Windows Installation Guide for Suricata IDS/IPS

This is a Suircata Windows Installation Guide –

Compilation from scratch.

Tested on Win XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008R2 64 bit.

Date: 26 May 2012

Document Version: 1.3

Author: Peter Manev

This is a guide of how to compile and come up with your own executable/binary of Suricata on Windows. If you do not want to do that – there is a auto installation (MSI) windows native package here:

http://www.openinfosecfoundation.org/index.php/download-suricata

just run it and it will install Suricata for you on your Windows system.

This guide consists of two sections.

Section I – is for advanced users, a quick overview of what needs to be done. If you have had experience with Cygwin and Suricata before, this section should be enough. Should you feel you need a bit more details, please jump to Section II.

Section II – is a step by step guide and detailed instructions on how to install and configure Suricata on Windows OS, for newbies.

SECTION I - Advanced users

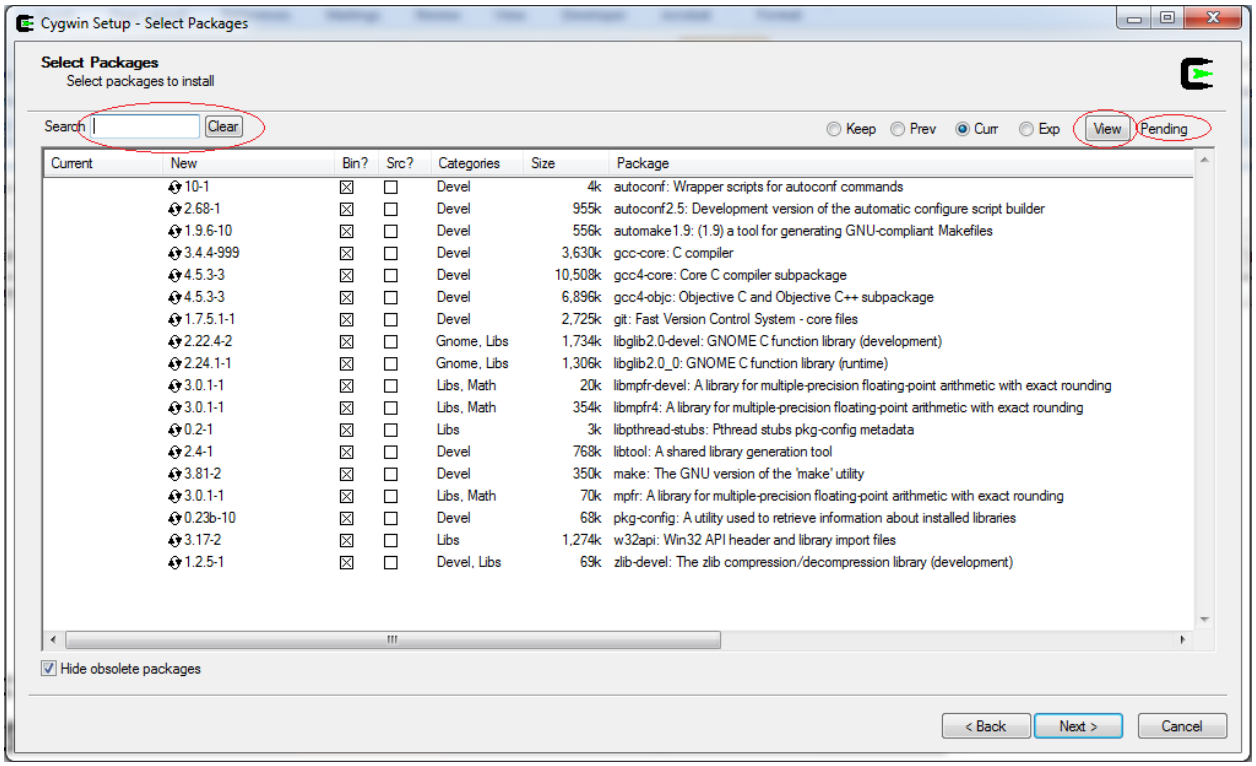
Step 1 – You need to download and install Cygwin

Download Cygwin – http://cygwin.com/setup.exe

After the installation is done you would need to add the packages below to your Cygwin installation - needed for Suricata to run.

w32api, mpfr, pthreads, gcc-core , gcc4-core , make , zlib , autoconf , automake , libtool , glib , pkg-config , pkg-config , git .

Or in a bit more detail:



Step 2 – Make sure you have WinPcap installed.

http://www.winpcap.org/install/default.htm

You would also need to download and unzip (anywhere you like) the devs pkgs of WinPcap

http://www.winpcap.org/devel.htm

Copy libraries (from the unpacked directory) like this:

- ✓ **Copy all the content of WpdPack\Lib\ to cygwin\lib**
- ✓ **Copy all headers (all the content)from WpdPack\Include\ to C:\cygwin\usr\include**
- ✓ **Rename "libwpcap" to "libpcap" (in your cygwin\lib\ directory)**

Step 3 Add some paths to the system path.

Add to system path (Win 7, 2008 - Control Panel\System and Security\System\Advanced system settings\Environment Variables), select "path" under "system variables", click "edit", append the following to the end:

C:\cygwin\bin;C:\cygwin\lib\pkgconfig;

Add the above to environment system variables in your windows system!!

Step 4 Get libyaml

Download the yaml package (at the time of this writing the current version is yaml-0.1.4.tar.gz)

http://pyyaml.org/download/libyaml/yaml-0.1.4.tar.gz

Unpack it in (for example in your Cygwin tmp directory) - C:\cygwin\tmp

Start Cygwin, go to the yaml directory then execute –

./configure --prefix=/usr && make && make install

Step 5 Get and compile Suricata.

As you are still in the CYGWIN environment -

Suricata from git:

If you want to install Suricata from git – latest version

go to a tmp dir. Type in :

a) *git clone git://phalanx.openinfosecfoundation.org/oisf.git*
b) *cd oisf*
c) *dos2unix.exe libhtp/configure.ac && dos2unix.exe libhtp/htp.pc.in && dos2unix.exe libhtp/Makefile.am*
d) *./autogen.sh && ./configure && make*

Suricata Stable (at the moment of this writing the stable version is 1.2.1):

If you want to install Suricata stable – latest stable version (production)

(You can find it here - http://www.openinfosecfoundation.org/index.php/download-suricata)

go to a tmp dir. Type in :

a) *wget http://www.openinfosecfoundation.org/download/suricata-1.2.1.tar.gz*
b) *tar –zxf suricata-1.2.1.tar.gz*
c) *cd suricata-1.2.1*
d) *dos2unix.exe libhtp/configure.ac && dos2unix.exe libhtp/htp.pc.in && dos2unix.exe libhtp/Makefile.am*
e) *libtoolize -c && autoreconf -fv --install && ./configure && make*

Ste 5.1 – MD5 support

OPTIONALLY – if you would like to compile Suricata with MD5s support ()to be able to log MD5s on opened/downloaded/transferred files coming through the wire- you must compile like this –

Make sure you add the following for Cygwin:

Then -

For stable -

libtoolize -c && autoreconf -fv --install && ./configure --with-libnss-libraries=/usr/lib --with-libnss-includes=/usr/include/nss/ --with-libnspr-libraries=/usr/lib --with-libnspr-includes=/usr/include/nspr && make

For git –

./autogen.sh && ./configure --with-libnss-libraries=/usr/lib --with-libnss-includes=/usr/include/nss/ --with-libnspr-libraries=/usr/lib --with-libnspr-includes=/usr/include/nspr && make

Make sure you add the following DLLs to the directory where you will run suricata (copy them from the Cygwin\bin directory):

cygfreebl3.dll

cygnspr4.dll

cygnss3.dll

cygnssckbi.dll

cygnssdbm3.dll

cygnssutil3.dll

cygplc4.dll

cygplds4.dll

cygsmime3.dll

cygsoftokn3.dll

cygssl3.dll

Then continue with the instructions below (the bellow mentioned DLLs are also needed), just substitute the **oisf** directory with **suricata-1.2.1** directory!

After it is done, go to your /oisf/src/.lib (or /suricata-1.2.1/src/.lib for Suricata stable) directory and copy the Suricata.exe file to a dedicated directory, for example –C:\Suricata

Also - copy classification.config , reference.config and suricata.yaml (form your oisf/ directory) to (your dedicated directory) C:\Suricata

NOTE: If you would like to make a standalone installation, copy (from C:\cygwin\bin)

cygz.dll

cygwin1.dll

cygpcre-0.dll

cygmagic-1.dll

cyggcc_s-1.dll

cygnspr4.dll

cygnss3.dll

to your C:\Suricata directory

Also copy C:\cygwin\usr\share\misc\magic.mgc to your C:\Suricata directory

Step 6 Configure and run Suricata

…run intruders…run….

Download some rule sets and copy them to your rules directory.

Edit your suricata.yaml - (for example, at least change these lines and create the necessary folders respectively):

"default-log-dir: C:\Suricata\log

……

- file:

enabled: yes

filename: C:\Suricata\suricata.log

…….

default-rule-path: C:\Suricata\rules

classification-file: C:\Suricata\classification.config"

Open a cmd.

cd to your Suricata directory , execute –

suricata.exe -c suricata.yaml -i 192.168.1.71

change 192.168.1.71 with your respective IP and you are done.

NOTE:

If you need to run Suricata on an un-ip'd interfaces(thanks to Rich Rumble for pointing that out):

You can get the NIC UUID in a variety of ways, the simplest is using a single command for WMIC:(from cmd prompt paste in the following)

wmic nicconfig get ipaddress,SettingID

If you know your NIC's IP you can filter the results with findstr:

wmic nicconfig get ipaddress,SettingID | findstr 1.2.3.4

(replace 1.2.3.4 with your NIC's IP)

Then use that as your interface argument:

suricata.exe -c suricata.yaml –i \\DEVICE\\NPF_\{EE7B2A76-9343-449F-B3D8-3CB0F37DCA49\}

Make sure the double slashes are used, and a backslash is placed before the curly braces!


OISF
OPEN INFORMATION SECURITY FOUNDATION


SURICATA


SURICATA


OISF
OPEN INFORMATION SECURITY FOUNDATION

SECTION II - Step By Step for newbie

The following installations instructions were executed on Windows Server 2008R2 64 bit.

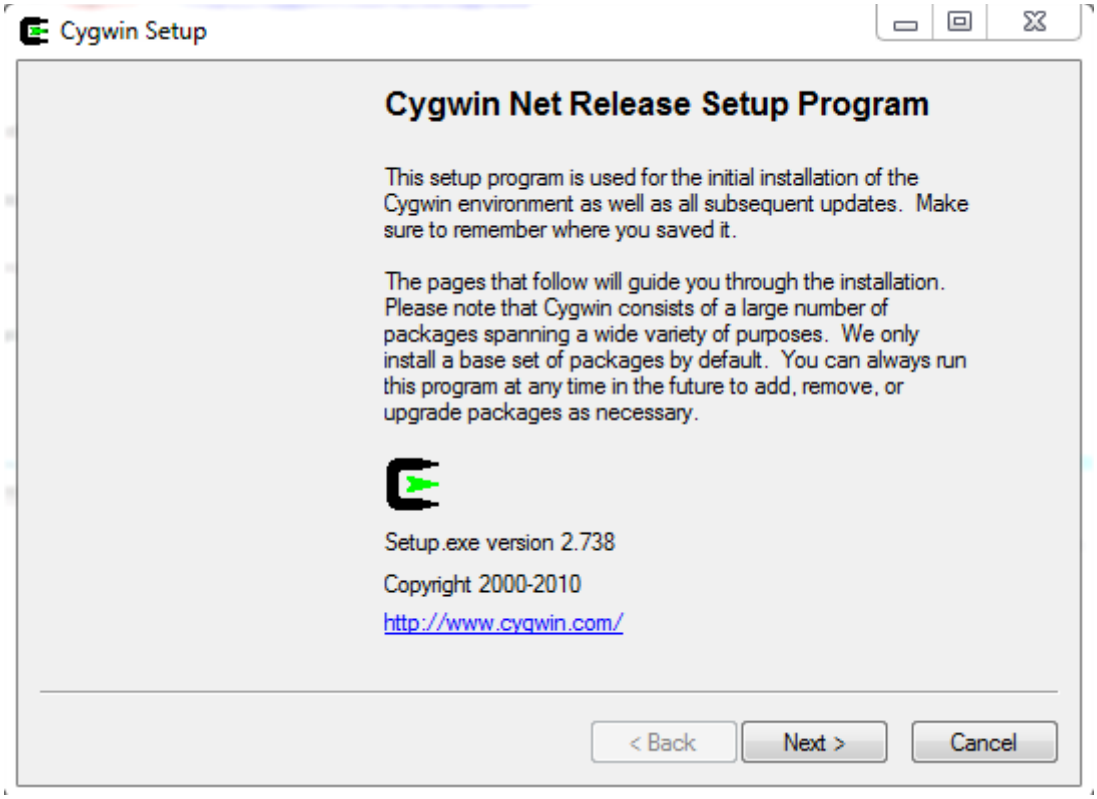
About 500 -600MB of space needed in total with all the necessary prerequisites installed.

Step 1 Download Cygwin

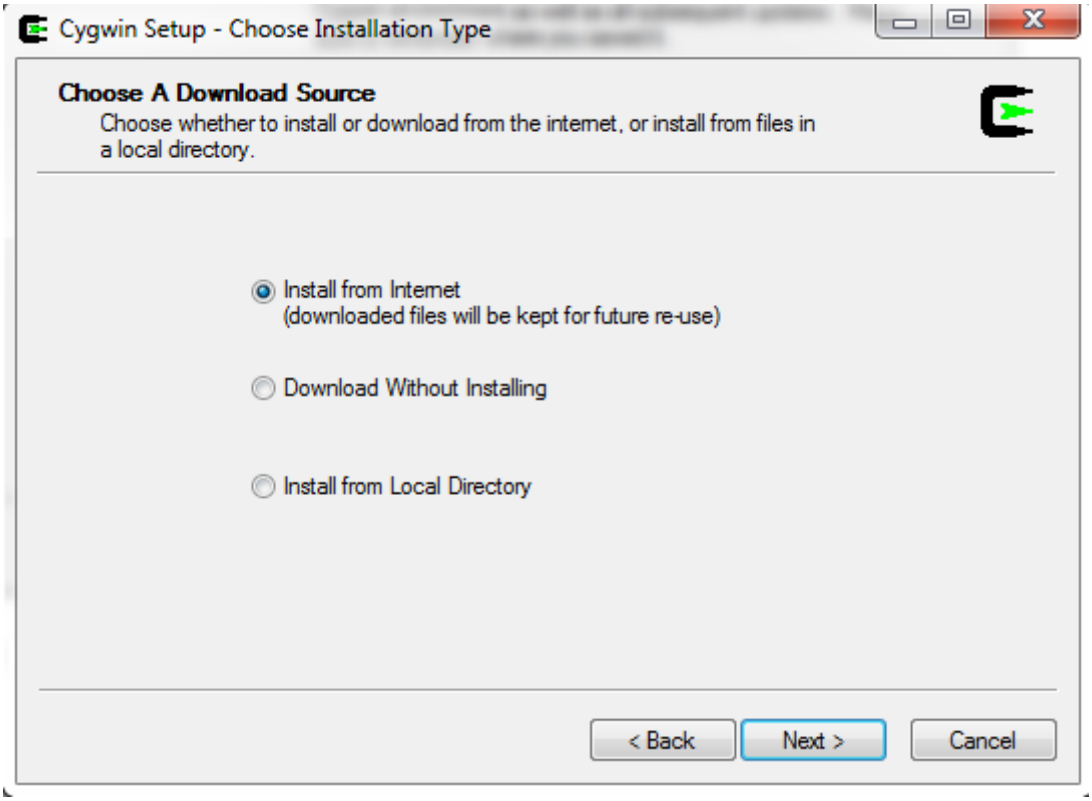
http://cygwin.com/setup.exe

Then double click the stup.exe to install

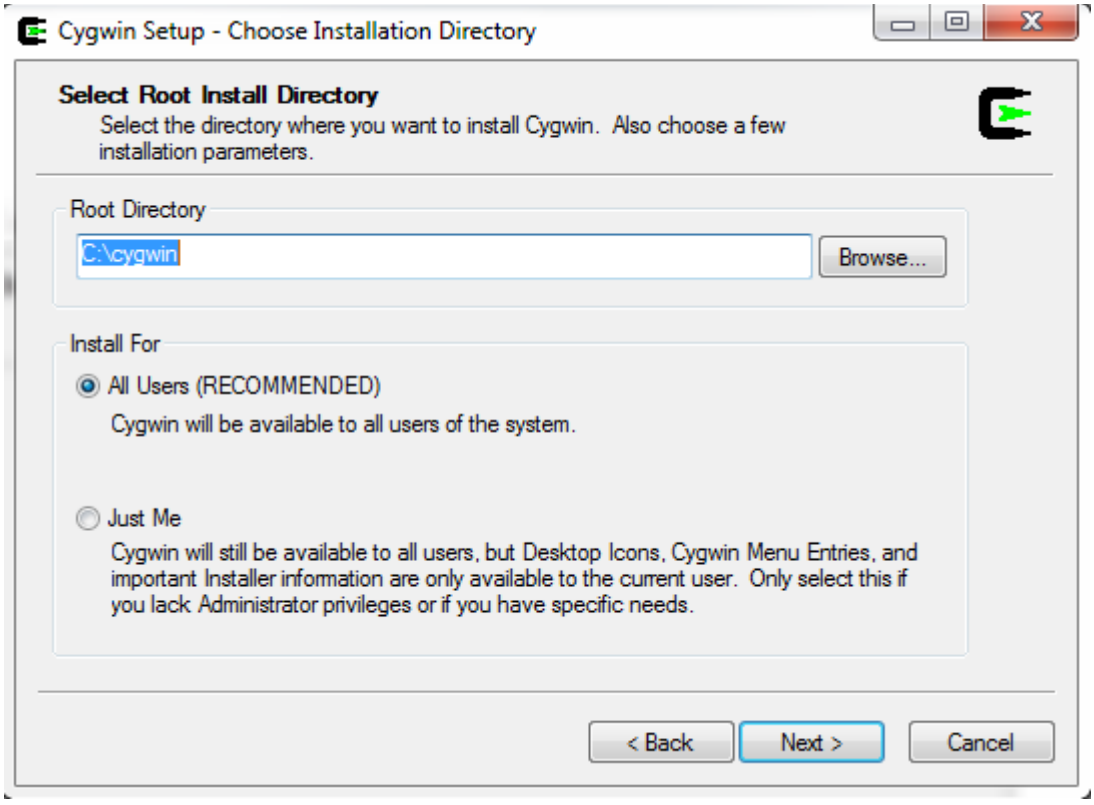
Go ahead and install it with the default options (basically just click next and ok)


Cygwin Setup
Cygwin Net Release Setup Program
This setup program is used for the initial installation of the Cygwin environment as well as all subsequent updates. Make sure to remember where you saved it.
The pages that follow will guide you through the installation. Please note that Cygwin consists of a large number of packages spanning a wide variety of purposes. We only install a base set of packages by default. You can always run this program at any time in the future to add, remove, or upgrade packages as necessary.
Setup.exe version 2.738
Copyright 2000-2010
http://www.cygwin.com/
< Back
Next >
Cancel

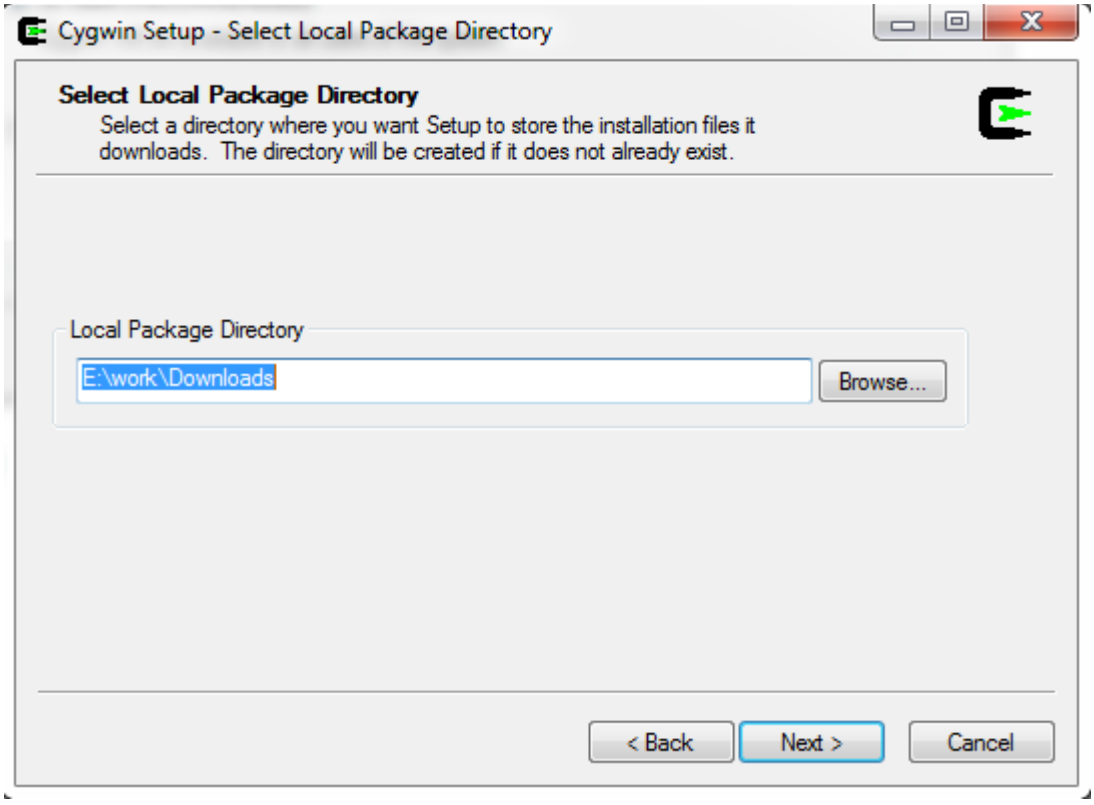
Pic1


Cygwin Setup - Choose Installation Type
Choose A Download Source
Choose whether to install or download from the internet, or install from files in a local directory.
Install from Internet
(downloaded files will be kept for future re-use)
Download Without Installing
Install from Local Directory
< Back
Next >
Cancel

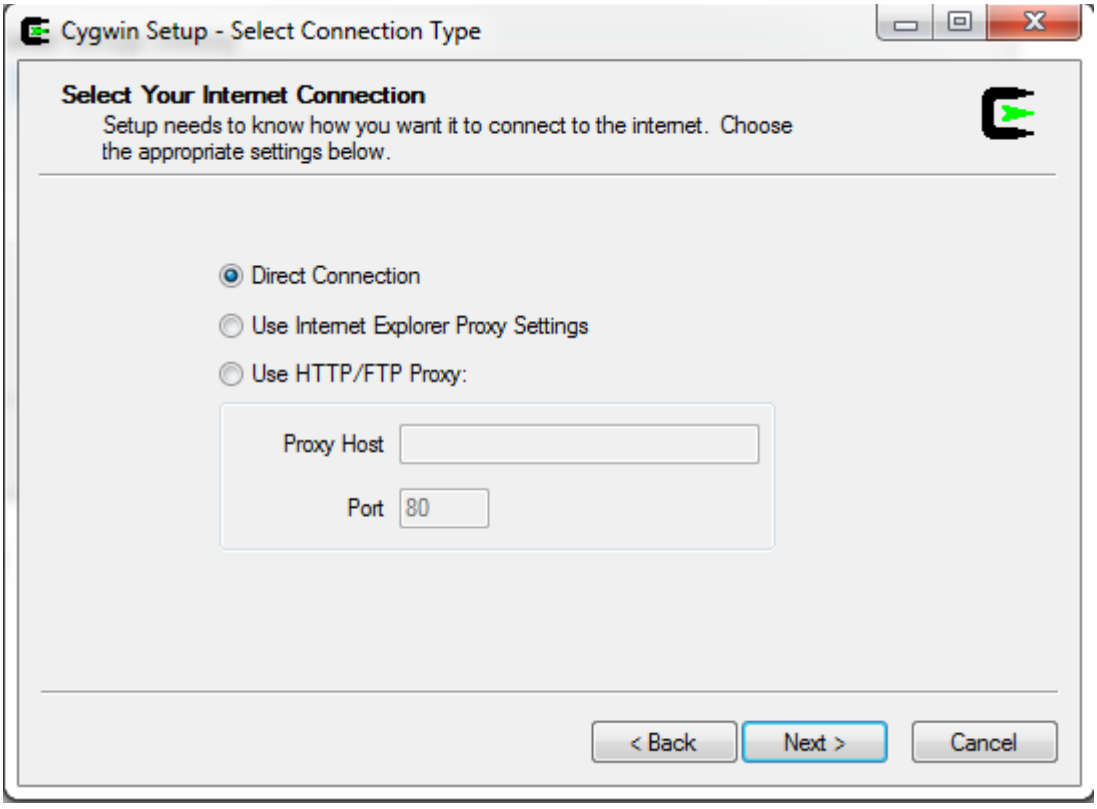
Pic2


Cygwin Setup - Choose Installation Directory
Select Root Install Directory
Select the directory where you want to install Cygwin. Also choose a few installation parameters.
Root Directory
C:\cygwin
Browse...
Install For
All Users (RECOMMENDED)
Cygwin will be available to all users of the system.
Just Me
Cygwin will still be available to all users, but Desktop Icons, Cygwin Menu Entries, and important Installer information are only available to the current user. Only select this if you lack Administrator privileges or if you have specific needs.
< Back
Next >
Cancel

Pic3

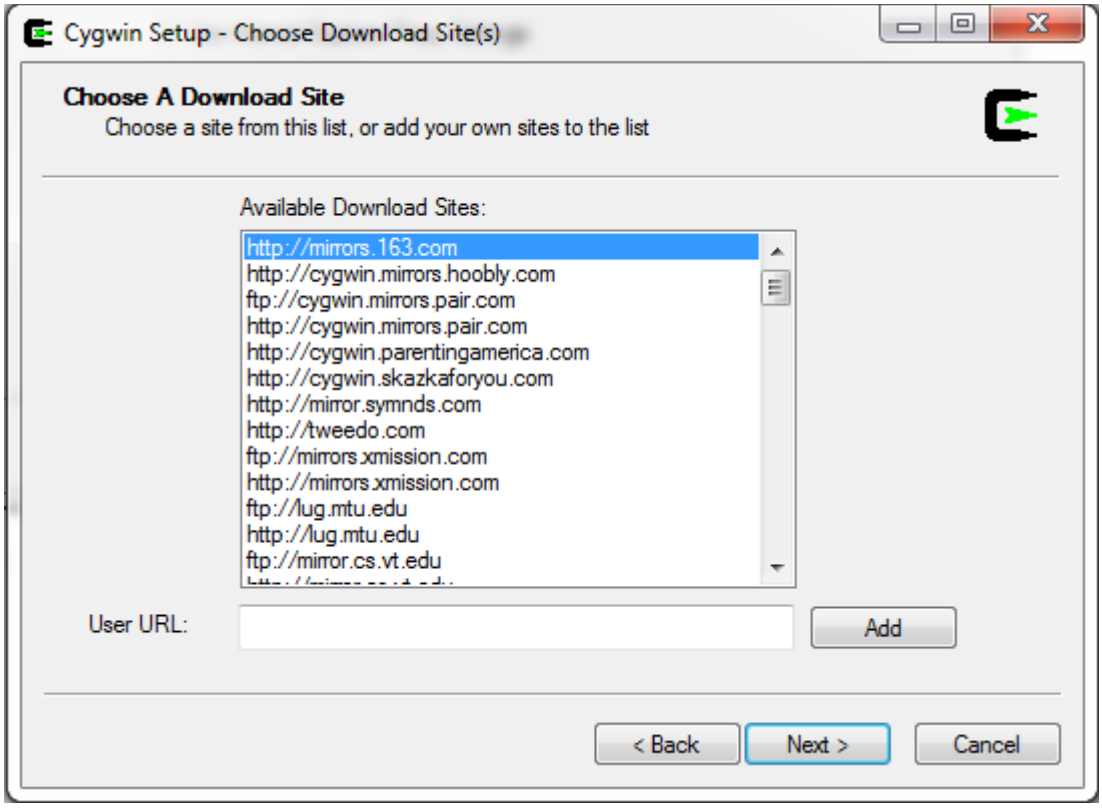

Cygwin Setup - Select Local Package Directory
Select Local Package Directory
Select a directory where you want Setup to store the installation files it downloads. The directory will be created if it does not already exist.
Local Package Directory
E:\work\Downloads
Browse...
< Back
Next >
Cancel

Pic4



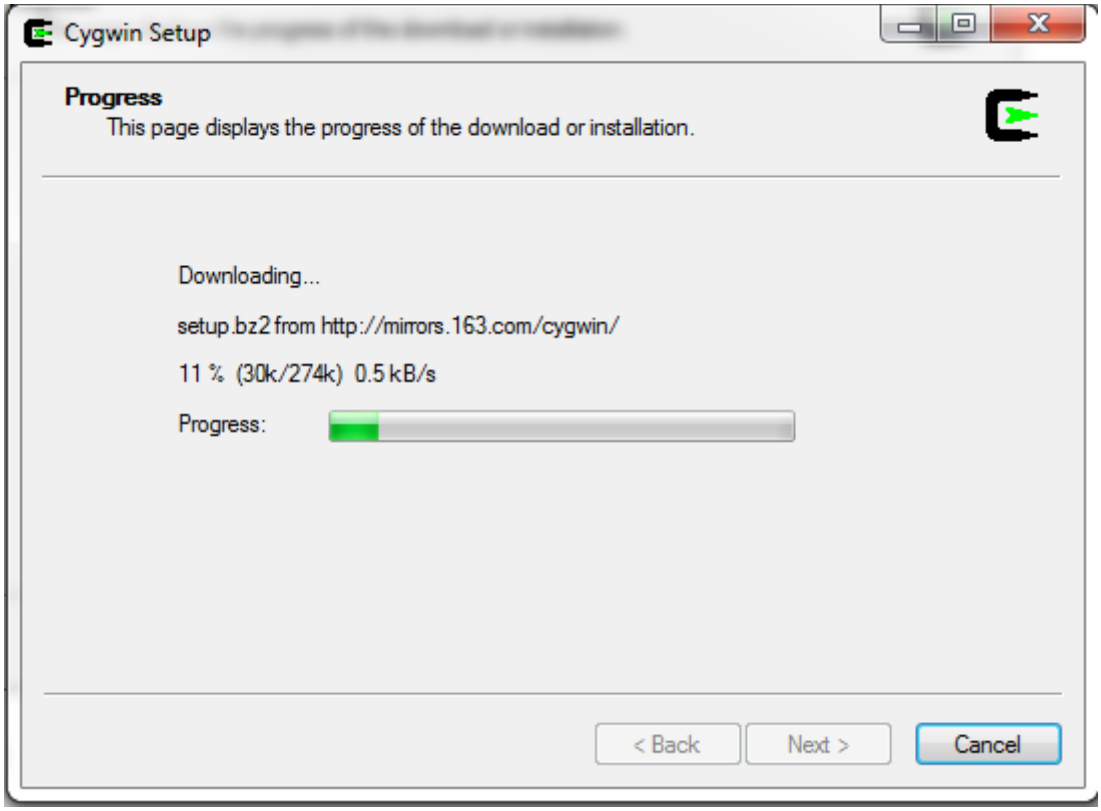
Pic5

Here , select any mirror you want:



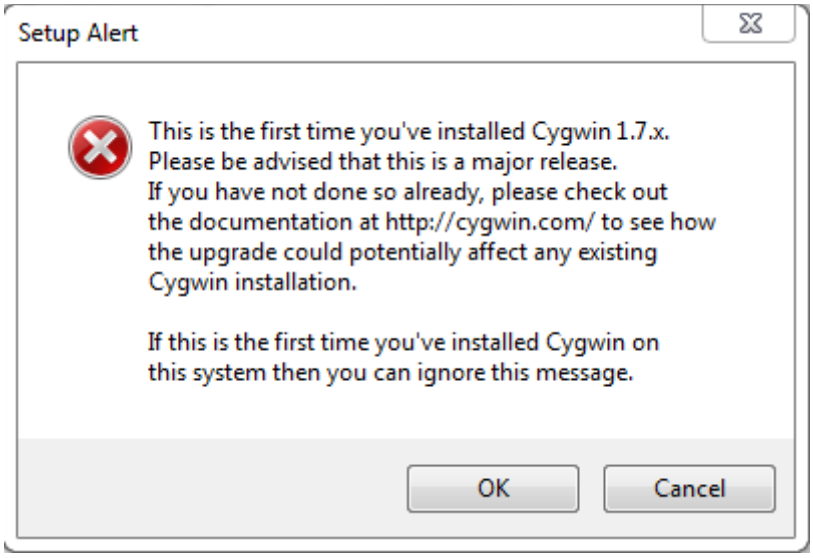
Pic6

Then you are going to see a progress bar:



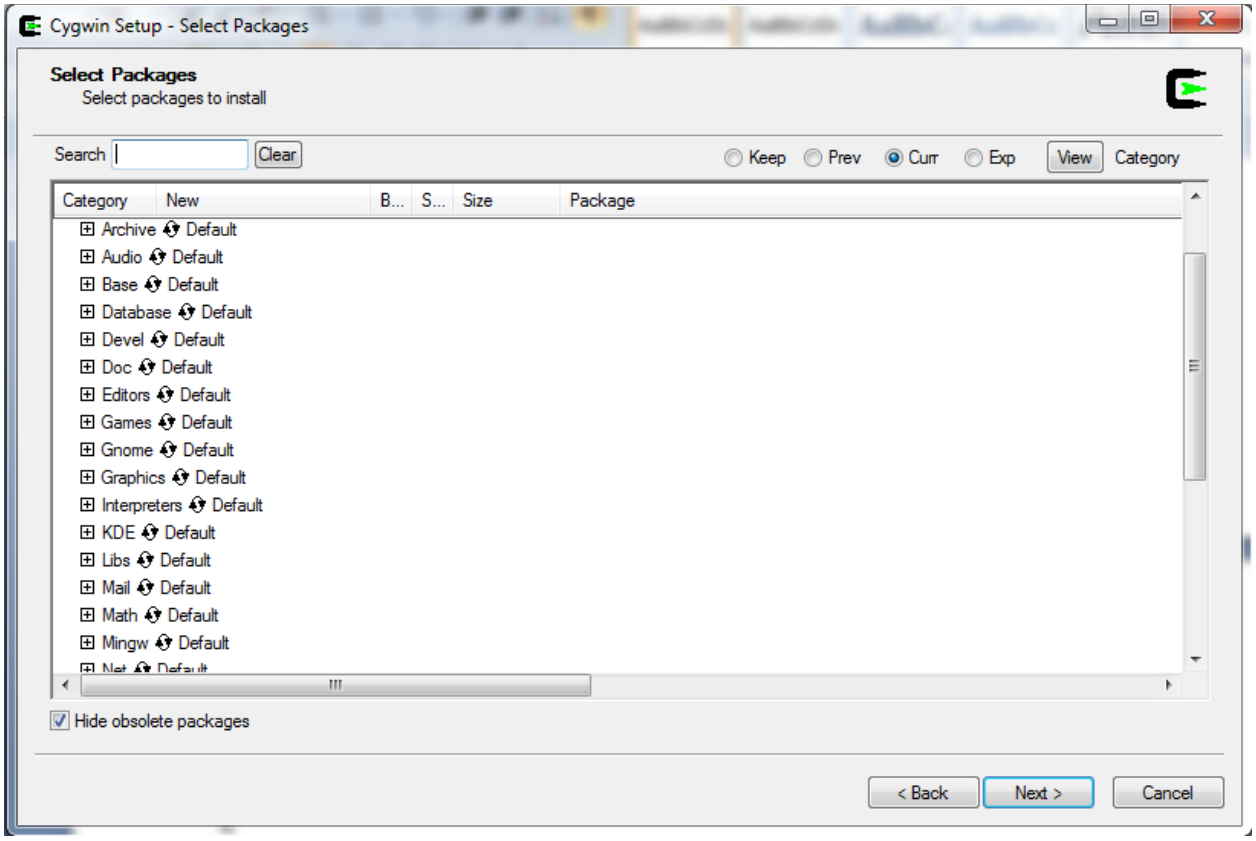
Pic7

You might get a warning if you already have installed CYGWIN – this is a guide for an installation from scratch :



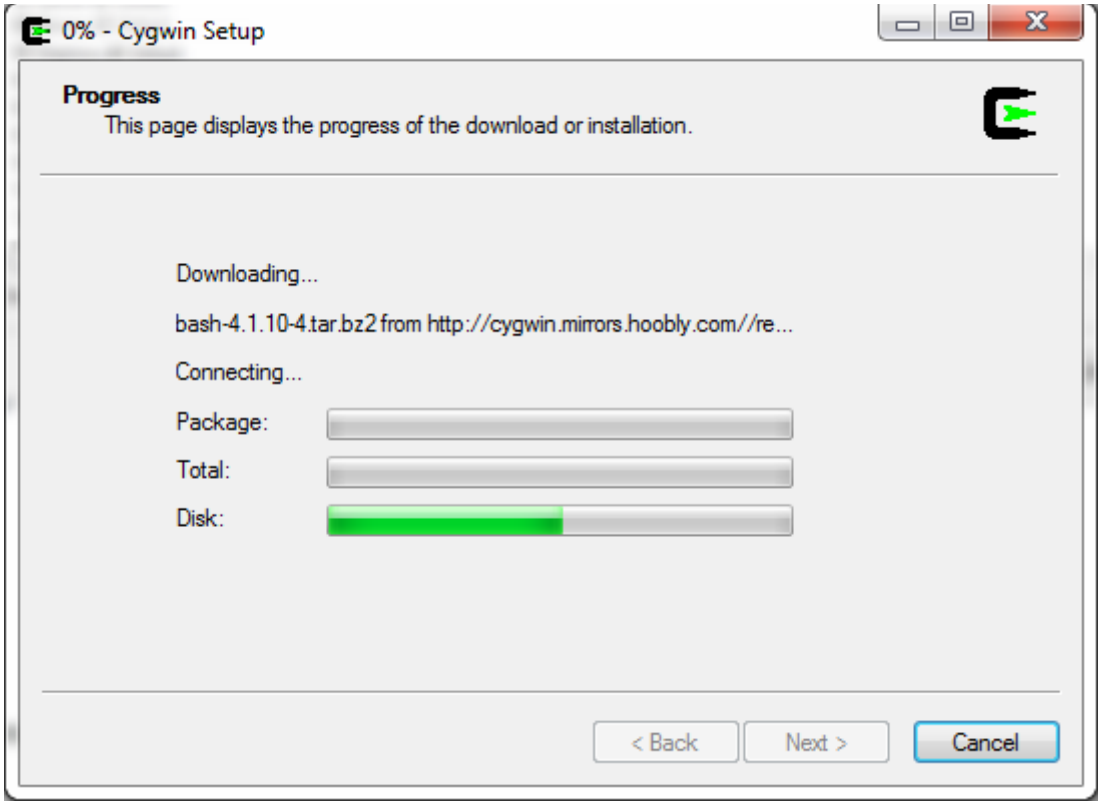
Pic8

Click next:



Pic9

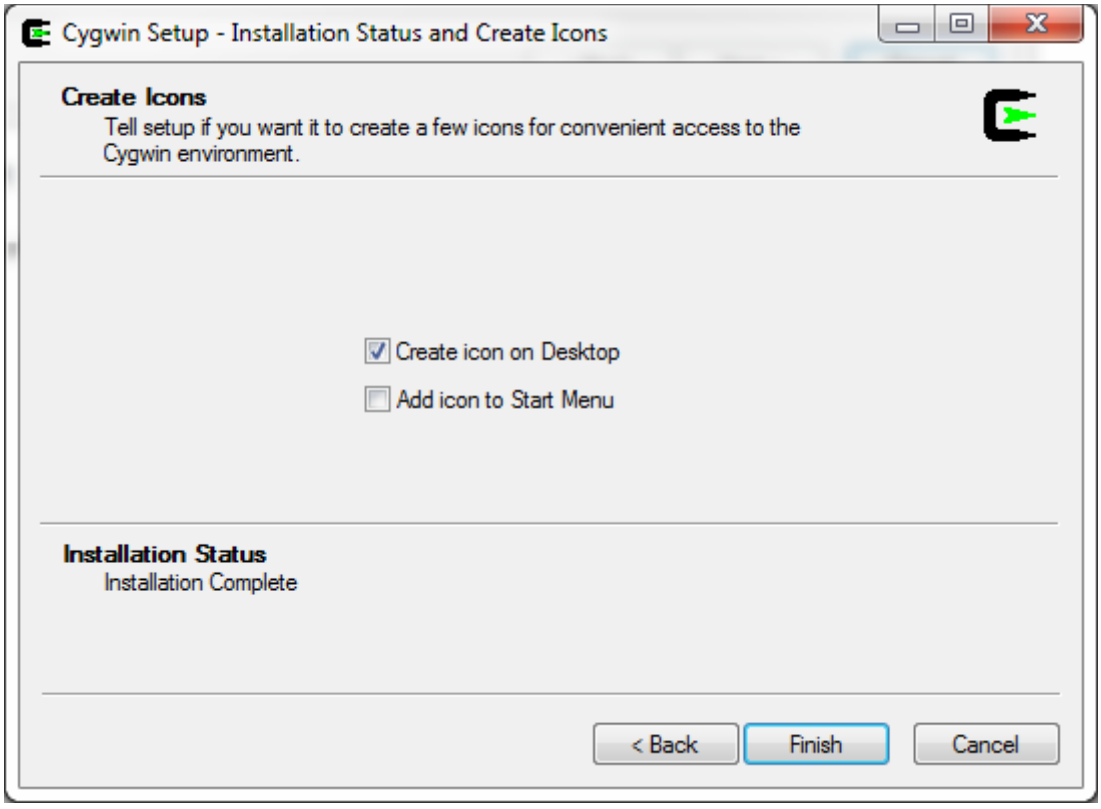
Then CYGWIN will start downloading and installing the necessary packages:



Pic10

It will probably take 10-15 min.

After it is finished - click finish ☺ :

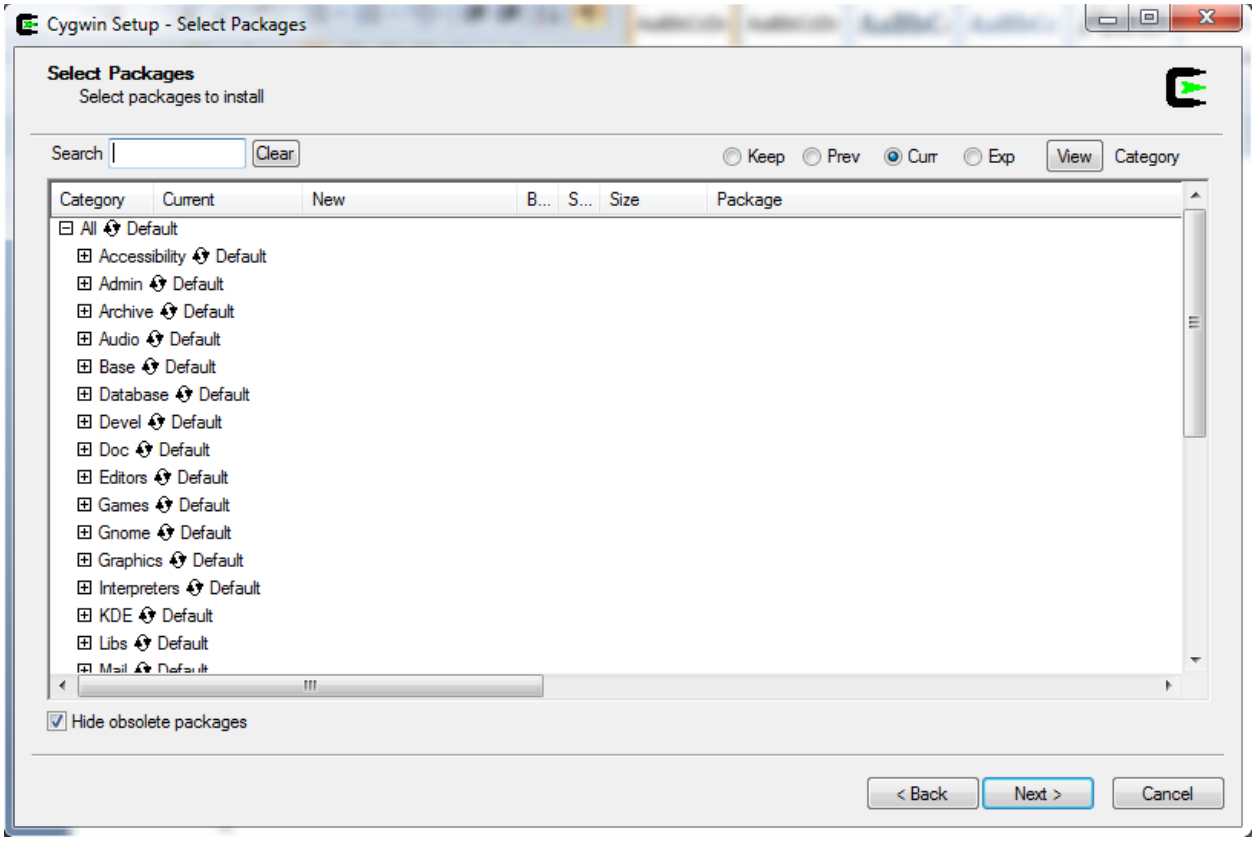


Pic11

Step 2 Install extra packages

Go back and double-click the very same setup.exe – we will need to install the extra packages necessary for Suricata to run.

Click next and ok until you are presented with the following screen:

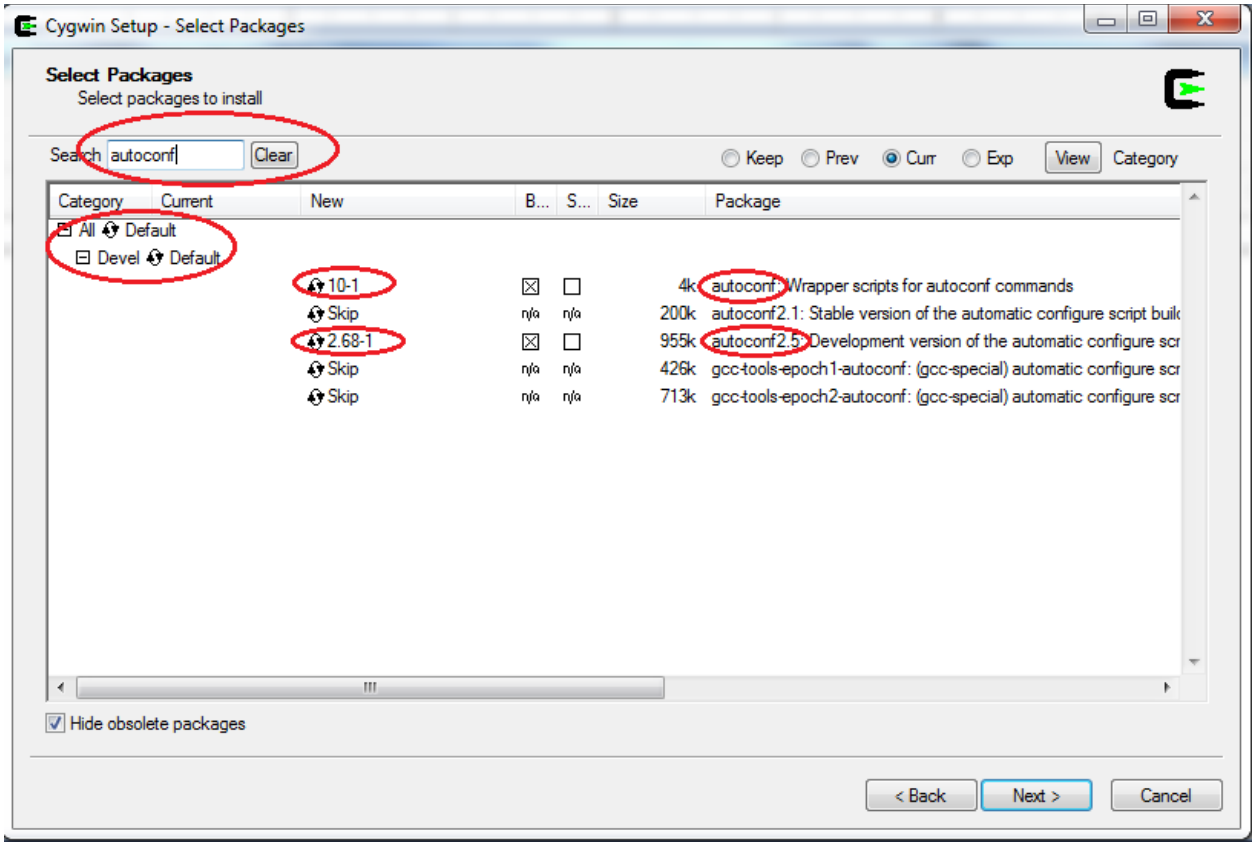


Pic12

Here (Pic below) is where we search select and queue for installation the additional packages needed.

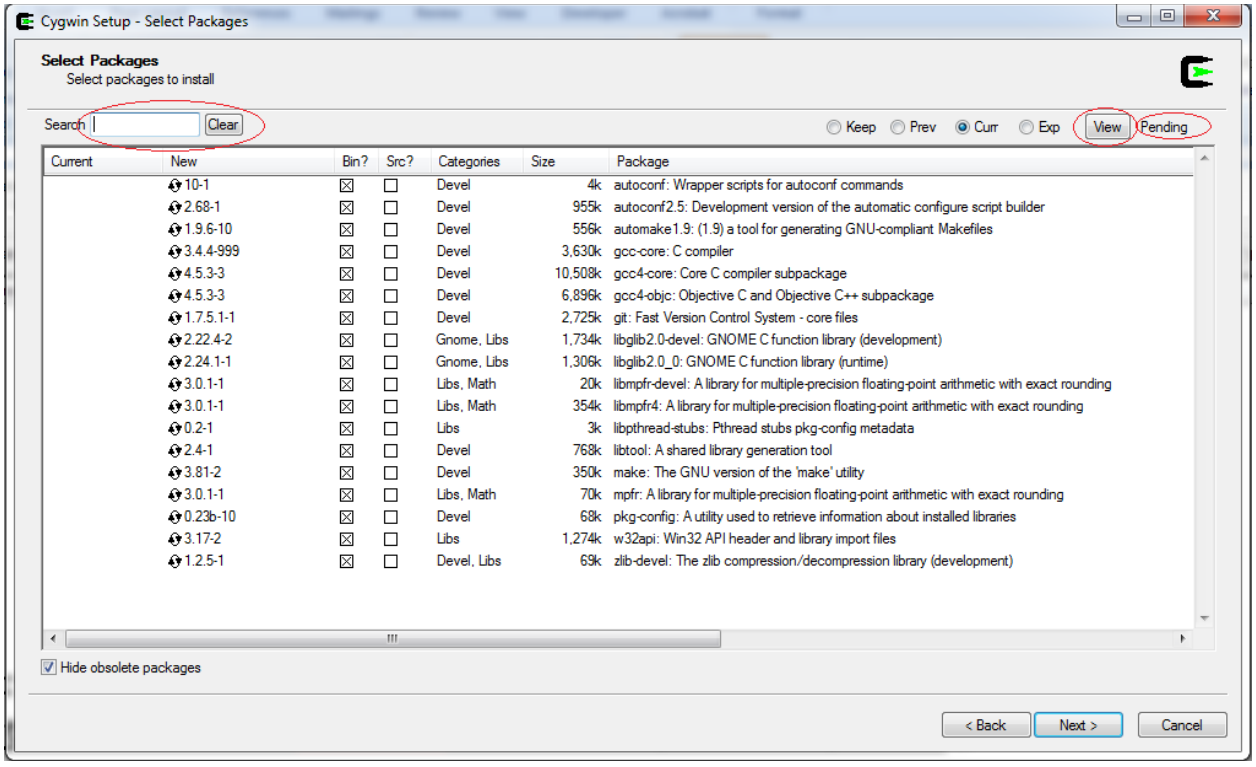
In the picture below , in the search box type in the name of the package- the search will return automatically , results , select the necessary package. Erase the contentment of the search box and type in the name of the next package, select …

Do the same for all the needed packages, DO NOT hit next until you have selected all the packages.



Pic13

The necessary packages are:



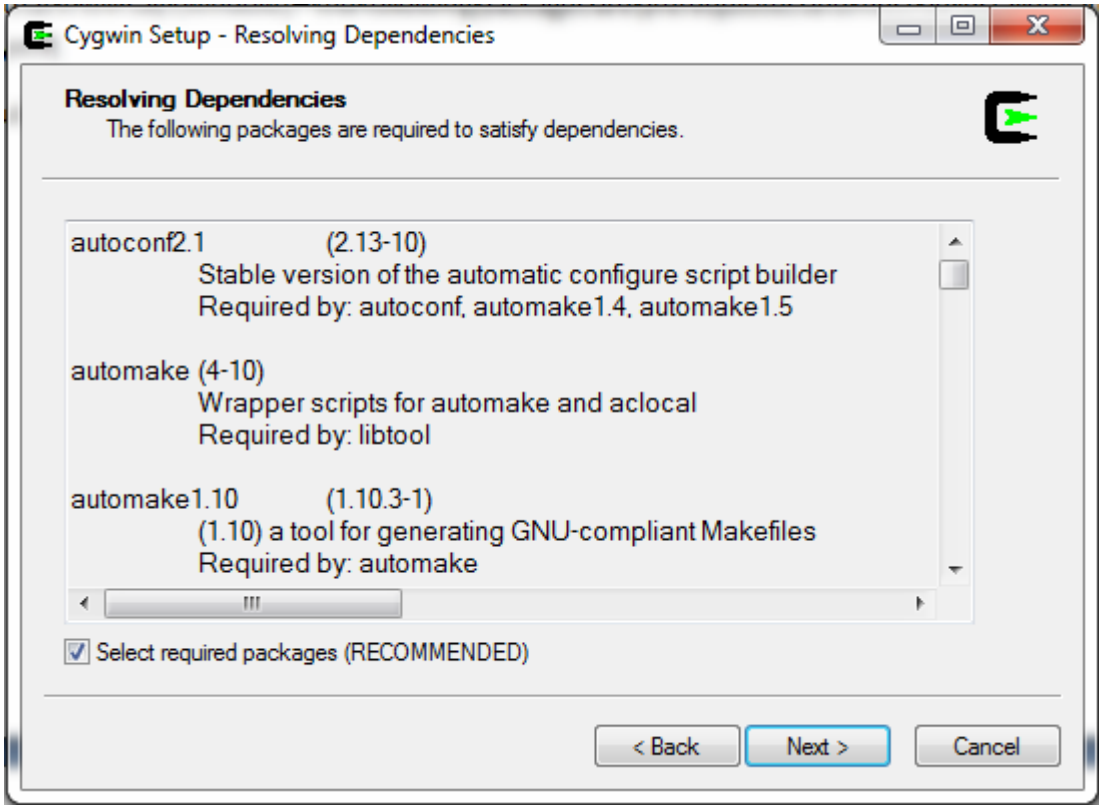
Pic14

After you are done selecting the packages – make sure the "search" box is cleared, click the "view" button until the text on the right of the button displays "pending".

Check and make sure all the needed packages are selected! If something is missing, go back and select it!

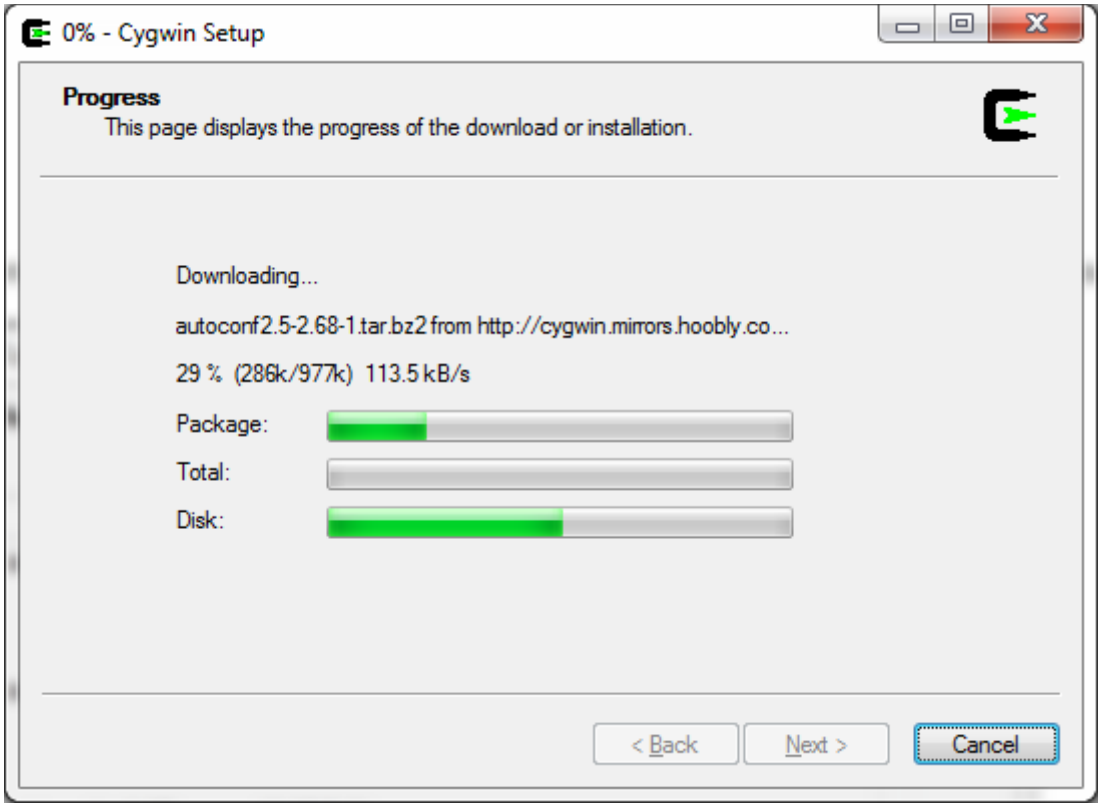
Click Next.

After that click next (make sure the option "select required packages (RECOMMENDED)" is selected!) :



Pic15

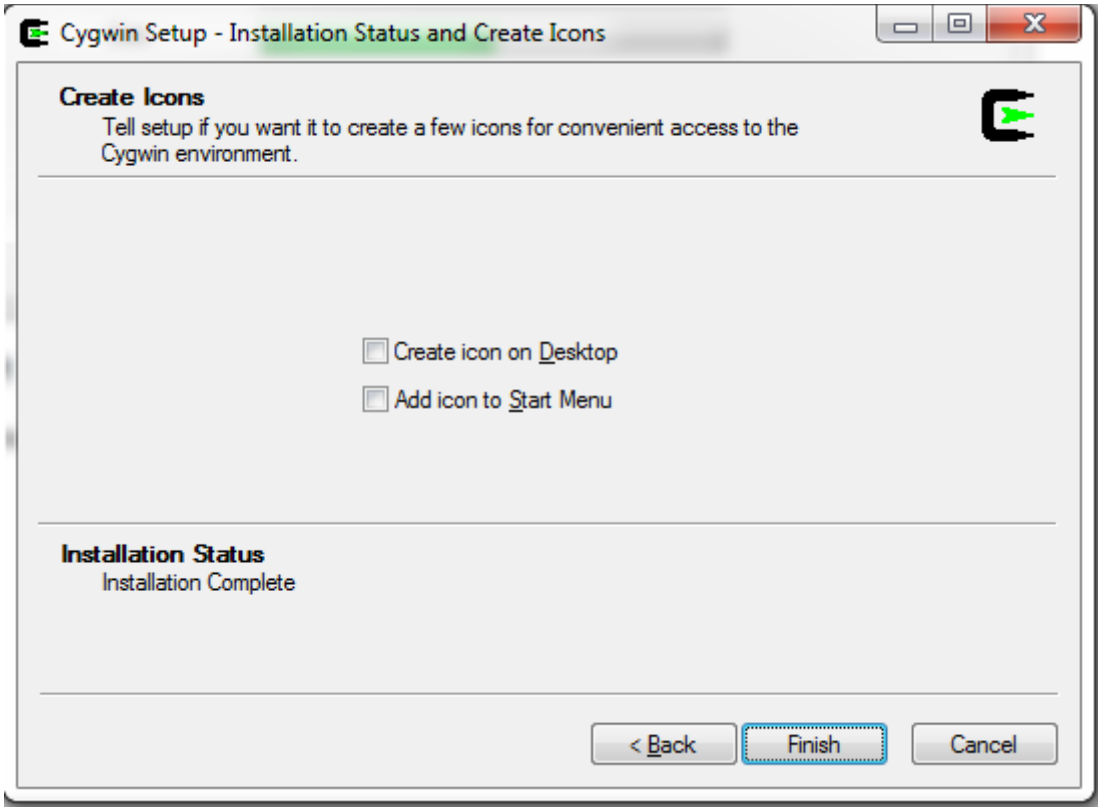
The extra packages that you have selected will start to download and install:



Pic16

This could also take 5 min or so.

Then click finish:



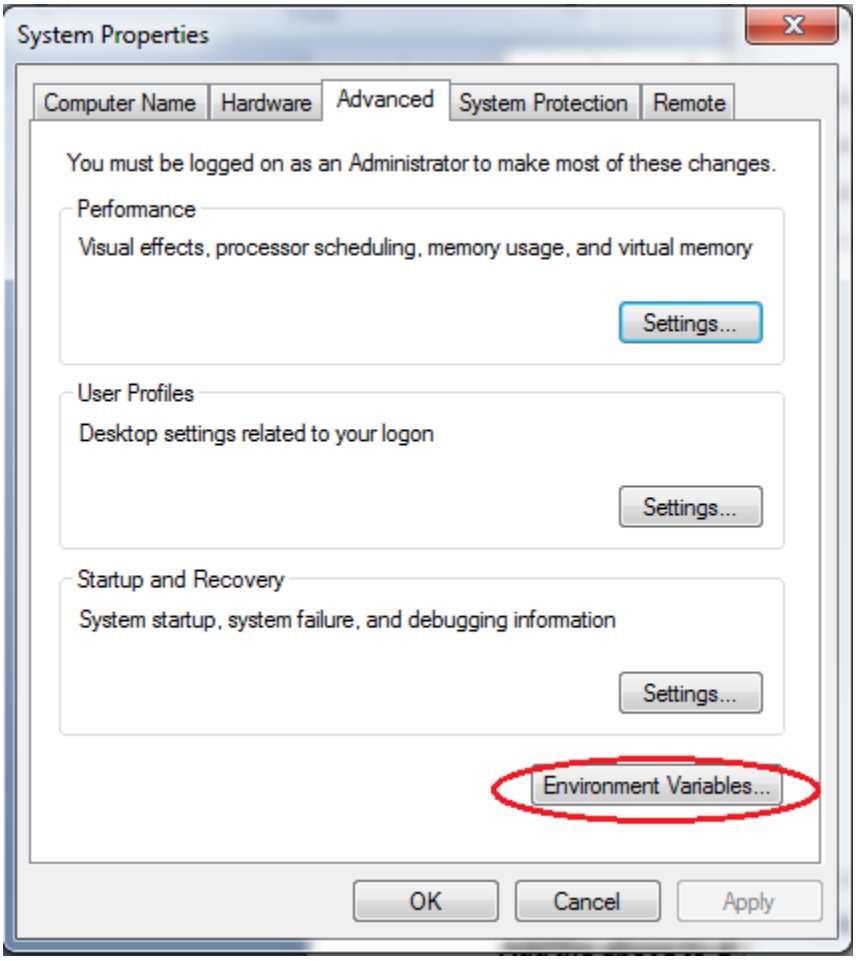
Pic17

Step 3 Add paths to system variables

Add path to system variables (Win 7, 2008 - Control Panel\System and Security\System\Advanced system settings\Environment Variables) :

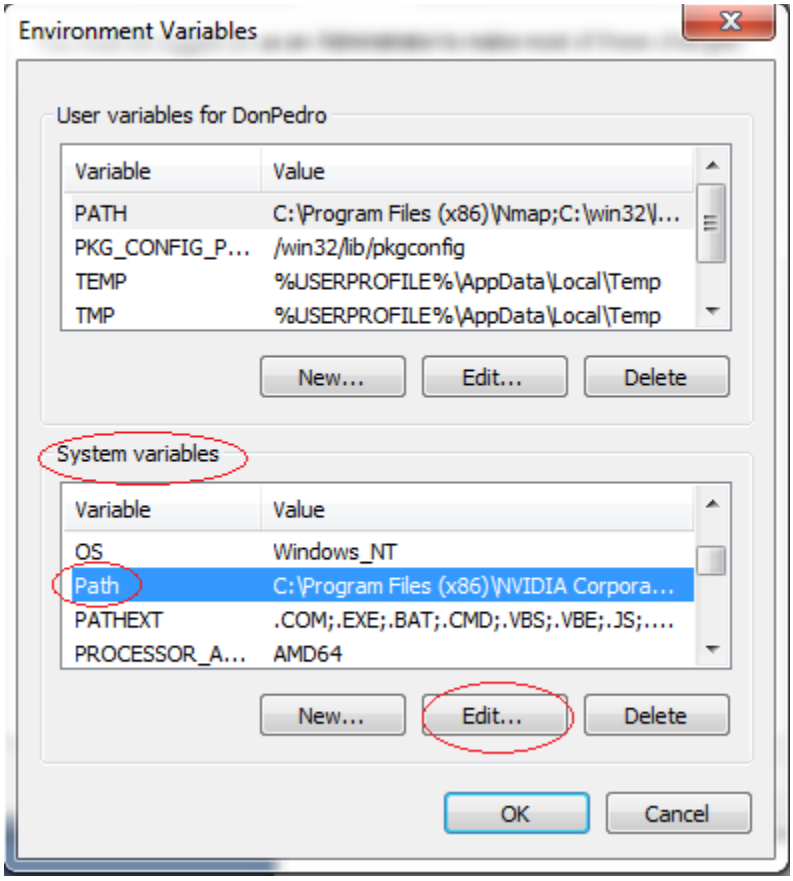
C:\cygwin\bin;C:\cygwin\lib\pkgconfig;

Add the above to environment system variables in your windows system!!
See the picture below



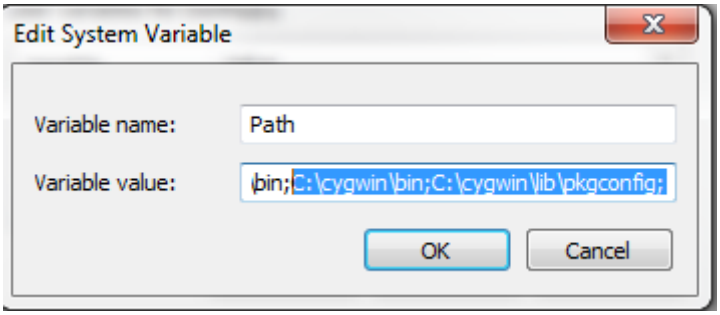
Pic18

Edit the system path variable:



Pic19

Add " C:\cygwin\bin;C:\cygwin\lib\pkgconfig; " without the quotes to the end of the " Variable value path " :



Pic20

Step 4 Get libyaml

Go to http://pyyaml.org/wiki/LibYAML

Download the yaml package (at the time of this writing the current version is yaml-0.1.4.tar.gz)

http://pyyaml.org/download/libyaml/yaml-0.1.4.tar.gz.

Unpack it in :

C:\cygwin\tmp

After you have unpacked it you should have the following directory:

C:\cygwin\tmp\yaml-0.1.4

Step 5 Get libpcap – for windows

Go to

http://www.winpcap.org/install/default.htm

and download the WinPcap installer for windows (at the time of this writing the current version was 4.1.2)

Install the WinPcap (double click, and just use the default options, basically click next and ok until finished.)

After that is done go to

http://www.winpcap.org/devel.htm

This is IMPORTANT , this is the development pack, we need that for Suricata to be able to run on Windows.

Download the package

Unpack it anywhere you like.

Copy libraries (from the unpacked directory) like this:

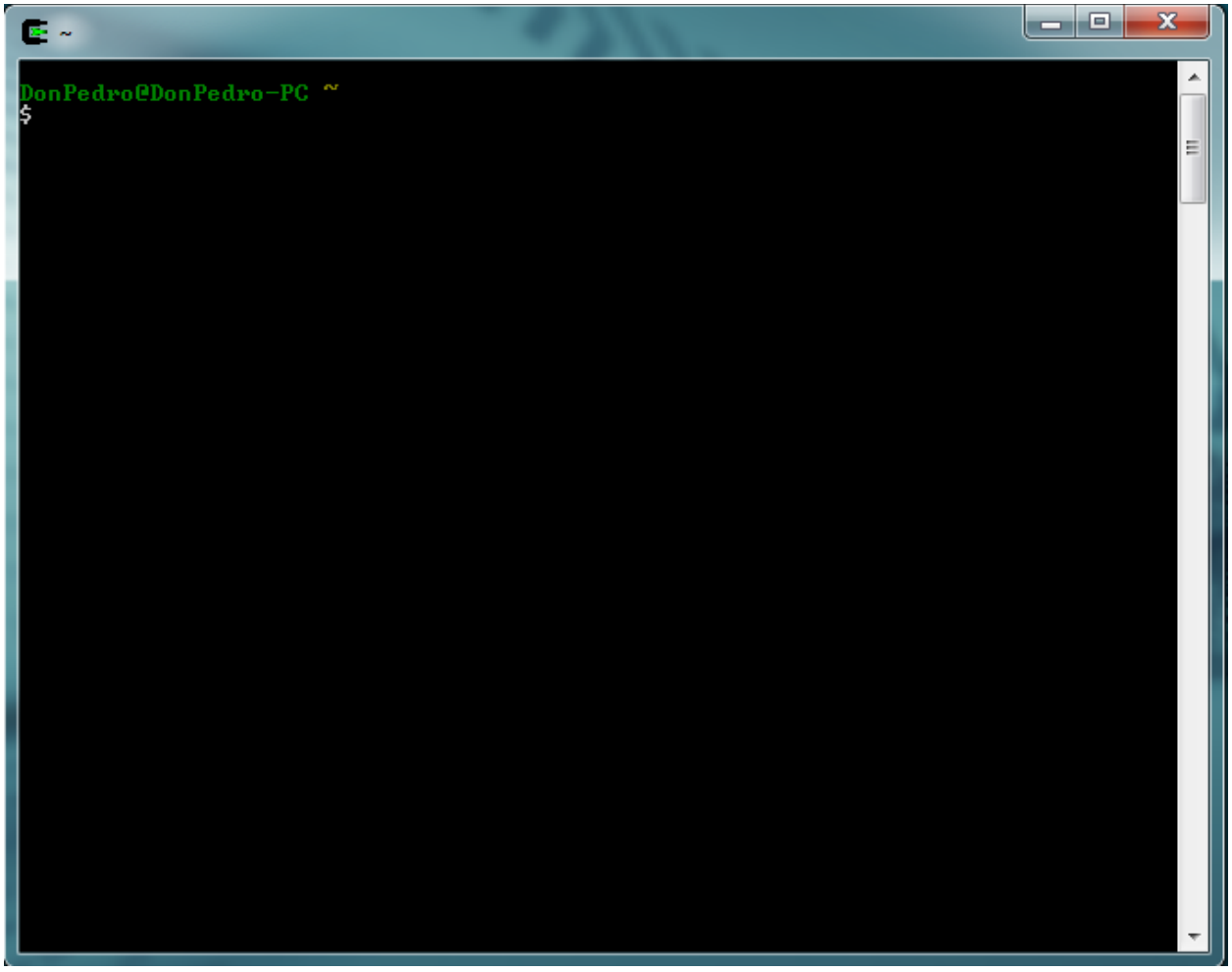
- ✓ **Copy ALL the content of WpdPack\Lib\ to cygwin\lib**
- ✓ **Copy all headers (all the content)from WpdPack\Include\ to C:\cygwin\usr\include**
- ✓ **Rename "libwpcap" to "libpcap" (in your cygwin\lib\ directory)**

Step 6 Start Cygwin and compile yaml

Open CYGWIN

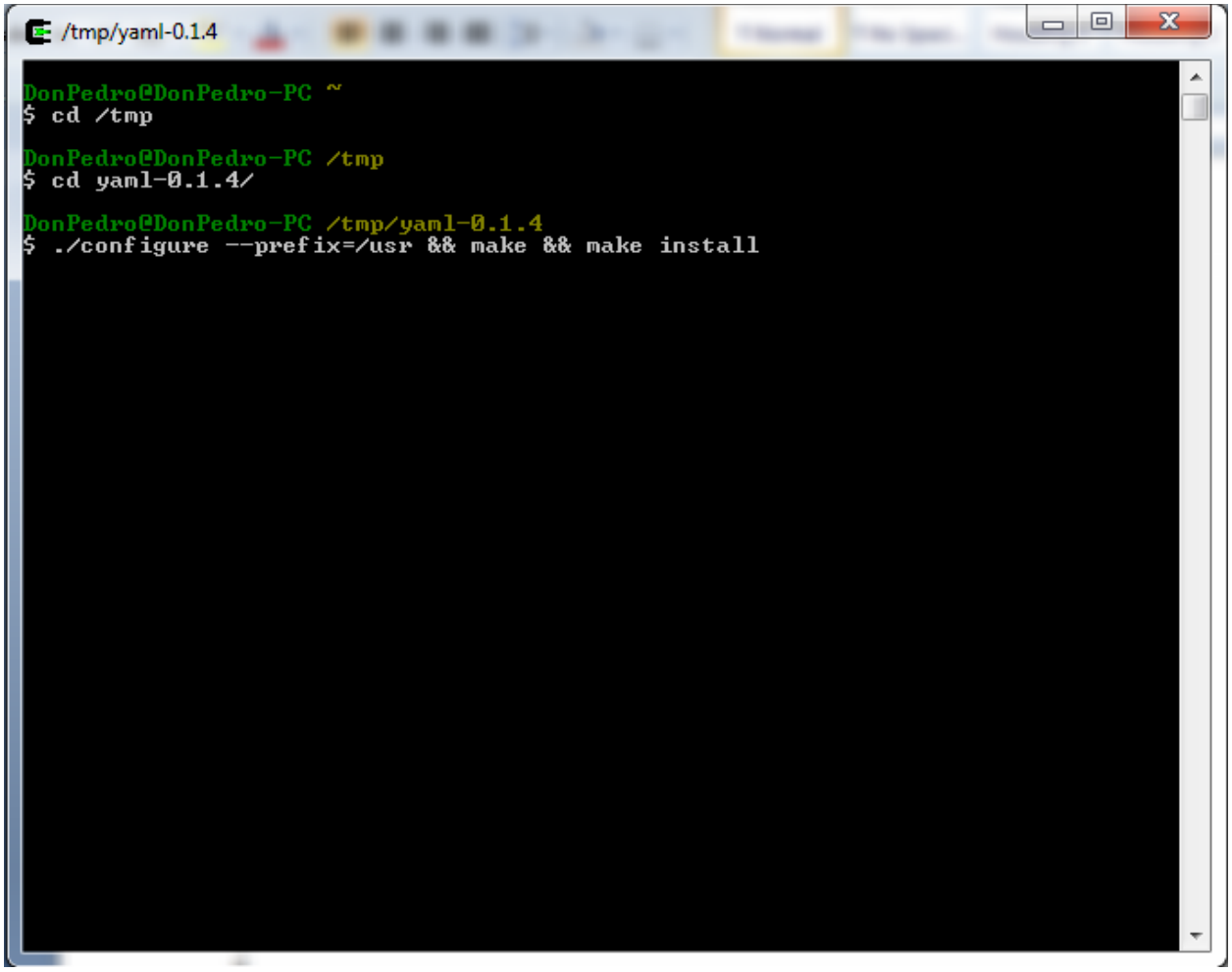
Double click your CYGWIN icon on your desktop.

A Linux/bash like command prompt will open:



Pic21

Type the following commands as shown in the picture below (hit enter after each command):



Pic22

Basically the commands are :

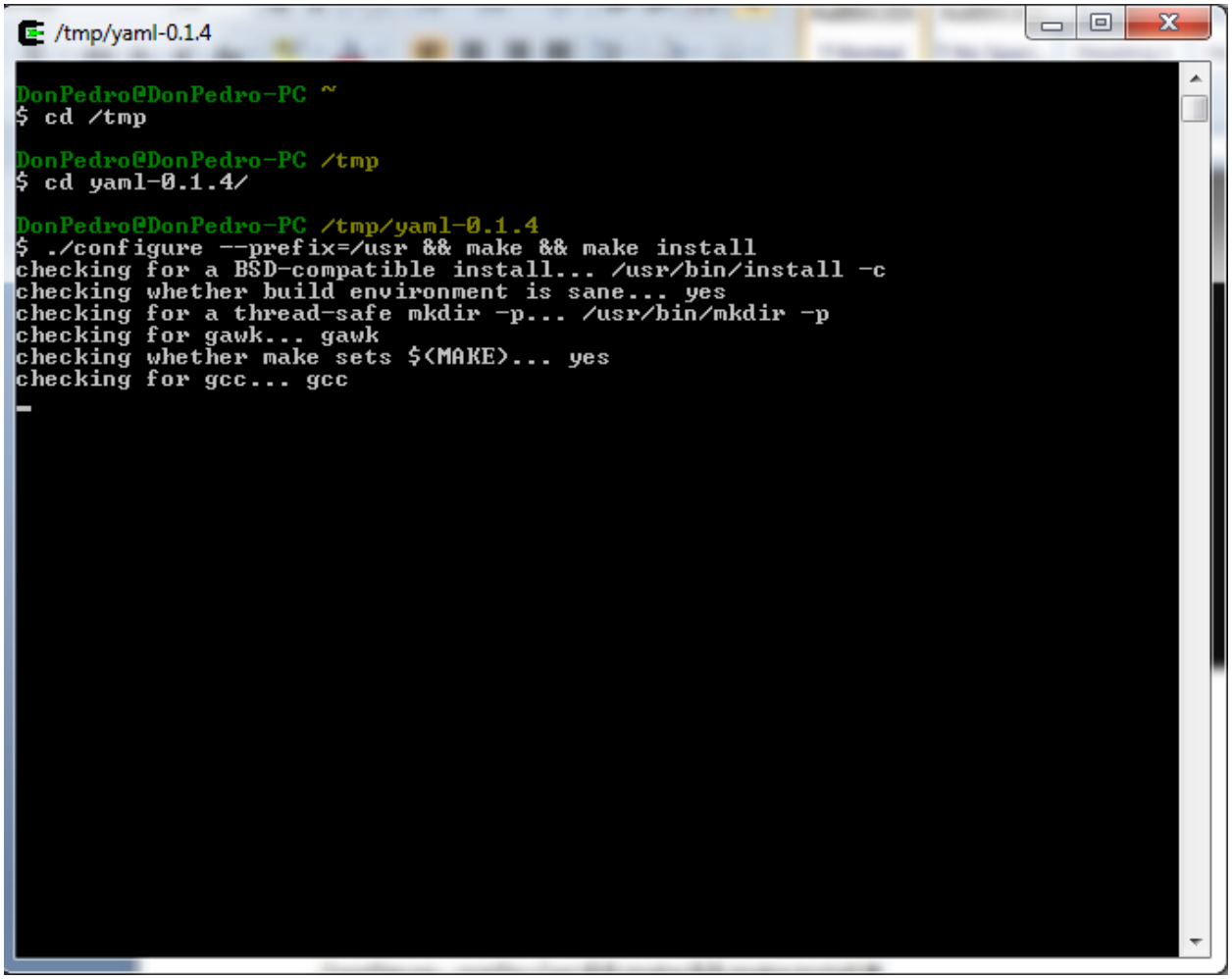
cd /tmp

cd yaml-0.1.4

./configure --prefix=/usr && make && make install

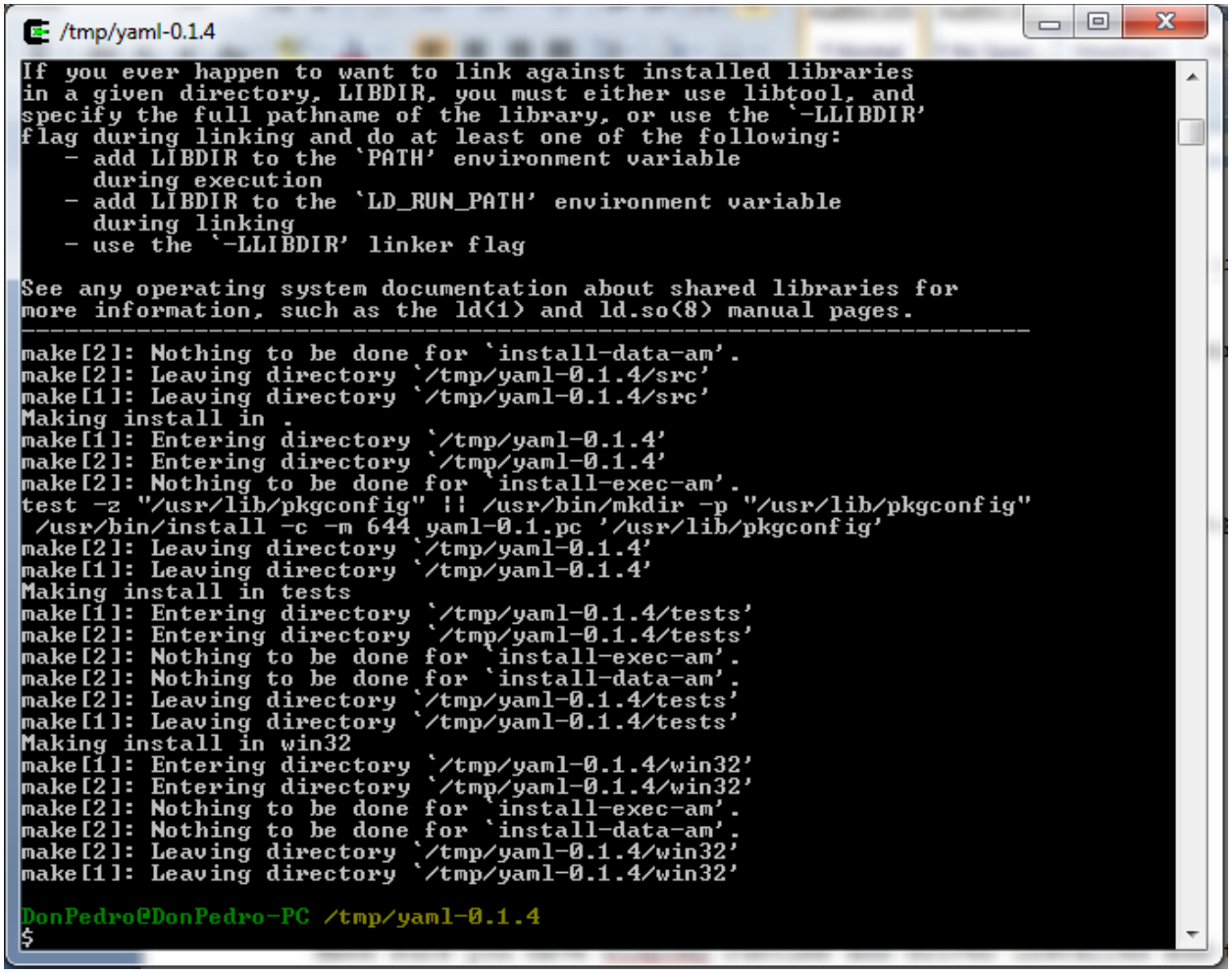
The last command above is on one line.

This will configure and install the yaml package that we need for Suricata, let it finish:



Pic23

After it is done, it should be something like this:



Pic24

Then go up one directory.

“ cd .. “

Step 7 Compile Suricata

Step 7.1 – Suricata from git – latest version

(Step 7.2 – follows just after (7.1) – Suricata stable – latest stable release , if you would like to use the stable version, please go to 7.2)

Get and compile Suricata.

As you are still in the CYGWIN environment -

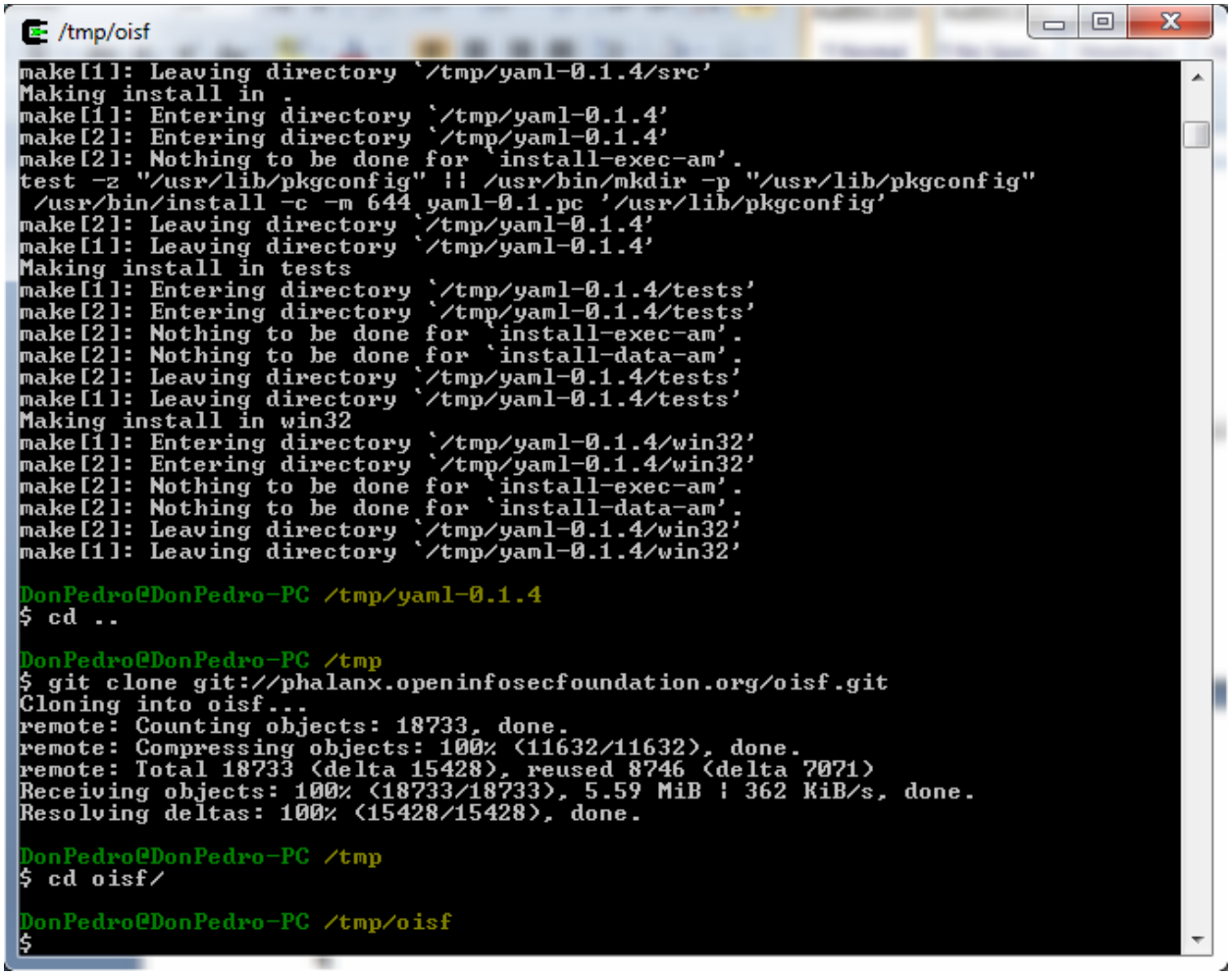
Type in

git clone git://phalanx.openinfosecfoundation.org/oisf.git

Then after it is done

cd oisf

like so:

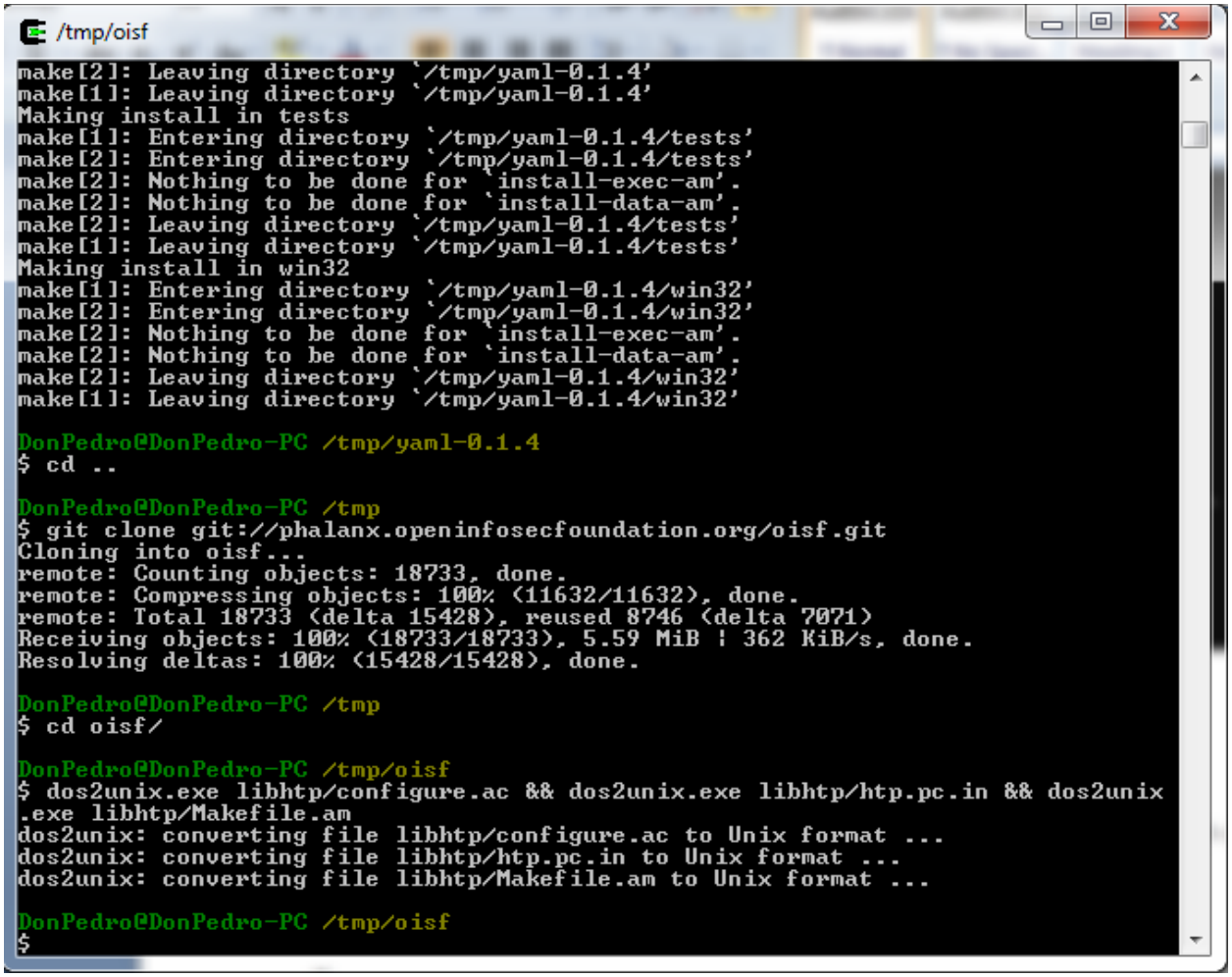


Pic25

After that we execute the following (one line):

dos2unix.exe libhtp/configure.ac && dos2unix.exe libhtp/htp.pc.in && dos2unix.exe libhtp/Makefile.am

Like so:



Pic26

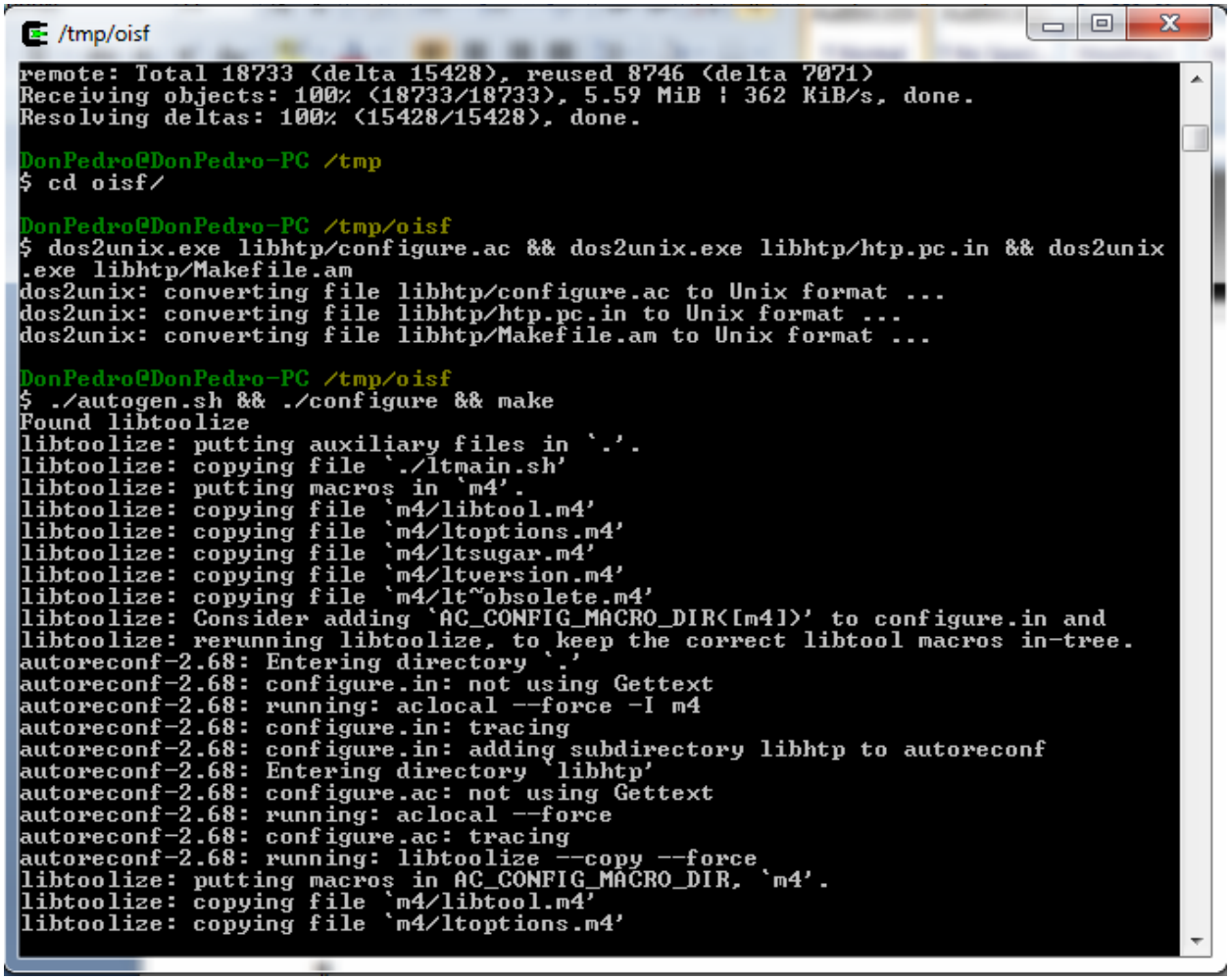
Then we execute the following command:

./autogen.sh && ./configure && make

The above command is on one line

That will start configuration and compilation of Suricata.

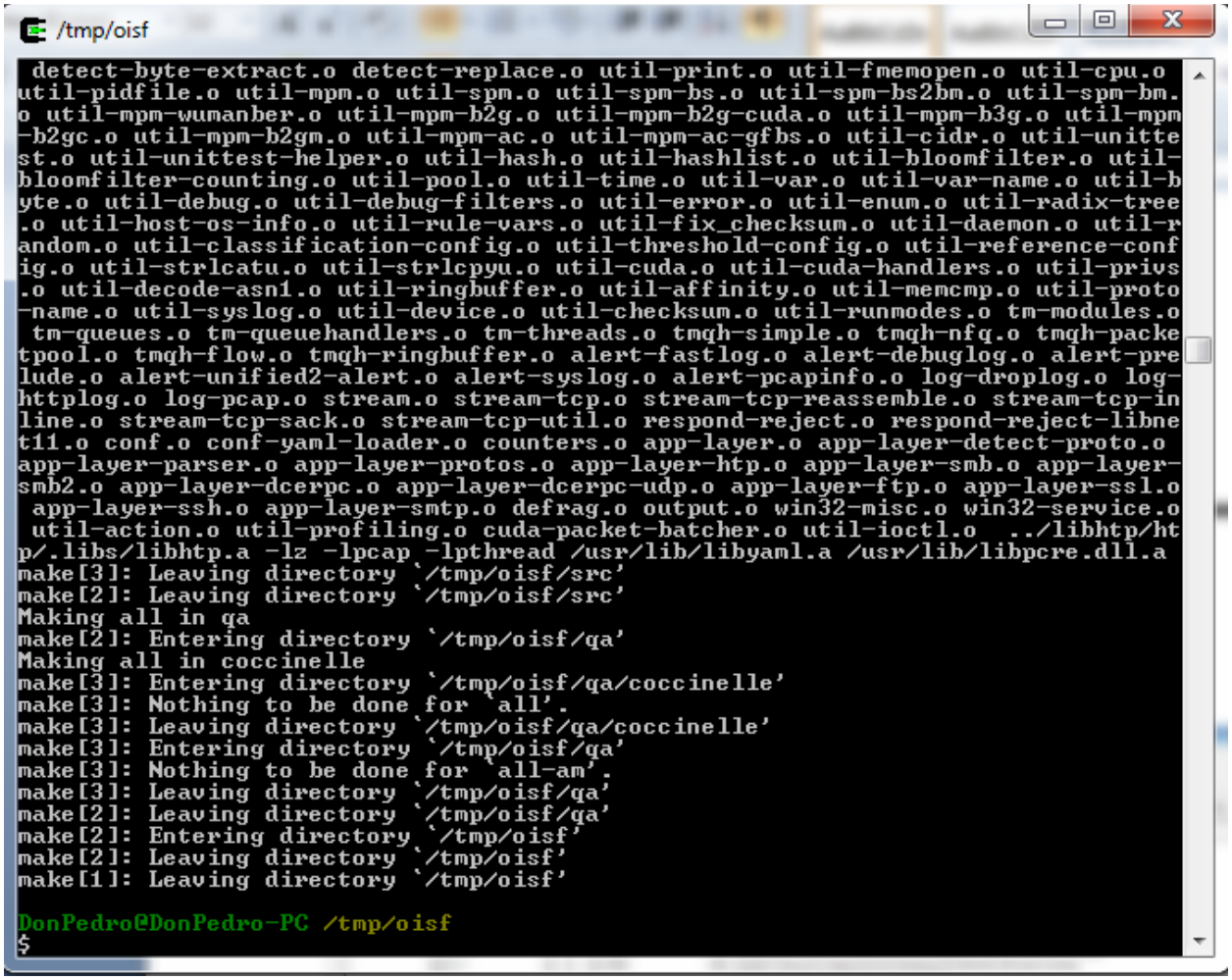
Like so:



Pic27

Let it run…..this could take 10 min. or so

After it is done:



Pic28

Step 7.2 Suricata stable

Get and compile Suricata.

As you are still in the CYGWIN environment -

Suricata Stable (at the moment of this writing the stable version is 1.2.1):

If you want to install Suricata stable – latest stable version (production)

(You can find it here - http://www.openinfosecfoundation.org/index.php/download-suricata)

go to a tmp dir. Type in (if you do not have "wget" installed - go ahead and install it the very same way you searched and added/installed the other pkgs to Cygwin) :

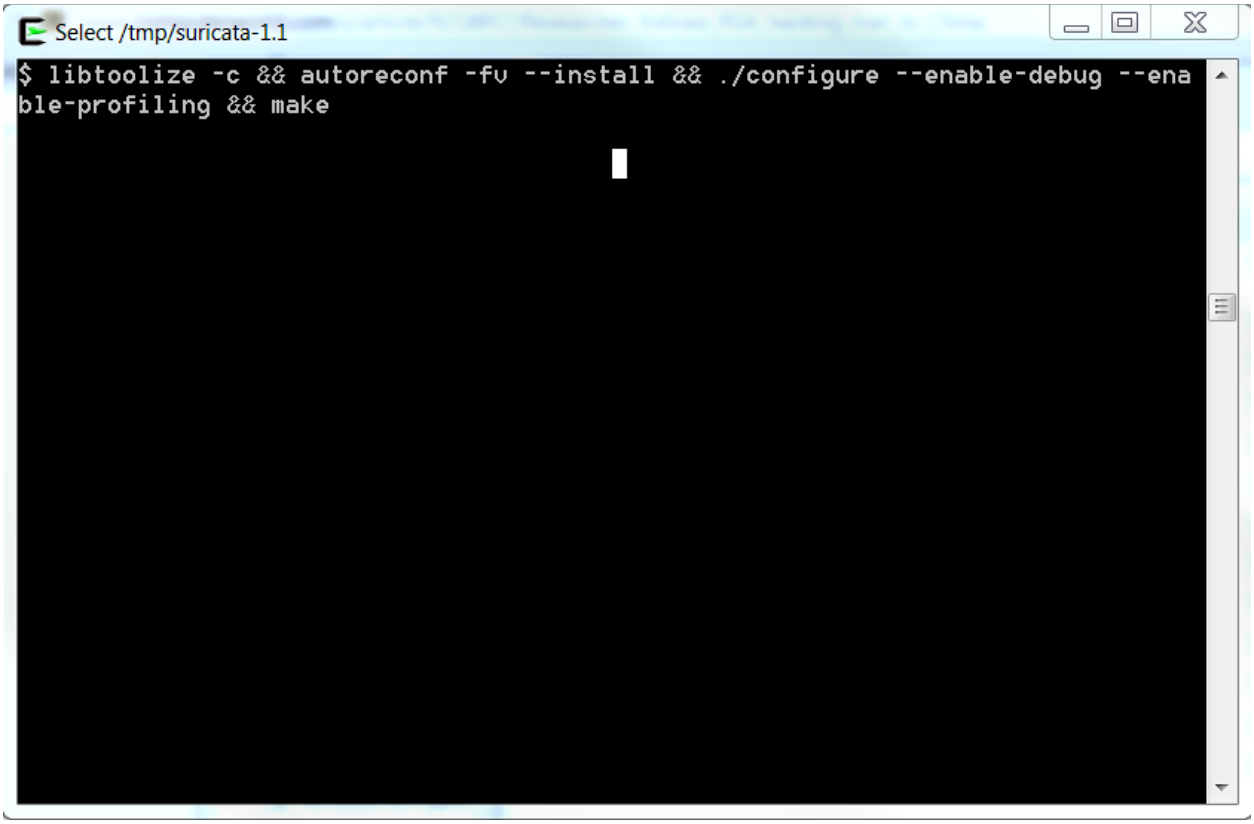
f) *wget http://www.openinfosecfoundation.org/download/suricata-1.2.1.tar.gz*

g) *tar –zxf suricata-1.2.1.tar.gz*

h) *cd suricata-1.2.1*

i) *dos2unix.exe libhtp/configure.ac && dos2unix.exe libhtp/htp.pc.in && dos2unix.exe libhtp/Makefile.am*

j) *libtoolize -c && autoreconf -fv --install && ./configure && make*



(--enable-debug and --enable-profiling are optional, you do not have to add them, I just add them because I like them, (pic above))☺

Then continue with the instructions below, just substitute the **oisf** directory with **suricata-1.2.1** directory!

Step 8 Set up Suricata for Windows

Create a directory C:\Suricata – you can use Win Explorer, you don't need to make it from Cygwin.

Then copy the Suricata.exe file from C:\cygwin\tmp\oisf\src\.libs

To

C:\Suricata

Create a directory C:\Suricata\log

Then create a directory C:\Suricata\rules

This will hold the rule files for Suricata.

Go to http://rules.emergingthreats.net/open/suricata/

Download a rule set.

http://rules.emergingthreats.net/open/suricata/emerging.rules.tar.gz

Or download rules from http://www.snort.org/ , whichever you like, however Emerging Threats are developing rules especially for Suricata, in order to use its capabilities to a full extend.

Unzip/untar the rule set in the C:\Suricata\rules directory.

Then go to C:\cygwin\tmp\oisf

Copy

classification.config , reference.config and suricata.yaml to

C:\Suricata

Open suricata.yaml with an editor – Notepad, Notepad++, whichever you like.

Change the following lines:

default-log-dir: C:\Suricata\log

……

- file:

enabled: yes

filename: C:\Suricata\suricata.log

…….

default-rule-path: C:\Suricata\rules

classification-file: C:\Suricata\classification.config

HOME_NET: "[192.168.0.0/16]" - (here actually you put any network you want Suricata to inspect)

Like shown on the pictures below:

suricata.yaml

```
# Preallocated size for packet. Default is 1514 which is the classical
# size for pcap on ethernet. You should adjust this value to the highest
# packet size (MTU + hardware header) on your system.
#default-packet-size: 1514

# Set the order of alerts bassed on actions
# The default order is pass, drop, reject, alert
action-order:
  - pass
  - drop
  - reject
  - alert


# The default logging directory.  Any log or output file will be
# placed here if its not specified with a full path name.  This can be
# overridden with the -l command line parameter.
default-log-dir: C:\Suricata\log

# Configure the type of alert (and other) logging you would like.
outputs:

  # a line based alerts log similar to Snort's fast.log
  - fast:
      enabled: yes
      filename: fast.log
      append: yes

  # log output for use with Barnyard
  - unified-log:
      enabled: no
      filename: unified.log

      # Limit in MB.
      #limit: 32
```

Normal text file | length : 23826 lines : 661 | Ln : 39 Col : 33 Sel : 0 | Dos\Windows | ANSI as UTF-8 | INS

Pic29

suricata.yaml

```
461   #
462   # This value is overriden by the SC_LOG_FORMAT env var.
463   #default-log-format: "[%i] %t - (%f:%l) <%d> (%n) -- "
464
465   # A regex to filter output.  Can be overridden in an output section.
466   # Defaults to empty (no filter).
467   #
468   # This value is overriden by the SC_LOG_OP_FILTER env var.
469   default-output-filter:
470
471   # Define your logging outputs.  If none are defined, or they are all
472   # disabled you will get the default - console output.
473   outputs:
474   - console:
475       enabled: yes
476   - file:
477       enabled: yes
478       filename: C:\Suricata\suricata.log
479   - syslog:
480       enabled: no
481       facility: local5
482       format: "[%i] <%d> -- "
483
484 # PF_RING configuration. for use with native PF_RING support
485 # for more info see http://www.ntop.org/PF_RING.html
486 pfring:
487   # Number of receive threads (>1 will enable experimental flow pinned
488   # runmode)
489   threads: 1
490
491   # Default interface we will listen on.
492   interface: eth0
493
494   # Default clusterid.  PF_RING will load balance packets based on flow.
495   # All threads/processes that will participate need to have the same
```

Normal text file | length : 23826 lines : 661 | Ln : 478 Col : 28 Sel : 11 | Dos\Windows | ANSI as UTF-8 | INS

Pic30

suricata.yaml

```
514 ipfw:
515
516   # Reinject packets at the specified ipfw rule number.  This config
517   # option is the ipfw rule number AT WHICH rule processing continues
518   # in the ipfw processing system after the engine has finished
519   # inspecting the packet for acceptance.  If no rule number is specified,
520   # accepted packets are reinjected at the divert rule which they entered
521   # and IPFW rule processing continues.  No check is done to verify
522   # this will rule makes sense so care must be taken to avoid loops in ipfw.
523   #
524   ## The following example tells the engine to reinject packets
525   # back into the ipfw firewall AT rule number 5500:
526   #
527   # ipfw-reinjection-rule-number: 5500
528
529 # Set the default rule path here to search for the files.
530 # if not set, it will look at the current working dir
531 default-rule-path: C:\Suricata\rules\
532 rule-files:
533  - emerging-current_events.rules
534
535 classification-file: C:\Suricata\classification.config
536 #reference-config-file: /etc/suricata/reference.config
537
538 # Holds variables that would be used by the engine.
539 vars:
540
541   # Holds the address group vars that would be passed in a Signature.
542   # These would be retrieved during the Signature address parsing stage.
543   address-groups:
544
545     HOME_NET: "[192.168.0.0/16]"
546
547     EXTERNAL_NET: any
548
549     HTTP_SERVERS: "$HOME_NET"
```

Normal text file | length : 23826 | lines : 661 | Ln : 531 | Col : 31 | Sel : 11 | Dos\Windows | ANSI as UTF-8 | INS

Pic31

Adjust your home network to whatever network you intend the Suricata to protect/inspect (as shown in the picture above).

Step 9 Runing Suricata

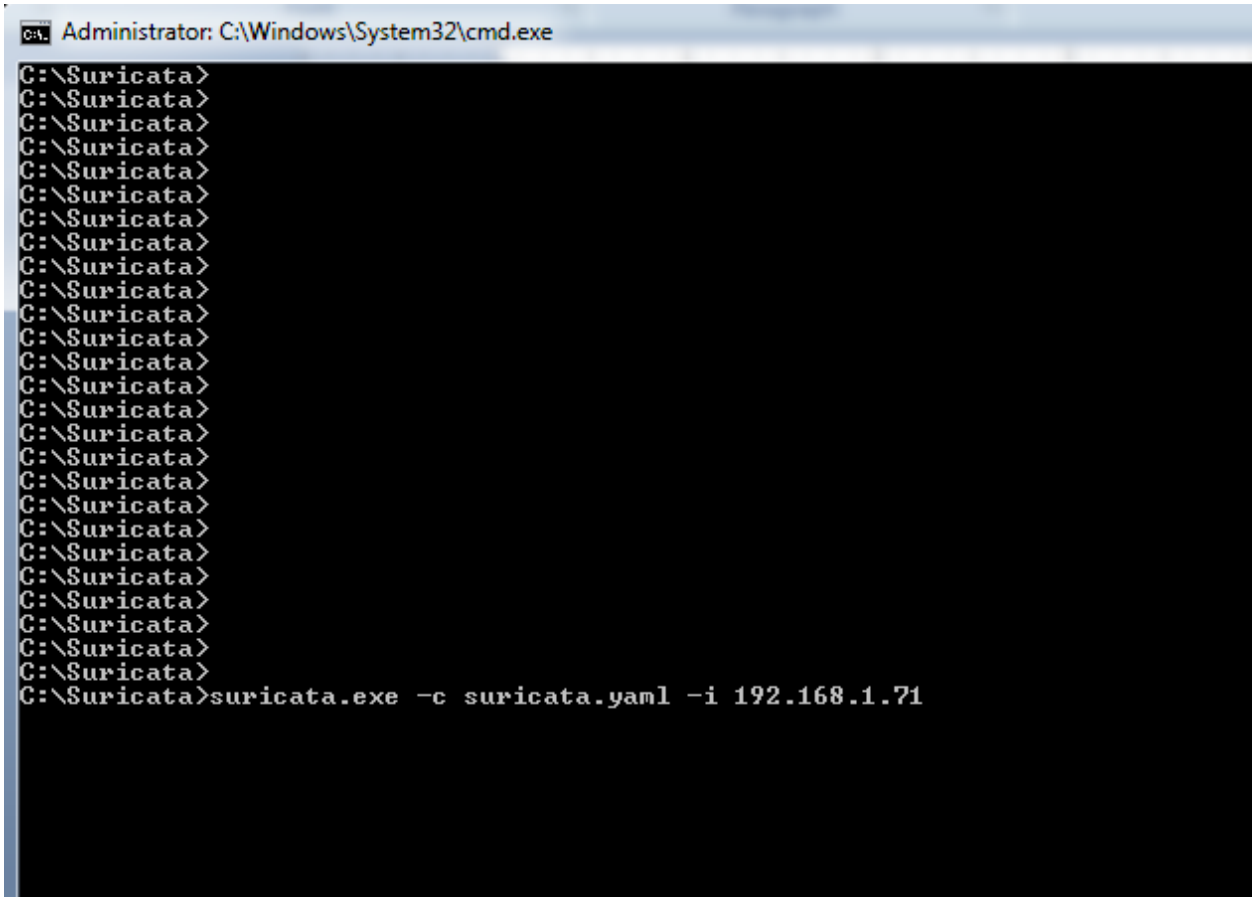
….run intruders run…

Open a cmd as ADMINISTRATOR!!!.

Got to C:\Suricata and execute

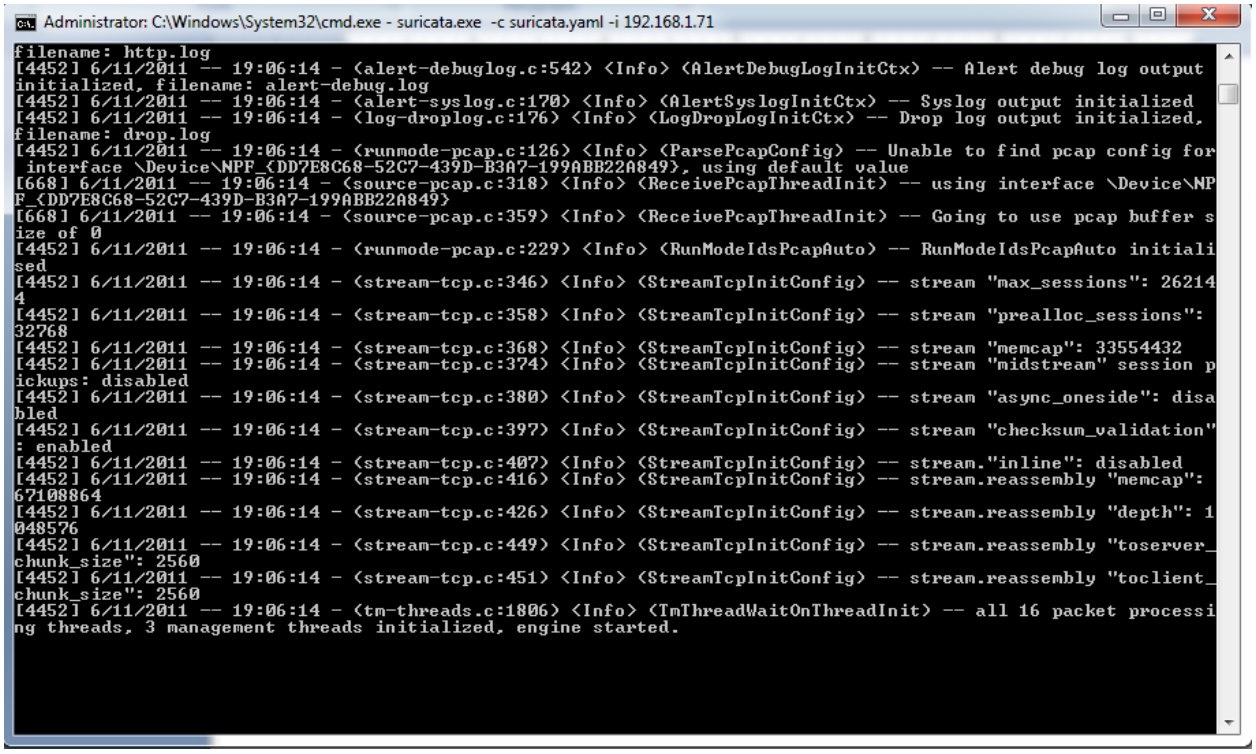
suricata.exe -c suricata.yaml -i 192.168.1.71

like shown on the picture below (in this case - 192.168.1.71 is the IP/interface I want Suricata to listen to, i.e. the IP that my network card has been configured with):



Pic32

And you have yourself Suricata running (the start time could depend the PC/Server CPU/MEM availability and of course how many rules do you load, but it is max about 1.5 min):



Pic33

That's it.

From here on it is up to you to configure Suricata the way it suits you best!

Thanks

More info and documentation

You can find much more info about setting up and tuning Suricata here:

https://redmine.openinfosecfoundation.org/projects/suricata/wiki


OISF
OPEN INFORMATION SECURITY FOUNDATION


SURICATA


SURICATA


OISF
OPEN INFORMATION SECURITY FOUNDATION