

Lab – Using Wireshark to Examine HTTP and HTTPS

Objectives

Part 1: Capture and view HTTP traffic

Part 2: Capture and view HTTPS traffic

Background / Scenario

HyperText Transfer Protocol (HTTP) is an application layer protocol that presents data via a web browser. With HTTP, there is no safeguard for the exchanged data between two communicating devices.

With HTTPS, encryption is used via a mathematical algorithm. This algorithm hides the true meaning of the data that is being exchanged. This is done through the use of certificates that can be viewed later in this lab.

Regardless of HTTP or HTTPS, it is only recommended to exchange data with websites that you trust. Just because a site uses HTTPS does not mean it is a trustworthy site. Threat actors commonly use HTTPS to hide their activities.

In this lab, you will explore and capture HTTP and HTTPS traffic using Wireshark.

Required Resources

- CyberOps Workstation VM
- Internet connection

Part 1: Capture and view HTTP traffic

In this part, you will use **tcpdump** to capture the content of HTTP traffic. You will use command options to save the traffic to a packet capture (pcap) file. These records can then be analyzed using different applications that read pcap files, including Wireshark.

Step 1: Start the virtual machine and log in.

Start the CyberOps Workstation VM. Use the following user credentials:

Username: **analyst**

Password: **cyberops**

Step 2: Open a terminal and start tcpdump.

- Open a terminal application and enter the command **ifconfig**.

```
[analyst@secOps ~]$ ifconfig
```

- List the interfaces and their IP addresses displayed in the ifconfig output.

-
- While in the terminal application, enter the command **sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap**. Enter the password **cyberops** for the user analyst when prompted.

```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
```

Lab – Using Wireshark to Examine HTTP and HTTPS

```
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

This command starts tcpdump and records network traffic on the **enp0s3** interface.

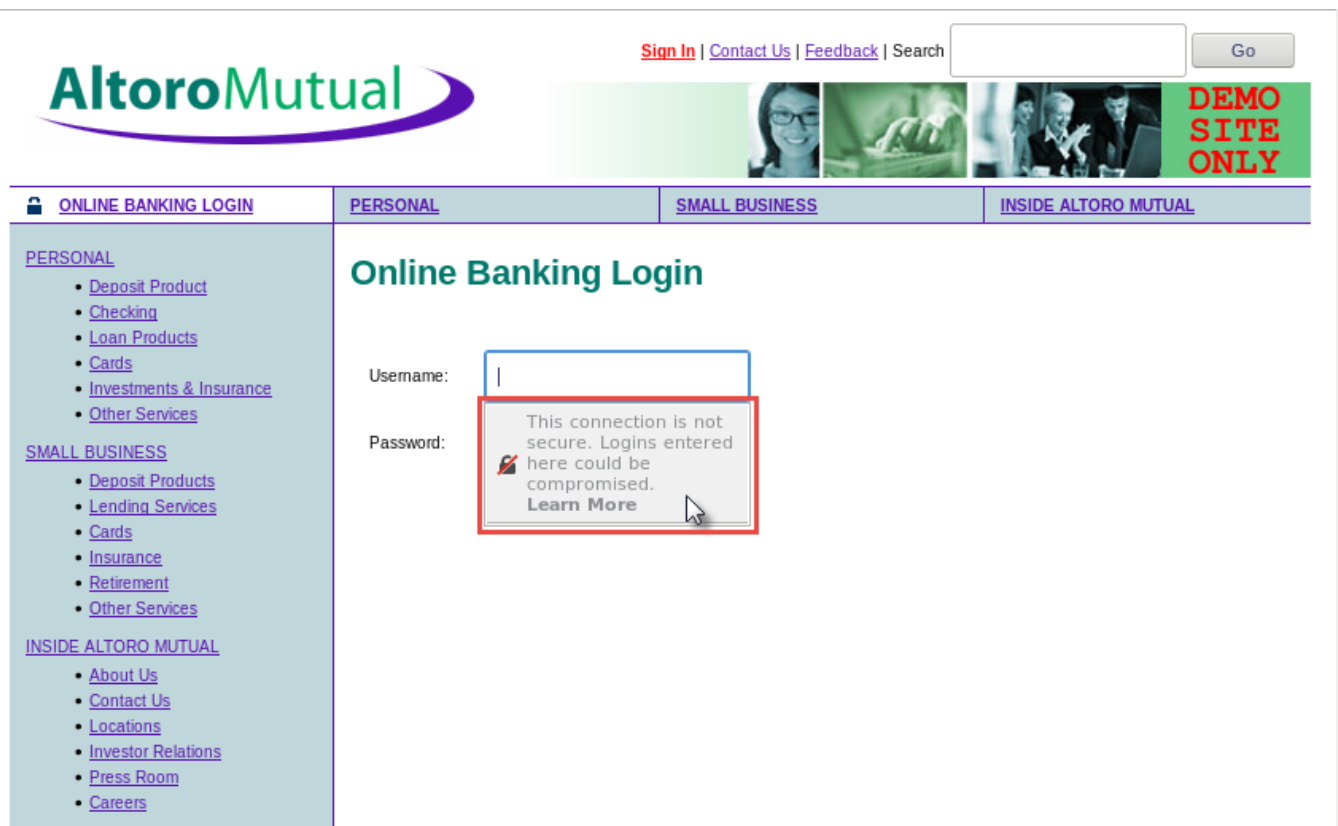
The **-i** command option allows you to specify the interface. If not specified, the tcpdump will capture all traffic on all interfaces.

The **-s** command option specifies the length of the snapshot for each packet. You should limit snaplen to the smallest number that will capture the protocol information in which you are interested. Setting snaplen to 0 sets it to the default of 262144, for backwards compatibility with recent older versions of tcpdump.

The **-w** command option is used to write the result of the tcpdump command to a file. Adding the extension .pcap ensures that operating systems and applications will be able to read to file. All recorded traffic will be printed to the file httpdump.pcap in the home directory of the user analyst.

Use the man pages for tcpdump to determine the usage of the -s and -w command options.

- d. Open a web browser from the launch bar within the Linux Workstation. Navigate to www.altoromutual.com/bank/login.aspx



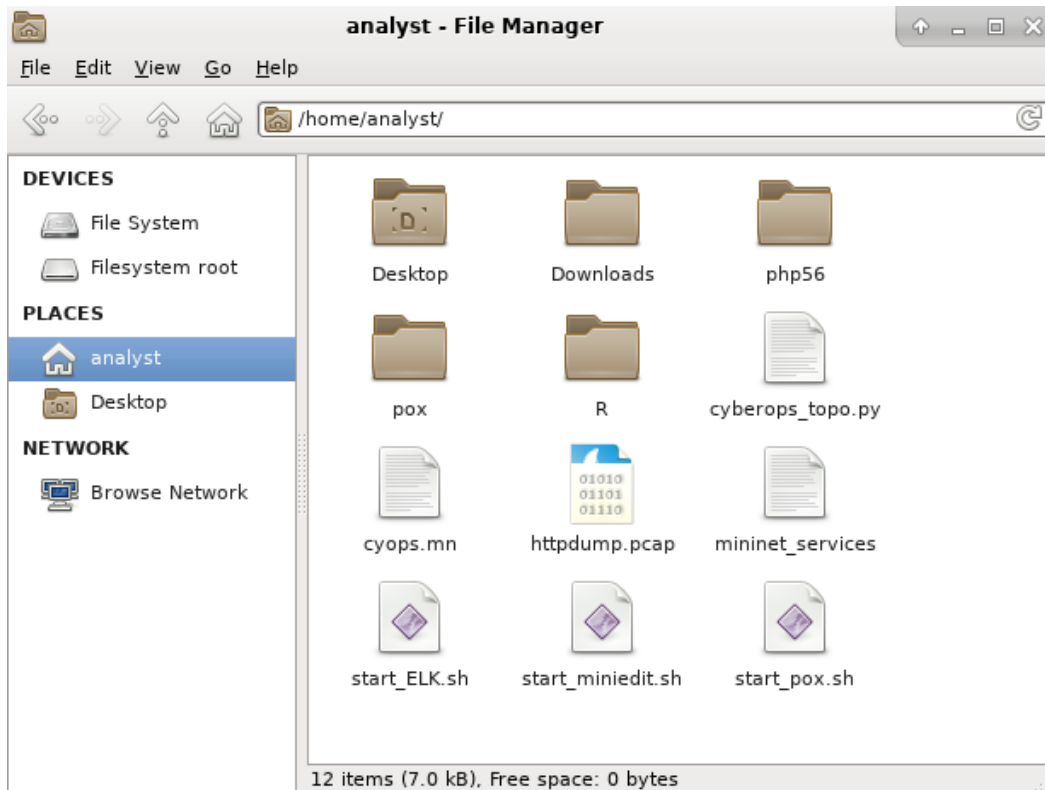
Because this website uses HTTP, the traffic is not encrypted. Click the Username field to see the warning pop up.

- e. Enter a username of **Admin** with a password of **Admin** and click **Login**.
- f. Close the virtual web browser.
- g. Return to the terminal window where tcpdump is running. Enter **CTRL+C** to stop the packet capture.

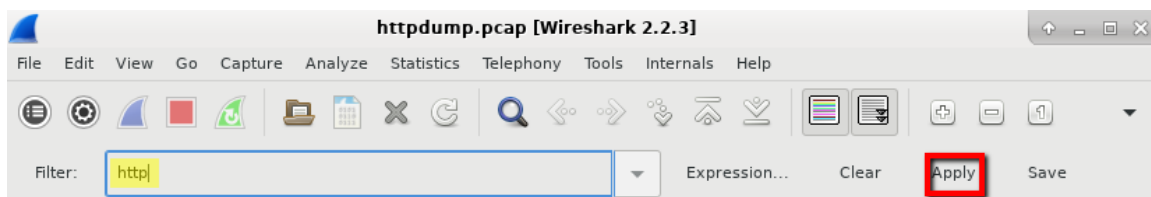
Step 3: View the HTTP capture.

The tcpdump, executed in the previous step, printed the output to a file named `httdump.pcap`. This file is located in the home directory for the user **analyst**.

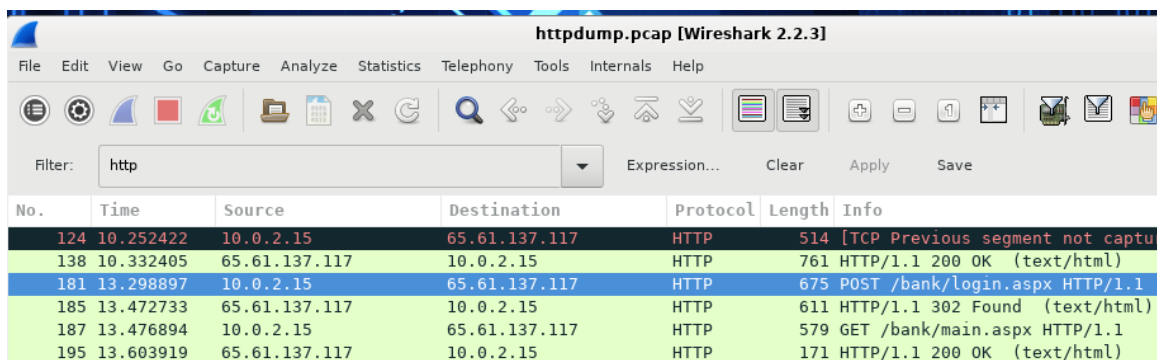
- Click the File Manger icon on the desktop and browse to the home folder for the user **analyst**. Double-click the **httdump.pcap** file to open it in Wireshark.



- In the Wireshark application, filter for **http** and click **Apply**.

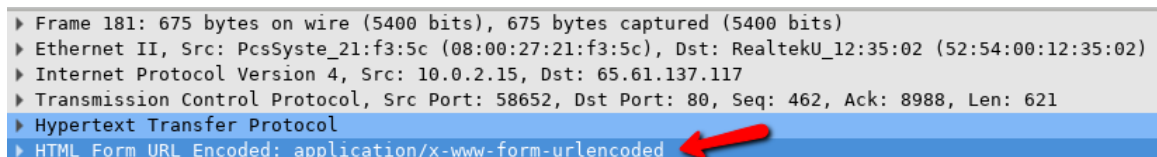


- c. Browse through the different HTTP messages and select the **POST** message.



No.	Time	Source	Destination	Protocol	Length	Info
124	10.252422	10.0.2.15	65.61.137.117	HTTP	514	[TCP Previous segment not captured]
138	10.332405	65.61.137.117	10.0.2.15	HTTP	761	HTTP/1.1 200 OK (text/html)
181	13.298897	10.0.2.15	65.61.137.117	HTTP	675	POST /bank/login.aspx HTTP/1.1
185	13.472733	65.61.137.117	10.0.2.15	HTTP	611	HTTP/1.1 302 Found (text/html)
187	13.476894	10.0.2.15	65.61.137.117	HTTP	579	GET /bank/main.aspx HTTP/1.1
195	13.603919	65.61.137.117	10.0.2.15	HTTP	171	HTTP/1.1 200 OK (text/html)

- d. In the lower window, the message is displayed. Expand the **HTML Form URL Encoded: application/x-www-form-urlencoded** section.



```
▶ Frame 181: 675 bytes on wire (5400 bits), 675 bytes captured (5400 bits) on interface 0
▶ Ethernet II, Src: PcsSyste_21:f3:5c (08:00:27:21:f3:5c), 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: 58652, Dst Port: 80, Seq: 462, Ack: 8988, Len: 621
▶ Hypertext Transfer Protocol
▶ HTML Form URL Encoded: application/x-www-form-urlencoded
```

What two pieces of information are displayed?

- e. Close the Wireshark application.

Part 2: Capture and View HTTPS Traffic

You will now use `tcpdump` from the command line of a Linux workstation to capture HTTPS traffic. After starting `tcpdump`, you will generate HTTPS traffic while `tcpdump` records the contents of the network traffic. These records will again be analyzed using Wireshark.

Step 1: Start `tcpdump` within a terminal.

- a. While in the terminal application, enter the command **`sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap`**. Enter the password **cyberops** for the user analyst when prompted.

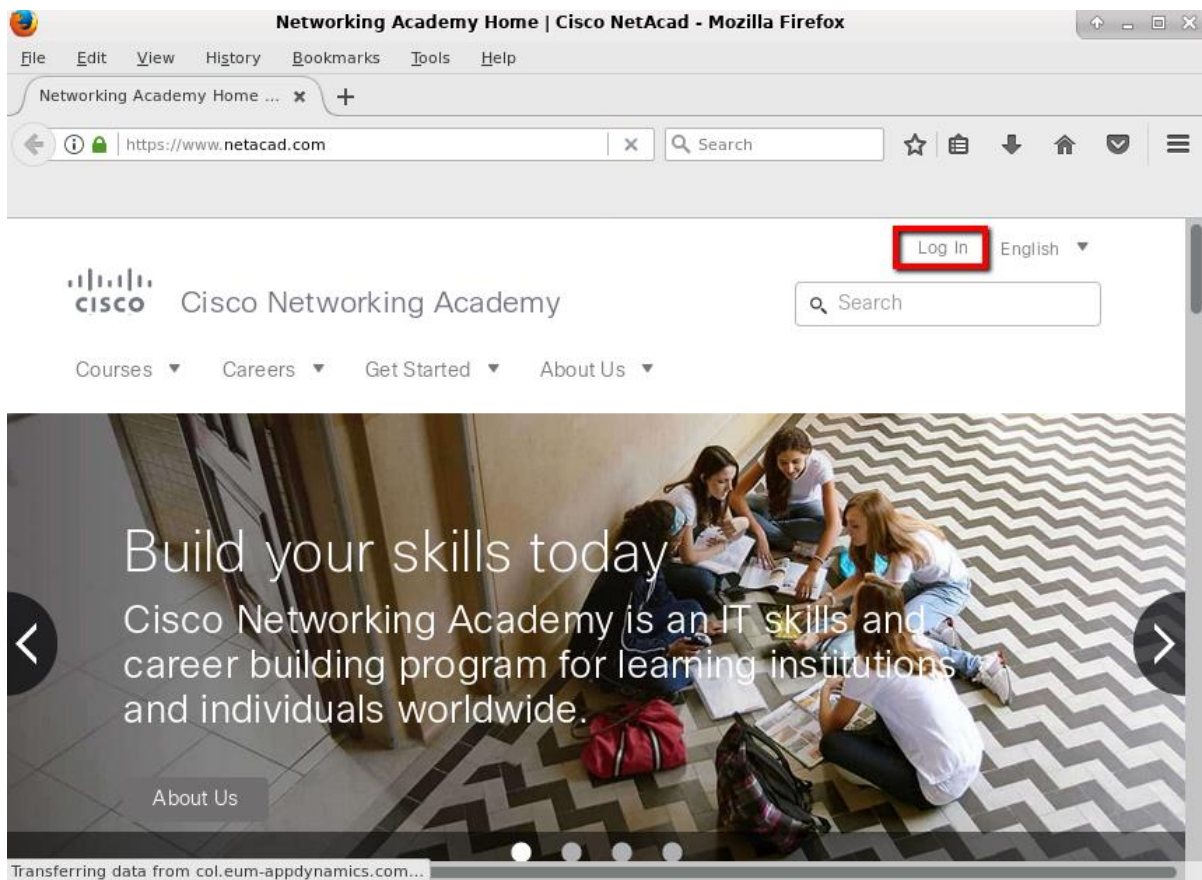
```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

This command will start `tcpdump` and record network traffic on the **enp0s3** interface of the Linux workstation. If your interface is different than `enp0s3`, please modify it when using the above command.

All recorded traffic will be printed to the file **httpsdump.pcap** in the home directory of the user analyst.

- b. Open a web browser from the launch bar within the Linux Workstation. Navigate to www.netacad.com. What do you notice about the website URL?

- c. Click **Log in**.



- d. Enter in your NetAcad username and password. Click **Log In**.

Cisco Networking Academy Log In

Email address or screen name

your_username

Password

●●●●●●●●●●

Cancel Log In

[Forgot Password](#) [Resend Activation Email](#) [Redeem Seat Token](#)

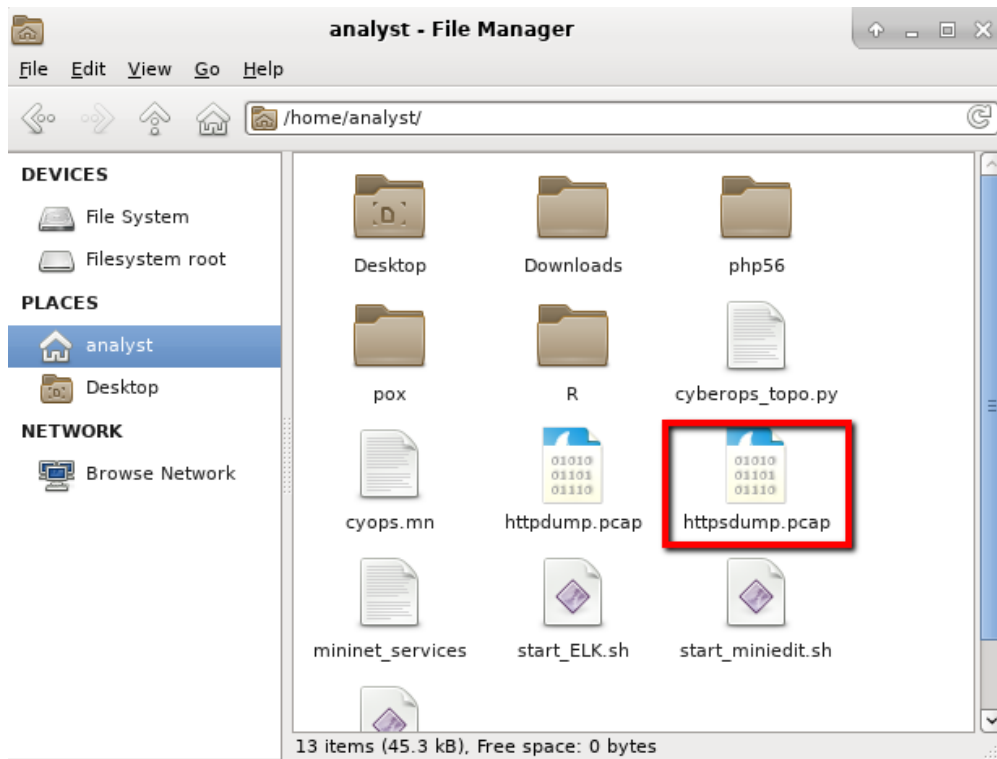
- e. Close the virtual web browser.
- f. Return to the terminal window where tcpdump is running. Enter **CTRL+C** to stop the packet capture.

Step 2: View the HTTPS capture.

The tcpdump executed in Step 1 printed the output to a file named httpsdump.pcap. This file is located in the home directory for the user **analyst**.

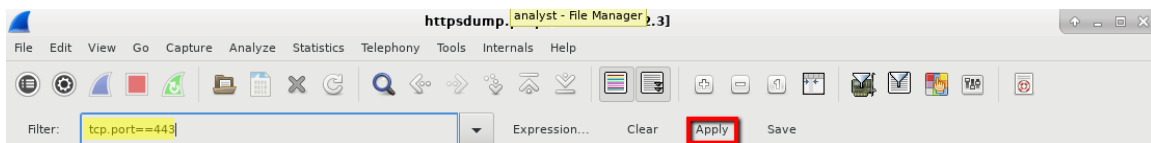
Lab – Using Wireshark to Examine HTTP and HTTPS

- a. Click the Filesystem icon on the desktop and browse to the home folder for the user analyst. Open the **httpsdump.pcap** file.

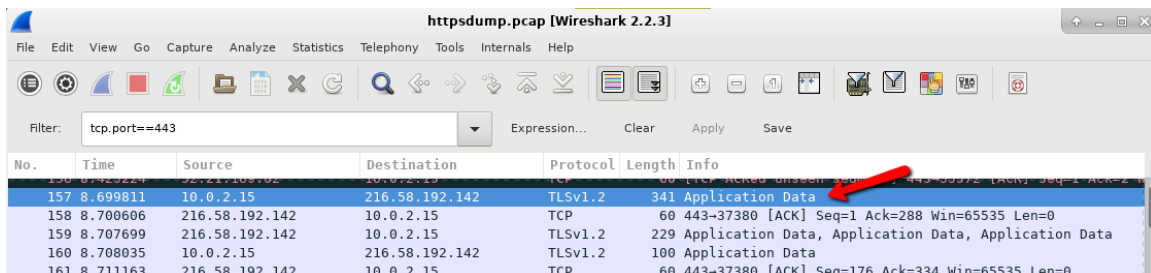


- b. In the Wireshark application, expand the capture window vertically and then filter by HTTPS traffic via port 443.

Enter **tcp.port==443** as a filter, and click **Apply**.



- c. Browse through the different HTTPS messages and select an **Application Data** message.



- d. In the lower window, the message is displayed.

What has replaced the HTTP section that was in the previous capture file?

- e. Completely expand the **Secure Sockets Layer** section.

```
▶ Frame 157: 341 bytes on wire (2728 bits), 341 bytes captured (2728 bits) on 0
▶ Ethernet II, Src: PcsSyste_21:f3:5c (08:00:27:21:f3:5c), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 216.58.192.142
▶ Transmission Control Protocol, Src Port: 37380, Dst Port: 443, Seq: 1, Ack: 1, Len: 287
▼ Secure Sockets Layer
  ▼ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 282
    Encrypted Application Data: 0000000000000000bed2031d6dabc4c685ca7854a009a7a56...
```

- f. Click the **Encrypted Application Data**.

Is the application data in a plaintext or readable format?

- g. Close all windows and shutdown the virtual machine.

Reflection

1. What are the advantages of using HTTPS instead of HTTP?

2. Are all websites that use HTTPS considered trustworthy?
