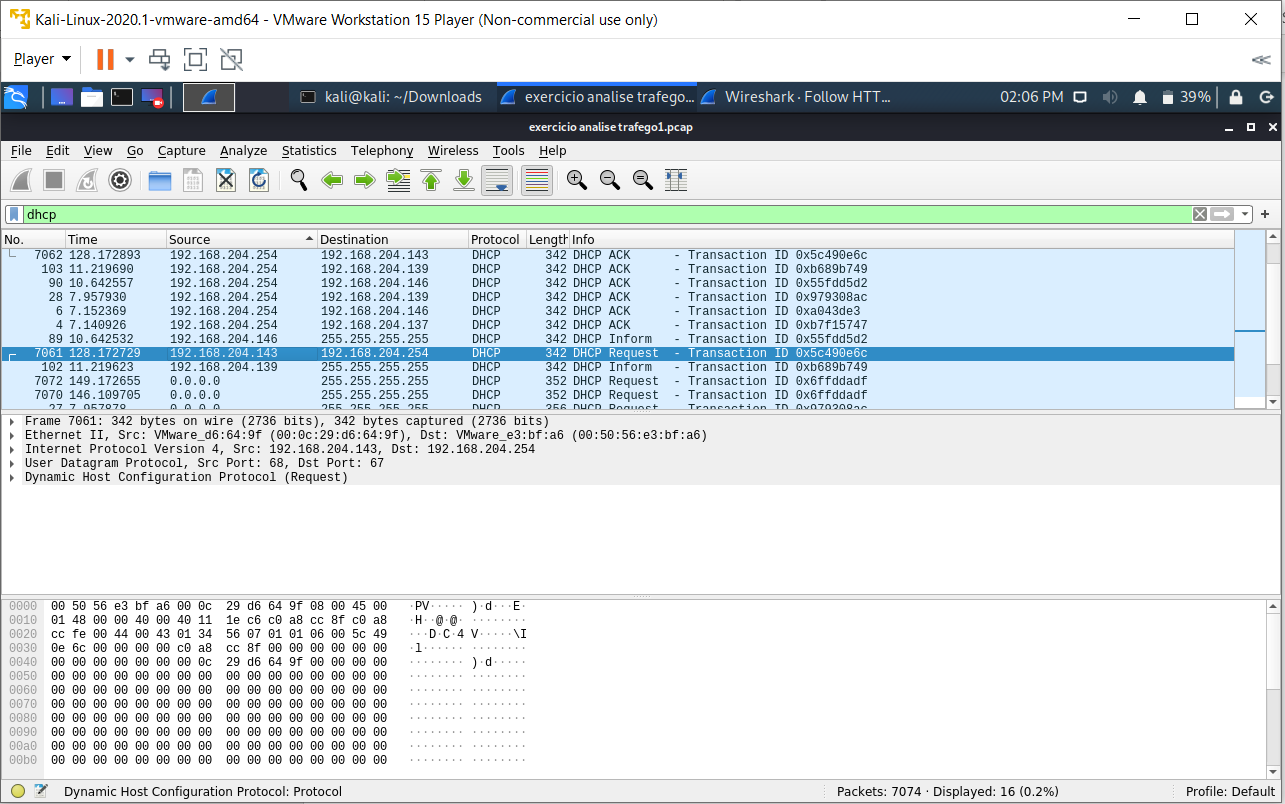
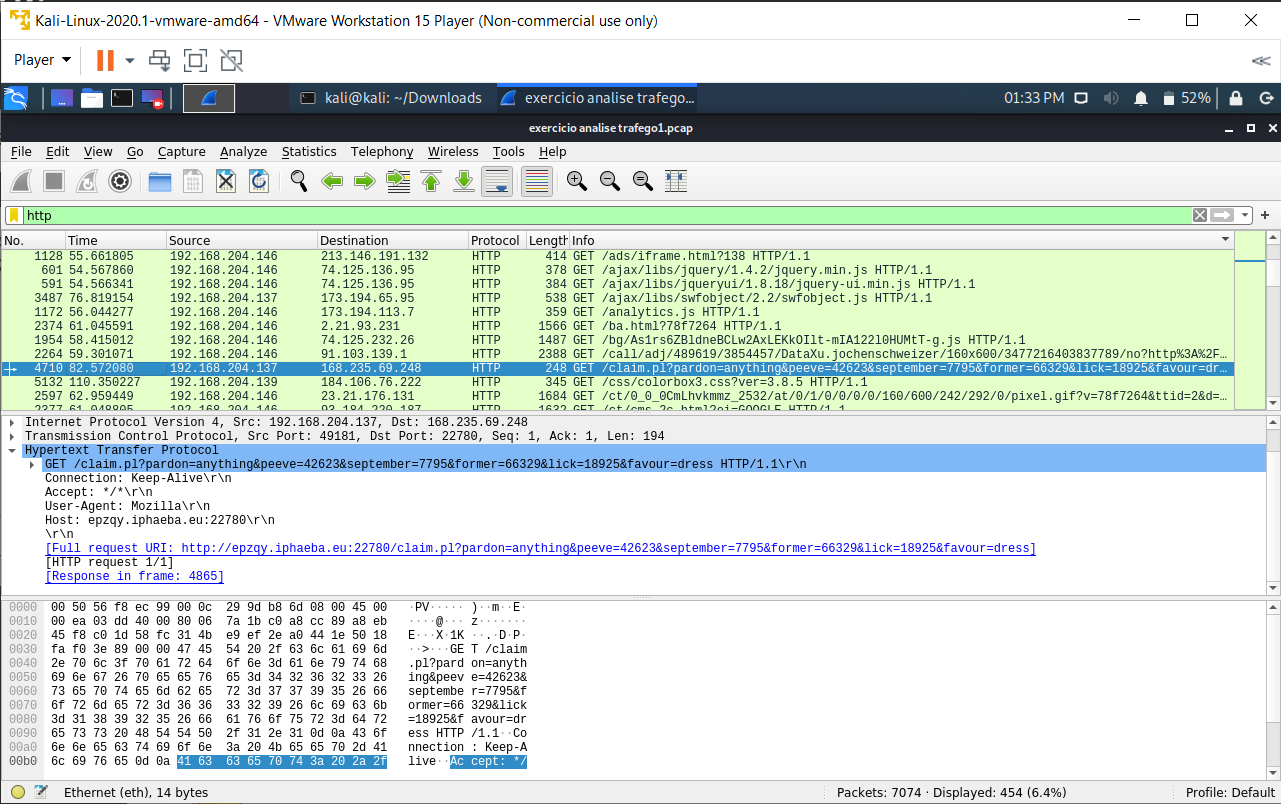
**Capturas de tela:**

* **Hosts Windows:**



* **Conexão suspeita:**



Primeiramente, a porta em que a conexão foi estabelecida não é a padrão da comunicacão http. Em Segundo lugar, o tipo de conexão estabelecida foi “keep-alive”, uma configuracão de conexão persistente perigosa e que não deveria ser usada:

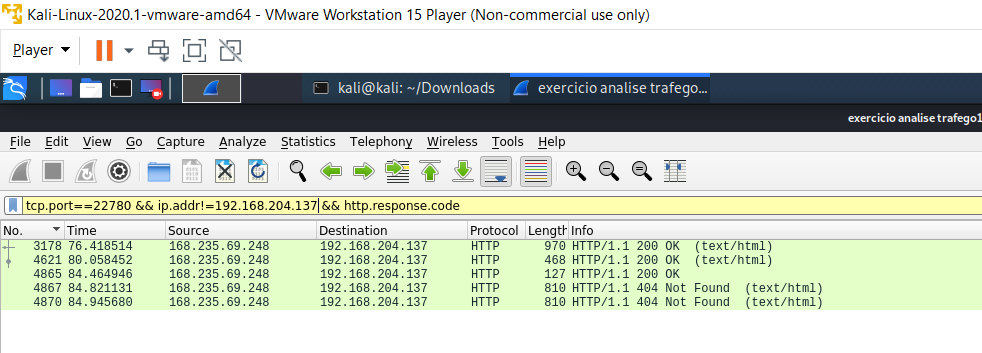
*“However, HTTP/1.1 clients (and HTTP/1.1 proxies acting as clients) MUST NOT send Keep-Alive: to a proxy (of any version), because of the danger that an HTTP/1.0 proxy will forward it improperly.*

*Instead, HTTP/1.1 clients (and HTTP/1.1 proxies acting as clients) wishing for a persistent connection should send:*

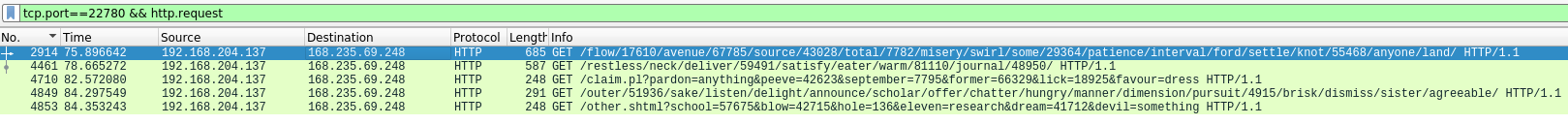
*Persist: <name of server or proxy>”*

Dada a descoberta do ip, fui atrás de outras comunicações estabelecidas pela mesma conexão maliciosa:

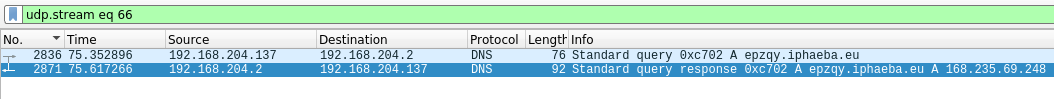
Resposta da maquina infectada:

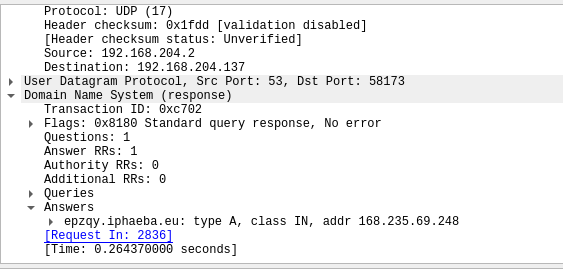


Requests da conexão maliciosa:

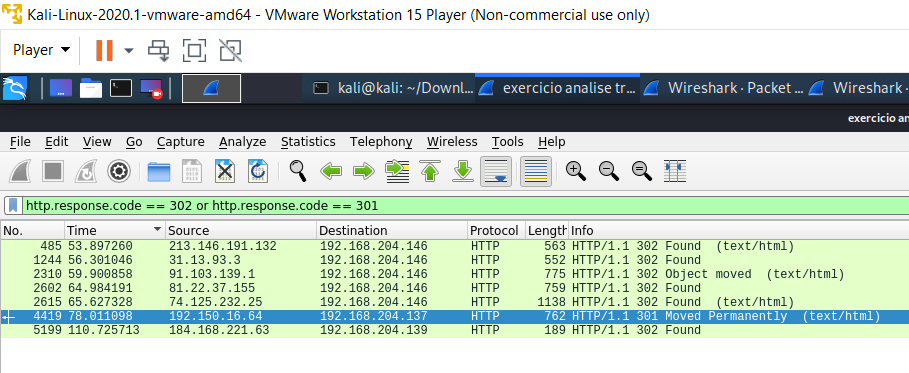


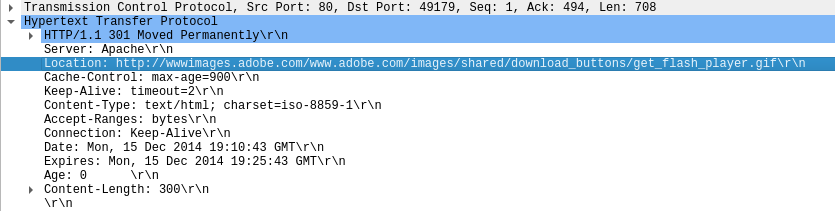
De maneira a encontrar o endereço de IP atrelado ao domínio de site infectado, foi preciso pesquisar pelas comunicações de DNS feita pela conexão maliciosa e procurar pelo domínio encontrado anteriormente:

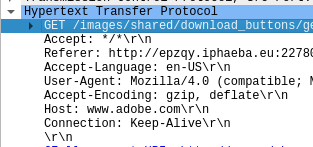




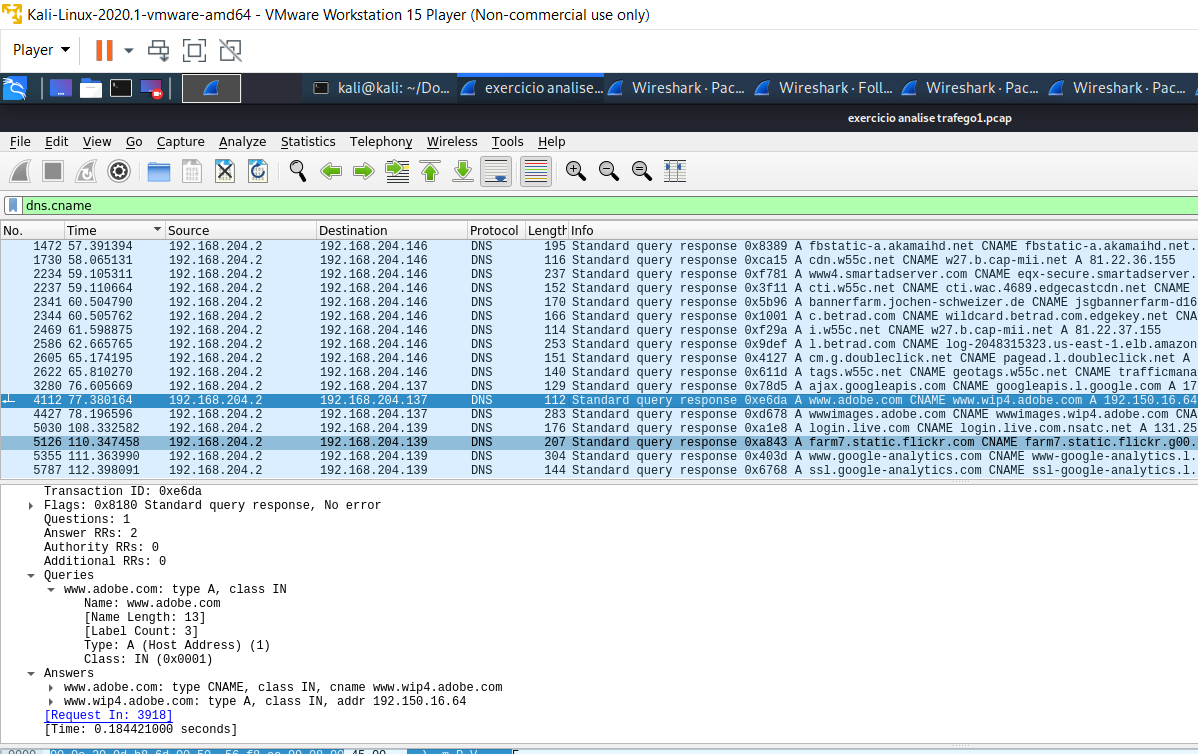
Achando a url que agiu como redirecionamento entre os sites comprometidos:







Descobrindo o IP da URL de redirecionamento:



1.2 a) Hosts windows:

1. 192.168.204.146, MAC: 00:0c:29:fc:bc:2e, TTL: 128, OS: Windows.
2. 192.168.204.139, MAC: 00:0c:29:61:c1:89, TTL:128, OS: Windows.
3. 192.168.204.137, MAC: 00:0c:29:9d:b8:6d, TTL: 128, OS: Windows.

1.2 b) O endereco de ip do host do windows e 192.168.204.137.

1.2 c)

http://epzqy.iphaeba.eu:22780/restless/neck/deliver/59491/satisfy/eater/warm/81110/journal/48950/

<http://epzqy.iphaeba.eu:22780/other.shtml?school=57675&blow=42715&hole=136&eleven=research&dream=41712&devil=something>

http://epzqy.iphaeba.eu:22780/claim.pl?pardon=anything&peeve=42623&september=7795&former=66329&lick=18925&favour=dress

<http://epzqy.iphaeba.eu:22780/outer/51936/sake/listen/delight/announce/scholar/offer/chatter/hungry/manner/dimension/pursuit/4915/brisk/dismiss/sister/agreeable/>

<http://epzqy.iphaeba.eu:22780/other.shtml?school=57675&blow=42715&hole=136&eleven=research&dream=41712&devil=something>

1.2 d) O endereço de IP do site comprometido é:

epzqy.iphaeba.eu: type A, class IN, addr **168.235.69.248**

1.2 e) A url que agiu como um redirecionamento foi [www.adobe.com](http://www.adobe.com)

1.2 f)O IP da URL de redirecionamento é 192.150.16.64