# BAB IV

# ANALISIS DATA

Hasil penelitian yang didapat oleh peneliti pada saat melakukan penelitian di Subdirektorat V Unit Siber POLDA NTT beserta data yang dilampirkan dan digambarkan pada BAB III, ditemukan bahwa :

Pada *tabel 3* tahun 2016 - 2018 terdapat 27 kasus yang ditangani oleh penyidik siber tetapi, hanya 10 kasus yang dilimpahkan ke Kejaksaan (P21), 7 kasus lain yang sementara disidik harus ditutup karena korban atau pelapor menarik laporannya dengan alasan telah berdamai dengan pelaku. Hal tersebut bisa saja terjadi karena kasus yang ditarik oleh pelapor atau korban merupakan Pasal 27 ayat (3) Undang-Undang ITE dimana delik yang terdapat pada pasal ini merupakan delik laporan atau aduan bukan delik biasa.

Pada *tabel 4*, selain 7 kasus yang ditutup karena laporan ditarik oleh pelapor atau korban, 5 kasus penyebaran berita bohong (hoaks) di SP3 karena bukan merupakan tindak pidana siber (pelaku menggunakan SMS / *Short Message Service*) dimana SMS bukan merupakan media sosial, sehingga kasus tersebut merupakan tindak pidana biasa bukan tindak pidana siber dan 5 kasus lain di SP3 karena tidak memiliki alat bukti yang cukup karena setelah dilakukan pemeriksaan profilling penyebar, ternyata akun yang digunakan pelaku merupakan akun anonymous (akun palsu). Seingga yang bisa dilakukan oleh

penyidik siber adalah menonaktifkan atau melakukan takedown terhadap akun tersebut agar tidak bisa digunakan lagi oleh pelaku.

Pada *tabel 5*, kasus-kasus yang ditangani oleh Subdirektorat V Unit Siber POLDA NTT semuanya mengunakan media sosial *Facebook*. Sedangkan untuk media sosial lainnya seperti *twitter, what's up, instagram* dan *line* belum ditemukan karena belum ada laporan yang masuk ke bagian Subdirektorat V Unit Siber POLDA NTT.

*Tabel 6*

**PENGHITUNGAN CLEARANCE RATE**

| TAHUN | KASUS | P21 |
|---|---|---|
| **2016** | 11 | 4 |
| **2017** | 10 | 2 |
| **2018** | 6 | 4 |
| **Jumlah** | **27** | **10** |

Pada *tabel 6*, jumlah kasus yang dilimpahkan ke Kejaksaan tidak sesuai dengan jumlah kasus yang ditangani, dimana hanya 10 kasus dari 27 kasus dalam kurun waktu 3 tiga tahun yaitu tahun 2016 sampai 2018 yang dilimpahkan ke Kejaksaan Negeri.

Terlepas dari 7 kasus yang ditarik oleh pelapor atau korban *(Tabel 3)*, jika dikaitkan dengan teori *Clearence Rate* (jumlah kasus yang ditangani apakah

sama dengan jumlah kasus yang diselesaikan) maka penyidik siber sudah menjalankan perannya dengan baik karena jumlah kasus yang diselesaikan atau di P21 sudah mencapai setengah dari kasus yang diterima. Ditambah lagi data pada *tabel 4*, penyidik siber sudah menjalankan perannya sesuai Standar Operasional Prosedur (SOP), dimana dalam *tabel 4* menerangkan bahwa penyidik siber tidak melewatkan satu tahap pun dalam menjalankan perannya sebagai penyidik siber.

Berikut adalah proses penanganan yang dilakukan penyidik siber dalam penyidikan tindak pidana penyebaran berita bohong (hoaks) melalui media sosial setelah menerima laporan atau aduan dari masyarakat :

1. **Membuat tanda terima**

   Setelah laporan atau aduan masuk, penyidik siber akan membuat Surat Tanda Penerimaan Laporan (STPL) yang berisi identitas lengkap dari pelapor dan jenis berita bohong (hoaks) apa yang dilaporkan. Biasanya laporan yang masuk mengenai berita bohong (hoaks) adalah pencemaran nama baik, penghinaan dan isu SARA.

2. **Membuat BAP awal**

   BAP adalah singkatan dari Berita Acara Pemeriksaan. Jika pelapor merupakan korban dari penyebaran berita bohong (hoaks) biasanya kasus penghinaan atau pencemaran nama baik, maka BAP awal ini merupakan hasil pemeriksaan terhadap pelapor/korban.

**3. Mengajukan ke kasubdit untuk disposisi**

Setelah BAP awal dibuat, penyidik menyerahkan berkas kepada Kepala Subdit V Unit Siber untuk disposisi untuk menentukan apakah kasus tersebut merupakan kasus yang berhubungan dengan tindak pidana siber atau tindak pidana biasa. Jika kasus tersebut merupakan tindak pidana biasa, maka berkas akan dilimpahkan ke bagian tindak pidana biasa. Namun, jika kasus tersebut merupakan tindak pidana Siber, maka kasubdit akan mengembalikan berkas kepada bawahannya agar segera diproses.

**4. Membuat surat perintah tugas (Springas) dan sprin Lidik/Sidik**

Setelah berkas dikembalikan oleh kasubdit, maka penyidik siber segera membuat surat perintah tugas dan surat perintah lidik/sidik yang ditanda tangani oleh kasubdit agar proses penyelidikan bisa dilanjutkan.

**5. Memeriksa profiling penyebar**

Setelah surat perintah tugas dan surat perintah lidik/sidik di tandatangani, penyidik siber langsung memeriksa akun yang diduga menyebarkan berita bohong (hoaks) untuk mendapatkan informasi tentang pelaku melalui akun yang memposting berita bohong (hoaks) di media sosial.

**6. Memeriksa saksi**

Setelah memeriksa akun yang menyebarkan berita bohong (hoaks), penyidik juga memeriksa saksi. Dalam hal ini, biasanya yang menjadi saksi

adalah pelapor itu sendiri. Keterangan saksi akan sangat membantu penyidik dalam menangani kasus tersebut.

**7. Meminta bantuan ahli**

Setelah memeriksa akun penyebar dan saksi, penyidik akan menentukan apakah postingan akun tersebut merupakan tindak pidana biasa atau tindak pidana siber. Jika mengalami kesulitan, penyidik siber bisa meminta bantuan dari ahli ITE, ahli bahasa dan ahli lainnya untuk menganalisa postingan pelaku di media sosial tersebut.

Setelah proses analisa selesai, dan ahli menyatakan bahwa ostingan tersebut merupakan tindak pidana siber, maka penyidik langsung melakukan penangkapan terhadap pelaku.

**8. Melakukan pemeriksaan terhadap perangkat yang digunakan**

Pemeriksaan terhadap perangkat dilakukan oleh penyidik siber setelah pelaku ditangkap. Hal ini biasa disebut oleh penyidik siber dengan sebutan pengolahan TKP. Yang menjadi bagian penting dalam pengolahan TKP adalah memeriksa perangkat yang digunakan oleh pelaku untuk memposting berita bohong (hoaks). Perangkat yang digunakan juga bermacam-macam, seperti laptop, handphone, komputer dan sebagainya.

**9. Digital Forensik**

Digital forensik adalah penggunaan teknik analisis dan investigasi untuk mengidentifikasi, mengumpulkan, memeriksa dan menyimpan bukti

atau informasi yang secara magnetis tersimpan pada komputer atau media penyimpan digital.

Proses ini dilakukan untuk memeriksa dengan saksama barang atau sistem elektronik yang mengandung informasiatau dokumen elektronik yang dapat dijadikan alat bukti.

Mekanisme kerja dari proses digital forensik antara lain :

- Proses Enginering dan Imaging :

  Setelah penyidik siber menerima barang bukti digital, maka harus dilakukan proses mengkopi (mengkloning atau menduplikat) secara tepat dan persis.

- Melakukan Analisis :

  Setelah penyidik siber melakukan proses enginering dan imaging maka dilanjutkan dengan menganalisis isi data terutama yang sudah dihapus atau disembunyikan sehingga bisa dienskrip. Jejak log file yang telah dihapus atau disembunyikan itu akan dianalisis sehingga hasil dari analisis itu akan dijadikan sebagai barang bukti digital untuk diserahkan ke kejaksaan.

**10. Teknik penyelidikan**

Pada bagian ini, penyidik siber tidak mau menjelaskan terlalu dalam mengenai teknik penyelidikan karena merupakan bagian yang bersifat

sangat rahasia sehingga peneliti hanya mendapatkan sedikit informasi mengenai teknik penyelidikan yang dilakukan penyidik siber di lapangan.

Subdirektorat V Unit Siber memiliki alat khusus yang bernama Direction Finder (DF). Alat ini dapat melacak keberadaan seseorang melalui sinyal handphone miliknya. Tidak hanya itu, alat ini juga bisa mendeteksi IP adress dan kapan terakhir kali akun yang menyebarkan berita bohong (hoaks) itu aktif atau diakses. Alat ini (Direction Finder) hanya dimiliki oleh Subdirektorat V Unit Siber POLDA NTT, Direktorat Intelijen POLDA NTT dan Direktorat Reserse Narkoba POLDA NTT.

Kemudian setelah mengetahui lokasi dari pelaku maka penyidik akan menugaskan beberapa orang untuk mengawasi pergerakan pelaku, orang-orang ini biasa disebut informan. Mereka hanya melakukan pengawasan sampai ada perintah dari kasubdit untuk menangkap pelaku.

Setelah ada perintah dari kasubdit untuk melakukan penangkapan, maka penyidk siber akan turun ke lapangan bersama informan dan melakukan penangkapan terhadap pelaku. Setelah pelaku ditangkap dan ditahan, penyidik akan melakukan pemeriksaan dan kemudian mengamankan barang bukti (akun dan alat yang digunakan). Setelah itu, penyidik mengunci (mengambil alih akun) dengan cara mengganti password media sosial pelaku dengan password baru yang jumlah digit password sebagian diketahui oleh penyidik dan sebagian diketahui oleh

pelaku. Sehingga akun itu aman dan hanya bisa dibuka ketika penyidik dan pelaku berada ditempat yang sama.

Untuk akun-akun palsu atau dikenal dengan sebutan anonymous yang menyebarkan berita bohong (hoaks), penyidik akan melakukan takedown atau menutup akun tersebut. Penyidik siber telah bekerja sama dengan seluruh platform media sosial (*facebook, twitter, instagram, what's up, line* dll) yang digunakan di Indonesia. Langkah yang digunakan oleh penyidik siber adalah dengan mengirim e-mail khusus dari Subdit V Unit Siber POLDA NTT ke platform media sosial yang digunakan untuk menyebarkan berita bohong (hoaks) agar segera menutup akun itu. E-mail khusus yang dimaksud adalah e-mail yang sudah disepakati oleh POLDA NTT dengan platform media sosial. Sehingga penyidik siber tidak membutuhkan waktu yang lama untuk menutup akun media sosial tersebut.