**Relazione Schematica: Utilizzo di Wireshark per Esaminare il Traffico HTTP e HTTPS**

**Obiettivo:** Acquisire e analizzare il traffico HTTP e HTTPS utilizzando Wireshark e tcpdump per comprendere le differenze tra comunicazioni non crittografate e crittografate.

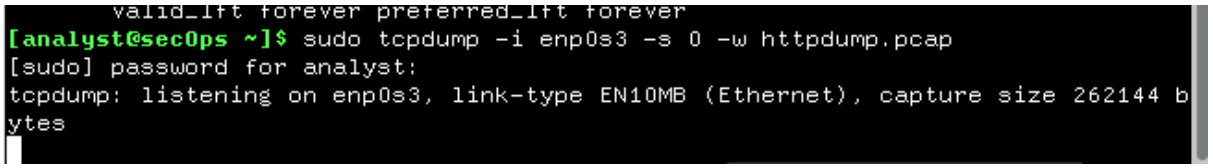
**Parte 1: Acquisizione e Visualizzazione del Traffico HTTP**

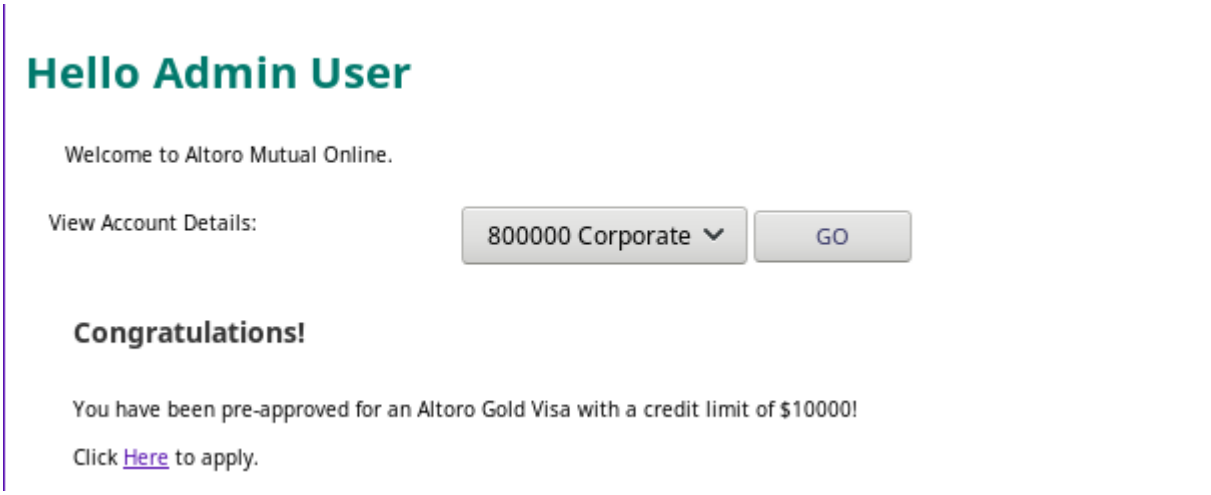
**Passaggio 1: Avvio della Macchina Virtuale e Accesso**

1. Avviare la VM CyberOps Workstation.
2. Accedere con:
    - Nome utente: **analyst**
    - Password: **cyberops**

**Passaggio 2: Acquisizione del Traffico HTTP con tcpdump**

1. Aprire un terminale.
2. Identificare le interfacce con il comando:
    - `ip address`
3. Avviare tcpdump per catturare il traffico HTTP:
    - `sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap`
    - Parametri:
        - `-i` specifica l'interfaccia di acquisizione.
        - `-s 0` imposta la lunghezza dello snapshot al valore massimo.
        - `-w` scrive i pacchetti catturati in un file.
4. Aprire un browser e visitare `http://www.altoromutual.com/login.jsp`.
5. Inserire **Admin** come username e password e cliccare su Login.
6. Chiudere il browser.
7. Tornare al terminale e interrompere tcpdump con `CTRL+C`.

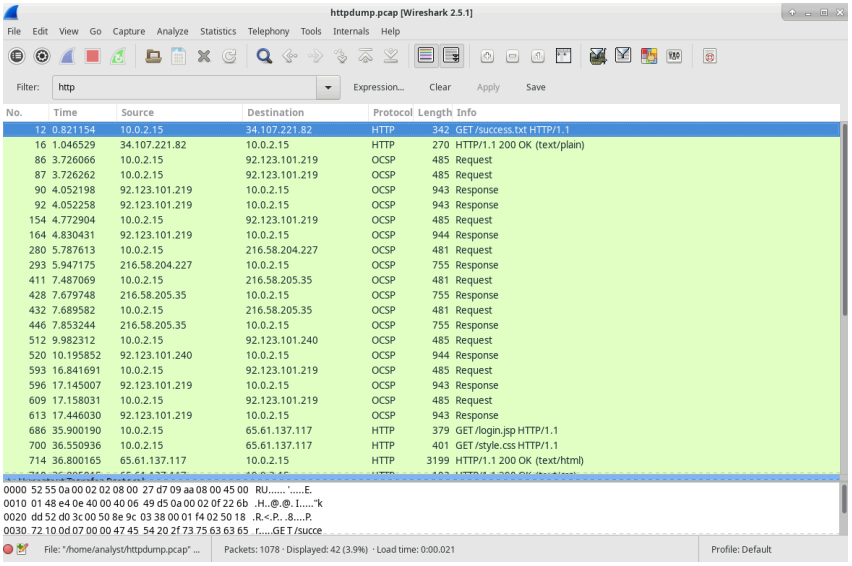


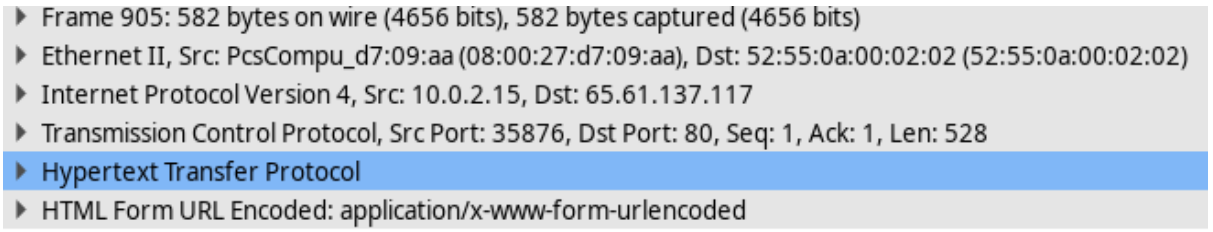


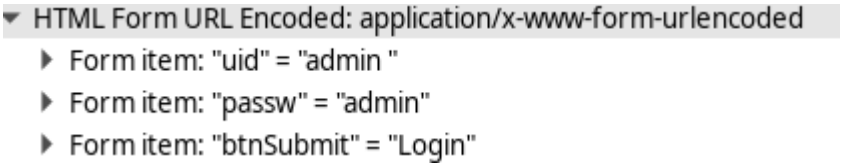

```
analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 b
ytes
^C1078 packets captured
1078 packets received by filter
0 packets dropped by kernel
analyst@secOps ~]$
```

**Passaggio 3: Analisi del Traffico HTTP con Wireshark**

1. Aprire `httpdump.pcap` con Wireshark.
2. Applicare il filtro HTTP.
3. Selezionare un pacchetto **POST**.
4. Espandere la sezione `application/x-www-form-urlencoded`.
5. Identificare:
    - **Username:** Admin
    - **Password:** Admin
6. Chiudere Wireshark.



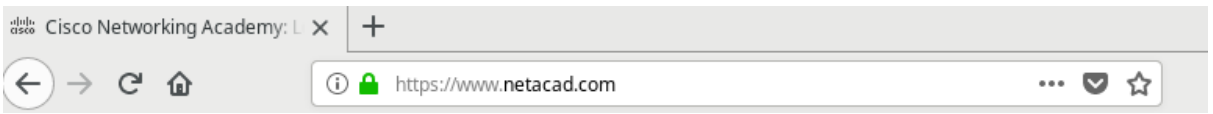



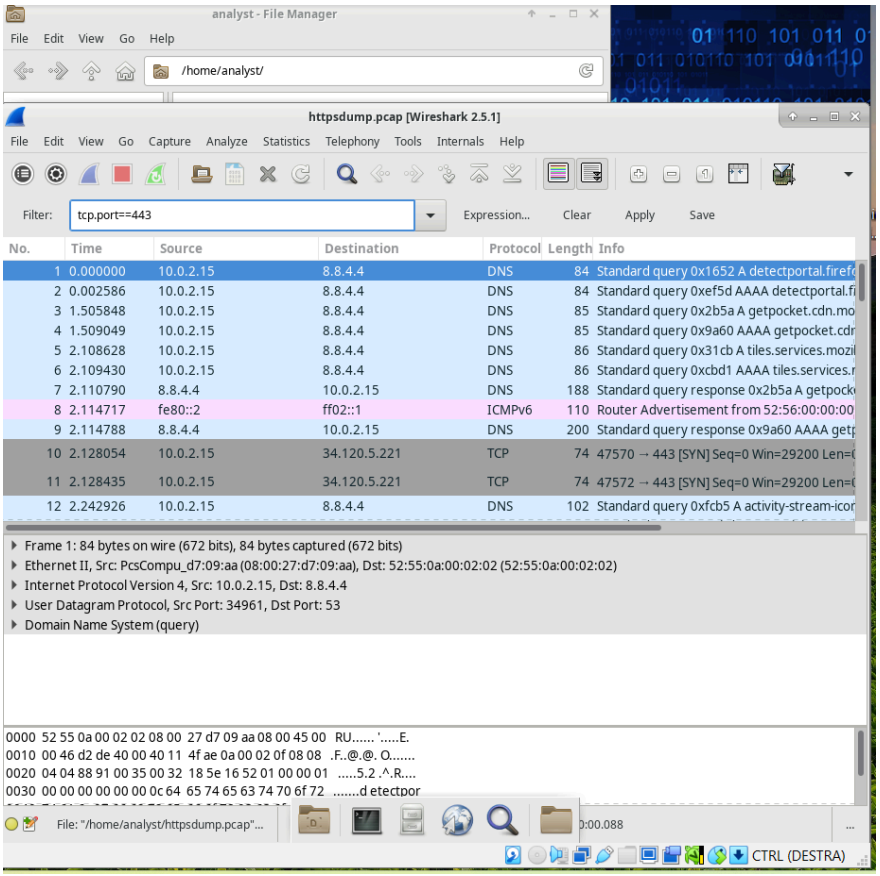



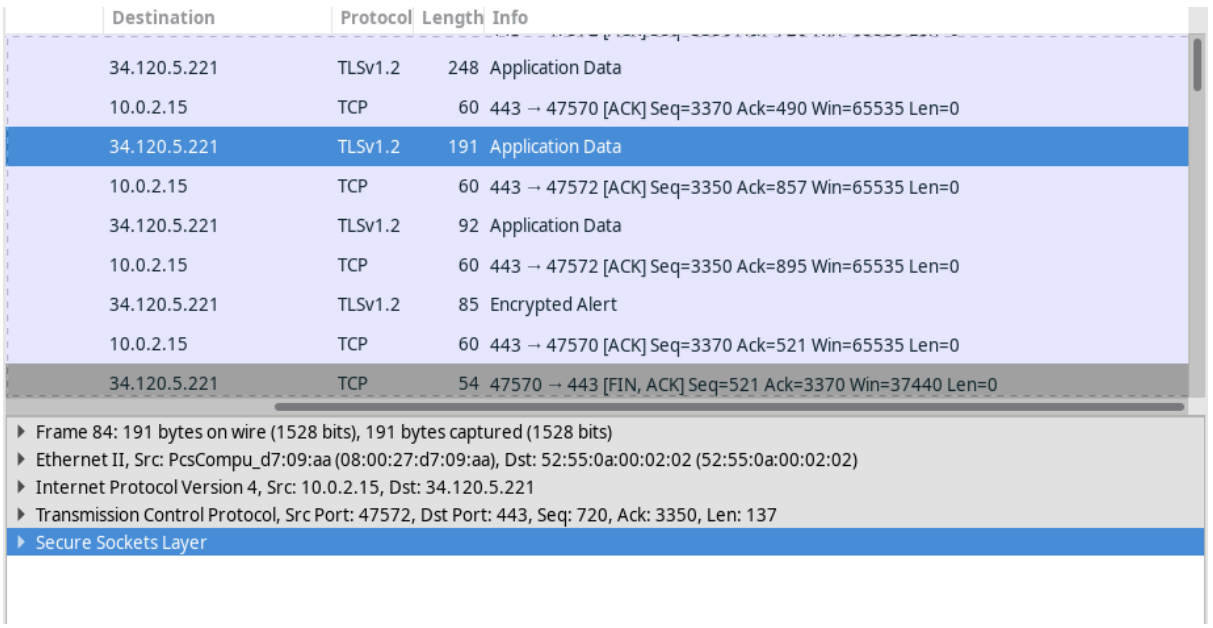

## Parte 2: Acquisizione e Visualizzazione del Traffico HTTPS

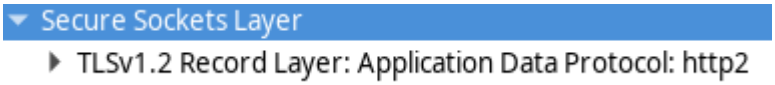
### Passaggio 1: Acquisizione del Traffico HTTPS con tcpdump

1. Aprire un terminale.
2. Avviare tcpdump:
    - `sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap`
3. Aprire un browser e visitare `https://www.netacad.com`.
4. Cliccare su **Accedi** e inserire le credenziali di NetAcad.
5. Chiudere il browser.
6. Tornare al terminale e interrompere tcpdump con `CTRL+C`.


Cisco Networking Academy: L
https://www.netacad.com


analyst - File Manager
File Edit View Go Help
/home/analyst/
httpsdump.pcap [Wireshark 2.5.1]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp.port==443
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
1 0.000000 10.0.2.15 8.8.4.4 DNS 84 Standard query 0x1652 A detectportal.firefo
2 0.002586 10.0.2.15 8.8.4.4 DNS 84 Standard query 0xef5d AAAA detectportal.fi
3 1.505848 10.0.2.15 8.8.4.4 DNS 85 Standard query 0x2b5a A getpocket.cdn.mo
4 1.509049 10.0.2.15 8.8.4.4 DNS 85 Standard query 0x9a60 AAAA getpocket.cdn
5 2.108628 10.0.2.15 8.8.4.4 DNS 86 Standard query 0x31cb A tiles.services.mozil
6 2.109430 10.0.2.15 8.8.4.4 DNS 86 Standard query 0xcbd1 AAAA tiles.services.m
7 2.110790 8.8.4.4 10.0.2.15 DNS 188 Standard query response 0x2b5a A getpock
8 2.114717 fe80::2 ff02::1 ICMPv6 110 Router Advertisement from 52:56:00:00:00
9 2.114788 8.8.4.4 10.0.2.15 DNS 200 Standard query response 0x9a60 AAAA getp
10 2.128054 10.0.2.15 34.120.5.221 TCP 74 47570 → 443 [SYN] Seq=0 Win=29200 Len=0
11 2.128435 10.0.2.15 34.120.5.221 TCP 74 47572 → 443 [SYN] Seq=0 Win=29200 Len=0
12 2.242926 10.0.2.15 8.8.4.4 DNS 102 Standard query 0xfcb5 A activity-stream-icon
Frame 1: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
Ethernet II, Src: PcsCompu_d7:09:aa (08:00:27:d7:09:aa), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 8.8.4.4
User Datagram Protocol, Src Port: 34961, Dst Port: 53
Domain Name System (query)
0000 52 55 0a 00 02 02 08 00 27 d7 09 aa 08 00 45 00 RU..... '.....E.
0010 00 46 d2 de 40 00 40 11 4f ae 0a 00 02 0f 08 08 .F..@.@. O.....
0020 04 04 88 91 00 35 00 32 18 5e 16 52 01 00 00 01 .....5.2 .^.R....
0030 00 00 00 00 00 00 0c 64 65 74 65 63 74 70 6f 72 .....d etectpor
File: "/home/analyst/httpsdump.pcap"...
CTRL (DESTRA)


Destination Protocol Length Info
34.120.5.221 TLSv1.2 248 Application Data
10.0.2.15 TCP 60 443 → 47570 [ACK] Seq=3370 Ack=490 Win=65535 Len=0
34.120.5.221 TLSv1.2 191 Application Data
10.0.2.15 TCP 60 443 → 47572 [ACK] Seq=3350 Ack=857 Win=65535 Len=0
34.120.5.221 TLSv1.2 92 Application Data
10.0.2.15 TCP 60 443 → 47572 [ACK] Seq=3350 Ack=895 Win=65535 Len=0
34.120.5.221 TLSv1.2 85 Encrypted Alert
10.0.2.15 TCP 60 443 → 47570 [ACK] Seq=3370 Ack=521 Win=65535 Len=0
34.120.5.221 TCP 54 47570 → 443 [FIN, ACK] Seq=521 Ack=3370 Win=37440 Len=0
Frame 84: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits)
Ethernet II, Src: PcsCompu_d7:09:aa (08:00:27:d7:09:aa), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 34.120.5.221
Transmission Control Protocol, Src Port: 47572, Dst Port: 443, Seq: 720, Ack: 3350, Len: 137
Secure Sockets Layer




**Passaggio 2: Analisi del Traffico HTTPS con Wireshark**

1. Aprire `httpsdump.pcap` con Wireshark.
2. Applicare il filtro `tcp.port==443`.
3. Selezionare un pacchetto di dati dell'applicazione.
4. Identificare la sostituzione della sezione HTTP con **SSL/TLS 1.2**.
5. Espandere la sezione **Secure Sockets Layer**.
6. Notare che i dati dell'applicazione sono crittografati e non leggibili.
7. Chiudere Wireshark e spegnere la macchina virtuale.