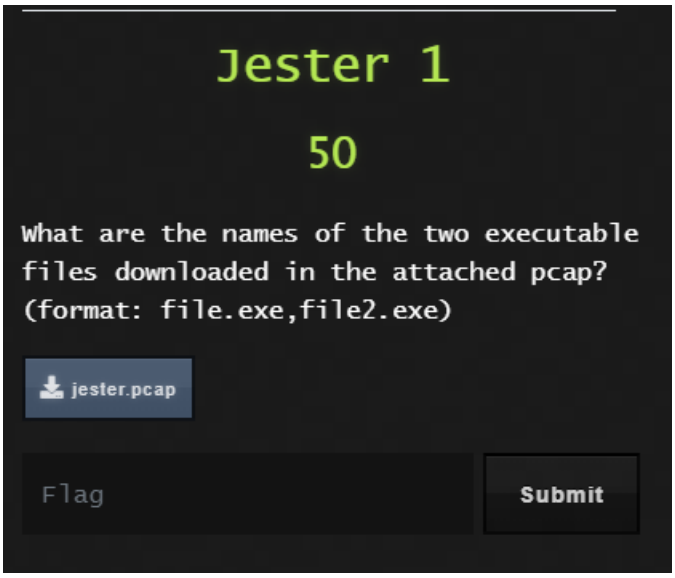


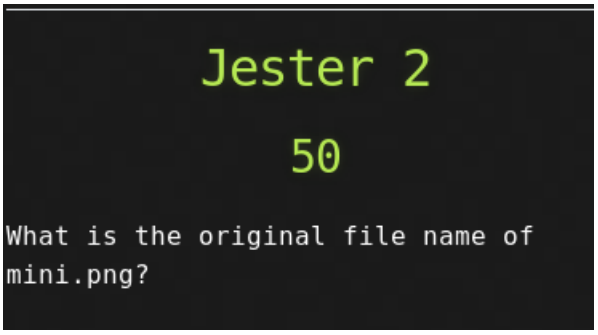
Opening up the Pcap file, we are looking for 2 files that are downloaded.

To start off check out the files that we can export under file -> export objects -> http

Packet	Hostname	Content Type	Size	Filename
1457	ipecho.net	text/html	15 bytes	plain
3021	203.176.135.102:8082	multipart/form-data	219 bytes	81
3025	203.176.135.102:8082	text/plain	3 bytes	81
3072	203.176.135.102:8082	multipart/form-data	4,748 bytes	90
3079	203.176.135.102:8082	text/plain	3 bytes	90
3100	203.176.135.102:8082	multipart/form-data	210 bytes	81
3104	203.176.135.102:8082	text/plain	3 bytes	81
3822	myexternalip.com	text/html	15 bytes	raw
12983	203.176.135.102:8082	multipart/form-data	219 bytes	81
12985	203.176.135.102:8082	text/plain	3 bytes	81
13022	203.176.135.102:8082	multipart/form-data	210 bytes	81
13024	203.176.135.102:8082	text/plain	3 bytes	81
14592	192.3.124.40	content-type:	679 kB	lastimg.png
15252	192.3.124.40	content-type:	679 kB	mini.png
16398	192.3.124.40	content-type:	679 kB	mini.png

We see only two files that might be anything, lastimg.png and mini.png

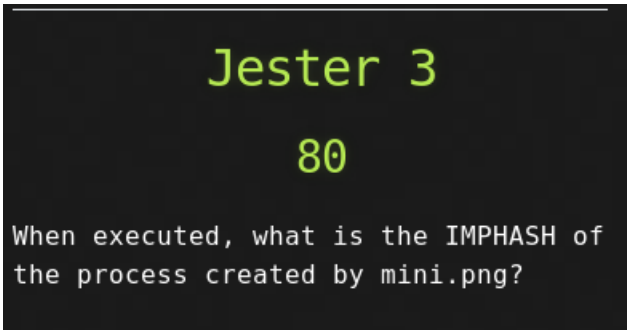
Flag: lastimg.png,mini.png



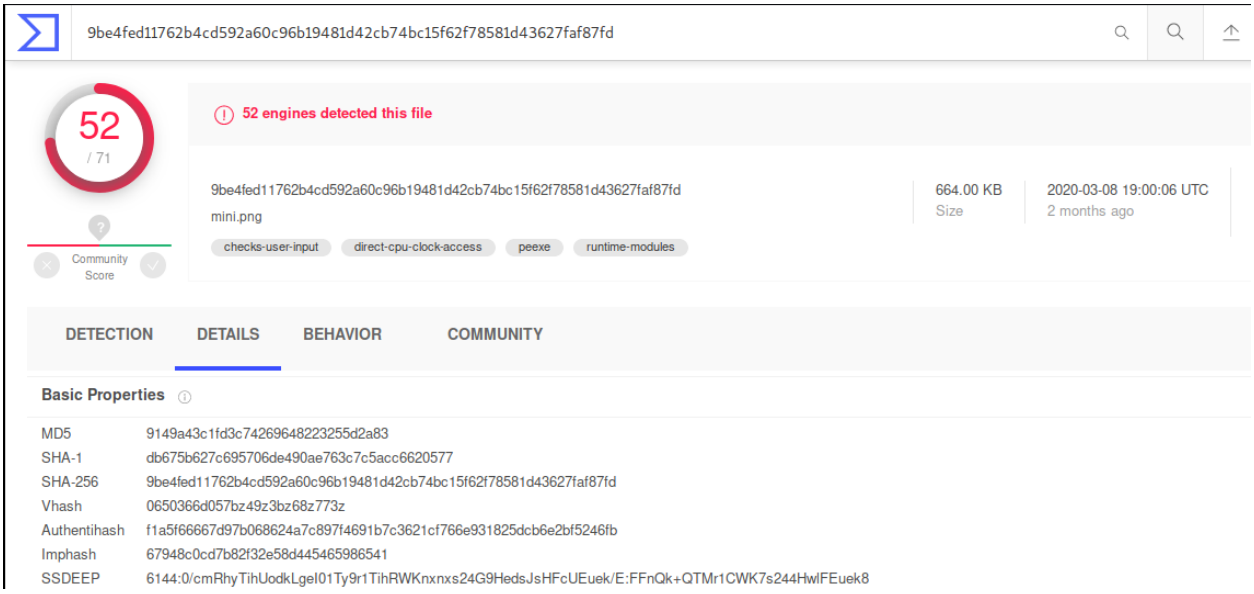
Go to the packet that downloaded this file and we can see that in the hex dump the original filename is visible.

```
·m·1···· ·8·····O
·r·i·g·i ·n·a·l·F
·i·l·e·n ·a·m·e··
·m·1··e ·x·e····
·PADDING XXPADDIN
GPADDING XXPADDIN
```

Flag: m1.exe



For this one we will upload the file to virustotal, you can drag and drop the file onto the vt homepage and it will either analyze the file or take us to the results of the file that has already been analyzed.



ImpHash is listed on this page

Flag: 67948c0cd7b82f32e58d445465986541

Jester 4

50

What is the file description of lastimg.png?

For this we need to examine the pe file, but we cannot just view the flag easily, I tried cyberchef, file command, and exif. I finally had luck with pev and the tool pestr.

It might be tough to see but we see a line that reads FileDescription and right after that is our flag.

```
CompanyName
King Dev Enterprise
FileDescription
Add faded text to your programs with ease!
LegalCopyright
Copyright
 1998 - 99 Dev Enterprise
ProductName
Dev Fade
FileVersion
1.1.0.69
ProductVersion
1.1.0.69
InternalName
OriginalFilename
m1.exe
root@kali:/home/kali/5ctf/jester# pestr lastimg.exe
```

Flag: Add faded text to your programs with ease!

Jester 5

80

Those downloads look nasty, but the intrusion seems to predate the download. What is the IP address of the networks gateway's WAN interface?

For this one we can look at DNS queries and we see that there are requests for myexternalip.com at packet 3814.

dns

No.	Time	Source	Destination	Protocol	Length	Info
7	0.168545	10.22.33.145	10.22.33.1	DNS	70	Standard query 0xae66 A google.com
8	0.200701	10.22.33.1	10.22.33.145	DNS	86	Standard query response 0xae66 A google.com A 172.217.1.238
25	0.351762	10.22.33.145	10.22.33.1	DNS	74	Standard query 0x89ae A www.google.com
26	0.388273	10.22.33.1	10.22.33.145	DNS	90	Standard query response 0x89ae A www.google.com A 172.217.9.132
1449	531.136391	10.22.33.145	10.22.33.1	DNS	70	Standard query 0x8569 A ipecho.net
1451	531.163278	10.22.33.1	10.22.33.145	DNS	134	Standard query response 0x8569 A ipecho.net A 216.239.38.21 A 216.239.32.21 A…
1587	590.962353	10.22.33.145	10.22.33.1	DNS	92	Standard query 0xf523 A 112.146.166.173.zen.spamhaus.org
1588	591.000998	10.22.33.1	10.22.33.145	DNS	108	Standard query response 0xf523 A 112.146.166.173.zen.spamhaus.org A 127.0.0.10
3814	2333.957212	10.22.33.145	10.22.33.1	DNS	76	Standard query 0xdb75 A myexternalip.com
3816	2333.979333	10.22.33.1	10.22.33.145	DNS	140	Standard query response 0xdb75 A myexternalip.com A 216.239.36.21 A 216.239.3…
3911	2373.316670	10.22.33.145	10.22.33.1	DNS	92	Standard query 0x99fb A 112.146.166.173.zen.spamhaus.org
3912	2373.349255	10.22.33.1	10.22.33.145	DNS	108	Standard query response 0x99fb A 112.146.166.173.zen.spamhaus.org A 127.0.0.10

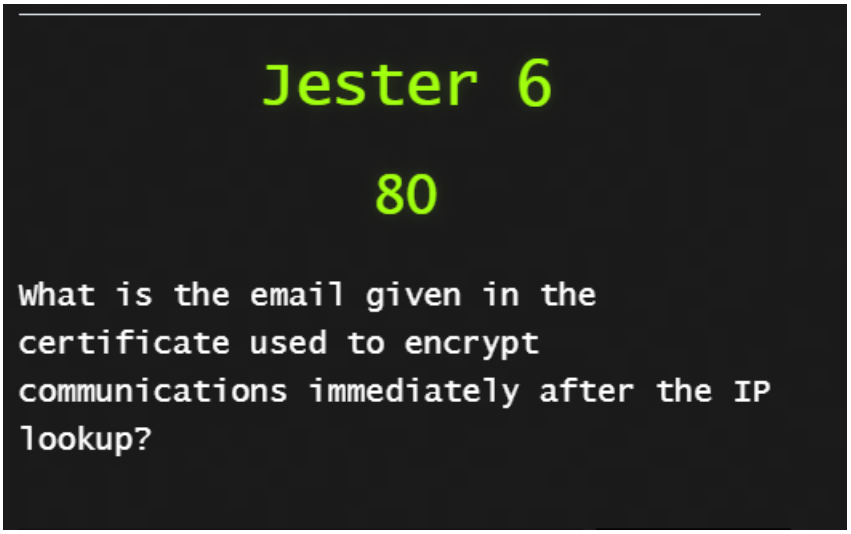
Then the http response to this is at packet 3822, and in this packet there is a text/html response of 173.166.146.112 which is our flag

3813	2333.912285	85.143.216.206	10.22.33.145	TLSv1.2	469	Application Data
3814	2333.957212	10.22.33.145	10.22.33.1	DNS	76	Standard query 0xdb75 A myexternalip.com
3815	2333.972205	10.22.33.145	85.143.216.206	TCP	54	49703 → 443 [ACK] Seq=467 Ack=2051 Win=63825 Len=0
3816	2333.979333	10.22.33.1	10.22.33.145	DNS	140	Standard query response 0xdb75 A myexternalip.com A 216.239.36.2
3817	2333.983000	10.22.33.145	216.239.36.21	TCP	66	49704 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
3818	2334.005152	216.239.36.21	10.22.33.145	TCP	58	80 → 49704 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
3819	2334.005480	10.22.33.145	216.239.36.21	TCP	54	49704 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
3820	2334.005841	10.22.33.145	216.239.36.21	HTTP	148	GET /raw HTTP/1.1
3821	2334.005953	216.239.36.21	10.22.33.145	TCP	54	80 → 49704 [ACK] Seq=1 Ack=95 Win=64240 Len=0
3822	2334.055935	216.239.36.21	10.22.33.145	HTTP	451	HTTP/1.1 200 OK (text/html)
3823	2334.057989	10.22.33.145	85.143.216.206	TLSv1.2	360	Application Data
3824	2334.058119	85.143.216.206	10.22.33.145	TCP	54	443 → 49703 [ACK] Seq=2051 Ack=773 Win=64240 Len=0
3825	2334.097543	10.22.33.145	216.239.36.21	TCP	54	49704 → 80 [ACK] Seq=95 Ack=398 Win=63843 Len=0
3826	2343.507861	85.143.216.206	10.22.33.145	TLSv1.2	1439	Application Data

```
X-Frame-Options: DENY\r\n
X-XSS-Protection: 1; mode=block\r\n
X-Content-Type-Options: nosniff\r\n
Referrer-Policy: strict-origin-when-cross-origin\r\n
Via: 1.1 google\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.050094000 seconds]
[Request in frame: 3820]
[Request URI: http://myexternalip.com/raw]
File Data: 15 bytes
Line-based text data: text/html (1 lines)
173.166.146.112
```

```
0170  65 66 65 72 72 65 72 2d  50 6f 6c 69 63 79 3a 20   eferrer- Policy:
0180  73 74 72 69 63 74 2d 6f  72 69 67 69 6e 2d 77 68   strict-o rigin-wh
0190  65 6e 2d 63 72 6f 73 73  2d 6f 72 69 67 69 6e 0d   en-cross -origin·
01a0  0a 56 69 61 3a 20 31 2e  31 20 67 6f 6f 67 6c 65   ·Via: 1. 1 google
01b0  0d 0a 0d 0a 31 37 33 2e  31 36 36 2e 31 34 36 2e   ····173. 166.146.
01c0  31 31 32                                           112
```

Flag: 173.166.146.112

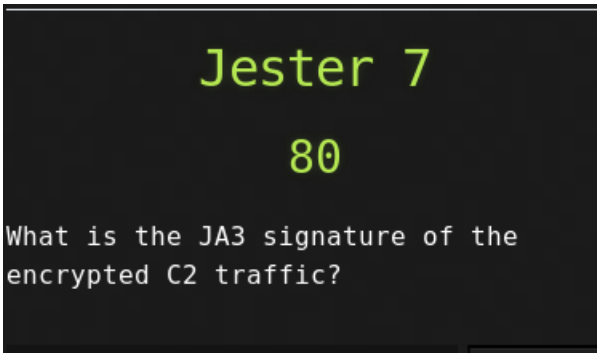


We want to look at the initial client hello packets for the conversation which happing in packet 3715

No.	Time	Source	Destination	Protocol	Length	Info
3712	1996.778789	10.22.33.145	45.138.72.155	TCP	54	49882 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
3713	1996.779468	10.22.33.145	45.138.72.155	TLSv1.2	206	Client Hello
3714	1996.779638	45.138.72.155	10.22.33.145	TCP	54	443 → 49882 [ACK] Seq=1 Ack=153 Win=64240 Len=0
3715	1997.003424	45.138.72.155	10.22.33.145	TLSv1.2	1442	Server Hello, Certificate
3716	1997.004216	45.138.72.155	10.22.33.145	TLSv1.2	164	Server Key Exchange, Server Hello Done
3717	1997.004514	10.22.33.145	45.138.72.155	TCP	54	49882 → 443 [ACK] Seq=153 Ack=1499 Win=64240 Len=0
3718	1997.006538	10.22.33.145	45.138.72.155	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
3719	1997.006641	45.138.72.155	10.22.33.145	TCP	54	443 → 49882 [ACK] Seq=1499 Ack=279 Win=64240 Len=0

```
    Length: 1080
  ▾ Handshake Protocol: Certificate
      Handshake Type: Certificate (11)
      Length: 1076
      Certificates Length: 1073
    ▾ Certificates (1073 bytes)
        Certificate Length: 1070
      ▾ Certificate: 3082042a30820312a003020102020250ef300d06092a8648… (pkcs-9-at-emailAddress=root@everettg3vc59m20.mskhost.pro,id-at-commonName=everettg3vc59m20.ms
        ▾ signedCertificate
            version: v3 (2)
            serialNumber: 20719
          ▸ signature (sha256WithRSAEncryption)
          ▾ issuer: rdnSequence (0)
            ▾ rdnSequence: 7 items (pkcs-9-at-emailAddress=root@everettg3vc59m20.mskhost.pro,id-at-commonName=everettg3vc59m20.mskhost.pro,id-at-organizationalUni
              ▸ RDNSequence item: 1 item (id-at-countryName=--)
              ▸ RDNSequence item: 1 item (id-at-stateOrProvinceName=SomeState)
              ▸ RDNSequence item: 1 item (id-at-localityName=SomeCity)
              ▸ RDNSequence item: 1 item (id-at-organizationName=SomeOrganization)
              ▸ RDNSequence item: 1 item (id-at-organizationalUnitName=SomeOrganizationalUnit)
              ▸ RDNSequence item: 1 item (id-at-commonName=everettg3vc59m20.mskhost.pro)
              ▸ RDNSequence item: 1 item (pkcs-9-at-emailAddress=root@everettg3vc59m20.mskhost.pro)
          ▸ validity
          ▸ subject: rdnSequence (0)
          ▸ subjectPublicKeyInfo
          ▸ extensions: 2 items
        ▸ algorithmIdentifier (sha256WithRSAEncryption)
          Padding: 0
```

Flag: root@everettg3vc59m20.mskhost.pro

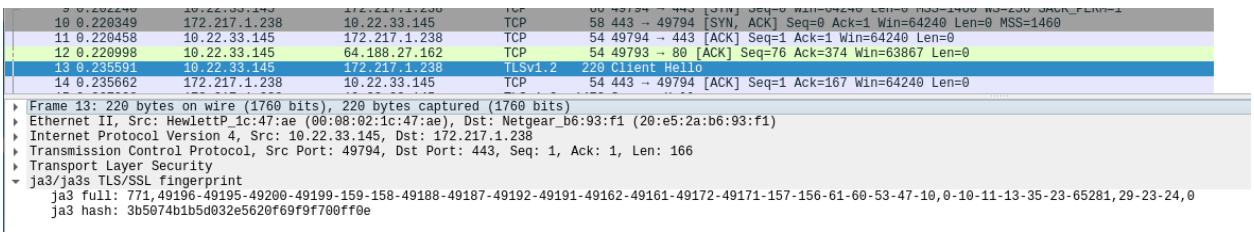


For this I needed to install a couple of LUAs in to wireshark, and here are the commands I ran from the following folder: /root/.local/lib/wireshark/plugins/3.2

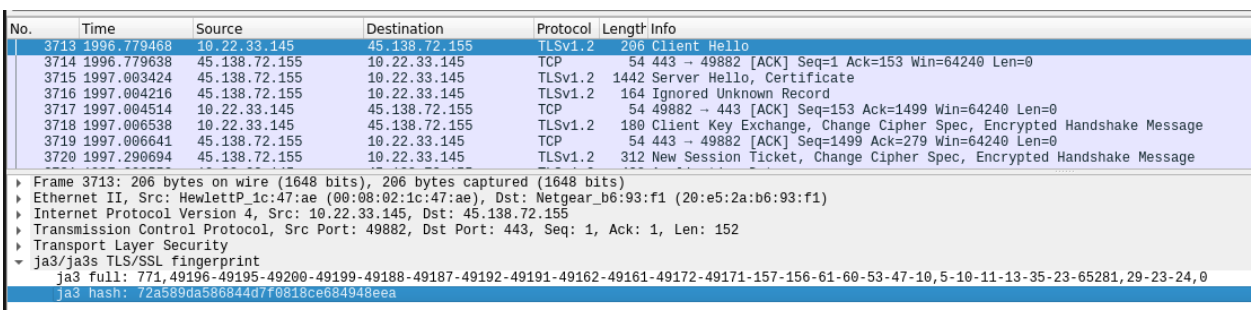
git clone https://github.com/fullylegit/ja3

git clone https://github.com/kikito/md5.lua

After running these commands restart wireshark and look at a hello packet to find an JA3 field



Next we need to look at packet 3715 to get the JA3 and our flag.



Flag: 72a589da586844d7f0818ce684948eea