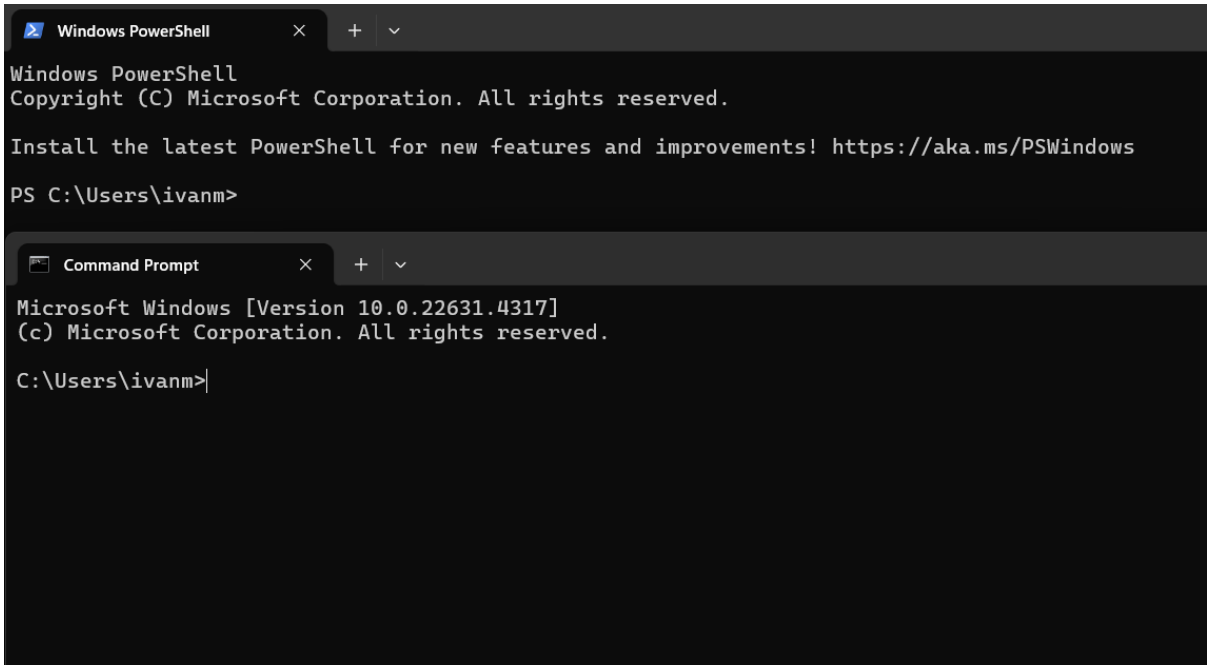
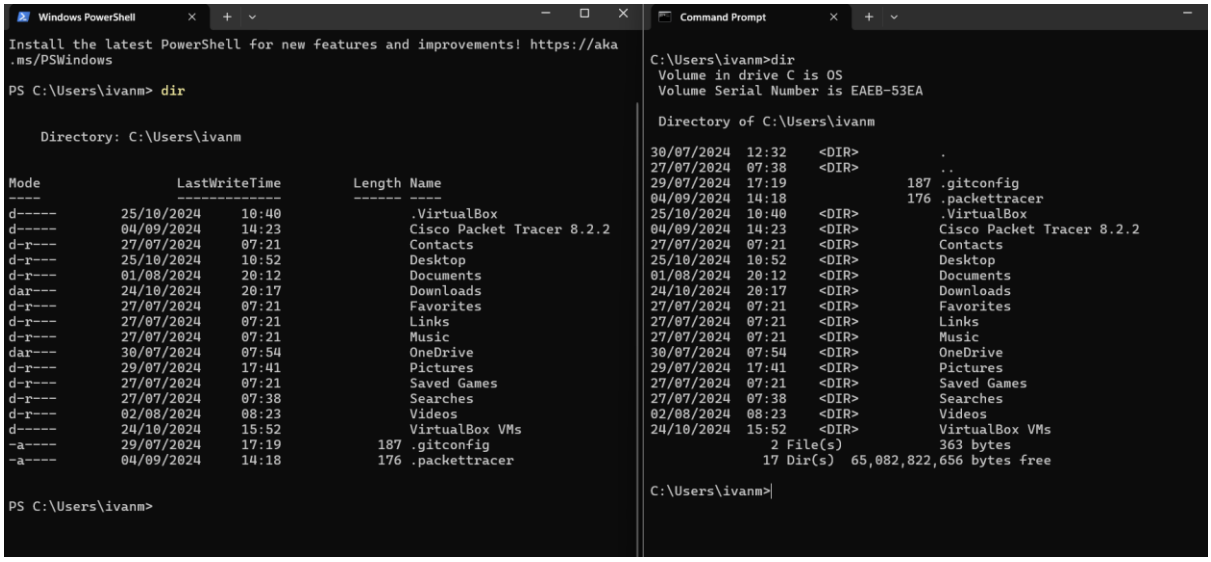
Consegna Venerdì 25 Ottobre 2024

Lab 1: Windows Power Shell

Seguendo la traccia, iniziamo aprendo il prompt di PowerShell e del terminale su una macchina Windows.



Eseguiamo il commando 'dir' su entrambi i terminali.



Successivamente eseguiamo il comnado 'ipconfig', di nuovo su entrambi i terminali, osservando che l'output risulta molto simile.

```
PS C:\Users\ivanm> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::fc36:c03c:66fa:4c77%19
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter WiFi:

   Connection-specific DNS Suffix  . : wind3.hub
   Link-local IPv6 Address . . . . . : fe80::ef29:9b2c:9d1f:602d%18
   IPv4 Address. . . . . . . . . . . : 192.168.1.179
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
PS C:\Users\ivanm>
```

```
C:\Users\ivanm>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::fc36:c03c:66fa:4c77%19
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter WiFi:

   Connection-specific DNS Suffix  . : wind3.hub
   Link-local IPv6 Address . . . . . : fe80::ef29:9b2c:9d1f:602d%18
   IPv4 Address. . . . . . . . . . . : 192.168.1.179
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\ivanm>
```

Spostandoci ora sul terminale di PowerShell, inseriamo il comando ‘Get-Alias dir’ per mostrare file e sottodirectory presenti.

```
PS C:\Users\ivanm> Get-Alias dir

CommandType     Name                                               Version
-----------     ----                                               -------
Alias           dir -> Get-ChildItem


PS C:\Users\ivanm>
```

Sempre sul terminale di PowerShell, inserimao il comando ‘netstat -h’ per vedere le opzioni disponibili per il comando ‘netstat’.

```
PS C:\Users\ivanm> netstat -h

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-i] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

  -a            Displays all connections and listening ports.
  -b            Displays the executable involved in creating each connection or
                listening port. In some cases well-known executables host
                multiple independent components, and in these cases the
                sequence of components involved in creating the connection
                or listening port is displayed. In this case the executable
                name is in [] at the bottom, on top is the component it called,
                and so forth until TCP/IP was reached. Note that this option
                can be time-consuming and will fail unless you have sufficient
                permissions.
  -e            Displays Ethernet statistics. This may be combined with the -s
                option.
  -f            Displays Fully Qualified Domain Names (FQDN) for foreign
                addresses.
  -i            Displays the time spent by a TCP connection in its current state.
  -n            Displays addresses and port numbers in numerical form.
  -o            Displays the owning process ID associated with each connection.
  -p proto      Shows connections for the protocol specified by proto; proto
                may be any of: TCP, UDP, TCPv6, or UDPv6.  If used with the -s
                option to display per-protocol statistics, proto may be any of:
                IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
  -q            Displays all connections, listening ports, and bound
                nonlistening TCP ports. Bound nonlistening ports may or may not
                be associated with an active connection.
  -r            Displays the routing table.
  -s            Displays per-protocol statistics.  By default, statistics are
                shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
                the -p option may be used to specify a subset of the default.
  -t            Displays the current connection offload state.
  -x            Displays NetworkDirect connections, listeners, and shared
                endpoints.
  -y            Displays the TCP connection template for all connections.
                Cannot be combined with the other options.
  interval      Redisplays selected statistics, pausing interval seconds
```

Quello che ci interessa in questo esercizio è lo switch -r, che mostra la routing table.

```
PS C:\Users\ivanm> netstat -r
===========================================================================
Interface List
 19...0a 00 27 00 00 13 ......VirtualBox Host-Only Ethernet Adapter
  8...22 0b 74 76 56 3e ......Microsoft Wi-Fi Direct Virtual Adapter
  3...22 0b 74 76 46 2e ......Microsoft Wi-Fi Direct Virtual Adapter #2
 18...20 0b 74 76 76 1e ......MediaTek Wi-Fi 6E MT7902 Wireless LAN Card
 15...20 0b 74 76 76 1f ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1    192.168.1.179     35
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.1.0    255.255.255.0         On-link     192.168.1.179    291
    192.168.1.179  255.255.255.255         On-link     192.168.1.179    291
    192.168.1.255  255.255.255.255         On-link     192.168.1.179    291
     192.168.56.0    255.255.255.0         On-link      192.168.56.1    281
     192.168.56.1  255.255.255.255         On-link      192.168.56.1    281
   192.168.56.255  255.255.255.255         On-link      192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link     192.168.1.179    291
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      192.168.56.1    281
  255.255.255.255  255.255.255.255         On-link     192.168.1.179    291
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
 19    281 fe80::/64                On-link
 18    291 fe80::/64                On-link
 18    291 fe80::ef29:9b2c:9d1f:602d/128
                                    On-link
 19    281 fe80::fc36:c03c:66fa:4c77/128
                                    On-link
  1    331 ff00::/8                 On-link
 19    281 ff00::/8                 On-link
 18    291 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
PS C:\Users\ivanm> |
```

Vediamo, come richiesto, il gateway.

```
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1    192.168.1.179     35
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
```

Apriamo ora un altro terminale PowerShell con i priviliegi di amministratore.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32>
```

Usiamo il comando ‘netstat -abno’ per mostrare i processi associatei alle connessioni TCP attive.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> netstat -abno

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1564
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       10028
  CDPSvc
 [svchost.exe]
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       1280
 [lsass.exe]
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1096
 Can not obtain ownership information
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       2692
  Schedule
 [svchost.exe]
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       3452
  EventLog
 [svchost.exe]
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       4488
 [spoolsv.exe]
  TCP    0.0.0.0:49674          0.0.0.0:0              LISTENING       1220
 Can not obtain ownership information
  TCP    127.0.0.1:6463         0.0.0.0:0              LISTENING       29660
 [Discord.exe]
  TCP    127.0.0.1:24830        0.0.0.0:0              LISTENING       4
```

Andiamo poi a trovare il PID (Process identifier) relativo ai risultati del comando appena eseguito.

svchost.exe	4892	Running	NETWORK SERVICE	00	3,672 K	x64

Infine, utilizziamo PowerShell per svuotare il cestino con il comando 'clear-recyclebin'.

```
Confirm
Are you sure you want to perform this action?
Performing the operation "Clear-RecycleBin" on target "All of the contents of the Recycle Bin".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

Lab 2: Traffico HTTP e HTTPS con Wireshark

Apriamo un terminale e inseriamo il comando 'ip address' e iniziamo a intercettare il traffico sull'interfaccia enp0s3 con il comando 'sudo tcpdump –i enp0s3 –s 0 –w httpdump.pcap'

```
[analyst@secOps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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: ovs-system: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group defaul
t qlen 1000
    link/ether a6:97:a5:fb:83:71 brd ff:ff:ff:ff:ff:ff
3: s1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1
000
    link/ether 66:56:bc:7f:bf:4f brd ff:ff:ff:ff:ff:ff
4: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:d0:83:7e brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.110/24 brd 192.168.50.255 scope global dynamic enp0s3
       valid_lft 7112sec preferred_lft 7112sec
    inet6 fe80::a00:27ff:fed0:837e/64 scope link
       valid_lft forever preferred_lft forever
```

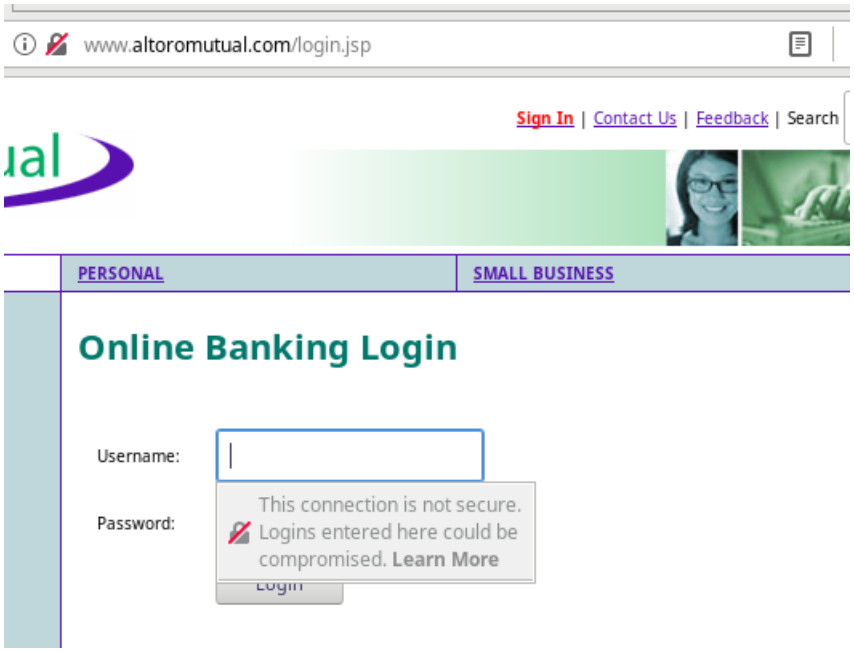
Usiamo il comando 'man tcpdump' per vedere le specifiche degli switch usati.

```
File  Edit  View  Terminal  Tabs  Help
TCPDUMP(1)                General Commands Manual                TCPDUMP(1)

NAME
       tcpdump - dump traffic on a network

SYNOPSIS
       tcpdump [ -AbdDefhHIJKlLnNOpqStuUvxX# ] [ -B buffer_size ]
               [ -c count ]
               [ -C file_size ] [ -G rotate_seconds ] [ -F file ]
               [ -i interface ] [ -j tstamp_type ] [ -m module ] [ -M secret ]
               [ --number ] [ -Q in|out|inout ]
               [ -r file ] [ -V file ] [ -s snaplen ] [ -T type ] [ -w file ]
               [ -W filecount ]
               [ -E spi@ipaddr algo:secret,...  ]
               [ -y datalinktype ] [ -z postrotate-command ] [ -Z user ]
               [ --time-stamp-precision=tstamp_precision ]
               [ --immediate-mode ] [ --version ]
               [ expression ]
```

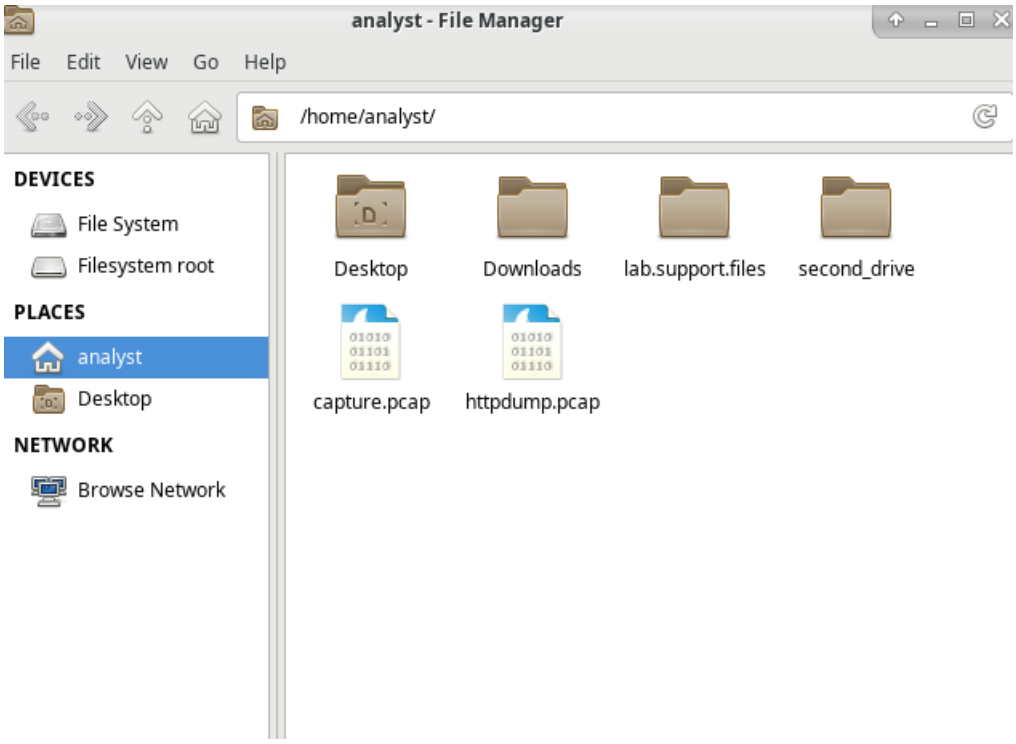
Mentre tcpdump è in esecuzione, apriamo un browser e navighiamo come da consegna al sito http://www.altoromutual.com/login.jsp. Notiamo il messsaggio di avviso che stiamo utilizzando una connessione non sicura.



Dopo esserci loggati con le credenziali 'Admin' e 'Admin', torniamo sul terminale dove abbiamo eseguito tcpdump e lo fermiamo 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
^C9375 packets captured
9383 packets received by filter
0 packets dropped by kernel
```

Andiamo a vedere il file della cattura, salvato come 'httpdump.pcap'.



Apriamo ilo file con Wireshark, filtrando con 'HTTP'.

Filter: http | Expression... | Clear | Apply | Save

No.	Time	Source	Destination	Protocol	Length	Info
8952	70.922071	192.168.50.110	65.61.137.117	HTTP	400	GET /images/logo.gif HTTP/1.1
8953	70.922256	192.168.50.110	65.61.137.117	HTTP	406	GET /images/header_pic.jpg HTTP/1.1
8967	71.070071	192.168.50.110	65.61.137.117	HTTP	403	GET /images/pf_lock.gif HTTP/1.1
8968	71.070588	192.168.50.110	65.61.137.117	HTTP	404	GET /images/gradient.jpg HTTP/1.1
8973	71.075155	65.61.137.117	192.168.50.110	HTTP	2351	HTTP/1.1 200 OK (GIF89a)
8984	71.201696	65.61.137.117	192.168.50.110	HTTP	1974	HTTP/1.1 200 OK (JPEG JFIF image)
8986	71.222041	65.61.137.117	192.168.50.110	HTTP	354	HTTP/1.1 200 OK (GIF89a)
8988	71.222174	65.61.137.117	192.168.50.110	HTTP	1175	HTTP/1.1 200 OK (JPEG JFIF image)
8994	71.268989	192.168.50.110	65.61.137.117	HTTP	408	GET /favicon.ico HTTP/1.1
9000	71.318568	192.168.50.110	65.61.137.117	HTTP	348	GET /favicon.ico HTTP/1.1
9004	71.437024	65.61.137.117	192.168.50.110	HTTP	2651	HTTP/1.1 404 Not Found (text/html)
9010	71.464965	65.61.137.117	192.168.50.110	HTTP	1191	HTTP/1.1 404 Not Found (text/html)
9086	84.084117	192.168.50.110	3.165.245.25	OCSP	494	Request
9092	84.605513	3.165.245.25	192.168.50.110	OCSP	919	Response
9296	139.841167	192.168.50.110	65.61.137.117	HTTP	589	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded
9300	139.983939	65.61.137.117	192.168.50.110	HTTP	278	HTTP/1.1 302 Found
9302	140.003771	192.168.50.110	65.61.137.117	HTTP	569	GET /bank/main.jsp HTTP/1.1
9312	140.158038	65.61.137.117	192.168.50.110	HTTP	508	HTTP/1.1 200 OK (text/html)

- Frame 8: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
- Ethernet II, Src: PcsCompu_d0:83:7e (08:00:27:d0:83:7e), Dst: PcsCompu_ff:e7:03 (08:00:27:ff:e7:03)
- Internet Protocol Version 4, Src: 192.168.50.110, Dst: 34.107.221.82
- Transmission Control Protocol, Src Port: 53492, Dst Port: 80, Seq: 1, Ack: 1, Len: 288
- Hypertext Transfer Protocol

Selezioniamo il messaggio POST ed espandiamo il messaggio HTML per mostrare le credenzilai con cui si è effettuato l'accesso.

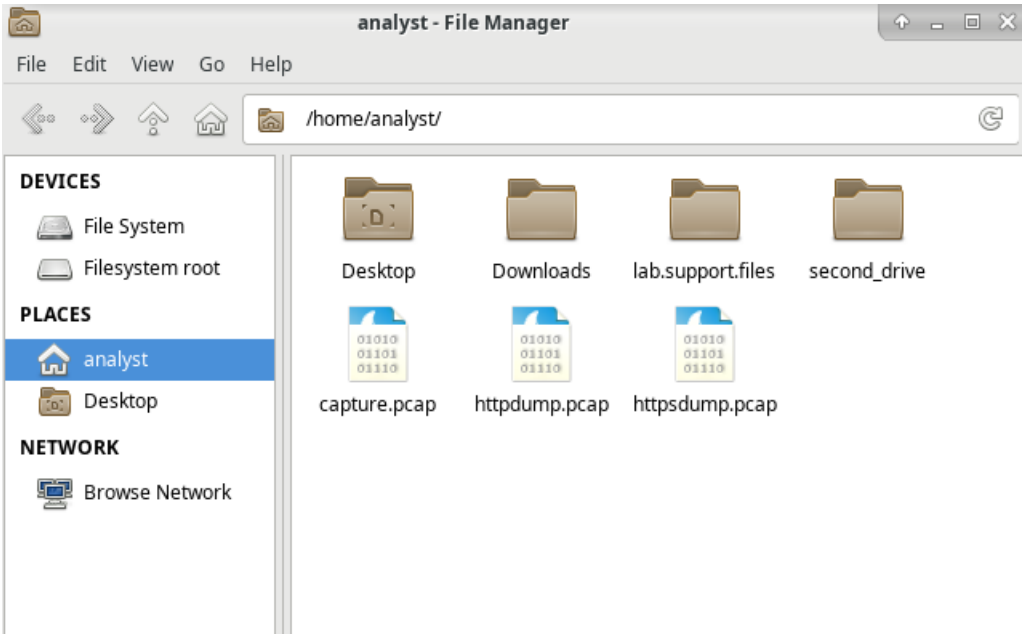
9296	139.841167	192.168.50.110	65.61.137.117	HTTP	589	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded

- Hypertext Transfer Protocol
- HTML Form URL Encoded: application/x-www-form-urlencoded
  - Form item: "uid" = "Admin"
    - Key: uid
    - Value: Admin
  - Form item: "passw" = "Admin"
    - Key: passw
    - Value: Admin

Passiamo adesso al protocollo HTTPS, iniziando con l'eseguire il comando 'sudo tcpdump –i enp0s3 –s 0 –w httpsdump.pcap'. Come prima, andiamo sul browser al sito www.netacad.com, dopodiché torniamo sul terminale e fermiamo la cattura con CTRL+C

```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 b
ytes
^C1234 packets captured
1234 packets received by filter
0 packets dropped by kernel
[analyst@secOps ~]$
```

Troviamo il file 'httpsdump'.



Su Wireshark, applichiamo il filtro per il traffico HTTPS attraverso port 443 inserendo tcp.port==443. Selezionando il messaggio di Application Data, vedendo il messaggio mostrato ed espandendo la sezione del Security Socket Layer.