Function Identification and Recovery Signature Tool

Angel M. Villegas
Research Engineer

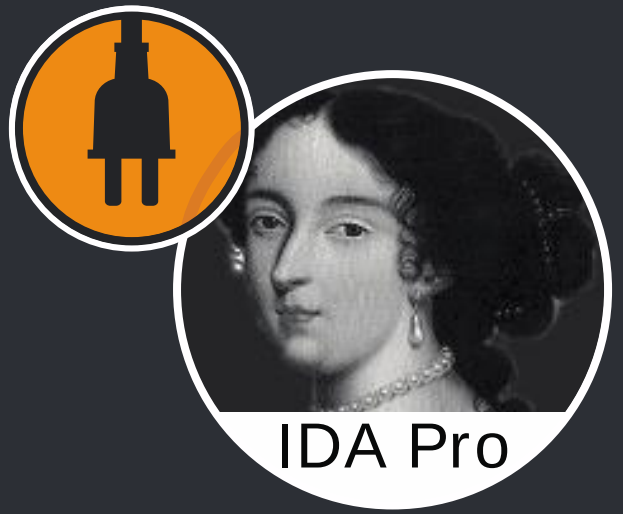
TALOS

BACKGROUND

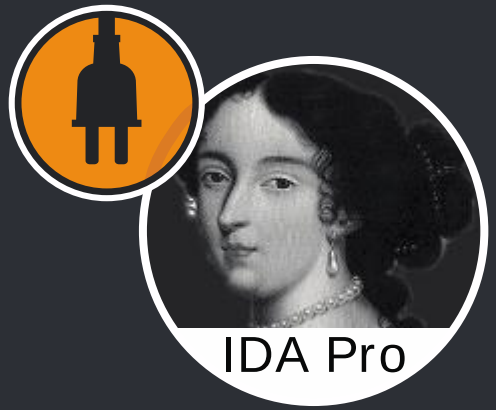
- Current reverse engineering process
  - Get a sample, analyze sample
    - Get next sample, analyze sample
      - Get next sample, analyze sample
        - » Rinse and repeat…
- Analysis work can be duplicated
  - For the analyst and others

FIRST

- FIRST: Function Identification and Recovery Signature Tool
- Streamlines code research
  - prevents duplicate effort
  - improves analysis time
- Flexible
  - Modular framework made for expanding



SYSTEM OVERVIEW



Check for Metadata

56 6A 0C 6A 01 E8 64 AB 00 00 …

Add Function Metadata

Name / Prototype / Comment

Update Function Metadata

With the most recent version

INSTALLATION

pip install requests

REQUIREMENTS

Python Requests Module
https://pypi.python.org/pypi/requests

OPTIONAL:
Requests-kerberos (if kerberos authentication is required)

GET THE PLUG-IN

Download Python Plug-in from
https://github.com/vrtadmin/FIRST-plugin-ida

Copy plug-in to IDA Pro plug-ins folder

Run IDA Pro

INSTALLATION

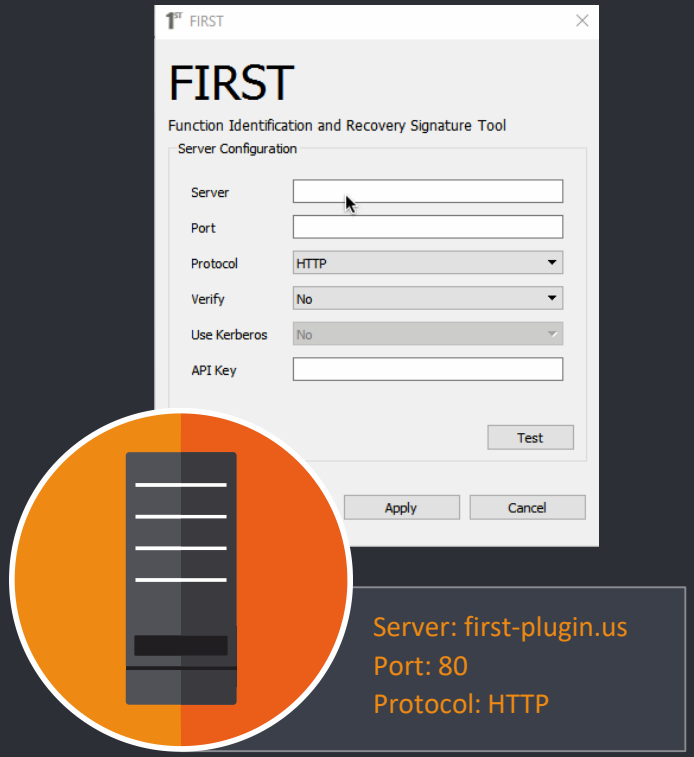
Windows:

```
pip install first-plugin-ida
C:\Python27\Scripts\first-plugin-ida
```

Mac:

```
pip install first-plugin-ida
/usr/local/bin/first-plugin-ida
```

CONFIGURATION



Server: first-plugin.us
Port: 80
Protocol: HTTP

OPTION 1

Enter configuration at the Welcome Screen (appears only when FIRST is not configured)

OPTION 2

- In IDA Pro View window

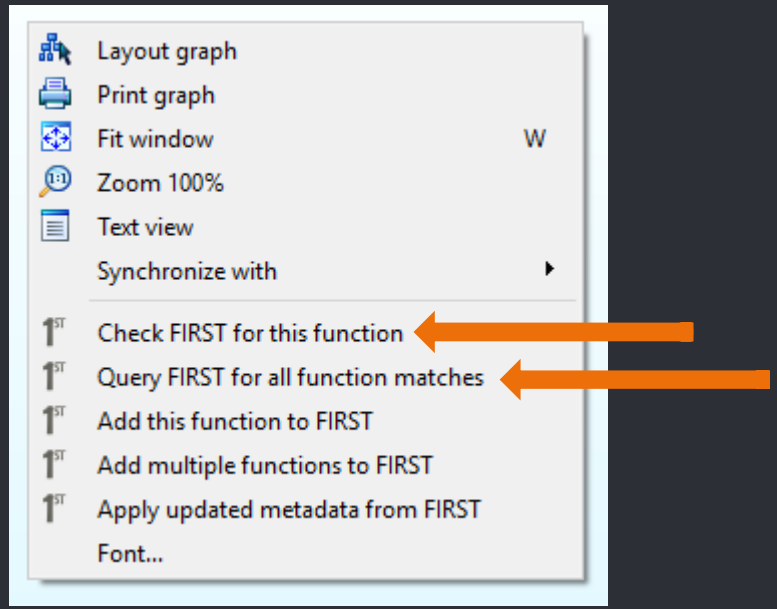
  Press ‘1’

- In IDA Pro’s menu

  Edit > Plugins > FIRST

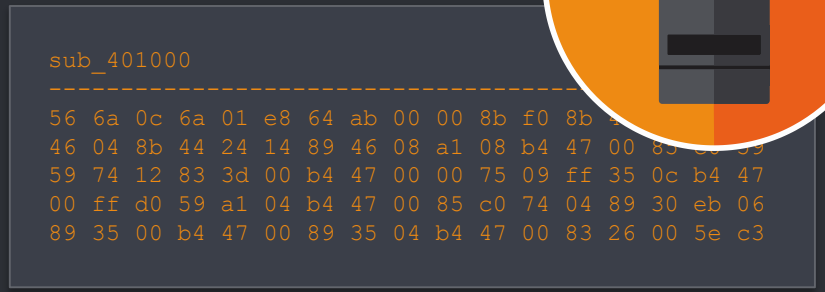
- Select Configuration

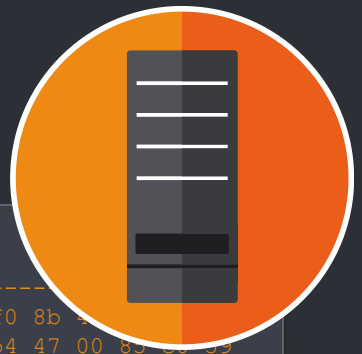
HOW THE PLUGIN WORKS



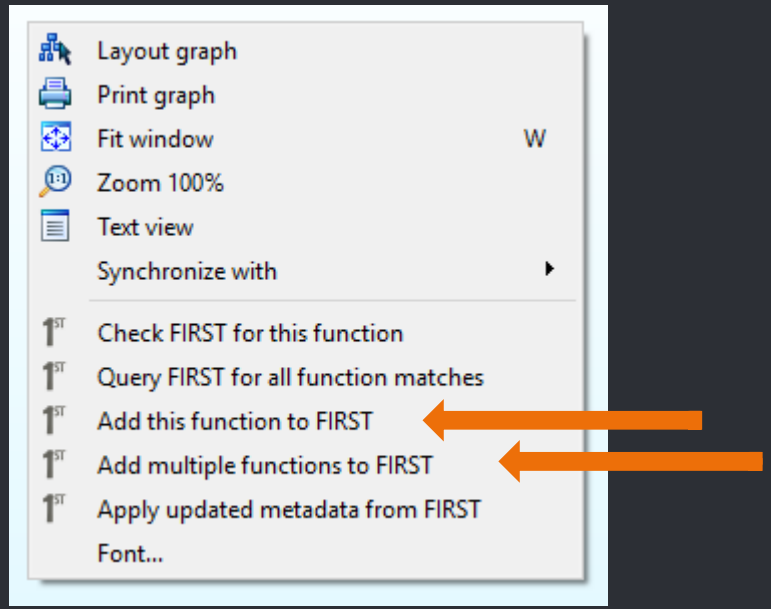
Check for a function or many at once

Plug-in sends the server the opcodes, architecture, and APIs called by function



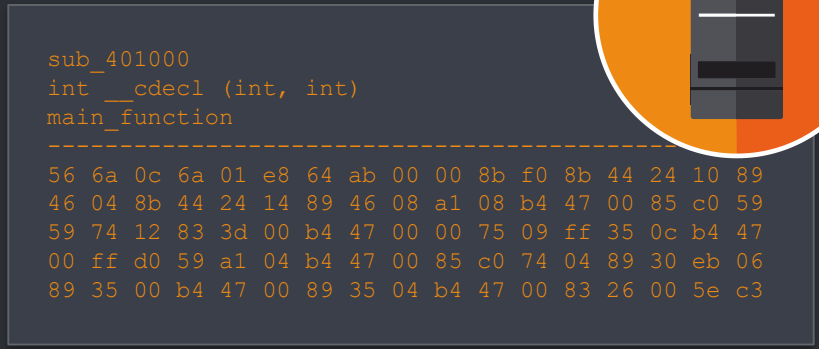


HOW THE PLUGIN WORKS

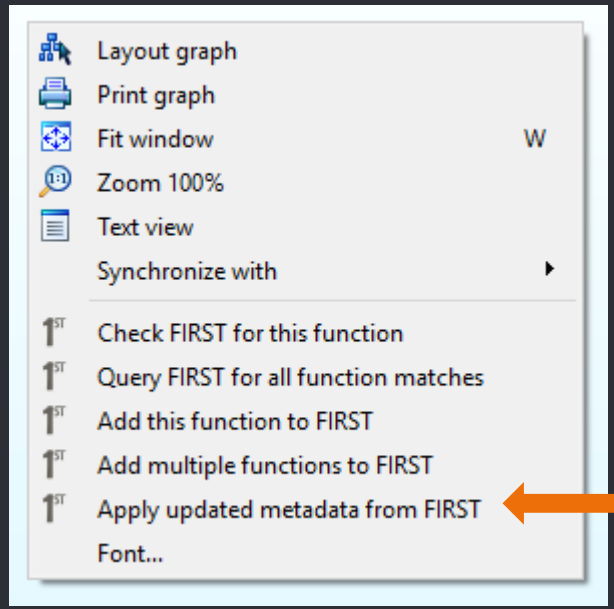


Adding a function or many at once

Plug-in sends the server the opcodes, architecture, APIs called by function and metadata (function's name, prototype, and repeatable comment)



HOW THE PLUGIN WORKS

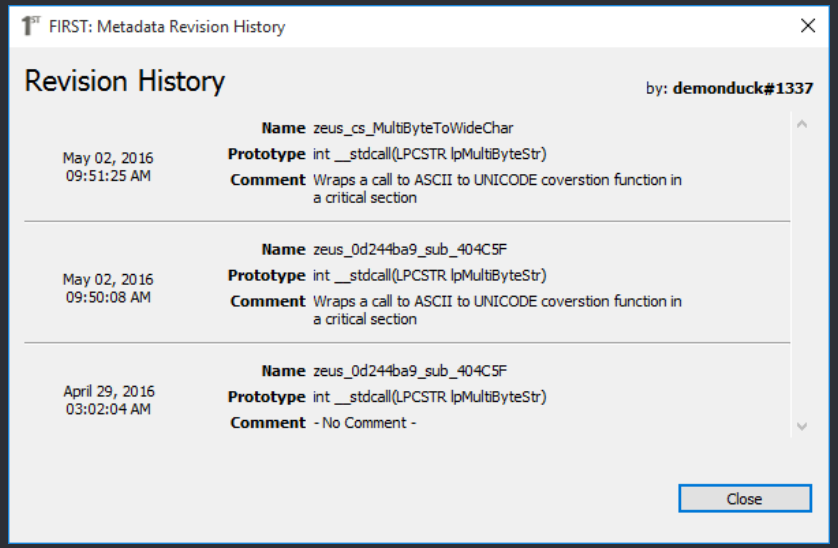


Updating metadata applied

Plug-in requests updated versions of the function's metadata

```
sub_401000 : <ID>
...
sub_403500 : <ID>
```

HOW THE PLUGIN WORKS



Viewing Metadata History

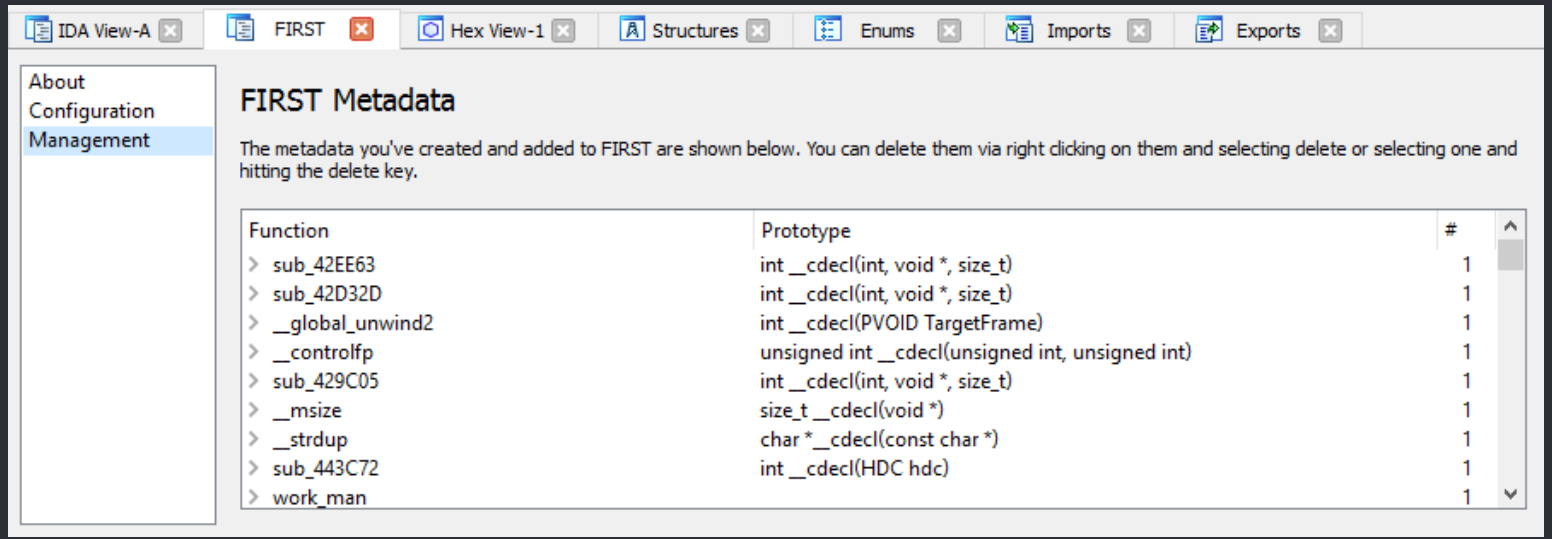
Right Click on function with metadata from FIRST to see its history

Tracks metadata changes over time for each function for each user

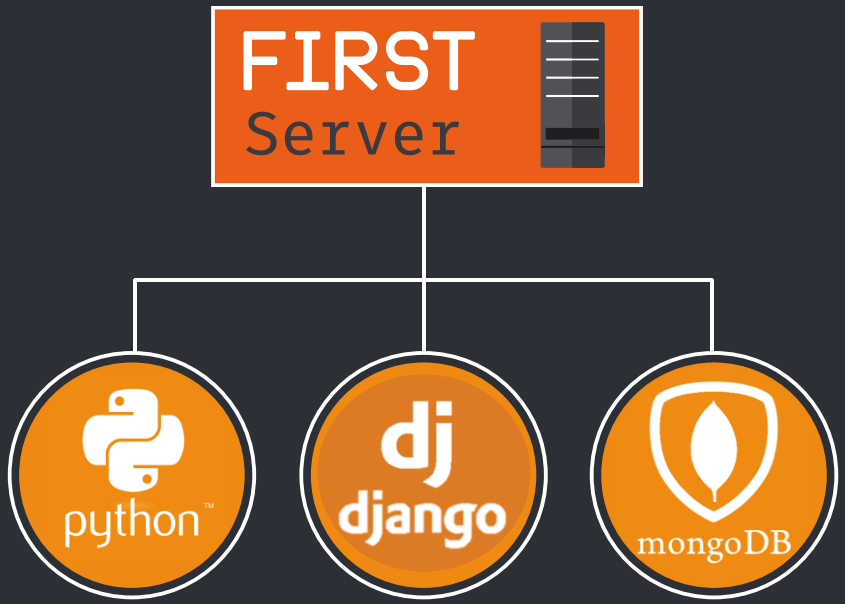
HOW THE PLUGIN WORKS

Deleting metadata you've created

Right click metadata and select delete, or select the metadata and hit the delete key.



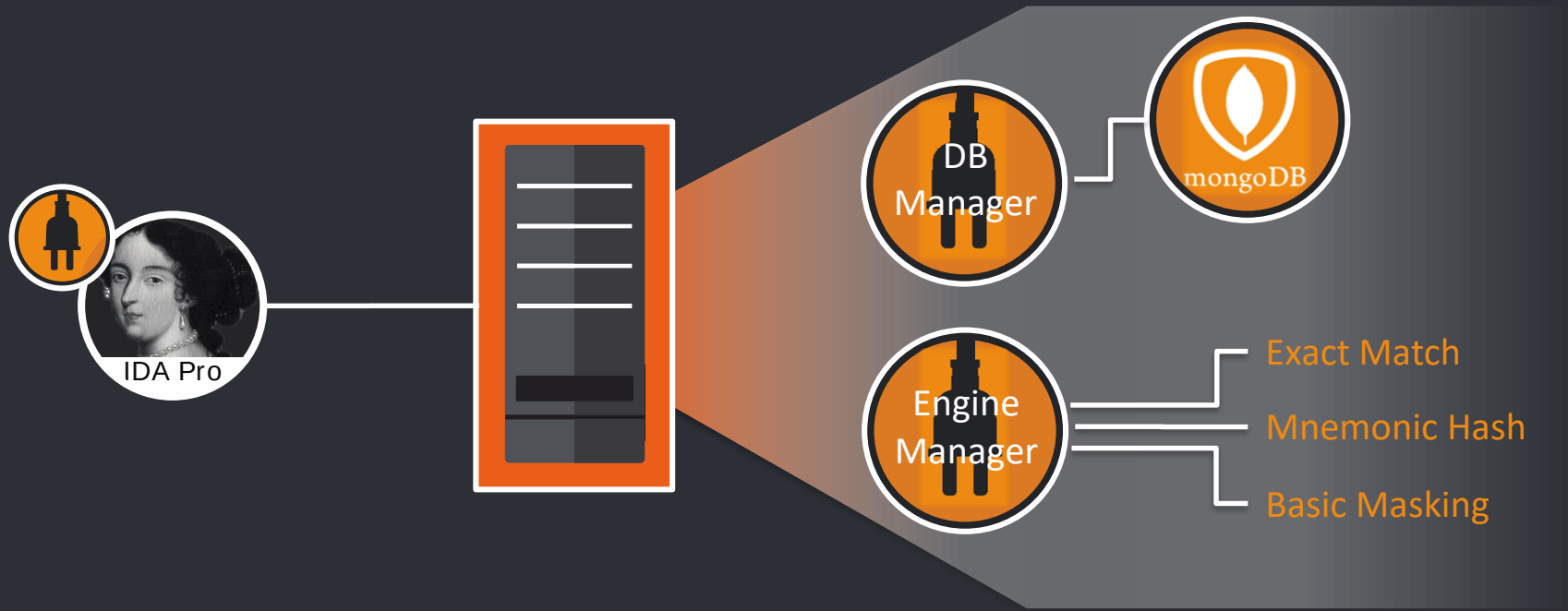
HOW THE SERVER WORKS



The server is a framework

- Uses Python, Django, and MongoDB
- Extensible and modular framework
- Modules
  - Authentication
    BETA leverages Google OAuth2
  - Detection Engines
    Exact Match, Mnemonic Hashing, and Basic Masking
  - Backend Databases
    BETA leverages mongoDB

HOW THE SERVER WORKS



THE DATA

- OpenSSL
- 7zip
- aPLib
- ucl
- LibreSSL 2.3.1
- Mimikatz
- aPackage
- UPX
- ClamWin
- Alina Spark
- Dexter
- Grum
- Pony
- Zeus
- HackingTeam RCS
- …

Demo

Questions

Register to use
http://first-plugin.us

Get the code
https://github.com/vrtadmin/FIRST

Read the docs
http://first-server.readthedocs.io
http://first-plugin-ida.readthedocs.io

FIRST

talosintel.com
blogs.cisco.com/talos
@talossecurity