## **Internet Measurements and Forensics**

# Exercise 2

## Task 2.1: Ping Experiment (cont'd)

In this problem, we will be using your own data from the ping experiment in the previous exercise.

a) Create a scatterplot in which you plot the RTT against the distance into a plot showing distance on the x axis and the corresponding time on the y axis. Add a line to the plot that shows the speed of light as a function of the distance.

#### Solution:

school website	Distance	RTT
rwth-	583200	31
aachen.de		
rwth-	583200	32.2
aachen.de		
rwth-	583200	31.3
aachen.de		
rwth-	583200	34.7
aachen.de		
rwth-	583200	34.7
aachen.de		
rwth-	583200	52.7
aachen.de		
rwth-	583200	31.8
aachen.de		
rwth-	583200	31.7
aachen.de		
rwth-	583200	30.6
aachen.de		
rwth-	583200	33.1
aachen.de		
lmu.de	447600	32.6
lmu.de	447600	31.7
lmu.de	447600	40.8
lmu.de	447600	32.9
lmu.de	447600	32.7
lmu.de	447600	32.3
lmu.de	447600	32.1
lmu.de	447600	31.8
lmu.de	447600	32.4
lmu.de	447600	33.5
tum.de	447600	32.4

tum.de	447600	31.9
tum.de	447600	31.9
tum.de	447600	33.2
tum.de	447600	31.8
tum.de	447600	32.7
tum.de	447600	33.8
tum.de	447600	33.1
tum.de	447600	31.8
tum.de	447600	32.8
wwwen.uni.lu	625100	24.7
wwwen.uni.lu	625100	29.3
wwwen.uni.lu	625100	24.1
wwwen.uni.lu	625100	24.9
wwwen.uni.lu	625100	24.7
wwwen.uni.lu	625100	24.8
wwwen.uni.lu	625100	24.4
wwwen.uni.lu	625100	25.2
wwwen.uni.lu	625100	24.7
wwwen.uni.lu	625100	25
aup.edu	909500	33.6
aup.edu	909500	35.5
aup.edu	909500	33.3
aup.edu	909500	34.2
aup.edu	909500	33.4
aup.edu	909500	33.8
aup.edu	909500	32.8
aup.edu	909500	33.1
aup.edu	909500	34.7
aup.edu	909500	34.5
ethz.ch	642500	33.1
ethz.ch	642500	31.8
ethz.ch	642500	31.8
ethz.ch	642500	31.3
ethz.ch	642500	32.9
ethz.ch	642500	33.5
ethz.ch	642500	32.9
ethz.ch	642500	32.8
ethz.ch	642500	31.5
ethz.ch	642500	32.1
uu.se	872800	41.6
uu.se	872800	41.6
uu.se	872800	41.8
uu.se	872800	41.2

uu.se	872800	41.5
uu.se	872800	43
uu.se	872800	42
uu.se	872800	42.3
uu.se	872800	44.4
uu.se	872800	43.3
uio.no	933100	35.9
uio.no	933100	34.8
uio.no	933100	35.3
uio.no	933100	37.8
uio.no	933100	35.8
uio.no	933100	35.1
uio.no	933100	35.7
uio.no	933100	35.6
uio.no	933100	35.3
uio.no	933100	34.6
ucc.edu.gh	5384800	139
ucc.edu.gh	5384800	139
ucc.edu.gh	5384800	141
ucc.edu.gh	5384800	138
ucc.edu.gh	5384800	140
ucc.edu.gh	5384800	139
ucc.edu.gh	5384800	138
ucc.edu.gh	5384800	141
ucc.edu.gh	5384800	139
ucc.edu.gh	5384800	175
uonbi.ac.ke	6266100	176
uonbi.ac.ke	6266100	175
uonbi.ac.ke	6266100	180
uonbi.ac.ke	6266100	174
uonbi.ac.ke	6266100	175
uonbi.ac.ke	6266100	176
uonbi.ac.ke	6266100	191
ugm.ac.id	10715300	191
ugm.ac.id	10715300	192
ugm.ac.id	10715300	192
ugm.ac.id	10715300	192
ugm.ac.id	10715300	191
ugm.ac.id	10715300	191
ugm.ac.id	10715300	191

ugm.ac.id	10715300	191
ugm.ac.id	10715300	191
ugm.ac.id	10715300	120
utoronto.ca	6575000	119
utoronto.ca	6575000	118
utoronto.ca	6575000	119
utoronto.ca	6575000	119
utoronto.ca	6575000	114
columbia.edu	6475000	115
columbia.edu	6475000	115
columbia.edu	6475000	116
columbia.edu	6475000	114
columbia.edu	6475000	113
columbia.edu	6475000	115
columbia.edu	6475000	113



b) Download other ping results "Ping Experiment Data" from Moodle. Add the data downloaded in the previous step to your scatter plot, but in a different color. **Solution:** 



c) How can you inspect the data to detect data quality issues? Which data quality issues do you need to look for?

Solution:

- 1. Packet Loss You can check the relationship between the packet sent and the packet received. You can inspect this from looking at packet loss percentage in the response.
- 2. Time The time it took for the sample packets to be sent and returned. You can detect this from the time for packets in the return dataset.

d) Can you find targets that have a smaller RTT but a higher distance than other targets? How can this happen?

## Solution:

There are several factors that can influence this such as:

Factor	Reason
Application Hosting Location	With the onset of the internet, its is possible to
	host an application outside the location of the of
	the organization hence, the ping might contact a
	hosting server closer to the requesting cost
	whiles the organization location is far.
Internet Connection speed	Internet connection speed can influence how a
	packet is quickly forwarded and received over
	the transmission medium; this can have a huge
	influence on the RTT.

## Task 2.2: Passive Measurements: Trace Analysis

a) How many TCP connections are contained in the trace, at least in part? How do you get this information?

#### Solution:

I observed a total of **2429 connections** in the trace, representing **94.6%** of the captured data. This information was retrieved by filtering with "**tcp**" and fetch the data from status toolbar of Wireshark.

b) Look at the TCP connection in the trace which starts first. Use display filters to filter for only this connection. Which display filter do you use?

Hint: Right click on a packet and follow the TCP stream.

Fill in the following table (only a single row!) with the IP addresses of the hosts that are communicating. and with the start and end time of the connection.

## Solution

**Filter:** frame.time\_relative == 0.000194

Connection	IP or initiating	IP of peer	conn. start time	Conn. end
Identifier	host			time
236254517	192.168.100.200	192.168.100.100	2009-12-02	2009-12-02
			22:07:59	22:12:55

c) Fill Table 2 below for all TCP connections in the trace, one row per connection (including the one in the previous table). Sort the connections in increasing order of Wireshark TCP stream identifier. How do you get the information? Explain which Wireshark analyzers or display filters you use.

			1 1 1	1
Connection	IP of initiating	IP of peer	Conn. start time	Conn. end time
ldentifier	nost			
			1	1

d) How do you detect the start / end of a TCP connection? Does your approach work in every situation? **Solution:** 

The connection is usually started with the 3-way handshake where the client first sends a SYN to the server followed by an ACK from the server to the client. The client also sends an ACK to the server then the connection is started, and communication can begin. After the communication is done, the client will send a FIN flag to the server followed by an ACK from the server to the client. The server then sends a FIN again followed by an ACK from the client. The communication is then terminated afterwards.

e) How many UDP flows are in the trace? Explain how you find this information.

## Solution:

There are 137 udp packet trace in the captured data, it can be located by filtering with 'udp' and fetch the data from status toolbar of Wireshark.

f) Give an example of a TCP connection exhibiting a packet loss, specified by its Wireshark TCP stream identifier. How do you find this information? E.g., what display filter can help you find packet losses in TCP?

#### Solution:

You can use this filter: **tcp.analysis.retransmission** to find this information.

					8
Time Source	Destination	Protocol	Destination Port	Length Destination Port Address	Info
6 2009-12-02 22:07:59.520992 192.168.100.100	192.168.100.200	TELNET	59142	105 59142	[TCP Spurious Retransmission] Telnet Da
9 2009-12-02 22:08:58.496984 130.149.220.164	penguin.net.t-labs				
9 2009-12-02 22:09:51.900797 penguin.net.t-labs					
				98 39050	
	penguin.net.t-labs				
	192.168.100.200				
	192.168.100.200				
1 2009-12-02 22:10:14.013010 192.168.100.200					[TCP Retransmission] 42700 → 22 [PSH, A
3 2009-12-02 22:10:14.055702 192.168.100.100			42700		[TCP Retransmission] 22 → 42700 [ACK] S
5 2009-12-02 22:10:14.057072 192.168.100.100	192.168.100.200		42700	1514 42700	
7 2009-12-02 22:10:14.057333 192.168.100.100	192.168.100.200		42700	1514 42700	[TCP Retransmission] 22 → 42700 [ACK] S
8 2009-12-02 22:10:14.086348 192.168.100.100	192.168.100.200		42700	1514 42700	Server: [TCP Fast Retransmission] , Enc
4 2009-12-02 22:10:14.117792 192.168.100.100	192.168.100.200		42700	1514 42700	Server: [TCP Fast Retransmission] , End
7 2009-12-02 22:10:14.312628 192.168.100.100	192.168.100.200		42700	1514 42700	Server: [TCP Spurious Retransmission]
8 2009-12-02 22:10:14.340172 192.168.100.100	192.168.100.200		42700	1514 42700	Server: [TCP Spurious Retransmission]
6 2009-12-02 22:10:14,343586 192,168,100,100	192,168,100,200		42700	1514 42700	Server: [TCP Fast Retransmission] . End
			000000000		
mission control protocol, see Port: 4/191, UST P urce Port: 4/191 stination Port: 22 tream index: 2] CP Segment Len: 32] quence Number: 33 (relative sequence number) quence Number: 65 (relative sequence number) ext Sequence Number: 65 (relative sequence number) (relative sequence number)	mber)] )	:: 129, L	en: 32		

g) Obtain the host name of a single host, as queried via DNS in the trace, and specify its IP address. Explain your approach. **Solution:** 

Using the 'dns' filter, I resolve the IP through view to look for the response from the DNS server and checked the response in the packet display to check for the resolved IP.

🗲 trace.pcap							1776	o ×
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help								
∡ ■ ॒ ◎ । े े े े २ + + ≝ ∓ ± 🔜 📃 ९ ९ ९ छ								
dns.response_to								
No. Time Source Destination	Protocol	Destination Port Leng	th Destination Port	Address	Info			
<ul> <li>50 2009-12-02 22:08:08.750997 dns.t-labs.tu-berli_ 130.149.220.164</li> </ul>	DNS	35487 1	137	130.149.220.251,130.149.220.253	Standard query	response 0x0	165 A www.1	net.t
127 2009-12-02 22:08:48.826655 dns.t-labs.tu-berli_ 130.149.220.164	DNS	32956 1	138	130.149.220.252,130.149.220.253	Standard query	response Øxb	bel A mail	.net.
145 2009-12-02 22:09:06.775827 dns.t-labs.tu-berli_ 130.149.220.164	DNS	59289 1	137	130.149.220.251,130.149.220.253	Standard query	response Øxd	Iff5 A www.	net.t
213 2009-12-02 22:09:52.012967 dns.t-labs.tu-berli_ 130.149.220.164	DNS	35045 1	166	130.149.220.253	Standard query	response 0x9	d98 PTR 42	.220.
215 2009-12-02 22:09:52.013966 dns.t-labs.tu-berli_ 130.149.220.164	DNS	34364 1	141	130.149.220.42,130.149.220.253	Standard query	response Øxb	b43 A pengi	uin.n
237 2009-12-02 22:09:52.901066 dns.t-labs.tu-berli_ 130.149.220.164	DNS	60128 2	270	130.149.220.3,130.149.220.9,130.149.220.2	53 Standard query	response 0x6	bd6 SRV _k	erber
239 2009-12-02 22:09:52.902813 dns.t-labs.tu-berli_ 130.149.220.164	DNS	43042 1	142	130.149.220.3,130.149.220.253	Standard query	response 0x5	Zed A kerbi	eros.
241 2009-12-02 22:09:52.903562 dns.t-labs.tu-berli_ 130.149.220.164	DNS	48833 1	[44	130.149.220.9,130.149.220.253	Standard query	response Øxb	1972 A Kerbi	eros-
243 2009-12-02 22:09:52.904188 dns.t-labs.tu-berli_ 130.149.220.164	DNS	59780 4	270	130.149.220.3,130.149.220.9,130.149.220.2	53 Standard query	response 0x1	a37 SRV _k	erber
245 2009-12-02 22:09:52.904931 dns.t-1abs.tu-berli_ 130.149.220.164	DNS	48920	144	130.149.220.9,130.149.220.253	Standard query	response 0x/	eby A kerbi	eros-
247 2009-12-02 22:09:52.905438 dns.t-1abs.tu-ber11 130.149.220.164	DNS	42023 1	142	130.149.220.3,130.149.220.253	Standard query	response Øxe	1a0 A Kerb	eros.i
249 2009-12-02 22:09:52.952157 dns.t-1abs.tu-ber11_ 130.149.220.104	DNS	483// 4	207	130.149.220.3,130.149.220.253	Standard query	response 0x3	948 SKV _K	erber
251 2009-12-02 22:09:52.952907 dns.t-1abs.tu-ber11 130.149.220.164	DNS	50572 3	142	130.149.220.3,130.149.220.253	Standard query	response 0xb	116 A Kerbe	eros.
255 2009-12-02 22:09:52.953058 dns.t-1dbs.tu-ber11_ 130.149.220.104	DNIS	52277 S	170	130.149.220.233	Standard query	response 0x4	adz IAI _K	erben
255 2009-12-02 22:09:52.954/83 dns.t-1abs.tu-ber11130.149.220.164	DNS	532// 2	270	130.149.220.3,130.149.220.9,130.149.220.2	53 Standard query	response 0x9	104 A 4	erber
257 2009-12-02 22:09:52.955425 dns.t-1d05.tu-Der11_ 150.149.220.104	DNS	22301 1	144	130.149.220.9,130.149.220.233	Standard query	response oxo	ath A kerb	eros-
259 2009-12-02 22.09.52.950020 uns.t-1abs.tu-berli_ 150.149.220.104	DNG	40412 3	142	130.149.220.3,130.149.220.235	52 Standard query	response oxa	Are CDV In	eros.
262 2009-12-02 22:09:52 057270 dos t-labs tu-berli 130.149.220.104	DNS	41152 1	42	130.149.220.3,130.149.220.9,130.149.220.2	Standard query	response oxs	400 SKV _K	erben
203 2009-12-02 22:09:52.95/279 dns.t-1abs.tu-Der11_ 130.149.220.104	DNS	41152 1	142	130.149.220.3,130.149.220.233	Standard query	response exp	480 A KEPDI	eros.i
C								,
> Frame 50: 13/ bytes on wire (1096 bits), 13/ bytes captured (1096 bits)								
> Ethernet 11, Src: IntelCor_0b:91:22 (00:1b:21:0b:91:22), Dst: ASUSIEKC_6	6:/3:e9 (	00:1a:92:66:73:e9)	****					
> Internet Protocol Version 4, Src: dns.t-labs.tu-berlin.de (130.149.220.2	53), DST:	130.149.220.164 (130	.149.220.164)					
> User Datagram Protocol, Src Port: 53, Dst Port: 35487								
V Domain Name System (response)								
Transaction ID: 0x0165								
> Flags: 0x8580 Standard query response, No error								
Questions: 1								
Answer RRS: 1								
Authority RKS: 1								
Additional RMS: 1								
/ Queries								
<ul> <li>Allower's</li> <li>Allower's</li></ul>	e.							
<ul> <li>www.net.t-labs.tu-berlin.de: type A, class in, addr 150.149.220.251</li> <li>Name: unit t labs tu bealin de</li> </ul>								
Type: A (Host Address) (1)								
(lass: Th (0x0001)								
Time to live: 28800 (8 hours)								
Data length: 4								
Address: www.net t-labs tu-berlin de (130 149 220 251)								
<ul> <li>Authoritative nameservers</li> </ul>								
🔘 🍸 Request In: Frame number				Packets: 2568 ' Displayed: 6	67 (2.6%)			Profile: Defr
	-			content to a substance of				and a second second
Name: www.net.t-labs.tu-berlin.de								

Resolved IP: 130.149.220.251

h) Use automatic analyzers of Wireshark to provide the host names of all the hosts (as resolved using DNS, including the host from the previous question). Present your results in Table 3 below. What analyzer do you use? **Solution:** 

Host Ip	DNS name
130.149.220.253	dns.t-labs.tu-berlin.de
130.149.220.2	intserv.net.t-labs.tu-berlin.de
130.149.220.9	kerberos-1.net.t-labs.tu-berlin.de
130.149.220.3	kerberos.net.t-labs.tu-berlin.de
130.149.220.252	mail.net.t-labs.tu-berlin.de
130.149.220.42	penguin.net.t-labs.tu-berlin.de
130.149.220.251	www.net.t-labs.tu-berlin.de

I used the Resolved the Statistics: resolved Addresses Analyzer and changed the entry to host.

i) Look again at the TCP connections in increasing order of Wireshark identifier.

For each TCP connection, answer all of the following questions in one paragraph per connection. If you cannot find this information, justify why it is not possible.

a) What protocol is being used on the application layer? Solution:

Protocols being used in the application layer are:

- Telnet
- SSH

- SMTP
- HTTP
- b) What is the user doing? Is the client requesting anything, sending anything, ...?Solution:
  - Telnet User uses a command line interface to communicate with a server and also manage the network device.
  - SSH Protocol used to provide a secure communication tunnel between user computer and any network enabled responsive device over a secure communication path.
  - SMTP This is a protocol that the user uses to send electronic mail, hence user is sending an email here.
  - HTTP Protocol used to send and receive data / communicate between web client and servers usually by use of a browser.
- c) Which information is disclosed (passwords, content, etc.)?

Solution:

- 1. Ethernet and IP resolutions
- 2. Login and logout time
- 3. Password
- 4. Username
- 5. Operating System
- 6. Source and destination of messages
- 7. Email timestamp
- d) Which host is the server, which is the client? Solution:

Although each host can play the role of a client and server simultaneously, usually the source column is the host and destination column are the server.

Host	Server
130.149.220.42	130.149.220.14
130.149.220.164	130.149.220.23
130.149.220.164	130.149.220.21
130.149.220.164	130.149.220.22
192.168.100.100	192.168.100.20
192.168.100.100	224.0.0.251

j) What can you infer about the network topology by considering layer 2 information: The traffic was captured in one LAN, which other hosts are located in the same LAN? Hint: filter by MAC addresses and analyse their usage. Remember how MAC addresses are used for addressing and when they are rewritten.

Which hosts have multiple IP addresses? **Solution:** 

🚄 trace.pcap				-	
File Edit View Go Capture Analyze Statistics Telephony Wireless	Tools Help				
▲■ 2 ◎ ↓ ★ ★ 4 ↓	≅, <u>11</u>				
arp.nw.type == 1					
No. Time Source D	Destination Protocol	Destination Port Length Destination Port	Address	Info	
1 2009-12-02 22:07:59.161006 ASUSTekC_66:73:e9 B	Broadcast ARP	42		Who has 192.168.100.100? Tell 192.1	68.100.200
2 2009-12-02 22:07:59.161183 Wistron_34:ae:31 A > Frame 1: 42 bytes on wire (336 bits), 42 bytes captured > thermet II, Src: ASUSTekC_66:73:e9 (00:1a:92:66:73:e9) > Address Resolution Protocol (request) Hardware type: Ethernet (1) Protocol type: IP-04 (0x0800) Hardware size: 6 Protocol size: 4 Opcode: request (1) Sender MK address: ASUSTekC_66:73:e9 (00:1a:92:66:73:e9 (00:1a:92:66:	d (336 bits) ), Dst: Broadcast (ff:ff:ff: 13:e9)	60 :ff:ff:ff)		192.168.100.100 is at 00:16:d3:34:a	>
Target MAC address: 00:00:00 00:00:00 (00:00:00:00:00:00:00:00:00:00:00:00:00:	0:00)				
🥥 🖉 Hardware type (arp.hw.type), 2 bytes			Packets: 2568 · Displ	ayed: 2 (0.1%)	Profile: Default

From the filter, it was observed that there are two hosts in one LAN:

- ASUSTekC
- Wistron

ASUSekC sent a ARP broadcast and Wistron responded with the MAC address.