

# Cygnos 360 Manual

Team Cygnos

Version 0.1  
(Preliminary)



# Contents

- 1 Introduction 4**
- 2 Preparations 6**
  - 2.1 Required Skills, Tools, and Materials . . . . . 6
  - 2.2 Lifting up the CE-Pin . . . . . 7
  - 2.3 Disabling eFuses Power Supply . . . . . 9
- 3 Installation 12**
  - 3.1 Installing Cygnos 360 . . . . . 12
  - 3.2 Installing Infectus with Cygnos 360 . . . . . 14
- 4 Basic Operations 15**
  - 4.1 Reading Xbox 360 NAND-Flash Memory . . . . . 15
  - 4.2 Writing Cygnos 360 NAND-Flash Memory . . . . . 17
- 5 Advanced Operations 20**

# 1 Introduction

Thank you for choosing Cygnos 360! Cygnos 360 is the first commercially available add-on for the Microsoft Xbox 360, that allows you to easily switch between two different NAND-flash memories.

In the Xbox 360, on-board NAND-flash memory stores important data like the hypervisor, kernel, and key vault. Through installation of Cygnos 360, the on-board NAND-flash memory is complemented with another NAND-flash memory contained on the Cygnos 360 printed-circuit board.

Being able to choose between both NAND-flash memories opens up a variety of new fascinating possibilities. The following list tries to give you an impression about what can be done with Cygnos 360:

- choose between the newest kernel for playing games or a vulnerable kernel for running Linux
- play imported games or movies by switching your region code

Please note that some of the possible uses of Cygnos 360 require you to know your Xbox 360 CPU key. At the moment, this key can only be extracted by booting a vulnerable kernel, such

as version 4532 or 4548. If your current kernel version is newer than 4548, you will have to downgrade, which is up to date only possible with the Xbox 360 Zephyr and Falcon models. A kernel version older than 4532 does not pose a problem, since it can be upgraded to either version 4532 or 4548. Downgrading the Xbox 360 as well as programming Cygnos 360 assumes the temporary installation of an Infectus 1 or 2 mod-chip.

Before Cygnos 360 can be installed to your Xbox 360, a few preparations need to be made, which are described in chapter 2. Chapter 3 details the installation process of Cygnos 360 and the Infectus mod-chip. In chapter 4, you will learn basic operations with your newly installed Cygnos 360, like reading and writing to its NAND-flash memory. Chapter 5 concludes with advanced topics, such as downgrading your Xbox 360 and modifying certain contents of the key vault.

## 2 Preparations

### 2.1 Required Skills, Tools, and Materials

During the development of Cygnos 360, we put great effort into making the installation of our product as quick and straightforward as possible. Yet, a fair amount of soldering skill is still required for a successful installation. We therefore do not recommend this procedure to customers who are new to soldering. Contrary, customers able to solder surface mount parts should not experience any troubles at all.

Like any printed-circuit board, the Xbox 360 mainboard is sensitive to high temperatures during soldering. In order to reduce the risk of damage to the mainboard, like lifted up tracks or pads, a temperature controlled soldering iron should be used.

For optimal results in hand-soldering Cygnos 360, use a thin leaded solder wire with flux core. The risk of bad solder joints is further reduced by using an eutectic solder wire (Sn63Pb37), as it goes directly from liquid to solid state when cooling down. In contrast, non-eutectic solder wire (e.g. Sn60Pb40) has a pasty stage in which movement of either the part or the wire may lead to a bad solder joint.

If a solder bridge builds up during soldering, it should preferably be removed using a desoldering iron or a desoldering pump. A desoldering braid can also be used, as long as it is only pushed down gently on the solder bridge. Using too much force can easily cause damage the printed-circuit board.

Installing Cygnos 360 requires a couple of wires to be soldered to the Xbox 360 mainboard, the toggle switch, and the Infectus mod-chip. For this task, we recommend a non-stranded AWG 28 wire insulated with Teflon or Kynar.

To sum it up, this is what you will need:

- soldering iron with a fine tip, preferably temperature controlled
- thin solder wire with flux core, use an Sn63Pb37 alloy for reduced risks of bad solder joints
- either a desoldering iron, desoldering pump or desoldering braid for removing solder bridges
- insulated wire, optimally non-stranded AWG 28 wire coated with Teflon or Kynar

## 2.2 Lifting up the CE-Pin

Lifting up the CE-pin of the on-board NAND-flash chip is the first preparation that has to be done before Cygnos 360 can be installed. Figure 2.1 shows the on-board NAND-flash chip, a HY27US08281A series 128MBit NAND-flash in a 48-pin TSOP

package manufactured by Hynix.

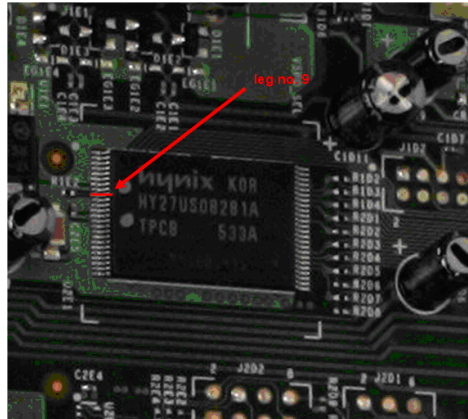


Figure 2.1: This picture shows the Xbox 360 on-board NAND-flash chip with the CE-pin, pin number 9, marked in red.

Pin number 9 is marked in red as it carries the NAND-flash's CE-signal (*chip enable*). This pin has to be lifted up from its corresponding pad because Cygnos 360 needs to control when the on-board NAND-flash is enabled. In the Xbox 360, the CE-signal is normally driven by the south-bridge. Leaving this pin connected to the pad would require Cygnos 360 to drive the signal against the south-bridge's output transistor. The risk of ultimately damaging this transistor due to excessive heat build-up and thus destroying the whole console was unacceptable for us. We therefore took the technically superior way of lifting up the CE-pin.



In order to lift up the CE-pin, we recommend to heat up the pad with a soldering iron until the solder is melted. When the solder is melted, use a needle and bend up the pin carefully. After you have finished, there should be a gap between the pin and the pad large enough so that intermittent contacts between both may not happen. Please try not to bend the pin several times as this may cause the pin to break at the location where it enters the package's body.

The result should look similar to figure 2.2.

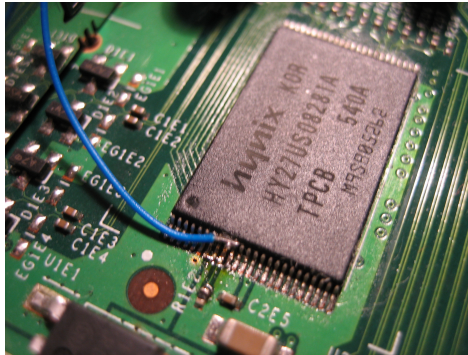


Figure 2.2: A picture of the on-board NAND-flash chip with its CE-pin lifted up and a wire soldered to it.

## 2.3 Disabling eFuses Power Supply

Please note that the information and recommendations given in this section possibly have to be changed with the release of the

next dashboard update, commonly referred to as NXE (*new Xbox experience*).

Disabling the eFuses power supply is suggested if you install Cygnos 360 into an Xbox 360 that will undergo a downgrade process or that will once be updated with a newer dashboard that blows an eFuse during the update process.

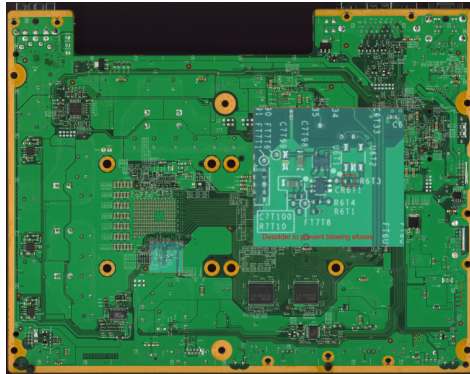


Figure 2.3: In this picture, the location of resistor R6T3 is shown which is feeding power to the eFuses inside Xbox 360's Xenon processor.

Blowing eFuses is used by certain dashboard updates as a means to prevent older kernels from running on this Xbox 360. In order to be able to switch between the on-board NAND-flash and Cygnos 360 after such a dashboard update has been applied, it is necessary to disable the eFuses power supply beforehand. Power to the eFuses inside the Xenon processor is fed through resistor R6T3 which is shown in figure 2.3. Removing this resistor will

cut the power supply to the eFuses.

Resistor R6T3 is most conveniently desoldered with a tweezer handpiece of a soldering station. If that tool is not available to you, you can also use a soldering iron. In this case, try to cover both ends of the resistor at the same time with one solder bubble. Continuously heat the bubble with your soldering iron until the resistor comes off. After the resistor has been desoldered, remove any residual solder from the motherboard and the resistor. Keep the resistor for a possible reinstallation later on.

## 3 Installation

### 3.1 Installing Cygnos 360

Installation of Cygnos 360 is a quick and easy task. Cygnos 360 is installed to the underside of the Xbox 360 motherboard. The exact location is shown in figure 3.1.

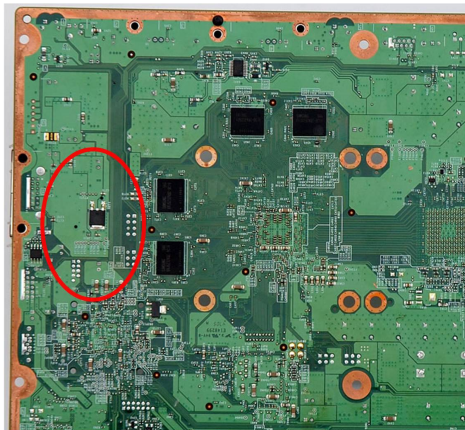


Figure 3.1: A picture of the underside of an Xbox 360 motherboard. The location where Cygnos 360 is to be installed is marked with a red circle.

Cygnos 360 is supposed to be directly soldered to the Xbox 360

motherboard. Therefore, we equipped Cygnos 360 with so-called *quick-solder pads*. Cygnos 360 has a total of 17 quick-solder pads as shown in figure 3.2. In order to install Cygnos 360, lay it on top of the motherboard, align the quick-solder pads with the vias and pins shown in figure 3.1 and solder each quick-solder pad to its corresponding via or pin. The via corresponding to the quick-solder pad at the lower left corner of Cygnos 360 is usually covered by lacquer. Soldering is thus not immediately possible. There are two possibilities in this case. Either the lacquer is removed carefully with e.g. a scalpel or a different soldering point is used as shown in figure 3.2.

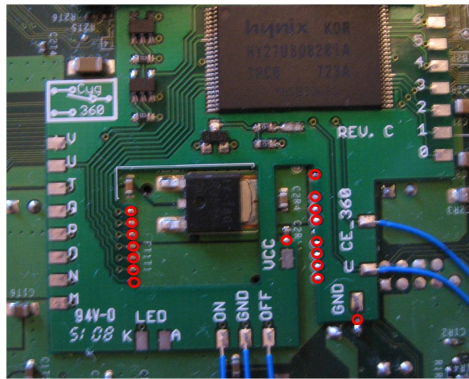


Figure 3.2: This picture shows a Cygnos 360 already installed to the underside of the Xbox 360 motherboard. Quick-solder pads are marked with red circles.

## **3.2 Installing Infectus with Cygnos 360**

The Infectus mod-chip 1/2 can be installed in addition to an already installed Cygnos 360. In this case, the installation procedure for the Infectus mod-chip remains largely the same, the only difference being that the wires for the soldering points M, N, O, P, Q, T, U, V, and, 0 - 7 are no longer directly soldered to the Xbox 360 motherboard as these points are already occupied by Cygnos 360. Instead, these wires are soldered to accordingly labeled pads on Cygnos 360 now.

Installation of the Infectus mod-chip 1/2 is not covered in this manual. Please refer to the official installation instructions and diagrams found at <http://www.infectus.biz/>.

## 4 Basic Operations

Now that the installation of Cygnos 360 and the Infectus mod-chip 1/2 is finished, we will show you the first basic steps. The procedures described in this chapter will also act as building blocks for the advanced topics in the following chapter.

### 4.1 Reading Xbox 360 NAND-Flash Memory

In order to read the Xbox 360's on-board flash memory, you have to flip the switch to the *OFF* position, disabling Cygnos 360. Next, plug in the power cord and connect the Infectus mod-chip to the USB cable. Please follow this sequence exactly!

Launch the Infectus programmer software. Figure 4.1 shows the applications main window. If the installation of Cygnos 360 and the Infectus mod-chip went correctly, the Infectus mod-chip will be recognized and the device and manufacturer ID of the on-board NAND-flash chip will be displayed at the bottom of the main window.

If there is any fault, the Infectus programmer software will show all the items in the *Flash Commands* menu grayed out, indicating

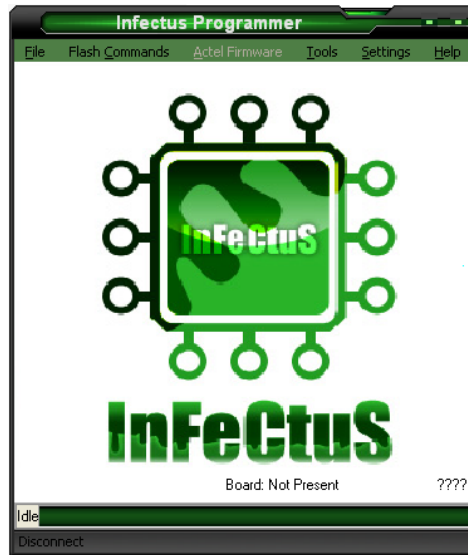


Figure 4.1: A picture of the Infectus programmer software main window.

they are not available at the moment.

In order to dump the contents of your on-board NAND-flash chip, select *Flash Commands* → *Read* from the menu and point the file save dialog that will pop up to a file, where the dump should be saved to. Reading the NAND-flash chip will take several minutes. The progress is displayed in the main window's status bar.



## 4.2 Writing Cygnos 360 NAND-Flash Memory

Cygnos 360 may not be directly programmed with a dump of the Xbox 360 on-board NAND-flash. The reason for this lies within the defect blocks both NAND-flashes may contain and which are very unlikely to be at the same places. Writing an on-board NAND-flash dump to Cygnos 360 would unrecoverably destroy its bad block information and probably store data in bad blocks. On the next boot-up, data corruption will be detected and an error message shown on screen.

Before Cygnos 360 can be programmed for the first time, a dump of the empty Cygnos 360 NAND-flash needs to be made. This dump will contain the bad block information needed for the following programming step. For generating the dump, flip the switch to the *ON* position and otherwise follow the steps in section 4.1. Please note that, as long as the Cygnos 360 NAND-Flash Memory is not programmed with a valid image, the box may not be connected to the power cord with the switch in the *ON* position! The reason for this lies within the Xbox 360's behaviour to read the code for the System Management Controller from the NAND-Flash memory as soon as stand-by power is available. Thus, reading from and writing to an empty Cygnos 360 NAND-Flash memory is only possible if the switch is flipped to the *ON* position after it has been connected to the power cord with the switch in the *OFF* position.

When the reading of the empty Cygnos 360 NAND-flash has finished, an image can be generated for programming into Cygnos

360. For this purpose, we wrote a tool called *NAND-Flash Tool* that can be downloaded from our website at <http://www.cygnos360.com/>. This tool will take care, that no data will be stored in bad blocks of Cygnos 360's NAND-flash. When you launch NAND-Flash Tool, you will be presented with a window as shown in figure 4.2.



Figure 4.2: A picture of Odirrus, Ltd. NAND-Flash Tool's main window.

In order to generate the programming image for Cygnos 360, enter the path to the NAND-flash image you would like to program into the first input line or use the button next to it to point to the image through a file dialog. The second input line is used accordingly to choose the image file of the empty Cygnos 360 NAND-flash.

Once both images have been selected, the *Generate* button can be pushed and an image suitable for programming into Cygnos 360 will be generated. When the process is complete, a file dia-

log will prompt you to enter the location where the newly created image should be saved.

Close the NAND-Flash Tool now and open the Infectus programmer software. Select *Flash Commands* → *Erase* to prepare the Cygnos 360 NAND-flash for reprogramming. Afterwards, Select *Flash Commands* → *Write* and choose the image file you generated in the previous step. Writing will commence now. If you experience a write error during programming, deselct *Write Verify* from the *Settings* menu and repeat the erase and write operations.

## **5 Advanced Operations**

Coming soon ...