PROSEDUR PENJEJAKAN PAKET RANGKAIAN BAGI KONSEP PILIH PERANTI ANDA SENDIRI (CYOD)

ABDUL RAFIZ MD YUSUF

UNIVERSITI KEBANGSAAN MALAYSIA

PROSEDUR PENJEJAKAN PAKET RANGKAIAN BAGI KONSEP PILIH PERANTI ANDA SENDIRI (CYOD)

ABDUL RAFIZ MD YUSUF

PROJEK YANG DIKEMUKAKAN UNTUK MEMENUHI SEBAHAGIAN DARIPADA SYARAT MEMPEROLEHI IJAZAH SARJANA KESELAMATAN SIBER

FAKULTI TEKNOLOGI DAN SAINS MAKLUMAT
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI

2022

PENGAKUAN

Saya akui karya ini adalah hasil kerja saya sendiri kecuali nukilan dan ringkasan yang tiap-tiap satunya telah saya jelaskan sumbernya.

27 April 2022

ABDUL RAFIZ BIN MD YUSUF
P95374

PENGHARGAAN

Syukur alhamdulillah kepada Allah S.W.T kerana dengan limpah kurnia-Nya, kajian ini telah berjaya disiapkan. Setinggi-tinggi penghargaan dan ucapan terima kasih ditujukan kepada Dr. Khairul Akram bin Zainol Ariffin selaku penyelia projek yang telah banyak membantu dan memberikan tunjuk ajar, perhatian, nasihat serta semangat di dalam menjalankan kajian ini. Begitu juga kepada semua tenaga pengajar daripada Fakulti Teknologi & Sains Maklumat (FTSM) dan Cyber Security Malaysia (CSM) yang telah banyak mencurahkan ilmu sepanjang pembelajaran Sarjana Keselamatan Siber ini.

Ucapan terima kasih juga ditujukan kepada Kerajaan Malaysia khususnya kepada Jabatan Perkhidmatan Awam (JPA) selaku penaja kepada program Sarjana ini.

Akhir sekali, penghargaan dan terima kasih kepada isteri Azleena Azlia Adian dan anak – anak, Umar Rasyad dan Zubayr Ihsan serta ahli keluarga tersayang yang tidak pernah jemu memberikan nasihat, sokongan dan semangat sepanjang tempoh menyediakan kajian ini. Kepada yang terlibat secara langsung dan tidak langsung juga diucapkan terima kasih yang tidak terhingga. Hanya Allah yang dapat membalas jasa kalian semua.

ABSTRAK

Prosedur penjejakan paket rangkaian bagi konsep Pilih Peranti Anda Sendiri (CYOD) merupakan sebuah struktur asas yang dibangunkan bagi memudahkan proses menjejak paket rangkaian di dalam sebuah persekitaran yang terkawal. Di dalam kajian ini, mesin maya telah dipilih sebagai wakil kepada peranti yang digunakan oleh organisasi. Dapatan kajian akan digunakan oleh organisasi bagi merangka polisi atau dasar berkaitan keselamatan siber seterusnya membantu organisasi dalam memilih peranti yang sesuai untuk digunakan oleh pekerja melalui konsep CYOD. Konsep CYOD dilihat dapat meningkatkan lagi produktiviti organisasi kerana pekerja dapat memilih peranti yang diinginkan dan biasa digunakan dalam kehidupan seharian. Ianya juga dapat menjimat kos latihan kepada pekerja mengenai cara penggunaan peranti tersebut selain dapat menjimatkan masa penyesuaian di antara pekerja dan peranti. Pekerja yang telah dibekalkan dengan peranti akan dapat mengakses kerja - kerja yang diarahkan dengan julat masa yang lebih luas iaitu selepas waktu bekerja atau semasa cuti di luar kawasan. Organisasi hanya perlu mengawal jenis peranti yang boleh digunakan dengan membuat kajian mengenai kesesuaian sesuatu peranti digunakan terutamanya dari segi keselamatan maklumat. Organisasi juga dapat menyediakan kaedah bagi mengekalkan tahap keselamatan maklumat yang bersesuaian jika terjadi sesuatu yang tidak diingini terhadap peranti yang digunakan oleh pekerja terbabit seperti kehilangan atau keciciran. Pembangunan prosedur penjejakan paket rangkaian ini diharap dapat membantu organisasi dalam mengenalpasti peranti yang sesuai dipilih dalam melaksanakan konsep CYOD. Prosedur ini boleh digunakan oleh Jabatan Teknologi Maklumat (IT) sesebuah organisasi dalam menjejak paket rangkaian di dalam peranti yang digunakan oleh pekerja. Personel di Jabatan IT dapat menjimatkan masa dalam mencari kaedah dan cara yang sesuai bagi mendapatkan maklumat mengenai pelbagai sambungan ke internet yang telah dilakukan oleh pekerja dalam mengenalpasti kemungkinan terdapat ancaman keselamatan siber terhadap maklumat kepunyaan organisasi yang terdapat dalam peranti tersebut. Eksperimen yang dijalankan telah menunjukkan kejayaan prosedur yang dibangunkan dalam menjejak paket rangkaian di dalam peranti yang membuat sambungan kepada penyedia perkhidmatan pengkomputeran awan. Diharap prosedur yang dibangunkan ini dapat terus dikembangkan dengan meneliti lebih lanjut fail Paket Rangkaian (PCAP) yang dihasilkan melalui prosedur penjejakan paket ini.

PROCEDURE TRACKING NETWORK PACKET FOR CHOOSE YOUR OWN DEVICE (CYOD) CONCEPT

ABSTRACT

The network packet tracking procedure for the Choose Your Own Device (CYOD) concept is a basic structure developed to facilitate the process of tracking network packets in a controlled environment. In this study, virtual machines were selected as representative of the devices used by the organization. The findings of the study will be used by the organization to formulate policies or regulation related to cyber security, in which it can assist the organization in selecting the appropriate device to be used by employees through the concept of CYOD. The concept of CYOD is seen to further increase the productivity of the organization as employees can choose the desired devices that are commonly used in their daily life. It can also save the cost to train the employees on using the device and time spent by the employees to familiarize the device. Employees who have been provided with the device will be able to access the work with a wider range of time especially after working hours or during holidays. Organizations will only need to control the types of devices that can be used by conducting a study on the suitability of a device especially in terms of information security. Organizations can also provide mechanisms to maintain an appropriate level of information security in the event of something unexpected occurs to the devices used by the employees, such as loss or dropout. The development of this network packet tracking procedure is expected to assist organizations in identifying the appropriate devices selected for implementing the CYOD concept. This procedure can be used by the Information Technology (IT) Department of an organization in tracking the network packets in devices used by employees. IT Department personnel can save time in finding appropriate methods and ways to obtain information on the various connections to the internet that have been made by employees in identifying possible cyber security threats to information belonging to the organization contained in the device. The experiment conducted has shown the success of the procedure in tracking network packets against connections to cloud computing service providers. It is hoped that this procedure can be expanded by further analysis of the network packet file (PCAP) generated through this procedure.

KANDUNGAN

Halaman

PENGAKUAN		**ii**
PENGHARGAAN		**iii**
ABSTRAK		**iv**
ABSTRACT		**v**
KANDUNGAN		**vi**
SENARAI JADUAL		**viii**
SENARAI SINGKATAN		**xi**
BAB I	**PENDAHULUAN**	
1.1	Pengenalan	1
1.2	Pernyataan Masalah	3
1.3	Persoalan Kajian	5
1.4	Objektif Kajian	6
1.5	Skop Kajian	6
1.6	Kepentingan Kajian	6
1.7	Organisasi Penulisan	7
BAB II	**KAJIAN KUSASTERAAN**	
2.1	Pengenalan	9
2.2	Pengkomputeran Awan	10
	2.2.1 Definisi serta konsep umum pengkomputeran awan	10
	2.2.2 Ciri – ciri pengkomputeran awan	10
	2.2.3 Model perkhidmatan pengkomputeran awan	12
	2.2.4 Model pembangunan pengkomputeran awan	13
2.3	Forensik Digital Bagi Pengkomputeran Awan	15
	2.3.1 Forensik digital	15
	2.3.2 Forensik awan	15
	2.3.3 Metodologi digital forensik	15
2.4	Bawa Peranti Anda Sendiri (BYOD)	16
	2.4.1 Faedah penggunaan BYOD	16
	2.4.2 Cabaran perlaksanaan BYOD	17
2.5	Pilih Peranti Anda Sendiri (CYOD)	18

	2.5.1	CYOD alternatif kepada BYOD	19
	2.5.2	Faedah penggunaan CYOD	19
	2.5.3	Cabaran perlaksanaan CYOD	20
2.6	Kesimpulan		21
BAB III	**METODOLOGI**		
3.1	Pengenalan		23
3.2	Metodologi Kajian		23
	3.2.1	Fasa 1: Kajian teoretikal	25
	3.2.2	Fasa 2 dan 3: Pembangunan prosedur pengesanan paket dan eksperimen serta analisis	25
	3.2.4	Fasa 4: Pengujian	34
3.3	Perbincangan		52
3.4	Kesimpulan		52
BAB IV	**ANALISIS**		
4.1	Pengenalan		54
4.2	Analisis Eksperimen		54
	4.2.1	Pengguna 1	54
	4.2.2	Pengguna 2	56
	4.2.3	Pengguna 3	57
4.3	Perbincangan		57
4.4	Kesimpulan		60
BAB V	**KESIMPULAN**		
5.1	Pengenalan		61
5.1	Rumusan Kajian		61
	5.2.1	Objektif Kajian : Mengenal pasti kelemahan/isu dalam konsep CYOD	61
5.3	Sumbangan Kajian		63
5.4	Kekangan Kajian		64
5.5	Cadangan Kajian Masa Hadapan		65
RUJUKAN			**66**

SENARAI JADUAL

No. Jadual		Halaman
Jadual 2.1	Ancaman biasa BYOD dengan punca dan implikasinya	18
Jadual 2.2	Isu-isu berkaitan konsep CYOD	21
Jadual 3.1	Perisian-perisian yang digunakan	25
Jadual 3.2	Senarai maklumat pengguna di dalam kajian	28
Jadual 3.3	Set data pengujian penggunaan storan di perkhidmatan awan	29

SENARAI ILUSTRASI

No. Rajah		Halaman
Rajah 2.1	Tiga lapisan pengkomputeran awan (Stanoevska-Slabeva & Wozniak 2010)	12
Rajah 3.1	Rekabentuk Kajian	24
Rajah 3.2	Spesifikasi komputer yang digunakan untuk tujuan kajian	26
Rajah 3.3	Perisian VMware yang telah dipasang perisian Windows 11 di dalam mesin maya.	27
Rajah 3.4	Laman pendaftaran pengguna baru bagi sync.com	28
Rajah 3.5	Pendaftaran pengguna di penyedia perkhidmatan awan	30
Rajah 3.6	Maklumat perisian VMware yang telah dipasang di komputer *host*	31
Rajah 3.7	Sistem pengoperasian Windows 11 telah di pasang di dalam mesin maya	32
Rajah 3.8	Prosedur mengesan penggunaan perkhidmatan awan dari konsep pilih peranti anda sendiri (CYOD)	33
Rajah 3.9	Pengguna 1 log masuk ke sync.com	35
Rajah 3.10	Pengguna 1 berjaya memuat naik 3 jenis fail ke storan awan yang disediakan oleh sync.com	36
Rajah 3.11	Pengguna 1 berjaya memuat turun 3 jenis fail ke komputer	37
Rajah 3.12	Arahan *snapshot* dilaksanakan bagi menghentikan segala proses dan sambungan oleh mesin maya	38
Rajah 3.13	Penggunaan perisian vmss2core-sb-8456865 untuk menjana fail *memory dump* "*memory.dmp*"	39
Rajah 3.14	Penggunaan perisian bulk_extractor64 untuk menjana fail pcap	39
Rajah 3.15	Pengguna 2 Log Masuk Ke sync.com	40
Rajah 3.16	Pengguna 2 Berjaya Log Masuk Ke sync.com	41
Rajah 3.17	Pengguna 2 memuat turun aplikasi pelanggan dari sync.com	42
Rajah 3.18	Pengguna 2 melakukan konfigurasi aplikasi pelanggan dari sync.com	42

Rajah 3.19	Pengguna 2 akan melakukan proses muat naik melalui aplikasi pelanggan dari sync.com	43
Rajah 3.20	Proses penukaran nama fail oleh pengguna 2 melalui aplikasi pelanggan dari sync.com berjaya	43
Rajah 3.21	Arahan *snapshot* dilaksanakan bagi menghentikan segala proses dan sambungan oleh mesin maya	44
Rajah 3.22	Penggunaan perisian vmss2core-sb-8456865 untuk menjana fail *memory dump* "*memory.dmp*"	45
Rajah 3.23	Penggunaan perisian bulk_extractor64 untuk menjana fail PCAP	45
Rajah 3.24	Pengguna 3 log masuk ke sync.com	46
Rajah 3.25	Pengguna 3 berjaya memuat naik 3 jenis fail ke storan awan yang disediakan oleh sync.com melalui pelayar Internet Google Chrome.	47
Rajah 3.26	Pengguna 3 membuat konfigurasi sambungan ke sync.com	48
Rajah 3.27	Pengguna 3 berjaya memasang aplikasi pelanggan yang disediakan oleh sync.com	48
Rajah 3.28	Proses memuat turun fail oleh pengguna 3 melalui aplikasi pelanggan dari sync.com berjaya	49
Rajah 3.29	Arahan *snapshot* bagi Pengguna 3 berjaya dilaksanakan	50
Rajah 3.30	Fail yang terdapat di dalam *folder user 3* untuk menjana fail *memory dump*.	51
Rajah 3.31	Proses menjana fail *memory dump*.	51
Rajah 3.32	Proses menjana fail PCAP	52
Rajah 4.1	Sambungan dari IP VMware (mesin maya) ke laman sesawang sync.com	55
Rajah 4.2	Pertanyaan Domain Name Server (DNS) dari mesin maya yang mendapat maklumbalas dari sync.com ke IP mesin maya	56
Rajah 4.3	Sambungan ke HyperText Transfer Protocol (HTTP) telah berjaya	57
Rajah 4.4	Sambungan HyperText Transfer Protocol (HTTP) telah berjaya dilakukan	58

SENARAI SINGKATAN

BYOD	Bring Your Own Device
CYOD	Choose You Own Device
UKM	Universiti Kebangsaan Malaysia
DDoS	Distributed Denial-of-Service

BAB I

PENDAHULUAN

1.1 PENGENALAN

Pada awal tahun 2020, seluruh dunia telah dikejutkan dengan penyebaran virus Covid-19. Terdapat banyak pengajaran dari pandemik Covid-19. Jutaan telah dijangkiti Covid-19 di seluruh dunia, ini memberi impak kepada perubahan cara dan tempat bekerja kepada pekerja sesebuah organisasi. Oleh kerana pergerakan setiap individu telah dihadkan, hampir semua individu dibenarkan bekerja dari rumah melainkan petugas di barisan hadapan. Kehidupan kerja dan kehidupan peribadi menjadi lebih berhubung. Ini memberikan kesan penting bagaimana sesuatu tugas atau pekerjaan itu perlu untuk diselesaikan di persekitaran yang berbeza dari pejabat.

Covid-19 dilihat mempercepatkan penggunaan teknologi digital di beberapa kawasan di mana adaptasi digital sebelum ini telah terhenti atau hanya berkembang perlahan-lahan. Penggunaan teknologi digital dalam teknik pengumpulan data, janji temu dan terapi dalam talian bagi urusan kesihatan, kerja dalam talian, pembelajaran dan perhubungan sosial (Hantrais et al. 2021). Cabaran baharu dalam penggunaan teknologi digital bagi menyokong urusan kehidupan harian sepanjang penyebaran Covid-19 dapat dilihat dengan peningkatan permintaan terhadap pengeluaran aplikasi-aplikasi mudah alih, pembinaan platform perniagaan dalam talian dan penggunaan persidangan video di seluruh dunia. Transformasi pendigitalan seluruh urusan seharian ini memerlukan kos yang tinggi. Penularan wabak memburukkan lagi cabaran sedia ada, campur tangan kerajaan diperlukan untuk memastikan segala yang telah dirancang dalam sektor Teknologi Maklumat dapat membantu menyelesaikan masalah penularan wabak dengan membangunkan aplikasi-aplikasi yang dapat mengurangkan keperluan individu untuk melakukan perjalanan ke tempat kerja atau keluar dari

rumah bagi menyelesaikan urusan seharian. Aplikasi-aplikasi yang dibangunkan juga dapat menyampaikan maklumat-maklumat penting mengenai kawasan dan kaedah penularan wabak. Dengan ini urusan kehidupan seharian dapat dilaksanakan dengan lebih teratur dan selamat.

Konsep Bawa Peranti Anda Sendiri (BYOD), telah lama diperkenalkan di dalam alam pekerjaan bagi meningkatkan lagi produktiviti dan kebolehlaksanaan sesuatu tugas di kalangan pekerja di Malaysia. BYOD merupakan suatu konsep atau dasar di mana organisasi membenarkan pekerja membawa peranti mudah alih sendiri ke tempat kerja untuk mengakses maklumat dan aplikasi organisasi. Kawalan terhadap peranti yang boleh berhubung dengan rangkaian organisasi menjamin keselamatan maklumat dan pelayan yang digunakan.

Revolusi Perindustrian Keempat (4IR) adalah titik bermulanya kemunculan pelbagai teknologi dan perisian canggih bagi meyokong perlaksanaan tugasan secara atas talian dengan aplikasi seperti Google Workspace, Zoom, WEBEX, Dropbox, Evernote dan lain–lain lagi. Ini secara tidak langsung memperlihatkan keupayaan teknologi tanpa limitasi lokasi yang menyokong sesuatu pekerjaan itu dilaksanakan tanpa mengira lokasi dan masa. Malahan perkembangan dan penggunaan teknologi seperti ini yang semakin mendapat tarikan dalam organisasi kerja pada hari ini seterusnya meningkatkan produktiviti dan menjimatkan kos serta masa bukan hanya kepada organisasi atau jabatan malahan juga memberikan banyak kemudahan dan kelebihan kepada para pekerja. Revolusi Perindustrian Keempat (4IR) dan kepesatan perkembangan teknologi merubah landskap ekonomi di seluruh dunia dengan cepat. Pandemik Covid-19 juga telah mempercepat gelombang perubahan yang mendorong rakyat, perniagaan dan Kerajaan untuk mengadaptasikan pendigitalan dalam urusan kehidupan seharian (Unit Perancang Ekonomi 2021).

Penggunaan pengkomputeran Awan (*Cloud Computing*) juga menyokong revolusi industri 4.0. Penggunaan aplikasi dan storan di persekitaran awan membolehkan pekerja-pekerja melaksanakan tugas pejabat dengan mudah melalui sambungan internet ke rangkaian selamat organisasi. Gabungan BYOD, CYOD dan penggunaan teknologi pengkomputeran awan merupakan kombinasi yang terbaik

dalam melaksanakan tugasan pejabat dari rumah semasa krisis pandemik Covid-19 ini. Ianya memberikan kelebihan kepada organisasi-organisasi yang telah menggunakan teknologi-teknologi ini untuk terus melaksanakan urusan organisasi mereka tanpa terkesan dengan dasar bekerja dari rumah yang diarahkan oleh pihak kerajaan bagi membendung penularan Covid-19 ini.

Walau bagaimanapun, isu-isu keselamatan maklumat dan rangkaian semasa menggunakan teknologi-teknologi ini juga perlu dititik beratkan. Peningkatan dan kepelbagaian ancaman siber seperti aktiviti penipuan dalam talian, perisian tebusan, kebocoran data, pengintipan siber, berita palsu dan ucapan kebencian amat membimbangkan. Pelbagai usaha telah dilaksanakan bagi memastikan keselamatan maklumat dan rangkaian sentiasa terpelihara. Sokongan pihak kerajaan dan organisasi sendiri adalah amat penting bagi memastikan setiap rakyat atau pekerja di organisasi mempunyai tahap kesedaran yang tinggi tentang keselamatan maklumat dan rangkaian yang digunakan terutamanya dalam menjalankan kerja-kerja dan urusan seharian.

1.2 PERNYATAAN MASALAH

Revolusi Perindustrian Keempat (4IR) yang melibatkan teknologi baru muncul seperti Data Raya, Realiti Terimbuh, Realiti Maya, *Blockchain*, Internet Benda, Pengkomputeran Awan, Kecerdasan Buatan dan sebagainya dilaksanakan bagi mentransformasikan Malaysia menjadi negara maju dan berpendapatan tinggi, malahan juga menjadi negara peneraju serantau dalam bidang ekonomi digital (Unit Perancang Ekonomi 2021).

Kepesatan peredaran ilmu pengetahuan dan kemajuan teknologi telah berkembang dengan begitu mendadak sejak beberapa tahun kebelakangan ini. Kemajuan teknologi ini telah memberi impak dan berupaya mengubah cara hidup dan peradaban manusia termasuk melakukan aktiviti rutin dalam kehidupan seharian kita. Perkembangan teknologi digital menunjukkan bahawa pencapaian manusia dalam kehidupan seharian semakin lancar, mudah dan cepat. Malah, perubahan teknologi dan kebergantungan terhadap Internet yang semakin tinggi ini juga telah mempengaruhi aktiviti seharian individu, pendidikan, kesihatan, perniagaan dan pentadbiran.

Pada masa sekarang terdapat isu-isu yang mendesak dalam persekitaran digital yang boleh menjejaskan keselamatan negara. Ancaman siber terbukti memberi kesan buruk kepada negara kerana ia menggalakkan aktiviti jenayah dan ketidakadilan sosio-ekonomi di kalangan masyarakat. Selari dengan perkembangan teknologi semasa dan tahap kecerdikan masyarakat, salah laku tersebut juga menjadi kian kompleks dan menyukarkan kegiatan jahat ini ditangani oleh pihak berkuasa. Peningkatan globalisasi dan digitalisasi telah membuka peluang kepada perkembangan jenayah siber. Jenayah ini dikesan mempunyai struktur organisasi yang mempunyai kelengkapan peralatan, kemahiran dan latihan bagi menjalankan operasi.

Penggunaan teknologi digital yang diguna pakai kini secara tidak langsung telah turut meningkatkan pelbagai ancaman siber di Malaysia seperti penipuan dalam talian, pencerobohan, kebocoran data dan lain-lain lagi. Perkembangan teknologi yang semakin canggih boleh menyebabkan maklumat organisasi dan maklumat individu terdedah kepada persekitaran yang tidak selamat secara sengaja atau tidak sengaja oleh pekerja di sesebuah organisasi. Penggunaan peranti digital juga menarik minat penjenayah untuk mengeksploitasi maklumat digital untuk mendapatkan faedah atau imbuhan menggunakan maklumat yang diperolehi secara tidak sah. Semakin ramai orang bergantung dan berurusan dengan Internet, semakin besar pula peluang penjenayah siber untuk mengambil kesempatan menimbulkan kekacauan terutamanya terhadap mereka yang berada dalam kesukaran lebih-lebih lagi dalam persekitaran pandemik Covid-19 kini. Mereka yang mudah menjadi mangsa adalah disebabkan tidak arif menggunakan Internet, kurang berpengetahuan mengenai isu semasa siber atau terlalu leka melayari Internet.

Tahun 2020 dunia telah menyaksikan bagaimana pandemik Covid-19 yang melanda telah menyebabkan meningkatnya penggunaan digital teknologi disebabkan perintah kawalan pergerakan dan norma baharu penjarakkan sosial. Peningkatan digitalisasi telah membawa organisasi dan institusi pendidikan untuk mengamalkan kaedah bekerja dari rumah. Perintah kawalan pergerakan dan bekerja dari rumah telah menyebabkan masyarakat terpaksa memilih internet untuk tujuan berkomunikasi, berinteraksi dan meneruskan tanggungjawab mereka berkerja dari rumah. Penggunaan teknologi seperti sidang video, media sosial, platform membeli-belah dalam talian

juga turut semakin meningkat dan merupakan pilihan yang terbaik dalam situasi Covid-19 kini. Bukan sahaja Covid-19 ini telah mengubah cara kita menghadapi teknologi digital semasa, tetapi turut mengubah cara kita menerapkan keselamatan siber. Perkara ini telah memberikan cabaran kepada masyarakat di seluruh dunia.

Cabaran dalam menentukan keselamatan maklumat organisasi ketika wabak Covid-19 ini juga dilihat sebagai satu aspek yang perlu diambil berat. Ketika penekanan kepada pekerja bagi memastikan produktiviti tidak terjejas walaupun melakukan kerja dari rumah, organisasi dilihat dapat membantu pekerja dalam meningkatkan produktiviti dengan memperkenalkan konsep CYOD. Konsep ini dapat membantu organisasi dalam memastikan keselamatan maklumat sentiasa terpelihara disamping produktiviti pekerja dapat ditingkatkan atau dikekalkan walaupun bekerja dari rumah. Organisasi hanya perlu memilih peranti yang sesuai untuk digunakan oleh pekerja mereka bagi memastikan aspek keselamatan maklumat organisasi dan produktiviti pekerja berada di tahap yang optimum.

Pada masa ini, keperluan bagi mengenal pasti peranti yang sesuai sebelum konsep CYOD diperkenalkan di sesebuah organisasi dilihat sangat penting. Tambahan pula, kebanyakan organisasi pada masa ini telah menggunakan perkhidmatan awan dalam segala urusan organisasi. Perkhidmatan awan yang telah terbukti lebih menjimatkan kos selenggaraan dan pada masa yang sama memudahkan organisasi meningkatkan sumber pada bila-bila masa menjadikan perkhidmatan awan pilihan yang tepat bagi meningkatkan keuntungan dan produktiviti organisasi.

1.3 PERSOALAN KAJIAN

Berdasarkan pernyataan masalah yang dinyatakan, persoalan kajian adalah seperti berikut:

i. Apakah kelemahan/isu dalam konsep CYOD?

ii. Apakah yang dapat membantu organisasi yang ingin mengesan sambungan peranti yang digunakan oleh pekerja ke laman sesawang yang menyediakan perkhidmatan pengkomputeran awan?

iii. Apakah prosedur bagi menjejak paket rangkaian bagi peranti yang melakukan sambungan kepada perkhidmatan awan berkesan dan boleh digunakan?

1.4 OBJEKTIF KAJIAN

Berdasarkan persoalan kajian yang telah dinyatakan, objektif kajian adalah seperti berikut:

i. Mengenal pasti kelemahan/isu dalam konsep CYOD.

ii. Membangunkan prosedur penjejakan paket rangkaian bagi jabatan IT di sesebuah organisasi untuk mengesan sambungan ke perkhidmatan awan.

iii. Menilai kejayaan prosedur penjejakan paket rangkaian yang dibangunkan.

1.5 SKOP KAJIAN

Skop kajian adalah seperti berikut:

i. Mengadakan eksperimen perlaksanaan konsep CYOD bagi peranti yang menggunakan sistem pengoperasian Windows dengan menggunakan mesin maya bagi mewujudkan persekitaran terkawal; dan

ii. Membangunkan serta menilai prosedur bagi menjejak paket rangkaian dan sambungan kepada perkhidmatan awan.

1.6 KEPENTINGAN KAJIAN

Menerusi kajian yang dijalankan, simulasi penjejakan paket rangkaian bagi mengesan sambungan terhadap perkhidmatan awan dari peranti yang menggunakan sistem pengoperasian Windows dapat diuji keberkesanannya. Analisis daripada simulasi yang dijalankan membolehkan maklumat tersebut digunakan oleh organisasi sebagai input untuk mereka bentuk prosedur keselamatan penggunaan peranti secara CYOD yang menggunakan perkhidmatan awan. Aktiviti simulasi yang dijalankan dapat membantu organisasi untuk mengenal pasti tahap kesesuaian peranti yang akan dipilih

untuk konsep CYOD di organisasi. Aktiviti simulasi ini boleh dijalankan secara dalaman, berkala dan tidak melibatkan kos. Selain itu juga, dapatan dari hasil analisis boleh membantu organisasi untuk menentukan polisi keselamatan siber yang bersesuaian.

Reka bentuk simulasi penjejakan paket rangkaian ini juga boleh diguna pakai sebagai rujukkan oleh organisasi yang lain dalam memperkenalkan konsep CYOD. Ini dapat mengurangkan kos kepada organisasi tersebut kerana tidak perlu mengulang semula proses simulasi atau menggunakan pihak ketiga di dalam menjalankan aktiviti simulasi. Reka bentuk simulasi yang dibangunkan secara teratur dan beretika juga menjadikan amalan terbaik keselamatan siber kepada organisasi. Amalan terbaik ini dapat menyumbang kepada pengukuhan persekitaran siber yang lebih selamat. Hasil kajian juga diharap dapat membantu organisasi menambahbaik polisi dengan mengambil kira elemen ketersediaan terhadap keselamatan siber supaya perkhidmatan forensik rangkaian dapat dilaksanakan dengan lebih praktikal. Penekanan terhadap aspek ketersediaan terhadap peranti berteknologi semasa dan cabaran dalam memilih peranti yang sesuai bagi konsep CYOD di organisasi dapat memudahkan personel di Jabatan Teknologi Maklumat di organisasi tersebut dalam merangka strategi bagi mengenakan kawalan atau polisi keselamatan yang sewajarnya. Hasil kajian diharap dapat meningkatkan penggunaan konsep CYOD yang memberikan faedah kepada organisasi dalam meningkatkan produktiviti dan pada masa yang sama aspek keselamatan maklumat organisasi dapat terus dijaga oleh semua pihak yang terlibat.

1.7 ORGANISASI PENULISAN

Disertasi kajian ini terbahagi kepada lima (5) bab seperti berikut:

a) **BAB I** terdiri daripada tentang pengenalan, penyataan masalah, objektif kajian, skop kajian, kepentingan kajian dan organisasi penulisan.

b) **BAB II** mengandungi kajian kesusasteraan yang dibuat terhadap konsep asas pengkomputeran awan. Penerangan mengenai konsep Bawa Peranti Anda Sendiri (BYOD) dan konsep Pilih Peranti Anda Sendiri (CYOD).

c) **BAB III** menerangkan metodologi kajian yang digunakan untuk mencapai objektif kajian. Dalam bab ini perincian metodologi kajian merangkumi reka bentuk kajian, proses eksperimentasi, kaedah penganalisaan, proses pengesahan penjejakan paket yang dilaksanakan dan pembangunan prosedur penjejakan paket rangkaian.

d) **BAB IV** menerangkan secara terperinci mengenai simulasi yang dilakukan secara eksperimentasi seterusnya mengesahkan mengenai penjejakan paket rangkaian penggunaan perkhidmatan pengkomputeran awan di dalam persekitaran simulasi CYOD. Ianya seterusnya membangunkan prosedur penjejakan paket rangkaian tersebut.

e) **BAB V** merupakan kesimpulan kepada kajian yang akan dilaksanakan mengandungi perbincangan dan ulasan sebagai rumusan hasil kajian menerusi dapatan kajian, sumbangan kajian dan cadangan penambahbaikan kajian ini pada masa hadapan.

BAB II

KAJIAN KUSASTERAAN

2.1 PENGENALAN

Bab ini akan membincangkan tentang kajian kesusasteraan mengenai pengkomputeran awan, jenis-jenis awan, model-model yang terdapat di dalam pengkomputeran awan serta perbandingan yang terdapat pada setiap jenis pengkomputeran awan. Kajian juga dibuat mengenai kaedah-kaedah forensik digital bagi pengkomputern awan yang mana ia menyentuh tentang ciri-ciri persamaan serta perbezaan di antara forensik digital tradisional dan forensik digital bagi pengkomputeran awan yang telah dibincang dan dirumuskan oleh kajian-kajian terdahulu melalui artikel jurnal, dokumen rasmi kerajaan dan kertas persidangan di dalam julat masa 10 tahun kebelakang. Segala penemuan hasil kajian ini akan disaring dan diproses bagi mengenalpasti segala maklumat tentang hasil penelitian dan penilaian tersebut untuk diambil sebagai rujukan bagi pembangunan sebuah kerangka dasar umum proses forensik digital bagi pengkomputeran awan.

Di dalam kajian kusasteraan ini juga memerlukan penyelidik untuk menjalankan proses meneliti, memahami dan menilai secara mendalam dan kritikal terhadap dapatan kajian dan penulisan yang telah dilaksanakan. Segala hasil penelitian dan penilaian kritikal yang telah dibuat akan mengenalpasti ruang-ruang dalam pengetahuan berkaitan boleh dicadangkan untuk ditambahbaik dan seterusnya disempurnakan. Bab ini juga memberi maklumat dan input kepada penyelidik bagi mendalami kajian dengan mengetahui keseluruhan persekitaran permasalahan kajian seterusnya membantu menjalankan kajian mengenai forensik digital bagi pengkomputeran awan ini dengan lebih efektif.

2.2 PENGKOMPUTERAN AWAN

2.2.1 Definisi serta konsep umum pengkomputeran awan

Institut Piawaian dan Teknologi Kebangsaan (NIST) mendefinasikan Pengkomputeran awan merupakan sebuah model yang menyediakan perkongsian sumber (seperti pelayan, rangkaian, storan, aplikasi, dan perkhidmatan) yang membenarkan ianya diakses dan dikonfigurasi melalui rangkaian dengan pantas dan hanya memerlukan pengurusan dan interaksi bersama pembekal perkhidmatan yang minimum. (Mell & Grance 2011)

Pengkomputeran awan juga ditafsirkan sebagai perkhidmatan yang menyediakan perkongsian sumber berskala melalui internet atau rangkaian yang menyediakan berskala, perkhidmatan yang dijamin (*Quality of Service*) atas permintaan yang boleh diakses melalui Internet (Lavania et al. 2013).

Pengkomputeran awan adalah model dalam teknologi maklumat yang berkaitan dengan pemindahan data melalui internet atau perkongsian maklumat, sumber, perisian kepada komputer atau mana-mana peranti lain yang gunakan bagi sesuatu tujuan khusus. Pengkomputeran awan juga membolehkan penggunaan sumber pengkomputeran yang disampaikan sebagai perkhidmatan atau aplikasi melalui rangkaian. Pengkomputeran awan disediakan oleh banyak perkhidmatan seperti *Amazon Web Service, Microsoft Azure, Google Cloud Platform*.(Prajapati et al. 2018)

2.2.2 Ciri – ciri pengkomputeran awan

Hari ini manusia secara tidak langsung bergantung kepada pengkomputeran Awan untuk menyimpan maklumat awam dan peribadi mereka. Penyedia Perkhidmatan Pengkomputeran Awan (*Cloud Service Provider*), bersedia memenuhi segala keperluan pengguna dengan menyediakan perkakasan, perisian dan perkhidmatan yang relevan. Tambahan pula faktor perkembangan pesat capaian internet, mengubah corak keperluan para pengguna terhadap pengkomputeran awan yang mana memerlukan Penyedia Perkhidmatan Pengkomputeran Awan menyediakan

penyimpanan data yang selamat, cepat, mudah dicapai ke semua aplikasi dan data dari mana-mana peranti rangkaian. (Rani & Ranjan 2014)

a. Penyelengaraan dan Perkakasan

Pengkomputeran awan dapat mengurangkan kos dari segi penggunaan perkakasan dan juga penyelenggaraan. Ini kerana pengguna hanya menggunakan sumber yang telah disediakan oleh penyedia perkhidmatan melalui rangkaian.

b. Antaramuka Program Perisian (*Application Programming Interface*)

Ianya menyediakan akses kepada perkhidmatan awan dilakukan melalui kaedah dan antaramuka yang sama sepertimana mengakses aplikasi-aplikasi tradisoinal. Pengguna merasa mudah dan selesa menggunakan perkhidmatan ini.

c. Perkhidmatan berdasarkan permintaan

Pengkomputeran awan menyediakan kumpulan sumber yang besar yang membolehkan pengguna membuat sebarang konfigurasi perkakasan dan storan mengikut keperluan semasa dengan cepat dan mudah.

d. Sentiasa dikemaskini

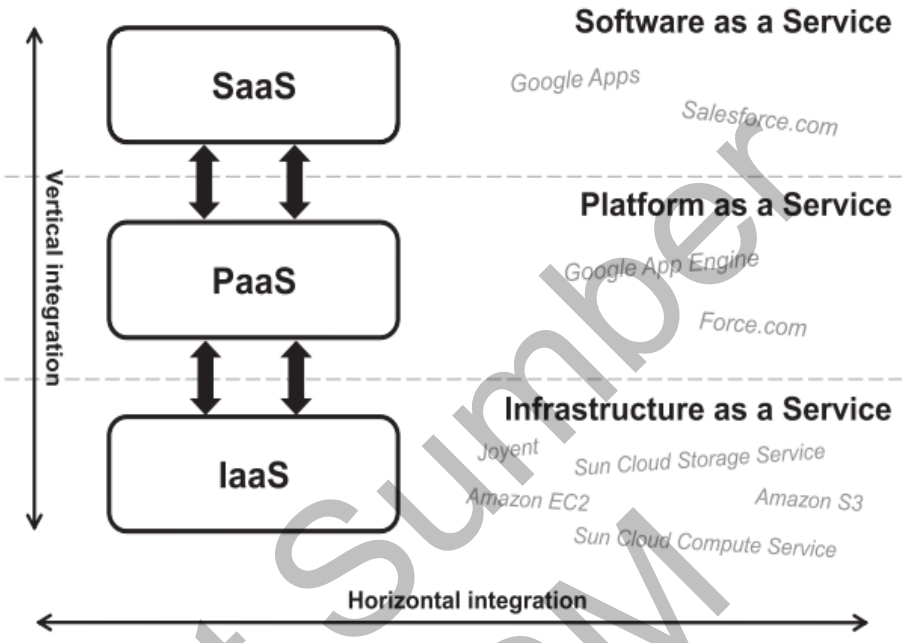
Proses kemaskini perkakasan dan perisian dilakukan oleh pihak penyedia perkhidmatan awan. Pihak pengguna tidak perlu merasa khuatir tentang perkara ini. Segala kemaskini yang telah diuji boleh diadaptasi di dalam persekitaran pengguna pada bila-bila masa setelah diuji oleh penyedia perkhidmatan awan.

e. Platform berskala Besar

Penyedia perkhidmatan awan menyediakan platform yang mempunyai kumpulan sumber yang besar. Sesuatu platform bukan sahaja boleh terdiri dari beribu kumpulan pelayan yang besar dari satu pusat data di sesuatu lokasi tetapi juga boleh didapati dari gabungan pelayan dari beberapa pusat data yang berada di lokasi yang berbeza. Pusat data tersebut juga boleh berada di beberapa negara yang berbeza.

2.2.3 Model perkhidmatan pengkomputeran awan

Terdapat 3 jenis model perkhidmatan pengkomputeran awan yang telah dikenalpasti dan disediakan seperti rajah 2.1 :



Rajah 2.1 Tiga lapisan pengkomputeran awan (Stanoevska-Slabeva & Wozniak 2010)

a. Infrastruktur Sebagai Perkhidmatan (IaaS)

Sebelum kemunculan Pengkomputeran Awan, penyedia perkhidmatan infrastruktur telah diperkenalkan dan digunakan secara meluas. Melalui IaaS ini, penyedia perkhidmatan infrastruktur menyediakan sumber pengkomputeran seperti pemprosesan atau penyimpanan yang boleh diperoleh sebagai perkhidmatan yang boleh diakses melalui rangkaian internet (Stanoevska-Slabeva & Wozniak 2010). Melalui IaaS, pengguna dapat menentukan tahap sumber pengkomputeran yang boleh diperolehi sebagai perkhidmatan seperti perkakasan, perisian, storan dan konfigurasi rangkaian serta keselamatan. IaaS memberikan ruang kepada pengguna untuk menentukan sesuatu sumber yang ditawarkan dikonfigurasi mengikut keperluan sendiri lebih cepat dan mudah.

b. Platform Sebagai Perkhidmatan (PaaS)

Perkhidmatan awan ini akan diakses oleh pengguna melalui rangkain internet. Pengguna tidak memerlukan pemasangan sistem pengoperasian, perisian dan keperluan perkakasan. PaaS menyediakan perkakasan terbina dalam, keselamatan terbina dalam dan antara muka perkhidmatan web untuk aplikasi yang digunakan. Aplikasi yang digunakan boleh disepadukan dengan aplikasi lain pada platform yang sama dan antara muka dengan aplikasi lain di platform yang berlainan. PaaS mempunyai perisian yang terdiri daripada pangkalan data, perisian tengah dan alat pembangunan. (Odun-Ayo et al. 2018)

c. Servis Sebagai Perkhidmatan (SaaS)

Penyedia perkhidmatan awan ini menyediakan perkhidmatan bagi pengguna menggunakan perisian aplikasi berlesen untuk digunakan dan pembelian bilangan lesen tersebut boleh dibuat berdasarkan keperluan semasa pengguna. Perisian aplikasi tersebut boleh diakses melalui rangkaian internet menggunakan pelayar web tanpa pengguna memasang perisian pelanggan atau ejen khusus (Rani & Ranjan 2014). Pengguna perkhidmatan diberi pilihan untuk menukar antaramuka dan rasa perisian aplikasi mengikut kesesuaian syarikat atau pengguna yang disasarkan.

2.2.4 Model pembangunan pengkomputeran awan

Umumnya, terdapat empat model pembangunan pengkomputeran awan yang telah digariskan dan dijadikan rujukan. Model pembangunan Awan yang dimaksudkan adalah seperti berikut:

a. Awan Persendirian (*Private Cloud*)

Model Awan Persendirian ini adalah sebuah model yang digunakan dan dimiliki oleh hanya sebuah organisasi. Hanya pengguna yang berdaftar dengan organisasi tersebut sahaja yang boleh menggunakan segala sumber dan perisian aplikasi di dalam model ini. Secara amnya konsep ini sama sahaja dengan pelayan di pusat data. Walaubagaimanapun, penggunaan teknologi virtualisasi membolehkan kumpulan

pemproses, kumpulan storan dan sumber rangkaian dimanfaatkan dengan kebolehskalaan mengikut keperluan penggunaan di organisasi tersebut (Prajapati et al. 2018). Model ini biasanya dibangunkan oleh pihak kerajaan dan organisasi yang besar dan kritikal kerana ianya menyediakan ciri–ciri keselamatan yang baik bagi menjalankan perisian aplikasi dan maklumat sulit atau rahsia.

b. Awan Awam (*Public Cloud*)

Model Awan Awam ini merupakan model awan yang boleh digunakan oleh orang awam yang mana kos bagi menggunakan model ini adalah berdasarkan kepada tahap penggunaan fungsi perkhidmatan awan tersebut. Perkhidmatan awan yang menggunakan model ini biasanya dimiliki oleh pihak ketiga yang menyediakannya infrastruktur yang dikongsi termasuk storan dan sumber rangkaian. Perkhidmatan awan ini biasanya diakses melalui rangkaian internet. Pengguna tidak dapat mengetahui perkakasan yang digunakan sebagai peranti storan untuk data dan tidak mengetahui lokasi sebenar data disimpan. Penyedia perkhidmatan awan awam seperti Amazon AWS, Microsoft dan Google memiliki dan mengendalikan infrastruktur dan menawarkan akses kepada aplikasi dan storan melalui Internet. Kelemahan bagi model ini ialah dari aspek keselamatan.

c. Awan Komuniti (*Community Cloud*)

Model Awan Komuniti ini merupakan sebuah model yang dikongsi oleh ramai pegguna dan ia memberikan sokongan kepada komuniti tertentu dengan tujuan yang khusus. (Suraj et al. 2018) Tujuan utama penggunaan Awan Komuniti adalah untuk menyediakan gabungan yang sempurna Awan Awam seperti penggunaan sumber dari penyedia perkhidmatan yang berbeza pada masa yang sama mendapatkan fasiliti, kemudahan dan pengebilan kepada setiap penggunaan secara privasi dan ciri keselamatan seperti model Awan Persendirian.

d. Awan Hibrid (*Hybrid Cloud*)

Model Awan Hibrid ini merupakan gabungan infrastruktur pusat data di premis sendiri, Awan Persendirian dan Awan Awam. Sebuah organisasi yang mempunyai

latar belakang berasaskan teknologi maklumat adalah sebuah organisasi hibrid melainkan sepenuhnya menggunakan infrastruktur pusat data di premis sendiri atau sepenuhnya menggunakan perkhidmatan awan (Odun-Ayo et al. 2018). Sebuah perisian aplikasi dengan keperluan yang sentiasa berubah meningkat dan menurun yang tidak konsisten untuk sumber rangkaian dan storan paling sesuai menggunakan awan awam, manakala awan persendirian pula akan digunakan aplikasi memerlukan sumber rangkaian tahap tinggi yang berterusan dan mengendalikan maklumat sulit atau rahsia.

2.3 FORENSIK DIGITAL BAGI PENGKOMPUTERAN AWAN

2.3.1 Forensik digital

Forensik digital adalah kaedah yang diterbitkan secara saintifik dan pembuktian yang bertujuan untuk memelihara, mengumpul, mengesahkan, mengenal pasti, menganalisis, mentafsir, mendokumenkan dan mempersembahkan bukti digital yang mengekalkan rantaian bukti yang didokumenkan untuk pembentangan di mahkamah (Morioka & Sharbaf 2016). Pada masa ini, pendakwaan dan sabitan penjenayah siber bergantung sepenuhnya kepada bukti digital yang dikumpul menggunakan prosedur yang mematuhi undang-undang biasa dan peraturan perundangan.

2.3.2 Forensik awan

Walaupun tiada definisi rasmi untuk forensik awan (Morioka & Sharbaf 2016) beberapa pengkaji bersetuju bahawa forensik awan merupakan disiplin yang bersamaan antara pengkomputeran awan dan forensik digital. Seperti dalam forensik digital, bukti yang terdapat dalam forensik awan mesti memenuhi keperluan yang sama seperti bukti konvensional, dan beberapa cabaran dalam forensik awan adalah bagi memenuhi keperluan tersebut.

2.3.3 Metodologi digital forensik

Keselamatan awan, privasi dan forensik merupakan isu yang saling berkaitan. Perkara–perkara ini selalunya diabaikan sehingga atau melainkan masalah timbul

dalam penggunaan sistem. Pelbagai jenis serangan yang berbeza boleh menyebabkan maklumat sensitif jatuh kepada pihak yang tidak sepatutnya, seterusnya kerahsiaan, integriti dan ketersediaan perkhidmatan awan turut terancam (Bhatia & Malhotra 2019). Penyedia perkhidmatan awan selalunya akan tergesa-gesa untuk melancarkan atau menyediakan lebih banyak perkhidmatan bagi menambah pelanggan baharu seawal mungkin untuk memperoleh lebih banyak hasil dan keuntungan tanpa pelaksanaan dan konfigurasi awan yang betul terhadap privasi, keselamatan dan kecekapan forensik. Sehingga hari ini, kajian mengenai metodologi dan alatan dalam bidang forensik awan masih kurang dan terdapat jurang keselamatan yang perlu dipenuhi.

2.4 BAWA PERANTI ANDA SENDIRI (BYOD)

Fenomena Bawa Peranti Anda Sendiri (BYOD), adalah di mana syarikat membenarkan pekerja membawa peranti elektronik mereka sendiri untuk mengakses data syarikat pada bila-bila masa, dari mana-mana sahaja, melalui mana-mana peranti, telah merebak dengan pantas dalam beberapa tahun kebelakangan ini (Iovan & Ivănuş 2018). Pada masa kini, boleh dikatakan kesemua pekerja mempunyai peralatan elektronik yang mempunyai sambungan internet sendiri samada melalui telefon pintar, tablet atau komputer riba. Sambungan internet ini mungkin sahaja dari pembekal perkhidmatan telefon atau kemudahan wifi percuma di tempat – tempat awam.

2.4.1 Faedah penggunaan BYOD

Dalam literatur tentang BYOD terdapat tiga faedah utama yang biasanya diketengahkan; peranti peribadi meningkat produktiviti, peningkatan fleksibiliti masa dan tempat serta peningkatan kepuasan pekerja dalam melaksanakan tugas (Brodin et al. 2015). Kajian menunjukkan bahawa pekerja yang dibenarkan menggunakan peranti elektronik yang sama untuk tujuan peribadi dan kerja melaksanakan kerja lebih banyak banyak daripada yang lain dan menjimatkan masa yang banyak untuk syarikat mereka. Ini disebabkan oleh fleksibiliti untuk bekerja pada bila-bila masa dan di mana sahaja pekerja mahu. Walau bagaimanapun fleksibiliti ini bukan sahaja memberi manfaat kepada organisasi dan pekerja dalam melaksanakan tugasan, malahan ianya juga pada masa yang sama memberikan kesan terhadap kehidupan peribadi pekerja.

Pekerja akan merasakan diri mereka terbeban untuk melakukan kerja pada bila-bila masa dengan segera kerana kerja-kerja dapat dicapai pada bila-bila masa melalui peranti yang telah dibekalkan oleh organisasi.

2.4.2 Cabaran perlaksanaan BYOD

Penggunaan BYOD di pejabat mempunyai cabaran yang tersendiri. Kebanyakannya cabaran yang telah dikenalpasti adalah mengenai keselamatan. Antara cabaran yang paling penting adalah peralatan/peranti yang di bawa untuk digunakan untuk mengakses data atau aplikasi organisasi tidak ditentusahkan sebagai peralatan yang selamat dan diuruskan oleh Jabatan IT organisasi tersebut (Morrow 2012; Olalere et al. 2015). Pada masa yang sama, ini menyukarkan organisasi untuk memastikan semua peranti yang digunakan oleh setiap pekerja dan mengandungi data organisasi dilindungi keselamatannya ke tahap maksimum. Tahap keselamatan setiap peranti yang dikeluarkan ketika ini adalah berbeza dan boleh dipersoalkan menyebabkan kawalan ke atas maklumat menjadi lebih sukar. Organisasi perlu melihat terhadap kebarangkalian yang akan berlaku kepada data apabila peranti yang disimpannya hilang atau dicuri, atau jika pekerja meninggalkan organisasi kerana berhenti bekerja untuk bersama dengan organisasi pesaing syarikat asal. Menurut (Olalere et al. 2015) terdapat tiga ancaman BYOD yang telah dikenalpasti terhadap organisasi adalah seperti Jadual 2.1 di bawah:

Jadual 2.1 Ancaman biasa BYOD dengan punca dan implikasinya

No.	Serangan	Punca Serangan	Implikasi Terhadap Organisasi
1	**Kebocoran Data**	• Pengguna mudah alih yang berniat jahat • Akses secara jauh melalui peranti mudah alih oleh penyerang • Kehilangan peranti • Aplikasi jahat • Kejuruteraan Sosial	• Maklumat rahsia organisasi terdedah kepada umum
2	**DDoS**	• Niat jahat oleh penyerang • Eksploitasi kelemahan rangkaian	• Kesan buruk kepada pelayan • Akses tidak dapat dicapai oleh pengguna yang sah.
3	**Perisian hasad**	• Aplikasi Trojan : Kod jahat yang dimasukan di dalam apolikasi oleh penyerang dengan niat bagi menyerang organisasi • Pautan dari Media Sosial, Emel dan pesanan ringkas • Aplikasi dari pihak ketiga yang tidak ditentusahkan keselamatannya kemungkinan memudarat peranti, sistem dan rangkaian	• Aplikasi korporat organisasi gagal berfungsi dengan baik • Infrastruktur korporat dan peralatan pekerja sendiri terkesan oleh kod jahat.

2.5 PILIH PERANTI ANDA SENDIRI (CYOD)

Melihat terdapatnya masalah pengurusan dalam implementasi BYOD terutamanya dari segi keselamatan maklumat organisasi dan kawalan terhadap peranti yang digunakan oleh pekerja bagi menjalankan tugas pejabat, satu konsep baru telah diperkenalkan bagi mengatasi masalah tersebut iaitu Pilih Peranti Anda Sendiri (*Choose Your Own Device* (CYOD)). Konsep serba baharu dalam syarikat CYOD, di mana syarikat membenarkan pekerja memilih peranti yang mereka mahu gunakan di pejabat, semakin popular sebagai alternatif kepada fenomena konsep BYOD (Iovan et al. 2018).

2.5.1 CYOD alternatif kepada BYOD

Alternatif yang cuba mencari 'jalan tengah' dalam menyelesaikan masalah/isu bagi perlaksanaan BYOD di organisasi adalah perlaksanaan konsep Pilih Peranti Anda Sendiri (CYOD). CYOD membolehkan pekerja memilih peranti, tanpa mengeluarkan kos peribadi, yang paling sesuai untuk mereka dalam melaksanakan tugas, pada masa yang sama organisasi dapat mengawal peranti tersebut (De Kok et al. 2015). Faedah yang boleh dimanfaat oleh kedua-dua belah pihak menjadikan CYOD semakin popular, terutamanya dalam organisasi yang lebih besar. Terdapat penyelidikan sedia ada mengenai BYOD digunakan sebagai asas dalam pertimbangan melaksanakan penyelidikan dalam bidang dasar konsep CYOD, terutamanya berdasarkan keselamatan maklumat organisasi.

2.5.2 Faedah penggunaan CYOD

Faedah penggunaan konsep CYOD adalah sangat besar, kerana setiap peranti yang dibekalkan boleh diprapasang dengan penyelesaian keselamatan dan tembok api serta tetapan rangkaian yang telah dikonfigurasi oleh pentadbir khusus di organisasi (Iovan & Ivănuş 2018). Pengurusan yang terhad terhadap sebilangan kecil spesifikasi peranti berbeza membolehkan penyimpanan rekod dilaksanakan dan memastikan pekerja sentiasa mematuhi keperluan pengurusan data dan maklumat.

Walau bagaimanapun, sebuah organisasi mesti menyediakan peranti pelbagai jenis yang terkenal sebagai sebahagian daripada program CYOD untuk menarik perhatian pekerja dan memperoleh minat mereka. Kemudahanyang disediakan oleh organisasi kepada pekerja melalui program CYOD baharu membuktikan keperluan dan juga kecekapan transformasi dan pengurusan perubahan ke dalam bentuk baharu penggunaan peranti di tempat kerja.

Keselamatan data dan maklumat adalah penting, dan organisasi menawarkan rangkaian dengan penyelesaian keselamatan yang diperlukan.Terdapat beberapa langkah mudah yang perlu diikuti oleh mana-mana organisasi, tanpa mengira perniagaan atau saiz, untuk memastikan keselamatan infrastruktur dan data.

Bagi memilih strategi dan peranti yang menyokong produktiviti pekerja. Adalah disyorkan agar organisasi menguji peranti secara menyeluruh dari perspektif keselamatan maklumat dan kemudahan pekerja bagi menentukan corak kerja terbaik untuk organisasi, sama ada BYOD atau CYOD. Pada masa yang sama, setiap ahli jabatan IT yang bertanggungjawab untuk peranti mudah alih mesti mempunyai pemahaman yang jelas tentang isu yang mereka hadapi.

Setiap organisasi perlu membentuk pasukan yang ideal untuk melaksanakan konsep CYOD yang mana ianya melibatkan IT, undang-undang, sumber manusia, keselamatan dan operasi perniagaan. Kesemua kumpulan ini mempunyai kepentingan dalam produktiviti dan keselamatan ruang kerja dan peranti yang digunakan dalam syarikat. Setiap individu hendaklah sentiasa memainkan peranan yang telah ditetapkan bagi menjamin perlaksanaan CYOD ini dapat meningkatkan produktiviti selain memastikan keselamatn data/maklumat organisasi sentiasa terpelihara.

2.5.3 Cabaran perlaksanaan CYOD

Isu yang menjadi perbincangan perlaksanaan CYOD di organisasi adalah siapakah yang akan mengeluarkan peruntukan bagi membeli peranti yang ingin digunakan. Bagi sebuah syarikat yang mempunyai ramai pekerja, membekalkan sebuah peranti yang diminati oleh pekerja merupakan satu cabaran kerana ianya mungkin melibatkan kos yang agak tinggi. Dari sudut pandangan pekerja pula, membeli sebuah peranti yang mudah digunakan dan diminati mungkin tiada masalah, cuma apabila peranti tersebut perlu dipasang dengan aplikasi-aplikasi keselamatan yang telah dikonfigurasi oleh organisasi menyebabkan terdapat rasa kurang senang kerana kemungkinan privasi kehidupan seharian mereka mungkin diceroboh oleh organisasi.

Di dalam konsep ini, organisasi telah menetapkan prapilihan peranti dan prakonfigurasi yang diperlukan sebelum ianya diterima untuk disambung kepada rangkaian organisasi. Perkara ini perlulah dipersetujui oleh pekerja juga kerana kemungkinan peranti tersebut digunakan untuk urusan harian/peribadi yang mana jejak audit urusan tersebut mungkin boleh dilihat oleh organisasi melalui aplikasi yang telah ditetapkan di dalam peranti tersebut menyebabkan akhirnya perlaksanaan CYOD

ini mungkin tidak dapat sambutan yang diharapkan oleh organisasi (Iovan & Ivănuş 2018).

Pekerja pada dasarnya mungkin bersetuju dengan organisasi untuk menguruskan aplikasi organisasi pada peranti mudah alihnya tetapi tidak bersetuju untuk pihak organisasi memutuskan perkara yang boleh atau tidak boleh dilakukan menggunakan peranti tersebut. Isu-isu utama berkaitan konsep CYOD adalah seperti jadual 2.3 (Akram & Markantonakis 2016):

Jadual 2.2 Isu-isu berkaitan konsep CYOD

Isu	Keterangan
1 Pemilikan Peranti	Pemilikan sebenar peranti adalah berdasarkan pihak yang membayar peranti tersebut. Walau bagaimanapun, organisasi akan menetapkan polisi atau peraturan pada peranti sedemikian.
2 Kawalan Aplikasi	Pekerja boleh memuat turun aplikasi pada peranti tetapi organisasi memasang beberapa aplikasi keselamatan pada peranti yang tidak boleh dipadamkan oleh pekerja. Pekerja mungkin diberi peluang untuk memasang dan memadam mana-mana aplikasi yang mereka mahu, kecuali yang telah dipasang oleh organisasi.
3 Melindungi Aset Syarikat	Organisasi mempunyai peranan utama dalam hal ini tetapi bantuan pekerja adalah perlu. Segala kemas kini berkaitan keselamatan boleh ditolak ke peranti tersebut. Pekerja perlu menggunakan peranti dengan cara yang selamat supaya ianya tidak menjadi laluan kepada kelompangan keselamatan.
4 Tanggungjawab untuk Menjaga Peranti	Tanggungjawab terletak pada kedua-dua organisasi dan pekerja
5 Isu Privasi	Organisasi mungkin masih boleh menangkap aktiviti pengguna tetapi terhad kepada aktiviti tertentu yang berkaitan dengan keselamatan dan kebolehpercayaan aplikasi organisasi.
6 Kebolehgunaan dan Kebebasan Penggunaan untuk Pekerja	Pengguna mempunyai kebebasan terhad untuk menggunakan peranti seperti yang mereka inginkan, selagi mereka tidak melanggar polisi keselamatan syarikat.

2.6 KESIMPULAN

Faedah yang dihubungkaitkan kepada kedua-dua konsep BYOD dan CYOD adalah peningkatan produktiviti oleh pekerja, walaupun bagi pekerja yang tidak berpengalaman ia mungkin mendapat keuntungan yang lebih besar dengan penggunaan kedua – dua konsep ini. Jika peranti CYOD dibenarkan untuk digunakan walaupun untuk tujuan persendirian peningkatan fleksibiliti masa dan ruang akan sama untuk kedua-dua BYOD dan CYOD. Kedua-dua faedah ini, dalam kedua-dua kes, akan membawa kepada peningkatan kepuasan pengguna menyelesaikan tugas

yang telah diberikan oleh organisasi menggunakan peranti yang disukai (Brodin 2016).

Perbezaan yang telah dikenalpasti pula adalah aspek keselamatan, cara melindungi maklumat pada peranti mudah alih. Apabila peranti yang digunakan adalah milik oleh organisasi, organisasi mempunyai lebih kawalan ke atas peranti itu dan boleh menetapkan peraturan dan polisi keselamatan pada peranti itu. Pada peranti milik persendirian, terpulang kepada pengguna untuk melindungi peranti dan maklumatnya. Apabila seorang pekerja meninggalkan organisasi peranti CYOD boleh dipadamkan sepenuhnya, tetapi untuk peranti BYOD, terpulang kepada pengguna untuk mengalih keluar semua data yang dimiliki oleh bekas majikan mereka.

Satu faktor yang dilihat memisahkan CYOD daripada BYOD adalah kemungkinan penyiasatan lebih mendalam dalam kes-kes pelanggaran sesuatu peraturan atau polisi yang disyaki. Jika peranti itu CYOD majikan boleh mengambil peranti dan melakukan penyiasatan forensik, jika ia adalah BYOD majikan telah tiada hak untuk memperolehi peranti itu dan tidak boleh menjalankan penyiasatan. Melalui BYOD pengguna boleh mempunyai lebih daripada satu peranti pada rangkaian, yang memerlukan lebih banyak kapasiti rangkaian dan ini boleh menyebabkan lebih banyak peranti memerlukan bantuan sokongan daripada organisasi.

Kesimpulan yang boleh didapati dari perbincangan ini walaupun kos peranti itu sendiri lebih tinggi dengan CYOD kerana peranti perlu disediakan oleh organisasi dengan pra pemasangan aplikasi keselamatan dan pra konfigurasi tetapan rangkaian, peningkatan tahap keselamatan bagi maklumat dan organisasi serta kawalan terhadap peranti mengatasi faktor peningkatan kos perolehan.

BAB III

METODOLOGI

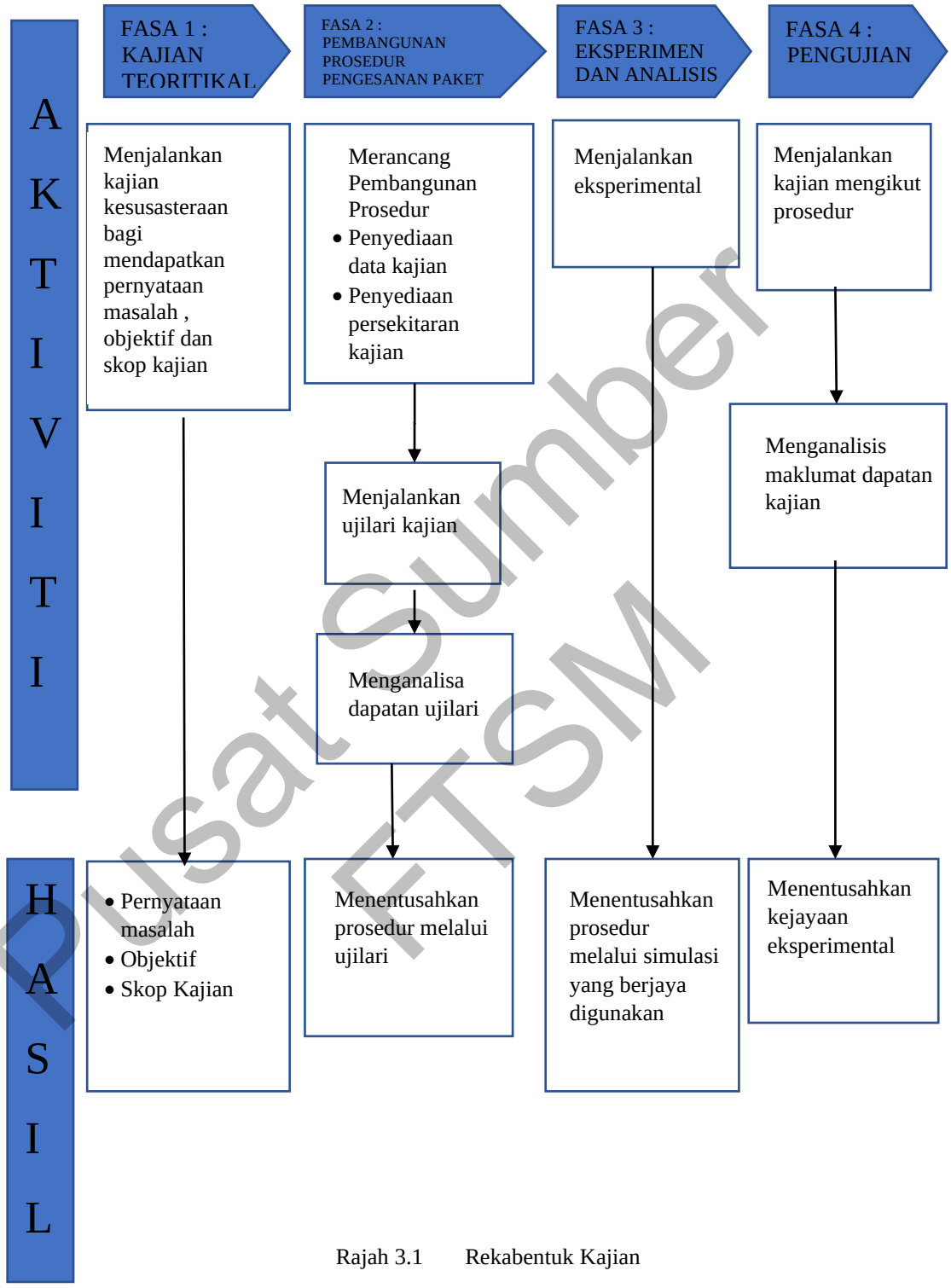
3.1 PENGENALAN

Bab ini membincangkan mengenai kaedah dan pendekatan yang digunakan semasa menjalankan kajian ini. Ianya juga menerangkan segala aktiviti yang dilaksanakan di dalam setiap fasa bagi mencapai objektif kajian yang telah ditetapkan.

3.2 METODOLOGI KAJIAN

Pendekatan yang digunakan dalam metodologi kajian melibatkan empat fasa iaitu (1) kajian teoretikal; (2) pembangunan prosedur pengesanan paket; (3) Eksperimen dan analisis; dan (4) pengujian. Rajah 3.1 menunjukkan metodologi kajian yang merangkumi fasa-fasa tersebut. Setiap fasa mempunyai beberapa aktiviti yang dirancang mengikut keutamaan berdasarkan kesesuaian organisasi yang dikaji untuk mencapai hasil dan objektif yang ditetapkan di Bab I. Pecahan fasa tersebut juga mampu memberi pemahaman terperinci tentang mengaplikasikan kaedah serta huraian tentang proses kajian.

Reka bentuk kajian ini adalah berbentuk kaedah eksperimen (Ross & Morrison 2013). Kaedah eksperimen ini dapat mengkaji isu yang terpilih secara terperinci dan mendalam. Kaedah ini turut memboleh matlamat utama dicapai melalui hasil maklumat yang lebih spesifik dan memudahkan pengumpulan maklumat serta dapat menumpukan lebih perhatian terhadap kajian yang dilakukan di dalam persekitaran yang terkawal. Kaedah eksperimen juga memberikan peluang untuk proses simulasi dilaksanakan berulang kali bagi mengesahkan kejayaan prosedur yang dibangunkan.



Rajah 3.1 Rekabentuk Kajian

3.2.1 Fasa 1: Kajian teoretikal

Permulaan kajian dimulakan dengan melaksanakan kajian kesusasteraan seperti yang dibincangkan di dalam Bab II iaitu mengenai pengkomputeran awan dan konsep Bawa Peranti Anda Sendiri (BYOD) dan Pilih Peranti Anda Sendiri (CYOD). Analisis tersebut juga bertujuan untuk mendapatkan penyataan masalah, objektif dan skop kajian seperti di Bab I.

3.2.2 Fasa 2 dan 3: Pembangunan prosedur pengesanan paket dan eksperimen serta analisis

Pembangunan prosedur pengesanan paket dan eksperimen dijalankan dengan menggunakan kaedah iaitu simulasi eksperimen yang melibatkan empat fasa iaitu (1) persediaan; (2) perancangan pengujian; (3) pelaksanaan; dan (4) pasca pengujian (Bruns 2010). Simulasi ini memberi anggapan bahawa persekitaran kajian yang terkawal menggunakan mesin maya adalah sebagai penganti peranti yang digunakan di dalam sesebuah organisasi yang mengaplikasikan konsep Pilih Peranti Anda Sendiri (CYOD).

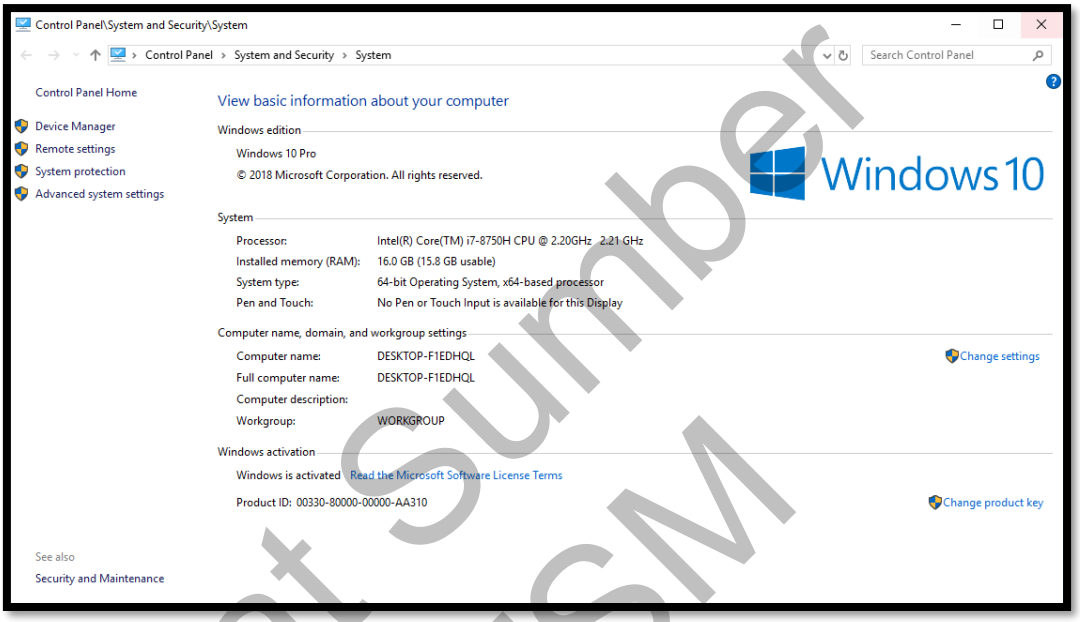
a. Fasa Persediaan

Sebelum memulakan aktiviti simulasi, pemilihan persekitaran hendaklah ditentukan terlebih dahulu. Pemilihan ini penting bagi memastikan kajian eksperimen dilakukan dalam persekitaran yang terkawal. Terlebih dahulu, Jadual 3.1 merupakan perisian-perisian yang telah dipilih bagi melaksanakan kajian ini.

Jadual 3.1 Perisian-perisian yang digunakan

	Perisian	Keterangan
1	**VMware (mesin maya)**	Mewujudkan persekitaran terkawal
2	**Windows 11**	Sistem pengoperasian yang digunakan sepanjang eksperimen
3	**Google Chrome**	Pelayar web yang digunakan
4	**sync.com**	Penyedia perkhidmatan awan yang digunakan
5	**Wireshark**	Perisian bagi analisa paket rangkaian

Spesifikasi komputer yang digunakan dalam melaksanakan eksperimen juga adalah penting bagi memastikan eksperimen dapat dijalankan dengan lancer dan tanpa apa-apa masalah dari segi keupayaan dalam menjalankan aplikasi-aplikasi yang telah dipilih di dalam mewujudkan persekitaran kawalan. Rajah 3.2 adalah rajah spesifikasi komputer yang digunakan dalam melaksanakan kajian ini.



Rajah 3.2 Spesifikasi komputer yang digunakan untuk tujuan kajian

Bagi tujuan persiapan perisian pula, berikut adalah langkah–langkah yang telah diambil bagi menyediakan persekitaran kajian.

1. Muat turun perisian VMware Workstation 16 Pro dari https://www.vmware.com/asean/products/workstation-pro/workstation-pro-evaluation.html

2. Muat turun Windows 11 dari https://www.microsoft.com/software-download/windows11

3. Muat turun perisian vmss2core-sb-8456865.exe dari https://kb.vmware.com/s/article/2003941 untuk menjana dump.dmp dari snap shot guest OS di VMware.

4. Muat turun perisian bulk_extractor64.exe dari https://bulk-extractor.software.informer.com/1.5/ untuk menjana PCAP fail dari fail dump.dmp

5. Muat turun perisian Google Chrome dari https://www.google.com/chrome/ untuk digunakan sebagai pelayar internet di dalam Guest OS.

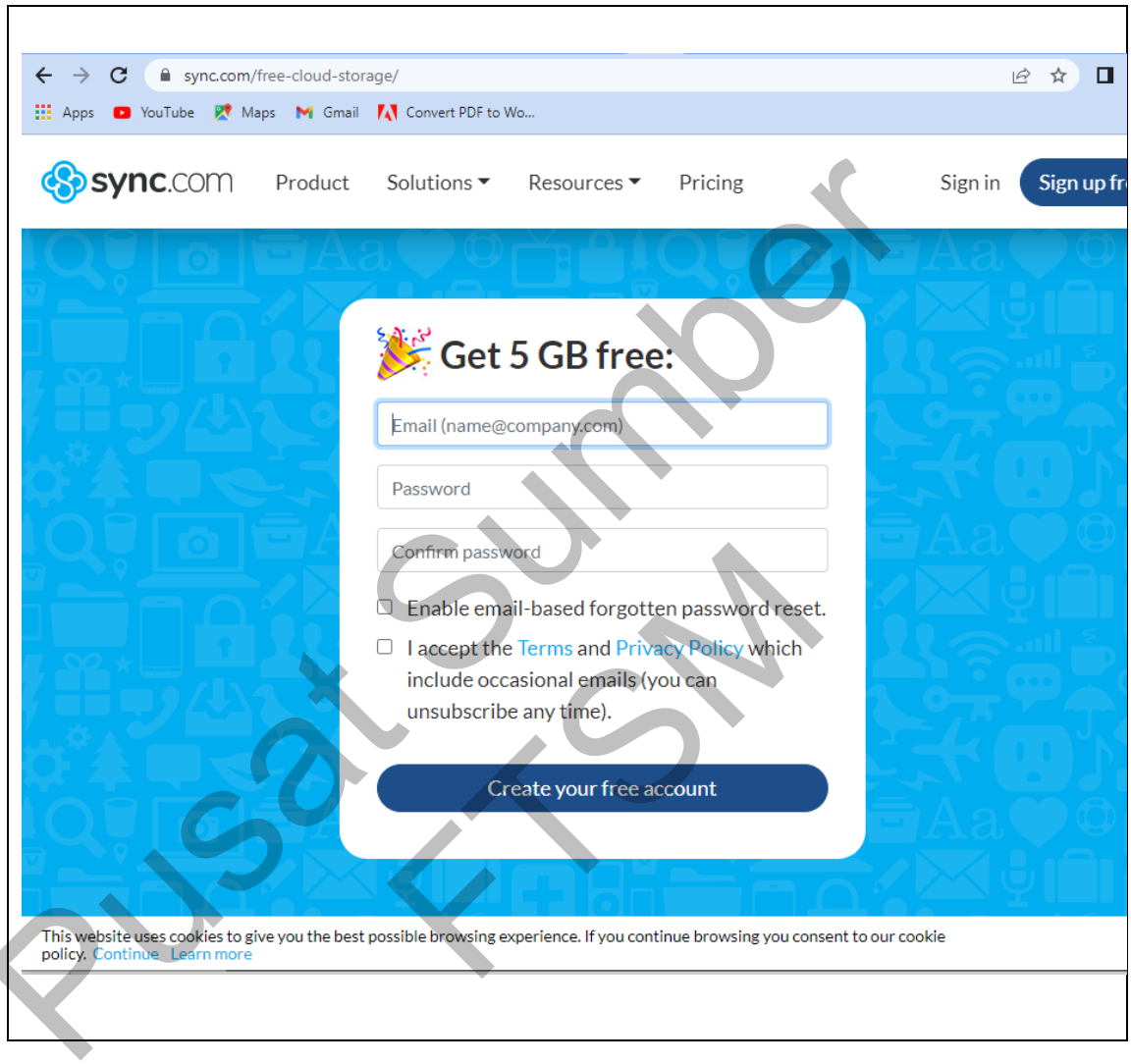
6. Muat turun perisian Network Analyzer (Wireshark) dari https://www.wireshark.org/download.html

b. Fasa Perancangan Pengujian

Setelah memuat turun semua perisian yang diperlukan. Proses penyediaan persekitaran terkawal untuk kajian diteruskan dengan memasang perisian-perisian tersebut di dalam komputer. Rajah 3.3 menunjukkan perisian VMware yang telah dipasang dan dilengkapkan dengan satu mesin maya yang dipasang sistem pengoperasian Windows 11.

Rajah 3.3 Perisian VMware yang telah dipasang perisian Windows 11 di dalam mesin maya.

Laman bagi pendaftaran pengguna baru adalah seperti di rajah 3.4. Manakala data pengujian bagi pengguna yang dipenyedia perkhidmatan awan iaitu www.sync.com juga telah disediakan seperti jadual 3.2:



Rajah 3.4 Laman pendaftaran pengguna baru bagi sync.com

Jadual 3.2 Senarai maklumat pengguna di dalam kajian

Pengguna	Alamat Emel	Kata Laluan
Pengguna 1	sarjana.user1@gmail.com	Sarjana@1234
Pengguna 2	cloudforensic.user2@gmail.com	Master@1234
Pengguna 3	saas.forensics@gmail.com	Saas@1234

Setiap pengguna juga disediakan satu set data untuk tujuan kajian penggunaan storan di perkhidmatan awan. Set data ini akan digunakan untuk sesi kajian di mana set data ini akan dimuat naik atau di muat turun dari laman web penyedia perkhidmatan awan sync.com menggunakan pelayan internet atau aplikasi client yang

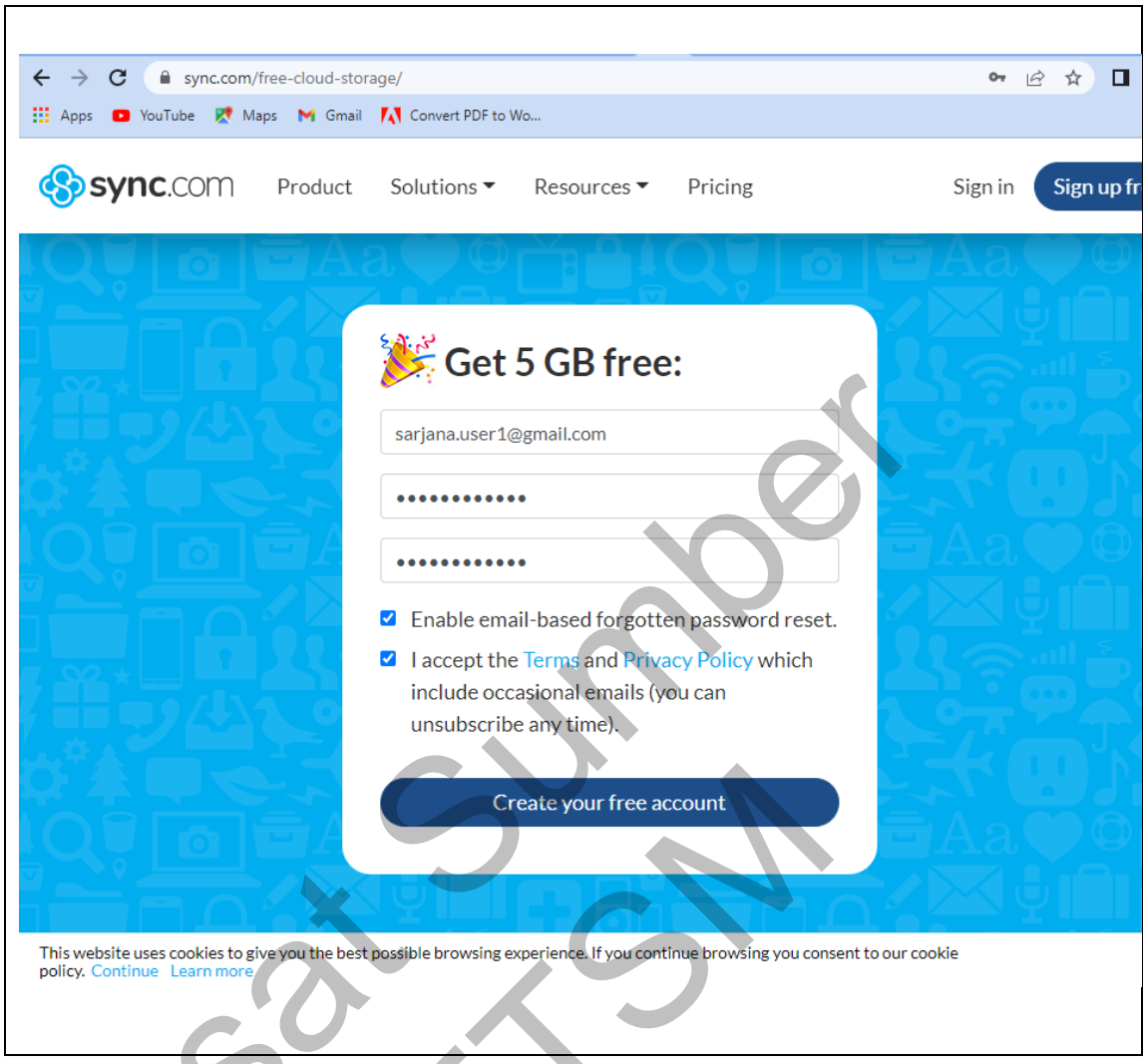
disediakan oleh sysnc.com. Aktiviti seperti ini akan melibatkan penggunaan paket rangkaian yang akan dikenalpasti seterusnya menjadi salah satu objektif kajian ini. Set data yang telah disediakan bagi tujuan eksperimen ini terdiri dari 3 jenis format iaitu fail jenis *.jpg, *.docx dan *.txt. Format-format ini dipilih kerana ianya merupakan jenis format yang biasa digunakan oleh pengguna dalam urusan pekerjaan seharian iaitu berkaitan dengan gambar, dokumen dan teks biasa. Set data tersebut adalah seperti di jadual 3.3 di bawah:

Jadual 3.3 Set data pengujian penggunaan storan di perkhidmatan awan

Pengguna	Nama Fail	Jenis Fail
Pengguna 1	Gambar User 1	.jpg
	Report User 1	.docx
	Memori User 1	.txt
Pengguna 2	Gambar User 2	.jpg
	Report User 2	.docx
	Memori User 2	.txt
Pengguna 3	Gambar User 3	.jpg
	Report User 3	.docx
	Memori User 3	.txt

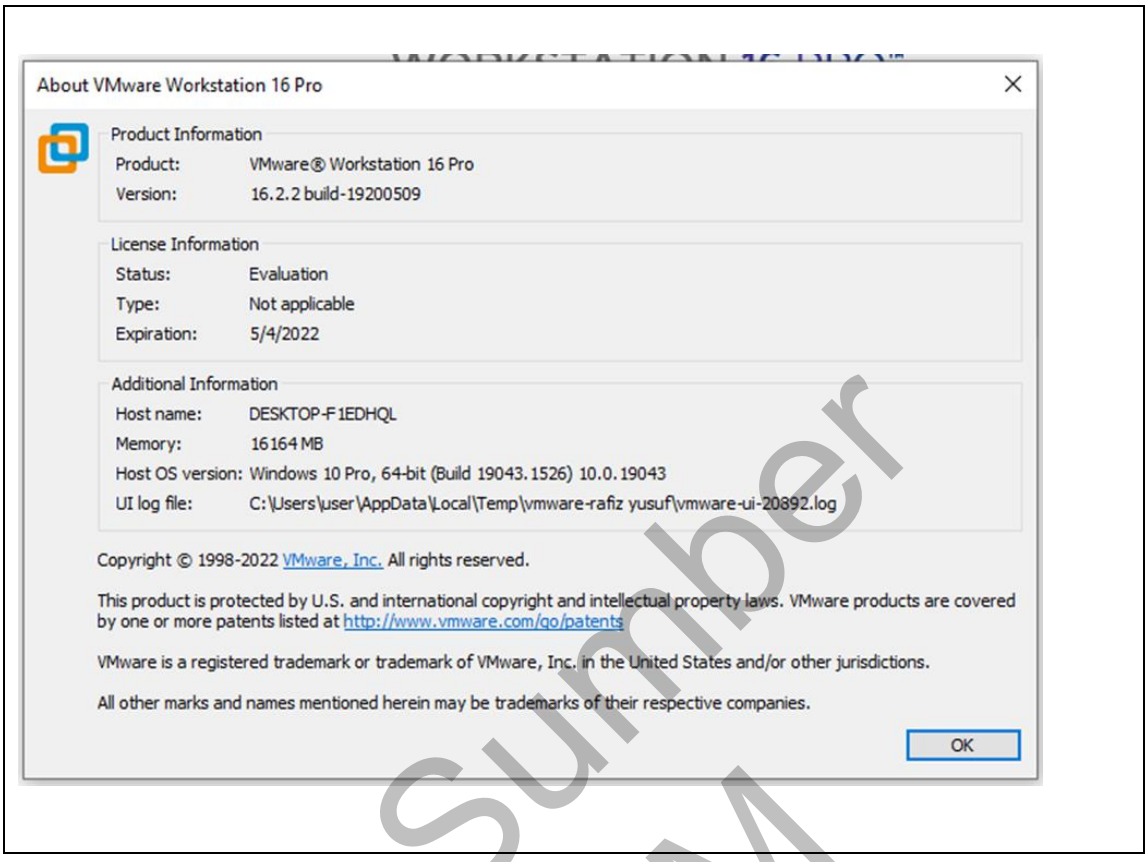
c. Fasa Pelaksanaan

Bagi memastikan aktiviti kajian berjalan dengan lancar. Proses pendaftaran pengguna telah dilakukan dengan memasukkan maklumat-maklumat pengguna yang telah disediakan di dalam Jadual 3.2. Aktiviti pendaftaran pengguna baharu di laman sesawang sync.com dilaksanakan seperti di Rajah 3.5.

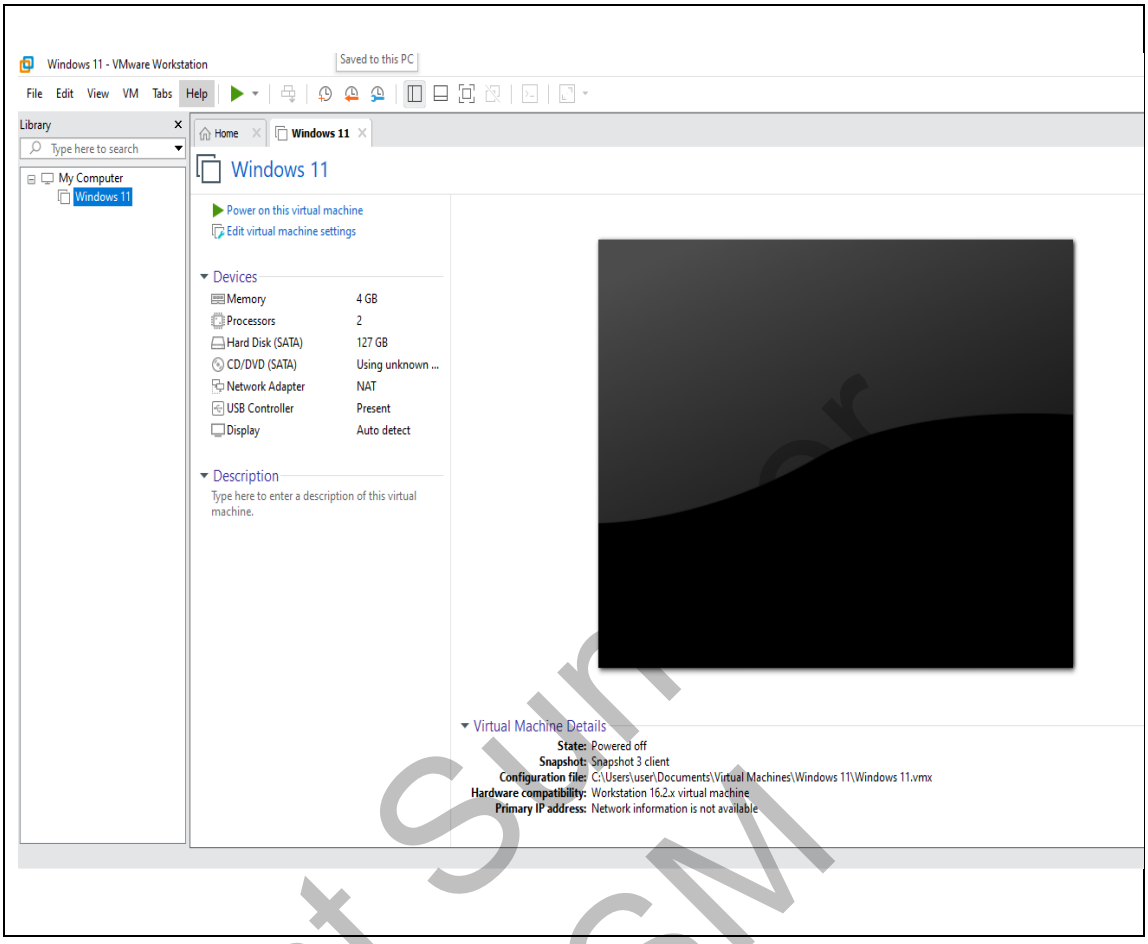


Rajah 3.5 Pendaftaran pengguna di penyedia perkhidmatan awan

Rajah 3.6 menunjukkan maklumat perisian VMware yang telah dipasang di komputer *host*. Perisian VMware ini akan digunakan untuk mencipta mesin maya yang akan digunakan sepanjang eksperimen dilaksanakan. Rajah 3.7 menunjukkan mesin maya yang telah dicipta di dalam perisian VMware telah dipasang sistem pengoperasian Windows 11 dengan konfigurasi sistem seperti di rajah tersebut.

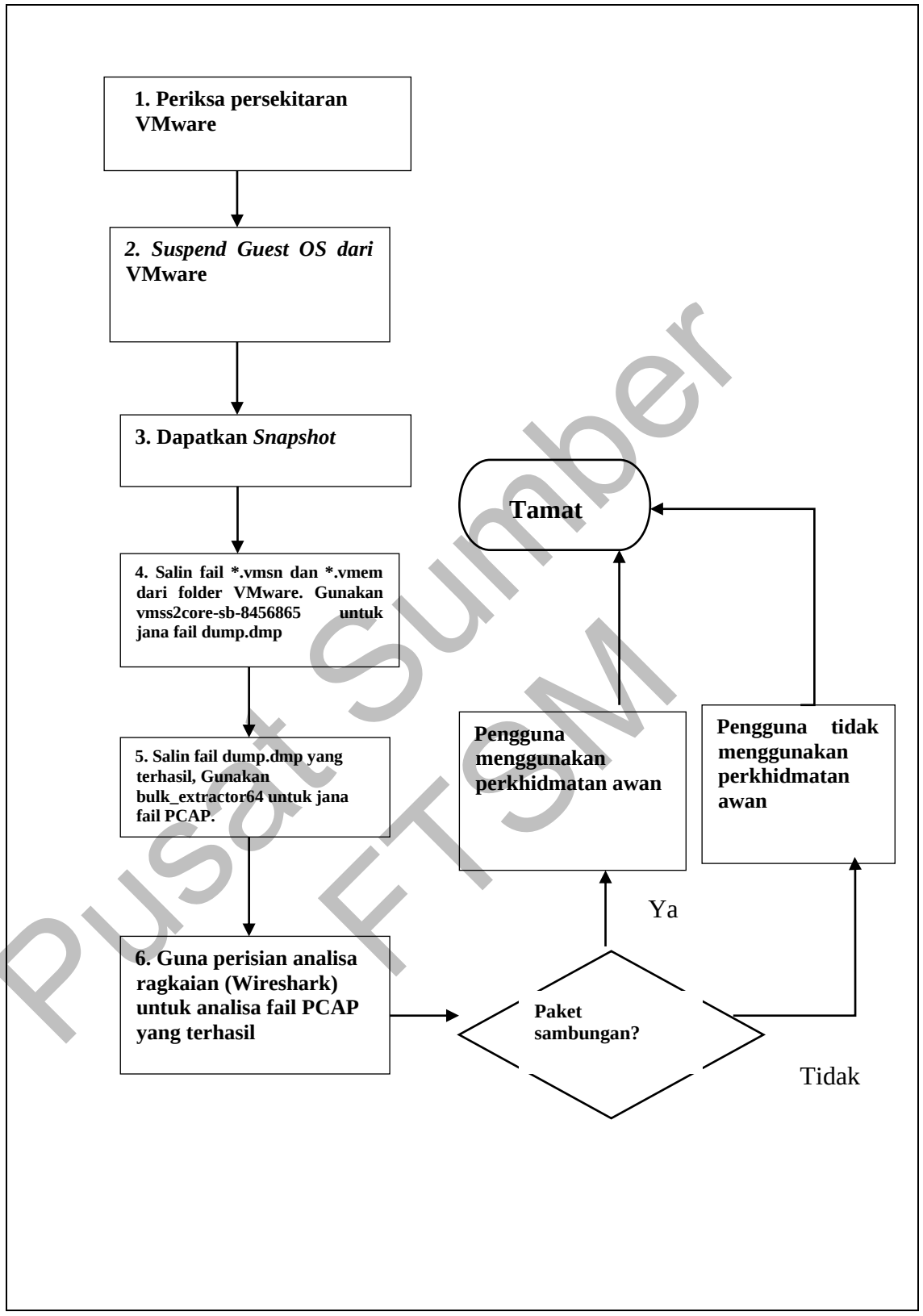


Rajah 3.6 Maklumat perisian VMware yang telah dipasang di komputer *host*



Rajah 3.7 Sistem pengoperasian Windows 11 telah di pasang di dalam mesin maya

Proses pelaksanaan ini dapat menentu sahkan prosedur penjejakan paket melalui simulasi kajian yang dibuat mengikut aliran kerja seperti yang ditunjukkan di dalam Rajah 3.8.



Rajah 3.8 Prosedur mengesan penggunaan perkhidmatan awan dari konsep pilih peranti anda sendiri (CYOD)

3.2.4 Fasa 4: Pengujian

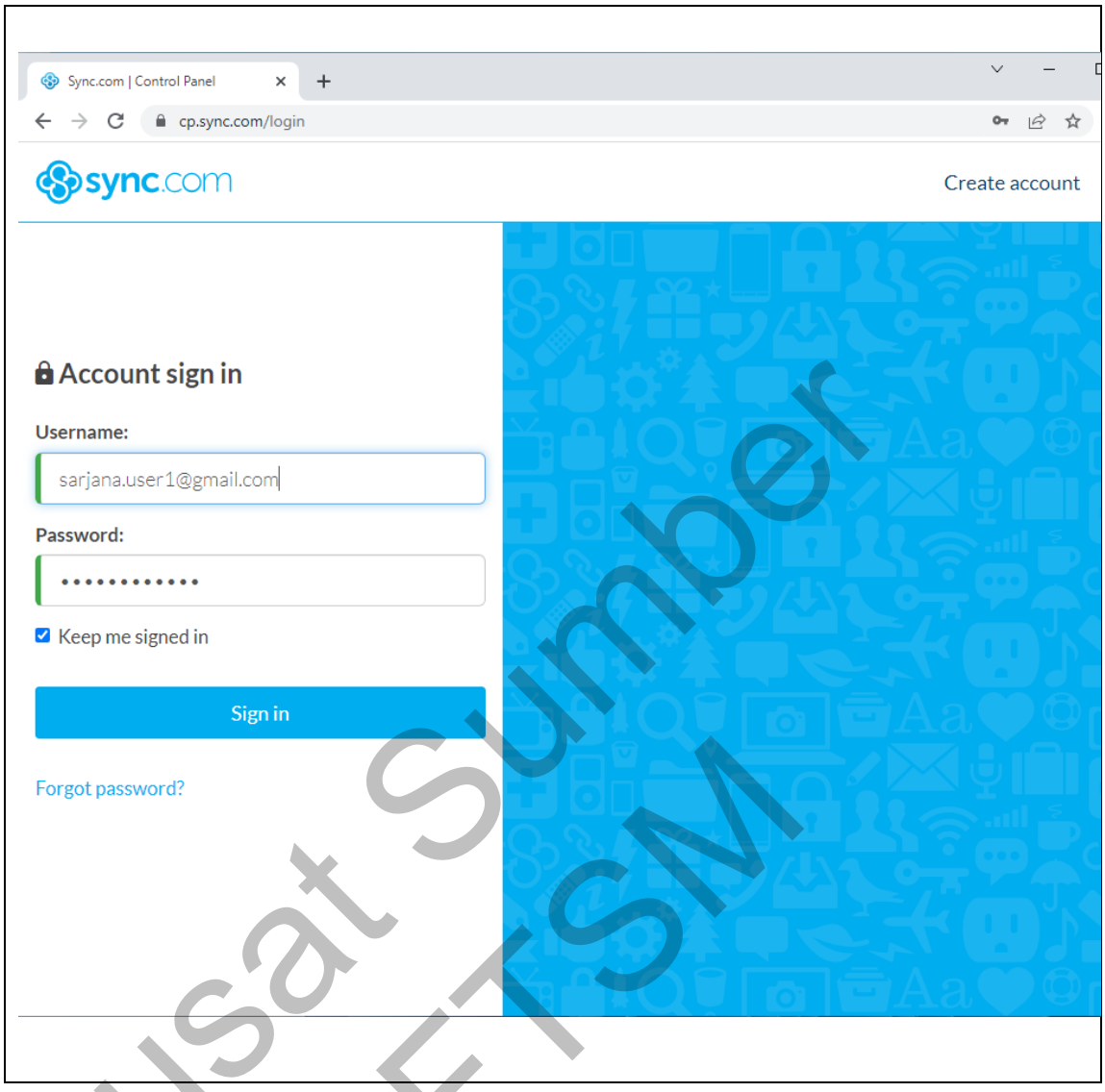
Kaedah eksperimen digunakan di dalam fasa pasca pengujian bertujuan untuk mengetahui keberkesanan prosedur penjejakan paket yang telah dibangunkan. Kaedah eksperimen ini juga dapat mengenal pasti maklumat yang dihasilkan seterusnya prosedur penjejakan paket yang dibangunkan dapat disahkan dengan segera.

a. Fasa Pengujian

Setelah eksperimen dijalankan mengikut prosedur yang telah dibangunkan ianya akan menentusahkan keberkesanan prosedur yang dibangunkan dengan melihat dapatan hasil eksperimen memenuhi objektif sesuatu aktiviti yang dijalankan. Berikut adalah perjalanan eksperimen bagi ketiga- tiga pengguna yang telah dilaksanakan menggunakan prosedur yang telah dibangunkan.

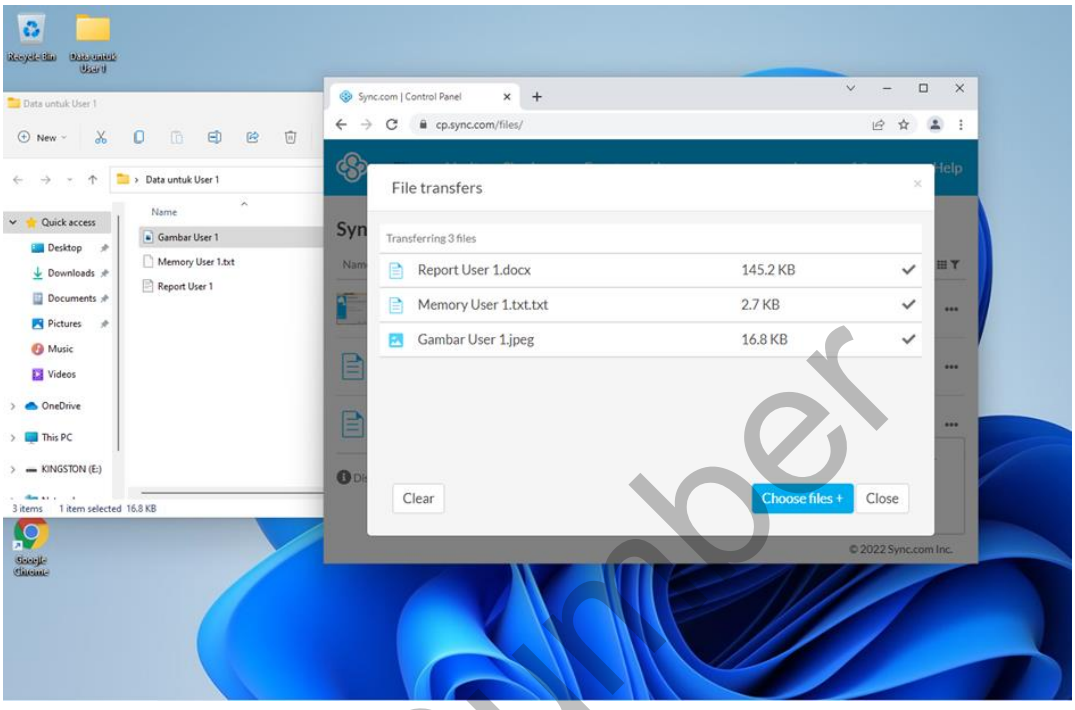
Pengguna 1

Pengguna 1 akan menggunakan data alamat emel "sarjana.user1@gmail.com" dan kata laluan "Sarjana@1234" untuk log masuk ke laman sesawang perkhidmatan awan yang disediakan oleh sync.com seperti di dalam Rajah 3.9 melalui pelayar Google Chrome.



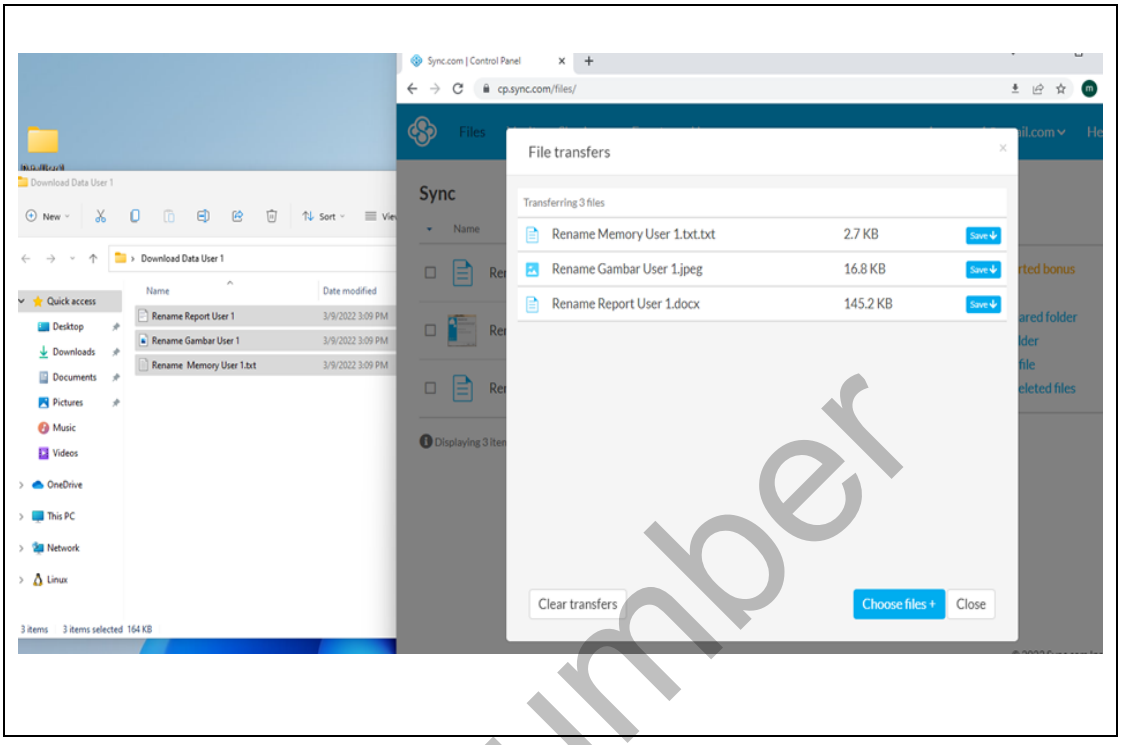
Rajah 3.9 Pengguna 1 log masuk ke sync.com

Setelah berjaya log masuk ke dalam laman sesawang sync.com, Pengguna 1 akan memuat naik tiga jenis fail (seperti dalam jadual 3.3) yang telah disediakan untuk tujuan eksperimen kajian seperti rajah 3.10.



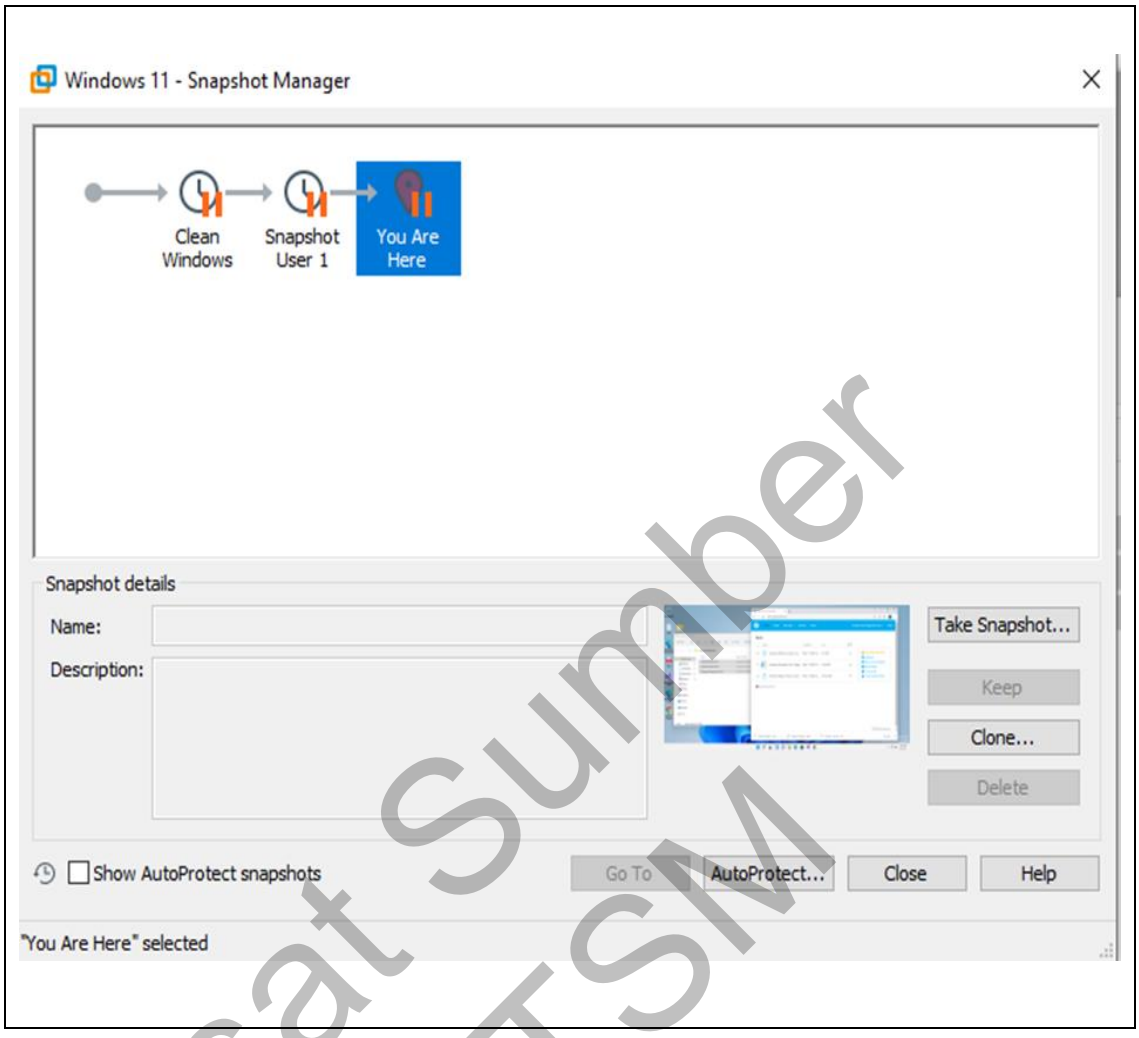
Rajah 3.10 Pengguna 1 berjaya memuat naik 3 jenis fail ke storan awan yang disediakan oleh sync.com

Rajah 3.10 juga menunjukkan Pengguna 1 telah berjaya memuat naik ketiga-tiga fail ke dalam storan yang disediakan oleh penyedia perkhidmatan dan juga saiz setiap fail tersebut. Rajah 3.11 pula menunjukkan Pengguna 1 telah menukar nama ketiga – tiga fail yang telah dimuat naik dengan nama “Rename Report User .docx”, “Rename memory User 1.txt” dan “Rename Gambar User 1.jpeg”. Pengguna 1 seterusnya akan memuat turun ketiga – tiga fail yang telah ditukar nama ke “*Folder Download Data User 1*” seperti yang ditunjukkan di dalam rajah 3.11 tersebut.



Rajah 3.11 Pengguna 1 berjaya memuat turun 3 jenis fail ke komputer

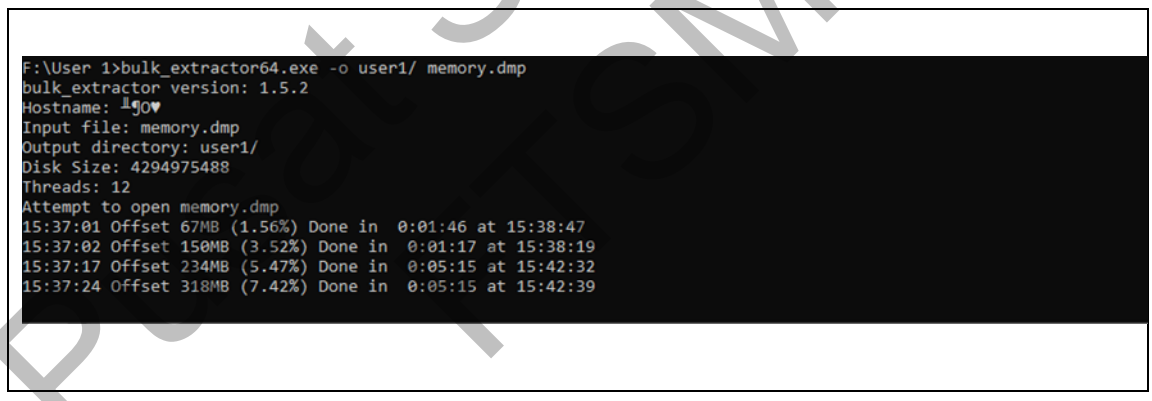
Pengguna 1 seterusnya log keluar dari laman sesawang sync.com. Kemudian langkah seterusnya adalah membuat arahan *suspend* bagi mesin maya tersebut. Arahan ini dilaksanakan bagi menghentikan segala proses atau sambungan yang mungkin berlaku oleh mesin maya tersebut. Setelah arahan *suspend* ini berjaya dilaksanakan, Satu *snapshot* telah dilakukan seperti di rajah 3.12 bagi merakam aktiviti–aktiviti dan sambungan yang telah dilakukan oleh mesin maya tersebut semasa proses memuat naik dan memuat turun fail-fail tersebut ke atau dari laman sesawang sync.com melalui pelayar internet Google Chrome.



Rajah 3.12 Arahan *snapshot* dilaksanakan bagi menghentikan segala proses dan sambungan oleh mesin maya

Setelah arahan *snapshot* ini berjaya dilaksanakan, proses eksperimen kajian ini akan diteruskan dengan menyalin fail *snapshot* yang dihasilkan iaitu fail **.vmsn* dan fail **.vmem* ke dalam sebuah *folder User 1* bagi proses menjana fail *memory dump* bertajuk *dump.dmp*. Rajah 3.13 menunjukkan perisian vmss2core-sb-8456865 digunakan untuk menjana fail *memory dump* yang diperlukan untuk proses menjana fail PCAP. Rajah 3.14 menunjukkan perisian bulk_extractor64 digunakan untuk menjana fail PCAP. Fail PCAP yang dijana akan digunakan di dalam proses analisa menggunakan perisian analisa rangkaian iaitu Wireshark untuk menentusahkan prosedur penjejakan paket yang dibangunkan berjaya mengesan sama ada terdapat sambungan dari mesin maya kepada laman sesawang penyedia perkhidmatan awan sync.com.

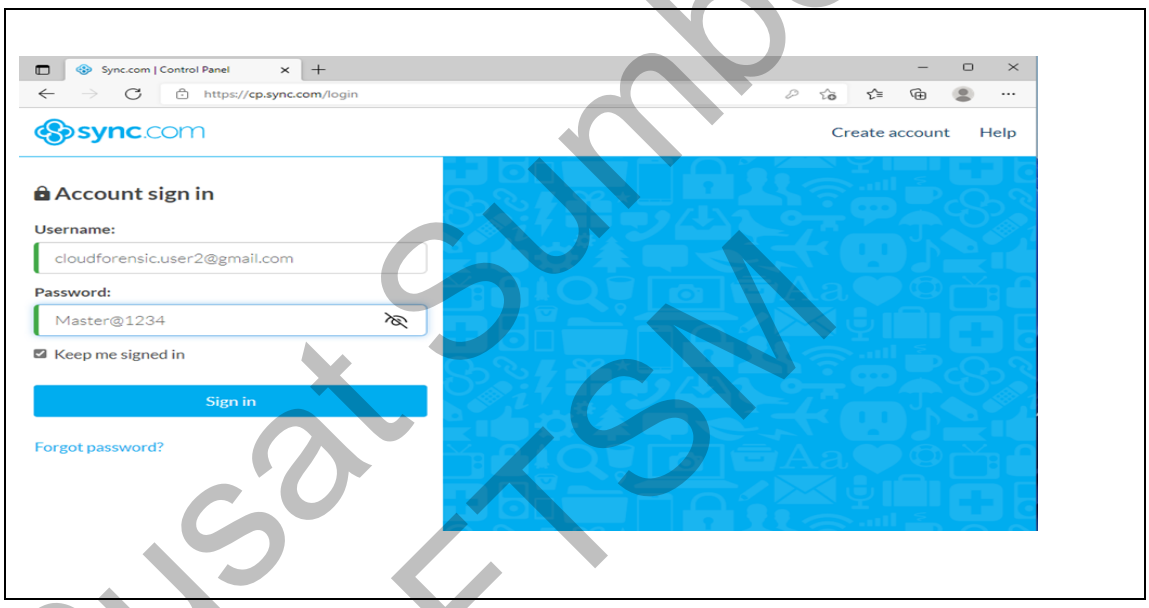
Rajah 3.13 Penggunaan perisian vmss2core-sb-8456865 untuk menjana fail *memory dump* "*memory.dmp*"



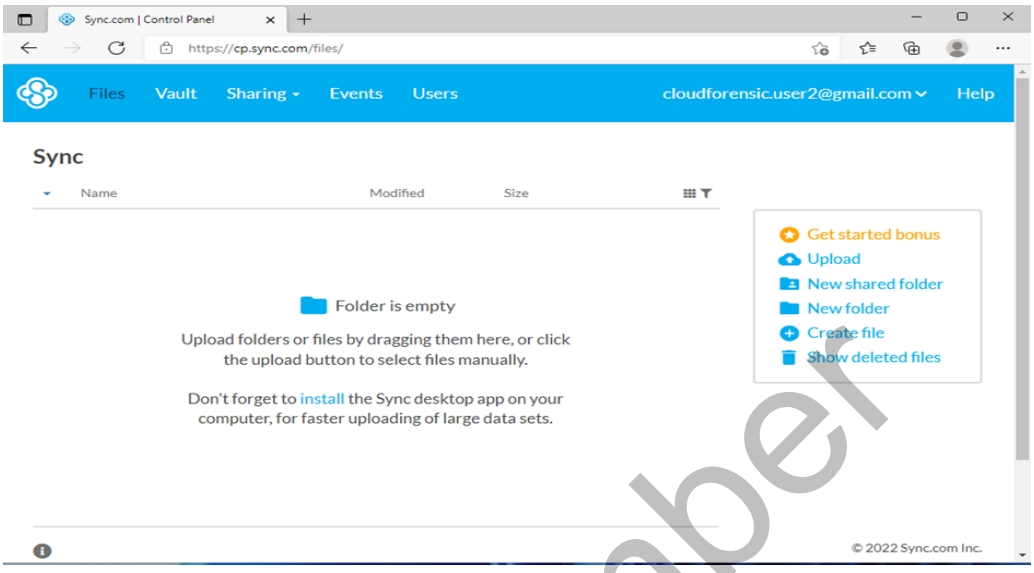
Rajah 3.14 Penggunaan perisian bulk_extractor64 untuk menjana fail pcap

Pengguna 2

Pengguna 2 akan menggunakan data alamat emel “cloudforensic.user2@gmail.com” dan kata laluan “Master@1234” untuk log masuk ke laman sesawang perkhidmatan awan yang disediakan oleh sync.com seperti yang ditunjukkan dalam rajah 3.15 melalui pelayar Internet Google Chrome. Rajah 3.16 pula menunjukkan laman utama sync.com setelah proses log masuk berjaya dilakukan dan menu perkhidmatan yang disediakan di halaman utama tersebut. Rajah 3.16 juga menunjukkan tiada fail yang terdapat di dalam storan awan Pengguna 2 pada masa tersebut.

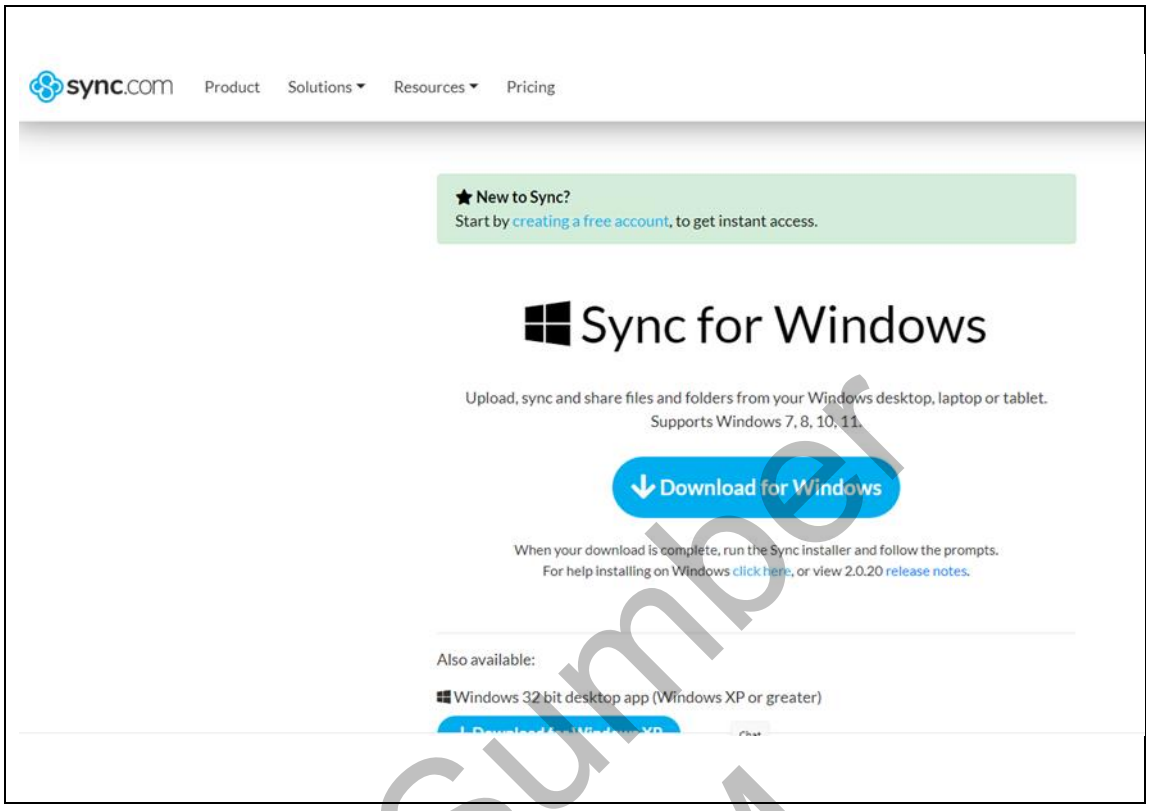


Rajah 3.15 Pengguna 2 Log Masuk Ke sync.com



Rajah 3.16 Pengguna 2 Berjaya Log Masuk Ke sync.com

Rajah 3.17 menunjukkan halaman untuk Pengguna 2 memuat turun aplikasi pelangan bagi sync.com. Aplikasi pelanggan yang telah siap dipasang ini akan digunakan untuk memuat naik tiga jenis fail yang telah disediakan untuk tujuan eksperimen kajian melalui perisian pelangan. Rajah 3.18 menunjukkan Pengguna 2 diminta untuk memasukkan semula ID log masuk dan kata laluan bagi membuat sambungan ke sync.com melalui aplikasi pelanggan.

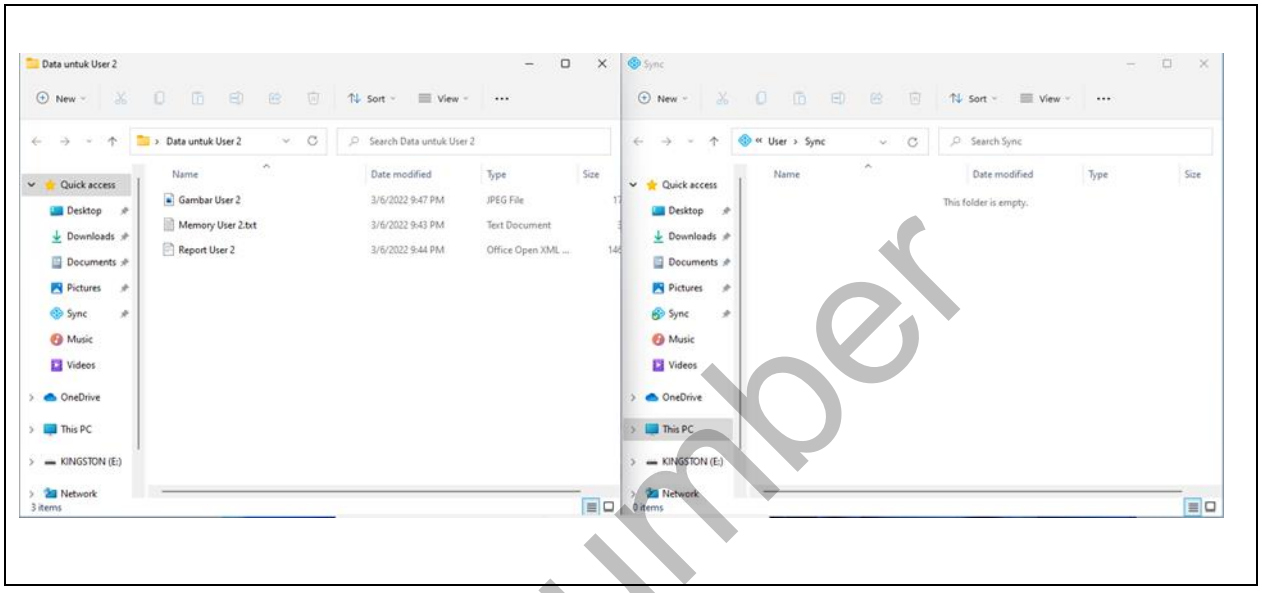


Rajah 3.17 Pengguna 2 memuat turun aplikasi pelanggan dari sync.com

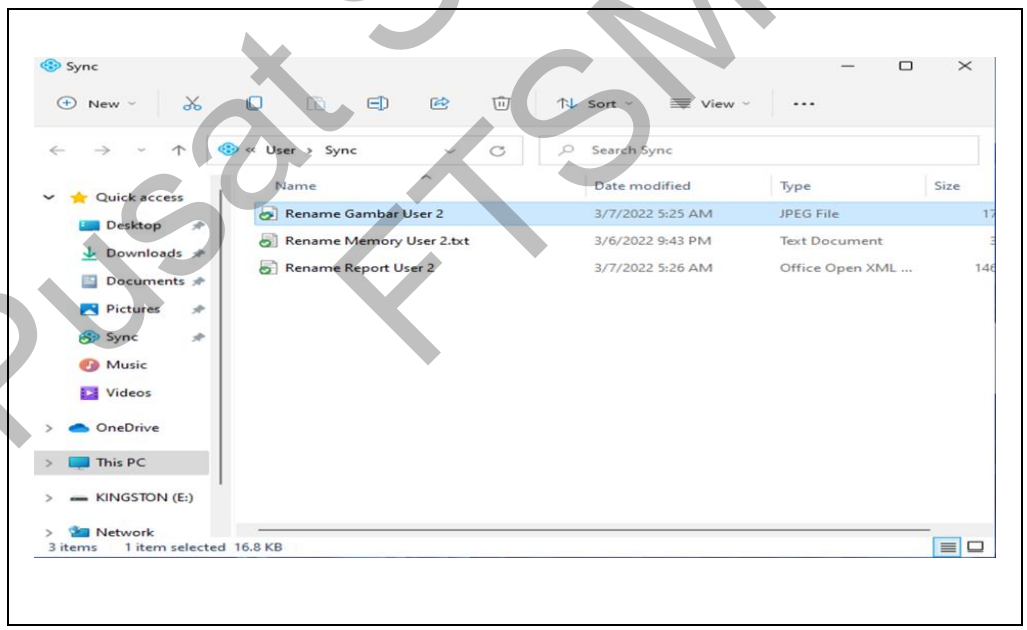
Rajah 3.18 Pengguna 2 melakukan konfigurasi aplikasi pelanggan dari sync.com

Rajah 3.19 menunjukkan Pengguna 2 melakukan proses muat naik 3 jenis fail ke storan awan menggunakan aplikasi pelanggan. Rajah 3.20 pula menunjukkan Pengguna 2 menukar nama ketiga–tiga fail yang telah dimuat naik dengan nama "Rename Report User 2 .docx", "Rename memory User 2.txt" dan "Rename Gambar

User 2.jpeg". Pengguna 2 seterusnya akan memuat turun ketiga – tiga fail yang telah ditukar nama ke "*Folder Download Data User 2*" melalui aplikasi pelanggan.



Rajah 3.19 Pengguna 2 akan melakukan proses muat naik melalui aplikasi pelanggan dari sync.com



Rajah 3.20 Proses penukaran nama fail oleh pengguna 2 melalui aplikasi pelanggan dari sync.com berjaya

Pengguna 2 menutup aplikasi pelanggan tersebut. Kemudian Langkah seterusnya adalah membuat arahan *suspend* bagi mesin maya tersebut. Arahan ini dilaksanakan bagi menghentikan segala proses atau sambungan yang mungkin berlaku oleh mesin tersebut. Setelah arahan *suspend* ini berjaya dilaksanakan, Satu *snapshot*