

Week2

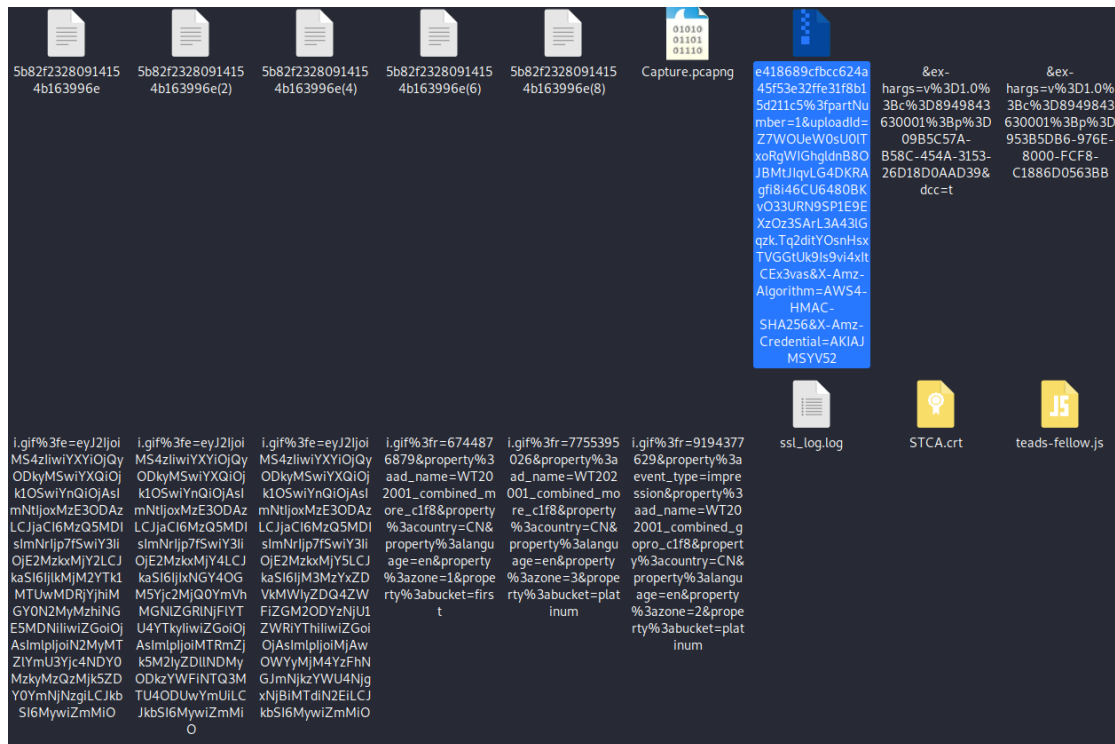
Misc1

下载得到包和 ssl

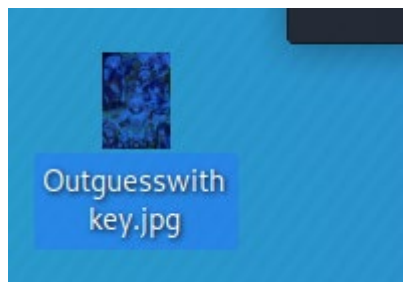
打开包并利用 ssllog 解密

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help					
Apply a display filter ... <Ctrl-/>					
No.	Time	Source	Destination	Protocol	Length Info
1231	20.499240	52.19.199.93	192.168.146.132	HTTP	561 HTTP/1.1 200 OK (text/plain)
1232	20.501999	192.168.146.132	52.19.199.93	TLSv1.2	1887 [TLS segment of a reassembled PDU]
1233	20.502112	192.168.146.132	52.19.199.93	HTTP	999 POST /com.snowplowanalytics.snowplow/tp2 HTTP/1.1 (appl
1234	20.502182	52.19.199.93	192.168.146.132	TCP	60 443 → 49202 [ACK] Seq=5847 Ack=3687 Win=64240 Len=0
1235	20.502292	52.19.199.93	192.168.146.132	TCP	60 443 → 49202 [ACK] Seq=5847 Ack=4632 Win=64240 Len=0
1236	20.551776	52.19.199.93	192.168.146.132	TLSv1.2	105 Change Cipher Spec, Finished
1237	20.552508	192.168.146.132	18.233.176.127	TCP	66 49205 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SAC
1238	20.597432	192.168.146.132	210.58.200.238	TCP	66 [TCP Retransmission] 49201 → 443 [SYN] Seq=0 Win=8192 Le
1239	20.652280	52.19.199.93	192.168.146.132	TCP	105 [TCP Retransmission] 443 → 49203 [PSH, ACK] Seq=5289 Ack
1240	20.652302	192.168.146.132	52.19.199.93	TCP	54 49203 → 443 [ACK] Seq=644 Ack=5340 Win=62997 Len=0
1241	20.811841	18.233.176.127	192.168.146.132	TCP	60 443 → 49205 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1
1242	20.811897	192.168.146.132	18.233.176.127	TCP	54 49205 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1243	20.812418	192.168.146.132	18.233.176.127	TLSv1.2	571 Client Hello
1244	20.812596	18.233.176.127	192.168.146.132	TCP	60 443 → 49205 [ACK] Seq=1 Ack=518 Win=64240 Len=0
1245	21.071412	18.233.176.127	192.168.146.132	TLSv1.2	1494 Server Hello
1246	21.090517	52.19.199.93	192.168.146.132	HTTP	561 HTTP/1.1 200 OK (text/plain)
1247	21.171975	18.233.176.127	192.168.146.132	TCP	1494 [TCP Retransmission] 443 → 49205 [PSH, ACK] Seq=1 Ack=51
1248	21.171999	192.168.146.132	18.233.176.127	TCP	54 49205 → 443 [ACK] Seq=518 Ack=1441 Win=62800 Len=0
1249	21.190892	52.19.199.93	192.168.146.132	TCP	66 [TCP Retransmission] 443 → 49202 [PSH, ACK] Seq=5847 Ack
1250	21.190931	192.168.146.132	52.19.199.93	TCP	54 49202 → 443 [ACK] Seq=4632 Ack=6354 Win=63175 Len=0
1251	21.614885	192.168.146.132	224.0.0.251	MDNS	82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" q
1252	21.652944	18.233.176.127	192.168.146.132	TCP	60 443 → 49204 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1
1253	21.652990	192.168.146.132	18.233.176.127	TCP	54 49204 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1254	21.653668	192.168.146.132	18.233.176.127	TLSv1.2	571 Client Hello
1255	21.653844	18.233.176.127	192.168.146.132	TCP	60 443 → 49204 [ACK] Seq=1 Ack=518 Win=64240 Len=0
▶ Frame 1231: 561 bytes on wire (4488 bits), 561 bytes captured (4488 bits) on interface \Device\NPF_{2E17BD68-F3FB-4025-A802-400A7DD3}					
▶ Ethernet II, Src: VMware_ee:45:16 (00:50:56:ee:45:16), Dst: VMware_47:56:08 (00:0c:29:47:56:08)					
▶ Internet Protocol Version 4, Src: 52.19.199.93, Dst: 192.168.146.132					
▶ Transmission Control Protocol, Src Port: 443, Dst Port: 49202, Seq: 5340, Ack: 2654, Len: 507					
▶ Transport Layer Security					
▼ Hypertext Transfer Protocol					
▶ HTTP/1.1 200 OK\r\n					
Access-Control-Allow-Credentials: true\r\n					
Access-Control-Allow-Origin: https://wettransfer.com\r\n					
Content-Type: text/plain; charset=UTF-8\r\n					
Date: Sat, 18 Jan 2020 12:58:13 GMT\r\n					
Server: Apache/2.4.18 (Ubuntu)					

因为提示图片，所以在文件里下载了所有的 http 传输的文件



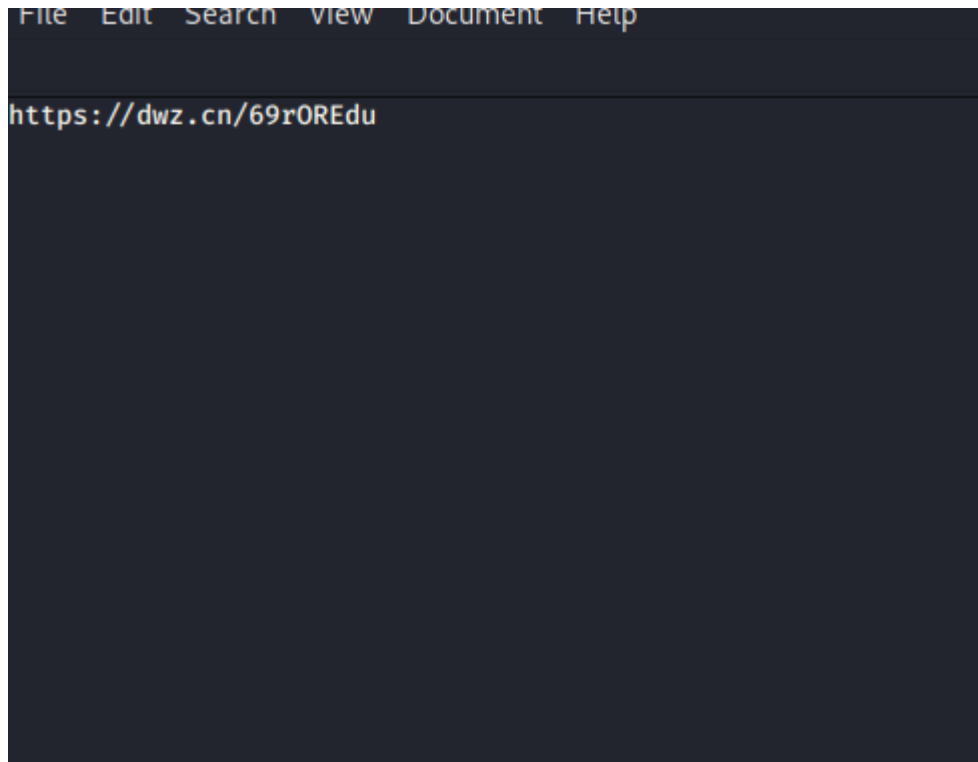
得到一些文件，这个文件的标志是压缩包，说明这是一个压缩包，解开得到图片



通过提示找到备注的 key

用 outguess 隐写解开

得到网址



进入网址得到二维码，然后扫码二维码得到 flag

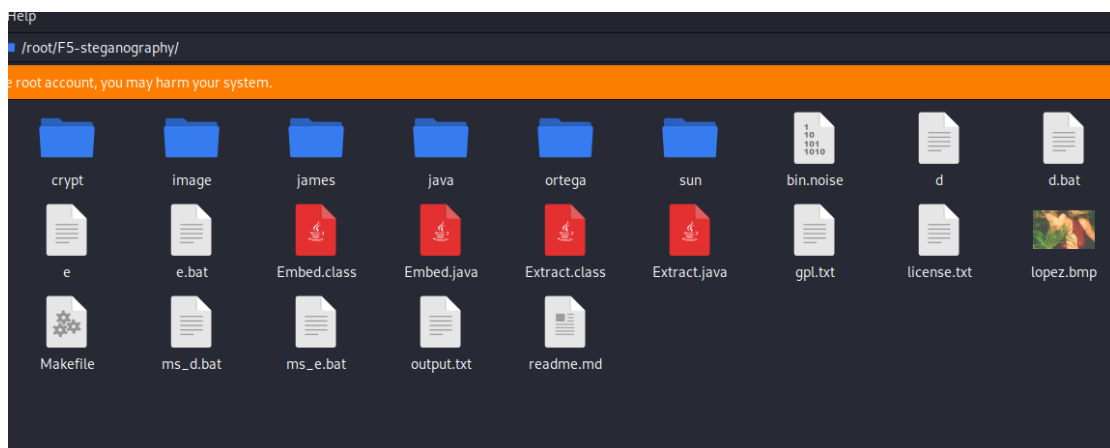
Misc2

下载压缩包并打开得到

名称	大小	压缩后大小	类型	修改时间	CRC32	
..			文件夹			
FLAG_IN_PICTURE.jpg *	1,067,904	1,064,702	JPG 文件	2020/1/20 15:28	4709DF1E	F5 key: N11d7CQon6dBsFLz

F5key 查了百度之后推测是用 f5 算法的图片隐写

然后在 kail 中 git clone 了 f5 的解码器



然后在这里用命令解包

```
File Edit Search View Document Help
/root/.ssh-steganography/output.txt - Mousepad
Warning, you are using the root account, you may harm your system.
j26172211a0701003392b5e50a0105060005010180000009327AE2402030BA70004A70020C85B0C2000000008666C6162E7478740A03029A006C65DFCED501686701606578343038375E7A2360737733344552746E46557971704855683264604C505736307D1D77565181050400
```

Output 里输出了字符观察发现是 16 进制的

用 16 进制转字符串，得到 flag。