Title:

Industrial Scale Hardware Hacking

Presented By: Anthony S. Clark

Introduction

Name:	**Anthony S. Clark**
Title:	Owner / Principal Researcher Red Crow Lab
Contact:	asclark@redcrowlab.com
Focus:	Reverse engineering, vulnerability discovery, PoC devel
Background:	**- LANL**: Red Team Founder, CSIRT Member, X-DIV Tech Sec, Int. Applied Tech - Research Scientist 4, Guest Scientist
	- Founder / CEO Attack Research: Security consulting (Exxon, Facebook, GM, Bridgewater, Panasonic Avionics, DOD, IC)
	- Founder / CTO Boldend: Software tooling for IC & FVEY
	- Founder Red Crow Lab: Hardware/Software RE, Tool Dev
	- Speaker & Trainer: Blackhat, Defcon, SANS, Infragard, BSides
	- **Original Contributor**: Metasploit, Cisco ThreatGrid, PTES, DARPA Cyber Fast Track

Specialty

Taking custom or proprietary technologies

Learning them,

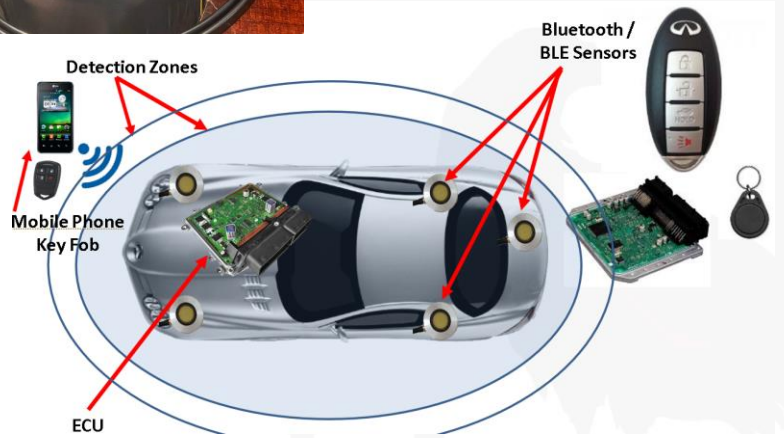
Reversing them,

& Leveraging them.

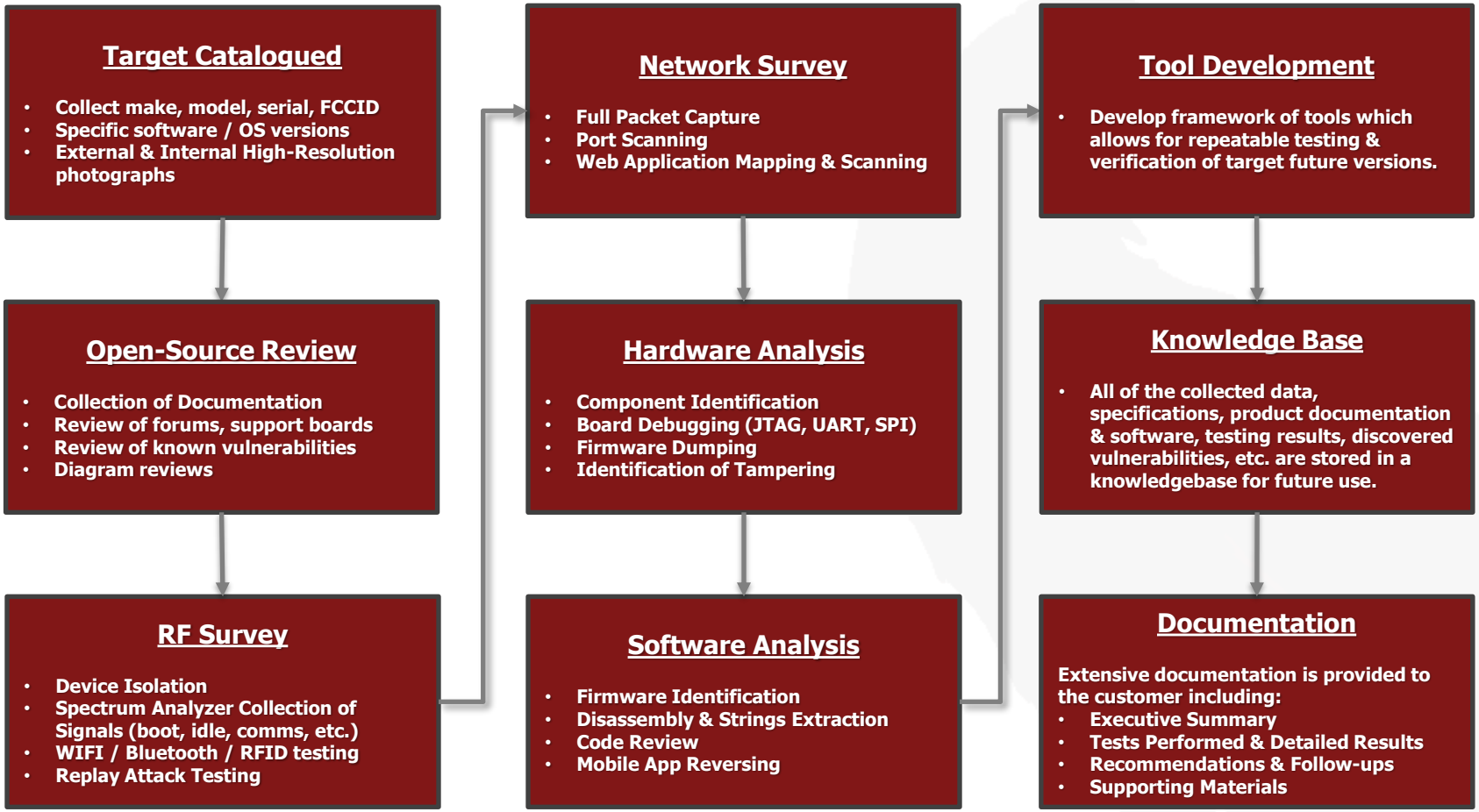
Types of Devices

- Scientific Instruments
- Avionics
- Automotive
- Security (ex. Locks)
- Legacy (Ex. AS400)
- Satellite
  - sensors
- OT/ICS/SCADA
- Financial
  - ATMs
  - POS
- Telecom
  - Routers
  - Switches
- Mobile

System Control Unit (SCU)



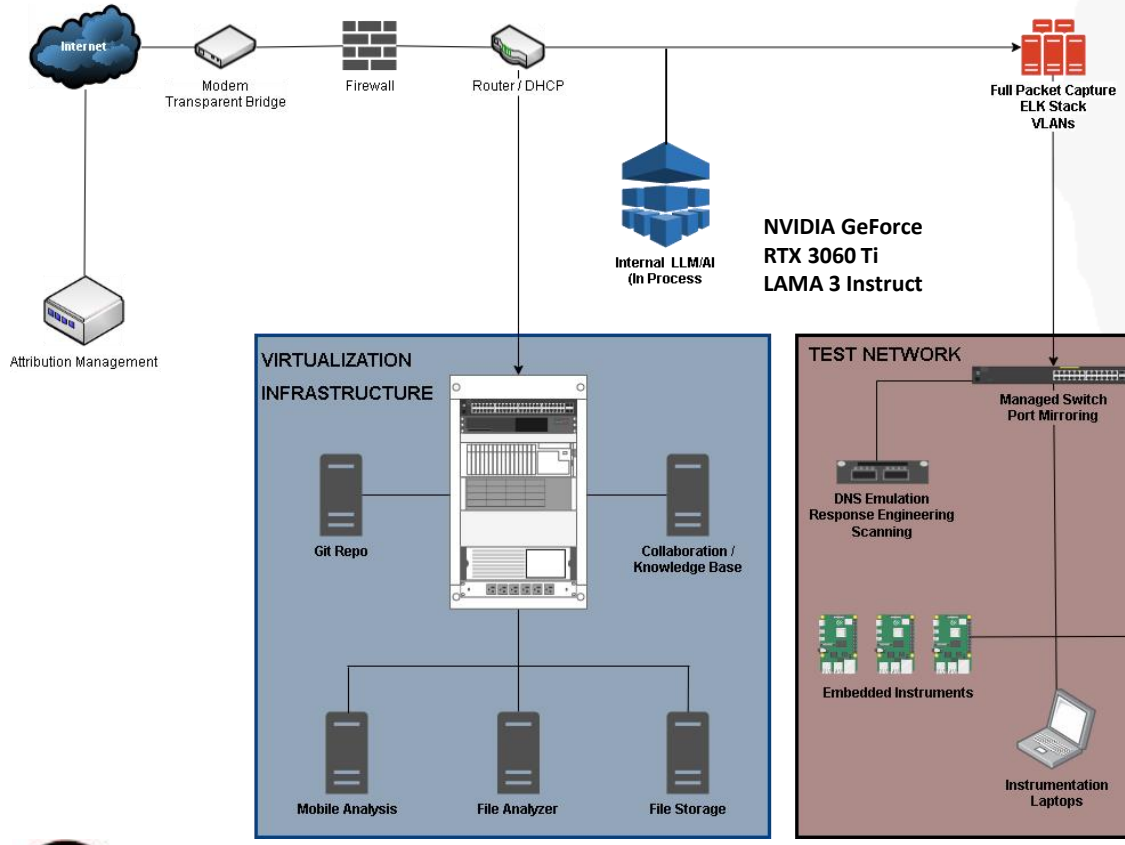
Industrial Scale Hardware Hacking Process



Setting Up A Lab

BENCH CONCEPT

INSTRUMENTATION COLLECTION
- Modifications
  - Network
  - File System
  - Process Table
  - Registry
  - Memory
  - Signals



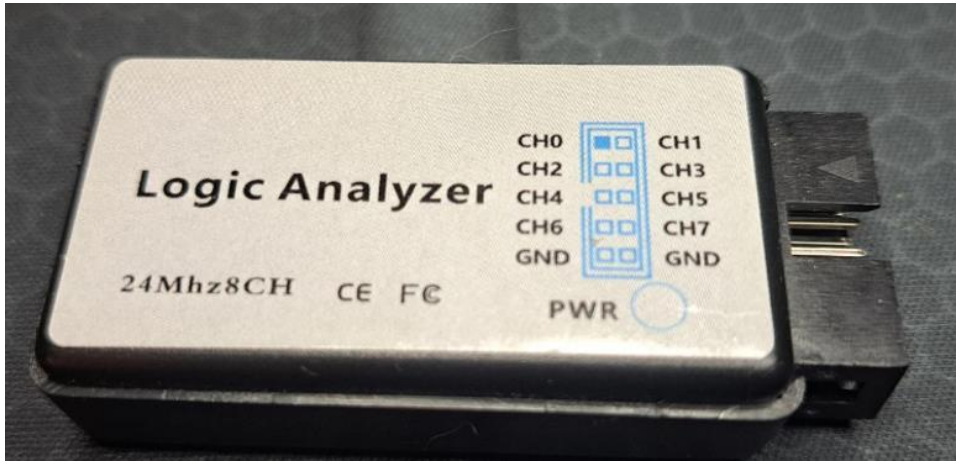
RF TEST BENCH

LAB GEAR
- Signal Isolation
- Spectrum Analysis
- Near Field Probing
- WIFI & Bluetooth Analysis
- Replay Tools
- RFID & Proxcard readers / writers
- SDRs

HARDWARE TEST BENCH

LAB GEAR
- Oscilloscopes
- Logic Analyzers
- JTAG/SPI/UART Debuggers
- Soldering & Hot Air Rework Stations
- Chip programmers / firmware dumpers
- Multimeters
- HID Emulators
- High Resolution Photography & Imaging

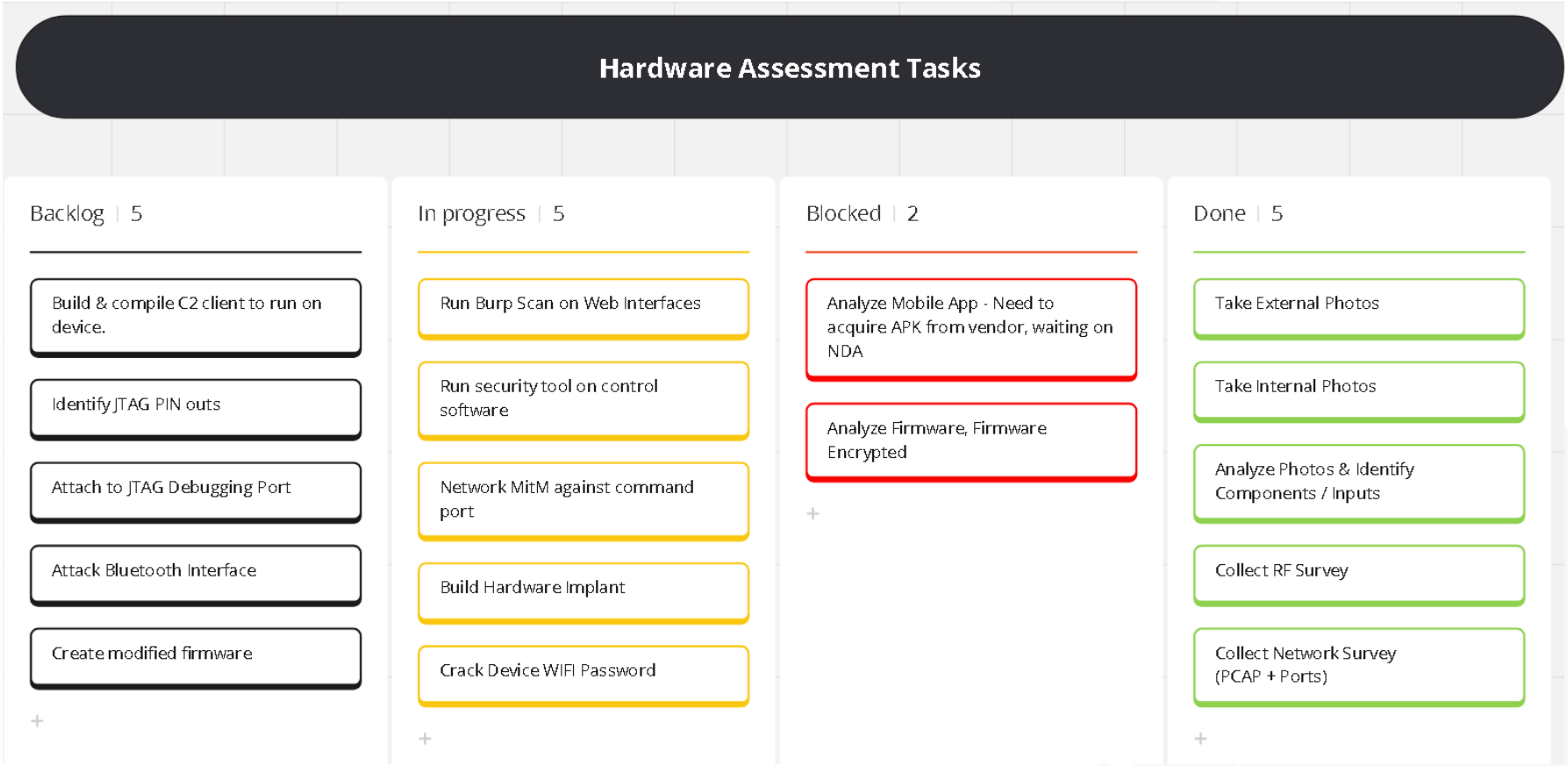
Lab Equipment



Lab Equipment

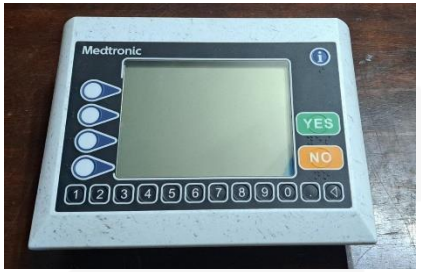
- **Network Gear**
  - Network Isolation / Network Switch With Port Mirroring / Router
  - Jump Hosts
  - DNS Control / Dynamic Host Configuration Protocol (DHCP) Server
  - Full Packet Capture
  - Man In The Middle (MiTM) Tools (fiddler, Ettercap, sslstrip)
- **Small Programmable Devices**
  - Arduino / Raspberry Pi / BeagleBone / Teensy / NanoPi / OrangePi
- **Radio Frequency Analysis**
  - HackRF / BladeRF / UberTooth / Proxmark / FlipperZero / Pineapple / SDR
- **Hardware Debugging & Measurement**
  - Multimeters
  - Oscilloscope
  - Logic Analyzer
  - Chip Reader - Dataman 48Pro2 Universal Programmer /
- **Imaging**
  - High Resolution Camera & Lighting
  - Electronics Microscope

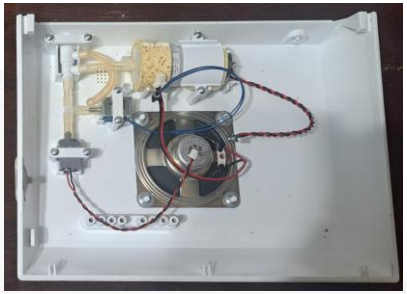
Build a Kanban Board



Target Catalogue

ITEM	VALUE
MAKE:	Medtronic
MODEL:	Commander Flex CD320-GV
SERIAL NUMBER:	1000869493
FCCID:	XTQ-CO320 IQOOBLE113
DESCRIPTION:	Medical Telemonitoring Device, is capable sending important medical information to your doctor, and or medical healthcare professional, via a wired telephone line. Measures weight, peak blood flow, oxygen saturation, blood pressure, and/or blood glucose levels
DATASHEET:	https://fccid.io/XTQ-CD320/User-Manual/User-Manual-2976121
IO:	USB RJ11 7V DC Power Audio PS2

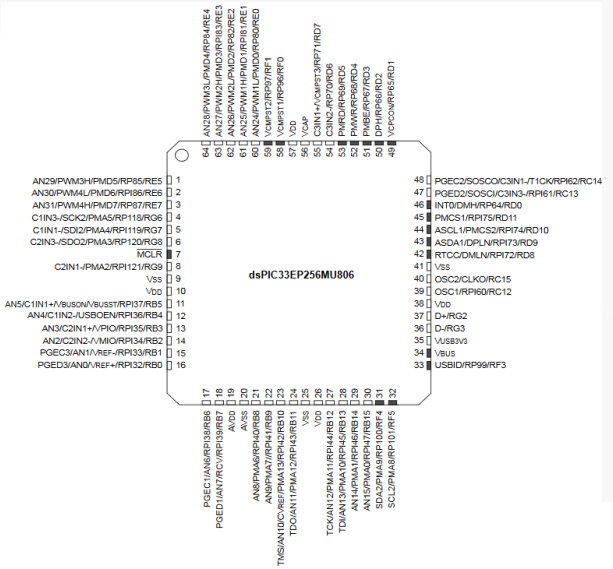




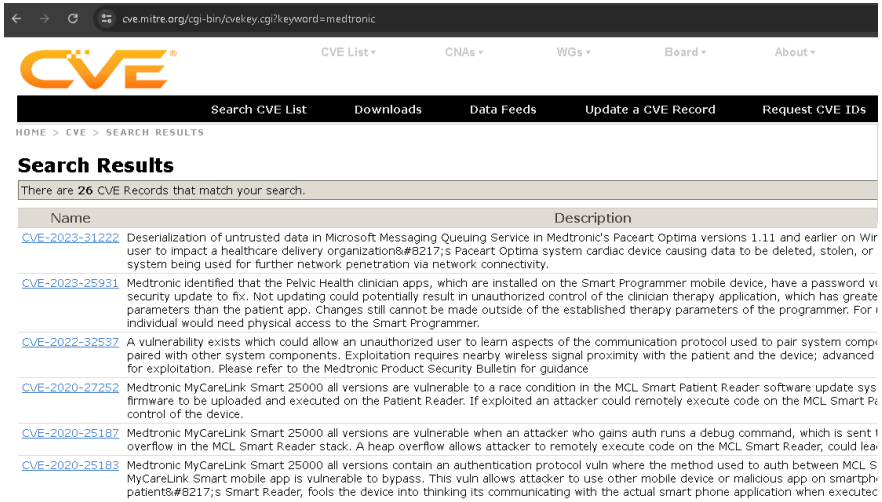
Target Catalogue

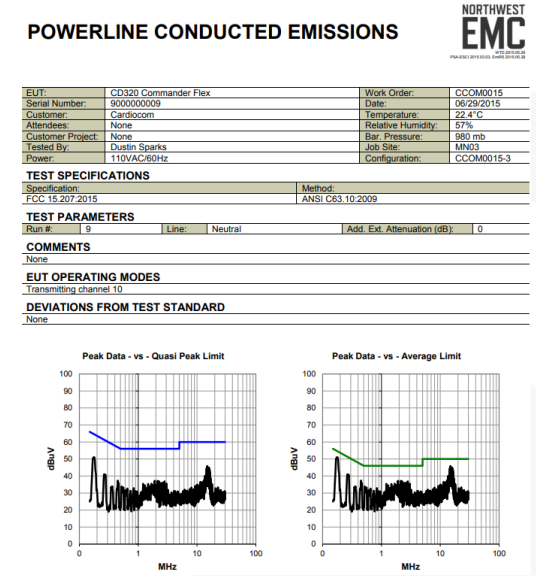
- Identify Critical Chips

ITEM	VALUE
MAKE:	Microchip
MODEL:	PIC24EP512
DESCRIPTION:	Primary microcontroller. The **PIC24EP512** has an 16-bit **CPU** core, (**C** and **Assembly**) based , with **IEEE 1149.2** Compatible (**JTAG**) Boundary Scan. A well as **15-Channel DMA** (**Direct Memory Access**) with User-Selectable Priority Arbitration: • 15-Channel DMA with 4 UART modules **(15 Mbps)**, with support for UART, SPI, ADC, ECAN and OC. • Four 4-Wire SPI modules **(15 Mbps)** • Two ECAN™ modules **(1 Mbaud)** CAN 2.0B Support • Two I2C modules **(up to 1 Mbaud)** with SMBus Support • Data Converter Interface **(DCI)** module with Support for I2S • Programmable Cyclic Redundancy Check **(CRC)** • Parallel Master Port **(PMP)** • PPS to allow Function Remap
DATASHEET:	https://ww1.microchip.com/downloads/aemDocuments/documents/OTH/ProductDocuments/DataSheets/70616g.pdf

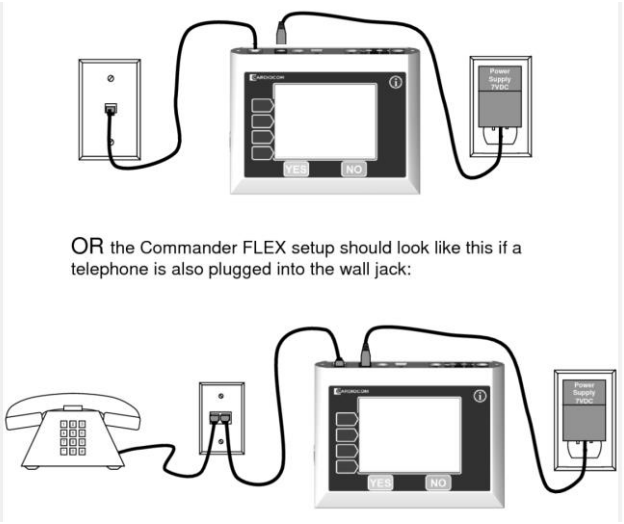


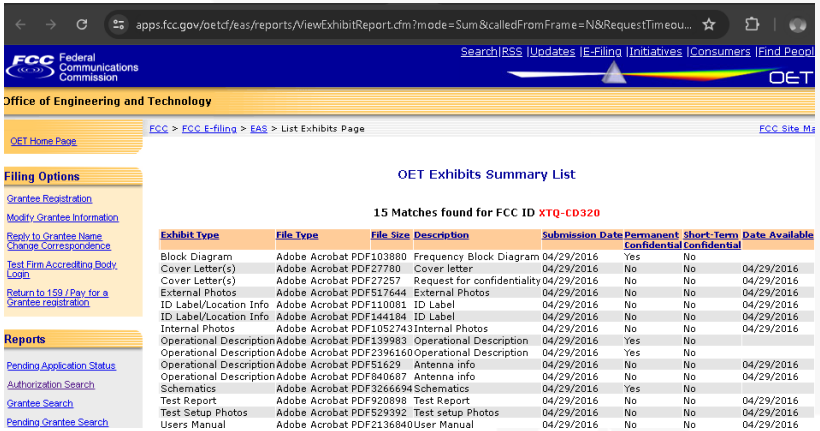
Open Source Review





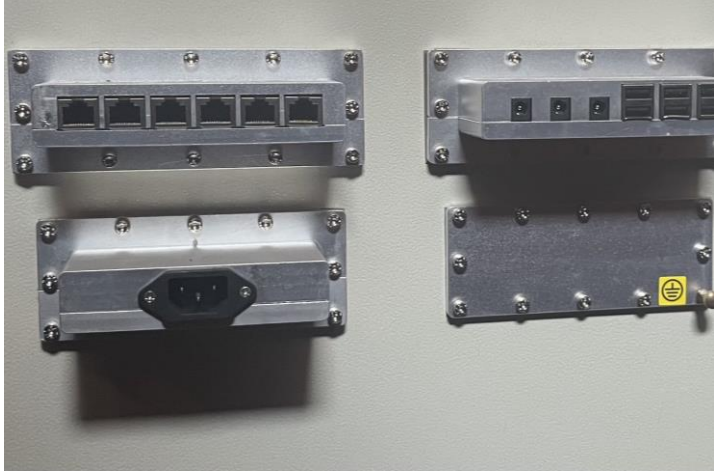
- Forums
- CVE / Vuln DBs
- FCCID Lookup
- Reddit

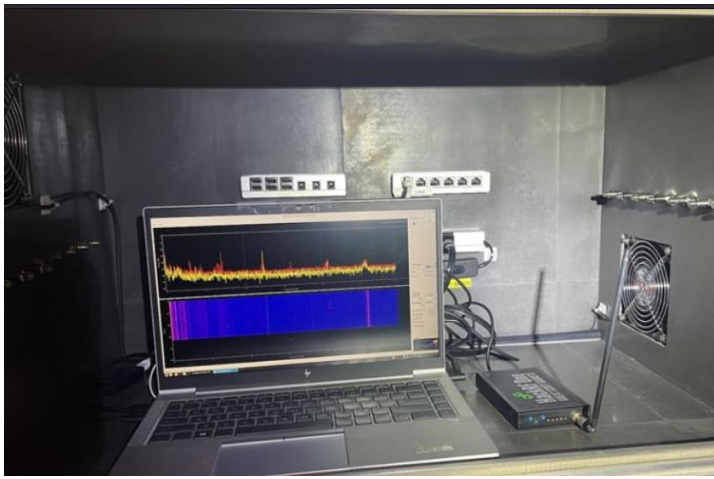


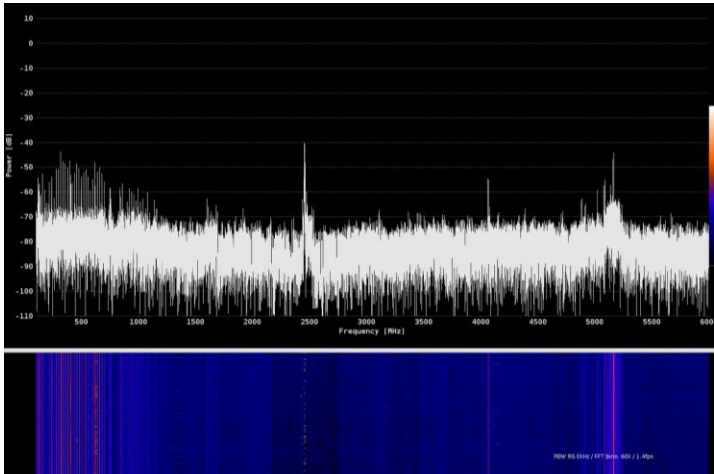


RF Survey

- Faraday Cage / Signal Isolation
- Spectrum Analyzer (1-6 GHz)
- Shielded Passthru Ports
- Look for signals that indicate RF coms
- Signals = Potential Attack Surfaces





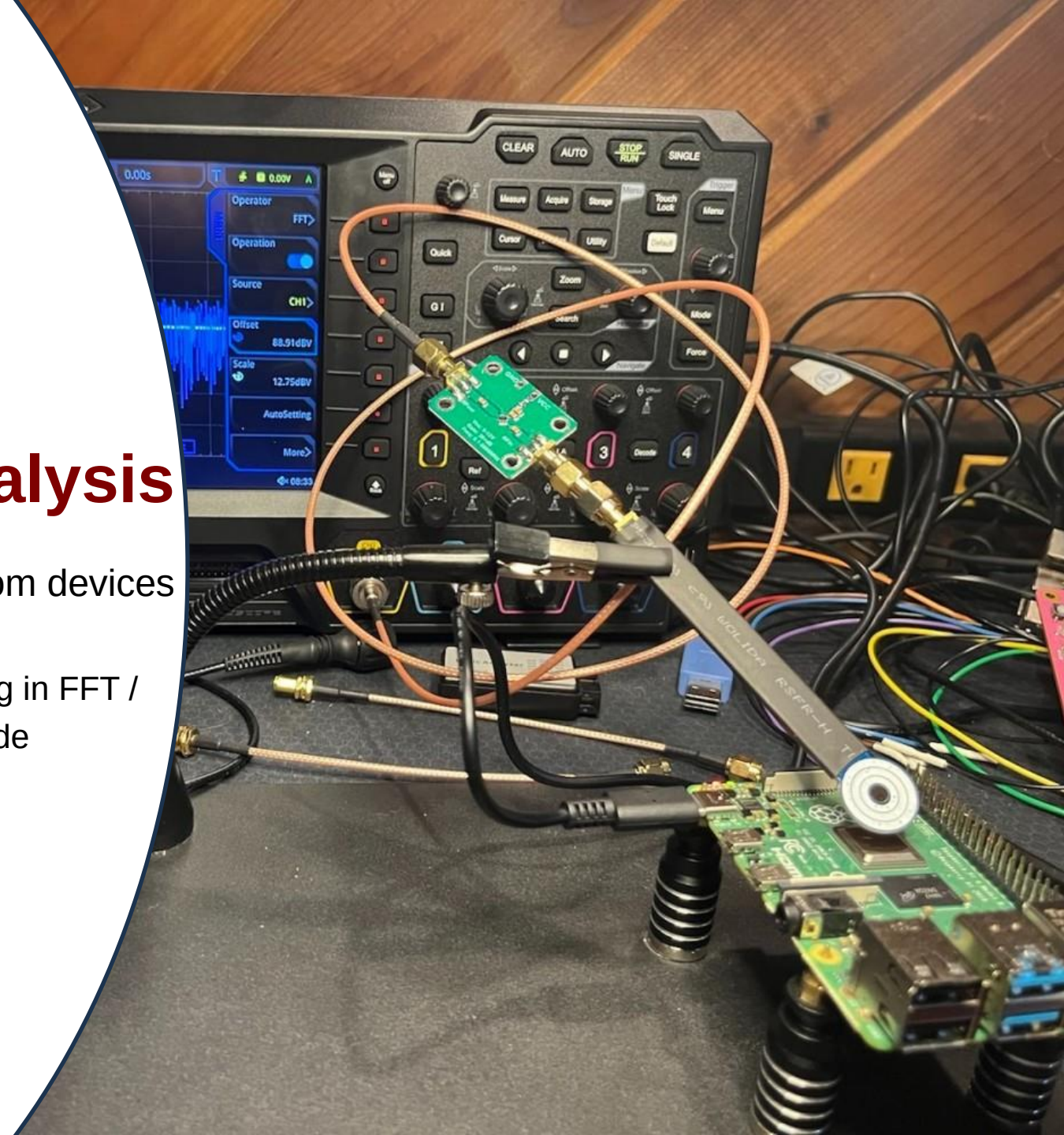


RF Survey

- HackRF
- QSpectrumAnalyzer in hackrf_sweep mode
- Signal Collection and Characterization
- Replay attacks
- Wifi testing
  - De-auth attacks
  - Traffic sniffing
  - Malicious AP attacks
- Bluetooth testing
- NFC, RFID, & other RF Tests

Near Field Analysis

- Look for emissions from devices
- Done using
  - Oscilloscope running in FFT / Spectrum Analyzer mode
  - HGLN Amplifier
  - Near field probes



Network Survey

- Internet controllable power switch
- Identify listening services

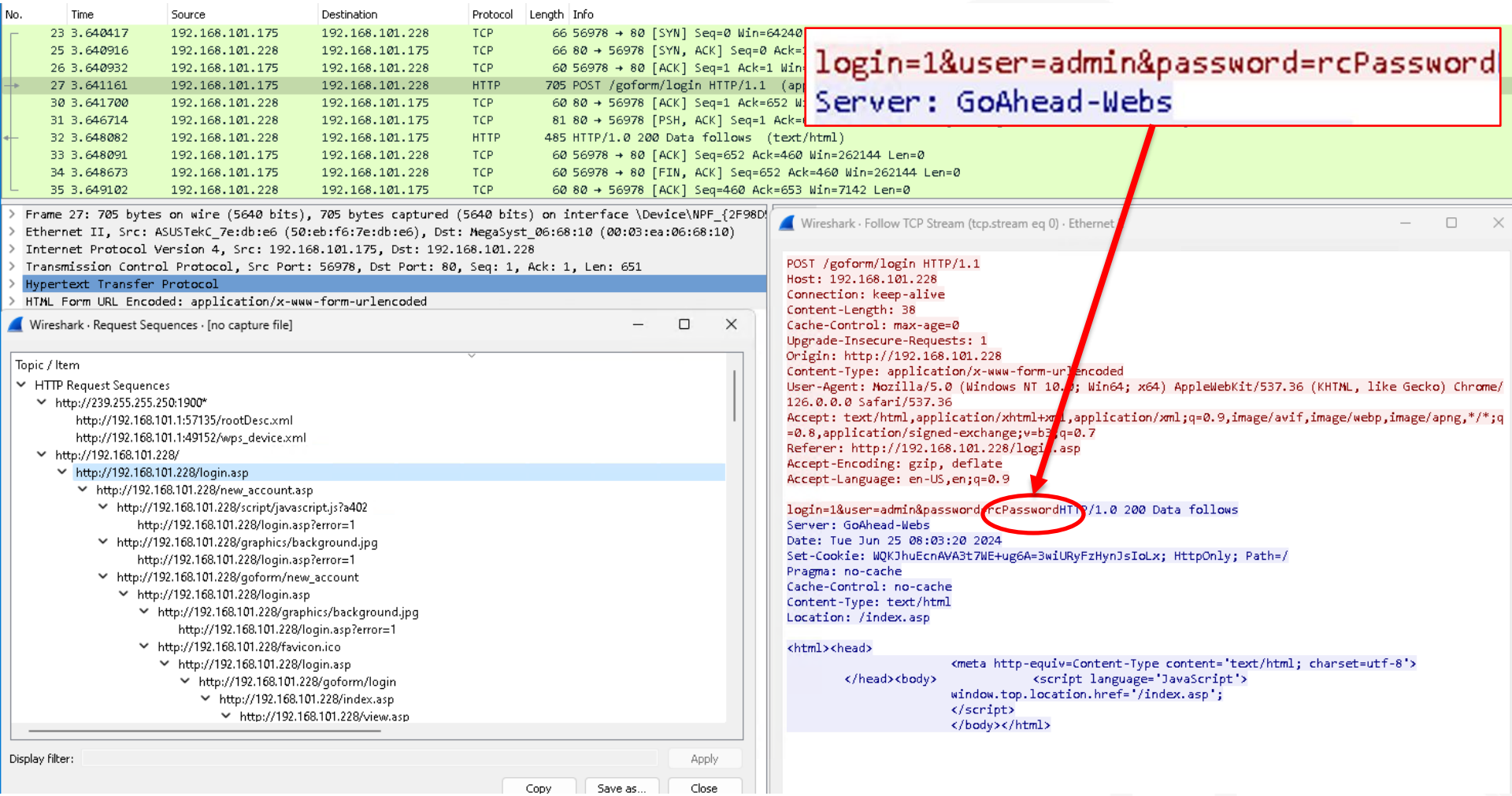
```
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
MAC Address:
00:03:EA:06:68:10 (Mega
System Technologies)
```

- Setup hardware network tap

Hak5 Plunderbug

Network Survey

- Using a tap, collect full packet capture of interaction with the device



Network Survey

- Scan for low-hanging fruit vulnerabilities

Time	Source	Issue type	Host	Path	Insertion point	Severity	Confidence	Commer
11:22:04 25 Jun 2024	Task 3	Input returned in response (stored)	http://192.168.101.228	/system.asp	WQKJhuEcnAVA3t7W...	Information	Certain	
11:13:43 25 Jun 2024	Task 3	Input returned in response (reflected)	http://192.168.101.228	/top2.htm	WQKJhuEcnAVA3t7W...	Information	Certain	
11:03:53 25 Jun 2024	Task 3	Open redirection (DOM-based)	http://192.168.101.228	/skype.asp		Low	Tentative	
11:03:52 25 Jun 2024	Task 3	Open redirection (DOM-based)	http://192.168.101.228	/config.asp		Low	Tentative	
11:03:45 25 Jun 2024	Task 3	Session token in URL	http://192.168.101.228	/view.asp		Medium	Firm	
11:03:45 25 Jun 2024	Task 3	Private IP addresses disclosed	http://192.168.101.228	/network.asp		Information	Certain	
11:03:45 25 Jun 2024	Task 3	HTML does not specify charset	http://192.168.101.228	/eventLog.asp		Information	Certain	
11:03:45 25 Jun 2024	Task 3	Private IP addresses disclosed	http://192.168.101.228	/cgi-bin/ExportSettings.sh		Information	Certain	
11:03:45 25 Jun 2024	Task 3	Cleartext submission of password	http://192.168.101.228	/mailSettings.asp		High	Certain	
11:03:45 25 Jun 2024	Task 3	File upload functionality	http://192.168.101.228	/saveUpgrade.asp		Information	Certain	
11:03:45 25 Jun 2024	Task 3	Session token in URL	http://192.168.101.228	/eventLog.asp		Medium	Firm	
11:03:45 25 Jun 2024	Task 3	Private IP addresses disclosed	http://192.168.101.228	/config.asp		Information	Certain	

Advisory | Request | Response | Path to issue

Pretty | Raw | Hex | Render

```
1  HTTP/1.0 200 OK
2  Date: Wed Jun 26 01:01:57 2024
3  Server: GoAhead-Webs
4  Pragma: no-cache
5  Cache-Control: no-cache
6  Content-type: text/html
7
8  <html>
9    <frameset frameborder="0" framespacing="0" border="0" rows="60,*">
10     <frame src="logChoose.asp" name="logchoose" scrolling="no" marginwidth="0" marginheight="0" noresize>
11       <frame src="/cgi-bin/eventlog.cgi?type=0&csrftoken=QJrwqx8Zb7QA32X8O" name="eventlog" marginwidth="0"
         marginheight="0" scrolling="no" target="right">
12       </frameset>
13     </html>
14
```

Inspector

Response headers 5

Name	Value
Date	Wed Jun 26 01:0...
Server	GoAhead-Webs
Pragma	no-cache
Cache-Control	no-cache
Content-type	text/html

HTTP Intercept

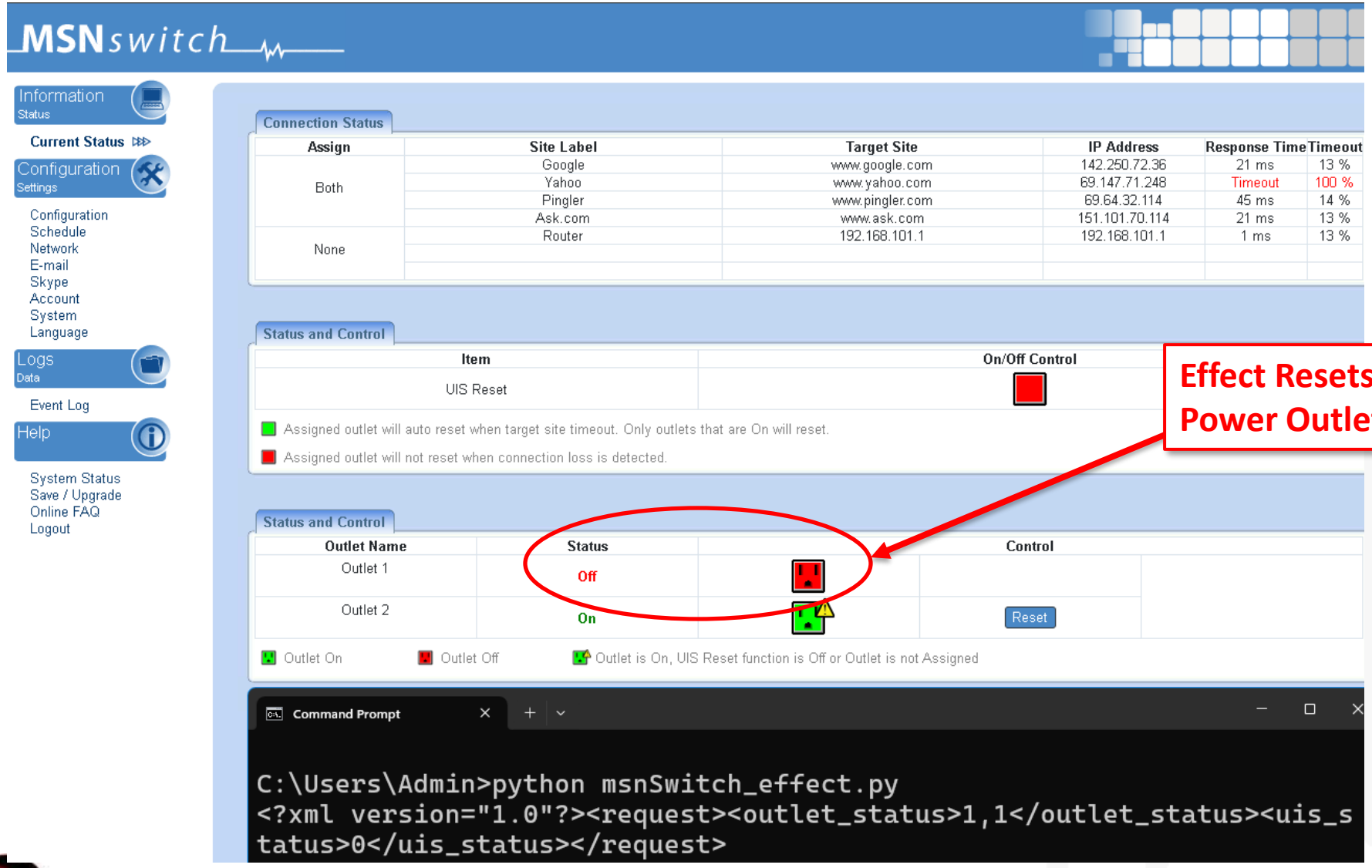
- Use Burp to identify useful actions
- Determine “effects”
- Create tool to generate effect

Network Effect Tool

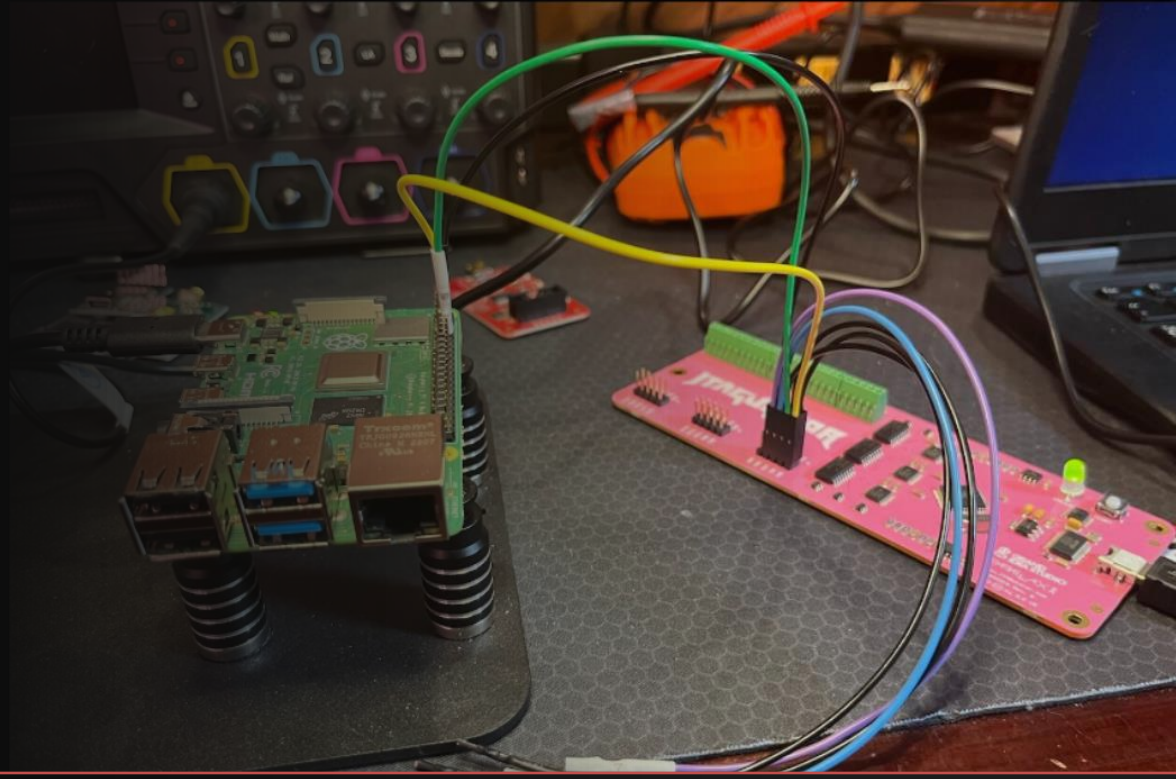
- **msnEffect.py**

```
import requests

url = "http://192.168.101.228/cgi-
bin/control.cgi?target=1&control=3&time=1719274366948&csrftoken=deNSxgwGhP9VSlOs5"

headers = {
    "Host": "192.168.101.228",
    "Upgrade-Insecure-Requests": "1",
    "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) Chrome/125.0.6422.112
Safari/537.36",
    "Accept":
"text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.7",
    "Referer": "http://192.168.101.228/status.asp",
    "Accept-Encoding": "gzip, deflate, br",
    "Accept-Language": "en-US,en;q=0.9",
    "Connection": "keep-alive"
}

cookies = {
    "WQKJhuEcnAVA3t7WE+ug6A": "OPns8R7gSpJvsWo3F"
}

response = requests.get(url, headers=headers, cookies=cookies, verify=False)

print(response.text)
```

Test Effect

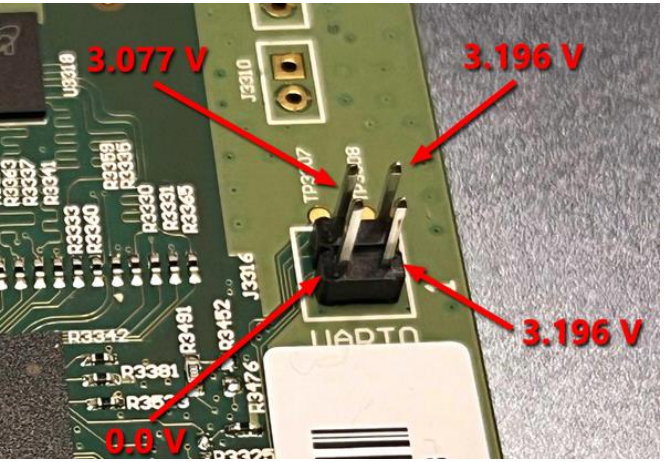

MSNswitch
Information
Status
Current Status
Configuration
Settings
Configuration
Schedule
Network
E-mail
Skype
Account
System
Language
Logs
Data
Event Log
Help
System Status
Save / Upgrade
Online FAQ
Logout
Connection Status
Assign
Site Label
Target Site
IP Address
Response Time
Timeout
Both
Google
www.google.com
142.250.72.36
21 ms
13 %
Yahoo
www.yahoo.com
69.147.71.248
Timeout
100 %
Pingler
www.pingler.com
69.64.32.114
45 ms
14 %
Ask.com
www.ask.com
151.101.70.114
21 ms
13 %
None
Router
192.168.101.1
192.168.101.1
1 ms
13 %
Status and Control
Item
On/Off Control
UIS Reset
Assigned outlet will auto reset when target site timeout. Only outlets that are On will reset.
Assigned outlet will not reset when connection loss is detected.
Effect Resets Power Outlet
Status and Control
Outlet Name
Status
Control
Outlet 1
Off
Outlet 2
On
Reset
Outlet On
Outlet Off
Outlet is On, UIS Reset function is Off or Outlet is not Assigned
Command Prompt
C:\Users\Admin>python msnSwitch_effect.py
<?xml version="1.0"?><request><outlet_status>1,1</outlet_status><uis_status>0</uis_status></request>

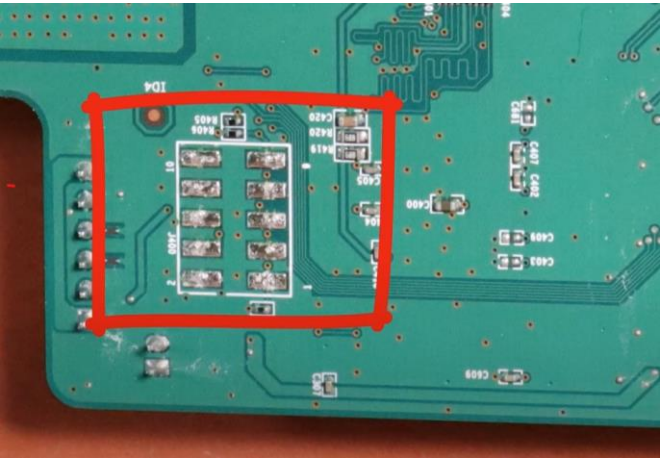
Hardware Analysis



```
RT> p
te: UART pin naming is from the target's perspectiv
ter X to disable either pin, if desired.
ter TXD pin [0]: 1
ter RXD pin [0]: 2
ter baud rate [0]: 115200
able local echo? [y/N]: y
tering UART passthrough! Press Ctrl-X to exit...
[    0.000000] Booting Linux on physical CPU 0x0
   0.000000] Linux version 5.15.61-v7l+ (dom@buildb
untu) 2.34) #1579 SMP Fri Aug 26 11:13:03 BST 2022
   0.000000] CPU: ARMv7 Processor [410fd083] revisi
   0.000000] CPU: div instructions available: patch
   0.000000] CPU: PIPT / VIPT nonaliasing data cach
   0.000000] OF: fdt: Machine model: Raspberry Pi 4
```

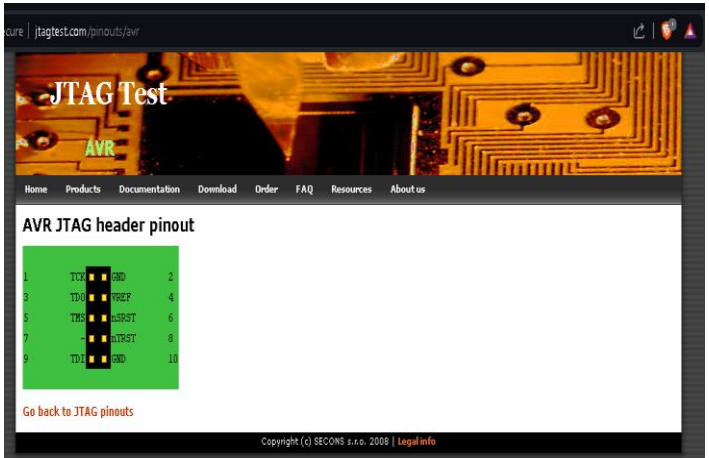
Hardware Analysis





- **JTAG, UART, SPI**

1. Take resistance measurements against ground with board powered off. Set Multimeter to ohms Ω.
2. Touch black probe to a ground point.
3. Touch red probe led to each pin and record measurements on a table.
4. Next take resistance measurements against VCC.
5. Find data sheet, locate VCC pin
6. Red probe on the VCC pin & touch the black probe to each candidate JTAG pins & record results in table
7. Power on board, switch multimeter to volts, measure voltage on each pin. Black probe on ground & red probe on each pin
8. Search http://jtagtest.com/pinouts for a pinout that matches findings.
    1. Know the device's architecture (arm, mips, etc.)



PINout Lookup

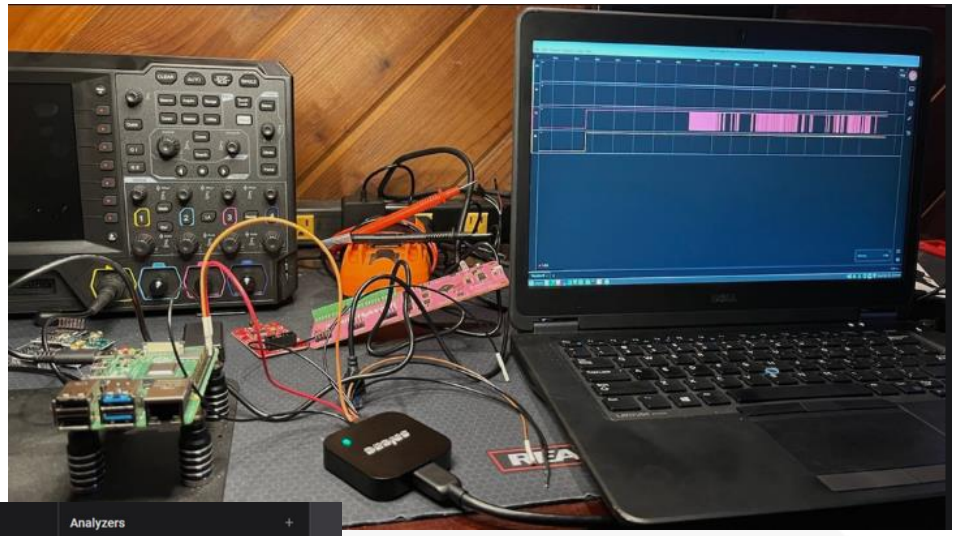
Example Pinout Analysis Table

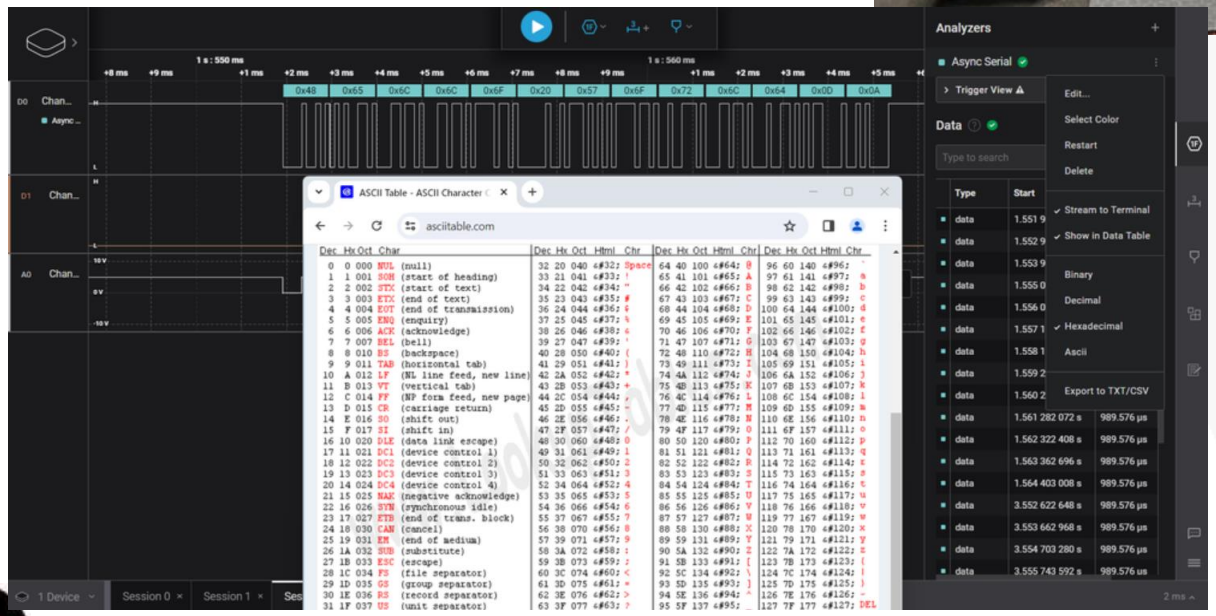
PIN	RGRND	RVCC	V	NOTES	PIN	RGND	RVCC	V	NOTES
1	1K Ω	1K Ω	0 V		2	0 Ω	90 Ω	0 V	Probably Ground (GND) because its all 0s
3	∞	∞	2.1 V	High Impedance PIN? Could be TDO	4	90 Ω	0 Ω	3.3 V	VCC because it has 0 resistance against VCC but 3.3 V
5	4.7K Ω	4.7K Ω	3.3 V		6	∞	∞	0 V	Not Connected?
7	5.7K Ω	5.7K Ω	3.3 V		8	∞	∞	0 V	Not Connected?
9	4.7K Ω	4.7K Ω	3.3 V		10	0 Ω	90 Ω	0 V	Probably Ground (GND)

Logic Analysis

Hex: "0x48, 0x65, 0x6C 0x6F, 0x20, 0x57, 0x6F, 0x72, 0x6C, 0x64, 0x0D 0x0D“

ASCII: "H" "e" "l" "l" "o" "space" "W" "o" "r" "l" "d"





Software Analysis

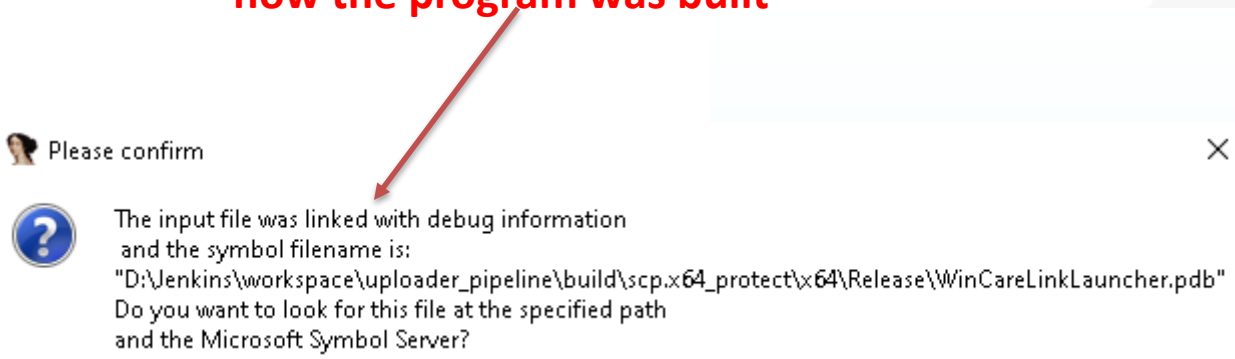
- Windows Device Software
  - PE (.exe) & DLL files
- Linux Device Software
  - ELF binaries and .so files
- Firmware Reverse Engineering
  - Firmware format identification
  - OS & file extraction

Static Software Analysis Example

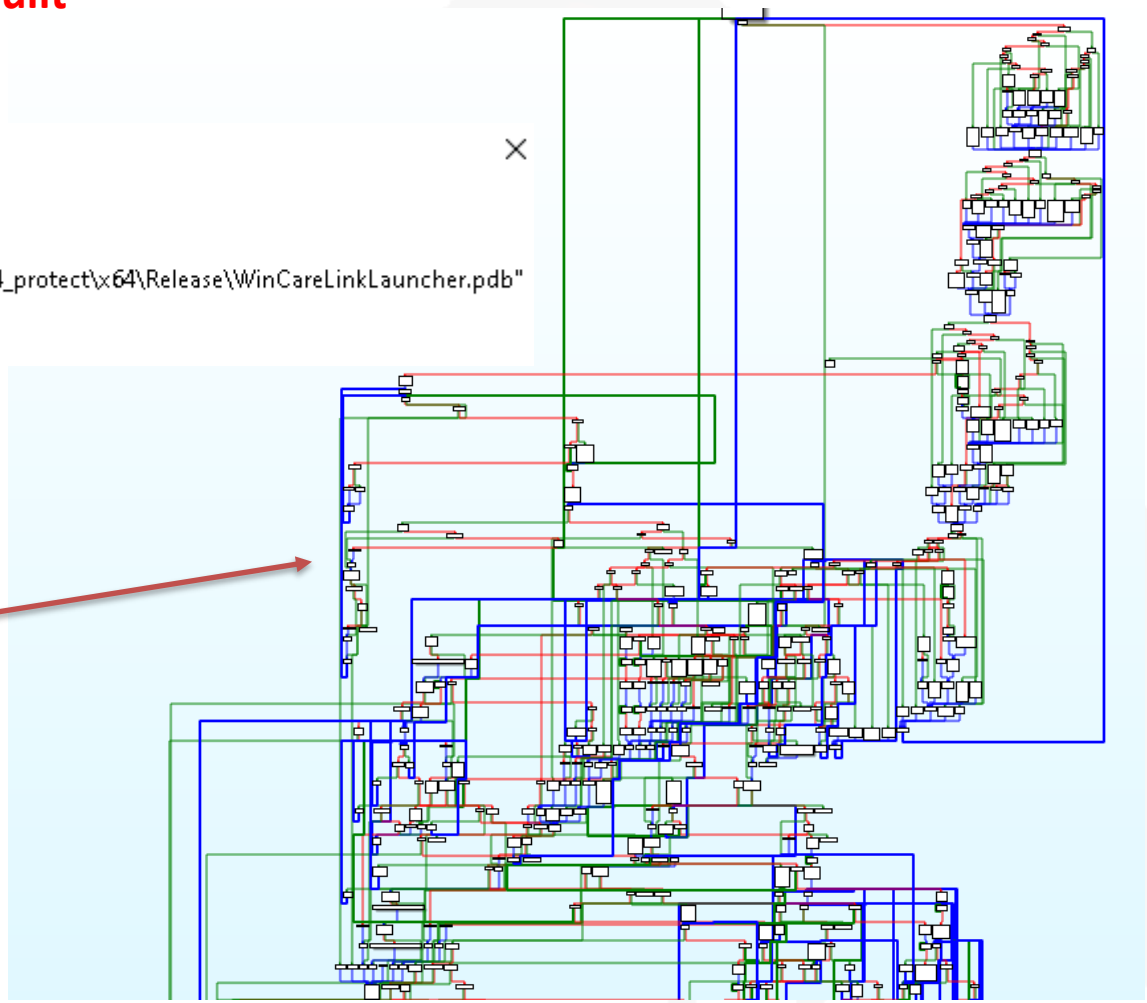
FILE NAME:	CareLinkUploader-ACC-7350-3.11.0-windows-installer.exe
FILE SIZE:	174372 / 171M
FILE TYPE:	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
MD5SUM:	cf0a57d5441239da426922e481a2a85e
SHA256SUM:	62b9e6928b3884bc67868423dc9a63d76bb05118ae7c5ada1ee453355981f383
COMPILE TIME:	2023-01-04 15:12:35
COMPILE SECURITY:	DEP: True ASLR: True NX: True SEH: True CFG: False
DEPENDENCIES:	'GDI32.dll', 'SHELL32.DLL', 'OLEAUT32.DLL', 'WS2_32.dll', 'OLE32.dll', 'USER32.dll', 'COMCTL32.DLL', 'msvcrt.dll', 'COMDLG32.DLL', 'IMM32.DLL', 'ADVAPI32.DLL', 'KERNEL32.dll'
SECTIONS:	11, '.text', '.data', '.rdata', '.eh_fram', '.bss', '.edata', '.idata', '.CRT', '.tls', '.rsrc', '.reloc'
ENTROPY:	7.9983 (High Entropy, likely contains compressed/encrypted data
IMPORTS:	GetSecurityDescriptorOwner, GetSidIdentifierAuthority, GetUserNameA, GetUserNameW, RegCloseKey, RegOpenKeyExA, RegQueryValueExA, CopyFileA, CreateDirectoryA, CreateEventA, CreateFileA,CreateFileW, CreatePipe, CreateProcessA, CreateProcessW, CreateThread, DeleteFileA, DeleteFileW, ExitProcess, FindClose, FindFirstFileA, FindFirstFileW, FindNextFileA, FindNextFileW, WriteConsoleW, WriteFile, lstrcpyA, lstrcpyW, lstrcpynA, lstrlenA, lstrlenW,_getpid, _stricmp, _strnicmp, _timezone, _tzset, _write, fputc, fputs, fread, free, frexp, fseek, ftell, fwrite, getenv, gmtime, isalnum, ldexp, localtime, log, log10, malloc, memcmp, memcpy, memmove, memset, mktime, modf, pow, printf, puts, qsort, realloc, setlocale, signal, sin, sinh, sprintf, sqrt, sscanf, strcat, strchr, strcmp, strcpy, strcspn, strerror, strlen, strncmp, strncpy, strpbrk, strrchr, strspn, strstr, strtod, strtol, strtoul, swprintf, tan, tanh, time, tolower, toupper, vfprintf, vsprintf, wcschr, wcscmp, wcscpy, wcslen, wcsncmp, GetAsyncKeyState, GetCapture, GetClipboardData, GetClipboardOwner, GetFocus, GetForegroundWindow, GetKeyState, GetKeyboardLayout, GetWindow, MessageBoxA, OpenClipboard, PeekMessageA, PostMessageA, PostQuitMessage, SendMessageW, accept, bind, closesocket, connect, gethostbyaddr, gethostbyname, gethostname, getpeername, getservbyname, getsockname, getsockopt, htons, inet_addr, inet_ntoa, ioctlsocket, listen, ntohs, recv, select, send, setsockopt, socket

Static Software Analysis Example

Interesting Error from IDA Indicating how the program was built

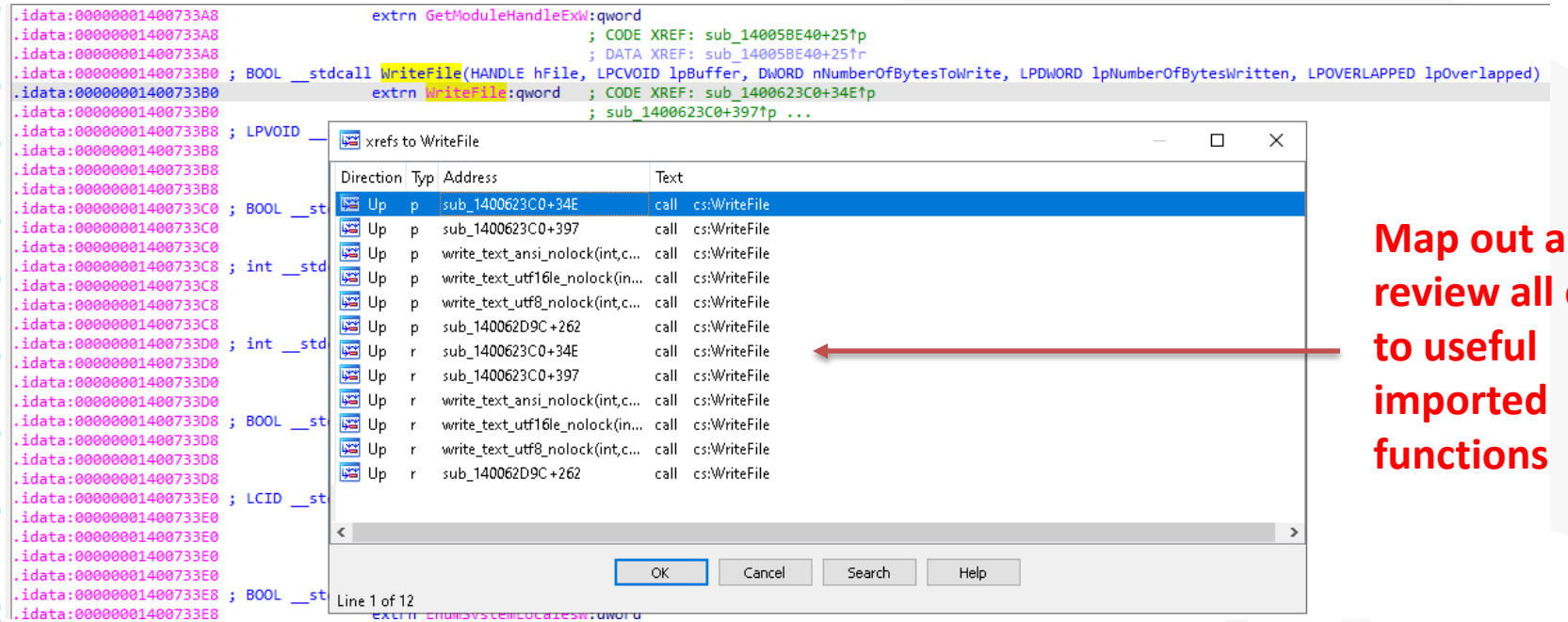


View Flow Graph to begin to understand the program



Static Software Analysis Example

- Look at potentially useful imports
  - **CreateFile, WriteFile, RegSetValue, fopen**
  - **Malloc, free, strcpy, gets, CreateProcess**
  - **Socket, connect, bind, CryptGenKey**



Map out and review all calls to useful imported functions

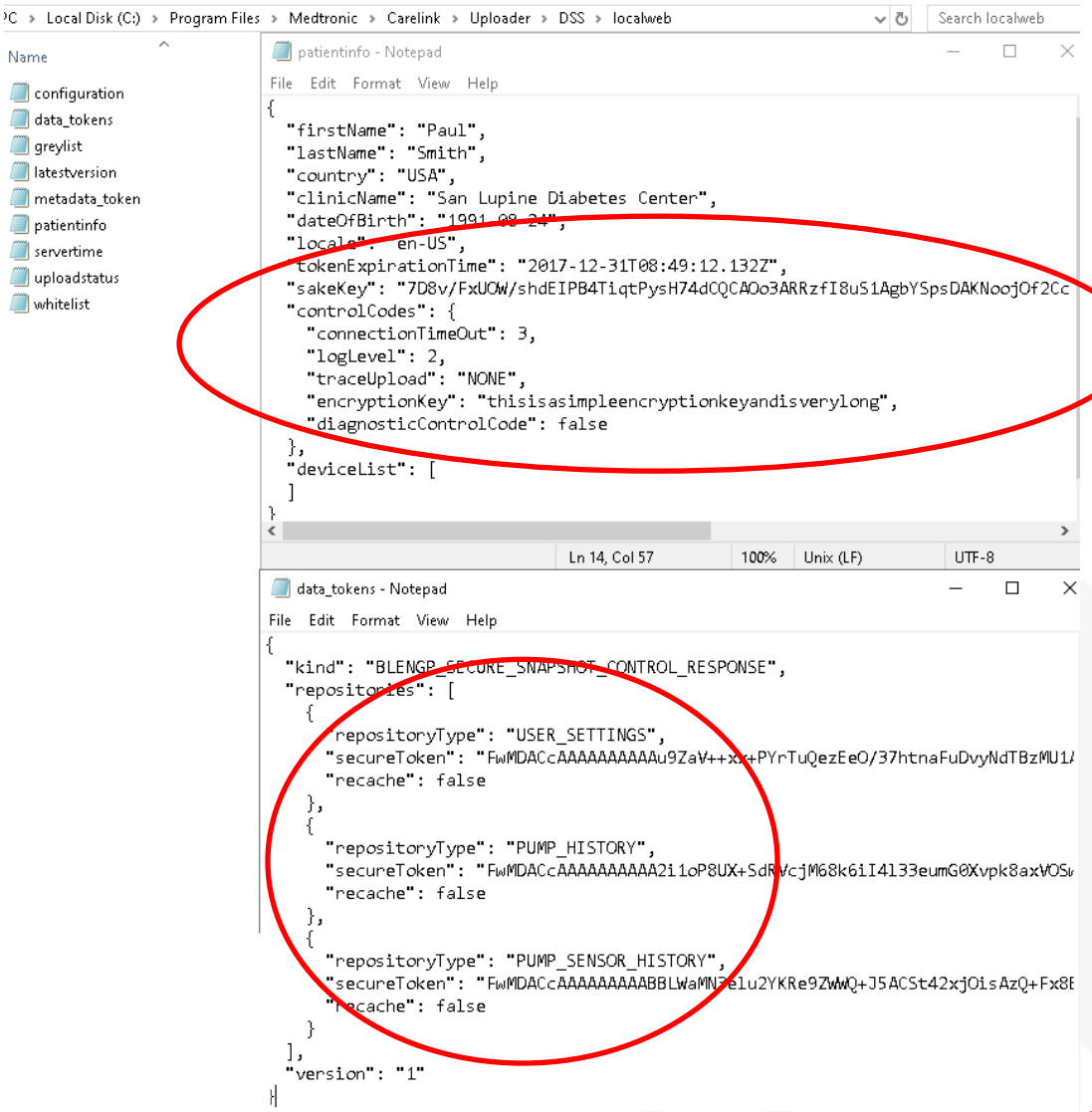
Static Software Analysis Example

- Map out installed files security: **EXEs, DLLs, Drivers, Services, Reg Keys**

FILE NAME	C:\Program Files\Medtronic\Carelink\Uploader\DSS\WinCareLinkLauncher.exe
IS PE	yes
FILE SIZE	0.767120361328125MB
MDSUM	2BCF5A8589360C5A9794774AD558A7C1
FILE PERMISSIONS	NT AUTHORITY\SYSTEM FullControl; BUILTIN\Administrators FullControl; BUILTIN\Users ReadAndExecute, Synchronize; APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES ReadAndExecute, Synchronize; APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES ReadAndExecute, Synchronize;
USED AS SERVICE	no
ARCHITECTURE	32BIT
SECURITY FEATURES	ASLR, DEP, SafeSEH, StrongNaming

Static Software Analysis Example

- **Identify files with:**
  - **Keys**
  - **Passwords**
  - **Secrets**
  - **Operation hints**
  - **Ips / Servers**



Static Software Analysis Example

- Disassemble JAVA files and look for device controls & secrets

SECRET HANDLING

```
package com.medtronic.diabetes.utils;

import com.whitecryption.skb.Cipher;
import com.whitecryption.skb.SkbException;
import java.util.UUID;
import libuploader.Loader;

public abstract class SecurityUtils {
  public static native byte[] encryptWithPadding(Cipher paramCipher, byte[] paramArrayOfbyte1, byt

  public static native byte[] getCipherIv(UUID paramUUID);

  public static native byte[] decryptWithNoPadding(Cipher paramCipher, byte[] paramArrayOfbyte1, b

  public static native byte[] getRandomIv();

  public static native byte[] encrypt(Cipher paramCipher, byte[] paramArrayOfbyte1, byte[] paramAr

  public static native byte[] encryptWithPadding(Cipher paramCipher, byte[] paramArrayOfbyte1, byt

  public static native String illlllllllllll(Object paramObject);

  public static native byte[] xorArrays(byte[] paramArrayOfbyte1, byte[] paramArrayOfbyte2);

  public static native byte[] decryptWithPadding(Cipher paramCipher, byte[] paramArrayOfbyte1, byt

  public static native byte[] encryptWithBlockSizeExtension(Cipher paramCipher, byte[] paramArrayO

  public static native byte[] encrypt(Cipher paramCipher, byte[] paramArrayOfbyte1, byte[] paramAr

  public static native UUID retrieveSystemId();
```

HARDWARE CONTROL

```
package com.ftdi;

import com.medtronic.diabetes.fusion.device.common.Util;
import com.sun.jna.Library;
import com.sun.jna.Memory;
import com.sun.jna.Platform;
import com.sun.jna.Pointer;
import com.sun.jna.Structure;
import com.sun.jna.Structure.FieldOrder;
import com.sun.jna.ptr.ByteByReference;
import com.sun.jna.ptr.IntByReference;
import com.sun.jna.ptr.PointerByReference;
import com.sun.jna.ptr.ShortByReference;
import java.nio.file.Path;
import java.nio.file.Paths;
import java.util.Objects;

public interface FTD2XX extends Library {
  public static final int DEVICE_INFO_LEN = 104;

  static String getLibraryPath() {
    String FTDI_DRIVER = "FTDI-Driver";
    String DRIVERS = "Drivers";
    Path path = null;
    if (Platform.isWindows()) {
      if (Platform.is64Bit()) {
        path = Paths.get("Drivers", new String[] { "usb", "FTDI-Driver", "amd64", "ftd2xx64" });
      } else {
        path = Paths.get("Drivers", new String[] { "usb", "FTDI-Driver", "i386", "ftd2xx" });
      }
    } else if (Platform.isMac()) {
      path = Paths.get("Uploader.bundle", new String[] { "Contents", "Home", "Drivers", "usb", "FTDI-Driver",
    } else if (Platform.isLinux()) {
      path = Paths.get("/home/andriy/Projects/GL/uploader/deployment/layouts/lin.x64/Drivers/usb/FTDI-Driver/
    }
    Objects.requireNonNull(path, "Error during initialization of path in FTD2XX");
    return path.toAbsolutePath().toString();
  }
```

Dynamic Software Analysis Example

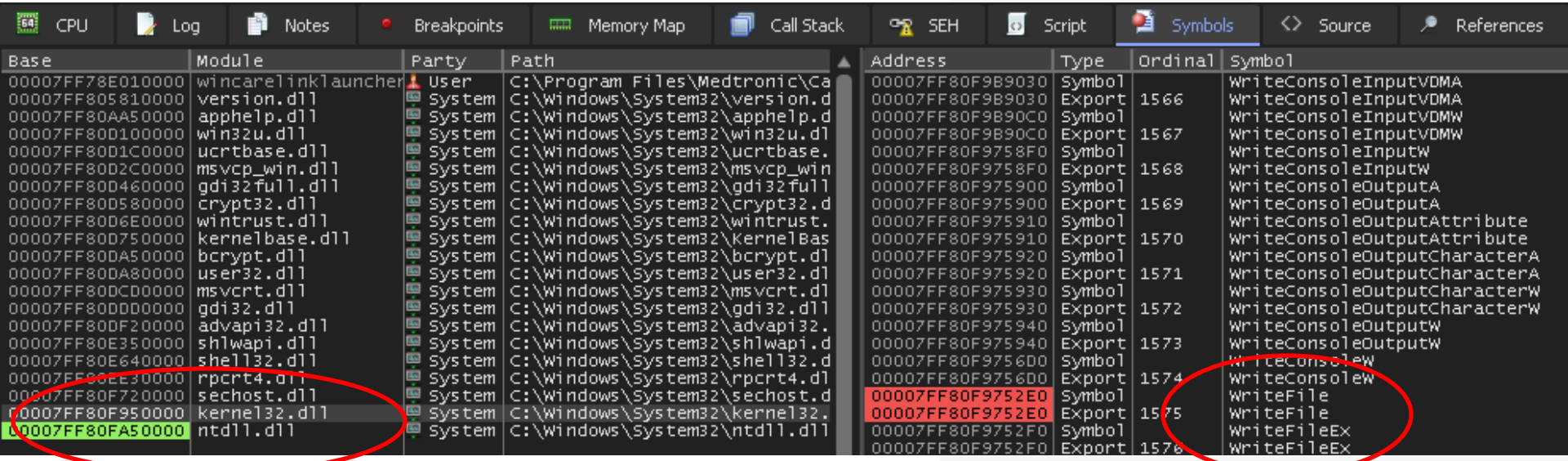
- **Monitor everything the application does**
  - **Registry modifications**
  - **File system modifications**
  - **Process table changes**
  - **Network connections**

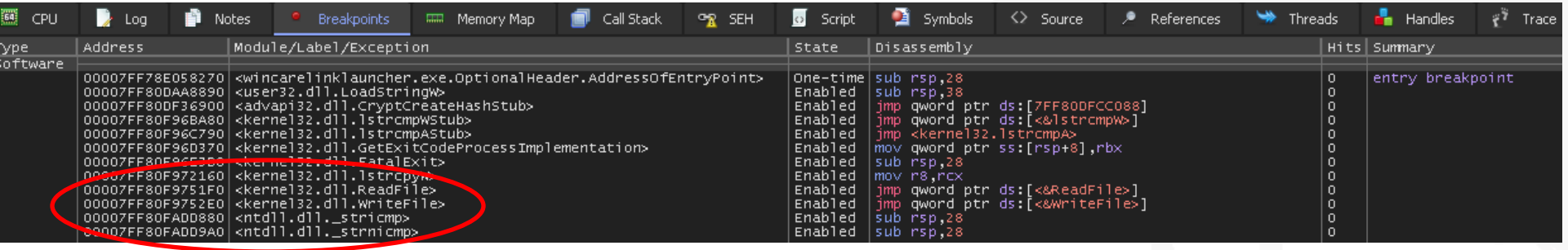
Sysinternals for windows system monitoring

3:38:47.9212878 PM	WinCareLinkLauncher.exe	5068	Load Image	C:\Windows\System32\crypt32.dll
3:38:47.9231303 PM	WinCareLinkLauncher.exe	5068	CreateFileMapping	C:\Windows\System32\version.dll
3:38:47.9231539 PM	WinCareLinkLauncher.exe	5068	CreateFileMapping	C:\Windows\System32\version.dll
3:38:47.9232705 PM	WinCareLinkLauncher.exe	5068	Load Image	C:\Windows\System32\version.dll
3:38:47.9249084 PM	WinCareLinkLauncher.exe	5068	CreateFileMapping	C:\Windows\System32\imm32.dll
3:38:47.9249216 PM	WinCareLinkLauncher.exe	5068	QueryStandardInformation...	C:\Windows\System32\imm32.dll
3:38:47.9249414 PM	WinCareLinkLauncher.exe	5068	CreateFileMapping	C:\Windows\System32\imm32.dll
3:38:47.9260144 PM	WinCareLinkLauncher.exe	5068	Load Image	C:\Windows\System32\imm32.dll
3:38:47.9309343 PM	WinCareLinkLauncher.exe	5068	CreateFileMapping	C:\Windows\System32\msasn1.dll
3:38:47.9309631 PM	WinCareLinkLauncher.exe	5068	CreateFileMapping	C:\Windows\System32\msasn1.dll
3:38:47.9311194 PM	WinCareLinkLauncher.exe	5068	Load Image	C:\Windows\System32\msasn1.dll
3:38:47.9320743 PM	WinCareLinkLauncher.exe	5068	QueryNameInformationFile	C:\Program Files\Medtronic\Carelink\Uploader\DSS\WinCareLinkLauncher.exe
3:38:47.9323933 PM	WinCareLinkLauncher.exe	5068	Load Image	C:\Windows\System32\SHCore.dll
3:38:47.9325684 PM	WinCareLinkLauncher.exe	5068	Load Image	C:\Windows\System32\combase.dll
3:38:47.9370315 PM	WinCareLinkLauncher.exe	5068	CreateFileMapping	C:\Windows\System32\TextShaping.dll
3:38:47.9370578 PM	WinCareLinkLauncher.exe	5068	CreateFileMapping	C:\Windows\System32\TextShaping.dll
3:38:47.9371417 PM	WinCareLinkLauncher.exe	5068	Load Image	C:\Windows\System32\TextShaping.dll
3:38:47.9459782 PM	WinCareLinkLauncher.exe	5068	QueryStandardInformation...	C:\Windows\Fonts\StaticCache.dat
3:38:47.9460460 PM	WinCareLinkLauncher.exe	5068	CreateFileMapping	C:\Windows\Fonts\StaticCache.dat
3:38:47.9460607 PM	WinCareLinkLauncher.exe	5068	QueryStandardInformation...	C:\Windows\Fonts\StaticCache.dat
3:38:47.9460845 PM	WinCareLinkLauncher.exe	5068	CreateFileMapping	C:\Windows\Fonts\StaticCache.dat

Dynamic Software Analysis Example

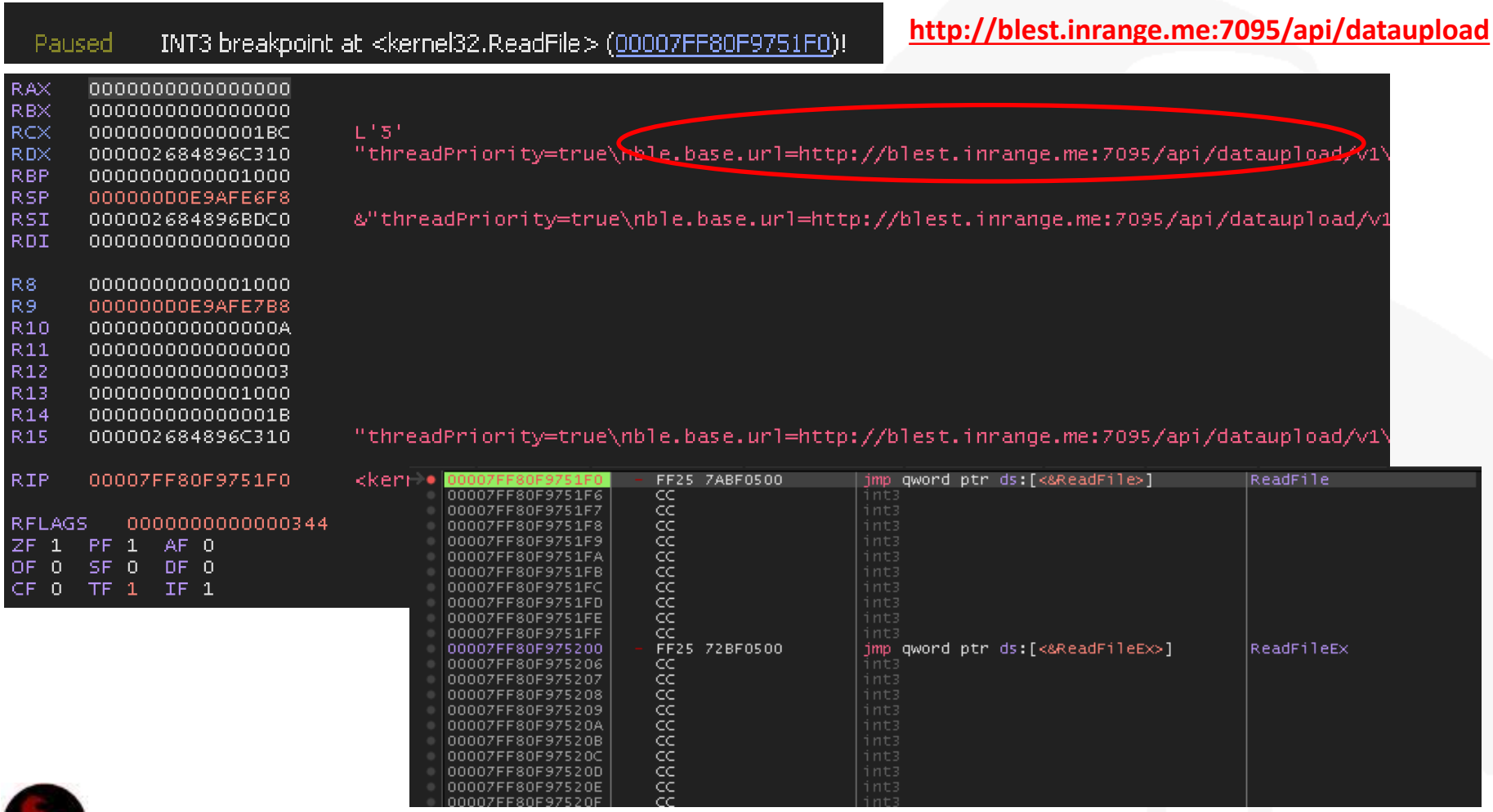
- Run software in debugger
- Identify useful imports, set breakpoints





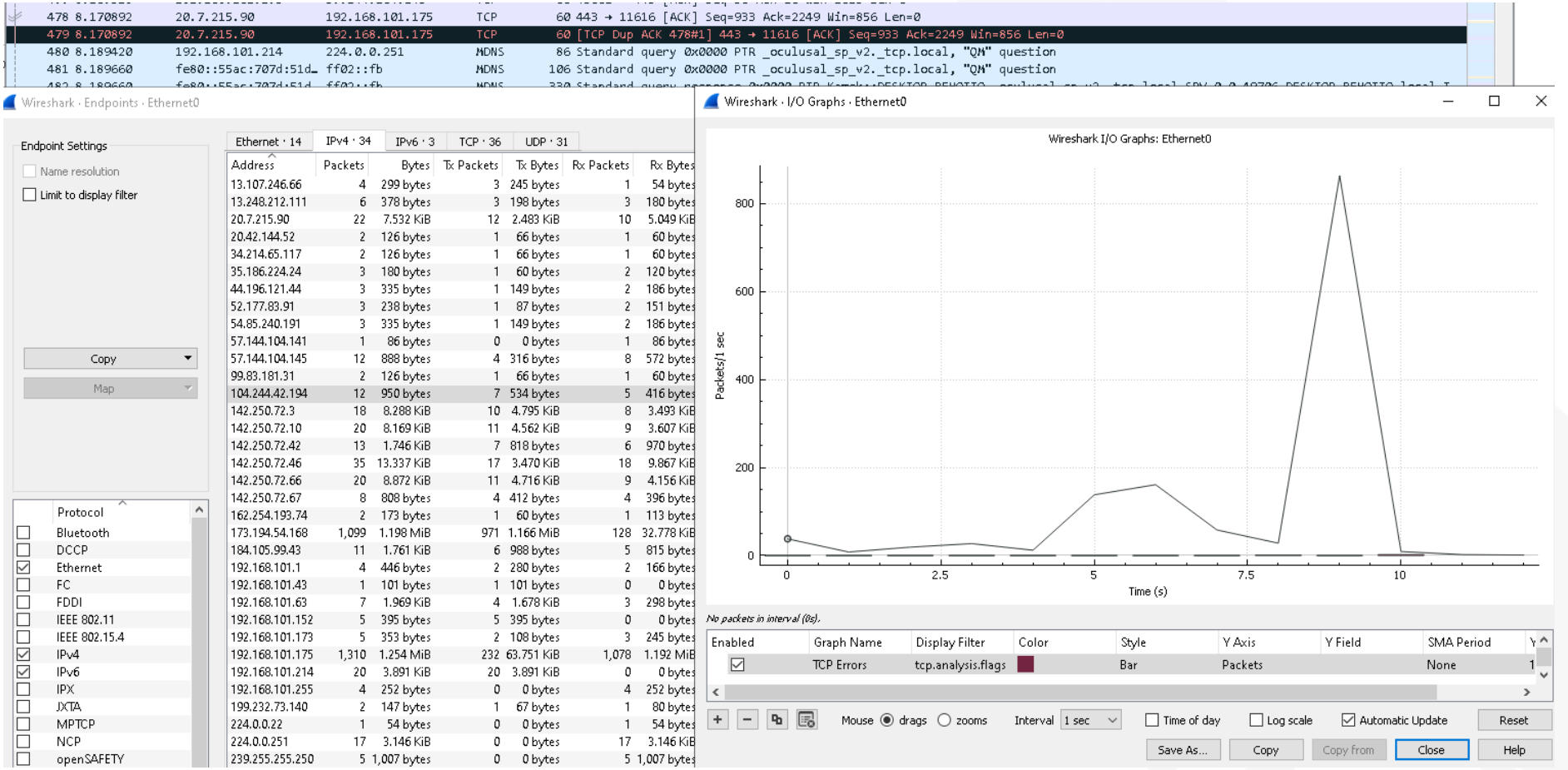
Dynamic Software Analysis Example

- Look for clues when breakpoints are hit



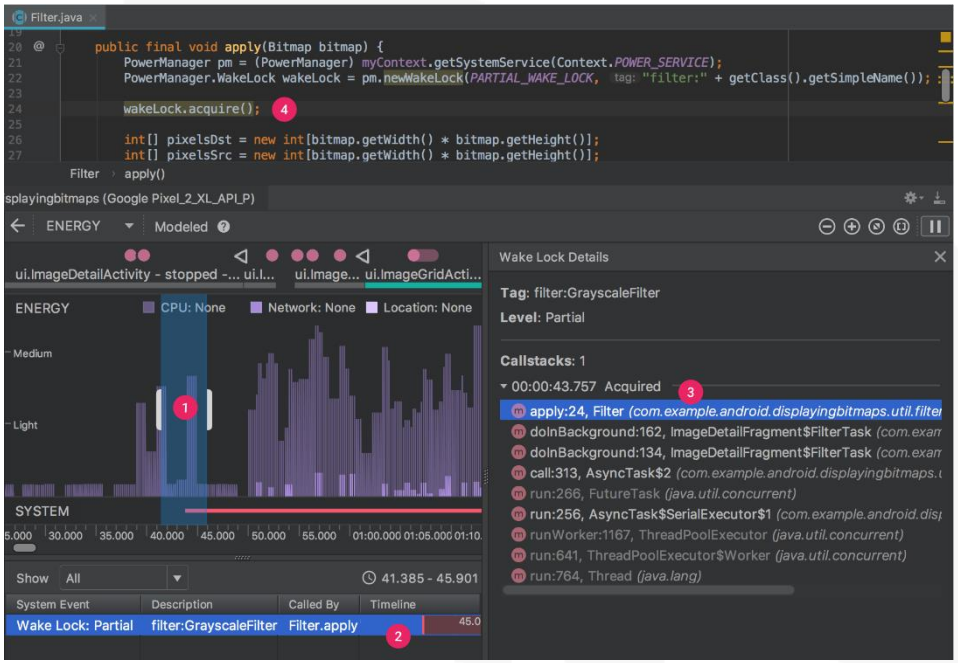
Dynamic Software Analysis Example

- Identify app communications & analyze



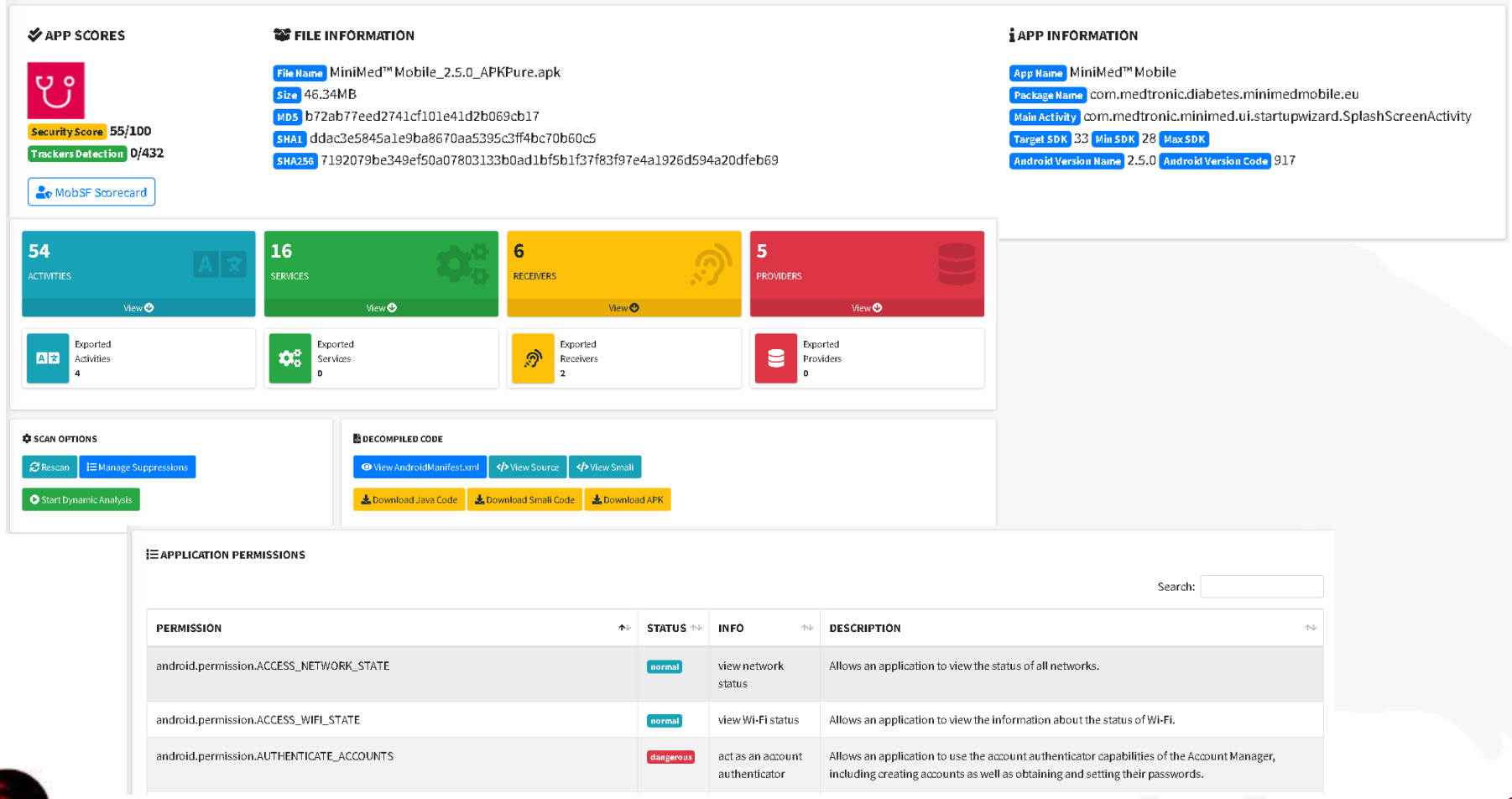
Mobile App Analysis

- Static Analysis
  - MobSF
  - IDA Pro, Ghidra, Radare2, JD-GUI
- Dynamic Analysis
  - Android Studio
    - Logcat, adb, Profiler
  - Fiddler
  - APK-MITM



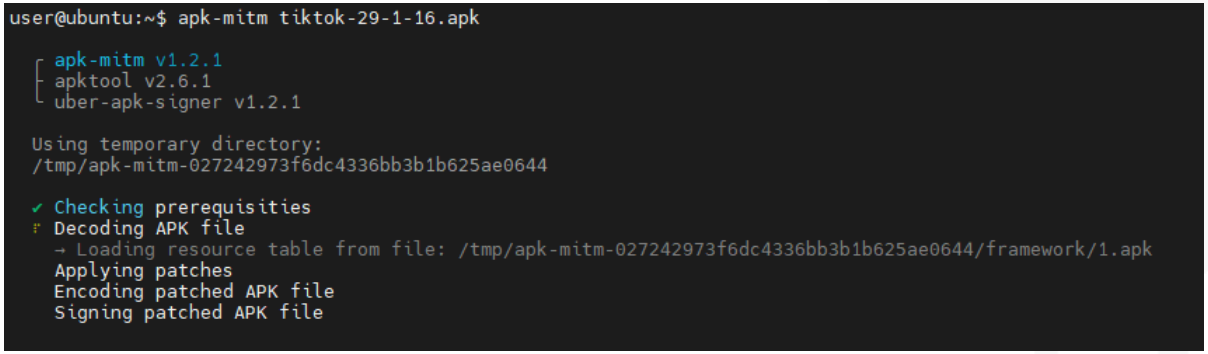
Mobile App Static Analysis

1. Acquire APK
2. Scan APK with MobSF



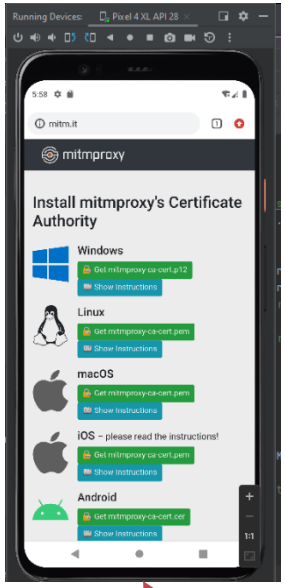
Mobile App Dynamic Analysis

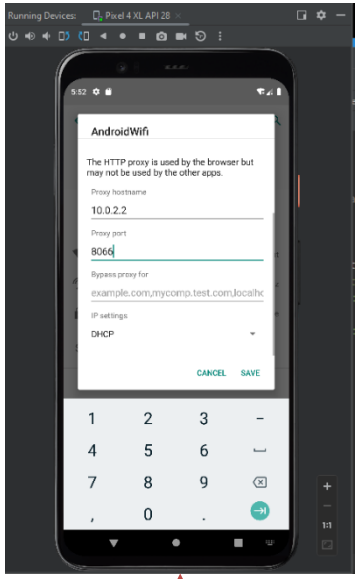
1. Create Android Emulator (not all APKs will work)
2. Install MITMProxy Certificate
3. Configure Android Web Proxy Settings
4. Use MITMProxy to analyze/modify web traffic
    1. Can use Burp and Burp Cert
5. If App Uses Cert Pinning use apk-mitm to strip cert from APK
    1. Large APKs can be stripped on a temporary high resource AWS node

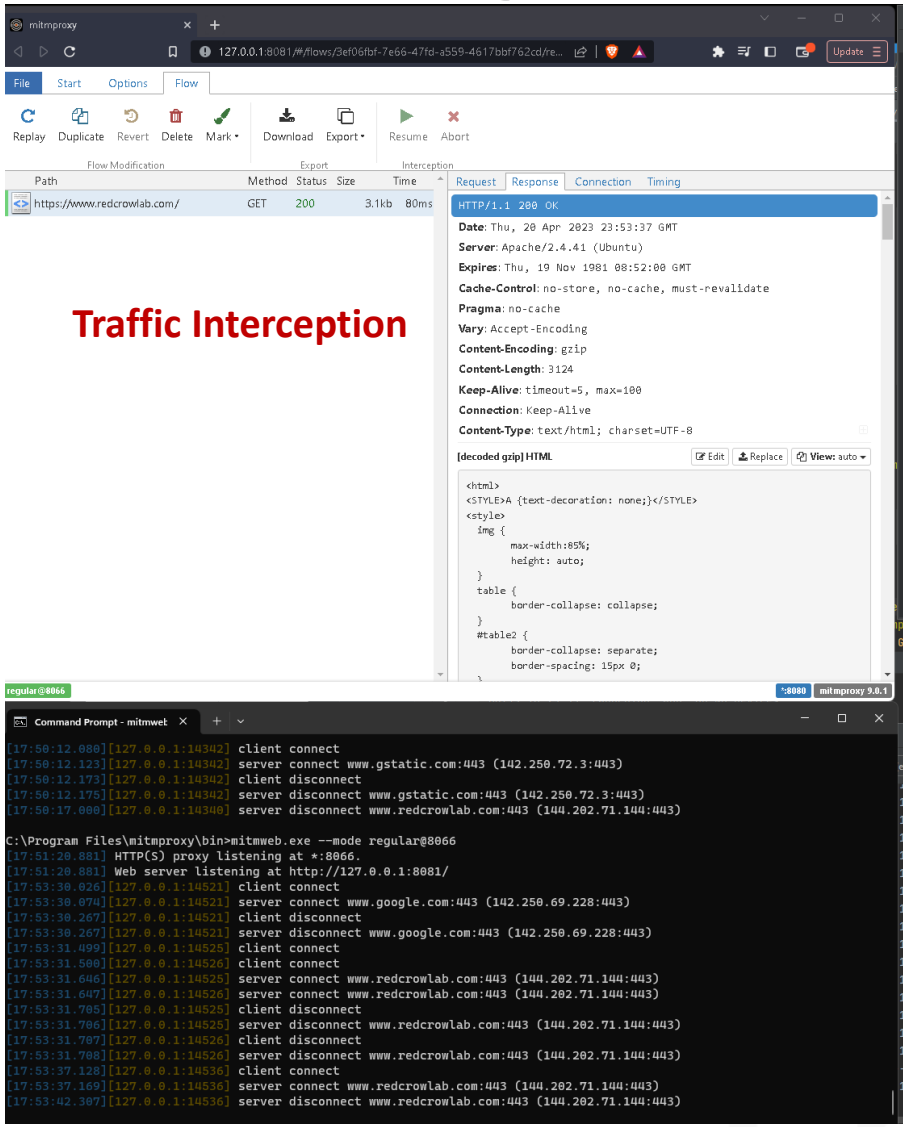


Mobile Analysis

Analyzed Website







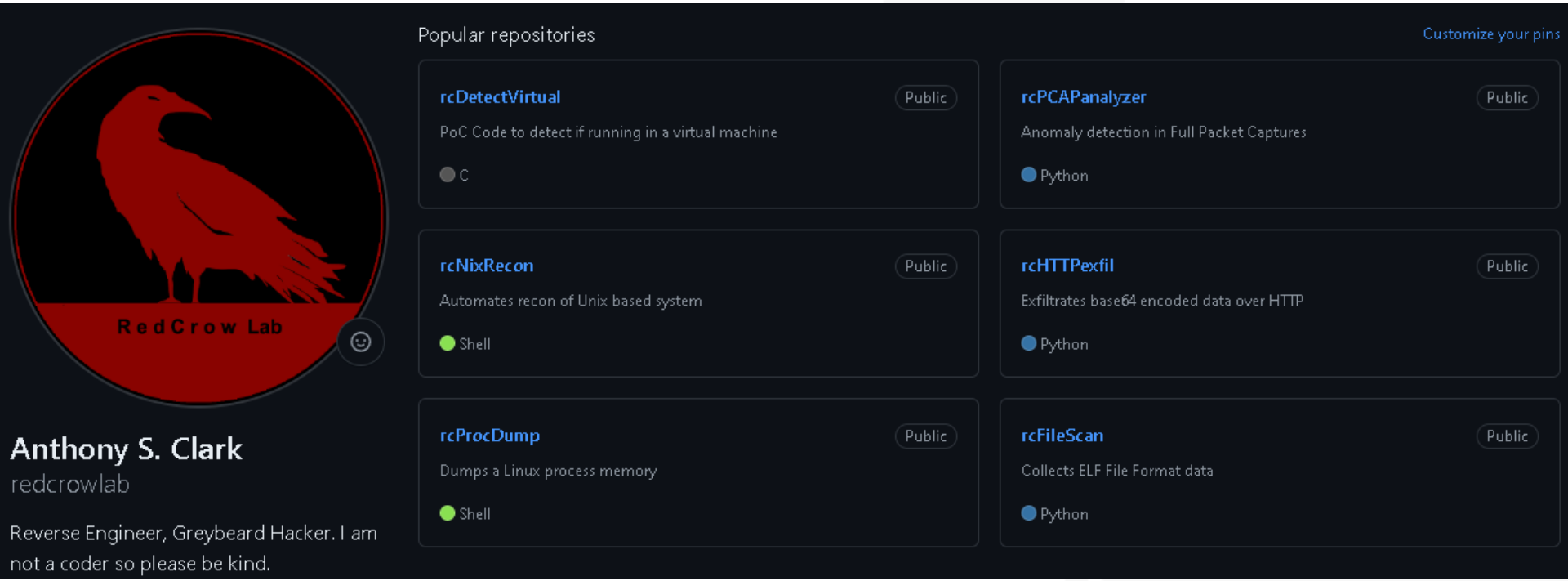
Traffic Interception

MITM Certificate Install

Android Emulator Web Proxy Setup

Tool Development

- Build tools to automate tasks, replicate attacks, and collect instrumentation data



Tool Development

rcWinFileScan.ps1

```powershell
#################################################################
# rcWinFileScan - PowerShell Script for analyzing a programs directory security.

# Import required module for PE analysis
#Install-Module -Name PESecurity -Force -SkipPublisherCheck

param ([string]$dirPath)

#################################################################
# Function to get file hashes
function Get-FileHashes {
    param ([string]$filePath)
    $md5 = Get-FileHash -Path $filePath -Algorithm MD5
    $sha256 = Get-FileHash -Path $filePath -Algorithm SHA256
    return $md5.Hash, $sha256.Hash
}

#################################################################
# Function to get PE file info
function Get-PEInfo {
    param ([string]$filePath)

    $peInfo = Get-PESecurity -file $filePath
    $arch = if ($peInfo.Is64Bit) { "64BIT" } else { "32BIT" }
    $secFeatures = @()

    if ($peInfo.ASLR) { $secFeatures += "ASLR" }
    if ($peInfo.DEP) { $secFeatures += "DEP" }
    if ($peInfo.SEH) { $secFeatures += "SEH" }
    if ($peInfo.SafeSEH) { $secFeatures += "SafeSEH" }
    if ($peInfo.StrongNaming) { $secFeatures += "StrongNaming" }
```

```
[* FILE NAME *] C:\Program Files\Medtronic\Carelink\Uploader\DSS\vc_redist.exe
[* FILE SIZE *] 24.0657730102539MB
[* MDSUM * ] CDCE5D5EE259D8071FA82F522C5C7D6E
[* SHA256 *] CE6593A1520591E7DEA2B93FD03116E3FC3B3821A0525322B0A430FAA6B3C0B4
[* FILE PERMISSIONS *] NT AUTHORITY\SYSTEM FullControl; BUILTIN\Administrators FullControl; BUILTIN\Users ReadAndExecute, Synchronize; APPLICATION PACKAGE AUTHORITY\ALL APPLIC
N PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES ReadAndExecute, Synchronize;
[* IS PE *] yes
[* USED AS SERVICE *] no
[* ARCHITECTURE *] 32BIT
[* SECURITY FEATURES * ] ASLR, DEP, SafeSEH, StrongNaming

[* FILE NAME *] C:\Program Files\Medtronic\Carelink\Uploader\DSS\WinCareLinkLauncher.exe
[* FILE SIZE *] 0.767120361328125MB
[* MDSUM * ] 2BCF5A8589360C5A9794774AD558A7C1
[* SHA256 *] 04CA6F0B8300C2032A8C97DC16CC2E414B66551ED332F00A376077FFAD26B486
[* FILE PERMISSIONS *] NT AUTHORITY\SYSTEM FullControl; BUILTIN\Administrators FullControl; BUILTIN\Users ReadAndExecute, Synchronize; APPLICATION PACKAGE AUTHORITY\ALL APPLIC
N PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES ReadAndExecute, Synchronize;
[* IS PE *] yes
[* USED AS SERVICE *] no
[* ARCHITECTURE *] 32BIT
[* SECURITY FEATURES * ] ASLR, DEP, SafeSEH, StrongNaming

[* FILE NAME *] C:\Program Files\Medtronic\Carelink\Uploader\DSS\Drivers\serial
[* FILE SIZE *] 9.5367431640625E-07MB
[* MDSUM * ]
[* SHA256 *]
[* FILE PERMISSIONS *] NT SERVICE\TrustedInstaller FullControl; NT SERVICE\TrustedInstaller 268435456; NT AUTHORITY\SYSTEM FullControl; NT AUTHORITY\SYSTEM 268435456; BUILTIN\
435456; BUILTIN\Users ReadAndExecute, Synchronize; BUILTIN\Users -1610612736; CREATOR OWNER 268435456; APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES ReadAndExecute, S
ION PACKAGES -1610612736; APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES ReadAndExecute, Synchronize; APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATI
[* IS PE *] no
```

Tool Development

```
root@[redacted]:~/data/medtronic/rcFileScan# python rcPEfileScan.py CareLinkUploader-AC
C-7350-3.11.0-windows-installer.exe
[+] File Type: PE
[+] File Size: 178548960 bytes
[+] MD5: cf0a57d5441239da426922e481a2a85e
[+] SHA256: 62b9e6928b3884bc67868423dc9a63d76bb05118ae7c5ada1ee453355981f383
[+] Entropy: 7.9983
[+] Number of Sections: 11
[+] Section Names: ['.text', '.data', '.rdata', '.eh_fram', '.bss', '.edata', '.idata',
'.CRT', '.tls', '.rsrc', '.reloc']
[+] Imports:
  ADVAPI32.DLL
    GetSecurityDescriptorOwner
    GetSidIdentifierAuthority
    GetUserNameA
    GetUserNameW
    RegCloseKey
    RegOpenKeyExA
    RegQueryValueExA
    listen
    ntohs
    recv
    select
    send
    setsockopt
    socket
[+] Exports:
  TclKit_AppInit
  TclKit_SetKitPath
[+] Dependencies: {'GDI32.dll', 'SHELL32.DLL', 'OLEAUT32.DLL', 'WS2_32.dll', 'OLE32.dll'
, 'USER32.dll', 'COMCTL32.DLL', 'msvcrt.dll', 'COMDLG32.DLL', 'IMM32.DLL', 'ADVAPI32.DLL
', 'KERNEL32.dll'}
[+] Security Options:
  DEP: True
  ASLR: True
  NX: True
  SEH: True
  CFG: False
[+] Compile Time: 2023-01-04 15:12:35
[+] Compiler Version: 2.22
```

Knowledge Base

Home New Device

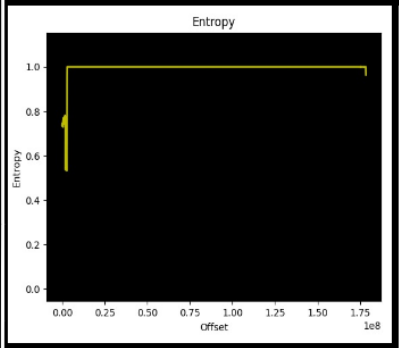
search for device, component, filename, m5sum

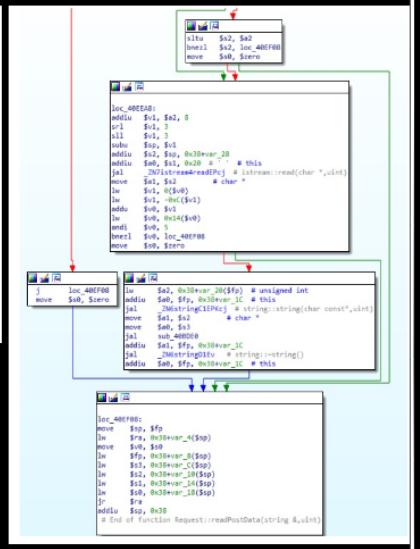
- MikroTik mAP2nd Router
- Catalog
  - Make: MikroTik
  - Model: RBmAP2m0
  - Serial Number: DE500FA1A1D4/141/r2
- Open Source Research
- Manuals & Datasheets
- Firmware Analysis
- Components
  - NANYA2113 NT5TU32M16FG-AC
  - Winbond 250128JVSM 3121
- Debugging Interfaces & Steps
- RF Survey Results
  - Spectrum Analysis
  - Bluetooth
  - Wifi
  - GSM
- Network Survey
  - Open Ports
  - Full Packet Capture
  - Burp Scan
- Vulnerabilities
- Testing Tools

Firmware Analysis

Firmware Type: Nova Package
Firmware Version: 6.38
Architecture: MIPS
Checksum: df0a57d5463239da426922e481a2a85f

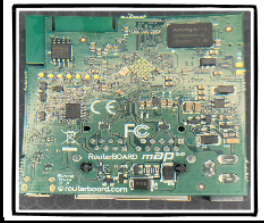
Firmware Call Graph





EXTERNAL PHOTOS

INTERNAL PHOTOS



< Upload & Scan Images

Click to zoom

Edit Device

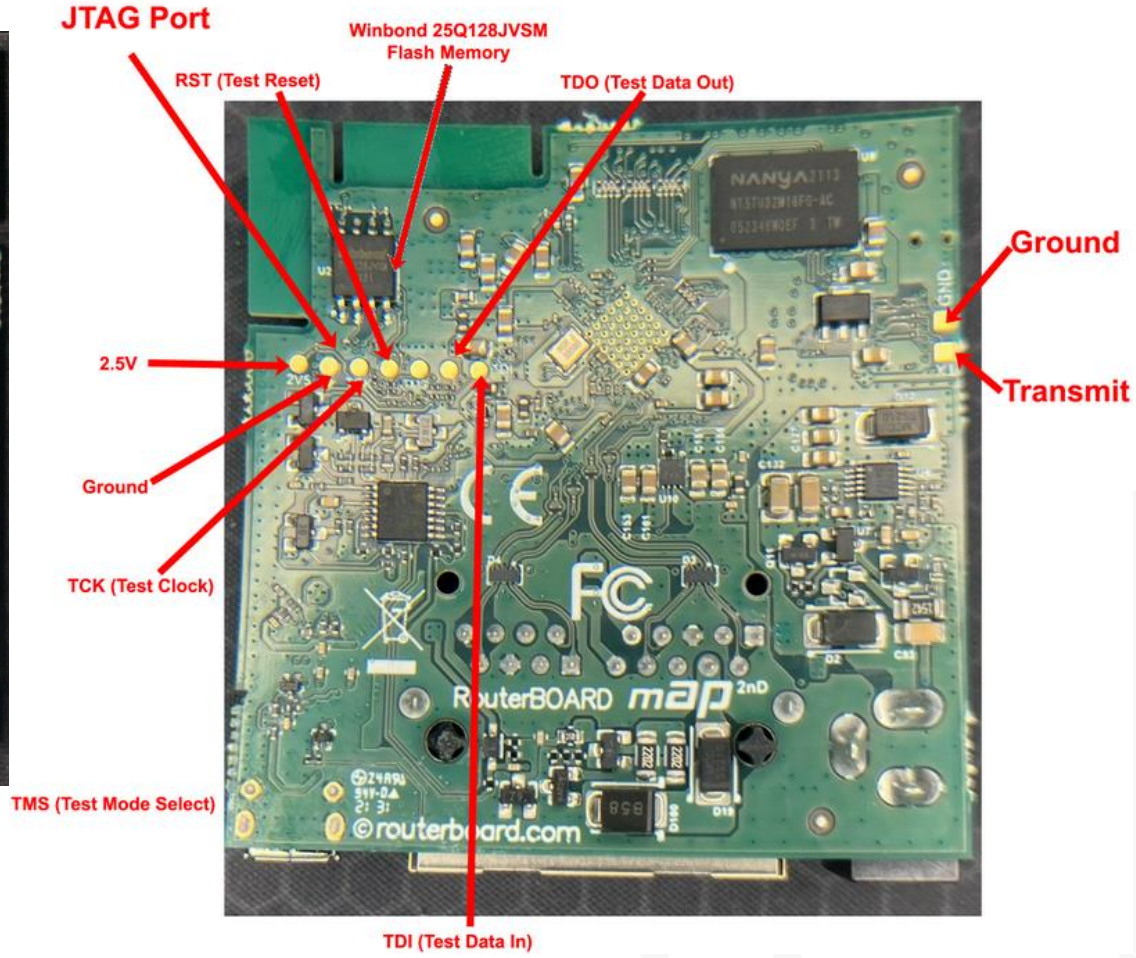
Documentation

"If You Didn't Document It, You Didn't Do It"

- Sections of report for different audiences
  - Executive Summary (Management)
  - High level technical details (Devs & Sysadmins)
  - Deep technical details (other RE's)
- Photos & device catalog
- Every test & results
  - Description of test conditions & steps to reproduce
- 1 Page per $1000
- CD, USB, Zip with all supporting data
  - PCAPS, RF captures, debug logs, scans

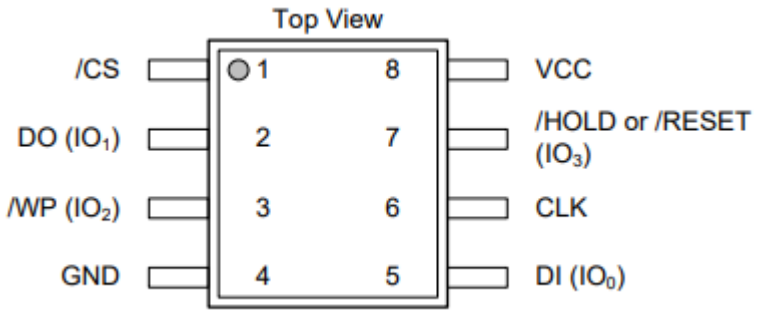
Example Case Study

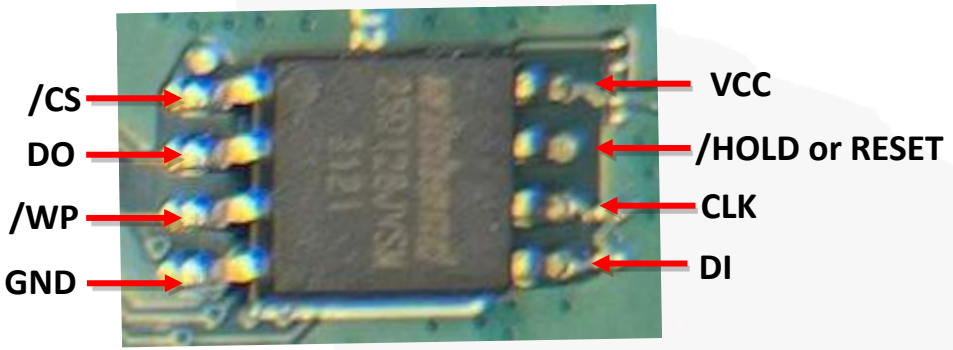
- Mikrotik mAP2nd Router



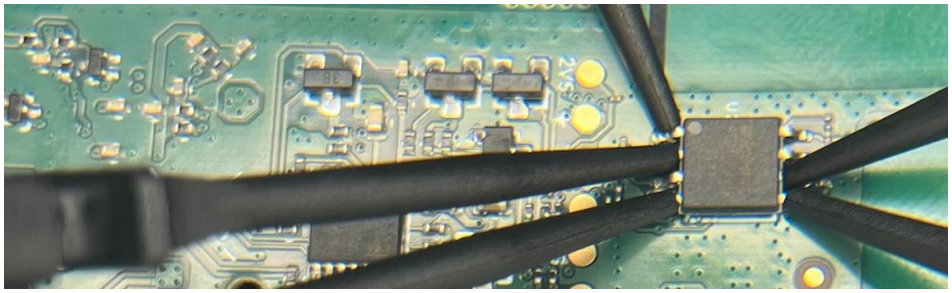
Example Case Study

- Winbond 25Q128JVSM
  - 3V 128M-BIT SERIAL FLASH MEMORY
  - Datasheet: https://datasheetspdf.com/pdf-file/1462146/Winbond/25Q128JVSM/1
  - Pin Configuration From Data Sheet:

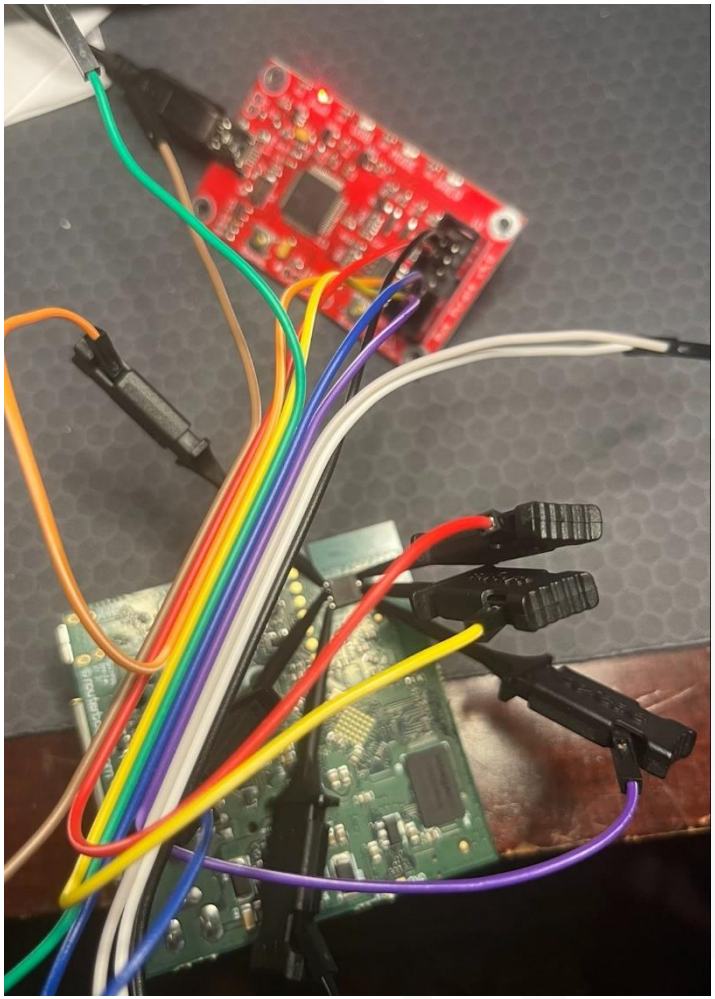




Example Case Study



WIRE COLOR	WB CHIP PINS	BUSPIRATE PINS
- Yellow	- CS	- CS
- Green	- DO	- MISO
- Blue	- WP	
- Purple	- GND	- GND
- Black	- VCC	- +3.3
- Brown	- RES	
- Red	- CLK	- CLK
- Orange	- DI	- MOSI



Example Case Study

- **Firmware Dump:**

```
# flashrom -p buspirate_spi:dev=/dev/ttyUSB0,spispeed=500k -r firmware_dump.bin -VVV

0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
done.
programmer_unmap_flash_region: unmapped 0x0000000000000000
buspirate_sendrecv: write 1, read 0 Sending 0x00
buspirate_sendrecv: write 0, read 4 , receiving 0x42 0x42 0x49 0x4f
buspirate_sendrecv: write 0, read 1 , receiving 0x31
Raw bitbang mode version 1
buspirate_sendrecv: write 1, read 0 Sending 0x0f
Bus Pirate shutdown completed.

-rw-r--r--  1 root root  16777216 Sep  9 17:47 firmware_dump.bin
```

Alternative Tools:
- OpenOCD
- PyOCD

Example Case Study

- **Search file for signatures:**

```
# binwalk -B firmware_dump.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
1936          0x790           CRC32 polynomial table, little endian
950480        0xE80D0         xz compressed data
6369136       0x612F70        gzip compressed data, has original file name: "roteros.dll", from Unix, last modified: 2021-05-31
9013347       0x898863        gzip compressed data, has original file name: "secure.dll", from Unix, last modified: 2021-05-31
9052581       0x8A21A5        gzip compressed data, has original file name: "wlan6.dll", from Unix, last modified: 2021-05-31
9130578       0x8B5252        gzip compressed data, has original file name: "iframe.html", from Unix, last modified: 2021-05-31
9131091       0x8B5453        PNG image, 7 x 7, 8-bit/color RGBA, non-interlaced
9132652       0x8B5A6C        PNG image, 512 x 64, 8-bit/color RGBA, non-interlaced
9218884       0x8CAB44        xz compressed data
9248368       0x8D1E70        xz compressed data
9288416       0x8DBAE0        xz compressed data
9288447       0x8DBAFF        gzip compressed data, has original file name: "dhcp.dll", from Unix, last modified: 2021-05-31 07:33:47
9368892       0x8EF53C        gzip compressed data, has original file name: "ipv6.dll", from Unix, last modified: 2021-05-31 07:36:07
9451262       0x9036FE        gzip compressed data, has original file name: "ppp.dll", from Unix, last modified: 2021-05-31 07:35:12
9551692       0x91BF4C        xz compressed data
9612800       0x92AE00        xz compressed data
9612831       0x92AE1F        gzip compressed data, has original file name: "master-min.js", from Unix, last modified: 2021-05-31
07:12:40
9698952       0x93FE88        gzip compressed data, has original file name: "curve255-min.js", from Unix, last modified: 2021-05-31
07:12:39
9784725       0x954D95        gzip compressed data, has original file name: "ipv6.jg", from Unix, last modified: 2021-05-31 07:36:07
9791354       0x95677A        gzip compressed data, has original file name: "mpls.jg", from Unix, last modified: 2021-05-31 07:35:47
11049606      0xA89A86        ELF, 32-bit MSB MIPS64 executable, MIPS, version 1 (SYSV)
13527889      0xCE6B51        Neighborly text, "neighbor discovery-settings set discover-interface-list=LAN /tool mac-server set
allowed-interface-list=LAN"
```

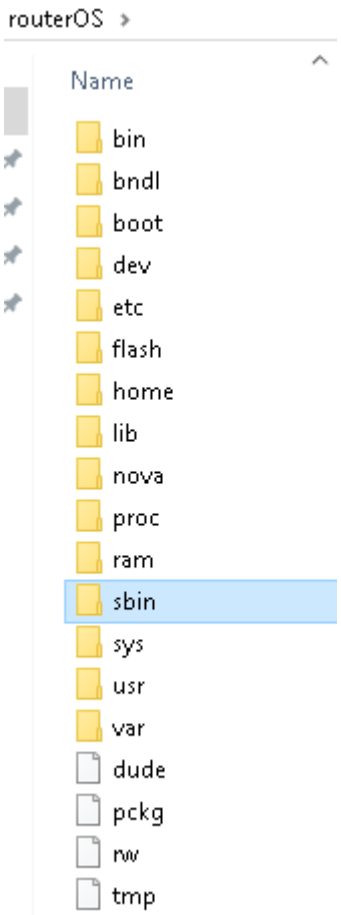
Example Case Study

- **Extract the files:**

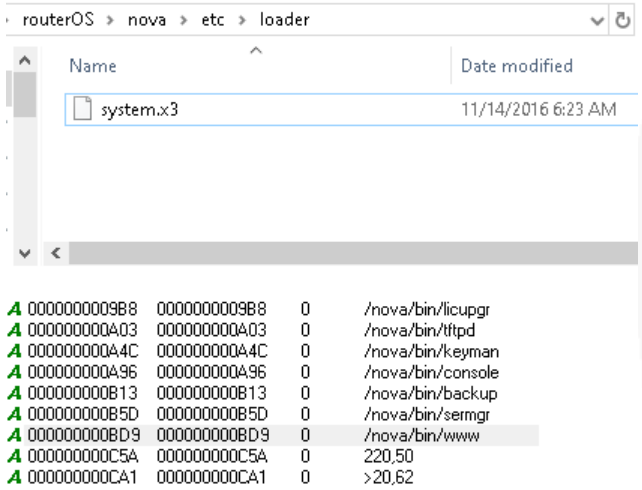
```
# binwalk --run-as=root -e -M firmware_dump.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
1936          0x790           CRC32 polynomial table, little endian

Scan Time:     2023-09-09 17:54:59
Target File:   /root/_firmware_dump.bin.extracted/E80D0
MD5 Checksum:  6eb40faa97ee5e0dd7d68c8fe51cd770
Signatures:    411

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             ELF, 32-bit MSB MIPS64 executable, MIPS, version 1 (SYSV)

Scan Time:     2023-09-09 17:54:59
Target File:   /root/_firmware_dump.bin.extracted/FD1FC
MD5 Checksum:  3c4464073496b309285d7339526e58ed
Signatures:    411
```

Example Case Study

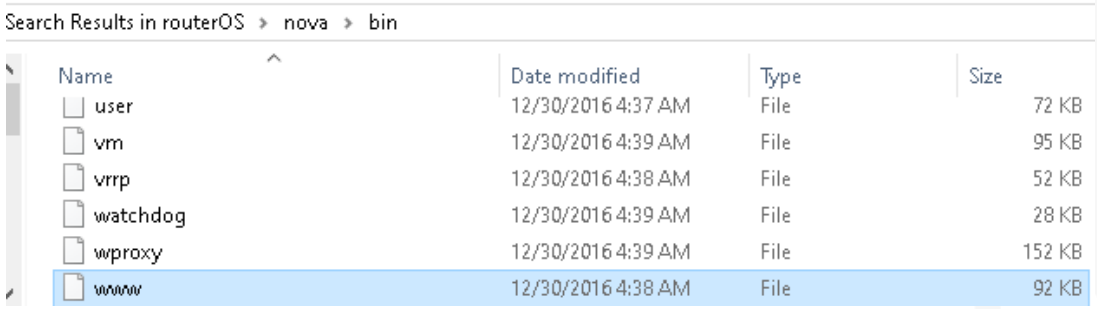
1. Filesystem Extracted From Firmware



2. Identify Loaded Binaries by looking at strings in the system.x3 binary



3. Find the www binary



4. Disassemble the MIPS www binary & identify potential vulns

```
var_28= -0x28
var_20= -0x20
var_1C= -0x1C
var_18= -0x18
var_14= -0x14
var_10= -0x10
var_C= -0xC
var_8= -8
var_4= -4

addiu   $sp, -0x38
sw      $fp, 0x38+var_8($sp)
sw      $s3, 0x38+var_C($sp)
move    $fp, $sp
move    $s3, $a1
lui     $a1, 0x41  # 'A'
sw      $s1, 0x38+var_14($sp)
la      $a1, aContentLength  # "content-length"
move    $s1, $a0
addiu   $a0, $fp, 0x38+var_1C  # this
sw      $ra, 0x38+var_4($sp)
sw      $s2, 0x38+var_10($sp)
sw      $s0, 0x38+var_18($sp)
move    $s2, $a2
jal     _ZN6stringC1EPKc  # string::string(char const*)
sw      $zero, 0x38+var_20($fp)
move    $a0, $s1          # this
addiu   $a1, $fp, 0x38+var_1C  # string *
jal     _ZNK7Headers9getHeaderERK6stringPj  # Headers::getHeader(string const&,uint *)
addiu   $a2, $fp, 0x38+var_20  # unsigned int *
move    $s0, $v0
jal     _ZN6stringD1Ev   # string::~string()
addiu   $a0, $fp, 0x38+var_1C  # this
bnez    $s0, loc_40EE94
nop
```

Example Case Study

- **Check extracted files:**

$ cat iframe.html

```
<html>
<body
onload="parent.generateContent(parent.location.hash.substr(1));"
>
</body>
</html>
<html>
  <head>
   <link rel="stylesheet" type="text/css"
href="master.css"></link>
  </head>
  <style>
    form {
        display: inline;
        width: 100%;
    }
    input {
        width: 100%;
        height: 26px;
        background: #fff;
        border: 1px solid #888;
        margin: 0;
        padding: 1px;
        font-family: verdana, arial, helvetica, sans-serif;
        font-size: 12px;
        box-shadow: none;
        -mox-box-shadow: none;
    }
  </style>
  <body  style="margin:0; white-space: nowrap">
    <form id="form" action="/jsproxy/upload" method="post"
          enctype="multipart/form-data">
      <input id="file" type="file" name="file">
    </form>
  </body>
</html>
```

- **Analyze binaries:**

```
$ strings A89A86.elf |more
mips
RouterOS for mipsbe RouterBOARDs, bridgeports.dat
bridgeports.idx
switch-config.dat
ether2
wlan10

#| Welcome to RouterOS!
#| RouterMode:
#|  * WAN port is protected by firewall and enabled DHCP client
#|  * Wireless and Ethernet interfaces (except WAN port/s)
#| LAN Configuration:
#|     IP address 192.168.88.1/24 is set on bridge (LAN port)
#|     DHCP Server: enabled;
#|     DNS: enabled;
#| wlan1 Configuration:
#|     mode:                ap-bridge;
#|     band:                2ghz-b/g/n;
#|     wpa2:       no;
#|     ht-extension:        20/40mhz-XX;
:if ($action = "apply") do={
  # wait for interfaces
  :local count 0;
  :while ([/interface ethernet find] = "") do={
    :if ($count = 30) do={
      :log warning "DefConf: Unable to find ethernet interfaces";
      /quit;
    }
    :delay 1s; :set count ($count +1);
  };
  :local count 0;
  :while ([/interface wireless print count-only] < 1) do={
    :set count ($count +1);
    :if ($count = 40) do={
      :log warning "DefConf: Unable to find wireless
interface(s)";
      /ip address add address=192.168.88.1/24 interface=ether1
comment="defconf";
      /quit
```

Questions

If you have questions or need further details please contact:

https://www.redcrowlab.com

asclark@redcrowlab.com