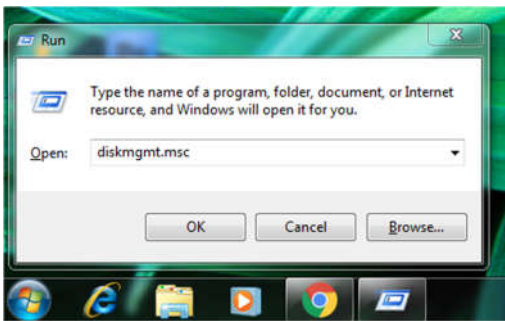
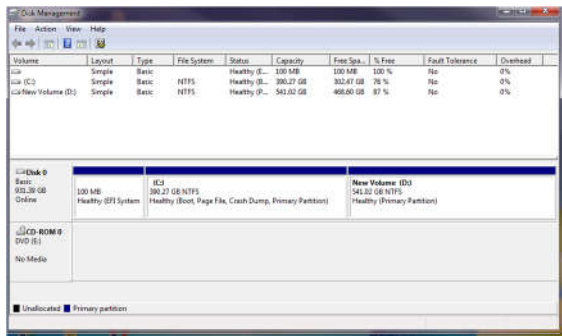
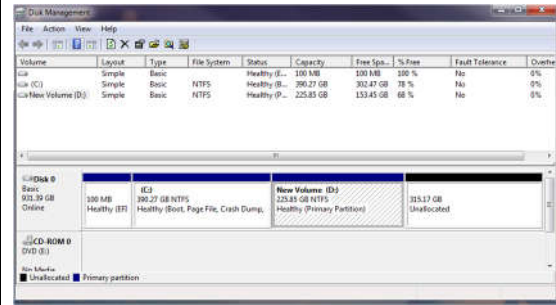


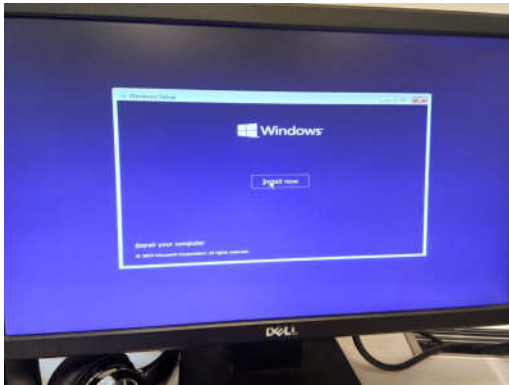
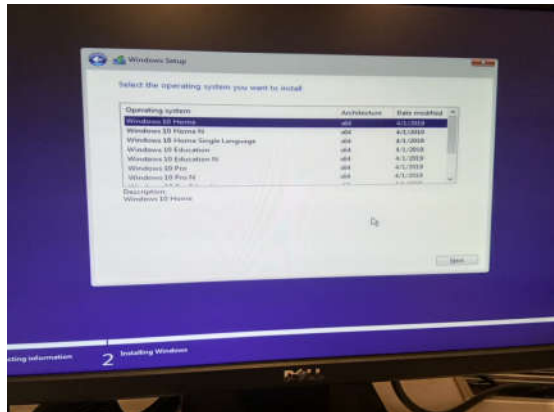
BUKTI FISIK KEGIATAN PRANATA KOMPUTER AHLI			Halaman 1 dari 2
Nama	Taufiqurrahman, S.Si.	Tanggal dibuat	Satu Kali AK = 0,435
NIP	198904272018021001	12 Maret 2020	
Pangkat/Golongan	Penata Muda / III/a		
Jabatan Fungsional	Pranata Komputer Ahli Pertama		
Lokasi Pengerjaan	Gd. Sutan Sjahrir Pushansiber Bainstrahan Kemhan RI		
Nama Kegiatan : MENGATUR ALOKASI DALAM MEDIA KOMPUTER			
SPESIFIKASI SISTEM KOMPUTER :			
Processor : Intel® Core™ i5-6500 CPU @ 3.20 GHz ~ 3.19 GHz RAM : 4,00 GB (3,87 GB Usable) System Type : 64-bit OS, x64-based processor HDD : 1 TB (931,39 GB Usable)			
IDENTITAS AREA :			
<ul style="list-style-type: none"> Area penyimpanan ini digunakan untuk instalasi OS Windows 10 serta program paket <i>Xampp</i> (server lokal) yang digunakan untuk aplikasi Sistem Repositori <i>Signature</i> Ancaman Siber beserta <i>databasenya</i>. Kapasitas yang disediakan hanya dapat menampung data aplikasi selama 6 bulan. Untuk itu diperlukan <i>back-up</i> serta pengarsipan berkala untuk data-data yang lampau 			
BESARAN AREA :			
209.175.134.208 bytes (194 GB)			
LOKASI Pengerjaan :			
Lab Malware, Gd. Sutan Sjahrir Pushansiber Bainstrahan Kemhan			
DOKUMENTASI Pengerjaan :			
1. Menggunakan Disk Management untuk melakukan Partisi 		2. Menentukan area penyimpanan yang akan di <i>resize</i> dan dipartisi 	

4. Proses partisi berhasil dan selesai dilaksanakan

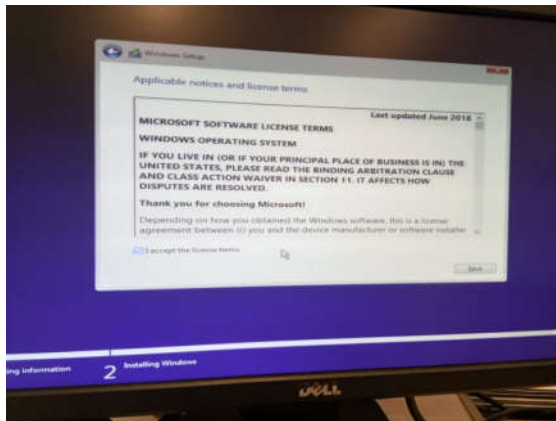


Jakarta, 16 Maret 2020
Pranata Komputer Ahli Pertama

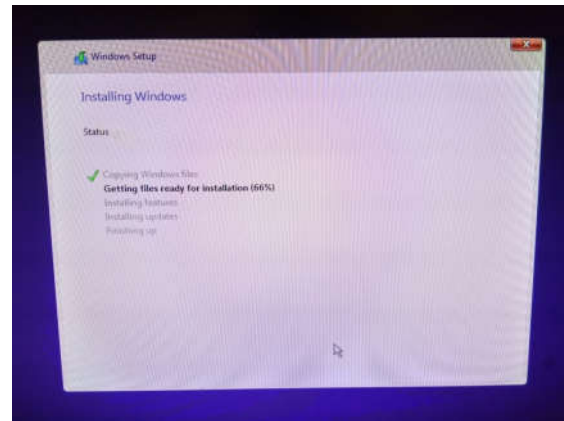
Taufiqurrahman, S.Si.
Penata Muda III/a NIP.198904272018021001

BUKTI FISIK KEGIATAN PRANATA KOMPUTER AHLI			Halaman 1 dari 2
Nama	Taufiqurrahman, S.Sl.	Tanggal dibuat	Satu Sistem AK = 0,371
NIP	198904272018021001	12 Maret 2020	
Pangkat/Golongan	Penata Muda / III/a		
Jabatan Fungsional	Pranata Komputer Ahli Pertama		
Lokasi Pengerjaan	Gd. Sutan Sjahrir Pushansiber Bainstrahan Kemhan RI		
Nama Kegiatan : MELAKUKAN INSTALASI DAN ATAU MENINGKATKAN (UPGRADE) SISTEM KOMPUTER			
SPESIFIKASI SISTEM KOMPUTER :			
Processor : Intel® Core™ i5-6500 CPU @ 3.20 GHz ~ 3.19 GHz RAM : 4,00 GB (3,87 GB Usable) System Type : 64-bit OS, x64-based processor HDD : 1 TB (931,39 GB Usable)			
SPESIFIKASI SISTEM OPERASI DAN WEB SERVER :			
Sistem Operasi : Window 10 Pro Web Server : Apache/2.4.41 (Win64) OpenSSL/1.1.1.c PHP/7.4.3 DBMS : MariaDB 10.4.11			
TANGGAL & LAMA Pengerjaan :			
12 Maret 2020 / 3 Jam Pengerjaan			
LOKASI Pengerjaan :			
Lab Malware, Gd. Sutan Sjahrir Pushansiber Bainstrahan Kemhan			
DOKUMENTASI Pengerjaan :			
1. Memulai pemasangan OS 		2. Memilih varian OS yang akan dipasang 	

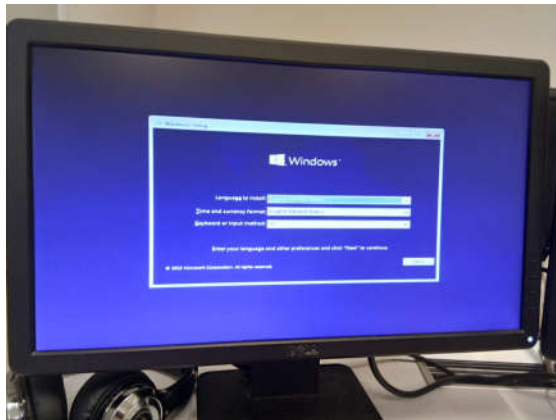
3. Persetujuan EULA instalasi OS



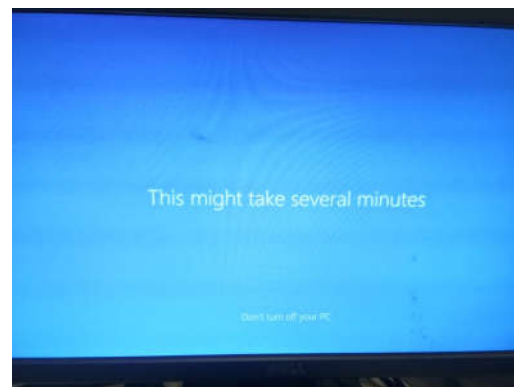
4. Proses instalasi berlangsung



5. Proses instalasi wilayah dan bahasa



6. proses instalasi berhasil dan selesai dilaksanakan



Mengetahui
Kasubbid Kam Aplikasi Bid Jamkam,

Eko Joko Murwanto, S.Kom., M.SI.
Pembina IV/a NIP. 197505252001121001

Jakarta, 16 Maret 2020
Pranata Komputer Ahli Pertama

Taufiqurrahman, S.SI.
Penata Muda III/a NIP.198904272018021001

BUKTI FISIK KEGIATAN PRANATA KOMPUTER AHLI			Halaman 1 dari 1
Nama	Taufiqurrahman, S.Sl.	Tanggal dibuat	Satu Kali AK = 0,239
NIP	198904272018021001	5 April 2020	
Pangkat/Golongan	Penata Muda / III/a		
Jabatan Fungsional	Pranata Komputer Ahli Pertama		
Lokasi Pengerjaan	Gd. Sutan Sjahrir Pushansiber Bainstrahan Kemhan RI		
Nama Kegiatan : <p style="text-align: center;">MELAKUKAN MONITORING AKSES</p>			
PERIODE PEMANTAUAN			
4 April 2020 – 5 April 2020			
DOKUMENTASI HASIL MONITORING AKSES :			
<ul style="list-style-type: none"> • Hasil monitoring akses perangkat dan jaringan terlampir • Hasil pemantauan website di lingkungan Kemhan RI terlampir 			
<p style="text-align: center;">Mengetahui Kasubbid Kam Aplikasi Bid Jamkam,</p> <p style="text-align: center;">Eko Joko Murwanto, S.Kom., M.Sl. Pembina IV/a NIP. 197505252001121001</p>		<p style="text-align: center;">Jakarta, 7 April 2020 Pranata Komputer Ahli Pertama</p> <p style="text-align: center;">Taufiqurrahman, S.Sl. Penata Muda III/a NIP.198904272018021001</p>	

BUKTI FISIK KEGIATAN PRANATA KOMPUTER AHLI			Halaman 1 dari 1
Nama	Taufiqurrahman, S.Sl.	Tanggal dibuat	Satu Kali AK = 0,239
NIP	198904272018021001	7 Mei 2020	
Pangkat/Golongan	Penata Muda / III/a		
Jabatan Fungsional	Pranata Komputer Ahli Pertama		
Lokasi Pengerjaan	Gd. Sutan Sjahrir Pushansiber Bainstrahan Kemhan RI		
Nama Kegiatan : MELAKUKAN MONITORING AKSES			
PERIODE PEMANTAUAN			
6 Mei 2020 – 7 Mei 2020			
DOKUMENTASI HASIL MONITORING AKSES :			
<ul style="list-style-type: none"> • Hasil monitoring akses perangkat dan jaringan terlampir • Hasil pemantauan website di lingkungan Kemhan RI terlampir 			
Mengetahui Kasubbid Kam Aplikasi Bid Jamkam, Eko Joko Murwanto, S.Kom., M.Sl. Pembina IV/a NIP. 197505252001121001		Jakarta, 11 Mei 2020 Pranata Komputer Ahli Pertama Taufiqurrahman, S.Sl. Penata Muda III/a NIP.198904272018021001	

BUKTI FISIK KEGIATAN PRANATA KOMPUTER AHLI			Halaman 1 dari 1
Nama	Taufiqurrahman, S.Sl.	Tanggal dibuat	Satu Kali AK = 0,239
NIP	198904272018021001	27 Mei 2020	
Pangkat/Golongan	Penata Muda / III/a		
Jabatan Fungsional	Pranata Komputer Ahli Pertama		
Lokasi Pengerjaan	Gd. Sutan Sjahrir Pushansiber Bainstrahan Kemhan RI		
Nama Kegiatan : MELAKUKAN MONITORING AKSES			
PERIODE PEMANTAUAN			
26 Mei 2020 – 27 Mei 2020			
DOKUMENTASI HASIL MONITORING AKSES :			
<ul style="list-style-type: none"> • Hasil monitoring akses perangkat dan jaringan terlampir • Hasil pemantauan website di lingkungan Kemhan RI terlampir 			
Mengetahui Kasubbid Kam Aplikasi Bid Jamkam, Eko Joko Murwanto, S.Kom., M.Sl. Pembina IV/a NIP. 197505252001121001		Jakarta, 28 Mei 2020 Pranata Komputer Ahli Pertama Taufiqurrahman, S.Sl. Penata Muda III/a NIP.198904272018021001	

BUKTI FISIK KEGIATAN PRANATA KOMPUTER AHLI			Halaman 1 dari 3																																									
Nama	Taufiqurrahman, S.Si.	Tanggal dibuat	Satu Analisa AK = 0,570																																									
NIP	198904272018021001	5 April 2020																																										
Pangkat/Golongan	Penata Muda / III/a																																											
Jabatan Fungsional	Pranata Komputer Ahli Pertama																																											
Lokasi Pengerjaan	Gd. Sutan Sjahrir Pushansiber Bainstrahan Kemhan RI																																											
Nama Kegiatan : MENGOLAH DAN MENGANALISIS HASIL VERIFIKASI ATAU VALIDASI SISTEM INFORMASI																																												
KETERANGAN																																												
<p>Melakukan analisa <i>signature</i> berdasarkan hasil pemantauan peta ancaman siber pada tanggal 04 s.d 05 April 2020. Dari pemantauan tersebut didapatkan <i>signature</i> kejadian yang menonjol dari peta ancaman siber sebagai berikut :</p> <table border="1"> <thead> <tr> <th>NO.</th> <th>SENSOR</th> <th>SIGNATURE</th> <th>IP SOURCE</th> <th>IP DESTINATION</th> </tr> <tr> <th>1</th> <th>2</th> <th>3</th> <th>4</th> <th>5</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Bintaro</td> <td><i>ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03</i></td> <td>184.105.139.74 (Amerika Serikat)</td> <td>139.255.70.212 (Indonesia)</td> </tr> <tr> <td>2</td> <td>Merdeka Barat</td> <td><i>ET P2P Edonkey Publicize File ACK</i></td> <td>150.109.12.150 (Singapura)</td> <td>172.16.60.173 (Indonesia)</td> </tr> <tr> <td>3</td> <td>Tugu Tani</td> <td><i>SURICATA TLS error message encountered</i></td> <td>139.255.27.202 (Indonesia)</td> <td>47.89.75.135 (Singapura)</td> </tr> <tr> <td>4</td> <td>Pondok Labu</td> <td><i>Signature ET P2P BitTorrent DHT ping request</i></td> <td>192.168.98.245 (Private IP)</td> <td>91.79.70.182 (Rusia)</td> </tr> <tr> <td>5</td> <td>Salemba</td> <td><i>SURICATA DNS malformed response data</i></td> <td>89.39.107.167 (Belanda)</td> <td>139.255.31.107 (Indonesia)</td> </tr> <tr> <td>6</td> <td>Sentul</td> <td><i>ET P2P Kaaza Media desktop p2pnetworking.exe Activity</i></td> <td>111.95.240.82 (Indonesia)</td> <td>10.2.25.181 (Indonesia)</td> </tr> </tbody> </table>					NO.	SENSOR	SIGNATURE	IP SOURCE	IP DESTINATION	1	2	3	4	5	1	Bintaro	<i>ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03</i>	184.105.139.74 (Amerika Serikat)	139.255.70.212 (Indonesia)	2	Merdeka Barat	<i>ET P2P Edonkey Publicize File ACK</i>	150.109.12.150 (Singapura)	172.16.60.173 (Indonesia)	3	Tugu Tani	<i>SURICATA TLS error message encountered</i>	139.255.27.202 (Indonesia)	47.89.75.135 (Singapura)	4	Pondok Labu	<i>Signature ET P2P BitTorrent DHT ping request</i>	192.168.98.245 (Private IP)	91.79.70.182 (Rusia)	5	Salemba	<i>SURICATA DNS malformed response data</i>	89.39.107.167 (Belanda)	139.255.31.107 (Indonesia)	6	Sentul	<i>ET P2P Kaaza Media desktop p2pnetworking.exe Activity</i>	111.95.240.82 (Indonesia)	10.2.25.181 (Indonesia)
NO.	SENSOR	SIGNATURE	IP SOURCE	IP DESTINATION																																								
1	2	3	4	5																																								
1	Bintaro	<i>ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03</i>	184.105.139.74 (Amerika Serikat)	139.255.70.212 (Indonesia)																																								
2	Merdeka Barat	<i>ET P2P Edonkey Publicize File ACK</i>	150.109.12.150 (Singapura)	172.16.60.173 (Indonesia)																																								
3	Tugu Tani	<i>SURICATA TLS error message encountered</i>	139.255.27.202 (Indonesia)	47.89.75.135 (Singapura)																																								
4	Pondok Labu	<i>Signature ET P2P BitTorrent DHT ping request</i>	192.168.98.245 (Private IP)	91.79.70.182 (Rusia)																																								
5	Salemba	<i>SURICATA DNS malformed response data</i>	89.39.107.167 (Belanda)	139.255.31.107 (Indonesia)																																								
6	Sentul	<i>ET P2P Kaaza Media desktop p2pnetworking.exe Activity</i>	111.95.240.82 (Indonesia)	10.2.25.181 (Indonesia)																																								

Berikut merupakan hasil pemantauan total serangan pada peta ancaman siber:

NO	ZONA	JUMLAH SERANGAN
1	2	3
1	BINTARO	517
2	MERDEKA BARAT	1.519
3	TUGU TANI	143
4	PONDOK LABU	55.828
5	SALEMBA	66
6	SENTUL	7.673
TOTAL		65.746

ANALISA DAN REKOMENDASI

Sensor Pondok Labu

1. Analisa Signature ET P2P BitTorrent DHT ping request

IP Source : 192.168.98.245 (Private IP)

```

NetRange: 192.168.0.0 - 192.168.255.255
CIDR: 192.168.0.0/16
NetName: PRIVATE-ADDRESS-CBLN-RFC1918-IANA-RESERVED
NetHandle: NET-192-168-0-0-1
Parent: NET192 (NET-192-0-0-0-0)
NetType: IANA Special Use
OriginAS:
Organization: Internet Assigned Numbers Authority (IANA)
RegDate: 1998-09-15
Updated: 2013-08-30
Comment: These addresses are in use by many millions of independently operated
networks, which might be as small as a single computer connected to a home gateway, and are
automatically configured in hundreds of millions of devices. They are only intended for use
within a private context, and traffic that needs to cross the Internet will need to use a
different, unique address.
Comment: These addresses can be used by anyone without any need to coordinate with
IANA or an Internet registry. The traffic from these addresses does not come from ICAHN or
IANA. We are not the source of activity you may see on logs or in e-mail records. Please
refer to http://www.iana.org/abuse/abusevec
Comment: These addresses were assigned by the IETF, the organization that develops
Internet protocols, in the Best Current Practice document, RFC 1918 which can be found at:
http://datatracker.ietf.org/doc/rfc1918
Ref: https://rdap.arin.net/registry/ip/192.168.0.0

OrgName: Internet Assigned Numbers Authority
OrgId: IANA
Address: 12025 Waterfront Drive
Address: Suite 300
City: Los Angeles
StateProv: CA
PostalCode: 90232
Country: US
RegDate: 2012-08-31
Updated: https://rdap.arin.net/registry/entity/IANA
Ref:

OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName: ICAHN
OrgAbusePhone: +1-310-301-1820
OrgAbuseEmail: abuse@iana.org
OrgAbuseRef: https://rdap.arin.net/registry/entity/IANA-IP-ARIN

```

IP Destination : 91.79.70.182 (Rusia)

```

inetnum: 91.78.0.0 - 91.79.255.255
netname: MTU-PPPOE
descr: Comstar-Direct CJSC
descr: Mamonovskij pereulok d.5
descr: P.O. BOX 38 123001
descr: Moscow, Russia
country: RU
admin-c: MTU1-RIPE
tech-c: MTU1-RIPE
status: ASSIGNED PA
mnt-by: MTU-NOC
created: 2009-06-22T12:41:30Z
last-modified: 2009-06-22T12:41:30Z
source: RIPE

```

IP destination tersebut berasal dari Rusia dan dikelola oleh MTS PJSC.

ET P2P BitTorrent DHT ping request adalah perangkat lunak berbagi file peer-to-peer BitTorrent. Peer-to-peer berbagi perangkat lunak memungkinkan untuk kemudahan distribusi file antara pengguna jaringan - termasuk bahan berpotensi Hak Cipta dilindungi. Kegiatan ini tidak hanya dapat menggunakan bandwidth tetapi juga dapat digunakan untuk mentransfer informasi rahasia perusahaan untuk tidak sah host eksternal untuk jaringan dilindungi melewati langkah-langkah keamanan lainnya di tempat.

2. Rekomendasi

Untuk mengatasi *ET P2P BitTorrent DHT ping request* agar membatasi penggunaan perangkat lunak *BitTorrent* dan sebaiknya semua hasil unduhan untuk segera dihapus dari komputer.

Mengetahui
Kasubbid Kam Aplikasi Bid Jamkam,

Eko Joko Murwanto, S.Kom., M.Si.
Pembina IV/a NIP. 197505252001121001

Jakarta, 7 April 2020
Pranata Komputer Ahli Pertama

Taufiqurrahman, S.Si.
Penata Muda III/a NIP.198904272018021001

BUKTI FISIK KEGIATAN PRANATA KOMPUTER AHLI			Halaman 1 dari 3																																									
Nama	Taufiqurrahman, S.Si.	Tanggal dibuat	Satu Analisa AK = 0,570																																									
NIP	198904272018021001	7 Mei 2020																																										
Pangkat/Golongan	Penata Muda / III/a																																											
Jabatan Fungsional	Pranata Komputer Ahli Pertama																																											
Lokasi Pengerjaan	Gd. Sutan Sjahrir Pushansiber Bainstrahan Kemhan RI																																											
Nama Kegiatan : MENGOLAH DAN MENGANALISIS HASIL VERIFIKASI ATAU VALIDASI SISTEM INFORMASI																																												
KETERANGAN																																												
<p>Melakukan analisa <i>signature</i> berdasarkan hasil pemantauan peta ancaman siber pada tanggal 06 s.d 07 Mei 2020. Dari pemantauan tersebut didapatkan <i>signature</i> kejadian yang menonjol dari peta ancaman siber sebagai berikut :</p> <table border="1"> <thead> <tr> <th>NO.</th> <th>SENSOR</th> <th>SIGNATURE</th> <th>IP SOURCE</th> <th>IP DESTINATION</th> </tr> <tr> <th>1</th> <th>2</th> <th>3</th> <th>4</th> <th>5</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Bintaro</td> <td>ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03</td> <td>104.153.105.184 (Amerika)</td> <td>139.255.70.212 (Indonesia)</td> </tr> <tr> <td>2</td> <td>Merdeka Barat</td> <td>-</td> <td>-</td> <td>-</td> </tr> <tr> <td>3</td> <td>Tugu Tani</td> <td>ET TROJAN Zeus P2P CnC</td> <td>103.252.21.130 (Indonesia)</td> <td>202.137.3.110 (Indonesia)</td> </tr> <tr> <td>4</td> <td>Pondok Labu</td> <td>ET POLICY Suspicious inbound to MSSQL port 1433</td> <td>220.162.244.136 (China)</td> <td>103.252.21.147 (Indonesia)</td> </tr> <tr> <td>5</td> <td>Salemba</td> <td>ET POLICY DNS Query for TOR Hidden Domain .onion Accessible Via TOR</td> <td>172.16.61.124 (IP Private)</td> <td>172.16.60.1 (IP Private)</td> </tr> <tr> <td>6</td> <td>Sentul</td> <td>ET POLICY Suspicious inbound to MSSQL port 1433</td> <td>139.255.122.194 (Indonesia)</td> <td>172.16.1.59 (IP Private)</td> </tr> </tbody> </table>					NO.	SENSOR	SIGNATURE	IP SOURCE	IP DESTINATION	1	2	3	4	5	1	Bintaro	ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03	104.153.105.184 (Amerika)	139.255.70.212 (Indonesia)	2	Merdeka Barat	-	-	-	3	Tugu Tani	ET TROJAN Zeus P2P CnC	103.252.21.130 (Indonesia)	202.137.3.110 (Indonesia)	4	Pondok Labu	ET POLICY Suspicious inbound to MSSQL port 1433	220.162.244.136 (China)	103.252.21.147 (Indonesia)	5	Salemba	ET POLICY DNS Query for TOR Hidden Domain .onion Accessible Via TOR	172.16.61.124 (IP Private)	172.16.60.1 (IP Private)	6	Sentul	ET POLICY Suspicious inbound to MSSQL port 1433	139.255.122.194 (Indonesia)	172.16.1.59 (IP Private)
NO.	SENSOR	SIGNATURE	IP SOURCE	IP DESTINATION																																								
1	2	3	4	5																																								
1	Bintaro	ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03	104.153.105.184 (Amerika)	139.255.70.212 (Indonesia)																																								
2	Merdeka Barat	-	-	-																																								
3	Tugu Tani	ET TROJAN Zeus P2P CnC	103.252.21.130 (Indonesia)	202.137.3.110 (Indonesia)																																								
4	Pondok Labu	ET POLICY Suspicious inbound to MSSQL port 1433	220.162.244.136 (China)	103.252.21.147 (Indonesia)																																								
5	Salemba	ET POLICY DNS Query for TOR Hidden Domain .onion Accessible Via TOR	172.16.61.124 (IP Private)	172.16.60.1 (IP Private)																																								
6	Sentul	ET POLICY Suspicious inbound to MSSQL port 1433	139.255.122.194 (Indonesia)	172.16.1.59 (IP Private)																																								

Berikut merupakan hasil pemantauan total serangan pada peta ancaman siber:

NO	ZONA	JUMLAH SERANGAN
1	2	3
1	BINTARO	316
2	MERDEKA BARAT	0
3	TUGU TANI	470
4	PONDOK LABU	56.602
5	SALEMBA	282
6	SENTUL	11.318
TOTAL		68.988

ANALISA DAN REKOMENDASI

Sensor Pondok Labu

1. Analisa ET POLICY Suspicious inbound to MSSQL port 1433

IP Source 220.162.244.136 (China)

IP Destination 103.252.21.147 (Indonesia)

IP Source tersebut berasal dari Fuzhou (fjtelecom.com)

IP tersebut berasal dari Pusdatin Kemhan RI.

IP Address	Country	Region	City
220.162.244.136	China	Fujian	Wuyishan
ISP	Organization	Latitude	Longitude
Fuzhou	CHINANET Fujian province network (fjtelecom.com)	27.7599	118.0307

IP Address	Country	Region	City
103.252.21.147	Indonesia	Jakarta	Jakarta
ISP	Organization	Latitude	Longitude
PUSDATIN KEMHAN RI	PUSDATIN KEMHAN RI (jasnita.net.id)	-6.2146	106.8451

Merupakan adanya *policy* yang mencurigakan yang masuk ke *Port* MSSQL 1433. *Port* TCP 1433 adalah *port default* untuk SQL Server. *Port* ini juga merupakan nomor soket *Internet Assigned Number Authority (IANA)* resmi untuk SQL Server. Sistem klien menggunakan TCP 1433 untuk terhubung ke mesin basis data. Kemudian SQL Server Management Studio (SSMS) menggunakan *port* tersebut untuk mengelola instance SQL Server di seluruh jaringan. SQL Server dapat dikonfigurasi agar menggunakan port yang berbeda, tetapi sejauh ini *port* 1433 merupakan implementasi yang paling umum.

2. Rekomendasi

Untuk mencegah *ET POLICY Suspicious inbound to MSSQL port 1433* menonaktifkan port MSSQL jika tak dibutuhkan, kemudian mengaktifkan firewall, memeriksa komunikasi data jaringan dan blokir semua jaringan yang mencurigakan.

Mengetahui
Kasubbid Kam Aplikasi Bid Jamkam,

Eko Joko Murwanto, S.Kom., M.Si.
Pembina IV/a NIP. 197505252001121001

Jakarta, 11 Mei 2020
Pranata Komputer Ahli Pertama

Taufiqurrahman, S.Si.
Penata Muda III/a NIP.198904272018021001

BUKTI FISIK KEGIATAN PRANATA KOMPUTER AHLI			Halaman 1 dari 3																																									
Nama	Taufiqurrahman, S.Si.	Tanggal dibuat	Satu Analisa AK = 0,570																																									
NIP	198904272018021001	26 Mei 2020																																										
Pangkat/Golongan	Penata Muda / III/a																																											
Jabatan Fungsional	Pranata Komputer Ahli Pertama																																											
Lokasi Pengerjaan	Gd. Sutan Sjahrir Pushansiber Bainstrahan Kemhan RI																																											
Nama Kegiatan : MENGOLAH DAN MENGANALISIS HASIL VERIFIKASI ATAU VALIDASI SISTEM INFORMASI																																												
KETERANGAN																																												
<p>Melakukan analisa <i>signature</i> berdasarkan hasil pemantauan peta ancaman siber pada tanggal 26 s.d 27 Mei 2020. Dari pemantauan tersebut didapatkan <i>signature</i> kejadian yang menonjol dari peta ancaman siber sebagai berikut :</p> <table border="1"> <thead> <tr> <th>NO</th> <th>SENSOR</th> <th>SIGNATURE</th> <th>IP SOURCE</th> <th>IP DESTINATION</th> </tr> <tr> <th>1</th> <th>2</th> <th>3</th> <th>4</th> <th>5</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Bintaro</td> <td><i>ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03</i></td> <td>23.228.109.146 (Amerika)</td> <td>139.255.70.212 (Indonesia)</td> </tr> <tr> <td>2</td> <td>Merdeka Barat</td> <td>-</td> <td>-</td> <td>-</td> </tr> <tr> <td>3</td> <td>Tugu Tani</td> <td><i>SURICATA TLS error message encountered</i></td> <td>139.255.27.202 (Indonesia)</td> <td>203.119.216.255 (China)</td> </tr> <tr> <td>4</td> <td>Pondok Labu</td> <td><i>ET DNS Non-DNS or Non-Compliant DNS traffic on DNS port Opcode 8 through 15 set</i></td> <td>103.252.21.151 (Indonesia)</td> <td>111.108.191.84 (Jepang)</td> </tr> <tr> <td>5</td> <td>Salemba</td> <td><i>Signature ET POLICY Suspicious inbound to MSSQL port 1433</i></td> <td>103.252.7.27 (India)</td> <td>118.98.44.20 (Indonesia)</td> </tr> <tr> <td>6</td> <td>Sentul</td> <td><i>ET P2P Kaaza Media desktop p2pnetworking.exe Activity</i></td> <td>74.125.12.71 (Amerika)</td> <td>10.3.160.168 (IP Private)</td> </tr> </tbody> </table>					NO	SENSOR	SIGNATURE	IP SOURCE	IP DESTINATION	1	2	3	4	5	1	Bintaro	<i>ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03</i>	23.228.109.146 (Amerika)	139.255.70.212 (Indonesia)	2	Merdeka Barat	-	-	-	3	Tugu Tani	<i>SURICATA TLS error message encountered</i>	139.255.27.202 (Indonesia)	203.119.216.255 (China)	4	Pondok Labu	<i>ET DNS Non-DNS or Non-Compliant DNS traffic on DNS port Opcode 8 through 15 set</i>	103.252.21.151 (Indonesia)	111.108.191.84 (Jepang)	5	Salemba	<i>Signature ET POLICY Suspicious inbound to MSSQL port 1433</i>	103.252.7.27 (India)	118.98.44.20 (Indonesia)	6	Sentul	<i>ET P2P Kaaza Media desktop p2pnetworking.exe Activity</i>	74.125.12.71 (Amerika)	10.3.160.168 (IP Private)
NO	SENSOR	SIGNATURE	IP SOURCE	IP DESTINATION																																								
1	2	3	4	5																																								
1	Bintaro	<i>ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03</i>	23.228.109.146 (Amerika)	139.255.70.212 (Indonesia)																																								
2	Merdeka Barat	-	-	-																																								
3	Tugu Tani	<i>SURICATA TLS error message encountered</i>	139.255.27.202 (Indonesia)	203.119.216.255 (China)																																								
4	Pondok Labu	<i>ET DNS Non-DNS or Non-Compliant DNS traffic on DNS port Opcode 8 through 15 set</i>	103.252.21.151 (Indonesia)	111.108.191.84 (Jepang)																																								
5	Salemba	<i>Signature ET POLICY Suspicious inbound to MSSQL port 1433</i>	103.252.7.27 (India)	118.98.44.20 (Indonesia)																																								
6	Sentul	<i>ET P2P Kaaza Media desktop p2pnetworking.exe Activity</i>	74.125.12.71 (Amerika)	10.3.160.168 (IP Private)																																								

Berikut merupakan hasil pemantauan total serangan pada peta ancaman siber:

NO	ZONA	JUMLAH SERANGAN
1	2	3
1	BINTARO	484
2	MERDEKA BARAT	0
3	TUGU TANI	9
4	PONDOK LABU	54.085
5	SALEMBA	164
6	SENTUL	9.083
TOTAL		63.825

ANALISA DAN REKOMENDASI

Sensor Pondok Labu

1. Analisa ET DNS Non-DNS or Non-Compliant DNS traffic on DNS port Opcode 8 through 15 set

IP Source 103.252.21.151 (Indonesia)

IP Source tersebut berasal milik Pusdatin Kemhan

Details for 103.252.21.151

IP: 103.252.21.151
 Decimal: 1744573847
 Hostname: 103.252.21.151
 ASN: 59137
 ISP: Pusdatin Kemhan Ri
 Organization: Pusdatin Kemhan Ri
 Services: None detected
 Type: [Broadband](#)
 Assignment: [Likely Static IP](#)
 Blacklist: [Click to Check Blacklist Status](#)
 Continent: Asia
 Country: Indonesia 🇮🇩
 State/Region: Jakarta
 City: Jakarta
 Latitude: -6.1741 (6° 10' 26.76" S)
 Longitude: 106.8296 (106° 49' 46.56" E)

IP Destination 111.108.191.84 (Jepang)

```
inetnum: 111.96.0.0 - 111.111.255.255
netname: KDDI
descr: KDDI CORPORATION
descr: Garden Air Tower, 3-10-10, Iidabashi, Chiyoda-ku, Tokyo, 102-8460, Japan
country: JP
admin-c: JNIC1-AP
tech-c: JNIC1-AP
status: ALLOCATED PORTABLE
remarks: Email address for spam or abuse complaints abuse@dion.ne.jp
mnt-by: MAINT-JPNIC
mnt-irt: IRT-JPNIC-JP
mnt-lower: MAINT-JPNIC
last-modified: 2015-12-01T22:21:21Z
source: APNIC
```

IP tersebut milik KDDI Corporation yang bertempat di Tokyo, Jepang

Merupakan aktifitas IDS yang mendeteksi sebuah DNS yang tidak aman yang menggunakan lalu lintas Secure DNS yang berjalan pada port 53 yang menggunakan protokol lalu lintas data UDP. Terpantau signature ini muncul saat IP milik Kemhan (103.252.21.151) mencoba mengakses IP 111.108.191.84 asal Jepang. Dari penelusuran menggunakan VirusTotal dan AbuseIPDB, IP tujuan memiliki reputasi baik. Diketahui, Port 53 biasa digunakan oleh service dari aplikasi Avast, Bittorrent ataupun Skype. Sehingga, signature ini adalah *false positive*.

2. Rekomendasi

Walaupun dinyatakan sebagai *false positive*, direkomendasikan untuk tetap melakukan pemeriksaan secara detail dan berkala pada log perangkat jaringan maupun sebuah server. Lakukan Drop IP jika terbukti membahayakan pada sebuah keamanan data/Jaringan.

Mengetahui
Kasubbid Kam Aplikasi Bid Jamkam,

Eko Joko Murwanto, S.Kom., M.SI.
Pembina IV/a NIP. 197505252001121001

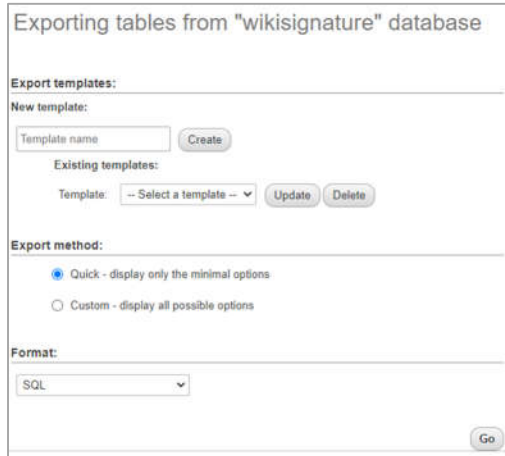
Jakarta, 28 Mei 2020
Pranata Komputer Ahli Pertama

Taufiqurrahman, S.SI.
Penata Muda III/a NIP.198904272018021001

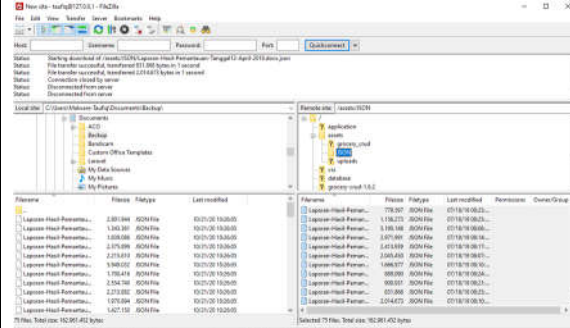
BUKTI FISIK KEGIATAN PRANATA KOMPUTER AHLI			Halaman 1 dari 2																																																																																																																				
Nama	Taufiqurrahman, S.Si.	Tanggal dibuat	Satu Kali AK = 0,155																																																																																																																				
NIP	198904272018021001	6 Januari 2020																																																																																																																					
Pangkat/Golongan	Penata Muda / III/a																																																																																																																						
Jabatan Fungsional	Pranata Komputer Ahli Pertama																																																																																																																						
Lokasi Pengerjaan	Lab Malware, Gd. Sutan Sjahrir Pushansiber																																																																																																																						
Nama Kegiatan : MELAKSANAKAN DUPLIKASI DATABASE																																																																																																																							
TUJUAN DUPLIKASI																																																																																																																							
<ul style="list-style-type: none"> • <i>Back-up</i> bulanan diperlukan untuk mengamankan data <i>signature</i> ancaman siber dan dokumen laporan terkait penanganan ancaman siber yang terdeteksi pada sensor dan <i>IDS (Intrusion Detection System)</i> yang ada di Pushansiber. • Selain itu data dan dokumen yang telah lampau dapat diarsipkan guna menyediakan area kosong untuk data dan dokumen yang baru 																																																																																																																							
NAMA, BESARAN DAN STRUKTUR DATABASE																																																																																																																							
DBMS : MariaDB 10.4.11 Database : wikisignature Jenis File Backup : SQL dan JSON Besaran data : SQL (307 KB), JSON (31,6 MB) Struktur Data :																																																																																																																							
wiki_signature <table border="1"> <thead> <tr> <th>Column</th> <th>Type</th> <th>Null</th> <th>Default</th> <th>Links to</th> <th>Comments</th> <th>Media (MIME) type</th> </tr> </thead> <tbody> <tr> <td>id_report (<i>Primary</i>)</td> <td>int(11)</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>date_created</td> <td>timestamp</td> <td>No</td> <td>current_timestamp()</td> <td></td> <td></td> <td></td> </tr> <tr> <td>date_updated</td> <td>timestamp</td> <td>No</td> <td>current_timestamp()</td> <td></td> <td></td> <td></td> </tr> <tr> <td>document</td> <td>varchar(100)</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>report_date</td> <td>varchar(100)</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>signature_name</td> <td>varchar(255)</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>location</td> <td>varchar(100)</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>ip_source</td> <td>varchar(100)</td> <td>No</td> <td>n/a</td> <td></td> <td></td> <td></td> </tr> <tr> <td>geo_source</td> <td>varchar(100)</td> <td>No</td> <td>n/a</td> <td></td> <td></td> <td></td> </tr> <tr> <td>ip_destination</td> <td>varchar(100)</td> <td>No</td> <td>n/a</td> <td></td> <td></td> <td></td> </tr> <tr> <td>geo_destination</td> <td>varchar(100)</td> <td>No</td> <td>n/a</td> <td></td> <td></td> <td></td> </tr> <tr> <td>analysis</td> <td>text</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>contributor</td> <td>varchar(100)</td> <td>No</td> <td>Admin</td> <td></td> <td></td> <td></td> </tr> </tbody> </table> Indexes <table border="1"> <thead> <tr> <th>Keyname</th> <th>Type</th> <th>Unique</th> <th>Packed</th> <th>Column</th> <th>Cardinality</th> <th>Collation</th> <th>Null</th> <th>Comment</th> </tr> </thead> <tbody> <tr> <td>PRIMARY</td> <td>BTREE</td> <td>Yes</td> <td>No</td> <td>id_report</td> <td>943</td> <td>A</td> <td>No</td> <td></td> </tr> </tbody> </table>				Column	Type	Null	Default	Links to	Comments	Media (MIME) type	id_report (<i>Primary</i>)	int(11)	No					date_created	timestamp	No	current_timestamp()				date_updated	timestamp	No	current_timestamp()				document	varchar(100)	No					report_date	varchar(100)	No					signature_name	varchar(255)	No					location	varchar(100)	No					ip_source	varchar(100)	No	n/a				geo_source	varchar(100)	No	n/a				ip_destination	varchar(100)	No	n/a				geo_destination	varchar(100)	No	n/a				analysis	text	No					contributor	varchar(100)	No	Admin				Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment	PRIMARY	BTREE	Yes	No	id_report	943	A	No	
Column	Type	Null	Default	Links to	Comments	Media (MIME) type																																																																																																																	
id_report (<i>Primary</i>)	int(11)	No																																																																																																																					
date_created	timestamp	No	current_timestamp()																																																																																																																				
date_updated	timestamp	No	current_timestamp()																																																																																																																				
document	varchar(100)	No																																																																																																																					
report_date	varchar(100)	No																																																																																																																					
signature_name	varchar(255)	No																																																																																																																					
location	varchar(100)	No																																																																																																																					
ip_source	varchar(100)	No	n/a																																																																																																																				
geo_source	varchar(100)	No	n/a																																																																																																																				
ip_destination	varchar(100)	No	n/a																																																																																																																				
geo_destination	varchar(100)	No	n/a																																																																																																																				
analysis	text	No																																																																																																																					
contributor	varchar(100)	No	Admin																																																																																																																				
Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment																																																																																																															
PRIMARY	BTREE	Yes	No	id_report	943	A	No																																																																																																																
TANGGAL DAN LAMA Pengerjaan																																																																																																																							
6 Januari 2020, ± 1 Jam Pengerjaan																																																																																																																							

DOKUMENTASI Pengerjaan

1. Melakukan export database melalui fitur phpmyadmin. Hasil export berupa file .sql



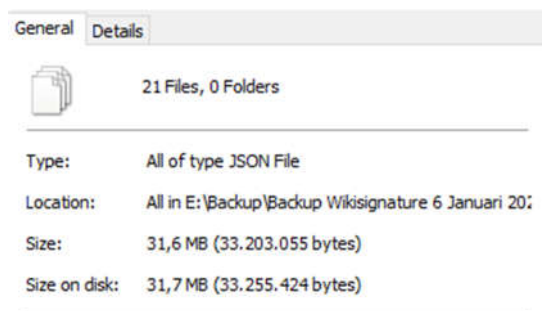
2. Melakukan duplikasi dokumen yang terdapat pada sistem untuk *back-up* data dan asset menggunakan filezilla



3. Hasil backup berupa file .sql yang menampung data dari database dan file JSON yang merupakan dokumen/asset dari sistem. Back-up ini disimpan dalam Hardisk External dan diberi penamaan sesuai dengan tanggal back-up dan nama sistem.

Name	Date modified	Type	Size
2020-01-06 backup wikisignature.sql	06/01/2020 10:37	SQL File	307 KB

Gambar 1 backup sql



Gambar 2 back-up JSON

Mengetahui
Kasubbid Kam Aplikasi Bid Jamkam,

Eko Joko Murwanto, S.Kom., M.SI.
Pembina IV/a NIP. 197505252001121001

Jakarta, 7 Januari 2020
Pranata Komputer Ahli Pertama

Taufiqurrahman, S.SI.
Penata Muda III/a NIP.198904272018021001

BUKTI FISIK KEGIATAN PRANATA KOMPUTER AHLI			Halaman 1 dari 2																																																																																																																				
Nama	Taufiqurrahman, S.Si.	Tanggal dibuat	Satu Kali AK = 0,155																																																																																																																				
NIP	198904272018021001	4 Februari 2020																																																																																																																					
Pangkat/Golongan	Penata Muda / III/a																																																																																																																						
Jabatan Fungsional	Pranata Komputer Ahli Pertama																																																																																																																						
Lokasi Pengerjaan	Lab Malware, Gd. Sutan Sjahrir Pushansiber																																																																																																																						
Nama Kegiatan : MELAKSANAKAN DUPLIKASI DATABASE																																																																																																																							
TUJUAN DUPLIKASI																																																																																																																							
<ul style="list-style-type: none"> • <i>Back-up</i> bulanan diperlukan untuk mengamankan data <i>signature</i> ancaman siber dan dokumen laporan terkait penanganan ancaman siber yang terdeteksi pada sensor dan <i>IDS (Intrusion Detection System)</i> yang ada di Pushansiber. • Selain itu data dan dokumen yang telah lampau dapat diarsipkan guna menyediakan area kosong untuk data dan dokumen yang baru 																																																																																																																							
NAMA, BESARAN DAN STRUKTUR DATABASE																																																																																																																							
DBMS : MariaDB 10.4.11 Database : wikisignature Jenis File Backup : SQL dan JSON Besaran data : SQL (374 KB), JSON (40,6 MB) Media Penyimpanan : Hardrive External Struktur Data : wiki_signature <table border="1"> <thead> <tr> <th>Column</th> <th>Type</th> <th>Null</th> <th>Default</th> <th>Links to</th> <th>Comments</th> <th>Media (MIME) type</th> </tr> </thead> <tbody> <tr> <td>id_report (<i>Primary</i>)</td> <td>int(11)</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>date_crated</td> <td>timestamp</td> <td>No</td> <td>current_timestamp()</td> <td></td> <td></td> <td></td> </tr> <tr> <td>date_updated</td> <td>timestamp</td> <td>No</td> <td>current_timestamp()</td> <td></td> <td></td> <td></td> </tr> <tr> <td>document</td> <td>varchar(100)</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>report_date</td> <td>varchar(100)</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>signature_name</td> <td>varchar(255)</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>location</td> <td>varchar(100)</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>ip_source</td> <td>varchar(100)</td> <td>No</td> <td>n/a</td> <td></td> <td></td> <td></td> </tr> <tr> <td>geo_source</td> <td>varchar(100)</td> <td>No</td> <td>n/a</td> <td></td> <td></td> <td></td> </tr> <tr> <td>ip_destination</td> <td>varchar(100)</td> <td>No</td> <td>n/a</td> <td></td> <td></td> <td></td> </tr> <tr> <td>geo_destination</td> <td>varchar(100)</td> <td>No</td> <td>n/a</td> <td></td> <td></td> <td></td> </tr> <tr> <td>analysis</td> <td>text</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>contributor</td> <td>varchar(100)</td> <td>No</td> <td>Admin</td> <td></td> <td></td> <td></td> </tr> </tbody> </table> Indexes <table border="1"> <thead> <tr> <th>Keyname</th> <th>Type</th> <th>Unique</th> <th>Packed</th> <th>Column</th> <th>Cardinality</th> <th>Collation</th> <th>Null</th> <th>Comment</th> </tr> </thead> <tbody> <tr> <td>PRIMARY</td> <td>BTREE</td> <td>Yes</td> <td>No</td> <td>id_report</td> <td>943</td> <td>A</td> <td>No</td> <td></td> </tr> </tbody> </table>				Column	Type	Null	Default	Links to	Comments	Media (MIME) type	id_report (<i>Primary</i>)	int(11)	No					date_crated	timestamp	No	current_timestamp()				date_updated	timestamp	No	current_timestamp()				document	varchar(100)	No					report_date	varchar(100)	No					signature_name	varchar(255)	No					location	varchar(100)	No					ip_source	varchar(100)	No	n/a				geo_source	varchar(100)	No	n/a				ip_destination	varchar(100)	No	n/a				geo_destination	varchar(100)	No	n/a				analysis	text	No					contributor	varchar(100)	No	Admin				Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment	PRIMARY	BTREE	Yes	No	id_report	943	A	No	
Column	Type	Null	Default	Links to	Comments	Media (MIME) type																																																																																																																	
id_report (<i>Primary</i>)	int(11)	No																																																																																																																					
date_crated	timestamp	No	current_timestamp()																																																																																																																				
date_updated	timestamp	No	current_timestamp()																																																																																																																				
document	varchar(100)	No																																																																																																																					
report_date	varchar(100)	No																																																																																																																					
signature_name	varchar(255)	No																																																																																																																					
location	varchar(100)	No																																																																																																																					
ip_source	varchar(100)	No	n/a																																																																																																																				
geo_source	varchar(100)	No	n/a																																																																																																																				
ip_destination	varchar(100)	No	n/a																																																																																																																				
geo_destination	varchar(100)	No	n/a																																																																																																																				
analysis	text	No																																																																																																																					
contributor	varchar(100)	No	Admin																																																																																																																				
Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment																																																																																																															
PRIMARY	BTREE	Yes	No	id_report	943	A	No																																																																																																																
TANGGAL DAN LAMA Pengerjaan																																																																																																																							
4 Februari 2020, ± 1 Jam Pengerjaan																																																																																																																							

1. Melakukan export database melalui fitur phpmyadmin. Hasil export berupa file .sql

Exporting tables from "wikisignature" database

Export templates:

New template:

Template name

Create

Existing templates:

Template: -- Select a template --

Update

Delete

Export method:

☒ Quick - display only the minimal options

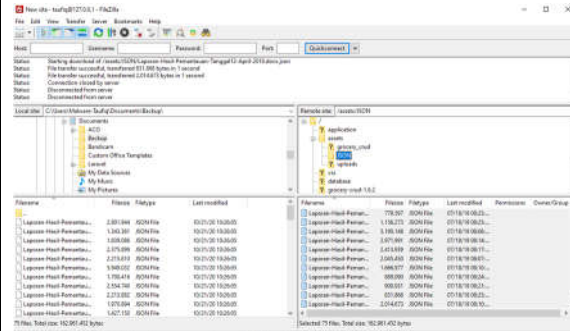
☐ Custom - display all possible options

Format:


SQL

Go

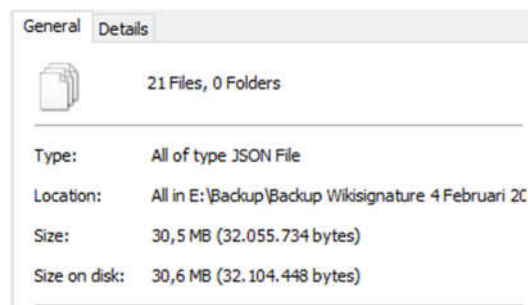
2. Melakukan duplikasi dokumen yang terdapat pada sistem untuk *back-up* data dan asset menggunakan filezilla



3. Hasil backup berupa file .sql yang menampung data dari database dan file JSON yang merupakan dokumen/asset dari sistem. Back-up ini disimpan dalam Hardisk External dan diberi penamaan sesuai dengan tanggal back-up dan nama sistem.

Name	Date modified	Type	Size
 2020-02-04 backup wikisignature.sql	04/02/2020 10:37	SQL File	341 KB

Gambar 1 backup sql



Gambar 2 back-up JSON

Mengetahui
Kasubbid Kam Aplikasi Bid Jamkam,

Jakarta, 5 Februari 2020
Pranata Komputer Ahli Pertama

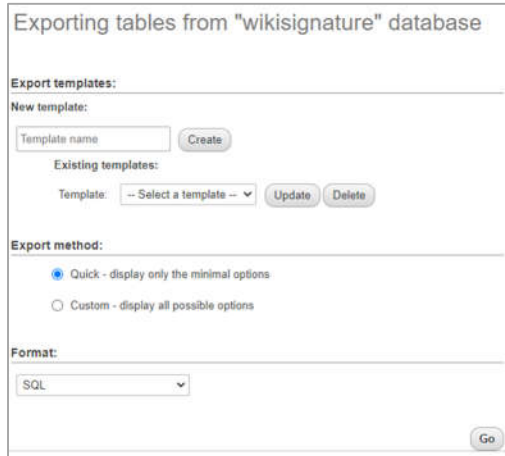
Eko Joko Murwanto, S.Kom., M.Si.
Pembina IV/a NIP. 197505252001121001

Taufiqurrahman, S.Si.
Penata Muda III/a NIP.198904272018021001

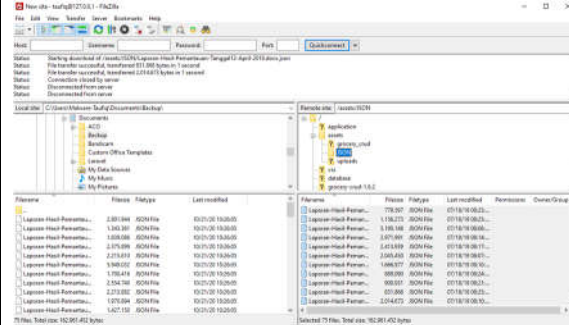
BUKTI FISIK KEGIATAN PRANATA KOMPUTER AHLI			Halaman 1 dari 2																																																																																																																				
Nama	Taufiqurrahman, S.Si.	Tanggal dibuat	Satu Kali AK = 0,155																																																																																																																				
NIP	198904272018021001	3 Maret 2020																																																																																																																					
Pangkat/Golongan	Penata Muda / III/a																																																																																																																						
Jabatan Fungsional	Pranata Komputer Ahli Pertama																																																																																																																						
Lokasi Pengerjaan	Lab Malware, Gd. Sutan Sjahrir Pushansiber																																																																																																																						
Nama Kegiatan : MELAKSANAKAN DUPLIKASI DATABASE																																																																																																																							
TUJUAN DUPLIKASI																																																																																																																							
<ul style="list-style-type: none"> • <i>Back-up</i> bulanan diperlukan untuk mengamankan data <i>signature</i> ancaman siber dan dokumen laporan terkait penanganan ancaman siber yang terdeteksi pada sensor dan <i>IDS (Intrusion Detection System)</i> yang ada di Pushansiber. • Selain itu data dan dokumen yang telah lampau dapat diarsipkan guna menyediakan area kosong untuk data dan dokumen yang baru 																																																																																																																							
NAMA, BESARAN DAN STRUKTUR DATABASE																																																																																																																							
DBMS : MariaDB 10.4.11 Database : wikisignature Jenis File Backup : SQL dan JSON Besaran data : SQL (374 KB), JSON (40,6 MB) Media Penyimpanan : Hardrive External Struktur Data : <div style="margin-top: 10px;"> <p>wiki_signature</p> <table border="1"> <thead> <tr> <th>Column</th> <th>Type</th> <th>Null</th> <th>Default</th> <th>Links to</th> <th>Comments</th> <th>Media (MIME) type</th> </tr> </thead> <tbody> <tr> <td>id_report (<i>Primary</i>)</td> <td>int(11)</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>date_created</td> <td>timestamp</td> <td>No</td> <td>current_timestamp()</td> <td></td> <td></td> <td></td> </tr> <tr> <td>date_updated</td> <td>timestamp</td> <td>No</td> <td>current_timestamp()</td> <td></td> <td></td> <td></td> </tr> <tr> <td>document</td> <td>varchar(100)</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>report_date</td> <td>varchar(100)</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>signature_name</td> <td>varchar(255)</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>location</td> <td>varchar(100)</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>ip_source</td> <td>varchar(100)</td> <td>No</td> <td>n/a</td> <td></td> <td></td> <td></td> </tr> <tr> <td>geo_source</td> <td>varchar(100)</td> <td>No</td> <td>n/a</td> <td></td> <td></td> <td></td> </tr> <tr> <td>ip_destination</td> <td>varchar(100)</td> <td>No</td> <td>n/a</td> <td></td> <td></td> <td></td> </tr> <tr> <td>geo_destination</td> <td>varchar(100)</td> <td>No</td> <td>n/a</td> <td></td> <td></td> <td></td> </tr> <tr> <td>analysis</td> <td>text</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>contributor</td> <td>varchar(100)</td> <td>No</td> <td>Admin</td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <p>Indexes</p> <table border="1"> <thead> <tr> <th>Keyname</th> <th>Type</th> <th>Unique</th> <th>Packed</th> <th>Column</th> <th>Cardinality</th> <th>Collation</th> <th>Null</th> <th>Comment</th> </tr> </thead> <tbody> <tr> <td>PRIMARY</td> <td>BTREE</td> <td>Yes</td> <td>No</td> <td>id_report</td> <td>943</td> <td>A</td> <td>No</td> <td></td> </tr> </tbody> </table> </div>				Column	Type	Null	Default	Links to	Comments	Media (MIME) type	id_report (<i>Primary</i>)	int(11)	No					date_created	timestamp	No	current_timestamp()				date_updated	timestamp	No	current_timestamp()				document	varchar(100)	No					report_date	varchar(100)	No					signature_name	varchar(255)	No					location	varchar(100)	No					ip_source	varchar(100)	No	n/a				geo_source	varchar(100)	No	n/a				ip_destination	varchar(100)	No	n/a				geo_destination	varchar(100)	No	n/a				analysis	text	No					contributor	varchar(100)	No	Admin				Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment	PRIMARY	BTREE	Yes	No	id_report	943	A	No	
Column	Type	Null	Default	Links to	Comments	Media (MIME) type																																																																																																																	
id_report (<i>Primary</i>)	int(11)	No																																																																																																																					
date_created	timestamp	No	current_timestamp()																																																																																																																				
date_updated	timestamp	No	current_timestamp()																																																																																																																				
document	varchar(100)	No																																																																																																																					
report_date	varchar(100)	No																																																																																																																					
signature_name	varchar(255)	No																																																																																																																					
location	varchar(100)	No																																																																																																																					
ip_source	varchar(100)	No	n/a																																																																																																																				
geo_source	varchar(100)	No	n/a																																																																																																																				
ip_destination	varchar(100)	No	n/a																																																																																																																				
geo_destination	varchar(100)	No	n/a																																																																																																																				
analysis	text	No																																																																																																																					
contributor	varchar(100)	No	Admin																																																																																																																				
Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment																																																																																																															
PRIMARY	BTREE	Yes	No	id_report	943	A	No																																																																																																																
TANGGAL DAN LAMA Pengerjaan																																																																																																																							
3 Maret 2020, ± 1 Jam Pengerjaan																																																																																																																							

DOKUMENTASI Pengerjaan

1. Melakukan export database melalui fitur phpmyadmin. Hasil export berupa file .sql



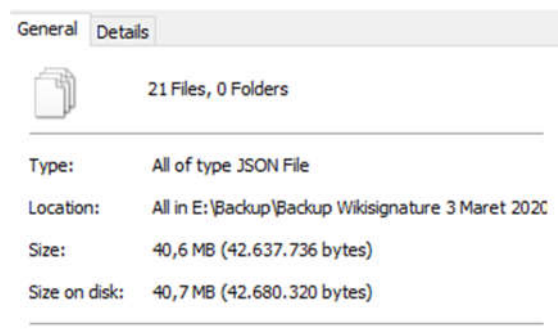
2. Melakukan duplikasi dokumen yang terdapat pada sistem untuk *back-up* data dan asset menggunakan filezilla



3. Hasil backup berupa file .sql yang menampung data dari database dan file JSON yang merupakan dokumen/asset dari sistem. Back-up ini disimpan dalam Hardisk External dan diberi penamaan sesuai dengan tanggal back-up dan nama sistem.

Name	Date modified	Type	Size
2020-03-03 backup wiki_signature.sql	03/03/2020 10:37	SQL File	374 KB

Gambar 1 backup sql



Gambar 2 back-up JSON

Mengetahui
Kasubbid Kam Aplikasi Bid Jamkam,

Eko Joko Murwanto, S.Kom., M.Si.
Pembina IV/a NIP. 197505252001121001

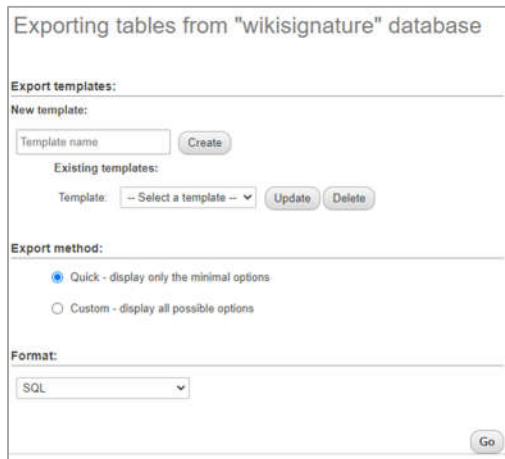
Jakarta, 4 Maret 2020
Pranata Komputer Ahli Pertama

Taufiqurrahman, S.Si.
Penata Muda III/a NIP.198904272018021001

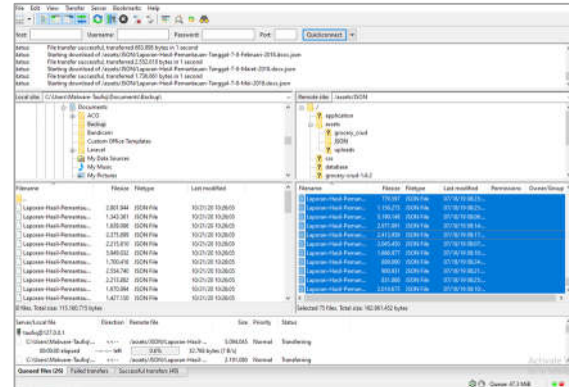
BUKTI FISIK KEGIATAN PRANATA KOMPUTER AHLI			Halaman 1 dari 2																																																																																																																				
Nama	Taufiqurrahman, S.Si.	Tanggal dibuat	Satu Kali AK = 0,155																																																																																																																				
NIP	198904272018021001	6 April 2020																																																																																																																					
Pangkat/Golongan	Penata Muda / III/a																																																																																																																						
Jabatan Fungsional	Pranata Komputer Ahli Pertama																																																																																																																						
Lokasi Pengerjaan	Lab Malware, Gd. Sutan Sjahrir Pushansiber																																																																																																																						
Nama Kegiatan : MELAKSANAKAN DUPLIKASI DATABASE																																																																																																																							
TUJUAN DUPLIKASI																																																																																																																							
<ul style="list-style-type: none"> • <i>Back-up</i> bulanan diperlukan untuk mengamankan data <i>signature</i> ancaman siber dan dokumen laporan terkait penanganan ancaman siber yang terdeteksi pada sensor dan <i>IDS (Intrusion Detection System)</i> yang ada di Pushansiber. • Selain itu data dan dokumen yang telah lampau dapat diarsipkan guna menyediakan area kosong untuk data dan dokumen yang baru 																																																																																																																							
NAMA, BESARAN DAN STRUKTUR DATABASE																																																																																																																							
DBMS : MariaDB 10.4.11 Database : wikisignature Jenis File Backup : SQL dan JSON Besaran data : SQL (401 KB), JSON (35,2 MB) Media Penyimpanan : Hardrive External Struktur Data : <div style="margin-top: 10px;"> <p>wiki_signature</p> <table border="1"> <thead> <tr> <th>Column</th> <th>Type</th> <th>Null</th> <th>Default</th> <th>Links to</th> <th>Comments</th> <th>Media (MIME) type</th> </tr> </thead> <tbody> <tr> <td>id_report (<i>Primary</i>)</td> <td>int(11)</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>date_crated</td> <td>timestamp</td> <td>No</td> <td>current_timestamp()</td> <td></td> <td></td> <td></td> </tr> <tr> <td>date_updated</td> <td>timestamp</td> <td>No</td> <td>current_timestamp()</td> <td></td> <td></td> <td></td> </tr> <tr> <td>document</td> <td>varchar(100)</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>report_date</td> <td>varchar(100)</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>signature_name</td> <td>varchar(255)</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>location</td> <td>varchar(100)</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>ip_source</td> <td>varchar(100)</td> <td>No</td> <td>n/a</td> <td></td> <td></td> <td></td> </tr> <tr> <td>geo_source</td> <td>varchar(100)</td> <td>No</td> <td>n/a</td> <td></td> <td></td> <td></td> </tr> <tr> <td>ip_destination</td> <td>varchar(100)</td> <td>No</td> <td>n/a</td> <td></td> <td></td> <td></td> </tr> <tr> <td>geo_destination</td> <td>varchar(100)</td> <td>No</td> <td>n/a</td> <td></td> <td></td> <td></td> </tr> <tr> <td>analysis</td> <td>text</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>contributor</td> <td>varchar(100)</td> <td>No</td> <td>Admin</td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <p>Indexes</p> <table border="1"> <thead> <tr> <th>Keyname</th> <th>Type</th> <th>Unique</th> <th>Packed</th> <th>Column</th> <th>Cardinality</th> <th>Collation</th> <th>Null</th> <th>Comment</th> </tr> </thead> <tbody> <tr> <td>PRIMARY</td> <td>BTREE</td> <td>Yes</td> <td>No</td> <td>id_report</td> <td>943</td> <td>A</td> <td>No</td> <td></td> </tr> </tbody> </table> </div>				Column	Type	Null	Default	Links to	Comments	Media (MIME) type	id_report (<i>Primary</i>)	int(11)	No					date_crated	timestamp	No	current_timestamp()				date_updated	timestamp	No	current_timestamp()				document	varchar(100)	No					report_date	varchar(100)	No					signature_name	varchar(255)	No					location	varchar(100)	No					ip_source	varchar(100)	No	n/a				geo_source	varchar(100)	No	n/a				ip_destination	varchar(100)	No	n/a				geo_destination	varchar(100)	No	n/a				analysis	text	No					contributor	varchar(100)	No	Admin				Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment	PRIMARY	BTREE	Yes	No	id_report	943	A	No	
Column	Type	Null	Default	Links to	Comments	Media (MIME) type																																																																																																																	
id_report (<i>Primary</i>)	int(11)	No																																																																																																																					
date_crated	timestamp	No	current_timestamp()																																																																																																																				
date_updated	timestamp	No	current_timestamp()																																																																																																																				
document	varchar(100)	No																																																																																																																					
report_date	varchar(100)	No																																																																																																																					
signature_name	varchar(255)	No																																																																																																																					
location	varchar(100)	No																																																																																																																					
ip_source	varchar(100)	No	n/a																																																																																																																				
geo_source	varchar(100)	No	n/a																																																																																																																				
ip_destination	varchar(100)	No	n/a																																																																																																																				
geo_destination	varchar(100)	No	n/a																																																																																																																				
analysis	text	No																																																																																																																					
contributor	varchar(100)	No	Admin																																																																																																																				
Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment																																																																																																															
PRIMARY	BTREE	Yes	No	id_report	943	A	No																																																																																																																
TANGGAL DAN LAMA Pengerjaan																																																																																																																							
6 April 2020, ± 1 Jam Pengerjaan																																																																																																																							

DOKUMENTASI Pengerjaan

1. Melakukan export database melalui fitur phpmyadmin. Hasil export berupa file .sql



2. Melakukan duplikasi dokumen yang terdapat pada sistem untuk *back-up* data dan asset menggunakan filezilla



3. Hasil backup berupa file .sql yang menampung data dari database dan file JSON yang merupakan dokumen/asset dari sistem. Back-up ini disimpan dalam Hardisk External dan diberi penamaan sesuai dengan tanggal back-up dan nama sistem.

Name	Date modified	Type	Size
2020-04-06 Backup Wikisignature.sql	06/04/2020 10:37	SQL File	401 KB

Gambar 1 backup sql

General	Details
20 Files, 0 Folders	
Type:	All of type JSON File
Location:	All in E:\Backup\Backup Wikisignature 6 April 2020\
Size:	35,2 MB (36.986.709 bytes)
Size on disk:	35,3 MB (37.027.840 bytes)

Gambar 2 back-up JSON

Mengetahui
Kasubbid Kam Aplikasi Bid Jamkam,

Eko Joko Murwanto, S.Kom., M.Si.
Pembina IV/a NIP. 197505252001121001

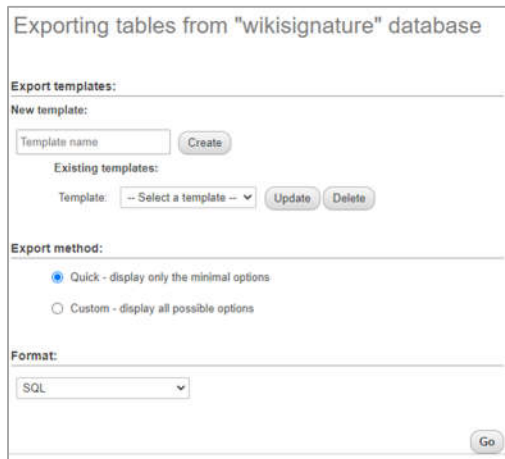
Jakarta, 7 April 2020
Pranata Komputer Ahli Pertama

Taufiqurrahman, S.Si.
Penata Muda III/a NIP.198904272018021001

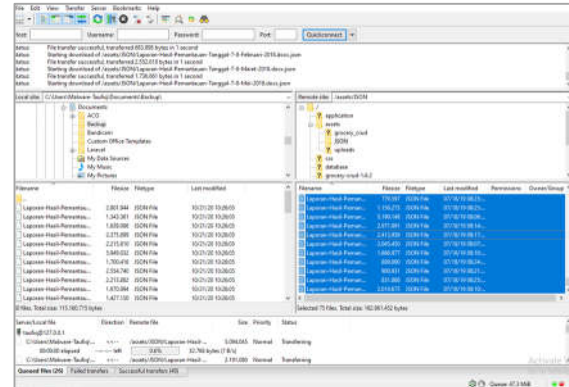
BUKTI FISIK KEGIATAN PRANATA KOMPUTER AHLI			Halaman 1 dari 2																																																																																																																				
Nama	Taufiqurrahman, S.Si.	Tanggal dibuat	Satu Kali AK = 0,155																																																																																																																				
NIP	198904272018021001	5 Mei 2020																																																																																																																					
Pangkat/Golongan	Penata Muda / III/a																																																																																																																						
Jabatan Fungsional	Pranata Komputer Ahli Pertama																																																																																																																						
Lokasi Pengerjaan	Lab Malware, Gd. Sutan Sjahrir Pushansiber																																																																																																																						
Nama Kegiatan : MELAKSANAKAN DUPLIKASI DATABASE																																																																																																																							
TUJUAN DUPLIKASI																																																																																																																							
<ul style="list-style-type: none"> • <i>Back-up</i> bulanan diperlukan untuk mengamankan data <i>signature</i> ancaman siber dan dokumen laporan terkait penanganan ancaman siber yang terdeteksi pada sensor dan <i>IDS (Intrusion Detection System)</i> yang ada di Pushansiber. • Selain itu data dan dokumen yang telah lampau dapat diarsipkan guna menyediakan area kosong untuk data dan dokumen yang baru 																																																																																																																							
NAMA, BESARAN DAN STRUKTUR DATABASE																																																																																																																							
DBMS : MariaDB 10.4.11 Database : wikisignature Jenis File Backup : SQL dan JSON Besaran data : SQL (421 KB), JSON (18,4 MB) Media Penyimpanan : Hardrive External Struktur Data : <div style="margin-top: 10px;"> <p>wiki_signature</p> <table border="1"> <thead> <tr> <th>Column</th> <th>Type</th> <th>Null</th> <th>Default</th> <th>Links to</th> <th>Comments</th> <th>Media (MIME) type</th> </tr> </thead> <tbody> <tr> <td>id_report (<i>Primary</i>)</td> <td>int(11)</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>date_crated</td> <td>timestamp</td> <td>No</td> <td>current_timestamp()</td> <td></td> <td></td> <td></td> </tr> <tr> <td>date_updated</td> <td>timestamp</td> <td>No</td> <td>current_timestamp()</td> <td></td> <td></td> <td></td> </tr> <tr> <td>document</td> <td>varchar(100)</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>report_date</td> <td>varchar(100)</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>signature_name</td> <td>varchar(255)</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>location</td> <td>varchar(100)</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>ip_source</td> <td>varchar(100)</td> <td>No</td> <td>n/a</td> <td></td> <td></td> <td></td> </tr> <tr> <td>geo_source</td> <td>varchar(100)</td> <td>No</td> <td>n/a</td> <td></td> <td></td> <td></td> </tr> <tr> <td>ip_destination</td> <td>varchar(100)</td> <td>No</td> <td>n/a</td> <td></td> <td></td> <td></td> </tr> <tr> <td>geo_destination</td> <td>varchar(100)</td> <td>No</td> <td>n/a</td> <td></td> <td></td> <td></td> </tr> <tr> <td>analysis</td> <td>text</td> <td>No</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>contributor</td> <td>varchar(100)</td> <td>No</td> <td>Admin</td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <p>Indexes</p> <table border="1"> <thead> <tr> <th>Keyname</th> <th>Type</th> <th>Unique</th> <th>Packed</th> <th>Column</th> <th>Cardinality</th> <th>Collation</th> <th>Null</th> <th>Comment</th> </tr> </thead> <tbody> <tr> <td>PRIMARY</td> <td>BTREE</td> <td>Yes</td> <td>No</td> <td>id_report</td> <td>943</td> <td>A</td> <td>No</td> <td></td> </tr> </tbody> </table> </div>				Column	Type	Null	Default	Links to	Comments	Media (MIME) type	id_report (<i>Primary</i>)	int(11)	No					date_crated	timestamp	No	current_timestamp()				date_updated	timestamp	No	current_timestamp()				document	varchar(100)	No					report_date	varchar(100)	No					signature_name	varchar(255)	No					location	varchar(100)	No					ip_source	varchar(100)	No	n/a				geo_source	varchar(100)	No	n/a				ip_destination	varchar(100)	No	n/a				geo_destination	varchar(100)	No	n/a				analysis	text	No					contributor	varchar(100)	No	Admin				Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment	PRIMARY	BTREE	Yes	No	id_report	943	A	No	
Column	Type	Null	Default	Links to	Comments	Media (MIME) type																																																																																																																	
id_report (<i>Primary</i>)	int(11)	No																																																																																																																					
date_crated	timestamp	No	current_timestamp()																																																																																																																				
date_updated	timestamp	No	current_timestamp()																																																																																																																				
document	varchar(100)	No																																																																																																																					
report_date	varchar(100)	No																																																																																																																					
signature_name	varchar(255)	No																																																																																																																					
location	varchar(100)	No																																																																																																																					
ip_source	varchar(100)	No	n/a																																																																																																																				
geo_source	varchar(100)	No	n/a																																																																																																																				
ip_destination	varchar(100)	No	n/a																																																																																																																				
geo_destination	varchar(100)	No	n/a																																																																																																																				
analysis	text	No																																																																																																																					
contributor	varchar(100)	No	Admin																																																																																																																				
Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment																																																																																																															
PRIMARY	BTREE	Yes	No	id_report	943	A	No																																																																																																																
TANGGAL DAN LAMA Pengerjaan																																																																																																																							
5 Mei 2020, ± 1 Jam Pengerjaan																																																																																																																							

DOKUMENTASI Pengerjaan

1. Melakukan export database melalui fitur phpmyadmin. Hasil export berupa file .sql



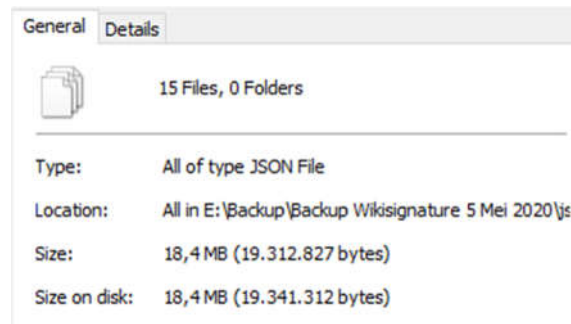
2. Melakukan duplikasi dokumen yang terdapat pada sistem untuk *back-up* data dan asset menggunakan filezilla



3. Hasil backup berupa file .sql yang menampung data dari database dan file JSON yang merupakan dokumen/asset dari sistem. Back-up ini disimpan dalam Hardisk External dan diberi penamaan sesuai dengan tanggal back-up dan nama sistem.

Name	Date modified	Type	Size
2020-05-06 Backup Wikisignature.sql	05/05/2020 10:37	SQL File	421 KB

Gambar 1 backup sql



Gambar 2 back-up JSON

Mengetahui
Kasubbid Kam Aplikasi Bid Jamkam,

Eko Joko Murwanto, S.Kom., M.Si.
Pembina IV/a NIP. 197505252001121001

Jakarta, 6 Mei 2020
Pranata Komputer Ahli Pertama

Taufiqurrahman, S.Si.
Penata Muda III/a NIP.198904272018021001