PENGESANAN PAKET RANGKAIAN UNTUK FORENSIK MEMORI

NOR NADIA ABDULLAH MARZUKI
KHAIRUL AKRAM ZAINOL ARIFFIN

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Forensik memori adalah analisis fail *memory dump* komputer yang merupakan satu fail yang isi kandungannya didapati daripada RAM yang mengandungi segala maklumat atau data yang digunakan oleh komputer termasuklah data sensitif. Cakera keras tidak menyimpan data sensitif dan penganalisisannya tidak dapat menghasilkan maklumat yang berharga. Pengumpulan maklumat daripada servis komputeran awan sukar kerana pihak servis tidak mahu kongsikan atau memberikan maklumat yang salah. Aplikasi pemantauan rangkaian boleh menghadapi ralat semasa operasi dan menghasilkan maklumat yang tidak tepat atau gagal untuk menyimpankannya. Projek ini adalah untuk membangunkan satu alat yang dinamakan *Trazador*. Alat ini akan menganalisis fail *memory dump* untuk mengesan paket rangkaian bagi mendapatkan data sensitif. Maklumat yang akan difokuskan adalah mengenai sambungan rangkaian lepas dan semasa. Protokol HTTPS dan TCP adalah protokol penting dalam pendekatan ini. *Trazador* berupaya untuk mendapatkan maklumat mengenai paket rangkaian. Pengujian yang dilakukan membuktikan bahawa paket rangkaian yang dikesan oleh *Trazador* membawa kepada maklumat mengenai laman web yang digunakan. Walau bagaimanapun, *Trazador* tidak dapat menyahsulitkan data yang disimpan dalam paket rangkaian kerana adanya protokol SSL. Untuk penambahbaikan, kajian terhadap algoritma RSA perlu dijalankan.

1 PENGENALAN

Rangkaian forensik merupakan cabang sains forensik yang berurusan dengan memantau dan menganalisis trafik rangkaian komputer bagi tujuan pengumpulan maklumat, bukti sah atau pengesanan pencerobohan. Forensik rangkaian secara tradisi digunakan untuk persekitaran berwayar dan difokuskan pada Protokol Internet Versi 4(*Internet Protocol version 4* – Ipv4) dan protokol yang berkaitan di lapisan rangkaian Protokol Kawalan Penghantaran/Protokol Internet (*Transmission Control Protocol/Internet Protocol* - TCP/IP).

Forensik memori adalah analisis fail longgokan ingatan (*memory dump*) komputer. Setiap maklumat atau data yang digunakan oleh program komputer akan melalui Ingatan Capaian Rawak (*Random Access Memory* - RAM) pada masa ia digunakan, maklumat ini akan terkandung dalam fail *memory dump* itu. Maklumat dalam RAM yang dijadikan focus kajian ini adalah mengenai sambungan rangkaian lepas dan semasa iaitu yang berkenaan dengan alamat Protokol Internet (*Internet Protocol - IP*) dan alamat Kawaln Capaian Media (*Media Access Control - MAC*). Data tersebut boleh mengandungi maklumat sensitif dan ini menjadikan RAM begitu penting ketika menjalankan forensik komputer. Salah satu protocol rangkaian yang memastikan komunikasi antara komputer dalam rangkaian adalah protokol TCP/IP. Protokol ini berhierarki protokol yang mempunyai tanggungjawab yang berbeza-beza.

Dalam kajian ini, hanya Protokol Pemindahan Hiperteks Selamat (*Secure Hypertext Transfer Protocol* - HTTPS) dan Protokol Kawalan Penghantaran (*Transmission Control Protocol* – TCP) diberi tumpuan.

2 PENYATAAN MASALAH

Alat forensik yang sedia ada memeriksa media, misalnya cakera keras yang diperolehi, untuk alamat e-mel, alamat laman web, dan nama domain. Biasanya alat ini berfungsi dengan memasuki *strings* yang boleh dicetak menggunakan *keyword* dari cache pelayar web, mesej e-mel, dan sebagainya. Pendekatan ini menimbulkan masalah kerana data sensitif tidak disimpan di dalam cakera keras (Joshi & Pilli, 2016).

Penggunaan servis komputeran awan boleh menimbulkan masalah ketika proses forensik dijalankan kerana sukar untuk mengumpul log yang dihasilkan. Antara sebabnya ialah semasa mendapatkan maklumat daripada pembekal perkhidmatan awan itu mungkin pihak tersebut tidak memberikan maklumat yang tepat ataupun menahan beberapa maklumat penting (Joshi & Pilli, 2016).

Aplikasi pemantauan rangkaian hanya boleh menunjukkan jenis data tertentu dan mungkin memperkenalkan ralat atau membuang maklumat dengan tidak sengaja semasa operasi. Apabila menangkap trafik rangkaian, kerugian boleh berlaku di beberapa tempat seperti kad antaramuka boleh jatuhkan paket atau program yang digunakan untuk menangkap trafik rangkaian boleh menjadi *overloaded* dan gagal untuk mengekalkan semua paket yang ditangkap oleh kernel (Casey, 2002).

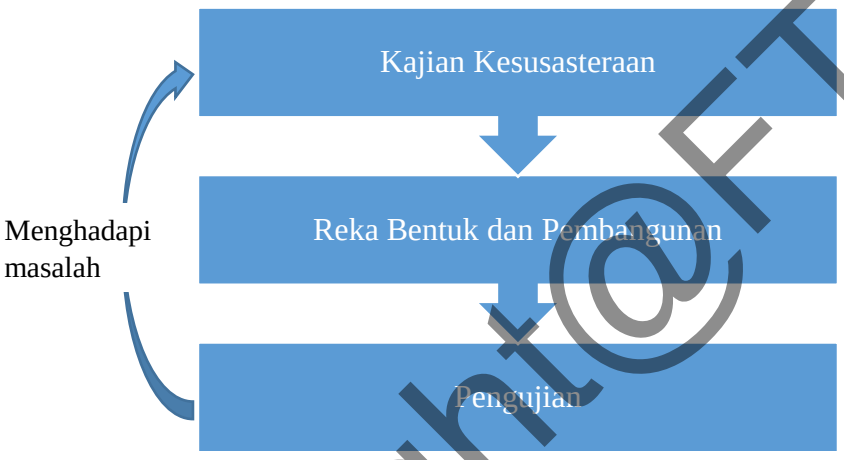
3 OBJEKTIF KAJIAN

Tujuan kajian ini adalah untuk membangunkan satu alat yang boleh mengesan paket rangkaian bagi mendapatkan data sensitif. Terdapat beberapa objektif yang disenaraikan sebagai garis panduan bagi memastikan kelancaran dan keberkesanan kajian ini. Objektif pertama ialah kebolehan alat ini untuk menganalisis fail *memory dump*. Kedua ialah pengesanan paket rangkaian melalui penganalisisan fail tersebut. Ketiga ialah memperoleh data sensitif daripada

penganalisisan paket rangkaian. Objektif terakhir ialah mamaparkan maklumat paket rangkaian kepada pengguna.

4 METOD KAJIAN

Metodologi kajian untuk mengesan paket rangkaian dalam fail *memory dump* untuk forensik memori melibatkan beberapa fasa iaitu fasa kajian kesusateraan, fasa reka bentuk dan pembangunan, dan fasa pengujian. Rajah 1 menggambarkan metodologi yang diguna untuk membina alat pengesanan paket rangkaian.

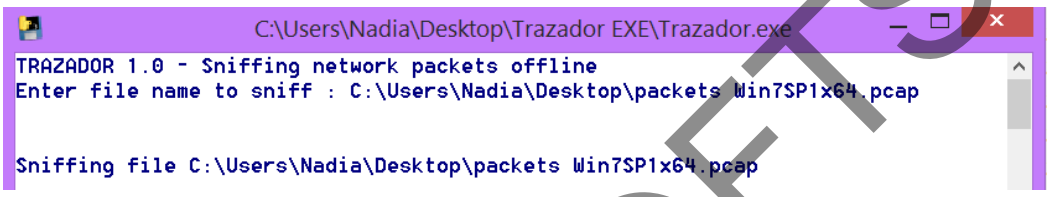


Rajah 1 Metodologi pembangunan alat pengesanan paket rangkaian

Fasa kajian kesusateraan berkait dengan kajian terhadap teori, artikel, dan sistem atau alat yang sedia ada yang berkaitan dengan kajian ini. Fasa reka bentuk dan pembangunan bertujuan untuk menentukan dan menggambarkan semua aspek penting mengenai pembangunan alat seperti bahasa pengaturcaraan yang digunakan, antaramuka alat yang dibangunkan serta kaedah pemprosesan yang digunakan. Setelah aspek-aspek tersebut ditentukan proses pembangunan alat dimulakan. Fasa pengujian akan dijalankan berulang kali untuk memastikan semua komponen yang terlibat boleh berfungsi dengan baik dan memenuhi objektif kajian. Sekiranya menghadapi masalah, imbas kembali fasa kajian kesusateraan bagi membuat penambahbaikan kajian yang mendalam.

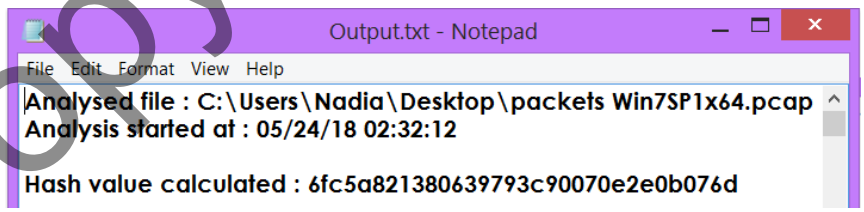
5 HASIL KAJIAN

Bahagian ini membincangkan hasil kajian pembangunan alat pengesanan paket rangkaian. *Trazador* dibangunkan menggunakan bahasa pengaturcaraan *Python*. Antara mukanya adalah mudah dan hanya memerlukan fail yang ingin dianalisis sebagai input. Apabila *Trazador* mula memproses fail, satu mesej akan dipaparkan untuk memberitahu pengguna bahawa fail tengan dianalisis, "*Sniffing file …*". Rajah 2 menunjukkan antara muka *Trazador* semasa ia memproses fail. Alat ini akan ditutup secara automatik apabila selesai pemprosesan dan fail output akan terletak di direktori root *Trazador* dengan nama fail, *Output.txt*.



Rajah 2 Antara muka *Trazador* semasa pemprosesan fail

Berdasarkan fasa pengujian, *Trazador* dapat memperoleh maklumat mengenai paket rangkaian yang berada dalam fail *memory dump*. Rajah 3 menunjukkan permulaan fail output yang merekodkan nama fail yang dianalisis, tarikh dan masa penganalisisan dan nilai *hash* fail. Butiran setiap struktur data seperti Bingkai Ethernet, Paket IP dan Paket TCP direkodkan dalam fail output, ini ditunjukkan dalam Rajah 4.

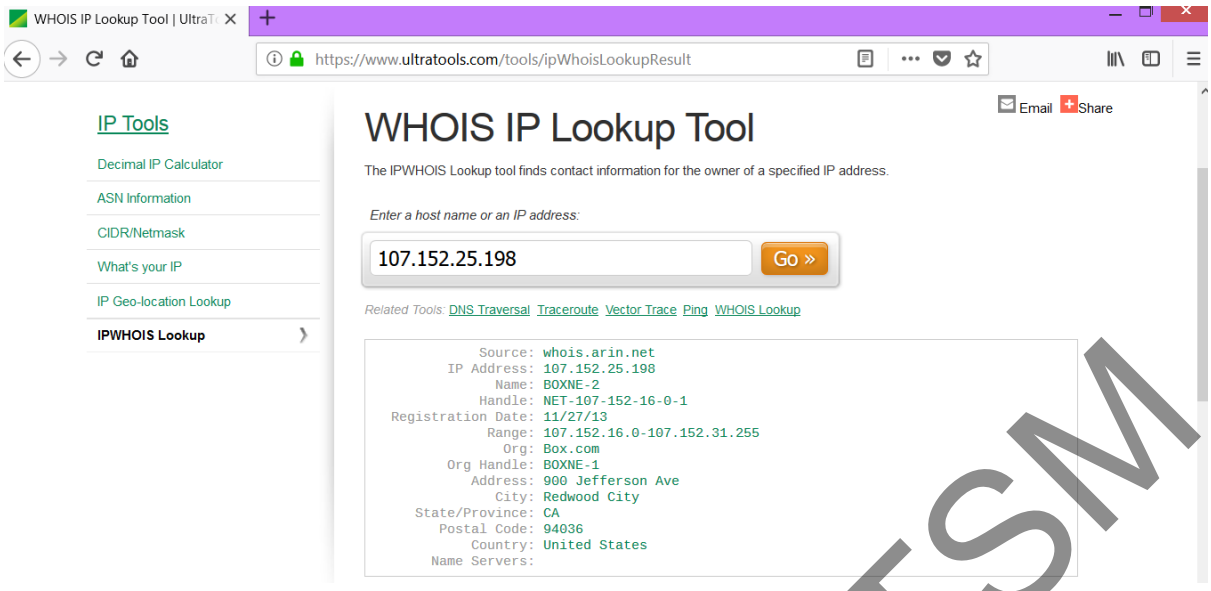


Rajah 3 Permulaan fail *Output.txt*

```
Ethernet Header :
Destination MAC : 0:12:41:17:14:15
Source MAC : 0:80:86:22:23:18
Protocol : 8

IP Header :
Version : 4
IP Header Length : 5
TTL : 128
Protocol : 6
Source Address : 107.152.25.198
Destination Address : 192.168.163.128

TCP Header :
Source Port : 443
Dest Port : 49707
Sequence Number : 1433963373
Acknowledgement : 3718659530
TCP header length : 5

Data : b'\x17\x03\x03\x02\xa0\x01\xf2U!\x04\x14j\xbc\n\xacf\x8e\x9b\xb7\xb2\x10\x9e\xd5\xcfj\xe7\xeae6$%h\xc6\f\xa6\xd6\x91\x9e\xedF
\xe8,\xbd\xc8\xe7e,\x9a\xe0\xd8a\xfb\xe9e\f/\x1f\xb2c?RK\x16\xd3\x94"\x85\x19\xe8\xb4f\xf5\x1f\xc3\xfdQT\xc2\xbb4\x1f@q\xd8EJ\x86cI
(\xb3}X -\x17\xdaI\x96\xb3\x1b\x95\xa1\x85C\xb5d\x8f\xdc\xb9C\x15\x1b\x9e.\x95\xba0\xc3\xcd\x94\xe5Aq\xf6\xfe\x00D\x86l\xba\xea
\x7f\xf9\xd3l\xe1\xcd\xf5\xe7io\x10\r$\xd3\xf4\xa5\x90\x19s3y\x03\xf6\xb3\x16\x15\xb4\x19r\xdf\xa7H)\xe7\rf(\x1cu\xd7\xff\xa2 \xd7\x89/
\x9a\x86P\xfa\x91~\x9f\xc4\x0bw\x16\xaa\x16-\x1e\xf1\xf1\x8aO\xc9gN\xd9\x81\x95\xa9~T\xbba8\f_\x1e\x16l\xb8\xb6\xc7W\x8fx\xa0\x9a
\xeb\xcd\x8d\x1e\x08\x87\xbf[\xb2\x13\xa4\xe0\xc4\xde\xabU2\xb8\x91XUn\x1a\xb67\xef\xe4%BPP\x0c\xa9\xe5|`?\xc9a\x1b~\xed, \xef
\xaa\x99\xd9#\xff\xde\'\x11\x8d(\r\xa8o\x1c\x8c6\xfb\xc9W\x888\\\xc8\xc1\x1d\x1b\x85,"}U\xe3y\xeb;\x00\xcb,W\x8f? \x00\x01R\xf1k
\xc7vh\xf5=\xd2!\x08\xc4D\xdf=P7\xac\x19i\x84"X\xd7\xfcX\x8a\xee\x14N\x91r\xc5\xec\x83 \x0f\xf1\xf2\x91W
\xb6\x03\x1cEG6\xc1\xc7\xc6\xa3{\xc5\xd0\xd7\x11\xf5\n\x99\xfb\xd9\xc2\xd3X\xa3:n8!\xee\x90u\x19\xeb\x94\x86y\xb7h\xafL\xcb
\xc85\x1f =\x1a>\xfd\x05i\x07+\x8d\x1bTY\xfb\x90\xb0\xa1B\xde\xbcr\x99\xce\xd4\x8bA\xe0\x9d\xf9G\x80\xd3\xb2xiee\xc5p
\xd18\xf3\xd1\xb0\xbdrv&\xb8\"\xd2\x8b\xf6$\xf9\xd8\x8aX\x93f\`3\x80\x80:\xb5\xf8\xd6\xc4\xcdJ`\xe7\xe0\xeb\xc3\xd38\xcc{6\xe6\xfbn
\xcf\xb2I\xcb6\xe9Pi\xff\xd2\x1f\n\x993m\x1b\xf5\xb1aB\xcd\xb7\x8c+\x8d?&\x8bV\xbb\xf0\x89TLK\x142sM\xef\xc2\x81\xc0\xc3`\xd7\'\xfe{L
\xd6\x93\xf5\xb5\xceG\xc3\x04f|?\x12\xc4?P\xe5p\x0fM \x11\x18\x86\x9d\x8b\xaae.\xecK2@\x91\'\xd33\x1ah\x87\x16Z\x88r\xbd|mw\r
\xf7\x0f"\x13NaTw[B\xed\x01\xc7\x95\x82\xd5\xe7@2\xe0K\xf0\x01\x1c^}\xdb\xcepk\x85\xb6\x14vD\xc4\x91M\x93c`\x97m\xab\xe9\xe3\x8b
\xab\x1f\x9c}\xce\xd6#\xa4\xf6QE{8\x17?\xeb\x11\x0bF\x9a,\xd8\x9e\x86\x0c\x01\xe8\x83\xc2\x14,\x12k\xca\xd3\xfd\xad?7\x91}\x9c
\x91\xaf\xdb\x9fuA9\xff\x9c\xac\f\xae'
```

Rajah 4 Contoh maklumat paket rangkaian dalam *Output.txt*

Fail *memory dump* yang digunakan diperoleh daripada komputer yang telah menggunakan laman web *www.box.com* iaitu suatu laman servis pengkomputeran awan. Alamat IP yang direkodkan dalam *Output.txt* (Rajah 4) dibandingkan dengan maklumat yang diperoleh daripada laman web *www.ultratools.com/tools/ipWhoisLookup*. Laman web ini akan mededahkan maklumat mengenai alamat IP yang diberikan seperti dalam Rajah 5. Pada segi forensik, maklumat yang dikumpulkan oleh *Trazador* adalh penting kerana ia membukitkan bahawa komputer yang diselidik telah melayari laman web *www.box.com*. Alamat IP direkodkan sebagai alamat sumber dan mempunyai *Data*, ini menunjukkan bahawa pengguna komputer telah mendapatkan sesuatu dokumen atau fail daripada laman web itu.



Rajah 5 Laman web *www.ultratools.com/tools/ipWhoisLookup* untuk membandingkan alamat IP

Walau bagaimanapun, pembangunan *Trazador* mempunyai satu kekangan utama yang berkenaan dengan objektif yang ditetapkan. Struktur data *Data* direkodkan dalam format yang tidak boleh dibaca. Hal ini kerana protokol SSL yang berada di antara protokol TCP dan HTTP. Protokol SSL menggunakan sijil digital dan *public key* untuk menyulitkan data yang dihantar atas rangkaian.

Cadangan bagi menyelesaikan masalah penyahsulitan data adalah dengan melakukan kajian mengenai *Rivest-Shamir- Adleman* (RSA) dan juga sijil digital. Secara ringkas, RSA adalah algoritma *Public-Key* (*Public Key Infrsastructure* - PKI) yang digunakan secara meluas. Terdapat 2 kunci RSA iaitu *public key* dan *private key* yang digunakan untuk penyulitan dan penyahsulitan data. Sijil digital adalah seperti kata laluan yang membenarkan (seseorang, sesuatu organisasi, laman web, atau aplikasi perisian) penukaran data dengan selamat melalui internet dengan menggunakan PKI (Mahajan & Sachdeva, 2013).

6 KESIMPULAN

Pengesanan paket rangkaian daripada fail *memory dump* boleh membantu dalam forensik memory sebagai alternatif untuk mendapatkan maklumat paket rangkaian secara *offline*. Walaupun *Trazador* dihadapi kekangan, cadangan untuk menyelesaikan kekangan tersebut

mungkin boleh mengatasinya supaya ia lebih sempurna. Kajian yang mendalam terhadap alat ini harus diteruskan bagi meningkatkan kualiti aplikasi. Diharapkan *Trazador* dapat diterima dan dimanfaatkan dengan baik oleh pengguna seterusnya dapat membantu pengguna dalam forensik memori.

7 RUJUKAN

Casey, E. (2002). Error, Uncertainty, and Loss in Digital Evidence. *International Journal of Digital Evidence*, *1*(2), 45.

Joshi, R. C., & Pilli, E. S. (2016). *Fundamentals of Network Forensics*. https://doi.org/10.1007/978-1-4471-7299-4

Mahajan, P., & Sachdeva, A. (2013). A Study of Encryption Algorithms AES, DES and RSA for Security. *Global Journal of Computer Science and Technology*, *13*(No 15-E). Retrieved from https://computerresearch.org/index.php/computer/article/view/272/272

Nor Nadia Abdullah Marzuki (A154287)
Khairul Akram Zainol Ariffin
Fakulti Teknologi & Sains Maklumat
Universiti Kebangsaan Malaysia.