



---

# 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

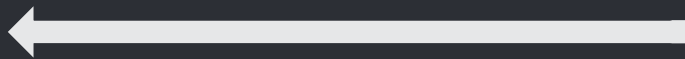
- FIRST: Function Identification and Recovery Signature Tool
- Streamlines code research
  - prevents duplicate effort
  - improves analysis time
- Flexible
  - Modular framework made for expanding



# SYSTEM OVERVIEW

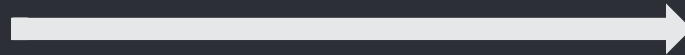
Check for Metadata

56 6A 0C 6A 01 E8 64 AB 00 00 ...



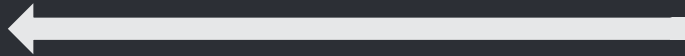
Add Function Metadata

Name / Prototype / Comment



Update Function Metadata

With the most recent version



IDA Pro



# INSTALLATION

pip install requests

## REQUIREMENTS

Python Requests Module

<https://pypi.python.org/pypi/requests>

OPTIONAL:

Requests-kerberos (if kerberos authentication is required)



**FIRST**  
IDA PRO PLUGIN

## 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

---

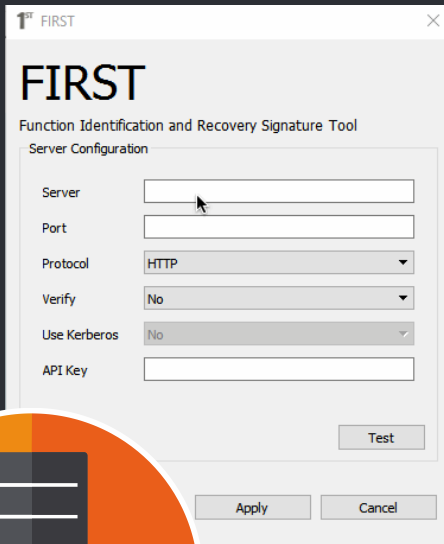
Windows:

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

Mac:

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

# CONFIGURATION



FIRST  
Function Identification and Recovery Signature Tool

Server Configuration

Server:

Port:

Protocol: HTTP

Verify: No

Use Kerberos: No

API Key:

Test


Apply Cancel

## 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

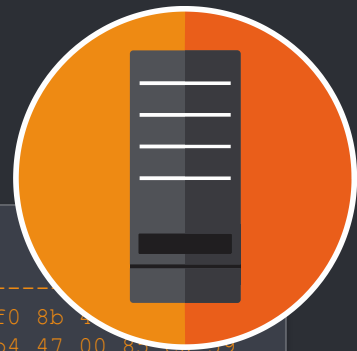
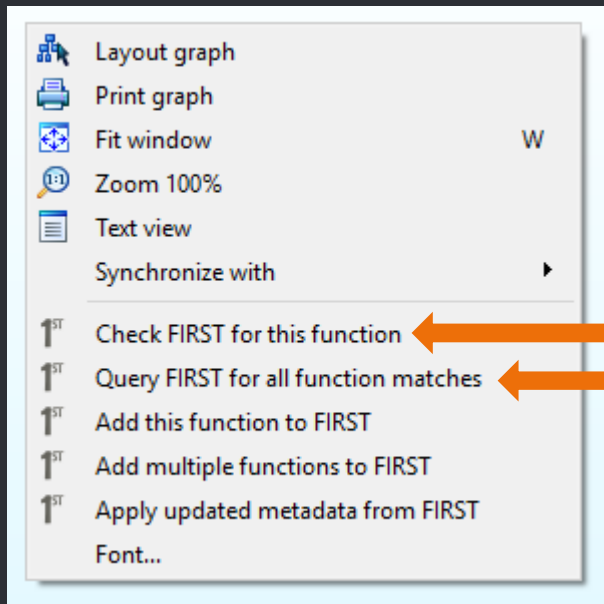


Server: [first-plugin.us](http://first-plugin.us)  
Port: 80  
Protocol: HTTP

# 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



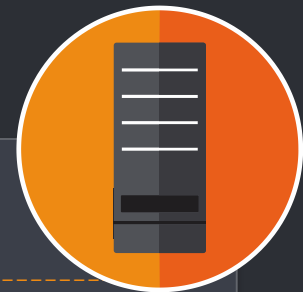
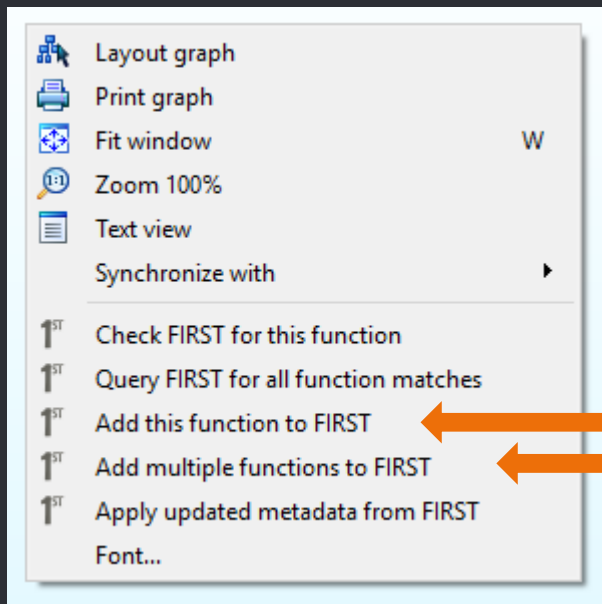
```
sub_401000
-----
56 6a 0c 6a 01 e8 64 ab 00 00 8b f0 8b
46 04 8b 44 24 14 89 46 08 a1 08 b4 47 00 83
59 74 12 83 3d 00 b4 47 00 00 75 09 ff 35 0c b4 47
00 ff d0 59 a1 04 b4 47 00 85 c0 74 04 89 30 eb 06
89 35 00 b4 47 00 89 35 04 b4 47 00 83 26 00 5e c3
```



# 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)

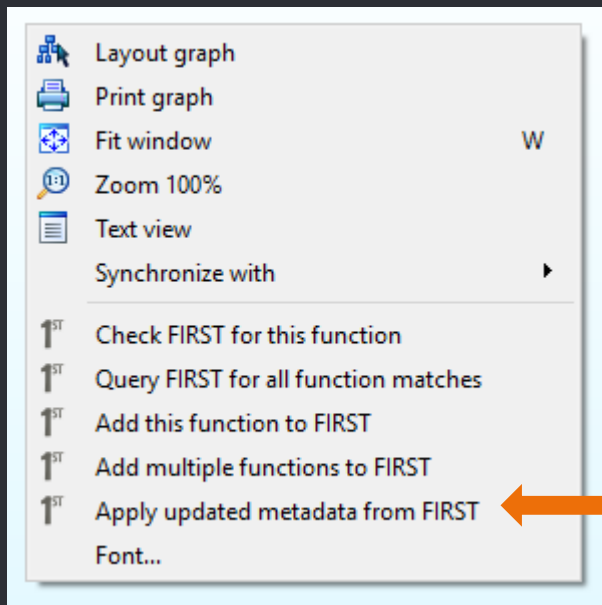


```
sub_401000
int __cdecl (int, int)
main_function
-----
56 6a 0c 6a 01 e8 64 ab 00 00 8b f0 8b 44 24 10 89
46 04 8b 44 24 14 89 46 08 a1 08 b4 47 00 85 c0 59
59 74 12 83 3d 00 b4 47 00 00 75 09 ff 35 0c b4 47
00 ff d0 59 a1 04 b4 47 00 85 c0 74 04 89 30 eb 06
89 35 00 b4 47 00 89 35 04 b4 47 00 83 26 00 5e c3
```

# HOW THE PLUGIN WORKS

## Updating metadata applied

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



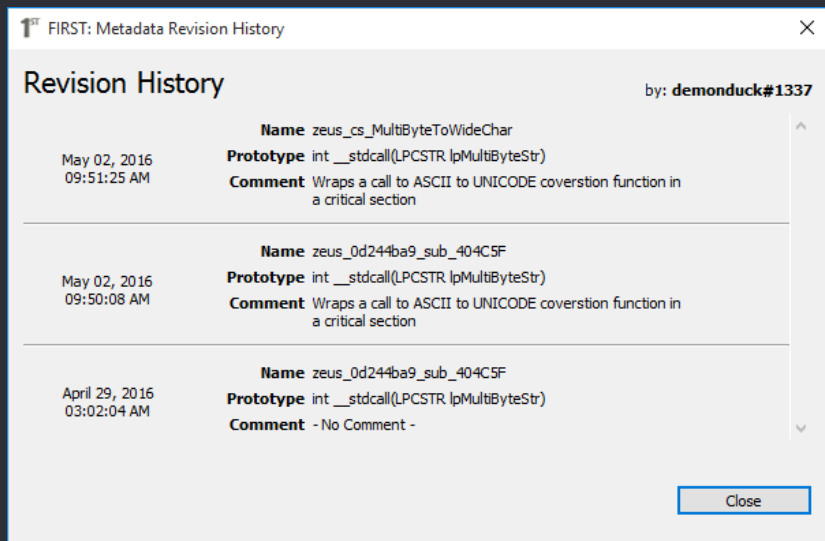
```
sub_401000 : <ID>  
...  
sub_403500 : <ID>
```

# 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



The screenshot shows a window titled "FIRST: Metadata Revision History" with a close button in the top right corner. The window content is as follows:

**Revision History** by: **demonduck#1337**

May 02, 2016 09:51:25 AM	<b>Name</b> zeus_cs_MultiByteToWideChar <b>Prototype</b> int __stdcall(LPCSTR lpMultiByteStr) <b>Comment</b> Wraps a call to ASCII to UNICODE conversion function in a critical section
May 02, 2016 09:50:08 AM	<b>Name</b> zeus_0d244ba9_sub_404C5F <b>Prototype</b> int __stdcall(LPCSTR lpMultiByteStr) <b>Comment</b> Wraps a call to ASCII to UNICODE conversion function in a critical section
April 29, 2016 03:02:04 AM	<b>Name</b> zeus_0d244ba9_sub_404C5F <b>Prototype</b> int __stdcall(LPCSTR lpMultiByteStr) <b>Comment</b> - No Comment -

Close

# HOW THE PLUGIN WORKS

## Deleting metadata you've created

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

IDA View-A FIRST Hex View-1 Structures Enums Imports Exports

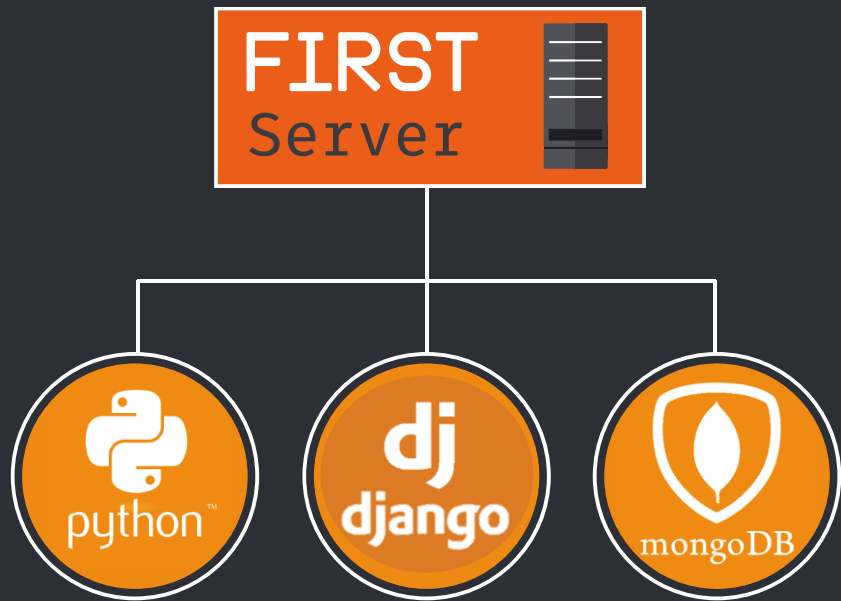
About  
Configuration  
Management

### FIRST Metadata

The metadata you've created and added to FIRST are shown below. You can delete them via right clicking on them and selecting delete or selecting one and hitting the delete key.

Function	Prototype	#
> sub_42EE63	int __cdecl(int, void *, size_t)	1
> sub_42D32D	int __cdecl(int, void *, size_t)	1
> __global_unwind2	int __cdecl(PVOID TargetFrame)	1
> __controlfp	unsigned int __cdecl(unsigned int, unsigned int)	1
> sub_429C05	int __cdecl(int, void *, size_t)	1
> __msize	size_t __cdecl(void *)	1
> __strdup	char * __cdecl(const char *)	1
> sub_443C72	int __cdecl(HDC hdc)	1
> work_man		1

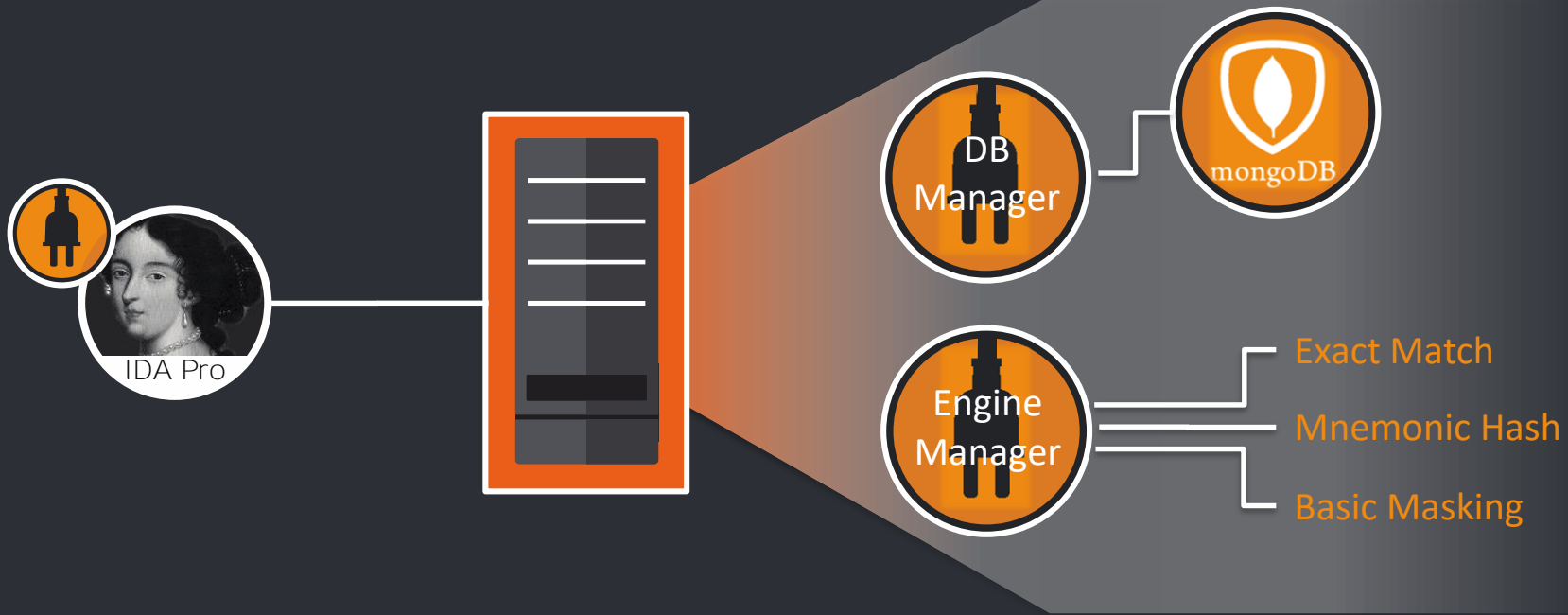
# HOW THE SERVER WORKS



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

# TALOS

[talosintel.com](https://talosintel.com)

[blogs.cisco.com/talos](https://blogs.cisco.com/talos)

@talossecurity

