BAB I
PEDAHULUAN

1.1 Latar Belakang

Di era perkembangan teknologi informasi yang sangat pesat, saat ini peramban menjadi aplikasi yang wajib di install pada perangkat *dekstop* maupun *mobile* bahkan tv dan kulkas saat ini juga terintregasi dengan peramban. Peramban adalah perangkat lunak yang digunakan untuk mengakses halaman web guna memperoleh informasi yang jelas dan mudah dibaca. Sumber daya informasi di identifikasikan oleh *Uniform Resource Identifier* (URI) dan dapat berupa halaman web, gambar, video, atau konten lainnya.[1] Aktivitas menggunakan peramban sendiri disebut *browsing*, biasanya pengguna peramban menggunakan peramban untuk mengakses halaman web seperti berberlanja secara daring, berinteraksi dengan orang menggunakan media sosial, mengakses surel maupun mengunggah dan mengunduh file.

Qutebrowser dan *LibreWolf* adalah salah dua contoh dari peramban yang ada. *Qutebrowser* adalah perambaan *open source* yang berfokus menggunakan keyboard[2]. QuteBrowser menggunakan Qt dan QtWebEngine secara default dan mendukung QtWebKit secara opsiona, menjadikan QuteBrowser ramah terhadap komputer yang memiliki *low memory*. QtWebEngine didasarkan pada Google Chromium. Dengan Qt versi terbaru, QtWebEngine memiliki lebih banyak framework pendukungnya dengan demikian mendukung fitur web yang lebih modern, QtWebEngine juga bisa dibilang lebih aman. [2] Sedangakan *LibreWolf* merupakan peramban yang diproduksi oleh komunitas perangkat lunak *open source* yang befokus pada keamanan dan privasi.[3].Librewolf sendiri telah dibuat sebersih mungkin dari telemetri yang membuat peramban ini aman digunakan tanpa merisaukan privasi saat pengguna menggunakannya.

Digital forensik sebagai bukti digital. Secara umum digital forensik sendiri adalah proses ilmiah atau untuk mengumpulkan, menganalisis dan menyajikan bukti untuk membantu dalam proses penegak hukum untuk menyelesaikan kasus kejahatan digital.[4] Salah satu contoh teknik digital forensik yaitu merupakan

dead forensic, dead forensic sendiri adalah teknik dimana akuisisi bukti digital diakuisisi pada sistem operasi dimana bukti digital yang akan di akuisisi tersimpan secara permanen di penyimpanan seperti solid slate drive atau harddisk.[5]

Pada saat pengguna peramban melakukan aktivitas di dunia maya, pengguna peramban biasanya meninggalkan jejak di perangkat seperti riwayat, *cookies, cache files*, bahkan alamat surel dan kata sandi.[6] Jejak jejak seperti ini biasanya bisa membantu pengguna dalam mengakses suatu situs web maupun menginputkan sesuatu, misalnya surel dan kata sandi. Jika informasi seperti surel atau kata sandi terlalu terbuka atau bisa mudah dikases orang lain akan ada kemungkinan terjadi penyalahgunaan data pribadi seperti penyalinan data informasi pada kartu ATM (*skimming)* dimana pelaku penyalahgunaan surel dan kata sandi bisa melakukan penarikan dana di tempat lain.[7]

Dari Latar belakang permasalahan diatas peneliti memutuskan untuk melakukan analisa *dead forensic* pada peramban dengan metode NIST 800-86 yang berfokus pada peramban *Qutebrowser* dan *LibreWolf*.

Jadi dengan adanya penelitian ini, dapat dijadikan sebagai tolak ukur untuk mengetahui tingkat keamanan dan mengetahui data krusial apa saja yang didapatkan melalui peramban *Qutebrowser* dan *LibreWolf*.

1.2 Rumusan Masalah

Berdasarkan latar belakang permasalahan yang diuraikan diatas maka rumusan masalah pada penelitian ini adalah bagaimana melakukan analisa *dead forensic* pada peramban *Librewolf* dan *Qutebrowser* untuk mendapatkan bukti digital yang berpotensi disalahgunakan?.

1.3 Pertanyaan Penelitian

Berdasarkan rumusan masalah yang diuraikan diatas maka pertanyaan yang timbul dari rumusan masalah diatas,bukti digital apa sajakah yang didapat melalui analisa *dead forensic* pada peramban *Librewolf* dan *Qutebrowser* dengan framework *National Institute of Standard and Technology* (NIST) 800-86.

1.4 Batasan Masalah

Batasan masalah yang digunakan pada penelitian ini sebagai berikut :

a. Metode yang digunakan peneliti pada penelitian ini adalah menggunakan metode *Dead Forensic* dengan framework *National Institute of Standard and Technology* (NIST) 800-86.
b. Peramban yang digunakan adalah *Qutebrowser* dan *LibreWolf*.
c. Penelitian ini dilakukan tanpa mode *private*.
d. Dimatikannya fungsi *Auto-delete cookies and data* untuk peramban *Librewolf*
e. Studi kasus yang dianalisa adalah situs *Twitter, YouTube, Telegram, Gmail, Facebook, instagram, whatsapp*
f. Software yang digunakan untuk pengujian adalah Autopsy.

1.5 Tujuan Penelitian

Tujuan dari penelitian ini adalah mendapatkan dan menganalisa bukti digital yang berupa *cache* pada *harddisk* di peramban *Librewolf* dan *Qutebrowser* dengan metode NIST 800-86.

1.6 Manfaat Penelitian

Manfaat peneletian yang diharapkan yaitu:

a. Sebagai rekomendasi pengguna peramban dalam menggunakan peramban yang mengutamakan keamanan.
b. Mengetahui tingkat keamanan peramban *Qutebrowser* dan *Librewolf*.
c. Mengetahui bukti digital apa saja yang didapat pada peramban *Qutebrowser* dan *Librewolf*.