

# Traffic analysis exercise

- Blank Clipboard

정지훈

# 목차

1.개요

2.분석

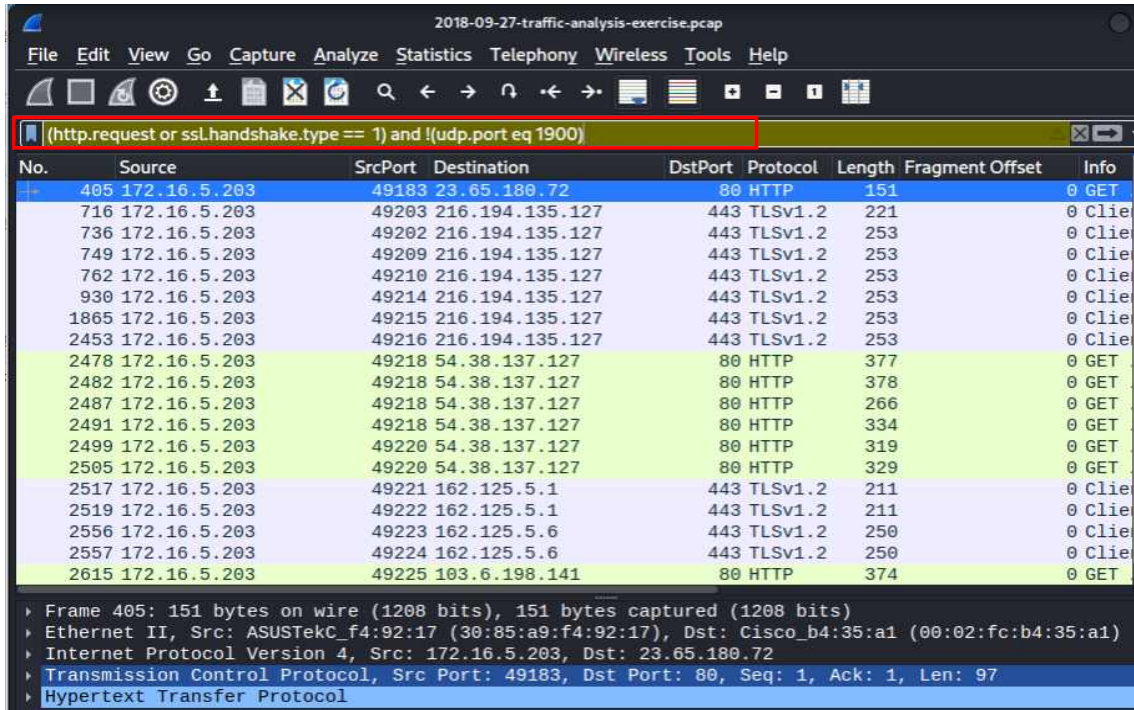
## 1.개요

- Windows Host OS가 감염되는 pcap
- 두 개의 이메일

두 개의 이메일 중 어떤 것이 pcap에서 감염 트래픽을 알아본다.

## 2. 분석

-wireshark 디스플레이 필터 적용



2018-09-27-traffic-analysis-exercise.pcap

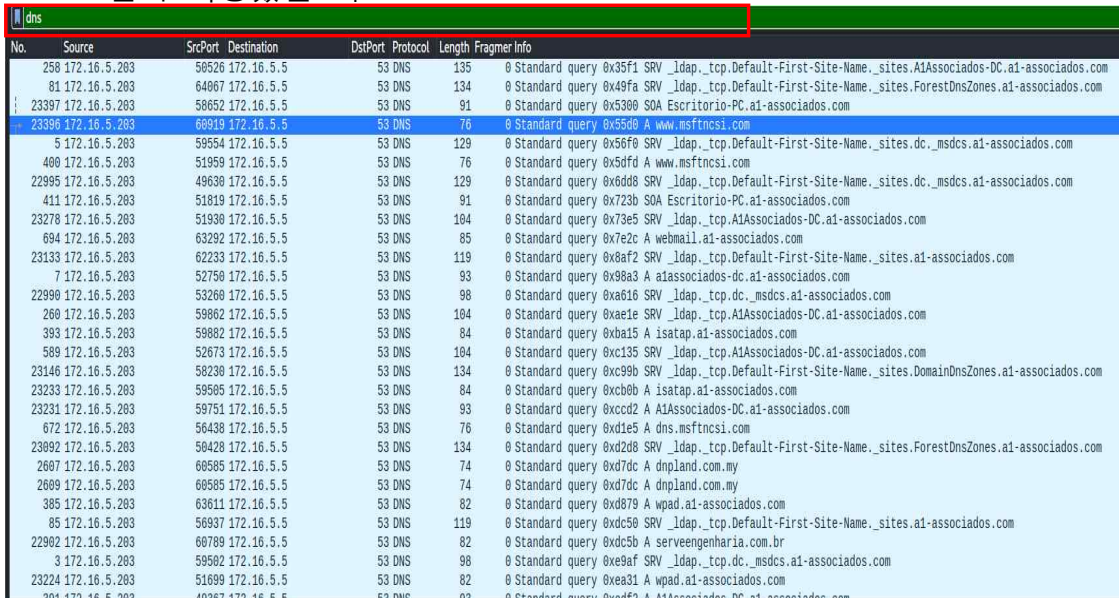
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(http.request or ssl.handshake.type == 1) and !(udp.port eq 1900)

No.	Source	SrcPort	Destination	DstPort	Protocol	Length	Fragment Offset	Info
405	172.16.5.203	49183	23.65.180.72	80	HTTP	151		0 GET
716	172.16.5.203	49203	216.194.135.127	443	TLSv1.2	221		0 Clie
736	172.16.5.203	49202	216.194.135.127	443	TLSv1.2	253		0 Clie
749	172.16.5.203	49209	216.194.135.127	443	TLSv1.2	253		0 Clie
762	172.16.5.203	49210	216.194.135.127	443	TLSv1.2	253		0 Clie
930	172.16.5.203	49214	216.194.135.127	443	TLSv1.2	253		0 Clie
1865	172.16.5.203	49215	216.194.135.127	443	TLSv1.2	253		0 Clie
2453	172.16.5.203	49216	216.194.135.127	443	TLSv1.2	253		0 Clie
2478	172.16.5.203	49218	54.38.137.127	80	HTTP	377		0 GET
2482	172.16.5.203	49218	54.38.137.127	80	HTTP	378		0 GET
2487	172.16.5.203	49218	54.38.137.127	80	HTTP	266		0 GET
2491	172.16.5.203	49218	54.38.137.127	80	HTTP	334		0 GET
2499	172.16.5.203	49220	54.38.137.127	80	HTTP	319		0 GET
2505	172.16.5.203	49220	54.38.137.127	80	HTTP	329		0 GET
2517	172.16.5.203	49221	162.125.5.1	443	TLSv1.2	211		0 Clie
2519	172.16.5.203	49222	162.125.5.1	443	TLSv1.2	211		0 Clie
2556	172.16.5.203	49223	162.125.5.6	443	TLSv1.2	250		0 Clie
2557	172.16.5.203	49224	162.125.5.6	443	TLSv1.2	250		0 Clie
2615	172.16.5.203	49225	103.6.198.141	80	HTTP	374		0 GET

Frame 405: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits)  
Ethernet II, Src: ASUSTekC\_f4:92:17 (30:85:a9:f4:92:17), Dst: Cisco\_b4:35:a1 (00:02:fc:b4:35:a1)  
Internet Protocol Version 4, Src: 172.16.5.203, Dst: 23.65.180.72  
Transmission Control Protocol, Src Port: 49183, Dst Port: 80, Seq: 1, Ack: 1, Len: 97  
Hypertext Transfer Protocol

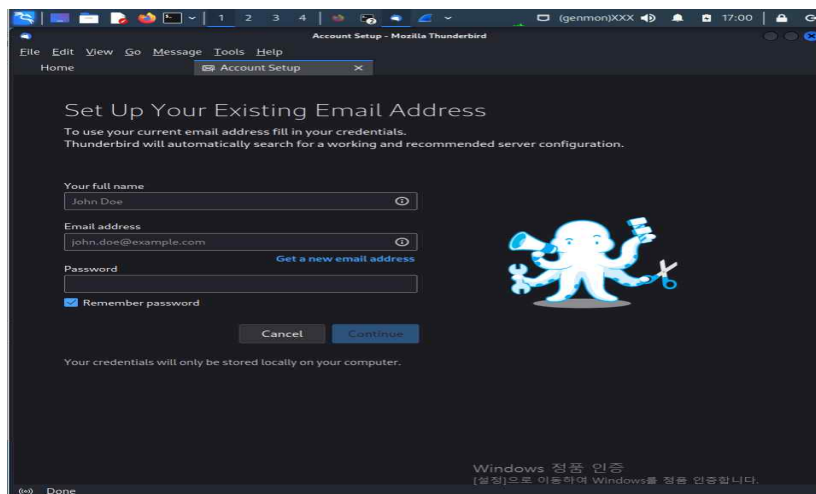
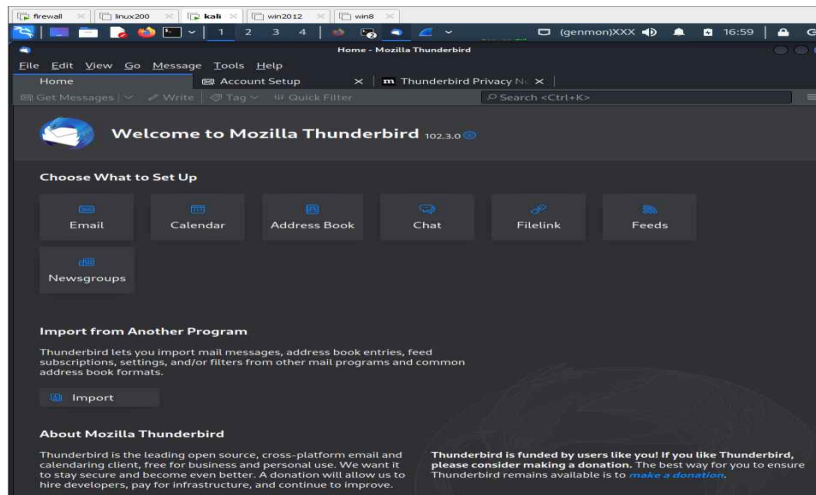
-DNS 필터 적용했을 때



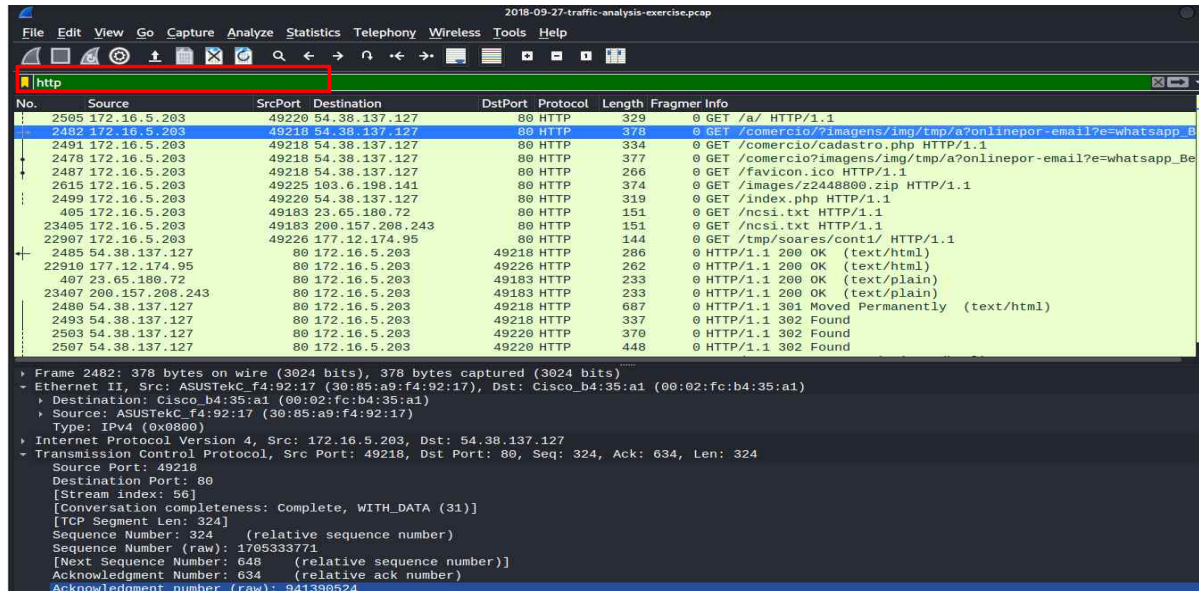
dns

No.	Source	SrcPort	Destination	DstPort	Protocol	Length	Fragment Info
258	172.16.5.203	50526	172.16.5.5	53	DNS	135	0 Standard query 0x35f1 SRV _ldap._tcp.Default-First-Site-Name._sites.A1Associados-DC.a1-associados.com
81	172.16.5.203	49697	172.16.5.5	53	DNS	134	0 Standard query 0x49fa SRV _ldap._tcp.Default-First-Site-Name._sites.ForestDnsZones.a1-associados.com
23397	172.16.5.203	58652	172.16.5.5	53	DNS	91	0 Standard query 0x5300 SOA Escritorio-PC.a1-associados.com
23396	172.16.5.203	60919	172.16.5.5	53	DNS	76	0 Standard query 0x55d0 A www.msftncsi.com
5	172.16.5.203	59554	172.16.5.5	53	DNS	129	0 Standard query 0x56f0 SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.a1-associados.com
400	172.16.5.203	51959	172.16.5.5	53	DNS	76	0 Standard query 0x5d0d A www.msftncsi.com
22995	172.16.5.203	49630	172.16.5.5	53	DNS	129	0 Standard query 0x6dd8 SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.a1-associados.com
411	172.16.5.203	51819	172.16.5.5	53	DNS	91	0 Standard query 0x723b SOA Escritorio-PC.a1-associados.com
23278	172.16.5.203	51930	172.16.5.5	53	DNS	104	0 Standard query 0x73e5 SRV _ldap._tcp.A1Associados-DC.a1-associados.com
694	172.16.5.203	63292	172.16.5.5	53	DNS	85	0 Standard query 0x7e2c A webmail.a1-associados.com
23133	172.16.5.203	62233	172.16.5.5	53	DNS	119	0 Standard query 0x8af2 SRV _ldap._tcp.Default-First-Site-Name._sites.a1-associados.com
7	172.16.5.203	52750	172.16.5.5	53	DNS	93	0 Standard query 0x98a3 A a1associados-dc.a1-associados.com
22990	172.16.5.203	53260	172.16.5.5	53	DNS	98	0 Standard query 0xa616 SRV _ldap._tcp.dc._msdcs.a1-associados.com
260	172.16.5.203	59862	172.16.5.5	53	DNS	104	0 Standard query 0xae1e SRV _ldap._tcp.A1Associados-DC.a1-associados.com
393	172.16.5.203	59882	172.16.5.5	53	DNS	84	0 Standard query 0xba15 A isatap.a1-associados.com
589	172.16.5.203	52673	172.16.5.5	53	DNS	104	0 Standard query 0xc135 SRV _ldap._tcp.A1Associados-DC.a1-associados.com
23146	172.16.5.203	58230	172.16.5.5	53	DNS	134	0 Standard query 0xc99b SRV _ldap._tcp.Default-First-Site-Name._sites.DomainDnsZones.a1-associados.com
23233	172.16.5.203	59605	172.16.5.5	53	DNS	84	0 Standard query 0xcb0b A isatap.a1-associados.com
23231	172.16.5.203	59751	172.16.5.5	53	DNS	93	0 Standard query 0xccd2 A A1Associados-DC.a1-associados.com
672	172.16.5.203	56438	172.16.5.5	53	DNS	76	0 Standard query 0xd1e5 A dns.msftncsi.com
23092	172.16.5.203	58428	172.16.5.5	53	DNS	134	0 Standard query 0xd2d8 SRV _ldap._tcp.Default-First-Site-Name._sites.ForestDnsZones.a1-associados.com
2607	172.16.5.203	60585	172.16.5.5	53	DNS	74	0 Standard query 0xd7dc A dnpland.com.my
2609	172.16.5.203	60585	172.16.5.5	53	DNS	74	0 Standard query 0xd7dc A dnpland.com.my
385	172.16.5.203	63611	172.16.5.5	53	DNS	82	0 Standard query 0xd879 A wpad.a1-associados.com
85	172.16.5.203	56937	172.16.5.5	53	DNS	119	0 Standard query 0xdc50 SRV _ldap._tcp.Default-First-Site-Name._sites.a1-associados.com
22902	172.16.5.203	60789	172.16.5.5	53	DNS	82	0 Standard query 0xdc5b A serveengenharia.com.br
3	172.16.5.203	59502	172.16.5.5	53	DNS	98	0 Standard query 0xe9af SRV _ldap._tcp.dc._msdcs.a1-associados.com
23224	172.16.5.203	51699	172.16.5.5	53	DNS	82	0 Standard query 0xea31 A wpad.a1-associados.com
204	172.16.5.203	49967	172.16.5.5	53	DNS	92	0 Standard query 0xfdf2 A A1Associados-DC.a1-associados.com

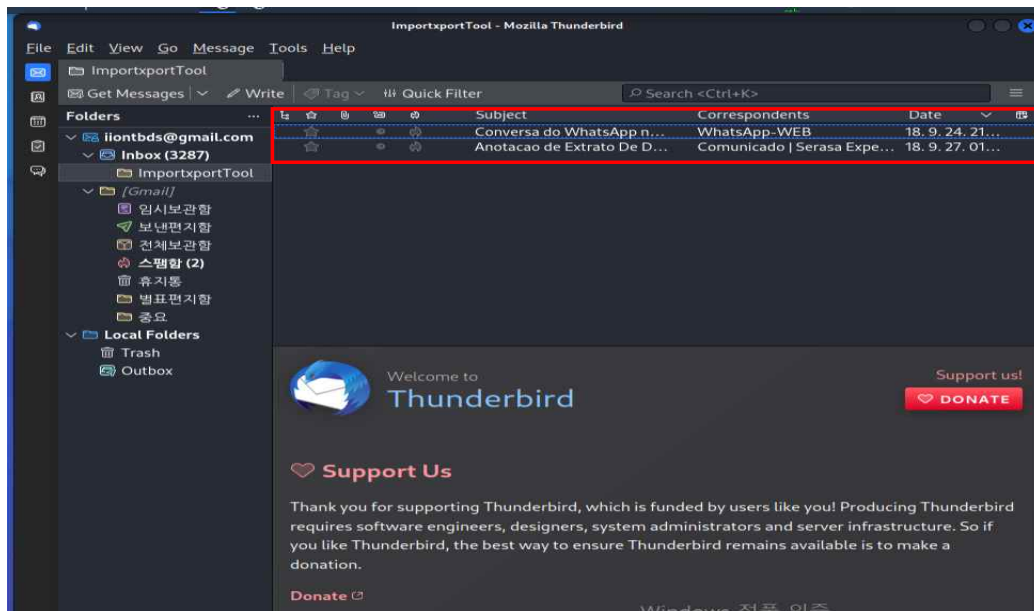
mozilla Thunderbird 실행 > 자신의 구글 계정으로 로그인



-HTTP 필터 적용

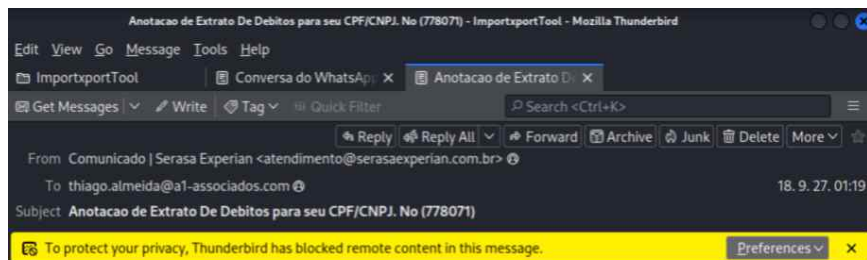
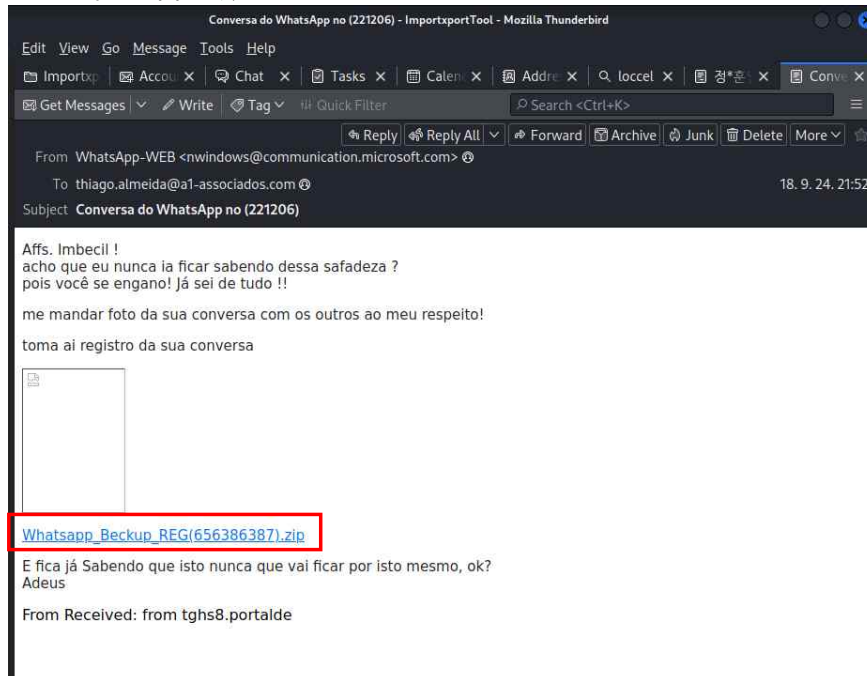


- Host OS에서 em1, em2 파일을 다운받은 후 kali linux 파일 옮기기 > Inbox 에 폴더 생성 > 생성한 파일에 1-em1, 2-em2을 mozilla Thunderbird 로 이동



-첫 번째 이메일에서 whatsapp\_Backup\_REG에 많은 정보를 찾을 수 있다. 인코딩된 데이터를 반환

-zip 아카이브는 트래픽을 구글 홈페이지로 리디렉션하였고 snort를 사용해 트래픽을 검토했을 때 의미 있는 경고를 트리거X



#### COMUNICADO IMPORTANTE Nº 20180354927618

São Paulo, quarta-feira 26 de setembro de 2018

Prezado(a) Senhor(a),

Para a preservação da qualidade e da segurança dos serviços prestado a comunidade e cumprimento do disposto no art.43, parágrafo segundo, da lei nº 8.078 de 11 de setembro de 1990, informamos que recebemos da instituição credora, pedido de inclusão em nossos registros da(s) anotação(ões) abaixo denominada(s), para o CPF/CNPJ correspondente ao E-mail .

#### Valor da anotação - Data da ocorrência - Natureza

[Consultar Extrato de Débitos Detalhados](#)

A Serasa Experian aguardará pelo prazo de 10 dias, contado da postagem desta correspondência, manifestação de V.Sa. ou da Instituição credora quanto a regularização da(s) dívidas(s). Na ausência da manifestação, a(s) inclusão(ões) será efetuada(s).

Comunicado Importante | Política de Privacidade | Canal de denúncias

©2018 Experian Information Solutions, Inc. Experian Marketing Services All rights reserved.