CHDK - “PWN” your Camera

By Aaron Grothe

Introduction

If anybody has any questions or comments at any time please let me know.

If I start to mumble please let me know as well :-)

Disclaimer

The CHDK software is designed to not have any lasting impact to your camera. However if you do try it out there is always the remote possibility of some problem.

Don't turn on LUA native methods unless you really need to.

CHDK is designed to not be a persistent change and removing it should be as simple as removing the SD card and rebooting.

CHDK?

CHDK - Canon Hack Development Kit is a piece of software that allows you to unlock additional capabilities in your Canon camera

Originally started out because “consumer grade” Canon cameras were prevented from saving photos in .raw format.

There was no apparent technical reason for this. It appeared to only be a marketing decision.

How does it work?

Andrey Gratchev and others figured out how to download the firmware from a couple of Canon cameras and began to make modifications to it.

The Canon cameras were running the VxWorks operating system from Wind River.

They added the capability to do .raw format and have added many more additional capabilities since then

Some of the Capabilities Enabled

- Raw format
- HDR
- Ulta-long shutter speeds up to 64 seconds (longer on some cameras)
- Ultra-fast shutter speeds up to 1/10,000 and higher
- Elimination of 1 GB video size-limit
- Live Histogram
- Battery Indicator

Some of the Capabilities Enabled

- Customizable CHDK display
- File browser
- Text Reader (worst ebook reader, ever)
- Calendar
- Games - Tetris, Sokoban, etc... No Doom yet.
- SCRIPTING
- And many other things

SCRIPTING???

Yep.

You can program it in either ubasic or Lua this adds a lot of additional capabilities as well

Couple of examples

- interval timer. Time-lapse photography
- Motion detection trigger - fast enough to capture lightning strikes
- USB cable remote shutter release
- Whatever else you can think of

Interval Camera - uBasic

```
@title Intervalometer
@chdk_version 1.3
@param a = interval (sec)
@default a 15

do
    s = get_tick_count
     shoot
    sleep a*1000 - (get_tick_count - s)
until ( 0 )
```

Interval Camera - Lua

```
--[[
@title Intervalometer
@chdk_version 1.3
@param a = interval (sec)
@default a 15
--]]
repeat
    start = get_tick_count()
     shoot()
    sleep(a*1000 - (get_tick_count() - start))
until ( false )
```

What Canon Cameras are supported?

List of supported cameras is available on the CHDK website

Pretty much any Canon Powershot Camera running DIGIC II, DIGIC III or DIGIC 4 platform

If it isn't available yet, might be your chance for fame. We'll talk a bit more about how they dump the firmware later as it is pretty cool.

Supports over 50 cameras currently and new ones are periodically added.

What do I need to get started?

A supported Canon Camera - firmware versions matter
A computer with an SD card reader
An empty SD card or one you don't mind reformatting

What firmware do I have?

Option #1:

There is a trick where you can create two empty files in the root directory of your SD card named ver.req and vers.req and then query the camera to get the version. This can be a bit hit or miss

Option #2:

Take a picture with a camera and then use the acid program to figure out the firmware of the Camera with that program on your computer. Let’s demo Option #2.

ACID?

ACID - the Automatic Camera Identifier and Downloader

Written in Java, requires version 1.4 or later of Java

Can download the relevant CHDK as well as part of the process

We'll run it now

Also a nice reminder about how much information you tag each photo with

We’ve identified the Camera version

In our case it is a Canon A4000 firmware 1.01a

Now we need to make an SD card with relevant firmware

For the first pass at this we’ll just use the STICK application

STICK

STICK - Simple Tool for Installing CHDK (STICK)

Rns on Windows, OSX and Linux

Another java app from the Author of ACID

Let it analyze picture, downloads the firmware and will reformat the sd card.

Note: if your PC has EMMC memory make sure you're writing to the correct place.

Now we'll run it.

Now we have an SD-card with CHDK on it

Two ways to run it on the Canon

#1. The very temporary way. Just put the SD card in and select firmware upgrade and it will temporarily load the CHDK into the running system.

#2. The easier way. Flip the write-protect flag on the SD card and just boot up the camera?

Wait. flipping the Write-protect switch flipped doesn't stop you from writing to an SD-card. Nope it is a suggestion.

Booting up the Camera

We've got an SD card read to go we should step through some of the options with it:

How to get into the CHDK menu on my camera hit the play and then menu button.

Consult your readme.txt for more info.

CHDK-PTP

We'll be using CHDK-PTP (Picture Transfer Protocol) to show the screen of the camera for the presentation.

Keep in mind if you have automounting on you have to disable it for your camera or else it will preempt the CHDK-PTP call and it won't work.

Couple of simple changes to udev and recognized devices to prevent.

CHDK what it does

We'll spend a couple of minutes going through the options on the camera. This will hopefully give you an idea of some of the things that CHDK can do on your camera.

CHDK Checklist

So we've gone through the menus a bit. Hope people found what it could do interesting.

Items to cover

Raw file output
Histogram
Games
Etc...

Example Project - Planned

Wanted to do a simple project to show some of what CHDK can make your Canon Camera do.

Decided to use intervalometer to capture a time-lapse drive from my house to the Conference Center

Drive from my house to Conference Center is about 20 minutes movie goes at a rate of about 24 fps want a 5 minute movie so figure grab a picture every 10 seconds.

Example Project - Actual

Decided to do a timelapse driving from my house to Feta's Gyros drive through and back.

Parameters - Capture an image every 15 seconds and see how it looks

Example Project

There are a lot of interval timers available for CHDK we'll just use the lua one we showed earlier.

So we'll load the script, set the timer parameter and away it goes.

So after that I have a bunch of pictures which I'll convert with the convert program from ImageMagick into a movie to show now.

Example Project

Let’s watch the movie :-)

Couple of Caveats with Scripting

It is running 100% on your camera meaning no sleep, cpu is going pretty hard all the time. Scripting will take a lot out of your battery if you run it for a long time.

There are tricks to help with this. E.g. if you have video out, put an empty cable in so the screen will blank.

Put a null-battery pack in there etc...

Some cool projects are available for this. Lightning, Motion Detection, Meteor, etc...

How does it get ported to Cameras?

First off have to get the firmware off the camera.

Several approaches to this are used

- Canon Basic Script - script that dumps the firmware currently used system
- WIF loader - uses the firmware updater to save a copy of the firmware, is interesting as you have to pass all the tests
- The hard way - not used in years, but deserves mention

The Hard Way

The Hard Way

Hook up a phototransistor to your sound card and write a bit of software to blink out the firmware using the status led on the camera.

You of course have to write a simple protocol and wait for it to finish.

It is obvious why this isn't the first choice anymore. Still incredibly clever and you can learn a lot about how the system works based on this.

Porting after Firmware dump

After you have a firmware dump you'll want to compare its code to other cameras/firmwares that have been dumped.

This used to be done with IDA pro but is being done with Ghidra in newer versions. IDA pro and Ghidra are both disassemblers able to do comparisons between similar binaries and highlight the differences.

After that is hopefully comparing code, writing some basic changes and testing, testing, testing...

Pinhole Photography

Pinhole Photography is one of the earliest forms of photography. You don't have a lens or anything optical. You put a simple pinhole on end of an oatmeal can and have photographic film on the other. The exposures typically have to be in the range of several seconds.

The ability to override the duration for a photograph opens up the option for playing with this old kind of photography in the modern day.

Provided your camera has a lens that lets you put a lens cap on it with a pinhole.

Astronomical Photography

The ability to override camera options makes CHDK an interesting piece of software for people interested in Astronomical Photography.

If you go with the motion detection software and use it during a meteor shower you can get some pretty interesting results.

Why this is interesting to me?

- CHDK has been around for years. I did a talk on it at OLUG over 10 years ago.
- It supports multiple camera models and firmwares
- It is all under the GPL v2 license
- Has an autobuild system
- Way new cameras/firmware is added is interesting
- Was written to “stick it to the man”
- Fills a real need

Other Firmwares

CHDK is just one example firmware that is available for your camera. There are several more. For some other manufacturers there are also alternative firmwares, but I haven't done any real research on them.

Some of these alternative Canon firmwares such as Spy Lantern a surveillance system are simple mods of CHDK, others do a lot more

We'll just mention a few of them.

SDM - Stereo Data Maker

SDM is a relative of CHDK that uses 2 or more Canon cameras to do 3-d photography. It syncs shots between the cameras with a custom cable.

Popular for some things like 3d high altitude ballooning and kite flights.

Doesn't support as many cameras/firmwares as does CHDK, but is a very cool project in its own right.

Another example is any movie that does bullet time. You'd need a lot of cameras but you can do it with CHDK or SDM.

400 Plus

Custom firmware for Canon 400d cameras.
Non-destructive.

Adds a lot of capabilities to this camera such as

- Custom white balance
- Change the ISO dynamically
- Spot metering mode
- Fixed exposure for M Models
- Lot of other things
- Goal is to do similar functionality to Magic Lantern on DryOS cameras

Magic Lantern

Supports higher end EOS cameras mostly

Designed more for video than still photography

- HDR Video
- Audio stuff such as on-screen audio meter
- Focus Peaking???
- 14-bit raw video on certain DSLRs
- Other stuff I also didn't understand

Tips to Increase your Success

5 Tips to Increase Your Success

1. Print out the CHDK user guide - it is only 10 pages
2. Read the CHDK user guide
3. Use a quality SD card
4. Used ACID & ASSIST at first to get SD card setup
5. Don't be afraid to give it a spin, just flip the SD card to read/write and restart the camera and you should be back to the stock firmware

Summary

If you've got a Canon camera that is supported it is amazing how many new features that CHDK can add to it for you.

If you don't you can pick up a Canon camera that is supported very cheaply on Ebay, Amazon or Craigslist.

I paid $40 for my Canon AS4000 on craigslist. Hint look for people spelling "Cannon" instead of "Canon"

Thanks & Q/A

Thank you all for listening.

Questions???

Links

CHDK - Wiki

https://chdk.fandom.com/wiki/CHDK

ACID - Automatic Camera Identifier

http://www.zenoshrdlu.com/acid/acid.html

STICK - Simple Tool for Installing ChdK

http://zenoshrdlu.com/stick/stick.html

Links

CHDK - PTP (Picture Transfer Protocol)

https://app.assembla.com/wiki/show/chdkptp

SDM Home Page

http://sdm.camera/index.htm

400Plus Firmware

https://github.com/400plus/400plus

Links

Magic Lantern Firmware

https://magiclantern.fm/

Rockbox - alternative firmware for mp3 players

https://www.rockbox.org/

DDWRT - alternative firmware for your router

https://dd-wrt.com/