LW-01. WIRESHARK INTRODUCTION.

1. LAB WORK GUIDELINES

Disclaimer. This guidelines was created on the basis of the textbook «Data Communication and Networking», 5th.Edition, 2012, -1269 pp., by Behrouz A. Forouzan.

We have created lab assignments for several layers of TCP/IP. We have only theoretical lab assignments for physical layer. We cannot use a standard packet sniffer, such as Wireshark, to capture bits. We cannot sniff management packets because we have normally no permission to act as a manager. In this document, we give an introduction to packet sniffing, introduce the Wireshark software, talk about the lab reports, and finally tell you what to do in this lab assignment.

1.1 PACKET SNIFFING

The purpose of lab assignments is to show how we can get a deeper understanding of the networking concepts by capturing and analysing the packets sent and received from our host. One way to do so is to use a packet sniffer. A packet sniffer is a piece of soft- ware that should be running in parallel with the application whose packets needed to be analysed. However, before running a packet sniffer, we need to interpret the term packet. Communication via the Internet is done using a five-layer suite. We can analyse the packets at four layers: application, transport, network, and data-link. There is no packet exchange at the physical layer; communication at this layer is done using bits.

Although it is useful to analyse the packets in each of the four upper layers of the TCP/IP protocol suite, should a packet sniffer software be designed to capture packets at each of these layers? The answer to this question can be found in encapsulation-decapsulation.

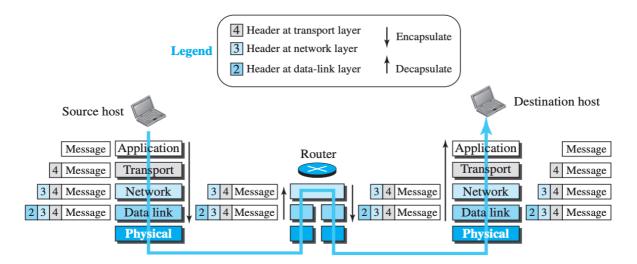


Figure 1.1 Encapsulation and Decapsulation

In an outgoing situation, a packet created at any upper-layer is encapsulated in a frame (at the data-link layer); in an incoming situation, a packet intended for any layer is decapsulated from the received frame. This means we need to capture only outgoing or incoming frames; a packet-sniffer software can extract the packets at any layer desired to be analysed from these frames. For this reason, a packet-sniffer software is normally having two components:

<u>a packet-capturer and a packet-analyser</u>. The packet-capturer captures a copy of all outgoing and incoming frames (at the data-link layer) and passes them to the packet-analyser. The packet- analyser can then extract different headers and the ultimate message for analysis.

Before we continue with our discussion, we need to make a point clear. Although Figure 1.1 in the textbook shows that the encapsulation starts or decapsulation ends at the application layer, a packet in the Internet can belong to any layer above the data- link layer. As we will see in future, protocols at the transport or network layer protocols also need to exchange packets. All of these packets are encapsulated in or decapsulated from the frames. A packet sniffer needs to capture all incoming and out- going frames and show the headers of all protocols used for communication. The source or the sink of a packet is not necessarily the application layer. Figure 1.2 shows two examples.

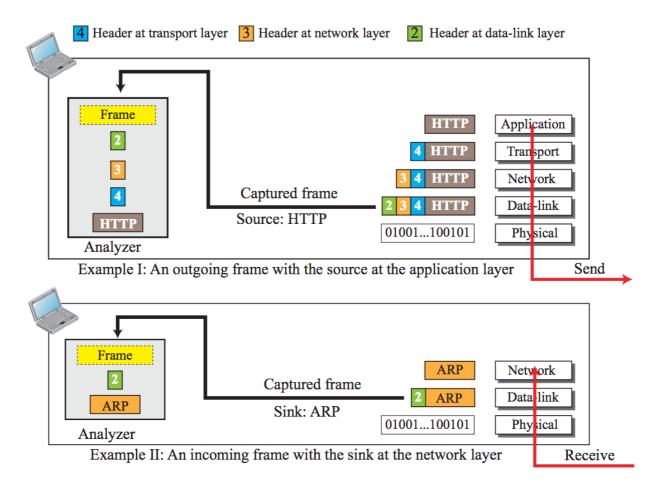


Figure 1.2 Role of frame capturing and packet analysing in a packet-sniffer

In Example I, an outgoing frames is captured. The source of the frame is the HTTP protocol at the application layer. A copy of the frame is passed to the analyser. The analyser extracts the general information in the frame (the box marked frame), headers 2, 3, and 4, and the HTTP message for analysis. In Example II, an incoming frame is captured. The sink (final destination) is the ARP protocol at the network layer. A copy of the frame is passed to the analyser. The analyser extracts the general information in the header (the box marked frame), header 2 and the ARP message for analysis.

1.2 WIRESHARK

In this and other lab assignments, we use a packet-sniffer called Wireshark. Wireshark is a free packet sniffer/analyser which is available for both UNIX-like (Unix, Linux, Mac OS X, BSD) and Windows operating systems. It captures



packets from a network interface and displays them with detailed protocol information.

Wireshark, however, is a passive analyser. It only captures packets without manipulate them; it neither sends packets to the network nor does other active operations. Wireshark is not an intrusion-detection tool either. It does not give warning about any network intrusion.

It, nevertheless, can help network administrators to figure out what is going on inside a network and to troubleshoot network problems. In addition, Wireshark is a valuable tool for protocol developers, who may use it to debug protocol implementations. It is also a great educational tool for computer-network students who can use it to see details of protocol operations in real time.

1.2.1 Main Window

The Wireshark main window (shown in Figure 1.3.) is made of seven sections: title bar, menu bar, filter bar, packet list pane, packet detail pane, packet byte pane, and status bar.

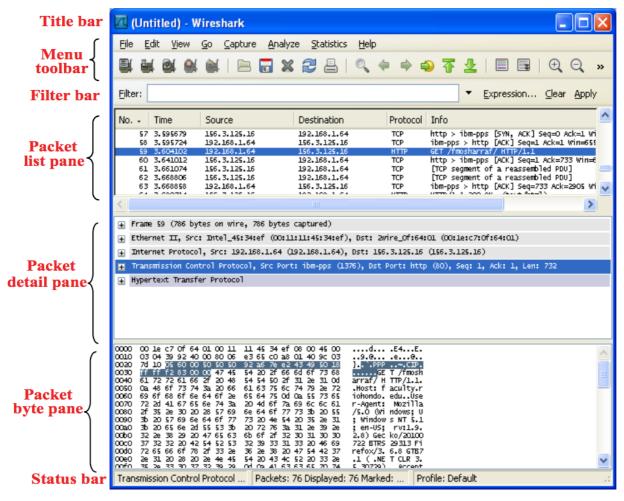


Figure 1.3 Main window of Wireshark

Title Bar

The title bar (like the one in any GUI) shows the title of the window, the closing, maximizing, and minimizing icons.

Menu Bar

The menu bar is made of several pull-down menus and tool bars used in most GUIs. We will use some of these menus in our lab assignments. We can use the File menu to perform some actions on the file itself such as saving and printing. The Capture menu is used to start and capturing frames. The View menu is useful to show or hide some of the sections in the window.

Filter Bar

The filter bar allows us to display packet we are interested in while hiding the rest. As we see later in this document, when we start capturing frames, Wireshark captures and analyse any outgoing and incoming frame no matter what is the source or sink protocol. Sometimes, this is not what we want. We may want to limit the analysis to a specific source or sink protocol. For example, we may want to analyse only packets sent or receive by the HTTP protocol at the application layer or the ARP protocol at the network layer. This is called filtering in the parlance of packet sniffing. After packets have been captured, we can type the name of the protocol in lowercase and click Apply.

Packet List Pane

The packet list pane displays a one-line summary for each captured packet (actually frame). The summary includes the packet (frame) number (added by the Wireshark and not part of the packet), the time when the packet was captured, the source and destination IP addresses of the packet (at the network layer), the packet source or sink proto- col, and the additional information about the packet contents. In other words, this pane shows the captured frames that will be passed for analysing to the packet analyser. For colouring packets use View \rightarrow Colorize Packet List.

Packet Detail Pane

The packet detail pane shows the detailed analysis for each frame (Figure 1.4). The information is limited to one frame, which means we need to select one of the frames in the packet list pane for analysis. This can be done by clicking on the corresponding frame in the packet list pane. Clicking on any frame in the packet list pane highlights the frame and shows the details of the frame in the packet details pane. Information exhibited in this pane for each frame is made of a tree structure. However, each top branch of the tree is shown as one line as it is common in GUI trees.

We can expand the branch (to see sub branches) by clicking on the plus box at the leftmost part of the line, which changes the plus sign to a minus sign; the branch can be collapsed again, which changes the minus sign to the plus sign. Note that the analyser first shows a general information at the data-link layer (frame). It then displays the information contained in each header from the data-link layer (H2) up to the source or sink protocol. It finally shows the whole message at the source or sink layer. Figure 1.4 shows an example of a packet details pane when the frame is expanded. It shows some general information and names of all protocols used in the frame (intermediate and source or sink).

🖻 Frame 5 (938 bytes on wire, 938 bytes captured)
Arrival Time: Aug 29, 2010 13:35:01.837483000
[Time delta from previous captured frame: 6.154714000 seconds]
[Time delta from previous displayed frame: 26.156885000 seconds]
[Time since reference or first frame: 26.156885000 seconds]
Frame Number: 5
Frame Length: 938 bytes
Capture Length: 938 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:tcp:http]
Ethernet II, Src: Intel_45:34:ef (00:11:11:45:34:ef), Dst: 2wire_0f:64:
■ Internet Protocol, Src: 192.168.1.64 (192.168.1.64), Dst: 156.3.125.16
Transmission Control Protocol, Src Port: sna-cs (1553), Dst Port: http
Hypertext Transfer Protocol
8

Figure 1.4 Packet detail pane

Packet byte pane

The packet byte pane shows the entire current frame (selected in the packet list pane) in hex dump format (hexadecimal view of data) and ASCII format. The number in the left field shows the offset in the packet data; the hex dump of the packet is shown in the middle field; the corresponding ASCII characters are shown in the right field. If we need the byte (or ASCII equivalent) of any line in the packet detail pane, we can click on the line in the packet detail pane and the byte contents will be highlighted. Figure 1.5 shows an example of a packet byte pane. It shows all the bytes in the frame, but we can select the bytes in any protocol header by highlighting it in the packet detail pane section.

0020	7d	10	06	11	00	50	95	03	e9	ac	5e	b9	db	0C	50	18	} · · · · P · ·	P.	~
0030	11	73	01	fe	00	00	47	45	54	20	21	66	6d	61	73	68		T /fmosh	
0040	61	72	72	61	66	21	45	6e	67	69	6e	65	65	72	69	6e	arraf/En	gineerin	100
0050	67	21	45	4e	47	52	25	32	30	32	31	37	21	65	6e	67	g/ENGR%2	0217/eng	
0060	72	5 f	32	31	37	2e	68	74	бđ	20	48	54	54	50	21	31	r_217.ht	m HTTP/1	
0070	2e	31	od	0a	48	61	73	74	3a	20	66	61	63	75	_	74		: facult	
0080	79	2e	72	69	61	68	61	6e	64	6Ť	2e	65	64	75	od	0a	y.riohon		1.00
0090	55	73	65	72	2 d	41	67	65	6e	74	зa	20	4d	61	7a	69	User-Age	nt: Mozi	
00a0	6C	6C	61	21	35	2e	30	20	28	57	69	6e	64	61	77	73	11a/5.0	(Windows	
00b0	зb	20	55	зb	20	57	69	6e	64	6f	77	73	20	4e	54	20	; U; Win	dows NT	
00c0	35	2e	31	36	20	65	6e	2 d	55	53	зb	20	72	76	зa		5.1; en-	US; rv:1	
00d0	2e	39	2e	32	2e	38	29	20	47	65	63	6b	61	21	32	30	.9.2.8)	Gecko/20	
00e0	31	30	30	37	32	32	20	42	54	52	53	32	39	33	31	33	100722 B		
00f0	20	46	69	72	65	66	61	78	21	33	2e	36	2e	38	20	47	Firefox		
0100	54	42	37	2e	31	20	28	20	2e	4e	45	54	20	43	40	52	TB7.1 (.NET CLR	
0110	20	33	2e		2e	33	30	37	32	39	29	od	oa		63	63	3.5.307		
0120	65	70	74	3a		74	65	78	74	2f	68	74	60	60	20	61	ept: tex		
0130	70	70	60	69	63	61	74	69	61	6e	21	78	68	74	6d	6C	pplicati	on/xhtml	
0140	20	78	60	6C	20	61	70	70	6C	69	63	61	74	69	6f		+xml,app		
0150	21	78	60	60	36	71	3d 41	30	2e	39	20	2a 74	21	2a	3b	71	/xml;q=0		
0160	3d 67	30	2e 61	38	0d 65	0a 3a	20	63	63	65 2 d	70	73	20	4C 0a	61 41	6e 63		cept-Lan	
0180	63		70	74	2d	45	6e	63	6e 6f	64	69		67				guage: e	n-usAc	
0190	7a	65 69	70	20	64	65	66	6C	61	74	65	6e 0d	0a	3a 41	20	67 63	cept-Enc zip.defl		
01a0		70	-	2d	43	68	61	72			74	3a		49	53	41	ept-Char	ateAcc set: ISO	100
onho	50	10	14	20	43	50	61	14	73	65	14	24	20	49	23	41	epc-char	Sec: 150	~
Transm	ission	n Co	ntrol	Pro	tocol		Pac	kets:	7 Dis	play	ed: :	2 Ma		Prof	ile: D	efault			

Figure 1.5 Packet byte pane

Status Bar

The last section of the window (at the bottom) is the status bar which shows the current protocol, the total number of packets captured, and so on.

1.2.2 Working with Wireshark

When we work with Wireshark in labs, there are some actions that we need to repeat over and over. We mention the details of some of this action to avoid rementioning them.

Start Capturing

To begin capturing, select the Capture from the pull down menu and click Options... to open the Wireshark capture dialog box. There are several steps that you need to follow before you start capturing:

1. The network interfaces are shown in the Interface list at the Input box. Select the network interface (or use the default interface chosen by Wireshark). If the IP address in the dialog box is unknown, you must select a different interface; otherwise, the Wireshark will not capture any packet (Figure 1.6).

▼ Wi-Fi: Ad	dresses: fe80::bae8:56ff:fe04		11 4	Ethernet	<	default	2	\square	
		8a4a, 192.168.1	11.4				~		
awdl0			11.4						
)			Ethernet		default	2	_	
Thung	derbolt Bridge: bridge0			Ethernet		default	2	_	
Thung	derbolt 1: en1			Ethernet		default	2	_	
p2p0				Raw IP		default	2	_	
Loopt	back: IoO			BSD loopback	\checkmark	default	2	_	
Cisco	remote capture: cisco			Remote capture dependent DLT	_	_	_	_	
	om packet generator: randpkt			Generator dependent DLT	_	_	_	_	
SSH r	emote capture: ssh			Remote capture dependent DLT	_	_	_	_	

Figure 1.6 Capture Input window

2. You normally will use the default values in the capture options dialog box, but there are some options that you may need to override the default (Figure 1.7).

• •	🚄 Wireshark · Captu	re Interfaces	🚄 Wireshark · Captu	ire Interfaces
	Input Output	Options	Input Output	Options
Capture to a permanent file			Display Options	Name Resolution
File: Leave blank to use a tempora	ary file		Update list of packets in real-time	Resolve MAC Addresses
			Automatically scroll during live capture	
Output format: 💿 pcap-ng 🔷 pca	ар		Show extra capture information dialog	Resolve transport names
Create a new file automatically at	iter			
1 ¢ kilobytes	\$		Stop capture automatically after	
Kilobytes	~		1 C packets	
1 \$\$ seconds	٥		□ 1	
_			□ 1 🗘 kilobytes ᅌ	
Use a ring buffer with 2	files		1 0 seconds ᅌ	

Figure 1.7 Capture Output and Options window

3. It is possible to configure packet filtering using the window Capture Filters (Figure 1.8).

	Wireshark	· Capture Filters
Name		Filter
Ethern	et address 00:00:5e:00:53:00	ether host 00:00:5e:00:53:00
Ethern	et type 0x0806 (ARP)	ether proto 0x0806
No Bro	adcast and no Multicast	not broadcast and not multicast
No ARF		not arp
IPv4 or	nly	ip
IPv4 ac	Idress 192.0.2.1	host 192.0.2.1
IPv6 or	nly	ip6
IPv6 ad	ldress 2001:db8::1	host 2001:db8::1
IPX onl	У	ipx
TCP or	ly	tcp
UDP or	nly	udp
TCP or	UDP port 80 (HTTP)	port 80
HTTP 1	CP port (80)	tcp port http
No ARF	P and no DNS	not arp and port not 53
Non-H	TTP and non-SMTP to/from www.wireshark.org	not port 80 and not port 25 and host www.wireshark.org
+ -	- Pb	
Help		Cancel OK

Figure 1.8 Capture Filters window

After the above three steps, click Start. Wireshark starts to captures packets that are exchanged between your computer and the network. If, after a minute, Wireshark does not capture any packet, there must be a problem; check for possible reason and troubleshooting.

Stop Capturing

Whenever you feel you have captured all the packets (frames) that you need to do your lab report, you can stop capturing. To do so, you need to use the Capture pull-down menu and click Stop. Wireshark stops capturing the frames.

Saving the Captured Information

After you have stopped capturing, you may want to save the captured information (File \rightarrow Save) or save interesting packet (Right Mouse Button \rightarrow Copy \rightarrow Copy Bytes as Hex Dump.

1.2.3 Incoming and Outgoing Frames

When we see the list of the captured frames, we often wonder which frames are the incoming and which ones are outgoing. This can be found by looking at the frame in packet list pane. The packet list pane shows the source and destination addresses of the frame (generated and inserted at the network layer). If the source address is the address of the host you are working with (shown on the Capture window when you start capturing), the frame is the outgoing frame; if the destination address is the address of your host, the frame is the incoming frame.

1.2.4 Analyse and Statistics

In addition, Wireshark has several convenient and useful functions. For example:

1. View \rightarrow Coloring Rules (see Figure 1.9)

lam	e	Filter
	Bad TCP	tcp.analysis.flags && !tcp.analys
 Image: A start of the start of	HSRP State Change	hsrp.state != 8 && hsrp.state !=
	Spanning Tree Topology Change	stp.type == 0x80
	OSPF State Change	ospf.msg != 1
	ICMP errors	icmp.type eq 3 icmp.type eq 4
	ARP	arp
\checkmark	ICMP	icmp icmpv6
	TCP RST	tcp.flags.reset eq 1
	SCTP ABORT	sctp.chunk_type eq ABORT
	TTL low or unexpected	(!ip.dst == 224.0.0.0/4 && ip.tt
 Image: A start of the start of	Checksum Errors	eth.fcs.status=="Bad" ip.checl
	SMB	smb nbss nbns nbipx ipx
	HTTP	http tcp.port == 80 http2

Double click to edit. Drag to move. Rules are processed in order until a match is found.

Figure 1.9 Coloring Rules window

2. Analyse \rightarrow Follow (TCP | UDP | SSL) Stream - allows you to assemble the transfer session together and view its contents as a whole - until the restoration of the HTML page transmitted during the session.

3. Analyse \rightarrow Expert Information (see Figure 1.10) will show a list of the main events that occurred during the capture - the opening of new sessions, not quite good protocol behaviour (repeated receipts in TCP, segment retransmissions, etc.).

4. Statistics \rightarrow Capture File Properties allows you to view some statistics for the capture session in general - including the average number of packets per second and the amount of data transferred (Figure 1.11).

ror ror ror	Invalid Version Malformed Packet (Exception occurred)	Malformed Malformed	QUIC	7	
	Malformed Packet (Exception occurred)	Malformed	01110	_	
or		Manornica	QUIC	5	
01	Malformed Packet (Exception occurred)	Malformed	SSL	34	
ror	Malformed Packet (Exception occurred)	Malformed	RTCP	1	
arning	Connection reset (RST)	Sequence	TCP	78	
arning	ACKed segment that wasn't captured (common at capture start)	Sequence	TCP	151	
arning	Previous segment(s) not captured (common at capture start)	Sequence	TCP	109	
arning	Ignored Unknown Record	Protocol	SSL	125	
arning	This frame is a (suspected) out-of-order segment	Sequence	TCP	54	
arning	TCP window specified by the receiver is now completely full	Sequence	TCP	2	
arning	No response seen to ICMP request	Sequence	ICMP	2	
	Echo (ping) request id=0x0001, seq=3929/22799, ttl=32 (no r				
ote		Sequence	TCP	31	
ote	This frame is a (suspected) retransmission	Sequence	TCP	119	
ote	Duplicate ACK (#1)	Sequence	TCP	117	
ote	HTTP body subdissector failed, trying heuristic subdissector	Malformed	HTTP	8	
ote	This session reuses previously negotiated keys (Session resu	Sequence	SSL	22	
ote	"Time To Live" only 1	Sequence	IPv4	20	
ote	Duplicate ACK (#2)	Sequence		25	
ote	Duplicate ACK (#3)	Sequence		1	
ote		Protocol		1	
at		Sequence			
lat	HTTP/1 1 200 OK\r\n	Sequence	HTTP	486	
a a a a a a a a a a a a a a a a a a a	rning rning rning rning rning 13186 13266 e e e e e e e e e e e e e e e e e e	rningConnection reset (RST)rningACKed segment that wasn't captured (common at capture start)rningPrevious segment(s) not captured (common at capture start)rningIgnored Unknown RecordrningThis frame is a (suspected) out-of-order segmentrningTCP window specified by the receiver is now completely fullrningNo response seen to ICMP request13186Echo (ping) request id=0x0001, seq=3926/22031, ttl=32 (no r13266Echo (ping) request id=0x0001, seq=3929/22799, ttl=32 (no r18266Echo (ping) request id=0x0001, seq=3929/22799, ttl=32 (no r19267This frame is a (suspected) spurious retransmissioneThis frame is a (suspected) retransmissioneThis session reuses previously negotiated keys (Session resue"Time To Live" only 1eDuplicate ACK (#2)eDuplicate ACK (#3)eThe acknowledgment number field is nonzero while the ACK flatGET /complete/search?client=chrome&hl=en-US&q=cr HTTP/atHTTP/1 1 200 OKIr\n	rningConnection reset (RST)SequencerningACKed segment that wasn't captured (common at capture start)SequencerningPrevious segment(s) not captured (common at capture start)SequencerningIgnored Unknown RecordProtocolrningThis frame is a (suspected) out-of-order segmentSequencerningTCP window specified by the receiver is now completely fullSequence13186Echo (ping) request id=0x0001, seq=3926/22031, ttl=32 (no rSequence13266Echo (ping) request id=0x0001, seq=3929/22799, ttl=32 (no rSequenceeThis frame is a (suspected) purious retransmissionSequenceeThis frame is a (suspected) retransmissionSequenceeThis frame is a (suspected) retransmissionSequenceeThis frame is a (suspected) retransmissionSequenceeThis session reuses previously negotiated keys (Session resuSequenceeThis session reuses previously negotiated keys (Session resuSequenceeDuplicate ACK (#1)SequenceeDuplicate ACK (#2)SequenceeDuplicate ACK (#3)SequenceeThe acknowledgment number field is nonzero while the ACK flProtocoletHTTP/1 1 200 OK/r\nSequence	rningConnection reset (RST)SequenceTCPrningACKed segment that wasn't captured (common at capture start)SequenceTCPrningPrevious segment(s) not captured (common at capture start)SequenceTCPrningIgnored Unknown RecordProtocolSSLrningThis frame is a (suspected) out-of-order segmentSequenceTCPrningTCP window specified by the receiver is now completely fullSequenceTCP13186Echo (ping) request id=0x0001, seq=3926/22031, ttl=32 (no rSequenceTCP13266Echo (ping) request id=0x0001, seq=3929/22799, ttl=32 (no rSequenceTCPeThis frame is a (suspected) spurious retransmissionSequenceTCPeThis frame is a (suspected) retransmissionSequenceTCPeThis frame is a (suspected) retransmissionSequenceTCPeThis frame is a (suspected) retransmissionSequenceTCPeThis session reuses previously negotiated keys (Session resuSequenceSSLe"Time To Live" only 1SequenceSequenceTCPeDuplicate ACK (#2)SequenceTCPFequenceTCPeThe acknowledgment number field is nonzero while the ACK flProtocolTCPetGET /complete/search?client=chrome&hl=en-US&q=cr HTTP/SequenceHTTPetHTTP/11 200 OK/rhnSequenceHTTP	rningConnection reset (RST)SequenceTCP78rningACKed segment that wasn't captured (common at capture start)SequenceTCP151rningPrevious segment(s) not captured (common at capture start)SequenceTCP109rningIgnored Unknown RecordProtocolSSL125rningTCP window specified by the receiver is now completely fullSequenceTCP213186Echo (ping) request id=0x0001, seq=3926/22031, ttl=32 (no rSequenceTCP3113266Echo (ping) request id=0x0001, seq=3929/22799, ttl=32 (no rSequenceTCP119eThis frame is a (suspected) purious retransmissionSequenceTCP119eThis frame is a (suspected) retransmissionSequenceTCP117eTTP body subdissector failed, trying heuristic subdissectorMalformedHTTP8eThis session reuses previously negotiated keys (Session resuSequenceSEQuenceSEQuence22e"Time To Live" only 1SequenceTCP12eDuplicate ACK (#2)SequenceTCP12eThe acknowledgment number field is nonzero while the ACK flProtocolTCP1etHTTP/1 200 OK\nnSequenceHTTP486

Figure 1.10 Expert Information window

🛑 🛑 🔵 Wireshark	· Capture Fi	le Properties ·	wireshar	k_en0_20171	01001094	42_fFqbba	ar
Details							-)
Time							
First packet: Last packet: Elapsed:	2017-10-10 2017-10-10 00:10:38						
Capture							
Hardware: OS: Application:	Mac OS X 1	e(TM) M-5Y5 10.12.6, build Wireshark) 2.4	16G29 (Da	arwin 16.7.0)			
Interfaces							
	<u>Dropped pa</u> Unknown	ackets <u>Captur</u> none	re filter	<u>Link type</u> Ethernet		<u>cket size limit</u> 4288 bytes):
Statistics							
Measurement Packets Time span, s Average pps Average packet si	<u>Captur</u> 1725 638.29 2.7 ze, 300.5		<u>Display</u> 1725 (1 638.29 2.7 300.5	00.0%)	<u>Marked</u> — — —		
B Bytes	517999	Э	517999	9 (100.0%)	0		

Figure 1.11 Capture File Properties window

5. Statistics \rightarrow Protocol Hierarchy - statistics on the protocols used (Figure 1.12).

-	-	

Wireshark · Protocol Hierarchy Statistics · wireshark_en0_20161013164525_wcjJkG

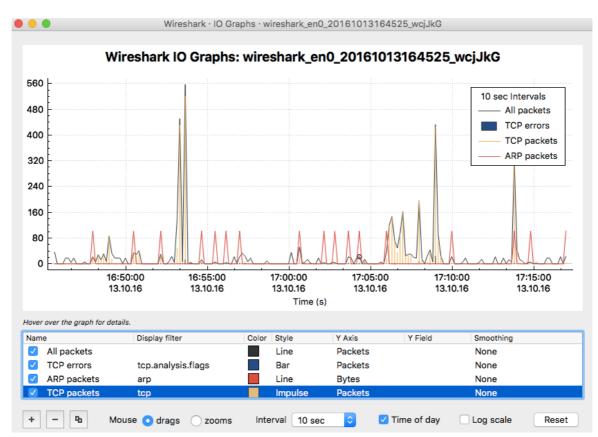
rotocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s
Frame	100.0	4347	100.0	1494517	6345
Ethernet	100.0	4347	4.1	60858	258
Internet Protocol Version 6	0.1	3	0.0	525	2
User Datagram Protocol	0.1	3	0.0	24	0
Multicast Domain Name System	0.1	3	0.0	381	1
Internet Protocol Version 4	99.1	4310	5.8	86200	365
 User Datagram Protocol 	23.2	1009	0.5	8072	34
Simple Service Discovery Protocol	20.5	892	21.3	318526	1352
QUIC (Quick UDP Internet Connections) 1.6	69	3.1	45624	193
Network Time Protocol	0.1	4	0.0	192	0
NetBIOS Name Service	0.4	19	0.1	1112	4
Multicast Domain Name System	0.1	3	0.0	381	1
Domain Name System	0.4	18	0.1	1148	4
Bootstrap Protocol	0.1	4	0.1	1200	5
Transmission Control Protocol	75.9	3301	64.9	969421	4115
SSH Protocol	38.7	1682	49.5	739264	3138
Malformed Packet	0.2	10	0.0	0	0
Secure Sockets Layer	8.2	357	8.2	122306	519
Data	0.2	8	0.0	616	2
Address Resolution Protocol	0.8	34	0.1	952	4

Figure 1.12 Protocol Hierarchy window

6. Statistics \rightarrow Conversations shows information about the participants in the communication, who sent packets and data to whom to whom and how (Figure 1.13).

		Ethernet · 5	IPv4 · 13	IPv6 · 1	TCP · 16	UDP · 79		
Address A 10.10.1.75 10.10.1.75 10.10.1.75 10.10.1.75 10.10.1.75 10.10.1.75 10.10.1.75 10.10.1.75 10.10.1.75 10.10.1.75 10.10.1.75 10.10.1.75 10.10.1.75	▲ Address B 239.255.255.250 10.10.1.255 85.254.142.227 192.168.68.249 54.165.177.196 52.206.41.133 17.253.38.253 216.58.211.142 216.58.209.142 17.252.92.20 17.172.238.201 224.0.0.251 17.248.150.111	Packets 892 19 2,540 22 28 3 4 659 86 6 6 3 42	Bytes 355 k 1910 913 k 3272 8114 206 360 151 k 40 k 704 704 507 14 k	Packets A → B	892 19 1,568 11 16 2 2 363 40 4 4 4 3 22	ytes A → B 355 k 1910 413 k 1419 1884 132 180 87 k 7062 466 466 507 4954	IEEE 802.11 ✓ IPv4 ✓ IPv6 IPX	ytes B → /

Figure 1.13 Conversations window	Figure	1.13	Conversations	window
----------------------------------	--------	------	---------------	--------



7. Statistics \rightarrow IO Graphs allows to you build an almost arbitrary statistical graph of the captured data (Figure 1.14).

Figure 1.14 IO Graphs window

8. Statistics \rightarrow Packet Lengths allows to you finding a very short and very long frames (Figure 1.15).

opic / Item 🔹 🔻		Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start	
Packet Lengths	27483	808.52	42	1514	0.0895	100%	4.5500	92.370	
0-19	0	-	-	-	0.0000	0.00%	-	-	
20-39	0	-	-	-	0.0000	0.00%	-	-	
40-79	10263	57.97	42	78	0.0334	37.34%	0.9200	92.396	
80-159	1578	125.59	81	159	0.0051	5.74%	0.6500	270.565	
160-319	653	201.31	161	319	0.0021	2.38%	0.4100	270.576	
320-639	258	438.79	323	639	0.0008	0.94%	0.1300	1.268	
640-1279	328	934.70	646	1279	0.0011	1.19%	0.0700	61.725	
1280-2559	14403	1449.43	1284	1514	0.0469	52.41%	3.1700	92.370	
2560-5119	0	-	-	-	0.0000	0.00%	-	-	
5120 and greater	0	-	-	-	0.0000	0.00%	-	-	
splay filter: Enter a di	1								Apply



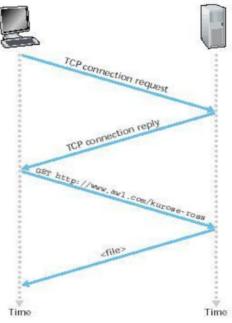
2. LW ASSIGNMENT

2.1. Lab Target

The LW assignment for this chapter is a warm-up testing of the Wireshark software. In this LW, we retrieve a web page and then, using Wireshark, capture and analyze packets.

Process:

- Visiting a Web site
- Type in the URL in Web browser
- First your computer will send a connection request message to the Web Server
- Web Server will respond by returning a connection reply message
- Your computer then sends the name of the web page
- Finally the server returns the page to you.



2.2. Assignment

2.2.1. Calculate Your variant number.

- a) Write your surname in the letters of the English alphabet. Must be at least 4 letters, if not enough, then add the required number of letters from the name. *For example, for student Li Yuriy there will be LIYU.*
- b) Replace the first 4 letters with their ordinal numbers in the alphabet, writing the numbers as two-digit decimal numbers.
 For example, 12 09 25 21.
- c) Consistently add modulo 26 these 4 numbers and add 1
 For example, (12 + 09 + 25 + 21)mod26 + 1 = 67mod26 + 1 = 15 + 1 = 16.
- d) The resulting will be your variant Nr. *For example, 16.*

Remark.

Find only unsecure http:// sites for your variant.

- a) Read "Why No HTTPS?" <u>https://whynohttps.com/</u> and select your site from Reports by Country.
- b) Read topic: <u>https://www.acunetix.com/websitesecurity/google-hacking/</u> and use Google operators to search inurl: and intitle:

For example, inurl:http\:+intitle:isma

Variant Nr:	Web site name (dns)	Variant Nr:	Web site name (dns)
1.	cn	14.	dz
2.	lv	15.	ee
3.	lt	16.	
4.	am	17.	
5.	es	18.	fo
6.	lu	19.	fi
7.	ch	20.	hu
8.	be	21.	јр
9.	bg	22.	ni
10.	са	23.	ua
11.	bz	24.	ru
12.	bd	25.	uz
13.	do	26.	de

2.2.3. Start your browser and clear cache.

Start up your web browser and clear the browser's cache memory (Use the following website if you don't know how to do this), but do not access any site yet.

• http://www.wikihow.com/Clear-Your-Browser's-Cache

2.2.3. Open and configure Wireshark.

a) Start Wireshark.

Variants

- b) Change interface language. Edit Preference Appearance Language English.
- c) Use the **display** filter box to show only frames that the source or the sink protocol is HTTP. Note that you need to type "**http**" in the display filter box and click Apply.
- d) Use the **capture** filter box to capture only frames that the destination port is HTTP. Note that you need to type "**tcp port 80 or tcp port 443**" in the capture filter box.
- e) Select Active Interface, example Local Area Connection.

•	· · ·	
🖉 Wireshark		
· · · · · · · · · · · · · · · · · · ·	Statistics Telephony Wireless 1	Tools Help
📕 🖉 🛞 🕌 🖾 🗙 🖸 🤇	← ⇒ 聲 주 业	$ \Theta \Theta \blacksquare $
http		Expression 🕇
Welcome to Wireshark		
Capture		
using this filter: 📙 tcp port 80	or tcp port 443	All interfaces shown 🔻
NdisWan Adapter Local Area Connection NdisWan Adapter NdisWan Adapter VirtualBox Host-Only Netwo	rk	
Learn		
User's Guide · Wiki · Que	stions and Answers 🕐 Mailing L	Lists
🔵 🏹 Всё готово к загрузке или захи		No Packets Profile: Default

2.2.4. Capturing traffic.

- a) Start Wireshark capturing;
- b) Now, go back to your browser, access one of your variant of web site;
- c) Stop capturing and save the captured file (File \rightarrow Save \rightarrow name.pcap).
- d) For open pcap file in Wireshark select File \rightarrow Open \rightarrow name.pcap.

1		i (tcp port 80 or tcp port		Usla		_ 🗆
		· · ·	elephony Wireless Tools			
	= 🧟 🛞 🕌	🗙 🖸 ९ 🗢 🖻	क ⊉ 🚍 🗏 🔍 व	l 🔍 🎹		
ŀ	ittp				🗙 🔜 💌 Expressi	ion
	Time	Source	Destination	Protocol	Length Info	
	108 3.315469	192.168.19.2	85.254.142.227	HTTP	714 GET / HTTP/1.1	
	117 3.331154	85.254.142.227	192.168.19.2	HTTP	199 HTTP/1.1 200 OK (text/html)	
	119 3.491288	192.168.19.2	85.254.142.227	HTTP	630 GET /css/mycss.css HTTP/1.1	
	120 3.491448	192.168.19.2	85.254.142.227	HTTP	612 GET /js/home.js HTTP/1.1	
	122 3.495841	85.254.142.227	192.168.19.2	HTTP	604 HTTP/1.1 404 Not Found (text/html)	
	123 3.498837	85.254.142.227	192.168.19.2	HTTP	606 HTTP/1.1 404 Not Found (text/html)	
	158 5.805742	192.168.19.2	85.254.142.227	HTTP	638 GET /im/pic/backgrnd.gif HTTP/1.1	
	159 5.805851	192.168.19.2	85.254.142.227	HTTP	636 GET /im/pic/bgmenu.jpg HTTP/1.1	
	160 5.814093	85.254.142.227	192.168.19.2	HTTP	610 HTTP/1.1 404 Hot Found (text/html)	
	161 5.814316	85.254.142.227	192.168.19.2	HTTP	612 HTTP/1.1 404 Not Found (text/html)	
Н	ransmission Contr ypertext Transfer	ol Protocol, Src Po Protocol	.168.19.2, Dst: 85.25 rt: 25646, Dst Port:		Ack: 1, Len: 660	
н	ransmission Contr ypertext Transfer B-GET / HTTP/1.1\ - Host: net.acade - Connection: kee - Upgrade-Insecur - User-Agent: Mot - DUIT: 1\r\n - Accept: text/ht	ol Protocol, Src Por Protocol my.lv/r\n p-alive\r\n e-Requests: 1\r\n illa/5.0 (Windows II ml,application/xhtmi	rt: 25646, Dst Port: T 6.1; Win64; x64) Ap	80, Seq: 1, ple⊎ebKit/5	Ack: 1, Len: 660 37.36 (KHTVL, like Gecko) Chrome/76.0.3809.132 Safar1/537.36\r\ e/webp,image/apng,'/';q=0.8,application/signed-ewchange;v=b3\r\	
•• H	ransmission Contr ypertext Transfer 9-GET / HTTP/1.1/ - Host: net.acade - Connection: kee - Upgrade-Insecur - Uger-Agent: Mor - DUT: 1/r/n - Accept: text/ht - Purnose: nrefet	ol Protocol, Src Por Protocol my.lv/r/n p-alive/r/n e-Requests: 1/r/n illa/5.0 (Windows UT ml,application/shtml ch/r/n	rt: 25646, Dst Port: T 6.1; Win64; x64) Ap L+xml,application/xml	80, Seq: 1, pleWebKit/5 .;q=0.9,imag	37.36 (KHT×L, like Gecko) Chrome/76.0.3809.132 Safari/537.36\r\ e/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\	
• H	ransmission Contr ypertext Transfer Host: net.acade Connection: kee Upgrade-Insecur User-Agent: Mor DUIT: l\r\n Accept: text/ht Purnase: nefet e4 8d 8c 95 49	<pre>cdl Protocol, Src Por Protocol rin my.lv/\n p-alive/rin e-Requests: 1\r\n illa/5.0 (Windows II' ml,application/whtml ch/rin cb 90 e5 ba d6 be</pre>	rt: 25646, Dst Port: [6.1; Win64; x64) Ap [+xml,application/xml fb 08 00 45 00	80, Seq: 1, pleWebKit/5 ;q=0.9,imag	37.36 (KHTVL, like Gecko) Chrome/76.0.3809.132 Safari/537.36\r\ e/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\ E·	
000	ransmission Contr ppertext Transfer ØGET / HTP/L1V Host: net.acade Connection: kee Uggrade-Insecur Uger-Agent: Most DUT: 1\r\n Accept: text/ht Purnose: neefet 0 e4 8d 8c 95 499 02 bc 73 fd 40	ol Protocol, Src Por Protocol r/n my.lv/r/n e-Requests: 1/r/n illa/5.0 (Windows W ml,application/xhtmi ch/P/n cb 90 e6 ba d6 be 00 40 06 00 00 c0	rt: 25646, Dst Port: [6.1; Win64; ×64) Ap 1+×ml,application/xml fb 08 00 45 00 a8 13 02 55 fe	80, Seq: 1, pleWebKit/5 ;q=0.9,imag .I	37.36 (KHT⊻L, like Gecko) Chrome/76.0.3809.132 Safari/537.36\r\ e/sebp,image/apng,†/†;q=0.8,application/signed-eschange;v=b3\r\ E· U·	
000 010 020	ransmission Contr ypertext Transfer Ø(6T / HTP/L1) Host: net.acade Connection: kee Uggrade-Insecur User-Agent: Moz DUT: 1/r/n Accept: text/ht Purnose: nrefet 0 e4 &0 &0 c 93 49 0 &0 bc 73 fd 40 0 &e e5 64 2e 00	ol Protocol, Src Por Protocol r/n my.lv/r/n p-alive/r/n e-Requests: 1/r/n illa/5.0 (Windows UT ml,application/xhtml ch/r/n cb 90 e6 ba d6 be 00 40 06 00 00 c0 50 d5 6b ae 6a da	rt: 25646, Dst Port: T 6.1; Win64; x64) Ap 1+xml,application/xml Tb 08 00 45 00 a8 13 02 55 Tes 13 63 71 50 18d	80, Seq: 1, pleWebKit/5 ;q=0.9,imag	37.36 (KHT≚L, like Gecko) Chrome/76.0.3809.132 Safari/537.36\r\ e/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\ E. U. p.	
000 010 020	ransmission Contr ppertext Transfer 9 deT / HTP/L1 Host: net.acade Connection: kee Upgrade=Insecur User-Agent: Mor DUT: 1/v\n Accept: text/ht Purpose: nefet 0 de & da de 39 A9 0 de bo 3a 69 A9 0 de bo 3a 00 5a 60 bb 3a 00	ol Protocol, Src Por Protocol r/n my.lv/r/n e-Requests: 1/r/n illa/5.0 (Windows W ml,application/xhtmi ch/P/n cb 90 e6 ba d6 be 00 40 06 00 00 c0	rt: 25646, Dst Port: [6.1; Win64; x64) Ap [+oml,application/oml fb 08 00 45 00 a8 13 02 55 fes 13 83 71 50 18d 20 48 54 54 50	80, Seq: 1, pleWebKit/5 ;g=0.9,imag .I	37.36 (KHTVL, like Gecko) Chrome/76.0.3809.132 Safari/537.36\r\ e/xebp,image/apng,'/';q=0.8,application/signed-exchange;v=b3\r\ E- U- QP TP	
000 010 020 0310 0320 0340	ransmission Contr ppertext Transfer 0 GET / HTP/L1V Host: net.acade Connection: kee Uggrade-Insecur Uger-Agent: %or DUT: 1\r\n Accept: text/ht <u>Purnose: neefet</u> 0 4 8 d8 6c 95 49 0 20 c7 3 f4 40 8 ea 3 64 2e 00 1 fa f0 bb 3a 00 2 f 31 2e 31 0d	col Protocol, Src Por Protocol r'n my.lv/rin p-alive/rin e-Requests: l/rin ml.application/shtmi ch/rin cb 90 65 ba d6 be 00 40 05 00 00 c0 50 d5 6b ae 6a da 00 47 45 54 20 2f	rt: 25646, Dst Port: [6.1; Win64; x64) Ap [+xm],application/xml [fb 06 00 45 00 a8 13 02 55 fe 13 83 71 50 18 20 48 54 54 50 20 6e 65 74 2e /1.	80, Seq: 1, pleWebKit/5 ;q=0.9,imag .P.k .j .P.k .j 1Ho st: n.	37.36 (KHTVL, like Gecko) Chrome/76.0.3809.132 Safari/537.36\r\ e/webp,image/apng,*/*;q=0.8,application/signed-ewchange;v=b3\r\ E. U. JP. TIP et.	
000 01 020 030 030 030	ransmission Contr ypertext Transfer 9 det / HTP/L1 Host: net.acade Commetion: kee Upgrade-Insecur User-Agent: %or DUT: 1/vin Accept: text/ht Purunsaz: neefet 0 de 4 8d 2e 00 1 fa 10 b3 a0 0 2f 31 2e 31 0d 61 63 61 64 65	ol Protocol, Src Por Protocol r/n my,lv\r\n p-alive\r\n e-Requests: 1\r\n illa/5.0 (Windows II' ml,application/xhtmi ch\r\n cb 90 e6 ba d6 be 00 40 06 00 00 00 50 d5 6b ae 6a da 00 47 45 54 20 2f 0a 48 6f 73 74 3a	rt: 25646, Dst Port: T 6.1; Win64; x64) Ap 1+vml,application/xml fb 08 00 45 00 a8 18 02 55 fe 18 38 71 50 18 20 68 65 74 2e /1. 00 43 56 66 68 aca	80, Seq: 1, pleWebKit/5 ;;=0.9,imag 	37.36 (KHT™L, like Gecko) Chrome/76.0.3809.132 Safari/537.36\r\ e/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\ E. U. p. TTP et. onn	
000 01 02) 03) 04) 05) 05)	ransmission Contr ppertext Transfer ØGET / HTP/L1V Host: net.acade Connection: kee Uggrade-Insecur Uger-Agent: %oc DUT: 1/v\n Accept: text/ht Purnose nesfet 02 bc 73 fd 40 0 48 d8 dc 93 49 02 bc 73 fd 40 0 6 e 3 64 26 00 0 2 f 31 2e 31 00 0 61 63 61 64 65 0 56 63 74 69 67	<pre>col Protocol, Src Por Protocol rin my.lv/\n p-alive/rin e-Requests: 1\r\n ml,application/xhtml ch/rin cb 90 e6 ba d6 be 00 40 06 00 00 c0 50 d5 6b ae 6a da 00 47 45 54 20 2f 0a 48 6f 73 74 3a 6d 79 2e 6c 76 0d</pre>	rt: 25646, Dst Port: [6.1; Win64; x64) Ap [+xml,application/xml fb 05 00 45 00 a8 13 02 55 fes 13 83 71 50 18d 20 48 54 50 20 48 65 74 2e /l. 0a 43 6f 66 6a aca 70 2d 6l 6c 69 ect	80, Seq: 1, pleWebKit/5 ;q=0.9,imag 	37.36 (KHTVL, like Gecko) Chrome/76.0.3809.132 Safari/537.36\r\ e/xebp,image/apng,'/';q=0.8,application/signed-exchange;v=b3\r\ E. U. ηP. TP et. onn ali	
000 010 020 030 030 030 030 030 030 030 030	ransmission Contr ypertext Transfer ØGET / HTP/L1V Host: net.acade Connection: kee Uggrade-Insecur Uger-Agent: %oc DUT: 1/r\n Accept: text/ht <u>Purmose: neefer</u> 04 & dd & c 93 & 49 02 & bc 73 & fd 40 & de e3 & 64 & 20 & 00 & fa f0 & bb 3a 00 & 2f 31 2e 31 & dd & 61 & 63 & 61 & 64 & 65 & 65 & 63 & 74 & 69 & 6f & 76 & 65 & 0d & 0a 55 & 76 & 75 & 0d & 0a 55 & 76 & 75 & 76 & 76 & 76 & 76 & 76 & 76 & 65 & 0d & 0a 55 & 76 & 75 & 0d & 0a 55 & 76 & 75 & 76 & 76 & 76 & 76 & 76 & 75 & 76 & 76 & 76 & 76 & 76 & 76	ol Protocol, Src Por Protocol r/n my.l/\r/n p-alive\r/n e-Requests: 1\r/n illa/5.0 (Windows W ml,application/shtml ch\r/n cb 90 e6 ba d6 be 00 40 06 00 00 c0 50 d5 6b ae 6a da 00 47 45 54 20 2f 0a 48 6f 73 74 3a 6d 79 2e 6c 76 0d 6e 3a 20 6b 65 65	rt: 25646, Dst Port: T 6.1; Win64; x64) Ap 1+xml,application/xml th 08 00 45 00 ab 13 02 55 fe 13 83 71 50 18 20 48 54 54 50 20 6e 65 74 2e /1. 0a 43 6f 6e 6e aca 70 2d 61 6c 69 ect 2d 49 6e 73 65 ve:	80, Seq: 1, pleWebKit/5 .;q=0.9,imag .P.k.j .P.k.j GE T / H' 1Ho st: n. demy. lvC. ion: keep	37.36 (KHT™L, like Gecko) Chrome/76.0.3809.132 Safari/537.36\r\ e/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\ E. U. qP. TTP et. omn ali ISe	
000 010 020	ransmission Contr pertext Transfer 96ET / HTP/L1 Host: net.acade Commection: kee Upgrade-Insecur User-Agent: Mor OUT: 1/V/N Accept: text/Nh Purnose: nefet 0 e4 8d 8c 93 49 0 2b c7 3 fd 40 8 ac 83 42 200 6 af 60 bb 3a 00 2 f 31 2e 31 0d 6 16 36 164 65 0 65 63 74 69 6f 76 65 0d 9a 65 6 37 57 265 2d	ol Protocol, Src Por Protocol r/n my,lu\r\n =-Requests: 1\r\n illa/5.0 (Windows II' ml,application/xhtmi ch\r\n cb 90 e6 ba d6 be 00 40 06 00 00 c0 50 d5 6b ae 6a da 00 47 45 54 20 2f 0a 48 6f 73 74 3a 6d 79 2e 6c 76 0d 6e 3a 20 6b 65 65 70 70 67 72 61 64 65	rt: 25646, Dst Port: [6.1; Win64; x64) Ap [+xm],application/xml fb 06 00 45 00 ···· a6 13 02 55 fe ··s 13 63 71 50 16 ··d 20 48 54 54 50 ···· 20 46 65 74 2e /1. 00 43 61 66 6e aca 70 24 61 6c 69 ect 2d 49 6e 73 65 ver 74 73 38 20 31 cur	80, Seq: 1, pleWebKit/5 ;q=0.9,imag 	37.36 (KHTVL, like Gecko) Chrome/76.0.3809.132 Safari/537.36\r\ e/xebp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\ E. -U. -U. -U. -U. -U. -U. -U. -U. -U. -U	
000 010 020 030 030 030 030 030 030 030 030	ransmission Contr pertext Transfer 0 dGT / HTP/L1V Host: net.acade Connection: kee Uggrade-Insecur Uger-Agent: Moz DUT: 1\n'n Accept: text/ht Purnoss: nesfet 0 e4 &d &c 93 499 0 2b c73 fd 40 0 ea e3 64 2e 00 0 fa 60 bb 3a 00 0 2f 31 2e 31 0d 0 fa 60 56 57 cb 32 0d 0 db 35 73 cb 35 2d 0 db 35 72 cb 35 2d 0 db 36 75 72 cb 35 2d 0 db 35 72 cb 35 2d 0 db 35 72 cb 35 2d 0 db 35 72 cb 35 2d 0 db 36 75	ol Protocol, Src Por Protocol rin my.lv/vh p-alive/vh e-Requests: l/r/n ml,application/shtmi ch/r/n cb 90 66 ba d6 be 00 40 06 00 00 c0 50 d5 6b ae 6a d6 00 47 45 54 20 2f 0a 48 6f 73 74 3a 6d 79 2e 6c 76 0d 6d 79 2e 6c 76 0d 6d 79 2e 16 76 55 70 67 72 61 64 65 52 65 71 75 65 73	<pre>rt: 25646, Dst Port: 6.1; Win64; x64) Ap 1+xml, application/aml fb 08 00 45 00 a6 13 02 55 fes 13 83 71 50 18d 20 48 54 50 20 48 54 55 20 48 64 54 50 20 48 64 54 50 20 48 64 54 50 20 48 64 56 20 48 64 56 20 49 66 73 65 ve- 74 73 38 20 31 cur 74 38 20 40 6f 74 38 20 40 6f</pre>	80, Seq: 1, pleWebKit/5 ;q=0.9,imag ·I······ ·0.0 ··························	37.36 (KHTVL, like Gecko) Chrome/76.0.3809.132 Safari/537.36\r\ e/webp,image/apng,*/*;q=0.8,application/signed-ewchange;v=b3\r\ E- U- gP- gP- tTP et. onn ali 1se : 1 ₩2	
000 010 020 030 030 030 030 030 030 030 030	ransmission Contr ypertext Transfer GGT / HTTP/L1 Host: net.acade Commetcion: kee Upgrade-Insecun User-Agent: Nor DUT: 1/Vin Accept: text/ht Purunsae: neefet 0 de 4 åd åc 93 49 00 bc 73 fd 40 0 åe 23 64 2e 00 0 fa 60 b3 a0 0 2f 31 2e 31 0d 0 61 63 61 64 65 0 65 63 74 69 67 67 65 00 40 85 0 73 73 73 65 0 37 5 72 65 2d 0 0 00 85 73 69 6c 6c 61	col Protocol, Src Por Protocol r/n my,lv/r/n =-Requests: 1/r/n illa/5.0 (Windows W ml,application/xhtmi ch/r/n cb 90 e6 ba d6 be cb 90 e6 ba d6 be co 40 06 00 00 co 50 d5 6b ae 6a da 00 47 45 54 20 2f 0a 48 6f 73 74 3a 6d 79 2e 6c 76 0d 6e 3a 20 6b 65 65 70 67 72 61 64 65 52 65 71 75 65 73 72 2d 41 67 65 73	rt: 25646, Dst Port: T 6.1; Win64; x64) Ap 1+vml,application/xml fb 08 00 45 00 a8 18 02 55 fes 18 37 75 56 20 66 65 74 2e /1. 00 43 67 66 6e aca 70 2d 61 66 69 ect 2d 49 66 73 65 ve- 74 38 20 31 cun 74 38 20 4d 6f 	80, Seq: 1, pleWebKit/5 ;;=0.9,imag ·I····· ·0.0: k ·j···· ····GE T / H' I··Ho st: n demy, lv··C ·Upgr ade-In e-Req uests ·Er-A gent:	87.36 (KHT×L, like Gecko) Chrome/76.0.3809.132 Safari/537.36\r\ e/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\ E- - - - - - - - - - - - - - - - - - -	
000 010 020 030 030 030 030 030 030 030 030 03	ransmission Contry pertext Transfer GGT / HTTP/L1 Host: net.acade Connection: kee Uggrade-Insecur Uger-Agent: Vor DIT: 1/Vin Accept: text/ht Purnnae: nefet 0 e4 8d 8c 95 49 02 bc 73 fd 40 6a e3 6d 2e 00 16 af 0 bb 3a 00 27 31 28 31 0d 61 63 61 64 65 65 63 74 69 61 63 75 72 65 24 0 40 85 73 65 0 40 8 57 35 7a 69 6c 6c 61 0 77 32 04 45 45	<pre>col Protocol, Src Por Protocol Prin my.lv/\n p-alive/r\n e-Requests: 1\r\n ml,application/xhtml chr\n cb 90 e6 ba d6 be 00 40 06 00 00 c0 50 45 6b ae 6a da 00 47 45 54 20 2f 0a 48 6f 73 74 3a 6d 79 2e 6c 76 0d 6e 3a 20 6b 65 65 70 67 72 61 64 65 52 65 71 75 65 73 72 2d 41 67 65 6e 2f 35 2e 30 20 28</pre>	rt: 25646, Dst Port: T 6.1; Win64; x64) Ap 1+vml,application/xml fb 08 00 45 00 a8 18 02 55 fes 18 37 75 56 20 66 65 74 2e /1. 00 43 67 66 6e aca 70 2d 61 66 69 ect 2d 49 66 73 65 ve- 74 38 20 31 cun 74 38 20 4d 6f 	80, Seq: 1, pleWebKit/5 ;q=0.9,imag ·I······· ·····GE T / H' I···Ho st: n. ······ keep ·upgr ade e-Req uests ser-A gent: la/5. 0 (Wi	87.36 (KHT×L, like Gecko) Chrome/76.0.3809.132 Safari/537.36\r\ e/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\ E- - - - - - - - - - - - - - - - - - -	n

2.2.5. Saving & Printing the Captured Information for next analysis

As a supporting document for lab assignment, you need to turn in a printout of the captured information. You can do this:

- or by Save Hex Dump Interesting Frame;
- or by make Screen Shots;
- or by Print from the File menu (mark "Selected packet only" and "All expanded").

Save Interesting frame for analysis

- a) Open the captured file from the previous paragraph (name.pcap).
- b) Find the first frame with the source protocol HTTP (interesting frame).
- c) From frame contecst menu (Right Mouse Button) select Copy → Copy Bytes as Hex Dump.
- d) Insert Hex Dump to Your Report or Save it Hex Dump as simple txt file. (Example in notepad.exe make: Edit → Paste and after File → Save → hex-dump.txt).
- e) For open Hex Dump file in Wireshark select File \rightarrow Import from Hex Dump...

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help Image: Comparison of the phone of the ph	
No. Time Source Destination Protocol Length Info 7 0.631856 85.254.142.227 192.168.19.2 TCP 62.80 - 2644 - 8 0.631883 192.168.19.2 85.254.142.227 TCP 68.0 6ET / HTT Mark/Unmark Packet Ctrl+M 192.168.19.2 TCP 60.80 - 2644 - Ignore/Unignore Packet Ctrl+D 192.168.19.2 TCP 192.168.19.2 TCP 60.80 - 2644 Ignore/Unignore Packet Ctrl+D 192.168.19.2 TCP 151.4.80 - 2644 - Set/Unset Time Reference Ctrl+T 192.168.19.2 TCP 151.4.80 - 2644 - Bett Resolved Name 192.168.19.2 TCP 151.4.80 - 2644 - - Packet Comment Ctrl+Alt+C 192.168.19.2 TCP 151.4.80 - 2644 - Bett Resolved Name - 192.168.19.2 TCP 151.4.80 - 2644 - - Prepare a Filter - - - - - - - - - - - - - <td></td>	
7 0.631856 85.254.142.227 192.168.19.2 TCP 62.80 - 2644 8 0.631883 192.168.19.2 85.254.142.227 TCP 54.26444 - 8 9 0.631883 192.168.19.2 85.254.142.227 TCP 54.26444 - 8 9 0.631853 192.168.19.2 TCP 54.26444 - 8 9 0.631853 192.168.19.2 TCP 54.26444 - 8 9 0.631853 192.168.19.2 TCP 60.80 - 2644 192.168.19.2 TCP 192.168.19.2 TCP 192.168.19.2 9 192.168.19.2 TCP 191.480 - 2644 192.168.19.2 TCP 191.480 - 2644 192.168.19.2 TCP 1514.80 - 2644 192.168.19.2 TCP 1514.80 - 2644 192.168.19.2 TCP 1514.80 - 2644 192.168.19.2 TCP 1514.80 - 2644 192.168.19.2 TCP 1514.80 - 2644 192.168.19.2 TCP 1514.80 - 2644 192.168.19.2 TCP 1514.80 - 2644 192.168.19.2 TCP 1514.80 - 2644 192.168.19.2 TCP 1514.80 - 2644 192.168.19.2 <td>ession 🛛 🕇</td>	ession 🛛 🕇
8 0.631883 192.168.19.2 85.254.142.227 TCP 54.26444 54.26443 54.26443 54.26443 54.26443 54.26443 54.26443 54.26443 54.26443 54.26443 54.26443 54.26443 56.264.142.227 TCP 151.4.80 2644 192.168.19.2 TCP 151.4.80 2.6443 58.254.142.227 TCP 151.4.80 2.6443 58.254.142.227 TCP 151.4.80 2.6443 58.254.142.227 TCP 151.4.80 2.6443 58.254.142.227 TCP 151.4.80 2.6444 192.168.19.2 TCP 151.4.80 2.6443 58.254.142.227 TCP 151.4.80 2.6443 58.254.142.227 TCP 151.4.80 2.6443 58.254.142.227 TCP 151.4.80 2.6443 58.254.142.227 TCP 151.4.80 2.64443 58.254.142.227	▲
Old G31948 192 168 19 2 85.254.142.227 HTTP 680 GET / HTT Mark/Unmark Packet Ctrl+M 192.168.19.2 TCP 60 80 - 2644 Ignore/Unignore Packet Ctrl+D 192.168.19.2 TCP 60 80 - 2644 Set/Unset Time Reference Ctrl+T 192.168.19.2 TCP 1514 80 - 2644 Packet Comment Ctrl+Shift+T 192.168.19.2 TCP 1514 80 - 2644 Packet Comment Ctrl+Alt+C 192.168.19.2 TCP 1514 80 - 2644 Box 254.142.227 TCP 1514 80 - 2644 -2644 192.168.19.2 TCP </td <td></td>	
Mark/Unmark Packet Ctrl+M Ignore/Unignore Packet Ctrl+D Set/Unset Time Reference Ctrl+T Time Shift Ctrl+Shift+T Packet Comment Ctrl+Alt+C Edit Resolved Name Ctrl+Alt+C Berly as Filter Conversation Filter Octorize Conversation SCTP Follow SCTP Protocol Preferences Protocol Preferences Protocol Preferences Amult Opecode As Conversation Filter Opecode As Converse trip to the with the second to the second t	
Ignore/Unignore Packet Ctrl+D Ignore/Unignore Packet Ctrl+D Set/Unset Time Reference Ctrl+T Time Shift Ctrl+Shift+T Packet Comment Ctrl+Alt+C Edit Resolved Name Ctrl+Alt+C Apply as Filter Prepare a Filter Octorize Conversation SCTP Follow SCTP Follow SCTP Protocol Preferences + Protocol Preferences + Off Protocol Preferences + Protocol Preferences + Decode As Ctrl+Alt Market	
Aginoroyongnoror data: Currb D Set/Unset Time Reference Ctrl+T Time Shift Ctrl+Shift+T Packet Comment Ctrl+Alt+C Edit Resolved Name 192.168.19.2 TCP 1514 80 - 2644 Apply as Filter 192.168.19.2 TCP 1514 80 - 2644 Apply as Filter 192.168.19.2 TCP 1514 80 - 2644 Apply as Filter 192.168.19.2 TCP 1514 80 - 2644 Apply as Filter 192.168.19.2 TCP 1514 80 - 2644 192.168.19.2 TCP 1514 80 - 2644 192.168.19.2 Prepare a Filter * 192.168.19.2 TCP 1514 80 - 2644 192.168.19.2 TCP 1514 80 - 2644 192.168.19.2 TCP 1514 80 - 2644 192.168.19.2 TCP 1514 80 - 2644 192.168.19.2 TCP 1514 80 - 2644 192.168.19.2 TCP 1514 80 - 2644 192.168.19.2 TCP 1514 80 - 2644 192.168.19.2 TCP 1514 80 - 2644 192.168.19.2 TCP 1514 80 - 2644 192.168.19.2 TCP 1514 80 - 2644 152 150 9	-
Time Shift Ctrl+Shift+T Packet Comment Ctrl+Alt+C Edit Resolved Name 192.168.19.2 TCP Apply as Filter 192.168.19.2 TCP Prepare a Filter 192.168.19.2 TCP Conversation Filter 192.168.19.2 TCP Conversation Filter 192.168.19.2 TCP Colorize Conversation 55.254.142.227 TCP SCTP 56.080 bytes captured (5440 bits) Pollow 55.680 bytes captured (5440 bits) Copy Summary as Text as CSV as CSV as YAML 50.1456.915	
Packet Comment Ctrl+Alt+C Packet Comment Ctrl+Alt+C Edit Resolved Name 192.168.19.2 TCP 1514 80 - 2644 Apply as Filter 192.168.19.2 TCP 1514 80 - 2644 Apply as Filter 192.168.19.2 TCP 1514 80 - 2644 Prepare a Filter 192.168.19.2 TCP 1514 80 - 2644 Conversation Filter 192.168.19.2 TCP 1514 80 - 2644 Colorize Conversation ts), 680 bytes captured (5440 bits) 199.168.19.2 HTP Colorize Conversation 5 5 600 45 00 100 100 SCTP ts), 680 bytes captured (5440 bits) 100 100 100 100 Copy Summary as Text as CSV as CSV as YAML as YAML Decode As the Detail Menuty data the Detail Menuty data the Detail Menuty data the Detail Menuty data	ί_
Edit Resolved Name 85.254.142.227 TCP 54.26443 - 8 Apply as Filter 192.168.19.2 TCP 1514.80 - 2644 Apply as Filter 192.168.19.2 TCP 1514.80 - 2644 Prepare a Filter 192.168.19.2 TCP 1514.80 - 2644 Conversation Filter 192.168.19.2 TCP 1514.80 - 2644 Colorize Conversation 192.168.19.2 HTTP 199 HTTP/1.1 Colorize Conversation 192.168.19.2 HTTP 199 HTTP/1.1 Colorize Conversation 192.168.19.2 192.168.19.2 192.168.19.2 Colorize Conversation 192.168.19.2 HTTP 199 HTTP/1.1 De fb 08 00 45 00 192.168.19.2 192.168.19.2 192.168.19.2 Of Copy 153 192.168.19.2 192.168.19.2 Of Copy 164.64 76 50 18 192.168.19.2 192.168.19.2 Of Protocol Preferences as CSV as CSV as YAML Of Decode As 192.168.19.16 192.168.19.16 192.168.19.16	[
Edit Resolved Name 192.168.19.2 TCP 1514 80 - 2644 Apply as Filter 192.168.19.2 TCP 1514 80 - 2644 Prepare a Filter 192.168.19.2 TCP 1514 80 - 2644 Original Conversation Filter 192.168.19.2 TCP 1514 80 - 2644 Conversation Filter 192.168.19.2 HTTP 199 HTTP/1.1 Colorize Conversation 192.168.19.2 HTTP 199 HTTP/1.1 SCTP 1 192.168.19.2 1000000000000000000000000000000000000	
Apply as Filter 192.168.19.2 TCP 1514 80 + 2644 Prepare a Filter 192.168.19.2 HTP 199 HTTP/1.1 Conversation Filter + 192.168.19.2 HTP 199 HTTP/1.1 Colorize Conversation + + + 192.168.19.2 + SCTP + + + + + + Follow +	
Apply as Filter • 192.168.19.2 HTTP 199 HTTP/1.1 Prepare a Filter • 192.168.19.2 HTTP 199 HTTP/1.1 • Conversation Filter • • • • • • • • • • • • • • •	L-
Prepare a Filter ************************************	aa -
Conversation Filter ts), 680 bytes captured (5440 bits) Colorize Conversation pe fb 08 00 45 00 ····I····E· Colorize Conversation pe fb 08 00 45 00 ····I····E· Colorize Conversation pe fb 08 00 45 00 ····I····E· Colorize Conversation pe fb 08 00 45 00 ····I····E· Colorize Conversation pe fb 08 00 45 00 ····I····E· Conversation pe fb 08 00 45 00 ····I····E· Conversation pe fb 08 00 45 00 ····I·····E· Conversation pe fb 08 00 45 00 ····I······E· Conversation pe fb 08 00 45 00 ····I······························	
Colorize Conversation > Oot SCTP Oot Follow Oot Follow Oot Follow Oot Copy Oot Copy Oot Copy Oot Protocol Preferences Oot Decode As Oot Chan Deduction Manual Mandama	
001 SCTP pe fb 08 00 45 00 \cdots I \cdots \cdots E 001 Follow pe fb 08 00 45 00 \cdots I \cdots \cdots E 001 Follow pe fb 08 00 45 00 \cdots I \cdots \cdots U 001 Follow pe fb 08 00 45 00 \cdots I \cdots \cdots U 001 Follow pe fb 08 00 45 00 \cdots I \cdots \cdots U 001 Follow pe fb 08 00 45 00 \cdots I \cdots \cdots U 001 Copy Summary as Text \cdots as CSV 001 Decode As max YAML The Delectric Net Worker	
00. Follow -<	
00: Pollow d6 4d 6d 76 50 18 eg(CP+++>+Vm/P+ 00: Copy Summary as Text 00: Protocol Preferences as CSV 00: Decode As as YAML	-
OO: Copy Summary as Text OO: Protocol Preferences as CSV OO: Decode As as YAML	
004 as CSV 005 Decode As 006 Decode As	
Ode Protocol Preferences Ode Decode As Ode Decode As	
001 Decode As	
chan Deduct to Man UP-dam An Ethen Children Children	
AND SHOW DEDUCTION WINDOW HISTING	
0090 0d 0a 55 73 65 72 2d 41 67 65	
00a0 7a 69 6c 6c 61 2f 35 2e 30 20 Copy Bytes as Hex + ASCII Dump	
00b0 77 73 20 4e 54 20 36 2e 31 3bas Hex Dump	
00c0 3b 20 78 36 34 29 20 41 70 70as Printable Text	
00d0 69 74 2f 35 33 37 2e 33 36 20as a Hex Stream	

2.2.6. Answer Questions

Using the first frame with the source protocol HTTP for answer the questions in your Lab Work Report Sheet (see below).

2.3. LW Report Sheet

To make the report of your observation easier and consistent, we have created Lab Work Report Sheet for lab assignment (see below).

A copy of the Lab Work Report sheets that contains:

- 1. The formation of an individual variant of the assignment;
- 2. Answered questions;
- 3. Hex dump interesting HTTP frame;
- 4. A Screen Shots or Printout of the supporting captured information.

Report send to teacher.

2.5. Grade.

Grade on 10 points: correctly formed individual variant, correctly made of all 10 assignments, hex-dump copies and captured information Screen Shots or Printout.

3. LAB WORK REPORT

Report for LW-01: Wireshark Introduction.

Student Name Surname	Student ID	Date			
Yuriy Li	12345	20.09.2025			

1. Assignment Variant

Instruction: The step by step formation of an individual variant of the assignment from the surname- name to the final number.	Example: <i>Li Yuriy → LIYU →</i> (12+09+25+21)mod26+1=16 → variant Nr.16 changed to (academy)

2. HTTP Frame Analyse

Nr	Question	Answer
1	Is the frame an outgoing or an incoming frame?	
2	What is the source MAC address of the data-link layer header in the frame?	
3	What is the destination MAC address of the data-link layer header in the frame?	
4	Source IP address of the network-layer header in the frame:	
5	Destination IP address of the network- layer header in the frame:	
6	Total number of bytes in the whole frame:	
7	Number of bytes in the Ethernet (data-link layer) header:	
8	Number of bytes in the IP header:	
9	Number of bytes in the TCP header:	
10	Total bytes in the message at the application layer ("payload"):	

3. A Hex Dump of the HTTP Captured Frame

Example:

0000	e4	8d	8c	93	49	cb	90	e6	ba	d6	be	fb	08	00	45	00
0010	02	46	2d	6e	40	00	40	06	00	00	c0	a8	13	02	55	fe
0020	8e	e3	67	4b	00	50	c 3	d5	2d	b0	d6	4d	90	3f	50	18
0030	fa	5f	ba	с4	00	00	47	45	54	20	2f	63	73	73	2f	6d
0040	<mark>79</mark>	63	73	73	2e	63	73	73	20	48	54	54	50	2f	31	2e
0050	31	0d	0a	48	6f	73	74	3a	20	6e	65	74	2e	61	63	<mark>61</mark>
0060	<mark>64</mark>	65	6d	79	2e	6c	76	0d	0a	43	6f	6e	6e	65	63	<mark>74</mark>
0070	<mark>69</mark>	6f	6e	3a	20	6b	65	65	70	2d	61	6c	69	76	65	0d
0080	<mark>0a</mark>	55	73	65	72	2d	41	67	65	6e	74	3a	20	4d	6f	7a
0090	<mark>69</mark>	6c	6c	61	2f	35	2e	30	20	28	57	69	6e	64	6f	77
00a0	<mark>73</mark>	20	4e	54	20	36	2e	31	3b	20	57	69	6e	36	34	3b
00b0	20	78	36	34	29	20	41	70	70	6c	65	57	65	62	4b	<mark>69</mark>
00c0	<mark>74</mark>	2f	35	33	37	2e	33	36	20	28	4b	48	54	4d	4c	2c
00d0	20	6c	69	6b	65	20	47	65	63	6b	6f	29	20	43	68	<mark>72</mark>
00e0	<mark>6f</mark>	6d	65	2f	37	36	2e	30	2e	33	38	30	39	2e	31	33
00f0	<mark>32</mark>	20	53	61	66	61	72	69	2f	35	33	37	2e	33	36	0d
0100	<mark>0a</mark>	44	4e	54	3a	20	31	0d	0a	41	63	63	65	70	74	3a
0110	<mark>20</mark>	74	65	78	74	2f	63	73	73	2c	2a	2f	2a	3b	71	3d
0120	<mark>30</mark>	2e	31	0d	0a	50	75	72	70	6f	73	65	3a	20	70	72
0130	<mark>65</mark>	66	65	74	63	68	0d	0a	52	65	66	65	72	65	72	3a
0140	20	68	74	74	70	3a	2f	2f	6e	65	74	2e	61	63	61	<mark>64</mark>
0150	<mark>65</mark>	6d	79	2e	6c	76	2f	0d	0a	41	63	63	65	70	74	2d
0160	<mark>45</mark>	6e	63	6f	64	69	6e	67	3a	20	67	7a	69	70	2c	20
0170	<mark>64</mark>	65	66	6c	61	74	65	0d	0a	41	63	63	65	70	74	2d
0180	<mark>4c</mark>	61	6e	67	75	61	67	65	3a	20	72	75	2c	65	6e	3b
0190	71	3d	30	2e	39	2c	6c	76	3b	71	3d	30	2e	38	2c	<mark>63</mark>
01a0	<mark>73</mark>	3b	71	3d	30	2e	37	0d	0a	43	6f	6f	6b	69	65	3a
01b0	20	5f	5f	75	74	6d	63	3d	32	36	37	31	31	32	30	31
01c0	37	3b	20	5f	5f	75	74	6d	7a	3d	32	36	37	31	31	32
01d0	<mark>30</mark>	31	37	2e	31	35	36	34	36	36	33	35	37	31	2e	31
01e0	<mark>2e</mark>	31	2e	75	74			73	72			64		72		<mark>63</mark>
01f0	74	29								3d						
0200		29								3d						
0210	<mark>3b</mark>									32		37		31		30
0220	31	37		32			33			30	31	33	33	2e	31	<mark>35</mark>
0230										31						
0240					31	35	36	38	30	33	31	37	38	36	2e	38
0250	0d	0a	0d	0a												

* Colorization remark: Data-link Network Transport Application layers

4. A Screenshots or Printout of the Captured HTTP Frame

4.1. Frame and Data-link layer (Ethernet)

<u>_</u> 1	et-pa1	.рсар				ĺ	<u> </u>	
File			Analyze Statistics Teleph					
$ \boxed{\blacksquare \ \textcircled{0} \ @ \ @ \ @ \ @ \ @ \ @ \ @ \ @ \ @ \ $								
No.	incep	Time	Source	Destination	Protocol	Length Info		
	9	0.631948	192.168.19.2	85.254.142.227	HTTP	680 GET / HTTP/1_	1 1	
-		0.646073	85.254.142.227	192.168.19.2	HTTP	199 HTTP/1.1 200_		
+	21	0.697355	192.168.19.2	85.254.142.227	HTTP	596 GET /css/myc_		
		0.698859	192.168.19.2	85.254.142.227	HTTP	578 GET /js/home_		
		0.701101	85.254.142.227	192.168.19.2	HTTP	606 HTTP/1.1 404_		
-	25	0.704313	85.254.142.227	192.168.19.2	HTTP	604 HTTP/1.1 404_	_	
<u>-</u>			on wire (5440 bits), (580 bytes captured (54	40 bits))		
			0e: Ethernet (1) 0 9, 2019 23:18:14.00	8977000 ELE Davlight	Time			
			his packet: 0.000000		TINE			
			060294.068977000 secor					
			previous captured fra		ids]			
	- [Ti	me delta from	previous displayed fr	ame: 0.000000000 seco				
			ence or first frame:	0.631948000 seconds]				
	:	me Number: 9						
	:	-) bytes (5440 bits)					
		ame is marked:	580 bytes (5440 bits) Ealcel					
		ame is ignored	-					
			me: eth:ethertype:ip:	tcp:http]				
		loring Rule Na						
	<u>ا</u> [Co	loring Rule St	ring: http://tcp.por					
			sustekC_d6:be:fb (90:a		Routerbo	o_93:49:cb (e4:8d:8c:	93:49:o	
			:erbo_93:49:cb (e4:8d:					
			_d6:be:fb (90:e6:ba:d0	s:be:fb)				
÷		e: IPv4 (0x080 et Protocol Va	ersion 4, Src: 192.160	3 19 2 Det· 85 254 14	12 227			
			l Protocol, Src Port:			Ack: 1, Len: 626		
		ext Transfer R			1 -	-		
•								
_	90 od	Sel Se 02 40 e	:b 90 e6 bad6 be fb	05 00 4E 00T		E .		
			0 40 05 00 00 c0 a8		· · · · · · · · ·		-	
00		e3 67 4b 00 5			· +> · Mmv			
003			0 47 45 54 20 2f 20	~	ET/HT			
004		31 2e 31 0d 0			o st: ne			
00	50 61	63 61 64 65 6		-	. $1 \vee \cdot \cdot \circ$	onn		
00		63 74 69 6f 6			keep-a			
00		65 0d 0a 55 7			r ade-In			
00		75 72 65 2d 5			q uests:		Ţ	
00		0a 55 73 65 7			A gent:		<u> </u>	
\bigcirc	E	ithernet (eth), 14 bγ	/tes	Packets: 38 · Displayed: 10 (2	6.3%) [,] Dro	opped: 0 (0.0%) Profile: De	efault 🛛	

4.2. Network layer (IP)

<u>_</u> n	iet-pa1	.рсар																				-	. 🗆	x
File	Edit	View Go) Capt	ure	Analy	ze Sta	tistics	Tel	epho	ny N	Wirele	ess	Tool	s Help)									
		۲	6	×	C	۹ 🗢	€	2	Ŷ.	<u>.</u>			Ð,	$\Theta_{\mathbf{c}}$	Q [
	http																	\times		•	Expre	ession.		+
No.		Time		s	iource				[Destin	ation	1			P	rotocol	Ler	ngth	Info					
-++	9	0.6319	948	1	92.1	68.19	. 2		٤	35.2	54.1	42.	227		Н	TTP		680	GET	/	HTTP.	/1_		
• †		0.6460				4.142				.92.						TTP					.1_2			Ţ
		0.6973				68.19				35.2			_			TTP		596	GET	10	ss/m	vc_ L		
	Etherr Interr 010 Dif Ide Fla - Fla - Fla - Hea - Hea - Sou Des	9: 680 net II, net Pro 00 . 0101 ferent 0000 0 al Len entific 0, 0, 0	Snc: tocol = Ver = Hea iated 0 = .00 = gth: (ation 4000, 000 00 ive: (TCP 1 ecksur hecksu 92.168 on: 85	Asu Ver rsio ader Diff Exp: 5666 : 0x. Don 000 (54 (6) n: 0 (6) n: 0 (6) n: 0 5,25	stek sion n: 4 Len; vice: ferer lici1 2d62 't fu 0000 tatu: .2 4,14;	C_d6:t 4, Sr 4, Sr gth: 2 s Fiel ntiate t Cong (1161 ragmen = Res = Don = Mor = Fra 0 [val s: Unv 2,227	<pre>det file re: 1 20 by d: 0 d Se d Se eesti 8) rt eerve idat rerif</pre>	o (9 192. rtes hx00 mvik on f inagn t or fied	0:e6 168. (5) (DS es loti it: ment ffse dis]	::ba 19.2 CP:: Code fica Not : Se : Not : Se : Not : Se : Not	:d6: 2, D cS0 poi tio set st st st set st	be: st: nt: n: L	fb), 85 CII: Def Iot	, Dst: .254.1 Not-E fault ECN-C	: R« 142 (0) Japa	buterb	o_9.	spor	t («	3)		:8c:9	93 : 4	·9∶€
		nission					Shc	Por	t: 2	6443	3, D	lst F	Port	t: 80,	, Se	eq: 1,	Ac	k: 1	., L«	en :	626			
	Hypert	text Tr	anste	r Pr	otoc	01							1											
-	_										_		1				_							
00		8d 8c															_							-
00:		9a 2d :e3 67												~		+> • Mm√								
		f0 bb														т / н								
00-		31 2e					74									st: ne								
00	50 61	63 61	64 65	5 6d	79.2	2e 6c	76	0d (ða 4	3 6f	6e	6e	ā	academ	ŋy.	$1 \vee \cdot \cdot c \in$	onn							
		63 74														keep-a								
00		5 65 Ød					64									ade-Ir								
00		75 72					65									uests								
00		0a 55 60 6a					65									gent:								
00		69 6c 73 20					3b									0 (⊎in 1; Win								
00		20 78					70									ppleWe								
00		74 2f					20									6 (KH1								-
		internet P							11							3%) [.] Dr		ed: 01	(0.0%	6)	Profi	le: Def	fault	
																				. 11				- ///

4.3. Transport layer (TCP)

🔏 net-pa1.pcap				_ 🗆 ×					
	e Analyze Statistics Telepl	hony Wireless Tools Help							
🥖 🔳 🔬 💿 🔰 🚠 🗙	🕻 🖸 । ९ 👄 🔿 聲 🕧	୍ 🕹 📑 🔳 🔍 ପ୍ ସ୍	. 99						
📙 http			×	Expression +					
No. Time	Source	Destination	Protocol Length	Info					
9 0.631948	192.168.19.2	85.254.142.227	HTTP 680	GET / HTTP/1_					
+ 19 0.646073	85.254.142.227	192.168.19.2		HTTP/1.1 200_					
				GET /css/mvc_					
<pre>Provide Control Protocol Protocol</pre>									
TCP payload (626 ⊡ ⊞ Hypertext Transfer I									
I supercexc transfer i	Prococol								
	al oo ac ha de ha dh	05 00 4E 00 T	-						
0000 e4 8d 8c 93 49 0 0010 02 9a 2d 62 40 0	cb 90 e6 bad6 be fb 30 40 06 00 00 c0 a8		· · · · · · · E ·	_					
0020 8e e3 67 4b 00 5			• +> •Mm∨P •						
0030 fa f0 bb 18 00 0			ЕТ/НТТР						
0040 2f 31 2e 31 0d 0	0a 48 6f 73 74 3a 20		o st: net.						
0050 61 63 61 64 65 6			. lv··Conn						
0060 65 63 74 69 6f (keep-ali						
0070 76 65 0d 0a 55 7			r ade-Inse						
0080 63 75 72 65 2d 5 0090 0d 0a 55 73 65 7			q uests: 1 A gent: Mo						
00a0 7a 69 6c 6c 61 2			. 0 (Windo						
00b0 77 73 20 4e 54 2			. 1; Win64						
00c0 3b 20 78 36 34 2			A ppleWebK						
00d0 69 74 2f 35 33 3	37 2e 33 36 20 28 4b		3 6 (KHTML	<u> </u>					
📔 🔘 🏹 🛛 Transmission Control	Protocol (tcp), 20 bytes	Packets: 38 · Displayed: 10 (2	6.3%) [,] Dropped: 0	(0.0%) Profile: Default //					

4.4. Application layer (HTTP)

🖉 пе	et-pa1	.рсар					_ 🗆 ×
File	Edit V		Analyze Statistics Teleph				
		💿 퉬 🔚 🗙	रे 🖸 ९ 🗢 🗢 🕾 🕧	<u>.</u>			
<mark> </mark> h	ttp						Expression +
No.		Time	Source	Destination	Protocol	Length Info	^
		0.631948	192.168.19.2	85.254.142.227	HTTP	680 GET / H	
t		0.646073	85.254.142.227	192.168.19.2 85.254.142.227	HTTP	199 HTTP/1.	
Trial I		0.697355	192.168.19.2	580 bytes captured (54	HTTP	596 GET /cs	SS/m/C=
	thern Intern Inansm Jypert	net II, Shc: As net Protocol V	sustekC_d6:be:fb (90: ersion 4, Src: 192.16 l Protocol, Src Port: Protocol \n	e6:ba:d6:be:fb), Dst: 8.19.2, Dst: 85.254.14 26443, Dst Port: 80,	Routerbo 42.227	o_93:49:cb (e4	
E	Con Upg Use DIIT Acc Pur Acc Coo Coo Coo Coo Coo Coo Coo Coo Coo C	nection: keep made-Insecure r-Agent: Moiii : 1\r\n ept: text/htm pose: prefetch ept-Encoding: ept-Language: kie:utmc=20 Cookie pair: _ Cookie pair: _ n	-alive\r\n -Requests: 1\r\n lla/5.0 (Windows NT 6 l,application/xhtml+xr h\r\n gzip, deflate\r\n ru,en;q=0.9,1v;q=0.8 57112017;utmz=26711 57112017;utmz=26711 _utmz=267112017.1564(_utmz=267112017.2013(_utma=267112017.2013(_utma=267112017.2013(_utma=267112017.2013(_utma=267112017.2013(_utma=267112017.2013(_utma=267112017.2013(_utma=267112017.2013(_utma=267112017.2013()	12017.1564663571.1.1.0 563571.1.1.utmcsr=(dir 560133.1564663571.1567	0.9,image utmcsr=(« rect) utm	e/webp,image/a direct) utmccn nccn=(direct)	ppng,*/*;q=0.8 =(direct) utm
4							Þ
002 003 004 005	0 02 0 8e 0 fa 0 2f 0 61 0 65	9a 2d 62 40 6 e3 67 4b 00 5 f0 bb 18 00 6 31 2e 31 0d 6 63 61 64 65 6 63 74 69 6f 6	cb 90 e6 ba d6 be fb 30 40 06 00 00 c0 a8 50 c3 d5 2b 3e d6 4d 30 47 45 54 20 2f 20 30 48 6f 73 74 3a 20 30 48 6f 73 74 3a 20 56 79 2e 6c 76 0d 0a 56 3a 20 6b 65 65 70 70 67 72 61 64 65 2d	$\begin{array}{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr$) iE T / HT lo st: ne v. lv··Co keep-a	.U. ∕P· TP ≇t. Donn Dli	
008 009	0 63 0 0d	75 72 65 2d 5 0a 55 73 65 7	52 65 71 75 65 73 74 72 2d 41 67 65 6e 74	73 3a 20 31 cure-Ra 3a 20 4d 6f ··User-	gr ade-In eq uests: A gent: 5. 0 (Win	: 1 Mo	
007 008	0 63 0 0d 0 7a	75 72 65 2d 5 0a 55 73 65 7 69 6c 6c 61 2	52 65 71 75 65 73 74	73 3a 20 31 cure-Re 3a 20 4d 6f · User- 69 6e 64 6f cilla/5	eq uests:	: 1 Mo ndo	Ţ