ANALYSIS OF (UNKNOWN) FILE FORMATS

22nd September 2011

Mario Suvajac

REVERSING LABS

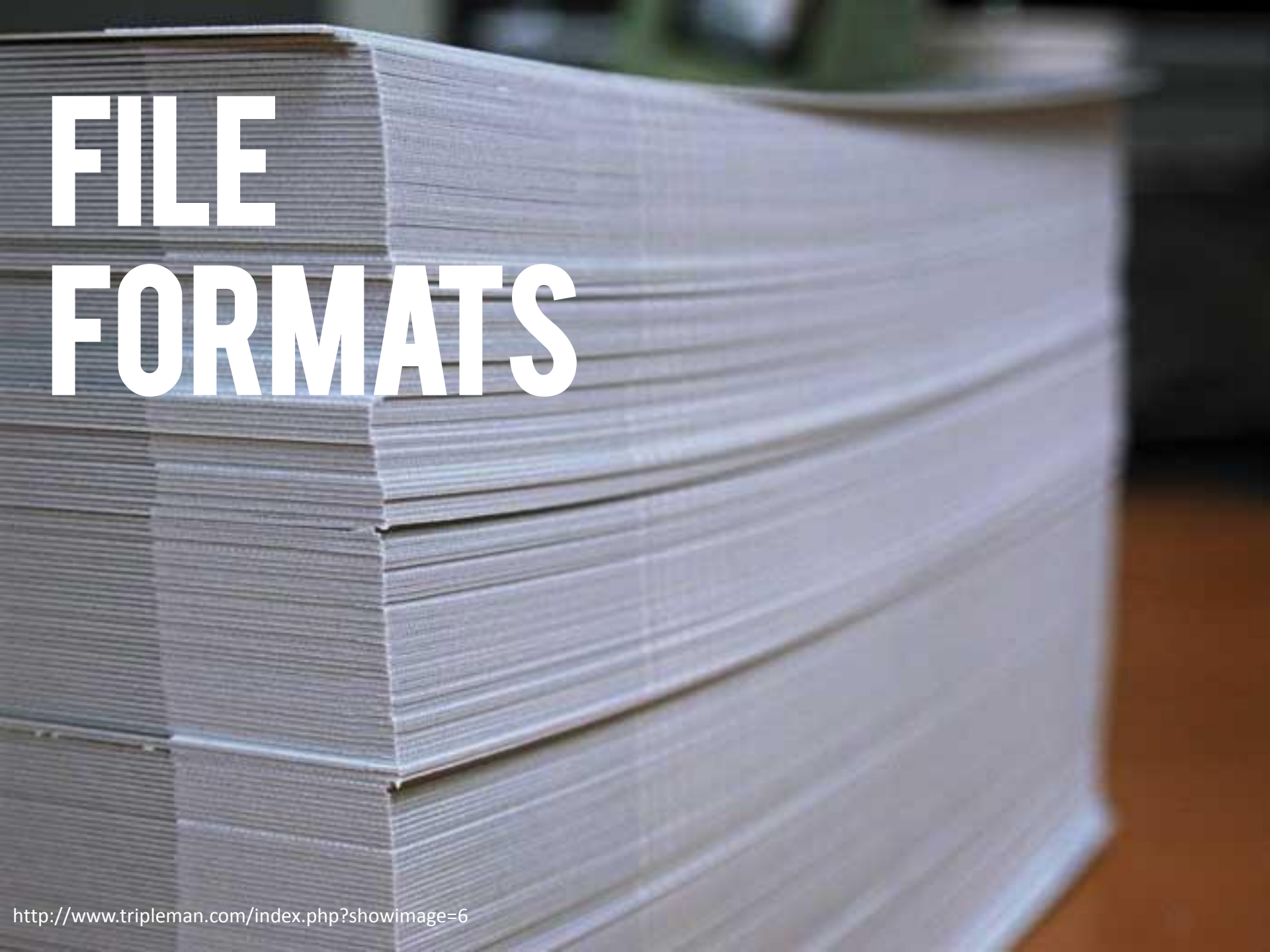
HI, I'M MARIO SUVAJAC

@msuvajac

suvajac.org

reversinglabs.com

FILE FORMATS



http://www.tripleman.com/index.php?showimage=6

FILE FORMATS

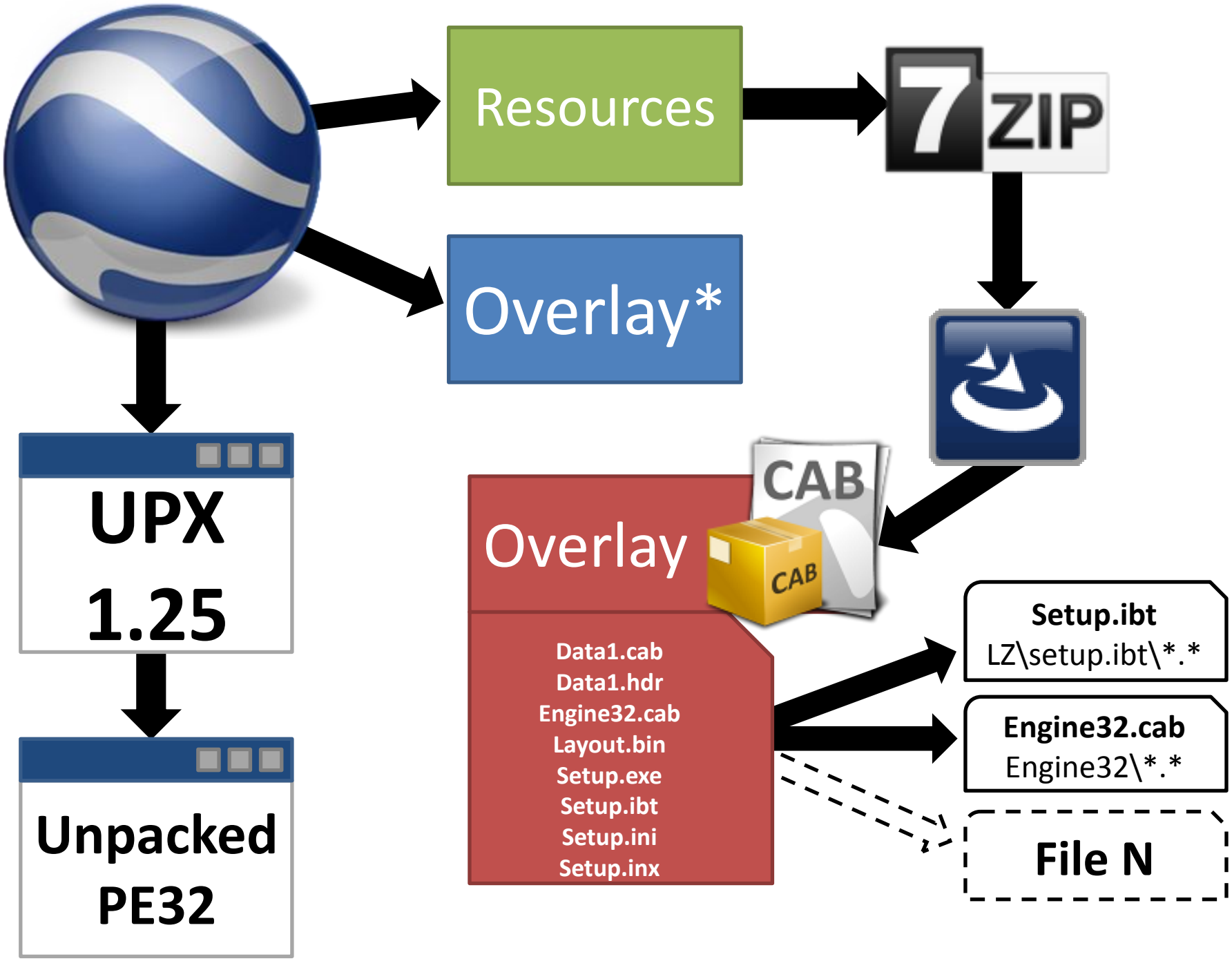
- Structured information storage/carriers
  - Compressed
  - Encrypted
  - All of the above

CATEGORIZATION

http://www.flickr.com/photos/fotomele/1072932978

CATEGORIZATION

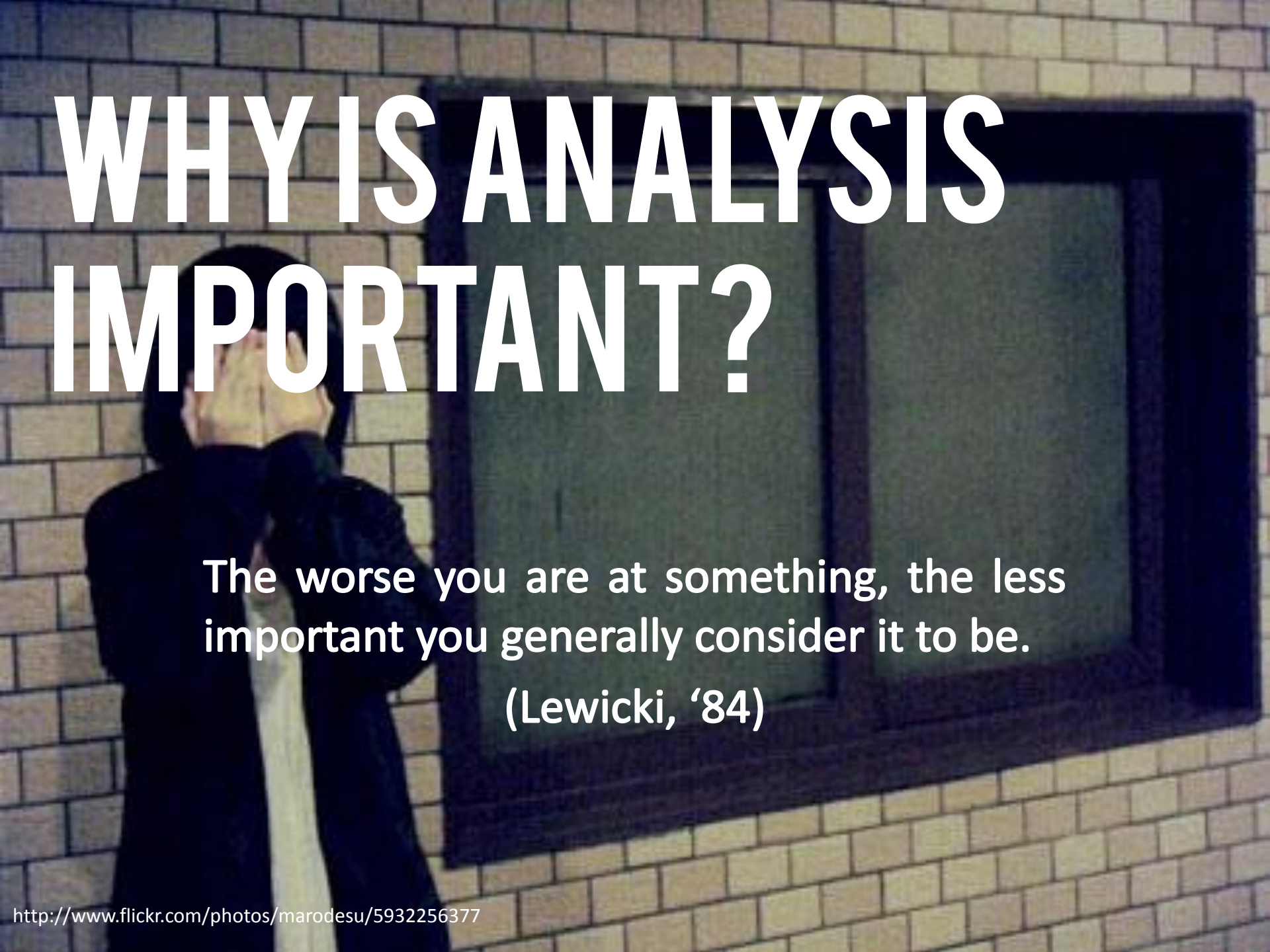
- Availability
  - Open
  - Proprietary
- Different for each information type or contained in generalized container format
- Executables, archives...


Resources
7ZIP
Overlay*
UPX
1.25
Unpacked
PE32
Overlay
CAB
CAB
Data1.cab
Data1.hdr
Engine32.cab
Layout.bin
Setup.exe
Setup.ibt
Setup.ini
Setup.inx
Setup.ibt
LZ\setup.ibt*.*
Engine32.cab
Engine32*.*
File N

WHY IS ANALYSIS IMPORTANT?

The worse you are at something, the less important you generally consider it to be.

(Lewicki, '84)



http://www.flickr.com/photos/marodesu/5932256377

WHY IS ANALYSIS IMPORTANT?

- Writing unpackers & validators
  - Anti-virus protection
  - Computer forensics
  - General software development
  - ...

HOW TO DO IT?

http://www.flickr.com/photos/karenilagan/2163284814

HOW TO DO IT?

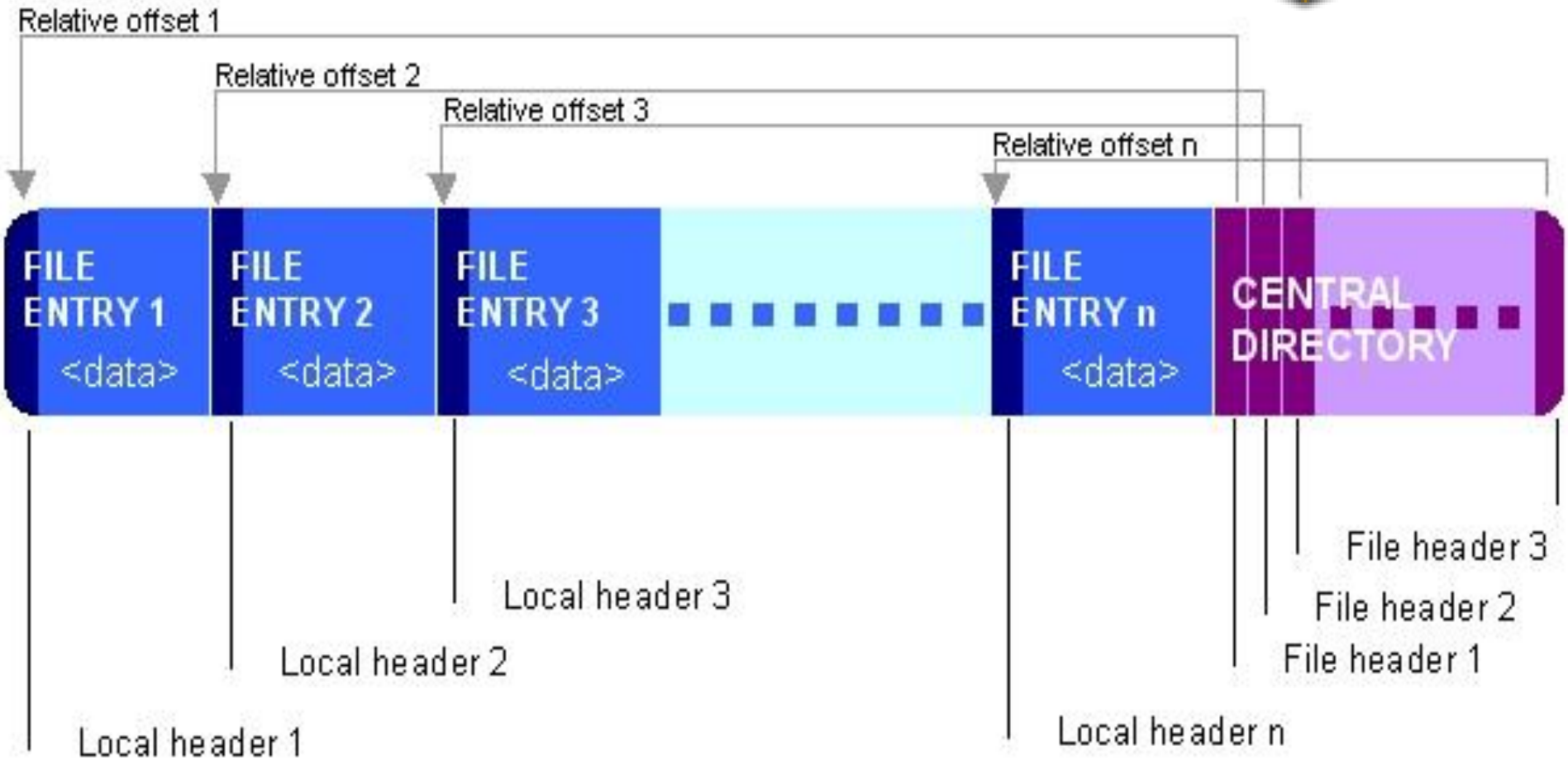
- Specifications
- Reverse Engineering
- Asking Please

http://www.flickr.com/photos/19666640@N00/2884433955

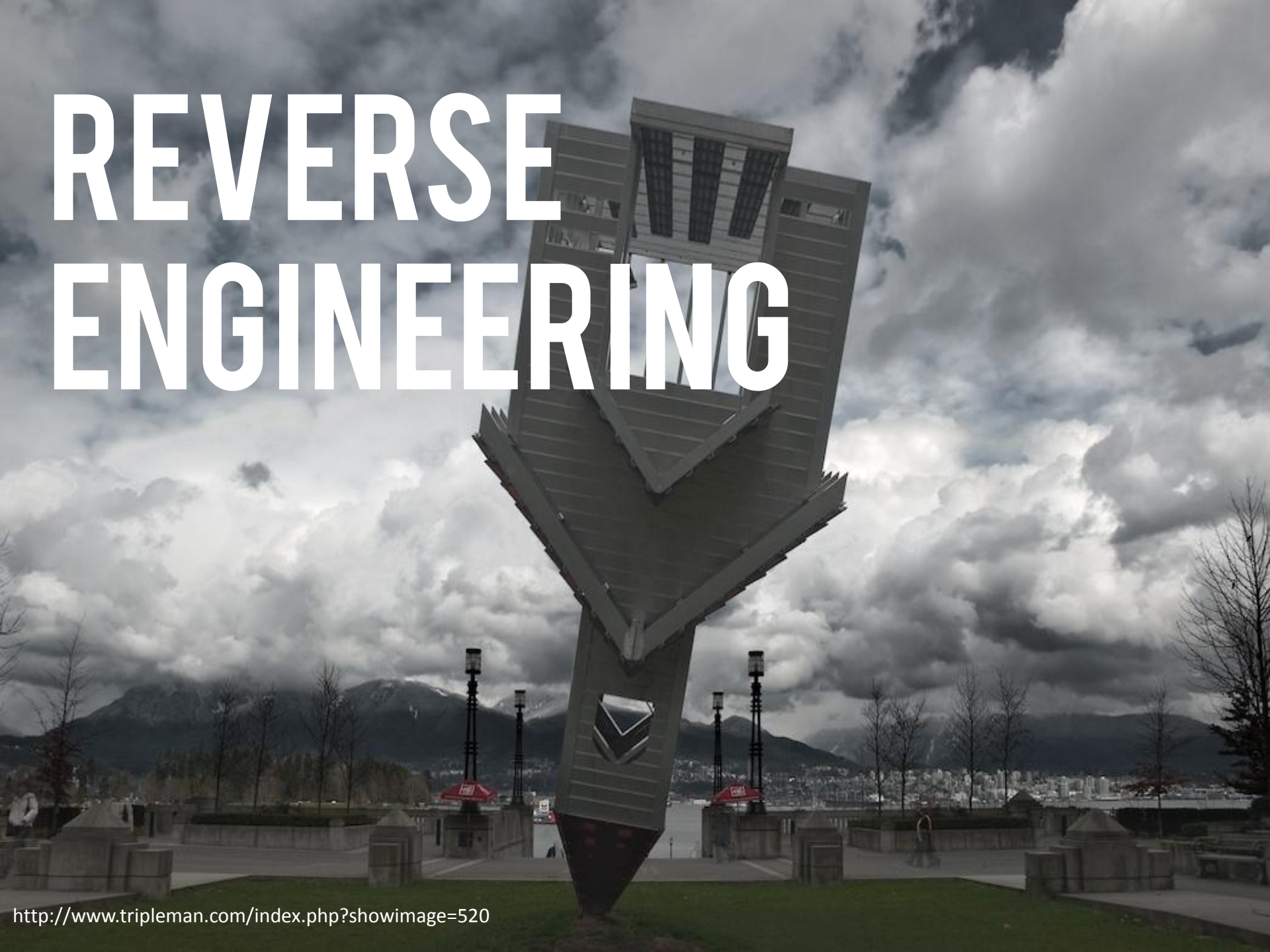
FILE FORMAT PATTERNS

- File header
  - Magic
  - Sizes
  - Offsets
  - Algorithm ids
  - Block descriptors
  - …
- Data

ZIP FILE FORMAT



REVERSE ENGINEERING



http://www.tripleman.com/index.php?showimage=520

BY JUST OBSERVING

- Experience based
- Hex editor
- Diffing’

BY DEBUGGING

- Watching reads & further data manipulation
- Compression & encryption algorithms reversing

CODING TIPS

http://www.flickr.com/photos/the8rgrl/4642045

CODING TIPS

- Security risks
- Problems in practice
- corelib

THANKS,
QUESTIONS?!
BTW. REVERSING LABS
IS HIRING