

Using Wireshark to Examine HTTP and HTTPS Traffic

Apriamo la VM, e nella console diamo il comando ip address

```
[analyst@sec0ps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:f3:12:a7 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 86328sec preferred_lft 86328sec
    inet6 fe80::a00:27ff:fef3:12a7/64 scope link
        valid_lft forever preferred_lft forever
[analyst@sec0ps ~]$
```

Ora diamo il comando sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap

```
[analyst@sec0ps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```


Il comando registra il traffico sull'interfaccia enp0s3

Andiamo ora sul sito <http://www.altoromutual.com/login.jsp> e inseriamo admin e admin come credenziali

Online Banking Login

Username:

Password:

This connection is not secure.
 Logins entered here could be compromised. [Learn More](#)

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details:

800000 Corporate ▼

GO

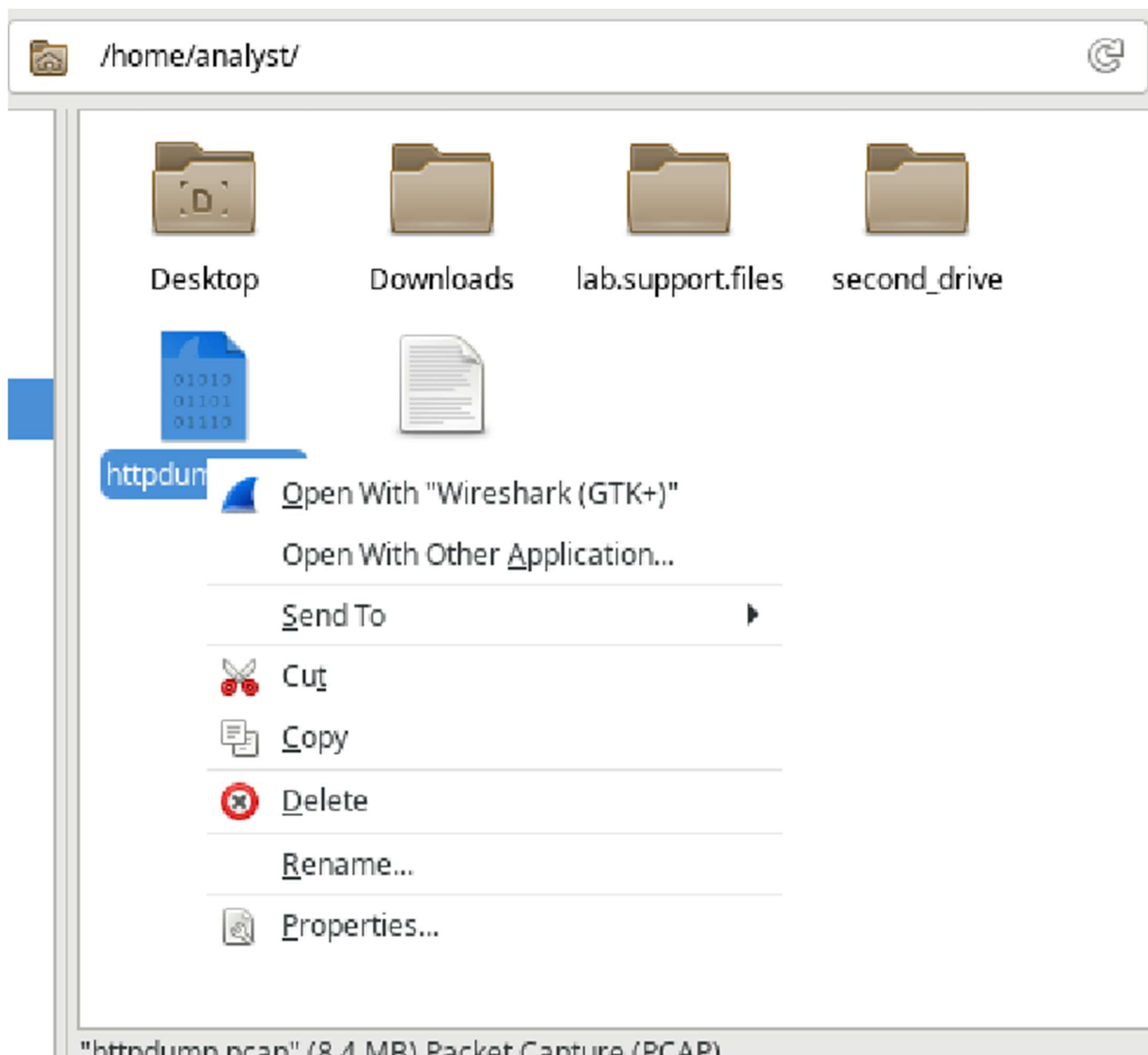
Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!

Click [Here](#) to apply.

Riceviamo un avviso sulla connessione non sicura, ma noi effettuiamo l'accesso, torniamo sul prompt e blocchiamo la cattura del traffico.

Navighiamo nella cartella base, apriamo il file con wireshark:



Filtriamo il traffico con http, cerchiamo il POST e controlliamo la voce HTML Form URL Encoded, troviamo le credenziali di accesso:

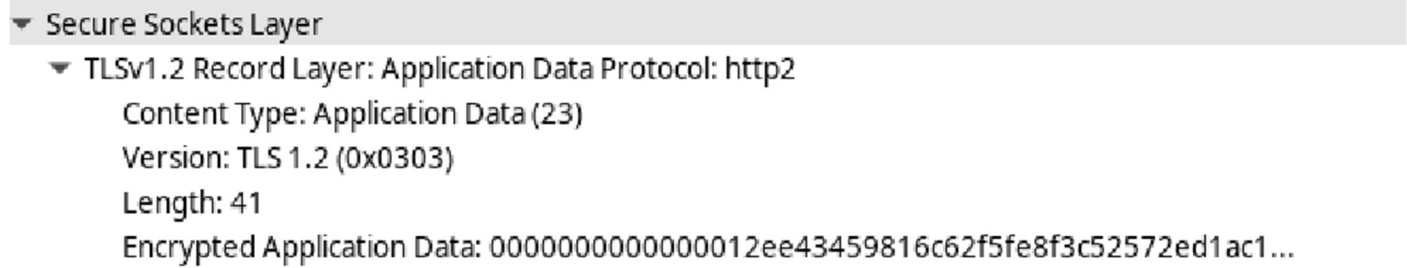
3538	116.455891	10.0.2.15	65.61.137.117	HTTP	589	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
3542	116.599309	65.61.137.117	10.0.2.15	HTTP	307	HTTP/1.1 302 Found
▶ Frame 3538: 589 bytes on wire (4712 bits), 589 bytes captured (4712 bits)						
▶ Ethernet II, Src: PcsCompu_f3:12:a7 (08:00:27:f3:12:a7), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)						
▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 65.61.137.117						
▶ Transmission Control Protocol, Src Port: 41442, Dst Port: 80, Seq: 1, Ack: 1, Len: 535						
▶ Hypertext Transfer Protocol						
▼ HTML Form URL Encoded: application/x-www-form-urlencoded						
▶ Form item: "uid" = "admin"						
▶ Form item: "passw" = "admin"						
▶ Form item: "btnSubmit" = "Login"						

Lanciamo ora `sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap`

```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Navighiamo ora su un sito HTTPS, per comodità scelgo google. Fatto l'accesso chiudo di nuovo il processo e carico il file su wireshark. Imposto il filtro tcp.port==443, e cerco Application Data come messaggio

Nella sezione inferiore troviamo la sezione del TLS



▼ Secure Sockets Layer

- ▼ TLSv1.2 Record Layer: Application Data Protocol: http2
 - Content Type: Application Data (23)
 - Version: TLS 1.2 (0x0303)
 - Length: 41
 - Encrypted Application Data: 00000000000000012ee43459816c62f5fe8f3c52572ed1ac1...

Il formato è cryptato e non può essere letto