The Application Of Reverse Engineering Techniques Against The Arduino Microcontroller To Acquire Uploaded Applications

By

Steve Watson

Presented At

The Digital Forensic Research Conference

DFRWS 2014 USA Denver, CO (Aug 3rd - 6th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

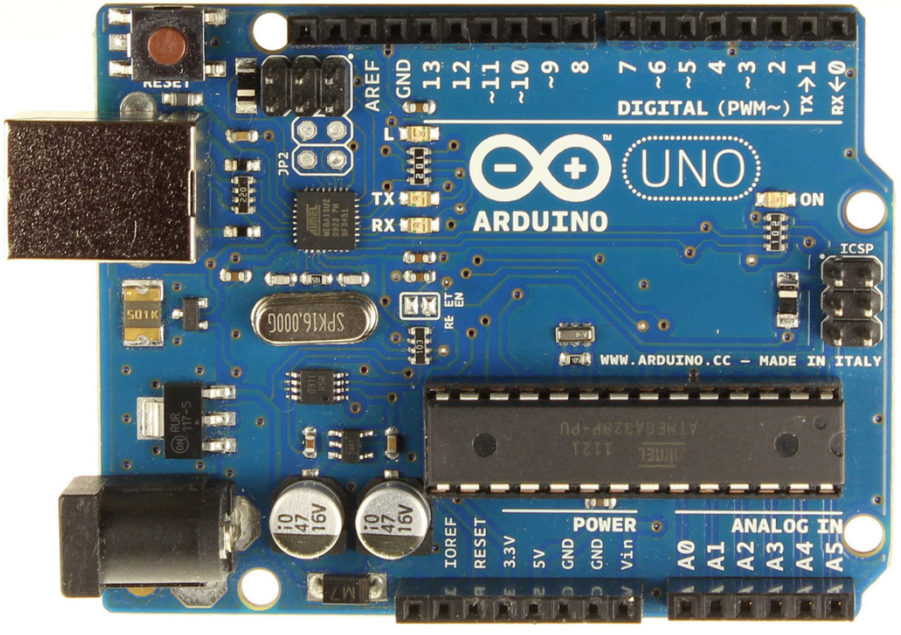
http:/dfrws.org

Disclaimer

The opinions expressed and materials shared in this presentation are my own and may not reflect the opinions, policies, or procedures of my employer.

What is Arduino?

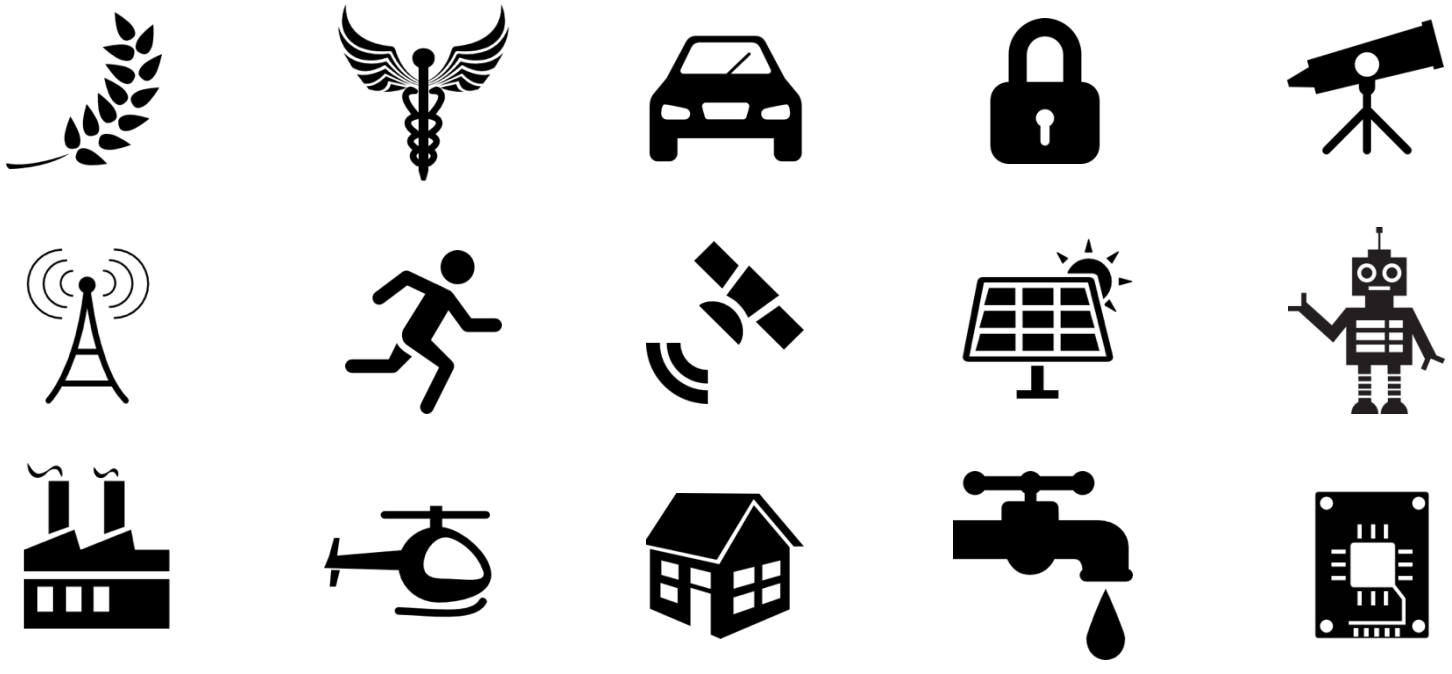
- A single board microcontroller platform.
- An open source electronics platform.

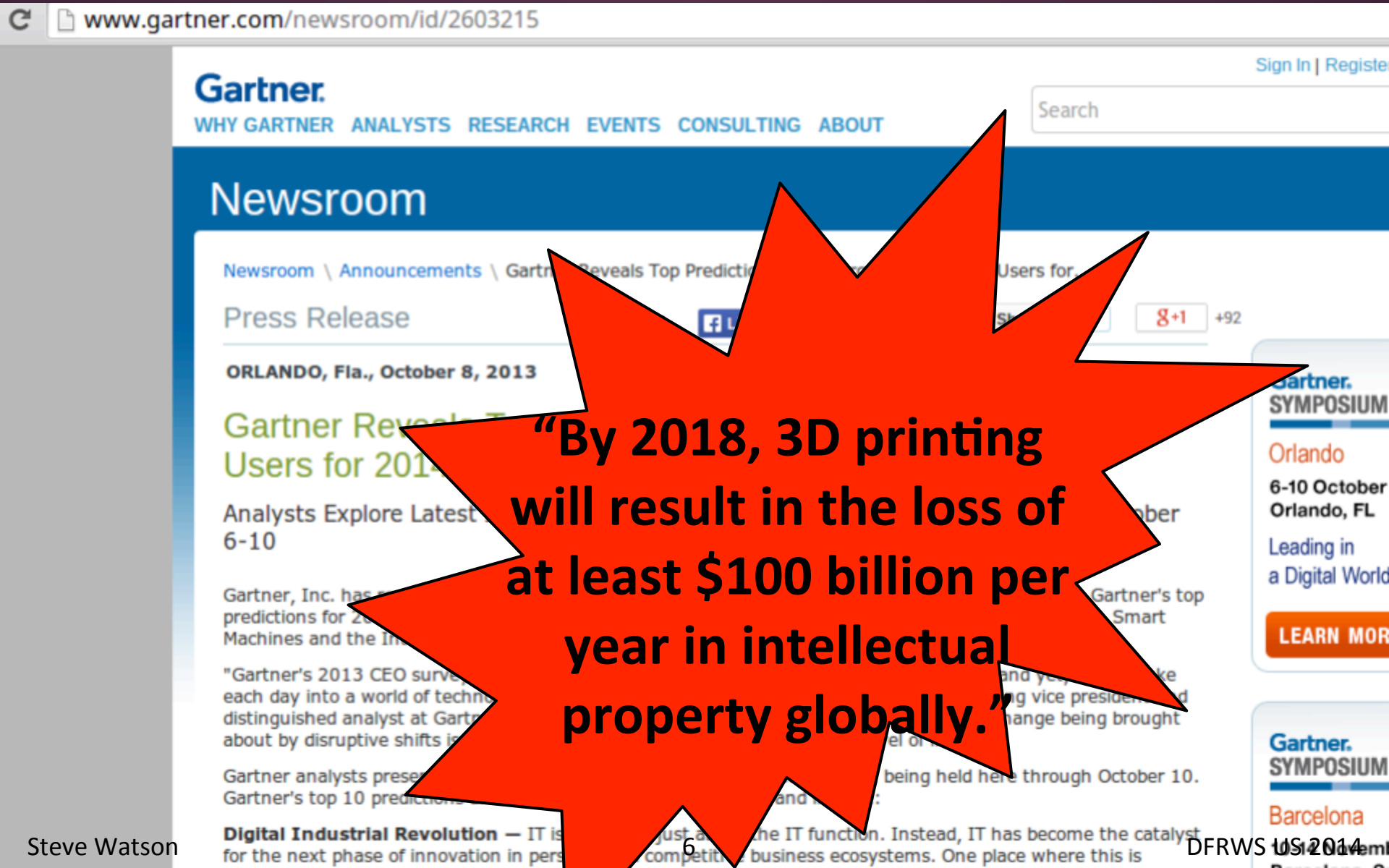


Why are we talking about Arduino?

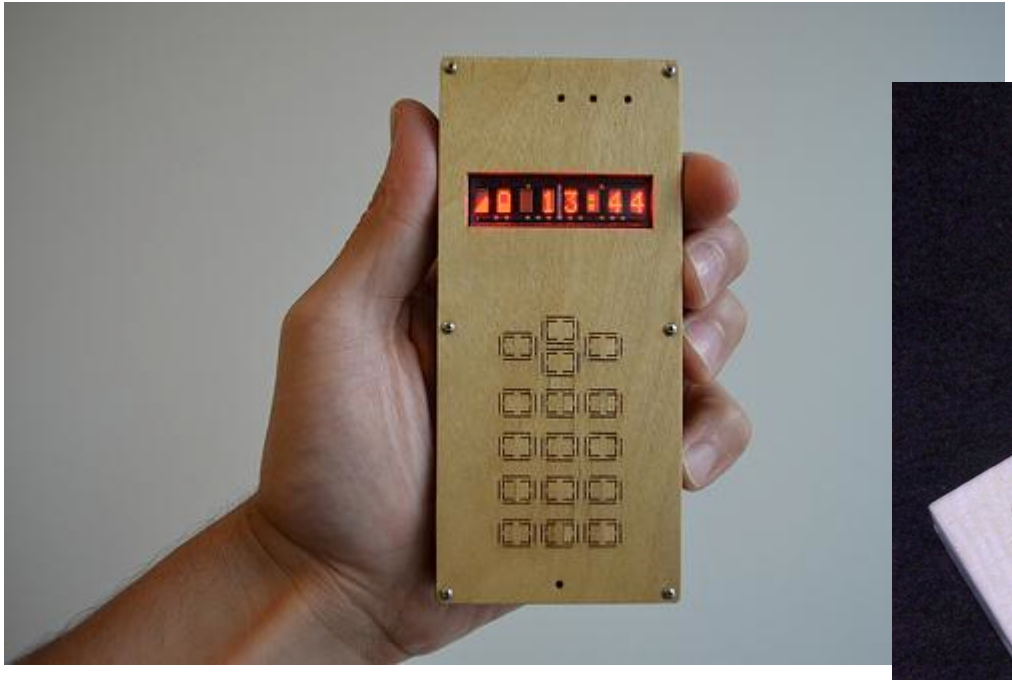
- New, foundational technology appearing in many different form factors.
- No clear direction on forensic acquisition of data on this evolving platform.

Where is Arduino today?




www.gartner.com/newsroom/id/2603215
Gartner
WHY GARTNER ANALYSTS RESEARCH EVENTS CONSULTING ABOUT
Sign In | Registe
Search
Newsroom
Newsroom \ Announcements \ Gartn Reveals Top Predictio Users for
Press Release
+92
ORLANDO, Fla., October 8, 2013
Gartner Reve Users for 201
Analysts Explore Latest ber
6-10
Gartner, Inc. has predictions for 2 Gartner's top Smart Machines and the In
"Gartner's 2013 CEO surve ke each day into a world of techn g vice presiden distinguished analyst at Gartn hange being brought about by disruptive shifts is el of
Gartner analysts prese being held here through October 10. Gartner's top 10 predictions and
Digital Industrial Revolution — IT is just a the IT function. Instead, IT has become the catalyst for the next phase of innovation in pers competitive business ecosystems. One place where this is
Gartner. SYMPOSIUM Orlando 6-10 October Orlando, FL Leading in a Digital World LEARN MOR
Gartner. SYMPOSIUM Barcelona
“By 2018, 3D printing will result in the loss of at least $100 billion per year in intellectual property globally.”

Example - Arduino Phone



http://blog.arduino.cc/2013/08/12/diy-cellphone/

http://www.instructables.com/id/ArduinoPhone/

Examples - ArduSat

Buy Download Products Learning Reference Support

KICKSTARTE

ARDUSAT SUCCESSFULLY LAUNCHED IN SPACE – WATCH VIDEO!

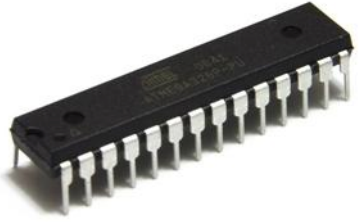
Zoe Romano — August 12th, 2013

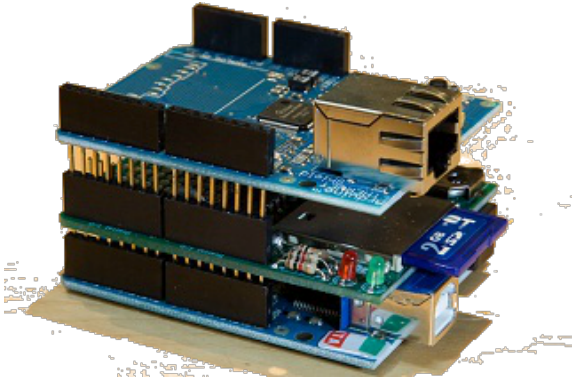
Exploration

0

ArduSat was successfully launched in space last Sunday 4th August and it's now

Arduino Basics

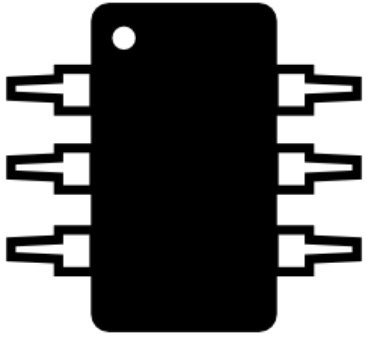




microcontroller	CPU, RAM and ROM on a single chip.
shield	daughter card that sits on top of the Arduino
sketch	the code or application written in C++ that is uploaded to the Arduino

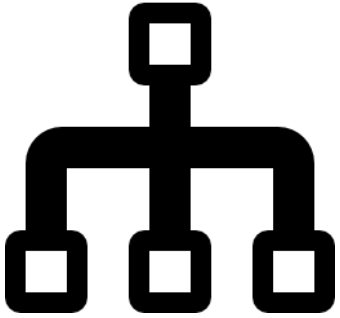
Is there data to recover?

Where is the data?



Microcontroller

Development Systems



Remote Endpoints

What is the data?

Microcontroller	Development Systems	Remote Endpoints
running applications (flash)	.ino (Arduino sketch)	cloud computing updates (Twitter, Facebook, IoT pages)
NVM, persistent (eeprom)	.elf (intermediate step between c++ and assembly)	control messages (c&c of other microcontroller devices)
.csv, .txt (asci or hex on SDCARD)	.hex (assembly)	.txt, .csv
Fuses (single byte hex values)		.json (JSON calls to other applications)

How I approach new devices

1. What is the operating system?
2. What is the storage?
3. What is the connectivity?
4. How is the system updated, installed, accessed?
5. What are the parallels with other systems and devices?
6. What existing documentation and information exists?

Focus on the Arduino

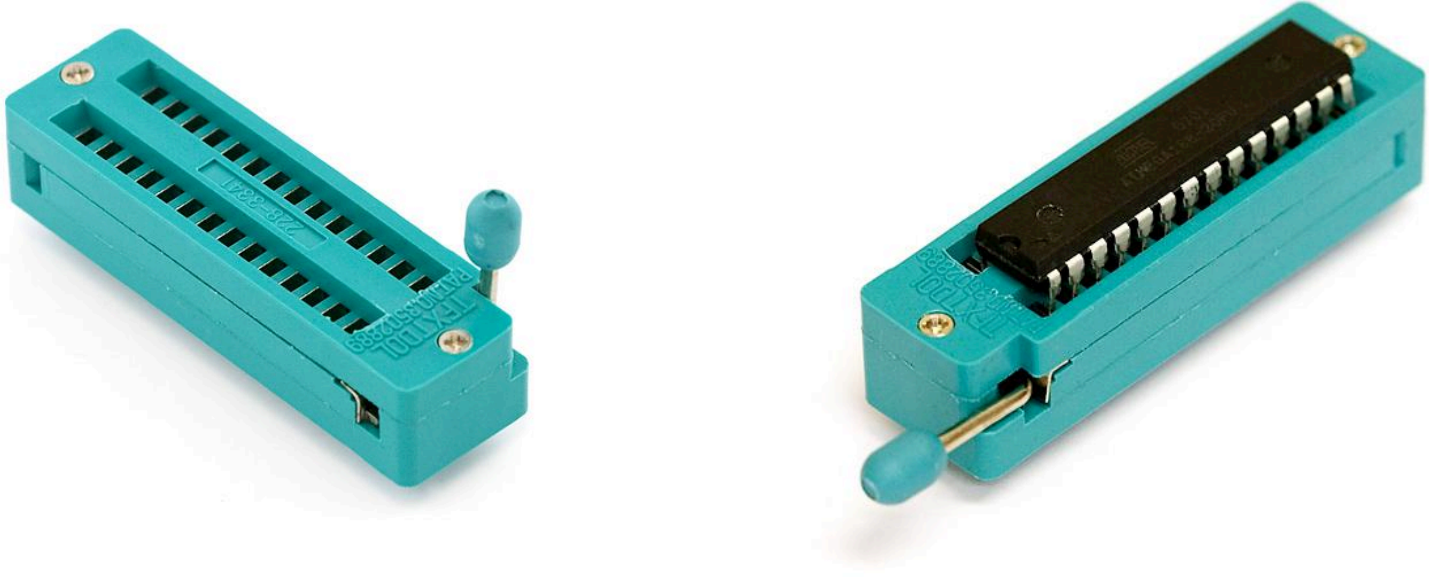
Connection to the target

1. Chip removal (chip-off equivalent)

2. Tethered to another Arduino (computer to computer equivalent)

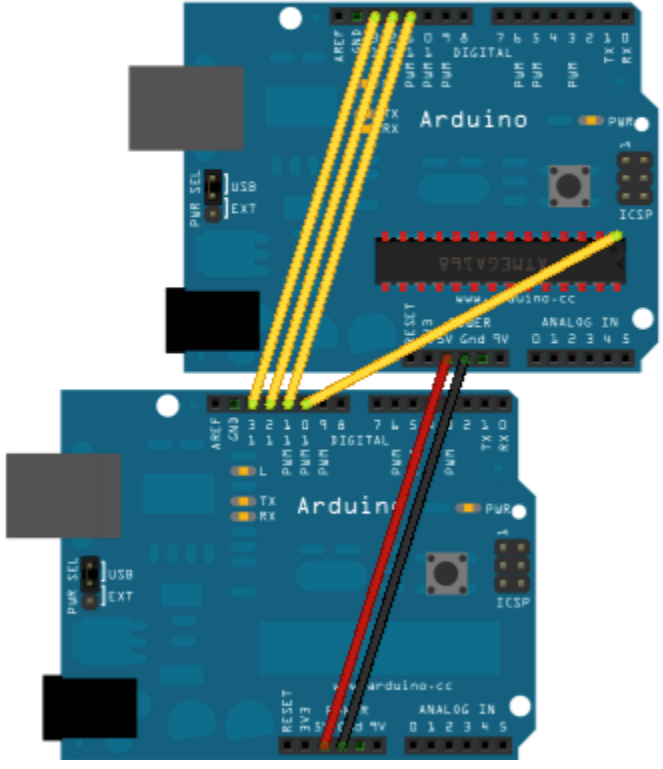
3. Connect to a programming port on the board (JTAG equivalent)

Connection: Chip-off



Example: ZIF Socket 28-Pin, https://www.sparkfun.com/products/9175

Connection: Tethered Arduino

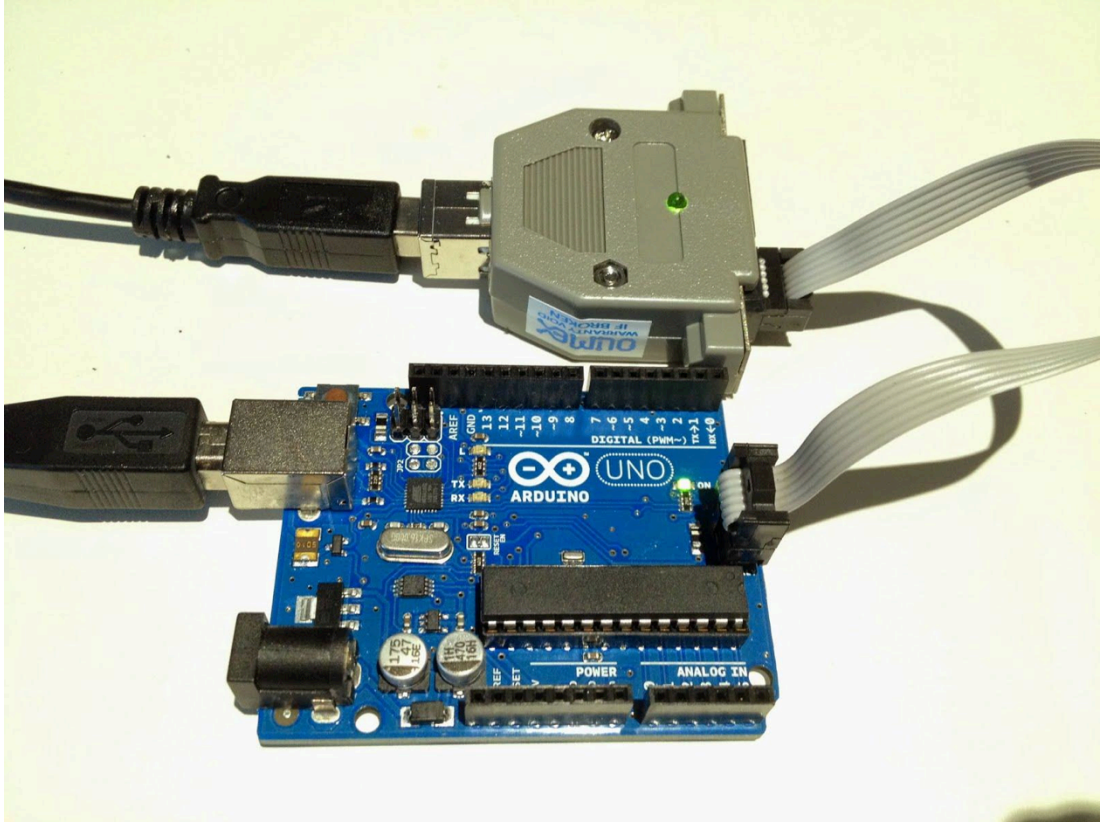


Arduino Tutorial:

Using an Arduino as an AVR ISP (In-System Programmer)

http://arduino.cc/en/Tutorial/ArduinoISP

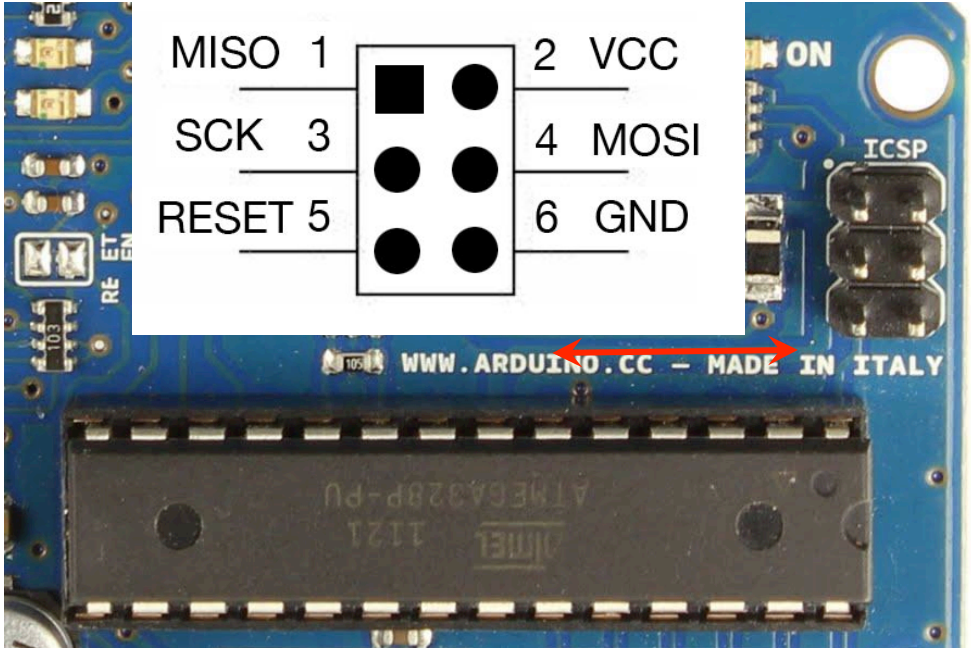
Connection: JTAG Equivalent

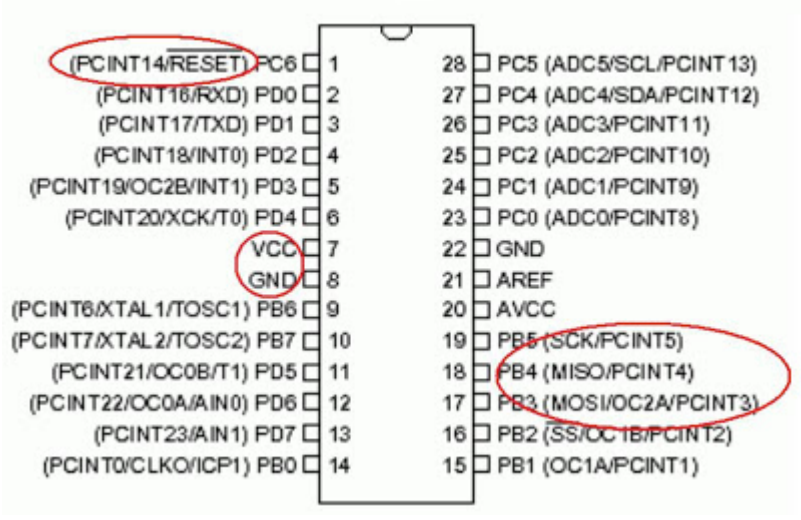


Olimex STK500v2
connected via ICSP to an
Arduino UNO

Connection: ICSP

ICSP - In-Circuit Serial Programming





Software used to acquire

1. AVRDUDE - AVR Downloader/UploaDEr
    a. opensource
    b. http://www.nongnu.org/avrdude/
    c. Included in the Arduino IDE install under install directory ../Arduino/hardware/tools/avr/bin/ avrdude.exe
2. Atmel AVR Studio

Data to acquire

Flash (32KB)

EEPROM (1KB)

- NVM reserved for persistence across uploads

Fuses (1B x 3 reserved)

- lfuse, hfuse, efuse
- single byte hex configurations related to clock, bootloader and voltage (see reference slide for more detail)

Software: AVRDUDE

Example: Read flash memory and dump hex to specific file.

avrdude -p m328p -c stk500v2 -P com4 -U flash:r:"[path/to/file/filename.hex]":r

-p [part number]
-c [programmer]
-P [com port]
-U [memory operation]

- Note the :r: and :r to define READ
- change ‘flash’ to eeprom, lfuse, hfuse and/or efuse to acquire reserved portions.

Software: AVRDUDE

```
C:\apps\avrdude -p m328p -c stk500v2 -P com4 -U flash:r:"c:/temp/arduino_uno.hex":r


avrdude: AVR device initialized and ready to accept instructions

Reading | ################################################## | 100% 0.03s

avrdude: Device signature = 0x1e950f

avrdude: reading flash memory:

Reading | ################################################## | 100% 94.89s

avrdude: writing output file "c:/temp/arduino_uno.hex"

avrdude: safemode: Fuses OK (E:05, H:D6, L:FF)

avrdude done.  Thank you.
```

Software: Atmel Studio

Full walkthrough (screenshots) of an MCU acquisition in the backup slides.

Investigations where data may be needed

1. Supply chain investigations
2. Malware analysis
3. Improvised devices
4. Automation and control systems
5. Medical, fitness
6. Security, access control
7. Drones
8. Cloud

Why does this matter?

1. Investigations and litigation are coming to this new technology area.

2. The principles applied here can be expanded to other embedded technologies.

Thank you!

Steve Watson
forensics@stevewatson.net
steve.watson@intel.com
Twitter @stevewatson
LinkedIn - watsonsteve

Backup Material

Credits

title slide - Arduino schematic, http://arduino.cc/en/uploads/Main/arduino-uno-schematic.pdf
slide 3 - Arduino UNO photo, http://arduino.cc/en/uploads/Main/ArduinoUno_R3_Front.jpg
slide 5 - Icons made by www.flaticon.com
slide 6 - Image http://upload.wikimedia.org/wikipedia/commons/8/87/Makerbot_Thing-O-Matic_Assembled_Printing_Blue_Rabbit.jpg
http://www.gartner.com/newsroom/id/2603215
slide 7 - http://blog.arduino.cc/2013/08/12/diy-cellphone/, http://farm6.staticflickr.com/5475/9474701418_798e142291.jpg,
http://www.instructables.com/id/ArduinoPhone/
slide 8 - Screenshots and images in order of animation:
https://www.kickstarter.com/projects/575960623/ardusat-your-arduino-experiment-in-space,
http://www.blogcdn.com/www.engadget.com/media/2012/06/ardustat8388676666666.jpg
slide 11 - Icons made by www.flaticon.com
slide 16 - Example: ZIF Socket 28-Pin, https://www.sparkfun.com/products/9175
slide 17 - image created with Fritzing
slide 19 - monochrome images http://allaboutee.com/2011/05/11/how-to-program-an-avr-microcontroller/

Reference - Fuses

lfuse hfuse

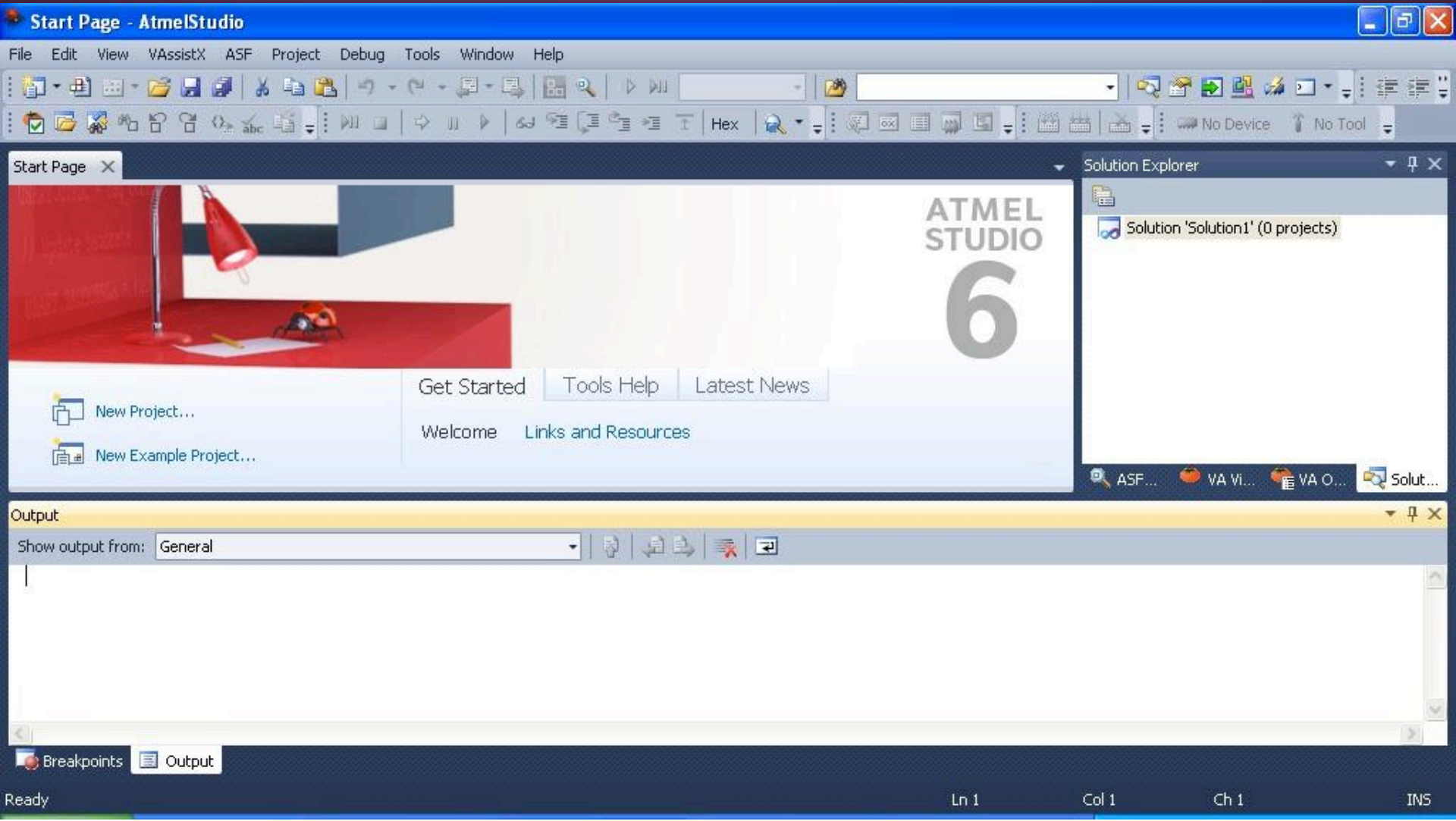
Bit	Low	High	efuse	Extended
7	☑ **CKDIV8** Divide clock by 8	☐ **RSTDISBL** External reset disable		
6	☐ **CKOUT** Clock output	☐ **DWEN** debugWIRE Enable		
5	☐ **SUT1** Select start-up time	☑ **SPIEN** Enable Serial programming and Data Downloading		
4	☑ **SUT0** Select start-up time	☐ **WDTON** Watchdog Timer Always On		
3	☑ **CKSEL3** Select Clock Source	☐ **EESAVE** EEPROM memory is preserved through chip erase		
2	☑ **CKSEL2** Select Clock Source	☑ **BOOTSZ1** Select boot size		☐ **BODLEVEL2** Brown-out Detector trigger level
1	☐ **CKSEL1** Select Clock Source	☑ **BOOTSZ0** Select boot size		☐ **BODLEVEL1** Brown-out Detector trigger level
0	☑ **CKSEL0** Select Clock Source	☐ **BOOTRST** Select reset vector		☐ **BODLEVEL0** Brown-out Detector trigger level

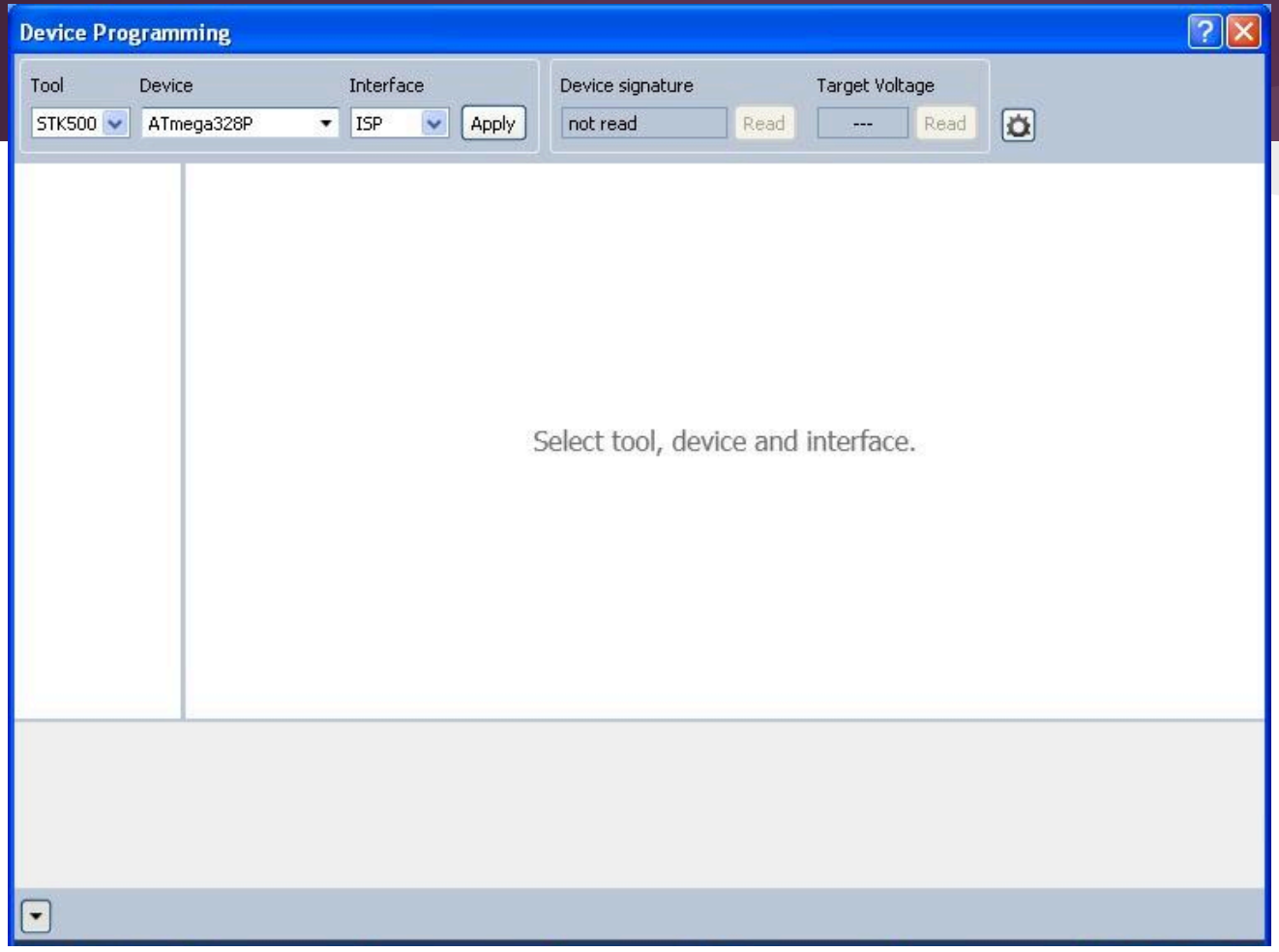
http://www.engbedded.com/fusecalc/

AVR Acquisition with Atmel Studio

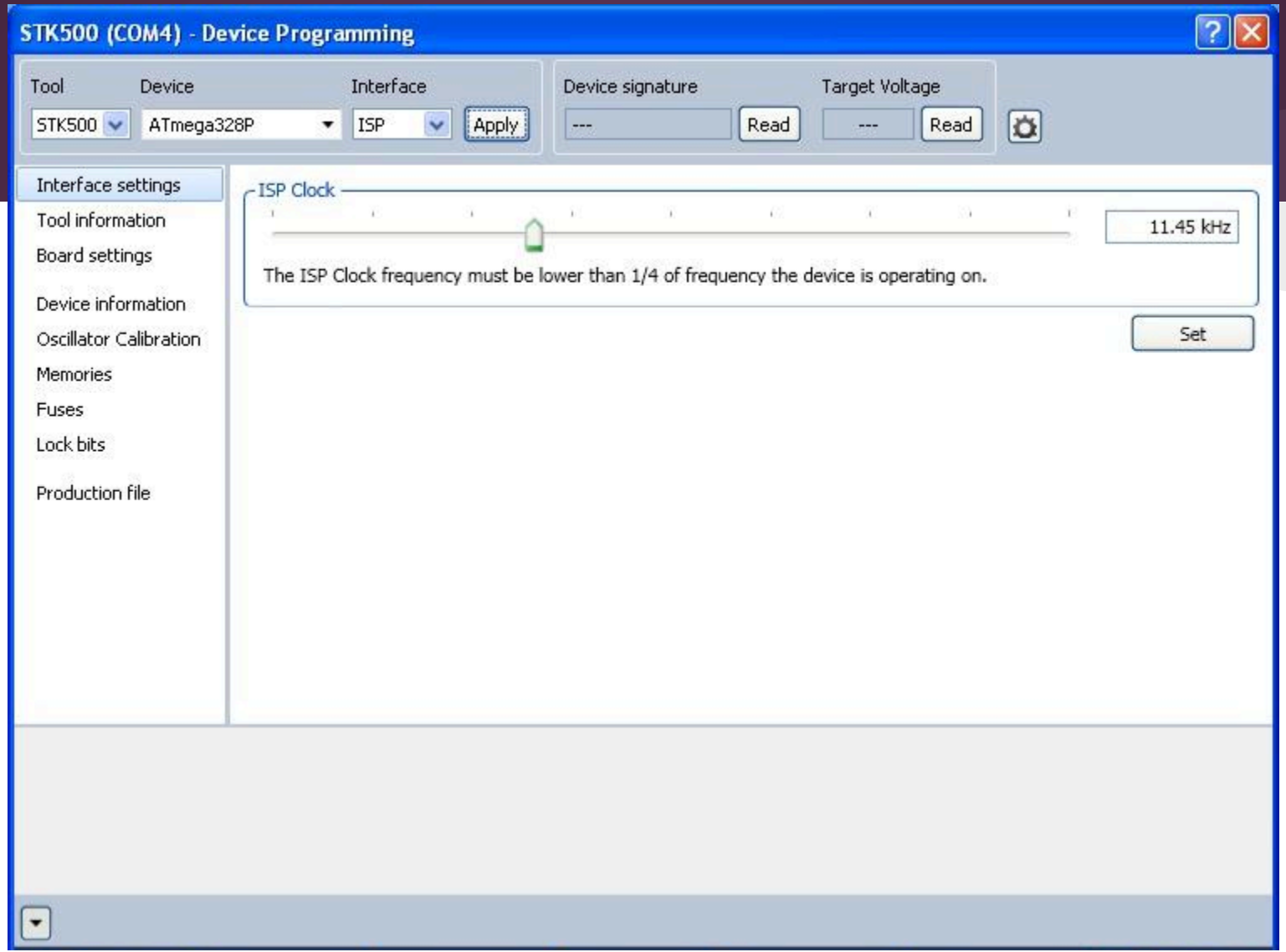
Begin

Software: Atmel Studio


Start Page - AtmelStudio
File Edit View VAssistX ASF Project Debug Tools Window Help
Hex
No Device
No Tool
Start Page
ATMEL STUDIO 6
Get Started
Tools Help
Latest News
New Project...
New Example Project...
Welcome
Links and Resources
Solution Explorer
Solution 'Solution1' (0 projects)
ASF...
VA Vi...
VA O...
Solut...
Output
Show output from: General
Breakpoints
Output
Ready
Ln 1
Col 1
Ch 1
INS

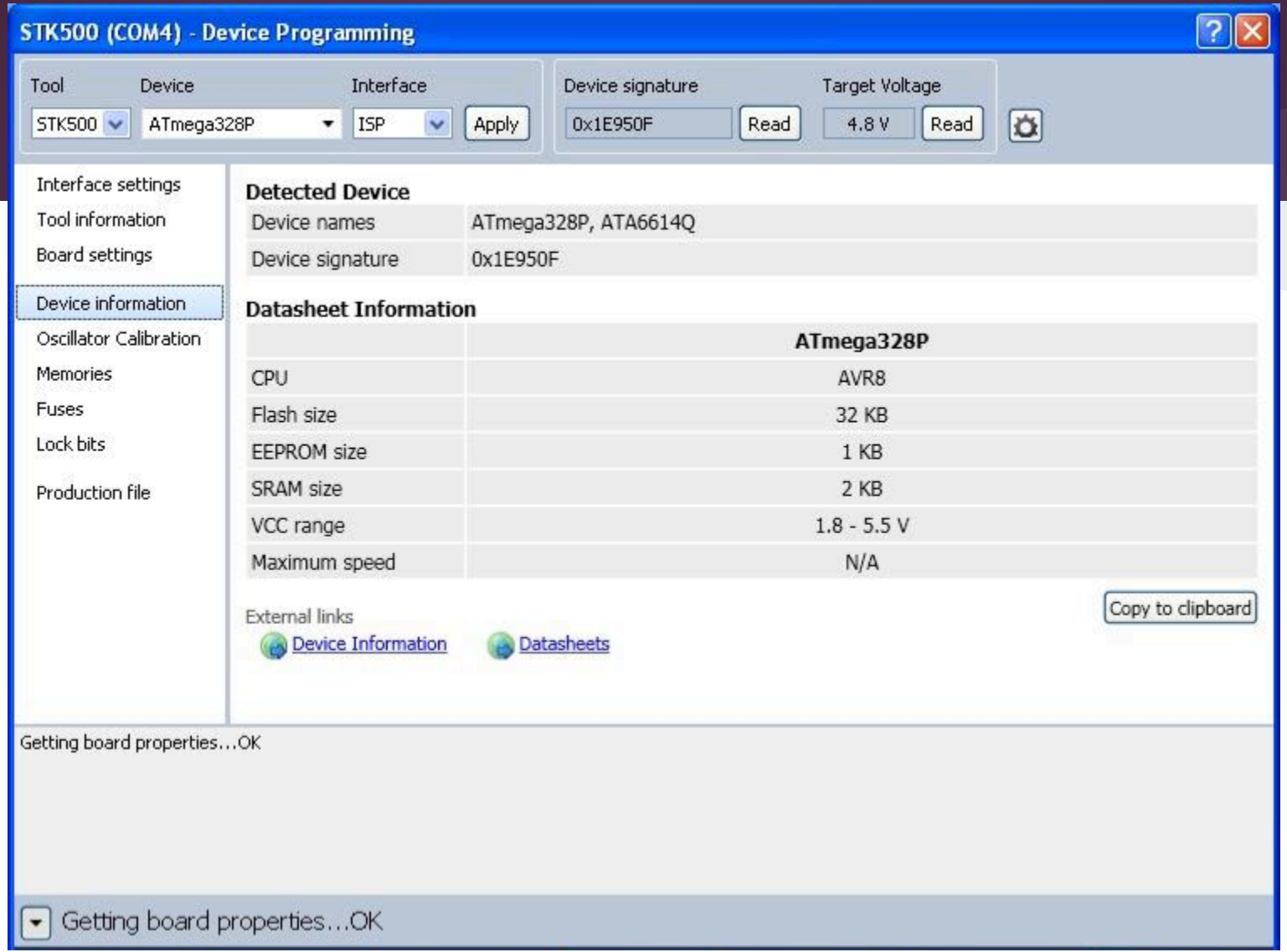


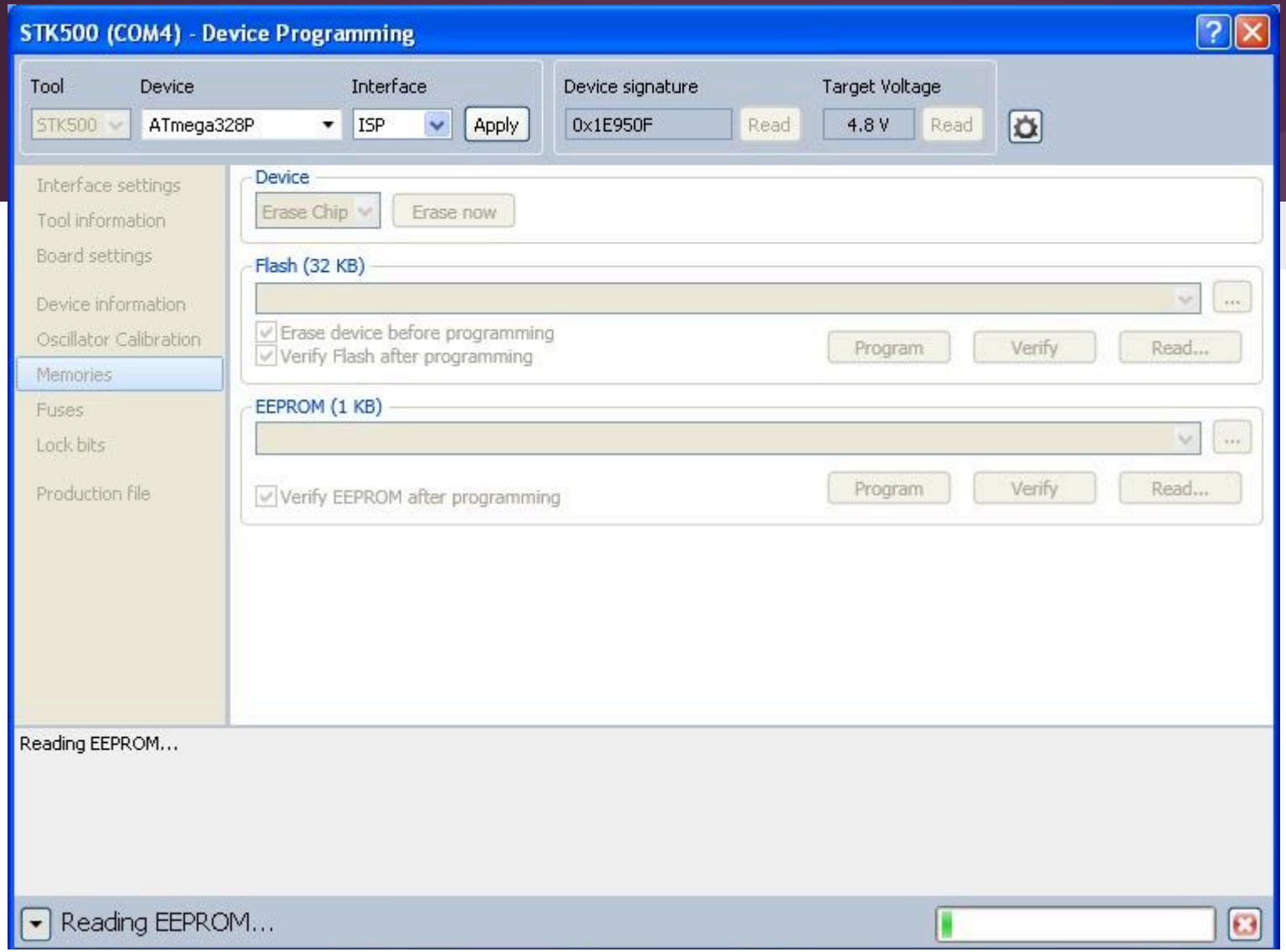
1. From Atmel Studio main screen, choose ‘Debug’ then ‘Device Programming’.
2. Identify the ‘Tool’, ‘Device’, and ‘Interface’ then click ‘Apply’.

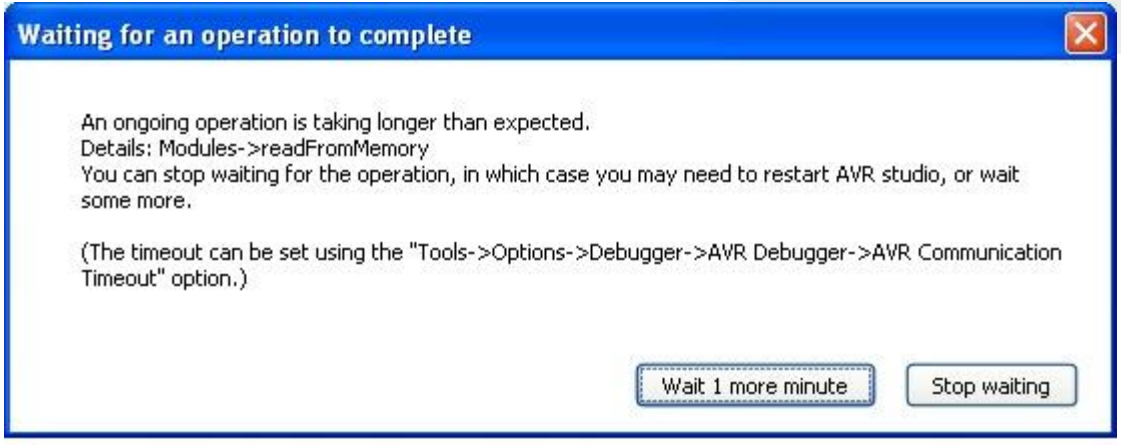

STK500 (COM4) - Device Programming
Tool
Device
Interface
STK500
ATmega328P
ISP
Apply
Device signature

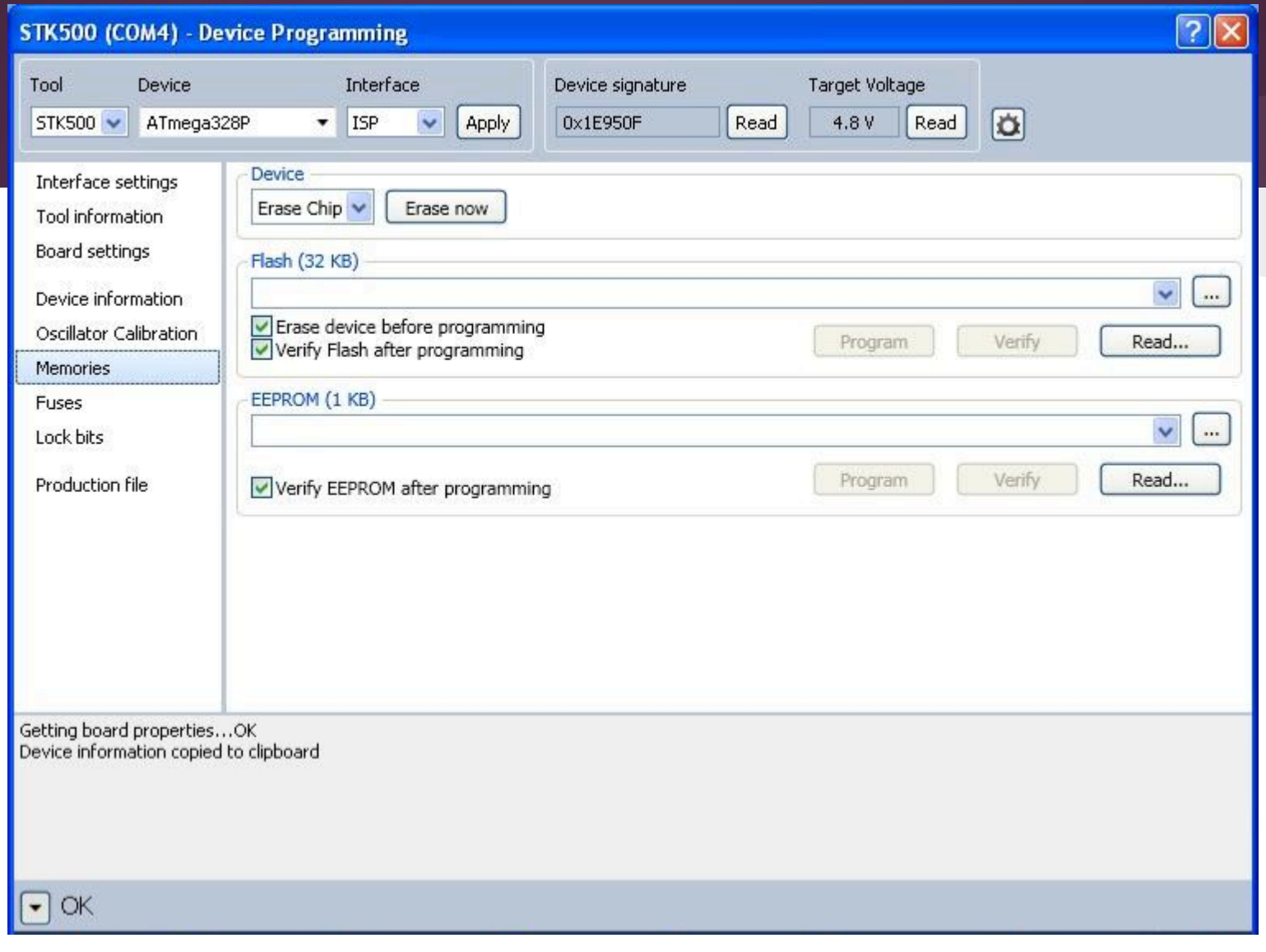
Read
Target Voltage

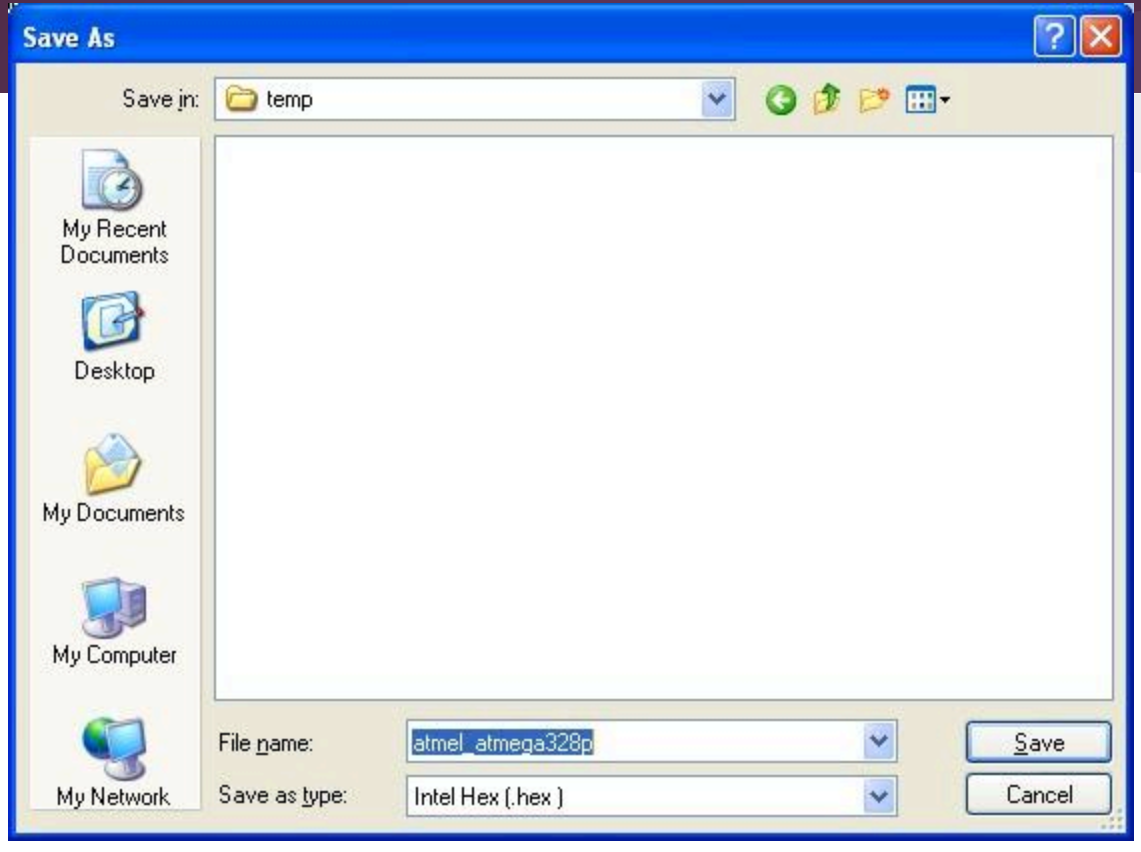
Read
Interface settings
Tool information
Board settings
Device information
Oscillator Calibration
Memories
Fuses
Lock bits
Production file
ISP Clock
11.45 kHz
The ISP Clock frequency must be lower than 1/4 of frequency the device is operating on.
Set

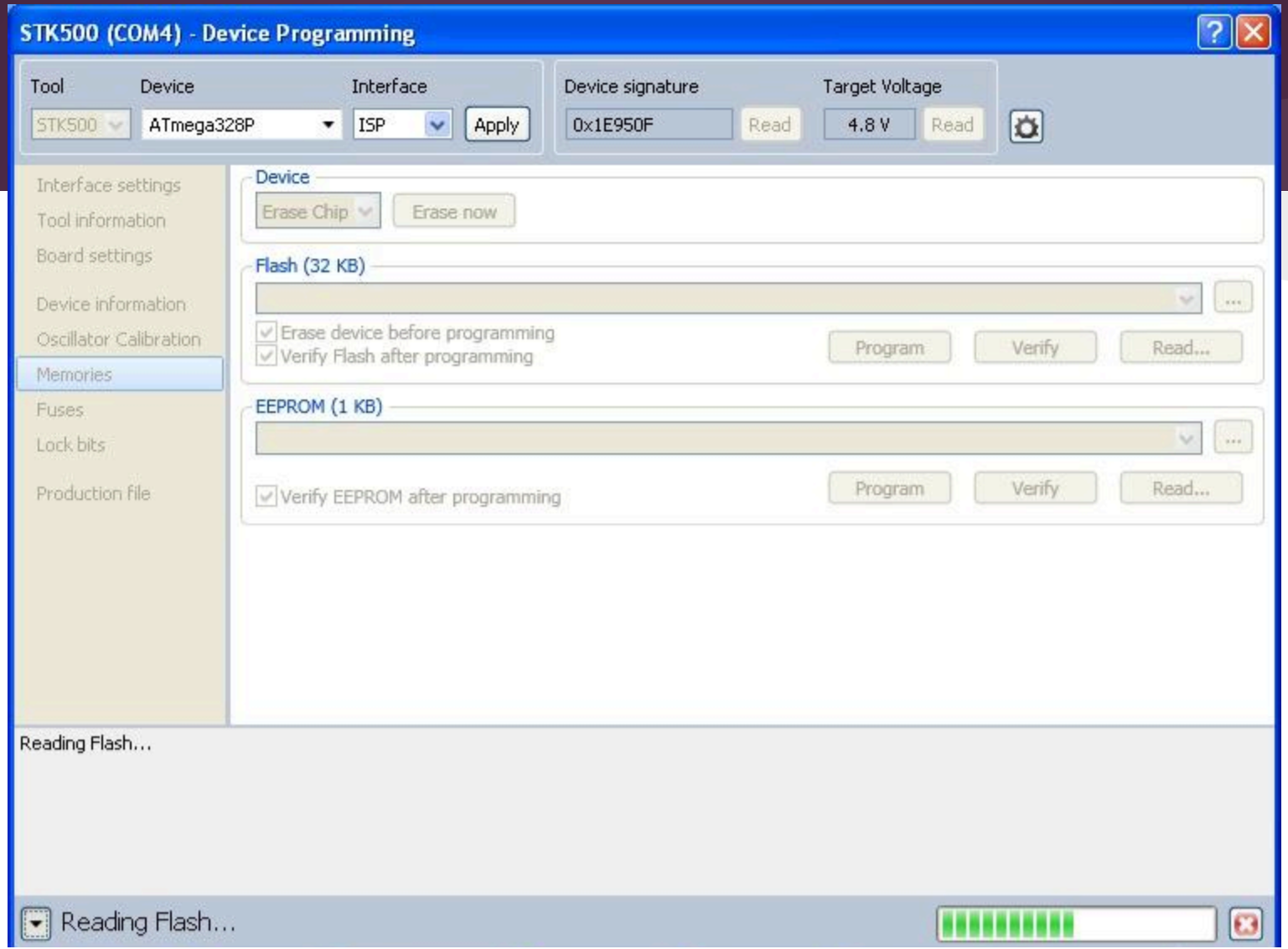

STK500 (COM4) - Device Programming
Tool
Device
Interface
STK500
ATmega328P
ISP
Apply
Device signature
0x1E950F
Read
Target Voltage
4.8 V
Read
Interface settings
Tool information
Board settings
Device information
Oscillator Calibration
Memories
Fuses
Lock bits
Production file
Detected Device
Device names
ATmega328P, ATA6614Q
Device signature
0x1E950F
Datasheet Information
ATmega328P
CPU
AVR8
Flash size
32 KB
EEPROM size
1 KB
SRAM size
2 KB
VCC range
1.8 - 5.5 V
Maximum speed
N/A
Copy to clipboard
External links
Device Information
Datasheets
Getting board properties...OK
Getting board properties...OK

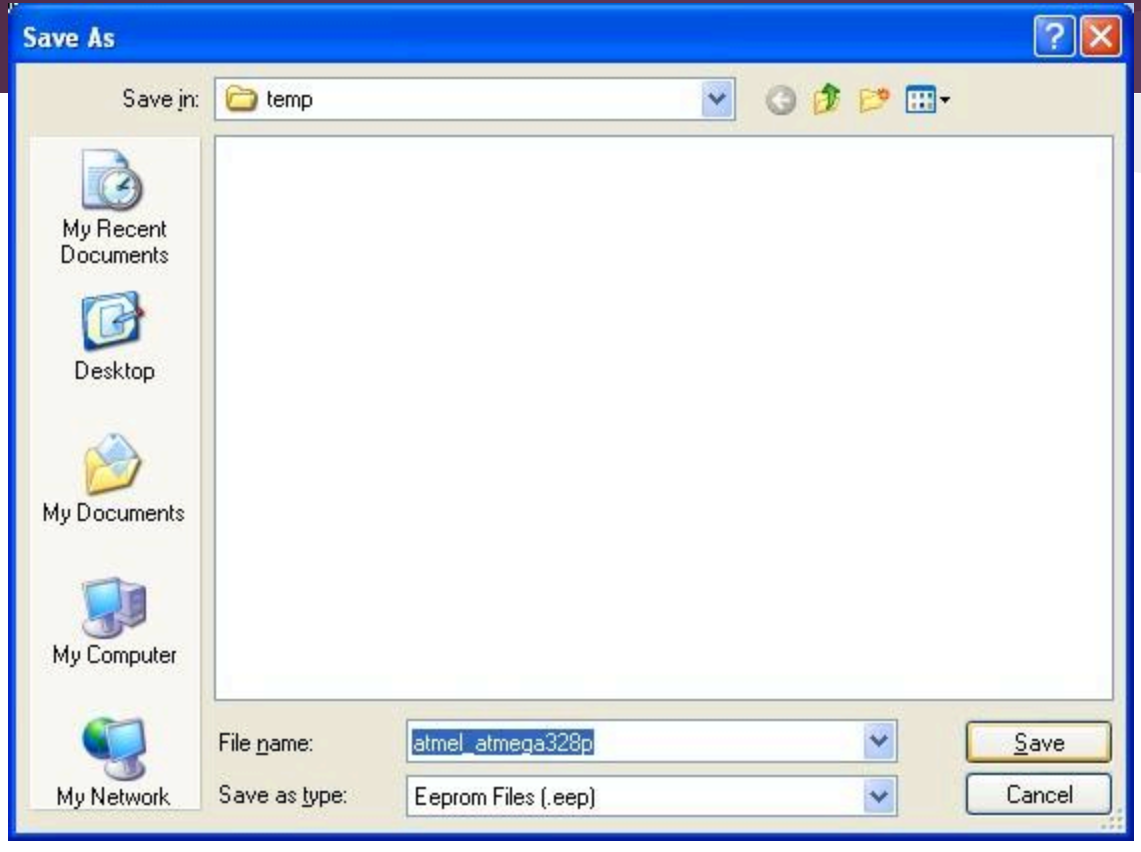

STK500 (COM4) - Device Programming
Tool
Device
Interface
STK500
ATmega328P
ISP
Apply
Device signature
Target Voltage
0x1E950F
Read
4.8 V
Read
Interface settings
Tool information
Board settings
Device information
Oscillator Calibration
Memories
Fuses
Lock bits
Production file
Device
Erase Chip
Erase now
Flash (32 KB)
Erase device before programming
Verify Flash after programming
Program
Verify
Read...
EEPROM (1 KB)
Verify EEPROM after programming
Program
Verify
Read...
Reading EEPROM...
Reading EEPROM...


Waiting for an operation to complete
An ongoing operation is taking longer than expected.
Details: Modules->readFromMemory
You can stop waiting for the operation, in which case you may need to restart AVR studio, or wait some more.
(The timeout can be set using the "Tools->Options->Debugger->AVR Debugger->AVR Communication Timeout" option.)
Wait 1 more minute
Stop waiting


STK500 (COM4) - Device Programming
Tool
Device
Interface
STK500
ATmega328P
ISP
Apply
Device signature
0x1E950F
Read
Target Voltage
4.8 V
Read
Interface settings
Tool information
Board settings
Device information
Oscillator Calibration
Memories
Fuses
Lock bits
Production file
Device
Erase Chip
Erase now
Flash (32 KB)
Erase device before programming
Verify Flash after programming
Program
Verify
Read...
EEPROM (1 KB)
Verify EEPROM after programming
Program
Verify
Read...
Getting board properties...OK
Device information copied to clipboard
OK


Save As
Save in:
temp
My Recent Documents
Desktop
My Documents
My Computer
My Network
File name:
atmel_atmega328p
Save as type:
Intel Hex (.hex)
Save
Cancel


STK500 (COM4) - Device Programming
Tool
Device
Interface
STK500
ATmega328P
ISP
Apply
Device signature
0x1E950F
Read
Target Voltage
4.8 V
Read
Interface settings
Tool information
Board settings
Device information
Oscillator Calibration
Memories
Fuses
Lock bits
Production file
Device
Erase Chip
Erase now
Flash (32 KB)
Erase device before programming
Verify Flash after programming
Program
Verify
Read...
EEPROM (1 KB)
Verify EEPROM after programming
Program
Verify
Read...
Reading Flash...
Reading Flash...


Save As
Save in:
temp
My Recent Documents
Desktop
My Documents
My Computer
My Network
File name:
atmel_atmega328p
Save as type:
Eeprom Files (.eep)
Save
Cancel

AVR Acquisition with Atmel Studio

End