Menyiapkan Ponsel untuk Dokumentasi Luring
Seri Pendokumentasian Saat Internet Shutdown

Oleh Yvonne Ng

Dengan kontribusi dari Arul Prakkash

Artikel ini adalah bagian dari Seri *Pendokumentasian Selama Pemadaman Internet*

Terakhir diulas: 31 Januari 2020

Meskipun terjadi pemadaman internet, para dokumenter masih bisa mengambil bukti video penting yang dapat dibagikan secara luring (offline) atau saat mereka bisa kembali daring (online).

Berikut adalah beberapa kiat yang kami pelajari dari aktivis dan praktisi lain dalam menyiapkan ponsel untuk dokumentasi *offline*. Perhatikan bahwa beberapa langkah **memerlukan akses internet**, jadi harus dilakukan sebelum *shutdown* terjadi atau selama periode pemulihan. Selain itu, jangan menunggu sampai berada pada situasi darurat atau tegang untuk melakukan langkah-langkah ini; lakukan sekarang dan luangkan waktu **untuk berlatih menggunakan ponsel** sebelum harus digunakan selama krisis.

Pemadaman internet sering bertepatan dengan kontrol terhadap informasi yang meningkat serta pembatasan kebebasan berekspresi dan berkumpul. Jika kamu melakukan dokumentasi foto/video/audio, lakukan tindakan pencegahan ekstra untuk melindungi diri dan informasi kamu selama periode ini. Jika ada risiko bahwa pihak berwenang akan menyita ponsel atau memaksa untuk membuka kunci dan menunjukkan kontennya (selama *shutdown* atau bukan), pertimbangkan untuk menggunakan ponsel untuk dokumentasi yang berbeda dari ponsel pribadi. Hal ini dapat membantu mengurangi informasi yang dapat dibocorkan (mis. kontak, pesan, akun, dll). Jika tidak bisa menggunakan gawai lain, panduan ini tetap dapat diikuti untuk mengurangi jumlah data sensitif dan meningkatkan keamanan pada ponsel utama.

Jika menggunakan ponsel lama, bersihkan dan hapus seluruh datanya terlebih dahulu

Untuk membersihkan ponsel, lakukan *Factory Reset* atau kembalikan pada pengaturan awal

Catatan: Penelitian menunjukkan bahwa melakukan *Factory Reset* tidak serta merta menghapus semua data. Faktanya, satu-satunya cara yang terbukti aman 100% untuk menghapus data adalah dengan menghancurkan ponsel, tetapi metode itu bukan pilihan jika kamu ingin menggunakan kembali ponsel tersebut! Pada artikel ini, seorang teknisi Android menyarankan untuk memastikan konten pada gawai kamu dienkripsi sebelum *Factory Reset*. Enkripsi biasanya merupakan settingan awal pada sebagian besar ponsel saat ini, tetapi jika belum terenkripsi, buka Pengaturan > Keamanan > Enkripsi Telepon (Settings > Security > Encrypt Phone) sebelum mengatur ulang. Dengan cara ini, ketika dilakukan *Factory Reset*, kunci enkripsi akan hilang, dan semua data yang tidak terhapus tidak akan bisa dibaca.

Praktik keamanan dasar ponsel

Ada sejumlah praktik keamanan umum ponsel yang masih relevan di segala situasi, baik bagi mereka yang sedang mendokumentasikan selama *internet shutdown* atau tidak. Berikut ini sejumlah sumber yang berguna bagi organisasi lain. Meskipun tidak ada yang menjamin 100% keamanan, sejumlah tips kunci meliputi:

- Pastikan ponsel terenkripsi. Ponsel lebih baru memiliki enkripsi *by default*. Kalau tidak yakin dengan ponsel yang digunakan, cek pengaturan keamanan di ponsel.
- Pastikan Sistem Operasi selalu ter-*update* secara rutin, karena kerap ada perbaikan celah keamanan.
- Perbaharui secara rutin aplikasi yang penting (seperti aplikasi Pesan Instan).
- Pasang kode sandi ponsel yang kuat yang memiliki setidaknya 6 digit dan tidak bergantung pada sidik jari / sentuhan atau ID wajah.
- Atur penguncian layar dan waktu penguncian.
- Matikan layanan lokasi jika kamu tidak membutuhkannya (termasuk layanan lokasi darurat, akurasi lokasi, riwayat lokasi, dan fitur berbagi lokasi, dan opsi pemindaian WiFi dan Bluetooth). Periksa juga izin lokasi untuk masing-masing aplikasi.
- Matikan Bluetooth dan WiFi saat tidak dibutuhkan, untuk menghindari pelacakan gawai.
- Matikan ponsel saat tidak digunakan.

Instal aplikasi dokumentasi yang berguna

Untuk dokumentasi foto atau video, gunakan aplikasi kamera bawaan pada ponsel. Atau gunakan aplikasi dokumentasi yang lebih khusus, seperti ProofMode atau yang lainnya, yang memungkinkan penangkapan metadata yang lebih kuat dan ekspor, identifikasi dan otentikasi, enkripsi, galeri aman, atau fitur lainnya.

Aplikasi yang berguna untuk mendokumentasikan suatu *shutdown* adalah OONI Probe, aplikasi open-source yang menjalankan tes dari ponsel kamu untuk mengukur apakah situs atau platform sedang diblokir. Ini dapat menunjukkan bagaimana, kapan, di mana, dan oleh siapa situs diblokir. Pastikan untuk memahami potensi resiko sebelum menggunakan aplikasi ini.

Tidak yakin aplikasi dokumentasi mana untuk digunakan? Kami sediakan beberapa pertanyaan panduan dalam tutorial "Haruskah Saya Menggunakan Aplikasi Dokumentasi ini?".

Meng-*install* beberapa aplikasi sehari-hari

Hanya memiliki sedikit data dan aplikasi khusus di ponsel bisa memunculkan kecurigaan. Agar gawai terlihat seperti ponsel sehari-hari, pasanglah beberapa aplikasi yang umumnya digunakan di lokasi di mana kamu melakukan dokumentasi (tetapi mereka diunduh dari sumber-sumber terpercaya), dan mengambil beberapa foto tidak berbahaya dari galeri kamu.

Untuk aplikasi media sosial, kamu mungkin bisa membuat dan masuk akun-akun alternatif. Meskipun harus diingat bahwa membuat akun palsu melanggar Ketentuan Penggunaan sebagian besar platform, dan persyaratan verifikasi identitas beberapa aplikasi mungkin susah dipalsukan. Selain itu, kamu juga memerlukan waktu cukup lama untuk membuat konten dan menambahkan teman.

Meng-*install* aplikasi ketika tidak ada internet

Mengunduh dan menginstal aplikasi tanpa akses internet merupakan tantangan. Kamu perlu mengunduh aplikasi terlebih dahulu jika kamu mengantisipasi adanya pemadaman internet.

Salah satu strategi yang dapat membantu kamu dan orang lain di kemudian hari adalah mengunduh dan menyimpan file Paket Android (.apk) untuk aplikasi (**diunduh dari sumber terpercaya**, mis. langsung dari pengembang) di penyimpanan ponsel atau di drive. Memiliki APK ini secara *offline* memungkinkan kamu atau orang lain untuk berbagi aplikasi ketika tidak ada internet.

Meskipun kami belum berkesempatan mencobanya, aplikasi F-Droid menyediakan antarmuka untuk menukar APK ini secara *offline*. Inilah tutorial mereka.

Jangan simpan informasi riil pribadi/informasi sensitif di luar gawai

Cobalah untuk memiliki gawai khusus untuk melakukan dokumentasi. Jangan menggunakannya untuk email, panggilan telepon, atau pesan dengan kontak pribadi atau aktivis yang dapat berisiko, dan jangan sambungkan gawai ini ke akun riil dan/atau akun utama kamu.

Gunakan fitur-fitur untuk mengaburkan konten

Jika ponsel kamu diutak-atik, mungkin akan membantu jika pada ponsel, kamu menyamarkan intensimu atau membuat kontenmu lebih sulit ditemukan. Untuk mengantisipasi situasi di mana ponsel kamu hanya akan diperiksa (orang lain) secara dangkal dan cepat, kamu dapat menggunakan taktik sederhana seperti:

- Mengubah nama dan ikon pintasan aplikasi dengan menggunakan aplikasi Launcher (mis. Nova Launcher, tetapi ada banyak ikon dan nama yang sama) sehingga aplikasi tertentu menjadi kurang jelas.
- Menggunakan fitur privasi bawaan seperti Mode Pribadi (Samsung) atau Content Lock (LG), jika ponsel kamu mendukungnya.
- Menempatkan file kosong bernama ".nomedia" di dalam folder apa saja yang ada, untuk mencegah media di folder muncul di galeri kamu. Catatan: Jika media masih muncul, kamu mungkin perlu menghapus cache Galeri kamu. Ini mungkin tidak sama hasilnya di semua gawai.
- Membuat folder tersembunyi (folder yang dimulai dengan ".") dengan menggunakan aplikasi manajer file. kamu dapat memindahkan file ke folder tersembunyi tersebut secara manual, atau jika bisa juga menggunakan aplikasi kamera seperti Open Camera. Kamu dapat menentukan di mana media yang kamu rekam disimpan. Pastikan untuk mematikan opsi "tampilkan file tersembunyi" di Pengaturan kamu sehingga file yang tersembunyi tidak terlihat.
- Beberapa aplikasi dokumentasi khusus, seperti Tella atau Eyewitness to Atrocities, menyimpan dokumentasi di galeri terenkripsi terpisah yang isinya hanya dapat diakses di dalam aplikasi, mungkin membuatnya kurang dapat dilihat jelas bagi seseorang yang mengutak-atik mencari-cari di ponsel kamu. Dokumentasi di galeri yang aman ini memerlukan kode sandi aplikasi yang terpisah, sehingga tetap dienkripsi bahkan ketika

ponsel kamu tidak terkunci.

Catatan penting tentang mengaburkan konten kamu

Penting untuk dicatat bahwa teknik-teknik di atas mungkin cukup untuk menghindari seseorang untuk dengan cepat menggeser-geser tampilan ponsel kamu, tetapi tidak akan secara efektif menyembunyikan kontenmu dari seseorang yang benar-benar menyelidiki.

Ingat juga bahwa beberapa negara mungkin memiliki undang-undang yang membatasi atau mengkriminalkan penggunaan aplikasi keamanan yang mengenkripsi atau menghapus data kamu. Menggunakan aplikasi tersebut untuk mencegah pihak berwenang mengakses data kamu dapat dilihat sebagai menghancurkan bukti atau menghambat penyelidikan, dan dapat dihukum sebagai kejahatan. Peta ini (komprehensif, tetapi dibuat pada tahun 2017) memberikan awalan yang baik jika kamu memiliki pertanyaan tentang undang-undang di negara kamu.

Persiapan Berbagi Luring/Offline

Ketika berada dalam situasi *offline*/luring, kamu mungkin ingin tetap menghapus beberapa dokumentasi, baik atas dasar keamanan, mengosongkan tempat penyimpanan, atau membagikannya dengan orang lain. Menghapus dokumentasi secara rutin di ponsel kamu, akan membantu mengurangi informasi jika dicuri atau dibuka kunci pengamannya.

Walaupun kamu tidak terhubung ke internet, kamu tetap dapat mengakses wifi atau bluetooth lokal yang ada di dalam ponsel, seperti melalui ponsel lain atau perangkat wifi USB. Ponsel kamu seharusnya sudah memiliki sebuah aplikasi untuk terhubung dengan kedua fitur diatas. Jika mendukung, kamu dapat memasang perangkat USB On-The-Go (OTG) guna memindahkan dokumentasi ke gawai lain.

Metode tersebut dapat didiskusikan secara lebih rinci di tutorial “Cara berbagi data dan berkomunikasi ketika Internet Shutdown” dan video “As Evidence: Tech Tools — Transferring Files”.

Berlatihlah sebelum kamu berada dalam situasi krisis

Setel ponselmu sekarang, selagi kamu sedang memiliki akses internet. Mulai berlatih menggunakan aplikasi dalam situasi sehari-hari (di mana tidak ada masalah keamanan) agar terbiasa dan nyaman menggunakannya. Jadikan keamanan dasar telepon yang baik sebagai praktik sehari-harimu. Dengan cara ini, metode yang digunakan kemudian akan menjadi hal yang biasa ketika kamu berada dalam situasi krisis saat banyak hal yang perlu dikhawatirkan.

Lihat posting berikutnya dalam seri ini, "Haruskah Saya Menggunakan Aplikasi Dokumentasi Ini?