Mengurai Kesamaan IP Address sebagai Alat Bukti Persaingan Tidak Sehat

Disusun oleh : Samsul, S.Sos, SCM. Cert. (ITC)

I. PENDAHULUAN

Diskusi tentang kesamaan IP Address yang digunakan sebagai salah satu penentu indikasi terjadinya persaingan tidak sehat dalam proses pemilihan penyedia barang/jasa pemerintah (PBJP) masih menjadi momok bagi kelompok kerja pemilihan pengadaan barang/jasa pemerintah.

Ditambah lagi dengan amplifikasi dalam ruang dengar publik terkait "kesamaan IP Addres" terdapat dalam setiap petunjuk lembaga resmi pemerintah dari sisi pengawasan, pemeriksaan, penyelidikan bahkan penyidikan. Ini memperkuat sangkaan bahwa jika terjadi atau ditemukan kesamaan IP Address antar peserta pemilihan maka secara otomatis proses pemilihan telah terjadi persaingan tidak sehat.

Stigma ini perlu didudukan dalam porsi yang adil dan berimbang. Hal ini penting agar pelaksana pengadaan barang/jasa pemerintah tidak diliputi ketakutan atas sesuatu yang diluar kendalinya. Disisi lain juga tidak membuat oknum-oknum merasa bebas melakukan praktik-praktik curang untuk mencapai tujuan jahatnya.

Implikasi lain dari amplifikasi "kesamaan IP Addres" adalah ketakutan pihak penandatangan kontrak, PA/KPA/PPK, melakukan perikatan. Hal ini didasari pada ketakutan akan status hukum dari kontrak yang terjadi apabila melanggar asas obyektif berkontrak karena peristiwa pelanggaran hukum akibat persaingan tidak sehat. Ketakutan ini tidak bisa diabaikan tentunya karena ada implikasi lain setelahnya, terutama potensi kerugian negara hingga kerugian keuangan negara.

Untuk itu kesamaan IP Address antar peserta pemilihan penyedia dalam pengadaan secara elektronik dikaitkan dengan persaingan tidak sehat menjadi sangat penting untuk dibahas dalam berbagai perspektif.

Semoga perspektif yang diurai dalam artikel ini dapat menjadi khazanah yang memperkaya kamus obyektifitas semua pihak dalam memandang fenomena kesamaan IP Address antar peserta pemilihan penyedia pengadaan barang/jasa pemerintah.

II. PERMASALAHAN

Permasalahan mendasar dari fenomena kesamaan IP Address adalah pertanyaan tentang :

1. Apakah benar kesamaan IP Address antar peserta pemilihan penyedia PBJP adalah indikasi dari persaingan yang tidak sehat?
2. Apakah benar kesamaan IP Address antar peserta pemilihan penyedia PBJP berakibat pada status hukum perikatan?
3. Apakah benar jika ditemukan kesamaan IP Address antar peserta pemilihan penyedia PBJP pasti melibatkan pelaksana pengadaan barang/jasa?

III. PEMBAHASAN

1. IP Address dalam Forensik Digital

Sebelum membahas terkait dengan IP Address mungkin perlu terelebih dahulu kita mengetahui bersama sebuah cabang keilmuan dalam pembuktian berbasis digital yaitu Forensik Digital (Digital Forensic).

Ilmu forensik adalah ilmu yang digunakan untuk tujuan hukum, bersifat tidak memihak yang merupakan bukti ilmiah untuk digunakan dalam kepentingan peradilan dan penyelidikan. Forensik digital merupakan salah satu cabang dari ilmu forensik, terutama untuk menyelidiki dan memulihkan konten perangkat digital,[1] berkaitan dengan bukti legal yang terdapat pada perangkat komputer dan media penyimpanan digital lainnya sebagai bukti-bukti digital yang digunakan dalam kejahatan komputer dan dunia maya.[2] Forensik digital diperlukan karena biasanya data di perangkat target dikunci, dihapus, atau disembunyikan.[3]

Forensik digital adalah ilmu yang menganalisis barang bukti digital sehingga dapat dipertanggungjawabkan di pengadilan.[4] Istilah forensik digital pada awalnya identik dengan forensik komputer tetapi definisinya telah diperluas hingga mencakup forensik semua teknologi digital. Sedangkan forensik komputer didefinisikan sebagai "kumpulan teknik dan alat yang digunakan untuk menemukan

---

[1] Reith, Mark; Carr, Clint & Gunsch, Gregg (2002). "An examination of digital forensic models". *International Journal of Digital Evidence* (dalam bahasa Inggris).

[2] Meiyanti, Ruci; Ismaniah (2015). "Perkembangan Digital Forensik Saat Ini dan Mendatang". Jurnal Kajian Ilmial UBJ. Jawa Barat: Universitas Bhayangkara Jakarta Raya.

[3] DHS (2016). Digital Forensics Tools (PDF). System Assessment and Validation for Emergency Responders (SAVER). U.S. Department of Homeland Security

[4] Meiyanti, Ruci; Ismaniah (2015). loc. cit.

bukti pada komputer.[5] Landasan forensik digital ialah praktik pengumpulan, analisis, dan pelaporan data digital.[6]

Menurut Meiyanti, Ruci; Ismaniah (2015) forensik digital dapat juga diartikan sebagai pengumpulan dan analisis data dari berbagai sumber daya komputer yang mencakup sistem komputer, jaringan komputer, jalur komunikasi, dan berbagai media penyimpanan yang layak untuk diajukan dalam sidang pengadilan.

Jadi jika dilihat dari sumbernya forensik digital terdiri dari cabang-cabang sebagai berikut:

a. Forensik komputer
b. Forensik peranti bergerak
c. Forensik jaringan
d. Analisis data forensik
e. Forensik basis data

Berkaitan dengan IP Address maka ini termasuk dalam cabang Forensik Jaringan. Forensik jaringan berkaitan dengan pengamatan dan analisis lalu lintas jaringan komputer, baik lokal maupun WAN/internet, untuk keperluan pengumpulan informasi, pengumpulan bukti, atau deteksi intrusi.[7] Tidak seperti forensik digital lainnya data jaringan sering berubah-ubah dan jarang terekam, membuat disiplin ini sering reaksioner. Ini menunjukkan bahwa forensik jaringan sangat memerlukan analisa yang kompleks.

Beberapa jenis peralatan menurut Volonino dan Anzaldua (2008) yang digunakan untuk memahami bagaimana dilakukan Forensik Jaringan, adalah:

1. Router: sebuah computer husus yang bertujuan memindahkan data yang melintasi dua jaringan IP address yang berbeda. Router bekerja pada lapisan tiga dalam model OSI.
2. Switch: computer jaringan yang menggunakan Media Access Control (MAC) identifikasi dari sebuah host pada jaringan untuk memindahkan data dalam jaringan. Switch bekerja pada lapisan tiga dalam model OSI yang merupakan penghubung jaringan multiport untuk menembatani segmen jaringan.

[5] Reith, Mark; Carr, Clint & Gunsch, Gregg (2002). op. cit. hlm. 2
[6] Kavrestad, Joakim (2018). Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications (dalam bahasa Inggris). Springer International Publishing AGw
7 Palmer, Gary, ed. (2001). A Road Map for Digital Forensic Research (PDF). Report From the First Digital Forensic Research Workshop (DFRWS) August 7-8, 2001. Utica, New York: Mitre Corporation.

3. Hub: merupakan bagian utama dari jaringan yang berfungsi untuk mengirimkan data yang diterima pada semua port. Perangkat ini bekerja pada layer dua karena tidak ada skema pengalamatan pada lapisan kedua. Sekarang hub jarang digunakan karena cenderung meningkatkan volume traffic dan memeperlambat jaringan sedangkan switch jauh lebih efisien dalam memindahkan data.
4. Network Interface Card (NIC): sebuah peangkat yang terdapat MAC (Media Access Control) yaitu alamat computer yang unik untuk mnegidentifikasi host atau computer. NIC adalah penghubung antara jaringan dan host.
5. Host: perangkat komputasi yang terpasang ke jaringan memiliki alamat IP dan alamat MAC. Computer adalah sebuah host yang memiliki alamat IP dan alamat MAC, juga laptop, PDA, WAP, router, switch, maupun perangkat mobile seperti smartphone, ipod juga telah memiliki alamat IP dan MAC.
6. Media: sebuah bagian dari jaringan yang dapat berbentuk kabel tembaga, kabel serat optic atau gelombang radio. Memungkinkan untuk menghubungkan perangkat ke jaringan dan media yang berbeda juga protokol yang berbeda untuk membantu menciptakan rentang waktu dan data yang dapat mengaitkan tersangka. [8]

Dari 6 jenis peralatan yang disebutkan oleh Volonino dan Anzaldua (2008), IP Address merupakan sebagian alat baca jaringan yang digunakan untuk memahami aliran data. Pada bagian host dijelaskan dengan gamblang bahwa setiap alat tidak hanya dilekatkan alamat IP tapi juga alamat Mac.

Internet Protocol Address (atau disingkat alamat IP) adalah label numerik yang ditetapkan untuk setiap perangkat yang terhubung ke jaringan komputer yang menggunakan Protokol Internet untuk komunikasi.9 Alamat IP memiliki dua fungsi utama: host atau identifikasi antarmuka jaringan dan pengalamatan lokasi.

Alamat IP ditetapkan untuk host baik secara dinamis, oleh protokol yang disebut DHCP, saat mereka bergabung dengan jaringan, atau secara statis mengikat pada konfigurasi perangkat keras atau perangkat lunak host.

MAC Address (Media Access Control Address) atau alamat MAC adalah merupakan alamat yang unik yang mengidentifikasikan sebuah komputer atau

[8] Volonino, Linda & Anzaldua, Reynaldo (2008). Computer forensics for dummies
[9] Postel, J. "Internet Protocol". tools.ietf.org

interface dalam jaringan. MAC Address juga sering disebut sebagai Ethernet address, physical address, atau hardware address.

Secara sederhana setiap perangkat keras memiliki alamat MAC dan ketika terkoneksi jaringan sekaligus mendapatkan alamat IP agar dapat mengalirkan data ke dalam jaringan. Sehingga dalam kondisi standar/umum satu alamat MAC bisa saja terlacak menggunakan beberapa IP Address, demikian juga beberapa MAC bisa saja terlacak menggunakan satu IP Address yang sama dalam waktu yang berbeda.

Misal dalam konfigurasi IP Dinamis, jika diakses dalam waktu yang berbeda dapat saja memberikan IP yang sama pada beberapa perangkat dengan alamat MAC yang berbeda. IP Dinamis adalah pemberian IP address secara dinamis atau acak berdasarkan urutan akses. Dengan demikian IP yang sama meski sudah diberikan kepada client tertentu, dapat saja diberikan pada client lain pada waktu yang berbeda, jika sudah tidak terpakai lagi. Maka dari itu dalam log system akan tercatat penggunaan IP yang sama.

Satu IP Publik yang sama bisa diakses secara bersama-sama oleh banyak client dengan berbeda IP Address, namun dalam record log system yang tercatat adalah 1 IP Publik. Tipologi ini biasa dipakai pada ruang publik atau hotspot atau bidding room.[10]

Dengan demikian kemungkinan kesamaan IP Address bukanlah sebuah hal yang mustahil dan unik sehingga tidak dapat langsung digunakan sebagai sebuah alat bukti peristiwa tertentu, apalagi peristiwa hukum. Bahkan secara normal IP Address tidak dapat berdiri sendiri untuk mengidentifikasi bukti fisik perangkat dia harus disandingkan dengan Mac Address.

Dalam merekonstruksi adanya kesamaan sumber dari beberapa input data berbeda, dalam hal ini file penawaran dari beberapa peserta, pada Sistem Pengadaan Secara Electronic (SPSE) paling tidak harus mengetahui kesamaan kombinasi antara Mac Address dan IP Address. Dengan demikian informasi IP address yang terekam dalam *log system* belum cukup aman dan andal dijadikan dasar bukti permulaan yang sah tentang adanya indikasi persaingan tidak sehat.

[10] https://samsulramli.net/2016/08/30/pokja-galau-karena-ip-addres/

2. IP Address sebagai Alat Bukti

Pasal 5 ayat (1) Undang-Undang Nomor 11 Tahun 2008 (11/2008) tentang ITE, meyatakan bahwa "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah". Apa yang dimaksud dengan informasi elektronik tersebut adalah sebagai berikut :

Informasi Elektonik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Pengertian mengenai informasi elektronik tersebut terdapat dalam Pasal 1 angka 1 UU 11/2008. Dijelaskan bahwa bukti elektronik berupa informasi elektronik. Kemudian Pasal 5 ayat (1) juga menerangkan mengenai dokumen elektronik sebagai alat bukti yang sah.

Pengertian dokumen elektronik menurut Pasal 1 angka 4 UU 11/2008 adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

Akan tetapi, tidak sembarang informasi elektronik dan/atau dokumen elektronik dapat dijadikan alat bukti yang sah. Menurut Undang-Undang Nomor 11 Tahun 2008 tersebut, suatu informasi elektronik/dokumen elektronik dinyatakan sah untuk dijadikan alat bukti apabila menggunakan sistem elektronik yang sesuai dengan ketentuan yang diatur dalam Undang-Undang Nomor 11 Tahun 2008 yaitu sistem elektronik yang andal dan aman, serta memenuhi persyaratan minimum sebagai berikut:

1. Dapat menampilkan kembali informasi elektronik dan/atau dokumen elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan Perundang-undangan;

2. Dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan informasi elektronik dalam penyelenggaraan sistem elektronik tersebut;
3. Dapat beroperasi sesuai dengan prosedur atau petunjuk dalam penyelenggaraan sistem elektronik tersebut;
4. Dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan penyelenggaraan sistem elektronik tersebut; dan
5. Memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

Dihubungkan dengan kekuatan IP Address sebagai informasi elektronik sebagai alat bukti KUHAP Pasal 184 dapat diimplementasikan penggunaanya dalam pemeriksaan perkara cyber crime, diantaranya sebagai berikut : [11]

1. Keterangan saksi

Berkenaan dengan sifat cyber crime yang virtual dan biasanya pelaku melakukan aksinya seorang diri, maka pembuktian dengan menggunakan keterangan saksi tidak dapat diperoleh secara langsung. Keterangan saksi hanya dapat berupa hasil pembicaraan atau hanya mendengar dari orang lain. Kesaksian ini dikenal sebagai testimonium de auditum atau hearsay evidence. Meskipun kesaksian sejenis ini tidak diperkenankan sebagai alat bukti, akan tetapi dalam praktiknya tetap dapat dipergunakan sebagai bahan pertimbangan bagi hakim untuk memperkuat keyakinannya sebelum menjatuhkan putusan.

Kemungkinan yang dapat dijadikan keterangan saksi ialah melalui hasil interaksi di dalam dunia cyber, seperti chatting dan e-mail antara pengguna internet atau juga dapat melalui keterangan seorang administrator sistem komputer yang telah disertifikasi oleh Penyelenggara Sertifikasi Elektronik adalah badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat Elektronik sebagaimana ketentuan Pasal 1 angka 10 UU 11/2008.

2. Keterangan ahli

[11] Arif Mansyur M, Dikdik dan Elisatris Gultom, 2005, Cyber Law: Aspek Hukum Teknologi Informasi, Bandung: PT. Refika Aditama

Keterangan ahli menjadi signifikan penggunaannya apabila jaksa mengajukan alat bukti elektronik untuk membuktikan kesalahan pelaku cyber crime. Peran keterangan ahli disini adalah untuk memberikan suatu penjelasan di dalam persidangan bahwa dokumen/data elektronik yang diajukan adalah sah dan dapat dipertanggungjawabkan secara hukum.

Peranan seorang ahli dalam cyber crime merupakan sesuatu yang tidak bisa ditawar-tawar lagi mengingat pembuktian dengan alat bukti elektronik masih sangat riskan penggunaannya di depan sidang pengadilan.

Kedudukan seorang Ahli sebagai *Testamentary Evidence* ini sangat penting untuk memperjelas kejahatan dunia maya yang terjadi serta dapat menerangkan/menjelaskan validitas suatu Bukti Elektronik yang memberikan keyakinan Hakim dalam memutus perkara kejahatan dunia maya.

Apa yang diurai oleh Arif Mansyur M, Dikdik dan Elisatris Gultom, 2005 juga diamini dalam kesimpulan penelitian M. Yustia A,[12] yang menyebutkan bahwa Keterangan ahli telematika dalam proses pemeriksaan perkara tindak pidana mayantara, baik pada tahap pemeriksaan penyidikan maupun pada pemeriksaan disidang pengadilan sangat penting dan dibutuhkan, terutama untuk membantu penyidik, penuntut umum ataupun hakim dalam mengungkapkan suatu kasus kejahatan mayantara (*Cyber Crime*) yang sangat rumit, kompleks yang bersifat spesifik.

Dari apa yang diuraikan sangat tegas dan jelas bahwa IP Address adalah salah satu informasi elektronik yang dapat dijadikan alat bukti. Namun demikian tidak sembarang informasi elektronik dan/atau dokumen elektronik dapat dijadikan alat bukti yang sah harus melalui serangkaian proses yang menjamin keandalan dan keamanan informasi. Keandalan dan keamanan informasi elektronik dijamin dengan sertifikasi elektronik yang diterbitkan oleh penyelenggara sertifikasi elektronik sesuai dengan UU 11/2008. Keabsahan informasi elektronik sebagai alat bukti harus berdasarkan keterangan ahli yang tersertifikasi.

[12] M. Yustia A, 2010, Pembuktian dalam Hukum Pidana Indonesia terhadap Cyber Crime, Fakultas Hukum Universitas Bengkulu, Jurnal Pranata Hukum Vol 5.

3. IP Address dalam Pedoman Audit dan Investigasi

Pertanyaan ikutan yang kemudian mengemuka adalah kenapa dalam setiap dokumen petunjuk pemeriksaan dan investigasi yang dikeluarkan lembaga pengawasan, pemeriksa maupun hukum, selalu menempatkan "kesamaan IP Address" sebagai prosedur baku yang harus diperiksa.

Lampiran II Peraturan Badan Pengawasan Keuangan Dan Pembangunan Republik Indonesia (BPKP-RI) Nomor 3 Tahun 2019 Tentang Pedoman Pengawasan Intern Atas Pengadaan Barang/Jasa Pemerintah, Pedoman Probity Audit, Bagian IV Audit atas pemilihan penyedia barang/jasa menyebutkan salah satu titik kritis yang harus diperhatikan adalah: ***"Beberapa calon penyedia memasukkan dokumen penawaran melalui IP address yang sama".***

Keberadaan klausul "kesamaan IP Address" dalam pedoman BPKP ini harus dipahami sebagai bagian dari tindakan *preventif* dan berada dalam domain *probity audit. Probity* Audit adalah audit selama proses pengadaan barang/jasa berlangsung (real time audit) dengan mendasarkan pada prinsip-prinsip *probity*. Prinsip-prinsip probity yang dimaksud adalah prinsip penegakan integritas, kebenaran, dan kejujuran dan memenuhi ketentuan perundangan berlaku yang bertujuan meningkatkan akuntabilitas penggunaan dana sektor publik. [13]

Hal mendasari diterbitkannya pedoman *probity* audit yaitu untuk mendorong peran dan fungsi APIP dalam *Prevent, Deter dan Detect* sebagai *Early Warning System* atas proses pengadaan barang dan jasa; serta dalam rangka peningkatan kualitas akuntabilitas keuangan negara melalui pengelolaan keuangan negara yang efektif, efisien, transparan, dan akuntabel. [14]

Maka sangat beralasan jika kesamaan *IP Address* menjadi mandatori dalam pedoman audit ini. Ditemukannya informasi kesamaan IP Address menjadi peringatan dini dalam rangka melindungi pelaksana pengadaan barang/jasa agar tidak terjebak pada kondisi yang menjurus pada pelanggaran hukum.

Ini pulalah yang mendasari kenapa akses kepada log system yang berisi data IP Address hanya diberikan kepada auditor dan aparat penegak hukum. Bukan

[13] http://www.bpkp.go.id/sakd/konten/1739/Selayang-Pandang-Tentang-Probity-Audit-Pengadaan-Barang-dan-Jasa-Pemerintah.bpkp diakses 25 Januari 2021.
[14] Ibid.

kepada Pokja, PPK, PA atau KPA. Independensi informasi diserahkan kepada pihak-pihak yang tidak terlibat langsung dalam proses pemilihan penyedia.

Penemuan kesamaan IP Address antar peserta pemilihan menjadi beban kerja bagi auditor untuk menemukan tanda-tanda lain hingga sampai pada kesimpulan adanya indikasi persaingan tidak sehat. Bahkan auditor pada tahap awal dapat melibatkan tenaga ahli forensik digital untuk memperkuat indikasi bahwa tidak terjadi atau terjadi peristiwa persaingan tidak sehat.

Berkaca, misalnya, dari putusan Komisi Pengawas Persaingan Usaha Republik Indonesia (KPPU) Perkara Nomor 04/KPPU-L/2018 yang sudah berkekuatan hukum tetap setidaknya disimpulkan bahwa kesamaan IP Address tidak dijadikan satu-satunya alat bukti, namun ada banyak alat bukti lain yang memperkuat putusan adanya persaingan tidak sehat. Alat bukti lain tersebut seperti kesamaan metadata file penawaran, kesamaan header dokumen dan pengakuan dari saksi. Ini menegaskan sekali lagi bahwa kesamaan IP Address bukanlah alat bukti permulaan yang berdiri sendiri.

4. IP Address dan Peran Pokja

Persoalan lain yang juga menjadi kekhawatiran adalah ketakutan pokja dengan dijadikannya kesamaan IP Address sebagai petunjuk dasar audit. Sangat wajar jika personil yang terlibat sebagai Pokja Pemilihan merasa terjebak karena mereka tidak memiliki akses dan kemampuan untuk mendeteksi kesamaan IP Address.

Sejak era Perpres 54/2010 kewenangan mengakses *log system* hanya diberikan kepada pihak selain Pokja Pemilihan. Sebagaimana tertuang dalam Lampiran Perka 1/2015 tentang e-Tendering Bagian III kewenangan mengakses log system pada SPSE hanya diberikan kepada auditor.

Dengan demikian pertanggungjawaban atas temuan kesamaan IP Address tidak dapat dibebankan kepada Pokja pemilihan. Justru temuan auditor tentang kesamaan IP Address akan sangat membantu Pokja pemilihan dalam menjalankan tugas menetapkan pemenang jika ditemukan indikasi persekongkolan sebagaimana petunjuk Perlem 9/2018 tentang Pengadaan Melalui Penyedia bahwa Indikasi persekongkolan antar Penyedia harus dipenuhi sekurang- kurangnya 2 (dua) indikasi di bawah ini:

a. Terdapat kesamaan dokumen teknis, antara lain: metode kerja, bahan, alat, analisa pendekatan teknis, harga satuan, dan/atau spesifkasi barang yang ditawarkan (merk/tipe/jenis) dan/atau dukungan teknis;
b. seluruh penawaran dari Penyedia mendekati HPS;
c. adanya keikutsertaan beberapa Penyedia Barang/Jasa yang berada dalam 1 (satu) kendali;
d. adanya kesamaan/kesalahan isi dokumen penawaran, antara lain kesamaan/kesalahan pengetikan, susunan, dan format penulisan;
e. jaminan penawaran dikeluarkan dari penjamin yang sama dengan nomor seri yang berurutan.

Apabila Pokja menemukan minimal 2 (dua) indikasi tersebut mestinya pemeriksaan kesamaan IP Address dapat dimintakan kepada auditor untuk memperkuat keyakinan Pokja. Hal ini tentu tidak bisa ditemukan pada proses *post audit* sehingga yang paling ideal adalah pada *probity* audit.

Ini juga menegaskan uraian sebelumnya bahwa, kesamaan IP Address adalah mandatori pada pedoman audit pada bagian probity audit, tujuannya justru membantu pelaksana pengadaan barang/jasa seperti Pokja, PPK, PA/KPA dalam rangka *early warning system* apabila ditemukan bukti-bukti permulaan indikasi persekongkolan. Terlebih pada paket-paket strategis yang berkaitan langsung dengan kepentingan masyarakat.

Jika kesamaan IP Address ditempatkan pada post audit untuk menemukan bukti-bukti lain yang memperkuat indikasi maka tidak salah jika banyak pelaku pengadaan yang paranoid terhadap jebakan "kesamaan IP Address".

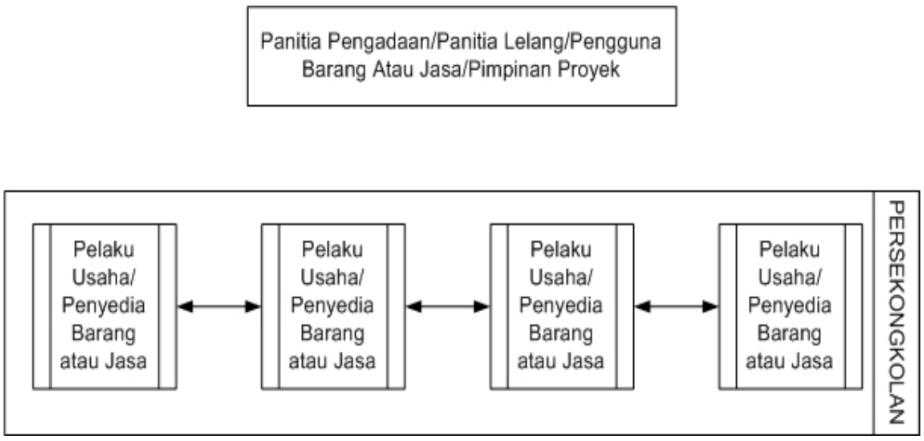
5. IP Address Sebab atau Akibat Persekongkolan

Persekongkolan dalam tender dapat dibedakan pada tiga jenis, yaitu persekongkolan horizontal, persekongkolan vertikal, dan gabungan persekongkolan vertikal dan horizontal. [15]

Persekongkolan Horizontal. Merupakan persekongkolan yang terjadi antara pelaku usaha atau penyedia barang dan jasa dengan sesama pelaku usaha atau

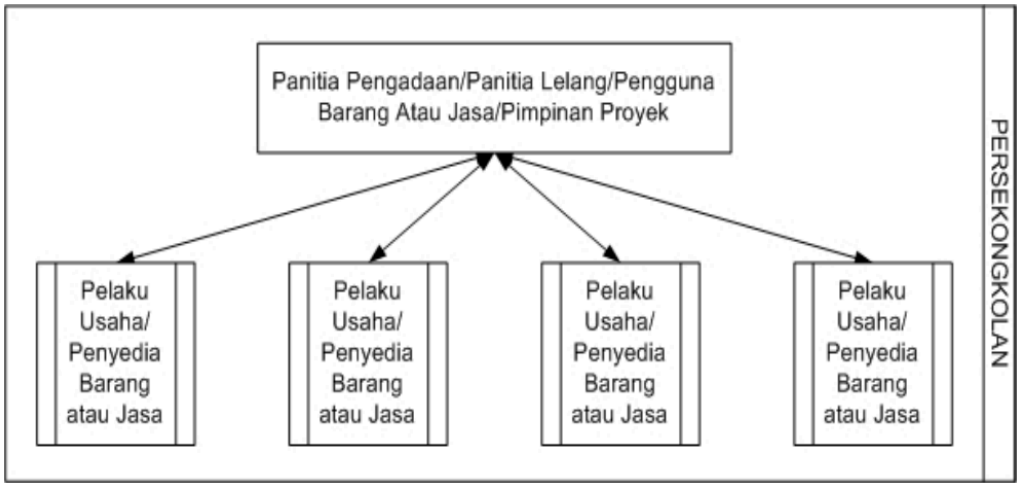
[15] Pedoman Pasal 22 Tentang Larangan Persekongkolan Dalam Tender Berdasarkan Undang-Undang No. 5 Tahun 1999 Tentang Larangan Praktek Monopoli dan Persaingan Usaha Tidak Sehat Komisi Pengawas Persaingan Usaha Republik Indonesia, KPPU, Jakarta, 2009. Hal. 15

penyedia barang dan jasa pesaingnya. Persekongkolan ini dapat dikategorikan sebagai persekongkolan dengan menciptakan persaingan semu di antara peserta tender. [16]



Bagan 1 Skema Persekongkolan Horisontal

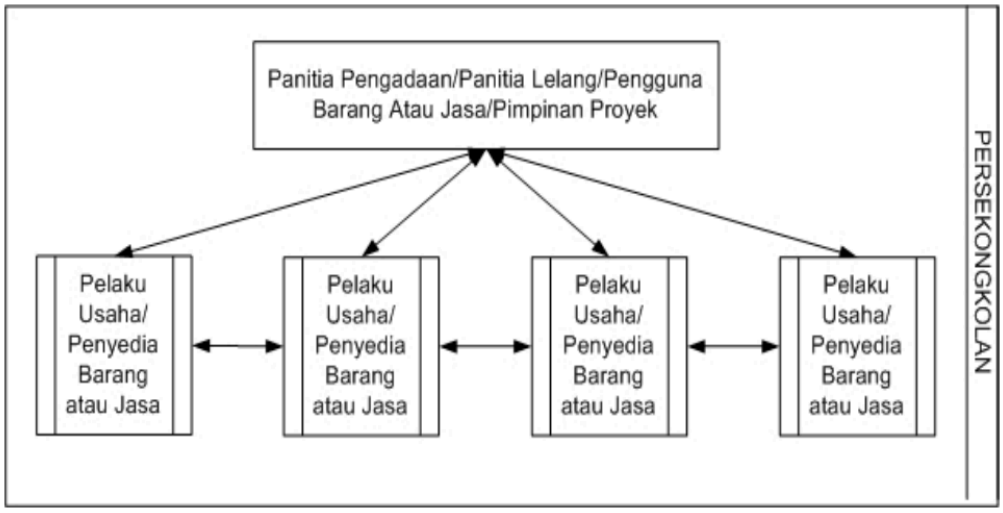
Persekongkolan Vertikal. Merupakan persekongkolan yang terjadi antara salah satu atau beberapa pelaku usaha atau penyedia barang dan jasa dengan panitia tender atau panitia lelang atau pengguna barang dan jasa atau pemilik atau pemberi pekerjaan. Persekongkolan ini dapat terjadi dalam bentuk dimana panitia tender atau panitia lelang atau pengguna barang dan jasa atau pemilik atau pemberi pekerjaan bekerjasama dengan salah satu atau beberapa peserta tender. [17]



Bagan 2 Skema Persekongkolan Vertikal

[16] ibid. hal 16
[17] ibid. hal 16

Persekongkolan Horizontal dan Vertikal. Merupakan persekongkolan antara panitia tender atau panitia lelang atau pengguna barang dan jasa atau pemilik atau pemberi pekerjaan dengan pelaku usaha atau penyedia barang dan jasa. Persekongkolan ini dapat melibatkan dua atau tiga pihak yang terkait dalam proses tender. Salah satu bentuk persekongkolan ini adalah tender fiktif, dimana baik panitia tender, pemberi pekerjaan, maupun para pelaku usaha melakukan suatu proses tender hanya secara administratif dan tertutup. [18]



Bagan 3 Skema Persekongkolan Horisontal dan Vertikal

Kegunaan temuan "Kesamaan IP Address" salah satunya adalah mengantisipasi terjadinya persaingan usaha yang tidak sehat. Dan ini menjadi tugas Pokja, PPK dan PA/KPA dalam menjalankan tugasnya. Bukan sebaliknya digunakan untuk menciptakan *barrier* dalam proses pengadaan barang/jasa pemerintah. Hal ini terlihat jelas dalam konsepsi yang diatur dalam Perpres 16/2018 pasal 51 ayat 2 yang menyatakan bahwa **Tender/Seleksi gagal** dalam hal diantaranya terjadi seluruh peserta terlibat Korupsi, Kolusi, dan Nepotisme (KKN) seluruh peserta terlibat persaingan usaha tidak sehat, seluruh penawaran harga Tender Barang/ Pekerjaan Konstruksi/Jasa Lainnya di atas HPS, dan/atau KKN melibatkan Pokja Pemilihan/PPK.

Jelas sekali indikasi persekongkolan dititipkan utamanya pada area proses tender agar sejak dini diantisipasi oleh semua pihak yang terlibat. Pokja hanya bisa mengidentifikasi persekongkolan horisontal dari sekurang- kurangnya 2 (dua) indikasi di bawah ini:

[18] ibid. hal 17

a. Terdapat kesamaan dokumen teknis, antara lain: metode kerja, bahan, alat, analisa pendekatan teknis, harga satuan, dan/atau spesifkasi barang yang ditawarkan (merk/tipe/jenis) dan/atau dukungan teknis;
b. seluruh penawaran dari Penyedia mendekati HPS;
c. adanya keikutsertaan beberapa Penyedia Barang/Jasa yang berada dalam 1 (satu) kendali;
d. adanya kesamaan/kesalahan isi dokumen penawaran, antara lain kesamaan/kesalahan pengetikan, susunan, dan format penulisan;
e. jaminan penawaran dikeluarkan dari penjamin yang sama dengan nomor seri yang berurutan.

Begitu Pokja menemukan indikasi sebagaimana disebutkan di atas, maka informasi kesamaan IP Address akan sangat membantu menambah keyakinan Pokja untuk melakukan tindakan selanjutnya termasuk menggagalkan pemilihan sebagaimana petunjuk pasal 51 Perpres 16/2018.

Temuan kesamaan IP Address oleh auditor semestinya untuk memperkuat putusan pokja. Bahkan informasi IP Address juga dapat digunakan APIP memperkuat putusan PA dalam penetapan daftar hitam. Sebagaimana diatur dalam Perlem 17/2018 tentang penetapan sanksi daftar hitam.

Jika kita cermati bersama, Perpres 16/2018 alurnya sangat jelas. Bahwa jika ditemukan indikasi penyimpangan maka melalui APIP dilakukan pemeriksaan. Dalam proses pemeriksaan, jika menemukan kesamaan IP Address misalnya, auditor dapat menemui Pokja/PPK/PA/KPA untuk memperoleh informasi lebih jauh.

Hasil tindak lanjut yang dilakukan oleh APIP, dilaporkan kepada Menteri/Pimpinan Lembaga/Kepala Daerah/Pimpinan institusi. Jika disetujui hasil temuan diyakini terdapat indikasi KKN yang akan merugikan keuangan negara, dapat dilaporkan kepada instansi yang berwenang dengan tembusan kepada LKPP dan BPKP. Jika ditemukan beberapa indikasi kuat adanya persekongkolan horisontal maka dapat dilaporkan kepada KPPU.

Sederhananya bukan karena kesamaan IP Address kemudian disebut persekongkolan. Tapi karena ditemukan indikasi persekongkolan maka ditemukan kesamaan IP Address. Kesamaan IP Address pada tahap awal adalah akibat bukan sebab.

Indikasi Persekongkolan yang ditemukan pada saat proses pemilihan sangat terbantu dengan penguatan informasi kesamaan IP Address untuk melanjutkan proses atau menghentikan proses.

Akibat ditemukannya indikasi oleh Pokja/PPK/PA/KPA, baik dari proses pemilihan atau informasi pihak luar, maka diperkuat dengan ditemukan kesamaan IP Address. Sehingga menjdi beralasan Pasal 77 Perpres 16/2018 mengamanatkan apabila ada pengaduan dalam proses pemilihan penyedia disalurkan melalui APIP terlebih dahulu untuk diklarifikasi kepada pelaksana pengadaan. Hasil klarifikasi dilakukan *cross check* secara keahlian melalui forensik digital terkhusus forensik jaringan. Semakin dini temuan dikuatkan maka penanganan dalam proses pengadaan semakin efektif dan efisien.

Dalam kacamata Pasal 22 UU 5/1999 tentang Larangan Praktek Monopoli dan Persaingan Usaha Tidak Sehat, jika benar ditemukan persekongkolan horisontal yang diperkuat dengan kesamaan IP address, maka konsekwensi hukum mengikat kepada pelaku kejahatan yaitu penyedia yang bersekongkol. Jika demikian Pokja semestinya tidak ikut dipersalahkan justru juga adalah korban.

Sesuai amanat UU 5/1999 pula yang berhak menetapkan sanksi adalah Komisi Pengawas Persaingan Usaha (KPPU). Untuk itu jawaban tentang apakah ada pengenaan sanksi pidana terhadap pelaksana pengadaan? Selama tidak ada persekongkolan vertikal yang bertujuan sengaja memperkaya diri dan orang lain maka masih wilayah hukum administrasi.

Sebagaimana penegasan KPPU, dalam Pedoman Pasal 22 Tentang Larangan Persekongkolan Dalam Tender, terhadap persekongkolan dalam tender yang melibatkan Pegawai atau Pejabat Pemerintah (PNS atau yang diperbantukan pada BUMN, BUMD, atau Swasta), maka untuk menegakkan hukum persaingan, KPPU menyampaikan informasi tentang persekongkolan tersebut kepada atasan Pegawai atau Pejabat bersangkutan atau Kejaksaan, maupun Komisi Pemberantasan Korupsi (KPK), untuk mengambil tindakan hukum sesuai dengan peraturan perundangundangan yang berlaku.

IV. KESIMPULAN

Dari uraian pada bagian pembahasan maka dapat diambil beberapa kesimpulan untuk menjawab permasalahan yang mengemuka terkait Kesamaan IP Address sebagai berikut:

1. Kesamaan IP Address bukanlah sebuah hal yang mustahil dan unik sehingga tidak dapat langsung digunakan sebagai sebuah alat bukti peristiwa tertentu, apalagi peristiwa hukum. Dengan demikian informasi IP address yang terekam dalam *log system* belum cukup lengkap untuk dijadikan bukti permulaan yang cukup tentang adanya indikasi persaingan tidak sehat apalagi dijadikan dasar untuk menghentikan proses pengadaan barang/jasa.
2. Untuk menetapkan kesamaan IP Address sebagai alat bukti hukum yang sah harus melibatkan ahli yang tersertifikasi oleh penyelenggaran sertifikasi elektronik sesuai ketentuan UU 11/2008.
3. Kesamaan IP Address termuat dalam pedoman legal formal lembaga pengawas/pemeriksa/penegakan hukum tidak menjadi patokan tentang bobot indikasi persekongkolan. Justru Kesamaan IP Address berfungsi sebagai salah satu alat untuk mendorong peran dan fungsi APIP dalam *Prevent, Deter dan Detect* sebagai Early Warning System atas proses pengadaan barang dan jasa yang dikenal dengan *probity audit*.
4. Kesamaan IP Address adalah mandatori pada pedoman *probity audit*, tujuannya justru membantu pelaksana pengadaan barang/jasa seperti Pokja, PPK, PA/KPA dalam rangka *early warning system* apabila ditemukan bukti-bukti permulaan indikasi persekongkolan. Terlebih pada paket-paket strategis yang berkaitan langsung dengan kepentingan masyarakat.
5. Kesamaan IP Address adalah akibat bukan sebab. Akibat ditemukannya indikasi oleh Pokja/PPK/PA/KPA baik dari proses pemilihan maupun dari informasi pihak luar maka diperkuat dengan ditemukan kesamaan IP Address.
6. Terbuktinya peristiwa persekongkolan horisontal dalam proses pemilihan yang diperkuat oleh temuan kesamaan IP Address ditetapkan oleh KPPU sebagai lembaga yang berwenang. Jika terdapat persekongkolan vertikal baru dilanjutkan kepada instansi hukum yang berwenang.

V. SARAN

Menyikapi item-item kesimpulan tersebut maka penulis dapat menyampaikan saran-saran sebagai berikut :

1. Pemeriksaan Kesamaan IP Address tidak lagi digunakan sebagai alat menakut-nakuti pelaksana pengadaan namun justru diperbesar manfaatnya dalam rangka mendukung keyakinan pokja dan PPK dalam mengambil putusan dalam proses pengadaan barang/jasa, salah satunya menempatkan pada *probity audit* bukan *post audit*.
2. Kesamaan IP Address tidak lagi digunakan sebagai alasan untuk serta merta menghentikan proses, apalagi sampai menunda penandatanganan kontrak yang pada akhirnya mengganggu pencapaian target pembangunan dan pelayanan kepada masyarakat.
3. Dalam hal terjadi kesamaan IP Address antar peserta tender yang mengakibatkan persaingan usaha tidak sehat maka pelaksana pengadaan harus diposisikan sebagai korban selama tidak ada bukti kuat dan nyata keterlibatannya dalam persekongkolan.