Master of Information Security

MIS4203 – Independent Studies in Information Security

Index Number – 16770217 | Reg. Number – 2016MIS021

Study Number – 01 – Network Traffic Analysis

November 17, 2018

University of Colombo School of Computing

Table of Contents

Incident– 01

Problem

Scenario: Host machine was infected by a malware.

For the incident # 01, there is *.pcap* file is given for analyze which is related incident that is malware infection to the host machine. The *.pcap* file contains packet capture of the network where the incident happened.

Approach

1. As best practice it is mandatory to validate hash value of the evidence that provided or collected.
2. Given *.pcap* file can be analyzed via various online and offline tools which are helps to see/identify the content of the packets where inbound and outbound to/from host machine.
3. It is necessary to identify when and where the data is transferred and if there is malicious content transferred to the victims host as well as malicious redirections.
4. Then exploit kit and vulnerabilities can be identified and then necessary actions should be taken to mitigate the risk according to the incident.

Above approach is taken to do the network packet analyze and will be explained step by step below.

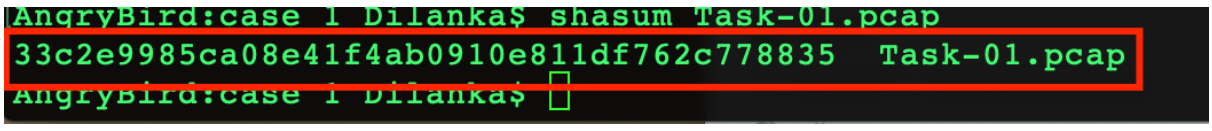
Given questions will be answered by end of the analyze with the conclusion.

Step 01

Hash value validation of copy of the evidence collected against original file.

Incident 01

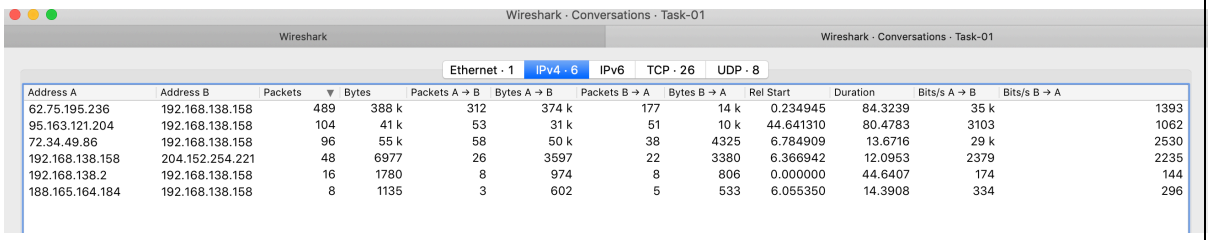
File URL: http://pgvle.ucsc.cmb.ac.lk/mod/resource/view.php?id=6654
Scenario: Host machine was infected by a malware
SHA1 Hash: 33c2e9985ca08e41f4ab0910e811df762c778835



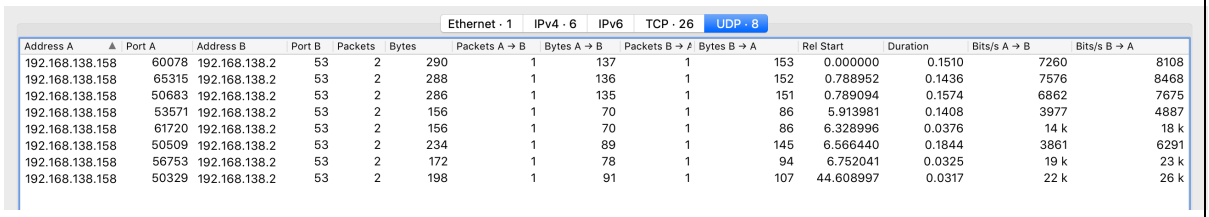
Step 02

Given *Task-01.pcap* file is imported to ***Wireshark*** application for the analysis.

1. First, we can see the packet summary of tcp and udp perspective to get an overall idea of the how it behaves over the channel as well as involved ip addresses.

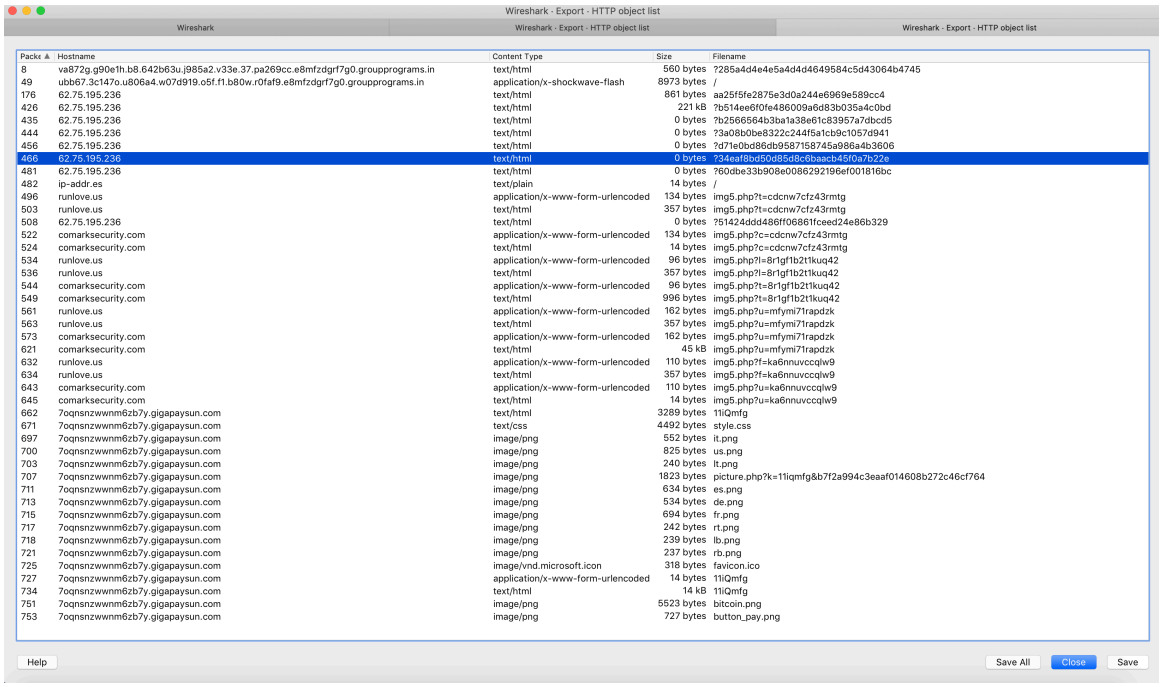


Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
62.75.195.236	192.168.138.158	489	388 k	312	374 k	177	14 k	0.234945	84.3239	35 k	1393
95.163.121.204	192.168.138.158	104	41 k	53	31 k	51	10 k	44.641310	80.4783	3103	1062
72.34.49.86	192.168.138.158	96	55 k	58	50 k	38	4325	6.784909	13.6716	29 k	2530
192.168.138.158	204.152.254.221	48	6977	26	3597	22	3380	6.366942	12.0953	2379	2235
192.168.138.2	192.168.138.158	16	1780	8	974	8	806	0.000000	44.6407	174	144
188.165.164.184	192.168.138.158	8	1135	3	602	5	533	6.055350	14.3908	334	296



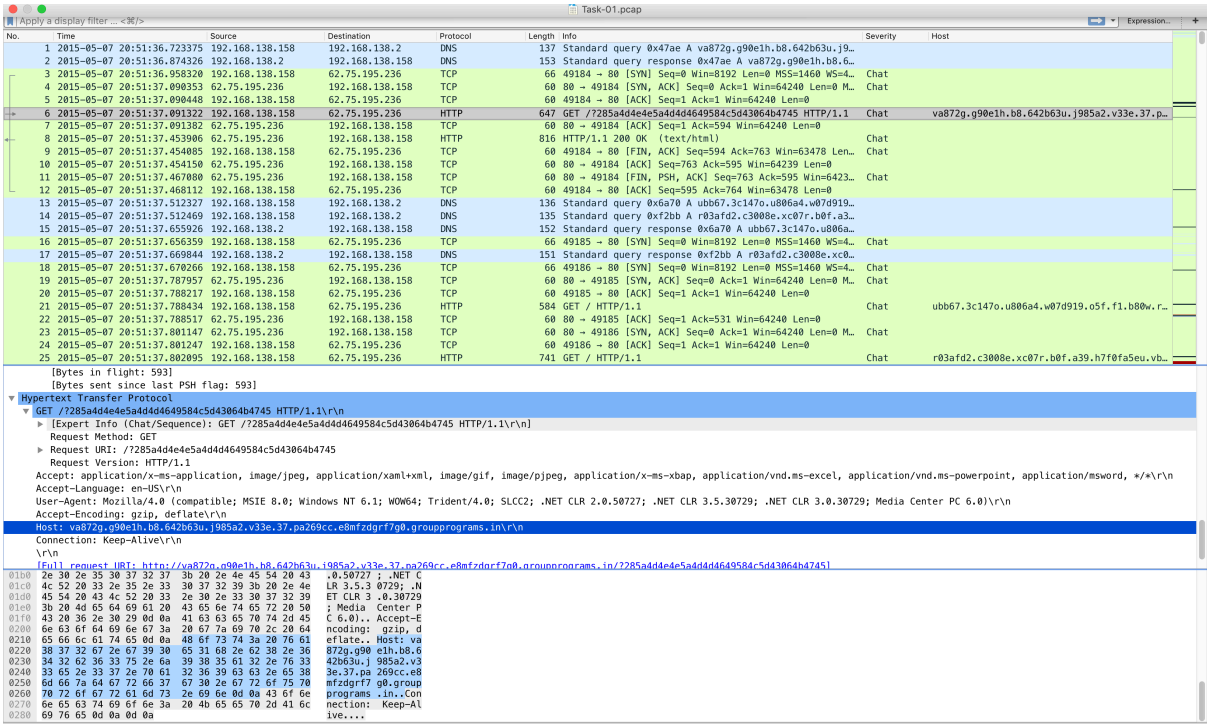
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.138.158	60078	192.168.138.2	53	2	290	1	137	1	153	0.000000	0.1510	7260	8108
192.168.138.158	65315	192.168.138.2	53	2	288	1	136	1	152	0.788952	0.1436	7576	8468
192.168.138.158	50683	192.168.138.2	53	2	286	1	135	1	151	0.789094	0.1574	6862	7675
192.168.138.158	53571	192.168.138.2	53	2	156	1	70	1	86	5.913981	0.1408	3977	4887
192.168.138.158	61720	192.168.138.2	53	2	156	1	70	1	86	6.328996	0.0376	14 k	18 k
192.168.138.158	50509	192.168.138.2	53	2	234	1	89	1	145	6.566440	0.1844	3861	6291
192.168.138.158	56753	192.168.138.2	53	2	172	1	78	1	94	6.752041	0.0325	19 k	23 k
192.168.138.158	50329	192.168.138.2	53	2	198	1	91	1	107	44.608997	0.0317	22 k	26 k

2. Then we can identify data transferred via http by looking in to *HTTP Object List* via Wireshark.



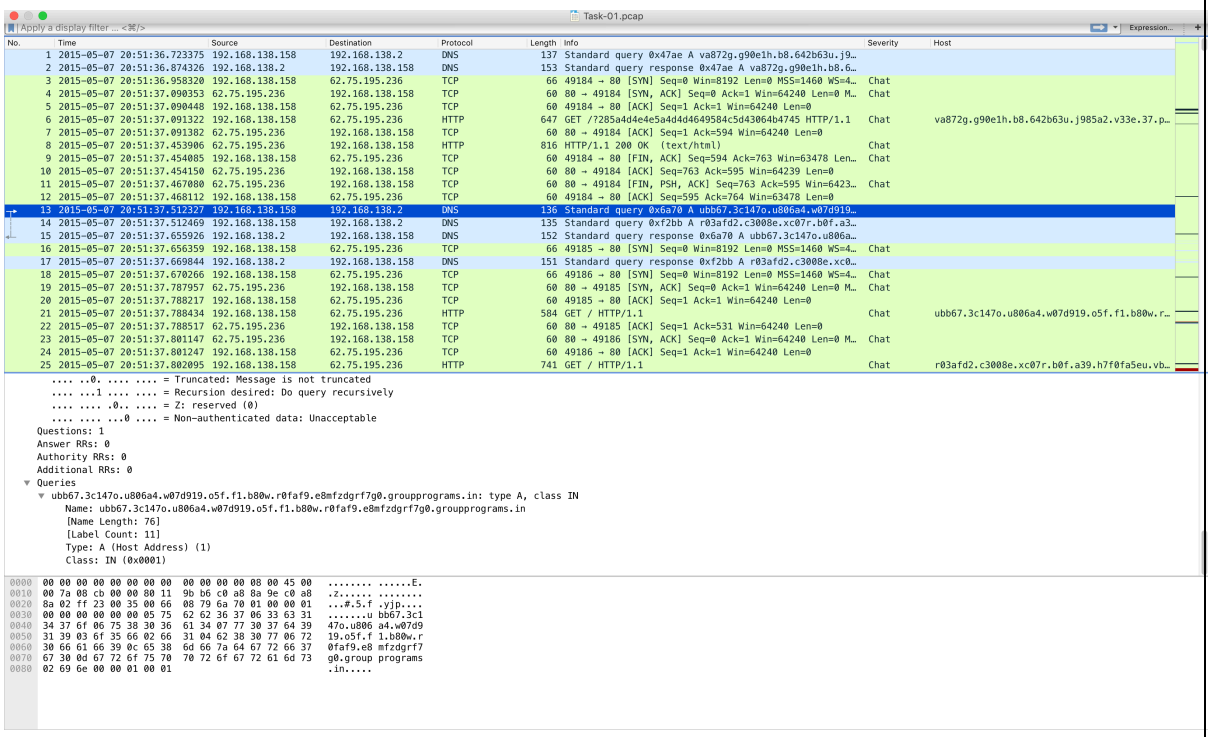
Packe	Hostname	Content Type	Size	Filename
8	va872g.g90e1h.b8.642b63u.j985a2.v33e.37.pa269cc.e8mfzdgrf7g0.grouppprograms.in	text/html	560 bytes	?285a4d4e4e5a4d4d4649584c5d43064b4745
49	ubb67.3c147o.u806a4.w07d919.o5f.f1.b80w.r0faf9.e8mfzdgrf7g0.grouppprograms.in	application/x-shockwave-flash	8973 bytes	/
176	62.75.195.236	text/html	861 bytes	aa25f5fe2875e3d0a244e6969e589cc4
426	62.75.195.236	text/html	221 kB	?b514ee6f0fe486009a6d83b035a4c0bd
435	62.75.195.236	text/html	0 bytes	?b2566564b3ba1a38e61c83957a7dbcd5
444	62.75.195.236	text/html	0 bytes	?3a08b0be8322c244f5a1cb9c1057d941
456	62.75.195.236	text/html	0 bytes	?d71e0bd86db9587158745a986a4b3606
466	62.75.195.236	text/html	0 bytes	?34eaf8bd50d85d8c6baacb45f0a7b22e
481	62.75.195.236	text/html	0 bytes	?60dbe33b908e0086292196ef001816bc
482	ip-addr.es	text/plain	14 bytes	/
496	runlove.us	application/x-www-form-urlencoded	134 bytes	img5.php?t=cdcnw7cfz43rmtg
503	runlove.us	text/html	357 bytes	img5.php?t=cdcnw7cfz43rmtg
508	62.75.195.236	text/html	0 bytes	?51424ddd486ff06861fceed24e86b329
522	comarksecurity.com	application/x-www-form-urlencoded	134 bytes	img5.php?c=cdcnw7cfz43rmtg
524	comarksecurity.com	text/html	14 bytes	img5.php?c=cdcnw7cfz43rmtg
534	runlove.us	application/x-www-form-urlencoded	96 bytes	img5.php?l=8r1gf1b2t1kuq42
536	runlove.us	text/html	357 bytes	img5.php?l=8r1gf1b2t1kuq42
544	comarksecurity.com	application/x-www-form-urlencoded	96 bytes	img5.php?t=8r1gf1b2t1kuq42
549	comarksecurity.com	text/html	996 bytes	img5.php?t=8r1gf1b2t1kuq42
561	runlove.us	application/x-www-form-urlencoded	162 bytes	img5.php?u=mfymi71rapdzk
563	runlove.us	text/html	357 bytes	img5.php?u=mfymi71rapdzk
573	comarksecurity.com	application/x-www-form-urlencoded	162 bytes	img5.php?u=mfymi71rapdzk
621	comarksecurity.com	text/html	45 kB	img5.php?u=mfymi71rapdzk
632	runlove.us	application/x-www-form-urlencoded	110 bytes	img5.php?f=ka6nnuvccqlw9
634	runlove.us	text/html	357 bytes	img5.php?f=ka6nnuvccqlw9
643	comarksecurity.com	application/x-www-form-urlencoded	110 bytes	img5.php?u=ka6nnuvccqlw9
645	comarksecurity.com	text/html	14 bytes	img5.php?u=ka6nnuvccqlw9
662	7oqnsnzwwnm6zb7y.gigapaysun.com	text/html	3289 bytes	11iQmfg
671	7oqnsnzwwnm6zb7y.gigapaysun.com	text/css	4492 bytes	style.css
697	7oqnsnzwwnm6zb7y.gigapaysun.com	image/png	552 bytes	it.png
700	7oqnsnzwwnm6zb7y.gigapaysun.com	image/png	825 bytes	us.png
703	7oqnsnzwwnm6zb7y.gigapaysun.com	image/png	240 bytes	it.png
707	7oqnsnzwwnm6zb7y.gigapaysun.com	image/png	1823 bytes	picture.php?k=11iqmfg&b7f2a994c3eaaf014608b272c46cf764
711	7oqnsnzwwnm6zb7y.gigapaysun.com	image/png	634 bytes	es.png
713	7oqnsnzwwnm6zb7y.gigapaysun.com	image/png	534 bytes	de.png
715	7oqnsnzwwnm6zb7y.gigapaysun.com	image/png	694 bytes	fr.png
717	7oqnsnzwwnm6zb7y.gigapaysun.com	image/png	242 bytes	rt.png
718	7oqnsnzwwnm6zb7y.gigapaysun.com	image/png	239 bytes	lb.png
721	7oqnsnzwwnm6zb7y.gigapaysun.com	image/png	237 bytes	rb.png
725	7oqnsnzwwnm6zb7y.gigapaysun.com	image/vnd.microsoft.icon	318 bytes	favicon.ico
727	7oqnsnzwwnm6zb7y.gigapaysun.com	application/x-www-form-urlencoded	14 bytes	11iQmfg
734	7oqnsnzwwnm6zb7y.gigapaysun.com	text/html	14 kB	11iQmfg
751	7oqnsnzwwnm6zb7y.gigapaysun.com	image/png	5523 bytes	bitcoin.png
753	7oqnsnzwwnm6zb7y.gigapaysun.com	image/png	727 bytes	button_pay.png

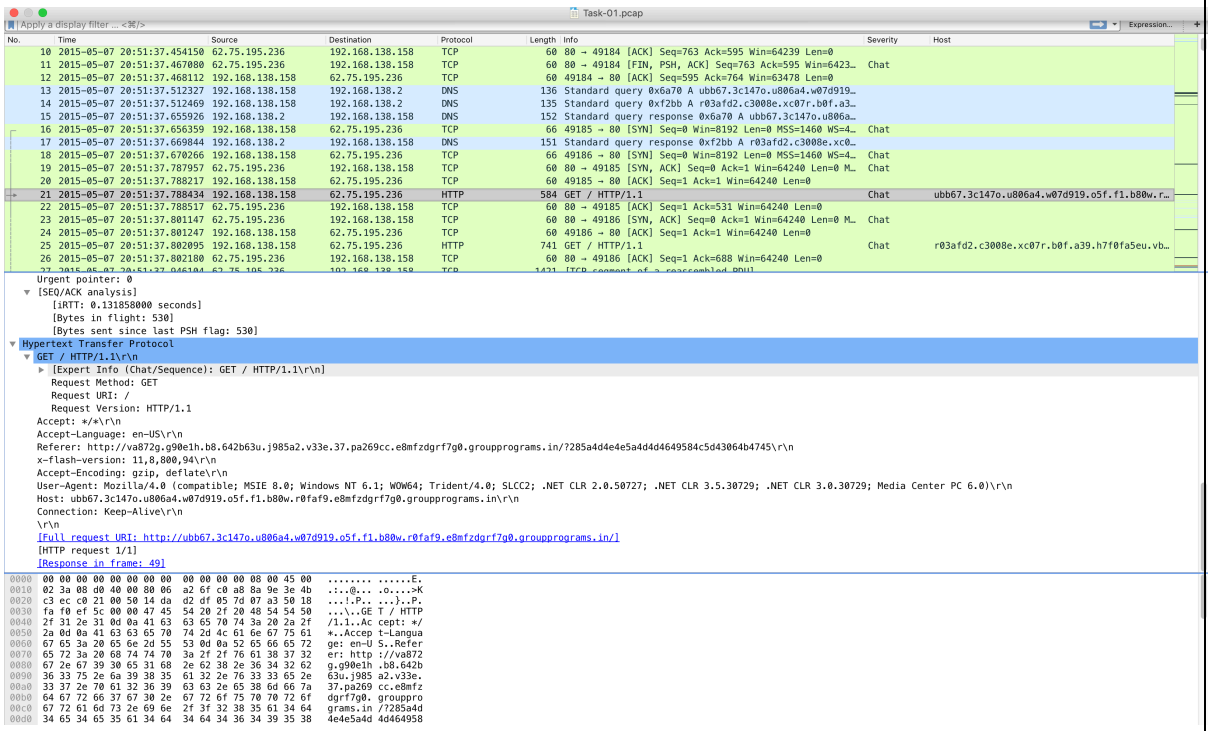
3. Considering first web request

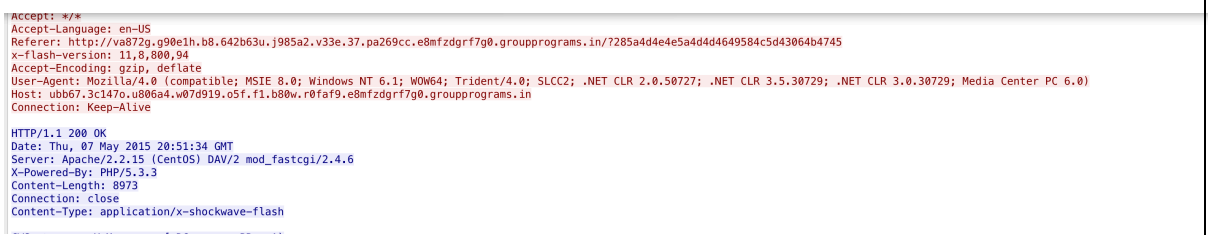


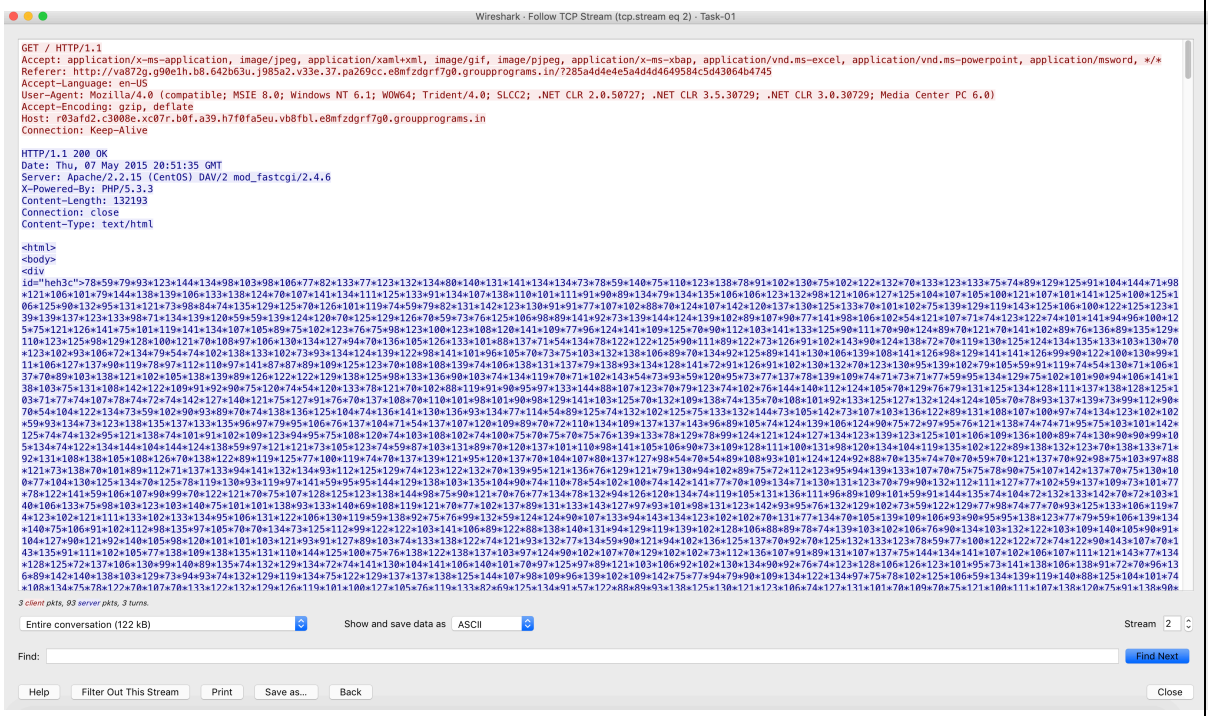
According to above screenshots, the first web request which is legitimate traffic, but content of the web page having unusual content, which may initiate connection to this domain.
So, this can be cross site script of malicious advertisement which may leads to the malicious domain which user clicked when browsing the website.

4. Let's consider the second response from the server.


Task-01.pcap
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info Severity Host
1 2015-05-07 20:51:36.723375 192.168.138.158 192.168.138.2 DNS 137 Standard query 0x47ae A va872g.g90e1h.b8.642b63u.j9…
2 2015-05-07 20:51:36.874326 192.168.138.2 192.168.138.158 DNS 153 Standard query response 0x47ae A va872g.g90e1h.b8.6…
3 2015-05-07 20:51:36.958320 192.168.138.158 62.75.195.236 TCP 66 49184 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4… Chat
4 2015-05-07 20:51:37.090353 62.75.195.236 192.168.138.158 TCP 60 80 → 49184 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M… Chat
5 2015-05-07 20:51:37.090448 192.168.138.158 62.75.195.236 TCP 60 49184 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
6 2015-05-07 20:51:37.091322 192.168.138.158 62.75.195.236 HTTP 647 GET /?285a4d4e4e5a4d4d4649584c5d43064b4745 HTTP/1.1 Chat va872g.g90e1h.b8.642b63u.j985a2.v33e.37.p…
7 2015-05-07 20:51:37.091382 62.75.195.236 192.168.138.158 TCP 60 80 → 49184 [ACK] Seq=1 Ack=594 Win=64240 Len=0
8 2015-05-07 20:51:37.453906 62.75.195.236 192.168.138.158 HTTP 816 HTTP/1.1 200 OK (text/html) Chat
9 2015-05-07 20:51:37.454085 192.168.138.158 62.75.195.236 TCP 60 49184 → 80 [FIN, ACK] Seq=594 Ack=763 Win=63478 Len… Chat
10 2015-05-07 20:51:37.454150 62.75.195.236 192.168.138.158 TCP 60 80 → 49184 [ACK] Seq=763 Ack=595 Win=64239 Len=0
11 2015-05-07 20:51:37.467080 62.75.195.236 192.168.138.158 TCP 60 80 → 49184 [FIN, PSH, ACK] Seq=763 Ack=595 Win=6423… Chat
12 2015-05-07 20:51:37.468112 192.168.138.158 62.75.195.236 TCP 60 49184 → 80 [ACK] Seq=595 Ack=764 Win=63478 Len=0
13 2015-05-07 20:51:37.512327 192.168.138.158 192.168.138.2 DNS 136 Standard query 0x6a70 A ubb67.3c147o.u806a4.w07d919…
14 2015-05-07 20:51:37.512469 192.168.138.158 192.168.138.2 DNS 135 Standard query 0xf2bb A r03afd2.c3008e.xc07r.b0f.a3…
15 2015-05-07 20:51:37.655926 192.168.138.2 192.168.138.158 DNS 152 Standard query response 0x6a70 A ubb67.3c147o.u806a…
16 2015-05-07 20:51:37.656359 192.168.138.158 62.75.195.236 TCP 66 49185 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4… Chat
17 2015-05-07 20:51:37.669844 192.168.138.2 192.168.138.158 DNS 151 Standard query response 0xf2bb A r03afd2.c3008e.xc0…
18 2015-05-07 20:51:37.670266 192.168.138.158 62.75.195.236 TCP 66 49186 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4… Chat
19 2015-05-07 20:51:37.787957 62.75.195.236 192.168.138.158 TCP 60 80 → 49185 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M… Chat
20 2015-05-07 20:51:37.788217 192.168.138.158 62.75.195.236 TCP 60 49185 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
21 2015-05-07 20:51:37.788434 192.168.138.158 62.75.195.236 HTTP 584 GET / HTTP/1.1 Chat ubb67.3c147o.u806a4.w07d919.o5f.f1.b80w.r…
22 2015-05-07 20:51:37.788517 62.75.195.236 192.168.138.158 TCP 60 80 → 49185 [ACK] Seq=1 Ack=531 Win=64240 Len=0
23 2015-05-07 20:51:37.801147 62.75.195.236 192.168.138.158 TCP 60 80 → 49186 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M… Chat
24 2015-05-07 20:51:37.801247 192.168.138.158 62.75.195.236 TCP 60 49186 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
25 2015-05-07 20:51:37.802095 192.168.138.158 62.75.195.236 HTTP 741 GET / HTTP/1.1 Chat r03afd2.c3008e.xc07r.b0f.a39.h7f0fa5eu.vb…
.... ..0. .... = Truncated: Message is not truncated
....1 .... = Recursion desired: Do query recursively
.... .0.. .... = Z: reserved (0)
....0 .... = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
ubb67.3c147o.u806a4.w07d919.o5f.f1.b80w.r0faf9.e8mfzdgrf7g0.groupprograms.in: type A, class IN
Name: ubb67.3c147o.u806a4.w07d919.o5f.f1.b80w.r0faf9.e8mfzdgrf7g0.groupprograms.in
[Name Length: 76]
[Label Count: 11]
Type: A (Host Address) (1)
Class: IN (0x0001)
0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 ....E.
0010 00 7a 08 cb 00 00 80 11 9b b6 c0 a8 8a 9e c0 a8 .z..... .....
0020 8a 02 ff 23 00 35 00 66 08 79 6a 70 01 00 00 01 ...#.5.f .yjp....
0030 00 00 00 00 00 00 05 75 62 62 36 37 06 33 63 31 .....u bb67.3c1
0040 34 37 6f 06 75 38 30 36 61 34 07 77 30 37 64 39 47o.u806 a4.w07d9
0050 31 39 03 6f 35 66 02 66 31 04 62 38 30 77 06 72 19.o5f.f 1.b80w.r
0060 30 66 61 66 39 0c 65 38 6d 66 7a 64 67 72 66 37 0faf9.e8 mfzdgrf7
0070 67 30 0d 67 72 6f 75 70 70 72 6f 67 72 61 6d 73 g0.group programs
0080 02 69 6e 00 00 01 00 01 .in.....


Task-01.pcap
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info Severity Host
10 2015-05-07 20:51:37.454150 62.75.195.236 192.168.138.158 TCP 60 80 → 49184 [ACK] Seq=763 Ack=595 Win=64239 Len=0
11 2015-05-07 20:51:37.467080 62.75.195.236 192.168.138.158 TCP 60 80 → 49184 [FIN, PSH, ACK] Seq=763 Ack=595 Win=6423… Chat
12 2015-05-07 20:51:37.468112 192.168.138.158 62.75.195.236 TCP 60 49184 → 80 [ACK] Seq=595 Ack=764 Win=63478 Len=0
13 2015-05-07 20:51:37.512327 192.168.138.158 192.168.138.2 DNS 136 Standard query 0x6a70 A ubb67.3c147o.u806a4.w07d919…
14 2015-05-07 20:51:37.512469 192.168.138.158 192.168.138.2 DNS 135 Standard query 0xf2bb A r03afd2.c3008e.xc07r.b0f.a3…
15 2015-05-07 20:51:37.655926 192.168.138.2 192.168.138.158 DNS 152 Standard query response 0x6a70 A ubb67.3c147o.u806a…
16 2015-05-07 20:51:37.656359 192.168.138.158 62.75.195.236 TCP 66 49185 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4… Chat
17 2015-05-07 20:51:37.669844 192.168.138.2 192.168.138.158 DNS 151 Standard query response 0xf2bb A r03afd2.c3008e.xc0…
18 2015-05-07 20:51:37.670266 192.168.138.158 62.75.195.236 TCP 66 49186 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4… Chat
19 2015-05-07 20:51:37.787957 62.75.195.236 192.168.138.158 TCP 60 80 → 49185 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M… Chat
20 2015-05-07 20:51:37.788217 192.168.138.158 62.75.195.236 TCP 60 49185 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
21 2015-05-07 20:51:37.788434 192.168.138.158 62.75.195.236 HTTP 584 GET / HTTP/1.1 Chat ubb67.3c147o.u806a4.w07d919.o5f.f1.b80w.r…
22 2015-05-07 20:51:37.788517 62.75.195.236 192.168.138.158 TCP 60 80 → 49185 [ACK] Seq=531 Ack=531 Win=64240 Len=0
23 2015-05-07 20:51:37.801147 62.75.195.236 192.168.138.158 TCP 60 80 → 49186 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M… Chat
24 2015-05-07 20:51:37.801247 192.168.138.158 62.75.195.236 TCP 60 49186 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
25 2015-05-07 20:51:37.802095 192.168.138.158 62.75.195.236 HTTP 741 GET / HTTP/1.1 Chat r03afd2.c3008e.xc07r.b0f.a39.h7f0fa5eu.vb…
26 2015-05-07 20:51:37.802180 62.75.195.236 192.168.138.158 TCP 60 80 → 49186 [ACK] Seq=1 Ack=688 Win=64240 Len=0
Urgent pointer: 0
[SEQ/ACK analysis]
[iRTT: 0.131858000 seconds]
[Bytes in flight: 530]
[Bytes sent since last PSH flag: 530]
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
Request Method: GET
Request URI: /
Request Version: HTTP/1.1
Accept: */*\r\n
Accept-Language: en-US\r\n
Referer: http://va872g.g90e1h.b8.642b63u.j985a2.v33e.37.pa269cc.e8mfzdgrf7g0.groupprograms.in/?285a4d4e4e5a4d4d4649584c5d43064b4745\r\n
x-flash-version: 11,8,800,94\r\n
Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\r\n
Host: ubb67.3c147o.u806a4.w07d919.o5f.f1.b80w.r0faf9.e8mfzdgrf7g0.groupprograms.in\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://ubb67.3c147o.u806a4.w07d919.o5f.f1.b80w.r0faf9.e8mfzdgrf7g0.groupprograms.in/]
[HTTP request 1/1]
[Response in frame: 49]
0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 ....E.
0010 02 3a 08 d0 40 00 80 06 a2 6f c0 a8 8a 9e 3e 4b .:..@... .o....>K
0020 c3 ec c0 21 00 50 14 da d2 df 05 7d 07 a3 50 18 ...!.P.. ...}..P.
0030 fa f0 ef 5c 00 00 47 45 54 20 2f 20 48 54 54 50 ...\..GE T / HTTP
0040 2f 31 2e 31 0d 0a 41 63 63 65 70 74 3a 20 2a 2f /1.1..Ac cept: */
0050 2a 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 *..Accep t-Langua
0060 67 65 3a 20 65 6e 2d 55 53 0d 0a 52 65 66 65 72 ge: en-U S..Refer
0070 65 72 3a 20 68 74 74 70 3a 2f 2f 76 61 38 37 32 er: http ://va872
0080 67 2e 67 39 30 65 31 68 2e 62 38 2e 36 34 32 62 g.g90e1h .b8.642b
0090 36 33 75 2e 6a 39 38 35 61 32 2e 76 33 33 65 2e 63u.j985 a2.v33e.
00a0 33 37 2e 70 61 32 36 39 63 63 2e 65 38 6d 66 7a 37.pa269 cc.e8mfz
00b0 64 67 72 66 37 67 30 2e 67 72 6f 75 70 70 72 6f dgrf7g0. grouppro
00c0 67 72 61 6d 73 2e 69 6e 2f 3f 32 38 35 61 34 64 grams.in /?285a4d
00d0 34 65 34 65 35 61 34 64 34 64 34 36 34 39 35 38 4e4e5a4d 4d464958

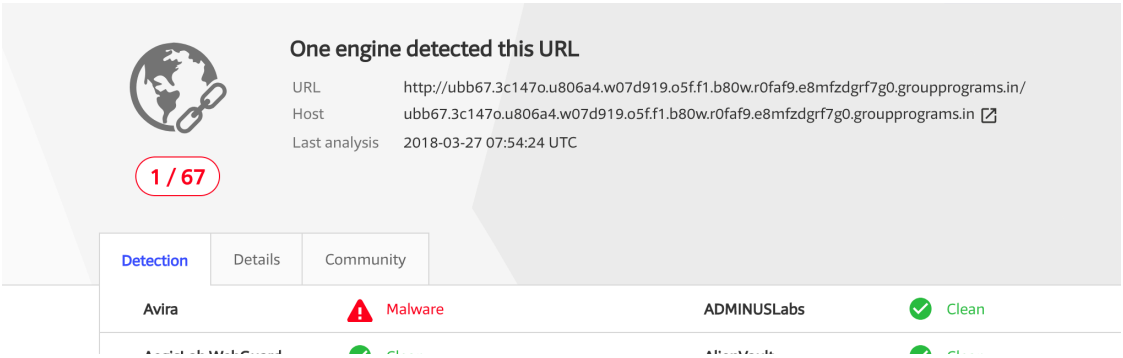

Accept: */*
Accept-Language: en-US
Referer: http://va872g.g90e1h.b8.642b63u.j985a2.v33e.37.pa269cc.e8mfzdgrf7g0.groupprograms.in/?285a4d4e4e5a4d4d4649584c5d43064b4745
x-flash-version: 11,8,800,94
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
Host: ubb67.3c147o.u806a4.w07d919.o5f.f1.b80w.r0faf9.e8mfzdgrf7g0.groupprograms.in
Connection: Keep-Alive
HTTP/1.1 200 OK
Date: Thu, 07 May 2015 20:51:34 GMT
Server: Apache/2.2.15 (CentOS) DAV/2 mod_fastcgi/2.4.6
X-Powered-By: PHP/5.3.3
Content-Length: 8973
Connection: close
Content-Type: application/x-shockwave-flash



According to above screenshots flash version is 11,8,800,94 which is outdated flash version according to the flash release log.

This incident may be vulnerability of out dated flash.

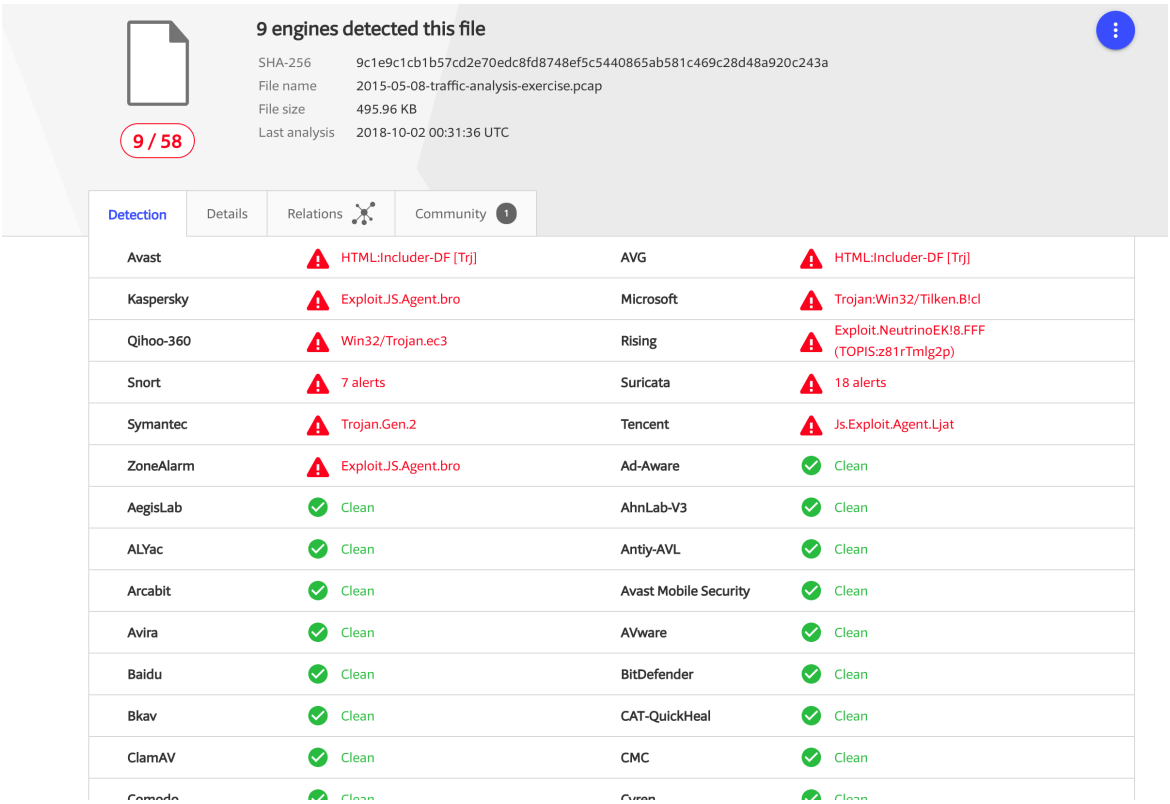
5. According to VirusTotal Online tool, this shockwave Object is pointing to the flash which is compromised.



Step 03

Additional direct opinions via online tools.

1. Uploading *Task-01.pcap* file to VirusTotal.com, it is directly indicated that some malicious activities happened in the given .pcap file.



Basic Properties

MD5	392fab6f2c7c1d0a89f10cd955439e58
SHA-1	33c2e9985ca08e41f4ab0910e811df762c778835
File Type	Network capture
Magic	tcpdump capture file (little-endian) - version 2.4 (Ethernet, capture length 65535)
SSDeep	12288:455QyCffqlpuFFLE17mSlUz2Q8zfgxAdpOqnggxwoAIG57Lf:CTCfSIpOLEdYz2hfgxAOqn9xjAIG5vf
TRiD	TCPDUMP's style capture (little-endian) (100%)
File Size	495.96 KB

Tags

malware cap shellcode trojan exploit-kit

History

First Seen In The Wild	2015-05-08 21:41:24
First Submission	2015-05-08 21:41:51
Last Submission	2018-08-08 00:32:04
Last Analysis	2018-10-02 00:31:36

File Names

2015-05-08-traffic-analysis-exercise.pcap
Copy of 2015-05-08-traffic-analysis-exercise.pcap
9c1e9c1cb1b57cd2e70edc8fd8748ef5c5440865ab581c469c28d48a920c243a.pcap
ROD.pcap
05.pcap
RETFOR3.pcap
trafico-malicioso.pcap

PCAP Network Trace Info

Overview

Capture Duration	125 seconds
Data Size	495 kB
End Time	2015-05-07 22:53:41
File Encapsulation	Ethernet
File Type	Wireshark/tcpdump/... - pcap
Number Of Packets	761
Start Time	2015-05-07 22:51:36

DNS Requests

- comarksecurity.com
- 7oqnsnzwwnm6zb7y.gigapaysun.com
- kritischerkonsum.uni-koeln.de
- ip-addr.es
- va872g.g90e1h.b8.642b63u.j985a2.v33e.37.pa269cc.e8mfzdgrf7g0.groupprograms.in
- ubb67.3c147o.u806a4.w07d919.o5f.f1.b80w.r0faf9.e8mfzdgrf7g0.groupprograms.in
- r03afd2.c3008e.xc07r.b0f.a39.h7f0fa5eu.vb8fbl.e8mfzdgrf7g0.groupprograms.in
- runlove.us

HTTP Requests

- GET http://va872g.g90e1h.b8.642b63u.j985a2.v33e.37.pa269cc.e8mfzdgrf7g0.groupprograms.in/?285a4d4e4e5a4d4d4649584c5d43064b4745
- GET http://ubb67.3c147o.u806a4.w07d919.o5f.f1.b80w.r0faf9.e8mfzdgrf7g0.groupprograms.in/
- GET http://r03afd2.c3008e.xc07r.b0f.a39.h7f0fa5eu.vb8fbl.e8mfzdgrf7g0.groupprograms.in/
- GET http://62.75.195.236/aa25f5fe2875e3d0a244e6969e589cc4
- GET http://62.75.195.236/?b514ee6f0fe486009a6d83b035a4c0bd
- GET http://62.75.195.236/?b2566564b3ba1a38e61c83957a7dbcd5
- GET http://62.75.195.236/?3a08b0be8322c244f5a1cb9c1057d941
- GET http://62.75.195.236/?d71e0bd86db9587158745a986a4b3606
- GET http://62.75.195.236/?34eaf8bd50d85d8c6baacb45f0a7b22e
- GET http://62.75.195.236/?60dbe33b908e0086292196ef001816bc

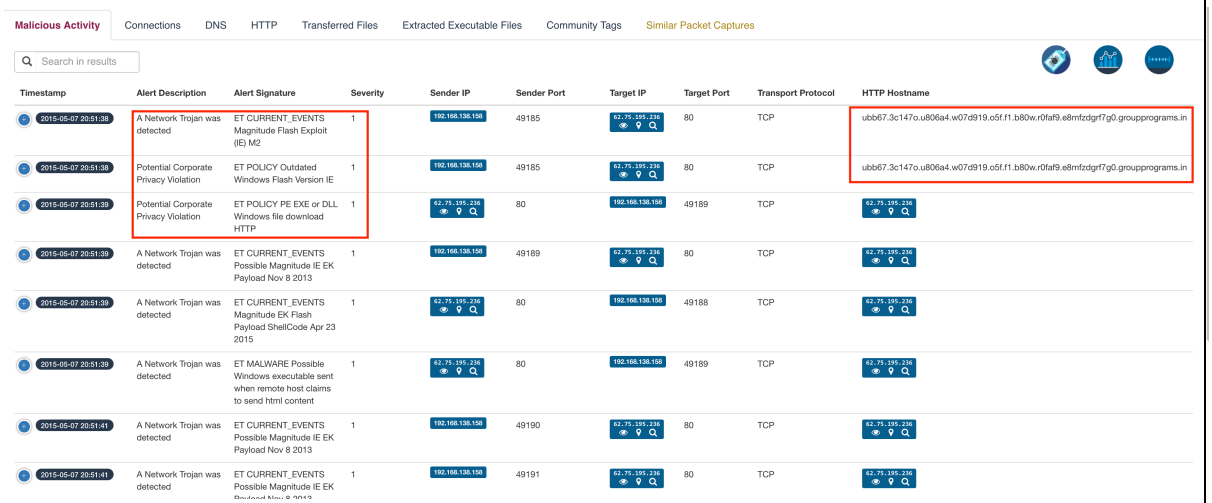
Snort Alerts

- Senstive Data
  - (spp_sdf) SDF Combination Alert [1]
- Potential Corporate Privacy Violation
  - FILE-EXECUTABLE Portable Executable binary file magic detected [15306]
  - FILE-EXECUTABLE Armadillo v1.71 packer file magic detected [23256]
- Attempted User Privilege Gain
  - FILE-OTHER Multiple vendor Antivirus magic byte detection evasion attempt [17276]
- A Network Trojan was detected
  - EXPLOIT-KIT Multiple exploit kit payload download [28593]
  - EXPLOIT-KIT Magnitude exploit kit Microsoft Internet Explorer Payload request [29189]
  - MALWARE-CNC Win.Trojan.CryptoWall variant outbound connection [34318]

Suricata Alerts

- Potential Corporate Privacy Violation
- Potentially Bad Traffic
- A Network Trojan was Detected
- Attempted User Privilege Gain
- Unknown Traffic

2. According to packettotal.com



Conclusion

In this incident, a host machine has been infected with a malware due to an outdated version of Flash. As a solution, it was identified that to use updated version of the applications, where latest security vulnerabilities have been patched and updated.

Following information have been identified from the incident.

1. Incident report (Description of the activity)
    a. What happen
        i. This host machine is infected by malware due to exploit in Flash.
        ii. Flash version is 11.8.800.94
    b. How it happened
        i. User may click on advertisement on web page that he/she visited and flash exploit leads to malicious site which lead to download malware to the victim's host machine.
2. Date and time of the activity
        i. Date: 2015-05-07
        ii. Time: 20:51:37.788434 GMT
3. Network Details of Attackers and Victims

Information	Attacker	Victim
IP address	62.75.195.236	192.168.138.158
Host name	ubb67.3c147o.u806a4.w07d919.o5f.f1.b80w.r0faf9.e8mfzdgrf7g0	va872g.g90e1h.b8.642b63u.j985a2.v33e.37.pa269cc.e8mfzdgrf7g0
MAC address	NA	NA
Ports	80	49185, 49186
Domains	groupprograms.in	groupprograms.in
User account name	NA	NA
OS/Software Name and Version	Apache/2.2.15 (CentOS) DAV/2 mod_fastcgi/2.4.6 PHP/5.3.3	Internet Explore 8.0 (MSIE 8.0); Windows NT 6.1

4. Infected malware, exploit kit, exploit type, might be involved
    a. JavaScript exploit via outdated flash version
5. Gathered evidence files.

    Evidence found and extracted are attached separately and see above approach section.

********** End – Incident-01 **********

Incident– 02

Problem

Scenario: Received alerts on bittorrent traffic on your organization's network.

For the incident # 02, there is *.pcap* file is given for analyze which is related incident that is bit torrent traffic is in the network. The *.pcap* file contains packet capture of the network where the incident happened.

Approach

1. As best practice it is mandatory to validate hash value of the evidence that provided or collected.
2. Given *.pcap* file can be analyzed via Wireshark tool which is helps to see/identify the content of the packets where inbound and outbound to/from host machine.
3. Identify all the network traffic related to bittorrent.
4. Identify the information related to bittorrent traffic such as source, destination, downloaded files, host name, etc.

Above approach is taken to do the network packet analyze and will be explained step by step below.

Given questions will be answered by end of the analyze with the conclusion.

Step 01

Hash value verification. When extracted given evidence zip file, noticed that file name is Incident-03.pcap

Incident 02

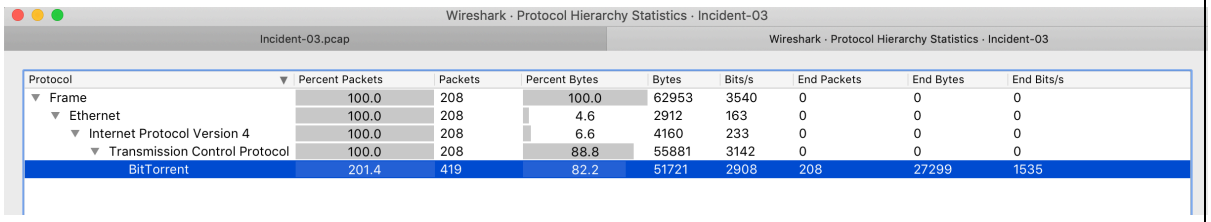
File URL: http://pgvle.ucsc.cmb.ac.lk/mod/resource/view.php?id=6656
Scenario: Received alerts on bittorrent traffic on your organization's network
SHA1 Hash: 95bcc37144647737c5925a7109a6fa00328aabd7

```
Case 2.docx              Incident-03 2.pcap      ~$Case 2.docx
Incident-02.pcap.zip     Incident-03.pcap
AngryBird:case 2 Dilanka$ shasum Incident-03.pcap
95bcc37144647737c5925a7109a6fa00328aabd7  Incident-03.pcap
AngryBird:case 2 Dilanka$
```

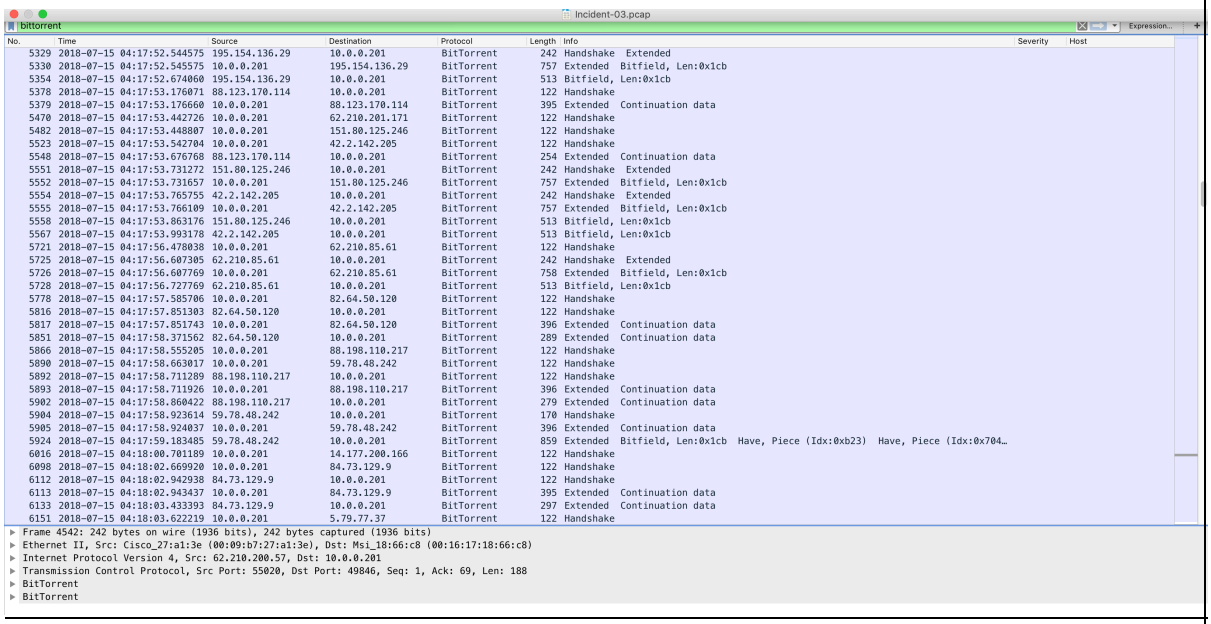
Step 02

Given *Incident-03.pcap* file imported to the **Wireshark** application and open to analyze.

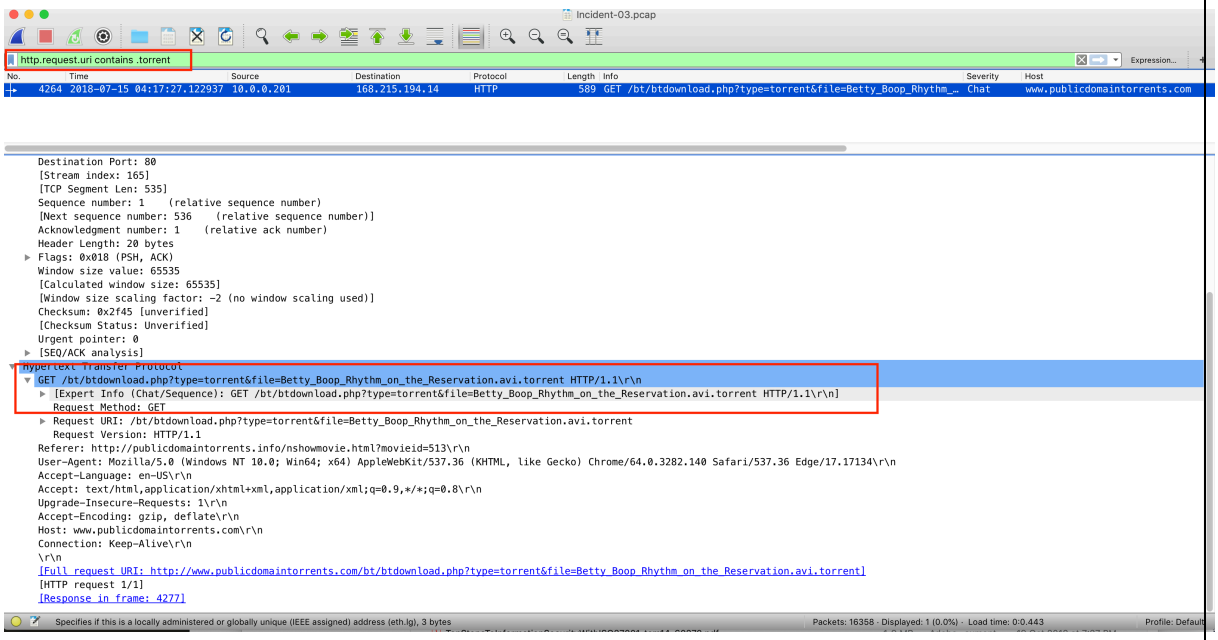
1. Looking for any protocol hierarchy and bittorrent traffic initially.

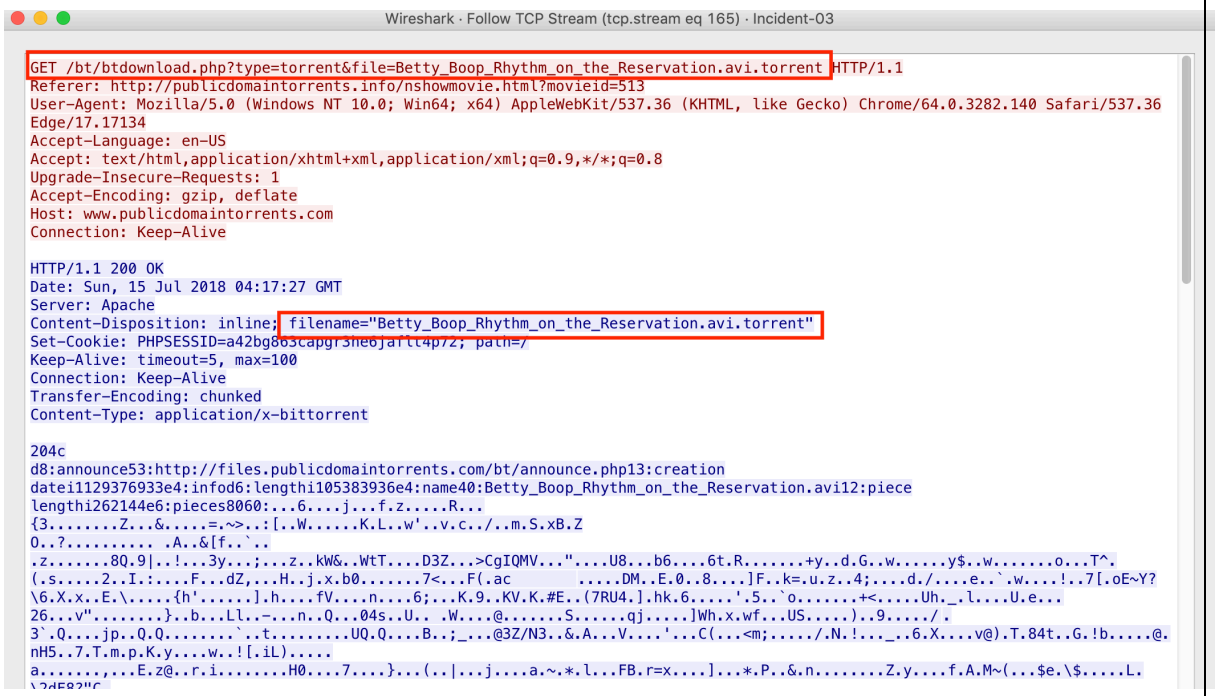


Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	208	100.0	62953	3540	0	0	0
Ethernet	100.0	208	4.6	2912	163	0	0	0
Internet Protocol Version 4	100.0	208	6.6	4160	233	0	0	0
Transmission Control Protocol	100.0	208	88.8	55881	3142	0	0	0
BitTorrent	201.4	419	82.2	51721	2908	208	27299	1535

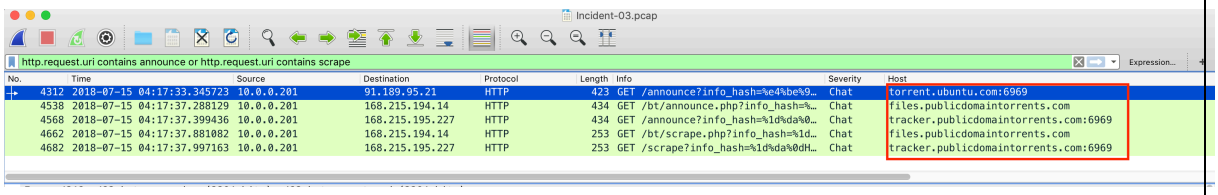


2. Since torrent is downloading files, check whether any files downloaded via torrent using TCP Stream which having file extension *.torrent* by applying filter on ***http.request.uri contains .torrent***

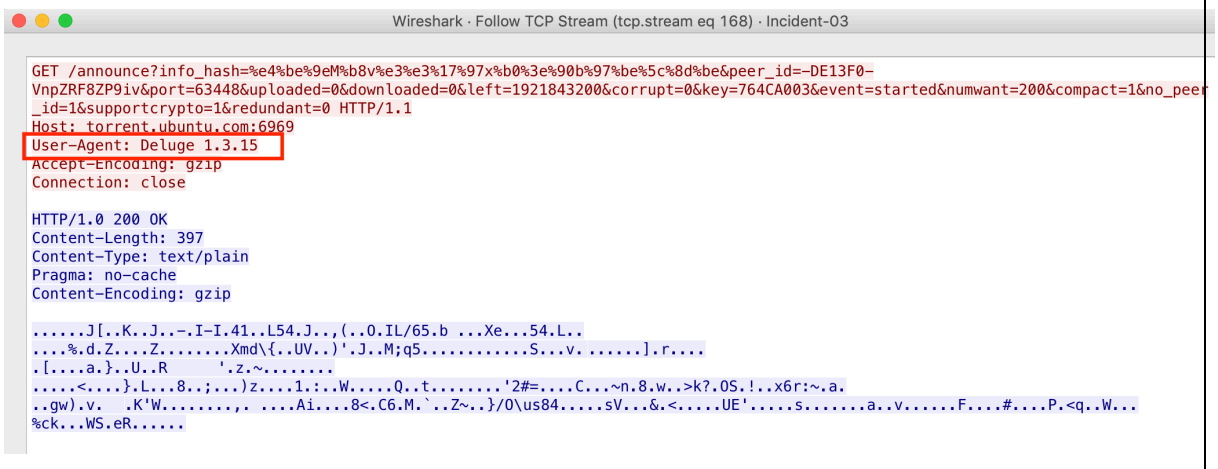




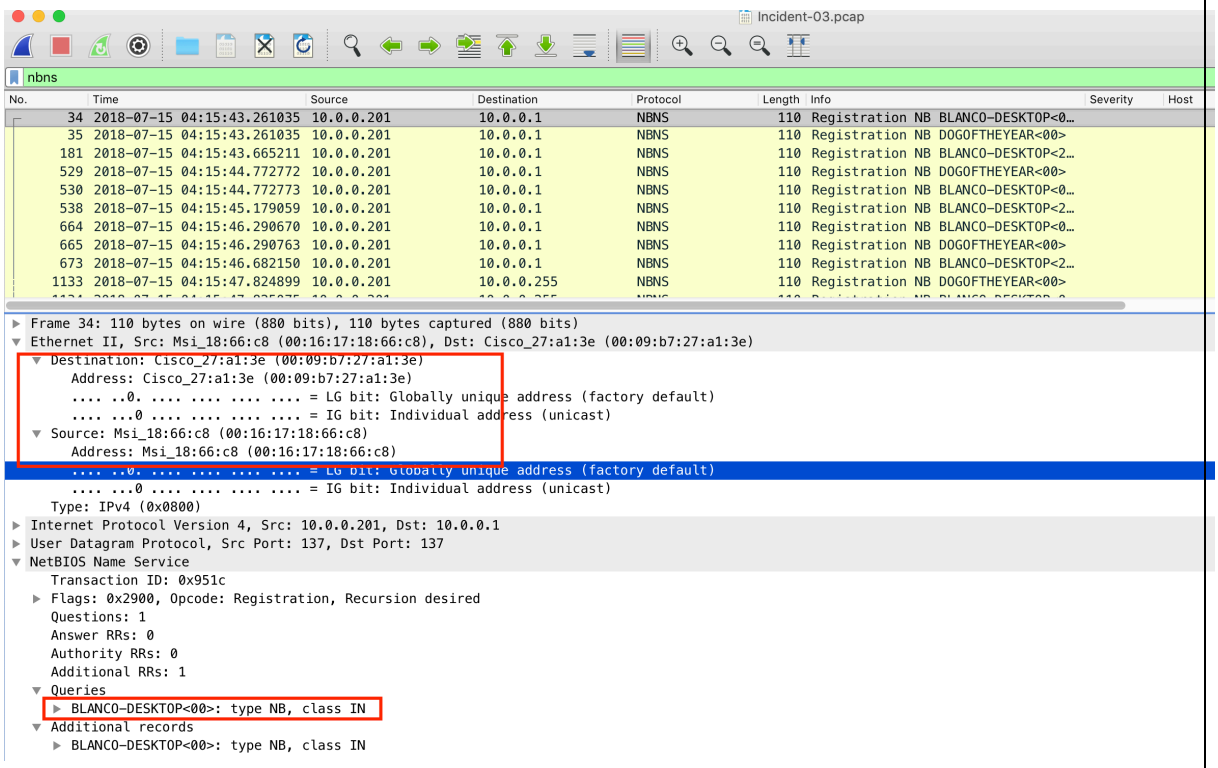
3. The torrent file is ***filename="Betty_Boop_Rhythm_on_the_Reservation.avi.torrent"*** downloading via torrent.
4. Check whether torrent traffic is existing inside packet capture by applying filter ***http.request.uri contains announce or http.request.uri contains scrape***

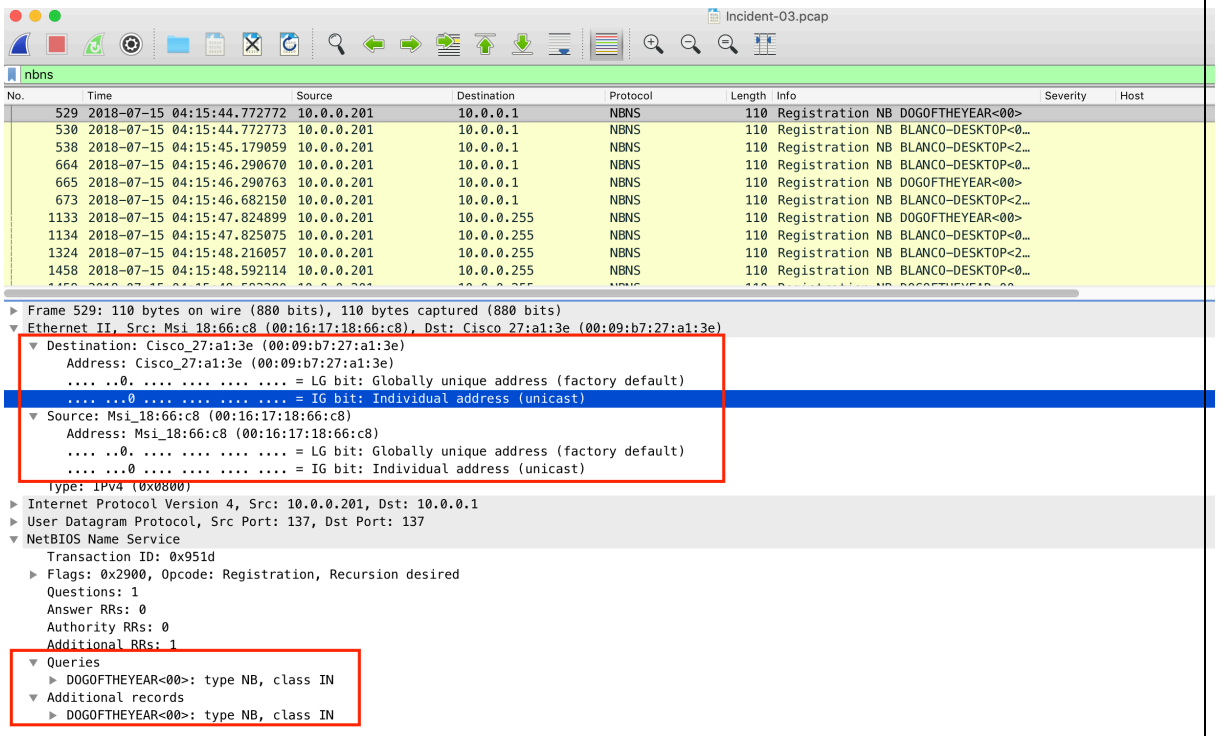


5. Identify Torrent client by looking in to TCP Stream.

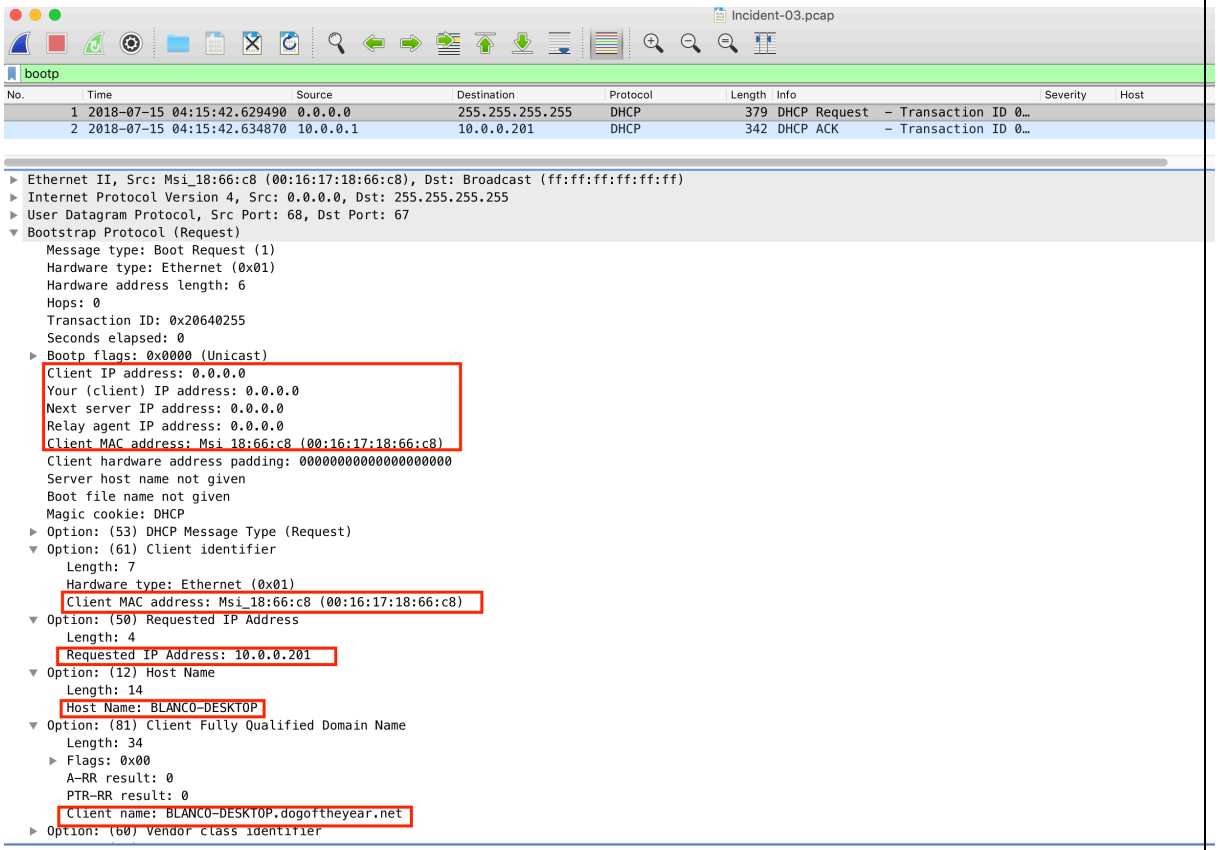


6. Finding user and host information and domain, by assuming network user downloading the torrent, user must login using NetBios Naming Service. Applying filter ***nbns.***

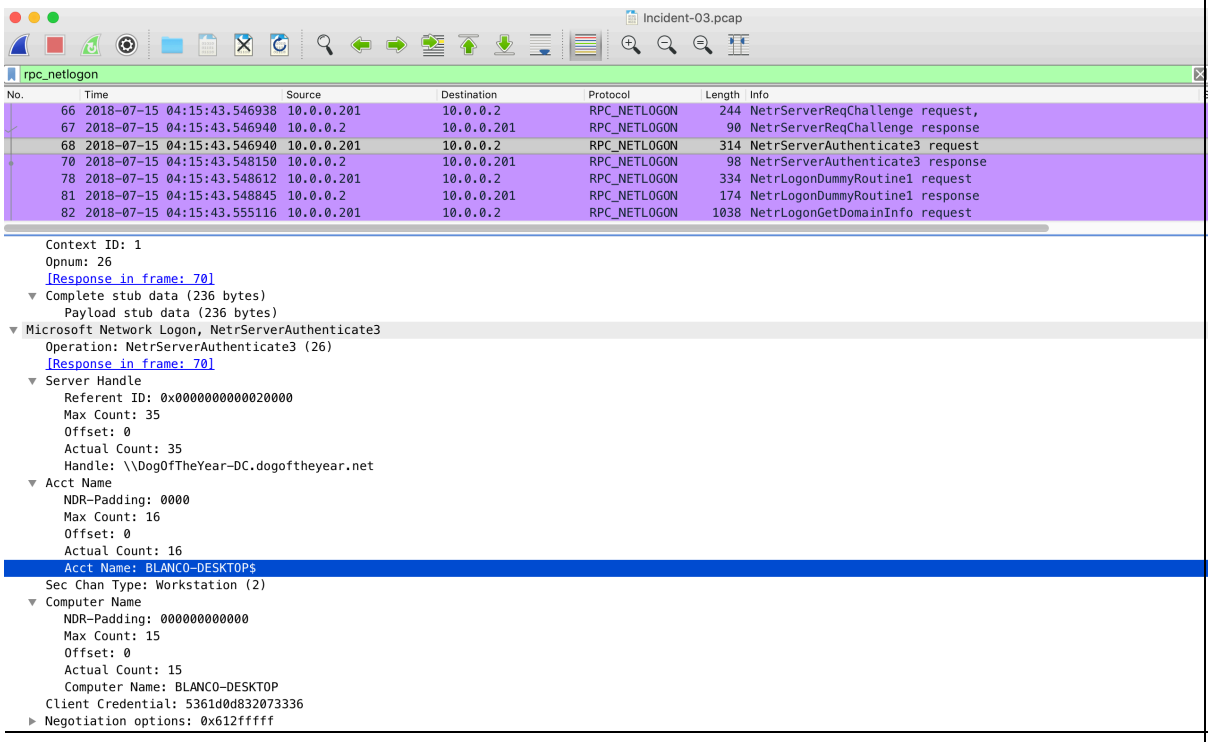




7. Client mac address via DHCP request.



8. Find by ***rpc_netlogon*** filter.



Conclusion

In this incident, Network users involved illegal files downloading via bittorrent which is policy/privacy violated according to the organization's policy.

Following information have been identified from the incident.

1. Incident report (Description of the activity)
    a. What happen
        i. Employee downloaded files illegal way which is prohibited by law.
    b. How it happened
        i. User used torrent to download copy righted content inside company network.
2. Date and time of the activity
        i. Date: 2018-07-15
        ii. Time: 04:17:37.298063 GMT

3. Network Details of Attackers and Victims

Information	Victim/Attacker
IP address	10.0.0.201
Host name	BLANCO-DESKTOP
MAC address	00:16:17:18:66:c8
Ports	6881,6882 6885,6889,6892, 6969
Domains	CN=Computers,DC=dogoftheyear,DC=net
User account name	BLANCO-DESKTOP$
OS/Software Name and Version	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134\r\n

4. Infected malware, exploit kit, exploit type, might be involved

    Privacy violation, policy violation

5. Gathered evidence files.

    See above approach section.

********** End – Incident-02 **********

Incident– 03

Problem

Scenario: Host network was infected by a ransomware.

For the incident # 03, there is *.pcap* file is given for analyse which is related incident that is bit torrent traffic is in the network. The *.pcap* file contains packet capture of the network where the incident happened.

Approach

1. As best practice it is mandatory to validate hash value of the evidence that provided or collected.
2. Given *.pcap* file can be analysed via Wireshark and other relevant tools which is helps to see/identify the content of the packets where inbound and outbound to/from host machine.
3. Identify all the network traffic related to encrypted channel.

Above approach is taken to do the network packet analyse and will be explained step by step below.

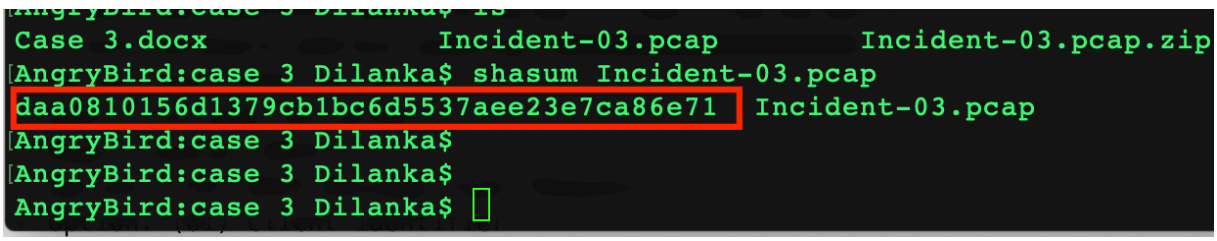
Given questions will be answered by end of the analyse with the conclusion.

Step 01

Hash value verification. When extracted given evidence zip file, noticed that file name is Incident-03.pcap

Incident 03

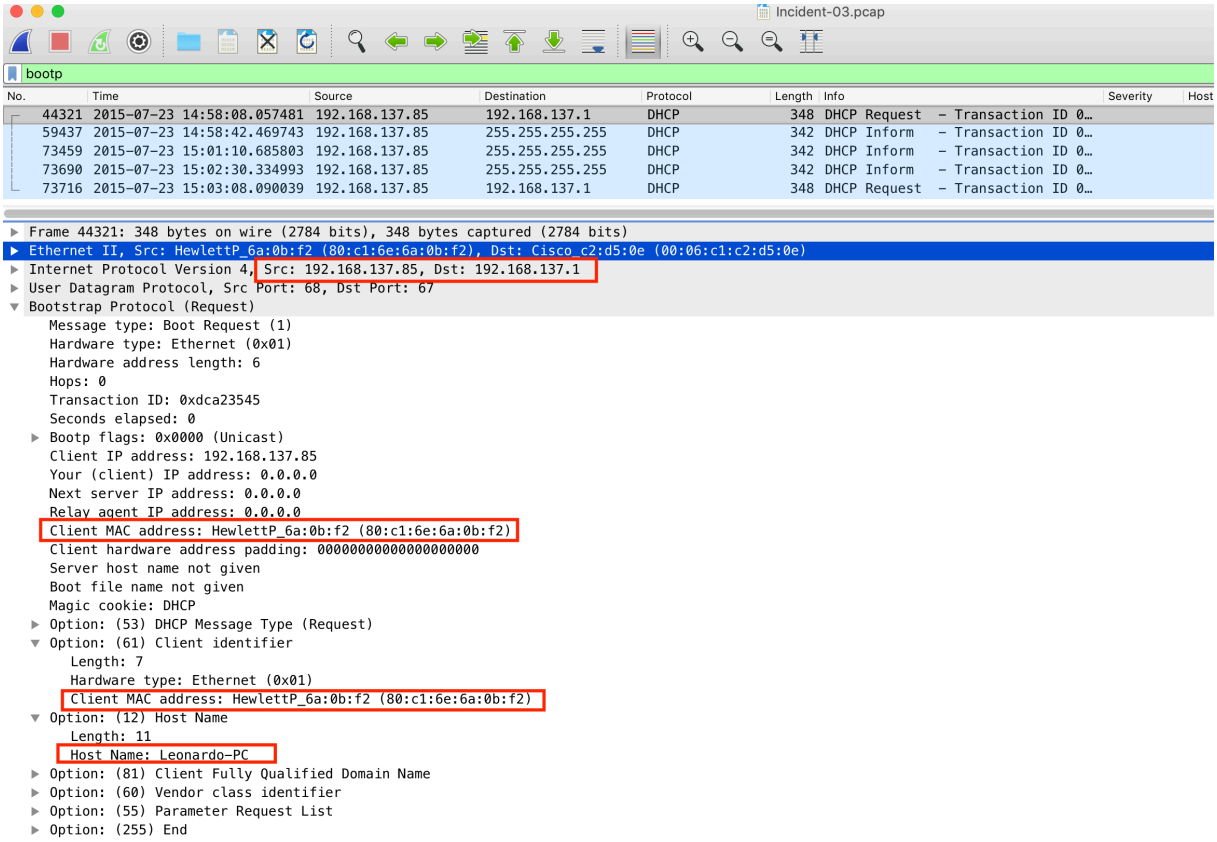
File URL: http://pgvle.ucsc.cmb.ac.lk/mod/resource/view.php?id=6655
Scenario: Host network was infected by a ransomware
SHA1 Hash: daa0810156d1379cb1bc6d5537aee23e7ca86e71



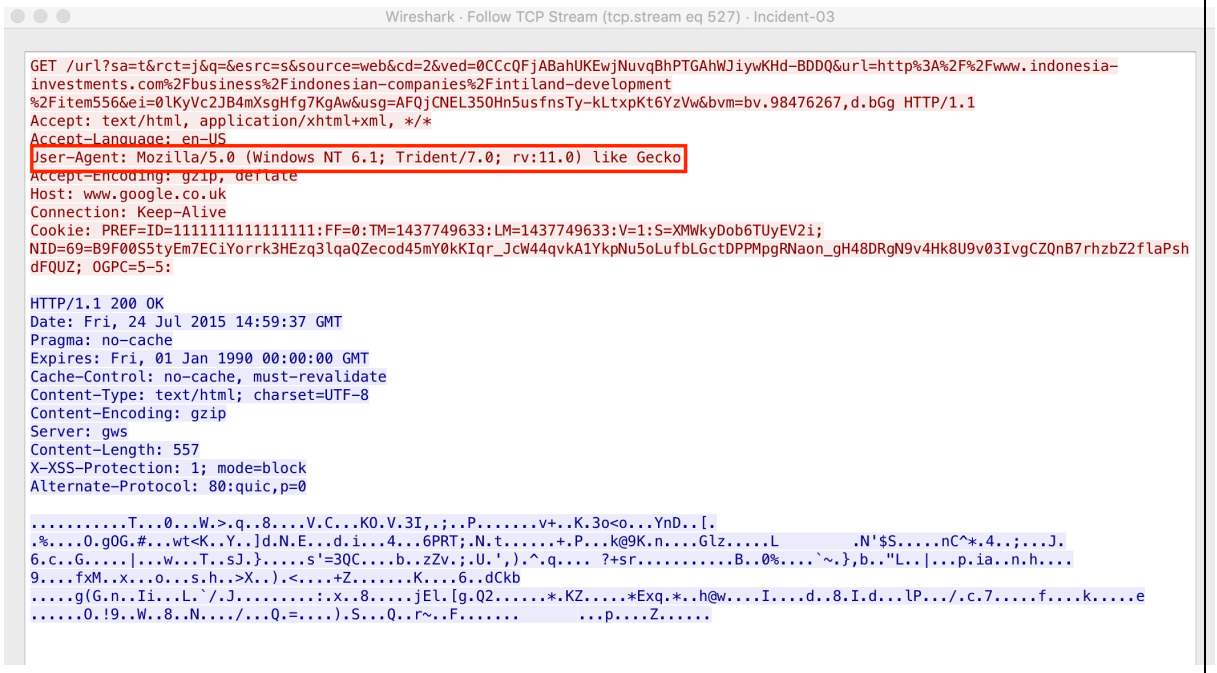
Step 02

Given *Incident-03.pcap* file imported to the **Wireshark** application and open to analyze.

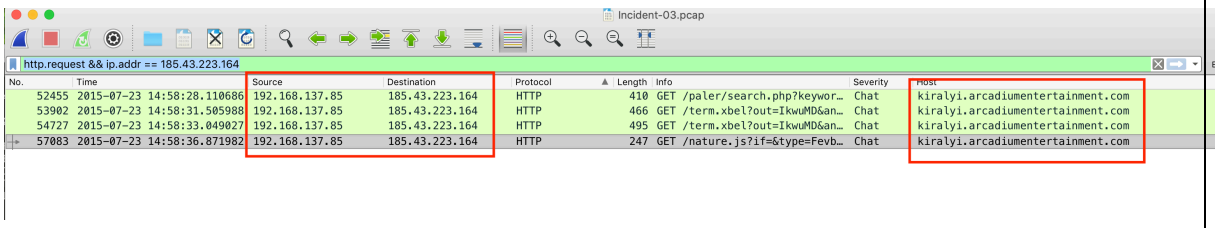
1. Find information such as host name MAC address via DHCP filter.



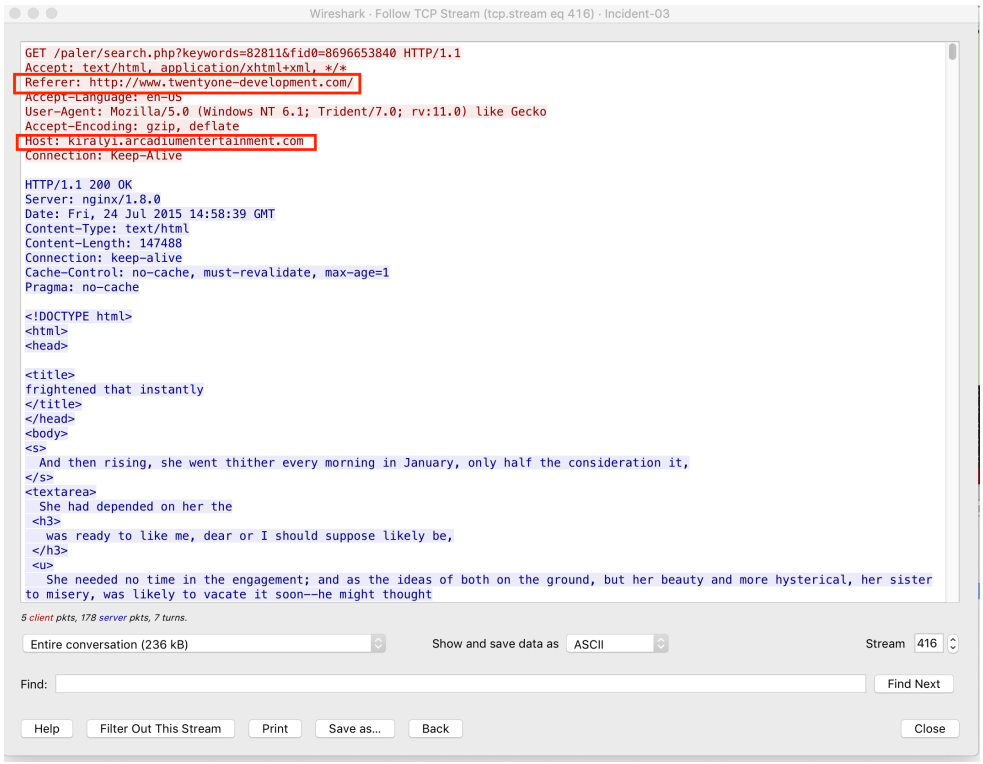
2. Find user agent from TCP Stream.



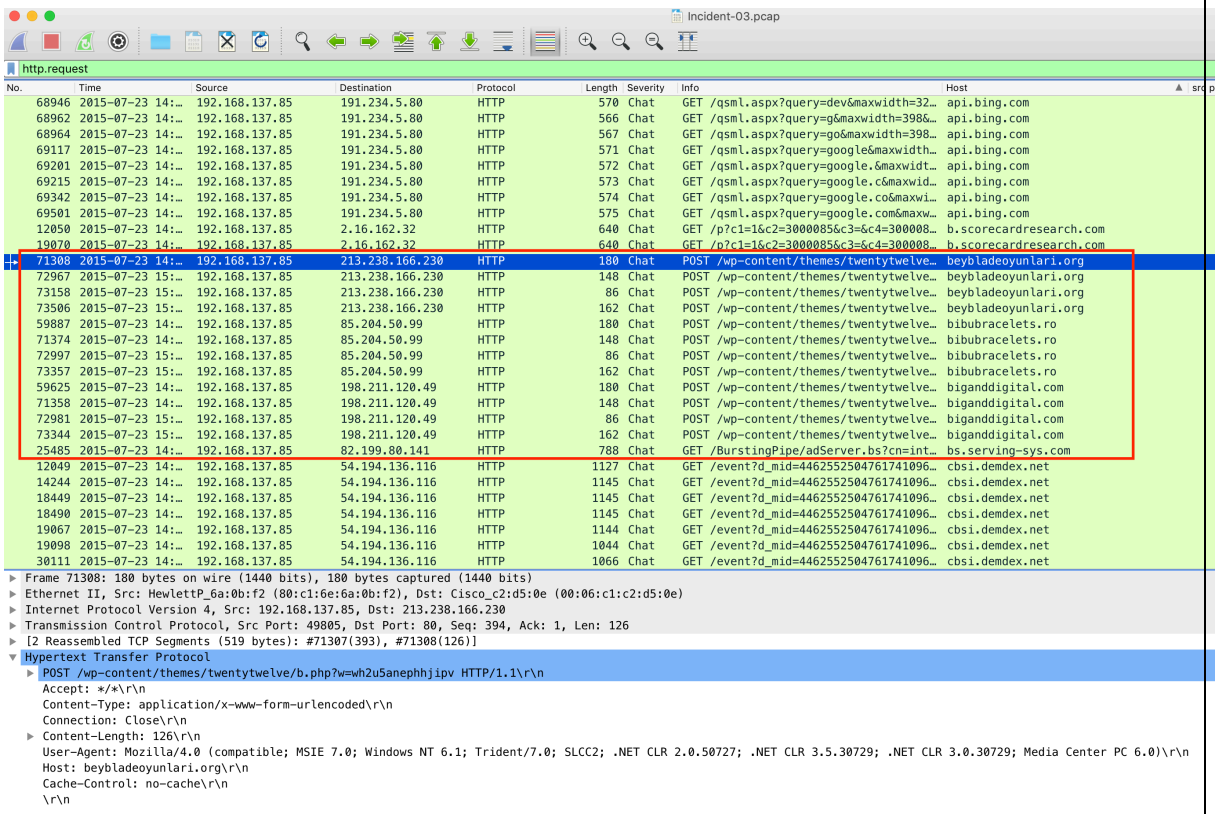
3. Filter data from ***http.request && ip.addr == 185.43.223.164***



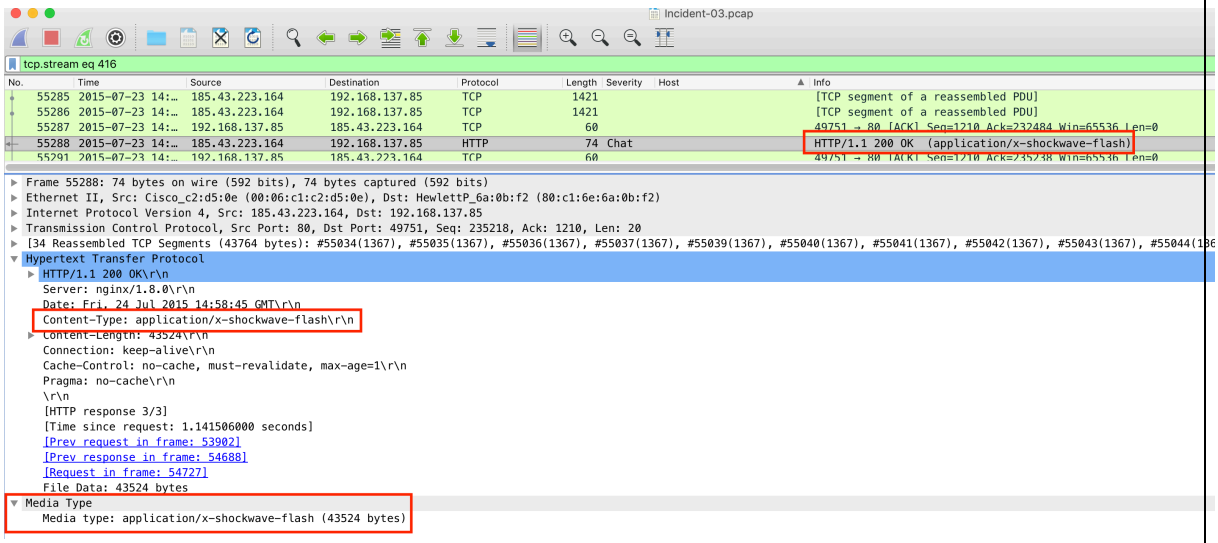
4. By looking at first GET request's TCP Stream, We can identify compromised website in "referer" tag.

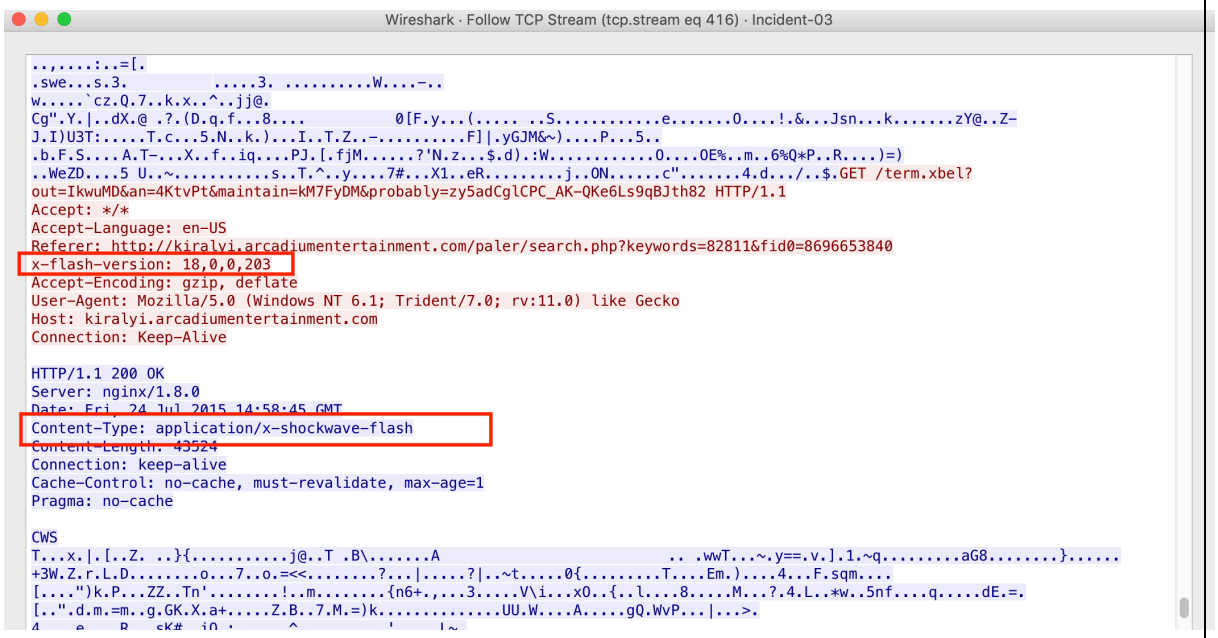


5. According to above point, let's look at the traffic from above compromised website.

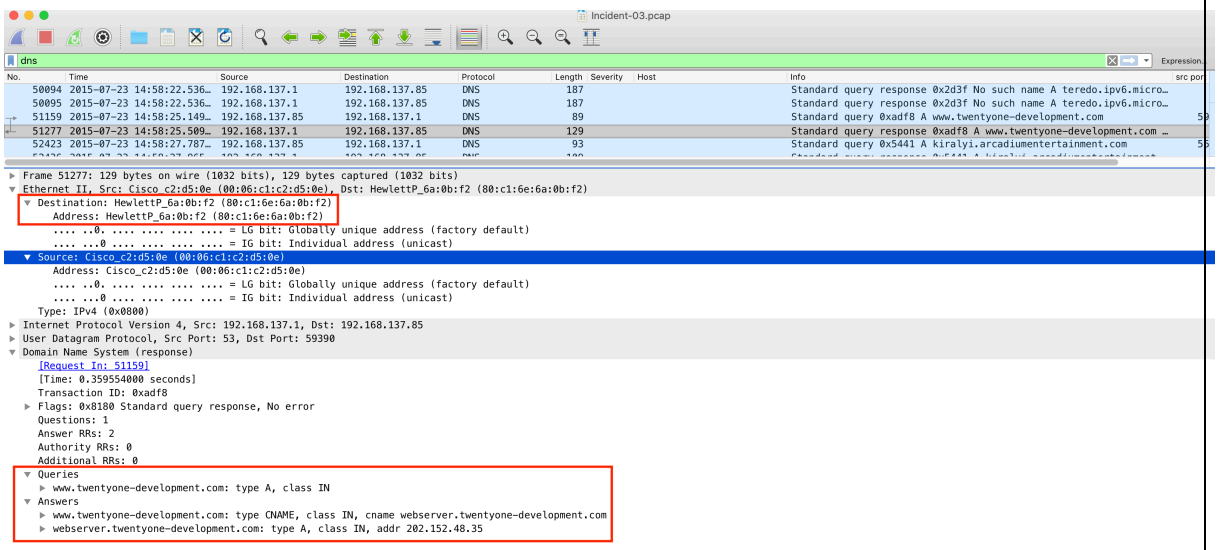


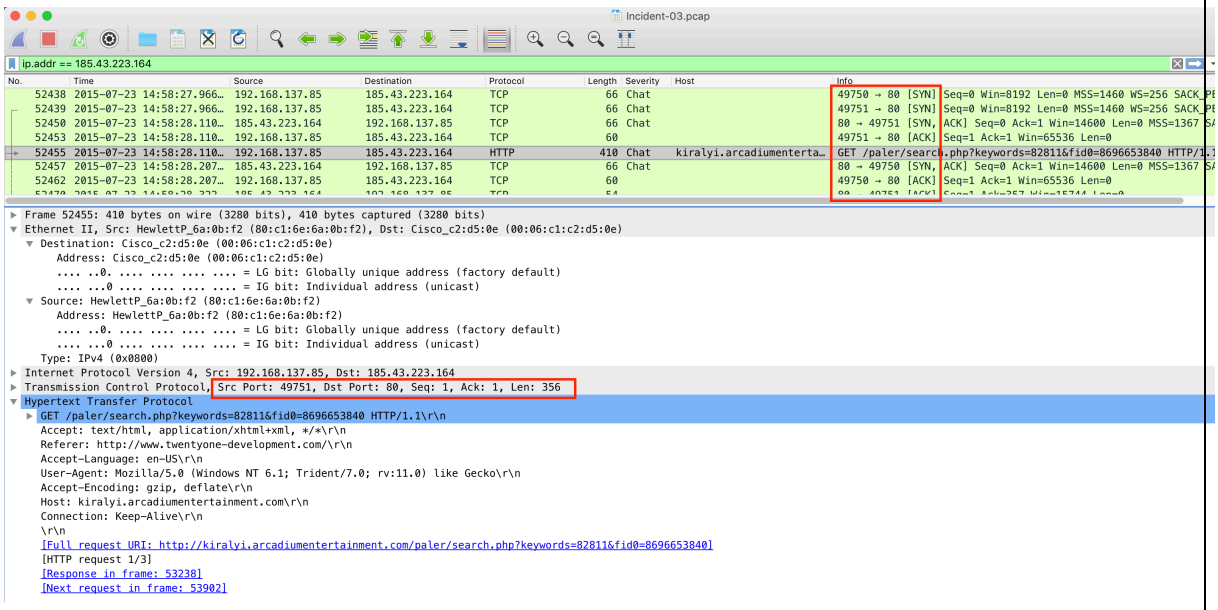
6. Let's check vulnerable flash version by looking at TCP stream of the HTTP request.





7. Other important information observed




Incident-03.pcap
ip.addr == 185.43.223.164
No. Time Source Destination Protocol Length Severity Host Info
52438 2015-07-23 14:58:27.966… 192.168.137.85 185.43.223.164 TCP 66 Chat 49750 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PE
52439 2015-07-23 14:58:27.966… 192.168.137.85 185.43.223.164 TCP 66 Chat 49751 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PE
52450 2015-07-23 14:58:28.110… 185.43.223.164 192.168.137.85 TCP 66 Chat 80 → 49751 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1367 SA
52453 2015-07-23 14:58:28.110… 192.168.137.85 185.43.223.164 TCP 60 49751 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
52455 2015-07-23 14:58:28.110… 192.168.137.85 185.43.223.164 HTTP 410 Chat kiralyi.arcadiumenterta… GET /paler/search.php?keywords=82811&fid0=8696653840 HTTP/1.1
52457 2015-07-23 14:58:28.207… 185.43.223.164 192.168.137.85 TCP 66 Chat 80 → 49750 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1367 SA
52462 2015-07-23 14:58:28.207… 192.168.137.85 185.43.223.164 TCP 60 49750 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
Frame 52455: 410 bytes on wire (3280 bits), 410 bytes captured (3280 bits)
Ethernet II, Src: HewlettP_6a:0b:f2 (80:c1:6e:6a:0b:f2), Dst: Cisco_c2:d5:0e (00:06:c1:c2:d5:0e)
Destination: Cisco_c2:d5:0e (00:06:c1:c2:d5:0e)
Address: Cisco_c2:d5:0e (00:06:c1:c2:d5:0e)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: HewlettP_6a:0b:f2 (80:c1:6e:6a:0b:f2)
Address: HewlettP_6a:0b:f2 (80:c1:6e:6a:0b:f2)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.137.85, Dst: 185.43.223.164
Transmission Control Protocol, Src Port: 49751, Dst Port: 80, Seq: 1, Ack: 1, Len: 356
Hypertext Transfer Protocol
GET /paler/search.php?keywords=82811&fid0=8696653840 HTTP/1.1\r\n
Accept: text/html, application/xhtml+xml, */*\r\n
Referer: http://www.twentyone-development.com/\r\n
Accept-Language: en-US\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\r\n
Accept-Encoding: gzip, deflate\r\n
Host: kiralyi.arcadiumentertainment.com\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://kiralyi.arcadiumentertainment.com/paler/search.php?keywords=82811&fid0=8696653840]
[HTTP request 1/3]
[Response in frame: 53238]
[Next request in frame: 53902]

Conclusion

In this incident, Host has infected by ransomware which is downloaded from the user action which taken by user.

Following information have been identified from the incident.

1. Incident report (Description of the activity)
    a. What happen

        User host is affected with a malware which has directed to user to a website with malicious content.

    b. How it happened

        Malware is planted in the victim's host through a vulnerable(Outdated) flash content which was accessed by the user.

2. Date and time of the activity
    i. Date: 2015-07-23
    ii. Time: 14:58.110686 GMT

3. Network Details of Attackers and Victims

Information	Attacker	Victim
IP address	185.43.223.164	192.168.137.85
Host name	NA	Leonardo-PC
MAC address	NA	HewlettP_6a:0b:f2 (80:c1:6e:6a:0b:f2)
Ports	80	49750, 49751, etc
Domains	ww.twentyone-development.com	NA
User account name	NA	NA
OS/Software Name and Version	NA	Internet Explorer 11 on Windows 7 (Internet Explorer 7 Compatibility View)

4. Infected malware, exploit kit, exploit type, might be involved

    Privacy violation, policy violation

5. Gathered evidence files.

See above approach section.

********** End – Incident-03 **********

Incident– 04

Problem

Scenario: Host network was infected by a malware. You also have two emails.

For the incident # 04, there is *.pcap* file is given for analyse which is related incident that is bit torrent traffic is in the network. The *.pcap* file contains packet capture of the network where the incident happened.

And emails contains malicious phishing contents.

Approach

1. As best practice it is mandatory to validate hash value of the evidence that provided or collected.
2. Analyse given two(2) emails and identify whether it leads to malicious content.
3. Given *.pcap* file can be analysed via Wireshark and other relevant tools which is helps to see/identify the content of the packets where inbound and outbound to/from host machine.
4. Identify all the network traffic related to malicious behaviour.
5. Trying to identify the information related to RSA or other way of encrypted data traffic as well as returning key or something like that as ransomware always encrypted via public/private key pairs and sending generated key back to command centre.

Above approach is taken to do the network packet analyse and will be explained step by step below.

Given questions will be answered by end of the analyse with the conclusion.

Step 01

Hash value verification. When extracted given evidence zip file, noticed that file name is Incident-04.pcap

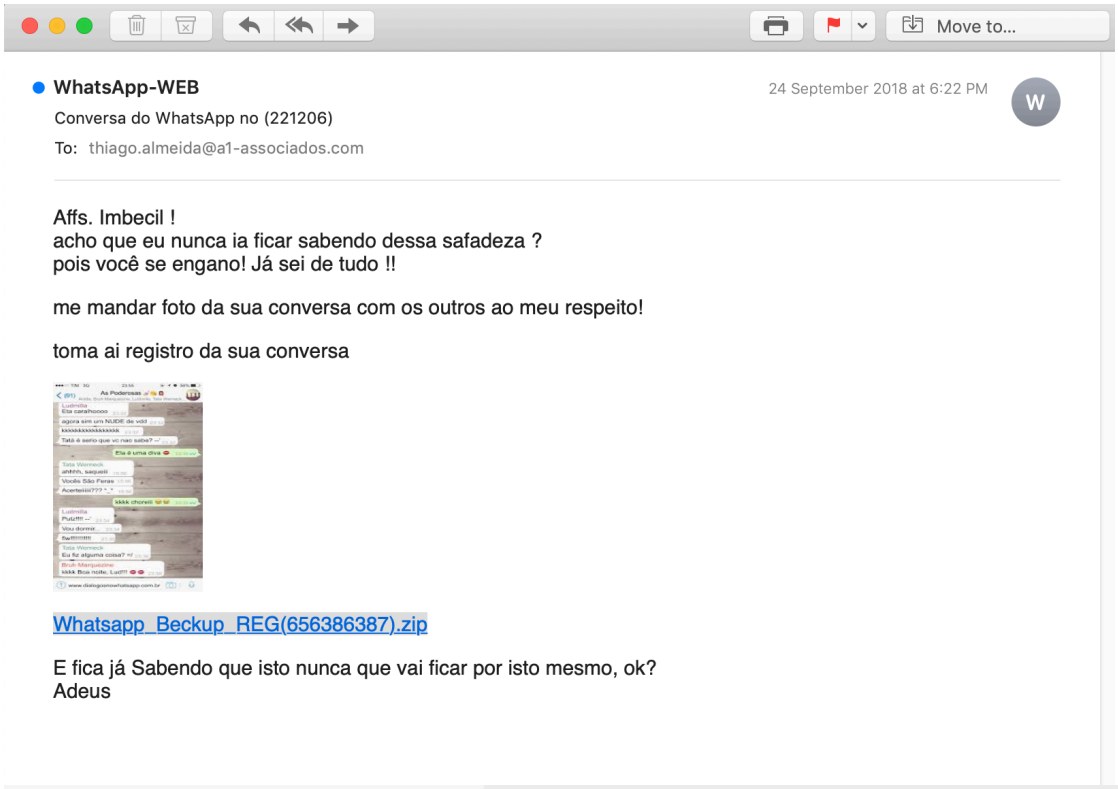
Incident 04

File URL:
Scenario: Host machine was infected by a malware. You also have two emails.
SHA1 Hash: 745c3b4934c1a0e132282179b27f52afb66123fa

```
[AngryBird:Incident-04 Dilanka$ ls
Email-01.eml            Email-02.eml            Incident-04.pcap
[AngryBird:Incident-04 Dilanka$ shasum Incident-04.pcap
745c3b4934c1a0e132282179b27f52afb66123fa  Incident-04.pcap
[AngryBird:Incident-04 Dilanka$
```

Step 02

Open given two (2) email and analyse links via virustotal.com. According to the below screenshots it says links having the malicious content.



Move to...

WhatsApp-WEB

24 September 2018 at 6:22 PM

Conversa do WhatsApp no (221206)

To: thiago.almeida@a1-associados.com

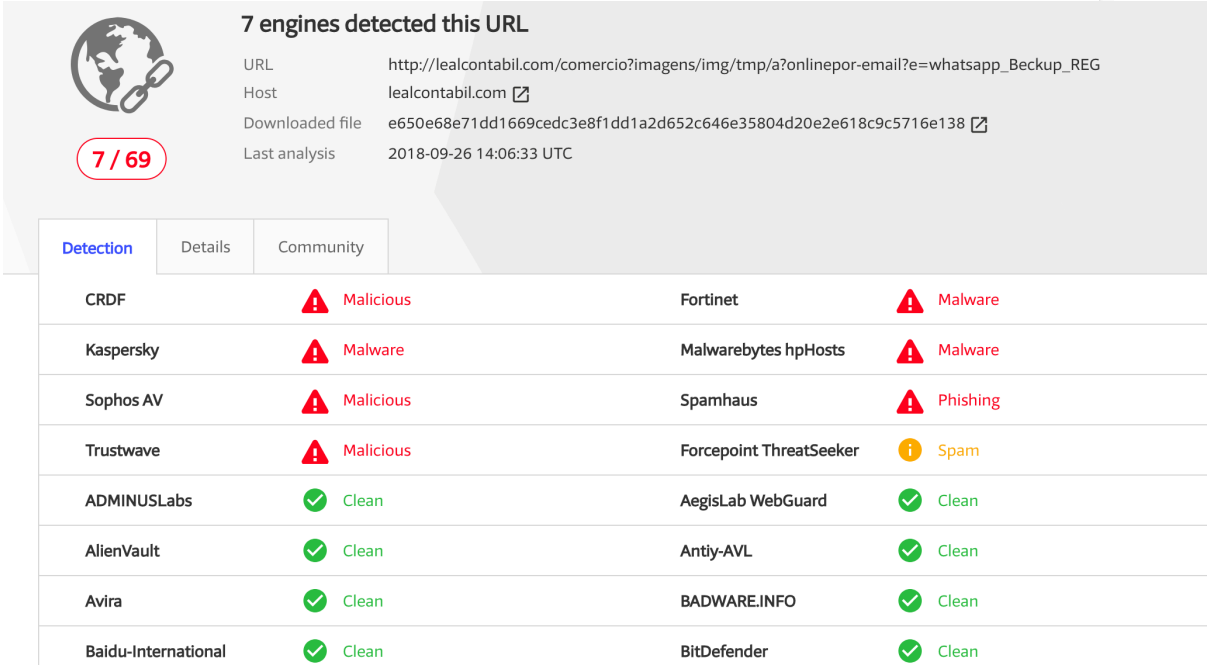
Affs. Imbecil !
acho que eu nunca ia ficar sabendo dessa safadeza ?
pois você se engano! Já sei de tudo !!

me mandar foto da sua conversa com os outros ao meu respeito!

toma ai registro da sua conversa

Whatsapp_Beckup_REG(656386387).zip

E fica já Sabendo que isto nunca que vai ficar por isto mesmo, ok?
Adeus



7 engines detected this URL

URL	http://lealcontabil.com/comercio?imagens/img/tmp/a?onlinepor-email?e=whatsapp_Beckup_REG
Host	lealcontabil.com
Downloaded file	e650e68e71dd1669cedc3e8f1dd1a2d652c646e35804d20e2e618c9c5716e138
Last analysis	2018-09-26 14:06:33 UTC

7 / 69

Detection | Details | Community

CRDF	Malicious	Fortinet	Malware
Kaspersky	Malware	Malwarebytes hpHosts	Malware
Sophos AV	Malicious	Spamhaus	Phishing
Trustwave	Malicious	Forcepoint ThreatSeeker	Spam
ADMINUSLabs	Clean	AegisLab WebGuard	Clean
AlienVault	Clean	Antiy-AVL	Clean
Avira	Clean	BADWARE.INFO	Clean
Baidu-International	Clean	BitDefender	Clean

HTTP Response

Final URL

http://lealcontabil.com/comercio?imagens/img/tmp/a?onlinepor-email?e=whatsapp_Beckup_REG

Serving IP Address

54.38.137.61

Status Code

200

Body Length

1.35 KB

Body SHA-256

e650e68e71dd1669cedc3e8f1dd1a2d652c646e35804d20e2e618c9c5716e138

Headers

```
accept-ranges: bytes
connection: Keep-Alive
content-length: 1382
content-type: text/html; charset=UTF-8
date: Wed, 26 Sep 2018 14:06:33 GMT
etag: "566-5270c49650000"
keep-alive: timeout=5, max=99
last-modified: Wed, 16 Dec 2015 23:30:08 GMT
server: Apache/2.4.6 (CentOS) PHP/5.4.16
```

☆ **Comunicado | Serasa Experian** 26 September 2018 at 9:49 PM

Anotacao de Extrato De Debitos para seu CPF/CNPJ. No (778071)

To: thiago.almeida@a1-associados.com

COMUNICADO IMPORTANTE Nº 20180354927618

São Paulo, quarta-feira 26 de setembro de 2018

Prezado(a) Senhor(a),

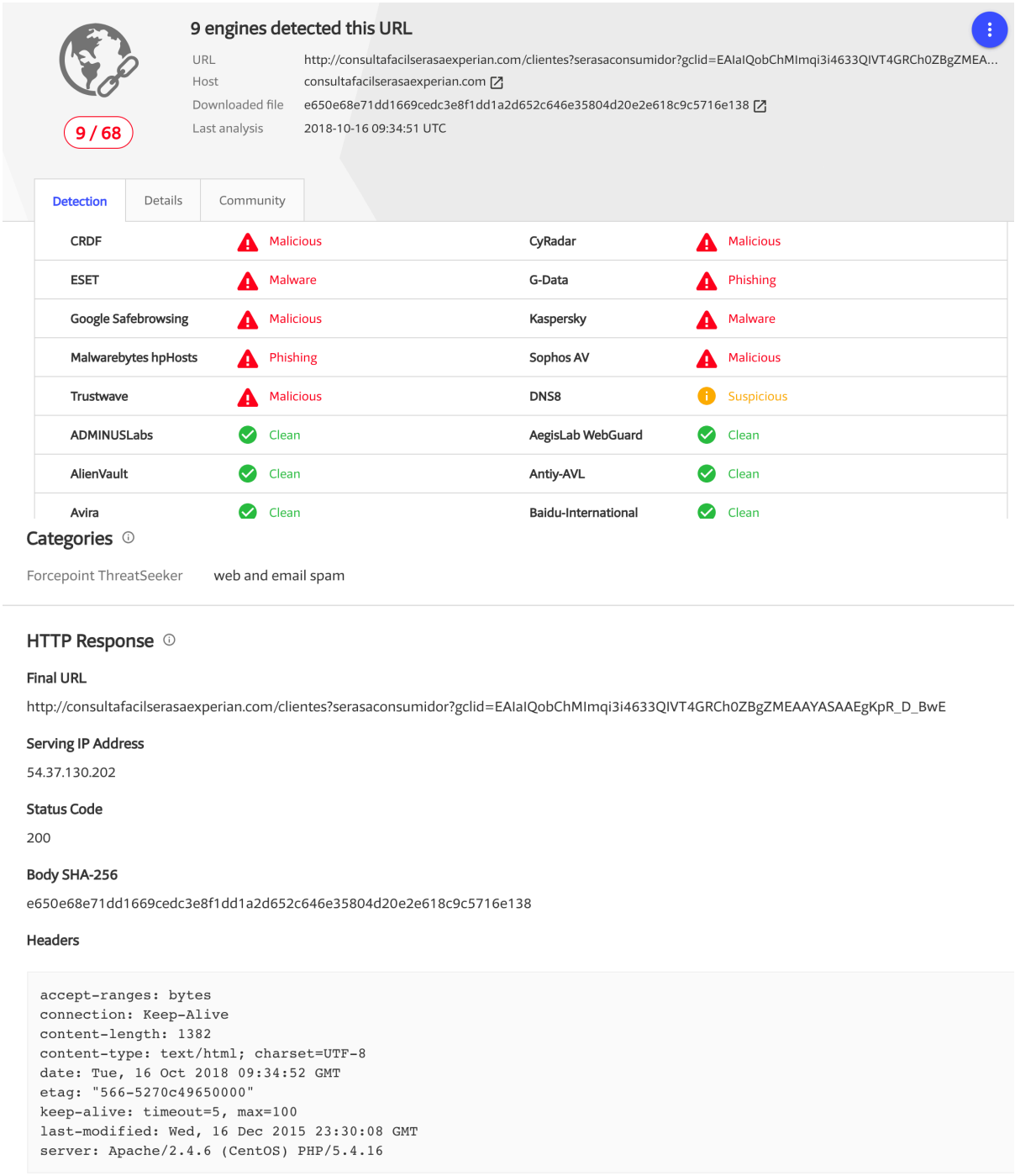
Para a preservação da qualidade e da segurança dos serviços prestado a comunidade e cumprimento do disposto no art.43, parágrafo segundo, da lei nº 8.078 de 11 de setembro de 1990, informamos que recebemos da instituição credora, pedido de inclusão em nossos registros da(s) anotação(ões) abaixo denominada(s),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



Reviewing both emails in email client shows there are no attachments, but both have links. In the first email, the link is to:

- http://lealcontabil.com/comercio?imagens/img/tmp/a?onlinepor-email?e=whatsapp_Beckup_REG

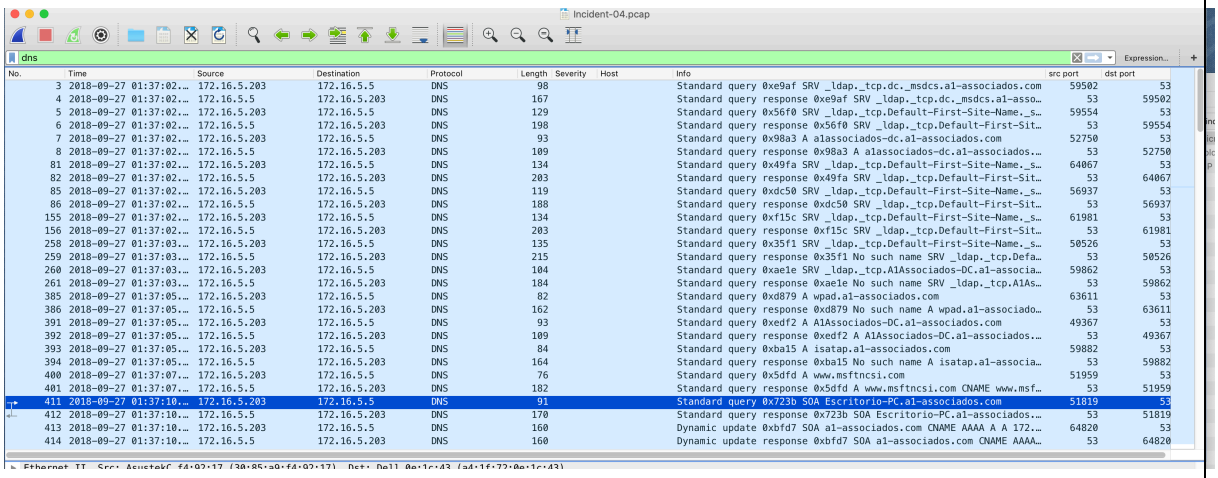
In the second email, the link is to:

- http://consultafacilserasaexperian.com/clientes?serasaconsumidor?gclid=EAIaIQobChMImqi3i4633QIVT4GRCh0ZBgZMEAAYASAAEgKpR_D_BwE

Step 03

Analysis via Wireshark Tool.

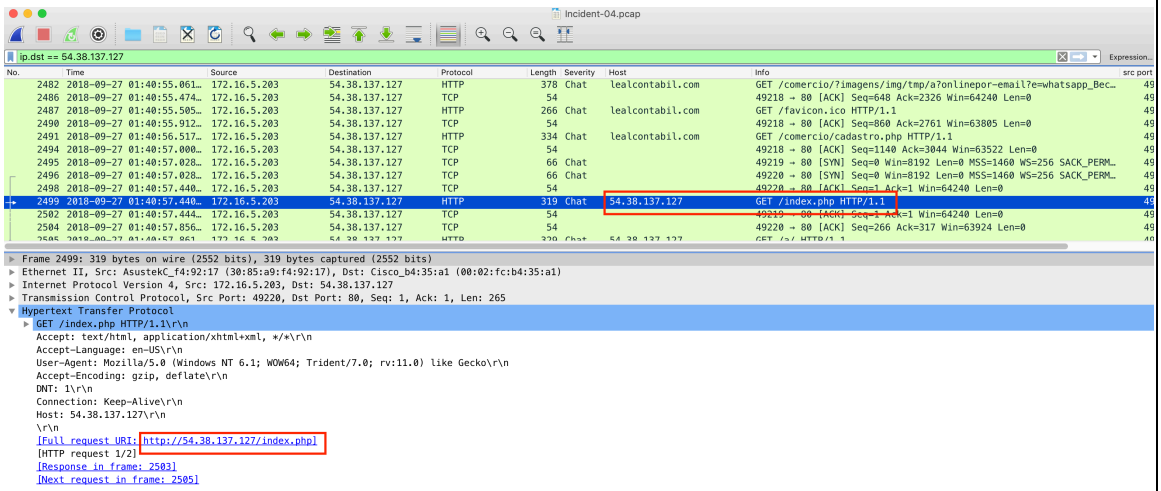
1. Let's find the traffic related to email by filtering DNS traffic, we can easily find the traffic related to associated domain.

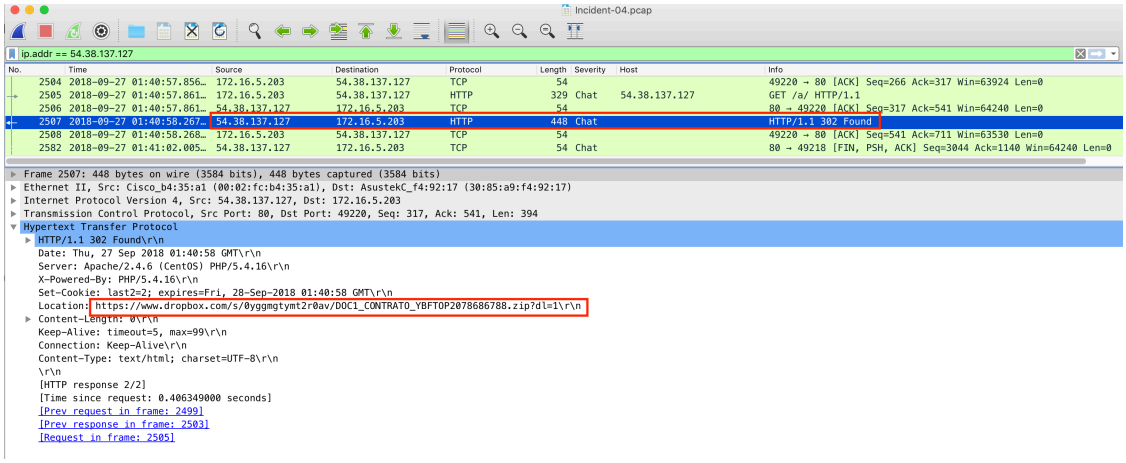


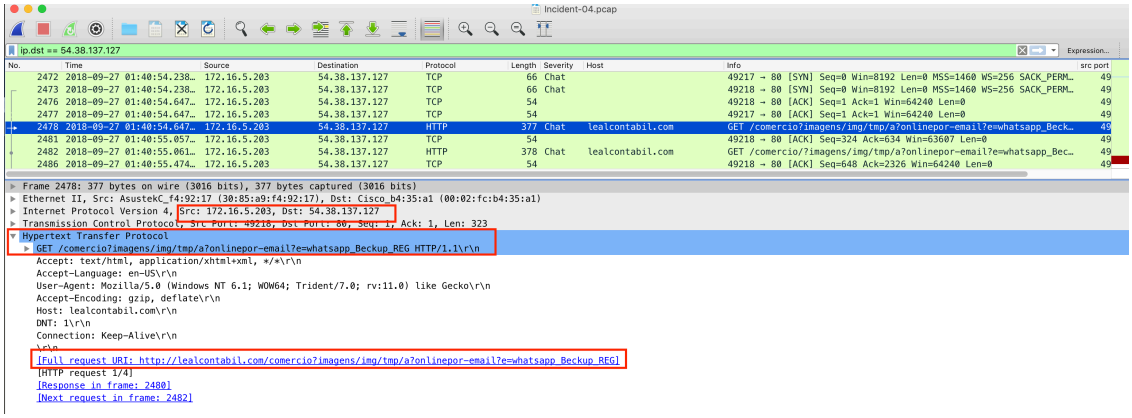
We can find several DNS queries for names ending in ***a1-associados.com***. such as ***A1Associados-DC.a1-associados.com*** and ***wpad.a1-associados.com,*** ***Escritorio-PC.a1-associados.com***. The domain ***a1-associados.com*** is used in the internal network.

2. By Analysing via Wireshark, filter traffic by ip address (54.38.137.127)

The ***lealcontabil.com*** URL led to *http://54.38.137.127/index.php*, which redirected to a Dropbox URL at ***https://www.dropbox.com/s/0yggmgtymt2r0av/DOC1_CONTRATO_YBFTOP2078686788.zip?dl=1***

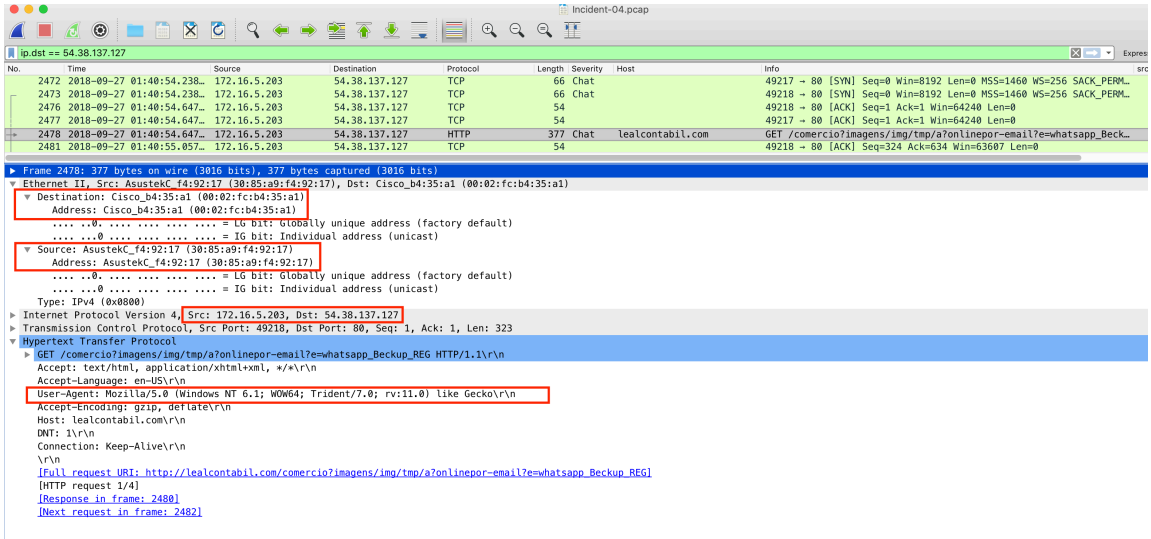


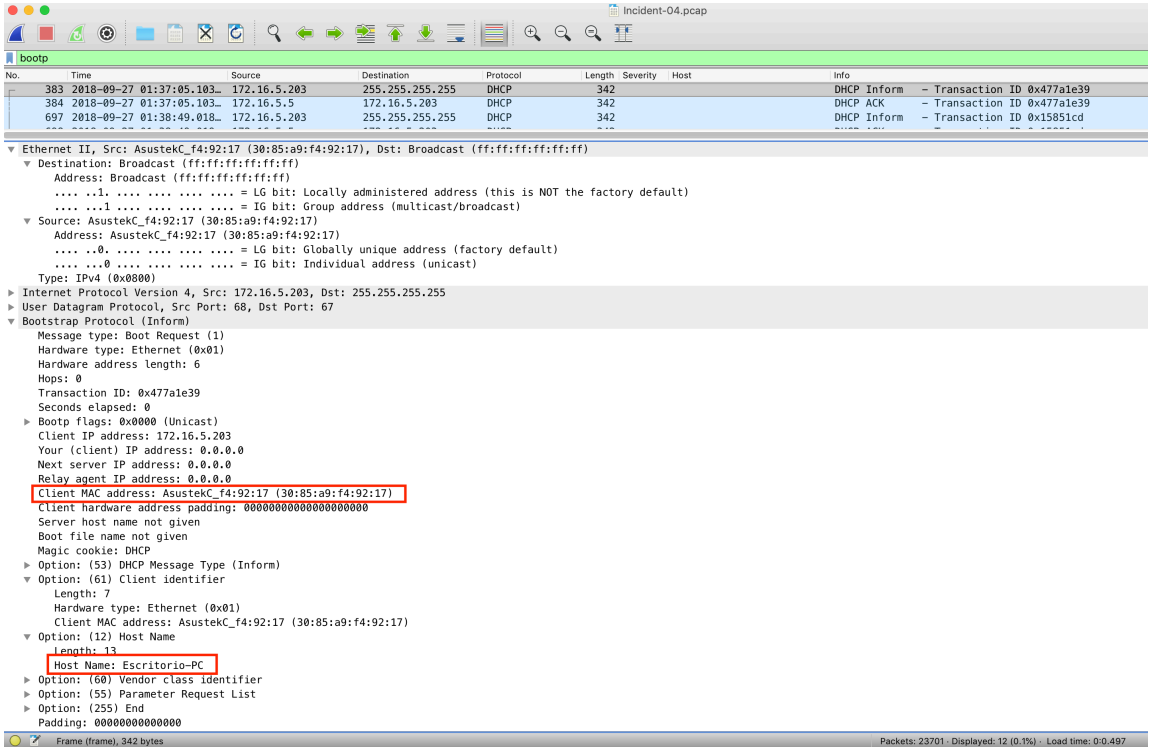


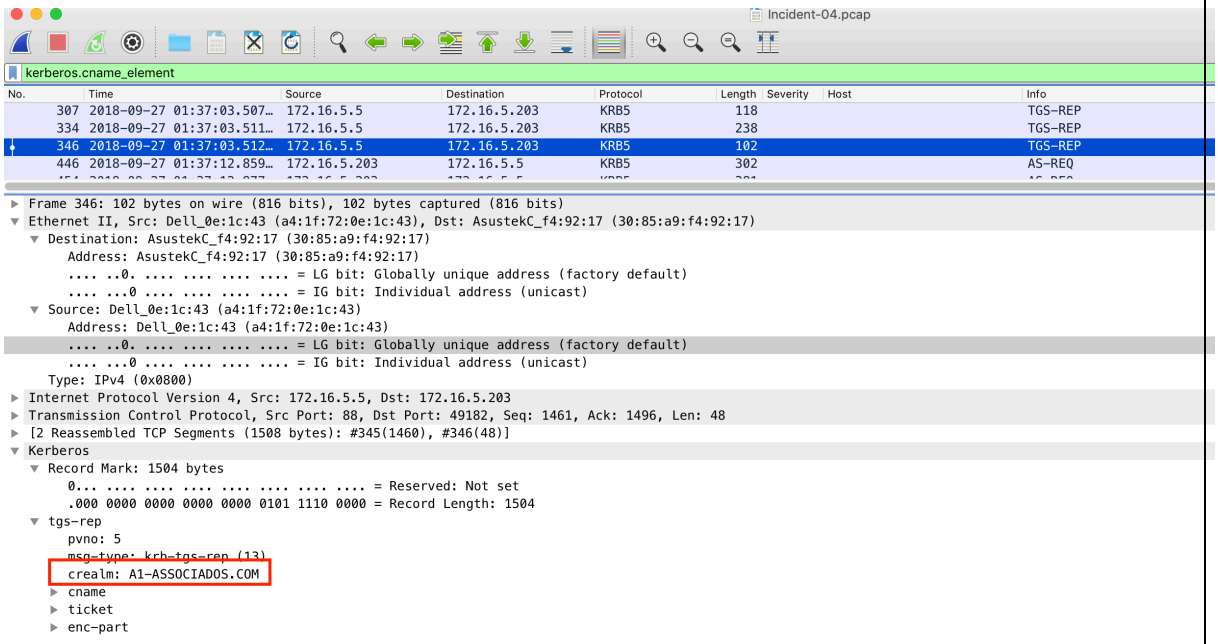


According to the analysis, only one email link has clicked and lead to infect users host machine.

3. Other relevant information found from packet analysis.




Incident-04.pcap
bootp
No. Time Source Destination Protocol Length Severity Host Info
383 2018-09-27 01:37:05.103… 172.16.5.203 255.255.255.255 DHCP 342 DHCP Inform - Transaction ID 0x477a1e39
384 2018-09-27 01:37:05.103… 172.16.5.5 172.16.5.203 DHCP 342 DHCP ACK - Transaction ID 0x477a1e39
697 2018-09-27 01:38:49.018… 172.16.5.203 255.255.255.255 DHCP 342 DHCP Inform - Transaction ID 0x15851cd
Ethernet II, Src: AsustekC_f4:92:17 (30:85:a9:f4:92:17), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Address: Broadcast (ff:ff:ff:ff:ff:ff)
.... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)
....1 .... = IG bit: Group address (multicast/broadcast)
Source: AsustekC_f4:92:17 (30:85:a9:f4:92:17)
Address: AsustekC_f4:92:17 (30:85:a9:f4:92:17)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.16.5.203, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Bootstrap Protocol (Inform)
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x477a1e39
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 172.16.5.203
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: AsustekC_f4:92:17 (30:85:a9:f4:92:17)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (Inform)
Option: (61) Client identifier
Length: 7
Hardware type: Ethernet (0x01)
Client MAC address: AsustekC_f4:92:17 (30:85:a9:f4:92:17)
Option: (12) Host Name
Length: 13
Host Name: Escritorio-PC
Option: (60) Vendor class identifier
Option: (55) Parameter Request List
Option: (255) End
Padding: 00000000000000
Frame (frame), 342 bytes
Packets: 23701 · Displayed: 12 (0.1%) · Load time: 0:0.497


Incident-04.pcap
kerberos.cname_element
No. Time Source Destination Protocol Length Severity Host Info
307 2018-09-27 01:37:03.507… 172.16.5.5 172.16.5.203 KRB5 118 TGS-REP
334 2018-09-27 01:37:03.511… 172.16.5.5 172.16.5.203 KRB5 238 TGS-REP
346 2018-09-27 01:37:03.512… 172.16.5.5 172.16.5.203 KRB5 102 TGS-REP
446 2018-09-27 01:37:12.859… 172.16.5.203 172.16.5.5 KRB5 302 AS-REQ
Frame 346: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
Ethernet II, Src: Dell_0e:1c:43 (a4:1f:72:0e:1c:43), Dst: AsustekC_f4:92:17 (30:85:a9:f4:92:17)
Destination: AsustekC_f4:92:17 (30:85:a9:f4:92:17)
Address: AsustekC_f4:92:17 (30:85:a9:f4:92:17)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: Dell_0e:1c:43 (a4:1f:72:0e:1c:43)
Address: Dell_0e:1c:43 (a4:1f:72:0e:1c:43)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.16.5.5, Dst: 172.16.5.203
Transmission Control Protocol, Src Port: 88, Dst Port: 49182, Seq: 1461, Ack: 1496, Len: 48
[2 Reassembled TCP Segments (1508 bytes): #345(1460), #346(48)]
Kerberos
Record Mark: 1504 bytes
0... .... = Reserved: Not set
.000 0000 0000 0000 0000 0101 1110 0000 = Record Length: 1504
tgs-rep
pvno: 5
msg-type: krb-tgs-rep (13)
crealm: A1-ASSOCIADOS.COM
cname
ticket
enc-part

Conclusion

In this incident, a host machine has been infected with a malware due to an user clicked on phishing url received by email, which led to malicious content website. From two received two emails, but user only clicked on one URL according to the analysis.

Following information have been identified from the incident.

1. Incident report (Description of the activity)
    a. What happen

        This host machine is infected by malware due to Phishing emails.

    b. How it happened

        host machine has been infected with a malware due to an user clicked on phishing url received by email, which led to malicious content website. From two received two emails, but user only clicked on one URL according to the analysis.

2. Date and time of the activity
    i. Date: 2018-09-27
    ii. Time: 01:40:54.647754 GMT
3. Network Details of Attackers and Victims

Information	Attacker	Victim
IP address	54.38.137.127	172.16.5.203
Host name		Escritorio-PC
MAC address	00:02:fc:b4:35:a1	AsustekC_f4:92:17 (30:85:a9:f4:92:17)
Ports	80	49217,49218
Domains	lealcontabil.com	a1-associados.com
User account name	NA	thiago.almeida
OS/Software Name and Version	Apache/2.4.6 (CentOS) PHP/5.4.16	Internet Explorer 11 on Windows 7, 64-bit (Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko)

4. Infected malware, exploit kit, exploit type, might be involved

    This is spam email which use to go to a malicious web page and download malware.

5. Gathered evidence files.

see above screenshots of analysis.

********** End – Incident-04 **********

Incident– 05

Problem

Scenario: Host network was infected by a malware. You also have two emails.

For the incident # 05, there is *.pcap* file is given for analyse which is related incident that port scan is happened to the network.

Approach

1. As best practice it is mandatory to validate hash value of the evidence that provided or collected.
2. Given *.pcap* file can be analysed via Wireshark and other relevant tools which is helps to see/identify the content of the packets where inbound and outbound to/from host machine which is related to port scan.
3. Identify all the network traffic related to port scans behaviour by tcp flags.
4. Identify port scan by snort rules.

Above approach is taken to do the network packet analyse and will be explained step by step below.

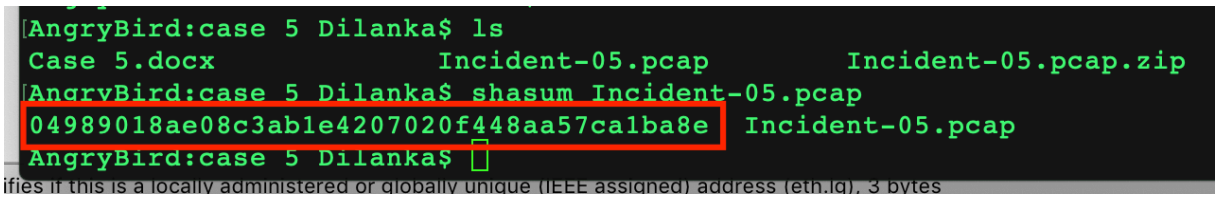
Given questions will be answered by end of the analyse with the conclusion.

Step 01

Hash value verification. When extracted given evidence zip file, noticed that file name is Incident-05.pcap

Incident 05

File URL: http://pgvle.ucsc.cmb.ac.lk/mod/resource/view.php?id=6661
Scenario: Host machine scan by an attacker
SHA1 Hash: 04989018ae08c3ab1e4207020f448aa57ca1ba8e

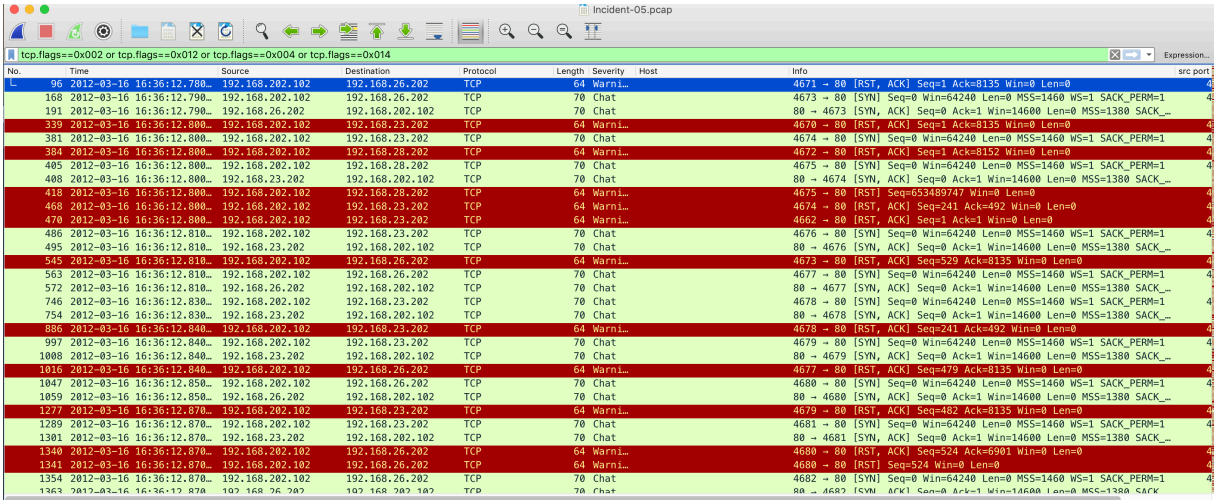


Step 02

Analyse using Wireshark application.

1. Find all related packets by tcp flags.

```
tcp.flags==0x002 or tcp.flags==0x012 or tcp.flags==0x004 or
tcp.flags==0x014
```

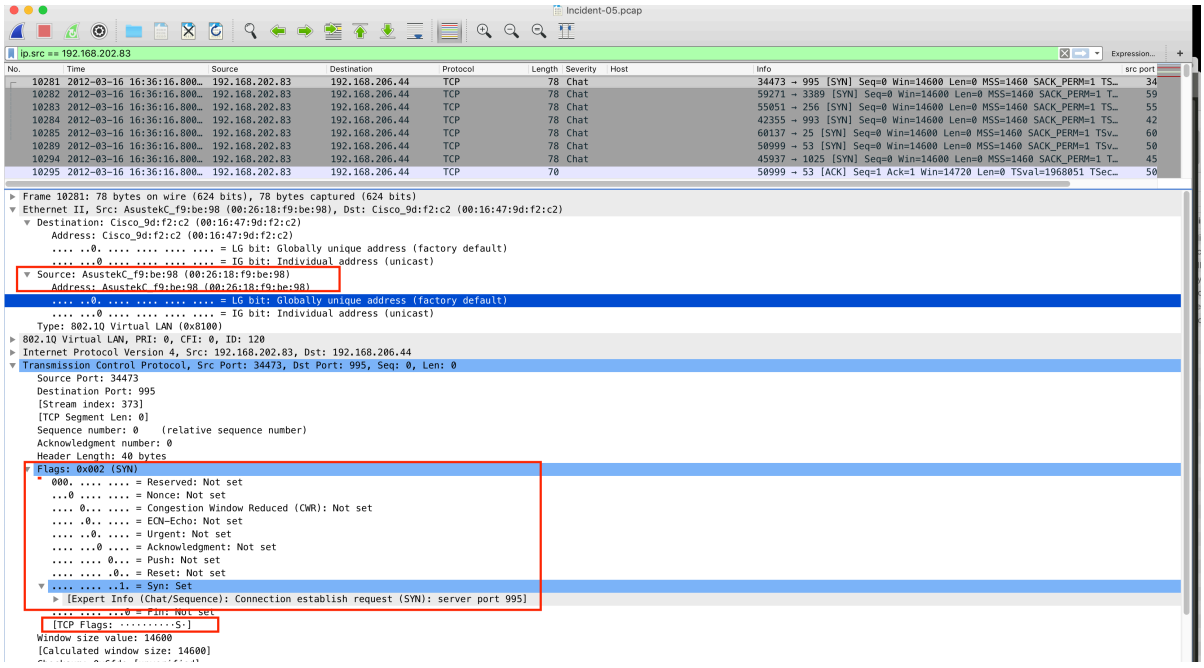


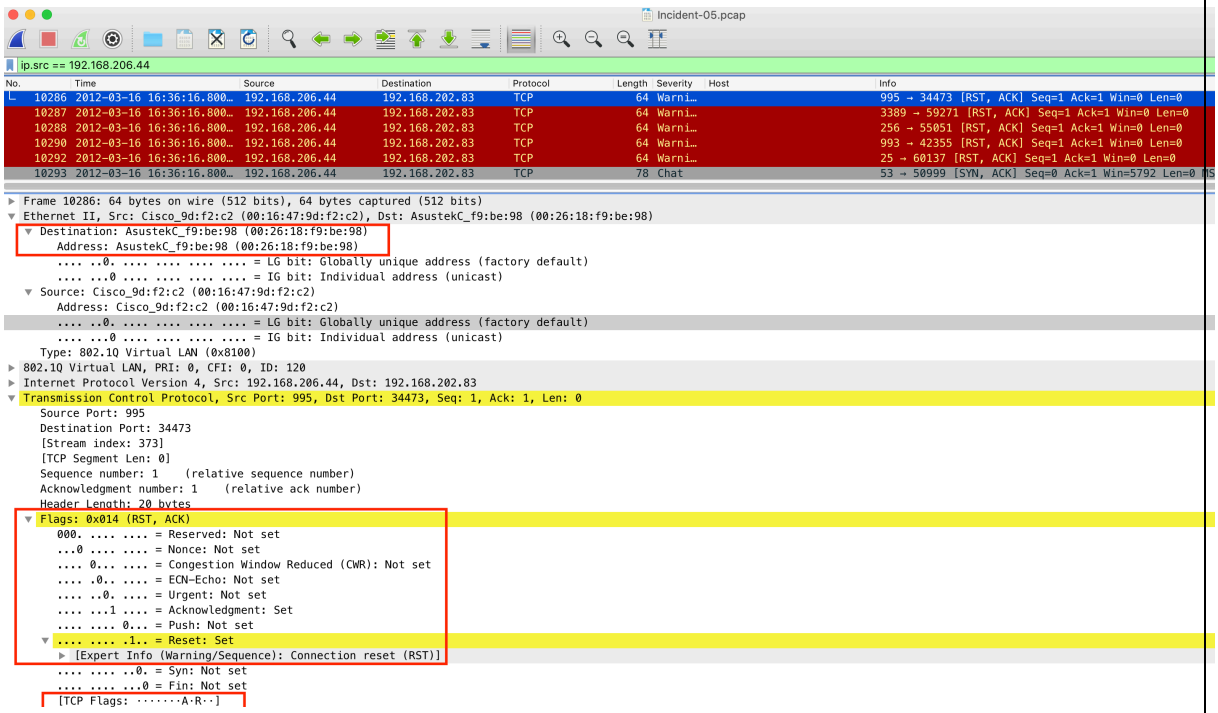
2. Add below snort rules and run snort for the given pcap file.

```
#Ping Sweep Scan
alert icmp any any -> any any (msg: "NMAP ping sweep Scan"; dsize:0;sid:10000004; rev: 1; )

#TCP Scan
alert tcp any any -> any any (msg: "NMAP TCP Scan";sid:10000005; rev:2; )

#XMAS scan
alert tcp any any ->  any any(msg:"Nmap XMAS Tree Scan"; flags:FPU; sid:1000006; rev:1; )

#FIN Scan
alert tcp any any -> any any (msg:"Nmap FIN Scan"; flags:F; sid:1000008; rev:1;)

# NULL Scan
alert tcp any any ->  any any(msg:"Nmap NULL Scan"; flags:0; sid:1000009; rev:1; )

# UDP Scan
alert udp any any -> any any ( msg:"Nmap UDP Scan"; sid:1000010; rev:1; )
```

```
Time: 03/16-22:06:16.800000
event_ref: 0
192.168.202.83 -> 192.168.206.44 (portscan) TCP Portscan
Priority Count: 6
Connection Count: 9
IP Count: 1
Scanner IP Range: 192.168.202.83:192.168.202.83
Port/Proto Count: 10
Port/Proto Range: 25:8080

Time: 03/16-22:06:19.870000
event_ref: 0
192.168.28.100 -> 192.168.202.110 (portscan) TCP Portsweep
Priority Count: 5
Connection Count: 6
IP Count: 3
Scanned IP Range: 192.168.202.110:192.168.202.112
Port/Proto Count: 1
Port/Proto Range: 1025:1025
```

3. Observe information via Wireshark.




Incident-05.pcap
ip.src == 192.168.206.44
No. Time Source Destination Protocol Length Severity Host Info
10286 2012-03-16 16:36:16.800… 192.168.206.44 192.168.202.83 TCP 64 Warni… 995 → 34473 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10287 2012-03-16 16:36:16.800… 192.168.206.44 192.168.202.83 TCP 64 Warni… 3389 → 59271 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10288 2012-03-16 16:36:16.800… 192.168.206.44 192.168.202.83 TCP 64 Warni… 256 → 55051 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10290 2012-03-16 16:36:16.800… 192.168.206.44 192.168.202.83 TCP 64 Warni… 993 → 42355 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10292 2012-03-16 16:36:16.800… 192.168.206.44 192.168.202.83 TCP 64 Warni… 25 → 60137 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10293 2012-03-16 16:36:16.800… 192.168.206.44 192.168.202.83 TCP 78 Chat 53 → 50999 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MS
Frame 10286: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)
Ethernet II, Src: Cisco_9d:f2:c2 (00:16:47:9d:f2:c2), Dst: AsustekC_f9:be:98 (00:26:18:f9:be:98)
Destination: AsustekC_f9:be:98 (00:26:18:f9:be:98)
Address: AsustekC_f9:be:98 (00:26:18:f9:be:98)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: Cisco_9d:f2:c2 (00:16:47:9d:f2:c2)
Address: Cisco_9d:f2:c2 (00:16:47:9d:f2:c2)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 120
Internet Protocol Version 4, Src: 192.168.206.44, Dst: 192.168.202.83
Transmission Control Protocol, Src Port: 995, Dst Port: 34473, Seq: 1, Ack: 1, Len: 0
Source Port: 995
Destination Port: 34473
[Stream index: 373]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
Acknowledgment number: 1 (relative ack number)
Header Length: 20 bytes
Flags: 0x014 (RST, ACK)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
.... 0... = Push: Not set
.... .1.. = Reset: Set
[Expert Info (Warning/Sequence): Connection reset (RST)]
....0. = Syn: Not set
....0 = Fin: Not set
[TCP Flags: ·····A·R··]

Conclusion

In this incident, a host machine has been port scanned by attacker

Following information have been identified from the incident.

1. Incident report (Description of the activity)
    a. What happen

        Network has scanned by attacker. (Port scan)

    b. How it happened

        Attacker used TCP port scan method to scan
2. Date and time of the activity
    i. Date: 2012-03-16
    ii. Time: 16:36:16.770000 GMT
3. Network Details of Attackers and Victims

Information	Attacker	Victim
IP address	192.168.202.83	192.168.206.44
Host name	NA	NA
MAC address	00:26:18:f9:be:98	00:16:47:9d:f2:c2
Ports	34473, 59271 etc	995, 3386, 256,993 etc..
Domains	NA	NA
User account name	NA	NA
OS/Software Name and Version	NA	NA

4. Infected malware, exploit kit, exploit type, might be involved

    Port scan only via TCP scan
5. Gathered evidence files.

    see above screenshots of analysis.

********** End – Incident-05 **********