# Networking/Computing Tips/Tricks

## Finding Text Strings in Wireshark Captures

Created: Thursday, 26 September 2019 10:19
Hits: 28189


Rate this content:

5 of 5 - 2 votes

A common question regarding Wireshark packet analysis is "Can I find a t
capture?"

The answer is that it depends on where the text string is (like header vs. packet content) and if the packets contain encrypted data.

Check out these great

Our custom profiles

Our Udemy course o

Our Udemy course o

### Usecase #1:

If you are looking for something like "password" in the contents of packets, and the user was on an HTTPS connection, then you will not find this string. However, if they are using HTTP or some other clear text protocol, then you will be able to find a string in the packet contents.

### Usecase #2:

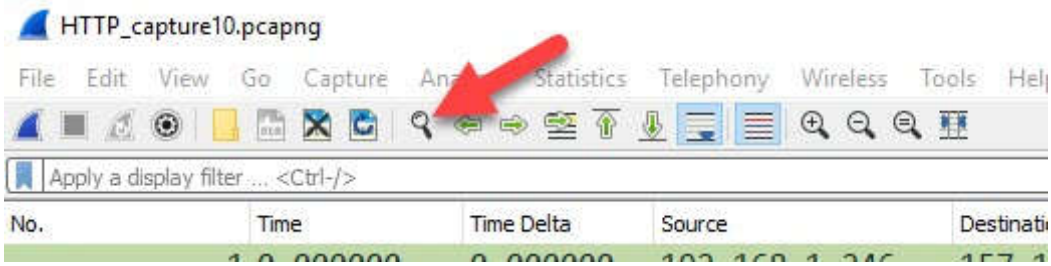
If you are looking for a string in the packet headers, it will depend on whether the header was inside or outside a VPN tu
headers outside such a tunnel are always searchable and not encrypted. Anything in the tunnel will be and therefore n

Alright, let's talk about what tools come in Wireshark to find a string.

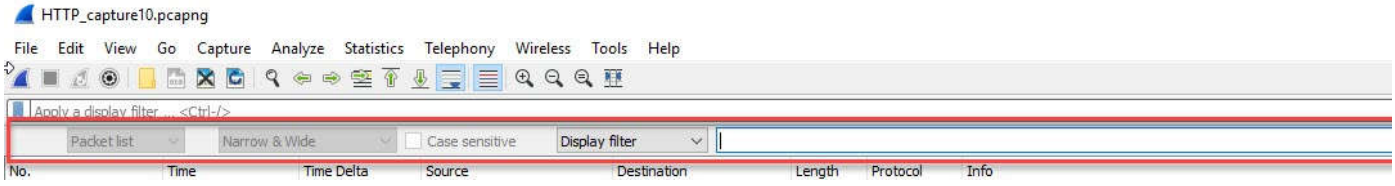
If you would like to see this - check out our video:

## Option 1

First there is the generic find/search capability in Wireshark that is found here:

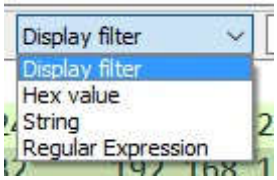



When you click on this looking glass button, or select Edit> Find Packet from the drop down menus, you will be present toolbar immediately below the display filter toolbar:



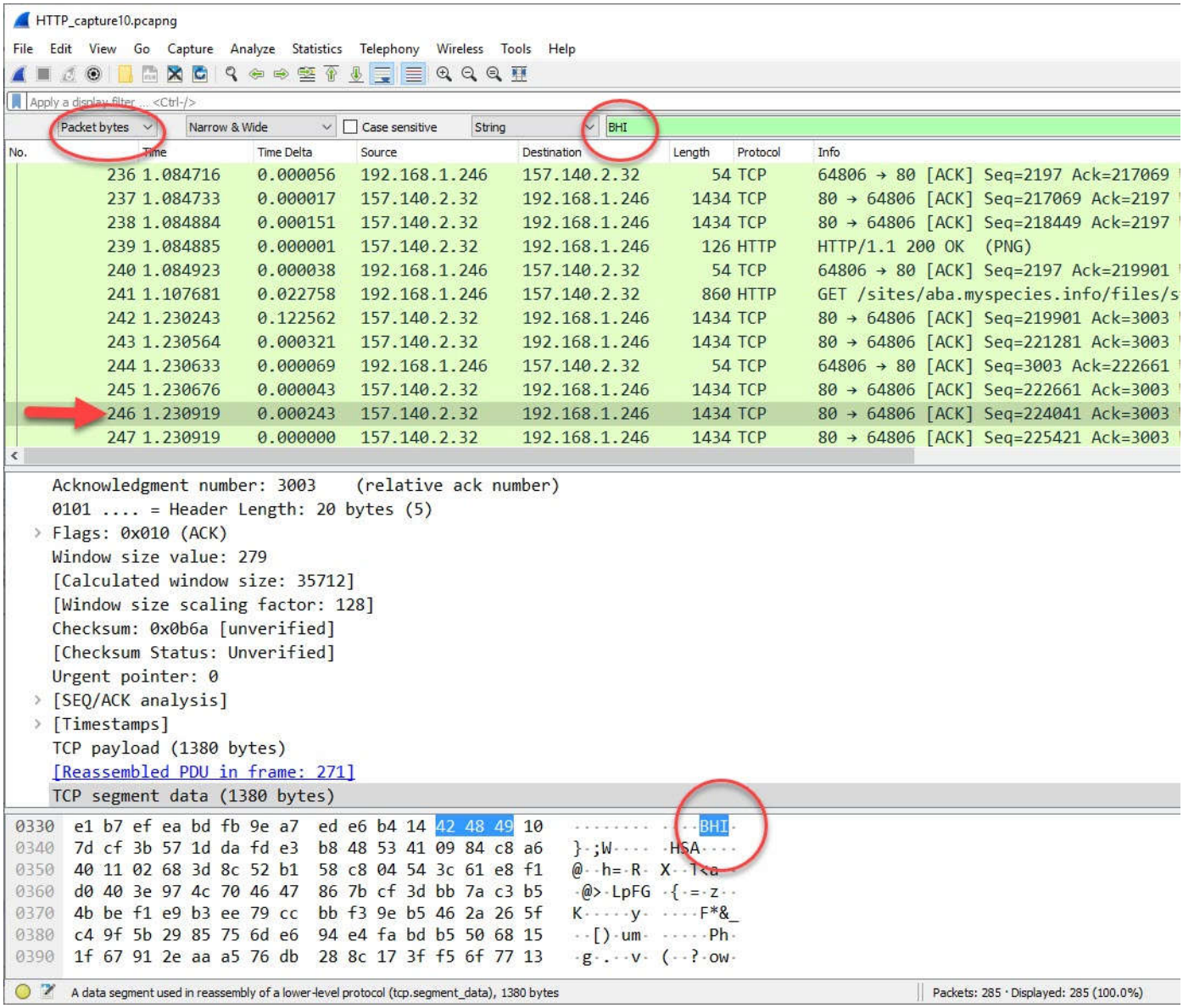

You will note the "Display filter" drop down just to the left of the string entry box.

The options are as follows:




To find a string, select string, and note that the two other drop down boxes are no longer greyed out.

Now select packet bytes if you want to look inside the packets, and then type the string you are looking for in the entry




Above, you can see I selected string, packet bytes, entered "BHI" as my string and then clicked find. Packet 246 has thi highlights this. This was the first instance, and if I clicked find again, Wireshark will look further into the capture. Eventu the capture and have to reset the view to the first packet to initiate the search once again.

This search is case insensitive. Whether I had entered "bhi" or "bHi" or "bhI", the search will find the same packet.

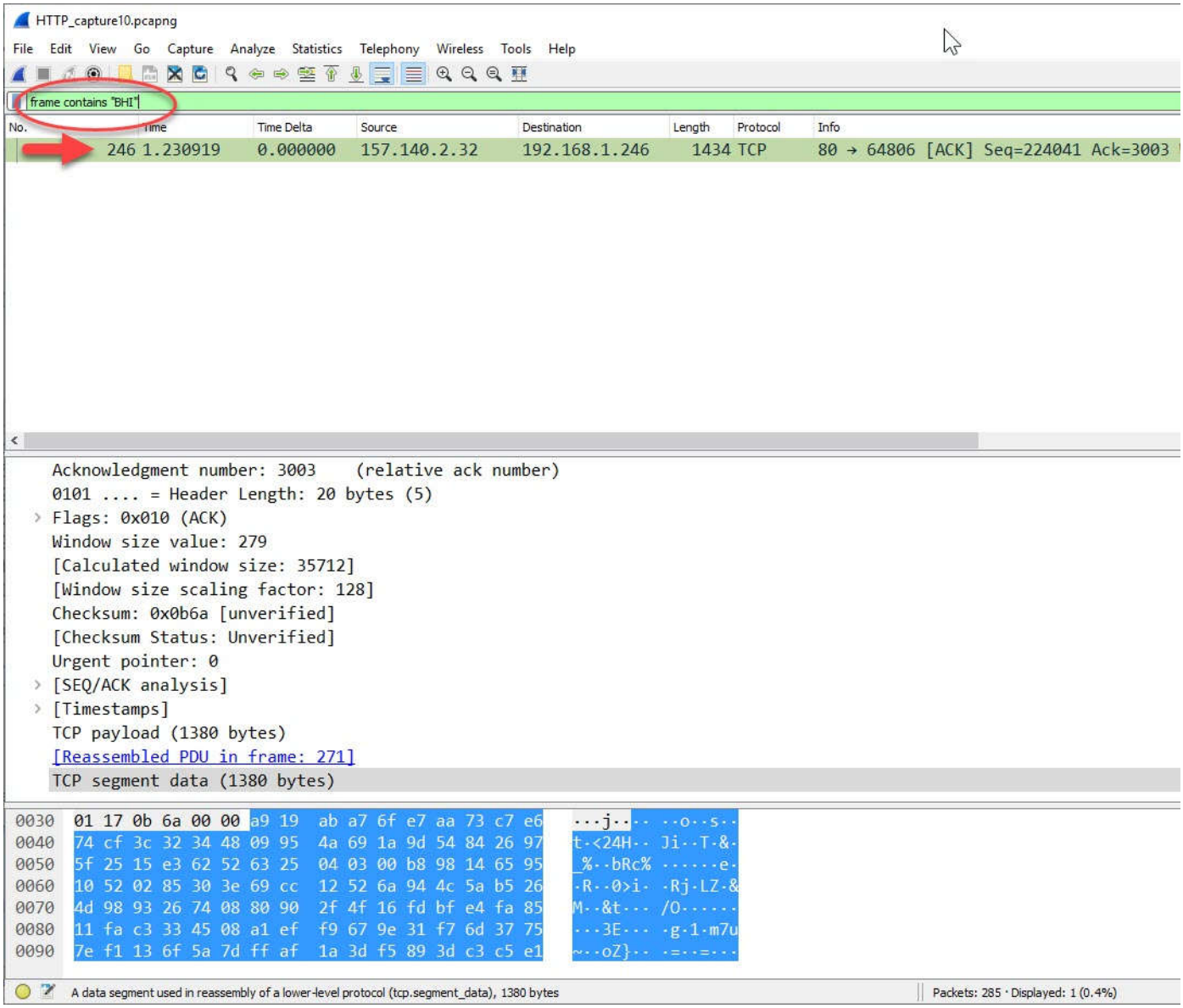
## Option 2

What if I just wanted to see the packets with "BHI" in them?

For this we need to use the Display Filter functionality of Wireshark. A reference with details regarding my examples b

Specifically there is a display filter terms called 'frame contains' and 'frame matches'. Contains is fairly stright forward.

```
frame contains "BHI"
```



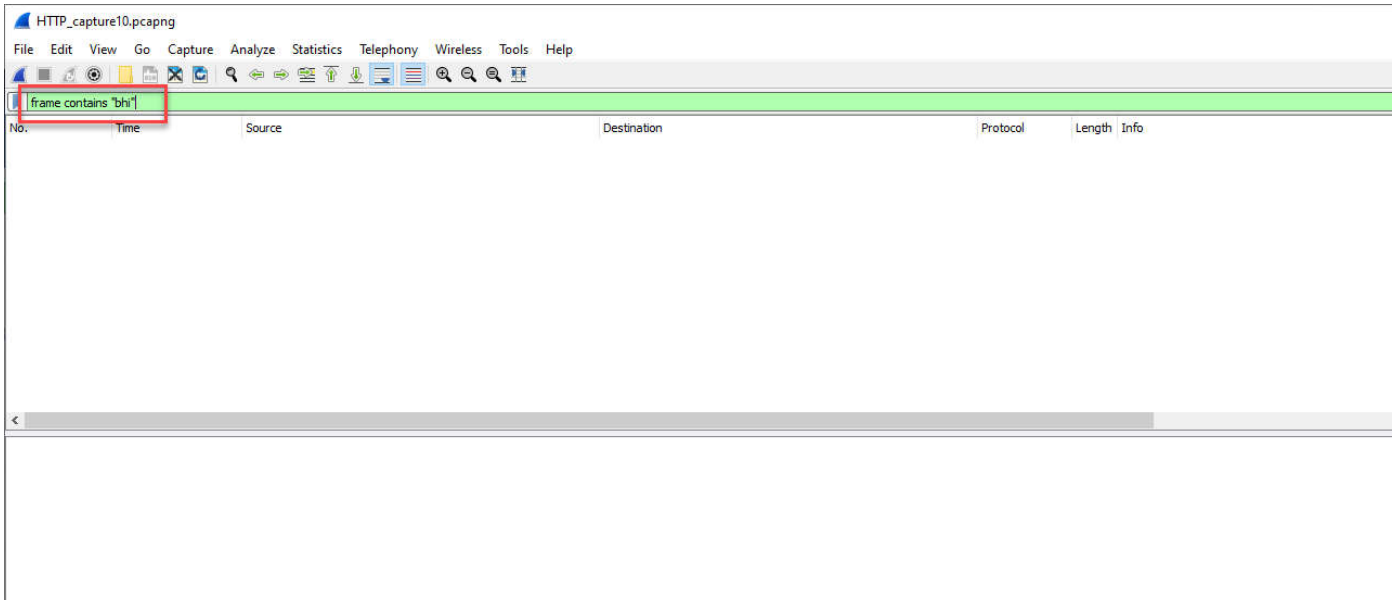

A couple of things here: you do not need to use quotes, and you cannot say something like an IP Address.

The 'frame matches' is a little different. This is a fairly flexible display filter and we will not cover all the options here. T "Regex next" to Wireshark - a Perl-compatible regular expression. You can find a great cheat sheet for Regex here. So details of this, we will provide and explain some examples commonly used. Hopefully from this you will understand it.

These 'frame contains' or 'frame matches' display filters are case sensitive. If I used:

```
frame contains "bhi"
```

I get no results:

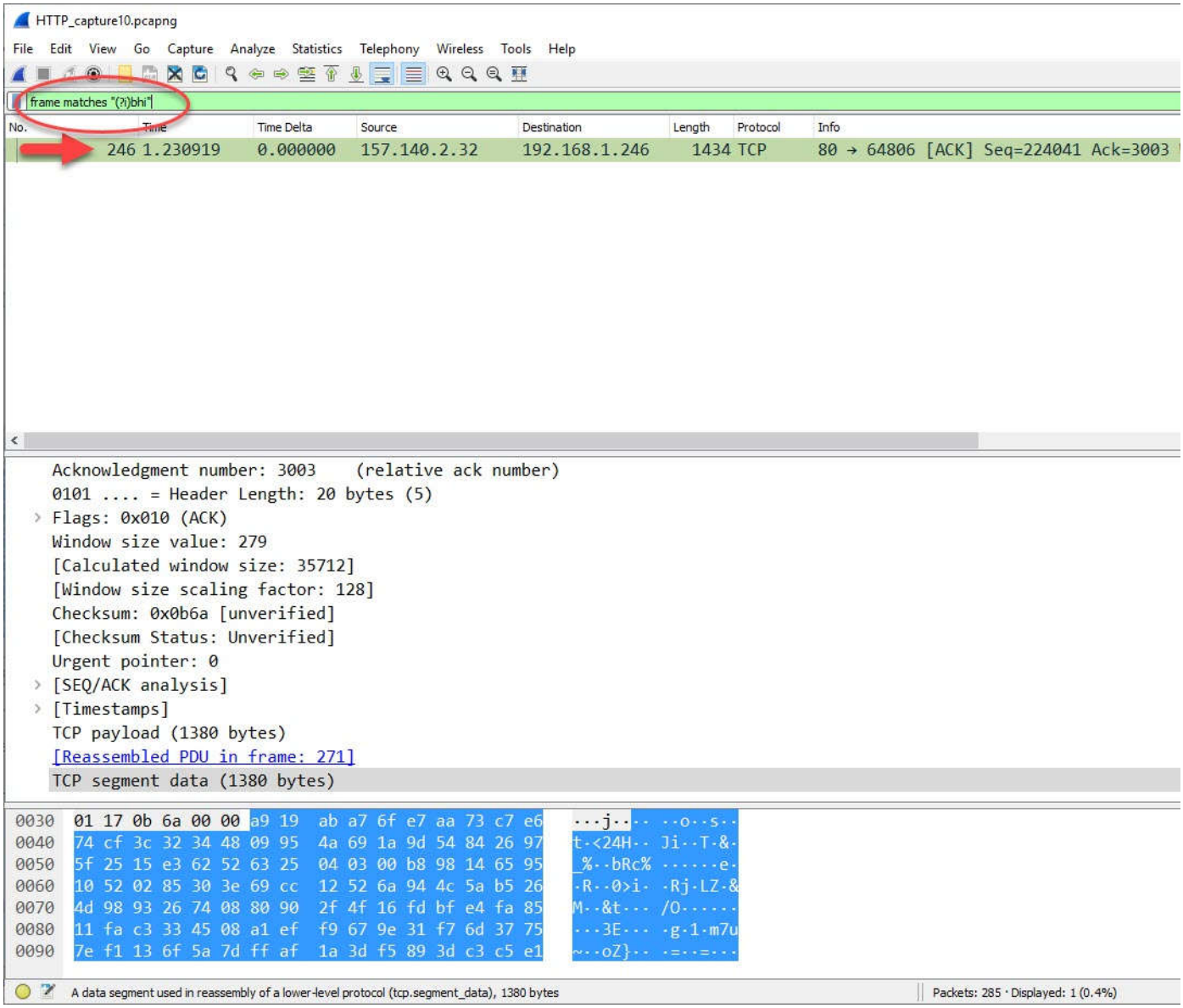



So a common command I use when performing these types of searches is the (?i) which makes the search case insensi

So I could have used the following command:

```
frame matches "(?i)bhi"
```

I now find the packet again:




Let's say I wanted to find "BHI" or "BHS", I would use:

```
frame matches "(?i)bh[is]"
```

Let's say I wanted to find "BHI" and all others through "BHS", I would use:

```
frame matches "(?i)bh[i-s]"
```

Let's say I wanted to match "BHI" or "BHS", I would use:

```
frame matches "(?i)(bhi|bhs)"
```

As you can imagine, another common one here would be:

```
frame matches "(?i)(username|password)"
```

You can also use the '^', which means start of field, and '$', which means end of field, commands.

Also the '\.' means look for a dot.

So if you wanted to find any listed web sites in a capture, perhaps you would use:

```
frame matches "\.com$"
```

Or perhaps you would want to find possible files:

```
frame matches "\.(?i)(exe|zip|doc|xls|ppt|jar)"
```

Lets say you wanted to look for email addresses, you would use this:

```
frame matches "(?i)[A-Z0-9._%~]+@[A-Z0-9.-]+\.[A-Z\>]{2,4}"
```

So those are just some ideas.

I hope you find this article and its content helpful. Comments are welcomed below. If you would like to see more artic
us by clicking the patron link where you will receive free bonus access to courses and more, or simply buying us a cup o
comments are welcome!

Wireshark

Prev

Add comment

Name required

E-mail required, but not visible

Title

Write your comment here...

1000 characters left

Notify me of follow-up comments

Accept privacy policy