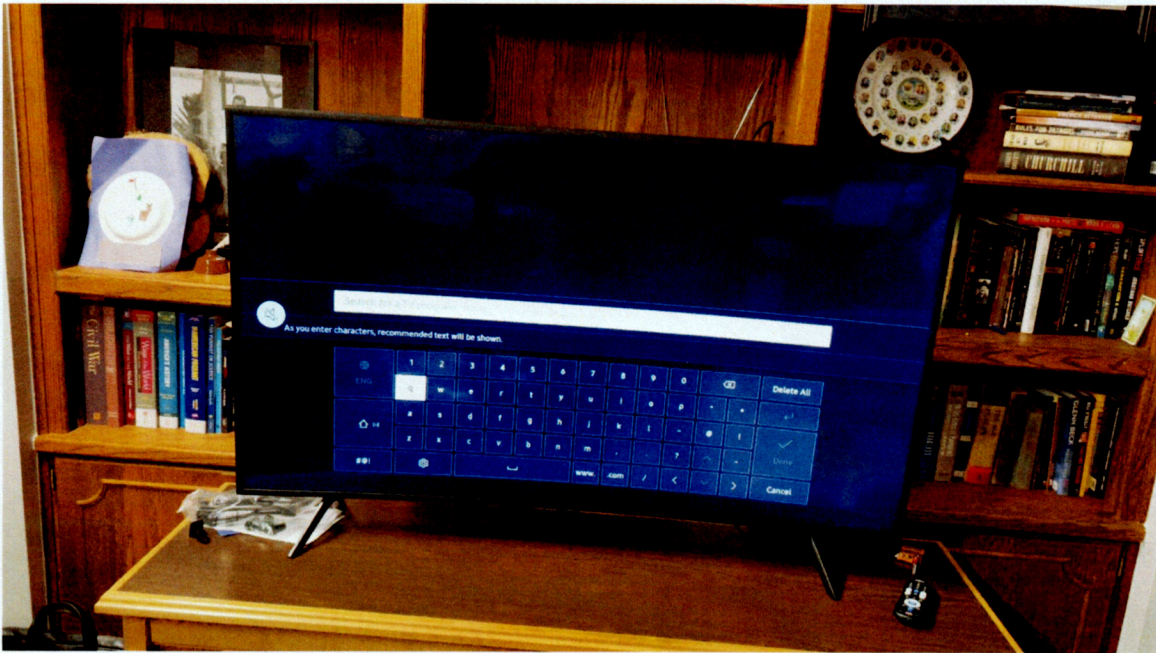


Figure 30: "Search" Feature of the Main Menu has predictive text, but no history of evidentiary value was located.

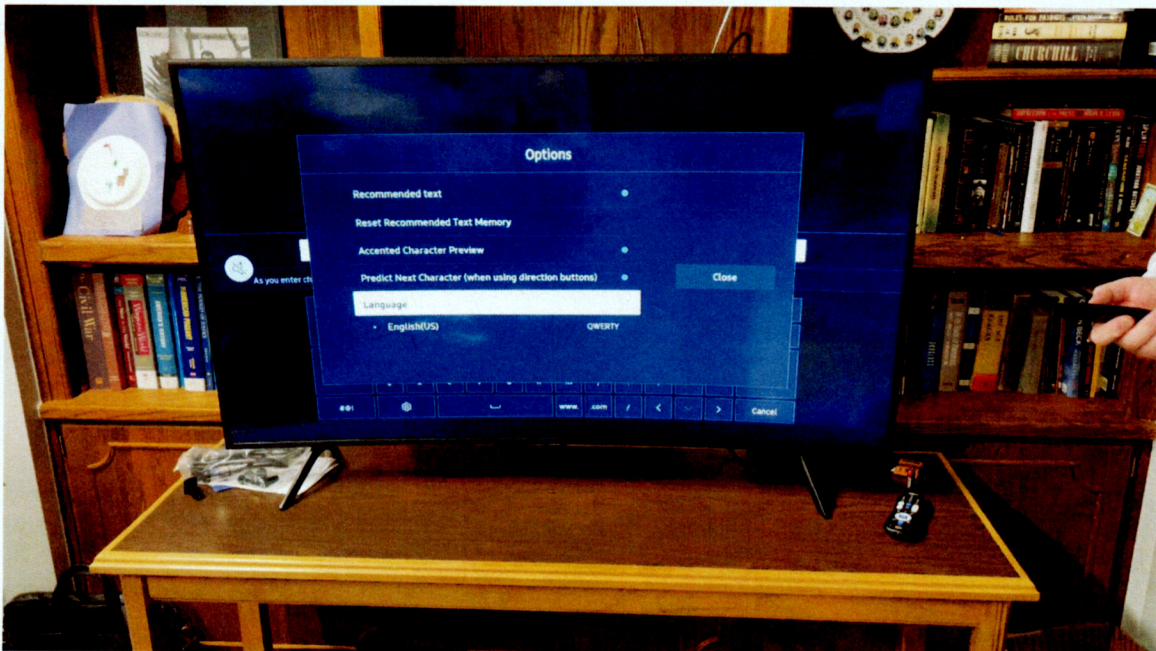


Figure 31: Predictive Text Settings Inside Search Menu



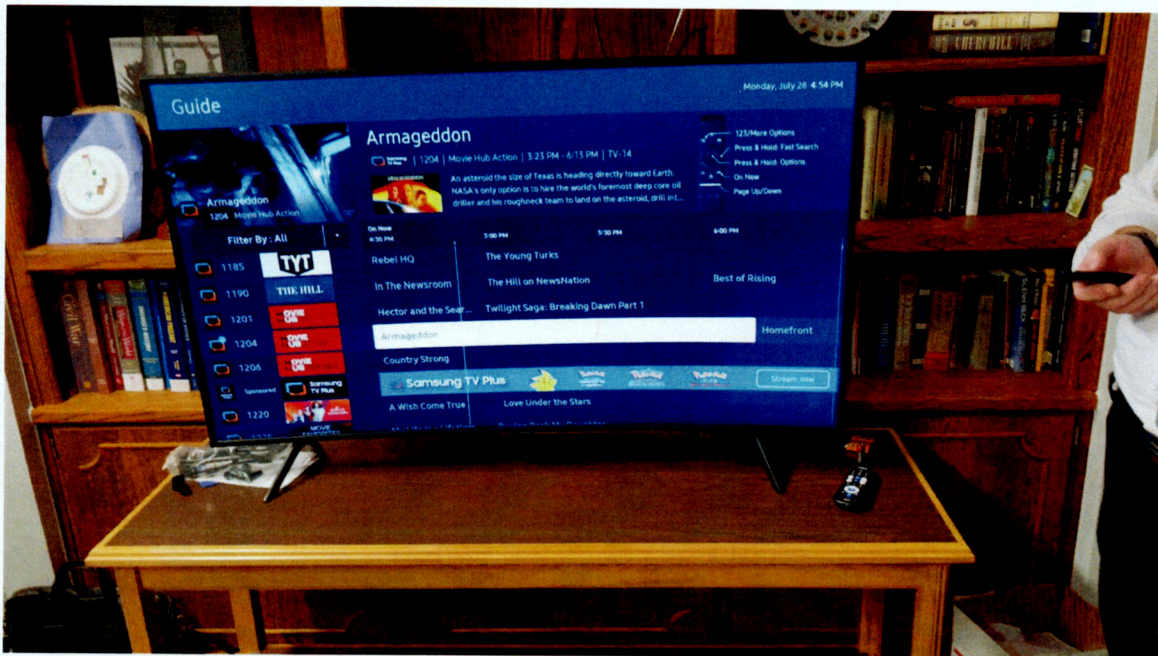


Figure 32: Samsung TV app "Guide" Displaying Channels and Program Schedule.



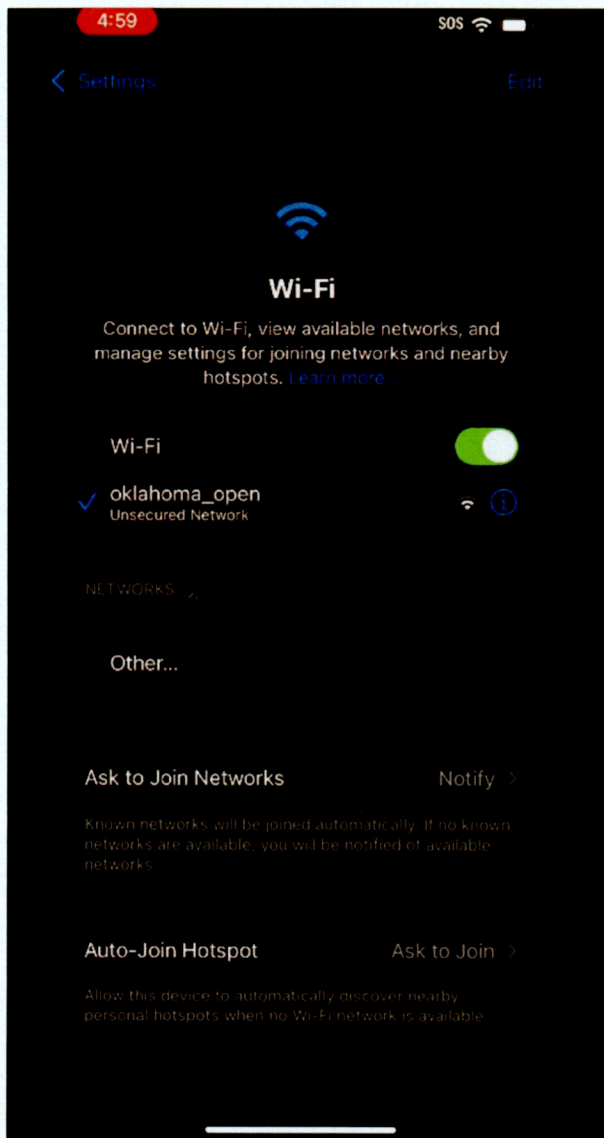


Figure 33: Examination Phone Connected to "oklahoma\_open" WiFi SSID.



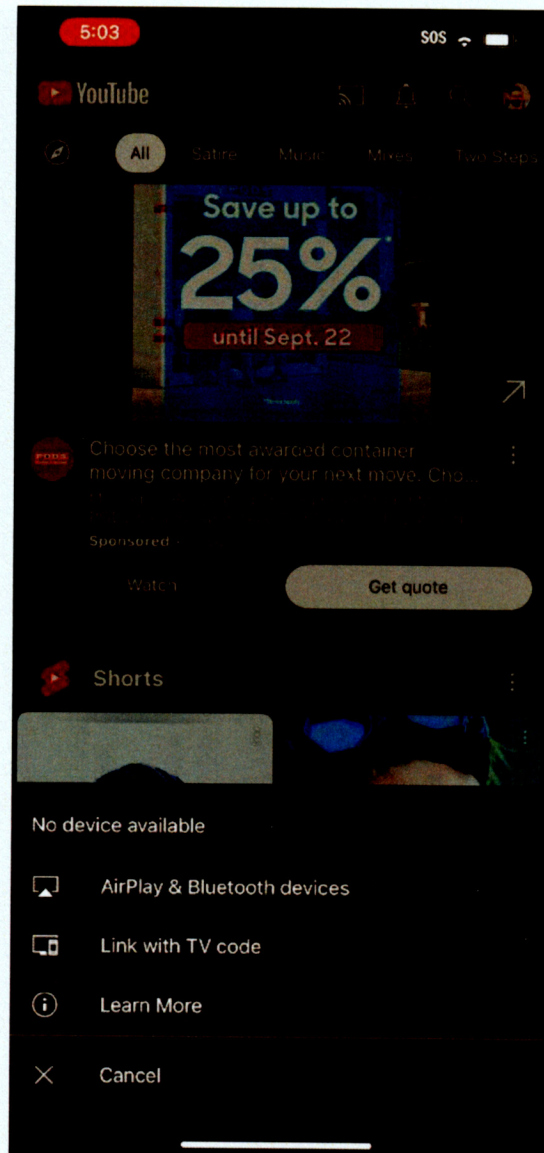


Figure 34: Examination Phone Attempted to Connect to the TV through the "Cast to Device" Button. No Device Called "Samsung 8 Series (55)" was located by the Phone.



```
Command Prompt
Connection-specific DNS Suffix . : fe80::4a71:ed4c:90:dacba21
Link-local IPv6 Address . . . . . : fe80::5b42:1907:12d1:e6e9%8
IPv4 Address . . . . . : 192.168.171.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Ethernet adapter Ethernet 3:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . : osf.ok.gov
Link-local IPv6 Address . . . . . : fe80::5b42:1907:12d1:e6e9%8
IPv4 Address . . . . . : 172.30.152.159
Subnet Mask . . . . . : 255.255.192.0
Default Gateway . . . . . : 172.30.128.1

Ethernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
```

Figure 35: Network Configuration for a Test PC that was connected to "oklahoma\_open" WiFi SSID.

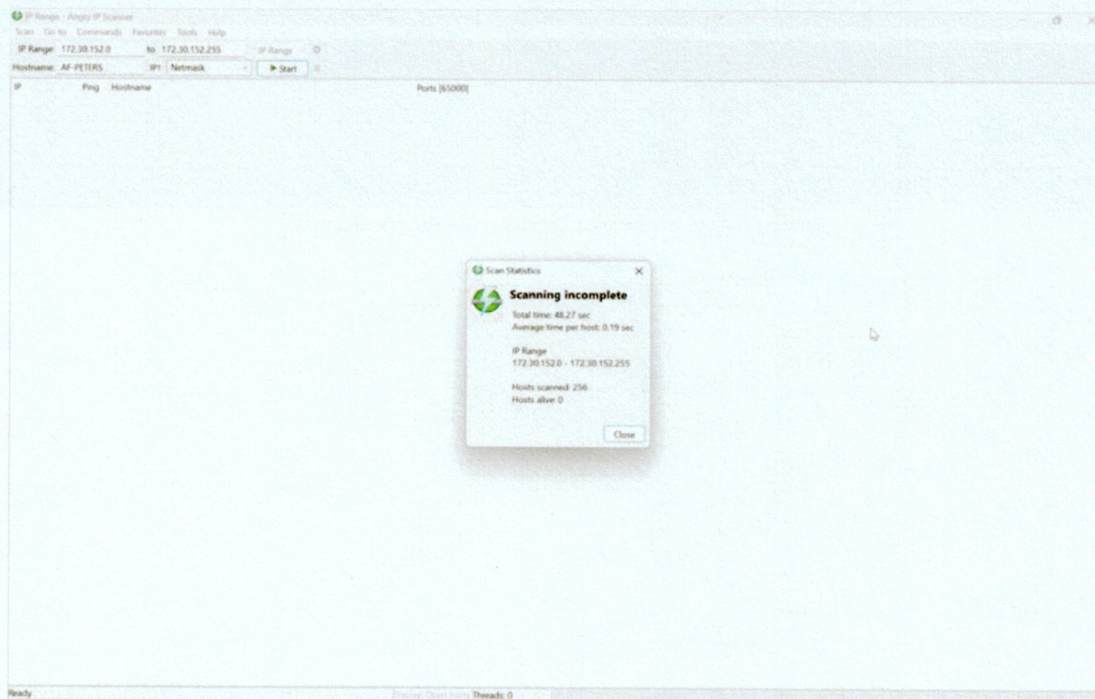


Figure 36: A Brief Network Scan of a portion of the "oklahoma\_open" Subnets Were Scanned to Identify Hosts. No Hosts Were Located due to Network Access Controls.



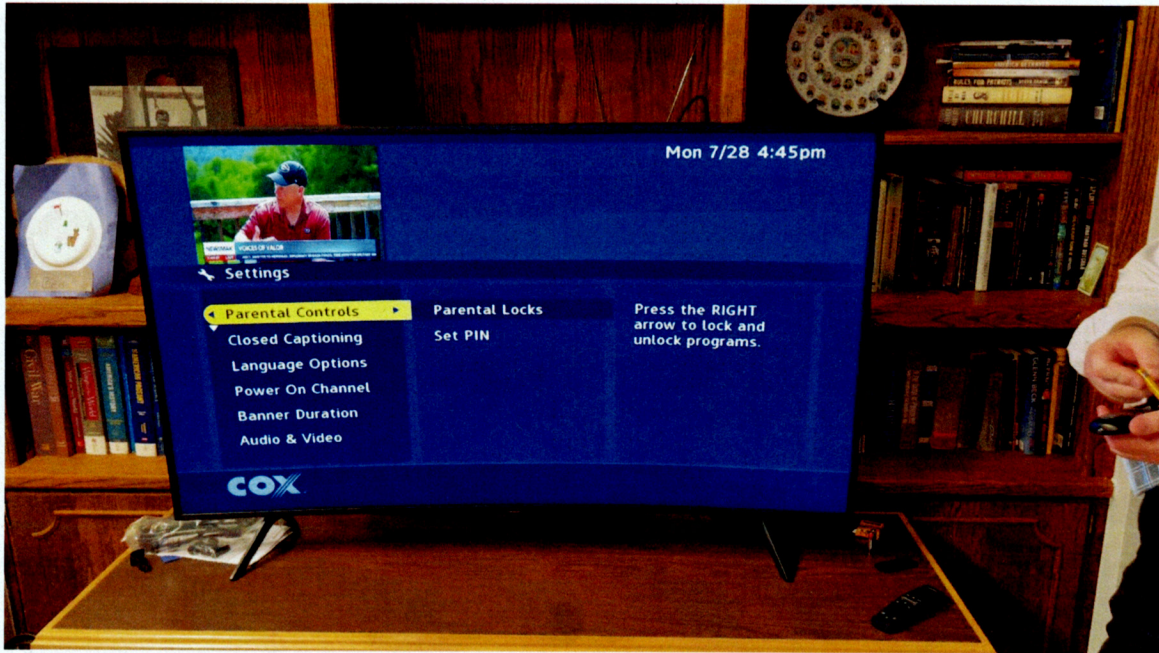


Figure 37: Alias Investigator Replacing Cox Remote Batteries.



Good afternoon,

The Office of Management and Enterprise Services is providing an update regarding a reported incident at the Oklahoma State Department of Education concerning explicit images, which was said to have occurred on Thursday, July 24.

### **Timeline**

Following the incident, OMES received a written complaint from an OSDE board member requesting to “file a formal complaint and request that his computers, personal devices and cell phones used by him at his office using government resources be preserved to ensure any pornography be preserved...” OMES then reached out to the Oklahoma County Sheriff and the Oklahoma State Bureau of Investigation out of an abundance of caution and in recognition that OMES is not a law enforcement agency and has no authority to investigate such matters.

On Monday, July 28, the State Superintendent also contacted OMES and asked OMES to examine equipment at OSDE. OMES sought clarity on which device(s) it was being asked to examine, and OSDE responded that it wanted OMES to analyze one Samsung TV (Model: UN55TU8300FXZA, Serial Number: 0AQP3CZW902443X, Type: 55" Class Crystal UHD TU830 (2020)) located in the Superintendent’s office, where board meeting executive sessions take place. That email exchange is attached for review.

OMES, along with three sheriff deputies, conducted a visit to OSDE on the afternoon of July 28 and engaged a third-party vendor to perform a thorough analysis of the TV. The findings from the review included the following:

- The TV had cable access, streaming services, was connected to an empty DVD player, and was equipped with a dipole antenna.
- The TV was connected to the state's open WiFi network.
- A one-time passcode was required to access screen casting to the TV, limiting the number of people with casting ability to the device.
- The search history on the TV was empty.
- The TV previously belonged to a former OSDE employee and was relocated to the Superintendent’s office earlier this month. The employee’s account was still connected to YouTube TV but under a new IP address.
- The Superintendent mentioned that on board meeting days, many staff members, board members, and the public could access his office.
- Due to the hundreds of preloaded apps on the TV, the streaming services were not given a full review as the TV remained on-site.

It is important to note that OMES can only review technology at an agency's request unless directed by the Legislature, law enforcement, or court system. Additionally, OMES cannot review other state or personal devices without permission from that agency and/or individuals.



Additionally, OMES has also been informed that the Superintendent's office uses hot spots to connect devices during board meetings; however, this has not been independently verified. OMES is only able to monitor state networks.

Finally, each state agency maintains its own human resources policies and disciplinary procedures, which are not dictated or enforced by OMES.

**Follow-up**

We are currently awaiting further word from the Oklahoma County Sheriff's Office. At this time, we cannot determine definitively whether or not an incident took place.

Please feel free to reach out if you have any questions or need further clarification.