REPUBLIK INDONESIA
KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA

SURAT PENCATATAN
CIPTAAN

Dalam rangka pelindungan ciptaan di bidang ilmu pengetahuan, seni dan sastra berdasarkan Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta, dengan ini menerangkan:

Nomor dan tanggal permohonan	:	EC00202305492, 18 Januari 2023
Pencipta		
Nama	:	**Drs. Ir. Faisal Syafar, M.Si., M.InfTech., Ph.D., IPU.**
Alamat	:	BTN Tabaria Tower E10/23 Kelurahan Mannuruki, Kecamatan Tamalate, Makassar, SULAWESI SELATAN, 90221
Kewarganegaraan	:	Indonesia
Pemegang Hak Cipta		
Nama	:	**Drs. Ir. Faisal Syafar, M.Si., M.InfTech., Ph.D., IPU.**
Alamat	:	BTN Tabaria Tower E10/23 Kelurahan Mannuruki, Kecamatan Tamalate, Makassar, SULAWESI SELATAN, 90221
Kewarganegaraan	:	Indonesia
Jenis Ciptaan	:	**Program Komputer**
Judul Ciptaan	:	**SIMULASI SPOOFING CYBER ATTACK BERBASIS EVIL TWIN**
Tanggal dan tempat diumumkan untuk pertama kali di wilayah Indonesia atau di luar wilayah Indonesia	:	17 Januari 2023, di Makassar
Jangka waktu pelindungan	:	Berlaku selama 50 (lima puluh) tahun sejak Ciptaan tersebut pertama kali dilakukan Pengumuman.
Nomor pencatatan	:	000438414

adalah benar berdasarkan keterangan yang diberikan oleh Pemohon.
Surat Pencatatan Hak Cipta atau produk Hak terkait ini sesuai dengan Pasal 72 Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta.

a.n Menteri Hukum dan Hak Asasi Manusia
Direktur Jenderal Kekayaan Intelektual
u.b.
Direktur Hak Cipta dan Desain Industri

Anggoro Dasananto
NIP.196412081991031002

Disclaimer:
Dalam hal pemohon memberikan keterangan tidak sesuai dengan surat pernyataan, Menteri berwenang untuk mencabut surat pencatatan permohonan.

SIMULASI SPOOFING CYBER ATTACK BERBASIS EVIL TWIN

Drs. Ir. Faisal Syafar, M.Si., M.InfTech., Ph.D., IPU

Januari 2023

Simulasi Kasus

Simulasi kasus merupakan proses uji coba terhadap *MITM Based Evil Twin attack* yang dilakukan pada area *hotspot* fakultas Teknik UNM.

Pada skenario ini pelaku akan menggunakan AP palsu untuk menjerat para korban, dan setelah korban terhubung ke dalam AP palsu yang dibuat dengan sengaja, pelaku dan dengan mudah melakukan serangan *MITM* untuk mendapatkan informasi rahasia yang dimiliki korban, seperti yang terlihat pada Gambar 1.

Gambar 1 Scenario *MITM Based Evil Twin*

Pola serangan yang digunakan pelaku adalah dengan melaukan kofigurasi AP palsu yang menggunakan *SSID* yang mirip dengan salah satu *SSID* target di sekitar area *Wifi*, seperti yang terlihat pada Gambar 2.

Gambar 2 Scanario *MITM Based Evil Twin*

Investigasi Forensik

Detection* Dan *Collection Evil Twin

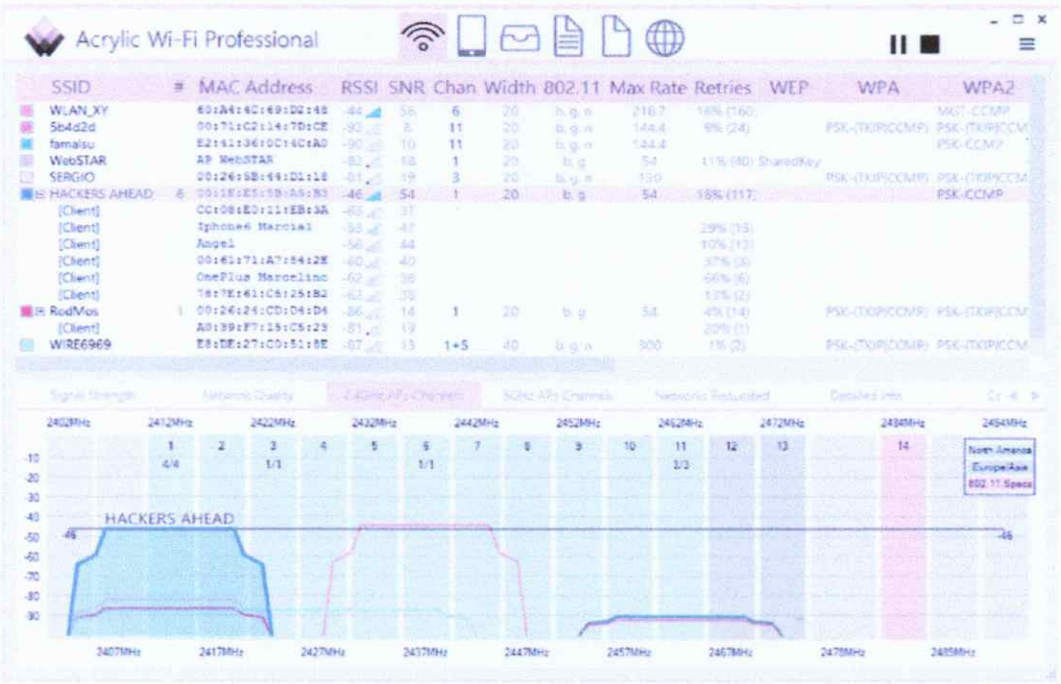
Pada kasus ini proses *scanning* yang dilakukan pada FT UNM, dalam hasil *scanning* dengan jangkauan 100 m terdapat beberapa *SSID* yang dapat ditemukan pada *area* tersebut, antara lainnya *SSID* AP milik FT sendiri seperti Dekanat FT, JPTIK, JPKK, PTP dan beberapa *SSID* yang kemungkinan berasal dari luar FT. Pada Gambar 3, proses *scanning* di *area* tersebut ditemukan adanya ancaman AP palsu dengan *SSID* "pusfid", dengan membaca notifikasi yang diberikan oleh aplikasi Chellam.

Gambar 3 Notifikasi Chellam

Setelah ditemukan notifikasi adanya ancaman AP palsu, peneliti yang bertindak sebagai investigator akan lakukan proses *scanning* lebih lanjut untuk mencari informasi lebih detail tentang accsses point palsu dan penyerang.

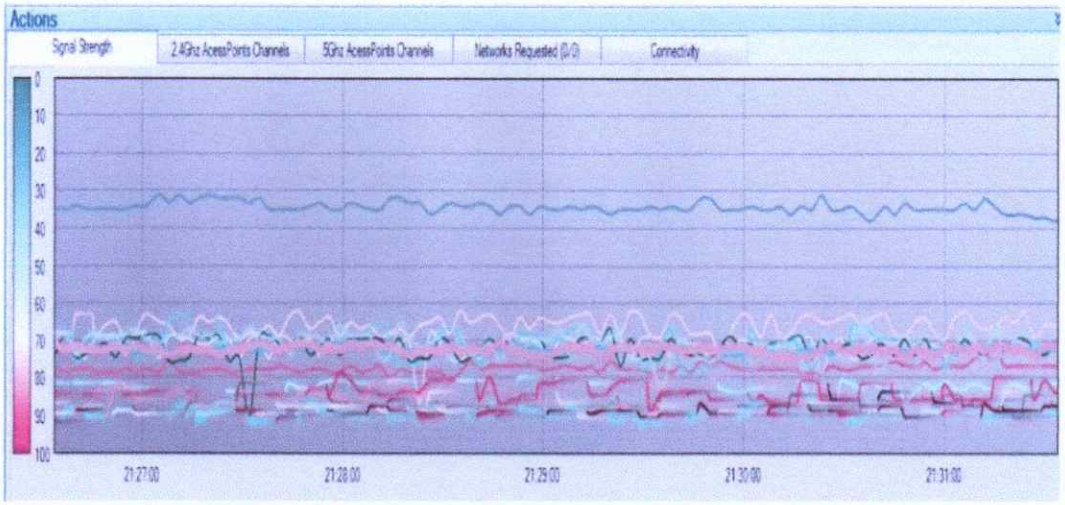
Dari hasil *scanning* ditemukan adanya dua AP yang menggunakan *SSID* "PUSFID", dengan Mac "e3:8d:8b:ca:8f:D1, dengan kode *vendor* : "Mapala.com, dengan kekuatan sinyal -81 db, aunthentikasi :"Rsnapsk", frekuensi 382300 dan *channel* : 1, sedangkan *SSID* kedua dengan Mac: f4:f2:6d:1c:76:15, dengan kode *Vendor* : "Tp-Link technologies.co.ltd", kekuatan sinyal - 34 db, aunthentikasi : "open", frekuensi 241700 dan *channel* : 8. Seperti yang terlihat pada Gambar 4.

Pada Gambar 5 *scanning* dilakukan dengan menggunakan aplikasi bantuan lain yaitu acrlyric-*Wifi*, aplikasi ini digunakan untuk menemukan informasi lebih detail terkait, yang mana berfungsi sebagai aplikasi analisis jaringan *Wifi*, pada hasil *scanning* AP dengan *SSID* : pusfid, diberikan tanda berwana merah muda untuk AP yang menggunakan mac "e4:8d:8c:ca:80:c0, dengan kode *vendor* : "routerboard.com, dengan kekuatan sinyal -74 db, aunthentikasi :"rsnapsk", frekuensi 241200 dan *channel* : 1, sedangkan *SSID* kedua dengan mac: f4:f2:6d:1c:76:15, dengan kode *vendor* : "tp-link technologies.co.ltd", kekuatan sinyal -34 db, aunthentikasi : "*open*", frekuensi 241700 dan *channel* : 8, diberi tanda dengan warna biru.

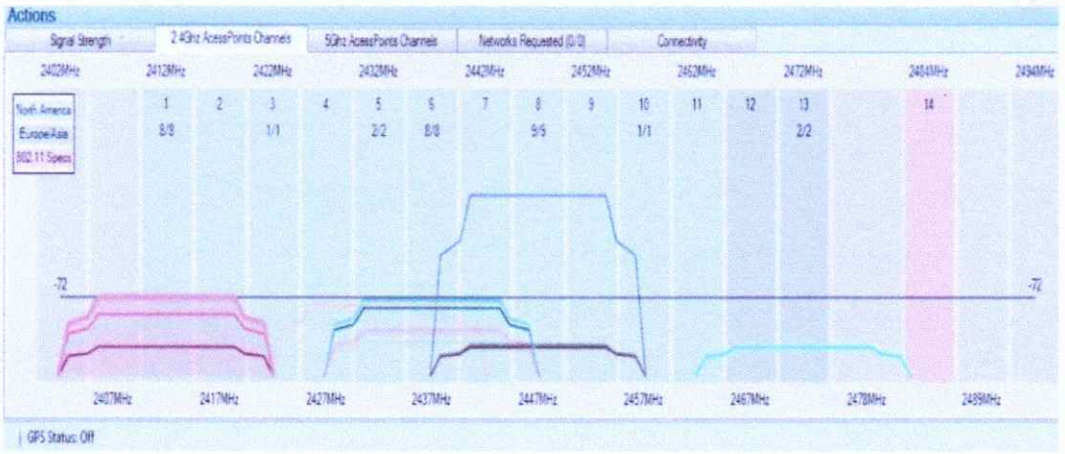


Gambar 5. *Scanning* Analisis Menggunakan Arcliric-Wifi

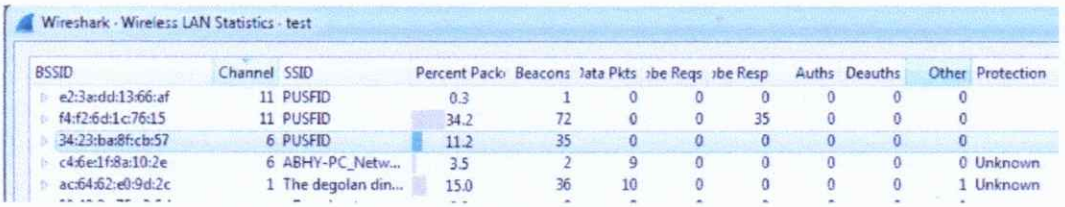
Pada capture jaringan *Wifi* menggunakan acrilyc-*Wifi* ditemukan rangkaian statistic sinyal *Wifi*, AP pusfid yang diberi tanda warna biru menunjukan tingkat kekuatan sinyal di atas rata-rata dengan -37db, dibanding dengan AP yang diberi tanda merah mudah yang hanya berkekutan sinyal -74 db. Menurut (Cai et al. 2022) *Rogue* AP/AP palsu biasanya memiliki *SSID* yang sama dan konfigurasi dengan AP yang sah. Selain itu *Rogue* AP harus memiliki sinyal yang lebih kuat daripada AP legal. Dan *Rogue* AP harus menawarkan otentikasi ulang antara sta (*station*/penerima) dan AP agar tidak membangkitkan kecurigaan. *Rogue* AP dapat dideteksi dengan menganalisa atribut yang dipancarakan oleh sinyal *beacoon* inteval, yaitu dengan *SSID*, vendor, rate sinyal, channel, B*SSID* dan IP, dengan cara dibandingkan dengan informasi AP yang sah, berikut adalah analisa kekuatan sinyal, ber dasarkan kekuatan sinyal, pada rate 2.4 ghz AP/channel,seperti yang terlihat pada Gambar 6 dan 7.



Gambar 6. Analisa Statistic Kekuatan Signal

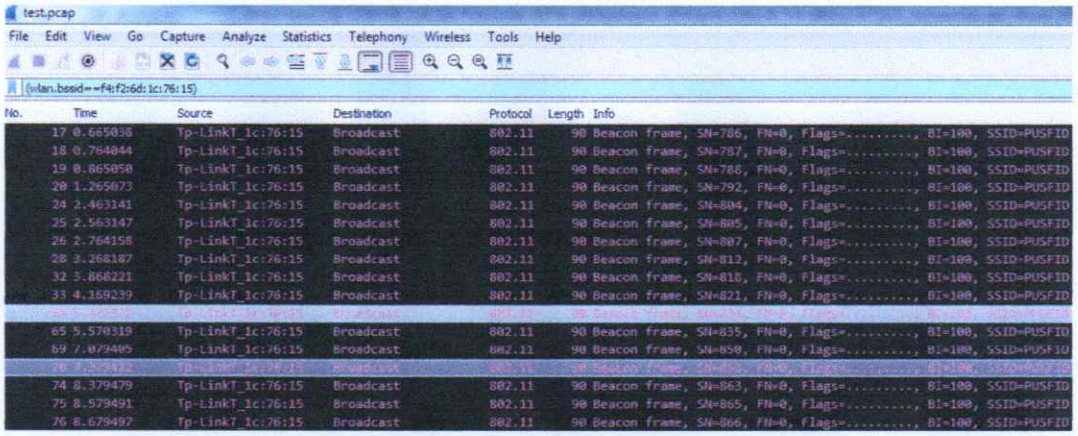


Gambar 7. Analisa Statistik *2.4 Ghz Acsses Point/Channel*



Gambar 8. Prensentasi *Capture Traffic Wifi*

Dari hasil *capture traffic Wifi* ditemukan terdapat SSID PUSFID, *channel* 11 dengan Mac f4:f2:6d:1c:76:15, memiliki presentasi paket yang paling tinggi yaitu 34.2 % dengan singnal *beacon* 72, untuk lebih jelasnya terliahat pada Gambar 8 dan 9.



Gambar 9. Akuisisi File Pcap *Capture Traffik*

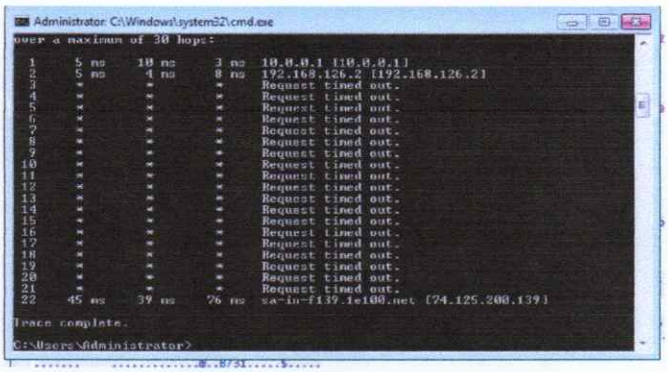
Approach Strategy

Approach Strategy merupakan suatu kegitan dimana peneliti melakukan persiapan untuk menangani kemungkinan-kemungkinan terjadi tindakan ilegal lainya, setelah ditemukan informasi dan data-data terkait AP palsu, peneliti akan berusaha masuk dengan sengaja ke dalam jangkauan AP palsu, seakan akan menjadi *user* dalam area *Evil Twin attack*, dengan tujuan agar dapat menemukan informasi lebih lanjut tentang tindak kejahatan ilegal seperti, serangan *man in the midle attack*, kemudian peneliti melakukan analisa-analisa terkait data-data yang nantinya digunakan untuk menemukan barang bukti. Dengan memanfatkan beberapa *tools* bantu yaitu Wireshark dan *network* miner untuk melakukan proses *sniffing* pada jaringan *Evil Twin* tersebut, selain itu akan digunakan juga salah satu *tools Arp detector* untuk memudahkan proses analisa untuk menemukan barang bukti yaitu xarp, karena pada dasarnya metode *sniffing* yang dilakukan melalui *user side* tidak terlalu efektif, maka dibutuhkan beberapa metode maupun *tools* bantu lainnya.

Deteksi Dan Collection Phase 2

Tracert IP

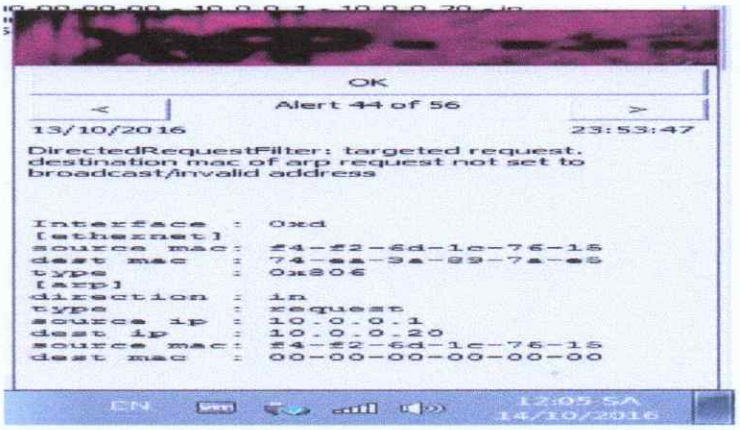
Pada tahapan ini, dimulai dengan mencari tau IP dari *router* pelaku dengan menggunakan perintah *tracert* seperti yang terlihat pada Gambar 10, telihat IP yang digunakan oleh pelaku adalah 10.0.0.1 sebagai *gateway* dan 192.168.126.2.



Gambar 10. Tracer IP

Xarp identifikasi

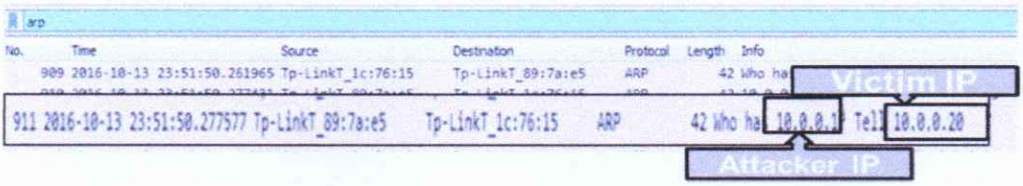
Pada dasarnya serangan *MITM* akan selalu memnfatkan *broadcase Arp* untuk mencoba melakukan poisioning, dan ketika pelaku memulai serangannya, maka dengan automatis xarp akan memberikan notifikasi adanya serangan *Arp* seperti yang terlihat pada Gambar 11, dimana terlihat *source* IP 10.0.0.1 melakukan *recquest* pada IP 10.0.0.20.



Gambar 11. Notifikasi Arp *Attack*

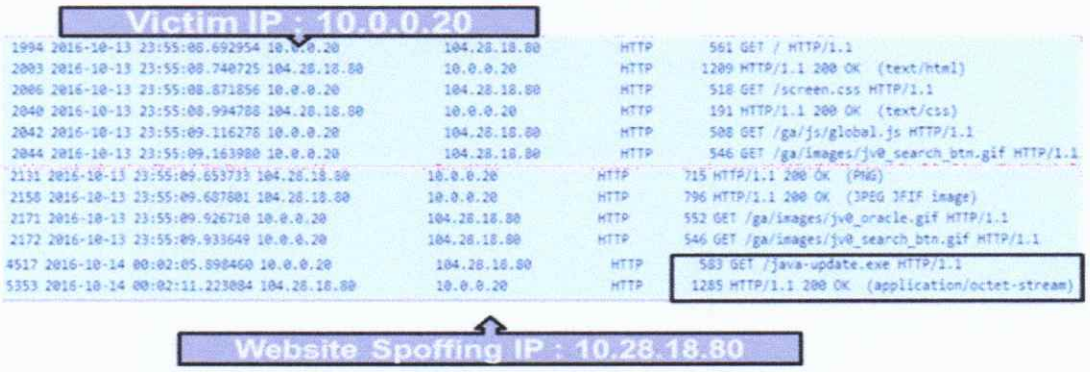
Capture trafik

Capture paket trafik dengan menggunakan Wireshark di dalam jaringan *Evil Twin* tersebut, dilakukukan selama beberapa menit untuk menemukan *beberapa* informasi yang dapat digunakan untuk proses analisa selanjutnya, berikut detail file pcap yang akan dianalisa, seperti yang terlihat pada tabel 1.

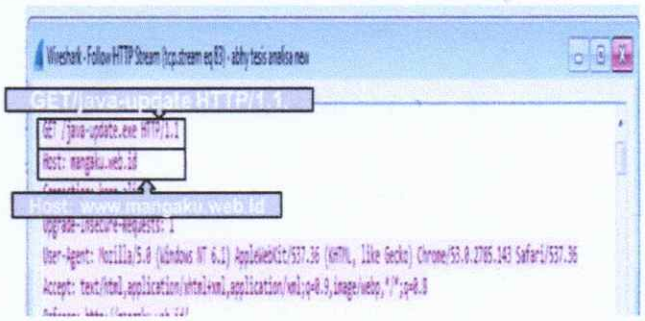


Gambar 13. *Arp* Filter

Pada Analisa filterisasi *port* HTTP, terlihat IP 10.0.0.20 melakukan *request* ke IP 104.28.18.80, kemudian IP 10.0.0.20 diarahkan untuk mengakses situs yang kemungkinan sengaja disiapkan. Dari hasil analisa pada *port* HTTP juga terlihat adanya beberapa file yang mencurigakan diantaranya adalah file Html, file.Css, file Jpg, file Png, dan file berksensi Exe yang ditemukan pada paket 5353 yaitu http/get java-update.exe. Untuk lebih jelasnya dapat dilihat pada Gambar 15. Kemudian pada Gambar 16, ditemukan adanya kegitan yang mencurigkan dimana Host yang sebenarnya dari IP 104.28.18.80 adalah http://www.mangaku.web.id.



Gambar 14. Http Filter



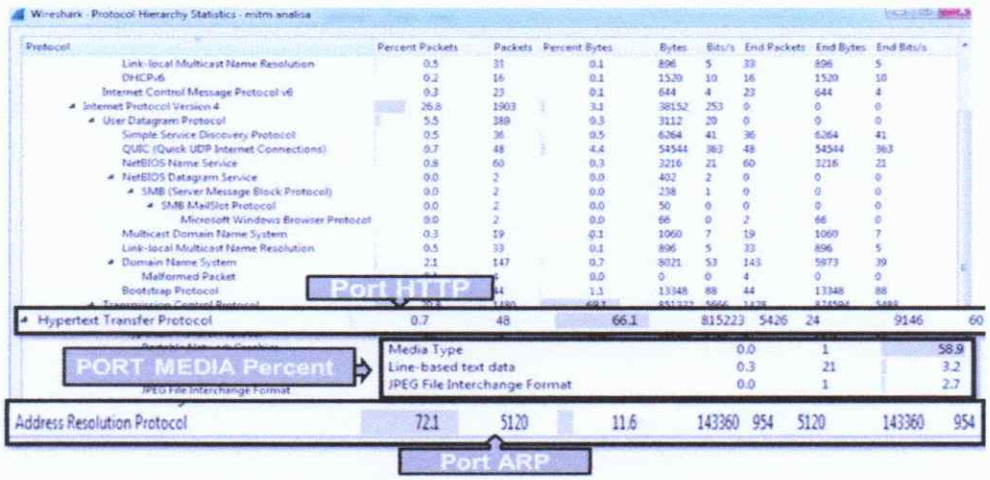
Gambar 15. Http Analisis

Tabel 1 Tabel File Pcap

Nama	*MITM* analisa,pcap
Tipe	File pcap
Hash (md5)	B9e31516e1b9ff8ab174503373687b82
Ukuran file	1.28 mb
Tools	Wireshark

Akuisisi data serangan

Tahapan Akuisisi serangan, dilakukan dengan menganalisa data maupun informasi yang ditemukan dalam tahapan pengkoleksian/ *Collection* sebelumnya. Proses Akusisi data serangan dilakukan dengan menganalisa file hasil capturing sebelumnya, *tools* Wireshark. Proses analisa dilakukan dengan cara memanfaatkan modul hierarki dan *comand-comand* filterisasi paket dari dari *tools* Wireshark. Dari hasil analisa tabel hirarki terdapat 3 objek yang dapat dijadikan sebagai bahan analisa yaitu *port* HTTP, *port* ARP dan presentasi media. Seperti yang terlihat pada Gambar 12.



Gambar 12. Wireshark Hirarki Modul

Pada Gambar 14, Pada analisa *port* ARP ditemukan kegiatan ARP *broadcase* dari MAC *address* tp_link/ *sourece* 1c: 76:15 dengan IP 10.0.0.1 mencoba menghubungi MAC *address destination* azurewav 79:5a:5c dengan IP 10.0.0.20