# WHY YOU SHOULD LEAVE YOUR SMART GRILL UNPLUGGED?

www.hack4career.com mert.sarica@gmail.com MertSARICA MertSARICA

# WHO AM I?

- Cyber security researcher, speaker & blogger.
  - Published **200+** technical write-ups @ **hack4career.com**
- 16 years of experience in the banking industry.
  - CISO, SOC VP, Threat & Vulnerability Management Lead, Lecturer in Malware Analysis
- Head of Strategy SOCRadar® Your Eyes Beyond Extended Threat Intelligence (**socradar.io**)
- Certifications: CCISO, CISSP, CEREA, OSCP, CREA, SSCP

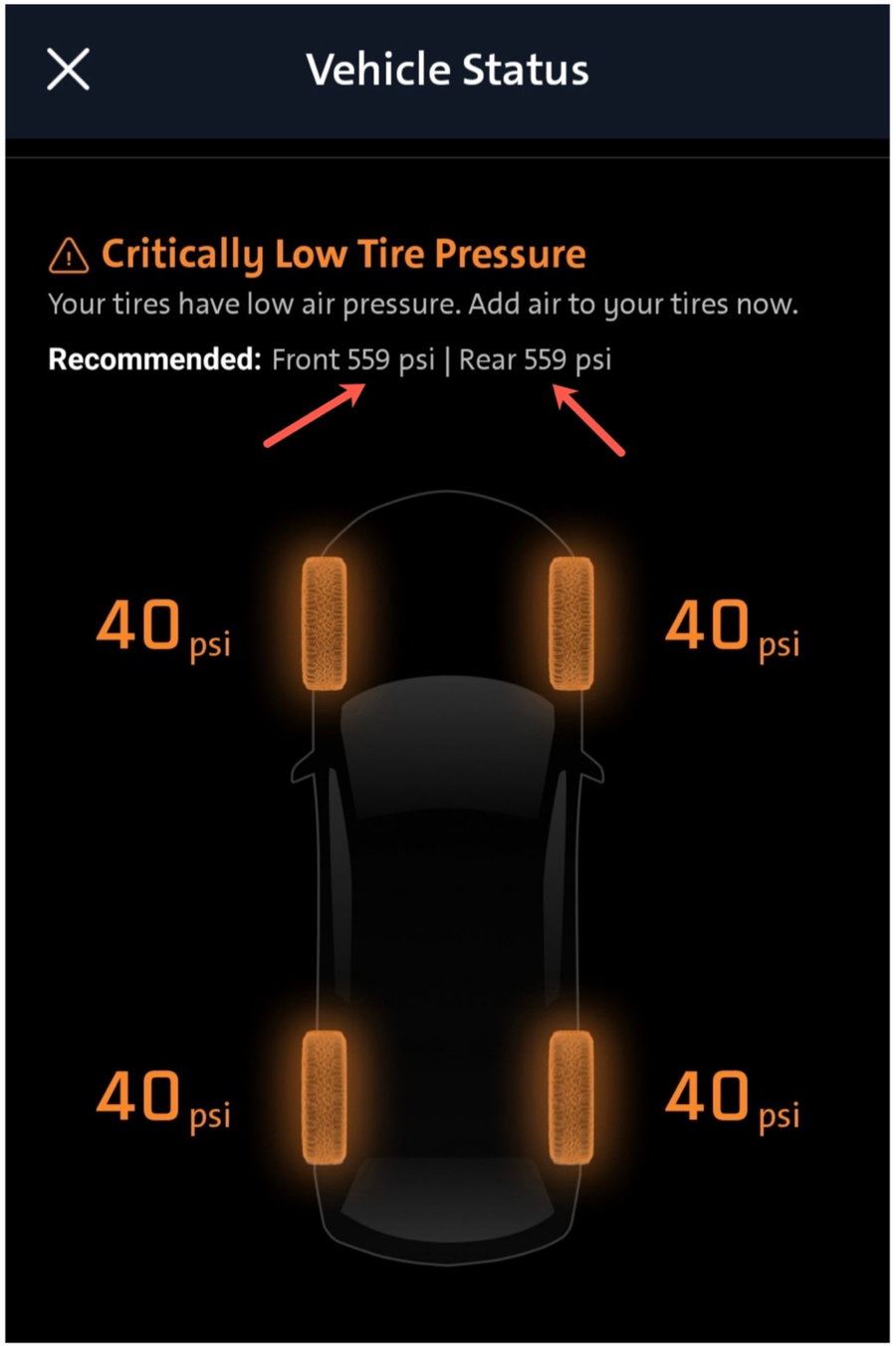
# WHAT IS IOT?

## WHAT YOU HEAR?

Smart
Better security
Cost and energy saving
Comfort
Automation
High-tech

## WHAT YOU HAVE?

A device with severe **weaknesses** due to its limited hardware and software capability.


Vehicle Status
Critically Low Tire Pressure
Your tires have low air pressure. Add air to your tires now.
Recommended: Front 559 psi | Rear 559 psi
40 psi
40 psi
40 psi
40 psi

# IOTS ARE EVERYWHERE

## AS OF 2023

**~8 BILLION**

Humans are living on our planet.

**~16 BILLION**

Connected IoT devices, equivalent to twice the total number of humans*.

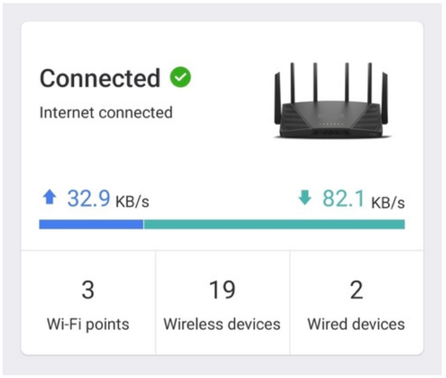
*IOT Analytics

# IOTS ARE EVERYWHERE

smart toilet


smart deodorant


smart belt




router

- From fish tanks to thermostats, toilets* to belts, and even **pellet grills.**
- IoTs are inevitable!
- Most of them use **Bluetooth Low Energy**.

*metrikus

# BLUETOOTH LOW ENERGY (BLE)

**1.**

Often seen in wearable devices, smart IoT devices, fitness monitoring equipment, etc.

**2.**

Run on battery power for years.

**3.**

Used for applications that do not need to exchange large amounts of data.

**4.**

Transfers data in far smaller pieces than a Bluetooth transmission of a similar length.

# WHAT ABOUT GRILLS?

**131.2 million**
households in the U.S. in 2022*.

**100 million**
grill-owning households in the U.S. in 2021*.

## 1/3

Approximately **one-third** of them own **multiple grills.**

Widespread use of smart grills (IoT) may bring **serious security risks.**

*USAFACTS *TRAEGER

# HOW THE STORY BEGAN

Settled in the U.S. at the end of 2022.

Purchased a **BLE-enabled** smart **pellet grill** in March 2023.


Enrolled it into my home WiFi network, and then a question appeared in my mind.

↳ Is it wise to keep an IoT that stores my **WiFi password** and **SSID** on the patio?

# SECURITY RISKS?

Changes depend on

- Who you are and who may target you,
- The type of vulnerability,
- Your risk appetite,
- How and where you use the IoT for.

# THE CASINO HACK*
## 2017

- A North American casino installed a high-tech fish tank (IoT) in the aquarium in the lobby.
- The casino configured the tank to use an individual VPN to isolate the tank's data.
- The hackers exploited a vulnerability in the thermostat to get a foothold in the network.
- They transferred **10GB** of data to a device (hacked IoT) in Finland.
- Data included the high-roller database of gamblers.

*The Washington Post

# WHAT IF

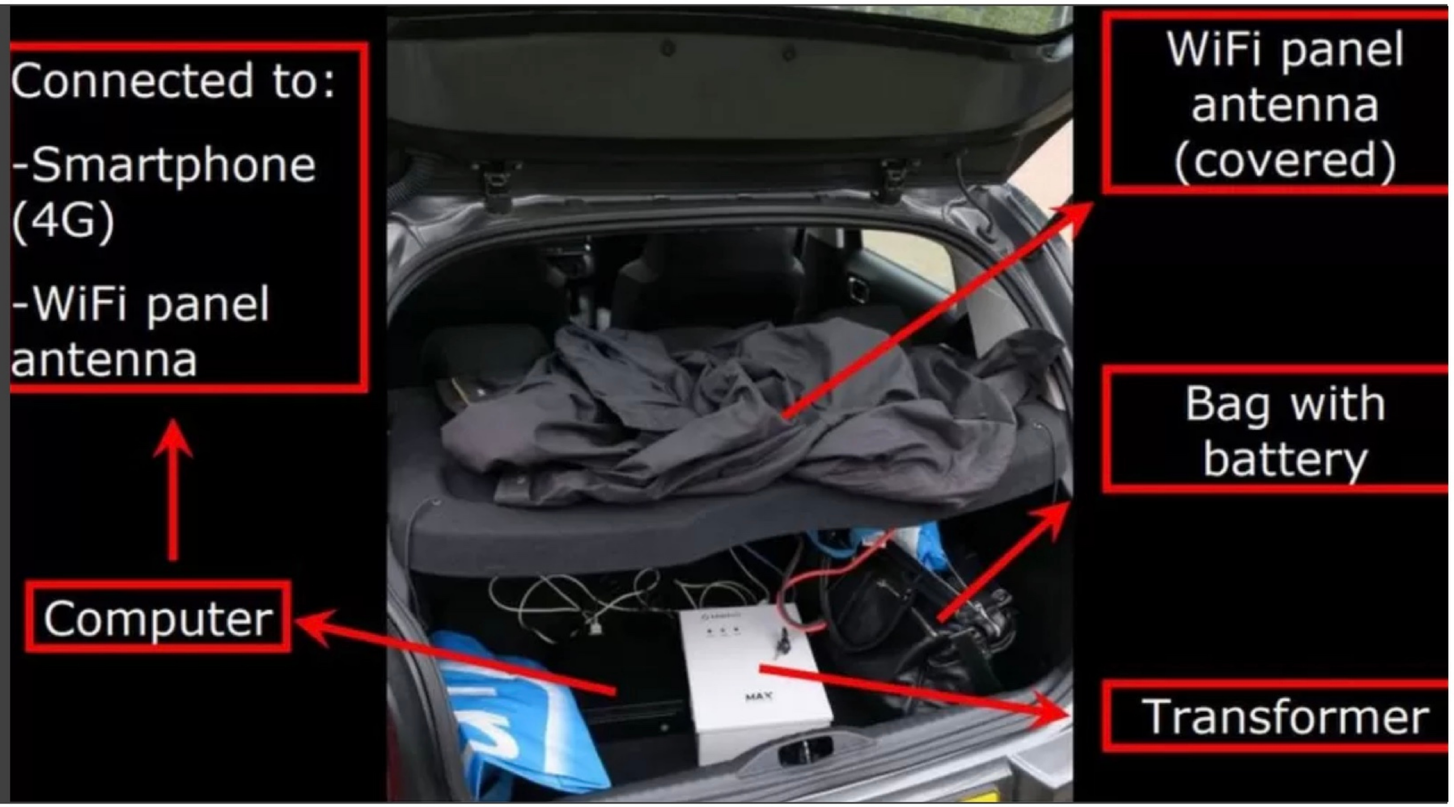
A threat actor targets you or your enterprise?

- Will they pay a visit to you not only in the cyber world but also in the real world to sneak into your network?
- Fact or fiction?

# WHO ARE THEY?

Colleagues attending a cyber security conference in Las Vegas?

# WHAT DO THEY CARRY?



# WHERE ARE THEY HEADING TO?

# OPERATION* OF THE FANCY BEAR / APT28 2018

- Traveled to the Netherlands on diplomatic passports.
- Hired a car and scouted the area around the OPCW building.
- They set up specialist equipment in the rear of the car.
- The goal was to **hack OPCW's WiFi network.**
- They were detained and expelled to Moscow by Dutch authorities.

*bbc

Dashboards
Attack Surface Management
Digital Risk Protection
Cyber Threat Intelligence
Threat Hunting
Local Threat Share
Dark Web News
Vulnerability Intelligence
Supply Chain Intelligence
Threat Feed / IOC
Threat Actor/Malware
Threat Hunting Rules
Malware Analysis
Threat Reports
Breach Datasets
Campaigns
Stealer Logs
Incidents

← Dashboard

# APT28 | Mitre ID: G0007

## Also Known As:

Sednit | G0007 | Tsar Team | FANCY BEAR | IRON TWILIGHT | Fighting Ursa | TG-4127 | T-APT-12 | FROZENLAKE | APT-C-20 | SIG40 | Group 74 | Blue Athena | Pawn Storm | SNAKEMACKEREL | Sofacy | Grizzly Steppe | ATK5 | UAC-0028 | Threat Group-4127 | TA422 | Fancy Bear | Swallowtail | STRONTIUM | ITG05

Details | Yara / Sigma Rules | References

## Description

**Description of MISP:** The Sofacy Group (also known as APT28, Pawn Storm, Fancy Bear and Sednit) is a cyber espionage group believed to have ties to the Russian government. Likely operating since 2007, the group is known to target government, military, and security organizations. It has been characterized as an advanced persistent threat.

**Description of Mitre:** APT28 is a threat group that has been attributed to Russia's Main Intelligence Directorate of the Russian General Staff by a July 2018 U.S. Department of Justice indictment. This group reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election. APT28 has been active since at least 2004.[1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11]

## Associated Malware/Software:

win.sedreco | win.xtunnel_net | win.xtunnel | xtunnel | cannon | JHUHUGIT | fusiondrive | popr-d30 | Dropper.DR/AutoIt.Gen | driveocean | win.computrace | oldbait | CHOPSTICK | osx.xagent | graphite | jar.jrat | credomap | win.oldbait | win.coreshell | xp_privesc | win.koadic | Win.Downloader.76944-1 | zebrocy | win.hermeticwiper | Fysbis | Zebrocy | win.xagent | USBStealer | xagent | GLOOXMAIL | win.credomap | osx.komplex | win.driveocean | koadic | sedreco | win.pocodown | Koadic | arguepatch | win.seduploader | win.xp_privesc | pocodown | Responder

## Target Countries

Afghanistan | Armenia | Australia | Azerbaijan | Belarus | Belgium | Brazil | Bulgaria | Canada | Chile | China | Croatia | Cyprus | France | Georgia | Germany | Hungary | India | Iran, Islamic Republic of | Iraq | Japan | Jordan | Kazakhstan | Latvia | Malaysia | Mexico | Mongolia | Montenegro | Netherlands | Norway | Pakistan | Poland | Slovakia | South Africa | Spain | Sweden | Switzerland | Tajikistan | Thailand | Turkey | Uganda | Ukraine | United Arab Emirates | United Kingdom | United States | Uzbekistan

# FACT OR FICTION?

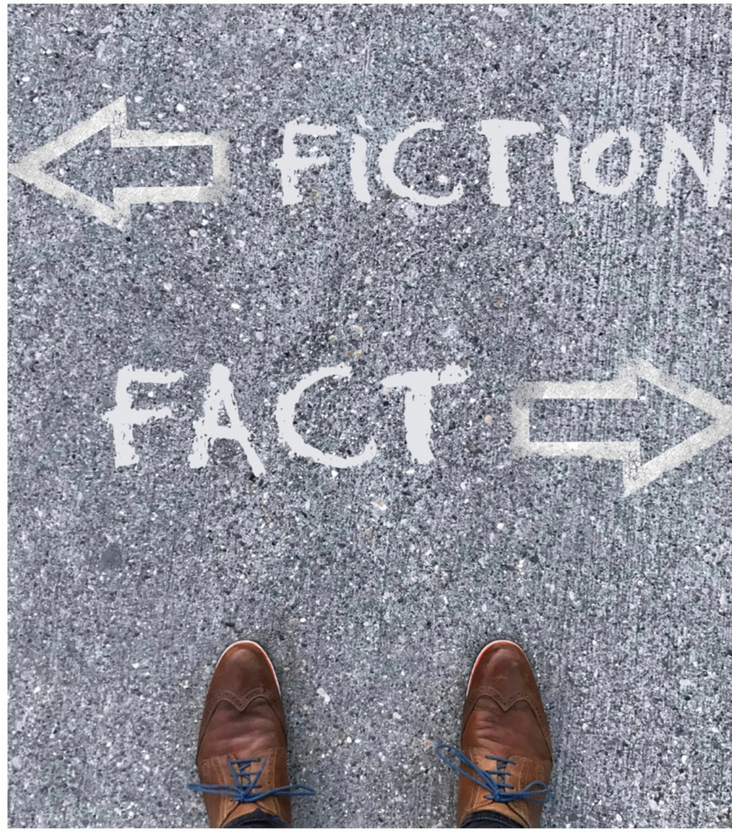
- Facts
  - APT groups may come after their targets in the cyber and **real world.**
  - No evidence of hacking someone by exploiting a vulnerability in an IoT.

- Fiction
  - What if they would come after a VIP Mert?
  - Easy or challenging to sneak into the WiFi network by hacking an IoT?

    ↳ Let's find out!

# TOOLS & DEVICES

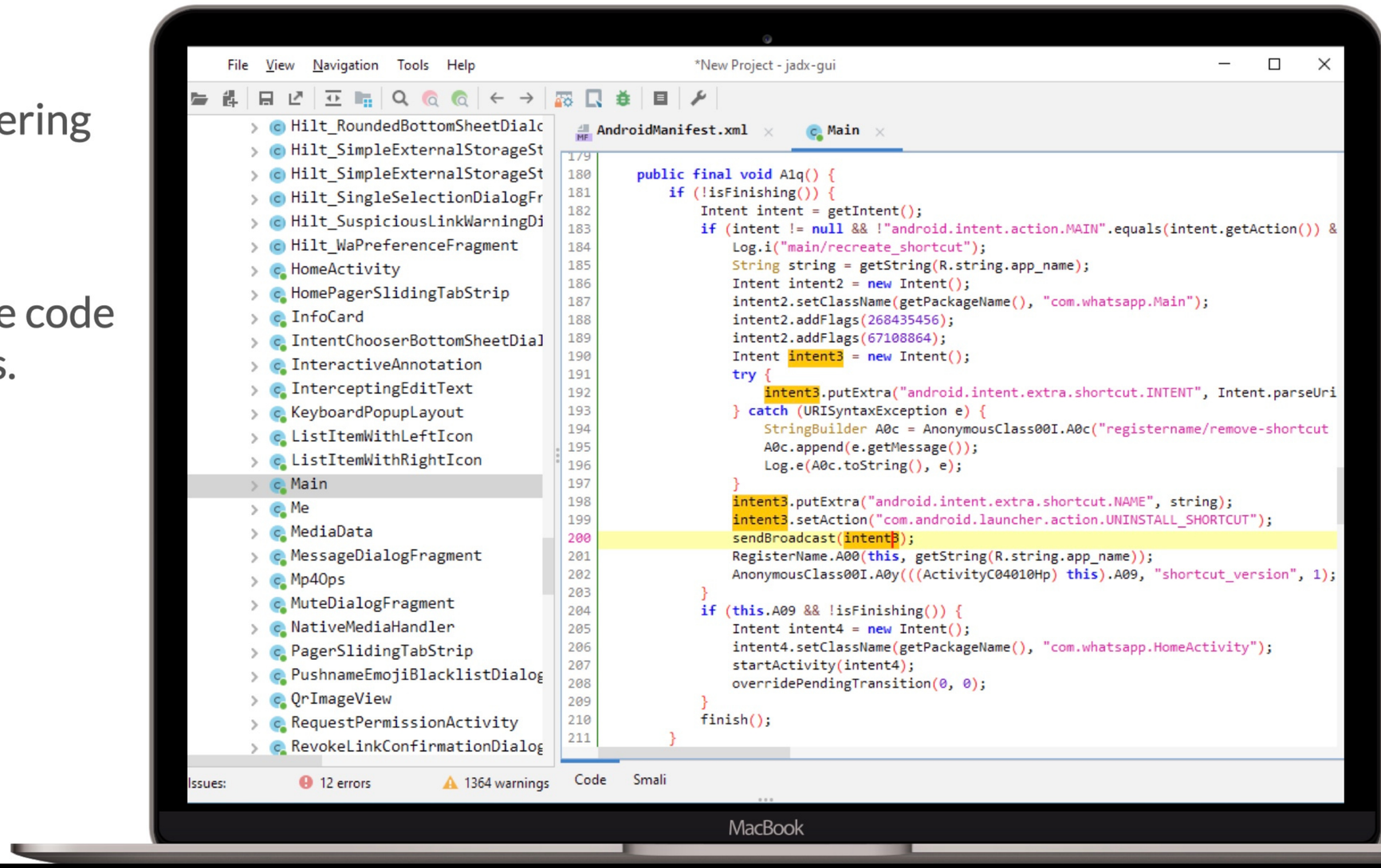
- Pellet grill's mobile application to reverse engineer with **jadx.**
- Android mobile device (**Galaxy S**) to capture BLE packets.
- **Wireshark** to analyze BLE packets.
- **Kali Linux** and Bluetooth USB adapter (**Parani-UD100**) to send and receive BLE packets.



# JADX

- Tool for reverse engineering Android applications.
- Allows to decompile bytecode to Java source code from APK and DEX files.

*JADX



# PARANI-UD100


- The Parani-UD100 is a class 1 type (longest range) Bluetooth USB adapter.
- Supports **300** meters (**984** ft) of wireless transmission distance by default.
- The working distance can be further extended up to **1000** meters.

*SENA

# REVERSING
# THE MOBILE APPLICATION

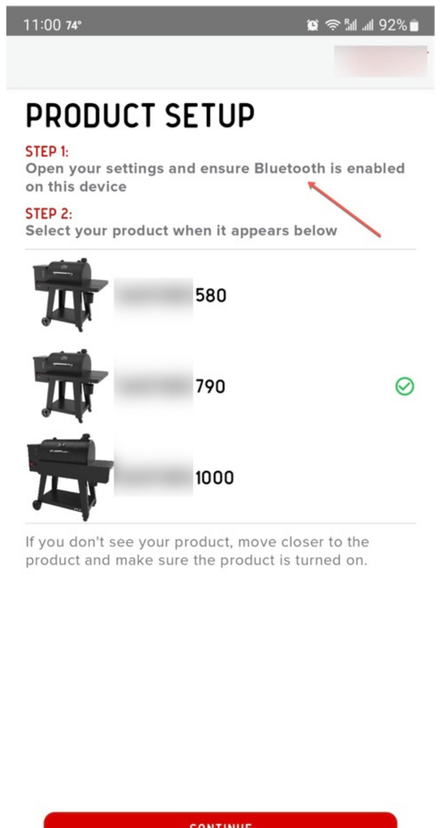
```
            if (PreferenceHelper.read(PreferenceHelper.CONNECTDEVICEN , false).booleanValue() ||      == null) {
                return;
            }
                    .addIntoQueue(new BleCommandMaker().getFileContent("init.js", 20), BaseBleServiceActivity.QUERY_COMMAND);
            return;
        }
        Crashlytics crashlytics3 = Crashlytics.INSTANCE;
        str2 = BluetoothLeService.TAG;
        crashlytics3.d(str2, "STATUS notification registered.");
                 = BluetoothLeService.this.blindActivity;
        if (      == null) {
            return;
        }
                 .onBleConnected();
    }
};
private final IBinder mBinder = new LocalBinder(this);

public final int getConnectionState() {
    return this.connectionState;
}

public boolean getBluetoothConnectDeviceisNXG1() {
    return this.bluetoothConnectDeviceisNXG1;
}
```

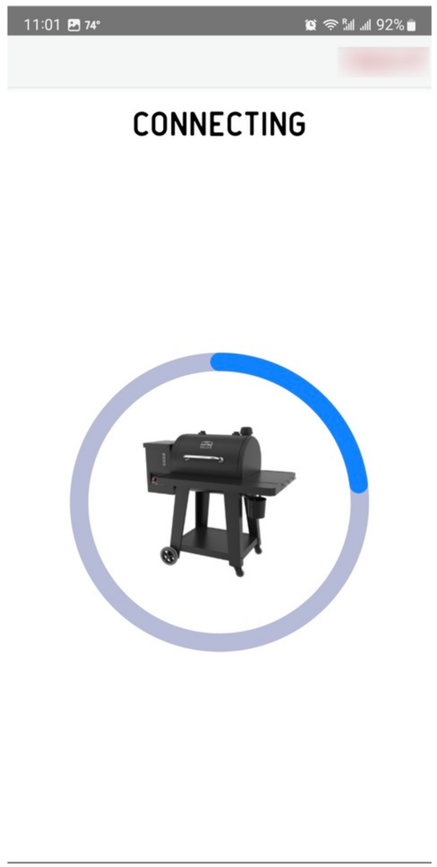
Is there a way to replace **init.js** with something valuable from the attacker's perspective?

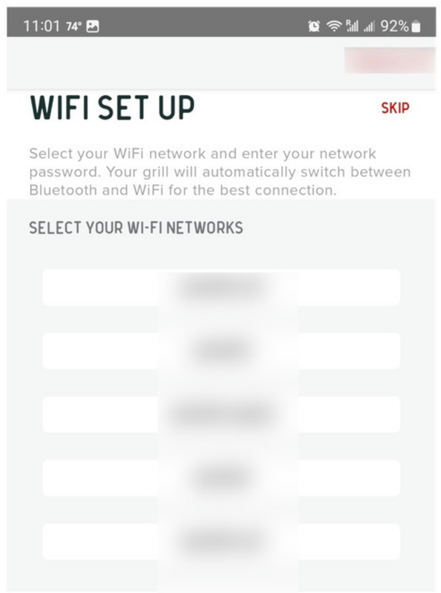
```
public final String getFileContent(String fileName, int i) {
    Intrinsics.checkNotNullParameter(fileName, "fileName");
    return " {\"id\":999,\"method\":\"FS.Get\",\"params\":{\"filename\":\"" + fileName + "\", \"offset\": 0, \"len\":" + i + "}} ";
}

public final String setUpWiFiWithSecurity(String ssid,      ring wifiPassword) {
    Intrinsics.checkNotNullParameter(ssid, "ssid");
    Intrinsics.checkNotNullParameter(wifiPassword, "wifiPassword");
    return "{  \"id\": 1205,  \"method\": \"Config.Set\",  \"params\":      \"config\": {      \"http\": {      \"hidden_files\": \"*.*\"
}

public final String sendSSID(String ssid) {
    Intrinsics.checkNotNullParameter(ssid, "ssid");
    return "{\"id\":1205,\"method\":\"Config.Set\",\"params\":{\"config\":
}

public final String sendPass(String pass) {
    Intrinsics.checkNotNullParameter(pass, "pass");
    return "{\"id\":1204,\"method\":\"Config.Set\",\"params\":{\"config\":
}

public final String setAWSFrequency(int i) {
```

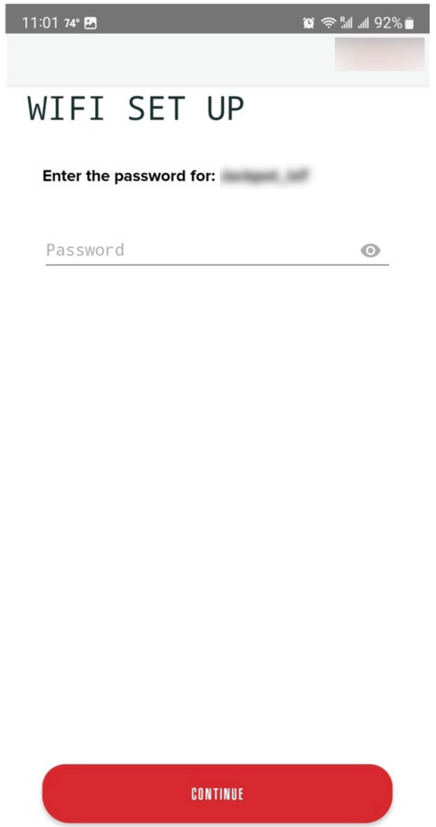
Might **FS.Get** method be a clue of the target operating system ?

# INSTALLING THE APPLICATION



# CAPTURING THE BLE PACKETS

Followed the same method*

I used to hack my treadmill with

my Samsung Galaxy S smartphone

(Write-up: Run Mert Run*)

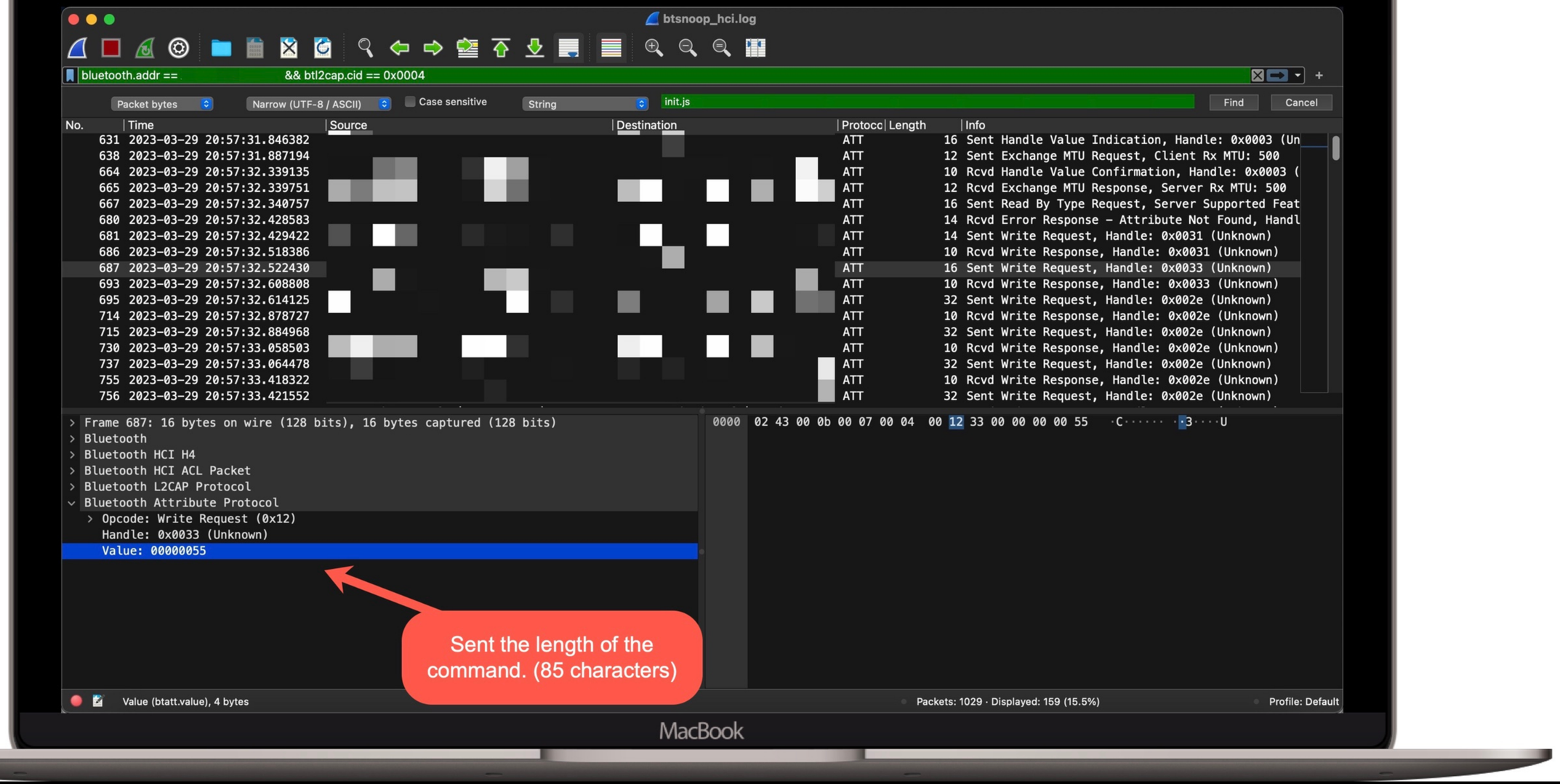
*Hack4Career *Samsung

Steps To Capture btSnoop & dumpsate Logs-

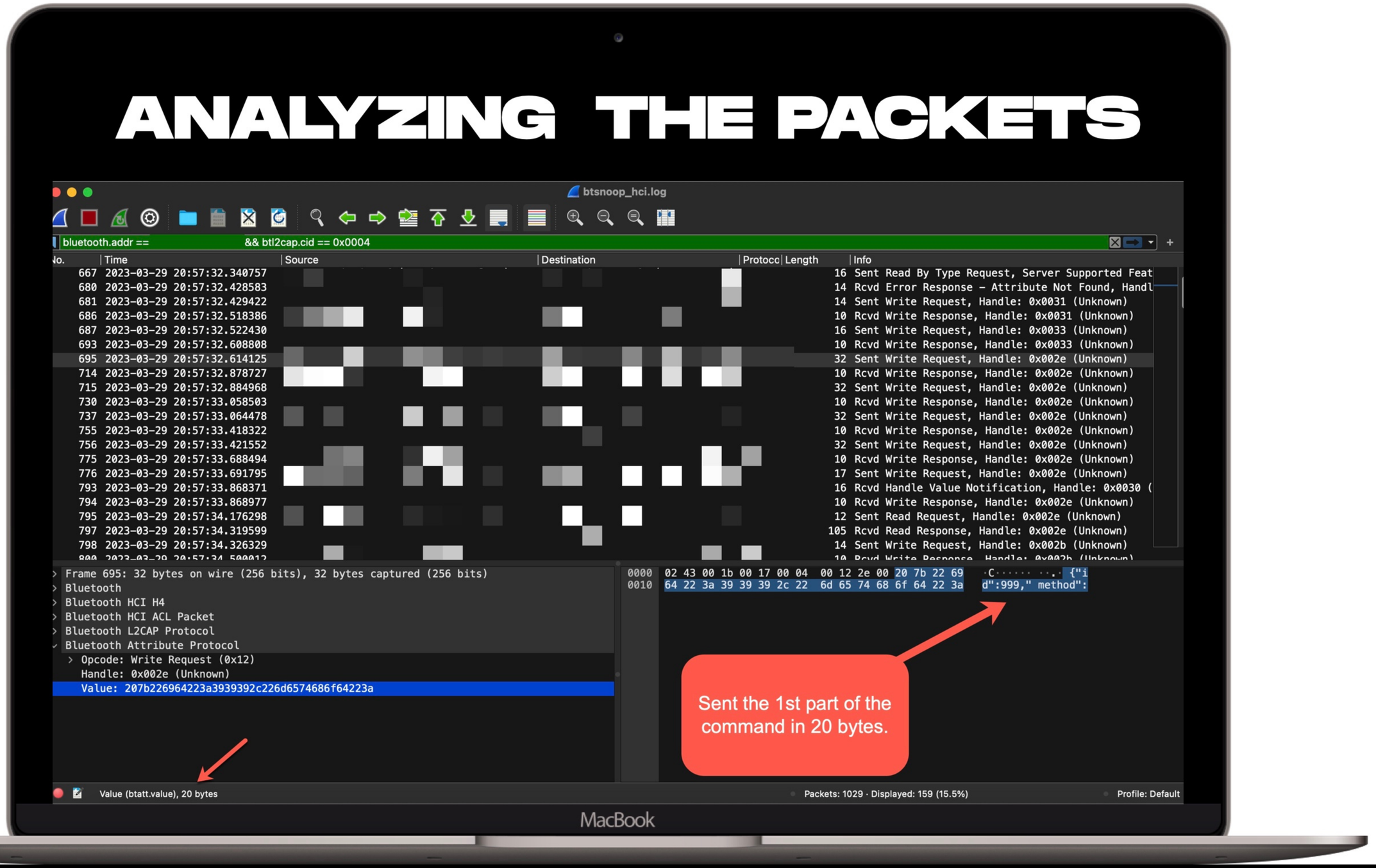
1. Press *#9900# on the dialer.
2. On USER Binary Go to Settings->About Device : Tap 7 times on Build Number to enable Developer Options
3. Go to Settings->Developer Options->Bluetooth HCI snoop log -> Enable this check box
4. Flight Mode > On / Off
5. Press *#9900# on the dialer -> Change Debug Level Disabled/LOW to MID -> Reboot device
6. REPRODUCE the issue scenario
7. Then capture the logs.
   a) Press *#9900# on the dialer
   b) Click on “RUN DUMPSTATE/LOGCAT”
   c) It will start dumping the dumpstate.
   d) Once it complete, Click on the “COPY TO SDCARD(INCLUDE CP RAMPDUMP”.
   e) Dumpstate will be stored in the device storage.
8. Attach the device to PC
9. Get the logs from the device LOG folder and share it with us.(This LOG folder will contain both btsnoop & dumpstate log files)
   Note : From the log folder in device, please ensure that files ‘dumpstate...’ and ‘btsnoop...’ files are present.

# ANALYZING THE PACKETS

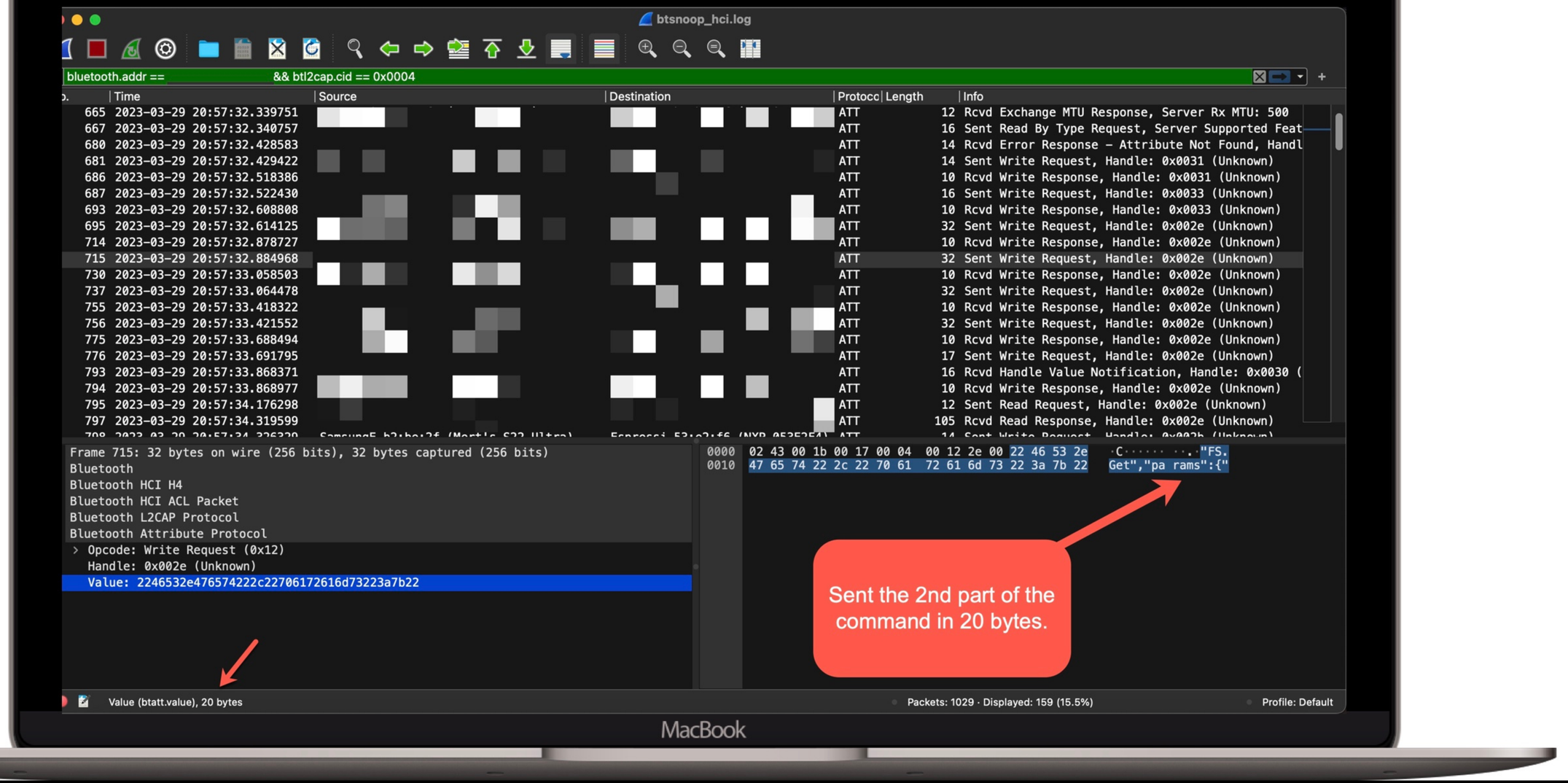
# ANALYZING THE PACKETS



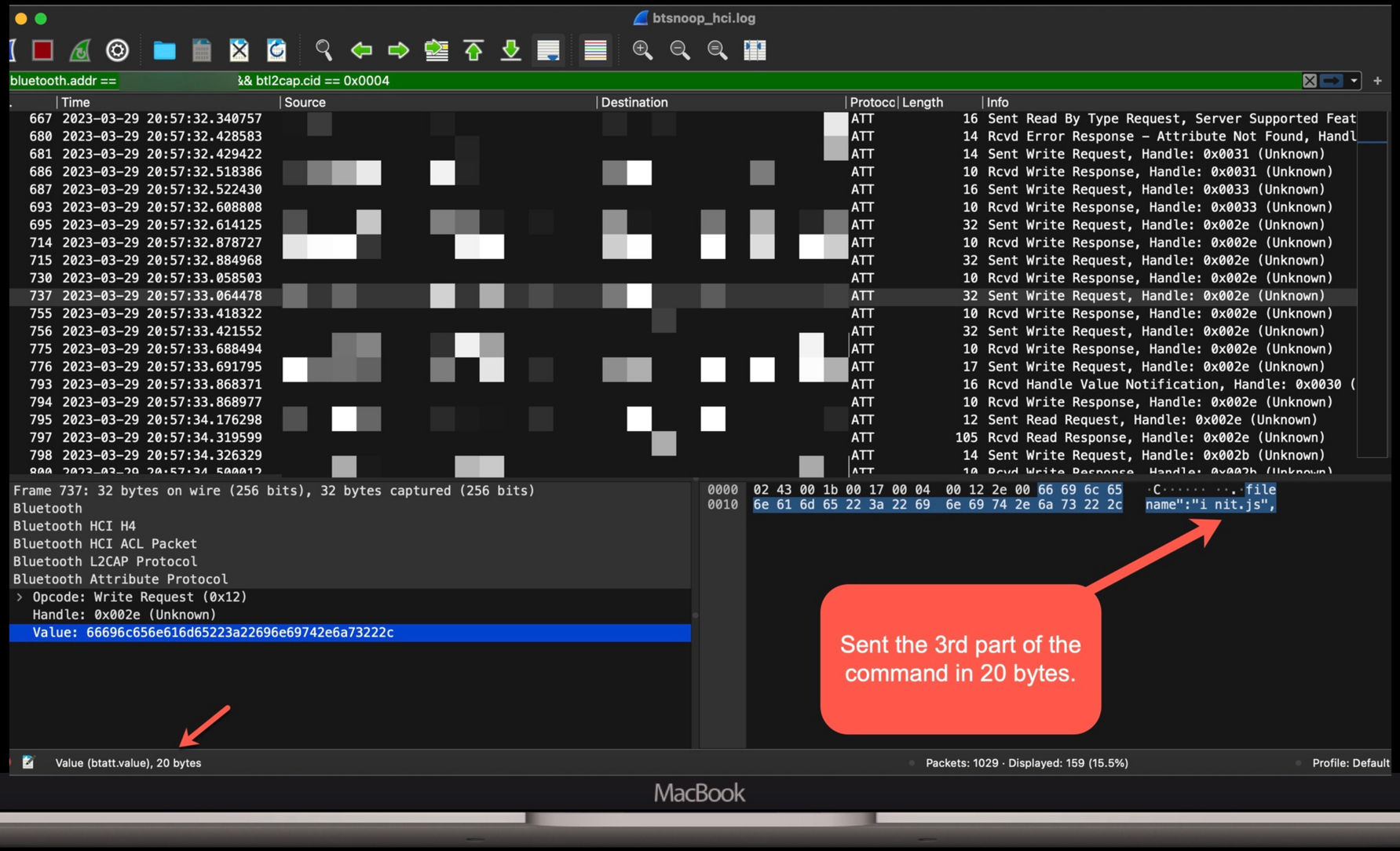
# ANALYZING THE PACKETS



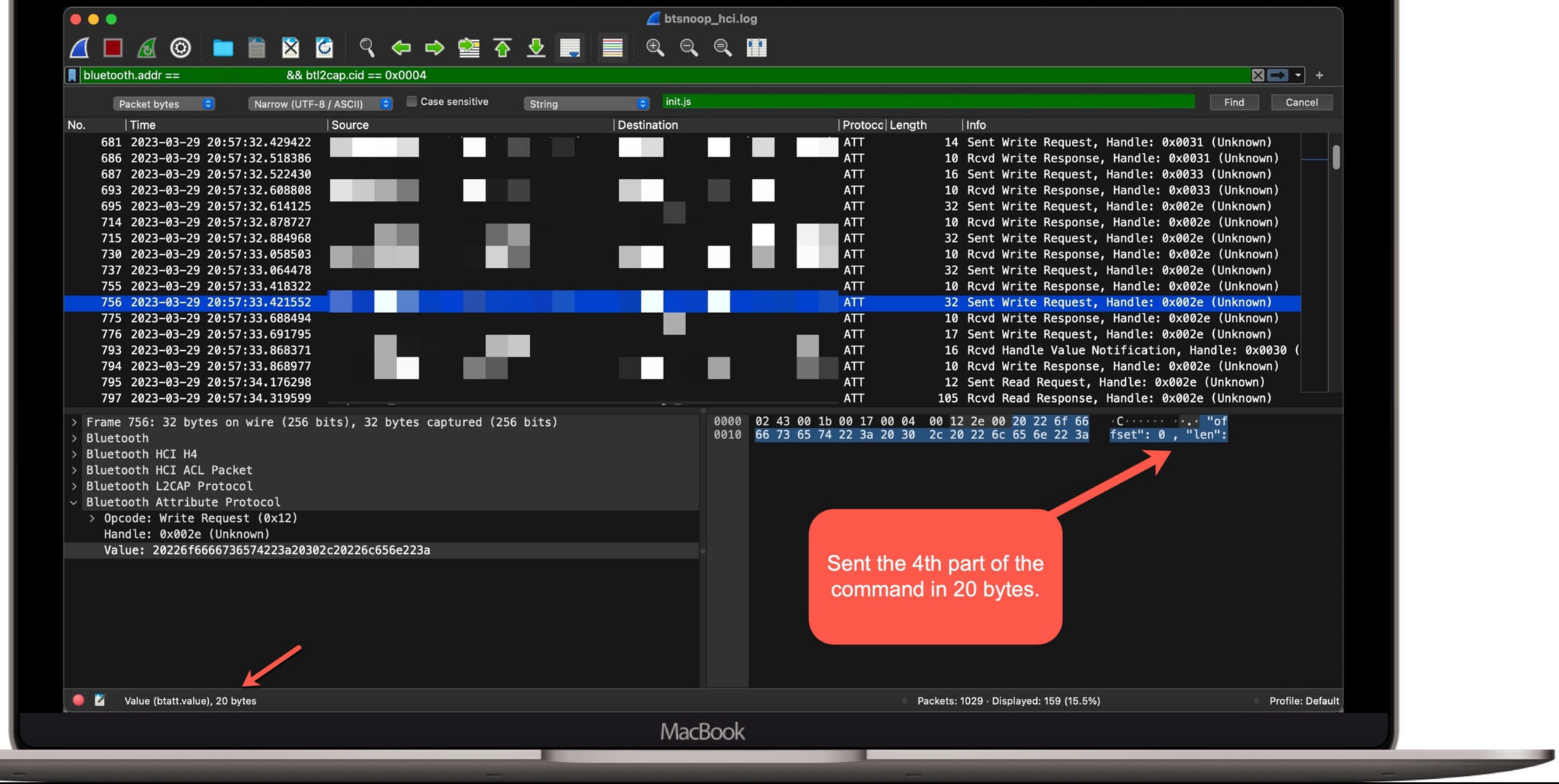
# ANALYZING THE PACKETS



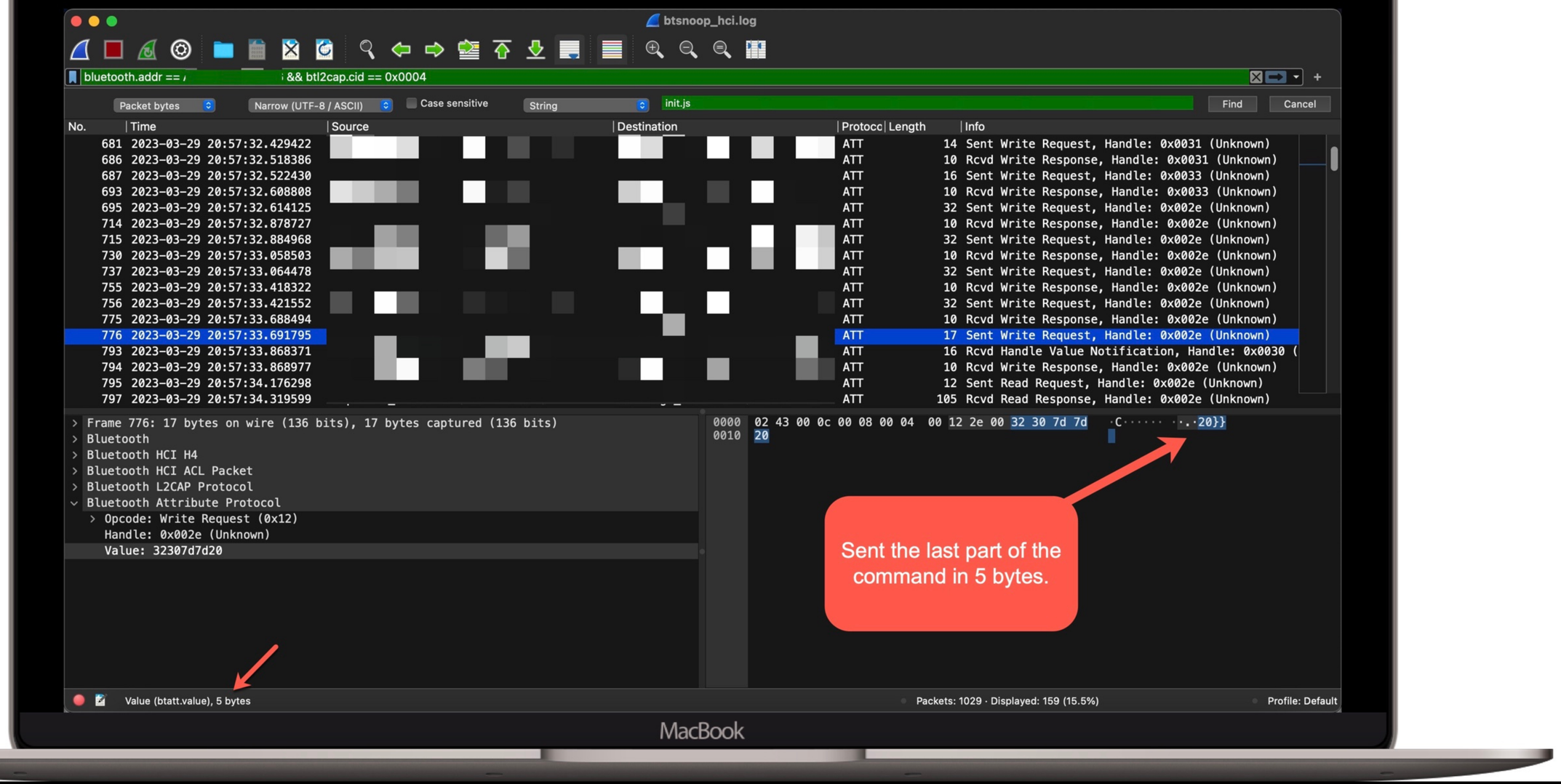
# ANALYZING THE PACKETS



# ANALYZING THE PACKETS



# ANALYZING THE PACKETS



BleConfiguration

```java
package nex;

import java.util.HashMap;

/* loaded from: classes3.dex */
public class BleConfiguration {
    public static String CHARACTERISTIC_[redacted]_SUBSCRIBE = "306d4f53-5f44-4247-5f6c-6f675f5f5f30";
    public static String CHARACTERISTIC_[redacted]_WRITE_COMMAND = "5f6d4f53-5f52-5043-5f64-6174615f5f5f";
    public static String CHARACTERISTIC_[redacted]_WRITE_DATA_LENGTH = "5f6d4f53-5f52-5043-5f74-785f63746c5f";
    public static String CLIENT_CHARACTERISTIC_CONFIG = "00002902-0000-1000-8000-00805f9b34fb";
    public static String MODEL_[redacted]_SUBSCRIBE = "[redacted] Subscribe Service";
    public static String MODEL_[redacted]_WRITE = "[redacted] WRITE services";
```

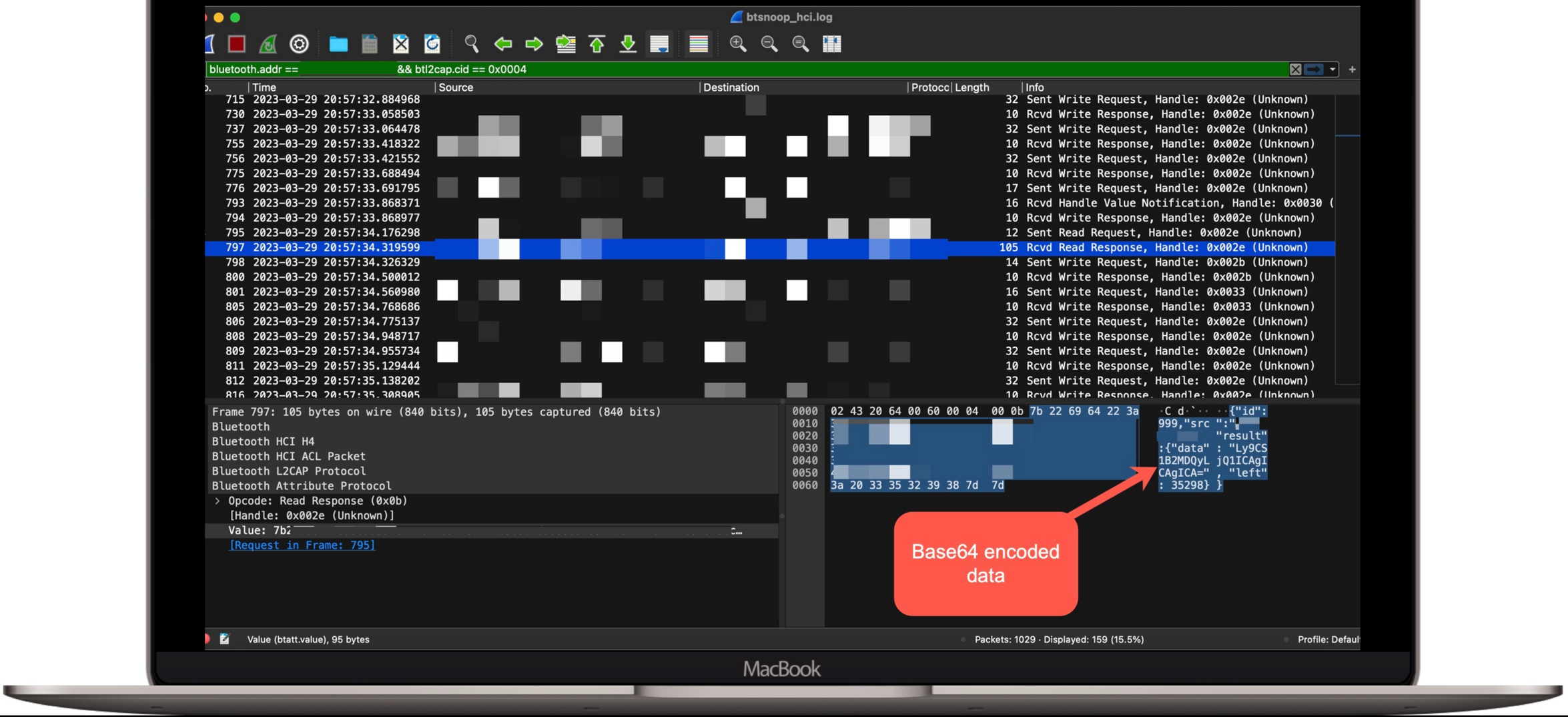
# ANALYZING THE PACKETS

- The mobile application sent;
  - “**00000055” (85 in decimal)** value to **CHARACTERISTIC_XXXXX_WRITE_DATA_LENGTH** characteristic.

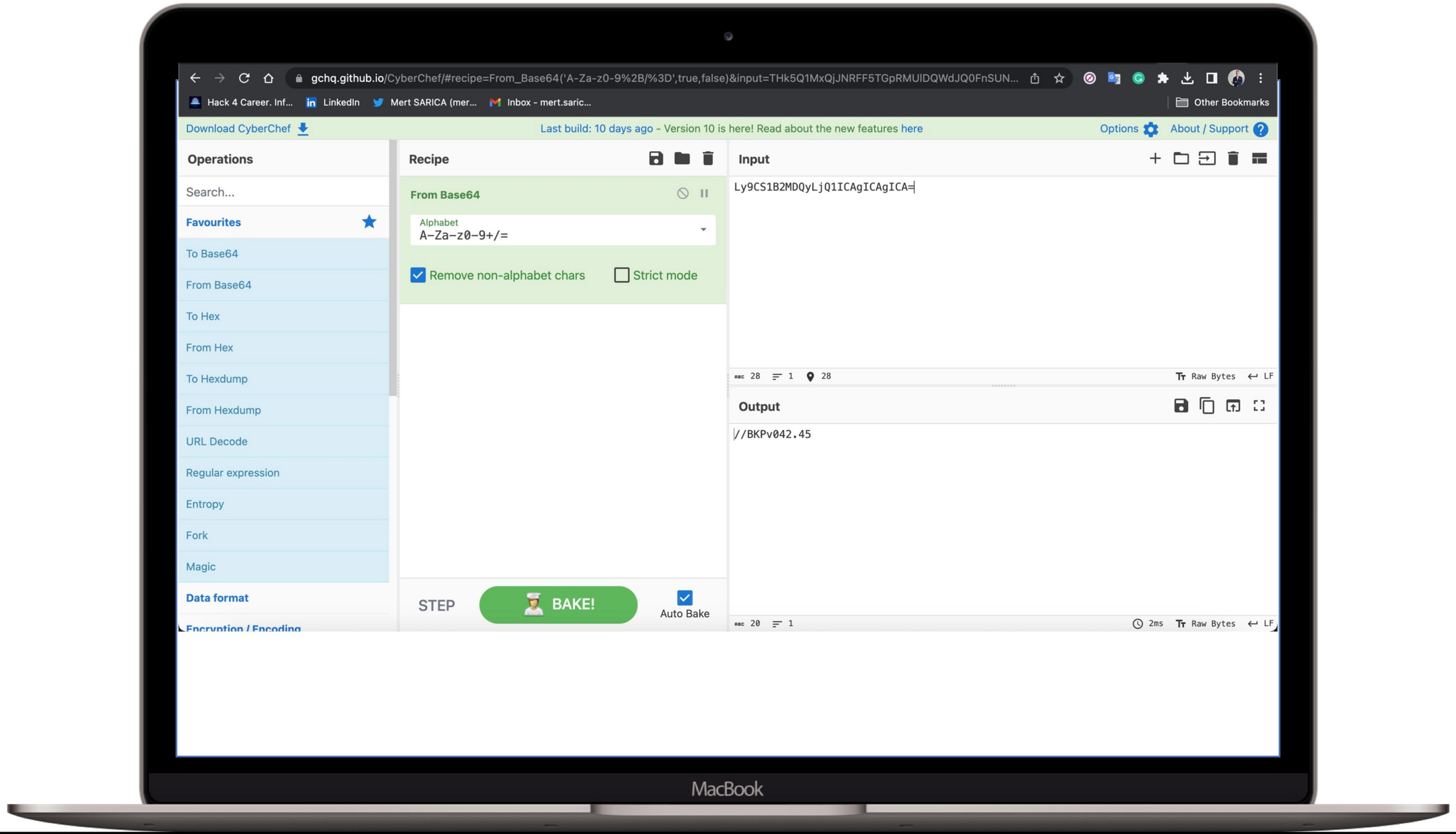
- **{“id”:999,”method”:”FS.Get”,”params”:{“filename”:”init.js”,”offset”: 0 , “len”:20}}** command to **CHARACTERISTIC_XXXXX_WRITE_COMMAND** characteristic in 5 pieces.

- Summary in human-readable form;
  - Notified the pellet grill of the length of the command. (**85 chars**)
  - Sent the command to read the content of **init.js** file.

# ANALYZING THE PACKETS

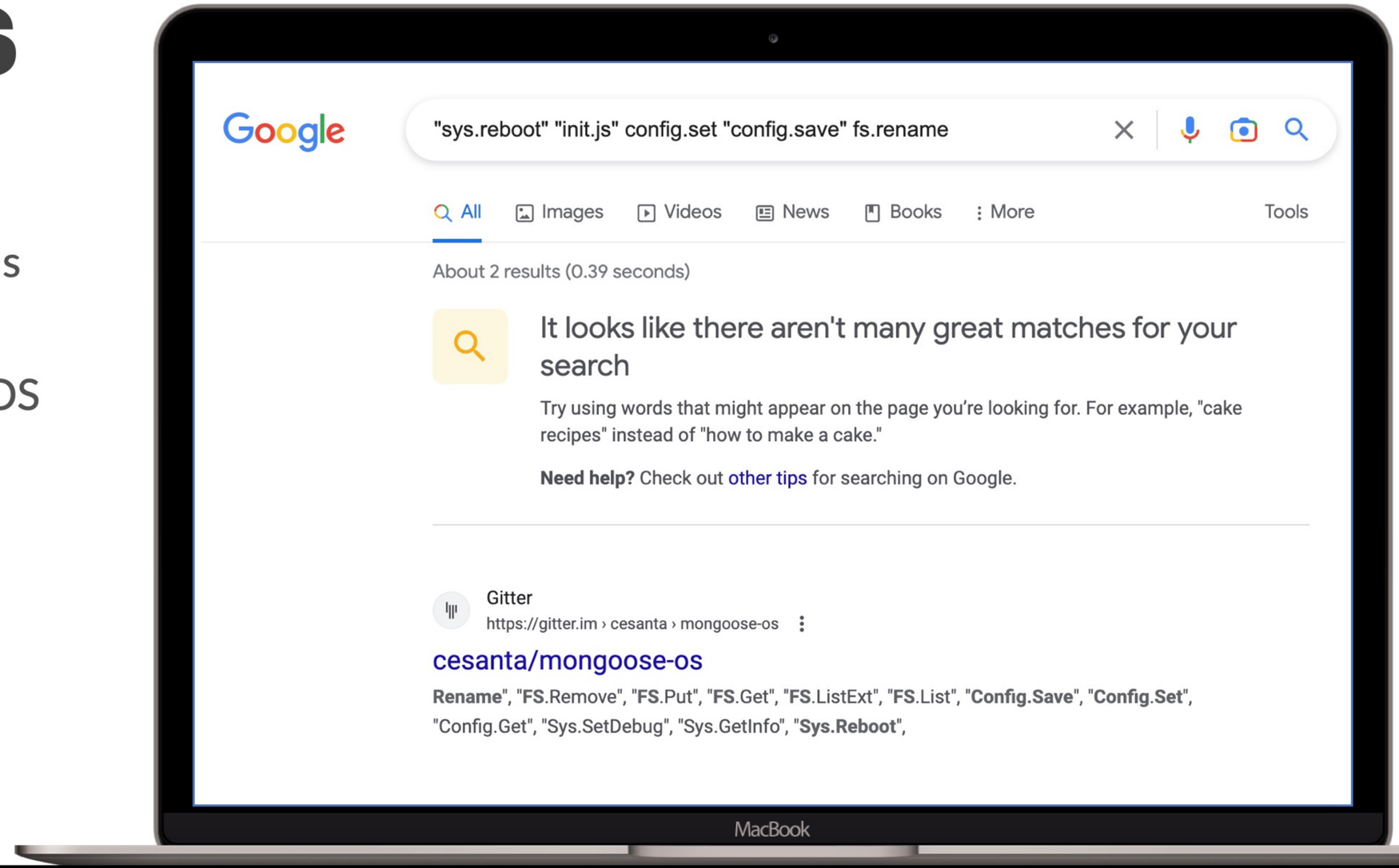



MacBook

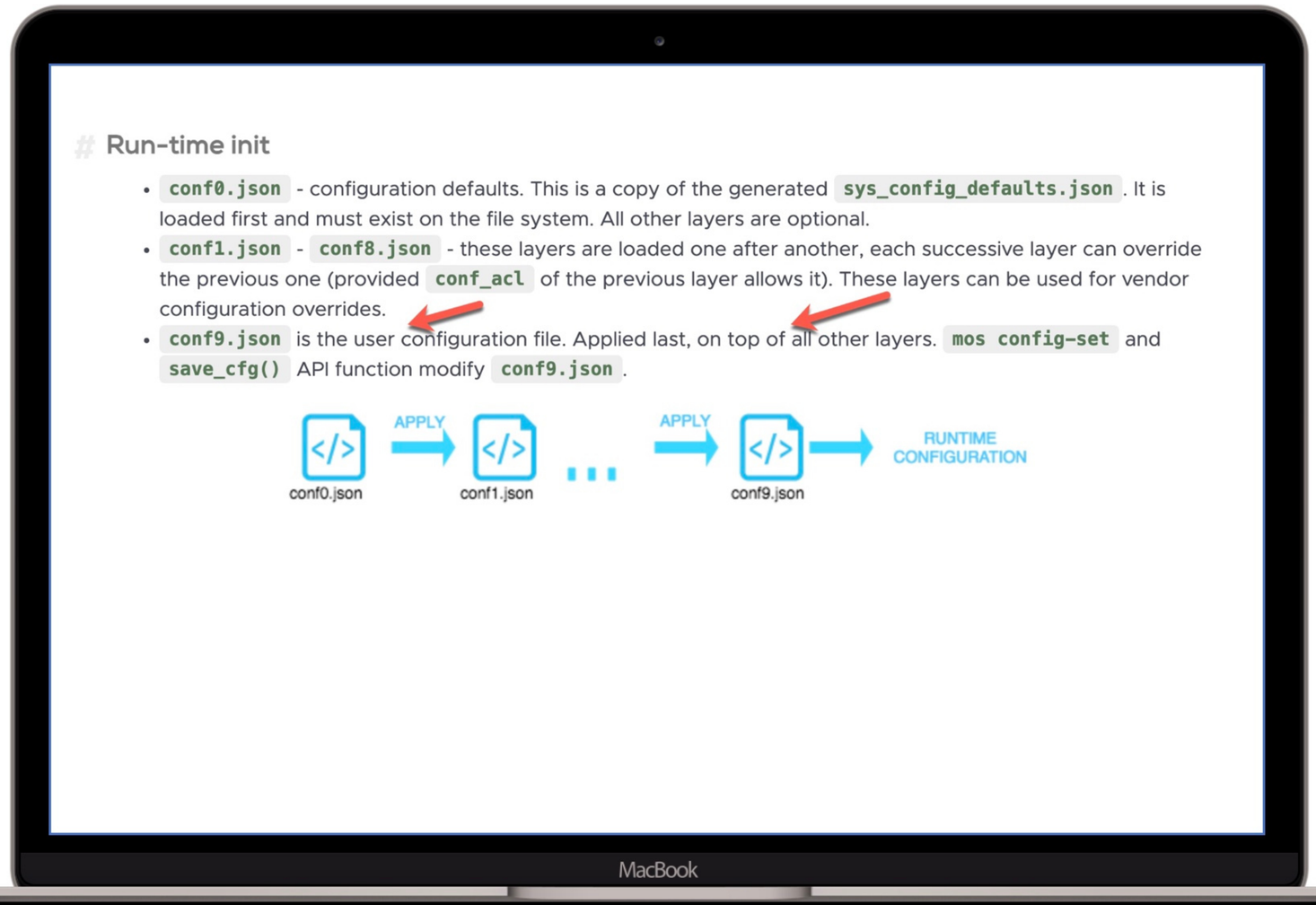

gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)&input=THk5Q1MxQjJNRFF5TGpRMUlDQWdJQ0FnSUN...
Hack 4 Career. Inf...
LinkedIn
Mert SARICA (mer...
Inbox - mert.saric...
Other Bookmarks
Download CyberChef
Last build: 10 days ago - Version 10 is here! Read about the new features here
Options
About / Support
Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Fork
Magic
Data format
Encryption / Encoding
Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
Strict mode
STEP
BAKE!
Auto Bake
Input
Ly9CS1B2MDQyLjQ1ICAgICAgICA=
28
1
28
Raw Bytes
LF
Output
//BKPv042.45
20
1
2ms
Raw Bytes
LF
MacBook

# DETERMINING THE OS

- Searched some of the filenames and methods on Google.
- Determined that the OS is **Mongoose OS***.



# DETERMINING THE FILENAME



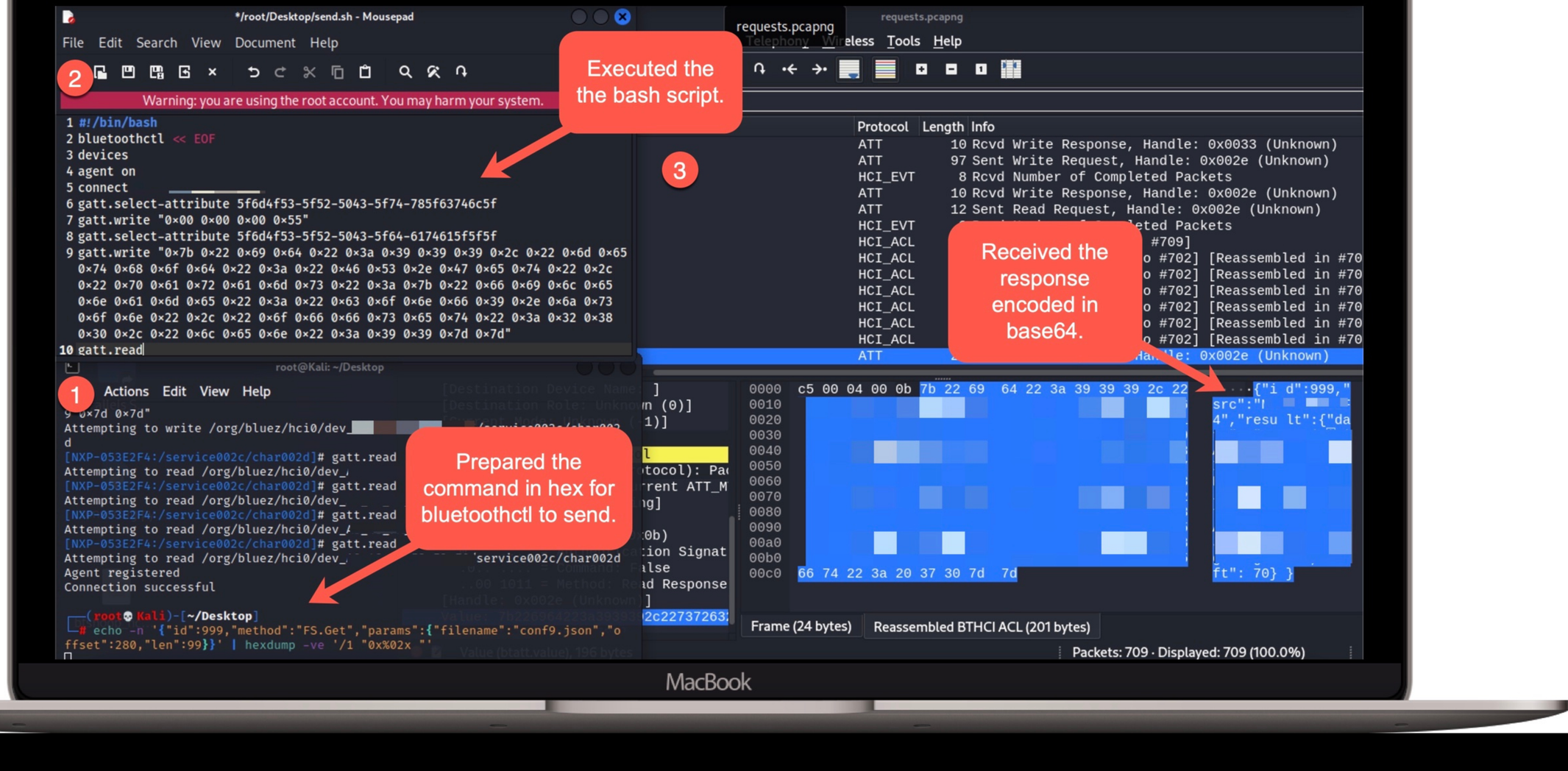

- Mongoose OS uses a structured, multi-layer configuration.
- It consists of two parts: a compile time part that defines configuration, and a run time part that uses configuration.
- **conf9.json** is the user configuration file. Applied last, on top of all other layers.

# PREPARING THE PACKETS

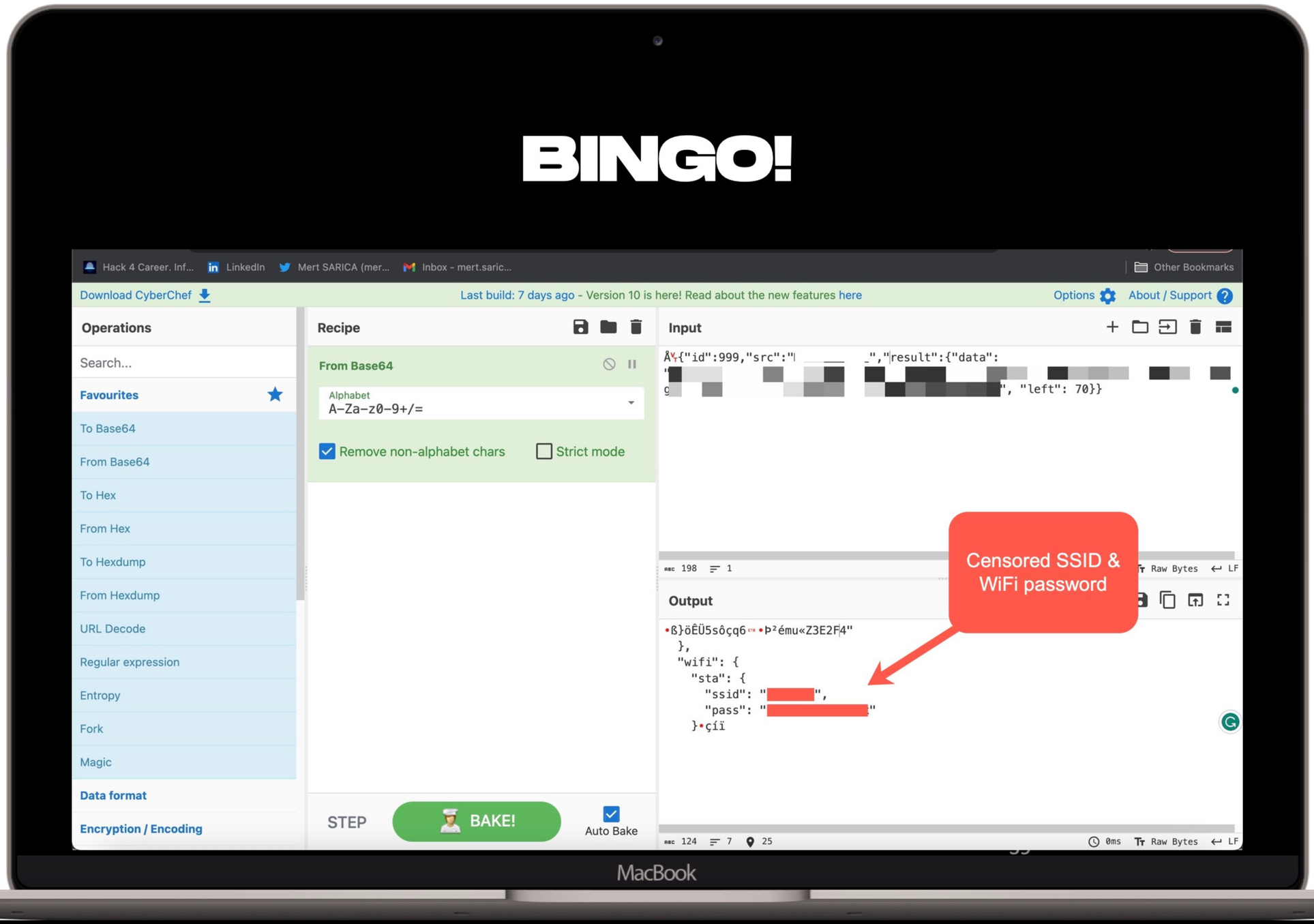
- The **bluetoothctl** is a handy tool for communicating with a **BE** device over the GATT protocol, to query the list of “Services” and “Characteristics” for manipulating the attributes.
- Prepared the command below and sent it to the pellet grill.

**{“id”:999,”method”:”FS.Get”,”params”:{“filename”:”conf9.json”,”offset”:280,”len”:99}}**

# REQUEST & RESPONSE



# BINGO!


Hack 4 Career. Inf...
LinkedIn
Mert SARICA (mer...
Inbox - mert.saric...
Other Bookmarks
Download CyberChef
Last build: 7 days ago - Version 10 is here! Read about the new features here
Options
About / Support
Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Fork
Magic
Data format
Encryption / Encoding
Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
Strict mode
STEP
BAKE!
Auto Bake
Input
Output
Censored SSID & WiFi password
Raw Bytes
LF
MacBook

# NOTIFIED THE MANUFACTURER IN APRIL BUT NO RESPONSE YET

Responsible Vulnerability Disclosure for [redacted] Pellet Grill

**Mert SARICA** <mert.sarica@gmail.com>
to support

Sat, Apr 1, 11:29 AM (3 days ago)

Dear Sir or Madam,

My name is Mert, and I am a seasoned cybersecurity professional who conducts cybersecurity research and publishes them on my blog for the benefit and awareness of the public.

According to various research, IoT (internet of things) devices, such as coffee machines, thermostats, smart speakers, smart bulbs, alarm systems, etc., might have vulnerabilities (https://www.fortinet.com/resources/cyberglossary/iot-device-vulnerabilities) due to their limited software and hardware capabilities.

Recently I purchased an [redacted] Pellet Grill from Home Depot two weeks ago. (By the way, I love cooking with my grill; it is fantastic!) I noticed that my grill as an IoT has Wi-Fi and Bluetooth features and can be controlled via a mobile app (https://play.google.com/store/apps/details?id=[redacted]&hl=en_US&gl=US). After I went through to installation procedure, I enrolled my grill into my Wi-Fi network.

# KEY TAKEAWAYS

- Surprisingly, the vulnerability can be exploited even if the grill is not turned on (POWER ON) and only plugged in.
    - If not necessary, keep your BLE IoTs unplugged.
    - Isolate your IoTs from your personal devices. (Guest network)
- Never underestimate your home network security. Harden it!
- Pentest your IoT devices if you can. Challenge yourself.

# ENJOY YOUR GRILL

## With Guest Network

# DON'T FORGET TO REGISTER. IT'S FREE!

# CONTACT


MertSARICA

@MertSARICA

www.hack4career.com

mert.sarica@gmail.com