# Binary parsing and visualization

## Summary

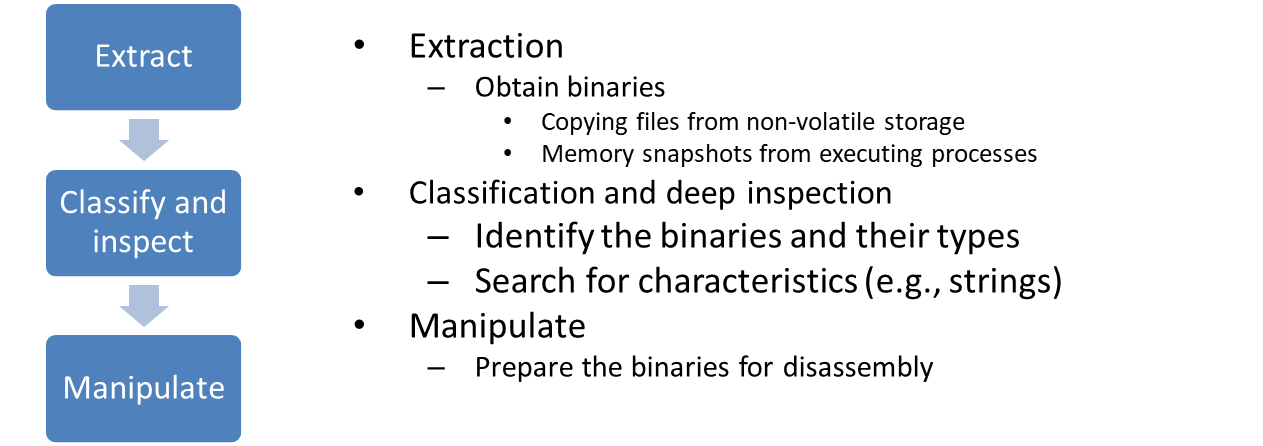
In this class exercise, we will introduce you to methods for automating parsing of binary file formats and visualizing their contents.

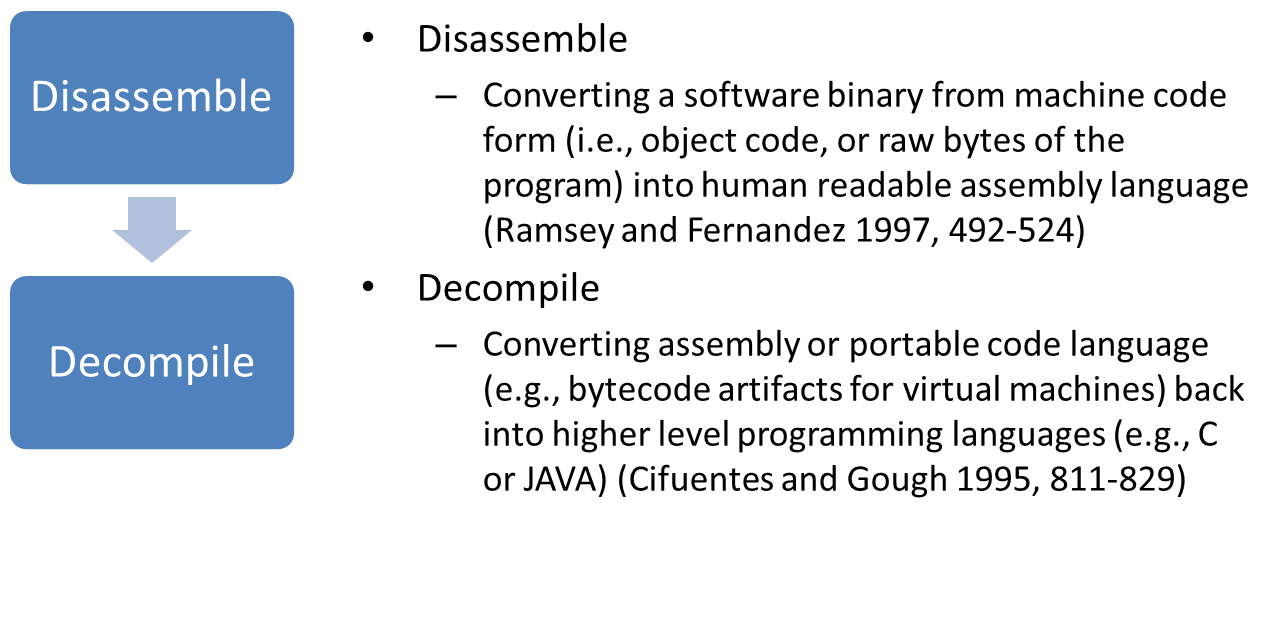
## Prerequisites

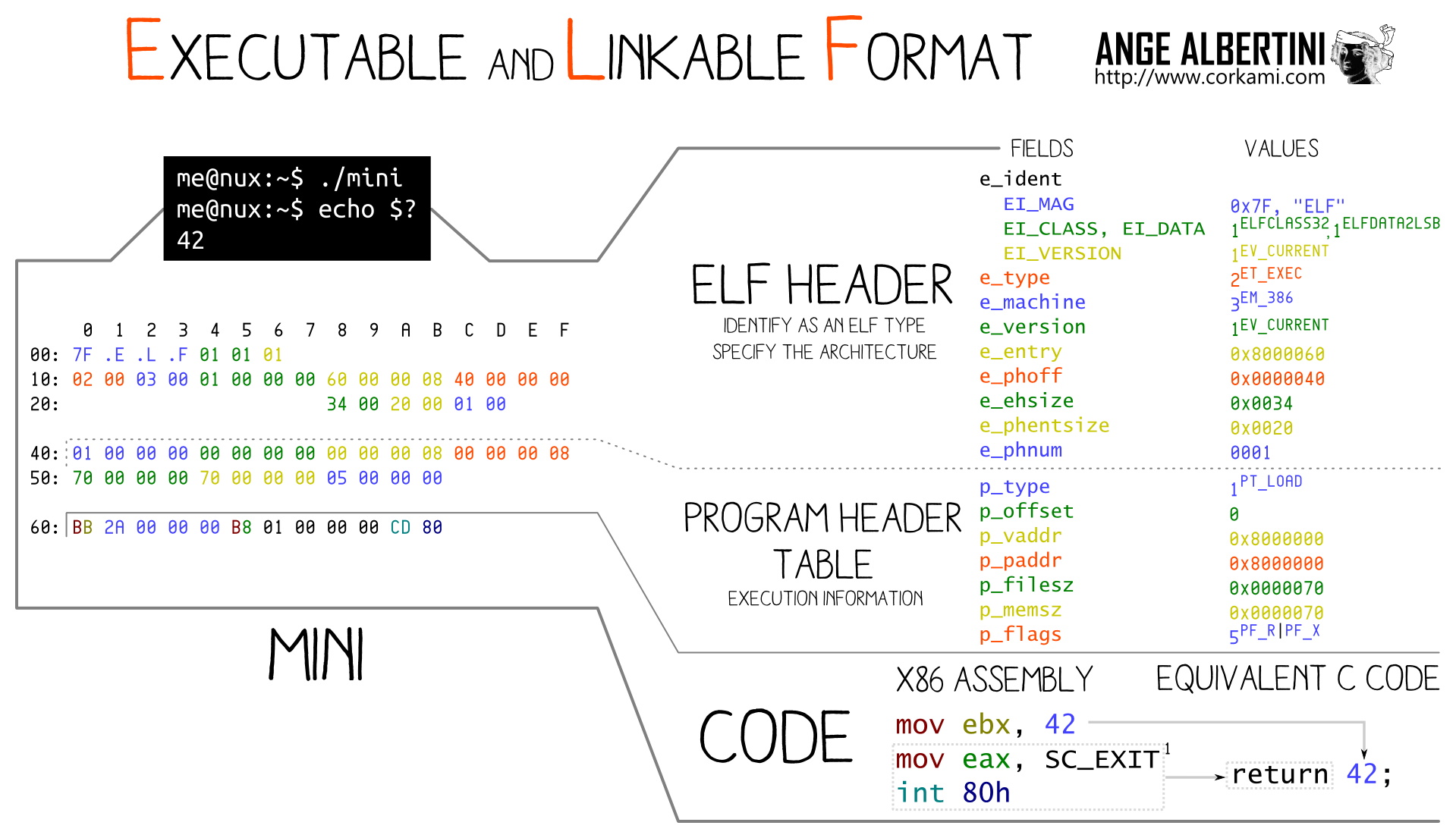
* Ubuntu Linux VM setup for development

## Details









### Parsing

* Install Kaitai struct compiler
* Import GPG key, if you never used any BinTray repos before
  + $ sudo apt-key adv --keyserver hkp://pool.sks-keyservers.net --recv 379CE192D401AB61
* Add stable repository
  + $ echo "deb https://dl.bintray.com/kaitai-io/debian jessie main" | sudo tee /etc/apt/sources.list.d/kaitai.list
* Install compiler
  + $ sudo apt-get update
  + $ sudo apt-get install kaitai-struct-compiler
* Install the kaitaistruct python package
  + $ pip install kaitaistruct
* Install ruby
* $ sudo apt-get install ruby
* Install kaitai struct visualizer
* $ sudo gem install kaitai-struct-visualizer
* Get the .ksy files
* $ git clone https://github.com/kaitai-io/kaitai\_struct\_formats.git
* Compile the .ksy file for .elf
* $ ksc kaitai\_struct\_formats/executable/elf.ksy -t python
* $ python

>>> import elf

>>> data=elf.Elf.from\_file("sandbox/HelloWorld/hello.elf")

>>> data.magic

* $ ksv sandbox/HelloWorld/hello.elf kaitai\_struct\_formats/executable/elf.ksy

### Visualization

* $ sudo apt-get install pkg-config libcairo2-dev tcl libopenjp2-7-dev liblcms2-dev zlib1g-dev libwebp-dev libfreetype6 libtiff-dev libjpeg-dev
* $ pip install pycairo
* $ git clone <https://github.com/cortesi/scurve.git>
* $ ./binvis ../HelloWorld/hello.elf
* $ eog hello.png
* Download Veles from <https://github.com/codilime/veles/releases/download/2018.05.0.TIF/Veles_2018.05_64bit_Ubuntu1604.deb>
* Install Veles
* $ sudo apt install ~/Downloads/Veles\_2018.05\_64bit\_Ubuntu1604.deb
* Run it
* $ veles
* Open hello.elf (File->Open)
* Start the visualization
* Dump the memory sections in another terminal using $ objdump -h hello.elf
* Select various ranges in the entropy plot for the memory sections

### Definitions

* N/A

### References

* [www.corkami.com](http://www.corkami.com/)
* [http://kaitai.io](http://kaitai.io/#download)
* <http://doc.kaitai.io/user_guide.html>
* <http://formats.kaitai.io/elf/>
* <https://corte.si/posts/visualisation/binvis/index.html>
* <https://github.com/codilime/veles>