SISTEM PENGURUSAN FORENSIK DIGITAL

NOR SHAHIRA ISMAIL
KHAIRUL AKRAM ZAINOL ARIFFIN

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Jenayah siber menjadi sebuah ancaman yang sangat serius di sebalik perkembangan teknologi yang pesat. Forensik digital merupakan prosedur penyiasatan terhadap komputer dan peranti digital seperti telefon bimbit, kamera litar tertutup dan sebagainya. Sistem ini dibangunkan atas dasar permasalahan yang timbul di mana terdapat permasalahan dalam mengendalikan kes kerana kebanyakan organisasi tidak mempunyai pengurusan yang berpusat dalam pengendalian kes forensik digital. Ini menyebabkan pihak yang terlibat dalam pendakwaan juga tidak dapat memantau perkembangan kes. Oleh itu, sistem berdasarkan web ini dibangunkan sebagai platform bagi sistem berpusat yang khusus dalam pengurusan forensik digital. Metodologi yang digunakan untuk membangun sistem ini ialah *System Development Life Cycle* yang merangkumi fasa perancangan di mana objektif, skop dan penyataan masalah dikaji untuk mengetahui tujuan sistem dibangunkan. Dalam fasa analisis, proses pengumpulan data dan bahan dimuatkan ke dalam sistem yang telah dibangunkan. Fasa seterusnya ialah fasa rekabentuk di mana model sistem yang menggambarkan sistem sebenar direka menggunakan *Justinmind*. Dalam fasa implementasi dan pengujian, peralihan sistem daripada pembangunan kepada pengeluaran dan pengguna akhir membuat pengujian terhadap sistem. Sistem berjaya dibangunkan mengikut spesifikasi yang telah dirancang dan mencapai objektif. Sistem ini diharapkan dapat memberi kemudahan kepada mana-mana organisasi yang memerlukan.

1 PENGENALAN

Di sebalik perkembangan teknologi yang pesat, jenayah siber menjadi sebuah ancaman yang cukup serius. Perkembangan pesat komputer dan telefon bimbit telah menyebabkan alatan peranti ini digunakan dalam aktiviti-aktiviti jenayah seperti menyalin perisian secara tidak sah, penyebaran virus dan menyalur maklumat palsu. Forensik digital adalah prosedur penyiasatan terhadap komputer dan peranti digital seperti telefon bimbit dan kamera litar tertutup.

Menurut *Ken Zatyko* dalam *Forensic Magazine,* forensik digital didefinisikan sebagai "Aplikasi komputer sains dan prosedur siasatan untuk tujuan siasatan yang melibatkan analisis bukti digital selepas carian yang betul oleh pihak berkuasa, rantaian pergerakan ekshibit, dengan pengesahan matematik, penggunaan alat-alat yang disahkan, pengulangan, laporan dan pembentangan pakar," (Mohay 2003)

Teknologi hari ini dapat membantu sesebuah organisasi untuk mengendalikan sebuah makmal *virtual* dengan pemeriksa dan pusat repositori bukti yang terletak di lokasi geografi

berasingan. Pengaturan ini mempunyai beberapa kelebihan termasuk penjimatan kos, pengaksesan sumber maklumat yang lebih luas dan meningkatkan kepakaran serta mengurangkan penduaan sumber maklumat yang tidak perlu.

Sistem Pengurusan Forensik Digital ini dibangunkan bertujuan untuk menyelesaikan permasalahan dalam merekod data kes-kes jenayah digital yang diterima. Oleh yang demikian, sistem ini menyediakan alternatif bagi penyimpanan data dan pengurusan. Melalui sistem ini juga data-data yang diterima akan direkodkan secara langsung ke dalam sistem bagi menjamin keselamatan data dan maklumat yang diperolehi.

2 PENYATAAN MASALAH

Permasalahan ini dibincangkan kerana setiap aktiviti yang dijalankan ke atas kes siasatan seperti membuat catatan kes, menulis laporan dan pengumpulan bahan bukti dilakukan secara manual. Pada masa yang sama, pegawai penyiasat dan juru analisis juga perlu mengisi borang secara manual bagi membuat laporan kes. Namun begitu, terdapat kelemahan dalam proses pengumpulan data kejadian jenayah yang berlaku kerana aktiviti yang dijalankan masih menggunakan kaedah di mana setiap data direkodkan secara manual. Sistem Pengurusan Forensik Digital ini dibangunkan bertujuan untuk menyelesaikan permasalahan dalam merekod data kes-kes jenayah digital yang diterima oleh sesebuah organisasi yang berkenaan. Hal ini akan menyebabkan rekod laporan mudah hilang dan kurang kecekapan dari segi pengurusan.

Selain itu, proses siasatan forensik digital juga mengambil masa yang lama sebelum kes di bawa ke mahkamah dan proses dakwaan kes juga melibatkan beberapa pihak pakar seperti ejen penguatkuasa undang-undang, pendakwa, ejen persendirian dan penganalisis. Hal ini akan menyukarkan pihak pakar apabila kes dibangkitkan semula tetapi maklumat tentang kes tidak ditemui. Begitu juga dengan bahan bukti yang telah diklonkan dan diimejkan, ianya hilang setelah lama disimpan kerana kecekapan peosedur yang lemah. Ini menyebabkan kes siasatan perlu dijalankan semula dari peringkat awal dan perkara yang sama juga mungkin berulang sepanjang tempoh dakwaan.

Di samping itu, tiada sistem berpusat di mana pihak yang terlibat tidak boleh memantau perkembangan kes. Pada masa yang sama, pihak berkuasa yang terlibat juga tidak mendapat

sebarang informasi secara terus tentang perkembangan kes. Hal ini menyebabkan pihak tersebut perlu melakukan banyak tugas seperti merujuk kepada pihak lain dan mencari pihak yang bertanggungjawab mengendalikan kes untuk mendapatkan informasi berkenaan kes dakwaan tetapi kes masih tidak selesai.

3 OBJEKTIF KAJIAN

Projek ini bertujuan untuk mewujudkan sebuah sistem berpusat bagi sesebuah organisasi yang memerlukan dalam mengendalikan kes forensik digital. Secara umum objektif kajian adalah untuk membangunkan sebuah Sistem Pengurusan Forensik Digital yang mempunyai sebuah pangkalan data bagi menyimpan data dan maklumat berkaitan kes. Sistem berdasarkan web ini juga dibangunkan sebagai platform sistem berpusat. Konsep ini dapat membantu meningkatkan kecekapan sistem pengurusan kepada lebih sistematik.

Kertas ini membincangkan tentang projek pembangunan sistem pengurusan forensik digital dan menjelaskan bagaimana sistem ini dibangunkan. Hasil pembangunan juga dibincangkan secara terperinci.

4 METOD KAJIAN

Rekabentuk sistem yang sesuai penting untuk memastikan perjalanan projek berjalan dengan lancar dan menjamin hasil kerja yang berkualiti. Antara muka grafik melibatkan beberapa fasa pembangunan dan ditambah dengan penggunaan perisian dan perkakasan yang bersesuaian. Fasa pembangunan termasuk fasa perancangan, analisis, reka bentuk, implementasi dan pengujian. Metod yang digunakan penting untuk memastikan perjalanan projek lancar dan teratur. Rajah 1 menunjukkan aliran pembangunan yang diguna untuk membangun dan mereka antara muka grafik sistem.

4.1 Fasa Perancangan

Fasa ini melibatkan proses pengenalpastian masalah, objektif, persoalan kajian dan menentukan skop. Langkah seterusnya adalah sorotan susastera yang melibatkan pengumpulan, pencarian dan pembacaan jurnal dan kajian lepas bagi mencetus idea dan inspirasi. Penggunaan internet untuk mencapai maklumat berkaitan. Maklumat dikumpul, distruktur dan disintesis dan dipersembah secara kritis dan kreatif dalam fasa analisis.

4.2 Fasa Analisis

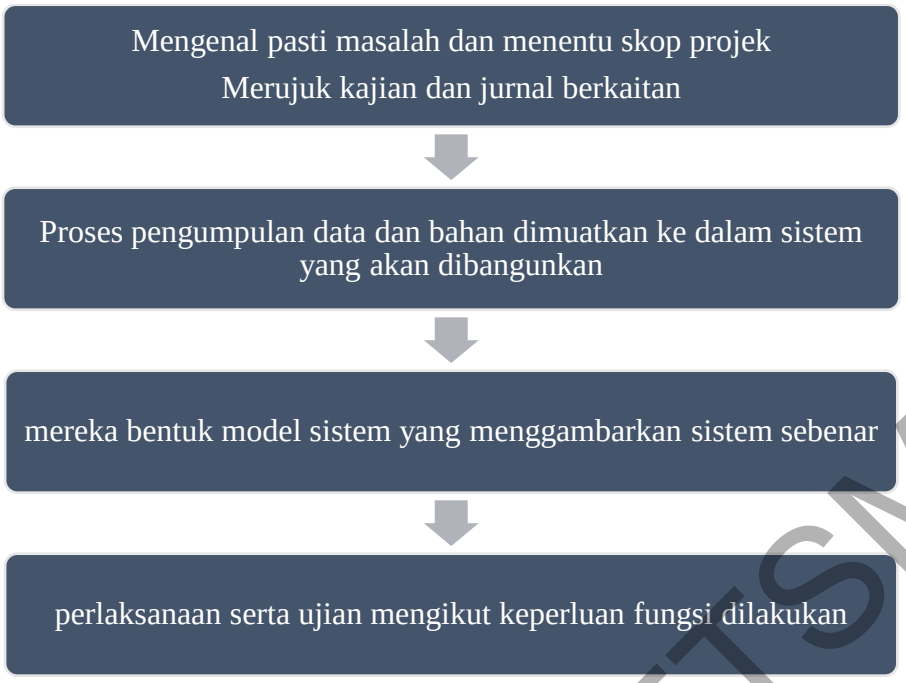
Fasa ini melibatkan analisis dan tafsiran maklumat yang dikumpul dalam fasa perancangan. Analisis tentang kesesuaian topik dan menilai kepentingan untuk menjalankan kajian ini dilakukan. Selain daripada itu, analisis tentang perkakasan dan perisian juga dijalankan untuk memasti perkakasan dan persisian yang sedia ada adalah sesuai untuk membangun projek ini.

4.3 Fasa Reka Bentuk

Fasa ini merupakan fasa yang penting dalam keseluruhan projek. Rekabentuk model sistem yang menggambarkan sistem sebenar, model konsepsual sistem, rekabentuk gambar rajah aliran data (DFD), reka bentuk pangkalan data dan carta alir yang dibangunkan bersesuaian dengan spesifikasi yang dikehendaki juga diterangkan dalam fasa ini. Fasa ini melibatkan proses penting, iaitu mereka bentuk antara muka sistem. Antara muka grafik direka dengan menggunakan Justinmind bagi menghasilkan antara muka sistem yang menarik.

4.4 Fasa Implementasi dan Pengujian

Pembangunan pangkalan data bagi sistem perlu dilaksanakan dengan teliti kerana pangkalan data merupakan tunjang kepada sesebuah sistem untuk berfungsi dengan baik. Pangkalan data yang digunakan ialah MySQL yang menjadikan laman web bersifat dinamik. Pengujian sistem dilakukakan setelah sistem siap dibangunkan dan pengguna akhir akan membuat pengujian terhadap sistem.



Rajah 1 Aliran pembangunan sistem

Perkakasan dan perisian yang diguna untuk membangun projek harus dipilih dengan teliti. Perkakasan dan perisian yang baik berfungsi dengan lancar serta menyokong pembangunan sistem. Pemilihan perkakasan dan persisian yang tidak tepat boleh menjejas hasil projek. Spesifikasi keperluan perkakasan yang diguna untuk menghasil antara muka grafik adalah perkakasan asas sesebuah komputer. Senarai spesifikasi keperluan perkakasan yang dicadang untuk menghasil antara muka grafik sistem pengurusan forensik digital ini ialah komputer peribadi, ruang simpanan 400GB, ruang memori 4GB RAM dan pemprosesan Intel Core i5.

Keperluan perisian pula merangkumi sistem pengoperasian, pelayar web, pangkalan data, dan perisian rekabentuk grafik. Perisian yang digunakan untuk pembangunan sistem ini ialah PhpMyAdmin. Pelayan pangkalan data digunakan untuk menyimpan data yang ditulis dalam kod bahasa PHP yang mengendalikan pentadbiran MySQL dengan menggunakan pelayar web dan lebih mudah untuk mengubah pangkalan data serta melaksana kenyataan SQL.

Apache merupakan aplikasi bagi memudahkan pembangun untuk menguji sistem yang sedang dibina. Apache merupakan salah satu *web container* yang paling popular di lingkungan pengaturcaraan web java. Apache juga berperanan sebagai penggerak yang menghubungkan php dan MySQL. MySQL merupakan satu aplikasi pengurusan pangkalan data sistem terbuka,

MySQL terkenal dengan kelajuan pemprosesan data, keselamatan dan fleksibel. Ia juga berperanan dalam pengurusan pangkalan data menggunakan kueri sql yang menguhubungkan pangkalan MySQL dengan php serta membuat hubungan kepada pangkalan data.

5 HASIL KAJIAN

Bahagian ini membincang hasil daripada proses pembangunan sistem pengurusan forensik digital. Penerangan yang mendalam tentang antara muka grafik sistem diperihalkan. Fasa reka bentuk adalah fasa yang penting dalam pembangunan projek. Dalam projek ini, antara muka sistem direka menggunakan Justinmind sebagai gambaran sebenar sistem pada peringkat awal. Antara muka kemudiannya dibina menggunakan atur cara HTML dan CSS bagi menghasilkan reka bentuk antara muka yang berfungsi mengikut spesifikasi yang telah ditetapkan. Seterusnya pengujian terhadap reka bentuk antara muka dijalankan untuk memasti hasil pembangunan adalah selaras dengan objektif yang ditetapkan sebelumnya.

Secara umumnya, sistem ini terbahagi kepada tiga modul. Antaramuka Sistem Pengurusan Forensik Digital melalui rajah yang ditunjukkan merupakan antaramuka sistem yang telah dibangunkan berpandukan reka bentuk antara muka sistem dan capaian objektif serta spesifiksasi fungsian yang telah ditetapkan.

Rajah 2 merupakan antara muka log masuk untuk pengguna bagi sistem ini di mana pengguna perlu memasukkan ID pengguna dan katalaluan yang sah untuk masuk ke dalam sistem. Rajah 3 menunjukkan pengguna telah memasukkan ID dan katalaluan yang tidak sah.

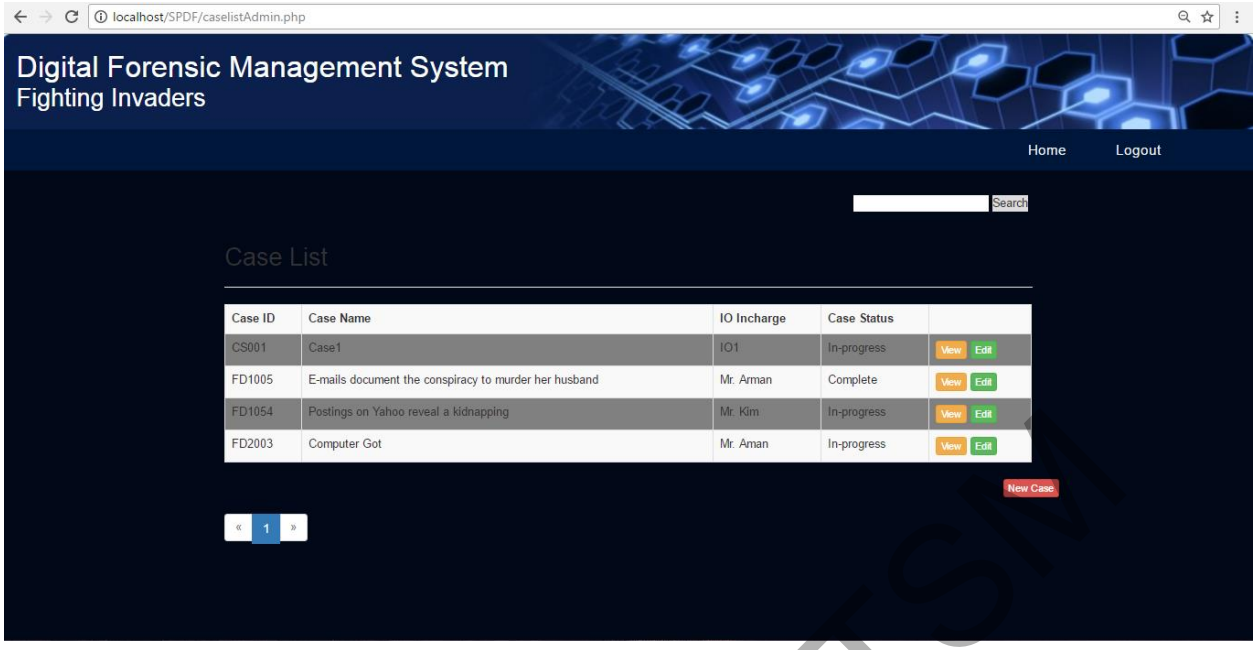
Rajah 2 Antara muka log masuk

Rajah 3 Antara muka tidak sah pengguna

Rajah 4 memaparkan antara muka halaman utama setelah pengguna berjaya masuk ke dalam sistem. Halaman ini terdapat tiga modul iaitu *cases*, *evidences* dan *task*. Pada halaman ini, pengguna juga boleh membuat penukaran katalaluan.

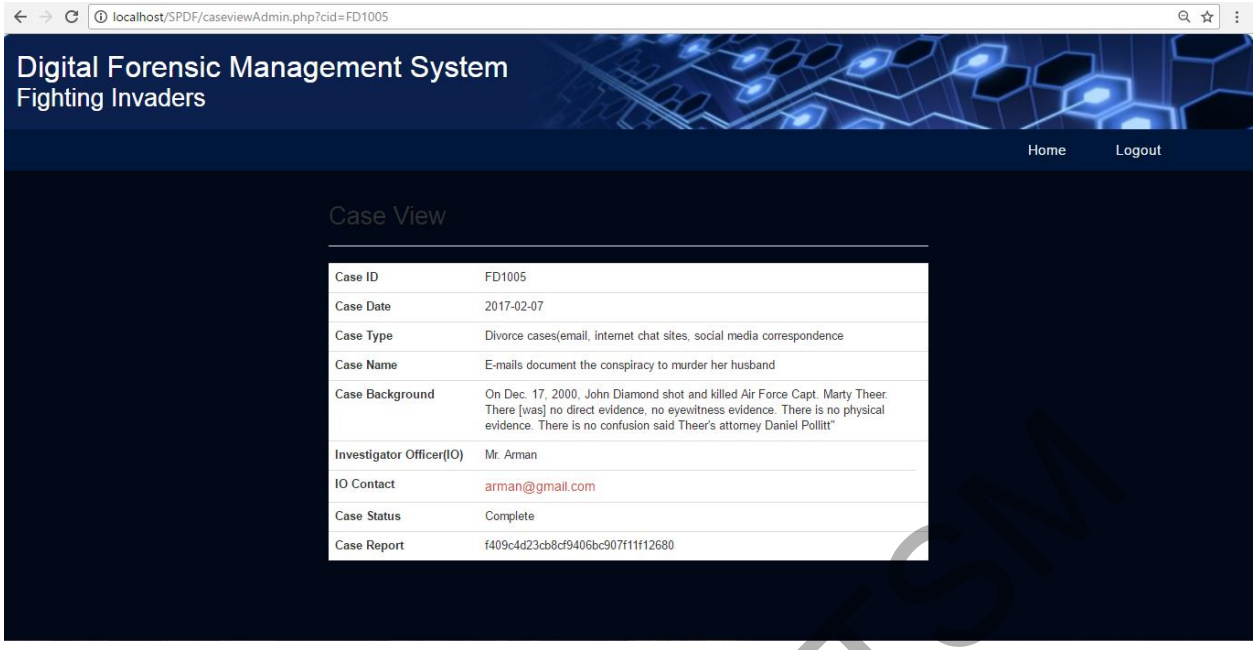
Rajah 4 Antara muka halaman utama

Rajah 5 halaman paparan senarai kes di mana pengguna boleh membuat paparan, kemaskini dan merekodkan kes baru.



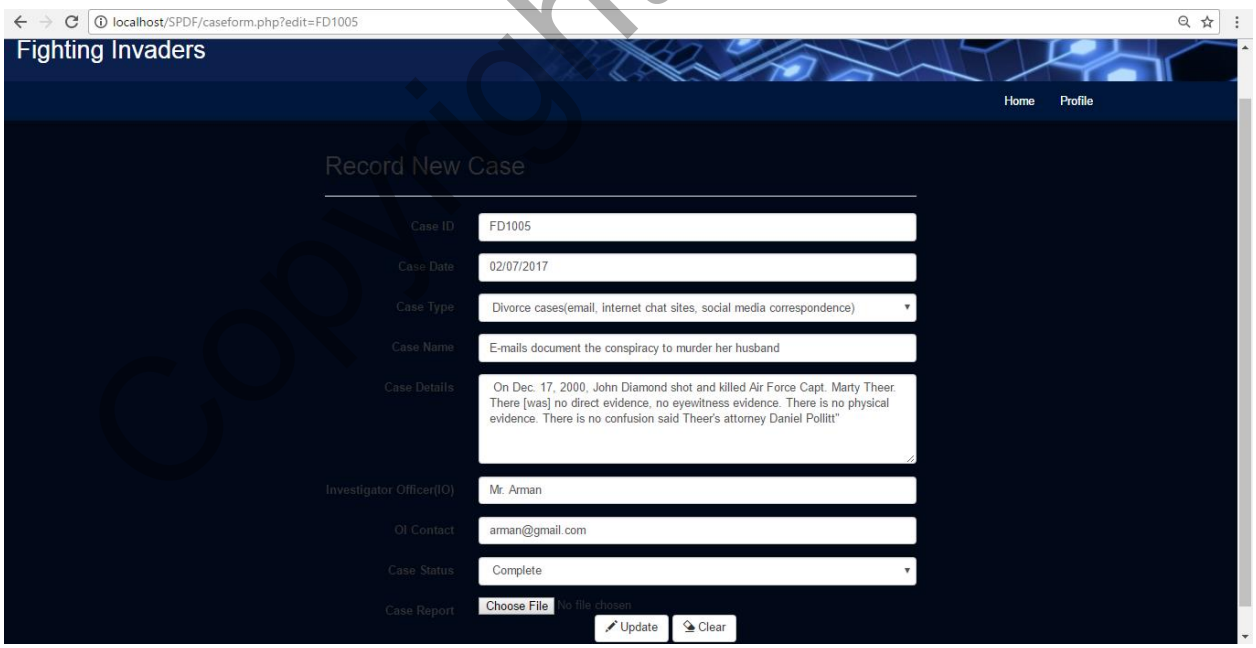
Rajah 5 Antara muka halaman senarai kes

Paparan halaman dalam rajah 5 merupakan paparan halaman di mana boleh membuat paparan, kemaskini dan merekodkan kes baru. Pengguna akan melihat halaman paparan kes seperti dalam rajah 6 sekiranya pengguna menekan pada butang *view* di mana halaman ini mengandungi butiran kes yang telah direkodkan. Seterusnya, pengguna perlu menekan atas butang *view* pada *case report* untuk melihat laporan kes. Pada halaman ini juga pengguna boleh membuat carian kes dengan menggunakan butang *search* di bawah navagasi bar. Sistem akan membuat carian setelah pengguna memasukkan kata kunci bagi carian yang ingin dibuat. Senarai kes merupakan domain bagi butang carian yang disediakan. Rajah 6 menunjukkan halaman paparan butiran kes di mana pengguna boleh melihat laporan kes



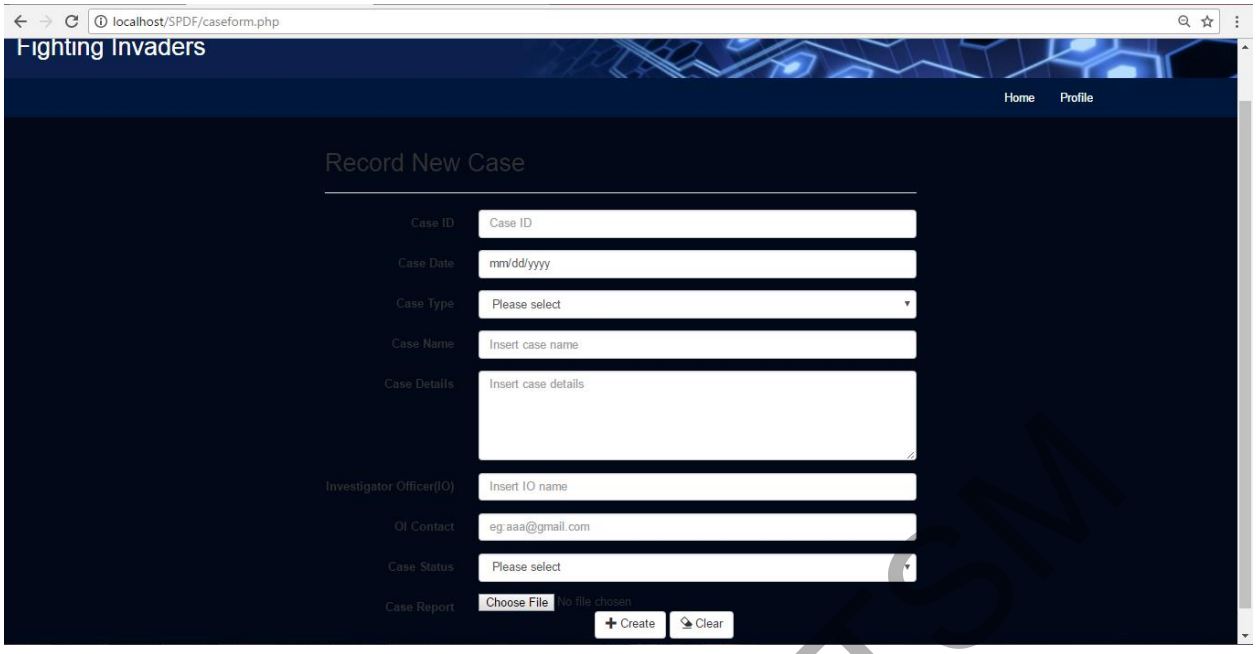
Rajah 6 Antara muka paparan kes

Rajah 7 menunjukkan halaman kemaskini butiran kes di mana pengguna boleh mengemaskini butiran kes sekiranya ada perubahan pada kes siasatan.



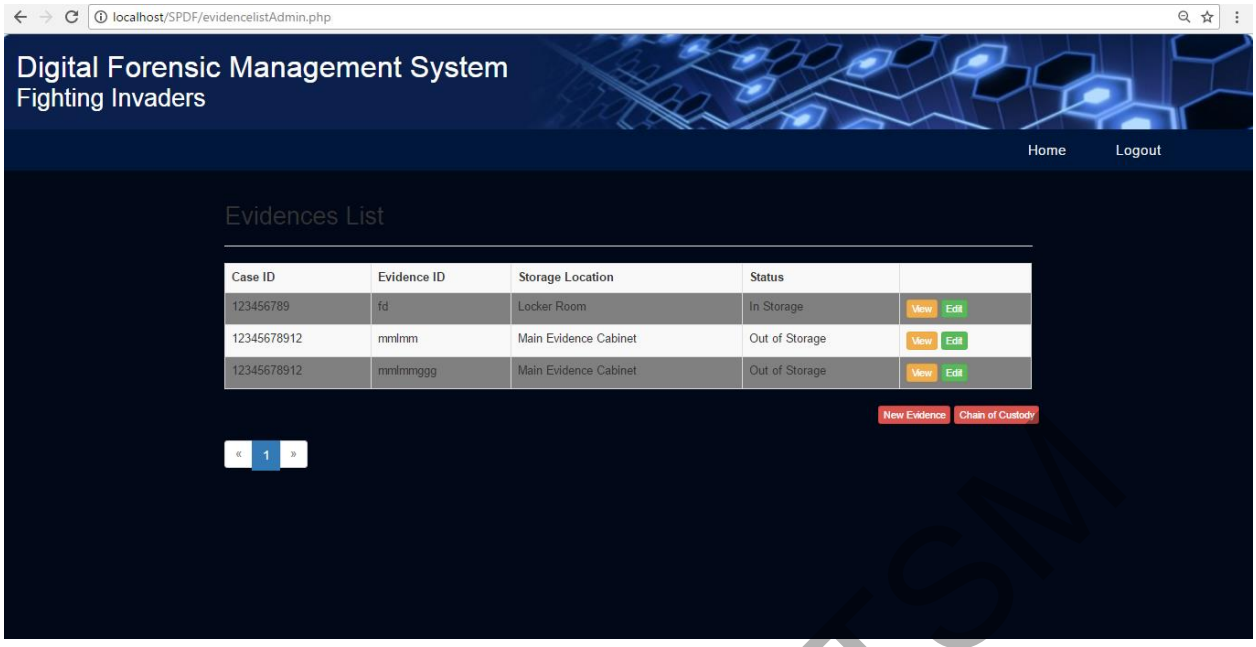
Rajah 7 Antara muka kemaskini kes

Rajah 8 menunjukkan antara muka halaman rekod kes di mana data kes dimasukkan dan laporan kes dimuatnaik.

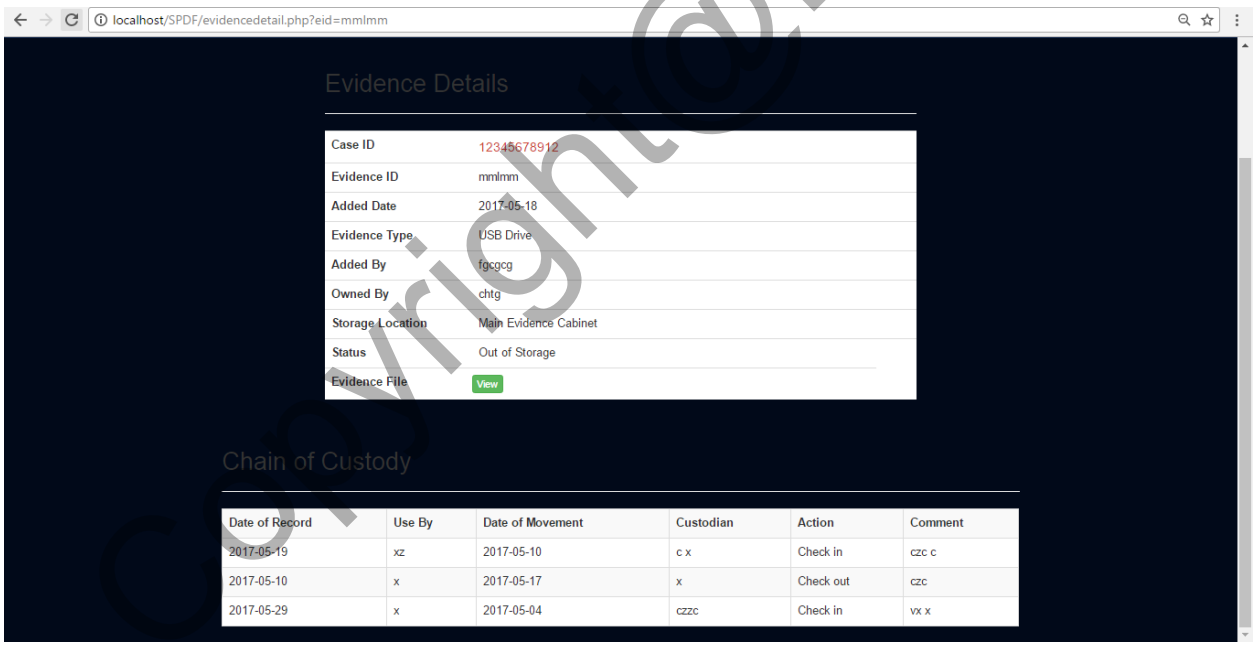


Rajah 8 Halaman rekod kes

Paparan halaman dalam rajah 7 merupakan paparan setelah pengguna menekan atas butang *edit.* Dalam halaman ini pengguna boleh mengemaskini butiran mahupun laporan kes sekiranya terdapat sebarang perubahan kes. Setelah selesai kemaskini dan menekan butang *update*, pengguna akan terima *pop-up* kemaskini berjaya dan pengguna akan kembali semula kepada halaman paparan senarai kes untuk papar semula kes yang telah dikemaskini. Seterusnya, pengguna akan pergi ke paparan halaman seperti dalam rajah 8 sekiranya pengguna menekan butang *new case* yang ada pada paparan senarai kes. Pada halaman ini pengguna boleh merekodkan kes baru dan memuatnaik laporan kes. Laporan kes yang telah dimuatkan naik akan di'hash'kan bagi menjaga integriti laporan. Pengguna akan kembali semula ke halaman senarai kes untuk memastikan kes berjaya direkodkan. Rajah 9 menunjukkan halaman senarai bukti dimana pengguna boleh merekod dan memuatnaik fail bukti seperti gambar, video dan audio.



Rajah 9 Antara muka halaman bukti

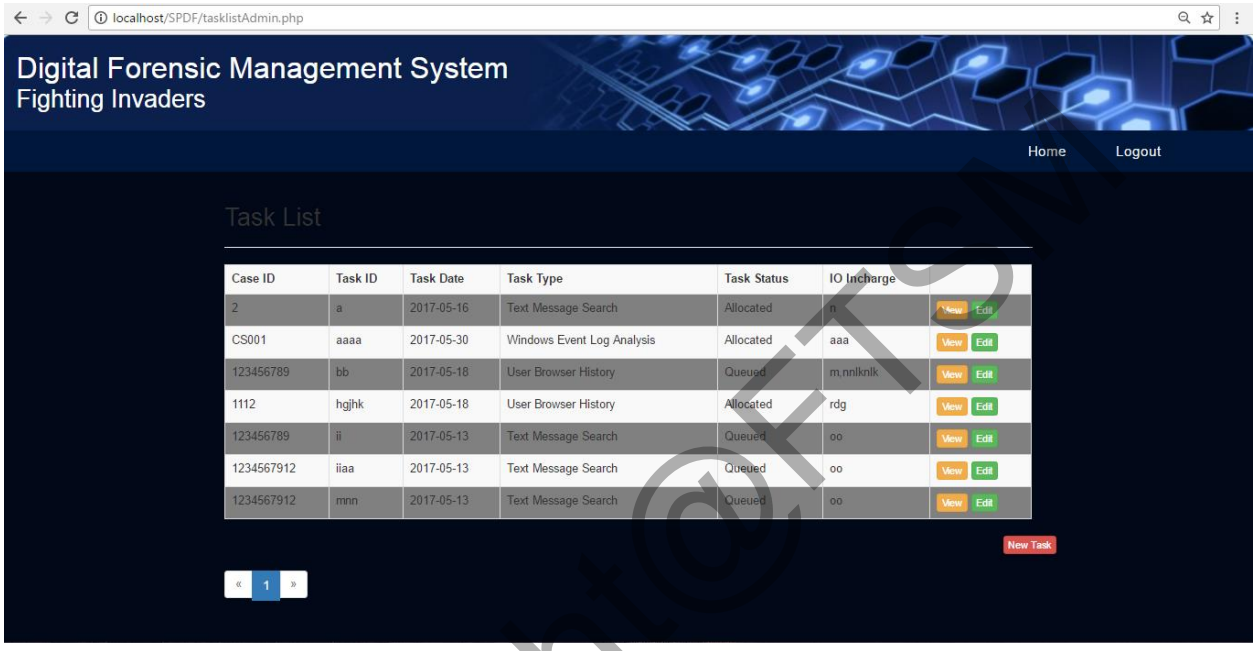


Rajah 10 Antara muka butiran bukti

Pada halaman rajah 9 menunjukkan paparan senarai bukti yang telah direkodkan. Pada halaman ini juga pengguna boleh membuat rekod bukti baru, memuatnaik bahan bukti dan membuat senarai rantaian jagaan di mana aktiviti antara pihak yang terlibat semasa bahan bukti diserahkan. Fail bahan bukti yang telah dimuatnaik akan ditukarkan ke dalam nilai 'hash' bagi memastikan ketelusannya. Rajah 10 menunjukkan butiran kes dan senarai rantaian jagaan bagi

setiap aktiviti penyerahan bahan bukti. Pengguna boleh menekan atas pautan ID kes untuk paparan butiran kes bagi maklumat butki yang dipaparkan.

Rajah 11 menunjukkan halaman paparan modul tugasan. Pada halaman ini pengguna akan menentukan pegawai yang bertugas untuk mengendalikan kes yang diterima. Pegawai yang menerima tugasan akan mendapat notifikasi melalui emel sebagai pemberitahuan.



Rajah 11 Antara muka senarai tugas

6 KESIMPULAN

Sistem Pengurusan Forensik Digital ini dijangka dapat membantu sesebuah organisasi dalam pengurusan kes forensik digital yang dikendalikan. Sistem ini juga berperanan sebagai sistem pusat yang berdasarkan web bagi membolehkan pengguna membuat pemantauan kes tanpa perlu berhubung dengan mana-mana pihak. Hal ini secara tidak langsung dapat meningkatkan lagi kecekapan pengurusan kes dan menjadi sistem pengurusan lebih sistematik di mana setiap data dan maklumat kes disimpan secara terus ke dalam pangkalan data.

Penggunaan aplikasi Apache dan localhost yang bertindak sebagai pelayan memudahkan lagi pembangunan sistem di mana pembangun tidak perlu memuatnaik fail atur cara ke dalam pelayan secara berulang kali sekiranya ada pembetulan pada kod atur cara setiap

kali diuji. Penggunaan bahasa atur cara HTML, PHP dan CSS yang mudah difahami juga memudahkan lagi pembangunan dan mereka antara muka grafik sistem.

RUJUKAN

Ademu, I. O., Imafidon, C. O. & Preston, D. S. 2011. A New Approach of Digital Forensic Model for Digital Forensic Investigation *2*(12), 175–178.

Carrier & Spafford. 2009. Digital Forensic Model Based On Malaysian Investigation Process.

CyberSecurity Malaysia | An Agency Under MOSTI. (n.d.). http://www.cybersecurity.my/en/our_services/digital_forensics/main/detail/2326/index.html [5 November 2016].

Mohay, G. M. 2003. *Computer and intrusion forensics*. Artech House. Retrieved from http://www.forensicmag.com/article/2007/01/commentary-defining-digital-forensics

Tanimoto, S. & Kakuta, T. 2015. A Study of Cost Structure Visualization for Digital Forensics Deployment. doi:10.1109/ACIT-CSI.2015.80

Tellefsen, A. 2012. Government Cloud Computing : Requirements , Specification and Design of a Cloud-Computing Environment for Police and Law Enforcement.