

# **TAPIR : Trustable Incident Response Parser**

CORI&IN 2022

# Who am I ?

- Solal Jacob
- Incident Response @ Cisco Talos
- Developer of DFF

# Plan

- The TAP library
- Bin2json
- TAP-Query
- TAPIR
- TAPyR
- TAPyR-Cmd
- TAPIR-Frontend

## Goals :

- Parse multiple artifacts type via plugins
- Virtually 'Extract' data (file) and metadata
- Stack plugins (ex: partition / filesystem / file metadata)
- Access of data and metadata in an homogenous way
- Ability to search and filter data & metadata
- Export info to JSON (or other common format)

## Safe :

- RUST

## Fast:

- Multithread
- IO bound

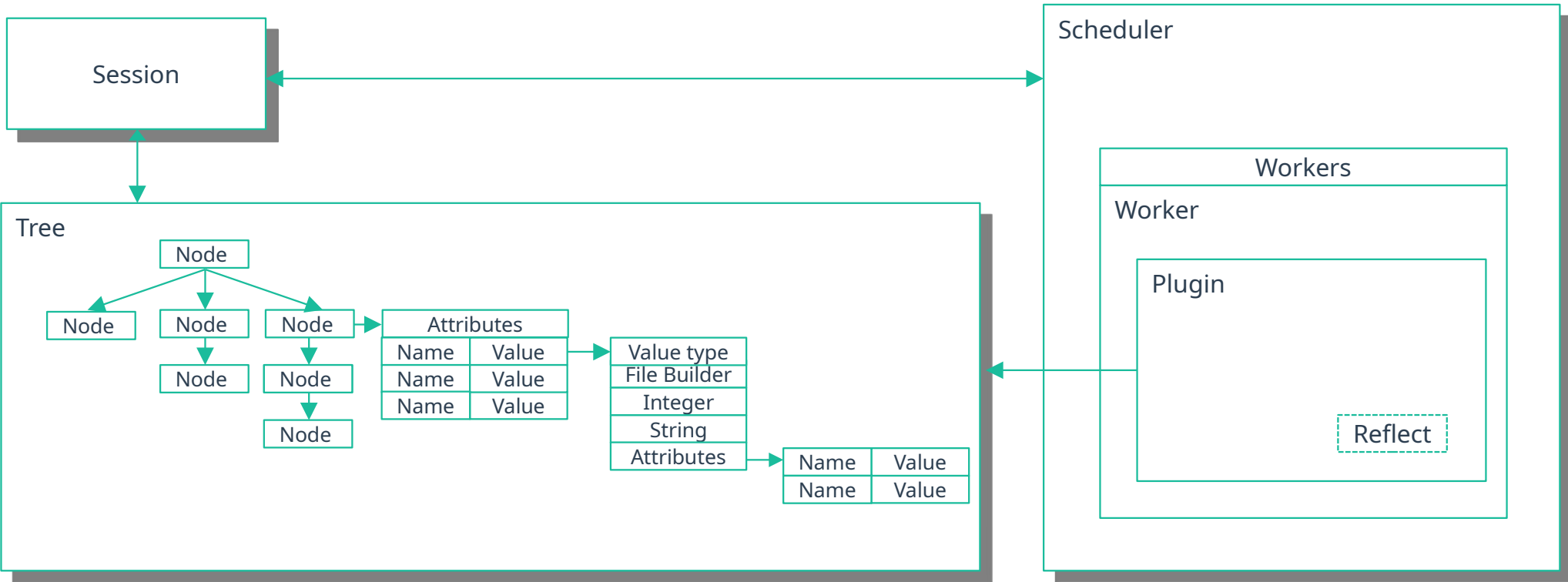
## Easily integrable :

- Library easily integrable into multiple project
- Easy to build
- Use and wrap other RUST forensics crate

## Multiplatform:

- Linux
- Windows
- MacOS X

# TAP : Architecture



# TAP : Plugins

## PLUGINS

### Input

S3  
LOCAL  
DEVICE

### Volume

PARTITION

### Windows

REGISTRY  
PREFETCH  
LNK  
EVTX

### File System

MFT  
NTFS

### Detection

YARA  
CLAMAV

### Metadata

EXIF  
HASH  
MAGIC

# Bin2Json

# Bin2Json

## Input :

- File (disk dump, mft, registry, ...)
- Directory (Collection of artefacts)
- Config file

## Output:

- JSON file

## Processing:

- Load input files
- Detect file type with magic
- Launch the relevant plugin
- Recurse
- Extract all metadata

```
{
  "attributes": {
    "registry": {
      "data": "Empty Recycle Bin"
    }
  },
  "name": "default",
  "path": "/root/cfreds_2015.dd/partition_2/ntfs/root/Users/Default/NTUSER.DAT/CM-CreateHive(D43B12B8-09B5-40DB-B4F6-80FEB78DAEC)/AppEvents/EventLabels/EmptyRecycleBin/default"
},
{
  "attributes": {
    "registry": {
      "data": "Smres.dll,-5831"
    }
  },
  "name": "DispFileName",
  "path": "/root/cfreds_2015.dd/partition_2/ntfs/root/Users/Default/NTUSER.DAT/CM-CreateHive(D43B12B8-09B5-40DB-B4F6-80FEB78DAEC)/AppEvents/EventLabels/EmptyRecycleBin/DispFileName"
},
{
  "attributes": {},
  "name": "FaxBeep",
  "path": "/root/cfreds_2015.dd/partition_2/ntfs/root/Users/Default/NTUSER.DAT/CM-CreateHive(D43B12B8-09B5-40DB-B4F6-80FEB78DAEC)/AppEvents/EventLabels/FaxBeep"
},
{
  "attributes": {
    "registry": {
      "data": "New Fax Notification"
    }
  },
  "name": "default",
  "path": "/root/cfreds_2015.dd/partition_2/ntfs/root/Users/Default/NTUSER.DAT/CM-CreateHive(D43B12B8-09B5-40DB-B4F6-80FEB78DAEC)/AppEvents/EventLabels/FaxBeep/default"
},
{
  "attributes": {
    "registry": {
      "data": "Smres.dll,-5858"
    }
  },
  "name": "DispFileName",
  "path": "/root/cfreds_2015.dd/partition_2/ntfs/root/Users/Default/NTUSER.DAT/CM-CreateHive(D43B12B8-09B5-40DB-B4F6-80FEB78DAEC)/AppEvents/EventLabels/FaxBeep/DispFileName"
},
{
  "attributes": {},
  "name": "FeedDiscovered",
  "path": "/root/cfreds_2015.dd/partition_2/ntfs/root/Users/Default/NTUSER.DAT/CM-CreateHive(D43B12B8-09B5-40DB-B4F6-80FEB78DAEC)/AppEvents/EventLabels/FeedDiscovered"
},
{
  "attributes": {
    "registry": {
      "data": "Feed Discovered"
    }
  },
  "name": "default",
  "path": "/root/cfreds_2015.dd/partition_2/ntfs/root/Users/Default/NTUSER.DAT/CM-CreateHive(D43B12B8-09B5-40DB-B4F6-80FEB78DAEC)/AppEvents/EventLabels/FeedDiscovered/default"
},
{
  "attributes": {
    "registry": {
      "data": "Sisframe.dll,-17315"
    }
  },
  "name": "DispFileName",
  "path": "/root/cfreds_2015.dd/partition_2/ntfs/root/Users/Default/NTUSER.DAT/CM-CreateHive(D43B12B8-09B5-40DB-B4F6-80FEB78DAEC)/AppEvents/EventLabels/FeedDiscovered/DispFileName"
}
```



**DEMO**

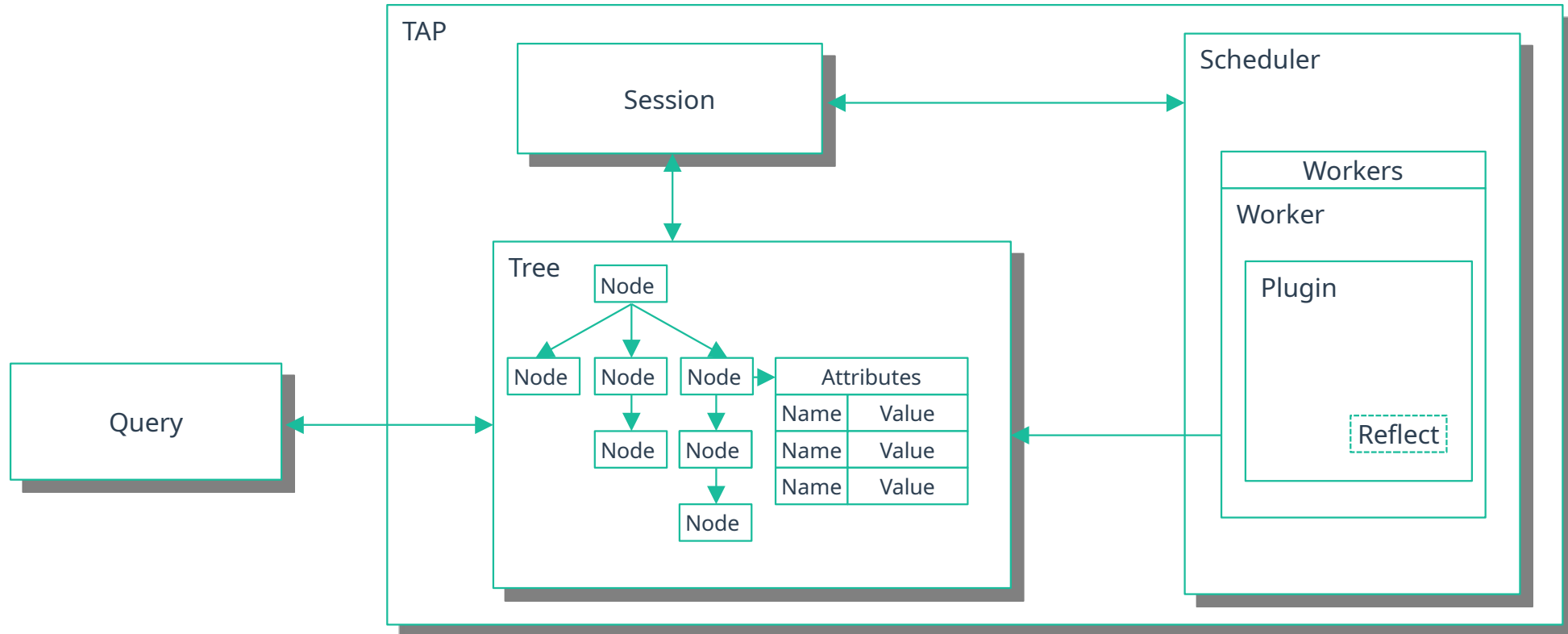
# TAP-Query

# TAP-Query

## Goals :

- Search engine for TAP
- List nodes matching query
- Match attributes : wildcard, regexp, fuzzy
- Match file data content : binary, regexp, UTF-8, UTF-16
- Operator (and, or, not)
- Multithreaded search
- Timeline

# TAP-Query : Architecture



# TAP-Query : Syntax & examples

## Syntax :

### Expression:

name  
attribute.name  
attribute:'attribute\_name'  
data

### Expression type:

(u) : fixed  
r : regexp  
w : wildcard  
f : fuzzy

### Data Expression type:

r : regex / binary  
t : text

### Operator:

and  
and not  
or

## Examples :

- Attribute named data : "attribute.name == 'data'"
- Name 'image1.jpg' : "name == 'image1.jpg'"
- Name with extension .jpg or .tiff using regexp : "name == r'([^\s]+\.(?i)(jpg|tiff))\$'"
- Name with extension .jpg using wildcard : "name == w'\*.jpg'"
- Name starting by image and with an underscore using wildcard : "w'image?\_\*.jpg":
- Name image1 or image2 : "name == 'image1.jpg' or name == w'image2\*'"
- Attribute named exif : "attribute.name == 'exif'"
- Attribute named exif.primary.model : "attribute.name == 'exif.primary.model'"
- Attribute named exif.anything.model : "attribute.name == w'exif.\*.model'"
- Attribute with any name contain a value that match 'powershell' : "attribute:w'\*' == w'\*powershell\*'"
- Attribute 'evtx.event.eventdata.imagepath' contain a value that match 'powershell' :  
attribute:'evtx.event.eventdata.imagepath' == w'\*powershell\*'"
- Attribute starting with evtx.event contain a value that match 'powershell' : "attribute:w'evtx.event\*' == w'\*powershell\*'"
- File binary or text data containing ascii character 'hello' : "data == 'hello'"
- File binary data contain ELF signature : "data == '\x7F\x45\x4C\x46'"
- Find text string inside UTF-8 or UTF-16 text file : "data == t'икра"

**TAPIR**

**TAPIR**

# TAPIR

## Goals :

- Interact with the TAP library
- Client, Server (local, network, cloud)
- Server side processing
- REST API
- Multi-User

## Portable :

- One binary for frontend + backend
- Static binary

## Interfaces :

- Command line
- Web UI

## Fast :

- Async

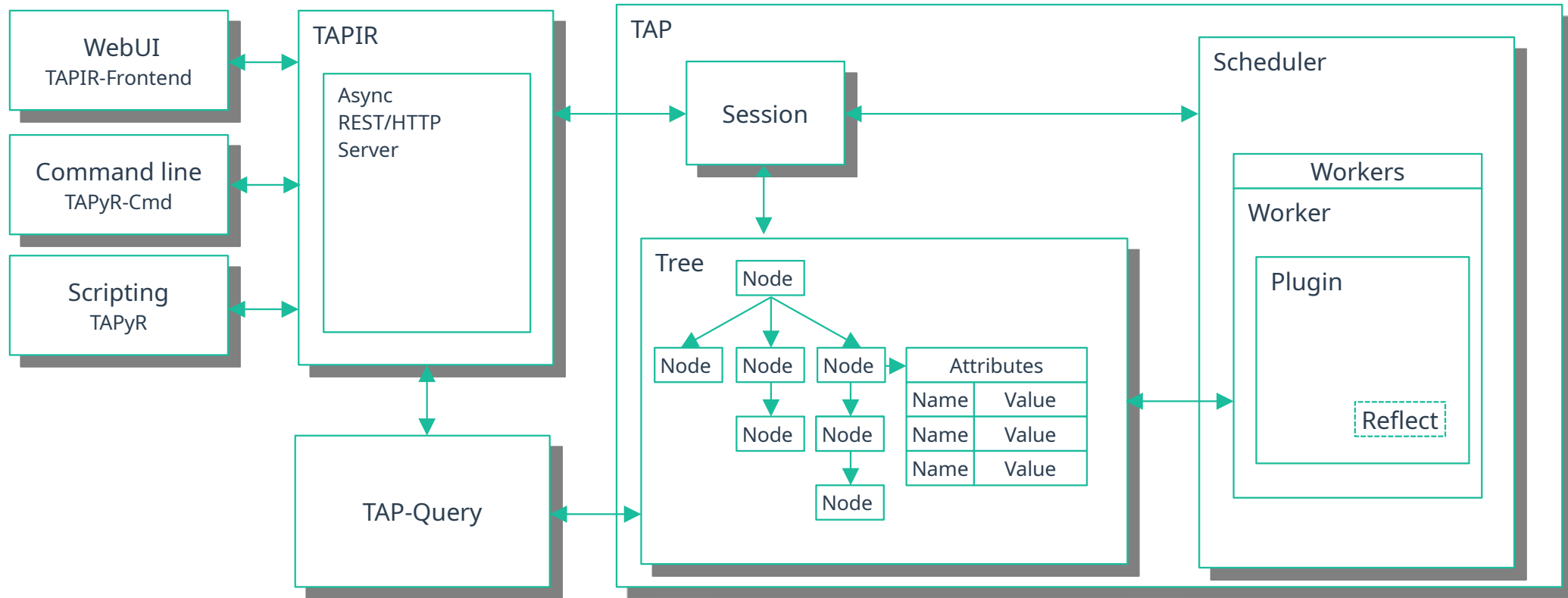
## Secure :

- API Key
- SSL

## Multiplatform (Server + Client):

- Linux
- Windows
- MacOS X

# TAPIR : Architecture





# TAPIR : REST API

## Node & Attributes :

- **upload** : POST /api/upload?<name>
- **root** : GET /api/root
- **node** : POST /api/node
- **nodes** : POST /api/nodes
- **node\_by\_path** : GET /api/root/<path..>
- **path** : POST /api/path
- **parent\_id** : POST /api/parent\_id
- **attribute** : POST /api/attribute
- **read** : POST /api/read
- **download** : POST /api/download
- **download\_id** : GET /api/download\_id?<apikey>&<node\_id>

## Plugins & Tasks:

- **plugins** : GET /api/plugins
- **plugin** : GET /api/plugin/<plugin\_name>
- **run** : POST /api/run
- **schedule** : POST /api/schedule
- **join** : POST /api/join
- **task** : POST /api/task?<task\_id>
- **tasks** : POST /api/tasks
- **scan** : POST /api/scan
- **task\_count** : POST /api/task\_count

## Query & Timeline :

- **query** : POST /api/query
- **timeline** : POST /api/timeline

# TAPyR

# TAPyR

- Python libray
- Binding for tapyr (Using REST API)
- Connect to a local or distant server
- Usefull for creating tool
- Usefull for live scripting
- Generate python object from REST API

# TAPyR-Cmd

- Use TaPYR
- Unix-like shell cmd
- Distant or local (host ip & key in env var.)
- Each cmd are a small python script
- Output can be piped (to JQ, other tapyr cmd, unix cmd)
- Some command have bash auto-completion

# TAPyR-Cmd

## Node & Attributes :

- **ls** : list files / directories
- **attr** : show and add attribute
- **cat** : output file content to stdout
- **download** : download a file
- **upload** : upload file to server for analysis

## Plugins & Tasks :

- **plugin** : list plugin argument
- **plugins** : list all available plugins on the server
- **scan** : detect file type and launch plugin automatically
- **ps** : display list of tasks
- **psstat** : display summary of tasks

## Query & Timeline :

- **timeline** : generate a json or csv timeline
- **shell** : run python shell for scripting
- **find** : list files using query
- **extract** : find and download files

# DEMO

# TAPIR-Frontend

# TAPIR-Frontend : Architecture

- Java Script (node / React / Antd)
- Multiple Window / Multi Screen
- JS Binding via the REST API
- Integrated directly into TAPIR binary
- SSL + API Key



# TAPIR-Fronted : Browser

- Browse nodes :
  - Files
  - Directories
  - Registry
  - Evtx
  - ...
- Download files (zip with password)
- Sort & filter column by attributes
- Copy selected attributes
- Export attributes as CSV & JSON
- Run plugins

The screenshot displays the TAPIR-Fronted Browser interface. The top navigation bar includes 'Browser', 'Timeline', and a search icon. The address bar shows the path: `/root/cfreds_2015.dd/partition_2/ntfs/root/Users/informant/Desktop/Download`. The left sidebar shows a file tree with 'Desktop' selected, and a 'Download' button is visible. The main area contains a table of files:

Name	Size	Modified	Accessed	Created	Type
ccsetup504.exe	5345280	2015-03-25T14:48:28Z	2015-03-25T14:48:28Z	2015-03-25T14:48:28Z	application/x-executable
ccsetup504.exe:Zone.Identifier	26	2015-03-25T14:48:28Z	2015-03-25T14:48:28Z	2015-03-25T14:48:28Z	application/octet-stream
Eraser 6.2.0.2962.exe	8318976	2015-03-25T14:47:40Z	2015-03-25T14:47:40Z	2015-03-25T14:47:40Z	application/x-executable
Eraser 6.2.0.2962.exe:Zone.Identifier	26	2015-03-25T14:47:40Z	2015-03-25T14:47:40Z	2015-03-25T14:47:40Z	application/octet-stream
IE11-Windows6.1-x64-en-us.exe	55918592	2015-03-22T15:11:04Z	2015-03-22T15:11:04Z	2015-03-22T15:11:04Z	application/x-executable
IE11-Windows6.1-x64-en-us.exe:Zone.Identifier	26	2015-03-22T15:11:04Z	2015-03-22T15:11:04Z	2015-03-22T15:11:04Z	application/octet-stream

On the right, a detailed view of the selected file's attributes is shown, including 'data' (size, type, datatype) and 'ntfs' (file\_name, accessed\_time, creation\_time, mft\_modification\_time, modification\_time, parent\_mft\_entry\_id, is\_deleted, standard\_information). A context menu is open over the 'data' section, showing options: CSV, JSON, and Zip.

# TAPIR-Fronted : Tasks

- Display & filter tasks
- Display plugin result error

The screenshot displays the TAPIR-Fronted application interface. At the top, there are tabs for 'Viewer', 'Tasks', 'Plugins', and 'Browser 1'. The 'Tasks' tab is active, showing a table of tasks. The table has columns for PID, Status, Plugin, and Argument. Below the table, a modal dialog titled 'result' is open, displaying an error message: 'Error parsing extra data: unknown extra block: size: 0x00000000, signature: 0x00000000'. The dialog has 'Cancel' and 'OK' buttons. To the right of the modal, a 'Result' column is visible, showing a series of checkmarks and crosses.

PID	Status	Plugin	Argument
1224	finished	registry	-file SECURITY.LOG
1225	finished	lnk	-file migwiz.lnk
1226	finished	registry	-file SCHEMA.DAT.LOG1
1227	finished	registry	-file schema.dat.LOG
1228	finished	registry	-file SCHEMA.DAT
1229	finished	exif	-files topGradRepeat.jpg
1230	finished	exif	-files darkBlue_GRAD.jpg
1231	finished	exif	-files ASPdotNET_logo.jpg
1232	finished	exif	-files topGradRepeat.jpg
1233	finished	exif	-files darkBlue_GRAD.jpg
1234	finished	exif	-files ASPdotNET_logo.jpg
1235	finished	exif	-files ASPdotNET_logo.jpg
1236	finished	exif	-files darkBlue_GRAD.jpg
1237	finished	exif	-files topGradRepeat.jpg

# TAPIR-Frontend : Viewer

Auto

Off

01 Hex

Text

PDF

Image

Video

Word

Excel

Csv

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000	eb	52	90	4e	54	46	53	20	20	20	00	02	08	00	00		.R.NTFS .....
0010	00	00	00	00	00	f8	00	00	3f	00	ff	00	00	28	03	00	.....?....(..
0020	00	00	00	00	80	80	80	00	ff	cf	7c	02	00	00	00	00	.....[.....
0030	00	00	0c	00	00	00	00	00	02	00	00	00	00	00	00	00	.....Hz.....
0040	f6	00	00	00	01	00	00	00	48	7a	0c	ca	8d	0c	ca	c8	.....3.....[.h..
0050	00	00	00	00	fa	33	c0	8e	d0	bc	00	7c	fb	68	c0	07	..hf.....f.>..N
0060	1f	1e	68	66	00	cb	88	16	0e	00	66	81	3e	03	00	4e	TFSu..A..U..x...
0070	54	46	53	75	15	b4	41	bb	aa	55	cd	13	72	0c	81	fb	U.u.....
0080	55	aa	75	06	f7	c1	01	00	75	03	e9	dd	00	1e	83	ec	.h...H.....
0090	18	68	1a	00	b4	48	8a	16	0e	00	8b	f4	16	1f	cd	13	....X.x;...u...
00a0	9f	83	c4	18	9e	58	1f	72	e1	3b	06	0b	00	75	db	a3	.....Z3...+.
00b0	0f	00	c1	2e	0f	00	04	1e	5a	33	db	b9	00	20	2b	c8	f.....
00c0	66	ff	06	11	00	03	16	0f	00	8e	c2	ff	06	16	00	e8	K.+..w.....f#.u-
00d0	4b	00	2b	c8	77	ef	b8	00	bb	cd	1a	66	23	c0	75	2d	f...TCPAuS...x...
00e0	66	81	fb	54	43	50	41	75	24	81	f9	02	01	72	1e	16	h...hp..h...fSfSf
00f0	68	07	bb	16	68	70	0e	16	68	09	00	66	53	66	53	66	U...h...fa...3...
0100	55	16	16	16	68	b8	01	66	61	0e	07	cd	1a	33	c0	bf	(.....f...
0110	28	10	b9	d8	0f	fc	f3	aa	e9	5f	01	90	90	66	60	1e	.f...f...fh...compressed files.....
0120	06	66	a1	11	00	66	03	06	1c	00	1e	66	68	00	00	00	.....
0130	00	66	50	06	53	68	01	00	68	10	00	b4	42	8a	16	0e	.fP.Sh..h...B...

Viewing the Results of an Erasure.....	10
Eraser Settings .....	12
Shell Integration .....	12



ATION LETTER

arch 25, 2015

r Mr. Manager,

stive today. Thank you for your guidance and support while working as your Development Manager.

.....

ears I spent with your organization. I wish you continued success.

Sincerely,

laman Informant

# TAPIR-Frontend : Search

- Enter query directly
- Use query editor to create complex query

(name == w\*.txt) and (data == t'hello')

	Name	Size	Mod
<input type="checkbox"/>	img27.jpg	2064384	2009-06-10T20:46:41Z
<input type="checkbox"/>	img25.jpg	1818624	2009-06-10T20:46:41Z
<input type="checkbox"/>	img22.jpg	1765376	2009-06-10T20:46:41Z
<input type="checkbox"/>	img26.jpg	1708032	2009-06-10T20:46:41Z
<input type="checkbox"/>	img12.jpg	1548288	2009-06-10T20:46:41Z
<input type="checkbox"/>	img4.jpg	1536000	2009-06-10T20:46:41Z
<input type="checkbox"/>	img14.jpg	1527808	2009-06-10T20:46:41Z
<input type="checkbox"/>	img10.jpg	1527808	2009-06-10T20:46:41Z
<input type="checkbox"/>	img15.jpg	1495040	2009-06-10T20:46:41Z
<input type="checkbox"/>	img3.jpg	1478656	2009-06-10T20:46:41Z
<input type="checkbox"/>	img19.jpg	1474560	2009-06-10T20:46:41Z
<input type="checkbox"/>	img23.jpg	1462272	2009-06-10T20:46:41Z
<input type="checkbox"/>	img1.jpg	1425408	2009-06-10T20:46:41Z
<input type="checkbox"/>	img17.jpg	1392640	2009-06-10T20:46:41Z
<input type="checkbox"/>	img29.jpg	1384448	2009-06-10T20:46:41Z
<input type="checkbox"/>	img11.jpg	1384448	2009-06-10T20:46:41Z
<input type="checkbox"/>	img21.jpg	1343488	2009-06-10T20:46:41Z
<input type="checkbox"/>	img2.jpg	1323008	2009-06-10T20:46:41Z
<input type="checkbox"/>	img20.jpg	1213888	2009-06-10T20:46:41Z

### Query editor

Name == \*.txt Wildcard

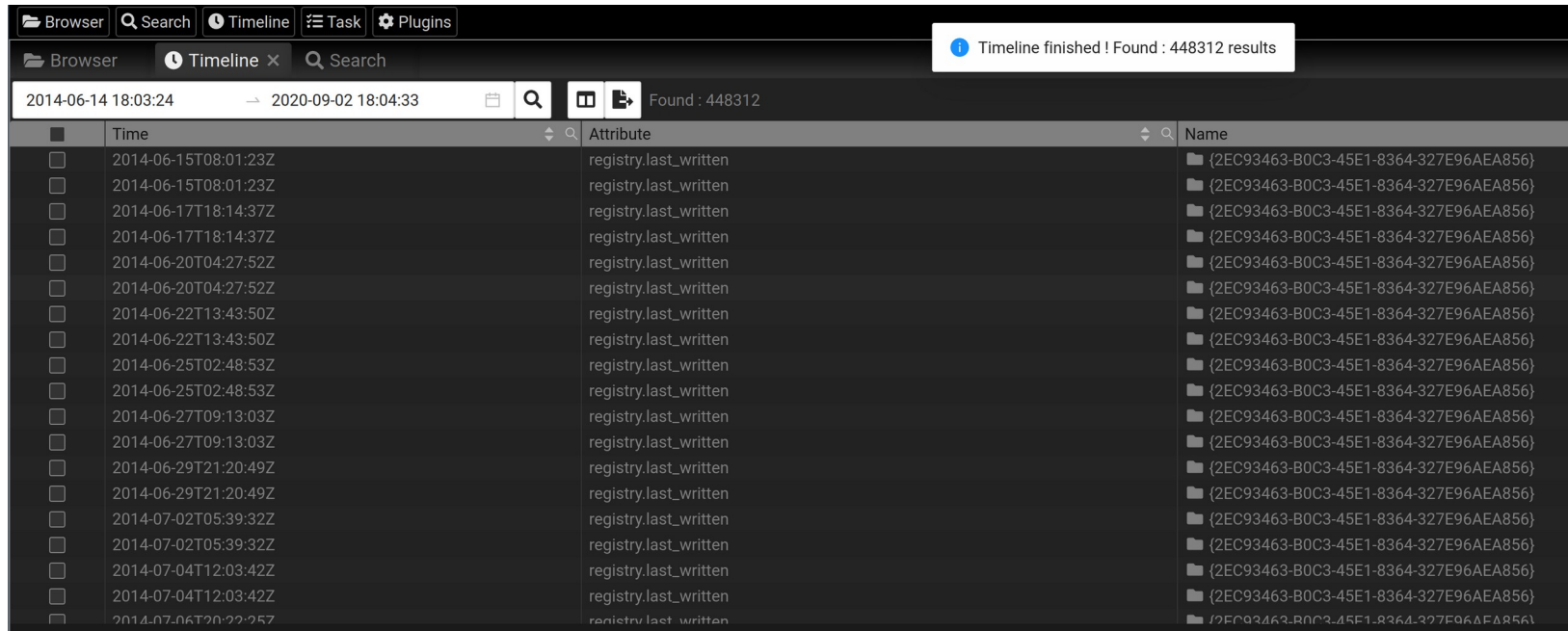
And Data == hello Text

+ Add expression

Cancel OK

# TAPIR-Frontend : Timeline

- Select timeframe
- Select columns and export timeline to CSV or JSON



	Time	Attribute	Name
<input type="checkbox"/>	2014-06-15T08:01:23Z	registry.last_written	{2EC93463-B0C3-45E1-8364-327E96AEA856}
<input type="checkbox"/>	2014-06-15T08:01:23Z	registry.last_written	{2EC93463-B0C3-45E1-8364-327E96AEA856}
<input type="checkbox"/>	2014-06-17T18:14:37Z	registry.last_written	{2EC93463-B0C3-45E1-8364-327E96AEA856}
<input type="checkbox"/>	2014-06-17T18:14:37Z	registry.last_written	{2EC93463-B0C3-45E1-8364-327E96AEA856}
<input type="checkbox"/>	2014-06-20T04:27:52Z	registry.last_written	{2EC93463-B0C3-45E1-8364-327E96AEA856}
<input type="checkbox"/>	2014-06-20T04:27:52Z	registry.last_written	{2EC93463-B0C3-45E1-8364-327E96AEA856}
<input type="checkbox"/>	2014-06-22T13:43:50Z	registry.last_written	{2EC93463-B0C3-45E1-8364-327E96AEA856}
<input type="checkbox"/>	2014-06-22T13:43:50Z	registry.last_written	{2EC93463-B0C3-45E1-8364-327E96AEA856}
<input type="checkbox"/>	2014-06-25T02:48:53Z	registry.last_written	{2EC93463-B0C3-45E1-8364-327E96AEA856}
<input type="checkbox"/>	2014-06-25T02:48:53Z	registry.last_written	{2EC93463-B0C3-45E1-8364-327E96AEA856}
<input type="checkbox"/>	2014-06-27T09:13:03Z	registry.last_written	{2EC93463-B0C3-45E1-8364-327E96AEA856}
<input type="checkbox"/>	2014-06-27T09:13:03Z	registry.last_written	{2EC93463-B0C3-45E1-8364-327E96AEA856}
<input type="checkbox"/>	2014-06-29T21:20:49Z	registry.last_written	{2EC93463-B0C3-45E1-8364-327E96AEA856}
<input type="checkbox"/>	2014-06-29T21:20:49Z	registry.last_written	{2EC93463-B0C3-45E1-8364-327E96AEA856}
<input type="checkbox"/>	2014-07-02T05:39:32Z	registry.last_written	{2EC93463-B0C3-45E1-8364-327E96AEA856}
<input type="checkbox"/>	2014-07-02T05:39:32Z	registry.last_written	{2EC93463-B0C3-45E1-8364-327E96AEA856}
<input type="checkbox"/>	2014-07-04T12:03:42Z	registry.last_written	{2EC93463-B0C3-45E1-8364-327E96AEA856}
<input type="checkbox"/>	2014-07-04T12:03:42Z	registry.last_written	{2EC93463-B0C3-45E1-8364-327E96AEA856}
<input type="checkbox"/>	2014-07-06T20:22:25Z	registry.last_written	{2EC93463-B0C3-45E1-8364-327E96AEA856}

# DEMO

# Download & contribute

- **Github** : <https://github.com/tap-ir>
- **Follow** : @arxsys

**Contributor are welcome !**



**Questions ?**