ManaTI

Web Assistance for the Threat Analyst, supported by Domain Similarity

SEBASTIÁN GARCÍA
sebastian.garcia@agents.fel.cvut.cz
@eldracote

RAÚL BENÍTEZ NETTO
raulbeni@gmail.com
@Piuliss

Czech Technical University in Prague

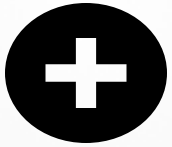
https://github.com/stratosphereips/Manati

STRATOSPHERE IPS PROJECT

Stratosphere Project

a free software Intrusion Prevention System

Free protection for NGOs.



Security and Machine Learning

Stratosphere Data Analysis Project

https://stratosphereips.org/

@StratosphereIPS

@stratosphereips

What and why?

ManaTI is a web-based system to analyze, store and organize weblogs faster in a threat analysis team.

ManaTI Purpose

ManaTI assists threat analysis team to make their work faster and more effective

Raúl Benítez Netto

- Master Student in CTU
- Member of Stratosphere Project
- Web/App developer focus cyber-security environment
- Photographer aficionado
- raulbeni@gmail.com
- @Piuliss

Sebastian García

- Founder of Stratosphere Project
- Creator of Stratosphere IPS
- Researcher on cybersecurity using Machine Learning
- eldraco@gmail.com
- @eldracote

Basic knowledge

- Weblogs
- WHOIS information
- IoCs (Indicators of Compromise)

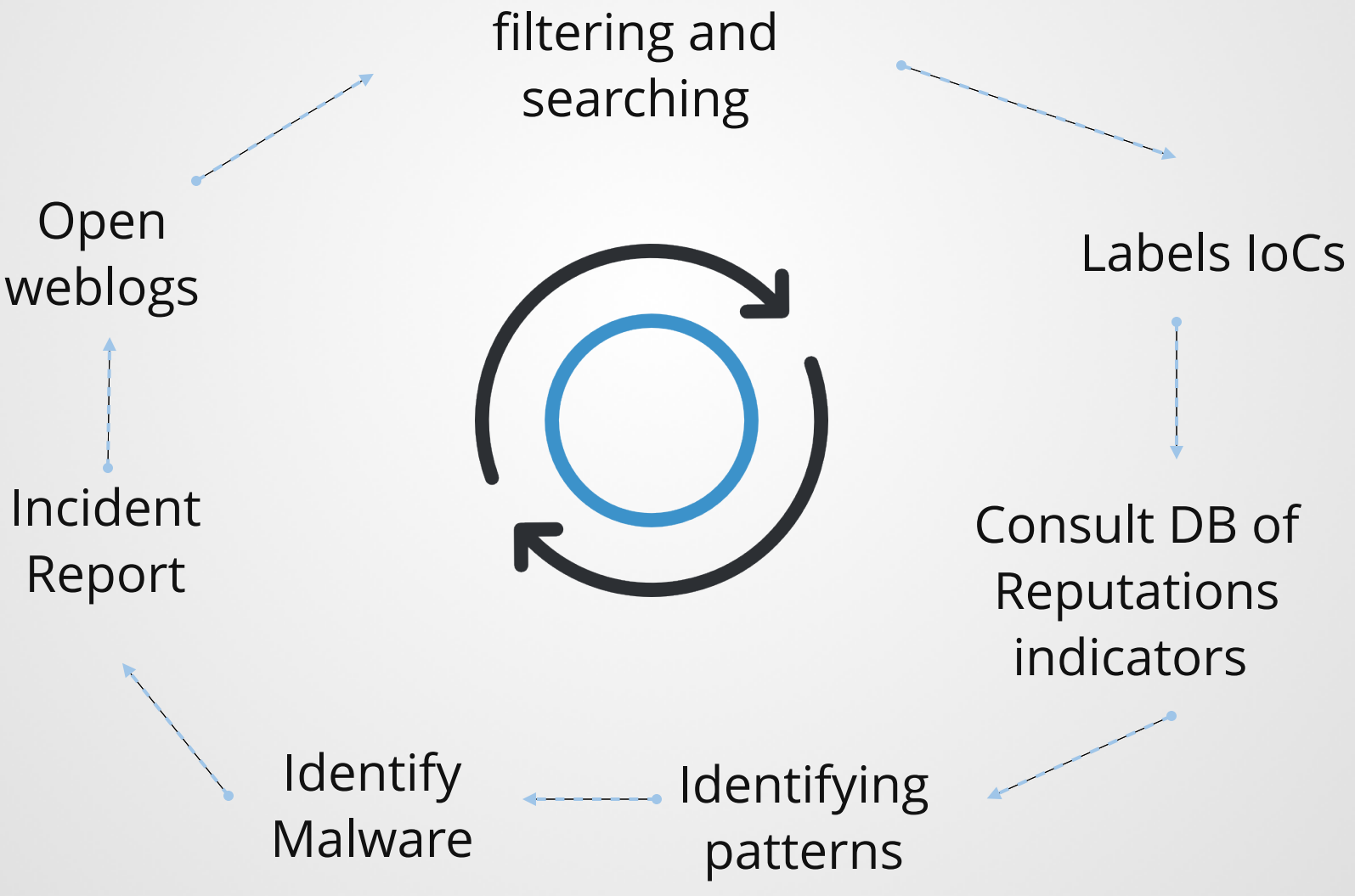
Analysis of Malware Behavior in the Network

The art of understanding the traces of the malware in the network logs.

Malware Traces

Records of connections that malware perform to connect with their C&C

Threat Analyst work



Tools used by Threat Analysts

Logs Viewer

- Log Parser
- Apache Log Viewer
- LogExpert

Terminal/Console

- VIM/VI
- WC (Word Count)
- AWK
- GREP

Big Data analysis

- splunk.com

Problems in Threat Analysis

Huge amount of Data

Labeling Data

Repetitive tasks

Much Knowledge lost over time

It is difficult and tiresome

ManaTI principles

Fast!

Storage 

 Work in teams

GUI - Web 

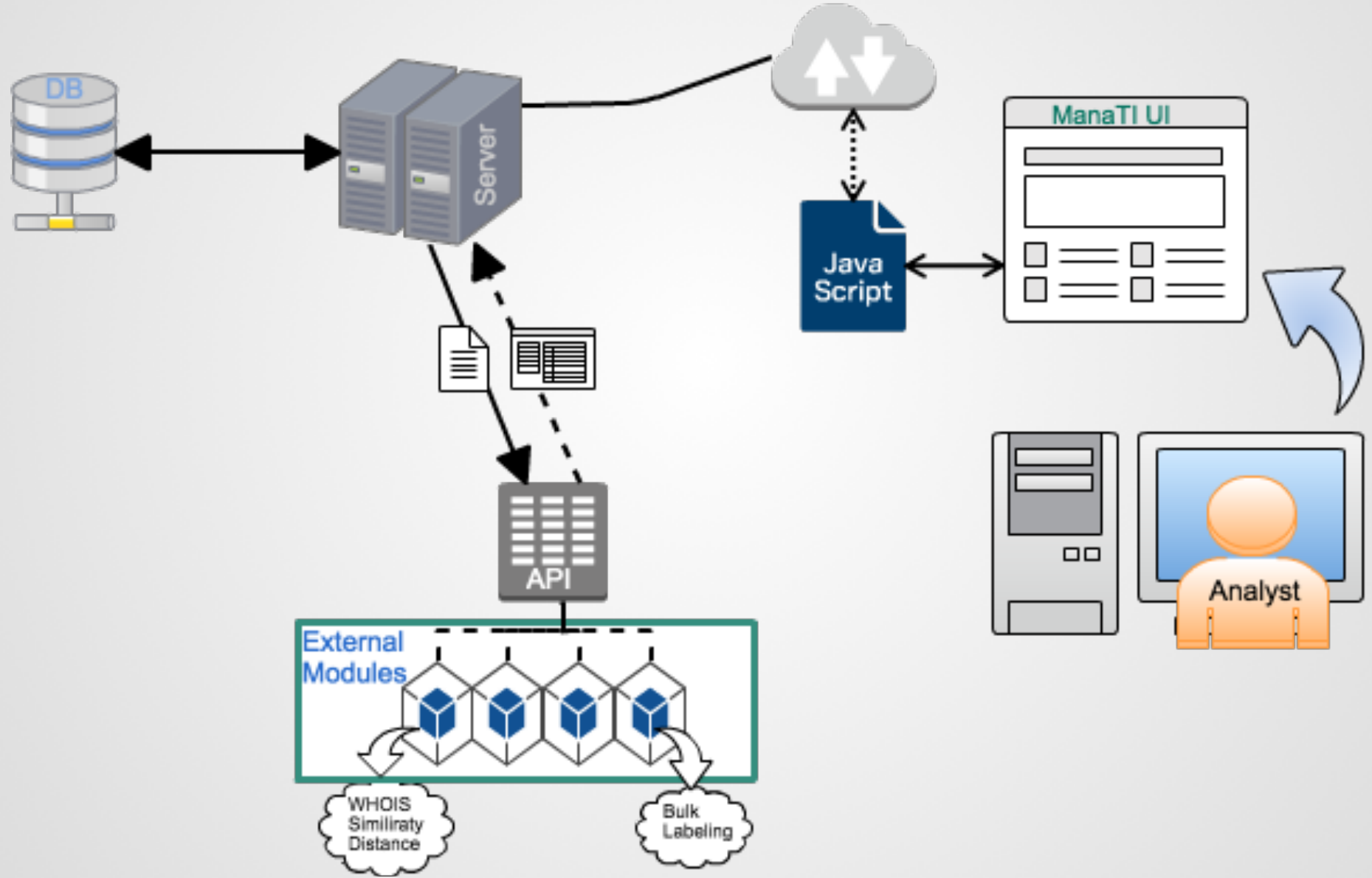
 Provide Assistance

API - Class Interface 

 Machine Learning Algorithm

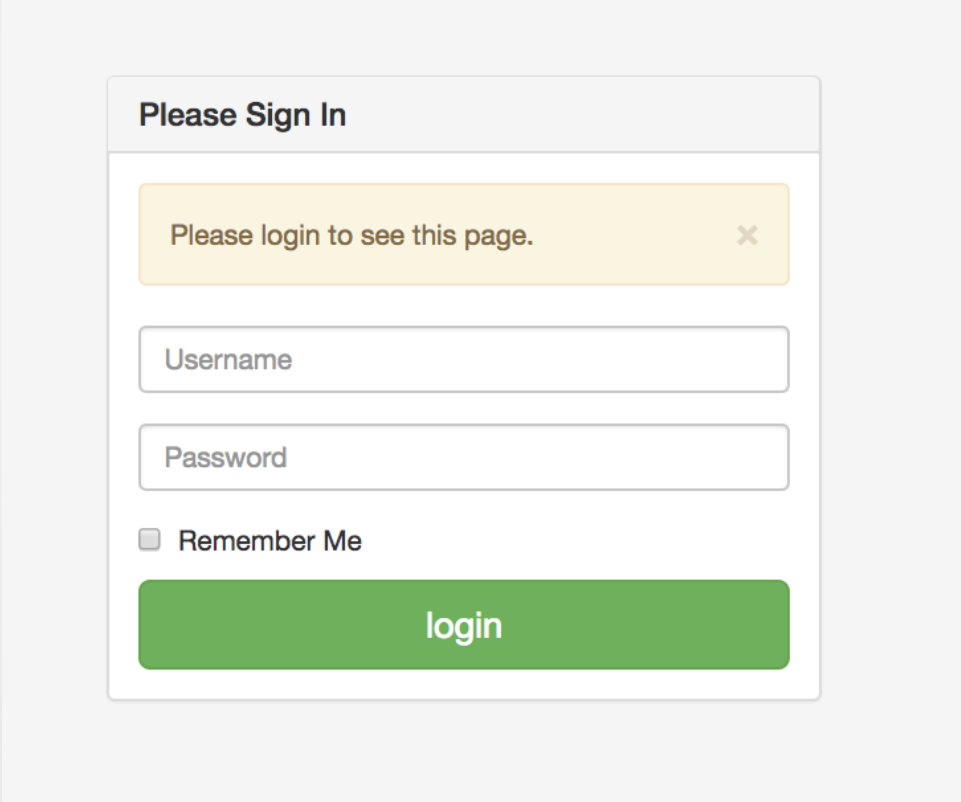
https://github.com/stratosphereips/Manati

ManaTI Workflow



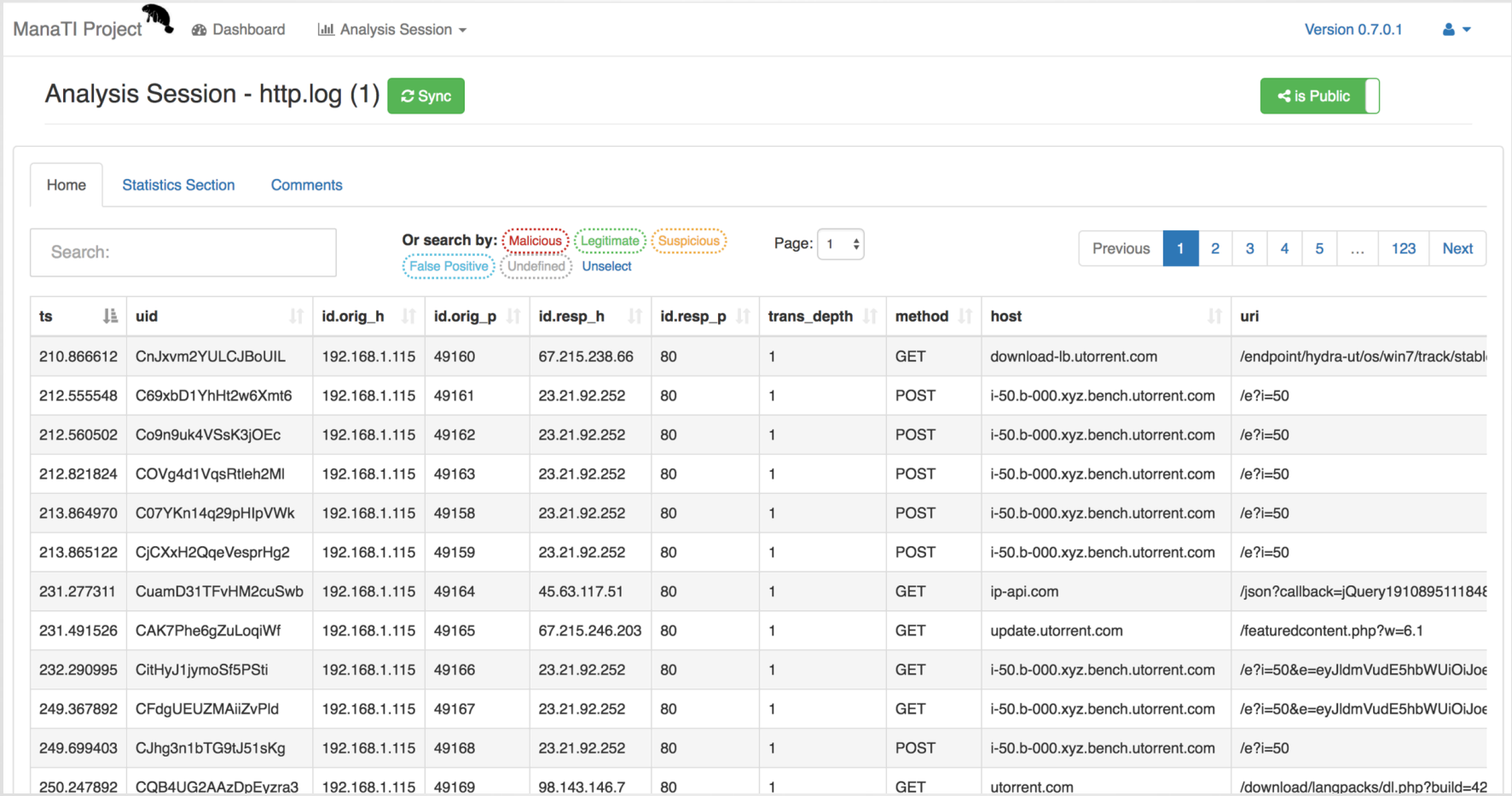
ManaTI basic features and usability

Analysis Sessions and Multi-users



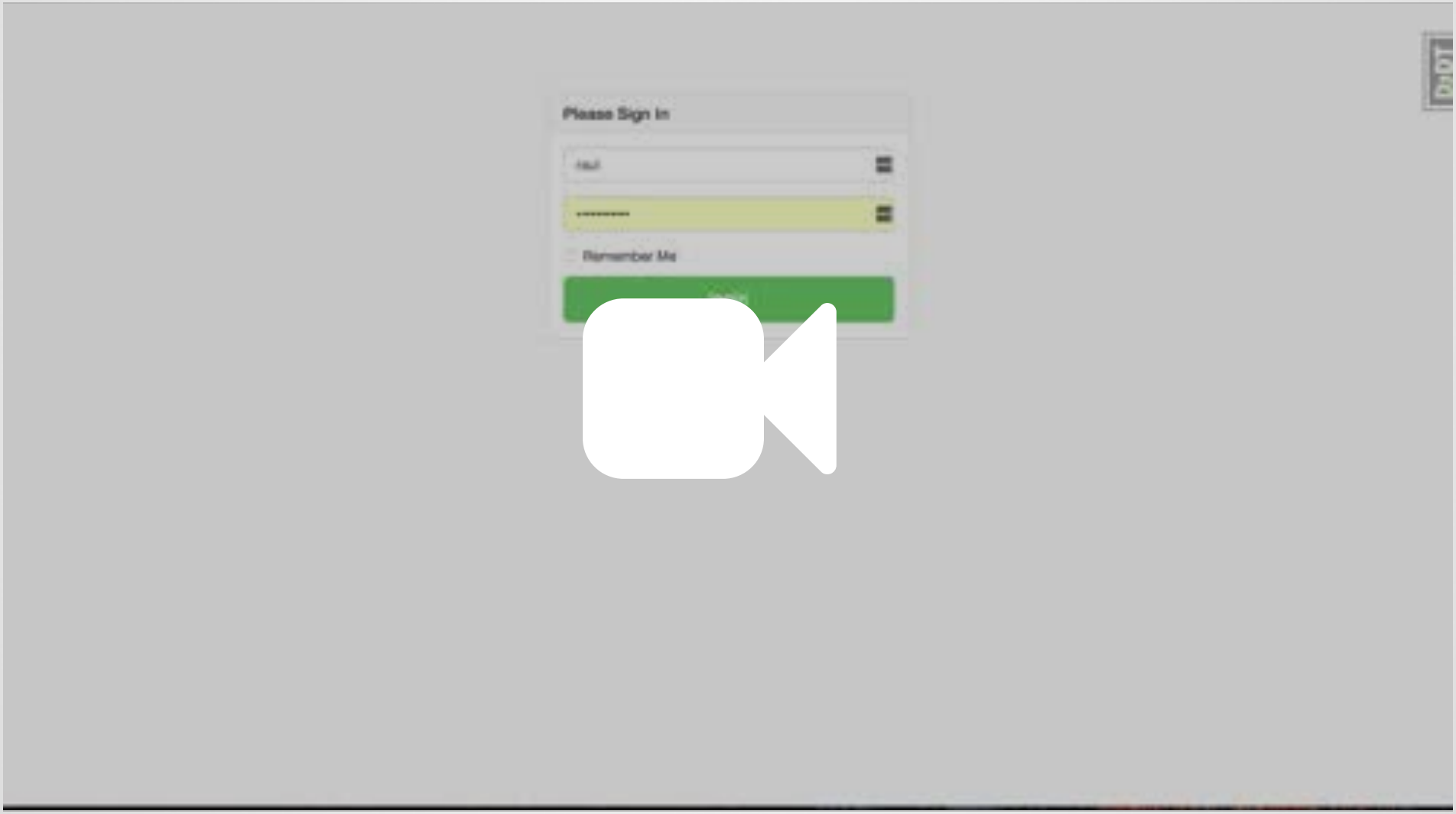
Basic Interface

GUI to vizualise weblogs files. Basic table to paginate, filter and search weblog data



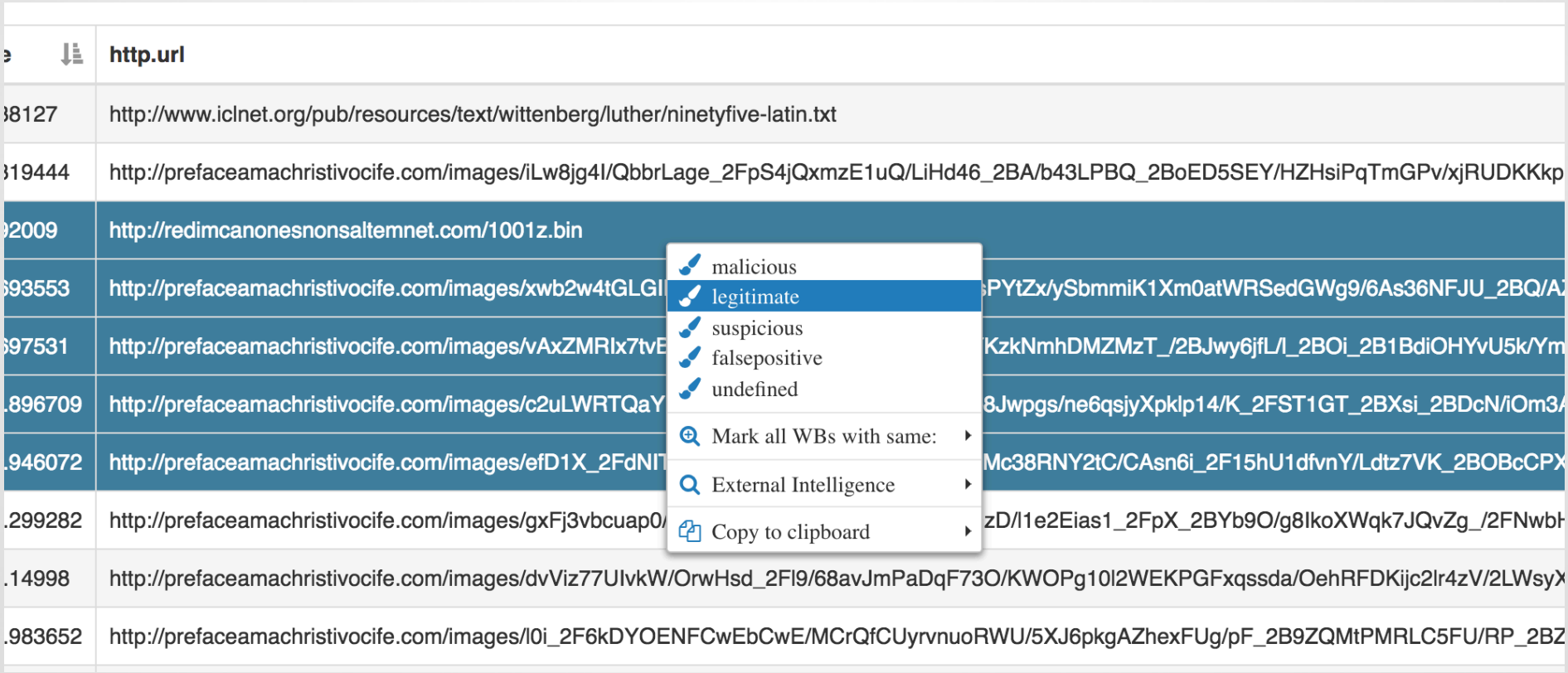
ts	uid	id.orig_h	id.orig_p	id.resp_h	id.resp_p	trans_depth	method	host	uri
210.866612	CnJxvm2YULCJBoUIL	192.168.1.115	49160	67.215.238.66	80	1	GET	download-lb.utorrent.com	/endpoint/hydra-ut/os/win7/track/stabl
212.555548	C69xbD1YhHt2w6Xmt6	192.168.1.115	49161	23.21.92.252	80	1	POST	i-50.b-000.xyz.bench.utorrent.com	/e?i=50
212.560502	Co9n9uk4VSsK3jOEc	192.168.1.115	49162	23.21.92.252	80	1	POST	i-50.b-000.xyz.bench.utorrent.com	/e?i=50
212.821824	COVg4d1VqsRtleh2Ml	192.168.1.115	49163	23.21.92.252	80	1	POST	i-50.b-000.xyz.bench.utorrent.com	/e?i=50
213.864970	C07YKn14q29pHIpVWk	192.168.1.115	49158	23.21.92.252	80	1	POST	i-50.b-000.xyz.bench.utorrent.com	/e?i=50
213.865122	CjCXxH2QqeVesprHg2	192.168.1.115	49159	23.21.92.252	80	1	POST	i-50.b-000.xyz.bench.utorrent.com	/e?i=50
231.277311	CuamD31TFvHM2cuSwb	192.168.1.115	49164	45.63.117.51	80	1	GET	ip-api.com	/json?callback=jQuery1910895111848
231.491526	CAK7Phe6gZuLoqiWf	192.168.1.115	49165	67.215.246.203	80	1	GET	update.utorrent.com	/featuredcontent.php?w=6.1
232.290995	CitHyJ1jymoSf5PSti	192.168.1.115	49166	23.21.92.252	80	1	GET	i-50.b-000.xyz.bench.utorrent.com	/e?i=50&e=eyJldmVudE5hbWUiOiJoe
249.367892	CFdgUEUZMAiiZvPld	192.168.1.115	49167	23.21.92.252	80	1	GET	i-50.b-000.xyz.bench.utorrent.com	/e?i=50&e=eyJldmVudE5hbWUiOiJoe
249.699403	CJhg3n1bTG9tJ51sKg	192.168.1.115	49168	23.21.92.252	80	1	POST	i-50.b-000.xyz.bench.utorrent.com	/e?i=50
250.247892	CQB4UG2AAzDpEyzra3	192.168.1.115	49169	98.143.146.7	80	1	GET	utorrent.com	/download/langpacks/dl.php?build=42

Demo Basic Dynamic Table

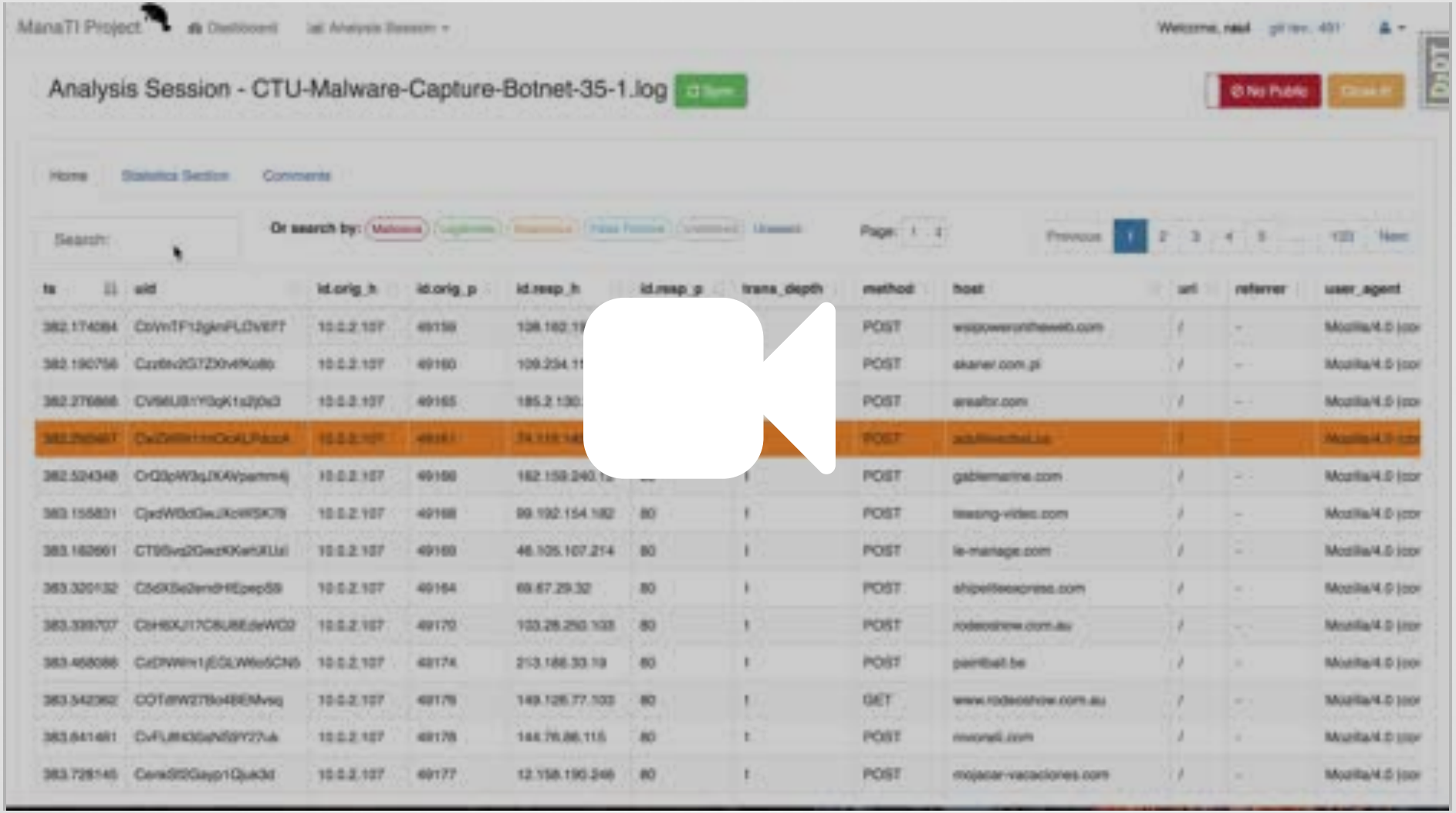


Weblogs Labelling

It is the basic and more important action for a malware behavior analyst. Detect malicious IoCs



Demo - Weblog labeling



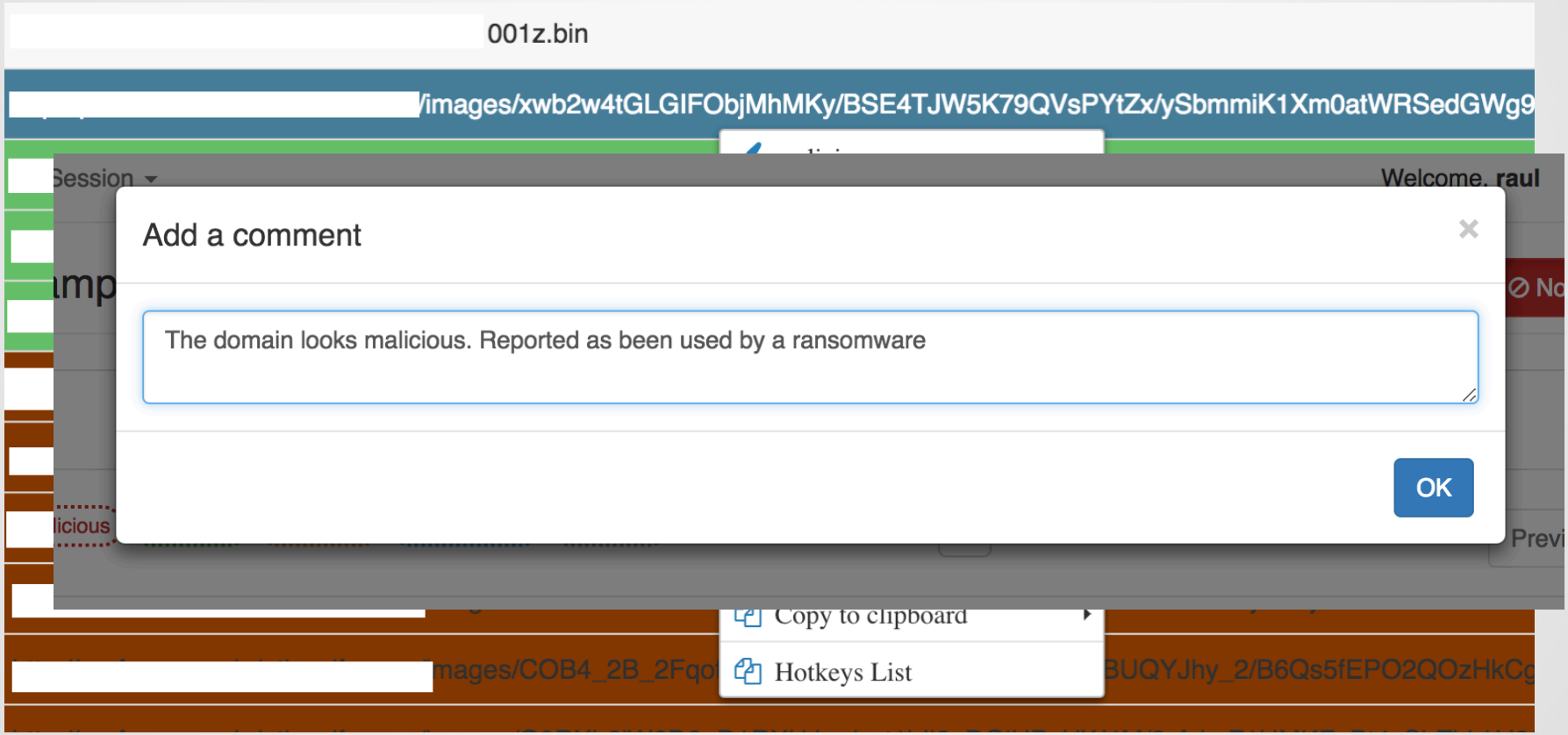
Exporting Dynamic Table

5769.187006	[redacted]images/YwBxC1l0JLaJhvqa4NhXCPH/86UQr2_2FV/AHGjCxXaQnYP7JkEJ/KM_
6169.8282	[redacted]images/SNF2_2BYPUAu/imisFBHnx9z/Fk_2B1l8x4pkvE/aDKo450yhlkgeP9h9Ft_
6568.989989	[redacted]KFbpOxbYbcffwWUFj/Obf7hbv221vu/WvTxA7whOqQ/CZBv7kQNMufkPx
6968.997117	[redacted]T7E4S_2F_2FOd4IrCEEVl/VkekyD7p1gEPc/Nj59G_2F/SsRMD3cf3nPP6
7369.3147	[redacted]hOCloYeIb2F/pcQec_2B_2Bcve/70uA3Asfo6BV_2FIG1G_2/FB7xXA0XW
7769.437834	[redacted]9jsSpof_2FkSh/41CIFLYh/rNmK34j8MssGlt3gA0I2gB5/EerFWN_2Fw/CqK
8169.13947	[redacted]nl2hF1qaMpgyAjvQKGc/lzTQWvt8u6af4og_2Bn/7ABKMwfNMKO35hRC
8569.23977	[redacted]J_2FFzLcquF098/KAWnWoODg/Z8hHGzHBC7K37ZGAXuQO/O7ZcF
8969.28119	[redacted]220dFHXVFr3G_2F/rZYPJLhzbgkTfjg/XLxEu0JukX_2BCCIZ2/6OkMVSc

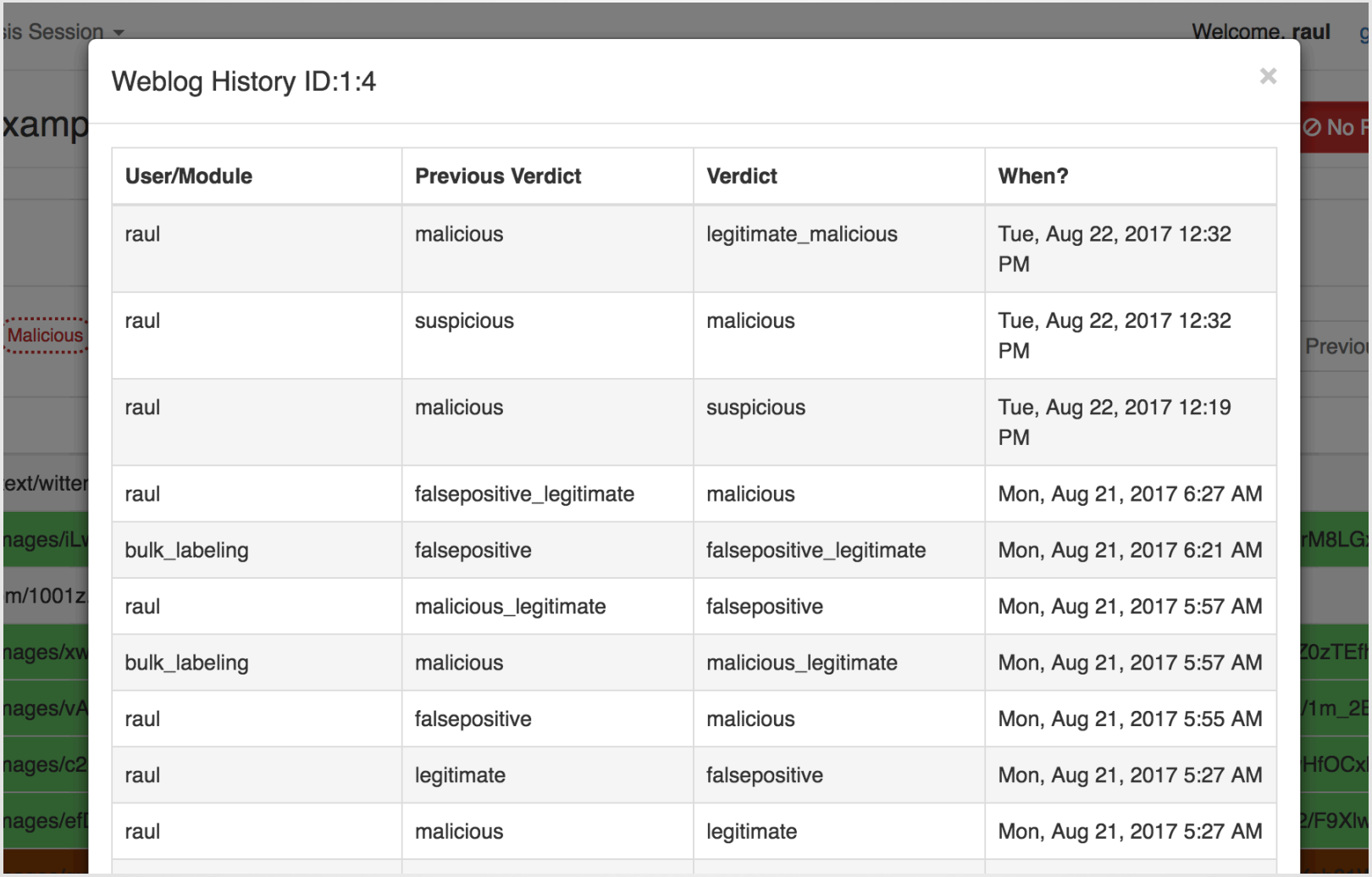
Show 25 entries

Copy | Excel | CSV | Column visibility

Comments


001z.bin
/images/xwb2w4tGLGIFObjMhMKy/BSE4TJW5K79QVsPYtZx/ySbmmiK1Xm0atWRSedGWg9
Session
Welcome, raul
Add a comment
The domain looks malicious. Reported as been used by a ransomware
OK
Copy to clipboard
Hotkeys List

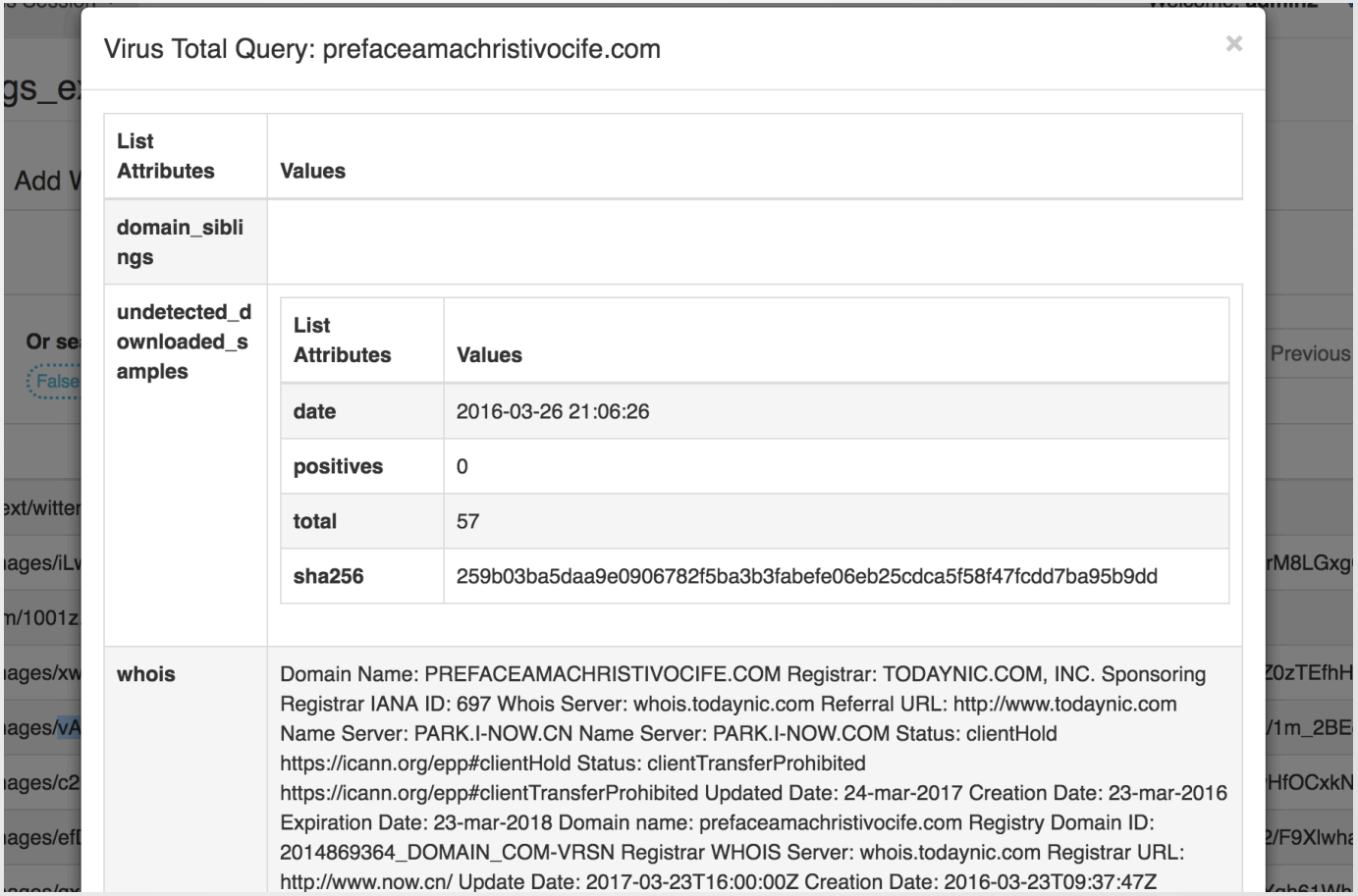
History of changes



User/Module	Previous Verdict	Verdict	When?
raul	malicious	legitimate_malicious	Tue, Aug 22, 2017 12:32 PM
raul	suspicious	malicious	Tue, Aug 22, 2017 12:32 PM
raul	malicious	suspicious	Tue, Aug 22, 2017 12:19 PM
raul	falsepositive_legitimate	malicious	Mon, Aug 21, 2017 6:27 AM
bulk_labeling	falsepositive	falsepositive_legitimate	Mon, Aug 21, 2017 6:21 AM
raul	malicious_legitimate	falsepositive	Mon, Aug 21, 2017 5:57 AM
bulk_labeling	malicious	malicious_legitimate	Mon, Aug 21, 2017 5:57 AM
raul	falsepositive	malicious	Mon, Aug 21, 2017 5:55 AM
raul	legitimate	falsepositive	Mon, Aug 21, 2017 5:27 AM
raul	malicious	legitimate	Mon, Aug 21, 2017 5:27 AM

Third-party intelligence tools

The threat analysts often use several external services to know about the IoCs



Virus Total Query: prefaceamachristivocife.com

List Attributes	Values
domain_siblings	
undetected_downloaded_samples	List Attributes / Values: date: 2016-03-26 21:06:26; positives: 0; total: 57; sha256: 259b03ba5daa9e0906782f5ba3b3fabefe06eb25cdca5f58f47fcdd7ba95b9dd
whois	Domain Name: PREFACEAMACHRISTIVOCIFE.COM Registrar: TODAYNIC.COM, INC. Sponsoring Registrar IANA ID: 697 Whois Server: whois.todaynic.com Referral URL: http://www.todaynic.com Name Server: PARK.I-NOW.CN Name Server: PARK.I-NOW.COM Status: clientHold https://icann.org/epp#clientHold Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Updated Date: 24-mar-2017 Creation Date: 23-mar-2016 Expiration Date: 23-mar-2018 Domain name: prefaceamachristivocife.com Registry Domain ID: 2014869364_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.todaynic.com Registrar URL: http://www.now.cn/ Update Date: 2017-03-23T16:00:00Z Creation Date: 2016-03-23T09:37:47Z

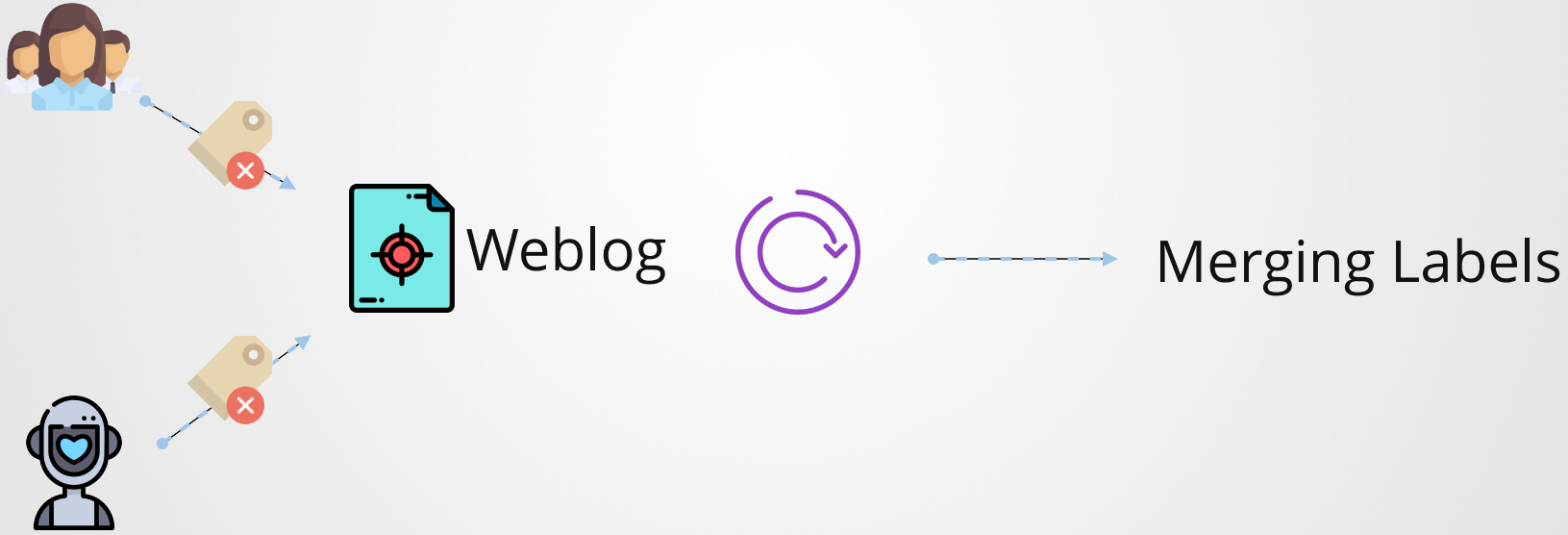
Statistics and Metrics

See in real time the perfomance progress of the user

External Modules

ManaTI allows analysts to create their own scripts and modules to increase the number of labels or weblogs analyzed in a period of time

Sync with Database - Merging Labels

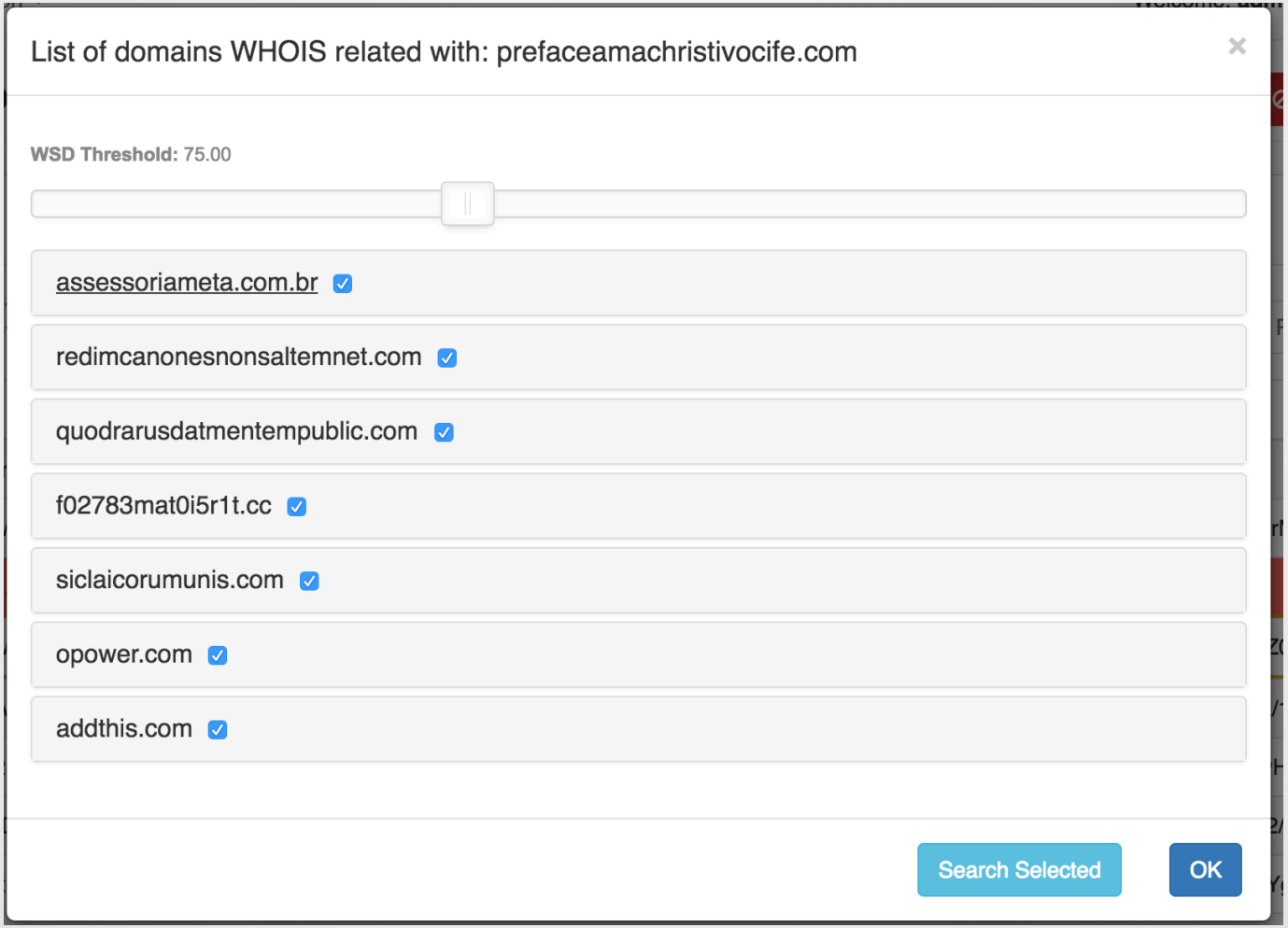


WHOIS Similarity Distance Algorithm

How similar are two domains ?

WHOIS fields	Domain A	Domain B	Distance
registrar's name	MARKMONITOR INC.	MARKMONITOR IN	0.0
contact's name.	DNS Admin	Domain Administrator	13.0
org.'s name	Google Inc.	Facebook, Inc.	8.0
contacts emails	dns-admin@google.com	[domain@fb.com]	11.0
zip code	94043	94025	2.0
domain's name	google.com	facebook.com	8.0
duration in days	8401	10229	0.82
servers' name	[ns1.google.com,...]	[a.ns.facebook.com ...]	11.0

WHOIS Similarity Distance Algorithm



WHOIS Similarity Distance Algorithm

 **How to determine is two domains are related?**

 **Machine Learning ?**

https://github.com/stratosphereips/whois-similarity-distance

ManaTI Contributions

All-in-one with Web interface

A scalable and extensible backend server

A novel WHOIS distance measure

Verification of performance improvements

Future of ManaTI

- Improving WHOIS Similarity Distance
- IOCs labeling
- Import/Export labelled IOCs
- Integration with Stratosphere IPS
- Add more types of files
- Malware Detection
- Active learning
- Community Ideas

Conclusion

ManaTI : is a novel tool to facilitate the work

is high functional scalable

user-friendly

can increase the weblogs labelling speed x3.4

OpenSource !

ManaTI Project

Thank you!

SEBASTIÁN GARCÍA

sebastian.garcia@agents.fel.cvut.cz

@eldracote

RAÚL BENÍTEZ NETTO

benitrau@fit.cvut.cz

raulbeni@gmail.com

@Piuliss

https://github.com/stratosphereips/Manati