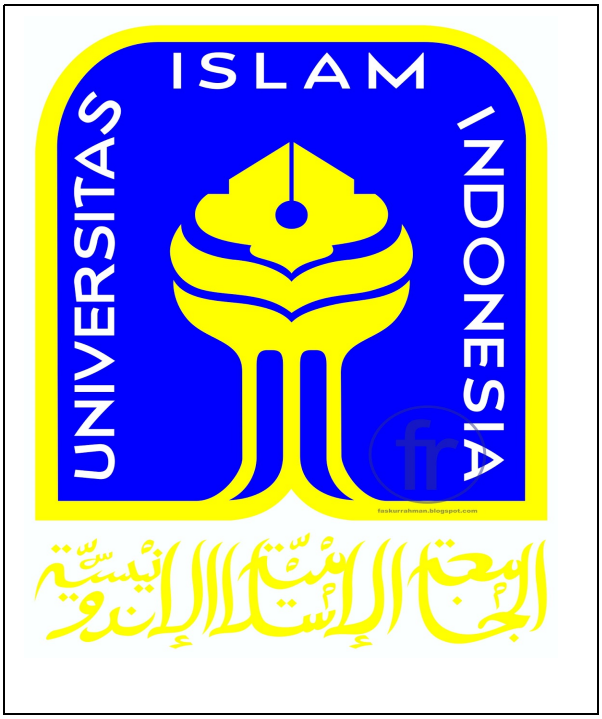
MANAJEMEN INVESTIGASI TINDAK KRIMINAL

LAPORAN INVESTIGASI

PEMERIKSAAN FORENSIK BUKTI DIGITAL TERHADAP KASUS ANN

Dosen Pengampu : Yudi Prayudi, M.Kom



oleh :

Andrian Sah 12917221

PROGRAM PASCA SARJANA TEKNIK INFORMATIKA

UNIVERSITAS ISLAM INDONESIA YOGYAKARTA

2015

DAFTAR ISI

1. IDENTITAS KASUS

a. Deskripsi Kasus

Kasus berawal dari Ann dan Mr X yang mendirikan basis baru operasi mereka. Baru-baru ini, Ann mendapat merek *AppleTV* baru, dan dikonfigurasi dengan alamat IP statik 192.168.1.10 yang kemudian melakukan aktivitas terhadap *AppleTV* barunya tersebut.

b. Ringkasan Kasus

a. Pemohon	Bp. Hamid, M.Eng dkk dari IT Centrum Universitas Islam Indonesia
b. Alamat Pemohon	Jl. Lingkar Utara Condong Catur, Depok, Sleman, Yogyakarta - 55283
c. Yang menerima	Andrian Sah (Lab. Digital Forensika Teknik Informatika UII)
d. Waktu	Sabtu 12 Agustus 2015, Pukul 13.30 WIB
e. Nomor Kasus	K007/MITK/VIII/2015

2. DESKRIPSI PERMOHONAN INVESTIGASI :

- Diajukan barang bukti berupa file *packet capture traffic* dengan ekstensi *.pcap* bernama *evidence03.pcap*, terkait dengan kejadian perkara yang melibatkan Ann and Mr. X yang sedang menjalani pemeriksaan perkara pidana di salah satu Pengadilan Negeri Meksiko.
- Awalnya investigator melakukan *packet capture* terhadap aktivitas Ann secara diam-diam, yang kemudian menghasilkan sebuah *file* yang selanjutnya dijadikan barang bukti digital dan diminta untuk diteliti dan dianalisa, sehingga didapat informasi sbb :
  a. Alamat *MAC* dari Ann di *Apple TV*.
  b. *User-Agent string* yang digunakan oleh Ann di *Apple TV* melalui permintaan *HTTP*.
  c. Empat istilah pertama yang dicari oleh Ann di *Apple TV*.
  d. Judul film pertama yang diklik oleh Ann.
  e. Alamat *URL* lengkap pada *movie trailer* yang diklik oleh Ann.
  f. Judul film kedua yang diklik oleh Ann.
  g. Jumlah harga untuk membeli film.
  h. Istilah terakhir yang dicari oleh Ann.

3. PROSES PENERIMAAN BARANG BUKTI

a. Barang bukti yang akan diuji dikirimkan oleh pemohon melalui sebuah *flashdisk* dan ditujukan kepada Lab. Forensika Digital Teknik Informatika UII yang kemudian dilanjutkan pada penerima untuk diproses lebih lanjut. Pada *flashdisk* yang diterima terdapat sebuah folder yang berisi 2 buah file, yaitu sebagai berikut :

1. File "*evidence03.pcap*"

2. File "*question03*"

b. Barang bukti File yang dikirimkan tersebut tidak disertai dengan kunci hash.

4. PROSES EKSAMINASI BARANG BUKTI

a. Team

Dibentuk tim investigasi berdasarkan surat no xxxxx dengan susunan team adalah sbb :

- Lead Examiner : Andrian Sah
- Co Examiner : Hamid dan Fietyata Yudha

b. Prosedur

1. Melakukan peng-*copy*-an file yang diterima dari *flashdisk* untuk kemudian disimpan dalam komputer Lab Forensika Digital Teknik Informatika UII.
2. Menyiapkan *environment system* untuk keperluan eksaminasi pada Lab. Forensika Digital Teknik Informatika yang berada pada area pusat pelatihan ITCentrum FTI UII.
3. Mengunakan sebuah aplikasi untuk kepentingan melihat isi file serta informasi digital lainnya dari file *packet traffic* tersebut. Dalam hal ini aplikasi yang digunakan adalah : *Wireshark-win32-1.12.4*
4. File *traffic* yang diterima memiliki jumlah *frame* yang sangat banyak sehingga satu demi satu dianalisis kemudian dibuatkan screen shoot yang mengarahkan pada temuan yang dikehendaki sesuai dengan target informasi yang diharapkan.
5. Melakukan expose hasil baik secara internal team maupun eksternal kepada pihak pemohon.

c. Waktu dan Tempat

1. Proses Eksaminiasi dilakukan pada hari Sabtu 12 Agustus 2015 jam 13.30 - 17.00 WIB.
2. Tempat proses eksaminasi adalah Laboratorium Forensika Digital Teknik Informatika yang berada pada area pusat pelatihan ITCentrum FTI UII Yogyakarta.

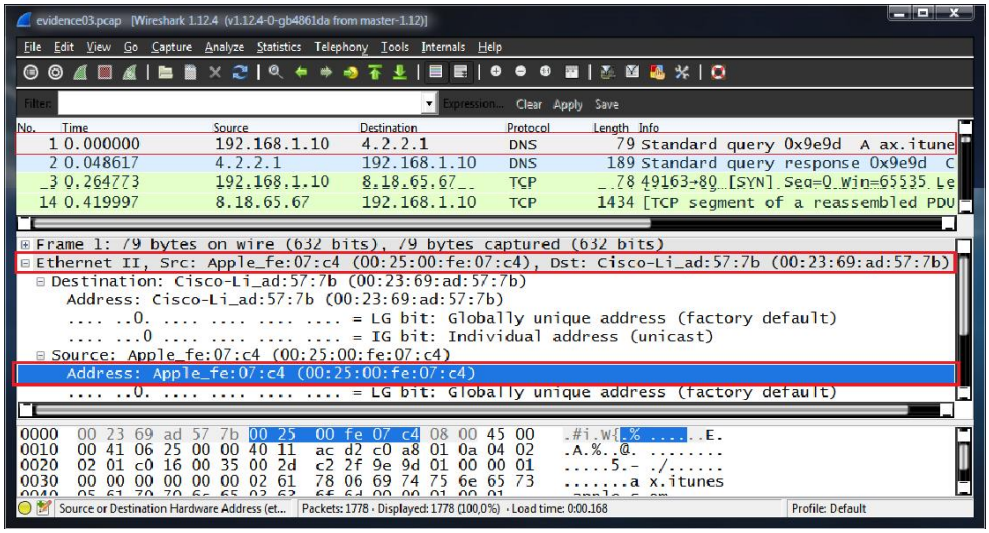
5. HASIL EKSAMINASI

a. Alamat *MAC* dari Ann di *Apple TV*.

Alamat *MAC* didapat dengan menggunakan aplikasi *Wireshark-win32-1.12.4*. Proses yang dilakukan adalah sebagai berikut :

- Pertama – tama membuka file *capture traffic* menggunakan aplikasi *Wireshark-win32-1.12.4*.
- Kemudian dilakukan processing evidence terhadap file tersebut. Diketahui Ann merupakan *source* yang memiliki IP address 192.168.1.10, maka untuk melihat alamat *MAC* dari Ann kita dapat merujuk pada detail dari *header* frame pertama, dari jendela detail frame tersebut kita dapat melihat pada

  Ethernet II, Src: Apple_fe:07:c4 (00:25:00:fe:07:c4), Dst: Cisco-Li_ad:57:7b (00:23:69:ad:57:7b). Secara detail kita dapat melihat pada alamat dari *source* tersebut, yaitu: *Address: Apple_fe :07:c4 (00:25:00:fe:07c4)*

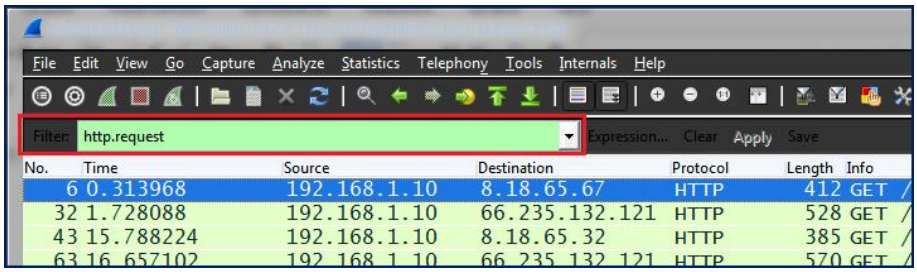


- Dari penjelasan poin diatas maka dapat disimpulkan bahwa *MAC address* yang dimiliki oleh Ann di *Apple TV* adalah ***00:25:00:fe:07:c4***.

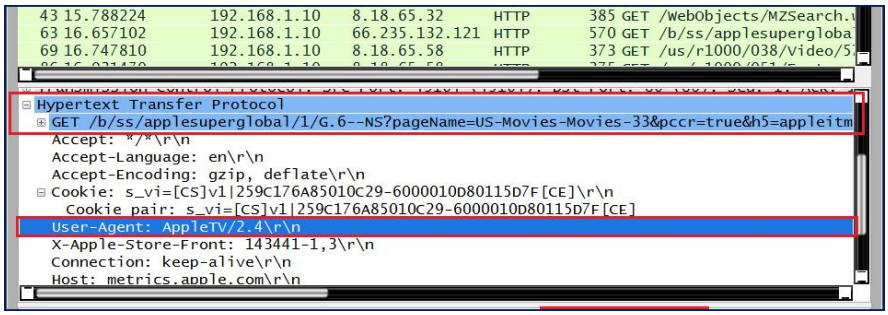
a. *User-Agent string* yang digunakan oleh Ann di *Apple TV* melalui permintaan *HTTP*.

Dalam melakukan proses pencarian di alamat *HTTP*, Ann menggunakan *Uses-Agent*. Untuk mengetahui informasi *Uses-Agent* yang dimiliki oleh Ann, maka kita dapat melakukan dengan cara sebagai berikut :

- Pertama-tama kita harus menemukan frame-frame mana yang dilakukan - *HTTP requests* yaitu dengan mengetik perintah *http.request* pada kotak *Filter* kemudian tekan tombol *Enter* pada *keyboard*, sehingga akan ditemukan deretan frame yang melakukan *HTTP requests*, seperti pada gambar berikut :



- Langkah selanjutnya menemukan *string User-Agent* dari Ann yaitu dengan menggunakan perintah *Find Packet* caranya adalah klik menu *Edit* kemudian klik *Find Packet* atau dengan menekan tombol kombinasi Ctrl + F secara bersamaan. Setelah melakukan perintah diatas maka secara otomatis akan tampil string dari User-Agent yang dicari, perhatikan gambar berikut :

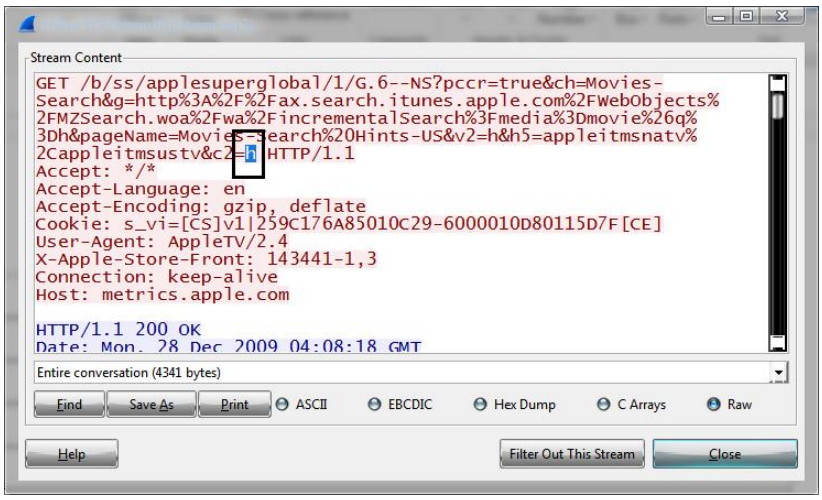


- Berdasarkan gambar diatas maka dapat dilihat pada detail *Hypertext Transfer Protocol* terdapat string *User-Agent* dari Ann yaitu AppleTV/2.4. Jadi dapat disimpulkan bahwa *User-Agent* yang dimiliki oleh Ann di *AppleTV* adalah ***AppleTV/2.4***.

b. Empat istilah pertama yang dicari oleh Ann di *AppleTV*.

Dalam melakukan pencarian di internet, Ann memasukan banyak istilah untuk mendapatkan sesuatu yang diinginkannya. Berdasarkan informasi yang diterima Ann memasukan empat istilah pertama di *AppleTV*. Untuk menemukan keempat istilah pertama tersebut, maka dapat dilakukan dengan cara sebagai beriktu :

- Pertama-tama kita harus menemukan frame-frame mana yang dilakukan pencarian istilah tersebut yaitu dengan mengetik perintah *http.request.uri contains "search"* pada kotak *Filter* kemudian tekan tombol *Enter* pada *keyboard*, sehingga akan ditemukan deretan frame.
- Diketahui *frame* pertama yang melakukan perintah *search* adalah *frame* ke 63, maka untuk mencari empat istilah pertama yang dilakukan oleh Ann Apple TV adalah dengan melakukan perintah *Follow TCP Stream* pada *frame* tersebut.

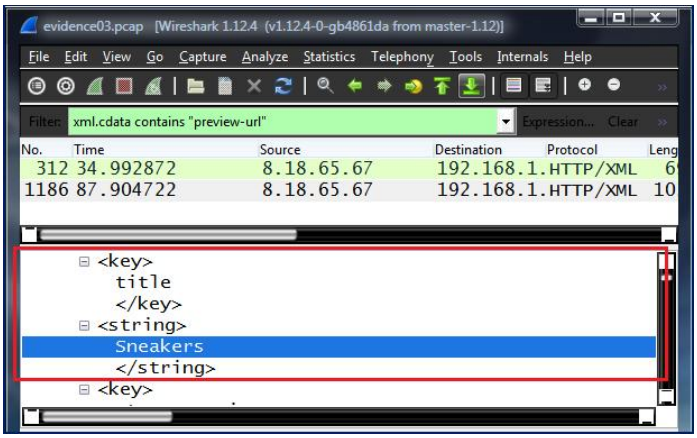


- Berdasarkan hasil temuan dari perintah diatas, maka dapat disimpulkan bahwa empat istilah pertama yang dimaksud adalah ***h***, ***ha***, ***hac***, dan ***hack***.

c. Judul film pertama yang diklik oleh Ann.

Berdasarkan informasi yang didapat bahwa salah satu yang dicari oleh Ann adalah film berdasarkan *preview-url*. Untuk mengetahui apa judul film pertama yang diklik oleh Ann, maka dapat dilakukan dengan cara sebagai berikut :

- Pertama-tama kita harus menemukan frame-frame mana yang memiliki *preview-url* yaitu dengan mengetik perintah *xml.cdata contains "preview-url"* pada kotak *Filter*, sehingga akan ditemukan deretan frame.
- Langkah selanjutnya menemukan *title* dari *preview-url* yaitu dengan menggunakan perintah *Find Packet*. Setelah melakukan perintah tersebut maka secara otomatis akan tampil string dari *preview-url* yang dicari, perhatikan gambar berikut :



- Berdasarkan gambar diatas maka dapat disimpulkan bahwa judul film pertama yang diklik oleh Ann adalah ***sneakers***.

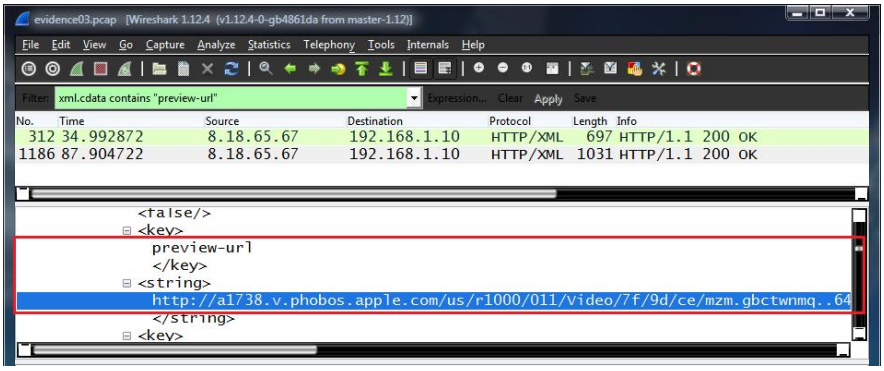
d. Alamat *URL* lengkap pada *movie trailer* yang diklik oleh Ann.

URL singkatan dari *Uniform Resource Locator*, adalah rangkaian karakter

menurut suatu format standar tertentu, yang digunakan untuk menunjukkan

alamat suatu sumber seperti dokumen, video, gambar dan lain – lain di Internet. Berdasarkan informasi yang didapat bahwa Ann mengklik beberapa video dan untuk menemukan alamat *URL* dari video tersebut, maka dapat dilakukan dengan cara sebagai berikut :

- Pertama-tama kita harus menemukan frame-frame mana yang memiliki *preview-url* yaitu dengan mengetik perintah *xml.cdata contains "preview-url"* pada kotak *Filter*, sehingga akan ditemukan deretan frame.
- Langkah selanjutnya menemukan *preview-url* yaitu dengan menggunakan perintah *Find Packet*. Dengan cara mengetikan perintah *preview-url* pada kotak *Find Packet* tersebut. Setelah melakukan perintah tersebut maka secara otomatis akan tampil string dari *preview-url* yang dicari, perhatikan gambar berikut :

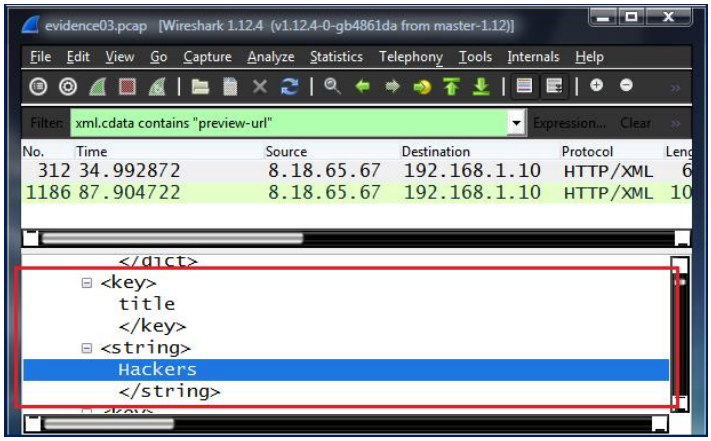


- Berdasarkan gambar diatas maka dapat disimpulkan bahwa alamat *URL* dari film yang diklik oleh Ann adalah
  1. ***http://a227.v.phobos.apple.com/us/r1000/008/Video/62/bd/1b/mzm.plqacyqb..640x278.h264lc.d2.p.m4v***
  2. ***http://a1738.v.phobos.apple.com/us/r1000/011/Video/7f/9d/ce/mzm.gbctwnmq..640x352.h264lc.D2.p.m4v***

f. Judul film kedua yang diklik oleh Ann.

Berdasarkan informasi yang didapat bahwa salah satu yang dicari oleh Ann adalah film berdasarkan *preview-url*. Untuk mengetahui apa judul film kedua yang diklik oleh Ann, maka dapat dilakukan dengan cara sebagai berikut :

- Pertama-tama kita harus menemukan frame-frame mana yang memiliki *preview-url* yaitu dengan mengetik perintah *xml.cdata contains "preview-url"* pada kotak *Filter*, sehingga akan ditemukan deretan frame.
- Langkah selanjutnya menemukan *title* dari *preview-url* yaitu dengan menggunakan perintah *Find Packet*. Setelah melakukan perintah tersebut maka secara otomatis akan tampil judul film pertama, namun karena informasi yang diinginkan adalah judul film kedua yang diklik maka langkah selanjutnya klik *next* pada perintah *Find Packet*, perhatikan gambar berikut :

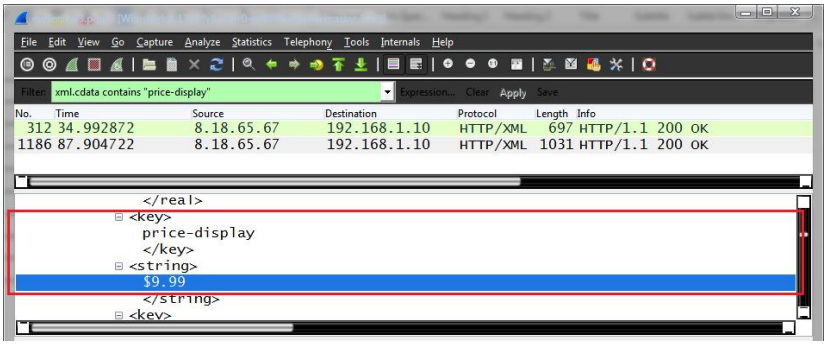


- Berdasarkan gambar diatas maka dapat disimpulkan bahwa judul film kedua yang diklik oleh Ann adalah ***Hackers***.

f. Jumlah harga untuk membeli film.

Dalam pencarian informasi diketahui bahwa dalam permintaan untuk mendapat sebuah film Ann harus membayar uang agar dapat memiliki film yang dimaksud. Untuk mengetahui jumlah harga dari film tersebut adalah dengan cara sebagai berikut :

- Pertama-tama kita harus menemukan frame-frame mana yang memiliki *price-display* yaitu dengan mengetik perintah *xml.cdata contains "price-display"* pada kotak *Filter*, sehingga akan ditemukan deretan frame yang dimaksud.
- Langkah selanjutnya menemukan *price-display* dengan menggunakan perintah *Find Packet*. Setelah melakukan perintah tersebut maka secara otomatis akan tampil daftar harga yang dimaksud, seperti gambar berikut :



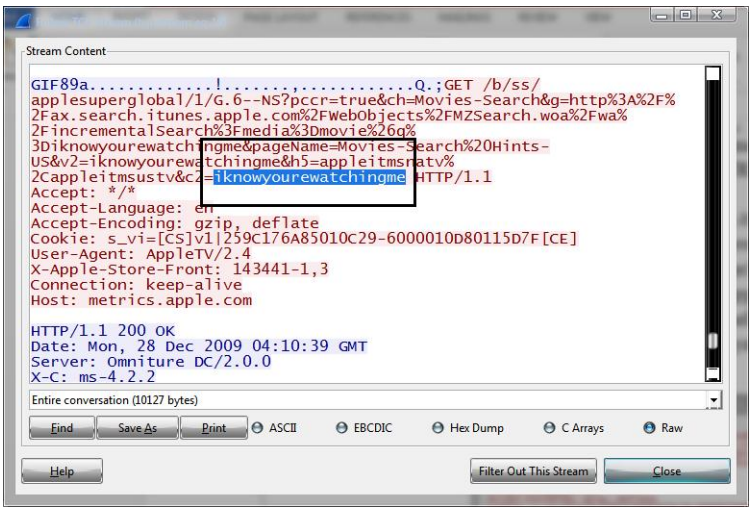
- Berdasarkan gambar diatas maka dapat disimpulkan bahwa jumlah harga yang terdapat pada film tersebut adalah **$9.99**..

g. Istilah terakhir yang dicari oleh Ann.

Dalam melakukan pencarian di internet, Ann memasukan banyak istilah untuk mendapatkan sesuatu yang diinginkannya. Berdasarkan informasi yang diterima Ann memasukan istilah terakhir di *AppleTV*. Untuk menemukan istilah terakhir

tersebut, maka dapat dilakukan dengan cara sebagai beriktu :

- Pertama-tama kita harus menemukan frame-frame mana yang dilakukan pencarian istilah tersebut yaitu dengan mengetik perintah *http.request.uri contains "search"* pada kotak *Filter* kemudian tekan tombol *Enter* pada *keyboard*, sehingga akan ditemukan deretan frame.
- Diketahui *frame* terakhir yang melakukan perintah *search* adalah *frame* ke 1771, maka untuk mencari empat istilah pertama yang dilakukan oleh Ann Apple TV adalah dengan melakukan perintah *Follow TCP Stream* pada *frame* tersebut.



- Berdasarkan hasil temuan dari perintah diatas, maka dapat disimpulkan bahwa istilah terakhir yang dimaksud adalah ***iknowyourewatchingme***.

6. KESIMPULAN AKHIR

1. Berdasarkan hasil analisa yang dilakukan terhadap file tersebut maka diketahui Ann melakukan banyak aktivitas yang berbeda-beda yang jika dihitung dalam bentuk frem maka jumlah frem yang dimilikinya adalah sebanyak 1778 frem dengan alamat IP 192.168.1.10.
2. Dari informasi yang didapat bahwa Ann melakukan pencarian menggunakan beberapa istilah dan mencari beberapa film yang diinginkannya film-film itu diantaranya berjudul sneakers dan hackers

Yogyakarta, 12 Agustus 2015
Jam 17.00
Lead Examiner

Andrian Sah

Co Examiner **Co Examiner**

Hamid **Fietyata Yudha**