ANALISIS LALU LINTAS DATA PENGGUNA CLOUD STORAGE PADA iOS 7

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat Memperoleh Gelar Sarjana

Teknik Informatika



Nama : Cahyo Amali

NIM : 10523400

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ISLAM INDONESIA

2014

ANALISIS LALU LINTAS DATA PENGGUNA CLOUD STORAGE PADA iOS 7

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat Memperoleh Gelar Sarjana

Teknik Informatika

Nama : Cahyo Amali

NIM : 10523400

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ISLAM INDONESIA

2014

LEMBAR PENGESAHAN PEMBIMBING

ANALISIS LALU LINTAS DATA PENGGUNA CLOUD STORAGE PADA iOS 7

TUGAS AKHIR

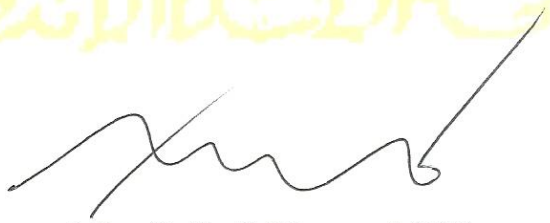
OLEH :

Nama : Cahyo Amali

NIM : 10523400

Yogyakarta, 18 Agustus 2014

Pembimbing



Ahmad Luthfi, S.Kom., M.Kom.

LEMBAR PENGESAHAN PENGUJI

ANALISIS LALU LINTAS DATA PENGGUNA CLOUD STORAGE PADA iOS 7

TUGAS AKHIR

OLEH :

Nama : Cahyo Amali

No. Mahasiswa : 10523400

Telah Dipertahankan di Depan Sidang Penguji sebagai Salah Satu Syarat untuk Memperoleh Gelar Sarjana Jurusan Teknik Informatika Fakultas Teknologi Industri Universitas Islam Indonesia

Yogyakarta, 18 Agustus 2014

Tim Penguji,

Ahmad Luthfi, S.Kom., M.Kom. _____

Ketua

Taufiq Hidayat, S.T., M.Cs. _____

Anggota I

Arwan Ahmad Khoirudin, S.Kom., M.Cs. _____

Anggota II

Mengetahui,

Ketua Jurusan Teknik Informatika

Universitas Islam Indonesia

Hendrik, S.T., M.Eng.

LEMBAR PERNYATAAN KEASLIAN

HASIL TUGAS AKHIR

Saya yang bertanda tangan di bawah ini,

Nama : Cahyo Amali
NIM : 10523400
Jurusan : Teknik Informatika

Menyatakan bahwa seluruh komponen dan isi dalam Laporan Tugas Akhir ini adalah hasil karya saya sendiri.Apabila dikemudian hari terbukti bahwa ada beberapa bagian dari karya ini adalah bukan hasil karya saya sendiri, maka saya siap menanggung resiko dan konsekuensi apapun.

Demikian pernyataan ini saya buat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 18 Agustus 2014

(Cahyo Amali)

HALAMAN PERSEMBAHAN

Tugas akhir ini saya persembahkan kepada……

"Allah SWT, Nabi Muhammad SAW

Kedua Orang tua saya yang tercinta,

Adik saya, pacar saya serta keluarga, sahabat, dan teman-teman"

HALAMAN MOTTO

"Bertakwalah pada Allah maka Allah akan mengajarimu. Sesungguhnya Allah Maha Mengetahui segala sesuatu."(Q.S.Al-Baqarah :282)

"Barangsiapa bertawakkal pada Allah, maka Allah akan memberikan kecukupan padanya, sesungguhnya Allah lah yang akan melaksanakan urusan (yang dikehendaki)-Nya." (QS. Ath-Thalaq: 3).

"Intelligence is not the determinant of success, but hard work is the real determinant of your success."

"The more grateful, the more happiness we get."

"Think big, and act now"

KATA PENGANTAR



Assalamu'alaikum Wr. Wb.

Puji syukur kehadirat Allah SWT yang telah melimpahkan rahmat dan hidayah-Nya sehingga kami dapat menyelesaikan laporan Tugas Akhir ini dengan pembuatan aplikasi yang berjudul "Analisis Lalu Lintas Data Pada Cloud Storage iOS 7". Penyusunan Laporan Tugas Akhir ini merupakan salah satu syarat untuk memperoleh gelar sarjana di jurusan Teknik Informatika Universitas Islam Indonesia.

Dengan menguraikan hal tersebut penulis banyak mengalami kesulitan pada proses penelitian. Namun, berkat bantuan, bimbingan, serta pengarahan dari pembimbung, penulis berhasil menyelesaikan skripsi ini. Oleh karena itu, pada kesempatan ini dengan kerendahan hati penulis mengucapkan terima kasih yang setulus-tulus kepada:

1. Allah SWT yang telah senantiasa memberikan rahmat serta hidayah-Nya.
2. Nabi Muhammad SAW yang telah memberikan panutan hidup.
3. Kepada kedua orang tuaku tercinta, yang selalu memberikan dukungan, berupa moral maupun materil, serta doanya selama ini
4. Kepada dosen pembimbing bapak Ahmad Luthfi, S.Kom, M.Kom, yang telah banyak memberikan bantuan, bimbingan, dan arahan dalam penyelesaian tugas akhir ini.
5. Adikku yang aku sayangi, dan segenap saudara yang telah banyak memberikan bantuan serta dukungan untuk penulis dapat menyelesaikan kuliah selama ini.
6. Nidya Putri Lestyanti S.E, yang sudah banyak memberikan bantuan, semangat, do'a, dan dorongan agar tugas akhir, serta kuliahku dapat segera terselesaikan dengan baik.

7. Aza, Abu, Ami, Ikhsan. Teman seperjuangan Skripsi yang sudah sangat banyak membantu dalam penulis melakukan percobaan, serta dalam menyelesaikan Tugas Akhir ini.
8. Teman-teman FTI UII yang tidak bisa saya sebutkan namanya satu per satu, terima kasih untuk persaudaraan selama ini. Teman-teman KKN Antar Waktu 2013-2014 Unit 72 (Lia,Virgin,Yudha,Aan,Arif,dan Tiwi) terimakasih atas motivasi, persaudaraan dan kenangan selama KKN!Saudaraku di kontrakan 117(Arista,Lukas,Fito,Denny,Adi,Dies,Mas Dwi,Mas Kelik,Mas Andhes) Terima kasih atas persaudaraan dan motivasinya selama ini
9. Serta ucapan terima kasih yang sebesar-besarnya kepada semua pihak yang tidak bisa penulis sebutkan namanya satu-persatu.

Penulis menyadari bahwa laporan ini masih belum sempurna karena keterbatasan kemampuan dan pengalaman penulis. Oleh karena itu, kritik dan saran sangat penulis harapkan sebagai bahan evaluasi dan pembelajaran agar penulis dapat menjadi lebih baik lagi di kemudian hari. Semoga laporan ini dapat bermanfaat bagi semua pihak yang membutuhkan.

Wassalamu'alaikum Wr Wb.

Yogyakarta, 18 Agustus 2014

Cahyo Amali

TAKARIR

Username	Serangkaian huruf yang merupakan tanda pengenal untuk masuk dan mengakses internet
Password	Kata rahasia yang digunakan sebagai pengenal
Public key	Kunci Publik
Upload	Unggah
Install	Pasang
Download	Unduh
Cloud Storage	Tempat/media penyimpanan Online
Apple device	Perangkat Apple
Dedicated server	Layanan hosting dengan menggunakan server secara keseluruhan tanpa dibagi dengan pengguna lain
Direct link	Alamat yang merujuk pada suatu lokasi file dalam suatu server
Access point	Perangkat komunikasi nirkabel yang memungkinkan antar perangkat untuk terhubung ke jaringan nirkabel dengan menggunakan wifi, Bloethooth, atau standar terkait
Command prompt	Baris perintah pada sebuah Sistem Operasi berbasis Antarmuka Pengguna untuk mengeksekusi sebuah file dengan cara menuliskan perintahnya
Hosted Network	fitur yang dapat membuat virtualisasi perangkat fisik nirkabel menjadi lebih dari satu, atau biasa disebut virtual wifi, bisa juga sebagai perangkat lunak akses point

ABSTRAK

Kecanggihan teknologi yang semakin berkembang sekarang ini menyebabkan perubahan yang pesat. Media penyimpanan adalah salah satunnya yang berkembang cukup pesat saat ini. Hadirnya berbagai macam bentuk media penyimpanan membuat orang dipermudah dalam menyimpan datanya sesuai kebutuhan masing-masing. *Cloud Storage* adalah salah satunya yang muncul sebagai media penyimpanan online alternatif menggantikan media disk, ataupun media flash. Salah satu *smarthphone* yang menggunakan *Cloud Storage* adalah iPhone dan iPod. Banyak ragam Aplikasi *Cloud storage* yang ditawarkan oleh iOS guna memberi kemudahan penggunanya melalui *Apple device* yang dimiliki. Melalui penelitian ini diharapkan dapat mengetahui seberapa jauh fitur keamanan yang ditawarkan oleh pihak pengembang aplikasi dari masing-masing *Cloud Storage* yang diujikan. Pada Penelitian ini dilakukan proses *capture data* dengan menggunakan Aplikasi dari *Network Analyzer* guna membantu mempermudah dalam membaca paket data yang ditangkap. Hasil yang didapatkan kemudian ditelaah dan diteliti lebih lanjut mengenai informasi-informasi yang berhasil didapatkan selama *capture data* berlangsung.

Dari temuan yang ada, kemudian akan dilakukan pembahasan secara mendasar, melihat dari aspek keamanan lalu lintas data saat data ditransmisikan. Sehingga nantinya penelitian ini dapat menjadi acuan penelitian selanjutnya ataupun acuan dalam kegiatan forensic digital yang berkaitan dengan aplikasi Cloud Storage pada sistem operasi iOS. Pada hasil akhir dari proses percobaan yang dilakukan didapatkan hasil berupa informasi file-file sertifikat yang digunakan untuk mengamankan proses pengunggahan dan pengunduhan file yang dilakukan. Selain itu didapatkan informasi lainnya berupa jenis koneksi yang digunakan untuk melakukan pengiriman data dari client menuju server dan juga sebaliknya, kemudian didapatkan juga informasi mengenai metode enkripsi yang digunakan pada masing-masing aplikasi Cloud Storage yang digunkan pada proses percobaan ini.

Kata kunci : Media Penyimpanan, *Smartphone, Network Analyzer, Lalu Lintas Data, Capture data***, iOS**

DAFTAR ISI

LEMBAR PENGESAHAN PEMBIMBING iii
LEMBAR PENGESAHAN PENGUJI iv
LEMBAR PERNYATAAN KEASLIAN v
HALAMAN PERSEMBAHAN vi
HALAMAN MOTTO vii
KATA PENGANTAR viii
TAKARIR x
ABSTRAK xi
DAFTAR ISI xii
DAFTAR GAMBAR xv
DAFTAR TABEL xvii
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 2
1.3 Batasan Masalah 2
1.4 Tujuan Penelitian 2
1.5 Manfaat Penelitian 3
1.6 Metode Penelitian 3
1.6.1 Studi Literatur 3
1.6.2 Pengumpulan Data 3
1.6.3 Analisis Data 3
1.7 Sistematika Penulisan 4
BAB II LANDASAN TEORI 5
2.1 Lalu Lintas Data 5
2.2 Keamanan Data 6
2.2.1 Data dan informasi 6
2.2.2 Keamanan data dan informasi 6
2.3 Kriptologi 7
2.1 Enkripsi 8

2.2 Dekripsi 9
2.4 Cloud Storage 9
2.5 Cloud Storage pada iOS 7 11
2.5.1 iCloud 11
2.5.2 Google drive 12
2.5.3 Dropbox 13
2.5.4 Box 14
2.5.5 Skydrive(Onedrive) 15
2.6 Skema Enkripsi Cloud Storage 16
BAB III METODOLOGI PENELITIAN 18
3.1 Diagram alur Penelitian 18
3.2 Studi Pustaka 18
3.3 Pengumpulan data 19
3.3.1 Topologi 19
3.4 Pengolahan Data 20
3.5 Analisis Hasil Pengolahan Data 20
3.5.1 Perancangan Tabel Analisis Aplikasi Cloud Storage pada iOS 7 21
3.6 Kebutuhan Perangkat Keras 22
3.7 Kebutuhan Perangkat Lunak 22
3.8 Flowchart 24
3.9 Hasil yang Dikehendaki 24
BAB IV HASIL DAN PEMBAHASAN 26
4.1 Proses Penangkapan Lalu Lintas Data 26
4.2 Aplikasi Cloud storage yang diuji 27
4.2.1 iCloud 27
4.2.2 Google drive 29
4.2.3 Dropbox 31
4.2.4 Box 32
4.2.5 Skydrive(Onedrive) 34
4.3 Analisis Hasil Lalu Lintas Data 36
4.3.1 iCloud 37
4.3.2 Google drive 39
4.3.3 Dropbox 42

4.3.4 Box 45
4.3.1 Skydrive(Onedrive) 48
4.4 Hasil Akhir 51
4.4.1 Metode Pengamanan 51
4.4.2 Informasi yang didapatkan 52
BAB V KESIMPULAN DAN SARAN 53
5.1 Kesimpulan 53
5.1 Saran 53
DAFTAR PUSTAKA 55
LAMPIRAN 56

DAFTAR GAMBAR

Gambar 2. 1 Ilustrasi Lalu Lintas Data Cloud Storage pada iOS 7 5
Gambar 2. 2 Cloud Storage pada iOS 7 10
Gambar 2. 3 iCloud 12
Gambar 2. 4 Google drive 13
Gambar 2. 5 Dropbox 14
Gambar 2. 6 Box 15
Gambar 2. 7 Skydrive(Onedrive) 16
Gambar 3. 1 Diagram Alur Metodologi Penelitian 18
Gambar 3. 2 Topologi 20
Gambar 3. 3 Flowchart Penelitian 24
Gambar 4. 1 Tampilan Aplikasi iCloud 28
Gambar 4. 2 Tampilan Aplikasi Google drive 30
Gambar 4. 3 Tampilan Aplikasi Dropbox 31
Gambar 4. 4 Tampilan Aplikasi Box 34
Gambar 4. 5 Tampilan Aplikasi Skyderive (Onedrive) 35
Gambar 4. 6 Tampilan pada tab files dari paket iCloud 37
Gambar 4. 7 Tampilan salah satu sertifikat dari iCloud 38
Gambar 4. 8 Screenshot dari paket handshake iCloud 38
Gambar 4. 9 Tampilan pada tab files dari paket Google drive 40
Gambar 4. 10 Tampilan salah satu sertifikat dari Google drive 40
Gambar 4. 11 Screenshot dari paket handshake Google drive 41
Gambar 4. 12 Tampilan pada tab files dari paket Dropbox 42
Gambar 4. 13 Tampilan salah satu sertifikat dari Dropbox 43
Gambar 4. 14 Screenshot dari paket handshake Dropbox 44

Gambar 4. 15 Tampilan pada tab files dari paket Box..... 45

Gambar 4. 16 Tampilan salah satu sertifikat dari Box..... 46

Gambar 4. 17 Screenshot dari paket handshake Box..... 46

Gambar 4. 18 Tampilan pada tab files dari paket Skydrive (Onedrive) 48

Gambar 4. 19 Tampilan salah satu sertifikat dari Skydrive (Onedrive) 49

Gambar 4. 20 Screenshot dari paket handshake Skydrive (Onedrive)..... 49

DAFTAR TABEL

Tabel 2. 1 Komponen untuk menjamin kerahasiaan dalam telekomunikasi..... 7

Tabel 3. 1 Hasil upload file aplikasi cloud storage pada iOS 7 21

Tabel 3. 2 Hasil download file aplikasi cloud storage pada iOS 7 22

Tabel 4. 1 Checklist iCloud dengan Wireshark 39

Tabel 4. 2 Checklist iCloud pada Network Miner 39

Tabel 4. 3 Checklist Google drive pada Wireshark 41

Tabel 4. 4 Checklist Google drive pada Network Miner 41

Tabel 4. 5 Checklist Dropbox pada Wireshark 44

Tabel 4. 6 Checklist Dropbox pada Network Miner 44

Tabel 4. 7 Checklist Box pada Wireshark..... 47

Tabel 4. 8 Checklist Box pada Network Miner..... 47

Tabel 4. 9 Checklist Skydrive (Onedrive) pada Wireshark 50

Tabel 4. 10 Checklist Skydrive (Onedrive) pada Network Miner 50

Tabel 4. 11 Tabel Perbandingan Seluruh Aplikasi Cloud storage 51

BAB I
PENDAHULUAN

1.1 Latar Belakang

Cloud Storage adalah tempat/media penyimpanan online. *Cloud Storage* muncul sebagai media penyimpanan alternatif menggantikan media disk, ataupun media *flash*. *Media cloud storage* dinilai lebih praktis, karena tidak memerlukan alat tambahan untuk digunakan sebagai media penyimpanan. *Cloud storage* pada saat ini telah masuk ke dalam dunia *smarthphone*. Salah satu *smarthphone* yang menggunakan *Cloud Storage* adalah iPhone.

iPhone adalah smarthphone buatan Apple yang cukup terkenal saat ini. iPhone menggunakan sistem operasi iOS 7. Di dalam Sistem Operasi tersebut memiliki banyak Aplikasi *Cloud Storage* yang dapat membantu penggunanya dalam menyimpan data yang dimiliki. Dengan adanya hal tersebut pembuat aplikasi telah memikirkan dalam segi keamanan data yang dimiliki si pengguna. Akan tetapi tingkat keamanan sebuah aplikasi pastinya berbeda-beda antara aplikasi *Cloud Storage* satu dengan lainnya.

Keamanan data merupakan salah satu aspek yang menjadi acuan dalam pengembangan sebuah aplikasi. Fitur-fitur keamanan dan juga privasi banyak disediakan oleh pengembang aplikasi. Akan tetapi bagi masyarakat awam, fitur keamanan yang disediakan oleh sebuah aplikasi belum menjadi perhatian utama. Kebanyakan pengguna aplikasi *Cloud Storage* hanya memikirkan bahwa data mereka tersimpan dengan aman.

Sebagai contoh, *Cloud Storage* digunakan oleh para penjahat *cyber* untuk menyimpan dan mendistribusikan data. *Cloud Storage* menawarkan kemampuan untuk menghindari pengawasan penegakan hukum dan badan-badan keamanan nasional bagi pelaku kejahatan guna melakukan kejahatan, dan untuk mengatasi kesulitan dalam menghubungkan kepemilikan atau hubungan dengan data terlarang (Biggs & Vidalis 2009). *Cloud Storage* juga dapat dijadikan sasaran serangan oleh penjahat cyber, yang mungkin dapat dibajak dan menggunakan sumber daya yang didapat untuk tujuan kriminal, sehingga menambah

pertumbuhan volume bukti digital dalam kasus-kasus yang sedang diselidiki (Quick, Martini, & Choo, 2013).

Dengan adanya tingkat keamanan yang berbeda-beda pada tiap aplikasi *Cloud Storage* maka perlu dilakukan pengamatan lalu lintas data pada aplikasi *Cloud Storage* yang diuji agar dapat diketahui tingkat keamanan dari lalu lintas data yang lewat. Pengamatan lalu lintas data dilakukan dengan menggunakan Wireshark, sedangkan untuk membantu dalam menganalisa hasil tangkapan dari aplikasi Wireshark dengan menggunakan aplikasi Network Miner. Selain adanya perbedaan dari tiap aplikasi cloud storage tersebut, pemilihan iOS 7 sebagai sasaran penelitian ini dikarenakan banyaknya pengguna peranggkat Apple ini beralih pada sistem operasi yang baru diluncurkan ini, selain itu penulis ingin mengetahui sejauh mana tingkat keamanan yang diberikan oleh Apple pada sistem operasi yang diluncurkan ini.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, maka dapat dilihat permasalahan pada penelitian ini adalah:

1. Informasi apa saja yang didapatkan ketika proses capture data berlangsung saat aplikasi Cloud Storage berjalan?
2. Metode pengamanan apa saja yang digunakan pada setiap aplikasi Cloud Storage?

1.3 Batasan Masalah

Ada pun beberapa batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Aplikasi yang dianalisis adalah aplikasi yang tersedia di *App Store*.
2. Aplikasi yang digunakan dalam penangkapan data yaitu Wireshark dan Network Miner.
3. Aplikasi yang menjadi acuan untuk dianalisis:
    a) Icloud
    b) Dropbox
    c) Google Drive
    d) Sky Drive/Onedrive dan Box

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk mengetahui keamanan yang diberikan oleh *Cloud Storage* berbasis iOS 7 pada saat proses data ditransmisikan.

1.5 Manfaat Penelitian

Dengan mengadakan penelitian ini, manfaat yang ingin didapatkan adalah:

1. Mengetahui keamanan lalu lintas data pada *Cloud storage* di IOS 7.
2. Mengetahui *file* apa saja yang didapat ketika proses lalu lintas data berlangsung.
3. Dengan diperolehnya hasil analisis, diharapkan dapat menambah kesadaran keamanan para pengguna *Cloud storage* berbasis sistem operasi IOS 7 .

1.6 Metode Penelitian

Metode penelitian yang akan digunakan dalam menyusun tugas akhir ini meliputi beberapa tahap-tahapan sebagai berikut:

1.6.1 Studi Literatur

Studi literatur digunakan untuk menggali informasi yang terkati dengan penelitian, yaitu melalui media buku, maupun internet. Hal ini dilakukan untuk mengumpulkan teori – teori yang menjadi landasan dalam pelaksanaan terkait penelitian, dan teori – teori pendukung yang dapat memberikan kesinambungan antara teori dan praktek..

1.6.2 Pengumpulan Data

Pengumpulan data dilakukan dengan melakukan percobaan langsung pada aplikasi *Cloud Storage* yang terdapat pada Sistem Operasi iOS 7. Percobaan dilakukan dengan menangkap lalu lintas atau paket data yang lewat dari aplikasi *Cloud Storage* menggunakan aplikasi *Wireshark*.

1.6.3 Analisis Data

Analisis data dilakukan dengan membaca hasil tangkapan yang telah ditangkap oleh aplikasi *Wireshark* menggunakan *Network Miner*. Kemudian menelaah metode-metode pengamanan yang dilakukan berdasarkan hasil tangkapan yang didapat.

1.7 Sistematika Penulisan

BAB I Pendahuluan

Membahas tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, sistematika penulisan, serta metode penelitian yang akan dilakukan.

BAB II Landasan Teori

Berisi dasar - dasar teori yang dijadikan panduan, pedoman, landasan dalam penelitian analisis lalu lintas data pada *Cloud Storage* di sistem operasi IOS 7 .

BAB III Metodologi

Membahas mengenai gambaran umum tentang penelitian, analisis kebutuhan perangkat keras maupun lunak dalam ujicoba yang dilakukan selama penelitian berlangsung.

BAB IV Hasil dan Pembahasan

Berisi data – data dokumentasi berlangsungya percobaan mulai dari tahap proses penangkapan data sampai dengan metode pengamanan yang dipakai dan informasi yang didapat, serta hasil akhir dari analisis tersebut.

BAB V Penutup

Menyajikan kesimpulan dari seluruh proses yang telah diujicoba, hasil analisis, saran – saran yang perlu dikaji, berdasarkan jalannya ujicoba, dan kelebihan maupun keterbatasan yang ditemukan selama proses ujicoba berlangsung.

BAB II
LANDASAN TEORI

2.1 Lalu Lintas Data

Lalu lintas tidak hanya terdapat pada kehidupan manusia, namun lalu lintas juga terdapat pada proses pengiriman informasi pada jaringan komunikasi data dengan menggunakan internet. Lalu lintas pada dunia nyata dikatakan sebagai proses perpindahan atau gerak pada suatu benda dari tempat asal ke tempat tujuan. Bentuk perpindahan ini dapat digambarkan dengan ilustrasi misalnya saja, mobil A melaju dari titik O menuju titik P untuk mencapai tujuannya dititik B. Adanya lalu lintas ini dimaksudkan agar ketika terjadi pergerakan dari satu tempat ke tempat lain, pergerakkan tersebut dapat dipantau sehingga apabila terjadi kecelakaan atau hal-hal yang tidak diinginkan dapat segera ditangani.

Pada dunia komunikasi lalu lintas data dapat digambarkan seperti sebuah proses dimana terjadinya perpindahan data, dari pengirim kepada penerima menggunakan perangkat elektronik sebagai perantaranya, sehingga data tersebut dapat diterima oleh penerima ataupun sebaliknya. Dalam proses pengiriman ini juga akan diawasi dengan seksama apabila terjadi kesalahan pada proses pengiriman data atau ketika proses pengiriman tidak berjalan dengan lancer.



Gambar 2. 1 Ilustrasi Lalu Lintas Data Cloud Storage pada iOS 7

Sumber : http://tex.org/wp-content/uploads/2014/03/apple-icloud.jpg

Terlihat pada gambar 2.1 pada proses lalu lintas data yang berlangsung dari perangkat penguji ke aplikasi *Cloud Storage* dan sebaliknya dari aplikasi *Cloud Storage* ke perangkat penguji, kemudian pada saat proses *upload* dan *download* berlangsung lalu lintas data akan diamati melalui wireshark.

2.2 Keamanan Data

2.2.1 Data dan informasi

Menurut (Zulkifli Amsyah, 2005) Data adalah fakta yang sudah ditulis dalam bentuk catatan atau direkam ke dalam berbagai bentuk media (contohnya komputer) sedangkan Informasi adalah data yang sudah diolah, dibentuk, ataupun dimanipulasi sesuai dengan keperluan tertentu.

Ada perbedaan antara data dan informasi. Data adalah fakta statistik dalam bentuk kumpulan simbol yang tidak mengartikan sesuatu. Informasi adalah data yang telah tersaring, terorganisir, terealisasi, dan saling berhubungan sehingga berguna untuk mencapai tujuan organisasi. John F Nash (1989). Sedangkan menurut Robert A, Leitch dan K. Roscoe Davis (1983) mendefinisikan data dan informasi secara berbeda. Data adalah fakta mentah, seperti rincian transaksi dari faktur penjualan. Sedangkan informasi pengetahuan dikomunikasikan dikembangkan dengan cara mencocokkan dan mengubah data sehingga output bentuk yang berguna bagi penerimanya.

2.2.2 Keamanan data dan informasi

Keamanan biasanya digambarkan sebagai kebebasan dari bahaya atau sebagai kondisi keselamatan. Keamanan komputer, secara rinci adalah perlindungan data di dalam suatu sistem melawan terhadap otorisasi tidak sah, modifikasi, atau perusakan dan perlindungan sistem komputer terhadap penggunaan tidak sah atau modifikasi (Harold F. Tipton, 2005).

Secara garis besarnya masalah keamanan dibagi menjadi 4 bagian yang saling berhubungan, yaitu: kerahasiaan, keaslian, pengakuan dan kontrol integritas. Kerahasiaan tentunya dimaksudkan agar data dijauhkan dari orang-orang yang tidak berkepentingan dengan hal yang dirahasiakan. Hal ini perlu diperhatikan ketika seseorang berbicara tentang jaringan komputer. Keaslian berhubungan dengan kepada siapa kita berbicara ketika ingin menyampaikan

pesan atau informasi yang sangat penting. Pengakuan berkaitan dengan adanya tanda tangan digital atau sertifikat digital.

Tujuan dari pengamanan data ini selain untuk meningkatkan keamanan data juga memiliki fungsi untuk menlindugi data agar tidak dapat dibaca oleh orang-orang yang tidak berhak dan mencegah agar orang-orang yang tidak berhak, menyisipkan atau menghapus data. (Kristanto, 2003:3). Menurut Kurniawan dkk (2009) secara umum, ada empat aspek utama yang harus diperhitungkan dalam keamanan data dan informasi, yaitu :

Tabel 2. 1 Komponen untuk menjamin kerahasiaan dalam telekomunikasi

Availability	berhubungan dengan ketersediaan sistem dan data (informasi) ketika dibutuhkan.
Integrity	usaha untuk menjaga data atau informasi tidak diubah oleh yang tidak berhak..
Authentication	usaha atau metoda untuk mengetahui keaslian dari informasi, misalnya apakah informasi yang dikirim dibuka oleh orang yang benar (asli) atau layanan dari server yang diberikan benar berasal dari server yang dimaksud.
Privacy/Confidentiality	yaitu usaha menjaga data informasi dari orang yang tidak berhak mengakses (memastikan bahwa data atau informasi pribadi kita tetap pribadi).

2.3 Kriptologi

Kriptologi adalah ilmu atau seni yang mempelajari semua aspek tulisan rahasia. Kriptologi dibagi menjadi 2 (dua) yaitu kriptografi dan kriptanalisis. Kriptografi adalah cara (sistem, metode) yang mengolah tata tulisan dalam berita sehingga menjadi tata tulisan yang berlainan dan tidak bermakna (incoherent). Sedangkan kriptanalisis adalah usaha mendapatkan teks terang dari suatu teks sandi yang tidak diketahui sistem serta kunci-kunci-nya.

Menurut buku “Pengantar Kriptologi” (Sumarkidjo, 1972), kata kriptologi mempunyai 2 (dua) pengertian :

1. Kriptologi sebagai ilmu, yang mempelajari semua aspek dalam tulisan rahasia. Ilmu persandian ini dibedakan menjadi 2 (dua) kelompok dasar :
   a. Sistem steganografi, meliputi sistem-sistem yang secara katawiyah menyembunyikan berita, seperti di dalam gumpalan lilin, dengan tanda-tanda tertentu, di dalam teks berita lain, "dihilangkan" dengan tinta rahasia dan lain sebagainya. Steganografi terbagi menjadi 3 jenis:

      Linguistis : Semagram, Open Code.

      Tehnologis : Secret (invisible) inks, Micro-photography.

      Concealments.
   b. Sistem kriptografik, meliputi sistem-sistem yang mengolah tata tulisan dalam berita sehingga menjadi tata tulisan yang berlainan dan tidak bermakna (incoherent). Sistem ini dibedakan menjadi 2 (dua) :

      Cipher : Transposisi dan Substitusi.

      Code : Placode (Plain Code) dan Encicode (Enciphered Code).
2. Kriptologi sebagai kegiatan, yang berkaitan dengan fungsinya di dalam kegiatan intelijen pada umumnya. Kegiatan intelijen pada umumnya terdiri dari kegiatan penyelidikan dan pengamanan. Kegiatan penyelidikan meliputi *Direction Finding* dan *Interception*, *Traffic Analysis* dan *Cryptanalysis*, sedangkan kegiatan pengamanan terhadap tindakan dari kegiatan penyelidikan tersebut adalah *Transmission Security*, *Traffic Security* dan *Crypt Security*.

2.1 Enkripsi

Enkripsi merupakan suatu teknik yang digunakan untuk mengubah kode yang awalnya dapat dimengerti kemudian menjadi kode yang tidak dapat dimengerti atau sulit dipahami. Enkripsi dapat diartikan sebagai kode atau *chipper*. Sebuah sistem pengkodean menggunakan suatu table atau kamus yang telah didefinisikan untuk mengganti kata dari informasi atau yang merupakan bagian dari infromasi yang dikirim. (Kristanto, 2003:24). Enkripsi ini sendiri memiliki maksud untuk melindungi informasi atau pesan agar tidak dapet dengan mudah dilihat oleh orang atau pihak yang tidak berkepentingan. Informasi atau

pesan ini misalnya saja dapat berupa sebuah *username, password* atau bahkan nomor rekening kartu kredit.

Enkripsi sendiri terbagi menjadi dua macam, yaitu :

a. Simetrik

Enkripsi ini menggunakan satu kunci untuk enkripsi dan dekripsinya. Contoh dari enkripsi simetrik adalah DES (Data Encryption Standard), AES (Advanced Encryption Standard), IDEA (International Data Encryption Algoritm) (Ariyus, 2008), RC4, OTP (On Time Pad).

b. Asimetrik

Enkripsi ini menggunakan kunci yang berbeda untuk enkripsi dan dekripsi. Enkripsi asimetrik tidak memerlukan key yang banyak, cukup dengan menggunakan *public key*. Contoh dari enkripsi asimetrik adalah RSA(Rivest, Shamir, Adlemana), DSA (Digital Signature Algorithm), DH (Diffle-Hellman), ECC Elliptic (Curve Cryptography).

2.2 Dekripsi

Dekripsi merupakan suatu cara yang digunakan untuk mengubah suatu informasi atau pesan rahasia yang tadinya tidak dapat dimengerti menjadi dapat dimengerti atau dibaca. Secara singkatnya dekripsi merupakan kebalikan dari enkripsi (Ariyus, 2008).

2.3 Aplikasi

Aplikasi merupakan sebuah pernagkat lunak yang diciptakan dengan maksud dan tujuan tertentu untuk dapat membantu sesorang didalam melakukan sebuah pekerjaan. Sebagai contoh dibuatnya aplikasi pengolah kata yang memiliki maksud untuk mempermudah pekerjaan manusia didalam mengolah pekerjaan berhubungan dengan pengolah kata.

Secara istilah Aplikasi adalah suatu subkelas perangkat lunak komputer yang menggunakan kemampuan komputer langsung untuk melakukan suatu tugas yang diinginkan pemakai. (ayapoe, 2013).

2.4 Cloud Storage

Cloud Storage adalah layanan penting komputasi awan, yang memungkinkan pemilik data (pemilik) untuk memindahkan data dari sistem

komputasi lokal mereka ke awan. *Cloud Storage* adalah model penyimpanan online jaringan, dimana data disimpan pada kotak virtualisasi penyimpanan yang umumnya diselenggarakan oleh pihak ketiga (misalnya, penyedia layanan penyimpanan: iCloud, Googledrive, Dropbox, Box, Onedrive). Dengan menggunakan *Cloud storage* sebagai penyimpanan data, pengguna dapat menyimpan data ke server pihak ketiga dan tidak harus menyimpannya di *dedicated server* yang lazim dipakai pada penyimpanan data di jaringan tradisional. Penyedia layanan ini mengoperasikan pusat data yang besar, dan pemilik data dapat menggunakan *Cloud storage* yang gratis maupun berbayar. Penyimpanan awan memberikan biaya yang rendah berbanding, terukur, dan memiliki lokasi platform sendiri untuk mengelola data pengguna, sehingga semakin banyak pemilik data yang mulai menyimpan data di awan.

Cloud storage mempunyai beberapa keunggulan ditinjau dari segi finansial dan keamanan data. Ditinjau dari segi finansial, sumber daya virtual biasanya lebih murah dibandingkansumber daya fisik yang terhubung ke PC atau jaringan. Adapun secara kemanan, data yang tersimpan di *Cloud Storage* lebih aman terhadap kemungkinan terhapus secara tidak sengaja atau *hardware crash* karena data ini diduplikasi di beberapa mesin fisik. Jadi ada beberapa salinan data dan data tersebut disimpan secara kontinu. Penyimpanan di *Cloud Storage* akan tetap normal walaupun satu atau lebih mesin *crash*. Data akan disimpan dan diduplikasi di *cloud* lain(Quick et al., 2013).



Gambar 2. 2 Cloud Storage pada iOS 7

Sumber : http://support.apple.com/kb/PH2608

2.5 Cloud Storage pada iOS 7

2.5.1 iCloud

iCloud merupakan layanan komputasi awan terbaru yang dipublikasikan oleh Apple Inc pada tanggal 6 Juni 2011. iCloud adalah layanan penyimpanan online gratis yang memungkinkan penggunanya mengakses konten pribadi mereka pada semua perangkat Apple secara otomatis melalui Apple ID masing-masing pengguna. Hal tersebut memungkinkan para penggunanya untuk mensinkronisasi data seperti foto, musik, dan dokumen ke dalam iPhone, iPad, iPod Touch, Mac dan komputer secara otomatis pada waktu yang bersamaan. Sehingga pengguna dapat mengaksesnya dimana saja dan kapan saja tanpa perlu melakukan *back up* data secara manual. iCloud juga melakukan *back up* seluruh data yang ada pada iOS device, membantu penggunanya menemukan perangkat yang hilang dengan fitur yang ada pada iCloud yang terhubung dengan setiap *device Apple*. Fitur-fitur yang terdapat pada iCloud sangat berguna bagi orang yang memiliki satu atau lebih perangkat Apple (Trudy Muller, 2014).

Kelebihan dari Icloud :

a. Membebaskan banyak backup data ke dalam Icloud
b. Apabila gadget hilang/rusak tidak perlu khawatir karena Icloud sudah membackup otomatis data yang ada di gadget tersebut
c. Icloud diunduh secara gratis ,kecuali membutuhkan upgrade kapasitas penyimpanan lebih.

Kekurangan dari Icloud :

a. Tidak dapat memilih beberapa data saja yang disimpan (harus semuanya).
b. Edit dokumen pada ponsel dan ipad bisa ,akan tetapi mengedit dokumen pada mac tidak bisa dilakukan (Sinkronisasi dari perangkat mac tidak ada)



Gambar 2. 3 iCloud

Sumber :

https://developer.apple.com/library/ios/documentation/General/Conceptual/iCloudDesignGuide/Chapters/Introduction.html#//apple_ref/doc/uid/TP40012094-CH1-SW1

2.5.2 Google drive

Google Drive adalah layanan penyimpanan daring (*data sharing*) milik Google yang diluncurkan pada 24 April 2012. Google drive adalah salah satu tempat untuk menyimpan, mengelola, dan mengakses semua *file*, dari mana saja dan pada perangkat apapun yang terhubung dengan internet. Ini memungkinkan pengguna menyimpan *file*, data, maupun dokumen dan berbaginya dengan pengguna lain. Pengguna dapat mengakses *file* ataupun foldernya dari web *browser* ataupun perangkat yang telah terinstall oleh aplikasi Google drive. Google drive selalu menjaga keamanan semua data penggunanya, dan selalu memperbaharui data penggunanya ketika ada data baru. Google Drive memberikan layanan penyimpanan gratis sebesar 5 GB dan dapat ditambahkan dengan pembayaran tertentu.

Kelebihan :

a. Google Drive telah terintegrasi dengan layanan google lainnya diantaranya gmail, simple, tampilan google sangat sederhana, tanpa iklan dan news.
b. Google memudahkan pencarian menggunakan kata kunci yang relevan.
c. Google mendukung *web service* yang diperuntukkan bagi *software developer*.

Kekurangan :

a. Sejak perubahan privasi di Google tanggal 31 Maret 2014, Google dapat memberikan informasi / data dalam akun kita ke pihak yang berwenang (Google, 2014).
b. Terkadang artikel yang kita buat sekarang baru terindex beberapa menit bahkan sampai berhari-hari.
c. Tidak bisa mengindeks halaman tertentu.



Gambar 2. 4 Google drive

Sumber : http://www.cirrusinsight.com/blog/google-drive-vs-dropbox/

2.5.3 Dropbox

Dropbox adalah layanan penyimpanan data berbasis web yang dioperasikan oleh Dropbox, Inc. Dropbox menggunakan sistem penyimpanan berjaringan yang memungkinkan pengguna untuk menyimpan dan berbagi data serta berkas dengan pengguna lain di internet menggunakan sinkronisasi data. Dropbox didirikan pada tahun 2007 oleh lulusan Massachusetts Institute of Technology (MIT) Drew Houston dan Arash Ferdowsi dengan modal awal yang didapat dari Y Combinator. Dropbox menyediakan layanan baik gratis ataupun berbayar. Dropbox adalah rumah untuk semua foto, dokumen, video, dan file. Apa pun yang ditambahkan ke Dropbox secara otomatis akan muncul di semua perangkat telepon, dan juga komputer yang telah diinstall dan terhubung dengan aplikasi Dropbox. Sehingga dapat mengakses data dan dokumen yang tersimpan dalam Dropbox dari mana saja. Dropbox juga mudah untuk berbagi data dengan pengguna lain. Dropbox bekerja keras untuk memastikan bahwa semua data pengguna adalah sama di mana pun pengguna berada. Mulai dokumen dari komputer di sekolah atau bekerja, mengedit dari perangkat telepon pengguna dalam perjalanan pulang, kemudian menambahkan sentuhan dari tablet di ruang tamu pengguna. Dengan aplikasi yang tersedia pada Dropbox pada komputer,

telepon, dan tablet, Anda bisa memamerkan video, secara otomatis meng-upload foto, atau membuka dokumen dari mana saja.

Dropbox menawarkan akun gratis yang dengan kapasitas data sebesar 2GB yang bisa ditingkatkan menjadi 18GB jika Anda mereferensikan ke teman. Dan setiap teman yang ikut mendaftar Anda akan mendapat tambahan 500MB. Untuk akun berbayar, Dropbox memisahkan menjadi 2, yakni Pro dengan kapastias 100, 200, dan 500GB dengan membayar mulai $9.99/bulan (kurang lebih 100 ribu rupiah per bulan), dan akun khusus Teams dengan kapasitas data sebesar 1TB yang bisa dibagi untuk 56 user dengan membayar mulai $795/tahun (Kurang lebih 8.745.000 rupiah per tahun).

Kelebihan dropbox :

a. *Miror* ke *server* dropbox
b. Akses data di mana saja, *desktop,mobile*
c. Akes *file* bisa di atur

Kekurangan dropbox :

a. Sejak perubahan privasi di Dropbox per tanggal 20 februari 2014, dropbox dapat memberikan informasi / data dalam akun kita ke pihak yang berwenang (Dropbox.com, 2014).



Gambar 2. 5 Dropbox

Sumber : http://www.iphoneincanada.ca/news/dropbox-secures-250-million-funding-company-valued-at-10-billion/

2.5.4 Box

Box Inc (sebelumnya Box.net) adalah *online file sharing* dan layanan penyimpanan data online untuk manajemen konten bisnis. Perusahaan ini berdiri pada tahun 2005, mengadopsi model bisnis premium, dan menyediakan hingga 50 GB penyimpanan gratis untuk rekening pribadi. Sebuah versi *mobile* dari layanan penyimpanan ini tersedia untuk Android, BlackBerry, iOS, WebOS, dan

perangkat Windows Phone. Perusahaan yang berbasis di Los Altos, California. Mereka menawarkan 10 GB penyimpanan gratis, tetapi untuk menerima 50 GB penyimpanan gratis, pengguna harus men-download & mencoba versi iOS Apple dari aplikasi mereka.

Kelebihan dari Box :

a. Gratis 10GB untuk kali daftar pertama.
b. Tidak ada iklan , *simple*, ringan,dan *Multiple download*
c. Adanya Cloud untuk pembuatan dokumen *office* , dll.

Kekurangan dari Box :

a. Sejak perubahan privasi di Box per tanggal 1 Agustus 2013, Box dapat memberikan informasi / data dalam akun kita ke pihak yang berwenang (Box.com, 2013).
b. Pada paket *Free* tidak tersedia *direct link*
c. Pada paket *Free* tidak tersedia *set password*



Gambar 2. 6 Box

Sumber : http://thenextweb.com/apps/2012/05/24/box-tweaks-its-cloud-storage-service-for-enterprise-users-upgrades-admin-controls-mobile-security-and-more/

2.5.5 Skydrive(Onedrive)

OneDrive berdiri pada tanggal 9 Agustus 2007 (nama resmi Microsoft OneDrive, sebelumnya adalah SkyDrive, Windows Live SkyDrive, dan Windows Live Folders) adalah layanan komputasi awan serupa dengan Dropbox dan Google Drive yang memungkinkan penggunanya mengunggah dan mensinkronkan berkas ke suatu penyimpanan awandan kemudian mengaksesnya melalui peramban Web atau perangkat tertentu. Layanan ini dibuat oleh Microsoft dan merupakan bagian dari layanan daring (*Data sharing*) Windows Live dan memungkinkan pengguna menyimpan berkas-berkasnya secara pribadi, membagikannya dengan orang-orang dalam kontak, atau menjadikan berkas-

berkas bersifat umum. Berkas-berkas yang dibagikan untuk umum tidak memerlukan akun Microsoft untuk mengaksesnya. Setelah gugatan dari televisi penyiar Inggris BskyB atas penggunaan kata "Sky", Microsoft setuju pada Juli 2013 untuk mengubah nama layanan SkyDrive dalam "jangka waktu yang wajar".Microsoft mengumumkan pada 27 Januari 2014 bahwa SkyDrive akan diganti namanya menjadi OneDrive. (Microsoft.com, 2014)

Kelebihan :

a. Mudah untuk melakukan *upload file*
b. Mudah berbagi share ,dan
c. Mudah digunakan penggunanya

Kekurangan :

a. Tidak adanya kemampuan *drag* , *drop* atau *move file*.
b. Nama atau alamat yang anda *share* tidak mempresentasikan nama pengguna



Gambar 2. 7 Skydrive(Onedrive)

Sumber : http://9mobileprice.in/post/microsofts-onedrive-takes-the-lead-on-google-drive-and-dropbox/

2.6 Skema Enkripsi Cloud Storage

Bab ini menjelaskan bahwa pada sumber yang tertera di *http://www.wuala.com/en/learn/technology* mengatakan bahwa pada proses *upload* dan *download* data dari perangkat penguji ke aplikasi *Cloud Storage* terdapat 3 skema berbeda yang digunakan dalam proses Enkripsi dari perangkat penguji ke *Cloud Storage* maupun sebaliknya, yaitu :

1. *None* (tidak menggunakan proses enkripsi)

   Pada saat proses *upload* dan *download* data berlangsung dari perangkat penguji ke *Cloud Storage* tidak ada enkripsi yang digunakan. Data yang

dikirim ke *Cloud Storage* akan terlihat jelas, dilihat oleh siapapun yang memiliki akses ke koneksi jaringan tersebut.

2. *Encrypted connection* (SSL)

   Pada skema kedua ini proses *upload* dan *download* data dari perangkat penguji ke *Cloud Storage* maupun sebaliknya diamankan (enkripsi) terlebih dahulu saat proses pengiriman data berlangsung ,akan tetapi ketika data telah sampai pada aplikasi *Cloud Storage* yang dituju data hanya dijaga privasinya (tidak di enkripsi pada sisi *server*).

3. *Client-Side Encryption*

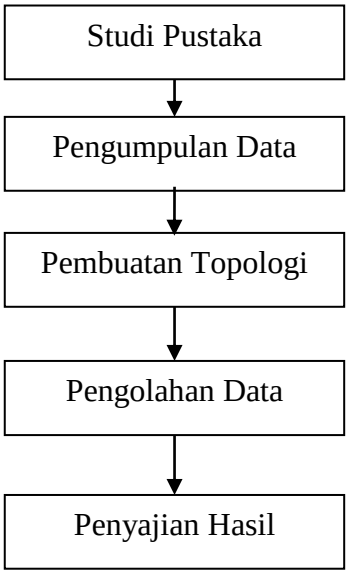
   Pada Skema yang terakhir ini menjelaskan bahwa sebelum proses *upload* dan *download* data berlangsung terlebih dahulu diamankan (enkripsi), setelah proses berjalan data tetap diamankan (enkripsi) baik dari perangkat penguji ke *Cloud storage* maupun sebaliknya ,kemudian pada saat data sampai pada aplikasi *Cloud Storage* yang dituju data tersebut tetap diamankan (enkripsi).

   (Lacie, 2013)

BAB III
METODOLOGI PENELITIAN

3.1 Diagram alur Penelitian

Berikut beberapa tahapan penelitian yang dilakukan oleh penulis yang dijabarkan kedalam bentuk diagram alur seperti yang terlihat pada gambar dibawah :



Gambar 3. 1 Diagram Alur Metodologi Penelitian

3.2 Studi Pustaka

Studi pustaka dilakukan dengan mempelajari bagaimana jalannya aplikasi-aplikasi pendukung, unuk menunjang penelitian. Seperti mempelajari cara kerja *Cloud Storage* yang terdapat pada iOS 7, hingga cara kerja WireShark sebagai aplikasi penangkap paket data pada saat aplikasi *Cloud Storage* dijalankan. Tidak lupa Aplikasi Network Miner sebagai *tools* yang digunakan untuk membaca paket data yang telah ditangkap oleh Wireshark.

3.3 Pengumpulan data

Pada penelitian yang dilakukan kali ini proses pengumpulan data dilakukan dengan 2 tahap. Tahap pertama yaitu melakukan proses penangkapan paket data yang ditransmisikan oleh masing-masing perangkat dengan menggunakan Wireshark. Proses penangkapan data ini dilakukan dengan menghubungkan perangkat yang akan diuji ke dalam jaringan yang telah dibuat dengan rancangan topologi yang sebelumnya sudah dirancang oleh penulis.

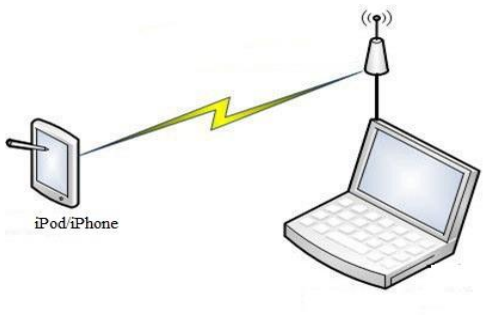
Proses penangkapan paket data ini dilakukan pada masing-masing aplikasi cloud storage yang dijadikan bahan penelitian. Pada tiap aplikasi cloud storage yang ada, langkah percobaan dilakukan dengan cara dan tahapan yang sama.

Tahapan berikutnya adalah melakukan penelaahan terhadap masing-masing paket data yang diperoleh dari hasil percobaan yang telah dilakukan. Untuk melakukan proses penelaaha terhadap hasil yang didapatkan, penulis menggunakan bantuan aplikasi Network Miner untuk menyatukan paket-paket data yang telah dipecahkan ketika proses transmisi dilakukan.

Untuk melakukan penangkapan paket data yang sedang dtransmisikan, dapat menggunakan cara sesuai dengan topologi dibawah ini.

3.3.1 Topologi

Topologi yang digunakan adalah percobaan dilakukan dengan menggunakan Aplikasi Wireshark, kemudian pada notebook di setting sebagai *access point*. Kemudian sebuah perangkat penguji (iPhone, iPod) terhubung di jaringan yang pada *notebook* yang telah terkoneksi internet ,sehingga *notebook* yang terinstall wireshark dapat dengan mudah menangkap paket-paket data yang telah ditransmisikan oleh perangkat penguji (iPhone, iPod).



Gambar 3. 2 Topologi Penangkapan data

Sumber: http://gameaplikasi.wordpress.com/2013/03/20/membuat-hotspot-dengan-windows-7-dan-software-connectify/

Dengan menggunakan topologi pada gambar 3. 2 diatas dalam percobaan, keuntungan yang di dapat adalah kemudahan dalam mendapat hasil paket data yang di tangkap karena hanya *device* ke laptop yang paket datanya di tangkap. Tetapi dengan menggunakan topologi ini sedikit merepotkan, karena perlu melakukan konfirugasi pada *command prompt* di notebook terlebih dahulu. Dan juga apabila menggunakan *Hosted Network,*, tidak semua *notebook* dapat mendukung, karena beberapa *notebook* model lama tidak mendukung *Hosted Network* dari segi *hardware*.

3.4 Pengolahan Data

Setelah semua data dari Cloud Storage yang akan diteliti berhasil didapatkan dari proses pengumpulan data,langkah selanjutnya adalah melakukan pengolahan data dari *Cloud Storage* tersebut, seperti meneliti hasil lalu lintas data yang sudah ditangkap sebelumnya. Untuk melakukan penelitian dari hasil pengumpulan data tadi dapat digunakan Wireshark dan juga Network Miner.

3.5 Analisis Hasil Pengolahan Data

Analisis data dilakukan terhadap jenis informasi yang bisa didapatkan dengan melakukan percobaan pada masing-masing aplikasi melalui tahapan yang sama ditiap langkahnya. Selain ingin mengetahui informasi apa saja yang bisa didapatkan pada proses percobaan ini penulis juga ingin meneliti metode-metode pengamanan yang digunakan pada masing-masing perocbaan berdasarkan pada paket yang didapat.

Hal tersebut dilakukan dengan cara mencari sertifikat-sertifikat yang disertakan ketika paket ditransmisikan. Sehingga akan dapat diketahui metode pengamanan apakah yang digunakan.

Pada tahap penyajian hasil pengolahan data, data dari pengolahan paket data yang didapat dari lalu lintas jaringanlah yang akan disajikan. Hasil juga akan

disajikan dalam bentuk tabel-tabel yang berisi daftar data/file hasil temuan selama dilakukan percobaan.

3.5.1 Informasi Tabel Analisis Aplikasi Cloud Storage pada iOS 7

Tabel informasi yang ada di bawah ini akan menjelaskan jenis informasi saja yang bisa didapatkan dengan melakukan proses percobaan yang sama ditiap aplikasi Cloud Storage yang digunakan.Terdapat dua penanda yang digunakan oleh penulis untuk menandakan hasil apa yang didapatkan pada proses penangkapan data ini. Hasil yang dimaksudkan pada tabel informasi yang ada di bawah ini mempunyai maksud bahwa didapatkan informasi baik berupa host, frame, files, message, session atau parameter dari hasil uji coba yang dilakukan.

Tanda centang menandakan bahwa terhadapat hasil yang didapatkan dari proses penangkapan data yang dilakukan, sedangkan tanda silang menandakan bahwa tidak didapatkan informasi apa-apa dari proses penangkapan data yang dilakukan.

Tabel 3. 1 Hasil upload file aplikasi Cloud Storage pada iOS 7

*: √ (jika didapatkan hasil) dan × (jika tidak didapatkan hasil sama sekali)

Aplikasi	Hosts	Frame	Files	Images	Messages	Sessions	Parameters
Box	√	√	√	×	×	√	×
Google drive	√	√	√	×	×	√	×
Dropbox	√	√	√	×	×	√	×
Skydrive	√	√	√	×	×	√	×
Icloud	√	√	√	×	×	√	×

Tabel 3. 2 Hasil download file aplikasi Cloud Storage pada iOS 7

Aplikasi	Hosts	Frame	Files	Images	Messages	Sessions	Parameters
Box	√	√	√	×	×	√	×
Google drive	√	√	√	×	×	√	×
Dropbox	√	√	√	×	×	√	×
Skydrive	√	√	√	×	×	√	×
Icloud	√	√	√	×	×	√	×

* : √ (jika didapatkan hasil) dan × (jika tidak didapatkan hasil sama sekali)

3.6 Kebutuhan Perangkat Keras

Mengacu kepada topologi yang dilakukan pada saat pengumpulan data, maka kebutuhan yang diperlukan untuk melakukan percobaan ini berupa:

a. Apple Device

   Apple device yang digunakan untuk melakukan percobaan adalah Ipod Touch 5 dan Iphone 4. Kedua Apple device ini yang digunakan sudah menggunakan iOS 7 resmi,jadi tidak perlu melakukan *jailbreak* agar paket data dapat di tangkap.

b. Netbook dan Notebook

   Netbook dan Notebook yang digunakan untuk percobaan adalah Hp Mini, dan Asus N43 yang telah terinstall *Wireshark* dan *Network Miner*.Kemudian Netbook disetting sebagai *Hosted Network.*

3.7 Kebutuhan Perangkat Lunak

Untuk dapat melakukan percobaan, mulai dari menangkap data, hingga mengolah data, akan menggunakan beberapa aplikasi *Network Analyzer*, yang diantaranya adalah sebagai berikut:

a. WireShark

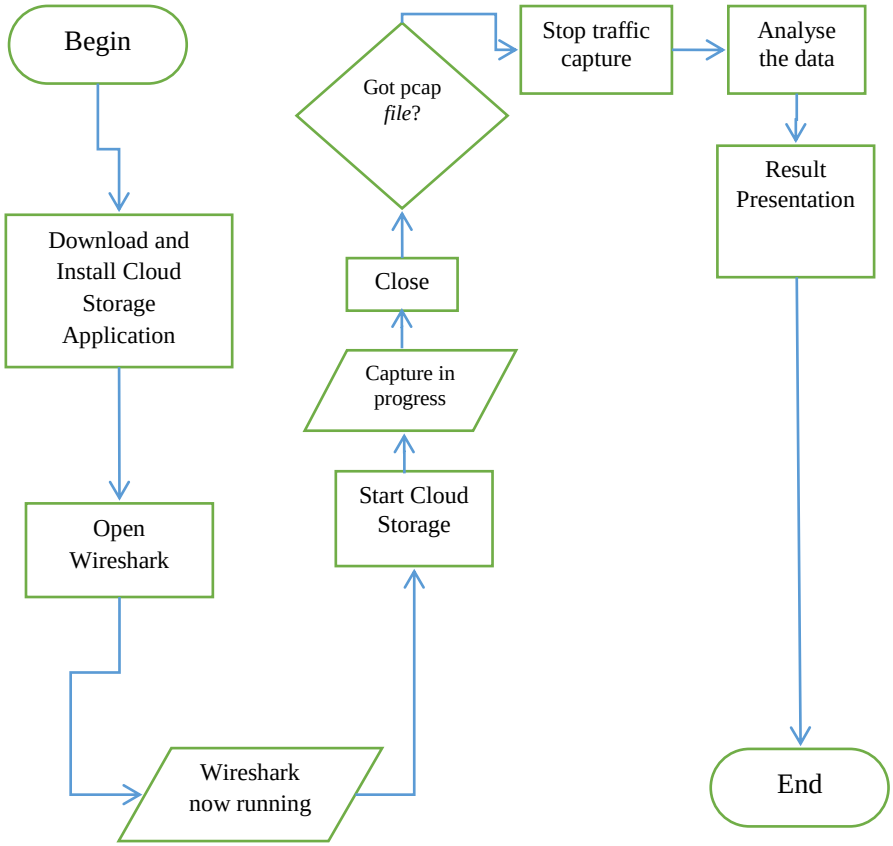
Wireshark merupakan salah satu aplikasi *Network Analyzer* yang banyak digunakan untuk menangkap lalu lintas data.Wireshark juga bisa digunakan untuk meneliti hasil file yang sudah ditangkap tersebut.

b. Network Miner

Network miner sama halnya dengan WireShark, digunakan untuk meneliti hasil file yang sudah ditangkap. Namun paket-paket data yang didapat langsung dipilah-pilah berdasarkan parameter yang tersedia. Sehingga tidak perlu memilah secara manual. Hal ini sangat memudahkan dalam penelitian dan pelaksanaan percobaan.

3.8 Flowchart

Pada Sub bab ini, merupakan tahap percobaan yang dilakukan penguji untuk mengimplementasikan penelitian. Berikut merupakan Flowchart (langkah - langkah) yang dibuat untuk membantu melaksanakan percobaan.



Gambar 3. 3 Flowchart Penelitian

3.9 Hasil yang Dikehendaki

Percobaan yang dilakukan selama proses penelitian, berdasarkan konfigurasi topologi yang dipilih, alat yang tersedia, serta aplikasi-aplikasi penunjang, diharapkan dapat memberikan beberapa hasil, diantaranya adalah :

a. Dapat mengetahui data atau file terenkripsi atau tidak pada saat proses upload dan download berlangsung.
b. Mampu mendapatkan data atau file yang ditransmisikan ketika proses upload dan download berlangsung.

c. Dapat mengetahui data yang tersimpan di masing-masing *Cloud Storage* terenkripsi atau tidak.
d. Dapat mengetahui metode pengamanan yang digunakan oleh masing-masing *Cloud Storage* yang tersedia.

BAB IV
HASIL DAN PEMBAHASAN

4.1 Proses Penangkapan Lalu Lintas Data

Proses penangkapan data dilakukan menggunakan perangkat netbook hp mini dan notebook Asus N43. Sambungkan notebook tersebut pada sebuah koneksi internet, kemudian lakukan pengaturan pada notebook yang akan digunakan tersebut dengan setting hosted network melalui perintah command prompt sehingga notebook tersebut akan menjadi sebuah *access point*. Langkah selanjutnya perangkat yang akan diuji nantinya harus terkoneksi dengan notebook yang telah diatur sebagai *access point*. Setelah semua perangkat terkoneksi dengan *access point* yang telah dibuat tersebut, maka proses selanjutnnya adalah menjalankan aplikasi *Cloud Storage* yang akan diuji secara bergantian. Proses percobaan ini dimulai dengan terlebih dahulu mematikan aplikasi lain, terutama aplikasi yang membutuhkan koneksi internet yang tidak digunakan.

Hal tersebut dilakukan agar hasil penangkapan data yang dilakukan akan lebih fokus pada lalu lintas data yang terjadi pada aplikasi *Cloud Storage* yang akan diuji. Jalankan Wireshark yang telah dipasang pada Notebook, kemudian lakukan proses pengunggahan dan pengunduhan file pada aplikasi Cloud Storage yang ada.

Dalam hal ini koneksi internet harus stabil agar didapatkan hasil yang maksimal saat penangkapan data berlangsung. Oleh karena itu proses pengujian dilakukan pada beberapa lokasi yang berbeda-beda untuk mendapatkan hasil yang terbaik.

Untuk mendapatkan hasil yang diinginkan, pada proses percobaan ini tidak dibatasi dengan waktu percobaan, melainkan membatasi percobaan melalui fitur apa saja yang akan diteliti pada tiap aplikasi yang digunakan. Setelah dilakukan percobaan pada tiap aplikasi dengan masing-masing fitur yang dimiliki, maka percobaan akan dihentikan.

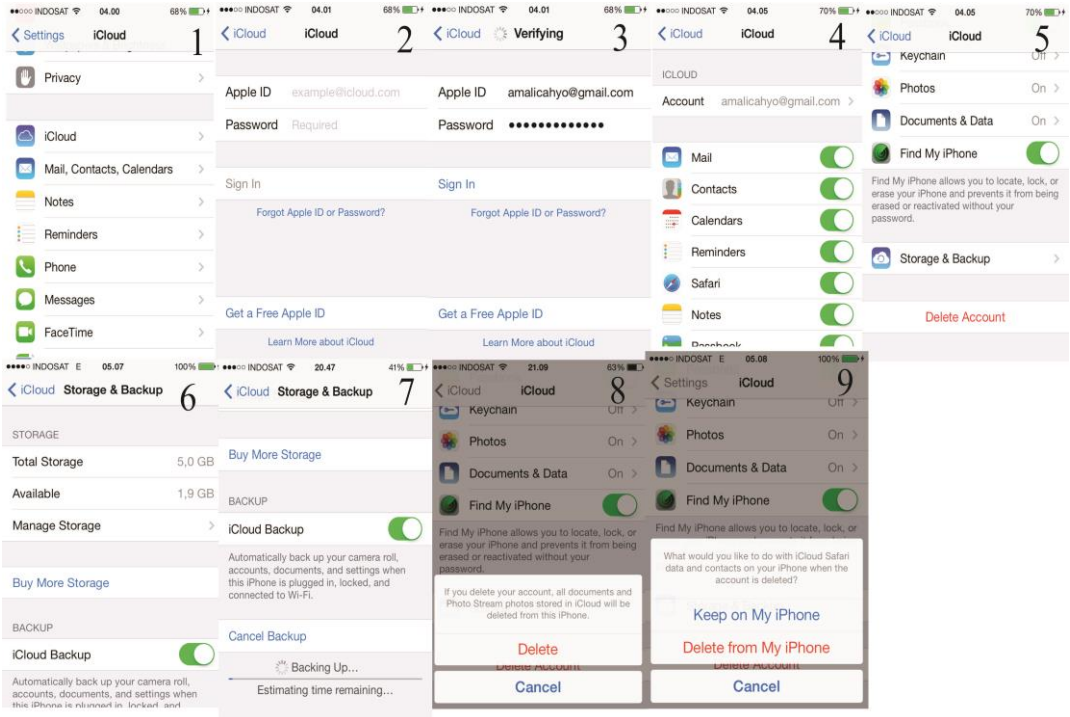
Pada percobaan ini aplikasi yang digunakan untuk melakukan proses penangkapan data dan menganalisisnya adalah Wireshark dan NetworkMiner. Wireshark memiliki kegunaan menganalisa kinerja jaringannnya termasuk dengan protokol didalamnya. NetworkMiner juga memiliki fungsi yang sama dengan Wireshark, namun NetworkMiner memiliki kemampuan untuk menyatukan paket data yang telah terpisah menjadi kebentuk semua, walaupun tidak semua paket data dapat disatukan. Adanya beberapa kelebihan dan kekurangan dari masing-masing aplikasi inilah yang menjadikan pertimbangan bagi penulisa untuk menggnunakan keduanya, dengan harapan hasil yang didapatkan akan maskimal.

4.2 Aplikasi Cloud storage yang diuji

4.2.1 iCloud

Aplikasi pertama yang menjadi bahan percobaan adalah iCloud. Dimana aplikasi ini adalah *Cloud Storage* bawaan yang terdapat pada setiap perangkat Apple. Jalankan aplikasi iCloud untuk melakukan proses *upload* dan *download* data yang terdapat pada iPhone. Ketika sedang terjadi proses *upload* dan *download* tersebut dilakukan proses penangkapan data dengan menggunakan aplikasi Wireshark.

Terkait dengan fitur upload dan download yang dimiliki tersebut ada pun file mampu di download dan di upload diantaranya seperti dokumen dan data, foto, *video, contact ,safari, calenders.*



Gambar 4. 1 Tampilan Aplikasi iCloud

Pada gambar 4.1 diatas dapat dilihat tampilan menu utama dari aplikasi iCloud tersebut. Setelah masuk ke dalam menu awal iCloud, pada halaman selanjutnya gambar 4.1 yaitu proses *sign in* iCloud menggunakan *Apple id*. Pada saat proses *sign in* berlangsung terdapat verifikasi data yang telah tersinkron antara iCloud dengan data yang terdapat pada perangkat yang akan berjalan, dimana pada saat itu terjadi proses *upload* dan *download* data apabila ada data baru yang yang terdapat pada perangkat belum ditambahkan di iCloud maka data akan secara otomatis ter-upload sendiri pada saat sinkronisasi *Apple id* berlangsung. Begitupun sebaliknya apabila pada data terbaru dari iCloud belum ada pada perangkat, maka akan secara otomatis melakukan *download* data setelah perangkat tersinkron dengan iCloud. Setelah *sign in* Apple id selesai, secara otomatis data yang yang terdapat pada iCloud akan ditampilkan pada perangkat. Pada halaman ini terdapat pilihan untuk mengaktifkan atau tidak data yang ada untuk di sinkronkan dengan iCloud. Pilihan tersebut memudahkan pengguna perangkat ini di dalam memilih data yang akan di sinkronkan dengan iCloud dan yang tidak.

Kemudian pada gambar 4.1 terdapat menu pilihan *delete account*, *storage* dan *backup*. Selanjutnya gambar 4.1 penggguna dapat melihat kapasitas

penyimpanan pada iCloud, dan kapasitas yang tersisa. Dalam hal ini apabila pengguna ingin menambahkan kapasitas *storage* dapat dilakukan dengan membelinya sesuai keinginan gambar 4.1 pada menu *storage* dan *backup* berupa pilihan untuk secara otomatis akan melakukan *backup* data yang terdapat pada perangkat yang berupa foto, video, akun, dan dokumen dimana saat perangkat terkoneksi dengan komputer atau saat terkoneksi dengan wifi.

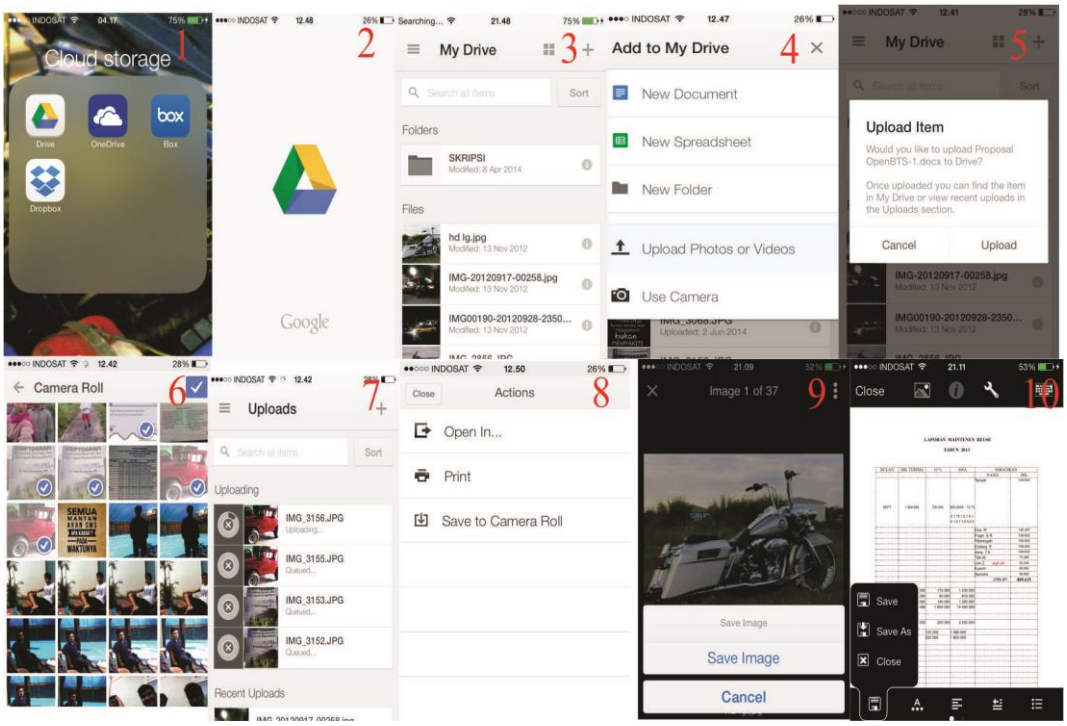
Data yang di *backup* tersebut merupakan data terbaru yang menggantikan data lama atau tersimpan sebelumnya pada iCloud. gambar 4.1 pada pilihan *delete account* ini pengguna iCloud dapat memilih untuk menghapus *account* yang telah tersinkron dengan *device* dan menggantinya dengan *account* yang baru. Namun pada saat *account* dihapus akan muncul dua pilihan yaitu safari data dan *contact* tetap disimpan dalam perangkat atau akan dihapus semua.

Setelah semua fitur tersebut dicoba, maka aplikasi Wireshark dihentikan dan ditutup, kemudian dilakukan penamaan ulang dan disimpan dalam folder yang telah diberi nama sesuai aplikasi yang akan diuji, hal tersebut dilakukan supaya tidak tertukar dengan *file* pcap dari aplikasi lain pada nantinya. Dengan mencoba semua fitur milik iCloud, diharapkan pada *file* hasil percobaan tersebut nantinya akan mendapatkan banyak hasil yang diinginkan, seperti foto-foto pada proses *upload* dan *download* berlangsung, maupun mendapatkan *file dokumen* yang dikirimkan .

4.2.2 Google drive

Aplikasi milik Google ini lebih dikenal sebagai media penyimpanan *online* yang sering digunakan oleh banyak penggunanya dikarenakan pengoperasiannya yang mudah. Tahapan percobaan dimulai setelah perangkat penguji terhubung dengan *access point* kemudian aplikasi Google drive yang terdapat pada Apple device dijalankan .Pada saat Google drive berjalan, aplikasi wireshark juga ikut dijalankan guna melakukan proses *capture* data yang sedang berlangsung pada aplikasi google drive yang sedang berjalan.

Kemudian terkait file yang akan di upload dan di download hampir sama dengan iCloud, kebanyakan meliputi dokumen dan data, foto, *video*.



Gambar 4. 2 Tampilan Aplikasi Google drive

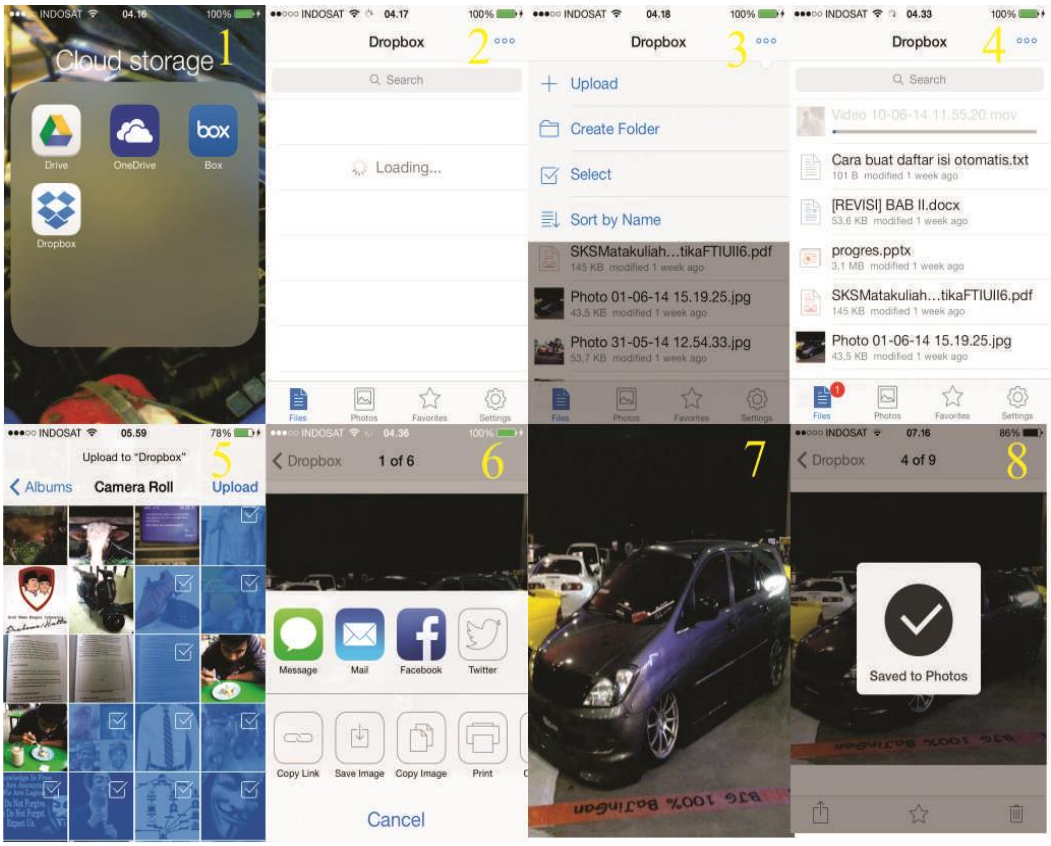
Pada halaman utama gambar 4.2 adalah tampilan aplikasi Google drive. Aplikasi sudah terlebih dahulu di sign in sebelum diujikan, sehingga pada waktu aplikasi tersebut dibuka tidak memerlukan proses sign in kembali. Kemudian menu utama setelah masuk aplikasi Google drive dimana pada terdapat tampilan menu untuk membuat dan mengunggah dokumen baru, mengunggah foto ataupun video. Kemudian pada gambar 4.2 adalah proses mengunggah file foto, video dan dokumen. Dilanjut dengan gambar 4.2 adalah contoh beberapa file foto yang akan diunggah di Google drive. Unttuk gambar 4.2 merupakan proses mengunggah file yang telah dipilih. Selanjutnya untuk gambar 4.2 adalah tampilan pilihan untuk mengunduh suatu file yang terdapat pada Google drive. Gambar 4.2 merupakan contoh file dan dokumen yang akan diunduh melalui google drive untuk disimpan di perangkat penguji.

Setelah semua fitur tersebut dicoba, maka aplikasi Wireshark dihentikan dan ditutup. Tidak lupa kemudian *file* pcap yang telah dibuat, dilakukan penamaan ulang dan disimpan pada folder yang telah dibuat berdasarkan nama aplikasi yang akan diuji, hal tersebut dilakukan agar tidak tertukar dengan *file* pcap dari aplikasi lain pada nantinya. Hasil yang diharapkan dari semua fitur diatas, adalah dapat menangkap segala sesuatunya dari hasil proses penangkapan data menggunakan

Wireshark. Termasuk mungkin apabila dapat menangkap file *foto, video dokumen dan data*.

4.2.3 Dropbox

Sama halnya dengan Icloud dan Google drive aplikasi ini tak kalah populernya di mata penggunanya dikarenakan kemudahan dalam pengoperasiannya. Dropbox juga diperlakukan hal yang sama. Dari tahap awal setelah Apple device terhubung dengan netbook/Notebook yang telah di setting sebagai access point kemudian aplikasi Dropbox yang terdapat pada iPhone dan iPod dijalankan. Pada saat Dropbox berjalan, aplikasi wireshark juga ikut dijalankan guna melakukan proses capture data yang sedang berlangsung pada aplikasi tersebut saat berjalan. Fitur-fitur pada Dropbox yang akan dipercobakan yakni meliputi proses upload dan download *foto ,video ,dokumen dan data* .



Gambar 4. 3 Tampilan Aplikasi Dropbox

Pada halaman awal gambar 4.3 dapat dilihat aplikasi-aplikasi yang menjadi acuan penguji untuk melakukan analisis, salah satu aplikasi tersebut adalah dropbox .Sebelumnya aplikasi sudah terlebih dahulu dilakukan sign in

sebelum diujikan. Hal tersebut dilakukan guna mempermudah proses pengujian. Terlihat pada gambar 4.3 halaman awal adalah tampilan menu utama dari aplikasi tersebut. Seperti Google drive aplikasi Dropbox juga telah di sign in terlebih dahulu oleh penguji guna mempermudah dalam membuka aplikasi sehingga tidak perlu lagi sign in terlebih dahulu. Sama halnya dengan Google drive pada gambar 4.3 terdapat tampilan menu pilihan untuk mengunggah file dokumen, foto, ataupun video. Ada juga pilihan untuk membuat folder baru dan memilih file yang akan diunggah.

Gambar 4.3 merupakan salah satu proses mengunggah video dari media penyimpanan yang terdapat pada apple device ke Dropbox. Kemudian gambar 4.3 adalah salah satu cara untuk memilih beberapa file foto yang diinginkan. Pada gambar 4.3 merupakan contoh menu pilihan untuk mengunduh sebuah file foto, video maupun dokumen yang terdapat pada Dropbox. Untuk selanjutnya pada gambar 4.3 adalah salah satu contoh file yang dapat diunduh dari Dropbox ke penyimpanan yang ada pada perangkat penguji.

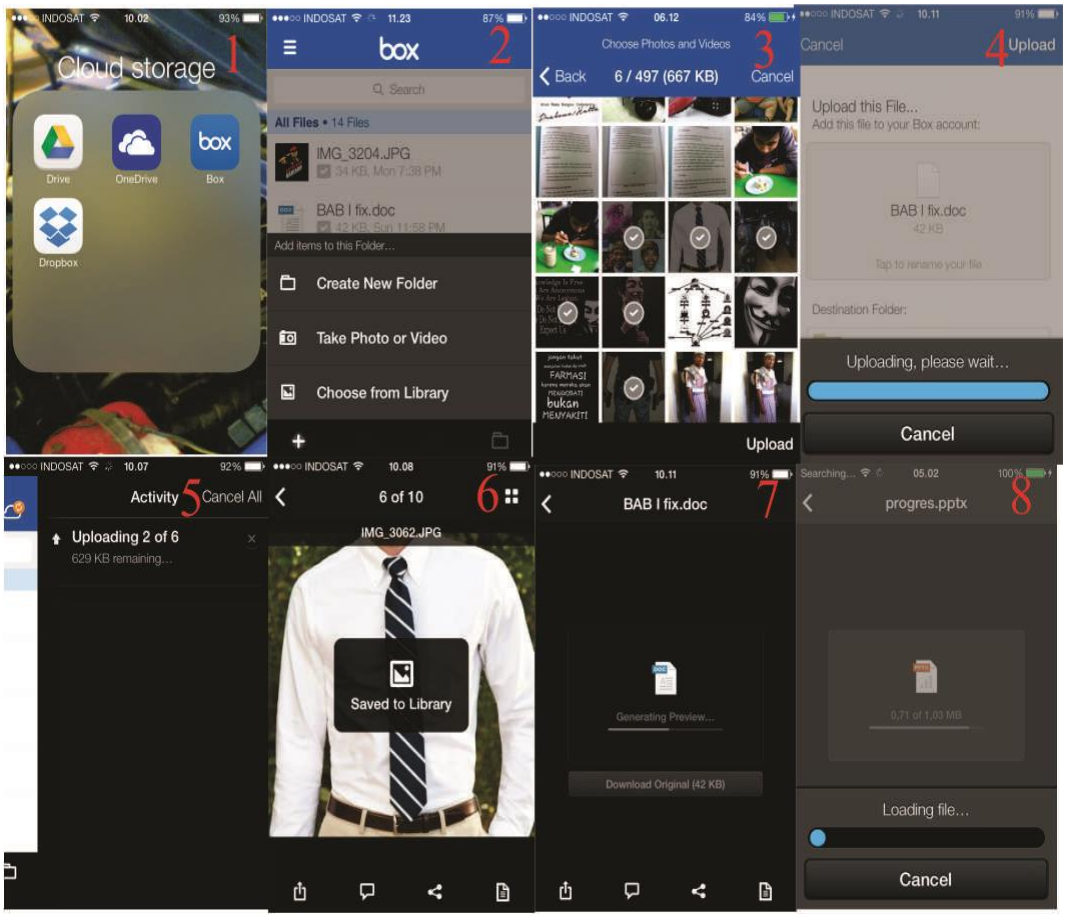
Setelah kesemua fitur dijalankan, maka yang berikutnya adalah segera menghentikan, menutup aplikasi Dropbox, dan juga Wireshark, lalu kemudian *file* pcap hasil buatan dari Wireshark disimpan dan diganti nama, supaya tidak membingungkan ataupun tertukar dengan *file* yang yang terdapat pada aplikasi lain. Setelah *file* pcap diberi nama kemudian masukkan file tersebut ke dalam folder yang telah dibuat berdasarkan nama dari masing-masing aplikasi tersebut. Hasil yang diharapkan adalah dapat menangkap segala sesuatunya dari hasil proses penangkapan data menggunakan Wireshark. Termasuk mungkin apabila dapat menangkap file *foto, video dokumen dan data*.

4.2.4 Box

Sama halnya dengan iCloud ,Google drive ,Dropbox. Box juga diperlakukan hal yang sama. Yakni Dilakukan dari tahap awal yaitu setelah Apple device terhubung dengan netbook/Notebook yang telah di setting sebagai access point kemudian aplikasi Box yang terdapat pada iPhone dan iPod dijalankan .Pada saat Box berjalan ,aplikasi wireshark juga ikut dijalankan guna melakukan proses capture data yang sedang berlangsung pada aplikasi Box saat berjalan. Sama halnya dengan percobaan yang dilakukan pada aplikasi iCloud, Dropbox, dan

google drive sebelumnya proses lalu lintas data pada saat upload dan download menjadi acuan Penguji untuk mendapatkan data. Terkait fitur-fitur yang akan diuji adalah *dokumen, data, foto dan video.*

Sebelum masuk ke Tampilan awal dari aplikasi ini penguji telah terlebih dahulu melakukan sign in pada aplikasi, agar dapat mempermudah dalam membuka aplikasi. sama halnya dengan aplikasi Cloud storage sebelumnya ,dapat dilihat pada gambar 4.4 dibawah ini tampak pada halaman utama Box. Terlihat pada gambar 4.4 dimana terdapat pilihan untuk membuat folder baru, mengunggah foto dari penyimpanan yang terdapat pada Apple device. Menu pilihan tersebut hampir sama dengan aplikasi-aplikasi sebelumnya terkecuali iCloud. Sama halnya dengan Google drive ataupun Dropbox ,pada gambar 4.4 salah satu contoh file foto atau video yang akan diunggah terlebih dahulu dipilih. Selanjutnya pada gambar 4.4 adalah proses mengunggah sebuah file yang diambil dari media penyimpanan yang terdapat pada perangkat penguji ke dalam aplikasi Box. Kemudian gambar 4.4 merupakan contoh proses mengunduh file yang berupa foto dan dokumen untuk kemudian disimpan pada media penyimpanan yang ada di perangkat penguji.



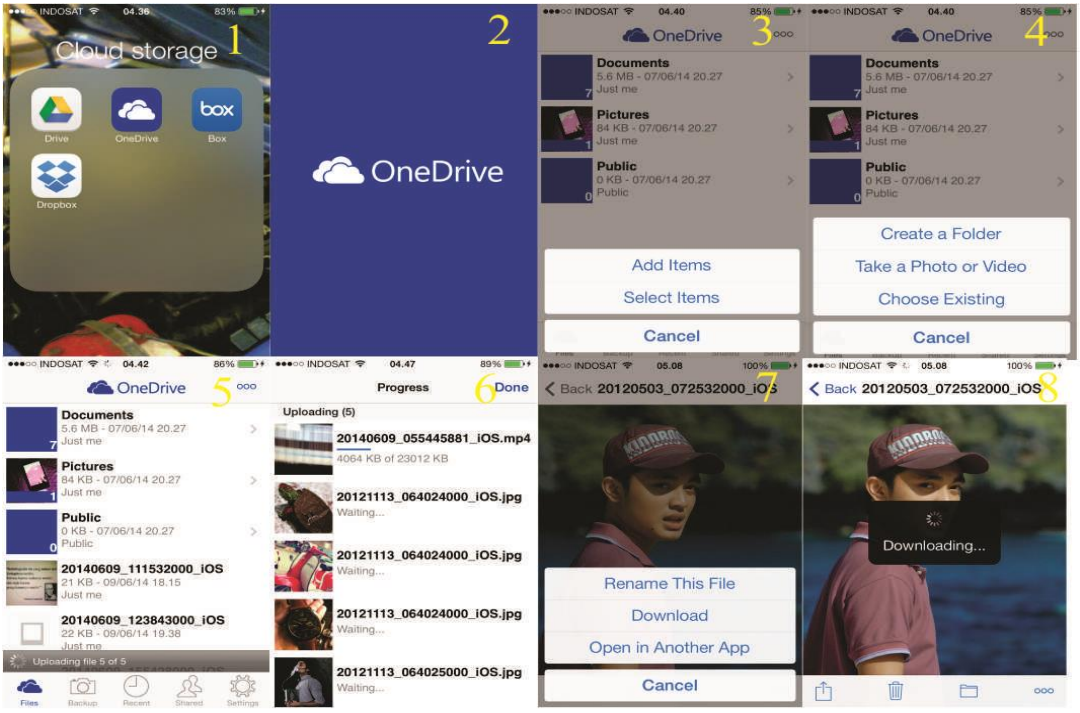
Gambar 4. 4 Tampilan Aplikasi Box

Setelah semua fitur pada aplikasi Box dicoba, maka selanjutnya adalah menutup aplikasi Box, dan diikuti dengan menutup aplikasi Wireshark. Kemudian setelah menutup kedua aplikasi tersebut langkah selanjutnya adalah melakukan penamaan ulang terhadap *file* pcap yang dihasilkan oleh Wireshark, dan menyimpannya kedalam folder yang telah diberi nama sesuai aplikasi yang menjadi bahan ujian agar mempermudah dalam mencari dan tidak tertukar antar aplikasi satu dengan yang lain. Hasil yang dikehendaki setelah fitur-fitur dicoba adalah dapat menangkap segala sesuatunya dari hasil proses penangkapan data menggunakan Wireshark. Termasuk mungkin apabila dapat menangkap file *foto, video dokumen dan data*.

4.2.5 Skydrive(Onedrive)

Aplikasi terakhir yang akan dilakukan penangkapan data yakni aplikasi *Cloud Storage* berupa Skydrive yang sekarang sudah berubah nama menjadi Onedrive. Aplikasi besutan Microsoft ini juga dikenal luas oleh penggunanya.

Sama dengan aplikasi-aplikasi sebelumnya mulai tahap awal yaitu setelah Apple device terhubung dengan netbook/Notebook yang telah di setting sebagai access point kemudian aplikasi Onedrive yang terdapat pada iPhone dan iPod dijalankan. .Pada saat Onedrive berjalan ,aplikasi wireshark juga ikut dijalankan guna melakukan proses capture data yang sedang berlangsung pada aplikasi Onedrive yang sedang berjalan. Sama halnya dengan percobaan yang dilakukan pada aplikasi iCloud, Dropbox, Google drive, dan Box sebelumnya. Proses lalu lintas data pada saat upload dan download menjadi untuk diuji guna mendapatkan data. Hampir sama dengan iCloud, Googledrive, Dropbox, dan Box, fitur-fitur yang akan dipercobakan pada aplikasi ini saat proses upload dan download berlangsung yaitu dokumen, data ,foto dan video.



Gambar 4. 5 Tampilan Aplikasi Skyderive (Onedrive)

Setelah melakukan sign in terlebih dahulu pada aplikasi Onedrive agar mempermudah Penguji dalam membuka aplikasi. Karena apabila Penguji belum terlebih dahulu melakukan sign in, maka akan muncul tampilan sign in terlebih dahulu, hal tersebut menjadikan proses menjadi lebih lama sehingga dilakukan sign in terlebih dahulu agar mempermudah dalam membuka aplikasi. Pada tahap selanjutnya gambar 4.5 merupakan macam-macam aplikasi yang menjadi acuan dan juga tampilan awal membuka aplikasi pada saat aplikasi telah sign

in.Kemudian pada gambar 4.5 pada halaman awal ada pilihan add item dan select item. Untuk proses add item pada gambar 4.5, ada pilihan untuk membuat folder baru, mengunggah foto, video maupun dokumen. Ini sama halnya dengan pilihan yang ada pada halaman awal aplikasi sebelumnya. Pada gambar 4.5 proses mengunggah data yang telah dipilih sedang berlangsung. Dilanjutkan pada gambar 4.5 salah satu proses mengunggah Video yang sedang berlangsung. Proses mengunggah video biasanya membutuhkan durasi waktu yang lebih lama, dikarenakan ukuran file yang besar. Selanjutnya pada gambar 4.5 adalah salah satu contoh proses mengunduh file foto dari Onedrive kemudian disimpan ke dalam media penyimpanan yang terdapat pada perangkat penguji.

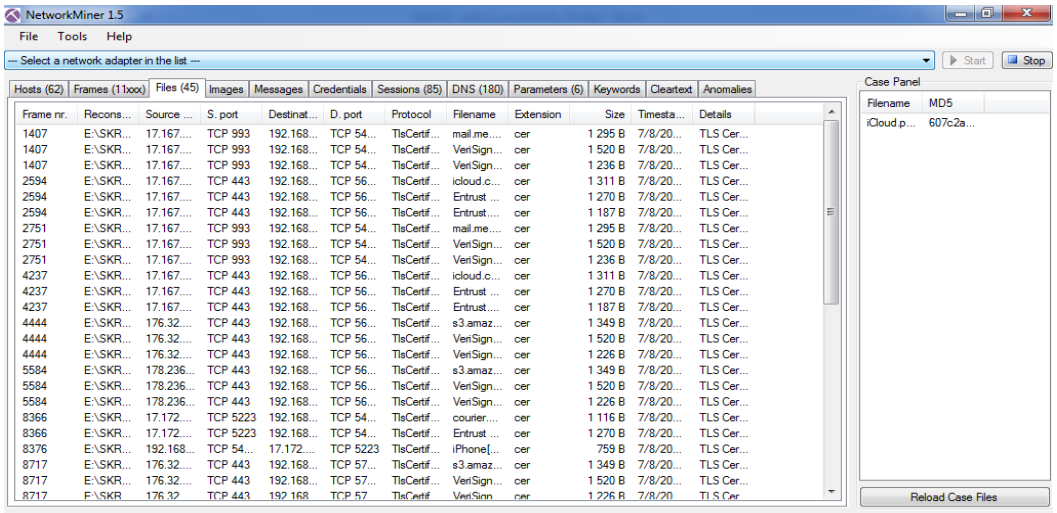
Proses penangkapan data yang sedang ditransmisikan sudah selesai. Mulai dari iCloud, Google drive, Dropbox, Box, dan Skydrive/Onedrive. Langkah selanjutnya setelah *file* pcap hasil tangkapan disimpan dalam folder yang telah diberi nama sesuai dengan nama masing-masing aplikasi yang menjadi acuan untuk diuji (folder tersebut disimpan pada netbook atau notebook yang menjadi alat uji). Kemudian folder yang berisi file hasil tangkapan tersebut ditelaah untuk mendapatkan data yang dikehendaki, dan dilakukan analisis paket-paket apa saja yang dapat dibaca maupun diambil oleh penguji.

4.3 Analisis Hasil Lalu Lintas Data

Setelah selesai mengambil data menggunakan Wireshark, langkah yang selanjutnya dilakukan yakni menelaah paket-paket data yang tertangkap. Aplikasi yang digunakan untuk menelaah *file-file* pcap yang ditangkap oleh Wireshark adalah Network Miner. Aplikasi Network Miner berguna untuk menyatukan kembali paket-paket data yang dipecah ketika proses lalu lintas data berlangsung. Akan tetapi tidak semua file dapat disatukan kembali setelah file tersebut dipecah. Karena tujuan yang ingin dicapai adalah untuk mendapatkan informasi sebanyak-banyaknya dari proses penangkapan data tersebut, maka penguji tidak membatasi harus mendapatkan suatu *file* ataupun tidak, hanya menggunakan fitur dari aplikasi *cloud storage* yang terdapat pada perangkat penguji sebagai acuan. Apabila didapatkan temuan lain, akan tetap dicantumkan sebagai hasil. Berikut merupakan hasil temuan dari paket data yang berhasil ditangkap.

4.3.1 iCloud

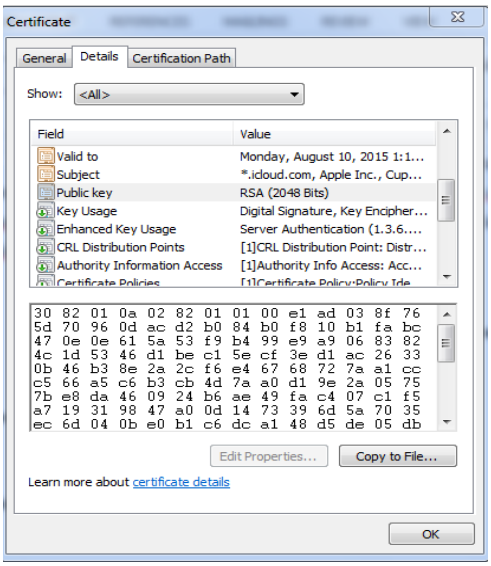
Selama proses penangkapan data yang berjalan pada saat proses *upload* dan *download*, pada aplikasi Icloud tercatat sebanyak 11404 *frame* paket yang ditransmisikan. Menggunakan *Network Miner*, *file* pcap yang ada lalu disusun ulang, sehingga menjadi lebih mudah untuk dibaca. Hasil yang didapatkan, yakni sebanyak 45 *file*, dan diantara paket yang ditangkap tersebut tidak satupun mendapatkan *file image* ataupun *text*. Hampir seluruh file yang tertangkap adalah *TLS (Transport Layer Security) certificate*. Untuk sesi yang tercatat, adalah sebanyak 85 sesi. Pada percobaan yang dilakukan, tidak mendapatkan *user id* maupun *password*. Seperti terlihat pada gambar 4.6 dibawah ini. Apabila menggunakan Wireshark, ketika dicoba untuk disusun ulang, *file* yang sedang ditransmisikan melalui jaringan, juga didapati banyak *file*, akan tetapi tidak semua *file* dapat disusun ulang oleh Wireshark. Lebih lengkap apabila proses penyusunan file berdasarkan kategorinya menggunakan Network Miner seperti terlihat dibawah ini.



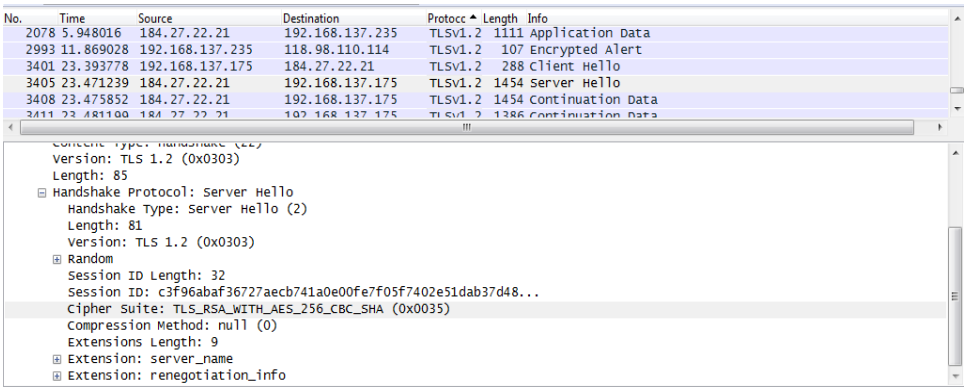
Gambar 4. 6 Tampilan pada tab files dari paket iCloud

Dari sekian banyak *file* yang ada, informasi *file certificate* yang paling banyak ditemukan pada aplikasi ini. Hal itu menandakan setiap file yang ditransmisikan pada saat proses upload dan download data di iCloud diamankan terlebih dahulu. Hampir seluruh *file* yang didapat adalah sertifikat dengan ekstensi *".cer"*. Metode pengamanan yang digunakan untuk mengamankan jalannya data yakni, untuk menggunakan koneksi TLS 1.2 antara aplikasi ke *server* milik

iCloud, dan data dienkripsi menggunakan AES, dengan panjang kunci 256 bit , dan untuk *hash* digunakan SHA. Sedangkan untuk pengamanan pertukaran kunci, menggunakan algoritma *public key* RSA dengan panjang kunci 2048 bit dapat dilihat pada gambar 4.7 dan 4.8 dibawah ini.



Gambar 4. 7 Tampilan salah satu sertifikat dari iCloud



Gambar 4. 8 Screenshot dari paket handshake iCloud

Karena banyak dari frame yang berhasil ditangkap, telah dienkripsi. Berdasarkan hasil olah data yang dilakukan, dapat disimpulkan dalam tabel dibawah ini. Tabel tersebut dibuat berdasarkan fitur umum yang terdapat pada aplikasi *iCloud*.

Tabel 4. 1 Checklist iCloud dengan Wireshark

Wireshark								
Photo and video	Contacts	Document and data	Notes	Calendars	Mail	Reminders	Safari	passbook
✕	✕	✕	✕	✕	✕	✕	✕	✕

*** :** √ (jika didapatkan hasil) dan ✕ (jika tidak didapatkan hasil sama sekali)

Tabel 4. 2 Checklist iCloud pada Network Miner

Network Miner								
Photo and video	Contacts	Document and data	Notes	Calendars	Mail	Reminders	Safari	passbook
✕	✕	✕	✕	✕	✕	✕	✕	✕

*** :** √ (jika didapatkan hasil) dan ✕ (jika tidak didapatkan hasil sama sekali)

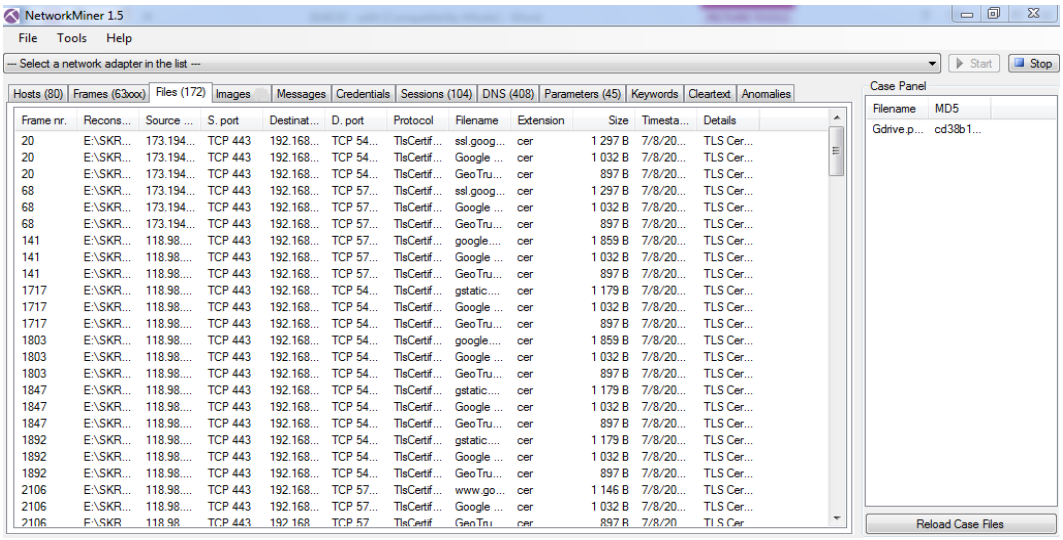
Pada tabel 4.1, pada waktu proses olah data *Photo upload dan download* tidak mendapatkan *file* foto yang di*upload* maupun *download*. Hanya didapat beberapa file .cer saja yang tertangkap oleh Wireshark. Sama seperti *photo upload* dan *download*, pada fitur *documents* dan *data*, *notes*, *calendars, mail, reminders* juga tidak didapatkan *file apapun* pada saat proses *upload* dan *download* berjalan. Pada kolom *safari* dan *passbook* juga sama, tidak terdapat satupun file yang didapat pada saat proses *transfer* data berlangsung.

Kemudian pada tabel 4.2 Network miner tidak didapatkan file foto maupun document data yang di *upload* atau *download*. Hanya file. cer saja yang ditangkap. Hal tersebut sama dengan percobaan yang dilakukan pada Wireshark

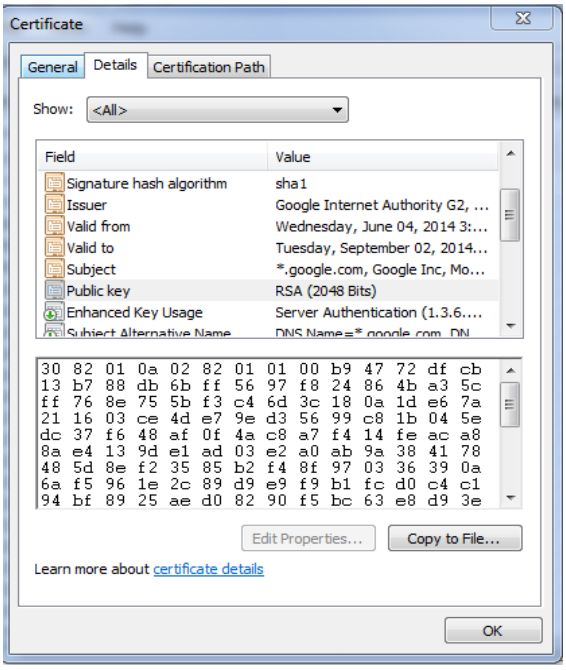
4.3.2 Google drive

Selama proses penangkapan data berlangsung, aplikasi Google drive tercatat sebanyak 63303 *frame* paket yang ditransmisikan. Menggunakan Network Miner, *file* pcap yang ada lalu disusun ulang, sehingga menjadi lebih mudah untuk dibaca. Hasil yang didapatkan, yakni sebanyak 172 *file* sertifikat yang digunakan oleh Google drive untuk mengamanakan jalannya data. Sesi yang tercatat, adalah sebanyak 104 sesi. Pada percobaan yang dilakukan, tidak mendapatkan file yang ditransmisikan, *user id* maupun *password*. Seperti terlihat pada gambar 4.9 dibawah ini. Metode pengamanan yang digunakan oleh aplikasi yakni,

menggunakan koneksi TLS 1.2, dan data dienkripsi menggunakan AES dengan panjang kunci 128 bit. Kemudian, menggunakan *hash* SHA1. Sedangkan untuk pengamanan pertukaran kunci, menggunakan algoritma *public key* RSA dengan panjang kunci 2048 bit dapat dilihat pada gambar 4.10.



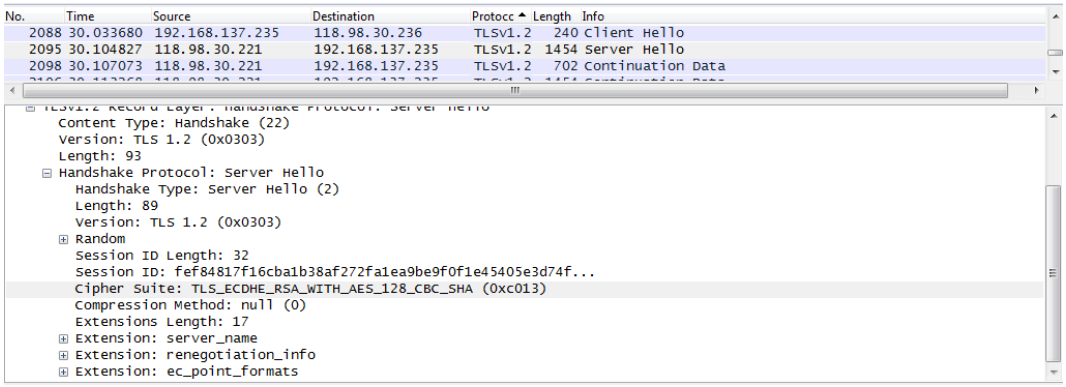
Gambar 4. 9 Tampilan pada tab files dari paket Google drive



Gambar 4. 10 Tampilan salah satu sertifikat dari Google drive

Sama seperti aplikasi iCloud. Dari semua sertifikat yang dikirimkan saat proses lalu lintas data pada Google drive berlangsung, kesemuanya menggunakan

metode yang sama. Dan juga dari detil paket *handshake* yang terdapat pada aplikasi *Wireshark* yang terdapat dalam gambar 4.11 dibawah ini.



Gambar 4. 11 Screenshot dari paket handshake Google drive

Berdasarkan hasil olah data yang dilakukan dari hasil penangkapan data pada aplikasi Google drive, dapat disimpulkan dalam bentuk tabel, seperti tabel 4.3 dan 4.4 berikut.

Tabel 4. 3 Checklist Google drive pada Wireshark

Wireshark				
Upload photo and video	Download Photo and video	upload documents and data	download documents and data	Shared file data
✕	✕	✕	✕	✕

*** :** √ (jika didapatkan hasil) dan ✕ (jika tidak didapatkan hasil sama sekali)

Tabel 4. 4 Checklist Google drive pada Network Miner

Network Miner				
Upload photo and video	Download Photo and video	upload documents and data	download documents and data	Shared file data
✕	✕	✕	✕	✕

*** :** √ (jika didapatkan hasil) dan ✕ (jika tidak didapatkan hasil sama sekali)

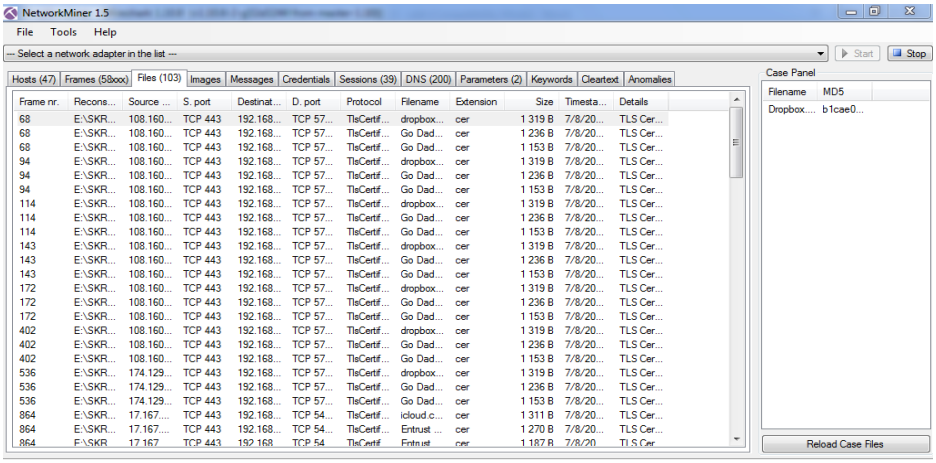
Pada tabel 4.3, *Upload, download photo or video*, kemudian *shared file data* merupakan fitur yang terdapat pada menu utama aplikasi Google drive. Dimana penguji melakukan proses *upload* data dari Apple device dan *download* data pada aplikasi yang terdapat di Google drive. Kemudian pada fitur *shared file data* dapat memperihatkan bahwa file yang telah dipilih dapat diakses oleh

pengguna googledrive lain yang dikehendaki dengan hak akses yaitu diperbolehkan untuk download file, lihat file, dapat memberi komentar, dan dapat edit file yang di share. Terlepas dari fitur yang diberikan tersebut Hak akses penuh dalam Google drive hanya dimiliki oleh pemilik account. Dari hasil yang didapat dari proses capture data mengggunakan wireshark, *Plaintext* maupun *ciphertext* tidak ada yang tertangkap. Begitupun juga dengan file foto, video maupun dokumen dan data, tidak satupun dapat tertangkap saat proses *capture* berlangsung. Hanya beberapa file notifikasi saja yang tertangkap oleh Wireshark dan Network miner.

Sesuai dari data sebelumnya, percobaan pada tabel 4.4 menggunakan Network miner bahwa di aplikasi Google drive pada saat proses upload dan download berlangsung, didapatkan *file* sertifikat.

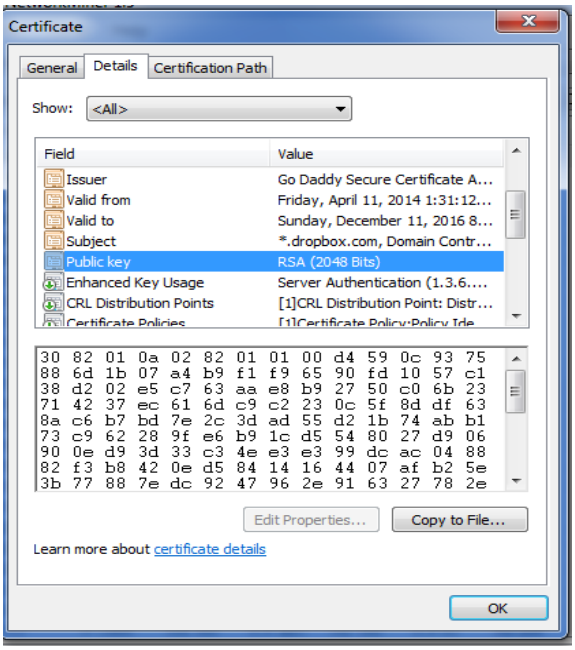
4.3.3 Dropbox

Selama proses penangkapan data, aplikasi Dropbox tercatat sebanyak 58295 *frame* paket yang ditransmisikan. Menggunakan Network Miner, *file* pcap yang ada lalu disusun ulang, sehingga menjadi lebih mudah untuk dibaca. Hasil yang didapatkan, yakni sebanyak 103 *file*, dan kesemua file tersebut adalah certificate. Sesi yang tercatat, adalah sebanyak 39 sesi. Pada percobaan yang dilakukan, tidak mendapatkan file yang ditransmisikan, *username* dan *password*, karena hampir semua file yang ditangkap dienkripsi. Berikut *screenshot* yang didapat dari aplikasi Network Miner mengenai *file-file* yang berhasil didapat pada aplikasi Dropbox. Seperti terlihat pada gambar 4.12 dibawah ini.

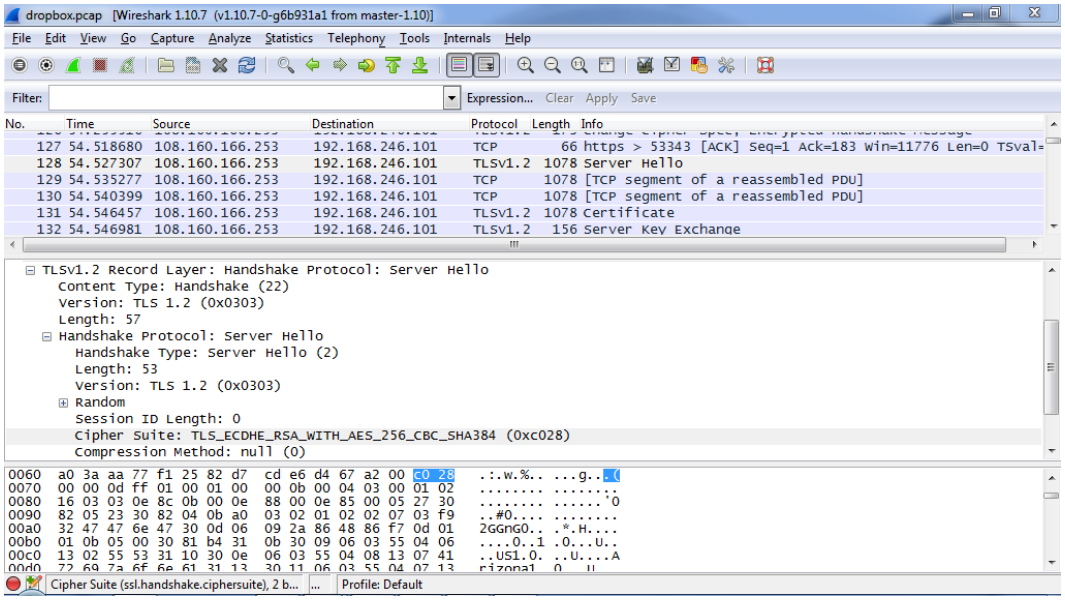


Gambar 4. 12 Tampilan pada tab files dari paket Dropbox

Untuk metode pengamanan yang digunakan oleh aplikasi Dropbox yaitu, menggunakan koneksi TLS 1.2, dan data dienkripsi menggunakan AES dengan panjang kunci 256 bit. Kemudian, menggunakan *hash* SHA. Sedangkan untuk pengamanan pertukaran kunci, menggunakan algoritma *public key* RSA dengan panjang kunci 2048 bit dapat dilihat pada gambar 4.13. Dari semua sertifikat yang dikirimkan saat proses lalu lintas data pada Dropbox berlangsung, kesemuanya menggunakan metode yang sama. Dan juga dari detil paket *handshake* yang terdapat pada aplikasi *Wireshark* yang terdapat dalam gambar 4.14 dibawah ini.



Gambar 4. 13 Tampilan salah satu sertifikat dari Dropbox



Gambar 4. 14 Screenshot dari paket handshake Dropbox

Berdasarkan hasil olah data yang dilakukan dari hasil penangkapan data pada aplikasi Dropbox, dapat disimpulkan dalam bentuk tabel, seperti tabel 4.5 berikut in

Tabel 4. 5 Checklist Dropbox pada Wireshark

Wireshark			
Upload photo and video	Download Photo and video	Upload documents and data	Download documents and data
✕	✕	✕	✕

*** :** √ (jika didapatkan hasil) dan ✕ (jika tidak didapatkan hasil sama sekali)

Tabel 4. 6 Checklist Dropbox pada Network Miner

Network Miner			
Upload photo and video	Download Photo and video	Upload documents and data	Download documents and data
✕	✕	✕	✕

*** :** √ (jika didapatkan hasil) dan ✕ (jika tidak didapatkan hasil sama sekali)

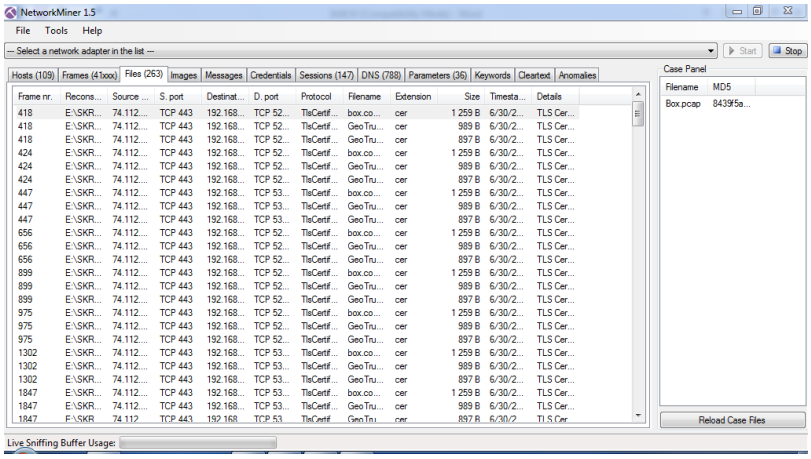
Kemudian pada tabel 4.5, pada waktu proses penangkapan data dengan Wireshark Photo upload dan download tidak mendapatkan file foto yang diupload maupun download. Sama seperti photo upload dan download, pada fitur documents dan data juga tidak didapatkan file apapun pada saat proses lalu lintas data berlangsung. Pada fitur camera upload terdapat pilihan turn on atau off

camera upload yang berfungsi sebagai pilihan untuk mengunggah seluruh file foto yang terdapat pada perangkat penguji yang tersinkron dengan dropbox. Fitur pilihan tersebut hampir sama dengan fitur yang ditawarkan oleh iCloud. Pada olah data yang diujikan, tidak terdapat satupun file yang didapat pada saat proses transfer data berlangsung.

Pada tabel 4.6 terlihat hasil yang didapat pada saat proses transfer data berlangsung, yang ditangkap oleh Network miner. Dari tabel tersebut tidak didapatkan file foto maupun document data yang di upload ataupun download. Hal tersebut menunjukkan bahwa proses penangkapan data dan olah data menggunakan tools Wireshark dan Network miner tidak mendapatkan hasil foto, video maupun document data yang di upload dan download terkecuali file sertifikat.

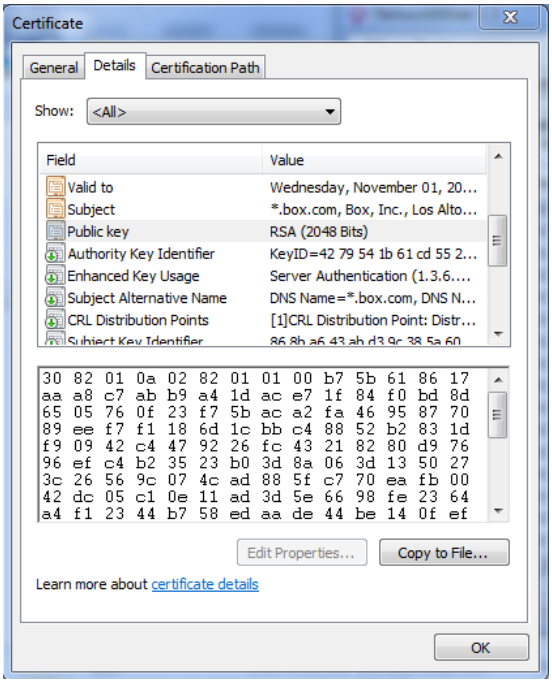
4.3.4 Box

Selama proses penangkapan data yang berjalan pada saat proses *upload* dan *download*, pada aplikasi Box tercatat sebanyak 39765 *frame* paket yang ditransmisikan. Menggunakan *Network Miner*, *file* pcap yang ada lalu disusun Checklist Dropbox pada Network Miner Checklist Dropbox pada Network Miner sebanyak 263 *file*, dan diantara paket yang ditangkap tersebut tidak satupun mendapatkan *file image* ataupun *text*. Hampir seluruh file yang tertangkap adalah TLS certificate. Untuk sesi yang tercatat, adalah sebanyak 147 sesi. Pada percobaan yang dilakukan, tidak mendapatkan *user id* maupun *password*. Seperti terlihat pada gambar 4.15 dibawah ini.

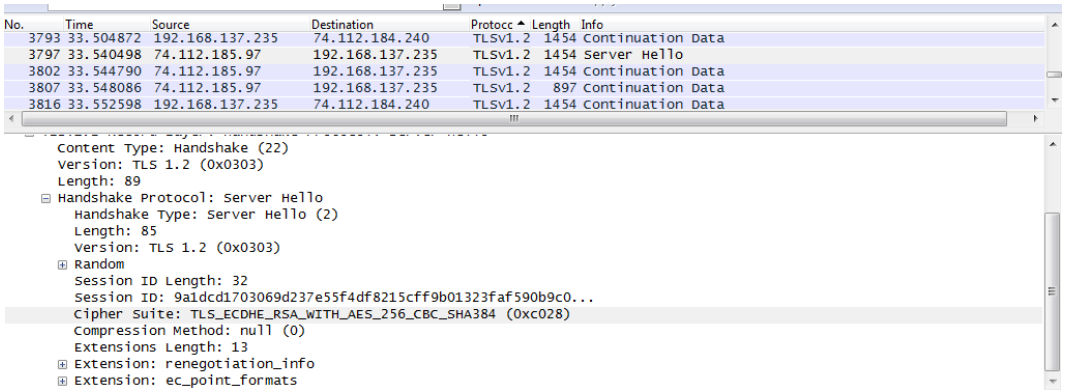


Gambar 4. 15 Tampilan pada tab files dari paket Box

Untuk metode pengamanan yang digunakan oleh aplikasi Box yaitu, menggunakan koneksi TLS 1.2, dan data dienkripsi menggunakan AES dengan panjang kunci 256 bit. Kemudian, menggunakan *hash* SHA. Sedangkan untuk pengamanan pertukaran kunci, menggunakan algoritma *public key* RSA dengan panjang kunci 2048 bit dapat dilihat pada gambar 4.16. Dari semua sertifikat yang dikirimkan saat proses lalu lintas data pada Dropbox berlangsung, kesemuanya menggunakan metode yang sama. Dan juga dari detil paket *handshake* yang terdapat pada aplikasi *Wireshark* yang terdapat dalam gambar 4.17 dibawah ini.



Gambar 4. 16 Tampilan salah satu sertifikat dari Box



Gambar 4. 17 Screenshot dari paket handshake Box

Berdasarkan hasil olah data yang dilakukan dari hasil penangkapan data pada aplikasi Box, dapat disimpulkan dalam bentuk tabel, seperti tabel 4.7berikut ini.

Tabel 4. 7 Checklist Box pada Wireshark

Wireshark			
Upload photo and video	Download Photo and video	Upload documents and data	Download documents and data
✕	✕	✕	✕

*** :** √ (jika didapatkan hasil) dan ✕ (jika tidak didapatkan hasil sama sekali)

Tabel 4. 8 Checklist Box pada Network Miner

Wireshark			
Upload photo and video	Download Photo and video	Upload documents and data	Download documents and data
✕	✕	✕	✕

* : √ **(**jika didapatkan hasil) dan ✕ (jika tidak didapatkan hasil sama sekali**)**

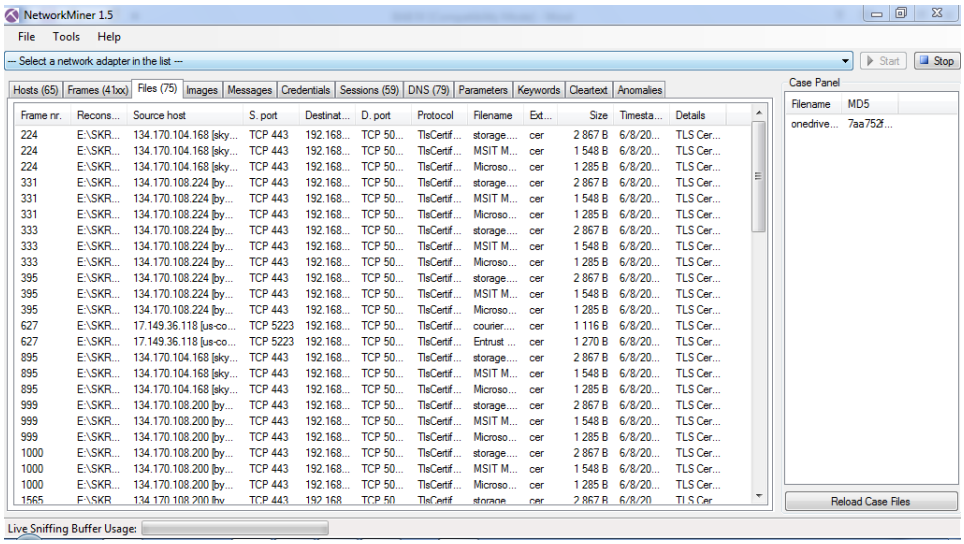
Pada tabel diatas saat proses *Photo or video upload dan download* berjalan aplikasi Wireshark tidak mendapatkan *file* foto maupun video yang ditransmisikan. Begitupun dengan fitur *documents* dan *data* juga tidak didapatkan *file apapun* pada saat proses lalu lintas data berlangsung. Berbeda dengan aplikasi Dropbox dan iCloud fitur *camera or video upload* pada aplikasi Box cenderung sama dengan Google drive, yaitu hanya memilih beberapa file foto ataupun video yang dikehendaki saja dari Apple device ke Cloud storage Box, untuk fitur *turn on* atau *off camera upload* yang berfungsi sebagai pilihan untuk mengunggah seluruh file foto seperti pada Dropbox atupun iCloud tidak ada pada aplikasi ini. Sedangkan untuk proses *upload, download documents* dan *data* pada aplikasi ini hampir sama dengan aplikasi-aplikasi yang diujikan sebelumnya. Pada olah data yang diujikan , tidak satupun file yang didapat ,terkecuali file *.cer* saat proses *transfer* data berlangsung.

Sama dengan hasil capture yang diperoleh oleh Wieshark, pada table 4.8 Network miner tidak didapatkan file foto. Video ataupun documents data pada saat proses upload dan download data berlangsung. Hal tersebut menunjukkan

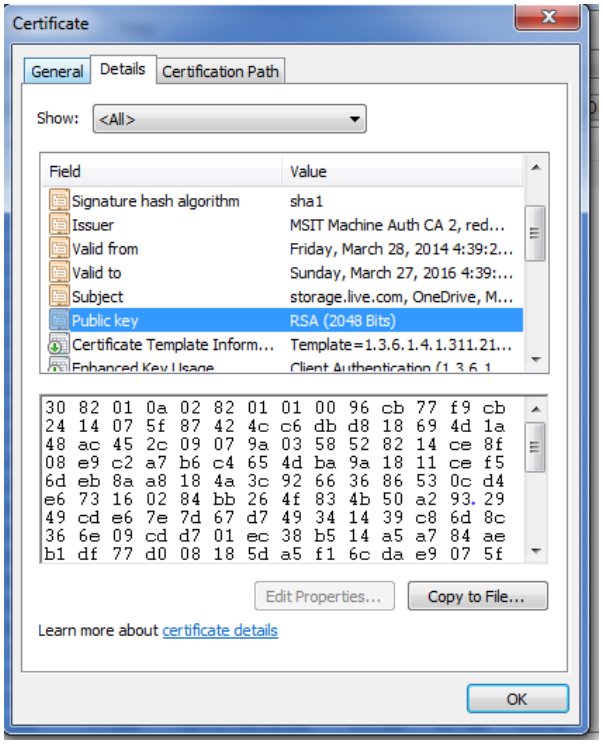
bahwa percobaan menggunakan Wireshark dan Network miner sama- sama tidak mendapatkan hasil, dan hanya memperoleh file .cer saja.

4.3.1 Skydrive(Onedrive)

Selama proses penangkapan data yang berjalan pada saat proses *upload* dan *download*, pada aplikasi Onedrive tercatat sebanyak 81204 *frame* paket yang ditransmisikan. Menggunakan *Network Miner*, *file* pcap yang ada lalu disusun ulang, sehingga menjadi lebih mudah untuk dibaca. Hasil yang didapatkan, yakni sebanyak 195 *file*, dan diantara paket yang ditangkap tersebut tidak satupun mendapatkan *file image* ataupun *text*. Hampir seluruh file yang tertangkap adalah TLS certificate. Untuk sesi yang tercatat, adalah sebanyak 80 sesi. Pada percobaan yang dilakukan, tidak mendapatkan *user id* maupun *password*. Seperti terlihat pada gambar 4. 18 dibawah ini.

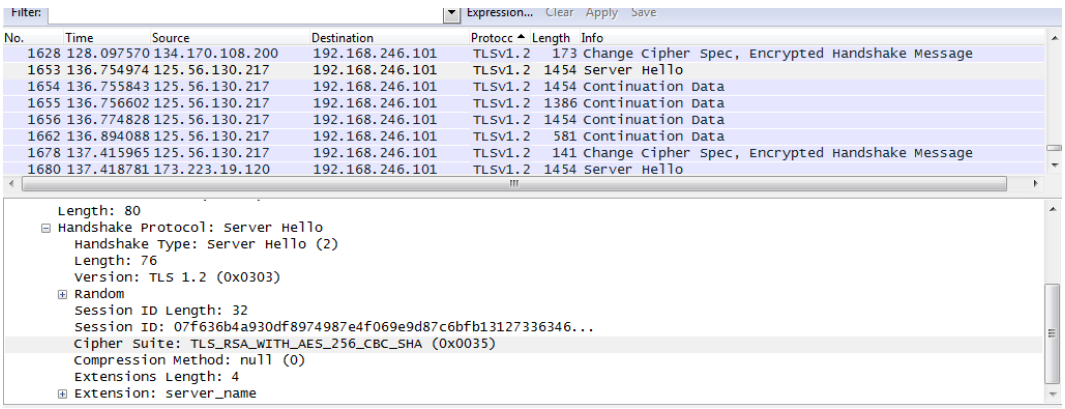


Gambar 4. 18 Tampilan pada tab files dari paket Skydrive (Onedrive)



Gambar 4. 19 Tampilan salah satu sertifikat dari Skydrive (Onedrive)

Untuk metode pengamanan yang digunakan oleh aplikasi Onedrive yaitu, menggunakan koneksi TLS 1.2, dan data dienkripsi menggunakan AES dengan panjang kunci 256 bit. Kemudian, menggunakan *hash* SHA. Sedangkan untuk pengamanan pertukaran kunci, menggunakan algoritma *public key* RSA dengan panjang kunci 2048 bit dapat dilihat pada gambar 4 .19 diatas. Dari semua sertifikat yang dikirimkan saat proses lalu lintas data berlangsung, kesemuanya menggunakan metode yang sama. Dan juga dari detil paket *handshake* yang terdapat pada aplikasi *Wireshark* yang terdapat dalam gambar 4 .20 dibawah ini.



Gambar 4. 20 Screenshot dari paket handshake Skydrive (Onedrive)

Tabel 4. 9 Checklist Skydrive (Onedrive) pada Wireshark

Wireshark			
Upload photo and video	Download Photo and video	Upload documents and data	Download documents and data
✗	✗	✗	✗

* : √ **(**jika didapatkan hasil) dan ✗ (jika tidak didapatkan hasil sama sekali**)**

Tabel 4. 10 Checklist Skydrive (Onedrive) pada Network Miner

Network Miner			
Upload photo and video	Download Photo and video	Upload documents and data	Download documents and data
✗	✗	✗	✗

* : √ **(**jika didapatkan hasil) dan ✗ (jika tidak didapatkan hasil sama sekali**)**

Dari tabel 4 .9 diatas dapat disimpulkan bahwa pada waktu proses penangkapan data *Photo upload dan download* tidak didapatkan *file* foto maupun video pada saat transfer data berjalan. Sama seperti *photo upload* dan *download*, pada fitur *documents* dan *data* juga tidak didapatkan *file apapun* pada saat proses lalu lintas data berlangsung. Pada menu pilihan utama terdapat fitur *camera backup* yang memungkinkan untuk pilihan *turn on* atau *off camera upload* yang berfungsi sebagai pilihan untuk mengunggah seluruh file foto yang terdapat pada *camera roll* di *apple device* dengan folder yang ada pada aplikasi Onedrive. Fitur pilihan tersebut hampir sama dengan fitur yang ditawarkan oleh iCloud dan Dropbox. Pada olah data yang diujikan , tidak terdapat satupun file yang didapat saat proses *transfer* data berlangsung.

Sama dengan hasil capture yang didapatkan oleh Wieshark, pada Network miner tidak didapatkan file foto, video ataupun documents data pada saat proses upload dan download data berlangsung. Hal tersebut menunjukkan bahwa percobaan menggunakan Wireshark dan Network miner sama- sama tidak mendapatkan hasil, dan hanya memperoleh file .cer saja.Secara umum, hasil dari semua Cloud storage yang dipercobakan, dapat disimpulkan dalam tabel 4.11 berikut ini

Tabel 4. 11 Tabel Perbandingan Seluruh Aplikasi Cloud storage

Fitur	iCloud	Googledrive	Dropbox	Box	Skydrive (Onedrive)
Upload Photo and video	×	×	×	×	×
Download Photo and video	×	×	×	×	×
Upload Document and data	×	×	×	×	×
Download Document and data	×	×	×	×	×

* : √ **(**jika didapatkan hasil) dan ✕ (jika tidak didapatkan hasil sama sekali**)**

4.4 Hasil Akhir

Setelah dilakukan pengambilan data, langkah selanjutnya adalah analisis terhadap seluruh paket data yang ditangkap berdasarkan data yang ditransmisikan oleh masing-masing aplikasi *Cloud Storage* yang diujikan. Dari proses penangkapan data hingga proses analisa paket data yang ditangkap menggunakan aplikasi Network Miner, didapakan hasil berupa kesimpulan-kesimpulan berikut ini.

4.4.1 Metode Pengamanan

Dari semua aplikasi Cloud storage yang digunakan sebagai bahan percobaan, ditemukan beberapa kesamaan dalam menggunakan metode pengamanan. Pada aplikasi Cloud storage yang diujikan tersebut mengamankan jalannya koneksi antara aplikasi terhadap *server* menggunakan TLS 1.2. Kemudian, algoritma yang digunakan untuk mengamankan pertukaran kunci yakni menggunakan kunci publik RSA dengan panjang kunci 2048 bit. Sementara, untuk enkripsi data yang digunakan masing-masing aplikasi hampir semuanya sama. iCloud, Dropbox, Box dan Onedrive menggunakan metode enkripsi simetrik AES dengan panjang kunci 256 bit. Sementara Google drive menggunakan metode Asimetrik AES dengan panjang kunci 128 bit. Untuk *hash method,* semua aplikasi Cloud Storage menggunakan SHA. Hal tersebut

ditemukan pada semua sertifikat yang dikumpulkan ketika proses pengujian berlangsung. Serta pada detil *frame handshake* yang terdapat pada aplikasi *Wireshark*.

4.4.2 Informasi yang didapatkan

Dari hasil percobaan yang sudah dilakukan, hampir seluruh file yang didapatkan dari Cloud Storage yang diujikan, hanya berupa certificate. Tidak satupun file yang ditransmisikan dapat ditangkap saat lalu lintas data berlangsung. Karena pada saat proses upload dan download berlangsung, data terlebih dahulu telah dienkripsi oleh service dari masing-masing cloud storage yang diujikan. Selain itu, dalam percobaan juga didapati banyak paket yang dikirimkan sudah menggunakan TLS 1.2, sehingga data yang dikirimkan tidak dapat dibaca dan ditelaah karena data tersebut dienkripsi. Hal ini juga menyulitkan ketika penguji harus melakukan dekripsi karena kunci untuk melakukan enkripsi data juga dienkripsi menggunakan enkripsi *Public Key*.

Berdasarkan penelitian yang telah dilakukan didapatkan hasil bahwa pada saat lalu lintas data berlangsung tidak didapat file apapun kecuali file.cer. Kemudian pada bab 2.6 sebelumnya telah dibahas tentang tiga skema enkripsi data yang digunakan saat proses data ditransmisikan baik dari perangkat penguji maupun sebaliknya. Dari ketiga skema tersebut masing-masing aplikasi Cloud Storage yang diujikan menggunakan skema enkripsi yang sama. *Encrypted connection* (SSL) digunakan oleh Dropbox semenjak perubahan privasi di Dropbox per tanggal 20 februari 2014, Dropbox dapat memberikan informasi / data dalam akun pengguna ke pihak yang berwenang jika dibutuhkan oleh pihak berwenang. Sama seperti Dropbox Google drive dari tanggal 31 Maret 2014 mengubah kebijakan privasinya, Box juga memberikan informasi / data dalam akun pengguna ke pihak yang berwenang jika dibutuhkan sejak tanggal 1 Agustus 2013. Sama halnya dengan aplikasi Cloud Storage sebelumnya pada iCloud dan Skydrive (Onedrive) juga memberi akses kepada pihak berwenang jika dibutuhkan oleh pihak berwenang.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari seluruh percobaan yang dilaksanakan penguji, didapatkan kesimpulan sebagai berikut:

1. Berdasarkan pada hasil uji coba pada proses penangkapan data dengan Aplikasi Wireshark dan Network Miner, sebagian besar data yang didapatkan terdiri dari informasi pengamanan yang digunakan oleh masing masing aplikasi cloud storage.
2. Pada percobaan yang telah dilakukan tidak diperoleh file apapun terkecuali file .certificate.
3. Jenis Metode Pengamanan yang digunakan pada aplikasi Cloud storage yang diujikan tersebut untuk mengamankan jalannya koneksi antara aplikasi terhadap *server* menggunakan TLS 1.2. Algoritma yang digunakan untuk mengamankan pertukaran kunci yakni menggunakan kunci publik RSA dengan panjang kunci 2048 bit. Untuk enkripsi data yang digunakan masing-masing aplikasi hampir semuanya sama. Pada aplikasi iCloud, Dropbox, Box dan Onedrive menggunakan metode enkripsi simetrik AES dengan panjang kunci 256 bit. Sementara untuk aplikasi Google drive menggunakan metode Simetrik AES dengan panjang kunci 128 bit. Untuk *hash method*, semua aplikasi Cloud Storage menggunakan SHA.

5.1 Saran

Berdasarkan hasil penelitian dan pengujian yang telah dilakukan oleh penulis, penulis memliki beberapa saran yang ingin disampaikan apabila nantinya ada yang ingin melakukan penelitian lebih mendalami mengenai judul ini. Adapun saran yang ingin diberikan adalah peneliti lainnya diharapkan dapat melakukan percobaan yang sama dengan menggunakan platform yang berbeda, misalnya saja pada Android dan Windows Mobile. Kemudian melakukan perbandingan tingkat keamanannya terhadap aplikasi yang ada pada masing-masing platform.

Kemudian diharapkan jika nantinya ada orang lain yang ingin melakukan penelitian pada platform yang berbeda, hendaknya mampu mendapatkan hasil yang lebih dengan acuan fitur yang sama dan juga mampu mendapatkan informasi mengenai jenis metode enkripsi yang digunakan oleh masing-masing aplikasi guna mengamankan data yang ditransmisikan. Selain itu diharapkan, peneliti selanjutnya dapat melakukan dekripsi terhadap data yang dienkripsi oleh aplikasi-aplikasi yang diteliti.

DAFTAR PUSTAKA

Ariyus, D. (2008). Yogyakarta: ANDI OFFSET (Penerbit ANDI).

Box.com. (2013, Agustus 1). Diambil kembali dari https://www.box.com/legal/privacypolicy/GB/

Dropbox.com. (2014, Februari 2014). Diambil kembali dari https://www.dropbox.com/id/privacy

Google.com. (2014, Maret 31). Diambil kembali dari https://www.google.com/intl/id/policies/privacy/

Harold F. Tipton. (2005). Information Security Management Handbook, Volume 2. United States of America.

Inc, A. (2014, Maret 1). Diambil kembali dari http://www.apple.com/legal/privacy/id/

Kurniawan, A. (2012). *Network Forensics menggunakan Wireshark.* Yogyakarta: Andi Offset.

Lacie. (2013). *Wuala - Technology - Secure Cloud Storage - Backup. Sync. Share. Access Everywhere.* Retrieved July 18, 2014, from http://www.wuala.com/en/learn/technology

Microsoft.com. (2014). Diambil kembali dari http://www.microsoft.com/security/online-privacy/onedrive.aspx

Quick, D., Martini, B., & Choo, R. (2013). *Cloud Storage Forensics* (Vol. 16, p. 208). Elsevier Science. Retrieved from http://books.google.com/books?id=_Q4rAQAAQBAJ&pgis=1

Quick, D. (2012). *Forensics Analysis of Cloud Storage Client Data.* Adelaide, Australia.

Trudy Muller, T. N. (2014, Januari 21). Dipetik Maret 14, 2014, dari http://www.apple.com/pr/library/2011/06/06Apple-Introduces-iCloud.html

Zulkifli Amsyah. (2005). *Manajemen Sistem Informasi* (kelima.). Jakarta: Gramedia Pustaka Utama. Retrieved from http://books.google.com/books?id

LAMPIRAN