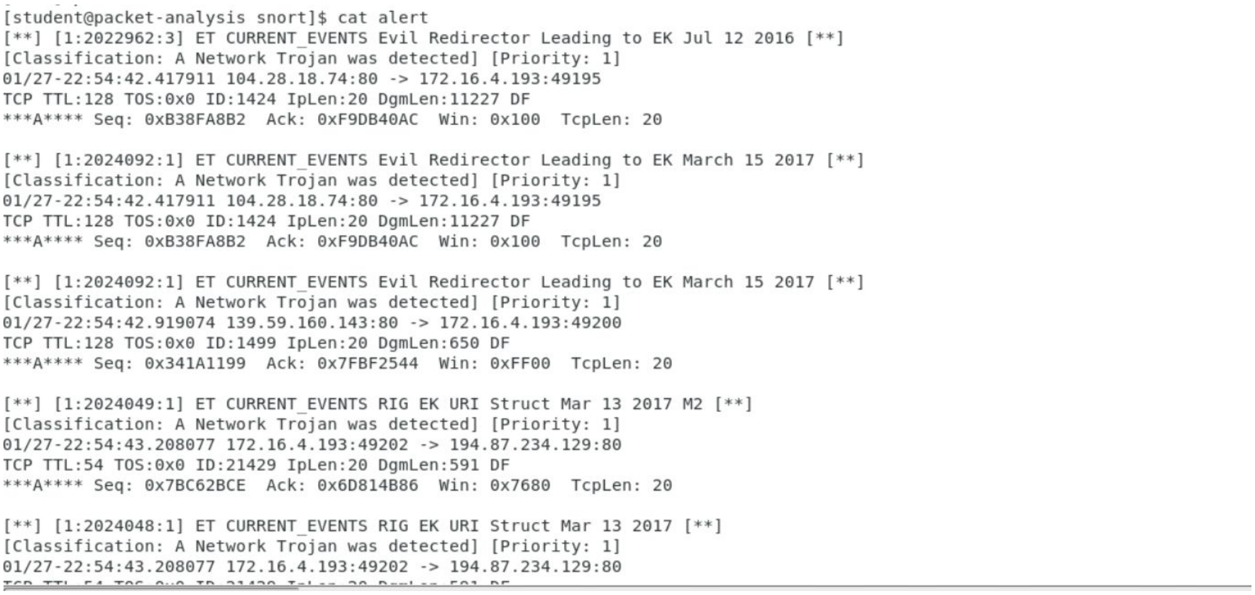
Packet Analysis Homework

Contents

Snort

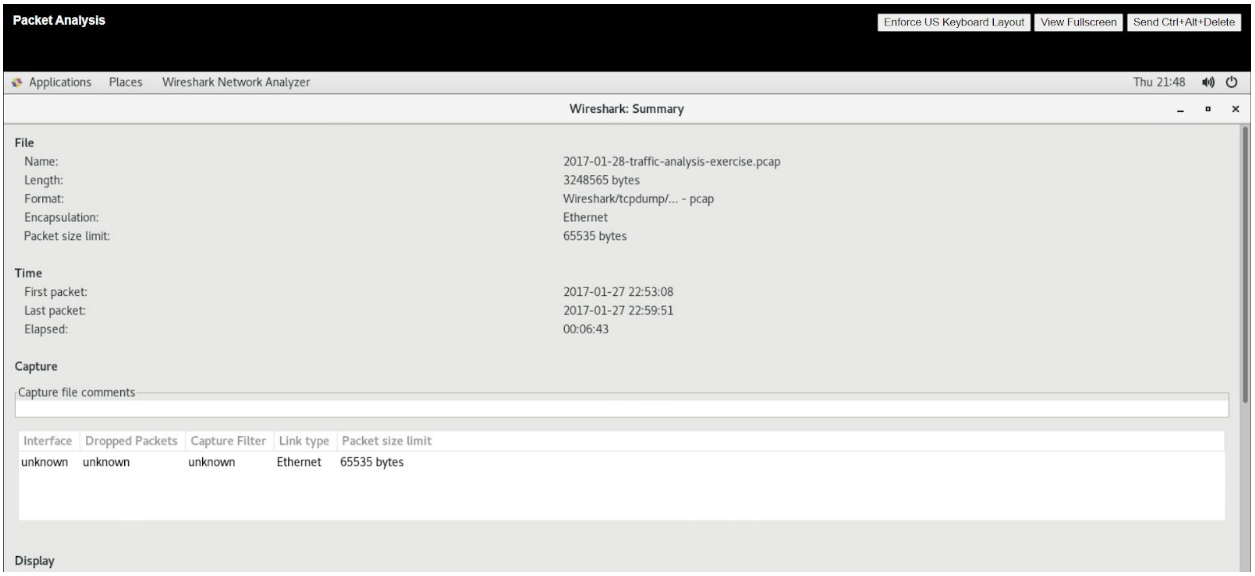
Results- alert file



```
[student@packet-analysis snort]$ cat alert
[**] [1:2022962:3] ET CURRENT_EVENTS Evil Redirector Leading to EK Jul 12 2016 [**]
[Classification: A Network Trojan was detected] [Priority: 1]
01/27-22:54:42.417911 104.28.18.74:80 -> 172.16.4.193:49195
TCP TTL:128 TOS:0x0 ID:1424 IpLen:20 DgmLen:11227 DF
***A**** Seq: 0xB38FA8B2  Ack: 0xF9DB40AC  Win: 0x100  TcpLen: 20

[**] [1:2024092:1] ET CURRENT_EVENTS Evil Redirector Leading to EK March 15 2017 [**]
[Classification: A Network Trojan was detected] [Priority: 1]
01/27-22:54:42.417911 104.28.18.74:80 -> 172.16.4.193:49195
TCP TTL:128 TOS:0x0 ID:1424 IpLen:20 DgmLen:11227 DF
***A**** Seq: 0xB38FA8B2  Ack: 0xF9DB40AC  Win: 0x100  TcpLen: 20

[**] [1:2024092:1] ET CURRENT_EVENTS Evil Redirector Leading to EK March 15 2017 [**]
[Classification: A Network Trojan was detected] [Priority: 1]
01/27-22:54:42.919074 139.59.160.143:80 -> 172.16.4.193:49200
TCP TTL:128 TOS:0x0 ID:1499 IpLen:20 DgmLen:650 DF
***A**** Seq: 0x341A1199  Ack: 0x7FBF2544  Win: 0xFF00  TcpLen: 20

[**] [1:2024049:1] ET CURRENT_EVENTS RIG EK URI Struct Mar 13 2017 M2 [**]
[Classification: A Network Trojan was detected] [Priority: 1]
01/27-22:54:43.208077 172.16.4.193:49202 -> 194.87.234.129:80
TCP TTL:54 TOS:0x0 ID:21429 IpLen:20 DgmLen:591 DF
***A**** Seq: 0x7BC62BCE  Ack: 0x6D814B86  Win: 0x7680  TcpLen: 20

[**] [1:2024048:1] ET CURRENT_EVENTS RIG EK URI Struct Mar 13 2017 [**]
[Classification: A Network Trojan was detected] [Priority: 1]
01/27-22:54:43.208077 172.16.4.193:49202 -> 194.87.234.129:80
```

Wireshark

Wireshark: Summary



Wireshark: Summary

File

Name:	2017-01-28-traffic-analysis-exercise.pcap
Length:	3248565 bytes
Format:	Wireshark/tcpdump/... - pcap
Encapsulation:	Ethernet
Packet size limit:	65535 bytes

Time

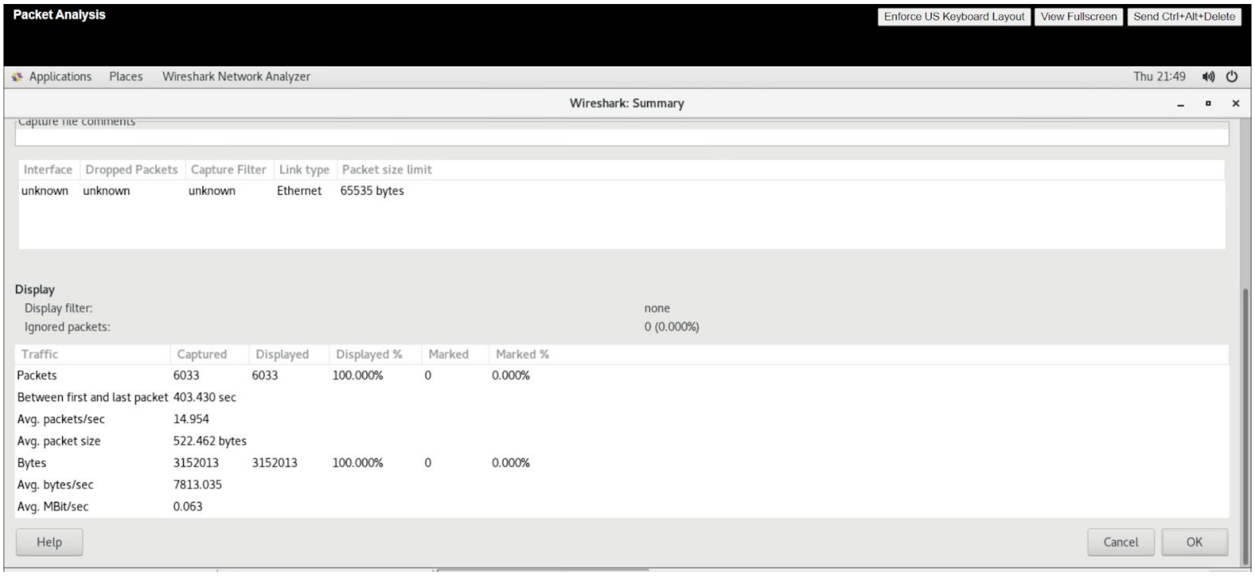
First packet:	2017-01-27 22:53:08
Last packet:	2017-01-27 22:59:51
Elapsed:	00:06:43

Capture

Capture file comments

Interface	Dropped Packets	Capture Filter	Link type	Packet size limit
unknown	unknown	unknown	Ethernet	65535 bytes

Display



Wireshark: Summary

Capture file comments

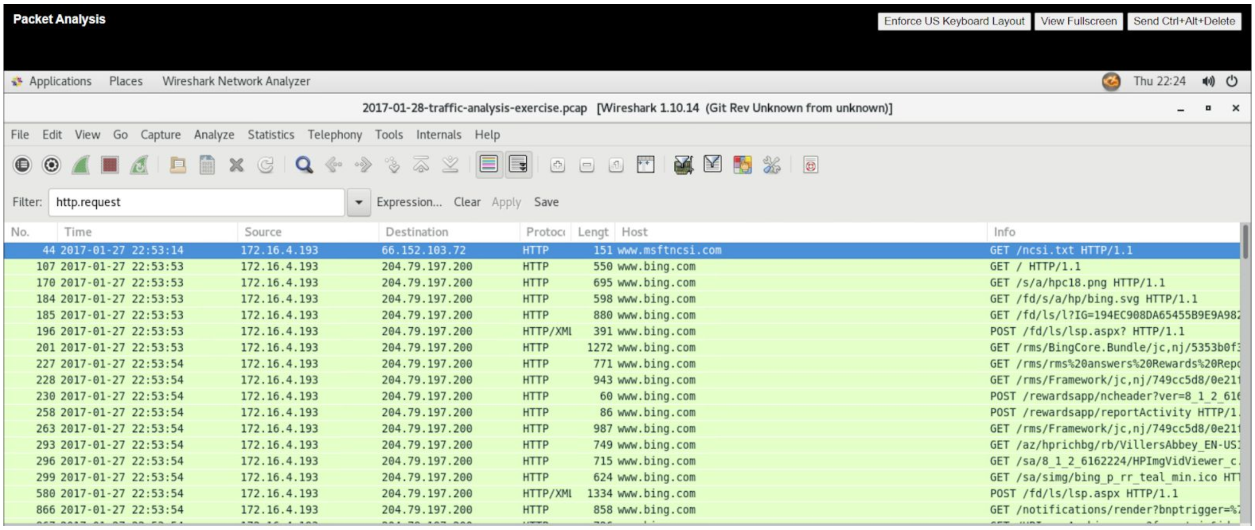
Interface	Dropped Packets	Capture Filter	Link type	Packet size limit
unknown	unknown	unknown	Ethernet	65535 bytes

Display

Display filter:	none
Ignored packets:	0 (0.000%)

Traffic	Captured	Displayed	Displayed %	Marked	Marked %
Packets	6033	6033	100.000%	0	0.000%
Between first and last packet	403.430 sec				
Avg. packets/sec	14.954				
Avg. packet size	522.462 bytes				
Bytes	3152013	3152013	100.000%	0	0.000%
Avg. bytes/sec	7813.035				
Avg. MBit/sec	0.063				

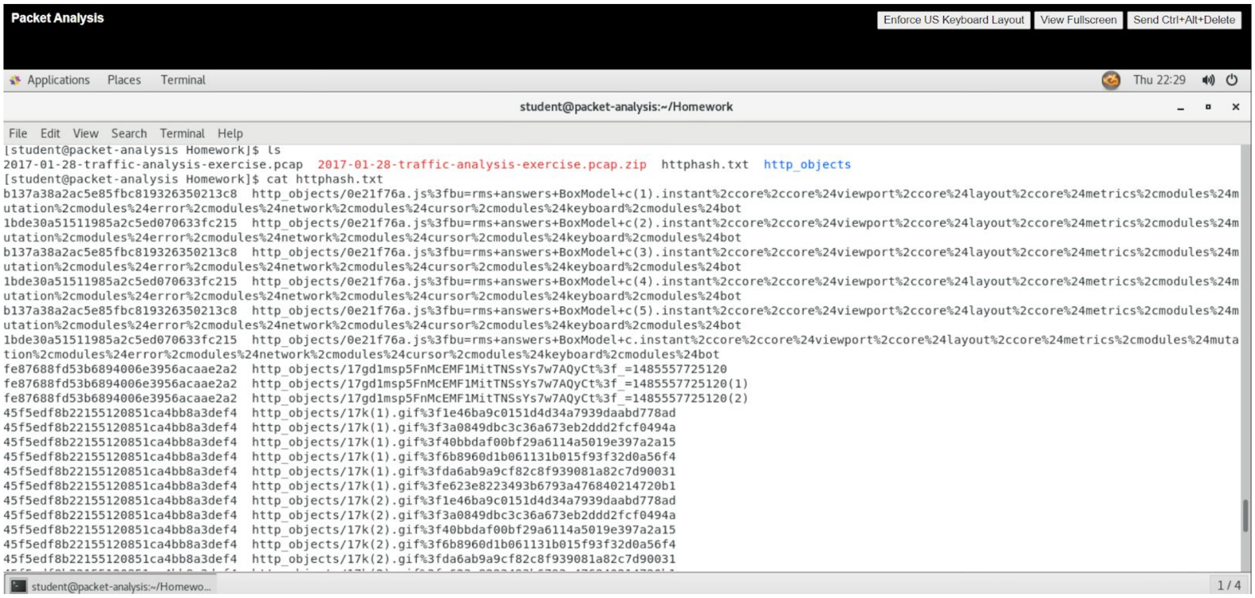
Summary panel



Filter: http.request

```
No.  Time                 Source        Destination     Protoco  Lengt Host                                    Info
  44 2017-01-27 22:53:14  172.16.4.193  66.152.103.72   HTTP       151 www.msftncsi.com                        GET /ncsi.txt HTTP/1.1
 107 2017-01-27 22:53:53  172.16.4.193  204.79.197.200  HTTP       550 www.bing.com                            GET / HTTP/1.1
 170 2017-01-27 22:53:53  172.16.4.193  204.79.197.200  HTTP       695 www.bing.com                            GET /s/a/hpc18.png HTTP/1.1
 184 2017-01-27 22:53:53  172.16.4.193  204.79.197.200  HTTP       598 www.bing.com                            GET /fd/s/a/hp/bing.svg HTTP/1.1
 185 2017-01-27 22:53:53  172.16.4.193  204.79.197.200  HTTP       880 www.bing.com                            GET /fd/ls/l?IG=194EC908DA65455B9E9A982
 196 2017-01-27 22:53:53  172.16.4.193  204.79.197.200  HTTP/XMl   391 www.bing.com                            POST /fd/ls/lsp.aspx? HTTP/1.1
 201 2017-01-27 22:53:53  172.16.4.193  204.79.197.200  HTTP      1272 www.bing.com                            GET /rms/BingCore.Bundle/jc,nj/5353b0f3
 227 2017-01-27 22:53:54  172.16.4.193  204.79.197.200  HTTP       771 www.bing.com                            GET /rms/rms%20answers%20Rewards%20Repo
 228 2017-01-27 22:53:54  172.16.4.193  204.79.197.200  HTTP       943 www.bing.com                            GET /rms/Framework/jc,nj/749cc5d8/0e21
 230 2017-01-27 22:53:54  172.16.4.193  204.79.197.200  HTTP        60 www.bing.com                            POST /rewardsapp/ncheader?ver=8_1_2_616
 258 2017-01-27 22:53:54  172.16.4.193  204.79.197.200  HTTP        86 www.bing.com                            POST /rewardsapp/reportActivity HTTP/1.
 263 2017-01-27 22:53:54  172.16.4.193  204.79.197.200  HTTP       987 www.bing.com                            GET /rms/Framework/jc,nj/749cc5d8/0e21
 293 2017-01-27 22:53:54  172.16.4.193  204.79.197.200  HTTP       749 www.bing.com                            GET /az/hprichbg/rb/VillersAbbey_EN-US
 296 2017-01-27 22:53:54  172.16.4.193  204.79.197.200  HTTP       715 www.bing.com                            GET /sa/8_1_2_6162224/HPImgVidViewer_c.
 299 2017-01-27 22:53:54  172.16.4.193  204.79.197.200  HTTP       624 www.bing.com                            GET /sa/simg/bing_p_rr_teal_min.ico HT
 580 2017-01-27 22:53:54  172.16.4.193  204.79.197.200  HTTP/XMl  1334 www.bing.com                            POST /fd/ls/lsp.aspx HTTP/1.1
 866 2017-01-27 22:53:54  172.16.4.193  204.79.197.200  HTTP       858 www.bing.com                            GET /notifications/render?bnptrigger=%
```

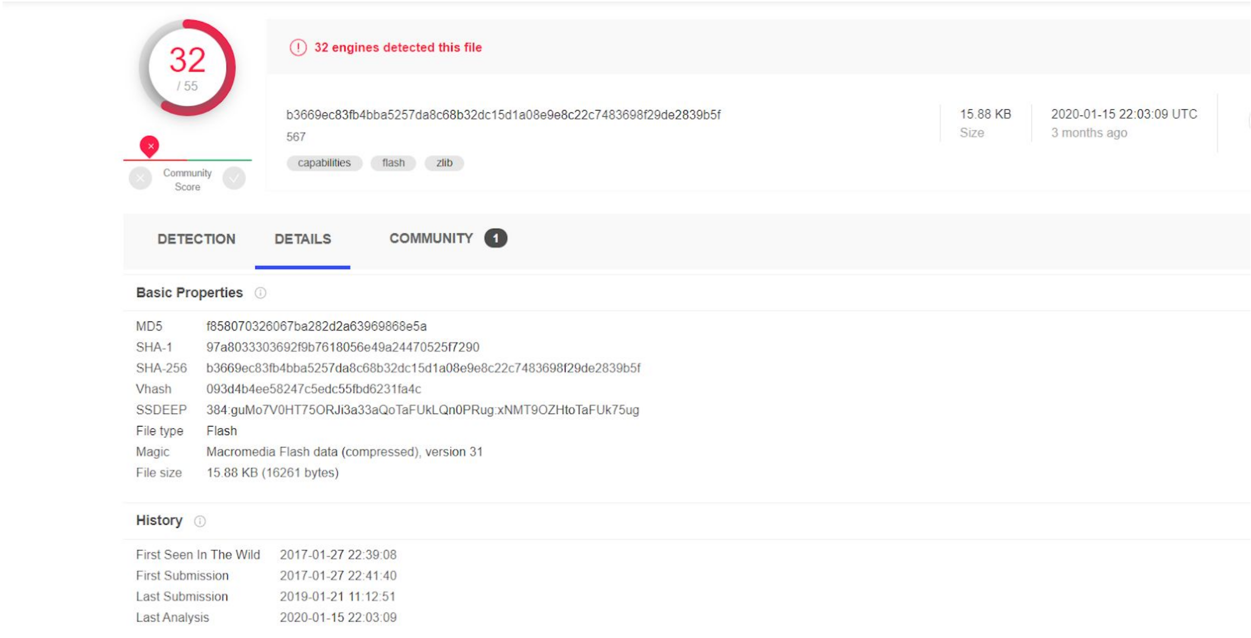
The contents of the httphash.txt



```
[student@packet-analysis Homework]$ ls
2017-01-28-traffic-analysis-exercise.pcap  2017-01-28-traffic-analysis-exercise.pcap.zip  httphash.txt  http_objects
[student@packet-analysis Homework]$ cat httphash.txt
b137a38a2ac5e85fbc819326350213c8  http_objects/0e21f76a.js%3fbu=rms+answers+BoxModel+c(1).instant%2ccore%2ccore%24viewport%2ccore%24layout%2ccore%24metrics%2cmodules%24m
utation%2cmodules%24error%2cmodules%24network%2cmodules%24cursor%2cmodules%24keyboard%2cmodules%24bot
1bde30a51511985a2c5ed070633fc215  http_objects/0e21f76a.js%3fbu=rms+answers+BoxModel+c(2).instant%2ccore%2ccore%24viewport%2ccore%24layout%2ccore%24metrics%2cmodules%24m
utation%2cmodules%24error%2cmodules%24network%2cmodules%24cursor%2cmodules%24keyboard%2cmodules%24bot
b137a38a2ac5e85fbc819326350213c8  http_objects/0e21f76a.js%3fbu=rms+answers+BoxModel+c(3).instant%2ccore%2ccore%24viewport%2ccore%24layout%2ccore%24metrics%2cmodules%24m
utation%2cmodules%24error%2cmodules%24network%2cmodules%24cursor%2cmodules%24keyboard%2cmodules%24bot
1bde30a51511985a2c5ed070633fc215  http_objects/0e21f76a.js%3fbu=rms+answers+BoxModel+c(4).instant%2ccore%2ccore%24viewport%2ccore%24layout%2ccore%24metrics%2cmodules%24m
utation%2cmodules%24error%2cmodules%24network%2cmodules%24cursor%2cmodules%24keyboard%2cmodules%24bot
b137a38a2ac5e85fbc819326350213c8  http_objects/0e21f76a.js%3fbu=rms+answers+BoxModel+c(5).instant%2ccore%2ccore%24viewport%2ccore%24layout%2ccore%24metrics%2cmodules%24m
utation%2cmodules%24error%2cmodules%24network%2cmodules%24cursor%2cmodules%24keyboard%2cmodules%24bot
1bde30a51511985a2c5ed070633fc215  http_objects/0e21f76a.js%3fbu=rms+answers+BoxModel+c.instant%2ccore%2ccore%24viewport%2ccore%24layout%2ccore%24metrics%2cmodules%24muta
tion%2cmodules%24error%2cmodules%24network%2cmodules%24cursor%2cmodules%24keyboard%2cmodules%24bot
fe87688fd53b6894006e3956acaae2a2  http_objects/17gd1msp5FnMcEMF1MitTNSsYs7w7AQyCt%3f_=1485557725120
fe87688fd53b6894006e3956acaae2a2  http_objects/17gd1msp5FnMcEMF1MitTNSsYs7w7AQyCt%3f_=1485557725120(1)
fe87688fd53b6894006e3956acaae2a2  http_objects/17gd1msp5FnMcEMF1MitTNSsYs7w7AQyCt%3f_=1485557725120(2)
45f5edf8b22155120851ca4bb8a3def4  http_objects/17k(1).gif%3f1e46ba9c0151d4d34a7939daabd778ad
45f5edf8b22155120851ca4bb8a3def4  http_objects/17k(1).gif%3f3a0849dbc3c36a673eb2ddd2fcf0494a
45f5edf8b22155120851ca4bb8a3def4  http_objects/17k(1).gif%3f40bbdaf00bf29a6114a5019e397a2a15
45f5edf8b22155120851ca4bb8a3def4  http_objects/17k(1).gif%3f6b8960d1b061131b015f93f32d0a56f4
45f5edf8b22155120851ca4bb8a3def4  http_objects/17k(1).gif%3fda6ab9a9cf82c8f939081a82c7d90031
45f5edf8b22155120851ca4bb8a3def4  http_objects/17k(1).gif%3fe623e8223493b6793a476840214720b1
45f5edf8b22155120851ca4bb8a3def4  http_objects/17k(2).gif%3f1e46ba9c0151d4d34a7939daabd778ad
45f5edf8b22155120851ca4bb8a3def4  http_objects/17k(2).gif%3f3a0849dbc3c36a673eb2ddd2fcf0494a
45f5edf8b22155120851ca4bb8a3def4  http_objects/17k(2).gif%3f40bbdaf00bf29a6114a5019e397a2a15
45f5edf8b22155120851ca4bb8a3def4  http_objects/17k(2).gif%3f6b8960d1b061131b015f93f32d0a56f4
45f5edf8b22155120851ca4bb8a3def4  http_objects/17k(2).gif%3fda6ab9a9cf82c8f939081a82c7d90031
```

VirusTotal

Hash Value No. - 5



32 engines detected this file

b3669ec83fb4bba5257da8c68b32dc15d1a08e9e8c22c7483698f29de2839b5f
567

15.88 KB
Size

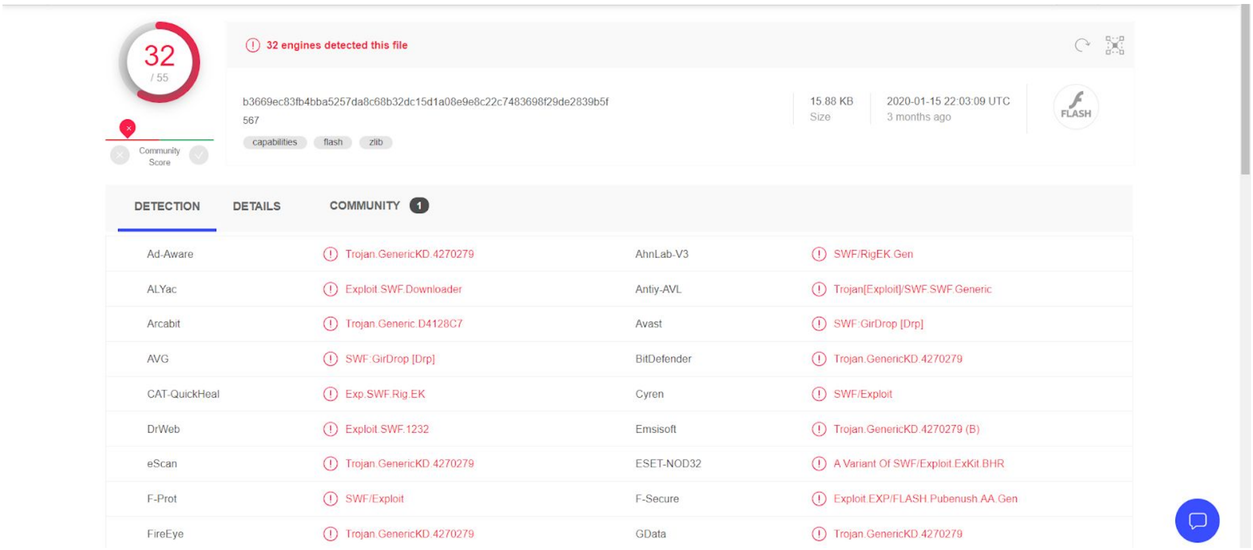
2020-01-15 22:03:09 UTC
3 months ago

Basic Properties

MD5	f858070326067ba282d2a63969868e5a
SHA-1	97a8033303692f9b7618056e49a24470525f7290
SHA-256	b3669ec83fb4bba5257da8c68b32dc15d1a08e9e8c22c7483698f29de2839b5f
Vhash	093d4b4ee58247c5edc55fbd6231fa4c
SSDEEP	384:guMo7V0HT75ORJi3a33aQoTaFUkLQn0PRug:xNMT9OZHtoTaFUk75ug
File type	Flash
Magic	Macromedia Flash data (compressed), version 31
File size	15.88 KB (16261 bytes)

History

First Seen In The Wild	2017-01-27 22:39:08
First Submission	2017-01-27 22:41:40
Last Submission	2019-01-21 11:12:51
Last Analysis	2020-01-15 22:03:09



32 engines detected this file

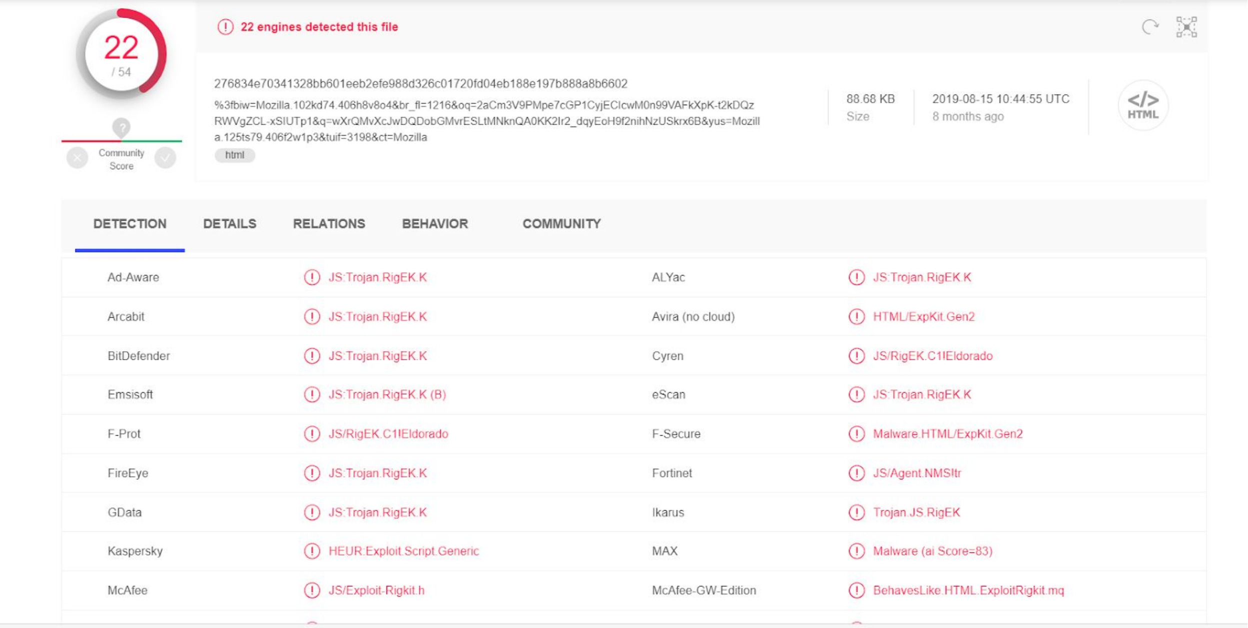
b3669ec83fb4bba5257da8c68b32dc15d1a08e9e8c22c7483698f29de2839b5f
567

15.88 KB
Size

2020-01-15 22:03:09 UTC
3 months ago

Ad-Aware	Trojan.GenericKD.4270279	AhnLab-V3	SWF/RigEK.Gen
ALYac	Exploit.SWF.Downloader	Antiy-AVL	Trojan[Exploit]/SWF.SWF.Generic
Arcabit	Trojan.Generic.D4128C7	Avast	SWF:GirDrop [Drp]
AVG	SWF:GirDrop [Drp]	BitDefender	Trojan.GenericKD.4270279
CAT-QuickHeal	Exp.SWF.Rig.EK	Cyren	SWF/Exploit
DrWeb	Exploit.SWF.1232	Emsisoft	Trojan.GenericKD.4270279 (B)
eScan	Trojan.GenericKD.4270279	ESET-NOD32	A Variant Of SWF/Exploit.ExKit.BHR
F-Prot	SWF/Exploit	F-Secure	Exploit.EXP/FLASH.Pubenush.AA.Gen
FireEye	Trojan.GenericKD.4270279	GData	Trojan.GenericKD.4270279

Hash Value No.- 16



22 / 54

Community Score

22 engines detected this file

276834e70341328bb601eeb2efe988d326c01720fd04eb188e197b888a8b6602

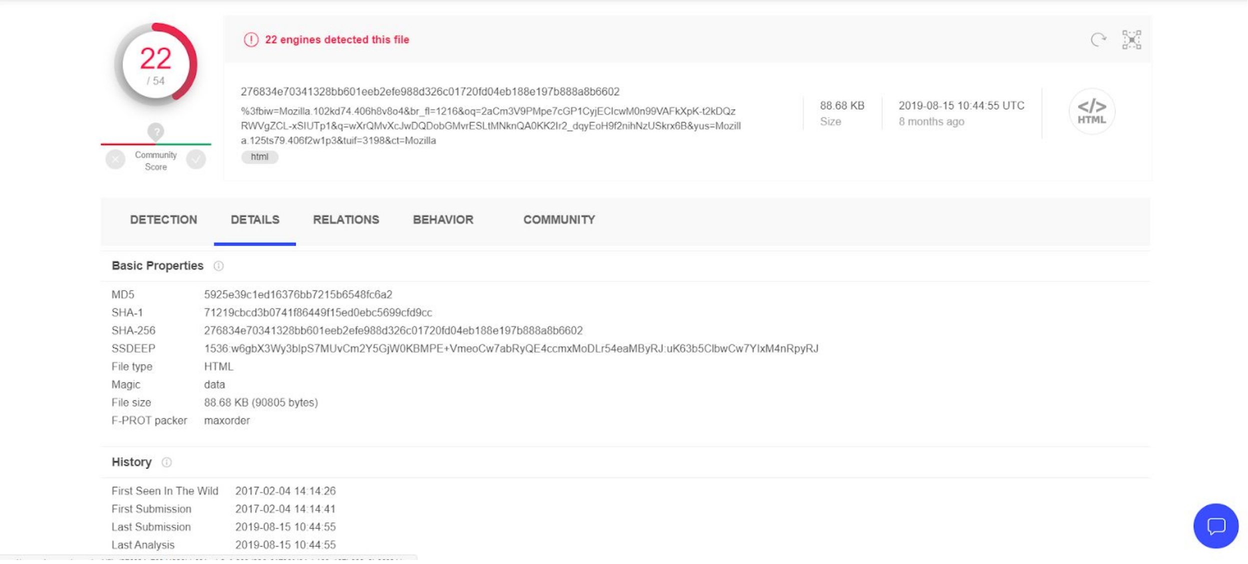
%3fbiw=Mozilla.102kd74.406h8v8o4&br_fl=1216&oq=2aCm3V9PMpe7cGP1CyjEClcwM0n99VAFkXpK-t2kDQz RWVgZCL-xSIUTp1&q=wXrQMvXcJwDQDobGMvrESLtMNknQA0KK2Ir2_dqyEoH9f2nihNzUSkrx6B&yus=Mozill a.125ts79.406f2w1p3&tuif=3198&ct=Mozilla

html

88.68 KB
Size

2019-08-15 10:44:55 UTC
8 months ago

Ad-Aware	ⓘ JS:Trojan.RigEK.K	ALYac	ⓘ JS:Trojan.RigEK.K
Arcabit	ⓘ JS:Trojan.RigEK.K	Avira (no cloud)	ⓘ HTML/ExpKit.Gen2
BitDefender	ⓘ JS:Trojan.RigEK.K	Cyren	ⓘ JS/RigEK.C1!Eldorado
Emsisoft	ⓘ JS:Trojan.RigEK.K (B)	eScan	ⓘ JS:Trojan.RigEK.K
F-Prot	ⓘ JS/RigEK.C1!Eldorado	F-Secure	ⓘ Malware.HTML/ExpKit.Gen2
FireEye	ⓘ JS:Trojan.RigEK.K	Fortinet	ⓘ JS/Agent.NMS!tr
GData	ⓘ JS:Trojan.RigEK.K	Ikarus	ⓘ Trojan.JS.RigEK
Kaspersky	ⓘ HEUR:Exploit.Script.Generic	MAX	ⓘ Malware (ai Score=83)
McAfee	ⓘ JS/Exploit-Rigkit.h	McAfee-GW-Edition	ⓘ BehavesLike.HTML.ExploitRigkit.mq



22 / 54

Community Score

22 engines detected this file

276834e70341328bb601eeb2efe988d326c01720fd04eb188e197b888a8b6602

%3fbiw=Mozilla.102kd74.406h8v8o4&br_fl=1216&oq=2aCm3V9PMpe7cGP1CyjEClcwM0n99VAFkXpK-t2kDQz RWVgZCL-xSIUTp1&q=wXrQMvXcJwDQDobGMvrESLtMNknQA0KK2Ir2_dqyEoH9f2nihNzUSkrx6B&yus=Mozill a.125ts79.406f2w1p3&tuif=3198&ct=Mozilla

html

88.68 KB
Size

2019-08-15 10:44:55 UTC
8 months ago

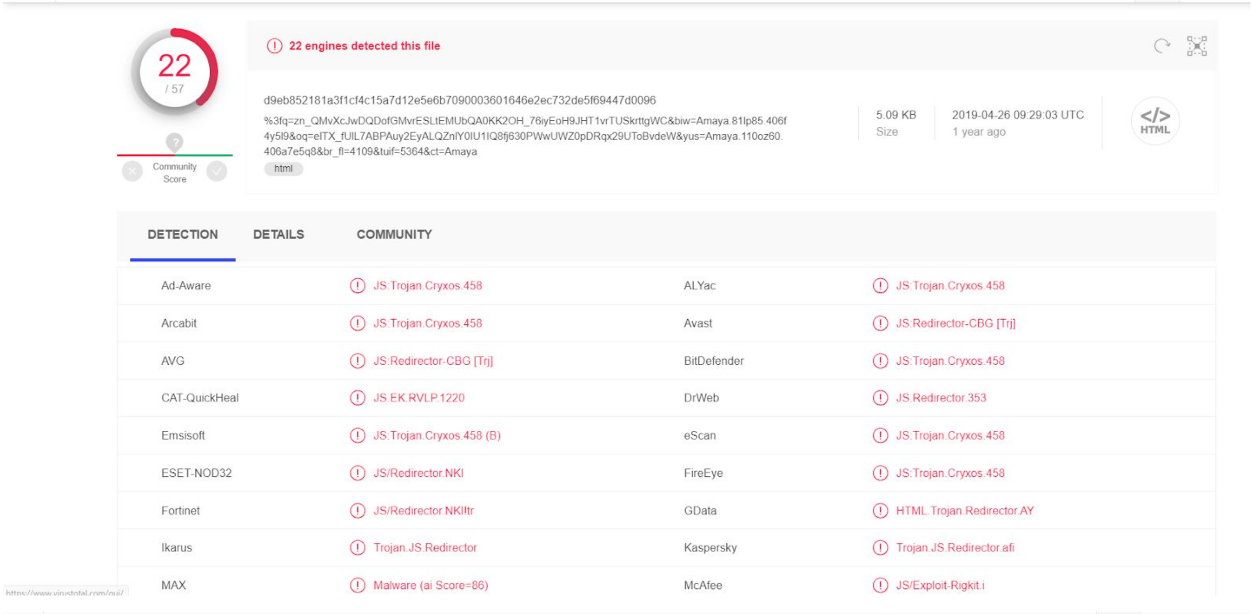
Basic Properties

MD5	5925e39c1ed16376bb7215b6548fc6a2
SHA-1	71219cbcd3b0741f86449f15ed0ebc5699cfd9cc
SHA-256	276834e70341328bb601eeb2efe988d326c01720fd04eb188e197b888a8b6602
SSDEEP	1536:w6gbX3Wy3blpS7MUvCm2Y5GjW0KBMPE+VmeoCw7abRyQE4ccmxMoDLr54eaMByRJ:uK63b5ClbwCw7YlxM4nRpyRJ
File type	HTML
Magic	data
File size	88.68 KB (90805 bytes)
F-PROT packer	maxorder

History

First Seen In The Wild	2017-02-04 14:14:26
First Submission	2017-02-04 14:14:41
Last Submission	2019-08-15 10:44:55
Last Analysis	2019-08-15 10:44:55

Hash Value No.- 19



22
/ 57

Community Score

22 engines detected this file

d9eb852181a3f1cf4c15a7d12e5e6b7090003601646e2ec732de5f69447d0096
%3fq=zn_QMvXcJwDQDofGMvrESLtEMUbQA0KK2OH_76iyEoH9JHT1vrTUSkrttgWC&biw=Amaya.81lp85.406f
4y5I9&oq=eITX_fUIL7ABPAuy2EyALQZnIY0IU1IQ8fj630PWwUWZ0pDRqx29UToBvdeW&yus=Amaya.110oz60.
406a7e5q8&br_fl=4109&tuif=5364&ct=Amaya
html

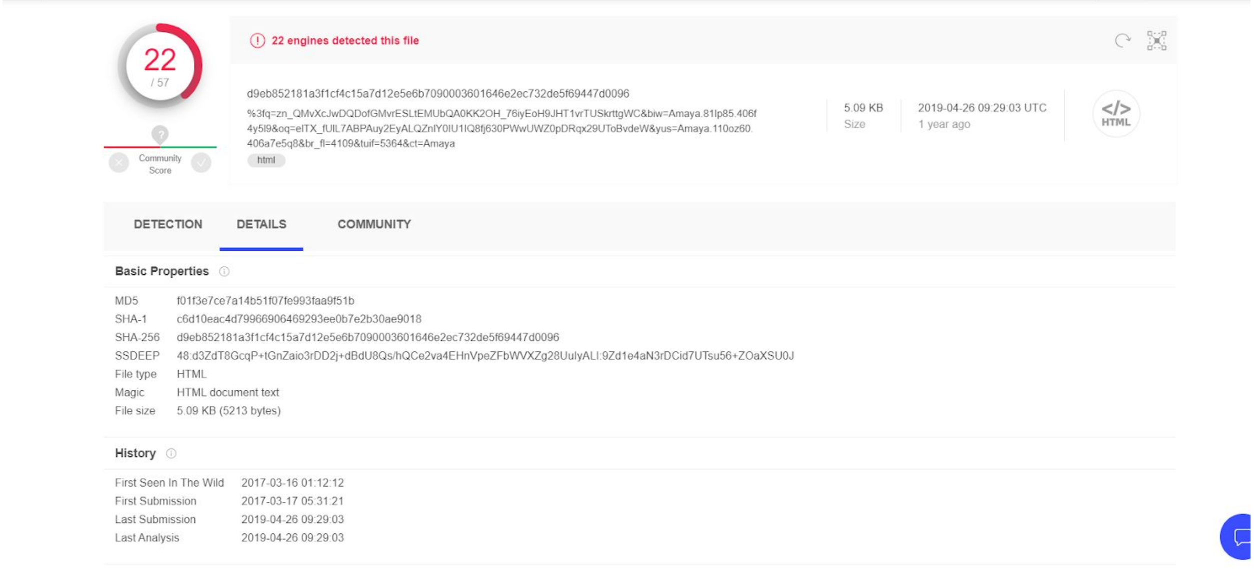
5.09 KB
Size

2019-04-26 09:29:03 UTC
1 year ago

DETECTION DETAILS COMMUNITY

Ad-Aware	JS:Trojan.Cryxos.458	ALYac	JS:Trojan.Cryxos.458
Arcabit	JS:Trojan.Cryxos.458	Avast	JS:Redirector-CBG [Trj]
AVG	JS:Redirector-CBG [Trj]	BitDefender	JS:Trojan.Cryxos.458
CAT-QuickHeal	JS.EK.RVLP.1220	DrWeb	JS.Redirector.353
Emsisoft	JS:Trojan.Cryxos.458 (B)	eScan	JS:Trojan.Cryxos.458
ESET-NOD32	JS/Redirector.NKI	FireEye	JS:Trojan.Cryxos.458
Fortinet	JS/Redirector.NKI!tr	GData	HTML.Trojan.Redirector.AY
Ikarus	Trojan.JS.Redirector	Kaspersky	Trojan.JS.Redirector.afi
MAX	Malware (ai Score=86)	McAfee	JS/Exploit-Rigkit.i

https://www.virustotal.com/gui/



22
/ 57

Community Score

22 engines detected this file

d9eb852181a3f1cf4c15a7d12e5e6b7090003601646e2ec732de5f69447d0096
%3fq=zn_QMvXcJwDQDofGMvrESLtEMUbQA0KK2OH_76iyEoH9JHT1vrTUSkrttgWC&biw=Amaya.81lp85.406f
4y5I9&oq=eITX_fUIL7ABPAuy2EyALQZnIY0IU1IQ8fj630PWwUWZ0pDRqx29UToBvdeW&yus=Amaya.110oz60.
406a7e5q8&br_fl=4109&tuif=5364&ct=Amaya
html

5.09 KB
Size

2019-04-26 09:29:03 UTC
1 year ago

DETECTION DETAILS COMMUNITY

Basic Properties

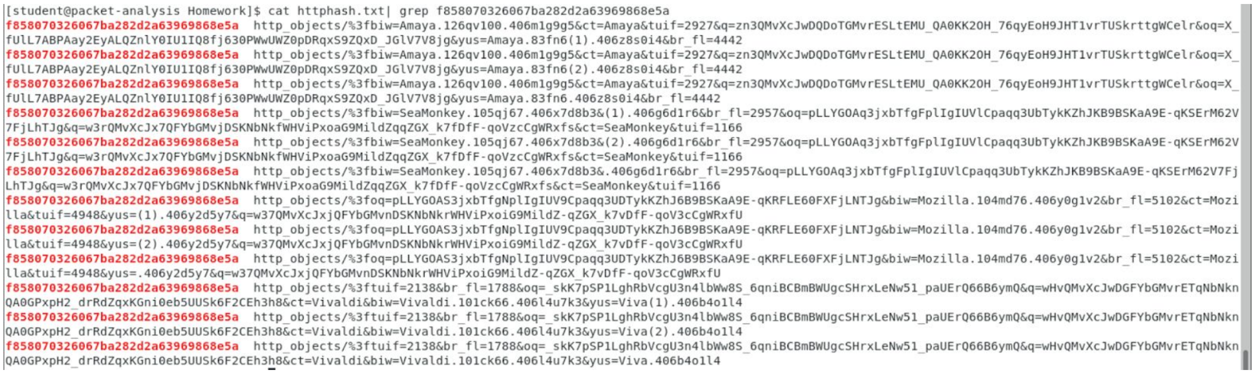
MD5	f01f3e7ce7a14b51f07fe993faa9f51b
SHA-1	c6d10eac4d79966906469293ee0b7e2b30ae9018
SHA-256	d9eb852181a3f1cf4c15a7d12e5e6b7090003601646e2ec732de5f69447d0096
SSDEEP	48:d3ZdT8GcqP+tGnZaio3rDD2j+dBdU8Qs/hQCe2va4EHnVpeZFbWVXZg28UulyALI:9Zd1e4aN3rDCid7UTsu56+ZOaXSU0J
File type	HTML
Magic	HTML document text
File size	5.09 KB (5213 bytes)

History

First Seen In The Wild	2017-03-16 01:12:12
First Submission	2017-03-17 05:31:21
Last Submission	2019-04-26 09:29:03
Last Analysis	2019-04-26 09:29:03

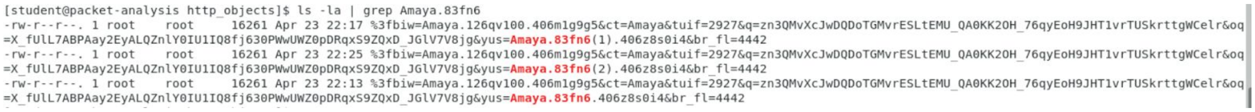
Extra Credit

Infected Hash No. 5 files



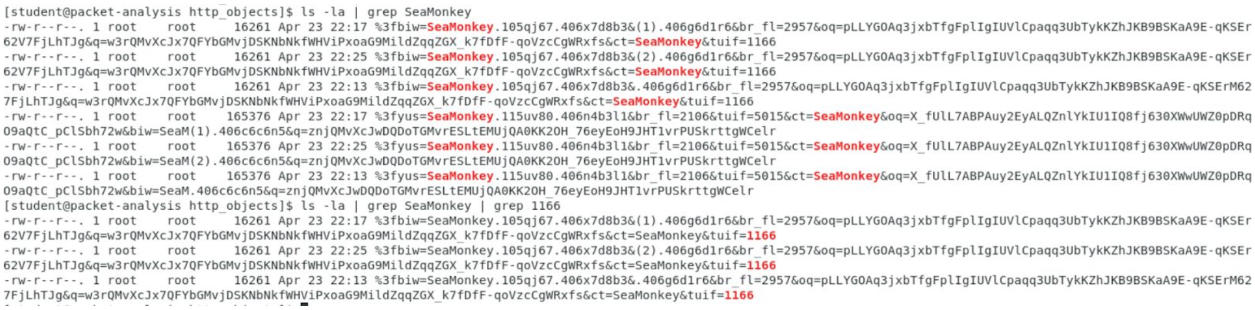
```
[student@packet-analysis Homework]$ cat httphash.txt| grep f858070326067ba282d2a63969868e5a
f858070326067ba282d2a63969868e5a  http_objects/%3fbiw=Amaya.126qv100.406m1g9g5&ct=Amaya&tuif=2927&q=zn3QMvXcJwDQDoTGMvrESLtEMU_QA0KK2OH_76qyEoH9JHT1vrTUSkrttgWCelr&oq=X_
fUlL7ABPAay2EyALQZnlY0IU1IQ8fj630PWwUWZ0pDRqxS9ZQxD_JGlV7V8jg&yus=Amaya.83fn6(1).406z8s0i4&br_fl=4442
f858070326067ba282d2a63969868e5a  http_objects/%3fbiw=Amaya.126qv100.406m1g9g5&ct=Amaya&tuif=2927&q=zn3QMvXcJwDQDoTGMvrESLtEMU_QA0KK2OH_76qyEoH9JHT1vrTUSkrttgWCelr&oq=X_
fUlL7ABPAay2EyALQZnlY0IU1IQ8fj630PWwUWZ0pDRqxS9ZQxD_JGlV7V8jg&yus=Amaya.83fn6(2).406z8s0i4&br_fl=4442
f858070326067ba282d2a63969868e5a  http_objects/%3fbiw=Amaya.126qv100.406m1g9g5&ct=Amaya&tuif=2927&q=zn3QMvXcJwDQDoTGMvrESLtEMU_QA0KK2OH_76qyEoH9JHT1vrTUSkrttgWCelr&oq=X_
fUlL7ABPAay2EyALQZnlY0IU1IQ8fj630PWwUWZ0pDRqxS9ZQxD_JGlV7V8jg&yus=Amaya.83fn6.406z8s0i4&br_fl=4442
f858070326067ba282d2a63969868e5a  http_objects/%3fbiw=SeaMonkey.105qj67.406x7d8b3&(1).406g6d1r6&br_fl=2957&oq=pLLYGOAq3jxbTfgFplIgIUVlCpaqq3UbTykKZhJKB9BSKaA9E-qKSErM62V
7FjLhTJg&q=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoaG9MildZqqZGX_k7fDfF-qoVzcCgWRxfs&ct=SeaMonkey&tuif=1166
f858070326067ba282d2a63969868e5a  http_objects/%3fbiw=SeaMonkey.105qj67.406x7d8b3&(2).406g6d1r6&br_fl=2957&oq=pLLYGOAq3jxbTfgFplIgIUVlCpaqq3UbTykKZhJKB9BSKaA9E-qKSErM62V
7FjLhTJg&q=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoaG9MildZqqZGX_k7fDfF-qoVzcCgWRxfs&ct=SeaMonkey&tuif=1166
f858070326067ba282d2a63969868e5a  http_objects/%3fbiw=SeaMonkey.105qj67.406x7d8b3&.406g6d1r6&br_fl=2957&oq=pLLYGOAq3jxbTfgFplIgIUVlCpaqq3UbTykKZhJKB9BSKaA9E-qKSErM62V7Fj
LhTJg&q=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoaG9MildZqqZGX_k7fDfF-qoVzcCgWRxfs&ct=SeaMonkey&tuif=1166
f858070326067ba282d2a63969868e5a  http_objects/%3foq=pLLYGOAS3jxbTfgNplIgIUV9Cpaqq3UDTykKZhJ6B9BSKaA9E-qKRFLE60FXFjLNTJg&biw=Mozilla.104md76.406y0g1v2&br_fl=5102&ct=Mozi
lla&tuif=4948&yus=(1).406y2d5y7&q=w37QMvXcJxjQFYbGMvnDSKNbNkrWHViPxoiG9MildZ-qZGX_k7vDfF-qoV3cCgWRxfU
f858070326067ba282d2a63969868e5a  http_objects/%3foq=pLLYGOAS3jxbTfgNplIgIUV9Cpaqq3UDTykKZhJ6B9BSKaA9E-qKRFLE60FXFjLNTJg&biw=Mozilla.104md76.406y0g1v2&br_fl=5102&ct=Mozi
lla&tuif=4948&yus=(2).406y2d5y7&q=w37QMvXcJxjQFYbGMvnDSKNbNkrWHViPxoiG9MildZ-qZGX_k7vDfF-qoV3cCgWRxfU
f858070326067ba282d2a63969868e5a  http_objects/%3foq=pLLYGOAS3jxbTfgNplIgIUV9Cpaqq3UDTykKZhJ6B9BSKaA9E-qKRFLE60FXFjLNTJg&biw=Mozilla.104md76.406y0g1v2&br_fl=5102&ct=Mozi
lla&tuif=4948&yus=.406y2d5y7&q=w37QMvXcJxjQFYbGMvnDSKNbNkrWHViPxoiG9MildZ-qZGX_k7vDfF-qoV3cCgWRxfU
f858070326067ba282d2a63969868e5a  http_objects/%3ftuif=2138&br_fl=1788&oq=_skK7pSP1LghRbVcgU3n4lbWw8S_6qniBCBmBWUgcSHrxLeNw51_paUErQ66B6ymQ&q=wHvQMvXcJwDGFYbGMvrETqNbNkn
QA0GPxpH2_drRdZqxKGni0eb5UUSk6F2CEh3h8&ct=Vivaldi&biw=Vivaldi.101ck66.406l4u7k3&yus=Viva(1).406b4o1l4
f858070326067ba282d2a63969868e5a  http_objects/%3ftuif=2138&br_fl=1788&oq=_skK7pSP1LghRbVcgU3n4lbWw8S_6qniBCBmBWUgcSHrxLeNw51_paUErQ66B6ymQ&q=wHvQMvXcJwDGFYbGMvrETqNbNkn
QA0GPxpH2_drRdZqxKGni0eb5UUSk6F2CEh3h8&ct=Vivaldi&biw=Vivaldi.101ck66.406l4u7k3&yus=Viva(2).406b4o1l4
f858070326067ba282d2a63969868e5a  http_objects/%3ftuif=2138&br_fl=1788&oq=_skK7pSP1LghRbVcgU3n4lbWw8S_6qniBCBmBWUgcSHrxLeNw51_paUErQ66B6ymQ&q=wHvQMvXcJwDGFYbGMvrETqNbNkn
QA0GPxpH2_drRdZqxKGni0eb5UUSk6F2CEh3h8&ct=Vivaldi&biw=Vivaldi.101ck66.406l4u7k3&yus=Viva.406b4o1l4
```

Type 1



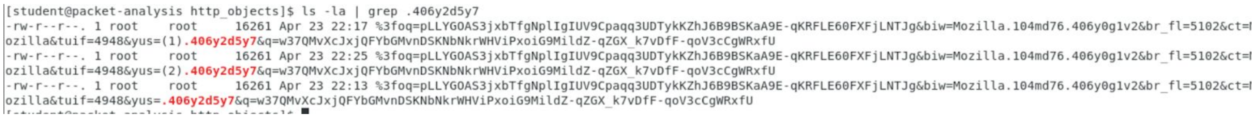
```
[student@packet-analysis http_objects]$ ls -la | grep Amaya.83fn6
-rw-r--r--. 1 root     root      16261 Apr 23 22:17 %3fbiw=Amaya.126qv100.406m1g9g5&ct=Amaya&tuif=2927&q=zn3QMvXcJwDQDoTGMvrESLtEMU_QA0KK2OH_76qyEoH9JHT1vrTUSkrttgWCelr&oq
=X_fUlL7ABPAay2EyALQZnlY0IU1IQ8fj630PWwUWZ0pDRqxS9ZQxD_JGlV7V8jg&yus=Amaya.83fn6(1).406z8s0i4&br_fl=4442
-rw-r--r--. 1 root     root      16261 Apr 23 22:25 %3fbiw=Amaya.126qv100.406m1g9g5&ct=Amaya&tuif=2927&q=zn3QMvXcJwDQDoTGMvrESLtEMU_QA0KK2OH_76qyEoH9JHT1vrTUSkrttgWCelr&oq
=X_fUlL7ABPAay2EyALQZnlY0IU1IQ8fj630PWwUWZ0pDRqxS9ZQxD_JGlV7V8jg&yus=Amaya.83fn6(2).406z8s0i4&br_fl=4442
-rw-r--r--. 1 root     root      16261 Apr 23 22:13 %3fbiw=Amaya.126qv100.406m1g9g5&ct=Amaya&tuif=2927&q=zn3QMvXcJwDQDoTGMvrESLtEMU_QA0KK2OH_76qyEoH9JHT1vrTUSkrttgWCelr&oq
=X_fUlL7ABPAay2EyALQZnlY0IU1IQ8fj630PWwUWZ0pDRqxS9ZQxD_JGlV7V8jg&yus=Amaya.83fn6.406z8s0i4&br_fl=4442
```

Type 2



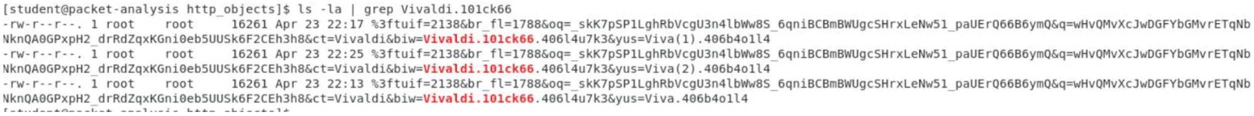
```
[student@packet-analysis http_objects]$ ls -la | grep SeaMonkey
-rw-r--r--. 1 root     root      16261 Apr 23 22:17 %3fbiw=SeaMonkey.105qj67.406x7d8b3&(1).406g6d1r6&br_fl=2957&oq=pLLYGOAq3jxbTfgFplIgIUVlCpaqq3UbTykKZhJKB9BSKaA9E-qKSEr
62V7FjLhTJg&q=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoaG9MildZqqZGX_k7fDfF-qoVzcCgWRxfs&ct=SeaMonkey&tuif=1166
-rw-r--r--. 1 root     root      16261 Apr 23 22:25 %3fbiw=SeaMonkey.105qj67.406x7d8b3&(2).406g6d1r6&br_fl=2957&oq=pLLYGOAq3jxbTfgFplIgIUVlCpaqq3UbTykKZhJKB9BSKaA9E-qKSEr
62V7FjLhTJg&q=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoaG9MildZqqZGX_k7fDfF-qoVzcCgWRxfs&ct=SeaMonkey&tuif=1166
-rw-r--r--. 1 root     root      16261 Apr 23 22:13 %3fbiw=SeaMonkey.105qj67.406x7d8b3&.406g6d1r6&br_fl=2957&oq=pLLYGOAq3jxbTfgFplIgIUVlCpaqq3UbTykKZhJKB9BSKaA9E-qKSErM62
7FjLhTJg&q=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoaG9MildZqqZGX_k7fDfF-qoVzcCgWRxfs&ct=SeaMonkey&tuif=1166
-rw-r--r--. 1 root     root      165376 Apr 23 22:17 %3fyus=SeaMonkey.115uv80.406n4b3l1&br_fl=2106&tuif=5015&ct=SeaMonkey&oq=X_fUlL7ABPAuy2EyALQZnlYkIU1IQ8fj630XWwUWZ0pDRq
O9aQtC_pClSbh72w&biw=SeaM(1).406c6c6n5&q=znjQMvXcJwDQDoTGMvrESLtEMUjQA0KK2OH_76eyEoH9JHT1vrPUSkrttgWCelr
-rw-r--r--. 1 root     root      165376 Apr 23 22:25 %3fyus=SeaMonkey.115uv80.406n4b3l1&br_fl=2106&tuif=5015&ct=SeaMonkey&oq=X_fUlL7ABPAuy2EyALQZnlYkIU1IQ8fj630XWwUWZ0pDRq
O9aQtC_pClSbh72w&biw=SeaM(2).406c6c6n5&q=znjQMvXcJwDQDoTGMvrESLtEMUjQA0KK2OH_76eyEoH9JHT1vrPUSkrttgWCelr
-rw-r--r--. 1 root     root      165376 Apr 23 22:13 %3fyus=SeaMonkey.115uv80.406n4b3l1&br_fl=2106&tuif=5015&ct=SeaMonkey&oq=X_fUlL7ABPAuy2EyALQZnlYkIU1IQ8fj630XWwUWZ0pDRq
O9aQtC_pClSbh72w&biw=SeaM.406c6c6n5&q=znjQMvXcJwDQDoTGMvrESLtEMUjQA0KK2OH_76eyEoH9JHT1vrPUSkrttgWCelr
[student@packet-analysis http_objects]$ ls -la | grep SeaMonkey | grep 1166
-rw-r--r--. 1 root     root      16261 Apr 23 22:17 %3fbiw=SeaMonkey.105qj67.406x7d8b3&(1).406g6d1r6&br_fl=2957&oq=pLLYGOAq3jxbTfgFplIgIUVlCpaqq3UbTykKZhJKB9BSKaA9E-qKSEr
62V7FjLhTJg&q=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoaG9MildZqqZGX_k7fDfF-qoVzcCgWRxfs&ct=SeaMonkey&tuif=1166
-rw-r--r--. 1 root     root      16261 Apr 23 22:25 %3fbiw=SeaMonkey.105qj67.406x7d8b3&(2).406g6d1r6&br_fl=2957&oq=pLLYGOAq3jxbTfgFplIgIUVlCpaqq3UbTykKZhJKB9BSKaA9E-qKSEr
62V7FjLhTJg&q=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoaG9MildZqqZGX_k7fDfF-qoVzcCgWRxfs&ct=SeaMonkey&tuif=1166
-rw-r--r--. 1 root     root      16261 Apr 23 22:13 %3fbiw=SeaMonkey.105qj67.406x7d8b3&.406g6d1r6&br_fl=2957&oq=pLLYGOAq3jxbTfgFplIgIUVlCpaqq3UbTykKZhJKB9BSKaA9E-qKSErM62
7FjLhTJg&q=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoaG9MildZqqZGX_k7fDfF-qoVzcCgWRxfs&ct=SeaMonkey&tuif=1166
```

Type 3



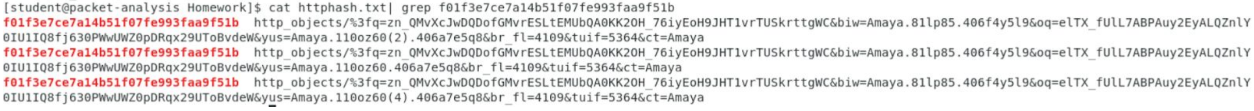
```
[student@packet-analysis http_objects]$ ls -la | grep .406y2d5y7
-rw-r--r--. 1 root     root      16261 Apr 23 22:17 %3foq=pLLYGOAS3jxbTfgNplIgIUV9Cpaqq3UDTykKZhJ6B9BSKaA9E-qKRFLE60FXFjLNTJg&biw=Mozilla.104md76.406y0g1v2&br_fl=5102&ct=M
ozilla&tuif=4948&yus=(1).406y2d5y7&q=w37QMvXcJxjQFYbGMvnDSKNbNkrWHViPxoiG9MildZ-qZGX_k7vDfF-qoV3cCgWRxfU
-rw-r--r--. 1 root     root      16261 Apr 23 22:25 %3foq=pLLYGOAS3jxbTfgNplIgIUV9Cpaqq3UDTykKZhJ6B9BSKaA9E-qKRFLE60FXFjLNTJg&biw=Mozilla.104md76.406y0g1v2&br_fl=5102&ct=M
ozilla&tuif=4948&yus=(2).406y2d5y7&q=w37QMvXcJxjQFYbGMvnDSKNbNkrWHViPxoiG9MildZ-qZGX_k7vDfF-qoV3cCgWRxfU
-rw-r--r--. 1 root     root      16261 Apr 23 22:13 %3foq=pLLYGOAS3jxbTfgNplIgIUV9Cpaqq3UDTykKZhJ6B9BSKaA9E-qKRFLE60FXFjLNTJg&biw=Mozilla.104md76.406y0g1v2&br_fl=5102&ct=M
ozilla&tuif=4948&yus=.406y2d5y7&q=w37QMvXcJxjQFYbGMvnDSKNbNkrWHViPxoiG9MildZ-qZGX_k7vDfF-qoV3cCgWRxfU
```

Type 4



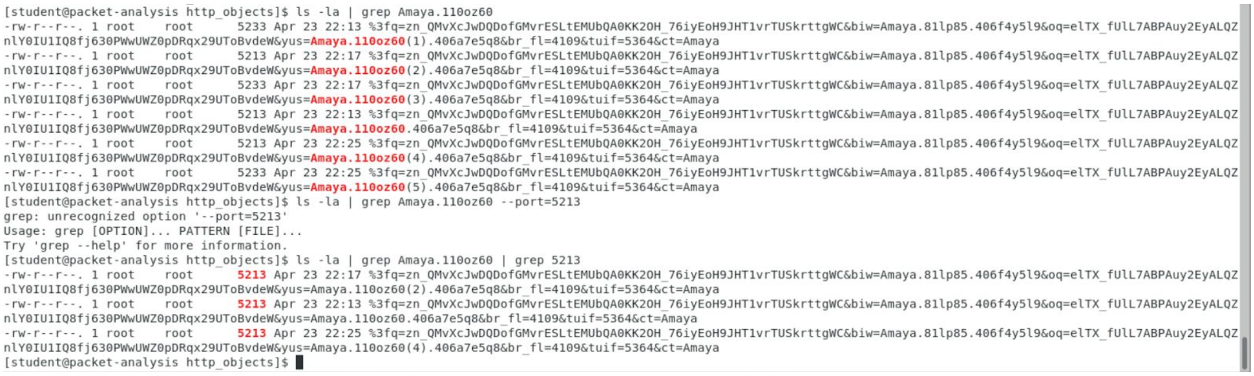
```
[student@packet-analysis http_objects]$ ls -la | grep Vivaldi.101ck66
-rw-r--r--. 1 root     root      16261 Apr 23 22:17 %3ftuif=2138&br_fl=1788&oq=_skK7pSP1LghRbVcgU3n4lbWw8S_6qniBCBmBWUgcSHrxLeNw51_paUErQ66B6ymQ&q=wHvQMvXcJwDGFYbGMvrETqNb
NknQA0GPxpH2_drRdZqxKGni0eb5UUSk6F2CEh3h8&ct=Vivaldi&biw=Vivaldi.101ck66.406l4u7k3&yus=Viva(1).406b4o1l4
-rw-r--r--. 1 root     root      16261 Apr 23 22:25 %3ftuif=2138&br_fl=1788&oq=_skK7pSP1LghRbVcgU3n4lbWw8S_6qniBCBmBWUgcSHrxLeNw51_paUErQ66B6ymQ&q=wHvQMvXcJwDGFYbGMvrETqNb
NknQA0GPxpH2_drRdZqxKGni0eb5UUSk6F2CEh3h8&ct=Vivaldi&biw=Vivaldi.101ck66.406l4u7k3&yus=Viva(2).406b4o1l4
-rw-r--r--. 1 root     root      16261 Apr 23 22:13 %3ftuif=2138&br_fl=1788&oq=_skK7pSP1LghRbVcgU3n4lbWw8S_6qniBCBmBWUgcSHrxLeNw51_paUErQ66B6ymQ&q=wHvQMvXcJwDGFYbGMvrETqNb
NknQA0GPxpH2_drRdZqxKGni0eb5UUSk6F2CEh3h8&ct=Vivaldi&biw=Vivaldi.101ck66.406l4u7k3&yus=Viva.406b4o1l4
```

Infected Hash No. 16 files



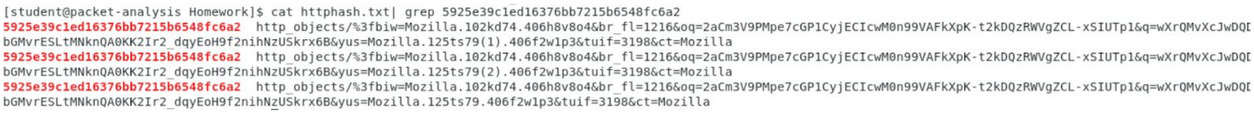
```
[student@packet-analysis Homework]$ cat httphash.txt| grep f01f3e7ce7a14b51f07fe993faa9f51b
f01f3e7ce7a14b51f07fe993faa9f51b  http_objects/%3fq=zn_QMvXcJwDQDofGMvrESLtEMUbQA0KK2OH_76iyEoH9JHT1vrTUSkrttgWC&biw=Amaya.81lp85.406f4y5l9&oq=elTX_fUlL7ABPAuy2EyALQZnlY
0IU1IQ8fj630PWwUWZ0pDRqx29UToBvdeW&yus=Amaya.110oz60(2).406a7e5q8&br_fl=4109&tuif=5364&ct=Amaya
f01f3e7ce7a14b51f07fe993faa9f51b  http_objects/%3fq=zn_QMvXcJwDQDofGMvrESLtEMUbQA0KK2OH_76iyEoH9JHT1vrTUSkrttgWC&biw=Amaya.81lp85.406f4y5l9&oq=elTX_fUlL7ABPAuy2EyALQZnlY
0IU1IQ8fj630PWwUWZ0pDRqx29UToBvdeW&yus=Amaya.110oz60.406a7e5q8&br_fl=4109&tuif=5364&ct=Amaya
f01f3e7ce7a14b51f07fe993faa9f51b  http_objects/%3fq=zn_QMvXcJwDQDofGMvrESLtEMUbQA0KK2OH_76iyEoH9JHT1vrTUSkrttgWC&biw=Amaya.81lp85.406f4y5l9&oq=elTX_fUlL7ABPAuy2EyALQZnlY
0IU1IQ8fj630PWwUWZ0pDRqx29UToBvdeW&yus=Amaya.110oz60(4).406a7e5q8&br_fl=4109&tuif=5364&ct=Amaya
```

Type 1



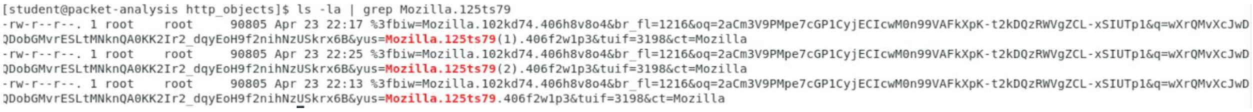
```
[student@packet-analysis http_objects]$ ls -la | grep Amaya.110oz60
-rw-r--r--. 1 root    root      5233 Apr 23 22:13 %3fq=zn_QMvXcJwDQDofGMvrESLtEMUbQA0KK2OH_76iyEoH9JHT1vrTUSkrttgWC&biw=Amaya.81lp85.406f4y5l9&oq=elTX_fUlL7ABPAuy2EyALQZ
nlY0IU1IQ8fj630PWwUWZ0pDRqx29UToBvdeW&yus=Amaya.110oz60(1).406a7e5q8&br_fl=4109&tuif=5364&ct=Amaya
-rw-r--r--. 1 root    root      5213 Apr 23 22:17 %3fq=zn_QMvXcJwDQDofGMvrESLtEMUbQA0KK2OH_76iyEoH9JHT1vrTUSkrttgWC&biw=Amaya.81lp85.406f4y5l9&oq=elTX_fUlL7ABPAuy2EyALQZ
nlY0IU1IQ8fj630PWwUWZ0pDRqx29UToBvdeW&yus=Amaya.110oz60(2).406a7e5q8&br_fl=4109&tuif=5364&ct=Amaya
-rw-r--r--. 1 root    root      5233 Apr 23 22:17 %3fq=zn_QMvXcJwDQDofGMvrESLtEMUbQA0KK2OH_76iyEoH9JHT1vrTUSkrttgWC&biw=Amaya.81lp85.406f4y5l9&oq=elTX_fUlL7ABPAuy2EyALQZ
nlY0IU1IQ8fj630PWwUWZ0pDRqx29UToBvdeW&yus=Amaya.110oz60(3).406a7e5q8&br_fl=4109&tuif=5364&ct=Amaya
-rw-r--r--. 1 root    root      5213 Apr 23 22:13 %3fq=zn_QMvXcJwDQDofGMvrESLtEMUbQA0KK2OH_76iyEoH9JHT1vrTUSkrttgWC&biw=Amaya.81lp85.406f4y5l9&oq=elTX_fUlL7ABPAuy2EyALQZ
nlY0IU1IQ8fj630PWwUWZ0pDRqx29UToBvdeW&yus=Amaya.110oz60.406a7e5q8&br_fl=4109&tuif=5364&ct=Amaya
-rw-r--r--. 1 root    root      5213 Apr 23 22:25 %3fq=zn_QMvXcJwDQDofGMvrESLtEMUbQA0KK2OH_76iyEoH9JHT1vrTUSkrttgWC&biw=Amaya.81lp85.406f4y5l9&oq=elTX_fUlL7ABPAuy2EyALQZ
nlY0IU1IQ8fj630PWwUWZ0pDRqx29UToBvdeW&yus=Amaya.110oz60(4).406a7e5q8&br_fl=4109&tuif=5364&ct=Amaya
-rw-r--r--. 1 root    root      5233 Apr 23 22:25 %3fq=zn_QMvXcJwDQDofGMvrESLtEMUbQA0KK2OH_76iyEoH9JHT1vrTUSkrttgWC&biw=Amaya.81lp85.406f4y5l9&oq=elTX_fUlL7ABPAuy2EyALQZ
nlY0IU1IQ8fj630PWwUWZ0pDRqx29UToBvdeW&yus=Amaya.110oz60(5).406a7e5q8&br_fl=4109&tuif=5364&ct=Amaya
[student@packet-analysis http_objects]$ ls -la | grep Amaya.110oz60 --port=5213
grep: unrecognized option '--port=5213'
Usage: grep [OPTION]... PATTERN [FILE]...
Try 'grep --help' for more information.
[student@packet-analysis http_objects]$ ls -la | grep Amaya.110oz60 | grep 5213
-rw-r--r--. 1 root    root      5213 Apr 23 22:17 %3fq=zn_QMvXcJwDQDofGMvrESLtEMUbQA0KK2OH_76iyEoH9JHT1vrTUSkrttgWC&biw=Amaya.81lp85.406f4y5l9&oq=elTX_fUlL7ABPAuy2EyALQZ
nlY0IU1IQ8fj630PWwUWZ0pDRqx29UToBvdeW&yus=Amaya.110oz60(2).406a7e5q8&br_fl=4109&tuif=5364&ct=Amaya
-rw-r--r--. 1 root    root      5213 Apr 23 22:13 %3fq=zn_QMvXcJwDQDofGMvrESLtEMUbQA0KK2OH_76iyEoH9JHT1vrTUSkrttgWC&biw=Amaya.81lp85.406f4y5l9&oq=elTX_fUlL7ABPAuy2EyALQZ
nlY0IU1IQ8fj630PWwUWZ0pDRqx29UToBvdeW&yus=Amaya.110oz60.406a7e5q8&br_fl=4109&tuif=5364&ct=Amaya
-rw-r--r--. 1 root    root      5213 Apr 23 22:25 %3fq=zn_QMvXcJwDQDofGMvrESLtEMUbQA0KK2OH_76iyEoH9JHT1vrTUSkrttgWC&biw=Amaya.81lp85.406f4y5l9&oq=elTX_fUlL7ABPAuy2EyALQZ
nlY0IU1IQ8fj630PWwUWZ0pDRqx29UToBvdeW&yus=Amaya.110oz60(4).406a7e5q8&br_fl=4109&tuif=5364&ct=Amaya
[student@packet-analysis http_objects]$ 
```

Infected Hash No. 19 files



```
[student@packet-analysis Homework]$ cat httphash.txt| grep 5925e39c1ed16376bb7215b6548fc6a2
5925e39c1ed16376bb7215b6548fc6a2  http_objects/%3fbiw=Mozilla.102kd74.406h8v8o4&br_fl=1216&oq=2aCm3V9PMpe7cGP1CyjECIcwM0n99VAFkXpK-t2kDQzRWVgZCL-xSIUTp1&q=wXrQMvXcJwDQD
bGMvrESLtMNknQA0KK2Ir2_dqyEoH9f2nihNzUSkrx6B&yus=Mozilla.125ts79(1).406f2w1p3&tuif=3198&ct=Mozilla
5925e39c1ed16376bb7215b6548fc6a2  http_objects/%3fbiw=Mozilla.102kd74.406h8v8o4&br_fl=1216&oq=2aCm3V9PMpe7cGP1CyjECIcwM0n99VAFkXpK-t2kDQzRWVgZCL-xSIUTp1&q=wXrQMvXcJwDQD
bGMvrESLtMNknQA0KK2Ir2_dqyEoH9f2nihNzUSkrx6B&yus=Mozilla.125ts79(2).406f2w1p3&tuif=3198&ct=Mozilla
5925e39c1ed16376bb7215b6548fc6a2  http_objects/%3fbiw=Mozilla.102kd74.406h8v8o4&br_fl=1216&oq=2aCm3V9PMpe7cGP1CyjECIcwM0n99VAFkXpK-t2kDQzRWVgZCL-xSIUTp1&q=wXrQMvXcJwDQD
bGMvrESLtMNknQA0KK2Ir2_dqyEoH9f2nihNzUSkrx6B&yus=Mozilla.125ts79.406f2w1p3&tuif=3198&ct=Mozilla
```

Type 1

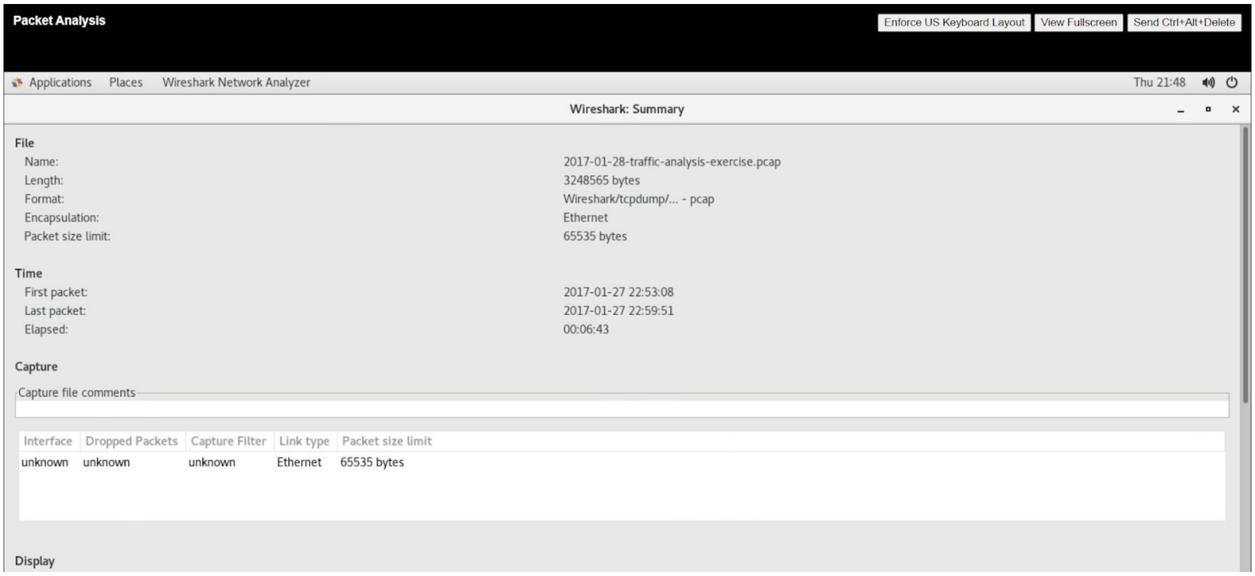


```
[student@packet-analysis http_objects]$ ls -la | grep Mozilla.125ts79
-rw-r--r--. 1 root    root     90805 Apr 23 22:17 %3fbiw=Mozilla.102kd74.406h8v8o4&br_fl=1216&oq=2aCm3V9PMpe7cGP1CyjECIcwM0n99VAFkXpK-t2kDQzRWVgZCL-xSIUTp1&q=wXrQMvXcJwD
QDobGMvrESLtMNknQA0KK2Ir2_dqyEoH9f2nihNzUSkrx6B&yus=Mozilla.125ts79(1).406f2w1p3&tuif=3198&ct=Mozilla
-rw-r--r--. 1 root    root     90805 Apr 23 22:25 %3fbiw=Mozilla.102kd74.406h8v8o4&br_fl=1216&oq=2aCm3V9PMpe7cGP1CyjECIcwM0n99VAFkXpK-t2kDQzRWVgZCL-xSIUTp1&q=wXrQMvXcJwD
QDobGMvrESLtMNknQA0KK2Ir2_dqyEoH9f2nihNzUSkrx6B&yus=Mozilla.125ts79(2).406f2w1p3&tuif=3198&ct=Mozilla
-rw-r--r--. 1 root    root     90805 Apr 23 22:13 %3fbiw=Mozilla.102kd74.406h8v8o4&br_fl=1216&oq=2aCm3V9PMpe7cGP1CyjECIcwM0n99VAFkXpK-t2kDQzRWVgZCL-xSIUTp1&q=wXrQMvXcJwD
QDobGMvrESLtMNknQA0KK2Ir2_dqyEoH9f2nihNzUSkrx6B&yus=Mozilla.125ts79.406f2w1p3&tuif=3198&ct=Mozilla
```

Questions

Analysis

1. The packets were captured during what day and time?



Wireshark: Summary

File

Name: 2017-01-28-traffic-analysis-exercise.pcap
Length: 3248565 bytes
Format: Wireshark/tcpdump/... - pcap
Encapsulation: Ethernet
Packet size limit: 65535 bytes

Time

First packet: 2017-01-27 22:53:08
Last packet: 2017-01-27 22:59:51
Elapsed: 00:06:43

Capture

Capture file comments

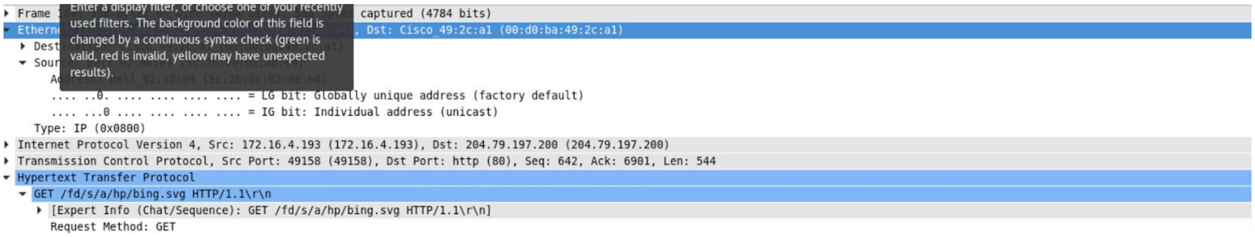
Interface	Dropped Packets	Capture Filter	Link type	Packet size limit
unknown	unknown	unknown	Ethernet	65535 bytes

Display

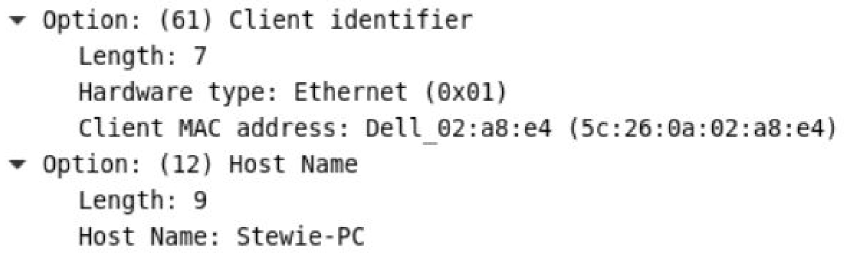
First packet - 01-27-2017 , 22:53:08

Last packet - 01-27-2017 , 22:59:51

2. What is the IP address, Mac address, and host name of the infected Windows computer?



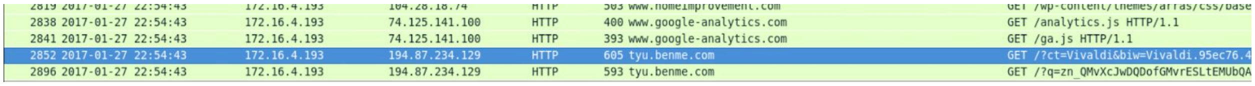
```
▸ Frame  Enter a display filter, or choose one of your recently    captured (4784 bits)
▾ Etherne used filters. The background color of this field is    , Dst: Cisco_49:2c:a1 (00:d0:ba:49:2c:a1)
  ▸ Dest  changed by a continuous syntax check (green is
  ▾ Sour  valid, red is invalid, yellow may have unexpected
      Ad  results).
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IP (0x0800)
▸ Internet Protocol Version 4, Src: 172.16.4.193 (172.16.4.193), Dst: 204.79.197.200 (204.79.197.200)
▸ Transmission Control Protocol, Src Port: 49158 (49158), Dst Port: http (80), Seq: 642, Ack: 6901, Len: 544
▾ Hypertext Transfer Protocol
  ▾ GET /fd/s/a/hp/bing.svg HTTP/1.1\r\n
    ▸ [Expert Info (Chat/Sequence): GET /fd/s/a/hp/bing.svg HTTP/1.1\r\n]
      Request Method: GET
```



```
▾ Option: (61) Client identifier
    Length: 7
    Hardware type: Ethernet (0x01)
    Client MAC address: Dell_02:a8:e4 (5c:26:0a:02:a8:e4)
▾ Option: (12) Host Name
    Length: 9
    Host Name: Stewie-PC
```

Source IP - 172.16.4.193
MAC - 5c:26:0a:02:a8:e4
Hostname - Stewie - PC

3. When did the infection begin? (Date and Time)



```
2819 2017-01-27 22:54:43   172.16.4.193   104.28.18.74     HTTP   503 www.homeimprovement.com       GET /wp-content/themes/arras/css/base
2838 2017-01-27 22:54:43   172.16.4.193   74.125.141.100   HTTP   400 www.google-analytics.com      GET /analytics.js HTTP/1.1
2841 2017-01-27 22:54:43   172.16.4.193   74.125.141.100   HTTP   393 www.google-analytics.com      GET /ga.js HTTP/1.1
2852 2017-01-27 22:54:43   172.16.4.193   194.87.234.129   HTTP   605 tyu.benme.com                 GET /?ct=Vivaldi&biw=Vivaldi.95ec76.4
2896 2017-01-27 22:54:43   172.16.4.193   194.87.234.129   HTTP   593 tyu.benme.com                 GET /?q=zn_QMvXcJwDQDofGMvrESLtEMUbQA
```

Infection started at 01-27-2017 , 22:54:43

4. What type of malware was the computer infected with?

The Malware type was Trojan Horse(Shown in VirusTotal Analysis).

5. What happened during the infection?

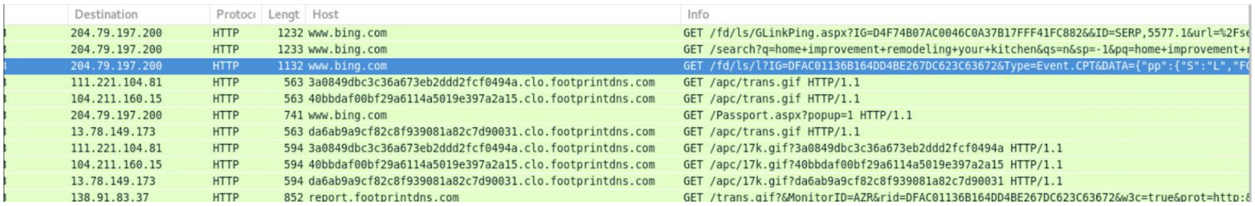
The malware tried to contact other urls and downloaded other malicious payloads including the exploit kits.

Recommended Cleanup and Mitigation Strategies

First we should try to kill any malware related processes detected using a combination of wireshark, any antivirus, tak manager, snort and other tools. Then we should Block all incoming and outgoing traffic using Firewall(Network Firewall Preferred, but can use ufw or iptables as well). Then use system tools and logs to remove all suspicious programs and reset all your passwords after that. Then create firewall rules to allow only required network traffic and install some good malware scanner and mitigation software for your system(preferably for web apps as well). Keep OS and apps like browsers up to date (especially security updates) and create a backup of the system and store it in case you have your system compromised in the future.

Extra Credit

1. Before the Windows computer was infected, what did the user search for on Bing?



Destination	Protoc	Lengt	Host	Info
204.79.197.200	HTTP	1232	www.bing.com	GET /fd/ls/GLinkPing.aspx?IG=D4F74B07AC0046C0A37B17FFF41FC882&&ID=SERP,5577.1&url=%2Fse
204.79.197.200	HTTP	1233	www.bing.com	GET /search?q=home+improvement+remodeling+your+kitchen&qs=n&sp=-1&pq=home+improvement+r
204.79.197.200	HTTP	1132	www.bing.com	GET /fd/ls/l?IG=DFAC01136B164DD4BE267DC623C63672&Type=Event.CPT&DATA={"pp":{"S":"L","FC
111.221.104.81	HTTP	563	3a0849dbc3c36a673eb2ddd2fcf0494a.clo.footprintdns.com	GET /apc/trans.gif HTTP/1.1
104.211.160.15	HTTP	563	40bbdaf00bf29a6114a5019e397a2a15.clo.footprintdns.com	GET /apc/trans.gif HTTP/1.1
204.79.197.200	HTTP	741	www.bing.com	GET /Passport.aspx?popup=1 HTTP/1.1
13.78.149.173	HTTP	563	da6ab9a9cf82c8f939081a82c7d90031.clo.footprintdns.com	GET /apc/trans.gif HTTP/1.1
111.221.104.81	HTTP	594	3a0849dbc3c36a673eb2ddd2fcf0494a.clo.footprintdns.com	GET /apc/17k.gif?3a0849dbc3c36a673eb2ddd2fcf0494a HTTP/1.1
104.211.160.15	HTTP	594	40bbdaf00bf29a6114a5019e397a2a15.clo.footprintdns.com	GET /apc/17k.gif?40bbdaf00bf29a6114a5019e397a2a15 HTTP/1.1
13.78.149.173	HTTP	594	da6ab9a9cf82c8f939081a82c7d90031.clo.footprintdns.com	GET /apc/17k.gif?da6ab9a9cf82c8f939081a82c7d90031 HTTP/1.1
138.91.83.37	HTTP	852	report.footprintdns.com	GET /trans.gif?&MonitorID=AZR&rid=DFAC01136B164DD4BE267DC623C63672&w3c=true&prot=http:&

User Searched - home improvement remodelling your kitchen

2. What exploit kit was used to infect the Windows computer?

Multiple Exploit Kits were used including -
Swf Exploit
ExpKit.Gen2
Exploit-RigKit.i

3. What is the name of the malware?

Multiple types of malware were used including -
Trojan Horse - Cryxos
Trojan Horse - GenericKD