https://doi.org/10.2352/ISSN.2470-1173.2021.3.MOBMU-043

Design of Professional Laboratory Exercises for Effective State-of-the-Art OSINT Investigation Tools - Part 1: RiskIQ Passive-Total

Klaus Schwarz[2,3], *Reiner Creutzburg*[1,2]

[1] *Technische Hochschule Brandenburg, Department of Informatics and Media, IT- and Media Forensics Lab, Magdeburger Str. 50, D-14770 Brandenburg, Germany*
Email: creutzburg@th-brandenburg.de

[2] *SRH Berlin University of Applied Sciences, Berlin School of Technology, Ernst-Reuter-Platz 10, D-10587 Berlin, Germany*
Email: klaus.schwarz@srh.de, reiner.creutzburg@srh.de

[3] *The University of Texas at San Antonio, College of Engineering, 1 UTSA Circle, San Antonio, TX 78249-0669, USA*

Abstract

Open-source technologies (OSINT) are becoming increasingly popular with investigative and government agencies, intelligence services, media companies, and corporations.
These OSINT technologies use sophisticated techniques and special tools to analyze the continually growing sources of information efficiently.
There is a great need for professional training and further education in this field worldwide.
After having already presented the overall structure of a professional training concept in this field in a previous paper [25], this series of articles offers individual further training modules for the worldwide standard state-of-the-art OSINT tools.
The modules presented here are suitable for a professional training program and an OSINT course in a bachelor's or master's computer science or cybersecurity study at a university.
In this part 1 of a series of 4 articles, the OSINT tool RiskIQ PassivTotal [26] is introduced, and its application possibilities are explained using concrete examples. In part 2 the OSINT tool Censys is explained [27]. Part 3 deals with Maltego [28] and Part 4 compares the 3 different tools of Part 1-3 [29].

Introduction and Motivation

Security and forensics experts today are confronted with extremely skilled, malicious, persistent threats and attacks [2]. The good news for analysts is that data can help expose the infrastructure used by attackers. In this way, attacks can be found, blocked, and prevented. PASSIVETOTAL accelerates investigations by linking internal activities, events, and indicators of threats to what is happening outside the firewall - making external threats, attackers, and associated infrastructure visible [1].

PassiveTotal – Accompanying Theory

PASSIVETOTAL centralizes numerous data sets on a single platform, making it easier to perform infrastructure analyses [3].

After entering the URL in the page's search line, one will be taken directly to the analysis page. At the top, one can see the so-called Heatmap. The PASSIVETOTAL Heatmap visualizes the last six months of passive DNA resolution information in a clear graph that allows analysts to quickly review large amounts of data and improve the evaluation of suspicious indicators (Fig. 1).

In the heatmap (Fig. 1), each box represents a single day. The heatmap uses colors, symbols, and numbers to create a context for passive DNS data. In the timeline below, one can also access and analyze periods that are further back in time.

There are two types of heat maps that are generated in PASSIVETOTAL. One for IP addresses and one for domains.
Heatmap symbols

- Blue Box - Represents a domain that is resolved to a publicly routable IP address.
- Green Box - Indicates that PASSIVETOTAL has observed the domain resolved on the same day for both public and non-public routable IP space.
- Orange Flags - This is the first time that a resolution is seen in passive DNS records.
- Rounded Fields - Provides a visual representation of the first and last day of a month.
- Numbers - Represents the number of domains or IP addresses called on a given day in the last 6 months.

Below the heatmap we find a bar with 12 different tabs for data analysis (Fig. 2):

1. **Resolutions**
   This tab contains data records for resolving the domain name into an IP address. This provides information about the time period during which the page was reached under which IP address. Each individual record has a start date and an end date. The last call has accordingly the current date or the date on which the page could last be called. (Fig. 3).
2. **WHOIS**
   WHOIS is a protocol that allows anyone to search for information about a domain, IP address, or subnet. One of the most common functions of the WHOIS in threat infrastructure research is to identify or link different units based on

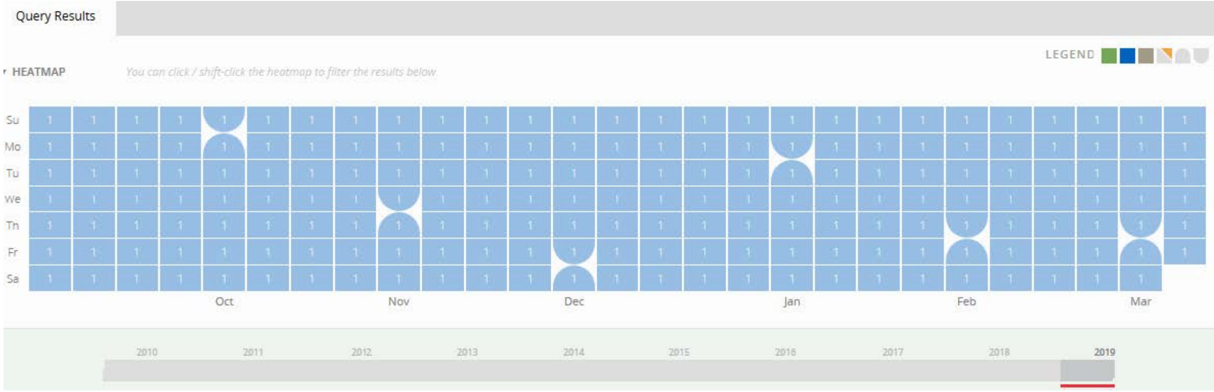


Figure 1. PASSIVETOTAL – *Heatmap*

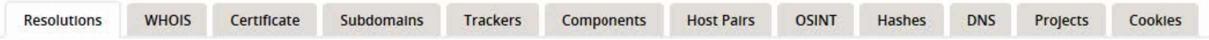
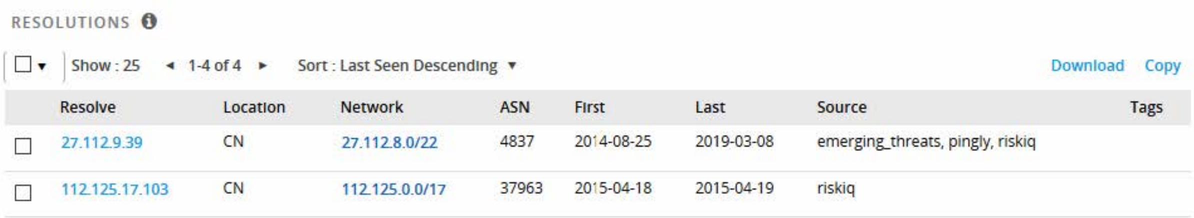


Figure 2. *Tab to select different data sets*



	Resolve	Location	Network	ASN	First	Last	Source	Tags
□	27.112.9.39	CN	27.112.8.0/22	4837	2014-08-25	2019-03-08	emerging_threats, pingly, riskiq	
□	112.125.17.103	CN	112.125.0.0/17	37963	2015-04-18	2015-04-19	riskiq	

Figure 3. PASSIVETOTAL – *Resolutions*

unique data shared in WHOIS datasets.

Each WHOIS record (Fig. 4) has several different sections, each of which may contain different information. Frequently found sections are "Registrar", "Registrant", "Administrator’" and "Technical", with each section possibly corresponding to a different contact for recording. In most cases, this data is duplicated section by section, but in some cases, there may be slight differences, especially if an actor has made a mistake. When WHOIS information is displayed within PASSIVETOTAL, you see a compressed data set that duplicates all data and notes from which part of the data set it originates. This process speeds up the analysis considerably and also prevents data from being overlooked.

3. **Certificate**

   When surfing the web, SSL Certificates are everywhere. Similar to a WHOIS record, SSL certificates require the user to provide information to generate the end product. Except for the domain for which the SSL certificate is created (unless self-signed), the user can create any of the additional information. SSL certificates' most significant value does not necessarily lie in the unique data that someone can use to create them but where they are hosted.

   What makes SSL Certificates more valuable is that they can establish connections that can be overlooked in passive DNS or WHOIS data. This means more ways to correlate potentially malicious infrastructures and identify potential outages in the actors' operational security. PASSIVETOTAL has collected over 30 million certificates from 2013 to date [4].

4. **Subdomains**

   The subdomains that PASSIVETOTAL could find in the context of the searched page over time can be found here. Each domain listed here has tags that identify a subpage differently (Fig. 5). This information can quickly be used to conclude the site's infrastructure. In the case of malicious sites, conclusions can be drawn about various campaigns such as phishing.

5. **Trackers**

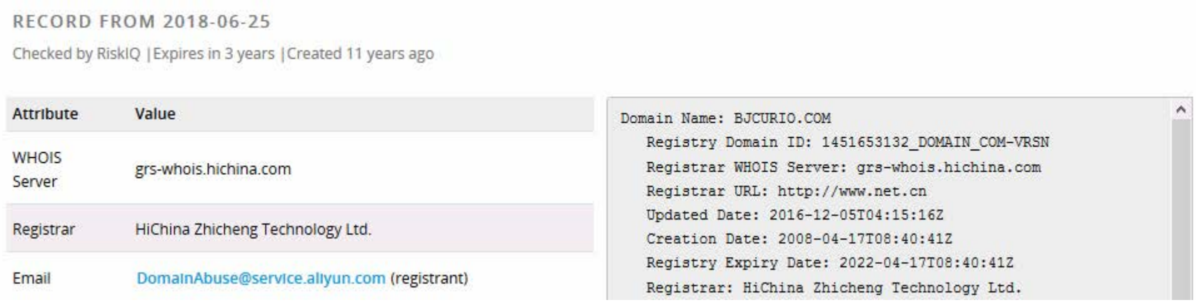
   Trackers are unique codes or values found on Web sites and are often used to track user interaction. These codes can be used to link a heterogeneous group of websites to a central entity. The tracker record of PASSIVETOTAL contains IDs of providers such as Google, Yandex, Mixpanel, New Relic, Clicky, etc. (Fig. 6).

6. **Components**

   Web components describe a Web site or server infrastructure obtained by performing a Web crawl using RiskIQ technology. These components provide a comprehensive understanding of what was used to host the site and what technologies were loaded at the Web search time. Whenever possible, PASSIVETOTAL will attempt to categorize the specific components and specify version numbers. (Fig. 7) [5].

7. **Host Pairs**

   Host pairs are two domains (a parent and a child) that share a connection observed by a RiskIQ web crawl. The connec-

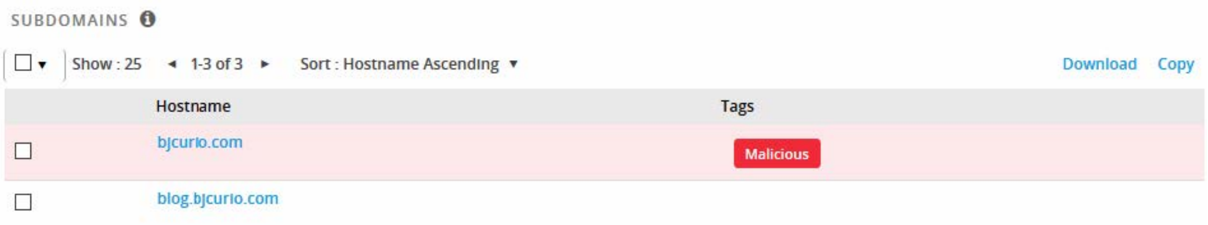

RECORD FROM 2018-06-25

Checked by RiskIQ |Expires in 3 years |Created 11 years ago

Attribute	Value
WHOIS Server	grs-whois.hichina.com
Registrar	HiChina Zhicheng Technology Ltd.
Email	DomainAbuse@service.aliyun.com (registrant)

```
Domain Name: BJCURIO.COM
   Registry Domain ID: 1451653132_DOMAIN_COM-VRSN
   Registrar WHOIS Server: grs-whois.hichina.com
   Registrar URL: http://www.net.cn
   Updated Date: 2016-12-05T04:15:16Z
   Creation Date: 2008-04-17T08:40:41Z
   Registry Expiry Date: 2022-04-17T08:40:41Z
   Registrar: HiChina Zhicheng Technology Ltd.
```

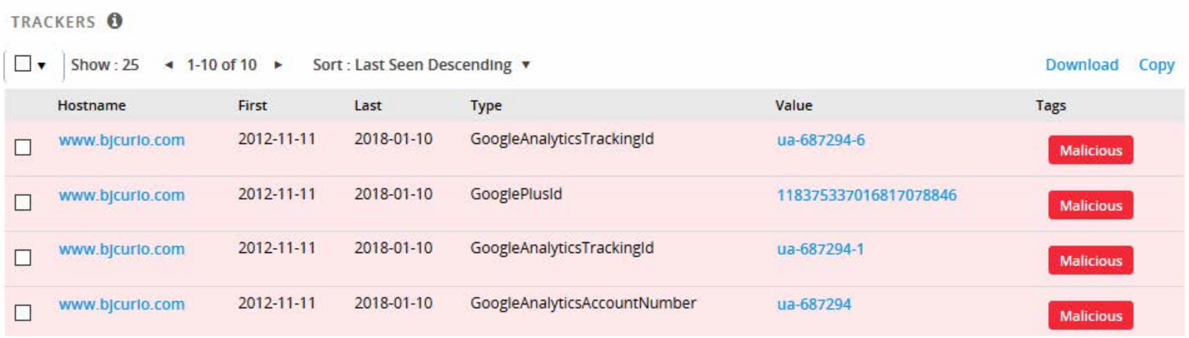
Figure 4. PASSIVETOTAL – *WHOIS*


SUBDOMAINS

□ ▾ Show : 25 ◂ 1-3 of 3 ▸ Sort : Hostname Ascending ▾ Download Copy

	Hostname	Tags
□	bjcurio.com	Malicious
□	blog.bjcurio.com	

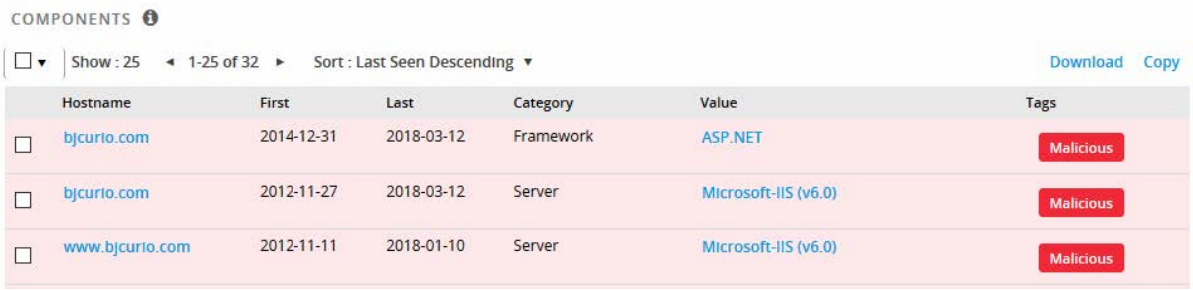
Figure 5. PASSIVETOTAL – *Subdomains*


TRACKERS

□ ▾ Show : 25 ◂ 1-10 of 10 ▸ Sort : Last Seen Descending ▾ Download Copy

	Hostname	First	Last	Type	Value	Tags
□	www.bjcurio.com	2012-11-11	2018-01-10	GoogleAnalyticsTrackingId	ua-687294-6	Malicious
□	www.bjcurio.com	2012-11-11	2018-01-10	GooglePlusId	118375337016817078846	Malicious
□	www.bjcurio.com	2012-11-11	2018-01-10	GoogleAnalyticsTrackingId	ua-687294-1	Malicious
□	www.bjcurio.com	2012-11-11	2018-01-10	GoogleAnalyticsAccountNumber	ua-687294	Malicious

Figure 6. PASSIVETOTAL – *Trackers*

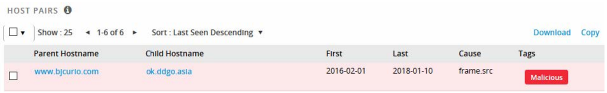

COMPONENTS

□ ▾ Show : 25 ◂ 1-25 of 32 ▸ Sort : Last Seen Descending ▾ Download Copy

	Hostname	First	Last	Category	Value	Tags
□	bjcurio.com	2014-12-31	2018-03-12	Framework	ASP.NET	Malicious
□	bjcurio.com	2012-11-27	2018-03-12	Server	Microsoft-IIS (v6.0)	Malicious
□	www.bjcurio.com	2012-11-11	2018-01-10	Server	Microsoft-IIS (v6.0)	Malicious

Figure 7. PASSIVETOTAL – *Components*

tion could range from a top-level redirection (HTTP 302) to something more complex like an iframe or a script source reference. (Fig. 8).


HOST PAIRS

□ ▾ Show : 25 ◂ 1-6 of 6 ▸ Sort : Last Seen Descending ▾ Download Copy

	Parent Hostname	Child Hostname	First	Last	Cause	Tags
□	www.bjcurio.com	ok.ddgo.asia	2016-02-01	2018-01-10	frame.src	Malicious

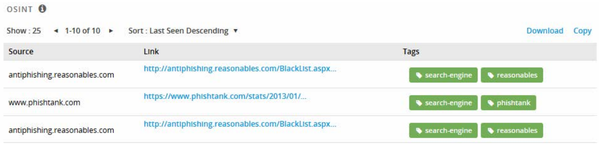
Figure 8. PASSIVETOTAL – *Host Pairs*

8. OSINT

Open Source Intelligence (OSINT) is a report, both short and long, developed by individuals and companies describing specific threats, methods or actors. PASSIVETOTAL maintains an extensive repository of parsed data from blogs, research papers, and presentations to map these reports to the infrastructure within the platform (Fig. 9) [8].

The data from the OSINT repository is public and freely accessible for all platform users. Once identified, OSINT data and its classification (i.e., malicious, not malicious, suspicious or unknown) are displayed on the item to be queried.

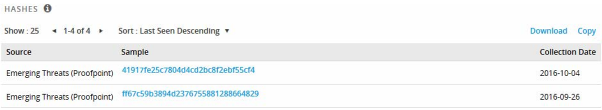
Users can click on the OSINT tab to view the detailed reporting or extract details from the context tags associated with the queried indicator [6].



Source	Link	Tags
antiphishing.reasonables.com	http://antiphishing.reasonables.com/BlackList.aspx...	search-engine reasonables
www.phishtank.com	https://www.phishtank.com/stats/2013/01/...	search-engine phishtank
antiphishing.reasonables.com	http://antiphishing.reasonables.com/BlackList.aspx...	search-engine reasonables

Figure 9. PASSIVETOTAL – *OSINT*

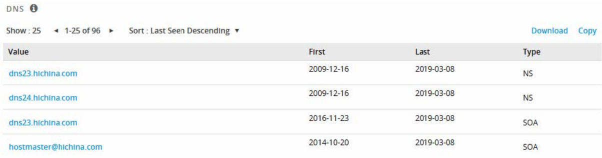
9. **Hashes**
   Files in the form of hashes that in the past could be associated with the domain or its infrastructure can be found here (Fig. 10). The data obtained in this way provides information about connections with other domains and infrastructures in which these files also appeared in the past.



Source	Sample	Collection Date
Emerging Threats (Proofpoint)	41917fe25c7804d4cd2bc8f2ebf55cf4	2016-10-04
Emerging Threats (Proofpoint)	ff67c59b3894d2376755881288664829	2016-09-26

Figure 10. PASSIVETOTAL – *Hashes*

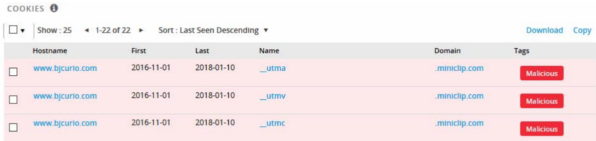
10. **DNS**
    DNS entries are like the phone book of the Internet. Not only do they provide information about the IP address behind a domain, but they also provide information about MX (Mail-Exchanger), NS (Name server), TXT (Text), SOA (Start of Authority), and CNAME (Canonical Name) records. These record types are interesting because some malicious players might use certain name servers (NS records) to segment their infrastructure over and over again or configure only one specific mail provider (MX records) to manage their command and control channel. More complex data types such as SOA and TXT provide unique information about the opposing infrastructure. For example, when registering a domain, a valid email address is required to complete the process. Experienced players can choose to protect their data through data protection, but their original email address can be included in an SOA record associated with the DNS zone without their knowledge. Analysts can perform a search in the WHOIS data to find more domains registered with this email. PASSIVETOTAL processes this data as follows (Fig. 11).



Value	First	Last	Type
dns23.hichina.com	2009-12-16	2019-03-08	NS
dns24.hichina.com	2009-12-16	2019-03-08	NS
dns23.hichina.com	2016-11-23	2019-03-08	SOA
hostmaster@hichina.com	2014-10-20	2019-03-08	SOA

Figure 11. PASSIVETOTAL – *DNS*

11. **Projects**
    In PASSIVETOTAL so-called projects can be created over a set of data. There are private and public projects. If there is a public project for a specific domain, it can be found here.
12. **Cookies**
    Cookies do not only offer the possibility of making a particular data state persistent on a page, such as a shopping cart, for example. They also provide an easy way to track a user across multiple pages. PASSIVETOTAL collects cookies and offers the ability to show changes in a website´s behavior. For example, different campaigns can be easily displayed (Fig. 12) [7].



	Hostname	First	Last	Name	Domain	Tags
□	www.bjcurio.com	2016-11-01	2018-01-10	__utma	.miniclip.com	Malicious
□	www.bjcurio.com	2016-11-01	2018-01-10	__utmv	.miniclip.com	Malicious
□	www.bjcurio.com	2016-11-01	2018-01-10	__utmc	.miniclip.com	Malicious

Figure 12. PASSIVETOTAL – *Cookies*

Extraction capabilities

PASSIVETOTAL offers the possibility to download single or collected and aggregated data sets as CSV for each of the tabs listed above. To do so, the datasets on the left must be selected with a checkmark and can then be downloaded via the download link on the right (Fig. 13).

PassiveTotal-API

Exercise 1 (Obtaining the PASSIVETOTAL API key)

PASSIVETOTAL *of course also offers an API interface. This can be set up as follows.*

1. *First click on the link* **Settings** *on the main page. (Fig. 14).*
2. *Afterwards, the API key and the Secret can be viewed in the settings under* **API ACCESS** *via the link* **Show** *(Fig. 15).*

The API is a simple REST API. This means that calls can be made via fixed addresses. A simple client is even possible with the Linux console. A simple Python client looks like this (Fig. 16).

This client returns the following results (Fig. 17):

Exercise 2 (PASSIVETOTAL API client setup)

Of course PASSIVETOTAL *also offers ready-made clients for their use and further development. Among them are a Rust-, a Ruby- and a Python-Client. The developer page of the Python client is available at the following URL:*

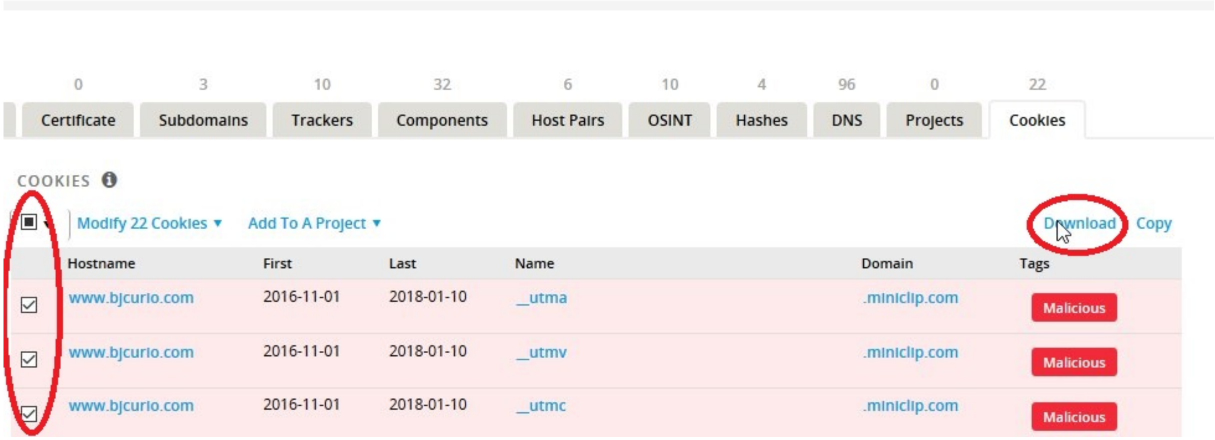
https://github.com/PassiveTotal/python_api.

However, they are very limited and should instead be regarded as a starting point for in-house development. In this exercise, you will therefore use a custom development of the client. This is available at the following address:

https://github.com/nored/PassiveTotal.

The client offers the following options:

- *Passive DNS queries*
- *Query of website components*
- *Query website trackers*
- *Query of subdomains*
- *Query malware knowledge about a given URL*



0	3	10	32	6	10	4	96	0	22
Certificate	Subdomains	Trackers	Components	Host Pairs	OSINT	Hashes	DNS	Projects	Cookies

COOKIES

☑	Hostname	First	Last	Name	Domain	Tags
☑	www.bjcurio.com	2016-11-01	2018-01-10	__utma	.miniclip.com	Malicious
☑	www.bjcurio.com	2016-11-01	2018-01-10	__utmv	.miniclip.com	Malicious
☑	www.bjcurio.com	2016-11-01	2018-01-10	__utmc	.miniclip.com	Malicious

Figure 13. *Download of collected data*

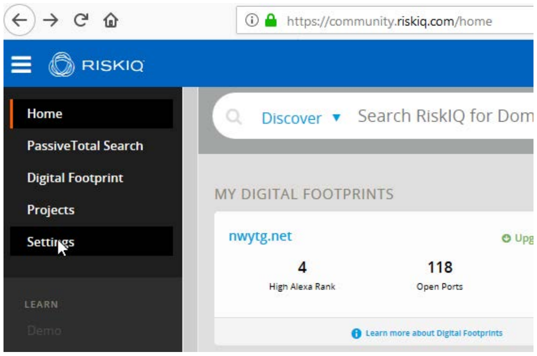
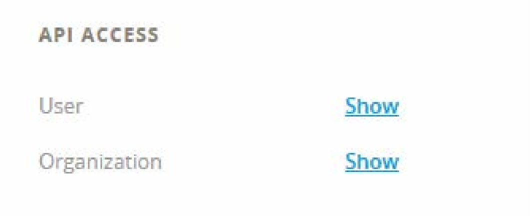


Figure 14. PASSIVETOTAL *– Settings menu*



API ACCESS

User Show

Organization Show

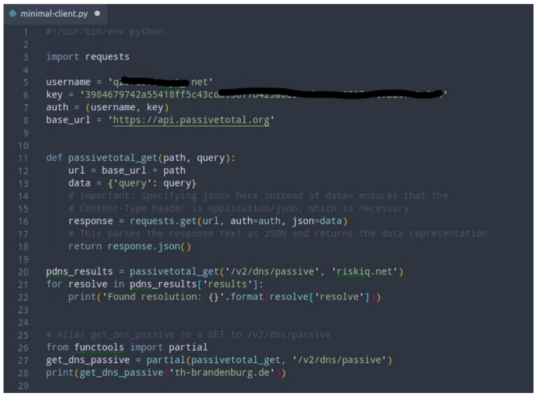
Figure 15. *Obtaining the API key*

- *WHOIS queries*
- *SSL certificates*
- *Export of the generated data records into the CSV format.*

The client can be set up relatively easy in the previously used virtual machine.

1. *To do this, open a terminal window and enter the following commands:*
   (a) **git clone https://github.com/nored/PassiveTotal.git**
   (b) **cd PassiveTotal**

2. *After entering and successfully running both commands, you should now be in the program directory. Start the program with the following command (Fig. 18):*



minimal-client.py ●

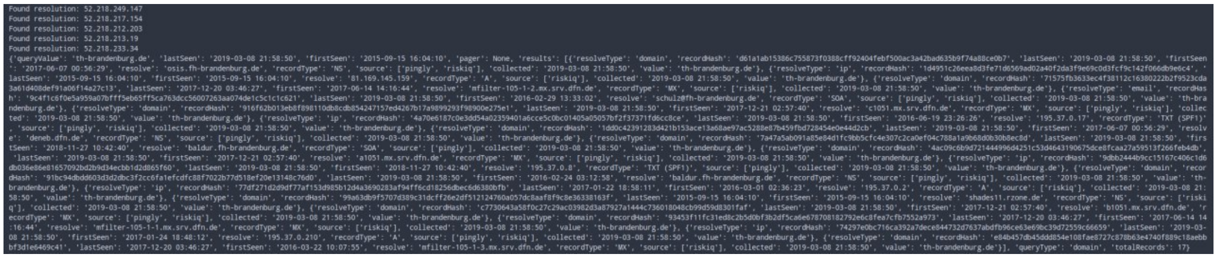
```python
#!/usr/bin/env python

import requests

username = 'q[redacted]net'
key = '3984679742a55418ff5c43cd[redacted]'
auth = (username, key)
base_url = 'https://api.passivetotal.org'


def passivetotal_get(path, query):
    url = base_url + path
    data = {'query': query}
    # Important: Specifying json= here instead of data= ensures that the
    # Content-Type header is application/json, which is necessary.
    response = requests.get(url, auth=auth, json=data)
    # This parses the response text as JSON and returns the data representation.
    return response.json()

pdns_results = passivetotal_get('/v2/dns/passive', 'riskiq.net')
for resolve in pdns_results['results']:
    print('Found resolution: {}'.format(resolve['resolve']))


# Alias get_dns_passive to a GET to /v2/dns/passive
from functools import partial
get_dns_passive = partial(passivetotal_get, '/v2/dns/passive')
print(get_dns_passive('th-brandenburg.de'))
```

Figure 16. *Simple API client in Python*

./minimal-client.py -a pdns -q th-brandenburg.de

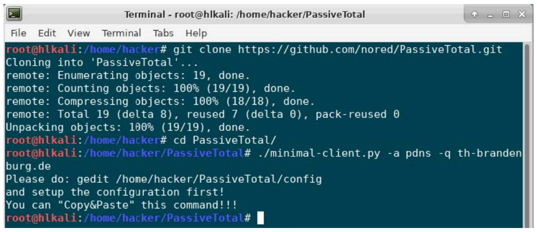
3. *Now you should be able to read the following output:*
4. *You can copy the command from the output or open the file with a text editor of your choice.*
5. *Fill in the missing fields* **api_key** *and* **api_username** *(Fig. 19).*
6. *The e-mail and the* **api_key can be** *found in the API data as described above.*

7. *After the successful setup, the client can be used.*



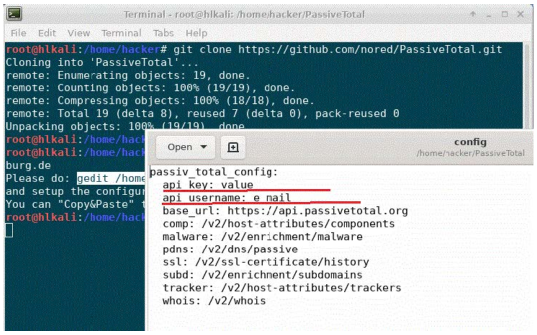
```
Found resolution: 52.218.249.147
Found resolution: 52.218.217.154
Found resolution: 52.218.212.203
Found resolution: 52.218.213.19
Found resolution: 52.218.233.34
{'queryValue': 'th-brandenburg.de', 'lastSeen': '2019-03-08 21:58:50', 'firstSeen': '2015-09-15 16:04:10', 'pager': None, 'results': [{'resolveType': 'domain', 'recordHash': 'd61a1ab15386c755873f0388cff92404febf500ac3a42bad635b9f74a88ce0b7', 'lastSeen': '2019-03-08 21:58:50', 'firstSeen
': '2017-06-07 00:56:29', 'resolve': 'osis.fh-brandenburg.de', 'recordType': 'NS', 'source': ['pingly', 'riskiq'], 'collected': '2019-03-08 21:58:50', 'value': 'th-brandenburg.de'}, {'resolveType': 'ip', 'recordHash': '1d4951c26eea8d3fe71d6569ad02a40f2da3f9e69c0d3fcf9c142f066db9e6c4', '
lastSeen': '2015-09-15 16:04:10', 'firstSeen': '2015-09-15 16:04:10', 'resolve': '81.169.145.159', 'recordType': 'A', 'source': ['riskiq'], 'collected': '2019-03-08 21:58:50', 'value': 'th-brandenburg.de'}, {'resolveType': 'domain', 'recordHash': '71575fb3633ec4f38112c16380222b2f9523cda
3a61d408def91a06f14a27c13', 'lastSeen': '2017-12-20 03:46:27', 'firstSeen': '2017-06-14 14:16:44', 'resolve': 'mfilter-105-1-2.mx.srv.dfn.de', 'recordType': 'MX', 'source': ['riskiq'], 'collected': '2019-03-08 21:58:50', 'value': 'th-brandenburg.de'}, {'resolveType': 'email', 'recordHas
h': '9c4f1c6f0e5a959a07bfff5eb65ff5ca763dcc56007263aa074de1c5c1c1c621', 'lastSeen': '2019-03-08 21:58:50', 'firstSeen': '2016-02-29 13:33:02', 'resolve': 'schulz@fh-brandenburg.de', 'recordType': 'SOA', 'source': ['pingly', 'riskiq'], 'collected': '2019-03-08 21:58:50', 'value': 'th-bra
ndenburg.de'}, {'resolveType': 'domain', 'recordHash': '916f62b013eb8f898110db8cdb854247157ed4267b17a9899293f98900e275e1', 'lastSeen': '2019-03-08 21:58:50', 'firstSeen': '2017-12-21 02:57:40', 'resolve': 'c1051.mx.srv.dfn.de', 'recordType': 'MX', 'source': ['pingly', 'riskiq'], 'collec
ted': '2019-03-08 21:58:50', 'value': 'th-brandenburg.de'}, {'resolveType': 'ip', 'recordHash': '4a70e6187c0e3dd54a02359401a6cce5c0bc01405a05057bf2f37371fd6cc8ce', 'lastSeen': '2019-03-08 21:58:50', 'firstSeen': '2016-06-19 23:26:26', 'resolve': '195.37.0.17', 'recordType': 'TXT (SPF1)'
, 'source': ['pingly', 'riskiq'], 'collected': '2019-03-08 21:58:50', 'value': 'th-brandenburg.de'}, {'resolveType': 'domain', 'recordHash': '1dd0c42391283d421b153ace13a68ae97ac5288e87b459fbd728454e0e44d2cb', 'lastSeen': '2019-03-08 21:58:50', 'firstSeen': '2017-06-07 00:56:29', 'resolv
e': 'deneb.dfn.de', 'recordType': 'NS', 'source': ['pingly', 'riskiq'], 'collected': '2019-03-08 21:58:50', 'value': 'th-brandenburg.de'}, {'resolveType': 'domain', 'recordHash': '7a47a5ab091a85e84d1fc9bb5cfc4e307c2ca0ef04c788a1a9b68d0b30b8ec8d', 'lastSeen': '2019-03-08 21:58:50', 'firs
tSeen': '2018-11-27 10:42:40', 'resolve': 'baldur.fh-brandenburg.de', 'recordType': 'SOA', 'source': ['pingly'], 'collected': '2019-03-08 21:58:50', 'value': 'th-brandenburg.de'}, {'resolveType': 'domain', 'recordHash': '4ac09c6b9d721444996d4251c53d4643190675dce8fcaa27a59513f266feb4db',
 'lastSeen': '2019-03-08 21:58:50', 'firstSeen': '2017-12-21 02:57:40', 'resolve': 'a1051.mx.srv.dfn.de', 'recordType': 'MX', 'source': ['pingly', 'riskiq'], 'collected': '2019-03-08 21:58:50', 'value': 'th-brandenburg.de'}, {'resolveType': 'ip', 'recordHash': '9dbb2444b9cc15167c406c1d6
db036e86e81657092bd2b9d34ecbb1d2d865f60', 'lastSeen': '2019-03-08 21:58:50', 'firstSeen': '2018-11-27 10:42:40', 'resolve': '195.37.0.8', 'recordType': 'TXT (SPF1)', 'source': ['pingly'], 'collected': '2019-03-08 21:58:50', 'value': 'th-brandenburg.de'}, {'resolveType': 'domain', 'recor
dHash': '91bc94dbdd603d3d2dbc3f2cc6fa1efcdfc88f7022b77d518ef20e13148c76d0', 'lastSeen': '2019-03-08 21:58:50', 'firstSeen': '2016-02-24 03:12:58', 'resolve': 'baldur.fh-brandenburg.de', 'recordType': 'NS', 'source': ['pingly', 'riskiq'], 'collected': '2019-03-08 21:58:50', 'value': 'th-
brandenburg.de'}, {'resolveType': 'ip', 'recordHash': '77df271d2d9df77af153d985b12d4a3690283af94ff6cd18256dbec6d6380bfb', 'lastSeen': '2017-01-22 18:58:11', 'firstSeen': '2016-03-01 02:36:23', 'resolve': '195.37.0.2', 'recordType': 'A', 'source': ['riskiq'], 'collected': '2019-03-08 21:
58:50', 'value': 'th-brandenburg.de'}, {'resolveType': 'domain', 'recordHash': '99a63db9f5707d389c31dcff26e2df512124760a057dc8aaf8f9c8e36338163f', 'lastSeen': '2015-09-15 16:04:10', 'firstSeen': '2015-09-15 16:04:10', 'resolve': 'shades11.rzone.de', 'recordType': 'NS', 'source': ['riski
q'], 'collected': '2019-03-08 21:58:50', 'value': 'th-brandenburg.de'}, {'resolveType': 'domain', 'recordHash': 'c7730643a58f0c27c29ac03982d3a87927a1444c736018048cb99d59d8301faf', 'lastSeen': '2019-03-08 21:58:50', 'firstSeen': '2017-12-21 02:57:40', 'resolve': 'b1051.mx.srv.dfn.de', 'r
ecordType': 'MX', 'source': ['pingly', 'riskiq'], 'collected': '2019-03-08 21:58:50', 'value': 'th-brandenburg.de'}, {'resolveType': 'domain', 'recordHash': '93453f11fc31ed8c2b5d0bf3b2df5ca6e678708182792e6c8fea7cfb7552a973', 'lastSeen': '2017-12-20 03:46:27', 'firstSeen': '2017-06-14 14
:16:44', 'resolve': 'mfilter-105-1-1.mx.srv.dfn.de', 'recordType': 'MX', 'source': ['riskiq'], 'collected': '2019-03-08 21:58:50', 'value': 'th-brandenburg.de'}, {'resolveType': 'ip', 'recordHash': '74297e0bc716ca392a7dece844732d7637abdfb96ce63e69bc39d72559c66659', 'lastSeen': '2019-03-
08 21:58:50', 'firstSeen': '2017-01-24 18:48:12', 'resolve': '195.37.0.210', 'recordType': 'A', 'source': ['pingly', 'riskiq'], 'collected': '2019-03-08 21:58:50', 'value': 'th-brandenburg.de'}, {'resolveType': 'domain', 'recordHash': 'e84b457db45ddd854e108fae8727c878b63e4740f889c18aebb
bf3d1e6469c41', 'lastSeen': '2017-12-20 03:46:27', 'firstSeen': '2016-03-22 10:07:55', 'resolve': 'mfilter-105-1-3.mx.srv.dfn.de', 'recordType': 'MX', 'source': ['riskiq'], 'collected': '2019-03-08 21:58:50', 'value': 'th-brandenburg.de'}], 'queryType': 'domain', 'totalRecords': 17}
```

Figure 17. *Output of the API client*


Terminal - root@hlkali: /home/hacker/PassiveTotal
File Edit View Terminal Tabs Help

```
root@hlkali:/home/hacker# git clone https://github.com/nored/PassiveTotal.git
Cloning into 'PassiveTotal'...
remote: Enumerating objects: 19, done.
remote: Counting objects: 100% (19/19), done.
remote: Compressing objects: 100% (18/18), done.
remote: Total 19 (delta 8), reused 7 (delta 0), pack-reused 0
Unpacking objects: 100% (19/19), done.
root@hlkali:/home/hacker# cd PassiveTotal/
root@hlkali:/home/hacker/PassiveTotal# ./minimal-client.py -a pdns -q th-branden
burg.de
Please do: gedit /home/hacker/PassiveTotal/config
and setup the configuration first!
You can "Copy&Paste" this command!!!
root@hlkali:/home/hacker/PassiveTotal# 
```

Figure 18. PassiveTotal *– Client installation*


Terminal - root@hlkali: /home/hacker/PassiveTotal
File Edit View Terminal Tabs Help
Open
config
/home/hacker/PassiveTotal

```
root@hlkali:/home/hacker# git clone https://github.com/nored/PassiveTotal.git
Cloning into 'PassiveTotal'...
remote: Enumerating objects: 19, done.
remote: Counting objects: 100% (19/19), done.
remote: Compressing objects: 100% (18/18), done.
remote: Total 19 (delta 8), reused 7 (delta 0), pack-reused 0
Unpacking objects: 100% (19/19), done.
root@hlkali:/home/hack
root@hlkali:/home/hack
burg.de
Please do: gedit /home
and setup the configur
You can "Copy&Paste" t
root@hlkali:/home/hack
```

```
passiv_total_config:
  api_key: value
  api_username: e_mail
  base_url: https://api.passivetotal.org
  comp: /v2/host-attributes/components
  malware: /v2/enrichment/malware
  pdns: /v2/dns/passive
  ssl: /v2/ssl-certificate/history
  subd: /v2/enrichment/subdomains
  tracker: /v2/host-attributes/trackers
  whois: /v2/whois
```

Figure 19. PassiveTotal *– API key configuration*

Summary

PassiveTotal provides access to Passive DNS resolution data, WHOIS registrant and registrar details (current and historical), SSL certificate information, web tracker information found on pages, Google Analytics, Clicky, New Relic, and more. Data such as web component information, details about software and frameworks running on web servers, host pairs, connections between a web page, and subsequent requests from that page is also provided by the tool. RiskIQ PassiveTotal aggregates data from across the Internet, absorbs intelligence to identify threats around attackers' infrastructure, and uses machine learning to scale threat detection and response. PassiveTotal provides context about who the attacker is, their tools and systems, and indicators of compromise outside the firewall - enterprise and third party.

In today's dynamic IT environment, many organizations struggle to find every system and application at risk before the attackers do [9]. Censys empowers defenders with the automated visibility they need to truly understand and to get ahead of these risks, enabling even small security teams to have an outsized impact. For this reason, it is important to have trained operators who have the necessary expertise and can use this tool effectively and profitably.

The course created in this work gives participants a comprehensive overview of the topic of Open Source Intelligence. It allows them to work independently with the newly taught tools, collect data from freely available sources, and aggregate it into investigation results. For this purpose, the tasks were designed for several laboratory exercises.

References

[1] Mercado, Stephen C. "Sailing the Sea of OSINT in the Information Age." Secret intelligence: A reader 78 (2009).

[2] Best Jr, Richard A., and Alfred Cumming. "Open source intelligence (OSINT): issues for congress." December 5 (2007): 28.

[3] Glassman, Michael, and Min Ju Kang. "Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT)." Computers in Human Behavior 28.2 (2012): 673-682.

[4] Quick, Darren, and Kim-Kwang Raymond Choo. "Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT+ OSINT): A timely and cohesive mix." Future Generation Computer Systems 78 (2018): 558-567.

[5] Williams, Heather J., and Ilana Blum. "Defining second generation open source intelligence (OSINT) for the defense enterprise." RAND Corporation Santa Monica United States, 2018.

[6] Benes, Libor. "OSINT, new technologies, education: Expanding opportunities and threats. A new paradigm." Journal of Strategic Security 6.3 (2013): 22-37.

[7] Schaurer, Florian, and Jan Störger. "The evolution of open source intelligence (OSINT)." Journal of US Intelligence Studies 19.3 (2013): 53-56.

[8] Pringle, Robert W. "The limits of OSINT: Diagnosing the Soviet media, 1985-1989." International Journal of Intelligence and CounterIntelligence 16.2 (2003): 280-289.

[9] Gibson, Helen. "Acquisition and preparation of data for OSINT investigations." Open Source Intelligence Investigation. Springer, Cham, 2016. 69-93.

[10] Carroll, Jami M. "OSINT Analysis using Adaptive Resonance Theory for Conterterrorism Warnings." Artificial Intelligence and Applications. 2005.

[11] Best, Clive. "OSINT, the Internet and Privacy." EISIC. 2012.

[12] Casanovas, Pompeu. "Cyber warfare and organised crime. A regulatory model and meta-model for open source intelligence (OSINT)." Ethics and Policies for Cyber Opera-

tions. Springer, Cham, 2017. 139-167.

[13] Layton, Robert, and Paul A. Watters. "Automating Open Source Intelligence: Algorithms for OSINT." Syngress, 2015.

[14] Steele, Robert David. "Open Source Intelligence (OSINT)."

[15] Berghel, Hal. "Robert David Steele on OSINT." Computer 47.7 (2014): 76-81.

[16] Weaver, Greg S. "Open Source Intelligence (OSINT)." The Police and the Military: Future Challenges and Opportunities in Public Safety 4.

[17] Revell, Quentin, Tom Smith, and Robert Stacey. "Tools for OSINT-Based Investigations." Open Source Intelligence Investigation. Springer, Cham, 2016. 153-165.

[18] Kalpakis, George, et al. "OSINT and the Dark Web." Open Source Intelligence Investigation. Springer, Cham, 2016. 111-132.

[19] Tabatabaei, Fahimeh, and Douglas Wells. "OSINT in the Context of Cyber-Security." Open Source Intelligence Investigation. Springer, Cham, 2016. 213-231.

[20] Danda, Matthew. "Open Source Intelligence and Cybersecurity." (2019).

[21] Steele, Robert D. "1997 OSINT What Is It – Why Is It Important to the Military (White Paper)." Academia.edu **www.academia.edu/9817888/1997_OSINT_What_Is_It_Why_Is_It_Important_to_the_Military_White_Paper_**.

[22] "Social Media Prisma 2017/2018, Ethority, **ethority.de/social-media-prisma/**.

[23] Mohsin, Maryam, et al. "10 Social Media Statistics You Need to Know in 2020 [Infographic]." Oberlo, Oberlo, 15 Jan. 2020, **www.oberlo.com/blog/social-media-marketing-statistics**.

[24] Tenzer: "Daten - Volumen Der Weltweit Generierten Daten 2025." Statista, Statista, 13 Feb. 2020, **de.statista.com/statistik/daten/studie/267974/umfrage/prognose-zum-weltweit-generierten-datenvolumen/**.

[25] Schwarz, Klaus; Franziska Schwarz, Reiner Creutzburg: "Conception and implementation of professional laboratory exercises in the field of open source intelligence (OSINT)". Proceed. Electronic Imaging Symposium 2020 (San Francisco, USA), Mobile Devices and Multimedia: Technologies, Algorithms & Applications Conference (MOBMU) 2020, **https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-278**

[26] Schwarz, Klaus; Reiner Creutzburg: "Design of Professional Laboratory Exercises for Effective State-of-the-Art OSINT Investigation Tools - Part 1: RiskIQ PassiveTotal". Proceed. Electronic Imaging Symposium 2021 (San Francisco, USA), Mobile Devices and Multimedia: Technologies, Algorithms & Applications Conference (MOBMU) 2021 (in print)

[27] Schwarz, Klaus; Reiner Creutzburg: "Design of Professional Laboratory Exercises for Effective State-of-the-Art OSINT Investigation Tools - Part 2: Censys". Proceed. Electronic Imaging Symposium 2021 (San Francisco, USA), Mobile Devices and Multimedia: Technologies, Algorithms & Applications Conference (MOBMU) 2021 (in print)

[28] Schwarz, Klaus; Reiner Creutzburg: "Design of Professional Laboratory Exercises for Effective State-of-the-Art OSINT Investigation Tools - Part 3: Maltego". Proceed. Electronic Imaging Symposium 2021 (San Francisco, USA), Mobile Devices and Multimedia: Technologies, Algorithms & Applications Conference (MOBMU) 2021 (in print)

[29] Schwarz, Klaus; Reiner Creutzburg: "Design of Professional Laboratory Exercises for Effective State-of-the-Art OSINT Investigation Tools - Part 3: Maltego". Proceed. Electronic Imaging Symposium 2021 (San Francisco, USA), Mobile Devices and Multimedia: Technologies, Algorithms & Applications Conference (MOBMU) 2021 (in print)

[30] Schwarz, Klaus: "Conception and Implementation of Professional Laboratory Exercises in the Field of Open Source Intelligence (OSINT) for use in English and German Training Market for Security Authorities". Master Thesis, Technische Hochschule Brandenburg, Department of Computing and Media, April 2020

[31] Kant, Daniel; Reiner Creutzburg: 'Investigation of risks for Critical Infrastructures due to the exposure of SCADA systems and industrial controls on the Internet based on the search engine Shodan". Proceed. Electronic Imaging Symposium 2020 (San Francisco, USA), Mobile Devices and Multimedia: Technologies, Algorithms & Applications Conference (MOBMU) 2020 **https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-253**

[32] Pilgermann, Michael; Thomas Bocklisch; Reiner Creutzburg: "Conception and implementation of a course for professional training and education in the field of IoT and smart home security". Proceed. Electronic Imaging Symposium 2020 (San Francisco, USA), Mobile Devices and Multimedia: Technologies, Algorithms & Applications Conference (MOBMU) 2020 **https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-277**

Author Biography

Klaus Schwarz received his B. Sc. and M.Sc. in Computer Science from Technische Hochschule Brandenburg (Germany) in 2017 and 2020, respectively. His research interests include IoT and Smart Home Security, OSINT, Mechatronics, Sensorics, Embedded Systems, Artificial Intelligence, and Cloud Security. As a faculty member, he is developing a graduate program in Applied Mechatronic Systems focusing on Artificial Intelligence at SRH Berlin University of Applied Sciences.

Reiner Creutzburg is a Retired Professor for Applied Computer Science at the Technische Hochschule Brandenburg in Brandenburg, Germany. Since 2019 he is a Professor of IT Security at the SRH Berlin University of Applied Sciences, Berlin School of Technology. He is a member of the IEEE and SPIE and chairman of the Multimedia on Mobile Devices (MOBMU) Conference at the Electronic Imaging conferences since 2005. In 2019, he was elected a member of the Leibniz Society of Sciences to Berlin e.V. His research interest is focused on Cybersecurity, Digital Forensics, Open Source Intelligence (OSINT), Multimedia Signal Processing, eLearning, Parallel Memory Architectures, and Modern Digital Media and Imaging Applications.

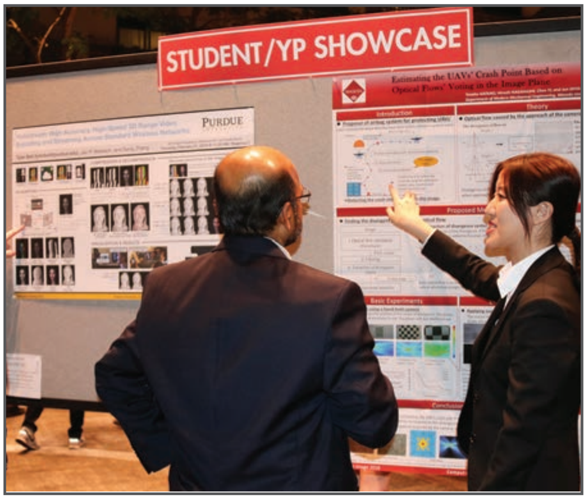
JOIN US AT THE NEXT EI!

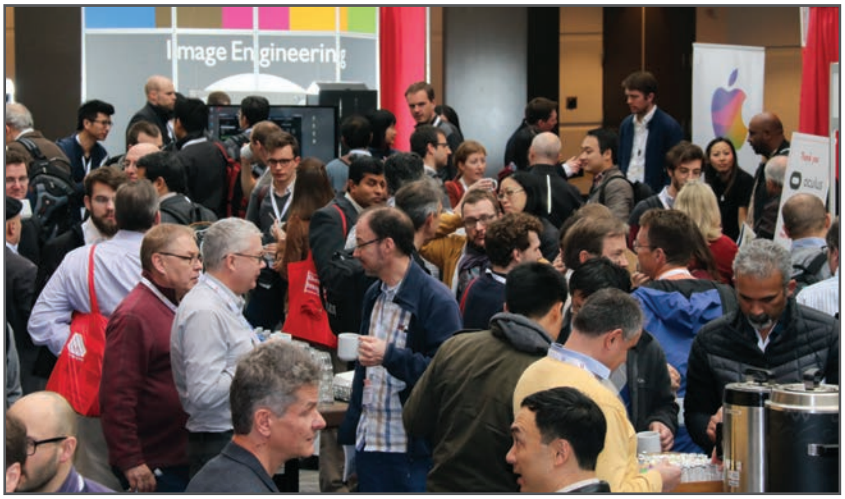
IS&T International Symposium on

Electronic Imaging

SCIENCE AND TECHNOLOGY

Imaging across applications . . . Where industry and academia meet!





- AR is a fundamental and transformative interface and platform.
- 20+ years from my initial working demo to today's AR displays
- Optimistic that it won't take another 20 to reach ubiquitous consumer AR!

• SHORT COURSES • EXHIBITS • DEMONSTRATION SESSION • PLENARY TALKS •
• INTERACTIVE PAPER SESSION • SPECIAL EVENTS • TECHNICAL SESSIONS •

www.electronicimaging.org

IS&T
imaging.org