

ANALISIS LALU LINTAS DATA PADA MEDIA SOSIAL BERBASIS SISTEM OPERASI IOS

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat Memperoleh Gelar Sarjana
Teknik Informatika



Nama : Abu Bakar Fuad Baridwan
NIM : 10523446

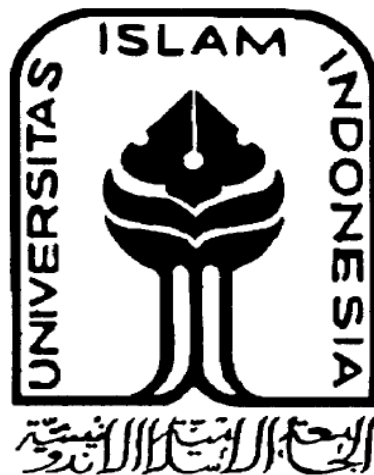
JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA

2014

ANALISIS LALU LINTAS DATA PADA MEDIA SOSIAL BERBASIS SISTEM OPERASI IOS

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat Memperoleh Gelar Sarjana
Teknik Informatika



Nama : Abu Bakar Fuad Baridwan
NIM : 10523446

**JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA**

2014

LEMBAR PENGESAHAN PEMBIMBING

**ANALISIS LALU LINTAS DATA PADA MEDIA
SOSIAL BERBASIS SISTEM OPERASI IOS**

TUGAS AKHIR

OLEH :

Nama : Abu Bakar Fuad Baridwan

NIM : 10523446

Yogyakarta, 14 Agustus 2014

Pembimbing



Ahmad Luthfi, S.Kom, M.Kom

LEMBAR PENGESAHAN PEMBIMBING**LEMBAR PENGESAHAN PENGUJI****ANALISIS LALU LINTAS DATA PADA MEDIA SOSIAL****BERBASIS SISTEM OPERASI iOS****TUGAS AKHIR****OLEH :****Nama : Abu Bakar****No. Mahasiswa : 10523446****Telah Dipertahankan di Depan Sidang Penguji sebagai Salah Satu Syarat****untuk Memperoleh Gelar Sarjana Jurusan Teknik Informatika****Fakultas Teknologi Industri Universitas Islam Indonesia****Yogyakarta, 14 Agustus 2014**

Tim Penguji,

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

Ketua

Ari Sujarwo, S.Kom., MIT: (Hons).

Anggota I

Taufiq Hidayat, S.T., 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 : Abu Bakar Fuad Baridwan

NIM : 10523446

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, 14 Agustus 2014

(Abu Bakar)

HALAMAN PERSEMBAHAN

Dengan mengucapkan syukur Alhamdulillah, kupersembahkan
tugas akhirku ini kepada :

Orang Tua tercinta

Dosen Pembimbing

Teman-teman FTI UII

HALAMAN MOTTO

"Maka bertaqwalah kamu kepada Allah menurut kesanggupanmu dan dengarlah serta taatlah dan nafkahkanlah nafkah yang baik untuk dirimu. Dan barangsiapa yang dipelihara dari kekikiran dirinya, maka mereka itulah orang-orang yang beruntung."

(At-Taghabun: 16)

"Always do your best. What you plant now, you will harvest later."

– Og Madino –

"You have to learn the rules of the game. And then you have to play better than anyone else."

– Albert Einstein –

"Selama kita masih hidup tidak ada hukuman; yang ada adalah peringatan agar kita memperbaiki diri."

– Mario Teguh –

KATA PENGANTAR



Assalamu'alaikum Wr. Wb.

Puji syukur kehadiran 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 Media Sosial Berbasis Sistem Operasi IOS”. 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 pengembangan. Namun, berkat bantuan, bimbingan, serta pengarahan dari pembimbing, 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 orang tua tercinta, segenap keluarga yang selalu memberikan dukungan, berupa moral maupun materil, serta doanya selama ini.
4. Kepada dosen pembimbing bapak Ahmad Luthfi, S.Kom, M.Kom, yang selalu membimbing dalam penyelesaian tugas akhir.
5. Serta ucapan terima kasih yang sebesar-besarnya kepada semua pihak yang tidak bisa penulis sebutkan namanya satu-persatu.

Saya menyadari bahwa laporan ini masih belum sempurna karena keterbatasan kemampuan dan pengalaman, oleh karena itu kritik dan saran saya harapkan sebagai bahan evaluasi dan pembelajaran agar dapat lebih baik dikemudian hari.

Besar harapan saya terhadap laporan Tugas Akhir yang telah saya selesaikan, semoga laporan ini dapat bermanfaat dan bisa menjadi wacana semua pihak.

Wassalamu'alaikum Wr Wb.

Yogyakarta, 14 Agustus 2014

Penulis

TAKARIR

<i>Username</i>	Nama Pengguna
<i>Password</i>	Kata Sandi
<i>Ciphertext</i>	Pesan yang sudah dienkripsi
<i>Message</i>	Pesan
<i>Public key</i>	Kunci public
<i>Hardware</i>	Perangkat Keras

ABSTRAK

Pesatnya perkembangan teknologi di zaman modern sekarang ini menyebabkan komunikasi sering kali dilakukan melalui dunia maya menggunakan *smartphone* yang di dalamnya dapat diinstal berbagai macam aplikasi media sosial. Kemudahan penggunaan dari fitur-fitur yang disediakan, ditambah dengan sifat ingin berbagi dan keinginan untuk mendapatkan reputasi adalah salah satu faktor media sosial banyak digunakan. Pengembang aplikasi media sosial sangatlah banyak, dengan berbedanya pengembang aplikasi media sosial pasti tingkat keamanan yang ada pada tiap aplikasi sosial media di iOS juga akan berbeda. Oleh karena itu perlu dilakukan pengamatan lalu lintas data pada aplikasi sosial media. Hal ini dilakukan untuk mengetahui tingkat keamanan media sosial dan para pengguna dapat mengetahui informasi apa saja yang bisa diambil dari lalu lintas data, agar para pengguna lebih berhati – hati dalam beraktifitas menggunakan media sosial supaya tidak menjadi korban kejahatan dunia maya. Dari pertimbangan tersebut maka memunculkan ide bagi penulis untuk meneliti lalu lintas data pada media sosial dengan menggunakan *network analyzer*. Penelitian dilakukan dengan melakukan *capture data*. Hasil yang didapat kemudian diteliti lebih lanjut mengenai informasi apa saja yang berhasil didapatkan

Kata kunci : Komunikasi, Smartphone, iOS, Network analyzer, Capture data

DAFTAR ISI

LEMBAR PENGESAHAN PEMBIMBING	ii
LEMBAR PENGESAHAN PENGUJI.....	ii
LEMBAR PERNYATAAN KEASLIAN	iv
HALAMAN PERSEMBAHAN	v
HALAMAN MOTTO	vi
KATA PENGANTAR.....	vii
TAKARIR.....	ix
ABSTRAK	x
DAFTAR ISI.....	xi
DAFTAR GAMBAR.....	xiii
DAFTAR TABEL	xiv
BAB I PENDAHULUAN.....	15
1.1 Latar Belakang.....	15
1.2 Rumusan Masalah	16
1.3 Batasan Masalah	16
1.4 Tujuan Penelitian.....	16
1.5 Manfaat Penelitian.....	16
1.6 Metode Penelitian.....	17
1.7 Sistematika Penulisan.....	17
BAB II LANDASAN TEORI	19
2.1 Lalu Lintas Data	19
2.2 Keamanan Data.....	19
2.3 Kriptologi.....	20
2.4 Enkripsi.....	21
2.5 Dekripsi.....	21
2.6 Media Sosial.....	22
BAB III METODOLOGI PENELITIAN	24
3.1 Studi Pustaka.....	24
3.2 Pengumpulan Data.....	24
3.2.1 Topologi.....	24

3.3	Pengolahan Data	25
3.4	Analisis Hasil Pengolahan Data	25
3.5	Kebutuhan Perangkat	26
3.5.1	Kebutuhan Perangkat Keras	26
3.5.2	Kebutuhan Perangkat Lunak	26
3.6	Flowchart	27
3.7	Hasil yang dikehendaki	28
BAB IV HASIL DAN PEMBAHASAN		29
4.1	Proses Penangkapan Lalu Lintas Data	29
4.1.1	iMessage	30
4.1.2	Wechat.....	31
4.1.3	Tango.....	32
4.1.4	Pinterest	34
4.1.5	Tumblr	36
4.2	Hasil Analisis Lalu Lintas Data	37
4.2.1	iMessage	37
4.2.2	Wechat.....	40
4.2.3	Tango.....	42
4.2.4	Pinterest	45
4.2.5	Tumblr	48
4.3	Hasil Akhir	51
4.3.1	Metode Pengamanan.....	51
4.3.2	Informasi yang Didapatkan	52
BAB V KESIMPULAN DAN SARAN		55
5.1	Kesimpulan.....	55
5.2	Saran	55
DAFTAR PUSTAKA.....		57
LAMPIRAN.....		58

DAFTAR GAMBAR

Gambar 2. 1 Ilustrasi Lalu Lintas Data	19
Gambar 3. 1 Topologi	24
Gambar 3. 2 Flowchart Proses Penangkapan Data	27
Gambar 4. 1 Proses Penangkapan Data.....	29
Gambar 4. 2 Tampilan iMessage	30
Gambar 4. 3 Tampilan Wechat	31
Gambar 4. 4 Tampilan Tango.....	33
Gambar 4. 5 Tampilan Pinterest	35
Gambar 4. 6 Tampilan Tumblr	36
Gambar 4. 7 Tampilan tab files iMessage.....	38
Gambar 4. 8 Tampilan sertifikat iMessage	39
Gambar 4. 9 Handshake Protocol iMessage	39
Gambar 4. 10 Tampilan tab files Wechat	40
Gambar 4. 11 Tampilan tab images Wechat	41
Gambar 4. 12 Handshake Protocol Wechat	41
Gambar 4. 13 Tampilan tab files Tango	42
Gambar 4. 14 Sertifikat Tango	43
Gambar 4. 15 Handshake protocol Tango.....	44
Gambar 4. 16 Tampilan tab images Tango	44
Gambar 4. 17 Tampilan tab files Pinterest.....	46
Gambar 4. 18 Sertifikat Pinterest.....	46
Gambar 4. 19 Handshake protocol Pinterest	47
Gambar 4. 20 Tampilan tab images Pinterest	47
Gambar 4. 21 Tampilan tab files Tumblr.....	49
Gambar 4. 22 Sertifikat Tumblr.....	49
Gambar 4. 23 Handshake protocol Tumblr	50
Gambar 4. 24 Tampilan tab images Tumblr	50
Gambar 4. 25 Grafik perbandingan aplikasi	53

DAFTAR TABEL

Tabel 3. 1 Tabel hasil pengolahan data.....	26
Tabel 4. 1 Tabel informasi iMessage	40
Tabel 4. 2 Tabel informasi Wechat.....	42
Tabel 4. 3 Tabel informasi Tango	45
Tabel 4. 4 Tabel informasi Pinterest	48
Tabel 4. 5 Tabel informasi Tumblr	51
Tabel 4. 6 Perbandingan hasil Tangkapan lalu lintas data.....	52

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pesatnya perkembangan teknologi di zaman modern sekarang ini menyebabkan komunikasi sering kali dilakukan melalui dunia maya dengan menggunakan media sosial yang tersedia pada perangkat gadget yang kita miliki. Media sosial adalah sebuah media online untuk para penggunanya agar bisa dengan mudah berpartisipasi, berbagi, berkomunikasi, dapat diakses dimana saja, kapan saja dan oleh siapa saja. Kemudahan penggunaan dari fitur-fitur yang disediakan, ditambah dengan sifat ingin berbagi dan keinginan untuk mendapatkan reputasi adalah salah satu faktor media sosial banyak digunakan.

iOS (sebelumnya iPhone OS) adalah sistem operasi yang dikembangkan dan didistribusikan oleh Apple Inc. Sistem operasi ini pertama diluncurkan tahun 2007 untuk iPhone dan iPod Touch, dan telah dikembangkan untuk mendukung perangkat Apple lainnya seperti iPad dan Apple TV. Tidak seperti Windows Phone (Windows CE) Microsoft dan Android Google, Apple tidak melisensikan iOS untuk diinstal di perangkat keras non-Apple. Interface untuk pengguna iOS didasarkan pada konsep manipulasi langsung menggunakan gerakan multisentuh. Elemen kontrol interface iOS meliputi slider, switch, dan tombol.

Setiap aplikasi pada iOS pasti dikembangkan oleh pengembang aplikasi yang berbeda. Para pengembang aplikasi pasti akan memikirkan tentang keamanan untuk para penggunanya, namun pasti ada perbedaan tingkat keamanan pada aplikasi yang tersedia untuk iOS. Dengan adanya tingkat keamanan yang berbeda-beda pada tiap aplikasi media sosial di iOS maka perlu dilakukan pengamatan lalu lintas data pada aplikasi media sosial agar dapat diketahui tingkat keamanannya dan juga para pengguna dapat mengetahui informasi apa saja yang bisa diambil dari lalu lintas data agar para pengguna lebih berhati-hati dalam beraktifitas menggunakan media sosial supaya tidak

menjadi korban kejahatan dunia maya. Pengamatan lalu lintas data dilakukan dengan menangkap paket - paket yang sedang ditransmisikan.

1.2 Rumusan Masalah

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

1. Bagaimana keamanan lalu lintas data pada aplikasi tersebut?
2. Informasi apa saja yang bisa didapat ketika lalu lintas data tersebut terjadi?
3. Apa metode enkripsi yang digunakan?

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 berjalan pada sistem operasi iOS 7.
3. Aplikasi media sosial yang akan dianalisis adalah:
 - a. iMessaging
 - b. Tango
 - c. Wechat
 - d. Pinterest
 - e. Tumblr

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk mengetahui sejauh mana keamanan yang ditawarkan pada media sosial berbasis sistem operasi iOS.

1.5 Manfaat Penelitian

Dengan mengadakan penelitian ini, manfaat yang ingin didapatkan adalah:

1. Mengetahui sejauh mana keamanan lalu lintas data dari media sosial berbasis sistem operasi iOS.
2. Dengan diperolehnya hasil analisis, diharapkan dapat menambah kesadaran keamanan para pengguna berbasis sistem operasi iOS.

1.6 Metode Penelitian

1.6.1 Studi Literatur

Studi literatur digunakan untuk menggali informasi yang terkait 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 pada dilakukan dengan melakukan percobaan langsung pada aplikasi media sosial berbasis sistem operasi iOS. Percobaan yang akan dilakukan adalah menangkap lalu lintas data atau paket yang lewat dari aplikasi media sosial menggunakan aplikasi *wireshark*.

1.6.3 Analisis Data

Analisis data dilakukan dengan menelaah metode-metode pengamanan yang dilakukan berdasarkan paket 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 aplikasi media sosial berbasis sistem operasi iOS.

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 berlangsungnya percobaan, terutama dalam masa pembangunan sistem untuk ujicoba, serta melakukan ujicoba dan analisisnya.

BAB V Penutup

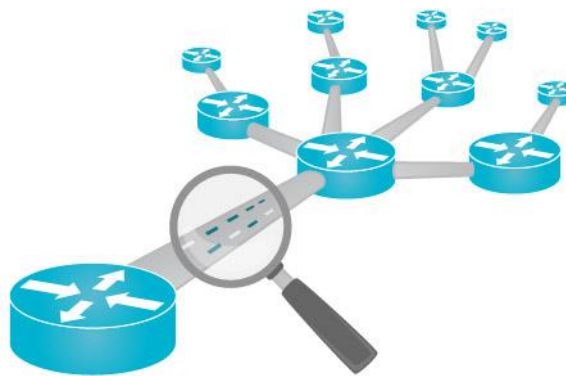
Menyajikan kesimpulan dari seluruh proses analisis, dan ujicoba, saran–saran yang perlu dikaji, berdasarkan jalannya ujicoba, dan kelebihan maupun keterbatasan yang ditemukan selama proses ujicoba berlangsung.

BAB II

LANDASAN TEORI

2.1 Lalu Lintas Data

Menurut UU No. 22 tahun 2009 lalu lintas didefinisikan sebagai gerak kendaraan dan orang di ruang lalu lintas jalan. Lalu lintas data sendiri dapat digambarkan seperti gerak atau perpindahan data yang terjadi di dalam jaringan, data yang bergerak di jaringan ditransmisikan dengan sangat cepat dan tidak kasat mata. Ketika terjadi komunikasi data yang ditransmisikan biasanya dipecah menjadi paket-paket tertentu.



Gambar 2. 1 Ilustrasi Lalu Lintas Data (Inveatech, 2008).

2.2 Keamanan Data

Keamanan data dalam komunikasi di sebuah jaringan merupakan hal penting, setiap orang selalu ingin mendapatkan informasi yang diinginkan baik dengan cara legal maupun cara tidak legal. Banyak cara yang digunakan oleh orang untuk berusaha mendapat informasi dari data tersebut. Bisa saja informasi data yang dikirimkan disalahgunakan oleh orang yang tidak bertanggung jawab. Apalagi dengan semakin berkembangnya teknologi pada saat ini, komunikasi dapat dilakukan dengan mudah serta dapat dilakukan dimana saja, kapan saja selama terhubung jaringan *Internet*.

Namun dengan kemudahan tersebut dapat menimbulkan masalah terkait dengan keamanan data. Maka dari itu tujuan dari pengamanan data yaitu untuk meningkatkan

keamanan dari data-data yang ditransmisikan dan juga memiliki fungsi untuk melindungi data agar tidak dapat dibaca oleh orang-orang yang tidak berhak menyisipkan atau menghapus data (Kristanto, 2003).

Secara garis besarnya masalah keamanan dibagi menjadi 4 bagian yang saling berhubungan, yaitu :

- a. Kerahasiaan
- b. Keaslian
- c. Pengakuan
- d. Kontrol integritas.

Segi-segi keamanan sendiri dapat didefinisikan menjadi lima, yaitu:

- a. *Confidentiality*, mensyaratkan bahwa informasi (data) hanya bisa diakses oleh pihak yang memiliki wewenang.
- b. *Integrity*, mensyaratkan bahwa informasi hanya dapat diubah oleh pihak yang memiliki wewenang.
- c. *Availability*, mensyaratkan bahwa informasi tersedia untuk pihak yang memiliki wewenang ketika dibutuhkan.
- d. *Authentication*, mensyaratkan bahwa pengirim suatu informasi dapat diidentifikasi dengan benar dan ada jaminan bahwa identitas yang didapat tidak palsu.
- e. *Nonrepudiation*, mensyaratkan bahwa baik pengirim maupun penerima informasi tidak dapat menyangkal pengiriman dan penerimaan pesan.

(Permana, 2013).

2.3 Kriptologi

Kriptologi adalah gabungan dari ilmu kriptografi dan analisis sandi. Kriptografi merupakan teknik untuk mengamankan data dari sisi kerahasiaan, ahlinya disebut *cryptographer*. *Cryptanalysis* adalah suatu ilmu dan seni membuka *ciphertext* dan orang yang melakukannya disebut *cryptanalyst*. Cabang matematika yang mencakup kriptografi dan *cryptanalysis* disebut *cryptology* (kriptologi) dan pelakunya disebut *cryptologists* (Kurniawan Y. , 2004).

2.4 Enkripsi

Enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. atau bisa didefinisikan juga Enkripsi merupakan proses untuk mengubah plainteks menjadi chiperteks. *Plainteks* adalah data atau pesan asli yang ingin dikirim, sedangkan Chiperteks adalah data hasil enkripsi. Enkripsi dapat diartikan sebagai kode atau chiper.

Enkripsi berguna untuk melindungi informasi agar tidak terlihat oleh orang lain atau pihak yang tidak berhak. Informasi ini dapat berupa nomor kartu kredit, catatan penting dalam komputer, maupun *username* dan *password* untuk mengakses sesuatu.

Enkripsi sendiri terbagi menjadi dua macam, yaitu:

a. Simetrik

Enkripsi ini menggunakan kunci atau key yang sama untuk melakukan enkripsi dan dekripsi. Enkripsi simetrik memiliki tingkat kecepatan operasi yang lebih tinggi dibandingkan dengan asimetrik, sehingga enkripsi simetrik dapat digunakan pada sistem real-time.

b. Asimetrik

Enkripsi ini menggunakan kunci atau key yang berbeda untuk melakukan enkripsi dan dekripsi. Satu key digunakan untuk enkripsi dan satu lagi digunakan untuk dekripsi. Enkripsi asimetrik tidak memerlukan key yang banyak, cukup dengan menggunakan *public key*.

2.5 Dekripsi

Dekripsi dalam dunia keamanan komputer merupakan proses untuk mengubah *chiperteks* menjadi *plainteks* atau pesan asli. Jadi dekripsi merupakan kebalikan dari enkripsi upaya pengolahan data menjadi sesuatu yang dapat diutarakan secara jelas dan tepat dengan tujuan agar dapat dimengerti oleh orang yang tidak langsung mengalaminya sendiri.

2.6 Media Sosial

Media sosial adalah sebuah media online, dimana para penggunanya bisa dengan mudah berpartisipasi, berbagi, dan menciptakan isi meliputi blog, jejaring sosial, forum dan dunia maya. Sedangkan menurut Andreas Kaplan dan Michael Haenlein mendefinisikan media sosial sebagai "sebuah kelompok aplikasi berbasis internet yang dibangun di atas dasar ideologi dan teknologi Web 2.0 , dan yang memungkinkan terjadinya penciptaan dan pertukaran user-generated content” (Sanusi, 2013) .

Banyak sekali macam-macam aplikasi media sosial yang beredar, ada pun aplikasi media sosial yang akan di teliti adalah:

1. iMessage

iMessage adalah layanan Apple yang memungkinkan mengirim pesan tak terbatas melalui koneksi Wi-Fi atau data seluler ke perangkat iOS lainnya menggunakan iOS 5 atau versi lebih baru. Dengan iMessage, dapat melihat kapan pengguna mengetik dan memberi tahu pengguna kapan pesan tersebut dibaca. iMessage ditampilkan di semua perangkat iOS yang masuk ke akun yang sama, sehingga anda dapat memulai percakapan di salah satu perangkat, dan melanjutkannya di perangkat lain.

Keunggulan yang diberikan oleh aplikasi ini diantaranya adalah:

- a. Dapat berkirim pesan secara mudah kepada pengguna iphone lain
- b. Dapat melakukan pemblokiran pesan pada iOS 7
- c. Dapat mengirim pesan grup

2. Wechat

Wechat adalah salah satu layanan komunikasi pesan teks dan juga suara yang dikembangkan oleh Tencent di China yang diperkenalkan pada januari 2011. Wechat juga mendukung Bahasa Indonesia sehingga lebih mudah digunakan oleh orang yang tidak bisa bahasa asing.

Keunggulan yang diberikan oleh aplikasi ini diantaranya adalah:

- a. Dapat berbagi *moments* berupa foto maupun teks.

- b. Dapat menambah teman dengan fitur *Look Around*, mencari pengguna Wechat yang berada disekitar.

3. Tango

Tango adalah aplikasi pihak ketiga yang berguna untuk berkirim pesan dan melakukan video call yang dikembangkan oleh TangoME pada September 2009. Menurut PCMag, Tango merupakan aplikasi chat sederhana dengan rentang dukungan yang baik.

Keunggulan yang diberikan oleh aplikasi ini diantaranya adalah:

- a. Dapat melakukan *video call* dan *voice call* secara gratis
- b. Dapat berbagi foto dan bermain game.

4. Pinterest

Pinterest merupakan media sosial yang memungkinkan penggunanya untuk berbagi gambar kepada pengguna lain yang bisa dimasukkan dalam kategori tertentu. Pinterest mulai dikembangkan pada Desember 2009 dan kemudian diluncurkan pada Maret 2010 dengan status close beta.

Keunggulan yang diberikan oleh aplikasi ini diantaranya adalah:

- a. Foto dapat dikategorikan sesuai keinginan
- b. Pencarian foto mudah karena sudah sesuai kategori.

5. Tumblr

Tumblr merupakan microblogging dan sosial networking yang didirikan oleh David Karp dan dimiliki oleh Yahoo!. Tumblr memungkinkan penggunanya untuk mengirim konten multimedia dan konten lain dalam bentuk singkat. Tumblr pertama dirilis untuk Iphone pada tahun 2009, kemudian pada 2012 tumblr merilis Tumblr 3.0 yang memungkinkan gambar dengan resolusi tinggi dan juga akses offline.

Keunggulan yang diberikan oleh aplikasi ini diantaranya adalah:

- a. Pengguna dapat mengikuti pengguna lain.
- b. Memungkinkan gambar dengan resolusi tinggi.

BAB III

METODOLOGI PENELITIAN

3.1 Studi Pustaka

Studi pustaka dilakukan untuk memahami bagaimana jalannya aplikasi-aplikasi pendukung yang akan menunjang penelitian. Seperti memahami cara kerja Wireshark, sebagai aplikasi yang digunakan untuk menangkap paket data dari aplikasi media sosial dijalankan. Memahami juga macam – macam fitur yang dimiliki oleh aplikasi media sosial yang akan diteliti.

3.2 Pengumpulan Data

Pengumpulan lalu lintas data pada penelitian ini dilakukan dengan cara menghubungkan koneksi perangkat ipod / iphone ke laptop yang dijadikan *access point*, kemudian data ditangkap dengan menggunakan Wireshark pada laptop. Setelah semua data didapatkan akan dilakukan filter terhadap paket-paket yang diterima agar lebih mudah dalam meneliti paket data tersebut.

Untuk melakukan penangkapan paket data yang sedang ditransmisikan, dapat dilakukan dengan topologi sebagai berikut:

3.2.1 Topologi

Topologi yang digunakan adalah dengan menggunakan Wireshark di laptop yang disetting sebagai *access point* (AP). Kemudian Ipod/Iphone dihubungkan ke laptop agar bisa terhubung ke Internet, sehingga Wireshark dapat menangkap paket-paket yang sedang ditransmisikan oleh Ipod/Iphone tersebut.



Gambar 3. 1 Topologi

Dengan menggunakan topologi ini dalam percobaan, keuntungan yang didapat adalah kemudahan dalam mendapat hasil paket data yang ditangkap karena hanya device yang terhubung ke laptop yang paket data nya ditangkap. Tetapi dengan menggunakan topologi ini sedikit merepotkan, karena perlu melakukan konfigurasi di laptop terlebih dahulu, dan juga apabila menggunakan *Hosted Network*,. *Hosted network* merupakan fitur yang dimiliki windows 7 yang memungkinkan laptop digunakan sebagai AP, tidak semua laptop dapat mendukung, karena beberapa laptop model lama tidak mendukung *Hosted Network* dari segi *hardware*.

3.3 Pengolahan Data

Setelah semua data dari media sosial yang akan diteliti berhasil didapatkan dari proses pengumpulan data, langkah selanjutnya adalah melakukan pengolahan data dari media sosial 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.

Analisis data dilakukan dengan meneliti metode-metode pengamanan yang dilakukan berdasarkan 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.

3.4 Presentasi Hasil Pengolahan Data

Pada tahap penyajian hasil pengolahan data, data dari pengolahan paket data yang didapat dari lalu lintas jaringan lah yang akan disajikan. Hasil juga akan disajikan dalam bentuk tabel-tabel yang berisi daftar data/file hasil temuan selama dilakukan percobaan.

Tabel 3. 1 Tabel hasil pengolahan data

Aplikasi	Hosts	Frame	Files	Images	Messages	Sessions
iMessaging	√	√	√	×	×	√
Wechat	√	√	√	√	×	√
Tango	√	√	√	√	×	√
Pinterest	√	√	√	√	×	√
Tumblr	√	√	√	√	×	√

√ (jika didapatkan hasil) dan × (jika tidak didapatkan hasil)

3.5 Kebutuhan Perangkat

3.5.1 Kebutuhan Perangkat Keras

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

a. Gadget iOS

Gadget yang digunakan untuk melakukan percobaan adalah Ipod Touch 5 dan Iphone 4. Kedua gadget yang digunakan sudah menggunakan iOS 7 resmi, karena tidak perlu melakukan *jailbreak* agar paket data dapat ditangkap.

b. Laptop

Laptop yang digunakan untuk percobaan adalah Asus N43. Laptop sudah terinstal Wireshark, Network Miner dan juga dilakukan setting sebagai *Hosted Network*.

3.5.2 Kebutuhan Perangkat Lunak

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

a. WireShark

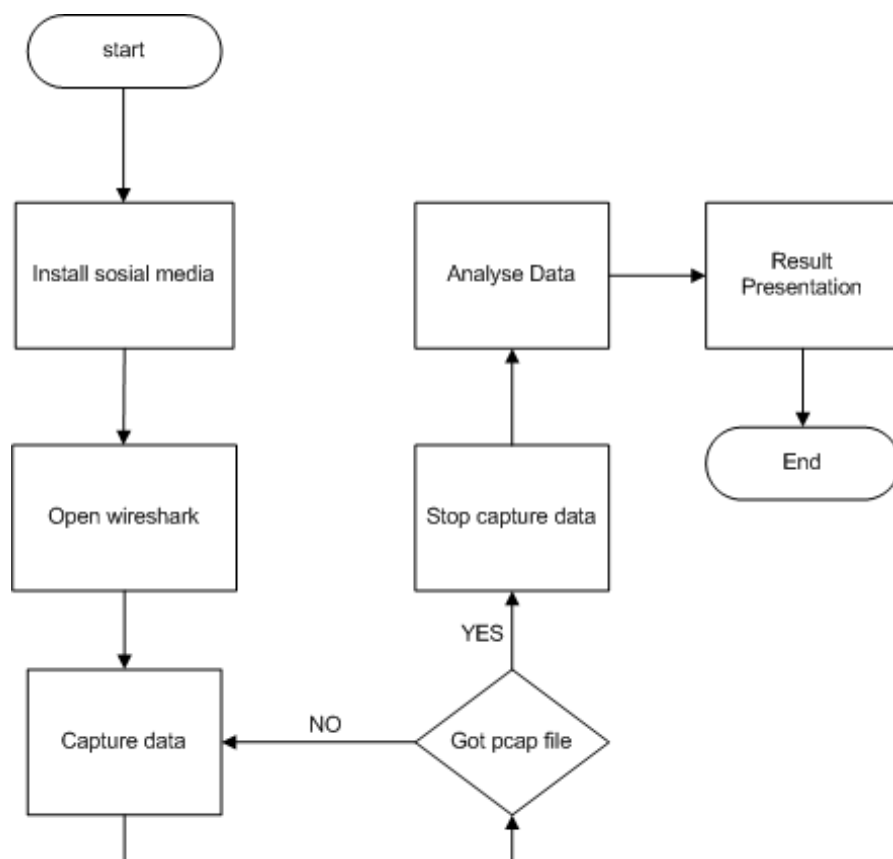
Wireshark merupakan salah satu aplikasi *Network Analyzer* terbaik yang bisa dijalankan pada berbagai macam OS dan memiliki fitur yang lengkap dalam menangkap maupun menganalisa paket data. Wireshark juga termasuk aplikasi *opensource*.

b. Network Miner

Network miner merupakan *Network Forensic Analysis Tool* (NFAT), fitur yang dimiliki network miner diantaranya adalah *network forensics*, *network sniffing*, dan *pcap parser*. Fitur *pcap parser* berguna untuk menggabungkan file dan sertifikat yang ada pada saat proses lalu lintas data terjadi, fitur ini juga bisa menggabungkan dan menyimpan file media seperti image, audio dan video. File yang bisa didapatkan adalah file yang ada pada protokol FTP, TFTP, HTTP, SMB dan SMTP (Netresec, 2010). Hal ini sangat memudahkan dalam penelitian dan pelaksanaan percobaan.

3.6 Flowchart

Berikut merupakan diagram alur yang dibuat untuk membantu melaksanakan percobaan.



Gambar 3. 2 Flowchart Proses Penangkapan Data

3.7 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 menangkap paket-paket data dari masing-masing komunikasi yang dilakukan antara aplikasi media sosial dengan server.
- b. Dapat mengetahui jenis metode pengamanan apa saja yang digunakan oleh masing-masing media sosial.
- c. Mampu mendapatkan data ataupun file yang ditransmisikan ketika terjadi komunikasi antara pengguna media sosial.

BAB IV

HASIL DAN PEMBAHASAN

Pada bab ini, merupakan tahap percobaan yang dilakukan penguji untuk mengimplementasikan penelitian.

4.1 Proses Penangkapan Lalu Lintas Data

Proses penangkapan paket data dilakukan dengan menjadikan laptop Asus N43 yang terhubung ke internet menjadi *access point* (AP), kemudian hubungkan Apple device yang digunakan pada percobaan ke AP yang sudah dibuat. Dalam percobaan ini penguji menggunakan ipod dan iphone, setelah Ipod dan Iphone terhubung maka dilakukan proses penangkapan lalu lintas data dengan menggunakan Wireshark yang dijalankan di laptop Asus N43. Proses penangkapan data sendiri dibatasi hanya dengan mencoba fitur-fitur yang ada pada aplikasi media sosial yang akan diteliti.

No.	Time	Source	Destination	Protocol	Length	Info
1244	69.610259	119.31.253.197	192.168.253.101	TCP	1506	[TCP segment of a reassembled PDU]
1245	69.610344	119.31.253.197	192.168.253.101	TCP	1506	[TCP segment of a reassembled PDU]
1246	69.610375	119.31.253.197	192.168.253.101	TCP	1506	[TCP segment of a reassembled PDU]
1247	69.610399	119.31.253.197	192.168.253.101	TCP	1506	[TCP segment of a reassembled PDU]
1248	69.613100	119.31.253.197	192.168.253.101	TCP	674	[TCP segment of a reassembled PDU]
1249	69.613153	119.31.253.197	192.168.253.101	TCP	674	[TCP segment of a reassembled PDU]
1250	69.613220	119.31.253.197	192.168.253.101	TCP	674	[TCP segment of a reassembled PDU]
1251	69.613243	119.31.253.197	192.168.253.101	TCP	674	[TCP segment of a reassembled PDU]
1252	69.615344	119.31.253.197	192.168.253.101	HTTP	440	HTTP/1.1 200 OK (GPEG JPEG image)
1253	69.615359	119.31.253.197	192.168.253.101	TCP	440	[TCP segment of a reassembled PDU]
1254	69.615423	119.31.253.197	192.168.253.101	TCP	440	[TCP segment of a reassembled PDU]
1255	69.615444	119.31.253.197	192.168.253.101	TCP	440	[TCP segment of a reassembled PDU]
1256	69.620043	119.31.253.197	192.168.253.101	TCP	417	[TCP segment of a reassembled PDU]
1257	69.620098	119.31.253.197	192.168.253.101	TCP	417	[TCP segment of a reassembled PDU]
1258	69.620124	119.31.253.197	192.168.253.101	TCP	417	[TCP segment of a reassembled PDU]
1259	69.620146	119.31.253.197	192.168.253.101	TCP	417	[TCP segment of a reassembled PDU]
1260	69.628470	119.31.253.197	192.168.253.101	TCP	1506	[TCP segment of a reassembled PDU]

Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
Ethernet II, Src: 72:2f:68:56:aa:f5 (72:2f:68:56:aa:f5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.253.1 (192.168.253.1), Dst: 192.168.253.255 (192.168.253.255)

```
0000 ff ff ff ff ff ff 72 2f 68 56 aa f5 08 00 45 00 .....P/hv....E.
0010 00 4e 04 eb 00 00 80 11 b9 61 c0 a8 fd 01 c0 88 ..N.....a.....
0020 fd ff 00 89 00 89 00 3a 96 1a a4 87 01 10 00 01 .....E JFDFBEE
0030 00 00 00 00 00 00 20 45 4a 46 44 45 42 46 45 45 .....E JFDFBEE
0040 42 46 41 43 41 43 41 43 41 43 41 43 41 43 41 43 BFACACAC ACACAC
0050 41 43 41 43 41 41 41 00 00 20 00 01 ACACAAA...
```

Gambar 4. 1 Proses Penangkapan Data

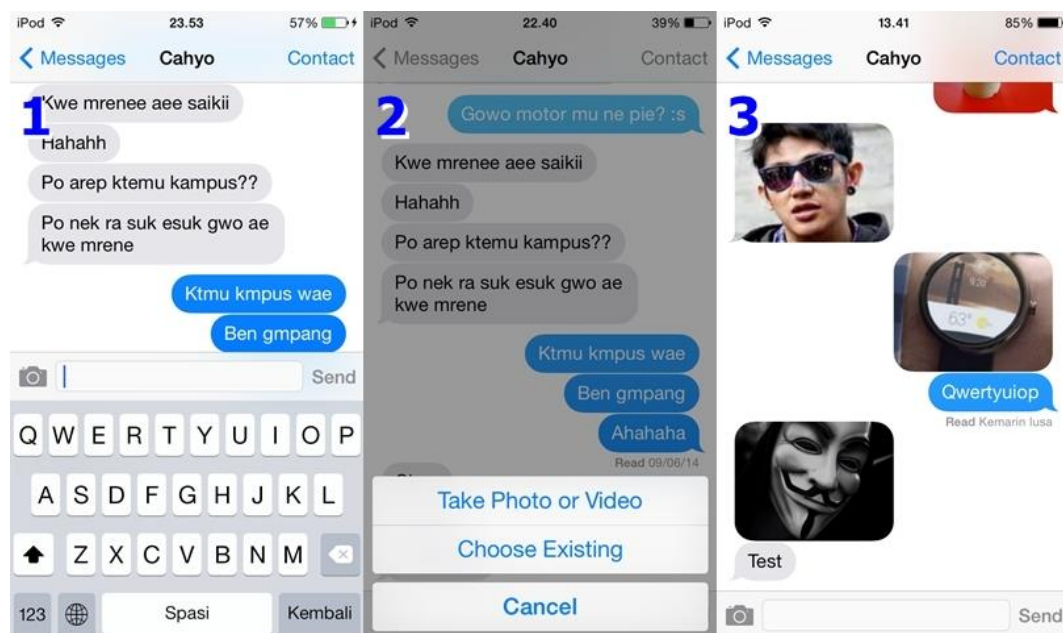
Pada gambar 4.1 merupakan contoh dari proses penangkapan lalu lintas data dari ipod atau iphone yang ditangkap melalui wireshark. Pada proses penangkapan data tidak dibatasi waktu penangkapannya, namun semakin lama ukuran file pcap yang berisi

tangkapan data akan semakin membesar. Berikut akan dijabarkan proses penangkapan data pada tiap aplikasi yang digunakan.

4.1.1 iMessage

Aplikasi pertama yang dijadikan bahan percobaan proses penangkapan data adalah iMessage yang merupakan aplikasi bawaan dari iOS. Aplikasi ini tergabung menjadi satu dengan aplikasi *message* pada ios, namun imessage mengirim pesan dengan menggunakan paket data atau wifi dan juga ada perbedaan visual pada pesan yang dikirim antara sms dan iMessage. Kolom input pesan akan bertuliskan iMessage, tombol send berwarna biru, balon teks juga berwarna biru ketika dalam mode iMessage. Berbeda dengan sms yang tombol send dan balon teks nya berwarna hijau.

Setelah wireshark di laptop jalankan, buka aplikasi message pada ipod atau iphone. Fitur dari imessage yang akan dicoba untuk dilakukan penangkapan datanya adalah berkirim pesan teks dan mengirim gambar ke user imessage lain.



Gambar 4. 2 Tampilan iMessage

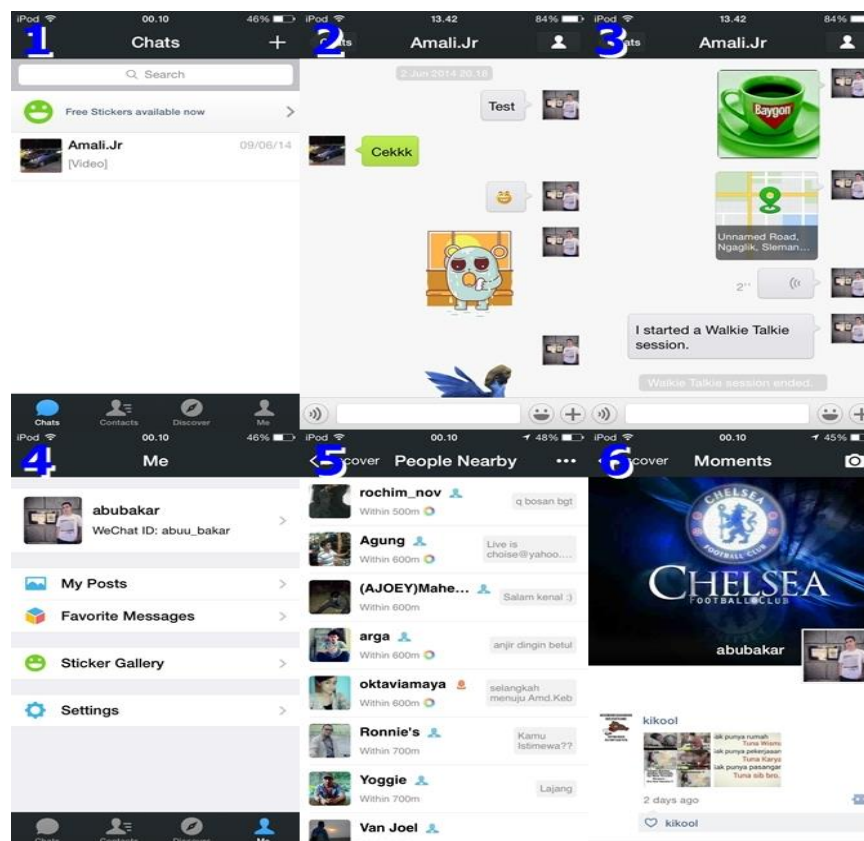
Pada gambar 4.2 (nomor 1) merupakan tampilan dari message pada iOS 7 ketika berkirim pesan, untuk yang dengan bubble box berwarna biru menandakan bahwa pesan

yang dikirim merupakan iMessage yang hanya bisa diterima oleh pengguna iMessage lainnya. Selanjutnya, pada gambar 4.2 (nomor 2) merupakan tampilan dari iMessage ketika akan mencoba melakukan pengiriman pesan berupa gambar atau video, baik dari gallery atau melakukan pengambilan foto dan video secara langsung.

Setelah memilih atau mengambil gambar yang akan dikirim menggunakan iMessage dan mengirimkannya ke pengguna iMessage lain maka tampilan dari gambar yang dikirim akan terlihat pada message box seperti pada gambar 4.2 (nomor 3).

4.1.2 Wechat

Aplikasi kedua yang dijadikan bahan percobaan proses pengungkapan data adalah Wechat. Pada aplikasi ini berbeda dengan iMessage, Fitur yang dijadikan bahan percobaan lebih banyak seperti mengirim pesan, mengirim gambar, mengirim stiker, *update moment*, dan *people nearby*.



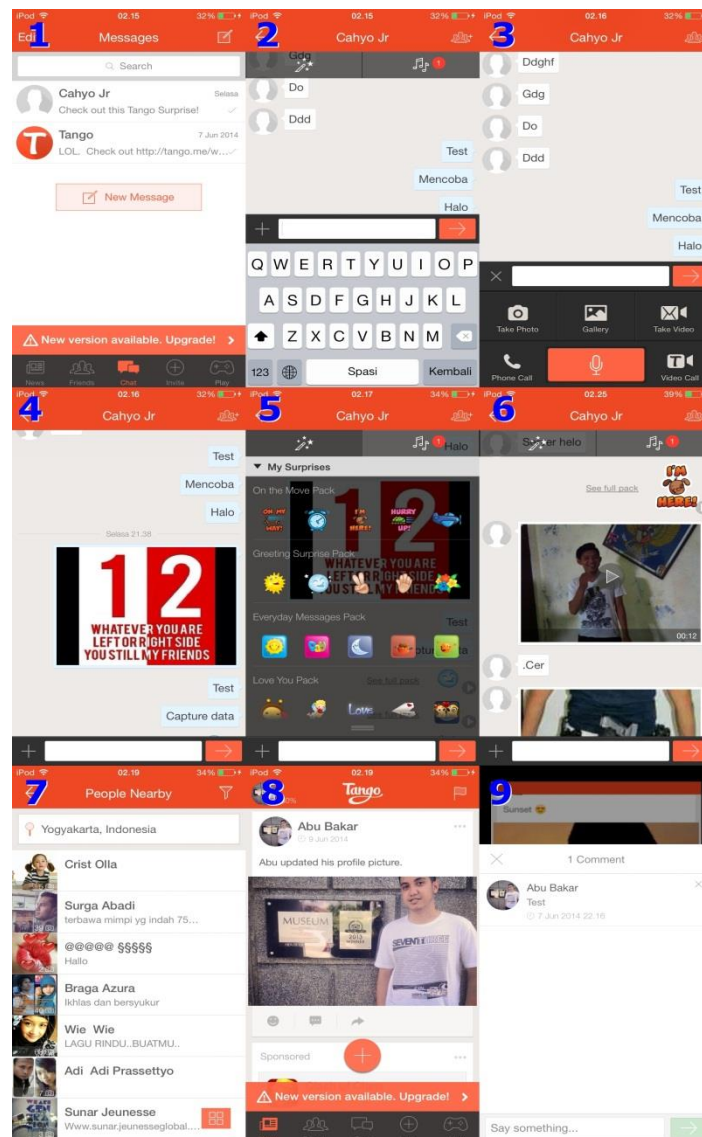
Gambar 4. 3 Tampilan Wechat

Pada gambar 4.3 (nomor 1) merupakan tampilan awal setelah membuka aplikasi Wechat sebelum memilih user yang akan diajak chatting. Kemudian pada gambar 4.3 (nomor 2) merupakan gambar ketika melakukan chatting dengan salah satu user Wechat dan mencoba mengirimkan pesan berupa teks dan juga stiker yang disediakan oleh Wechat. Setelah mencoba mengirim pesan teks dan juga stiker, dilanjutkan dengan mencoba mengirimkan file berupa gambar ke user lain seperti terlihat pada gambar 4.3 (nomor 3).

Pada gambar 4.3 (nomor 4) merupakan gambar dari profile Wechat yang menampilkan Wechat ID dan juga setting pada Wechat. Kemudian pada gambar 4.3 (nomor 5) menampilkan gambar yang diperoleh dari fitur Wechat yaitu *people nearby*, pada gambar tersebut menampilkan pengguna Wechat yang berada disekitar kita dengan radius tertentu. Gambar selanjutnya yaitu gambar 4.3 (nomor 6) menampilkan *update moment* dari user lain yang sudah berteman dengan akun milik penguji, *update moment* bisa berupa gambar maupun kata-kata.

4.1.3 Tango

Sama halnya dengan iMessage dan Wechat, Tango juga dilakukan percobaan penangkapan data dengan memanfaatkan fitur yang sudah ada. Fitur yang dipercobakan yaitu *Chat*, mengirim gambar, mengirim *video*, *people nearby*, dan *share photo*.



Gambar 4. 4 Tampilan Tango

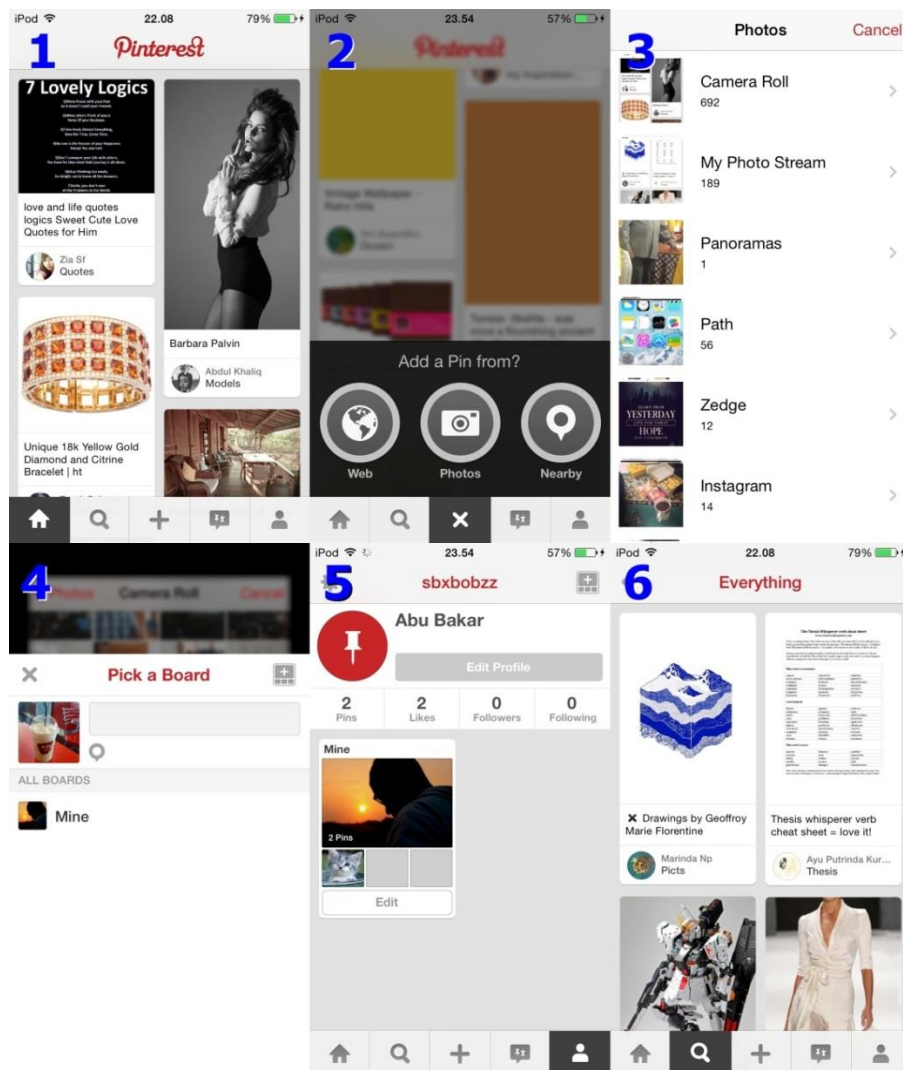
Pada gambar 4.4 (nomor 1) merupakan tampilan awal ketika membuka aplikasi Tango, pada tampilan tersebut menampilkan user yang pernah melakukan *chat* dengan penguji. Gambar 4.4 (nomor 2) merupakan tampilan ketika penguji sudah memilih user untuk diajak chat serta menampilkan chat yang sudah penguji terima dari user lain dan penguji kirim ke user Tango lain. Selanjutnya pada gambar 4.4 (nomor 3) menampilkan fitur yang disediakan oleh Tango seperti *take photo*, *gallery*, *take video*, *phone call*, dan *video call*.

Disini penguji akan mencoba memanfaatkan fitur *gallery* untuk mengirim gambar dari *device* penguji ke *user* lain. Kemudian pada gambar 4.4 (nomor 4) terlihat gambar yang sudah penguji kirim ke *user* lain. Selanjutnya penguji juga mencoba untuk mengirimkan beberapa *sticker* yang sudah disediakan oleh Tango seperti terlihat pada gambar 4.4 (nomor 5). Pada gambar 4.4 (nomor 6) merupakan tampilan ketika penguji sudah berhasil mengirimkan *sticker* kepada *user* Tango lain dan terlihat juga penguji mendapat kiriman berupa *video* dan juga gambar.

Gambar selanjutnya yaitu gambar 4.4 (nomor 7) merupakan gambar dari tampilan fitur *people nearby* milik Tango, di mana pada fitur tersebut menampilkan *user* lain di sekitar penguji dengan radius tertentu yang juga menggunakan aplikasi Tango. Pada gambar 4.4 (nomor 8) menampilkan fitur *news* dari Tango yang berguna untuk menampilkan aktifitas terbaru yang dilakukan baik oleh penguji atau oleh *user* Tango lain yang sudah berteman dengan penguji, pada fitur *news* ini kita juga bisa melakukan proses *upload* gambar, *video*, teks dan juga *music*. Sedangkan pada gambar 4.4 (nomor 9) menampilkan gambar ketika melakukan *comment* pada gambar yang sudah penguji *upload* di *news*.

4.1.4 Pinterest

Proses pengujian pada Pinterest dilakukan dengan melakukan *upload* foto karena pinterest merupakan aplikasi media sosial yang fokus pada fitur berbagi foto.



Gambar 4. 5 Tampilan Pinterest

Pada gambar 4.5 (nomor 1) merupakan tampilan awal ketika penguji membuka Pinterest, di sana ditampilkan foto yang baru saja para pengguna Pinterest *upload*. Selanjutnya pada gambar 4.5 (nomor 2) adalah gambar ketika penguji akan mencoba melakukan *upload* foto ke Pinterest, setelah itu penguji memilih foto yang akan di *upload*, di sini penguji melakukan *upload* foto dari foto yang sudah ada pada device ipod seperti terlihat pada gambar 4.5 (nomor 3).

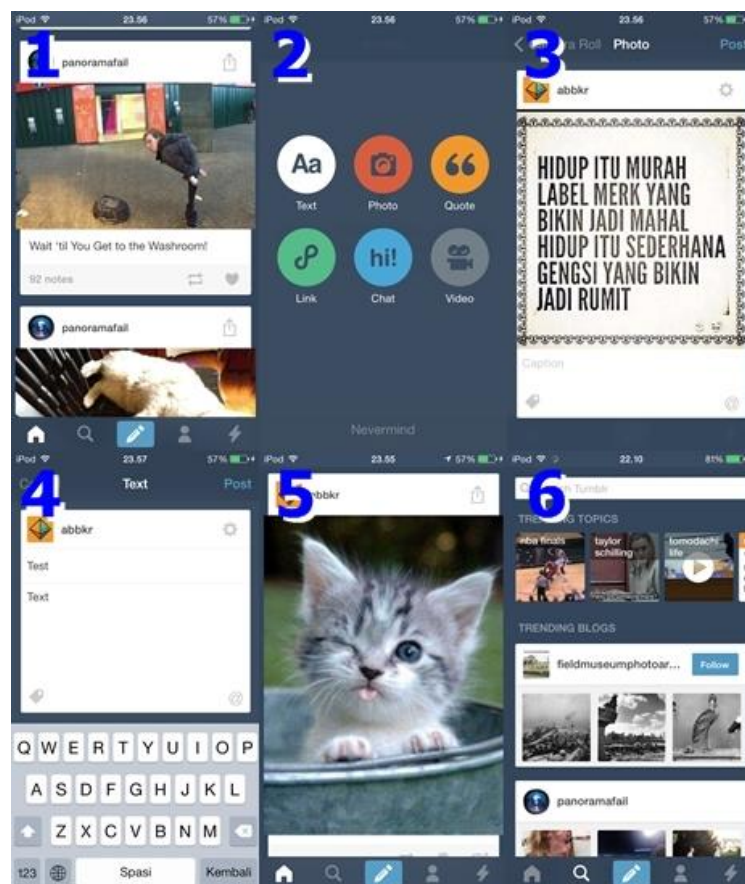
Pada gambar selanjutnya yaitu gambar 4.5 (nomor 4) adalah gambar setelah penguji memilih foto yang akan di *upload* dan diharuskan memilih *board* milik penguji,

karena pada Pinterest foto yang akan dilakukan proses *upload* bisa dikategorikan sesuai dengan *board* yang sudah dibuat. Gambar 4.5 (nomor 5) menampilkan profil Pinterest milik penguji di mana di sana terlihat jumlah *pins*, *likes*, *followers*, dan *following*.

Terakhir pada gambar 4.5 (nomor 6) menampilkan pencarian pada pinterest pada fitur pencarian tersebut user dapat melakukan pencarian berdasar *keyword* sesuai keinginan pengguna atau melakukan pencarian sesuai kategori yang sudah disediakan oleh Pinterest.

4.1.5 Tumblr

Aplikasi terakhir yang dilakukan pengujian adalah Tumblr, tidak berbeda jauh dengan Pinterest karena Tumblr merupakan aplikasi untuk berbagi foto namun Tumblr juga bisa untuk berbagi *video*. Penguji melakukan pengujian dengan melakukan proses *upload* foto, *video*, dan teks.



Gambar 4. 6 Tampilan Tumblr

Pada Gambar 4.6 (nomor 1) merupakan tampilan dari Tumblr ketika penguji membuka aplikasi Tumblr, di sana terlihat foto yang sudah diposting oleh akun yang sudah penguji *follow*. Gambar selanjutnya (nomor 2) merupakan tampilan ketika penguji akan mencoba melakukan *upload*, tersedia beberapa pilihan yaitu *text*, *photo*, *quote*, *link*, *chat*, dan *video*. Selanjutnya penguji mencoba untuk melakukan *upload* file berupa gambar seperti terlihat pada gambar 4.6 (nomor 3). Dilanjutkan dengan penguji mencoba untuk melakukan *upload text* seperti terlihat pada gambar 4.6 (nomor 4), disini penguji mencoba untuk *upload* tulisan dengan *subject* “test” dengan isi pesan bertuliskan “text”.

Gambar selanjutnya merupakan tampilan dari file *video* yang sudah penguji *upload* ke Tumblr seperti terlihat pada gambar 4.6 (nomor 5). Terakhir, gambar 4.6 (nomor 6) merupakan tampilan dari menu pencarian yang ada pada Tumblr, selain untuk bisa melakukan pencarian di sana juga diperlihatkan file yang menjadi *trending topics* dan juga *trending blogs*.

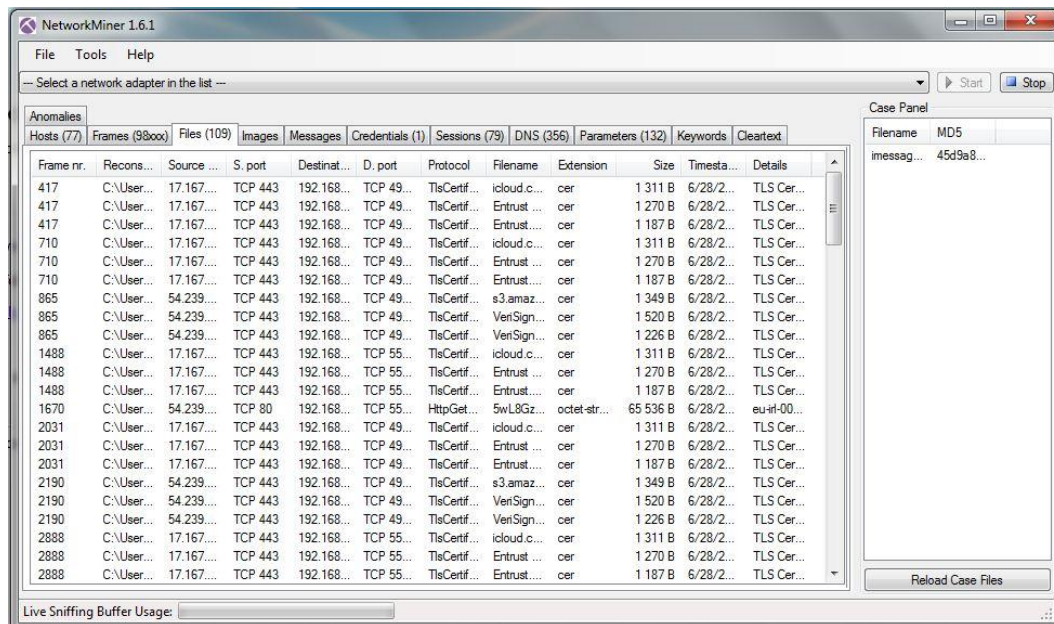
4.2 Hasil Analisis Lalu Lintas Data

Setelah selesai melakukan pengambilan data, langkah selanjutnya yang dilakukan yaitu analisis paket – paket data yang tertangkap. *Software* untuk analisis yang digunakan adalah Network Miner. Diharapkan dari proses analisis pada penangkapan data bisa diperoleh informasi sebanyak-banyaknya.

Pembacaan file hasil penangkapan data dilakukan dengan aplikasi Network Miner, yang berguna untuk menyatukan kembali paket-paket data yang dipecah ketika proses lalu lintas data. Namun tidak semua file dapat disatukan kembali setelah file tersebut dipecah. Berikut merupakan hasil temuan dari lalu lintas data yang berhasil ditangkap.

4.2.1 iMessage

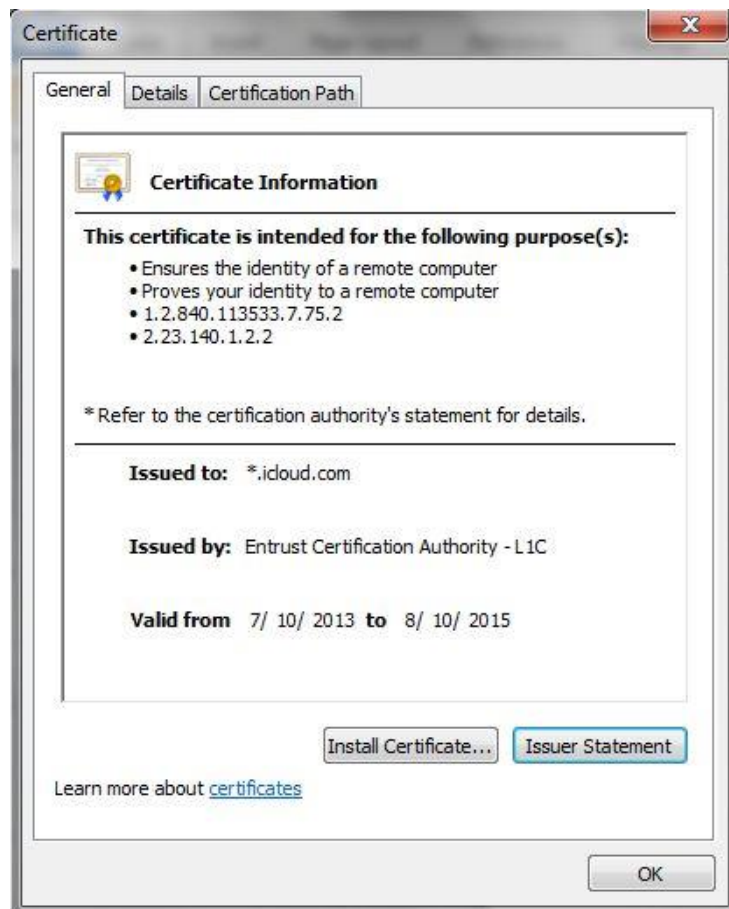
Pada file hasil tangkapan iMessage terdapat 98361 paket data, kemudian penguji menggunakan Network miner untuk menyatukan kembali paket lalu lintas data yang ada sehingga mempermudah dalam proses pembacaan file.



Gambar 4. 7 Tampilan tab files iMessage

Dari banyak paket lalu lintas data yang ditangkap, file yang mendominasi hasil tangkapan adalah file sertifikat, file tersebut mempunyai ekstensi CER. Pada paket lalu lintas data imessage tidak terdapat sama sekali file gambar dan teks yang sudah dikirim maupun diterima oleh penguji. Hal tersebut dikarenakan lalu lintas data pada imessage menggunakan HTTPS.

Berikutnya akan ditampilkan salah satu sertifikat yang ditangkap pada paket lalu lintas data imessage.



Gambar 4. 8 Tampilan sertifikat iMessage

14	0.364638	17.167.139.39	192.168.137.118	TLSv1	146 Server Hello, change cipher spec
15	0.364689	17.167.139.39	192.168.137.118	TLSv1	146 [TCP Retransmission] Server Hello, change cipher spec
16	0.364712	17.167.139.39	192.168.137.118	TLSv1	146 [TCP Retransmission] Server Hello, change cipher spec
17	0.366448	17.167.139.39	192.168.137.118	TLSv1	91 Encrypted Handshake Message
18	0.366488	17.167.139.39	192.168.137.118	TLSv1	91 [TCP Retransmission] Encrypted Handshake Message
19	0.366510	17.167.139.39	192.168.137.118	TLSv1	91 [TCP Retransmission] Encrypted Handshake Message
20	0.367151	192.168.137.118	17.167.139.39	TCP	54 55643 > https [ACK] Seq=230 Ack=93 Win=65535 Len=0
21	0.370725	192.168.137.118	17.167.139.39	TCP	54 [TCP Dup ACK 20#1] 55643 > https [ACK] Seq=230 Ack=93 Win=65535 Len=0
22	0.370727	192.168.137.118	17.167.139.39	TCP	54 [TCP Dup ACK 20#2] 55643 > https [ACK] Seq=230 Ack=93 Win=65535 Len=0
23	0.370728	192.168.137.118	17.167.139.39	TCP	54 55643 > https [ACK] Seq=230 Ack=130 Win=65535 Len=0
24	0.370728	192.168.137.118	17.167.139.39	TCP	54 [TCP Dup ACK 23#1] 55643 > https [ACK] Seq=230 Ack=130 Win=65535 Len=0

random gmt_unix_time: Jun 28, 2014 04:56:45.000000000 SE Asia Standard Time random_bytes: ec94ef29fb63dceea3ede320d9c5af3fa47d5ceac425ded3... Session ID Length: 32 Session ID: Dcd0cc9b0ab1761d4b9c3eb985dc95bb856df4e70e3c71a5... Cipher suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004) Compression Method: null (0)

Gambar 4. 9 Handshake Protocol iMessage

iMessage mengamankan koneksi ke server dengan menggunakan TLSv1, dan data pada iMessage dienkripsi menggunakan RC4 dengan panjang kunci 128bit. Berikut kesimpulan dari hasil tangkapan lalu lintas data akan dijabarkan dalam bentuk tabel.

Tabel 4. 1 Tabel informasi iMessage

Text	Image	Video
×	×	×

√ (jika didapatkan hasil) dan × (jika tidak didapatkan hasil)

4.2.2 Wechat

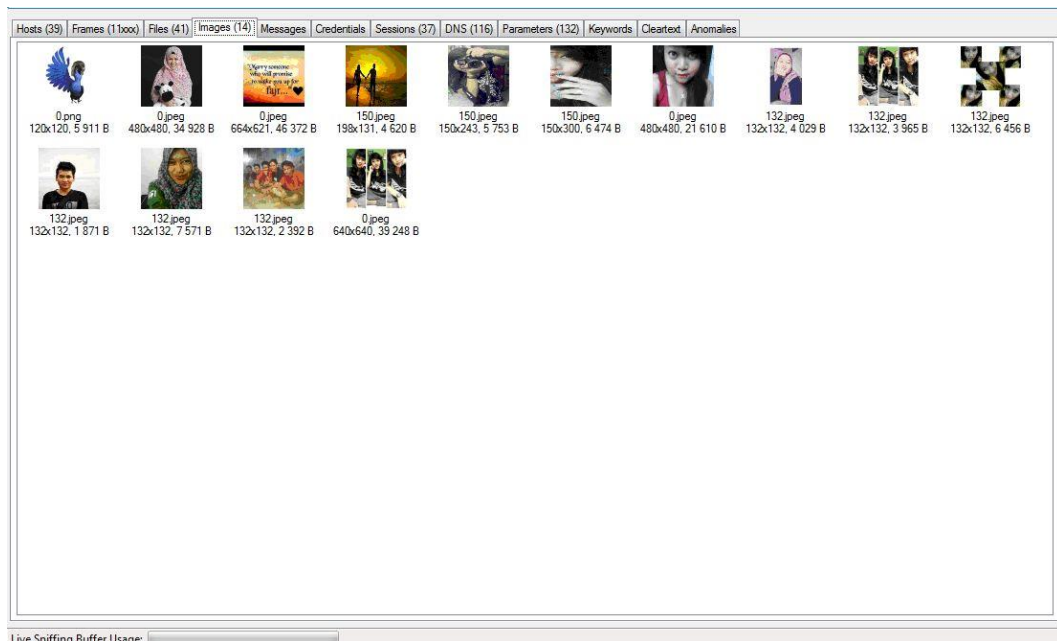
Pada aplikasi Wechat diperoleh paket data sebanyak 11046. Dari hasil tangkapan paket lalu lintas data Wechat dan setelah dibuka menggunakan network miner diketahui bahwa ada 41 files, 14 diantaranya adalah file *images*. Berikut akan ditampilkan tab files pada Wechat.

Hosts (39)	Frames (11000)	Files (41)	Images (14)	Messages	Credentials	Sessions (37)	DNS (116)	Parameters (132)	Keywords	Cleartext	Anomalies
Frame nr.	Recons...	Source ...	S. port	Destinat...	D. port	Protocol	Filename	Extension	Size	Timesta...	Details
5505	C:\User...	54.255...	TCP 80	192.168...	TCP 49...	HttpGetNormal	0.jpeg	jpeg	34 928 B	6/28/2...	wx.qlog...
8199	C:\User...	54.255...	TCP 80	192.168...	TCP 49...	HttpGetNormal	0.jpeg	jpeg	46 372 B	6/28/2...	mmsns...
8699	C:\User...	54.251...	TCP 80	192.168...	TCP 49...	HttpGetNormal	0.jpeg	jpeg	21 610 B	6/28/2...	wx.qlog...
9082	C:\User...	54.251...	TCP 80	192.168...	TCP 49...	HttpGetNormal	0.jpeg	jpeg	39 248 B	6/28/2...	wx.qlog...
2575	C:\User...	103.7.3...	TCP 80	192.168...	TCP 49...	HttpGetNormal	0.png	png	5 911 B	6/28/2...	mmbiz.q...
8810	C:\User...	54.255...	TCP 80	192.168...	TCP 49...	HttpGetNormal	132.jpeg	jpeg	4 029 B	6/28/2...	wx.qlog...
8857	C:\User...	54.251...	TCP 80	192.168...	TCP 49...	HttpGetNormal	132.jpeg	jpeg	3 965 B	6/28/2...	wx.qlog...
8865	C:\User...	54.251...	TCP 80	192.168...	TCP 49...	HttpGetNormal	132.jpeg	jpeg	6 456 B	6/28/2...	wx.qlog...
8944	C:\User...	54.251...	TCP 80	192.168...	TCP 49...	HttpGetNormal	132.jpeg	jpeg	1 871 B	6/28/2...	wx.qlog...
8900	C:\User...	54.251...	TCP 80	192.168...	TCP 49...	HttpGetNormal	132.jpeg	jpeg	7 571 B	6/28/2...	wx.qlog...
8984	C:\User...	54.255...	TCP 80	192.168...	TCP 49...	HttpGetNormal	132.jpeg	jpeg	2 392 B	6/28/2...	wx.qlog...
8595	C:\User...	54.255...	TCP 80	192.168...	TCP 49...	HttpGetNormal	150.jpeg	jpeg	4 620 B	6/28/2...	mmsns...
8627	C:\User...	54.255...	TCP 80	192.168...	TCP 49...	HttpGetNormal	150.jpeg	jpeg	5 753 B	6/28/2...	mmsns...
8634	C:\User...	54.251...	TCP 80	192.168...	TCP 49...	HttpGetNormal	150.jpeg	jpeg	6 474 B	6/28/2...	mmsns...
2879	C:\User...	17.154...	TCP 443	192.168...	TCP 49...	TlsCertificate	buy.itun...	cer	3 735 B	6/28/2...	TLS Cer...
16	C:\User...	54.251...	TCP 8080	192.168...	TCP 49...	HttpGetNormal	download		57 520 B	6/28/2...	/downlo...
627	C:\User...	54.251...	TCP 8080	192.168...	TCP 49...	HttpGetNormal	download		31 818 B	6/28/2...	/downlo...
6308	C:\User...	54.251...	TCP 8080	192.168...	TCP 49...	HttpGetNormal	download		57 515 B	6/28/2...	/downlo...
7300	C:\User...	54.251...	TCP 8080	192.168...	TCP 49...	HttpGetNormal	download		57 515 B	6/28/2...	/downlo...
9285	C:\User...	54.251...	TCP 8080	192.168...	TCP 49...	HttpGetNormal	download		57 515 B	6/28/2...	/downlo...
10086	C:\User...	54.251...	TCP 8080	192.168...	TCP 49...	HttpGetNormal	download		57 515 B	6/28/2...	/downlo...
10930	C:\User...	125.160...	TCP 80	192.168...	TCP 49...	HttpGetNormal	goc.html	html	2 B	6/28/2...	gspl.ap...
2284	C:\User...	54.254...	TCP 80	192.168...	TCP 49...	HttpGetNormal	microms...	octet-str...	666 B	6/28/2...	http://h...
5308	C:\User...	54.255...	TCP 80	192.168...	TCP 55...	HttpGetNormal	microms...	octet-str...	874 B	6/28/2...	http://h...
2789	C:\User...	54.254...	TCP 80	192.168...	TCP 49...	HttpGetNormal	microms...	octet-str...	666 B	6/28/2...	http://h...
3029	C:\User...	54.254...	TCP 80	192.168...	TCP 49...	HttpGetNormal	microms...	octet-str...	666 B	6/28/2...	http://h...
3834	C:\User...	54.254...	TCP 80	192.168...	TCP 49...	HttpGetNormal	microms...	octet-str...	874 B	6/28/2...	http://h...
2924	C:\User...	184.29...	TCP 80	192.168...	TCP 49...	HttpGetNormal	pipeline...	html	213 B	6/28/2...	configur...
10963	C:\User...	125.160...	TCP 80	192.168...	TCP 49...	HttpGetNormal	tile.vf.5...	jpeg	2 121 B	6/28/2...	gspl9...
3147	C:\User...	54.251...	TCP 8080	192.168...	TCP 49...	HttpGetNormal	uploadv3		442 B	6/28/2...	/upload...
3924	C:\User...	54.254...	TCP 8080	192.168...	TCP 55...	HttpGetNormal	uploadv3		166 B	6/28/2...	/upload...
3488	C:\User...	54.251...	TCP 8080	192.168...	TCP 49...	HttpGetNormal	uploadv...		442 B	6/28/2...	/upload...
4232	C:\User...	54.254...	TCP 8080	192.168...	TCP 55...	HttpGetNormal	uploadv...		152 B	6/28/2...	/upload...
4796	C:\User...	54.254...	TCP 8080	192.168...	TCP 55...	HttpGetNormal	uploadv...		167 B	6/28/2...	/upload...

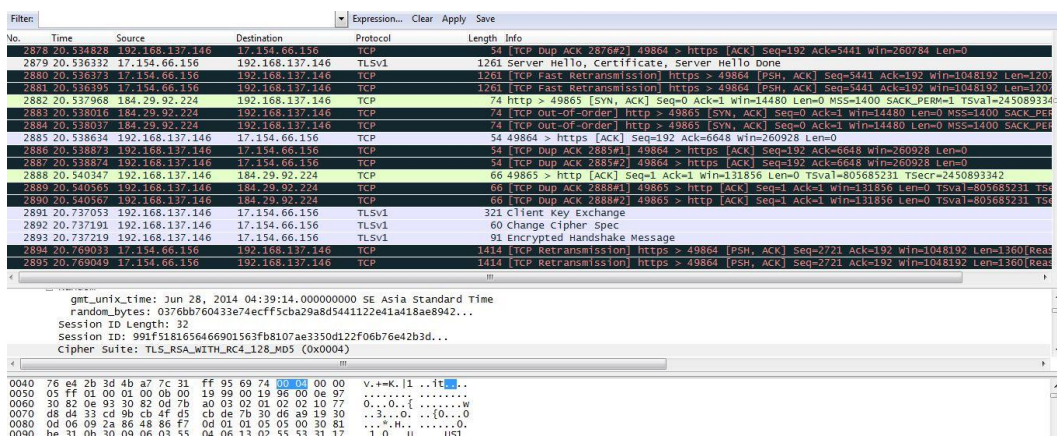
Gambar 4. 10 Tampilan tab files Wechat

Dari hasil tangkapan Wechat *images* yang didapatkan merupakan gambar yang didapat dari fitur Wechat yaitu, *look around*, *moment* dan *stickers*. Sedangkan untuk

gambar yang dikirim atau diterima oleh penguji sama sekali tidak didapatkan filenya. Berikut tampilan tab *images* pada hasil tangkapan lalu lintas data wechat.



Gambar 4. 11 Tampilan tab images Wechat



Gambar 4. 12 Handshake Protocol Wechat

Aplikasi Wechat mengamankan koneksi ke server menggunakan TLSv1. Data pada Wechat dienkripsi menggunakan RC4 dengan panjang kunci 128bit. Berikut kesimpulan yang didapat berdasarkan hasil penangkapan lalu lintas data Wechat.

Tabel 4. 2 Tabel informasi Wechat

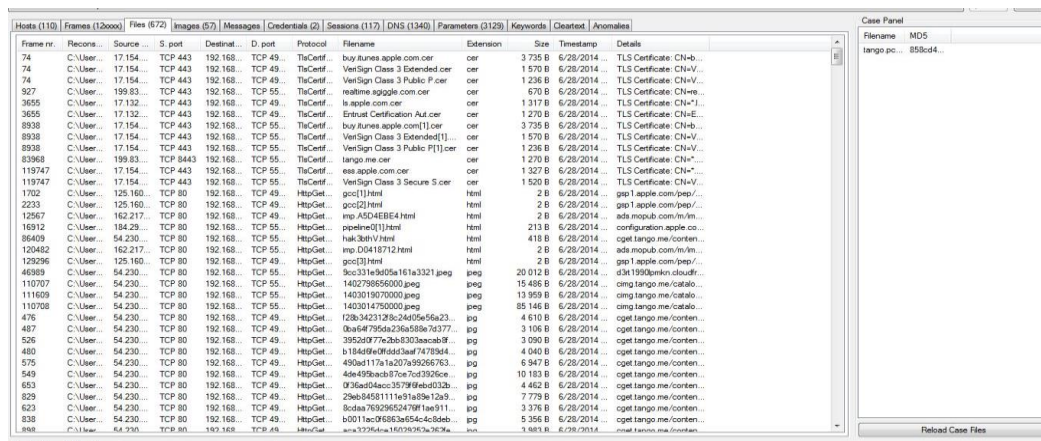
Text	Profil Picture	Photo	Video	Moments	Locations	Look Around
×	✓	×	×	✓	×	✓

✓ (jika didapatkan hasil) dan × (jika tidak didapatkan hasil)

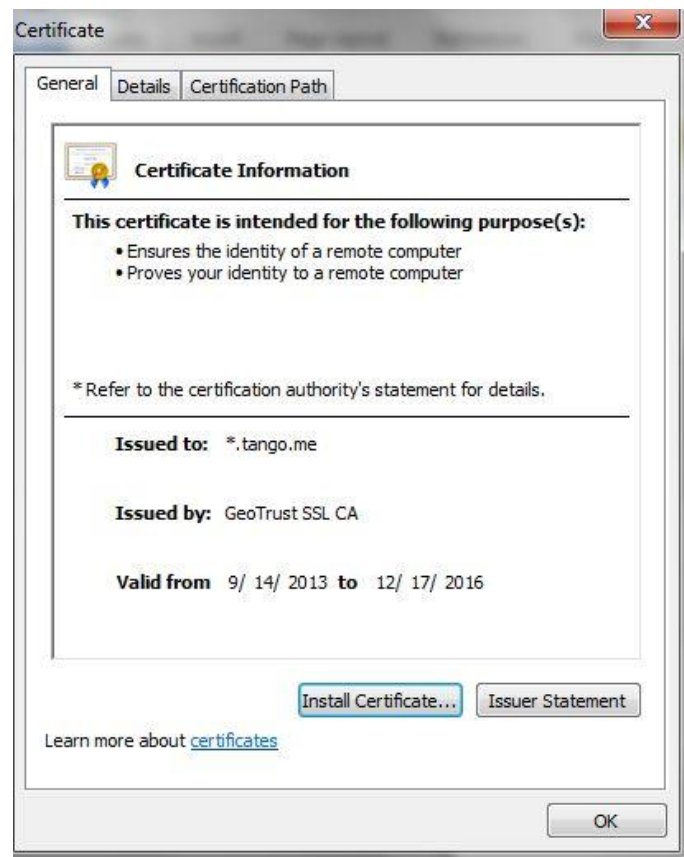
Dari tabel di atas dapat diketahui bahwa pada aplikasi wechat file yang bisa tertangkap dari lalu lintas datanya hanya profil picture, moments, dan look around, file yang ditangkap mayoritas berupa gambar. Sedangkan pesan teks, gambar, video, dan locations yang penguji kirim maupun terima tidak tertangkap sama sekali.

4.2.3 Tango

Ketika proses penangkapan lalu lintas data dilakukan, jumlah banyak paket yang didapatkan adalah 129707. Terdapat 672 files, 12 diantaranya adalah file sertifikat , 57 files berupa images, dan sisanya file dengan ekstensi html, json, xml dan zip. Berikut tampilan Tango yang sudah dibuka menggunakan Network miner.

**Gambar 4. 13** Tampilan tab files Tango

Pada hasil tangkapan lalu lintas data Tango tertangkap sertifikat yang memang dikeluarkan untuk aplikasi Tango. Berikut akan ditampilkan sertifikat aplikasi Tango

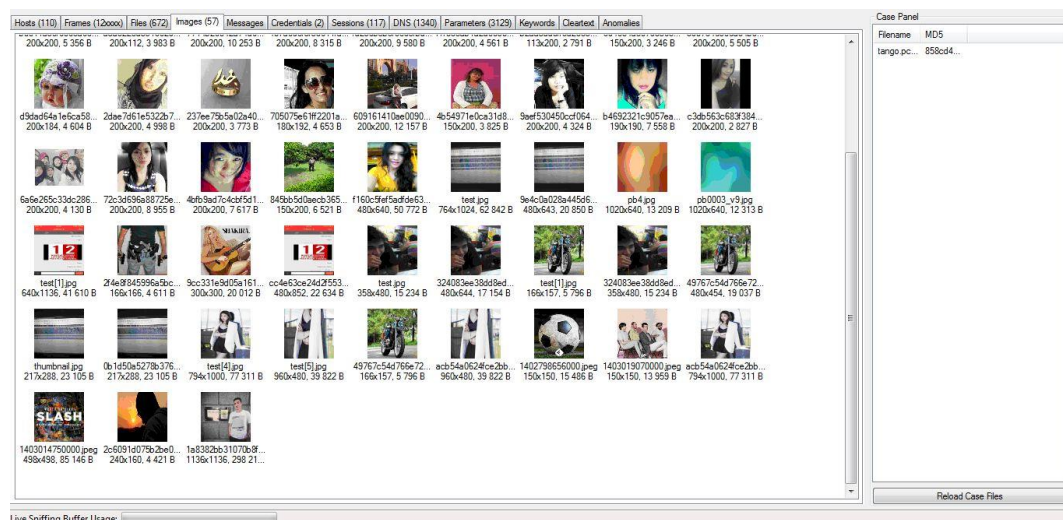


Gambar 4. 14 Sertifikat Tango

Untuk mengamankan koneksi ke server, Tango menggunakan TLSv1 dengan enkripsi menggunakan AES 128 bit seperti terlihat pada gambar di bawah.

Filter	Expression...	Clear	Apply	Save		
Io.	Time	Source	Destination	Protocol	Length	Info
922	8.056602	192.168.137.146	54.230.159.95	TCP	66	49924 > http [ACK] Seq=547 Ack=10057 win=129680 Len=0 TSval=805992270 TSecr=2506950304
923	8.075701	192.168.137.146	54.230.159.95	TCP	66	[TCP Dup ACK 922#1] 49924 > http [ACK] Seq=547 Ack=10057 win=129680 Len=0 TSval=805992270 TSecr=2506950304
924	8.074396	199.83.168.194	192.168.137.118	TCP	66	https > 55462 [ACK] Seq=1 Ack=64 win=14592 Len=0 TSval=1679546643 TSecr=389079101
925	8.07437	199.83.168.194	192.168.137.118	TCP	66	[TCP Dup ACK 924#1] https > 55462 [ACK] Seq=1 Ack=64 win=14592 Len=0 TSval=1679546643 TSecr=389079101
926	8.071457	199.83.168.194	192.168.137.118	TCP	66	[TCP Dup ACK 924#2] https > 55462 [ACK] Seq=1 Ack=64 win=14592 Len=0 TSval=1679546643 TSecr=389079101
927	8.076353	199.83.168.194	192.168.137.118	TLSv1	818	Server Hello, Certificate, Server Hello Done
928	8.076395	199.83.168.194	192.168.137.118	TLSv1	818	[TCP Retransmission] Server Hello, Certificate, Server Hello Done
929	8.076418	199.83.168.194	192.168.137.118	TLSv1	818	[TCP Retransmission] Server Hello, Certificate, Server Hello Done
930	8.084844	54.230.159.95	192.168.137.146	TCP	1454	[TCP segment of a reassembled PDU]
931	8.084889	54.230.159.95	192.168.137.146	TCP	1454	[TCP Retransmission] [TCP segment of a reassembled PDU]
932	8.084913	54.230.159.95	192.168.137.146	TCP	1454	[TCP Retransmission] [TCP segment of a reassembled PDU]
933	8.087063	192.168.137.146	54.230.159.95	TCP	66	49923 > http [ACK] Seq=1051 Ack=37008 win=129680 Len=0 TSval=805992300 TSecr=2506938629
934	8.087065	192.168.137.146	54.230.159.95	TCP	66	[TCP Dup ACK 933#1] 49923 > http [ACK] Seq=1051 Ack=37008 win=129680 Len=0 TSval=805992300 TSecr=2506938629
935	8.102887	54.230.159.95	192.168.137.146	TCP	1454	[TCP Previous segment not captured] [TCP segment of a reassembled PDU]
936	8.102930	54.230.159.95	192.168.137.146	TCP	1454	[TCP Retransmission] [TCP segment of a reassembled PDU]
937	8.102954	54.230.159.95	192.168.137.146	TCP	1454	[TCP Retransmission] [TCP segment of a reassembled PDU]
938	8.105064	192.168.137.146	54.230.159.95	TCP	78	[TCP window update] 49923 > http [ACK] Seq=1051 Ack=37008 win=131072 Len=0 TSval=805992300 TSecr=2506938629
939	8.105066	192.168.137.146	54.230.159.95	TCP	78	[TCP Dup ACK 938#1] 49923 > http [ACK] Seq=1051 Ack=37008 win=131072 Len=0 TSval=805992300 TSecr=2506938629
gmt_unix_time: Jun 28, 2014 04:44:22.000000000 SE Asia Standard Time random_bytes: 8c985565fbb5c988949eb13f065d85ecbf87f028821e1cf... Session ID Length: 0 cipher_suite: TLSv1.2 SSLv3 TLSv1.2 CBC_SHA (0x002f) compression Method: null (0)						
.....!..a..#.....0..0..1...a.0. ...H.....0.. 1.0...U...l.. ...U...californ tal.0...U...Pal o altcol. 0...U... ..sglggle Inc.1.0 ...U...Certific ate Auth ority1.0 ...U...Tango CA						

Gambar 4. 15 Handshake protocol Tango



Gambar 4. 16 Tampilan tab images Tango

Pada gambar 4.16 yang merupakan tab images dari tango, terlihat tampilan gambar yang tertangkap. Gambar yang tertangkap berasal dari fitur – fitur tango, baik berkirim gambar ke sesama pengguna tango, people nearby, dan update news. Berikut kesimpulan yang didapat berdasarkan hasil penangkapan lalu lintas data Tango.

Tabel 4. 3 Tabel informasi Tango

Text	Photo	Video	News	People nearby	Stickers
×	✓	×	✓	✓	✓

✓ (jika didapatkan hasil) dan × (jika tidak didapatkan hasil)

Dari tabel di atas diketahui bahwa pesan teks, video pada tango tidak bisa ditangkap ketika melakukan penangkapan lalu lintas data. Pada tango yang tertangkap adalah *photo*, *news*, *people nearby*, dan *stickers*.

Photo yang ditangkap pada Tango merupakan photo yang dikirim ataupun diterima oleh penguji. Sedangkan News yang ditangkap adalah file gambar yang penguji *upload*. *People nearby* berisi gambar dari profil picture pengguna tango lain. Pada *stickers*, file yang tertangkap berupa file zip di mana dalam file zip tersebut berisi file untuk membentuk *stickers* dan untuk mengeluarkan suara dari *stickers*.

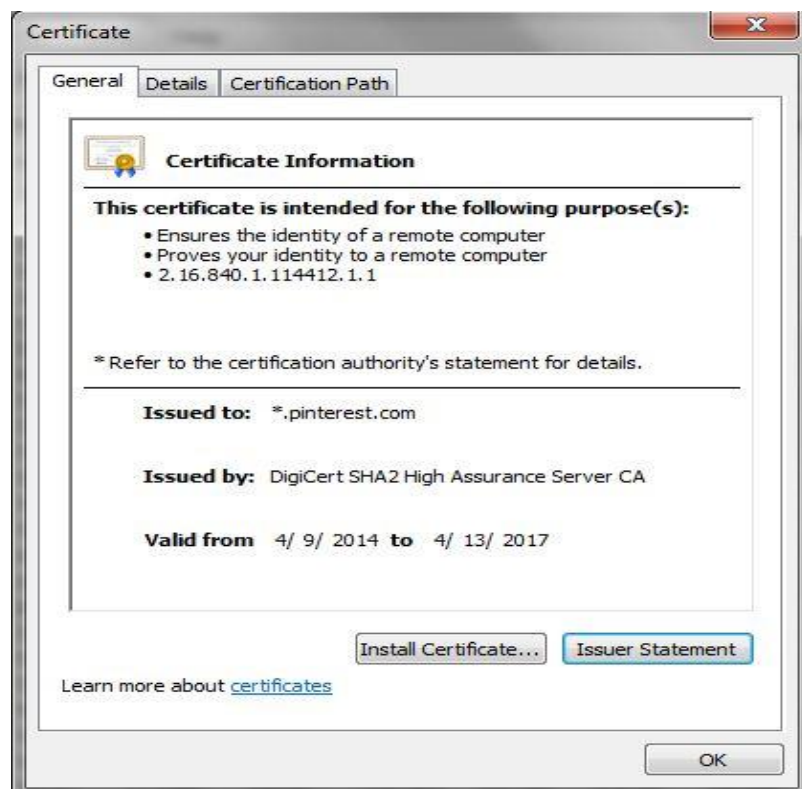
4.2.4 Pinterest

Pada aplikasi Pinterest paket data yang tertangkap sebanyak 43782. Terdapat 328 files pada hasil tangkapan pinterest. 164 diantaranya berupa images, sisanya adalah file sertifikat dan javascript. Berikut akan ditampilkan hasil tangkapan pinterest yang dibuka menggunakan network miner.

Frame nr.	Reconn.	Source	S port	Destinat.	D port	Protocol	Filename	Extension	Size	Timestamp	Details
82	C:\User...	54.243...	TCP 443	192.168...	TCP 50...	TlsCert...	pinterest.com.cer	cer	1369 B	6/28/2014...	TLS Certificate: CN="pinterest.co...
92	C:\User...	54.243...	TCP 443	192.168...	TCP 50...	TlsCert...	DigiCert SHA2 High Assurance...	cer	1205 B	6/28/2014...	TLS Certificate: CN=DigiCert SHA...
101	C:\User...	54.243...	TCP 443	192.168...	TCP 50...	TlsCert...	pinterest.com[1].cer	cer	1369 B	6/28/2014...	TLS Certificate: CN="pinterest.co...
101	C:\User...	54.243...	TCP 443	192.168...	TCP 50...	TlsCert...	DigiCert SHA2 High Assurance[1]...	cer	1205 B	6/28/2014...	TLS Certificate: CN=DigiCert SHA...
120	C:\User...	54.243...	TCP 443	192.168...	TCP 50...	TlsCert...	pinterest.com[2].cer	cer	1369 B	6/28/2014...	TLS Certificate: CN="pinterest.co...
120	C:\User...	54.243...	TCP 443	192.168...	TCP 50...	TlsCert...	DigiCert SHA2 High Assurance[2]...	cer	1205 B	6/28/2014...	TLS Certificate: CN=DigiCert SHA...
142	C:\User...	54.243...	TCP 443	192.168...	TCP 50...	TlsCert...	pinterest.com[3].cer	cer	1369 B	6/28/2014...	TLS Certificate: CN="pinterest.co...
142	C:\User...	54.243...	TCP 443	192.168...	TCP 50...	TlsCert...	DigiCert SHA2 High Assurance[3]...	cer	1205 B	6/28/2014...	TLS Certificate: CN=DigiCert SHA...
175	C:\User...	54.241...	TCP 443	192.168...	TCP 50...	TlsCert...	criticism.com.cer	cer	1295 B	6/28/2014...	TLS Certificate: CN="criticism.c...
175	C:\User...	54.241...	TCP 443	192.168...	TCP 50...	TlsCert...	PositiveSSL CA 2.cer	cer	1257 B	6/28/2014...	TLS Certificate: CN=PositiveSSL...
175	C:\User...	54.241...	TCP 443	192.168...	TCP 50...	TlsCert...	AddTrust External CA Root.cer	cer	1082 B	6/28/2014...	TLS Certificate: CN=AddTrust Ext...
199	C:\User...	216.52...	TCP 443	192.168...	TCP 50...	TlsCert...	runy.com.cer	cer	1369 B	6/28/2014...	TLS Certificate: CN="runy.com. O...
199	C:\User...	216.52...	TCP 443	192.168...	TCP 50...	TlsCert...	07965287.cer	cer	1250 B	6/28/2014...	TLS Certificate: SERIALNUMBER...
199	C:\User...	216.52...	TCP 443	192.168...	TCP 50...	TlsCert...	Go Daddy Class 2 Certific.cer	cer	1028 B	6/28/2014...	TLS Certificate: OU=Go Daddy Cl...
3479	C:\User...	173.194...	TCP 443	192.168...	TCP 50...	TlsCert...	ssl.google-analytics.com.cer	cer	1297 B	6/28/2014...	TLS Certificate: CN=ssl.google-an...
3479	C:\User...	173.194...	TCP 443	192.168...	TCP 50...	TlsCert...	Google Internet Authority.cer	cer	1032 B	6/28/2014...	TLS Certificate: CN=Google Intern...
3479	C:\User...	173.194...	TCP 443	192.168...	TCP 50...	TlsCert...	GeoTrust Global CA.cer	cer	897 B	6/28/2014...	TLS Certificate: CN=GeoTrust Glo...
13086	C:\User...	118.98...	TCP 443	192.168...	TCP 50...	TlsCert...	gstatic.com.cer	cer	1179 B	6/28/2014...	TLS Certificate: CN="gstatic.com...
13086	C:\User...	118.98...	TCP 443	192.168...	TCP 50...	TlsCert...	Google Internet Authority.cer	cer	1032 B	6/28/2014...	TLS Certificate: CN=Google Intern...
13086	C:\User...	118.98...	TCP 443	192.168...	TCP 50...	TlsCert...	GeoTrust Global CA.cer	cer	897 B	6/28/2014...	TLS Certificate: CN=GeoTrust Glo...
14803	C:\User...	126.56...	TCP 443	192.168...	TCP 50...	TlsCert...	gstatic.ak.facebook.com.cer	cer	1092 B	6/28/2014...	TLS Certificate: CN=static.ak.fac...
14803	C:\User...	126.56...	TCP 443	192.168...	TCP 50...	TlsCert...	Cybertrust Public Server.cer	cer	1059 B	6/28/2014...	TLS Certificate: CN=Cybertrust Pu...
14803	C:\User...	126.56...	TCP 443	192.168...	TCP 50...	TlsCert...	Baltimore CyberTrust Root.cer	cer	1049 B	6/28/2014...	TLS Certificate: CN=Baltimore Cyb...
15132	C:\User...	199.59...	TCP 443	192.168...	TCP 50...	TlsCert...	twitter.com.cer	cer	1550 B	6/28/2014...	TLS Certificate: CN=twitter.com. O...
15132	C:\User...	199.59...	TCP 443	192.168...	TCP 50...	TlsCert...	VeriSign Class 3 Extended.cer	cer	1512 B	6/28/2014...	TLS Certificate: CN=VeriSign Clas...
20506	C:\User...	31.13.7...	TCP 443	192.168...	TCP 50...	TlsCert...	facebook.com.cer	cer	1375 B	6/28/2014...	TLS Certificate: CN="facebook.c...
20506	C:\User...	31.13.7...	TCP 443	192.168...	TCP 50...	TlsCert...	DigiCert High Assurance CA.cer	cer	1628 B	6/28/2014...	TLS Certificate: CN=DigiCert High...
20552	C:\User...	118.98...	TCP 443	192.168...	TCP 50...	TlsCert...	www.google.com.cer	cer	1146 B	6/28/2014...	TLS Certificate: CN=www.google...
20552	C:\User...	118.98...	TCP 443	192.168...	TCP 50...	TlsCert...	Google Internet Authority.cer	cer	1032 B	6/28/2014...	TLS Certificate: CN=Google Intern...
20552	C:\User...	118.98...	TCP 443	192.168...	TCP 50...	TlsCert...	GeoTrust Global CA.cer	cer	897 B	6/28/2014...	TLS Certificate: CN=GeoTrust Glo...
20694	C:\User...	74.125...	TCP 443	192.168...	TCP 50...	TlsCert...	g.doubleclick.net.cer	cer	1356 B	6/28/2014...	TLS Certificate: CN="g.doublecl...
20694	C:\User...	74.125...	TCP 443	192.168...	TCP 50...	TlsCert...	Google Internet Authority.cer	cer	1032 B	6/28/2014...	TLS Certificate: CN=Google Intern...
20694	C:\User...	74.125...	TCP 443	192.168...	TCP 50...	TlsCert...	GeoTrust Global CA.cer	cer	897 B	6/28/2014...	TLS Certificate: CN=GeoTrust Glo...
21147	C:\User...	54.225...	TCP 443	192.168...	TCP 50...	TlsCert...	pinterest.com.cer	cer	1369 B	6/28/2014...	TLS Certificate: CN="pinterest.co...

Gambar 4. 17 Tampilan tab files Pinterest

Pada hasil tangkapan lalu lintas data pinterest tertangkap sertifikat pinterest. Berikut akan ditampilkan sertifikat aplikasi Tango



Gambar 4. 18 Sertifikat Pinterest

Untuk mengamankan koneksi ke server, Tango menggunakan TLSv1.2 dengan enkripsi menggunakan AES 128 bit seperti terlihat pada gambar di bawah.

No.	Time	Source	Destination	Protocol	Length	Info
81	1.012121	192.168.137.146	54.243.121.164	TCP	66	[TCP window update] 50027 > https [ACK] Seq=185 Ack=1389 win=131072 Len=0 TSval=80733857...
82	1.012709	54.243.121.164	192.168.137.146	TLVSLv2	1454	Certificate
83	1.017751	54.243.121.164	192.168.137.146	TCP	1454	[TCP Retransmission] https > 50027 [ACK] Seq=1389 Ack=185 win=15616 Len=388 TSval=431606...
84	1.017774	54.243.121.164	192.168.137.146	TCP	1454	[TCP Retransmission] https > 50027 [ACK] Seq=1389 Ack=185 win=15616 Len=388 TSval=431606...
85	1.019401	192.168.137.146	54.243.121.164	TCP	66	50027 > https [ACK] Seq=185 Ack=2777 win=129680 Len=0 TSval=80733857 TSrc=431608364
86	1.019769	54.243.121.164	192.168.137.146	TLVSLv2	323	Server Key Exchange
87	1.019806	54.243.121.164	192.168.137.146	TCP	323	[TCP Retransmission] https > 50027 [PSH, ACK] Seq=2777 PSN=185 win=15616 Len=257 TSval=...
88	1.019829	54.243.121.164	192.168.137.146	TCP	323	[TCP Retransmission] https > 50027 [PSH, ACK] Seq=2777 PSN=185 win=15616 Len=257 TSval=...
89	1.020210	54.243.121.164	192.168.137.146	TCP	66	https > 50026 [ACK] Seq=1 Ack=185 win=15616 Len=0 TSval=431608369 TSrcer=807338273
90	1.020248	54.243.121.164	192.168.137.146	TCP	66	[TCP Dup ACK 89#1] https > 50026 [ACK] Seq=185 Ack=3034 win=130800 Len=0 TSval=807338577 TSrc=431608369
91	1.020258	54.243.121.164	192.168.137.146	TCP	66	[TCP Dup ACK 89#2] https > 50026 [ACK] Seq=185 Ack=3034 win=130800 Len=0 TSval=807338577 TSrc=431608369
92	1.020826	192.168.137.146	54.243.121.164	TCP	66	[TCP window update] 50027 > https [ACK] Seq=185 Ack=2777 win=131072 Len=0 TSval=80733857...
93	1.022646	192.168.137.146	54.243.121.164	TCP	66	50027 > https [ACK] Seq=185 Ack=3034 win=130800 Len=0 TSval=807338577 TSrc=431608365
94	1.022648	192.168.137.146	54.243.121.164	TCP	66	[TCP Dup ACK 93#1] 50027 > https [ACK] Seq=185 Ack=3034 win=130800 Len=0 TSval=80733857...
95	1.030049	192.168.137.146	54.243.121.164	TCP	66	[TCP Dup ACK 93#2] 50027 > https [ACK] Seq=185 Ack=3034 win=130800 Len=0 TSval=80733857...
96	1.030471	54.243.121.164	192.168.137.146	TLVSLv2	1454	Server Hello
97	1.030789	54.243.121.164	192.168.137.146	TLVSLv2	1454	[TCP Retransmission] Server Hello
98	1.030817	54.243.121.164	192.168.137.146	TLVSLv2	1454	[TCP Retransmission] Server Hello

Version: TLS 1.2 (0x0303)

Random

Session ID Length: 32

Session ID: 3c65bf815417772ca530e32df845ffe1b78ea6f878e5a92...

Cipher Suites: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0x0027)

Compression Method: null (0)

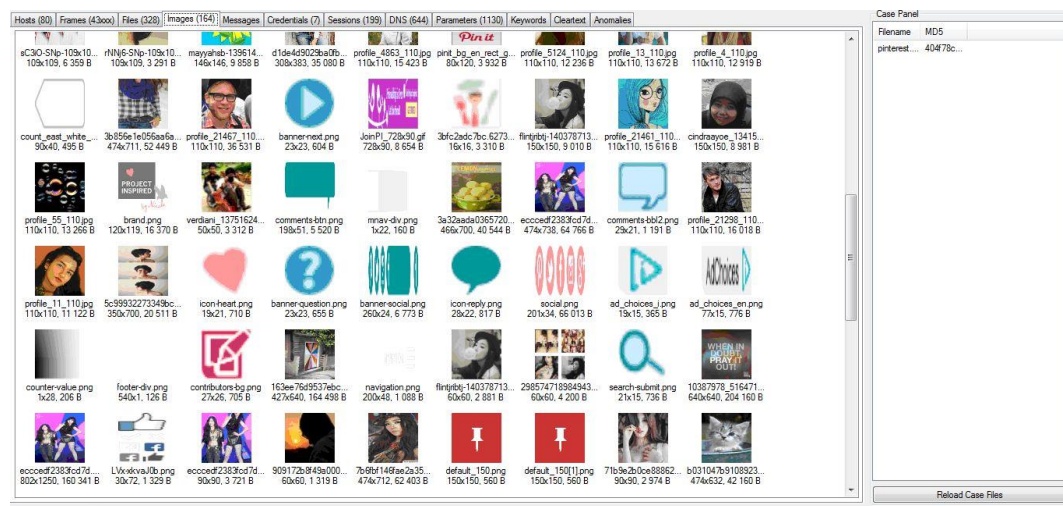
```

0000 86 a5 87 8e 5a 92 ee 19 3f 1c 41 d7 7e 70 43 00 00  ....Z...7-A-...
0090 00 00 0d ff 01 00 01 00 00 00 0a 04 03 00 01 02  ....
00c0 16 03 03 04 1b 0b 0c 0a 17 00 0a 14 00 05 59 30  ....
0130 82 53 30 82 3d 3d 00 00 00 00 00 00 00 00 00 00  ....
01c0 74 32 4e 1f 7b ce df 03 70 28 8b 3f a7 0d 30 10  t2N...p...o...
0230 0069 29 a8 48 86 ff 0d 01 01 0b 05 00 30 70 31  ...H...Op1
0280 30 00 06 03 55 04 06 13 02 55 53 31 30 13 00  ...U...U513
0330 00f0 06 03 55 04 04 1c 04 69 67 69 43 65 72 7a 20  ...U...d igtCrt
0380 49 6e 63 31 19 30 17 0c 05 55 04 03 10 77 77  incl...U...mw
0430 77 2e 64 69 67 69 63 65 74 2e 63 6f 6d 3f 2f  ...digitCrt.com
0480 30 20 03 05 03 03 13 26 44 69 67 69 43 65 72 0  ...U...d igtCrt
0530 74 20 5d 48 41 32 20 48 67 68 20 41 73 73 73  t SHA2 H High Assu
0580 77 61 61 63 65 30 63 65 67 76 72 70 41 50 10  ...

```

Gambar 4. 19 Handshake protocol Pinterest

Dari hasil penangkapan lalu lintas data pada pinterest, penguji mendapatkan gambar yang penguji dan user pinterest lain *upload*. Gambar yang didapat ada juga icon yang memang ada pada aplikasi pinterest. Berikut akan ditampilkan hasil gambar yang berhasil ditangkap.



Gambar 4. 20 Tampilan tab images Pinterest

Berikut hasil yang dapat disimpulkan dari hasil tangkapan pinterest mengacu pada fitur yang ada.

Tabel 4. 4 Tabel informasi Pinterest

Text	Photo	Locations	Notifications
×	✓	×	×

✓ (jika didapatkan hasil) dan × (jika tidak didapatkan hasil)

Tampilan dari isi table di atas merupakan hasil yang didapatkan dari proses penangkapan lalu lintas data. Ketika proses *upload* photo dilakukan photo yang di *upload* berhasil tertangkap, photo yang ada pada halaman home pinterest juga tertangkap. Namun pada proses *upload* locations dan memberikan comments tidak berhasil ditangkap. Adanya hasil demikian ditandai dengan tanda silang yang diberikan penguji di dalam tabel *checklist* tersebut.

4.2.5 Tumblr

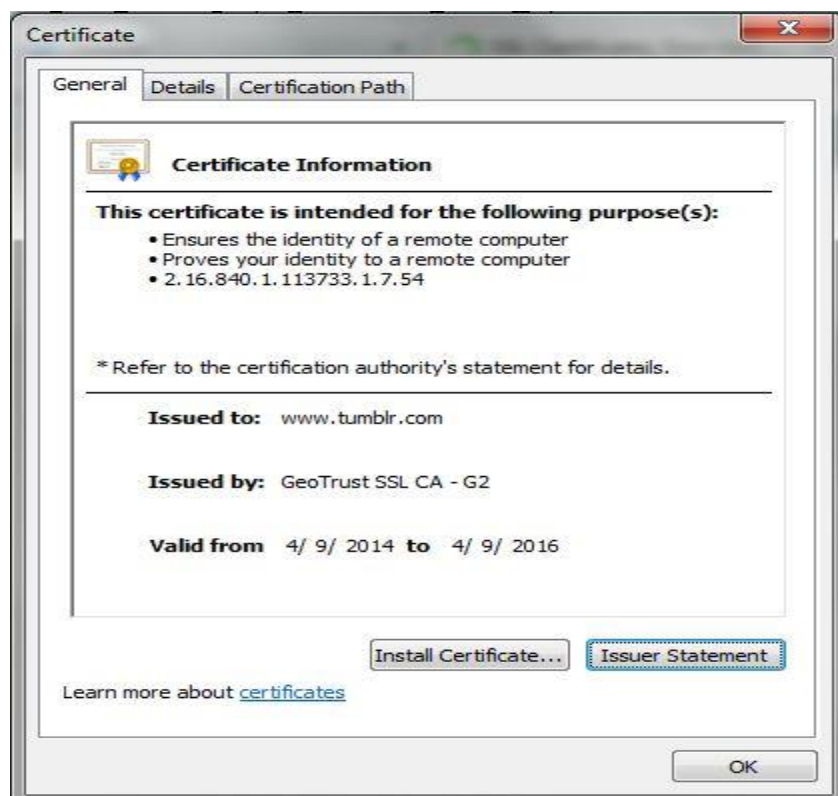
Pada aplikasi Tumblr diperoleh paket data sebanyak 42081. Dari hasil tangkapan paket lalu lintas data tumblr dan setelah dibuka menggunakan network miner diketahui bahwa ada 114 files, 55 diantaranya adalah file *images* user Tumblr. Berikut akan ditampilkan tab files pada Tumblr.

Hosts (53) Frames (4200) Files (114) Images (55) Messages Credentials (6) Sessions (90) DNS (396) Parameters (546) Keywords Cleartext Anomalies												Case Panel	
Frame nr.	Reconn.	Source	S. port	Destinat.	D. port	Protocol	Filename	Extension	Size	Timestamp	Details	Filename	MD5
13532	C:\User...	66.6.40...	TCP 443	192.168...	TCP 50...	TlsCertf...	www.tumblr.com.cer	cer	1 226 B	6/28/2014 ...	TLS Certificate: CN=www.tumblr.c...	tumblr.p...	92067c...
13532	C:\User...	66.6.40...	TCP 443	192.168...	TCP 50...	TlsCertf...	GeoTrust SSL CA - G2.cer	cer	1 117 B	6/28/2014 ...	TLS Certificate: CN=GeoTrust SS...		
13532	C:\User...	66.6.40...	TCP 443	192.168...	TCP 50...	TlsCertf...	GeoTrust Global CA.cer	cer	897 B	6/28/2014 ...	TLS Certificate: CN=GeoTrust Glo...		
24976	C:\User...	66.6.40...	TCP 443	192.168...	TCP 50...	TlsCertf...	www.tumblr.com.cer	cer	1 226 B	6/28/2014 ...	TLS Certificate: CN=www.tumblr.c...		
24976	C:\User...	66.6.40...	TCP 443	192.168...	TCP 50...	TlsCertf...	GeoTrust SSL CA - G2.cer	cer	1 117 B	6/28/2014 ...	TLS Certificate: CN=GeoTrust SS...		
24976	C:\User...	66.6.40...	TCP 443	192.168...	TCP 50...	TlsCertf...	GeoTrust Global CA.cer	cer	897 B	6/28/2014 ...	TLS Certificate: CN=GeoTrust Glo...		
32592	C:\User...	118.98...	TCP 443	192.168...	TCP 50...	TlsCertf...	google.com.cer	cer	1 859 B	6/28/2014 ...	TLS Certificate: CN="+google.com...		
32592	C:\User...	118.98...	TCP 443	192.168...	TCP 50...	TlsCertf...	Google Internet Authority.cer	cer	1 032 B	6/28/2014 ...	TLS Certificate: CN=Google Intern...		
32592	C:\User...	118.98...	TCP 443	192.168...	TCP 50...	TlsCertf...	GeoTrust Global CA.cer	cer	897 B	6/28/2014 ...	TLS Certificate: CN=GeoTrust Glo...		
32961	C:\User...	66.6.40...	TCP 443	192.168...	TCP 50...	TlsCertf...	www.tumblr.com[1].cer	cer	1 226 B	6/28/2014 ...	TLS Certificate: CN=www.tumblr.c...		
32961	C:\User...	66.6.40...	TCP 443	192.168...	TCP 50...	TlsCertf...	GeoTrust SSL CA - G2[1].cer	cer	1 117 B	6/28/2014 ...	TLS Certificate: CN=GeoTrust SS...		
32961	C:\User...	66.6.40...	TCP 443	192.168...	TCP 50...	TlsCertf...	GeoTrust Global CA[1].cer	cer	897 B	6/28/2014 ...	TLS Certificate: CN=GeoTrust Glo...		
34413	C:\User...	74.6.16...	TCP 443	192.168...	TCP 50...	TlsCertf...	zenfs.com.cer	cer	793 B	6/28/2014 ...	TLS Certificate: CN="+zenfs.com...		
35692	C:\User...	118.98...	TCP 443	192.168...	TCP 55...	TlsCertf...	www.google.com.cer	cer	1 146 B	6/28/2014 ...	TLS Certificate: CN=www.google...		
35692	C:\User...	118.98...	TCP 443	192.168...	TCP 55...	TlsCertf...	Google Internet Authority.cer	cer	1 032 B	6/28/2014 ...	TLS Certificate: CN=Google Intern...		
35692	C:\User...	118.98...	TCP 443	192.168...	TCP 55...	TlsCertf...	GeoTrust Global CA.cer	cer	897 B	6/28/2014 ...	TLS Certificate: CN=GeoTrust Glo...		
35723	C:\User...	118.98...	TCP 443	192.168...	TCP 55...	TlsCertf...	google.com.cer	cer	1 859 B	6/28/2014 ...	TLS Certificate: CN="+google.com...		
35723	C:\User...	118.98...	TCP 443	192.168...	TCP 55...	TlsCertf...	Google Internet Authority[1].cer	cer	1 032 B	6/28/2014 ...	TLS Certificate: CN=Google Intern...		
35723	C:\User...	118.98...	TCP 443	192.168...	TCP 55...	TlsCertf...	GeoTrust Global CA[1].cer	cer	897 B	6/28/2014 ...	TLS Certificate: CN=GeoTrust Glo...		
35777	C:\User...	173.194...	TCP 443	192.168...	TCP 55...	TlsCertf...	ssl.google-analytics.com.cer	cer	1 297 B	6/28/2014 ...	TLS Certificate: CN=ssl.google-an...		
35777	C:\User...	173.194...	TCP 443	192.168...	TCP 55...	TlsCertf...	Google Internet Authority.cer	cer	1 032 B	6/28/2014 ...	TLS Certificate: CN=Google Intern...		
35777	C:\User...	173.194...	TCP 443	192.168...	TCP 55...	TlsCertf...	GeoTrust Global CA.cer	cer	897 B	6/28/2014 ...	TLS Certificate: CN=GeoTrust Glo...		
37350	C:\User...	66.6.40...	TCP 443	192.168...	TCP 50...	TlsCertf...	www.tumblr.com[2].cer	cer	1 226 B	6/28/2014 ...	TLS Certificate: CN=www.tumblr.c...		
37350	C:\User...	66.6.40...	TCP 443	192.168...	TCP 50...	TlsCertf...	GeoTrust SSL CA - G2[2].cer	cer	1 117 B	6/28/2014 ...	TLS Certificate: CN=GeoTrust SS...		
37350	C:\User...	66.6.40...	TCP 443	192.168...	TCP 50...	TlsCertf...	GeoTrust Global CA[2].cer	cer	897 B	6/28/2014 ...	TLS Certificate: CN=GeoTrust Glo...		
41754	C:\User...	66.6.40...	TCP 443	192.168...	TCP 50...	TlsCertf...	www.tumblr.com[3].cer	cer	1 226 B	6/28/2014 ...	TLS Certificate: CN=www.tumblr.c...		
41754	C:\User...	66.6.40...	TCP 443	192.168...	TCP 50...	TlsCertf...	GeoTrust SSL CA - G2[3].cer	cer	1 117 B	6/28/2014 ...	TLS Certificate: CN=GeoTrust SS...		
41754	C:\User...	66.6.40...	TCP 443	192.168...	TCP 50...	TlsCertf...	GeoTrust Global CA[3].cer	cer	897 B	6/28/2014 ...	TLS Certificate: CN=GeoTrust Glo...		
7228	C:\User...	125.160...	TCP 80	192.168...	TCP 50...	HttpGet...	tumblr_n7on30mg.gif	gif	68 785 B	6/28/2014 ...	37.media.tumblr.com/fd5d599951...		
8941	C:\User...	192.229...	TCP 80	192.168...	TCP 50...	HttpGet...	tumblr_n72u7o1u45.gif	gif	277 591	6/28/2014 ...	38.media.tumblr.com/8842215a1d...		
8969	C:\User...	192.229...	TCP 80	192.168...	TCP 50...	HttpGet...	tumblr_n72u7o1u45[1].gif	gif	277 591	6/28/2014 ...	38.media.tumblr.com/8842215a1d...		
8942	C:\User...	125.160...	TCP 80	192.168...	TCP 50...	HttpGet...	tumblr_n60noekH.gif	gif	561 292	6/28/2014 ...	37.media.tumblr.com/8cb41d111e...		
8940	C:\User...	125.160...	TCP 80	192.168...	TCP 50...	HttpGet...	tumblr_n60noekH[1].gif	gif	561 292	6/28/2014 ...	37.media.tumblr.com/8cb41d111e...		
17006	C:\User...	125.160...	TCP 80	192.168...	TCP 50...	HttpGet...	tumblr_n72u7o1u45[2].gif	gif	65 965 B	6/28/2014 ...	37.media.tumblr.com/8cb41d111e...		

Reload Case Files

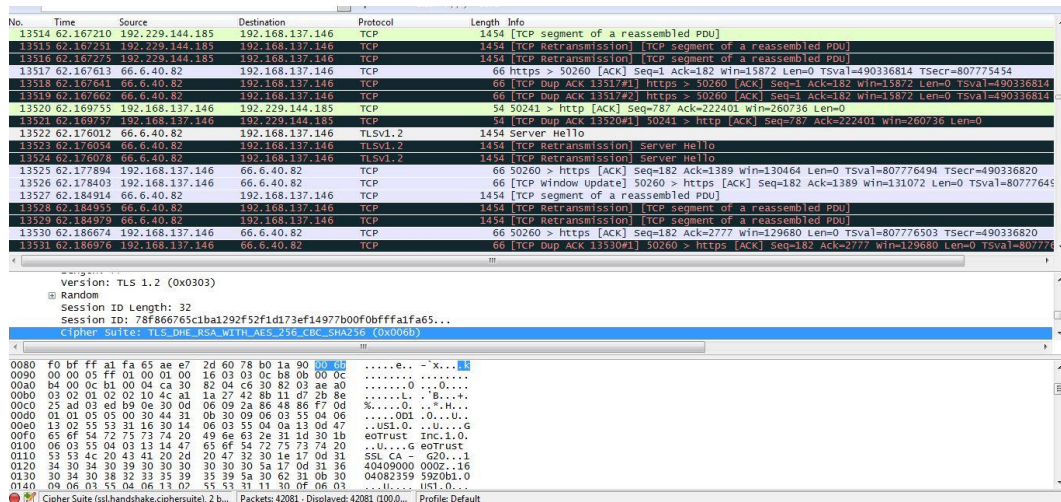
Gambar 4. 21 Tampilan tab files Tumblr

Pada hasil tangkapan Tumblr didapatkan juga sertifikat milik Tumblr yang akan ditampilkan pada gambar di bawah ini.

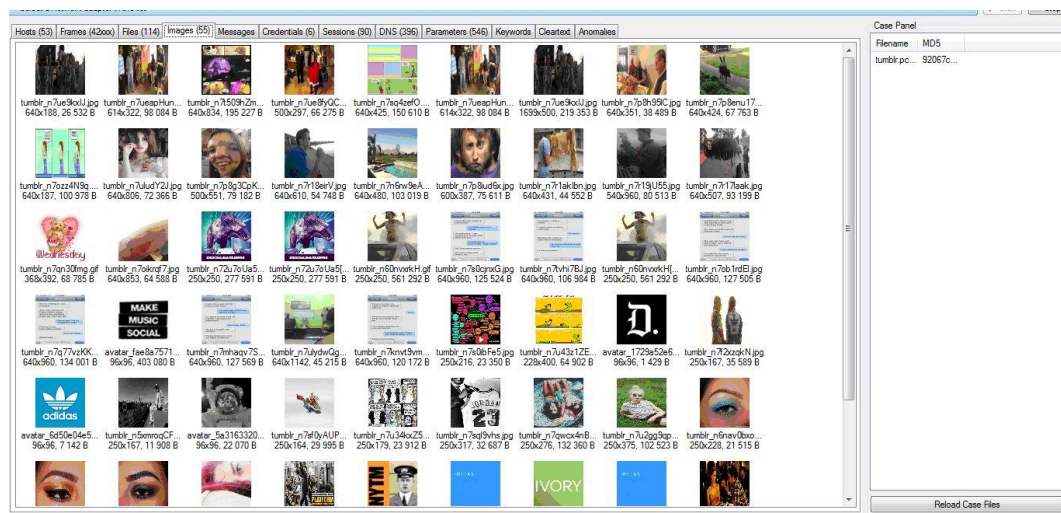


Gambar 4. 22 Sertifikat Tumblr

Tumblr menggunakan TLSv1.2 dalam pengamanan koneksinya, data dienkripsi dengan menggunakan AES 256bit seperti terlihat pada gambar di bawah ini.



Gambar 4. 23 Handshake protocol Tumblr



Gambar 4. 24 Tampilan tab images Tumblr

Dari hasil tangkapan tumblr didapat 55 images, images tersebut berekstensi JPG, PNG, GIF. Gambar yang user Tumblr upload berekstensi JPG dan GIF dengan penamaan menggunakan kata “tumblr_” didepan nama file, sedangkan untuk file avatar

atau *profile picture* dari *user* Tumblr menggunakan kata “avatar_” didepan nama file dengan ekstensi file untuk avatar adalah PNG.

Berikut hasil yang dapat disimpulkan dari hasil tangkapan tumblr mengacu pada fitur yang ada.

Tabel 4. 5 Tabel informasi Tumblr

Text	Profil Picture	Photo	Video	Link
×	✓	✓	×	×

✓ (jika didapatkan hasil) dan × (jika tidak didapatkan hasil)

Tampilan dari isi table di atas merupakan hasil yang didapatkan dari proses penangkapan lalu lintas data. Ketika proses *upload* photo dilakukan photo yang di *upload* berhasil tertangkap, photo yang ada pada halaman dashboard tumblr juga tertangkap. Namun pada proses *upload* teks, video dan link tidak berhasil ditangkap. Adanya hasil demikian ditandai dengan tanda silang yang diberikan penguji di dalam tabel *checklist* tersebut.

4.3 Hasil Akhir

Dari proses-proses yang sudah dikerjakan, didapatkan hasil berupa kesimpulan-kesimpulan berikut ini.

4.3.1 Metode Pengamanan

Pada kelima aplikasi media sosial yang digunakan kemudian telah dilakukan percobaan diketahui bahwa tiga dari aplikasi media sosial masih menggunakan TLSv1, dan dua yang lain sudah menggunakan TLSv1.2., Aplikasi yang sudah menggunakan TLSv1.2 adalah Pinterest dan Tumblr. *Transport Layer Security* (TLS) merupakan protokol yang menjamin privasi komunikasi aplikasi dan pengguna di Internet.

Aplikasi iMessage dan Wechat menggunakan RC4 dengan panjang kunci 128 bit, aplikasi Pinterest dan Tango menggunakan enkripsi AES dengan panjang kunci 128 bit. Untuk aplikasi Tumblr menggunakan enkripsi AES dengan panjang kunci 256 bit.

Hal ini ditemukan pada sertifikat dan pembacaan pada file dari hasil penangkapan lalu lintas data yang dilakukan oleh penguji.

4.3.2 Informasi yang Didapatkan

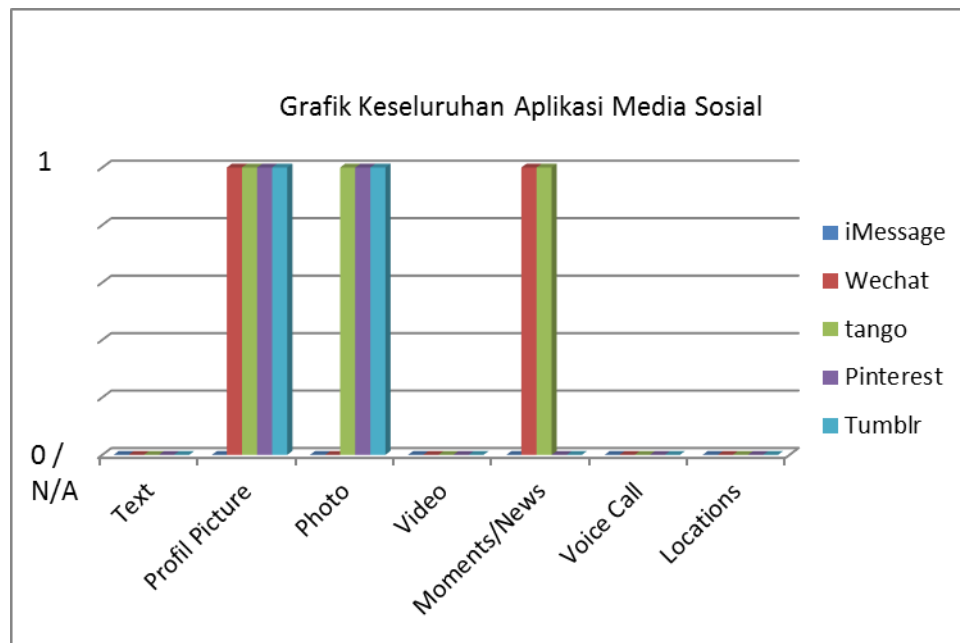
Berdasarkan pada proses penangkapan data yang dilakukan dengan menggunakan aplikasi pendukung, didapatkan informasi bahwa dari semua aplikasi berhasil menangkap file berupa gambar kecuali pada iMessage. Gambar yang didapatkan kebanyakan merupakan gambar dari file yang sudah dilakukan proses *upload* oleh penguji, gambar yang berada pada halaman home aplikasi dan juga gambar yang dijadikan *profil picture* oleh penguji dan pengguna lain.

Sedangkan untuk file teks dan video tidak berhasil ditangkap karena diamankan dengan menggunakan enkripsi, dan juga paket data yang ditangkap berupa HTTPS.

Tabel 4. 6 Perbandingan hasil Tangkapan lalu lintas data

Fitur	iMessage	Wechat	Tango	Pinterest	Tumblr
Text	×	×	×	×	×
Profil Picture	×	✓	✓	✓	✓
Photo	×	×	✓	✓	✓
Video	×	×	×	N/A	×
Moments/News	N/A	✓	✓	N/A	N/A
Voice Call	N/A	×	×	N/A	N/A
Locations	N/A	×	×	×	N/A

✓ (jika didapatkan hasil), × (jika tidak didapatkan hasil), N/A (fitur tidak tersedia)



1 (jika didapatkan hasil), 0 (jika tidak didapatkan hasil), N/A (fitur tidak tersedia)

Gambar 4. 25 Grafik perbandingan aplikasi

Dari hasil grafik yang dibuat sesuai tabel hasil penangkapan lalu lintas data, terlihat bahwa tidak ada pesan teks yang tertangkap sama sekali dari kelima aplikasi yang diteliti. Untuk profil picture aplikasi Wechat, Tango, Pinterest dan Tumblr semua tertangkap pada saat proses penangkapan data, sedangkan untuk iMessage tidak berhasil didapat karena fitur tersebut tidak tersedia.

Kemudian pada grafik photo, di sana terlihat ada tiga aplikasi yang tertangkap ketika mengirimkan photo atau melakukan *upload* photo. Pada iMessage dan Wechat photo yang dikirimkan ke pengguna lain tidak berhasil tertangkap, sedangkan pada Tango, Pinterest dan Tumblr berhasil ditangkap ketika proses penangkapan lalu lintas data.

Pada fitur *video*, hanya empat aplikasi yang bisa dicoba melakukan proses *upload video* karena pada pinterest tidak bisa melakukan *upload video*. Dan dari hasil *upload video* empat aplikasi yang lain, tidak ada file *video* yang berhasil ditangkap.

Sedangkan pada fitur *moments/news* dilakukan percobaan penangkapan pada aplikasi Wechat dan Tango karena fitur ini hanya ada pada dua aplikasi tersebut. Ketika dilakukan update *moments/news*, file gambar yang berhasil ditangkap namun untuk update *moments/news* berupa teks tidak ada pesan teks yang tertangkap.

Pada fitur *voice call* yang hanya terdapat pada aplikasi Wechat dan Tango, tidak berhasil ditemukan apapun. Seperti terlihat pada grafik, tidak ada grafik yang menjulang pada bagian *voice call*. Begitu juga pada fitur *locations* yang tersedia pada aplikasi Wechat, Tango dan Pinterest, tidak berhasil ditemukan apapun.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

1. Pada aplikasi iMessage, Wechat, dan Tango menggunakan koneksi TLS versi 1.0, sedangkan pada aplikasi Pinterest dan Tumblr menggunakan TLS versi 1.2 dan pertukaran kunci menggunakan algoritma kunci publik RSA dengan panjang kunci 2048 bit.
2. Berdasarkan pada hasil uji coba pada proses penangkapan lalu lintas data, data yang didapatkan bukanlah informasi yang berbahaya bagi pengguna aplikasi terkait. Informasi yang diperoleh hanya berupa gambar, seperti gambar yang didapatkan dari profil picture pengguna dan profil picture milik pengguna lain. Pada iMessage dan Wechat tidak didapatkan gambar yang dikirim oleh pengguna ke pengguna lain.
3. Metode enkripsi untuk keamanan data yang digunakan pada aplikasi iMessage dan Wechat menggunakan RC4 dengan panjang kunci 128 bit, aplikasi Pinterest dan Tango menggunakan enkripsi AES dengan panjang kunci 128 bit. Sedangkan aplikasi Tumblr menggunakan enkripsi AES dengan panjang kunci 256 bit.

5.2 Saran

Berdasarkan hasil penelitian dan pengujian yang telah dilakukan oleh penulis, penulis memiliki beberapa saran yang ingin disampaikan apabila nantinya ada yang ingin melakukan penelitian lebih mendalam mengenai judul ini. Ada pun saran yang ingin diberikan adalah peneliti lainnya diharapkan dapat melakukan percobaan yang sama dengan menggunakan platform yang berbeda.

Selain itu diharapkan dapat melakukan percobaan dengan cara yang berbeda untuk mendapatkan hasil yang sama atau bahkan bisa mendapatkan hasil yang lebih dengan berdasarkan pada acuan penggunaan fitur yang sama. Kemudian peneliti lainnya diharapkan juga mampu untuk mendapatkan informasi mengenai jenis metode enkripsi

yang digunakan pada tiap-tiap aplikasi untuk mengamankan percakapan yang dilakukan. Selain metode enkripsi, diharapkan juga peneliti lainnya mampu melakukan dekripsi terhadap pesan yang telah dienkripsi oleh aplikasi-aplikasi yang diteliti.

DAFTAR PUSTAKA

- Inveatech. (2008, Oktober 12). Diakses pada September 11, 2014, dari
https://www.invea.com/img/monitoring_web_2.jpg
- Kristanto, A. (2003). *Keamanan Data Pada Jaringan Komputer*. Yogyakarta: GAVA MEDIA.
- Kurniawan, A. (2012). *Network Forensics Panduan Analisis & Investigasi Paket Data Jaringan Menggunakan Wireshark*. Yogyakarta: ANDI OFFSET.
- Kurniawan, Y. (2004). *Kriptografi Keamanan Internet dan Jaringan Telekomunikasi*. Bandung: Informatika Bandung.
- Netresec. (2010). Diakses pada September 11, 2014, dari
<http://www.netresec.com/?page=NetworkMiner>
- Permana, R. S. (2013, Februari 9). Diakses pada Mei 14, 2014, dari
<http://regasetiadipermana.wordpress.com/2013/02/09/keamanan-jaringan/>
- Sanusi, A. (2013, Januari 14). Diakses pada Mei 14, 2014, dari
<http://sanusiadam79.wordpress.com/2013/01/14/sosial-media-dan-sosial-network/>

LAMPIRAN