SISTEM PENGURUSAN KES FORENSIK DIGITAL MENGGUNAKAN VIRTUAL PRIVATE NETWORK (VPN)

NURELISHA SHAFWANA BINTI MOHD GHAZALI
KHAIRUL AKRAM ZAINOL ARIFFIN

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRACT

Forensik digital merupakan prosedur penyiasatan terhadap komputer dan peranti digital seperti telefon bimbit, kamera litar tertutup dan sebagainya. Pertumbuhan teknologi maklumat dan kerumitan jenayah siber, memerlukan aktiviti forensik digital yang ada saling berhubungan. Ini perlu disokong oleh saluran komunikasi yang selamat. Keselamatan dan kepercayaan merupakan isu penting dalam forensik digital kerana ia sering dikaitkan dengan integriti dan ketulenan bukti digital. Sistem ini dibangunkan atas dasar permasalahan yang timbul. Terdapat beberapa pihak terlibat di dalam penyimpanan mekanisma, akses serta perkongsian analisis bukti digital. Semua aktiviti forensik digital haruslah terjamin dan ketulenan bahan bukti terpelihara. Oleh itu, sistem berdasarkan web ini dibangunkan bagi memelihara bahan bukti supaya tidak terdedah kepada pihak yang tidak bertanggungjawab. Metodologi yang digunakan untuk membangunkan sistem ini ialah *System Development Life Cycle* yang menggunakan Rapid *Application Development* (RAD) sebagai model dalam merangka proses-proses yang terlibat dalam pembinaan sistem ini. Sistem ini diharapkan dapat memberi kemudahan kepada mana-mana organisasi yang memerlukan

1 PENGENALAN

Perkembangan pesat teknologi komputer pada masa kini telah menyumbang kepada kegiatan jenayah siber dan telah menjadi suatu ancaman yang serius. Oleh itu, menyediakan keselamatan yang lengkap dan mencukupi merupakan satu tugasan yang rumit kerana peranti teknologi yang semakin kompleks dan menyebabkan penyiasatan yang melibatkan alat-alat ini menjadi sukar. Forensik digital adalah prosedur penyiasatan terhadap komputer dan peranti digital seperti telefon bimbit dan kamera litar tertutup.

Menurut Husin Jazri dalam Laporan Tahunan CyberSecurity Malaysia 2011, sebagai sebuah negara yang pesat membangun, kebergantungan rakyat Malaysia terhadap teknologi sudah tentu meningkat. Walaupun kemajuan dalam bidang siber merupakan satu perkembangan positif, malangnya kemajuan ini jugalah yang membuat rakyat terdedah kepada pelbagai bentuk ancaman siber.

Kegiatan forensik digital merupakan proses yang melibatkan beberapa pihak, seperti responden pertama, penyiasat forensik, saksi ahli sidang, anggota penguatkuasa undang-undang, pegawai polis, mangsa, suspek dan saksi. Penglibatan banyak pihak bakal menjana

interaksi yang sangat kompleks mekanisme yang harus difasilitasi oleh infrastruktur yang mencukupi.

Responden pertama dan penyiasat adalah pelaku di dalam forensik digital yang mempunyai tahap mobiliti yang tinggi dan keperluan sistem bagi melaksanakan akses jauh ke dalam sistem dan pangkalan data utama. Bagi melaksanakan aktiviti tersebut, keperluan untuk forensik digital infrastruktur yang selamat dan dipercayai adalah sangat penting.

CyberSecurity Malaysia merupakan agensi keselamatan siber nasional di bawah Kementerian Sains, Teknologi dan Inovasi (MOSTI) dan mempunyai Forensik Digital sebagai salah unit perkhidmatan di dalam agensi ini. Unit ini menyediakan bantuan penyiasatan tempat kejadian jenayah siber (CyberCSI) kepada agensi-agensi penguatkuasaan undang-undang, badan-badan yang mengawal selia, agensi kerajaan dan organisasi.

Sistem Pengurusan Kes Forensik Digital menggunakan Virtual Private Network (VPN) ini dibangunkan bertujuan untuk memelihara bahan bukti digital, sebarang jenis media storan digital dan semua laporan dan testimoni dari penganalisis yang boleh digunakan sebagai bukti di mahkamah daripada terdedah kepada pihak yang tidak bertanggungjawab. Melalui sistem ini juga hanya beberapa pihak sahaja dapat mengakses kepada bahan bukti digital dan laporan (Boddington, R. (n.d.). *Digital Evidence. Emerging Forensic Tools for Locating and Analyzing Digital Evidence*).

2 PENYATAAN MASALAH

Permasalahan ini dibincangkan kerana penganalisis forensik digital berhadapan dengan maklumat yang berpunca dari komputer, telefon bimbit, sistem navigasi satelit dan alat hi-tech yang lain. Data ini sangat penting kepada isu-isu dalam kes ini. Kerap kali maklumat serta bahan bukti yang peribadi dan sulit hilang dan didapati sudah diubah oleh pihak yang tak bertanggungjawab. Oleh yang demikian, kesahihan dan keselamatan maklumat yang diperolehi tidak dapat dipelihara secara telus.

Selain itu, dalam proses tradisional, bahan bukti digital hasil dari siasatan digital tidak dapat diperolehi pada masa yang singkat. Kesannya, bahan bukti yang ditemui tidak digunakan bagi membentuk hipotesis terhadap kes siasatan tersebut. Masa pemulihan bahan bukti juga mengambil masa yang lama kerana pegawai penyiasatan tidak mempunyai akses terus ke pentadbiran sistem.

Di samping itu, bahan bukti digital sering terdedah kepada korupsi dan pencerobohan dan diragui keselamatan, ketepatan serta kesahihan barang bukti digital tersebut. Pangkalan data

yang menyimpan data berkaitan kes-kes mahkamah haruslah telus dan terpelihara apabila digunakan oleh pihak pakar. Oleh itu, sistem ini dibangunkan bagi mengatasi permasalahan ini.

3 OBJEKTIF KAJIAN

Sistem pengurusan kes digital forensik ini dibangunkan bagi memenuhi objektif berikut:

i. Mengawal sesebuah pangkalan data yang menyimpan data dan maklumat berkaitan kes dan membenarkan hanya pihak yang dibenarkan mengakses pangkalan tersebut.
ii. Sistem yang berasaskan web sebagai sistem pangkalan yang mempunyai sekuriti menggunakan *Virtual Private Network* (VPN) agar bahan bukti digital tidak hilang dan terpelihara.
iii. Untuk menguji keberkesanan sistem dan mendapat maklum balas yang baik daripada pengguna setelah menggunakan sistem ini.

4 METOD KAJIAN

Asas metodologi yang digunakan dalam membangunkan sistem ini adalah "*System Development Life Cycl*e" atau lebih dikenali sebagai SDLC. Dalam metodologi ini terdapat beberapa fasa yang terlibat seperti fasa perancangan, analisis, rekabentuk, implementasi, dan penyelenggaraan.

Seterusnya metodologi yang akan digunakan adalah kaedah "*Rapid Application Development* (RAD)" dalam merangka proses-proses yang terlibat dalam pembinaan sistem ini. Saya memilih metodologi ini kerana apabila terdapat kesalahan atau tertinggal satu fasa pihak pembangunan boleh berulang ke fasa sebelumnya untuk memperbetulkan kesalahan tersebut dan tinjauan awal yang cepat dapat berlaku.

4.1 Fasa Perancangan

i. Pemilihan sistem yang hendak dibangunkan.

ii. Mengumpul maklumat hasil daripada temuramah dan pemerhatian.

iii. Mengenalpasti objektif dan skop projek.

4.2 Fasa Analisis

i. Menganalisis masalah yang sering berlaku apabila dilakukan secara manual.

ii. Analisis terhadap masalah ini dilakukan agar sistem yang dibangunkan dapat mengatasi masalah-masalah tersebut.

iii. Menemuramah pegawai CyberSecurity Malaysia di pejabat CyberSecurity Malaysia.

4.3 Fasa Rekabentuk

i. Merekabentuk gambar rajah konteks, carta aliran data, dan rajah hubungan entiti.

ii. Merekabentuk antara muka sistem yang interaktif dan mudah difahami pengguna.

iii. Merekabentuk jadual aliran dalam setiap proses yang berlaku dalam sistem.

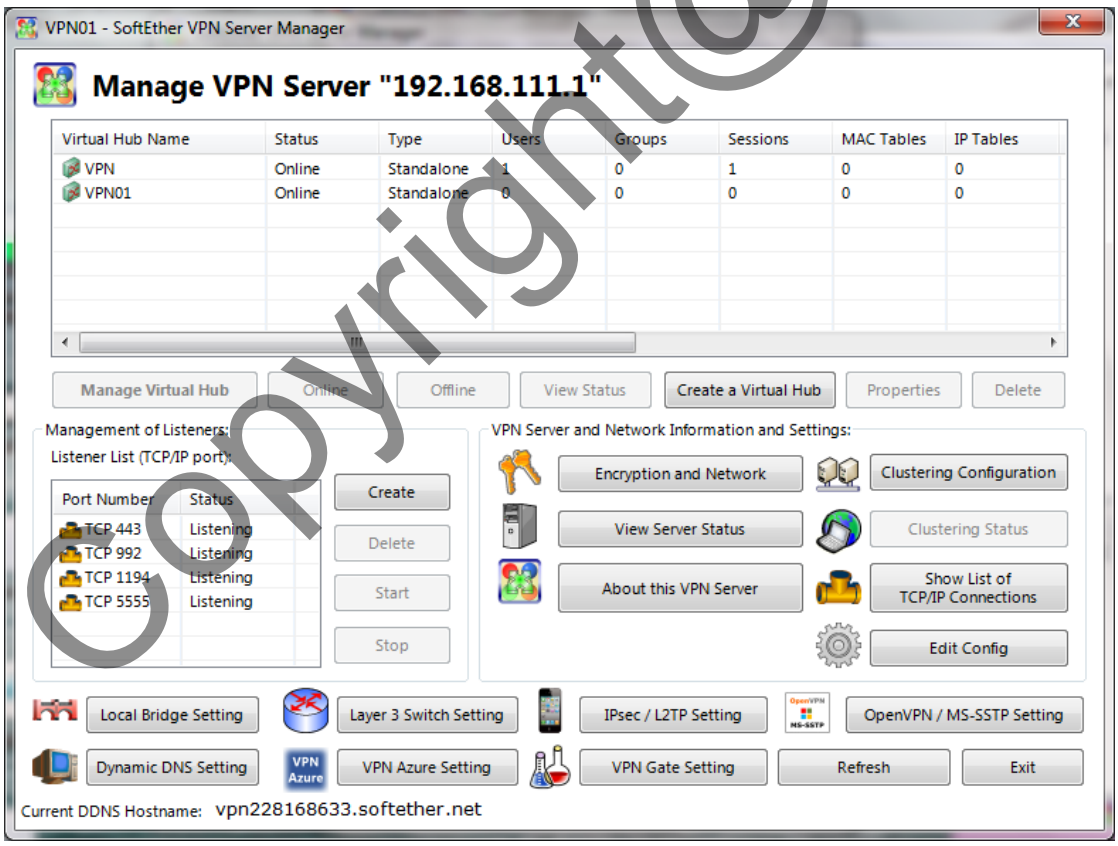
4.4 Fasa Pengujian

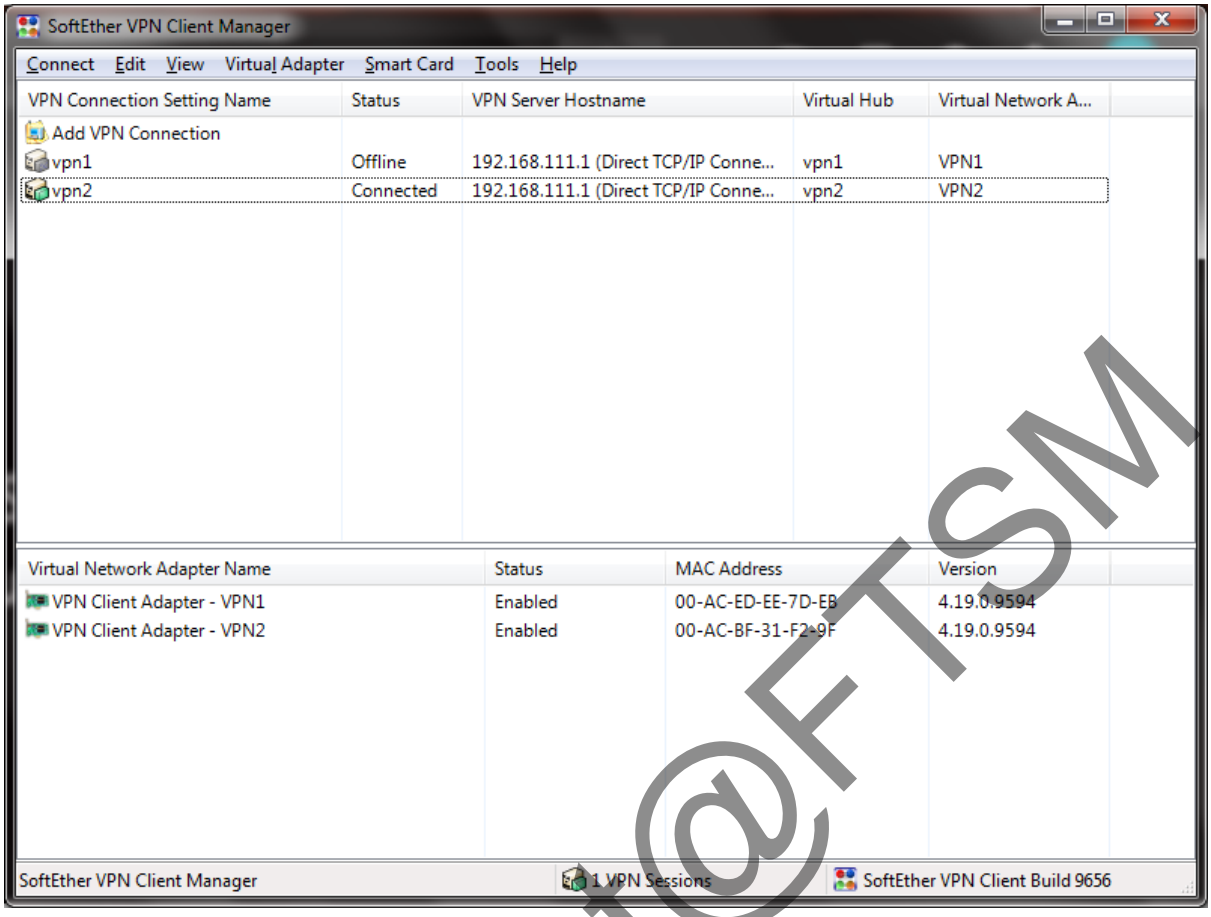
i. Mengaplikasikan aturcara bahasa PHP bagi membolehkan sistem ini dapat berjalan dengan baik.

ii. Mengimplementasi antara muka sistem menggunakan bahasa pengaturcaraan yang telah dipilih.

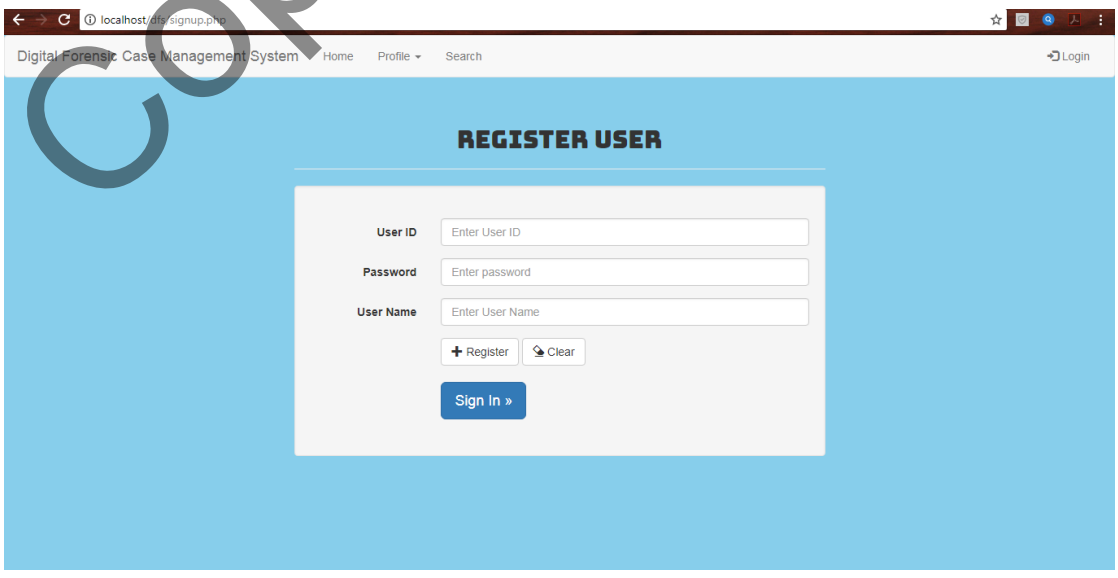
iii. Mengimplementasi fungsi sistem dengan menggunakan bahasa pengaturcaraan yang telah dipilih.

5 HASIL KAJIAN

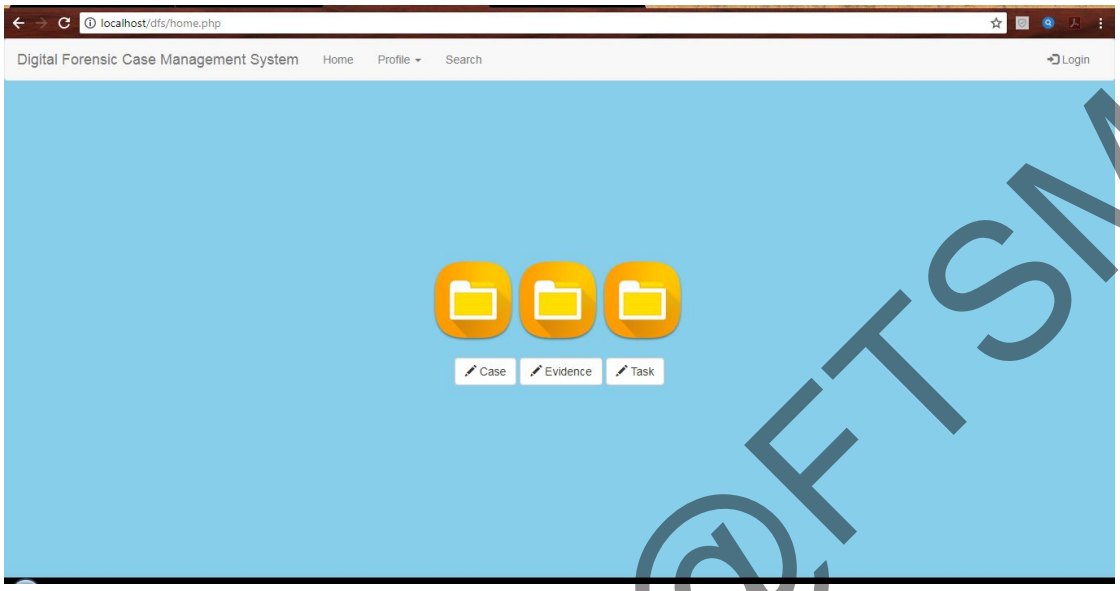




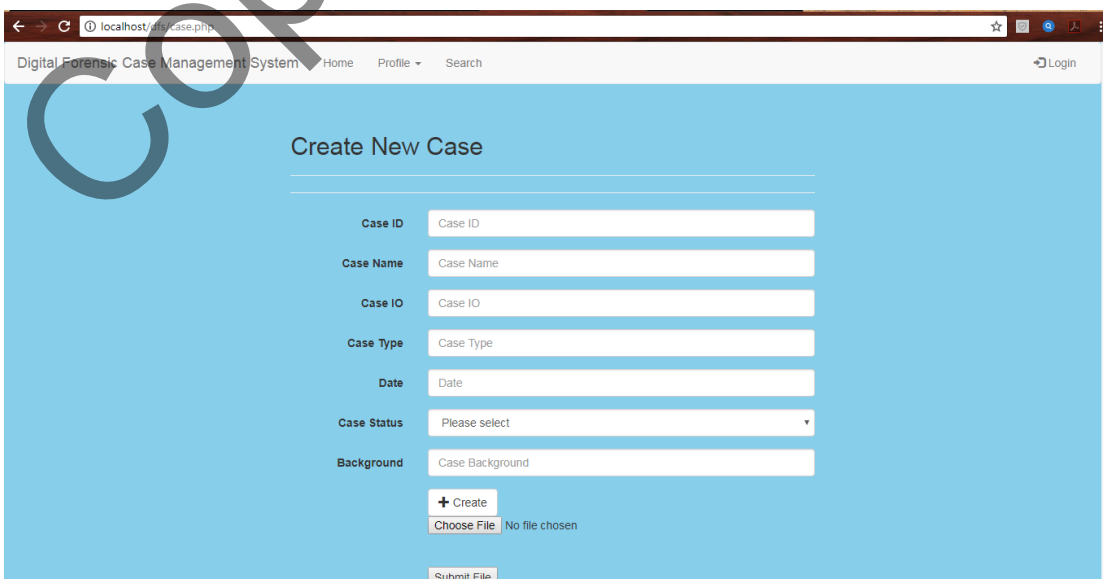
Rajah di atas menunjukkan penetapan *Virtual Private Network* (VPN) bagi klien dan pelayan. Admin atau pegawai teknikal perlu menetapkan alamat *host* dan *port number*. Selain itu, admin juga perlu memasukkan nama pengguna dan kata laluan bagi penetapan *VPN Server*. Kata laluan juga dihashkan bagi langkah sekuriti terhadap penetapan *VPN Server* ini terhadap sistem web.



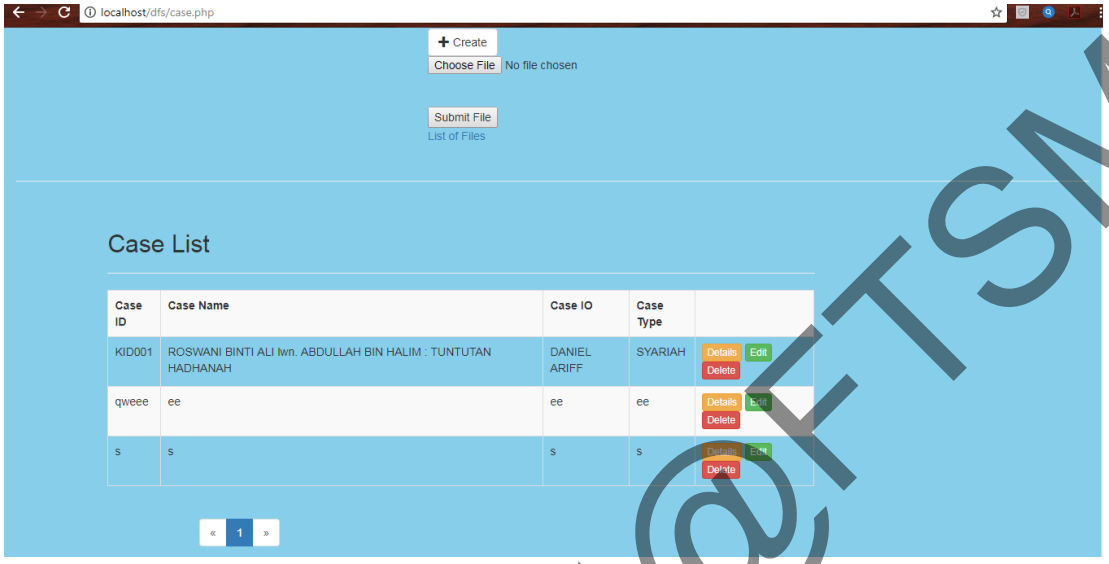
Rajah di atas menunjukkan antaramuka daftar pengguna. Pengguna akan mendaftar pengguna terlebih dahulu sebelum ke halaman log masuk. Jika pengguna sudah berdaftar, pengguna boleh menekan butang *Sign In* untuk log masuk ke sistem web ini.



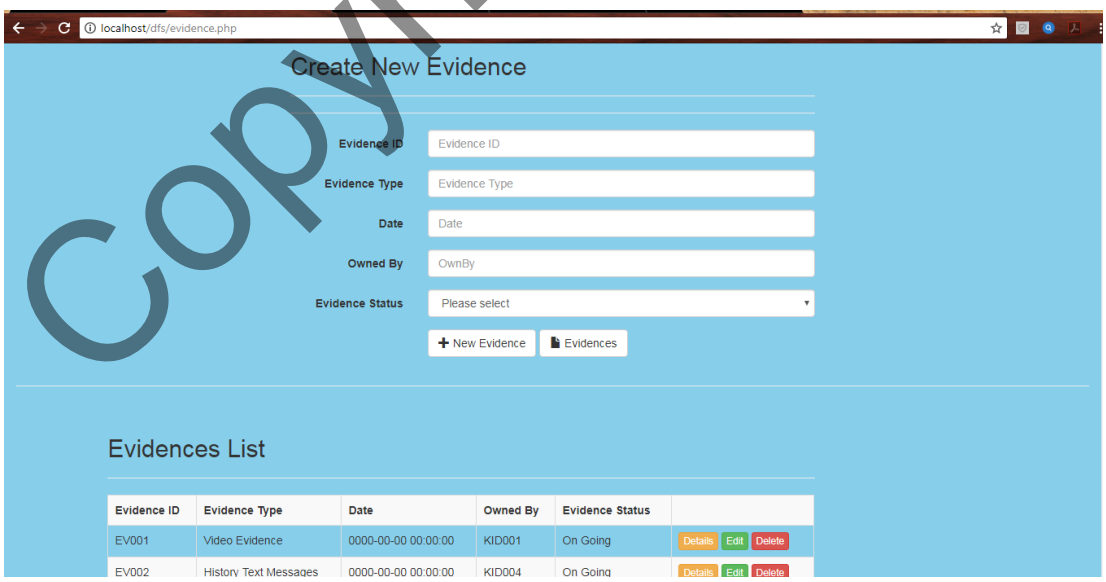
Rajah seterusnya menunjukkan antaramuka halaman utama Sistem Pengurusan Kes Forensik Digital. Pada bahagian Case, adalah halaman dimana pengguna boleh menambah kes baru, mengedit dan memadam kes di dalam sistem. Seterusnya, pada bahagian Evidence, pengguna boleh menambah bahan bukti baru serta memuatnaik fail ke dalam sistem web ini. Terdapat pelbagai jenis fail boleh dimuatnaik ke sistem ini. Pada bahagian Task adalah dimana juruteknik akan memberikan tugas kepada *Investigator Officer* (IO) untuk bertugas terhadap kes yang telah diberikan.



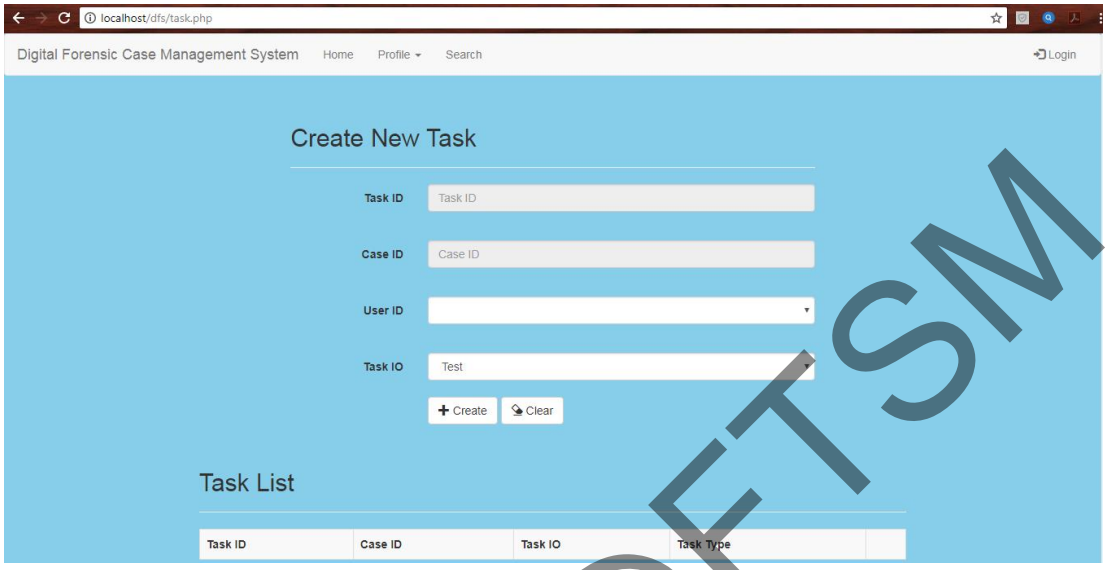
Rajah di atas merupakan halaman dimana pengguna boleh menambah kes siasatan baru. Rajah ini juga menunjukkan senarai kes yang telah didaftarkan dan pengguna boleh mengedit dan melihat info mengenai kes siasatan. Pengguna juga boleh memuatnaik fail berkaitan kes.



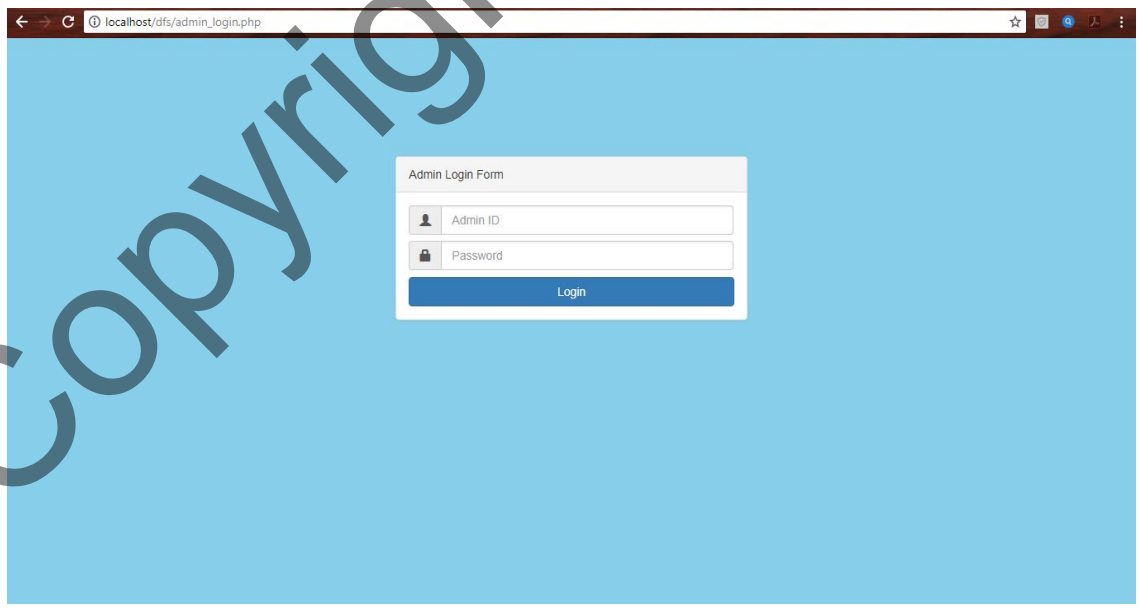
Rajah dia atas menunjukkan antaramuka senarai kes yang telah disimpan di dalam sistem web ini. Pengguna boleh mengubah, memadam dan melihat latarbelakang kes yang sedang mereka siasat. Terdapat kes id, nama kes, nama IO bertugas dan jenis kes bagi memudahkan pengguna untuk mencari kes yang sedang disiasat.



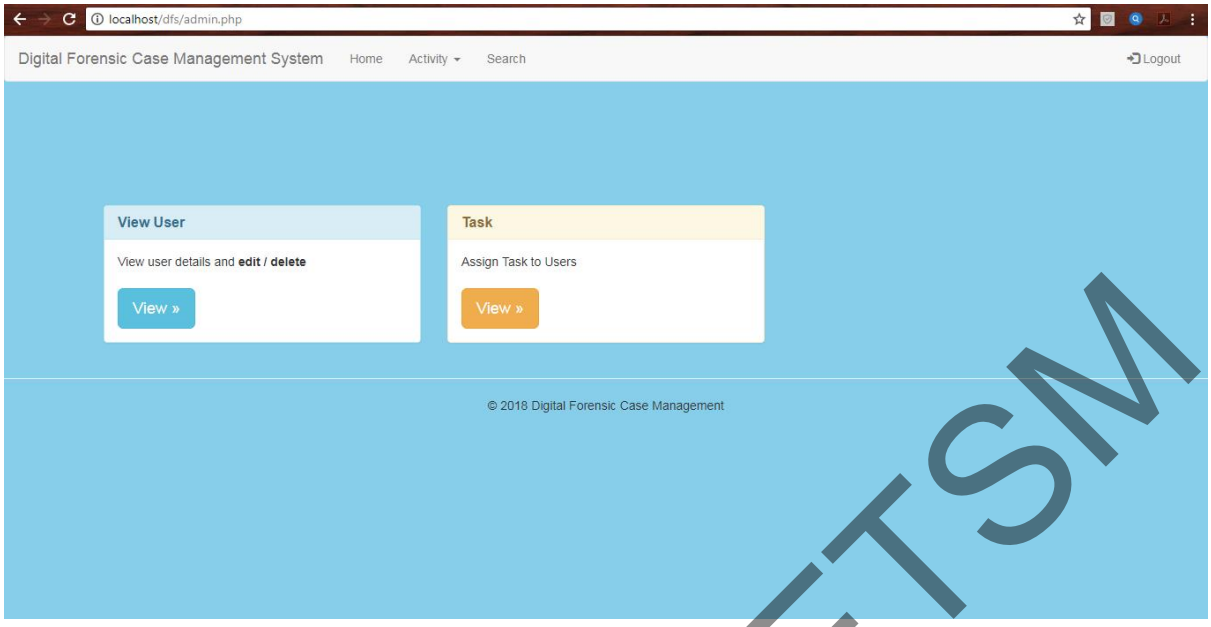
Rajah seterusnya merupakan halaman bagi menambah bukti baru dan melihat senarai bahan bukti yang telah disimpan di pangkalan data. Pengguna boleh menambah, mengubah dan memadam bahan bukti digital yang terdapat di dalam sistem ini.

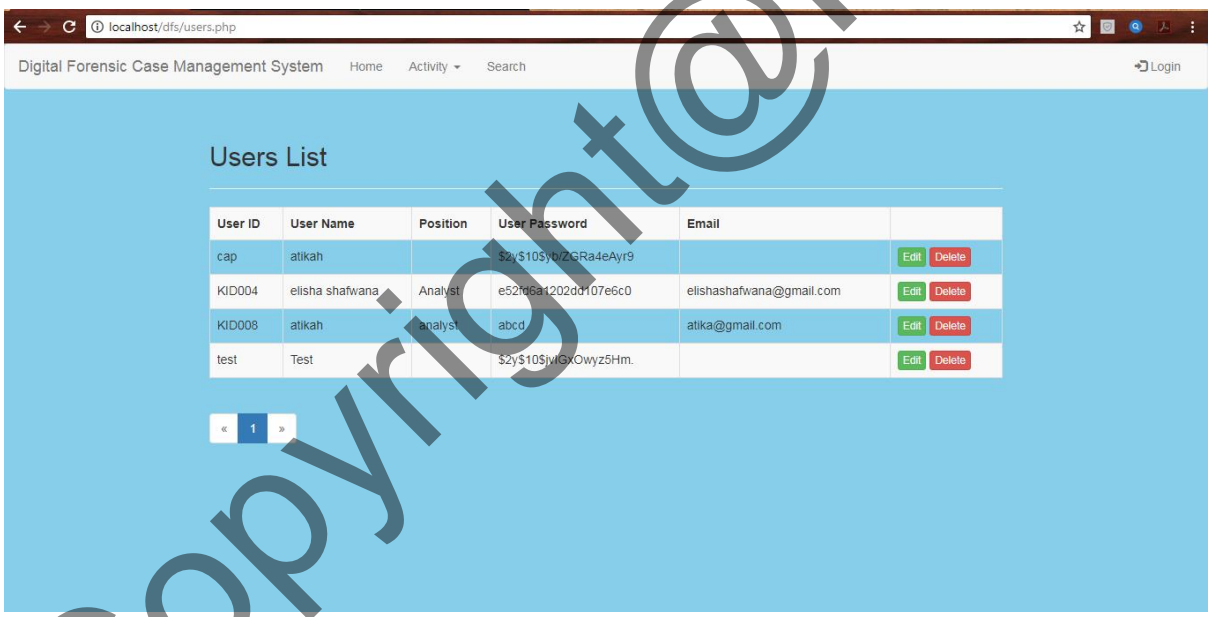


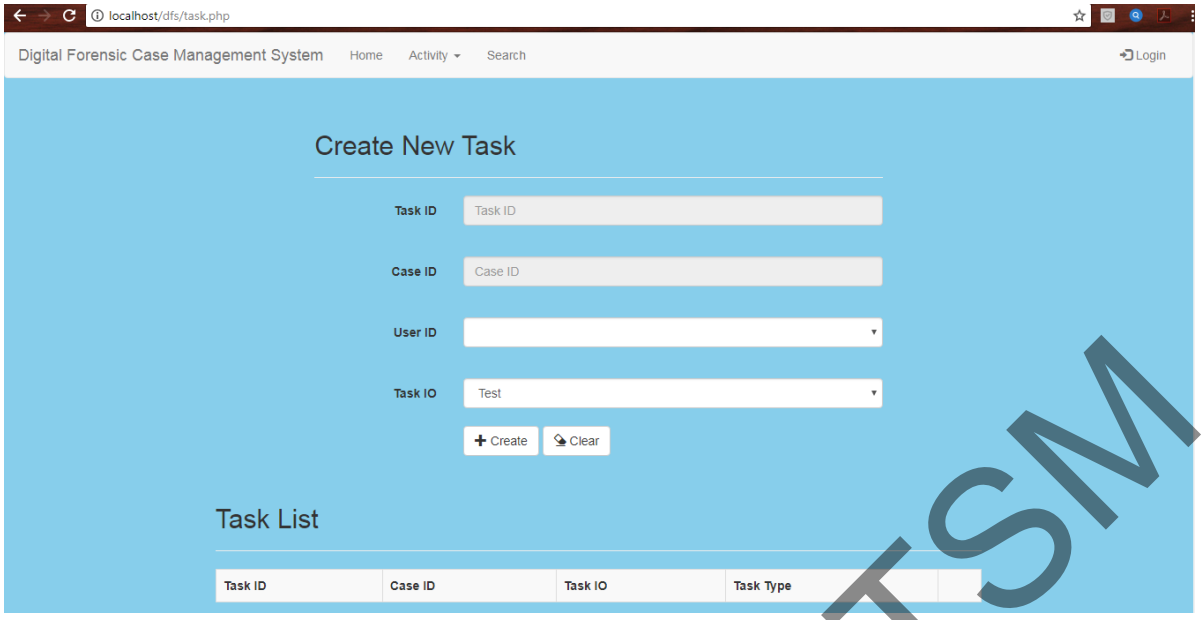
Rajah diatas menunjukkan antarmuka menambah tugas dan senarai tugas. Halaman ini hanya boleh diakses oleh juruteknik yang bertindak sebagai admin untuk menentukan memberikan tugas kepada *Investigator Officer* (IO) untuk mengambil alih kes siasatan.



Rajah di atas menunjukkan log masuk bagi admin iaitu pegawai teknikal. Tugas admin antaranya ialah *view user* dan menambah tugasan kepada pengguna.







6 KESIMPULAN

Pembangunan sistem web pengurusan kes forensik digital menggunakan sekuriti VPN ini berjalan dengan lancar walaupun menghadapi pelbagai masalah dan kekangan. Walaupun terdapat beberapa masalah yang dihadapi semasa fasa pembangunan, dengan bantuan penyelia, rakan-rakan dan teknologi, masalah berjaya diatasi.

Secara keseluruhannya, Sistem Pengurusan Kes Forensik Digital menggunakan *Virtual Private Network* (VPN) telah berjaya dibangunkan kerana telah memenuhi skop kajian. Walaupun terdapat beberapa kelemahan dan kekangan tetapi semuanya dapat diaatasi dengan baik. Kelebihan dan kekurangan sistem juga telah dikenalpasti. Oleh itu, penambahbaikan perlu dijalankan untuk menghasilkan sebuah sistem yang sempurna dan dapat memenuhi kehendak pengguna.

RUJUKAN

Boddington, R. (n.d.). Digital Evidence. Emerging Forensic Tools for Locating and Analyzing Digital Evidence,958-1671. doi:10.4018/978-1-4666-9591-7.les2

Prayudi, Y., & Ashari, A. (2015). A Study on Secure Communication for Digital Forensics Environment [Abstract]. International Journal of Scientific and Engineering Research, 6(1), 1036-1043. doi:10.14299/ijser.2015.01.010

Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common Phases of Computer Forensics Investigation Models. International Journal of Computer Science and Information Technology, 3(3), 17-31. doi:10.5121/ijcsit.2011.3302

Perumal, S., & Norwawi, N. M. (2010). Integrated computer forensic investigation model based on Malaysian standards. International Journal of Electronic Security and Digital Forensics, 3(2), 108. doi:10.1504/ijesdf.2010.033780

(2015) A Study in Secure Communication for Digital Forensics Environment. 6:\

ITAR, ABD. AZIZ. “Jabatan Digital Forensik MCMC Kemuka Bukti Forensik Bantu Siasatan Kes Jenayah Digital.” Utusan Online

Nurelisha Shafwana Binti Mohd Ghazali (A155844)
Khairul Akram Zainol Ariffin
Fakulti Teknologi & Sains Maklumat,
Universiti Kebangsaan Malaysia