Available online at https://ejournal.almaata.ac.id/index.php/IJUBI
Indonesian Journal of Business Intelligence
Volume 2 | Issue 1 | June (2019)
IJUBI
Indonesian Journal
---- of ----
Business Intelligence

# MEMBANGUN TELEGRAMBOT UNTUK CRAWLING MALWARE OSINT MENGGUNAKAN RASPBERRY PI

Dedy Hariyadi[1], Fazulrahman[2]
[1]Teknologi Informasi, Fakultas Teknik dan Teknologi Informasi, Universitas Jenderal Achmad Yani Yogyakarta
[2]Komunitas NgeSec Yogyakarta
[1]milisdad@gmail.com, [2]fazlurbima@gmail.com
[1]Jl. Ringroad Barat, Gamping Kidul, Ambarketawang, Gamping, Sleman, DI Yogyakarta
[2]JL. Brigjend Katamso, Prawirodirjan GM II/1226, Gondomanan, Yogyakarta

***Keywords:***

*Cyber Attack, Malware, OSINT, Single Board Computer, TelegramBot*

**Abstract**

Data on cyber attacks released by Badan Siber dan Sandi Negara (BSSN) with the Indonesia Honeynet Project (IHP) indicate that there are cyber attacks originating from Indonesia or domestically. The source of cyber attack information that is categorized as Open Source Intelligent (OSINT) is available on the Internet in various formats. Even the information is spread depending on the provider. In this study it was proposed to collect various OSINT-based cyber attacks using the crawling method that is accessed via Instant Messenger. Telegram is an Instant Messenger that has provided automation features using Robots. This Robot application does not require many lines of code so that it is easily installed on Single Board Computer (SBC). With the form of a small Single Board Computer makes it easy to install anywhere as long as it has internet access to process information. Through Instant Messenger Telegram makes it easy to access OSINT-based cyber attacks by combining crawling and TelegramBot methods.

***Kata Kunci***

*Malware, OSINT, Serangan Siber, Single Board Computer, TelegramBot*

**Abstrak**

Data serangan siber yang dirilis oleh Badan Siber dan Sandi Negara (BSSN) bersama *Indonesia Honeynet Project* (IHP) menunjukan bahwa terdapat serangan siber yang berasal dari Indonesia atau dalam negeri. Sumber informasi serangan siber yang dikategorikan sebagai *Open Source Intelligent* (OSINT) tersedia di Internet dengan berbagai *format*. Bahkan informasinya tersebar tergantung dari pihak penyedia. Pada penelitian ini diusulkan mengumpulkan berbagai serangan siber berbasis OSINT dengan metode *crawling* yang diakses melalui *Instant Messenger*. Telegram merupakan *Instant Messenger* yang telah menyediakan fitur otomatisasi menggunakan *Robot*. Aplikasi *Robot* ini tidak memerlukan baris kode yang banyak sehingga mudah dipasang pada *Single Board Computer* (SBC). Dengan bentuk *Single Board Computer* yang kecil memudahkan pemasangan dimana saja asalkan memiliki akses internet untuk memproses informasi. Melalui *Instant Messenger* Telegram mempermudah mengakses serangan siber berbasis OSINT tersebut dengan menggabungkan metode *crawling* dan *TelegramBot*.

## Pendahuluan

Badan Siber dan Sandi Negara (BSSN) bersama *Indonesia Honeynet Project (IHP)* pada awal tahun 2019 merilis peta serangan siber di Indonesia yang dapat diakses pada halaman https://honeynet.bssn.go.id/. Berdasarkan sensor *Honeynet* yang aktif bahwa serangan siber pada rentang waktu Januari sampai dengan Desember 2018 sejumlah 12.895.554 serangan. Sedangkan jumlah serangan *malware* sejumlah 512.863 serangan. Tabel 1

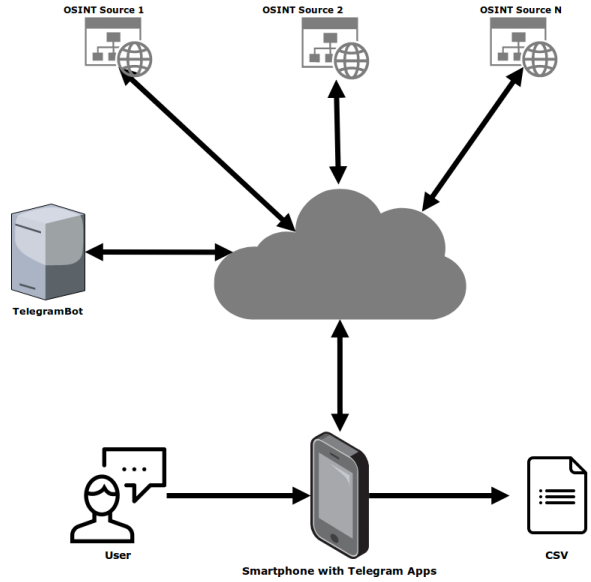
menunjukan sumber serangan berdasarkan negara dan jumlah serangannya [1].

Tabel 1. Sumber Serangan Tahun 2018

| No | Sumber Serangan (Negara) | Jumlah |
|---|---|---|
| 1 | Rusia | 2.597.256 |
| 2 | Tiongkok | 1.871.363 |
| 3 | Amerika Serikat | 1.428.440 |
| 4 | Singapura | 1.030.769 |
| 5 | Belanda | 964.482 |
| 6 | Perancis | 775.257 |
| 7 | Indonesia | 713.878 |
| 8 | India | 674.689 |
| 9 | Canada | 493.897 |
| 10 | Jerman | 211.310 |

Peta yang disajikan pada halaman https://honeynet.bssn.go.id/ dalam bentuk visualisasi serangan siber baik dari negara lain ke Indonesia atau sebaliknya. Adapun dalam visualisasi tersebut diantaranya: menampilkan tren malware (jenis *malware* yang paling banyak menyerang Indonesia), *live feed* (informasi serangan siber yang terjadi secara real time), peringkat serangan (negara yang paling banyak melakukan serangan siber ke Indonesia), dan rentang waktu (grafik intensitas jumlah serangan yang terjadi per satuan waktu). Kedepannya, *Indonesia Honeynet Project* akan melakukan penelitian untuk membangun *Malicious Domain List* khusus domain nasional [2]. Hal ini akan memperkaya informasi terkait serangan siber yang dapat dikaji dan diteliti oleh peneliti keamanan informasi di Indonesia. Saat ini daftar serangan siber berupa *malware* yang mudah didapatkan adalah Malc0de dan MalShare. Sumber serangan siber ini dapat disebut sebagai *Malware OSINT Source* [3].

Oleh sebab itu penulis melakukan sebuah penelitian kecil dengan membangun *crawler* informasi serangan siber dari *OSINT Source*. Mesin *crawler* ini diintegrasikan dengan *TelegramBot* untuk mempermudah mendapatkan informasi serangan dalam bentuk tabel melalui ponsel cerdas melalui *instant messenger* Telegram. Gambar 1 menunjukan arsitektur dari pengembangan *TelegramBot* untuk meng-*crawling* serangan siber berupa *malware* dari *OSINT Source*.




Gambar 1. Arsitektur Proses Malware Crawler

## Perancangan TelegramBot

### *Raspberry Pi*

*Single board Computer (SBC)* dapat diartikan sebagai komputer yang dibangun dalam satu kesatuan pada sebuah papan elektronik yang terdiri dari *CPU*, memori, *port I/O*, dan fitur lain-lain yang mendukung fungsional sebuah komputer [4]. *Raspberry Pi Foundation* secara resmi pada tahun 2012 mengeluarkan *SBC* yang dikenal dengan Raspberry Pi [5]. Saat ini *Raspberry Pi Foundation* telah mengeluarkan *SBC* Raspberry Pi sebanyak tujuh varian. Tabel 2 menunjukan komparasi dasar tujuh varian Raspberry Pi. Masing-masing varian *SBC* Raspberry Pi memiliki konektivitas yang berbeda-beda seperti ditunjukan pada Tabel 3 [6]. Pada penelitian ini menggunakan Raspberry Pi 3 Model B.

Tabel 2. Komparasi Varian Raspberry Pi

| | Raspberry Pi 1 Model A | Raspberry Pi 1 Model A+ | Raspberry Pi 1 Model B | Raspberry Pi 1 Model B+ | Raspberry Pi 2 Model B | Raspberry Pi 3 Model B | Raspberry Pi Zero |
|---|---|---|---|---|---|---|---|
| Release Date | 2013 | 2014 | 2012 | 2014 | 2015 | 2016 | 2015 |
| SoC | Broadcom BCM2835 | Broadcom BCM2835 | Broadcom BCM2835 | Broadcom BCM2835 | Broadcom BCM2836 | Broadcom BCM2837 | Broadcom BCM2835 |
| CPU Speed | 700 Mhz ARM-1176JZF-S | 700 Mhz ARM-1176JZF-S | 700 MHz ARM-1176JZF-S | 700 Mhz ARM-1176JZF-S | 900 Mhz ARM-Cortex-A7 | 1.2 Ghz ARM-Cortex-A53 | 1 Ghz ARM1176JZF-S |
| Cores | 1 | 1 | 1 | 1 | 4 | 4 | 1 |
| SDRAM | 256 MB | 256 MB | 512 MB | 512 MB | 1 GB | 1 Gb | 512 MB |

Tabel 3. Komparasi Konektivitas Varian Raspberry Pi

| | Raspberry Pi 1 Model A | Raspberry Pi 1 Model A+ | Raspberry Pi 1 Model B | Raspberry Pi 1 Model B+ | Raspberry Pi 2 Model B | Raspberry Pi 3 Model B | Raspbe Pi Zero |
|---|---|---|---|---|---|---|---|
| USB 2.0 Ports | 1 | 1 | 2 | 4 | 4 | 4 | 1 (Micr USB) |
| Ethernet | None | None | 10/100 Mbit/s | 10/100 Mbit/s | 10/100 Mbit/s | 10/100 Mbit/s | None |
| Bluetooth | None | None | None | None | None | 4.1 | None |
| WiFi | None | None | None | None | None | 802.11n | None |
| Audio In | I²S | I²S | I²S | I²S | I²S | I²S | I²S |
| Audio Out | I²S, analog (3.5mm jack), digital (HDMI) | I²S, analog (3.5mm jack), digital (HDMI) | I²S, analog (3.5mm jack), digital (HDMI) | I²S, analog (3.5mm jack), digital (HDMI) | I²S, analog (3.5mm jack), digital (HDMI) | I²S, analog (3.5mm jack), digital (HDMI) | Digital (mini-HDMI), analog GPIO PWM |
| Video In | CSI Camera Connector | CSI Camera Connector | CSI Camera Connector | CSI Camera Connector | CSI Camera Connector | CSI Camera Connector | None |
| Video Out | HDMI, Composite (RCA) | HDMI, Composite (TRRS) | HDMI, Composite (RCA) | HDMI, Composite (TRRS) | HDMI, Composite (TRRS) | HDMI, Composite (TRRS) | Mini-HDMI, GPIO Compo |
| External Storage | SD | MicroSD | SD | MicroSD | MicroSD | MicroSD | MicroS |

### *Raspbian*

Sistem operasi yang mudah digunakan pada *SBC* Raspberry Pi salah satunya adalah Rasbian. Sistem operasi Rasbian merupakan turunan Debian GNU/Linux yang telah dirancang sedemikian rupa untuk mempermudah bagi pengguna MS Windows ataupun Mac OS. Kebutuhan dasar penggunaan komputer telah disediakan oleh sistem operasi Raspbian [7]. Untuk mempermudah pengembangan pada penelitian ini, digunakan Raspbian sebagai sistem operasi yang dipasang pada *SBC* Raspberry Pi.

### *Python*

Sebuah perusahaan yang fokus melakukan pengukuran dan penilaian kualitas dari perangkat lunak, TIOBE melakukan survey popularitas bahasa pemrograman. Menurut TIOBE bahwa bahasa pemrograman Python termasuk 20 bahasa pemrograman terpopuler di dunia [8]. Python juga dapat dijalankan di berbagai sistem operasi seperti MS Windows, Mac OS dan Linux. Berhubung penelitian ini menggunakan sistem operasi Raspbian yang merupakan turunan Debian GNU/Linux maka implementasi bahasa pemrograman Python dapat berfungsi dengan baik. Fitur-fitur yang digunakan dalam bahasa pemrograman Python diantaranya dukungan *object-oriented programming* [9] dan *tuples* [10].

## Membangun *TelegramBot*

Telegram telah menyediakan ekosistem pengembangan *TelegramBot* yang mempermudah pengembang perangkat lunak. *TelegramBot* yang digunakan dalam penelitian ini adalah *BotFather* sesuai rekomendasi dari pihak Telegram [11]. *BotFather* mempermudah proses pembuatan *TelegramBot* dengan menyediakan API dengan kode token yang telah disesuaikan saat pembuatan akun *TelegramBot* [12]. *TelegramBot* yang dirancang dapat digunakan secara bersamaan (*multiuser*) dalam suatu *group chat*.

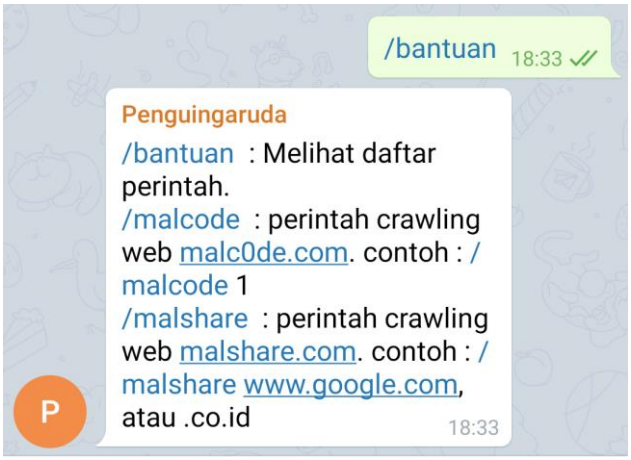
*TelegramBot* dibangun menggunakan bahasa pemrograman Python yang berjalan pada sistem operasi Raspbian untuk melakukan *crawling OSINT Source*. Pada pengembangan awal ini *OSINT Source* yang digunakan adalah situs web basis data *malware*, seperti Malc0de dan MalShare. Kode Python yang digunakan untuk meng-crawling *OSINT Source* tersebut mengambil dari kode repositori Github (malc0de dan malshare). Beberapa kebutuhan dasar kode ini diantaranya pustaka *urllib3, requests, argparse* dan *telepot*.

Mesin *crawler* berupa *SBC* Raspberry Pi yang telah terinstall Raspbian sebagai sistem operasi dan kode crawler Malc0de dan MalShare hanya membutuhkan koneksi internet baik melalui jaringan kabel atau nirkabel. Konfigurasi jaringan mengikuti kaidah yang berlaku pada lokasi penyedia jaringan internet, seperti tampak pada Gambar 1.

## Hasil dan Pembahasan

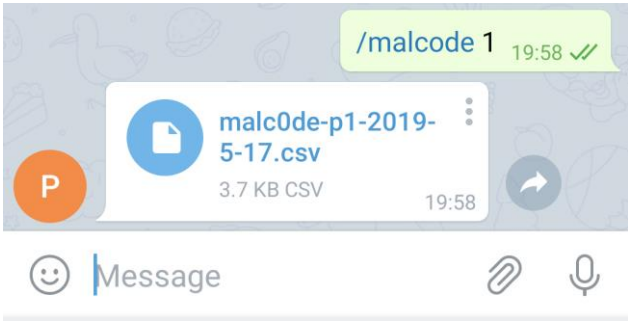
*TelegramBot* yang dirancang dengan tipe *multiuser* jadi harus dimasukan ke dalam sebuah *group chat*. Tujuannya dimasukan dalam *group chat* supaya antar pengguna dapat melakukan pemantauan halaman *OSINT Source*

yang di-*crawling secara* bersama-sama. Setelah *TelegramBot* dimasukan dalam sebuah *group chat* dapat memulai dengan memanggil perintah */bantuan* untuk mendapat informasi daftar perintah seperti pada Gambar 2.




Gambar 2. Panduan Penggunaan TelegramBot

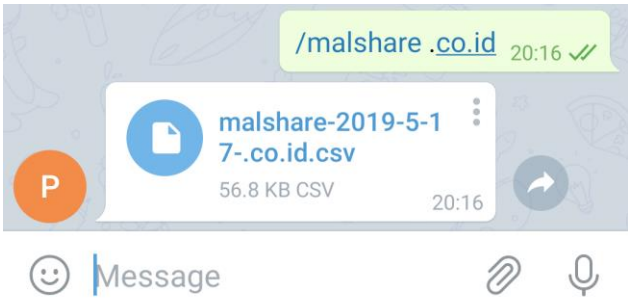
Malc0de dengan pola perintah */malcode* x. X merupakan halaman situs web dari Malc0de. Sebagai contoh akan melakukan *crawling* halaman ke-1 dari situs web Malc0de maka perintah yang dipanggil adalah */malcode 1*, seperti tampak pada Gambar 3.




Gambar 3. Crawling Malc0de

MalShare dengan pola perintah */malshare y*. Y merupakan *domain* atau *second level domain* yang terserang *malware*. Sebagai contoh akan melakukan *crawling* dari sebuah *second level domain .co.id* maka perintah yang dipanggil adalah */malshare .co.id*, seperti tampak pada Gambar 4.

Hasil crawling dari TelegramBot ini dalam bentuk berkas berformat CSV [13]. Halaman situs web Malc0de menampilkan informasi serangan malware di Indonesia dengan format *header* tabel diantaranya: *Date, Domain, IP Address,* dan *ASN Number*, seperti tampak pada Tabel 4. Halaman situs web MalShare menampilkan informasi dengan format *header* tabel diantaranya: *Date, Domain, File Type* dari Terinfeksi, dan Detil informasi dari sumber serangan, seperti tampak pada




Gambar 4. Crawling MalShare

Tabel 5.

Tabel 4. Contoh Hasil Crawling Malc0de

| Date | Domain | IP | ASN Number |
|---|---|---|---|
| 2019-05-02 | pepperbagz.com/wp-content/themes/basel/fonts/1c.jpg | 202.179.136.69 | 136170 |
| 2019-04-30 | pepperbagz.com/wp-content/themes/basel/fonts/1c.jpg | 202.179.136.69 | 136170 |
| 2019-04-29 | pepperbagz.com/wp-content/themes/basel/fonts/1c.jpg | 202.179.136.69 | 136170 |
| 2019-04-28 | pepperbagz.com/wp-content/themes/basel/fonts/1c.jpg | 202.179.136.69 | 136170 |
| 2019-04-27 | pepperbagz.com/wp-content/themes/basel/fonts/1c.jpg | 202.179.136.69 | 136170 |
| 2019-04-26 | pepperbagz.com/wp-content/them | 202.179.136.69 | 136170 |

| Date | Domain | IP | ASN Number |
|---|---|---|---|
| | es/basel/fonts/1c.jpg | | |
| 2019-01-24 | reogtiket.com/templates/beez_20/css/ssj.jpg | 116.90.165.210 | 18059 |
| 2019-01-23 | defidaitari.web.id/wp-content/themes/masterblog/css/ssj.jpg | 103.28.149.106 | 58477 |
| 2019-01-23 | reogtiket.com/templates/beez_20/css/ssj.jpg | 116.90.165.210 | 18059 |

Tabel 5. Contoh Hasil Crawling MalShare

| Date | Domain | File Type | Detail |
|---|---|---|---|
| 2018-06-06 00:50:17 | http://indostraits.co.id/soppp.exe | PE32 | https://malshare.com/sample.php?action=detail&hash=4db20b8091333255ff2785928d4551e7 |
| 2018-06-06 00:45:07 | http://sandboxgallery.com/Past-Due-Invoices/ | Composite | https://malshare.com/sample.php?action=detail&hash=18d913117bd76794a1b68d9473a2fc1d |
| 2018-06-05 01:00:52 | http://indostraits.co.id/PO-04062018.exe | PE32 | https://malshare.com/sample.php?action=detail&hash=e5be80183a03600941750e05467c07f3 |
| 2018-06-05 01:00:46 | http://indostraits.co.id/palll.exe | PE32 | https://malshare.com/sample.php?action=detail&hash=198a7bf497c06263feb3519b1dcf445c |
| 2018-06-01 12:57:06 | http://poshsmetal.com/Notification-de-facture... | Composite | https://malshare.com/sample.php?action=detail&hash=bc66adc709fec188bb140ef6b9fd1430 |
| 2018-06-01 12:50:10 | http://indostraits.co.id/good.exe | PE32 | https://malshare.com/sample.php?action=detail&hash=61aed8f813031c69602251c695cdf09f |
| 2018-06-01 00:45:06 | http://rebovo.de/Facture-impayee-31-mai/ | Composite | https://malshare.com/sample.php?action=detail&hash=f8180accb6f8ef7e2dbb7b869e3a672e |
| 2018-05-31 13:17:07 | http://indostraits.co.id/man.exe | PE32 | https://malshare.com/sample.php?action=detail&hash=a47e3065d00ed5de55fe35a6cdee1bfa |
| 2018-05-31 12:47:31 | http://indostraits.co.id/noblll.exe | PE32 | https://malshare.com/sample.php?action=detail&hash=8eb8cda92a96397e1a7ac364dd71bcd0 |
| 2018-05-30 12:55:52 | http://ptgut.co.id/Facturation/ | Composite | https://malshare.com/sample.php?action=d |

| Date | Domain | File Type | Detail |
|---|---|---|---|
| | | | etail&hash=e3930b5c8f88f81ce0474e3217b601bb |

*Dari sisi server* TelegramBot mencatat aktivitas pemanfaatan *robot* berupa *log*. Adapun *format log*-nya adalah waktu pengakses, perintah yang digunakan dan pengguna, seperti tampak pada Gambar 5.

```
14-5-2019 19:44:45 Chat-id - 575519994 Text - /bantuan Sender - KomodoTest
14-5-2019 19:44:45 Chat-id - 575519994 Text - /start Sender - KomodoTest
14-5-2019 19:56:9 Chat-id - 575519994 Text - /start Sender - KomodoTest
14-5-2019 19:57:21 Chat-id - 575519994 Text - /bantuan Sender - KomodoTest
14-5-2019 19:57:21 Chat-id - 575519994 Text - /malshare .co.id Sender - KomodoTest
14-5-2019 19:57:21 Chat-id - -223857708 Text - /bantuan Sender - orangmiliter
14-5-2019 19:57:21 Chat-id - -223857708 Text - /malshare .go.id Sender - orangmiliter
14-5-2019 19:57:21 Chat-id - -223857708 Text - /malshare .co.id Sender - milisdad
14-5-2019 19:57:21 Chat-id - -223857708 Text - /bantuan Sender - UnjaniYK
14-5-2019 19:57:21 Chat-id - -223857708 Text - /malcode 4 Sender - UnjaniYK
14-5-2019 19:57:21 Chat-id - -223857708 Text - /malcode 1 Sender - UnjaniYK
14-5-2019 19:57:21 Chat-id - -223857708 Text - /malshare .co.id Sender - UnjaniYK
```

Gambar 5. Log pada Mesin Server TelegramBot

## Kesimpulan dan Saran

TelegramBot yang dibangun ini masih memiliki banyak keterbatasan seperti, saat ini masih tersedia dua *OSINT Source* yang digunakan, belum menampilkan data dalam bentuk grafik atau peta serangan siber, proses *crawling* masih berdasarkan dari halaman web Malc0de dan MalShare dan belum menerapkan manajemen pengelolaan berkas hasil *crawling* berserta *log* pada *server*. Walaupun masih terdapat banyak keterbatasan harapannya penelitian ini dapat mendukung pekerjaan terkait dengan *cyber threat information sharing* sesuai standar dari *National Institute of Standard and Technology (NIST) - U.S. Department of Commerce* [14]:

1. Kesadaran bersama terkait situasi serangan siber.
2. Improvisasi keamanan informasi.
3. Pengetahuan yang dalam.
4. Peningkatan pertahanan siber.

## Referensi

[1] Badan Siber dan Sandi Negara and Indonesia Honeynet Project, "Laporan Tahunan Honeynet Project," Jakarta, 2018.

[2] Badan Siber dan Sandi Negara, "Mengenali Serangan Siber Global dan Nasional Melalui Laporan Tahunan Honeynet Project BSSN-IHP Tahun 2018 | bssn.go.id," 2019. [Online]. Available: https://bssn.go.id/mengenali-serangan-siber-global-dan-nasional-melalui-laporan-tahunan-honeynet-project-bssn-ihp-tahun-2018/. [Accessed: 08-Feb-2019].

[3] F. E. Nastiti, D. Hariyadi, and Fazlurrahman, "TelegramBot : Crawling Data Serangan Malware dengan Telegram," J. Comput. Eng. Syst. Sci., vol. 4, no. 1, 2019.

[4] P. Jovanović, M. Mileusnic, B. Pavić, and B. Mišković, "Applications of the Single Board Computers in the Software Defined Radio Systems," no. June 2016, pp. 882–886, 2014.

[5] Raspberry Pi Foundation, "Raspberry Pi Foundation Annual Review 2017," 2017.

[6] Core Electronics, "Raspberry Pi Boards Compared - Tutorial Australia." [Online]. Available: https://core-electronics.com.au/tutorials/compare-raspberry-pi-boards.html. [Accessed: 01-Feb-2019].

[7] G. Halfacree, "The Official Raspberry Pi Beginner 's Guide," Raspberry Pi PRESS, 2018.

[8] TIOBE, "February Headline: Groovy re-enters the TIOBE index top 20." [Online]. Available: https://www.tiobe.com/tiobe-index/. [Accessed: 15-Feb-2019].

[9] Python, "Beginners Guide." [Online]. Available: https://wiki.python.org/moin/BeginnersGuide/Overview. [Accessed: 21-Sep-2018].

[10] W3Schools, "Python Tuples." [Online]. Available: https://www.w3schools.com/python/python_tuples.asp. [Accessed: 21-Sep-2018].

[11] Telegram, "Bots: An introduction for developers." [Online]. Available: https://core.telegram.org/bots. [Accessed: 30-Oct-2018].

[12] Bots for Telegram, "The Bot Father." [Online]. Available: https://botsfortelegram.com/project/the-bot-father/. [Accessed: 15-Oct-2018].

[13] Y. Shafranovich, "Common Format and MIME Type for Comma-Separated Values (CSV) Files," Oct. 2005.

[14] C. S. Johnson, M. L. Badger, D. A. Waltermire, J. Snyder, and C. Skorupka, "Guide to Cyber Threat Information Sharing," 2016.