IE2042 – Systems and Network Programming

MALWARE TRAFFIC ANALYSIS

Specialized in Cyber Security
Year 2, Semester 1
Group 02.01

Sri Lanka Institute of Information Technology

Jayawikrama K.D.S.P. IT21170720

Abstract

Malware traffic analyze based on the Wireshark tool. Gerald Combs created the open-source, Windows- and Unix-compatible protocol analyzer known as Wireshark. Its main objective is traffic analysis, and it's an excellent, straightforward tool for examining communications and resolving network problems. Initially called Ethereal Wireshark has several filters that make it simpler to establish search criteria and now supports over 1100 protocols. It has an easy-to-use front-end that lets you divide the captured packets by layer. In many industries, Wireshark, the top network protocol analyzer in the world, is the standard. The project has been going on since 1998.Since Wireshark comprehends the structure of various networking protocols and enables you to inspect the fields of each of the headers and layers of the packets being analyzed, network administrators have a wide range of options when doing traffic analysis tasks.

This try hack me box based on the Wireshark tool and those who are try this room, they must answer some question using the given pcap file. That question based on the given pcap file and finally those who can find the flag of that pacp file.

Foreword

In the present day, computer networks have transformed into far more sophisticated and intelligent systems. At the same time, cybercriminals from across the world are developing and deploying various internet attacks for a range of reasons, such as data theft, machine corruption, and hijacking. Most users of the system, including administrators and forensic investigators, are affected by these attacks. All these problems drive network engineers to develop their ability to examine and comprehend network data. Organizations must routinely examine their resources for the existence of harmful components due to the number of threats. A resource may get infected because of hackers taking advantage of a vulnerability. During the exploitation, professionals could look at instances connected to the danger.

Additionally, some of these investigations' conclusions could already be known to the public. Such reports are useful in real life. Additionally, indicators of compromise are usually included in reports on APT campaigns By spotting attacks early on and acting quickly to stop them or minimize damage, organizations can stop attacks in their tracks. This is done by keeping an eye out for signs of compromise. Out of all the precise technical information regarding a certain Advanced Persistent Threat, "Indicators of compromise" offer the security managers the most useful practical information (APT).

This book discusses how to gather data for a few fundamental indications of compromise using a packet analysis tool like Wireshark.

Acknowledgment

We would like to thank Dr. Lakmal Perera, kindly cooperating with us and encouraging us, which allowed me to complete this book effectively.

Contents

Introduction

What is the try hack me.?

Try Hack Me is an online platform that uses brief, gamified real-world laboratories to educate cyber security. We provide information that is appropriate for both inexperienced and experienced hackers, incorporating challenges and guidelines to accommodate various learning styles.

What is the Wireshark.?

Wireshark is a network packet analyzer. A network packet analyzer displays collected packet data in as much detail as feasible. Consider a network packet analyzer as a measuring tool for determining what is occurring within a network cable, like how an electrician uses a voltmeter to determine what is happening inside an electric wire. Such tools were either exceedingly costly, proprietary, or both in the past. That has altered, though, with the introduction of Wireshark. One of the top packet analyzers available today, Wireshark is free and open source.

PCAP, sometimes referred to as libpcap, is an application programming interface (API) that collects live network packet data from OSI model Layers 2–7. To gather and store packet data from a network, network analyzers like Wireshark create.pcap files. PCAP is available in several formats, including Libpcap, WinPcap, and PCAPng. Network packets for TCP/IP and UDP may be seen using these PCAP files. You must build a. pcapfile if you wish to capture network traffic. Using a network analyzer or packet sniffing program like Wireshark or tcpdump, you may build a. pcapfile.

This booklet focuses the pcap file analyze using the Wireshark. you can deeply learn about what is the Wireshark, what is the advantages of Wireshark, how packet analyze using Wireshark, how to find server name, IP address, MAC address ...etc.

Why we use Wireshark.?

- To debug network issues, network administrators utilize it.
- To analyze security issues, network security engineers utilize it.
- To validate network applications, QA engineers utilize it.
- It is used by developers to troubleshoot protocol implementations.
- To study the internals of network protocols, people utilize it.

Some features of Wireshark

- Available for UNIX and Windows.
- Capture live packet data from a network interface.
- Open files containing packet data captured with tcpdump/WinDump, Wireshark, and many other packets capture programs.
- Import packets from text files containing hex dumps of packet data.
- Display packets with very detailed protocol information.
- Save packet data captured

Benefits of Wireshark

1. Operating system support

Only a handful of the modern operating systems that are supported by Wireshark include Windows, Mac OS X, and Linux-based platforms. On the Wire- shark main page, you may find a comprehensive list of supported OS systems.

2. Cost

Under the GPL, Wire- shark is made available as free software. It is available for download from its official website and may be used for either private or business purposes.

3. Program support

Windows, Mac OS X, and Linux-based platforms are only a few of the contemporary operating systems that Wireshark supports. CACE Technologies' SharkNet program offers paid support for Wireshark as well.

4. Supported protocols

More than 850 protocols are supported by Wireshark. These range from basic private protocols like IP and DHCP to more complex ones like AppleTalk and BitTorrent. A new protocol is supported by Wireshark with each version since it is built using an open-source methodology.

5. User-friendliness

Of all the packet-sniffing applications, the Wireshark interface is one of the simplest to comprehend. It is GUI-based, has a simple interface, and has extremely clear context menus. The usefulness of Wireshark is improved by several features including protocol-based color coding and intricate graphical representations of raw data. The Wireshark GUI is excellent for individuals who are just starting out in the field of packet analysis as opposed to the command line interface of other packet sniffing tools like tcpdump, which is highly complex.

Traffic analyzing

The performance of the network they oversee has, at some point or another, suffered for all network managers. Due to a lack of time and money, a lack of knowledge about the proper instruments, or an underlying mystery, they are aware that situations like that are not always simple. At times, connectivity is disrupted, or certain terminals have mysteriously been unplugged.

These problems are typically the result of poor network configuration, which includes duplicate lines, spanning trees, badly designed broadcast storms, etc. A DoS (Denial of Service) attack, traffic delivered with an infected ARP to locate hosts to infect, or simply infecting terminals with malware to join a zombie network or botnet are some examples of external attacks that may be to blame in specific circumstances.

The first step toward taking appropriate action and achieving proper protection in either scenario is identifying the incident's cause. Traffic analyzers may then be very helpful in detecting, analyzing, and mapping traffic, identifying network dangers, and limiting their eventual effect. There are sophisticated tools available on the market to help with that, including the Monitoring, Analysis and Response System by Intrusion Detection System/Internet Protocol System based on hardware from various vendors. However, due to the cost not adhering to the fundamental proportionality principle and the inability to justify its acquisition, these solutions are not always affordable to all businesses.

Therefore INTECO-CERT is presenting this "Guide to analyzing traffic using Wireshark" to meet the needs of organizations with more basic technical infrastructures. The goal is to educate administrators and technicians on the benefits of utilizing Wireshark, a free and open-source traffic analyzer, to audit the network. It also provides real-world instances of frequent local network assaults, which are presently the number one opponent in corporate settings.

Path of develop try hack me box

Users may simply assign work to one another in rooms, a virtual place. A specific workshop or training session can be performed in a room that has been created specifically for challenges (CTFs).

Instead of linking stuff to a space, it is tied to a job (either through virtual machines or downloading media). There can be several downloads or virtual machines for a single room, but there can only be one of each type of resource attached to a job at a time.

Process of making room

1. Create a room
2. Upload material (VMs or other files) or use the ones we provide.
3. Go to the manage room page and click on your newly created room
4. Click the "Tasks" tab and create room tasks; this is where you include your uploads (VMs or files)
5. When managing a room there is a blue "Share Room" button at the top right of the page, click this to get a link to share with your users to invite them to your room.

Manage the room as public

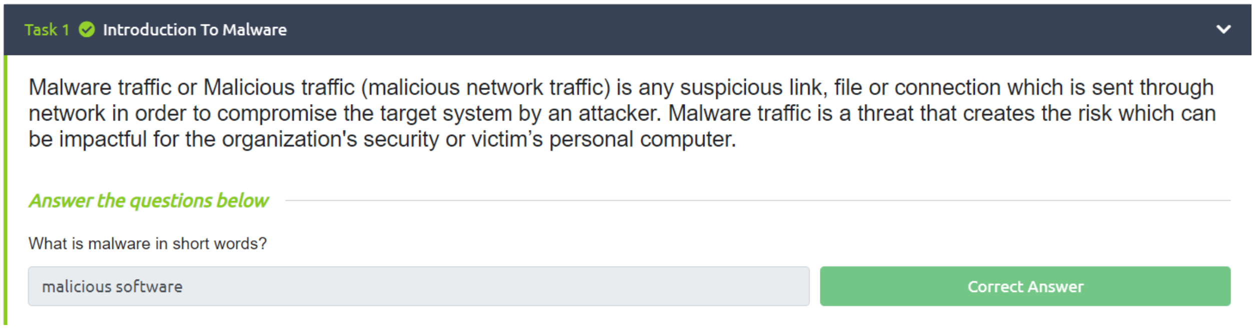
You may utilize the room sharing link to privately invite visitors to your room without making it visible to the public. A room becomes accessible to all users of the TryHackMe platform once it is made public. When you publish a room on the room management website, a review will be done. If something is determined to be broken, to be lacking material, or to be otherwise not quite right, it will either be rejected with comments, or a room reviewer will contact you. A release date will be set once your room has been examined and authorized. After clearance, your accommodation won't be immediately made available.

Task 1 - Introduction to Malware

Any malicious program is one that has been made specifically with the intention of causing harm to a computer, server, client, or computer network, leaking private information, gaining access to systems or data without authorization, denying users access to information, or unintentionally jeopardizing user privacy and security on computers.

This task based on the basic introduction of malware. This try hack me box ask the malware short word, that answer is ‘malicious software’.

Answer: malicious software



Malware traffic or Malicious traffic (malicious network traffic) is any suspicious link, file or connection which is sent through network in order to compromise the target system by an attacker. Malware traffic is a threat that creates the risk which can be impactful for the organization's security or victim’s personal computer.

Answer the questions below

What is malware in short words?

malicious software

Task 2 - Introduction of Wireshark

A free and open-source packet analyzer is Wireshark. It is employed for network analysis, troubleshooting, software and communications protocol creation, and instruction. The leading and most popular network protocol analyzer on the planet is called Wireshark. It is the de facto (and frequently de jure) norm across many commercial and nonprofit firms, governmental organizations, and educational institutions because it enables you to observe what's occurring on your network at a microscopic level. Gerald Combs began working on the project in 1998, and it is now flourishing because to the voluntary contributions of networking professionals from all around the world.

Wireshark has a rich feature set that includes the following:

- ✓ Deep inspection of hundreds of protocols, with more being added all the time
- ✓ Live capture and offline analysis
- ✓ Standard three-pane packet browser
- ✓ Multi-platform: Runs on Windows, Linux, macOS, Solaris, FreeBSD, NetBSD, and many others
- ✓ Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility
- ✓ The most powerful display filters in the industry
- ✓ Rich VoIP analysis

It may be used for a variety of things, including:

- ✓ finding and fixing network issues, such as congestion and network load failure sites.
- ✓ spotting security irregularities such rogue hosts, unusual port use, and suspicious traffic
- ✓ examining and learning about protocol specifics, such as response codes and
- ✓ Guided User Interface (GUI) and Data

Toolbar:

For packet sniffing and processing, including filtering, sorting, summarizing, exporting, and merging, the main toolbar has numerous menus and shortcuts.

Display Filter Bar:

The main query and filtering section

Status Bar:

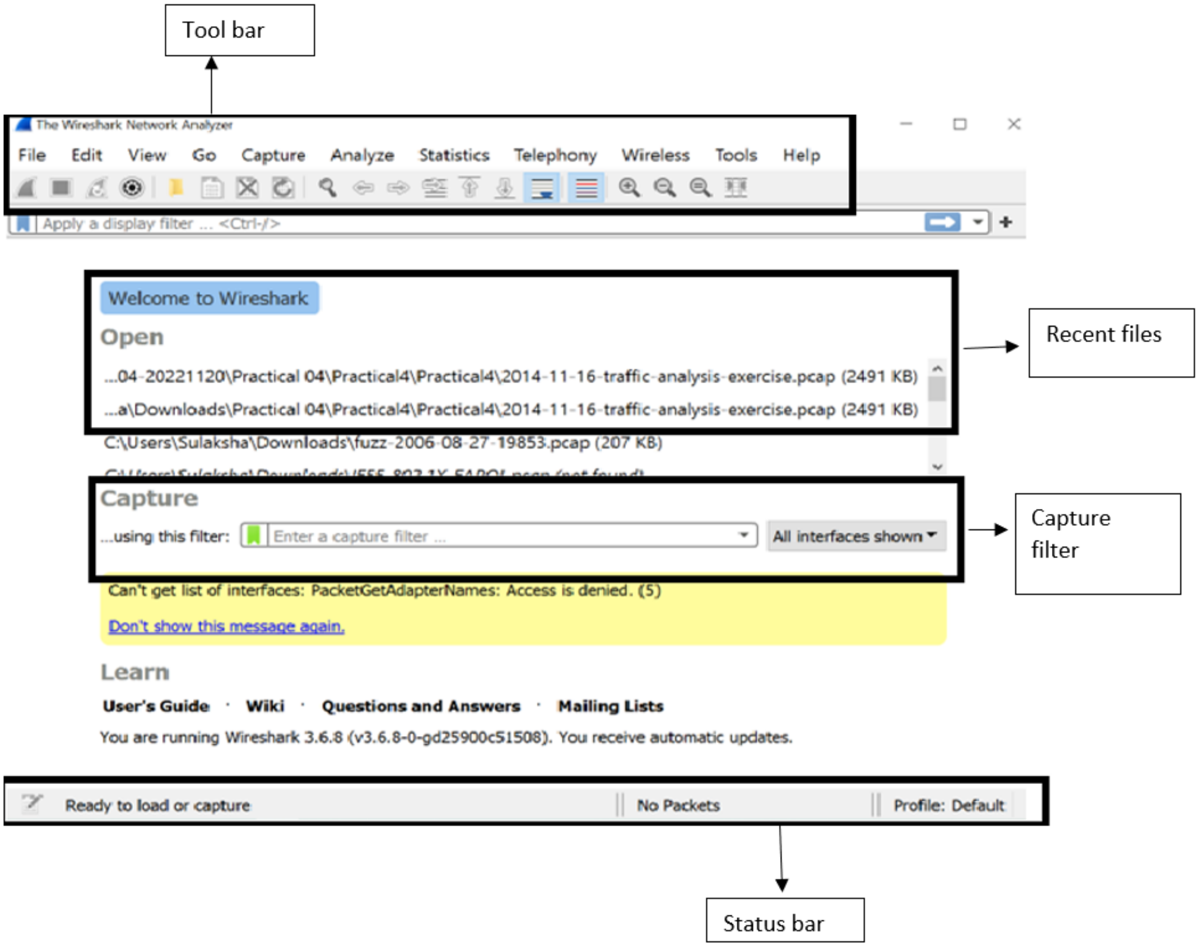
Tool status, profile, and numeric packet information.

Recent Files:

A list of the files that have most recently been investigated. A double-click will bring up the list of files.

Capture filter:

Filters for capturing data and available sniffing points A computer and a network are connected at the network interface. Networking hardware is made possible by the software connection.

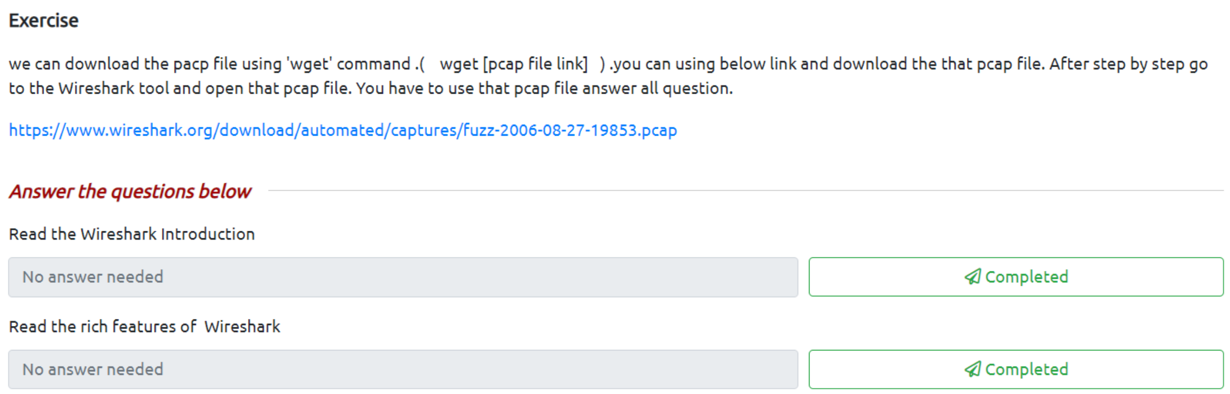


...04-20221120\Practical 04\Practical4\Practical4\2014-11-16-traffic-analysis-exercise.pcap (2491 KB)
...a\Downloads\Practical 04\Practical4\Practical4\2014-11-16-traffic-analysis-exercise.pcap (2491 KB)
C:\Users\Sulaksha\Downloads\fuzz-2006-08-27-19853.pcap (207 KB)
C:\Users\Sulaksha\Downloads\EEE-802.1X-EAPOL.pcap (not found)

Can't get list of interfaces: PacketGetAdapterNames: Access is denied. (5)
Don't show this message again.

You are running Wireshark 3.6.8 (v3.6.8-0-gd25900c51508). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default



Exercise

we can download the pacp file using 'wget' command .(wget [pcap file link]) .you can using below link and download the that pcap file. After step by step go to the Wireshark tool and open that pcap file. You have to use that pcap file answer all question.

https://www.wireshark.org/download/automated/captures/fuzz-2006-08-27-19853.pcap

Answer the questions below

Read the Wireshark Introduction

No answer needed

Read the rich features of Wireshark

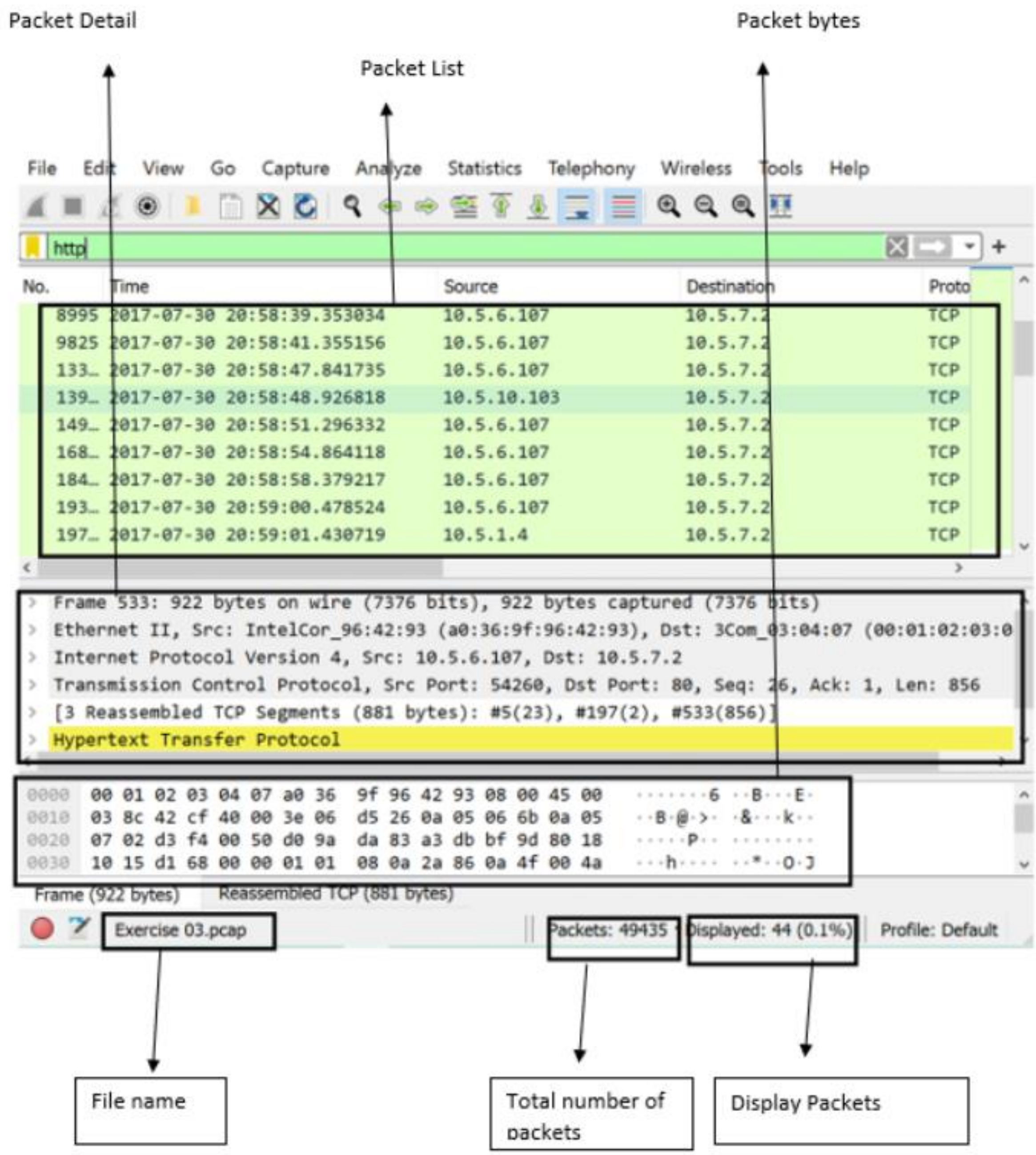
No answer needed

This task based on the given pcap file. Users who can download this pcap file via terminal or browser. There are 2 questions in this task both are reading question only. Any user can read and complete that task,

Task 3 - Introduction of Pcap File and analyze

Packet capture is a networking practice involving the interception of data packets travelling over a network. Once the packets are captured, they can be stored by IT teams for further analysis. The inspection of these packets allows IT teams to identify issues and solve network problems affecting daily operations.

you can also use the "File" menu, dragging and dropping the file, or double-clicking on the file to load a pcap.



http

No.	Time	Source	Destination	Proto
8995	2017-07-30 20:58:39.353034	10.5.6.107	10.5.7.2	TCP
9825	2017-07-30 20:58:41.355156	10.5.6.107	10.5.7.2	TCP
133…	2017-07-30 20:58:47.841735	10.5.6.107	10.5.7.2	TCP
139…	2017-07-30 20:58:48.926818	10.5.10.103	10.5.7.2	TCP
149…	2017-07-30 20:58:51.296332	10.5.6.107	10.5.7.2	TCP
168…	2017-07-30 20:58:54.864118	10.5.6.107	10.5.7.2	TCP
184…	2017-07-30 20:58:58.379217	10.5.6.107	10.5.7.2	TCP
193…	2017-07-30 20:59:00.478524	10.5.6.107	10.5.7.2	TCP
197…	2017-07-30 20:59:01.430719	10.5.1.4	10.5.7.2	TCP

```
> Frame 533: 922 bytes on wire (7376 bits), 922 bytes captured (7376 bits)
> Ethernet II, Src: IntelCor_96:42:93 (a0:36:9f:96:42:93), Dst: 3Com_03:04:07 (00:01:02:03:0
> Internet Protocol Version 4, Src: 10.5.6.107, Dst: 10.5.7.2
> Transmission Control Protocol, Src Port: 54260, Dst Port: 80, Seq: 26, Ack: 1, Len: 856
> [3 Reassembled TCP Segments (881 bytes): #5(23), #197(2), #533(856)]
> Hypertext Transfer Protocol
```

```
0000  00 01 02 03 04 07 a0 36  9f 96 42 93 08 00 45 00   ·······6 ··B···E·
0010  03 8c 42 cf 40 00 3e 06  d5 26 0a 05 06 6b 0a 05   ··B·@·>· ·&···k··
0020  07 02 d3 f4 00 50 d0 9a  da 83 a3 db bf 9d 80 18   ·····P·· ········
0030  10 15 d1 68 00 00 01 01  08 0a 2a 86 0a 4f 00 4a   ···h···· ··*··O·J
```

Frame (922 bytes)   Reassembled TCP (881 bytes)

Exercise 03.pcap   Packets: 49435 · Displayed: 44 (0.1%)   Profile: Default

We can view the processed filename, a complete breakdown of the number of packets, and packet information. The three different panes that show the packet details enable us to view them in various formats.

1.Packet List Pane:

Each packet's summary. Selecting a packet for additional research requires clicking on the list. The specifics will show up in the other panels once you choose a packet.

2.Packet Bytes Pane:

The chosen packet is shown in hexadecimal and decoded ASCII. Depending on the details pane area that was clicked, the packet field is highlighted.

3.Packet Detail Pane:

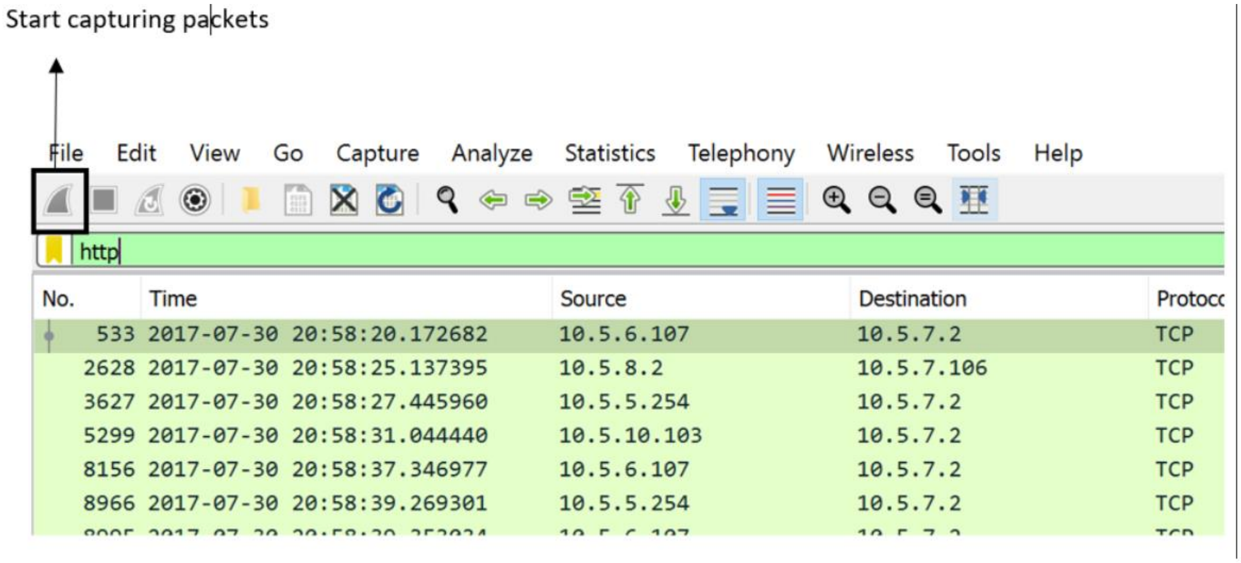
Detailing the selected packet's protocol.

Colouring Packets

There are two different kinds of packet coloring techniques available in Wireshark: temporary rules that are only used during a program session and permanent rules that are kept in the preference file (profile) and accessible during the subsequent program session. Permanent coloring rules may be created using the "right-click menu" or the "View --> Coloring Rules" menu. The "Colourize Packet List" option enables/disenables the coloring guidelines.

Traffic Sniffing

Network sniffing may be started using the blue "shark button," stopped with the red button, and restarted using the green button. The employed sniffing interface and the total number of packets captured are also displayed in the status bar.



No.	Time	Source	Destination	Protoco
533	2017-07-30 20:58:20.172682	10.5.6.107	10.5.7.2	TCP
2628	2017-07-30 20:58:25.137395	10.5.8.2	10.5.7.106	TCP
3627	2017-07-30 20:58:27.445960	10.5.5.254	10.5.7.2	TCP
5299	2017-07-30 20:58:31.044440	10.5.10.103	10.5.7.2	TCP
8156	2017-07-30 20:58:37.346977	10.5.6.107	10.5.7.2	TCP
8966	2017-07-30 20:58:39.269301	10.5.5.254	10.5.7.2	TCP

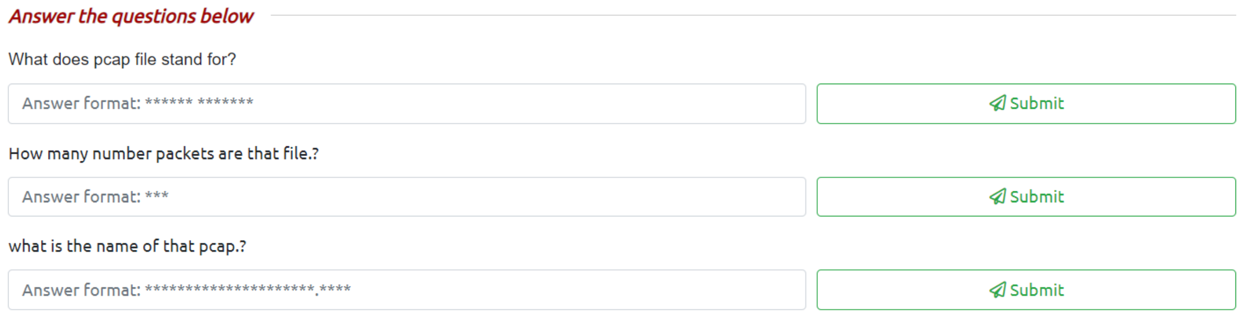
Merge PACP files

Two pcap files can be combined into one file using Wireshark. To combine a pcap with the one that has been processed, use the "File —> Merge" menu option. Wireshark will display the total number of packets in the selected file when you select the second file. After you click "open," it will combine the current pcap file with the one you've selected to create a new pcap file. Remember to save the "merged" pcap file before making any changes to it.

View Image Detail

It helps to know the file's specifics. You may occasionally need to know and recollect the file details (File hash, capture time, capture file comments, interface, and statistics), especially when working with several pcap files, to recognize, categorize, and prioritize a particular file. By selecting the "pcap icon placed on the left bottom" of the window or by going to "Statistics --> Capture File Properties," you may check the specifics.

Now we are going to question of task 3. There are 3 questions there.



Answer the questions below

What does pcap file stand for?

Answer format: ****** *******

How many number packets are that file.?

Answer format: ***

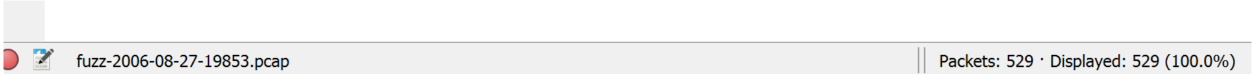
what is the name of that pcap.?

Answer format: ********************.****

First one is the "What does pcap file stand for?". It is very basic question. If we read the note attentionally, we can find correct standard word for pcap. Otherwise, we can google and find it.

Second question is "How many number packets are that file.?". after the open pcap file we can see number of packets in the right-side bottom of Wireshark tool. Its answer is "529" packets.

Third question is "what the name of the pcap is.?". after the open pcap file we can see number of packets in the left-side bottom of Wireshark tool. Its answer is "fuzz-2006-08-27-19853.pcap" packets.



fuzz-2006-08-27-19853.pcap

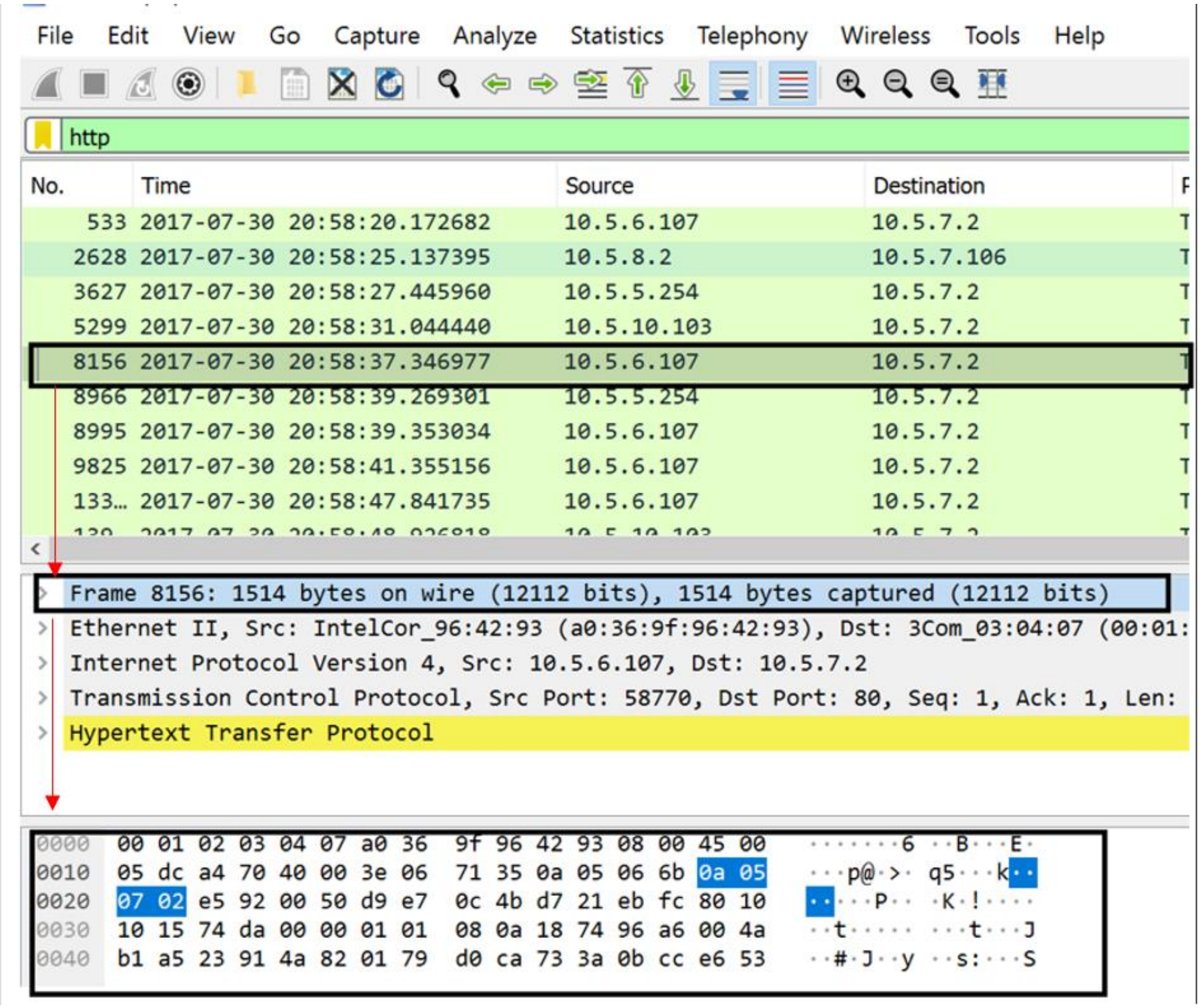
Packets: 529 · Displayed: 529 (100.0%)

Task 4 - Packet Dissection

Protocol dissection, another name for packet dissection, is the investigation of packet specifics through the decoding of accessible protocols and fields. This section explains the OSI layers and how Wireshark utilizes them to decompose packets for analysis. You should be familiar with the OSI model's principles and workings already.

Packet Detail

A packet's information may be seen by clicking on it in the packet list pane. Based on the OSI model, packets have 5 to 7 layers. In an HTTP packet from a sample capture, we will go through each one of them.



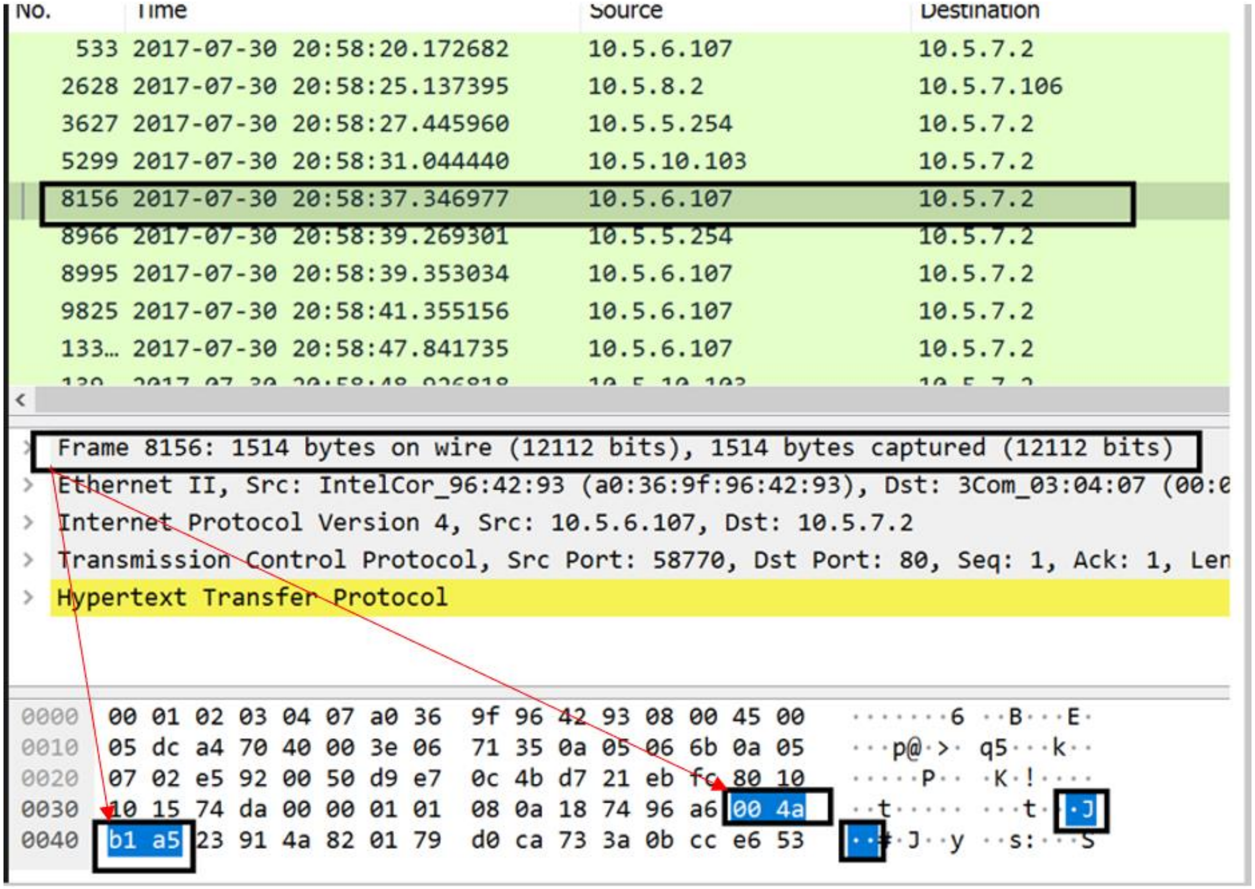
http

```
No.    Time                          Source         Destination    P
  533 2017-07-30 20:58:20.172682     10.5.6.107     10.5.7.2       T
 2628 2017-07-30 20:58:25.137395     10.5.8.2       10.5.7.106     T
 3627 2017-07-30 20:58:27.445960     10.5.5.254     10.5.7.2       T
 5299 2017-07-30 20:58:31.044440     10.5.10.103    10.5.7.2       T
 8156 2017-07-30 20:58:37.346977     10.5.6.107     10.5.7.2       T
 8966 2017-07-30 20:58:39.269301     10.5.5.254     10.5.7.2       T
 8995 2017-07-30 20:58:39.353034     10.5.6.107     10.5.7.2       T
 9825 2017-07-30 20:58:41.355156     10.5.6.107     10.5.7.2       T
 133… 2017-07-30 20:58:47.841735     10.5.6.107     10.5.7.2       T
 139… 2017-07-30 20:58:48.926818     10.5.10.103    10.5.7.2       T
```

```
> Frame 8156: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
> Ethernet II, Src: IntelCor_96:42:93 (a0:36:9f:96:42:93), Dst: 3Com_03:04:07 (00:01:
> Internet Protocol Version 4, Src: 10.5.6.107, Dst: 10.5.7.2
> Transmission Control Protocol, Src Port: 58770, Dst Port: 80, Seq: 1, Ack: 1, Len:
> Hypertext Transfer Protocol
```

```
0000  00 01 02 03 04 07 a0 36  9f 96 42 93 08 00 45 00   ·······6 ··B···E·
0010  05 dc a4 70 40 00 3e 06  71 35 0a 05 06 6b 0a 05   ···p@·>· q5···k··
0020  07 02 e5 92 00 50 d9 e7  0c 4b d7 21 eb fc 80 10   ·····P·· ·K·!····
0030  10 15 74 da 00 00 01 01  08 0a 18 74 96 a6 00 4a   ··t····· ···t···J
0040  b1 a5 23 91 4a 82 01 79  d0 ca 73 3a 0b cc e6 53   ··#·J··y ··s:···S
```

When you click a detail, the appropriate section of the packet bytes window is highlighted.



```
No.   Time                          Source          Destination
 533 2017-07-30 20:58:20.172682     10.5.6.107      10.5.7.2
2628 2017-07-30 20:58:25.137395     10.5.8.2        10.5.7.106
3627 2017-07-30 20:58:27.445960     10.5.5.254      10.5.7.2
5299 2017-07-30 20:58:31.044440     10.5.10.103     10.5.7.2
8156 2017-07-30 20:58:37.346977     10.5.6.107      10.5.7.2
8966 2017-07-30 20:58:39.269301     10.5.5.254      10.5.7.2
8995 2017-07-30 20:58:39.353034     10.5.6.107      10.5.7.2
9825 2017-07-30 20:58:41.355156     10.5.6.107      10.5.7.2
133… 2017-07-30 20:58:47.841735     10.5.6.107      10.5.7.2
139… 2017-07-30 20:58:48.926818     10.5.10.103     10.5.7.2
```

```
> Frame 8156: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
> Ethernet II, Src: IntelCor_96:42:93 (a0:36:9f:96:42:93), Dst: 3Com_03:04:07 (00:0
> Internet Protocol Version 4, Src: 10.5.6.107, Dst: 10.5.7.2
> Transmission Control Protocol, Src Port: 58770, Dst Port: 80, Seq: 1, Ack: 1, Len
> Hypertext Transfer Protocol
```

```
0000  00 01 02 03 04 07 a0 36  9f 96 42 93 08 00 45 00   ·······6 ··B···E·
0010  05 dc a4 70 40 00 3e 06  71 35 0a 05 06 6b 0a 05   ···p@·>· q5···k··
0020  07 02 e5 92 00 50 d9 e7  0c 4b d7 21 eb fc 80 10   ·····P·· ·K·!····
0030  10 15 74 da 00 00 01 01  08 0a 18 74 96 a6 00 4a   ··t····· ···t··J
0040  b1 a5 23 91 4a 82 01 79  d0 ca 73 3a 0b cc e6 53   ··#·J··y ··s:···S
```

Let's have a closer view of the details pane.

1.The Frame:

The information unique to the Physical layer of the OSI model will be displayed here, along with the frame or packet you are now viewing.

2.Source [MAC]:

From the OSI model's Data Link layer, this will display the source and destination MAC addresses.

3.Soruce [IP]:

According to the OSI model's Network layer, this will display the source and destination IPv4 addresses.

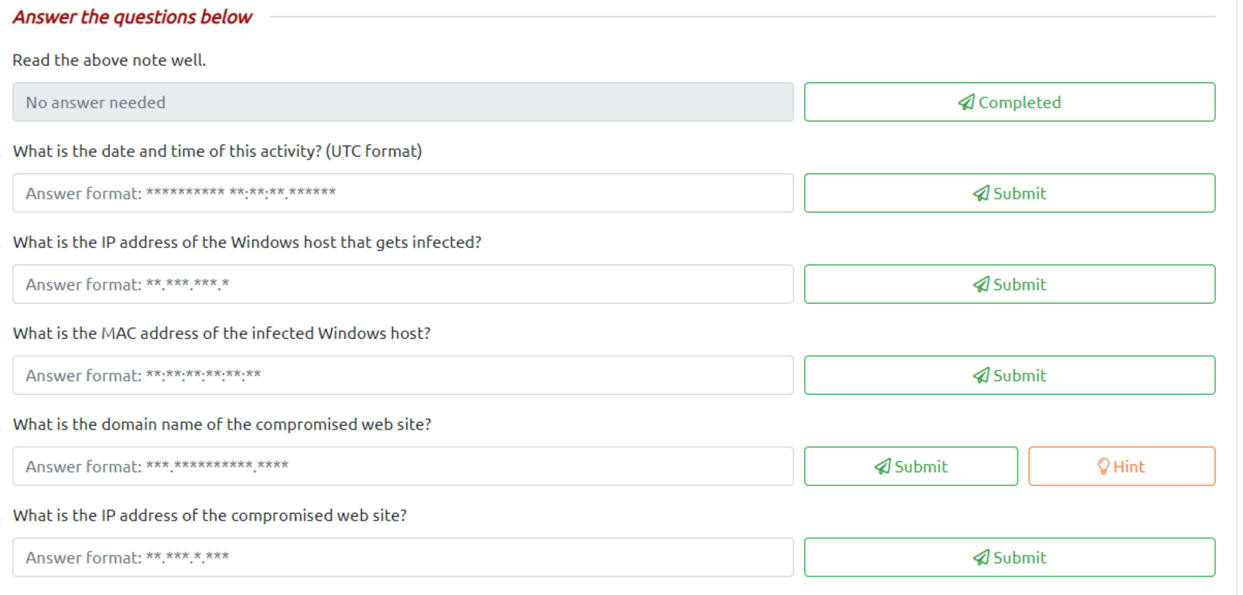
4.Protocol:

This will display information on the source and destination ports, as well as the UDP/TCP protocol used, according to the OSI model's Transport layer.

5.Application Protocol:

The specifics of the employed protocol, such as HTTP, FTP, and SMB, will be shown here. originating at the OSI model's Application layer.

There are 6 questions in the task 4.



Answer the questions below

Read the above note well.

No answer needed

. What is the date and time of this activity? (UTC format)

Answer format: ********** **:**:**.******

. What is the IP address of the Windows host that gets infected?

Answer format: **.***.***.*

. What is the MAC address of the infected Windows host?

Answer format: **:**:**:**:**:**

. What is the domain name of the compromised web site?

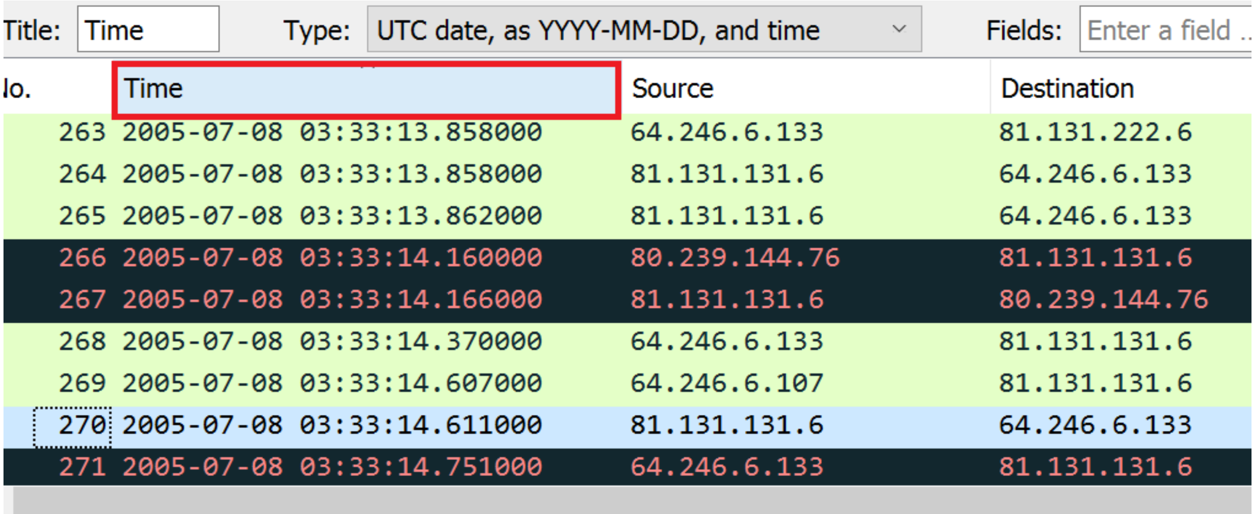
Answer format: ***.**********.****

. What is the IP address of the compromised web site?

Answer format: **.***.*.***

First one is read only question. Second one is “what is date and time of the activity?”. You can click the time column and click the edit column, after you can get the real time of UTC standard. Answer for that question “2005-07-28 03:33:15.097002”.

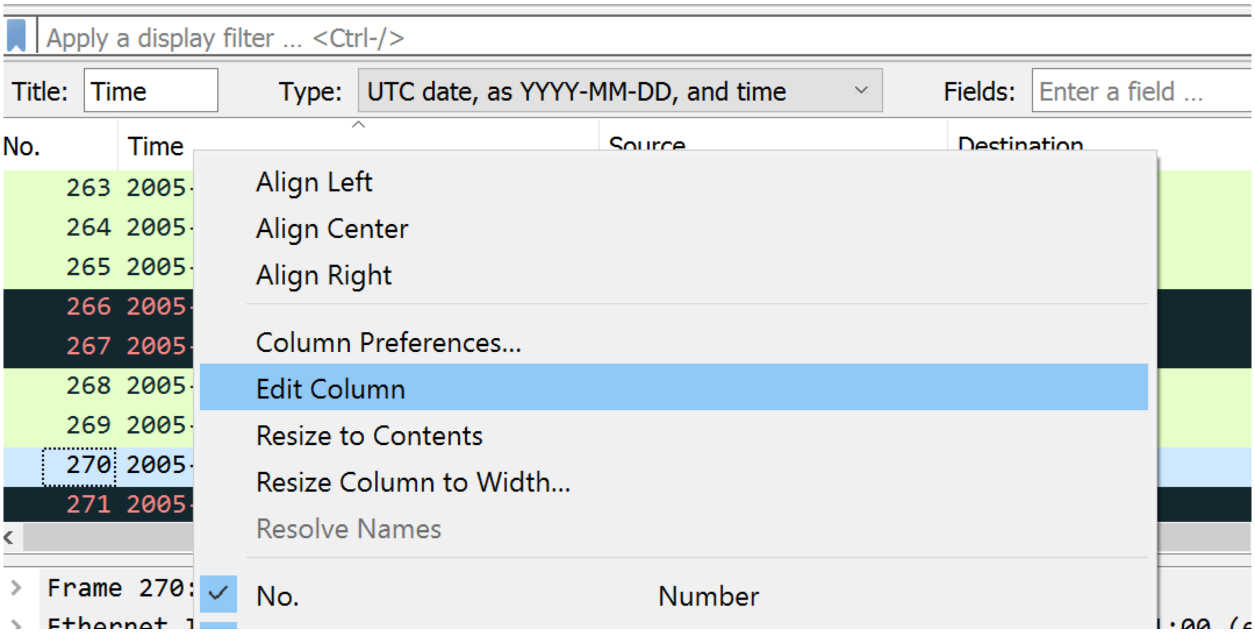
Step 1



Title: Time Type: UTC date, as YYYY-MM-DD, and time Fields: Enter a field ..

lo.	Time	Source	Destination
263	2005-07-08 03:33:13.858000	64.246.6.133	81.131.222.6
264	2005-07-08 03:33:13.858000	81.131.131.6	64.246.6.133
265	2005-07-08 03:33:13.862000	81.131.131.6	64.246.6.133
266	2005-07-08 03:33:14.160000	80.239.144.76	81.131.131.6
267	2005-07-08 03:33:14.166000	81.131.131.6	80.239.144.76
268	2005-07-08 03:33:14.370000	64.246.6.133	81.131.131.6
269	2005-07-08 03:33:14.607000	64.246.6.107	81.131.131.6
270	2005-07-08 03:33:14.611000	81.131.131.6	64.246.6.133
271	2005-07-08 03:33:14.751000	64.246.6.133	81.131.131.6

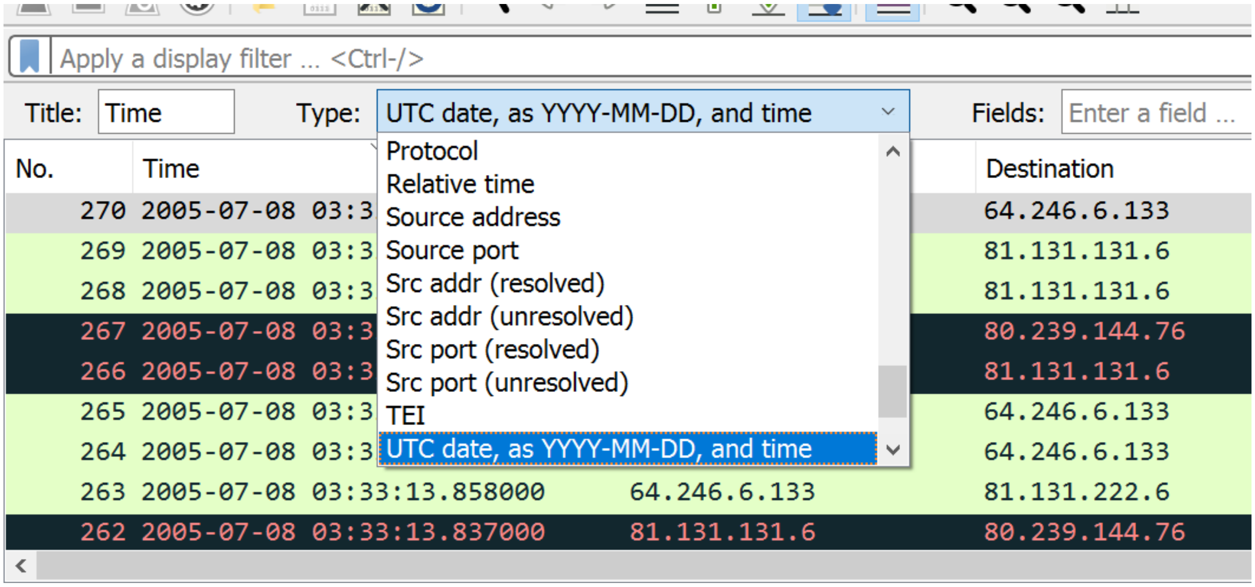
Step 2



Apply a display filter ... <Ctrl-/>

Title: Time Type: UTC date, as YYYY-MM-DD, and time Fields: Enter a field ...

Step 3



Apply a display filter ... <Ctrl-/>

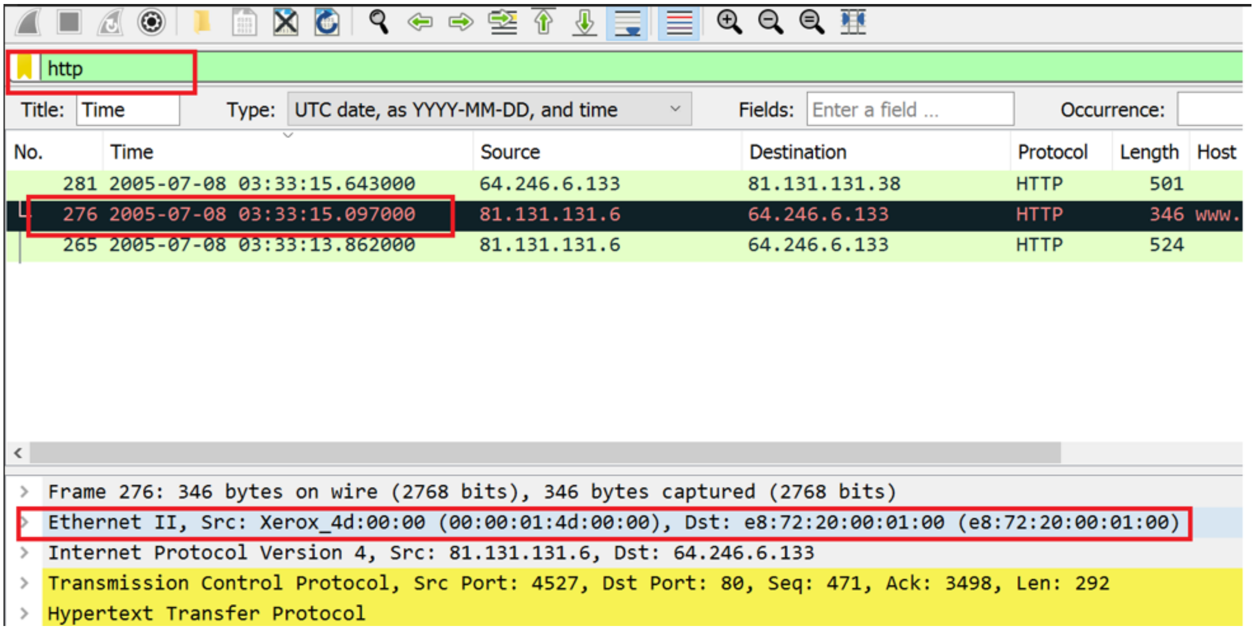
Title: Time   Type: UTC date, as YYYY-MM-DD, and time   Fields: Enter a field ...

No.	Time		Destination
270	2005-07-08 03:3		64.246.6.133
269	2005-07-08 03:3		81.131.131.6
268	2005-07-08 03:3		81.131.131.6
267	2005-07-08 03:3		80.239.144.76
266	2005-07-08 03:3		81.131.131.6
265	2005-07-08 03:3		64.246.6.133
264	2005-07-08 03:3		64.246.6.133
263	2005-07-08 03:33:13.858000	64.246.6.133	81.131.222.6
262	2005-07-08 03:33:13.837000	81.131.131.6	80.239.144.76

Third question is “What is the IP address of the Windows host that gets infected?”. Its answer is “81.131.131.6”. It can be gotten by “source” column.

Fourth question is “What is the MAC address of the infected Windows host?”. We can filter the “http” and go to packet detail part and expand ethernet part. Now we can get MAC address.MAC address is “ 00:00:01:4d:00:00”.

Step 1



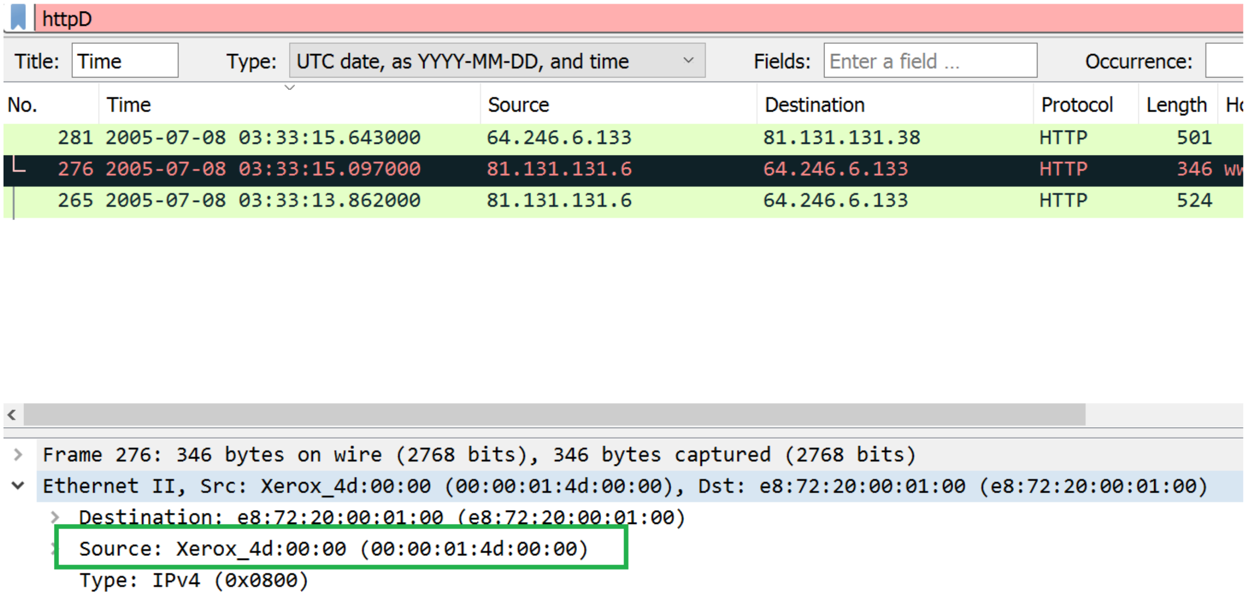
http

Title: Time Type: UTC date, as YYYY-MM-DD, and time Fields: Enter a field ... Occurrence:

```
No.  Time                        Source          Destination     Protocol  Length  Host
 281 2005-07-08 03:33:15.643000  64.246.6.133    81.131.131.38   HTTP      501
 276 2005-07-08 03:33:15.097000  81.131.131.6    64.246.6.133    HTTP      346 www.
 265 2005-07-08 03:33:13.862000  81.131.131.6    64.246.6.133    HTTP      524
```

```
> Frame 276: 346 bytes on wire (2768 bits), 346 bytes captured (2768 bits)
> Ethernet II, Src: Xerox_4d:00:00 (00:00:01:4d:00:00), Dst: e8:72:20:00:01:00 (e8:72:20:00:01:00)
> Internet Protocol Version 4, Src: 81.131.131.6, Dst: 64.246.6.133
> Transmission Control Protocol, Src Port: 4527, Dst Port: 80, Seq: 471, Ack: 3498, Len: 292
> Hypertext Transfer Protocol
```

Step 2



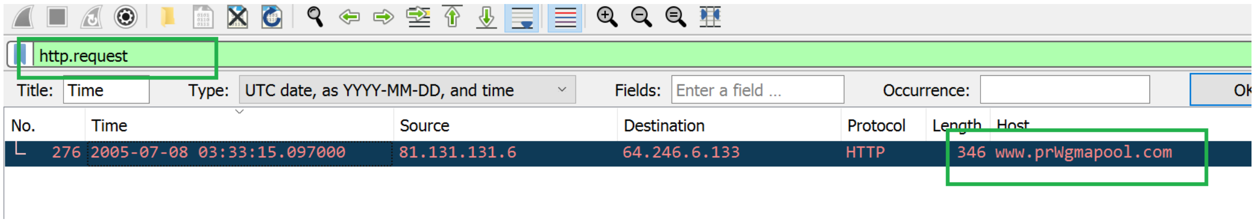
httpD

Title: Time Type: UTC date, as YYYY-MM-DD, and time Fields: Enter a field ... Occurrence:

```
No.  Time                        Source          Destination     Protocol  Length  H
 281 2005-07-08 03:33:15.643000  64.246.6.133    81.131.131.38   HTTP      501
 276 2005-07-08 03:33:15.097000  81.131.131.6    64.246.6.133    HTTP      346 ww
 265 2005-07-08 03:33:13.862000  81.131.131.6    64.246.6.133    HTTP      524
```

```
> Frame 276: 346 bytes on wire (2768 bits), 346 bytes captured (2768 bits)
v Ethernet II, Src: Xerox_4d:00:00 (00:00:01:4d:00:00), Dst: e8:72:20:00:01:00 (e8:72:20:00:01:00)
   > Destination: e8:72:20:00:01:00 (e8:72:20:00:01:00)
   > Source: Xerox_4d:00:00 (00:00:01:4d:00:00)
     Type: IPv4 (0x0800)
```

Fifth question is “What is the domain name of the compromised web site?”. we can use “http. Request” and get directly answer of this question. Answer for this question “www.prWgmapool.com”.



http.request

Title: Time   Type: UTC date, as YYYY-MM-DD, and time   Fields: Enter a field ...   Occurrence: Ok

No.	Time	Source	Destination	Protocol	Length	Host
276	2005-07-08 03:33:15.097000	81.131.131.6	64.246.6.133	HTTP	346	www.prWgmapool.com

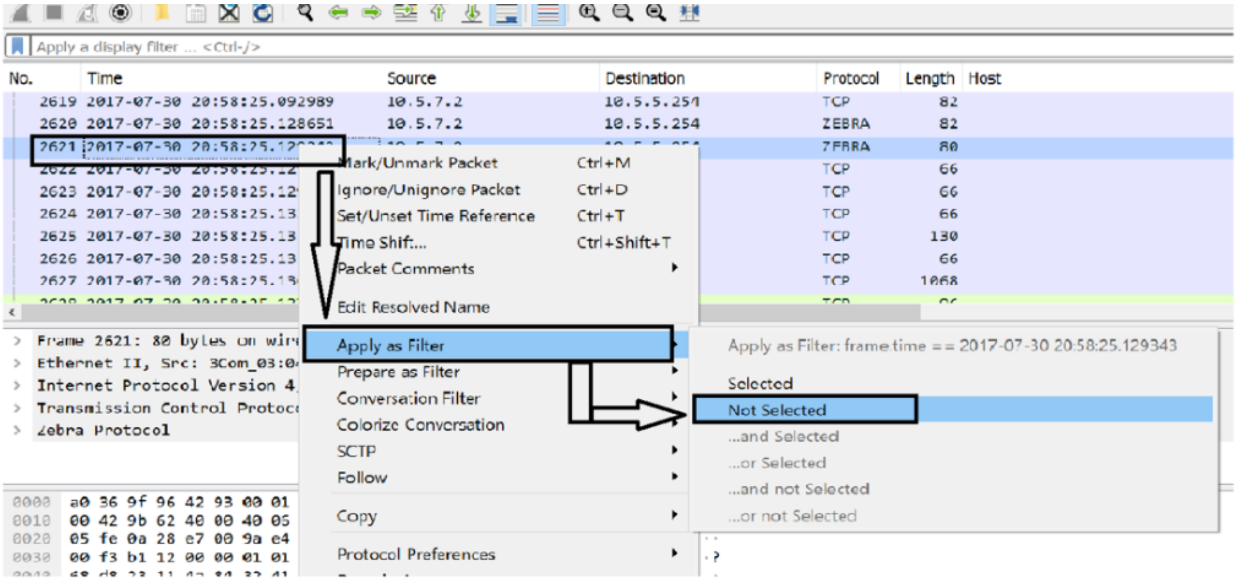
Last question is “What is the IP address of the compromised web site?”. that IP address visible on the “Destination” column. Answer for this question “64.246.6.133”.

Task 5 - Filtering of packet

The robust filter engine in Wireshark enables analysts to focus on the relevant events by reducing the volume of traffic. Both capture filters and display filters are available in Wireshark. Only valid packets for the chosen filter are "captured" by capture filters. For "seeing" the packets that are valid for the selected filter, display filters are utilized. In the room next to us, we'll talk about the variations and sophisticated applications of these filters. Let's now concentrate on the fundamental use of the display filters, which will first benefit analysts. Filters are queries created for protocols included in Wireshark's official protocol reference. While there are two techniques to filter traffic and eliminate noise from the capture file, filters are merely an option to examine the event of interest. In the first, queries are used, whereas in the second, the right-click menu is used.

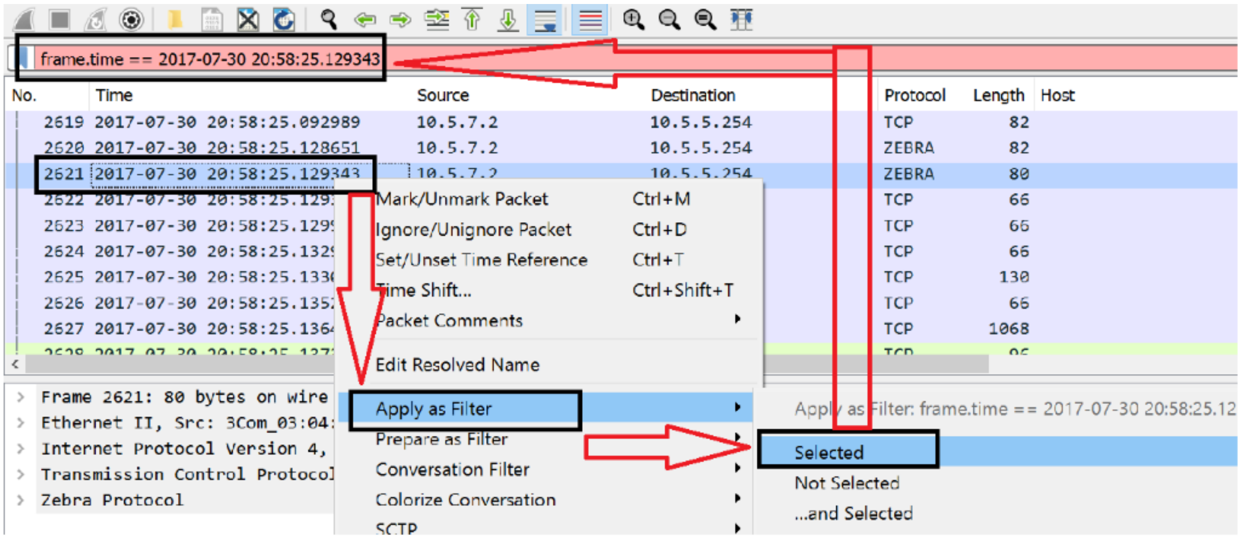
The simplest method of filtering traffic is as described here. You may utilize the "right-click menu" or "Analyze --> Apply as Filter" option while looking through a capture file to filter a specific value by clicking on the field you wish to filter. Following the application of the filter, Wireshark will create the necessary filter query, use it, display the packets in accordance with your selections, and conceal the unselected packets from view in the packet list window. Keep in mind that the status bar always displays the total number of packets and the number of visible packets.

Part 1



```
Apply a display filter ... <Ctrl-/>

No.   Time                        Source        Destination    Protocol  Length  Host
 2619 2017-07-30 20:58:25.092989  10.5.7.2      10.5.5.254     TCP           82
 2620 2017-07-30 20:58:25.128651  10.5.7.2      10.5.5.254     ZEBRA         82
 2621 2017-07-30 20:58:25.12                                   ZEBRA         80
                                                               TCP           66
 2623 2017-07-30 20:58:25.12                                   TCP           66
 2624 2017-07-30 20:58:25.13                                   TCP           66
 2625 2017-07-30 20:58:25.13                                   TCP          130
 2626 2017-07-30 20:58:25.13                                   TCP           66
 2627 2017-07-30 20:58:25.13                                   TCP         1068

> Frame 2621: 80 bytes on wir
> Ethernet II, Src: 3Com_03:0
> Internet Protocol Version 4
> Transmission Control Protoc
> Zebra Protocol

0000  a0 36 9f 96 42 93 00 01
0010  00 42 9b 62 40 00 40 05
0020  05 fe 0a 28 e7 00 9a e4
0030  00 f3 b1 12 00 00 01 01
```

Part 2

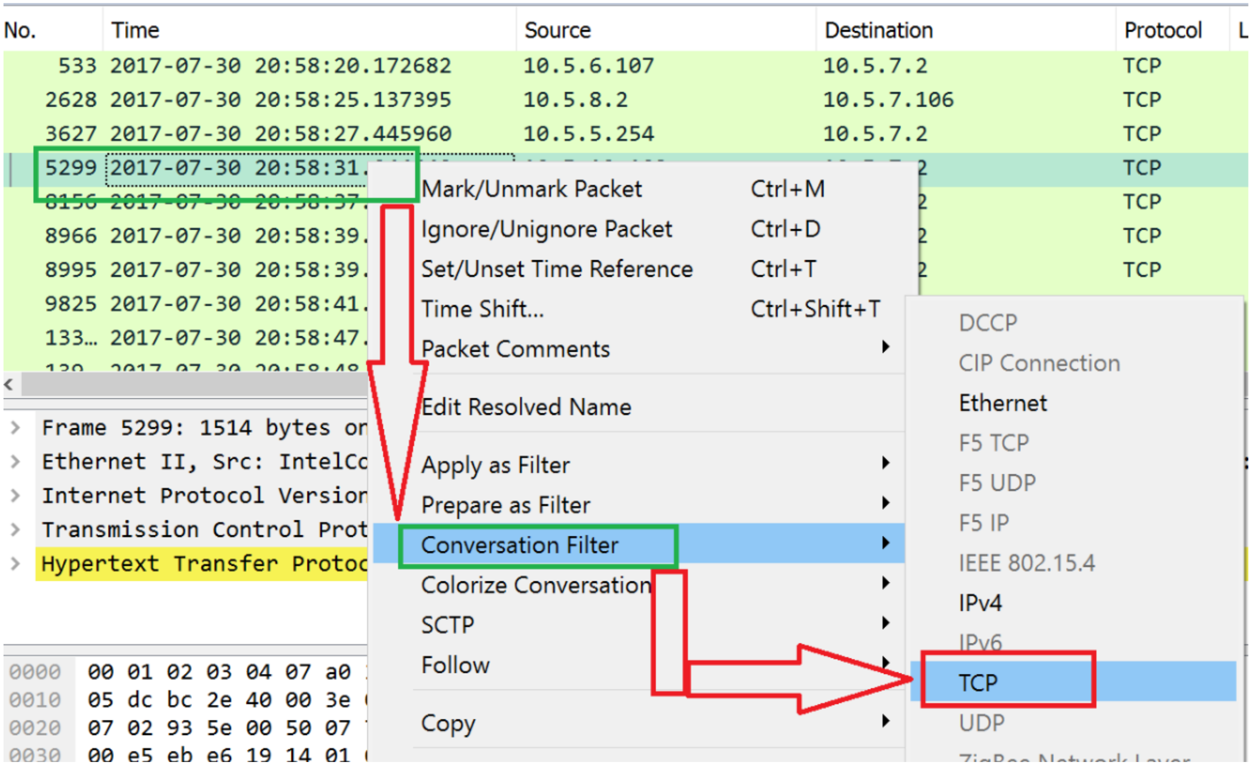


```
frame.time == 2017-07-30 20:58:25.129343

No.   Time                        Source        Destination    Protocol  Length  Host
 2619 2017-07-30 20:58:25.092989  10.5.7.2      10.5.5.254     TCP           82
 2620 2017-07-30 20:58:25.128651  10.5.7.2      10.5.5.254     ZEBRA         82
 2621 2017-07-30 20:58:25.129343  10.5.7.2      10.5.5.254     ZEBRA         80
 2622 2017-07-30 20:58:25.129                                  TCP           66
 2623 2017-07-30 20:58:25.129                                  TCP           66
 2624 2017-07-30 20:58:25.132                                  TCP           66
 2625 2017-07-30 20:58:25.133                                  TCP          130
 2626 2017-07-30 20:58:25.135                                  TCP           66
 2627 2017-07-30 20:58:25.136                                  TCP         1068

> Frame 2621: 80 bytes on wire
> Ethernet II, Src: 3Com_03:04:
> Internet Protocol Version 4,
> Transmission Control Protocol
> Zebra Protocol
```

Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Apply as Filter: frame.time == 2017-07-30 20:58:25.12
Selected
Not Selected
...and Selected

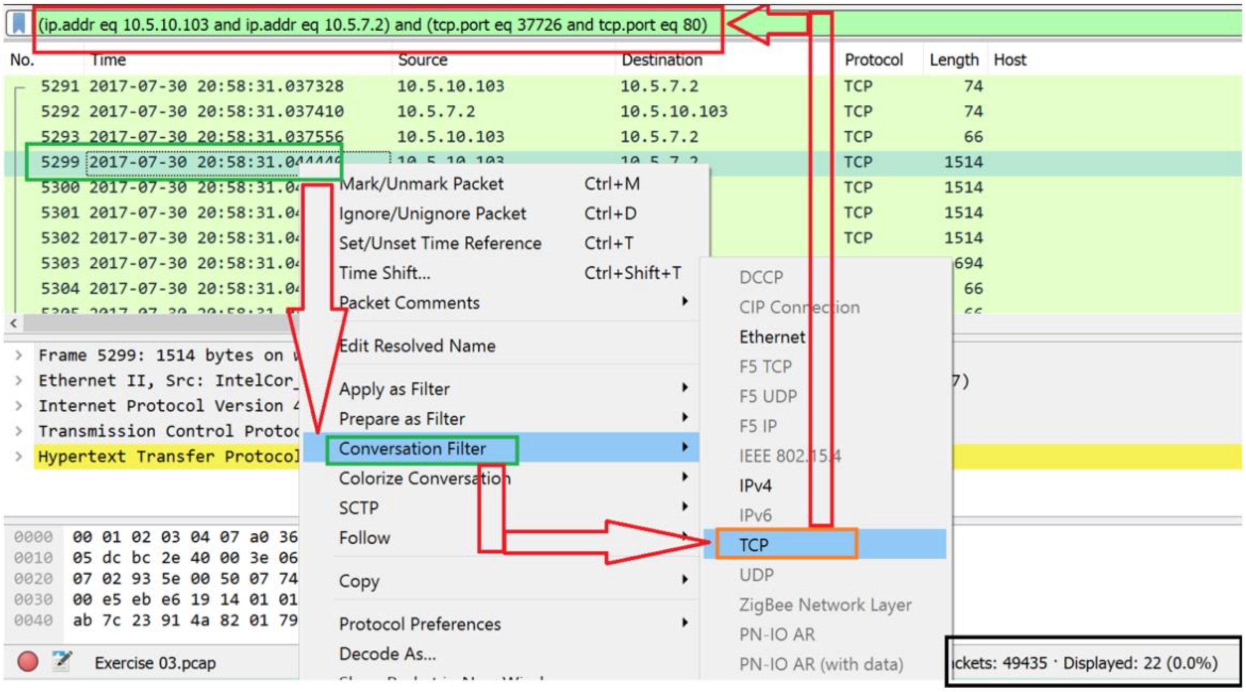
Only one entity of the packet will be filtered when you choose the "Apply as a Filter" option. A handy technique to examine a specific value in packets is by using this option. Imagine, however, that you wish to focus on IP addresses and port numbers to examine a certain packet number and all associated packets. With the "Conversation Filter" option, you may quickly inspect only while hiding the others. To filter chats, select "Analyze --> Conversation Filter" from the menu options or utilize the "right-click menu. The packets that are relevant

Part 1



```
No.   Time                             Source         Destination    Protocol
  533 2017-07-30 20:58:20.172682       10.5.6.107     10.5.7.2       TCP
 2628 2017-07-30 20:58:25.137395       10.5.8.2       10.5.7.106     TCP
 3627 2017-07-30 20:58:27.445960       10.5.5.254     10.5.7.2       TCP
 5299 2017-07-30 20:58:31.                               2           TCP
 8156 2017-07-30 20:58:37.                               2           TCP
 8966 2017-07-30 20:58:39.                               2           TCP
 8995 2017-07-30 20:58:39.                               2           TCP
 9825 2017-07-30 20:58:41.
 133… 2017-07-30 20:58:47.

> Frame 5299: 1514 bytes or
> Ethernet II, Src: IntelCo
> Internet Protocol Version
> Transmission Control Prot
> Hypertext Transfer Protoc

0000  00 01 02 03 04 07 a0
0010  05 dc bc 2e 40 00 3e
0020  07 02 93 5e 00 50 07
0030  00 e5 eb e6 19 14 01
```

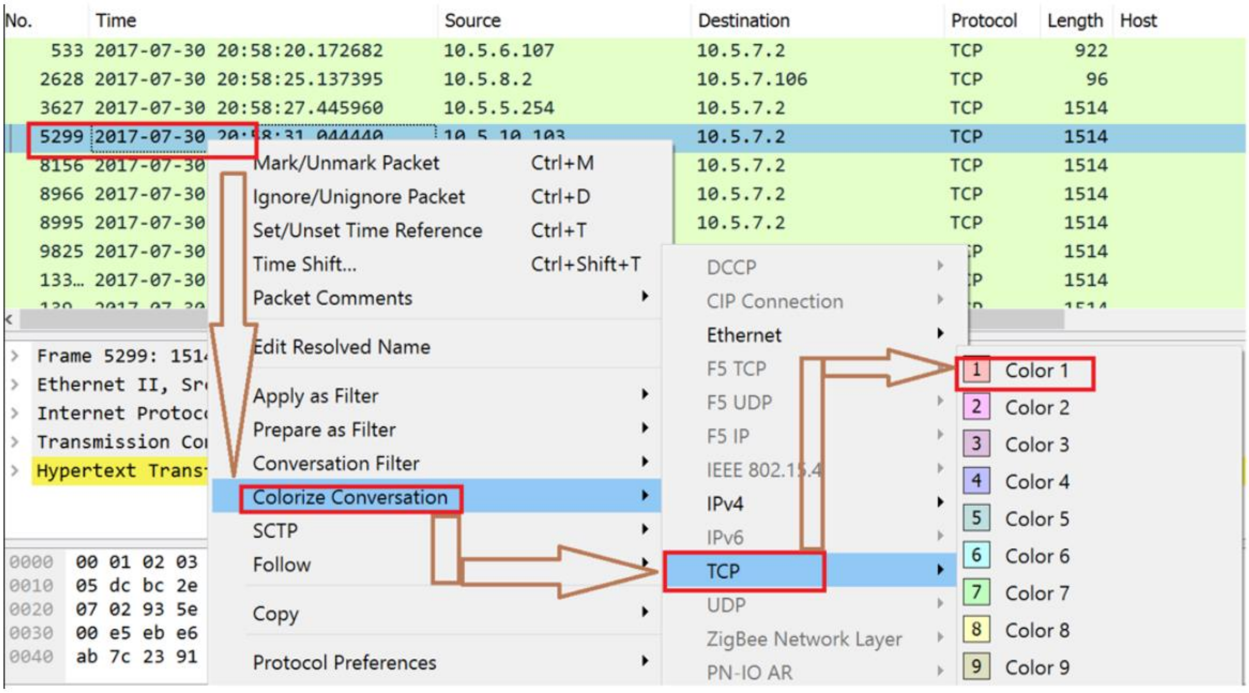
Part 2



```
(ip.addr eq 10.5.10.103 and ip.addr eq 10.5.7.2) and (tcp.port eq 37726 and tcp.port eq 80)

No.   Time                        Source         Destination    Protocol  Length  Host
5291  2017-07-30 20:58:31.037328  10.5.10.103    10.5.7.2       TCP           74
5292  2017-07-30 20:58:31.037410  10.5.7.2       10.5.10.103    TCP           74
5293  2017-07-30 20:58:31.037556  10.5.10.103    10.5.7.2       TCP           66
5299  2017-07-30 20:58:31.04444(  10.5.10.103    10.5.7.2       TCP         1514
5300  2017-07-30 20:58:31.0(                                    TCP         1514
5301  2017-07-30 20:58:31.0(                                    TCP         1514
5302  2017-07-30 20:58:31.0(                                    TCP         1514
5303  2017-07-30 20:58:31.0(                                                 694
5304  2017-07-30 20:58:31.0(                                                  66

> Frame 5299: 1514 bytes on w
> Ethernet II, Src: IntelCor_
> Internet Protocol Version 4
> Transmission Control Protoc
> Hypertext Transfer Protocol

0000  00 01 02 03 04 07 a0 36
0010  05 dc bc 2e 40 00 3e 06
0020  07 02 93 5e 00 50 07 74
0030  00 e5 eb e6 19 14 01 01
0040  ab 7c 23 91 4a 82 01 79

Exercise 03.pcap          ckets: 49435 · Displayed: 22 (0.0%)
```

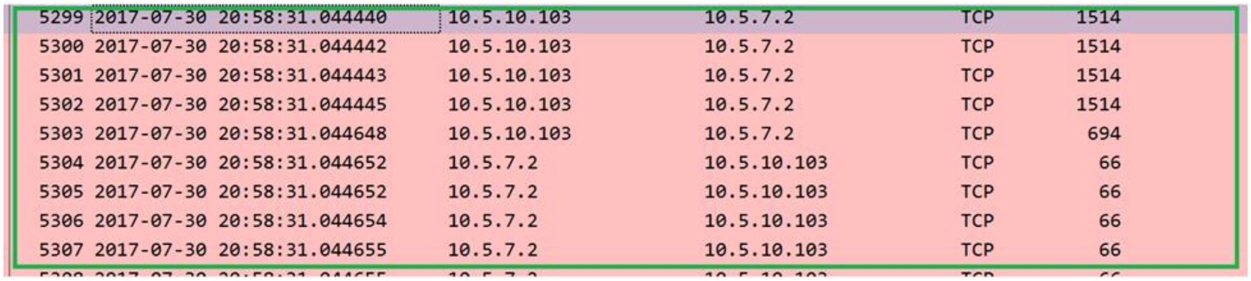
now that the discourse has taken on some color Except for one change, this option is comparable to the "Conversation Filter." Without using a display filter, it emphasizes the related packets and reduces the number of packets that are being shown. This option alters the packet colors without considering the previously used color rule. It works with the "Colouring Rules" option. With only one click, you can colorize a connected packet using the "right-click menu" or "View --> Colourise Conversation" option. You may reverse this action by selecting "View --> Colourise Conversation --> Reset Colourisation" from the menu.

Part1



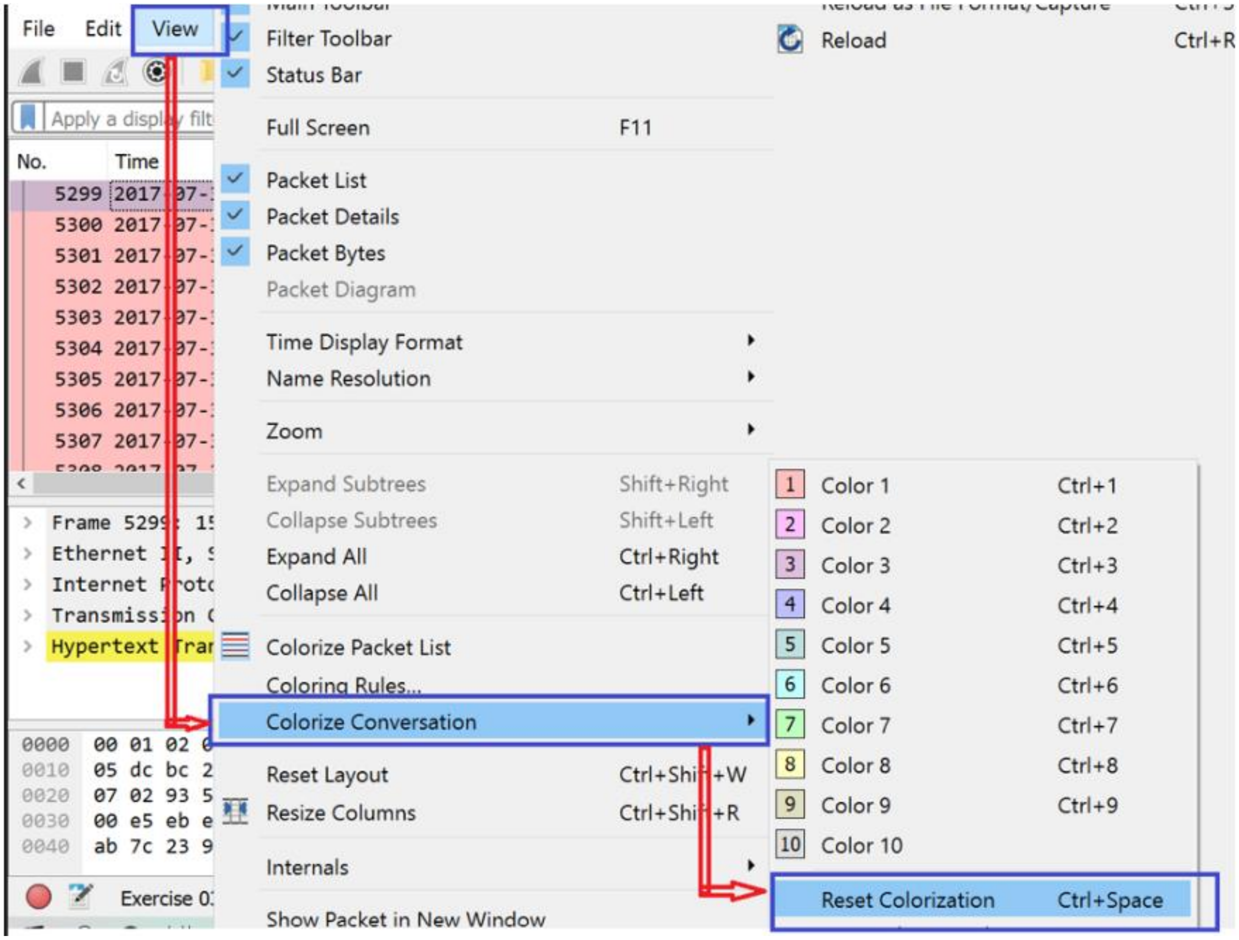
```
No.   Time                          Source         Destination   Protocol  Length  Host
  533 2017-07-30 20:58:20.172682    10.5.6.107     10.5.7.2      TCP          922
 2628 2017-07-30 20:58:25.137395    10.5.8.2       10.5.7.106    TCP           96
 3627 2017-07-30 20:58:27.445960    10.5.5.254     10.5.7.2      TCP         1514
 5299 2017-07-30 20:58:31.044440    10.5.10.103    10.5.7.2      TCP         1514
 8156 2017-07-30                                   10.5.7.2      TCP         1514
 8966 2017-07-30                                   10.5.7.2      TCP         1514
 8995 2017-07-30                                   10.5.7.2      TCP         1514
 9825 2017-07-30                                                             1514
 133… 2017-07-30                                                             1514

> Frame 5299: 151
> Ethernet II, Sr
> Internet Protoc
> Transmission Co
> Hypertext Trans

0000  00 01 02 03
0010  05 dc bc 2e
0020  07 02 93 5e
0030  00 e5 eb e6
0040  ab 7c 23 91
```

Part 2

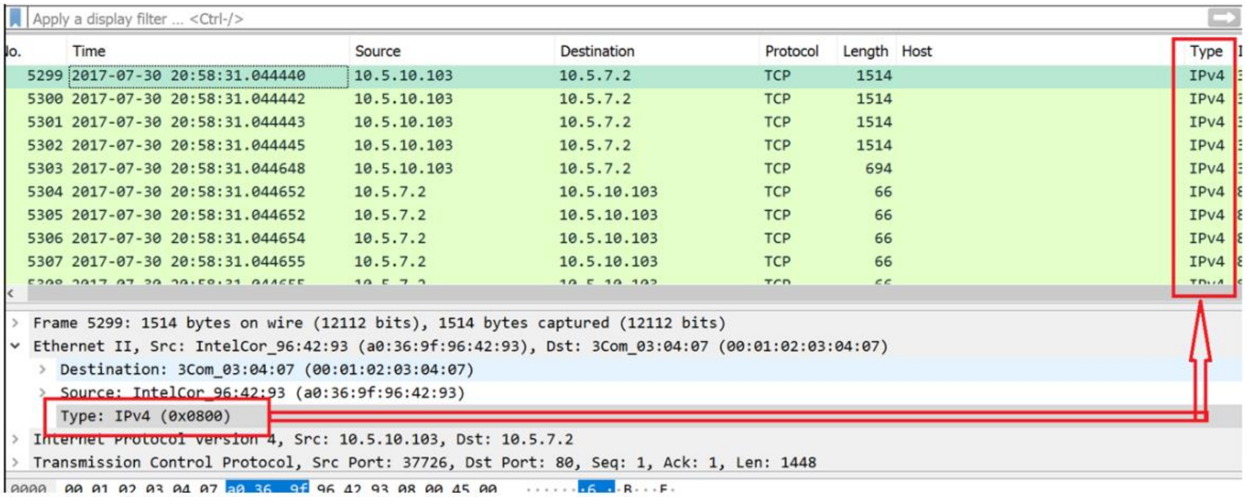


```
 5299 2017-07-30 20:58:31.044440    10.5.10.103    10.5.7.2      TCP         1514
 5300 2017-07-30 20:58:31.044442    10.5.10.103    10.5.7.2      TCP         1514
 5301 2017-07-30 20:58:31.044443    10.5.10.103    10.5.7.2      TCP         1514
 5302 2017-07-30 20:58:31.044445    10.5.10.103    10.5.7.2      TCP         1514
 5303 2017-07-30 20:58:31.044648    10.5.10.103    10.5.7.2      TCP          694
 5304 2017-07-30 20:58:31.044652    10.5.7.2       10.5.10.103   TCP           66
 5305 2017-07-30 20:58:31.044652    10.5.7.2       10.5.10.103   TCP           66
 5306 2017-07-30 20:58:31.044654    10.5.7.2       10.5.10.103   TCP           66
 5307 2017-07-30 20:58:31.044655    10.5.7.2       10.5.10.103   TCP           66
```

Part 3


File
Edit
View
Apply a display filt
No.
Time
5299 2017-07-
5300 2017-07-
5301 2017-07-
5302 2017-07-
5303 2017-07-
5304 2017-07-
5305 2017-07-
5306 2017-07-
5307 2017-07-
Frame 5299: 15
Ethernet II,
Internet Proto
Transmission
Hypertext Trar
0000 00 01 02
0010 05 dc bc 2
0020 07 02 93 5
0030 00 e5 eb e
0040 ab 7c 23 9
Exercise 0
Filter Toolbar
Status Bar
Full Screen F11
Packet List
Packet Details
Packet Bytes
Packet Diagram
Time Display Format
Name Resolution
Zoom
Expand Subtrees Shift+Right
Collapse Subtrees Shift+Left
Expand All Ctrl+Right
Collapse All Ctrl+Left
Colorize Packet List
Coloring Rules...
Colorize Conversation
Reset Layout Ctrl+Shift+W
Resize Columns Ctrl+Shift+R
Internals
Show Packet in New Window
Reload Ctrl+R
1 Color 1 Ctrl+1
2 Color 2 Ctrl+2
3 Color 3 Ctrl+3
4 Color 4 Ctrl+4
5 Color 5 Ctrl+5
6 Color 6 Ctrl+6
7 Color 7 Ctrl+7
8 Color 8 Ctrl+8
9 Color 9 Ctrl+9
10 Color 10
Reset Colorization Ctrl+Space

Part 4



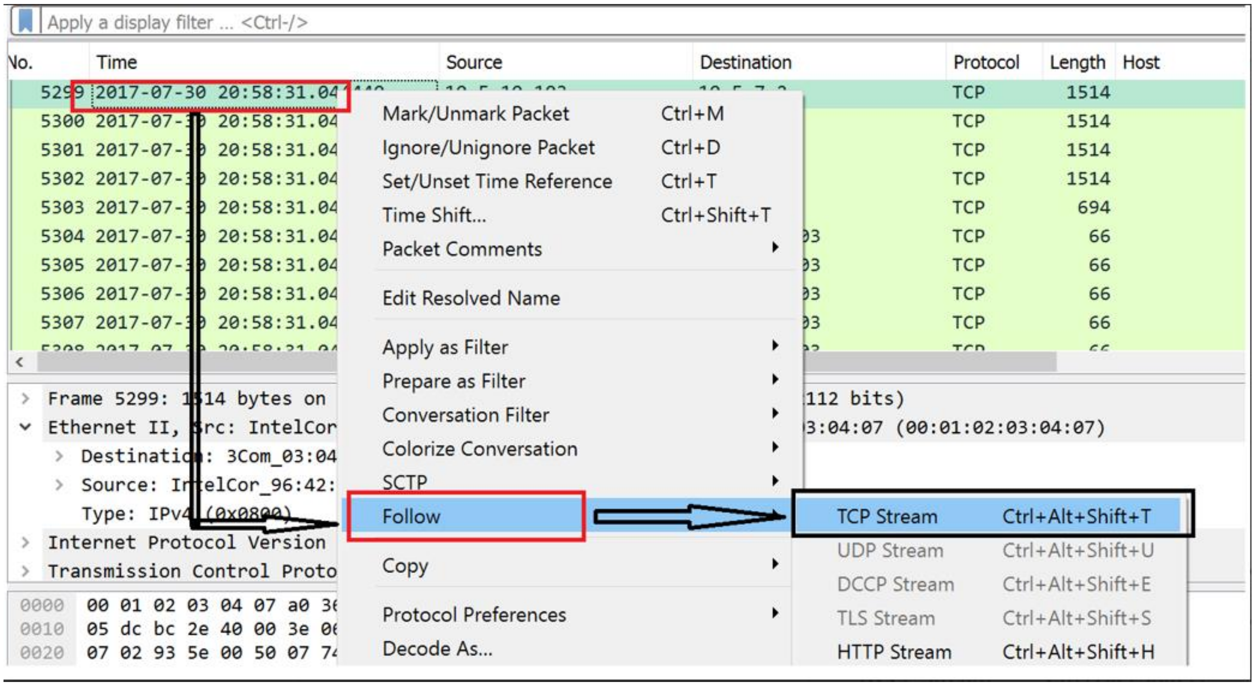
No.	Time	Source	Destination	Protocol	Length	Host	Type
5299	2017-07-30 20:58:31.044440	10.5.10.103	10.5.7.2	TCP	1514		IPv4
5300	2017-07-30 20:58:31.044442	10.5.10.103	10.5.7.2	TCP	1514		IPv4
5301	2017-07-30 20:58:31.044443	10.5.10.103	10.5.7.2	TCP	1514		IPv4
5302	2017-07-30 20:58:31.044445	10.5.10.103	10.5.7.2	TCP	1514		IPv4
5303	2017-07-30 20:58:31.044648	10.5.10.103	10.5.7.2	TCP	694		IPv4
5304	2017-07-30 20:58:31.044652	10.5.7.2	10.5.10.103	TCP	66		IPv4
5305	2017-07-30 20:58:31.044652	10.5.7.2	10.5.10.103	TCP	66		IPv4
5306	2017-07-30 20:58:31.044654	10.5.7.2	10.5.10.103	TCP	66		IPv4
5307	2017-07-30 20:58:31.044655	10.5.7.2	10.5.10.103	TCP	66		IPv4
5308	2017-07-30 20:58:31.044655	10.5.7.2	10.5.10.103	TCP	66		IPv4

```
> Frame 5299: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
v Ethernet II, Src: IntelCor_96:42:93 (a0:36:9f:96:42:93), Dst: 3Com_03:04:07 (00:01:02:03:04:07)
  > Destination: 3Com_03:04:07 (00:01:02:03:04:07)
  > Source: IntelCor_96:42:93 (a0:36:9f:96:42:93)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 10.5.10.103, Dst: 10.5.7.2
> Transmission Control Protocol, Src Port: 37726, Dst Port: 80, Seq: 1, Ack: 1, Len: 1448
0000  00 01 02 03 04 07 a0 36  9f 96 42 93 08 00 45 00   ······6··B···E·
```

Everything is shown in packet chunk size in Wireshark. However, it is feasible to rebuild the streams and see the unprocessed traffic as it is shown at the application level. Streams that adhere to the protocol assist analysts in recreating the application-level data and comprehending the relevant event. Additionally, the unencrypted protocol data, including usernames, passwords, and other exchanged data, may be seen.

To track traffic streams, utilize the "right-click menu" or "Analyze --> Follow TCP/UDP/HTTP Stream" option. Streams are displayed in a separate dialogue box; packets coming from the server are marked in blue, while those coming from the client are highlighted in red.

Part 1



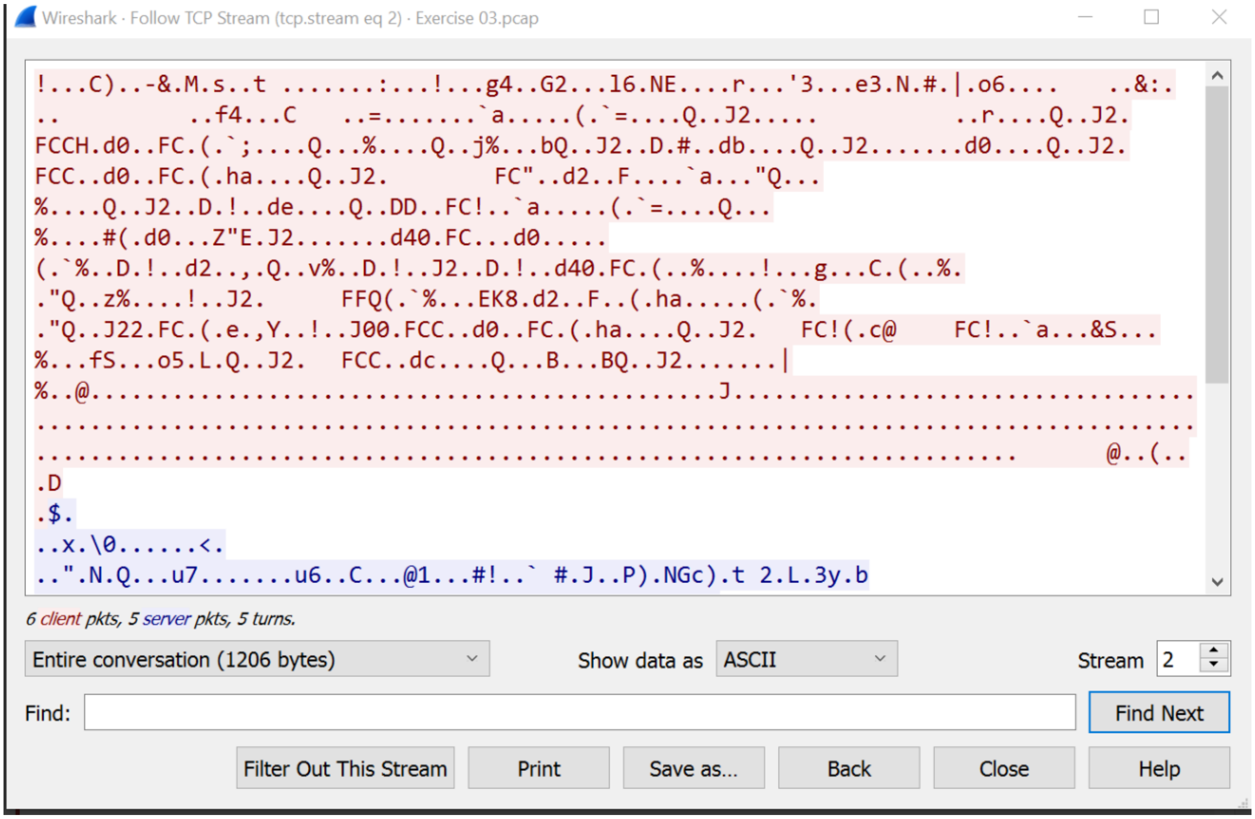
No.	Time	Source	Destination	Protocol	Length	Host
5299	2017-07-30 20:58:31.04			TCP	1514	
5300	2017-07-30 20:58:31.04			TCP	1514	
5301	2017-07-30 20:58:31.04			TCP	1514	
5302	2017-07-30 20:58:31.04			TCP	1514	
5303	2017-07-30 20:58:31.04			TCP	694	
5304	2017-07-30 20:58:31.04		03	TCP	66	
5305	2017-07-30 20:58:31.04		03	TCP	66	
5306	2017-07-30 20:58:31.04		03	TCP	66	
5307	2017-07-30 20:58:31.04		03	TCP	66	

```
> Frame 5299: 1514 bytes on                             112 bits)
v Ethernet II, Src: IntelCor                           3:04:07 (00:01:02:03:04:07)
   > Destination: 3Com_03:04
   > Source: IntelCor_96:42:
     Type: IPv4 (0x0800)
> Internet Protocol Version
> Transmission Control Proto
```

```
0000  00 01 02 03 04 07 a0 36
0010  05 dc bc 2e 40 00 3e 06
0020  07 02 93 5e 00 50 07 74
```

Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
DCCP Stream Ctrl+Alt+Shift+E
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H

Part 2



Wireshark · Follow TCP Stream (tcp.stream eq 2) · Exercise 03.pcap

```
!...C)..-&.M.s..t .......:...!...g4..G2...l6.NE....r...'3...e3.N.#.|.o6....   ..&:.
..          ..f4...C    ..=.......`a.....(.`=....Q..J2.....          ..r....Q..J2.
FCCH.d0..FC.(.`;....Q...%....Q..j%...bQ..J2..D.#..db....Q..J2.......d0....Q..J2.
FCC..d0..FC.(.ha....Q..J2.       FC"..d2..F....`a..."Q...
%....Q..J2..D.!..de....Q..DD..FC!..`a.....(.`=....Q...
%....#(.d0...Z"E.J2.......d40.FC...d0.....
(.`%..D.!..d2..,.Q..v%..D.!..J2..D.!..d40.FC.(..%....!...g...C.(..%.
."Q..z%....!..J2.     FFQ(.`%...EK8.d2..F..(.ha.....(.`%.
."Q..J22.FC.(.e.,Y..!..J00.FCC..d0..FC.(.ha....Q..J2.   FC!(.c@    FC!..`a...&S...
%...fS...o5.L.Q..J2.   FCC..dc....Q...B...BQ..J2.......|
%..@...............................................J..................................
......................................................................................
........................................................................      @..(..
.D
.$.
..x.\0......<.
..".N.Q...u7.......u6..C...@1...#!..` #.J..P).NGc).t 2.L.3y.b
```

6 client pkts, 5 server pkts, 5 turns.

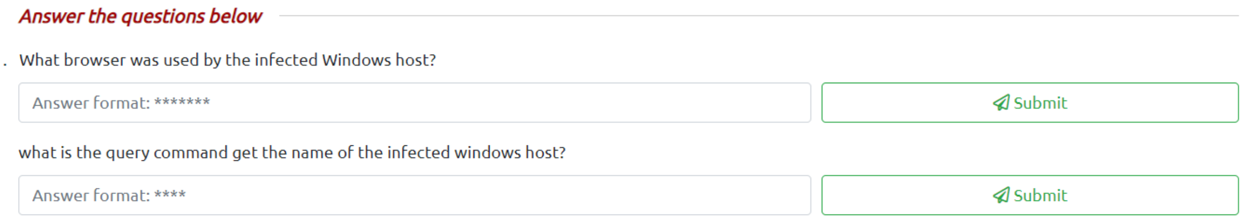
Entire conversation (1206 bytes)

Show data as ASCII

Stream 2

Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

There are 5 questions in the task 5.



Answer the questions below

. What browser was used by the infected Windows host?

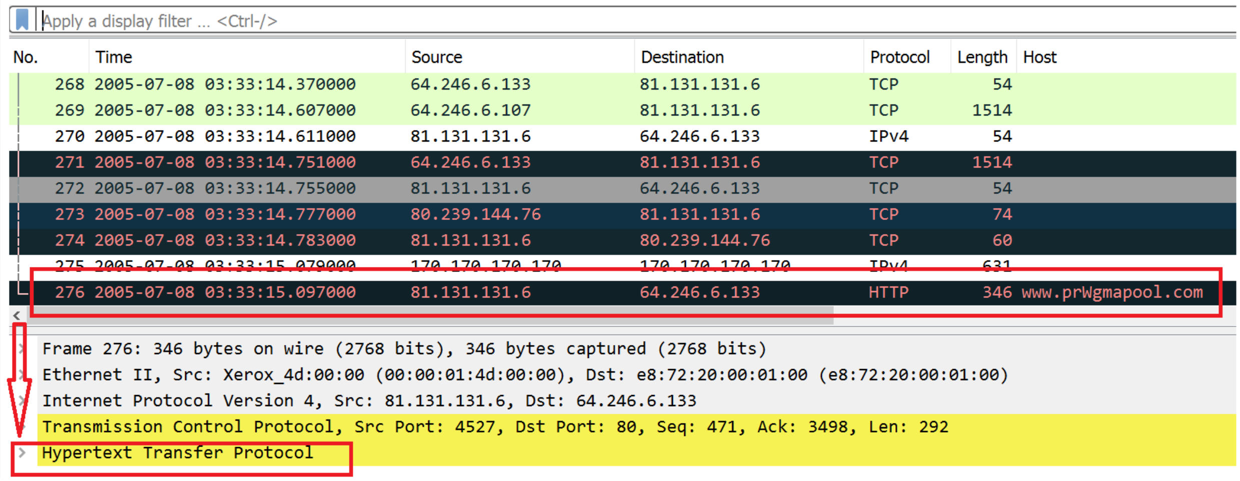
Answer format: *******

what is the query command get the name of the infected windows host?

Answer format: ****

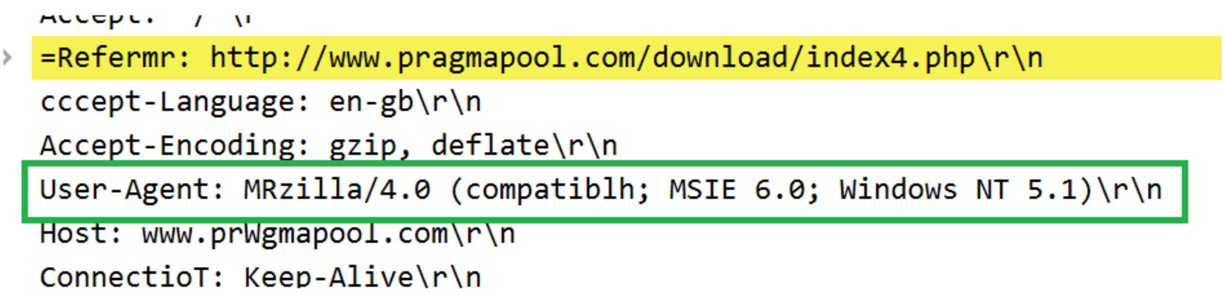
First one is “What browser was used by the infected Windows host?”. we can click the respective packet and after going to packet detail section. It has “Hypertext transfer protocol section”. It is drop down section. In that section has “User agent” part. User agent is browser of the infected windows host. That question answer is “MRzilla”.

Step 1



```
Apply a display filter ... <Ctrl-/>
No.  Time                        Source           Destination      Protocol  Length  Host
 268 2005-07-08 03:33:14.370000  64.246.6.133     81.131.131.6     TCP         54
 269 2005-07-08 03:33:14.607000  64.246.6.107     81.131.131.6     TCP       1514
 270 2005-07-08 03:33:14.611000  81.131.131.6     64.246.6.133     IPv4        54
 271 2005-07-08 03:33:14.751000  64.246.6.133     81.131.131.6     TCP       1514
 272 2005-07-08 03:33:14.755000  81.131.131.6     64.246.6.133     TCP         54
 273 2005-07-08 03:33:14.777000  80.239.144.76    81.131.131.6     TCP         74
 274 2005-07-08 03:33:14.783000  81.131.131.6     80.239.144.76    TCP         60
 275 2005-07-08 03:33:15.079000  170.170.170.170  170.170.170.170  IPv4       631
 276 2005-07-08 03:33:15.097000  81.131.131.6     64.246.6.133     HTTP       346 www.prWgmapool.com

> Frame 276: 346 bytes on wire (2768 bits), 346 bytes captured (2768 bits)
> Ethernet II, Src: Xerox_4d:00:00 (00:00:01:4d:00:00), Dst: e8:72:20:00:01:00 (e8:72:20:00:01:00)
> Internet Protocol Version 4, Src: 81.131.131.6, Dst: 64.246.6.133
> Transmission Control Protocol, Src Port: 4527, Dst Port: 80, Seq: 471, Ack: 3498, Len: 292
> Hypertext Transfer Protocol
```

Step 2



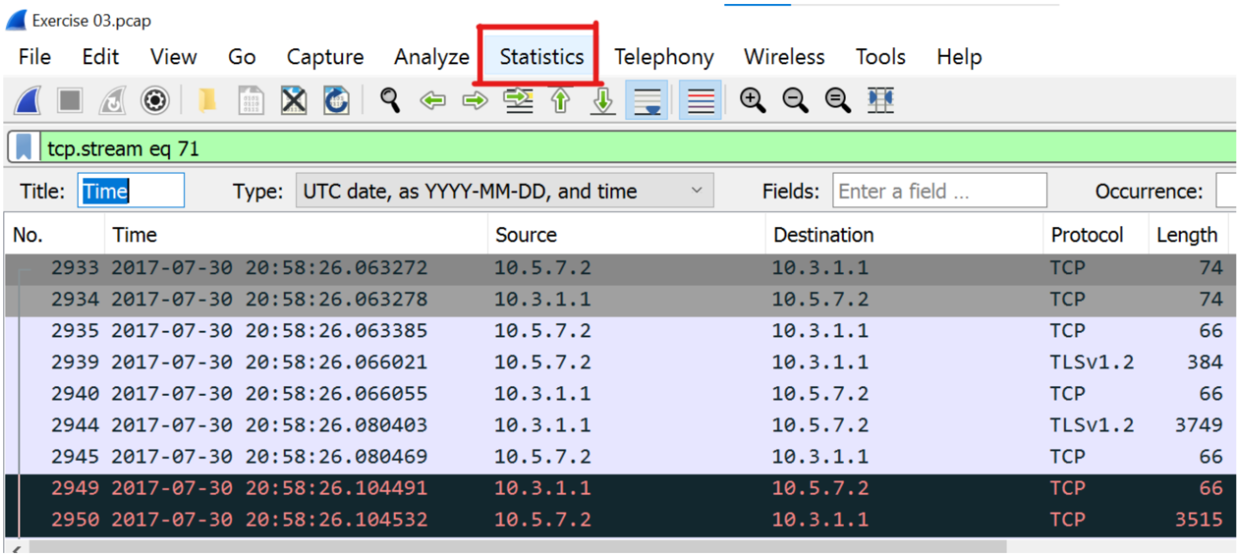
```
  Accept: */*\r\n
> =Refermr: http://www.pragmapool.com/download/index4.php\r\n
  cccept-Language: en-gb\r\n
  Accept-Encoding: gzip, deflate\r\n
  User-Agent: MRzilla/4.0 (compatiblh; MSIE 6.0; Windows NT 5.1)\r\n
  Host: www.prWgmapool.com\r\n
  ConnectioT: Keep-Alive\r\n
```

Second question is “what is the query command get the name of the infected windows host?”. We can get name of the infected windows host from using “dhcp” protocol or “nbns” protocol. If We use DHCP protocol. Now we should filter as the ‘dhcp’. DHCP is dynamic host control protocol. Now select we want IP address and go to the frame detail. After click on the “dynamic host configuration protocol”. now we go to under that path host name option and get the host name.

Task 6 - Static Analyzing of packet

We can get the more accurate information about our packet using the static tab. we can go to static tab and right on it. after it will visible the menu. we can click the capture file properties or ctrl+alt+shift+c.

Step 1

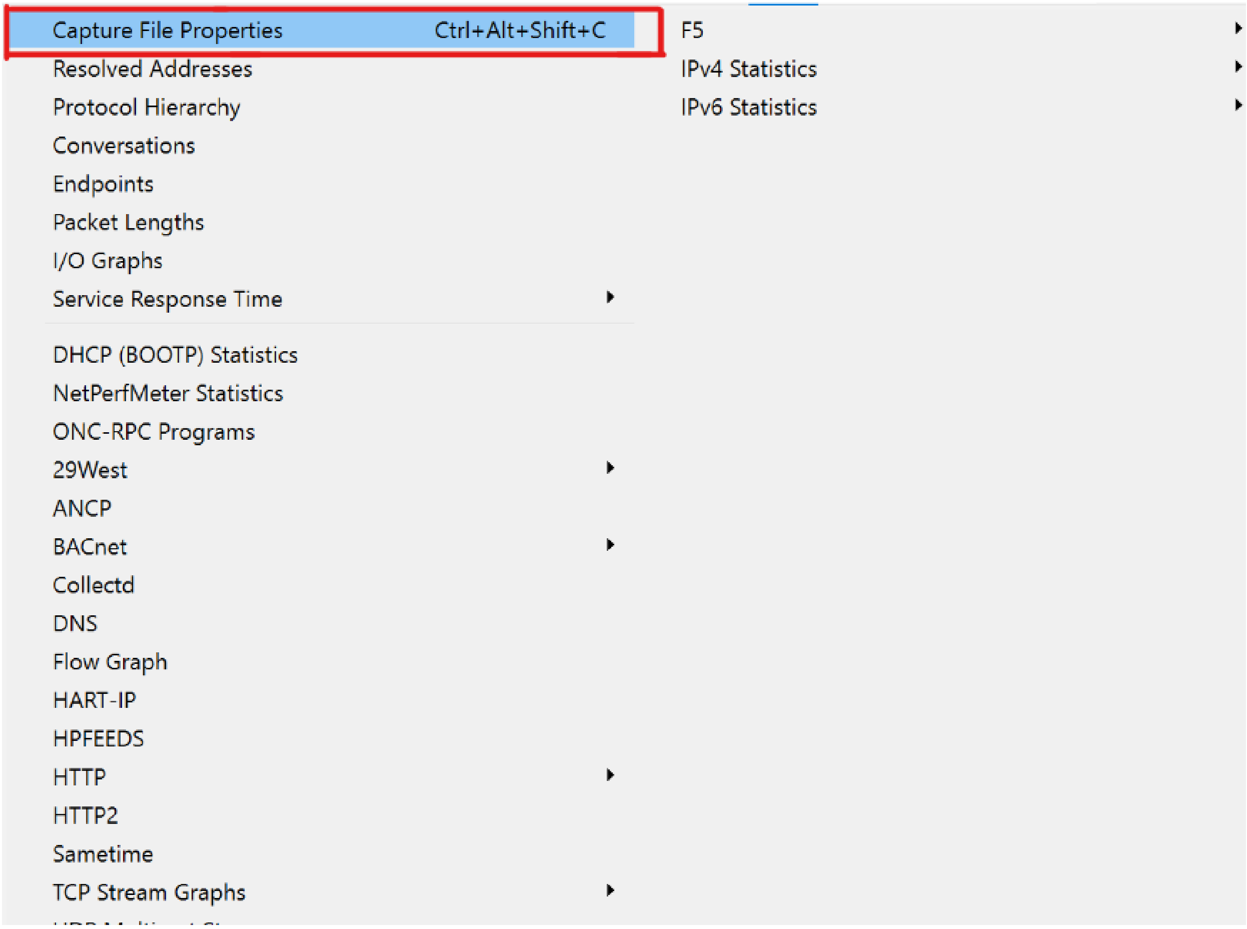


tcp.stream eq 71

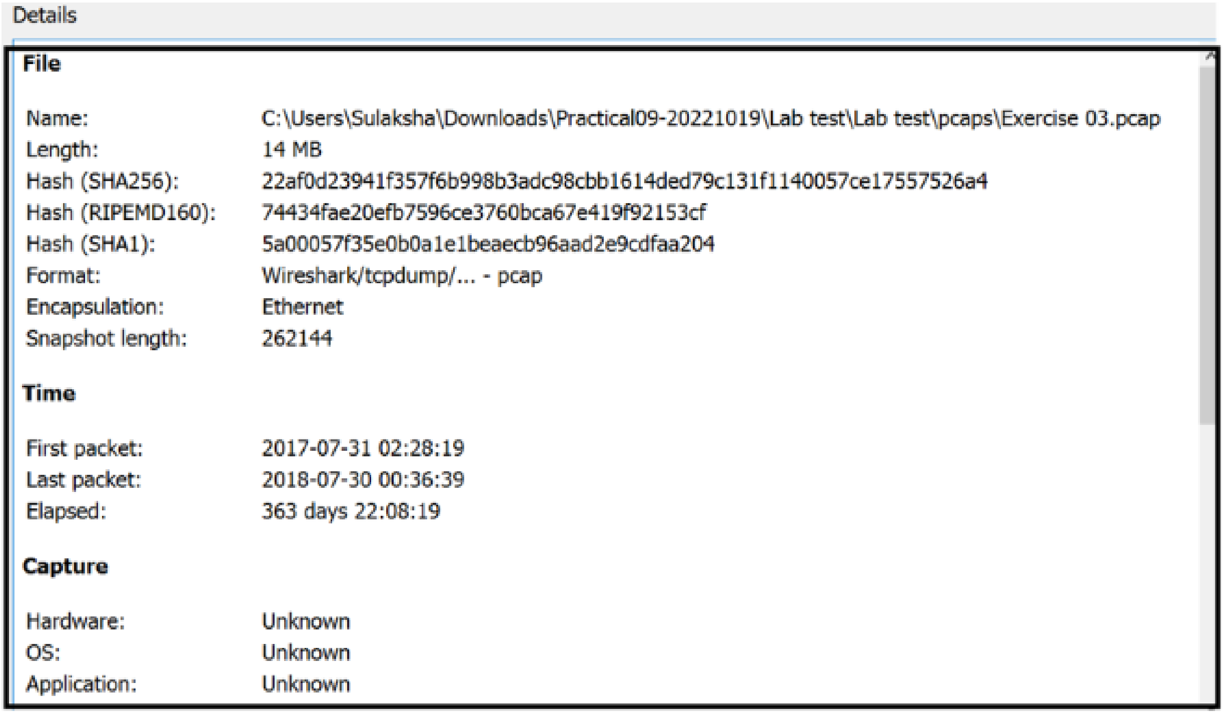
Title: Time Type: UTC date, as YYYY-MM-DD, and time Fields: Enter a field ... Occurrence:

No.	Time	Source	Destination	Protocol	Length
2933	2017-07-30 20:58:26.063272	10.5.7.2	10.3.1.1	TCP	74
2934	2017-07-30 20:58:26.063278	10.3.1.1	10.5.7.2	TCP	74
2935	2017-07-30 20:58:26.063385	10.5.7.2	10.3.1.1	TCP	66
2939	2017-07-30 20:58:26.066021	10.5.7.2	10.3.1.1	TLSv1.2	384
2940	2017-07-30 20:58:26.066055	10.3.1.1	10.5.7.2	TCP	66
2944	2017-07-30 20:58:26.080403	10.3.1.1	10.5.7.2	TLSv1.2	3749
2945	2017-07-30 20:58:26.080469	10.5.7.2	10.3.1.1	TCP	66
2949	2017-07-30 20:58:26.104491	10.3.1.1	10.5.7.2	TCP	66
2950	2017-07-30 20:58:26.104532	10.5.7.2	10.3.1.1	TCP	3515

Step 2


Capture File Properties Ctrl+Alt+Shift+C
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graphs
Service Response Time
DHCP (BOOTP) Statistics
NetPerfMeter Statistics
ONC-RPC Programs
29West
ANCP
BACnet
Collectd
DNS
Flow Graph
HART-IP
HPFEEDS
HTTP
HTTP2
Sametime
TCP Stream Graphs
F5
IPv4 Statistics
IPv6 Statistics

Step 3



Details

File

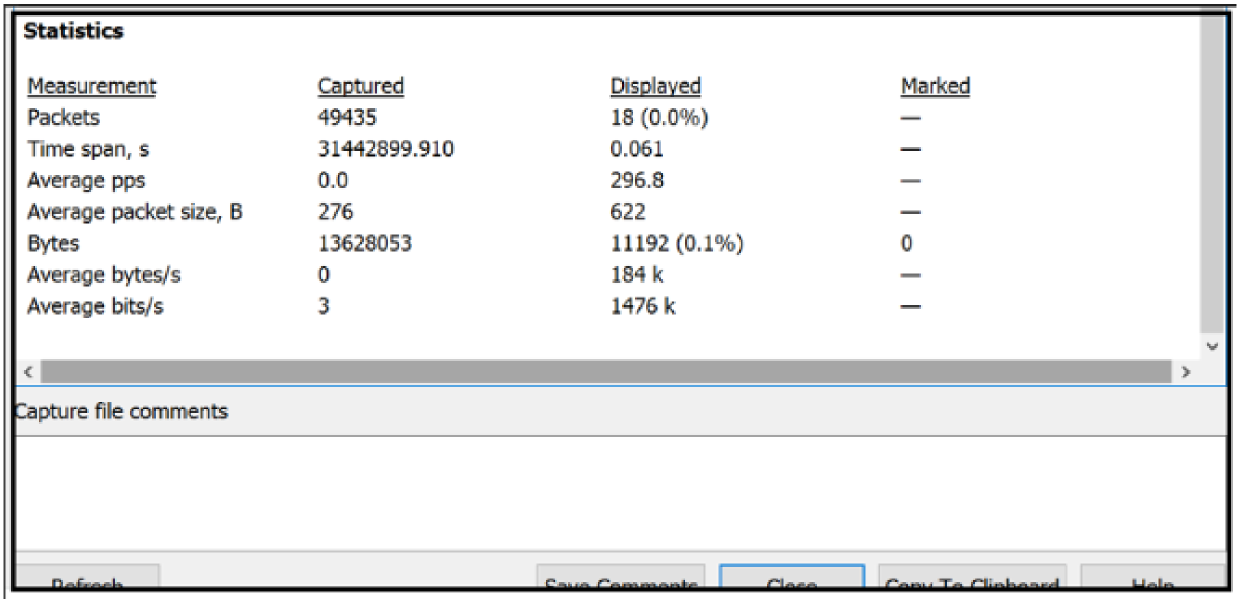
Name:	C:\Users\Sulaksha\Downloads\Practical09-20221019\Lab test\Lab test\pcaps\Exercise 03.pcap
Length:	14 MB
Hash (SHA256):	22af0d23941f357f6b998b3adc98cbb1614ded79c131f1140057ce17557526a4
Hash (RIPEMD160):	74434fae20efb7596ce3760bca67e419f92153cf
Hash (SHA1):	5a00057f35e0b0a1e1beaecb96aad2e9cdfaa204
Format:	Wireshark/tcpdump/... - pcap
Encapsulation:	Ethernet
Snapshot length:	262144

Time

First packet:	2017-07-31 02:28:19
Last packet:	2018-07-30 00:36:39
Elapsed:	363 days 22:08:19

Capture

Hardware:	Unknown
OS:	Unknown
Application:	Unknown

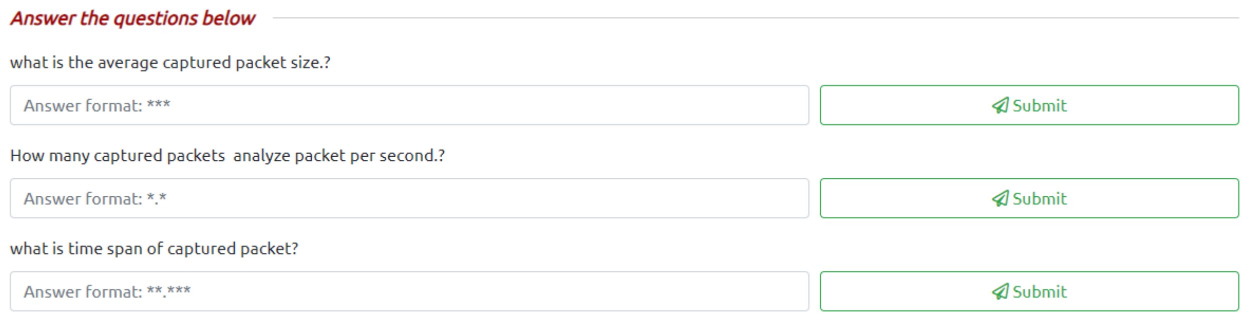


Statistics

Measurement	Captured	Displayed	Marked
Packets	49435	18 (0.0%)	—
Time span, s	31442899.910	0.061	—
Average pps	0.0	296.8	—
Average packet size, B	276	622	—
Bytes	13628053	11192 (0.1%)	0
Average bytes/s	0	184 k	—
Average bits/s	3	1476 k	—

Capture file comments

There are 3 questions in the task 6.



Answer the questions below

what is the average captured packet size.?

Answer format: ***

How many captured packets analyze packet per second.?

Answer format: *.*

what is time span of captured packet?

Answer format: **.***

First question is “what is the average captured packet size.?”. We can go to static tab and go to the “captured file propertise”.it will be visible the there are four parts. They are file, time, capture, statics. Under the static part, average capture packet size visible. That question answer is “386”.

Second question is “How many captured packets analyze packet per second.?”. Under the static part also included captured packets analyze packet per second. That question answer is “6.6”.

Third question is “what is time span of captured packet?”. Under the static part also included time span of captured packet. That question answer is “80.279”.

Task 7 - How to View the Contents of a Pcap File on The Linux Command Line

If you use Linux, it's probable that you are familiar with the pcap file format. This file format is used to store network data using tools for packet sniffing like Wireshark. The tcpdump tool may be used on the Linux command line to browse through a pcap file's contents.

You may explore the content of pcap files using the command-line tool tcpdump. When using tcpdump, you must pick the pcap file you want to read and the output format.

If you want to view the content of a pcap file ASCII format, you should use the following command:

```
tcpdump -A -r pcap_file
```

If you want to view the content of a pcap file hexadecimal format, you should use the following command:

```
Tcpdump -x -r pcap_file
```

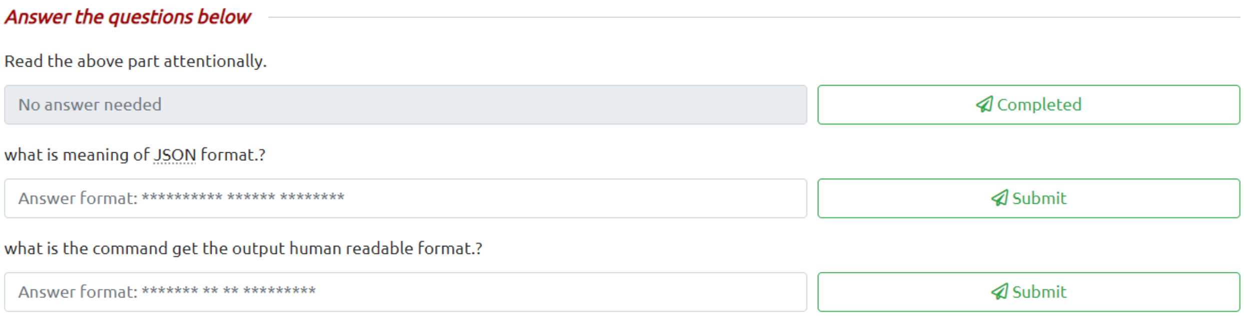
If you want to view the content of a pcap file human readable format, you should use the following command:

tcpdump -e -r pcap_file

If you want to view the content of a pcap file JSON format, You should use the following command:

tcpdump -j -r pcap_file

There are 3 questions in the task 7.



Answer the questions below

Read the above part attentionally.

No answer needed

what is meaning of JSON format.?

Answer format: ********** ****** ********

what is the command get the output human readable format.?

Answer format: ******* ** ** *********

First one is “read only question”. Second one is “what is meaning of JSON format?”. Its answer is “JavaScript Object Notation”.

Third question is “what is the command get the output human readable format?”. If you read that task description, you can find easily answer for this question, That question answer is “tcpdump -e -r pcap_file”.

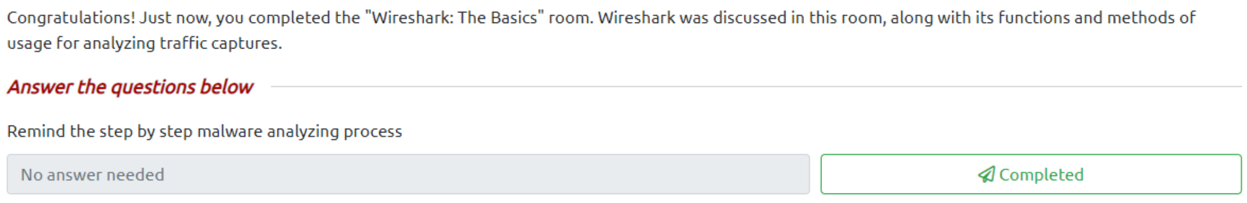
Task 8 – Conclusion

Numerous features of Wireshark allow to evaluate a wide range of network issues, including both internal and external attacks that take many different forms. These issues include those brought on by both inadequate configuration and device failures.

The first stage in resolving network difficulties is a thorough analysis of traffic for the sections or locations that have worse performance or just stop working completely. Making network administrators aware of the value of using this kind of tool is a good idea because it can be a useful tool to find the source of some issues that would take a long time to find using other methods, with the implications that come with it in terms of availability and information confidentiality taking priority over the rest of your services. This book details various ways of using Wireshark to analyze traffic, depending on the circumstances and the available means, in addition to identifying DDoS attacks and specific measures to mitigate or at least moderate the impact that these generate on the performance of our network. Examples of common attacks used on local area networks are also provided, as well as examples of some common attacks used on local area networks.

Apart from being one of the greatest protocol analyzers available today, Wireshark is a fantastic resource for anybody interested in networking or communications.

When talked about task 8, It is only completed one.



Congratulations! Just now, you completed the "Wireshark: The Basics" room. Wireshark was discussed in this room, along with its functions and methods of usage for analyzing traffic captures.

Answer the questions below

Remind the step by step malware analyzing process

No answer needed

Challenges of the when created try hack me box

1. when implementing web exploitations at times due to coding issues, the exploitation was not done properly

2. finding the correct server for the tray hack me was very hard

   Desktop version cannot be uploaded to try hack me.so we have to upload the server version. Because we should find out proper version for that box. It is very hard to find the correct version. other one is, we must find proper kernel for that server. We must upload whatever server It should be lower than 20GB.

3. Finding the necessary option was very hard

   When we are adding task, we should add the task best order which called A-Z. It is very hard to find best order

4. Environment was unfamiliar

   In country situation, always have the power failures, so at that I cannot do this room making tutorial properly due to the network issue.

5. When creating the box, the implementation was hard

   After the create the box, I had to add question proper order. It was something hard to implementation of this box.

6. When finding a topic, I didn’t know how to manage the topic

   There are many topics about this assignment. But I had to get best decision for this topic. I have selected malware analysis and Wireshark.

7. Finding myself in a place where I couldn’t export the OVA

   Due to the connection issues and power failures, I could not export properly sometime. But finally, it was exported successfully.

8. Finding my way through try hack me was hard

9. How open VPN works, how hard it was to connect it to the try hack me

Summary

The purpose of this book is to provide a quick overview of network troubleshooting with Wireshark and how to use Wireshark tool, how to handle Wireshark tool via command line, what are the features of Wireshark tool likewise different type of essential parts have been discussed with in this book.