



# YAFFS2 Support

# Android YAFFS2

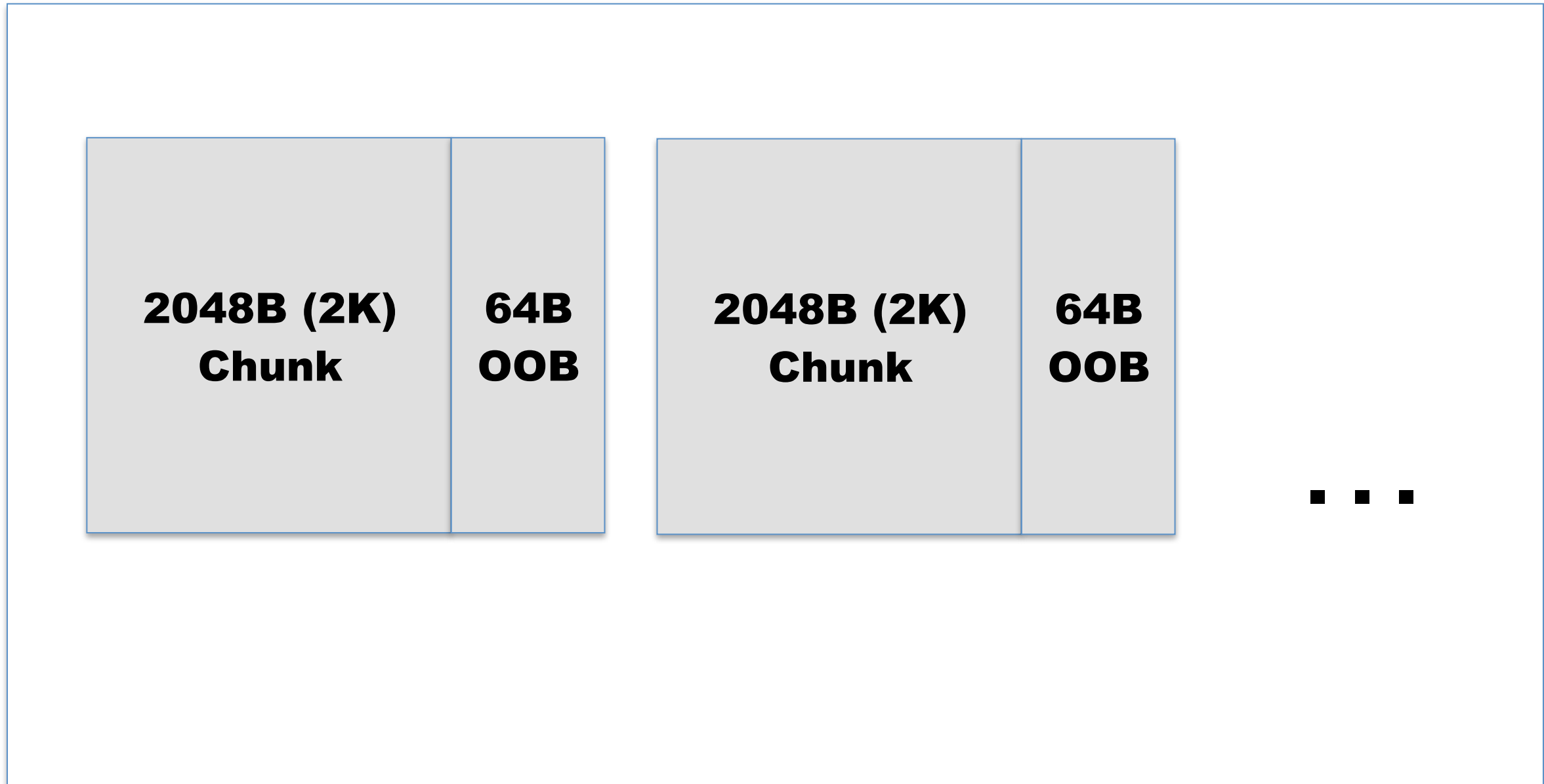
- Yet Another Flash File System 2
- Open source
- Have to compile tools/kernel module yourself (some optional support in newer kernels)
- Provides
  - Log-structured file system (think versioning)
  - Wear leveling
  - Much faster than YAFFS and JFFS, uses less RAM
  - Supports many flash geometries
  - Built in error correction (important to use nandread/nandwrite tools!)

# YAFFS2 Data Structures

- Data stored in YAFFS2 are referred to as Objects
  - Files
  - Directories
  - Symbolic and hard links
- Chunk stores either an Object or an `yaffs_ObjectHeader`
  - Metadata about the Object
    - Object type, the parent object, a checksum of the name to speed up searching, the object name, permissions and ownership, MAC information and the size of the object if it is a file
  - All objects are identified by a unique `objectId` (i.e. inodes)

# YAFFS2 – Block/Chunk/OOB diagram

**Block (128KB = 64 2k chunks + OOB)**



# Ever tried to mount YAFFS2 on Linux?

```
$ sudo apt-get install mtd-utils
```

Compile YAFFS2 from source

```
$ sudo modprobe mtd
```

```
$ sudo modprobe mtdblock
```

```
$ sudo modprobe nandsim first_id_byte=0x20 second_id_byte=0xa2  
third_id_byte=0x00 fourth_id_byte=0x15
```

```
$ cat /proc/mtd
```

```
dev:      size    erasesize  name
```

```
mtd0: 04000000 00020000 "NAND simulator partition 0"
```

```
$ sudo insmod ~/yaffs2/yaffs2.ko
```

(optional) 

```
$ sudo nandwrite -autoplace -oob /dev/mtd0 yaffs2.nanddump
```

```
$ sudo mount -t yaffs2 /dev/mtdblock0 ~/mnt/yaffs2/
```

# Mount YAFFS2 results (or order of likeliness)

Fail

-----

```
mount: wrong fs type, bad option, bad superblock on /dev/mtdblock0,  
missing codepage or helper program, or other error  
In some cases useful info is found in syslog - try  
dmesg | tail or so
```

No data

-----

```
$ ls -la ~/mnt/yaffs2/  
total 8  
drwxr-xr-x 1 root  root  2048 2011-02-03 11:37 .  
drwxr-xr-x 3 ahoog ahoog 4096 2011-02-03 07:21 ..  
drwx----- 1 root  root  2048 2011-02-03 11:37 lost+found
```

Actually worked (rare)

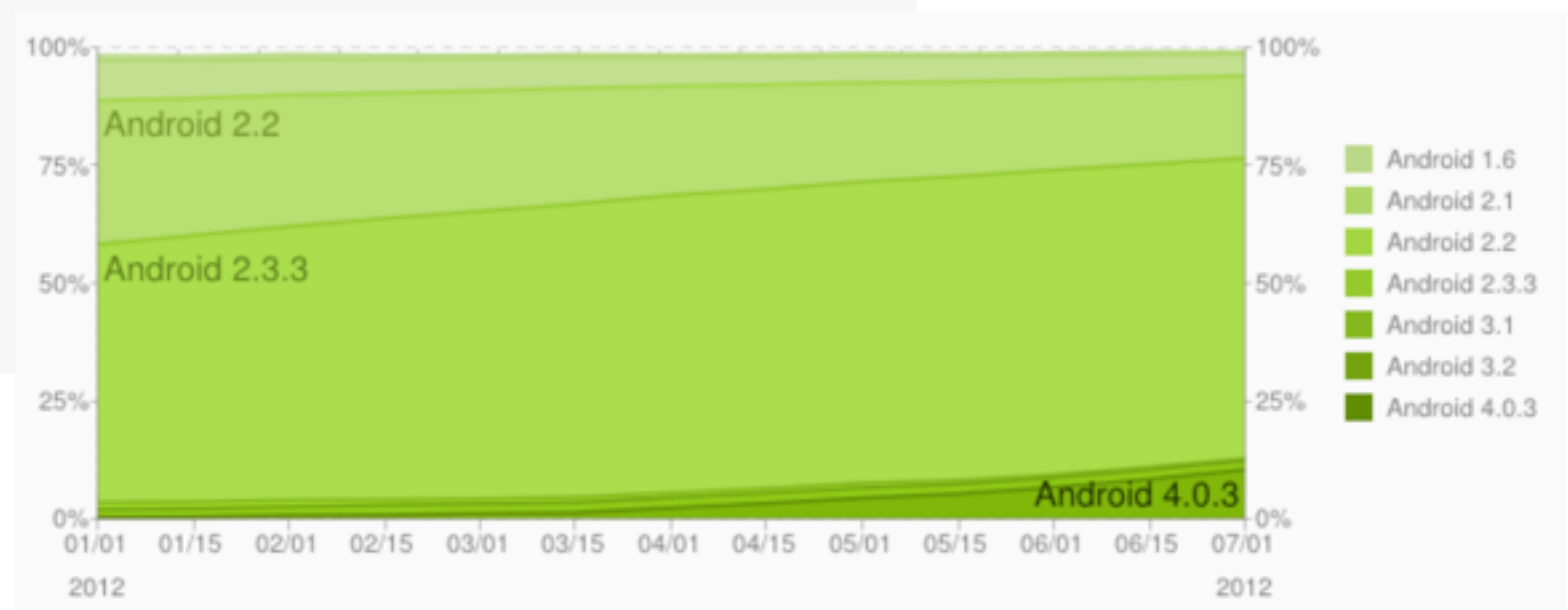
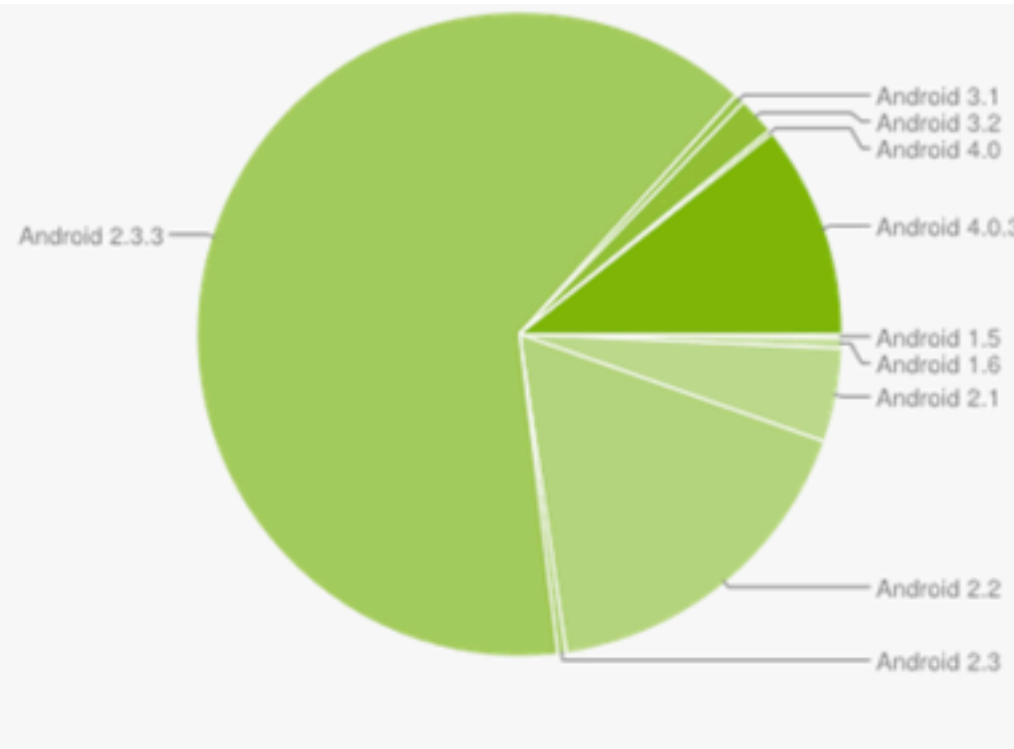
-----

<Imagine listing of files here>

# Why Fail?

Version	Codename	API Level	Distribution
1.5	Cupcake	3	0.2%
1.6	Donut	4	0.5%
2.1	Eclair	7	4.7%
2.2	Froyo	8	17.3%
2.3 - 2.3.2	Gingerbread	9	0.4%
2.3.3 - 2.3.7		10	63.6%
3.1	Honeycomb	12	0.5%
3.2		13	1.9%
4.0 - 4.0.2	Ice Cream Sandwich	14	0.2%
4.0.3 - 4.0.4		15	10.7%

Data collected during a 14-day period ending on July 2, 2012



<https://viaforensics.com>

# Header Objects

Yaffs2\_ObjectHeader

struct {

....

}

Parent →

Name →

```
struct yaffs_obj_hdr {
    enum yaffs_obj_type type; ← Obj Type
    int parent_obj_id;
    u16 sum_no_longer_used; /* checksum of name. No longer used */
    YCHAR name[YAFFS_MAX_NAME_LENGTH + 1];
    u32 yst_mode;
    u32 yst_uid;
    u32 yst_gid;
    u32 yst_atime; ← File Times
    u32 yst_mtime;
    u32 yst_ctime;
    int file_size; (object type: file)
    int equiv_id; (object type: symbolic)
    YCHAR alias[YAFFS_MAX_ALIAS_LENGTH + 1];
    u32 yst_rdev;
    u32 win_ctime[2];
    u32 win_atime[2];
    u32 win_mtime[2];
    u32 inband_shadowed_obj_id;
    u32 inband_is_shrink;
    u32 reserved[2];
    int shadows_obj;
    u32 is_shrink;};
```

A few highlights

<https://viaforensics.com>



# Out Of Band / Spare Area

blockState      blockSequence      objectID      chunkID      nBytes

ff	ff	02 10 00 00	01 01 00 00	3f 00 00 00	00 08
00	00	2a 00 00 00	0d 00 00 00	f2 ff ff ff	ff ff
ff	ff	ff ff ff ff	ff ff 55 65	5b 69 a6 5b	55 66
a7	9a	95 57 c3 f3	33 aa 59 a7	96 99 a7 66	a5 57

OOB Data Chunk

0x800 file size means page is fully used.

OOB File Header

blockState      blockSequence      objectID      chunkID      nBytes

ff	ff	08 10 00 00	09 01 00 10	01 00 00 80	00 00
02 00	29 00 00 00	0e 00 00 00	f1 ff ff ff	ff ff	
ff ff	ff ff ff ff	ff ff a9 9a	5b fc f0 3f	ff ff	
ff ff	ff ff ff ff	ff ff ff ff	ff ff ff ff	ff ff	

Object Type

<https://viaforensics.com>

# Verification through OOB

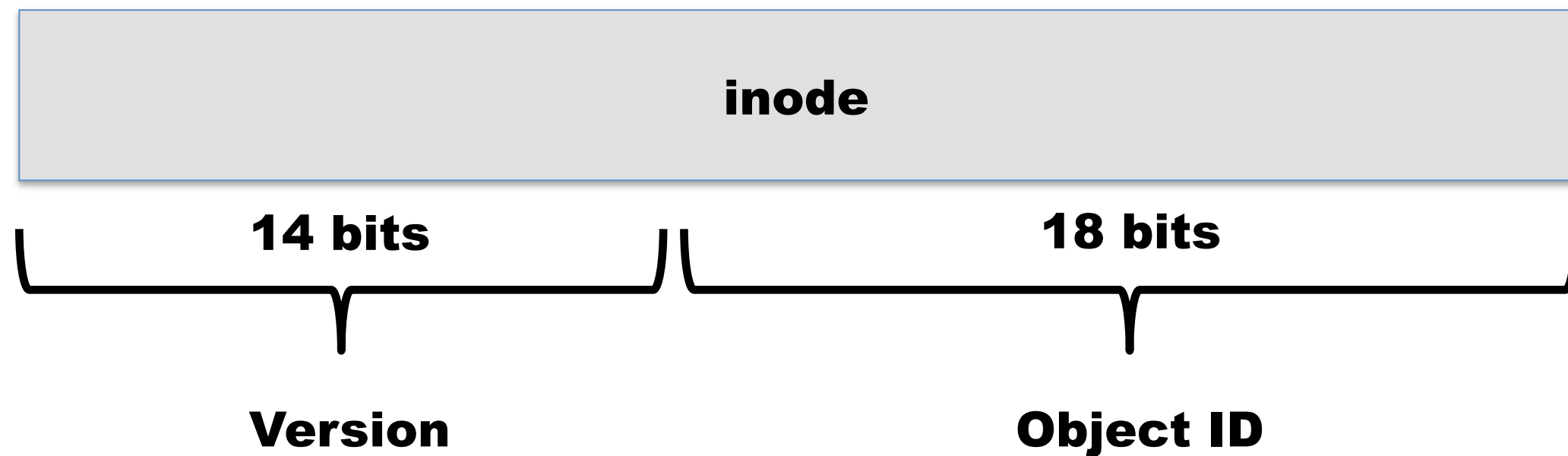
Field	Size for 1024 bytes chunks	Size for 2048 bytes chunks
blockState	1 byte	1 byte
chunkID	4 bytes	4 bytes
objectID	4 bytes	4 bytes
nBytes	2 bytes	2 bytes
blockSequence	4 bytes	4 bytes
tagsEcc	3 bytes	3 bytes
ecc	12 bytes	24 bytes

- 0x00: Unknown object type
- 0x01: file
- 0x02: symbolic link
- 0x03: directory
- 0x04: hard link
- 0x05: special

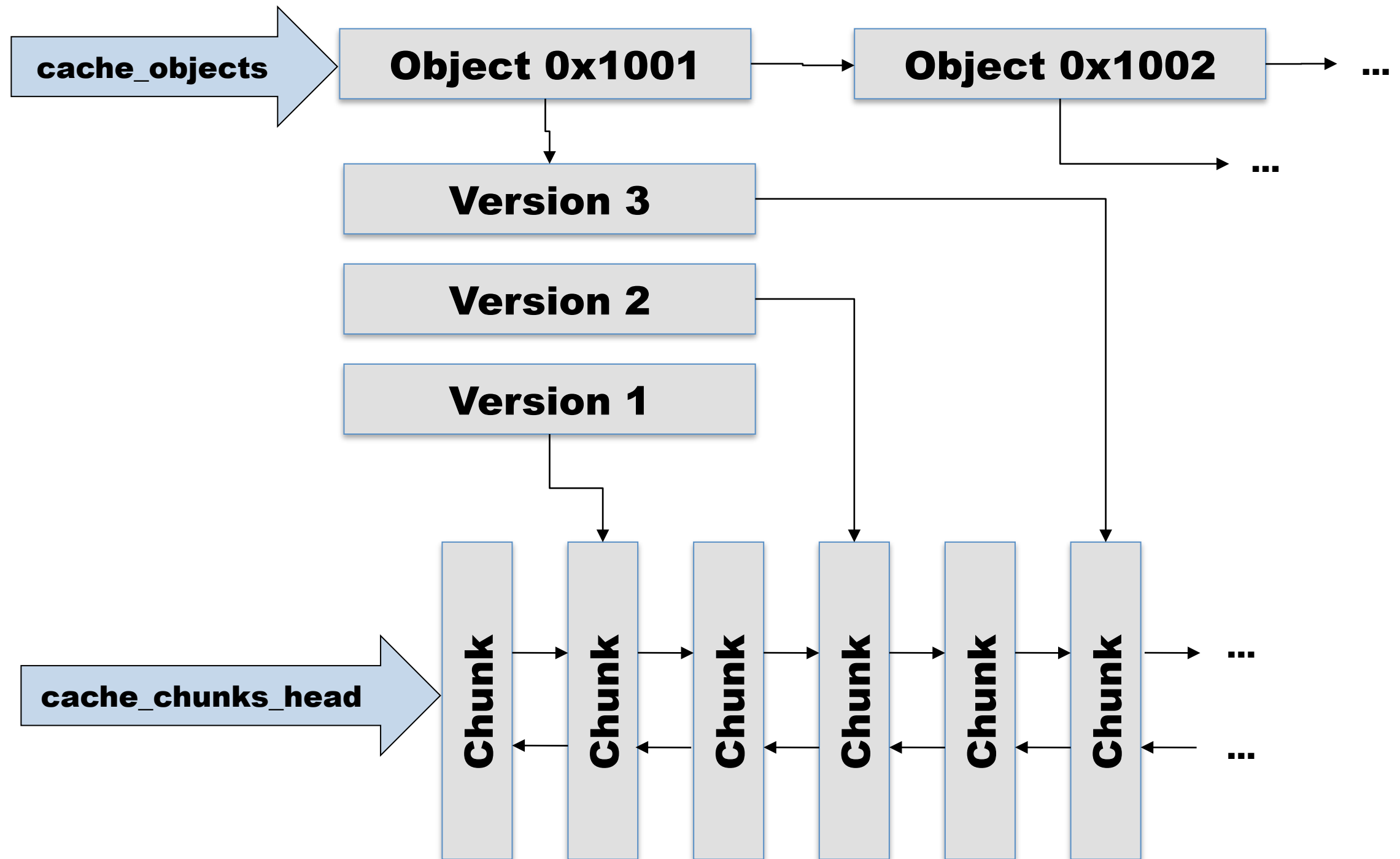
The chunk is identified as object header when it meets the requirements:

1. The size of the chunk must be larger than 512 bytes.
2. Bytes 0-3 should be equal to one of the object type values
3. Bytes 8-9 should be equal to 0xFFFF (not used)
4. All bytes from offset 512 onward should be equal to 0xFF

# YAFFS2 – TSK inode Mapping



# YAFFS2 – TSK Cache scanned at tsk\_open



# Looking at a Simple FS

```
yaffs-experiments — investigator — 186x54
+++++
Listing Files...
* 1 -      listing
* 2 -      subfolder
* 3 -      listing
* 4 -
* 5 -      .#file.txt
* 6 -
* 7 -      file.txt
* 8 -      [chunk]
* 9 -      file.txt
* 10 -     unlinked
* 11 -     deleted
* 12 -
* 13 -     .#underdog.txt
* 14 -     subfolder
* 15 -     #underdog.txt#
* 16 -     [chunk]
* 17 -     #underdog.txt#
* 18 -     [chunk]
* 19 -     #underdog.txt#
* 20 -     #underdog.txt#
* 21 -     [chunk]
* 22 -     #underdog.txt#
* 23 -     underdog.txt
* 24 -     [chunk]
* 25 -     underdog.txt
* 26 -     unlinked
* 27 -     deleted
* 28 -     unlinked
* 29 -     deleted
* 30 -     subfolder
* 31 -     undercopy.txt
* 32 -     [chunk]
* 33 -     undercopy.txt
* 34 -     [chunk]
* 35 -     .#file.txt
* 36 -
* 37 -     file.txt~
* 38 -     file.txt
* 39 -     [chunk]
* 40 -     file.txt
* 41 -     unlinked
* 42 -     deleted
* 43 -     file.txt
* 44 -
* 45 -     file.txt
* 46 -     [chunk]
* 47 -     file.txt
* 48 -     listing
----- listing 48 objects -----
:
```



# 5 Entries Later...

## We have Version 3

```
*****
Entry 21 - (null)
x54 x68 x65 x72 x65 x27 x73 x20 x6e x6f x20 x6e x65 x65 x64 x20      There's no need
x74 x6f x20 x66 x65 x61 x72 x21 x20 x55 x6e x64 x65 x72 x64 x6f      to fear! Underdo
x67 x20 x69 x73 x20 x68 x65 x72 x65 x21 x8a x8a x77 x68 x65 x6e      g is here!..when
x20 x63 x72 x69 x6d x69 x6e x61 x6c x20 x69 x6e x20 x74 x68 x69      criminal in thi
x73 x20 x77 x6f x72 x6c x64 x20 x61 x70 x70 x65 x61 x72 x20 x8a      s world appear .
x61 x6e x64 x20 x62 x72 x65 x61 x6b x20 x74 x68 x65 x20 x6c x61      and break the la
x77 x73 x20 x74 x68 x61 x74 x20 x74 x68 x65 x79 x20 x73 x68 x6f      ws that they sho
x75 x6c x64 x20 x66 x65 x61 x72 x8a x61 x6e x64 x20 x66 x72 x69      uld fear.and fri
x67 x68 x74 x65 x6e x20 x61 x6c x6c x20 x77 x68 x6f x20 x73 x65      ghten all who se
x65 x20 x6f x72 x20 x68 x65 x61 x72 x8a x74 x68 x65 x20 x63 x72      e or hear.the cr
x79 x20 x67 x6f x65 x73 x20 x75 x70 x20 x62 x6f x74 x68 x20 x66      y goes up both f
x61 x72 x20 x61 x6e x64 x20 x6e x65 x61 x72 x8a x66 x6f x72 x20      ar and near.for
x55 x6e x64 x65 x72 x64 x6f x67 x21 x20 x20 x55 x6e x64 x65 x72      Underdog! Under
x64 x6f x67 x21 x20 x20 x55 x6e x64 x65 x72 x64 x6f x67 x21 x20      dog! Underdog!
x20 x55 x6e x64 x65 x72 x64 x6f x67 x21 x8a x8a x73 x70 x65 x65      Underdog!..spee
x64 x20 x6f x66 x20 x6c x69 x67 x68 x74 x6e x69 x6e x67 x2c x20      d of lightning,
x72 x6f x61 x72 x20 x6f x66 x20 x74 x68 x75 x6e x64 x65 x72 x8a      roar of thunder.
x66 x69 x67 x68 x74 x69 x6e x67 x20 x61 x6c x6c x20 x77 x68 x6f      fighting all who
x20 x72 x6f x62 x20 x6f x72 x20 x70 x6c x75 x6e x64 x65 x72 x8a      rob or plunder.
x55 x6e x64 x65 x72 x64 x6f x67 x2e x20 x20 x55 x6e x64 x65 x72      Underdog. Under
x64 x6f x67 x21 x8a x8a x77 x68 x65 x6e x20 x69 x6e x20 x74 x68      dog!..when in th
x69 x73 x20 x77 x6f x72 x6c x64 x20 x74 x68 x65 x20 x68 x65 x61      is world the hea
x64 x6c x69 x6e x65 x73 x20 x72 x65 x61 x64 x8a x6f x66 x20 x74      dlines read.of t
x68 x6f x73 x65 x20 x77 x68 x6f x73 x20 x68 x65 x61 x72 x74 x73      hose whos hearts
x20 x61 x72 x65 x20 x66 x69 x6c x6c x65 x64 x20 x77 x69 x74 x68      are filled with
x20 x67 x72 x65 x65 x64 x8a x77 x68 x6f x20 x72 x6f x62 x20 x61      greed.who rob a
x6e x64 x20 x73 x74 x72 x65 x61 x6c x20 x66 x72 x6f x6d x20 x74      nd steal from t
x68 x6f x73 x65 x20 x77 x68 x6f x20 x6e x65 x65 x64 x8a x74 x6f      hose who need.to
x20 x72 x69 x67 x68 x74 x20 x74 x68 x69 x73 x20 x77 x72 x6f x6e      right this wron
x67 x20 x77 x69 x74 x68 x20 x62 x6c x69 x6e x64 x00 x00 x00 x00      g with blind....
x00 x00 x00 x00 x00 x00 x00 x00 x00 x00 x00 x00 x00 x00
x00 x00 x00 x00 x00 x00 x00 x00 x00 x00 x00 x00 x00 x00
..... clearing .....
```

<https://viaforensics.com>

# Objects & Chunks (with ownership)

```
yaffs-experiments — investigator — 186x54
+++++
Listing Files...
* 1 -      listing
* 2 -      subfolder
* 3 -      listing
* 4 -
* 5 -      .#file.txt
* 6 -
* 7 -      file.txt
* 8 -      [chunk]      file.txt
* 9 -      file.txt
* 10 -     unlinked
* 11 -     deleted
* 12 -
* 13 -     .#underdog.txt
* 14 -     subfolder
* 15 -     #underdog.txt#
* 16 -     [chunk]      #underdog.txt#
* 17 -     #underdog.txt#
* 18 -     [chunk]      #underdog.txt#
* 19 -     #underdog.txt#
* 20 -     #underdog.txt#
* 21 -     [chunk]      #underdog.txt#
* 22 -     #underdog.txt#
* 23 -     underdog.txt
* 24 -     [chunk]      underdog.txt
* 25 -     underdog.txt
* 26 -     unlinked
* 27 -     deleted
* 28 -     unlinked
* 29 -     deleted
* 30 -     subfolder
* 31 -     undercopy.txt
* 32 -     [chunk]      undercopy.txt
* 33 -     undercopy.txt
* 34 -     [chunk]      #underdog.txt#
* 35 -     .#file.txt
* 36 -
* 37 -     file.txt-
* 38 -     file.txt
* 39 -     [chunk]      file.txt
* 40 -     file.txt
* 41 -     unlinked
* 42 -     deleted
* 43 -     file.txt
* 44 -
* 45 -     file.txt
* 46 -     [chunk]      file.txt
* 47 -     file.txt
* 48 -     listing

----- listing 48 objects -----
:
```

<https://viaforensics.com>



# Reordering FS by Blocks

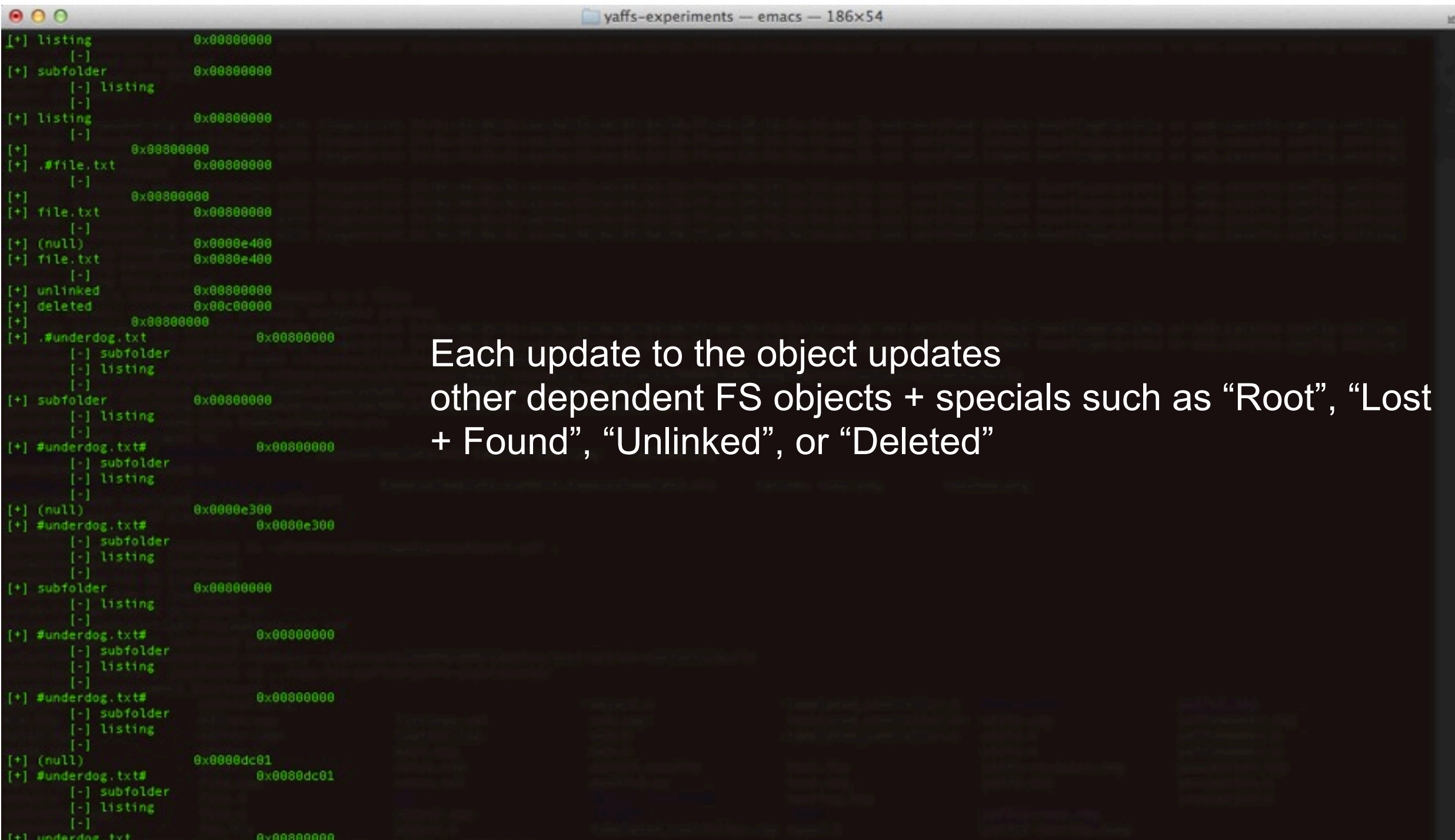
```
yaffs-experiments — emacs — 186x54

Block 00004201 -----
      (null)          0x0a010000
      (null)          0x0b010000
Block 00007002 -----
      (null)          0x07010000
      (null)          0x08010000
Block 0000dc01 -----
      (null)          0x06010000
Block 0000e300 -----
      (null)          0x06010000
Block 0000e400 -----
      (null)          0x04010000
Block 00800000 -----
      listing         0x01010030
      subfolder       0x02010030
      listing         0x01010030
      0x01000030
      .#file.txt      0x03010020
      0x01000030
      file.txt        0x04010010
      unlinked        0x03010020
      0x01000030
      .#underdog.txt  0x05010020
      subfolder       0x02010030
      #underdog.txt#   0x06010010
      subfolder       0x02010030
      #underdog.txt#   0x06010010
      #underdog.txt#   0x06010010
      underdog.txt     0x07010010
      unlinked        0x05010020
      unlinked        0x06010010
      subfolder       0x02010030
      undercopy.txt    0x08010010
      listing         0x01010030
      .#file.txt      0x09010020
      0x01000030
      file.txt        0x0a010010
      unlinked        0x09010020
      0x01000030
      file.txt        0x0b010010
      listing         0x01010030
Block 00804201 -----
      file.txt        0x0a010010
      file.txt        0x0a010010
      file.txt        0x0b010010
Block 00807002 -----
      underdog.txt     0x07010010
      undercopy.txt    0x08010010
Block 0080dc01 -----
      #underdog.txt#   0x06010010
Block 0080e300 -----
      #underdog.txt#   0x06010010
```

<https://viaforensics.com>



# Mapping Actions to a Timeline



```
yaffs-experiments — emacs — 186x54
[+] listing      0x00000000
[-]
[+] subfolder    0x00000000
[-] listing
[-]
[+] listing      0x00000000
[-]
[+]              0x00000000
[+] .#file.txt    0x00000000
[-]
[+]              0x00000000
[+] file.txt      0x00000000
[-]
[+] (null)        0x0000e400
[+] file.txt      0x0000e400
[-]
[+] unlinked      0x00000000
[+] deleted       0x00c00000
[+]              0x00000000
[+] .#underdog.txt 0x00000000
[-] subfolder
[-] listing
[-]
[+] subfolder    0x00000000
[-] listing
[-]
[+] #underdog.txt# 0x00000000
[-] subfolder
[-] listing
[-]
[+] (null)        0x0000e300
[+] #underdog.txt# 0x0000e300
[-] subfolder
[-] listing
[-]
[+] subfolder    0x00000000
[-] listing
[-]
[+] #underdog.txt# 0x00000000
[-] subfolder
[-] listing
[-]
[+] #underdog.txt# 0x00000000
[-] subfolder
[-] listing
[-]
[+] (null)        0x0000dc01
[+] #underdog.txt# 0x0000dc01
[-] subfolder
[-] listing
[-]
[+] underdog.txt  0x00000000
```

Each update to the object updates other dependent FS objects + specials such as “Root”, “Lost + Found”, “Unlinked”, or “Deleted”

# YAFFS2 in hex

```
0002940: 0100 0000 1a01 0000 ffff 6261 7474 6572 .....batter
0002950: 7973 7461 7473 2e62 696e 0000 0000 0000 ystats.bin.....
0002960: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0002970: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0002980: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0002990: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00029a0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00029b0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00029c0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00029d0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00029e0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00029f0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0002a00: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0002a10: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0002a20: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0002a30: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0002a40: 0000 0000 0000 0000 0000 ffff 8081 0000 .....
0002a50: e803 0000 e803 0000 6899 b34c 6899 b34c .....h..Lh..L
0002a60: 6899 b34c 80ab 0000 ffff ffff ffff ffff h..L.....
```

# fsstat output

```
$ fsstat -f yaffs2 yaffs2-nexus-one-postdeletion.nanddump
```

## FILE SYSTEM INFORMATION

-----

File System Type: YAFFS2

Page Size: 2048

Spare Size: 64

## METADATA INFORMATION

-----

Number of Allocated Objects: 961

Object Id Range: 1 - 1341

Number of Total Object Versions: 7365

Object Version Range: 4097 - 4930

YAFFS2 images: <https://viaforensics.com/products/tools/sleuth-kit-yaffs2/>

# fls output

```
$ fls -p -r -f yaffs2 yaffs2-nexus-one-postdeletion.nanddump (7364 results)
d/d 262146:      lost+found:2,1
d/d 262405:      dontpanic:261,1
d/d 4980998:     misc:262,19
r/r 2359555:     misc:262,19/AK8973Prms.txt:259,9
d/d 262407:     misc:262,19/bluetoothd:263,1
d/d 262408:     misc:262,19/keystore:264,1
d/d 262409:     misc:262,19/vpn:265,1
d/d 262410:     misc:262,19/vpn:265,1/profiles:266,1
d/d 524555:     misc:262,19/wifi:267,2
d/d 524564:     misc:262,19/wifi:267,2/sockets:276,2
r/- 4719206:     misc:262,19/wifi:267,2/sockets:276,2/wpa_ctrl_97-0:614,18
r/- 1311349:     misc:262,19/wifi:267,2/sockets:276,2/wpa_ctrl_97-1:629,5
d/d 262420:     misc:262,19/wifi:267,2/sockets:276,1
r/r 3670612:    misc:262,19/wifi:267,2/wpa_supPLICant.conf:596,14
r/r 3408468:    misc:262,19/wifi:267,2/wpa_supPLICant.conf:596,13
d/d 262411:     misc:262,19/wifi:267,1
d/d 524565:     misc:262,19/dhcp:277,2
r/r 786976:     misc:262,19/dhcp:277,2/dhcpd-eth0.pid:544,3
r/r 1311275:     misc:262,19/dhcp:277,2/dhcpd-eth0.lease:555,5
d/d 262421:     misc:262,19/dhcp:277,1
r/r 524566:     misc:262,19/rild_ril.prefer.network.select-type:278,2
r/r 262422:     misc:262,19/rild_ril.prefer.network.select-type:278,1
r/r 524567:     misc:262,19/rild_ril.band.select-mode:279,2
```

# Two versions of wpa\_supplicant file

```
$ icat -f yaffs2 yaffs2-nexus-one-postdeletion.nanddump 3408468
```

```
##### wpa_supplicant configuration file template #####  
update_config=1  
ctrl_interface=eth0  
eapol_version=1  
ap_scan=1  
fast_reauth=1
```

```
$ icat -f yaffs2 yaffs2-nexus-one-postdeletion.nanddump 3670612
```

```
ctrl_interface=eth0  
update_config=1  
  
network={  
    ssid="Droid"  
    psk="mountyaffs2"  
}
```

# YAFFS2 in hex

```
$ grep 596\, ~/fls.txt
```

```
r/r 3670612:      misc:262,19/wifi:267,2/wpa_supPLICant.conf:596,14
```

```
r/r 3408468:      misc:262,19/wifi:267,2/wpa_supPLICant.conf:596,13
```

```
r/r 2359892:      data:270,10/com.google.android.server.checkin:320,3/  
databases:436,266/checkin.db-journal:596,9
```

```
r/r 262740:       data:270,10/com.google.android.providers.gmail:329,3/  
databases:624,40/mailstore.yaffs2.drjohn@gmail.com.db-journal:596,1
```

```
r/r 3146324:      <deleted>/deleted:596,12
```

```
r/r 2884180:      <deleted>/deleted:596,11
```

```
r/r 2622036:      <deleted>/deleted:596,10
```

```
r/r 2097748:      <deleted>/deleted:596,8
```

```
r/r 1835604:      <deleted>/deleted:596,7
```

```
r/r 1573460:      <deleted>/deleted:596,6
```

```
r/r 1311316:      <deleted>/deleted:596,5
```

```
r/r 1049172:      <deleted>/deleted:596,4
```

```
r/r 787028:       <deleted>/deleted:596,3
```

```
r/r 524884:       <deleted>/deleted:596,2
```

# Looking at SQLite journal file

```
$ icat -f yaffs2 yaffs2-nexus-one-postdeletion.nanddump 262740 | xxd -a
```

```
00000000: d9d5 05f9 20a1 63d7 0000 0000 922f 78c3  .... .c...../x.
00000010: 0000 0030 0000 0200 0000 0400 0000 0000  ...0.....
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  .....
*
00001f0: 0000 0000 0000 0000 0000 0000 0000 0000  .....
```

Recall from fls:

```
r/r 262740:      data:270,10/com.google.android.providers.gmail:329,3/
databases:624,40/mailstore.yaffs2.drjohn@gmail.com.db-journal:596,1
```

# Santoku Linux

- Free and open bootable Linux distribution full of tools
- Project is a collaboration with other mobile security and forensic pros
- Mobile Forensics
- Mobile App Security Testing
- Mobile Malware Analysis



Check out the Alpha release at <https://santoku-linux.com>



# Sources

- YAFFS2 Object Headers - Identifying and parsing YAFFS2 objects. Ivo Pooters, Pascal Arends and Steffen Moorress
- Reverse Engineering of the Android File System - YAFFS 2. Sven Schmitt, Michael Spreitzenbarth, Christian Zimmerman.
- How YAFFS Works. Charles Manning
- A. Hoog Android Forensics: Investigation, Analysis and Mobile Security for Google Android 1st ed. Syngress Press, 2011.



Andrew Hoog  
Chief Investigative Officer

[ahoog@viaforensics.com](mailto:ahoog@viaforensics.com)

+1 312-878-1100

<https://viaforensics.com>